在思科防御协调器中通过 云交付的防火墙管理中心 管理防火墙威胁防御

首次发布日期: 2022 年 6 月 28 日

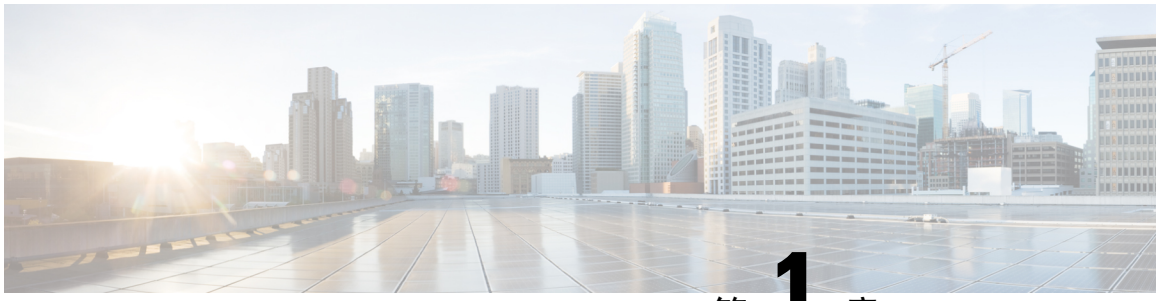
上次修改日期: 2022 年 7 月 22 日

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

目录

第 部分

使用云交付的防火墙管理中心来管理 Cisco Secure Firewall Threat Defense



第 1 章

使用云交付的防火墙管理中心来管理 Cisco Secure Firewall Threat Defense 设备

云交付的防火墙管理中心是一种软件即服务 (SaaS) 产品，可管理 Cisco Secure Firewall Threat Defense 并通过思科防御协调器 (CDO) 交付。云交付的防火墙管理中心提供了许多与本地 Cisco Secure Firewall Management Center 相同的功能。

云交付的防火墙管理中心与本 Cisco Secure Firewall Management Center 具有相同的外观和行为，并且它们都使用相同的 FMC API。

作为 SaaS 产品，思科防御协调器 (CDO) 运营团队负责云交付的防火墙管理中心软件的部署与维护。随着新功能的推出，CDO 运营团队会为您更新 CDO 租户的云交付的防火墙管理中心。

迁移向导可帮助您将 Cisco Secure Firewall Threat Defense 设备从本地 Cisco Secure Firewall Management Center 迁移到云交付的防火墙管理中心。设备必须安装威胁防御软件版本 7.0.3 或更高版本 7.0.x，或者安装版本 7.2 或更高版本才能进行迁移。不支持威胁防御 7.1 版本。

在 CDO 中使用熟悉的流程（例如使用设备序列号载入设备或使用包含注册密钥的 CLI 命令）来载入安全防火墙威胁防御设备。在载入设备后，将同时显示在 CDO 和云交付的防火墙管理中心中，但是，您可以在云交付的防火墙管理中心中配置设备。

CDO 可为其通过数据接口管理的威胁防御设备提供高可用性支持。运行 7.2 或更高版本软件的设备支持此功能。

您可以使用安全分析和日志记录 (SaaS) 或安全分析和日志记录（本地）分析已载入的威胁防御设备生成的系统日志事件。SaaS 版本会将事件存储在云端，您可以在 CDO 中查看事件。本地版本会将事件存储在本地安全网络分析设备中，而分析在本地安全防火墙管理中心完成。在这两种情况下，就像今天的本地 FMC 一样，您仍然可以直接从传感器将日志发送到您选择的日志收集器。

云交付的防火墙管理中心的许可证是按设备管理的许可证，而云交付的防火墙管理中心本身不需要许可证。现有的安全防火墙威胁防御设备会重复使用其现有的智能许可证，而新的安全防火墙威胁防御设备会为 FTD 上实施的每项功能调配新的智能许可证。

现有客户可以继续使用 CDO 来管理其他设备类型，例如 Cisco Secure Firewall ASA、Meraki、思科 IOS 设备、Cisco Secure Firewall Cloud Native、Umbrella 和 AWS 虚拟私有云。如果您使用 CDO 管理已配置为通过 Firepower 设备管理器进行本地管理的安全防火墙威胁防御设备，则也可以继续使用 CDO 对其进行管理。

要了解如何在租户上调配云交付的防火墙管理中心，请参阅为您的 CDO 租户请求 云交付的防火墙管理中心 ， 第 2 页。

为您的 CDO 租户请求 云交付的防火墙管理中心

如果要使用 云交付的防火墙管理中心 来管理 Cisco Secure Firewall Threat Defense 设备，您可以请求在租户上调配 云交付的防火墙管理中心。

Procedure

步骤 1 在 CDO 菜单栏中，点击**工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。

步骤 2 点击 **请求 FMC**。

步骤 3 点击**发送请求 (Send Request)** 以确认您的云交付的防火墙管理中心 请求。

在您确认后，请求会被发送到CDO团队以调配云交付的防火墙管理中心。在调配后，您将收到一封从 *cdo-alert@cisco.com* 发送到您注册电子邮箱的邮件。您还将在CDO通知面板和已配置传入Webhook的应用上收到**云交付的防火墙管理中心 就绪**通知。有关详细信息，请参阅通知设置。

然后，您可以将 威胁防御 设备载入 云交付的防火墙管理中心 并进行管理。

硬件和软件支持

云交付的防火墙管理中心 支持 Cisco Secure Firewall Threat Defense版本 7.0.3 和 7.0.x 版本 7.0.3 及更高版本以及版本 7.2 及更高版本，可安装在许多不同的 Firepower 硬件设备或虚拟机上。

云交付的防火墙管理中心 不支持任何版本的 Cisco Secure Firewall Threat Defense版本 7.1。

有关详细信息，请参阅 Firepower 威胁防御支持说明。

思科防御协调器平台维护计划

思科防御协调器维护计划

CDO 会每周更新其平台，提供新功能和质量改进。根据此计划，更新可在 3 小时内完成。

大多数情况下，更新会在星期四完成，但如有必要，也可以安排在星期五和星期日进行维护。

表 *1: CDO* 维护时间表

星期	时间 （24 小时制）
星期四	09:00 UTC - 12:00 UTC
星期五	09:00 UTC - 12:00 UTC
星期日	09:00 UTC - 12:00 UTC

在此维护期间，您仍然可以访问您的租户，并且如果您有 云交付的防火墙管理中心，也可以访问该平台。此外，您已载入CDO的设备将继续执行其安全策略。

注释 我们建议您在维护期间不要使用 CDO 来在其管理的设备上部署配置更改。

如果发生阻止 CDO 或 云交付的防火墙管理中心 进行通信的故障，则会尽快在所有受影响的租户上解决该故障，即使并非是在维护时间窗口之内。

云交付的防火墙管理中心维护时间表

在CDO更新云交付的防火墙管理中心环境前大约1周通知在租户上部署了云交付的防火墙管理中心的客户。通过邮件通知租户的超级管理员和管理员用户。CDO还会在其主页上显示一个横幅，通知所有用户即将发布的更新。

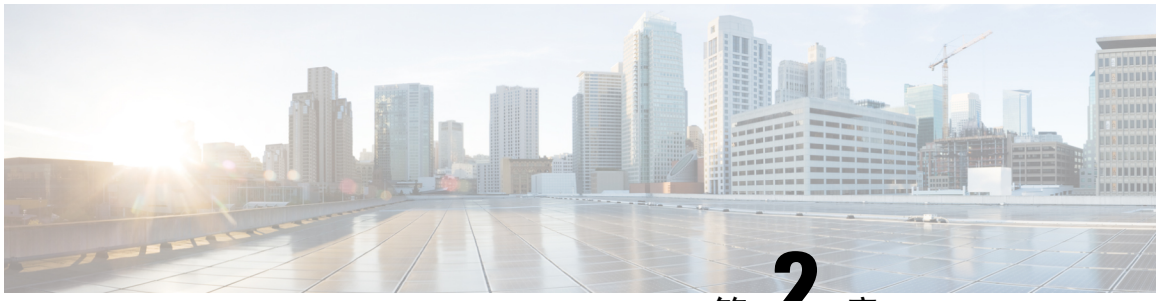
在分配给租户区域的维护日的 3 小时维护期内，对租户进行更新最多可能需要 1 小时。在更新租户时，您将无法访问云交付的防火墙管理中心环境，但仍可访问 CDO 的其余部分。

表 *2:* 云交付的防火墙管理中心维护时间表

星期	时间 （24 小时制）	地区
星期三	04:00 UTC - 07:00 UTC	欧洲、中东或非洲 (EMEA)
星期三	17:00 UTC - 20:00 UTC	亚太、日本、中国 (APJC)
星期四	09:00 UTC - 12:00 UTC	美国 (US)

第 II 部分

将设备载入 云交付的防火墙管理中心。



第 2 章

将 FTD 载入 云交付的防火墙管理中心

阅读以下信息，了解载入的前提条件和程序。

载入概述

查看 云交付的防火墙管理中心 支持的型号和使用案例。

支持的设备

您可以字啊如以下设备型号：

- Firepower 1000 系列
- Firepower 2100 系列
- Secure Firewall 3100 系列
- Firepower 4100 系列
- Firepower 9300 系列
- ISA 3000
- 虚拟Secure Firewall Threat Defense

支持的使用案例

云交付的防火墙管理中心 目前支持以下设备的载入场景：

- 设备必须运行版本 7.0.3 或 7.2.0 以及更高版本。要查看所有支持的版本和产品兼容性，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》以了解详细信息。

- 配置为由 设备管理器进行本地管理的设备。在载入之前，设备可能已登录，也可能未登录。对于尚未登录的设备，您可以通过通过低接触调配激活设备来载入设备。

注释 如果您将 FDM 管理 设备载入 云交付的防火墙管理中心，则无法再使用 设备管理器 来管理设备。

- 由 本地管理中心 管理的设备。

  如果您已有由 本地管理中心 管理的 威胁防御 设备，则可以迁移该设备以进行云管理。有关详细信息，请参阅将安全防火墙威胁防御迁移到云。

注释 将设备移动或迁移到 云交付的防火墙管理中心 时会发生以下情况：

- 如果您从 本地管理中心 或 Secure Firewall Threat Defense 设备管理器 中删除设备以载入 云交付的防火墙管理中心，则管理器的更改会擦除通过 本地管理中心 配置的任何策略。
- 如果将设备从 本地管理中心 **迁移**到 云交付的防火墙管理中心，则该设备将保留您之前配置的大多数策略。

如果您不知道您的设备是否已由备用管理器管理，请在设备的 CLI 中使用 `show managers` 命令。

载入方法

云交付的防火墙管理中心 支持以下载入方法：

- 使用 CLI 注册密钥载入设备 - 使用注册密钥载入设备。在设备上完成初始设置向导。
- 通过低接触调配激活设备 - 对**未**在设备上执行初始设备安装向导的新出厂设备进行载入。请注意，此方法仅支持 Firepower 1000、Firepower 2100 或 Secure Firewall 3100 设备。

注释 版本 7.0.3 不支持低接触调配。

- 通过序列号载入设备 - 载入已初始配置序列号的设备。请注意，此方法仅支持 Firepower 1000、Firepower 2100 或 Secure Firewall 3100 设备。

注释 版本 7.0.3 不支持使用序列号载入。

将设备载入 云交付的防火墙管理中心的前提条件

自行激活限制和要求

将设备载入 云交付的防火墙管理中心时，请注意以下限制：

- 设备 **必须** 运行 7.0.3 版本或 7.2 或更高版本。我们 **强烈** 建议使用 7.2 或更高版本。
- 您不需要本地或虚拟 SDC 来载入设备。
- 您可以按照 迁移 FTD 到云交付的防火墙管理中心 流程来迁移由 本地防火墙管理中心 管理的 HA 对。在迁移之前，确认两个对等体都处于正常状态。
- 只有配置为本地管理且由 设备管理器 管理的设备才能使用序列号和低接触调配方法自行激活。
- 如果设备由 本地管理中心管理，您可以将设备载入或迁移到 云交付的防火墙管理中心 。迁移会保留任何现有策略和对象，而自行激活设备会删除大多数策略和所有对象。有关详细信息，请参阅 将 FTD 迁移到云交付的防火墙管理中心 。
- 如果您的设备当前由 设备管理器管理，请在将设备载入之前取消注册所有智能许可证。即使您切换了设备管理，思科智能软件管理器仍将保留智能许可证。
- 如果您之前载入了由 设备管理器 管理的设备，并从 CDO 中删除了该设备，以便重新载入以进行云管理，则 **必须** 在删除设备后将 设备管理器 注册到 安全服务交换 云。请参阅《*Firepower* 和思科 *SecureX* 威胁响应集成指南》中的“访问安全服务交换”章节。

提示 将设备自行激活到 云交付的防火墙管理中心 会删除通过上一个管理器配置的任何策略和大多数对象。如果您的设备当前由 本地管理中心管理，则可以迁移设备并保留您的策略和对象。有关详细信息，请参阅 将 FTD 迁移到云交付的防火墙管理中心 。

网络要求

在载入设备之前，请确保以下端口具有外部和出站访问权限。确认允许设备上的以下端口。如果通信端口被防火墙阻止，则激活设备可能会失败。

注释 您无法在 CDO UI 中配置这些端口。您必须通过设备的 SSH 来启用这些端口。

表 *3:* 设备端口要求

端口	协议/功能	详细信息
443/tcp	HTTPS	发送和接收来自互联网的数据。
443	HTTPS	与 AMP 云（公共或私有）通信

端口	协议/功能	详细信息
8305/tcp	设备通信	在同一部署中的设备之间安全地进行通信。

管理和数据接口

确保您的设备已正确配置管理或数据接口。

要在设备上配置管理或数据接口，请参阅使用 CLI 完成 Secure Firewall Threat Defense 设备初始配置，第 2208 页。

使用 CLI 注册密钥载入设备

使用以下程序通过 CLI 注册密钥为 云交付的防火墙管理中心 载入设备。

注释 如果您的设备当前由 本地管理中心管理，则载入设备将失败。您可以从 本地管理中心 删除设备并作为没有策略或对象的全新设备载入，也可以迁移设备并保留现有策略和对象。有关详细信息，请参阅将 FTD 迁移到云交付防火墙管理中心。

重要事项 您可以使用 Cisco Secure Firewall 机箱管理器或 FXOS CLI 来创建 CDO 托管的独立逻辑 威胁防御 设备。

开始之前

在载入设备之前，请务必完成以下任务：

- 已为您的租户启用 云交付的防火墙管理中心。
- 确认设备的 CLI 配置已成功完成。有关详细信息，请参阅 使用 CLI 完成 Secure Firewall Threat Defense 设备初始配置，第 2208 页。
- 在载入设备之前，请查看前提条件和限制。有关详细信息，请参阅《使用思科防御协调器中的云交付防火墙管理中心来管理防火墙威胁防御》中的“将设备载入云交付的防火墙管理中心的前提条件”。
- 可以将设备配置为使用 Secure Firewall 设备管理器 进行本地管理或使用 Cisco Secure Firewall Management Center 进行远程管理。
- 设备必须运行版本 7.0.3 或 7.2.0 以及更高版本。

过程

步骤 1 登录 CDO。

步骤 2 在导航窗格中，点击**清单 (Inventory)**，然后点击蓝色加号按钮。

步骤 3 点击 **FTD** 磁贴。

步骤 4 在 **管理模式**下，确保选择 **FTD** 。

警告 在**管理模式 (Management Mode)** 下选择 **FTD**，您将无法使用之前的管理平台来管理设备。除接口配置外，所有现有策略配置都会被重置。载入设备后，您必须重新配置策略。

如果您希望设备从 Secure Firewall 设备管理器 保持管理，请选择 **FDM** 并参阅 使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+ 以了解详细信息。

步骤 5 选择**使用 CLI 注册密钥 (Use CLI Registration Key)** 作为载入方法。

步骤 6 在 **设备名称** 字段中输入设备名称，然后点击 **下一步**。

步骤 7 在策略分配步骤中，使用下拉菜单选择在设备载入后要部署的访问控制策略。如果未配置策略，请选择**默认访问控制策略 (Default Access Control Policy)**。

步骤 8 指定要载入的设备是物理设备还是虚拟设备。如果要载入虚拟设备，则必须从下拉菜单中选择设备的性能级别。

步骤 9 选择要应用于设备的许可证。点击**下一步**。

步骤 10 CDO 使用注册密钥生成命令。使用 SSH 连接到您要载入的设备。以“admin”或具有同等管理员权限的用户身份登录，并将整个注册密钥按原样粘贴到设备的 CLI 中。

注意：对于 Firepower 1000、Firepower 2100、ISA 3000 和 threat defense virtual 设备，打开与设备的 SSH 连接并以 `admin` 登录。复制整个注册命令，并在提示符后将其粘贴到设备的 CLI 界面中。在 CLI 中，输入 **Y** 完成注册。如果您的设备以前由 设备管理器管理，请输入 **是 (Yes)** 以确认提交。

步骤 11 在 CDO 载入向导中点击 **下一步 (Next)** 。

步骤 12 （可选）向设备添加标签，以帮助对**清单 (Inventory)** 页面进行排序和过滤。输入标签，然后选择蓝色加号按钮。标签会在设备载入 CDO后应用到设备。

下一步做什么

在设备同步后，从**清单 (Inventory)** 页面中选择您刚刚载入的设备，然后选择位于右侧的**管理 (Management)** 窗格下列出的任何选项。我们强烈建议您执行以下操作：

- 如果还没有创建，请创建自定义访问控制策略，以自定义环境的安全性。有关详细信息，请参阅《使用思科防御协调器中的云交付防火墙管理中心来管理防火墙威胁防御》中的访问控制概述。
- 启用思科安全分析和日志记录 (SAL) 以在 CDO 控制面板中查看事件**或**将设备注册到 Cisco Secure Firewall Management Center 以进行安全分析。有关详细信息，请参阅《使用思科防御协调器中的云交付防火墙管理中心来管理防火墙威胁防御》中的思科安全分析和日志记录。

通过低接触调配激活设备

只有 Firepower 1000、Firepower 2100 和 Secure Firewall 3100 设备可以使用低接触调配方法来载入。

开始之前

在载入之前，确认已完成以下操作：

- 已为您的租户启用 云交付的防火墙管理中心。
- 设备是全新安装的，但从未通过设备 CLI 或 设备管理器 登录。
- 设备正在运行 7.2 或更高版本。版本 7.0.3 不支持低接触调配。

过程

步骤 1 登录 CDO。

步骤 2 在导航窗格中，点击**清单 (Inventory)**，然后点击蓝色加号按钮。

步骤 3 点击 **FTD** 磁贴。

步骤 4 在 **管理模式**下，确保选择 **FTD** 。

警告 在**管理模式 (Management Mode)** 下选择 **FTD**，您将无法使用之前的管理平台来管理设备。除接口配置外，所有现有策略配置都会被重置。载入设备后，您必须重新配置策略。

如果您希望设备从 Secure Firewall 设备管理器 保持管理，请选择 **FDM** 并参阅 使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+ 以了解详细信息。

步骤 5 输入 **设备序列号** 和 **设备名称**。选择**下一步**。

步骤 6 密码重设选择**是，此新设备从未登录或配置管理器 (Yes, this new device has never been logged into or configured for a manager)** 选项。

如果您的设备之前已注册管理器或 仍 注册到管理器，请参阅 通过序列号载入设备，第 13 页。

步骤 7 点击**下一步 (Next)**。

步骤 8 在策略分配步骤中，使用下拉菜单选择在设备载入后要部署的访问控制策略。如果未配置策略，请选择**默认访问控制策略 (Default Access Control Policy)**。

步骤 9 选择要应用于设备的所有许可证。点击**下一步**。

下一步做什么

在设备同步后，从**清单 (Inventory)** 页面中选择您刚刚载入的设备，然后选择位于右侧的**管理 (Management)** 窗格下列出的任何选项。我们强烈建议您执行以下操作：

- 如果还没有创建，请创建自定义访问控制策略，以自定义环境的安全性。有关详细信息，请参阅《使用思科防御协调器中的云交付防火墙管理中心来管理防火墙威胁防御》中的访问控制概述。

- 启用思科安全分析和日志记录(SAL)以在CDO控制面板中查看事件或将设备注册到Cisco Secure Firewall Management Center 以进行安全分析。有关详细信息，请参阅《使用思科防御协调器中的云交付防火墙管理中心来管理防火墙威胁防御》中的思科安全分析和日志记录。

通过序列号载入设备

只有 Firepower 1000、Firepower 2100 和 Secure Firewall 3100 设备可以使用序列号载入方法来载入。

开始之前

请确保在载入之前完成以下操作：

- 已为您的租户启用 云交付的防火墙管理中心。
- 确认设备的 CLI 配置已成功完成。有关详细信息，请参阅 使用 CLI 完成 Secure Firewall Threat Defense 设备初始配置 ， 第 2208 页。
- 在载入设备之前，请查看前提条件和限制。有关详细信息，请参阅《使用思科防御协调器中的云交付防火墙管理中心来管理防火墙威胁防御》中的“将设备载入云交付的防火墙管理中心的前提条件”。
- 取消注册设备在载入之前可能已启用的任何现有智能许可证。
- 确认设备已被配置为本地管理并且当前由 Secure Firewall 设备管理器 管理。
- 设备正在运行 7.2 或更高版本。版本 7.0.3 不支持使用序列号载入。

过程

步骤 1 在 Secure Firewall 设备管理器 UI 中，请转至 **系统设置 (System Settings)** > **云服务 (Cloud Services)** ，然后选 **通过 Cisco 防御协调器自动注册租用 (Auto-enroll with Tenancy from Cisco Defense Orchestrator)** 选项并点击 **注册 (Register)**。

步骤 2 登录 CDO。

步骤 3 在导航窗格中，点击**清单 (Inventory)** ，然后点击蓝色加号按钮。

步骤 4 点击 **FTD** 磁贴。

步骤 5 在 **管理模式**下，确保选择 **FTD** 。

在**管理模式**下选择**FTD**，您将无法使用之前的管理平台来管理设备。除接口配置外，所有现有策略配置都会被重置。载入设备后，您必须重新配置策略。

步骤 6 输入 **设备序列号** 和 **设备名称**。点击**下一步 (Next)**。

步骤 7 密码重设选择**否，此设备已登录并为管理器配置 (No, this device has been logged into and configured for a manager)**。这意味着该设备已被注册至 设备管理器 ，并且默认密码已作为该配置的一部分进行了更改。

如果您的设备是全新的，并且从未配置过管理器，请参阅 通过低接触调配激活设备 ， 第 12 页。

步骤 8 点击**下一步 (Next)**。

步骤 9 在策略分配步骤中，使用下拉菜单选择在设备载入后要部署的访问控制策略。如果未配置策略，请选择**默认访问控制策略 (Default Access Control Policy)**。

步骤 10 选择要应用于设备的所有许可证。点击**下一步**。

下一步做什么

在设备同步后，从**清单 (Inventory)** 页面中选择您刚刚载入的设备，然后选择位于右侧的**管理 (Management)** 窗格下列出的任何选项。我们强烈建议您执行以下操作：

- 如果还没有创建，请创建自定义访问控制策略，以自定义环境的安全性。有关详细信息，请参阅《使用思科防御协调器中的云交付防火墙管理中心来管理防火墙威胁防御》中的访问控制概述。
- 启用思科安全分析和日志记录 (SAL) 以在 CDO 控制面板中查看事件**或**将设备注册到 Cisco Secure Firewall Management Center 以进行安全分析。有关详细信息，请参阅《使用思科防御协调器中的云交付防火墙管理中心来管理防火墙威胁防御》中的思科安全分析和日志记录。

载入与 AWS VPC 关联的 威胁防御 设备

使用以下程序载入并初步调配与要由 云交付的防火墙管理中心 管理的 AWS VPC 关联的 威胁防御 设备的防火墙。

开始之前

在载入之前，确认满足以下前提条件：

- 您必须启用 云交付的防火墙管理中心 功能并将其与您的租户关联。
- AWS VPC 必须已被载入 CDO。有关更多信息，请参阅载入 AWS VPC。

过程

步骤 1 登录 CDO。

步骤 2 在导航窗格中，点击**清单 (Inventory)**，然后点击蓝色加号按钮。

步骤 3 选择 **FTD** 磁贴。

步骤 4 在 **管理模式**下，确保选择 **FTD** 。

步骤 5 选择**使用 AWS VPC (Use AWS VPC)** 作为载入方法。如果没有已载入的 AWS VPC，您可以点击此步骤中提供的链接并载入虚拟环境。

步骤 6 从下拉菜单选择**可用性区域**。选择云 威胁防御 所在的区域，而不是本地计算机所在的区域。

步骤 7 通过以下任一选项来选择管理接口子网：

- **使用现有子网 (Use existing subnets)** - 展开下拉菜单并为管理接口、内部接口和外部接口子网选择适当的子网。
- **创建新子网 (Create new subnets)** - 添加一组子网接口，供设备在载入后使用。作为载入程序的一部分，CDO 会自动创建这些子网并将其应用于 AWS VPC。

请注意，诊断接口将使用与管理接口相同的接口。

步骤 8 点击**选择 (Select)** 以分配子网。点击**下一步**。

步骤 9 在 **设备名称** 字段中输入设备名称，然后点击 **下一步**。

步骤 10 在策略分配步骤中，使用下拉菜单选择在设备载入后要部署的访问控制策略。如果未配置策略，请选择**默认访问控制策略 (Default Access Control Policy)**。

步骤 11 选择您要应用于设备的**订用许可证 (Subscription Licenses)**。您必须至少拥有为虚拟 威胁防御 设备选择的 URL 许可证。

下一步做什么

设备可能需要几分钟才能显示在CDO的**清单 (Inventory)** 页面中，因为在 CDO 成功部署云形成、初始化设备连接并与虚拟设备和 AWS VPC 环境建立通信之前，设备无法同步。

如有必要，您可以在载入后通过 云交付的防火墙管理中心 UI 来修改虚拟 威胁防御 设备性能层选择。

从云交付的防火墙管理中心删除设备

虽然设备已注册到 云交付的防火墙管理中心，但 CDO 仍会管理设备注册。您必须从 CDO 控制面板中删除设备才能从云交付的防火墙管理中心中删除设备。

注释 CDO 不会同步与 AWS VPC 环境关联的设备的删除。您必须从 AWS VPC UI 中直接删除设备目录。有关详细信息，请参阅 AWS 文档。

过程

步骤 1 登录 CDO 并点击**清单 (Inventory)**。

步骤 2 使用过滤器或搜索栏找到要删除的设备。选择它以突出显示设备行。

步骤 3 在右侧的设备操作窗格中，点击**删除 (Remove)**。

步骤 4 出现提示时，选择**确定 (OK)** 以确认删除所选设备。点击**取消 (Cancel)** 以使设备保持已载入状态。

故障排除

使用以下场景对任何载入问题进行故障排除。

使用 CLI 注册密钥将设备载入 云交付的防火墙管理中心进行故障排除

错误：载入后设备仍处于待处理设置状态

当设备注册失败时，设备的连接状态显示为**待设置 (Pending Setup)**。在右侧的面板中，CDO 会显示一条**注册失败 (Registration Failed)** 消息以及一个**重试载入 (Retry Onboarding)** 按钮，以允许您立即重新尝试载入设备。

如果您在将其载入 CDO 后的 3 分钟内未在设备 CLI 中执行 `configuration manager` 命令，则设备的注册尝试会到期并导致注册失败。使用以下程序解决此问题：

过程

步骤 1 登录 CDO 并导航至**清单 (Inventory)** 页面。找到注册失败的设备。

步骤 2 在右侧的面板中，找到**注册失败 (Registration Failed)** 窗口。在设备的 CLI 注册密钥旁边，点击**复制 (Copy)**。此操作会将 CLI 密钥复制到本地剪贴板。

步骤 3 打开到设备的 SSH 连接并以管理员身份登录。

步骤 4 将 CLI 注册密钥粘贴到设备的 CLI 界面中。在 CLI 中，输入 **Y** 完成注册。如果您的设备以前由 设备管理器管理，请输入 **是 (Yes)** 以确认提交。

对使用序列号将设备载入 云交付的防火墙管理中心 进行故障排除

设备离线或无法访问

如果设备在载入过程中或在载入后的任何时候无法访问，CDO 会显示**无法访问 (Unreachable)** 连接状态。在设备能够连接之前，设备将无法完全载入CDO。这可能是以下情况所致：

- 设备布线不正确。
- 您的网络可能要求提供设备的静态 IP 地址。
- 您的网络使用自定义 DNS，或者存在阻止网络的外部 DNS。
- 如果您的设备与欧洲地区 (https://defenseorchestrator.eu/) 相关联，则您可能需要启用 PPPoE 身份验证。对于其他域，请查看域要求。
- 设备可能被防火墙阻止，或者错误地阻止了用于连接的端口。查看设备 网络要求，第 9 页 并确认已启用正确的传出端口。

错误：序列号已被申领

设备是从外部供应商处购买的

如果设备是从外部供应商处购买的，并且由于**序列号已申领 (Serial Number Already Claimed)** 错误而无法载入，则该设备可能仍与供应商的租户相关联。使用以下步骤来申领设备及其序列号：

1. 从 CDO 租户中删除设备。
2. 在设备上安装 FXOS 映像。有关详细信息，请参阅《Firepower 1000/21000 和 Cisco Secure Firewall 3100 Firepower 威胁防御的 FXOS 故障排除指南》南的“重新映像程序”一章。
3. 将笔记本电脑连接到设备的控制台端口。
4. 连接到 FXOS CLI 并以**管理员**身份登录。
5. 在 FXOS CLI 中，通过 `firepower # connect local-mgmt` 命令连接到 **local-mgmt**。
6. 执行 `firepower(local-mgmt) # cloud deregister` 命令，以便从云租户取消注册设备。
7. 一旦设备成功取消注册，CLI 接口会返回成功消息。消息示例：

```
Example: firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success
 MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
```

注释 如果设备从未注册到其他 CDO 租户，则上面的消息会指出 `RESULT=success MESSAGE=DEVICE_NOT_FOUND`。

8. 使用序列号将设备载入 CDO 租户。有关详细信息，请参阅 通过序列号载入设备，第 13 页。

设备被其他区域的 CDO 租户申领

该设备之前可能已由其他区域中的另一个 CDO 实例管理，并仍注册到该租户。

如果您**确实**有权访问设备当前注册到的租户，请使用以下程序：

1. 从错误的 CDO 租户中删除设备。
2. 登录设备的 设备管理器 UI。
3. 导航至**系统设置 (System Settings)** > **云服务 (Cloud Services)**。
4. 点击**云服务 (Cloud Services)**，然后从下拉列表中选择**取消注册云服务 (Unregister Cloud Services)**。
5. 确认操作，然后点击**取消注册 (Unregister)**。此操作会生成警告，指明设备已从 CDO 中删除。这是预期行为。
6. 登录到正确区域的 CDO 租户并载入设备。有关详细信息，请参阅 通过序列号载入设备，第 13 页。
7. 导航至**系统设置 (System Settings)** > **云服务 (Cloud Services)**。

8. 点击**云服务 (Cloud Services)**，然后从下拉列表中选择**取消注册云服务 (Unregister Cloud Services)**。
9. 选择**通过思科防御协调器自动注册租用 (Auto-enroll with Tenancy from Cisco Defense Orchestrator)**并点击**注册 (Register)**。设备会映射到属于新区域的新租户，而 CDO 会载入设备。

如果您**无权**访问租户，请使用以下程序：

1. 从控制台端口连接到 FXOS CLI 并以**管理员**身份登录。有关如何登录 FXOS CLI 的信息，请参阅访问 FXOS CLI。
2. 在 FXOS CLI 中，通过 `firepower # connect local-mgmt` 命令连接到 **local-mgmt**。
3. 执行 `firepower(local-mgmt) # cloud deregister` 命令，以便从云租户取消注册设备。
4. 一旦设备成功取消注册，CLI 接口会返回成功消息。消息示例：

```
Example: firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success
 MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
```

注释 如果设备从未注册到其他 CDO 租户，则上面的消息会指出 `RESULT=success MESSAGE=DEVICE_NOT_FOUND`。

5. 在正确域中的 CDO 租户中，载入设备。有关详细信息，请参阅 通过序列号载入设备，第 13 页。
6. 在设备的 设备管理器 中，导航至**系统设置 (System Settings)** > **云服务 (Cloud Services)**。
7. 选择**通过思科防御协调器自动注册租用 (Auto-enroll with Tenancy from Cisco Defense Orchestrator)**并点击**注册 (Register)**。设备会映射到属于新区域的新租户，而 CDO 会载入设备。

错误：申领错误

如果在载入设备时输入错误的序列号，CDO 会生成**申领错误 (Claim Error)** 状态。

注释 确认设备已在 CDO 内正确的区域中申领。

使用以下方法解决此问题：

过程

步骤 1 登录 CDO 并导航至**清单 (Inventory)** 页面。找到存在错误的设备。

步骤 2 选择设备，使其突出显示，然后从 CDO **删除**设备。

步骤 3 确认以下内容：

- 设备处于在线状态并且可以访问互联网。

- 设备尚未注册到您的 CDO 实例或由其他区域的 CDO 租户申领。

步骤 4 找到设备的序列号。可以使用以下一种方法：

- 对于 1000、2100 和 3100 系列型号，请找到实际设备上的序列号。
- 打开与设备的 SSH 连接并发出 `show serial-number` 命令。
- 如果设备当前是 FDM 管理，请登录 设备管理器 UI 并在**云服务 (Cloud Services)** 页面上找到序列号。

步骤 5 在 CDO 中，使用正确的序列号载入设备。有关详细信息，请参阅通过序列号载入设备，第 13 页。

错误：申领失败

如果您在尝试载入设备后看到**错误：无法申领 (Error: Failed to Claim)** 连接状态或错误消息，则可能是以下原因造成的：

- 安全服务交换 平台可能存在会导致无连接的临时问题。
- CDO 服务器可能已关闭。

请按照以下步骤解决此问题：

过程

步骤 1 登录 CDO 并导航至**清单 (Inventory)** 页面。找到注册失败的设备。

步骤 2 选择设备，使其突出显示，然后从 CDO 租户**删除**设备。

步骤 3 等待至少 10 分钟，然后再尝试将设备载入 CDO 租户。有关详细信息，请参阅通过低接触调配激活设备，第 12 页。

下一步做什么

如果您仍无法申领设备，请查看设备的工作流程，以确认是否存在错误消息。如果有，请导出工作流程并创建支持案例以进一步解决问题。

错误：临时错误

设备密码尚未更改

如果您在配置设备以进行远程管理时未更改设备的默认密码，并且在将设备载入CDO时选择了**否，此设备已登录并配置为管理器 (No, this device has been logged into and configured for a manager)** 选项，则设备将在**清单 (Inventory)** 页面中生成**未调配 (UnProvisioned)** 连接状态。

使用以下程序解决此问题：

1. 登录 CDO 并导航至**清单 (Inventory)** 页面。
2. 找到并选择连接状态为**未调配 (UnProvisioned)** 的设备，使其突出显示。
3. 在右侧窗格中，找到**更改密码 (Change Password)** 窗口。
4. 点击**更改密码 (Change Password)**，然后输入设备的新密码。这样就会覆盖默认密码。

设备可能需要几分钟才能载入并完全同步到 CDO。

设备密码已被更改

如果您在配置设备以进行远程管理时**确实**更改了设备的默认密码，并选择了**此设备是否为从未登录或配置过的新设备？(Is this a new device that has never been logged into or configured before?)** 选项将设备载入 CDO 时，CDO 会在**清单 (Invenotry)** 页面中生成**未调配 (UnProvisioned)** 连接状态。

使用以下程序解决此问题：

1. 登录 CDO 并导航至**清单 (Inventory)** 页面。
2. 找到并选择连接状态为**未调配 (UnProvisioned)** 的设备，使其突出显示。
3. 在右侧窗格中，找到**确认并继续 (Confirm and Proceed)** 窗口。
4. 点击**确认并继续 (Confirm and Proceed)**。此操作会忽略载入向导中提供的密码，并恢复设备的默认密码。然后 CDO 会继续载入设备。

其他临时错误场景

无论设备的默认密码配置如何，设备在载入过程中仍可能处于**未调配 (UnProvisioned)** 连接状态。如果您确认在载入向导中选择的密码对于设备的状态是准确的，请考虑使用以下选项来解决问题：

- 选择设备以便将其突出显示。在屏幕右侧窗格的窗口中，点击**重试 (Retry)** 以强制 CDO 使用现有临时参数重新载入设备。
- 从**清单 (Inventory)** 页面删除设备，然后尝试重新载入设备。
- 在设备的 设备管理器 中，导航至**系统设置 (System Settings)** > **云服务 (Cloud Services)**。选择**通过思科防御协调器自动注册租用 (Auto-enroll with Tenancy from Cisco Defense Orchestrator)** 并点击**注册 (Register)**。

如果您仍无法申领设备，请查看设备的工作流程，以确认是否存在错误消息。如果有，请导出工作流程并创建支持案例以进一步解决问题。

关于设备管理

使用 管理中心 来管理您的设备。

管理接口

设置设备时，指定您要连接到的 IP 地址。管理和事件流量都在初始注册时转到此地址。

注释 在某些情况下，设备可能会在其他管理接口上建立初始连接；后续连接应使用具有指定 IP 地址的管理接口。

如果设备具有单独的仅事件接口，则托管设备会在网络允许的情况下将后续事件流量发送到仅事件接口。此外，某些托管设备型号包括一个额外的管理接口，您可以为仅事件流量配置该接口。

注释 请注意，如果您配置用于管理的数据接口，则不能使用单独的管理接口和事件接口。

如果事件网络关闭，则事件流量将恢复到托管设备上的常规管理接口。

关于数据接口

您可以使用专用的管理接口或常规数据接口与设备通信。如果想要从外部接口远程管理 FTD，或者您没有单独的管理网络，则在数据接口上进行CDO访问非常有用。CDO支持从数据接口远程管理的 FTD 上的高可用性。

从数据接口进行 FTD 管理访问具有以下限制：

- 只能在一个物理数据接口上启用管理器访问。不能使用子接口或 EtherChannel。
- 仅路由防火墙模式，使用路由接口。
- 不支持 PPPoE。如果您的 ISP 需要 PPPoE，则必须在 FTD 与 WAN 调制解调器之间放入支持 PPPoE 的路由器。
- 接口只能位于全局 VRF 中。
- 默认不对数据接口启用SSH，因此必须稍后使用CDO启用SSH。由于管理接口网关将更改为数据接口，因此您也无法启动从远程网络到管理接口的 SSH 会话，除非您使用 **configure network static-routes** 命令为管理接口添加静态路由。对于 Amazon Web 服务上的 FTDv，控制台端口不可用，因此您应保持对管理接口的 SSH 访问：在继续配置之前为管理添加静态路由。或者，请确保在配置数据接口并断开连接之前完成所有 CLI 配置（包括 **configure manager add** 命令）。

设备管理接口上的网络路由

管理接口（包括事件专用接口）仅支持通过静态路由到达远程网络。在设置托管设备时，设置进程将为您指定的网关 IP 地址创建一个默认路由。不能删除此路由；只能修改网关地址。

注释 如果配置用于管理的数据接口而不是使用专用管理接口，则流量将通过背板路由以使用数据路由表。本节中的信息不适用。

如果要访问远程网络，建议为每个管理接口使用至少一个静态路由。我们建议将每个接口放在单独的网络中，以避免潜在的路由问题，包括从其他设备到设备的路由问题。如果同一网络上的接口没有遇到问题，请务必正确配置静态路由。例如，management0 和 management1 位于同一网络上，但 FTD 管理接口和事件接口则位于不同的网络上。网关是 192.168.45.1。如果您希望 management1 连接到位于 10.6.6.1/24 的管理的仅事件接口，则可以通过 management1 使用相同的网关 192.168.45.1 来创建 10.6.6.0/24 的静态路由。到达 10.6.6.0/24 的流量会在到达默认路由之前到达此路由，因此按照预期会使用管理。

登录 威胁防御 设备上的命令行界面

您可以在 威胁防御 设备上直接登录命令行界面。

注释 当用户连续三次尝试通过 SSH 登录 CLI 失败时，系统会终止 SSH 连接。

开始之前

使用默认 **admin** 用户进行初始登录，完成初始安装过程。创建可以使用 **configure user add** 命令登录 CLI 的其他用户账户。

过程

步骤 1 通过控制台端口或使用 SSH连接至 威胁防御 CLI。

可以通过SSH连接到威胁防御设备的管理接口。如果您为SSH连接打开某个数据接口，您也可以连接到该接口上的地址。默认情况下，禁用 SSH 数据接口访问。请参阅配置安全外壳，第 631 页，以允许与特定数据接口建立 SSH 连接。

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

在控制台端口上访问的初始 CLI 因设备类型而异。

- ISA 3000 和 threat defense virtual - 控制台端口上的 CLI 是常规 威胁防御 CLI。
- 其他型号-控制台端口上的 CLI 是 FXOS。您可以使用 **connect ftd** 命令进入 威胁防御 CLI。仅将 FXOS CLI 用于机箱级配置和故障排除。使用 威胁防御 CLI 进行基本配置、监控和正常的系统故障排除。有关 FXOS 命令的信息，请参阅 FXOS 文档。

步骤 2 使用 **admin** 用户名和密码登录。

步骤 3 在 CLI 提示符 (>) 处，使用命令行访问级别所允许的任何命令。

步骤 4 （可选）访问诊断 CLI：

system support diagnostic-cli

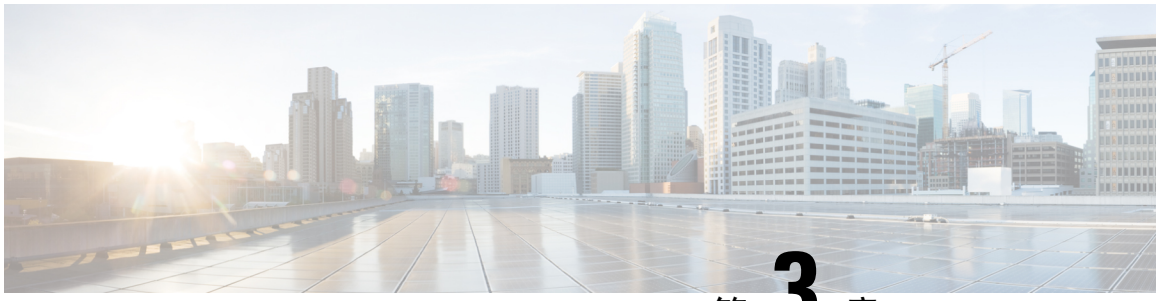
使用此 CLI 可进行高级故障排除。此CLI包括额外 **show** 和其他命令。

此 CLI 有两种子模式：用户 EXEC 和特权 EXEC 模式。在特权 EXEC 模式中，有更多命令可用。要进入特权 EXEC 模式，请输入 **enable** 命令；在收到提示时按 Enter 键，无需输入密码。

示例：

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

要返回到常规 CLI，请键入 **Ctrl+a**, **d**。



第 3 章

将 Cisco Secure Firewall Threat Defense 迁移到云

将 Secure Firewall Threat Defense 从 Cisco Secure Firewall Management Center 迁移到云

思科防御协调器 允许具有 CDO 管理员权限的用户将 威胁防御 设备从 管理中心 迁移到云。

在威胁防御设备上启动迁移过程之前，与这些设备关联的 管理中心 必须已经被载入到 CDO。

在将 威胁防御 迁移到云时，CDO 会载入设备并将所有共享策略和关联对象、设备特定策略以及设备配置从 管理中心 导入至 CDO。

注释 CDO 会处理 管理中心 迁移过程中识别的所有重复策略和对象名称。本文档的后续部分将详细介绍此行为。

事件和分析管理可以转移到 CDO 或保留在管理中心上。

在执行迁移后，您有14天的时间来评估更改。评估期允许您修改或更改特定操作，或者将这些设备的管理更改回管理中心。在评估期之后，您将无法恢复任何更改。

支持的软件

本节介绍迁移的最低软件要求：

- 管理中心: 7.2

- Secure Firewall Threat Defense：
  - 7.0.3 或更高版本
  - 7.2 或更高版本

注释 运行软件版本 7.1 的 威胁防御 上未提供此支持。

许可

- 当 威胁防御 被迁移到云后，与设备关联的所有功能许可证都将转移到 CDO，并从 管理中心 释放到智能许可证池。设备会在向 CDO 注册期间收回设备特定的许可证。您无需再次在设备上申请许可证。
- 如果要将设备保留在 管理中心 中以进行分析，则不需要设备特定许可证。
- 确保您已使用智能许可证注册 云交付的防火墙管理中心。

支持的功能

处理共享策略和对象

在迁移过程开始时，首先导入与 威胁防御 设备关联的共享策略和关联对象，然后导入设备配置。

更改 威胁防御 设备上的管理器后，将以下共享策略导入 CDO：

- 访问控制
- IPS
- SSL
- 预过滤器
- NAT
- QoS
- 身份
- 平台设置
- Flex config
- 网络分析
- DNS
- 恶意软件和文件

- 运行状况
- 远程接入 VPN

如果 CDO 中的策略或对象与从 Cisco Secure Firewall Management Center 导入的策略或对象同名，则 CDO 会在成功更改管理后执行以下操作。

策略、对象	条件	操作
访问控制、SSL、IPS、预过滤器、NAT、QoS、身份、平台设置、网络分析、DNS、恶意软件和文件策略。	云交付的防火墙管理中心策略的名称与 管理中心 策略匹配。	使用 云交付的防火墙管理中心 策略而不是从 管理中心 导入的策略。
RA VPN 默认组策略 **DfltGrpPolicy**	管理中心 中的默认组策略 **DfltGrpPolicy** 将被忽略。	改为使用现有的 云交付的防火墙管理中心 默认组策略 **DfltGrpPolicy**。
网络、端口对象	云交付的防火墙管理中心 中的网络和端口对象的名称和内容与管理中心 中的匹配。	使用具有相同名称和内容的现有 云交付的防火墙管理中心 网络和端口对象，而不是从 管理中心 导入的对象。 如果对象具有相同的名称但内容不同，则会创建对象覆盖。请参阅对象覆盖。
所有其他对象		使用现有 云交付的防火墙管理中心 对象，而不是从 管理中心 导入的对象。

与访问控制策略关联的任何系统日志警报对象都会被导入 思科防御协调器。

高可用性对中的 威胁防御 迁移支持

您可以迁移高可用性对中的设备。主用和备用设备的设备管理会被更改并导入到 CDO 中。

重要事项 强烈建议在执行任何高级操作之前提交管理器更改，例如在正在迁移的设备上创建 HA 配置或中断 HA。

不支持在评估期间执行此类操作，否则可能会导致意外行为。

高可用性对中的 管理中心 迁移支持

您可以将 威胁防御 设备从配置了高可用性的 管理中心 迁移到云。

管理中心 可以使用 SecureX 或凭证通过 SDC 方法载入。始终载入主用管理中心，而不是备用管理中心。

注释 如果您已载入独立管理中心，而稍后又将其配置为备用管理中心，请删除该备用管理中心并载入主用管理中心。

要点回顾：

- **SecureX 载入方法**
  - 在14天评估期内，不支持高可用性中断。您可以在评估期后手动或自动提交更改后中断高可用性。
  - 在 14 天评估期内，支持高可用性切换。
- **使用 SDC 的凭证载入方法**
  - 在14天评估期内，不支持高可用性中断或高可用性切换。您可以在手动提交更改后执行这些操作，也可以在评估期后自动提交。
  - 在切换后，载入之前处于备用模式的新主用设备，然后在设备上启动迁移作业。

不支持的功能

在以下情况下，将 FTD 迁移到云 屏幕不允许将设备迁移到云：

- 集群的设备部分。
- 向 管理中心 注册的仅用于分析的设备。

以下配置不会作为迁移的一部分从 管理中心 导入到 CDO：

- 自定义构件、应用检测器、关联、SNMP 和邮件警报、扫描程序、组、动态访问策略、自定义 AMP 配置、用户、域、计划的部署任务、ISE 配置、计划的 GeoDB 更新、威胁智能导向器配置、动态分析连接。
- ISE 内部证书对象不会作为迁移的一部分导入。您必须从 ISE 导出新的系统证书或某个证书及其关联的专用密钥并将其导入 CDO。

Cisco Secure Firewall 推荐规则

将 威胁防御 迁移到云会导入与入侵策略关联的 Cisco Secure Firewall IPS 建议的规则。但是，当执行刷新计划程序时，云交付的防火墙管理中心 不会在迁移后自动更新这些规则。请参阅思科自动推荐的规则。

自定义网络分析

如果设备与自定义网络分析策略相关联，则必须在迁移前从本地中删除对该策略的所有引用。

1. 登录本地 管理中心。

2. 选择**策略 (Policies)** > **访问控制 (Access Control)**。
3. 点击要取消关联自定义 NAP 的访问控制策略上的编辑图标，然后点击**高级 (Advanced)** 选项卡。
4. 在**网络分析和入侵策略 (Network Analysis and Intrusion Policies)** 区域中，点击编辑图标。
5. 在**默认网络分析策略 (Default Network Analysis Policy)** 列表中，选择系统提供的策略。
6. 点击**确定 (OK)**。
7. 点击**保存 (Save)** 以保存更改，然后点击**部署 (Deploy)** 将更改下载到设备。

在迁移后，您可以在 CDO 中手动创建网络分析策略。

VPN 配置的迁移准则和限制

在使用 VPN 配置迁移设备时，请记住以下几点：

远程访问 VPN 策略的迁移支持

作为迁移的一部分，CDO 会导入远程访问 VPN 策略的所有设置。

在迁移过程中，CDO 会导入远程访问 VPN 策略的所有设置，但以下设置除外：

- 不导入对象覆盖。

  如果在地址池对象中使用了覆盖，则必须在迁移后使用CDO将其手动添加到导入的对象。请参阅对象覆盖。

- 不导入本地用户。

  如果身份验证服务器配置为用于用户身份验证的本地数据库，则关联的本地领域对象将被导入 CDO。但是，您必须在迁移后使用 CDO 将本地用户手动添加到导入的本地领域对象。请参阅创建领域和领域目录。

- VPN 负载均衡配置不会迁移。
- 不导入具有域配置的 RA VPN 认证登记。

  您可以在迁移后执行以下操作：

  1. 在 CDO 中，点击**清单 (Inventory)** > **FTD**。
  2. 选择迁移的 FTD，然后在右侧的**设备管理 (Device Management)** 中，点击**设备概述 (Device Overview)**。
  3. 选择**设备 (Devices)** > **证书 (Certificates)**。

     执行下列操作之一：

     - 如果在错误状态下导入证书，请点击**刷新证书状态 (Refresh certificate status)** 图标以将证书状态与设备同步。证书状态会变为绿色。
     - 如果未导入证书，则必须手动添加在管理中心中配置的 RA VPN 策略中定义的证书。

用户角色

迁移后，管理中心的用户角色不再适用于 CDO。您执行任务的授权基于您在 CDO 中的用户角色。

CDO 用户角色	说明
CDO 管理员	超级管理员和管理员用户可以访问产品中的所有内容。此用户可以创建、读取、修改和删除策略和对象，并将其部署到设备。
CDO 仅部署	仅部署用户可以查看所有策略和对象。将暂存更改部署到一个或多个设备。
CDO 仅编辑	“仅编辑”用户可以修改并保存策略和对象，但不能将其部署到设备。
CDO 只读	“只读”用户可以查看所有策略和对象，但不能将其部署到设备。

管理威胁防御事件和分析

事件和分析管理可以保留在 管理中心 中，也可以转移到 CDO，其中设备必须配置为将事件发送到 CDO。在启动迁移过程时，您可以选择必须将设备事件发送到哪个管理器进行分析。

如果选择发送到 管理中心 进行分析，则 CDO 将成为所选设备的管理器，但会在 管理中心 上以仅分析模式保留这些设备的副本。设备会继续向 管理中心 发送事件，而 CDO 会管理配置更改。

如果选择发送到 CDO 进行分析，则 CDO 将成为所选设备的管理员，并会从 管理中心 中删除这些设备。CDO 会管理配置更改以及事件和分析管理。您必须配置威胁防御设备以将事件发送到思科云。您可以使用 安全服务交换 或安全事件连接器 (SEC) 将事件从设备发送到云中的 Cisco Secure 分析和日志记录 (SAL)。

启用通知设置

您可以订用电子邮件通知，以便在将 威胁防御 设备迁移到 CDO 时，当与您的租户关联的设备遇到特定操作时从 CDO 接收通知。

如果启用 ，则 CDO 会在将 FTD 迁移到云作业期间接收以下状态的通知：

- **失败 (Failed)**：迁移作业失败时。
- **已开始 (Started)**：启动迁移作业时。
- **成功 (Succeeded)**：迁移作业成功完成时。
- **提交待定 (Commit Pending)**：在提交管理器更改时。

要启用通知设置，请参阅通知设置。

通过 云交付的防火墙管理中心 验证威胁防御连接

本节提供用于确定 威胁防御 与 云交付的防火墙管理中心 的连接的命令。

检查设备上的互联网连接

执行 **ping system** <*any OpenDNS server address*> 命令以检查设备是否可以访问互联网。

1. 通过控制台端口或使用 SSH 连接至设备的 CLI。
2. 使用“管理员”(Admin) 用户名和密码登录。
3. 输入 **ping system** <*OpenDNS IPAddress*>。

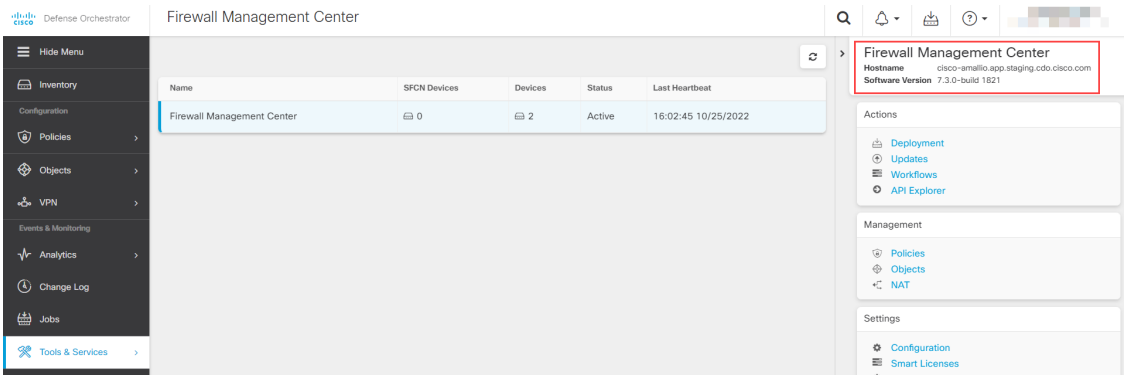
```
ping system 208.67.222.222
PING 208.67.222.222 (208.67.222.222) 56(84) bytes of data.
64 bytes from 208.67.222.222: icmp_seq=1 ttl=48 time=22.10 ms
64 bytes from 208.67.222.222: icmp_seq=2 ttl=48 time=22.10 ms
64 bytes from 208.67.222.222: icmp_seq=3 ttl=48 time=22.8 ms
64 bytes from 208.67.222.222: icmp_seq=4 ttl=48 time=22.6 ms
^C
--- 208.67.222.222 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 22.588/22.841/22.995/0.223 ms
```

上面的示例显示了设备可以使用 OpenDNS 服务器 IP 地址连接到互联网。此外，传输的数据包数与接收的数据包数相同，表明设备上的互联网连接可用。这就表明设备可以访问互联网。

注释 如果结果不匹配，请手动检查互联网连接。

检查与 云交付的防火墙管理中心 的设备连接

1. 获取 云交付的防火墙管理中心 的主机名。
    1. 从 CDO 导航窗格中，点击**工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。
    2. 点击**防火墙管理中心 (Firewall Management Center)** 可在右侧窗格中查看详细信息。
    3. 在**主机名 (Hostname)** 字段中，仅复制以下图例中显示的主机名。



在上图中，突出显示的文本是要复制的 FMC 的主机名 (*cdo-acc10.app.us.cdo.cisco.com*)。

2. 通过控制台端口或使用 SSH 连接至设备的 CLI。
3. 输入 **ping system** <*hostname of the FMC*>。

```
ping system cdo-acc10.app.us.cdo.cisco.com
PING cdo-acc10.app.us.cdo.cisco.com (54.187.125.161) 56(84) bytes of data.
^C
--- cdo-acc10.app.us.cdo.cisco.com ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 64ms
```

在上面的示例中，主机名会使用 IP 地址来解析，表示连接成功。忽略响应中显示的“100% 丢包”(100% packet loss) 消息。

注释 如果无法连接到主机，您可以使用 **configure network dns** <*address*> 在 CLI 中纠正 DNS 配置。

迁移程序

开始之前

在开始此过程之前，请确保满足以下前提条件：

- 已调配的 CDO 租户。
- CDO 已使用智能许可证进行注册。
- 管理中心 已被载入到 CDO。载入 管理中心 还会载入注册到 管理中心 的所有 威胁防御 设备。请参阅载入 FMC。

注释 在 管理中心 中创建具有管理员角色的新用户或具有用于载入的“设备”和“系统”权限的自定义用户角色。

注意 如果您将 本地管理中心 载入 CDO 并同时使用相同的用户名登录 本地管理中心 管理中心，则载入会失败。

- 威胁防御 设备必须同步，并且没有待处理的更改。如果CDO识别出该设备上有待处理的更改，则该设备上的迁移作业将失败。
- 管理中心 应允许出站 HTTP/HTTPS 将配置上传到 Amazon S3。
- CDO 会从 管理中心 导入访问控制策略中使用的系统日志 (Syslog) 警报对象。如果 CDO 已包含名称相同但类型不同的警报对象（SNMP、邮件），则会在配置导入期间重复使用该对象。

  用户必须检查系统日志对象名称是否与 CDO 中的现有 SNMP 或邮件警报对象匹配。如果名称匹配，则您必须在本地 管理中心 中重命名系统日志对象，然后才能开始迁移过程。
- 如果您尝试将包含已修改的系统定义的 FlexConfig 文本对象的防火墙从 本地管理中心 迁移到 云交付的防火墙管理中心，则修改后的系统定义的 FlexConfig 文本对象的值不会迁移到 云交付的防火墙管理中心，并且部署将失败。

  为避免这种情况，请在开始迁移之前执行以下任务：
  - 在迁移之前，将修改后的系统定义的 FlexConfig 文本对象值从 本地管理中心 复制到 云交付的防火墙管理中心。
  - 在验证预定义的 FlexConfig 文本对象后，启动从 本地管理中心 到 云交付的防火墙管理中心 的迁移。

过程

步骤 1 在左侧的导航栏中，点击**工具和服务 (Tools & Services)** > **迁移 (Migrations)** > **将 FTD 迁移到云**。

步骤 2 点击  图标启动 威胁防御 迁移流程。

注释 一次只能启动一个迁移作业。

步骤 3 在**选择本地 FMC (Select OnPrem FMC)** 步骤中，执行以下操作：

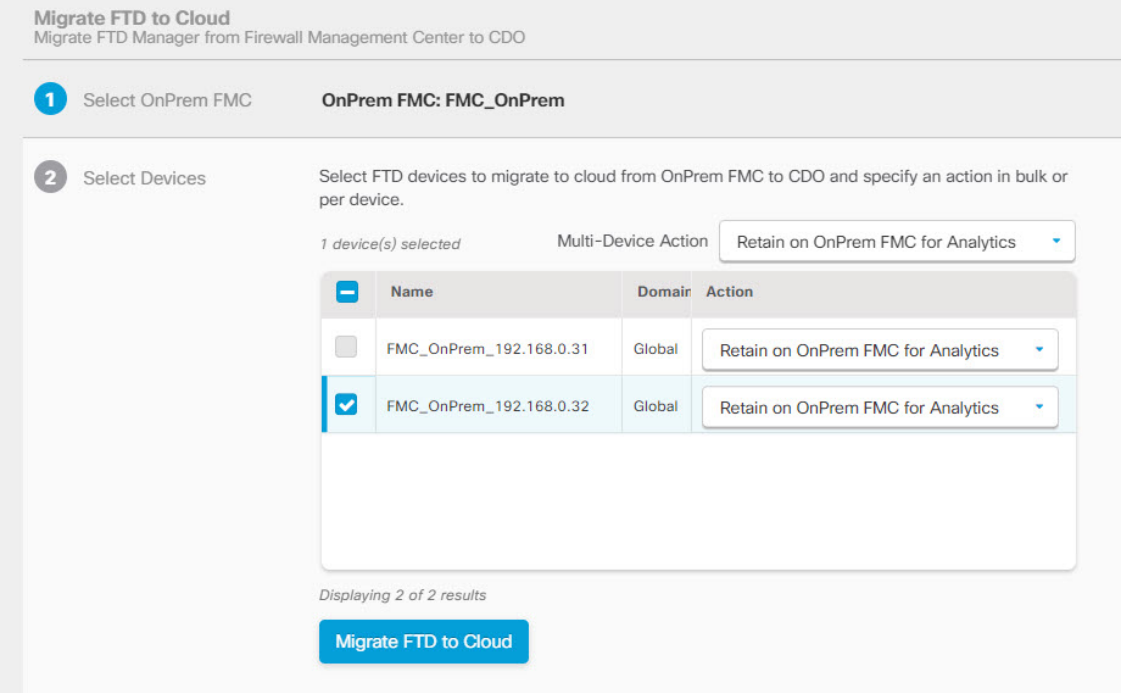
1. 如果尚未完成，可以点击**载入 FMC (Onboard an FMC)** 链接以载入本地 管理中心。请参阅载入 FMC。
2. 从可用列表中选择 管理中心 并点击**下一步 (Next)**。

在**选择设备 (Select Devices)** 步骤中，您将看到所选 管理中心 管理的 威胁防御 设备。

上次同步时间 (Last Synced time) 字段指明自设备配置同步到 管理中心 以来经过的时间。您可以点击**立即从本地 FMC 同步 (Sync from OnPrem FMC Now)** 以获取最新的设备更改。

步骤 4 在**选择设备 (Select Devices)** 步骤中，执行以下操作：

a) 选择要迁移的设备。



注释
- 无法选择在不支持的版本上运行的设备。
- 只在管理中心注册分析的设备或具有待部署的更改的设备不符合迁移的条件。
- CDO 仅允许选择高可用性对中的主用设备。在成功更改主用设备的管理器后，CDO 会自动更改备用设备的管理器，并在设备上保留高可用性配置。

b) 在**多设备操作 (Multi-Device Action)** 列表中，您可以选择要应用于所有设备的通用操作。

c) 在**提交操作 (Commit Action)** 列中，您可以为所选设备选择以下操作之一：

- **保留在本地 FMC 以进行分析 (Retain on OnPrem FMC for Analytics)**：在迁移过程完成后，所选 威胁防御 设备的分析管理将保留在 管理中心 上。
- **从本地 FMC 删除 FTD (Delete FTD from OnPrem FMC)**：迁移过程完成后，所选设备将从管理中心 中删除，并可供 CDO 用于处理分析。您必须配置设备，以便将事件发送至 CDO 进行管理分析。一旦将设备从 管理中心 中删除，它们就无法撤销。

  注释 除非自动或手动提交更改，否则不会从 管理中心 中删除设备。

注释 此处指定的操作将在 14 天评估期后自动提交，或在手动提交更改后提交。

步骤 5 点击**将 FTD 迁移到云 (Migrate FTD to Cloud)**。

步骤 6 点击**查看迁移到云的进度 (View Migration to Cloud Progress)** 以查看作业的进度。

下一步做什么

您可以查看迁移作业的整体和个别状态，并在作业成功完成时生成报告。请参阅查看 威胁防御 迁移作业，第 35 页。

查看 威胁防御 迁移作业

您可以查看从 CDO 启动的所有迁移作业的状态。您可以展开作业以查看与 管理中心 关联的各个设备的状态。

如果您已启用通知设置设备工作流程的警报，请点击通知图标  以查看迁移期间发生的警报。如果您已订用从 CDO 接收邮件通知，您也会收到邮件通知。

迁移作业成功后，您有 14 天的时间使用 CDO 来评估您的设备。在此期间，您可以修改或更改特定操作，或者将这些设备的管理更改回 管理中心。

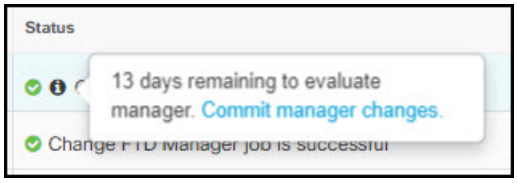
如果您确信迁移更改，我们建议手动提交设备。评估期到期后，CDO 会自动提交更改，而您无需执行进一步操作。提交操作会将更改应用于设备。请参阅手动提交管理器变更，第 38 页。

提交更改后，您将无法撤销在窗口中指定的操作。

重要事项 在评估期内，可以进行更改并使用 CDO 将其部署到使用的设备。如果您选择将设备管理恢复为 管理中心，则在恢复其管理器后，在评估期间进行的CDO特定更改将不会在设备上保留。在恢复设备管理器后，您必须将更改从本地 管理中心 部署到设备。

- **名称 (Name)**：表示作业名称，显示作业启动时的 管理中心 名称以及日期和时间。
- **FTD 数量 (Number of FTDs)**：这显示正在迁移到云的设备总数。
- **状态 (Status)**：显示作业的状态。展开作业以查看各个设备的状态。

  作业成功完成后，**状态 (Status)** 列中会显示 **FTD 迁移作业成功 (FTD Migration job is successful)** 消息。您可以点击工具提示以查看评估管理器的剩余天数。

  您可以点击手动提交管理器变更，在 14 天评估期结束之前手动提交更改。

- **上次更新 (Last Update)**：仅当设备发生更改时，才会更新日期和时间。

- **操作 (Actions)**：
  - **工作流程 (Workflows)**：提供一个链接，可将您定向到用于监控作业的工作流程页面。请参阅工作流程页面。
  - **下载报告 (Download Report)**：允许您生成并下载成功完成的每个作业的报告。请参阅生成威胁防御迁移报告，第 38 页。
  - **提交管理器更改 (Commit Manager Changes)**：允许您在评估期结束之前将更改手动应用到设备。请参阅手动提交管理器变更，第 38 页。
  - **删除迁移作业 (Remove Migration Job)**：允许您删除已完成的作业。此链接仅适用于已完成的作业。

在成功迁移后，CDO 会将配置部署到设备。如果系统在要部署的更改中发现错误或警告，则会在**验证消息 (Validation Messages)** 窗口中显示它们。要查看完整详细信息，请点击警告或错误前的箭头图标。如果部署失败，请参阅《Firepower 管理中心配置指南 X.Y》中的 部署配置更改最佳实践部分。

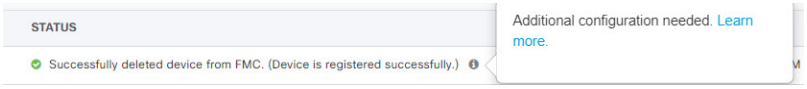
重要事项 在 14 天的评估期内，您无法从 CDO 中删除设备或本地 FMC。执行以下操作之一，然后删除设备或本地 FMC：

- 执行与要删除的本地 FMC 或设备关联的删除迁移作业。
- 选择**将管理器恢复至本地 FMC (Revert Manager to OnPrem FMC)**并手动提交管理器变更。

为身份策略配置领域序列

如果设备包含具有领域或 ISE 配置的身份策略，请将设备配置为 CDO 的代理以便与身份源通信。如果 CDO 无法连接到身份领域，则身份策略将不起作用。

需要额外配置的设备的**状态 (Status)** 列中会显示工具提示。

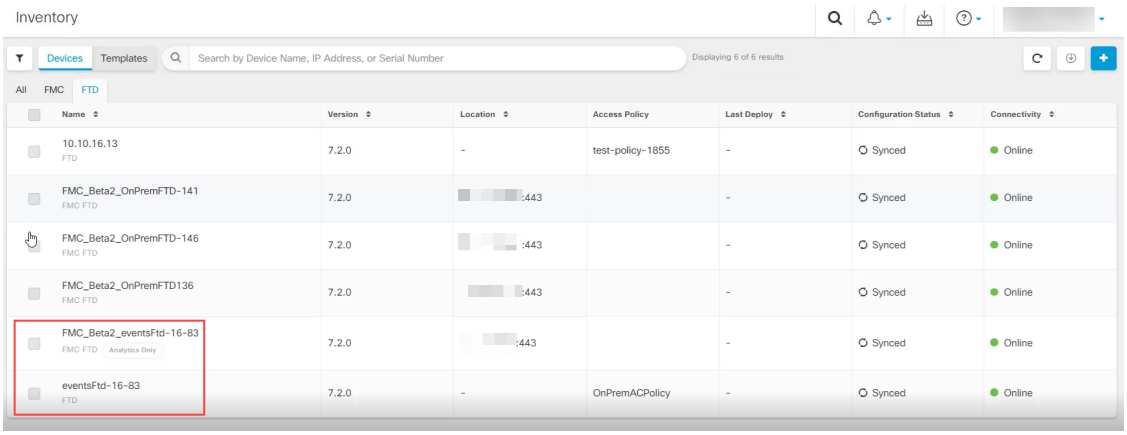


1. 点击工具提示图标，然后点击**了解更多 (Learn more)**。
2. 在**配置代理 (Configure Proxy)** 窗口中，点击**配置我的领域 (Configure my realms)**。

   要添加代理序列，请参阅《Firepower 管理中心设备配置指南，7.2》中的创建代理序列部分。

分析仅威胁防御设备示例

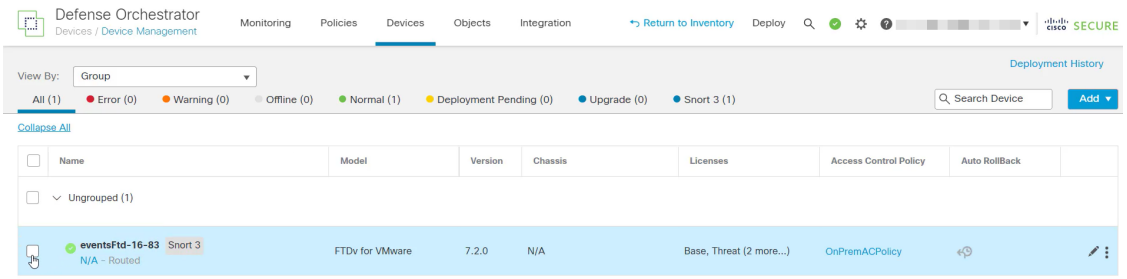
CDO 会创建同一个设备的两个实例，而该设备会被配置为保留在管理中心上进行分析。



带有 **FMC FTD** 和**仅分析 (Analytics Only)** 标签的设备实例显示由管理中心处理分析。带有 **FTD** 标签的设备实例表示由 CDO 管理其配置。

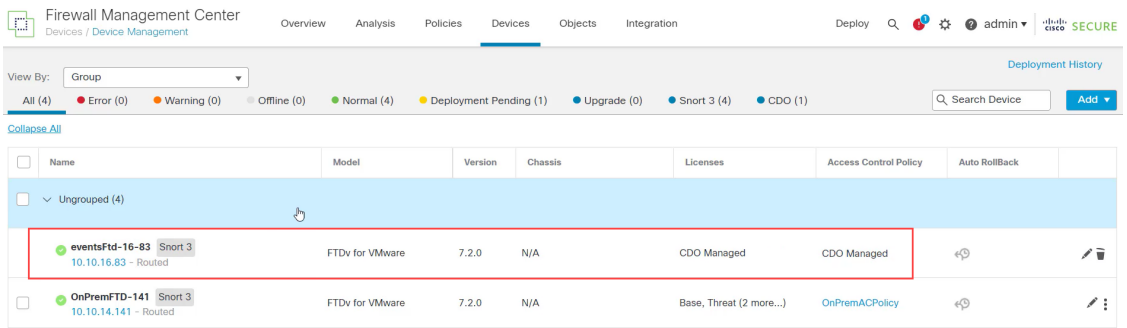
您可以使用CDO来管理设备的配置。要查看云交付的防火墙管理中心中的设备，请执行以下操作：

选择带有 **FTD** 标签的设备，然后在右侧的**管理 (Management)** 窗格中，点击**设备摘要 (Device Summary)**。



您可以在管理中心中查看设备中的事件。要查看事件，请执行以下操作：

1. 选择具有 **FMC FTD** 和**仅分析 (Analytics Only)** 标签的设备，然后点击右侧的**管理设备 (Manage Devices)** 链接。
2. 登录本地管理中心。
3. 点击**设备 (Device)** > **设备管理 (Device Management)**。



您无法选择此设备，因为 CDO 会管理配置。管理中心 会显示此设备的 **CDO 托管**标签。

要查看管理中心中的实时事件，请点击**分析 (Analysis)** > **事件 (Events)**。

生成威胁防御迁移报告

在迁移作业成功后，您可以生成并下载 PDF 格式的报告，以分析从 CDO 管理中心导入的每个参数的值。该报告提供与作业关联的每个设备的详细信息。详细信息包括有关设备、共享策略值、对象、路由详细信息、接口、网络设置等的信息。

在迁移作业页面上，点击已完成作业的**操作 (Actions)** 列下的 ...，然后点击**下载报告 (Download Report)**。。

手动提交管理器变更

如果您确信所做的更改正确无误，我们建议您手动提交管理器更改，而无需等待 CDO 自动提交更改。该窗口显示要恢复到作为设备管理器的管理中心或更改操作并将更改提交到CDO的剩余天数。在评估期间，您可以在确认更改之前更改所选威胁防御设备的指定操作。

更改一旦提交，您就无法撤销窗口中指定的操作。

注释 在以下情况时，提交管理器更改操作将被禁用：

- 已超出 14 天的评估期。
- 威胁防御 设备已被恢复或删除，在这种情况下，无法执行进一步操作。

过程

步骤 1 在迁移作业页面上，点击已完成作业的**操作 (Actions)** 列下的 ...。

步骤 2 点击**提交管理器更改 (Commit Manager Changes)**。仅当作业成功完成时，此链接才可用。

步骤 3 如果要更改为设备指定的操作，请选择设备，然后在**操作 (Actions)** 列表中选择操作：

- **保留本地 FMC 以进行分析 (Retain on OnPrem FMC for Analytics)**：在提交更改后，所选威胁防御设备的分析管理将保留在管理中心。
- **从本地 FMC 删除 FTD (Delete FTD from OnPrem FMC)**：在提交更改后，所选设备将从管理中心删除，并可供 CDO 用于处理分析。您必须配置威胁防御，以便将事件发送至 CDO 进行管理分析。一旦将威胁防御从 管理中心 中删除，它们就无法撤销。
- **将管理器恢复为本地 FMC (Revert Manager to OnPrem FMC)**：在提交更改后，设备管理将从 CDO 返回到 管理中心。

注释

- 在提交此操作后，您无法再次将设备的管理更改为 CDO。

  解决方法：您必须从 管理中心 中删除设备并将其载入。然后，您可以在 CDO 中更改设备的管理。

- 在提交此操作后，设备不会在 管理中心 中显示“过期”(Out-of-Date) 状态。

  解决方法：在本地 管理中心 上部署对设备的更改。

步骤 4 点击**提交 (Commit)** 会立即执行指定的操作，而无需进一步确认。

步骤 5 在迁移作业屏幕上，您可以展开作业以查看指定操作的进度。

删除迁移作业

您可以删除迁移作业，结果取决于删除时间

- 在 14 天的评估期内：停止迁移，并将与迁移作业关联的设备的配置恢复为原始状态。
- 提交迁移更改后：从迁移作业列表中删除记录。

过程

步骤 1 在迁移作业页面上，点击**操作 (Actions)** 列下的 ⋯，然后点击**删除迁移作业 (Remove Migration Job)**。

步骤 2 点击**删除 (Delete)** 以确认操作。

对 FTD 迁移到云进行故障排除

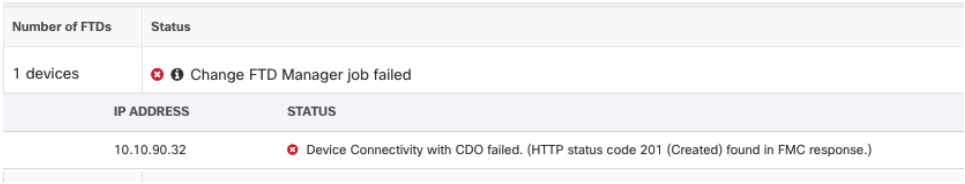
本节提供对将 FTD 迁移到云时可能发生的特定错误进行故障排除的信息。

在 FMC 响应中找到 HTTP 状态代码 201（已创建）

CDO 会在设备级别显示此错误。

问题：

安全设备连接器 (SDC) 版本不兼容。

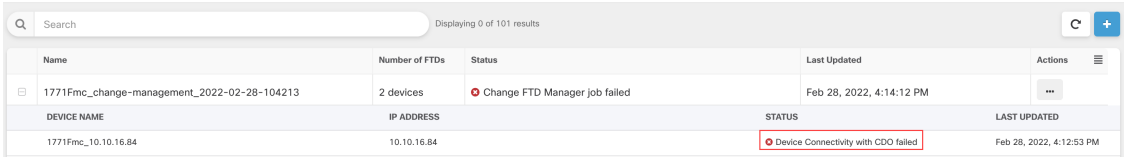


解决方法：

确保将 SDC 升级到“202205191350”或更高版本。

1. 导航至**管理 (Admin)** > **安全连接器 (Secure Connectors)**。
2. 点击 SDC，在右侧的**详细信息 (Details)** 窗格中查看现有 SDC 版本。
3. 更新安全设备连接器。

设备与 CDO 的连接失败



设备由于以下原因之一而无法访问 CDO：

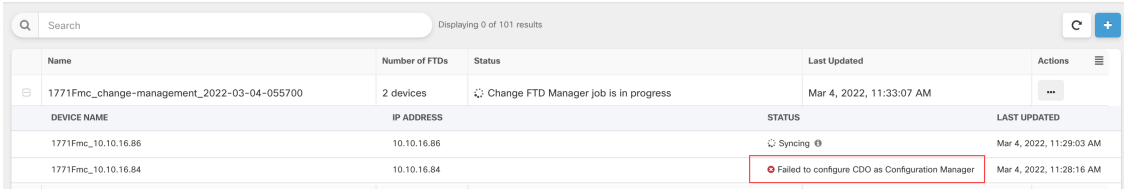
- 设备布线不正确。
- 您的网络可能要求提供设备的静态 IP 地址。
- 您的网络使用自定义 DNS，或者客户网络上存在外部 DNS 屏蔽。
- 需要进行 PPPoE 身份验证。
- 设备位于代理后面。

解决方法：

- 检查布线和网络连接。
- 确保您的防火墙未阻止任何流量。
- 通过 云交付的防火墙管理中心 验证威胁防御连接。

未能将 CDO 配置为配置管理器

当 CDO 由于网络丢失而无法与设备通信时，它无法使用云提供的防火墙管理中心来执行 configure manager 命令。



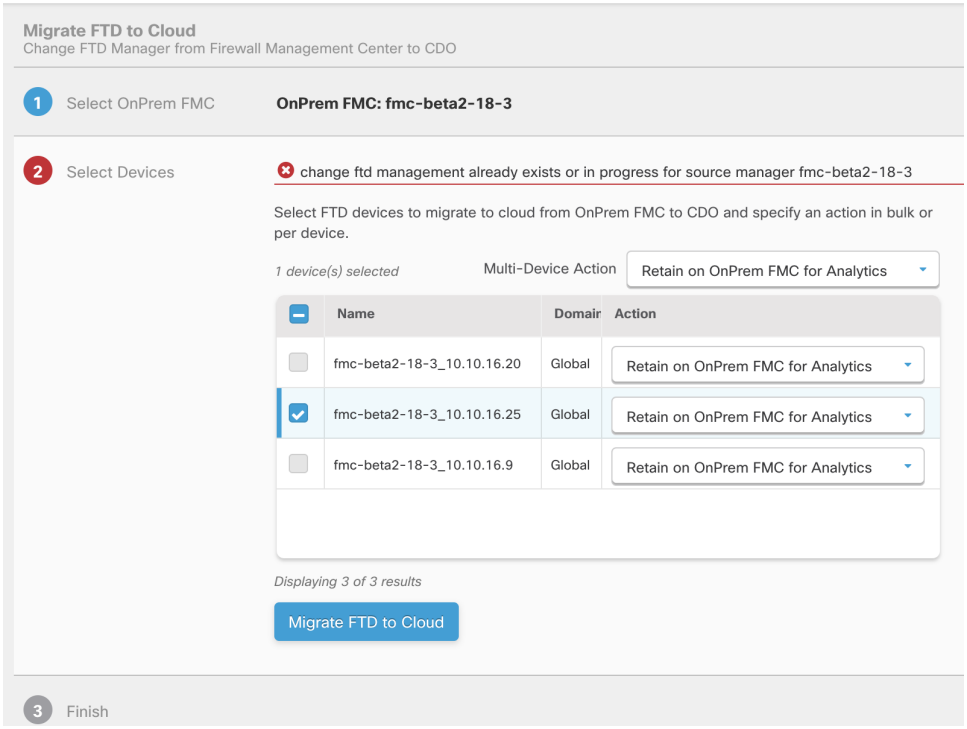
解决方法：

1. 检查布线和网络连接。
2. 确保您的防火墙未阻止任何流量。
3. 确保 FTD 具有互联网连接，并且 DNS 地址已被解析为 IP 地址。请参阅通过 云交付的防火墙管理中心 验证威胁防御连接，第 31 页。
4. 在新的变更管理器作业中，重新尝试从 CDO 迁移此 FTD。

变更管理器已存在或正在成为源管理器

只有当上一个作业完成时，才能为 本地管理中心 创建 FTD 迁移作业。

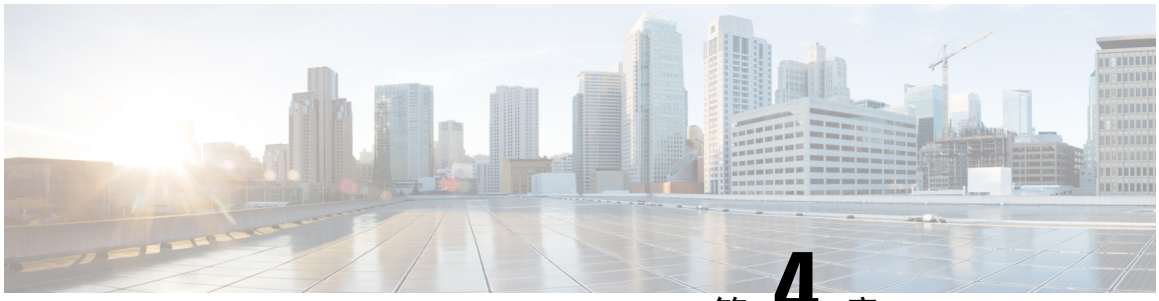
如果上一个作业正在进行中，在创建新作业时会发生此错误。



解决方法：

1. 导航到迁移表，以查看特定源本地管理中心是否正在进行其他作业。
2. 等待当前迁移作业完成。

3. 启动下一个迁移作业。



第 4 章

设备管理

本指南适用于作为主要管理器或仅作为分析管理器的本地 Cisco Secure Firewall Management Center。在将 思科防御协调器 (CDO) 云交付的防火墙管理中心 用作主管理器时，您只能使用本地部署 管理中心 进行分析。请勿将本指南用于 CDO 管理；请参阅使用 Cisco 防御协调器中的云交付防火墙管理中心管理防火墙威胁防御。

本章介绍如何在 Cisco Secure Firewall Management Center中 管理设备。

关于设备管理

使用 管理中心 来管理您的设备。

关于 管理中心 和设备管理

在 管理中心 管理设备时，它会在自己和设备之间设置双向、SSL 加密的通信信道。管理中心使用此信道向设备发送有关要如何分析和管理流向设备的网络流量的信息。设备评估流量时，会生成事件并使用同一信道将其发送到管理中心。

通过使用 管理中心管理设备，您可以执行以下操作：

- 从单个位置为所有设备配置策略，从而更轻松地更改配置
- 在设备上安装各种类型的软件更新
- 向受管设备推送运行状况策略并监控其运行状态 管理中心

注释 如果您有 CDO 托管设备，并且仅将本地部署 管理中心 用于分析，则本地部署 管理中心 不支持策略配置或升级。本指南中与设备配置和其他不支持的功能有关的章节和程序不适用于主管理器为CDO的设备。

管理中心汇总并关联入侵事件、网络发现信息和设备性能数据，从而能够监控设备报告的相互关联的信息，以及评估网络上出现的整体活动。

可以使用 管理中心来管理设备行为的几乎每个方面。

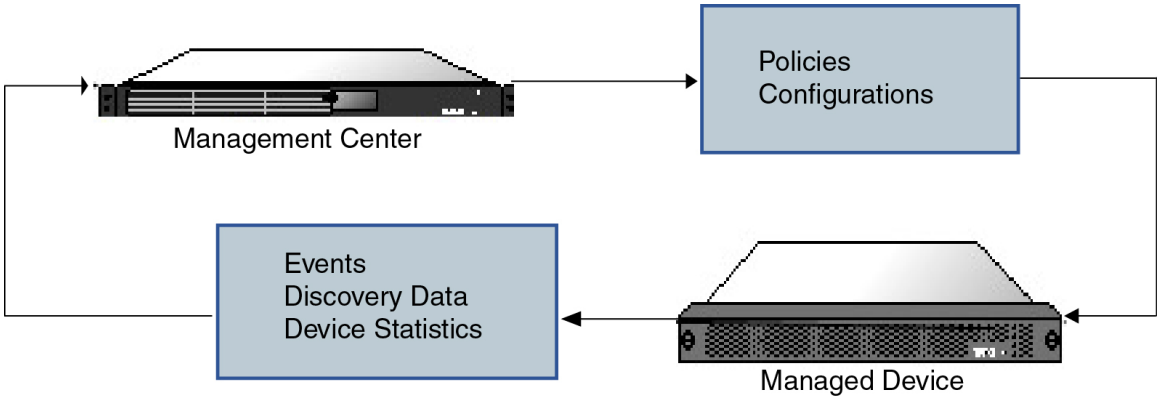
注释 尽管 管理中心 可以按照 http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html 处可用的兼容性矩阵中指定的那样管理运行之前的某些版本的设备，但需要最新版本 威胁防御 软件的新功能不适用于这些以前发布的设备。某些 管理中心 功能可能适用于早期版本。

Cisco Secure Firewall Management Center可以管理哪些内容？

您可以将 Cisco Secure Firewall Management Center 用作集中管理点来管理 威胁防御 设备。

管理设备时，信息通过 SSL 加密的安全 TCP 隧道在 管理中心和该设备之间传输。

下图列出了在管理中心 及其托管设备之间传输的内容。请注意，设备间发送的事件和策略的类型基于设备类型。



关于管理连接

使用 管理中心 信息配置设备并将设备添加到 管理中心后，设备或 管理中心 可以建立管理连接。根据初始设置：

- 设备或 管理中心 都可以启动。
- 只有设备可以启动。

- 只有 管理中心 可以发起。

启动始终使用 管理中心 上的 eth0 或设备上编号最低的管理接口。如果未建立连接，则会尝试其他管理接口。管理中心上的多个管理接口可让您连接到离散网络或隔离管理和事件流量。但是，发起方不会根据路由表选择最佳接口。

注释 管理连接是信道自身与设备之间的 SSL 加密的安全通信信道。出于安全目的，您不需要通过额外的加密隧道（例如站点间 VPN）运行此流量。例如，如果 VPN 发生故障，您将失去管理连接，因此我们建议使用简单的管理路径。

除策略和事件以外的其他功能

除将策略部署到设备和从其接收事件以外，还可以在 管理中心上执行其他设备相关任务。

备份设备

您无法从 FTD CLI 备份物理托管设备。要备份配置数据和（可选的）统一文件，请使用管理管理中心执行设备备份。

要备份事件数据，请对管理设备的 管理中心 执行备份。

更新设备

思科会不定期发布 Firepower 系统更新，包括：

- 入侵规则更新，其中可能包含新的和已更新的入侵规则
- 漏洞数据库 (VDB) 更新
- 地理位置更新
- 软件补丁和更新

可以使用 管理中心在其管理的设备上安装更新。

关于设备管理接口

每个设备都包含一个用于与 管理中心通信的管理接口。您可以选择将设备配置为使用数据接口进行管理，而不是专用的管理接口。

您可以在管理接口或控制台端口上执行初始设置。

管理接口还用于与智能许可服务器通信、下载更新以及执行其他管理功能。

威胁防御上的管理和事件接口

设置设备时，指定要连接到的管理中心IP地址或主机名称（如已知）。如果设备启动了连接，管理和事件流量都在初始注册时转到此地址。如果 管理中心 未知，则 管理中心 建立初始连接。在这种

情况下，它最初可能从与 威胁防御上指定的不同的 管理中心 管理接口连接。后续连接应使用具有指定 IP 地址的 管理中心 管理接口。

如果 管理中心 具有单独的仅事件接口，则托管设备会在网络允许的情况下将后续事件流量发送到管理中心 仅事件接口。此外，某些托管设备型号包括一个额外的管理接口，您可以为仅事件流量配置该接口。请注意，如果您配置用于管理的数据接口，则不能使用单独的管理接口和事件接口。如果事件网络关闭，则事件流量将恢复到 管理中心 和/或托管设备上的常规管理接口。

使用 威胁防御 数据接口进行管理

您可以使用专用的管理接口或常规数据接口与管理中心通信。如果想要从外部接口远程管理威胁防御 ，或者您没有单独的管理网络，则在数据接口上进行管理器访问非常有用。

管理器访问要求

从数据接口进行管理器访问遵循以下要求。

- 只能在 物理数据接口上启用管理器访问。不能使用子接口或 EtherChannel。
- 此接口不能是仅管理接口。
- 仅路由防火墙模式，使用路由接口。
- 不支持 PPPoE。如果您的 ISP 需要 PPPoE，则必须在 威胁防御 与 WAN 调制解调器之间放入支持 PPPoE 的路由器。
- 接口只能位于全局 VRF 中。
- 默认不对数据接口启用 SSH，因此必须稍后使用 管理中心 来启用 SSH。由于管理接口网关将更改为数据接口，因此您也无法启动从远程网络到管理接口的 SSH 会话，除非您使用 **configure network static-routes** 命令为管理接口添加静态路由。对于 Amazon Web 服务上的 threat defense virtual ，控制台端口不可用，因此您应保持对管理接口的 SSH 访问：在继续配置之前为管理添加静态路由。或者，请确保在配置用于管理器访问的数据接口并断开连接之前完成所有 CLI 配置（包括 **configure manager add** 命令）。
- 不支持集群技术。在这种情况下，必须使用管理接口。
-

每个设备型号的管理接口支持

有关管理接口位置，请参阅您的型号的硬件安装指南。

注释 对于 Firepower 4100/9300，MGMT 接口用于机箱管理，而不是用于 威胁防御逻辑设备管理。必须将单独的接口配置为 mgmt（和/或 firepower-eventing）类型，然后将其分配给 威胁防御 逻辑设备。

注释 对于任何机箱上的 威胁防御，物理管理接口在诊断逻辑接口（对 SNMP 或系统日志有用，并且与管理中心中的数据接口一起配置）与管理逻辑接口（用于 管理中心通信）之间共享。有关详细信息，请参阅管理/诊断接口，第 491 页。

有关每个托管设备型号上支持的管理接口，请参阅下表。

表 4: 受管设备上的管理接口支持

型号	管理界面	可选的事件接口
Firepower 1000	management0 注释 management0 是管理 1/1 接口的内部名称。	不支持
Firepower 2100	management0 注释 management0 是管理 1/1 接口的内部名称。	不支持
Secure Firewall 3100	management0 注释 management0 是管理 1/1 接口的内部名称。	不支持
Firepower 4100 和 9300	management0 注释 management0 是此接口的内部名称，与物理接口 ID 无关。	management1 注释 management1 是此接口的内部名称，与物理接口 ID 无关。
ISA 3000	br1 注释 br1 是管理 1/1 接口的内部名称。	不支持
Cisco Secure Firewall Threat Defense Virtual	eth0	不支持

设备管理接口上的网络路由

管理接口（包括事件专用接口）仅支持通过静态路由到达远程网络。在设置托管设备时，设置进程将为您指定的网关 IP 地址创建一个默认路由。不能删除此路由；只能修改网关地址。

注释 用于管理接口的路由完全独立于您为数据接口配置的路由。如果配置用于管理的数据接口而不是使用专用管理接口，则流量将通过背板路由以使用数据路由表。本节中的信息不适用。

在某些平台上，可以配置多个管理接口（一个管理接口和一个仅事件接口）。默认路由不包括出口接口，因此选择的接口取决于您指定的网关地址以及网关属于哪个接口的网络。如果默认网络上有多个接口，设备将使用编号较低的接口作为出口接口。

如果要访问远程网络，建议为每个管理接口使用至少一个静态路由。我们建议将每个接口放在单独的网络中，以避免潜在的路由问题，包括从其他设备到 威胁防御的路由问题。

注释 用于管理连接的接口不由路由表决定。始终首先使用编号最低的接口来进行连接。

NAT 环境

网络地址转换 (NAT) 是一种通过路由器传输和接收网络流量的方法，其中涉及重新分配源或目标 IP 地址。NAT 最常见的用途是允许专用网络与互联网进行通信。静态 NAT 执行 1:1 转换，这不会引发管理中心与设备的通信问题，但端口地址转换 (PAT) 更为常用。PAT 允许您使用单一的公共 IP 地址和独特端口来访问公共网络；这些端口是根据需要动态分配的，因此您无法启动与 PAT 路由器后的设备的连接。

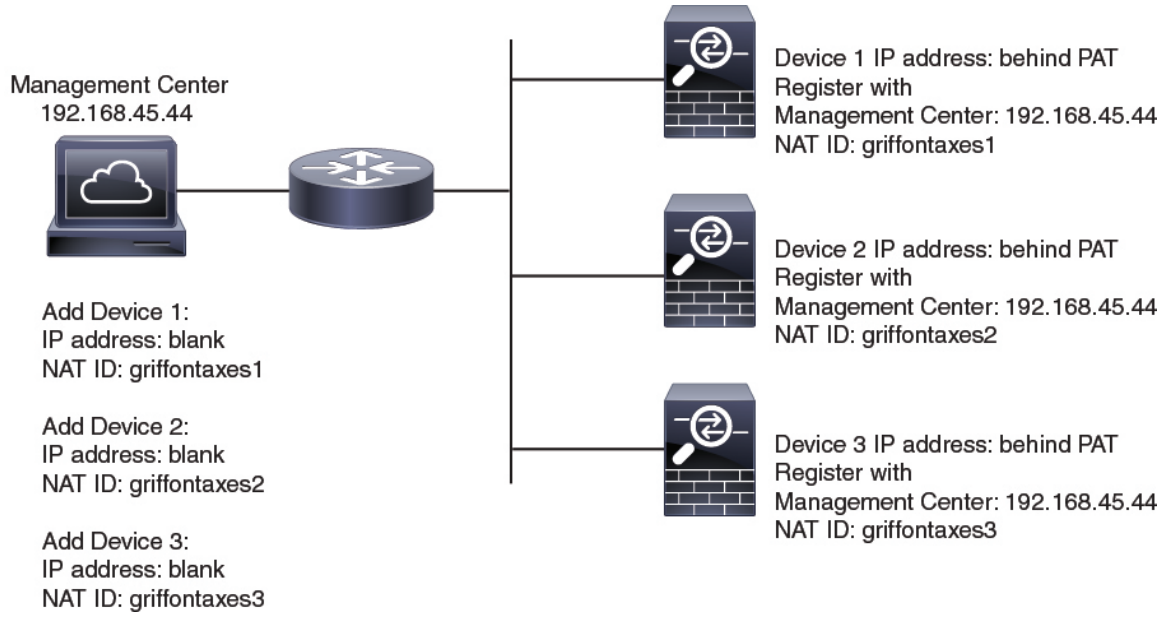
通常，无论是路由目的还是身份验证，都需要两个IP地址（连同一个注册密钥）：管理中心 当添加一个设备时，指定设备 IP 地址，设备指定 管理中心 IP 地址。但是，如果您只知道其中一个 IP 地址（这是实现路由目的的最低要求），您还必须在连接的两端指定唯一的NAT ID，以建立对初始通信的信任，并查找正确的注册密钥。管理中心和设备使用注册密钥和 NAT ID（而不是 IP 地址）对初始注册进行身份验证和授权。

例如，您将设备添加到 管理中心，但不知道设备 IP 地址（例如，设备在 PAT 路由器后），因此只需要在 管理中心 上指定 NAT ID 和注册密钥；将 IP 地址留空。在设备上，指定 管理中心 IP 地址、相同的 NAT ID 和相同的注册密钥。设备将注册到 管理中心的 IP 地址。此时，管理中心将使用 NAT ID 而不是 IP 地址对设备进行身份验证。

尽管 NAT ID 最常用于 NAT 环境，但您可以选择使用 NAT ID 来简化向 管理中心添加多个设备的过程。在 管理中心上，在将 IP 地址留空的同时为要添加的每个设备指定唯一的 NAT ID，然后在每个设备上指定 管理中心 IP 地址和 NAT ID。注意：每个设备的 NAT ID 必须是唯一的。

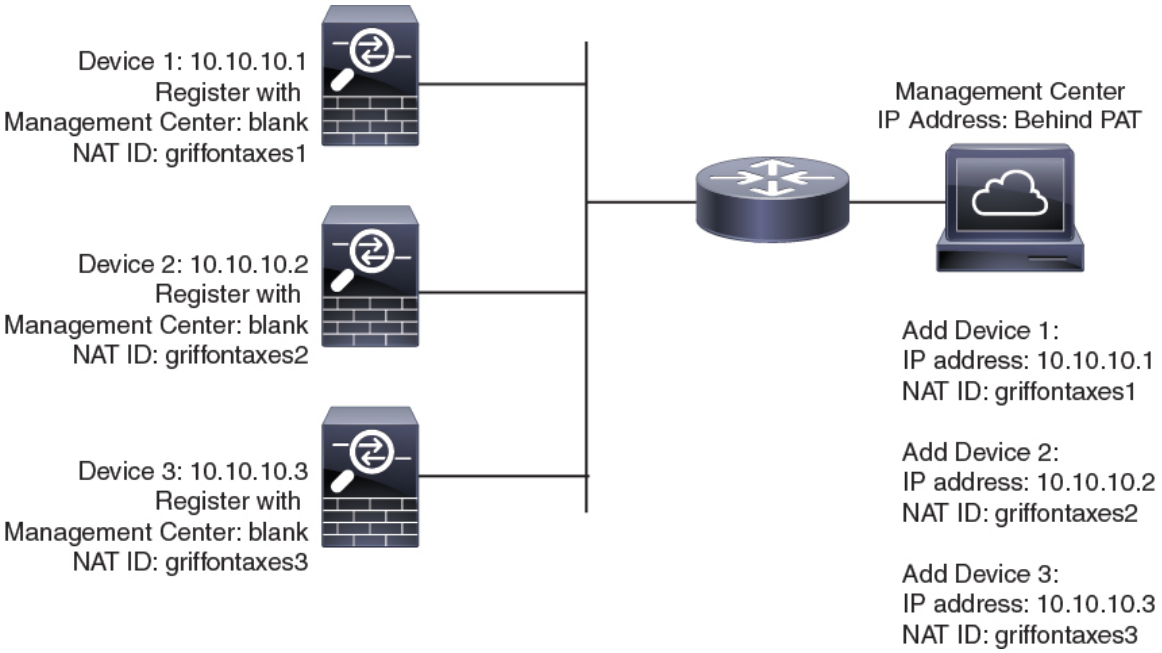
以下示例为 PAT IP 地址后的三个设备。在这种情况下，在 管理中心 和这些设备上为每个设备指定一个唯一的 NAT ID，并在这些设备上指定 管理中心 IP 地址。

图 *1: PAT* 后的受管设备 *NAT ID*



以下示例为 PAT IP 地址后的 管理中心。在这种情况下，在 管理中心 和这些设备上为每个设备指定一个唯一的 NAT ID，并在 管理中心 上指定设备 IP 地址。

图 *2: PAT* 后的 *FMC NAT ID*

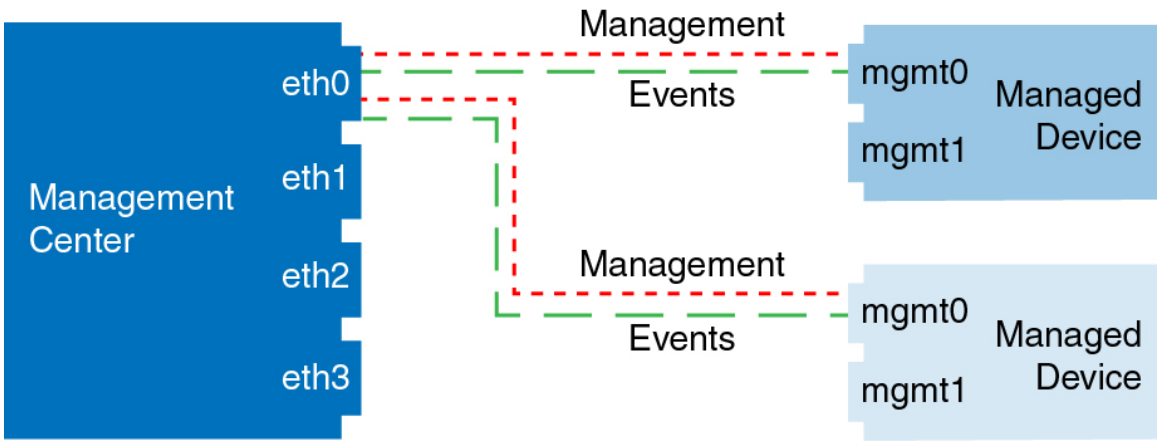


管理和事件流量通道示例

注释 如果在 威胁防御上使用数据接口进行管理，则不能对该设备使用单独的管理接口和事件接口。

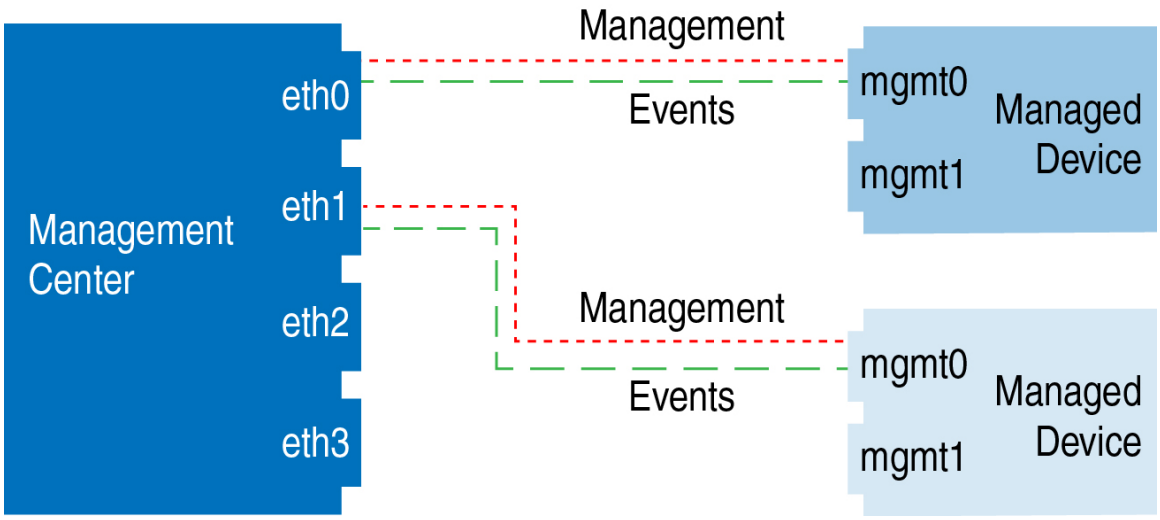
以下示例显示仅使用默认管理接口的 管理中心和受管设备。

图 *3: Cisco Secure Firewall Management Center*上的单个管理接口



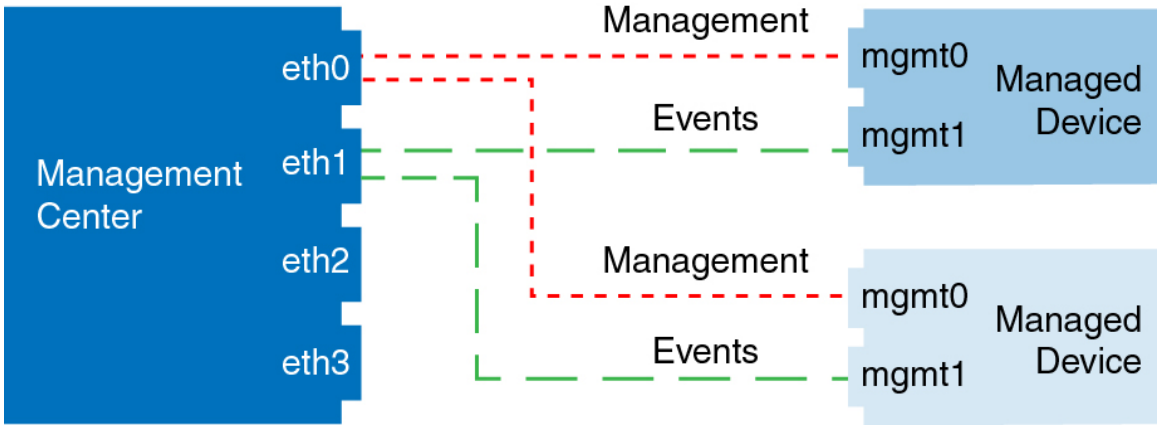
以下示例显示为设备使用单独管理接口的 管理中心；每台受管设备均使用 1 管理接口。

图 *4: Cisco Secure Firewall Management Center*上的多个管理接口



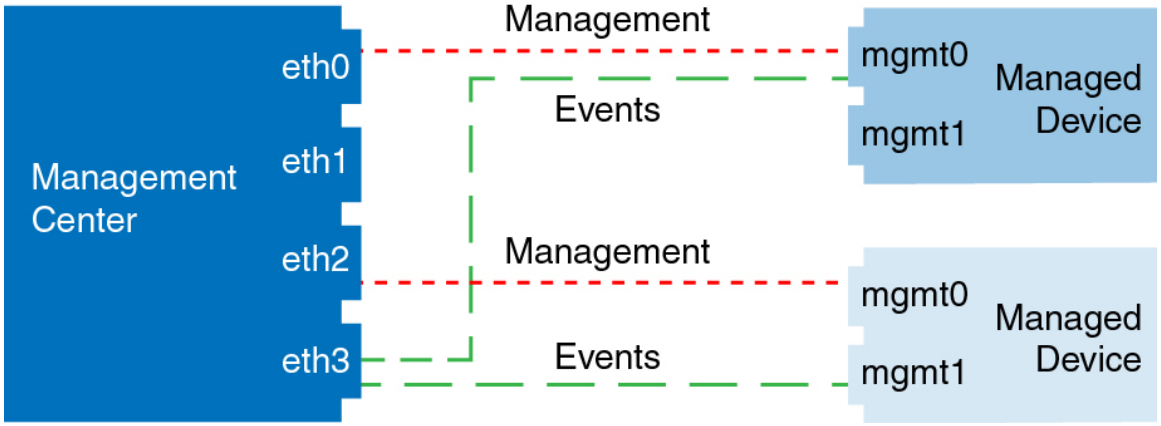
以下示例显示使用单独事件接口的 管理中心和受管设备。

图 *5: Cisco Secure Firewall Management Center*和受管设备上的单独事件接口



以下示例显示 管理中心上多个管理接口与单个事件接口的混合，以及使用单独事件接口或使用单个管理接口的受管设备的混合。

图 *6:* 混合管理和事件接口用法



添加设备组

管理中心允许将设备分组，从而可以在多台设备上轻松部署策略和安装更新。您可以展开和折叠组中的设备列表。

在多域部署中，您可以只在分叶域内创建设备组。当您为多租户配置Cisco Secure Firewall Management Center时，现有设备组会被删除；您可以在分叶域级别重新添加这些组。

如果将高可用性对中的主设备添加到某个组，则系统会将两台设备均添加到该组中。如果取消高可用性，则两台设备均会保留在该组中。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 从**添加 (Add)** 下拉菜单中，选择**添加组 (Add Group)**。

要编辑现有的组，请点击要编辑的组的 **编辑**（）。

步骤 3 输入 **Name**。

步骤 4 在**可用设备 (Available Devices)** 下，选择一台或多台要添加到设备组的设备。点击的同时使用 Ctrl 或 Shift 选择多台设备。

步骤 5 点击**添加 (Add)** 将所选设备包含在设备组中。

步骤 6 或者，要将设备从设备组中删除，请点击要删除的设备旁边的 **删除**（）。

步骤 7 点击**确定 (OK)** 以添加组。

关闭设备

正确关闭系统非常重要。仅拔掉电源或按下电源开关可能会导致文件系统严重损坏。请记住，有许多进程一直在后台运行，拔掉或关闭电源不能正常关闭防火墙。

请参阅以下任务以正确关闭系统。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要重新启动的设备旁边，点击 **编辑**（）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击**设备 (Device)**。

步骤 4 要关闭设备：

a) 在**系统 (System)** 部分中点击 **关闭设备**（）。

b) 出现提示时，确认是否要关闭设备。

c) 如果您与防火墙建立了控制台连接，请在防火墙关闭时留意系统提示。您将看到以下提示：

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

如果没有控制台连接，请等待大约 3 分钟以确保系统已关闭。

步骤 5 要重启设备：

a) 请点击 **重启设备**（）。

b) 出现提示时，确认是否要重启设备。

配置设备设置

“设备管理”(Device Management) 页面为您提供一系列信息和选项：

- “查看方式”(View By) - 使用此选项可根据组、许可证、型号、或访问控制策略查看设备。
- “设备状态”(Device State) - 您还可以根据设备的状态来查看设备。您可以点击状态图标查看属于它的设备。括号内为各状态所对应的的设备数量。
- “搜索”(Search) - 您可以通过提供设备名称、主机名或 IP 地址来搜索已配置的设备。
- “添加选项”(Add options) - 您可以添加设备、高可用性对、集群和组。
- “编辑和其他操作”(Edit and other actions) - 针对每个已配置的设备，使用 **编辑**（ ） 图标来编辑设备参数和属性。点击 **更多**（ ） 图标并执行其他操作：
  - “访问控制策略”(Access Control Policy) - 点击访问控制策略列中的链接以查看部署到设备的策略。
  - “删除”(Delete) - 删除设备。
  - “数据包跟踪器”(Packet Tracer) - 导航至数据包跟踪器页面，以便通过将模型数据包注入系统来检查设备上的策略配置。
  - “数据包捕获”(Packet Capture) - 导航至数据包捕获页面，您可以在其中查看系统在处理数据包时所采取的判定和操作。
  - “恢复升级”(Revert Upgrade) - 恢复上次升级后所做的升级和配置更改。此操作会将设备恢复到升级前的版本。
  - “运行状况监控器”(Health Monitor) - 导航至设备的运行状况监控页面。
  - “故障排除文件”(Troubleshooting Files) - 生成故障排除文件，您可以在其中选择要在报告中包含的数据类型。
  - 对于 Firepower 4100/9300 系列设备，是一个指向 机箱管理器 Web 界面的链接。

点击设备时，系统将显示包含多个选项卡的设备属性页面。您可以使用选项卡来查看设备信息，以及配置路由、接口、内联集和 DHCP。

编辑常规设置

设备 (Device) 页面上的 **常规 (General)** 部分会显示下表所述信息。

表 5:“常规”(General) 部分表字段

字段	说明 (Description)
名称	管理中心上的设备的显示名称。
传输数据包	显示受管设备是否将数据包数据随事件一起发送到 管理中心 。
模式	显示设备的管理接口的模式：**路由**或**透明**。
合规模式	显示设备的安全认证合规性。有效值为 CC、UCAPL 和 None。
TLS 加密加速：	显示 TLS 加密加速是已启用还是已禁用。
设备配置	允许您复制、导出或导入配置。请参阅将配置复制到另一台设备，第 54 页和导出和导入设备配置，第 56 页。

您可以在此部分编辑其中一些设置。

过程

步骤 1 选择 **设备** > **设备管理**。

步骤 2 在要修改的设备名单旁，点击 **编辑**（ ）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击**设备 (Device)**。

步骤 4 在**常规 (General)** 部分中，点击 **编辑**（ ）。

a) 输入托管设备的**名称 (Name)**。

b) 选择**转换数据包 (Transfer Packets)** 复选框以允许数据包数据随事件一起存储在 管理中心 上。

c) 点击**强制部署 (Force Deploy)** 以强制将当前策略和设备配置部署到设备。

注释 强制部署比常规部署需要更多时间，因为它涉及要在 威胁防御上部署的策略规则的完整生成。

步骤 5 有关**设备配置** 操作，请参阅将配置复制到另一台设备，第 54 页和导出和导入设备配置，第 56 页。

步骤 6 点击**部署 (Deploy)**。

下一步做什么

- 部署配置更改。

将配置复制到另一台设备

在网络中部署新设备时，可以直接复制预配置设备上的配置和策略，而无需手动重新配置新设备。

开始之前

确认：

- 源和目标 威胁防御 设备型号相同并运行同一版本的软件。
- 源设备为独立 Cisco Secure Firewall Threat Defense设备或 Cisco Secure Firewall Threat Defense高可用性对。
- 目标设备为独立 威胁防御设备。
- 源和目标 威胁防御设备具有相同数量的物理接口。
- 源和目标 威胁防御设备的防火墙模式相同 - 路由或透明。
- 源和目标 威胁防御设备的安全认证合规性模式相同。
- 源和目标 威胁防御设备在同一域中。
- 源或目标 威胁防御设备上未在进行配置部署。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要修改的设备名单旁，点击 **编辑**（）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备**。

步骤 4 在**常规**部分中，执行以下操作之一：

- 点击 **获取设备配置** （） 以将设备配置从其他设备复制到新设备。在**获取设备配置**页面中，从**选择设备**下拉列表中选择源设备。
- 点击 **推送设备配置** （） 以将设备配置从当前设备复制到新设备。在**推送设备配置**页面上，从**目标设备**下拉列表中选择复制配置的目标设备。

步骤 5 （可选）选中**包括共享策略配置 (Include shared policies configuration)** 复选框以复制策略。

共享策略（例如访问控制策略、NAT、平台设置和 FlexConfig 策略）可在多个设备之间共享。

步骤 6 点击**确定**。

您可以在消息中心中的 **任务 (Tasks)** 监控复制设备配置任务的状态。

复制设备配置任务发起后，便会擦除目标设备上的配置，并将源设备的配置复制到目标设备。

警告 完成复制设备配置任务后，无法将目标设备还原为其原始配置。

导出和导入设备配置

您可以导出设备特定的配置：

- 接口
- 内联集
- 路由
- DHCP
- 关联对象

然后，您可以在以下使用案例中为同一设备导入已保存的配置：

- 将设备移动到其他 管理中心 - 首先从原始 管理中心中删除设备，然后将设备添加到新的 管理中心。然后，您可以导入保存的配置。
- 在域之间移动设备 - 在域之间移动设备时，不会保留某些设备特定的配置，因为新域中不存在支持对象（例如安全区域的接口组）。通过在域移动后导入配置，将为该域创建任何必要的对象，并恢复设备配置。
- 恢复旧配置 - 如果部署的更改会对设备的运行产生负面影响，则可以导入已知工作配置的备份副本，以恢复以前的运行状态。
- 重新注册设备 - 如果从管理中心中删除设备，但随后想要重新添加，则可以导入已保存的配置。

请参阅以下准则：

- 您只能将配置导入到同一设备（UUID 必须匹配）。您无法将配置导入到其他设备，即使是同一型号也是如此。
- 如果对象不存在，系统将创建该对象。如果对象存在，但值不同，请参阅下文：

表 *6:* 对象导入操作

场景	导入操作
存在具有相同名称的对象	重用现有对象
存在名称相同但值不同的对象	• 网络和端口对象 - 为此设备创建对象覆盖。请参阅对象覆盖 ， 第 967 页。 • 接口对象 - 创建新对象。例如，如果类型（安全区域或接口组）和接口类型（例如，路由或交换）不匹配，则会创建新对象。 • 所有其他对象 - 即使值不同，也可重复使用现有对象。
对象不存在	创建新对象

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑的设备旁边，点击 **编辑**（ ）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备**。

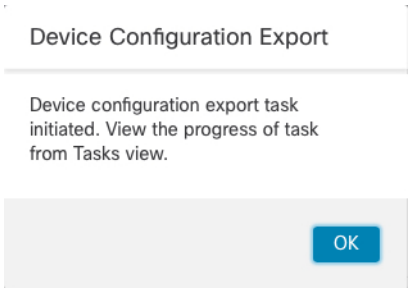
步骤 4 导出配置。

a) 在**常规 (General)** 区域，点击**导出 (Export)**。

图 7: 导出设备配置

系统将提示您确认导出；点击**确定 (OK)**。

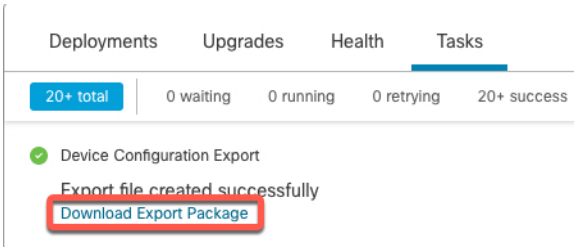
图 8: 确认导出



您可以在**任务 (Tasks)** 页面中查看导出进度。

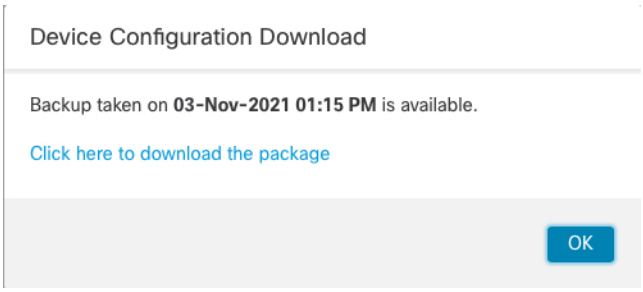
b) 在**通知 (Notifications)** > **任务 (Tasks)** 页面上，确保导出已完成；点击**下载导出包 (Download Export Package)**。或者，您可以点击**常规 (General)** 区域中的**下载 (Download)** 按钮。

图 *9:* 导出任务



系统将提示您下载软件包；点击**点击此处下载软件包 (Click here to download the package)** 以本地保存文件，然后点击**确认 (OK)** 以退出对话框。

图 *10:* 下载软件包



步骤 5 导入配置。

a) 在**常规 (General)** 区域中，点击**导入 (Import)**。

图 *11:* 导入设备配置

系统将提示您确认将替换当前配置。点击**是 (Yes)**，然后导航到配置包（使用后缀 .sfo；请注意，此文件与备份/恢复文件不同）。

图 *12:* 导入软件包

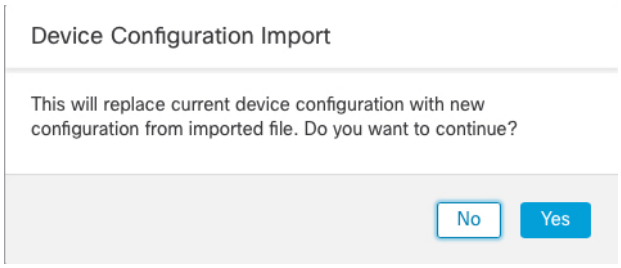
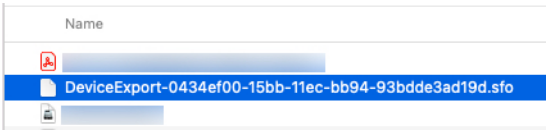
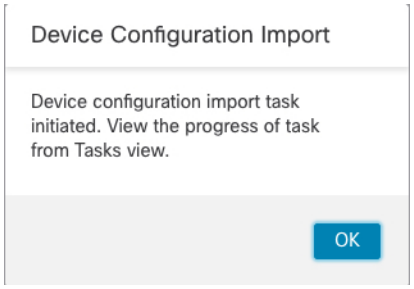


图 *13:* 导航至软件包



系统将提示您确认导入；点击**确认 (OK)**。

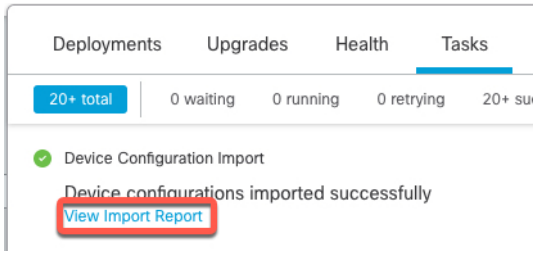
图 *14:* 确认导入



您可以在**任务 (Tasks)** 页面中查看导入进度。

b) 查看导入报告，以便查看导入的内容。在导入任务的**通知 (Notifications)** > **任务 (Tasks)** 页面上，点击**查看导入报告 (View Import Report)**。

图 *15:* 查看导入报告



设备配置导入报告 (Device Configuration Import Reports) 页面提供可用报告的链接。

Cisco Firepower Management Center

Device Configuration Import Reports

Device	Shared Policies	Device Configurations
0434ef00-15bb-11ec-bb94-93bdde3ad19d	Report does not exist	Device configurations import report

编辑许可证设置

设备 (Device) 页面的**许可证 (License)** 部分显示为设备启用的许可证。

如果在管理中心上有可用的许可证，则可以启用设备上的许可证。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要启用或禁用许可证的设备旁边，点击 **编辑**（）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击**设备 (Device)**。

步骤 4 在**许可证 (License)** 部分中，点击 **编辑**（）。

步骤 5 选中或取消选中要为受管设备启用或禁用的许可证旁边的复选框。

步骤 6 点击**保存 (Save)**。

下一步做什么

- 部署配置更改。

查看系统信息

设备 (Device) 页面的“系统”(System) 部分显示只读系统信息表，如下表中所述。

也可以关闭或重新启动设备。

表 *7:* 系统部分表字段

字段	说明 (Description)
型号	受管设备的型号名称和编号。

字段	说明 (Description)
序列 (Serial)	受管设备的机箱的序列号。
时间	设备的当前系统时间。
时区	显示时区。
版本	受管设备上当前安装的软件版本。
时间型规则的时区设置：	设备的当前系统时间，以设备平台设置中指定的时区为准。

查看检测引擎

设备 (Device) 页面的“检测引擎”(Inspection Engine) 部分会显示您的设备是使用 Snort2 还是 Snort3。要切换检测引擎，请参阅 《Cisco Secure Firewall Management Center Snort 3 配置指南》 。

查看运行状况信息

设备 (Device) 页面上的**运行状况 (Health)** 部分显示下表所述信息。

表 *8:* 运行状况部分表字段

字段	说明 (Description)
状态 (Status)	一个代表设备当前运行状况的图标。点击该图标将显示设备的“运行状况监控器”(Health Monitor)。
策略	一个指向当前部署在设备上的运行状况策略的只读版本的链接。
已排除	一个指向“运行状况排除”(Health Exclude) 页面的链接，您可以在该页面上启用和禁用运行状况排除模块。

编辑管理设置

您可以在**管理 (Management)** 区域中编辑管理设置。

更新 管理中心中的主机名或 IP 地址

如果您在将设备的主机名或 IP 地址添加到 管理中心 后，对其进行编辑（例如使用设备的 CLI），可能需要使用以下操作步骤手动更新管理 管理中心 上的主机名或 IP 地址。

更改设备管理 IP 地址的步骤，请参阅 在 CLI 中修改 威胁防御 管理接口 ， 第 78 页。

过程

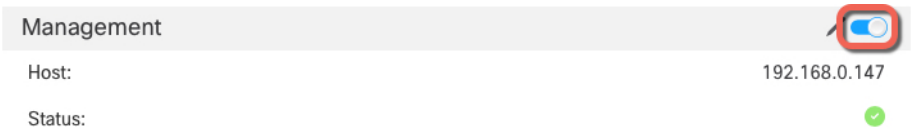
步骤 1 选择**设备** > **设备管理**。

步骤 2 在要修改管理选项的设备旁边，点击 **编辑**（）。

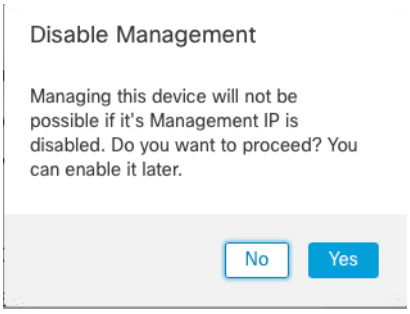
在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击**设备 (Devices)**，并查看**管理 (Management)** 区域。

步骤 4 点击滑块暂时禁用管理，使其处于禁用状态（）。

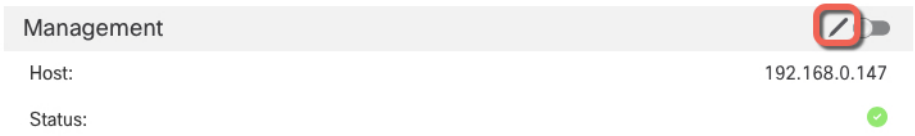


系统将提示您继续禁用管理；点击 **是**。



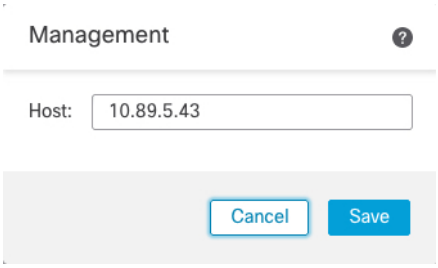
禁用管理会阻止 管理中心和设备之间的连接，但**不**会从 管理中心删除设备。

步骤 5 通过点击 **编辑**（） 来编辑**主机** IP 地址或主机名。



步骤 6 在**管理 (Management)** 对话框中，在**主机 (Host)** 字段中修改名称或 IP 地址，然后点击**保存 (Save)**。

图 *16:* 管理 *IP* 地址



步骤 7 点击滑块重新启用管理，使其处于启用状态 （）。

图 *17:* 启用管理连接

将管理器访问接口从管理更改为数据

你可以从专门的管理界面，或从数据界面管理 威胁防御。如果要在添加设备转至 管理中心 后更改管理器访问接口，请按照以下步骤从管理接口迁移到数据接口。要迁移另一个方向，请参阅 将管理器访问接口从数据更改为管理，第 66 页。

启动从管理到数据的管理器访问迁移会导致 管理中心 在部署到 威胁防御 时应用阻止。要删除数据块，请在数据接口上启用管理器访问。

请参阅以下步骤以启用数据接口上的管理器访问，并配置其他所需的设置。

过程

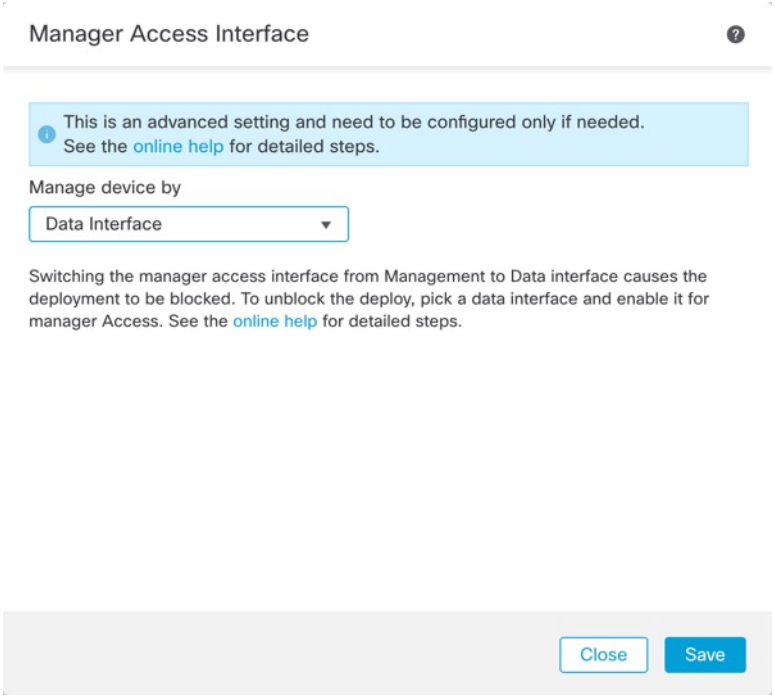
步骤 1 初始化接口迁移。

a) 在 **设备 (Devices)** > **设备管理 (Device Management)** 页面，然后点击设备的 **编辑**（）。

b) 转到**设备 (Device)** > **管理 (Management)** 部分，然后点击**管理器访问接口 (Manager Access Interface)** 的链接。

管理器访问接口 (Manager Access Interface) 字段会显示当前管理接口。当您点击链接时，在 **管理设备依据** 下拉列表中选择新接口类型 **数据接口**。

图 *18:* 管理器访问接口



c) 点击**保存 (Save)**。

您现在必须完成此程序中的其余步骤，才能在数据接口上启用管理器访问。**管理 (Management)** 区域现在会显示**管理器访问接口：数据接口 (Manager Access Interface: Data Interface)** 以及**管理器访问详细信息：配置 (Manager Access Details: Configuration)**。

图 *19:* 管理器访问

如果点击**配置 (Configuration)**，将打开**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框。**管理器访问模式 (Manager Access Mode)** 将显示“等待部署” (Deploy pending) 状态。

步骤 2 在**设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** > **管理器访问 (Manager Access)** 页面上启用数据接口上的管理器访问。

请参阅配置路由模式接口，第 551 页。您可在一个数据接口上启用管理器访问。确保此接口使用名称和 IP 地址进行了充分配置，并且已启用。

步骤 3 （可选） 如果对接口使用DHCP，请在 **设备** > **设备管理** > **DHCP** > **DDNS** 页面上启用 Web 类型 DDNS 方法。

请参阅配置动态 DNS，第 590 页。如果 FTD 的 IP 地址发生变化，DDNS 可确保 管理中心 接通完全限定域名 (FQDN) 内的 威胁防御。

步骤 4 确保 威胁防御 可以通过数据接口路由到 管理中心；如果需要，在 **设备 (Devices)** > **设备管理 (Device Management)** > **路由 (Routing)** > **静态路由 (Routing)** 上添加静态路由。

请参阅添加静态路由，第 794 页。

步骤 5 （可选） 在平台设置策略中配置 DNS，并将其应用到位于 **设备** > **平台设置** > **DNS** 的此设备。

请参阅配置 DNS，第 617 页。如果使用 DDNS，则需要 DNS。您也可以将 DNS 用于安全策略中的 FQDN。

步骤 6 （可选） 在平台设置策略中为数据接口启用 SSH，并通过 **设备** > **平台设置** > **安全外壳** 将其应用于此设备。

请参阅配置安全外壳，第 631 页。默认情况下，数据接口上未启用 SSH，因此，如果要使用 SSH 管理 威胁防御，则需要明确允许它。

步骤 7 部署配置更改。

管理中心 将通过当前管理接口部署配置更改。部署后，数据接口现在可供使用，但与管理的原始管理连接仍处于活动状态。

步骤 8 在 威胁防御 CLI（最好从控制台端口），将管理接口设置为使用静态 IP 地址，并将网关设置为使用数据接口。

configure network {**ipv4** | **ipv6**} **manual** *ip_*地址网络掩码 **data-interfaces**

- *ip_address netmask*-虽然您不打算使用管理接口，但必须设置静态IP地址，例如专用地址，以便将网关设置为 **数据接口**（请参阅下一个项目符号）。您无法使用 DHCP，因为默认路由（必须是 **数据接口**）可能会被从 DHCP 服务器收到的路由覆盖。
- **data-interfaces** - 此设置将在背板上转发管理流量，因此可路由通过管理器访问数据接口。

我们建议您使用控制台端口而不是 SSH 连接，因为当您更改管理接口网络设置时，您的 SSH 会话将断开。

步骤 9 如有必要，请重新连接 威胁防御，使其能够到达数据接口上的 管理中心。

步骤 10 在 管理中心 中，禁用管理连接，在 **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** 部分中更新 威胁防御 的 **主机 (Host)** IP 地址 (IP address)，然后重新启用连接。

请参阅更新 管理中心中的主机名或 IP 地址，第 61 页。如果在将 威胁防御 添加到 管理中心 时使用了 威胁防御 主机名或仅使用了 NAT ID，则不需要更新该值；但是，您需要禁用并重新启用管理连接才能重新启动连接。

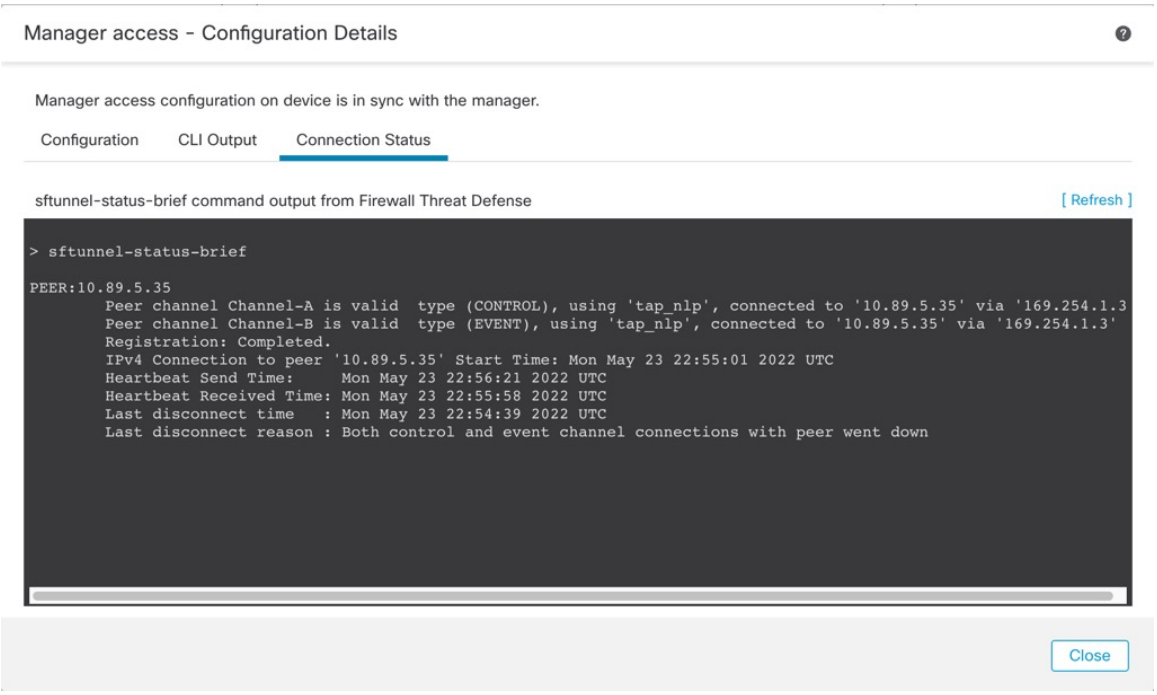
步骤 11 确保管理连接已重新建立。

在 管理中心 中，在 **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** > **管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** > **连接状态 (Connection Status)** 页面上检查管理连接状态。

在 威胁防御 CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

以下状态显示数据接口成功连接，显示内部“ tap_nlp”接口。

图 *20*: 连接状态



如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅排除数据接口上的管理连接故障，第 88 页。

将管理器访问接口从数据更改为管理

你可以从专门的管理界面，或从数据界面管理 威胁防御。如果要在添加设备到 管理中心 后更改管理器访问接口，请按照以下步骤从数据接口迁移到管理接口。要迁移另一个方向，请参阅将管理器访问接口从管理更改为数据，第 63 页。

启动从数据到管理的管理器访问迁移会导致 管理中心 在部署到 威胁防御 时应用阻止。您必须在数据接口上禁用管理器访问权限才能删除数据块。

请参阅以下步骤以禁用数据接口上的管理器访问，并配置其他所需的设置。

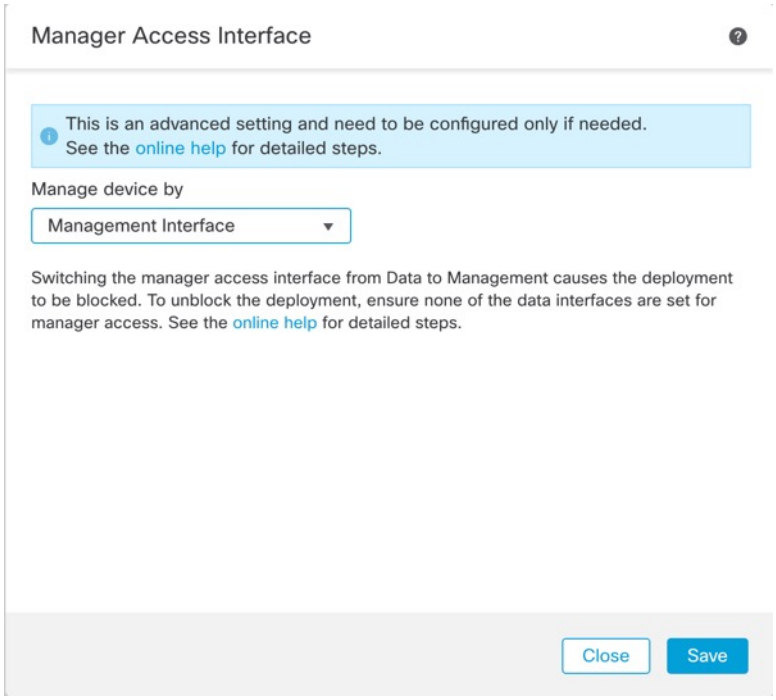
过程

步骤 1 初始化接口迁移。

a) 在 **设备 (Devices)** > **设备管理 (Device Management)** 页面，然后点击设备的 **编辑**（ ）。
b) 转到**设备 (Device)** > **管理 (Management)** 部分，然后点击**管理器访问接口 (Manager Access Interface)** 的链接。

管理器访问接口 (Manager Access Interface) 字段会将当前管理接口显示为数据。点击链接时，在 **管理设备依据** 下拉列表中选择新接口类型， **管理接口**。

图 *21:* 管理器访问接口



c) 点击**保存 (Save)**。

您现在必须完成此程序中的其余步骤，才能在管理接口上启用管理器访问。**管理 (Management)** 区域现在会显示**管理器访问接口：管理接口 (Manager Access Interface: Management Interface)** 以及**管理器访问详细信息：配置 (Manager Access Details: Configuration)**。

图 *22:* 管理器访问

如果点击**配置 (Configuration)**，将打开**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框。**管理器访问模式 (Manager Access Mode)** 将显示“等待部署”(Deploy pending) 状态。

步骤 2 在**设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** > **管理器访问 (Manager Access)** 页面上禁用数据接口上的管理器访问。

请参阅配置路由模式接口，第 551 页。此步骤将删除部署时的阻止。

步骤 3 如果尚未执行此操作，请在“平台设置”策略中为数据接口配置 DNS 设置，然后在 **设备** > **平台设置** > **DNS**上将其应用至设备。

请参阅配置 DNS，第 617 页。在数据接口上禁用管理器访问的 管理中心 部署将删除任何本地 DNS 配置。如果该 DNS 服务器用于任何安全策略，例如访问规则中的 FQDN，则必须使用 管理中心 重新应用 DNS 配置。

步骤 4 部署配置更改。

将 管理中心 通过当前数据接口部署配置更改。

步骤 5 如有必要，请重新连接 威胁防御，以便它可以到达管理接口上的 管理中心。

步骤 6 在 威胁防御 CLI 中，使用静态 IP 地址或 DHCP 配置管理接口 IP 地址和网关。

当您最初配置用于管理器访问的数据接口时，管理网关设置为 data-interfaces，它通过背板转发管理流量，以便可以通过管理器访问数据接口路由。您现在需要为管理网络上的网关设置 IP 地址。

静态 IP 地址：

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask gateway_ip*

DHCP:

configure network {**ipv4** | **ipv6**} **dhcp**

步骤 7 在 管理中心 中，禁用管理连接，在**设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** 部分中更新 威胁防御 的**主机 (Host)**IP 地址 (IP address)，然后重新启用连接。

请参阅更新 管理中心中的主机名或 IP 地址，第 61 页。如果在将 威胁防御 添加到 管理中心 时使用了 威胁防御 主机名或仅使用了 NAT ID，则不需要更新该值；但是，您需要禁用并重新启用管理连接才能重新启动连接。

步骤 8 确保管理连接已重新建立。

在 管理中心 中，检查**设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** > **状态 (Status)**字段上的管理连接状态或查看 管理中心 中的通知。

在 威胁防御 CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅排除数据接口上的管理连接故障，第 88 页。

将管理器访问接口从管理更改为高可用性对中的数据

你可以从专门的管理界面，或从数据界面管理 FTD。如果要在添加设备转至 CDO后更改 思科防御协调器 访问接口，请按照以下步骤从管理接口迁移到数据接口。要迁移另一个方向，请参阅在高可用性对中将管理器访问接口从“数据”更改为“管理”，第 72 页。

启动从管理到数据的 CDO 访问迁移会导致 CDO 在部署到FTD时应用阻止。要删除数据块，请在数据接口上启用 CDO 访问。

注释 除非另有说明，否则仅限在主用设备上执行本节中提到的所有步骤。一旦配置更改被部署，备用设备会同步主用设备的配置和其他状态信息。

请参阅以下步骤以在数据接口上启用 CDO 访问，并配置其他所需设置。

开始之前

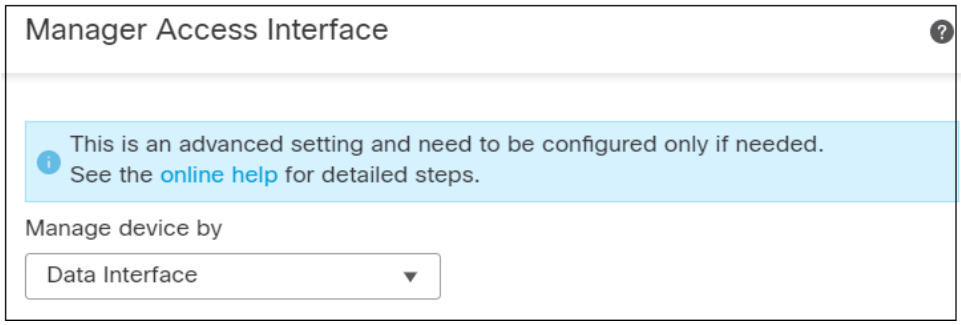
型号支持-威胁防御

过程

步骤 1 初始化接口迁移。

a) 在导航栏中，点击**清单 (Inventory)**。
b) 点击 **FTD** 选项卡。
c) 选择主用设备，然后在右侧的**管理 (Management)** 窗格中，点击**设备摘要 (Device Summary)**。
d) 在**管理 (Management)** 区域下，点击**管理器访问接口 (Manager Access Interface)** 的链接。

管理器访问接口 (Manager Access Interface) 字段会显示当前管理接口。当您点击链接时，在 **管理设备依据** 下拉列表中选择新接口类型 **数据接口**。

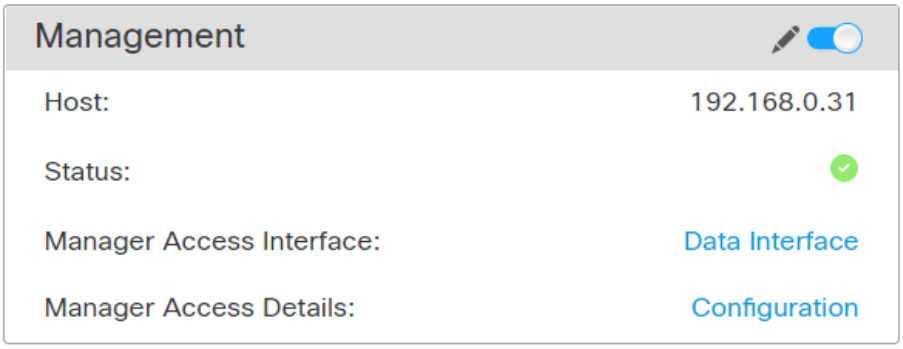


注释 链接对备用设备不可用，因为可以在主用设备上更改访问接口。

e) 点击**保存 (Save)**。

您现在必须完成此程序中的其余步骤，才能在数据接口上启用 CDO 访问。**管理 (Management)** 区域现在会显示**管理器访问接口：数据接口 (Manager Access Interface: Data Interface)** 和**管理器访问详细信息：配置 (Manager Access Details: Configuration)**。

图 *23:* 管理器访问



如果点击**配置 (Configuration)**，系统将打开**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框。**管理器访问模式 (Manager Access Mode)** 显示“等待部署”(Deploy pending) 状态。

步骤 2 在 **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** > **管理器访问 (Manager Access)** 页面上启用对数据接口的 CDO 访问。

请参阅配置路由模式接口。您可在一个数据接口上启用 CDO 访问。确保此接口使用名称和 IP 地址进行了充分配置，并且已启用。

步骤 3 确保 FTD 可以通过数据接口路由到 CDO；如果需要，在 **设备** > **设备管理** > **路由** > **静态路由**上添加静态路由。

请参阅添加静态路由，第 794 页。

步骤 4 （可选） 在平台设置策略中配置 DNS，并将其应用到位于 **设备** > **平台设置** > **DNS**的此设备。

配置 DNS，第 617 页。如果使用 DDNS，则需要 DNS。您也可以将 DNS 用于安全策略中的 FQDN。

步骤 5 （可选） 在平台设置策略中为数据接口启用 SSH，并通过 **设备** > **平台设置** > **安全外壳**将其应用于此设备。

请参阅配置安全外壳，第 631 页。默认情况下，数据接口上未启用 SSH，因此，如果要使用 SSH 管理 FTD，则需要明确允许它。

步骤 6 部署配置更改。

CDO 将通过当前管理接口部署配置更改。部署后，数据接口现在可供使用，但与管理的原始管理连接仍处于活动状态。

步骤 7 在 FTD CLI（最好从控制台端口），将管理接口设置为使用静态 IP 地址，并将网关设置为使用数据接口。

configure network {**ipv4** | **ipv6**} **manual** *ip_*地址网络掩码 **data-interfaces**

- *ip_address netmask*-虽然您不打算使用管理接口，但必须设置静态IP地址，例如专用地址，以便将网关设置为 **数据接口**（请参阅下一个项目符号）。
- **data-interfaces**-此设置将在背板上转发管理流量，因此可路由通过 CDO 访问数据接口。

我们建议您使用控制台端口而不是SSH连接，因为当您更改管理接口网络设置时，您的SSH会话将断开。

注释　　在备用设备上重复此步骤。

步骤 8 当部署完成大约 90% 时，新的管理界面就会生效。在此阶段，您必须为 FTD 重新布线，以便 CDO 到达数据接口上的 FTD 并成功完成部署。

重新布线后，如果在与新接口重新建立管理连接之前发生超时，则部署可能会失败。在这种情况下，您必须在重新布线后重新启动部署，然后才能成功部署。

注释　　在备用设备上重复此步骤。

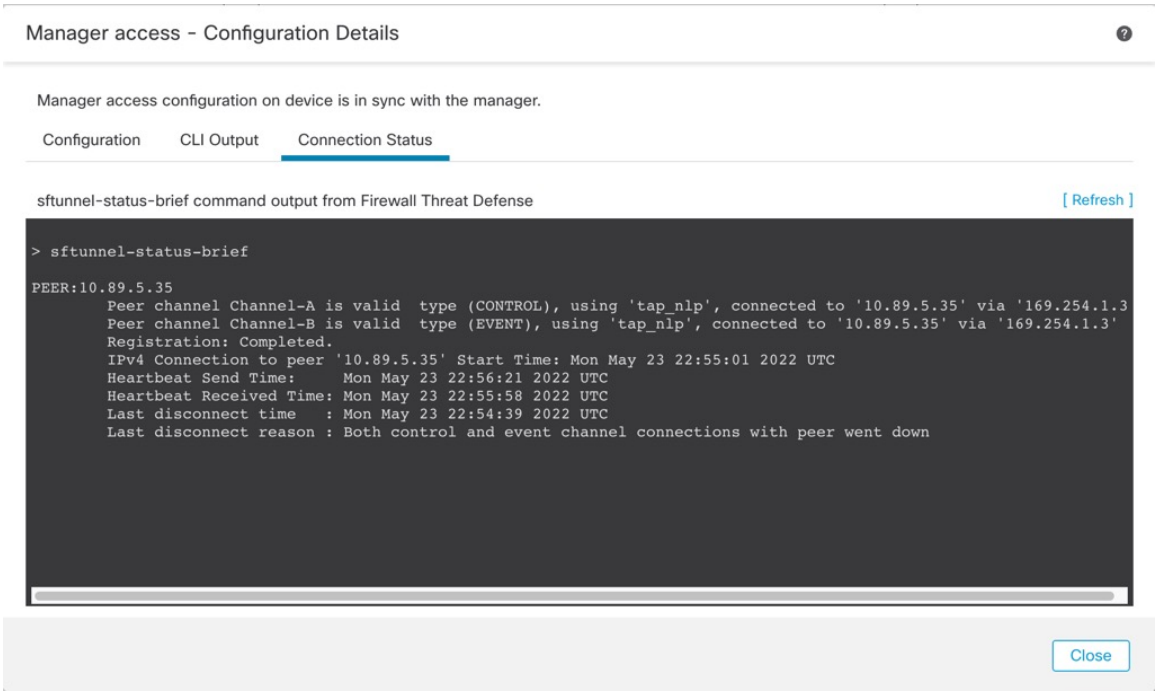
步骤 9 确保管理连接已重新建立。

在 CDO 中，在**设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** > **管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** > **连接状态 (Connection Status)** 页面上检查管理连接状态。

在 FTD CLI 上，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

以下状态显示数据接口成功连接，显示内部“ tap_nlp”接口。

图 *24:* 连接状态



如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅排除数据接口上的管理连接故障，第 88 页。

在高可用性对中将管理器访问接口从“数据”更改为“管理”

你可以从专门的管理界面，或从数据界面管理 FTD。如果要在添加设备到 CDO后更改 思科防御协调器 访问接口，请按照以下步骤从数据接口迁移到管理接口。要迁移另一个方向，请参阅将管理器访问接口从管理更改为高可用性对中的数据，第 68 页。

启动从数据到管理的 CDO 访问迁移会导致 CDO 在部署到 FTD 时应用阻止。您必须在数据接口上禁用 CDO 访问权限才能删除数据块。

注释 除非另有说明，否则仅限在主用设备上执行本节中提到的所有步骤。一旦配置更改被部署，备用设备会同步主用设备的配置和其他状态信息。

请参阅以下步骤以禁用数据接口上的 CDO 访问，并配置其他所需的设置。

过程

步骤 1 初始化接口迁移。

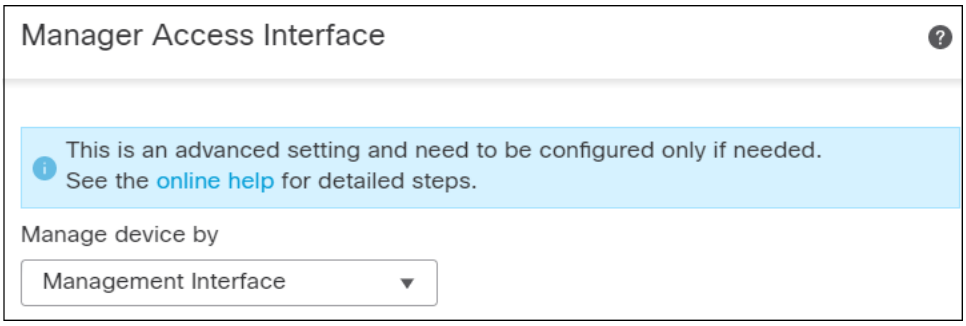
a) 在导航栏中，点击**清单 (Inventory)**。

b) 点击 **FTD** 选项卡。

c) 选择主用设备，然后在右侧的**管理 (Management)** 窗格中，点击**设备摘要 (Device Summary)**。

d) 在**管理 (Management)** 区域下，点击**管理器访问接口 (Manager Access Interface)** 的链接。

管理器访问接口 (Manager Access Interface) 字段会将当前管理接口显示为数据。点击链接时，在 **管理设备依据** 下拉列表中选择新接口类型， **管理接口**。

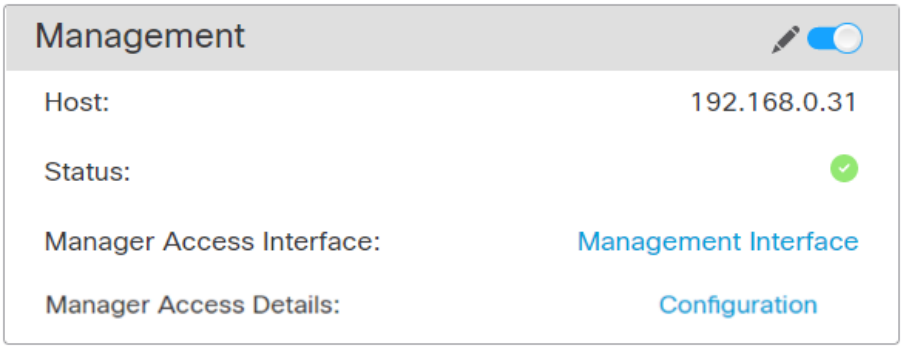


注释 链接对备用设备不可用，因为可以在主用设备上更改访问接口。

e) 点击**保存 (Save)**。

您现在必须完成此程序中的其余步骤，才能在数据接口上启用 CDO 访问。**管理 (Management)** 区域现在会显示**管理器访问接口：管理接口 (Manager Access Interface: Management Interface)** 和**管理器访问详细信息：配置 (Manager Access Details: Configuration)**。

图 *25:* 管理器访问



如果点击**配置 (Configuration)**，系统将打开**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框。**管理器访问模式 (Manager Access Mode)** 显示“等待部署” (Deploy pending) 状态。

步骤 2 在 **设备** > **设备管理** > **接口** > **编辑物理接口** > **FMC 访问** 页面上禁用数据接口上的 CDO 访问。

请参阅配置路由模式接口。此步骤将删除部署时的阻止。

步骤 3 如果尚未执行此操作，请在“平台设置”策略中为数据接口配置 DNS 设置，然后在 **设备** > **平台设置** > **DNS** 上将其应用至设备。

请参阅配置 DNS，第 617 页。在数据接口上禁用 CDO 访问的 CDO 部署将删除任何本地 DNS 配置。如果该 DNS 服务器用于任何安全策略，例如访问规则中的 FQDN，则必须使用 CDO重新应用 DNS 配置。

步骤 4 部署配置更改。

将 CDO 通过当前数据接口部署配置更改。

步骤 5 当部署完成大约 90% 时，新的管理界面就会生效。在此阶段，您必须为 FTD 重新布线，以便 CDO 到达管理接口上的 FTD 并成功完成部署。

重新布线后，如果在与新接口重新建立管理连接之前发生超时，则部署可能会失败。在这种情况下，您必须在重新布线后重新启动部署，然后才能成功部署。

注释　　在备用设备上重复此步骤。

步骤 6 在 FTD CLI 中，使用静态 IP 地址或 DHCP 配置管理接口 IP 地址和网关。

当您最初配置用于 CDO 访问的数据接口时，管理网关设置为 data-interfaces，它通过背板转发管理流量，以便可以通过 CDO 访问数据接口路由。您现在需要为管理网络上的网关设置 IP 地址。

静态 IP 地址：

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask gateway_ip*

DHCP:

configure network{**ipv4** | **ipv6**} **dhcp**

注释　　在备用设备上重复此步骤。

步骤 7 确保管理连接已重新建立。

在CDO中，检查**设备** > **设备管理** > **设备** > **管理** > **状态**字段上的管理连接状态或查看 CDO中的通知。

在 FTD CLI 上，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅排除数据接口上的管理连接故障，第 88 页。

查看数据接口管理的管理器访问详细信息

型号支持-威胁防御

当使用数据接口进行 管理中心 管理而不是使用专用管理接口时，必须注意在 管理中心 中更改设备的接口和网络设置，以免中断连接。您也可以在设备上本地更改数据接口设置，这就要求您在 管理中心 中手动协调这些更改。**设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **设备管理 (Management)** > **管理器访问 + 配置详细信息 (Manager Access - Configuration Details)** 对话框可帮助您解决 管理中心 和 威胁防御 本地配置之间的任何差异。

通常，在将 威胁防御 添加到 管理中心 之前，您可以作为初始 威胁防御 设置的一部分来配置管理器访问数据接口。当您将 威胁防御 添加到 管理中心时， 管理中心 会发现并维护接口配置，包括以下设置：接口名称和 IP 地址、网关静态路由、DNS 服务器和 DDNS 服务器。对于 DNS 服务器，如果在注册期间发现了它，则在本地维护配置，但不会将其添加到 管理中心 中的平台设置策略。

将 威胁防御 添加到 管理中心 后，如果使用 **configure network management-data-interface** 命令在 威胁防御 上本地更改数据接口设置，则 管理中心 会检测到配置更改，并阻止部署到 威胁防御。管理中心 会使用以下方法之一来检测配置更改：

- 部署到 威胁防御。在部署 管理中心 之前，它将检测配置差异并停止部署。
- **接口 (Interfaces)** 页面中的**同步 (Sync)** 按钮。
- **管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框上的**刷新 (Refresh)** 按钮

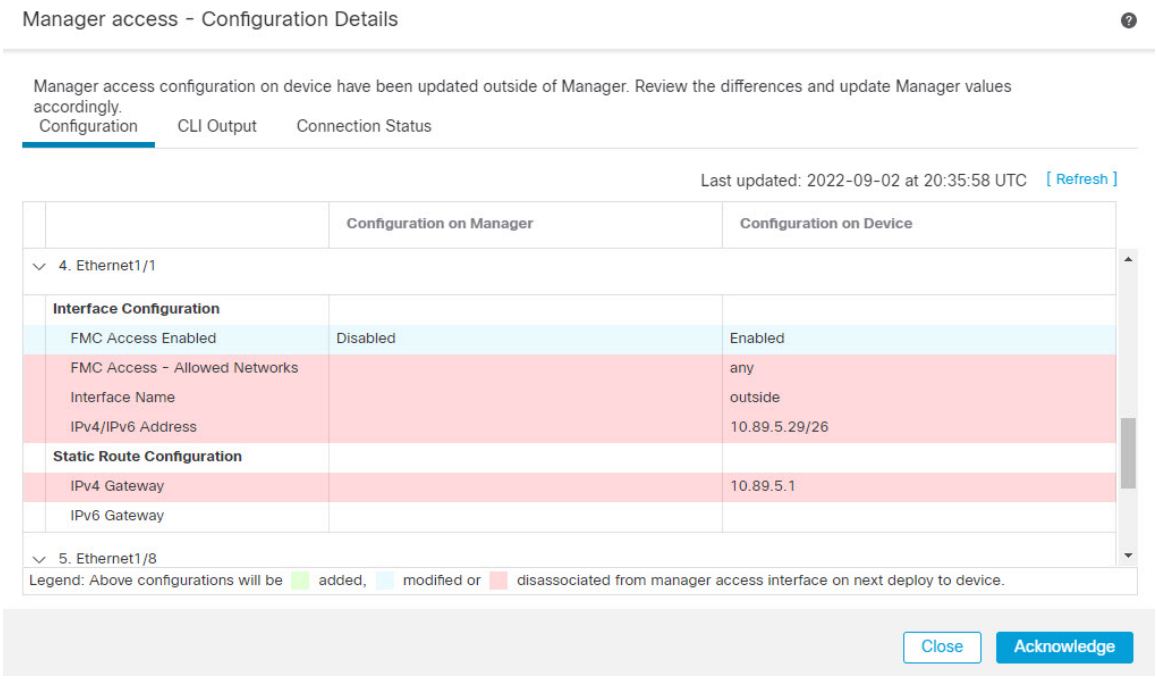
要删除阻止，您必须转到**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框，然后点击**确认 (Acknowledge)**. 下次部署时，管理中心 配置将覆盖 威胁防御 上任何剩余的冲突设置。在您重新部署之前，您有责任在 管理中心 中手动修复配置。

请参阅此对话框中的以下页面。

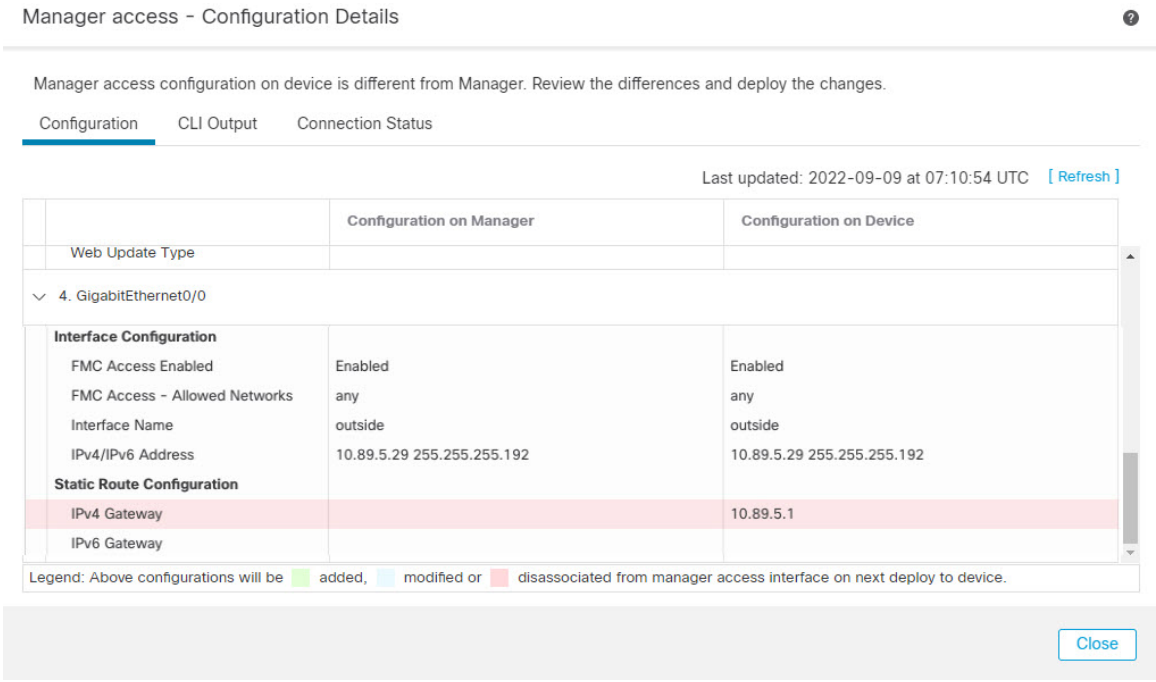
配置

查看 管理中心 和 威胁防御 上的管理器访问数据接口的配置对比。

以下示例显示了在 威胁防御 上输入 **configure network management-data-interface** 命令的位置的 威胁防御 配置详细信息。以粉红色突出显示的内容显示了如果您**确认**差异但不匹配 管理中心 中的配置，则 威胁防御 配置将被删除。以蓝色突出显示的内容显示了将在 威胁防御 上修改的配置。以绿色突出显示的内容显示了将被添加到 威胁防御 的配置。



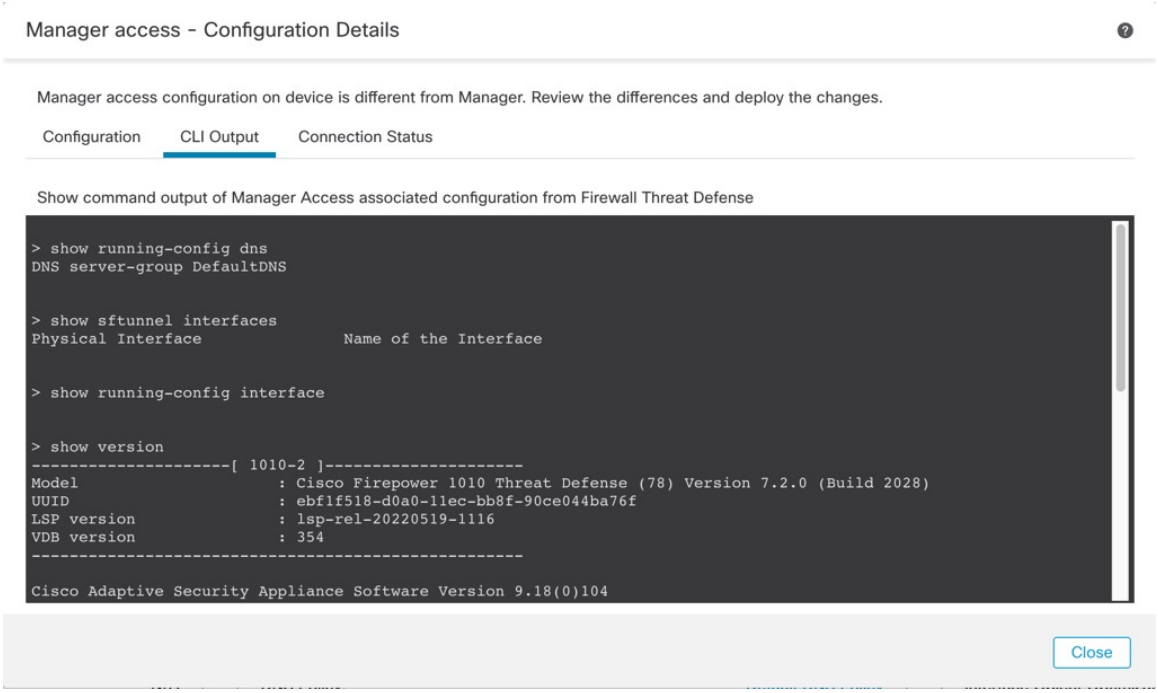
以下示例显示在 管理中心中配置接口后的此页面；接口设置匹配，并且已删除粉红色突出显示。



CLI 输出

查看管理器访问数据接口的 CLI 配置，如果您熟悉底层 CLI，这将非常有用。

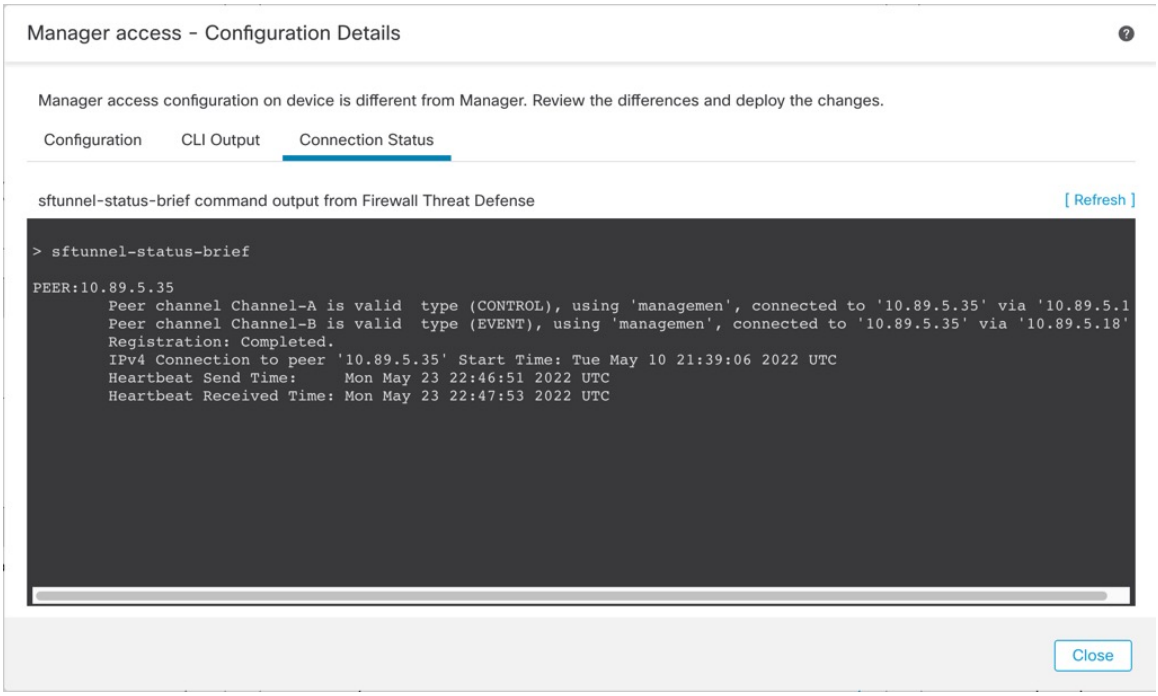
图 *26: CLI* 输出



连接状态

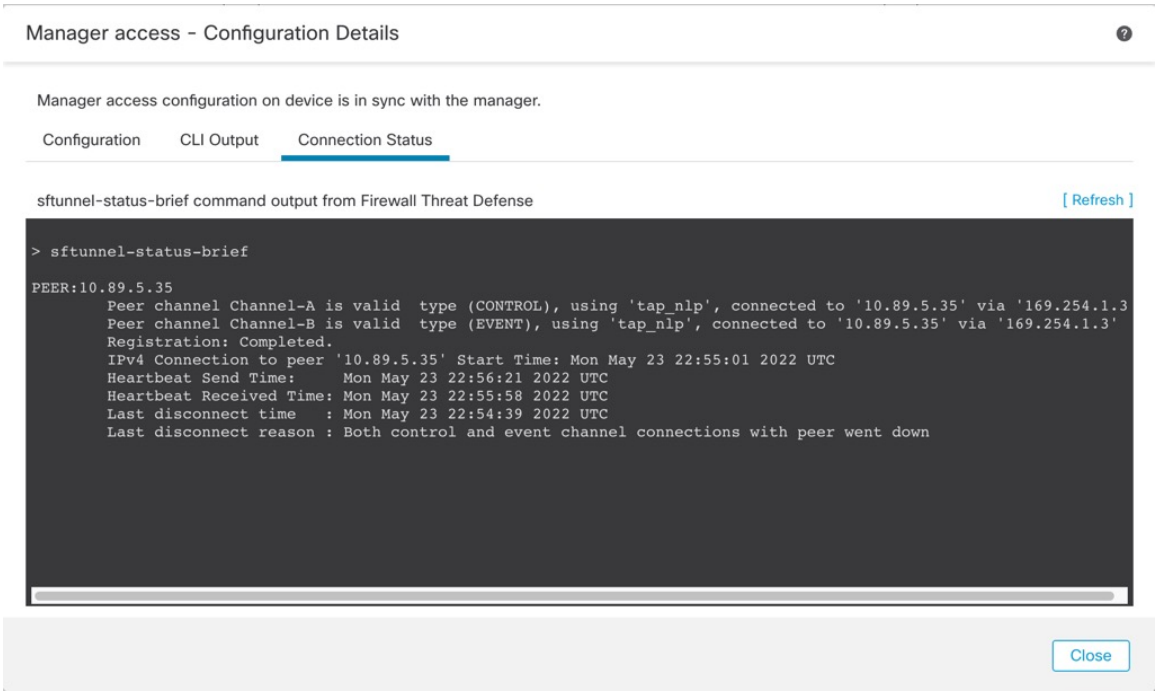
查看管理连接状态。以下示例显示了管理连接仍在使用管理“management0”接口。

图 *27:* 连接状态



以下状态显示数据接口成功连接，显示内部“ tap_nlp”接口。

图 *28:* 连接状态



请参阅以下有关关闭连接的输出示例；没有显示“连接至“信息，也没有显示心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

请参阅以下关于已建立连接的输出示例，其中显示了对等信道和心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
 '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

在 CLI 中修改 威胁防御 管理接口

使用 CLI 修改受管设备上的管理接口设置。这些设置中有许多是您在执行初始设置时设置的；此过程允许您更改这些设置，并设置其他设置，例如，启用事件接口（如果您的型号支持）或添加静态路由。

注释 本主题适用于专用管理接口。您也可以为管理配置数据接口。如果要更改该接口的网络设置，则应在 管理中心 中而不是在CLI中执行此操作。如果您需要对中断的管理连接进行故障排除，并且需要直接在 威胁防御 上进行更改，请参阅 修改 CLI 中用于管理的 威胁防御 数据接口，第 83 页。

有关 威胁防御 CLI 的信息，请参阅Cisco Secure Firewall Threat Defense 命令参考。

注释 使用 SSH 时，在对管理接口进行更改时要小心；如果由于配置错误而无法重新连接，您将需要访问设备控制台端口。

注释 如果更改设备管理 IP 地址，请参阅以下有关 管理中心 连接的任务，具体取决于您在初始设备设置期间使用 **configure manager add** command：

- **IP 地址—无操作**。如果您使用可访问的IP地址识别 管理中心，则几分钟后会自动重新建立管理连接。我们还建议您更改 管理中心 中显示的设备 IP 地址，以保持信息同步；请参阅 更新 管理中心中的主机名或 IP 地址，第 61 页。此操作有助于更快地重新建立连接。**注意**：如果您指定了无法访问的 管理中心 IP 地址，请参阅下面的 NAT ID 程序。
- **仅限 NAT ID-手动重新建立连接**。如果仅使用 NAT ID 识别 管理中心，则无法自动重新建立连接。在这种情况下，请根据 更新 管理中心中的主机名或 IP 地址，第 61 页 更改 管理中心 中的设备管理 IP 地址。

注释 在高可用性 管理中心 配置中，当您从设备 CLI 或 管理中心 修改管理 IP 地址时，即使在 HA 同步后，辅助 管理中心 也不会反映更改。要确保辅助 管理中心 也更新，请在两个 管理中心之间切换角色，使辅助 管理中心 成为主用设备。在当前活动的 管理中心的设备管理页面上修改已注册设备的管理 IP 地址。

开始之前

- 您可以使用 **configure user add** 命令创建可登录到 CLI 的用户账户；请参阅 在 CLI 中添加内部用户，第 111 页。您还可以根据为 SSH 配置外部身份验证，第 619 页配置 AAA 用户。

过程

步骤 1 通过控制台端口或使用 SSH 连接至设备 CLI。

步骤 2 使用“管理员”(Admin) 用户名和密码登录。

步骤 3 （仅 Firepower 4100/9300））启用第二个管理接口作为仅事件的接口。

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

您始终需要用于管理通信的管理接口。如果您的设备有第二个管理接口，则可以为仅事件流量启用该接口。

Cisco Secure Firewall Management Center仅事件接口不能接受管理通道流量，因此您应在设备事件接口上禁用管理通道。

您可以选择使用 **configure network management-interface disable-events-channel** 命令禁用主管理接口的事件。不管是哪种情况，设备都会尝试通过事件专属接口发送事件，如果该接口关闭，那么即使您禁用了事件通道，设备也会通过管理接口发送事件。

无法同时禁用接口上的事件通道和管理通道。

示例：

```
> configure network management-interface enable management1
Configuration updated successfully

> configure network management-interface disable-management-channel management1
Configuration updated successfully

>
```

步骤 4 配置管理接口和/或事件接口的网络设置：

如果未指定 *management_interface* 参数，则更改默认管理接口的网络设置。配置事件接口时，请确保指定 *management_interface* 参数。事件接口可以与管理接口位于不同的网络中，也可以位于同一网络中。如果连接到您正在配置的接口，您将断开连接。您可以重新连接到新 IP 地址。

a) 配置 IPv4 地址：

- 手动配置：

  configure network ipv4 manual *ip_address netmask gateway_ip* [*management_interface*]

  请注意，此命令中的 门户*_ip* 用于为设备创建默认路由。如果配置仅事件接口，则必须输入 门户*_ip* 作为命令的一部分；但是，此条目只是将默认路由配置为您指定的值，并且不会为事件接口创建单独的静态路由。如果您在与管理接口不同的网络上使用仅事件接口，我们建议您设置 门户*_ip* 以用于管理接口，然后使用 **configure network static-routes** 命令单独为仅事件接口创建静态路由。

  示例：

  ```
  > configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
  Setting IPv4 network configuration.
  ```

```
Network settings changed.

>
```

- DHCP（只有默认的管理接口上才支持）：

  configure network ipv4 dhcp

b) 配置 IPv6 地址：

- 无状态自动配置：

  configure network ipv6 router [*management_interface*]

  示例：

```
> configure network ipv6 router management0
Setting IPv6 network configuration.
Network settings changed.

>
```

- 手动配置：

  configure network ipv6 manual *ip6_address ip6_prefix_length* [*ip6_gateway_ip*] [*management_interface*]

  请注意，此命令中的 *ipv6_gateway_ip* 用于为设备创建默认路由。如果配置仅事件接口，则必须输入 *ipv6_gateway_ip* 作为命令的一部分；但是，此条目只是将默认路由配置为您指定的值，并且不会为事件接口创建单独的静态路由。如果您在与管理接口不同的网络上使用仅事件接口，我们建议您将 *ipv6_gateway_ip* 设置为与管理接口配合使用，然后使用 **configure network static-routes** 命令单独为仅事件接口创建静态路由。

  示例：

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
Setting IPv6 network configuration.
Network settings changed.

>
```

- DHCPv6（只有默认的管理接口上才支持）：

  configure network ipv6 dhcp

步骤 5 对于IPv6，启用或禁用ICMPv6回应应答和目的地不可达消息。默认情况下，系统会启用这些消息。

configure network ipv6 destination-unreachable {**enable** | **disable**}

configure network ipv6 echo-reply {**enable** | **disable**}

您可能希望禁用这些数据包以防止潜在的拒绝服务攻击。禁用回应应答数据包意味着无法使用 IPv6 ping 到设备管理接口，以进行测试。

示例：

```
> configure network ipv6 destination-unreachable disable
> configure network ipv6 echo-reply disable
```

步骤 6 在默认管理接口上启用 DHCP 服务器，以便向已连接的主机提供 IP 地址：

configure network ipv4 dhcp-server-enable *start_ip_address end_ip_address*

示例：

```
> configure network ipv4 dhcp-server-enable 10.10.10.200 10.10.10.254
DHCP Server Enabled

>
```

只有手动设置管理接口 IP 地址时，才能配置 DHCP 服务器。management center virtual上不支持此命令。要显示 DHCP 服务器的状态，请输入 **show network-dhcp-server**：

```
> show network-dhcp-server
DHCP Server Enabled
10.10.10.200-10.10.10.254
```

步骤 7 如果 管理中心位于远程网络上，则将为仅事件接口添加静态路由；否则，所有流量都将通过管理接口与默认路由匹配。

configure network static-routes {**ipv4** | **ipv6**} **add** *management_interface destination_ip netmask_or_prefix gateway_ip*

对于 默认 路由，请勿使用此命令；当您使用 **configure network ipv4** 或 **ipv6** 命令时，只能更改默认路由网关 IP 地址（请参阅步骤 4）。

示例：

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully

> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully

>
```

要显示静态路由，请输入 **show network-static-routes**（不显示默认路由）：

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                : management1
Destination              : 192.168.6.0
Gateway                  : 10.10.10.1
Netmask                  : 255.255.255.0
[…]
```

步骤 8 设置主机名：

configure network hostname *name*

示例：

```
> configure network hostname farscape1.cisco.com
```

在重新启动之后，系统日志消息不会反映新的主机名。

步骤 9 选择搜索域：

configure network dns searchdomains *domain_list*

示例：

```
> configure network dns searchdomains example.com,cisco.com
```

为设备设置搜索域，用逗号隔开。如果没有在命令中指定完全限定域名，例如 **ping system**，则这些域将添加到主机名中。这些域仅用于管理接口，或通过管理接口的命令。

步骤 10 设置多达 3 个 DNS 服务器，用逗号隔开：

configure network dns servers *dns_ip_list*

示例：

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

步骤 11 设置与 管理中心通信的远程管理端口：

configure network management-interface tcpport *number*

示例：

```
> configure network management-interface tcpport 8555
```

管理中心和受管设备使用双向、SSL 加密的通信通道（默认情况下在端口 8305 上）进行通信。

注释 思科强烈建议保留远程管理端口的默认设置，但如果管理端口与网络中的其他通信冲突，可以选择其他端口。如果更改管理端口，则必须在部署中需要相互通信的所有设备上做出该更改。

步骤 12 （仅限 威胁防御）设置管理或事件接口 MTU。默认 MTU 为 1500 字节。

configure network mtu [字节] [*interface_id*]

- 字节-设置 MTU（以字节为单位）。对于管理接口，如果启用 IPv4，则值可以介于 64 和 1500 之间；如果启用 IPv6，则值可以介于 1280 和 1500 之间。对于事件接口，如果启用 IPv4，该值可以介于 64 和 9000 之间；如果启用 IPv6，该值可以介于 1280 和 9000 之间。如果同时启用 IPv4 和 IPv6，则最小值为 1280。如果不输入 字节，系统会提示您输入值。

- *interface_id*-指定要设置 MTU 的接口 ID。使用 **show network** 命令查看可用的接口 ID，例如 management0、management1、br1 和 eth0，具体取决于平台。如果未指定接口，则使用管理接口。

示例：

```
> configure network mtu 8192 management1
MTU set successfully to 1500 from 8192 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
>
```

步骤 13 配置 HTTP 代理。该设备配置为直接连接到互联网上的端口 TCP/443 (HTTPS) 和 TCP/80 (HTTP)。您可以通过 HTTP 摘要对代理服务器进行身份验证。发出命令后，系统将提示您 HTTP 代理地址和端口，是否需要进行代理身份验证，如果需要，还会提示代理用户名、代理密码和代理密码确认。

注释　　对于 威胁防御 上的代理密码，只能使用 A-Z、a-z 和 0-9 字符。

configure network http-proxy

示例：

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

步骤 14 如果更改设备管理 IP 地址，请参阅以下有关 管理中心 连接的任务，具体取决于您在初始设备设置期间使用 **configure manager add** command：

- **IP 地址—无操作**。如果您使用可访问的IP地址识别 管理中心，则几分钟后会自动重新建立管理连接。我们还建议您更改 管理中心 中显示的设备 IP 地址，以保持信息同步；请参阅 更新 管理中心中的主机名或 IP 地址，第 61 页。此操作有助于更快地重新建立连接。**注意**：如果指定了无法访问的 管理中心 IP 地址，则必须使用 更新 管理中心中的主机名或 IP 地址，第 61 页 手动重新建立连接。
- **仅限 NAT ID-手动重新建立连接**。如果仅使用 NAT ID 识别 管理中心，则无法自动重新建立连接。在这种情况下，请根据 更新 管理中心中的主机名或 IP 地址，第 61 页 更改 管理中心 中的设备管理 IP 地址。

修改 CLI 中用于管理的 威胁防御 数据接口

如果 威胁防御 和 管理中心 之间的管理连接中断，并且您希望指定新的数据接口来替换旧接口，请使用 威胁防御 CLI 配置新接口。此程序假设您要在同一网络上用新接口替换旧接口。如果管理连接

处于活动状态，则应使用管理中心对现有数据接口进行任何更改。有关数据管理接口的初始设置，请参阅 使用 CLI 完成威胁防御初始配置 。

注释 本主题适用于为管理配置的数据接口，而不是专用的管理接口。如果要更改管理接口的网络设置，请参阅 在 CLI 中修改 威胁防御 管理接口 ， 第 78 页。

有关 威胁防御 CLI 的信息，请参阅Cisco Secure Firewall Threat Defense 命令参考。

开始之前

- 您可以使用 **configure user add** 命令。您还可以根据为 SSH 配置外部身份验证 ， 第 619 页配置 AAA 用户。

过程

步骤 1 如果要将数据管理接口更改为新接口，请将当前接口电缆移至新接口。

步骤 2 连接到设备 CLI。

使用这些命令时，应使用控制台端口。如果您正在执行初始设置，则可能会断开与管理接口的连接。如果由于管理连接中断而正在编辑配置，并且您具有专用管理接口的 SSH 访问权限，则可以使用该 SSH 连接。

步骤 3 使用“管理员”(Admin) 用户名和密码登录。

步骤 4 禁用接口，以便您重新配置其设置。

configure network management-data-interface disable

示例：

```
> configure network management-data-interface disable

 Configuration updated successfully..!!


Configuration disable was successful, please update the default route to point to a gateway
 on management interface using the command 'configure network'
```

步骤 5 配置用于管理器访问的新数据接口。

configure network management-data-interface

然后，系统会提示您为数据接口配置基本网络设置。

当您将数据管理接口更改为同一网络上的新接口时，请使用与上一个接口相同的设置（接口 ID 除外）。此外，对于 **是否希望在应用之前清除所有设备配置？(y/n) [n]:** 选项，选择 **y**。此选项将清除旧的数据管理接口配置，以便您可以成功地在新接口上重新使用IP地址和接口名称。

```
> configure network management-data-interface
Data interface to use for management: ethernet1/4
Specify a name for the interface [outside]: internet
```

```
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]: y

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

步骤 6 （可选） 限制在特定网络上通过数据接口访问 管理中心。

configure network management-data-interface client *ip_address netmask*

默认情况下，允许所有网络。

步骤 7 连接将自动重新建立，但在管理中心 中禁用和重新启用连接将有助于更快地重新建立连接。请参阅更新 管理中心中的主机名或 IP 地址 ， 第 61 页。

步骤 8 检查管理连接是否已重新建立。

sftunnel-status-brief

请参阅以下关于已建立连接的输出示例，其中显示了对等通道和心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
 '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

步骤 9 在 管理中心 中，选择**设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** > **管理器访问 - 配置详细信息 (Manager Access - Configuration Details)**，然后点击**刷新 (Refresh)**。

管理中心 检测接口和默认路由配置更改，并阻止部署到威胁防御。当您在设备上本地更改数据接口设置时，必须在 管理中心 中手动协调这些更改。您可以在**配置 (Configuration)** 选项卡上查看 管理中心 和 威胁防御 之间的差异。

步骤 10 选择 **设备** > **设备管理** > **接口**，然后做作一下更改。

a) 从旧数据管理接口中删除 IP 地址和名称，并禁用此接口的管理器访问。

b) 使用旧接口（在 CLI 中使用的接口）的配置配置新的数据管理接口，并为其启用管理器访问。

步骤 11 选择 **设备** > **设备管理** > **路由** > **静态路由** ，然后将默认路由从旧数据管理接口更改为新路由。

步骤 12 返回**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框，然后点击**确认 (Acknowledge)** 以删除部署块。

下次部署时，管理中心 配置将覆盖 威胁防御 上任何剩余的冲突设置。在您重新部署之前，您有责任在 管理中心 中手动修复配置。

您将看到“配置已清除”(Config was cleared) 和“管理器 访问已更改并确认 (Manager/FMC access changed and acknowledged)”的预期消息。

如果管理中心断开连接，则手动回滚配置

如果将威胁防御上的数据接口用于管理器访问，并从管理中心部署影响网络连接的配置更改，则可以将威胁防御上的配置回滚到上次部署的配置，以便恢复管理连接。然后，您可以调整管理中心中的配置设置，以便保持网络连接并重新部署。即使没有丢失连接，也可以使用回滚功能；它不仅限于此故障排除情况。

或者，如果在部署后失去连接，您可以启用配置的自动回滚；请参阅 编辑部署设置，第 103 页。

请参阅以下准则：

- 只有以前的部署可以在 威胁防御 上本地提供；您无法回滚到任何较早的部署。
- 支持回滚以实现高可用性，但不支持集群部署。
- 创建高可用性后，不支持立即回滚。
- 回滚只会影响您可以在管理中心中设置的配置。例如，回滚不会影响与专用管理接口相关的任何本地配置，您只能在 威胁防御 CLI 中进行配置。请注意，如果您在上次 管理中心 部署后使用 **configure network management-data-interface** 命令更改了数据接口设置，然后使用了回滚命令，则这些设置将不会保留；它们将回滚到上次部署的 管理中心 设置。
- UCAPL/CC 模式无法回滚。
- 无法回滚上一次部署期间更新的带外 SCEP 证书数据。
- 在回滚期间，连接将被丢弃，因为当前配置将被清除。

过程

步骤 1 在 威胁防御 CLI 中，回滚到之前的配置。

configure policy rollback

注释 对于高可用性对，仅允许在主用设备上使用此命令。

回滚后，威胁防御 会通知 管理中心 已成功完成回滚。在 管理中心 中，部署屏幕将显示一条横幅，说明配置已回滚。

注释 如果回滚失败且 管理中心 管理已恢复，请参阅https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html以了解常见的部署问题。在某些情况下，恢复管理中心管理访问权限后回滚可能会失败；在这种情况下，您可以解决 管理中心 配置问题，并从 管理中心 重新部署。

示例：

对于使用数据接口进行管理器访问的 威胁防御 ：

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
.....................
.....................
>
```

示例：

对于使用数据接口进行 管理中心 访问的高可用性对中的 威胁防御：

```
> configure policy rollback

Checking Eligibility ....
============= DEVICE DETAILS =============
Device Version: 7.2.0
Device Type: FTD
Device Mode: Offbox
Device in HA: true
Is HA disabled: false
HA state: active - standby ready
==========================================
Device is eligible for policy rollback
Do you want to continue [YES/NO]?

YES

Starting rollback...
    Preparing policy configuration on the device.           Status: success
    Applying updated policy configuration on the device.    Status: success
    Applying Lina File Configuration on the device.         Status: success
    Applying Lina Configuration on the device.              Status: success
    Commit Lina Configuration.                              Status: success
    Commit Lina File Configuration.                         Status: success
    Commit Lina File Configuration.                         Status: success
================================================================
POLICY ROLLBACK STATUS: SUCCESS
================================================================
>
```

步骤 2 检查管理连接是否已重新建立。

在 管理中心中，在 **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** > **管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** > **连接状态 (Connection Status)** 页面上检查管理连接状态。

在 威胁防御 CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅排除数据接口上的管理连接故障，第 88 页。

排除数据接口上的管理连接故障

当使用数据接口进行管理器访问而不是使用专用管理接口时，必须注意在 管理中心 中更改 威胁防御 的接口和网络设置，以免中断连接。如果在将 威胁防御 添加到 管理中心 后更改管理接口类型（从数据到管理，或从管理到数据），如果接口和网络设置未正确配置，则可能会丢失管理连接。

本主题可帮助您排除管理连接丢失的问题。

查看管理连接状态

在 管理中心 中，在 **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** > **管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** > **连接状态 (Connection Status)** 页面上检查管理连接状态。

在 威胁防御 CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。您还可以使用 **sftunnel-status** 查看更完整的信息。

请参阅以下有关关闭连接的输出示例；没有显示“连接至“信息，也没有显示心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

请参阅以下关于已建立连接的输出示例，其中显示了对等信道和心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

查看 威胁防御 网络信息

在 威胁防御 CLI 上，查看管理和管理器访问数据接口网络设置：

show network

```
> show network
===============[ System Information ]===============
Hostname                  : 5516X-4
DNS Servers               : 208.67.220.220,208.67.222.222
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
IPv6 Default route
  Gateway                 : data-interfaces

======================[ br1 ]=======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8D
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.99.10.4
Netmask                   : 255.255.255.0
Gateway                   : 10.99.10.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers               :
Interfaces                : GigabitEthernet1/1

===============[ GigabitEthernet1/1 ]===============
State                     : Enabled
Link                      : Up
Name                      : outside
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8F
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.89.5.29
Netmask                   : 255.255.255.192
Gateway                   : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled
```

检查向 管理中心注册 威胁防御

在 威胁防御 CLI 中，检查 管理中心 注册是否已完成。请注意，此命令不会显示管理连接的 当前 状态。

show managers

```
> show managers
Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
```

```
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

Ping the 管理中心

在 威胁防御 CLI 上，使用以下命令从数据接口对 管理中心 执行 ping 操作：

ping *fmc_ip*

在 威胁防御 CLI 上，使用以下命令从管理接口对 管理中心 执行 ping 操作，该接口应通过背板路由到数据接口：

ping system *fmc_ip*

捕获 威胁防御 内部接口上的数据包

在 威胁防御 CLI 上，捕获内部背板接口 (nlp_int_tap) 上的数据包，以查看是否发送了管理数据包：

capture 名称 **interface nlp_int_tap trace detail match ip any any**

show capture*name* **trace detail**

检查内部接口状态，统计信息和数据包计数

在 威胁防御 CLI 上，查看有关内部背板接口 nlp_int_tap 的信息：

show interace detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
```

```
 Interface config status is active
 Interface state is active
```

检查路由和 NAT

在 威胁防御 CLI 中，检查是否已添加默认路由 (S *)，以及管理接口 (nlp_int_tap) 是否存在内部 NAT 规则。

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface  service
 tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

检查其他设置

请参阅以下命令以检查是否存在所有其他设置。您还可以在 管理中心的 **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** > **管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** > **CLI 输出 (CLI Output)** 页面上看到许多这些命令。

show running-config sftunnel

```
> show running-config sftunnel
```

```
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

检查 DDNS 更新是否成功

在 威胁防御 CLI 中，检查 DDNS 更新是否成功：

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfuly updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

如果更新失败，请使用 **debug http** 和 **debug ssl** 命令。对于证书验证失败，请检查是否已在设备上安装根证书：

show crypto ca certificates *trustpoint_name*

要检查 DDNS 操作，请执行以下操作：

show ddns update interface *fmc_访问_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

检查 管理中心 日志文件

请参阅 https://cisco.com/go/fmc-reg-error。

对高可用性对中的数据接口上的管理连接进行故障排除

本主题可帮助您排除高可用性中数据接口上管理连接丢失的故障。

型号支持-威胁防御

主用对等体与 CDO 之间的管理连接可能会由于以下原因而中断：

- 主用设备上用于管理的数据接口存在连接问题。

  您应手动故障切换到备用设备，然后配置新的数据接口进行 CDO 访问。

- 互联网服务提供商已更改。

  您应使用 CLI 命令手动更新主用设备上的新网络详细信息，以便恢复与 CDO 的设备连接。

主用设备上的数据管理接口存在连接问题

1. 在 CDO 中，将主用设备手动切换到备用设备。请参阅在 威胁防御 高可用性对中切换主用对等体，第 476 页。

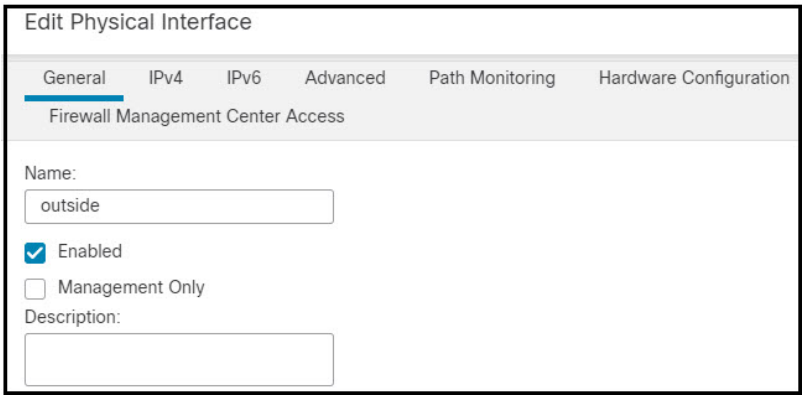
   或者，您可以在主用设备上运行 **no failover active** 命令。

   备用设备成为高可用性对中的新主用设备，并与 CDO 建立通信。

2. 在要编辑的设备高可用性对旁边，点击**编辑** ( )。
3. 选择**路由 (Routing) > 静态路由 (Static Route)**，然后删除为旧数据管理接口定义的静态路由。
4. 点击**接口 (Interfaces)** 选项卡，并进行以下更改。
   1. 从旧数据管理接口中删除 IP 地址和名称，并禁用此接口的 CDO 访问。

注释 在删除旧的数据管理接口信息之前，如果您要使用相同的信息，请记住详细信息。

   1. 点击要删除的接口旁边的**编辑** ( )。



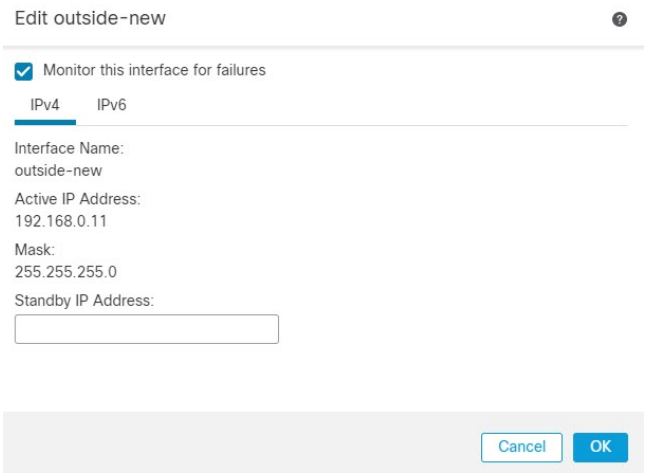
   2. 清除**名称 (Name)** 字段中的内容。
   3. 取消选中**启用 (Enabled)** 复选框。

4. 在 **IPv4** 或 **IPv6** 选项卡中，删除活动地址。
5. 在 **Firewall 管理中心访问 (Firewall Management Center Access)** 选项卡中，取消选中**在此接口上为 Firepower 管理中心启用管理 (Enable management on this interface for the Firepower Management Center)**。
6. 点击**确定 (OK)**。
7. 点击**是 (Yes)** 确认更改。

2. 使用旧接口（在 CLI 中使用的接口）的配置配置新的数据管理接口，并为其启用 CDO 访问。
   1. 点击要用于处理管理流量的数据接口旁边的**编辑** (✎)。
   2. 在**名称 (Name)** 字段中，指定接口名称。
   3. 选中**启用 (Enabled)** 复选框。
   4. 在 **IPv4** 或 **IPv6** 选项卡中，指定活动地址。
   5. 在 **Firewall 管理中心访问 (Firewall Management Center Access)** 选项卡中，选中**在此接口上为 Firepower 管理中心启用管理 (Enable management on this interface for the Firepower Management Center)**。
   6. 点击**确定 (OK)**。
   7. 点击**是 (Yes)** 确认更改。

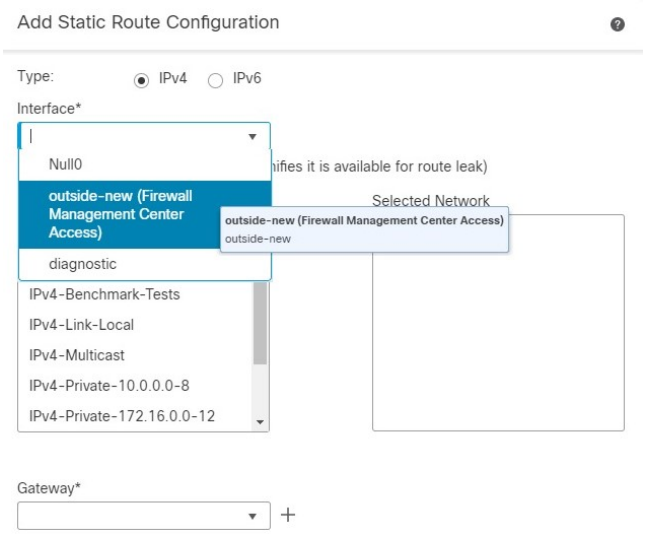
5. 点击**高可用性 (High Availability)** 选项卡，并进行以下更改。
   1. 在**监控的接口 (Monitored Interfaces)** 区域中，点击新数据管理接口旁边的**编辑** (✎)。

   主用 IP 地址 (Active IP Address) 显示主用设备的 IP 地址。
   2. 在 **IPv4** 选项卡上，输入**备用 IP 地址 (Standby IP Address)** 和**网关 (Gateway)** 地址。



3. 如果手动配置了 IPv6 地址，请在 IPv6 选项卡上，点击活动 IP 地址旁边的**编辑** ()，输入**备用 IP 地址 (Standby IP Address)**，然后点击**确定 (OK)**。
4. 点击**确定 (OK)**。

6. 点击右上角的**保存 (Save)** 以保存更改。
7. 选择**路由 (Routing) > 静态路由 (Static Route)**，然后添加为新数据管理接口定义的静态路由。新的数据接口显示在**接口 (Interface)** 列表中。



8. 点击右上角的**保存 (Save)** 以保存更改。
9. 部署配置更改。。
10. 当部署完成大约 90% 时，新的管理界面就会生效。在此阶段，您必须为 FTD 重新布线，以便 CDO 到达新接口上的 FTD 并成功完成部署。

注释 重新布线后，如果在与新接口重新建立管理连接之前发生超时，则部署可能会失败。在这种情况下，您必须在重新布线后重新启动部署，然后才能成功部署。

11. 确保管理连接已重新建立。

    在 管理中心中，在 **设备** > **设备管理** > **设备** > **管理** > **FMC 访问详细信息** > **连接状态** 页面上检查管理连接状态。

    此外，在 FTD CLI 上，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

互联网服务提供商已更改

如果更改了 ISP，即使高可用性运行状况正常，您也可能会丢失管理连接。使用 CLI 命令来配置管理接口的新网络详细信息。

注释 这些命令仅可用于主用设备上，无法用于备用设备上。

关于 威胁防御 CLI 的信息，请参阅 FTD 命令参考。

1. 连接到设备 CLI。

   使用这些命令时，应使用控制台端口。如果由于管理连接中断而正在编辑配置，并且您具有专用管理接口的 SSH 访问权限，则可以使用该 SSH 连接。

   请参阅登录 威胁防御 设备上的命令行界面 ， 第 22 页。

2. 使用“管理员”(Admin) 用户名和密码登录。

3. 根据要更新的网络值，请使用以下命令之一：

   - **configure network management-data-interface ipv4 manual** *ip_address ip_netmask* **interface** *interface_id*
   - **configure network management-data-interface ipv4** *gateway_ip* **interface** *interface_id*
   - **configure network management-data-interface ipv4 manual** *ip_address ipv4_netmask gateway_ip* **interface** *interface_id*

   示例：

```
Configure network management-data-interface ipv4 manual 10.10.6.7 255.255.255.0 interface
 gig0/0
Configuration updated successfully..!!
```

注释 高可用性对中的设备不支持 **configure network management-data-interface** 的所有其他 CLI 命令。

配置会被自动推送到备用设备。

4. **可选**：限制在特定网络上通过数据接口访问 CDO。

   configure network management-data-interface client *ip_address netmask*

   默认情况下，允许所有网络。

5. 检查管理连接是否已重新建立。

   sftunnel-status-brief

   请参阅以下关于已建立连接的输出示例，其中显示了对等通道和心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

6. 在 CDO 中，点击**清单 (Inventory)** > **FTD**。
7. 选择您的 威胁防御，然后在右侧的**管理 (Management)** 窗格中点击**设备摘要 (Device Summary)**。
8. 在**管理 (Management)** > **FMC 访问详细信息 (FMC Access Details)** 中，点击**刷新 (Refresh)**。

   CDO 检测接口和默认路由配置更改，并阻止部署到 FTD。当您在设备上本地更改数据接口设置时，必须在 CDO 中手动协调这些更改。您可以在**配置 (Configuration)** 选项卡上查看 CDO 和 威胁防御 之间的差异。

9. 返回到 **FMC 访问详细信息** 对话框，然后点击 **确认** 以删除部署块。

   下次部署时， CDO 配置将覆盖 FTD 上任何剩余的冲突设置。在您重新部署之前，您有责任在 CDO 中手动修复配置。

   您将看到“配置已清除”和“FMC 访问已更改并确认”的预期消息。

   在主用设备上进行的配置更改会被自动推送到备用设备。在 CDO 恢复与主用设备的连接后，CDO 会更新备用 IP 地址。

查看清单详细信息

设备 (Device) 页面上的**清单详细信息 (Inventory Details)** 部分会显示机箱详细信息，例如 CPU 和内存。

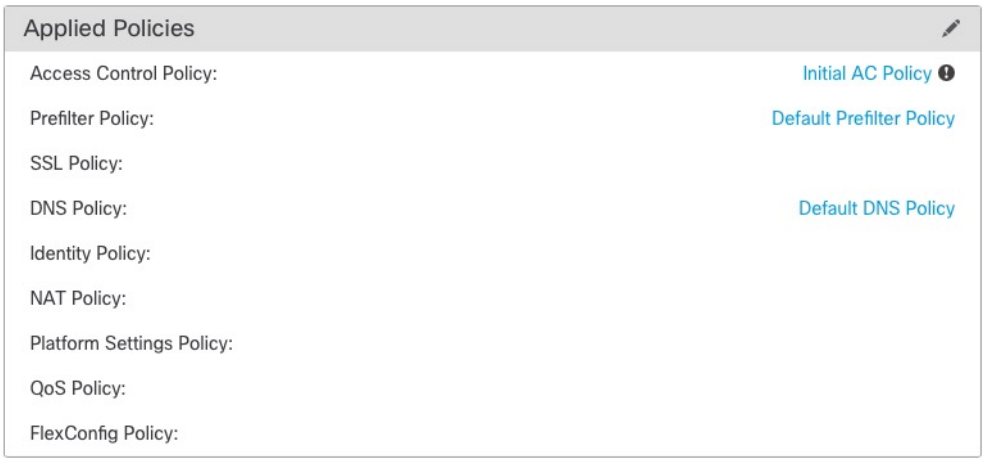
图 *29:* 设备清单详细信息

要更新信息，请点击 **刷新** （ ）。

编辑应用的策略

设备 (Device) 页面的**应用的策略 (Applied Policies)** 部分显示了应用于防火墙的以下策略：

图 *30:* 应用的策略



对于包含链接的策略，您可以点击链接以查看策略。

对于访问控制策略，请点击 **感叹号** （ ） 图标以查看**用于故障排除的访问策略信息 (Access Policy Information for Troubleshooting)** 对话框。该对话框显示了如何将访问规则扩展为访问控制条目 (ACE)。

图 *31:* 用于故障排除的访问策略信息

您可以从**设备管理 (Device Management)** 页面将策略分配给单个设备。

过程

步骤 1 选择**设备** > **设备管理**。

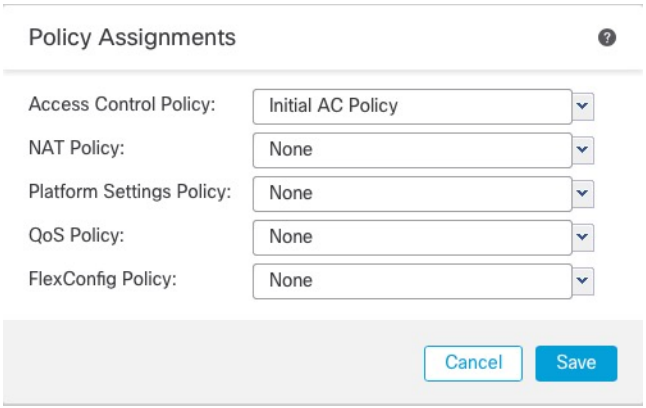
步骤 2 在要为其分配策略的设备旁边，点击 **编辑**（）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备**。

步骤 4 在**应用的策略 (Applied Policides)** 部分中，点击 **编辑**（）。

图 *32:* 策略分配



步骤 5 对于每种策略类型，请从下拉菜单选择一个策略。只有现有的策略会被列出。

步骤 6 点击**保存 (Save)**。

下一步做什么

- 部署配置更改。

编辑高级设置

设备 (Device) 页面的**高级设置 (Advanced Settings)** 部分会显示高级配置设置表，如下所述。您可以编辑任何这些设置。

表 9:“高级”(Advanced) 部分表字段

字段	说明 (Description)
应用绕行 (Application Bypass)	设备上“自动应用绕行”(Automatic Application Bypass) 的状态。
旁路阈值	“自动应用绕行”(Automatic Application Bypass) 阈值（以毫秒为单位）。
对象组搜索	设备上对象组搜索的状态。运行时，FTD 设备会根据访问规则中使用的任何网络或接口对象的内容，将访问控制规则扩展为多个访问控制列表条目。您可以通过启用对象组搜索来减少搜索访问规则所需的内存。启用对象组搜索后，系统不会扩展网络或接口对象，而是根据这些组定义在访问规则中搜索匹配项。对象组搜索不会影响访问规则的定义方式或它们在 Firepower 管理中心中的显示方式，而只会影响将连接与访问控制规则匹配时设备如何对其进行解释和处理。 **注释** 默认情况下，当您首次在管理中心添加威胁防御时，将启用**对象组搜索 (Object Group Search)**。
接口对象优化	设备上的接口对象优化状态。部署期间，访问控制策略和预过滤器策略中使用的接口组和安全区域生成用于每个源/目的接口对的单独规则。如果启用接口对象优化，则系统将转而为每个访问控制/预过滤器规则部署一个规则，这可简化设备配置并提高部署性能。如果选择此选项，则还需选择**对象组搜索 (Object Group Search)** 选项以降低设备上的内存使用。

以下主题介绍如何编辑高级设备设置。

注释 有关“传输数据包”(Transfer Packets) 设置的信息，请参阅编辑常规设置，第 53 页。

配置自动应用旁路

自动应用绕行 (AAB) 允许数据包在 Snort 关闭或时绕过检测，或者对于经典设备，如果数据包处理时间过长，则 。AAB 会导致 Snort 在故障发生后的十分钟内重新启动，并生成可用于分析 Snort 故障原因的故障排除数据。

注意 部分激活 AAB 会重启 Snort 进程，这会暂时中断对几个数据包的检测。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。

请参阅以下行为：

FTD 行为：如果 Snort 关闭，则在指定的计时器持续时间后触发 AAB。如果 Snort 已启用，则即使数据包处理超过配置的计时器，也不会触发 AAB。

经典设备行为：AAB 限制通过接口处理数据包所允许的时间。通过网络的数据包延迟容限来平衡数据包处理时延。

该功能适用于任何部署；但在内联部署中最有价值。

通常，在超过延迟阈值后使用入侵策略中的“规则延迟阈值”通过快速路径传送数据包。“规则延迟阈值”不关闭引擎或生成故障排除数据。

如果绕过了检测，则设备会生成运行状况监控警报。

AAB 默认为禁用；要启用 AAB，请按照所述步骤进行操作。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑高级设备设置的设备旁边，点击 **编辑**（）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备**，然后点击 **高级设置** 部分的 **编辑**（） 。

步骤 4 选中**自动应用旁路**。

步骤 5 输入介于 250 毫秒到 60,000 毫秒之间的**旁路阈值**。默认设置为 3000 毫秒 (ms)。

步骤 6 点击**保存 (Save)**。

下一步做什么

- 部署配置更改。

配置对象组搜索

运行时，威胁防御 设备会根据访问规则中使用的任何网络或接口对象的内容，将访问控制规则扩展为多个访问控制列表条目。您可以通过启用对象组搜索来减少搜索访问规则所需的内存。启用对象组搜索后，系统不会扩展网络或接口对象，而是根据这些组定义在访问规则中搜索匹配项。对象组搜索不会影响访问规则的定义方式或它们在 管理中心中的显示方式，而只会影响将连接与访问控制规则匹配时设备如何对其进行解释和处理。

启用对象组搜索可以降低包含网络或接口对象的访问控制策略的内存要求。但是，请务必注意，对象组搜索还可能会降低规则查找性能，从而提高 CPU 利用率。您应该在 CPU 影响与降低特定访问控制策略的内存要求之间取得平衡。在大多数情况下，启用对象组搜索可提高网络运营性能。

默认情况下会为在管理中心中首次添加的威胁防御设备启用对象组搜索。对于升级的设备，如果设备配置了禁用的对象组搜索，则需要手动将其启用。一次只能在一台设备上启用；您无法将其全局启用。我们建议您在部署使用网络或接口对象的访问规则的任何设备上将其启用。

注释 如果您启用对象组搜索，然后配置并操作设备一段时间，请注意，随后禁用该功能可能会导致不良结果。如果禁用对象组搜索，现有访问控制规则将按照设备的运行配置进行扩展。如果扩展所需的内存超过设备上的可用内存，设备可能会处于不一致状态，并且可能会影响性能。如果设备运行正常，则在启用对象组搜索后不应将其禁用。

开始之前

- 型号支持-威胁防御
- 我们建议您同时在每台设备上启用事务提交。在设备 CLI 中，输入 **asp rule-engine transactional-commit access-group** 命令。
- 更改此设置可能会在设备重新编译ACL时中断系统操作。我们建议您在维护窗口期间更改此设置。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要配置规则的 威胁防御设备旁，点击 **编辑**（ ）。

步骤 3 点击**设备 (Device)** 选项卡，然后点击**高级设置 (Advanced Settings)** 部分的 **编辑**（ ）。

步骤 4 选中**对象组搜索 (Object Group Search)**。

步骤 5 要使对象组搜索除网络对象外还适用于接口对象，请选中**接口对象优化 (Interface Object Optimization)**。

如果不选择**接口对象优化 (Interface Object Optimization)**，则系统会为每个源/接口对部署单独的规则，而不是使用规则中使用的安全区域和接口组。这意味着接口组不可用于对象组搜索处理。

步骤 6 点击**保存 (Save)**。

配置接口对象优化

部署期间，访问控制策略和预过滤器策略中使用的接口组和安全区域生成用于每个源/目的接口对的单独规则。如果启用接口对象优化，则系统将转而为每个访问控制/预过滤器规则部署一个规则，这可简化设备配置并提高部署性能。如果选择此选项，则还需选择**对象组搜索 (Object Group Search)** 选项以降低设备上的内存使用。

默认情况下，接口对象优化处于禁用状态。一次只能在一台设备上启用；您无法将其全局启用。

注释 如果禁用接口对象优化，则现有访问控制规则将在不使用接口对象的情况下进行部署，但这样可能会延长部署时间。此外，如果启用了对象组搜索，则其优势将不会应用于接口对象，并且您可能会在设备的运行配置中看到访问控制规则的扩展。如果扩展所需的内存超过设备上的可用内存，设备可能会处于不一致状态，并且可能会影响性能。

开始之前

型号支持-威胁防御

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要配置规则的 FTD 设备旁，点击 **编辑**（✎）。

步骤 3 点击**设备 (Device)** 选项卡，然后点击**高级设置 (Advanced Settings)** 部分的 **编辑**（✎）。

步骤 4 选中**接口对象优化 (Interface Object Optimization)**。

步骤 5 点击**保存 (Save)**。

编辑部署设置

设备 (Device) 页面上的**运行状况 (Deployment Settings)** 部分显示下表所述信息。

图 *33:* 部署设置

表 *10:* 部署设置

字段	说明 (Description)
连接失败时自动回滚部署	“启用”(Enabled) 或“禁用”(Disabled)。 您可以在管理连接因部署而失败时启用自动回滚；特别是如果您将数据用于管理中心访问，然后又错误地配置了数据接口。
连接监控间隔（分钟）	显示在回滚配置之前等待的时间。

您可以从**设备管理 (Device Management)** 页面设置部署设置。部署设置包括在管理连接因部署而失败时启用部署自动回滚；特别是如果您将数据用于管理中心访问，然后又错误地配置了数据接口。您也可以使用 **configure policy rollback** 命令手动回滚配置（请参阅如果管理中心断开连接，则手动回滚配置，第 86 页）。

请参阅以下准则：

- 只有以前的部署可以在 威胁防御 上本地提供；您无法回滚到任何较早的部署。
- 支持回滚以实现高可用性，但不支持集群部署。
- 创建高可用性后，不支持立即回滚。
- 回滚只会影响您可以在管理中心中设置的配置。例如，回滚不会影响与专用管理接口相关的任何本地配置，您只能在 威胁防御 CLI 中进行配置。请注意，如果您在上次 管理中心 部署后使用 **configure network management-data-interface** 命令更改了数据接口设置，然后使用了回滚命令，则这些设置将不会保留；它们将回滚到上次部署的 管理中心 设置。
- UCAPL/CC 模式无法回滚。
- 无法回滚上一次部署期间更新的带外 SCEP 证书数据。
- 在回滚期间，连接将被丢弃，因为当前配置将被清除。

过程

步骤 1 选择**设备** > **设备管理**。

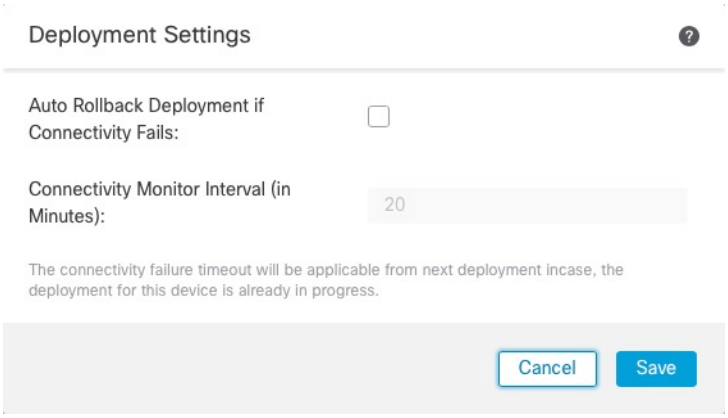
步骤 2 在要为其分配策略的设备旁边，点击 **编辑**（）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备**。

步骤 4 在**部署设置 (Deployment Settings)** 部分中，点击 **编辑**（）。

图 *34:* 部署设置



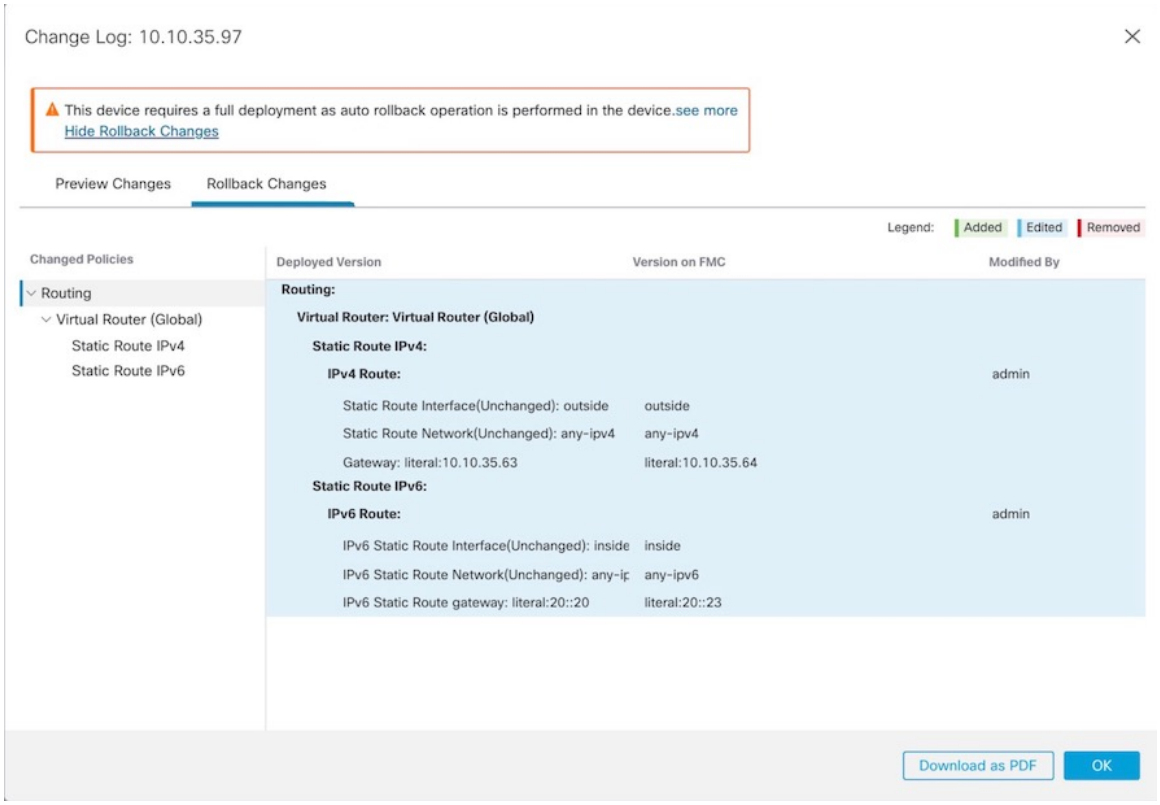
步骤 5 选中**连接失败时自动回滚部署 (Auto Rollback Deployment if Connectivity Fails)** 以启用自动回滚。

步骤 6 设置**连接监控间隔（分钟）(Connectivity Monitor Interval [in Minutes])** 以设置在回滚配置之前要等待的时间。默认值为 20 分钟。

步骤 7 如果发生回滚，请参阅以下内容以了解后续步骤。

- 如果自动回滚成功，您会看到一条成功消息，指示您执行完整部署。
- 您还可以转到**部署 (Deployment)** 屏幕，然后点击**预览 (Preview)** ( ) 图标以查看已回滚的配置部分（请参阅部署预览，第 132 页）。点击**显示回滚更改 (Show Rollback Changes)** 以查看更改，然后点击**隐藏回滚更改 (Hide Rollback Changes)** 以隐藏更改。

图 *35:* 回滚更改



- 在部署历史记录预览中，您可以查看回滚更改。请参阅查看部署历史记录预览，第 142 页。

步骤 8 检查管理连接是否已重新建立。

在 管理中心中，在 **设备** > **设备管理** > **设备** > **管理** > **FMC 访问详细信息** > **连接状态** 页面上检查管理连接状态。

在 威胁防御 CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅排除数据接口上的管理连接故障，第 88 页。

Cisco Secure Firewall 3100 上的热插拔 SSD

如果您有两个SSD，它们会在您启动时形成RAID。防火墙启动时，您可以在CLI上执行以下任务：威胁防御

- 热插拔其中一个 SSD - 如果 SSD 出现故障，您可以更换它。请注意，如果您只有一个 SSD，则无法在防火墙开启时将其删除。

- 删除一个 SSD - 如果您有两个 SSD，可以删除一个。
- 添加第二个 SSD - 如果您有一个 SSD，可以添加第二个 SSD 并形成 RAID。

⚠

注意 请勿在未使用此程序从 RAID 中移除 SSD 的情况下将其移除。可能会导致数据丢失。

过程

步骤 1 删除其中一个 SSD。

a) 从 RAID 中删除 SSD。

configure raid remove-secure local-disk {**1** | **2**}

remove-secure 关键字将从 RAID 中删除 SSD，禁用自加密磁盘功能，并对 SSD 执行安全擦除。如果您只想从 RAID 中删除 SSD 并保持数据不变，可以使用 **remove** 关键字。

示例：

```
> configure raid remove-secure local-disk 2
```

b) 监控 RAID 状态，直到 SSD 不再显示在清单中。

show raid

从 RAID 中删除 SSD 后， **可操作性** 和 **驱动器状态** 将显示为 **降级**。第二个驱动器将不再列为成员磁盘。

示例：

```
> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                operable
Presence:                   equipped
Lifecycle:                  available
Drive State:                optimal
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   0
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
```

```
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) 从机箱中取出 SSD。

步骤 2 添加 SSD。

a) 将 SSD 物理添加到空插槽。

b) 将 SSD 添加到 RAID。

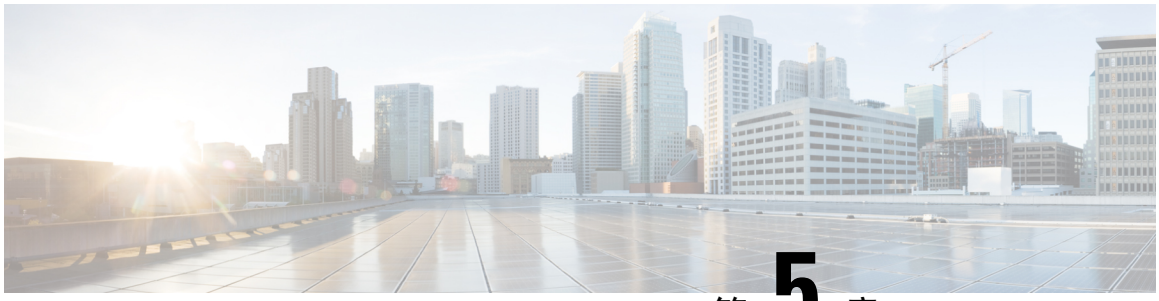
configure raid add local-disk {**1** | **2**}

将新 SSD 同步到 RAID 可能需要几个小时，在此期间防火墙完全正常运行。您甚至可以重新启动，同步将在启动后继续。使用 **show raid** 命令显示状态。

如果您安装的 SSD 以前在另一个系统上使用过，并且仍处于锁定状态，请输入以下命令：

configure raid add local-disk {**1** | **2**} *psid*

Psid 印在 SSD 背面的标签上。或者，您可以重新启动系统，SSD 将被重新格式化并添加到 RAID。



第 5 章

设备

托管设备中有一个用于 CLI 访问的默认**管理员**账户。本章介绍如何创建自定义用户帐户。

关于用户

您可以在托管设备上作为内部用户添加自定义用户账号，也可以作为 LDAP 或 RADIUS 服务器上的外部用户添加自定义用户账号。每个托管设备单独维护用户账号。例如，将某个用户添加到 管理中心时，该用户只能访问管理中心；您不能使用该用户名直接登录受管设备。您必须单独在受管设备上添加用户。

内部和外部用户

托管设备支持两种用户类型：

- 内部用户 - 设备在本地数据库中检查用户。
- 外部用户 - 如果本地数据库中没有用户，则系统会查询外部 LDAP 或 RADIUS 身份验证服务器。

CLI 访问

Firepower 设备包括一个在 Linux 上运行的 Firepower CLI。您可以使用 CLI 在设备上创建内部用户。您可以使用 管理中心在 威胁防御 设备上建立外部用户。。

⚠

注意 拥有 CLI 配置级别访问权的用户可以使用 **expert** 命令来访问 Linux 外壳，并在 Linux 外壳中获得 `sudoers` 权限，这可能会带来安全风险。出于系统安全原因，我们强烈建议：

- 仅在 TAC 监督下或在 Firepower 用户文档明确指示时使用 Linux 外壳。
- 请确保相应地限制具有 CLI 访问权限的用户列表。
- 在授予 CLI 访问权限时，请显示具有“配置”级别访问权限的用户列表。
- 请勿在 Linux 外壳中直接添加用户；请仅使用本章中的这些程序。
- 除非思科 TAC 指示或 Firepower 用户文档中有明确说明，否则请不要使用 CLI 专家模式来访问 Firepower 设备。

CLI 用户角色

在托管设备上，用户在 CLI 中的命令访问权限取决于您所分配的角色。

无

用户无法在命令行上登录设备。

配置

用户可以访问所有命令，包括配置命令。请谨慎将此访问级别分配给用户。

基本

用户只能访问非配置命令。只有内部用户和 威胁防御 外部 RADIUS 用户支持基本角色。

设备用户账号的要求和必备条件

型号支持

- 威胁防御 - 内部和外部用户

支持的域

任意

用户角色

配置外部用户 - 超级管理员或管理员用户

配置内部用户 - 超级管理员或管理员用户

设备的用户账号的准则和限制

默认值

所有设备都包括一个 **admin** 用户作为本地用户帐户；您不能删除 **admin** 用户。默认初始密码为 **Admin123**；系统会强制您在初始化过程中更改此设置。有关系统初始化的详细信息，请参阅您的型号的入门指南 。

在 CLI 中添加内部用户

使用 CLI 可在 威胁防御上创建内部用户。

过程

步骤 1 使用具有配置权限的帐户登录设备 CLI。

管理员用户帐户具有所需的权限，但具有配置权限的任何帐户都可以执行操作。您可以使用 SSH 会话或控制台端口。

对于某些 威胁防御型号，控制台端口会带您进入 FXOS CLI。使用 **connect ftd** 命令进入 威胁防御 CLI。

步骤 2 创建用户账户。

configure user add *username* {**basic** | **config**}

- 用户名-设置用户名。用户名必须对 Linux 有效：
  - 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
  - 全部小写
  - 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)
- **basic**- 提供用户基本访问权限。此角色不允许用户输入配置命令。
- **config**- 提供用户配置访问权限。此角色将赋予用户完整管理员权限，让其可以输入所有配置命令。

示例：

以下示例将添加一个名为 johncrichton 且具有配置访问权限的用户帐户。在您键入密码时，密码不会显示。

```
> configure user add johncrichton config
Enter new password for user johncrichton: newpassword
Confirm new password for user johncrichton: newpassword
> show user
```

```
Login             UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin            1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
johncrichton     1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

注释　　告知用户他们可以使用 **configure password** 命令更改自己的密码。

步骤 3　（可选）根据安全要求调整该账户的特性。

您可以使用以下命令更改默认账户行为。

- **configure user aging** *username max_days warn_days*

  设置用户密码的到期日。指定密码最大有效天数，以及密码到期前向用户发出密码即将到期警告的天数。两个值均介于 1 到 9999 之间，但是警告天数必须小于最大天数。当您创建账户时，密码没有到期日。

- **configure user forcereset** *username*

  强制用户下次登录时更改密码。

- **configure user maxfailedlogins** *username number*

  设置在锁定账户之前您允许的最大连续失败登录次数，该值介于 1 至 9999 之间。使用 **configure user unlock** 命令解锁账户。新账户的默认值为 5 次连续失败登录。

- **configure user minpasswdlen** *username number*

  设置最小密码长度，此值介于 1 至 127 之间。

- **configure user strengthcheck** *username* {**enable** | **disable**}

  启用或禁用密码强度检查，此检查要求用户在更改密码时要满足特定的密码条件。如果用户密码到期或使用了 **configure user forcereset** 命令，则此要求会在用户下次登录时自动启用。

步骤 4　根据需要管理用户账户。

用户可能被锁定在账户之外了，也可能您需要删除账户或解决其他问题。使用以下命令管理系统中的用户账户。

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

  更改用户账户的权限。

- **configure user delete** *username*

  删除指定的账户。

- **configure user disable** *username*

  禁用指定的账户，而不将其删除。用户无法登录，直到您启用该账户为止。

- **configure user enable** *username*

  启用指定的账户。

- **configure user password** *username*

更改指定用户的密码。通常情况下，用户应使用 **configure password** 命令更改自己的密码。

- **configure user unlock** *username*

  解锁因超出最大连续失败登录尝试次数而被锁定的用户账户。

配置 FTD 的外部身份验证

要启用 FTD 设备的外部身份验证，您需要添加一个或多个外部身份验证对象。

关于 威胁防御外部身份验证

在为 威胁防御 用户启用外部身份验证时，威胁防御 会使用外部身份验证对象中指定的 LDAP 或 RADIUS 服务器验证用户凭证。

管理中心 和 威胁防御 设备可使用外部身份验证对象。不同应用/设备可共享同一个对象，也可以为它们创建不同的对象。对于 威胁防御，您智能在部署到设备的平台设置中激活一个外部身份验证对象。

只有外部身份验证对象中一个子集的字段可用于威胁防御SSH访问。如果填入其他字段，它们将被忽略。如果对于其他设备类型也使用此对象，系统将使用这些字段。

LDAP 用户始终具有“配置”权限。RADIUS 用户可定义为“配置”或“基本”用户。

您可以在 RADIUS 服务器上（通过 Service-Type 属性）定义用户，也可以预定义外部身份验证对象中的用户列表。对于 LDAP，您可以指定过滤器来匹配 LDAP 服务器上的 CLI 用户。

注释 具有配置层级访问权限的用户可以使用 CLI **expert** 命令访问 Linux 外壳程序。Linux 外壳用户可以获得 root 权限，带来安全风险。确保：

- 限制具有 Linux 外壳访问权限的用户列表。
- 请勿创建 Linux 外壳用户。

关于 LDAP

通过轻量级目录访问协议(LDAP)，可以在网络上设置一个目录，用于在一个集中位置组织对象，如用户凭证。然后，多个应用可以访问这些凭证和用于描述凭证的信息。如果需要更改用户凭证，则可以在一个位置进行更改。

Microsoft 已宣布 Active Directory 服务器将在 2020 年开始实施 LDAP 绑定和 LDAP 签名。Microsoft 将这些作为一项要求，因为在使用默认设置时，Microsoft Windows 中存在一个权限提升漏洞，该漏洞可能允许中间人攻击者将身份验证请求成功转发到 Windows LDAP 服务器。有关详细信息，请参阅 Microsoft 支持站点上的 Windows 2020 LDAP 通道绑定和 LDAP 签名要求 。

如果您尚未执行此操作，我们建议您开始使用 TLS / SSL 加密对 Active Directory 服务器进行身份验证。

关于 RADIUS

远程身份验证拨入用户服务 (RADIUS) 是用于验证/授权和说明用户对网络资源的访问的一种身份验证协议。可以为符合 RFC 2865 的任何 RADIUS 服务器创建身份验证对象。

Firepower 设备支持使用 SecurID 令牌。使用 SecurID 通过服务器来配置身份验证时，利用该服务器进行身份验证的用户会将 SecurID 令牌追加到其 SecurID PIN 的末尾，并使用此代码作为其登录密码。在 Firepower 设备上无需配置任何其他信息来支持 SecurID。

为 威胁防御 添加 LDAP 外部身份验证对象

添加 LDAP 服务器以支持外部用户执行 威胁防御 管理。

共享外部身份验证对象

管理中心 和 威胁防御 设备可使用外部 LDAP 对象。管理中心 和设备可共享同一个对象，也可以为它们创建不同的对象。

威胁防御 支持的字段

只有 LDAP 对象中一个子集的字段可用于 威胁防御 SSH 访问。如果填入其他字段，它们将被忽略。如果您也将此对象用于 管理中心，则将使用这些字段。此程序仅涵盖 威胁防御 支持的字段。对于其他字段，请参阅添加 CDO的 LDAP 外部身份验证对象 ， 第 164 页。

用户名

用户名必须为使用字母数字字符加句点 (.) 或连字符 (-) 的 Linux 有效用户名，且仅可使用小写字母。不支持其他特殊字符，例如 at 符号 (@) 和斜线 (/)。不能为外部身份验证添加**管理员**用户。只能在管理中心添加外部用户（作为外部身份验证对象的一部分）；不能在 CLI 中添加他们。请注意，内部用户只能在 CLI 中添加，不能在管理中心添加。

如果您之前使用 **configure user add** 命令为内部用户配置过相同的用户名，则 威胁防御 首先对照此内部用户检查密码，如果失败，再检查 LDAP 服务器。请注意，此后不能再将具有相同名称的内部用户添加为外部用户；仅支持以前存在的内部用户。

特权等级

LDAP 用户始终具有“配置”权限。

开始之前

您必须在设备上指定 DNS 服务器用于域名查找。即使您在此程序中为 LDAP 服务器指定了 IP 地址而非主机名，LDAP 服务器也可能返回可能包括主机名的身份验证 URI。解析主机名需要进行 DNS 查询。请参阅在 CLI 中修改 威胁防御 管理接口 ， 第 78 页来添加 DNS 服务器。

过程

步骤 1 选择**系统**（⚙）> **用户 (Users)**。

步骤 2 点击 **External Authentication** 选项卡。

步骤 3 点击**添加外部身份验证对象 (Add External Authentication Object)**。

步骤 4 将**身份验证方法**设置为 **LDAP** 。

步骤 5 输入**名称**和可选**说明**。

步骤 6 从下拉列表中选择**服务器类型**。

步骤 7 对于**主服务器**，输入**主机名/IP 地址**。

如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与此字段中使用的主机名匹配。此外，加密连接不支持 IPv6 地址。

步骤 8 （可选） 更改**端口**使用的默认值。

步骤 9 （可选） 输入**备份服务器**参数。

步骤 10 输入 **LDAP 特定参数**。

a) 在**基础 DN** 中为要访问的 LDAP 目录输入基础 DN。例如，要对 Example 公司的 Security 组织中的名称进行身份验证，请输入 `ou=security,dc=example,dc=com`。或者，点击**获取 DN**，然后从下拉列表中选择相应的基本可分辨名称。

b) （可选） 输入**基本过滤器**。例如，如果目录树中的用户对象具有 `physicalDeliveryOfficeName` 属性，并且 New York 办公室中的用户对于该属性具有属性值 `NewYork`，要仅检索 New York 办公室中的用户，请输入 `(physicalDeliveryOfficeName=NewYork)`。

c) 为有足够凭证浏览 LDAP 服务器的用户输入**用户名**。例如，如果是连接到 OpenLDAP 服务器，其中用户对象具有 `uid` 属性，并且 Example 公司 Security 部门的管理员对象的 `uid` 值为 `NetworkAdmin`，则您可以输入 `uid=NetworkAdmin,ou=security,dc=example,dc=com`。

d) 在**密码**和**确认密码**字段中输入用户密码。

e) （可选） 点击**显示高级选项**配置以下高级选项。

- **加密** - 点击**无**、**TLS** 或 **SSL**。

  如果在指定端口后更改加密方法，则会将端口重置为该方法的默认值。对于**无**或 **TLS**，端口将重置为默认值 389。如果选择 SSL 加密，端口将重置为 636。

- **SSL 证书上传路径** - 对于 SSL 或 TLS 加密，必须通过点击**选择文件**选择一个证书。

  如果之前已上传证书并要将其替换，请上传新证书并将该配置重新部署到设备，以复制转移新证书。

  注释 TLS 加密要求所有平台上均有证书。对于 SSL，威胁防御 同样要求有证书。对于其他平台，SSL 不要求有证书。但我们建议您始终上传 SSL 证书以防中间人攻击。

- （未使用）**用户名模板** - 威胁防御 未使用。

- **超时 (Timeout)** - 输入滚动到备份连接之前等待的秒数（1-30 秒）。默认值为 30。

步骤 11 （可选）如果要使用用户可分辨类型之外的 CLI 访问属性，请设置 **CLI 访问属性 (CLI Access Attribute)**。例如，在 Microsoft Active Directory Server 上，通过在 **CLI 访问属性 (CLI Access Attribute)** 字段中键入 `sAMAccountName` 来使用 `sAMAccountName` CLI 访问属性检索 CLI 访问用户。

注释 具有配置层级访问权限的用户可以使用 CLI **expert** 命令访问 Linux 外壳程序。Linux 外壳用户可以获得 root 权限，带来安全风险。请确保限制具有 CLI 或 Linux 外壳访问的用户列表。

步骤 12 设置 **CLI 访问过滤器**。

选择以下方法之一：

- 要使用配置身份验证设置时指定的同一过滤器，请选择**与基本过滤器相同 (Same as Base Filter)**。
- 要根据属性值检索管理用户条目，请输入要用作过滤器的属性名、比较运算符和属性值（用括号括起来）。例如，如果所有网络管理员都具有属性值为 `shell` 的 `manager` 属性，则可以设置基本过滤器 `(manager=shell)`。

用户名必须对 Linux 有效：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

注释 如果您之前为某个内部用户配置过相同的用户名，则威胁防御会首先对照该内部用户的密码，如果失败，则会再检查 LDAP 服务器。请注意，此后不能再将具有相同名称的内部用户添加为外部用户；仅支持以前存在的内部用户。

步骤 13 点击**保存 (Save)**。

步骤 14 启用此服务器。请参阅为 SSH 配置外部身份验证，第 619 页。

步骤 15 如果以后在 LDAP 服务器上添加或删除用户，必须刷新用户列表并在托管设备上重新部署“平台设置”。

a) 点击每个 LDAP 服务器旁边的**刷新**（ ）。

如果用户列表发生变化，您将看到一条消息，建议您为设备部署配置更改。

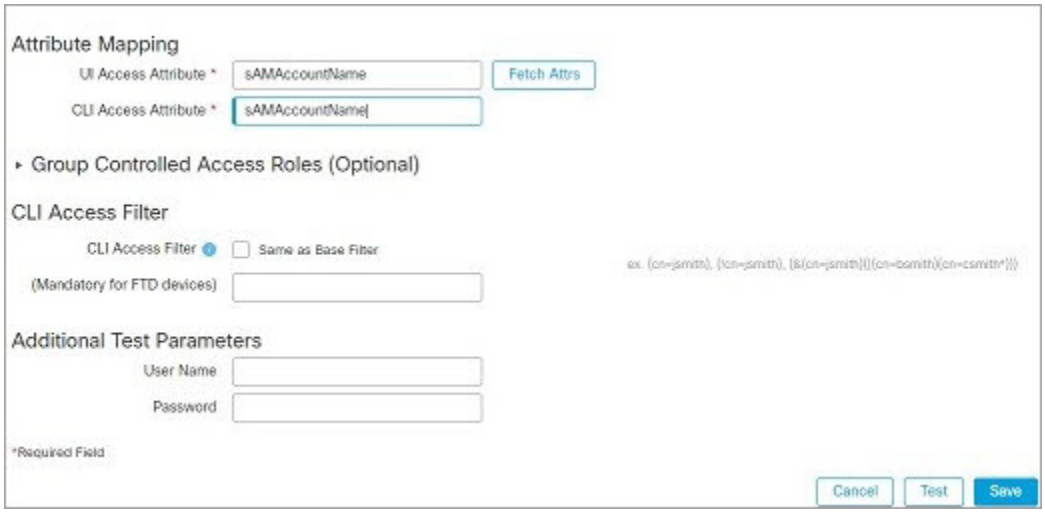
b) 部署配置更改；请参阅部署配置更改，第 136 页。

示例

基本示例

下图说明 Microsoft Active Directory Server 的 LDAP 登录身份验证对象的基本配置。此示例中的 LDAP 服务器的 IP 地址为 10.11.3.4。此连接使用端口 389 进行访问。

此示例显示对于示例公司的信息技术领域中的安全组织使用基本可分辨名称 `OU=security,DC=it,DC=example,DC=com` 的连接。



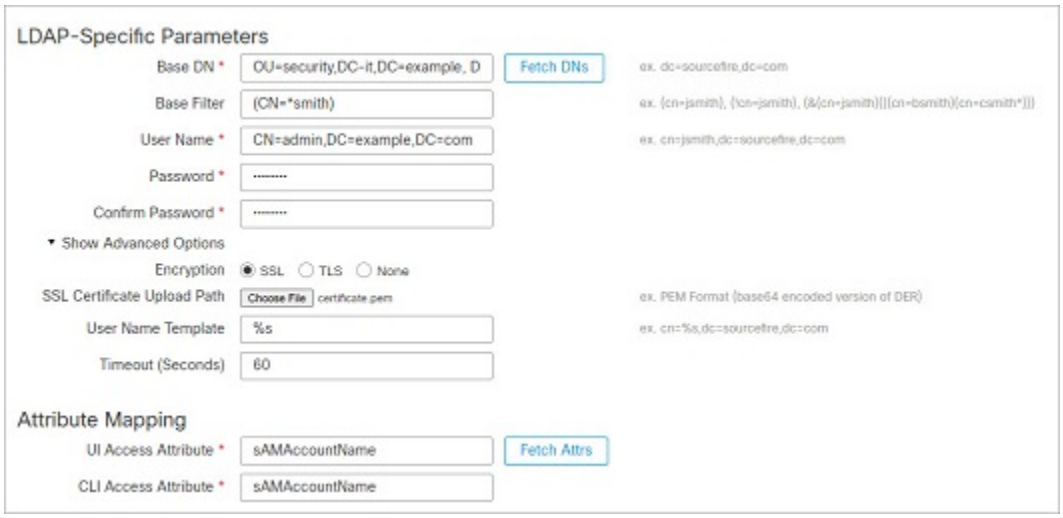
当用户登录 威胁防御 时，`sAMAccountName` 的 **CLI 访问属性**会导致检查目录中所有对象的 `sAMAccountName` 属性以查找匹配项。

请注意，由于未对此服务器应用基本过滤器，因此 威胁防御 会检查目录中基本可分辨名称所指示的所有对象的属性。经过默认时间段（或 LDAP 服务器上设置的超时期）后，与服务器的连接将超时。

高级示例

此示例说明 Microsoft Active Directory Server 的 LDAP 登录身份验证对象的高级配置。此示例中的 LDAP 服务器的 IP 地址为 10.11.3.4。此连接使用端口 636 进行访问。

此示例显示对于示例公司的信息技术领域中的安全组织使用基本可分辨名称 `OU=security,DC=it,DC=example,DC=com` 的连接。但请注意，此服务器具有基本过滤器 `(cn=*smith)`。该过滤器将从服务器检索到的用户限制为公用名称以 `smith` 结尾的用户。

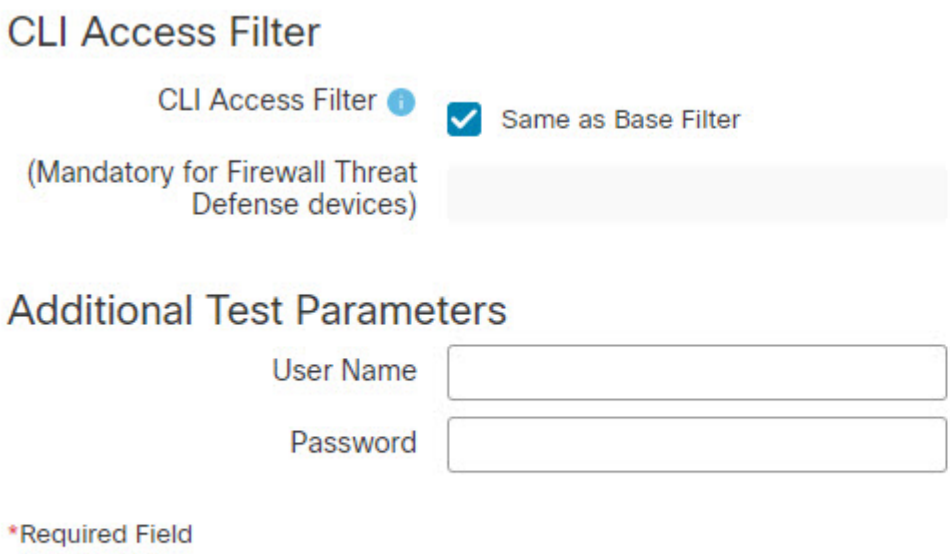


与服务器的连接使用 SSL 进行加密，并且会为该连接使用一个名为 `certificate.pem` 的证书。此外，由于**超时 (Timeout)** 设置，与服务器的连接在 60 秒后将超时。

由于此服务器是 Microsoft Active Directory 服务器，因此其使用 `sAMAccountName` 属性存储用户名而不是 `uid` 属性。

当用户登录 威胁防御 时，`sAMAccountName` 的 **CLI 访问属性**会导致检查目录中所有对象的 `sAMAccountName` 属性以查找匹配项。

在以下示例中，CLI 访问过滤器设置为与基本过滤器相同。



为 威胁防御 添加 RADIUS 外部身份验证对象

添加 RADIUS 服务器以支持外部用户进行威胁防御。

在多域部署中，外部身份验证对象仅在创建对象的域中可用。

共享外部身份验证对象

管理中心 和设备可共享同一个对象，也可以为它们创建不同的对象。请注意，威胁防御 支持在 RADIUS 服务器上定义用户，而 管理中心 要求您在外部身份验证对象中预定义用户列表。您可以选择针对 威胁防御使用预定义列表方法，但如果要在 RADIUS 服务器上定义用户，则必须为 威胁防御 和 管理中心创建单独的对象。

威胁防御 支持的字段

只有 RADIUS 对象中一个子集的字段可用于 威胁防御 SSH 访问。如果填入其他字段，它们将被忽略。如果您也将此对象用于 管理中心，则将使用这些字段。此程序仅涵盖 威胁防御 支持的字段。有关其他字段，请参阅《Cisco Secure Firewall Management Center 管理指南》中的为 管理中心 添加 RADIUS 外部身份验证对象。

用户名

不能为外部身份验证添加**管理员**用户。只能在管理中心添加外部用户（作为外部身份验证对象的一部分）；不能在 CLI 中添加他们。请注意，内部用户只能在 CLI 中添加，不能在管理中心添加。

如果您之前使用 **configure user add** 命令为内部用户配置过相同的用户名，则 威胁防御 首先对照此内部用户检查密码，如果失败，再检查 RADIUS 服务器。请注意，此后不能再将具有相同名称的内部用户添加为外部用户；仅支持以前存在的内部用户。对于 RADIUS 服务器上定义的用户，请务必将权限级别设置为与任何内部用户相同的权限级别；否则您无法使用外部用户密码登录。

过程

步骤 1 使用 Service-Type 属性在 RADIUS 服务器上定义用户。

以下是受支持的 Service-Type 属性值：

- 管理员 (6) - 提供 CLI 的配置访问授权。这些用户可以在 CLI 中使用所有命令。
- NAS 提示 (7) 或除级别 6 以外的任何级别 - 提供 CLI 的基本访问授权。这些用户可以使用只读命令，例如**show**命令，用于监控和故障排除。

名称必须是 Linux 有效的用户名：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含 at 符号 (@) 或斜线 (/)

或者，您可以在外部身份验证对象中预定义用户（参见步骤步骤 12，第 120 页）。要在为 威胁防御 使用 Service-Type 属性的同时对 威胁防御 和 管理中心 使用相同的 RADIUS 服务器，请创建可识别相同 RADIUS 服务器的两个外部身份验证对象：其中一个对象包括预定义的 **CLI 访问过滤器** 用户（用于 管理中心），另一个对象则将 **CLI 访问过滤器** 留空（用于 威胁防御）。

步骤 2 在 管理中心 中，选择**系统**（⚙）> **用户 (Users)**。

步骤 3 点击**外部身份验证 (External Authentication)**。

步骤 4 点击**添加外部身份验证对象 (Add External Authentication Object)**。

步骤 5 将**身份验证方法**设置为 **RADIUS**。

步骤 6 输入**名称**和可选**说明**。

步骤 7 对于**主服务器**，输入**主机名/IP 地址**。

注释 如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与此字段中使用的主机名匹配。此外，加密连接不支持 IPv6 地址。

步骤 8 （可选） 更改**端口**使用的默认值。

步骤 9 输入 **RADIUS 服务器密钥**。

步骤 10 （可选） 输入**备份服务器**参数。

步骤 11 （可选） 输入 **RADIUS 特定参数**。

a) 在**超时 (Timeout)** 中输入重试主服务器之前允许的秒数（介于 1 和 300 之间）。默认值为 30。

b) 输入滚动到备份服务器之前允许的**重试次数**。默认值为 3。

步骤 12 （可选）不要使用RADIUS定义的用户（请参阅步骤 步骤 1，第 119 页），在**CLI 访问过滤器 (CLI Access Filter)** 区域**管理员 CLI 访问用户列表 (Administrator CLI Access User List)** 字段中，输入应具有 CLI 访问权限的用户名并以逗号分隔。例如，输入 **`jchrichton`**、**`aerynsun`**、**`rygel`**。

您可能想要使用 威胁防御 的 **CLI 访问过滤器** 方法以便对 威胁防御 和其他平台类型使用相同的外部身份验证对象。

注释 如果想要使用 RADIUS 定义的用户，则必须将 **CLI 访问过滤器 (CLI Access Filter)** 留空。

请确保这些用户名匹配 RADIUS 服务器上的用户名。名称必须是 Linux 有效的用户名：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

注释 具有配置层级访问权限的用户可以使用 CLI **expert** 命令访问 Linux 外壳程序。Linux 外壳用户可以获得 root 权限，带来安全风险。请确保限制具有 CLI 或 Linux 外壳访问的用户列表。

步骤 13 （可选） 点击**测试 (Test)**以测试与 RADIUS 服务器的 管理中心 连接。

此功能只能测试 管理中心 与 RADIUS 服务器的连接；没有用于托管设备与 RADIUS 服务器的连接的测试功能。

步骤 14 （可选） 此外，还可以输入**其他测试参数**来测试应可以执行身份验证的用户的用户凭证：输入**用户名**和**密码**，然后点击**测试**。

提示 如果测试用户的名称或密码键入不正确，即使服务器配置正确，测试也会失败。要验证服务器配置是否正确，请点击**测试**，而无需首先在**其他测试参数**字段中输入用户信息。如果成功，请提供要通过特定用户进行测试的用户名和密码。

示例：

要测试是否可以在 Example 公司检索到 `JSmith` 用户凭证，请输入 `JSmith` 和正确的密码。

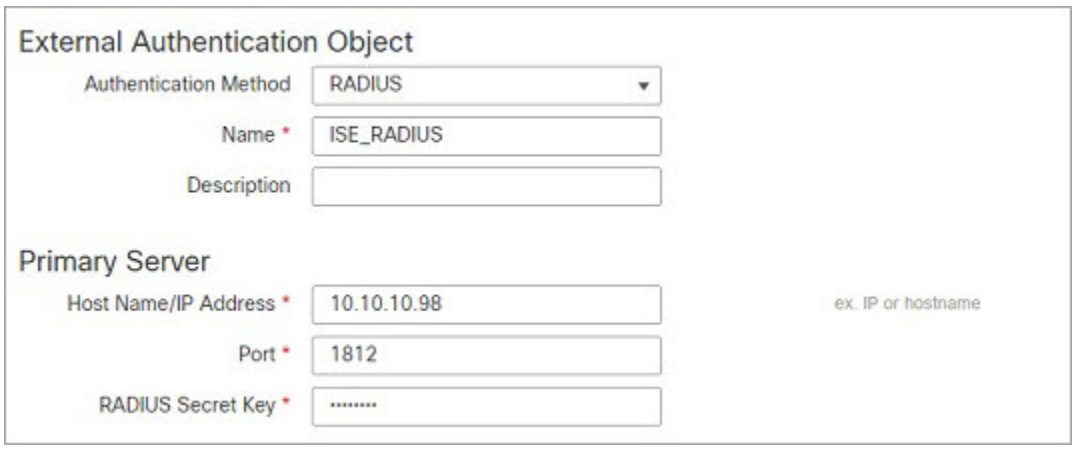
步骤 15 点击**保存 (Save)**。

步骤 16 启用此服务器。请参阅 为 SSH 配置外部身份验证，第 619 页

示例

简单的用户角色指定

下图说明端口 1812 上 IP 地址为 10.10.10.98 的运行 Cisco Identity Services Engine (ISE) 的服务器的示例 RADIUS 登录身份验证对象。未定义备份服务器。



以下示例显示 RADIUS 特定参数，包括超时（30 秒）和系统尝试联系备份服务器（如有）之前的失败重试次数。

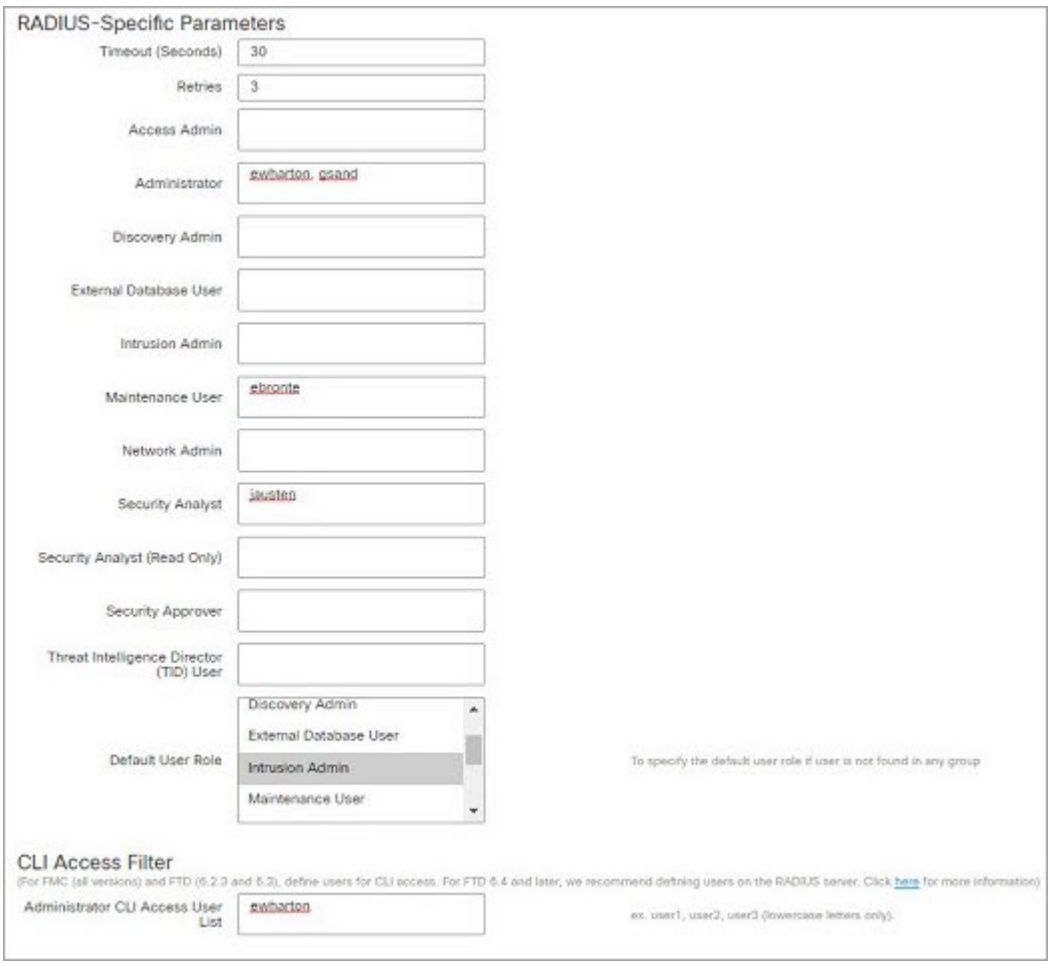
此示例说明 RADIUS 用户角色配置的重要方面：

授予用户 `ewharton` 和 `gsand` Web 界面管理权限。

授予用户 `cbronte` Web 界面“维护用户”权限。

授予用户 `jausten` Web 界面“安全分析师”权限。

用户 `ewharton` 可以使用 CLI 帐户登录到设备中。



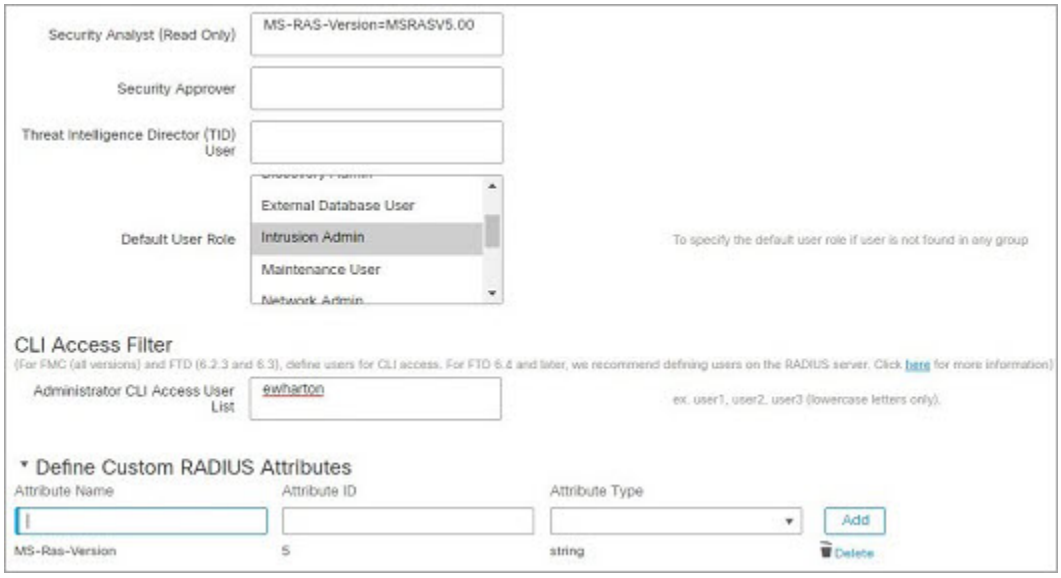
下图说明示例的角色配置：

匹配属性-值对的用户角色

可以使用属性-值对识别应接收特定用户角色的用户。如果使用的属性是自定义属性，必须定义该自定义属性。

下图说明与前一示例中相同的 ISE 服务器的示例 RADIUS 登录身份验证对象中的角色配置和自定义属性定义。

但是，在此示例中，由于正在使用 Microsoft 远程访问服务器，因此为一个或多个用户返回了 `MS-RAS-Version` 自定义属性。请注意，`MS-RAS-Version` 自定义属性为字符串。在此示例中，通过 Microsoft v. 5.00 远程访问服务器登录 RADIUS 的所有用户都应得到“安全分析师（只读）”(Security Analyst [Read Only]) 角色，因此请在**安全分析师（只读）(Security Analyst [Read Only]** 字段中输入属性-值对 `MS-RAS-Version=MSRASV5.00`。



为 FTD 设备上的用户启用外部身份验证

在 Firepower 威胁防御平台设置中启用“外部身份验证”(External Authentication)，然后将这些设置部署到受管设备。有关详细信息，请参阅为 SSH 配置外部身份验证 ，第 619 页。

LDAP 身份验证连接故障排除

如果创建 LDAP 身份验证对象，并且其无法成功连接到选择的服务器或无法检索所需的用户列表，则可以调整该对象中的设置。

如果在测试连接时该连接失败，请尝试以下建议对配置进行故障排除。

- 使用 Web 界面屏幕顶部和测试输出中显示的消息确定对象的哪些方面导致问题。
- 检查用于对象的用户名和密码是否有效：
  - 检查用户是否有权通过使用第三方 LDAP 浏览器连接到 LDAP 服务器来浏览至基本可分辨名称中指示的目录。
  - 检查用户名对于 LDAP 服务器的目录信息树是否唯一。
  - 如果在测试输出中显示 LDAP 绑定错误 49，则表明用户的用户绑定失败。请尝试通过第三方应用对服务器进行身份验证，以了解通过该连接进行的绑定是否也失败。
- 检查是否已正确识别服务器：
  - 检查服务器 IP 地址或主机名是否正确。
  - 检查是否有从本地设备到要连接的身份验证服务器的 TCP/IP 访问权限。
  - 检查对服务器的访问是否未被防火墙阻止，以及在对象中配置的端口是否已打开。

- 如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与用于服务器的主机名匹配。
- 如果是对 CLI 访问进行身份验证，请检查是否未对服务器连接使用 IPv6 地址。
- 如果使用了服务器类型默认值，请检查是否具有正确的服务器类型，并再次点击**设置默认值 (Set Defaults)** 以重置默认值。

- 如果键入了基本可分辨名称，请点击**获取 DN (Fetch DNs)** 以检索服务器上的所有可用基本可分辨名称，然后从列表中选择名称。
- 如果使用的是任意过滤器、访问属性或高级设置，请检查各项是否有效且正确键入。
- 如果使用的是任意过滤器、访问属性或高级设置，请尝试移除各设置并测试没有此设置的对象。
- 如果使用的是基本过滤器或 CLI 访问过滤器，请确保用括号将过滤器括起来，并且使用的是有效的比较运算符（包括括号在内，最大450个字符）。
- 要测试受限更多的基本过滤器，请尝试将其设置为基本可分辨名称，以使用户仅检索该用户。
- 如果使用的是加密连接：
  - 检查证书中 LDAP 服务器的名称是否与用于连接的主机名匹配。
  - 检查是否未对加密服务器连接使用 IPv6 地址。
- 如果使用的是测试用户，请确保正确键入用户名和密码。
- 如果使用的是测试用户，请移除用户凭证并测试对象。
- 通过连接到 LDAP 服务器并使用以下语法测试使用的查询：

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

例如，如果是尝试使用 `domainadmin@myrtle.example.com` 用户和基本过滤器 (`cn=*`) 连接到 `myrtle.example.com` 上的安全域，则可以使用以下语句测试连接：

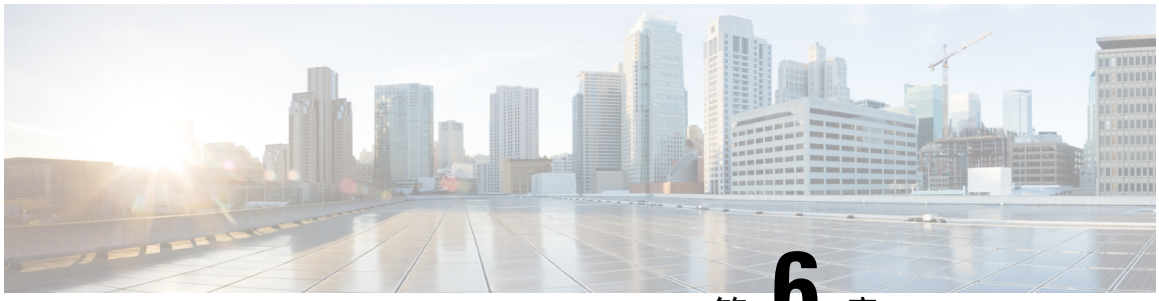
```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

如果可以成功测试连接，但在部署平台设置策略后身份验证不起作用，请检查在应用到设备的平台设置策略中是否已启用要使用的身份验证和对象。

如果成功连接，但要调整连接检索到的用户列表，则可以添加或更改基本过滤器或CLI访问过滤器，或者使用限制较多或较少的基本 DN。

在对与 Active Directory (AD) 服务器的连接进行身份验证时，尽管与 AD 服务器的连接成功，但连接事件日志很少指示受阻 LDAP 流量。当 AD 服务器发送重复的重置数据包时，会出现此不正确的连

接日志。威胁防御 设备将第二个重置数据包识别为新连接请求的一部分，并使用“阻止”操作记录连接。



第 6 章

配置部署

以下主题介绍如何在 Cisco Secure Firewall Management Center上管理各种策略：

策略管理的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 网络管理员
- 安全审批人

策略部署

注意 如果隧道也被配置为用于管理流量，请勿通过直接在 威胁防御 上终止的 VPN 隧道来推送 管理中心 部署。推动 管理中心 部署可能会停用隧道并断开 管理中心 和 威胁防御 的连接。

从这种情况下恢复设备可能会造成很大的中断，需要执行灾难恢复过程。此过程通过将管理器从 管理中心 更改为本地并从头配置设备，将 威胁防御 配置重置为出厂默认值。有关详细信息，请参阅通过 VPN 隧道部署 管理中心 策略配置，第 128 页。

在配置部署后，无论何时对该配置进行更改，您都必须向受影响设备部署更改。您可以在消息中心查看部署状态。

部署会更新以下组件：

- 设备和接口配置
- 与设备相关的策略：NAT、VPN、QoS、平台设置
- 访问控制策略以及相关策略：DNS、文件、身份、入侵、网络分析、预过滤器、SSL
- 网络发现策略
- 入侵规则更新
- 与其中任一元素相关联的配置和对象

您可以将系统配置为自动部署，方法如下：安排一个部署任务，或者将系统设置为在导入入侵规则更新时进行部署。如果允许入侵规则更新修改系统提供的基本策略以进行入侵和网络分析，则自动部署策略的方法尤其有用。入侵规则更新还可修改访问控制策略中高级预处理和性能选项的默认值。

在多域部署中，可以为您的用户帐户所属的任何域部署更改。

- 切换到祖先域，以便将更改同时部署到所有子域。
- 切换到分叶域，以便仅将更改部署到该域。

部署配置更改的最佳实践

以下是部署配置更改的指导原则。

通过 VPN 隧道部署 管理中心 策略配置

只有针对未终止隧道的设备进行部署时，才能通过 VPN 隧道部署 管理中心 策略配置。管理中心 到 威胁防御 管理流量应为其自身的安全传输 SF 隧道，无需通过 S2S VPN 隧道进行任何连接。

对于基于策略的 VPN 隧道，请选择两侧的受保护网络以排除 管理中心 到 威胁防御 的管理流量。对于基于路由的 VPN 隧道，配置路由以排除 VTI 接口的 管理中心 到 威胁防御 管理流量。

当您通过 VPN 隧道推送 管理中心 部署且管理流量也通过隧道时，如果出现任何 VPN 错误配置，则会停用隧道并导致 管理中心 和 威胁防御 断开连接。

要重新实例化隧道配置，您可以：

- 从 威胁防御 和 管理中心 中删除传感器（导致其所有配置丢失），然后再次将传感器添加到 管理中心。

  或

- 联系思科 TAC：

注释 重新实例化隧道配置需要彻底检查系统。

内联部署和被动部署

请勿将内联配置应用于被动部署的设备，反之亦然。

部署时间和内存限制

部署所需的时间取决于多个因素，包括（但不限于）：

- 发送至设备的配置。例如，如果阻止的安全情报条目数显示增加，部署时间可能要长一些。
- 设备型号和内存。内存较低的设备，部署时间可能要长一些。

请勿超过设备的能力。如果超过目标设备所支持的规则或策略最大数量，系统会显示警告。最大值取决于许多因素 - 不仅包括设备内存及处理器的数量，还与策略和规则复杂性有关。有关优化策略和规则的信息，请参阅访问控制规则的最佳实践，第 1253 页。

部署期间的流量和检测中断

在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，部署某些配置会重新启动 Snort 进程，这会中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。请参阅Snort 重启流量行为，第 144 页和部署或激活时重启 Snort 进程的配置，第 146 页。

对于 威胁防御 设备，如果部署中断了流量或检测，“部署”(Deploy) 对话框中的**检测中断 (Inspect Interruption)** 列会显示警告。您可以继续，也可以取消或延迟部署；有关详细信息，请参阅威胁防御 设备的重启警告，第 130 页。

注意 我们强烈建议在维护窗口或在中断的影响最低时部署。

自动启用应用检测器

如果执行的是应用控制，但是禁用所需的检测器，则系统会在策略部署时自动启用系统提供的适当检测器。如果不存在检测器，则系统会为该应用启用最新修改的用户定义检测器。

网络发现策略更改带来的资产重新发现

将更改部署到网络发现策略时，系统会删除并重新发现受监控网络中主机的网络映射中的 MAC 地址、TTL 和跳数信息。此外，受影响的受管设备还会放弃任何尚未发送到 管理中心的发现数据。

相关主题

Snort® 重新启动场景，第 143 页

威胁防御 设备的重启警告

部署过程中，“部署”页中的 **检查中断** 列会指定部署的配置是否在 威胁防御 设备上重启 Snort 进程。当名为 *Snort* 进程的流量检测引擎重启时，检测会中断，直到该进程恢复为止。流量将会中断还是在中断期间允许未经检测而通过，取决于设备对流量的处理方式。请注意，您可以继续进行部署，取消部署并修改配置，也可以将部署推迟到部署对网络的影响最低时执行。

当**检查中断**列显示**是**并展开设备配置列表时，系统会以**检查中断**（）指示任何将重启 Snort 进程的特定配置类型。将鼠标指针悬停在图标上时，会显示一条消息，通知您部署配置可能会中断流量。

下表总结了“部署”页面中显示的检测中断警告。

表 *11:* 检测中断指示器

类型	检测中断	说明
威胁防御	**检查中断**（）是	至少有一个配置（如果已部署）会中断设备上的检测并可能会中断流量，具体取决于设备对流量的处理方式。展开设备配置列表可以了解详细信息。
	--	部署的配置不会中断设备上的流量。
	未确定	系统无法确定部署的配置是否可能会中断设备上的流量。 进行软件升级后，有些情况下是在呼叫支持期间，首次部署之前会显示“不确定”状态。
	错误（）	系统因内部错误而无法确定状态。 取消操作，然后再次点击**部署 (Deploy)**，以便系统可以重新确定**检测中断 (Inspect Interruption)** 状态。如果问题仍然存在，请与支持人员联系。
sensor	--	被识别为 传感器 的设备不是 威胁防御 设备；系统无法确定部署的配置是否会中断此设备上的流量。

有关会为各类设备重启 Snort 进程的所有配置的信息，请参阅部署或激活时重启 Snort 进程的配置，第 146 页。

部署状态

在“部署”页上，**状态**列提供每个设备的部署状态。如果正在进行部署，则会显示部署进度的实时状态，否则会显示以下状态之一：

- 待处理 - 表示设备中有要部署的更改。
- 警告或错误 - 表示部署前检查已发现部署的警告或错误之处，而且您没有继续部署。如果出现任何警告，可以继续进行部署，但如果有任何错误，则不能继续。

注释 “状态”列仅提供“部署”页上单个用户会话的警告或错误状态。如果您离开或刷新该页面，状态将变为“待处理”。

- 失败 - 表示先前的部署失败。点击状态以查看详细信息。
- 排队中 - 表示部署已启动，而系统尚未开始部署过程。
- 已完成 - 表示部署已成功完成。

部署估计

选择设备、策略或配置后，“部署”(Deployment)页上将提供**估计 (Estimate)**链接。点击**估计 (Estimate)**链接可获取部署持续时间的估计值。持续时间是一个粗略估计值（精确度约为 70%），在少数情况下，部署所花费的实际时间可能有所不同。请参阅少数 威胁防御 设备部署的持续时间估计值。如果部署不超过 20 个 威胁防御 设备，该估计值是可靠的。

当估计值不可用时，表示数据不可用，因为所选设备上的第一次成功部署还未完成。此情况可能在管理中心 版本升级或全新安装后出现。

注释 当批量更改策略（在批量策略迁移的情况下）和选择性部署时，估计值不正确且不可靠，因为估计值基于启发式技术。

部署说明

部署说明是用户可以在部署过程中添加的自定义说明，而这些说明是可选的。

您可以在**部署历史记录 (Deployment History)** 页面中查看部署说明。在 Firepower 管理中心菜单栏中，点击**部署 (Deploy)**，然后选择**部署历史记录 (Deployment History)** 以查看每个作业的**部署说明 (Deployment Notes)** 列。

使用**部署历史记录 (Deployment History)** 页面上的“搜索”(Search) 选项按作业名称、设备名称、用户名、状态、部署说明或“收藏”等关键词进行搜索。

部署预览

预览提供要在设备上部署的所有策略和对象更改的快照。策略更改包括新策略、现有策略的更改以及已删除的策略。对象更改包括策略中使用的已添加和修改的对象。未使用的对象更改不会显示，因为它们没有部署在设备上。

在“部署”页上，“预览”列为列出的每个设备提供一个**预览**（）图标。点击预览图标后， 管理中心 会显示列出所有策略和对象更改的 UI 页。预览页上的左侧窗格以树状结构组织列出设备中更改的所有不同策略类型。

预览页面上提供的**过滤器**图标()提供了在用户级别和策略级别过滤策略的选项。点击**过滤器**图标()。选择策略或用户名，或同时选择两者，然后点击**应用 (Apply)**，将显示的列表限制为仅选定的项目。要查看所有待处理部署，请确保点击**过滤器 (Filter)** 图标并选择**重置 (Reset)**。

左侧窗格中列出策略中的所有添加、更改或删除项，或者在左侧窗格中选择的对象。右侧窗格中的两个列提供上次部署的配置设置（在 **“部署版本”** 列中）与应该部署的更改（在 **“待处理版本”** 列中）。上次部署的配置设置源自管理中心 中上次保存的部署的快照，而不是来自设备。设置的背景颜色根据页面右上角的图例分类显示。

修改者列列出了修改或添加了配置设置的用户。在策略级别， 管理中心 显示所有修改过策略的用户，而在规则级别， 管理中心 只显示最后修改规则的用户。

支持对安全情报、地理定位、Sinkhole 和文件列表对象的更改进行部署预览。有关 管理中心支持的这些和其他可重用对象的说明，请参阅 对象管理， 第 957 页。

您可以点击**下载为 PDF (Download as PDF)** 按钮下载更改日志的副本。

注释

- 要预览部署更改，您需要能从REST API访问 管理中心。要启用REST API访问，请执行《Cisco Secure Firewall Management Center 管理指南》中 启用 *REST API* 访问 中的步骤。
- 预览不会显示跨策略的规则重新排序。

  对于DNS策略，重新排序的规则作为规则添加和删除项显示在预览列表中。例如，将规则从规则顺序中的位置 1 移动到位置 3 显示为好像该规则已从位置 1 中删除，并作为新规则添加到位置 3 中。同样，删除规则时，其下的规则会列为已编辑的规则，因为它们的位置已更改。更改按它们在策略中出现的最终顺序显示。
- 首次添加接口或平台设置策略时，预览中显示所有默认值（即使未有变更）以及其他配置的设置。同样，在高可用性对配置或中断后的首次预览中也会显示设置的高可用性相关策略和默认值（即使未有变更）。
- 某些对象不支持预览。
- 仅当对象与任何设备或接口关联时，预览中才会显示添加的对象和属性的更改。删除的对象不显示。
- 以下策略不支持预览：
  - 高可用性
  - 网络发现
  - 网络分析
  - 设备设置
- 规则级别的用户信息不可用于入侵策略。
- 管理中心 将用户名显示为 **system** 以执行以下操作：
  - 回滚
  - 升级
  - 威胁防御 备份和恢复
  - SRU 更新
  - LSP 更新
  - VDB 更新
- 如果您在 **系统**（⚙）> **配置** > **信息** 中更改 管理中心 名称，则部署预览不会指定此更改，但它需要部署。
- 要查看自动回滚导致的更改，请参阅编辑部署设置，第 103 页。

对部署的过滤支持

“部署”(Deployment) 页面上的**过滤器**图标（）会提供一个选项，用于过滤待部署的设备列表。过滤器图标提供了根据所选设备和用户名过滤列表的选项。您可以使用过滤器和搜索选项来缩小到所需列表的范围。

点击过滤器图标（）。选择设备或用户名，或同时选择两者，然后点击**应用 (Apply)**，将显示的列表限制为仅选定的项目。要查看所有待处理部署，请确保点击过滤器图标（）并选择**重置 (Reset)**。

选择性策略部署

注意 如果隧道也被配置为用于管理流量，请勿通过直接在 威胁防御 上终止的 VPN 隧道来推送 管理中心 部署。推动 管理中心 部署可能会停用隧道并断开 管理中心 和 威胁防御 的连接。

从这种情况下恢复设备可能会造成很大的中断，需要执行灾难恢复过程。此过程通过将管理器从 管理中心 更改为本地并从头配置设备，将 威胁防御 配置重置为出厂默认值。有关详细信息，请参阅通过 VPN 隧道部署 管理中心 策略配置，第 128 页。

管理中心 允许您在设备上应该部署的所有更改的列表内选择特定的策略，并只部署所选的策略。选择性部署仅可用于以下策略：

- 访问控制策略
- 入侵策略
- 恶意软件和文件策略
- DNS 策略
- 身份策略
- SSL 策略
- QoS 策略
- 预过滤策略
- 网络发现
- NAT 策略
- 路由策略
- VPN 策略

在部署页面上，点击**展开箭头**（）查看设备特定的配置更改后，才会显示**策略选择**（）图标。策略选择图标可让您选择要部署的个别策略或配置，而保留其余的更改不予部署。您也可以使用此

选项查看特定策略或配置之间相互依赖的更改。管理中心 动态检测策略之间的依赖关系（例如，访问控制策略和入侵策略之间），以及共享对象和策略之间的依赖关系。相互依赖的更改以彩色标记表示，以指定一组相互依赖的部署更改。选择一个部署更改时，相互依赖的更改将自动选中。

注释

- 部署共享对象的更改后，受影响的策略也应随其一起部署。在部署过程中选择共享对象时，受影响的策略会自动选中。
- 计划部署和使用 REST API 的部署不支持选择性部署。在这些情况下，您只能选择完全部署所有更改。
- 部署前对警告和错误的检查不仅在所选策略上执行，还在所有过期的策略上执行。因此，警告或错误列表也显示取消选择的策略。
- 同样，“部署”页上**检查中断**列的指示会考虑所有过时的策略，而不仅是选定的策略。有关**检查中断**列的信息，请参阅威胁防御 设备的重启警告，第 130 页。

选择性部署策略有特定的限制。按照下表中的内容，了解何时可以使用选择性策略部署。

表 *12:* 选择性部署的限制

类型	说明	情景
完整部署	对于特定部署场景，完整部署是必要的， 管理中心 在这类场景下不支持选择性部署。如果在这类场景下遇到错误，可选择要部署在设备上的所有更改以继续。	需要完整部署的场景包括： • 升级 威胁防御 或 管理中心后的第一次部署。 • 恢复 威胁防御 后的第一次部署。 • 修改 威胁防御 接口设置后的第一次部署。 • 修改虚拟路由器设置后的第一次部署。 • 威胁防御 设备移动到新域（从全局域到子域或从子域到全局域）时。
关联策略部署	管理中心 识别相互关联和依赖的策略。选择一个相互关联的策略时，其余相互关联的策略将自动选中。	自动选择关联策略的场景： • 新对象与现有策略关联时。 • 修改现有策略的对象时。 自动选择多个策略的场景： • 当新对象与现有策略关联并且同一对象已与其他策略关联时，所有关联的策略将自动选中。 • 修改共享对象时，所有关联的策略将自动选中。

类型	说明	情景
相互依赖的策略更改（使用彩色标记显示）	管理中心动态检测策略之间以及共享对象与策略之间的依赖关系。对象或策略的相互依赖关系使用彩色标记显示。	自动选择以彩色显示的互相依赖策略或对象的场景： • 所有过期策略都有相互依赖的更改时。 例如，当访问控制策略、入侵策略和NAT策略过期时。由于访问控制策略和 NAT 策略共享一个对象，因此系统将同时选择所有策略进行部署。 • 所有过期策略共享一个对象，而该对象被修改时。
访问策略组规范	当您点击**显示或隐藏策略**（  ）时，访问策略组的策略将同时在预览窗口中的**访问策略组 (Access Policy Group)** 下列出。	访问策略组策略的场景和预期行为如下： • 如果访问控制策略过期，则在选择访问控制策略进行部署时，将选择该组下的所有其他过期策略，但文件策略和入侵策略除外。 但是，如果访问控制策略已过期，则无论是否选择访问控制策略，都可以单独选择或取消选择入侵和文件策略，除非有任何相关更改。例如，如果为访问控制规则分配了新的入侵策略，则表明存在相关更改，则选择访问控制策略和入侵策略中的任何一个时，都会自动选择访问控制策略和入侵策略。 • 如果没有过期的访问控制策略，可以选择此组中的其他过期策略单独部署。

部署配置更改

注意 如果隧道也被配置为用于管理流量，请勿通过直接在 威胁防御 上终止的 VPN 隧道来推送 管理中心 部署。推动 管理中心 部署可能会停用隧道并断开 管理中心 和 威胁防御 的连接。

从这种情况下恢复设备可能会造成很大的中断，需要执行灾难恢复过程。此过程通过将管理器从 管理中心 更改为本地并从头配置设备，将 威胁防御 配置重置为出厂默认值。有关详细信息，请参阅通过 VPN 隧道部署 管理中心 策略配置，第 128 页。

更改配置后，将其部署到受影响的设备。我们强烈建议在维护窗口或在任何流量和检测中断的影响最低时部署。

注意 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，部署某些配置会重新启动Snort进程，这会中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。请参阅Snort 重启流量行为，第 144 页和部署或激活时重启 Snort 进程的配置，第 146 页。

开始之前

- 查看部署配置更改的最佳实践，第 128 页中所述的准则。
- 确保所有受管设备都使用安全区域对象的相同修订版。如果已编辑安全区域对象：在编辑要同步的全部设备上接口的区域设置前，请勿将配置更改部署到任何设备。您必须同时部署到所有受管设备。。

注释 如果在部署期间系统读取传感器配置，则策略部署过程将失败。从传感器 CLI 执行 `show running-config` 等命令会干扰部署，从而导致部署失败。

过程

步骤 1 在 管理中心 菜单栏中，点击**部署 (Deploy)**，然后选择**部署 (Deployment)**。

GUI 页面列出了具有待处理状态的过期配置的设备。

- **修改者**列列出了修改策略或对象的用户。展开设备列表时，您可以参照每个策略列表查看修改了策略的用户。

  注释 没有为已删除的策略和对象提供用户名。

- **检查中断**列指示在部署过程中是否可能导致设备中的流量检查中断。

  请参阅 威胁防御 设备的重启警告，第 130 页 中的信息，可帮助您识别在部署到 威胁防御 设备时会中断流量检查并可能中断流量的配置。

  如果设备的此列中这一条为空白，则表明在部署过程中该设备上不会出现流量检查中断。

- **上次修改时间**列指定上次更改配置的时间。
- **预览**列允许您预览下一次要部署的更改。有关详细信息，请参阅部署预览，第 132 页。
- **状态**列提供每个部署的状态。有关详细信息，请参阅部署状态，第 131 页。

步骤 2 识别并选择要部署配置更改的设备。

- 搜索 - 在搜索框中搜索设备名称、类型、域、组或状态。
- 展开 - 点击 **展开箭头** （ › ） 以查看要部署的设备特定的配置更改。

选中设备复选框后，该设备下列出的设备的所有更改都会推送到部署中。但是，您可以使用 **策略选择**（）选择部署个别策略或配置，而保留其余的更改不予部署。有关详细信息，请参阅选择性策略部署，第 134 页。

（可选）使用 **显示或隐藏策略**（）可选择性地查看或隐藏关联的未修改策略。

注释

- 当**检查中断 (Inspect Interruption)** 列中的状态指示（是）部署会中断 威胁防御 设备上的检查并可能中断流量时，展开的列表将用 **检查中断**（）指示导致中断的特定配置。
- 当接口组、安全区或对象发生更改时，受影响的设备在 管理中心中显示为过期。为确保这些更改生效，包含这些接口组、安全区或对象的策略也需要随这些更改一起部署。受影响的策略在 管理中心的“预览”页上显示为过期。

步骤 3 （可选）点击**估计 (Estimate)** 以获取粗略估计的部署持续时间。

有关详细信息，请参阅部署估计，第 131 页。

步骤 4 点击 **部署**。

步骤 5 如果系统在要部署的更改中发现错误或警告，则会在**验证消息**窗口中显示它们。要查看完整详细信息，请点击警告或错误前的箭头图标。

有以下选项可供选择：

- 部署 - 继续部署而无需解决警告情况。如果系统识别错误，则无法继续。
- 关闭 - 退出而不部署。解决错误和警告情况，并尝试重新部署该配置。

下一步做什么

- （可选）监控部署状态；请参阅《Cisco Secure Firewall Management Center 管理指南》中的 查看部署消息 。
- 如果部署失败，请参阅部署配置更改的最佳实践，第 128 页。
- 在部署过程中，如果由于任何原因导致部署失败，则可能会影响流量。不过，这取决于某些条件。如果部署中存在特定的配置更改，则部署失败可能导致流量中断。请参阅下表，了解在部署失败时可能导致流量中断的配置更改。

配置更改	存在？	流量受影响？
访问控制策略中的**威胁防护服务**更改	是	是
VRF	是	是
接口	是	是
QoS	是	是

注释 仅当 管理中心 和 威胁防御 版本为 6.2.3 或更高版本时，部署期间中断流量的配置更改才是有效的。

相关主题

Snort® 重新启动场景，第 143 页

将现有配置重新部署到设备

可以将现有（未改变）的配置强制部署到单台受管设备。我们强烈建议在维护窗口或在任何流量和检测中断的影响最低时部署。

注意 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，部署某些配置会重新启动 Snort 进程，这会中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。请参阅Snort 重启流量行为，第 144 页和部署或激活时重启 Snort 进程的配置，第 146 页。

开始之前

查看部署配置更改的最佳实践，第 128 页中所述的准则。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击要强制部署的设备旁边的 **编辑**（ ）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备**。

步骤 4 点击 **常规** 部分标题旁边的 **编辑**（ ）。

步骤 5 请点击 **强制部署** （ ）。

注释 强制部署比常规部署需要更多时间，因为它涉及要在 FTD 上部署的策略规则的完整生成。

步骤 6 点击 **部署**。

系统会识别出您正在部署的配置中的所有错误或警告。您可以点击**继续**继续，而不解决警告状况。但是，如果系统识别到错误，则无法继续。

下一步做什么

- （可选）监控部署状态；请参阅《Cisco Secure Firewall Management Center 管理指南》中的 查看部署消息 。
- 如果部署失败，请参阅部署配置更改的最佳实践 ， 第 128 页。

相关主题

Snort® 重新启动场景 ， 第 143 页

查看部署历史记录

过程

步骤 1 在 Cisco Secure Firewall Management Center 菜单栏中，点击**部署 (Deploy)**，然后选择**部署历史 (Deployment History)**。

所有先前部署和回滚作业的列表按时间倒序显示。

步骤 2 点击所需部署作业旁边的 **展开箭头** （ ），以便查看作业中包含的设备及其部署状态。

步骤 3 （可选）点击 **脚本详细信息** （ ） 以查看发送到设备的命令以及收到的响应。

该脚本包含以下各节：

- **Snort 应用 (Snort Apply)** - 如果 Snort 相关的策略中有任何故障或响应，则此部分中会显示消息。通常，该部分为空。
- **CLI 应用 (CLI Apply)** - 此部分涵盖使用发送到设备的命令配置的功能。
- **Infrastructure Messages** - 此部分显示不同部署模块的状态。

在 **CLI 应用 (CLI Apply)** 部分中，部署脚本包括发送到设备的命令以及从该设备返回的任何响应。这些响应可以是信息性消息或错误消息。对于失败的部署，请查找指示命令错误的消息。如果您正在使用 FlexConfig 策略配置自定义的功能，则检查这些错误特别有用。这些错误可帮助您纠正尝试配置这些命令的 FlexConfig 对象中的脚本。

注释 为托管功能发送的命令与从 FlexConfig 策略生成的命令之间没有显著差异。

例如，以下序列显示管理中心发送了命令来为 GigabitEthernet0/0 配置外部逻辑名。设备的响应是自动将安全级别设置为 0。威胁防御 不会将安全级别用于任何操作。

```
========== CLI APPLY ==========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

步骤 4 （可选）点击**预览** （ ）以查看设备上部署的策略和对象更改与之前部署的版本。

修改者列列出了修改策略或对象的用户。在策略级别，管理中心 会显示已修改策略的所有用户名。在规则级别，管理中心 会显示最后修改规则的用户。

此外，要比较任意两个版本并查看更改日志，请在下拉框中选择所需的版本，然后点击**显示 (Show)** 按钮。点击**下载为 PDF (Download as PDF)** 按钮以下载更改日志的副本。

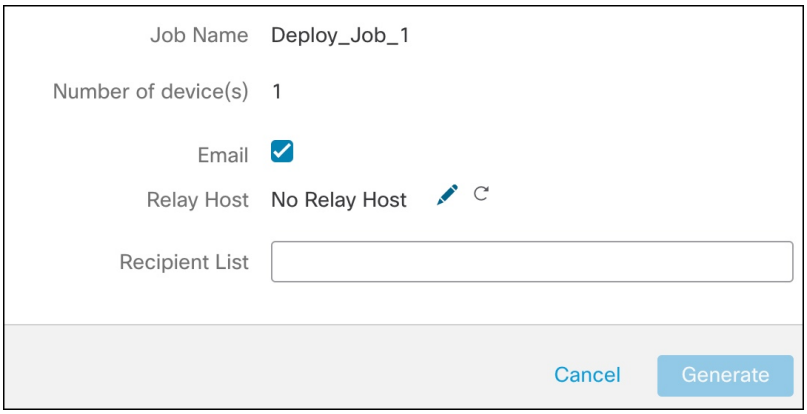
注释 认证登记、HA 操作和失败的部署不支持部署历史记录预览。

步骤 5 （可选）针对每个部署作业，点击 **更多**（⋮） 图标并执行其他操作：

- “书签”(Bookmark) - 为部署作业添加书签。
- “编辑部署说明”(Edit Deployment Notes) - 编辑为部署作业添加的自定义部署说明。
- “生成报告”(Generate Report) - 生成可用于审核的部署报告。此报告包括具有预览和脚本信息的作业属性，并且报告可以作为 PDF 文件下载。

1. 点击**生成报告 (Generate Report)** 以再次生成报告。

   图 *36:* 生成报告



2. 在**生成报告 (Generate Report)** 弹出窗口中，选中**邮件 (Email)** 复选框。
3. 如果配置了邮件中继主机，也可以通过邮件发送报告。如果未配置邮件中继主机，请使用**编辑**（✎）图标来配置或修改邮件中继主机。有关更多信息，请参阅《Cisco Secure Firewall Management Center 管理指南》中的配置邮件中继主机和通知地址。
4. 在**收件人列表 (Recipient List)** 中，您可以输入多个邮件地址并以分号分隔。
5. 点击**生成 (Generate)** 以生成报告，然后此报告将通过邮件发送给收件人。
6. 在“通知任务”(Notifications task) 选项卡中，您可以跟踪进度。完成报告生成后，点击通知任务选项卡中的链接以下载 PDF 报告。

查看部署历史记录预览

如果您看到有关自动回滚部署的横幅，请参阅编辑部署设置，第 103 页以了解详细信息。

过程

步骤 1 在 Cisco Secure Firewall Management Center 菜单栏中，点击**部署 (Deploy)**，然后选择**部署历史 (Deployment History)**。

所有先前部署和回滚作业的列表按时间倒序显示。

步骤 2 点击所需部署作业旁边的 **展开箭头**（ ），以便查看作业中包含的设备及其部署状态。

步骤 3 （可选）点击**预览**（ ）以查看设备上部署的策略和对象更改与之前部署的版本。

1. 要比较任意两个版本并查看更改日志，请在下拉框中选择所需的版本，然后点击**显示 (Show)** 按钮。下拉框会显示部署作业名称和部署结束时间。

   注释　　下拉框还会显示失败的部署。

2. 修改者列列出了修改策略或对象的用户。
   1. 在策略级别，FMC 会显示已修改策略的所有用户名。
   2. 在规则级别，FMC 会显示最后修改规则的用户。
3. 您还可以点击“下载为 PDF”(Download as PDF) 按钮下载更改日志的副本。

修改者列列出了修改策略或对象的用户。在策略级别，FMC 会显示已修改策略的所有用户名。在规则级别，FMC 会显示最后修改规则的用户。

此外，要比较任意两个版本并查看更改日志，请在下拉框中选择所需的版本，然后点击**显示 (Show)** 按钮。点击**下载为 PDF (Download as PDF)** 按钮以下载更改日志的副本。

注释　　认证登记、HA 操作和失败的部署不支持部署历史记录预览。

注释
- 部署历史预览仅支持在 FMC 7.0 版本中完成的所有部署。7.0 之前的部署不支持预览。
- 注册设备后，创建的作业历史记录不支持预览。
- 在部署历史记录中，将捕获最近 10 次成功部署、最近 5 次失败部署以及最近 5 次回滚部署。

不支持预览的 HA 场景

以下 HA 场景不支持预览：

- 如果设备处于单机模式并已建立链，则会触发自动部署。对于该特定作业，不支持预览。将鼠标悬停在 **预览** （） 上时会显示一条消息，指明这是 HA 引导程序部署，并且不支持预览。
- **配置组** - 考虑设备最初为独立设备的流程。随后进行了三个部署。在第四个部署中，设备是 HA 引导程序部署。在这些之后，用户会部署设备 5、6 和 7。部署 7 是 HA 中断部署，而用户会部署设备 8、9 和 10。

  在此流程中，不支持 3 和 5 之间的预览，因为 4 是 HA 部署。同样，也不支持 8 和 3 之间的预览。仅支持从 3 到 1、7、6、5、4 和 10、9 和 8 的预览。
- 如果设备已损坏（HA 已损坏），则新设备会被视为新设备。

Snort® 重新启动场景

当受管设备上的流量检测引擎（称为 *Snort* 进程）重启时，检测会中断，直到该进程继续运行。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。 此外，无论 Snort 进程是否重新启动，部署时的资源需求都可能导致少量数据包未经检测即被丢弃。

下表中的任何场景都将导致 Snort 进程重新启动。

表 *13: Snort* 重新启动场景

重新启动场景	更多信息
部署需要 Snort 进程重新启动的特定配置。	部署或激活时重启 Snort 进程的配置，第 146 页
修改立即重新启动 Snort 进程的配置。	会立即重新启动 Snort 进程的更改，第 147 页
流量激活当前部署的自动应用程序旁路 (AAB) 配置。	配置自动应用旁路，第 101 页

相关主题

访问控制策略高级设置，第 1271 页
部署或激活时重启 Snort 进程的配置，第 146 页

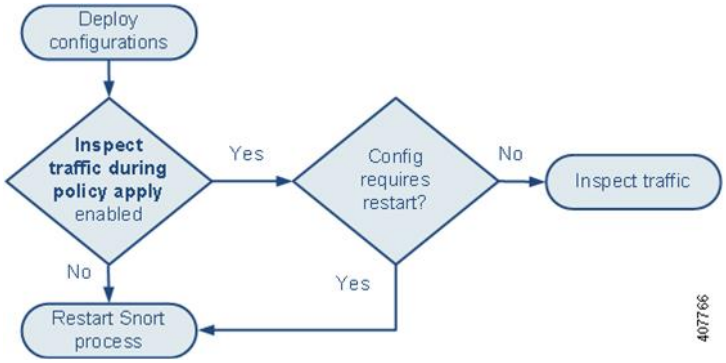
在策略应用期间检测流量

在策略应用期间检查流量是一项高级访问控制策略常规设置，支持受管设备在部署配置更改时检查流量；该设置在部署的配置需要重启 Snort 进程时不适用。可以按如下方式配置此选项：

- 已启用 - 在部署过程中会检查流量，除非某些配置要求重启 Snort 进程。

  当部署的配置不需要 Snort 重启时，系统最初使用当前部署的访问控制策略检查流量，并在部署期间切换到您正在部署的访问控制策略。
- 已禁用 - 部署期间不会检查流量。Snort 进程在您部署时总是会重启。

下图展示了当启用或禁用**在策略应用期间检查流量 (Inspect traffic during policy apply)** 时，Snort 如何重启。



注意 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，部署某些配置会重新启动 Snort 进程，这会中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。请参阅Snort 重启流量行为，第 144 页和部署或激活时重启 Snort 进程的配置，第 146 页。

Snort® 重启流量行为

下表说明在 Snort 进程重新启动时不同设备处理流量的方式。

表 *14:* 威胁防御 和 *Threat Defense Virtual* 重新启动流量影响

接口配置	重启流量行为
内联：**Snort 故障时自动打开：关闭：**禁用	被丢弃
内联：**Snort 故障时自动打开：关闭：**启用	不检查直接通过 在系统识别 Snort 已关闭之前，某些数据包可能会在缓冲区中延迟几秒钟。此延迟可能因负载分布而异。但是，缓冲的数据包最终会通过。

接口配置	重启流量行为
路由式、透明（包括 EtherChannel、冗余、子接口）：**preserve-connection**启用（**configure snort preserve-connection enable**；默认） 有关详细信息，请参阅Cisco Secure Firewall Threat Defense 命令参考。	现有 TCP/UDP 流：只要在 Snort 关闭时至少有一个数据包到达，无需检查即可通过 新 TCP/UDP 数据流和所有非 TCP/UDP 数据流：丢弃 请注意，即使启用 **preserve-connection**，以下流量也会丢弃： • 纯文本、与**Analyze**规则操作或**Analyze all tunnel traffic** 默认策略操作匹配的贯通式隧道流量 • 与访问控制规则不匹配，并由默认操作处理的连接。 • 解密的 TLS/SSL 流量 • 安全搜索流量 • 强制网络门户流量
路由式、透明（包括 EtherChannel、冗余、子接口）：**preserve-connection**禁用 (**configure snort preserve-connection disable**)	被丢弃
内联：分流模式	立即传出数据包，副本绕过 Snort
被动	不中断，不检查

注释 除了当 Snort 进程在重启时关闭这一情况下的流量处理外，在 Snort 进程繁忙时，流量也可不检查直接通过或丢弃，具体取决于 Snort 故障时自动打开**繁忙**选项（请参阅配置内联集，第 582 页）的配置。设备只支持“故障保护”选项或“Snort 故障时自动打开”选项，不同时支持这两个选项。

注释 如果 Snort 进程在部署期间正忙但未关闭，则在 CPU 总负载超过 60% 的情况下，路由式、交换式或透明接口上可能会丢弃某些数据包。

警告 在 Snort 规则更新过程中，请勿重新启动系统。

当 snort 无法足够快速地处理数据包时，会出现 Snort-busy 丢弃。Lina 不知道 Snort 是否由于处理延迟而繁忙，是否卡住或由于呼叫阻塞。当传输队列已满时，发生 snort-busy 丢弃。根据传输队列利用率，Lina 将尝试在队列服务正常时进行访问。

部署或激活时重启 Snort 进程的配置

如下所述，部署以下任何配置（AAB 除外）都会重启 Snort 进程。部署 AAB 不会导致重启，但过多的数据包延迟会激活当前部署的 AAB 配置，从而导致 Snort 进程的部分重启。

访问控制策略高级设置

- 禁用**应用策略期间检查流量**时部署。
- 添加或删除 SSL 策略。

文件策略

首先或最后部署以下任一配置；请注意，尽管以其他方式部署这些文件策略配置不会导致重启，但部署非文件策略配置则可能会导致重启。

- 执行下列操作之一：
  - 当部署的访问控制策略包括至少一个文件策略时，启用或禁用**检查存档**。
  - 当已启用**检查存档**时，添加第一个文件策略规则或删除最后一个文件策略规则（请注意，需要至少一个规则才能使**检查存档**生效）。
- 在 **Detect Files** 或 **Block Files** 规则中启用或禁用 **Store files**。
- 添加第一个将**恶意软件云查找**或**阻止恶意软件**规则操作与分析选项（**Spero 分析**或 **MSEXE**、**动态分析**或**本地恶意软件分析**）或存储文件选项（**恶意软件**、**未知**、**正常**或**自定义**）组合到一起的活动文件规则，或删除最后一个符合上述条件的活动文件规则。

请注意，仅在您的配置满足以下条件时，将这些文件策略配置部署到安全区或隧道区域的访问控制规则才会导致重启：

- 您的访问控制规则中的源或目标安全区必须匹配与目标设备上的接口相关的安全区。
- 除非您的访问控制规则中的目标区域为任何，否则规则中的源隧道区域必须与分配给预过滤器策略中隧道规则的隧道区域相匹配。

身份策略

- 当禁用 SSL 解密时（即，当访问控制策略不包含 SSL 策略时），请添加第一个或删除最后一个主动身份验证规则。

  主动身份验证规则具有**主动身份验证**规则操作或**被动身份验证**规则操作，并且**如果无法建立被动或 VPN 识别，则使用主动身份验证**已选中。

网络发现

- 使用网络发现策略，通过 HTTP、FTP 或 MDNS 协议启用或禁用基于流量的非授权用户检测。

设备管理

- MTU：在设备上的所有非管理接口中更改最高 MTU 值。
- 自动应用旁路 (AAB)：当前部署的 AAB 配置会在 Snort 进程出现故障或设备误配置导致单个数据包使用过多处理时间时激活。结果是Snort进程部分重启，以缓解极高的延迟或防止流量彻底停顿。此部分重启会导致几个数据包在不检查的情况下通过或丢弃，具体取决于设备处理流量的方式。

更新

- 系统更新：在包含新版本 Snort 二进制或数据采集库 (DAQ) 的软件更新后首次部署配置。
- VDB：对于运行 Snort 2 的受管设备，在安装包含适用于受管设备的更改的漏洞数据库 (VDB) 更新后首次部署配置需要重新启动检测引擎，并可能导致临时流量中断。这些情况下，系统会显示消息，警告您选择 管理中心 以开始安装。当 VDB 更改处于待处理状态时，部署对话框将为 威胁防御 设备提供其他警告。仅适用于 管理中心 的 VDB 更新不会导致检测引擎重启，并且您无法部署这些更新。

  对于运行 Snort 3 的受管设备，在安装漏洞数据库 (VDB) 更新后首次部署配置可能会暂时中断应用检测，但不会出现流量中断。

相关主题

部署配置更改，第 136 页
Snort® 重新启动场景，第 143 页

会立即重新启动 Snort 进程的更改

以下更改将立即重新启动 Snort 进程，而不执行部署过程。 重启对流量的影响取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。

- 采取以下任何涉及应用或应用检测器的操作：
  - 激活或者停用系统或自定义应用检测器。
  - 删除激活的自定义检测器。
  - **保存并重新激活**已激活的自定义检测器。
  - 创建用户定义的应用。

  系统会提醒您继续操作会重新启动所有受管设备上的Snort进程，并允许您取消；重启会在当前域或其任何子域中的任何受管设备上发生。
- 创建或中断 威胁防御高可用性对 - 系统会提醒您继续操作会重新启动所有受管设备上的 Snort 进程，并允许您取消。

策略比较

要查看策略更改是否符合您的组织的标准或优化系统性能，您可以检查两个策略之间的区别，或者已保存策略和正在运行策略之间的区别。

您可以比较以下策略类型：

- DNS
- 文件
- 健康状况
- 身份
- 入侵（仅限 Snort 2 策略）
- 网络分析
- SSL

比较视图以并排形式显示两个策略。突出显示两个策略之间的差异：

- 蓝色表示两个策略中此突出显示的设置存在不同，并且用红色文本注明其不同之处。
- 绿色表示突出显示的设置出现在一个策略中但未出现在另一个策略中。

比较策略

仅当您有特定策略的访问权限和任何所需的许可，并且处于配置该策略的正确域中时，才能比较策略。

过程

步骤 1 访问要比较的策略的管理页面：

- DNS - **策略** > **访问控制** > **DNS**
- 文件 - **策略** > **访问控制** > **恶意软件和文件**
- 运行状况 - **系统**（⚙） > **运行状况** > **策略**
- 身份 - **策略** > **访问控制** > **身份**
- 入侵 - **策略** > **访问控制** > **入侵**

  注释 您只能比较 Snort 2 策略。

- 网络分析 - **策略** > **访问控制**，然后点击 **网络分析策略** 或 **策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**

注释　如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

- SSL - **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**

步骤 2 点击**比较策略 (Compare Policies)**。

步骤 3 从**对比 (Compare Against)** 下拉列表中，选择要进行的比较类型：

- 要比较两个不同的策略，请选择**其他策略 (Other Policy)**。
- 要比较同一策略的两个版本，请选择**其他版本 (Other Revision)**。
- 要将其他策略与当前有效的策略进行比较，请选择**运行配置 (Running Configuration)**。

步骤 4 根据所选的比较类型，您将具有以下选项：

- 如果要比较两个不同的策略，请从**策略 A (Policy A)** 和**策略 B (Policy B)** 下拉列表中选择要比较的策略。
- 如果要比较运行配置与其他策略，请从**策略 B (Policy B)** 下拉列表中选择第二个策略。

步骤 5 点击**确定 (OK)**。

步骤 6 查看比较结果：

- 比较查看器 - 要使用比较查看器逐个浏览策略差异，请点击标题栏上方的**上一个 (Previous)**或**下一个 (Next)**。
- 比较报告 - 要生成 PDF 报告来列出两个策略之间的差异，请点击**比较报告 (Comparison Report)**。

策略报告

对于大多数策略，可以生成两种报告。有关单个策略的报告提供该策略的当前已保存配置的详细信息，而比较报告仅列出两个策略之间的区别。您可以为运行状况策略之外的所有策略类型生成单策略报告。

注释　入侵策略报告将基本策略中的设置与策略层的设置组合在一起，不区分源自基本策略或策略层的设置。

生成当前策略报告

仅当您有特定策略的访问权限和任何所需的许可，并且处于配置该策略的正确域中时，才能生成策略报告。

过程

步骤 1 访问要为其生成报告的策略的管理页面：

- 访问控制 -**策略** > **访问控制**
- DNS - **策略** > **访问控制** > **DNS**
- 文件 - **策略** > **访问控制** > **恶意软件和文件**
- 运行状况 - **系统**（⚙） > **运行状况** > **策略**
- 身份 - **策略** > **访问控制** > **身份**
- 入侵 - **策略** > **访问控制** > **入侵**
- NAT-**设备** > **NAT**
- 网络分析 - **策略** > **访问控制**，然后点击 **网络分析策略** 或 **策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**

  注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

- SSL - **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**

步骤 2 点击要生成报告的策略旁边的**报告**（📋）。

过时策略

Firepower 系统使用红色状态文本标记过期策略，表明其需要策略更新的目标设备的数量。要清除此状态，必须将策略重新部署到设备。

要求策略重新部署的配置更改包括：

- 修改访问控制策略：对访问控制规则、默认操作、策略目标、安全情报过滤、高级选项（包括预处理）等等的任何更改。
- 修改访问控制策略调用的任何策略：SSL 策略、网络分析策略、入侵策略、文件策略、身份策略或 DNS 策略。
- 更改访问控制策略或其调用的策略中所使用的任何可重用对象或配置：
  - 网络、端口、VLAN 标记、URL 和地理位置对象。
  - 安全情报列表和源
  - 应用过滤器或检测器
  - 入侵策略变量集
  - 文件列表
  - 与解密相关的对象和安全区域

- 更新系统软件、入侵规则或漏洞数据库 (VDB)。

请记住，可以从 Web 界面中的多个位置更改其中某些配置。例如，可以使用对象管理器（**对象** > **对象管理**）修改安全区域，但是修改设备配置（**设备** > **设备管理**）中的接口类型还可更改区域并要求策略重新部署。

请注意，以下更新**不**要求策略重新部署：

- 使用上下文菜单自动对安全情报源进行更新和对安全情报全局阻止或不阻止列表进行添加
- 对 URL 过滤数据的自动更新
- 计划的地理位置数据库 (GeoDB) 更新

有限部署的性能注意事项

通过主机、应用和用户发现数据，系统可以创建完整、最新的网路配置文件。系统还可用作入侵检测和防御系统 (IPS)，分析网络流量是否存在入侵和漏洞利用，或者丢弃攻击性数据包。

将发现和 IPS 组合可提供网络活动情景并允许您利用许多功能，包括：

- 影响标志和危害指示，可以告诉您哪些主机易受特定漏洞、攻击或某种恶意软件的攻击
- 自适应配置文件 和思科 建议，允许您根据目标主机以不同方式检查流量
- 关联，允许您根据受影响主机以不同方式响应入侵（和其他事件）

但是，如果您的组织对仅执行 IPS 或仅执行发现感兴趣，则有一些配置可以优化系统的性能：

不带入侵防御的发现

通过发现功能，可以监控网络流量并确定网络上主机（包括网络设备）的数量和类型，以及这些主机上的操作系统、活动应用和开放式端口。您还可以配置受管设备以监控网络上的用户活动。可以使用发现数据执行流量量变分析，评估网络合规性和对策略违规作出响应。

在基本部署中（仅包含发现和简单、基于网络的访问控制），可以通过在配置设备的访问控制策略时遵循一些重要准则来提高该设备的性能。

注释 必须使用访问控制策略，即使其只是允许所有流量也如此。网络发现策略**只**能检查访问控制策略允许通过的流量。

首先，确保访问控制策略不要求复杂的处理并仅使用简单、基于网络的条件处理网络流量。必须实施以下**所有**准则；错误配置其中任何一个选项都会消除性能优势：

- 请**勿**使用安全情报功能。从策略的安全情报配置中移除任何已填充的全局阻止或不阻止列表。
- 请**勿**包含具有 Monitor 或 Interactive Block 操作的访问控制规则。仅使用 Allow、Trust 和 Block 规则。请记住，可以通过发现检查允许的流量，但无法检查受信任和受阻止的流量。

- 请**勿**包含具有应用、用户、URL，ISE 属性或基于地理位置的网络条件的访问控制规则。仅使用简单的基于网络的条件：区域、IP 地址、VLAN 标记和端口。
- 请**勿**包含执行文件、恶意软件或入侵检查的访问控制规则。换句话说，请勿将文件策略或入侵策略与任何访问控制规则相关联。
- 在访问控制策略的“高级”(Advanced) 设置中，确保**确定访问控制规则前使用的入侵策略 (Intrusion Policy used before Access Control rule is determined)** 被设为**没有活动规则 (No Rules Active)**。
- 选择 **Network Discovery Only** 作为策略的默认操作。请**勿**为执行入侵检查的策略选择默认操作。

与访问控制策略相结合，可以配置并部署网络发现策略，它指定系统为发现数据检查的网段、端口和区域，以及是否在网段、端口和区域上发现了主机、应用和用户。

相关主题

在识别流量之前检查通过的数据包，第 2042 页

不带发现的入侵防御

在不需要的情况下禁用发现（例如，在仅限 IPS 的部署中）可以提高性能。要禁用发现，必须实施所有这些更改：

- 从网络发现策略中删除所有规则。
- 仅使用简单的、基于网络的条件执行访问控制：区域、IP 地址、VLAN 标记和端口。

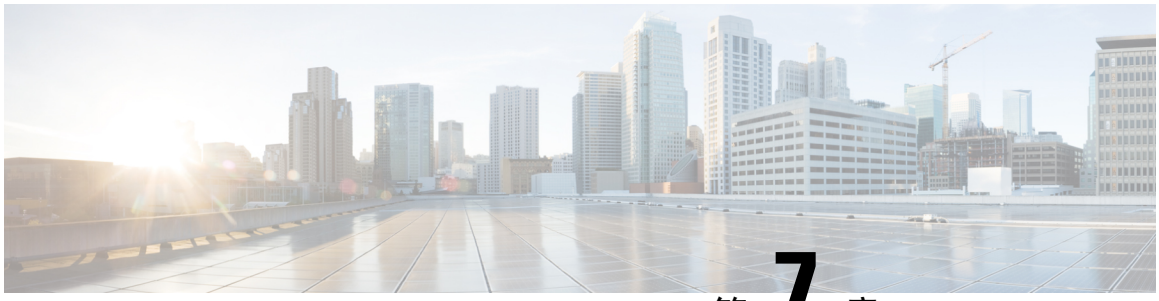
  不执行任何类型的安全情报、应用、用户、URL 或地理位置控制。虽然可以禁止系统存储发现数据，但系统仍须收集和检查该数据才能实施这些功能。
- 通过从访问控制策略的安全情报配置中删除所有阻止和不阻止列表（包括默认全局名单）来禁用基于网络和 URL 的安全情报。
- 通过删除或禁用关联的 DNS 策略中的所有规则（包括 DNS 的默认全局不阻止列表和 DNS 规则的全局阻止列表）来禁用基于 DNS 的安全情报。

部署后，目标设备上会停止进行新发现。系统会根据超时偏好设置逐渐删除网络映射中的信息。或者，可以立即清除所有发现数据。

配置部署的历史记录

第 III 部分

系统设置



第 7 章

系统配置

以下主题介绍如何在 Cisco Secure Firewall Management Center和托管设备上配置系统配置设置：

系统配置的要求和前提条件

型号支持

管理中心

支持的域

全局

用户角色

管理员

关于系统配置

系统配置设置适用于您的 Cisco Secure Firewall Management Center。

导航 Cisco Secure Firewall Management Center系统配置

系统配置可标识 管理中心 的基本设置。

过程

步骤 1 选择**系统**（⚙）>**配置**。

步骤 2 使用导航面板选择要更改的配置；有关详细信息，请参阅表 15: 系统配置设置 ，第 156 页。

系统配置设置

请注意，对于受管设备，其中许多配置由从 管理中心应用的 平台设置 策略处理；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 平台设置 。

表 *15:* 系统配置设置

设置	说明
访问控制首选项 (Access Control Preferences)	将系统配置为在用户添加或修改访问控制策略时提示他们添加注释；请参阅策略更改注释 ，第 158 页。
更改调节	将系统配置为发送过去 24 小时内出现的系统变化的详细报告；请参阅更改调节 ，第 156 页。
电子邮件通知	配置邮件主机，选择加密方法，并为基于邮件的通知和报告提供身份验证凭证；请参阅邮件通知 ，第 159 页。
入侵策略首选项 (Intrusion Policy Preferences)	将系统配置为在用户修改入侵策略时提示他们添加注释；请参阅策略更改注释 ，第 158 页。
网络分析策略首选项 (Network Analysis Policy Preferences)	将系统配置为在用户修改网络分析策略时提示他们添加注释；请参阅策略更改注释 ，第 158 页。

更改调节

要监控用户进行的更改并确保它们符合您的组织的首选标准，可以将系统配置为通过邮件发送有关过去24小时内进行的更改的详细报告。每当用户保存对系统的配置更改时，就会生成更改快照。更改调节报告将汇总这些快照的信息，以提供最新系统更改的清晰摘要。

以下示例图表显示更改调节报告示例的“用户”部分，并且列出每个配置更改前和更改后的值。如果用户多次更改同一配置，报告会按时间顺序列出每次不同更改的摘要，最近的更改最先列出。

可以查看过去 24 小时内所做的更改。

配置更改调节

开始之前

- 配置邮件服务器，以接收过去24小时对系统进行的更改的报告邮件；有关详细信息，请参阅配置邮件中继主机和通知地址，第 159 页。

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击**更改调节**。

步骤 3 选中**启用**复选框。

步骤 4 从**运行时间 (Time to Run)** 下拉列表中选择您希望系统每天发出更改调节报告的具体时间。

步骤 5 在**邮件收件人 (Email to)** 字段中输入邮箱地址。

提示 添加邮箱地址后，点击**重新发送上一报告 (Resend Last Report)** 以向收件人发送另一个最新更改调节报告的副本。

步骤 6 如果要包含策略更改，请选中**包含策略配置 (Include Policy Configuration)** 复选框。

步骤 7 如果要包含过去 24 小时进行的所有更改，请选中**显示完整更改历史记录 (Show Full Change History)** 复选框。

步骤 8 点击**保存 (Save)**。

相关主题

使用审核日志检查更改

更改调节选项

包括策略配置 (Include Policy Configuration) 选项用于控制系统是否在更改调节报告中包括策略更改记录。这包括对访问控制策略、入侵策略、系统策略、运行状况策略和网络发现策略的更改。如果未选择该选项，报告将不会显示对任何策略的更改。此选项仅适用于 管理中心。

显示完整更改历史记录 (Show Full Change History) 选项用于控制系统是否在更改调节报告中包括过去24小时内发生的所有更改的记录。如果未选择该选项，报告仅包括每个类别的更改的整合视图。

注释 更改调节报告不包括对 威胁防御 接口和路由设置的更改。

策略更改注释

当用户修改访问控制、入侵或网络分析策略时，可以配置Firepower系统以使用注释功能跟踪多个与策略相关的更改。

在启用策略更改注释的情况下，管理员可以快速评估修改部署中的关键策略的原因。或者，可以将对入侵策略和网络分析策略的更改写入到审核日志中。

配置跟踪策略更改的注释

可以将系统配置为在用户修改访问控制策略、入侵策略或网络分析策略时提示他们添加注释。可以使用注释来跟踪用户更改策略的原因。如果对策略更改启用了注释功能，则可以将注释设置为可选或必填项。每次保存对策略所作的新更改时，系统都会提示用户输入注释。

过程

步骤 1 选择**系统**（⚙）> **配置**。

系统配置选项显示在左侧导航面板中。

步骤 2 为以下各项配置策略注释首选项：

- 点击**访问控制首选项 (Access Control Preferences)** 为访问控制策略配置注释首选项。
- 点击**入侵策略首选项 (Intrusion Policy Preferences)** 为入侵策略配置注释首选项。
- 点击**网络分析策略首选项 (Network Analysis Policy Preferences)** 为网络分析策略配置注释首选项。

步骤 3 每个策略类型有以下选项：

- **已禁用 (Disabled)** - 禁用更改注释。
- **可选 (Optional)** - 让用户可以根据需要在注释中描述其更改。
- **必需 (Required)** - 要求用户在保存之前在注释中描述其更改。

步骤 4 对于入侵或网络分析策略注释，还可以：

- 选中**将入侵策略中的更改写入审核日志 (Write changes in Intrusion Policy to audit log)** 以将所有入侵策略更改写入审核日志。
- 选中**将网络分析策略中的更改写入审核日志 (Write changes in Network Analysis Policy to audit log)** 以将所有网络分析策略更改写入审核日志。

步骤 5 要在LSP更新期间获取任何 已覆盖的 系统定义的规则更改的通知，请确保选中 **保留已删除的 Snort 3 规则的用户覆盖** 复选框。系统默认情况下，此复选框为选中状态。选中此复选框时，系统会在LSP更新过程中添加的新替换规则中保留规则覆盖。通知显示在 **齿轮** 旁边的 **通知** 图标下的 **任务** 选项卡中（⚙）。

步骤 6 点击**保存 (Save)**。

邮件通知

如果要执行以下操作，请配置邮件主机：

- 通过邮件发送基于事件的报告
- 通过邮件发送有关预定任务的报告
- 通过邮件发送更改调节报告
- 通过邮件发送数据删除通知
- 将邮件用于发现事件、影响标志、关联事件警报，入侵事件警报和运行状况事件警报

配置邮件通知时，可以为系统与邮件中继主机之间的通信选择加密方法，并可根据需要为邮件服务器提供身份验证凭证。配置后，可以测试连接。

配置邮件中继主机和通知地址

过程

步骤 1 选择**系统**（⚙）> **配置**。

步骤 2 点击 **Email Notification**。

步骤 3 在**邮件中继主机 (Mail Relay Host)** 字段中，输入要使用的邮件服务器的主机名或 IP 地址。输入的邮件主机**必须**允许从设备进行访问。

步骤 4 在**端口号 (Port Number)** 字段，请输入邮件服务器上使用的端口号。

典型的端口包括：

- 25，使用加密时
- 465，使用 SSLv3 时
- 587，使用 TLS 时

步骤 5 在**加密方法 (Encryption Method)** 中选择一种加密方法。

- **TLS** - 使用传输层安全加密通信。
- **SSLv3** - 使用安全套接字层加密通信。
- **无 (None)** - 允许未加密的通信。

注释 设备和邮件服务器之间的加密通信不要求进行证书验证。

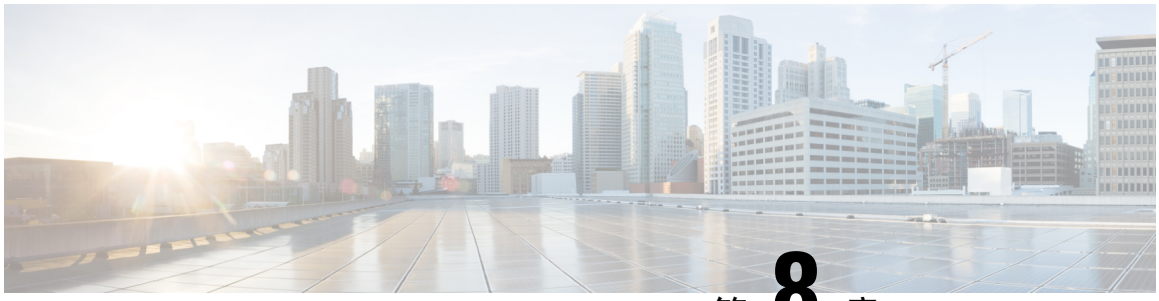
步骤 6 在**源地址 (From Address)** 字段，输入要将其用作设备发送消息的源邮箱地址的有效邮箱地址。

步骤 7 或者，要在连接到邮件服务器时提供用户名和密码，请选择**使用身份验证 (Use Authentication)**。在**用户名 (Username)** 字段中输入用户名。在**密码 (Password)** 字段中输入密码。

步骤 8 要使用已配置的邮件服务器发送测试邮件，请点击**测试邮件服务器设置 (Test Mail Server Settings)**。

系统会在按钮旁边显示一条消息，以指明测试是否成功。

步骤 9 点击**保存 (Save)**。



第 8 章

管理中心 的

管理中心 包括用于 Web 和 CLI 访问的默认 **管理员** 账户。本章介绍如何创建自定义用户帐户。

关于用户

您可以在托管设备上作为内部用户添加自定义用户账号，也可以作为 LDAP 或 RADIUS 服务器上的外部用户添加自定义用户账号。每个托管设备单独维护用户账号。例如，将某个用户添加到 管理中心时，该用户只能访问管理中心；您不能使用该用户名直接登录受管设备。您必须单独在受管设备上添加用户。

内部和外部用户

托管设备支持两种用户类型：

- 内部用户 - 设备在本地数据库中检查用户。
- 外部用户 - 如果本地数据库中没有用户，则系统会查询外部 LDAP 或 RADIUS 身份验证服务器。

用户角色

CLI 用户角色

管理中心 上的 CLI 外部用户没有用户角色；他们可以使用所有可用命令。

Web 界面用户角色

思科防御协调器 (CDO) 中有多种用户角色：只读、仅编辑、仅部署、管理员和超级管理员。为每个租户上的每个用户配置用户角色。如果 CDO 用户可以访问多个租户，则他们可能具有相同的用户

ID，但在不同的租户中具有不同的角色。用户可能在一个租户上具有只读角色，在另一个租户上具有超级管理员角色。当界面或文档提及只读用户、仅部署、仅编辑、管理员用户或超级管理员用户时，我们描述的是该用户对特定租户的权限级别。

只读

只读用户无法编辑策略和对象，也无法将更改部署到设备，只能查看它们。

仅部署

仅部署用户可以查看所有策略和对象。将暂存更改部署到一个或多个设备。

仅编辑

“仅编辑”用户可以修改并保存策略和对象，但不能将其部署到设备。

超级管理员和管理员

超级管理员和管理员用户可以访问产品中的所有内容。此用户可以创建、读取、修改和删除任何策略和对象，并将其部署到设备。

使用您的 CDO 用户名创建 CDO 用户记录

只有具有“超级管理员”权限的 CDO 用户才能创建 CDO 用户记录。超级管理员应使用上述 **创建您的 CDO 用户名** 任务中指定的相同邮箱地址创建用户记录。

使用以下程序创建具有适当用户角色的用户记录：

Procedure

步骤 1 登录 CDO。

步骤 2 从 CDO 菜单栏中，选择 **设置** > **用户管理**。

步骤 3 点击蓝色加号按钮  ，将新用户添加到租户。

步骤 4 提供用户的邮件地址。

Note 用户的邮箱地址必须与 Cisco Secure Log-On 账户的邮箱地址相对应。

步骤 5 从下拉菜单中选择用户的 角色 。

步骤 6 点击**确定 (OK)**。

为 管理中心配置外部身份验证

要启用外部身份验证，您需要添加一个或多个外部身份验证对象。

关于 管理中心外部身份验证

在为管理用户启用外部身份验证时，管理中心 会使用 外部身份验证对象中指定的 LDAP 或 RADIUS 服务器验证用户凭证。

您可以为 Web 界面访问配置多个外部身份验证对象。例如，如果您有 5 个外部身份验证对象，则其中任意对象的用户均可通过身份验证来访问 Web 界面。对于 CLI 访问，仅可使用一个外部身份验证对象。如果您启用了多个外部身份验证对象，用户仅可使用列表中的第一个对象进行身份验证。

对于管理中心，请直接在 **系统** > **用户** > **外部身份验证** 选项卡上启用外部身份验证对象；此设置仅会影响 管理中心 的使用情况，无需在此选项卡上为了受管设备的使用而启用此设置。对于 威胁防御 设备，必须在部署到设备的平台设置中启用外部身份验证对象。

Web 界面用户由外部身份验证对象中的 CLI 用户单独定义。对于 RADIUS 上的 CLI 用户，您必须预配置外部身份验证对象中的 RADIUS 用户名列表。对于 LDAP，您可以指定过滤器来匹配 LDAP 服务器上的 CLI 用户。

注释 具有配置层级访问权限的用户可以使用 CLI **expert** 命令访问 Linux 外壳程序。Linux 外壳用户可以获得 root 权限，带来安全风险。确保：

- 限制具有 CLI 或 Linux 外壳访问权限的用户列表。
- 请勿创建 Linux 外壳用户。

关于 LDAP

通过轻量级目录访问协议 (LDAP)，可以在网络上设置一个目录，用于在一个集中位置组织对象，如用户凭证。然后，多个应用可以访问这些凭证和用于描述凭证的信息。如果需要更改用户凭证，则可以在一个位置进行更改。

Microsoft 已宣布 Active Directory 服务器将在 2020 年开始实施 LDAP 绑定和 LDAP 签名。Microsoft 将这些作为一项要求，因为在使用默认设置时，Microsoft Windows 中存在一个权限提升漏洞，该漏洞可能允许中间人攻击者将身份验证请求成功转发到 Windows LDAP 服务器。有关详细信息，请参阅 Microsoft 支持站点上的 Windows 2020 LDAP 通道绑定和 LDAP 签名要求 。

如果您尚未执行此操作，我们建议您开始使用 TLS / SSL 加密对 Active Directory 服务器进行身份验证。

关于 RADIUS

远程身份验证拨入用户服务 (RADIUS) 是用于验证/授权和说明用户对网络资源的访问的一种身份验证协议。可以为符合 RFC 2865 的任何 RADIUS 服务器创建身份验证对象。

Firepower 设备支持使用 SecurID 令牌。使用 SecurID 通过服务器来配置身份验证时，利用该服务器进行身份验证的用户会将 SecurID 令牌追加到其 SecurID PIN 的末尾，并使用此代码作为其登录密码。在 Firepower 设备上无需配置任何其他信息来支持 SecurID。

添加 CDO的 LDAP 外部身份验证对象

添加 LDAP 服务器以支持外部用户执行设备管理。

在多域部署中，外部身份验证对象仅在创建对象的域中可用。

开始之前

- 您必须在设备上指定 DNS 服务器用于域名查找。即使您在此程序中为 LDAP 服务器指定了 IP 地址而非主机名，LDAP 服务器也可能返回可能包括主机名的身份验证 URI。解析主机名需要进行 DNS 查询。
- 如果是配置用于 CAC 身份验证的 LDAP 身份验证对象，请勿移除在计算机中插入的 CAC。启用用户证书后，必须一直插入 CAC。

过程

步骤 1 选择**系统**（⚙）> **用户 (Users)**。

步骤 2 点击 **External Authentication** 选项卡。

步骤 3 点击**添加外部身份验证对象 (Add External Authentication Object)**。

步骤 4 将**身份验证方法**设置为 **LDAP** 。

步骤 5 输入**名称**和可选**说明**。

步骤 6 从下拉列表中选择**服务器类型**。

提示 如果点击**设置默认值 (Set Defaults)**，设备将使用服务器类型的默认值填充**用户名模板 (User Name Template)**、**UI 访问属性 (UI Access Attribute)**、**CLI 访问属性 (CLI Access Attribute)**、**组成员属性 (Group Member Attribute)** 和**组成员 URL 属性 (Group Member URL Attribute)** 字段。

步骤 7 对于**主服务器**，输入**主机名/IP 地址**。

如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与此字段中使用的主机名匹配。此外，加密连接不支持 IPv6 地址。

步骤 8 （可选） 更改**端口**使用的默认值。

步骤 9 （可选） 输入**备份服务器**参数。

步骤 10 输入 **LDAP 特定参数**。

a) 在**基础 DN** 中为要访问的 LDAP 目录输入基础 DN。例如，要对 Example 公司的 Security 组织中的名称进行身份验证，请输入 `ou=security,dc=example,dc=com`。或者，点击**获取 DN**，然后从下拉列表中选择相应的基本可分辨名称。

b) （可选） 输入**基本过滤器**。例如，如果目录树中的用户对象具有 `physicalDeliveryOfficeName` 属性，并且 New York 办公室中的用户对于该属性具有属性值 `NewYork`，要仅检索 New York 办公室中的用户，请输入 `(physicalDeliveryOfficeName=NewYork)`。

如果使用 CAC 身份验证，要仅过滤活动用户账号（禁用的用户账号除外），请输入 `(!(userAccountControl:1.2.840.113556.1.4.803:=2))`。此条件检索 AD 中属于 `ldpgrp` 组且 `userAccountControl` 属性值不为 `2` （已禁用）的用户账户。

c) 为有足够凭证浏览 LDAP 服务器的用户输入**用户名**。例如，如果是连接到 OpenLDAP 服务器，其中用户对象具有 `uid` 属性，并且 Example 公司 Security 部门的管理员对象的 `uid` 值为 `NetworkAdmin`，则您可以输入 `uid=NetworkAdmin,ou=security,dc=example,dc=com`。

d) 在**密码**和**确认密码**字段中输入用户密码。

e) （可选） 点击**显示高级选项**配置以下高级选项。

- **加密** - 点击**无**、**TLS** 或 **SSL**。

  如果在指定端口后更改加密方法，则会将端口重置为该方法的默认值。对于**无**或 **TLS**，端口将重置为默认值 389。如果选择 SSL 加密，端口将重置为 636。

- **SSL 证书上传路径** - 对于 SSL 或 TLS 加密，必须通过点击**选择文件**选择一个证书。

  如果之前已上传证书并要将其替换，请上传新证书并将该配置重新部署到设备，以复制转移新证书。

  注释 TLS 加密要求所有平台上均有证书。但我们建议您始终上传 SSL 证书以防中间人攻击。

- **用户名模板** - 提供与您的 **UI 访问属性**对应的模板。例如，要通过连接到 UI 访问属性为 `uid` 的 OpenLDAP 服务器来对 Example 公司的 Security 组织中工作的所有用户进行身份验证，可在**用户名模板**字段中输入 `uid=%s,ou=security,dc=example,dc=com`。对于 Microsoft Active Directory Server，可以输入 `%s@security.example.com`。

  CAC 身份验证需要使用此字段。

- **外壳用户名模板 (Shell User Name Template)** - 提供与您的 **CLI 访问属性 (CLI Access Attribute)** 对应的模板以进行 CLI 用户身份验证。例如，要通过连接到 CLI 访问属性为 `sAMAccountName` 的 OpenLDAP 服务器来对 Security 组织中工作的所有用户进行身份验证，可在**外壳用户名模板 (Shell User Name Template)** 字段中输入 `%s` 。

- **超时 (Timeout)** - 输入滚动到备份连接之前等待的秒数（1-1024 秒）。默认值为 30。

  注释 威胁防御 和 管理中心的超时范围不同，因此，如果共享对象，请确保不要超过威胁防御的较小超时范围（1-30 秒）。如果将超时设置为更高的值，则 威胁防御 LDAP 配置将不起作用。

步骤 11 （可选） 配置**属性映射 (Attribute Mapping)** 以基于属性检索用户。

- 输入 **UI 访问属性**或点击**获取属性**，以检索可用属性的列表。例如，在 Microsoft 活动目录服务器上，可能要使用 UI 访问属性检索用户，因为在 Active 目录服务器用户对象上可能没有 `uid` 属性。相反，可以通过在 **UI 访问属性 (UI Access Attribute)** 字段中输入 `userPrincipalName` 来搜索 `userPrincipalName` 属性。

- 如果要使用用户可分辨类型之外的外壳访问属性，请设置 **CLI 访问属性 (CLI Access Attribute)** 。例如，在 Microsoft 活动目录服务器上，通过键入 `sAMAccountName` 可使用 `sAMAccountName` CLI 访问属性来检索外壳访问用户。

步骤 12 （可选） 配置**组控制的访问角色**。

如果不使用组控制的访问角色配置用户权限，则用户仅具有外部身份验证策略默认授予的权限。

a) （可选） 在与用户角色对应的字段中，输入包含应向其分配这些角色的用户的 LDAP 组的可分辨名称。

引用的任何组都必须存在于 LDAP 服务器上。可以引用静态 LDAP 组或动态 LDAP 组。静态 LDAP 组是成员身份由指向特定用户的组对象属性确定的组，动态 LDAP 组是通过创建根据用户对象属性检索组用户的 LDAP 搜索来确定成员身份的组。角色的组访问权限仅影响身为组成员的用户。

如果使用动态组，则完全按照 LDAP 查询在 LDAP 服务器上的配置来使用 LDAP 查询。因此，Firepower 设备将搜索的递归数限制为 4，以防搜索语法错误导致无限循环。

示例：

在**管理员**字段中输入以下内容，以便对 Example 公司信息技术部门中的名称进行身份验证：

```
cn=itgroup,ou=groups, dc=example,dc=com
```

b) 对于不属于任何指定组的用户，选择**默认用户角色**。

c) 如果使用静态组，请输入**组成员属性 (Group Member Attribute)**。

示例：

如果使用 `member` 属性指示默认“安全分析师”访问权限静态组中的成员身份，请输入 `member`。

d) 如果使用动态组，请输入**组成员 URL 属性 (Group Member URL Attribute)**。

示例：

如果 `memberURL` 属性包含用于检索为默认“管理员”访问权限指定的动态组成员的 LDAP 搜索，请输入 `memberURL`。

步骤 13 （可选） 设置 **CLI 访问过滤器 (Shell Access Attribute)** 以允许 CLI 用户。

为防止对 CLI 访问进行 LDAP 身份验证，请将此字段留空。要指定 CLI 用户，请选择以下方法之一：

- 要使用配置身份验证设置时指定的同一过滤器，请选择**与基本过滤器相同 (Same as Base Filter)**。
- 要根据属性值检索管理用户条目，请输入要用作过滤器的属性名、比较运算符和属性值（用括号括起来）。例如，如果所有网络管理员都具有属性值为 `shell` 的 `manager` 属性，则可以设置基本过滤器 `(manager=shell)`。

用户名必须对 Linux 有效：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)

- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

注释 具有配置层级访问权限的用户可以使用 CLI **expert** 命令访问 Linux 外壳程序。Linux 外壳用户可以获得 root 权限，带来安全风险。请确保限制具有 CLI 或 Linux 外壳访问的用户列表。

注释 请勿创建与包括在 **CLI 访问过滤器 (CLI Access Filter)** 中的用户具有相同用户名的任何内部用户。唯一的内部 管理中心 用户应为 **admin**；请勿在 **CLI 访问过滤器 (CLI Access Filter)** 中包含**管理员**用户。

步骤 14 （可选） 点击**测试**以测试与 LDAP 服务器的连接状况。

测试输出列出有效和无效的用户名。有效用户名是唯一的，并且可以包含下划线 (_)、句号 (.)、连字符 (-) 和字母数字字符。请注意，受 UI 页面大小限制，测试与具有 1000 个以上用户的服务器的连接仅会返回 1000 个用户。如果测试失败，请参阅LDAP 身份验证连接故障排除，第 176 页。

步骤 15 （可选） 此外，还可以输入**其他测试参数**来测试应可以执行身份验证的用户的用户凭证：输入**用户名** `uid` 和**密码**，然后点击**测试**。

如果是连接到 Microsoft Active Directory Server 并提供 UI 访问属性来代替 `uid`，请使用该属性的值作为用户名。还可以为用户指定完全限定的可分辨名称。

提示 如果测试用户的名称或密码键入不正确，即使服务器配置正确，测试也会失败。要验证服务器配置是否正确，请点击**测试**，而无需首先在**其他测试参数**字段中输入用户信息。如果成功，请提供要通过特定用户进行测试的用户名和密码。

示例：

要测试是否可以在 Example 公司检索到 `JSmith` 用户凭证，请输入 `JSmith` 和正确的密码。

步骤 16 点击**保存 (Save)**。

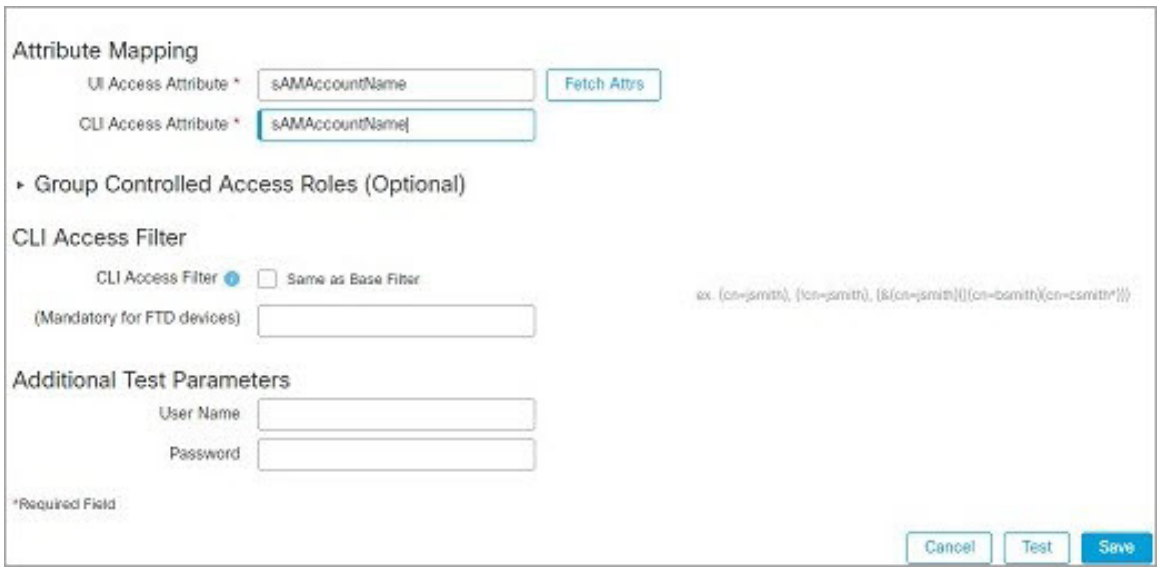
步骤 17 启用此服务器。请参阅为 CDO上的用户启用外部身份验证，第 175 页。

示例

基本示例

下图说明 Microsoft Active Directory Server 的 LDAP 登录身份验证对象的基本配置。此示例中的 LDAP 服务器的 IP 地址为 10.11.3.4。此连接使用端口 389 进行访问。

此示例显示对于示例公司的信息技术领域中的安全组织使用基本可分辨名称 `OU=security,DC=it,DC=example,DC=com` 的连接。



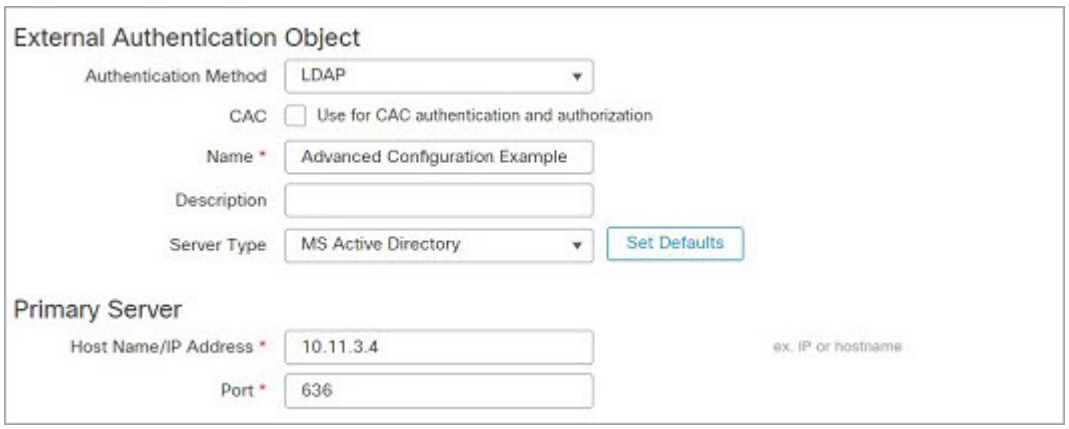
但是，由于此服务器是 Microsoft Active Directory 服务器，因此其使用 `sAMAccountName` 属性存储用户名而不是 `uid` 属性。选择 MS Active Directory 服务器类型并点击**设置默认值 (Set Defaults)** 会将“UI 访问属性”(UI Access Attribute) 设置为 `sAMAccountName`。因此，当用户尝试登录系统时，系统会检查各对象的 `sAMAccountName` 属性以查找匹配的用户名。

此外，当用户登录到设备上的 CLI 账户中时， `sAMAccountName` 的 CLI会导致检查目录中所有对象的 `sAMAccountName` 属性以查找匹配项。

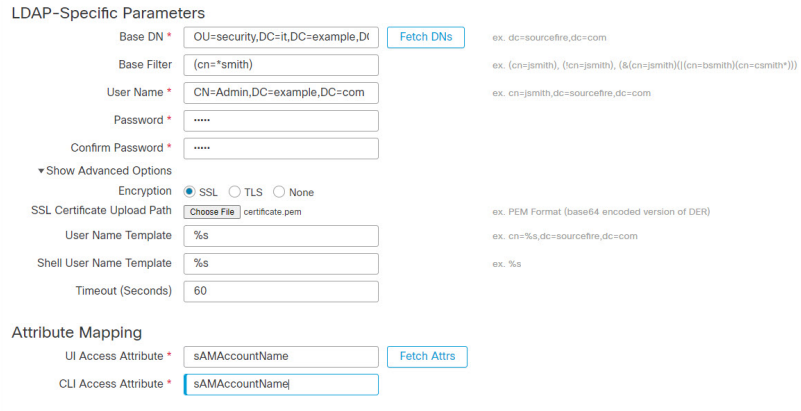
请注意，由于未对此服务器应用基本过滤器，因此系统会检查目录中基本可分辨名称所指示的所有对象的属性。经过默认时间段（或 LDAP 服务器上设置的超时期）后，与服务器的连接将超时。

高级示例

此示例说明 Microsoft Active Directory Server 的 LDAP 登录身份验证对象的高级配置。此示例中的 LDAP 服务器的 IP 地址为 10.11.3.4。此连接使用端口 636 进行访问。



此示例显示对于示例公司的信息技术领域中的安全组织使用基本可分辨名称 `OU=security,DC=it,DC=example,DC=com` 的连接。但请注意，此服务器具有基本过滤器 `(cn=*smith)`。该过滤器将从服务器检索到的用户限制为公用名称以 `smith` 结尾的用户。

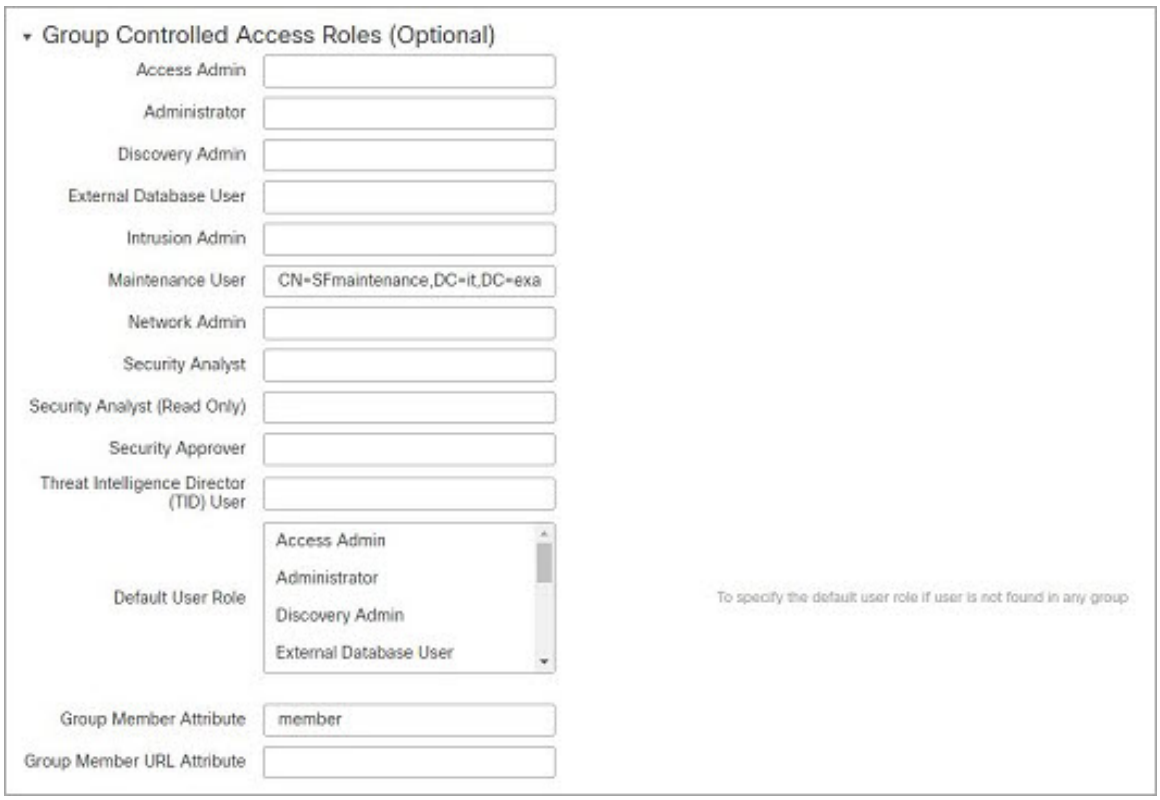


与服务器的连接使用 SSL 进行加密，并且会为该连接使用一个名为 `certificate.pem` 的证书。此外，由于**超时 (Timeout)** 设置，与服务器的连接在 60 秒后将超时。

由于此服务器是 Microsoft Active Directory 服务器，因此其使用 `sAMAccountName` 属性存储用户名而不是 `uid` 属性。请注意，配置包括 `sAMAccountName`的 **UI 访问属性 (UI Access Attribute)**。因此，当用户尝试登录系统时，系统会检查各对象的 `sAMAccountName` 属性以查找匹配的用户名。

此外，当用户登录到设备上的 CLI 账户中时， `sAMAccountName` 的 **CLI 访问属性** 会导致检查目录中所有对象的 `sAMAccountName` 属性以查找匹配项。

此示例还具有相应的组设置。“维护用户”角色将被自动分配给具有`成员`组属性且基本域名为 `CN=SFmaintenance,DC=it,DC=example,DC=com` 的组的所有成员。



CLI 访问过滤器 设置为与基本过滤器相同，因此相同用户可以通过 CLI 访问设备，如同通过 web 接口进行访问一样。

添加 CDO的 RADIUS 外部身份验证对象

添加 RADIUS 服务器以支持外部用户执行设备管理。

过程

步骤 1 选择系统（⚙）> 用户 **(Users)**。

步骤 2 点击**外部身份验证 (External Authentication)**。

步骤 3 点击**添加外部身份验证对象 (Add External Authentication Object)**。

步骤 4 将**身份验证方法**设置为 **RADIUS**。

步骤 5 输入**名称**和可选**说明**。

步骤 6 对于**主服务器**，输入**主机名/IP 地址**。

步骤 7 （可选） 更改**端口**使用的默认值。

步骤 8 输入 **RADIUS 服务器密钥**。

步骤 9 （可选） 输入**备份服务器**参数。

步骤 10 （可选） 输入 **RADIUS 特定参数**。

a) 在 **超时** 中输入重试主服务器之前允许的秒数（介于 1 和 1024 之间）。默认值为 30。

b) 输入滚动到备份服务器之前允许的**重试次数**。默认值为 3。

c) 在与用户角色对应的字段中，输入各用户的名称或确定应分配给这些角色的属性-值对。

将用户名和属性-值对以逗号分隔。

示例：

如果您知道所有本应为“安全分析师”的用户的 `User-Category` 属性值为 `Analyst`，则可以在**安全分析师**字段中输入 `User-Category=Analyst`，以将该角色授予这些用户。

示例：

要将“管理员”角色授予用户 `jsmith` 和 `jdoe`，请在**管理员**字段中输入 `jsmith, jdoe`。

示例：

要将“维护用户”角色授予 `User-Category` 值为 `Maintenance` 的所有用户，请在**维护用户**字段中输入 `User-Category=Maintenance`。

d) 对于不属于任何指定组的用户，请选择**默认用户角色**。

如果更改用户的角色，必须保存/部署更改的外部身份验证对象，并从**用户**屏幕中移除该用户。该用户下次登录时会自动被重新添加。

步骤 11 （可选） **定义自定义 RADIUS 属性**。

如果 RADIUS 服务器返回 `/etc/radiusclient/` 中 `dictionary` 文件内不包含的属性值，并且您计划使用这些属性来设置具有这些属性的用户的角色，则需要定义这些属性。可以通过查看 RADIUS 服务器上的用户配置文件来查找为用户返回的属性。

a) 输入**属性名称**。

定义属性时，请提供属性的名称，其中包含字母数字字符。请注意，属性名称中的单词应以破折号而不是空格进行分隔。

b) 以整数形式输入**属性 ID**。

属性 ID 应为整数且不应与 `etc/radiusclient/dictionary` 文件中的任何现有属性 ID 冲突。

c) 从下拉列表中选择**属性类型**。

还请指定属性的类型：字符串、IP 地址、整数或日期。

d) 点击**添加**以添加自定义属性。

在创建 RADIUS 身份验证对象时，系统会在设备上的 `/var/sf/userauth` 目录中创建该对象的新目录文件。添加的所有自定义属性都会添加到字典文件。

示例：

如果在含有思科路由器的网络上使用 RADIUS 服务器，则可能要使用 `Ascend-Assign-IP-Pool` 属性向从特定 IP 地址池登录的所有用户授予特定角色。`Ascend-Assign-IP-Pool` 是一个整数属性，用于定义允许用户登录的地址池，其中整数指示已分配的 IP 地址池的编号。

要声明自定义属性，请创建一个自定义属性，使其属性名称为 `Ascend-IP-Pool-Definition`，属性 ID 为 `218`，并且属性类型为 `integer`。

然后，可以在**安全分析（只读）(Security Analyst [Read Only])** 字段中输入 `Ascend-Assign-IP-Pool=2`，将只读安全分析师权限授予 `Ascend-IP-Pool-Definition` 属性值为 `2` 的所有用户。

步骤 12 （可选） 在 **CLI 访问过滤器** 区域**管理员 CLI 用户列表** 字段中，输入应具有外壳访问权限的用户名并以逗号分隔。

请确保这些用户名匹配 RADIUS 服务器上的用户名。名称必须是 Linux 有效的用户名：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

为防止对 CLI 访问进行 RADIUS 身份验证，请将此字段留空。

注释 具有配置层级访问权限的用户可以使用 CLI **expert** 命令访问 Linux 外壳程序。Linux 外壳用户可以获得 root 权限，带来安全风险。请确保限制具有 CLI 或 Linux 外壳访问的用户列表。

注释 删除与包括在外壳访问过滤器中的用户具有相同用户名的任何内部用户。对于 管理中心，唯一的内部 CLI 用户是 **管理员**，因此请勿同时创建 **管理员** 外部用户。

步骤 13 （可选） 点击 **测试** 以测试与 RADIUS 服务器的 管理中心 连接。

步骤 14 （可选） 此外，还可以输入**其他测试参数**来测试应可以执行身份验证的用户的用户凭证：输入**用户名**和**密码**，然后点击**测试**。

提示 如果测试用户的名称或密码键入不正确，即使服务器配置正确，测试也会失败。要验证服务器配置是否正确，请点击**测试**，而无需首先在**其他测试参数**字段中输入用户信息。如果成功，请提供要通过特定用户进行测试的用户名和密码。

示例：

要测试是否可以在 Example 公司检索到 `JSmith` 用户凭证，请输入 `JSmith` 和正确的密码。

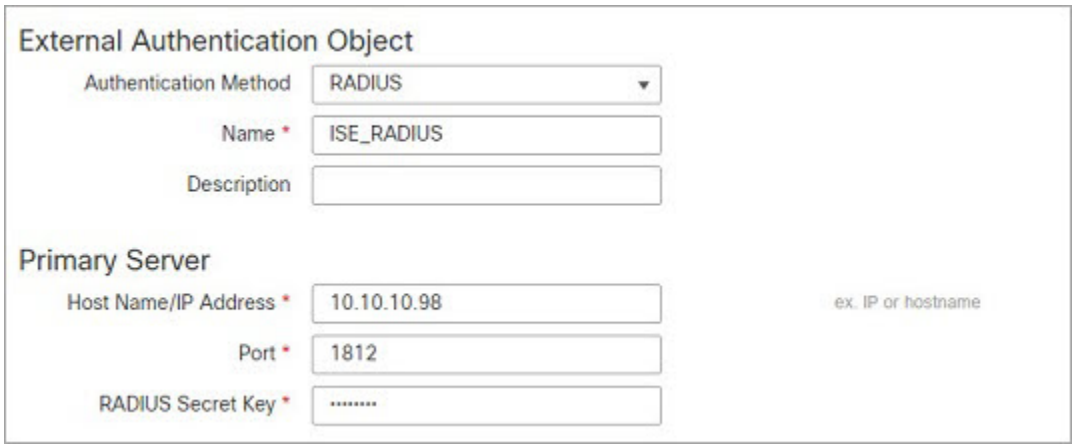
步骤 15 点击**保存 (Save)**。

步骤 16 启用此服务器。请参阅为 CDO上的用户启用外部身份验证 ，第 175 页。

示例

简单的用户角色指定

下图说明端口 1812 上 IP 地址为 10.10.10.98 的运行 Cisco Identity Services Engine (ISE) 的服务器的示例 RADIUS 登录身份验证对象。未定义备份服务器。



以下示例显示RADIUS特定参数，包括超时（30秒）和Firepower系统尝试联系备份服务器（如有）之前的失败重试次数。

此示例说明 RADIUS 用户角色配置的重要方面：

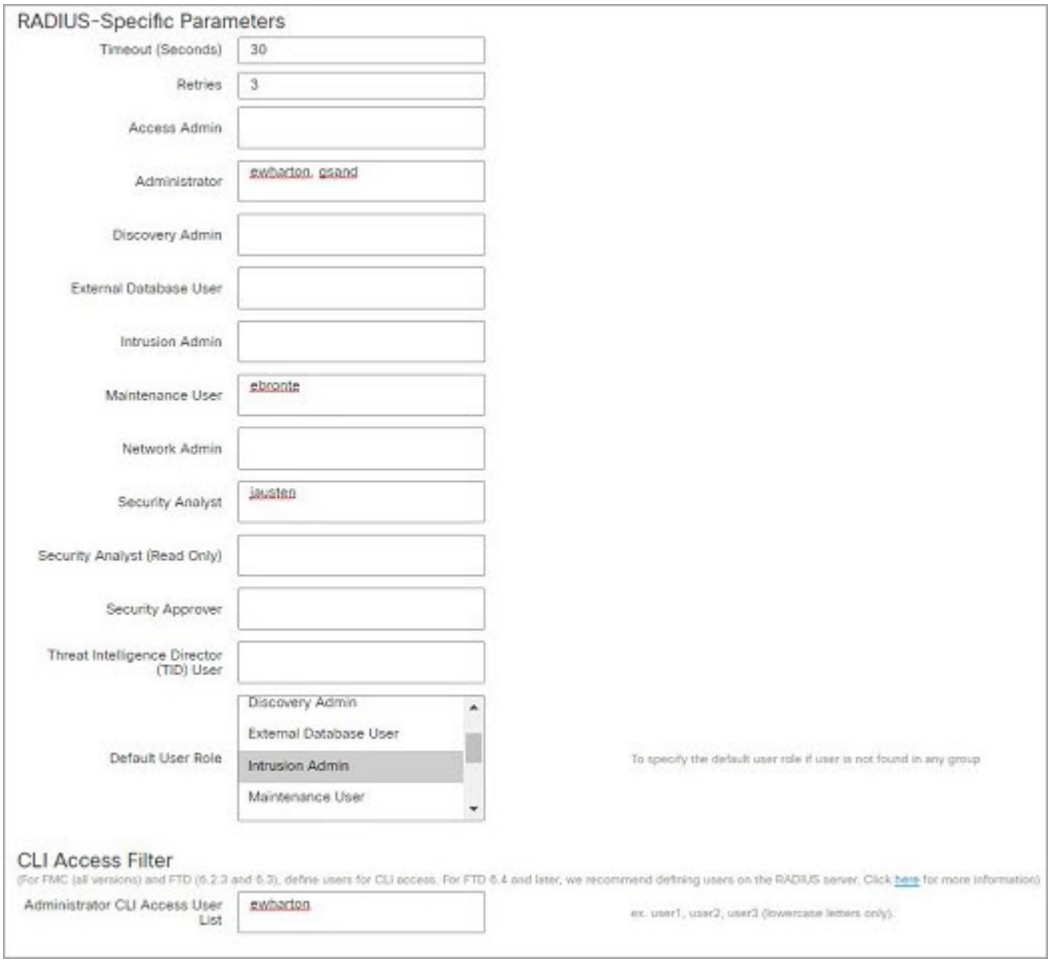
授予用户 `ewharton` 和 `gsand` Web 界面管理权限。

授予用户 `cbronte` Web 界面“维护用户”权限。

授予用户 `jausten` Web 界面“安全分析师”权限。

用户 `ewharton` 可以使用 CLI 帐户登录到设备中。

下图说明示例的角色配置：

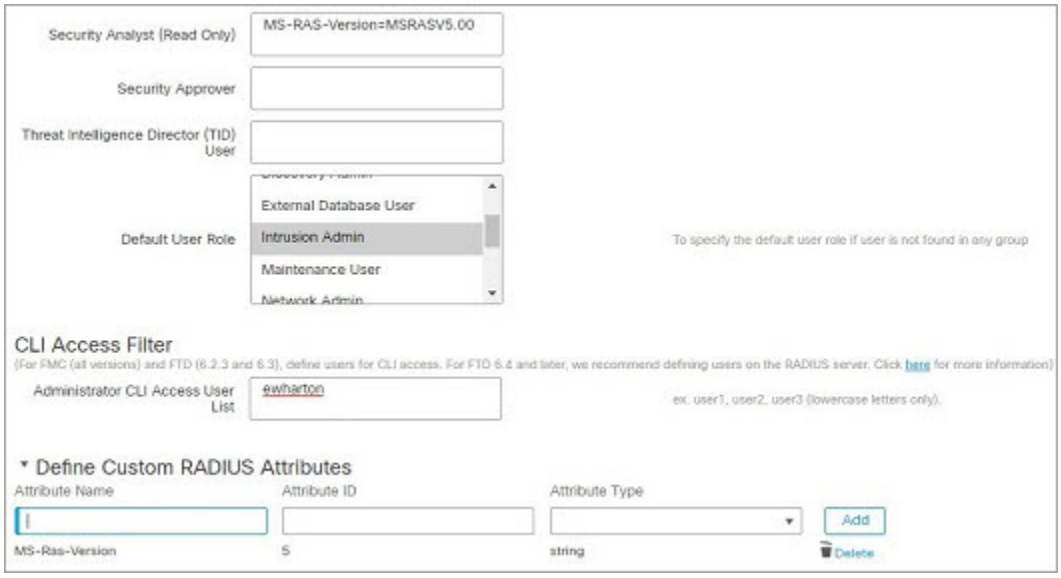


匹配属性-值对的用户角色

可以使用属性-值对识别应接收特定用户角色的用户。如果使用的属性是自定义属性，必须定义该自定义属性。

下图说明与前一示例中相同的 ISE 服务器的示例 RADIUS 登录身份验证对象中的角色配置和自定义属性定义。

但是，在此示例中，由于正在使用 Microsoft 远程访问服务器，因此为一个或多个用户返回了 `MS-RAS-Version` 自定义属性。请注意，`MS-RAS-Version` 自定义属性为字符串。在此示例中，通过 Microsoft v. 5.00 远程访问服务器登录 RADIUS 的所有用户都应得到“安全分析师（只读）”(Security Analyst [Read Only]) 角色，因此请在**安全分析师（只读）(Security Analyst [Read Only]** 字段中输入属性-值对 `MS-RAS-Version=MSRASV5.00`。



为 CDO上的用户启用外部身份验证

在为管理用户启用外部身份验证时，管理中心会使用外部身份验证对象中指定的 LDAP 或 RADIUS 服务器验证用户凭证。

开始之前

根据 添加 CDO的 LDAP 外部身份验证对象，第 164 页 和 添加 CDO的 RADIUS 外部身份验证对象，第 170 页中所述，添加一个或多个外部身份验证对象。

过程

步骤 1 选择**系统**（⚙）> **用户 (Users)**。

步骤 2 点击**外部身份验证 (External Authentication)**。

步骤 3 为外部 Web 界面用户设置默认用户角色。

没有角色的用户无法执行任何操作。外部身份验证对象中定义的任何用户角色将覆盖此默认用户角色。

a) 点击**默认用户角色**值（默认为未选定）。

a) 在**默认用户角色配置**对话框中，选中要使用的角色。

b) 点击**保存 (Save)**。

步骤 4 点击要使用的每个外部身份验证对象旁边的**滑块已启用**（🔵）。如果启用多个对象，系统会按指定顺序参照服务器比较用户。请参阅后续步骤对服务器重新排序。

如果启用外壳身份验证，则必须启用包括**CLI 访问过滤器 (CLI Access Filter)** 的外部身份验证对象。另外，CLI 访问用户只能参照其身份验证对象在列表中排在第一位的服务器进行身份验证。

步骤 5 （可选） 拖放服务器可更改出现身份验证请求时访问身份验证的顺序。

步骤 6 如果要允许外部用户执行 CLI 访问，请选择**外壳身份验证 (Shell Authentication)** > **已启用 (Enabled)**。

第一个外部身份验证对象名称显示在**已启用 (Enabled)** 选项旁边，提醒您只有第一个对象用于 CLI。

步骤 7 点击**保存并应用**。

LDAP 身份验证连接故障排除

如果创建 LDAP 身份验证对象，并且其无法成功连接到选择的服务器或无法检索所需的用户列表，则可以调整该对象中的设置。

如果在测试连接时该连接失败，请尝试以下建议对配置进行故障排除。

- 使用 Web 界面屏幕顶部和测试输出中显示的消息确定对象的哪些方面导致问题。
- 检查用于对象的用户名和密码是否有效：
  - 检查用户是否有权通过使用第三方 LDAP 浏览器连接到 LDAP 服务器来浏览至基本可分辨名称中指示的目录。
  - 检查用户名对于 LDAP 服务器的目录信息树是否唯一。
  - 如果在测试输出中显示 LDAP 绑定错误 49，则表明用户的用户绑定失败。请尝试通过第三方应用对服务器进行身份验证，以了解通过该连接进行的绑定是否也失败。
- 检查是否已正确识别服务器：
  - 检查服务器 IP 地址或主机名是否正确。
  - 检查是否有从本地设备到要连接的身份验证服务器的 TCP/IP 访问权限。
  - 检查对服务器的访问是否未被防火墙阻止，以及在对象中配置的端口是否已打开。
  - 如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与用于服务器的主机名匹配。
  - 如果是对 CLI 访问进行身份验证，请检查是否未对服务器连接使用 IPv6 地址。
  - 如果使用了服务器类型默认值，请检查是否具有正确的服务器类型，并再次点击**设置默认值 (Set Defaults)** 以重置默认值。
- 如果键入了基本可分辨名称，请点击**获取 DN (Fetch DNs)** 以检索服务器上的所有可用基本可分辨名称，然后从列表中选择名称。
- 如果使用的是任意过滤器、访问属性或高级设置，请检查各项是否有效且正确键入。
- 如果使用的是任意过滤器、访问属性或高级设置，请尝试移除各设置并测试没有此设置的对象。

- 如果使用的是基本过滤器或 CLI 访问过滤器，请确保用括号将过滤器括起来，并且使用的是有效的比较运算符（包括括号在内，最大450个字符）。
- 要测试受限更多的基本过滤器，请尝试将其设置为基本可分辨名称，以使用户仅检索该用户。
- 如果使用的是加密连接：
  - 检查证书中 LDAP 服务器的名称是否与用于连接的主机名匹配。
  - 检查是否未对加密服务器连接使用 IPv6 地址。
- 如果使用的是测试用户，请确保正确键入用户名和密码。
- 如果使用的是测试用户，请移除用户凭证并测试对象。
- 通过连接到 LDAP 服务器并使用以下语法测试使用的查询：

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

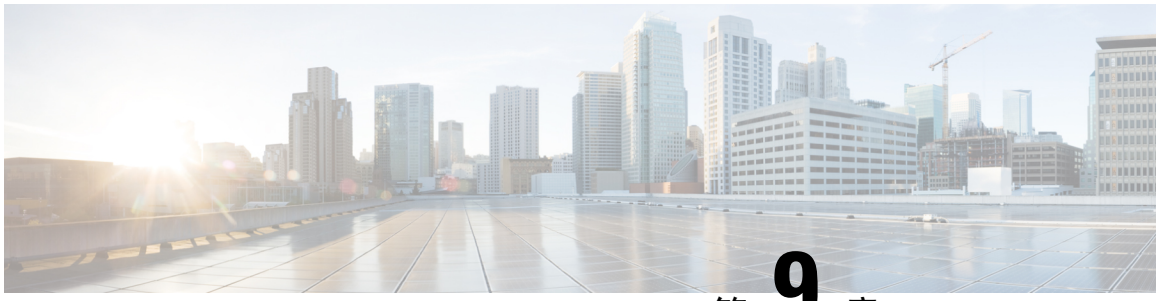
例如，如果是尝试使用 `domainadmin@myrtle.example.com` 用户和基本过滤器 (`cn=*`) 连接到 `myrtle.example.com` 上的安全域，则可以使用以下语句测试连接：

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

如果可以成功测试连接，但在部署平台设置策略后身份验证不起作用，请检查在应用到设备的平台设置策略中是否已启用要使用的身份验证和对象。

如果成功连接，但要调整连接检索到的用户列表，则可以添加或更改基本过滤器或CLI访问过滤器，或者使用限制较多或较少的基本 DN。

在对与 Active Directory (AD) 服务器的连接进行身份验证时，尽管与 AD 服务器的连接成功，但连接事件日志很少指示受阻 LDAP 流量。当 AD 服务器发送重复的重置数据包时，会出现此不正确的连接日志。威胁防御设备将第二个重置数据包识别为新连接请求的一部分，并使用“阻止”操作记录连接。



第 9 章

更新

以下主题介绍如何更新 Firepower 部署：

关于系统更新

您可以使用管理中心为自身及其管理的设备升级系统软件。您还可以更新提供高级服务的各种数据库和源。

对于可以访问互联网的 管理中心，系统通常可以直接从思科获取更新。我们建议您尽可能安排或启用自动更新。某些更新在初始设置过程中或在您启用相关功能时自动启用。您必须自行安排其他更新。完成初始设置后，我们建议您查看所有自动更新，并在必要时进行调整。

表 *16:* 升级和更新

组件	说明	详细信息
系统软件	主要 软件版本包含新功能、新功能和增强功能。它们可能包括基础设施或架构更改。 维护 版本包含常规漏洞和安全相关修复。行为更改很少见，并且与这些修复相关。 补丁 是按需更新，仅限于具有紧急性的关键修复程序。 热补丁 可以解决特定的客户问题。	**直接下载：** 仅选择版本，通常在版本可用于手动下载后的一段时间。延迟的长度取决于版本类型、版本采用情况和其他因素。 **计划：** 仅安装补丁，在 **系统**（⚙）> **工具** > **计划**。 **卸载：** 仅修补程序。 **恢复/重新映像：** 仅限主版本和维护版本。 **请参阅：** 升级系统软件， 第 181 页

组件	说明	详细信息
漏洞数据库 (VDB)	思科漏洞数据库 (VDB) 包含主机可能易受感染的已知漏洞，以及操作系统、客户端和应用指纹。系统借助 VDB 来确定某个特定主机是否会增加遭受危害的风险。	**直接下载：** 确认。 **计划：** 确认，在 **系统**（⚙）> **工具** > **计划**。 **卸载：** 否。 **请参阅：** 更新漏洞数据库 (VDB)，第 181 页
地理位置数据库 (GeoDB)	思科地理位置数据库 (GeoDB) 是一个与可路由的 IP 地址关联的地理数据数据库。	**直接下载：** 确认。 **计划：** 确认，在 **系统**（⚙）> **更新**。 **卸载：** 否。 **请参阅：** 更新地理定位数据库，第 183 页
入侵规则 (SRU/LSP)	入侵规则更新提供全新和更新的入侵规则及预处理器规则、现有规则的修改状态和修改的默认入侵策略设置。 另外，规则更新还可能删除规则，提供新规则类别和默认变量，并修改默认变量值。	**直接下载：** 确认。 **计划：** 确认，在 **系统**（⚙）> **更新**。 **卸载：** 否。 **请参阅：** 更新入侵规则，第 185 页
安全情报源	安全情报源是 IP 地址、域名和 URL 的集合，可用于快速过滤与条目匹配的流量。	**直接下载：** 确认。 **计划：** 确认，在 **对象** > **对象管理**。 **卸载：** 否。 **请参阅：** 《Cisco Secure Firewall Management Center 设备配置指南》
新 URL 类别和信誉	URL 过滤可以根据 URL 的一般分类（类别）和风险级别（信誉）控制对网站的访问。	**直接下载：** 确认。 **计划：** 是，在 **集成** > **其他集成** > **云服务** 或 **系统**（⚙）> **工具** > **计划**上，具体取决于您的要求。 **卸载：** 否。 **请参阅：** 《Cisco Secure Firewall Management Center 设备配置指南》

系统更新的要求和必备条件

型号支持

任意

支持的域

全局 除非另有说明。

用户角色

管理员

系统更新的准则和限制

在更新之前

在更新部署的任何组件（包括入侵规则、VDB或GeoDB）之前，请阅读更新随附的版本说明或建议性文本。这些内容提供版本特定的关键信息，包括兼容性、必备条件、新功能、行为更改和警告。

计划的更新

系统以UTC时间安排任务（包括更新）。这意味着它们在本地发生的时间取决于日期和您的特定位置。此外，由于更新是以UTC为单位进行计划的，因此它们不会针对夏令时、夏令时或您在地点可能观察到的任何季节性调整进行调整。如果受影响，则根据当地时间，计划的更新会在夏天比冬季中的一个小时开始。

重要事项 我们 强烈 建议您查看计划任务，确保计划的更新在您预期的时间执行。

带宽准则

要升级系统软件或执行就绪性检查，升级包必须位于设备上。升级包大小不同。请确保您的带宽足以将大量数据传输到您管理的设备。请参阅将数据从Firepower管理中心下载到受管设备的准则（故障排除技术说明）。

升级系统软件

本指南不包含系统软件或配套操作系统的详细升级说明。请参阅适用于您的版本的 《适用于管理中心的 Cisco 安全防火墙威胁防御升级指南》 。

有关安排下载和安装特定更新的信息，请参阅软件更新自动化，第 318 页。请注意，初始设置过程会自动安排每周下载一次。设置后，您应查看自动安排的配置，并在必要时对其进行调整。

更新漏洞数据库 (VDB)

思科漏洞数据库 (VDB) 包含主机可能易受感染的已知漏洞，以及操作系统、客户端和应用指纹。系统借助 VDB 来确定某个特定主机是否会增加遭受危害的风险。

思科定期发布 VDB 更新。在 管理中心上更新 VDB 及其关联映射所需的时间取决于网络映射中的主机数量。一般说来，将主机数除以 1000，即可估算出执行更新所需的大致时间（分钟）。

从 VDB 343 开始，所有应用检测器信息均可通过 Cisco Secure Firewall 应用检测器来获取。该站点包含一个可搜索的应用检测器数据库。版本说明提供了有关特定 VDB 版本的变更信息。

注释 作为一次性操作，管理中心上的初始设置会自动下载并安装思科提供的最新 VDB。或者，安排任务以下载和安装 VDB 更新以及部署配置。有关详细信息，请参阅漏洞数据库更新自动化，第 321 页。

手动更新 VDB

使用此程序手动更新 VDB。

注意 请勿执行与映射的漏洞相关的任务，直至更新完成。即使消息中心在几分钟内不显示进度或指示更新失败，也不要重启更新。相反，请联系思科 TAC。

在大多数情况下，VDB 更新后的第一次部署都会重新启动 Snort 进程，从而中断流量检查。系统会在发生这种情况时向您发出警告（更新的应用检测器和操作系统指纹需要重新启动；漏洞信息则不需要）。在此中断期间，流量是被丢弃还是不经进一步检查直接通过，将取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。

开始之前

如果您计划将 VDB 手动上传到 管理中心，请从 https://www.cisco.com/go/firepower-software 下载。

过程

步骤 1 选择 **系统**（⚙）> **更新**，然后点击**产品更新 (Product Updates)**。

步骤 2 获取 VDB 到 管理中心。您可以：

- 从思科直接下载：点击**下载更新 (Download Updates)** 按钮可立即为您的部署下载最新的 VDB、最新的维护版本和最新的关键补丁。
- 手动上传：点击**上传更新 (Upload Update)**，然后点击**选择文件 (Choose File)**。浏览到更新并点击**上传 (Upload)**。

步骤 3 安装 VDB。

a) 点击漏洞和指纹数据库更新旁的**安装**图标。
b) 选择 管理中心。
c) 点击**安装**。

在消息中心监控更新进度。在更新完成后，系统将使用新的漏洞信息。但您必须先进行部署，已更新的应用检测器和操作系统指纹才会生效。

步骤 4 验证更新是否成功。

选择 **帮助** （ ） > **关于** 以查看当前的 VDB 版本。

下一步做什么

部署配置更改。

安排 VDB 更新

如果 管理中心可以访问互联网，我们建议您安排定期更新 GeoDB。请参阅漏洞数据库更新自动化，第 321 页。

更新地理定位数据库

地理位置数据库 (GeoDB) 是可用于根据地理位置查看和过滤流量的数据库。

系统随附一个将 IP 地址映射到国家/地区/大洲的初始 GeoDB 国家/地区代码包，因此信息应始终可用。如果您更新 GeoDB，系统还会下载 包含 情景数据的 IP 数据包。此情景数据包括其他位置详细信息，以及连接信息，例如 ISP、连接类型、代理类型、域名等。我们还会定期更新 GeoDB，您必须定期更新 GeoDB 才能获得准确的地理位置信息。

作为初始配置的一部分， 系统配置每周的自动 GeoDB 更新。如果配置更新失败且 管理中心 可以访问互联网，我们建议您配置常规 GeoDB 更新，如 安排 GeoDB 更新，第 183 页。

更新 GeoDB 所需的时间取决于您的设备，但最多可能需要 45 分钟，具体取决于更新的大小（例如，如果这是您第一次下载完整的 GeoDB）。虽然 GeoDB 更新不会中断任何其他系统功能（包括正在进行的地理位置信息收集），但更新执行时的确会占用系统资源。制定更新计划时需要考虑这一点。

GeoDB 更新将会覆盖之前的所有 GeoDB 版本并立即生效。更新 GeoDB 时，管理中心会自动更新其受管设备上的相关数据。GeoDB 更新可能需要几分钟时间才能在整个部署中生效。更新后，无需重新部署。

系统（ ） > **更新** > **地理位置更新** 页面和 **帮助** （ ） > **关于** 页面均列出了当前版本。

安排 GeoDB 更新

作为初始配置的一部分， 系统配置每周的自动 GeoDB 更新。如果配置更新失败且 管理中心 可以访问互联网，我们建议您配置常规 GeoDB 更新，如 此程序。

开始之前

确保 管理中心可以访问互联网。

过程

步骤 1 选择系统（⚙）> 更新 > 地理位置更新。

步骤 2 在周期性地理位置更新下，选择 从支持站点启用周期性每周更新。

步骤 3 指定更新开始时间。

步骤 4 点击保存 (Save)。

手动更新 GeoDB（互联网连接）

如果 管理中心 可以访问互联网，请使用此程序对 GeoDB 执行按需更新。

过程

步骤 1 选择系统（⚙）> 更新 > 地理位置更新。

步骤 2 在一次性地理位置更新下，选择 从支持站点下载并安装地理位置更新。

步骤 3 点击导入。

您可以在消息中心监控更新的进度。

步骤 4 验证更新是否成功。

“地理位置更新”页面和 帮助 （?）> 关于 页面均列出当前版本。

手动更新 GeoDB（无互联网连接）

如果 管理中心 无法访问互联网，请使用此程序执行 GeoDB 的按需更新。

过程

步骤 1 从 思科支持和下载站点下载 GeoDB： https://www.cisco.com/go/firepower-software。

选择或搜索您的型号（或选择任何型号 - 对所有 管理中心型号使用相同的 GeoDB），然后浏览至 覆盖和内容更新 页面。

确保下载国家/地区代码和 IP 软件包。

步骤 2 选择系统（⚙）> 更新 > 地理位置更新。

步骤 3 在一次性地理位置更新下，选择 上传并安装地理位置更新。

步骤 4 点击 选择文件，然后浏览到您之前下载的 国家/地区代码 包。

步骤 5 点击导入。

您可以在消息中心监控更新的进度。

步骤 6 对 IP 包重复步骤 4 和 5。

步骤 7 验证更新是否成功。

“地理位置更新”页面和 **帮助** （ ） > **关于** 页面均列出当前版本。

更新入侵规则

随着新漏洞的暴露，Talos 情报小组 会发布可导入到 管理中心上的入侵规则更新，然后通过将已更改的配置部署到受管设备进行实施。这些更新会影响入侵规则、预处理器规则和使用这些规则的策略。

入侵规则更新是累加性的，并且思科建议始终导入最新的更新。不能导入与当前安装的规则的版本匹配或早于该版本的入侵规则更新。

入侵规则更新可能提供以下内容：

- **新的和修改的规则和规则状态** - 规则更新提供新的和更新的入侵和预处理器规则。对于新的规则，每个系统提供的入侵规则中的规则状态可能不同。例如，一个新规则在 Security over Connectivity 入侵策略中可能是启用状态，在 Connectivity over Security 入侵策略中则可能是禁用状态。规则更新也可以更改现有规则的默认状态，或者完全删除现有规则。
- **新规则类别** - 规则更新可能包括始终添加的新规则类别。
- **修改的预处理器和高级设置**规则更新可能更改系统提供的入侵策略中的高级设置，以及系统提供的网络分析策略中的预处理器设置。它们也可以更新访问控制策略中的高级预处理和性能选项的默认值。
- **新的和修改的变量** - 规则更新可能修改现有默认变量的默认值，但不会覆盖您的更改。始终会添加新变量。

在多域部署中，可以在任何域中导入本地入侵规则，但是，只能在全局域中从 Talos 导入入侵规则更新。

了解入侵规则更新何时修改策略

入侵规则更新可以影响系统提供的和自定义网络分析策略，以及所有访问控制策略：

- **系统提供** - 对系统提供的网络分析和入侵策略的更改以及对高级访问控制设置的任何更改将在您更新后重新部署策略时自动生效。
- **自定义** - 因为每个自定义网络分析和入侵策略都使用系统提供的策略作为其基础，或作为策略链中的事件基础，所以规则更新可以影响自定义网络分析和入侵策略。但是，您可以阻止规则更新自动执行这些更改。这使您能够在独立于规则更新导入的计划中手动更新系统提供的基本策略。无论您的选择（在每个自定义策略基础上实施）如何，更新系统提供的策略**都不会**覆盖您定制的任何设置。

请注意，导入规则更新会丢弃对网络分析和入侵策略所做的所有已缓存更改。为了方便起见，Rule Updates 页面列出了包含已缓存更改的策略以及做出这些更改的用户。

部署入侵规则更新

为使入侵规则更新所做的更改生效，必须重新部署配置。在导入规则更新时，可以将系统配置为自动重新部署到受影响设备。如果允许入侵规则更新修改系统提供的基本入侵策略，则此方法尤其有用。

周期性入侵规则更新

可以在 Rule Updates 页面上设置为按日、周或月导入规则更新。

如果部署包括管理中心的高可用性对，则仅在主防御中心上导入更新。辅助管理中心会在常规同步过程中接收规则更新。

入侵规则更新导入中的适用子任务按以下顺序出现：下载、安装、基本策略更新和策略部署。完成一个子任务后，才会开始下一个子任务。

在计划的时间，系统按照在先前步骤中所指定，安装规则更新并部署已更改的配置。在导入之前或导入过程中，可注销或使用 Web 界面执行其他任务。在导入过程中访问时，“规则更新日志”显示**红色状态**（  ），此外，您还可以在“规则更新日志”详细视图中查看消息。根据规则更新大小和内容，可能几分钟之后才会显示状态消息。

作为初始配置的一部分，系统配置每日从 思科支持和下载站点 为 Snort 2 设备自动更新入侵规则 (SRU)。如果配置更新失败且 管理中心 可以访问互联网，我们建议您配置定期入侵规则更新，如 计划入侵规则更新，第 188 页.

导入本地入侵规则

本地入侵规则是从本地计算机以采用 ASCII 或 UTF-8 编码的纯文本文件形式导入的自定义标准文本规则。可以使用 Snort 用户手册（可在 http://www.snort.org 上获取）中的说明创建本地规则。

在多域部署中，可以在任何域中导入本地入侵规则。可以查看在当前域和祖先域中导入的本地入侵规则。

一次性手动更新入侵规则

如果 管理中心无法访问互联网，则请手动导入新的入侵规则更新。

过程

步骤 1 从思科支持站点 (http://www.cisco.com/cisco/web/support/index.html) 手动下载更新。

步骤 2 选择 **系统**（⚙）> **更新**，然后点击 **规则更新**。

步骤 3 如果要将已创建或导入的所有用户定义的规则都移至已删除的文件夹，则必须点击工具栏中的**删除所有本地规则 (Delete All Local Rules)**，然后点击**确定 (OK)**。

步骤 4 选择**要上传并安装的规则更新或文本规则文件 (Rule Update or text rule file to upload and install)**，然后点击**浏览 (Browse)** 以浏览并选择规则更新文件。

步骤 5 如果要在更新完成后自动将策略重新部署到受管设备，请选择**在规则更新导入完成后重新应用所有策略 (Reapply all policies after the rule update import completes)**。

步骤 6 点击 **Import**。系统将安装规则更新并显示“规则更新日志”(Rule Update Log) 详细视图。

注释 如果在安装规则更新时出现错误消息，请联系支持部门。

一次性自动更新入侵规则

注释 此部分适用于 Snort 2。

要自动导入新的入侵规则更新，设备必须具有互联网访问权限以连接到支持站点。

开始之前

- 确保 管理中心能够访问互联网；请参阅安全、互联网接入和通信端口，第 2219 页。

过程

步骤 1 选择**系统**（⚙）> **更新**。

注释 也可以点击入侵规则编辑器页面（**对象** > **入侵规则**）上的**导入规则**。

步骤 2 点击 **规则更新**。

步骤 3 如果要将已创建或导入的所有用户定义的规则都移至已删除的文件夹，请点击工具栏中的**删除所有本地规则 (Delete All Local Rules)**，然后点击**确定 (OK)**。

步骤 4 选择**从支持站点下载新规则更新 (Download new Rule Update from the Support Site)**。

步骤 5 如果要在更新完成后自动将已更改的配置部署到受管设备，请选中**在规则更新导入完成后重新应用所有策略 (Reapply all policies after the rule update import completes)** 复选框。

步骤 6 点击 **Import**。
系统将安装规则更新并显示“规则更新日志”(Rule Update Log) 详细视图。

注意 如果在安装规则更新时出现错误消息，请联系支持部门。

计划入侵规则更新

注释　此部分适用于 Snort 2。

作为初始配置的一部分，系统配置每日从 思科支持和下载站点 为 Snort 2 设备自动更新入侵规则 (SRU)。如果配置更新失败且 管理中心 可以访问互联网，我们建议您配置定期入侵规则更新，如 此部分。

过程

步骤 1 选择**系统**（⚙）> **更新**。

注释　也可以点击入侵规则编辑器页面（**对象** > **入侵规则**）上的**导入规则**。

步骤 2 点击 **规则更新**。

步骤 3 如果要将已创建或导入的所有用户定义的规则都移至已删除的文件夹，请点击工具栏中的**删除所有本地规则 (Delete All Local Rules)**，然后点击**确定 (OK)**。

步骤 4 选中 **启用从支持网站重复规则更新导入** 复选框。

导入状态消息显示在 **Recurring Rule Update Imports** 部分下方。

步骤 5 在**导入频率 (Import Frequency)** 字段中，指定：

- 更新频率（**每天 [Daily]**、**每周 [Weekly]** 或**每月 [Monthly]**）
- 要发生更新的周日期或月日期
- 要开始更新的时间

步骤 6 如果要在更新完成后自动将已更改的配置重新部署到受管设备，请选中**在规则更新完成后将已部署的策略部署到目标设备 (Deploy updated policies to targeted devices after rule update completes)** 复选框。

步骤 7 点击**保存 (Save)**。

注意　如果在安装入侵规则更新时收到错误消息，请联系支持部门。

Recurring Rule Update Imports 部分下方的状态信息会发生变化，以指明尚未运行规则更新。

导入本地入侵规则最佳实践

导入本地规则文件时，请遵循以下准则：

- 规则导入程序要求以 ASCII 或 UTF-8 编码的纯文本文件导入所有自定义规则。

- 文本文件名称可包含字母数字字符和空格，不可包含除下划线 (_)、句号 (.) 和破折号 (-) 以外的其他特殊字符。
- 系统会导入以一个井号 (#) 开头的本地规则，但它们被标记为已删除。
- 系统会导入以一个井号 (#) 开头的本地规则，但不会导入以两个井号 (##) 开头的本地规则。
- 规则不能包含任何转义字符。
- 在多域部署中，系统将为导入到“全局”域或在该域中创建的规则分配一个为 1 的 GID，并为所有其他域分配一个特定于域的 GID，数值介于 1000 与 2000 之间。
- 导入本地规则时，不必指定生成器 ID (GID)。如果指定了生成器 ID，则请仅为标准文本规则指定 GID 1。
- 首次导入规则时，请勿指定 Snort ID (SID) 或修订版本号。这可避免与其他规则的 SID 发生冲突，包括已删除的规则。系统会自动为规则分配下一个可用的自定义规则 SID（1000000 或更高） 以及版本号 1。

  如果必须导入带有 SID 的规则，则 SID 可以是 1,000,000 或以上的任何唯一数字。

  在多域部署中，如果多个管理员同时导入本地规则，则单个域中的 SID 可能不连续，因为系统已将该序列的中间编号分配给其他域。
- 导入之前已导入的本地规则的更新版本时，或者重新安装已删除的本地规则时，必须包含由系统分配的 SID 以及高于当前编号的修订版本号。您可以通过编辑规则确定当前或已删除规则的修订版本号。

注释 删除本地规则时，系统会自动增加修订版本号；这样方便恢复本地规则。所有已删除的本地规则从会从本地规则类别转移到已删除规则类别。

- 请在高可用性对中的主 Firepower 管理中心上导入本地规则，以避免 SID 编号问题。
- 如果规则包含以下任意一项，则导入失败：
  - 大于 2147483647 的 SID。
  - 长度超过 64 个字符的源或目的端口列表。
  - 在多域部署中，在导入到“全局”域时，GID:SID 组合使用 GID 1 和一个已存在于其他域中的 SID；这表示该组合在版本 6.2.1 之前就已存在。可以使用 GID 1 和一个唯一的 SID 重新导入规则。
- 如果启用某个导入的本地规则，而该规则将弃用的 `threshold` 关键字与某个入侵策略中的入侵事件阈值功能结合起来使用，策略验证将会失败。
- 所有导入的本地规则都会自动保存在本地规则类别中。
- 系统始终将导入的本地规则设置为禁用状态。必须手动设置本地规则的状态后，才能将其用于入侵策略中。

导入本地入侵规则

- 请确保您的本地规则文件遵循导入本地入侵规则最佳实践，第 188 页中所述的准则，
- 并确保导入本地入侵规则的过程符合您的安全策略。
- 请考虑导入因带宽约束和Snort重启而带给流量和检测的影响。我们建议将规则更新安排在维护窗口执行。
- 您可以在任何域中执行此任务。

使用以下程序导入本地入侵规则。导入的入侵规则以被禁用的状态显示在本地规则类别中。

过程

步骤 1 选择 **系统**（⚙）> **更新**，然后点击 **规则更新**。

步骤 2 （可选）删除现有的本地规则。

点击**删除所有本地规则**，然后确认是否想要将创建和导入的所有入侵规则移至删除的文件夹。

步骤 3 在 **一次性规则更新/规则导入**下，选择 **规则更新或文本规则文件以上传和安装**，然后点击 **选择文件**并浏览到您的本地规则文件。

步骤 4 点击 **Import**。

步骤 5 可以在消息中心监控导入进度。

要显示消息中心，请点击菜单栏上的“系统状态”。即使在消息中心有几分钟时间不显示，或指示导入失败，也不要重启导入，而是联系思科 TAC。

下一步做什么

- 编辑入侵策略，并启用已导入的规则。
- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 部署配置更改

规则更新日志

管理中心会为导入的规则更新和本地规则文件生成记录。

每个记录都包含时间戳、导入文件的用户名称以及指明导入成功或失败的状态图标。可保留导入的所有规则更新和本地规则文件的列表，删除列表中的任何记录，以及访问有关所有导入的规则和规则更新组成部分的详细记录。

“规则更新导入日志”详细视图列出导入到规则更新或本地规则文件中的每个对象的详细记录。此外，还可以根据列出的记录创建仅包含符合特定需求的信息的自定义工作流程或报告。

入侵规则更新日志表

表 *17:* 入侵规则更新日志字段

字段	说明
摘要	导入文件的名称。如果导入失败，文件名称下方会显示有关导入失败原因的简要说明。
时间	导入开始的时间和日期。
用户 ID	触发导入的用户的用户名。
状态	导入有以下状态： • **成功图标**（） • 失败或进行中 **红色状态**（） 导入过程中，Rule Update Log 页面上会显示红色状态图标，表示导入失败或未完成；成功完成导入后，该红色状态图标会变为绿色状态图标。

提示 可以在入侵规则更新导入正在进行中时查看显示的导入详细信息。

查看入侵规则更新日志

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**系统**（）> **更新**。

提示 也可以点击入侵规则编辑器页面（**对象** > **入侵规则**）上的**导入规则**。

步骤 2 点击 **规则更新**。

步骤 3 点击 **Rule Update Log**。

步骤 4 此时您有两种选择：

- 查看 - 要查看规则更新或本地规则文件中导入的每个对象的详细信息，请点击要查看的文件旁边的 **视图**（）；请参阅 查看入侵规则更新导入日志的详细信息，第 193 页。
- 删除 - 要删除导入日志中的导入文件记录（包括文件中包含的所有对象的详细记录），请点击导入文件名旁边的 **删除**（）。

注释 删除日志中的文件并不会删除导入到导入文件中的任何对象，而只是删除导入日志记录。

入侵规则更新日志中的字段

提示 即使是通过在仅显示单个导入文件记录的“规则更新导入日志”(Rule Update Import Log) 详细视图中的工具栏上点击**搜索 (Search)** 发起搜索，也可以搜索整个规则更新导入日志数据库。确保将时间限制条件设置为包含所有搜索中要包含的对象。

表 *18:* 规则更新导入日志详细视图字段

字段	说明 (Description)
操作	指明对对象类型执行了以下其中一项操作： • `new`（对于规则而言，是指第一次把规则存储在此设备上） • `changed`（对于规则更新组成部分或规则而言，规则更新组成部分已被修改，或者规则的版本号更高且 GID 和 SID 相同） • `collision`（对于规则更新组成部分或规则而言，由于版本与设备上的现有组成部分或规则冲突，因此跳过导入） • `deleted`（对于规则而言，已从规则更新删除规则） • `enabled`（对于规则更新编辑而言，已在系统提供的默认策略中启用了预处理器、规则或其他功能） • `disabled`（对于规则而言，已在系统提供的默认策略中禁用规则） • `drop`（对于规则而言，已在系统提供的默认策略中将规则设置为“丢弃并生成事件”[Drop and Generate Events]） • `error`（对于规则更新或本地规则文件而言，导入失败） • `apply`（为导入启用了**在规则更新导入完成后重新应用所有策略 [Reapply all policies after the rule update import completes]** 选项）
默认操作	规则更新定义的默认操作。当导入对象类型是 `rule` 时，默认操作是 `Pass`、`Alert` 或 `Drop`。对于所有其他导入对象类型，没有默认操作。
详细信息	组成部分或规则独有的字符串。对于规则、GID、SID 以及已更改规则的上一个版本号，此字段显示为 `previously (GID:SID:Rev)`。对于未更改的规则，此字段为空白。
域	其入侵策略可使用更新规则的域。后代域中的入侵策略也可以使用该规则。此字段只存在于多域部署中。

字段	说明 (Description)
GID	规则的生成器 ID。例如，1（标准文本规则、全局域或旧 GID）或 3（共享对象规则）。
名称	导入对象的名称（对于规则，对应的是规则“消息”[Message] 字段；对于规则更新，对应的是组成部分名称）。
策略	对于导入的规则，此字段显示所有。这表示规则导入成功，并可在所有相应的默认入侵策略中启用。对于其他导入对象类型，此字段为空白。
版本	规则的版本号。
规则更新	规则更新文件名。
SID	规则的 SID。
时间	导入开始的时间和日期。
类型	导入对象的类型，可以是以下类型之一： • rule update component（已导入的组成部分，例如规则包或策略包） • rule（对于规则而言，是指新的或更新后的规则；请注意，在版本 5.0.1 中，此值替换为 update 值，后者已被弃用） • policy apply（为导入启用了**在规则更新导入完成后重新应用所有策略**选项）
计数	每条记录的计数 (1)。当表受限时，“计数”(Count) 字段显示在表视图中，而且在默认情况下，“规则更新日志”(Rule Update Log) 详细视图受限于规则更新记录。此字段不可搜索。

查看入侵规则更新导入日志的详细信息

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**系统**（⚙）> **更新**。

提示 也可以点击入侵规则编辑器页面（**对象** > **入侵规则**）上的**导入规则**。

步骤 2 点击 **规则更新**。

步骤 3 点击 **Rule Update Log**。

步骤 4 点击要查看的详细记录的文件的旁边的 **视图**（👁）。

步骤 5 可以采取以下任何操作：

- 书签 - 要将当前页面加入书签，请点击 **将此页面加入书签**。

- 编辑搜索 - 要打开使用当前单一限制预填充的搜索页面，请选择“搜索限制”旁边的 **编辑搜索** 或 **保存搜索** 。
- 管理书签 - 要导航至书签管理页面，请点击 **报告设计器**。
- 报告 - 要根据当前视图中的数据生成报告，请点击 **报告设计器**。
- 搜索 - 要搜索整个规则更新导入日志数据库以查找规则更新导入记录，请点击 **搜索**。
- 排序 - 要对当前工作流程页面上的记录进行排序和限制。
- 切换工作流程 - 要暂时使用其他工作流程，请点击 （**切换工作流程**）。

第 10 章

许可证

本章提供有关不同许可证类型、服务订用、许可要求等的深入信息。

注释 管理中心 支持智能许可证或传统 PAK（产品激活密钥）许可证作为其平台许可证。

关于许可证

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

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

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

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

智能软件管理器和账户

当购买一个或多个许可证时，您可在智能软件管理器中对其进行管理： https://software.cisco.com/#module/SmartLicensing。通过智能软件管理器，您可以为组织创建一个主账户。如果您还没有账户，请点击此链接以设置新账户。通过智能软件管理器，您可以为组织创建一个主帐户。

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

您可以通过虚拟账户管理许可证。只有该虚拟账户的设备可以使用分配给该账户的许可证。如果您需要其他许可证，则可以从另一个虚拟账户传输未使用的许可证。您还可以在虚拟账户之间迁移设备。

管理中心和设备的许可工作原理

管理中心 向智能软件管理器注册，然后为每个受管设备分配许可证。设备不直接向智能软件管理器注册。

物理 管理中心 本身不需要许可证。

与智能软件管理器的定期通信

为维护产品许可证授权，您的产品必须与智能软件管理器定期通信。

您可以使用产品实例注册令牌通过思科智能软件管理器注册 管理中心 。智能软件管理器会为 管理中心 和智能软件管理器之间的通信颁发 ID 证书。此证书有效期为 1 年，但需要每 6 个月续签一次。如果 ID 证书到期（一年后没有通信）， 管理中心 可能会从您的账户中删除。

管理中心 定期与智能软件管理器通信。如果您在智能软件管理器中进行更改，则可以刷新 管理中心 上的授权，以使更改立即生效。另外，也可以等待 管理中心 按计划通信。

您的 管理中心 必须具有对智能软件管理器的直接互联网访问权限。在 non-airgapped 部署中，常规许可证通信每 30 天进行一次，但如果具有宽限期，则 管理中心 会最多运行 90 天，而不会联系智能软件管理器。确保 管理中心 在 90 天内联系智能软件管理器，，否则 管理中心 将恢复为未注册状态。

评估模式

在 管理中心 向智能软件管理器注册之前，它会在评估模式下运行 90 天。您可以将功能许可证分配给受管设备，它们将在评估模式的持续时间内保持合规。此时间段结束后， 管理中心 将取消注册。

如果您向智能软件管理器注册 管理中心 ，则评估模式将结束。如果您稍后取消注册 管理中心，则无法恢复评估模式，即使最初没有使用所有 90 天。

有关未注册状态的详细信息，请参阅已注销状态 ， 第 197 页。

注释 您不能接收评估许可证进行强加密 (3DES/AES)；您必须向智能软件管理器注册，以接收可启用强加密 (3DES/AES) 许可证的导出合规性令牌。

不合规状态

管理中心 在以下情况下可能会处于不合规状态：

- 许可证到期 - 当托管设备基于时间的许可证到期时。

在不合规状态下，请参阅以下影响：

- 所有 托管设备许可证 - 操作不受影响。

在您解决许可问题后，管理中心将显示它现在符合智能软件管理器的定期计划授权。要强制授权，请点击 **系统**（⚙）> **许可证** > **智能许可证** 页面上的 **重新授权** 。

已注销状态

在以下情况下， 管理中心 可能会取消注册：

- 评估模式到期-评估模式在 90 天后到期。
- 手动注销 管理中心
- 与智能软件管理器缺少通信- 管理中心 在 1 年内不与智能软件管理器通信。注意：90 天后， 管理中心授权将到期，但可以在一年内成功恢复通信，以自动重新授权。一年后，ID 证书到期，将从您的账户中删除 管理中心 ，因此您必须手动重新注册 管理中心。

在未注册状态下， 管理中心 无法将任何配置更改部署到 需要许可证的功能的设备。

最终用户许可证协议

http://www.cisco.com/go/softwareterms 提供了用于监管您使用此产品的思科最终用户许可证协议 (EULA) 和所有适用补充协议 (SEULA)。

许可证类型和限制

本节介绍可用的许可证类型。

表 *19:* 智能许可证

您分配的许可证	您购买的订用	持续时间	授予的功能
基本	基于许可证类型	永久或订用 注释 基本 订用许可证仅在 Threat Defense Virtual上受支持。	除特定许可证预留和安全防火墙 3100、 基本 永久许可证会自动分配给所有 威胁防御。 用户和应用控制 交换和路由 NAT 有关详细信息，请参阅基本许可证， 第 199 页。
威胁	• T • TC (威胁 + URL) • TMC（ 威胁+恶意软件 防御 + URL）	订用	入侵检测和预防 文件控制 安全情报过滤 有关详细信息，请参阅 威胁许可证， 第 200 页
恶意软件 防御	• TM (威胁 + 恶意软件 防御) • TMC（ 威胁+恶意软件 防御 + URL） • AMP	订用	恶意软件 防御 Secure Secure Malware Analytics 文件存储 有关详细信息，请参阅中的文件和恶意软件策略的许可证要求。恶意软件 防御 许可证， 第 200 页《Cisco Secure Firewall Management Center 设备配置指南》
URL 过滤	• TC (威胁 + URL) • TMC（ 威胁+恶意软件 防御 + URL） • URL	订用	基于类别和信誉的 URL 过滤 有关详细信息，请参阅URL过滤许可证， 第 201 页。
出口管制功能	无需订用	永久	受国家安全、外交政策和反恐怖主义法律和法规约束的功能；请参阅出口控制功能的许可， 第 202 页。

您分配的许可证	您购买的订用	持续时间	授予的功能
远程接入 VPN： • AnyConnect Apex • AnyConnect Plus • 仅限 AnyConnect VPN	基于许可证类型	订用或永久	远程接入 VPN 配置。您的账户必须允许出口控制功能，以便配置远程访问 VPN。在注册设备时，您需要选择是否满足出口要求。 威胁防御 可以使用任何有效 AnyConnect 客户端 许可证。可用功能不因许可证类型不同而不同。 有关详细信息，请参阅 AnyConnect 客户端许可证，第 201 页 和 《Cisco Secure Firewall Management Center 设备配置指南》中的 *VPN* 许可 。

注释 订用许可证是基于期限的许可证。

基本许可证

基本 许可证允许您：

- 配置您的设备以执行交换和路由（包括 DHCP 中继和 NAT）
- 将设备配置为高可用性对
- 配置集群
- 通过将用户和应用条件添加到访问控制规则实施用户和应用控制
- 更新思科漏洞数据库 (VDB) 和地理位置数据库 (GeoDB)。
- 下载入侵规则，例如 SRU/LSP。但是，除非已启用 威胁 许可证，否则无法将具有入侵策略的访问控制策略或规则部署到设备。

Secure Firewall 3100

您在购买安全防火墙 3100 时获得 基本 许可证。

其他型号

除使用特定许可证预留的部署外，对于已注册到 管理中心的每个账户， 基本 许可证会自动添加到您的账户。对于特定许可证预留，您需要将 基本 许可证添加到您的帐户。

恶意软件 防御 许可证

通过恶意软件 防御 许可证，您可以执行 恶意软件防护 和 Secure Secure Malware Analytics。通过此功能，您可以使用设备检测并阻止通过网络传输的文件中的恶意软件。要支持此功能许可证，您可以购买恶意软件 防御 (AMP) 服务订阅作为独立订阅，或与 威胁 (TM) 或 威胁 和 URL 过滤 (TMC) 订用相结合。

注释 已启用恶意软件防御许可证的受管设备会定期尝试连接到安全恶意软件分析云，即使尚未配置动态分析也如此。因此，设备的接口流量控制面板构件显示传输的流量；这是预期行为。

配置恶意软件防护作为文件策略的一部分，然后与一个或多个访问控制规则相关联。文件策略可以检测到用户通过特定应用协议上传或下载特定类型文件。恶意软件防护 支持使用本地恶意软件分析和文件预分类来检查一组受限的恶意软件文件类型。您也可以将特定文件类型下载并提交到 Secure Secure Malware Analytics 云进行动态和 Spero 分析，从而确定文件是否包含恶意软件。对于这些文件，您可以查看网络文件轨迹，其中详述文件通过网络所采用的路径。恶意软件许可证还可用于将特定文件添加至文件列表，并在文件策略中启用文件列表，从而在检测时自动允许或拦截这些文件。

请注意，仅在部署 恶意软件防护 和 Secure Secure Malware Analytics时，才需要恶意软件 防御 许可证。恶意软件 防御 许可证，则 管理中心 可以从安全恶意软件分析云接收 Cisco Secure EndpointSecure Endpoint 恶意软件事件和危害表现 (IOC)。

另请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 文件和恶意软件策略的许可证要求 中的重要信息。

禁用此许可证时：

- 系统会停止查询安全恶意软件分析云，并且还会停止确认从安全恶意软件分析云发送的追溯性事件。
- 如果现有访问控制策略包含恶意软件防护 配置，则无法对其重新部署。
- 请注意，在禁用恶意软件防御 许可证后的很短时间内，系统可以使用现有缓存文件处置情况。在时间窗口到期后，系统会向这些文件分配处置情况 `Unavailable`。

威胁许可证

威胁 许可证可用于执行入侵检测和阻止、文件控制和安全情报过滤：

- 入侵检测和防御可用于分析网络流量是否存在入侵和漏洞利用，或者丢弃攻击性数据包。
- 文件控制 可用于检测和/或阻止用户通过特定应用协议上传（发送）或下载（接收）特定类型的文件。 恶意软件防护需要恶意软件 防御 许可证， 可用于基于某组受限文件类型的处置情况对其进行检查和阻止。
- 安全情报过滤 ，允许您在流量接受访问控制规则的分析之前，拒绝发送到特定 IP 地址、URL 和DNS域名或从其发送的流量，即，将其阻止。动态源可用于根据最新情报立即阻止连接。或者，可将“仅监控”设置用于安全情报过滤。

您可以购买 威胁 许可证作为独立订用 (T) 或与 URL 过滤 (TC)、恶意软件 防御 (TM) 或二者的组合 (TMC)。

禁用此许可证时：

- 管理中心 会停止从受影响设备确认入侵和文件事件。因此，使用这些事件作为触发器条件的关联规则停止开启。
- 管理中心 将不会连接互联网获取思科提供的信息或第三方安全情报信息。
- 在重新启用 威胁之前，您无法重新部署现有入侵策略。

URL 过滤许可证

URL 过滤许可证可用于编写访问控制规则，该规则可根据受监控主机请求的 URL 确定可横越网络且与那些 URL 的相关信息关联的流量。要支持此功能许可证，您可以购买 URL 过滤 服务订用作为独立订用，或与 威胁 (TC) 或威胁和恶意软件防御 (TMC) 订用相结合。

提示 如果没有 URL 过滤许可证，则可以指定要允许或阻止的单个 URL 或 URL 组。这个选项将对网络流量进行精细和自定义控制，但是，不允许使用 URL 类别和信誉数据来过滤网络流量。

虽然您无需 URL 过滤许可证即可将基于类别和信誉的 URL 条件添加到访问控制规则，但 管理中心 将不会下载 URL 信息。只有先将 URL 过滤许可证添加到 管理中心，然后在该策略针对的设备上进行启用，才能部署访问控制策略。

禁用此许可证时：

- 您可能会失去对 URL 过滤的访问权限。
- 具有 URL 条件的访问控制规则会立即停止过滤 URL。
- 您的 管理中心 不再可供下载 URL 数据更新。
- 如果现有访问控制策略包括的规则带有基于类别和信誉的URL条件，则不能重新部署现有的访问控制策略。

AnyConnect 客户端许可证

您可以使用 AnyConnect 客户端 和基于标准的 IPSec / IKEv2 配置远程访问 VPN。

要启用远程访问 VPN 功能，必须购买并启用以下许可证之一： AnyConnect Plus、 AnyConnect Apex 或 仅限 AnyConnect VPN。如果你有 AnyConnect Plus 和 AnyConnect Apex ，并想同时使用这两个许可证，则可以两个都选择。 仅限 AnyConnect VPN许可证不能与 **Apex** 或 **Plus**一起使用。 AnyConnect 客户端 许可证必须与智能帐户共享。有关更多说明，请参阅http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf。

如果指定的设备不具有至少其中一个指定的 AnyConnect 客户端 许可证类型的权利，则无法将远程访问VPN配置部署到设备。如果注册的许可证不符合规定或权利到期，系统将显示授权警报和运行状况事件。

使用远程访问 VPN 时，您的智能帐户必须已启用导出控制功能（强加密）。威胁防御需要强加密（高于 DES），才能与 AnyConnect 客户端 客户端成功建立远程接入 VPN 连接。

如果以下情况属实，则无法部署远程访问 VPN：

- 管理中心上的智能许可在评估模式下运行。
- 您的智能帐户未配置为使用导出控制功能（强加密）。

出口控制功能的许可

需要出口控制功能的功能

某些软件功能受国家安全、外交政策和反恐怖主义法律和法规约束。这些出口控制功能包括：

- 安全认证合规性
- 远程接入 VPN
- 具有强加密的站点间 VPN
- 具有强加密的 SSH 平台策略
- 具有强加密的 SSL 策略
- 具有强加密的功能，例如 SNMPv3

如何确定系统当前是否启用了出口控制功能

要确定系统当前是否启用了出口控制功能：请转至**系统 > 许可证 > 智能许可证**，查看**出口控制功能**是否显示为**启用**。

关于启用出口控制功能

如果 **出口控制功能** 显示 **禁用**，而您想要使用需要强加密的功能，有两种方式。您的组织可能有资格使用其中一种方法（或者二者皆不可使用），但不可同时使用这两种方法。

- 在智能软件管理器中生成新的产品实例注册令牌时，如果 没有 启用出口控制功能的选项：
- 如果在智能软件管理器中生成新的产品实例注册令牌时，显示选项“在使用此令牌注册的产品上允许导出控制功能”，请确保在生成令牌之前选中该选项。

  如果未为用于注册 管理中心的产品实例注册令牌启用导出控制功能，则必须使用启用了导出控制功能的新产品实例注册令牌取消注册，然后重新注册 管理中心 。

如果在评估模式下或在上 管理中心 启用强加密之前将设备注册到 管理中心，请重新启动每台受管设备以提供强加密。在高可用性部署中，主用和备用设备必须同时重启以避免出现主主状态。

授权永久有效，无需订用。

更多信息

有关出口控制的一般信息，请参阅https://www.cisco.com/c/en/us/about/legal/global-export-trade.html。

Threat Defense Virtual许可证

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

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

Threat Defense Virtual 智能许可的性能级别

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

表 *20:* 基于授权的 ***Threat Defense Virtual*** 许可功能限制

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

FTDv 性能级许可准则和限制

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

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

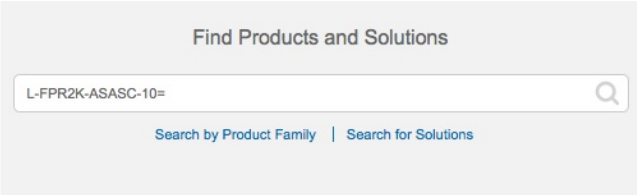
注释 确保智能许可账户包含所需的可用许可证。选择与您账户中的许可证相匹配的级别很重要。如果要将 threat defense virtual 升级到 7.0 版，可以选择 **FTDv - 变量**来保持当前的许可证合规性。threat defense virtual 会根据您的设备功能（内核数/RAM）继续执行会话限制。

- 部署新 threat defense virtual 设备或使用 REST API 调配 threat defense virtual 时，默认性能级别为 FTDv50。
- 基本许可证以订用为基础，并映射到性能级别。您的虚拟帐户需要具有 threat defense virtual 设备的 基本 许可证授权，以及 威胁、恶意软件和 URL 过滤 许可证的授权。
- 每个 HA 对等体使用一个授权，并且每个 HA 对等体上的授权必须匹配，包括基本许可证。
- 高可用性对的性能级别更改应应用于主对等体。
- 您可以将功能许可证分配到整个集群，而不是单个节点。但是，对于每个功能，集群中的每个节点都会使用一个单独的许可证。集群功能本身不需要任何许可证。
- 通用 PLR 许可单独应用于高可用性对中的每台设备。辅助设备不会自动镜像主设备的性能级别，而是必须手动更新。

许可证 PID

当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。但是，如果您需要自己添加许可证，则请使用Cisco Commerce Workspace上的 **Find Products and Solutions** 搜索字段。搜索以下许可证产品 ID (PID)。

图 *37:* 许可证搜索



Threat Defense Virtual PID

订购 FTDV-SEC-SUB 时，必须选择 基本 许可证和可选功能许可证（12 个月期限）：

- 基本许可证：
  - FTD-V-5S-BSE-K9
  - FTD-V-10S-BSE-K9
  - FTD-V-20S-BSE-K9
  - FTD-V-30S-BSE-K9
  - FTD-V-50S-BSE-K9
  - FTD-V-100S-BSE-K9
- 威胁、恶意软件防御和 URL 许可证组合：
  - FTD-V-5S-TMC
  - FTD-V-10S-TMC

- FTD-V-20S-TMC
- FTD-V-30S-TMC
- FTD-V-50S-TMC
- FTD-V-100S-TMC

- RA VPN - 请参阅 Cisco Secure 客户端订购指南。

Firepower 1010 PID

- 威胁、恶意软件防御和 URL 许可证组合：
  - L-FPR1010T-TMC=

  当您将上述 PID 添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- RA VPN - 请参阅 Cisco Secure 客户端订购指南。

Firepower 1100 PID

- 威胁、恶意软件防御和 URL 许可证组合：
  - L-FPR1120T-TMC=
  - L-FPR1140T-TMC=
  - L-FPR1150T-TMC=

  当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：
  - L-FPR1120T-TMC-1Y
  - L-FPR1120T-TMC-3Y
  - L-FPR1120T-TMC-5Y
  - L-FPR1140T-TMC-1Y
  - L-FPR1140T-TMC-3Y
  - L-FPR1140T-TMC-5Y
  - L-FPR1150T-TMC-1Y
  - L-FPR1150T-TMC-3Y
  - L-FPR1150T-TMC-5Y

- RA VPN - 请参阅 Cisco Secure 客户端订购指南。

Firepower 2100 PID

- 威胁、恶意软件防御和 URL 许可证组合：
  - L-FPR2110T-TMC=
  - L-FPR2120T-TMC=
  - L-FPR2130T-TMC=
  - L-FPR2140T-TMC=

  当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：
  - L-FPR2110T-TMC-1Y
  - L-FPR2110T-TMC-3Y
  - L-FPR2110T-TMC-5Y
  - L-FPR2120T-TMC-1Y
  - L-FPR2120T-TMC-3Y
  - L-FPR2120T-TMC-5Y
  - L-FPR2130T-TMC-1Y
  - L-FPR2130T-TMC-3Y
  - L-FPR2130T-TMC-5Y
  - L-FPR2140T-TMC-1Y
  - L-FPR2140T-TMC-3Y
  - L-FPR2140T-TMC-5Y
- RA VPN - 请参阅 Cisco Secure 客户端订购指南。

安全防火墙 3100 PID

- 基本许可证：
  - L-FPR3110-BSE=
  - L-FPR3120-BSE=
  - L-FPR3130-BSE=
  - L-FPR3140-BSE=
- 威胁、恶意软件防御和 URL 许可证组合：

- L-FPR3110T-TMC =
- L-FPR3120T-TMC =
- L-FPR3130T-TMC =
- L-FPR3140T-TMC =

当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：

- L-FPR3110T-TMC-1Y
- L-FPR3110T-TMC-3Y
- L-FPR3110T-TMC-5Y
- L-FPR3120T-TMC-1Y
- L-FPR3120T-TMC-3Y
- L-FPR3120T-TMC-5Y
- L-FPR3130T-TMC-1Y
- L-FPR3130T-TMC-3Y
- L-FPR3130T-TMC-5Y
- L-FPR3140T-TMC-1Y
- L-FPR3140T-TMC-3Y
- L-FPR3140T-TMC-5Y

- RA VPN - 请参阅 Cisco Secure 客户端订购指南。

Firepower 4100 PID

- 威胁、恶意软件防御和 URL 许可证组合：
  - L-FPR4110T-TMC=
  - L-FPR4112T-TMC=
  - L-FPR4115T-TMC=
  - L-FPR4120T-TMC=
  - L-FPR4125T-TMC=
  - L-FPR4140T-TMC=
  - L-FPR4145T-TMC=
  - L-FPR4150T-TMC=

当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：

- L-FPR4110T-TMC-1Y
- L-FPR4110T-TMC-3Y
- L-FPR4110T-TMC-5Y
- L-FPR4112T-TMC-1Y
- L-FPR4112T-TMC-3Y
- L-FPR4112T-TMC-5Y
- L-FPR4115T-TMC-1Y
- L-FPR4115T-TMC-3Y
- L-FPR4115T-TMC-5Y
- L-FPR4120T-TMC-1Y
- L-FPR4120T-TMC-3Y
- L-FPR4120T-TMC-5Y
- L-FPR4125T-TMC-1Y
- L-FPR4125T-TMC-3Y
- L-FPR4125T-TMC-5Y
- L-FPR4140T-TMC-1Y
- L-FPR4140T-TMC-3Y
- L-FPR4140T-TMC-5Y
- L-FPR4145T-TMC-1Y
- L-FPR4145T-TMC-3Y
- L-FPR4145T-TMC-5Y
- L-FPR4150T-TMC-1Y
- L-FPR4150T-TMC-3Y
- L-FPR4150T-TMC-5Y

- RA VPN - 请参阅 Cisco Secure 客户端订购指南。

Firepower 9300 PID

- 威胁、恶意软件防御和 URL 许可证组合：
  - L-FPR9K-24T-TMC=

- L-FPR9K-36T-TMC=
- L-FPR9K-40T-TMC=
- L-FPR9K-44T-TMC=
- L-FPR9K-48T-TMC=
- L-FPR9K-56T-TMC=

当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：

- L-FPR9K-24T-TMC-1Y
- L-FPR9K-24T-TMC-3Y
- L-FPR9K-24T-TMC-5Y
- L-FPR9K-36T-TMC-1Y
- L-FPR9K-36T-TMC-3Y
- L-FPR9K-36T-TMC-5Y
- L-FPR9K-40T-TMC-1Y
- L-FPR9K-40T-TMC-3Y
- L-FPR9K-40T-TMC-5Y
- L-FPR9K-44T-TMC-1Y
- L-FPR9K-44T-TMC-3Y
- L-FPR9K-44T-TMC-5Y
- L-FPR9K-48T-TMC-1Y
- L-FPR9K-48T-TMC-3Y
- L-FPR9K-48T-TMC-5Y
- L-FPR9K-56T-TMC-1Y
- L-FPR9K-56T-TMC-3Y
- L-FPR9K-56T-TMC-5Y

- RA VPN - 请参阅思科 AnyConnect 订购指南。

ISA 3000 PID

- 威胁、恶意软件防御和 URL 许可证组合：
  - L-ISA3000T-TMC=

当您将上述 PID 添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：

- L-ISA3000T-TMC-1Y
- L-ISA3000T-TMC-3Y
- L-ISA3000T-TMC-5Y

- RA VPN - 请参阅思科 AnyConnect 订购指南。

许可的要求和必备条件

一般前提条件

- 确保在 管理中心 和托管设备上配置了 NTP。时间必须同步才能成功注册。

  对于 Firepower 4100/9300，必须使用与 管理中心相同的机箱 NTP 服务器在机箱上配置 NTP。

支持的域

全局，除非另有说明。

用户角色

- 管理员

高可用性、集群和多实例许可的要求和必备条件

本节介绍 设备高可用性的许可要求。

FTD 服务不支持集群或多实例部署。

设备高可用性许可

高可用性配置中的两台 威胁防御 设备必须具有相同的许可证。

高可用性配置需要两种许可证权利；对中的每个设备各一个。

在建立高可用性之前，将哪些许可证分配给辅助/备用设备并不重要。进行高可用性配置期间，管理中心 会释放分配给备用设备的所有不必要的许可证，并用分配给主/主用设备的相同许可证替换它们。例如，如果主用设备具有 基本 许可证和 威胁 许可证，而备用设备只有 基本 许可证， 管理中心 将与智能软件管理器通信，以从您的备用设备的账户获取可用 威胁 许可证。如果您的许可证帐户不包含足够的购买权利，则您的帐户将在您购买正确数量的许可证之前变得不符合要求。

设备集群许可

每个 threat defense virtual 集群节点都需要相同的性能层许可证。我们建议为所有成员使用相同数量的CPU和内存，否则将限制所有节点上的性能，以匹配功能最低的成员。吞吐量级别将从控制节点复制到每个数据节点，以便它们匹配。

您可以将功能许可证分配到整个集群，而不是单个节点。但是，对于每个功能，集群中的每个节点都会使用一个单独的许可证。集群功能本身不需要任何许可证。

在将控制节点添加到 管理中心时，您可以指定要用于该集群的功能许可证。在创建集群之前，将哪些许可证分配给数据节点并不重要；控制节点的许可证设置将复制到每个数据节点。您可以在 **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **许可证 (License)** 区域中修改集群的许可证。

注释 如果在 管理中心 获得许可（并在评估模式下运行）之前添加了集群，当您许可 管理中心 时，会在将策略更改部署到集群时遇到流量中断的情况。更改为许可模式会导致所有数据单元先退出集群，然后重新加入。

创建智能账户以保添加许可证

购买许可证之前，您应设置此账户。

开始之前

您的客户代表可以代表您设置智能账户。如果是这样，则无须按照本程序进行操作，而是从该客户代表处获取访问该账户所需的信息，并确认可以访问该账户。

有关智能账户的一般信息，请参阅http://www.cisco.com/go/smartaccounts。

过程

步骤 1 申请智能账户：

有关说明，请参阅https://community.cisco.com/t5/licensing-enterprise-agreements/request-a-smart-account-for-customers/ta-p/3636515?attachment-id=150577 。

有关其他信息，请参阅https://communities.cisco.com/docs/DOC-57261。

步骤 2 等待智能账户已做好设置准备的通知邮件。在收到邮件时，按照指示点击邮件中的链接。

步骤 3 设置智能账户：

请访问：https://software.cisco.com/software/company/smartaccounts/home?route=module/accountcreation。

有关说明，请参阅https://community.cisco.com/t5/licensing-enterprise-agreements/complete-smart-account-setup-for-customers/ta-p/3636631?attachment-id=132604。

步骤 4 验证您是否可以在智能软件管理器中访问该账户。

转至 https://software.cisco.com/#module/SmartLicensing 并登录。

步骤 5 请确保智能许可帐户包含所需的可用许可证。

当您从 Cisco 或经销商那里购买设备时，您的许可证应该已链接到您的智能帐户。但是，如果您需要自己添加许可证，请参阅 Cisco 商务工作空间。有关许可证 PID，请参阅 许可证 PID，第 204 页。

配置智能许可

本节介绍如何通过智能软件管理器或本地智能软件管理器使用智能许可。

注册 管理中心 以进行智能许可

您可以通过互联网将 管理中心 直接注册到智能软件管理器，或者在使用气隙网络时，使用本地智能软件管理器注册。

将 管理中心 注册到智能软件管理器

将 管理中心 注册到智能软件管理器。

开始之前

- 请确保智能许可帐户包含所需的可用许可证。

  当您从 Cisco 或经销商那里购买设备时，您的许可证应该已链接到您的智能帐户。但是，如果您需要自己添加许可证，请参阅 Cisco 商务工作空间。有关许可证 PID，请参阅 许可证 PID，第 204 页。

- 确保 管理中心 可以在 tools.cisco.com:443 上到达智能软件管理器。
- 确保配置 NTP。在注册过程中，密钥交换发生在智能代理和智能软件管理器之间，因此时间必须同步才能正确注册。

  对于 Firepower 4100/9300，必须使用与 管理中心 相同的机箱 NTP 服务器在机箱上配置 NTP。

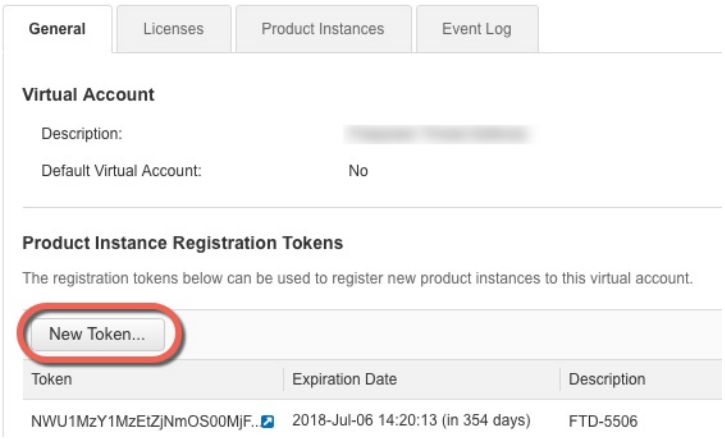
- 如果您的阻止有多个 管理中心，请确保每个 管理中心 拥有唯一的名称，以与可能注册到同一虚拟账户的其他 管理中心 进行区分。此名称对于管理智能许可证授权至关重要，而使用模糊名称稍后会出现问题。

过程

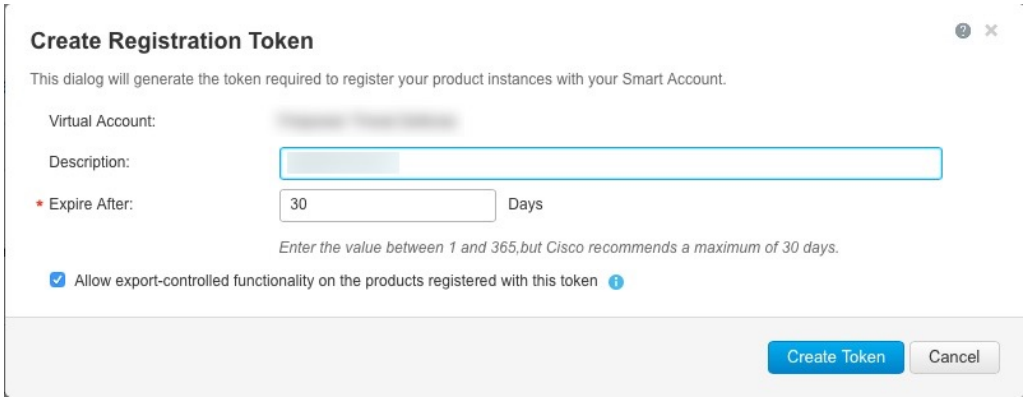
步骤 1 在 智能软件管理器 中，为要将此设备添加到的虚拟帐户请求并复制注册令牌。

a) 点击**清单 (Inventory)**。

b) 在 **General** 选项卡上，点击 **New Token**。



c) 在 **Create Registration Token** 对话框中，输入以下设置，然后点击 **Create Token**：



- **Description**
- **Expire After** - 思科建议该时间为 30 天。
- **在使用此令牌注册的产品上允许导出控制的功能 (Allow export-controlled functionality on the products registered with this token** — 在您所在的国家/地区允许进行强加密的情况下启用导出合规性标志。如果打算使用此功能，则须立即选择该选项。如果稍后启用此功能，则需要使用新产品密钥重新注册设备并重新加载设备。如果您没有看到此选项，则您的帐户不支持出口控制功能。

系统将令牌添加到您的清单中。

d) 点击令牌右侧的箭头图标可以打开 **Token** 对话框，可以从中将令牌 ID 复制到剪贴板。当需要注册威胁防御时，请准备好此令牌，以在该程序后面的部分使用。

图 *38:* 查看令牌

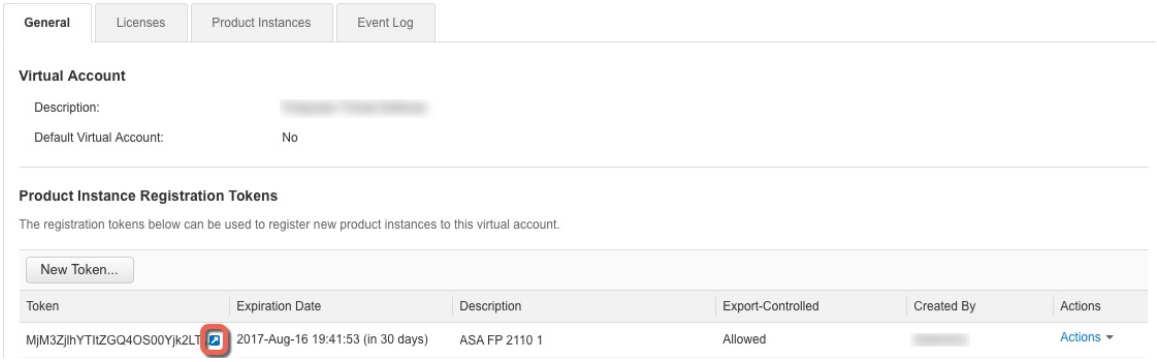
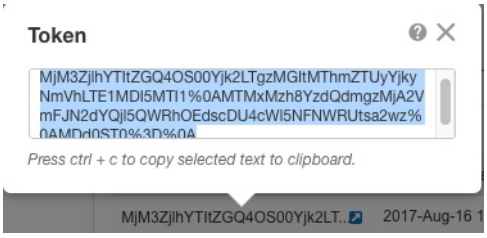


图 *39:* 复制令牌



步骤 2 在 管理中心上，选择 **系统**（⚙）> **许可证** > **智能许可证**。

步骤 3 点击**注册 (Register)**。

步骤 4 将您从 智能软件管理器 生成的令牌粘贴到 **产品实例注册令牌** 字段中。

确保文本开头和结尾处没有空格或空行。

步骤 5 点击 **Apply Changes**（应用更改）。

下一步做什么

- 将设备添加到 管理中心；请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的将设备添加到 管理中心。

将许可证分配到设备

将设备注册到 管理中心时，可以分配大多数许可证。您还可以为每台设备或为多台设备分配许可证。

将许可证分配给单个设备

尽管有一些例外，但如果在受管设备上禁用许可证，就无法使用与该许可证关联的功能。

注释 对于同一 安全模块/引擎上的容器实例，您将对每个实例应用许可证；请注意，对于 安全模块/引擎上的所有实例，安全模块/引擎仅对每个功能占用一个许可证。

注释 对于威胁防御集群，您将对整个集群应用许可证；请注意，集群中的每个设备将对每个功能占用单独的许可证。

开始之前

您必须具有管理员或网络管理员权限才能执行此任务。使用多个域时，必须在分叶域中执行此任务。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要分配或禁用许可证的设备旁边，点击 **编辑**（）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备**。

步骤 4 点击 **许可证** 部分旁边的 **编辑**（）。

步骤 5 选中或清除相应的复选框，以便为设备分配或禁用许可证。

步骤 6 点击**保存 (Save)**。

步骤 7 部署配置更改；请参阅部署配置更改，第 136 页。

下一步做什么

验证许可证状态：转至 **系统**（）> **许可证** > **智能许可证**，将设备的主机名或 IP 地址输入“智能许可证”表顶部的过滤器中，验证每个许可证类型是否仅对每个设备显示一个带有 **复选标记**（）的绿色圆圈 。如有任何其他图标，则将鼠标悬停在图标上查看详细信息。

将许可证分配给多个受管设备

受 管理中心 管理的设备通过 管理中心获取许可证，而非直接通过智能软件管理器获取。

使用本程序在多个设备上启用许可。

注释 对于同一 安全模块/引擎上的容器实例，您将对每个实例应用许可证；请注意，对于 安全模块/引擎上的所有实例，安全模块/引擎仅对每个功能占用一个许可证。

注释 对于威胁防御集群，您将对整个集群应用许可证；请注意，集群中的每个设备将对每个功能占用单独的许可证。

过程

步骤 1 选择**系统**（⚙）>**许可证**>**智能许可证**或**特定许可证**。

步骤 2 点击**编辑许可证**。

步骤 3 对于想要添加到设备的每种类型的许可证：

a) 点击该类型许可证的选项卡。

b) 点击左侧列表中的设备。

c) 点击**添加**将该设备移至右侧列表。

d) 为每个设备重复此操作以接收该类型的许可证。

现在无需再担心是否拥有想要添加的所有设备的许可证。

e) 为想要添加的每种类型许可证重复此子程序。

f) 要删除许可证，请点击设备旁边的 **删除**（🗑）。

g) 点击**应用**。

下一步做什么

验证许可证是否已正确安装。请按照监控智能许可证，第 217 页中的程序操作。

管理智能许可

本部分介绍如何管理智能软件许可。

取消注册 管理中心

从智能软件管理器中取消注册您的管理中心，以将所有许可证授权释放回您的智能帐户，以便可用于其他设备。例如，如果需要停用 管理中心 或重新映像，请注销。

有关在未注册状态下执行许可证的详细信息，请参阅 已注销状态，第 197 页。

过程

步骤 1 选择**系统**（⚙）>**许可证**>**智能许可证**。

步骤 2 请点击 **取消注册**（⛔）。

监控智能许可状态

系统 > 许可证 > 智能许可证 页面的 **智能许可证状态** 部分提供 管理中心上许可证使用情况的概览，如下所述。

使用授权

可能的状态值包括：

- **不合规** （  ） - 分配到受管设备的所有许可证均合规，并且 管理中心 与思科许可证颁发机构通信成功。
- **许可证符合规定，但与许可证授权机构的通信失败** - 设备许可证合规，但 管理中心 无法与思科许可证颁发机构通信。
- **不合规图标或无法与许可证颁发机构通信**- 一个或多个受管设备使用的许可证不合规，或 管理中心 已有超过 90 天未与思科许可证颁发机构通信。

产品注册

指定 管理中心 联系智能软件管理器并向其注册的最后日期。

分配的虚拟帐户

指定用于生成产品实例注册令牌和注册 管理中心的智能账户下的虚拟账户。如果此部署未关联智能账户内的某个特定虚拟账户，则不会显示此信息。

出口管制功能

如果启用此选项，则可部署受限制的功能。有关详细信息，请参阅出口控制功能的许可，第 202 页。

思科成功网络

指定是否为 管理中心启用了思科成功网络。如果启用此选项，您可以向思科提供使用情况信息和统计数据，这些信息对为您提供技术支持非常重要。通过此信息，思科还可以改进产品，并使您获悉未使用的可用功能，以便您能够在网络中将产品的价值最大化。

监控智能许可证

要查看 管理中心 及其管理设备的许可证状态，请使用智能许可证页面。

对于部署中每种类型的许可证，该页面都会列出使用的许可证总数、许可证是合规还是不合规、设备类型以及设备部署所在的域和组。您还可以查看 管理中心的智能许可证状态。在同一 安全模块/引擎 上的容器实例仅会为每个 安全模块/引擎使用一个许可证。因此，即使 管理中心 在每个许可证类型下单独列出每个容器实例，功能许可证类型占用的许可证数量也将为一。

除了 **智能许可证** 页面之外，还有其他一些方法可用于查看许可证：

- **产品许可** 控制面板构件提供了许可证概览。
- **设备管理** 页面 （**设备 > 设备管理**）列出应用于每个受管设备的许可证。

- **智能许可证监控** 运行状况模块在运行状况策略中使用时传达许可证状态。

过程

步骤 1 选择**系统**（⚙）> **许可证** > **智能许可证**。

步骤 2 在**智能许可证**表中，点击每个**许可证类型**文件夹左侧的箭头以展开该文件夹。

步骤 3 在每个文件夹中，验证 **许可证状态** 列中每个设备是否有具有 **复选标记**（✓） 的绿色圆圈 。

如果每个设备都显示带 **复选标记**（✓）的绿色圆圈，则表示设备已正确许可并可供使用。

如果未显示带 **复选标记**（✓）的绿色圆圈，请将鼠标悬停在状态图标上以查看消息。

下一步做什么

- 如果存在不带 **复选标记**（✓）的绿色圆圈的任何设备，则可能需要购买更多许可证。

智能许可疑难解答

我的智能账户中没有显示预期许可证

如果期望看到的许可证未出现在您的智能账户中，则请尝试以下操作：

- 确保许可证不在其他虚拟账户中。您的组织的许可证管理员也许可以给予协助。
- 联系您的许可证销售者，确定许可证已转移到您的账户中。

无法连接到智能许可证服务器

首先检查明显的原因。例如，确保您的 管理中心 具有外部连接。请参阅互联网接入要求，第 2220 页。

意外出现不合规通知或其他错误

- 如果设备已向其他 管理中心注册，则需要先注销原始 管理中心，然后才能在新的 管理中心下许可该设备。请参阅取消注册 管理中心，第 216 页。
- 检查订用许可证的期限是否已到期。

排除其他问题

有关其他常见问题的解决方案，请参阅 https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/215838-fmc-and-ftd-smart-license-registration-a.html

有关许可的其他信息

有关有助于解决许可问题的其他信息，请参阅以下文档：

- FAQ—https://www.cisco.com/c/en/us/td/docs/security/firepower/licensing/faq/firepower-license-FAQ.html
- 许可证路线图 -https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html

第 11 章

安全认证合规性

以下主题介绍如何配置系统来符合安全认证标准：

安全认证合规性模式

组织只能使用符合由美国国防部和全球认证组织制定的安全标准的设备和软件。Firepower 支持符合以下安全认证标准：

- 通用标准 (CC)：国际共同标准承认协定建立的全球标准，用于定义安全产品的属性
- 统一功能获批产品列表 (UCAPL)：符合美国国防信息系统机构 (DISA) 建立的安全要求的产品列表

注释 美国政府已将统一功能获批产品列表 (UCAPL) 的名称改为国防部信息网络获批产品列表 (DODIN APL)。本文档和 Cisco Secure Firewall Management CenterWeb 接口中对 UCAPL 的引用可以解释为对 DODIN APL 的引用。

- 联邦信息处理标准 (FIPS) 140：加密模块的要求规范

可以在 CC 模式或 UCAPL 模式下启用安全认证合规性。启用安全认证合规性不保证严格符合所选安全模式的所有要求。有关强化操作步骤的详细信息，请参阅由认证实体提供的此产品的相关规定。

注意 启用此设置后，您将无法将其禁用。如果设备需要退出 CC 或 UCAPL 模式，必须重新映像。

安全认证合规性特征

下表描述了启用 CC 或 UCAPL 模式时的行为更改。（对登录账户的限制是指命令行访问，而不是 Web 界面访问。）

系统更改	Cisco Secure Firewall Management Center		经典受管设备		Cisco Secure Firewall Threat Defense	
	CC 模式	UCAPL 模式	CC 模式	UCAPL 模式	CC 模式	UCAPL 模式
启用 FIPS 合规性。	是	是	是	是	是	是
系统不允许远程存储备份或报告。	是	是	—	-	-	-
系统启动额外的系统审核后台守护程序。	不支持	是	不支持	是	否	不支持
系统引导加载程序受到保护。	不支持	是	不支持	是	否	不支持
系统对登录帐户应用额外保护。	不支持	是	不支持	是	否	不支持
系统禁用重启按键序列 Ctrl+Alt+Del。	不支持	是	不支持	是	否	不支持
系统最多同时执行 10 个登录会话。	不支持	是	不支持	是	否	不支持
密码必须至少包含 15 个字符，且必须由大小写混合的字母数字字符组成，还必须至少包含一个数字字符。	不支持	是	不支持	是	否	不支持
可以使用本地设备 CLI 配置对本地 `admin` 用户要求的最低密码长度。	不支持	不支持	不支持	不支持	是	是
密码中包含的单词不能是在词典中出现过的单词或包含连续的重复字符。	不支持	是	不支持	是	否	不支持
连续三次登录尝试失败后，系统会锁定除 `admin` 以外的用户。在这种情况下，管理员必须重置密码。	不支持	是	不支持	是	否	不支持
默认情况下，系统会存储密码历史记录。	不支持	是	不支持	是	否	不支持
在失败次数超过可通过 Web 界面配置的最大失败登录尝试次数之后，`admin` 用户会被锁定。	是	是	是	是	—	-
在失败次数超过可通过本地设备 CLI 配置的最大失败登录尝试次数之后，`admin` 用户会被锁定。	不支持	不支持	是，无论是否启用安全认证合规性。	是，无论是否启用安全认证合规性。	是	是

系统更改	Cisco Secure Firewall Management Center		经典受管设备		Cisco Secure Firewall Threat Defense	
	CC 模式	UCAPL 模式	CC 模式	UCAPL 模式	CC 模式	UCAPL 模式
系统会自动为与设备进行的 SSH 会话重新生成密钥： • 某个密钥用于会话活动达一小时后 • 某个密钥用于通过连接传输 1 GB 的数据后	是	是	是	是	是	是
系统在启动时执行文件系统完整性检查(FSIC)。如果 FSIC 失败，则 Firepower 软件无法启动，远程 SSH 访问会被禁用，您只能通过本地控制台访问该设备。如果出现此问题，请联系思科 TAC。	是	是	是	是	是	是

安全认证合规性建议

在使用启用安全认证合规性的系统时，思科建议您遵循以下最佳实践：

- 要在部署中启用安全认证合规性，请首先在 Cisco Secure Firewall Management Center上将其启用，然后在所有托管设备上的同一模式下将其启用。

⚠

注意 Cisco Secure Firewall Management Center不会接受来自受管设备的事件数据，除非两者在同一安全认证合规性模式下运行。

- 对于所有用户，启用密码强度检查，并将最小密码长度设置为认证机构要求的值。
- 如果您在高可用性配置下使用 Cisco Secure Firewall Management Center，请将它们配置为使用同一安全认证合规性模式。
- 如果将 Firepower 4100/9300机箱上的 Cisco Secure Firewall Threat Defense配置为以 CC 或 UCAPL 模式运行，还应将 Firepower 4100/9300 配置为以 CC 模式运行。有关详细信息，请参阅思科 *FXOS Firepower* 机箱管理器配置指南。
- 请勿将系统配置为使用以下任意一种功能：
  - 邮件报告、警报或数据修剪通知。
  - Nmap 扫描、思科 IOS 空路由、设置属性值或 ISE EPS 补救。
  - 备份或报告的远程存储。
  - 第三方客户端访问系统数据库。

- 通过邮件 (SMTP) 传送的外部通知或警报、SNMP 陷阱或系统日志。
- 审核未使用 SSL 证书传输到 HTTP 服务器或系统日志服务器的日志消息，以保护设备和服务器之间的通道。

- 请勿在使用 CC 模式的部署中使用 LDAP 或 RADIUS 启用外部身份验证。
- 请勿使用 CC 模式在部署中启用 CAC。
- 使用 CC 或 UCAPL 模式在部署中通过 Firepower REST API 禁用访问 Cisco Secure Firewall Management Center和受管设备。
- 使用 UCAPL 模式在部署中启用 CAC。
- 请勿使用 CC 模式在部署中配置 SSO。
- 请勿将 Cisco Secure Firewall Threat Defense设备配置为高可用性对，除非它们都使用相同的安全认证合规模式。

注释 Firepower 系统对于以下各项不支持 CC 或 UCAPL 模式：

- 集群中的 Cisco Secure Firewall Threat Defense设备
- Cisco Secure Firewall Threat Defense 容器实例，位于 Firepower 4100/9300

设备强化

有关可用于进一步强化系统的功能的信息，请参阅最新版本的 *Cisco Firepower* 管理中心强化指南 和 *Cisco Cisco Secure Firewall Threat Defense* 强化指南，以及本文档中的以下主题：

- 许可证 ， 第 195 页
- 管理中心 的 ， 第 161 页
- 在 《Cisco Secure Firewall Management Center 设备配置指南》中为威胁防御配置 NTP 时间同步
- 创建邮件警报响应 ， 第 341 页
- 配置入侵事件的邮件警报 ， 第 350 页
- 在《Cisco Secure Firewall Management Center 设备配置指南》中配置 *SMTP*
- 关于《Cisco Secure Firewall Management Center 设备配置指南》中的 *Firepower 1000/2100* 系列的 SNMP
- 在《Cisco Secure Firewall Management Center 设备配置指南》中配置 *SMTP*
- 创建 SNMP 警报响应 ， 第 336 页
- 《Cisco Secure Firewall Management Center 设备配置指南》中的配置动态 *DNS*

- 安全认证合规性， 第 221 页
- 关于在 《Cisco Secure Firewall Management Center 设备配置指南》中配置系统日志
- 《Cisco Secure Firewall Management Center 设备配置指南》中的适用于 威胁防御的站点间 *VPN*
- 《Cisco Secure Firewall Management Center 设备配置指南》中的远程接入 *VPN*
- 《Cisco Secure Firewall Management Center 设备配置指南》中的*FlexConfig* 策略

保护您的网络

请参阅以下主题以了解可配置用于网络保护的功能：

- 访问控制策略， 第 1259 页
- 《Cisco Secure Firewall Management Center 设备配置指南》安全情报
- 《Cisco Secure Firewall Management Center 设备配置指南》侵策略使用入门
- 使用《Cisco Secure Firewall Management Center 设备配置指南》规则调整入侵策略
- 自定义《Cisco Secure Firewall Management Center 设备配置指南》入侵规则
- 更新入侵规则， 第 185 页
- 《Cisco Secure Firewall Management Center 设备配置指南》入侵事件日志记录的全局限制
- 《Cisco Secure Firewall Management Center 设备配置指南》传输层和网络层预处理器
- 《Cisco Secure Firewall Management Center 设备配置指南》具体威胁检测
- 《Cisco Secure Firewall Management Center 设备配置指南》应用层预处理器
- 《Cisco Secure Firewall Management Center 设备配置指南》设备管理
- 更新， 第 179 页

第 IV 部分

运行状态监控

第 12 章

运行状况

以下主题介绍如何在 Firepower 系统中使用运行状况监控：

运行状况监控的要求和前提条件

型号支持

任意

支持的域

任意

用户角色

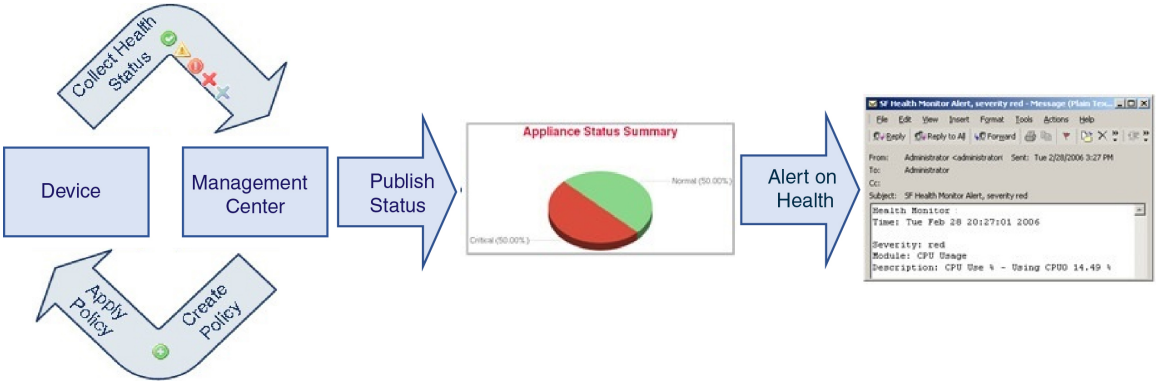
管理员

维护用户

关于运行状况监控

管理中心 上的运行状况监控器跟踪各种运行状况指标，以确保系统中的硬件和软件正常工作。您可以使用运行状况监控器检查整个系统部署中关键功能的状态。

您可以配置运行状况模块以发出警报的频率。管理中心还支持时间序列数据收集。您可以在设备及其运行状况模块上收集时间序列数据的频率。默认情况下，设备监控器会在多个预定义的运行状况监控器控制面板中报告这些指标。收集指标数据以供分析，因此没有与之关联的警报。



可以使用运行状况监控器创建一个测试集合（称为运行状况策略），并将该运行状况策略应用到一个或多个设备上。测试（称为运行状况模块）是用来测试您指定的标准的脚本。您可以通过启用或禁用测试或者通过更改测试设置来修改运行状况策略，可以删除不再需要的运行状况策略。您还可以将来自所选设备的消息加入黑名单，从而排除这些消息。

运行状况策略中的测试以所配置的时间间隔自动运行。您还可以按需运行所有测试或特定测试。运行状况监控器基于配置的测试条件收集运行状况事件。

注释 所有设备都通过“硬件警报“运行状况模块自动报告其硬件状态。管理中心还使用默认运行状况策略中配置的模块自动报告状态。某些运行状况模块（例如“设备测信号”模块）在 管理中心上运行并报告 管理中心的受管设备的状态。要使运行状况模块提供受管设备状态，必须将所有运行状况策略部署到设备。

可以使用运行状况监控器访问特定设备（在多域部署中，则是特定域）的整个系统的运行状态信息。“运行状况监控器”页面上的六边形图和状态表提供网络上所有设备（包括 管理中心）的状态的可视摘要。单个设备运行状况监视器使您可以向下钻取到特定设备的运行状况详细信息。

完全可自定义的事件视图使您可以快速轻松地分析运行状况监控器所收集的运行状况事件。这些事件视图使您可以搜索和查看事件数据，并访问可能与正调查的事件有关的其他信息。例如，如果要查看 CPU 使用率达到特定百分比的所有状况，您可以搜索 CPU 使用率模块并输入百分比值。

您还可以配置响应运行状况事件的邮件、SNMP 或者系统日志警报。运行状况警报是指标准警报和运行状况级别之间的关联。例如，如果要确保设备不会因硬件过载出现故障，您可以设置邮件警报。然后，您可以创建运行状况警报，每当 CPU、磁盘或内存占用率达到您在该设备所应用的运行状况策略中配置的“警告”级别时，就会触发该邮件警报。您可以设置警报阈值，以最小化您收到的重复警报的数量。

注释 运行状况监控可能需要 5-6 分钟才能生成运行状况警报。

如果支持人员要求您为设备生成故障排除文件，您也可以执行此操作。

由于运行状况监控是管理活动，因此只有具有管理员用户角色权限的用户才可以访问系统运行状况数据。

运行状况模块

运行状况模块或运行状况测试会测试您在运行状况策略中指定的条件。

表 *21:* 运行状况模块（所有设备）

模块	说明
CPU 使用率（每个核心）	该模块检查所有内核的CPU使用率是否超载，并在CPU使用率超过为该模块配置的百分比时发出警报。**警告阈值 %** 默认值为 `80`。**临界阈值 %** 默认值为 `90`。
磁盘状态	该模块检测硬盘的性能和设备上的恶意软件存储包（如果已安装）。 当硬盘和 RAID 控制器（如果安装）存在发生故障的危险时，或者，如果安装的其他安装硬盘驱动器不是恶意软件包时，该模块生成“警告”(Warning)（黄色）运行状况警报。当无法检测到已安装恶意软件存储包时，该模块生成“警报”(Warning)（红色）运行状况警报。
磁盘使用情况	该模块将设备的硬盘驱动器和恶意软件存储包中的磁盘使用率与为该模块配置的限值进行对比，并在使用率超过为模块配置的百分比时发出警报。基于模块阈值，当系统删除过多的监控磁盘使用类别的文件，或者当这些类别以外的磁盘使用率达到过高级别时，该模块也发出警报。 使用磁盘使用率运行状况模块监控设备上的 `/` 和 `/volume` 分区的磁盘使用率并跟踪耗尽频率。尽管磁盘使用率模块将 `/boot` 分区列为监控分区，但是分区的大小是静态的，因此该模块在引导分区中不发出警报。 **注意** 如果您收到有关分区 `/卷` 的高非托管磁盘使用率的警报，即使使用率低于运行状况策略中指定的严重阈值或警告阈值，也可能表示存在需要从系统中手动删除的文件。如果收到这些警报，请联系 TAC。
文件系统完整性检查	如果系统启用了 CC 模式或 UCAPL 模式，或者如果系统运行使用 DEV 密钥签名的映像，则此模块会执行文件系统完整性检查。默认情况下，该模块会被启用。
运行状况监视器流程	该模块监控运行状况监视器本身的状态，并且如果管理中心最后收到运行状况事件后的分钟数超过“警告”或“严重”限值，则发出警报。
运行状况监视器流程	该模块监控运行状况监视器本身的状态，并且如果管理中心最后收到运行状况事件后的分钟数超过“警告”或“严重”限值，则发出警报。

模块	说明
接口状态	此模块确定设备当前是否收集流量并根据物理接口和汇聚接口的流量状态发出警报。对于物理接口，信息包括接口名称、链路状态和带宽。对汇聚接口，信息包括接口名称、活动链路的数量和总汇聚带宽。 **注释** 此模块还监控 HA 备用设备流量。虽然已知备用设备不会接收任何流量，但 管理中心 会发出警报，指出接口未接收任何流量。当端口通道上的某些子接口未收到流量时，应用相同的警报原则。 如果您使用 **show interface** CLI 命令来查看设备的接口统计数据，CLI 命令结果中的输入和输出速率可能会与接口模块中出现的流量速率有所不同。 此模块根据 Snort 性能监控的值显示流量速率。Snort 性能监控和 管理中心 接口统计信息的采样间隔不同。由于采样间隔的差异，管理中心 GUI 中的吞吐量值可能与 威胁防御 CLI 结果中显示的吞吐量值不同。
本地恶意软件分析	该模块监控本地恶意软件分析的 ClamAV 更新。
内存使用率	该模块将设备的内存使用率与为模块配置的限值进行对比，并在使用率超过为该模块配置的级别时发出警报。 对于内存超过 4 GB 的设备而言，基于一个公式来预设警报阈值，该公式计算在可能导致系统问题的可用内存中所占的比例。在内存超过 4 GB 的设备上，因为“警告” 和“严重”阈值之间的时间间隔可能非常短，所以 Cisco 建议您将 **警告阈值 %** 值手动设置为 `50`。这将进一步确保您及时收到设备的内存警报来解决问题。 从版本 6.6.0 开始， management center virtual 升级到版本 6.6.0+ 所需的最低 RAM 为 28 GB，management center virtual 部署的建议 RAM 为 32 GB。我们建议您不要降低默认设置：为大多数 management center virtual 实例分配 32 GB RAM，为 management center virtual 300 分配 64 GB（仅限 VMware）。 **注意** 当为 management center virtual 部署分配的 RAM 不足时，运行状况监控器会生成严重警报。 复杂的访问控制策略和规则可控制重要资源并对性能产生不利影响。
进程状态	该模块确定设备上的进程是否在进程管理器外部退出或终止。 如果进程在进程管理器外部被故意退出，模块状态变更为“警告”(Warning)，并且运行状况事件消息指示哪一个进程被退出，直到该模块再次运行、该进程重新启动为止。如果进程在进程管理器外部异常终止或者崩溃，模块状态变更为“严重”(Critical)，并且运行状况事件消息指示被终止的进程，直到该模块再次运行、该进程重新启动为止。

模块	说明
设备中威胁数据更新	在 管理中心，设备用于检测威胁的某些情报数据和配置每 30 分钟会从云进行一次更新。 此模块会提醒您此信息在指定时间段内是否未在设备上更新。 监控的更新包括： • 本地 URL 类别和信誉数据 • 安全情报 URL 列表和源，包括全局阻止列表和 不阻止 列表以及来自威胁情报导向器的 URL • 安全情报网络列表和源（IP 地址），包括全局阻止列表和 不阻止 列表以及来自威胁情报导向器的 IP 地址 • 安全情报 DNS 列表和源，包括全局阻止列表和 不阻止 列表以及来自威胁情报导向器的域。 • 本地恶意软件分析签名（来自 ClamAV） • 如**对象 > 对象管理 > 安全情报 > 网络列表和源**页面上列出的来自威胁情报导向器的 SHA 列表 • **集成 (Integration) > AMP > 动态分析连接 (Dynamic Analysis Connections)** 页面上配置的动态分析设置 • 与缓存 URL 到期相关的威胁配置设置，包括 **系统 > 集成 > 云服务** 页面上的缓存 URL 到期设置。（URL 缓存的更新不受此模块监控。） • 用于发送事件的 Cisco 云的通信问题。请参阅 **系统 > 集成 > 云服务** 页面上的 **Ciscco 云**框。 **注释** 仅当已在系统上配置 TID 且拥有源的情况下才会包括威胁情报导向器更新。 默认情况下，此模块会在 1 小时后发送警告，在 24 小时后发送严重警报。 如果此模块显示 管理中心或任何设备上发生故障，请验证 管理中心是否可以访问这些设备。

表 *22:* 管理中心 运行状况模块

模块	说明
面向终端的 AMP 状态	如果 管理中心 在初始成功连接后无法连接到 AMP 云或 Cisco AMP 私有云，或者如果私有云无法联系公有 AMP 云，则该模块发出警报。如果您使用 Cisco Secure EndpointSecure Endpoint 管理控制台撤销注册 AMP 云连接，该模块也发出警报。

模块	说明
面向 Firepower 的 AMP 状态	如果发生以下情况，则该模块发出警报： • 管理中心 无法联系 AMP 云（公有或私有） 或 Secure Secure Malware Analytics 云或设备，或 AMP 私有云无法联系公有 AMP 云。 • 用于连接的加密密钥无效。 • 设备无法联系 Secure Secure Malware Analytics 云或 Secure Secure Malware Analytics 设备以提交进行动态分析的文件。 • 根据文件策略配置，在网络流量中检测到大量文件。 如果管理中心丢失与互联网的连接，则系统最多可能需要30分钟生成一个运行状况警报。
设备心跳	该模块确定设备是否正监听设备心跳并基于设备心跳状态发出警报。
数据库大小	此模块检查配置数据库的大小，并在大小超过为该模块配置的值（以千兆字节为单位）时发出警报。
发现主机限制	此模块确定 管理中心可以监控的主机数量是否即将达到限制，并基于为该模块配置的警告级别发出警报。有关详细信息，请参阅Firepower 系统主机限制。
事件积压状态	如果等待从设备传输到 管理中心的事件数据积压已持续增长超过 30 分钟，则该模块警报。 若要减少积压，请评估带宽并考虑减少记录的事件。
事件监控器	该模块监控整体事件传入 管理中心速率。
事件流状态	该模块监控管理使用 管理中心上事件流转换器的第三方客户端应用的连接。
ISE 连接监控	该模块监控 Cisco 身份服务引擎（ISE）和 管理中心之间的服务器连接状态。ISE 提供其他用户数据、设备类型数据、设备位置数据、SGT（安全组标记）和 SXP（安全交换协议）服务。
许可证监控	该模块监控许可证到期情况。
管理中心 访问配置更改	该模块监控使用 **配置网络管理-数据-接口** 命令直接对 管理中心 设备执行的 FMC 访问配置更改
管理中心 高可用性状态	此模块会对 管理中心的高可用性状态进行监控和发出警报。如果尚未建立 管理中心高可用性，则 HA 状态为未设置高可用性。 **注释** 此模块将替换高可用性状态模块，其是之前提供的管理中心的高可用性状态。在版本 7.0 中，我们添加了受管设备的高可用性状态。
MySQL 统计信息	此模块监控MySQL数据库的状态，包括数据库大小、活动连接数和内存使用情况。默认情况下已禁用。
电源	该模块确定设备的电源是否需要更换，并基于电源状态发出警报。

模块	说明
RadiusMQ 状态	此模块收集 RabbitMQ 的各种统计信息。
RRD 服务器进程	该模块确定存储时序数据的轮询数据服务器是否正常运行。如果自上次 RRD 服务器更新后其重新启动，则该模块将发出警报；如果在 RRD 服务器重新启动后连续更新的次数达到模块配置中指定的次数，则该模块将输入“严重”或“警告”状态。
安全情报	如果安全情报使用中且 管理中心无法更新源，或者源数据已损坏或不包含可识别的 IP 地址，该模块报警。 另请参阅设备上的威胁数据更新模块。
智能许可证监控	该模块监控智能许可状态。
智能许可证监控	如果发生以下情况，则该模块发出警报： • 智能许可证代理（智能代理）与智能软件管理器之间存在通信错误。 • 产品实例注册令牌已过期。 • 智能许可证使用情况不合规。 • 智能许可证授权或评估模式已过期。
Sybase 统计信息	该模块监控上 管理中心Sybase 数据库的状态，包括数据库大小、活动连接数和内存使用情况。
时序数据 (RRD) 监视器	该模块跟踪已损坏文件在存储时序数据（例如关联事件计数）的目录中的存在情况，并且在文件标记为已损坏和已移除时发出警报。
时间同步状态	该模块跟踪将 NTP 与 NTP 服务器上的时钟配合使用以获取时间的设备时钟的同步状态，并且在两个时钟的时间差超过十秒钟时发出警报。
未解析的组监控	监控策略中使用的未解析组。
URL 过滤监视器	如果 管理中心 未能成功完成以下操作，则此模块会发出警报： • 注册 Cisco 云。 • 从 Cisoc 云下载 URL 威胁数据更新。 • 完成 URL 查找。 您可以配置这些警报的时间阈值。 另请参阅设备上的威胁数据更新模块。
VPN 统计信息	此模块监控 Firepower 设备之间的站点到站点和 RA VPN 隧道。

模块	说明
VPN 状态	此模块在 Firepower 设备之间的一个或多个 VPN 隧道关闭时发出警报。 此模块跟踪： • 适用于 Cisco Secure Firewall Threat Defense的站点间 VPN • 适用于 Cisco Secure Firewall Threat Defense的远程接入 VPN

表 *23:* 设备运行状况模块

模块	说明
AMP 连接状态	如果 威胁防御 在初始成功连接后无法连接到 AMP 云或 Cisco AMP 私有云，或者如果私有云无法联系公有 AMP 云，则该模块发出警报。默认情况下已禁用。
AMP Threat Grid 连接	在初始连接成功后，如果 威胁防御 无法连接到 AMP 威胁网格云，则模块警报。
ASP 丢弃	该模块监控数据平面加速安全路径所放弃的连接。
自动应用旁路	该模块监控绕过的检测应用。
集群/HA 故障转移状态	该模块监控设备集群的状态。如果发生以下情况，则该模块发出警报： • 集群选举出新的主设备。 • 新的辅助设备会加入集群。 • 主设备或辅助设备会退出集群。
配置资源利用率	如果已部署的配置的大小使设备面临内存耗尽的风险，此模块会发出警报。 警报会显示您的配置需要多少内存，以及超出可用内存的数量。如果发生此情况，请重新评估您的配置。通常来说，您可以减少访问控制规则或入侵策略的数量或降低其复杂性。 **Snort 内存分配** • 总 *Snort* 内存表示为 威胁防御 设备上运行的 Snort 2 实例分配的内存。 • 可用内存 表示系统为 Snort 2 实例分配的内存。请注意，此值不仅是 总 *Snort* 内存 与为其他模块保留的组合内存之间的差。此值经过几次其他计算后得出，然后除以 Snort 2 进程数。 可用内存 值为负表示 Snort 2 实例没有足够的内存来部署配置。寻求支持，请联系 Cisco 技术支持中心 (TAC)。
连接统计信息	此模块监控连接统计信息和 NAT 转换计数。
CPU 使用率数据平面	该模块检查设备上所有数据平面进程的平均 CPU 使用率是否超载，并在 CPU 使用率超过为该模块配置的百分比时发出警报。**警告阈值 %** 默认值为 `80`。**临界阈值 %** 默认值为 `90`。

模块	说明
Snort 的 CPU 使用情况	该模块检查设备上所有 Snort 进程的平均 CPU 使用率是否超载，并在 CPU 使用率超过为该模块配置的百分比时发出警报。**警告阈值 %** 默认值为 80。**临界阈值 %** 默认值为 90。
系统的 CPU 使用情况	该模块检查设备上所有系统进程的平均CPU使用率是否超载，并在CPU使用率超过为该模块配置的百分比时发出警报。**警告阈值 %** 默认值为 80。**临界阈值 %** 默认值为 90。
关键流程统计信息	该模块监控关键进程的状态、资源消耗和重新启动计数。
已部署配置统计信息	该模块监控有关已部署配置的统计信息，例如 ACE 数、IPS 规则数。
Firepower 平台故障	此模块为 Firepower 1000、2100、3000 系列设备生成平台故障警报，故障是由 管理中心管理的可变对象。每个故障均表示Firepower 1000、2100、3000 实例中的一个故障或已发出的警报阈值。在一个故障的生命周期中，故障可从一个状态或一种严重性更改为另一个状态或另一种严重性。 每个故障包含有关发生故障时受影响对象的运行状态的信息。如果故障是临时性的并已得到解决，则对象会转换到正常运行状态。 有关详细信息，请参阅 《*Cisco Firepower 1000/2100 FXOS* 故障和错误消息指南》。
流分流统计信息	该模块监控受管设备的硬件流分流统计信息。
硬件告警	该模块确定物理受管设备上的硬件是否需要更换并基于硬件状态发出警报。该模块还报告与硬件有关的守护程序的状态。
内联链路不匹配告警	该模块监控与内联集相关的端口，并且如果内联对的两个接口协商不同的速度，则发出警报。
入侵和文件事件率	该模块将每秒钟入侵事件的数量与为该模块配置的限值进行对比。如果超过限值，则该模块发出警报。如果入侵和文件事件速率为零，则入侵进程可能已关闭或者受管设备可能没有发送事件。选择**分析** > **入侵** > **事件**，检查是否正从该设备接收事件。 通常，网段的事件速率平均为每秒 20 个事件。对于具有本平均速率的网段，每秒事件（严重）数应设置为 50，每秒事件（警告）数应该设置为30。要确定系统的限值，请在设备的“统计信息”页面（**系统**（⚙） > **监控** > **统计信息**）找到“事件/秒”值，然后使用以下公式计算限值： • 每秒事件（严重）数 = “事件/秒”(Events/Sec) * 2.5 • 每秒事件（警告）数 = “事件/秒”(Events/Sec) * 1.5 您可以为每种限值设置的最大事件数是 999，“严重”(Critical) 限值必须高于“警告”(Warning) 限值。

模块	说明
链路状态传播	仅限于 ISA 3000。 该模块确定成对的内联集中链路发生故障的时间，并且触发链路状态传播模式。如果链路状态传播到该对，该模块的状态分类变更为“严重”，并且状态读作： `Module Link State Propagation: ethx_ethy is Triggered` 其中 `x` 和 `y` 为成对的接口编号。
内存使用率数据平面	此模块检查数据平面进程使用的已分配内存百分比，并在内存使用率超过为该模块配置的百分比时发出警报。**警告阈值 %** 默认值为 `80`。**临界阈值 %** 默认值为 `90`。
Snort 的内存使用情况	此模块检查Snort进程使用的已分配内存百分比，并在内存使用率超过为该模块配置的百分比时发出警报。**警告阈值 %** 默认值为 `80`。**临界阈值 %** 默认值为 `90`。
网卡重置	该模块检查由于硬件故障而重新启动的网卡，并且在发生重置时发出警报。
NTP 统计信息	该模块监控受管设备的 NTP 时钟同步状态。默认情况下已禁用。
领域	允许为领域或用户不匹配设置警告阈值，包括： • 用户不匹配：系统不下载某个用户而是报告给 管理中心 。 造成用户不匹配通常是因为该用户属于不予下载至 管理中心。请回顾《Cisco Secure Firewall Management Center 设备配置指南》中介绍的信息。 • 领域不匹配：某个用户登录到某个域，而该域对应 管理中心未知的某个领域。 有关详细信息，《Cisco Secure Firewall Management Center 设备配置指南》。 当您尝试下载的用户数超过每个领域支持的最大下载用户数时，此模块还会显示运行状况警报。单一领域下载用户的最大数目取决于您的管理中心型号。 有关详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的用户限制
路由统计信息	该模块监控路由表的当前状态。
Snort3 统计信息	该模块收集和监控 Snort 3 统计信息的事件，流和数据包。
Snort 身份内存使用情况	使您能够在内存使用率超过为模块配置的级别时为 Snort 身份处理和警报设置警告阈值。**临界阈值 %** 默认值为 `80`。 此运行状况模块专门跟踪Snort中用于用户身份信息的总空间。它显示当前内存使用情况详细信息，用户到 IP 绑定的总数以及用户组映射详细信息。Snort 在文件中记录这些详细信息。如果内存使用情况文件不可用，则此模块的运行状况警报显示 等待数据。这可能发生在由于新安装或主要更新，从 Snort2 切换到 Snort3 或重新启动或主要策略部署而导致的 Snort 重启期间。根据运行状况监控周期以及当文件可用时，警告会消失，运行状况监控器会显示此模块的详细信息，其状态变为绿色。

模块	说明
Snort 重新配置检测	如果设备重新配置失败，则该模块发出警报。
Snort 统计信息	该模块监控事件、流和数据包的 Snort 统计信息。
SSE 连接状态	在初始连接成功后，如果 威胁防御 无法连接到 SSE 云，则模块警报。默认情况下已禁用。
威胁防御 HA（裂脑检查）	此模块会对 威胁防御的高可用性状态进行监控和发出警报，并提供拆分情景的运行状况警报。如果尚未建立 威胁防御高可用性，则 HA 状态为未设置高可用性。
XTLS 计数器	该模块监控 XTLS/SSL 流、内存和缓存有效性。默认情况下已禁用。

配置运行状况监控

过程

步骤 1 确定要监控的运行状况模块，如运行状况模块，第 231 页中所述。

您可以为 Firepower 系统中的每种设备设定特定策略、仅为该设备执行适当的测试。

提示 要快速启用运行状态监控而不定义监控行为，可以应用为此目的提供的默认策略。

步骤 2 将运行状态策略应用到要跟踪运行状态的每台设备，如创建运行状况策略，第 240 页中所述。

步骤 3 （可选。）配置运行状况监控器警报，如创建运行状况监控器警报，第 246 页中所述。

您可以设置在运行状况级别达到特定运行状况模块的特定严重性级别时触发的邮件、系统日志或 SNMP 警报。

运行状况策略

运行状况策略包含为若干模块配置的运行状况测试标准。您可以控制针对每个设备要运行的运行状况模块，并可配置每个模块运行的测试中所用的具体限值。

当配置运行状况策略时，由您决定是否为该策略启用每个运行状况模块。此外，还可以选择每个已启用模块每次评估进程运行状况时报告的运行状况的控制标准。

您可以创建在系统中每个设备上应用的一个运行状况策略、定制您计划在特定设备上应用的每个运行状况策略，或者使用为您提供的默认运行状况策略。在多域部署中，祖先域中的管理员可以将运行状况策略应用于后代域中的设备，而后代域可以使用这些策略或者将其替换为自定义本地策略。

默认运行状况策略

管理中心 设置过程会创建并应用初始运行状况策略，其中大多数（但不是全部）可用的运行状况模块均已启用。系统还会将此初始策略应用于添加到 管理中心的设备。

此 初始 运行状况策略基于 默认 运行状况策略，您既不能查看也不能编辑，但可以在创建自定义运行状况策略时进行复制。

升级和默认运行状况策略

升级 管理中心 时，任何新的运行状况模块都将添加到所有运行状况策略，包括初始运行状况策略、默认运行状况策略和任何其他自定义运行状况策略。通常，新的运行状况模块以启用状态添加。

注释 要使新的运行状况模块开始监控和发出警报，请在升级后重新应用运行状况策略。

创建运行状况策略

如果要定制用于设备的运行状况策略，您可以创建一个新策略。策略中的设置初始填充您选定为新策略基础的运行状况策略的设置。您可以编辑策略以指定首选项，例如启用或禁用策略中的模块，根据需要更改每个模块的警报条件，并指定运行时间间隔。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。 祖先域中的管理员可以将运行状况策略应用于后代域中的设备，而后代域可以使用这些策略或者将其替换为自定义本地策略。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **策略** 。

步骤 2 点击**创建策略**。

步骤 3 输入策略的名称。

步骤 4 从 **基本策略** 下拉列表中选择要用作新策略基础的现有策略。

步骤 5 输入策略的说明。

步骤 6 选择**保存**。

下一步做什么

- 如 应用运行状况策略， 第 241 页 中所述，对设备应用运行状况策略。
- 编辑策略以指定模块级策略设置，如 编辑运行状况策略， 第 241 页中所述。

应用运行状况策略

当您将运行状况策略应用到设备时，您在策略中启用的所有模块的运行状况测试自动监控设备上的进程和硬件的运行状况。然后，运行状况测试继续以您在策略中配置的时间间隔运行，为设备收集运行状况数据并将该数据转发到 管理中心。

如果您在运行状况策略中启用一个模块，然后将该策略应用到不需要该运行状况测试的设备，则运行状况监控器报告该运行状况模块的状态为禁用。

如果您将启用所有模块的策略应用到设备中，它从该设备移除所有已应用的运行状况策略，以便不应用任何运行状况策略。

当您将不同的策略应用到已应用策略的设备时，请基于新应用的测试在显示新数据时使用一些延迟。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。 祖先域中的管理员可以将运行状况策略应用于后代域中的设备，而后代域可以使用这些策略或者将其替换为自定义本地策略。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **策略** 。

步骤 2 点击要应用的策略旁边的 **部署运行策略** (📥) 。

步骤 3 选择要应用运行状况策略的设备。

注释 部署策略后，无法从设备中删除策略。要停止设备的运行状况监控，请创建一个所有模块都禁用的运行状况策略并将其应用到设备。

步骤 4 点击**应用 (Apply)** 以将该策略应用到所选设备上。

下一步做什么

- 或者，监控任务状态；请参阅查看任务消息 ， 第 277 页。

  只要成功应用该策略，设备监控即开始。

编辑运行状况策略

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。 祖先域中的管理员可以将运行状况策略应用于后代域中的设备，而后代域可以使用这些策略或者将其替换为自定义本地策略。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **策略** 。

步骤 2 点击要修改的策略旁边的 **编辑**（✎） 。

步骤 3 要编辑策略名称及其说明，请点击针对策略名称提供的 **编辑**（✎） 图标。

步骤 4 **运行状况模块** 选项卡显示所有设备模块及其属性。点击针对模块及其属性提供的切换按钮-打开（  ）或关闭（  ）以分别启用或禁用运行状况测试。要在运行状况模块上执行批量启用或禁用测试，请点击 **全选** 切换按钮。有关模块的信息，请参阅运行状况模块 ，第 231 页。

注释
- 模块和属性使用支持设备（威胁防御、管理中心 或两者）进行标记。
- 不能选择包含或排除 CPU 和内存模块的各个属性。

步骤 5 酌情设置 **严重** 和 **警告** 阈值比例。

步骤 6 在 **运行时间间隔** 选项卡中，在字段中输入相关值：

- **运行状况模块运行间隔 (Health Module Run Interval)** - 运行运行状况模块的频率。最小间隔为 5 分钟。
- **指标收集间隔**-在设备及其运行状况模块上收集时间序列数据的频率。默认情况下，设备监控器会在多个预定义的运行状况监控器控制面板中报告这些指标。有关控制面板的详细信息，请参阅 关于控制面板。收集指标数据以供分析，因此没有与之关联的警报。

步骤 7 点击**保存**。

下一步做什么

- 如应用运行状况策略 ，第 241 页中所述，将该运行状况策略应用到每台设备。此选项允许您将应用更改并更新所有受影响策略的策略状态。

删除运行状况策略

您可以删除不再需要的运行状况策略。如果您删除仍然应用于设备的策略，直到您应用不同的策略，该策略设置仍然有效。此外，如果您删除应用到设备的运行状况策略，在您禁用基础的相关警报响应之前，该设备仍在生效的任何运行状况监控警报仍然处于活动状态。

在多域部署中，只能删除在当前域中创建的运行状况策略。

提示 要停止设备的运行状况监控，请创建一个所有模块都禁用的运行状况策略并将其应用到设备。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **策略** 。

步骤 2 点击要删除的策略旁边的 **删除**（🗑），然后点击 **删除运行状况策略** 将其删除。
系统将显示一则消息，指示删除是否成功。

运行状况监控中的设备排除

在正常的网络维护过程中，您禁用设备或使其暂时不可用。由于此类停运是有意而为，因此您不希望这些设备的运行状态影响 管理中心上的摘要运行状态。

您可以使用运行状况监视器排除功能禁用对设备或模块的运行状况监控状态报告。例如，如果您知道一个网段将不可用，因为到该网段上受管设备的连接失效，所以您可以临时禁用对该设备的运行状况监控，以禁止管理中心上的运行状况显示警告或严重状态。

当您禁用运行状况监控状态时，仍会生成运行状况事件，但是它们处于禁用状态，不会影响运行状况监视器的运行状况。如果您从排除名单移除设备或模块，排除过程中生成的事件继续显示禁用的状态。

要在设备上临时禁用运行状况事件，请转到排除配置页面并将设备添加至设备排除名单。在设置生效后，系统在计算整体运行状况时，不再考虑列入排除名单的设备。“运行状况监控设备状态摘要”(Health Monitor Appliance Status Summary) 列出处于禁用状态的设备。

您还可以禁用单个运行状况模块。例如，当在管理中心上达到主机限制时，可以将 主机限制状态消息禁用。

请注意，在“运行状况监控”主页面，如果您通过点击该状态行上的箭头来展开以查看具有特定状态的设备列表，就可以区分被排除的设备。

注释 在管理中心上，运行状况监视器排除设置是本地配置设置。因此，如果您将设备排除，接着将其删除，然后使用 管理中心重新注册，排除设置保持不变。最近重新注册的设备仍旧被排除。

在多域部署中，祖先域中的管理员可以将后代域中的设备或运行状况模块排除。但是，后代域中的管理员可以覆盖祖先配置并清除其域中设备的排除。

从运行状况监控中排除设备

您可以单独或按组、型号或关联运行状况策略将设备排除。

如果需要将单个设备的事件和运行状况设置为禁用，您可以将该设备排除。在排除设置生效后，该设备在“运行状况监控设备模块摘要”中显示为已禁用，并且该设备的运行状况事件的状态为已禁用。

在多域部署中，将祖先域中的设备排除会针对所有后代域将该设备排除。后代域可以覆盖此继承配置并清除排除。您只能在全局级别将 管理中心 排除。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **排除**。

步骤 2 点击**添加设备**。

步骤 3 在 **设备排除** 对话框中的 **可用设备**下，点击 **添加**（⊕） 要从运行状况监控中排除的设备。

步骤 4 点击 **排除**。所选设备显示在排除项主页中。

步骤 5 要从排除项列表中删除设备，请点击 **删除**（🗑）。

步骤 6 点击**应用**。

下一步做什么

要排除设备上的单个运行状况策略模块，请参阅 排除运行状况策略模块，第 244 页。

排除运行状况策略模块

您可以将设备上的单个运行状况策略模块排除。您可能想要执行此操作以禁止来自模块的事件将设备的状态变更为警告或严重。

排除项设置生效后，设备会显示设备中从运行状况监控中排除的模块数量。

提示 确保您跟踪单独排除的模块，以便您可以在需要时重新激活它们。如果您意外地禁用模块，则可能漏掉所需的警告或严重消息。

在多域部署中，祖先域中的管理员可以将后代域中的运行状况模块排除。但是，后代域中的管理员可以覆盖此祖先配置，并清除在其域中应用的策略的排除。您只能在全局级别将管理中心运行状况模块排除。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **排除**。

步骤 2 点击要修改的设备旁边的 **编辑**（✎） 。

步骤 3 在**排除运行状况**模块对话框中，默认情况下，设备的所有模块都从运行状况监控中排除。某些模块仅适用于特定设备；有关详细信息，请参阅运行状况模块，第 231 页。

步骤 4 要指定设备的排除持续时间，请从 **排除周期** 下拉列表中选择持续时间。

步骤 5 要选择要从运行状况监控中排除的模块，请点击 **启用模块级别排除** 链接。 **排除运行状况模块** 对话框显示设备的所有模块。默认情况下，禁用不适用于关联运行状况策略的模块。要排除模块，请执行以下操作：

1. 点击所需模块旁边的 **滑块** （ ） 按钮。
2. 要指定所选模块的排除持续时间，请从 **排除周期** 下拉列表中选择持续时间。

步骤 6 如果为排除项配置选择 **排除周期** 而不是 **永久**，则可以选择在配置到期时自动将其删除。要启用此设置，请选中 **自动删除过期配置** 复选框。

步骤 7 点击**确定**。

步骤 8 在设备排除主页中，点击 **应用**。

过期的运行状况监控器排除项

当设备或模块的排除期限到期时，您可以选择清除或更新排除项。

过程

步骤 1 选择**系统**（ ） > **运行状况** > **排除**。

设备上会显示 **警告**（ ） 图标，指示从警报中排除设备或模块的持续时间到期。

步骤 2 要更新设备排除项，请点击设备旁边的 **编辑**（ ） 。在 **排除运行状况模块** 对话框中，点击 **续约** 链接。使用当前值扩展排除期。

步骤 3 要清除排除设备，请点击设备旁边的 **删除**（ ），点击 **从排除项中删除设备**，然后点击 **应用**。

步骤 4 要更新或清除模块排除项，请点击设备旁边的 **编辑**（ ） 。在 **排除运行状况模块** 对话框中，点击 **启用模块级别排除** 链接，然后针对模块点击 **续约** 或 **清除** 链接。当您点击 **续约**时，模块上的排除期限将使用当前值延长。

运行状况监控器警报

您可以设置警报以在运行状况策略中的模块状态变更时，通过邮件、SNMP 或系统日志通知您。您可以将现有警报响应与运行状况事件级别相关联，以在特定级别的运行状况事件发生时触发和发出警报。

例如，如果您担心设备可能用尽硬盘空间，可以在剩余磁盘空间达到警告级别时自动向系统管理员发送一封邮件。如果硬盘驱动器继续加载，您可以在硬盘驱动器达到严重性级别时发送第二封邮件。

在多域部署中，只能查看和修改在当前域中创建的运行状况监控器警报。

运行状况监控器警报信息

运行状况监视器生成的警报包含以下信息：

- 严重程度，指明警报的严重性级别。
- 模块，指定其测试结果触发警报的运行状况模块。
- 说明，包括触发警报的运行状况测试结果。

下表介绍了这些严重级别。

表 *24:* 警报严重性

严重性	说明
严重	运行状况测试结果符合触发“严重”(Critical) 警报状态的标准。
警告	运行状况测试结果符合触发“警告”(Warning) 警报状态的标准。
正常状态	运行状况测试结果符合触发“正常”(Normal) 警报状态的标准。
错误	运行状况测试未运行。
已恢复	运行状况测试结果符合在“严重”(Critical) 或“警告”(Warning) 警报状态之后返回到正常警报状态的条件。

创建运行状况监控器警报

您必须是管理员用户才能执行此程序。

当您创建运行状况监控器警报时，您可以在严重性级别、运行状况模块和警报响应之间建立关联。您可以使用现有警报或特别配置新的警报以报告系统运行状况。当选定的模块发生严重性级别时，警报触发。

如果您以复制现有阈值的方式创建或更新阈值，将会收到冲突通知。当存在重复的阈值时，运行状况监控器使用生成最少警报的阈值并忽略其他阈值。该阈值的超时值必须介于 5 和 4,294,967,295 分钟之间。

在多域部署中，只能查看和修改在当前域中创建的运行状况监控器警报。

开始之前

- 配置用于管理 管理中心与 SNMP、系统日志或邮件服务器（用于发送运行状况警报）通信的警报响应；请参阅Cisco Secure Firewall Management Center 警报响应，第 335 页。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **监控警报**。

步骤 2 点击 **Add**。

步骤 3 在 **添加运行状况警报** 对话框，在 **运行状况警报名称** 字段输入运行状况警报的名称。

步骤 4 从 **严重性** 下拉列表中，选择要用于触发警报的严重性级别。

步骤 5 从 **警报** 下拉列表中，选择在达到指定的严重性级别时要触发的警报响应。如果尚未 Cisco Secure Firewall Management Center 警报响应，请点击 **警报** 以访问 **警报** 页面并进行设置。

步骤 6 从 **运行状况模块** 列表中选择要为其应用警报的运行状况策略模块。

步骤 7 或者，在**阈值超时 (Threshold Timeout)** 字段中，输入在每个阈值期间结束和阈值计数重置之前应经过的分钟数。

即使策略运行时间间隔值小于阈值超时值，给定模块中报告的两个运行状况事件之间的间隔始终较大。例如，如果将阈值超时更改为 8 分钟，并且策略运行时间间隔为 5 分钟，则报告的事件之间的时间间隔为 10 (5 x 2) 分钟。

步骤 8 点击**保存 (Save)** 保存运行状况警报。

编辑运行状况监控器警报

您必须是管理员用户才能执行此程序。

您可以编辑现有运行状况监视器警报以更改与运行状况监控器警报相关的严重性级别、运行状况模块或警报响应。

在多域部署中，只能查看和修改在当前域中创建的运行状况监控器警报。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **监控警报**。

步骤 2 点击针对您要修改的所需运行状况警报提供的 **编辑**（✎） 图标。

步骤 3 在 **编辑运行状况警报** 对话框中，从 **警报** 下拉列表中选择所需的警报条目，或点击 **警报** 链接以配置新的警报条目。

步骤 4 点击**保存 (Save)**。

删除运行状况监控器警报

在多域部署中，只能查看和修改在当前域中创建的运行状况监控器警报。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **监控警报**。

步骤 2 点击要删除的运行状况警报旁边的 **删除**（🗑），然后点击 **删除运行状况警报** 将其删除。

下一步做什么

- 禁用或删除基础警报响应，以确保不会继续发出警报；请参阅Cisco Secure Firewall Management Center 警报响应，第 335 页。

使用运行状况监控器

您必须是管理员、运维或安全分析师用户才能执行此程序。

运行状况监控器为管理中心管理的所有设备以及管理中心提供已编译的运行状况。运行状况监控器由以下部分组成：

- 运行状况摘要页面 - 提供 管理中心 和 管理中心 管理的所有设备的运行状况概览视图。设备将单独列出，或根据其地理位置、高可用性或集群状态（如果适用）进行分组。
  - 将鼠标悬停在表示设备运行状况的六边形上时，可查看 管理中心 和任何设备的运行状况摘要。
  - 设备左侧的点表示其运行状况：
    - 绿色 — 无警报。
    - 橙色 — 至少一个运行状况警告。
    - 红色 — 至少一个严重运行状况警报。
- 监控导航窗格 — 允许您导航设备层次结构。您可以从导航窗格查看各个设备的运行状况监控器。

在多域部署中，祖先域中的运行状况监控器显示所有后代域中的数据。在后代域中，它仅显示当前域中的数据。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **监控**。

步骤 2 在 **运行状况** 登录页面中查看 管理中心 及其受管设备的状态。

a) 将鼠标指针悬停在六边形上可查看设备的运行状况摘要。弹出窗口显示前五个运行状况警报的截断摘要。点击弹出窗口可打开运行状况警报摘要的详细视图。

b) 在设备列表中，点击 **展开**（ ） 和 **折叠**（ ） 以展开和折叠设备的运行状况警报列表。

展开该行时，系统将列出所有运行状况警报，包括状态、标题和详细信息。

注释 运行状况警报按严重性级别排序。

步骤 3 使用监控导航窗格访问设备特定的运行状况监控器。使用监控导航窗格时：

a) 点击 **主页** 返回运行状况摘要页面。

b) 点击**防火墙管理中心 (Firewall Management Center)** 以查看 Cisco Secure Firewall Management Center 本身的运行状况监控器。

c) 在设备列表中，点击 **展开**（ ） 和 **折叠**（ ） 以展开和折叠受管设备列表。

展开该行时，系统会列出所有设备。

d) 点击设备可查看设备特定的运行状况监控器。

下一步做什么

- 有关由管理中心管理的任何设备的已编译运行状况和指标的信息，请参阅 设备运行状况监控器，第 251 页。
- 有关 管理中心运行状况的信息，请参阅 使用 管理中心 运行状况监控器，第 249 页。

  要随时返回运行状况登录页面，请点击 **主页**。

使用 管理中心 运行状况监控器

您必须是管理员、运维或安全分析师用户才能执行此程序。

管理中心 监控器提供 管理中心的运行状态的详细视图。运行状况监控器由以下部分组成：

- 高可用性（如果已配置）－高可用性 (HA) 面板显示当前 HA 状态，包括主用和备用设备的状态、上次同步时间和整体设备运行状况。
- 事件速率－“事件速率”面板将最大事件速率显示为基准，以及 管理中心接收的整体事件速率。
- 事件容量－“事件容量”面板按事件类别显示当前消耗量，包括事件的保留时间、当前事件容量与最大事件容量，以及容量溢出机制，其中 管理中心在存储的事件超出配置的最大容量时向您发出警报。
- 进程运行状况－“进程运行状况”面板提供关键进程的概览视图，以及一个选项卡，可让您查看所有已处理进程的状态，包括每个进程的 CPU 和内存使用情况。
- CPU－“CPU” 面板允许您在平均 CPU 使用率（默认）和所有核心的 CPU 使用率之间切换。
- 内存－“内存”面板显示 管理中心上的整体内存使用情况。
- 接口－“接口”面板显示所有接口的平均输入和输出速率。

- 磁盘使用—“磁盘”使用面板显示整个磁盘的使用情况，以及存储管理中心数据的关键分区的使用情况。

提示 在会话处于不活动状态达到 1 小时（或配置的其他时间间隔）之后，会话通常注销。如果计划长时间被动监控运行状态，请考虑免除某些用户发生会话超时，或者更改系统超时设置。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **监控**。

步骤 2 使用 **监控** 导航窗格访问 管理中心 和设备特定的运行状况监控器。

- 独立 管理中心 显示为单个节点；高可用性 管理中心 显示为一对节点。
- 运行状况监控器可用于 HA 对中的主用设备和备用 管理中心 。

步骤 3 了解 管理中心 控制面板。

管理中心 控制面板包括 管理中心 的 HA 状态摘要视图（如果已配置），以及 管理中心 进程和设备指标（例如 CPU、内存和磁盘使用情况）的概览视图。

运行设备的所有模块

您必须是管理员、运维或安全分析师用户才能执行此程序。

在您创建运行状况策略时配置的策略运行时间间隔内，运行状况模块测试自动运行。但是，您也可以按需运行所有运行状况模块测试，以收集该设备的最新运行状况信息。

在多域部署中，可以运行当前域和任何后代域中的设备的运行状况模块测试。

过程

步骤 1 查看设备的运行状况监控器。

步骤 2 点击**运行所有模块 (Run All Modules)**。状态栏指示测试进程，然后“运行状况监控设备”(Health Monitor Appliance) 页面刷新。

注释 当您手动运行运行状况模块时，第一次自动发生的刷新可能不会影响自动运行测试的数据。如果没有为您手动运行的模块更改该值，请等待几秒钟，然后点击设备名称来刷新该页面。您还可以等待页面再次自动刷新。

运行特定运行状况模块

您必须是管理员、运维或安全分析师用户才能执行此程序。

在您创建运行状况策略时配置的策略运行时间间隔内，运行状况模块测试自动运行。但是，您也可以按需运行一个运行状况模块测试以收集该模块的最新运行状况信息。

在多域部署中，可以运行当前域和任何后代域中的设备的运行状况模块测试。

过程

步骤 1 查看设备的运行状况监控器。

步骤 2 在**模块状态摘要 (Module Status Summary)** 图形中，点击要查看的运行状况警报状态类别的颜色。

步骤 3 在要查看其事件列表的警报的**警报详细信息 (Alert Detail)** 行，请点击**运行 (Run)**。

状态栏指示测试进程，然后“运行状况监控设备”(Health Monitor Appliance) 页面刷新。

注释 当您手动运行运行状况模块时，第一次自动发生的刷新可能不会影响自动运行测试的数据。如果没有为您刚才手动运行的模块更改该值，请等待几秒钟，然后点击设备名称来刷新该页面。您还可以等待页面再次自动刷新。

生成运行状况模块警报图形

您必须是管理员、运维或安全分析师用户才能执行此程序。

您可以图表表示特定设备的特定运行状况测试的一段时间内的结果。

过程

步骤 1 查看设备的运行状况监控器。

步骤 2 在“运行状况监控设备”(Health Monitor Appliance) 页面的**模块状态摘要 (Module Status Summary)** 图形中，点击要查看的运行状况警报状态类别的颜色。

步骤 3 在要查看其事件列表的警报的 **Alert Detail** 行，请点击 **Graph**。

提示 如果未显示事件，您可能需要调整时间范围。

设备运行状况监控器

设备运行状况监控器为 管理中心管理的任何设备提供已编译的运行状况。设备运行状况监控器收集 Firepower 设备的运行状况指标，以便预测和响应系统事件。设备运行状况监控器由以下组件组成：

- 系统详细信息 - 显示有关受管设备的信息，包括已安装的 Firepower 版本和其他部署详细信息。

- 故障排除和链接 - 提供常用故障排除主题和程序的便捷链接。
- 运行状况警报 - 运行状况警报监控器提供设备运行状况的概览视图。
- 时间范围 - 用于限制各种设备指标窗口中显示的信息的可调时间窗口。
- 设备指标 - 跨预定义控制面板分类的一系列关键 Firepower 设备运行状况指标，包括：
  - CPU - CPU 利用率，包括按进程和物理核心划分的 CPU 使用情况。
  - 内存 - 设备内存使用率，包括数据平面和 Snort 内存使用率。
  - 接口 - 接口状态和汇聚流量统计信息。
  - 连接 - 连接统计信息（例如大象流、活动连接、峰值连接等）和 NAT 转换计数。
  - Snort - 与 Snort 进程相关的统计信息。
  - 磁盘使用率 - 设备磁盘使用率，包括磁盘大小和每个分区的磁盘使用率。
  - 关键进程 - 与托管进程相关的统计信息，包括进程重新启动和其他选定的运行状况监控器，例如 CPU 和内存使用率。

查看系统详细信息和故障排除

您必须是管理员、运维或安全分析师用户才能执行此程序。

“系统详细信息”部分提供所选设备的常规系统信息。您还可以启动该设备的故障排除任务。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **监控**。

使用监控导航窗格访问设备特定的运行状况监控器。

步骤 2 在设备列表中，点击 **展开**（>） 和 **折叠**（⌄） 以展开和折叠受管设备列表。

步骤 3 点击设备可查看设备特定的运行状况监控器。

步骤 4 点击 **查看系统和故障排除详细信息...**的链接

默认情况下，此面板处于折叠状态。点击链接可展开折叠部分，以查看设备的 **系统详细信息** 和 **故障排除和链接** 。系统详细信息包括：

- **版本**： FirePOWER 软件版本。
- **型号**： 设备型号。
- **模式**： 防火墙模式。Firepower 威胁防御设备面向普通防火墙接口支持两种防火墙模式：路由模式和透明模式。
- **VDB**： 思科漏洞数据库 (VDB) 版本。
- **SRU**： 入侵规则集版本。

- **Snort**： Snort 版本。

步骤 5 有以下故障排除选项可供选择：

- 生成故障排除文件；请参阅 为特定系统功能生成故障排除文件 ， 第 283 页
- 生成和下载高级故障排除文件；请参阅 下载高级故障排除文件 ， 第 284 页。
- 创建和修改运行状况策略；请参阅 创建运行状况策略 ， 第 240 页。
- 创建和修改运行状况监控器警报；请参阅 创建运行状况监控器警报 ， 第 246 页。

查看设备运行状况监控器

您必须是管理员、运维或安全分析师用户才能执行此程序。

设备运行状况监控器提供防火墙设备的运行状态的详细视图。设备运行状况监控器会编译设备指标，并在一系列控制面板中提供设备的运行状况和趋势。

过程

步骤 1 选择**系统**（⚙） > **运行状况** > **监控**。

使用监控导航窗格访问设备特定的运行状况监控器。

步骤 2 在设备列表中，点击 **展开**（>） 和 **折叠**（⌄） 以展开和折叠受管设备列表。

步骤 3 在设备名称右侧的页面顶部的警报通知中查看设备的**运行状况警报 (Health Alerts)**。

将鼠标指针悬停在**运行状况警报 (Health Alerts)** 上可查看设备的运行状况摘要。弹出窗口显示前五个运行状况警报的截断摘要。点击弹出窗口可打开运行状况警报摘要的详细视图。

步骤 4 您可以从右上角的下拉列表中配置时间范围。您可以更改时间范围以反映短至前一小时（默认），或长至前一年的时间周期信息。从下拉列表中选择**自定义 (Custom)** 以配置自定义开始和结束日期。

点击刷新图标可将自动刷新设置为 5 分钟或关闭自动刷新。

步骤 5 点击 **显示部署信息**（  ） 图标，在趋势图上根据所选时间范围显示部署重叠。

显示部署信息（  ） 图标指示所选时间范围内的部署数量。垂直条带表示部署开始和结束时间。在多个部署的情况下，将显示多个频段/行。点击虚线顶部的图标可查看部署详细信息。

步骤 6 默认情况下，设备监控器会在多个预定义的控制面板中报告这些运行状况和性能。指标控制面板包括：

- 概述 — 突出显示其他预定义控制面板中的关键指标，包括CPU、内存、接口、连接统计信息；以及磁盘使用情况和关键进程信息。
- CPU - CPU 利用率，包括按进程和物理核心划分的 CPU 使用情况。
- 内存 - 设备内存使用率，包括数据平面和 Snort 内存使用率。

- 接口 - 接口状态和汇聚流量统计信息。
- 连接 - 连接统计信息（例如大象流、活动连接、峰值连接等）和 NAT 转换计数。
- Snort - 与 Snort 进程相关的统计信息。

您可以通过点击标签浏览各种指标控制面板。有关支持的设备指标的全面列表，请参阅Firepower 设备指标，第 255 页。

步骤 7 点击设备监控器右上角的加号 (+)，通过从可用指标组构建您自己的变量集来创建自定义关联控制面板；请参阅关联设备指标，第 254 页。

关联设备指标

您必须是管理员、运维或安全分析师用户才能执行此程序。

设备运行状况监控器包括一系列用于预测和响应系统事件的关键 Firepower 设备指标。任何 Firepower 设备的运行状况都可以通过这些报告的指标来确定。

默认情况下，设备监控器会在多个预定义的控制面板中报告这些指标。这些控制面板包括：

- 概述 — 突出显示其他预定义控制面板中的关键指标，包括 CPU、内存、接口、连接统计信息；以及磁盘使用情况和关键进程信息。
- CPU - CPU 利用率，包括按进程和物理核心划分的 CPU 使用情况。
- 内存 - 设备内存使用率，包括数据平面和 Snort 内存使用率。
- 接口 - 接口状态和汇聚流量统计信息。
- 连接 - 连接统计信息（例如大象流、活动连接、峰值连接等）和 NAT 转换计数。
- Snort - 与 Snort 进程相关的统计信息。
- ASP 丢包 - 与加速安全路径 (ASP) 性能和行为相关的统计信息。

您可以添加自定义控制面板来关联相互关联的指标。从预定义的关联组中选择，例如 CPU 和 Snort；或通过从可用指标组构建您自己的变量集来创建自定义关联控制面板。

开始之前

要在运行状况监控控制面板中查看和关联时间序列数据（设备指标），请启用 REST API（**设置** > **配置** > **REST API 首选项**）。

注释 关联设备指标仅适用于 威胁防御 6.7 及更高版本。因此，对于 6.7 之前的 威胁防御 版本，即使启用 REST API，运行状况监控控制面板也不会显示这些指标。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **监控**。

使用监控导航窗格访问设备特定的运行状况监控器。

步骤 2 在设备列表中，点击 **展开**（>）和 **折叠**（∨）以展开和折叠受管设备列表。

步骤 3 点击设备监控器右上角的加号 (+) 以添加新的控制面板。

步骤 4 从**选择关联组 (Select Correlation Group)** 下拉列表中，选择预定义的关联组或创建自定义组。

步骤 5 要从预定义的关联组创建控制面板，请选择该组，然后点击**添加 (Add)**。

- CPU - 数据平面
- CPU - Snort
- CPU - 其他
- 内存 - 数据平面
- 丢包

步骤 6 要创建自定义关联控制面板，请执行以下操作：

a) 选择**自定义 (Custom)**。

b) 或者，在**控制面板名称 (Dashboard Name)** 字段中输入唯一名称或接受默认名称。

c) 接下来，从 **选择指标组** 下拉列表中选择一个组，然后从 **选择指标** 下拉列表中选择相应的指标。

- 连接；有关可用指标，请参阅 连接组指标，第 257 页。
- CPU；有关可用指标，请参阅 CPU 组指标，第 255 页。
- 关键流程；有关可用指标，请参阅 关键进程组指标，第 262 页。
- 已部署的配置；有关可用指标，请参阅 已部署的配置组指标，第 261 页。
- 磁盘；有关可用指标，请参阅 磁盘组指标，第 261 页。
- 接口；有关可用指标，请参阅 接口组指标，第 257 页。
- Snort；有关可用指标，请参阅 Snort 组指标，第 258 页。
- ASP 丢包；有关可用指标，请参阅 ASP 丢弃指标，第 259 页。

步骤 7 点击 **添加指标** 以从另一个组中添加和选择指标。

步骤 8 要删除单个指标，请点击项目右侧的 **x**。点击删除图标（垃圾桶）可删除该组。

步骤 9 点击**添加 (Add)** 以完成工作流程并将控制面板添加到运行状况监控器。

步骤 10 您可以**编辑**或**删除**自定义关联控制面板。

Firepower 设备指标

以下各节介绍 Firepower 威胁防御设备提供的运行状况指标。

CPU 组指标

运行状况监控器跟踪与 CPU 使用率相关的统计信息，包括按进程和物理核心划分的 CPU 使用情况。

表 *25: CPU* 组指标

指标	说明	格式
控制平面	控制平面过去一分钟的平均 CPU 使用率。	%
数据平面	数据平面过去一分钟的平均 CPU 使用率。	%
Snort	Snort 进程最近一分钟的平均 CPU 使用率。	%
系统	最近一分钟系统进程的平均 CPU 使用率。	%
物理核心	最后一分钟所有核心的平均 CPU 使用率。	%

内存组指标

运行状况监控器跟踪与设备内存使用率相关的统计信息，包括数据平面和 Snort 内存使用情况。

表 *26:* 内存组指标

指标	说明	格式
缓冲区缓存	缓冲区缓存。	bytes
空闲	总可用内存。	bytes
最大数据平面	数据平面使用的最大内存。	bytes
最大 Snort	Snort 进程使用的最大内存。	bytes
Snort 最大切换	Snort 进程使用的最大交换内存。	bytes
剩余内存块 (1550)	1550 字节块中的可用内存。	数字
剩余内存块 (256)	256 字节块中的可用内存。	数字
已用系统	系统使用的总内存。	bytes
总数	总可用内存。	bytes
总计切换	可用于 swap 的总内存。	bytes
数据平面	数据平面使用的总内存。	bytes
数据平面使用百分比	数据平面使用内存百分比。	%
Snort 使用百分比	Snort 进程使用内存百分比。	%
用于交换的百分比	用于交换的内存百分比。	%
系统使用百分比	系统使用内存百分比。	%

指标	说明	格式
系统和 Swap 使用百分比	系统和交换空间组合使用内存百分比。	%
Snort	Snort 进程使用的总内存。	bytes
已使用切换	用于交换的总内存。	bytes
Snort 已使用的切换	Snort 进程使用的总交换内存。	bytes

接口组指标

运行状况监控器跟踪与设备接口相关的统计信息，包括接口状态和汇聚流量统计信息。

表 *27:* 接口组指标

指标	说明	格式
丢弃数据包	丢弃的数据包数。	数字
平均输入数据包大小	传入数据包的平均大小。	bytes
输入速率	总传入字节数。	bytes
输入包数	总传入数据包数。	数字
平均输出数据包大小	传出数据包的平均大小。	bytes
输出速率	传出总字节数。	bytes
输出包数	传出数据包总数。	数字
状态	接口的状态； 1 表示开启，0 表示关闭。	1 或 0

连接组指标

健康监控器跟踪与连接和 NAT 转换计数相关的统计。

表 *28:* 连接组指标

指标	说明	格式
大象流	显示活动大象流数。 大象流是指大到足以影响整体系统性能的连接。默认情况下，大象流是速率大于每 10 秒 1GB 的流。您可以使用 **系统支持大象流检测** 命令调整字节和时间阈值，以在威胁防御CLI中识别大象流。 **注释** 仅当超过字节和时间阈值时，流才被视为大象流。	数字
使用中的连接	显示正在使用的连接数。	数字
峰值连接	显示最大同时连接数。	数字
每秒连接总数	所有连接类型的每秒连接数。	数字
每秒 TCP 连接数	TCP 连接类型的每秒连接数。	数字
每秒 UDP 连接数	UDP 连接类型的每秒连接数。	数字
保留已启用的连接	在 Snort 进程关闭时保留路由和透明接口上的现有 TCP/UDP 连接。	数字
保留的连接	当前启用了保留连接的连接。	数字
保留启用最多的连接	保留的最大连接数。	数字
保留的连接峰值	保留的最大高峰连接数。	数字
NAT 转换	显示转换计数。	数字
NAT 转换峰值	一次显示并发转换的历史最大值。	数字

Snort 组指标

运行状况监控器跟踪与 Snort 进程相关的统计信息。

表 *29: Snort* 组指标

指标	说明	格式
阻止的列表流	Snort 在策略配置中丢弃的流数。	数字
被阻止的数据包	被阻止的数据包的数量。	数字

指标	说明	格式
被拒绝的流	被拒绝的流事件的数量。当数据平面决定在将流发送到 Snort 之前丢弃流时，数据平面进程会向 Snort 发送拒绝流事件	数字
流结束	当快速路径流结束时，数据平面会向 Snort 发送流结束事件。	数字
快速转发的流	由策略快速转发并因此未检查的流的数量。	数字
已丢弃转发自数据平面的帧	已丢弃转发自数据平面的帧数。	数字
已丢弃注入数据包	Snort 添加到已丢弃的流量流的数据包数。	数字
注入的数据包	Snort 创建并添加到流量流的数据包数。例如，如果配置具有重置操作的阻止，Snort 会生成数据包以重置连接。	数字
实例 (Instances)	Snort 实例数（进程）。	数字
数据包接收队列的利用率百分比	数据平面接收队列的队列利用率。	%
由于 Snort 繁忙而绕过的数据包	当 Snort 太忙而无法处理数据包时，绕过检测的数据包的数量。	数字
由于 Snort 关闭而绕过的数据包	Snort 关闭时绕过检测的数据包数量。	数字
由于 RX 队列已满而绕过的数据包	由于接收队列已满而绕过的数据包数。	数字
由于 TX 队列已满而绕过的数据包	由于传输队列已满而绕过的数据包数。	数字
通过的流	从数据平面发送到 Snort 的数据包数。	数字
流开始	流开始事件的数量。这些事件有助于 Snort 跟踪连接并报告连接事件。	数字

ASP 丢弃指标

运行状况监控器跟踪与加速安全路径 (ASP) 丢弃的数据包或连接相关的统计信息。

表 *30: ASP* 丢弃指标

指标	说明	格式
超出连接限制	计算超出连接限制时关闭的流数。	数字

指标	说明	格式
达到连接限制	统计在超出连接限制或主机连接限制时被丢弃的数据包数。	数字
L2 规则丢弃	统计由于第2层ACL而被拒绝的数据包的数量。	数字
L2 规则 VXLAN 丢弃	统计由于在应用第 2 层 ACL 检查时未能找到 VXLAN out_tag 而被拒绝的数据包数。	数字
NAT 逆向路径失败	统计拒绝尝试使用转换后的主机实际地址连接到转换后的主机的次数。	数字
NAT 失败	统计尝试创建 xlate 以转换 IP 或传输报头的失败次数。	数字
没有有效的 v4 邻接	对安全设备尝试获取邻接关系但无法获取下一跳 (IPv4) 的 MAC 地址时丢弃的数据包的数量进行计数。	数字
没有有效的 v6 邻接	对安全设备尝试获取邻接关系但无法获取下一跳 (IPv6) 的 MAC 地址时丢弃的数据包的数量进行计数。	数字
被 Snort 列入阻止列表的数据包；被 Snort 阻止的数据包	对 Snort 模块请求的数据包进行计数。	数字
丢帧 - Snort 繁忙；丢帧 - Snort down；丢帧 - Snort 丢弃	对由于 Snort 模块繁忙且无法处理帧而丢弃的帧进行计数； Snort模块已关闭； Snort模块请求丢弃。	数字
达到调度队列限制	计算设备的负载均衡ASP调度程序达到其队列限制的次数。当尝试更多数据包时，会发生尾部丢弃，并且此计数器递增。	数字
目标 MAC L2 查找失败	计算失败的第 2 层目的 MAC 地址查找的次数。一旦查找失败，设备将开始目标MAC发现过程，并尝试通过 ARP 和/或 ICMP 消息查找主机的位置。	数字
检测失败	计算设备未能启用网络处理器对连接执行的协议检测的次数。原因可能是内存分配失败，或者对于 ICMP 错误信息，设备无法找到与 ICMP 错误信息中嵌入的帧相关的任何已建立的连接。	数字
NAT 无 PAT 池的 xlate	统计未找到目标与PAT池中的映射地址相匹配的连接的现存 xlate 的次数。	数字

指标	说明	格式
无主机路由	计算安全设备尝试从接口发送数据包但未在路由表中找到该接口的路由的次数。	数字
丢包数占排队数据包数的比例	计算设备收到已在无序数据包队列中的重新传输的数据包时丢弃的数据包数。	数字
已排队等待检测的数据段数达到上限	对于流，排队等待检查器的数据包数量已达到限制，因此会终止该流。	数字
被 Snort 阻止或列入阻止列表	统计 Snort 模块所请求的数据包被丢弃的次数。	数字
被 Snort 静默丢弃的数据包	统计Snort模块请求的数据包被静默丢弃的次数。	数字
未同步的第一个 TCP 数据包	统计作为非拦截和非固定连接的首个数据包收到非 SYN 数据包的次数。	数字

已部署的配置组指标

运行状况监控器跟踪有关已部署配置的统计信息，例如 IPS 规则数和 ACE 数。

表 *31:* 已部署的配置组指标

指标	说明	格式
ACE 数	访问控制条目 (ACE) 数或规则。访问控制列表 (ACL) 由一个或多个 ACE 组成。	数字
规则数	入侵策略中的规则数量。	数字

磁盘组指标

运行状况监控器跟踪与设备磁盘使用情况相关的统计信息，包括每个分区的磁盘大小和磁盘利用率。

表 *32:* 磁盘组指标

指标	说明	格式
总数	设备磁盘的总大小。	bytes
已使用	设备磁盘上使用的总空间。	bytes
/ngfw 使用量 (%)	/ngfw 分区使用的磁盘空间百分比。	%
/ngfw/Volume 使用量 (%)	/ngfw/Volume 分区使用的磁盘空间百分比。	%
/dev/cgroups 使用量 (%)	/dev/cgroups 分区使用的磁盘空间百分比。	%
/mnt/disk0 使用量 (%)	/mnt/disk0 分区使用的磁盘空间百分比。	%

指标	说明	格式
/var/volatile 使用量 (%)	/var/volatile 分区使用的磁盘空间百分比。	%

关键进程组指标

运行状况监控器跟踪与受管进程的进程重启相关的统计信息。此外，对于每个关键进程，运行状况监控器会跟踪 CPU 利用率、内存利用率、正常运行时间和状态。

表 *33:* 关键进程组指标

指标	说明	格式
CPU 利用率	控制平面和数据平面组合的平均CPU 使用率（最后一分钟）。	%
重新启动计数	控制平面过去一分钟的平均 CPU 使用率。	%
状态	数据平面过去一分钟的平均 CPU 使用率。	%
正常运行时间	Snort 进程最近一分钟的平均 CPU 使用率。	%
已用内存	最近一分钟系统进程的平均 CPU 使用率。	%

运行状况监控器状态类别

可用状态类别按严重性在下表中列出。

表 *34:* 运行状况指示灯

状态级别	状态图标	饼形图中的状态颜色	说明
错误	**错误**（  ）	黑色	表示设备中的至少一个运行状况监控模块出现故障，并且自故障发生后未能成功重新运行。请与您的技术支持代表联系以获得对运行状况监控模块的更新。
严重	**严重**（  ）	红色	表示对于设备中的至少一个运行状况模块而言，已超过严重限值，并且该问题尚未解决。
警告	**警告**（  ）	黄色	表示对于设备中的至少一个运行状况模块而言，已超过警告限值，并且该问题尚未解决。 此状态还表示一种过渡状态，在这种状态下，由于设备配置发生更改，所需数据暂时不可用或无法处理。根据监控周期，此过渡状态会自动更正。

状态级别	状态图标	饼形图中的状态颜色	说明
正常	**正常**（  ）	绿色	表示设备中的所有运行状况模块都在应用于该设备的健康策略中配置的限值内运行。
已恢复	**已恢复**（  ）	绿色	表示设备中的所有运行状况模块（包括处于“严重”或“警告”状态的模块）都在应用于该设备的运行状况策略中配置的限值内运行。
禁用	**已禁用**（  ）	蓝色	表示设备被禁用或排除，设备没有应用运行状况策略，或者设备当前无法访问。

运行状况事件视图

通过“运行状况事件视图”页面，您可以查看由运行状况监控器在 管理中心日志运行状况事件中记录的运行状况事件。完全可自定义的事件视图使您可以快速轻松地分析运行状况监控器所收集的运行状况事件。可以搜索事件数据，以便轻松访问可能与正调查的事件有关的其他信息。如果您了解每个运行状况模块测试的条件，就可以更有效地配置运行状况事件的警报。

可以在运行状况事件视图页面执行许多标准事件视图功能。

查看运行状况事件

您必须是管理员、运维或安全分析师用户才能执行此程序。

“运行状况事件表视图”(Table View of Health Events) 页面提供指定设备上所有运行状况事件的列表。

当您在管理中心中从 Health Monitor 页面访问运行状况事件时，您可以检索所有受管设备的所有运行状况事件。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

提示 您可以为该视图添加书签，使您可以返回到其中包含事件的运行状况事件表的运行状况事件工作流程页面。加入书签的视图检索您当前正查看的时间范围内的事件，但是如果需要，您可以稍后修改时间范围以使用较新的信息更新该表。

过程

选择**系统**（⚙）> **运行状况** > **事件**。

提示　如果您使用的自定义工作流程不包括运行状况事件表视图，请点击（**切换工作流程**）**([switch workflow])**。在“选择工作流程”(Select Workflow) 页面上，点击**运行状况事件 (Health Events)**。

注释　如果未显示事件，您可能需要调整时间范围。

查看运行状况事件表

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**系统**（⚙）> **运行状况** > **事件**。

步骤 2 有以下选项可供选择：

- 书签 - 要将当前页面加入书签，以便可以快速返回到该页面，请点击**将此页面加入书签 (Bookmark This Page)**，提供书签的名称，然后点击**保存 (Save)**。
- 更改工作流程 - 要选择其他运行状况事件工作流程，请点击（**切换工作流程**）**([switch workflows])**。
- 删除事件 - 要删除运行状况事件，请选中要删除的事件旁边的复选框，然后点击**删除 (Delete)**。要删除当前受限制视图中的所有事件，请点击 **Delete All**，然后确认要删除所有事件。
- 生成报告 - 根据表视图中的数据生成报告 - 点击**报告设计器 (Report Designer)**。
- 修改 - 修改在“运行状况”(Health) 表视图中列出的事件的时间和日期范围。请注意，如果按时间限制事件视图，则在设备配置的时间窗口外生成的事件（无论是全局还是特定事件）可能显示在事件视图中。即使为设备配置了滑动时间窗口，也可能发生这种情况。
- 导航 - 浏览事件视图页面。
- 导航书签 - 要导航至书签管理页面，请点击任何事件视图中的**查看书签**。
- 导航其他 - 导航至其他事件表以查看关联事件。
- 排序 - 对显示的事件进行排序，更改事件表中显示的列，或者限制显示的事件
- 查看全部 - 要查看视图中所有事件的事件详细信息，请点击**查看全部 (View All)**。
- 查看详细信息 - 要查看与单个运行状况事件关联的详细信息，请点击事件左侧的向下箭头链接。
- 查看多个 - 要查看多个运行状况事件的事件详细信息，请选中与要查看其详细信息的事件对应的行旁边的复选框，然后点击**查看 (View)**。
- 查看状态 - 要查看特定状态的所有事件，请点击“状态”列中的“状态”以获取具有该状态的事件。

运行状况事件表

您在运行状况策略中选择启用的“运行状况监控”模块会运行各种测试，以确定设备运行状况。当运行状况满足您指定的标准时，系统将生成一个运行状况事件。

下表介绍在运行状况事件表中可以查看和搜索的字段。

表 *35:* 运行状况事件字段

字段	说明 (Description)
模块名称	指定生成要查看的运行状况事件的模块的名称。例如，要查看衡量 CPU 性能的事件，请键入 `CPU`。搜索应检索适用的 CPU 使用率和 CPU 温度事件。
测试名称 （仅限搜索）	生成事件的运行状况模块的名称。
时间 （仅限搜索）	运行状况事件的时间戳。
说明	生成事件的运行状况模块的描述。例如，当无法执行进程时生成的运行状况事件被标记为 `Unable to Execute`。
值	生成事件的运行状况测试所获得的结果值（单位数量）。 例如，如果只要其正在监控的设备使用的 CPU 资源达到 80% 或以上，管理中心就会生成运行状况事件，则该值可以是介于 80 到 100 之间的一个数字。
单位	结果的单位描述符。您可以使用星号 (*) 创建通配符搜索。 例如，如果其正在监控的设备使用的 CPU 资源达到 80% 或以上时，管理中心会生成运行状况事件，则单位描述符为百分号 (%)。
状态	为设备报告的状态（严重、黄色、绿色或已禁用）。
域	对于受管设备报告的运行状况事件，即报告运行状况事件的设备的域。对于管理中心报告的运行状况事件，即为`全局`。此字段只存在于多域部署中。
设备	报告运行状况事件的设备。

运行状况监控历史

功能	版本	详细信息
运行状况监控器 UI 修改	7.1	以下 UI 页面经过临时改进，以提高数据的可用性和显示效果： • 策略 • 排除 • 监控警报 新增/经修改的屏幕：**设置** > **运行状况** > **策略**、**设置** > **运行状况** > **排除**以及 **设置** > **运行状况** > **监控警报**。
象流检测	7.1	运行状况警报包含以下增强功能： • 连接统计信息包括活动的象流。 • 连接组指标包括活动的象流数。 思科 Firepower 2100 系列不支持象流检测功能。
已停用非托管磁盘使用率高 (high unmanaged disk usage) 警报。	7.0.6	“磁盘使用情况”(Disk Usage) 运行状况模块不再针对非托管磁盘使用率过高 (high unmanaged disk usage) 发出警报。升级后，您可能会继续看到这些警报，直到将运行状况策略部署到托管设备（停止显示警报）或升级设备（停止发送警报）。 **注释** 版本 7.0 – 7.0.5、7.1.x、7.2.0 – 7.2.3 和 7.3.x 继续支持这些警报。如果您的管理中心正在运行这些版本中的任何一个，您也可能会继续看到警报。

功能	版本	详细信息
新的运行状况模块	7.0	我们添加了以下运行状况模块： • AMP 连接状态：从 威胁防御监控 AMP 云连接。 • AMP Threat Grid 状态：从 威胁防御监控 AMP Threat Grid 云连接。 • ASP 丢弃：监控数据平面加速安全路径所放弃的连接。 • 高级 Snort 统计信息：监控与数据包性能、流计数器和流事件相关的 Snort 统计信息。 • 事件流状态：监控使用事件流转换器的第三方客户端应用的连接 • FMC 访问配置更改：监控直接在 管理中心上进行的访问配置更改。 • FMC HA 状态：监控主用和备用 管理中心 以及设备之间的同步状态。替换高可用性状态模块。 • FTD HA 状态：监控主用和备用 威胁防御 HA 对以及设备之间的同步状态。 • 文件系统完整性检查：如果系统启用了 CC 模式或 UCAPL 模式，则执行文件系统完整性检查。 • 流量分流：监控 Firepower 9300 和 4100 平台上的硬件流量分流统计信息。 • 命中计数：监控访问控制策略中特定规则的命中次数。 • MySQL 状态：监控 MySQL 数据库的状态。 • NTP 状态：监控托管设备的 NTP 时钟同步状态。 • RabbitMQ 状态：监控 RabbitMQ 消息传递代理的状态。 • 路由统计信息：监控来自 威胁防御的 IPv4 和 IPv6 路由信息。 • SSE 连接状态：从 威胁防御监控 SSE 云连接。 • Sybase 状态：监控 Sybase 数据库的状态。 • 未解析组监控器：监控访问控制策略中使用的未解析组。 • VPN 统计信息：监控站点间和远程访问 VPN 隧道统计信息。 • xTLS 计数器：监控 xTLS/SSL 流、内存和缓存有效性

功能	版本	详细信息
运行状况监控增强功能	7.0	运行状况监控器添加了以下增强功能： • 增强的 管理中心 控制面板，提供以下内容的摘要视图： • 高可用性 • 事件速率和容量 • 流程运行状况 • CPU 阈值 • Memory • 接口速率 • 磁盘使用情况 • 增强型 威胁防御 控制面板： • 裂脑情景的运行状况警报 • 新运行状况模块提供的其他运行状况指标
新的运行状况模块	6.7	不再使用 CPU 使用率模块。相反，请参阅以下模块了解 CPU 使用情况： • CPU 使用情况（每个核心）：监控所有核心上的 CPU 使用情况。 • CPU 使用率数据平面：监控设备上所有数据平面进程的平均 CPU 使用率。 • CPU 使用率 Snort：监控设备上 Snort 进程的平均 CPU 使用率。 • CPU 使用率系统：监控设备上所有系统进程的平均 CPU 使用率。 添加了以下模块以跟踪统计信息： • 连接统计信息：监控连接统计信息和 NAT 转换计数。 • 关键进程统计信息：监控关键进程的状态、资源消耗和重新启动计数。 • 部署的配置统计信息：监控有关已部署配置的统计信息，例如 ACE 数、IPS 规则数。 • Snort 统计信息：监控事件、流和数据包的 Snort 统计信息。 添加了以下模块以跟踪内存使用情况： • 内存使用率数据平面：监控数据平面进程使用的已分配内存的百分比。 • 内存使用情况 Snort：监控 Snort 进程使用的已分配内存的百分比。

功能	版本	详细信息
运行状况监控增强功能	6.7	运行状况监控器添加了以下增强功能： • 运行状况摘要页面，提供 Firepower 管理中心和 管理中心 管理的所有设备的运行状况概览视图。 • 监控导航窗格允许您导航设备层次结构。 • 受管设备单独列出，或根据其地理位置、高可用性或集群状态（如果适用）分组。 • 您可以从导航窗格查看各个设备的运行状况监控器。 • 用于关联相关指标的自定义控制面板。从预定义的关联组中选择，例如 CPU 和 Snort；或通过从可用指标组构建您自己的变量集来创建自定义关联控制面板。
功能移动至设备模块上的威胁数据更新	6.7	不再使用本地恶意软件分析模块。有关此信息，请参阅设备上的威胁数据更新。 以前由安全情报模块和 URL 过滤模块提供的一些信息现在由设备上的威胁数据更新模块提供。
新增运行状况模块：配置内存分配	7.0 6.6.3	版本 6.6.3 改进了设备内存管理，并引入了新的运行状况模块：配置内存分配。 当已部署的配置的大小使设备面临内存耗尽的风险，此模块会发出警报。警报会显示您的配置需要多少内存，以及超出可用内存的数量。如果发生此情况，请重新评估您的配置。通常来说，您可以减少访问控制规则或入侵策略的数量或降低其复杂性。
URL 过滤监控器改进	6.5	如果 管理中心 无法注册到思科云，URL 过滤监控模块现在会发出警报。
URL 过滤监控器改进	6.4	您可以配置 URL 过滤监控器警报的时间阈值。
新增运行状况模块：设备中威胁数据更新	6.3	新增模块**设备中威胁数据更新**。 如果设备用于检测威胁的某些情报数据和配置未在您指定的时间段内于设备上更新，则此模块会提醒您。

第 13 章

故障排除

以下主题描述如何诊断您可能在 Firepower 系统中遇到的问题：

故障排除的首要步骤

- 在您进行更改以尝试修复问题之前，请生成故障排除文件以捕获原始问题。请参阅用于故障排除的运行状况监控器报告， 第 283 页及其子节。

  如果您需要联系思科 TAC 以获得支持，则您可能需要此故障排除文件。

- 可以通过查看“消息中心”中的错误和警告消息开始调查。请参阅 系统消息， 第 271 页

- 可以在您的产品的产品文档页面上的“故障排除和警报”标题下，查找适用的技术说明和其他故障排除资源。请参阅故障排除的首要步骤， 第 271 页。

系统消息

当需要跟踪发生在 Firepower 系统中的问题时，请从消息中心开始调查。通过此功能，可以查看 Firepower 系统持续生成的有关系统活动和状态的消息。

要打开消息中心，请点击位于主菜单中“部署”菜单旁边的“系统状态”图标。根据系统状态，此图标可采用以下形式之一：

- - 指示系统上存在一个或多个错误和任意数量的警告。
- - 指示系统上存在一个或多个警告而没有错误。
- - 指示系统上不存在任何警告或错误。

如果随该图标显示数字，则其指示错误或警告消息的当前总数。

要关闭消息中心，请点击 Firepower 系统 Web 界面内其外部的任意位置。

除消息中心以外，Web 界面也会显示对您的活动和日常系统活动的立即响应中的弹出通知。某些弹出通知在五秒后自动消失，而其他通知则“粘滞”，意味着它们会显示直至您通过点击 **解除**（）明确将其消除为止。点击通知列表顶部的**消除 (Dismiss)** 链接以一次性解除所有通知。

提示 将光标悬停在非粘滞弹出通知的上方会导致其粘滞。

系统根据用户的许可证、域和访问角色确定在弹出通知和消息中心内向其显示哪些消息。

消息类型

消息中心显示消息报告系统活动和状态，分为三个不同选项卡：

部署

此选项卡显示与系统中的每个设备的配置部署相关的当前状态，按域分组。系统在此选项卡上报告以下部署状态值。通过点击**显示历史记录**，可以获得有关部署作业的其他详细信息。

- 运行（**旋转**）- 该配置处于部署过程中。
- **成功** - 该配置已成功部署。
- **警告**（） - 警告部署状态利用 **警告系统状态图标**为所显示的消息计数提供帮助。
- **失败** - 该配置未能部署；请参阅 过时策略，第 150 页。失败的部署利用 **错误系统状态图标** 为所显示的消息计数提供帮助。

升级

此选项卡显示与托管设备的软件升级任务相关的当前状态。系统在此选项卡上报告以下升级状态值：

- **正在进行 (In progress)** - 表示升级任务正在进行。
- **已完成 (Completed)** - 表示软件升级任务已成功完成。
- **失败 (Failed)** - 表示软件升级任务未能完成。

运行状况

此选项卡显示系统中每个设备的当前运行状况信息，按域分组。运行状况由运行状况模块生成，如关于运行状况监控，第 229 页中所述。系统在此选项卡上报告以下运行状况状态值：

- **警告**（  ） - 表示对于设备中的运行状况模块而言，已超过警告限值，并且该问题尚未解决。“运行状况监控”页面利用 **黄色三角形**（  ）来指示这些状况。警告状态利用 **警告系统状态图标**为所显示的消息计数提供帮助。
- **严重**（  ） - 表示对于设备中的运行状况模块而言，已超过严重限值，并且该问题尚未解决。“运行状况监控”(Health Monitor) 页面利用 **严重**（  ） 图标来指示这些状况。严重状态利用 **错误系统状态图标**为所显示的消息计数提供帮助。
- **错误**（  ） - 表示设备中的运行状况监控模块出现故障，并且自故障发生后未能成功重新运行。“运行状况监控”页面利用 **错误图标**来指示这些状况。错误状态利用 **错误系统状态图标**为所显示的消息计数提供帮助。

可以点击“运行状况”(Health) 选项卡中的链接来查看有关“运行状况监控”(Health Monitor) 页面的详细信息。如果没有当前运行状况条件，“运行状况”(Health) 选项卡不显示消息。

任务

某些任务（例如配置备份或更新安装）需要一些时间来完成。此选项卡显示这些长时间运行任务的状态，并且可以包括由您或系统中的其他用户（如果您有适合的访问权限）发起的任务。此选项卡根据每条消息的最新更新时间，按时间倒序显示消息。某些任务状态消息包括有关所述任务的更详细信息的链接。系统在此选项卡上报告以下任务状态值：

- **等待()** - 表示等待另一个正在进行的任务完成后再运行的任务。此消息类型显示更新进度条。
- **运行** - 表示正在进行的任务。此消息类型显示更新进度条。
- **重试** - 表示自动重试的任务。请注意，并非所有的任务都可以重试。此消息类型显示更新进度条。
- **成功** - 表示已成功完成的任务。
- **失败** - 表示未成功完成的任务。失败的任务利用 **错误系统状态图标**为所显示的消息计数提供帮助。
- **停止或暂停** - 表示由于系统更新而中断的任务。停止的任务不能恢复。恢复正常操作后，再次启动任务。
- 已跳过 - 正在进行的进程阻止了任务的启动。重试以启动任务。

当新任务开始时，此选项卡中显示新消息。随着任务完成（状态成功、失败或停止），此选项卡继续以指示的最终状态显示消息，直至删除它们。思科建议您删除消息以减少“任务”(Tasks) 选项卡和消息数据库的混乱。

消息管理

从“消息中心”(Message Center) 可以执行以下操作：

- 选择以显示弹出通知。
- 显示系统数据库中的更多任务状态消息（如有任何尚未移除的此类消息）。
- 移除单个任务状态消息。（此操作会影响到可以查看已移除消息的所有用户。）
- 批量移除任务状态消息。（此操作会影响到可以查看已移除消息的所有用户。）

提示 思科建议您定期在“任务”(Task) 选项卡中移除积累的任务状态消息，使显示画面和数据库减少凌乱感。当数据库中的消息数接近 100,000 条时，系统会自动删除您已移除的任务状态消息。

查看基本系统信息

“关于”(About) 页面显示有关设备的信息，包括型号、序列号和 Firepower 系统各组件的版本信息。此页面还包含思科的版权信息。

过程

步骤 1 点击页面顶部工具栏中的**帮助 (Help)**。

步骤 2 选择**关于 (About)**。

查看设备信息

过程

选择**系统**（⚙）> **配置**。

管理系统消息

过程

步骤 1 点击**通知 (Notifications)** 以显示消息中心。

步骤 2 有以下选项可供选择：

- 点击 **部署** 以查看与配置部署相关的消息。请参阅查看部署消息，第 275 页。您必须是 Admin 用户或者拥有**将配置部署到设备**的权限才能查看这些消息。
- 点击**升级 (Upgrades)** 以查看与设备升级任务相关的消息。请参阅“查看升级消息”。请参阅查看升级消息。您必须是管理员用户或者拥有**更新**权限才能查看这些消息。
- 点击 **运行状况** 以查看与您的 管理中心 和在其中注册的设备相关的消息。请参阅查看运行状况消息，第 277 页。您必须是管理员用户或者拥有 **运行状况** 的权限才能查看这些消息。
- 点击 **任务** 以查看或管理与长期运行任务相关的消息。请参阅查看任务消息，第 277 页或管理任务消息，第 278 页。每个人都可以看到自己的任务。要查看其他用户的任务，您必须是 Admin 用户或拥有**查看其他用户的任务**权限。
- 点击**显示通知 (Show notifications)** 滑块以启用或禁用弹出通知显示。

查看部署消息

您必须是 Admin 用户或者拥有**将配置部署到设备**的权限才能查看这些消息。

过程

步骤 1 点击“系统状态”(System Status) 以显示消息中心。

步骤 2 点击**部署 (Deployments)**。

步骤 3 有以下选项可供选择：

- 点击**总计 (total)** 以查看所有当前部署状态。
- 点击状态值以只查看具有该部署状态的消息。
- 将光标悬停在消息的已逝时间指标上（例如，**1m 5s**）可查看已逝时间，以及部署的开始和停止时间。

步骤 4 点击**显示部署历史 (show deployment history)** 查看有关部署作业的更多详细信息。

Deployment History 表在左侧列中以时间倒序列出部署作业。

a) 选择部署作业。

右侧列中的表显示该作业中包含的各个设备，以及每个设备的部署状态。

b) 要查看设备的响应以及部署期间发送到设备的命令，请点击设备的**脚本 (Transcript)** 列中的下载图标。

该脚本包含以下各节：

- **Snort Apply** - 如果 Snort 相关的策略中有任何故障或响应，此部分中会显示消息。通常，该部分为空。
- **CLI Apply** - 此部分涵盖使用发送到 Lina 进程的命令配置的功能。
- **Infrastructure Messages** - 此部分显示不同部署模块的状态。

在 **CLI Apply** 部分中，部署脚本包括发送到设备的命令以及从该设备返回的任何响应。这些响应可以是信息性消息或错误消息。对于失败的部署，请查找指示命令错误的消息。如果您正在使用 FlexConfig 策略配置自定义的功能，则检查这些错误特别有用。这些错误可帮助您纠正尝试配置这些命令的 FlexConfig 对象中的脚本。

注释 为托管功能发送的命令与从 FlexConfig 策略生成的命令之间没有显著差异。

例如，以下序列显示 管理中心 发送了命令来为 GigabitEthernet0/0 配置外部逻辑名。设备的响应是自动将安全级别设置为 0。威胁防御 不使用任何安全级别。

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

查看升级消息

您必须是管理员用户或者拥有**更新**权限才能查看这些消息。

过程

步骤 1 点击**通知 (Notifications)** 以显示消息中心。

步骤 2 点击**升级 (Upgrades)**。

步骤 3 可以执行以下操作：

- 点击**总计**以查看所有当前升级任务。
- 点击状态值以只查看具有该状态的消息。
- 点击**设备管理 (Device Management)**，了解有关升级任务的更多详细信息。

查看运行状况消息

您必须是管理员用户或者拥有 **运行状况** 的权限才能查看这些消息。

过程

步骤 1 点击“系统状态”(System Status) 以显示消息中心。

步骤 2 点击 **运行状况**。

步骤 3 有以下选项可供选择：

- 点击 **总计** 以查看所有当前运行状态。
- 点击状态值以只查看具有该状态的消息。
- 将光标悬停在消息的相对时间指标上（例如，**3 天前**）可查看该消息最新更新的时间。
- 要查看特殊信息的详细运行状态信息，请点击该消息。
- 要查看“运行状况监控器”(Health Monitor) 页面上的完整运行状态，请点击 **运行状况监控器**。

查看任务消息

每个人都可以看到自己的任务。要查看其他用户的任务，您必须是 Admin 用户或拥有**查看其他用户的任务**权限。

过程

步骤 1 点击“系统状态”(System Status) 以显示消息中心。

步骤 2 点击**任务 (Tasks)**。

步骤 3 有以下选项可供选择：

- 点击**总计 (total)**以查看所有当前任务状态。
- 点击状态值以只查看具有该状态的任务的消息。

  注释 已停止任务的消息仅显示在任务状态消息总列表中。您无法过滤已停止任务。

- 将光标悬停在消息的相对时间指标上（例如，**3 天前**）可查看该消息最新更新的时间。
- 点击消息中的任何链接，查看有关该任务的详细信息。
- 如果可显示更多任务状态消息，请点击消息列表底部的**获取更多消息 (Fetch more messages)** 以对其进行检索。

管理任务消息

每个人都可以看到自己的任务。要查看其他用户的任务，您必须是 Admin 用户或拥有**查看其他用户的任务**权限。

过程

步骤 1 点击“系统状态”(System Status) 以显示消息中心。

步骤 2 点击“任务”(Tasks)。

步骤 3 有以下选项可供选择：

- 如果可显示更多任务状态消息，请点击消息列表底部的**获取更多消息 (Fetch more messages)** 以对其进行检索。
- 要移除一条已完成的任务的消息（状态为已停止、成功或失败），请点击该消息旁边的 **删除**（ ）。
- 要移除已完成的所有任务的全部消息（状态为已停止、成功或失败），请使用**总数 (total)** 过滤消息，然后点击**移除所有已完成的任务 (Remove all completed tasks)**。
- 要移除已成功完成的所有任务的全部消息，请使用**成功 (success)** 过滤消息，然后点击**移除所有成功的任务 (Remove all successful tasks)**。
- 要移除已失败的所有任务的全部消息，请使用**失败 (failure)** 过滤消息，然后点击**移除所有失败的任务 (Remove all failed tasks)**。

运行状况监控器警报的内存使用阈值

内存使用率情况模块将设备的内存使用率与为模块配置的限值进行对比，并在使用率超过该级别时发出警报。模块监控来自受管设备和 FMC 本身的数据。

内存使用率的两个可配置阈值（严重和警告）可设置为已用内存的百分比。当超过这些阈值时，系统将生成具有指定严重性级别的运行状况警报。但是，运行状况警报系统不会以准确的方式计算这些阈值。

使用高内存设备时，某些进程预计会使用比低内存占用的设备更大的总系统内存百分比。设计的目的是尽可能多地使用物理内存，同时为辅助进程留出少量可用内存。

比较两台设备，一台有 32 GB 内存，一台有 4 GB 内存。在具有 32 GB 内存的设备中，5% 内存 (1.6GB) 是比具有 4 GB 内存的设备（4GB 的 5% = 200MB）留给辅助进程更大的内存值。

为了说明某些进程使用系统内存的百分比较高，FMC 会计算总内存以包括总物理内存和总交换内存。因此，用户配置的阈值输入的强制内存阈值可能会导致运行状况事件，其中事件的“值”列与为确定超出阈值而输入的值不匹配。

下表显示用户输入阈值和强制阈值的示例，具体取决于安装的系统内存。

注释 此表中的值为示例。您可以使用此信息外推与此处显示的已安装 RAM 不匹配的设备的阈值，也可以联系 Cisco TAC 进行更精确的阈值计算。

表 *36:* 基于已安装 ***RAM*** 的内存使用率阈值

用户输入阈值	每个安装的内存 (RAM) 的实施阈值			
	4 GB	**6 GB**	**32 GB**	**48 GB**
10%	10%	34%	72%	81%
20%	20%	41%	75%	83%
30%	30%	48%	78%	85%
40%	40%	56%	81%	88%
50%	50%	63%	84%	90%
60%	60%	70%	88%	92%
70%	70%	78%	91%	94%
80%	80%	85%	94%	96%
90%	90%	93%	97%	98%
100%	100%	100%	100%	100%

磁盘使用率和事件消耗情况运行状况监控警报

硬盘使用状况模块将受管设备的硬盘驱动器和恶意软件存储包中的磁盘使用率与为该模块配置的限值进行对比，并在使用率超过为模块配置的百分比时发出警报。基于模块阈值，当系统删除过多的监控磁盘使用类别的文件，或者当这些类别以外的磁盘使用率达到过高级别时，该模块也发出警报。

本主题介绍磁盘使用状况运行状况模块生成的两个运行状况警报的症状和故障排除指南：

- 频繁事件消耗
- 未处理事件消耗

磁盘管理器进程管理设备的磁盘使用情况。磁盘管理器监控的每种文件类型都分配有一个孤岛。根据系统上可用的磁盘空间量，磁盘管理器会为每个孤岛计算高水位线（HWM）和低水位线（LWM）。

要显示系统每个部分（包括孤岛、低水位线和高水位线）的磁盘使用情况详细信息，使用 **show disk-manager** 命令。

示例

以下是磁盘管理器信息的示例。

```
> show disk-manager
Silo                                Used        Minimum     Maximum
Temporary Files                     0 KB        499.197 MB  1.950 GB
Action Queue Results                0 KB        499.197 MB  1.950 GB
User Identity Events                0 KB        499.197 MB  1.950 GB
UI Caches                           4 KB        1.462 GB    2.925 GB
Backups                             0 KB        3.900 GB    9.750 GB
Updates                             0 KB        5.850 GB    14.625 GB
Other Detection Engine              0 KB        2.925 GB    5.850 GB
Performance Statistics              33 KB       998.395 MB  11.700 GB
Other Events                        0 KB        1.950 GB    3.900 GB
IP Reputation & URL Filtering       0 KB        2.437 GB    4.875 GB
Archives & Cores & File Logs        0 KB        3.900 GB    19.500 GB
Unified Low Priority Events         1.329 MB    4.875 GB    24.375 GB
RNA Events                          0 KB        3.900 GB    15.600 GB
File Capture                        0 KB        9.750 GB    19.500 GB
Unified High Priority Events        0 KB        14.625 GB   34.125 GB
IPS Events                          0 KB        11.700 GB   29.250 GB
```

运行状况警报格式

当 管理中心 上的运行状况监控进程运行时（每 5 分钟一次或触发手动运行）时，磁盘使用情况模块会查看diskmanager.log文件，如果满足正确的条件，则会触发相应的运行状况警报。

这些运行状况警报的结构如下：

- *<SILO NAME>*的频繁消耗
- 来自 *<SILO NAME>*的未处理事件的消耗

例如，

- 频繁消耗低优先级事件
- 来自低优先级事件中的未处理事件的消耗

任何孤岛都可能会生成 *<SILO NAME>*频繁消耗 运行状况警报。但是，最常见的是与事件相关的警报。在事件孤岛中，通常会看到 低优先级事件 ，因为这些类型的事件是由设备更频繁地生成的。

频繁消耗 *<SILO NAME>* 当与事件相关的孤岛相关联时，事件的严重性级别为**警告** ，因为事件将排队发送到 管理中心。对于与事件无关的孤岛（例如 备份 孤岛），警报的严重性级别为 **严重** ，因为此信息会丢失。

重要事项 只有事件孤岛会生成 来自 *<SILO NAME>*的未处理事件的消耗 运行状况警报。此警报的严重性级别始终为 **严重** 。

除警报外，其他症状还包括：

- 管理中心 用户界面上的速度缓慢
- 事件丢失

常见故障排除场景

频繁消耗<*SILO NAME*> 事件是由于在孤岛中输入的数据过多而导致的。在这种情况下，磁盘管理器会在最后 5 分钟间隔内至少两次清除（清除）该文件。在事件类型孤岛中，这通常是由该事件类型的过多日志记录导致的。

在 来自 <*SILO NAME*>的未处理事件的消耗 运行状况警报，这也可能是事件处理路径中的瓶颈导致的。

这些磁盘使用率警报存在三个潜在瓶颈：

- 日志记录过多 - 威胁防御 上的事件处理程序进程超额订用（其读取速度比 Snort 写入的速度慢）。
- Sftunnel 瓶颈-事件接口不稳定或超订用。
- SFDataCorrelator 瓶颈 - 管理中心 和托管设备之间的数据传输通道超订用。

过多日志记录

此类运行状况警报的最常见原因之一是输入过多。从 **show disk-manager** 命令中收集的低水位线（LWM）和高水位线（HWM）之间的差异显示，该筒仓中有多少空间可用于从LWM（刚耗尽）到HWM值。如果事件频繁耗尽（有或没有未处理的事件），首先要检查的是日志记录配置。

- 检查重复日志记录-如果您查看 管理中心上的相关器 *perfstats*，则可以识别重复日志记录场景：

  ```
  admin@FMC:~$ sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
  ```

- 检查 ACP 的日志记录设置-检查访问控制策略（ACP）的日志记录设置。如果同时记录连接的“开始”和“结束”，则仅记录结束，因为它将包括记录开始时的所有内容，并减少事件数量。

通信瓶颈-Sftunnel

Sftunnel 负责 管理中心 和托管设备之间的加密通信。事件通过隧道发送到 管理中心。托管设备和 管理中心 之间的通信信道 (sftunnel) 中的连接问题和/或不稳定可能是由于：

- Sftunnel 关闭或不稳定（振荡）。

  确保 管理中心 和托管设备在其 TCP 端口 8305 上的管理接口之间具有可访问性。

  sftunnel 进程应稳定且不应意外重启。通过检查 **/var/log/message** 文件并搜索包含 ***sftunneld*** 字符串的消息来验证此项。

- Sftunnel 已超额订用。

  查看来自健康监控器的趋势数据，并查找 管理中心管理接口超订用的迹象，这可能是管理流量激增或持续超订用。

作为 Firepower-eventing 的辅助管理接口使用。要使用此接口，您必须在 威胁防御 CLI 上使用 **configure network management-interface** 命令来配置其 IP 地址和其他参数。

通信瓶颈 - SFDataCorrelator

SFDataCorrelator 管理 管理中心 和托管设备之间的数据传输；在 管理中心上，它会分析系统创建的二进制文件以生成事件，连接数据和网络映射。第一步是查看 **diskmanager.log** 文件，了解要收集的重要信息，例如：

- 消耗的频率。
- 耗尽未处理事件的文件数。
- 发生未处理事件的情况。

每次磁盘管理器进程运行时，都会在其自己的日志文件（位于 **[/ngfw]/var/log/diskmanager.log**下）为每个不同的孤岛生成一个条目。从 diskmanager.log（CSV 格式）收集的信息可用于帮助缩小搜索范围。

额外故障排除步骤：

- 该 **stats_unified.pl** 命令可帮助您确定托管设备是否确实有一些数据需要发送到 管理中心。当托管设备和 管理中心 遇到连接问题时，可能会发生这种情况。受管设备将日志数据存储到硬盘驱动器上。

  ```
  admin@FMC:~$ sudo stats_unified.pl
  ```

- **manage_proc.pl** 命令可以在 管理中心 端重新配置相关器。

  ```
  root@FMC:~# manage_procs.pl
  ```

在联系 Cisco 技术支持中心 (TAC) 之前 。

强烈建议您在联系 Cisco TAC之前收集以下物品：

- 看到的运行状况警报的截图。
- 对从 管理中心生成的文件进行故障排除。
- 对从受影响的受管设备生成的文件进行故障排除。

  首次发现问题的日期和时间。

- 有关最近对策略所做的任何更改的信息（如果适用）。

  stats_unified.pl 命令的输出，如 通信瓶颈 - SFDataCorrelator ， 第 282 页中所述。

用于故障排除的运行状况监控器报告

某些情况下，如果您的设备有问题，支持人员可能要求您提供故障排除文件以帮助诊断该问题。系统可以使用以特定功能区域为目标的信息生成故障排除文件，以及您可与支持人员合作检索的高级故障排除文件。您可以选择下表中列出的任何选项，为特定功能定制故障排除文件的内容。

请注意，在所报告的数据方面，某些选项重叠，但是无论您选择什么选项，故障排除文件都不会包含冗余备份。

表 *37:* 可选择的故障排除选项

该选项...	报告...
Snort 性能和配置 (Snort Performance and Configuration)	与设备上的 Snort 相关的数据和配置设置
硬件性能和日志 (Hardware Performance and Logs)	与设备硬件性能相关的数据和日志
系统配置、策略和日志	与设备的当前系统配置相关的配置设置、数据和日志
检测配置、策略和日志	与对设备的检测相关的配置设置、数据和日志
接口和网络相关数据 (Interface and Network Related Data)	与设备的内联集和网络配置相关的配置设置、数据和日志
发现、感知、VDB 数据和日志	与设备上当前的发现和感知配置相关的配置设置、数据和日志
升级数据和日志 (Upgrade Data and Logs)	与设备的前期升级相关的数据和日志
所有数据库数据 (All Database Data)	包含在故障排除报告中的所有数据库相关数据
所有日志数据 (All Log Data)	设备数据库收集的所有日志
网络映射信息 (Network Map Information)	当前网络拓扑数据

为特定系统功能生成故障排除文件

可以生成和下载可发送给支持人员的自定义故障排除文件。

在多域部署中，您可以为后代域中的设备生成并下载故障排除文件。

开始之前

您必须是管理员、维护人员、安全分析师或安全分析师（只读）用户才能执行此任务。

过程

步骤 1 点击**生成故障排除文件**。

步骤 2 选择“所有数据”生成所有可能的故障排除数据或选中单个复选框，如 查看任务消息，第 277 页中所述。

步骤 3 点击 **OK**。

步骤 4 在消息中心查看任务消息；请参阅查看任务消息，第 277 页。

步骤 5 找出对应所生成的故障排除文件的任务。

步骤 6 在设备生成故障排除文件并且任务状态变更为已完成之后，点击**点击检索生成的文件**。

步骤 7 按照浏览器的提示下载文件。（故障排除文件将下载到一个 `.tar.gz` 文件中。）

步骤 8 按照支持部门的指示将故障排除文件发送给思科。

下载高级故障排除文件

在多域部署中，您可以为后代域中的设备生成并下载故障排除文件。您只可以从全局域中的 管理中心下载文件。

开始之前

您必须是管理员、维护人员、安全分析师或安全分析师（只读）用户才能执行此任务。

过程

步骤 1 查看设备的运行状况监控器。

步骤 2 点击**高级故障排除 (Advanced Troubleshooting)**。

步骤 3 在 **文件下载**，输入支持部门提供的文件名。

步骤 4 点击**下载 (Download)**。

步骤 5 按照浏览器的提示下载文件。

注释 对于受管设备，系统通过将设备名称置于文件名前面来重命名文件。

步骤 6 按照支持部门的指示将故障排除文件发送给思科。

一般故障排除

内部电源故障(硬件故障、电涌等)或外部电源故障(未插线)可能导致系统不正常关闭或重新启动。这些情况可能导致数据损坏。

基于连接的故障排除

基于连接的故障排除或调试可跨模块提供统一调试，以收集特定连接的相应日志。它还支持最多七级的基于级别的调试，并为 lina 和 Snort 日志启用统一的日志收集机制。基于连接的调试支持以下功能：

- 一种常见的基于连接的调试子系统，用于对 Firepower 威胁防御中的问题进行故障排除
- 跨模块的调试消息的统一格式
- 重新启动后的持续调试消息
- 基于现有连接的跨模块端到端调试
- 调试正在进行的连接

注释 Firepower 2100 系列设备不支持基于连接的调试。

有关连接故障排除更多信息，请参阅 连接故障排除 ， 第 285 页。

连接故障排除

过程

步骤 1 使用 **调试数据包-条件** 命令配置过滤器以识别连接。

示例：

```
Debug packet-condition match tcp 192.168.100.177 255.255.255.255 192.168.102.177
255.255.255.255
```

步骤 2 为感兴趣的模块和相应级别启用调试。输入 **调试数据包** 命令。

示例：

```
Debug packet acl 5
```

步骤 3 使用以下命令开始调试数据包：

```
debug packet-start
```

步骤 4 使用以下命令从数据库获取调试消息以分析调试消息：

```
show packet-debugs
```

步骤 5 使用以下命令停止调试数据包：

```
debug packet-stop
```

Cisco Secure Firewall Threat Defense 设备的高级故障排除

可以使用数据包跟踪器和数据包捕获功能在 Cisco Secure Firewall Threat Defense设备上执行深度故障排除分析。数据包跟踪器允许防火墙管理员向安全装置中注入虚拟数据包，跟踪从入口到出口的流量。在跟踪过程中，根据流量和路由查找、ACL、协议检查、NAT 和入侵检测。该实用程序强大的原因在于它能通过使用协议和端口信息指定源和目标地址来模拟实际流量的功能。跟踪选项可捕获数据包，从而判断出数据包是否已删除或是否成功。

有关故障排除文件的详细信息，请参阅 下载高级故障排除文件，第 284 页。

从 Web 界面使用 威胁防御 CLI

您可以从 管理中心 Web 界面执行所选的 威胁防御 命令行界面 (CLI) 命令。这些命令是 **ping**、**traceroute**和 **show** (除了 **show history** 和 **show banner**)。

在多域部署中，可以通过后代域中的受管设备的 管理中心 Web 界面输入 威胁防御 CLI 命令。

注释 在使用 管理中心高可用性的部署中，此功能仅在主用 管理中心中可用。

有关 威胁防御 CLI 的详细信息，请参阅 Cisco Secure Firewall Threat Defense 命令参考。

开始之前

您必须是管理员、维护人员或安全分析师用户才能使用 CLI。

过程

步骤 1 查看设备的运行状况监控器。

步骤 2 点击**高级故障排除 (Advanced Troubleshooting)**。

步骤 3 点击 **威胁防御 CLI**。

步骤 4 从**命令 (Command)** 下拉列表中，选择命令。

步骤 5 或者，在**参数 (Parameters)** 文本框中输入命令参数。

步骤 6 点击**执行 (Execute)** 以查看命令输出。

数据包跟踪器概览

使用数据包跟踪器，您可以通过根据源和目标寻址以及协议特征为数据包建模，测试您的策略配置。跟踪会执行策略查找以测试访问规则、NAT、路由、访问策略和速率限制策略，以便检查系统会允许还是拒绝数据包。数据包流基于接口、源地址、目标地址、端口和协议进行模拟。通过这样测试数据包，您可以看到策略结果并测试系统是否会按照需要处理要允许或拒绝的流量类型。除了验证

配置之外，您还可以使用跟踪器调试意外行为，例如数据包本应被允许，但却被拒绝的情况。为了充分模拟数据包，数据包跟踪器将跟踪数据路径；慢速路径和快速路径模块。处理基于每会话和每数据包进行。当下一代防火墙 (NGFW) 处理基于每会话或每数据包处理数据包时，通过跟踪来跟踪数据包和捕获将会基于每数据包记录跟踪数据。

您现在可以使用具有完整流的 PCAP 文件启动数据包跟踪器。目前，仅支持具有最多 100 个数据包的单个基于 TCP/UDP 的流的 PCAP。在重放期间动态修改数据包的功能（例如 IPsec、VPN、SSL 或 HTTPS 解密、NAT 等）不支持 PCAP 重放。

数据包跟踪器工具读取 PCAP 文件，初始化客户端和服务器重放实体的状态。该工具开始以同步方式重放数据包，方法是在 PCAP 中收集和存储每个数据包的跟踪输出，以便进行后续处理和显示。

数据包重放按 PCAP 文件中的数据包顺序执行，对重放活动的任何干扰都会终止重放活动并结束重放。

系统将为指定入口接口和出口接口上的 PCAP 中的所有数据包生成跟踪输出，从而提供流评估的完整情景。

使用数据包跟踪器

您可以在 Cisco Secure Firewall Threat Defense 设备上使用数据包跟踪器。您必须是管理员或维护用户才能使用此工具。

过程

步骤 1 在管理中心上，选择**设备** > **Packet Tracer**。

步骤 2 从 **选择设备** 下拉列表中，选择要为其运行跟踪的设备。

步骤 3 从 **接口** 下拉列表中，选择数据包跟踪的入口接口。

注释 请勿选择 VTI。数据包跟踪器不支持 VTI 作为入口接口。

步骤 4 要在数据包跟踪器中使用 PCAP 重放，请执行以下操作：

a) 点击 **选择 PCAP 文件**。

b) 要上传新的 PCAP 文件，请点击 **上传 PCAP 文件**。要重新使用最近上传的文件，请点击列表中的文件。

注释 仅支持 .pcap 和 .pcapng 文件格式。PCAP 文件只能包含一个基于 TCP/UDP 的流，最多 100 个数据包。PCAP 文件名（包括文件格式）的最大字符数限制为 64。

c) 在 **上传 PCAP** 框中，您可以拖动 PCAP 文件，也可以在框中点击以浏览并上传文件。选择文件后，上传过程会自动启动。

d) 转至此 步骤 13.

步骤 5 要定义跟踪参数，请从 **协议** 下拉菜单中选择跟踪的数据包类型，并指定协议特征：

- **ICMP** - 输入 ICMP 类型、ICMP 代码 (0-255)，并且可以选择键入 ICMP 标识符。
- **TCP**/**UDP**/**SCTP** - 输入源和目标端口号。

- **GRE**/**IPIP**-输入协议编号 0-255。
- **ESP**-输入源的 SPI 值 0-4294967295。
- **RAWIP**-输入端口号 0-255。

步骤 6 选择数据包跟踪的**源**类型，然后输入源 IP 地址。

源和目标类型包括 IPv4、IPv6 和完全限定域名 (FQDN)。如果使用思科 TrustSec，则可以指定 IPv4 或 IPv6 地址和 FQDN。

步骤 7 选择数据包跟踪的**源端口**。

步骤 8 选择数据包跟踪的**目标**类型，然后输入目标 IP 地址。

目标类型选项因您选择的源类型而异。

步骤 9 选择数据包跟踪的**目标端口**。

步骤 10 （可选）如果要跟踪安全组标记 (SGT) 值嵌入到层 2 CMD 标头 (TrustSec) 中的数据包，请输入有效的 **SGT 编号**。

步骤 11 如果希望数据包跟踪器进入父接口（稍后重定向到子接口），请输入 **VLAN ID**。

此值仅对非子接口可选，因为可以在子接口上配置所有接口类型。

步骤 12 为数据包跟踪指定**目标 MAC 地址**。

如果 Cisco Secure Firewall Threat Defense设备在透明防火墙模式下运行，并且入口接口为 VTEP，那么如果您在 **VLAN ID**中输入值，需要填写**目标 MAC 地址**。如果接口是桥接组成员，输入 **VLAN ID** 值时，**目标 MAC 地址**可选，不输入 **VLAN ID** 值时该值必填。

如果 Cisco Secure Firewall Threat Defense 在路由防火墙模式下运行时，如果输入接口是桥接组成员，**VLAN ID** 和 **目标 MAC 地址** 可选。

步骤 13 （可选）如果您希望 Packet Tracer 忽略对模拟数据包的安全检查，请点击 **绕过模拟数据包的所有安全检查**。这使得数据包跟踪器能够通过系统继续跟踪数据包，否则这些数据包将被丢弃。

步骤 14 （可选）要允许通过出口接口从设备发出数据包，请点击 **允许从设备传输模拟数据包**。

步骤 15 （可选）如果您希望 Packet Tracer 将注入的数据包视为 IPsec/SSL VPN 解密的数据包，请点击 **将模拟数据包视为 IPsec/SSL VPN 解密**。

步骤 16 点击 **Trace**（**跟踪**）。

跟踪结果 显示 PCAP 数据包通过系统的每个阶段的结果。点击单个数据包可查看数据包的跟踪结果。可以执行以下操作：

- 将 () 跟踪结果复制到剪贴板。
- 展开或折叠 () 显示的结果。
- 最大化 () 跟踪结果屏幕。

系统将显示每个阶段的已用时间信息，这些信息有助于衡量处理工作量。结果部分还会显示从入口接口流向出口接口的整个数据包流所花费的总时间。

跟踪历史记录 窗格显示每个 PCAP 跟踪的已存储跟踪详细信息。它最多可以存储 100 个数据包跟踪。您可以选择已保存的跟踪并再次运行数据包跟踪活动。可以执行以下操作：

- 使用任何跟踪参数搜索跟踪。
- 禁用使用  按钮将跟踪保存到历史记录。
- 删除特定跟踪结果。
- 清除所有痕迹。

数据包捕获概述

带有跟踪选项的数据包捕获功能允许通过系统跟踪在入口接口上捕获的真实数据包。跟踪信息将在以后阶段显示。这些数据包不会在出口接口上被丢弃，因为它们是真正的数据路径流量。面向 Firepower 威胁防御设备的数据包捕获支持对数据包进行故障排除和分析。

获取数据包后，Snort 将检测在数据包中启用的跟踪标志。Snort 会写入跟踪器元素，数据包通过它进行遍历。由于捕获数据包而导致的 Snort 断言可以是以下：之一。

表 *38: Snort* 判定

裁定	说明
通过	允许分析的数据包。
阻止	数据包未转发。
更换	数据包已修改。
AllowFlow	流直接通过，不经过检查。
BlockFlow	流被阻止。
忽略	流被阻止；仅当流在被动接口上受阻时才会发生。
重试	流停滞，正在等待 enamelware 或 URL 类别/信誉查询。在超时的情况下，处理继续进行，但结果未知：如果是漆包，则允许该文件；在 URL 类别/信誉的情况下，AC 规则查找将继续使用未分类和未知的信誉。

根据 Snort 判定，丢弃或允许数据包。例如，如果 Snort 判定为 **BlockFlow**，数据包将被丢弃，并且会话中的后续数据包在到达 Snort 之前会被丢弃。当 Snort 判定为 **阻止** 或 **BlockFlow**时， **丢弃原因** 可以是以下其中一项：

表 *39:* 丢弃原因

被阻止或流被阻止...	原因
Snort	Snort无法处理数据包，例如，由于数据包已损坏或格式无效，snort 无法解码。
预处理的应用 ID	应用 ID 模块/预处理本身不会阻止数据包；但这可能表示应用 ID 检测导致其他模块（例如，防火墙）匹配阻止规则。
SSL 预处理	SSL 策略中存在与流量匹配的阻止/重置规则。
防火墙	防火墙策略中有一个阻止/重置规则来匹配流量。
已预处理的强制网络门户	存在使用身份策略匹配流量的阻止/重置规则。
安全搜索预处理	有使用防火墙策略中的安全搜索功能来匹配流量的阻止/重置规则。
SI 预处理	AC 策略的“安全情报”选项卡中有一个阻止/重置规则，用于阻止流量、例如 DNS 或 URL SI 规则。
过滤器预处理	AC 策略的过滤器选项卡中有一个阻止/重置规则来匹配流量。
已预处理的数据流	存在入侵规则阻止/重置流连接，例如，当 TCP 规范化错误时阻止。
会话预处理	此会话之前已被某个其他模块阻止，因此会话预处理将阻止同一会话的更多数据包。
分片预处理	阻塞，因为数据的较早分片被阻止。
预处理的 Snort 响应	有一个 react snort 规则，例如，发送有关特定 HTTP 流量的响应页面。
预处理的 Snort 响应	有一个 snort 规则，用于在数据包匹配条件时发送自定义响应。
信誉预处理	数据包匹配信誉规则，例如阻止给定 IP 地址。
预处理后的 x-Link2State	由于在 SMTP 中检测到缓冲区溢出漏洞而被阻止。
后孔预处理	由于检测到 backorifice 数据而阻塞。
SMB 预处理	有一条 snort 规则可阻止 SMB 流量。
已预处理的文件进程	有阻止文件的文件策略，例如，阻止程序。

被阻止或流被阻止...	原因
IPS 预处理	有一个使用 IPS 的 snort 规则，例如，速率过滤。

数据包捕获功能支持捕获和下载存储在系统内存中的数据包。但是，由于内存限制，缓冲区大小限制为 32 MB。能够处理大量数据包捕获的系统会快速超出最大缓冲区大小，从而有必要提高数据包捕获限制。使用辅助内存（通过创建文件写入捕获数据）可达到此目的。支持的最大文件大小为 10 GB。

配置了 **file-size** 时，捕获的数据会存储到该文件，系统则会基于捕获名称 **recapture** 分配文件名称。

当需要捕获大小限制超过 32 MB 的数据包时，就会使用该 **file-size** 选项。

有关信息，请参阅 *Firepower* 威胁防御命令参考。

使用捕获跟踪

数据包捕获是一种实用程序，可根据定义的条件提供通过设备的指定接口的网络流量的实时快照。只要此过程未暂停或分配的内存未耗尽，它就会继续捕获数据包。

数据包捕获信息包括来自 Snort 和预处理器的关于裁定以及系统在处理数据包时所采取的操作的信息。同时可以进行多个数据包捕获。可将系统配置为修改、删除、清除和保存捕获。

注释 捕获数据包数据需要数据包复制。此操作可能会导致处理数据保持出现延迟，并有可能降低数据包吞吐量。思科建议使用数据包过滤器来捕获特定的流量数据。

开始之前

要在 Cisco Secure Firewall Threat Defense 设备上使用数据包捕获工具，您必须是管理员或维护用户。

过程

步骤 1 在管理中心上，选择**设备** > **数据包捕获**。

步骤 2 选择设备。

步骤 3 点击**添加捕获**。

步骤 4 为捕获跟踪输入**名称**。

步骤 5 为捕获跟踪选择**接口**。

步骤 6 指定**匹配条件**详细信息：

a) 选择**协议**。

b) 为**源主机**输入 IP 地址。

c) 为**目标主机**输入 IP 地址。

d) （可选）选中 **SGT 编号**复选框，然后输入安全组标记 (SGT)。

步骤 7 指定**缓冲区**详细信息：

a) （可选）输入最大**数据包大小**。
b) （可选）输入最小**缓冲区大小**。
c) 如果希望捕获的流量没有中断，请选择**连续捕获**；如果希望捕获在达到最大缓冲区大小时停止，则请选择**在已满时停止**。

注释 如果启用了 **继续捕获** ，则当分配的内存已满时，内存中最早捕获的数据包将被新捕获的数据包覆盖。

d) 如果希望捕获每个数据包的详细信息，请选择**跟踪**。
e) （可选）选中**跟踪计数**复选框。默认值为 50。可以输入介于 1-1000 范围内的值。

步骤 8 点击**保存**。

数据包捕获屏幕显示数据包捕获详细信息及其状态。要自动刷新数据包捕获页面，请选中 **启用自动刷新** 复选框，然后输入自动刷新间隔（以秒为单位）。

您可以对数据包执行以下操作：

- **编辑**（ ） 修改捕获条件。
- **删除**（ ） 以删除数据包捕获和捕获的数据包。
- **清除**（ ）清除数据包捕获中捕获的所有数据包。要从所有现有数据包捕获中清除捕获的数据包，请点击 **清除所有数据包**。
- **暂停**（ ） 暂时停止捕获数据包。
- **保存**（ ） 在本地计算机上以 ASCII 或 PCAP 格式保存捕获的数据包的副本。选择所需的格式选项，然后点击 **保存**。保存的数据包捕获将下载到您的本地计算机。
- 要查看正在捕获的数据包的详细信息，请点击所需的捕获行。

功能特定的故障排除

有关功能特定的故障排除技巧和技术，请参阅下表。

表 *40:* 功能特定的故障排除主题

功能	相关故障排除信息
应用控制	在 《Cisco Secure Firewall Management Center 设备配置指南》中应用控制的最佳实践
LDAP 外部身份验证	LDAP 身份验证连接故障排除 ， 第 176 页
许可	智能许可疑难解答 ， 第 218 页

功能	相关故障排除信息
用户规则条件	在 《Cisco Secure Firewall Management Center 设备配置指南》中的用户控制故障排除
用户身份源	有关 ISE/ISE-PIC、TS 代理身份源、强制网络门户身份源和远程接入 VPN 身份源的故障排除信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的相应部分 LDAP 身份验证连接故障排除， 第 176 页
URL 筛选	在 《Cisco Secure Firewall Management Center 设备配置指南》中的*URL* 过滤故障排除
领域和用户数据下载	在 《Cisco Secure Firewall Management Center 设备配置指南》中的领域和用户下载故障排除
网络发现	在 《Cisco Secure Firewall Management Center 设备配置指南》中的对网络发现策略进行故障排除
自定义安全组标记 (SGT) 规则条件	中的自定义 SGT 规则条件 《Cisco Secure Firewall Management Center 设备配置指南》
SSL 规则	在 《Cisco Secure Firewall 设备管理器配置指南》中的 SSL 规则一章
思科 Threat Intelligence Director (TID)	在 《Cisco Secure Firewall Management Center 设备配置指南》中的故障排除 *Cisco Secure Firewall* 威胁智能导向器
Cisco Secure Firewall Threat Defense系统日志	在 《Cisco Secure Firewall Management Center 设备配置指南》中的关于配置系统日志
入侵性能统计数据	在 《Cisco Secure Firewall Management Center 设备配置指南》中的入侵性能统计信息日志记录配置
基于连接的故障排除	基于连接的故障排除， 第 285 页

第 V 部分

工具

第 14 章

备份/恢复

关于备份和恢复

灾难恢复能力是任何系统维护计划的重要组成部分。作为灾难恢复计划的一部分，我们建议您定期备份到安全的远程位置。

按需备份

您可以对 CDO 中的多台 Cisco Secure Firewall Threat Defense 设备执行按需备份。

注释 威胁防御 高可用性对不支持按需备份。

有关详细信息，请参阅备份托管设备， 第 302 页。

存储备份文件

您只能在本地存储备份。不支持将 威胁防御 设备备份到安全的远程位置。

有关详细信息，请参阅备份托管设备， 第 302 页。

恢复托管设备

您必须使用 威胁防御 CLI 来恢复 威胁防御 设备。

有关详细信息，请参阅恢复 CDO 托管设备， 第 303 页。

备份的内容是什么？

设备备份始终仅用于配置。

恢复的内容是什么？

恢复配置会覆盖所有备份配置，只有少数例外。在 CDO 上，恢复事件和威胁智能导向器 (TID) 数据会覆盖所有现有事件和 TID 数据，但入侵事件除外。

确保您了解并计划以下事项：

- 您无法恢复未备份的内容。
- 威胁防御 恢复过程会从 威胁防御 设备中删除 VPN 证书和所有 VPN 配置，包括在执行备份后添加的证书。恢复 威胁防御 设备后，必须重新添加/重新注册所有 VPN 证书，并重新部署设备。

备份和还原要求

Backup and Restore具有以下要求。

型号要求：备份

您可以备份：

- 威胁防御 独立设备，本地实例，容器实例和 HA 对
- Threat Defense Virtual 适用于 VMware 设备，无论是独立或 HA 对

不 支持备份：

- 威胁防御 集群
- Threat Defense Virtual 除 VMware 的实施

如果需要更换不支持备份和恢复的设备，则必须手动重新创建设备特定的配置。

型号要求：恢复

替换受管设备必须与您要替换的设备具有相同的型号，具有相同数量的网络模块和相同类型和数量的物理接口。

版本要求

作为任何备份的第一步，请注意补丁级别。要恢复备份，旧设备和新设备必须运行相同的防火墙版本，包括补丁。

许可证要求

解决最佳实践和程序中所述的许可或孤立权利问题 。如果您发现许可冲突，请联系思科 TAC。

域要求

到：

- 恢复设备：无。在本地恢复设备。

在多域部署中，不能仅备份事件/ TID 数据。您还必须备份配置。

备份和恢复的指南和限制

Backup and Restore有以下指南和限制。

⚠

注意 具有 CLI 访问权限的用户可以使用 **expert** 命令访问 Linux 外壳，这可能会带来安全风险。出于系统安全原因，我们强烈建议：

- 仅在 TAC 监督下或在防火墙和 CDO 用户文档明确指示时使用 Linux 外壳。
- 限制具有 Linux 外壳访问权限的用户列表。
- 请勿在 Linux 外壳中直接添加用户；请仅使用本章中的这些程序。

备份和恢复适用于灾难恢复//退货许可

备份和恢复主要用于退货许可(RMA)场景。在开始故障或发生故障的物理设备的恢复过程之前，请联系更换硬件。

你也可以使用Backup and Restore来在管理中心之间迁移配置和事件。这使得更换管理中心（由于不断增长的组织、从物理实施迁移到虚拟实施、硬件更新等技术或业务等方面的原因）变得更容易。

Backup and Restore 不是配置导入/导出

备份文件包含唯一识别设备的信息，并且不能共享。不要使用备份和恢复过程在设备或装置之间复制配置，或作为测试新配置时保存配置的一种方式。相反，请使用导入/导出功能。

例如， 威胁防御 设备备份包括设备的管理 IP 地址以及设备连接到其管理 CDO 所需的所有信息。请勿将 FTD 备份恢复到由其他 管理器管理的设备；恢复的设备将尝试连接到备份中指定的管理器。

恢复为单个和本地恢复

您可以单独和本地恢复 威胁防御设备。这意味着：

- 您无法批量恢复到高可用性（HA）设备。本指南中的还原程序介绍如何在高可用性环境中还原。
- 您无法使用 CDO 恢复设备。 对于 威胁防御 设备，必须使用 威胁防御 CLI，但 ISA 3000 零接触恢复除外，该恢复使用 SD 卡和重置按钮。
- 您不能使用 管理中心 用户账号登录并从其受管设备之一恢复。管理中心 和 威胁防御 设备维护自己的用户账号。

备份和还原的最佳实践

Backup and Restore具有以下最佳实践。

何时备份

我们建议在维护时段或其他使用率较低的时间进行备份。

当系统收集备份数据时，数据的关联性可能会暂时停顿（仅限FMC），而且你可能无法改变与备份有关的配置。如果包含事件数据，则 eStreamer 等事件相关功能不可用。

您应在以下情况下进行备份：

- 常规计划的备份

  作为灾难恢复计划的一部分，我们建议您定期执行备份。

- 在升级或重新映像之前。

  如果升级失败是灾难性的，您可能必须重新映像并恢复。重新映像会将大多数设置恢复为出厂默认设置，包括系统密码。如果您有最近的备份，可以更快地恢复正常操作。

- 升级后。

  在升级后进行备份，以便获得新升级的部署的快照。我们建议您在升级其托管设备后 备份 FMC，以便新的 FMC 备份文件“知道”其设备已升级。

维护备份文件安全

备份存储为未加密的存档（.tar）文件。

PKI 对象中的私钥--代表支持你的部署所需的公钥证书和成对的私钥--在被备份之前被解密在恢复备份时，将使用随机生成的密钥重新加密密钥。

威胁防御 高可用性部署中的Backup and Restore

在 威胁防御 HA 部署中，您必须：

- 从 FMC备份设备对，但从 威胁防御 CLI 单独和本地恢复。

  备份过程会为 威胁防御 HA 设备生成唯一的备份文件。请勿使用来自另一个 HA 的备份文件恢复一个 HA 对等体。备份文件包含唯一识别设备的信息，并且不能共享。

  威胁防御 HA 设备的角色记录在其备份文件名中。还原时，请确保选择适当的备份文件：主要与辅助。

- 在恢复之前， 请勿 暂停或中断 HA。

  保持 HA 配置可确保替换设备在恢复后可以轻松重新连接。请注意，您必须恢复 HA 同步才能执行此操作。

- 请勿 同时在两个对等体上运行 restore CLI 命令。

假设您已成功备份，您可以替换高可用性对中的一个或两个对等体。您可以同时执行的任何物理更换任务：取消安装，重新安装等。但是，请勿在第二台设备上运行 restore 命令，直到第一台设备的恢复过程完成，包括重新启动。

备份前

在备份之前，您必须：

- 检查磁盘空间。

  在开始备份之前，请确保设备上有足够的磁盘空间。可用空间显示在“备份管理”页面上。

  如果没有足够的空间，备份可能会失败。尤其是在安排备份时，请确保定期删除备份文件或为远程存储位置分配更多磁盘空间。

还原前

在恢复之前，您必须：

- 恢复许可更改。

  请恢复自备份以来所做的任何许可更改。

  否则，恢复后您可能会遇到许可证冲突 或孤立的权利问题 。 但是， 请勿 从 Cisco 智能软件管理器（CSSM）注销。如果从 CSSM 注销，则必须在恢复后再次注销，然后重新注册。

  恢复完成后，重新配置许可。如果您发现许可冲突 或孤立的权利，请联系思科 TAC 。

- 断开故障设备。

  断开管理接口，对于设备，断开数据接口。

  恢复 威胁防御 设备会将替换设备的管理 IP 地址设置为旧设备的管理 IP 地址。为避免 IP 地址冲突，请先断开旧设备与管理网络的连接，然后再更换备份。

- 请勿 取消注册受管设备。

  无论您是恢复托管设备，都不要从 CDO 注销设备，即使您从网络上物理断开设备。

  如果取消注册，则必须重做一些设备配置，例如安全区域到接口的映射。恢复后，CDO 和设备应开始正常通信。

- 重新映像。

  在 RMA 场景中，替换设备将配置为出厂默认设置。但是，如果已配置替换设备，我们建议您重新映像。重新映像会将大多数设置恢复为出厂默认设置，包括系统密码。您只能重新映像到主要版本，因此您可能必须在重新映像后进行修补。

  如果不重新映像，请记住，CDO 入侵事件和文件列表会合并而不是覆盖。

还原后

在恢复之后，您必须：

- 重新配置未恢复的任何内容。

  这可能包括重新配置许可，远程存储和审核日志服务器证书设置。 您还必须重新添加/重新注册失败的 威胁防御 VPN 证书。

- 部署。

  恢复设备后，部署到该设备。您 必须 部署。如果设备未标记为过期，请从"设备管理"页面强制部署。

备份托管设备

您可以对支持的设备执行按需或计划备份。

使用 CDO 备份设备不需要使用备份配置文件。

有关详细信息，请参阅从 FMC 备份威胁防御设备 ， 第 302 页。

从 FMC 备份威胁防御设备

使用此程序对以下任何设备执行按需备份：

- 威胁防御：物理设备，独立、HA
- Threat Defense Virtual：VMware，独立、HA

备份和恢复不支持任何其他平台或配置。

开始之前

您必须阅读并了解要求、指南、限制和最佳实践。不要跳过任何步骤或忽略安全问题。认真规划和准备可以帮助您避免失误。

- 备份和还原要求 ， 第 298 页
- 备份和恢复的指南和限制 ， 第 299 页
- 备份和还原的最佳实践 ， 第 300 页

⚠

注意 具有 CLI 访问权限的用户可以使用 **expert** 命令访问 Linux 外壳，这可能会带来安全风险。出于系统安全原因，我们强烈建议：

- 仅在 TAC 监督下或在防火墙和 CDO 用户文档明确指示时使用 Linux 外壳。
- 限制具有 Linux 外壳访问权限的用户列表。
- 请勿在 Linux 外壳中直接添加用户；请仅使用本章中的这些程序。

过程

步骤 1 登录 CDO。

步骤 2 从 CDO 菜单中，导航至 **工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。

步骤 3 在“操作”(Actions) 窗格中，点击**监控 (Monitoring)**。

步骤 4 选择 **系统**（⚙），然后点击**托管设备备份 (Managed Device Backup)**。

步骤 5 选择 **Managed Device Backup**。

步骤 6 在**托管设备 (Managed Devices)** 中选择一个或多个威胁防御设备。

步骤 7 设备备份文件的**存储位置**是 `/var/sf/remote-backup/`中的本地存储。

步骤 8 如果未配置远程存储，请选择是否要 **检索到管理中心**。

- 已启用 （默认）：将备份保存到 `/var/sf/remote-backup/`中的 FMC。
- 已禁用：将备份保存到 `/var/sf/backup`中的设备。

步骤 9 点击 **开始备份** 开始按需备份。

步骤 10 在**通知 (Notifications)**窗格中的**任务 (Tasks)** 下监控进度。

恢复 CDO 托管设备

对于 威胁防御 设备，您必须使用 威胁防御 CLI 从备份中恢复。您无法使用 管理中心 恢复设备。

以下各节介绍如何恢复托管设备。

- 恢复 威胁防御 设备，第 303 页
- 从备份恢复威胁防御：威胁防御虚拟，第 306 页

恢复 威胁防御 设备

威胁防御 备份和恢复适用于 RMA。恢复配置会覆盖设备上的 所有 配置，包括管理 IP 地址。也重启设备。

万一发生硬件故障，此程序概述了如何更换防火墙设备（独立或 HA 对）。它假定您有权访问要替换的设备的成功备份。

在 威胁防御 HA 部署中，您可以使用此程序替换任一或两个对等体。要同时替换两者，请同时在两台设备上执行所有步骤，但恢复 CLI命令本身除外。请注意，您可以在没有成功备份的情况下替换威胁防御 HA 设备。

注释 请勿 从 CDO注销，即使在断开设备与网络的连接时也是如此。在 威胁防御 HA 部署中， 请勿 暂停或中断 HA。维护这些链路可确保替换设备在恢复后可以自动重新连接。

开始之前

您必须阅读并了解要求、指南、限制和最佳实践。不要跳过任何步骤或忽略安全问题。认真规划和准备可以帮助您避免失误。

- 备份和还原要求， 第 298 页
- 备份和恢复的指南和限制， 第 299 页
- 备份和还原的最佳实践， 第 300 页

过程

步骤 1 联系 思科 TAC 更换硬件。

获取相同的型号，具有相同数量的网络模块和相同类型和数量的物理接口。您可以从 思科退货门户 开始 RMA 进程。

步骤 2 导航到**系统**（⚙）> **工具 (Tools)** > **备份/恢复 (Backup/Restore)**。

步骤 3 从**备份管理 (Backup Management)** 下的**设备备份 (Device Backups)** 中找到故障设备的成功备份。

根据备份配置，可以存储设备备份：

- 在故障设备上 - 将备份保存到 `/var/sf/backup` 中的 FMC。
- 在管理中心 - 将备份保存到 `/var/sf/remote-backup/` 中的设备。

在 威胁防御 HA 部署中，您将对作为一个单元进行备份，但备份过程会为对中的每个设备生成唯一的备份文件。设备的角色在备份文件名中注明。

如果备份的唯一副本位于故障设备上，请立即将其复制到其他位置。如果重新映像设备，备份将被清除。如果出现其他问题，您可能无法恢复备份。

替换设备需要备份，但可以在恢复过程中使用安全复制协议 (SCP) 命令进行检索。我们建议您将备用设备放在 SCP 可访问的位置，以供替换设备使用。或者，您可以将备份复制到替换设备本身。

步骤 4 移除（拆开）故障设备并断开所有接口。在威胁防御 HA 部署中，这包括故障切换链路。

请参阅适用于您的型号的硬件安装和入门指南：《思科 Firepower NGFW：安装和升级指南》。

注释 请勿从管理中心取消注册，即使在断开设备与网络的连接时也是如此。在威胁防御 HA 部署中，请勿暂停或中断 HA。维护这些链路可确保替换设备在恢复后可以自动重新连接。

步骤 5 安装替换设备并将其连接到管理网络。

将设备连接至电源并将管理接口连接至管理网络。在威胁防御 HA 部署中，请连接故障切换链路。但是， 请勿 连接数据接口。

请参阅适用于您的型号的硬件安装指南：《思科 Firepower NGFW：安装和升级指南》。

步骤 6 （可选）重新映像替换 设备。

在 RMA 场景中，替换设备将配置为出厂默认设置。如果替换设备运行的主版本与故障设备不同，我们建议您重新映像。

请参阅《Cisco Secure Firewall ASA 和威胁防御重新映像指南》。

步骤 7 在替换设备上执行初始配置。

以 admin 用户身份访问 威胁防御 CLI。您可以使用控制台，也可以通过 SSH 连接到出厂默认管理接口IP地址（192.168.45.45）。安装向导会提示您配置管理 IP 地址，网关和其他基本网络设置。

请参阅您的型号的入门指南中的初始配置主题： 《Cisco Firepower NGFW：安装和升级指南》。

注释 如果需要修补替换设备，请按照入门指南中的说明启动管理中心注册过程。如果不需要修补， 请勿注册。

步骤 8 确保替换设备运行与故障设备相同的 Firewall 软件版本， 包括补丁。

不应从管理中心删除现有设备。替换设备应不受物理网络的管理，新硬件以及替换的威胁防御补丁应具有相同的版本。威胁防御 CLI 没有升级命令。要修补，请执行以下操作：

a) 从管理中心 Web 界面完成设备注册过程：请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的将设备添加到管理中心。

   创建新的AC策略并使用默认操作“网络发现”。保持此策略不变；请勿添加任何功能或修改。这用于注册设备和部署无功能的策略，以便您不需要许可证，然后便可以修补设备。备份恢复后，应将许可和策略恢复到预期状态。

b) 为设备打补丁：《Cisco Firewall 管理中心升级指南》。

c) 从管理中心取消注册新安装的设备：请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的从管理中心删除设备。

   如果不取消注册，则在恢复过程将“旧”设备恢复后，您将有一个Ghost设备注册到管理中心。

步骤 9 确保替换设备有权访问备份文件。

恢复过程可以使用 SCP 检索备份，因此我们建议您将备份放在可访问的位置。或者，您可以手动将备份复制到替换设备本身，复制到 `/var/sf/backup`。

步骤 10 从 FTD CLI 恢复备份。

以 admin 用户身份访问 威胁防御 CLI。您可以使用控制台，也可以通过 SSH 连接到新配置的管理接口（IP 地址或主机名）。请记住，恢复过程将更改此 IP 地址。

要恢复，请执行以下操作：

- 使用 SCP：**restore remote-manager-backup location scp-hostname username filepath backup tar-file**

- 从本地设备：**restore remote-manager-backup backup tar-file**

步骤 11 登录 CDO 并等待设备进行连接。

还原完成后，设备会退出 CLI，重新启动并自动连接到 CDO。此时，设备应显示为过时。

此时，设备应显示为过时。

步骤 12 在部署之前，请执行任何恢复后任务并解决任何恢复后问题：

- 解决许可冲突或孤立授权问题。联系思科 TAC：
- 恢复 HA 同步。
- 重新添加/重新注册所有 VPN 证书。恢复过程会从 FTD 设备中删除 VPN 证书，包括在执行备份后添加的证书。

步骤 13 部署配置。

您 必须 部署。如果恢复的设备未标记为过期，请从“设备管理”页面强制部署。

步骤 14 连接设备的数据接口。

请参阅适用于您的型号的硬件安装指南：《Cisco Secure Firewall Threat Defense：安装和升级指南》。

从备份恢复威胁防御：威胁防御虚拟

使用此程序可为 VMware 更换故障或发生故障的 threat defense virtual 设备。

注释 请勿从管理中心注销，即使在断开设备与网络的连接时也是如此。保持注册可确保替换设备在恢复后可以自动重新连接。

开始之前

您必须阅读并了解要求、指南、限制和最佳实践。不要跳过任何步骤或忽略安全问题。认真规划和准备可以帮助您避免失误。

- 备份和还原要求，第 298 页
- 备份和恢复的指南和限制，第 299 页
- 备份和还原的最佳实践，第 300 页

过程

步骤 1 导航到**系统**（⚙）> **工具 (Tools)** > **备份/恢复 (Backup/Restore)**。

步骤 2 从**备份管理 (Backup Management)** 下的**设备备份 (Device Backups)** 中找到故障设备的成功备份。

对于集群，节点备份文件捆绑在集群的单个压缩文件中 (*cluster_name.timestamp*.**tar.gz**)。在恢复节点之前，需要提取单个节点备份文件 (*node_name*_**control**_*timestamp*.**tar** or *node_name*_**data**_*timestamp*.**tar**)。

根据备份配置，可以存储设备备份：

- 在故障设备上 - 将备份保存到 `/var/sf/backup` 中的 CDO。
- 在 管理中心 - 将备份保存到 `/var/sf/remote-backup/` 中的设备。

如果备份的唯一副本位于故障设备上，请立即将其复制到其他位置。如果重新映像设备，备份将被清除。如果出现其他问题，您可能无法恢复备份。

替换设备需要备份，但可以在恢复过程中使用 SCP 进行检索。我们建议您将备用设备放在 SCP 可访问的位置，以供替换设备使用。或者，您可以将备份复制到替换设备本身。

步骤 3 删除故障设备。

关机、关闭电源并删除虚拟机。对于程序，请参阅您的虚拟托管环境的相关文档。

步骤 4 部署替换设备。

请参阅《适用于 VMware 的 Cisco Firepower Threat Defense Virtual 入门指南》。

步骤 5 在替换设备上执行初始配置。

使用 VMware 控制台以管理员用户身份访问 threat defense virtual CLI。安装向导会提示您配置管理 IP 地址，网关和其他基本网络设置。

请勿设置与故障设备相同的管理 IP 地址。如果您需要注册设备以进行修补，这可能会导致问题。恢复过程将正确重置管理 IP 地址。

请参阅入门指南中的 CLI 设置主题：《适用于 VMware 的 Cisco Firepower Threat Defense Virtual 入门指南》。

步骤 6 确保替换设备运行与故障设备相同的 Firewall 软件版本， 包括补丁。

确保不应从 CDO 中删除现有设备。替换设备应不受物理网络的管理，新硬件以及替换的 threat defense virtual 补丁应具有相同的版本。 threat defense virtual CLI 没有升级命令。要修补，请执行以下操作：

1. 完成 CDO 中的 threat defense virtual 注册流程。
2. 修补 threat defense virtual 设备。
3. 从 CDO 取消注册最新修补的设备。

步骤 7 确保替换设备有权访问备份文件。

恢复过程可以使用 SCP 检索备份，因此我们建议您将备份放在可访问的位置。或者，您可以手动将备份复制到替换设备本身，复制到 `/var/sf/backup`。

步骤 8 从 威胁防御 CLI 恢复备份。

以 admin 用户身份访问 threat defense virtual CLI。您可以使用控制台，也可以通过 SSH 连接到新配置的管理接口（IP 地址或主机名）。请记住，恢复过程将更改此 IP 地址。

要恢复，请执行以下操作：

- 使用 SCP：**restore remote-manager-backup location scp-hostname username filepath backup tar-file**
- 从本地设备：**restore remote-manager-backup backup tar-file**

步骤 9 登录 CDO 并等待设备进行连接。

还原完成后，设备会退出 CLI，重新启动并自动连接到 CDO。此时，设备应显示为过时。

此时，设备应显示为过时。

步骤 10 在部署之前，请执行任何恢复后任务并解决任何恢复后问题：

- 解决许可冲突或孤立授权问题。联系思科 TAC：
- 恢复 HA 同步。
- 重新添加/重新注册所有 VPN 证书。恢复过程会从 threat defense virtual 设备中删除 VPN 证书，包括在执行备份后添加的证书。

步骤 11 部署配置。

您 必须 部署。如果恢复的设备未标记为过期，请从“设备管理”页面强制部署。

步骤 12 连接设备的数据接口。

请参阅适用于您的型号的硬件安装指南：《Cisco Secure Firewall Threat Defense：安装和升级指南》。

第 15 章

计划

以下主题介绍如何安排任务：

关于任务安排

可安排各种任务在指定时间运行一次或反复运行。

任务在后端UTC中安排的，这意味着它们在本地发生的时间取决于日期和您的特定位置。此外，由于任务是以UTC为单位进行计划的，因此它们不会针对夏令时、夏令时或您在地点可能观察到的任何季节性调整进行调整。如果受影响，则根据当地时间，计划任务会在夏天比冬季中的一个小时开始。

某些任务由初始设置过程自动安排或执行：

- 下载并安装最新 VDB 的一次性任务。
- 用于下载最新可用软件更新的每周计划任务。
- 执行 管理中心 本地存储的仅配置备份的每周计划任务。

您应查看每周任务并在必要时进行调整。或者，安排新的周期性任务以实际更新 VDB 和/或软件，并部署配置。

重要事项 我们强烈建议您查看计划任务，确保这些任务在您预期的时间执行。有些任务（例如，那些涉及自动化软件更新的任务，或者要求将更新推送到受管设备的任务）可能会显著增加低带宽网络的负载。应安排此类任务在网络使用量较低的时段运行。其他任务（例如部署配置）可能会导致流量中断。您应在维护窗口期间安排此类任务。

任务安排的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 维护用户

配置周期性任务

使用相同流程为所有类型的任务设置周期性任务的频率。

请注意，Web 界面上大多数页面中显示的时间为本地时间，由您在本地配置中指定的时区决定。而且，管理中心将在适当时自动调整本地显示的夏令时 (DST) 时间。但是，从 DST 到标准时以及从标准时到 DST 跨越转换日期的周期性任务不会调整转换。即，如果创建的某项任务安排在标准时上午 2:00 执行，则它将于 DST 上午 3:00 运行。同理，如果创建的某项任务安排在 DST 上午 2:00 执行，则它将于标准时上午 1:00 运行。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从**作业类型 (Job Type)** 列表中，选择要安排的任务类型。

步骤 4 点击 **安排要运行的任务** 选项旁边的 **周期性** 。

步骤 5 在 **Start On** 字段中，指定想要开始周期性任务的日期。

步骤 6 在 **Repeat Every** 字段中，指定想要任务重复的频率。

可键入数字，或者点击 **向上**（▲） 和 **向下**（▼） 指定时间间隔。例如，键入 2 并点击 **天数** 让任务每两天运行一次。

步骤 7 在 **Run At** 字段中，指定想要开始周期性任务的时间。

步骤 8 如需每周或每月运行一次任务，请在**重复日期 (Repeat On)** 字段中选择要运行任务的天数。

步骤 9 为正在创建的任务类型选择其余选项：

- “备份”(Backup) - 安排备份作业，如从 FMC 备份威胁防御设备 ，第 302 页中所述。

- “下载 CRL”(Download CRL) - 安排证书撤销列表下载，如配置证书撤销列表下载，第 312 页中所述。
- “部署策略”(Deploy Policies) - 安排策略部署，如自动执行策略部署，第 313 页中所述。
- “Nmap 扫描”(Nmap Scan) - 安排 Nmap 扫描，如安排 Nmap 扫描，第 314 页中所述。
- “报告”(Report) - 安排报告生成，如 中所述 自动执行报告生成，第 315 页
- Cisco 建议规则 - 安排 Cisco 建议规则的自动更新，如 自动生成 思科 建议，第 316 页中所述
- “下载最新更新”(Download Latest Update) - 安排软件或 VDB 更新下载，如自动执行软件下载，第 318 页或自动执行 VDB 更新下载，第 321 页中所述。
- “安装最新更新” - 安排在 Cisco Secure Firewall Management Center或受管设备上安装软件或 VDB 更新，如自动执行软件安装，第 320 页或自动执行 VDB 更新安装，第 322 页中所述
- “推送最新更新”(Push Latest Update) - 安排将软件更新推送到受管设备，如自动执行软件推送，第 319 页中所述。
- “更新 URL 过滤数据库”(Update URL Filtering Database) - 安排 URL 过滤数据的自动更新，如中所述 使用已安排任务自动执行 URL 过滤更新，第 322 页

步骤 10 点击**保存**

计划的备份

您可以在 Cisco Secure Firewall Management Center 上使用调度程序自动执行自己的备份。您还可以从管理中心安排远程设备备份。

请注意，并非所有设备都支持远程备份。

安排远程设备备份

您可以使用 管理中心 上的调度程序来自动执行 管理中心 和设备备份。请注意，并非所有设备都支持远程备份。

您必须在全局域中才能执行此任务。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 从 **Job Type** 列表中，选择 **Backup**。

步骤 3 指定要备份 **一次** 还是 **定期**备份。

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 对于定期任务，请参阅 配置周期性任务，第 310 页。

步骤 4 输入 **作业名称**。

步骤 5 对于**备份类型**，请点击**设备**。

步骤 6 选择一个或多个设备。

如果您的设备未列出，则表示它不支持远程备份。

步骤 7 如果未配置远程备份存储，请选择是否要 **检索到管理中心**。

- 已启用（默认）：将备份保存到 `/var/sf/remote-backup/` 中的 管理中心。
- 已禁用：将备份保存到 `/var/sf/backup/`中的设备。

如果配置了远程备份存储，则远程保存备份文件，并且此选项无效。

步骤 8 （可选）输入 **注释**。

请保持注释简短。他们将显示在计划日历页面的“任务详细信息”部分中。

步骤 9 （可选）在 **邮件发送状态：** 字段中输入邮件地址或邮件地址的逗号分隔列表。

有关设置邮件中继服务器以发送任务状态消息的信息，请参阅 配置邮件中继主机和通知地址 ， 第 159 页。

步骤 10 点击**保存 (Save)**。

配置证书撤销列表下载

必须使用 管理中心。在多域部署中，仅在 管理中心的全局域中支持此任务。

当支持在启用用户证书或审核日志证书的设备上的本地配置中下载证书吊销列表 (CRL) 时，系统会自动创建下载 CRL 任务。可以使用计划程序来编辑任务以设置更新频率。

开始之前

- 启用并配置用户证书，或者审核日志证书并设置一个或多个CRL 下载URL。有关详细信息，请参阅 需要有效的 HTTPS 客户端证书 和 需要有效的审核日志服务器证书 。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从 **作业类型**中，选择 **下载 CRL**。

步骤 4 指定要如何安排 CRL 下载，**一次 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务 ， 第 310 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 7 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须在管理中心上配置一台有效的邮件中继服务器，以发送状态消息。

步骤 8 点击**保存 (Save)**。

相关主题

配置邮件中继主机和通知地址，第 159 页

自动执行策略部署

在 管理中心 中修改配置设置后，必须将这些更改部署到受影响的设备。

在多域部署中，只能为当前域安排策略部署。

注意 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，部署某些配置会重新启动 Snort 进程，这会中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。请参阅Snort 重启流量行为，第 144 页和部署或激活时重启 Snort 进程的配置，第 146 页。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从 **作业类型**，选择 **部署策略**。

步骤 4 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 310 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 在**设备 (Device)** 字段中，选择要部署策略的设备。

步骤 7 根据需要选中或取消选中 **跳过最新设备的部署** 复选框。

默认情况下，系统会启用**跳过最新设备的部署**以提高策略部署过程中的性能。

注释 如果从 Firepower 管理中心 Web 界面发起的策略部署正在进行，则系统不会执行已安排的部署策略任务。相应地，如果已安排的策略部署任务正在进行，则系统不允许从 Web 界面发起策略部署。

步骤 8 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Tasks Details) 部分中；请保持注释简短。

步骤 9 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 10 点击**保存 (Save)**。

相关主题

配置邮件中继主机和通知地址，第 159 页
过时策略，第 150 页

Nmap 扫描自动化

您可在网络上安排定期 Nmap 目标扫描。自动化扫描允许您刷新 Nmap 扫描之前提供的信息。由于 Firepower 系统无法更新 Nmap 提供的数据，因此需要定期重新扫描以保持数据为最新。还可安排扫描，使其自动在网络主机上测试未识别的应用或服务器。

请注意，发现管理员也可使用 Nmap 扫描作为补救。例如，主机上发生的操作系统冲突可能会触发 Nmap 扫描。运行扫描可以获取主机的最新操作系统信息，这样可以解决冲突。

如果之前未曾使用 Nmap 扫描功能，则在定义计划扫描之前，需要配置 Nmap 扫描。

相关主题

Nmap 扫描，第 1926 页

安排 Nmap 扫描

Nmap 使用 Nmap 扫描结果替换系统检测到的主机操作系统、应用或服务器之后，系统不再更新 Nmap 替换的主机信息。Nmap 提供的服务和操作系统数据将保持不变，直到您运行另一个 Nmap 扫描为止。如果计划使用 Nmap 扫描主机，则可能要设置定期安排的扫描，以使 Nmap 提供的操作系统、应用或服务器保持最新。如从网络删除主机并重新添加，则将丢弃任何 Nmap 扫描结果，系统假设监控主机的所有操作系统和服务数据。

在多域部署中：

- 只能为当前域安排扫描
- 选择的补救和 Nmap 目标必须存在于当前域或祖先域中。
- 选择对非分叶域执行 Nmap 扫描将会扫描该域的每个后代中的相同目标。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type**，选择 **Nmap Scan**。

步骤 4 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 310 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 在 **Nmap 补救**字段中，选择 Nmap 补救。

步骤 7 在 **Nmap 目标 (Nmap Target)** 字段中，选择扫描目标。

步骤 8 在**域 (Domain)** 字段中，选择要扩充其网络映射的域。

步骤 9 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

提示 注释字段显示在日历计划页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 10 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 11 点击**保存 (Save)**。

相关主题

配置邮件中继主机和通知地址，第 159 页

自动执行报告生成

可自动生成报告，以使它们按固定间隔运行。

在多域部署中，只能为当前域安排报告。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表，选择 **Report**。

步骤 4 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 310 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 在**报告模板 (Report Template)** 字段中，选择风险报告或报告模板。

步骤 7 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Tasks Details) 部分中；请保持注释简短。

步骤 8 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

注释 配置此选项**不会**分发报告。

步骤 9 如果不想在报告没有数据时（例如，当报告期间未发生特定类型的事件时）接收报告邮件附件，请选中**如果报告为空，仍附加到邮件中 (If report is empty, still attach to email)** 复选框。

步骤 10 点击**保存 (Save)**。

指定计划报告的报告生成设置

您必须具有管理员或安全分析师权限才能执行此任务。

要指定或更改计划报告的文件名、输出格式、时间窗口或邮件分发设置，请执行以下操作：

过程

步骤 1 选择**概述 > 报告 > 报表模板**。

步骤 2 针对要更改的报告模板，点击**编辑**。

步骤 3 如果您将选择 PDF 输出：

a) 查看报告中是否有任何部分在结果数量旁边显示一个黄色三角形。

b) 如果您看到任何黄色三角形，请将光标悬停在该三角形上，以查看该部分 PDF 输出允许的最大结果数。

c) 对于带有黄色三角形的每个部分，将结果数量减少到低于该限制的数量。

d) 如果没有其他黄色三角形，请点击**保存**。

步骤 4 点击**生成 (Generate)**。

注释 如果要更改报告生成设置而不立即生成报告，则必须从模板配置页中点击**生成**。如果从模板列表视图中点击**生成**，系统不会保存更改，除非您生成报表。

步骤 5 修改设置。

步骤 6 要保存新设置而不生成报告，请点击**取消**。

要保存新设置并生成报告，请点击**生成**，然后跳过此过程中的其余步骤。

步骤 7 点击**保存 (Save)**。

步骤 8 如果您看到有关保存的提示，即使您未进行更改，请点击**确定**。

自动生成 思科 建议

可使用自定义入侵策略中最近保存的配置设置，根据网络发现数据，自动生成规则状态建议。

注释 如果系统自动为入侵策略生成预定建议并且不保存更改，则必须丢弃在入侵策略中所做出的更改，而且如果想要策略反映自动生成的建议，还必须执行此策略。

当任务运行时，系统自动生成建议规则状态，并且根据策略的配置修改入侵规则的状态。已修改的规则状态在下次部署入侵策略时生效。

在多域部署中，可以在当前域级别自动生成入侵策略的建议。 系统会为每个枝叶域构建单独的网络映射。在多域部署中，如果您在祖先域的入侵策略中启用此功能，则系统会使用来自所有后代枝叶域的数据生成建议。这可能使得入侵规则针对可能不存在于所有枝叶域的资产进行定制，从而影响性能。

开始之前

- 在入侵策略中配置 思科 建议的规则，如 《Cisco Secure Firewall Management Center 设备配置指南》中所述。
- 如果要通过邮件发送任务状态消息，请配置有效的邮件中继服务器。
- 您必须具有 威胁 智能许可证或保护经典许可证才能生成建议。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从 **作业类型**中，选择 **Firepower 建议规则**。

步骤 4 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 310 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中输入名称。

步骤 6 在**策略 (Policies)** 旁边，选择要在其中生成建议的一个或多个入侵策略。选中 **所有策略** 复选框以选择所有策略。

步骤 7 （可选）在**注释 (Comment)** 字段中输入备注。

请保持注释简短。注释显示在计划日历页面的“任务详细信息”(Task Details) 部分中。

步骤 8 （可选）要通过邮件发送任务状态消息，请在**邮件状态收件人：(Email Status To:)** 字段中输入邮件地址（或以逗号分隔的多个邮件地址）。

步骤 9 点击**保存 (Save)**。

相关主题

冲突和更改：网络分析和入侵策略，第 1459 页

关于思科 建议的规则，第 1621 页

软件更新自动化

您可以自动下载并应用选定的版本。

作为初始配置的一部分，系统安排每周下载最新软件的任务，包括最新 VDB。如果任务计划失败且管理中心 有互联网访问权限，我们建议您安排一个周期性任务来下载软件更新，如 自动执行软件下载，第 318 页。 此任务只会下载更新。您负责安装此任务下载的任何更新。

必须安排安装软件更新的任务因正在更新管理中心还是正在使用管理中心更新受管设备而异。

- 要更新 管理中心，请使用“安装最新更新”任务安排软件安装。
- 要使用管理中心自动对其受管设备执行软件更新，必须安排两个任务：
  - 使用“推送最新更新”(Push Latest Update) 任务将更新推送（复制）至受管设备。
  - 使用“安装最新更新”(Install Latest Update) 任务在受管设备上安装更新。

对受管设备安排更新时，请连续安排推送和安装任务；必须首先将更新推送到设备，然后才能进行安装。要自动在设备组上执行软件更新，必须首先选择此组内的所有设备。请在两次任务之间留出足够的时间来完成流程；安排任务至少间隔 30 分钟。如果安排一个更新安装任务，且更新尚未完成从 管理中心 到设备的复制，则安装任务将不成功。然而，如果安排的安装任务每天重复一次，它将在第二天运行时安装推送的更新。

注释 在两种情况下，必须手动上传和安装更新。第一，您无法安排系统进行主要更新。第二，无法为不能访问支持网站的 管理中心 安排更新，或者无法安排来自这些设备的推送。如果 管理中心 未直接连接到互联网，应使用管理接口配置设置一个代理，以便其从支持网站下载更新。

请注意，为在设备组上安装更新而安排的任务会将推送的更新同时安装到设备组内的每台设备。请留出足够的时间，以便设备组内的每台设备都可完成安排的任务。

如果想要加大对此过程的控制，可在得知更新已发布之后，在非高峰时段使用 **Once** 选项下载和安装更新。

相关主题

更新，第 179 页

自动执行软件下载

可创建一个预定任务，自动从思科下载最新软件更新。可使用此任务安排下载计划手动安装的更新。

您必须在全局域中才能执行此任务。

过程

步骤 1 选择系统（⚙）> 工具 > 计划。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表，选择 **Download Latest Update**。

步骤 4 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 310 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 选中 **更新项目**旁边的 **软件** 复选框。

步骤 7 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 8 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 9 点击**保存 (Save)**。

相关主题

配置邮件中继主机和通知地址，第 159 页

自动执行软件推送

如果想要在受管设备上自动安装软件更新，必须先将更新推送至设备，然后再安装。

创建向受管设备推送软件更新的任务时，确保在推送任务与预定安装任务之间预留充分时间，以便将更新复制至设备。

您必须在全局域中才能执行此任务。

过程

步骤 1 选择系统（⚙）> 工具 > 计划。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表，选择 **Push Latest Update**。

步骤 4 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 310 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 从**设备 (Device)** 下拉列表中，选择要更新的设备。

步骤 7 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 8 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 9 点击**保存 (Save)**。

相关主题

配置邮件中继主机和通知地址，第 159 页

自动执行软件安装

请确保在向受管设备推送更新的任务与安装更新的任务之间预留充分的时间。

您必须在全局域中才能执行此任务。

注意 视乎正在安装的更新，设备可能在安装软件之后重新启动。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从**作业类型 (Job Type)** 列表中，选择**安装最新更新 (Install Latest Update)**。

步骤 4 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 310 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 在**设备**下拉列表中，选择要在其上安装更新的设备（包括 管理中心）。

步骤 7 选中**更新项目 (Update Items)** 旁边的**软件 (Software)** 复选框。

步骤 8 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 9 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 10 点击**保存 (Save)**。

相关主题

配置邮件中继主机和通知地址，第 159 页

漏洞数据库更新自动化

可以使用安排功能更新思科漏洞数据库 (VDB)，从而确保正在使用最新信息评估网络主机。您必须将下载、安装和后续部署安排为单独的任务，以便在任务之间留出足够的时间。

注释 作为一次性操作，管理中心上的初始设置会自动下载并安装思科提供的最新VDB。或者，安排任务以下载和安装 VDB 更新以及部署配置。

自动执行 VDB 更新下载

您必须在全局域中才能执行此任务。

开始之前

请确保 管理中心能够访问互联网。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表，选择 **Download Latest Update**。

步骤 4 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 310 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 在**更新项目 (Update Items)** 旁边，选中**漏洞数据库 (Vulnerability Database)** 复选框。

步骤 7 （可选）在 **注释 (Comment)** 字段中输入简要注释。

步骤 8 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 9 点击**保存 (Save)**。

相关主题

配置邮件中继主机和通知地址，第 159 页

自动执行 VDB 更新安装

在 VDB 更新下载任务与更新安装任务之间预留足够的时间。

您必须在全局域中才能执行此任务。

⚠

注意 在大多数情况下，VDB 更新后的第一次部署都会重新启动 Snort 进程，从而中断流量检查。系统会在发生这种情况时向您发出警告（更新的应用检测器和操作系统指纹需要重新启动；漏洞信息则不需要）。在此中断期间，流量是被丢弃还是不经进一步检查直接通过，将取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从**作业类型 (Job Type)** 列表中，选择**安装最新更新 (Install Latest Update)**。

步骤 4 指定要如何安排任务，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 310 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 从**设备**下拉列表中，选择 管理中心。

步骤 7 在**更新项目 (Update Items)** 旁边，选中**漏洞数据库 (Vulnerability Database)** 复选框。

步骤 8 （可选）在 **注释 (Comment)** 字段中输入简要注释。

步骤 9 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 10 点击**保存 (Save)**。

相关主题

配置邮件中继主机和通知地址，第 159 页

使用已安排任务自动执行 URL 过滤更新

为了确保 URL 过滤的威胁数据为最新，系统必须从思科综合安全情报 (CSI) 云获取数据更新。

默认情况下，在启用URL过滤时，也会启用自动更新。但是，如果需要控制这些更新的发生时间，请使用本主题中所述的程序，而不要使用默认更新机制。

尽管每日更新往往较小，如果距离上次更新已超过五天，新 URL 过滤数据可能需要 20 分钟才能下载完成，具体情况视带宽而定。然后，执行更新也可能最多需要 30 分钟。

开始之前

- 确保 管理中心能够访问互联网；请参阅安全、互联网接入和通信端口，第 2219 页。
- 确保 URL 过滤已启用。有关详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 使用类别和信誉启用 *URL* 过滤。
- 验证未选中 **集成** > **其他集成** 菜单下 **云服务** 上的 **启用自动更新** 。
- 您必须在全局域中才能执行此任务。您必须具有 URL 过滤许可证。

过程

步骤 1 选择**系统**（⚙） > **工具** > **计划**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表，选择 **Update URL Filtering Database**。

步骤 4 指定要如何安排更新，**一次性 (Once)** 或者**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 310 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 7 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 8 点击**保存 (Save)**。

相关主题

配置邮件中继主机和通知地址，第 159 页

预定任务审核

添加预定任务后，即可查看这些任务，评估它们的状态。在页面的“查看选项”(View Options) 部分，查使用日历和预定任务列表查看预定任务。

Calendar 视图选项可用于查看哪些预定任务在哪天发生。

“任务列表”(Task List) 显示一列任务及其状态。打开日历时，任务列表出现在日历下方。此外，也可通过从日历中选择日期或任务来查看它。

可编辑先前创建的预定任务。如果想要测试一次预定任务，确保参数正确，此功能特别有用。稍后，任务成功完成后，即可将其更改为周期性任务。

可从“计划视图”(Schedule View) 页面执行两类删除。可删除尚未运行的特定一次性任务，也可删除周期性任务的每个实例。如果删除周期性任务的一个实例，该任务的所有实例均将删除。如果删除预定运行一次的任务，则仅删除该任务。

任务列表详细信息

表 *41:* 任务列表列

列	说明
名称	显示预定任务的名称及与其关联的注释。
类型	显示预定任务的类型。
开始时间 (Start Time)	显示预定任务的开始日期和时间。
频率 (Frequency）	显示任务的运行频率。
上次运行时间	显示实际开始日期和时间。 对于周期性任务，这适用于最近执行。
上次运行状态	描述预定任务的当前状态。 • **复选标记** （） 指明任务已成功运行。 • 问号图标 (**问号** （）) 指明任务处于未知状态。 • 感叹号图标 () 指明任务已失败。 对于周期性任务，这适用于最近执行。
下次运行时间	显示周期性任务的下次执行时间。 为一次性任务显示“不适用”(N/A)。
创建者	显示创建预定任务的用户的名称。
编辑	编辑预定任务。
删除	删除预定任务。

在日历中查看预定任务

在多域部署中，只能查看当前域的预定任务。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 可使用日历视图执行以下任务：

- 点击 **双左箭头**（«）可后退一年。
- 点击 **单左箭头**（‹）可后退一个月。
- 点击 **单右箭头**（›）可向前移动一个月。
- 点击 **双右箭头**（»）可向前移动一年。
- 点击**今天 (Today)**，返回当前月份和年份。
- 点击**添加任务 (Add Task)**，安排新任务。
- 点击一个日期，在日历下方的任务列表中查看所有预定任务的特定日期。
- 点击在某个日期发生的特定任务，在日历下方的任务列表中查看此任务。

编辑预定任务

在多域部署中，只能为当前域编辑预定任务。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 在日历上，点击要编辑的任务，或者任务出现的日期。

步骤 3 在 **任务详细信息** 表中，点击要编辑的任务旁边的 **编辑**（✎）。

步骤 4 编辑任务。

步骤 5 点击**保存 (Save)**。

删除预定任务

在多域部署中，只能删除当前域的预定任务。

过程

步骤 1 选择**系统**（⚙）> **工具** > **计划**。

步骤 2 在日历中，点击要删除的任务。对于周期性任务，请点击任务的实例。

步骤 3 在 **任务详情** 表中，点击 **删除**（ ），然后确认您的选择。

第 16 章

导入/导出

以下主题介绍如何使用导入/导出功能：

关于配置导入/导出

可以使用导入/导出功能在设备之间复制配置。导入/导出不是备份工具，但可简化将新设备添加到部署的过程。

既可导出单项配置，也可通过单次操作导出一组（相同类型或不同类型的）配置。当您稍后将软件包导入另一台设备时，您可选择要导入软件包中的哪些配置。

导出的数据包包含该配置的版本信息，从而确定是否可以将该配置导入到另一设备上。当设备兼容但数据包包含重复配置时，系统会提供解决方法选项。

注释 导入和导出设备必须运行相同版本的Firepower系统。对于访问控制及其子策略（包括入侵策略），入侵规则更新版本也必须匹配。如果版本不匹配，导入将失败。您可以使用导入/导出功能更新入侵规则。相反，请下载并应用最新的规则更新版本。

支持导入/导出的配置

以下配置支持导入/导出：

- 访问控制策略及其调用的策略：预过滤器、网络分析、入侵、SSL、文件、威胁防御服务策略
- 入侵策略，与访问控制无关
- NAT 策略（仅限 Cisco Secure Firewall Threat Defense）

- FlexConfig 策略。但在导出该策略时，将会清除任何密钥变量的内容。在导入使用密钥的 FlexConfig 策略后，必须手动编辑所有密钥的值。
- 平台设置
- 运行状况策略
- 警报响应
- 应用检测器（用户定义的检测器以及那些由思科专业服务提供的检测器）
- 控制面板
- 自定义表
- 自定义工作流程
- 保存的搜索
- 自定义用户角色
- 报告模板
- 第三方产品和漏洞映射

配置导入/导出的特殊注意事项

当导出配置时，系统也会导出其他所需的配置。例如，导出访问控制策略也会导出该策略调用的任何子策略、该策略使用的对象和对象组、祖先策略（在多域部署中）等等。又例如，如果导出启用了外部身份验证的平台设置策略，则也会导出身份验证对象。但是，也有一些例外：

- 系统提供的数据库和源 - 系统不会导出 URL 过滤类别和信誉数据、思科情报源数据或地理位置数据库 (GeoDB)。确保部署中的所有设备可从思科获取最新信息。
- 全局安全情报列表 - 系统会导出与导出的配置关联的全局安全情报阻止和 不阻止 名单。（在多域部署中，不管当前域如何，都会发生此情况。系统**不**导出后代域列表。）导入过程将这些名单转换为用户创建的列表，然后将这些新列表用于导入的配置中。这可确保导入的列表不会与现有全局阻止和 不阻止 名单发生冲突。要在导入 管理中心 时使用全局列表，请将这些列表手动添加到导入的配置中。
- 入侵策略共享层 - 导出过程会中断入侵策略共享层。以前共享的层包含在数据包中，而导入的入侵策略不包含共享层。
- 入侵策略默认变量集 - 导出数据包包含一个默认变量集，此变量集包含自定义变量及带用户定义值的系统提供的变量。导入过程会使用导入的值更新导入 管理中心上的默认变量集。但是，导入过程**不**会删除不存在于导出数据包中的自定义变量。对于在导出数据包中未设置的值，导入过程也不会恢复导入 管理中心上的用户定义值。因此，如果导入 管理中心具有配置不同的默认变量，则导入的入侵策略的行为可能会与预期大不相同。
- 自定义用户对象 - 如果您在 管理中心中创建了自定义用户组或对象，并且此类自定义用户对象是访问控制策略中任何规则的一部分，那么请注意，导出文件 (.sfo) 不会包含用户对象信息，因此在导入此类策略时，对此类自定义用户对象的任何引用都将被删除，不会导入到目标 管理中

心。为了避免由于缺少用户组而引起的检测问题，请手动将自定义的用户对象添加到新的 管理中心，并在导入后重新配置访问控制策略。

导入对象和对象组时：

- 通常，导入过程将对象和对象组作为新对象和对象组导入，您不能替换现有的对象和对象组。但是，如果采用导入的配置的网络和端口对象或对象组与现有对象或对象组匹配，则导入的配置将重用现有对象/对象组，而不是创建新的对象/对象组。系统通过比较每个网络和端口对象/对象组的名称（不包括任何自动生成的编号）和内容来确定匹配。
- 如果在导入 管理中心时导入对象的名称与现有对象匹配，系统会将自动生成的编号附加到导入的对象和对象组的名称，以使其唯一。
- 您必须将导入的配置中使用的任何安全区域和接口组映射到导入 管理中心管理的匹配类型区域和组。
- 如果导出使用包含私钥的 PKI 对象的配置，系统会在导出之前解密私钥。导入时，系统会使用随机生成的密钥加密密钥。

配置导入/导出的要求和必备条件

型号支持

任意

支持的域

任意

用户角色

- 管理员

导出配置

导出过程可能需要几分钟，取决于正在导出的配置数量以及这些配置引用的对象数量。

提示 Firepower 系统中的许多列表页面的列表项旁均包括 **YouTube EDU**（ ）。如果该图标存在，您可将其作为下列导出步骤的快速替代项。

开始之前

- 确认导入和导出设备运行的是同一版本的Firepower系统。对于访问控制及其子策略（包括入侵策略），入侵规则更新版本也必须匹配。

过程

步骤 1 选择**系统**（⚙）> **工具** > **导入/导出**。

步骤 2 点击 **折叠**（∨） 和 **展开**（>） 图标以折叠和展开可用配置列表。

步骤 3 选中要导出的配置并点击**导出 (Export)**。

步骤 4 按照网页浏览器提示将已导出软件包保存至计算机。

导入配置

视乎正在导入的配置数量以及这些配置所引用的对象数量，导入过程可能需要几分钟。

注释 如果您注销系统 或者点击 **导入 (Import)**后用户会话超时，导入过程将在后台继续进行，直到完成为止。

开始之前

- 确认导入和导出设备运行的是同一版本的软件系统。对于访问控制及其子策略（包括入侵策略），入侵规则更新版本也必须匹配。

过程

步骤 1 在导入设备上，选择**系统**（⚙）> **工具** > **导入/导出**。

步骤 2 点击**上传软件包**。

步骤 3 输入已导出的软件包的路径或浏览到其位置，然后点击**上传 (Upload)**。

步骤 4 如果没有版本不匹配情况或其他问题，请选择要导入的配置，然后点击**导入 (Import)**。
如果无需执行任何冲突解决方案或接口对象映射，则表明导入完成，并会显示成功消息。跳过此程序的其余步骤。

步骤 5 如果提示，请在导入冲突解决方案页面上，将已导入的配置中使用的接口对象映射到具有由导入 管理中心管理的匹配接口类型的区域和组。

源和目标接口对象的接口对象类型（安全区域或接口组）以及接口类型（被动，内联，路由等等）必须匹配。有关信息，请参阅接口，第 995 页。

如果您正在导入的配置引用尚不存在的安全区域或接口组，则可以将其映射到现有接口对象或创建新接口对象。

注释　对于单个访问控制策略，您可以选择将现有策略替换为导入的策略。但是，对于嵌套访问控制策略，只能将其作为新策略导入。

步骤 6　点击 **Import**。

步骤 7　如果提示，请在“导入解决方案”(Import Resolution) 页面上，展开每项配置并选择相应的选项，如解决导入冲突，第 331 页中所述。

步骤 8　点击 **Import**。

步骤 9　更新所有源。

例如，转到 **对象 > 对象管理 > 安全情报**，然后点击 URL、网络和 DNS 列表和源页面上的 **更新源** 按钮。

导入的策略不包括源内容。

步骤 10　等待所有源更新完成，然后再将策略部署到设备。

下一步做什么

- 或者，查看总结已导入的配置的报告；请参阅查看任务消息，第 277 页。

解决导入冲突

当您尝试导入配置时，系统会确定设备上是否已存在同一名称和类型的配置。在多域部署中，系统还会确定某个配置是在当前域还是在其任何祖先域或后代域中定义的配置的重复。（您无法查看后代域中的配置，但如果后代域中存在具有重复名称的配置，则系统会通知您发生冲突。）当导入包含重复配置时，系统会提供适合于您的部署的解决方法选项，其中包括：

- **保持现有配置 (Keep existing)**

  系统不导入该配置。

- **替换现有配置 (Replace existing)**

  系统使用选择用于导入的配置覆盖当前配置。

- **保留最新配置 (Keep newest)**

  仅在所选配置的时间戳比设备上的当前配置中的时间戳更新时，系统才会导入所选配置。

- **导入为新配置 (Import as new)**

  系统导入所选重复配置，将系统生成的编号附加到名称以使其唯一。（可以在完成导入过程之前更改此名称。）设备上的原始配置保持不变。

系统提供的解决方法选项取决于部署是否使用域，以及导入的配置是在当前域中定义的配置的重复，还是在当前域的祖先或后代中定义的配置的重复。下表列出系统何时提供或不提供解决方法选项。

解决方法选项	Cisco Secure Firewall Management Center		受管设备
	在当前域中重复	在祖先域或后代域中重复	
保持现有配置 (Keep existing)	是	是	是
替换现有配置 (Replace existing)	是	不支持	是
保留最新配置 (Keep newest)	是	不支持	是
导入为新配置 (Import as new)	是	是	是

当导入包含使用干净或自定义检测文件列表的文件策略的访问控制策略，并且文件列表出现重复名称冲突时，系统会提供上表中所述的冲突解决方法选项，但是系统对策略和文件列表执行的操作会有所差异，如下表所述：

解决方法选项	系统操作	
	访问控制策略及其关联的文件策略导入为新策略，并且合并文件列表	现有访问控制策略及其关联的文件策略和文件列表保持不变
保持现有配置 (Keep existing)	不支持	是
替换现有配置 (Replace existing)	是	否
导入为新配置 (Import as new)	是	否
保持最新配置 (Keep newest)，并且导入的访问控制策略为最新策略	是	否
保持最新配置 (Keep newest)，并且现有访问控制策略为最新策略	不支持	是

如果修改设备上的已导入配置，然后将该配置重新导入到同一设备，则必须选择要保留的配置版本。

第 VI 部分

报告和警报

第 17 章

含警报响应的外部警报

以下主题介绍如何使用警报响应从 Cisco Secure Firewall Management Center发送外部事件警报：

Cisco Secure Firewall Management Center 警报响应

通过 SNMP、系统日志或邮件发送外部事件通知有助于重要系统监控。Cisco Secure Firewall Management Center使用可配置的警报响应与外部服务器交互。警报响应是一种配置，用于表示与电子邮件、SNMP 或系统日志服务器的连接。它们称为响应的原因在于，可将它们用于发送警报，以响应由 Firepower 检测到的事件。可以配置多个警报响应，以便向不同的监控服务器和/或人员发送不同类型的警报。

注释 根据您的设备和 Firepower 版本，警报响应可能不是发送系统日志消息的最佳方式。请参阅 《Cisco Secure Firewall Management Center 设备配置指南》关于系统日志和 配置安全事件系统日志消息的最佳实践。。

注释 使用警报响应的警报是由 Cisco Secure Firewall Management Center发送的。不使用警报响应的入侵电子邮件警报也是由 Cisco Secure Firewall Management Center发送的。相比之下，基于单个入侵规则触发的 SNMP 和 系统日志警报是由受管设备直接发送的。

在大多数情况下，外部警报中的信息与您记录到数据库中的任何相关联事件中的信息相同。但是，无论是何种基础事件类型，对于关联规则中包含连接跟踪器的关联事件警报，您收到的信息都与流量量变曲线更改警报相同。

可在“警报”页面（**策略** > **操作** > **警报**）上创建和管理警报响应。新的警报响应自动启用。要暂停警报生成，可以禁用警报响应，而非将它们删除。

对警报响应所做的更改会立即生效，但将连接日志发送到 SNMP 陷阱或系统日志服务器时除外。

在多域部署中，当您创建警报响应时，它属于当前域。后代域也可以使用此警报响应。

支持警报响应的配置

创建警报响应后，可以使用它从 Cisco Secure Firewall Management Center发送以下外部警报。

警报/事件类型	有关详细信息，请参阅
按影响标志划分的入侵事件	配置影响标志警报，第 341 页
按类型划分的发现事件	配置发现事件警报，第 342 页
由 恶意软件防护 检测到的恶意软件和追溯性恶意软件事件（“基于网络”）	配置 恶意软件防护警报，第 342 页
按运行状况模块和严重性级别划分的运行状况事件	创建运行状况监控器警报，第 246 页

警报报告的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员

创建 SNMP 警报响应

对于除了 威胁防御的设备类型，可使用 SNMPv1、SNMPv2 或 SNMPv3 创建 SNMP 警报响应。

注释 为 SNMP 协议选择 SNMP 版本时，请注意 SNMPv2 仅支持只读社区，SNMPv3 仅支持只读用户。此外，SNMPv3 还支持使用 AES128 加密。

如果想要使用 SNMP 监控 64 位值，则必须使用 SNMPv2 或 SNMPv3。SNMPv1 不支持 64 位监控。

开始之前

- 如果网络管理系统需要 Cisco Secure Firewall Management Center的管理信息库 (MIB) 文件，则可在 `/etc/sf/DCEALERT.MIB` 处获取该文件。

过程

步骤 1 选择**策略** > **操作** > **警报**。

步骤 2 从**创建警报 (Create Alert)** 下拉菜单中，选择**创建 SNMP 警报 (Create SNMP Alert)**。

步骤 3 编辑 SNMP 警报配置字段：

a) **名称**-输入名称以指定 SNMP 响应。

b) **陷阱服务器**-输入 SNMP 陷阱服务器的主机名或 IP 地址。

注释 如果在此字段中输入了无效的 IPv4 地址（例如 192.169.1.456），则系统**不会**发出警告。相反，无效地址会被视为主机名。

c) **版本**-从下拉列表中，选择要使用的 SNMP 版本。SNMPv3 是默认设置。

选项包括：

- **SNMPv1** 或 **SNMPv2**：在 **社区字符串** 字段中输入只读 SNMP 社区名称，然后跳至程序末尾。

  注释 不包含特殊字符 (< > / % # & ? ' 等）在 SNMP 社区字符串名称中。

- 对于 **SNMP v3**：在 **用户名** 字段中，输入要使用 SNMP 服务器对其进行身份验证的用户的名称并继续下一步。

d) **身份验证协议**-从下拉列表中选择要用于身份验证的协议。

选项包括：

- **MD5**- 消息摘要 5 (MD5) 散列功能。
- **SHA**—安全散列算法 (SHA) 散列函数。

e) **身份验证密码**-输入用于身份验证的密码。

f) **隐私协议**－从下拉列表中选择要用于加密私有密码的协议。

选项包括：

- **DES**-在对称密钥块算法中使用 56 位密钥的数据加密标准 (DES)。
- **AES**-在对称密码算法中使用 56 位密钥的高级加密标准 (AES)。
- **AES128**-在对称密码算法中使用 128 位密钥的 AES。密钥越长，其提供的安全性就越高，但性能会随之降低。

g) **隐私密码**-输入 SNMP 服务器所需的隐私密码。如果指定私有密码，则隐私被启用，且还必须指定身份验证密码。

h) **引擎 ID**-使用偶数数字（十六进制表示法）输入 SNMP 引擎的标识符。

使用 SNMPv3 时，系统使用引擎 ID 值对消息进行编码。SNMP 服务器需要使用该值对消息进行解码。

思科建议您使用十六进制版本的 Cisco Secure Firewall Management Center的 IP 地址。例如，如果 Cisco Secure Firewall Management Center 的 IP 地址为 10.1.1.77，请使用 0a01014D0。

步骤 4 点击**保存 (Save)**。

下一步做什么

更改会立即生效，但以下情况除外：

如果你使用警报响应来发送连接日志，你必须在编辑这些警报响应后部署配置更改。

创建系统日志警报响应

配置系统警报响应时，可指定与系统日志消息相关联的严重性和消息来源，以确保它们得到系统日志服务器的正确处理。消息来源指明创建消息的子系统，严重性界定消息的严重性。消息来源和严重性不显示在系统日志中的实际消息中，而是告知接收系统日志消息的系统如何对消息进行归类。

提示 有关系统日志如何运行及如何对其进行配置的更多详细信息，请参阅系统文档。在 UNIX 系统上，`syslog` 和 `syslog.conf` 的 `man` 页面提供了概念信息和配置说明。

虽然在创建系统日志警报响应时可选择任何类型的设施，但是应根据系统日志服务器选择合适的设施；并非所有系统日志服务器都支持所有设施。对于 UNIX 系统日志服务器，`syslog.conf` 文件应指示哪些设备保存到了服务器的哪些日志文件上。

开始之前

- 在许多情况下，不建议使用此程序发送系统日志消息。
- 确认系统日志服务器可接受远程消息。

过程

步骤 1 选择**策略** > **操作** > **警报**。

步骤 2 从**创建警报 (Create Alert)** 下拉菜单中，选择**创建系统日志警报 (Create Syslog Alert)**。

步骤 3 输入警报的**名称 (Name)**。

步骤 4 在**主机 (Host)** 字段中，输入系统日志服务器的主机名或 IP 地址。

注释 如在此字段中输入了无效的 IPv4 地址（例如 192.168.1.456），则系统**不会**发出警告。相反，无效地址会被视为主机名。

步骤 5 在**端口 (Port)** 字段中，输入服务器用于系统日志消息的端口。默认情况下，此值为 514。

步骤 6 从**设施 (Facility)** 列表中，选择系统日志警报设施，第 339 页中所述的设施。

步骤 7 从**严重性 (Severity)** 列表中，选择系统日志严重性级别，第 340 页中所述的严重性。

步骤 8 在**标记 (Tag)** 字段中，输入要与系统日志消息一起显示的标记名称。

例如，如果要在发送到系统日志的所有消息前加上 `FromMC`，请在字段中输入 `FromMC`。

步骤 9 点击**保存 (Save)**。

下一步做什么

更改会立即生效，但以下情况除外：

如果你使用警报响应来发送连接日志到系统日志服务器，你必须在编辑这些警报响应后部署配置更改。

系统日志警报设施

下表列出了可选择的系统日志设施。

表 *42:* 可用的系统日志设施

设施	说明
ALERT	警报消息。
审计	审核子系统生成的消息。
AUTH	与安全和授权关联的消息。
AUTHPRIV	与安全和授权关联的访问受限的消息。在很多系统上，这些消息会转发至一个安全文件。
CLOCK	时钟后台守护程序生成的消息。 请注意，运行 Windows 操作系统的系统日志服务器将使用 `CLOCK` 消息来源。

设施	说明
CRON	时钟守护程序生成的消息。 请注意，运行 Linux 操作系统的系统日志服务器将使用 CRON 消息来源。
DAEMON	系统后台守护程序生成的消息。
FTP	FTP 后台守护程序生成的消息。
KERN	内核生成的消息。很多系统会在这些消息出现后将其传送至控制台打印。
LOCAL0-LOCAL7	内部进程生成的消息。
LPR	打印子系统生成的消息。
邮件	邮件系统生成的消息。
NEWS	网络新闻子系统生成的消息。
NTP	NTP 守护程序生成的消息。
SYSLOG	系统日志后台守护程序生成的消息。
USER	用户级进程生成的消息。
UUCP	UUCP 子系统生成的消息。

系统日志严重性级别

下表列出可选择的标准系统日志严重性级别。

表 *43:* 系统日志严重性级别

级别	说明
ALERT	应立即更正的状况。
CRIT	临界状况。
DEBUG	包含调试信息的消息。
EMERG	向所有用户广播的紧急状况。
ERR	错误状况。
INFO	参考性消息。
通知	需要注意但非错误的状况。
警告	警告消息。

创建邮件警报响应

开始之前

- 确认 Cisco Secure Firewall Management Center可反向解析其自身的 IP 地址。
- 配置邮件中继主机，如配置邮件中继主机和通知地址 ， 第 159 页中所述。

注释 不可以使用邮件警报记录连接。

过程

步骤 1 选择**策略 > 操作 > 警报**。

步骤 2 从**创建警报 (Create Alert)** 下拉菜单中，选择**创建邮件警报 (Create Email Alert)**。

步骤 3 为警报响应输入**名称 (Name)**。

步骤 4 在**收件人 (To)** 字段中，输入要将警报发送到其中的邮箱地址（用逗号分隔）。

步骤 5 在**发件人 (From)** 字段中，输入要显示为警报发件人的邮箱地址。

步骤 6 在 **Relay Host** 旁，验证列出的邮件服务器是要用于发送警报的服务器。

提示 要更改电邮服务器，请点击 **编辑**（ ）。

步骤 7 点击**保存 (Save)**。

配置影响标志警报

可将系统配置为只要出现带有特定影响标志的入侵事件就会发出警报。影响标志可通过将入侵数据、网络发现数据和漏洞信息相关联来帮助评估入侵对网络的影响。

您必须具有 威胁 智能许可证或保护经典许可证才能配置这些警报。

过程

步骤 1 选择**策略 > 操作 > 警报**。

步骤 2 点击 **影响标志警报**。

步骤 3 在**警报 (Alerts)** 部分中，选择要用于每种警报类型的警报响应。

提示 要创建新警报响应，请从任何下拉列表中选择**新建 (New)**。

步骤 4 在**影响配置 (Impact Configuration)** 部分中，选中相应复选框为每个影响标志指定要接收的警报。

步骤 5 点击**保存 (Save)**。

配置发现事件警报

可将系统配置为只要出现特定类型的发现事件就会发出警报。

开始之前

- 将网络发现策略配置为记录要为其配置警报的发现事件类型，如 《Cisco Secure Firewall Management Center 设备配置指南》中 网络发现策略 中所述

过程

步骤 1 选择**策略 > 操作 > 警报**。

步骤 2 点击 **发现事件警报**。

步骤 3 在**警报 (Alerts)** 部分中，选择要用于每种警报类型的警报响应。

提示 要创建新警报响应，请从任何下拉列表中选择**新建 (New)**。

步骤 4 在**事件配置 (Events Configuration)** 部分中，选中与要为每种发现事件类型接收的警报对应的复选框。

步骤 5 点击**保存 (Save)**。

配置 恶意软件防护警报

可将系统配置为只要 恶意软件防护 生成任何恶意软件事件（包括回溯性事件）（即，生成“基于网络的恶意软件事件”），就向您发出警报。不能对面向终端的AMP生成的恶意软件事件（“基于终端的恶意软件事件”）发出警报。

开始之前

- 配置文件策略以执行恶意软件云查找并将该策略与访问控制规则相关联，。 有关详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的访问控制概述。
- 您必须具有 恶意软件 许可证才能配置这些警报。

过程

步骤 1 选择策略 > 操作 > 警报。

步骤 2 点击 高级恶意软件防护警报。

步骤 3 在警报 (Alerts) 部分中，选择要用于每种警报类型的警报响应。

提示 要创建新警报响应，请从任何下拉列表中选择新建 (New)。

步骤 4 在事件配置 (Event Configuration) 部分中，选中与要为每种恶意软件事件类型接收的警报对应的复选框。

请注意，所有基于网络的恶意软件事件 (All network-based malware events) 包括追溯性事件 (Retrospective Events)。

（根据定义，基于网络的恶意软件事件不包括由面向终端的 AMP 生成的事件。）

步骤 5 点击保存 (Save)。

第 18 章

入侵事件的外部警报

以下主题介绍如何配置入侵事件的外部警报：

关于入侵规则的外部警报

外部入侵事件通知可帮助进行关键系统监控：

- SNMP - 按照入侵策略配置并从受管设备发送。您可以按照入侵规则启用 SNMP 警报。
- 系统日志 - 按照入侵策略配置并从受管设备发送。当您在入侵策略中启用系统日志警报时，可以为该策略中的每个规则将其打开。
- 邮件 - 跨所有入侵策略配置并从 Cisco Secure Firewall Management Center发送。您可以按照入侵规则启用邮件警报，并限制警报的长度和频率。

请记住，如果您配置了入侵事件抑制或阈值，系统可能不会每次在规则触发时都生成入侵事件（因此可能不会发送警报）。

在多域部署中，可以配置任何域中的外部警报。在祖先域中，系统会为后代域中的入侵事件生成通知。

注释 Cisco Secure Firewall Management Center还使用 SNMP、系统日志和邮件警报响应来发送不同类型的外部警报；请参阅Cisco Secure Firewall Management Center 警报响应，第 335 页。系统不使用警报响应来根据单个入侵事件发送警报。

相关主题

入侵策略中的入侵事件通知过滤器，第 1489 页

入侵事件外部警报的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

入侵事件外部警报的要求和前提条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

配置入侵事件的 SNMP 警报

在入侵策略中启用外部 SNMP 警报后，可以配置各个规则以便在触发规则时发送 SNMP 警报。这些警报是从受管设备发送的。

过程

步骤 1 在入侵策略编辑器的导航窗格中，点击**高级设置**。

步骤 2 确保 **SNMP 警报**是**已启用**状态，然后点击**编辑**。
页面底部消息会识别包含配置的入侵策略层。

步骤 3 选择 **SNMP 版本**，然后按入侵 SNMP 警报选项，第 347 页中所述指定配置选项。

步骤 4 在导航窗格中，点击**规则**。

步骤 5 在规则窗格中，选择要设置 SNMP 警报的规则，然后选择**警报** > **添加 SNMP 警报**。

步骤 6 要保存自上次策略确认以来在此策略中进行的更改，请选择**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

入侵 SNMP 警报选项

如果网络管理系统要求使用管理信息库文件 (MIB)，您可以从Cisco Secure Firewall Management Center 中获取，具体位置为 `/etc/sf/DCEALERT.MIB`。

SNMP v2 选项

选项	说明
陷阱类型	警报中出现的 IP 地址所用到的陷阱类型。 如果网络管理系统正常显现 INET_IPV4 地址类型，则选择**二进制形式**选项。否则，应选择**字符串形式**。例如，HP Openview 需要选择**字符串形式**。
陷阱服务器 (Trap Server)	收到 SNMP 陷阱通知的服务器。 可指定单一 IP 地址或主机名。
社区字符串 (Community String)	群体名称。

SNMP v3 选项

受管设备使用引擎 ID 值对 SNMPv3 警报进行编码。要解码警报，您的 SNMP 服务器需要此值，即发送设备的管理接口 IP 地址的十六进制版本，并附加“01”。

例如，如果发送 SNMP 警报的设备的管理接口 IP 地址是 172.16.1.50，则引擎 ID 值为 0xAC10013201。

选项	说明
陷阱类型	警报中出现的 IP 地址所用到的陷阱类型。 如果网络管理系统正常显现 INET_IPV4 地址类型，则选择**二进制形式**选项。否则，应选择**字符串形式**。例如，HP Openview 需要选择**字符串形式**。

选项	说明
陷阱服务器 (Trap Server)	收到 SNMP 陷阱通知的服务器。 可指定单一 IP 地址或主机名。
身份验证密码 (Authentication Password)	身份验证所需的密码。SNMP v3 使用消息摘要 5 (MD5) 散列函数或安全散列算法 (SHA) 散列函数进行密码加密，具体取决于配置。 一旦指定身份验证密码，身份验证即可启用。
私有密码 (Private Password)	用于保护隐私的 SNMP 密钥。SNMP v3 采用数据加密标准 (DES) 分组密码对密码进行加密。输入 SNMP v3 密码后，初始配置期间的密码会以明文显示，但以加密格式保存。 如果指定私有密码，则隐私被启用，且还必须指定身份验证密码。
用户名	SNMP 用户名。

为入侵事件配置系统日志警报

在入侵策略中启用系统日志警报后，系统将在受管设备自身或者一台或多台外部主机上向系统日志发送所有入侵事件。如果指定了外部主机，系统将从受管设备发送系统日志警报。

过程

步骤 1 在入侵策略编辑器的导航窗格中，点击**高级设置**。

步骤 2 请确保**系统日志警报**为**已启用**，然后点击**编辑**。
页面底部消息会识别包含配置的入侵策略层。**系统日志警报**页面添加在**高级设置**下。

步骤 3 输入您要发送系统日志警报的**日志记录主机**的 IP 地址。

如果您将**日志记录主机**字段留空，则系统将从关联访问控制策略中的“日志记录”获取日志记录主机详细信息。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

步骤 4 选择**设施**和**严重性**级别，如入侵系统日志警报的设施和严重性，第 349 页中所述。

步骤 5 要保存自上次策略确认以来在此策略中进行的更改，请选择**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

入侵系统日志警报的设施和严重性

受管设备可以使用特定的设施和**严重性**将入侵事件作为系统日志警报发送，以便日志主机可以对警报进行分类。设施指定生成警报的子系统。这些设施和**严重性**值不会出现在实际的系统日志消息中。

根据您的环境选择有意义的值。本地配置文件（如基于 UNIX 的日志记录主机上的 syslog.conf）可能指示将哪些设施保存到哪些日志文件中。

系统日志警报设施

设施	说明
ALERT	警报消息。
AUTH	与安全和授权关联的消息。
AUTHPRIV	与安全和授权关联的访问受限的消息。在很多系统上，这些消息会转发至一个安全文件。
CRON	时钟守护程序生成的消息。
DAEMON	系统后台守护程序生成的消息。
FTP	FTP 后台守护程序生成的消息。
KERN	内核生成的消息。很多系统会在这些消息出现后将其传送至控制台打印。
LOCAL0-LOCAL7	内部进程生成的消息。
LPR	打印子系统生成的消息。
邮件	邮件系统生成的消息。
NEWS	网络新闻子系统生成的消息。
SYSLOG	系统日志后台守护程序生成的消息。
USER	用户级进程生成的消息。
UUCP	UUCP 子系统生成的消息。

系统日志警报严重性

级别	说明
EMERG	紧急状况，向所有用户广播
ALERT	需要立即更正的状况
CRIT	严重的状况

级别	说明
ERR	错误状况
WARNING	警告消息
通知	并未出现错误，但需引起注意的状况
INFO	参考性消息
DEBUG	包含调试信息的消息

配置入侵事件的邮件警报

如果启用了入侵邮件警报，无论哪个受管设备或入侵策略检测到入侵，系统都可以在生成入侵事件时发送邮件。这些警报从 Cisco Secure Firewall Management Center发送。

开始之前

- 配置邮件主机以接收邮件警报；请参阅配置邮件中继主机和通知地址，第 159 页。
- 确保 Cisco Secure Firewall Management Center可以反转解析自己的 IP 地址。

过程

步骤 1 选择**策略 > 操作 > 警报**。

步骤 2 点击 **入侵邮件**。

步骤 3 如入侵邮件警报选项，第 350 页中所述，选择警报选项，包括要警报的入侵规则或规则组。

步骤 4 点击**保存 (Save)**。

入侵邮件警报选项

On/Off

启用或禁用入侵邮件警报。

注释 启用它将为所有规则启用警报，除非选择单个规则。

发件人/收件人地址

邮件发件人和收件人。您可以指定一个以逗号分隔的收件人列表。

最大警报数和频率

Cisco Secure Firewall Management Center将按时间间隔发送（**频率**）的邮件警报最大数（**最大警报数**）。

Coalesce Alerts

通过将具有相同源 IP 和规则 ID 的警报分组来减少发送的警报数。

Summary Output

启用简要警报，适用于文本受限的设备。简要警报包含以下内容：

- 时间戳
- 协议
- 源和目标 IP 和端口
- 消息
- 同一个源 IP 生成的入侵事件数量

例如：`2011-05-18 10:35:10 10.1.1.100 icmp 10.10.10.1:8 -> 10.2.1.3:0 snort_decoder: Unknown Datagram decoding problem! (116:108)`

如果启用**摘要输出**，还应考虑启用**组合警报**。您可能还希望降低**最大警报数**，以避免超过文本消息限制。

时区

警报时间戳的时区。

Email Alerting on Specific Rules Configuration

允许您选择要在其中设置邮件警报的规则。

第 VII 部分

事件和资产

第 19 章

思科安全分析和日志记录

关于安全分析和日志记录

安全分析和日志记录 (SAL) 是一项集中日志管理和高级威胁检测服务，可提供可扩展的思科防火墙日志记录及相关分析。集中日志记录有助于提供可视性，帮助解决网络访问问题（包括中断），同时启用设备和整体网络运行状况监控。分析可提供针对高级威胁的检测。

SAL 服务可通过以下两种方法使用：

- 安全分析和日志记录 (SaaS) - 一种托管软件即服务 (SaaS)，使用 Cisco Secure Cloud Analytics（以前称为 Stealthwatch 云）存储事件并提供安全分析数据。此服务会将安全分析和日志记录云数据存储连接到防火墙云管理器 思科防御协调器 (CDO)。

  在本文档中，此方法也被称为 SAL (SaaS)。

- 安全分析和日志记录（本地部署） - 在 Secure Network Analytics（以前称为 Stealthwatch）设备上运行的服务，用于在客户自己的场所存储事件日志。此服务将 安全分析和日志记录（本地部署） 数据连接到本地管理器，Cisco Secure Firewall Management Center。

  在本文档中，此方法也被称为 SAL（本地）。

有关 安全分析和日志记录 的详细信息，请参阅 https://www.cisco.com/c/en/us/products/security/security-analytics-logging/index.html。

SAL 远程事件存储和监控选项的比较

SAL 集成显示了在 管理中心 和 CDO 外部的存储事件数据的类似选项：

	SAL（本地）	SAL (SaaS)
为什么选择此解决方案？	您想增大本地防火墙事件数据存储容量，将此数据保留更长时间，并将事件数据导出到安全网络分析设备。	您希望发送防火墙事件进行存储，并使用 Cisco Secure Cloud Analytics 选择性地让防火墙事件数据可用于安全分析。
许可	购买、许可并设置防火墙后的存储系统。 有关详细信息，请参阅SAL（本地） 的许可 ，第 357 页	购买许可证和数据存储计划，并将数据发送到思科云。 有关详细信息，请参阅SAL (SaaS) 的许可 ，第 362 页
支持的事件类型	• 连接 • 文件和恶意软件 • 入侵 • LINA • 安全情报	• 连接 • 文件和恶意软件 • 入侵 • 安全情报
支持的事件发送方法	支持系统日志和直接集成。	支持系统日志和直接集成。
事件查看	• 查看 Cisco Secure Network Analytics 管理器上的事件。 • 从 管理中心 事件查看器交叉启动，以查看 Cisco Secure Network Analytics 管理器上的事件。 • 在管理中心中查看远程存储的连接和安全智能事件	在 CDO 中查看事件，或者 Cisco Secure Network Analytics 管理器，具体取决于您的许可证。从管理中心 事件查看器交叉启动。

关于SAL（本地）

您可以配置 SAL（本地） 以存储防火墙事件数据，从而在更长的保留期内增加存储量。通过部署安全网络分析设备并将其与防火墙部署集成，您可以将事件数据导出到安全网络分析设备。

这会为您提供以下功能：

- 在 Cisco Secure Network Analytics 设备上存储事件。
- 指定此远程数据源以便在管理中心查看这些事件。
- 使用事件查看器从安全网络分析管理器（以前称为 Stealthwatch 管理控制台）Web 应用 UI 中查看事件数据。
- 从管理中心 UI 交叉启动到事件查看器，以便查看有关交叉启动信息的其他情景。

SAL（本地） 的许可

您必须获取日志记录和故障排除智能许可证才能使用 SAL（本地）。您可以根据预期的数据量获取许可证，同时每天将系统日志数据从防火墙部署发送到您的 Secure Network Analytics 设备。

有关许可 Secure Network Analytics 设备的信息，请参阅《Cisco Secure Network Analytics 智能软件许可指南》。

有关可用 SAL（本地） 许可选项的信息，请参阅《思科安全分析和日志记录订购指南》。

注释 出于许可证计算的目标，数据量会以最接近的整数 GB 来报告。例如，如果一天会发送 4.9 GB，则报告为 4 GB。

管理 CDO 托管 威胁防御 设备的 SAL（本地）

从 Cisco Secure Firewall Threat Defense（以前称为 Firepower 威胁防御）版本 7.2 开始，您可以选择将由 CDO 托管的 威胁防御 设备生成的完全限定事件发送到 管理中心。管理中心 会接收并显示这些事件的数据分析。接收和显示事件数据的 管理中心 也称为仅分析管理中心。。

如果已启用设备以使用 SAL（本地） 向 Cisco Secure Network Analytics 管理器 发送连接事件，您可以在管理中心的事件查看器和情景管理器中查看和使用这些远程存储的事件，并在生成报告时包括这些事件。通过部署 Secure Network Analytics 设备并将其与防火墙部署集成，您可以将事件数据导出到安全网络分析设备。这让您能够在管理中心 UI 中查看和管理事件。您还可以从管理中心 UI 交叉启动到 Cisco Secure Network Analytics 管理器，以便查看和管理事件数据。

管理中心可以接收和显示以下 CDO 托管 威胁防御 设备的事件分析：

- 已载入 CDO 的新设备或现有 威胁防御 设备

  有关将 威胁防御 设备载入 CDO 的信息，请参阅将设备载入 云交付的防火墙管理中心的前提条件 ， 第 9 页。

  工作流程如下：

  1. 将 威胁防御 设备载入 CDO。

     使用将设备载入 云交付的防火墙管理中心的前提条件 ， 第 9 页中所述的载入方法来载入 威胁防御 设备。载入过程包括分配策略和选择适当的许可证。

2. 在相应的管理中心注册此 威胁防御设备。

   要使管理中心显示由 CDO 管理的 威胁防御 设备生成的事件，必须在管理中心注册该 威胁防御 设备。要在 管理中心 中注册此设备，请使用 **configure manager add** {*hostname* | *IPv4_address* | *IPv6_address*}*reg_key*[*nat_id*] CLI 启用要注册的设备，然后使用 **CDO 托管设备 (CDO Managed Device)** 复选框将设备添加到 管理中心。

注释 注册密钥和 NAT ID 必须与在将设备载入 CDO 时使用的密钥和 NAT ID 不同。

   有关详细信息，请参阅《Firepower 管理中心设备配置指南》中的将设备添加到管理中心和使用 *CLI* 完成威胁防御初始配置。

3. 在管理中心查看事件或交叉启动到已配置的 Cisco Secure Network Analytics 管理器。

   在管理中心事件查看器中查看和处理事件。如果 Secure Network Analytics 设备已部署并与防火墙部署集成，则可以将事件数据导出到 Secure Network Analytics 设备。这使您可以从管理中心 UI 交叉启动到 Cisco Secure Network Analytics 管理器，以便查看和管理事件数据。

   有关详细信息，请参阅事件和清单以及使用外部工具的事件分析。

- 管理中心的现有 威胁防御 设备。

  您可以使用更改威胁防御管理器功能将 威胁防御 设备的管理从管理中心更改为 CDO。更改威胁防御管理器功能使您能够将 威胁防御 设备管理从管理中心更改为 CDO。在更改管理器时，您可以选择将这些威胁防御设备生成的事件数据保留在管理中心。如果您选择将事件数据保留在管理中心，则仅在分析模式下才会在管理中心上保留 威胁防御 设备的副本。

  有关详细信息，请参阅将 Cisco Secure Firewall Threat Defense 迁移到云。

  工作流程如下：

  1. 将管理中心载入 CDO

     要将现有的 威胁防御 设备从管理中心载入 CDO，您必须将相应的管理中心载入 CDO。

     有关详细信息，请参阅载入 FMC。

  2. 完成变更威胁防御管理流程

     在更改威胁防御管理过程中更改设备管理器时，您可以选择将这些 威胁防御 设备生成的事件数据保留在管理中心。

     有关详细信息，请参阅将 Cisco Secure Firewall Threat Defense 迁移到云。

  3. 在管理中心查看事件或交叉启动到已配置的 Secure Network Analytics 设备。

     在管理中心事件查看器中查看和处理事件。如果 Secure Network Analytics 设备已部署并与防火墙部署集成，则可以将事件数据导出到 Secure Network Analytics 设备。这使您可以从管理中心 UI 交叉启动到 Cisco Secure Network Analytics 管理器，以便查看和管理事件数据。

     有关详细信息，请参阅事件和清单以及使用外部工具的事件分析。

配置 SAL（本地） 集成

您可以使用以下部署选项之一将 CDO 配置为将事件发送到安全网络分析设备：

- 仅安全网络分析管理器 - 部署独立管理器以接收和存储事件。威胁防御设备会将事件数据发送到网络分析管理器。所有事件数据都会被存储在网络分析管理器上。从管理中心用户界面中，您可以交叉启动管理器以查看有关存储事件的更多信息。
- 安全网络分析数据存储 - 部署思科安全网络分析流收集器以接收事件，部署思科安全网络分析数据存储（包含 3 个思科安全网络分析数据节点）以存储事件和管理器。威胁防御设备会将事件数据发送到流收集器，然后再将事件发送到数据存储进行存储。从管理中心用户界面中，您可以交叉启动管理器以查看有关存储事件的更多信息。

  从 威胁防御 版本 7.2 开始，您可以选择将不同的流收集器关联到不同的设备。

配置 Cisco Secure Network Analytics 管理器

配置 Cisco Secure Network Analytics 管理器 部署以便将 SAL（本地） 与 CDO 托管的 威胁防御 设备集成。

开始之前

请确保执行以下操作：

- 您有一个已调配的 CDO 租户，并具有以下 CDO 用户角色：
  - 管理
  - 超级管理员
- 您的 威胁防御 设备按预期工作，并且正在生成事件。
- 如果您当前使用系统日志将事件从支持直接发送事件的设备版本发送到 Cisco Secure Network Analytics 管理器，请禁用这些设备的系统日志（或为这些设备分配不包含系统日志配置的访问控制策略），以避免在远程卷上复制事件。
- 您有 Cisco Secure Network Analytics 管理器 的主机名或 IP 地址。

注释 您可能会在注册过程中从Cisco Secure Network Analytics管理器注销；请完成所有正在进行的工作，然后再开始使用部署向导。

过程

步骤 1 登录 CDO。

步骤 2 从 CDO 菜单中，导航至 **工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。

步骤 3 选择**防火墙管理中心 (Firewall Management Center)**，然后点击**配置 (Configuration)**。

步骤 4 导航至**集成 (Integration)** > **安全分析和日志记录 (Security Analytics & Logging)**。

步骤 5 在**仅 Cisco Secure Network Analytics 管理器 (Secure Network Analytics Manager Only)** 构件中，点击**开始 (Start)**。

步骤 6 输入 Cisco Secure Network Analytics 管理器 的主机名或 IP 地址和端口号，然后点击**下一步 (Next)**。

步骤 7 将更改部署到托管设备。

在将日志记录策略更改部署到已注册的威胁防御设备之前，事件数据不会被记录到SAL（本地）。

注释 如果必须更改其中任何配置，请再次运行向导。如果禁用配置或再次运行向导，则会保留除帐户凭证之外的所有设置。

您可以在管理中心的事件查看器和情景管理器中查看和使用这些远程存储的事件，并在生成报告时包括这些事件。您还可以从管理中心中的事件交叉启动，以便查看 Secure Network Analytics 设备上的相关数据。

有关详情，请参阅管理中心的在线帮助。

步骤 8 点击**确定 (OK)**。

配置 Secure Network Analytics 数据存储

配置 Secure Network Analytics 数据存储部署以便将 SAL（本地） 与 CDO 管理的 威胁防御 设备集成。

开始之前

请确保执行以下操作：

- 您有一个已调配的 CDO 租户，并具有以下 CDO 用户角色：
  - 管理
  - 超级管理员
- 您的 威胁防御 设备按预期工作，并且正在生成事件。
- 如果您当前使用系统日志将事件从支持直接发送事件的设备版本发送到安全网络分析设备，请禁用这些设备的系统日志（或为这些设备分配不包含系统日志配置的访问控制策略），以避免在远程卷上复制事件。
- 收集以下信息：
  - Cisco Secure Network Analytics 管理器 的主机名或 IP 地址。
  - 流收集器的 IP 地址。

注释 您可能会在注册过程中从Cisco Secure Network Analytics管理器注销；请完成所有正在进行的工作，然后再开始使用部署向导。

过程

步骤 1 登录 CDO。

步骤 2 从 CDO 菜单中，导航至 **工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。

步骤 3 选择**防火墙管理中心 (Firewall Management Center)**，然后点击**配置 (Configuration)**。

步骤 4 导航至**集成 (Integration)** > **安全分析和日志记录 (Security Analytics & Logging)**。

步骤 5 在**仅 Cisco Secure Network Analytics 数据存储 (Secure Network Analytics Data Store)** 构件中，点击**开始 (Start)**。

步骤 6 输入流收集器的主机名或 IP 地址和端口号。

要添加更多流收集器，请点击 **+添加其他流收集器 (+Add another Flow Collector)**。

步骤 7 如果配置了多个流收集器，请将托管设备与不同的流收集器相关联：

注释 默认情况下，所有托管设备都会被分配给默认流收集器。

a) 点击**分配设备 (Assign Devices)**。
b) 选择要分配的托管设备。
c) 从重新分配设备下拉列表中选择流收集器。

如果您不希望托管设备将事件数据发送到任何流收集器，请选择该设备，然后从重新分配设备的下拉列表中选择**不记录到流收集器 (Do not log to flow collector)**。

您可以通过将鼠标悬停在预期的流收集器上并点击**设置默认值 (Set default)** 来更改默认流收集器。

d) 点击 **Apply Changes**（应用更改）。
e) 点击**下一步 (Next)**。

步骤 8 点击**下一步 (Next)**。

步骤 9 将更改部署到已注册的托管设备。

在将日志记录策略更改部署到已注册的威胁防御设备之前，事件数据不会被记录到SAL（本地）。

注释 如果必须更改其中任何配置，请再次运行向导。如果禁用配置或再次运行向导，则会保留除帐户凭证之外的所有设置。

您可以在管理中心的事件查看器和情景管理器中查看和使用这些远程存储的事件，并在生成报告时包括这些事件。您还可以从管理中心中的事件交叉启动，以便查看 Cisco Secure Network Analytics 管理器 上的相关数据。

有关详情，请参阅管理中心的在线帮助。

关于SAL (SaaS)

SAL (SaaS) 允许您从所有威胁防御设备捕获连接、入侵、文件、恶意软件和安全情报事件，并在CDO中的一个位置进行查看。事件存储在思科云中，可从CDO中的“事件日志记录”(Event Logging)页面查看，您可以在其中过滤和查看事件，以便清楚地了解在网络中触发的安全规则。

通过额外许可，在捕获这些事件后，您可以从CDO交叉启动为您调配的安全云分析门户。安全云分析是一种软件即服务 (SaaS) 解决方案，通过对事件和网络流数据执行行为分析来跟踪网络状态。通过从源（包括防火墙事件和网络流数据）收集有关网络流量的信息，它会创建有关流量的观察结果，并根据其流量模式自动识别网络实体的角色。使用此信息与其他威胁情报来源（例如 Talos）相结合，安全云分析会生成警报，警告可能存在恶意行为。除警报外，安全云分析还提供网络和主机可视性以及所收集的情景信息，为您研究警报和查找恶意行为的来源提供更好的基础。

SAL (SaaS) 的许可

SAL (SaaS) 许可证允许您使用 CDO 租户来查看防火墙日志和思科 Cisco Secure Cloud Analytics 分析实例，而无需为这些产品单独持有许可证。

有关可用 SAL (SaaS) 许可选项的详细信息，请参阅《思科安全分析和日志记录订购指南》。

配置 SAL (SaaS) 集成

要部署此集成，您必须使用系统日志或直接连接在 SAL (SaaS) 中设置事件数据存储。

- 使用系统日志将事件发送到 SAL (SaaS)，第 363 页
- 使用直接连接将事件发送到 SAL (SaaS)，第 365 页

SAL (SaaS)集成的要求

要求类型	要求
Cisco Secure Firewall Threat Defense	• CDO管理的独立威胁防御设备，版本7.2及更高版本。 • 使用系统日志发送事件：威胁防御版本 6.4 或更高版本 • 直接发送事件：威胁防御版本 7.2 • 必须部署防火墙系统并成功生成事件。

要求类型	要求
区域云	• 确定要向其发送事件的区域云。 • 无法在不同的区域云之间查看或移动事件。 • 如果您使用直接连接将事件发送到云以与 SecureX 或思科 SecureX 威胁响应集成，则必须使用相同的区域 CDO 云来进行此集成。 • 如果直接发送事件，则在 CDO 中指定的区域云必须与 CDO 租户的区域相匹配。
数据计划	• 您必须购买一个数据计划，以反映思科云每天从威胁防御设备接收的事件数量。这称为“每日注入速率”。 • 使用日志记录量估算器工具来估算您的数据存储要求。
帐户	当您购买此集成的许可证时，系统会为您提供一个 CDO 租户账户来支持集成。

使用系统日志将事件发送到 SAL (SaaS)

此程序记录从CDO管理的设备发送安全事件（连接、安全情报、入侵、文件和恶意软件事件）的系统日志消息的最佳实践配置。

开始之前

- 配置策略以生成安全事件，并验证您希望看到的事件显示在“分析”菜单下的适用表中。
- 收集系统日志服务器 IP 地址，端口和协议（UDP 或 TCP）

  从 CDO 浏览器窗口右上角的用户菜单中选择**安全连接器 (Secure Connectors)**，以查看所需的信息。
- 确保您的设备可以访问系统日志服务器。

过程

步骤 1 登录 CDO。

步骤 2 从 CDO 菜单中，导航至 **工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。

步骤 3 选择**防火墙管理中心 (Firewall Management Center)**，然后点击**配置 (Configuration)**。

步骤 4 为威胁防御设备配置系统日志设置：

a) 导航至**设备 (Devices)** > **平台设置 (Platform Settings)** 并编辑与您的威胁防御设备关联的平台设置策略。

b) 在左侧导航窗格中，点击**系统日志 (Syslog)** 并配置系统日志设置，如下所示：

点击	要执行以下操作
日志记录设置	启用日志记录，制定 FTP 服务器设置，以及闪存用法。
日志记录目标	启用对特定目标的日志记录，并指定对邮件严重性级别、事件类或自定义事件列表的过滤。
邮件设置	指定用作以邮件形式发送的系统日志消息的源地址的邮件地址。
事件列表	定义包括事件类、严重性级别和事件 ID 的自定义事件列表。
速率限制	指定发送到所有配置的目标的邮件数量，并定义要为其分配速率限制的邮件严重性级别。
系统日志设置	指定日志记录设施，启用时间戳包含，并启用其他设置以将服务器设置为一个系统日志目标。
系统日志服务器	为指定为日志记录目标的系统日志服务器指定 IP 地址、使用的协议、格式和安全区域。

c) 点击**保存 (Save)**。

步骤 5 配置访问控制策略的常规日志记录设置（包括文件和恶意软件日志记录）：

a) 导航至 **策略 (Policies)** > **访问控制 (Access Control)** 以编辑与威胁防御设备关联的访问控制策略。

b) 点击**日志记录 (Logging)** 选项卡并配置访问控制策略的常规日志记录设置（包括文件和恶意软件日志记录），如下所示：

点击	要执行以下操作
使用特定系统日志警报发送	从现有的预定义警报列表中选择一个系统日志警报，或者通过指定名称、日志主机、端口、设施和严重程度来添加一个警报。
使用在设备上部署的 FTD 平台设置策略中配置的系统日志设置	通过在“平台设置”中配置系统日志配置并重新使用访问控制策略中的设置来统一系统日志配置。所选的严重性适用于所有连接和入侵事件。默认严重性为警报。
发送 IPS 事件的系统日志消息	将事件作为系统日志消息发送。除非覆盖，否则将使用上面设置的默认值。
发送文件和恶意软件事件的系统日志消息	将文件和恶意软件事件作为系统日志消息发送。除非覆盖，否则将使用上面设置的默认值。

c) 点击**保存**。

步骤 6 为访问控制策略启用安全情报事件日志记录：

a) 在同一访问控制策略中，点击 **安全情报** 选项卡。

b) 在以下每个位置，点击**日志记录 (Logging)** 图标并启用连接的开始和结束和系统日志服务器：

- 在**DNS 策略 (DNS Policy)** 旁边。
- 在**阻止列表 (Block List)** 框中，对于**网络 (Networks)** 和 **URLs**。

c) 点击**保存**。

步骤 7 为访问控制策略中的每个规则启用系统日志记录：

a) 在同一访问控制策略中，点击 **规则** 选项卡。

b) 点击要编辑的规则。

c) 点击规则中的**日志记录 (Logging)** 选项卡。

d) 在连接开始和结束时启用。

e) 如果要记录文件事件，请选择 **日志文件**。

f) 启用 **系统日志服务器**。

g) 验证规则是“**在访问控制日志记录中使用默认系统日志配置**”。

h) 点击**保存 (Save)**。

i) 对策略中的每个规则重复上述步骤。

下一步做什么

如果完成更改，请将更改部署到托管设备。

使用直接连接将事件发送到 SAL (SaaS)

配置 云交付的防火墙管理中心 以便直接向 SAL (SaaS) 发送事件。

开始之前

- 将设备载入云交付的防火墙管理中心，将许可证分配给这些设备，然后将这些设备配置为直接将事件发送到 SAL (SaaS)。
- 通过编辑规则并选择**在连接开始时记录 (Log at Beginning of Connection)** 和**在连接结束时记录 (Log at End of Connection)** 选项来启用基于每个规则的连接日志记录。

过程

步骤 1 登录 CDO。

步骤 2 从 CDO 菜单中，导航至 **工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。

步骤 3 选择 **Firewall 管理中心 (Firewall Management Center)**，然后在右侧的“设置”(Settings) 窗格中，选择**思科云事件 (Cisco Cloud Events)**。

步骤 4 在**配置思科云事件 (Configure Cisco Cloud Events)** 构件中，执行以下操作：

1. 点击**将事件发送到云 (Send Events to the Cisco Cloud)** 滑块以启用整个配置。
2. 选中**将入侵事件发送到云 (Send Intrusion Events to the cloud)** 复选框以将入侵事件发送到云。
3. 选中**将文件和恶意软件事件发送到云 (Send File and Malware Events to the cloud)** 复选框，将文件和恶意软件事件发送到云。
4. 选择一个选项以便将连接事件发送到云：
   - 点击**无 (None)** 单选按钮可不将连接事件发送到云。
   - 点击**安全事件 (Security Events)** 单选按钮，仅将安全情报事件发送到云。
   - 点击**全部 (All)** 单选按钮，将所有连接事件发送到云。
5. 点击**保存 (Save)**。

查看和处理 CDO 中的事件

过程

步骤 1 登录 CDO。

步骤 2 从 CDO 菜单中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

步骤 3 使用**历史 (Historical)** 选项卡查看所有历史事件数据。默认情况下，查看器会显示此选项卡。

步骤 4 要查看实时事件，请点击**实时 (Live)** 选项卡。

有关可以在此页面上执行的操作的详细信息，请参阅 CDO 在线帮助。

查看和处理思科安全云分析中的事件

开始之前

为确保事件无缝传输，在使用事件查看器之前，请在 Stealthwatch 云门户中执行以下操作：

- 验证 Cisco Secure Cloud Analytics 是否与正确的 CDO 租户集成。

  要查看 CDO 租户，请点击**设置 (Settings)** > **传感器 (Sensors)**。
- 将要监控的子网添加到 Cisco Secure Cloud Analytics。

要添加子网，请点击**设置 (Settings)** > **子网 (Subnets)**。

过程

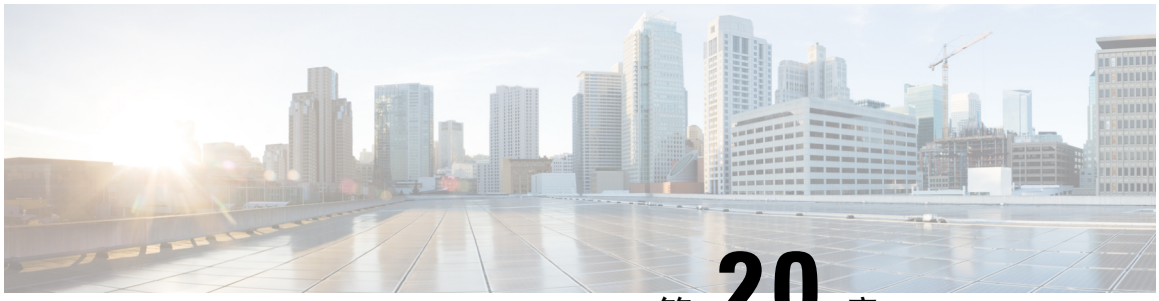
步骤 1 登录 CDO。

步骤 2 从 CDO 菜单中，选择 **分析 (Analytics)** > **安全云分析 (Secure Cloud Analytics)**。

Cisco Secure Cloud Analytics 门户将在新的浏览器选项卡中打开。

步骤 3 点击**调查 (Investigate)** > **事件查看器 (Event Viewer)**。

有关详细信息，请参阅 Cisco Secure Cloud Analytics 联机帮助。



第 20 章

FTD 控制面板

关于 FTD 控制面板

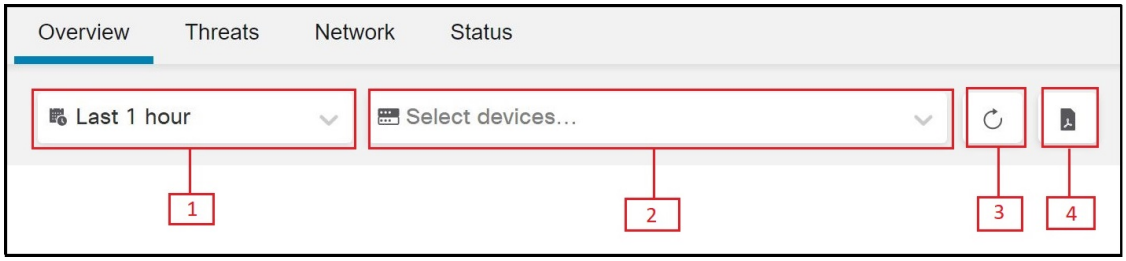
FTD 控制面板为您提供状态概览视图，包括所有 CDO 管理的威胁防御设备收集和生成的事件数据。

您可以使用此控制面板来查看与部署中的设备状态和整体运行状况相关的综合信息。FTD 控制面板提供的信息取决于您如何在系统中许可、配置和部署设备。虽然 FTD 控制面板会显示所有 CDO 管理的威胁防御设备的数据，但您也可以选择过滤基于设备的数据。您还可以选择时间范围以便显示特定时间范围内的数据。

此控制面板使用选项卡显示预定义构件：提供对系统的不同方面的见解的小型独立组件。例如，“网络活动”(Network Activity) 构件显示了事件图，其中可显示有关所有连接、恶意软件和入侵事件的信息。控制面板中的构件均已预定义且无法自定义。有权访问 CDO 租户的所有 CDO 用户均会看到此控制面板。

- 控制面板不会显示历史事件的任何事件统计信息。
- 由于汇聚服务批处理每五分钟进行一次汇聚，因此从事件汇聚到统计信息显示之间可能会存在五分钟的延迟。

图 *40: FTD* 控制面板



编号	说明
1	允许您更改时间范围以反映短至前一小时，或长至前一年的时间周期信息。当您更改时间范围时，构件会自动更新事件数据以反映新的时间范围。
2	允许您根据所选的设备来过滤事件数据。如果未选择任何设备，构件将显示所有可用的事件数据。
3	重新启动事件数据查询
4	以 PDF 输出格式显示事件数据。您可以选择在本地计算机上下载或保存此 PDF 的副本。

查看 FTD 控制面板

从 CDO 菜单中，选择 **分析 (Analytics)** > **FTD 控制面板 (FTD Dashboard)** 以查看 **FTD 控制面板 (FTD Dashboard)**。

默认情况下，租户的主页将显示**概述 (Overview)** 选项卡。

控制面板包括每个选项卡下列出的构件：“威胁”(Threat)、“网络”(Network)、“应用和用户”(Application and Users) 以及“状态”(Status) 选项卡。

下表列出了每个选项卡下的可用构件：

选项卡名称	可用构件
概述	所有可用构件
威胁	• 排名靠前的入侵规则 • 排名靠前的入侵攻击者 • 排名靠前的入侵目标 • 排名靠前的恶意软件签名 • 排名靠前的恶意软件发件人 • 排名靠前的恶意软件接收者 • 按处理结果排列的恶意软件事件

选项卡名称	可用构件
网络	• 网络活动 • 事件活动 • 访问控制操作 • 排名靠前的访问控制策略 • 排名靠前的访问控制规则 • 排名靠前的设备 • 排名靠前的用户
状态	• 运行不正常的设备 • 排名靠前的已加载设备

FTD 控制面板构件

FTD 控制面板会显示预定义的构件，它们可为您提供当前系统状态的概览视图。这些视图包括：

- 威胁防御 设备托管的 FMC 收集和生成的事件相关数据。
- 有关部署中的设备的状态和整体运行状况的信息。

排名靠前的入侵规则构件

排名靠前的入侵规则构件 (Top Intrusion Rules) 构件会显示在指定时间范围内发生的入侵事件计数，并按优先级进行组织。这些计数包括有丢弃数据包和不同影响的入侵事件的统计数据。生成的列表可滚动。

排名靠前的入侵攻击者构件

排名靠前的入侵攻击者 (Top Intrusion Attackers) 构件以条形图形式显示受监控网络中排名靠前的攻击性主机 IP 地址（导致这些事件的地址）的入侵事件的计数。

排名靠前的入侵目标构件

排名靠前的入侵目标 (Top Intrusion Targets) 构件以条形图形式显示受监控网络中排名靠前的目标主机 IP 地址（导致这些事件的连接中的目标）的入侵事件计数。

排名靠前的恶意软件签名构件

排名靠前的恶意软件签名 (Top Malware Signatures) 构件显示在网络流量中检测到的排名靠前的文件发送主机 IP 地址发出的恶意软件签名计数。

排名靠前的恶意软件发件人构件

排名靠前的恶意软件发件人 (Top Malware Senders) 构件显示在网络流量中检测到的排名靠前的文件发送主机 IP 地址发出的恶意软件威胁计数。

排名靠前的恶意软件接收者构件

排名靠前的恶意软件接收者 (Top Malware Receivers) 构件显示在网络流量中检测到的所有排名靠前的文件接收主机 IP 地址发出的恶意软件威胁计数。

按处理结果排列的恶意软件事件构件

按处理结果排列的恶意软件事件 (Malware Events by Disposition) 构件显示托管设备检测到包含恶意软件的文件时生成的所有恶意软件事件处置情况的计数。

网络活动构件

网络活动 (Network Activity) 构件显示基于连接事件信息的所有入口和出口数据速率。

事件活动构件

事件活动 (Event Activity) 构件显示最近一小时内发生的事件计数以及数据库中可用的每种事件类型的总数。

访问控制操作构件

访问控制操作 (Access Control Actions) 构件可显示基于每个事件允许或阻止的访问控制操作记录的事件计数。如果将光标悬停在饼形图上，则可以查看允许和阻止的操作百分比。

排名靠前的访问控制策略构件

排名靠前的访问控制策略 (Top Access Control Policies) 构件会显示生成事件的排名靠前的访问控制策略的计数。

排名靠前的访问控制规则构件

排名靠前的访问控制规则 (Top Access Control Rules) 构件显示用于每个事件的访问控制规则的前五个计数。这些计数可以按字节数或事件数排序。

排名靠前的设备构件

排名靠前的设备 (Top Devices) 构件显示每台设备的事件计数。这些计数可以按字节数或事件数排序。

排名靠前的用户构件

排名靠前的用户 (Top Users) 构件会显示与最高入侵事件计数关联的受监控网络上的用户。它主要从入侵检测 (IDS) 的“用户统计数据”(User Statistics) 和“入侵事件”(Intrusion Events) 表提取数据。它显示授权的用户数据。

运行状况不佳的设备构件

运行不正常的设备 (Unhealthy Devices) 构件显示 CDO 管理的威胁防御设备的当前编译运行状况。

排名靠前的已加载设备构件

排名靠前的已加载设备构件 (Top Loaded Devices) 构件显示威胁防御设备列表以及 CPU 使用情况信息。

修改 FTD 控制面板的时间设置

您可以更改时间范围以反映短至前一小时（默认），或长至前一年的时间周期信息。当您更改时间范围时，可按时间限制构件自动更新以反映新的时间范围。

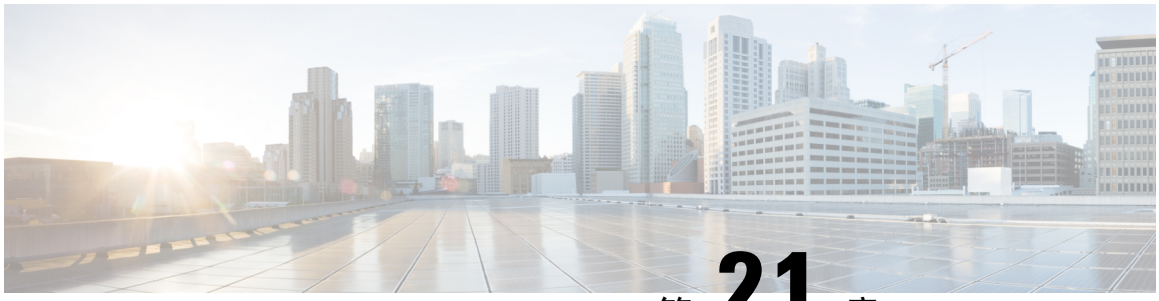
任何图形中的最大数据点数为 300，时间设置确定在每个数据点内汇总的时间。以下是每个时间范围的 FTD 控制面板中的数据点数量和覆盖的时间范围：

- 1 小时 = 12 个数据点，每个数据点 5 分钟
- 6 小时 = 72 个数据点，每个数据点 5 分钟
- 1 天 = 288 个数据点，每个数据点 5 分钟
- 1 周 = 300 个数据点，每个数据点 33.6 分钟
- 2 周 = 300 个数据点，每个数据点 67.2 分钟
- 30 天 = 300 个数据点，每个数据点 144 分钟
- 90 天 = 300 个数据点，每个数据点 432 分钟

- 180 天 = 300 个数据点，每个数据点 864 分钟
- 1 年 = 300 个数据点，每个数据点 1752 分钟

第 VIII 部分

设备运营



第 21 章

透明或路由防火墙模式

本章介绍如何将防火墙模式设置为路由或透明模式，以及防火墙在各种防火墙模式下的工作方式。

注释 防火墙模式只影响常规的防火墙接口，而不影响仅 IPS 接口，如内联集或被动接口。仅 IPS 接口可以在两种防火墙模式下使用。有关仅 IPS 接口的详细信息，请参阅内联集和被动接口，第 575 页。内嵌集可能是您所熟悉的“透明内联集”，但内联接口类型与本章介绍的透明防火墙模式或防火墙类型接口无关。

关于防火墙模式

威胁防御面向普通防火墙接口支持两种防火墙模式：路由防火墙模式和透明防火墙模式。

关于路由防火墙模式

在路由模式中，威胁防御设备被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。

通过集成路由和桥接，您可以使用您用来对网络的多个接口进行分组的“网桥组”，威胁防御设备使用桥接技术在接口之间传递流量。每个桥接组包括一个网桥虚拟接口 (BVI)，供您为其分配一个网络 IP 地址。威胁防御设备在 BVI 与正规的路由接口之间进行路由。如果您不需要集群或 EtherChannel 成员接口，则可以考虑使用路由模式而非透明模式。在路由模式下，可以像在透明模式下一样具有一个或多个隔离的网桥组，但也可以使用正常的路由接口进行混合部署。

关于透明防火墙模式

通常情况下，防火墙是一个路由跃点，并充当与其中一个被屏蔽子网连接的主机的默认网关。另一方面，透明防火墙是一个第 2 层防火墙，充当“线缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。但是，与其他防火墙一样，接口之间的访问控制是受控制的，需要进行通常的所有防火墙检查。

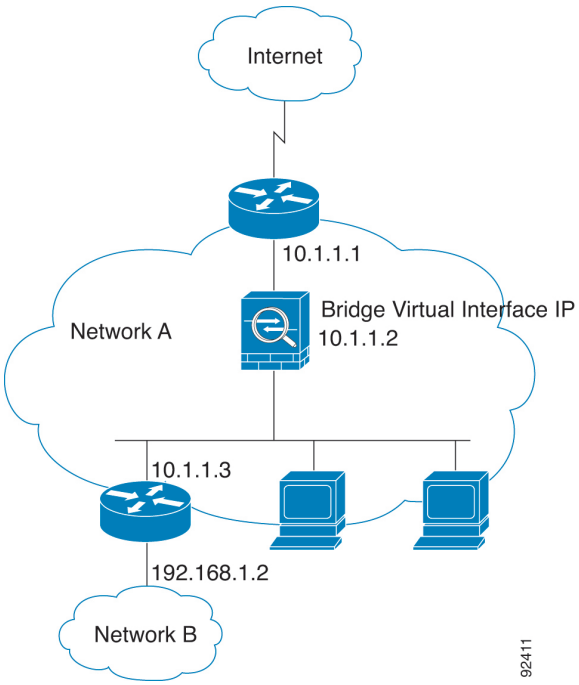
第 2 层连接使用您用来对网络的内部和外部接口进行分组的“网桥组”来实现，威胁防御设备使用桥接技术在接口之间传递流量。每个桥接组包括一个网桥虚拟接口 (BVI)，供您为其分配一个网络 IP 地址。多个网络可以有多个网桥组。在透明模式下，这些网桥组无法相互通信。

在网络中使用透明防火墙

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

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

图 *41:* 透明防火墙网络



允许路由模式功能通过流量

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

关于网桥组

网桥组是指 威胁防御设备 网桥（而非路由）的接口组。 网桥组在透明和路由防火墙模式下受支持。与任何其他防火墙接口一样，接口之间的访问控制将受控制，并将部署所有普通防火墙检查。

网桥虚拟接口 (BVI)

每个网桥组包括一个网桥虚拟接口 (BVI)。威胁防御设备使用该 BVI IP 地址作为源自网桥组的数据包的源地址。BVI IP 地址必须与网桥组成员接口位于同一子网。BVI 不支持辅助网络上的流量；只有与 BVI IP 地址相同的网络上的流量才受支持。

在透明模式下：只有网桥组成员接口会被命名并可以与基于接口的功能配合使用。

在路由模式下：BVI 充当网桥组和其他路由接口之间的网关。要在网桥组/路由接口之间进行路由，必须为 BVI 命名。对于一些基于接口的功能，您可以单独使用 BVI：

- DHCPv4 服务器 - 只有 BVI 支持 DHCPv4 服务器配置。
- 静态路由 - 可以为 BVI 配置静态路由；不能为成员接口配置静态路由。
- 系统日志服务器和其他源自 威胁防御设备的流量 - 当指定系统日志服务器（或 SNMP 服务器，或流量源自 威胁防御设备的其他服务）时，可以指定 BVI 或成员接口。

如果您在路由模式下没有命名 BVI，则 威胁防御设备不会路由网桥组流量。此配置将为网桥组复制透明防火墙模式。如果您不需要集群或 EtherChannel 成员接口，则可以考虑改用路由模式。在路由模式下，可以像在透明模式下一样具有一个或多个隔离的网桥组，但也可以使用正常的路由接口进行混合部署。

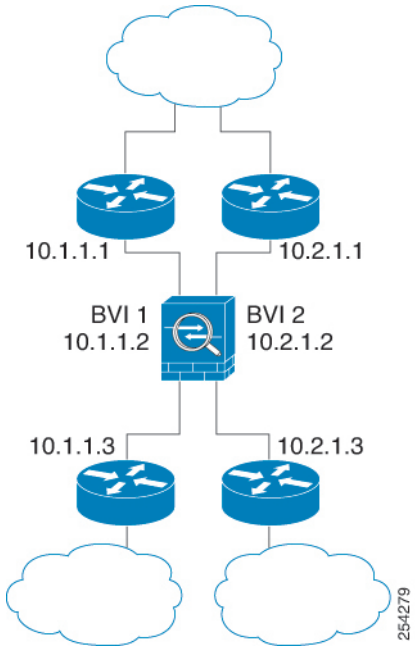
透明防火墙模式下的网桥组

网桥组的流量相互分离；流量不会路由至 威胁防御设备 中的另一个网桥组，并且流量必须退出 威胁防御设备 后才能通过外部路由器路由回 威胁防御设备 中的另一个网桥组。虽然每个网桥组的桥接功能是独立的，但所有网桥组之间可共享很多其他功能。例如，所有网桥组都共享系统日志服务器或 AAA 服务器的配置。

可以在每个网桥组中包含多个接口。有关支持的网桥组和接口的确切数量，请参阅防火墙模式指南，第 385 页。如果您在每个网桥组中使用的接口数超过 2 个，则可以控制同一网络上多个网段之间的通信，而不只是在内部和外部之间的通信。例如，如果您有三个不需要彼此通信的内部网段，则可以将每个网段设置在单独的接口上，并且仅允许它们与外部接口通信。或者，您可以自定义接口之间的访问规则，以根据需要允许任意程度的访问。

下图显示连接到 威胁防御设备且具有两个网桥组的两个网络。

图 *42:* 具有两个网桥组的透明防火墙网络

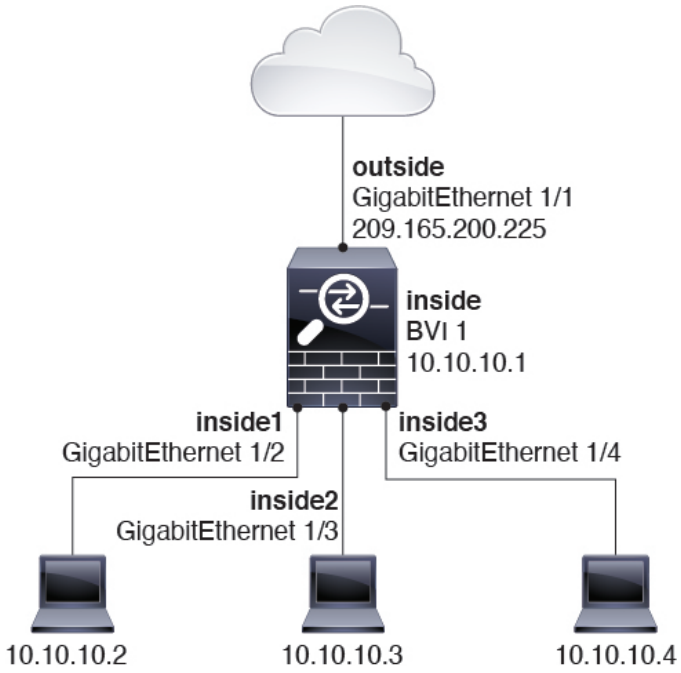


路由防火墙模式下的网桥组

网桥组流量可以路由到其他网桥组或路由接口。您可以选择通过不为网桥组的 BVI 接口分配名称来隔离网桥组流量。如果命名了 BVI，则 BVI 将像其他任何普通接口一样参与路由。

路由模式下网桥组的一种用途是在 威胁防御上而非外部交换机上使用额外接口。例如，某些设备的默认配置包括一个外部接口作为普通接口，还包括分配给内部网桥组的其他接口。由于此网桥组的目的是替换外部交换机，因此您需要配置访问策略，以便所有网桥组接口都可以自由通信。

图 *43:* 具有内部网桥组和外部路由接口的路由防火墙网络



允许第 3 层流量

- 单播 IPv4 和 IPv6 流量需要允许一个访问规则通过网桥组。
- 允许 ARP 双向通过网桥组，而无需访问规则。ARP 流量可通过 ARP 检测进行控制。
- IPv6 邻居发现和路由器请求数据包可以使用访问规则传递。
- 可使用访问规则允许广播和组播流量通过。

允许的 MAC 地址

如果得到您的访问策略的允许，将允许以下目标 MAC 地址通过网桥组（请参阅允许第 3 层流量，第 381 页）。系统会丢弃此列表中未列出的任何 MAC 地址。

- 实际广播目标 MAC 地址等于 FFFF.FFFF.FFFF
- IPv4 组播 MAC 地址的范围是 0100.5E00.0000 至 0100.5EFE.FFFF
- IPv6 组播 MAC 地址的范围是 3333.0000.0000 至 3333.FFFF.FFFF
- BPDU 组播地址等于 0100.0CCC.CCCD

BPDU 处理

为防止环路使用生成树协议，默认情况下允许 BPDU 通过。

默认情况下，BPDU 也会被转发以进行高级检测，这对此类型数据包并无必要，并且有可能导致例如由于检测重启而被阻止的问题发生。我们建议您始终免除对 BPDU 进行高级检测。为此，请使用 FlexConfig 配置信任 BPDU 的 EtherType ACL，并在每个成员接口上免除对其进行高级检测。请参阅 #unique_456。

FlexConfig 对象应部署以下命令，在其中将 <if-name> 替换为接口名称。添加所需数量的 access-group 命令以涵盖设备上的每个网桥组成员接口。您还可以为 ACL 选择其他名称。

```
access-list permit-bpdu ethertype trust bpdu
access-group permit-bpdu in interface <if-name>
```

MAC 地址与路由查找

对于网桥组中的流量，通过执行目标 MAC 地址查找而不是路由查找来确定数据包的传出接口。

但是，路由查找对于以下情况是必要的：

- 源自 威胁防御设备的流量 - 例如，在 威胁防御设备上为发往系统日志服务器所在的远程网络的流量添加一个默认/静态路由。
- IP 语音 (VoIP) 和 TFTP 流量，并且终端至少在一跳之外 - 在 威胁防御设备上为发往成功建立辅助连接的远程终端的流量添加静态路由。威胁防御设备会在访问控制策略中创建一个临时“针孔”以允许辅助连接；由于连接可能会使用一组不同于主连接的 IP 地址，所以 威胁防御设备需要执行路由查找以便在正确的接口上安装针孔。

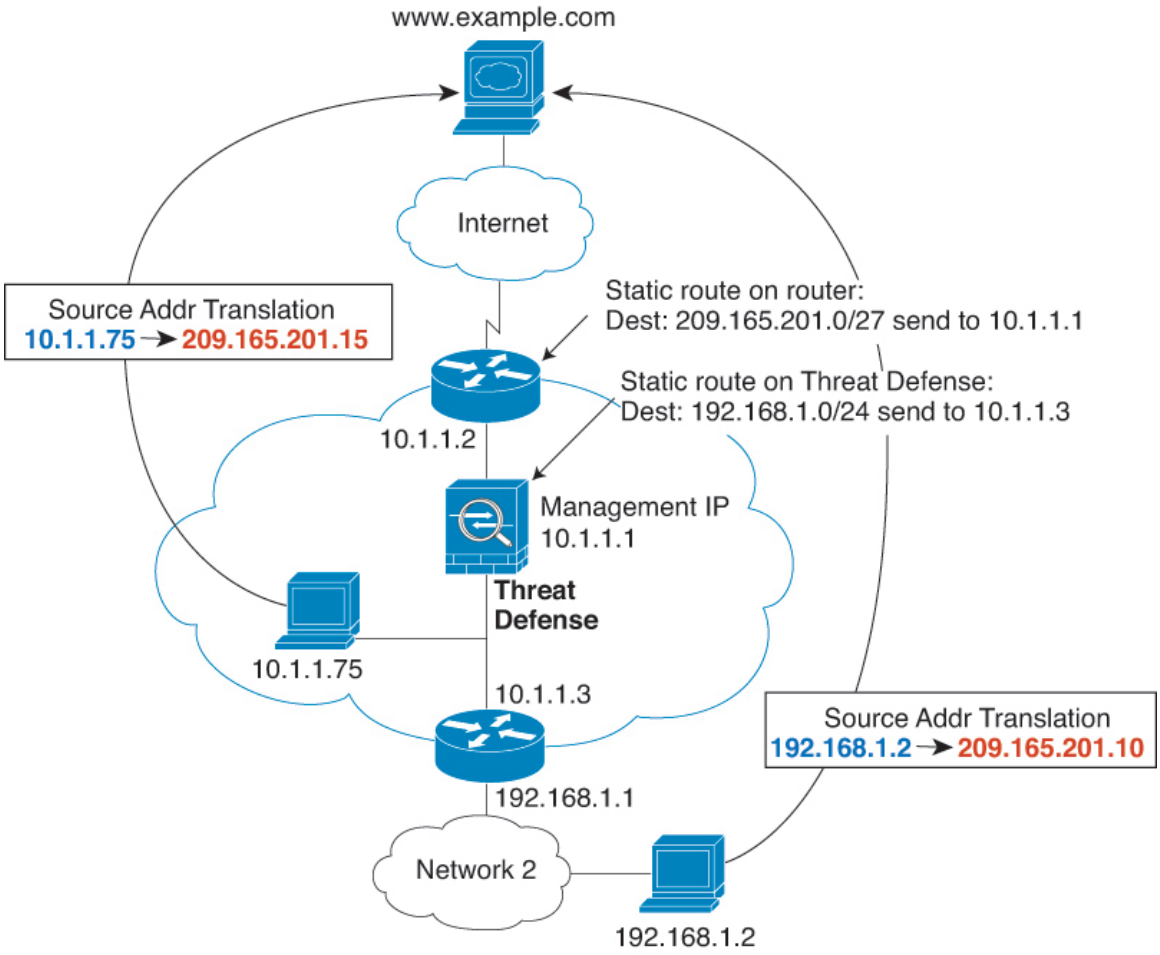
  受影响的应用包括：

  - H.323
  - RTSP
  - SIP
  - Skinny (SCCP)
  - SQL*Net
  - SunRPC
  - TFTP

- 威胁防御设备对其执行 NAT 的至少一跳开外的流量 - 在 威胁防御设备上为发往远程网络的流量配置静态路由。您还需要在上游路由器上为要发送到 威胁防御设备的已映射地址的流量配置静态路由。

  此路由要求也适用 NAT 的 VoIP 和 DNS 的嵌入式 IP 地址，这些嵌入式 IP 地址都必须至少在一跳之外。威胁防御设备需要识别正确的出口接口，以便可以执行转换。

图 *44: NAT* 示例：网桥组中的 *NAT*



透明模式下网桥组不支持的功能

下表列出了在透明模式下网桥组中不受支持的功能。

表 *44:* 在透明模式下不支持的功能

特性	说明
动态 DNS	-
DHCP 中继	透明防火墙可作为 DHCPv4 服务器，但它不支持 DHCP 中继。不需要使用 DHCP 中继，因为可使用两个访问规则来允许 DHCP 流量通过：一个规则用于允许从内部接口向外部发送 DCHP 请求；另一个用于允许来自另一个方向的服务器的应答。

特性	说明
动态路由协议	但是，对于网桥组成员接口，可以为 威胁防御设备上发起的流量添加静态路由。您还可以使用访问规则来允许动态路由协议通过 威胁防御设备。
组播 IP 路由	通过在访问规则中允许组播流量，可以允许组播流量通过 威胁防御设备。
QoS	-
针对直通流量终止 VPN	透明防火墙仅支持在网桥组成员接口上使用站点间的VPN隧道传输管理连接。它不会针对通过 威胁防御设备 的流量终止 VPN 连接。您可以使用访问规则允许 VPN 流量通过 ASA，但它不会终止非管理连接。

路由模式下网桥组不支持的功能

下表列出了在路由模式下网桥组中不支持的功能。

表 *45:* 路由模式下不受支持的功能

特性	说明
EtherChannel 成员接口	仅支持物理接口、冗余接口和子接口作为网桥组成员接口。 诊断 接口也不受支持。
集群	集群中不支持网桥组。
动态 DNS	-
DHCP 中继	路由防火墙可以作为 DHCPv4 服务器，但它不支持在 BVI 或网桥组成员接口上使用 DHCP 中继。
动态路由协议	但您可以为 BVI 添加静态路由。您还可以使用访问规则来允许动态路由协议通过 威胁防御设备。非网桥组接口支持动态路由。
组播 IP 路由	通过在访问规则中允许组播流量，可以允许组播流量通过 威胁防御设备。非网桥组接口支持组播路由。
QoS	非网桥组接口支持 QoS。
针对直通流量终止 VPN	您无法终止 BVI 上的 VPN 连接。非网桥组接口支持 VPN。 网桥组成员接口仅支持将站点间VPN隧道用于管理连接。它不会针对通过 威胁防御设备 的流量终止 VPN 连接。您可以使用访问规则通过网桥组传递 VPN 流量，但它不会终止非管理连接。

默认设置

网桥组默认设置

默认情况下，所有 ARP 数据包都在网桥组内通过。

防火墙模式指南

桥接组指南（透明和路由模式）

- 您可以创建最多 250 个桥接组，每个桥接组 64 个接口。
- 各个直连网络必须在同一子网上。
- 威胁防御设备不支持辅助网络上的流量；只有与 BVI IP 地址相同的网络上的流量才受支持。
- 每个桥接组都需要 BVI 的 IP 地址，以用于管理往返设备的流量和使流量通过 威胁防御设备。对于 IPv4 流量，请指定 IPv4 地址。对于 IPv6 流量，请指定 IPv6 地址。
- 您仅可手动配置 Ipv6 地址。
- BVI IP 地址必须与已连接网络位于同一子网上。您不能将该子网设置为主机子网 (255.255.255.255)。
- 不支持将管理接口作为桥接组成员。
- 对于多实例模式，共享接口不支持用于网桥组成员接口（在透明模式或路由模式下）。
- 对于具有桥接 ixgbevf 接口的 VMware 上的 threat defense virtual ，透明模式不受支持，在路由模式中网桥组不受支持。
- 对于 Firepower 2100 系列，在路由模式下不支持网桥组。
- 对于 Firepower 1010，不能将逻辑 VLAN 接口和物理防火墙接口混合在同一个桥接组中。
- 对于 Firepower 4100/9300，不支持将数据共享接口作为网桥组成员。
- 在透明模式下，必须至少使用 1 个桥接组；数据接口必须属于桥接组。
- 在透明模式下，请勿将 BVI IP 地址指定为所连接设备的默认网关；设备需要将位于 威胁防御另一端的路由器指定为默认网关。
- 在透明模式下，默认路由（为管理流量提供返回路径所需的路由）仅适用于来自一个桥接组网络的管理流量。这是因为默认路由会指定网桥组中的接口以及网桥组网络上的路由器 IP 地址，而您只能定义一个默认路由。如果您具有来自多个桥接组网络的管理流量，则需要指定常规静态路由来确定预期会发出管理流量的网络。
- 在透明模式下，诊断接口不支持 PPPoE。

- Amazon Web 服务、Microsoft Azure、Google Cloud Platform 和 Oracle Cloud Infrastructure 上部署的威胁防御虚拟实例不支持透明模式。
- 在路由模式下，要在桥接组和其他路由接口之间路由，您必须指定 BVI。
- 在路由模式下，威胁防御 - 不支持将 EtherChannel 接口定义为网桥组成员。 Firepower 4100/9300 上的 Etherchannel 可以是网桥组成员。
- 使用网桥组成员时，不允许双向转发检测 (BFD) 回应数据包通过 威胁防御。如果 威胁防御 的一端有两个邻居运行 BFD，则 威胁防御 会因二者具有相同的源 IP 地址和目标 IP 地址且疑似属于 LAND 攻击而丢弃 BFD 回应数据包。

设置防火墙模式

智能许可证	经典许可证	支持的设备	支持的域	访问权限
任意	不适用	威胁防御	任意	管理员 访问管理员 网络管理员

在 CLI 中执行初始系统设置时，可以设置防火墙模式。我们建议在安装过程中设置防火墙模式，因为更改防火墙模式会清除您的配置，以确保不存在不兼容的设置。如果以后需要更改防火墙模式，则必须从 CLI 中执行此操作。

过程

步骤 1 从管理中心注销 威胁防御设备。

撤销设备之前，不能更改防火墙模式。

a) 选择**设备** > **设备管理**。
b) 从受管设备列表中选择设备。
c) 删除设备（点击垃圾桶），确认并等待系统删除设备。

步骤 2 访问 威胁防御设备 CLI，首选使用控制台端口。

如果您使用 SSH 连接到诊断接口，则更改模式会清除您的接口配置，并断开连接。此时，您应改为连接到管理接口。

步骤 3 更改防火墙模式：

configure firewall [**routed** | **transparent**]

示例：

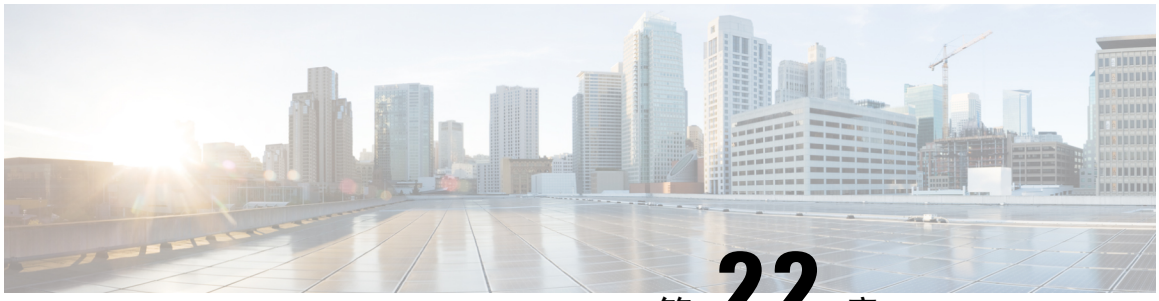
```
> configure firewall transparent
This will destroy the current interface configurations, are you sure that you want to
proceed? [y/N] y
The firewall mode was changed successfully.
```

步骤 4 向 管理中心重新注册：

configure manager add {*hostname* | *ip_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

其中：

- {*hostname* | *ip_address* | **DONTRESOLVE** }指定 管理中心 的完全限定主机名或 IP 地址。如果 管理中心不是直接可寻址的，请使用 **DONTRESOLVE**。
- *reg_key* 是向 管理中心 注册设备所需的唯一字母数字注册密钥。
- *nat_id* 是在 管理中心与设备之间的注册流程中使用的可选字母数字字符串。如果主机名设置为 **DONTRESOLVE**，此项为必填项。



第 22 章

Firepower 4100/9300上的逻辑设备

Firepower 4100/9300 是具有灵活性的安全平台，可在其中安装一个或多个逻辑设备。在可将 威胁防御 添加到 管理中心 之前，必须配置机箱接口，添加逻辑设备，并使用 Cisco Secure Firewall 机箱管理器或 FXOS CLI 将接口分配到 Firepower 4100/9300机箱上的设备。本章介绍基本的接口配置以及如何使用 Cisco Secure Firewall 机箱管理器添加独立或高可用性逻辑设备。要使用 FXOS CLI，请参阅 FXOS CLI 配置指南。有关更多高级 FXOS 程序和故障排除，请参阅 FXOS 配置指南。

关于接口

Firepower 4100/9300 机箱支持物理接口、容器实例的 VLAN 子接口和 EtherChannel（端口通道）接口。EtherChannel 接口最多可以包含同一类型的 16 个成员接口。

机箱管理接口

机箱管理接口用于通过 SSH 或 机箱管理器来管理 FXOS 机箱。此接口在**接口 (Interfaces)** 选项卡顶部显示为 **MGMT**，您只可在**接口 (Interfaces)** 选项卡上启用或禁用此接口。此接口独立于分配给应用管理用逻辑设备的 MGMT 型接口。

要配置此接口参数，必须从 CLI 进行配置。要在 FXOS CLI 中查看此接口，请连接到本地管理并显示管理端口：

Firepower # **connect local-mgmt**

Firepower(local-mgmt) # **show mgmt-port**

请注意，即使将物理电缆或小型封装热插拔模块拔下，或者执行了 **mgmt-port shut** 命令，机箱管理接口仍会保持正常运行状态。

注释 机箱管理接口不支持巨型帧。

接口类型

物理接口、容器实例的 VLAN 子接口， 和 EtherChannel（端口通道）接口可以是下列类型之一：

- 数据 - 用于常规数据。不能在逻辑设备之间共享数据接口，且逻辑设备无法通过背板与其他逻辑设备通信。对于数据接口上的流量，所有流量必须在一个接口上退出机箱，并在另一个接口上返回以到达另一个逻辑设备。
- 数据共享 - 用于常规数据。仅容器实例支持这些数据接口，可由一个或多个逻辑设备/容器实例（仅限威胁防御-使用-管理中心 ）共享。 每个容器实例都可通过背板与共享此接口的所有其他实例通信。共享的接口可能会影响您可以部署容器实例的数量。共享接口不支持用于网桥组成员接口（在透明模式或路由模式下）、内联集、被动接口、集群或故障切换链路。
- 管理 - 用于管理应用程序实例。这些接口可以由一个或多个逻辑设备共享，以访问外部主机；逻辑设备无法通过此接口与共享接口的其他逻辑设备通信。只能为每个逻辑设备分配一个管理接口。根据您的应用和管理器，您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。有关独立机箱管理接口的信息，请参阅机箱管理接口 ， 第 389 页。

注释 管理接口更改会导致逻辑设备重新启动，例如将管理接口从 e1/1 更改为 e1/2 会导致逻辑设备重新启动以应用新的管理接口。

- 事件 - 用作 威胁防御-using-管理中心 设备的辅助管理接口。 要使用此接口，您必须在 威胁防御 CLI 上配置其 IP 地址和其他参数。例如，您可以将管理流量从活动（例如网络活动）中分隔出来。有关详细信息，请参阅《管理中心配置指南》。事件接口可以由一个或多个逻辑设备共享，以访问外部主机；逻辑设备无法通过此接口与共享接口的其他逻辑设备通信。 如果稍后为管理配置数据接口，则无法使用单独的事件接口。

注释 安装每个应用实例时，会分配一个虚拟以太网接口。如果应用不使用事件接口，则虚拟接口将处于管理员关闭状态。

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- 集群 - 用作集群逻辑设备的集群控制链路。默认情况下，系统会在端口通道 48 上自动创建集群控制链路。“集群”类型仅在 EtherChannel 接口上受支持。 对于多实例集群，无法在设备之间共享集群类型接口。您可以将 VLAN 子接口添加到集群 EtherChannel，以便为每个集群提供单

独的集群控制链路。如果向某个集群接口添加子接口，则不能将该接口用于本地集群。设备管理器 和 CDO 不支持集群。

注释 本章仅讨论 *FXOS* VLAN 子接口。您还可以在 威胁防御 应用内单独创建子接口。有关详细信息，请参阅FXOS 接口与应用接口 ，第 392 页。

有关独立部署和集群部署中威胁防御和 ASA 应用的接口类型支持，请参阅下表。

表 *46:* 接口类型支持

应用		数据	数据：子接口	数据共享	数据共享：子接口	管理	Eventing	集群（仅 EtherChannel）	集群：子接口
威胁防御	独立本地实例	支持	—	-	—	支持	支持	—	-
	独立容器实例	支持	支持	支持	支持	支持	支持	—	-
	集群本地实例	支持（EtherChannel 仅用于机箱间集群）	-	-	—	支持	支持	支持	—
	集群容器实例	支持（EtherChannel 仅用于机箱间集群）	-	-	—	支持	支持	支持	支持
ASA	独立本地实例	支持	—	-	—	支持	—	支持	—
	集群本地实例	支持（EtherChannel 仅用于机箱间集群）	-	-	—	支持	—	支持	—

FXOS 接口与应用接口

Firepower 4100/9300 管理物理接口、容器实例的 VLAN 子接口和 EtherChannel（端口通道）接口的基本以太网设置。在应用中，您可以配置更高级别的设置。例如，您只能在 FXOS 中创建 EtherChannel；但是，您可以为应用中的 EtherChannel 分配 IP 地址。

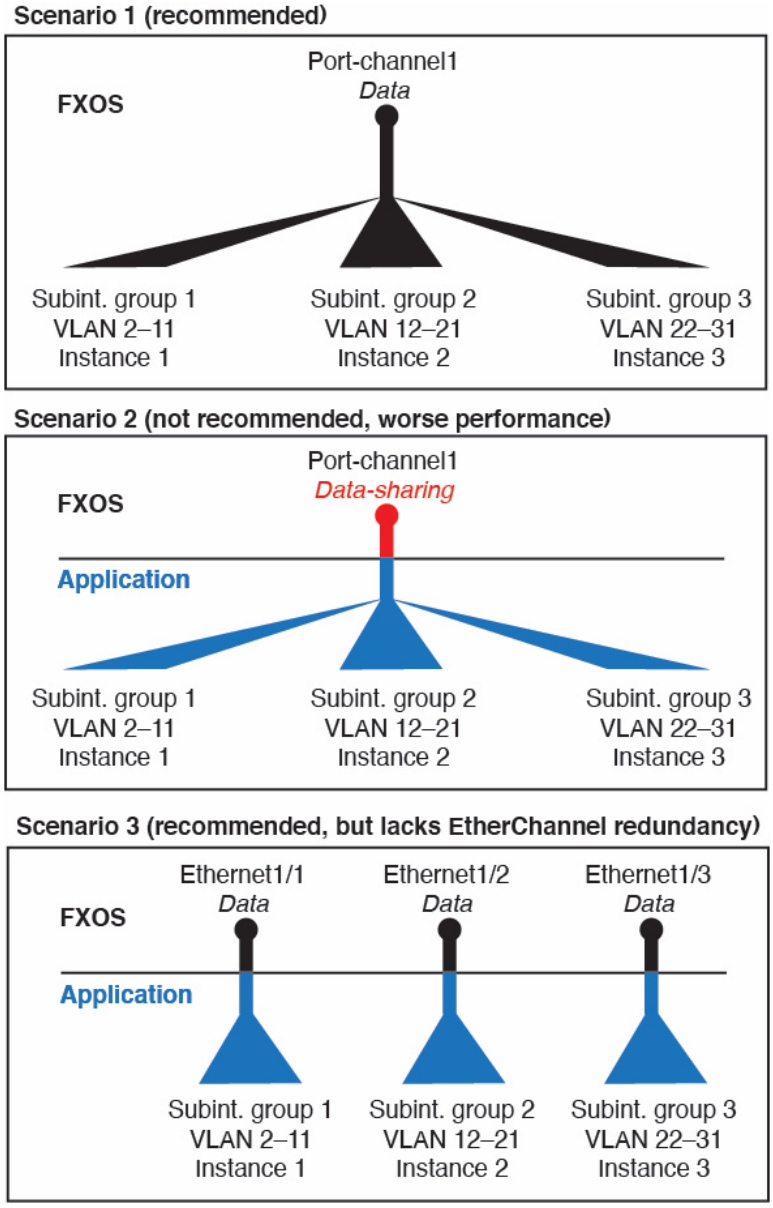
下文将介绍 FXOS 接口与应用接口之间的交互。

VLAN 子接口

对于所有逻辑设备，您可以在应用内创建 VLAN 子接口。

仅对于独立模式下的容器实例，您还可以在 FXOS 中创建 VLAN 子接口。 除集群类型接口外，多实例集群不支持 FXOS 中的子接口。应用定义的子接口不受 FXOS 限值的约束。选择在哪个操作系统创建子接口取决于网络部署和个人偏好。例如，要共享子接口，必须在 FXOS 中创建子接口。偏好 FXOS 子接口的另一种场景包含将单个接口上的单独子接口组分配至多个实例。例如，您想要结合使用端口通道 1 与实例 A 上的 VLAN 2-11、实例 B 上的 VLAN 12-21 和实例 C 上的 VLAN 22-31。如果您在应用内创建这些子接口，则必须在 FXOS 中共享父接口，但这可能并不合适。有关可以用于实现这种场景的三种方法，请参阅下图：

图 *45: FXOS* 中的 *VLAN* 与容器实例的应用



机箱和应用中的独立接口状态

您可以从管理上启用和禁用机箱和应用中的接口。必须在两个操作系统中都启用能够正常运行的接口。由于接口状态可独立控制，因此机箱与应用之间可能出现不匹配的情况。

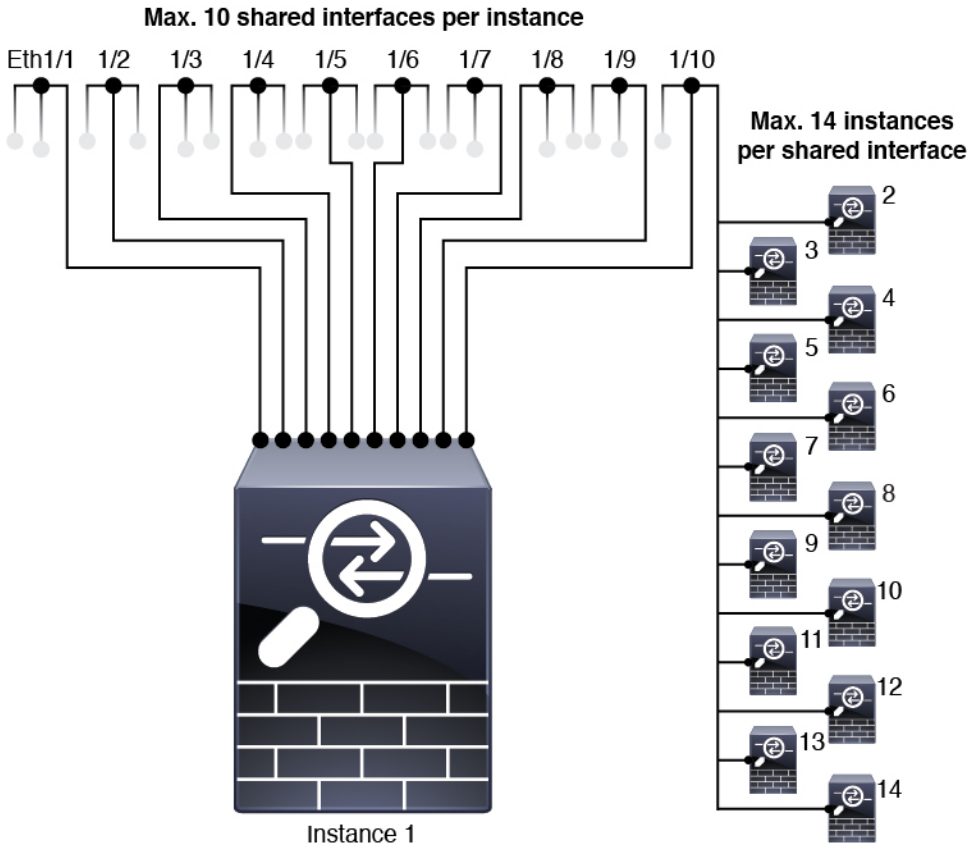
应用内接口的默认状态取决于接口类型。例如，在应用内，默认禁用物理接口或 EtherChannel，但默认启用子接口。

共享接口可扩展性

实例可以共享数据共享型接口。此功能允许您保存物理接口的使用情况，以及支持灵活的网络部署。当您共享接口时，机箱会使用唯一 MAC 地址将流量转发至适当实例。然而，由于需要在机箱内实现全网状拓扑，因此共享接口将导致转发表规模扩大（每个实例都必须能够与共享同一接口的所有其他实例进行通信）。因此，您可以共享的接口存在数量限制。

除转发表外，机箱还维护用于 VLAN 子接口转发的 VLAN 组表。 您最多可以创建 500 个 VLAN 子接口。

请参阅共享接口分配的以下限制：



共享接口最佳实践

为确保转发表的最佳可扩展性，请共享尽可能少的接口。相反，您可以在一个或多个物理接口上创建最多 500 个 VLAN 子接口，然后在容器实例之间划分 VLAN。

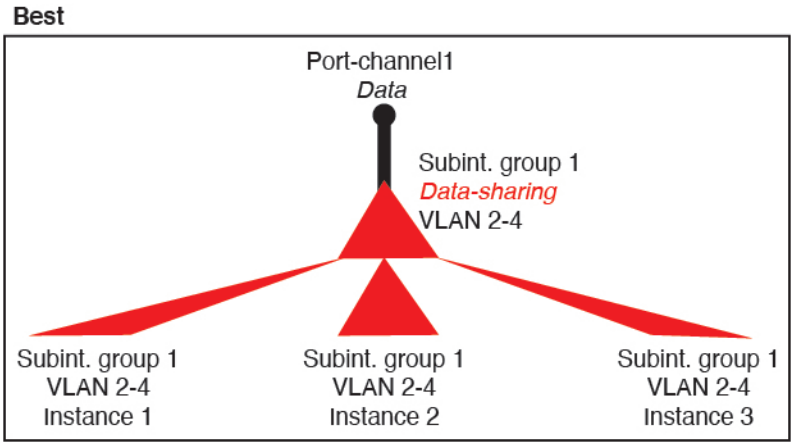
共享接口时，请按照可扩展性从高到低的顺序遵循这些最佳实践：

1. 最佳 - 共享单父项下的子接口，并结合使用相同集合的子接口和同组实例。

   例如，创建一个大型 EtherChannel 以将所有类似接口捆绑在一起，然后共享该 EtherChannel 的子接口：Port-Channel1.2, 3 和 4 而不是 Port-Channel2、Port-Channel3 和 Port-Channel4。与跨父项共

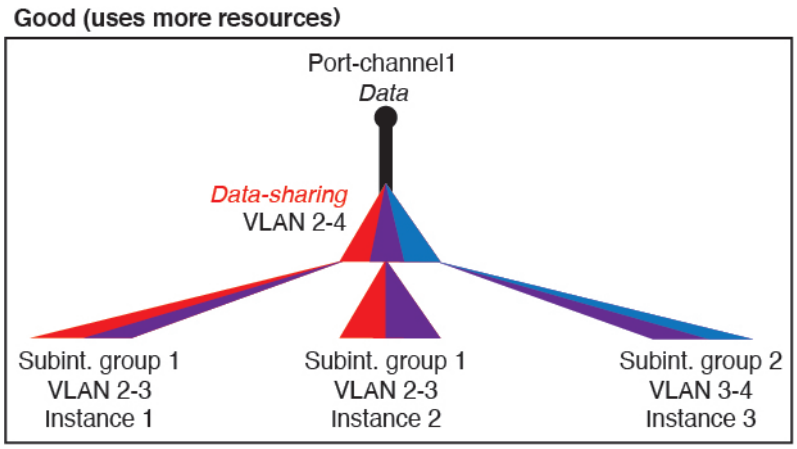
享物理/EtherChannel 接口或子接口相比，当您共享单父项子接口时，VLAN 组表提供更高的转发表可扩展性。

图 *46:* 最佳：一个父项上的共享子接口组



如果未与一组实例共享相同集合的子接口，则配置会提高资源使用率（更多 VLAN 组）。例如，与实例 1、2 和 3（一个 VLAN 组）共享 Port-Channel1.2, 3 和 4 而不是与实例 1 和 2 分享 Port-Channel1.2 和 3，同时与实例 3（两个 VLAN 组）共享 Port-Channel1.3 和 4。

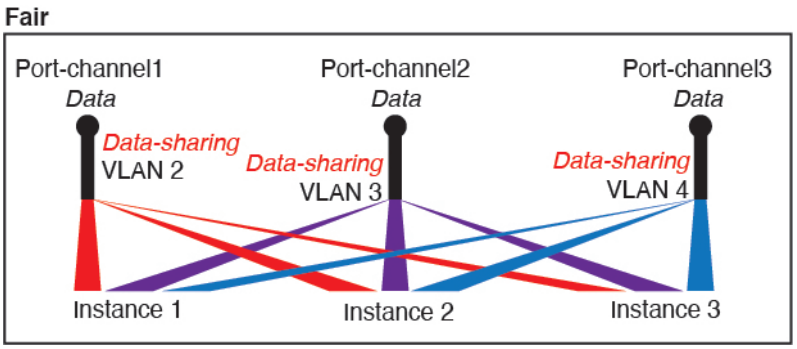
图 *47:* 良好：一个父项上共享多个子接口组



2. 一般 - 跨父项共享子接口。

   例如，共享 Port-Channel1.2、Port-Channel2.3 和 Port-Channel3.4 而不是 Port-Channel2、Port-Channel4 和 Port-Channel4。虽然这种使用方法的效率低于仅共享同一父项上的子接口，但仍可利用 VLAN 组。

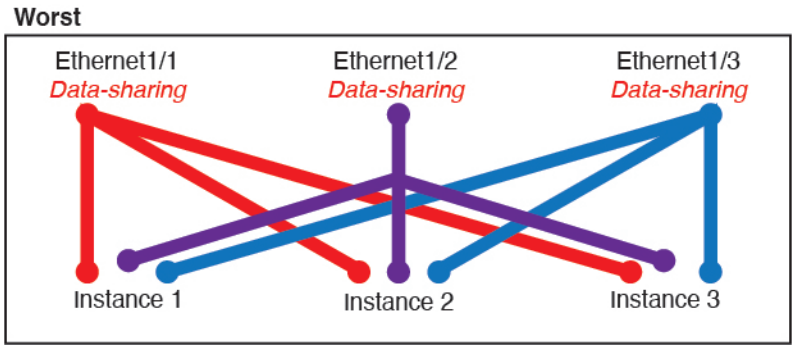
图 *48:* 一般：独立父项上的共享子接口



3. 最差 - 共享单个父接口（物理或 EtherChannel）。

   此方法使用的转发表条目最多。

图 *49:* 最差：共享父接口



共享接口使用示例

有关接口共享示例和可扩展性，请参阅下表。以下情景假设使用一个在所有实例中共享的物理/EtherChannel 接口来实现管理，和另一个设有专用子接口的物理或 EtherChannel 接口，用于实现高可用性。

- 表 47: Firepower 9300（设有三个 SM-44）上的物理/EtherChannel 接口和实例， 第 397 页
- 表 48: Firepower 9300（设有三个 SM-44）上的一个父接口的子接口和实例， 第 399 页
- 表 49: Firepower 9300（设有一个 SM-44）上的物理/EtherChannel 接口和实例， 第 402 页
- 表 50: Firepower 9300（设有一个 SM-44）上的一个父接口的子接口和实例， 第 404 页

Firepower 9300（设有三个 SM-44）

下表适用于仅使用物理接口或 Etherchannel 的 9300 上的三个 SM-44 安全模块。在未设子接口的情况下，接口的最大数量受限。此外，与共享多个子接口相比，共享多个物理接口所使用的转发表资源更多。

每个 SM-44 模块最多可支持 14 个实例。如有必要，系统会拆分模块之间的实例，以将实例数维持在限值范围内。

表 *47: Firepower 9300*（设有三个 *SM-44*）上的物理*/EtherChannel* 接口和实例

专用接口	共享接口	实例数	转发表使用百分比
32: • 8 • 8 • 8 • 8	**0**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	16%
30: • 15 • 15	**0**	**2:** • 实例 1 • 实例 2	14%
14: • 14（每个实例 1 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
33: • 11（每个实例 1 个专用子接口） • 11（每个实例 1 个专用子接口） • 11（每个实例 1 个专用子接口）	**3:** • 1 • 1 • 1	**33:** • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33	98%

专用接口	共享接口	实例数	转发表使用百分比
33: • *11*（每个实例 *1* 个专用接口） • *11*（每个实例 *1* 个专用接口） • *12*（每个实例 *1* 个专用接口）	***3:*** • *1* • *1* • *1*	***34:*** • 实例 *1* 至实例 *11* • 实例 *12* 至实例 *22* • 实例 *23* 至实例 *34*	*102%* 禁止使用
30: • 30（每个实例 1 个专用接口）	**1**	**6：** • 实例 1 实例 6	25%
30: • 10（每个实例 5 个专用接口） • 10（每个实例 5 个专用接口） • 10（每个实例 5 个专用接口）	**3:** • 1 • 1 • 1	**6：** • 实例 1 至实例 2 • 实例 2 至实例 4 • 实例 5 至实例 6	23%
30: • 30（每个实例 6 个专用接口）	**2**	**5：** • 实例 1 至实例 5	28%

专用接口	共享接口	实例数	转发表使用百分比
30: • 12（每个实例 6 个专用接口） • 18（每个实例 6 个专用接口）	**4:** • 2 • 2	**5:** • 实例 1 至实例 2 • 实例 2 至实例 5	26%
24: • 6 • 6 • 6 • 6	**7**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	44%
24: • 12（每个实例 6 个专用接口） • 12（每个实例 6 个专用接口）	**14:** • 7 • 7	**4:** • 实例 1 至实例 2 • 实例 2 至实例 4	41%

下表适用于使用单父项物理接口上子接口的 9300 的三个 SM-44 安全模块。例如，创建一个大型 EtherChannel 以将所有类似接口捆绑在一起，然后共享该 EtherChannel 的子接口。与共享多个子接口相比，共享多个物理接口所使用的转发表资源更多。

每个 SM-44 模块最多可支持 14 个实例。如有必要，系统会拆分模块之间的实例，以将实例数维持在限值范围内。

表 ***48: Firepower 9300***（设有三个 ***SM-44***）上的一个父接口的子接口和实例

专用子接口	共享子接口	实例数	转发表使用百分比
168: • 168（每个实例 4 个专用子接口）	**0**	**42:** • 实例 1 至实例 42	33%

专用子接口	共享子接口	实例数	转发表使用百分比
224: • 224（每个实例 16 个专用子接口）	**0**	**14:** • 实例 1 至实例 14	27%
14: • 14（每个实例 1 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
33: • 11（每个实例 1 个专用子接口） • 11（每个实例 1 个专用子接口） • 11（每个实例 1 个专用子接口）	**3:** • 1 • 1 • 1	**33:** • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33	98%
70: • 70（每个实例 5 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
165: • 55（每个实例 5 个专用子接口） • 55（每个实例 5 个专用子接口） • 55（每个实例 5 个专用子接口）	**3:** • 1 • 1 • 1	**33:** • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33	98%

专用子接口	共享子接口	实例数	转发表使用百分比
70: • 70（每个实例 5 个专用子接口）	**2**	**14:** • 实例 1 至实例 14	46%
165: • 55（每个实例 5 个专用子接口） • 55（每个实例 5 个专用子接口） • 55（每个实例 5 个专用子接口）	**6:** • 2 • 2 • 2	**33:** • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33	98%
70: • 70（每个实例 5 个专用子接口）	**10**	**14:** • 实例 1 至实例 14	46%
165: • *55*（每个实例 *5* 个专用子接口） • *55*（每个实例 *5* 个专用子接口） • *55*（每个实例 *5* 个专用子接口）	***30:*** • *10* • *10* • *10*	***33:*** • 实例 *1* 至实例 *11* • 实例 *12* 至实例 *22* • 实例 *23* 至实例 *33*	*102%* 禁止使用

Firepower 9300（设有一个 SM-44）

下表适用于仅使用物理接口或 Etherchannel 的 Firepower 9300（设一个 SM-44）。在未设子接口的情况下，接口的最大数量受限。此外，与共享多个子接口相比，共享多个物理接口所使用的转发表资源更多。

Firepower 9300（设有一个 SM-44）最多可支持 14 个实例。

表 *49: Firepower 9300*（设有一个 *SM-44*）上的物理*/EtherChannel* 接口和实例

专用接口	共享接口	实例数	转发表使用百分比
32: • 8 • 8 • 8 • 8	**0**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	16%
30: • 15 • 15	**0**	**2:** • 实例 1 • 实例 2	14%
14: • 14（每个实例 1 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
14: • 7（每个实例 1 个专用子接口） • 7（每个实例 1 个专用子接口）	**2:** • **1** • **1**	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%
32: • 8 • 8 • 8 • 8	**1**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	21%

专用接口	共享接口	实例数	转发表使用百分比
32: • 16（每个实例 8 个专用接口） • 16（每个实例 8 个专用接口）	**2**	**4:** • 实例 1 至实例 2 • 实例 3 至实例 4	20%
32: • 8 • 8 • 8 • 8	**2**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	25%
32: • 16（每个实例 8 个专用接口） • 16（每个实例 8 个专用接口）	**4:** • 2 • 2	**4:** • 实例 1 至实例 2 • 实例 3 至实例 4	24%
24: • 8 • 8 • 8	**8**	**3:** • 实例 1 • 实例 2 • 实例 3	37%
10: • 10（每个实例 2 个专用接口）	**10**	**5:** • 实例 1 至实例 5	69%

专用接口	共享接口	实例数	转发表使用百分比
10: • 6（每个实例2个专用接口） • 4（每个实例2个专用接口）	**20:** • 10 • 10	**5：** • 实例 1 至实例 3 • 实例 4 至实例 5	59%
14: • *12*（每个实例 *2* 个专用接口）	***10***	***7*：** • 实例 *1* 至实例 *7*	*109%* 禁止使用

下表适用于使用单父项物理接口上子接口的Firepower 9300（设有一个SM-44）。例如，创建一个大型 EtherChannel 以将所有类似接口捆绑在一起，然后共享该 EtherChannel 的子接口。与共享多个子接口相比，共享多个物理接口所使用的转发表资源更多。

Firepower 9300（设有一个 SM-44）最多可支持 14 个实例。

表 *50: Firepower 9300*（设有一个 *SM-44*）上的一个父接口的子接口和实例

专用子接口	共享子接口	实例数	转发表使用百分比
112： • 112（每个实例 8 个专用子接口）	**0**	**14:** • 实例 1 至实例 14	17%
224: • 224（每个实例 16 个专用子接口）	**0**	**14:** • 实例 1 至实例 14	17%
14: • 14（每个实例 1 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%

专用子接口	共享子接口	实例数	转发表使用百分比
14: • 7（每个实例1个专用子接口） • 7（每个实例1个专用子接口）	**2:** • 1 • 1	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%
112： • 112（每个实例 8 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
112： • 56（每个实例 8 个专用子接口） • 56（每个实例 8 个专用子接口）	**2:** • 1 • 1	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%
112： • 112（每个实例 8 个专用子接口）	**2**	**14:** • 实例 1 至实例 14	46%
112： • 56（每个实例 8 个专用子接口） • 56（每个实例 8 个专用子接口）	**4:** • 2 • 2	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%
140: • 140（每个实例 10 个专用子接口）	**10**	**14:** • 实例 1 至实例 14	46%

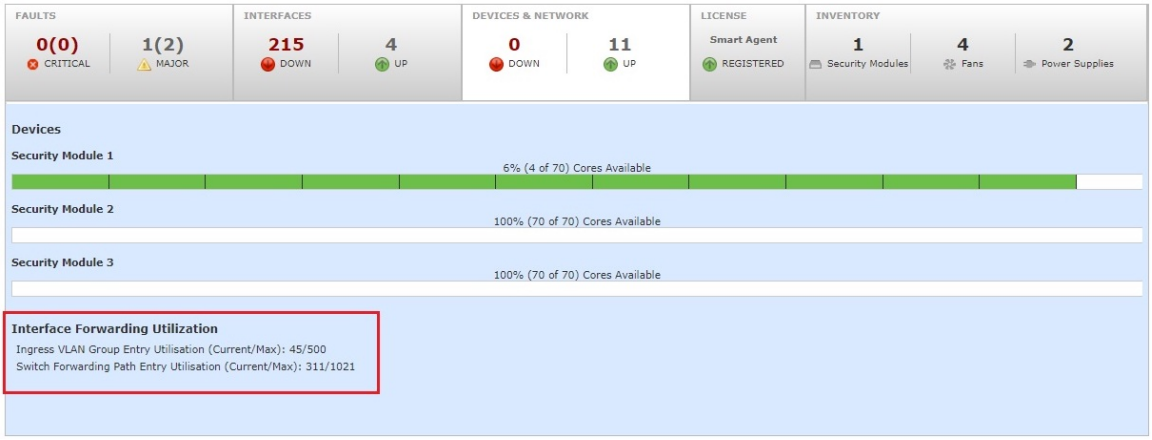
专用子接口	共享子接口	实例数	转发表使用百分比
140: • 70（每个实例10个专用子接口） • 70（每个实例10个专用子接口）	**20:** • 10 • 10	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%

查看共享接口资源

要查看转发表和 VLAN 组使用情况，请参阅**设备和网络 (Devices & Network)** > **接口转发利用率 (Interface Forwarding Utilization)** 区域在 **scope fabric-interconnect** 下输入 **show detail** 命令。例如：

```
Firepower# scope fabric-interconnect
Firepower /fabric-interconnect # show detail

Fabric Interconnect:
    ID: A
    Product Name: Cisco FPR9K-SUP
    PID: FPR9K-SUP
    VID: V02
    Vendor: Cisco Systems, Inc.
    Serial (SN): JAD104807YN
    HW Revision: 0
    Total Memory (MB): 16185
    OOB IP Addr: 10.10.5.14
    OOB Gateway: 10.10.5.1
    OOB Netmask: 255.255.255.0
    OOB IPv6 Address: ::
    OOB IPv6 Gateway: ::
    Prefix: 64
    Operability: Operable
    Thermal Status: Ok
    Ingress VLAN Group Entry Count (Current/Max): 0/500
    Switch Forwarding Path Entry Count (Current/Max): 16/1021
    Current Task 1:
    Current Task 2:
    Current Task 3:
```



威胁防御 支持的内联集链路状态传播

内联集类似于导线上的凹凸，用于将两个接口绑定在一起插入到现有网络中。此功能使系统可以安装在任何网络环境中，而无需配置相邻网络设备。内联接口无条件接收所有流量，但是，除非已明确丢弃，否则这些接口上接收的所有流量将在内联集外重传。

当您在 威胁防御 应用中配置内联集并启用链路状态传播时，威胁防御 会向 FXOS 机箱发送内联集成员身份。链路状态传播意味着，当内联集的一个接口断开时，机箱将自动关闭内联接口对的第二个接口。当被关闭的接口恢复运行时，第二个接口也将自动恢复运行。换句话说，如果一个接口的链路状态更改，机箱会感知该更改并更新其他接口的链路状态以与其匹配。请注意，机箱最多需要 4 秒即可传播链路状态更改。在将路由器配置为在处于故障状态的网络设备上自动重新路由流量的弹性网络环境中，链路状态传播特别有用。

关于逻辑设备

逻辑设备允许您运行一个应用实例（ASA 或 威胁防御）和一个可选修饰器应用 (Radware DefensePro) 以形成服务链。

当您添加逻辑设备时，还应定义应用实例类型和版本，分配接口，并配置推送至应用配置的引导程序设置。

注释 对于 Firepower 9300，可以在机箱中的独立模块上安装不同类型的应用（ASA 和 威胁防御）。还可以在独立模块上运行一种应用实例的不同版本。

独立和群集逻辑设备

您可以添加以下类型的逻辑设备：

- 独立 - 独立逻辑设备作为独立单元或高可用性对中的单元运行。

- 集群 - 集群逻辑设备允许您将多个单元集合在一起，具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。Firepower 9300 等多模块设备支持机箱内群集。对于 Firepower 9300，所有三个模块必须参与集群，同时适用于本地实例和容器实例。设备管理器不支持集群。

逻辑设备应用程序实例：容器和本地

应用实例在以下类型部署中运行：

- 本地实例 - 本地实例使用安全模块/引擎的所有资源（CPU、RAM 和磁盘空间），因此您仅可安装一个本地实例。
- 容器实例 - 容器实例使用安全模块/引擎的部分资源，因此您可以安装多个容器实例。仅使用 管理中心 的 威胁防御 支持多实例功能；ASA 或使用 设备管理器 的 威胁防御 不支持。

注释 尽管实现方式不同，但多实例功能与 ASA 多情景模式类似。多情景模式下区分了单个应用实例，而多实例功能允许独立容器实例。容器实例允许硬资源分离、单独配置管理、单独重新加载、单独软件更新和完全威胁防御功能支持。由于共享资源，多情景模式支持给定平台上的更多情景。威胁防御 的多情景模式不可用。

对于 Firepower 9300，可以在某些模块上使用本地实例，在其他模块上使用容器实例。

容器实例接口

要确保灵活使用容器实例的物理接口，可以在 FXOS 中创建 VLAN 子接口，还可以在多个实例之间共享接口（VLAN 或物理接口）。本地实例不得使用 VLAN 子接口或共享接口。 多实例集群不得使用 VLAN 子接口或共享接口。集群控制链路例外，它可以使用集群 EtherChannel 的子接口。请参阅共享接口可扩展性，第 394 页和为容器实例添加 VLAN 子接口，第 429 页。

注释 本文档仅讨论 *FXOS* VLAN 子接口。您还可以在 威胁防御 应用内单独创建子接口。有关详细信息，请参阅FXOS 接口与应用接口，第 392 页。

机箱如何将数据包分类

必须对进入机箱的每个数据包进行分类，以便机箱能够确定将数据包发送到哪个实例。

- 唯一接口 - 如果仅有一个实例与传入接口相关联，则机箱会将数据包分类至该实例。对于桥接组成员接口（在透明模式或路由模式下）、内联集或被动接口，此方法用于始终与数据包进行分类。
- 唯一 MAC 地址 - 机箱将自动生成包括共享接口在内的所有接口的唯一 MAC 地址。如果多个实例共享一个接口，则分类器在每个实例中使用分配给该接口的唯一 MAC 地址。上游路由器无

法直接路由至不具有唯一MAC地址的实例。在应用内配置每个接口时，您也可以手动设置MAC地址。

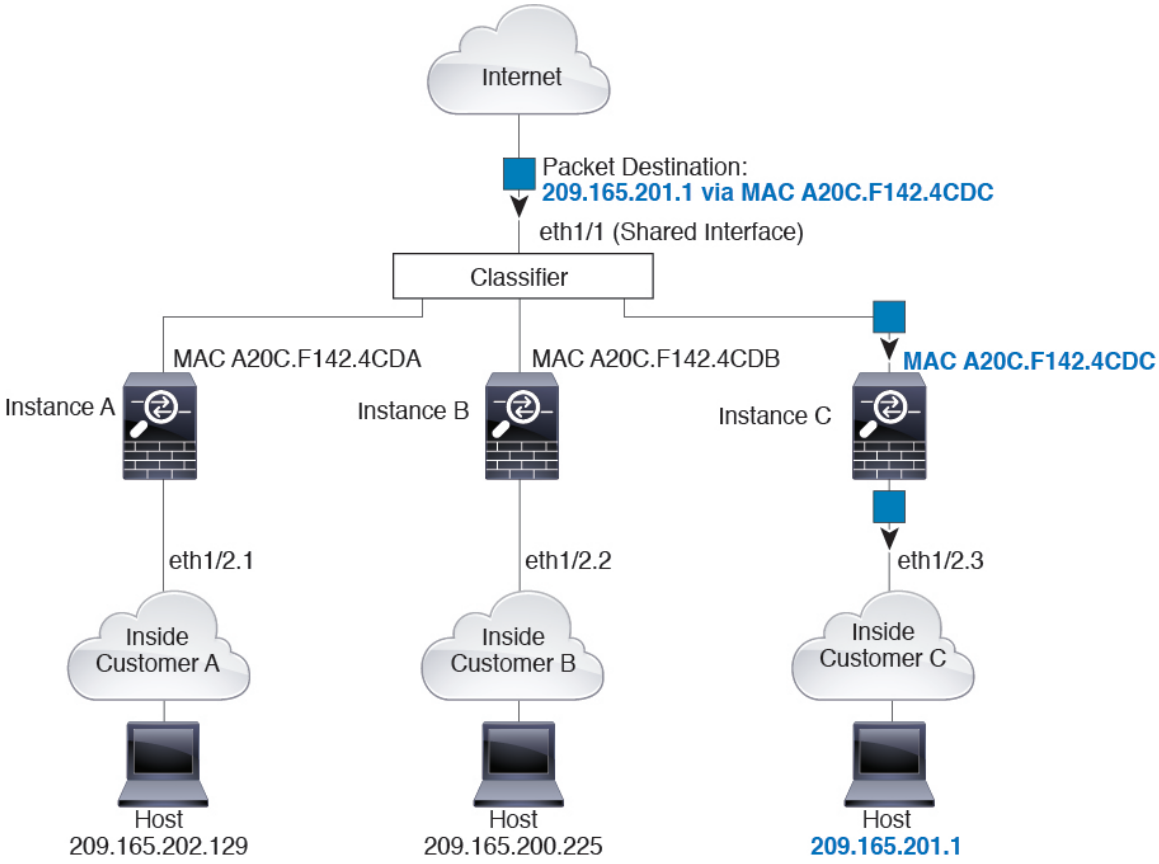
注释 如果目的 MAC 地址为组播或广播 MAC 地址，则数据包会复制并传递到每个实例。

分类示例

使用 MAC 地址通过共享接口进行数据包分类

下图显示共享外部接口的多个实例。因为实例 C 包含路由器将数据包发送到的 MAC 地址，因此分类器会将该数据包分配至实例 C。

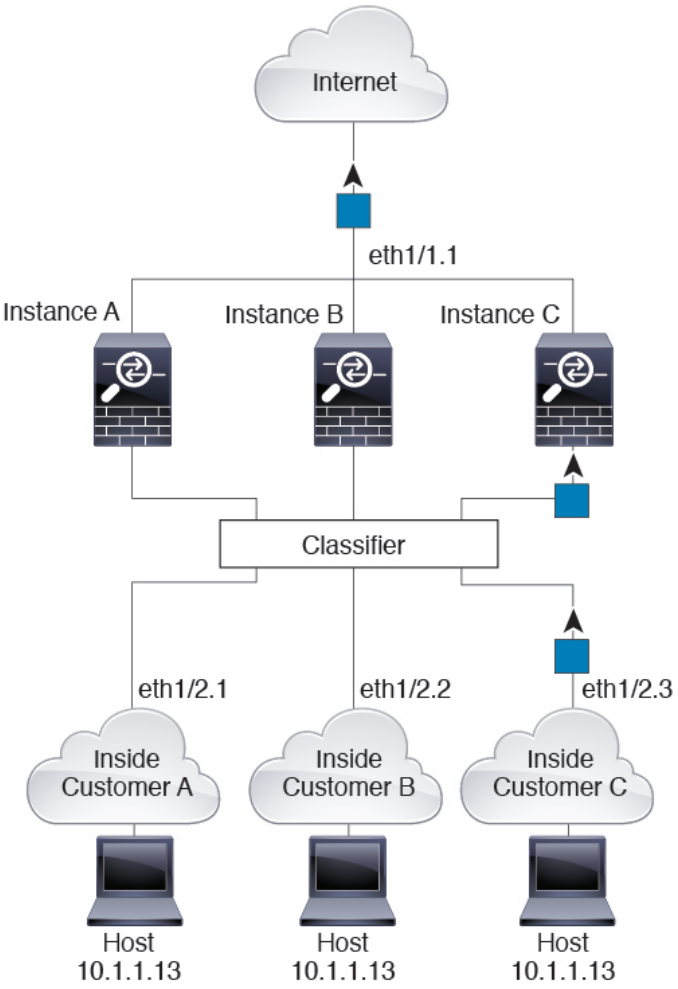
图 *50:* 使用 *MAC* 地址通过共享接口进行数据包分类



来自内部网络的传入流量

请注意，必须对所有新的传入流量加以分类，即使其来自内部网络。下图展示了实例 C 内部网络上的主机访问互联网。由于传入接口是分配至实例 C 的以太网接口 1/2.3，因此分类器会将数据包分配至实例 C。

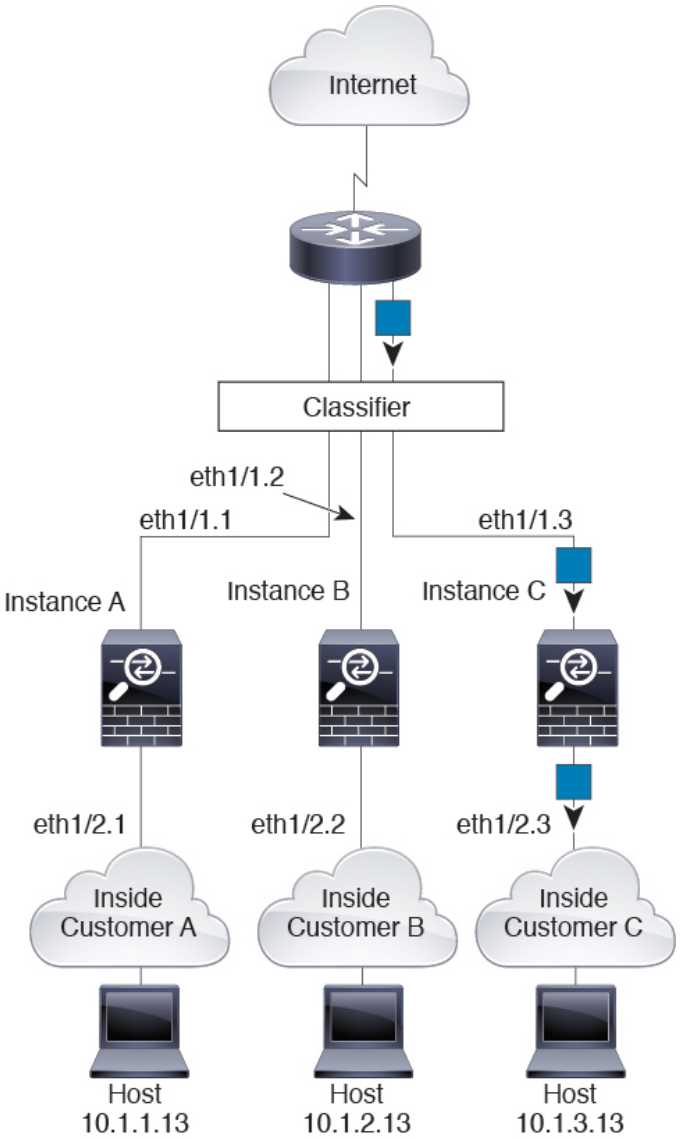
图 *51:* 来自内部网络的传入流量



透明防火墙实例

对于透明防火墙，您必须使用唯一接口。下图展示了来自互联网并以实例 C 内部网络上的主机为目标的数据包。由于传入接口是分配至实例 C 的以太网接口 1/2.3，因此分类器会将数据包分配至实例 C。

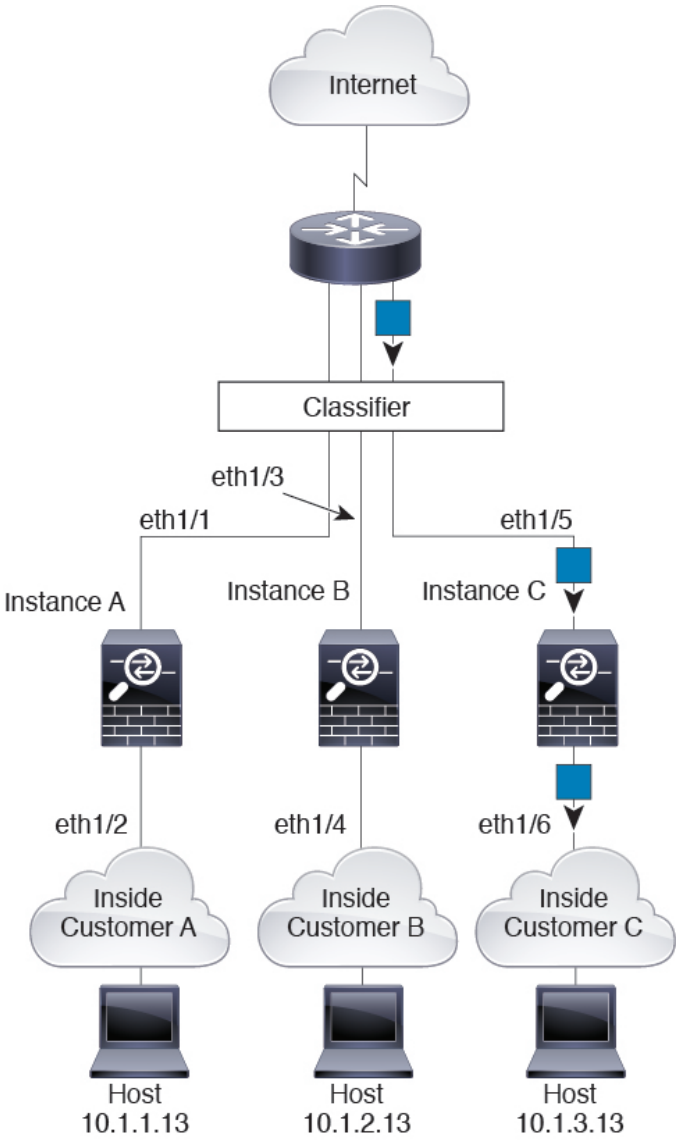
图 *52:* 透明防火墙实例



内联集

对于内联集，必须使用唯一接口，并且这些接口必须为物理接口或 Etherchannel 接口。下图展示了来自互联网并以实例 C 内部网络上的主机为目标的数据包。由于传入接口是分配至实例 C 的以太网接口 1/5，因此分类器会将数据包分配至实例 C。

图 *53:* 内联集

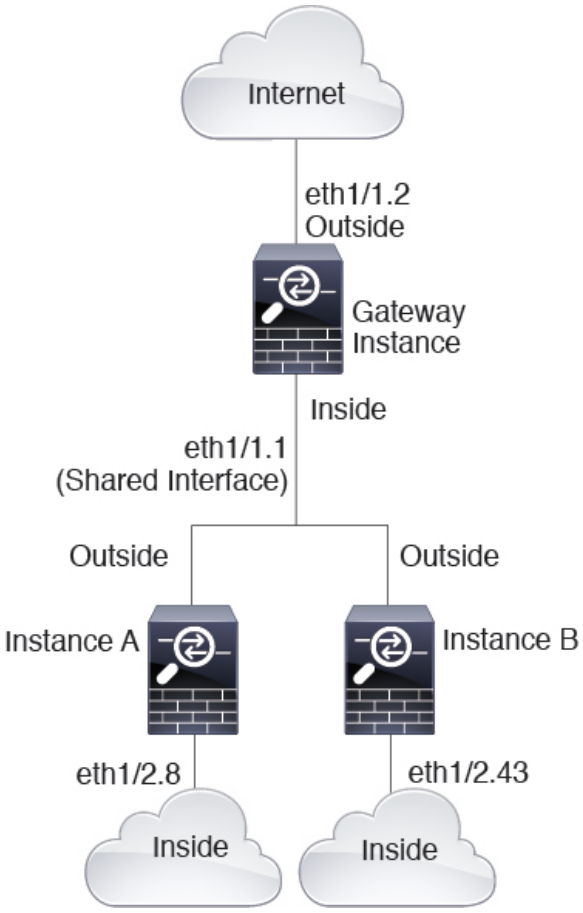


级联容器实例

直接在一个实例前面放置另一个实例的行为称为级联实例；一个实例的外部接口与另一个实例的内部接口完全相同。如果您希望通过在顶级实例中配置共享参数，从而简化某些实例的配置，则可能要使用级联实例。

下图显示了在网关后有两个实例的网关实例。

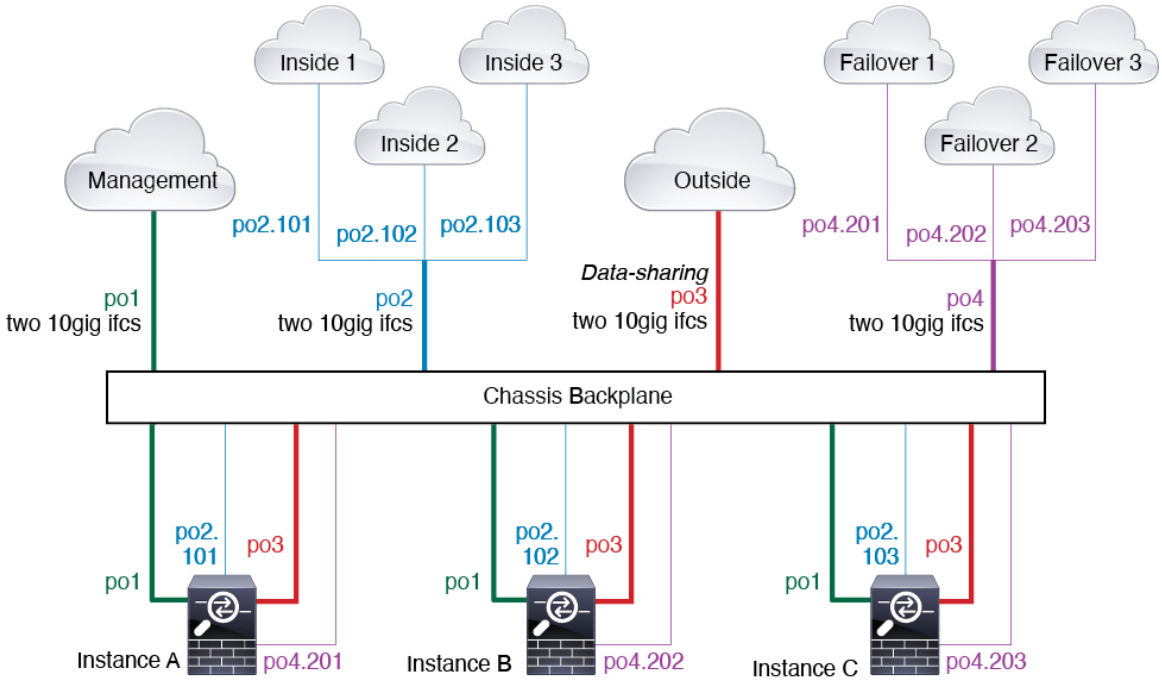
图 *54:* 级联实例



典型多实例部署

以下示例包括路由防火墙模式下的三个容器实例。这三个容器实例包括以下接口：

- 管理 - 所有实例都使用端口通道 1 接口（管理类型）。此 EtherChannel 包括两个万兆以太网接口。在每个应用内，该接口都使用同一管理网络上的唯一 IP 地址。
- 内部 - 每个实例使用端口通道 2 上的子接口（数据类型）。此 EtherChannel 包括两个万兆以太网接口。每个子接口位于独立的网络中。
- 外部 - 所有实例都使用端口通道 3 接口（数据共享类型）。此 EtherChannel 包括两个万兆以太网接口。在每个应用内，该接口都使用同一外部网络上的唯一 IP 地址。
- 故障切换 - 每个实例都使用端口通道 4 上的子接口（数据类型）。此 EtherChannel 包括两个万兆以太网接口。每个子接口位于独立的网络中。



容器实例接口的自动 MAC 地址

机箱会自动为实例接口自动生成 MAC 地址，以确保各个实例中的共享接口使用唯一 MAC 地址。

如果您手动为实例中的共享接口分配了一个 MAC 地址，则使用手动分配的 MAC 地址。如果您随后删除了手动 MAC 地址，则会使用自动生成的地址。在极少数情况下，生成的 MAC 地址会与网络中的其他专用 MAC 地址冲突，我们建议您在实例中为接口手动设置 MAC 地址。

由于自动生成的地址以 A2 开头，因此您不应该分配以 A2 开头的手动 MAC 地址，以避免出现地址重叠。

机箱使用以下格式生成 MAC 地址：

A2*xx.yyzz.zzzz*

其中， *xx.yy* 是用户定义的前缀或系统定义的前缀，*zz.zzzz* 是由机箱生成的内部计数器。系统定义的前缀与已在 IDPROM 中编程的烧录 MAC 地址池中的第一个 MAC 地址的 2 个低位字节相匹配。使用 **connect fxos**，然后通过 **show module** 查看 MAC 地址池。例如，如果显示的适用于模块 1 的 MAC 地址范围为 b0aa.772f.f0b0 至 b0aa.772f.f0bf，则系统前缀将是 f0b0。

用户定义的前缀是转换为十六进制的整数。如何使用用户定义前缀的示例如下：如果将前缀设置为 77，则机箱会将 77 转换为十六进制值 004D (*yyxx*)。在 MAC 地址中使用时，该前缀会反转 (*xxyy*)，以便与机箱的本地形式匹配：

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

对于前缀 1009 (03F1)，MAC 地址为：

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

容器实例资源管理

要指定每个容器实例的资源使用情况，请在FXOS中创建一个或多个资源配置文件。部署逻辑设备/应用实例时，请指定想要使用的资源配置文件。资源配置文件会设置CPU核心数量；系统会根据核心数量动态分配RAM，并将每个实例的磁盘空间设为40 GB。要查看每个型号的可用资源，请参阅容器实例的要求和前提条件，第 418 页。要添加资源配置文件，请参阅为容器实例添加资源配置文件，第 432 页。

多实例功能的性能扩展因素

计算平台的最大吞吐量（连接数、VPN 会话数和 TLS 代理会话数）是为了得出本地实例的内存和 CPU 使用情况（此值显示在 **show resource usage** 中）。如果使用多个实例，则需要根据分配给实例的 CPU 核心百分比来计算吞吐量。例如，如果使用具有 50% 核心的容器实例，则最初应计算 50% 的吞吐量。此外，尽管扩展可能会因为您的网络而更好或更差，但容器实例可用的吞吐量可能低于本地实例可用的吞吐量。

有关计算实例吞吐量的详细说明，请参阅https://www.cisco.com/c/en/us/products/collateral/security/firewalls/white-paper-c11-744750.html。

容器实例与高可用性

您可以在 2 个独立机箱上使用容器实例来实现高可用性；例如，如果您有 2 个机箱，每个机箱设 10 个实例，您可以创建 10 个高可用性对。请注意，不得在FXOS中配置高可用性；在应用管理器中配置每个高可用性对。

有关详细要求，请参阅高可用性的要求和前提条件，第 419 页和添加高可用性对，第 450 页。

容器实例和集群

您可以每个安全模块/引擎各使用一个容器实例创建容器实例集群。

容器实例的许可证

所有许可证按每个引擎/机箱（对于 Firepower 4100）或每个安全模块（对于 Firepower 9300）予以使用，而不是按每个容器实例使用。请查看以下详细信息：

- 基本 许可证自动分配：每个 安全模块/引擎一个。
- 功能许可证手动分配到每个实例；但每个 安全模块/引擎每个功能只能使用一个许可证。例如，对于具有 3 个安全模块的 Firepower 9300，每个模块只需要一个 URL 过滤 许可证，总共需要 3 个许可证，而无须考虑正在使用的实例数。

例如：

表 *51: Firepower 9300* 上容器实例的许可证使用情况示例

Firepower 9300	实例	许可证
Security Module 1	实例 1	基本、 URL 过滤、 恶意软件
	实例 2	基本、 URL 过滤
	实例 3	基本、 URL 过滤
安全模块 2	实例 4	基本、 威胁
	实例 5	基本、 URL 过滤、 恶意软件、 威胁
安全模块 3	实例 6	基本、 恶意软件、 威胁
	实例 7	基本、 威胁

表 *52:* 许可证总数

基本	URL 过滤	恶意软件	威胁
3	2	3	2

逻辑设备的要求和必备条件

有关要求和必备条件，请参阅以下章节。

硬件和软件组合的要求与前提条件

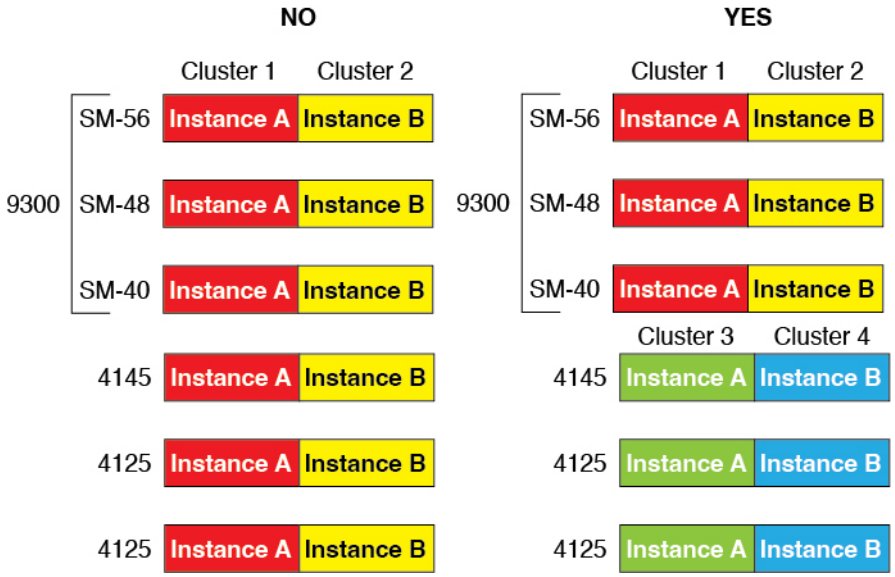
Firepower 4100/9300支持多种型号、安全模块、应用类型以及高可用性和可扩展性功能。请参阅以下要求，了解允许的组合。

Firepower 9300 的要求

Firepower 9300 包括 3 个安全模块插槽和多种类型的安全模块。请参阅以下要求：

- 安全模块类型 - 您可以在 Firepower 9300 中安装不同类型的模块。例如，您可以将 SM-48 作为模块 1、SM-40 作为模块 2、SM-56 作为模块 3 安装。
- 本地实例 集群 - 集群中的所有安全模块（无论是机箱内还是机箱间）都必须为同一类型。您可以在各机箱中安装不同数量的安全模块，但机箱中存在的所有模块（包括任何空插槽）必须属于集群。例如，您可以在机箱 1 中安装 2 个 SM-40，在机箱 2 中安装 3 个 SM-40。 如果在同一机箱中安装了 1 个 SM-48 和 2 个 SM-40，则无法使用集群。

- 容器实例集群 - 您可以使用不同型号类型上的实例创建集群。例如，您可以使用 Firepower 9300 SM-56、SM-48 和 SM-40 上的实例创建集群。但是，不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。

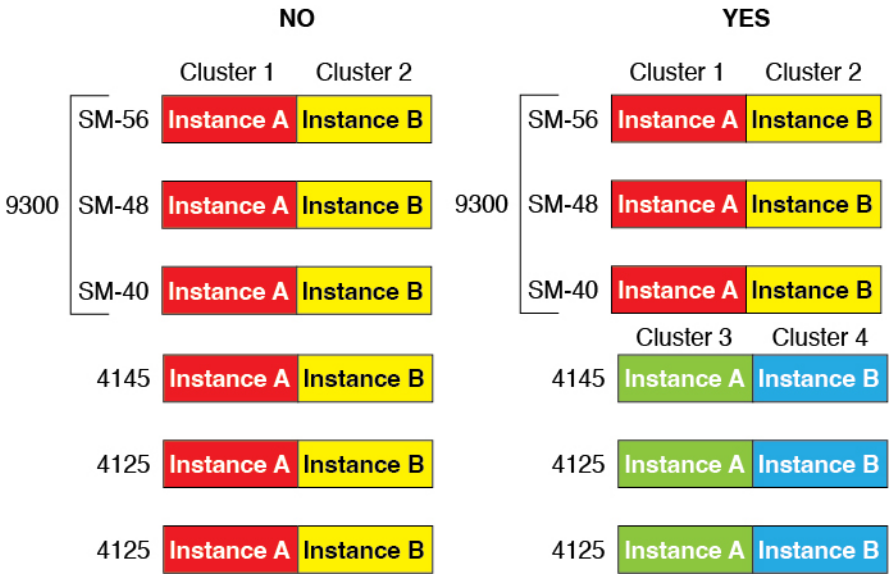


- 高可用性 - 仅在 Firepower 9300 上的同类模块间支持高可用性。 但是，这两个机箱可以包含混合模块。例如，每个机箱都设有 SM-40、SM-48 和 SM-56。可以在 SM-40 模块之间、SM-48 模块之间和 SM-56 模块之间创建高可用性对。
- ASA 和 威胁防御 应用类型-您可以在机箱中的独立模块上安装不同类型的应用。例如，您可以在模块 1 和模块 2 上安装 ASA，在模块 3 上安装 威胁防御 。
- ASA 或 威胁防御 版本 - 您可以在单独的模块上运行不同版本的应用实例类型，或在同一模块上运行单独的容器实例。例如，您可以在模块 1 上安装 威胁防御 6.3，在模块 2 上安装 威胁防御 6.4，在模块 3 上安装 威胁防御 6.5。

Firepower 4100 的要求

Firepower 4100 有多个型号。请参阅以下要求：

- 本地和容器实例 - 在 Firepower 4100 上安装容器实例时，该设备只能支持其他容器实例。本地实例将使用设备的所有资源，因此只能在设备上安装一个本地实例。
- 本地实例 集群 - 集群内的所有机箱都必须为同一型号。
- 容器实例集群 - 您可以使用不同型号类型上的实例创建集群。例如，您可以使用 Firepower 4145 和 4125 上的实例创建集群。但是，不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。



- 高可用性 - 仅在同类模块间支持高可用性。
- ASA 和 威胁防御 应用类型 - Firepower 4100 只能运行一种应用类型。
- 威胁防御 容器实例版本 - 您可以在同一模块上将不同版本的 威胁防御 作为单独的容器实例运行。

容器实例的要求和前提条件

受支持应用类型

- 使用 管理中心 的 威胁防御

每个型号的最大容器实例数和资源容量

对于每个容器实例，您可以指定要分配至实例的 CPU 核心数量。系统会根据核心数量动态分配 RAM，并将每个实例的磁盘空间设为 40 GB。

表 *53:* 每个型号的最大容器实例数和资源容量

型号	最大容器实例数	可用 **CPU** 核心	可用 **RAM**	可用磁盘空间
Firepower 4110	3	22	53 GB	125.6 GB
Firepower 4112	3	22	78 GB	308 GB
Firepower 4115	7	46	162 GB	308 GB
Firepower 4120	3	46	101 GB	125.6 GB
Firepower 4125	10	62	162 GB	644 GB

型号	最大容器实例数	可用 CPU 核心	可用 RAM	可用磁盘空间
Firepower 4140	7	70	222 GB	311.8 GB
Firepower 4145	14	86	344 GB	608 GB
Firepower 4150	7	86	222 GB	311.8 GB
Firepower 9300 SM-24 安全模块	7	46	226 GB	656.4 GB
Firepower 9300 SM-36 安全模块	11	70	222 GB	640.4 GB
Firepower 9300 SM-40 安全模块	13	78	334 GB	1359 GB
Firepower 9300 SM-44 安全模块	14	86	218 GB	628.4 GB
Firepower 9300 SM-48 安全模块	15	94	334 GB	1341 GB
Firepower 9300 SM-56 安全模块	18	110	334 GB	1314 GB

管理中心 要求

对于在 Firepower 4100 机箱或 Firepower 9300 模块上的所有情况下，由于许可实施，您必须使用相同 管理中心 。

高可用性的要求和前提条件

- 高可用性故障转移配置中的两个设备必须：
  - 位于单独的机箱上；不支持 Firepower 9300 的机箱内高可用性。
  - 型号相同。
  - 将同一接口分配至高可用性逻辑设备。
  - 拥有相同数量和类型的接口。启用高可用性之前，所有接口必须在 FXOS 中进行相同的预配置。
- 仅 Firepower 9300 上同种类型模块之间支持高可用性；但是两个机箱可以包含混合模块。例如，每个机箱都设有 SM-56、SM-48 和 SM-40。可以在 SM-56 模块之间、SM-48 模块之间和 SM-40 模块之间创建高可用性对。
- 对于容器实例，每个单元必须使用相同的资源配置文件属性。
- 有关其他高可用性系统要求，请参阅 高可用性系统要求 ， 第 456 页一章。

逻辑设备的准则和限制

有关准则和限制，请参阅以下章节。

接口的准则和限制

VLAN 子接口

- 本文档仅讨论 *FXOS* VLAN 子接口。您还可以在 威胁防御 应用内单独创建子接口。有关详细信息，请参阅FXOS 接口与应用接口，第 392 页。
- 子接口（和父接口）仅可分配至容器实例。

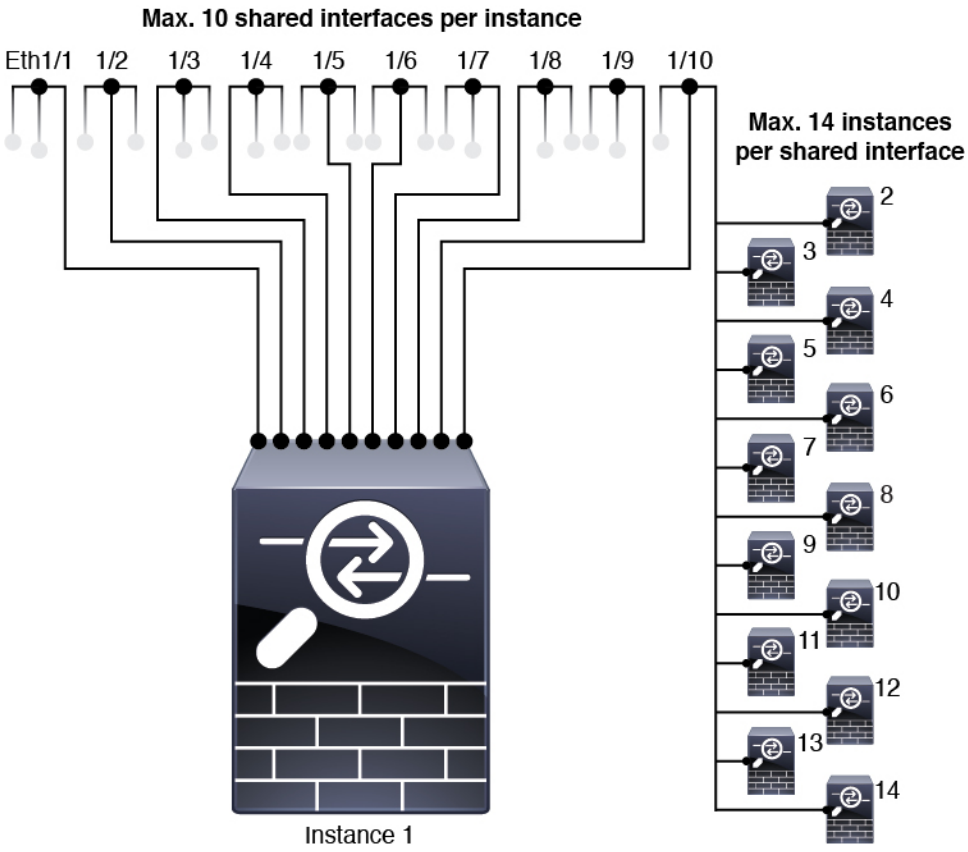
注释 如果将父接口分配至容器实例，该接口将仅传递未标记（非 VLAN）流量。除非您想要传递未标记流量，否则不予分配父接口。对于集群类型接口，不得使用父接口。

- 子接口在数据或数据共享型接口以及集群类型接口上受支持。如果向某个集群接口添加子接口，则不能将该接口用于本地集群。
- 对于多实例集群，数据接口上不支持 FXOS 子接口。但是，集群控制链路支持子接口，因此可以将专用 EtherChannel 或 EtherChannel 子接口用于集群控制链路。请注意，数据接口支持 应用定义的子接口。
- 最多可以创建 500 个 VLAN ID。
- 请参阅逻辑设备应用中的以下限制；规划接口分配时，请谨记这些限制。
  - 不得将子接口用于 威胁防御 内联集或用作被动接口。
  - 如果将子接口用于故障转移链路，则该父接口及其上的所有子接口仅限于用作故障转移链路。不得将某些子接口用作故障转移链路，而将某些用作常规数据接口。

数据共享接口

- 不得结合使用数据共享接口和本地实例。
- 每个共享接口最多 14 个实例。例如，您可以将以太网接口 1/1 分配至实例 1 至实例 14。

  每个实例最多 10 个共享接口。例如，您可以将以太网接口 1/1.1 至以太网接口 1/1.10 分配至实例 1。



- 不得在集群中使用数据共享接口。
- 请参阅逻辑设备应用中的以下限制；规划接口分配时，请谨记这些限制。
  - 不得结合使用数据共享接口和透明防火墙模式设备。
  - 不得结合数据共享接口和 威胁防御 内联集或被动接口。
  - 不得将数据共享接口用于故障转移链路。

FTD 的内联集 威胁防御

- 支持物理接口（常规端口和分支端口）和 Etherchannel。 不支持子接口。
- 支持链路状态传播。

硬件旁路

- 支持 威胁防御；可以将它们用作 ASA 的常规接口。
- 威胁防御仅支持包含内联集的 硬件旁路。
- 不可为分支端口配置具有硬件旁路功能的接口。

- 不得包含 EtherChannel 中的硬件旁路接口包含在并将它们用于硬件旁路；可以将它们用作 EtherChannel 中的常规接口。
- 硬件旁路不支持高可用性。

默认 MAC 地址

对于本地实例：

默认 MAC 地址分配取决于接口类型。

- 物理接口 - 物理接口使用已刻录的 MAC 地址。
- EtherChannel - 对于 EtherChannel，属于通道组的所有接口共用同一个 MAC 地址。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。端口通道接口使用来自池中的唯一 MAC 地址；接口成员身份不影响 MAC 地址。

对于容器实例：

- 所有接口的 MAC 地址均取自一个 MAC 地址池。对于子接口，如果决定要手动配置 MAC 地址，请确保将唯一 MAC 地址用于同一父接口上的所有子接口，从而确保分类正确。请参阅容器实例接口的自动 MAC 地址，第 414 页。

一般准则和限制

防火墙模式

您可以在 威胁防御 的引导程序配置中将防火墙模式设置为路由或透明模式。

高可用性

- 在应用配置中配置高可用性。
- 可以将任何数据接口用作故障转移和状态链路。 不支持数据共享接口。

多实例

- 包含容器实例的多实例功能仅适用于使用 管理中心 的 威胁防御。
- 对于 威胁防御 容器实例，单个 管理中心必须管理安全模块/引擎上的所有实例。
- 对于 威胁防御 容器实例，不支持以下功能：
  - Radware DefensePro 链路修饰器
  - 管理中心 UCAPL/CC 模式
  - 到硬件的数据流分流

配置接口

默认情况下，物理接口处于禁用状态。可以启用接口，添加 Etherchannel，添加 VLAN 子接口，编辑接口属性。

启用或禁用接口

可以将每个接口的**管理状态**更改为启用或禁用。默认情况下，物理接口处于禁用状态。 对于 VLAN 子接口，其管理状态继承自父接口。

过程

步骤 1 选择**接口 (Interfaces)** 打开接口页面。

“接口 (Interfaces)”页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 要启用接口，请点击已禁用**滑块已禁用**（  ），使其更改为已启用**滑块已启用**（  ）。

点击**是**，确认更改。以直观展示图表现的对应接口从灰色变为绿色。

步骤 3 要禁用接口，请点击已启用**滑块已启用**（  ），使其更改为已禁用**滑块已禁用**（  ）。

点击**是**，确认更改。以直观展示图表现的对应接口从绿色变为灰色。

配置物理接口

您可以通过物理方式启用和禁用接口，并设置接口速度和双工。要使用某一接口，必须在 FXOS 中以物理方式启用它，并在应用中以逻辑方式启用它。

注释 对于 QSFPH40G-CUxM，默认情况下自动协商会始终处于启用状态，并且您无法将其禁用。

开始之前

- 不能单独修改已经是 EtherChannel 成员的接口。务必在将接口添加到 EtherChannel 之前为其配置设置。

过程

步骤 1 选择**接口 (Interfaces)** 打开“接口”(Interfaces) 页面。

所有接口页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 在您要编辑的接口所对应的行中点击**编辑 (Edit)**，可打开**编辑接口 (Edit Interface)** 对话框。

步骤 3 要启用接口，请选中**启用**复选框。要禁用接口，请取消选中**启用**复选框。

步骤 4 选择接口**类型**：

有关接口类型使用的详细信息，请参阅接口类型，第 390 页。

- **数据**
- **数据共享** - 仅用于容器实例。
- **管理**
- **Firepower 事件** - 仅用于 威胁防御 。
- **集群** - 请勿选择**集群**类型；默认情况下，系统会自动在端口通道 48 上创建集群控制链路。

步骤 5 （可选） 从**速度 (Speed)** 下拉列表中选择接口的速度。

步骤 6 （可选） 如果您的接口支持**自动协商**，请点击**是 (Yes)** 或**否 (No)** 单选按钮。

步骤 7 （可选） 从**双工 (Duplex)** 下拉列表中选择接口双工。

步骤 8 （可选） 明确配置**防反跳时间 (ms)**。输入 0-15000 毫秒之间的值。

步骤 9 点击**确定 (OK)**。

步骤 10 进入接口模式。

scope eth-uplink

scope fabric a

步骤 11 启用接口。

enter interface *interface_id*

enable

示例：

```
Firepower /eth-uplink/fabric # enter interface Ethernet1/8
Firepower /eth-uplink/fabric/interface # enable
```

注释 不能单独修改作为端口通道成员的接口。如果您在作为端口通道成员的接口上使用**enter interface** 或 **scope interface** 命令，将会收到一条错误消息，说明对象不存在。应先使用 **enter interface** 命令编辑接口，然后在将接口添加到端口通道。

步骤 12 （可选）设置防反跳时间。

set debounce-time 5000 {Enter a value between 0-15000 milli-seconds}

示例：

```
Firepower /eth-uplink/fabric/interface # set debounce-time 5000
```

步骤 13 （可选）设置接口类型。

set port-type {**data** | **mgmt** | **cluster**}

示例：

```
Firepower /eth-uplink/fabric/interface # set port-type mgmt
```

data 关键字为默认类型。请勿选择 **cluster** 关键字；默认情况下，系统会自动在端口通道 48 上创建集群控制链路。

步骤 14 启用或禁用自动协商（如果您的接口支持）。

set auto-negotiation {**on** | **off**}

示例：

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

步骤 15 设置接口速度。

set admin-speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

示例：

```
Firepower /eth-uplink/fabric/interface* # set admin-speed 1gbps
```

步骤 16 设置接口双工模式。

set admin-duplex {**fullduplex** |**halfduplex**}

示例：

```
Firepower /eth-uplink/fabric/interface* # set admin-duplex halfduplex
```

步骤 17 如果您编辑了默认流量控制策略，则它已应用于接口。如果您创建了新策略，请将其应用于接口。

set flow-control-policy *name*

示例：

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

步骤 18 保存配置。

commit-buffer

示例：

```
Firepower /eth-uplink/fabric/interface* # commit-buffer
Firepower /eth-uplink/fabric/interface #
```

添加 EtherChannel（端口通道）

EtherChannel（也称为端口通道）最多可以包含 16 个同一介质类型和容量的成员接口，并且必须设置为相同的速度和双工模式。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。链路汇聚控制协议 (LACP) 将在两个网络设备之间交换链路汇聚控制协议数据单元 (LACPDU)，进而汇聚接口。

您可以将 EtherChannel 中的每个物理数据或数据共享接口配置为：

- Active - 发送和接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。
- 开启 - EtherChannel 始终开启，并且不使用 LACP。“开启”的 EtherChannel 只能与另一个“开启”的 EtherChannel 建立连接。

注释 如果将其模式从打开更改为主用或从主用更改为打开状态，则可能需要多达三分钟的时间才能使 EtherChannel 进入运行状态。

非数据接口仅支持主用模式。

LACP 将协调自动添加和删除指向 EtherChannel 的链接，而无需用户干预。LACP 还会处理配置错误，并检查成员接口的两端是否连接到正确的通道组。 如果接口发生故障且未检查连接和配置，“开启”模式将不能使用通道组中的备用接口。

Firepower 4100/9300 机箱 创建 EtherChannel 时，EtherChannel 将处于**挂起**状态（对于主动 LACP 模式）或**关闭**状态（对于打开 LACP 模式），直到将其分配给逻辑设备，即使物理链路是连通的。EtherChannel 在以下情况下将退出**挂起**状态：

- 将 EtherChannel 添加为独立逻辑设备的数据或管理端口
- 将 EtherChannel 添加为属于集群一部分的逻辑设备的管理接口或集群控制链路
- 将 EtherChannel 添加为属于集群一部分的逻辑设备的数据端口，并且至少有一个单元已加入该集群

请注意，EtherChannel 在您将它分配到逻辑设备前不会正常工作。如果从逻辑设备移除 EtherChannel 或删除逻辑设备，EtherChannel 将恢复为**挂起**或**关闭**状态。

过程

步骤 1 选择**接口 (Interfaces)** 打开“接口”(Interfaces) 页面。

所有接口页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 点击接口表上方的**添加端口通道 (Add Port Channel)**，可打开**添加端口通道 (Add Port Channel)** 对话框。

步骤 3 在**端口通道 ID (Port Channel ID)** 字段中输入端口通道 ID。有效值介于 1 与 47 之间。

部署集群逻辑设备时，端口通道 48 为集群控制链路预留。如果不想将端口通道 48 用于集群控制链路，可以将其删除并为集群类型 EtherChannel 配置不同的 ID。您可以添加多个集群类型 Etherchannel，并添加 VLAN 子接口以与多实例集群结合使用。对于机箱内集群，请不要将任何接口分配给集群 EtherChannel。

步骤 4 要启用端口通道，请选中**启用**复选框。要禁用端口通道，请取消选中**启用**复选框。

步骤 5 选择接口**类型**：

有关接口类型使用的详细信息，请参阅接口类型，第 390 页。

- **数据**
- **数据共享** - 仅用于容器实例。
- **管理**
- **Firepower 事件** - 仅用于 威胁防御 。
- **集群**

步骤 6 从下拉列表设置成员接口要求的**管理速度**。

如果添加未达到指定速度的成员接口，接口将无法成功加入端口通道。

步骤 7 对于数据或数据共享接口，选择 LACP 端口通道**模式**、**主用**或**保持**。

对于非数据或数据共享接口，模式始终是主用模式。

步骤 8 为成员接口、**全双工**或**半双工**设置所需的**管理双工**。

如果添加以指定双工配置的成员接口，接口将无法成功加入端口通道。

步骤 9 要将接口添加到端口通道，请在**可用接口 (Available Interface)** 列表中选择该接口，点击**添加接口 (Add Interface)**，将接口移动至“成员 ID”列表。

您最多可以添加相同介质类型和容量的16个成员接口。成员接口必须设置为相同的速度和双工，并且必须与您为此端口通道配置的速度和双工相匹配。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的SFP。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。

提示 一次可添加多个接口。要选择多个独立接口，请点击所需的接口，同时按住 **Ctrl** 键。要选择一个接口范围，请选择范围中的第一个接口，然后，在按住 **Shift** 键的同时，点击选择范围中的最后一个接口。

步骤 10 要从端口通道删除接口，请点击“成员 ID”(Member ID) 列表中接口右侧的**删除 (Delete)** 按钮。

步骤 11 点击**确定 (OK)**。

步骤 12 进入接口模式：

scope eth-uplink

scope fabric a

步骤 13 创建端口通道：

create port-channel *id*

enable

步骤 14 分配成员接口：

create member-port *interface_id*

您最多可以添加相同介质类型和容量的16个成员接口。成员接口必须设置为相同的速度和双工，并且必须与您为此端口通道配置的速度和双工相匹配。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的SFP。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。

示例：

```
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
```

步骤 15 （可选） 设置接口类型。

set port-type {**data** | **mgmt** | **cluster**}

示例：

```
Firepower /eth-uplink/fabric/port-channel # set port-type data
```

data 关键字为默认类型。请勿选择 **cluster** 关键字，除非要将此端口通道用作集群控制链路，而不是默认设置。

步骤 16 为端口通道的成员设置所需的接口速度。

set speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

如果添加未达到指定速度的成员接口，接口将无法成功加入端口通道。默认值为 **10gbps**。

示例：

```
Firepower /eth-uplink/fabric/port-channel* # set speed 1gbps
```

步骤 17 （可选） 为端口通道的成员设置所需的双工。

set duplex {**fullduplex** | **halfduplex**}

如果添加以指定双工配置的成员接口，接口将无法成功加入端口通道。默认值为 **fullduplex**。

示例：

```
Firepower /eth-uplink/fabric/port-channel* # set duplex fullduplex
```

步骤 18 启用或禁用自动协商（如果您的接口支持）。

set auto-negotiation {**on** | **off**}

示例：

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

步骤 19 如果您编辑了默认流量控制策略，则它已应用于接口。如果您创建了新策略，请将其应用于接口。

set flow-control-policy *name*

示例：

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

步骤 20 提交配置：

commit-buffer

为容器实例添加 VLAN 子接口

您可以向机箱添加 250 至 500 个 VLAN 子接口，具体取决于网络部署。您最多可以将 500 个子接口连接到您的机箱。

对于多实例集群，只能将子接口添加到集群类型接口；不支持数据接口上的子接口。

每个接口的 VLAN ID 都必须具有唯一性，并且在容器实例内，VLAN ID 在所有已分配接口上也必须具有唯一性。只要系统将 VLAN ID 分配至不同的容器实例，您就可以在单独接口上重新使用它们。然而，即使每个子接口使用相同的 ID，这些子接口仍将计入限值。

本文档仅讨论 *FXOS* VLAN 子接口。您还可以在 威胁防御 应用内单独创建子接口。有关何时使用 FXOS 子接口与应用子接口的详细信息，请参阅FXOS 接口与应用接口，第 392 页。

过程

步骤 1 选择**接口 (Interfaces)**打开**所有接口 (All Interfaces)**选项卡。

页面顶部的**所有接口 (All Interfaces)** 选项卡显示当前已安装的接口的直观展示图，并在下表中提供已安装接口列表。

步骤 2 点击**添加新** > **子接口**打开**添加子接口**对话框。

步骤 3 选择接口**类型**：

有关接口类型使用的详细信息，请参阅接口类型，第 390 页。

- 数据
- 数据共享
- 集群 - 如果向某个集群接口添加子接口，则不能将此接口用于本地集群。

对于数据和数据共享接口：此类型独立于父接口类型；例如，您可以设数据共享父接口和数据子接口。

步骤 4 从下拉列表选择父**接口**。

不得将子接口添加到当前已分配至逻辑设备的物理接口。如果系统已分配父接口的其他子接口，只要未分配此父接口，您就可以添加新的子接口。

步骤 5 输入一个介于 1 和 4294967295 之间的**子接口 ID**。

此 ID 将附加到父接口 ID，作为 *interface_id.subinterface_id*。例如，如果您将子接口添加到 ID 为 100 的以太网接口 1/1，则子接口 ID 将为：以太网接口 1/1.100。尽管可以出于方便目的将此 ID 和 VLAN ID 设置为相互匹配，但两者始终不同。

步骤 6 设置介于 1 和 4095 之间的 **VLAN ID** 。

步骤 7 点击**确定 (OK)**。

展开父接口查看其项下所有子接口。

步骤 8 进入交换矩阵模式。

scope eth-uplink

scope fabric a

示例：

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric #
```

步骤 9 输入要添加子接口的接口。

enter {**interface** | **port-channel**} *interface_id*

不得将子接口添加到当前已分配至逻辑设备的物理接口。如果系统已分配父接口的其他子接口，只要未分配此父接口，您就可以添加新的子接口。

子接口在数据或数据共享型接口以及集群类型接口上受支持。

示例：

```
Firepower /eth-uplink/fabric # enter interface Ethernet1/8
Firepower /eth-uplink/fabric/interface #
```

步骤 10 创建子接口。

enter subinterface *id*

- *id* - 设置介于 1 和 4294967295 之间的 ID。此 ID 将附加到父接口 ID，作为 *interface_id.subinterface_id*。例如，如果您将子接口添加到 ID 为 100 的以太网接口 1/1，则子接口 ID 将为：以太网接口 1/1.100。尽管可以出于方便目的将此 ID 和 VLAN ID 设置为相互匹配，但两者始终不同。

示例：

```
Firepower /eth-uplink/fabric/interface # enter subinterface 100
Firepower /eth-uplink/fabric/interface/subinterface* #
```

步骤 11 设置 VLAN。

set vlan *id*

- *id* - 设置介于 1 和 4095 之间的 VLAN ID。

示例：

```
Firepower /eth-uplink/fabric/interface/subinterface* # set vlan 100
```

步骤 12 设置接口类型。

set port-type {**data** | **data-sharing**}

示例：

```
Firepower /eth-uplink/fabric/interface/subinterface* # set port-type data
```

对于数据和数据共享接口：此类型独立于父接口类型；例如，您可以设数据共享父接口和数据子接口。默认类型为数据。

步骤 13 保存配置。

commit-buffer

示例：

```
Firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
Firepower /eth-uplink/fabric/interface/subinterface #
```

示例

以下示例在以太网接口 1/1 上创建 3 个子接口，并将这些接口设置为数据共享接口。

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # enter interface Ethernet1/1
Firepower /eth-uplink/fabric/interface # enter subinterface 10
Firepower /eth-uplink/fabric/interface/subinterface* # set vlan 10
Firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
```

```
Firepower /eth-uplink/fabric/interface/subinterface* # exit
Firepower /eth-uplink/fabric/interface # enter subinterface 11
Firepower /eth-uplink/fabric/interface/subinterface* # set vlan 11
Firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
Firepower /eth-uplink/fabric/interface/subinterface* # exit
Firepower /eth-uplink/fabric/interface # enter subinterface 12
Firepower /eth-uplink/fabric/interface/subinterface* # set vlan 12
Firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
Firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
Firepower /eth-uplink/fabric/interface/subinterface #
```

配置逻辑设备

在 Firepower 4100/9300上添加独立逻辑设备或高可用性对。

为容器实例添加资源配置文件

要指定每个容器实例的资源使用情况，请创建一个或多个资源配置文件。部署逻辑设备/应用实例时，请指定想要使用的资源配置文件。资源配置文件会设置CPU核心数量；系统会根据核心数量动态分配 RAM，并将每个实例的磁盘空间设为 40 GB。

- 最小核心数量为 6。

注释 与具有较大内核数量的实例相比，具有较小核心数量的实例可能具有相对更高的 CPU 利用率。具有较小核心数量的实例对流量负载变化更敏感。如果出现流量丢弃情况，请尝试分配更多核心。

- 您可以分配偶数（6、8、10、12、14 等）个核心，乃至最大值。
- 最大可用核心数取决于安全模块/机箱型号，请参阅容器实例的要求和前提条件，第 418 页。

机箱包括一个命名为 "Default-Small" 的默认资源配置文件，此文件包括最小核心数。您可以更改此配置文件定义，甚至可在未使用情况下将其删除。请注意，此配置文件在机箱重新加载且系统上不存在任何其他配置文件时创建而成。

如果当前正在使用，则无法更改资源配置文件设置。必须禁用使用此文件的任何实例，然后更改资源配置文件，最后重新启用该实例。如果调整已建立高可用性对或集群中实例的大小，稍后应尽可能快地确保所有成员大小一致。

如果在将威胁防御实例添加到管理中心后更改资源配置文件设置，稍后应在管理中心 **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **系统 (System)** > **清单 (Inventory)** 对话框上更新每个设备的清单。

过程

步骤 1 选择**平台设置 (Platform Settings)** > **资源配置文件 (Resource Profiles)**，然后点击**添加 (Add)**。

系统将显示**添加资源配置文件**对话框。

步骤 2 设置以下参数。

- **Name** - 设置介于 1 和 64 个字符之间的配置文件名称。请注意，此配置文件名称添加后无法更改。
- **Description** - 设置最多 510 个字符的配置文件说明。
- **Number of Cores** - 设置介于 6 和最大值之间的配置文件核心数（偶数），具体取决于机箱。

步骤 3 点击**确定 (OK)**。

步骤 4 进入安全服务模式。

scope ssa

示例：

```
Firepower# scope ssa
Firepower /ssa #
```

步骤 5 创建资源配置文件。

enter resource-profile *name*

- *name* - 设置介于 1 和 64 个字符之间的配置文件名称。请注意，此配置文件名称添加后无法更改。

示例：

```
Firepower /ssa # enter resource-profile gold
Firepower /ssa/resource-profile* #
```

步骤 6 输入说明。

set description *description*

- *description* - 设置最多 510 个字符的配置文件说明。在含有空格的短语两侧使用引号 (")。

示例：

```
Firepower /ssa/resource-profile* # set description "highest level"
```

步骤 7 设置 CPU 核心数。

set cpu-core-count *cores*

- *cores* - 设置介于 6 和最大值之间的配置文件核心数（偶数），具体取决于机箱。 无法指定 8 个核心。

示例：

```
Firepower /ssa/resource-profile* # set cpu-core-count 14
```

步骤 8 保存配置。

commit-buffer

示例：

```
Firepower /ssa/resource-profile* # commit-buffer
Firepower /ssa/resource-profile #
```

步骤 9 从安全服务模式查看资源配置文件分配情况。

show resource-profile user-defined

示例：

```
Firepower /ssa # show resource-profile user-defined
Profile Name       Is In Use  CPU Logical Core Count Description
------------------ ---------- ---------------------- -----------
bronze               No               6             low end device
gold                 No               14            highest
silver               No               10             mid-level
```

步骤 10 查看安全模块/引擎插槽的资源使用情况。

show monitor detail

示例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # show monitor detail
Monitor:
    OS Version:
    CPU Total Load 1 min Avg: 18.959999
    CPU Total Load 5 min Avg: 19.080000
    CPU Total Load 15 min Avg: 19.059999
    Memory Total (MB): 252835
    Memory Free (MB): 200098
    Memory Used (MB): 52738
    CPU Cores Total: 72
    CPU Cores Available: 30
    Memory App Total (MB): 226897
    Memory App Available (MB): 97245
    Data Disk Total (MB): 1587858
    Data Disk Available (MB): 1391250
    Secondary Disk Total (MB): 0
    Secondary Disk Available (MB): 0
    Disk File System Count: 7
    Blade Uptime:
    Last Updated Timestamp: 2018-05-23T14:26:06.132
```

步骤 11 查看应用实例的资源配置情况。

show resource detail

示例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd ftd1
Firepower /ssa/slot/app-instance # show resource detail
Resource:
    Allocated Core NR: 10
    Allocated RAM (MB): 32413
    Allocated Data Disk (MB): 49152
    Allocated Binary Disk (MB): 3907
    Allocated Secondary Disk (MB): 0
```

示例

以下示例添加了三个资源配置文件。

```
Firepower# scope ssa
Firepower /ssa # enter resource-profile basic
Firepower /ssa/resource-profile* # set description "lowest level"
Firepower /ssa/resource-profile* # set cpu-core-count 6
Firepower /ssa/resource-profile* # exit
Firepower /ssa # enter resource-profile standard
Firepower /ssa/resource-profile* # set description "middle level"
Firepower /ssa/resource-profile* # set cpu-core-count 10
Firepower /ssa/resource-profile* # exit
Firepower /ssa # enter resource-profile advanced
Firepower /ssa/resource-profile* # set description "highest level"
Firepower /ssa/resource-profile* # set cpu-core-count 12
Firepower /ssa/resource-profile* # commit-buffer
Firepower /ssa/resource-profile #
```

为 管理中心

独立逻辑设备可单独使用，也可在高可用性对中使用。在具有多个安全模块的 Firepower 9300 上，可以配置集群或独立设备。集群必须使用所有模块，因此无法将双模块集群和独立设备进行混用和搭配。

可以在某些模块上使用本地实例，在其他模块上使用容器实例。

开始之前

- 从 Cisco.com 下载要用于逻辑设备的应用映像，然后将映像上传下载到 Firepower 4100/9300 机箱。

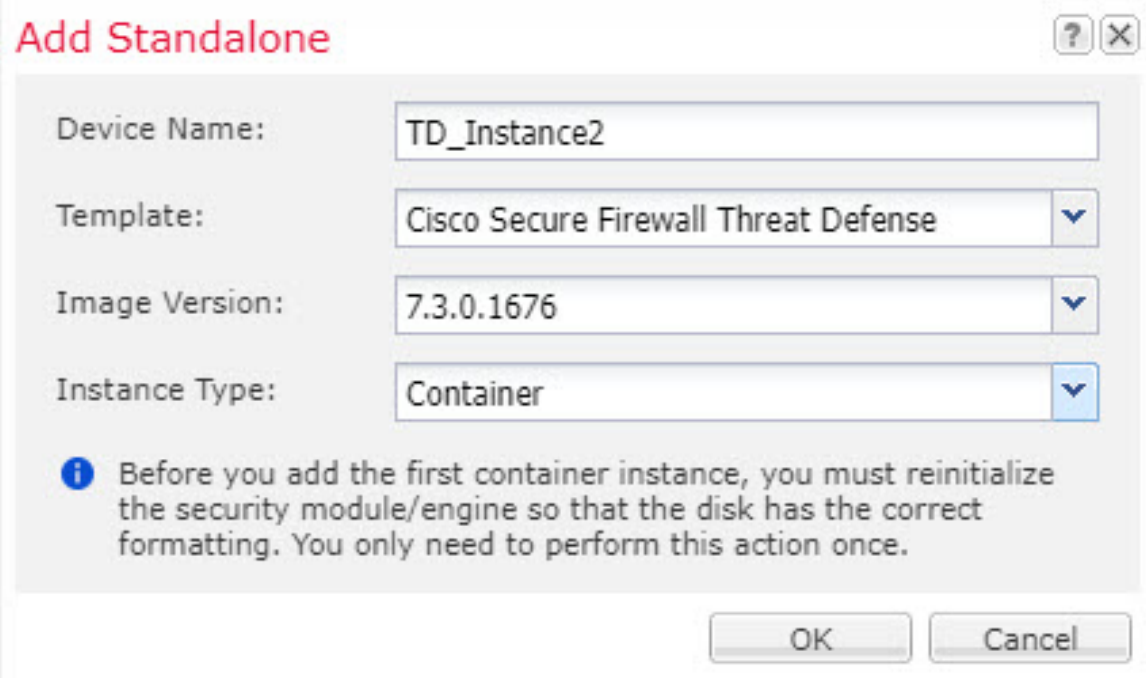
注释 对于 Firepower 9300，可以在机箱中的独立模块上安装不同类型的应用（ASA 和 威胁防御）。还可以在独立模块上运行一种应用实例的不同版本。

- 配置逻辑设备要使用的管理接口。管理接口是必需的。请注意，此管理接口不同于仅用于机箱管理的机箱管理端口（在 FXOS 中，可能会看到该接口显示为 MGMT、management0 或其他类似名称）（并且在**接口**选项卡的顶部显示为 **MGMT**）。
- 您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。有关详细信息，请参阅 FTD 命令参考中的 **configure network management-data-interface** 命令。
- 您还必须至少配置一个数据类型的接口。或者，您也可以创建Firepower事件接口，传输所有事件流量（例如 Web 事件）。有关详细信息，请参阅接口类型，第 390 页。
- 对于容器实例，如果您不想使用默认配置文件，则请根据为容器实例添加资源配置文件，第432页添加资源配置文件。
- 对于容器实例，在首次安装容器实例之前，必须重新初始化安全模块/引擎，以保证磁盘具有正确的格式。选择**安全模块**或**安全引擎**，然后点击**重新初始化图标**。首先删除现有逻辑设备，然后将其重新安装为新设备，这会丢失任何本地应用配置。如果要使用容器实例替换本地实例，则在任何情况下都需要删除本地实例。无法自动将本地实例迁移到容器实例。
- 收集以下信息：
  - 此设备的接口 ID
  - 管理接口 IP 地址和网络掩码
  - 网关 IP 地址
  - 您选择的管理中心 IP 地址和/或 NAT ID
  - DNS 服务器 IP 地址
  - 威胁防御 主机名和域名

过程

步骤 1 选择**逻辑设备**。

步骤 2 点击**添加** > **独立设备**，并设置以下参数：



a) 提供**设备名称**。

此名称由机箱管理引擎用于配置管理设置和分配接口；它不是在应用配置中使用的设备名称。

b) 对于**模板**，请选择 **Cisco Firepower 威胁防御**。

c) 选择**映像版本**。

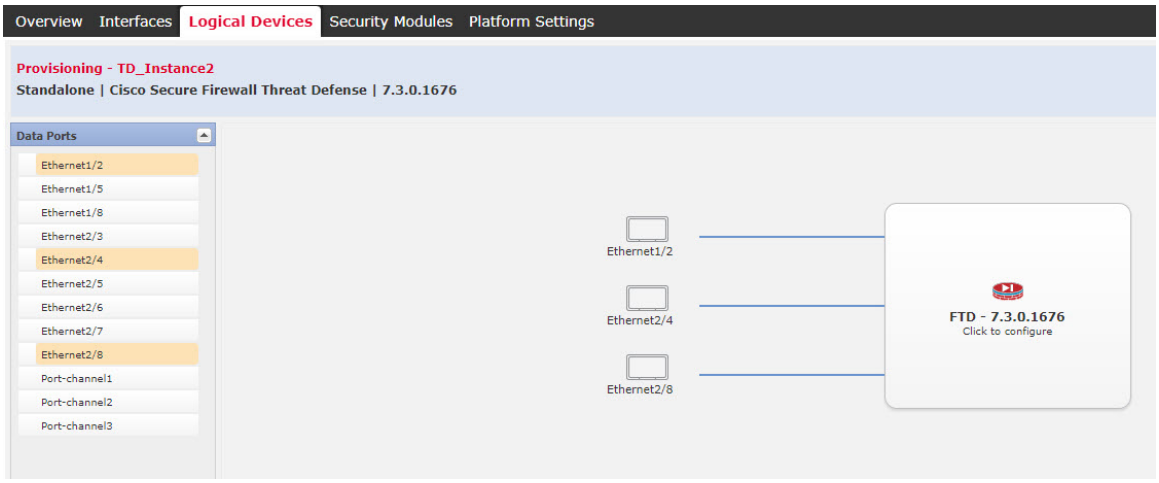
d) 选择**实例类型**：**容器**或**本地**。

本地实例使用安全模块/引擎的所有资源（CPU、RAM和磁盘空间），因此仅可安装一个本地实例。容器实例使用部分安全模块/引擎资源，因此可以安装多个容器实例。

e) 点击**确定 (OK)**。

屏幕会显示调配 - 设备名称窗口。

步骤 3 展开**数据端口 (Data Ports)** 区域，然后点击要分配给设备的每个接口。



您仅可分配先前在接口 (Interfaces) 页面上启用的数据**和数据共享**接口。稍后您需要在 管理中心 中启用和配置这些接口，包括设置 IP 地址。

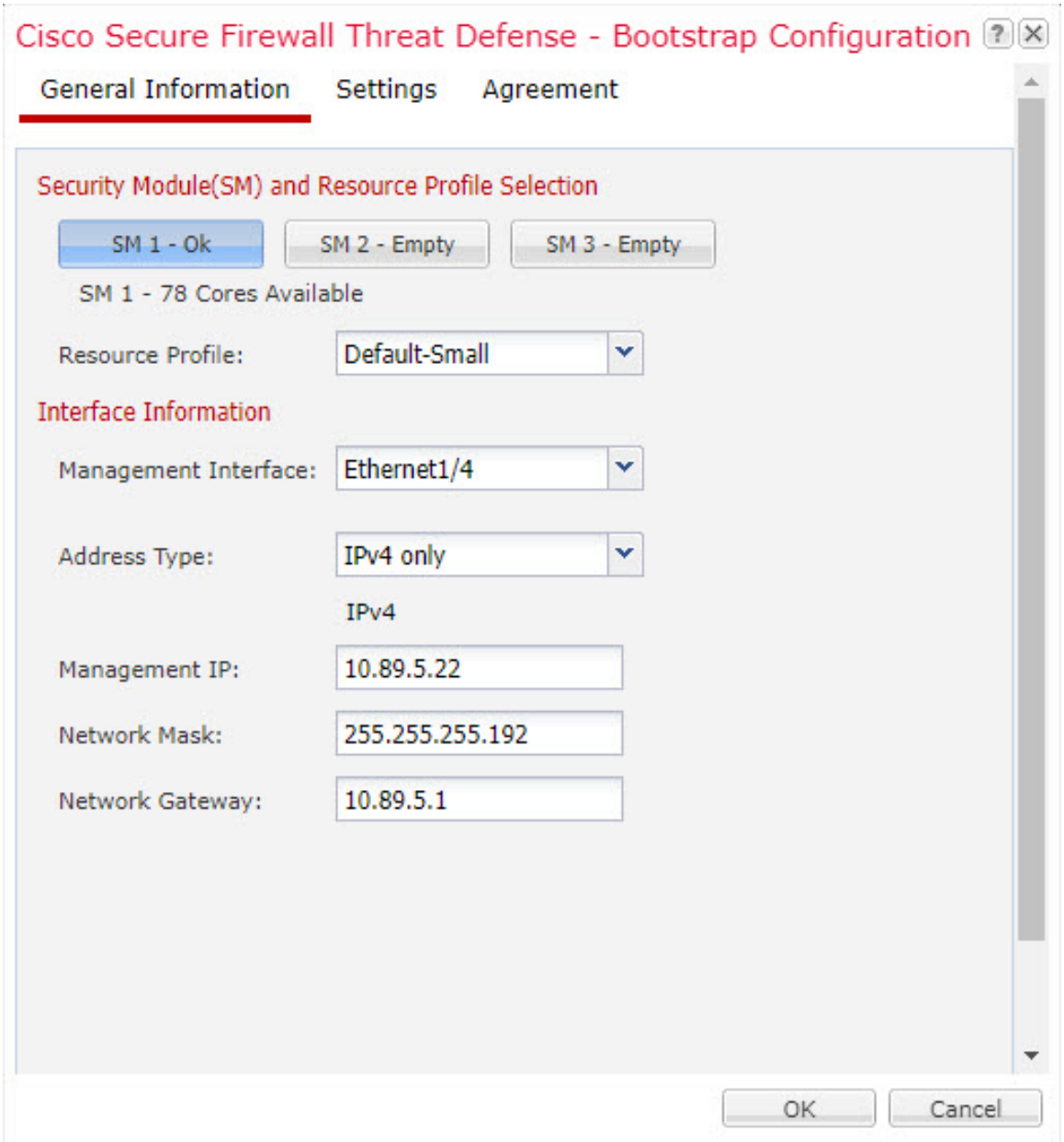
仅可向一个容器实例分配最多 10 个数据共享接口。此外，可以将每个数据共享接口分配至最多 14 个容器实例。数据共享接口以共享图标（ ） 表示。

具有硬件旁路功能的端口使用以下图标显示： 。对于某些接口模块，仅可启用用于内联集接口的硬件旁路功能（请参阅 管理中心 配置指南）。硬件绕行确保流量在断电期间继续在接口对之间流动。在软件或硬件发生故障时，此功能可用于维持网络连接性。如果您未同时分配一个硬件旁路对中的两个接口，则会收到一条警告消息，确认您是故意这样分配。您不需要使用硬件旁路功能，因此如果您愿意，可以分配单个接口。

步骤 4 点击屏幕中心的设备图标。

系统将显示对话框，可以在该对话框中配置初始引导程序设置。这些设置仅用于仅初始部署或灾难恢复。为了实现正常运行，稍后可以更改应用 CLI 配置中的大多数值。

步骤 5 在**一般信息 (General Information)** 页面上，完成下列操作：



a) （对于 Firepower 9300）在**安全模块选择**下，点击您想用于此逻辑设备的安全模块。

b) 对于容器实例，指定**资源配置文件**。

如果您稍后分配一个不同的资源配置文件，则实例将重新加载，这可能需要大约 5 分钟的时间。请注意，对于已建立的高可用性对或集群，如果分配不同大小的资源配置文件，请务必尽快确保所有成员大小一致。

c) 选择**管理接口**。

此接口用于管理逻辑设备。此接口独立于机箱管理端口。

d) 选择管理接口**地址类型**：**仅 IPv4**、**仅 IPv6** 或 **IPv4 和 IPv6**。

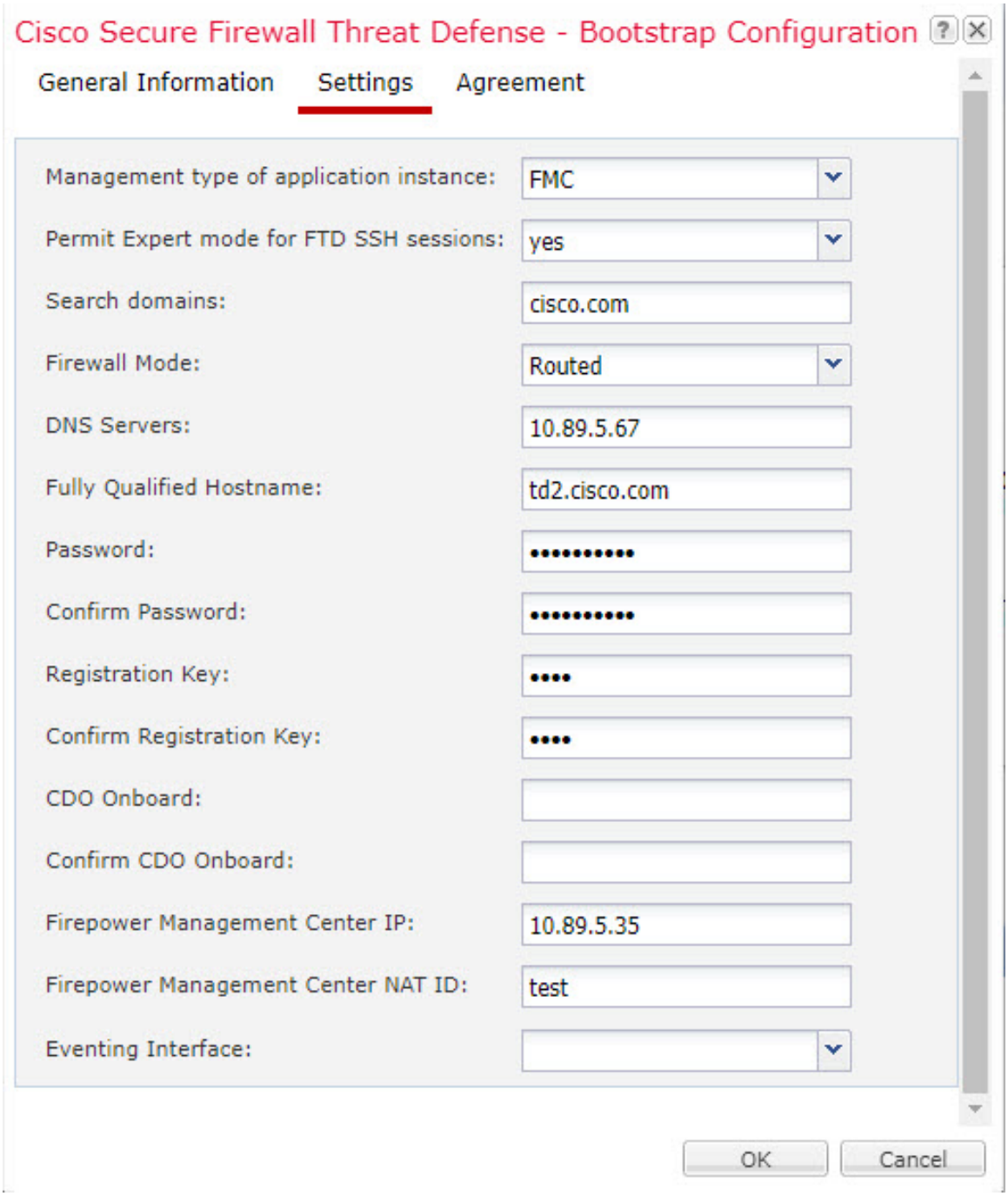
e) 配置**管理 IP** 地址。

设置用于此接口的唯一 IP 地址。

f) 输入**网络掩码**或**前缀长度**。

g) 输入**网络网关**地址。

步骤 6 在**设置**选项卡上，完成下列操作：



a) 对于本地实例，在**应用实例的管理类型**下拉列表中，选择 **FMC**。

本地实例还支持 设备管理器 作为管理器。部署逻辑设备后，无法更改管理器类型。

b) 输入管理 管理中心 的 **Firepower 管理中心 IP**。如果您不知道 管理中心 IP 地址，请将此字段留空，并在 **Firepower 管理中心 NAT ID (Firepower Management Center NAT ID)** 字段中输入口令。

c) 对于容器实例，选择**是否允许 FTD SSH 会话专家模式 (Permit Expert mode from FTD SSH sessions)：是 (Yes)** 或**否 (No)**。专家模式提供 威胁防御 shell 访问权限以确保实现高级故障排除。

对于此选项，如果您选择**是 (Yes)**，拥有直接从 SSH 会话访问容器实例的权限的用户可以输入专家模式。如果您选择**否 (No)**，只有拥有从 FXOS CLI 访问容器实例的权限的用户可以输入专家模式。我们建议选择**否 (No)** 以加强实例之间的隔离。

仅当书面程序指出必须使用或思科技术支持中心要求使用专家模式时，才使用专家模式。要进入此模式下，请在 威胁防御 CLI 中使用 **expert** 命令。

d) 输入逗号分隔列表形式的**搜索域**。

e) 选择**防火墙模式：透明**或**路由式**。

在路由模式中，威胁防御被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。另一方面，透明防火墙是一个第 2 层防火墙，充当“线缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。

系统仅在初始部署时设置防火墙模式。如果您重新应用引导程序设置，则不会使用此设置。

f) 输入逗号分隔列表形式的 **DNS 服务器**。

例如，如果指定 管理中心 主机名，则 威胁防御 使用 DNS。

g) 输入 威胁防御 的**完全限定主机名**。

h) 输入注册期间要在管理中心和设备之间共享的**注册密钥**。

可以为此密钥选择介于 1 至 37 个字符之间的任何文本字符串；添加威胁防御时，需要在管理中心上输入相同的密钥。

i) 输入供威胁防御管理员用户用于 CLI 访问的**密码**。

j) 选择应该发送事件的**事件接口**。如果未指定，系统将使用管理接口。

此接口必须定义为 Firepower 事件接口。

k) 对于容器实例，请将**硬件加密**设置为**已启用**或**已禁用**。

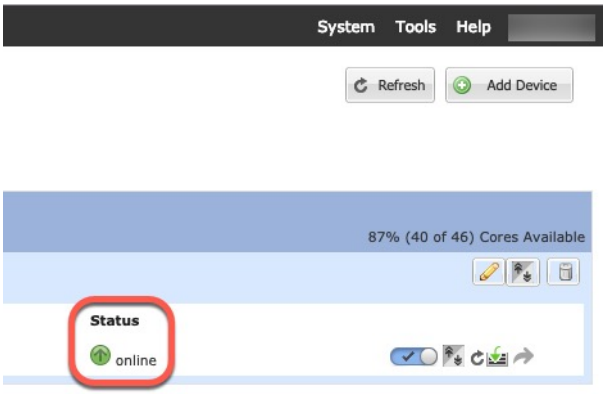
此设置在硬件中启用 TLS 加密加速，并提高某些类型流量的性能。默认情况下启用此功能。您最多可以为每个安全模块的 16 个实例启用 TLS 加密加速。始终为本地实例启用此功能。要查看分配给该实例的硬件加密资源百分比，请输入 **show hw-crypto** 命令。

步骤 7 在**协议**选项卡上，阅读并接受最终用户许可协议 (EULA)。

步骤 8 点击**确定 (OK)** 关闭配置对话框。

步骤 9 点击**保存**。

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。在**逻辑设备 (Logical Devices)** 页面中，查看新逻辑设备的状态。当逻辑设备将其**状态**显示为**在线**时，可以开始在应用中配置安全策略。



步骤 10 进入安全服务模式。

scope ssa

示例：

```
Firepower# scope ssa
Firepower /ssa #
```

步骤 11 接受想要使用的 威胁防御 版本的最终用户许可协议。如果尚未接受此版本的 EULA，则只需执行此步骤即可。

a) 查看可用映像。请注意您想要使用的版本号。

show app

示例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default
 App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
```

b) 将范围设置为映像版本。

scope app ftd *application_version*

示例：

```
Firepower /ssa # scope app ftd 6.2.3
Firepower /ssa/app #
```

c) 接受许可协议。

accept-license-agreement

示例：

```
Firepower /ssa/app # accept-license-agreement

End User License Agreement: End User License Agreement

Effective: May 22, 2017

This is an agreement between You and Cisco Systems, Inc. or its affiliates
("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the
individual or legal entity licensing the Software under this EULA. "Use" or
"Using" means to download, install, activate, access or otherwise use the
Software. "Software" means the Cisco computer programs and any Upgrades made
available to You by an Approved Source and licensed to You by Cisco.
"Documentation" is the Cisco user or technical manuals, training materials,
specifications or other documentation applicable to the Software and made
available to You by an Approved Source. "Approved Source" means (i) Cisco or
(ii) the Cisco authorized reseller, distributor or systems integrator from whom
you acquired the Software. "Entitlement" means the license detail; including
license metric, duration, and quantity provided in a product ID (PID) published
on Cisco's price list, claim certificate or right to use notification.
"Upgrades" means all updates, upgrades, bug fixes, error corrections,
enhancements and other modifications to the Software and backup copies thereof.

[...]

Please "commit-buffer" if you accept the license agreement, otherwise "discard-buffer".

Firepower /ssa/app* #
```

d) 保存配置。

commit-buffer

示例：

```
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app #
```

e) 退出到安全服务模式。

exit

示例：

```
Firepower /ssa/app # exit
Firepower /ssa #
```

步骤 12 设置应用实例映像版本。

a) 将范围设置为安全模块/引擎插槽。

scope slot *slot_id*

对于 Firepower 4100，*slot_id*1、2 或 3。

示例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

b) 创建应用实例。

enter app-instance ftd

示例：

```
Firepower /ssa/slot # enter app-instance ftd
Firepower /ssa/slot/app-instance* #
```

c) 设置 威胁防御 映像版本。

set startup-version *version*

输入您接受 EULA 时在此程序中事先记录的版本号。

示例：

```
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
```

d) 退出到插槽模式。

exit

示例：

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

e) 退出到 ssa 模式。

exit

示例：

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

示例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

步骤 13 创建逻辑设备。

enter logical-device *device_name* **ftd** *slot_id* **standalone**

示例：

```
Firepower /ssa # enter logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* #
```

步骤 14 向逻辑设备分配管理和数据接口。对各个接口重复此步骤。

create external-port-link *name interface_id* **ftd**

set description *description*

exit

- 名称- 由 Firepower 4100/9300 机箱 管理引擎使用；它不是在 威胁防御 配置中使用的接口名称。
- *description* - 在含有空格的短语两侧使用引号 (")。

管理接口与机箱管理端口不同。稍后您需要在管理中心中启用和配置数据接口，包括设置IP地址。

示例：

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 ftd
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 ftd
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 ftd
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

步骤 15 配置管理引导程序参数。

这些设置仅用于仅初始部署或灾难恢复。为了实现正常运行，稍后可以更改应用 CLI 配置中的大多数值。

a) 创建引导程序对象。

create mgmt-bootstrap ftd

示例：

```
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) 指定管理 管理中心的 IP 地址或主机名：

设置以下其中一项：

- **enter bootstrap-key FIREPOWER_MANAGER_IP**

  set value *IP_address*

  exit

- **enter bootstrap-key FQDN**

  set value *fmc_hostname*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.10.10.7
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) 指定防火墙模式：路由或透明。

create bootstrap-key FIREWALL_MODE

set value {**routed** |**transparent**}

exit

在路由模式中，设备被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。另一方面，透明防火墙是一个第2层防火墙，充当“线缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。

系统仅在初始部署时设置防火墙模式。如果您重新应用引导程序设置，则不会使用此设置。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) 指定设备和 管理中心之间要共享的密钥。可以为此密钥选择介于 1 至 37 个字符之间的任何密码；添加 威胁防御 时，需要在 管理中心 上输入相同的密钥。

create bootstrap-key-secret REGISTRATION_KEY

set value

输入值：*registration_key*

确认值：*registration_key*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret
REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: gratuitousapples
Confirm the value: gratuitousapples
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

e) 指定管理员密码。此密码供管理员用户用于 CLI 访问。

create bootstrap-key-secret PASSWORD

set value

输入值： 密码

确认值： 密码

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

f) 指定完全限定主机名。

create bootstrap-key FQDN

set value *fqdn*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value ftd1.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

g) 指定 DNS 服务器列表（用逗号隔开）。

create bootstrap-key DNS_SERVERS

set value *dns_servers*

exit

例如，如果指定 管理中心 主机名，则 威胁防御 使用 DNS。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.9.8.7,10.9.6.5
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

h) 指定搜索域列表（用逗号隔开）。

create bootstrap-key SEARCH_DOMAINS

set value *search_domains*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
cisco.com,example.com
```

```
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

i) 配置 IPv4 管理接口设置。

create ipv4 *slot_id* **firepower**

set ip *ip_address* **mask** *network_mask*

set gateway *gateway_address*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask
255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

j) 配置 IPv6 管理接口设置。

create ipv6 *slot_id* **firepower**

set ip *ip_address* **prefix-length** *prefix*

set gateway *gateway_address*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

k) 退出管理引导程序模式。

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

步骤 16 保存配置。

commit-buffer

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。使用 **show app-instance** 命令检查部署状态。当**管理状态**为**已启用**且**运行状态**为**在线**时，应用实例正在运行且可供使用。

示例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 ----------- ------------ --------------- ------------
asa        asa1       2          Disabled    Not Installed                    9.12.1
    Native                   Not Applicable  None
ftd        ftd1       1          Enabled     Online           6.4.0.49        6.4.0.49
    Container   Default-Small Not Applicable  None
```

步骤 17 请参阅 管理中心 配置指南，将 威胁防御 添加为受管设备，并开始配置安全策略。

示例

```
Firepower# scope ssa
Firepower /ssa* # scope app ftd 6.3.0
Firepower /ssa/app* # accept-license-agreement
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app # exit
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 ftd 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 ftd
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 ftd
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 ftd
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.0.0.100
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: juniorwindowpane
Confirm the value: juniorwindowpane
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
```

```
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value ftd.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 192.168.1.1
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value search.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

添加高可用性对

威胁防御 高可用性（也称为故障转移）是在应用中配置，而不是在 FXOS 中配置。但为了让您的机箱做好配置高可用性的准备，请参阅以下步骤。

开始之前

请参阅高可用性的要求和前提条件，第 419 页。

过程

步骤 1 将相同的接口分配给各个逻辑设备。

步骤 2 为故障转移和状态链路分配 1 个或 2 个数据接口。

这些接口用于交换 2 个机箱之间的高可用性流量。我们建议您将一个 10 GB 数据接口用于组合的故障转移和状态链路。如果您有可用的接口，可以使用单独的故障转移和状态链路；状态链路需要的带宽最多。不能将管理类型的接口用于故障转移或状态链路。我们建议您在机箱之间使用一个交换机，并且不将同一网段中的其他任何设备作为故障转移接口。

对于容器实例，故障转移链路不支持数据共享接口。我们建议您在父接口或 EtherChannel 上创建子接口，并为每个实例分配子接口以用作故障转移链路。请注意，您必须将同一父接口上的所有子接口用作故障转移链路。不得将一个子接口用作故障转移链路，然后将其他子接口（或父接口）用作常规数据接口。

步骤 3 在逻辑设备上启用高可用性。请参阅高可用性，第 455 页。

步骤 4 如果您在启用高可用性后需要更改接口，请先在备用设备上执行更改，然后再在主用设备上执行更改。

更改威胁防御逻辑设备上的接口

可以在 威胁防御 逻辑设备上分配或取消分配接口，或者替换管理接口。然后，您可以在 管理中心 中同步接口配置。

添加新接口或删除未使用接口对 威胁防御配置的影响最小。但是，删除安全策略中使用的接口会影响配置。可以直接在 威胁防御 配置中的很多位置引用接口，包括访问规则、NAT、SSL、身份规则、VPN、DHCP 服务器等。引用安全区的策略不受影响。还可以编辑已分配的 EtherChannel 的成员关系，而不影响逻辑设备或要求在管理中心上进行同步。

删除接口将删除与该接口相关的任何配置。

开始之前

- 根据配置物理接口，第 423 页和添加 EtherChannel（端口通道），第 426 页配置您的接口，并添加任何 EtherChannel。
- 如果您要将已分配的接口添加到 EtherChannel（例如，默认情况下将所有接口分配给集群），则需要先从逻辑设备取消分配接口，然后再将该接口添加到 EtherChannel。对于新的 EtherChannel，您可以随后将 EtherChannel 分配到设备。
- 如果要将管理或事件接口替换为管理 EtherChannel，则需要创建至少具有 1 个取消分配数据成员接口的 EtherChannel，然后将当前管理接口替换为 EtherChannel。威胁防御 重新启动（管理接口更改导致重新启动），并且在 管理中心中同步配置后，还可以将（目前取消分配的）管理接口添加到 EtherChannel。
- 如果要替换管理或事件接口，则必须使用 机箱管理器；CLI 不支持此更改。
- 对于集群或高可用性，请确保在所有设备上添加或删除该接口，然后在管理中心 中同步配置。我们建议先在数据/备用设备上更改接口，然后再在控制/主用设备上更改接口。请注意，新的接口在管理权限关闭的状态下添加，因此，它们不会影响接口监控。

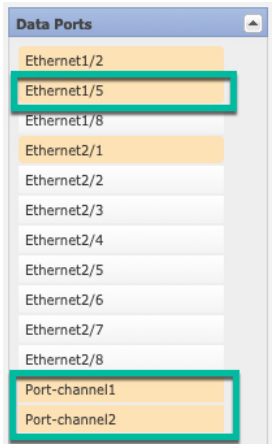
过程

步骤 1 在 机箱管理器中，选择**逻辑设备**。

步骤 2 点击右上角的**编辑**图标以编辑逻辑设备。

步骤 3 通过在**数据端口**区域中选择新的数据接口来分配该接口。

请勿删除任何接口。



步骤 4 替换管理或事件接口：

对于这些类型的接口，在您保存更改后，设备会重新启动。

a) 点击页面中心的设备图标。
b) 在**常规**或**集群信息**选项卡上，从下拉列表中选择新的**管理接口**。
c) 在**设置**选项卡上，从下拉列表中选择新的**事件接口**。
d) 点击**确定**。

如果更改管理接口的 IP 地址，则还必须更改 管理中心中设备的 IP 地址：转到**设备** > **设备管理** > **设备/集群**。在**管理**区域中，设置 IP 地址以匹配引导程序配置地址。

步骤 5 点击**保存 (Save)**。

步骤 6 进入安全服务模式：

Firepower# **scope ssa**

步骤 7 编辑逻辑设备：

Firepower /ssa # **scope logical-device** *device_name*

步骤 8 将新的接口分配到逻辑设备：

Firepower /ssa/logical-device* # **create external-port-link** *name interface_id* **ftd**

请勿删除任何接口。

步骤 9 提交配置：

commit-buffer

提交系统配置任务。

步骤 10 同步 管理中心 中的接口。

a) 登录至管理中心。
b) 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（ ）。系统默认选择**接口 (Interfaces)** 页面。
c) 点击**接口 (Interfaces)** 页面左上方的**同步设备 (Sync Device)** 按钮。
d) 检测到更改后，可以在**接口 (Interfaces)** 页面上看到红色横幅，表明接口配置已发生更改。点击**点击了解详情**链接以查看接口更改。
e) 如果计划删除接口，请手动将任何接口配置从旧接口传输至新接口。

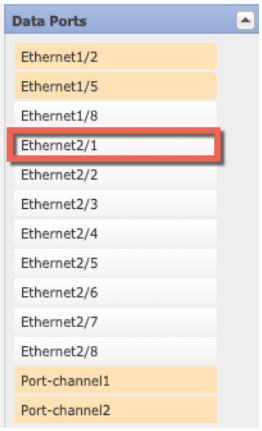
由于尚未删除任何接口，因此可以引用现有配置。在删除旧接口并重新运行验证后，将有额外的机会来修复配置。验证将显示仍在使用旧接口的所有位置。

f) 点击**验证更改 (Validate Changes)** 以确保策略在接口更改后仍有效。

如出现任何错误，则需要更改配置并重新运行验证。

g) 点击**保存 (Save)**。
h) 依次点击**部署** > **部署**。
i) 选择设备然后点击**部署**，以将策略部署到所分配的设备。在部署更改之后，更改才生效。

步骤 11 在 机箱管理器 中，通过在**数据端口 (Data Ports)** 区域中取消选择数据接口来取消分配该接口。



步骤 12 点击**保存**。

步骤 13 在 FXOS 中，从逻辑设备取消分配接口：

Firepower /ssa/logical-device # **delete external-port-link** *name*

输入 **show external-port-link** 命令以查看接口名称。

步骤 14 提交配置：

commit-buffer

提交系统配置任务。

步骤 15 再次在 管理中心 中同步接口。

连接到应用控制台

使用以下程序连接至应用的控制台。

过程

步骤 1 使用控制台连接或 Telnet 连接来连接至模块 CLI。

connect module *slot_number* {**console** | **telnet**}

要连接至不支持多个安全模块的设备的安全引擎，请使用 **1** 作为 *slot_number*。

使用 Telnet 连接的优点在于，您可以同时对模块开展多个会话，并且连接速度更快。

示例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
```

```
CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

步骤 2 连接到应用控制台。

connect ftd *name*

要查看实例名称，请输入不含名称的命令。

示例：

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

步骤 3 退出应用控制台到 FXOS 模块 CLI。

- 威胁防御 - 输入 **exit**

步骤 4 返回 FXOS CLI 的管理引擎层。

退出控制台：

a) 输入 **~**

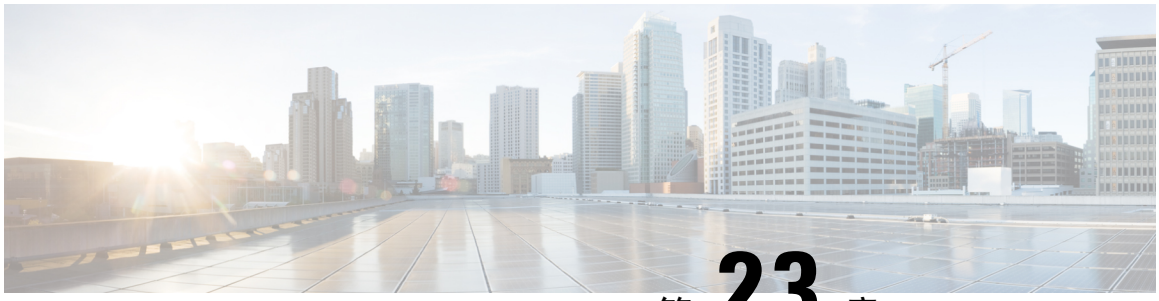
您将退出至 Telnet 应用。

b) 要退出 Telnet 应用，请输入：

telnet>**quit**

退出 Telnet 会话：

a) 输入 **Ctrl-],**。



第 23 章

高可用性

以下主题介绍如何配置主用/备用设备故障转移，以实现 威胁防御 的高可用性。

关于 Cisco Secure Firewall Threat Defense高可用性

配置高可用性需要两台相同的 威胁防御设备，二者之间通过专用故障切换链路和（可选）状态链路彼此互连。威胁防御支持主用/备用故障切换，其中一台设备为传递流量的主用设备。备用设备不会主动传递流量，但会使配置和其他状态信息与主用设备同步。发生故障切换时，主用设备会故障切换到备用设备，后者随即变为主用状态。

系统会对主用设备的运行状况（硬件、接口、软件以及环境状态）进行监控，以便确定是否符合特定的故障切换条件。如果符合这些条件，将执行故障切换。

注释 在公共云中运行的 threat defense virtual不支持高可用性。

远程分支机构部署中 威胁防御 设备上的高可用性支持

在远程分支机构部署中，威胁防御 设备的数据接口会被用于管理 思科防御协调器，而不是设备上的管理接口。由于大多数远程分支机构都只有一个互联网连接，因此外部CDO访问让集中管理成为了可能。

您可以将任何数据接口用于 CDO 访问，例如，如果您有内部 CDO，则使用内部接口。但是，本指南主要介绍外部接口访问，因为它是远程分支机构最可能遇到的场景。

CDO 可在其通过数据接口管理的 威胁防御 设备上提供高可用性支持。运行 7.2 或更高版本软件的设备支持此功能。

有关详细信息，请参阅《思科 Firepower 入门指南》中的使用远程 *FMC* 部署 *Firepower* 威胁防御。

高可用性系统要求

本部分介绍在高可用性配置中对于威胁防御 设备的硬件、软件和许可证要求。

硬件要求

高可用性配置中的两台设备必须：

- 型号相同。 此外，对于容器实例，它们必须使用相同的资源配置文件属性。

  对于 Firepower 9300，高可用性仅在同种类型模块之间受支持；但是两个机箱可以包含混合模块。例如，每个机箱都设有 SM-56、SM-48 和 SM-40。可以在 SM-56 模块之间、SM-48 模块之间和 SM-40 模块之间创建高可用性对。

  如果在将高可用性对添加到 CDO 后更改资源配置文件，则稍后应在**设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **系统 (System)** > **清单 (Inventory)**对话框中更新每个设备的清单。

- 拥有相同数量和类型的接口。

  对于平台模式下的Firepower 4100/9300 机箱，在启用之前，所有接口都必须在 FXOS 中进行相同的预配置。高可用性如果您在启用高可用性后更改接口，请在备用设备上的 FXOS 中更改接口，然后在主用设备上进行相同更改。

- 在远程分支机构部署中包含以下设置：
  - 具有处理远程部署中管理流量的相同数据管理接口。

    例如，如果您在设备 1 中使用的是 eth0，也要在设备 2 中使用相同的接口，即还是 eth0。

  - 将数据管理接口用于管理通信。

    不能让一台设备使用数据接口进行管理，而另一台设备却使用管理接口进行管理。

如果在高可用性配置中使用闪存大小不同的设备，请确保闪存较小的设备具有足够的空间来容纳软件映像文件和配置文件。如果闪存较小的设备没有足够的空间，从闪存较大的设备向闪存较小的设备进行配置同步将会失败。

软件要求

高可用性 配置中的两台设备必须：

- 处于相同的防火墙模式（路由或透明）。

- 具有相同的软件版本。
- 位于管理中心上的同一个域或组中。
- 具有相同的 NTP 配置。请参阅为威胁防御配置 NTP 时间同步。
- 在管理中心上完全部署且没有未提交的更改。
- 在其任一接口中都未配置 DHCP 或 PPPoE。
- （Firepower 4100/9300）具有相同的流量分流模式，同时启用或禁用。

高可用性对中 威胁防御 设备的许可证要求

高可用性配置中的两台 威胁防御 设备必须具有相同的许可证。

高可用性配置需要两种许可证权利；对中的每个设备各一个。

在建立高可用性之前，将哪些许可证分配给辅助/备用设备并不重要。进行高可用性配置期间，管理中心 会释放分配给备用设备的所有不必要的许可证，并用分配给主/主用设备的相同许可证替换它们。例如，如果主用设备具有 基本 许可证和 威胁 许可证，而备用设备只有 基本 许可证， 管理中心 将与智能软件管理器通信，以从您的备用设备的账户获取可用 威胁 许可证。如果您的许可证帐户不包含足够的购买权利，则您的帐户将在您购买正确数量的许可证之前变得不符合要求。

故障转移和状态故障转移链路

故障切换链路和可选的有状态故障切换链路是两台设备之间的专用连接。思科建议在故障切换链路或状态故障切换链路中的两台设备之间使用同一接口。例如，在故障切换链路中，如果您在设备 1 中使用的是 eth0，也要在设备 2 中使用相同的接口，即还是 eth0。

故障转移链路

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

故障切换链路数据

以下信息将通过故障切换链路传输：

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

故障切换链路接口

您可以使用未使用的数据接口（物理接口 EtherChannel 接口）作为故障切换链路；但不能指定当前已配置名称的接口。 如果接口被配置为与 CDO 通信，则您无法使用数据管理接口。 您也无法使用

子接口，在机箱上定义用于多实例模式的子接口除外。故障转移链路接口不会配置为常规网络接口；该接口仅会因为故障转移而存在。该接口只能用于故障转移链路（还用于状态链路）。

威胁防御用户数据和故障切换链路之间共享接口。您也不能在同一父接口上使用单独的子接口用于故障切换链路和数据（仅限多实例机箱子接口）。如果将机箱子接口用于故障转移链路，则该父接口及其上的所有子接口仅限于用作故障转移链路。

注释 使用 EtherChannel 作为故障链路或状态链路时，必须在建立高可用性之前，确认具有相同成员接口的同一 EtherChannel 在两台设备上都存在。

请参阅下列有关故障切换链路的指南：

- Firepower 4100/9300- 我们建议您将一个 10 GB 数据接口用于组合的故障切换和状态链路。
- 所有其他型号 - 1 GB 接口对于组合的故障切换和状态链路而言已足够大。

交替频率等于设备保持时间。

注释 如果配置较大且设备保持时间较短，则在成员接口之间交替可以防止辅助设备加入/重新加入。这种情况下，请禁用其中一个成员接口，直到辅助设备加入。

对于用作故障切换链路的 EtherChannel，要阻止无序数据包，仅使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。您不能在 EtherChannel 配置用作故障转移链路时对其进行修改。

连接故障切换链路

您可以使用以下两种方法之一连接故障切换链路：

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

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

状态故障转移链路

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

共享故障切换链路

共享故障切换链路是节约接口的最佳方式。但是，如果您有一个大型配置和高流量网络，必须考虑对状态链路和故障转移链路使用专用接口。

状态故障切换链路的专用接口

您可以将专用接口（物理或 EtherChannel）用于状态链路。有关专用状态链路的要求，请参阅故障切换链路接口，第 457 页，以及有关连接状态链路的信息，请参阅连接故障切换链路，第 458 页。

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

避免中断故障转移和数据链路

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

请参阅以下连接情景，以设计具有弹性的故障转移网络。

情景 1 - 不推荐

如果单台交换机或一组交换机用于连接两台 威胁防御设备之间的故障转移和数据接口，则交换机或交换机间链路发生故障时，两台 威胁防御设备都将处于主用状态。因此，建议**不要**使用下图中显示的 2 种连接方法。

图 ***55:*** 使用单交换机连接 - 不推荐

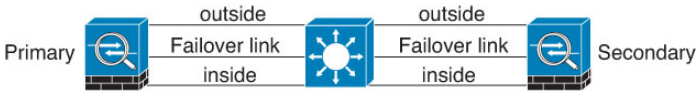
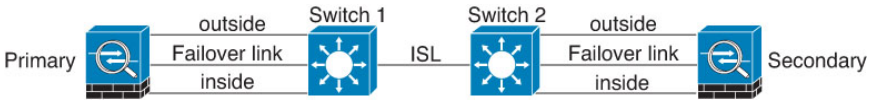


图 ***56:*** 使用双交换机连接 - 不推荐



情景 2 - 推荐

我们建议不要让故障转移链路和数据接口使用相同的交换机，而是应使用不同的交换机或使用直连电缆来连接故障转移链路，如下图所示。

图 ***57:*** 使用其他交换机连接

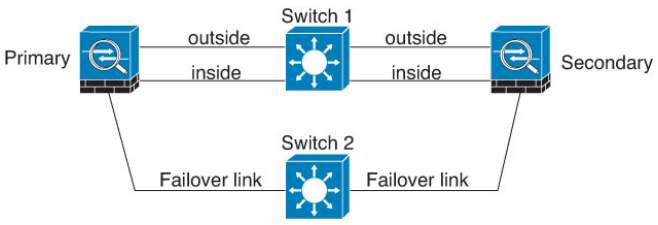
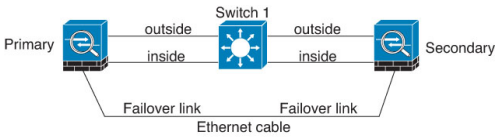


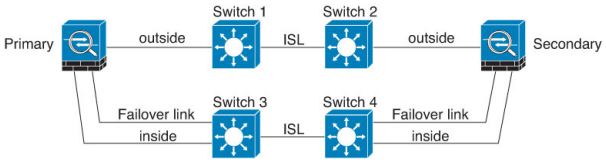
图 *58:* 通过电缆连接



情景 3 - 推荐

如果 威胁防御数据接口连接到多台交换机，则故障转移链路可以连接到其中一台交换机，最好是处于网络的安全一侧（内部）的交换机，如下图所示。

图 *59:* 使用安全交换机连接



情景 4 - 推荐

最可靠的故障转移配置使用故障转移链路上的冗余接口，如下图所示。

图 *60:* 使用冗余接口连接

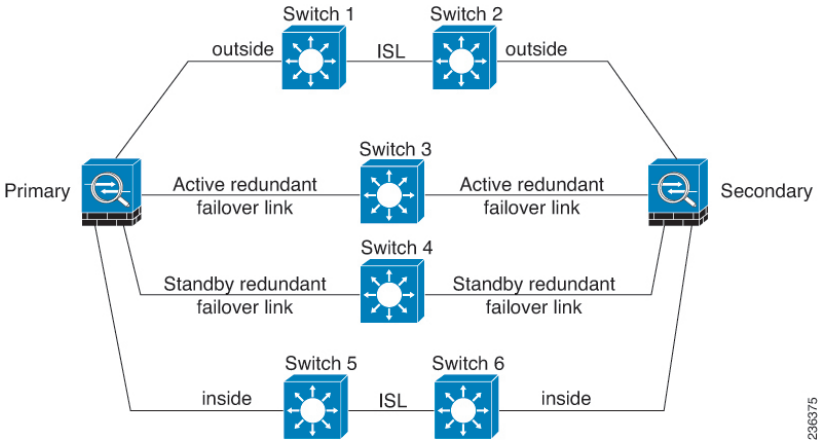
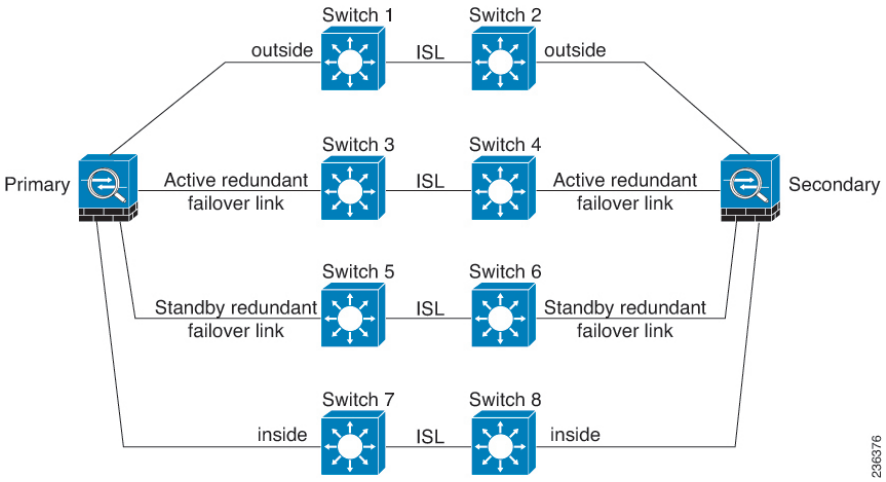


图 *61:* 使用交换机间链路连接



高可用性中的 MAC 地址和 IP 地址

当您配置接口时，可以在相同网络上指定一个主用 IP 地址和一个备用 IP 地址。通常情况下，当发生故障转移时，新的主用设备会接管主用 IP 地址和 MAC 地址。由于网络设备不会发现 MAC 与 IP 地址配对的变化，网络上的任意位置都不会发生 ARP 条目变化或超时。

注释 虽然建议指定备用 IP 地址，但它并不是必需的。如果没有备用 IP 地址，则主用设备无法执行用于检查备用接口运行状态的网络测试；它只能跟踪链路状态。此外，您也无法出于管理目的，连接到该接口上的备用设备。

在发生故障转移时，状态链路的 IP 地址和 MAC 地址不会更改。

主用/备用 IP 地址和 MAC 地址

对于主用/备用高可用性，请参阅下文，了解故障转移事件期间 IP 地址和 MAC 地址的使用情况：

1. 主用设备始终使用主设备的 IP 地址和 MAC 地址。
2. 当主用设备进行故障切换时，备用设备会使用故障设备的 IP 地址和 MAC 地址，并开始传送流量。
3. 当故障设备恢复在线状态时，它现在处于备用状态，并且接管备用 IP 地址和 MAC 地址。

但如果辅助设备启动时未检测到主设备，辅助设备将成为主用设备，并使用其自己的 MAC 地址，因为它不知道主设备的MAC 地址。当主设备变为可用时，辅助（主用）设备会将MAC 地址更改为主设备的 MAC，这可能会导致网络流量中断。同样，如果您用新硬件替换主设备，将使用新 MAC 地址。

使用虚拟MAC 地址可防范这种中断，因为对于启动时的辅助设备，主用MAC 地址是已知的，并在采用新的主设备硬件时保持不变。如果您没有配置虚拟 MAC 地址，则可能需要清除连接的路由器

上的 ARP 表，以便恢复流量。当 MAC 地址发生变化时，威胁防御设备不会发送静态 NAT 地址的免费 ARP，因此连接的路由器不会知道这些地址的 MAC 地址发生变化。

虚拟 MAC 地址

威胁防御设备 有多种方法配置虚拟 MAC 地址。我们建议仅使用一种方法。如果使用多种方法设置 MAC 地址，所使用的 MAC 地址会取决于许多变量，可能会不可预测。

对于多实例功能，FXOS 机箱仅为所有接口自动生成主 MAC 地址。如果同时具有主 MAC 地址和辅助 MAC 地址，则可以使用虚拟 MAC 地址覆盖生成的 MAC 地址，但预定义辅助 MAC 地址并非不可或缺；设置辅助 MAC 地址可确保在使用新的辅助设备硬件的情况下发送到设备的管理流量不会中断。

状态故障切换

状态故障切换期间，主用设备会不断将每个连接的状态信息发送至备用设备。发生故障切换之后，相同的连接信息在新主用设备上可用。支持的最终用户应用不需要通过重新连接来保持同一通信会话。

支持的功能

对于状态故障转移，以下状态信息会传送至备用 威胁防御设备：

- NAT 转换表。
- TCP 和 UDP 连接和状态，包括 HTTP 连接状态。其他类型的 IP 协议和 ICMP 不会通过主用设备解析，因为它们是在新数据包到达时在新的主用设备上建立的。
- Snort 连接状态、检查结果和引脚信息，包括严格 TCP 实施。
- ARP 表
- 第 2 层网桥表（适用于桥接组）
- ISAKMP 和 IPsec SA 表
- GTP PDP 连接数据库
- SIP 信令会话和引脚。
- 静态和动态路由表 - 状态故障转移会参与动态路由协议（如 OSPF 和 EIGRP），因此通过主用设备上的动态路由协议获悉的路由，将会保留在备用设备的路由信息库 (RIB) 表中。发生故障转移事件时，数据包可以正常传输，并且只会对流量产生极小的影响，因为主用辅助设备一开始就具有镜像主设备的规则。进行故障转移后，新的主用设备上的重新融合计时器会立即启动。随后 RIB 表中的代编号将会增加。在重新融合期间，OSPF 和 EIGRP 路由将使用新的代编号进行更新。计时器到期后，过时的路由条目（由代编号确定）将从表中删除。于是 RIB 将包含新主用设备上的最新的路由协议转发信息。

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

- DHCP 服务器 - 不会复制 DHCP 地址租用。但是，在接口上配置的 DHCP 服务器将发送 ping 命令，以确保在向 DHCP 客户端授予地址前不使用地址，使得服务不会受到影响。对于 DHCP 中继代理或 DDNS，状态信息不相关。
- 访问控制策略决策 - 在故障转移期间，会保留与流量匹配（包括 URL、URL 类别、地理位置等）、入侵检测、恶意软件和文件类型相关的决策。但是，对于在故障转移时评估的连接，有以下注意事项：
  - AVC - 系统会复制 App-ID 裁定，而不是检测状态。只要 App-ID 裁定是完整的，并且在发生故障转移之前完成同步，即可实现正确的同步。
  - 入侵检测状态 - 进行故障转移时，一旦出现拾取中间流的情况，新检测既已完成，但旧状态会丢失。
  - 文件恶意软件阻止 - 文件处置必须在故障转移之前变为可用。
  - 文件类型检测和阻止 - 文件类型必须在故障转移之前加以识别。如果在原始主用设备识别文件时发生故障转移，则文件类型不同步。即使文件策略阻止该文件类型，新的主用设备也会下载该文件。
- 身份策略中的用户身份决策，包括通过 ISE 会话目录被动收集的用户到 IP 地址映射以及通过强制网络门户进行的主动身份验证。发生故障转移时进行主动身份验证的用户，可能会被提示再次进行身份验证。
- 网络 AMP - 云查找独立于每台设备，因此故障转移通常不会影响此功能。具体包括：
  - 签名查找 - 如果在文件传输过程中发生故障转移，则不生成文件事件，也不进行检测。
  - 文件存储 - 如果在存储文件时发生故障转移，则文件将存储在原始主用设备上。如果在存储文件时原始主用设备关闭，则不存储文件。
  - 文件预分类（本地分析）- 如果在预分类期间发生故障转移，则检测失败。
  - 文件动态分析（连接至云）- 如果发生故障转移，则系统可能会将文件提交至云。
  - 存档文件支持 - 如果在分析期间发生故障转移，则系统可能会丢失对文件/存档的可视性。
  - 自定义阻止操作 - 如果发生故障转移，系统将不生成事件。
- 安全智能决策。但是，不会完成故障转移过程中发生的基于 DNS 的决策。
- RA VPN - 故障转移后，远程访问 VPN 终端用户不必对 VPN 会话重新进行身份验证，也不必重新连接。但是，在VPN连接上运行的应用，在故障转移过程中可能会丢失数据包，并且无法从数据包丢失中恢复。
- 在所有连接中，只有已建立的连接会复制到备用 ASA 上。

不支持的功能

对于状态故障转移，以下状态信息不会传送至备用 威胁防御设备：

- 明文隧道（例如 GRE 或 IP-in-IP）中的会话。不会复制隧道内部的会话，并且新的主动节点不能重复使用现有检测判定来匹配正确的策略规则。
- 已解密的 TLS/SSL 连接 - 解密状态不同步，如果主用设备发生故障，则系统会重置已解密的连接。需要与新的主用设备建立新连接。未解密的连接（也就是匹配TLS/SSL“不解密”规则操作的连接）不受影响，并且可以正确复制。
- TCP 状态绕行连接
- 组播路由。

高可用性的桥接组要求

使用网桥组时，高可用性存在特殊的注意事项。

当主用设备故障切换到备用设备时，运行生成树协议 (STP) 的交换机端口在感知到拓扑变化时，系统会进入阻塞状态30秒至50秒。当端口处于阻塞状态时，为避免桥接组成员接口上出现流量丢失，您可以配置以下任一变通方案：

- 交换机端口处于接入模式 - 在交换机上启用 STP PortFast 功能：

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

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

- 如果交换机端口处于中继模式，或无法启用STP PortFast，则您可以使用以下一种会影响故障切换功能或 STP 稳定性的不太理想的变通方案：
  - 对桥接组和成员接口禁用接口监控。
  - 将故障切换条件中的接口保持时间增加到较高的值，以使 STP 在设备进行故障切换之前融合。
  - 减小交换机上的 STP 计时器，以使 STP 比接口保持时间更快地融合。

故障切换运行状态监控

威胁防御 设备会监控每台设备的整体运行状态和接口运行状态。此部分包括有关 威胁防御 设备如何执行测试以确定每台设备状态的信息。

设备运行状况监控

威胁防御 设备会通过 Hello 消息监控故障切换链路，进而确定其他设备的运行状况。当设备在故障切换链路上没有收到三条连续的 Hello 消息时，设备将在每个数据接口（包括故障切换链路）上发送接口 LANTEST 消息，来验证对等体是否响应。威胁防御 设备采取的操作取决于来自其他设备的响应。请参阅以下可以执行的操作：

- 如果 威胁防御 设备在故障切换链路上收到响应，则不会进行故障切换。
- 如果威胁防御设备在故障切换链路上未收到响应，但在数据接口上收到响应，则设备不会进行故障切换。故障转移链路会标记为发生故障。您应尽快恢复故障转移链路，因为当故障转移切换发生故障时，设备无法故障转移到备用设备。
- 如果威胁防御设备未在任何接口上收到响应，则备用设备会切换至主用模式，并会将另一台设备分类为故障设备。

接口监控

当设备在 15 个秒，未在受监控的接口上收到 hello 消息时，将运行接口测试。如果对于某个接口，其中一个接口测试失败，但在另一设备上的此接口继续成功传送流量，则此接口会被视为发生故障，设备停止运行测试。

如果满足为故障接口数量定义的阈值（请参阅命令，或者对于主用/主用故障切换，请使用命令）（请参阅配置设备管理高可用性和可扩展性故障切换标准接口策略）（请参阅设备设备管理高可用性故障切换）触发条件（Trigger Criteria）），并且主用设备的故障接口比备用设备多，则发生故障切换。> > > 如果某个接口在两个单元上都失败，则这两个接口会进入“Unknown”状态，并且不会计入由故障切换接口政策制定的故障切换限制。

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

如果接口上配置了 IPv4 和 IPv6 地址， 设备会使用 IPv4 地址执行运行状况监控。如果接口上仅配置了 IPv6 地址，则 设备会使用 IPv6 邻居发现，而不是 ARP 来执行运行状况监控测试。对于广播 Ping 测试， 设备会使用所有的 IPv6 节点地址 (FE02::1)。

接口测试

威胁防御 设备使用以下接口测试。默认情况下，每个测试的持续时间约为1.5秒。

1. 链路打开/关闭测试 - 一种接口状态测试。如果链路打开/关闭测试指示接口关闭，则 设备视为测试失败，然后测试停止。如果状态为打开，则 设备执行 Network Activity 测试。
2. 网络活动测试 - 接收的网络活动测试。测试开始时，每台设备会清除其接口收到的数据包计数。在测试期间，一旦设备收到符合条件的数据包，则接口会被视为正常运行。如果两台设备都收到流量，则测试会停止。如果一台设备收到测试流量，另一设备未收到，则未收到流量的设备会被视为已发生故障。如果两台设备均收到了流量，则 设备开始进行 ARP 测试。
3. ARP 测试 - 用于测试成功的 ARP 回复。每台设备都向其 ARP 表中最新条目中的 IP 地址发送一个 ARP 请求。如果设备在测试期间收到 ARP 回复或其他网络流量，则认为该接口运行正常。如果设备未收到 ARP 回复，则 设备会向 ARP 表中的下一个条目中的 IP 地址发送一次 ARP 请求。

如果设备在测试期间收到 ARP 回复或其他网络流量，则认为该接口运行正常。如果两台设备都收到流量，则测试会停止。如果一台设备收到测试流量，另一设备未收到，则未收到流量的设备会被视为已发生故障。如果两台设备均收到了流量，则 设备开始进行广播 Ping 测试。

4. 广播 Ping 测试 - 测试成功的 Ping 回复。每台设备发送一个广播 Ping，然后对收到的所有数据包进行计数。在测试期间，当设备收到任何数据包，则接口会被视为正常运行。如果两台设备都收到流量，则测试会停止。如果一台设备收到测试流量，另一设备未收到，则未收到流量的设备会被视为已发生故障。如果未收到任何流量，则测试将通过 ARP 测试再次开始。如果两台设备继续没有收到来自 ARP 和广播 Ping 测试的流量，则测试将会一直运行下去。

接口状态

受监控接口可以具有以下状态：

- Unknown - 初始状态。此状态也可能意味着状态无法确定。
- Normal - 接口正在接收流量。
- Normal (Waiting) - 接口已打开，但尚未从对等体设备上的对应接口接收欢迎数据包。
- Normal (Not-Monitored) - 接口已打开，但未受故障切换进程监控。
- Testing - 接口上有 5 个轮询时间未收听到 Hello 消息。
- Link Down - 接口或 VLAN 通过管理方式关闭。
- Link Down (Waiting) - 接口或 VLAN 已通过管理方式关闭，并且尚未从对等体设备上的对应接口接收欢迎数据包。
- Link Down (Not-Monitored) - 接口或 VLAN 已通过管理方式关闭，但未受故障切换进程监控。
- No Link - 接口的物理链路关闭。
- No Link (Waiting) - 接口的物理链路已关闭，并且尚未从对等体设备上的对应接口接收欢迎数据包。
- No Link (Not-Monitored) - 接口的物理链路已关闭，但未受故障切换进程监控。
- Failed - 在接口上没有收到流量，但在对等体接口上收听到流量。

故障切换触发器和检测时间

以下事件会在 Firepower 高可用性对中触发故障切换：

- 主用设备上超过 50% 的 Snort 实例已关闭。
- 主用设备上使用的磁盘空间已超过 90%。
- 主用设备上运行的是 **no failover active** 命令，而备用设备上运行的是 **failover active** 命令。
- 主用设备的故障接口比备用设备更多。
- 主用设备上的接口故障超过配置的阈值。

默认情况下，单个接口发生故障会导致故障转换。您可以通过配置接口数量的阈值或为发生故障切换而必须发生故障的受监控接口的百分比来更改默认值。如果在主用设备上达到阈值，则会发生故障切换。如果备用设备上的阈值超出阈值，则设备将进入“**故障**”状态。

要更改默认故障转移条件，在全局配置模式下输入以下命令：

表 *54:*

命令	目的
failover interface-policy num [%] `hostname (config)# failover interface-policy 20%`	更改默认故障切换条件。 指定特定接口数时，*num* 参数可以介于 1 和 250 之间。 指定接口百分比时，*num* 参数可以介于 1 和 100 之间。

下表列出了故障切换触发事件及关联的故障检测时间。如果出现故障切换，您可以在消息中心中查看故障切换的原因，以及有关高可用性对的各种操作。您可以将这些阈值配置为指定的最小-最大范围内的值。

表 *55:* 威胁防御故障切换时间

故障切换触发事件	最小	默认	最大
主用设备断电，硬件关闭或软件重新加载或崩溃。当出现这些情况时，受监控接口或故障切换链路不会收到任何 Hello 消息。	800 毫秒	15 秒	45 秒
主用设备接口物理链路发生故障。	500 毫秒	5 秒	15 秒
主用设备接口正常运行，但是连接问题导致接口测试。	5 秒	25 秒	75 秒

关于主用/备用故障转移

主用/备用故障转移允许您使用备用 威胁防御设备来接管故障设备的功能。当主用设备发生故障时，备用设备将变为主用设备。

主/辅助角色和主用/备用状态

当设置主用/备用故障转移时，需要将一台设备配置为主设备，将另一台配置为辅助设备。配置过程中，主设备的策略将同步到辅助设备。此时，两台设备将作为单台设备进行设备和策略配置。但对于事件、控制面板、报告和运行状况监控，它们仍显示为单独的设备。

在故障转移对中这两台设备之间的主要区别是哪台是主用设备，哪台是备用设备，即要使用哪些 IP 地址以及哪台设备积极传递流量。

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

- 如果两台设备同一时间启动（并且运行状况相同），则主设备总是会成为主用设备。
- 主设备 MAC 地址始终与主用 IP 地址相匹配。此规则的例外是，当辅助设备成为主用设备并且无法通过故障转移链路获取主设备 MAC 时。在这种情况下，会使用辅助设备的 MAC 地址。

启动时的主用设备确定

主用设备按以下方式确定：

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

故障转移事件

在主用/备用故障转移中，故障转移会在设备级别进行。

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

表 *56:* 故障转移事件

故障事件	策略	主用设备操作	备用设备操作	说明
主用设备发生故障（电源或硬件）	故障转移	不适用	成为主用设备 将主用设备标记为发生故障	在任何受监控接口或故障转移链路上，均未收到 Hello 消息。
以前的主用设备恢复	禁用故障转移	成为备用设备	无需操作	无。
备用设备发生故障（电源或硬件）	禁用故障转移	将备用设备标记为发生故障	不适用	备用设备被标记为发生故障后，主用设备不会尝试进行故障切换，即使超过接口故障阈值也是如此。
故障转移链路在运行过程中发生故障	禁用故障转移	将故障转移链路标记为发生故障	将故障转移链路标记为发生故障	您应尽快恢复故障转移链路，因为当故障转移链路发生故障时，设备无法故障转移到备用设备。
故障转移链路在启动时发生故障	禁用故障转移	成为主用设备 将故障转移链路标记为发生故障	成为主用设备 将故障转移链路标记为发生故障	如果故障转移链路在启动时发生故障，则两台设备都会成为主用设备。

故障事件	策略	主用设备操作	备用设备操作	说明
状态链路发生故障	禁用故障转移	无需操作	无需操作	如果发生故障转移，状态信息会过时，而且会话会被终止。
主用设备上的接口故障超过阈值	故障转移	将主用设备标记为发生故障	成为主用设备	无。
备用设备上的接口故障超过阈值	禁用故障转移	无需操作	将备用设备标记为发生故障	备用设备被标记为发生故障后，主用设备不会尝试进行故障切换，即使超过接口故障阈值也是如此。

高可用性的要求和前提条件

型号支持

Cisco Secure Firewall Threat Defense

支持的域

任意

用户角色

管理员

高可用性指南

型号支持

- Firepower 1010：
  - 使用高可用性时，不应使用交换机端口功能。由于交换机端口在硬件中运行，因此会继续在主用设备 和备用设备上传输流量。高可用性旨在防止流量通过备用设备，但此功能不会扩展至交换机端口。在正常 高可用性网络设置中，两台设备上的活动交换机端口将导致网络环路。建议将外部交换机用于任何交换功能。请注意，VLAN接口可通过故障转移监控，而交换机端口无法通过故障转移监控。理论上，您可以将单个交换机端口置于 VLAN 上并成功使用 高可用性，但更简单的设置是改用物理防火墙接口。
  - 仅可使用防火墙接口作为故障转移链路。

注释 在 6.5 或更高版本由 管理中心 6.5 或更高版本新安装和管理的 Firepower 1010 设备上，默认接口将为交换机端口类型。由于故障切换不支持交换机端口功能，请关闭这些接口上的交换机端口，执行部署，然后创建故障切换。对于从 6.5 之前的版本升级的 Firepower 1010 系统，默认接口将与之前版本中的相同。

- Firepower 9300 - 不支持机箱内高可用性。
- 由于需要第 2 层的连接，因此不支持高可用性在公共云网络（如 Microsoft Azure 和 Amazon Web 服务）上使用 threat defense virtual。

其他规定

- 当主用设备故障切换到备用设备时，所连接的运行生成树协议 (STP) 的交换机端口在感知到拓扑变化时，会进入阻塞状态 30 秒至 50 秒。当端口处于阻塞状态时，为避免流量丢失，您可以根据交换机启用 STP PortFast 功能：

  interface *interface_id* **spanning-tree portfast**

  此解决方法适用于连接到路由模式和桥接组接口的交换机。链路打开时，PortFast 功能会立即使端口转换到 STP 转发模式。该端口仍会参与 STP。因此，如果端口是环路的一部分，则端口最终会转换为 STP 阻塞模式。

- 发生故障切换事件时，在连接到 威胁防御设备故障切换对的交换机上配置端口安全性，可能会导致通信问题。一个安全端口上配置或获悉的安全 MAC 地址移至另一安全端口，交换机端口安全功能标记违例时，会发生此问题。
- 对于主用/备用 高可用性和 VPN IPSec 隧道，无法使用 SNMP 通过 VPN 隧道监控主用设备和备用设备。备用设备没有有效的 VPN 隧道，将丢弃发往 NMS 的流量。您可以改为使用具有加密功能的 SNMPv3，因此不需要 IPsec 隧道。
- 两个对等设备都进入未知状态，如果在创建高可用性对时在任何对等设备中运行 clish，高可用性配置会失败。
- 故障切换后，系统日志消息的源地址将立即成为故障切换接口地址几秒钟。
- 为了更好地融合（在故障切换期间），您必须关闭 HA 对上未与任何配置或实例关联的接口。
- 如果您在评估模式下配置 HA 故障转移加密，系统将使用 DES 进行加密。如果随后您使用出口合规账户注册设备，则设备将在重新启动后使用 AES。因此，如果系统出于任何原因重新启动，包括安装升级后，对等体将无法通信，两台设备将变为主用设备。建议您在注册设备之前不要配置加密。如果您在评估模式下进行此配置，建议您在注册设备之前删除加密。
- 当使用具有故障切换功能的 SNMPv3 时，如果更换故障切换设备，则 SNMPv3 用户不会复制到新设备。您必须删除用户、重新添加，然后重新部署配置，以强制用户复制到新单元。
- 威胁防御 不再与其对等体共享 SNMP 客户端引擎数据。

- 如果您有大量访问控制和NAT规则，则配置的大小可能会阻止有效的配置复制，导致备用设备需要过长的时间才能达到备用就绪状态。这也会影响您在通过控制台或SSH会话进行复制期间连接到备用设备的能力。要提高配置复制性能，请使用 **asp rule-engine transactional-commit access-group** 和 **asp rule-engine transactional-commit nat** 命令为访问规则和NAT启用事务提交。
- 转换为备用角色的高可用性对中的设备可将其时钟与主用设备同步。

  示例：

```
firepower#show clock
01:00:52 UTC Mar 1 2022

...
01:01:18 UTC Mar 1 2022 <======= Incorrect (previous) clock
Cold Standby               Sync Config               Detected an Active mate

19:38:21 UTC Apr 9 2022 <======= Updated clock
Sync Config                Sync File System          Detected an Active mate
...
firepower/sec/stby#show clock
19:38:40 UTC Apr 9 2022
```

- 高可用性（故障切换）中的设备不会动态同步时钟。以下是进行同步时的一些事件示例：
  - 将创建一个新的 HA 对。
  - HA 已中断并已重新创建。
  - 故障切换链路上的通信中断并重新建立。
  - 已使用 **no failover/failover** 或 **configure high-availability suspend/resume** (威胁防御 CLISH) 命令来手动更改故障切换状态。
- 在平台上运行的 ASA/威胁防御 HA 对中，同步仅适用于 ASA/威胁防御 等应用，而不适用于机箱。
- 启用 HA 会强制删除所有路由，并会在 HA 进程变为“活动”状态后重新添加这些路由。在此阶段，您可能会遇到连接丢失的情况。
- 在使用管理中心或设备管理器创建威胁防御高可用性期间，所选辅助威胁防御设备上的所有现有配置都将替换为从所选主要威胁防御设备复制的配置，因此在高可用性期间请谨慎选择主设备（ HA) 创建。例如，如果在现有主设备出现故障并使用退货授权 (RMA) 进行更换时，HA 被破坏并重新创建，则在创建 HA 期间，应选择更换设备作为辅助设备，以便从所选的主设备将被复制到替换设备。

添加 威胁防御 高可用性对

建立主用/备用高可用性对时，请将其中一台设备指定为主设备，将另一台指定为辅助设备。系统会将合并的配置应用于配对设备。如果存在冲突，则系统会应用已指定为主设备的设备中的配置。

注释 系统使用故障切换链路同步配置，而使用状态故障切换链路同步对等体之间的应用内容。故障切换链路和状态故障切换链路位于专用 IP 空间中，仅用于高可用性对中的对等体之间的通信。在高可用性对建立后，无法在不破坏高可用性对并重新配置的情况下修改所选接口链路和加密设置。

注意 创建或中断 威胁防御高可用性对会立即在主设备和辅助设备上重启 Snort 进程，从而暂时中断两个设备上的流量检查。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。系统会向您发出警告，指明继续创建高可用性对会重启主用和辅助设备上的 Snort 进程，并允许您取消。

开始之前

确认两台设备：

- 型号相同。
- 拥有相同数量和类型的接口。
- 具有处理远程部署中管理流量的相同数据接口。例如，如果您在设备 1 中使用的是 eth0，也要在设备 2 中使用相同的接口，即还是 eth0。
- 将静态 IP 地址分配给处理远程部署管理流量的数据接口。
- 在远程部署中具有兼容的 IPv6 地址。数据托管接口上的辅助 IPv6 地址列表大小应与主 IPv6 地址列表大小匹配。
- 在远程部署中具有相同的 IPV6 地址前缀。主设备中的每个 IPv6 地址前缀都应与辅助 IPv6 地址列表中的一个完全匹配。
- 请勿在远程部署中为 IPv6 地址启用 EUI 64 选项。如果为任何设备启用此选项，则高可用性创建失败。
- 在远程部署中具有同一子网中的 IP 地址。
- 为它们分配不同的 IP 地址。
- 位于同一个域和组中。
- 具有正常运行状态且运行相同的软件。
- 处于路由模式或透明模式下。

注释 远程部署仅支持路由模式。

- 具有相同的 NTP 配置。请参阅为威胁防御配置 NTP 时间同步，第 661 页。
- 完全部署且没有尚未确认的更改。

- 在其任一接口中都未配置 DHCP 或 PPPoE。

注释 如果主设备上可用的证书在辅助设备上不存在，那么两台 威胁防御设备之间可能会形成高可用性。形成高可用性时，证书将在辅助设备上同步。

过程

步骤 1 在 CDO 导航栏中，点击 **清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡并选择要建立为主设备的设备。

步骤 4 在 **管理** 窗格中，点击 **高可用性**。

步骤 5 为高可用性对输入显示**名称 (Name)**。

步骤 6 在**设备类型 (Device Type)** 下，选择 **Firepower 威胁防御 (Firepower Threat Defense)**。

步骤 7 为高可用性对选择**主对等 (Primary Peer)** 设备。

步骤 8 为高可用性对选择**辅助对等 (Secondary Peer)** 设备。

注释 在远程部署中， **辅助对等体** 列表中显示的设备取决于在 **主对等体** 列表中选择的主用设备：

- 如果选定的主要对等体使用数据接口进行管理，则辅助对等体列表中仅列出数据接口受管设备。
- 如果主对等体上的数据管理接口配置了 IPv4 地址，则辅助对等体仅列出配置了 IPv4 地址的数据接口受管设备。相同的规则也适用于 IPv6 管理的设备。
- 主设备和辅助设备的数据管理接口名称应相同。具有不同接口名称的设备不会列在辅助对等体列表中。

步骤 9 点击**继续 (Continue)**。

步骤 10 在 LAN 故障切换链路下，选择为故障切换通信保留足够带宽的**接口 (Interface)**。

注释 只有没有逻辑名称，不属于安全区域且不用于处理管理流量的接口将在 **添加高可用性对** 对话框的 **接口** 下列列表中列出。

步骤 11 键入任何识别**逻辑名称 (Logical Name)**。

步骤 12 为主用设备上的故障切换链路键入**主要 IP (Primary IP)** 地址。

此地址应处于未使用的子网上。 此子网可以是 31 位 (255.255.255.254 或 /31) 的，仅包含两个 IP 地址。

注释 169.254。1.0/24 and fd00:0:0:*::/64 是内部使用的子网，不能用于故障切换或状态链路。

步骤 13 或者，选择**使用 IPv6 地址 (Use IPv6 Address)**。

步骤 14 为备用设备上的故障切换链路键入**辅助 IP (Secondary IP)** 地址。此 IP 地址必须与主要地址在同一子网中。

步骤 15 如果使用 IPv4 地址，请键入适用于主要和辅助 IP 地址的**子网掩码 (Subnet Mask)**。

步骤 16 或者，在状态性故障切换链路下，选择同一**接口 (Interface)**，或选择不同的接口并输入高可用性配置信息。

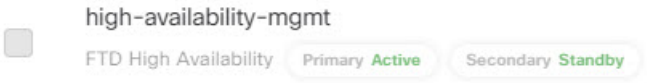
此子网可以是 31 位 (255.255.255.254 或 /31) 的，仅包含两个 IP 地址。

注释 169.254。1.0/24 and fd00:0:0:*::/64 是内部使用的子网，不能用于故障切换或状态链路。

步骤 17 或者，选择**已启用 (Enabled)** 并为故障切换链路之间的 IPsec 加密选择**密钥生成 (Key Generation)** 方法。

步骤 18 点击 **OK**。由于此过程会同步系统数据，因此需要花费几分钟时间。

成功配置后，您可以在 CDO **清单 (Inventory)** 页面上的 威胁防御 节点上看到 **FTD 高可用性 (FTD High Availability)** 标签。选择节点以查看您为实现高可用性而配置的主用和备用设备



。

下一步做什么

确保来备份设备。您可以使用备份在设备发生故障时快速更换设备，并在不断开与管理中心的连接的情况下恢复高可用性服务。

配置可选高可用性参数

您可以在 管理中心上查看初始高可用性配置。您无法在不破坏高可用性对，然后重新建立它的情况下编辑这些设置。

您可以编辑故障切换触发条件，以改进故障切换结果。通过接口监控，您可以确定哪些接口更适合于故障切换。

配置备用 IP 地址和接口监控

为每个接口设置一个备用 IP 地址。虽然建议指定备用 IP 地址，但它并不是必需的。如果没有备用 IP 地址，则主用设备无法执行用于检查备用接口运行状态的网络测试；它只能跟踪链路状态。

默认情况下，在所有物理接口上启用监控，而对于 Firepower 1010 的所有 VLAN 接口，还会配置逻辑名称。您可能希望排除连接到非关键网络的接口，以免影响故障切换策略。Firepower 1010 交换机端口无法进行接口监控。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑的设备高可用性对旁边，点击 **编辑**（✎）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击**高可用性 (High Availability)** 选项卡。

步骤 4 在**监控的接口**区域中，点击要编辑的接口旁边的 **编辑**（✎）。

步骤 5 选中**监控此接口的故障情况**复选框。

步骤 6 在 **IPv4** 选项卡上，输入**备用 IP 地址**。

此地址必须是与活动 IP 地址位于同一网络的可用地址。

步骤 7 如果手动配置了 IPv6 地址，请在 **IPv6** 选项卡上，点击活动 IP 地址旁边的 **编辑**（✎），输入**备用 IP 地址**，然后点击**确定**。

此地址必须是与活动 IP 地址位于同一网络的可用地址。对于自动生成的地址和**强制 EUI 64** 地址，系统会自动生成备用地址。

步骤 8 点击**确定 (OK)**。

编辑高可用性故障切换条件

您可以根据网络部署自定义故障切换条件。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑的设备高可用性对旁边，点击 **编辑**（✎）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 选择**高可用性**。

步骤 4 在**故障切换触发条件 (Failover Trigger Criteria)** 旁边，点击 **编辑**（✎）。

步骤 5 在**接口故障阈值 (Interface Failure Threshold)** 下，选择在设备进行故障切换之前必须出现故障的接口数目或百分比。

步骤 6 在**呼叫数据包间隔 (Hello packet Intervals)** 下，选择通过故障切换链路发送呼叫数据包的频率。

注释 如果在 Firepower 2100 上使用远程访问 VPN，请使用默认 Hello 数据包间隔。否则，您可能会看到高 CPU 使用率，从而导致发生故障切换。

步骤 7 点击**确定 (OK)**。

配置虚拟 MAC 地址

可以在 Cisco Secure Firewall Management Center上的两个位置配置主用和备用 MAC 地址以进行故障切换：

- 配置接口期间“编辑接口”页面的“高级”选项卡；请参阅配置 MAC 地址，第 569 页。
- 从“高可用性”页面访问的“添加接口 MAC 地址”页面；请参阅

如果在两个位置都配置了主用和备用MAC地址，则在配置接口期间定义的地址优先进行故障切换。

通过将主用和备用 MAC 地址指定到物理接口，可以最大限度地减少故障切换期间的流量损失。此功能为故障切换提供了针对 IP 地址映射的冗余。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑的设备高可用性对旁边，点击 **编辑**（）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 选择**高可用性**。

步骤 4 选择接口 Mac 地址旁边的 **添加**（）。

步骤 5 选择**物理接口**。

步骤 6 在**主用接口 Mac 地址**中键入相应的值。

步骤 7 在**备用接口 Mac 地址**中键入相应的值。

步骤 8 点击**确定 (OK)**。

管理高可用性

本部分介绍您在启用高可用性后如何管理高可用性，包括如何更改高可用性设置以及如何强制从一台设备故障切换到另一台设备。

在 威胁防御 高可用性对中切换主用对等体

在建立威胁防御高可用性对以后，可以手动切换主用和备用设备，出于持续性故障或运行状况事件等原因有效执行故障切换。两台设备应该已经完全部署，然后才能完成此程序。

开始之前

刷新单个 威胁防御 高可用性对的节点状态 ， 第 477 页。这样可以确保 威胁防御 高可用性设备对上的状态与 管理中心 上的状态同步。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要更改主用对等体的高可用性对旁边，点击**切换主用对等体 (Switch Active Peer)**。

步骤 3 您可以执行以下操作：

- 点击**是**将使备用设备立即变成高可用性对中的主用设备。
- 点击 **No** 将取消并返回到 Device Management 页面。

刷新单个 威胁防御 高可用性对的节点状态

每当重新引导 威胁防御 高可用性对中的主用或备用设备时， 管理中心 可能不会显示这两种设备的准确高可用性状态。这是因为，当设备重新引导时，高可用性状态会在设备上立即更新，其相应的事件将会发送到 管理中心。但是，状态可能不会在 管理中心 上更新，因为设备和 管理中心 之间的通信尚未建立。

管理中心 与设备之间出现通信故障或通信隧道信号弱，可能会导致数据不同步。切换高可用性对中的主用设备和备用设备时，即使持续很长时间，这种更改可能也不会反映在 管理中心中。

在此类情况下，可以刷新高可用性节点状态以获取有关高可用性对中主用设备和备用设备的准确信息。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在希望刷新节点状态的高可用性对旁边，点击 **刷新 HA 节点状态**。

步骤 3 点击 **是** 来刷新节点状态。

暂停和恢复高可用性

可以暂停高可用性对中的设备。此功能适用于以下情形：

- 两台设备都在主用 - 主用情况下，且修复故障转移链路上的通信不能更正问题。
- 希望对主用或备用设备进行故障排除，并且不希望设备在此期间发生故障切换。

暂停高可用性时，停止将设备对用作故障转移设备。当前主用设备保持活动状态，并处理所有用户连接。但是，不会再监控故障转移条件，并且系统永远不会故障切换到现在的伪备用设备。备用设备将保留其配置，但将保持非活动状态。

暂停 HA 和中断 HA 之间的主要区别是，在暂停的 HA 设备上将保留高可用性配置。如果中断 HA，则会清除配置。因此，您可以选择在暂停系统上恢复高可用性，这样可启用现有配置并再次将两台设备设置为故障转移对。

要暂停高可用性，请使用 **configure high-availability suspend** 命令。

```
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in
progress and 'NO' if you wish to abort: YES
Successfully suspended high-availability.
```

如果您从主用设备暂停高可用性，配置将在主用和备用设备上暂停。如果从备用设备暂停，配置仅在备用设备上暂停，但主用设备不会尝试故障切换至暂停的设备。

要恢复故障切换，请使用 **configure high-availability resume** 命令。

```
> configure high-availability resume
Successfully resumed high-availablity.
```

只能恢复处于暂停状态的设备。该设备将与对等设备协商主用/备用状态。

注释 暂停高可用性是一种临时状态。如果您重新加载一台设备，它会自动恢复高可用性配置，并与对等体协商主用/备用状态。

更换 威胁防御 高可用性对中的设备

要使用备份文件替换 威胁防御 高可用性对中的故障设备，请参阅 《Cisco Secure Firewall Management Center 管理指南》中的 恢复管理中心和托管设备 。

如果没有故障设备的备份，则必须中断高可用性。然后，将替换设备注册到 Cisco Secure Firewall Management Center 并重新建立高可用性。该过程会因设备是主设备还是辅助设备而有所不同：

- 将主 威胁防御 高可用性设备替换为无备份 ， 第 478 页
- 将辅助 威胁防御 HA 单元更换为无备份 ， 第 479 页

将主 威胁防御 高可用性设备替换为无备份

按照以下步骤更换 威胁防御 高可用性对中出现故障的主设备。如果无法执行这些步骤，系统可能会覆盖现有的高可用性配置。

注意 创建或中断 威胁防御 高可用性对会立即在主设备和辅助设备上重启 Snort 进程，从而暂时中断两个设备上的流量检查。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。系统会向您发出警告，指明继续创建高可用性对会重启主用和辅助设备上的 Snort 进程，并允许您取消。

注意 切勿在未重新映像磁盘的情况下将磁盘从传感器或 管理中心 移动到其他设备。这是不受支持的配置，可能会导致功能中断。

过程

步骤 1 选择**强制中断**以分隔高可用性对；请参阅高可用性对中的独立设备，第 480 页。

注释 中断操作会从 威胁防御 和 管理中心删除与 HA 相关的所有配置，您需要稍后手动重新创建。要成功配置同一 HA 对，请确保在执行 HA 中断操作之前保存所有接口/子接口的 IP，MAC 地址和监控配置。

步骤 2 从 管理中心注销出现故障的主 威胁防御 设备。

步骤 3 将替换 威胁防御 注册到 管理中心将设备载入 云交付的防火墙管理中心的前提条件 ，第 9 页。

步骤 4 配置高可用性，在注册期间使用现有的辅助/主用设备作为主设备，并将更换设备用作辅助/备用设备；请参阅添加 威胁防御 高可用性对，第 471 页。

将辅助 威胁防御 HA 单元更换为无备份

按照以下步骤替换 威胁防御 高可用性对中出现故障的辅助设备。

注意 创建或中断 威胁防御 高可用性对会立即在主设备和辅助设备上重启 Snort 进程，从而暂时中断两个设备上的流量检查。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。系统会向您发出警告，指明继续创建高可用性对会重启主用和辅助设备上的 Snort 进程，并允许您取消。

过程

步骤 1 选择**强制中断**以分隔高可用性对；请参阅高可用性对中的独立设备，第 480 页。

注释 中断操作会从 威胁防御 和 管理中心删除与 HA 相关的所有配置，您需要稍后手动重新创建。要成功配置同一 HA 对，请确保在执行 HA 中断操作之前保存所有接口/子接口的 IP，MAC 地址和监控配置。

步骤 2 从 管理中心。

步骤 3 将替换 威胁防御 注册到 管理中心将设备载入 云交付的防火墙管理中心的前提条件 ， 第 9 页。

步骤 4 在注册期间使用现有主/主用设备作为主设备并将替换设备作为辅助/备用设备配置高可用性；请参阅添加 威胁防御 高可用性对 ， 第 471 页。

高可用性对中的独立设备

断开高可用性对后，主用设备将保留所有已部署功能。备用设备将丢失故障切换和接口配置，并成为独立设备。

在断开操作之前尚未部署到主用设备的策略，在断开操作完成后仍会保持未部署状态。请在断开操作完成后，在独立设备上部署这些策略。

提示 FlexConfig 策略例外。在主用设备上部署的 FlexConfig 策略可能会在中断高可用性操作后显示部署失败。您必须在主用设备上修改并重新部署 FlexConfig 策略。

注释 您无法使用 管理中心访问高可用性对，请使用 CLI 命令 **configure high-availability disable** 删除两个设备上的故障切换配置。

开始之前

- 刷新单个 威胁防御 高可用性对的节点状态 ， 第 477 页。这样可以确保 威胁防御 高可用性设备对上的状态与 管理中心 上的状态同步。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要中断的高可用性对旁边，点击 **中断高可用性**图标。

步骤 3 （可选）选中该复选框可以在备用对等体不响应时强制断开。

步骤 4 点击 **Yes**。系统分隔设备高可用性对。

断开操作将从主用和备用设备中删除故障切换配置。

下一步做什么

（可选）如果在主用设备上使用 flex-config 策略，请修改并重新部署 flex-config 策略以消除部署错误。

取消注册高可用性对

您可以从 管理中心中删除该对，并使用 CLI 禁用每个设备的高可用性。

开始之前

此过程需要 CLI 访问权限。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要注销的高可用性对旁边，点击 **删除**（ ）。

步骤 3 点击 **Yes**。设备高可用性对随即会被删除。

步骤 4 在每个设备上，访问 威胁防御 CLI，然后输入以下命令：

configure high-availability disable

如果不输入此命令，则无法重新注册这些设备并形成一个新的 HA 对。

注释 在更改防火墙模式之前输入此命令；如果更改该模式，则该设备以后将不会允许您输入 **configure high-availability disable** 命令，并且 管理中心无法在没有此命令的情况下重新形成高可用性对。

监控 高可用性

此部分用于监控高可用性状态。

查看故障切换历史记录

您可以在单个视图中查看两个高可用性设备的故障切换历史记录。历史记录按时间顺序显示，并包括任何故障切换的原因。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑的设备高可用性对旁边，点击 **编辑**（ ）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 选择**摘要**。

步骤 4 在“常规”(General) 下，点击 **视图**（）。

查看状态故障切换统计信息

您可以在高可用性对中查看主设备和辅助设备的状态故障切换链路统计信息。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑的设备高可用性对旁边，点击 **编辑**（）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 选择**高可用性**。

步骤 4 在“状态故障切换链路”(Stateful Failover Link) 下，点击 **视图**（）。

步骤 5 选择一个设备来查看统计信息。

对远程分支机构部署中的高可用性中断进行故障排除

本部分介绍如何解决在远程部署中中断高可用性对时可能遇到的一些常见问题。

- 两台设备均处于主用-主用状态。
- 主设备或辅助设备已断开与 CDO 的连接，并且故障切换链路已无法运行。
- 辅助设备处于故障或禁用状态，并且已断开与 CDO 的连接。

如何中断处于主用-主用状态的高可用性对

远程部署中的两台设备均处于主用-主用状态，因为故障转移接口无法运行，并且它们停止了在其数据接口上接收响应。在这种情况下，两台设备都会使用其数据管理接口上的活动 IP 地址，而这样会导致设备和 CDO 之间的网络不稳定。

您可以通过登录设备 CLI 并在两台设备上使用“show failover state”命令来确定它们是否都处于主用模式。两台设备的设备状态均显示为“活动”，并且为两台设备分配了相同的活动 IP 地址。

注释 您可以尝试纠正故障转移接口以恢复两个对等体之间的通信，然后执行**强制中断**操作。

如果无法修复故障转移接口的连接问题，请执行以下步骤：

过程

步骤 1 在两台设备中确定要从网络中删除的设备。

步骤 2 通过控制台端口或使用 SSH 连接至已确定设备的 CLI。

步骤 3 使用“管理员”(Admin) 用户名和密码登录。

步骤 4 输入 **pmtool disablebyid sftunnel** 命令。

注释 只能在思科技术支持中心的指导下使用 **pmtool** 命令。

步骤 5 断开所有接口与要从网络中删除的设备的连接。

步骤 6 输入 **configure network management-data-interface ipv4 manual** *ip_address ipv4_netmask gateway_ip_address* **interface***interface_id* 命令。

在 *ip_address* 中指定备用设备的 IP 地址。

示例：

```
Configure network management-data-interface ipv4 manual 10.10.6.7 255.255.255.0 interface
gig0/0
Configuration updated successfully..!!
```

步骤 7 输入 **configure high-availability suspend** 以暂停 HA。

```
configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in
progress and 'NO' if you wish to abort: YES
Successfully suspended high-availability.
```

步骤 8 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 9 点击 **设备** 选项卡，找到您的设备。

步骤 10 点击 **FTD** 选项卡并选择主设备。

步骤 11 在左侧的**管理 (Management)** 窗格中，点击**高可用性 (High Availability)**。

步骤 12 选择**设备 (Device)** > **设备管理 (Device Management)**。

步骤 13 在要分隔高可用性对的高可用性对旁边，点击**强制中断 (Force Break)**。

系统将显示一条消息，表明已成功分离高可用性对。

步骤 14 将所有接口连接到设备。

步骤 15 在 FTD CLI 中，输入 **pmtool enablebyId sftunnel**。

威胁防御设备会在某个时间与 CDO 建立连接。

注释 设备可能需要 5 分钟才能与 CDO 建立通信。

步骤 16 输入 **sftunnel-status-brief** 命令以查看管理连接状态。

```
sftunnel-status-brief
```

```
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Wed Feb 9 09:21:57 2020 UTC
Last disconnect time : Wed Feb 9 09:19:09 2020 UTC
```

步骤 17 选择**部署 (Deploy)** > **部署 (Deployment)** 以部署更改。

在 CDO 部署更改之前，它将检测配置差异并停止部署。CDO 会检测在防御协调器之外对设备进行的 IP 地址更改。

步骤 18 与 CDO 同步接口更改。请参阅与 管理中心同步接口更改 ， 第 499 页。

步骤 19 现在，您可以将待处理的更改部署到设备。请参阅部署配置更改。。

设备现在成为了具有备用设备的新 IP 地址的独立设备。

下一步做什么

（可选）将所有待处理更改部署到具有主用设备 IP 地址的其他设备。

如何在主用或备用设备失去连接时中断高可用性对

问题：其中一个对等体断开与 管理中心 的连接，并且故障转移链路已无法运行。

表 *57:* 场景：

主设备状态	辅助设备状态	与 CDO 的主设备连接？	与 CDO 的辅助设备连接？	故障转移链路是否正常运行？ （主设备和辅助设备之间的连接）
主用	待机	是	否	不支持
备用	主用	不支持	是	否

解决方案：

首先，您可以尝试纠正故障转移接口以恢复两个对等体之间的通信，然后执行中断或强制中断操作来分隔设备。

如果无法修复故障转移接口的连接问题，则必须在执行高可用性中断操作后使用设备 CLI 来完成其他步骤。

过程

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡，找到您的设备。

步骤 3 点击 **FTD** 选项卡并选择主设备。

步骤 4 在左侧的**管理 (Management)** 窗格中，点击**高可用性 (High Availability)**。

步骤 5 依次选择**设备** > **设备管理**。

步骤 6 在要中断的高可用性对旁边，点击**中断 HA (Break HA)**。

步骤 7 （可选）您也可以选中此复选框以便在其中一个对等体无响应时强制中断。

步骤 8 点击 **Yes**。

步骤 9 从 CDO 中删除备用设备。

a) 依次选择**设备** > **设备管理**。

b) 在要删除的设备旁，点击**删除 (Delete)**。

步骤 10 通过控制台端口或使用 SSH 连接至备用设备的 CLI。

步骤 11 使用“管理员”(Admin) 用户名和密码登录。

步骤 12 输入 **configure manager delete** 以删除管理器。

此命令将会禁用当前的管理器 CDO。

步骤 13 输入 **configure high-availability disable** 以删除故障转移配置并禁用设备上的数据管理接口。

步骤 14 输入 **configure network management-data-interface**。

示例：

```
configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.
```

新的网络设置会被分配给数据设备。

下一步做什么

如果需要，您可以将设备作为独立设备载入 CDO。

如何在辅助设备处于故障或禁用状态时中断高可用性对

问题：辅助设备处于故障或禁用状态，并且已断开与 CDO 的连接。此外，故障转移链路可能会运行，但也可能不会运行。

表 *58:* 场景：

主设备状态	辅助设备状态	与 CDO 的主设备连接？	与 CDO 的辅助设备连接？	故障转移链路是否正常运行？ （主设备和辅助设备之间的连接）
主用	失败	是	否	是/否
活动	已禁用	是	否	是/否

解决方案：

执行高可用性强制中断以便分隔设备，然后使用设备 CLI 从备用设备中删除配置，并让设备成为独立设备。

过程

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡，找到您的设备。

步骤 3 点击 **FTD** 选项卡并选择主设备。

步骤 4 在左侧的**管理 (Management)** 窗格中，点击**高可用性 (High Availability)**。

步骤 5 依次选择**设备** > **设备管理**。

步骤 6 在要中断的高可用性对旁边，点击**中断 HA (Break HA)**。

步骤 7 选中此复选框可在其中一个对等体无响应时强制中断。

步骤 8 点击 **Yes**。

步骤 9 从 CDO 中删除备用设备。

a) 依次选择**设备** > **设备管理**。

b) 在要删除的设备旁，点击**删除 (Delete)**。

步骤 10 通过控制台端口或使用 SSH 连接至备用设备的 CLI。

步骤 11 使用“管理员”(Admin) 用户名和密码登录。

步骤 12 输入 **configure high-availability disable** 以删除故障转移配置并禁用设备上的数据管理接口。

步骤 13 输入 **configure network management-data-interface**。

示例：

```
configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:
```

```
Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.
```

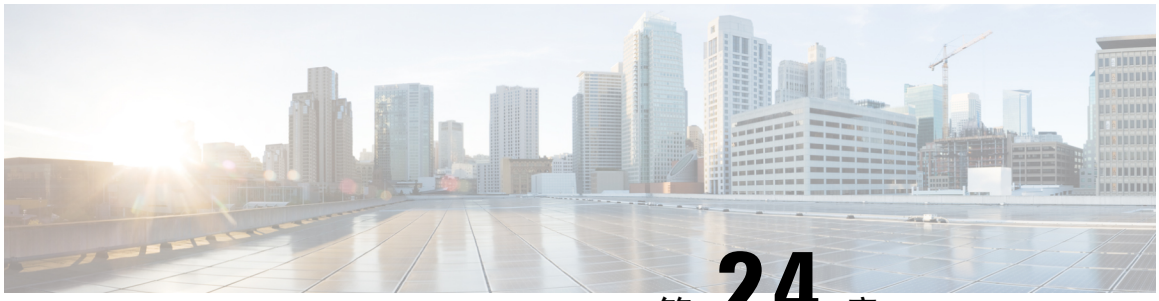
新的网络设置会被分配给数据设备。

下一步做什么

如果需要，您可以将设备作为独立设备载入 CDO。

第 IX 部分

接口和设备设置



第 24 章

接口概述

威胁防御 设备包括可在不同模式下配置的数据接口，以及管理/诊断 接口。

管理/诊断接口

物理管理接口由诊断逻辑接口和管理逻辑接口共用。

管理接口

管理接口与设备上的其他接口分离。它用于设置设备并将其注册到管理中心。它使用自己的 IP 地址和静态路由。您可以在 CLI 中使用 **configure network** 命令配置其设置。如果在将 IP 地址添加到 管理中心后在 CLI 中更改该地址，则可以通过**设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Devices)** > **管理 (Management)** 区域在 Cisco Secure Firewall Management Center中匹配该 IP 地址。

您也可以使用数据接口而不是管理接口来管理 威胁防御 。

诊断接口

诊断逻辑接口可以连同其余数据接口一起在 **设备** > **设备管理** > **接口**屏幕上进行配置。可以选择是否使用诊断接口（请参阅方案的路由和透明模式部署）。诊断接口只允许管理流量，而不允许通过流量。它不支持 SSH；仅可以对数据接口或管理接口进行 SSH。诊断接口可帮助进行 SNMP 或系统日志监视。

注释 虽然诊断接口和管理接口共享一个物理端口，但必须为同一网络上的每个接口分配不同的IP地址。

接口模式和类型

您可以在两种模式下部署 威胁防御 接口：常规防火墙模式和仅 IPS 模式。您可以在同一设备上同时配置防火墙和仅 IPS 接口。

常规防火墙模式

防火墙模式接口需要对流量执行防火墙功能，例如维持流量、跟踪 IP 和 TCP 层的流量状态、IP 分片重组和 TCP 规范化。另外，您还可以根据安全策略，选择为此流量配置 IPS 功能。

可以配置的防火墙接口类型取决于为设备设置的防火墙模式：路由或透明模式。有关详细信息，请参阅透明或路由防火墙模式，第 377 页。

- 路由模式接口（仅路由防火墙模式）- 要在其间路由的每个接口都在不同的子网中。
- 网桥组接口（路由和透明防火墙模式）- 您可以将网络上的多个接口组合在一起，Firepower 威胁防御设备将使用桥接技术在接口之间传递流量。每个桥接组包括一个网桥虚拟接口 (BVI)，供您为其分配一个网络 IP 地址。 在路由模式下，Firepower 威胁防御设备在 BVI 和常规路由接口之间路由。在透明模式下，每个网桥组都是独立的，相互之间无法通信。

仅 IPS 模式

仅 IPS 模式的接口将绕过许多防火墙检查，仅支持 IPS 安全策略。如果您有单独的防火墙来保护这些接口，并且不希望造成防火墙功能的开销，则可能需要实施仅限 IPS 的接口。

注释 防火墙模式只影响常规的防火墙接口，而不影响仅 IPS 接口，如内联集或被动接口。仅 IPS 接口可以在两种防火墙模式下使用。

仅 IPS 接口可以部署为以下类型：

- 内嵌集，带有可选分路模式 - 内嵌集的作用类似于导线上的凹凸，并将两个接口绑定在一起插入到现有网络中。此功能使 FTD 可以安装在任何网络环境中，而无需配置相邻网络设备。内联接口无条件接收所有流量，但是，除非已明确丢弃，否则这些接口上接收的所有流量将在内联集外重传。

  在分流模式下，FTD 会进行内联部署，但网络流量不受干扰。相反，FTD 会复制每个数据包，这样它就可以对数据包进行分析。请注意，这些类型的规则在触发时会生成入侵事件，而且入侵事件表视图显示了触发数据包会在内联部署中被丢弃。在已部署内联的 FTD 上使用分流模式有很多优点。例如，您可以设置 FTD 和网络之间的布线，就像 FTD 是内联，并分析 FTD 生成的多种入侵事件。根据结果，您可以修改入侵策略，并添加最好地保护您的网络却不影响有效

性的丢弃规则。准备部署 FTD 内联时，您可以禁用分流模式，并开始丢弃可疑流量，而无需重新配置 FTD 和网络之间的走线。

注释 分流模式显著影响 FTD 性能，具体取决于流量。

注释 内嵌集可能是您所熟悉的“透明内联集”，但内联接口类型与透明防火墙模式或防火墙类型接口无关。

- 被动或 ERSPAN 被动 - 被动接口使用交换机 SPAN 或镜像端口监控网络中流动的流量。SPAN 或镜像端口允许从交换机的其他端口复制流量。此功能可以提供网络内的系统可视性，而不会影响网络流量。如果在被动部署中配置 FTD，FTD 将无法执行某些操作，例如，阻止流量或流量整形。被动接口无条件接收所有流量，这些接口不会重传接收到的流量。封装远程交换端口分析器 (ERSPAN) 接口允许您监控分布于多个交换机的源端口流量，并使用 GRE 来封装流量。仅当 FTD 处于路由防火墙模式时，才允许 ERSPAN 接口。

注释 由于混杂模式限制，某些使用 SR-IOV 驱动程序的 Intel 网络适配器（例如 Intel X710 或 82599）不支持在 NGFWv 上将 SR-IOV 接口用作被动接口。在此情况下，请使用支持此功能的网络适配器。有关英特尔网络适配器的详细信息，请参阅英特尔以太网产品。

安全区域和接口组

每个接口可以被分配给安全区域和/或接口组。然后，根据区域或组应用您的安全策略。例如，您可以把一个或多个设备上的“内部”接口分配到“内部”区域；而把“外部”接口分配到“外部”区域。然后，您可以配置访问控制策略，以便为使用相同区域的每台设备启用从内部区域到外部区域的流量。

要查看属于每个对象的接口，请选择**对象 (Objects)** > **对象管理 (Object Management)**，然后点击**接口 (Interface)**。此页面列出受管设备上配置的区域安全区域和接口组。您可以展开每个接口对象以查看每个接口对象中的接口类型。

注释 适用于**任何**区域的策略（全局策略）也适用于区域中的接口以及未分配给区域的任何接口。

注释 诊断/管理接口不属于区域或接口组。

安全区域 vs. 接口组

有两种类型的接口对象：

- 安全区域 - 接口只能属于一个安全区域。
- 接口组 - 接口可属于多个接口组（和一个安全区域）。

  您可以在 NAT 策略、预过滤器策略和 QoS 策略中使用接口组，也可以使用直接指定接口名称的功能，例如系统日志服务器或 DNS 服务器。

某些策略仅支持安全区域，而其他策略则支持区域和组。除非您需要接口组提供的功能，否则应默认使用安全区域，因为所有功能都支持安全区域。

不能将现有安全区域更改为接口组（反之亦然）；而必须创建新接口对象。

注释 尽管隧道区域不是接口对象，但您可以在某些配置中使用它们代替安全区域；请参阅隧道区域与预过滤，第 1403 页。

接口对象类型

请参阅以下接口对象类型：

- 被动 - 适用于仅 IPS 被动或 ERSPAN 接口。
- 内联 - 适用于仅 IPS 内联集接口。
- 已交换 - 适用于常规防火墙网桥组接口。
- 已路由 - 适用于常规防火墙路由接口。
- ASA -（仅安全区域）适用于传统 ASA FirePOWER 设备接口。

接口对象中的所有接口都必须为同一类型。创建接口对象后，不能更改其包含的接口类型。

接口名称

请注意，接口（或区域名称）本身不提供有关安全策略的任何默认行为。我们建议使用自描述的名称，以避免在未来的配置中出错。好的名称能表明逻辑网段或流量规范，例如：

- 内部接口的名称 - InsideV110、InsideV160、InsideV195
- DMZ 接口的名称 - DMZV11、DMZV12、DMZV-TEST
- 外部接口的名称 - Outside-ASN78、Outside-ASN91

接口对象和多租户

在多域部署中，您可以在任何级别创建接口对象。在祖先域中创建的区域接口对象可以包含位于不同域中的设备上的接口。在此情况下，在对象管理器中查看祖先接口对象配置的子域用户只能看到其域中的接口。

除非受角色限制，否则子域用户可以查看和编辑祖先域中创建的接口对象。子域用户可以从这些接口对象添加和删除接口。但是，他们无法删除或重命名接口对象。您既不能查看也不能编辑后代域中创建的接口对象。

Auto-MDI/MDIX 功能

对于 RJ-45 接口，默认的自动协商设置还包括 Auto-MDI/MDIX 功能。Auto-MDI/MDIX 在自动协商阶段检测直通电缆时执行内部交叉，从而消除交叉布线的需要。如要启用接口的 Auto-MDI/MDIX，必须将速度或双工设置为自动协商。如果将速度和双工明确设置为固定值，从而禁用了两种设置的自动协商，则 Auto-MDI/MDIX 也将被禁用。对于千兆以太网，当速度和双工被设置为 1000 和全值时，接口始终会自动协商；因此，Auto-MDI/MDIX 始终会启用，且您无法禁用它。

接口默认设置

本部分列出接口的默认设置。

接口的默认状态

接口的默认状态取决于类型。

- 物理接口 - 已禁用。对初始设置启用的管理接口是个例外。
- 冗余接口 - 已启用。但是，要使流量通过冗余接口，还必须启用成员物理接口。
- VLAN 子接口 - 已启用。但是，要使流量通过子接口，还必须启用物理接口。
- EtherChannel port-channel 接口（ASA 型号）- 已启用。但是，要使流量通过 EtherChannel 接口，还必须启用通道组物理接口。
- EtherChannel port-channel 接口（Firepower 型号）- 已禁用。

注释 对于 Firepower 4100/9300，您可以出于管理需要同时启用和禁用机箱和 管理中心 上的接口。为使接口正常运行，必须同时在两个操作系统中启用该接口。由于接口状态可独立控制，因此机箱与 管理中心 之间可能出现不匹配的情况。

默认速度和双工

默认情况下，铜缆 (RJ-45) 接口的速度和双工设置为自动协商。

默认情况下，光纤 (SFP) 接口的速度和双工会被设为最大速度，同时启用自动协商。

对于 Cisco Secure Firewall 3100，速度设置为检测已安装的 SFP 速度。

创建安全区域和接口组对象

添加您可以为其分配设备接口的安全区域和接口组。

提示 可以创建空的接口对象并随后向其添加接口。要添加接口，该接口必须具有名称。您还可以配置接口时创建安全区域（但不是接口组）。

开始之前

了解每种类型的接口对象的使用要求和限制。请参阅安全区域和接口组 ， 第 493 页。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**接口**。

步骤 3 点击**添加 (Add)** > **安全区域 (Security Zone)** 或**添加 (Add)** > **接口组 (Interface Group)**。

步骤 4 输入 **Name**。

步骤 5 选择**接口类型 (Interface Type)**。

步骤 6 （可选） 从**设备 (Device)** > **接口 (Interfaces)** 下拉列表中，选择包含要添加的接口的设备。

您不需要在此屏幕上分配接口；您可以在配置接口时将接口分配给区域或组。

步骤 7 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

启用物理接口并配置以太网设置

本节介绍如何执行以下操作：

- 启用物理接口。默认情况下，物理接口处于禁用状态（诊断接口除外）。
- 设置特定的速度和复用。默认情况下，速度和复用设置为“自动”。

此过程仅涵盖一小部分接口设置。此时不能设置其他参数。例如，不能命名要用作 EtherChannel 或冗余接口一部分的接口。

注释 对于 Firepower 4100/9300，可在 FXOS 中配置基本接口设置。有关详细信息，请参阅配置物理接口，第 423 页。

注释 有关 Firepower 1010 交换机端口，请参阅 配置 Firepower 1010 交换机端口，第 518 页。

威胁防御 功能历史记录：

- 7.2 - 对 Firepower 2100，Cisco Secure Firewall 3100 的 LLDP 支持。Cisco Secure Firewall 3100 的流量控制支持。
- 7.2 - 支持 Cisco Secure Firewall 3100 的前向纠错
- 7.2 - 支持基于 SFP 为 Cisco Secure Firewall 3100 设置速度
- 7.2 -对 Firepower 1100 的 LLDP 支持
- 7.2 - 接口自动协商现在独立于速度和复用设置，改进了接口同步

开始之前

如果在将设备添加到 管理中心后更改了设备上的物理接口，需要点击 **接口**左上角的 **从设备同步接口** 刷新接口列表。 对于支持热插拔的安全防火墙 3100，在更改设备上的接口之前，请参阅 管理 Cisco Secure Firewall 3100 的网络模块，第 502 页 。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（✎）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑**（✎）。

步骤 3 选中**启用**复选框以启用此接口。

步骤 4 （可选） 在**说明**字段中添加说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 5 （可选） 通过点击 **硬件配置** > **速度**，设置复用和速度。

- **复用**—选择 **全** 或 **半**。SFP 接口仅支持 **全** 复用。
- **速度**-选择速度（因型号而异）。 Cisco Secure Firewall 3100）选择 **检测 SFP** 以检测已安装的 SFP 模块的速度并使用适当的速度。复用始终为全复用，并且始终启用自动协商。如果您稍后将网络模块更改为其他型号，并希望速度自动更新，则此选项非常有用。
- **自动协商**-设置接口以协商速度、链路状态和流量控制。对于低于 1000 Mbps 的速度，无法编辑此设置。对于 SFP 接口，只能在速度设置为 1000 Mbps 时禁用自动协商。

- **前向纠错模式** Cisco Secure Firewall 3100）对于 25 Gbps 及更高的接口，请启用前向纠错 (FEC)。对于 EtherChannel 成员接口，必须先配置 FEC，然后才能将其添加到 EtherChannel。使用**自动 (Auto)** 时选择的设置取决于收发器类型，以及接口是固定接口（内置）还是在网络模块上。

表 *59:* 用于自动设置的默认 *FEC*

收发器类型	固定端口默认 **FEC**（以太网 **1/9** 至 **1/16**）	网络模块默认 **FEC**
25G-SR	Clause 74 FC-FEC	Clause 108 RS-FEC
25G-LR	Clause 74 FC-FEC	Clause 108 RS-FEC
10/25G-CSR	Clause 74 FC-FEC	Clause 74 FC-FEC
25G-AOC*x*M	Clause 74 FC-FEC	Clause 74 FC-FEC
25G-CU2.5/3M	自动协商	自动协商
25G-CU4/5M	自动协商	自动协商

步骤 6 （可选）（Firepower 1100、2100、Cisco Secure Firewall 3100）通过点击 **硬件配置 (Hardware Configuration)** > **网络连接 (Network Connectivity)** 启用链路层发现协议 (LLDP)。

- **启用 LLDP 接收**-启用防火墙以从其对等体接收 LLDP 数据包。
- **启用 LLDP 传输**-启用防火墙以将 LLDP 数据包发送到其对等体。

步骤 7 （可选） (Cisco Secure Firewall 3100) ）通过点击**硬件配置 (Hardware Configuration)** > **网络连接 (Network Connectivity)**，然后选中**流量控制发送 (Flow Control Send)** 来为流量控制启用暂停 (XOFF) 帧。

流量控制通过允许拥塞节点在另一端暂停链路操作，从而让连接的以太网端口能够在拥塞期间控制流量速率。如果威胁防御端口遇到拥塞（内部交换机上的排队资源耗尽）并且无法接收更多流量，则它会通过发送暂停帧来通知另一个端口停止发送，直到状况恢复正常为止。在收到暂停帧后，发送设备会停止发送任何数据包，从而防止在拥塞期间丢失任何数据包。

注释 威胁防御 支持传输暂停帧，以便远程对等体可以对流量进行速率控制。

但是，不支持接收暂停帧。

内部交换机有一个包含 8000 个缓冲区的全局池，而每个缓冲区都有 250 个字节，并且交换机会为每个端口动态分配缓冲区。当缓冲区使用量超过全局高水位标记（2 MB [8000 个缓冲区]）时，会在每个启用了流量控制的接口上发送暂停帧；当特定接口的缓冲区超过端口高水位标记（0.3125 MB [1250 个缓冲区]）时，会从该接口发送暂停帧。在发送暂停后，如果缓冲区使用率降低至低水位标记之下（全局 1.25 MB [5000 个缓冲区]；每个端口 0.25 MB [1000 buffers]），则可发送 XON 帧。链接伙伴可在收到 XON 帧之后恢复流量。

系统仅支持 802.3x 中定义的流量控制帧。系统不支持基于优先级的流量控制。

步骤 8 在**模式**下拉列表中，选择以下选项之一：

- **无** - 为常规防火墙接口和内联集选择此设置。该模式将基于后续配置自动更改为路由、交换或内联。
- **被动** - 为被动仅限 IPS 接口选择此设置。
- **Erspan** - 为 ERSPAN 被动仅限 IPS 接口选择此设置。

步骤 9 在 **优先级** 字段中，输入一个介于 0 和 65535 之间的数字。

此值在策略型路由配置中使用。优先级用于确定如何跨多个出口接口分配流量。

步骤 10 点击**确定 (OK)**。

步骤 11 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

步骤 12 继续配置接口。

- 常规防火墙接口 ， 第 517 页
- 内联集和被动接口 ， 第 575 页

与 管理中心同步接口更改

在设备上进行的接口配置更改可能导致 管理中心 和设备不同步。管理中心 可以通过以下方法之一检测到接口更改：

- 设备发送的事件
- 部署时同步 管理中心

  当 管理中心 尝试部署时检测到接口更改，部署将失败。必须先接受接口更改。

- 手动同步

在 管理中心 外部执行的两种类型的接口更改需要同步：

- 添加或删除物理接口-添加新接口或删除未使用接口对 威胁防御 配置的影响最小。但是，删除安全策略中使用的接口会影响配置。可以直接在 威胁防御 配置中的很多位置引用接口，包括访问规则、NAT、SSL、身份规则、VPN、DHCP 服务器等。删除接口将删除与该接口相关的任何配置。引用安全区域的策略不受影响。还可以编辑已分配的 EtherChannel 的成员关系，而不影响逻辑设备或要求在 管理中心上进行同步。

  当 管理中心 检测到更改时，“**接口**”页面会在每个接口左侧显示状态（已删除、已更改或已添加）。

- 管理中心 访问接口更改-如果使用 命令配置用于管理管理中心 FMC 的数据接口，则必须在管理中心 FMC 中手动进行匹配的配置更改，然后确认更改。**configure network management-data-interface** 这些接口更改无法自动进行。

本程序介绍在需要时如何手动同步设备以及如何确认检测到的更改。如果设备更改为临时性的，则不应在 管理中心 中保存更改；而应等待设备稳定后重新同步。

开始之前

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 如果需要，请点击 **接口**左上方的 **同步设备** 。

步骤 3 检测到更改后，请参阅以下步骤。

添加或删除物理接口

a) 您可以在 **接口** 上看到红色横幅，表明接口配置已发生更改。点击**点击了解详情**链接以查看接口更改。

b) 点击**验证更改 (Validate Changes)** 以确保策略在接口更改后仍有效。

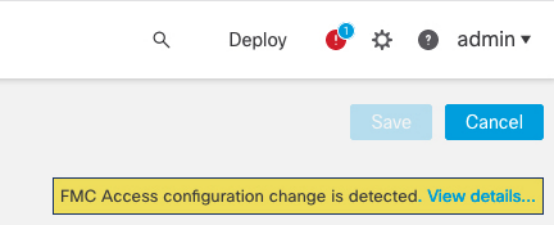
如出现任何错误，则需要更改配置并重新运行验证。

c) 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。

FMC 访问接口更改

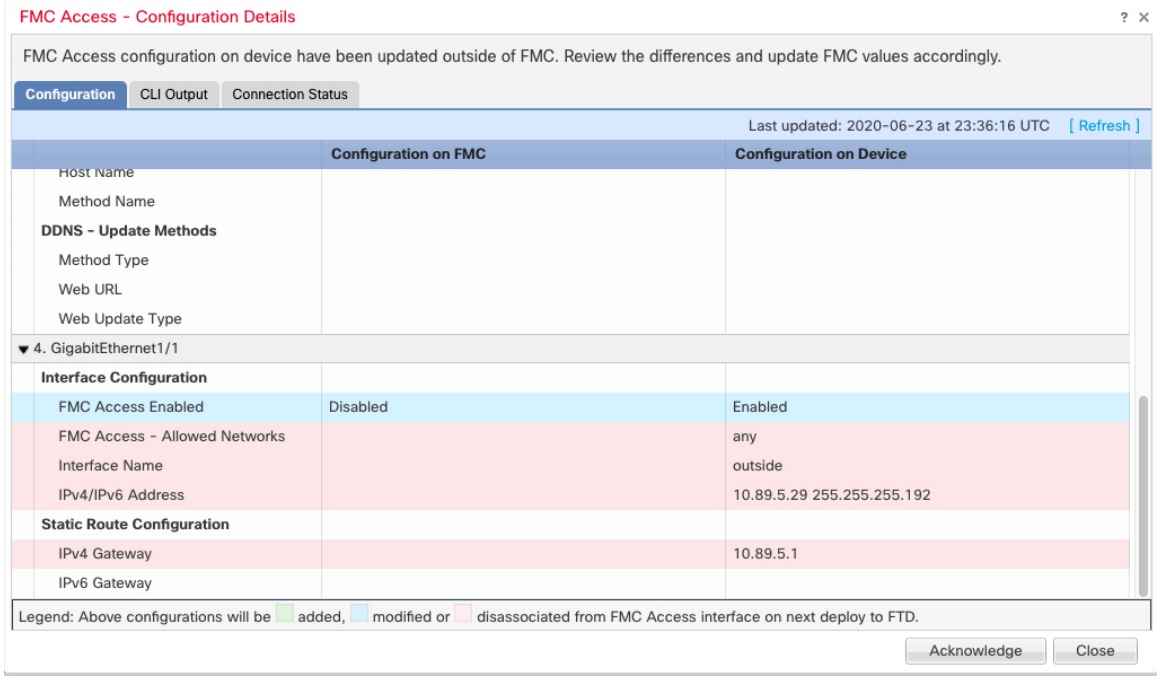
a) 您将在 “**设备**” 页面的右上角看到一个黄色横幅，指示 管理中心 访问配置已更改。点击 **查看详情** 链接以查看接口更改。



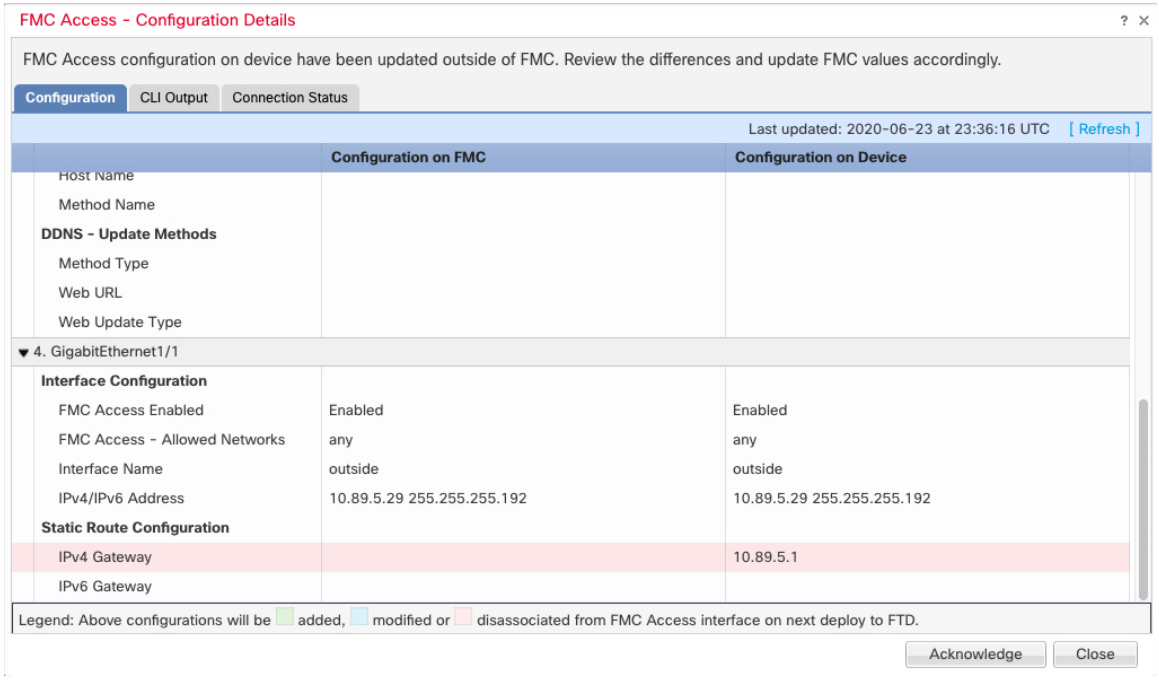
系统将打开 **FMC 访问 - 配置详细信息** 对话框。

b) 记下所有突出显示的配置，尤其是粉红色突出显示的配置。您需要通过在 管理中心上手动配置来匹配 威胁防御 上的任何值。

例如，下面的粉红色突出显示 威胁防御 上存在但尚不存在于 管理中心的配置。



以下示例显示在管理中心中配置接口后的此页面；接口设置匹配，并且已删除粉红色突出显示。



c) 点击 **确认**。

我们建议您在完成管理中心配置并准备部署之前，不要点击 **确认**。点击 **确认** 将删除部署阻止。下次部署时，管理中心 配置将覆盖 威胁防御 上任何剩余的冲突设置。在您重新部署之前，您有责任在 管理中心 中手动修复配置。

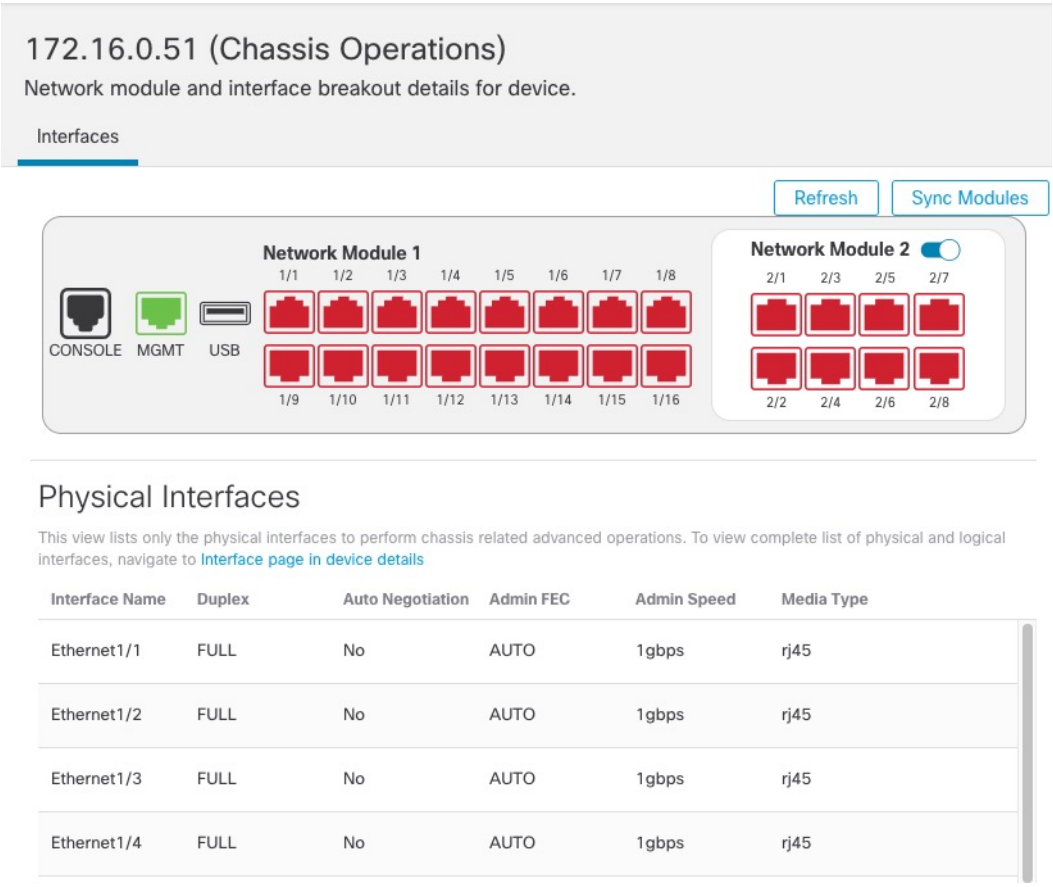
d) 此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。

管理 Cisco Secure Firewall 3100 的网络模块

如果在首次打开防火墙之前安装网络模块，则无需执行任何操作；网络模块已启用并可供使用。

要查看设备的物理接口详细信息并管理网络模块，请打开**机箱操作 (Chassis Operations)** 页面。从 **设备** > **设备管理**，点击**机箱** 列中的 **管理**。对于集群或高可用性，此选项仅适用于控制节点/主用设备。系统将打开设备 **机箱操作** 页面。

图 *62*: 机箱操作



点击 **刷新** 以刷新接口状态。如果您在需要检测的设备上进行了硬件更改，请点击 **同步模块**。

如果您需要在初始启动后更改网络模块安装，请参阅以下程序。

配置分支端口

您可以为每个 40GB 或更高的接口配置 10GB 分支端口。此程序介绍如何断开和重新加入端口。分支端口可以像任何其他物理以太网端口一样使用，包括添加到 EtherChannel。

更改会立即生效；您不需要部署到设备。在中断或重新加入后，您无法回滚到之前的接口状态。

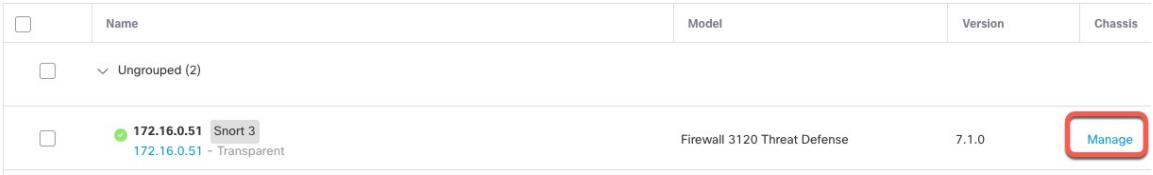
开始之前

- 您必须使用受支持的分支电缆。有关详细信息，请参阅硬件安装指南。
- 在中断或重新加入之前，接口不能用于以下对象：
  - 故障切换链路
  - 集群控制链路
  - 拥有一个子接口
  - EtherChannel 成员
  - BVI 成员
  - 管理器访问接口
- 中断或重新加入直接用于安全策略中的接口可能会影响配置；但是，操作不会被阻止。

过程

步骤 1 从 **设备** > **设备管理**，点击**机箱** 列中的 **管理** 。对于集群或高可用性，此选项仅适用于控制节点/主用设备；网络模块的更改会被复制到所有的节点。

图 *63:* 管理机箱



系统将打开设备的**机箱操作 (Chassis Operations)** 页面。此页面会显示设备的物理接口详细信息。

步骤 2 从 40GB 或更高的接口分支出 10GB 端口。

a) 点击接口右侧的 **中断**（）。

在确认对话框中点击**是 (Yes)**。如果接口正在使用，您将看到一条错误消息。您必须先解决任何使用案例，然后才能重试分支。

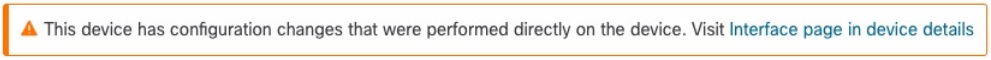
例如，要拆分出 Ethernet2/1 40GB 接口，生成的子接口将被标识为 Ethernet2/1/1、Ethernet2/1/2、Ethernet2/1/3 和 Ethernet2/1/4。

在接口图形上，断开的端口具有以下外观：

图 *64:* 分支端口

b) 点击屏幕顶部消息中的链接，转至**接口 (Interfaces)** 页面以保存接口更改。

图 *65:* 转到接口页面



c) 在**接口 (Interfaces)** 页面顶部，点击**点击了解更多信息 (Click to know more)**。系统将打开**接口更改 (Interface Changes)** 对话框。

图 *66:* 查看接口更改

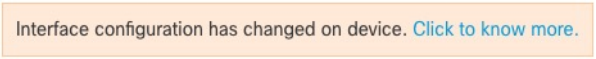
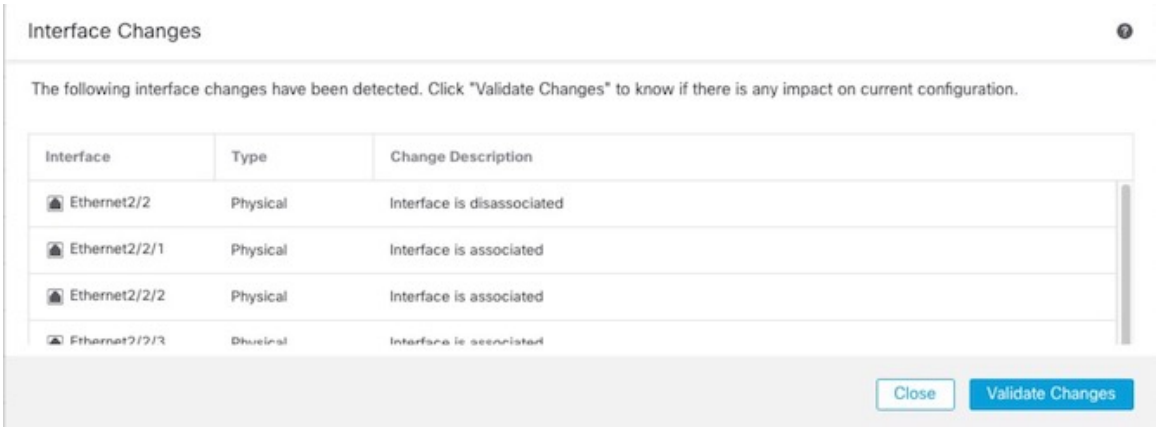


图 *67:* 接口更改



d) 点击**验证更改 (Validate Changes)** 以确保策略在接口更改后仍有效。

如出现任何错误，则需要更改配置并重新运行验证。

但是，删除安全策略中使用的接口会对配置造成影响。可以直接在配置中的很多位置引用接口，包括访问规则、NAT、SSL、身份规则、VPN、DHCP 服务器等。删除接口将删除与该接口相关的任何配置。引用安全区域的策略不受影响。

e) 点击**关闭 (Close)** 返回**接口 (Interfaces)** 页面。

f) 点击**保存 (Save)**，以便将接口更改保存到防火墙。

g) 如果您必须更改任何配置，请转至**部署 (Deploy)** > **部署 (Deployment)** 并部署策略。

您无需部署即可保存分支端口更改。

步骤 3 重新加入分支端口。

您必须重新加入该接口的所有子端口。

a) 点击接口右侧的 **加入**（）。

在确认对话框中点击**是 (Yes)**。如果有任何子端口正在使用，您将看到一条错误消息。您必须先解决任何使用案例，然后才能重试重新加入。

b) 点击屏幕顶部消息中的链接，转至**接口 (Interfaces)** 页面以保存接口更改。

图 *68:* 转到接口页面

c) 在**接口 (Interfaces)** 页面顶部，点击**点击了解更多信息 (Click to know more)**。系统将打开**接口更改 (Interface Changes)** 对话框。

图 *69:* 查看接口更改

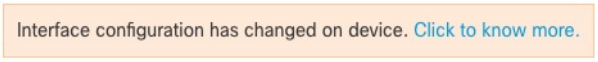
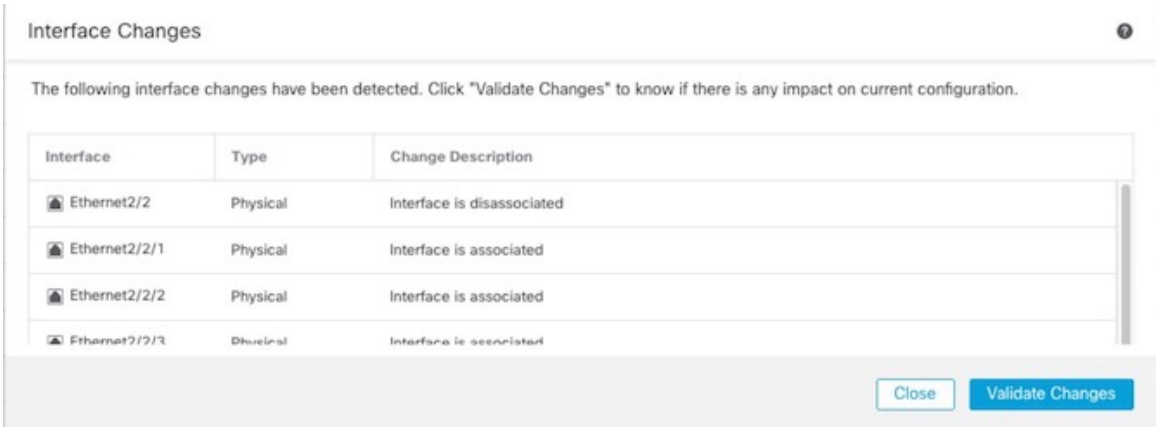


图 *70:* 接口更改



d) 点击**验证更改 (Validate Changes)** 以确保策略在接口更改后仍有效。

如出现任何错误，则需要更改配置并重新运行验证。

替换安全策略中使用的子接口可能会对配置造成影响。可以直接在配置中的很多位置引用接口，包括访问规则、NAT、SSL、身份规则、VPN、DHCP 服务器等。删除接口将删除与该接口相关的任何配置。引用安全区域的策略不受影响。

e) 点击**关闭 (Close)** 返回**接口 (Interfaces)** 页面。

f) 点击**保存 (Save)**，以便将接口更改保存到防火墙。

g) 如果您必须更改任何配置，请转至**部署 (Deploy)** > **部署 (Deployment)** 并部署策略。

您无需部署即可保存分支端口更改。

增加网络模块

要在初始启动后将网络模块添加到防火墙，请执行以下步骤。添加新模块需要重新启动。

过程

步骤 1 根据硬件安装指南安装网络模块。

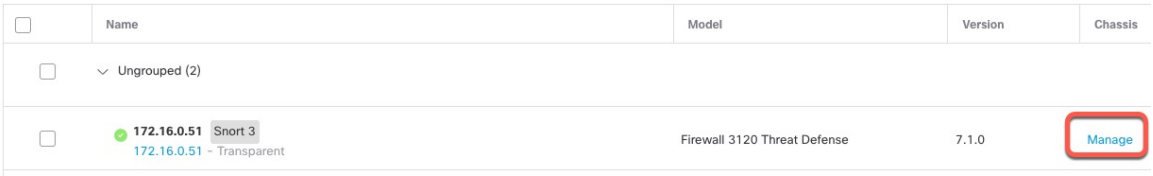
对于集群或高可用性，请在所有节点上安装网络模块。

步骤 2 重新启动防火墙；请参阅关闭设备，第 52 页。

对于集群或高可用性，请首先重新启动数据节点/备用设备，然后等待它们重新启动。然后，您可以更改控制节点（请参阅更改控制节点）或主用设备，并重新启动之前的控制节点/主用设备。

步骤 3 从 **设备** > **设备管理**，点击**机箱** 列中的 **管理** 。对于集群或高可用性，此选项仅适用于控制节点/主用设备；网络模块的更改会被复制到所有的节点。

图 *71:* 管理机箱

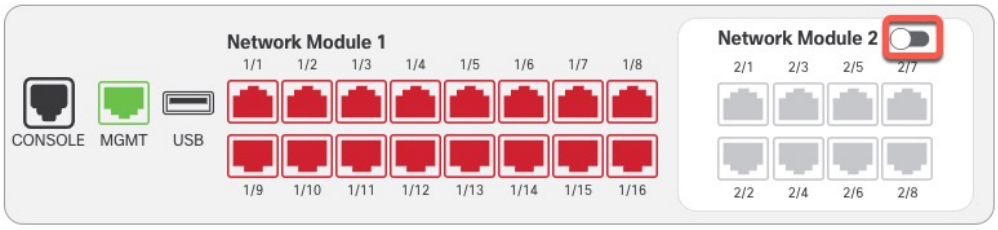


系统将打开设备 **机箱操作** 页面。此页面会显示设备的物理接口详细信息。

步骤 4 点击**同步模块 (Sync Modules)**，使用新的网络模块详细信息更新页面。

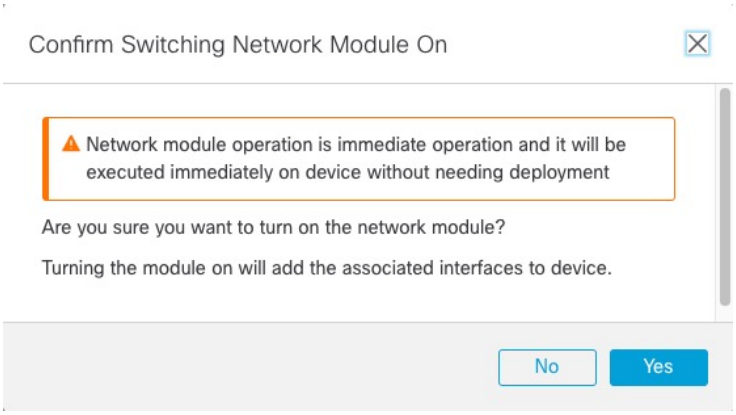
步骤 5 在接口图形上，点击滑块（  ）以启用网络模块。

图 *72:* 启用网络模块



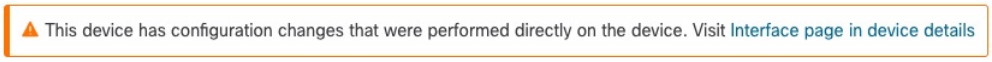
步骤 6 系统将提示您确认是否要开启网络模块。点击 **Yes**。

图 *73:* 确认启用



步骤 7 您会在屏幕顶部看到一条消息；点击链接可转至**接口 (Interfaces)** 页面以保存接口更改。

图 *74:* 转到接口页面



步骤 8 （可选）在**接口 (Interfaces)** 页面顶部，您会看到接口配置已更改的消息。您可以点击**点击了解更多 (Click to know more)** 打开**接口更改 (Interface Changes)** 对话框以查看更改。

图 *75:* 查看接口更改

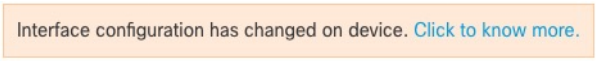
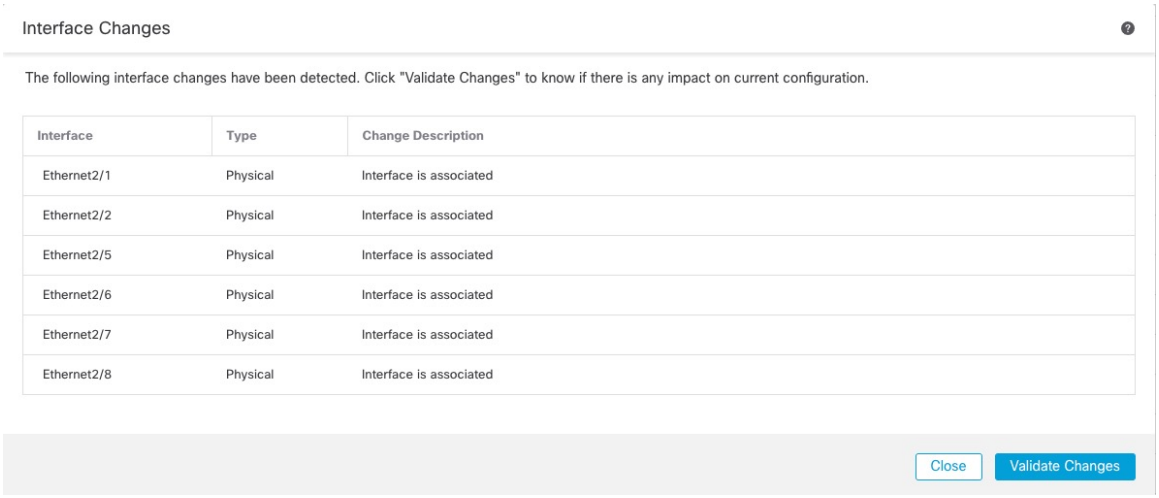


图 *76:* 接口更改



点击**关闭 (Close)** 返回**接口 (Interfaces)** 页面。（由于您要添加新模块，因此不应有任何配置影响，所以您无需点击**验证更改 (Validate Changes)**。）

步骤 9 点击**保存 (Save)**，以便将接口更改保存到防火墙。

热插拔网络模块

您可以将网络模块热插拔为相同类型的新模块，而无需重新启动。但是，您必须关闭当前模块才能安全地将其删除。此程序介绍如何关闭旧模块、安装新模块以及如何启用它。

对于群集或高可用性，您只能在控制节点/主用设备上执行机箱操作。如果集群控制链路/故障转移链路在模块上，则不能禁用该模块。

开始之前

过程

步骤 1 对于集群或高可用性，请执行以下步骤。

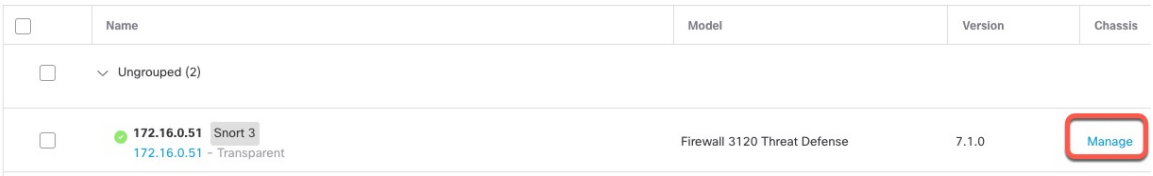
- **集群 (Clustering)** - 确保要执行热插拔的设备是数据节点；然后中断节点，使其不再位于集群中。

  在执行热插拔后，您需要将节点添加回集群。或者，您可以在控制节点上执行所有操作，然后网络模块更改将同步到所有数据节点。但在热插拔期间，您将无法在所有节点上使用这些接口。

- **高可用性 (High Availability)** - 要在禁用网络模块时避免故障切换，请执行以下操作：
  - 如果故障切换链路位于网络模块上，则必须中断高可用性。请参阅高可用性对中的独立设备，第 480 页。不允许禁用具有主动故障切换链路的网络模块。
  - 对网络模块上的接口禁用接口监控。请参阅配置备用 IP 地址和接口监控，第 474 页。

步骤 2 从 **设备** > **设备管理**，点击**机箱** 列中的 **管理** 。对于集群或高可用性，此选项仅适用于控制节点/主用设备；网络模块的更改会被复制到所有的节点。

图 77: 管理机箱



系统将打开设备 **机箱操作** 页面。此页面会显示设备的物理接口详细信息。

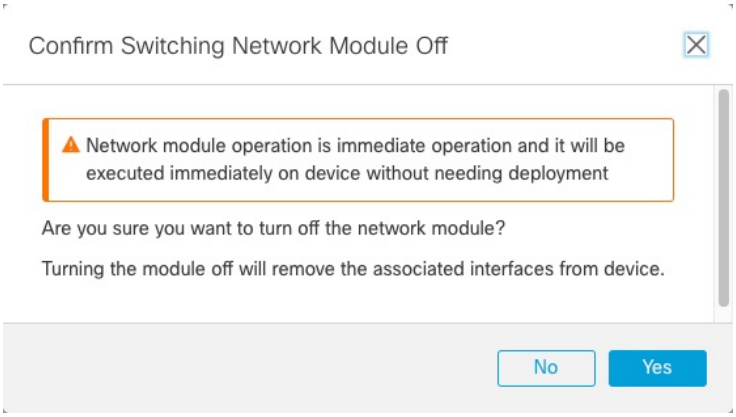
步骤 3 在接口图形上，点击滑块 （ ） 以禁用网络模块。

图 *78:* 禁用网络模块

不要在**接口 (Interfaces)** 页面上保存任何更改。由于您要更换网络模块，因此您不会希望中断任何现有配置。

步骤 4 系统将提示您确认是否要关闭网络模块。点击 **Yes**。

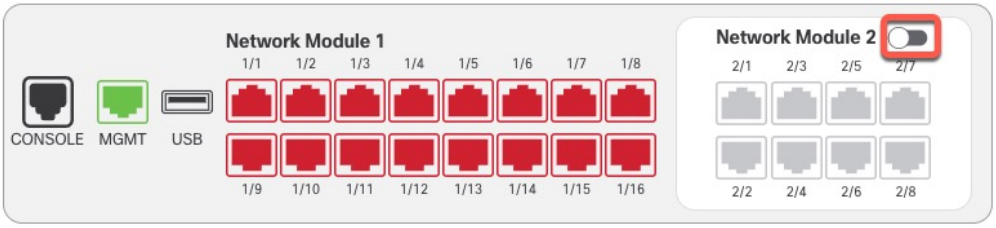
图 *79:* 确认禁用



步骤 5 在设备上，根据硬件安装指南，取下旧的网络模块并更换为新的网络模块。

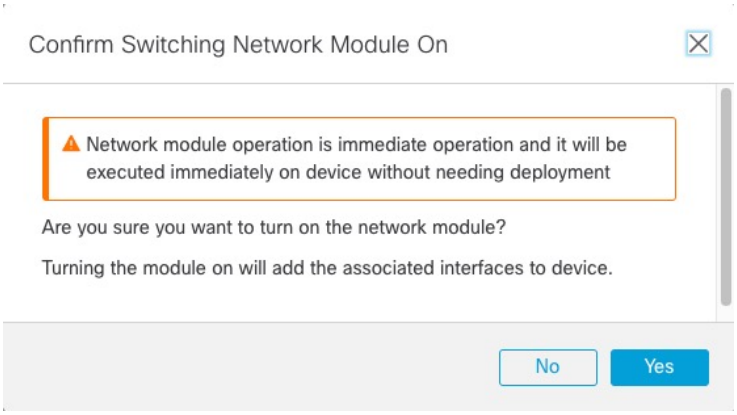
步骤 6 在 管理中心 中，通过点击滑块 （ ） 来启用新模块。

图 *80:* 启用网络模块



步骤 7 系统将提示您确认是否要开启网络模块。点击 **Yes**。

图 *81:* 确认启用



步骤 8 对于集群或高可用性，请执行以下步骤。

- **群集 (Clustering)** - 将节点添加回集群。
- **高可用性 (High Availability)** -
  - 如果您中断了高可用性，则要重新构建高可用性。请参阅添加 威胁防御 高可用性对 ， 第 471 页。
  - 为网络模块上的接口重新启用接口监控。请参阅配置备用 IP 地址和接口监控 ， 第 474 页。

将网络模块更换为其他类型

如果您更换了其他类型的网络模块，则需要重新启动。如果新模块的接口少于旧模块，则必须手动删除与不再存在的接口相关的任何配置。

对于群集或高可用性，您只能在控制节点/主用设备上执行机箱操作。

开始之前

对于高可用性，如果故障切换链路在模块上，则不能禁用该网络模块。您必须中断高可用性（请参阅高可用性对中的独立设备 ， 第 480 页），这意味着您会在重新启动主用设备时遇到停机。设备完成重新启动后，您可以重新设置高可用性。

过程

步骤 1 对于集群或高可用性，请执行以下步骤。

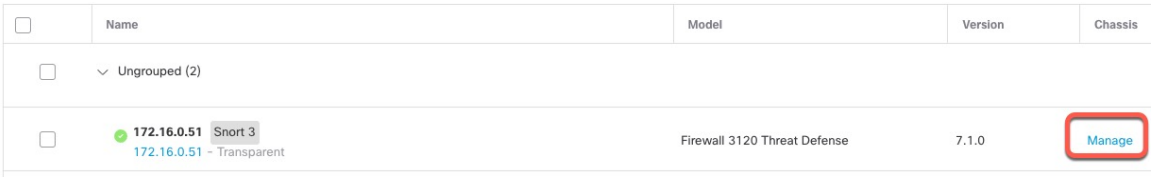
- **群集** - 为避免停机，您可以一次中断每个节点，使其在执行网络模块更换时不再位于集群中。

  执行替换后，您需要将节点添加回集群。

- **高可用性** - 要在更换网络模块时避免故障转移，请对网络模块上的接口禁用接口监控。请参阅配置备用 IP 地址和接口监控，第 474 页。

步骤 2 从 **设备** > **设备管理**，点击**机箱** 列中的 **管理** 。对于集群或高可用性，此选项仅适用于控制节点/主用设备；网络模块的更改会被复制到所有的节点。

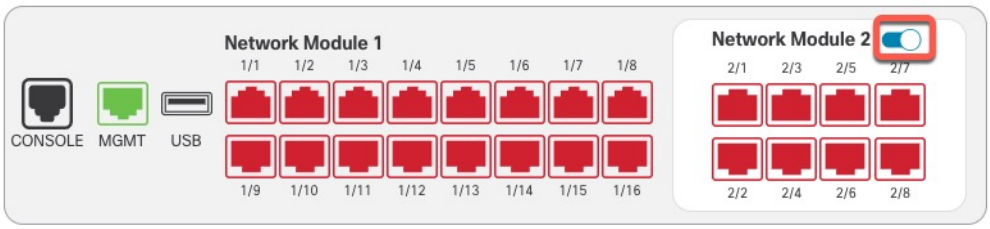
图 *82:* 管理机箱



系统将打开设备 **机箱操作** 页面。此页面会显示设备的物理接口详细信息。

步骤 3 在接口图形上，点击滑块 （ ） 以禁用网络模块。

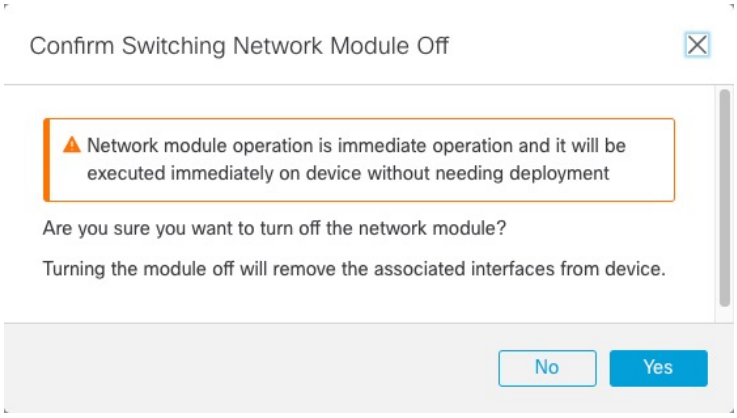
图 *83:* 禁用网络模块



不要在**接口 (Interfaces)** 页面上保存任何更改。由于您要更换网络模块，因此您不会希望中断任何现有配置。

步骤 4 系统将提示您确认是否要关闭网络模块。点击 **Yes**。

图 *84:* 确认禁用



步骤 5 在设备上，根据硬件安装指南，取下旧的网络模块并更换为新的网络模块。

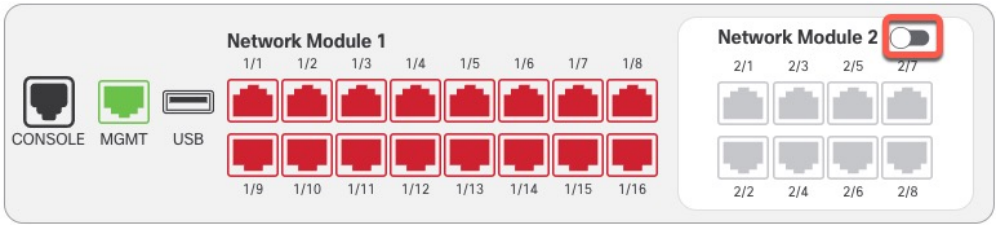
步骤 6 重新启动防火墙；请参阅关闭设备，第 52 页。

对于集群或高可用性，请首先重新启动数据节点/备用设备，然后等待它们重新启动。然后，您可以更改控制节点（请参阅更改控制节点）或主用设备，并重新启动之前的控制节点/主用设备。

步骤 7 在 管理中心 中，点击**同步模块 (Sync Modules)** 以便使用新的网络模块详细信息来更新页面。

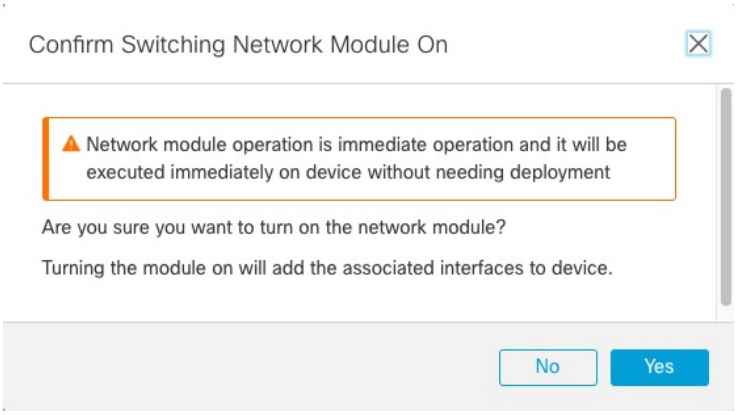
步骤 8 通过点击滑块启用新模块（  ）。

图 ***85:*** 启用网络模块



步骤 9 系统将提示您确认是否要开启网络模块。点击 **Yes**。

图 ***86:*** 确认启用



步骤 10 点击屏幕顶部消息中的链接，转至**接口 (Interfaces)** 页面以保存接口更改。

图 ***87:*** 转到接口页面

步骤 11 如果网络模块的接口较少：

a) 在**接口 (Interfaces)** 页面顶部，点击**点击了解更多信息 (Click to know more)**。系统将打开**接口更改 (Interface Changes)** 对话框。

图 ***88:*** 查看接口更改

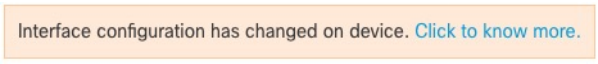
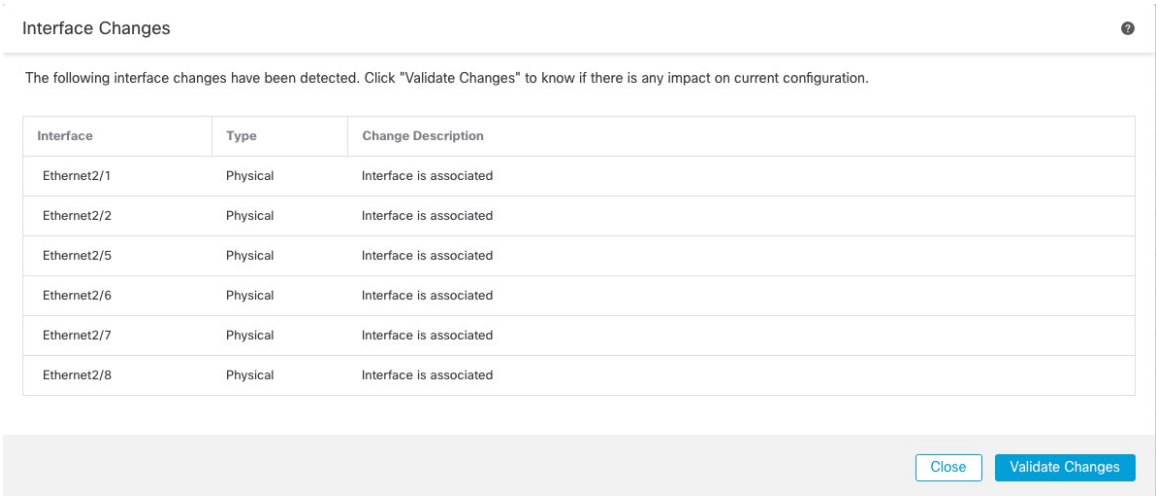


图 *89:* 接口更改



b) 点击**验证更改 (Validate Changes)** 以确保策略在接口更改后仍有效。

如出现任何错误，则需要更改配置并重新运行验证。

删除安全策略中使用的接口会影响配置。可以直接在配置中的很多位置引用接口，包括访问规则、NAT、SSL、身份规则、VPN、DHCP 服务器等。删除接口将删除与该接口相关的任何配置。引用安全区域的策略不受影响。

c) 点击**关闭 (Close)** 返回**接口 (Interfaces)** 页面。

步骤 12 要更改接口速度，请参阅 启用物理接口并配置以太网设置，第 496 页。

默认速度设置为“检测 SFP”，用于检测已安装的 SFP 的正确速度。仅当您手动将速度设置为特定值并且现在需要新的速度时，才需要修复速度。

步骤 13 点击**保存 (Save)**，以便将接口更改保存到防火墙。

步骤 14 如果您必须更改任何配置，请转至**部署 (Deploy)** > **部署 (Deployment)** 并部署策略。

无需部署即可保存网络模块更改。

步骤 15 对于集群或高可用性，请执行以下步骤。

- **群集 (Clustering)** - 将节点添加回集群。
- **高可用性 (High Availability)** - 对网络模块上的接口重新启用接口监控。请参阅配置备用 IP 地址和接口监控，第 474 页。

拆卸网络模块

如果要永久删除网络模块，请执行以下步骤。拆卸网络模块需要重新启动。

对于群集或高可用性，您只能在控制节点/主用设备上执行机箱操作。

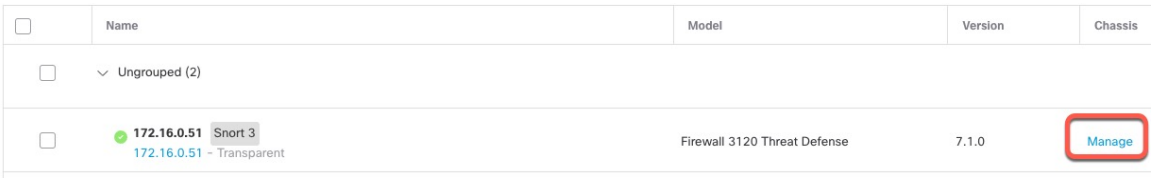
开始之前

对于集群或高可用性，请确保集群/故障转移链路不在网络模块上。

过程

步骤 1 从 **设备** > **设备管理**，点击**机箱** 列中的 **管理** 。对于集群或高可用性，此选项仅适用于控制节点/主用设备；网络模块的更改会被复制到所有的节点。

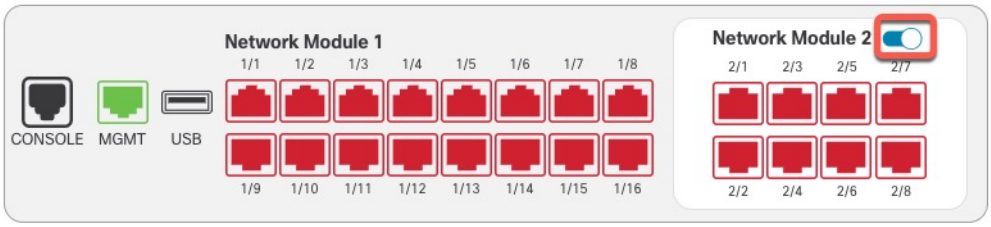
图 *90:* 管理机箱



系统将打开设备 **机箱操作** 页面。此页面会显示设备的物理接口详细信息。

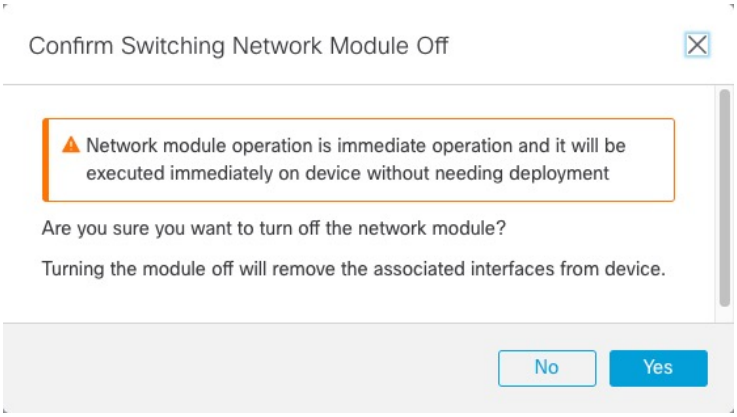
步骤 2 在接口图形上，点击滑块 （ ） 以禁用网络模块。

图 *91:* 禁用网络模块



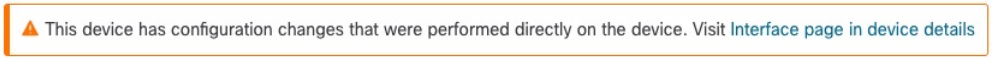
步骤 3 系统将提示您确认是否要关闭网络模块。点击 **Yes**。

图 *92:* 确认禁用



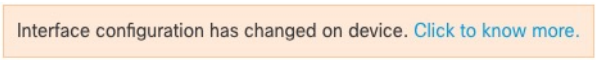
步骤 4 您会在屏幕顶部看到一条消息；点击链接可转至**接口 (Interfaces)** 页面以保存接口更改。

图 *93:* 转到接口页面



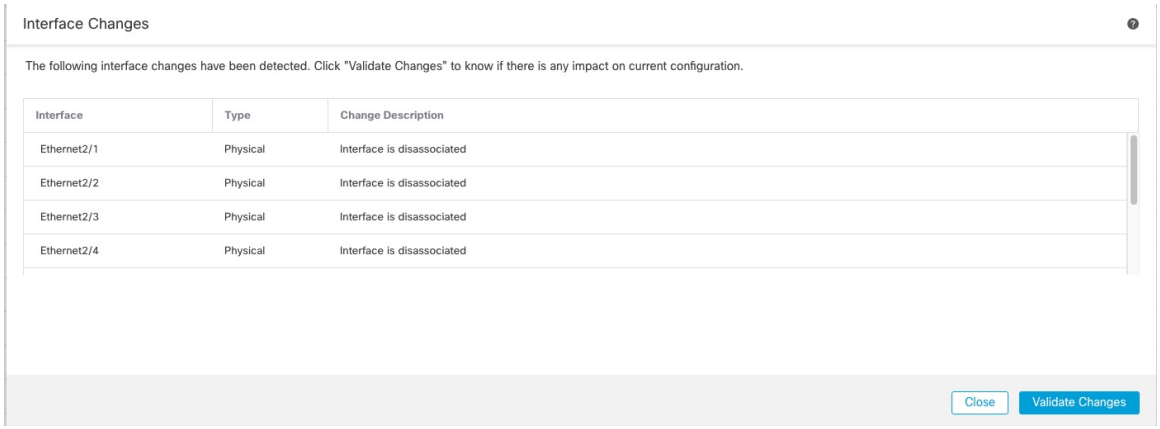
步骤 5 在**接口 (Interfaces)** 页面顶部，您会看到接口配置已更改的消息。

图 *94:* 查看接口更改



a) 点击**点击了解更多 (Click to know more)** 打开**接口更改 (Interface Changes)** 对话框以查看更改。

图 *95:* 接口更改



b) 点击**验证更改 (Validate Changes)** 以确保策略在接口更改后仍有效。

如出现任何错误，则需要更改配置并重新运行验证。

删除安全策略中使用的接口会影响配置。可以直接在配置中的很多位置引用接口，包括访问规则、NAT、SSL、身份规则、VPN、DHCP 服务器等。删除接口将删除与该接口相关的任何配置。引用安全区域的策略不受影响。

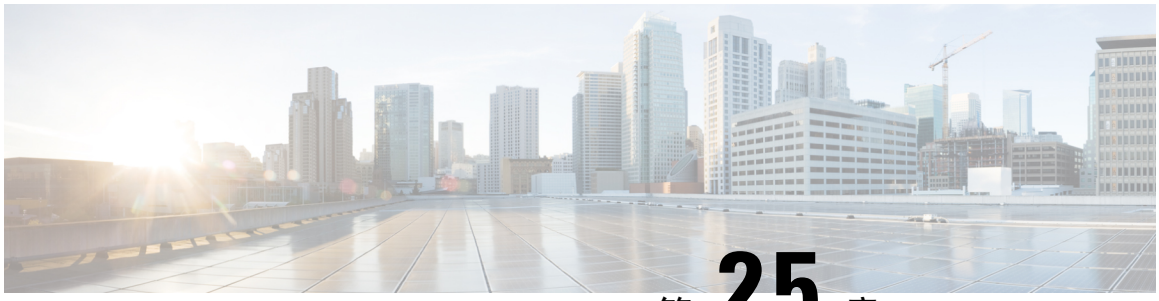
c) 点击**关闭 (Close)** 返回**接口 (Interfaces)** 页面。

步骤 6 点击**保存 (Save)**，以便将接口更改保存到防火墙。

步骤 7 如果您必须更改任何配置，请转至**部署 (Deploy)** > **部署 (Deployment)** 并部署策略。

步骤 8 重新启动防火墙；请参阅关闭设备，第 52 页。

对于集群或高可用性，请首先重新启动数据节点/备用设备，然后等待它们重新启动。然后，您可以更改控制节点（请参阅更改控制节点）或主用设备，并重新启动之前的控制节点/主用设备。



第 25 章

常规防火墙接口

本章包括常规防火墙 威胁防御 接口配置，包括 EtherChannel、VLAN 子接口、IP 寻址等。

注释 有关 Firepower 4100/9300上的初始接口配置，请参阅配置接口，第 423 页。

常规防火墙接口的要求和必备条件

型号支持

威胁防御

用户角色

- 管理员
- 访问管理员
- 网络管理员

配置 Firepower 1010 交换机端口

可以将各 Firepower 1010 接口配置为作为常规防火墙接口或第 2 层硬件交换机端口运行。这部分包括用于启动交换机端口配置的任务，包括启用或禁用交换模式以及创建 VLAN 接口和将它们分配给 VLAN。本节还介绍如何在受支持接口上自定义以太网供电 (PoE)。

关于 Firepower 1010 交换机端口

本节介绍 Firepower 1010 的交换机端口。

了解 Firepower 1010 端口和接口

端口和接口

对于各物理 Firepower 1010 接口，可以将其操作设置为防火墙接口或交换机端口。请参阅以下有关物理接口和端口类型的信息，以及为其分配交换机端口的逻辑 VLAN 接口：

- 物理防火墙接口 - 在路由模式下，这些接口使用已配置的安全策略在第 3 层网络之间转发流量，以应用防火墙和 VPN 服务。 在透明模式下，这些接口是桥接组成员，用于在第 2 层同一网络上的接口之间转发流量，使用已配置的安全策略应用防火墙服务。在路由模式下，还可以将集成路由和桥接与某些接口一起用作桥接组成员，将其他接口用作第 3 层接口。默认情况下，以太网 1/1 接口配置为防火墙接口。 还可以将这些接口配置为仅限 IPS（内联集和被动接口）。
- 物理交换机端口 - 交换机端口使用硬件中的交换功能在第 2 层转发流量。同一 VLAN 上的交换机端口可使用硬件交换互相通信，且流量不受 威胁防御安全策略的限制。接入端口仅接受未标记流量，可以将其分配给单个 VLAN。中继端口接受未标记和已标记流量，且可以属于多个 VLAN。默认情况下，以太网 1/2 至 1/8 配置为 VLAN 1 上的接入交换机端口。不能将 诊断接口配置为交换机端口。
- 逻辑 VLAN 接口 - 这些接口的运行方式与物理防火墙接口相同，但不同的是，无法创建子接口仅 IPS 接口（内联集和被动接口）或 EtherChannel 接口。如果交换机端口需要与另一个网络进行通信，则 威胁防御 设备将安全策略应用至 VLAN 接口，并路由至另一个逻辑 VLAN 接口或防火墙接口。甚至可以将集成路由和桥接与 VLAN 接口一起用作桥接组成员。同一 VLAN 上的交换机端口之间的流量不受安全策略 威胁防御的限制，但桥接组中 VLAN 之间的流量会受到安全策略的限制，因此，可以选择将桥接组和交换机端口进行分层，以在某些分段之间实施安全策略。

以太网供电

以太网 1/7 和以太网 1/8 支持以太网供电+ (PoE+)。

Auto-MDI/MDIX 功能

如果是所有 Firepower 1010 接口，默认的自动协商设置还包括 Auto-MDI/MDIX 功能。Auto-MDI/MDIX 在自动协商阶段检测直通电缆时执行内部交叉，从而消除交叉布线的需要。如要启用接口的

Auto-MDI/MDIX，必须将速度或双工设置为自动协商。如果将速度和双工明确设置为固定值，从而禁用了两种设置的自动协商，则 Auto-MDI/MDIX 也将被禁用。当速度和双工被设置为 1000 和全值时，接口始终会自动协商；因此，Auto-MDI/MDIX 始终会启用，且您无法禁用它。

Firepower 1010 交换机端口准则和限制

高可用性和集群

- 无集群支持。
- 使用高可用性时，不应使用交换机端口功能。由于交换机端口在硬件中运行，因此会继续在主用设备 和备用设备上传输流量。高可用性旨在防止流量通过备用设备，但此功能不会扩展至交换机端口。在正常 高可用性网络设置中，两台设备上的活动交换机端口将导致网络环路。建议将外部交换机用于任何交换功能。请注意，VLAN 接口可通过故障转移监控，而交换机端口无法通过故障转移监控。理论上，您可以将单个交换机端口置于 VLAN 上并成功使用 高可用性，但更简单的设置是改用物理防火墙接口。
- 仅可使用防火墙接口作为故障转移链路。

逻辑 VLAN 接口

- 您可以创建多达 60 个 VLAN 接口。
- 如果还在防火墙接口上使用 VLAN 子接口，则无法使用与逻辑 VLAN 接口相同的 VLAN ID。
- MAC 地址：
  - 路由防火墙模式 - 所有 VLAN 接口共享一个 MAC 地址。确保所有连接的交换机均可支持此方案。如果连接的交换机需要唯一MAC地址，可手动分配MAC地址。请参阅配置MAC地址，第 569 页。
  - 透明防火墙模式 - 每个 VLAN 接口都有唯一的 MAC 地址。如有需要，您可通过手动分配 MAC 地址覆盖生成的 MAC 地址。请参阅配置 MAC 地址，第 569 页。

网桥组

您不能将逻辑 VLAN 接口和物理防火墙接口混合在同一个网桥组中。

VLAN 接口和交换机端口不支持的功能

VLAN 接口和交换机端口不支持：

- 动态路由
- 组播路由
- 等价多路径路由 (ECMP)
- 内联集或被动接口

- EtherChannel
- 故障转移和状态链路
- 安全组标记 (SGT)

其他准则和限制

- 您最多可以在 Firepower 1010 上配置 60 个命名接口。
- 不能将 诊断接口配置为交换机端口。

默认设置

- 以太网 1/1 是一个防火墙接口。
- 以太网 1/2 至以太网 1/8 是分配给 VLAN 1 的交换机端口。
- 默认速度和复用 - 默认情况下，速度和复用设置为自动协商。

配置交换机端口和以太网供电

要配置交换机端口和 PoE，请完成以下任务。

启用或禁用交换机端口模式

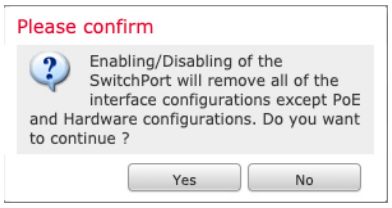
您可以将每个接口单独设置为防火墙接口或交换机端口。默认情况下，以太网 1/1 是防火墙接口，而剩余的以太网接口则配置为交换机端口。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击**交换机端口 (SwitchPort)** 列中的滑块，设置交换机端口模式，使其显示为 **滑块已启用**（）或 **滑块已禁用**（）。

默认情况下，交换机端口在 VLAN 1 中会被设为访问模式。您必须手动添加逻辑 VLAN 1 接口（或为这些交换机端口设置的任何 VLAN），以便路由流量并参与 FTD 安全策略（请参阅配置 VLAN 接口，第 521 页）。您无法将管理接口设置为交换机端口模式。更改交换机端口模式时，会删除所有不支持的配置：



配置 VLAN 接口

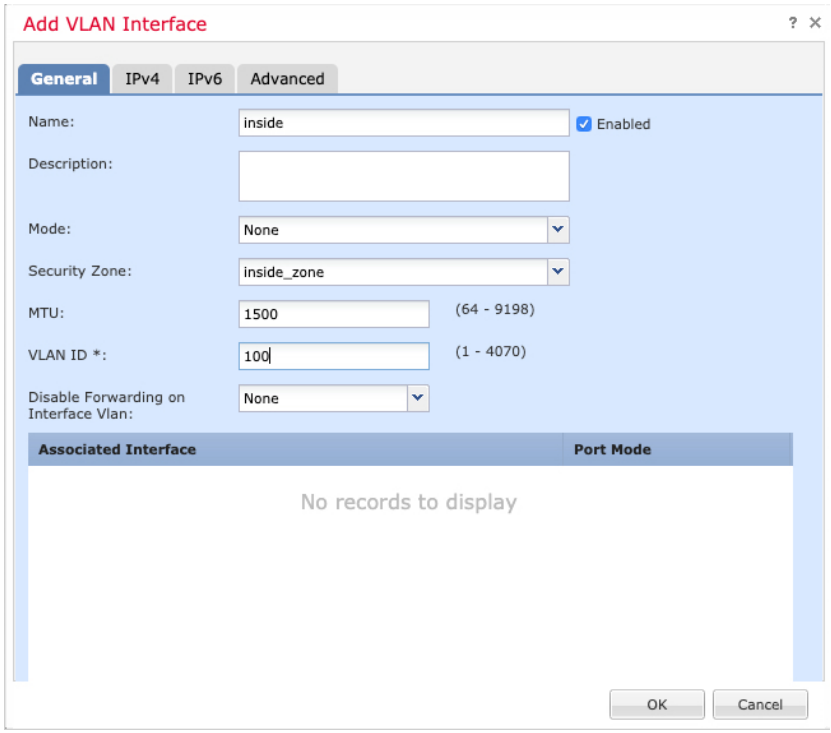
本节介绍如何配置 VLAN 接口以用于关联交换机端口。默认情况下，交换机端口分配给 VLAN1；但是，您必须手动添加逻辑 1 接口（或为这些交换机端口设置的任何 VLAN），以便路由流量并参与 FTD 安全策略。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击**添加接口 (Add Interfaces)** > **VLAN 接口 (VLAN Interface)**。

步骤 3 在 **常规**上，设置以下 VLAN 特定参数：



如果编辑的是现有 VLAN 接口，则 **关联接口** 表会显示此 VLAN 上的交换机端口。

a) 设置 **VLAN ID**，介于 1 和 4070 之间，不包括 3968 到 4047 范围内的ID（保留供内部使用）。

保存接口后，无法更改 VLAN ID；VLAN ID 既是使用的 VLAN 标记，也是您的配置中的接口 ID。

b) （可选）为 **接口 VLAN 上的禁用转发** 选择 VLAN ID，以禁用转发到另一个 VLAN。

例如，您有一个 VLAN 分配给外部以供互联网访问，另一个 VLAN 分配给内部企业网络，第三个 VLAN 分配给您的家庭网络。家庭网络无需访问企业网络，因此，您可以禁用家庭 VLAN 上的转发；企业网络可以访问家庭网络，但家庭网络不能访问企业网络。

步骤 4 要完成接口配置，请参阅以下过程之一：

- 配置路由模式接口，第 551 页
- 配置常规网桥组成员接口参数，第 555 页

步骤 5 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

将交换机端口配置为接入端口

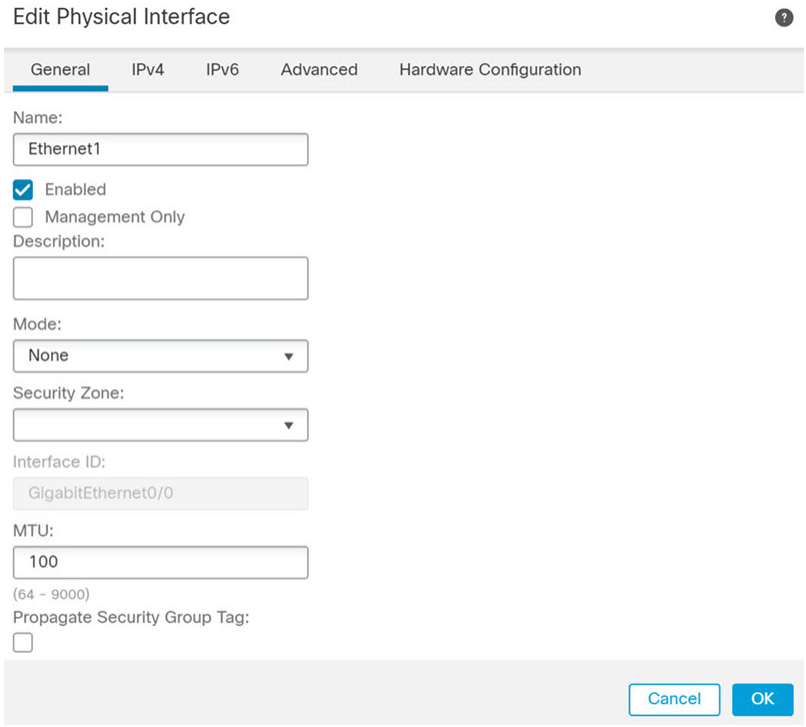
要将交换机端口分配给单个 VLAN，请将其配置为接入端口。接入端口仅接受未标记流量。默认情况下，以太网 1/2 至以太网 1/8 交换机端口会被分配给 VLAN 1。

注释 Firepower 1010 不支持在网络中进行环路检测的生成树协议。因此，您必须确保与 FTD 的任何连接均不会在网络环路中结束。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（✎）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑**（✎）。



步骤 3 选中**启用**复选框以启用此接口。

步骤 4 （可选） 在**说明**字段中添加说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 5 将**端口模式 (Port Mode)** 设为**访问 (Access)**。

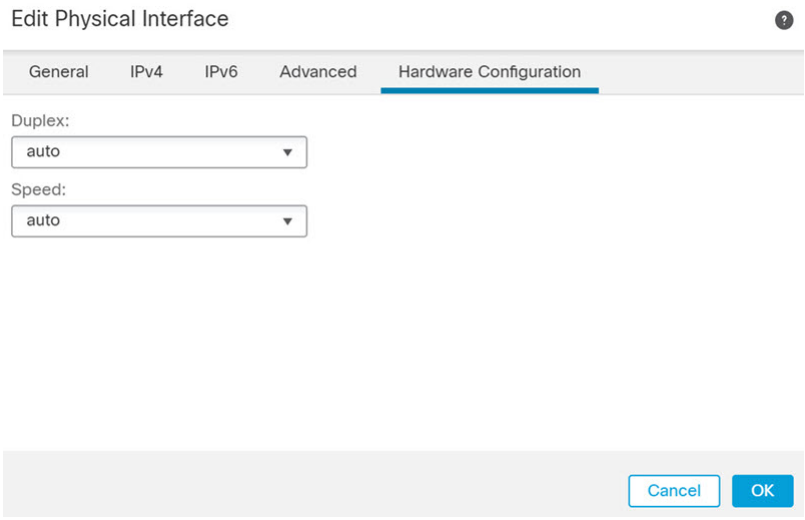
步骤 6 在 **VLAN ID** 字段中，设置此交换机端口的 VLAN，范围介于 1 和 4070 之间。

默认的 VLAN ID 为 1。

步骤 7 （可选） 选中**受保护 (Protected)** 复选框以将此交换机端口设置为受保护端口， 因此您可以阻止交换机端口与同一 VLAN 上的其他受保护交换机端口进行通信。

在以下情况下，您可能想要防止交换机端口相互之间进行通信：主要从其他 VLAN 访问这些交换机端口上的设备；您不需要允许 VLAN 间访问；如出现病毒感染或其他安全漏洞，则需要将设备相互隔离开。例如，如果具有托管 3 台 Web 服务器的 DMZ，当您在交换机端口上启用**受保护 (Protected)** 后，则可以将 Web 服务器相互隔离。内部网络和外部网络均可以与这 3 台网络服务器进行通信，反之亦然，但这些网络服务器相互之间无法进行通信。

步骤 8 （可选） 点击**硬件配置 (Hardware Configuration)**，设置双工和速度。



选中**自动协商 (Auto-negotiation)** 复选框（默认）以自动检测速度和双工。如果取消选中，您可以手动设置速度和双工：

- **复用**—选择 **全** 或 **半**。
- **速度 (Speed)** - 选择 **10mbps**、**100mbps** 或 **1gbps**。

步骤 9 点击**确定 (OK)**。

步骤 10 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

将交换机端口配置为中继端口

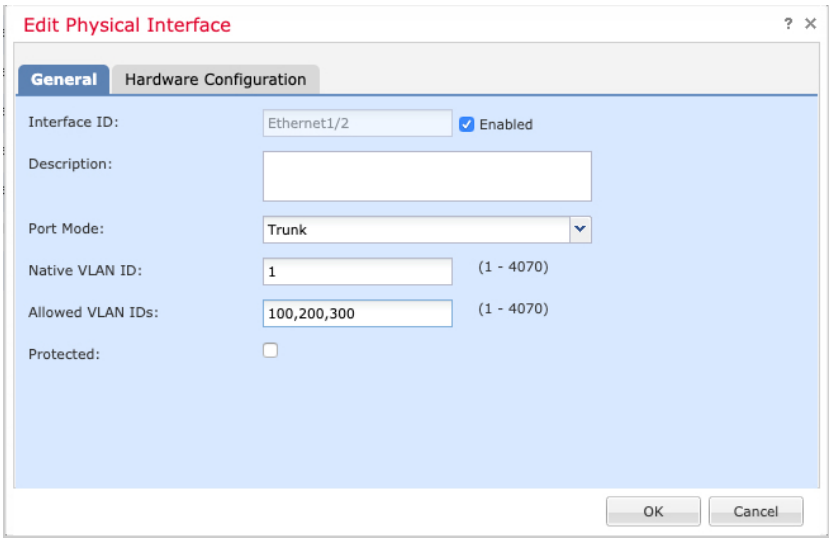
此程序介绍如何创建可以使用 802.1 Q 标记传输多个 VLAN 的中继端口。中继端口接受未标记和标记流量。允许的 VLAN 上的流量通过中继端口保持不变。

中继端口接收未标记流量后将其标记为本地 VLAN ID，以便 ASA 可以将流量转发至正确交换机端口，或可以将流量路由至另一个防火墙接口。如果 ASA 从中继端口发送本地 VLAN ID 流量，则会删除 VLAN 标记。请务必在另一台交换机上的中继端口上设置相同的本地 VLAN，以便将未标记流量标记至同一 VLAN。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（✎）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑**（✎）。



步骤 3 选中**启用**复选框以启用此接口。

步骤 4 （可选） 在**说明**字段中添加说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 5 将**端口模式 (Port Mode)** 设为**干线 (Trunk)**。

步骤 6 在**本地 VLAN ID (Native VLAN ID)** 字段中，设置此交换机端口的本地 VLAN，范围介于 1 和 4070 之间。

默认的本地 VLAN ID 为 1。

每个端口只能有一个本地 VLAN，但各端口的本地 VLAN 可以相同也可以不同。

步骤 7 在**允许的 VLAN ID (Allowed VLAN IDs)** 字段中，输入此中继端口的 VLAN，范围介于 1 和 4070 之间。

您可以通过以下方式之一识别最多 20 个ID：

- 单一编号 (n)
- 范围 (n-x)
- 用逗号将编号和范围隔开，例如：

  5,7-10,13,45-100

  您可以输入空格而不是逗号。

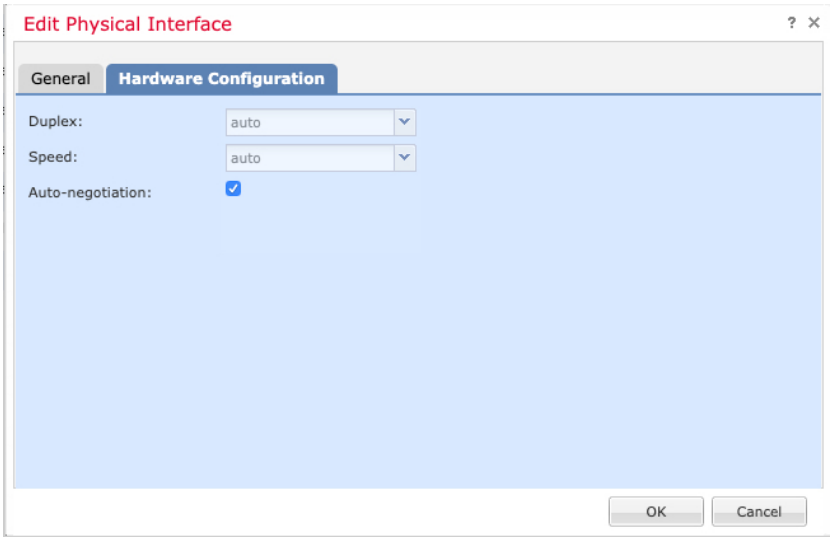
如果在此字段中包含本地 VLAN，则将忽略该本地 VLAN；从端口发送本地 VLAN 流量时，中继端口始终会删除 VLAN 标记。此外，不会接收仍具有 VLAN 标记的流量。

步骤 8 （可选） 选中**受保护 (Protected)** 复选框以将此交换机端口设置为受保护端口， 因此您可以阻止交换机端口与同一 VLAN 上的其他受保护交换机端口进行通信。

在以下情况下，您可能想要防止交换机端口相互之间进行通信：主要从其他 VLAN 访问这些交换机端口上的设备；您不需要允许 VLAN 间访问；如出现病毒感染或其他安全漏洞，则需要将设备相互

隔离开。例如，如果具有托管 3 台 Web 服务器的 DMZ，当您在交换机端口上启用**受保护 (Protected)** 后，则可以将 Web 服务器相互隔离。内部网络和外部网络均可以与这 3 台网络服务器进行通信，反之亦然，但这些网络服务器相互之间无法进行通信。

步骤 9 （可选） 点击**硬件配置 (Hardware Configuration)**，设置双工和速度。



选中**自动协商 (Auto-negotiation)** 复选框（默认）以自动检测速度和双工。如果取消选中，您可以手动设置速度和双工：

- **复用**—选择 **全** 或 **半**。
- **速度 (Speed)** - 选择 **10mbps**、**100mbps** 或 **1gbps**。

步骤 10 点击**确定 (OK)**。

步骤 11 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置以太网供电

以太网 1/7 和以太网 1/8 支持 IP 电话或无线接入点等设备的以太网供电 (PoE)。Firepower 1010 支持 IEEE 802.3af (PoE) 和 802.3at (PoE+)。PoE+ 使用链路层发现协议 (LLDP) 来协商功率级别。PoE+ 可以为受电设备提供 30 瓦的功率。仅在需要时提供功率。

如果关闭接口或者将接口配置为防火墙接口，则会禁用设备电源。

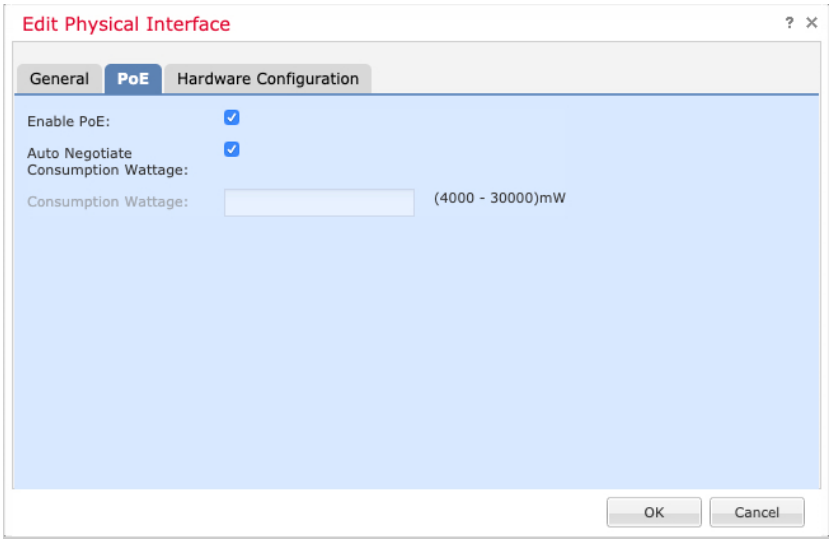
默认情况下，在以太网 1/7 和以太网 1/8 上启用 PoE。此过程介绍如何禁用和启用 PoE 以及如何设置可选参数。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击 Ethernet1/7 或 1/8 的 **编辑**（）。

步骤 3 点击 **PoE**。



步骤 4 选中**启用 PoE (Enable PoE)** 复选框。

默认情况下，PoE 处于启用状态。

步骤 5 （可选） 取消选中**自动协商功耗功率 (Auto Negotiate Consumption Wattage)** 复选框，如果您知道所需的确切功率，请输入**功耗功率 (Consumption Wattage)**。

默认情况下，PoE 使用适合受电设备类别的瓦数将电源自动传送至受电设备。Firepower 1010 使用 LLDP 进一步协商正确的瓦数。如果知道特定瓦数并想要禁用 LLDP 协商，请输入介于 4000 和 30000 毫瓦的值。

步骤 6 点击**确定 (OK)**。

步骤 7 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 EtherChannel 接口

本节介绍如何配置 EtherChannel 接口。

注释 对于 Firepower 4100/9300，可在 FXOS 中配置 EtherChannel。有关详细信息，请参阅添加 EtherChannel（端口通道），第 426 页。

关于 EtherChannels

本节介绍 EtherChannel 。

关于 EtherChannel

802.3ad EtherChannel 是逻辑接口（称为端口通道接口），该接口由一组单独的以太网链路（通道组）组成，以便可以提高单个网络的带宽。配置接口相关功能时，可以像使用物理接口一样来使用端口通道接口。

最多可以配置 48 个 Etherchannel，具体取决于型号支持的接口数量。

通道组接口

各信道组最多可以有 16 个活动接口，但 Firepower 1000，2100，Cisco Secure Firewall 3100 模块除外，支持 8 个活动接口。对于仅支持 8 个主用接口的交换机，您最多可以将 16 个接口分配给一个通道组：但仅有 8 个接口可用作主用接口，其余接口在出现接口故障的情况下用作备用链路。对于 16 个主用接口，请确保交换机支持此功能（例如，带有 F2 系列 10 千兆以太网模块的思科 Nexus 7000 支持此功能）。

通道组中的所有接口都必须属于同一类型且具有相同速度。添加到通道组的第一个接口确定正确的类型和速度。

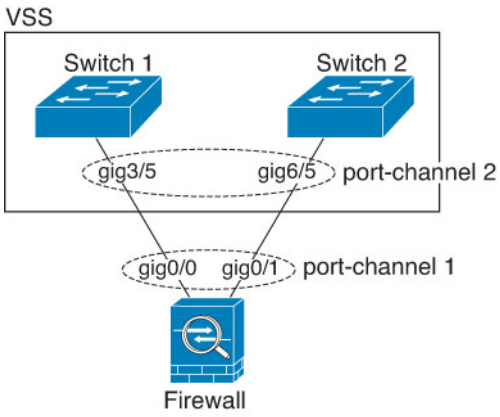
EtherChannel 汇聚通道中所有可用活动接口上的流量。系统根据源或目标 MAC 地址、IP 地址、TCP 端口号、UDP 端口号和 VLAN 编号使用专有散列算法来选择接口。

连接到其他设备上的 EtherChannel

威胁防御EtherChannel 连接到的设备还必须支持 802.3ad EtherChannel；例如，可以连接到 Catalyst 6500 交换机或 Cisco Nexus 7000。

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

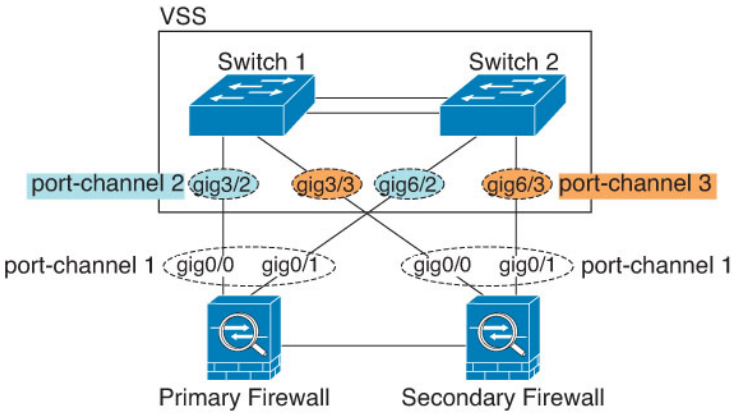
图 *96:* 连接至 ***VSS/vPC***



注释 如果 威胁防御 设备处于透明防火墙模式下，并且将 威胁防御 设备置于两组 VSS/vPC 交换机之间，请确保在使用 EtherChannel 连接到 威胁防御 设备的所有交换机端口上禁用单向链路检测 (UDLD)。如果启用 UDLD，则交换机端口可能会接收来自另一个 VSS/vPC 对中的两台交换机的 UDLD 数据包。接收交换机会将接收接口置于关闭状态，原因是“UDLD 邻居不匹配”。

如果您在主用/备用故障转移部署中使用 威胁防御 设备，则需要在 VSS/vPC 中的交换机上创建单独的 EtherChannel，为每个 威胁防御 设备创建一个。在每个 威胁防御 设备上，单个 EtherChannel 连接至两台交换机。即使您可以将所有的交换机接口分组到连接两个 威胁防御 设备的一个 EtherChannel 中（在这种情况下，将不会建立 EtherChannel，因为 威胁防御 系统 ID 是单独的），但单个 EtherChannel 并不可取，因为您不希望将流量发送到备用 威胁防御 设备。

图 *97:* 主用/备用故障转移和 ***VSS/vPC***



链路汇聚控制协议

链路汇聚控制协议 (LACP) 将在两个网络设备之间交换链路汇聚控制协议数据单元 (LACPDU)，进而汇聚接口。

您可以将 EtherChannel 中的每个物理接口配置为：

- Active - 发送和接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。
- 被动 - 接收 LACP 更新。备用 EtherChannel 只能与主用 EtherChannel 建立连接。在硬件型号上不受支持。
- 开启 - EtherChannel 始终开启，并且不使用 LACP。“开启”的 EtherChannel 只能与另一个“开启”的 EtherChannel 建立连接。

LACP 将协调自动添加和删除指向 EtherChannel 的链接，而无需用户干预。LACP 还会处理配置错误，并检查成员接口的两端是否连接到正确的通道组。如果接口发生故障且未检查连接和配置，“开启”模式将不能使用通道组中的备用接口。

负载均衡

威胁防御 设备通过对数据包的源 IP 地址和目标 IP 地址进行散列处理来将数据包分发给 EtherChannel 中的接口（此条件可配置）。在模数运算中，将得到的散列值除以主用链路数，得到的余数确定哪个接口拥有流量。*hash_value* **mod** *active_links* 结果为 0 的所有数据包都发往 EtherChannel 中的第一个接口，结果为 1 的发往第二个接口，结果为 2 的数据包发往第三个接口，依此类推。例如，如果您有 15 个主用链路，则模数运算的值为 0 到 14。如果有 6 个主用链路，则值为 0 到 5，依此类推。

如果主用接口发生故障且未由备用接口替代，则流量会在剩余的链路之间重新均衡。该故障会在第 2 层的生成树和第 3 层的路由表中被屏蔽，因此故障切换对其他网络设备是透明的。

EtherChannel MAC 地址

属于通道组一部分的所有接口都共享同一 MAC 地址。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。

Firepower 和 Cisco Secure Firewall 硬件

端口通道接口使用内部接口 Internal-Data 0/1 的 MAC 地址。或者，您可以为端口通道接口手动配置 MAC 地址。机箱上的所有 EtherChannel 接口都使用相同的 MAC 地址，因此请注意，例如，如果使用 SNMP 轮询，则多个接口将具有相同的 MAC 地址。

注释 成员接口仅在重新启动后使用内部数据 0/1 MAC 地址。在重新启动之前，成员接口使用自己的 MAC 地址。如果在重新启动后添加新的成员接口，则必须再次重新启动以更新其 MAC 地址。

EtherChannel 的准则

桥接组

在路由模式下，不支持将 管理中心-定义的 EtherChannel 接口作为桥接组成员。 Firepower 4100/9300 上的 Etherchannel 可以是网桥组成员。

高可用性

- 如果要将 EtherChannel 接口用作 高可用性 链路，则必须在 高可用性 对中的两台设备上预配置要使用的接口；不能在主设备上配置该接口并期望它会复制到辅助设备，因为复制需要 高可用性链路本身。
- 如果要将 EtherChannel 接口用于状态链路，则无需特殊配置；可以照常从主设备复制配置。Firepower 4100/9300 机箱 的所有接口（包括 EtherChannel）均需在两台设备上进行预配置。
- 可以使用 **monitor-interface** 命令监控 EtherChannel 余接口 以实现高可用性 ；请务必引用逻辑冗余接口名称。如果主用成员接口故障切换到备用接口，则此活动不会在监控设备级高可用性时导致 EtherChannel 接口出现故障。仅在所有物理接口都出现故障的情况下，EtherChannel 接口或 EtherChannel 接口才会出现故障（对于 EtherChannel 接口，可配置允许出现故障的成员接口数量）。
- 如果将 EtherChannel 接口用于高可用性或状态链路，然后防止无序数据包，则仅会使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。您不能在 EtherChannel 配置用作高可用性链路时对其进行修改。要修改配置，您需要暂时禁用高可用性，以防止在此期间发生高可用性。

型号支持

- 无法在 管理中心 中添加用于 Firepower 4100/9300 或 threat defense virtual的 EtherChannel。Firepower 4100/9300 支持 EtherChannel，但必须在机箱上的 FXOS 中执行 EtherChannel 的所有硬件配置。
- 无法在 Etherchannel 中使用 Firepower 1010 交换机端口或 VLAN 接口。

《通用 EtherChannel 准则》

- 最多可以配置 48 个 Etherchannel，具体取决于型号可用的接口数量。
- 各信道组最多可以有 16 个活动接口，但 Firepower 1000，2100，Cisco Secure Firewall 3100 模块除外，支持 8 个活动接口。对于仅支持 8 个主用接口的交换机，您最多可以将 16 个接口分配给一个通道组：但仅有 8 个接口可用作主用接口，其余接口在出现接口故障的情况下用作备用链路。对于 16 个主用接口，请确保交换机支持此功能（例如，带有 F2 系列 10 千兆以太网模块的思科 Nexus 7000 支持此功能）。
- 通道组中的所有接口都必须具有相同的介质类型和速度能力。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。不能通过在较大容量的接口上将速度设置为较低来混合接口容量（例如 1GB 和 10GB 接口），但 Cisco Secure Firewall 3100 除外，它支持不同的接口容量，只要速度设置为检测 SFP；在此情况下会使用较低的常见速度。
- 威胁防御EtherChannel 连接到的设备还必须支持 802.3ad EtherChannel。
- 威胁防御 设备不支持带有 VLAN 标记的 LACPDU。如果使用 Cisco IOS **vlan dot1Q tag native** 命令在相邻交换机上启用本地 VLAN 标记，则 威胁防御 设备将会丢弃已标记的 LACPDU。请务必禁用相邻交换机上的本地 VLAN 标记。

- Firepower 1000, Firepower 2100，Cisco Secure Firewall 3100 不支持快速 LACP 速率；LACP 始终使用正常速率。此设置不可配置。请注意，在 FXOS 中配置 EtherChannel 的 Firepower 4100/9300 默认将 LACP 速率设置为快速；在这些平台上，速率是可配置的。
- 在低于 15.1(1)S2 的 Cisco IOS 软件版本中， 威胁防御 不支持将 EtherChannel 连接到交换机堆叠。在默认交换机设置下，如果跨堆叠连接 威胁防御 EtherChannel，则当主要交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。要提高兼容性，请将 **stack-mac persistent timer** 命令设置为足够大的值，以将重载时间计算在内；例如，可将其设置为 8 分钟，或设置为 0 以表示无穷大。或者，您可以升级到更加稳定的交换机软件版本，例如 15.1(1)S2。
- 所有 威胁防御 配置均引用 EtherChannel 接口，而不是成员物理接口。

配置 EtherChannel

本节介绍如何创建 EtherChannel 端口通道接口，如何向 EtherChannel 分配接口，以及如何自定义 EtherChannel。

指南

- 最多可以配置 48 个 Etherchannel，具体取决于型号具有的接口数量。
- 各信道组最多可以有 8 个活动接口，但 ISA 3000 除外，支持 16 个活动接口。对于仅支持 8 个主用接口的交换机，您最多可以将 16 个接口分配给一个通道组：但仅有 8 个接口可用作主用接口，其余接口在出现接口故障的情况下用作备用链路。
- 通道组中的所有接口都必须具有相同的介质类型和速度能力。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。不能通过在较大容量的接口上将速度设置为较低来混合接口容量（例如 1GB 和 10GB 接口），但 Cisco Secure Firewall 3100 除外，它支持不同的接口容量，只要速度设置为检测 SFP；在此情况下会使用较低的常见速度。

注释 对于 Firepower 4100/9300，可在 FXOS 中配置 EtherChannel。有关详细信息，请参阅添加 EtherChannel（端口通道），第 426 页。

开始之前

- 如果已为物理接口配置了名称，则不能将该物理接口添加到通道组。您必须先删除该名称。

注释 如果使用的是配置中已有的物理接口，则删除名称将会清除引用该接口的任何配置。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 根据启用物理接口并配置以太网设置，第 496 页启用成员接口。

步骤 3 点击**添加接口** > **以太通道接口**。

步骤 4 在 **常规** 选项卡上，将 **以太通道 ID** 设置为介于 1 和 48 之间的数字 （1-8 针对于 Firepower 1010）。

步骤 5 在**可用接口**区域中，点击某个接口对，然后点击**添加**，以将其移动至**选定的接口**区域。对要使其成为成员的所有接口重复此步骤。

确保所有接口的类型和速度相同。

步骤 6 （可选） 点击**高级**选项卡可自定义 EtherChannel。在**信息**子选项卡上设置下列参数：

- （仅限 ISA 3000） **负载均衡**-选择在组通道接口之间对数据包进行负载均衡所用的标准。默认情况下，威胁防御 根据数据包的源 IP 地址和目标 IP 地址来均衡接口上的数据包负载。如果要更改分类数据包所依据的属性，请选择另一组条件。例如，如果流量严重偏向于相同的源 IP 地址和目标 IP 地址，则分配给 EtherChannel 中的接口的流量将失去平衡。更改为其他算法可使流量分布更均匀。有关负载均衡的详细信息，请参阅负载均衡，第 530 页。
- **LACP 模式** - 选择“主动”、“被动”或“启用”。我们建议使用 Active 模式（默认）。
- （仅限 ISA 3000） **主用物理接口: 范围**-从左侧的下拉列表中，选择 EtherChannel 要作为主用接口所需的最小主用接口数量（1 到 16）。默认值为 1。从右侧的下拉列表中，选择 EtherChannel 中允许的最大主用接口数量（1 到 16）。默认值为 16。如果交换机不支持 16 个主用接口，请务必将此命令设置为 8 或更小的值。
- **主用 Mac 地址** - 如果需要，请设置手动 MAC 地址。mac_address 的格式为 H.H.H，其中 H 是 16 位十六进制数字。例如， MAC 地址 00-0C-F1-42-4C-DE 以 000C.F142.4CDE 的形式输入。

步骤 7 点击 **硬件配置** 选项卡，并为所有成员接口设置复用和速度。

步骤 8 点击 **OK**。

步骤 9 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

步骤 10 （可选） 添加 VLAN 子接口请参阅添加子接口，第 535 页。

步骤 11 配置路由或透明模式接口参数。请参阅配置路由模式接口，第 551 页或配置网桥组接口，第 555 页。

配置 VLAN 子接口和 802.1Q 中继

通过 VLAN 子接口，您可以将物理接口、冗余接口或 EtherChannel 接口划分为标记有不同 VLAN ID 的多个逻辑接口。带有一个或多个 VLAN 子接口的接口将自动配置为 802.1Q 中继。由于 VLAN 允

许您在特定物理接口上将流量分开，所以您可以增加网络中可用的接口数量，而无需增加物理接口或设备。

VLAN 子接口的指南和限制

型号支持

- Firepower 1010 - 交换机端口或 VLAN 接口上不支持 VLAN 子接口。

高可用性和群集

不能将子接口用于故障切换或状态链路，或用于集群控制链路。多实例模式例外：您可以为这些链路使用 机箱 定义的子接口。

其他准则

- 防止物理接口上的未标记数据包 - 如果使用子接口，则通常表明也不希望物理接口传递流量，因为物理接口会传递未标记的数据包。此属性对冗余接口对中的主用物理接口以及 EtherChannel 链路同样适用。由于必须启用物理接口、冗余接口或 EtherChannel 接口才能使子接口传递流量，请通过不为接口配置名称来确保物理接口、冗余接口或 EtherChannel 接口不传递流量。如果要使物理接口、冗余接口或 EtherChannel 接口传递未标记的数据包，可以照常配置名称。
- 您无法在管理接口上配置子接口。
- 同一父接口上的所有子接口必须为网桥组成员或路由接口；您无法混合搭配。
- 威胁防御不支持动态中继协议 (DTP)，因此您必须无条件地将连接的交换机端口配置到中继上。
- 您可能想要为 威胁防御 上定义的子接口分配唯一 MAC 地址，因为它们使用父接口上相同的固化 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 威胁防御 上特定实例内发生流量中断。

各设备型号的最大 VLAN 子接口数量

设备型号限制可配置的最大 VLAN 子接口数量。请注意，仅可在数据接口上而不可在管理接口上配置子接口。

下表介绍各设备型号的限制。

型号	最大 VLAN 子接口数量
Firepower 1010	60
Firepower 1120	512
Firepower 1140 和 1150	1024
Firepower 2100	1024

型号	最大 VLAN 子接口数量
Secure Firewall 3100	1024
Firepower 4100	1024
Firepower 9300	1024
Threat Defense Virtual	50
ISA 3000	100

添加子接口

向物理接口、冗余接口或 port-channel 接口添加一个或多个子接口。

对于 Firepower 4100/9300，您可以在 FXOS 中配置子接口用于容器实例；请参阅为容器实例添加 VLAN 子接口，第 429 页。这些子接口显示在 管理中心 接口列表中。您还可以在 管理中心 中添加子接口，但仅可在未于 FXOS 中定义子接口的父接口上进行操作。

注释 父物理接口会传递未标记的数据包。您可能不想传递未标记的数据包，因此请确保未在安全策略中包括父接口。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 根据启用物理接口并配置以太网设置，第 496 页启用父接口。

步骤 3 点击 **添加接口** > **子接口**。

步骤 4 在 **常规**上，设置以下参数：

a) **接口** - 选择要将子接口添加到的物理、冗余或端口通道接口。

b) **子接口 ID** - 以整数形式输入介于 1 和 4294967295 之间的子接口 ID。允许的子接口数因平台而异。此 ID 一旦设置便不可更改。

c) **VLAN ID** - 输入 VLAN ID，介于 1 和 4094 之间，用于标记该子接口上的数据包。

此 VLAN ID 对父接口必须为唯一。

步骤 5 点击 **OK**。

步骤 6 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

步骤 7 配置路由或透明模式接口参数。请参阅配置路由模式接口，第 551 页或配置网桥组接口，第 555 页。

配置 VXLAN 接口

本章介绍如何配置虚拟可扩展局域网 (VXLAN) 接口。VXLAN 接口作为第 3 层物理网络之上的第 2 层虚拟网络，可对第 2 层网络进行扩展。

关于 VXLAN 接口

VXLAN 提供与 VLAN 相同的以太网第 2 层网络服务，但其可扩展性和灵活性更为出色。与 VLAN 相比，VXLAN 提供以下优势：

- 可在整个数据中心中灵活部署多租户网段。
- 更高的可扩展性可提供更多的第 2 层网段，最多可达 1600 万个 VXLAN 网段。

本节介绍 VXLAN 如何工作。有关 VXLAN 的详细信息，请参阅 RFC 7348。有关 Geneve 的详细信息，请参阅 RFC 8926。

封装

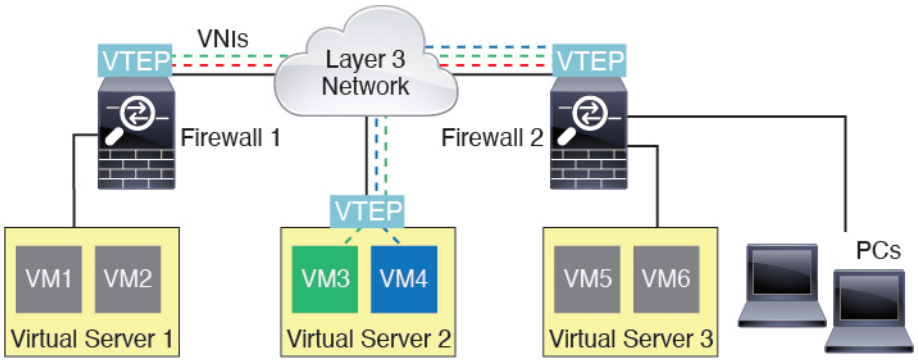
威胁防御 支持两种类型的 VXLAN 封装：

- VXLAN（所有型号）- VXLAN 使用 MAC Address-in-User 数据报协议 (MAC-in-UDP) 的封装方式。原始第 2 层帧已添加 VXLAN 报头，然后放入 UDP-IP 数据包中。
- Geneve（仅限 threat defense virtual）- Geneve 具有不限于 MAC 地址的灵活内部报头。要在 Amazon Web 服务 (AWS) 网关负载均衡器和设备之间透明路由数据包，以及发送额外信息，则需要使用 Geneve 封装。

VXLAN 隧道端点

VXLAN 隧道终端 (VTEP) 设备执行 VXLAN 封装和解封。每个 VTEP 有两种接口类型：一个或多个虚拟接口称为 VXLAN 网络标识符 (VNI) 接口，您可以向其应用安全策略；以及称为 VTEP 源接口的常规接口，用于为 VTEP 之间的 VNI 接口建立隧道。VTEP 源接口连接到传输 IP 网络，进行 VTEP 至 VTEP 通信。

下图显示两个 威胁防御 和充当第 3 层网络中的 VTEP 的虚拟服务器 2，用于在站点之间扩展 VNI 1、2 和 3 网络。威胁防御 充当 VXLAN 和非 VXLAN 网络之间的网桥或网关。



VTEP 之间的底层 IP 网络与 VXLAN 重叠无关。封装的数据包根据外部 IP 地址报头路由，该报头具有初始 VTEP（用作源 IP 地址）和终止 VTEP（作为目标 IP 地址）。对于 VXLAN 封装：当远程 VTEP 未知时，目标 IP 地址可以是组播组。在使用 Geneve 时，威胁防御 仅支持静态对等体。默认情况下，VXLAN 的目标端口是 UDP 端口 4789（用户可配置）。Geneve 的目的端口是 6081。

VTEP 源接口

VTEP 源接口是一个计划要与所有 VNI 接口相关联的常规 接口（物理、EtherChannel 接口，甚至 VLAN 接口）。每个 threat defense virtual 设备可以配置一个 VTEP 源接口。 由于只能配置一个 VTEP 源接口，因此不能在同一设备上同时配置 VXLAN 和 Geneve 接口。AWS 上的 threat defense virtual 集群有一个例外，您可以在其中有两个 VTEP 源接口：一个 VXLAN 接口用于集群控制链路，一个 Geneve 接口可用于 AWS 网关负载均衡器。

尽管并未将 VTEP 源接口限制为全部用于传输 VXLAN 流量，但是可以实现该用途。如果需要，可以使用该接口传输常规流量，并将一个安全策略应用于传输此类流量的该接口。但是，对于 VXLAN 流量，必须对 VNI 接口应用所有安全策略。VTEP 接口仅作为物理端口。

在透明防火墙模式下，VTEP 源接口不是 BVI 的一部分，并且类似于对待管理接口的方式，不为该源接口配置 IP 地址。

VNI 接口

VNI 接口类似于 VLAN 接口：它们是虚拟接口，通过使用标记，实现网络流量在给定物理接口上的分离。将安全策略直接应用于每个 VNI 接口。

您智能添加一个 VTEP 接口，并且所有 VNI 接口都与同一 VTEP 接口相关联。AWS上的 threat defense virtual 集群例外。对于 AWS 集群，您可以在其中有两个 VTEP 源接口：一个 VXLAN 接口用于集群控制链路，一个 Geneve 接口可用于 AWS 网关负载均衡器。

VXLAN 数据包处理

VXLAN

进出 VTEP 源接口的流量取决于 VXLAN 处理，特别是封装或解封。

封装处理包括以下任务：

- VTEP 源接口通过 VXLAN 报头封装内部 MAC 帧。

- UDP 校验和字段设置为零。
- 外部帧源 IP 设置为 VTEP 接口 IP。
- 外部帧目标 IP 通过远程 VTEP IP 查找确定。

解封；威胁防御 仅在以下条件下解封 VXLAN 数据包：

- VXLAN 数据包是目标端口设置为 4789（用户可配置该值）的 UDP 数据包。
- 入口接口是 VTEP 源接口。
- 入口接口 IP 地址与目标 IP 地址相同。
- VXLAN 数据包格式符合标准。

日内瓦

进出 VTEP 源接口的流量取决于 Geneve 处理，特别是封装或解封。

封装处理包括以下任务：

- VTEP 源接口通过 Geneve 报头封装内部 MAC 帧。
- UDP 校验和字段设置为零。
- 外部帧源 IP 设置为 VTEP 接口 IP。
- 外部帧目标 IP 会被设置为您配置的对等体 IP 地址。

解封；ASA 仅在以下条件下解封 Geneve 数据包：

- VXLAN 数据包是目标端口设置为 6081（用户可配置该值）的 UDP 数据包。
- 入口接口是 VTEP 源接口。
- 入口接口 IP 地址与目标 IP 地址相同。
- Geneve 数据包格式符合标准。

对等体 VTEP

当 威胁防御 将数据包发送到对等体 VTEP 之后的设备时，威胁防御 需要两条重要的信息：

- 远程设备的目标 MAC 地址
- 对等体 VTEP 的目标 IP 地址

威胁防御 会维护目标 MAC 地址到 VNI 接口的远程 VTEP IP 地址的映射。

VXLAN 对等体

有两种方法使 威胁防御 可以找到此信息：

- 可以在 威胁防御 上静态配置单个对等体 VTEP IP 地址。

然后， 威胁防御 设备将已封装 VXLAN 的 ARP 广播发送到 VTEP，以获取终端节点 MAC 地址。

- 可以在 威胁防御 上静态配置一组对等体 VTEP IP 地址。

  然后， 威胁防御 设备将已封装 VXLAN 的 ARP 广播发送到 VTEP，以获取终端节点 MAC 地址。

- 可以在每个 VNI 接口（或者总的来说，在 VTEP 上）配置组播组。

  威胁防御 将通过 VTEP 源接口在 IP 组播数据包内发送一个 VXLAN 封装的 ARP 广播数据包。对此 ARP 请求的响应使 威胁防御 可以获取远程终端节点的远程 VTEP IP 地址和目标 MAC 地址。

  Geneve 不支持此选项。

Geneve 对等体

threat defense virtual 仅支持静态定义的对等设备。您可以在 AWS 网关负载均衡器上定义 threat defense virtual 对等体 IP 地址。由于 threat defense virtual 绝不会向网关负载均衡器发起流量，因此您也不必在 threat defense virtual 上指定网关负载均衡器 IP 地址；它会在收到 Geneve 流量时获知对等体 IP 地址。Geneve 不支持组播组。

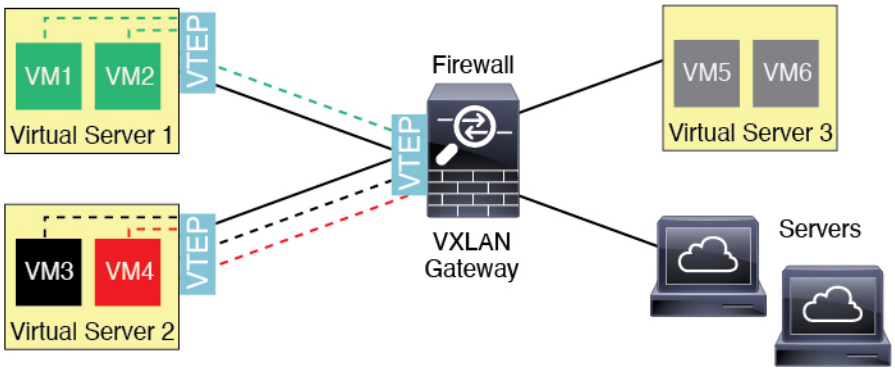
VXLAN 使用案例

本节介绍在 威胁防御 上实施 VXLAN 的使用案例。

VXLAN 网桥或网关概述

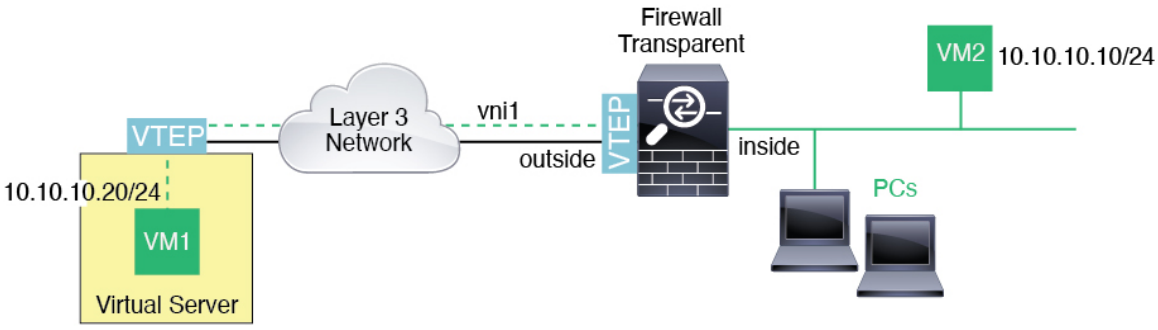
每个 威胁防御 VTEP 都可作为终端节点（例如 VM、服务器和 PC）和 VXLAN 重叠网络之间的网桥或网关。对于通过 VTEP 源接口借助 VXLAN 封装接收的传入帧，威胁防御 去掉 VXLAN 报头，并基于内部以太网帧的目标 MAC 地址，将传入帧转发到连接非 VXLAN 网络的物理接口。

威胁防御 始终会处理 VXLAN 数据包；而不仅仅是在两个其他 VTEP 之间转发未处理的 VXLAN 数据包。



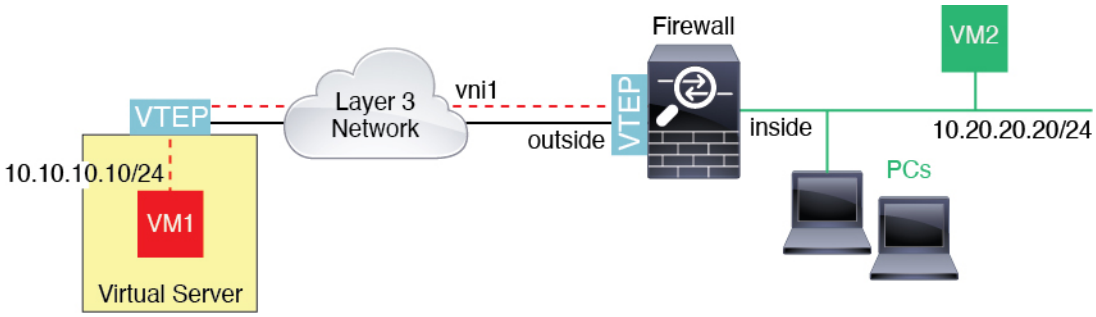
VXLAN 网桥

在使用网桥组（透明防火墙模式或可选的路由模式）时，威胁防御 可以用作 VXLAN 网段与本地网段之间的 VXLAN 网桥（远程），其中二者均位于同一网络中。在这种情况下，网桥组的一个成员是常规接口，而另一个成员是 VNI 接口。



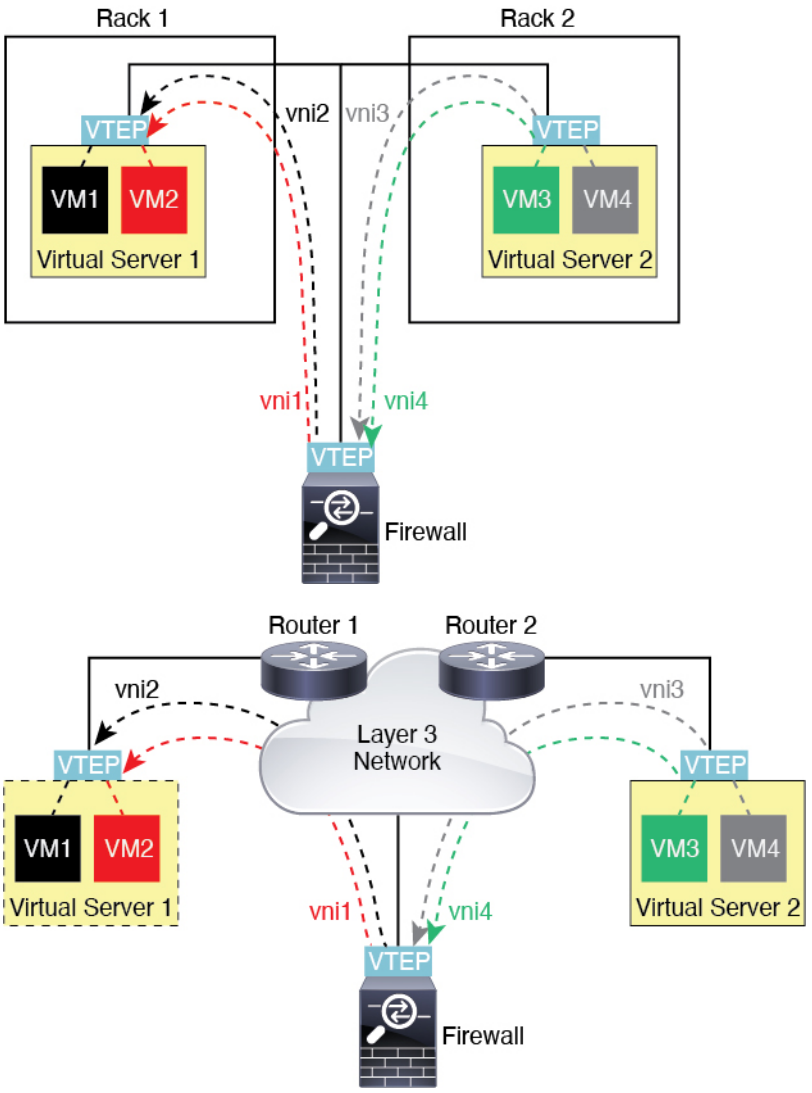
VXLAN 网关（路由模式）

威胁防御 可充当 VXLAN 和非 VXLAN 域之间的路由器，用于连接不同网络上的设备。



VXLAN 域之间的路由器

借助通过 VXLAN 扩展的第 2 层域，虚拟机可以指向一个 威胁防御 作为其网关，即使 威胁防御 位于不同机架中，甚至当 威胁防御 位于第 3 层网络上很远的位置也是如此。



请参阅有关此场景的以下注释：

1. 对于从 VM3 到 VM1 的数据包，目标 MAC 地址为 威胁防御 MAC 地址，因为 威胁防御 是默认网关。
2. 虚拟服务器 2 上的 VTEP 源接口接收来自 VM3 的数据包，然后使用 VNI 3 的 VXLAN 标签封装数据包，并将数据包发送到 威胁防御。
3. 当 威胁防御 接收数据包时，会解封数据包以获得内部帧。
4. 威胁防御 使用内部帧进行路由查找，然后发现目标位于 VNI 2 上。如果尚不具有 VM1 的映射，威胁防御 会在 VNI 2 上的组播组 IP 上发送封装的 ARP 广播。

注释 威胁防御 必须使用动态 VTEP 对等体发现，因为 ASA 在此场景下有多个 VTEP 对等体。

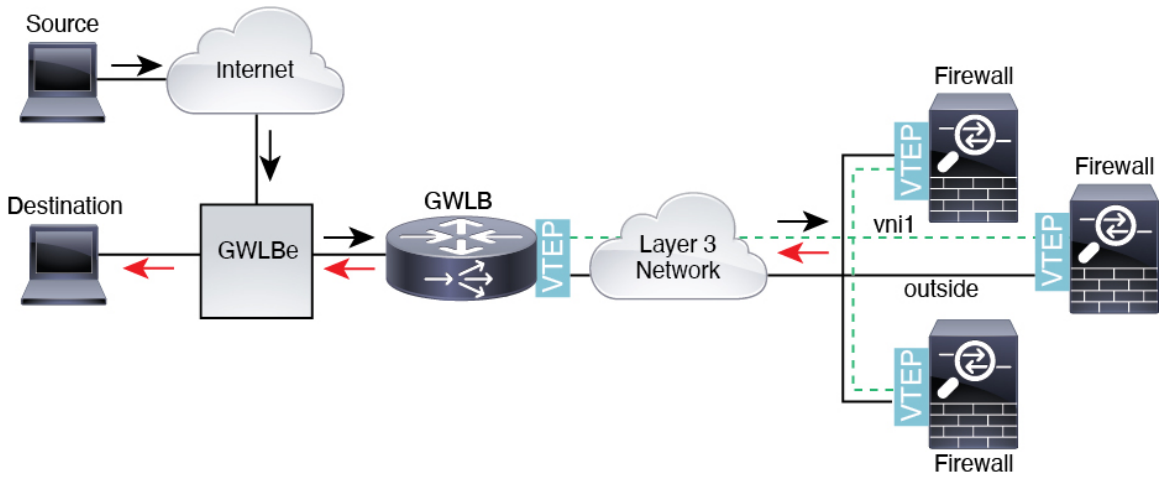
5. 威胁防御 再次使用 VXLAN 标签为 VNI 2 封装数据包，并且将数据包发送到虚拟服务器 1。在封装之前，威胁防御 将内部帧目标 MAC 地址更改为 VM1 的 MAC 地址（威胁防御 可能需要组播封装的 ARP，以获取 VM1 MAC 地址）。
6. 当虚拟服务器 1 接收 VXLAN 数据包时，该虚拟服务器会解封数据包并向 VM1 提供内部帧。

Geneve 单臂代理

注释 这是 Geneve 接口当前唯一支持的使用案例。

AWS 网关负载均衡器结合了透明网络网关和按需分配流量和扩展虚拟设备的负载均衡器。threat defense virtual 支持具有分布式数据平面的网关负载均衡器集中控制平面（网关负载均衡器终端）。下图显示了从网关负载均衡器终端转发到网关负载均衡器的流量。网关负载均衡器会在多个流量之间进行均衡，这些流量在丢弃流量或将其发送回网关负载均衡器之前对其进行检查（掉头流量）。threat defense virtual然后，网关负载均衡器会将流量发送回网关负载均衡器终端和目的地。

图 *98: Geneve* 单臂代理



VXLAN 接口的要求和必备条件

型号要求

- 不支持将 Firepower 1010 交换机端口和 VLAN 接口用作 VTEP 接口。
- 以下型号支持 Geneve 封装：
  - Amazon Web 服务 (AWS) 中的 Threat Defense Virtual

VXLAN 接口准则

防火墙模式

- Geneve 接口仅在路由防火墙模式下支持。

IPv6

- VNI 接口支持 IPv4 和 IPv6 流量。
- VTEP 源接口 IP 地址仅支持 IPv4。

集群

- 集群在单个接口模式下不支持 VXLAN，但集群控制链路除外（仅限threat defense virtual ）仅跨区以太网通道模式支持 VXLAN。

  而 AWS 是一个例外，它可以使用额外的 Geneve 接口与 GWLB 配合使用。

路由

- VNI 接口上仅支持静态路由或策略型路由；动态路由协议不受支持。

MTU

- VXLAN 封装-如果源接口 MTU 少于 1554 个字节，则 威胁防御 会自动将 MTU 提高到 1554 个字节。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的MTU。如果其他设备使用的 MTU 更大，则您应。对于 threat defense virtual，此 MTU 需要您重新启动以启用巨帧保留。
- Geneve 封装 (Geneve encapsulation) - 如果源接口 MTU 少于 1806 个字节，威胁防御 会自动将 MTU提高到1806个字节。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的MTU。如果其他设备使用的MTU更大，您应将源接口MTU设置为网络MTU+306个字节。此 MTU 需要您重新启动以启用巨帧保留。

配置 VXLAN 接口

要配置 VXLAN，请执行下列步骤：

注释 您可以配置 VXLAN 或 Geneve（仅限 threat defense virtual）。有关 Geneve 接口，请参阅配置 Geneve 接口 ，第 545 页。

1. 配置 VTEP 源接口 ，第 544 页。
2. 配置 VNI 接口 ，第 545 页。

配置 VTEP 源接口

每个 威胁防御 设备可以配置一个 VTEP 源接口。VTEP 定义为网络虚拟化终端 (NVE)。VXLAN 是默认的封装类型。

过程

步骤 1 如果要指定一组对等 VTEP，请添加具有对等体 IP 地址的网络对象。请参阅创建网络对象，第 999 页。

步骤 2 选择**设备** > **设备管理**。

步骤 3 点击要配置 VXLAN 的设备旁边的**编辑** ( )。

步骤 4 （可选） 将源接口指定为仅限 NVE。

在路由模式下，此设置限制此接口上仅允许流向 VXLAN 的流量和常见的管理流量，这种情下此设置是可选的。对于透明防火墙模式，系统会自动启用此设置。

a) 点击**接口 (Interfaces)**。

b) 点击 VTEP 源接口的**编辑 (Edit)** ( )。

c) 在**常规 (General)** 页面中，点击**仅限 NVE (NVE Only)**。

步骤 5 如果尚未显示，点击 **VTEP**。

步骤 6 选中**启用 NVE (Enable NVE)**。

步骤 7 点击**添加 VTEP (Add VTEP)**。

步骤 8 对于**封装类型 (Encapsulation Type)**，请选择 **VxLAN**。

对于 AWS，您可以在 **VxLAN** 和 **Geneve** 之间进行选择。其他平台会自动选择 **VxLAN**。

步骤 9 在**封装端口 (Encapsulation port)** 中输入指定范围内的值。

默认值为 4789。

步骤 10 选择 **VTEP 源接口 (VTEP Source Interface)**。

从设备上的可用物理接口列表中进行选择。如果源接口 MTU 少于 1554 个字节，则 管理中心 会自动将 MTU 提高到 1554 个字节。

步骤 11 选择**邻居地址 (Neighbor Address)**。可用选项包括：

- **无 (None)** - 未指定邻居地址。
- **对等体 VTEP (Peer VTEP)** - 指定对等体 VTP 地址。
- **对等体组 (Peer Group)** - 指定具有对等体 IP 地址的网络对象。
- **默认组播 (Default Multicast)** - 指定所有相关 VNI 接口的默认组播组。如果每个 VNI 接口未配置组播组，则使用该组。如果配置一个 VNI 接口级别的组，则该组将覆盖此设置。

步骤 12 点击**确定 (OK)**。

步骤 13 点击**保存 (Save)**。

步骤 14 配置已路由的接口参数。请参阅配置路由模式接口。

配置 VNI 接口

添加 VNI 接口，将其与 VTEP 源接口相关联，并配置基本的接口参数。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击要配置 VXLAN 的设备旁边的**编辑** ( )。

步骤 3 点击**接口 (Interfaces)**。

步骤 4 点击**添加接口 (Add Interfaces)**，，然后选择 **VNI 接口 (VNI Interface)**。

步骤 5 输入接口**名称 (Name)** 和**说明 (Description)**。

步骤 6 从**安全区域 (Security Zone)** 下拉列表中选择一个安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

步骤 7 在指定范围内为**优先级 (Priority)** 字段输入值。默认情况下会选择 0。

步骤 8 输入值介于 1 和 10000 之间的 **VNI ID**。

此 ID 仅为内部接口标识符。

步骤 9 为 **VNI 网段 ID (VNI Segment ID)** 设置为 1 和 16777215 之间值。

网段 ID 用于 VXLAN 标记。

步骤 10 输入**多播组 IP 地址 (Multicast Group IP Address)**。

如果没有为 VNI 接口设置组播组，请使用源自 VTEP 源接口配置的默认组（如果有）。如果手动设置 VTEP 源接口的 VTEP 对等体 IP，则无法为 VNI 接口指定组播组。

步骤 11 选中 **NVE 已映射到 VTEP 接口 (NVE Mapped to VTEP Interface)**。

此选项会将该接口与 VTEP 源接口相关联。

步骤 12 点击**确定 (OK)**。

步骤 13 点击**保存 (Save)** 以保存接口配置。

步骤 14 配置路由或透明接口参数。请参阅配置路由和透明模式接口，第 548 页。

配置 Geneve 接口

要为 threat defense virtual 配置 Geneve 接口，请执行以下步骤：

注释 您可以配置 VXLAN 或 Geneve。有关 VXLAN 接口的信息，请参阅配置 VXLAN 接口，第 543 页。

1. 配置 VTEP 源接口，第 546 页。
2. 配置 VNI 接口，第 546 页。
3. 允许网关负载均衡器运行状况检查，第 547 页。

配置 VTEP 源接口

每个 threat defense virtual 设备可以配置一个 VTEP 源接口。VTEP 定义为网络虚拟化终端 (NVE)。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击要配置 Geneve 的设备旁边的**编辑** ( )。

步骤 3 点击 **VTEP**。

步骤 4 选中**启用 NVE (Enable NVE)**。

步骤 5 点击**添加 VTEP (Add VTEP)**。

步骤 6 对于**封装类型 (Encapsulation Type)**，请选择 **Geneve**。

步骤 7 在**封装端口 (Encapsulation port)** 中输入指定范围内的值。

我们不建议更改 Geneve 端口；AWS 需要使用端口 6081。

步骤 8 选择 **VTEP 源接口 (VTEP Source Interface)**。

您可以从设备上的可用物理接口列表中进行选择。如果源接口 MTU 少于 1806 个字节，管理中心 会自动将 MTU 提高到 1806 个字节。

步骤 9 点击**确定 (OK)**。

步骤 10 点击**保存 (Save)**。

步骤 11 配置已路由的接口参数。请参阅配置路由模式接口。

配置 VNI 接口

添加 VNI 接口，将其与 VTEP 源接口相关联，并配置基本的接口参数。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击要配置 Geneve 的设备旁边的**编辑** ( )。

步骤 3 点击**接口 (Interfaces)**。

步骤 4 点击**添加接口 (Add Interfaces)**，，然后选择 **VNI 接口 (VNI Interface)**。

步骤 5 输入接口**名称 (Name)** 和**说明 (Description)**。

步骤 6 输入值介于 1 和 10000 之间的 **VNI ID**。

此 ID 仅为内部接口标识符。

步骤 7 选中**启用代理 (Enable Proxy)**。

此选项会启用单臂代理，并允许流量退出其所进入的同一接口（掉头流量）。如果您稍后对接口进行编辑，则无法禁用单臂代理。为此，您需要删除现有接口并创建一个新的 VNI 接口。

此选项仅适用于 Geneve VTEP。

步骤 8 选择 **NVE 已映射到 VTEP 接口 (NVE Mapped to VTEP Interface)**。

此选项会将该接口与 VTEP 源接口相关联。

步骤 9 点击**确定 (OK)**。

步骤 10 点击**保存 (Save)** 以保存接口配置。

步骤 11 配置已路由的接口参数。请参阅配置路由模式接口。

允许网关负载均衡器运行状况检查

AWS GWLB 要求设备对运行状况检查进行正确应答。GWLB 只会将流量发送到被视为正常的设备。您必须将 threat defense virtual 配置为响应 SSH、HTTP 或 HTTPS 运行状况检查。

配置以下方法之一。

过程

步骤 1 配置 SSH。请参阅配置安全外壳

允许来自 GWLB IP 地址的 SSH。GWLB 将尝试与 threat defense virtual 建立连接，而 threat defense virtual 的登录提示将被视为运行状况的证明。SSH 登录尝试会在 1 分钟后超时。为了适应此超时，您需要在 GWLB 上配置更长的运行状况检查间隔。

步骤 2 使用支持端口转换的静态接口 NAT 来配置 HTTP(S) 重定向。

您可以将 threat defense virtual 配置为将运行状况检查重定向到元数据 HTTP(S) 服务器。对于 HTTP(S) 运行状况检查，HTTP(S) 服务器必须使用 200 到 399 范围内的状态代码来回复 GWLB。由于 threat defense virtual 对同时管理连接的数量存在限制，因此您可以选择将运行状况检查分流到外部服务器。

支持端口转换的静态接口 NAT 允许您将某个端口（例如端口 80）的连接重定向到其他 IP 地址。例如，将来自 GWLB 的 HTTP 数据包转换为 threat defense virtual 外部接口的目标，使其看起来像是来自目标为 HTTP 服务器的 threat defense virtual 外部接口。threat defense virtual 随后会将数据包转发到

映射的目标地址。HTTP 服务器会响应 threat defense virtual 外部接口，然后 threat defense virtual 会将响应转发回 GWLB。您需要允许从 GWLB 到 HTTP 服务器的流量的访问规则。

a) 在访问规则中允许来自 GWLB 网络的外部接口上的 HTTP(S) 流量。请参阅访问控制规则，第 1279 页。

b) 对于 HTTP(S)，请将源 GWLB IP 地址转换为 threat defense virtual 外部接口 IP 地址；然后将外部接口 IP 地址的目的地转换为 HTTP(S) 服务器 IP 地址。请参阅配置静态手动 NAT，第 704 页。

配置路由和透明模式接口

本部分介绍在路由或透明防火墙模式下为所有型号完成常规接口配置的相关任务。

关于路由和透明模式接口

防火墙模式接口需要对流量执行防火墙功能，例如维持流量、跟踪 IP 和 TCP 层的流量状态、IP 分片重组和 TCP 规范化。另外，您还可以根据安全策略，选择为此流量配置 IPS 功能。

可以配置的防火墙接口类型取决于为设备设置的防火墙模式：路由或透明模式。有关详细信息，请参阅透明或路由防火墙模式，第 377 页。

- 路由模式接口（仅路由防火墙模式）- 要在其间路由的每个接口都在不同的子网中。
- 网桥组接口（路由和透明防火墙模式）- 您可以将网络上的多个接口组合在一起，Firepower 威胁防御设备将使用桥接技术在接口之间传递流量。每个桥接组包括一个网桥虚拟接口 (BVI)，供您为其分配一个网络 IP 地址。 在路由模式下，Firepower 威胁防御设备在 BVI 和常规路由接口之间路由。在透明模式下，每个网桥组都是独立的，相互之间无法通信。

双 IP 堆栈（IPv4 和 IPv6）

威胁防御设备在接口上同时支持 IPv6 和 IPv4 地址。请确保配置一条同时适用于 IPv4 和 IPv6 的默认路由。

31 位子网掩码

对于路由接口，您可以在 31 位子网上为点对点连接配置 IP 地址。31 位子网只包含 2 个地址；通常，该子网中的第一个和最后一个地址预留用于网络和广播，因此，不可使用包含 2 个地址的子网。但是，如果您有点对点连接，并且不需要网络或广播地址，则 31 位子网是在 IPv4 中保留地址的有用方式。例如，2 个 威胁防御 之间的故障切换链路只需要 2 个地址；该链路一端传输的任何数据包始终由另一端接收，无需广播。您还可以拥有运行 SNMP 或系统日志的一个直连管理站。

31 位子网和集群

您可以在跨集群模式，但管理接口和集群控制链路除外。

31 位子网和故障切换

进行故障切换时，如果为 威胁防御 接口 IP 地址使用 31 位子网，则无法为该接口配置备用 IP 地址，因为没有足够的地址。通常，用于进行故障切换的接口应有一个备用 IP 地址，以便主设备可以执行接口测试来确保备用接口正常运行。如果没有备用IP地址，威胁防御无法执行任何网络测试；只能跟踪链路状态。

对于故障切换和可选的独立状态链路（点对点连接），也可以使用 31 位子网。

31 位子网和管理

如果您有直接连接的管理工作站，则对于 威胁防御 的 SSH 或 HTTP，或管理工作站上的 SNMP 或 Syslog，可使用点对点连接。

31 位子网不支持的功能

以下功能不支持 31 位子网：

- 网桥组的 BVI 接口 - 网桥组需要至少 3 个主机地址：BVI 和连接到两个网桥组成员接口的两台主机。您必须使用 /29 子网或更小的子网。
- 组播路由

路由和透明模式接口指南和限制

高可用性、 集群和多实例

- 请勿采用本章中的程序配置故障切换接口。有关详细信息，请参阅高可用性。
- 对于集群接口，请参阅“集群”一章了解要求。
- 对于多实例模式，共享接口不支持用于网桥组成员接口（在透明模式或路由模式下）。
- 在使用高可用性时，则必须为数据接口手动设置 IP 地址和备用地址；不支持 DHCP 和 PPPoE。在**监控接口**区域中的**设备** > **设备管理** > **高可用性**选项卡上设置备用 IP 地址。有关详细信息，请参阅高可用性章节。

IPv6

- 所有接口上都支持 IPv6。
- 只能在透明模式下手动配置 IPv6 地址。
- 威胁防御设备 不支持 IPv6 任播地址。

型号规定

- 对于具有桥接 ixgbevf 接口的 VMware 上的threat defense virtual，桥接组不受支持。
- 对于 Firepower 2100 系列，在路由模式下不支持网桥组。

透明模式和网桥组准则

- 您可以创建最多 250 个桥接组，每个桥接组 64 个接口。
- 各个直连网络必须在同一子网上。
- 威胁防御设备不支持辅助网络上的流量；只有与 BVI IP 地址相同的网络上的流量才受支持。
- 每个桥接组都需要 BVI 的 IP 地址，以用于管理往返设备的流量和使流量通过 威胁防御设备。对于 IPv4 流量，请指定 IPv4 地址。对于 IPv6 流量，请指定 IPv6 地址。
- 您仅可手动配置 Ipv6 地址。
- BVI IP 地址必须与已连接网络位于同一子网上。您不能将该子网设置为主机子网 (255.255.255.255)。
- 不支持将管理接口作为桥接组成员。
- 对于多实例模式，共享接口不支持用于网桥组成员接口（在透明模式或路由模式下）。
- 对于具有桥接 ixgbevf 接口的 VMware 上的 threat defense virtual ，透明模式不受支持，在路由模式中网桥组不受支持。
- 对于 Firepower 2100 系列，在路由模式下不支持网桥组。
- 对于 Firepower 1010，不能将逻辑 VLAN 接口和物理防火墙接口混合在同一个桥接组中。
- 对于 Firepower 4100/9300，不支持将数据共享接口作为网桥组成员。
- 在透明模式下，必须至少使用 1 个桥接组；数据接口必须属于桥接组。
- 在透明模式下，请勿将 BVI IP 地址指定为所连接设备的默认网关；设备需要将位于 威胁防御另一端的路由器指定为默认网关。
- 在透明模式下，默认路由（为管理流量提供返回路径所需的路由）仅适用于来自一个桥接组网络的管理流量。这是因为默认路由会指定网桥组中的接口以及网桥组网络上的路由器 IP 地址，而您只能定义一个默认路由。如果您具有来自多个桥接组网络的管理流量，则需要指定常规静态路由来确定预期会发出管理流量的网络。
- 在透明模式下，诊断接口不支持 PPPoE。
- Amazon Web 服务、Microsoft Azure、Google Cloud Platform 和 Oracle Cloud Infrastructure 上部署的威胁防御虚拟实例不支持透明模式。
- 在路由模式下，要在桥接组和其他路由接口之间路由，您必须指定 BVI。
- 在路由模式下，威胁防御 - 不支持将 EtherChannel 接口定义为网桥组成员。 Firepower 4100/9300 上的 Etherchannel 可以是网桥组成员。
- 使用网桥组成员时，不允许双向转发检测 (BFD) 回应数据包通过 威胁防御。如果 威胁防御 的一端有两个邻居运行 BFD，则 威胁防御 会因二者具有相同的源 IP 地址和目标 IP 地址且疑似属于 LAND 攻击而丢弃 BFD 回应数据包。

其他指南和规定

- 威胁防御 仅支持数据包中的一个 802.1Q 报头，不支持防火墙接口的多个报头（称为 QinQ 支持）。**注意**：对于内联集和被动接口，FTD 在数据包中最多支持 Q-in-Q 两个 802.1Q 报头，但 Firepower 4100/9300 仅支持一个 802.1Q 报头。

配置路由模式接口

此程序介绍如何设置名称、安全区域和 IPv4 地址。

注释 并非所有接口类型都支持所有的字段。

开始之前

- **Firepower 4100/9300**
  1. 配置物理接口，第 423 页
  2. （可选）配置任何特殊接口。
     - 添加 EtherChannel（端口通道），第 426 页
     - 为容器实例添加 VLAN 子接口，第 429 页 在 FXOS 中
     - 添加子接口，第 535 页 在 管理中心
     - 配置 VXLAN 接口，第 543 页
- （可选） **所有其他型号**：
  - 配置 EtherChannel，第 532 页
  - 添加子接口，第 535 页
  - 配置 VXLAN 接口，第 543 页
  - AWS 上的 Threat Defense Virtual：配置 Geneve 接口，第 545 页
  - Firepower 1010： 配置 VLAN 接口，第 521 页

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（✎）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑**（✎）。

步骤 3 在**名称**字段中，输入长度最大为 48 个字符的名称。

步骤 4 选中**启用**复选框以启用此接口。

步骤 5 （可选） 将此接口设置为**管理专用**以限制到管理流量的流量；不允许通过设备的流量。

步骤 6 （可选） 在**说明**字段中添加说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 7 在**模式**下拉列表中，选择**无**。

常规防火墙接口的模式设置为“无”。其他模式用于仅 IPS 接口类型。

步骤 8 从**安全区域**下拉列表中选择一个安全区域，或者点击**新建**添加一个新的安全区域。

路由接口是路由类型的接口，只能属于路由类型的区域。

步骤 9 有关 **MTU** 的详细信息，请参阅配置 MTU，第 569 页。

步骤 10 在 **优先级** 字段中，输入一个介于 0 和 65535 之间的数字。

此值在策略型路由配置中使用。优先级用于确定如何跨多个出口接口路由流量。有关详细信息，请参阅配置基于策略的路由策略，第 946 页。

步骤 11 点击 **Ipv4** 选项卡。要设置 IP 地址，请使用 **IP 类型**下拉列表中的下列选项之一。

高可用性、集群接口仅支持静态 IP 地址配置；不支持 DHCP 和 PPPoE。

- **使用静态 IP** - 输入 IP 地址和子网掩码。对于点对点连接，可以指定 31 位子网掩码 (255.255.255.254)。在这种情况下，不会为网络或广播地址预留 IP 地址。在此情况下，无法设置备用 IP 地址。对于高可用性，只能使用静态 IP 地址。在 **监控接口** 区域中的 **设备** > **设备管理** > **高可用性**选项卡上设置备用 IP 地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。
- **使用 DHCP** - 配置以下可选参数：
  - **使用 DHCP 获取默认路由 (Obtain default route using DHCP)** - 从 DHCP 服务器获取默认路由。
  - **DHCP 路由指标 (DHCP route metric)** - 分配到所获悉路由的管理距离，介于 1 和 255 之间。获悉的路由的默认管理距离为 1。
- **使用 PPPoE** - 如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，请配置以下参数：
  - **VPDN 组名称** - 指定您选择的组名称来表示此连接。
  - **PPPoE 用户名** - 指定 ISP 提供的用户名。
  - **PPPoE 密码/确认密码** - 指定并确认 ISP 提供的密码。
  - **PPP 身份验证** - 选择 **PAP**、**CHAP** 或 **MSCHAP**。

    PAP 在身份验证过程中传递明文用户名和密码，这样并不安全。使用 CHAP 时，客户端可返回加密的 [challenge plus password] 和明文用户名来响应服务器质询。CHAP 比 PAP 更安全，但其不会加密数据。MSCHAP 与 CHAP 类似但更安全，因为服务器只对加密密码进行

存储和比较，而不是像 CHAP 一样存储和比较明文密码。MSCHAP 还可生成密钥，以便 MPPE 进行数据加密。

- **PPPoE 路由指标** - 向获悉的路由分配管理距离。有效值为从 1 到 255。默认情况下，获悉的路由的默认管理距离为 1。
- **启用路由设置** - 要手动配置 PPPoE IP 地址，请选中此框，然后输入 **IP 地址**。

  如果选中 **启用路由设置** 复选框并将 **IP 地址** 留空，则会应用 **ip address pppoe setroute** 命令，如下例所示：

```
interface GigabitEthernet0/2
nameif inside2_pppoe
cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
security-level 0
pppoe client vpdn group test
pppoe client route distance 10
ip address pppoe setroute
```

- **在闪存中存储用户名和密码** - 在闪存中存储用户名和密码。

  威胁防御 设备将用户名和密码存储在 NVRAM 中的专用位置。

步骤 12 （可选） 要在 **IPv6** 选项卡上配置 IPv6 寻址，请参阅配置 IPv6 寻址 ， 第 559 页。

步骤 13 （可选） 要在**高级**选项卡上手动配置 MAC 地址，请参阅配置 MAC 地址 ， 第 569 页。

步骤 14 （可选） 通过点击 **硬件配置** > **速度**，设置复用和速度。

- **复用**—选择 **全** 或 **半**。SFP 接口仅支持 **全** 复用。
- **速度**-选择速度（因型号而异）。 Cisco Secure Firewall 3100）选择 **检测 SFP** 以检测已安装的 SFP 模块的速度并使用适当的速度。复用始终为全复用，并且始终启用自动协商。如果您稍后将网络模块更改为其他型号，并希望速度自动更新，则此选项非常有用。
- **自动协商**-设置接口以协商速度、链路状态和流量控制。对于低于 1000 Mbps 的速度，无法编辑此设置。对于 SFP 接口，只能在速度设置为 1000 Mbps 时禁用自动协商。
- **前向纠错模式** Cisco Secure Firewall 3100）对于 25 Gbps 及更高的接口，请启用前向纠错 (FEC)。对于 EtherChannel 成员接口，必须先配置 FEC，然后才能将其添加到 EtherChannel。使用**自动 (Auto)** 时选择的设置取决于收发器类型，以及接口是固定接口（内置）还是在网络模块上。

表 *60:* 用于自动设置的默认 *FEC*

收发器类型	固定端口默认 **FEC**（以太网 **1/9** 至 **1/16**）	网络模块默认 **FEC**
25G-SR	Clause 74 FC-FEC	Clause 108 RS-FEC
25G-LR	Clause 74 FC-FEC	Clause 108 RS-FEC
10/25G-CSR	Clause 74 FC-FEC	Clause 74 FC-FEC
25G-AOC*x*M	Clause 74 FC-FEC	Clause 74 FC-FEC

收发器类型	固定端口默认 FEC（以太网 1/9 至 1/16）	网络模块默认 FEC
25G-CU2.5/3M	自动协商	自动协商
25G-CU4/5M	自动协商	自动协商

步骤 15 （可选） 在**管理访问 (Manager Access)** 页面上启用数据接口上的 管理中心 管理器访问。

首次设置 威胁防御 时，您可以从数据接口启用管理器访问。如果要在将 威胁防御 添加到 管理中心 后启用或禁用管理器访问，请参阅：

- 启用管理器访问：将管理器访问接口从管理更改为数据，第 63 页

  注释 除非先启动管理器接口从管理到数据接口的迁移，否则无法启用管理器访问。启动迁移后，您可以在**管理器访问 (Manager Access)** 页面上启用管理器访问并成功保存配置。

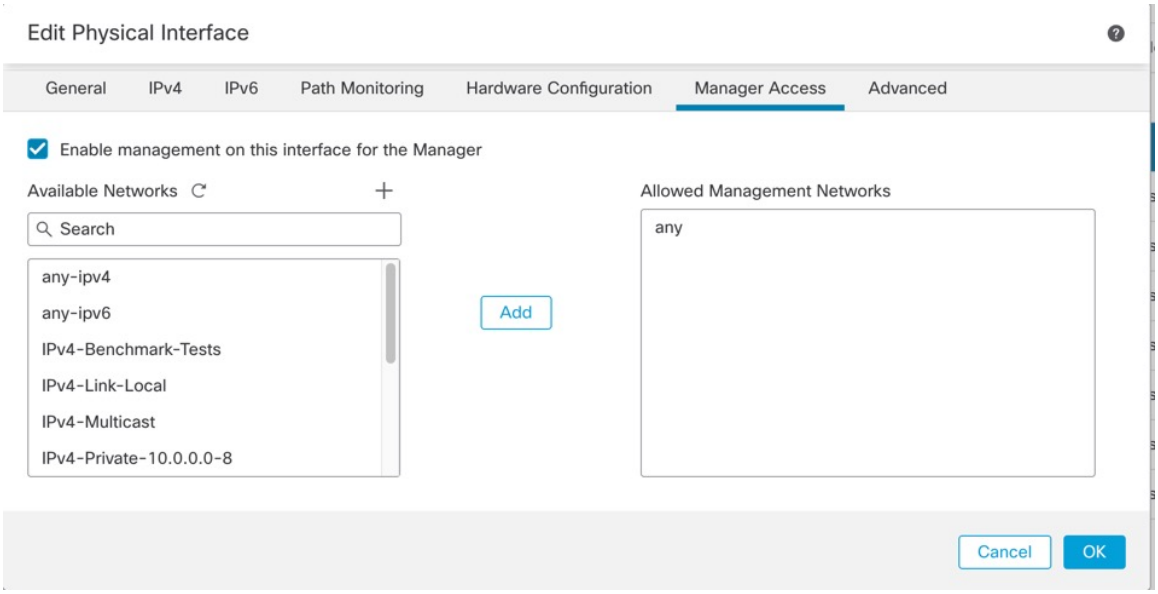
- 禁用管理器访问：将管理器访问接口从数据更改为管理，第 66 页

如果要将管理器访问接口从一个数据接口更改为另一个数据接口，必须在原始数据接口上禁用管理器访问，但不要禁用接口本身；必须使用原始数据接口执行部署。如果要在新管理器访问接口上使用相同的 IP 地址，可以删除或更改原始接口上的 IP 配置；此更改不应影响部署。如果为新接口使用不同的 IP 地址，则还要更改 管理中心 中显示的设备 IP 地址；请参阅更新 管理中心中的主机名或 IP 地址，第 61 页。请务必同时更新相关配置，以使用新接口，例如静态路由、DDNS 和 DNS 设置。

从数据接口进行管理器访问具有以下限制：

- 只能在 物理数据接口上启用管理器访问。不能使用子接口或 EtherChannel。
- 此接口不能是仅管理接口。
- 仅路由防火墙模式，使用路由接口。
- 不支持 PPPoE。如果您的 ISP 需要 PPPoE，则必须在 威胁防御 与 WAN 调制解调器之间放入支持 PPPoE 的路由器。
- 接口只能位于全局 VRF 中。
- 默认不对数据接口启用 SSH，因此必须稍后使用 管理中心 来启用 SSH。由于管理接口网关将更改为数据接口，因此您也无法启动从远程网络到管理接口的 SSH 会话，除非您使用 **configure network static-routes** 命令为管理接口添加静态路由。对于 Amazon Web 服务上的 threat defense virtual，控制台端口不可用，因此您应保持对管理接口的 SSH 访问：在继续配置之前为管理添加静态路由。或者，请确保在配置用于管理器访问的数据接口并断开连接之前完成所有 CLI 配置（包括 **configure manager add** 命令）。
- 不支持集群技术。在这种情况下，必须使用管理接口。
-

图 *99:* 管理器访问



- 选中**在此接口上为管理器启用管理 (Enable management on this interface for the manager)** 以便使用此数据接口进行管理，而不是专用管理接口。
- （可选）在**允许的管理网络 (Allowed Management Networks)** 框中，添加要允许管理器访问的网络。默认情况下，允许任何网络。

步骤 16 点击**确定 (OK)**。

步骤 17 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置网桥组接口

网桥组是指 Secure Firewall Threat Defense网桥（而非路由）的接口组。 网桥组在透明和路由防火墙模式下受支持。有关网桥组的详细信息，请参阅 关于网桥组 ， 第 379 页。

要配置网桥组和关联接口，请执行以下步骤。

配置常规网桥组成员接口参数

此程序描述如何为每个网桥组成员接口设置名称和安全区域。同一网桥组可以包括不同类型的接口：物理接口、 Firepower 1010 VLAN 子接口、VNI 接口、 EtherChannel 接口和冗余接口管理接口不受支持。 在路由模式中，不支持 EtherChannels。对于 Firepower 4100/9300，不支持数据共享类型的接口。

开始之前

- **Firepower 4100/9300**
  1. 配置物理接口，第 423 页
  2. （可选）配置任何特殊接口。
     - 添加 EtherChannel（端口通道），第 426 页
     - 为容器实例添加 VLAN 子接口，第 429 页 在 FXOS 中
     - 添加子接口，第 535 页 在 管理中心
- （可选） **所有其他型号**：
  - 配置 EtherChannel，第 532 页
  - 添加子接口，第 535 页
  - Firepower 1010： 配置 VLAN 接口，第 521 页

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（✎）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑**（✎）。

步骤 3 在**名称**字段中，输入长度最大为 48 个字符的名称。

步骤 4 选中**启用**复选框以启用此接口。

步骤 5 （可选） 将此接口设置为**管理专用**以限制到管理流量的流量；不允许通过设备的流量。

步骤 6 （可选） 在**说明**字段中添加说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 7 在**模式**下拉列表中，选择**无**。

常规防火墙接口的模式设置为“无”。其他模式用于仅IPS接口类型。在将此接口分配到网桥组后，该模式将显示为**交换**。

步骤 8 从**安全区域**下拉列表中选择一个安全区域，或者点击**新建**添加一个新的安全区域。

桥接组成员接口是交换类型的接口，只能属于交换类型的区域。请勿为此接口设置任何 IP 地址设置。您将只设置桥接虚拟接口 (BVI) 的 IP 地址。请注意，BVI 不属于某个区域，您不能将访问控制策略应用到 BVI。

步骤 9 有关 **MTU** 的详细信息，请参阅配置 MTU，第 569 页。

步骤 10 （可选） 通过点击 **硬件配置** > **速度**，设置复用和速度。

- **复用**—选择 **全** 或 **半**。SFP 接口仅支持 **全** 复用。

- **速度**-选择速度（因型号而异）。 Cisco Secure Firewall 3100）选择 **检测 SFP** 以检测已安装的 SFP 模块的速度并使用适当的速度。复用始终为全复用，并且始终启用自动协商。如果您稍后将网络模块更改为其他型号，并希望速度自动更新，则此选项非常有用。
- **自动协商**-设置接口以协商速度、链路状态和流量控制。对于低于 1000 Mbps 的速度，无法编辑此设置。对于 SFP 接口，只能在速度设置为 1000 Mbps 时禁用自动协商。
- **前向纠错模式** Cisco Secure Firewall 3100）对于 25 Gbps 及更高的接口，请启用前向纠错 (FEC)。对于 EtherChannel 成员接口，必须先配置 FEC，然后才能将其添加到 EtherChannel。使用**自动 (Auto)** 时选择的设置取决于收发器类型，以及接口是固定接口（内置）还是在网络模块上。

表 *61:* 用于自动设置的默认 *FEC*

收发器类型	固定端口默认 **FEC**（以太网 **1/9** 至 **1/16**）	网络模块默认 **FEC**
25G-SR	Clause 74 FC-FEC	Clause 108 RS-FEC
25G-LR	Clause 74 FC-FEC	Clause 108 RS-FEC
10/25G-CSR	Clause 74 FC-FEC	Clause 74 FC-FEC
25G-AOC*x*M	Clause 74 FC-FEC	Clause 74 FC-FEC
25G-CU2.5/3M	自动协商	自动协商
25G-CU4/5M	自动协商	自动协商

步骤 11 （可选） 要在 **IPv6** 选项卡上配置 IPv6 寻址，请参阅配置 IPv6 寻址 ，第 559 页。

步骤 12 （可选） 要在**高级**选项卡上手动配置 MAC 地址，请参阅配置 MAC 地址 ，第 569 页。

步骤 13 点击**确定 (OK)**。

步骤 14 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置网桥虚拟接口 (BVI)

每个网桥组都需要一个您应为其配置 IP 地址的 BVI。威胁防御 使用此 IP 地址作为源自网桥组的数据包的源地址。BVI IP 地址必须与所连接的网络位于同一子网。对于 IPv4 流量，任何流量的传递都需要使用 BVI IP。对于 IPv6 流量，您必须至少配置链路本地地址以传递流量，但要实现完整功能（包括远程管理和其他管理操作），建议采用全局管理地址。

对于路由模式，如果为 BVI 提供一个名称，则 BVI 将参与路由。如果不提供名称，网桥组在透明防火墙模式下将保持隔离状态。

注释 对于单独的诊断接口，不可配置的桥组 (ID 301) 会自动添加至您的配置。此网桥组未包含在网桥组限制中。

开始之前

您不能将 BVI 添加到安全区域；因此，不能将访问控制策略应用到 BVI。必须根据其区域将策略应用于网桥组成员接口。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 选择**添加接口** > **网桥组接口**。

步骤 3 （路由模式）在**名称**字段中，输入长度最大为 48 个字符的名称。

如果要在网桥组成员之外路由流量，例如路由到外部接口或其他网桥组的成员，则必须为 BVI 命名。该名称不区分大小写。

步骤 4 在**网桥组 ID** 字段中，输入 1 和 250 之间的网桥组 ID。

步骤 5 在**说明**字段中，输入此网桥组的说明。

步骤 6 在**接口**选项卡上，点击某个接口对，然后点击**添加**，以将其移动至**选定的接口**区域。对要使其成为网桥组成员的所有接口重复此步骤。

步骤 7 （透明模式）点击 **IPv4** 选项卡。在 **IP 地址**字段中，输入 IPv4 地址和子网掩码。

请勿为 BVI 分配主机地址（/32 或 255.255.255.255）。此外，请勿使用主机地址不足 3 个（分别用于上游路由器、下游路由器和透明防火墙）的其他子网，例如 /30 子网 (255.255.255.252)。威胁防御设备会丢弃传入子网中第一个和最后一个地址或从其传出的所有 ARP 数据包。例如，如果您使用 /30 子网，并从该子网中为上游路由器分配了一个预留地址，那么 威胁防御 设备将丢弃从下游路由器发送至上游路由器的 ARP 请求。

对于高可用性，请在**监控接口**区域的**设备** > **设备管理** > **高可用性**选项卡中设置备用 IP 地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

步骤 8 （路由模式）点击 **IPv4** 选项卡。要设置 IP 地址，请使用 **IP 类型**下拉列表中的下列选项之一。

高可用性和集群接口仅支持静态 IP 地址配置；不支持 DHCP。

- **使用静态 IP** - 输入 IP 地址和子网掩码。对于高可用性，只能使用静态 IP 地址。在**监控接口**区域中的**设备** > **设备管理** > **高可用性**选项卡上设置备用 IP 地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。
- **使用 DHCP** - 配置以下可选参数：
  - **使用 DHCP 获取默认路由 (Obtain default route using DHCP)** - 从 DHCP 服务器获取默认路由。

- **DHCP 路由指标 (DHCP route metric)** - 分配到所获悉路由的管理距离，介于 1 和 255 之间。获悉的路由的默认管理距离为 1。

步骤 9 （可选） 请参阅配置 IPv6 寻址，第 559 页配置 Ipv6 寻址。

步骤 10 （可选） 要配置 **ARP** 和 **MAC** 设置，请参阅添加静态 ARP 条目，第 570 页和添加静态 MAC 地址并为网桥组禁用 MAC 学习，第 571 页（仅对于透明模式）。

步骤 11 点击**确定 (OK)**。

步骤 12 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 IPv6 寻址

本节介绍如何在路由模式和透明模式下配置 IPv6 寻址。

关于 IPv6

本节包括关于 IPv6 的信息。

IPv6 寻址

您可以为 IPv6 配置两种类型的单播地址：

- 全局 - 全局地址是可在公用网络上使用的公用地址。对于网桥组，需要为 BVI（而不必为每个成员接口）配置此地址。还可以为透明模式下的管理接口配置全局 IPv6 地址。
- 链路本地 - 链路本地地址是只能在直连网络上使用的专用地址。路由器不使用链路本地地址转发数据包；它们仅用于在特定物理网段上通信。链路本地地址可用于地址配置或邻居发现功能，例如地址解析。在网桥组中，只有成员接口具有链路本地地址；BVI 没有链路本地地址。

至少需要配置链路本地地址，IPv6 才会起作用。如果配置全局地址，则接口上会自动配置链路本地地址，因此无需另外专门配置链路本地地址。对于网桥组成员接口，在 BVI 上配置全局地址时，威胁防御设备 将为成员接口自动生成链路本地地址。如果不配置全局地址，则需要自动或手动配置链路本地地址。

注释 如果希望仅配置链路本地地址，请参阅命令参考中的 **ipv6 enable**（自动配置）或 **ipv6 address link-local**（手动配置）命令。

修改的 EUI-64 接口 ID

RFC 3513：互联网协议第 6 版 (IPv6) 寻址架构要求所有单播 IPv6 地址（以二进制值 000 开头的地址除外）的接口标识符部分的长度为 64 位，并以修改的 EUI-64 格式进行构造。威胁防御设备 可为连接到本地链路的主机执行该要求。

在接口上启用此功能时，该接口接收的 IPv6 数据包源地址根据源 MAC 地址进行验证，以确保接口标识符使用修改的 EUI-64 格式。如果 IPv6 数据包不将修改的 EUI - 64 格式用于接口标识符，则会丢弃数据包并生成以下系统日志消息：

```
325003: EUI-64 source address check failed.
```

只有在创建流量时才会执行地址格式验证。不检查来自现有流量的数据包。此外，只能对本地链路上的主机执行地址验证。

配置全局 IPv6 地址

要为任何路由模式接口和透明或路由模式 BVI 配置全局 IPv6 地址，请执行以下步骤。

注释 配置全局地址将自动配置链路本地地址，因此无需单独对其进行配置。对于网桥组，在 BVI 上配置全局地址会自动在所有成员接口上配置链路本地地址。

对于在 威胁防御 上定义的子接口，建议您同样手动设置 MAC 地址，这是因为它们使用父接口上相同的固化 MAC 地址。由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一的 MAC 地址分配给子接口会允许唯一的 IPv6 链路本地地址，这能够避免 威胁防御 上特定实例内发生流量中断。请参阅配置 MAC 地址，第 569 页。

开始之前

对于网桥组的 IPv6 邻居发现，您必须使用双向访问规则明确允许邻居请求（ICMPv6 类型 135）和邻居通告（ICMPv6 类型 136）数据包通过 威胁防御 网桥组成员接口。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（✎）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑**（✎）。

步骤 3 点击 **IPv6** 页面。

对于路由模式，**基本 (Basic)** 页面默认处于选中状态。对于透明模式，**地址 (Address)** 页面默认处于选中状态。

步骤 4 在**基本 (Basic)** 页面上，选中**启用 IPv6 (Enable IPv6)**。

步骤 5 使用以下其中一种方法配置全局 IPv6 地址。

- （路由接口）无状态自动配置 - 选中**自动配置**复选框。

  在接口上启用无状态自动配置时，将基于路由器通告消息中接收到的前缀来配置 IPv6 地址。启用无状态自动配置时，将基于修改的 EUI-64 接口 ID 自动生成接口的链路本地地址。

虽然 RFC 4862 规定为无状态自动配置所配置的主机不发送路由器通告消息，但 威胁防御 设备在这种情况下确实会发送路由器通告消息。取消选中**IPv6** > **设置** > **启用 RA** 复选框以抑制邮件。

- 手动配置 - 要手动配置全局 IPv6 地址，请执行以下操作：

  1. 点击**地址 (Address)** 页面并点击**添加地址 (Add Address)**。

     系统将显示**添加接口**对话框。

  2. 在**地址**字段中，输入完整全局 IPv6 地址（包括接口 ID），或输入 IPv6 前缀以及 IPv6 前缀长度。（路由模式）如果仅输入前缀，请务必选中**强制 EUI 64** 复选框，以使用修改的 EUI-64 格式生成接口 ID。例如，2001:0DB8::BA98:0:3210/48（完整地址）或 2001:0DB8::/48（前缀，且选中 EUI 64）。

     对于高可用性（如果未设置**强制 EUI 64 (Enforce EUI 64)**），请在**设备 (Devices)** > **设备管理 (Device Management)** > **高可用性 (High Availability)** 页面的**受监控接口 (Monitored Interfaces)** 区域中设置备用 IP 地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

步骤 6 对于路由接口，您可以选择在**基本 (Basic)** 页面上设置下列值：

- 要在本地链路上的 IPv6 地址中强制使用修改的 EUI-64 格式的接口标识符，请选中**强制 EUI-64** 复选框。
- 要手动设置链路本地地址，请在**链路本地地址**字段中输入地址。

  链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feee:6a82。如果您不想配置全局地址，且只需配置链路本地地址，则可以选择手动定义链路本地地址。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。
- 选中**为地址配置启用 DHCP** 复选框以在 IPv6 路由器通告数据包中设置托管地址配置标志。

  IPv6 路由器通告中的此标志通知 IPv6 自动配置客户端应使用 DHCPv6 来获取相关地址以及派生的无状态自动配置地址。
- 选中**为非地址配置启用 DHCP** 复选框以在 IPv6 路由器通告数据包中设置其他地址配置标志。

  IPv6 路由器通告中的此标志通知 IPv6 自动配置客户端应使用 DHCPv6 从 DHCPv6 获取其他信息，如 DNS 服务器地址。

步骤 7 对于路由接口，请参阅配置 IPv6 邻居发现，第 562 页以配置**前缀 (Prefixes)** 和**设置 (Settings)** 页面上的设置。对于 BVI 接口，请参阅**设置 (Settings)** 页面上的以下参数：

- **DAD 尝试次数** - DAD 尝试的最大数，介于 1 和 600 之间。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。此设置可配置当对 IPv6 地址执行 DAD 时，接口上发送的连续邻居请求消息的数量。默认值为 1 次尝试。
- **NS 间隔** - 接口上 Ipv6 邻居请求重新传输之间的间隔，介于 1000 和 3600000 毫秒之间。默认值为 1000 毫秒。

- **可达时间** - 可达性确认事件发生后远程 IPv6 节点被视为可达的时长，介于 0 和 3600000 毫米之间。默认值为 0 毫秒。当该值为 0 时，将发送未确定的可访问时间。由接收设备来设置和跟踪可访问时间的值。邻居可访问时间可启用检测不可用邻居循环。配置时间越短，检测不可用邻居的速度就越快，但是，时间缩短却在所有 IPv6 网络设备中占用了更多的 IPv6 网络带宽和处理资源。在正常 IPv6 操作中不建议设置很短的配置时间。

步骤 8 点击**确定 (OK)**。

步骤 9 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 IPv6 邻居发现

IPv6 邻居发现过程使用 ICMPv6 消息和请求节点组播地址，确定同一网络（本地链路）中邻居的链路层地址、验证邻居的可读性及跟踪相邻路由器。

节点（主机）使用邻居发现确定已知驻留在连接的链路上邻居的链路层地址并快速清除变为无效的缓存值。主机还使用邻居发现查找愿意代表自己转发数据包的邻居路由器。此外，节点使用协议主动跟踪哪些邻居可访问及哪些邻居不可访问，并检测已更改的链路层地址。当路由器或路由器的路径发生故障时，主机会主动搜索起作用的替代项。

开始之前

仅在路由模式下受支持。有关透明模式下支持的 IPv6 邻居设置，请参阅配置全局 IPv6 地址，第 560 页。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（✎）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑**（✎）。

步骤 3 点击 **IPv6**，然后点击**前缀 (Prefixes)**。

步骤 4 （可选） 要配置包含在 IPv6 路由器通告中的 IPv6 前缀，请执行以下步骤：

a) 点击**添加前缀**。

b) 在**地址**字段中，输入带有前缀长度的 IPv6 地址，或选中**默认**复选框以使用默认前缀。

c) （可选） 取消选中**通告**复选框，以指示未通告 IPv6 前缀。

d) 选中**关闭链路**复选框以指示指定的前缀已分配给链路。向包含指定前缀的地址发送流量的节点会将目标视为在链路上本地可访问。此前缀不得用于链路上确定。

e) 要使用指定的前缀进行自动配置，请选中**自动配置**复选框。

f) 对于**前缀有效期**，请点击**持续时间**或**到期日期**。

- **持续时间** - 以秒为单位输入前缀的**首选有效期**。此设置是将指定的 IPv6 前缀通告为有效的时间。最大值代表无穷大。有效值为 0 到 4294967295。默认值为 2592000 秒（30 天）。以

秒为单位输入前缀的**有效期**。此设置是将指定的 IPv6 前缀通告为首选时间。最大值代表无穷大。有效值为 0 到 4294967295。默认设置为 604800 秒（七天）。或者，选中**无限**复选框以设置不受限制的持续时间。

- **到期日期** - 选择**有效**和**首选**日期和时间。

g) 点击 **OK**。

步骤 5 点击**设置 (Settings)**。

步骤 6 （可选） 设置介于 1 和 600 之间的 **DAD 尝试次数**最大值。默认值为 1 次尝试。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。

此设置可配置当对 IPv6 地址执行 DAD 时，接口上发送的连续邻居请求消息的数量。

在无状态自动配置过程中，重复地址检测会验证新单播 IPv6 地址的唯一性，再将地址分配给接口。

识别出重复地址后，该地址的状态会设置为 DUPLICATE，且不会使用该地址并生成以下错误消息：

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

如果重复地址是接口的链路本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。

步骤 7 （可选） 在 **NS 间隔**字段中配置 IPv6 邻居请求重新传输之间的间隔，介于 1000 和 3600000 毫秒之间。

默认值为 1000 毫秒。

邻居请求消息（ICMPv6 类型 135）由尝试发现本地链路上其他节点的链路层地址的节点在本地链路上发送。在收到邻居请求消息后，目标节点通过在本地链路上发送邻居通告消息（ICPMv6 类型 136）作出应答。

源节点接收邻居通告后，源节点与目标节点即可通信。识别邻居的链路层地址后，邻居请求消息也用于验证邻居的可访问性。当节点要验证邻居的可访问性时，邻居请求消息中的目标地址是邻居的单播地址。

本地链路中一个节点的链路层地址发生变化时，也会发送邻居通告消息。

步骤 8 （可选） 在**可达时间**字段中，配置可达性确认事件发生后远程 IPv6 节点被视为可达的时长，介于 0 和 3600000 毫米之间。

默认值为 0 毫秒。当该值为 0 时，将发送未确定的可访问时间。由接收设备来设置和跟踪可访问时间的值。

邻居可访问时间可启用检测不可用邻居。配置时间越短，检测不可用邻居的速度就越快，但是，时间缩短却在所有 IPv6 网络设备中占用了更多的 IPv6 网络带宽和处理资源。在正常 IPv6 操作中不建议设置很短的配置时间。

步骤 9 （可选） 要禁用路由器通告传输，请取消选中**启用 RA** 复选框。如果启用路由器通告传输，则可以设置 RA 的有效期和间隔。

路由器通告消息（ICMPv6 类型 134）会自动发送，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

在不希望 威胁防御 提供 IPv6 前缀的所有接口（例如，外部接口）上，您可能想要禁用这些消息。

- **RA 有效期** - 在 IPv6 路由器通告中配置路由器有效期的值，介于 0 和 9000 秒之间。

  默认值为 1800 秒。

- **RA 间隔** - 配置 IPv6 路由器通告传输之间的间隔，介于 3 和 1800 秒之间。

  默认值为 200 秒。

步骤 10 点击**确定 (OK)**。

步骤 11 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置高级接口设置

本部分介绍如何为常规防火墙模式接口配置 MAC 地址，如何设置最大传输单元 (MTU) 以及如何设置其他高级参数。

关于高级接口配置

本节介绍高级接口设置。

关于 MAC 地址

您可以手动分配 MAC 地址以覆盖默认值。 对于容器实例，FXOS 机箱会自动为所有接口生成唯一 MAC 地址。

注释 您可能想要为 威胁防御 上定义的子接口分配唯一 MAC 地址，因为它们使用父接口上相同的固化 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 威胁防御 上特定实例内发生流量中断。

注释 对于容器实例，即使您未共享子接口，如果您手动配置 MAC 地址，请确保您为同一父接口上的所有子接口使用唯一 MAC 地址，从而确保分类得当。

默认 MAC 地址

对于本地实例：

默认 MAC 地址分配取决于接口类型。

- 物理接口 - 物理接口使用已刻录的 MAC 地址。
- VLAN 接口 (Firepower 1010) - 路由防火墙模式：所有 VLAN 接口均共享一个 MAC 地址。确保所有连接的交换机均可支持此方案。如果连接的交换机需要唯一 MAC 地址，可手动分配 MAC 地址。请参阅配置 MAC 地址，第 569 页。

  透明防火墙模式：各 VLAN 接口均有唯一的 MAC 地址。如有需要，您可通过手动分配 MAC 地址覆盖生成的 MAC 地址。请参阅配置 MAC 地址，第 569 页。
- EtherChannels（Firepower 型号） - 对于 EtherChannel，属于通道组的所有接口均共享同一 MAC 地址。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。端口通道接口使用来自池中的唯一 MAC 地址；接口成员身份不影响 MAC 地址。
- EtherChannel（ASA 型号）- 端口通道接口使用编号最小的通道组接口 MAC 地址作为端口通道 MAC 地址。或者，您可以为端口通道接口配置 MAC 地址。我们建议在组通道接口成员身份更改时，配置唯一的 MAC 地址。如果删除提供端口通道 MAC 地址的接口，则端口通道 MAC 地址会更改为下一个编号最小的接口，从而导致流量中断。
- 子接口（威胁防御 定义）- 物理接口的所有子接口都使用同一个烧录 MAC 地址。您可能想为子接口分配唯一的 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 威胁防御 上特定实例内发生流量中断。

对于容器实例：

- 所有接口的 MAC 地址均取自一个 MAC 地址池。对于子接口，如果决定要手动配置 MAC 地址，请确保将唯一 MAC 地址用于同一父接口上的所有子接口，从而确保分类正确。请参阅容器实例接口的自动 MAC 地址，第 414 页。

关于 MTU

MTU 指定 威胁防御设备 在给定以太网接口上传输的最大帧负载大小。MTU 值是没有以太网报头、VLAN 标记或其他系统开销情况下的帧大小。例如，将 MTU 设置为 1500 时，预期帧大小为 1518 字节（含报头）或 1522 字节（使用 VLAN）。请勿为容纳这些报头而将 MTU 的值设得过高。

对于 Geneve，帧中会封装整个以太网数据报，因此新的 IP 数据包更大，需要更大的 MTU：您应该将 ASA VTEP 源接口 MTU 设置为网络 MTU + 306 字节。

路径 MTU 发现

威胁防御设备 支持路径 MTU 发现（如 RFC 1191 中所定义），从而使两个主机之间的网络路径中的所有设备均可协调 MTU，以便它们可以标准化路径中的最低 MTU。

默认 MTU

威胁防御设备 上的默认 MTU 为 1500 字节。该值不包括 18-22 字节的以太网报头、VLAN 标记和其他开销。

MTU 和分段

对于IPv4，如果传出IP数据包大于指定MTU，则该数据包将分为2帧或更多帧。片段在目标处（有时在中间跃点处）重组，而分片可能会导致性能下降。对于 IPv6，通常不允许对数据包进行分段。因此，IP 数据包大小应在 MTU 大小范围内，以避免分片。

对于 TCP 数据包，终端通常使用它们的 MTU 来确定 TCP 最大报文段长度（例如，MTU-40）。如果之后添加额外的 TCP 报头，例如对于站点间的 VPN 隧道，则 TCP MSS 可能需要由隧道传输实体向下调整。请参阅关于 TCP MSS，第 566 页。

对于 UDP 或 ICMP，应用应将 MTU 考虑在内，以避免分段。

注释 只要有内存空间，威胁防御设备 就可接收大于所配置的 MTU 的帧。

MTU 和巨型帧

MTU 越大，您能发送的数据包越大。加大数据包可能有利于提高网络效率。请参阅以下准则：

- 与流量路径上的 MTU 相匹配 - 我们建议将所有 威胁防御接口以及流量路径的其他设备接口上的 MTU 设为相同。匹配 MTU 可防止中间设备对数据包进行分片。
- 容纳巨型帧 - 在启用巨型帧时，MTU 可设置为 9000 字节或更高。最大值取决于型号。

关于 TCP MSS

TCP 最大报文段长度 (MSS) 是 TCP 负载在添加任何 TCP 和 IP 报头前的大小。UDP 数据包不会受到影响。建立连接时，客户端和服务器会在三次握手期间交换 TCP MSS 值。

您可以使用 FlexConfig#unique_456；默认情况下，最大 TCP MSS 设置为 1380 字节。当 威胁防御设备 需要增加数据包长度以执行 IPsec VPN 封装时，此设置非常有用。不过，对于非 IPsec 终端，应在 威胁防御设备 上禁用最大 TCP MSS。

如果设置了 TCP MSS 的最大值，当连接的任一终端请求的 TCP MSS 大于 威胁防御设备 中设定的值时，威胁防御设备 会使用 威胁防御设备 最大值覆盖请求数据包中的 TCP MSS。如果主机或服务器没有请求 TCP MSS，威胁防御设备 会假定采用 RFC 793 的默认值 536 字节 (IPv4) 或 1220 字节 (IPv6)，但不会修改数据包。例如，可以将默认 MTU 保留为 1500 字节。如果主机请求的 MSS 为 1500 减去 TCP 和 IP 报头长度，这会将 MSS 设置为 1460。如果 威胁防御设备 上的最大 TCP MSS 为 1380（默认值），威胁防御设备 会将 TCP 请求数据包中的 MSS 值改为 1380。然后，服务器会发送 1380 字节负载的数据包。然后，威胁防御设备 可向数据包中增加最多 120 字节的报头，并且仍然符合 1500 的 MTU 大小。

您还可以配置最小 TCP MSS；如果主机或服务器请求一个非常小的 TCP MSS，则 威胁防御设备 可将该值调高。默认情况下，最小 TCP MSS 未启用。

对于流向设备的流量，包括用于 SSL VPN 连接的流量，此设置不适用。威胁防御设备 使用 MTU 来推导 TCP MSS：MTU - 40 (IPv4) 或 MTU - 60 (IPv6)。

默认 TCP MSS

默认情况下，威胁防御设备 上的最大 TCP MSS 是 1380 字节。此默认值符合 VPN 连接的要求（在 VPN 连接中，报头最多可达到 120 字节）；此值在默认 MTU（1500 字节）范围内。

建议的最大 TCP MSS 设置

默认 TCP MSS 假定 威胁防御设备作为 IPv4 IPsec VPN 终端，并且 MTU 为 1500。当 威胁防御设备 用作 IPv4 IPsec VPN 终端时，它需要为 TCP 和 IP 报头容纳最多 120 个字节。

如果您要更改 MTU 值、使用 IPv6，或者不使用 威胁防御设备作为 IPsec VPN 终端，则应更改 TCP MSS 设置（使用 FlexConfig 中的 Sysopt_Basic 对象。

注释 即使您明确设置了 MSS，如果 TLS/SSL 解密或服务器发现等组件需要某个特定 MSS，它也会根据接口 MTU 设置该 MSS 并忽略您设置的 MSS。

请参阅以下准则：

- 正常流量 - 禁用 TCP MSS 限制，并接受在连接终端之间建立的值。由于连接终端一般是从 MTU 获得 TCP MSS，因此非 IPsec 数据包通常符合此 TCP MSS。
- IPv4 IPsec 终端流量 - 将最大 TCP MSS 设置为 MTU - 120。例如，如果使用巨帧并将 MTU 设置为 9000，则需要将 TCP MSS 设置为 8880，以利用新 MTU。
- IPv6 IPsec 终端流量 - 将最大 TCP MSS 设置为 MTU - 140。

网桥组流量的 ARP 检测

默认情况下，桥接组成员之间允许所有 ARP 数据包。可以通过启用 ARP 检测来控制 ARP 数据包的流量。

ARP 检测可防止恶意用户模拟其他主机或路由器（称为 ARP 欺骗）。ARP 欺骗能够启用“中间人”攻击。例如，主机向网关路由器发送 ARP 请求；网关路由器使用网关路由器 MAC 地址进行响应。但是，攻击者使用攻击者 MAC 地址（而不是路由器 MAC 地址）将其他 ARP 响应发送到主机。这样，攻击者即可在所有主机流量转发到路由器之前将其拦截。

ARP 检测确保只要静态 ARP 表中的 MAC 地址和相关 IP 地址正确，攻击者就无法利用攻击者 MAC 地址发送 ARP 响应。

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

- 如果 IP 地址、MAC 地址和源接口与 ARP 条目匹配，则数据包可以通过。
- 如果 MAC 地址、IP 地址或接口之间不匹配，则 威胁防御设备 会丢弃数据包。

- 如果 ARP 数据包与静态 ARP 表中的任何条目都不匹配，则可以将 威胁防御设备 设置为从所有接口向外转发数据包（泛洪），或者丢弃数据包。

注释 即使此参数设置为 flood，专用诊断接口也绝不会以泛洪方式传输数据包。

MAC 地址表

当你使用网桥组时，威胁防御 以与一般网桥或交换机相似的方式获悉和构建 MAC 地址表：当某个设备通过网桥组发送数据包时，威胁防御 将在其表中添加 MAC 地址。此表将 MAC 地址与源接口相关联，以便 威胁防御 可了解如何将要发送到设备的任何数据包从正确的接口发出。由于网桥组成员之间的流量须遵守 威胁防御 安全策略，因此如果数据包的目标 MAC 地址不在此表中，则 威胁防御 不会像一般网桥那样以泛洪方式传输所有接口上的原始数据包。相反，它会为直连设备或远程设备生成以下数据包：

- 面向直连设备的数据包 - 威胁防御 将生成针对目标 IP 地址的 ARP 请求，以使它能了解哪个接口接收 ARP 响应。
- 面向远程设备的数据包 - 威胁防御将生成一个针对目标 IP 地址的 ping，以使它能了解哪个接口接收 ping 应答。

系统会丢弃原始数据包。

默认设置

- 如果启用 ARP 检测，则默认情况下会以泛洪方式传输不匹配的数据包。
- 动态 MAC 地址表条目的默认超时值为 5 分钟。
- 默认情况下，每个接口会自动获悉进入流量的 MAC 地址，并且 威胁防御设备 会将对应的条目添加到 MAC 地址表中。

注释 Secure Firewall Threat Defense 生成重置数据包以重置状态检测引擎拒绝的连接。在这里，数据包的目标 MAC 地址不是根据 ARP 表查找确定的，而是直接从被拒绝的数据包（连接）中获取的。

ARP 检测和 MAC 地址表指南

- ARP 检测仅支持网桥组。
- MAC 地址表配置仅支持网桥组。

配置 MTU

自定义接口上的 MTU，以便实现允许巨型帧等目的。

对于 ISA 3000 和 threat defense virtual：将 MTU 更改为 1500 字节以上会自动启用巨帧预留。您必须重新启动系统，然后才能使用巨帧。 对于支持集群的 threat defense virtual，您可以在 Day0 配置中启用巨帧预留，因此在这种情况下无需重新启动。重新启动后，您将无法禁用巨帧预留。threat defense virtual 的例外情况是，您可以在 Day0 配置中禁用巨帧预留（如果支持）。如果在内联集中使用接口，则不使用 MTU 设置。但是，巨帧保留设置与内联集相关；巨帧使内嵌接口能够接收多达 9000 字节的数据包。要启用巨帧保留，您必须将任何接口的 MTU 设置为 1500 字节以上。

默认情况下，其他平台上会启用巨帧。

注意 当部署配置更改时，为数据接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有数据接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。此警告不适用于诊断接口或仅管理接口。有关详细信息，请参阅Snort 重启流量行为，第 144 页。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑**（）。

步骤 3 在 **常规** 选项卡上，设置 **MTU**。最小值和最大值取决于您的平台。

默认值为 1500 字节。

步骤 4 点击 **OK**。

步骤 5 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

步骤 6 对于 ISA 3000 和 threat defense virtual，如果您将 MTU 设置为 1500 字节以上，则请重新启动系统以启用巨帧保留。请参阅关闭设备，第 52 页。

配置 MAC 地址

可能需要手动分配 MAC 地址。您还可以在**设备** > **设备管理** > **高可用性**选项卡上设置主用和备用 MAC 地址。如果您在两个屏幕中均设置某个接口的 MAC 地址，则**接口** > **高级**选项卡上的地址具有较高优先级。

注释 对于容器实例，即使您未共享子接口，如果您手动配置 MAC 地址，请确保您为同一父接口上的所有子接口使用唯一 MAC 地址，从而确保分类得当。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑**（）。

步骤 3 点击 **Advanced** 选项卡。
将选择**信息 (Information)** 选项卡。

步骤 4 在**主用 MAC 地址 (Active MAC Address)** 字段中，输入 H.H.H 格式的 MAC 地址，其中 H 表示 16 位的十六进制数字。

例如，MAC 地址 00-0C-F1-42-4C-DE 将需要输入 000C.F142.4CDE。不得为 MAC 地址设置组播位，即左起第二个十六进制数字不能是奇数。

步骤 5 在**备用 MAC 地址 (Standby MAC Address)** 字段中，输入用于高可用性的 MAC 地址。

如果主用设备发生故障切换，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

步骤 6 点击**确定 (OK)**。

步骤 7 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

添加静态 ARP 条目

默认情况下，桥接组成员之间允许所有 ARP 数据包。可以通过启用 ARP 检测来控制 ARP 数据包的流量（请参阅配置 ARP 检测，第 615 页）。ARP 检测会对比 ARP 数据包与 ARP 表中的静态 ARP 条目。

对于路由接口，可以输入静态 ARP 条目，但通常动态条目就足够了。对于路由接口，使用 ARP 表向直连主机交付数据包。虽然发件人可根据 IP 地址识别数据包目标，但在以太网上实际交付数据包依赖于以太网 MAC 地址。当路由器或主机希望在直连网络上交付数据包时，它会发送 ARP 请求来寻求与该 IP 地址关联的 MAC 地址，然后根据 ARP 响应将数据包交付到 MAC 地址。主机或路由器可保留 ARP 表，所以不必对需要交付的每个数据包都发送 ARP 请求。只要在网络上发送 ARP 响应，便会动态更新 ARP 表，但如果一段时间未使用条目，则它会超时。如果某个条目错误（例如给定 IP 地址的 MAC 地址改变），该条目需要超时后，才能为其更新新信息。

对于透明模式，威胁防御 仅对进出 威胁防御 的流量（例如管理流量）使用 ARP 表中的动态 ARP 条目。

开始之前

此屏幕仅适用于指定的接口。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑**（）。

步骤 3 点击**高级**选项卡，然后点击 **ARP** 选项卡（在透明模式下，称为 **ARP 和 MAC**）。

步骤 4 点击**添加 ARP 配置**。
屏幕上随即会显示**添加 ARP 配置**对话框。

步骤 5 在 **IP 地址**字段中，输入主机的 IP 地址。

步骤 6 在 **MAC 地址**字段中，输入主机的 MAC 地址；例如，00e0.1e4e.3d8b。

步骤 7 要对该地址执行代理 ARP，请选中**启用别名**复选框。

如果 威胁防御 设备收到指定 IP 地址的 ARP 请求，则会使用指定 MAC 地址做出响应。

步骤 8 点击**确定**，然后再次点击**确定**退出“高级”设置。

步骤 9 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

添加静态 MAC 地址并为网桥组禁用 MAC 学习

通常，当来自特定 MAC 地址的流量进入某个接口时，MAC 地址会动态添加到 MAC 地址表中。可以禁用 MAC 地址获悉；然而除非将 MAC 地址静态添加到表中，否则没有流量可以通过 威胁防御 设备。还可以向 MAC 地址表中添加静态 MAC 地址。添加静态条目的一个好处是，可以防止 MAC 欺骗。如果与静态条目具有相同 MAC 地址的客户端尝试向与静态条目不匹配的接口发送流量，则威胁防御 设备会丢弃这些流量并生成系统消息。当添加静态 ARP 条目时（请参阅添加静态 ARP 条目，第 570 页），静态 MAC 地址条目会自动添加到 MAC 地址表中。

开始之前

此屏幕仅适用于指定的接口。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑**（）。

步骤 3 点击**高级 (Advanced)**选项卡，然后点击 **ARP 和 MAC (ARP and MAC)** 选项卡。

步骤 4 （可选） 通过取消选中**启用 MAC 学习**复选框来禁用 MAC 学习。

步骤 5 要添加静态 MAC 地址，请点击**添加 MAC 配置 (Add MAC Config)**。
此时将显示**添加 MAC 配置**对话框。

步骤 6 在 **MAC 地址 (MAC Address)** 字段中，输入主机的 MAC 地址；例如，00e0.1e4e.3d8b。点击**确定 (OK)**。

步骤 7 点击**确定 (OK)** 以退出高级设置。

步骤 8 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

设置安全配置参数

本部分介绍如何防止 IP 欺骗、允许完整分段重组以及覆盖在**平台设置**中的设备级别设置的默认分段设置。

反欺骗

本部分使您可以在接口上启用单播反向路径转发。单播 RPF 根据路由表来确保所有数据包均有与正确的源接口匹配的源 IP 地址，从而避免 IP 欺骗（即数据包使用不正确的源 IP 地址以掩盖其真正来源）。

通常情况下，威胁防御 设备在确定向何处转发数据包时只查看目标地址。单播 RPF 会指示设备还查找源地址；其因此被称为“反向路径转发”。对于您要允许通过威胁防御 设备的任何流量，设备路由表必须包括回到源地址的路由。有关详细信息，请参阅 RFC 2267。

例如，对于外部流量，威胁防御 设备可使用默认路由来满足单播 RPF 保护。如果流量从外部接口进入，则路由表不知道源地址，而设备使用默认路由将外部接口正确识别为源接口。

如果流量从路由表中包含的已知地址进入外部接口，但与内部接口关联，则威胁防御 设备会丢弃该数据包。同样，如果流量从未知源地址进入内部接口，则设备会丢弃数据包，因为匹配的路由（默认路由）指示外部接口。

单播 RPF 的实施过程如下：

- ICMP 数据包没有会话，因此要检查每个数据包。
- UDP 和 TCP 有会话，因此初始数据包要求反向路由查找。对于在会话期间到达的后续数据包，使用作为部分会话来维护的现有状态进行检查。系统会检查非初始数据包，以确保它们到达初始数据包使用的同一接口。

每个数据包的分段数

默认情况下，威胁防御设备允许每个 IP 数据包最多包含 24 个分段，以及最多 200 个等待重组的分段。如果您有定期对数据包进行分段的应用（如 NFS over UDP），可能需要让分段位于您的网络上。但是，如果没有对流量分段的应用，则我们建议您不要允许分段通过威胁防御 设备。分段的数据包通常用作 DoS 攻击。

分段重组

威胁防御 设备执行以下分段重组过程：

- 系统会收集 IP 分段，直到形成分段集或达到超时间隔。
- 如果分段集形成，则对片段集执行完整性检查。这些检查包括无重叠、无尾部溢出和无链溢出。
- 在 威胁防御 设备处终止的 IP 分段始终会完全重组。
- 如果禁用了**完全分段重组**（默认设置），则分段集会转发到传输层以进一步处理。
- 如果启用了**完全分段重组**，则分段集首先会合并为单个 IP 数据包。然后，该单个 IP 数据包被转发到传输层，以供进一步处理。

开始之前

此屏幕仅适用于指定的接口。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑**（）。

步骤 3 点击**高级**选项卡，然后点击**安全配置**选项卡。

步骤 4 要启用单播反向路径转发，请选中**反欺骗**复选框。

步骤 5 要启用完整分段重组，请选中**完整分段重组**复选框。

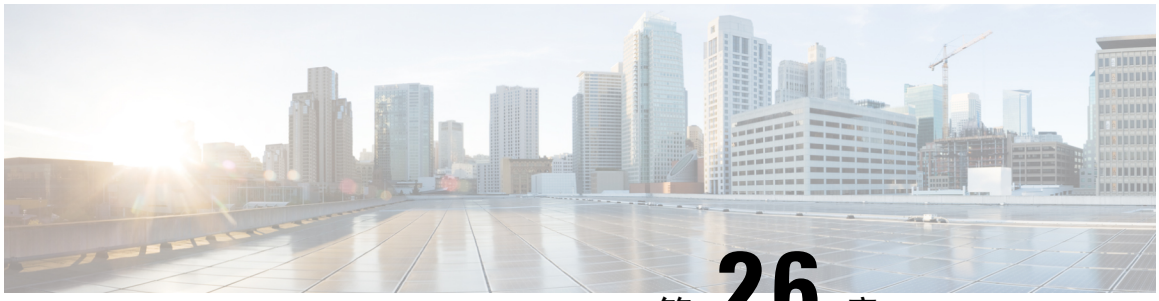
步骤 6 要更改每个数据包所允许的分段数，请选中**覆盖默认分段设置**复选框，并设置以下值：

- **大小** - 设置 IP 重组数据库中等待重组的最大数据包数。默认值为 200。将该值设置为 1 会禁用分段。
- **链** - 设置完整 IP 数据包可分成的最大数据包数。默认值为 24 个数据包。
- **超时** - 设置等待整个分段数据包到达的最大秒数。在数据包的第一个分段到达后计时器启动。如果在指定秒数后数据包的分段没有全部抵达，则已收到的数据包的所有分段将被丢弃。默认值为 5 秒。

步骤 7 点击**确定 (OK)**。

步骤 8 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。



第 26 章

内联集和被动接口

您可以配置仅限 IPS 被动接口、被动 ERSPAN 接口和内联集。仅 IPS 模式的接口将绕过许多防火墙检查，仅支持 IPS 安全策略。如果您有单独的防火墙来保护这些接口，并且不希望造成防火墙功能的开销，则可能需要实施仅限 IPS 的接口。

关于 IPS 接口

本节介绍了 IPS 接口。

IPS 接口类型

仅 IPS 模式的接口将绕过许多防火墙检查，仅支持 IPS 安全策略。如果您有单独的防火墙来保护这些接口，并且不希望造成防火墙功能的开销，则可能需要实施仅限 IPS 的接口。

注释 防火墙模式只影响常规的防火墙接口，而不影响仅 IPS 接口，如内联集或被动接口。仅 IPS 接口可以在两种防火墙模式下使用。

仅 IPS 接口可以部署为以下类型：

- 内嵌集，带有可选分路模式 - 内嵌集的作用类似于导线上的凹凸，并将两个接口绑定在一起插入到现有网络中。此功能使 FTD 可以安装在任何网络环境中，而无需配置相邻网络设备。内联接口无条件接收所有流量，但是，除非已明确丢弃，否则这些接口上接收的所有流量将在内联集外重传。

  在分流模式下，FTD 会进行内联部署，但网络流量不受干扰。相反，FTD 会复制每个数据包，这样它就可以对数据包进行分析。请注意，这些类型的规则在触发时会生成入侵事件，而且入

侵事件表视图显示了触发数据包会在内联部署中被丢弃。在已部署内联的FTD上使用分流模式有很多优点。例如，您可以设置FTD和网络之间的布线，就像FTD是内联，并分析FTD生成的多种入侵事件。根据结果，您可以修改入侵策略，并添加最好地保护您的网络却不影响有效性的丢弃规则。准备部署FTD内联时，您可以禁用分流模式，并开始丢弃可疑流量，而无需重新配置FTD和网络之间的走线。

注释 分流模式显著影响FTD性能，具体取决于流量。

注释 内嵌集可能是您所熟悉的“透明内联集”，但内联接口类型与透明防火墙模式或防火墙类型接口无关。

- 被动或ERSPAN被动 - 被动接口使用交换机SPAN或镜像端口监控网络中流动的流量。SPAN或镜像端口允许从交换机的其他端口复制流量。此功能可以提供网络内的系统可视性，而不会影响网络流量。如果在被动部署中配置FTD，FTD将无法执行某些操作，例如，阻止流量或流量整形。被动接口无条件接收所有流量，这些接口不会重传接收到的流量。封装远程交换端口分析器(ERSPAN)接口允许您监控分布于多个交换机的源端口流量，并使用GRE来封装流量。仅当FTD处于路由防火墙模式时，才允许ERSPAN接口。

注释 由于混杂模式限制，某些使用SR-IOV驱动程序的Intel网络适配器（例如Intel X710或82599）不支持在NGFWv上将SR-IOV接口用作被动接口。在此情况下，请使用支持此功能的网络适配器。有关英特尔网络适配器的详细信息，请参阅英特尔以太网产品。

关于内联集的硬件旁路

对于支持的型号上的某些接口模块（请参阅内联集的要求和必备条件，第577页），您可以启用硬件旁路功能。硬件旁路可确保流量在停电期间继续在内联接口对之间流动。在软件或硬件发生故障时，此功能可用于维持网络连接性。

硬件旁路触发器

硬件旁路可以在以下情况下触发：

- 威胁防御崩溃
- 威胁防御 重新启动
- 安全模块重新启动
- 机箱崩溃
- 机箱重新启动或升级

- 手动触发
- 机箱断电
- 安全模块断电

注释 硬件旁路适用于计划外/意外故障情况，并且在计划的软件升级期间不会自动触发。硬件旁路仅在计划的升级过程结束时，当 威胁防御 应用重新启动时才会启用。

硬件旁路切换

当从正常操作切换到硬件旁路或从硬件旁路切换回正常操作时，流量可能会中断几秒钟。中断时长可能受许多因素影响；例如，铜缆端口自动协商、光纤链路合作伙伴的行为（比如如何处理链路故障和去抖时间）、生成树协议汇聚、动态路由协议汇聚等等。在此期间，您可能会遇到连接中断。

还有可能在恢复正常运行后分析连接中游时由于应用识别错误而遇到连接中断。

Snort 故障开启与硬件旁路

对于不是分路模式下的内联集的内联集，您可以使用“Snort 故障开启”选项，在不检查 Snort 进程何时繁忙或关闭的情况下丢弃流量或允许流量通过。除了分路模式下的内联集，其他所有内联集上都支持“Snort 故障开启”，而不仅仅是支持硬件旁路的接口。

硬件旁路功能允许流量在硬件故障（包括完全断电以及有限的一些软件故障）期间流动。触发Snort故障开启的软件故障不会触发硬件旁路。

硬件旁路 状态

如果系统通电，则旁路 LED 指示灯指示硬件旁路状态。请参阅 Firepower 机箱硬件安装指南中有关 LED 的说明。

内联集的要求和必备条件

型号支持

威胁防御

用户角色

- 管理员
- 访问管理员
- 网络管理员

硬件旁路 支持

对于以下型号上特定网络模块的接口对，威胁防御 支持 硬件旁路：

- Firepower 9300
- Firepower 4100
- Secure Firewall 3100
- Firepower 2130 和 2140

注释 ISA 3000 会对硬件旁路进行单独实施，你可以只用 FlexConfig 来启用它（请参阅 FlexConfig 策略，第 1991 页）。不要按照本章来配置 ISA 3000 硬件旁路。

注释 您可以将 硬件旁路 接口用作常规接口，而无需启用 硬件旁路 功能。

这些型号的受支持 硬件旁路 网络包括：

- Firepower 4100：
  - Firepower 6 端口 1G SX FTW 单位宽网络模块 (FPR4K-NM-6X1SX-F)
  - Firepower 6 端口 10G SR FTW 单位宽网络模块 (FPR4K-NM-6X10SR-F)
  - Firepower 6 端口 10G LR FTW 单位宽网络模块 (FPR4K-NM-6X10LR-F)
  - Firepower 2 端口 40G SR FTW 单位宽网络模块 (FPR4K-NM-2X40G-F)
  - Firepower 8 端口 1G 铜 FTW 单位宽网络模块 (FPR4K-NM-8X1G-F)
- Firepower 9300：
  - Firepower 6 端口 10G SR FTW 单位宽网络模块 (FPR9K-NM-6X10SR-F)
  - Firepower 6 端口 10G LR FTW 单位宽网络模块 (FPR9K-NM-6X10LR-F)
  - Firepower 2 端口 40G SR FTW 单位宽网络模块 (FPR9K-NM-2X40G-F)
- Cisco Secure Firewall 3100:
  - 6 端口 1G SFP 故障时自动旁路网络模块，SX（多模）(FPR3K-XNM-6X1SXF)
  - 6 端口 10G SFP 故障时自动旁路网络模块，SR（多模）(FPR3K-XNM-6X10SRF)
  - 6 端口 10G SFP 故障时自动旁路网络模块，LR（单模式）(FPR3K-XNM-6X10LRF)
  - 6 端口 25G SFP 故障时自动旁路网络模块，SR（多模）(FPR3K-XNM-X25SRF)
  - 6 端口 25G 故障时自动旁路网络模块，LR（单模式）(FPR3K-XNM-6X25LRF)

- 8 端口 1G 铜缆故障时自动旁路网络模块，RJ45（铜）(FPR3K-XNM-8X1GF)

- Firepower 2130 和 2140：
  - Firepower 6 端口 1G SX FTW 单位宽网络模块 (FPR2K-NM-6X1SX-F)
  - Firepower 6 端口 10G SR FTW 单位宽网络模块 (FPR2K-NM-6X10SR-F)
  - Firepower 6 端口 10G LR FTW 单位宽网络模块 (FPR2K-NM-6X10LR-F)

硬件旁路 仅可使用以下端口对：

- 1、2
- 3、4
- 5、6
- 7、8

内联集和被动接口的准则

防火墙模式

- 仅当设备处于路由防火墙模式时，才允许 ERSPAN 接口。

多实例模式

- 不支持多实例共享接口。您必须使用非共享接口。
- 不支持多实例机箱定义的子接口。必须使用物理接口或 EtherChannel 接口。

一般准则

- 内联集和被动接口仅支持物理接口和 EtherChannel，并且不能使用 VLAN 或其他虚拟接口，包括多实例机箱定义的子接口。
- 使用内联集时，不允许双向转发检测 (BFD) 回应数据包通过 威胁防御。如果 威胁防御 的一端有两个邻居运行 BFD，则 威胁防御 会因二者具有相同的源 IP 地址和目标 IP 地址且疑似属于 LAND 攻击而丢弃 BFD 回应数据包。
- 对于内联集和被动接口， 威胁防御 在数据包中最多支持两个 802.1Q 报头（也称为 Q-in-Q 支持），但 Firepower 4100/9300 仅支持一个 802.1Q 报头。**注意**：防火墙类型的接口不支持 Q-in-Q，并且仅支持一个 802.1Q 报头。

硬件旁路 指南

- 硬件旁路 端口仅对内联集支持。

- 硬件旁路 端口不能是 EtherChannel 的一部分。
- 硬件旁路 在高可用性模式下不受支持。
- Firepower 9300 支持使用机箱内集群的硬件旁路 端口。当机箱中的最后一个设备出现故障时，将端口置于硬件旁路模式。不支持机箱间集群，因为机箱间集群仅支持跨区以太网通道； 硬件旁路 端口不能是 EtherChannel 的一部分。
- 如果 Firepower 9300 上机箱内集群中的所有模块都发生故障，则在最后一个设备上触发硬件旁路，使流量继续通过。当设备重新恢复时，硬件旁路将恢复为备用模式。但是，当您使用匹配应用程序流量的规则时，这些连接可能会被丢弃，且需要重新建立。由于在集群设备上未保留状态信息，并且设备无法将流量标识为属于允许的应用程序，连接会被丢弃。若要避免流量被丢弃，请使用基于端口的规则，而不是基于应用程序的规则（如果适合您的部署）。
- 您可以将 硬件旁路 接口用作常规接口，而无需启用 硬件旁路 功能。

IPS 接口上不支持的防火墙功能

- DHCP 服务器
- DHCP 中继
- DHCP 客户端
- TCP 拦截
- 路由
- NAT
- VPN
- 应用检测
- QoS
- NetFlow
- VXLAN

配置被动接口

本节介绍如何执行以下操作：

- 启用接口。默认情况下，接口处于禁用状态。
- 将接口模式设为被动或 ERSPAN。对于 ERSPAN 接口，需要设置 ERSPAN 参数和 IP 地址。
- 更改 MTU。默认情况下，MTU 设置为 1500 字节。有关 MTU 的详细信息，请参阅关于 MTU，第 565 页。
- 设置特定的速度和双工（如有）。默认情况下，速度和双工均设置为“自动”。

注释 对于 FXOS 机箱上的 Cisco Secure Firewall Threat Defense，可在 Firepower 4100/9300上配置基本接口设置。有关详细信息，请参阅配置物理接口，第 423 页。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑**（）。

步骤 3 在**模式**下拉列表中，选择**被动**或 **Erspan**。

步骤 4 选中**启用**复选框以启用此接口。

步骤 5 在**名称**字段中，输入长度最大为 48 个字符的名称。

步骤 6 从**安全区域**下拉列表中选择一个安全区域，或者点击**新建**添加一个新的安全区域。

步骤 7 （可选） 在**说明**字段中添加说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 8 （可选） 在**常规 (General)** 中，将 **MTU** 设置为介于 64 和 9198 字节之间；对于 Cisco Secure Firewall Threat Defense Virtual 和 FXOS 机箱上的 Cisco Secure Firewall Threat Defense，最大值为 9000 字节。

默认值为 1500 字节。

步骤 9 对于 ERSPAN 接口，请设置以下参数：

- **流 ID** - 配置源和目标会话使用的 ID 来标识 ERSPAN 流量，介于 1 和 1023 之间。在 ERSPAN 目标会话配置中也必须输入此 ID。
- **源 IP** - 配置用作 ERSPAN 流量的源的 IP 地址。

步骤 10 对于 ERSPAN 接口，请在 **IPv4** 上设置 IPv4 地址和掩码。

步骤 11 （可选） 点击**硬件配置 (Hardware Configuration)**，设置双工和速度。

确切的速度和复用选项取决于您的硬件。

- **复用 (Duplex)** - 选择**全 (Full)**、**半 (Half)**或**自动 (Auto)**。默认值为“自动”。
- **速度 (Speed)** - 选择 **10**、**100**、**1000** 或**自动 (Auto)**。默认值为“自动”。

步骤 12 点击**确定 (OK)**。

步骤 13 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置内联集

此部分启用并命名可以添加到内联集的两个物理接口。您也可以选择为支持的接口对启用硬件旁路。

注释 对于 Firepower 4100/9300，可在 FXOS 中配置基本接口设置。有关详细信息，请参阅配置物理接口，第 423 页。

开始之前

- 我们建议您为连接到 威胁防御 内联接口对且启用 STP 的交换机设置 STP PortFast。此设置对硬件旁路配置尤其有用，可以减少绕行时间。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑**（）。

步骤 3 在**模式 (Mode)** 下拉列表中，选择**无 (None)**。

在将此接口添加到内联集后，此字段将显示的模式为“内联”。

步骤 4 选中**启用**复选框以启用此接口。

步骤 5 在**名称**字段中，输入长度最大为 48 个字符的名称。

暂时不要设置安全区域；此过程中，必须在稍后创建好内联集后，再设置它。

步骤 6 （可选） 在**说明**字段中添加说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 7 （可选） 点击**硬件配置 (Hardware Configuration)**，设置双工和速度。

确切的速度和复用选项取决于您的硬件。

- **复用 (Duplex)** - 选择**全 (Full)**、**半 (Half)**或**自动 (Auto)**。默认值为“自动”。
- **速度 (Speed)** - 选择 **10**、**100**、**1000** 或**自动 (Auto)**。默认值为“自动”。

步骤 8 点击**确定 (OK)**。

请勿为此接口设置任何其他设置。

步骤 9 对于要添加到内联集的第二个接口，请点击**编辑**（）。

步骤 10 同第一个接口一样配置相应设置。

步骤 11 点击**内联集 (Inline Sets)**。

步骤 12 点击**添加内联集 (Add Inline Set)**。
此时将显示**添加内联集 (Add Inline Set)** 对话框，其中**常规 (General)** 处于选中状态。

步骤 13 在**名称**字段中，输入内联集的名称。

步骤 14 （可选） 更改 **MTU** 以启用巨帧。

对于内联集，不使用 MTU 设置。但是，巨型帧设置与内联集相关；巨型帧使内嵌接口能够接收多达 9000 字节的数据包。要启用巨型帧，必须将设备上的任意接口的 MTU 设置为 1500 字节以上。

步骤 15 配置 硬件旁路。

a) 对于**绕行 (Bypass)** 模式，请选择以下其中一个选项：

- **禁用** - 对支持硬件旁路的接口，将硬件旁路设置为禁用，或使用不支持硬件旁路的接口。
- **备用** - 在支持硬件旁路的接口上，将硬件绕行设为备用状态。只有成对的硬件旁路接口才会显示出来。在“备用”状态下，接口可以保持正常运行，直至发生触发事件。
- **强制绕行** - 手动强制接口对进入绕行状态。对于处于“强制绕行”模式的任何接口对，**内联集**均显示**是**。

b) 在**可用接口对 (Available Interfaces Pairs)** 区域中，点击某个接口对，然后点击**添加 (Add)**，以将其移动至**选定的接口对 (Selected Interface Pair)** 区域。

此区域中会显示模式设置为“无”的已命名接口和已启用接口之间所有可能的配对。

步骤 16 （可选） 点击**高级 (Advanced)** 设置以下可选参数：

- **分流模式** - 设置为内联分流模式。

  请注意，您不能在同一内联集中启用此选项和严格 TCP 执行选项。

  注释 分流模式 显著 影响 威胁防御 性能，具体取决于流量。

- **传播链路状态** - 配置链路状态传播。

  当内联集的一个接口断开时，链路状态传播自动关闭内联接口对的第二个接口。当被关闭的接口恢复运行时，第二个接口也将自动恢复运行。换句话说，如果一个接口的链路状态更改，设备会感知该更改并更新其他接口的链路状态以与其匹配。请注意，设备最多需要 4 秒即可传播链路状态更改。在将路由器配置为在处于故障状态的网络设备上自动重新路由流量的弹性网络环境中，链路状态传播特别有用。

- **严格 TCP 执行** - 为最大程度地提高 TCP 安全性，您可以启用严格执行，从而阻止未完成三次握手的连接。

  严格执行功能也阻止：

  - 三次握手尚未完成的连接的非 SYN TCP 数据包
  - TCP 连接上由发起方发出的、响应方尚未发送 SYN-ACK 数据包的非 SYN/RST 数据包
  - TCP 连接上由响应方在 SYN 数据包之后、但在会话建立前发出的非 SYN-ACK/RST 数据包

- 来自发起方或响应方的已建立 TCP 连接上的 SYN 数据包

- **Snort 故障时自动打开** - 如果您希望在 Snort 进程繁忙或关闭时，新流量和现有流量不检查直接通过（启用）或丢弃（禁用），请启用或禁用**繁忙 (Busy)** 和**关闭 (Down)** 选项之一或两项都启用。

  默认情况下，当Snort进程关闭时，流量会不进行检查就通过，而当进程繁忙时，流量会丢弃。

  当 Snort 进程处于以下状态时：

  - “繁忙”- 由于流量缓冲区已满，进程无法足够快速地处理流量，这表明流量超过设备的处理能力，或者存在其他软件资源问题。
  - “关闭”- 由于您部署了要求进程重启的配置，因此它会重启。请参阅部署或激活时重启 Snort 进程的配置，第 146 页。

    当Snort进程关闭并重新启动后，它会检查新的连接。为了防止误报和漏报，此进程不检查内联、路由或透明接口上的现有连接，因为最初的会话信息可能已经在它关闭时丢失。

  注释 如果 Snort 无法打开，则依赖 Snort 进程的功能会停止运行，这些功能包括应用控制和深度检查。借助简单、易于确定的传输层和网络层特征，系统仅执行基本访问控制。

步骤 17 点击**接口 (Interfaces)**。

步骤 18 对一个成员接口点击**编辑**（ ）。

步骤 19 从**安全区域 (Security Zone)** 下拉列表中选择一个安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

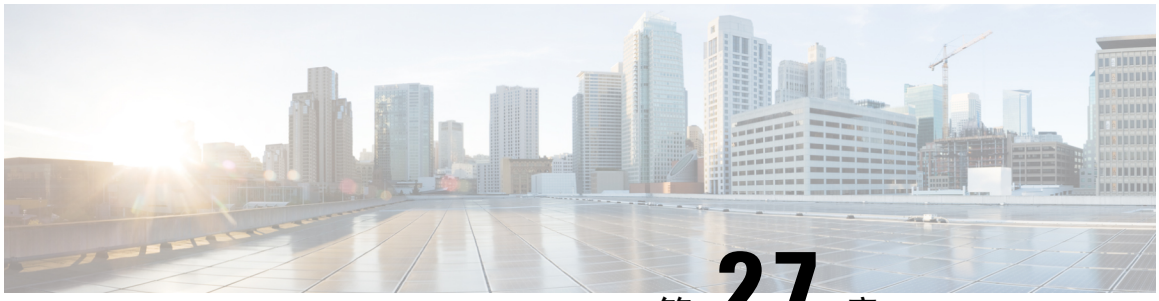
只有在将接口添加到内联集之后，才能设置安全区域；将接口添加到内联集可将模式配置为“内联”(Inline)，并且可让您选择内联类型的安全区域。

步骤 20 点击**确定 (OK)**。

步骤 21 设置第二个接口的安全区域。

步骤 22 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。



第 27 章

DHCP 和 DDNS

以下主题介绍 DHCP 和 DDNS 服务以及如何在威胁防御设备上配置这些服务。

关于 DHCP 和 DDNS 服务

以下主题介绍 DHCP 服务器、DHCP 中继代理和 DDNS 更新。

关于 DHCPv4 服务器

DHCP 为 DHCP 客户端提供网络配置参数，如 IP 地址。威胁防御设备 可以为连接到 威胁防御设备 接口的 DHCP 客户端提供 DHCP 服务器。DHCP 服务器直接为 DHCP 客户端提供网络配置参数。

IPv4 DHCP 客户端使用广播而非组播地址到达服务器。DHCP 客户端侦听 UDP 端口 68 上的消息；DHCP 服务器侦听 UDP 端口 67 上的消息。

IPv6 的 DHCP 服务器不受支持；但您可以为 IPv6 流量启用 DHCP 中继。

DHCP 选项

DHCP 提供用于将配置信息传递至 TCP/IP 网络中主机的标准。配置参数在存储于 DHCP 消息的 Options 字段中的标记项目中携带，数据也称为选项。供应商信息也存储在 Options 中，并且所有供应商信息扩展均可用作 DHCP 选项。

例如，思科 IP 电话从 TFTP 服务器下载其配置。当思科 IP 电话启动时，如果其不让 IP 地址和 TFTP 服务器 IP 地址均得以预配置，则其将向 DHCP 服务器发送带有选项 150 或 66 的请求以获取此信息。

- DHCP 选项 150 提供 TFTP 服务器列表的 IP 地址。

- DHCP 选项 66 提供单一 TFTP 服务器的 IP 地址或主机名。
- DHCP 选项 3 设置默认路由。

单一请求可能同时包括选项 150 和 66。在此情况下，如在 ASA 上已配置这两个选项，则 ASA DHCP 服务器将在响应中为两个选项提供值。

您可以使用高级 DHCP 选项将 DNS、WINS 和域名参数提供给 DHCP 客户端；DHCP 选项 15 用于 DNS 域名后缀。您还可以使用 DHCP 自动配置设置获得这些值或手动定义这些值。如果使用多种方法定义此信息，则按以下序列将其传递给 DHCP 客户端：

1. 手动配置的设置。
2. 高级 DHCP 选项设置。
3. DHCP 自动配置设置。

例如，可以手动定义要 DHCP 客户端接收的域名，然后启用 DHCP 自动配置。尽管 DHCP 自动配置要结合 DNS 和 WINS 服务器来发现域，但手动定义的域名将与已发现的 DNS 和 WINS 服务器名称一起传递到 DHCP 客户端，因为手动定义的域名将取代通过 DHCP 自动配置过程发现的域名。

关于 DHCP 中继代理

您可以配置 DHCP 中继代理以向一个或多个 DHCP 服务器转发接口上收到的 DHCP 请求。DHCP 客户端使用 UDP 广播发送其初始 DHCPDISCOVER 消息，因为它们没有与其所连接网络有关的信息。如果客户端位于不包含服务器的网段，则通常 UDP 广播不会由 威胁防御设备 进行转发，因为它不转发广播流量。DHCP 中继代理可用于配置用来接收广播的 威胁防御设备 的接口，以将 DHCP 请求转发至另一接口上的 DHCP 服务器。

DHCP 和 DDNS 的要求和必备条件

型号支持

威胁防御

用户角色

- 管理员
- 访问管理员
- 网络管理员

DHCP 和 DDNS 服务准则

本节介绍在配置 DHCP 和 DDNS 服务之前应检查的准则和限制。

防火墙模式

- 在透明防火墙模式下，或在 BVI 或网桥组成员接口上的路由模式下，不支持 DHCP 中继。
- 在网桥组成员接口上的透明防火墙模式下，支持 DHCP 服务器。 在路由模式下，在 BVI 接口（而非网桥组成员接口）上支持 DHCP 服务器。BVI 必须具有名称，DHCP 服务器才能运行。
- 在透明防火墙模式下，或在 BVI 或网桥组成员接口上的路由模式下，不支持 DDNS。

IPv6

不支持 IPv6支持 IPv6 用于 DHCP 中继。

DHCPv4 服务器

- 最大可用 DHCP 池为 256 个地址。
- 只能在每个接口上配置一个 DHCP 服务器。每个接口均可使用其自己的地址池。但是，其他 DHCP 设置（如 DNS 服务器、域名、选项、ping 超时和 WINS 服务器）以全局方式配置，且供 DHCP 服务器在所有接口上使用。
- 如果某个接口也启用了 DHCP 服务器，则不能将该接口配置为 DHCP 客户端；您必须使用静态 IP 地址。
- 不能在同一设备上同时配置 DHCP 服务器和 DHCP 中继，即使要在不同接口上启用它们也是如此；只能配置一种类型的服务。
- 威胁防御设备 不支持 QIP DHCP 服务器与 DHCP 代理服务一起使用。
- DHCP 服务器不支持 BOOTP 请求。

DHCP 中继

- 最多可以配置 10 台 DHCPv4 中继服务器，这些服务器为全局和接口专用服务器的组合，其中每个接口最多允许 4 台服务器。
- 最多可以配置 10 台 DHCPv6 中继服务器。不支持 IPv6 的接口专用服务器。
- 不能在同一设备上同时配置 DHCP 服务器和 DHCP 中继，即使要在不同接口上启用它们也是如此；只能配置一种类型的服务。
- 在透明防火墙模式下， DHCP 中继服务不可用。但是，可以通过使用访问规则允许 DHCP 流量通过。要允许 DHCP 请求和回复通过 威胁防御设备，需要配置两条访问规则，一条允许从内部接口到外部接口（UDP 目标端口 67）的 DCHP 请求，另一条允许来自其他方向（UDP 目标端口 68）的服务器的回复。
- 对于 IPv4，客户端必须直接连接到 威胁防御设备 且不能通过另一个中继代理或路由器发送请求。对于 IPv6，威胁防御设备支持来自另一个中继服务器的数据包。
- DHCP 客户端必须与 威胁防御设备 中继请求的 DHCP 服务器位于不同接口。
- 不能在流量区域内的接口上启用 DHCP 中继。

- 虚拟隧道接口 (VTI) 上不支持 DHCP 中继。

配置 DHCPv4 服务器

请参阅以下步骤来配置 DHCPv4 服务器。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 依次选择 **DHCP** > **DHCP 服务器**。

步骤 3 配置以下 DHCP 服务器选项：

- **Ping 超时** - 威胁防御设备等待 DHCP ping 尝试超时的时间量（以毫秒为单位）。值的范围为 10 到 10000 毫秒。默认值为 50 毫秒。

  为避免地址冲突，威胁防御设备会向一个地址发动两个 ICMP ping 数据包，然后再将该地址分配给 DHCP 客户端。

- **租赁时长** - 客户端在租赁到期前可以使用其已分配的 IP 地址的时间量（以秒为单位）。值的范围为 300 到 1048575 秒。默认值为 3600 秒（1 小时）。

- （路由模式）**自动配置** - 在 威胁防御设备上启用 DHCP 自动配置。自动配置使 DHCP 服务器能为 DHCP 客户端提供从运行于指定接口上的 DHCP 客户端获得的 DNS 服务器、域名和 WINS 服务器信息。否则，可以禁用自动配置，并在第 4 步自行添加值。

- （路由模式）**接口** - 指定用于自动配置的接口。 对于具有虚拟路由功能的设备，此接口只能是全局虚拟路由器接口。

步骤 4 要覆盖自动配置的设置，请进行以下操作：

- 输入接口的域名：例如，您的设备可能位于 Your_Company 域中。

- 从下拉列表中，选择为该接口配置的DNS服务器（主服务器和辅助服务器）。要添加新的DNS服务器，请参阅创建网络对象， 第 999 页。

- 从下拉列表中，选择为该接口配置的 WINS 服务器（主服务器和辅助服务器）。要添加新的 WINS 服务器，请参阅创建网络对象， 第 999 页。

步骤 5 选择 **服务器**，点击 **添加**，然后配置以下选项：

- **接口** -- 从下拉列表中选择接口。在透明模式下，指定命名桥接组成员接口。 在路由模式下，请指定一个命名路由接口或命名 BVI；请勿指定桥接组成员接口。请注意，还必须指定 BVI 每个桥接组成员接口才能使 DHCP 服务器运行。

- **地址池** - DHCP 服务器使用的 IP 地址的范围（从最低到最高）。IP 地址范围必须与选定接口位于相同的子网上，且不能包括接口自身的 IP 地址。

- **启用 DHCP 服务器** - 在所选接口上启用 DHCP 服务器。

步骤 6 点击**确定**以保存 DHCP 服务器配置。

步骤 7 （可选）选择 **高级**，点击 **添加**，然后指定希望该选项返回到 DHCP 客户端的信息的类型：

- **选项代码** - 威胁防御设备支持 RFC 2132、RFC 2562 和 RFC 5510 中列出的 DHCP 选项，以发送信息。所有 DHCP 选项 (1-255) 均受支持，但 1、12、50 – 54、58 – 59、61、67 和 82 除外。有关 DHCP 选项代码的更多信息，请参阅关于 DHCPv4 服务器，第 585 页。

  注释 威胁防御设备不会验证您提供的选项类型和值是否与RFC 2132中定义的选项代码的预期类型和值匹配。有关选项代码及其关联的类型和期望值的详细信息，请参阅RFC 2132。

- **类型** - DHCP 选项类型。可用选项包括 **IP**、**ASCII** 和 **十六进制**。如果选择了“IP”，则必须在“IP 地址”字段中添加 IP 地址。如果选择了“ASCII”，则必须在“ASCII”字段中添加 ASCII 值。如果选择了“十六进制”，则必须在“十六进制”字段中添加十六进制值。
- **IP 地址 1** 和 **IP 地址 2** - 要通过此选项代码返回的 IP 地址。要添加新的 IP 地址，请参阅创建网络对象，第 999 页。
- **ASCII** - 将返回到 DHCP 客户端的 ASCII 值。字符串不能包含空格。
- **十六进制** - 将返回到DHCP客户端的十六进制值。该字符串的位数必须是偶数，并且不含空格。您无需使用 0x 前缀。

步骤 8 点击**确定**以保存选项代码配置。

步骤 9 在“DHCP”页面上点击**保存**，以保存更改。

配置 DHCP 中继代理

您可以配置 DHCP 中继代理以向一个或多个 DHCP 服务器转发接口上收到的 DHCP 请求。DHCP 客户端使用UDP广播发送其初始DHCPDISCOVER消息，因为它们没有与其所连接网络有关的信息。如果客户端位于不包含服务器的网段，则通常 UDP 广播不会由 威胁防御 设备进行转发，因为它不转发广播流量。

您可以通过配置接收广播来将DHCP请求转发到另一个接口上DHCP服务器的 威胁防御设备接口来对此情况做出补救。

注释 在透明防火墙模式中不支持 DHCP 中继。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择 **DHCP** > **DHCP 中继**。

步骤 3 在**超时**字段中，输入 威胁防御设备等待 DHCP 中继代理超时的时间（以秒为单位）。值的范围为 1 到 3600 秒。默认值为 60 秒。

超时用于通过本地 DHCP 中继代理进行的地址协商。

步骤 4 在 **DHCP 中继代理 (DHCP Relay Agent)** 上，点击**添加 (Add)**，并配置以下选项：

- **接口** - 连接到 DHCP 客户端的接口。
- **启用 IPv4 中继** - 为该接口启用 IPv4 DHCP 中继。
- **设置路由** -（对于 IPv4）将来自服务器的 DHCP 消息中默认网关地址更改为最接近 DHCP 客户端的 威胁防御设备接口的地址，该客户端中继原始 DHCP 请求。通过此操作，客户端可以将其默认路由设置为指向 威胁防御设备，即使 DHCP 服务器指定了另一个路由器也如此。如果数据包内无默认路由器选项，则 威胁防御设备将添加一个包含接口地址的选项。
- **启用 IPv6 中继** - 为该接口启用 IPv6 DHCP 中继。

步骤 5 点击**确定**，保存 DHCP 中继代理更改。

步骤 6 在 **DHCP 服务器 (DHCP Servers)** 上，点击**添加 (Add)**，并配置以下选项：

将 IPv4 和 IPv6 服务器地址添加为单独的条目，即使它们属于同一台服务器亦是如此。

- **服务器** - DHCP 服务器的 IP 地址。从该下拉列表中选择一个 IP 地址。要添加新的 IP 地址，请参阅 创建网络对象，第 999 页
- **接口** - 指定的 DHCP 服务器连接到的接口。DHCP 中继代理和 DHCP 服务器不能配置在同一接口上。

步骤 7 点击**确定**，保存 DHCP 服务器更改。

步骤 8 在“DHCP”页面上点击**保存**，以保存更改。

配置动态 DNS

当接口使用 DHCP IP 寻址时，分配的 IP 地址可以在续约 DHCP 租用时更改。当需要使用完全限定域名 (FQDN) 访问接口时，更改 IP 地址可能导致 DNS 服务器资源记录 (RR) 失效。动态 DNS (DDNS) 提供一种机制，会在 IP 地址或主机名更改时更新 DNS RR。您还可以将 DDNS 用于静态或 PPPoE IP 寻址。

DDNS 在 DNS 服务器上更新以下 RR：A RR 包括名称到 IP 地址的映射，而 PTR RR 将地址映射到名称。

FTD 支持以下 DDNS 更新方法：

- 标准 DDNS，即标准 DDNS 更新方法由 RFC 2136 定义。

  通过此方法，FTD 和 DHCP 服务器使用 DNS 请求更新 DNS RR。FTD 或 DHCP 服务器向其本地 DNS 服务器发送 DNS 请求以获取有关主机名的信息，并根据响应确定拥有 RR 的主 DNS 服务器。然后，FTD 或 DHCP 服务器直接向主 DNS 服务器发送更新请求。请参阅以下典型场景。

  - FTD 更新 A RR，而 DHCP 服务器更新 PTR RR。

    通常情况下，FTD “拥有” A RR，而 DHCP 服务器“拥有” PTR RR，因此两个实体需要单独请求更新。当 IP 地址或主机名更改时，FTD 将向 DHCP 服务器发送 DHCP 请求（包括 FQDN 选项），以通知它需要请求 PTR RR 更新。

  - DHCP 服务器既更新 A，也更新 PTR RR。

    如果 FTD 无权更新 A RR，请使用此场景。当 IP 地址或主机名更改时，FTD 将向 DHCP 服务器发送 DHCP 请求（包括 FQDN 选项），以通知它需要请求 A 和 PTR RR 更新。

  您可以根据安全需求和主 DNS 服务器的要求配置不同的所有权。例如，对于静态地址，FTD 应拥有两个记录的更新。

- Web - Web 更新方法使用使用 DynDNS 远程 API 规范 (https://help.dyn.com/remote-access-api/) 的任何 DDNS 服务器。

  使用此方法，当 IP 地址或主机名更改时，FTD 会直接向您拥有帐户的 DNS 提供商发送 HTTP 请求。

DDNS 页面还支持设置与 DDNS 相关的 DHCP 服务器设置。

注释 BVI 或网桥组成员接口上不支持使用 DDNS。

开始之前

- 在 **对象** > **对象管理** > **DNS 服务器组**上配置 DNS 服务器组，然后为 **设备** > **平台设置** > **DNS**上的接口启用该组。请参阅配置 DNS，第 617 页。
- 配置设备主机名。您可以在执行 FTD 初始设置时配置主机名，也可以使用 **configure network hostname** 命令配置主机名。如果未指定每个接口的主机名，则使用设备主机名。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择 **DHCP** > **DDNS**.

步骤 3 标准 DDNS 方法： 配置 DDNS 更新方法以启用来自 FTD 的 DNS 请求。

如果 DHCP 服务器将执行所有请求，则无需配置 DDNS 更新方法。

a) 在 **DDNS 更新方法**上，点击 **添加**。
b) 设置 **方法名称**。
c) 点击 **DDNS**。
d) （可选） 配置 DNS 请求之间的**更新间隔**。默认情况下，当所有值都设置为 0 时，每当 IP 地址或主机名更改时，都会发送更新请求。要定期发送请求，请设置**天数**(0-364)、**小时**、**分钟**和**秒**。
e) 设置您希望 FTD 更新的 **更新记录** 。

此设置仅影响您要直接从 FTD 更新的记录；要确定您希望 DHCP 服务器更新的记录，请按接口或全局配置 DHCP 客户端设置。请参见第 步骤 5 ， 第 592 页 步。

- **未定义**-未从 FTD 禁用 DNS 更新。
- **A 和 PTR 两者记录**-将 FTD 设置为同时更新 A 和 PTR RR。使用此选项进行静态或 PPPoE IP 寻址。
- **A 记录**- 将 FTD 设置为仅更新 A RR。如果您希望 DHCP 服务器更新 PTR RR，请使用此选项。

f) 点击“**确定**”。
g) 将此方法分配到第 步骤 5 ， 第 592 页 步中的接口。

步骤 4 Web 方法：配置 DDNS 更新方法，启用来自 FTD 的 HTTP 更新请求。

a) 在 **DDNS 更新方法**上，点击 **添加**。
b) 设置 **方法名称**。
c) 点击 **Web**。
d) 设置 **Web 更新类型** 以更新 IPv4 和/或 IPv6 地址类型。
e) 设置 **Web URL**。指定更新 URL。请咨询您的 DNS 提供商，获取所需的 URL。

使用以下语法：

https://*username***:***password***@***provider-domain***/***path***?hostname=<h>&myip=<a>**

示例：

https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>

f) （可选） 配置 DNS 请求之间的**更新间隔**。默认情况下，当所有值都设置为 0 时，每当 IP 地址或主机名更改时，都会发送更新请求。要定期发送请求，请设置**天数**(0-364)、**小时**、**分钟**和**秒**。
g) 点击“**确定**”。
h) 将此方法分配到第 步骤 5 ， 第 592 页 步中的接口。
i) DDNS 的 Web 类型方法还要求您识别 DDNS 服务器根证书，以验证 HTTPS 连接的 DDNS 服务器证书。请参见第 步骤 9 ， 第 594 页 步。

步骤 5 配置 DDNS 的接口设置，包括为此接口设置更新方法、DHCP 客户端设置和主机名。

a) 在 **DDNS 接口设置**上，点击 **添加**。
b) 从下拉列表中选择**接口**。
c) 选择在 **DDNS 更新方法** 页面中创建的 **方法名称** 。

（标准 DDNS 方法）如果您希望 DHCP 服务器执行所有更新，则无需分配方法。

d) 设置此接口的 **主机名** 。

如果未设置主机名，则会使用设备主机名。如果未指定 FQDN，则会附加 DNS 服务器组中的默认域（用于静态或 PPPoE IP 寻址），或附加来自 DHCP 服务器的域名（用于 DHCP IP 寻址）。

e) 标准 DDNS 方法： 配置 **DHCP 客户端请求 DHCP 服务器以更新请求** ，以确定希望 DHCP 服务器更新哪些记录。

FTD 将 DHCP 客户端请求发送到 DHCP 服务器。请注意，还必须将 DHCP 服务器配置为支持 DDNS。可以将该服务器配置为满足客户端请求，也可以覆盖客户端（在这种情况下，它将回复客户端，因此客户端也不会尝试执行服务器正在执行的更新）。

静态或 PPPoE IP 寻址，请忽略这些设置。

注释 还可以在 **DDNS** 页面上为所有接口全局设置这些值。每个接口的设置优先于全局设置。

- **未选择**-禁用对 DHCP 服务器的 DDNS 请求。即使客户端不请求 DDNS 更新，也可以将 DHCP 服务器配置为始终发送更新。
- **无更新**-请求 DHCP 服务器不执行更新。此设置与**同时启用了 A 和 PTR 记录**的 DDNS 更新方法配合一起使用。
- **仅 PTR**-请求 DHCP 服务器执行 PTR RR 更新。此设置与启用 **A 记录**的 DDNS 更新方法配合使用。
- **A 和 PTR 两者记录**-请求 DHCP 服务器同时执行 A 和 PTR RR 更新。此设置不需要将 DDNS 更新方法与接口关联。

f) 点击**确定**。

注释 当您在 FTD 上启用 DHCP 服务器时， **动态 DNS 更新** 设置与 DHCP 服务器设置相关。有关详细信息，请参阅步骤 步骤 6 ， 第 593 页 。

步骤 6 如果在 FTD 上启用 DHCP 服务器，则可以为 DDNS 配置 DHCP 服务器设置。

要启用 DHCP 服务器，请参阅 配置 DHCPv4 服务器 ， 第 588 页）。您可以配置 DHCP 客户端使用标准 DDNS 更新方法时的服务器行为。如果服务器执行任何更新，则如果客户端租约到期（且未续约），则服务器将请求 DNS 服务器删除其负责的 RR。

a) 您可以全局或按接口配置服务器设置。有关全局设置，请参阅 **DDNS** 主页。有关每个接口的设置，请参阅 **DDNS接口设置** 页面。接口的设置优先于全局设置。

b) 配置您希望 DHCP 服务器在 **动态 DNS 更新**下更新的 DNS RR。

- **未选定**-未禁用 DDNS 更新，即使客户端请求也是如此。
- **仅 PTR**-启用 DDNS 更新。如果启用 **覆盖 DHCP 客户端请求** 设置，则服务器将仅更新 PTR RR。否则，服务器将更新客户端请求的 RR。如果客户端未使用 FQDN 选项发送更新请求，则服务器将使用 DHCP 选项 12 中发现的主机名请求 A 和 PTR RR 的更新。
- **A 和 PTR 两者记录**-启用 DDNS 更新。如果启用 **覆盖 DHCP 客户端请求** 设置，则服务器将同时更新 A 和 PTR RR。否则，服务器将更新客户端请求的 RR。如果客户端未使用 FQDN

选项发送更新请求，则服务器将使用 DHCP 选项 12 中发现的主机名请求 A 和 PTR RR 的更新。

c) 要覆盖 DHCP 客户端请求的更新操作，请选中 **覆盖 DHCP 客户端请求**。

服务器会回复客户端，表示请求被覆盖了，所以客户端不会同时尝试执行服务器正在执行的更新。

步骤 7 （可选）配置常规 DHCP 客户端设置。这些设置与 DDNS 不相关，但与 DHCP 客户端的行为相关。

a) 在 **DDNS** 页面上，选中 **启用 DHCP 客户端广播** 以请求 DHCP 服务器广播 DHCP 应答（DHCP 选项 1）。

b) 要强制将 MAC 地址存储在选项 61 的 DHCP 请求数据包中而不是默认内部生成的字符串中，请在 **DDNS** > **DHCP 客户端 ID 接口**，从 **可用接口** 列表中选择接口，然后点击 **添加** 将其移动到 **选定的接口** 列表。

某些 ISP 期望选项 61 成为接口 MAC 地址。如果 MAC 地址未包含在 DHCP 请求数据包中，则不会分配 IP 地址。此设置与 DDNS 不直接相关，而是常规 DHCP 客户端设置。

步骤 8 点击设备页面上的 **保存** 以保存更改。

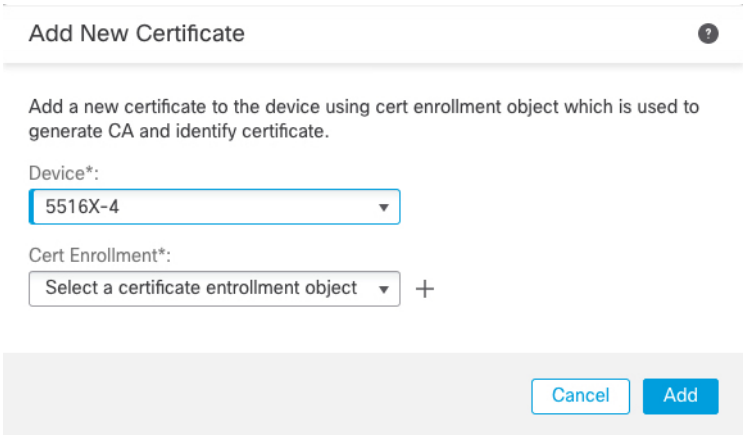
步骤 9 DDNS 的 Web 方法还要求您识别 DDNS 服务器根证书，以验证 HTTPS 连接的 DDNS 服务器证书。

以下示例显示如何将 DDNS 服务器的证书添加为信任点。

a) 获取 DDNS 服务器 CA 证书。此程序显示使用 PEM 格式的手动导入，但您也可以使用 PKCS12。

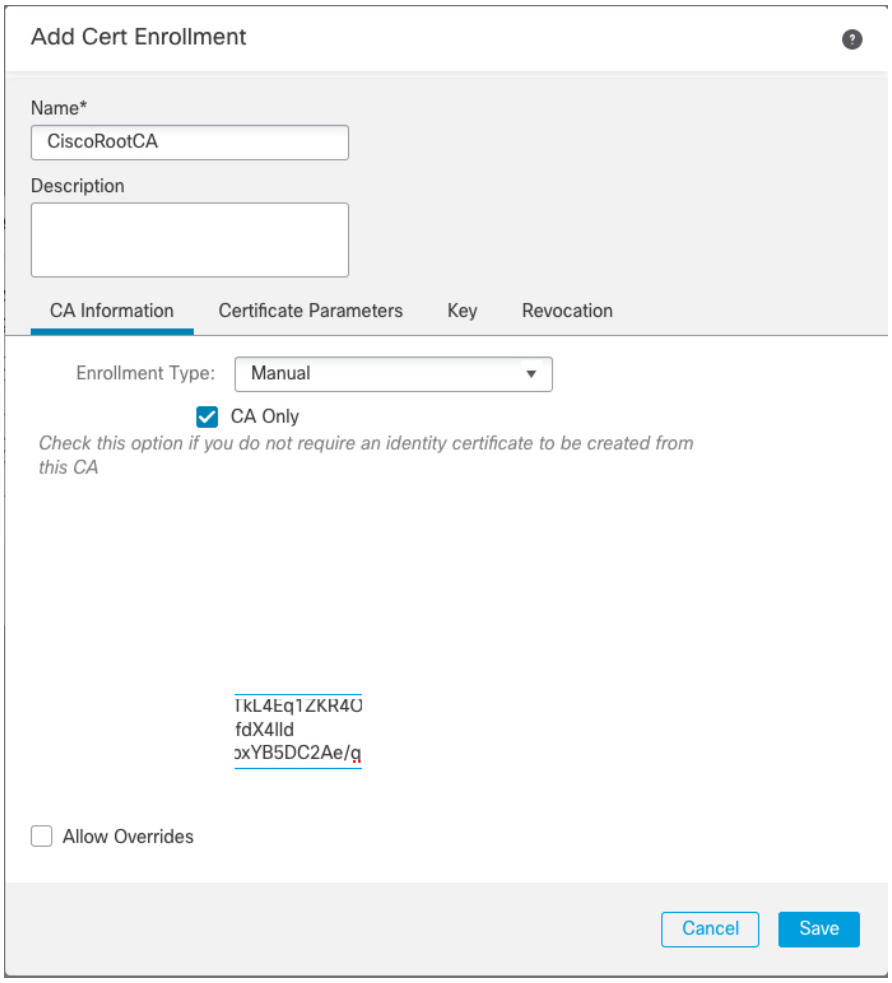
b) 在FMC中，选择 **设备** > **证书** 并点击 **添加**。

c) 选择 **设备**，点击 **添加**（+）。



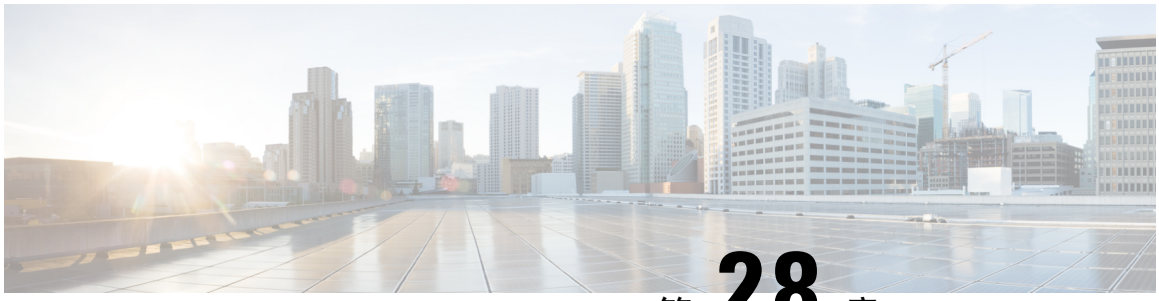
系统将显示 **添加 Cert 注册** 对话框。

d) 输入以下字段值，然后点击 **保存**。



- 输入 **Name**。
- 选择 **注册类型** > **手动**。
- 点击 **仅 CA**。
- 从步骤 9.a， 第 594 页粘贴 CA 文本。

e) 点击**保存 (Save)**。



第 28 章

Firepower 1000/2100 的 SNMP

本章介绍如何为 Firepower 1000/2100 配置 SNMP。

关于 Firepower 1000/2100 系列的 SNMP

简单网络管理协议 (SNMP) 是一个应用层协议，用于为 SNMP 管理器和代理之间的通信提供消息格式。SNMP 提供用于监控和管理网络中的设备的标准化框架和通用语言。

SNMP 框架由三个部分组成：

- SNMP 管理器 - 用于通过 SNMP 来控制和监控网络设备的活动的系统。
- SNMP 代理 - Firepower 1000/2100 机箱内的软件组件，用于维护 Firepower 机箱的数据并根据需要向 SNMP 管理器报告数据。Firepower 机箱包含代理和 MIB 集合。要启用 SNMP 代理并创建管理器和代理之间的关系，请在 Firepower 管理中心中启用并配置 SNMP。
- 管理信息库 (MIB) - SNMP 代理上的受管对象集合。

Firepower 1000/2100 机箱支持 SNMPv1、SNMPv2c 和 SNMPv3。SNMPv1 和 SNMPv2c 都使用基于社区形式的安全性。

为 Firepower 1000/2100 启用 SNMP 并配置 SNMP 属性

注释 此程序仅适用于 Firepower 2100 和 Firepower 1000 系列设备。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 点击 **SNMP**。

步骤 3 填写以下字段：

名称	说明
管理状态 (Admin State) 复选框	SNMP 已启用还是已禁用。仅当系统包含与 SNMP 服务器的集成时才启用此服务。
端口字段	Firepower 机箱与 SNMP 主机通信时使用的端口。无法更改默认端口。
社区字段	Firepower 机箱在它发送给 SNMP 主机的任何陷阱消息中包含的默认 SNMP v1 或 v2 社区名或 SNMP v3 用户名。 输入介于 1 和 32 个字符之间的字母数字字符串。请勿使用 @（at 号）、\（反斜线）、"（双引号）、?（问号）或空格。默认值为 **public**。 请注意，如果**社区**字段已设置，空字段右侧会显示文本**已设置：是**。如果**社区**字段尚未填充值，空字段右侧会显示文本**已设置：否**。
系统管理员名称字段	负责 SNMP 实施的联系人。 输入一个字符串，最多 255 个字符，例如邮件地址或姓名和电话号码。
位置字段	SNMP 代理（服务器）运行所在的主机的位置。 输入一个字母数字字符串，最多 510 个字符。

步骤 4 点击**保存 (Save)**。

下一步做什么

创建 SNMP 陷阱和用户。

为 Firepower 1000/2100 创建 SNMP 陷阱

注释 此程序仅适用于 Firepower 2100 和 Firepower 1000 系列设备。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 点击 **SNMP**。

步骤 3 在 **SNMP 陷阱配置**区域中，点击**添加**。

步骤 4 在 **SNMP 陷阱配置**对话框中，填写以下字段：

名称	说明
主机名 (Host Name) 字段	Firepower 机箱应向其发送陷阱的 SNMP 主机的主机名或 IP 地址。
社区字段	向 SNMP 主机发送陷阱时，Firepower 机箱包含的 SNMP v1 或 v2 社区名或 SNMP v3 用户名。这必须与为 SNMP 服务配置的社区或用户名相同。 输入介于 1 和 32 个字符之间的字母数字字符串。请勿使用 @（at 号）、\（反斜线）、"（双引号）、?（问号）或空格。
端口字段	Firepower 机箱与 SNMP 主机通信以布设陷阱时使用的端口。 输入一个介于 1 和 65535 之间的整数。
版本 字段	用于陷阱的 SNMP 版本和型号。这可以是以下其中一项： • **V1** • **V2** • **V3**
类型字段	如果为版本选择 **V2** 或 **V3**，则是要发送的陷阱类型。这可以是以下其中一项： • **陷阱 (Traps)** • **告知 (Informs)**
权限字段	如果为版本选择 **V3**，与陷阱相关联的权限。这可以是以下其中一项： • **身份验证 (Auth)** - 有身份验证，但没有加密 • **无身份验证 (Noauth)** - 没有身份验证和加密 • **权限 (Priv)** - 有身份验证和加密

步骤 5 点击 **OK** 以关闭 **SNMP Trap Configuration** 对话框。

步骤 6 点击**保存 (Save)**。

为 Firepower 1000/2100 创建 SNMP 用户

注释 此程序仅适用于 Firepower 2100 和 Firepower 1000 系列设备。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 点击 **SNMP**。

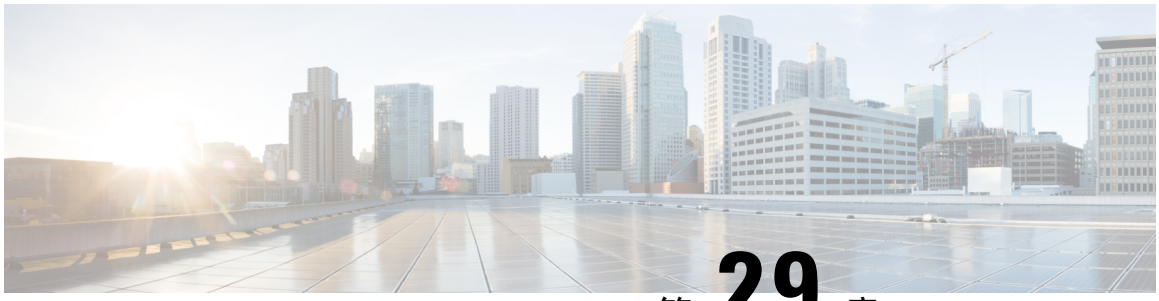
步骤 3 在 **SNMP 用户配置**区域中，点击**添加**。

步骤 4 在 **SNMP 用户配置**对话框中，填写以下字段：

名称	说明
用户名字段	分配给 SNMP 用户的用户名。 最多输入 32 个字母或数字。名称必须以字母开始，也可以指定 _（下划线）、.（句点）、@（邮箱符号）和 -（连字符）。
授权语法类型字段	授权类型：**SHA**。
使用 AES-128 复选框	如果选中此复选框，则此用户使用 AES-128 加密。 注释 SNMPv3 不支持 DES。如果未选中 AES-128 框，则不会进行隐私加密，任何配置的隐私密码都不会生效。
身份验证密码字段	用户的密码。
确认字段	用于确认目的的再次输入的密码。
加密密码字段	用户的隐私密码。
确认字段	用于确认目的的再次输入的隐私密码。

步骤 5 点击**确定**以关闭 **SNMP 用户配置**对话框。

步骤 6 点击**保存 (Save)**。



第 29 章

服务质量

以下主题介绍如何将服务质量 (QoS) 功能用于采用 威胁防御设备的策略网络流量：

QoS 简介

访问控制允许或信任的服务质量（也称 QoS）、速率限制（策略）网络通信。系统不对快速路径的流量进行速率限制。

虽然 QoS 仅在 威胁防御 设备的路由接口上支持，但在站点间 VPN 和 VTI 接口上并不支持。

日志记录速率限制连接

没有用于 QoS 的日志记录配置。可以在不记录的情况下对连接限制速率，但不能仅因为连接被限制速率而不记录连接。要查看连接事件中的 QoS 信息，必须单独将相应连接的两端记录到 管理中心数据库。

速率限制连接的连接事件包含流量被丢弃的数量信息，以及有关限制流量的 QoS 配置的信息。您可以在事件视图（工作流）、仪表板和报表中查看此信息。

关于 QoS 策略

部署到受管设备上的 QoS 策略用于监管速率闲置。每项 QoS 策略可以多台设备为目标；每天设备每次只能部署一项 QoS 策略。

在一项 QoS 策略中，最多有 32 条 QoS 规则用于处理网络流量。系统按照您指定的顺序将流量与 QoS 规则相匹配。系统根据第一条规则（其中所有规则的条件都与流量匹配）对流量进行速率限制。与任何规则都不匹配的流量不受速率限制。

必须按源接口或目标（路由）接口来限制 QoS 规则。系统将对其中每个接口单独强制实施速率限制；不能为一组接口指定一个汇聚速率限制。

QoS规则还可以按其他网络特性以及情景信息（如应用、URL、用户身份和自定义安全组标记(SGT)）对流量实施速率限制。

您可以单独对下载流量和上传流量进行速率限制。系统根据连接发起方确定下载和上传方向。

注释 QoS 不从属于主访问控制配置；您将单独配置 QoS。不过，部署到同一设备上的访问控制和 QoS 策略将共享身份配置；请参阅将其他策略与访问控制相关联，第 1276 页。

QoS 策略和多租户

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

位于祖先域中的管理员可向位于不同后代域中的设备部署同一 QoS 策略。位于这些后代域中的管理员，既可使用这一祖先部署的 QoS 只读策略，也可使用本地策略替换此策略。

QoS 的要求和必备条件

型号支持

威胁防御

支持的域

任意

用户角色

管理员

访问管理员

网络管理员

使用 QoS 策略的速率限制

要执行基于策略的速率限制，请配置 QoS 策略并将它们部署到受管设备。每项 QoS 策略可以多台设备为目标；每天设备每次只能部署一项 QoS 策略。

一个用户一次只能使用一个浏览器窗口编辑一个策略。如果多个用户保存同一个策略，系统会保留最后的更改。为方便起见，系统会显示有关当前正在编辑每条策略的人员（如有任何人）的信息。为保护会话隐私，当策略编辑器 30 分钟无任何活动后，系统将显示警告。60 分钟后，系统将放弃更改。

过程

步骤 1 选择**设备** > **QoS**。

步骤 2 点击**新建策略**创建新的 QoS 策略，并且可以选择分配目标设备；请参阅创建 QoS 策略，第 603 页。

还可以 **复制**（  ） 或 **编辑**（） 现有策略。

步骤 3 配置 QoS 规则；请参阅配置 QoS 规则，第 604 页和QoS 规则条件，第 606 页。

QoS 策略编辑器中的规则将按评估顺序列出每条规则，并显示规则条件和速率限制配置的摘要。右键点击菜单提供规则管理选项，包括移动、启用和禁用。

为有助于较大规模的部署，可以**按设备过滤**，以仅显示影响特定设备或设备组的规则。可以搜索规则，也可以在规则内部进行搜索；系统会将您在**搜索规则**字段中输入的文本匹配与规则名称和条件值相匹配，包括对象和对象组。

注释 正确创建规则并将其排序是一项复杂的任务，但却是构建有效部署的一项重要任务。如果不认真规划，这些规则会抢占其他规则、需要额外的许可证或包含无效配置。图标代表注释、警告和错误。如果存在问题，请点击**显示警告**显示列表。有关详细信息，请参阅访问控制规则的最佳实践，第 1253 页。

步骤 4 点击**策略分配**识别策略针对的受管设备；请参阅为 QoS 策略设置目标设备，第 604 页。

如果在创建策略过程中识别出了目标设备，请验证您的选择。

步骤 5 保存 QoS 策略。

步骤 6 由于此功能必须允许某些数据包通过，因此必须将系统配置为检查这些数据包。请参阅处理在流量识别之前通过的数据包的最佳实践，第 2042 页和指定策略以处理在流量识别之前通过的数据包，第 2042 页。

步骤 7 部署配置更改。

创建 QoS 策略

没有规则的新 QoS 策略不会执行速率限制。

过程

步骤 1 选择**设备** > **QoS**。

步骤 2 点击**新建策略**。

步骤 3 输入**名称 (Name)** 和**说明 (Description)**（后者为可选项）。

步骤 4 （可选）选择要部署策略的**可用设备**，然后点击**添加到策略**或拖放**所选设备**。要减少显示的设备，请在 **Search** 字段中键入搜索字符串。

在部署策略之前必须分配设备。

步骤 5 点击**保存 (Save)**。

下一步做什么

- 配置和部署 QoS 策略；请参阅使用 QoS 策略的速率限制，第 602 页。

为 QoS 策略设置目标设备

每个 QoS 策略都可以将多个设备作为目标；每个设备一次可以有一个已部署的 QoS 策略。

过程

步骤 1 在 QoS 策略编辑器中，点击**策略分配**。

步骤 2 制定目标联系人列表：

- 添加 - 选择一个或多个**可用设备**，然后点击**添加到策略**或拖放到**所选设备**列表。
- 删除 - 点击单个设备旁边 **删除**（ ），或选择多个设备，点击鼠标右键，然后选择 **删除所选项**。
- 搜索 - 在搜索字段中输入搜索字符串。点击 **清除**（ ） 以清除搜索。

步骤 3 点击**确定**以保存策略分配。

步骤 4 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改。

配置 QoS 规则

创建或编辑规则时，请使用规则编辑器的上半部分配置常规规则属性。使用规则编辑器的下半部分来配置规则条件和注释。

过程

步骤 1 在 QoS 策略编辑器的“规则”上：

- 添加规则 - 点击**添加规则 (Add Rule)**。
- 编辑规则-点击 **编辑**（ ）。

步骤 2 输入 **Name**。

步骤 3 配置规则组成部分。

- **已启用** -指定规则是否为已启用。
- QoS 应用位置 - 选择要进行速率限制的接口：**目标接口对象中的接口 (Interfaces in Destination Interface Objects)** 或**源接口对象中的接口 (Interfaces in Source Interface Objects)**。您的选择必须与填入的接口限制相对应（不为**任意 [any]**）。
- 每个接口的流量限制 - 以兆位/秒为单位输入**下载限制**和**上传限制**。默认值**无限制**可防止在该方向上对匹配流量进行速率限制。
- 条件 - 点击要添加的相应的条件。必须配置源或目标接口条件，与您选择的 **QoS 应用位置**相对应。
- 注释-点击 **注释**。要添加注释，请点击**新建注释 (New Comment)**，输入注释，然后点击**确定 (OK)**。您可以在保存规则之前编辑或删除此注释。

如需有关规则组成部分的详细信息，请参阅QoS 规则组成部分，第 605 页。

步骤 4 保存规则。

步骤 5 在策略编辑器中，设置规则位置。点击并拖动，或使用右键点击菜单剪切并粘贴。

规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。流量匹配的第一条规则是处理该流量的规则。适当的规则顺序可减少处理网络流量所需的资源，并防止规则抢占。

步骤 6 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改。

相关主题

访问控制规则的最佳实践，第 1253 页

QoS 规则组成部分

状态（启用/禁用）

默认情况下，规则处于启用状态。如果禁用某规则，系统将不使用该规则并停止为该规则生成警告和错误。

接口（QoS 应用位置）

您不能保存对所有流量都进行速率限制的 QoS 规则。对于每个 QoS 规则，必须将 QoS 应用于以下两个选项之一：

- 源接口对象中的接口 - 对通过规则源接口的流量进行速率限制。如果选择此选项，必须至少添加一个源接口限制（不能为**任何 [any]**）。
- 目标接口对象中的接口 - 对通过规则目标接口的流量进行速率限制。如果选择此选项，必须至少添加一个目标接口限制（不能为**任何 [any]**）。

每个接口的流量限制

QoS 规则对您使用“QoS 应用位置”(Apply QoS On) 选项指定的每个接口单独实施速率限制。不能为一组接口指定汇聚速率限制。

您可以按兆位/秒对流量进行速率限制。默认值**无限制 (Unlimited)** 可防止对匹配流量进行速率限制。

您可以单独对下载流量和上传流量进行速率限制。系统根据连接发起方确定下载和上传方向。

如果指定限制大于接口的最大吞吐量高，系统不会对匹配的流量进行速率限制。最大吞吐量可能受接口的硬件配置影响，可在每台设备的属性中指定硬件配置（**设备** > **设备管理**）。

条件

条件指定规则处理的特定流量。您可以为每个规则配置多个条件。流量必须匹配所有条件才能与规则匹配。每种条件类型在规则编辑器中都有自己的选项卡。有关详细信息，请参阅QoS 规则条件，第 606 页。

备注

每次保存对规则所做的更改时，都可以添加备注。例如，您可为其他用户汇总整体配置，或者当您变更规则和更改的原因时进行记录。

在策略编辑器中，系统会显示规则具有的注释数量。在规则编辑器中，请使用“注释”(Comments) 选项卡查看现有注释和新注释。

QoS 规则条件

条件指定规则处理的特定流量。您可以为每个规则配置多个条件。流量必须匹配所有条件才能与规则匹配。每种条件类型在规则编辑器中都有自己的选项卡。您可以使用以下方式对流量进行速率限制：

有关详细信息，请参阅以下各节之一：

相关主题

接口规则条件，第 606 页
网络规则条件，第 607 页
用户规则条件，第 607 页
应用规则条件，第 607 页
端口规则条件，第 609 页
URL 规则条件，第 610 页
自定义 SGT 规则条件，第 610 页

接口规则条件

接口规则条件按流量的源接口和目标接口控制流量。

根据规则类型和部署中的设备，您可以使用名为 安全区域 或 接口组 的预定义 接口对象 构建接口条件。接口对象对网络进行分段，以通过跨多个设备将接口分组来帮助管理和分类流量；请参阅接口，第 995 页。

提示 按接口限制规则是提高系统性能的一种最佳方式。如果规则排除了某个设备的所有接口，则该规则不影响该设备的性能。

正如接口对象中的所有接口都必须为同一类型（均为内联、被动、交换、路由或ASA FirePOWER），接口条件中使用的所有接口对象也必须为同一类型。由于被动部署的设备不会传输流量，因此无法在被动部署中按目标接口限制规则。

网络规则条件

网络规则条件使用内部报头按流量的源和目标IP地址来控制流量。使用外部报头的隧道规则具有隧道终端条件而不是网络条件。

您可以使用预定义对象构建网络条件，或手动指定单个 IP 地址或地址块。

注释 您 不能 在身份规则中使用 FDQN 网络对象。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字IP地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

用户规则条件

用户规则条件会根据发起连接的用户或用户所属的组来匹配流量。例如，您可以配置阻止规则以禁止财务组中的任何人访问网络资源。

（仅适用于访问控制规则）您必须首先将身份策略与访问控制策略相关联，如将其他策略与访问控制相关联，第 1276 页中所述。

除了为已配置的领域配置用户和组之外，您还可以为以下特殊身份的用户设置策略：

- 身份验证失败：强制网络门户身份验证失败的用户。
- 访客：在强制网络门户中被配置为访客用户的用户。
- 无需身份验证：匹配**无需身份验证 (No Authentication Required)** 规则操作的用户。
- 未知：无法识别的用户；例如，配置的领域未下载的用户。

应用规则条件

系统分析IP流量时，可以识别网络上的常用应用并将其分类。这种基于发现的应用感知是应用控制的基础 - 能够控制应用流量。

借助系统提供的应用过滤器，您可以根据应用的基本特征（类型、风险、业务关联性、类别和标记）组织应用，从而执行应用控制。您可以系统提供的过滤器的组合或以应用的自定义组合为基础，创建可重复使用的用户定义过滤器。

对于策略中的每个应用程序规则条件，必须启用至少一个检测器。如果没有为应用启用检测器，则系统会为该应用自动启用所有系统提供的检测器；如果不存在检测器，则系统为该应用启用最新修改的用户定义的检测器。有关应用检测器的详细信息，请参阅应用检测器基础知识，第 1946 页。

您可以使用应用过滤器和单独指定的应用来确保完整覆盖。但是，在订购访问控制规则之前，请了解以下说明。

应用过滤器的优势

应用过滤器可帮助您快速配置应用控制。例如，您可以轻松地使用系统提供的过滤器创建一条访问控制规则，用于识别并阻止所有业务关联性较低的高风险应用。如果用户尝试使用其中一个应用，则系统会阻止会话。

使用应用过滤器可简化策略创建和管理。此方法可保证系统按预期控制应用流量。由于思科经常通过系统和漏洞数据库 (VDB) 更新和添加应用检测器，因此您可确保系统使用最新的检测器监控应用流量。您还可以创建自己的检测器并将特征分配给其检测到的应用，自动将应用添加到现有过滤器。

应用特征

系统使用下表中所述的条件来展示其检测到的每个应用的特征。这些特征用作应用过滤器。

表 *62:* 应用特征

特征	说明 (Description)	示例
类型	应用协议代表主机之间的通信。 客户端代表在主机上运行的软件。 Web 应用代表 HTTP 流量的内容或所请求的 URL。	HTTP 和 SSH 是应用协议。 网络浏览器和邮件客户端是客户端。 MPEG 视频和 Facebook 是网络应用。
风险	应用用于可能违反您的组织安全策略的用途的可能性。	点对点应用的风险通常很高。
业务相关性	应用用于您的组织的业务运营（相对于娱乐目的）的情景中的可能性。	游戏应用的业务相关性通常很低。
类别	说明应用的最基本功能的应用通用分类。每个应用至少属于一个类别。	Facebook 属于社交网络类别。
标签	有关应用的附加信息。应用可以包括任何数量的标记，也可以没有标记。	视频流网络应用通常标记为 `high bandwidth` 和 `displays ads`。

相关主题

配置应用控制的最佳实践，第 1250 页

端口规则条件

通过端口条件，您可以按流量的源端口和目标端口控制该流量。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

基于端口的规则的最佳实践

指定端口是目标应用的传统方式。但是，可以将应用配置为使用唯一端口绕过访问控制块。因此，尽可能使用应用过滤条件而不是端口条件来确定流量目标。

应用过滤也建议用于动态打开单独通道的应用（如 FTD），以实现控制和数据流。使用基于端口的访问控制规则可能会阻止此类应用正确执行，并可能导致阻止所需的连接。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为源端口条件。

端口、协议和 **ICMP** 代码规则条件

端口条件根据源和目标端口匹配流量。根据规则类型，“端口”可以表示以下任何一项：

- TCP 和 UDP - 可以根据端口控制 TCP 和 UDP 流量。系统使用括号内的协议号，以及可选的关联端口或端口范围来表示此配置。例如：TCP(6)/22。
- ICMP - 可以根据 ICMP 和 ICMPv6 (IPv6-ICMP) 流量的互联网层协议及可选类型和代码控制该流量。例如：ICMP(1):3:3。
- 协议-您可以借助于未使用端口的其他协议控制流量。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

基于端口的规则的最佳实践

指定端口是目标应用的传统方式。但是，可以将应用配置为使用唯一端口绕过访问控制块。因此，尽可能使用应用过滤条件而不是端口条件来确定流量目标。请注意，应用过滤在预过滤器规则中不可用。

应用过滤也建议用于动态打开单独通道的应用（如 FTP），以实现控制和数据流。使用基于端口的访问控制规则可能会阻止此类应用正确执行，并可能导致阻止所需的连接。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为目标端口条件。

将非 TCP 流量与端口条件相匹配

您可以匹配非基于端口的协议。默认情况下，如果不指定端口条件，则匹配 IP 流量。虽然可以将端口条件配置为与非 TCP 流量相匹配，但有一些限制：

- 访问控制规则 - 对于典型设备，可以通过使用 GRE (47) 协议作为目标端口条件将 GRE 封装的流量与访问控制规则相匹配。对于 GRE 限制的规则，只能添加基于网络的条件：区域、IP 地址、端口和 VLAN 标签。此外，系统使用外部报头将访问控制策略中的**所有**流量与 GRE 限制的规则相匹配。对于 威胁防御设备，请使用预过滤器策略中的隧道规则来控制 GRE 封装的流量。
- SSL 规则 - SSL 规则仅支持 TCP 端口条件。
- IMCP 回应 - 类型设置为 0 的目标 ICMP 端口或类型设置为 129 的目标 ICMPv6 端口仅与主动回应回复相匹配。为应答 ICMP 回应请求而发送的 ICMP 回应回复被忽略。为使某个规则匹配任何 ICMP 回应，请使用 ICMP 类型 8 或 ICMPv6 类型 128。

URL 规则条件

使用 URL 条件控制网络上的用户可以访问的网站。

有关完整信息，请参阅URL 过滤，第 1335 页。

自定义 SGT 规则条件

如果未将 ISE/ISE-PIC 配置为身份源，可以使用**非** ISE 分配的安全组标记 (SGT) 来控制流量。SGT 会指定可信网络内的流量源的权限。

自定义 SGT 规则条件使用手动创建的 SGT 对象来过滤流量，而不是使用从系统与 ISE 服务器的连接中获取的 ISE SGT 进行过滤。这些手动创建的 SGT 对象与要控制的流量的 SGT 属性相对应。使用自定义 SGT 控制流量不属于用户控制。

ISE SGT 与自定义 SGT 规则条件

某些规则允许您根据分配的 SGT 来控制流量。根据规则类型和您的身份源配置，您可以使用 ISE 分配的 SGT 或自定义 SGT 将流量与分配的 SGT 属性进行匹配。

注释　如果您使用 ISE SGT 匹配流量，即使一个数据包没有分配的 SGT 属性，当与该数据包的源 IP 地址关联的 SGT 在 ISE 中已知时，该数据包仍会匹配 ISE SGT 规则。

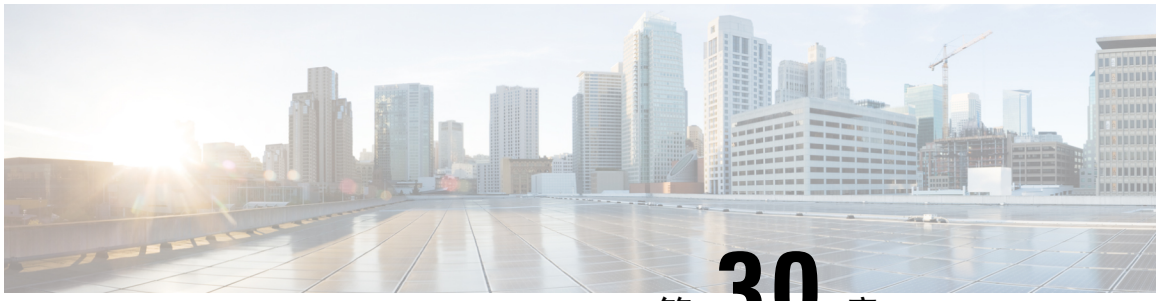
条件类型	要求在目录	规则编辑器中列出的 SGT
ISE SGT	ISE 身份源	通过查询 ISE 服务器获得的 SGT，包含自动更新的元数据
自定义 SGT	无 ISE/ISE-PIC 身份源	您创建的静态 SGT 对象

从自定义 SGT 自动过渡到 ISE SGT

如果您创建与自定义 SGT 匹配的规则，然后将 ISE/ISE-PIC 配置为身份源，则系统：

- 禁用对象管理器中的**安全组标记**选项。尽管系统会保留现有 SGT 对象，但您不能修改它们或添加新的 SGT 对象。
- 保留使用自定义 SGT 条件的现有规则。但是，这些规则与流量不匹配。您也不能为现有规则添加其他自定义 SGT 条件，或创建具有自定义 SGT 条件的新规则。

如果您配置了 ISE，则思科建议您删除或禁用具有自定义 SGT 条件的现有规则。相反，使用 ISE 属性条件将流量与 SGT 属性相匹配。



第 30 章

平台设置

威胁防御 设备的平台设置用于配置您可能希望在多台设备之间共享其值的一系列无关功能。即使您希望每台设备的设置不同，也必须创建共享策略并将其应用到所需设备。

平台设置简介

平台设置策略是用于定义受管设备的可能类似于您的部署中其他受管设备的方面（例如时间设置和外部身份验证）的共享功能集或参数集。

通过共享策略，可以同时配置多个受管设备，从而在部署中提供一致性并精简管理工作。对平台设置策略的任何更改都会影响已应用该策略的所有受管设备。即使您希望每台设备的设置不同，也必须创建共享策略并将其应用到所需设备。

例如，您的组织的安全策略可能会要求您的设备在用户登录时显示“无授权使用”(No Unauthorized Use) 消息。通过平台设置，您可以在平台设置策略中设置一次登录横幅。

在单一管理中心上具有多个平台设置策略也有好处。例如，如果您具有在不同情况下使用的不同邮件中继主机，或者如果要测试不同的访问列表，则可以创建多个平台设置策略并在其之间切换，而非编辑单个策略。

平台设置策略的要求和必备条件

支持的域

任意

用户角色

管理员

访问管理员

网络管理员

管理平台设置策略

使用“平台设置”页面（**设备** > **平台设置**）管理平台设置策略。此页面指示每个策略的设备类型。“状态”(Status) 列显示策略的设备目标。

过程

步骤 1 选择**设备** > **平台设置**。

步骤 2 对于现有策略，您可以**复制**（）、**编辑**（）或**删除**（）策略。

注意 不应删除上一次部署于任何目标设备的策略，即使该策略已过时。在完全删除该策略之前，最好是将其他策略部署到这些目标。

步骤 3 要创建新策略，请点击**新建策略 (New Policy)**。

a) 从下拉列表中选择设备类型。

- **Firepower 设置** 为典型托管设备创建共享策略。
- **威胁防御设置** 以创建 威胁防御 托管设备的共享策略。

b) 为新策略输入**名称 (Name)** 和**说明 (Description)**（可选）。

c) 或者，选择要应用策略的**可用设备 (Available Devices)**，然后点击**添加到策略 (Add to Policy)**（或拖放）以添加所选设备。可以在**搜索 (Search)** 字段中输入搜索字符串以缩小设备列表。

d) 点击**保存**。

系统创建策略，并打开以进行编辑。

步骤 4 要更改策略的目标设备，请点击要编辑的平台设置策略旁边的 **编辑**（ ） 图标。

a) 点击**策略分配 (Policy Assignment)**。
b) 要将设备、高可用性对或设备组分配给策略，请在**可用设备 (Available Devices)** 列表中将其选中，然后点击**添加到策略 (Add toPolicy)**。还可以进行拖放。
c) 要删除设备分配，请点击**所选设备 (Selected Devices)** 列表中的设备、高可用性对或设备组旁边的 **删除**（ ）。
d) 点击**确定 (OK)**。

下一步做什么

- 部署配置更改。

配置 ARP 检测

默认情况下，桥接组成员之间允许所有 ARP 数据包。可以通过启用 ARP 检测来控制 ARP 数据包的流量。

ARP 检测可防止恶意用户模拟其他主机或路由器（称为 ARP 欺骗）。ARP 欺骗能够启用“中间人”攻击。例如，主机向网关路由器发送 ARP 请求；网关路由器使用网关路由器 MAC 地址进行响应。但是，攻击者使用攻击者 MAC 地址（而不是路由器 MAC 地址）将其他 ARP 响应发送到主机。这样，攻击者即可在所有主机流量转发到路由器之前将其拦截。

ARP 检测确保只要静态 ARP 表中的 MAC 地址和相关 IP 地址正确，攻击者就无法利用攻击者 MAC 地址发送 ARP 响应。

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

- 如果 IP 地址、MAC 地址和源接口与 ARP 条目匹配，则数据包可以通过。
- 如果 MAC 地址、IP 地址或接口之间不匹配，则 威胁防御设备 会丢弃数据包。
- 如果 ARP 数据包与静态 ARP 表中的任何条目都不匹配，则可以将 威胁防御设备 设置为从所有接口向外转发数据包（泛洪），或者丢弃数据包。

注释 即使此参数设置为 flood，专用诊断接口也绝不会以泛洪方式传输数据包。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**ARP 检测**。

步骤 3 将条目添加到 ARP 检查表。

a) 点击**添加**以创建新条目，如果该条目已存在，则点击**编辑**。

b) 选择所需的选项。

- **已启用检查** - 对选定接口和区域执行 ARP 检查。
- **已启用洪流** - 是否将不匹配静态 ARP 条目的 ARP 请求以洪流形式自除原始接口或专用管理接口以外的所有接口发出。此为默认行为。

  如果您不选择以洪流形式发出 ARP 请求，则只允许与静态 ARP 条目完全匹配的请求。
- **安全区域** - 添加包含要在其上执行所选操作的接口的区域。区域必须为交换区域。对于不在区域中的接口，您可以在“所选安全区域”列表下方的字段中键入接口名称，然后点击**添加 (Add)**。仅当设备包含所选接口或区域时，才会将这些规则应用于该设备。

c) 点击**确定 (OK)**。

步骤 4 根据添加静态 ARP 条目，第 570 页中所述添加静态 ARP 条目。

步骤 5 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置横幅

您可以将消息配置为在用户连接到设备命令行界面 (CLI) 时显示这些用户。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**横幅**。

步骤 3 配置横幅。

下面是关于横幅的几点提示和要求。

- 只允许使用 ASCII 字符。您可以使用换行符（按 Enter），但不能使用制表符。
- 通过包含变量 **$(hostname)** 或 **$(domain)**，可以动态添加设备的主机名或域名。
- 虽然横幅上没有绝对长度限制，但如果没有足够的系统内存来处理横幅消息，则 Telnet 或 SSH 会话将关闭。
- 从安全角度来看，重要的是横幅阻止未经授权的访问。请勿使用“欢迎”或“请”等措辞，因为它们像是在邀请入侵者。以下横幅为未经授权的访问设置正确的语调：

```
You have logged in to a secure device.
```

```
If you are not authorized to access this device,
log out immediately or risk criminal charges.
```

步骤 4 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 DNS

域名系统 (DNS) 服务器用来将主机名解析到 IP 地址。有两种适用于不同类型流量的 DNS 服务器设置：数据流量和特殊管理流量。数据流量包括使用需要进行 DNS 查找的 FQDN 的任何服务，例如访问控制规则和远程访问 VPN。特殊管理流量包括管理接口上发出的流量，例如配置和数据库更新。此程序仅适用于 数据 DNS 服务器。有关 管理 DNS 设置，请参阅 CLI **configure network dns servers** 和 **configure network dns searchdomains** 命令。.

为了确定 DNS 服务器通信的正确接口，受管设备使用路由查找，但使用哪种路由表取决于您启用 DNS 的接口。有关详细信息，请参阅下面的接口设置。

您可以选择配置多个 DNS 服务器组，并使用它们来解析不同的 DNS 域。例如，您可能有一个使用公共DNS服务器的可捕获默认组，用于与互联网的连接。然后，您可以配置一个单独的组，以将内部 DNS 服务器用于内部流量，例如，与 example.com 域中的计算机的任何连接。因此，使用您的组织的域名与FQDN的连接将使用内部DNS服务器进行解析，而与公共服务器的连接则使用外部DNS服务器。这些解析由使用数据 DNS 解析的任何功能使用，例如 NAT 和访问控制规则。

您可以使用受信任 DNS 服务器选项卡为 DNS 监听配置受信任 DNS 服务。DNS 监听用于将应用域映射到IP，以便检测第一个数据包上的应用。除了配置受信任的DNS服务器之外，您还可以将 DNS 组，DHCP 池，DHCP 中继和 DHCP 客户端中已配置的服务器作为受信任的 DNS 服务器。

注释 对于基于应用的 PBR，必须配置受信任的 DNS 服务器。您还必须确保 DNS 流量以明文格式通过 威胁防御 （不支持加密 DNS），以便解析域以检测应用。

开始之前

- 确保已创建一个或多个DNS服务器组。有关详细信息，请参阅创建DNS服务器组对象，第986页。
- 确保您已创建用于连接到 DNS 服务器的接口对象。
- 确保受管设备具有适当的静态路由或动态路由来访问 DNS 服务器。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)** 并创建或编辑威胁防御策略。

步骤 2 点击 **DNS**。

步骤 3 点击 **DNS 设置** 选项卡。

步骤 4 选中 **启用按设备 DNS 域名解析**。

步骤 5 配置 DNS 服务器组。

a) 在 DNS 服务器组列表中执行以下任一操作：

- 要将值添加到列表，请点击 **添加**。如果在现有服务器组列表中配置了 30 个过滤器域，则无法添加其他组。
- 要编辑组的设置，请点击组旁边的 **编辑**（ ）。
- 要删除组，请点击该组旁边的 **删除**（ ）。删除组不会删除 DNS 服务器组对象，只是将其从此列表中删除。

b) 在添加或编辑组时，请配置以下设置，然后点击 **确定**：

- **选择 DNS 组**-选择现有 DNS 服务器组对象，或点击 + 创建新的 DNS 服务器组对象。
- **作为默认**-选择此选项可使此组成为默认组。任何与其他组的过滤器不匹配的DNS解析请求都将使用此组中的服务器进行解析。
- **过滤域**-仅对于非默认组，是逗号分隔的域名列表，例如example.com，example2.com。不能包含空格。

  该组将仅用于这些域的DNS解析。您可以在添加到此DNS平台设置策略的所有组中最多输入 30 个单独的域。每个名称最多可包含 127 个字符。

  请注意，这些过滤器域与该组的默认域名无关。过滤器列表可以与默认域不同。

步骤 6 （可选） 输入 **过期条目计时器** 和 **轮询计时器** 值，以分钟计。

这些选项仅适用于在网络对象中指定的 FQDN。这些不适用于其他功能中使用的 FQDN。

- **到期条目计时器** 指定DNS条目的最短生存时间（TTL），以分钟为单位。如果到期计时器长于条目的TTL，则TTL增加到到期条目时间值。如果TTL比到期计时器长，则将忽略到期条目时间值：在这种情况下，不会向TTL添加额外时间。到期后，该条目将从DNS查找表中删除。删除条目要求重新编译表，使频繁删除能够增加设备上的处理负载。因为某些DNS条目可以有非常短的TTL（短至3秒），所以您能够使用此设置实际上延长TTL。默认值为1分钟（即，所有分辨率的最小TTL为1分钟）。范围为 1 至 65535 分钟。

  请注意，对于运行7.0或更早版本的系统，到期时间实际上会添加到TTL中：它不指定最小值。

- **轮询计时器** 指定设备查询 DNS 服务器以解析网络对象中定义的 FQDN 的时间限制。在轮询 DNS 计时器到期时或解析的 IP 条目的 TTL 到期时（以先到者为准），定期解析 FQDN。

步骤 7 在所有接口或特定接口上启用 DNS 查找。这些选择还会影响所使用的路由表。

请注意，在接口上启用 DNS 查找与指定用于查找的源接口不同。威胁防御 始终使用路由查询来确定源接口。

- 未选择任何接口 - 在所有接口上启用 DNS 查找，包括管理接口和管理专用接口。威胁防御 检查数据路由表，如果未找到路由，则回退到管理专用路由表。
- 选择了特定接口而不是**同时通过诊断/管理接口启用 DNS 查找 (Enable DNS Lookup via diagnostic interface also)** 选项 - 在指定接口上启用 DNS 查找。威胁防御 仅检查数据路由表。
- 选择了特定接口并且选择了**同时通过诊断/管理接口启用 DNS 查找 (Enable DNS Lookup via diagnostic interface also)** 选项 - 在指定接口和 诊断 接口上启用 DNS 查找。威胁防御 检查数据路由表，如果未找到路由，则回退到管理专用路由表。
- 仅限 **通过诊断启用 DNS 查找 接口及** 选项-在 诊断上启用 DNS 查找。威胁防御 仅检查管理专用路由表。 确保在 **设备** > **设备管理** > **编辑设备** > **接口** 页面上为诊断接口配置 IP 地址。

步骤 8 要配置受信任的 DNS 服务器，请点击 **受信任的 DNS 服务器** 选项卡。

步骤 9 默认情况下，在 DHCP 池，DHCP 中继，DHCP 客户端或 DNS 服务器组中配置的现有DNS服务器作为受信任DNS服务器。如果要排除其中任何一个，请取消选中相应的复选框。

步骤 10 要添加受信任的 DNS 服务器，请在 **指定 DNS 服务器**下，点击 **编辑**。

步骤 11 在 **选择 DNS 服务器** 对话框中，选择主机对象作为受信任 DNS 服务器或直接指定受信任 DNS 服务器的 IP 地址：

a) 要选择现有主机对象，请在 **可用主机对象**下，选择所需的主机对象，然后点击 **添加** 以将其包含到 **所选DNS服务器**中。有关添加主机对象的信息，请参阅 创建网络对象， 第 999 页。

b) 要直接提供受信任 DNS 服务器的 IP 地址（IPv4 或 IPv6），请在给定文本字段中输入地址，然后点击 **添加** 以将其包含到 **所选 DNS 服务器**中。

c) 点击**保存 (Save)**。添加的DNS服务器显示在 **受信任的 DNS 服务器** 页面中。

注释 每个策略最多可以配置 12 个 DNS 服务器。

步骤 12 （可选）要使用主机名或 IP 地址搜索已添加的 DNS 服务器，请使用 **指定 DNS 服务器** 下的搜索字段。

步骤 13 点击**保存 (Save)**。

下一步做什么

要将 FQDN 对象用于访问控制规则，请创建一个 FQDN 网络对象，然后将其分配给访问控制规则。有关说明，请参阅创建网络对象， 第 999 页。

为 SSH 配置外部身份验证

注释 您必须具有管理员权限才能执行此任务。

在为管理用户启用外部身份验证时，威胁防御会使用外部身份验证对象中指定的 LDAP 或 RADIUS 服务器验证用户凭证。

共享外部身份验证对象

管理中心 和 威胁防御 设备可使用外部身份验证对象。管理中心 和设备可共享同一个对象，也可以为它们创建不同的对象。请注意， 威胁防御 支持在 RADIUS 服务器上定义用户，而 管理中心 要求您在外部身份验证对象中预定义用户列表。您可以选择针对 威胁防御使用预定义列表方法，但如果要在 RADIUS 服务器上定义用户，则必须为 威胁防御 和 管理中心创建单独的对象。

注释 威胁防御 和 管理中心 的超时范围不同，因此，如果共享对象，请确保不要超过 威胁防御 的较小超时范围（对于 LDAP 为 1-30 秒，对于 RADIUS 为 1-300 秒）。如果将超时设置为更高的值，则 威胁防御 外部身份验证配置将不起作用。

为设备分配外部身份验证对象

对于 管理中心，请直接在 **系统** > **用户** > **外部身份验证**启用外部身份验证对象；此设置仅会影响 管理中心 的使用情况，无需为了受管设备的使用而启用此设置。对于 威胁防御 设备，必须在部署到设备的平台设置中启用外部身份验证对象，并且每个策略只能激活一个外部认证对象。已启用 CAC 身份验证的 LDAP 对象也不能用于 CLI 访问。

威胁防御 支持的字段

只有外部身份验证对象中一个子集的字段可用于 威胁防御 SSH 访问。如果填入其他字段，它们将被忽略。如果您也将此对象用于 管理中心，则将使用这些字段。此程序仅涵盖 威胁防御 支持的字段。有关其他字段，请参阅 《Cisco Secure Firewall Management Center 管理指南》中的 《配置 管理中心 外部身份验证》。

用户名

用户名必须为使用字母数字字符加句点 (.) 或连字符 (-) 的 Linux 有效用户名，且仅可使用小写字母。不支持其他特殊字符，例如 at 符号 (@) 和斜线 (/)。不能为外部身份验证添加**管理员**用户。只能在管理中心添加外部用户（作为外部身份验证对象的一部分）；不能在 CLI 中添加他们。请注意，内部用户只能在 CLI 中添加，不能在管理中心添加。

如果您之前使用 **configure user add** 命令为内部用户配置过相同的用户名，则 威胁防御 首先对照此内部用户检查密码，如果失败，再检查 AAA 服务器。请注意，此后不能再将具有相同名称的内部用户添加为外部用户；仅支持以前存在的内部用户。 对于 RADIUS 服务器上定义的用户，请务必将权限级别设置为与任何内部用户相同的权限级别；否则您无法使用外部用户密码登录。

特权等级

LDAP 用户始终具有“配置”权限。RADIUS 用户可定义为“配置”或“基本”用户。

开始之前

- 管理接口上的 SSH 访问默认处于启用状态。要在数据接口上启用 SSH 访问，请参阅配置安全外壳 ，第 631 页。诊断接口上不支持 SSH。
- 请告知 RADIUS 用户以下操作，使他们合理设定预期：

- 外部用户首次登录时，威胁防御 会创建所需的结构，但不能同时创建用户会话。用户只需再次进行身份验证，即可启动会话。用户将看到与以下消息类似的消息：“已识别新的外部用户名。请重新登录以启动会话。”
- 同样地，如果自上次登录以来，用户的 Service-Type 授权发生了更改，则用户将需要重新进行身份验证。用户将看到与以下消息类似的消息：“您的授权权限已更改。请重新登录以启动会话。”

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 点击**外部身份验证 (External Authentication)**。

步骤 3 点击**管理外部身份验证服务器**链接。

您还可以通过点击 **系统** > **用户** > **外部身份验证**打开外部身份验证屏幕。

步骤 4 配置 LDAP 身份验证对象。

a) 点击**添加外部身份验证对象 (Add External Authentication Object)**。

b) 将**身份验证方法**设置为 **LDAP**

c) 输入**名称**和可选**说明**。

d) 从下拉列表中选择**服务器类型**。

e) 对于**主服务器**，输入**主机名/IP 地址**。

注释 如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与此字段中使用的主机名匹配。此外，加密连接不支持 IPv6 地址。

f) （可选）更改**端口**使用的默认值。

g) （可选）输入**备份服务器**参数。

h) 输入 **LDAP 特定参数**。

- **基础 DN** - 为要访问的 LDAP 目录输入基本可分辨名称。例如，要对 Example 公司的 Security 组织中的名称进行身份验证，请输入 `ou=security,dc=example,dc=com`。或者，点击**获取 DN**，然后从下拉列表中选择相应的基本可分辨名称。
- **基本过滤器** - 例如，如果目录树中的用户对象具有 `physicalDeliveryOfficeName` 属性，并且纽约办公室中的用户对于该属性具有属性值 `NewYork`，要仅检索纽约办公室中的用户，请输入 `(physicalDeliveryOfficeName=NewYork)`。
- **用户名** - 为有足够凭证浏览 LDAP 服务器的用户输入可分辨的名称。例如，如果是连接到 OpenLDAP 服务器，其中用户对象具有 `uid` 属性，并且 Example 公司 Security 部门的管理员对象的 `uid` 值为 `NetworkAdmin`，则您可以输入 `uid=NetworkAdmin,ou=security,dc=example,dc=com`。
- **密码**和**确认密码** - 输入并确认用户的密码。
- （可选）**显示高级选项** - 配置以下高级选项。

- **加密** - 点击**无**、**TLS** 或 **SSL**。

  注释 如果在指定端口后更改加密方法，则会将端口重置为该方法的默认值。对于**无**或 **TLS**，端口将重置为默认值 389。如果选择 SSL 加密，端口将重置为 636。

- **SSL 证书上传路径** - 对于 SSL 或 TLS 加密，必须通过点击**选择文件**选择一个证书。
- （未使用）**用户名模板** - 威胁防御 未使用。
- **超时**-输入滚动到备份连接之前等待的秒数（1-30 秒）。默认值为 30。

  注释 威胁防御 和 管理中心的超时范围不同，因此，如果共享对象，请确保不要超过 威胁防御的较小超时范围（1-30 秒）。如果将超时设置为更高的值，则 威胁防御 外部身份验证配置将不起作用。

i) （可选）如果要使用用户可分辨类型之外的外壳访问属性，请设置 **CLI 访问属性** 。例如，在 Microsoft Active Directory Server 上，通过在 **CLI 访问属性** 字段中键入 `sAMAccountName` 来使用 `sAMAccountName` 外壳访问属性检索外壳访问用户。

j) 设置 **CLI 访问过滤器**。

选择以下方法之一：

- 要使用配置身份验证设置时指定的同一过滤器，请选择**与基本过滤器相同 (Same as Base Filter)**。
- 要根据属性值检索管理用户条目，请输入要用作过滤器的属性名、比较运算符和属性值（用括号括起来）。例如，如果所有网络管理员都具有属性值为 `shell` 的 `manager` 属性，则可以设置基本过滤器 `(manager=shell)`。

LDAP 服务器上的名称必须是 Linux 有效的用户名：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

k) 点击**保存 (Save)**。

步骤 5 对于LDAP，如果以后在LDAP服务器上添加或删除用户，必须刷新用户列表并重新部署平台设置。

a) 依次选择**系统** > **用户** > **外部身份验证**。

b) 点击 LDAP 服务器旁边的 **刷新** （ ） 。

如果用户列表发生变化，您将看到一条消息，建议您为设备部署配置更改。Firepower 威胁防御平台设置还会显示它在“*x* 个目标设备上过时。"

c) 部署配置更改；请参阅部署配置更改 ， 第 136 页。

步骤 6 配置 RADIUS 身份验证对象。

a) 使用 Service-Type 属性在 RADIUS 服务器上定义用户。

以下是受支持的 Service-Type 属性值：

- 管理员 (6) - 提供 CLI 的配置访问授权。这些用户可以在 CLI 中使用所有命令。
- NAS 提示 (7) 或除级别 6 以外的任何级别 - 提供 CLI 的基本访问授权。这些用户可以使用只读命令，例如**show**命令，用于监控和故障排除。

名称必须是 Linux 有效的用户名：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

或者，您可以在外部身份验证对象中预定义用户（参见步骤6.j，第623页）。要在为 威胁防御 使用 Service-Type 属性的同时对 威胁防御 和 管理中心 使用相同的 RADIUS 服务器，请创建可识别相同 RADIUS 服务器的两个外部身份验证对象：其中一个对象包括预定义的 **CLI 访问过滤器** 用户（用于 管理中心），另一个对象则将 **CLI 访问过滤器** 留空（用于 威胁防御）。

b) 在 管理中心 中，点击**添加外部身份验证对象**。
c) 将**身份验证方法**设置为 **RADIUS**。
d) 输入**名称**和可选**说明**。
e) 对于**主服务器**，输入**主机名/IP 地址**。

注释 如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与此字段中使用的主机名匹配。此外，加密连接不支持 IPv6 地址。

f) （可选） 更改**端口**使用的默认值。
g) 输入 **RADIUS 服务器密钥**。
h) （可选） 输入**备份服务器**参数。
i) 输入 **RADIUS 特定参数**。
   - **超时（秒）** - 输入滚动到备份连接之前等待的秒数。默认值为 30。
   - **重试次数** - 输入在滚动到备份连接之前应当尝试主服务器连接的次数。默认值为 3。
j) （可选）不使用 RADIUS 定义的用户，在 **CLI 访问过滤器**下，在 **管理员 CLI 访问用户列表** 字段中输入一个逗号分隔的用户名列表。例如，输入 **`jchrichton`**、**`aerynsun`**、**`rygel`**。

   您可能想要使用 威胁防御 的 **CLI 访问过滤器** 方法以便对 威胁防御 和其他平台类型使用相同的外部身份验证对象。请注意，如果想要使用 RADIUS 定义的用户，则必须将 **CLI 访问过滤器** 留空。

   请确保这些用户名匹配 RADIUS 服务器上的用户名。名称必须是 Linux 有效的用户名：

   - 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
   - 全部小写
   - 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

注释　　如果要在 RADIUS 服务器上仅定义用户，则必须将此部分留空。

k) 点击**保存 (Save)**。

步骤 7 返回 **设备** > > **平台设置** > **外部身份验证**。

步骤 8 点击 **刷新**（ ）可查看新添加的任何对象。

为 LDAP 指定 SSL 或 TLS 加密时，必须上传证书才能进行连接；否则，此窗口中将不会列出该服务器。

步骤 9 点击要使用的外部身份验证对象旁边的 **滑块已启用**（ ）。只能启用一个对象。

步骤 10 点击**保存 (Save)**。

步骤 11 部署配置更改；请参阅部署配置更改，第 136 页。

配置分段处理

默认情况下，威胁防御设备允许每个 IP 数据包最多包含 24 个分段，以及最多 200 个等待重组的分段。如果您有定期对数据包进行分段的应用（如 NFS over UDP），可能需要让分段位于您的网络上。但如果您没有对流量进行分段的应用，则我们建议您通过将**链**设置为 1 来禁止分段。分段数据包通常用作拒绝服务 (DoS) 攻击。

注释　这些设置将为已分配此策略的设备建立默认值。可以通过选择接口配置中的**覆盖默认分段设置**，为设备上的特定接口覆盖这些设置。在编辑接口时，可以找到**高级 (Advanced)** > **安全配置 (Security Configuration)** 上的选项。选择**设备 (Devices)** > **设备管理 (Device Management)**，编辑 威胁防御设备，然后选择**接口 (Interfaces)** 以编辑接口属性。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**碎片设置 (Fragment Settings)**。

步骤 3 配置以下选项。如果希望使用默认设置，请点击**重置为默认值**。

- **大小（块）** - 来自所有连接的可能正在等待重组的总体数据包分段的最大数量。默认值为 200 个分段。
- **链（分段）** - 可将一个完整 IP 数据包分段为数据包的最大数量。默认为 24 个数据包。将此选项设置为 1 将禁止分段。
- **超时（秒）** - 等待整个分段数据包到达所需的最大秒数。默认值为 5 秒。如果在此时间内未收到所有分段，则将放弃所有分段。

步骤 4 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 HTTP

如果希望允许到 威胁防御设备上的一个或多个接口的 HTTPS 连接，则请配置 HTTPS 设置。可以使用 HTTPS 来下载用于故障排除的数据包捕获。

开始之前

- 当您使用 Cisco Secure Firewall Management Center管理 威胁防御时，针对 威胁防御的 HTTP 访问选线仅可用于查看数据包捕获文件。威胁防御没有用于在此管理模式下进行配置的 Web 接口。
- 只能使用 **configure user add** 命令在 CLI 中配置 HTTPS 本地用户。默认情况下，有一个您在初始设置期间为其配置密码的 **admin** 用户。不支持 AAA 外部身份验证。
- 此配置仅适用于数据接口，包括您配置为仅管理的任何接口。它主题不适用于专用管理接口。物理管理接口在“诊断”逻辑接口与“管理”逻辑接口之间共享；此配置仅适用于“诊断”逻辑接口（如果使用）或其他数据接口。管理逻辑接口与设备上的其他接口分离。它用于设置设备并将其注册到 管理中心。它具有独立 IP 地址和静态路由。
- 要使用 HTTPS，无需允许主机 IP 地址的访问规则。只需按照本部分配置 HTTPS。
- 只能将 HTTPS 用于可访问的接口；如果 HTTPS 主机位于外部接口上，则只能向该外部接口直接发起管理连接。
- 不能在同一接口上为同一 TCP 端口同时配置 HTTPS 和 AnyConnect 远程访问 SSL VPN 。例如，如果在外部接口上配置远程访问 SSL VPN，则也无法在端口 443 上打开 HTTPS 连接的外部接口。如果必须在同一接口上同时配置这两项功能，则请使用不同的端口。例如，在端口 4443 上打开 HTTPS。
- 需要网络对象，用于定义将要允许建立到设备的 HTTPS 连接的主机或网络。您可以在此过程中添加对象，但如果要使用对象组标识一组 IP 地址，请确保规则中所需的组已经存在。选择**对象** > **对象管理**以配置对象。

注释 不能使用系统提供的**任意**网络对象组。而应使用**任意 ipv4** 或**任意 ipv6**。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择 **HTTP**。

步骤 3 选中**启用 HTTP 服务器 (Enable HTTP Server)** 复选框以启用 HTTP 服务器。

步骤 4 （可选）更改 HTTP 端口。默认值为 443。

步骤 5 标识允许 HTTP 连接的接口和 IP 地址。

使用此表来限制哪些接口将接受 HTTP 连接，以及允许建立这些连接的客户端的 IP 地址。您可以使用网络地址而不是单个 IP 地址。

a) 点击**添加 (Add)** 以添加新规则，或点击**编辑 (Edit)** 以编辑现有规则。

b) 配置规则属性：

- **IP 地址** - 用于标识允许建立 HTTP 连接的主机或网络的网络对象或组。从下拉列表中选择一个对象，或者点击 + 以添加新的网络对象。
- **安全区域** - 添加包含将允许进行 HTTP 连接的接口的区域。对于不在区域中的接口，可以在**所选安全区域** 列表下方的字段中键入接口名称，然后点击 **添加**。仅当设备包含所选接口或区域时，才会将这些规则应用于该设备。

c) 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 ICMP 访问规则

默认情况下，您可以使用 IPv4 或 IPv6 将 ICMP 数据包发送到任何接口，以下情况例外：

- 威胁防御 不响应定向至广播地址的 ICMP 回显请求。
- 威胁防御 仅响应发送至流量进入的接口的 ICMP 流量；不能通过某个接口将 ICMP 流量发送至远端接口。

为了保护设备免受攻击，您可以使用 ICMP 规则将接口的 ICMP 访问限制为特定主机、网络或 ICMP 类型。ICMP 规则的工作原理与访问规则类似，将对规则进行排序，与数据包匹配的第一条规则将定义操作。

如为某个接口配置任何 ICMP 规则，则将隐式拒绝 ICMP 规则添加至 ICMP 规则列表的末尾，从而更改默认行为。因此，如果想要仅拒绝几种消息类型，则须在 ICMP 规则列表的末尾纳入一条允许任何消息类型的规则，以便允许剩余的消息类型。

我们建议，始终为 ICMP 不可到达消息类型（类型 3）授予权限。拒绝 ICMP 不可达消息会禁用 ICMP 路径 MTU 发现，从而可能阻止 IPsec 和 PPTP 流量。此外，IPv6 中的 ICMP 数据包用于 IPv6 邻居发现进程。

开始之前

确保规则中所需的对象已经存在。选择**对象** > **对象管理**以配置对象。您需要网络对象或组来定义所需的主机或网络，并且需要端口对象来定义要控制的 ICMP 消息类型。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择 **ICMP**。

步骤 3 配置 ICMP 规则。

a) 点击**添加 (Add)** 以添加新规则，或点击**编辑 (Edit)** 以编辑现有规则。

b) 配置规则属性：

- **操作** - 许可（允许）还是拒绝（丢弃）匹配的流量。
- **ICMP 服务** - 标识 ICMP 消息类型的端口对象。
- **网络 (Network)** - 标识您要控制其访问权限的主机或网络的网络对象或组。
- **安全区域 (Security Zones)** - 添加包含您所保护的接口的区域。对于不在区域中的接口，可以在**所选安全区域 (Selected Security Zones)** 列表下方的字段中键入接口名称，然后点击 **添加 (Add)**。仅当设备包含所选接口或区域时，才会将这些规则应用于该设备。

c) 点击**确定 (OK)**。

步骤 4 （可选。）设置对 ICMPv4 无法访问的消息的速率限制。

- **速率限制** - 设置不可达消息的速率限制，该限制介于每秒 1 至 100 条消息之间。默认值为每秒 1 条消息。
- **突发大小** - 设置突发速率，其值介于 1 至 10 之间。系统会发送此数量的回复，但在达到速率限制之前不会发送后续回复。

步骤 5 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 SSL 设置

注释 您必须具有管理员权限并在分叶域中才能执行此任务。

必须确保您运行的是 Cisco Secure Firewall Management Center的完全许可版本。如果是在评估模式下运行 Cisco Secure Firewall Management Center 时，“SSL 设置”将被禁用。此外，当许可的 Cisco Secure Firewall Management Center 版本不符合导出标准时，“SSL 设置”将被禁用。如果您使用的是带有 SSL 的远程接入 VPN，则您的智能帐户必须启用强加密功能。有关详细信息，请参阅《Cisco Secure Firewall Management Center 管理指南》中的 许可证类型和限制 。

过程

步骤 1 选择**设备 > 平台设置**，并创建或编辑 威胁防御策略。

步骤 2 选择 **SSL**。

步骤 3 将条目添加到**添加 SSL 配置**表中。

a) 点击**添加**以创建新条目，如果该条目已存在，则点击**编辑**。

b) 从下拉列表中选择所需的安全配置。

- **协议版本** - 指定在建立远程接入 VPN 会话时要使用的 TLS 协议。
- **安全级别** - 指示希望为 SSL 设置的安全定位类型。

步骤 4 根据您选择的协议版本选择**可用算法**，然后点击**添加**以针对所选协议包括这些算法。有关详细信息，请参阅关于 SSL 设置 ， 第 628 页。

这些算法根据您选择的协议版本列出。每个安全协议标识用于设置安全级别的唯一算法。

步骤 5 点击**确定**以保存更改。

下一步做什么

选择 **部署** > **部署** 然后点击 **部署** 以将策略部署到所分配的设备。

关于 SSL 设置

威胁防御设备使用安全套接字层 (SSL) 协议和传输层安全 (TLS) 对来自远程客户端的远程访问 VPN 连接支持安全消息传输。通过 SSL 设置窗口，您可以配置在通过 SSL 远程 VPN 访问传输邮件过程中协商和使用的 SSL 版本和加密算法。

在以下位置配置 SSL 设置：

设备 > 平台设置 > SSL

字段

充当服务器时的最低 SSL 版本- 指定在充当服务器时， 威胁防御 设备使用的最低 SSL/TLS 协议版本。例如，用作远程访问 VPN 网关时。

TLS 版本—从下拉列表中选择以下 TLS 版本之一：

TLS V1	接受 SSLv2 客户端问候并协商 TLSv1（或更高版本）。
TLSV1.1	接受 SSLv2 客户端问候并协商 TLSv1.1（或更高版本）。
TLSV1.2	接受 SSLv2 客户端问候并协商 TLSv1.2（或更高版本）。

DTLS 版本—根据所选的 TLS 版本，从下拉列表中选择 DTLS 版本。默认情况下，DTLSv1 在 威胁防御 设备上配置，您可以根据需要选择 DTLS 版本。

注释 确保 TLS 协议版本高于或等于所选的 DTLS 协议版本。TLS 协议版本支持以下 DTLS 版本：

TLS V1	DTLSv1
TLSV1.1	DTLSv1
TLSV1.2	DTLSv1、DTLSv1.2

Diffie-Hellman 组—从下拉列表中选择一个组。可用选项为 Group1 - 768 位模数、Group2 - 1024 位模数、Group5 - 1536 位模数、Group14 - 2048 位模数、224 位素数阶和 Group24 - 2048 位模数、256 位素数阶。默认值为 Group1。

椭圆曲线 Diffie-Hellman 组 - 从下拉列表中选择一个组。可用选项为 Group19 - 256 位 EC、Group20 - 384 位 EC 和 Group21 - 521 位 EC。默认值为 Group19。

TLSv1.2 增加了对以下密码的支持：

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256

注释 ECDSA 和 DHE 密码具有最高优先级。

SSL 配置表可用于指定要在 Cisco Secure Firewall Threat Defense设备上支持的协议版本、安全级别和密码算法。

协议版本 - 列出 Cisco Secure Firewall Threat Defense设备支持和用于 SSL 连接的协议版本。可用的协议版本有：

- 默认

- TLSV1
- TLSV1.1
- TLSV1.2
- DTLSv1
- DTLSv1.2

安全级别—列出 威胁防御设备支持和用于 SSL 连接的加密安全级别。

如果您的 威胁防御 设备具有评估许可证，默认情况下安全级别为“低”。使用 威胁防御 智能许可证时，默认安全级别为“高”。您可以选择以下选项之一来配置所需的安全级别：

- **All** 包括 NULL-SHA 等所有密码。
- **Low** 包括除 NULL-SHA 之外的所有密码。
- **Medium** 包括所有密码，但 NULL-SHA、DES-CBC-SHA、RC4-SHA 和 RC4-MD5（这是默认密码）除外。
- **Fips** 包括所有符合 FIPS 的密码，但 NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA 和 DES-CBC3-SHA 除外。
- **High** 只包含带有 SHA-2 加密的 AES-256，并适用于 TLS 版本 1.2 和默认版本。
- **Custom** 包括您在 Cipher algorithms/custom string 框中指定的一个或多个密码。此选项使您可以使用 OpenSSL 密码定义字符串对密码套件进行全面控制。

密码算法/自定义字符串- 列出 威胁防御 设备支持和用于 SSL 连接的加密算法。有关使用 OpenSSL 的密码的详细信息，请参阅 https://www.openssl.org/docs/apps/ciphers.html

威胁防御设备指定用于受支持密码的优先级顺序：

仅受 TLSv1.2 支持的密码

ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
AES256-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256

DHE-RSA-AES128-GCM-SHA256
AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
AES128-SHA256

TLSv1.1 或 TLSv1.2 不支持的密码

RC4-SHA
RC4-MD5
DES-CBC-SHA
NULL-SHA

配置安全外壳

如果在数据接口（例如外部）上启用了管理中心访问，则应使用此程序在该接口上启用SSH。本节介绍如何启用 威胁防御上一个或多个 数据 接口的 SSH 连接。 诊断逻辑接口上不支持 SSH。

注释 管理接口上默认已启用 SSH，但此屏幕不会影响管理 SSH 访问。

管理接口与设备上的其他接口分离。它用于设置设备并将其注册到管理中心。数据接口的 SSH 与管理接口的 SSH 共用内部和外部用户列表。其他设置单独进行配置：对于数据接口，使用此屏幕启用 SSH 和访问列表；数据接口的 SSH 流量使用常规路由配置，并不是所有静态路由均在设置时或 CLI 中配置。

对于管理接口，要配置 SSH 访问列表，请参阅 Cisco Secure Firewall Threat Defense 命令参考中的 **configure ssh-access-list** 命令。要配置静态路由，请参阅 **configure network static-routes** 命令。默认情况下，在初始设置时通过管理接口配置默认路由。

要使用 SSH，您也不需要允许主机 IP 地址的访问规则。您只需按照本部分配置 SSH。

您只能SSH到可访问接口；如果SSH主机位于外部接口上，则只能直接向外部接口发起管理连接。

注释 在您连续三次尝试使用 SSH 登录 CLI 失败后，设备会终止 SSH 连接。

开始之前

- 可以使用 **configure user add** 命令在 CLI 中配置 SSH 内部用户，请参阅 在 CLI 中添加内部用户，第 111 页。默认情况下，有一个您在初始设置期间为其配置密码的 **admin** 用户。还可以通过在平台设置中配置**外部身份验证**，在 LDAP 或 RADIUS 上配置外部用户。请参阅为 SSH 配置外部身份验证，第 619 页。
- 您需要定义允许与设备建立 SSH 连接的主机或网络网络对象。您可以在此过程中添加对象，但如果要使用对象组标识一组 IP 地址，请确保规则中所需的组已经存在。选择**对象** > **对象管理**以配置对象。

注释 不能使用系统提供的 **any** 网络对象。而是使用 **any-ipv4** 或 **any-ipv6**。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**安全外壳 (Secure Shell)**。

步骤 3 标识允许 SSH 连接的接口和 IP 地址。

使用此表可以限制哪些接口将接受 SSH 连接，以及允许建立这些连接的客户端的 IP 地址。您可以使用网络地址而不是单个 IP 地址。

a) 点击**添加 (Add)** 以添加新规则，或点击**编辑 (Edit)** 以编辑现有规则。

b) 配置规则属性：

- **IP 地址**-用于标识允许建立 HTTPS 连接的主机或网络的网络对象 或组 。从下拉列表中选择一个对象，或者点击 + 以添加新的网络对象。
- **安全区域** - 添加包含将允许进行 SSH 连接的接口的区域。对于不在区域中的接口，可以在**所选安全区域** 列表下方的字段中键入接口名称，然后点击 **添加**。仅当设备包含所选接口或区域时，才会将这些规则应用于该设备。

c) 点击**确定 (OK)**。

步骤 4 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 SMTP

如果在“系统日志”设置中配置了邮件警报，则必须标识 SMTP 服务器。为“系统日志”配置的源邮件地址必须是 SMTP 服务器上的有效帐户。

开始之前

确保存在用于定义主 SMTP 服务器和辅助 SMTP 服务器的主机地址的网络对象。依次选择**对象** > **对象管理**，以定义对象。或者，也可以在编辑策略时创建对象。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 点击 **SMTP 服务器**。

步骤 3 选择标识**主服务器 IP 地址**的网络对象，以及可选的**辅助服务器 IP 地址**。

步骤 4 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 SNMP

简单网络管理协议 (SNMP) 为在 PC 或工作站上运行的网络管理工作站定义了一种监控许多类型的设备（包括交换机、路由器和安全设备）的运行状况和状态的标准方法。您可以使用 SNMP 页面来配置防火墙设备，以便通过 SNMP 管理工作站进行监控。

简单网络管理协议 (SNMP) 支持从中心位置监控网络设备。思科安全设备支持使用 SNMP 版本 1、2c 和 3 进行网络监控，也支持陷阱和 SNMP 读取访问，但不支持 SNMP 写入访问。

SNMPv3 支持使用 DES（已弃用）、3DES、AES256、AES192 和 AES128 的只读用户和加密。

注释 DES 选项已被弃用。如果您的部署包括使用 6.5 之前的版本创建的使用 DES 加密的 SNMP v3 用户，则可以继续将这些用户用于 威胁防御运行 6.6 及更低版本的 。但是，您不能编辑这些用户并保留 DES 加密，也不能使用 DES 加密创建新用户。如果您的 管理中心 管理任何运行版本 7.0+ 的 威胁防御，则将使用 DES 加密的平台设置策略部署到这些 威胁防御将会失败。

注释 SNMP 配置仅支持路由和诊断接口。

注释 要创建发送至外部 SNMP 服务器的警报，请访问**策略 (Policies)** > **操作 (Action)** > **警报 (Alerts)**

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择 **SNMP**。

步骤 3 启用 SNMP 并配置基本选项。

- **启用 SNMP 服务器** - 是否向配置的 SNMP 主机提供 SNMP 信息。您可以取消选择此选项，以便在保留配置信息的同时禁用 SNMP 监控。
- **读取社区字符串、确认** - 输入在向 威胁防御设备发送请求时，SNMP 管理工作站使用的密码。SNMP 社区字符串是 SNMP 管理工作站与受管的网络节点之间的共享密钥。安全设备使用此密码确定传入的 SNMP 请求是否有效。密码是区分大小写的字母数字字符串，最多可包含 32 个字符；不允许使用空格和特殊字符。
- **系统管理员名称** - 输入设备管理员或其他联系人的名称。该字符串区分大小写，最多可以包含 127 个字符。接受空格，但多个空间缩为一个空格。
- **位置** - 输入此安全设备的位置（例如，54 区 42 号楼）。该字符串区分大小写，最多可以包含 127 个字符。接受空格，但多个空间缩为一个空格。
- **端口** - 输入将在其上接受传入请求的 UDP 端口。默认值为 161。

步骤 4 （仅限 SNMPv3）。添加 SNMPv3 用户，第 638 页。

步骤 5 添加 SNMP 主机，第 641 页。

步骤 6 配置 SNMP 陷阱，第 642 页。

步骤 7 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

关于 SNMP

SNMP 是一种应用层协议，可促进网络设备之间的管理信息交换，是 TCP/IP 协议簇的一部分。 威胁防御 为使用 SNMP 版本 1、2c 和 3 的网络监控提供支持，并支持同时使用所有三个版本。利用在威胁防御 接口上运行的 SNMP 代理，您可以通过诸如 HP OpenView 之类的网络管理系统 (NMS) 监控网络设备。威胁防御 通过发出 GET 请求来支持 SNMP 只读访问。不允许 SNMP 写访问，因此您无法对 SNMP 进行更改。此外，不支持 SNMP SET 请求。

您可以将 威胁防御 配置为向 NMS 发送陷阱，即针对特定事件从托管设备发送到管理站的未经请求的消息（事件通知），也可以使用 NMS 浏览安全设备上的管理信息库 (MIB)。MIB 是定义的集合，而 威胁防御 维护由每个定义的值组成的数据库。浏览 MIB 意味着从 NMS 发出 MIB 树的一系列 GET-NEXT 或 GET-BULKGET 请求以确定值。

SNMP 代理可在发生预定义为需要通知（例如，当网络中的链路开启或关闭时）的事件的情况下通知指定的管理站。它发送的通知包括用于向管理站表明其自身身份 SNMP OID。代理还会在管理站请求信息时进行回复。

SNMP 术语

下表列出在使用 SNMP 时常用的术语。

表 *63: SNMP* 术语

术语	说明
代理	在 Cisco Secure Firewall Threat Defense 上运行的 SNMP 服务器。SNMP 代理具有以下功能： • 对来自网络管理站的信息和操作请求作出响应。 • 控制对其管理信息库（即 SNMP 可以查看或更改的对象的集合）的访问。 • 不允许 SET 操作。
浏览	通过从设备上的 SNMP 代理轮询所需信息来从网络管理站监控该设备的运行状况。此活动可能包括从网络管理站发出 MIB 树的一系列 GET-NEXT 或 GET-BULK 请求以确定值。
管理信息库 (MIB)	用于收集有关数据包、连接、缓冲区、故障切换等的信息的标准化数据结构。MIB 由大多数网络设备使用的产品、协议和硬件标准来定义。SNMP 网络管理站可以浏览 MIB，并请求在出现特定数据或事件时将其发送。
网络管理站 (NMS)	设置 PC 或工作站是为了监控 SNMP 事件和管理设备。
对象标识符 (OID)	用于向设备的 NMS 表明该设备的身份并向用户指示监控和显示的信息源的系统。
陷阱	用于生成从 SNMP 代理到 NMS 的消息的预定义事件。事件包括警报条件，例如链路开启、链路关闭、冷启动、热启动、身份验证或系统日志消息。

MIB 和陷阱

MIB 特定于标准或特定于企业。标准 MIB 由 IETF 创建并记录在各种 RFC 中。陷阱报告发生在网络设备上的重大事件，大多数情况下是错误或故障。SNMP 陷阱在特定于标准或特定于企业的 MIB 中进行定义。标准陷阱由 IETF 创建并记录在各种 RFC 中。SNMP 陷阱会编译成 ASA 软件。

如果需要，您还可以从以下位置下载 RFC、标准 MIB 和标准陷阱：

http://www.ietf.org/

浏览 SNMP 对象导航器，从以下位置查找思科 MIB、陷阱和 OID：

https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

此外，从以下位置通过 FTP 下载思科 OID：

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

MIB 支持的表和对象

以下部分列出了对指定 MIB 支持的表和对象。

远程接入 VPN 轮询

表 64: CISCO-REMOTE-ACCESS-MONITOR-MIB

计数器	OID	说明
活动会话	crasNumSessions (1.3.6.1.4.1.9.9.392.1.3.1)	当前活动会话的数量。
用户	crasNumUsers (1.3.6.1.4.1.9.9.392.1.3.3)	具有活动会话的用户数。
峰值会话	crasNumPeakSessions (1.3.6.1.4.1.9.9.392.1.3.41)	自系统启动以来的峰值 RA 会话数。

站点间 VPN 隧道轮询

表 65: CISCO-REMOTE-ACCESS-MONITOR-MIB

计数器	OID	说明
LAN 到 LAN 会话	crasL2LNumSessions (1.3.6.1.4.1.9.9.392.1.3.29)	当前活动的 LAN 到 LAN 会话数。
峰值 LAN 到 LAN 会话数	crasL2LPeakConcurrentSessions (1.3.6.1.4.1.9.9.392.1.3.31)	自系统启动以来的峰值并发 LAN 会话数。

连接轮询

表 66: CISCO-FIREWALL-MIB

计数器	OID	说明
活动连接数	cfwConnectionActive (1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.6)	整个防火墙当前使用的连接数。
峰值连接	cfwConnectionPeak (1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.7)	自系统启动以来在任何时间使用的最高连接数。
每秒连接数	cfwConnectionPerSecond (1.3.6.1.4.1.9.9.147.1.2.2.3)	防火墙上的当前每秒连接数。

计数器	OID	说明
每秒峰值连接数	cfwConnectionPerSecondPeak (1.3.6.1.4.1.9.9.147.1.2.2.4)	自系统启动以来防火墙上的每秒最高连接数。

NAT 转换轮询

表 *67: CISCO-NAT-EXT-MIB*

计数器	OID	说明
活动转换	cneAddrTranslationNumActive (1.3.6.1.4.1.9.9.532.1.1.1.1)	NAT 设备中当前可用的地址转换条目总数。这表示从静态和动态地址转换机制创建的转换条目的汇总。
峰值活动转换	cneAddrTranslationNumPeak (1.3.6.1.4.1.9.9.532.1.1.1.2)	自系统启动以来任何时候处于活动状态的最大地址转换条目数。这表示自系统启动以来任何时候处于活动状态的地址转换条目的高水印。 该对象包括从静态和动态地址转换机制创建的转换条目。

路由表条目轮询

表 *68: IP-FORWARD-MIB*

计数器	OID	说明
活动转换	inetCidrRouteNumber (1.3.6.1.2.1.4.24.6)	当前有效的 inetCidrRouteTable 条目总数。

接口双工状态轮询

表 *69: CISCO-IF-EXTENSION-MIB*

计数器	OID	说明
双工状态	cieIfDuplexCfgStatus (1.3.6.1.4.1.9.9.276.1.1.2.1.20)	此对象会指定给定接口上配置的双工状态。

计数器	OID	说明
检测到的双工状态	cieIfDuplexDetectStatus (1.3.6.1.4.1.9.9.276.1.1.2.1.21)	此对象指定给定接口上检测到的双工状态。

Snort 3 入侵事件速率轮询

表 70: CISCO-UNIFIED-FIREWALL-MIB

计数器	OID	说明
Snort 3 入侵事件速率	cufwAaicIntrusionEvtRate (1.3.6.1.4.1.9.9.491.1.5.3.2.1)	在过去 300 秒内，Snort 在此防火墙上记录入侵事件的平均速率。

BGP 对等翻板陷阱通知

表 71: BGP4-MIB

计数器	OID	说明
BGP 对等翻板	bgpBackwardTransition (1.3.6.1.4.1.9.9.491.1.5.3.2.1)	当 BGP FSM 从较高编号状态移动到较低编号状态时，就会生成 BGPBackwardTransition 事件。

注释 在 ASA FirePOWER 上删除了与 CPU 监控（hrProcessorTable 和 hrNetworkTable）相关的 SNMP OID 1.3.6.1.2.1.25.3.3 和 1.3.6.1.2.1.25.3.4。您只能通过设备管理器查看和监控设备的 CPU 运行状况详细信息。

添加 SNMPv3 用户

注释 您只为 SNMPv3 创建用户。这些步骤不适用于 SNMPv1 或 SNMPv2c。

请注意，SNMPv3 只支持只读用户。

SNMP 用户具有指定的用户名、身份验证密码、加密密码以及要使用的身份验证和加密算法。

注释 将 SNMPv3 用于群集或高可用性时，如果在初始集群形成后添加新的集群设备或更换高可用性设备，则 SNMPv3 用户不会复制到新设备。您必须删除用户、重新添加，然后重新部署配置，以强制用户复制到新单元。

身份验证算法选项包括 MD5（解密，仅限预-6.5）、 SHA、SHA224、SHA256 和 SHA384。

注释 MD5 选项已被弃用。如果您的部署包括使用 6.5 之前版本创建的使用 MD5 身份验证算法的 SNMP v3 用户，则可以继续将这些用户用于运行 6.7 及更低版本的 FTD。但是，您无法编辑这些用户并保留 MD5 身份验证算法，或使用 MD5 身份验证算法创建新用户。如果您的 管理中心 管理任何运行 7.0 以上版本的 威胁防御，则将使用 MD5 身份验证算法的平台设置策略部署到这些 威胁防御将失败。

加密算法选项是 DES（解密、仅限预-6.5）、3DES、AES256、AES192 和 AES128。

注释 DES 选项已被弃用。如果您的部署包括使用 6.5 之前的版本创建的使用 DES 加密的 SNMP v3 用户，则可以继续将这些用户用于运行 6.7 及更低版本的 威胁防御。但是，您不能编辑这些用户并保留 DES 加密，也不能使用 DES 加密创建新用户。如果您的 管理中心 管理任何运行版本 7.0+ 的 威胁防御，则将使用 DES 加密的平台设置策略部署到这些 威胁防御将会失败。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 请点击 **SNMP** > **用户 (Users)**。

步骤 3 点击 **Add**。

步骤 4 从**安全级别**下拉列表中选择用户的安全级别。

- **Auth** - 有身份验证但无隐私，意味着消息会进行身份验证。
- **No Auth** - 无身份验证且无隐私，意味着未对消息应用安全设置。
- **Priv** - 有身份验证且有隐私，意味着对消息进行身份验证和加密。

步骤 5 在**用户名**字段中输入 SNMP 用户的名字。用户名长度不得超过 32 个字符

步骤 6 在**加密密码类型**下拉列表中选择要使用的密码类型。

- **明文** - 威胁防御设备在部署到设备时仍将对密码进行加密。
- **加密** - 威胁防御设备将直接部署加密的密码。

步骤 7 在 **授权算法类型** 下拉列表中选择要使用的身份验证类型： SHA、 SHA224、 SHA256或 SHA384。

注释 MD5 选项已被弃用。如果您的部署包括使用 6.5 之前版本创建的使用 MD5 身份验证算法的 SNMP v3 用户，则可以继续将这些用户用于运行 6.7 及更低版本的 FTD。但是，您无法编辑这些用户并保留 MD5 身份验证算法，或使用 MD5 身份验证算法创建新用户。如果您的 管理中心 管理任何运行 7.0 以上版本的 威胁防御，则将使用 MD5 身份验证算法的平台设置策略部署到这些 威胁防御将失败。

步骤 8 在**身份验证密码**字段中，输入用于身份验证的密码。如果选择“加密为加密密码类型”，则密码必须格式化为 xx:xx:xx...，其中 xx 为十六进制值。

注释 密码的长度将取决于所选的身份验证算法。对于所有密码，长度必须不能超过 256个字符。

如果选择“明文”作为“加密密码”类型，请在**确认**字段中重复该密码。

步骤 9 在**加密类型 (Encryption Type)** 下拉列表中，选择要使用的加密类型：AES128、AES192、AES256、3DES。

注释 要使用 AES 或 3DES 加密，必须在设备上安装相应的许可证。

注释 DES 选项已被弃用。如果您的部署包括使用 6.5 之前的版本创建的使用 DES 加密的 SNMP v3 用户，则可以继续将这些用户用于运行 6.7 及更低版本的 威胁防御。但是，您不能编辑这些用户并保留 DES 加密，也不能使用 DES 加密创建新用户。如果您的 管理中心 管理任何运行版本 7.0+ 的 威胁防御，则将使用 DES 加密的平台设置策略部署到这些 威胁防御将会失败。

步骤 10 在**加密密码 (Encryption Password)** 字段中输入用于加密的密码。如果选择“加密为加密密码类型”，则密码必须格式化为 xx:xx:xx...，其中 xx 为十六进制值。对于加密的密码，密码的长度取决于所选的加密类型。密码大小如下（每个 xx 是一个八进制值）：

- AES 128 需要 16 个八进制值
- AES 192 需要 24 个八进制值
- AES 256 需要 32 个八进制值
- 3DES 需要 32 个八进制值
- DES 可以是任意大小

注释 对于所有密码，长度必须不能超过 256个字符。

如果选择“明文”作为“加密密码”类型，请在**确认**字段中重复该密码。

步骤 11 点击**确定 (OK)**。

步骤 12 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

添加 SNMP 主机

使用“主机”(Host) 以在 SNMP 页面上的“SNMP 主机”(SNMP Hosts) 表中添加或编辑条目。这些条目表示允许访问 威胁防御设备的 SNMP 管理站。

最多可以添加 8192 台主机。但是，其中仅 128 台可用于陷阱。

开始之前

确保存在定义 SNMP 管理站的网络对象。选择**设备** > **对象管理**以配置网络对象。

注释 支持的网络对象包括 IPv6 主机、IPv4 主机、IPv4 范围和 IPv4 子网地址。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 点击 **SNMP** > **主机 (Hosts)**。

步骤 3 点击 **Add**。

步骤 4 在 **IP 地址**字段中，输入有效的 IPv6 或 IPv4 主机或选择定义 SNMP 管理站主机地址的网络对象。

IP 地址可以是 IPv6 主机、IPv4 主机、IPv4 范围或 IPv4 子网。

步骤 5 从 **SNMP 版本**下拉列表中选择适当的 SNMP 版本。

步骤 6 （仅限 SNMPv3。）从**用户名**下拉列表中选择您配置的 SNMP 用户的用户名。

注释 每个 SNMP 主机最多可以关联 23 个 SNMP 用户。

步骤 7 （仅限 SNMPv1、2c。）在**读取社区字符串**字段中，输入已配置的社区字符串，以便对设备进行读取访问。重新输入该字符串以进行确认。

注释 仅当与此 SNMP 工作站一起使用的字符串与**启用 SNMP 服务器**部分中定义的字符串不同时，才需要此字符串。

步骤 8 选择设备与 SNMP 管理站之间的通信类型。您可以选择以下两种类型。

- **轮询** - 管理站会定期从设备请求信息。
- **陷阱** - 在发生陷阱事件时，设备将陷阱事件发送到管理站。

注释 当 SNMP 主机 IP 地址是 IPv4 范围或 IPv4 子网时，您可以配置**轮询**或**陷阱**，而不是同时配置两者。

步骤 9 在**端口**字段中，输入 SNMP 主机的 UDP 端口号。默认值为 162。有效范围为 1 至 65535。

步骤 10 在**访问方式 (Reachable By)** 选项下，选择设备与 SNMP 管理站之间通信的接口类型。您可以选择设备的管理接口或可用的安全区域/命名接口。

- **设备管理接口 (Device Management Interface)** - 设备和 SNMP 管理站之间通过管理接口进行通信。

- 当您选择此接口进行 SNMPv3 轮询时，系统将允许所有已配置的 SNMPv3 用户进行轮询，而不限于步骤 步骤 6，第 641 页中选择的用户。此处，SNMPv3 主机不允许 SNMPv1 和 SNMPv2c。
- 当您为 SNMPv1 和 SNMPv2c 轮询选择此接口时，轮询完全不受步骤 步骤 5，第 641 页中所选版本的限制。

- **安全区域或命名接口 (Security Zones or Named Interface)** - 设备和 SNMP 管理站之间通过安全区域或接口进行通信。
  - 在**可用区域 (Available Zones)** 字段中搜索区域。
  - 添加包含设备可通过其与管理站通信的接口的区域至 **选择的区域/接口 (Selected Zone/Interface)** 字段中。对于不在区域中的接口，您可以在**所选区域/接口**列表下方的字段中键入接口名称，然后点击**添加**。仅在设备包含所选接口或区域时，系统才会在设备上配置主机。

步骤 11 点击**确定 (OK)**。

步骤 12 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 SNMP 陷阱

使用“SNMP 陷阱”为 威胁防御 设备配置 SNMP 陷阱（事件通知）。 陷阱不同于浏览；它们是特定事件（例如上行链路、下行链路和系统日志事件）的从 威胁防御设备到管理站的未经请求的“注释"。该设备的 SNMP 对象 ID (OID) 显示在从设备发送的 SNMP 事件陷阱中。

某些陷阱不适用于某些硬件型号。如果将策略应用于其中某个型号，则这些陷阱将被忽略。例如，并非所有型号都有可现场更换的设备，因此不会在这些型号上配置**现场可更换的设备插入/删除**陷阱。

SNMP 陷阱在特定于标准或特定于企业的 MIB 中进行定义。标准陷阱由 IETF 创建并记录在各种 RFC 中。SNMP 陷阱会编译成 威胁防御软件。

如果需要，您还可以从以下位置下载 RFC、标准 MIB 和标准陷阱：

http://www.ietf.org/

从以下位置浏览思科 MIB、陷阱和 OID 的完整列表：

SNMP 对象导航器

此外，从以下位置通过 FTP 下载思科 OID：

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 使用 **SNMP** > **SNMP 陷阱** 为 威胁防御 设备配置 SNMP 陷阱（事件通知）。

步骤 3 选择适当的“启用陷阱”选项。您可以选择其中任一或两个选项。

a) 选中**启用所有 SNMP 陷阱**可在随后的四个部分中快速选择所有陷阱。

b) 选中**启用所有系统日志陷阱**以启用与陷阱相关的系统日志消息的传输。

注释 SNMP 陷阱预计近乎是实时的，因此优先级高于 威胁防御发出的其他通知消息。启用所有 SNMP 或系统日志陷阱时，SNMP 进程可能会消耗代理和网络中的过多资源，导致系统挂起。如果您发现系统延迟、未完成的请求或超，可以选择性地启用 SNMP 和系统日志陷阱。您也可以限制按严重性级别或消息 ID 生成系统日志消息的速率。例如，所有以数字 212 开头的系统日志消息 ID 都与 SNMP 类相关联。请参阅限制系统日志消息生成速率，第 656 页。

步骤 4 默认情况下，为现有策略启用**标准**部分中的事件通知陷阱：

- **身份验证** - 未经授权的 SNMP 访问。对于具有不正确的社区字符串的数据包，将会出现此身份验证失败。
- **上行链路 (Link Up)** - 设备的一个通信链路已变为可用（已“出现"），如通知中所示。
- **下行链路 (Link Down)** - 设备的一个通信链路已出现故障，如通知中所示。
- **冷启动 (Cold Start)** - 设备正在重新初始化自身，以使其配置或协议实体实现可能被更改。
- **热启动 (Warm Start)** - 设备正在重新初始化自身，以使其配置或协议实体实现不更改。

步骤 5 在**实体 MIB** 部分中选择所需的事件通知陷阱：

- **现场可更换设备插入** - 已插入现场可更换单元 (FRU)，如通知中所示。（FRU 包括电源、风扇、处理器模块、接口模块等组件）
- **现场可更换设备删除** - 已删除现场可更换单元 (FRU)，如通知中所示。
- **配置更改** - 已发生硬件更改，如通知中所示

步骤 6 在**资源**部分中选择所需的事件通知陷阱：

- **已达到连接限制** - 此陷阱指示连接尝试被拒绝，因为已达到配置的连接限制。

步骤 7 在**其他**部分中选择所需的事件通知陷阱：

- **NAT 数据包丢弃** - 此通知在 NAT 功能丢弃 IP 数据包时生成。可用的网络地址转换地址或端口已低于所配置的阈值。
- **CPU 上升阈值 (CPU Rising Threshold)** - 在配置的时间段内，当 CPU 使用率上升超过预定义阈值时，生成此通知。选中此选项可启用 CPU 上升阈值通知：

- **百分比 (Percentage)** - 对于高阈值通知，默认值为 70%；范围介于 10% 和 94% 之间。临界阈值硬编码为 95%。
- **期间 (Period)** - 默认监控周期为 1 分钟；范围介于 1 到 60 分钟之间。

- **内存上升阈值 (Memory Rising Threshold)** - 当内存利用率上升超过预定义阈值时，会生成此通知，从而减少可用内存。选中此选项可启用内存上升阈值通知：
  - **百分比 (Percentage)** - 对于高阈值通知，默认值为 70%；范围介于 50% 和 95% 之间。
- **故障转移 (Failover)** - 当 CISCO-UNIFIED-FIREWALL-MIB 报告的故障切换状态发生变化时，生成此通知。
- **集群 (Cluster)** - 当 CISCO-UNIFIED-FIREWALL-MIB 报告集群运行状况发生变化时，生成此通知。
- **对等体摆动** - 当存在 BGP 路由摆动（即 BGP 系统发送过多的更新消息来通告网络可访问性信息）时，生成此通知。

步骤 8 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置系统日志

您可以为 威胁防御设备启用系统日志记录（系统日志）。日志记录信息可以帮助您发现并隔离网络或设备配置问题。您还可以将一些安全事件发送到系统日志服务器。以下主题介绍日志记录以及如何配置日志记录。

关于系统日志

系统日志记录是将来自设备的消息收集到运行系统日志后台守护程序的服务器的方法。将信息记录到中央系统日志服务器有助于汇聚日志和提醒。思科设备可以将其日志消息发送到 UNIX 样式的系统日志服务。系统日志服务接受消息并将其存储在文件中，或者根据简单配置文件打印消息。以这种形式记录日志可为日志提供受保护的长期存储。日志对常规故障排除及事件处理均有帮助。

表 *72: ...*的系统日志 *Cisco Secure Firewall Threat Defense*

与以下各项相关的日志	详细信息	配置位置
设备和系统运行状况、网络配置	此系统日志配置可为在数据平面上运行的功能（即在 CLI 配置中定义的功能，可以使用 **show running-config** 命令查看这些功能）生成消息。这包括诸如路由、VPN、数据接口、DHCP 服务器、NAT 等功能。数据平面系统日志消息将被编号，并且这些消息与运行 ASA 软件的设备所生成的那些消息相同。但是，Cisco Secure Firewall Threat Defense不一定会生成每种可用于 ASA 软件的消息类型。有关这些消息的信息，请参阅思科 *Cisco Secure Firewall Threat Defense*系统日志消息，网址为：https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html。此配置将在以下主题中加以说明。	**平台设置**
安全事件	此系统日志配置会生成文件和恶意软件、连接、安全情报和入侵事件的警报。	访问控制策略中的**平台设置**和 **日志记录**
（所有设备） 策略、规则和事件	此系统日志配置将为访问控制规则、入侵规则和中所述的其他高级服务生成警报，如 《Cisco Secure Firewall Management Center 管理指南》中的配置支持警报响应。这些消息不会被编号。有关配置这种类型的系统日志的信息，请参阅 《Cisco Secure Firewall Management Center 管理指南》中的 创建系统日志警报响应 。	访问控制策略中的**警报响应**和 **日志记录**

可以配置多个系统日志服务器，并可控制发送到每个服务器的消息和事件。还可配置不同目标，如控制台、邮件、内部缓冲区等。

严重性级别

下表列出系统日志消息严重性级别。

表 *73:* 系统日志消息严重级别

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

级别号	严重性级别	说明
6	**信息性**	消息仅供参考。
7	**调试**	消息仅供调试。 调试问题时，仅临时记录此级别的日志。此日志级别可能会生成太多消息，从而影响系统性能。

注释 ASA 和 威胁防御 不会生成严重性级别为零 (emergencies) 的系统日志消息。

系统日志消息过滤

您可以过滤生成的系统日志消息，以便仅将某些系统日志消息发送到特定输出目标。例如，您可以将 威胁防御设备配置为将所有系统日志消息发送至一个输出目标，而将这些系统日志消息中的一部分发送至其他输出目标。

具体而言，您可以根据以下条件将系统日志消息定向到输出目标：

- 系统日志消息 ID 号

  （这不适用于连接和入侵事件等安全事件的系统日志消息。）

- 系统日志消息严重性级别
- 系统日志消息类（相当于一个功能区）

  （这不适用于连接和入侵事件等安全事件的系统日志消息。）

通过创建一个在设置输出目标时可以指定的消息列表来自定义这些条件。或者，可以将 威胁防御设备 配置为将一个特定的消息类发送至每种类型的输出目标，而不管消息列表是什么。

（消息列表不适用于连接和入侵事件等安全事件的系统日志消息。）

系统日志消息类

注释 此主题不适用于安全事件（连接、入侵等）的消息。

可以通过两种方法使用系统日志消息类：

- 指定整个类别的系统日志消息的输出位置。使用 **logging class** 命令。
- 创建指定消息类的消息列表。使用 **logging list** 命令。

系统日志消息类提供一个按类型将系统日志消息分类的方法，相当于设备的特性或功能。例如，RIP 类表示 RIP 路由。

特定类中的所有系统日志消息共享其系统日志消息 ID 号中相同的前三位数字。例如，所有以数字 611 开头的系统日志消息 ID 都与 vpnc（VPN 客户端）类相关联。与 VPN 客户端功能相关联的系统日志消息范围从 611101 至 611323。

此外，大多数 ISAKMP 系统日志消息都具有公用预置对象集来帮助识别隧道。这些对象在适用时前置于系统日志消息的描述性文本。如果在生成系统日志消息时对象未知，则不显示特定的 heading = value 组合。

对象的前缀如下：

Group = *groupname*, Username = *user*, IP = *IP_address*

其中组是隧道组，用户名是来自本地数据库或 AAA 服务器的用户名，IP 地址是远程访问客户端或第 2 层对等体的公用 IP 地址。

下表列出消息类以及每个类中的消息 ID 范围。

表 *74:* 系统日志消息类和关联的消息 *ID* 号

类别	定义	系统日志消息 ID 号
auth	用户身份验证	109、113
-	访问列表	106
-	应用防火墙	415
bridge	透明防火墙	110、220
ca	PKI 证书颁发机构	717
citrix	Citrix Client	723
-	集群	747
-	卡管理	323
config	命令界面	111、112、208、308
csd	安全桌面	724
cts	Cisco TrustSec	776
dap	动态访问策略	734
eap, eapoudp	用于网络准入控制的 EAP 或 EAPoUDP	333、334
eigrp	EIGRP 路由	336
电子邮件	邮件代理	719
-	环境监控	735
ha	故障切换	101、102、103、104、105、210、311、709

类别	定义	系统日志消息 ID 号
-	基于身份认证的防火墙	746
ids	入侵检测系统	400、733
-	IKEv2 工具包	750、751、752
ip	IP 堆栈	209、215、313、317、408
ipaa	IP 地址分配	735
ips	入侵保护系统	400、401、420
-	IPv6	325
-	僵尸网络流量过滤。	338
-	许可	444
mdm-proxy	MDM 代理	802
nac	网络准入控制	731、732
nacpolicy	NAC 策略	731
nacsettings	配置 NAC 设置，以应用 NAC 策略	732
-	网络无线接入点	713
np	网络处理器	319
-	NP SSL	725
ospf	OSPF 路由	318、409、503、613
-	密码加密	742
-	电话代理	337
rip	RIP 路由	107、312
rm	资源管理器	321
-	Smart Call Home	120
session	用户会话	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
snmp	SNMP	212
-	ScanSafe	775

类别	定义	系统日志消息 ID 号
ssl	SSL 堆栈	725
svc	SSL VPN 客户端	722
sys	System	199、211、214、216、306、307、315、414、604、605，606、610、612、614、615、701、711、741
-	威胁检测	733
tre	事务规则引擎	780
-	UC-IME	339
标记交换	服务标记交换	779
vm	VLAN 映射	730
vpdn	PPTP 和 L2TP 会话	213、403、603
vpn	IKE 和 IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN 客户端	611
vpnfo	VPN 故障切换	720
vpnlb	VPN 负载均衡	718
-	VXLAN	778
webfo	WebVPN 故障切换	721
webvpn	WebVPN 和 AnyConnect 客户端	716
-	NAT 与 PAT	305

日志记录准则

本节介绍您在配置日志记录之前应审阅的准则和限制。

IPv6 准则

- 支持 IPv6。可以使用 TCP 或 UDP 发送系统日志。
- 确保配置用于发送系统日志的接口已经启用，支持 IPv6，并且可以通过指定接口到达系统日志服务器。
- 不支持通过 IPv6 进行安全登录。

其他准则

- 请勿配置 管理中心 为主系统日志服务器。 管理中心 可以记录一些系统日志。但是，它没有足够的存储调配来容纳来自每个传感器的连接事件的大量信息，尤其是在使用多个传感器并且都发送系统日志时。
- 系统日志服务器必须运行一个名为 syslogd 的服务器程序。Windows 提供了一个系统日志服务器，作为其操作系统的组成部分。
- 要查看由 威胁防御设备 生成的日志，必须指定日志记录输出目标。如果启用日志记录而未指定日志记录输出目标，则 威胁防御设备 会生成消息，但不会将其保存到可对其进行查看的位置。必须单独指定每个不同的日志记录输出目标。
- 如果您使用 TCP 作为传输协议，系统会打开与系统日志服务器的 4 个连接，以确保消息不会丢失。如果您使用系统日志服务器从大量设备收集消息，并且合并的连接开销对该服务器来说太大，请改用 UDP。
- 不能将两个不同的列表或类分配给不同的系统日志服务器或相同位置。
- 您最多可以配置 16 个系统日志服务器。
- 应该可以通过 威胁防御设备 到达系统日志服务器。应将该设备配置为拒绝可以从其到达系统日志服务器的接口上的 ICMP 不可达消息，并将系统日志发送到同一服务器。请确保已对所有严重性级别启用日志记录。要防止系统日志服务器崩溃，请抑制系统日志 313001、313004 和 313005 的生成。
- 用于系统日志的 UDP 连接数与硬件平台上的 CPU 数量和您配置的系统日志服务器数量直接相关。在任何时刻，UDP 系统日志连接的数量都等于 CPU 数量乘以已配置的系统日志服务器数量的积。这是预期行为。请注意，全局 UDP 连接空闲超时适用于这些会话，默认值为 2 分钟。如果您想更快关闭这些会话，可以调整该设置，但超时适用于所有 UDP 连接，而不仅是系统日志。
- 当 威胁防御设备 通过 TCP 发送系统日志时，在系统日志服务重新启动后，需要大约一分钟来启动连接。

配置 FTD 设备的系统日志日志记录

提示 如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则大多数 FTD 平台设置不适用于这些消息。请参阅适用于安全事件系统日志消息的 威胁防御 平台设置，第 651 页。

要配置系统日志设置，请执行以下步骤：

开始之前

请参阅日志记录准则，第 649 页中的要求。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 从目录中选择**系统日志**。

步骤 3 点击**日志记录设置 (Logging Setup)** 以启用日志记录，指定 FTP 服务器设置，并指定闪存用法。有关详细信息，请参阅启用日志记录并配置基本设置，第 652 页

步骤 4 点击**日志记录目标 (Logging Destinations)** 可以启用对特定目标的日志记录，并指定对邮件严重性级别、事件类或自定义事件列表的过滤。有关详细信息，请参阅启用日志记录目标，第 653 页

必须启用日志记录目标才能查看该目标的消息。

步骤 5 点击**邮件设置 (E-mail Setup)** 以指定用作以邮件形式发送的系统日志消息的源地址的邮件地址。有关详细信息，请参阅将系统日志消息发送给邮件消息，第 654 页

步骤 6 点击**事件列表 (Events List)** 可定义包括事件类、严重性级别和事件 ID 的自定义事件列表。有关详细信息，请参阅创建自定义事件列表，第 655 页

步骤 7 点击**速率限制 (Rate Limit)** 可指定发送到所有配置的目标的邮件数量，并定义要为其分配速率限制的邮件严重性级别。有关详细信息，请参阅限制系统日志消息生成速率，第 656 页

步骤 8 点击**系统日志设置 (Syslog Settings)** 以指定日志记录设施，启用时间戳包含，并启用其他设置以将服务器设置为一个系统日志目标。有关详细信息，请参阅配置系统日志设置，第 656 页

步骤 9 点击**系统日志服务器 (Syslog Servers)** 以便为指定为日志记录目标的系统日志服务器指定 IP 地址、使用的协议、格式和安全区域。有关详细信息，请参阅配置系统日志服务器，第 658 页

适用于安全事件系统日志消息的 威胁防御 平台设置

“安全事件”包括连接、安全情报、入侵以及文件和恶意软件事件。

设备 > 平台设置 > 威胁防御设置 > 系统日志 页面及其选项卡上的某些系统日志设置适用于安全事件的系统日志消息，但大多数只适用于与系统运行状况和网络有关的事件的信息。

以下设置适用于安全事件的系统日志消息：

- **日志记录设置**选项卡：
  - **发送 EMBLEM 格式的系统日志**
- **系统日志设置**选项卡：
  - **在系统日志消息中启用时间戳**
  - **时间戳格式**
  - **启用系统日志设备 ID**
- **系统日志服务器**选项卡：
  - **添加系统日志服务器**表单 （以及已配置的服务器列表） 上的所有选项。

启用日志记录并配置基本设置

您必须为系统启用日志记录，才能为数据平面事件生成系统日志消息。

您还可以将闪存或 FTP 服务器上的存档设置为本地缓冲区已满时使用的存储位置。您可以在保存日志记录数据后对其进行操作。例如，可以指定在记录特定类型的系统日志消息后要执行的操作，从日志提取数据并将记录保存到其他文件以进行报告，或者使用特定于站点的脚本跟踪统计信息。

下面的过程介绍了一些基本系统日志设置。

提示 如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则大多数 威胁防御 平台设置不适用于这些消息。请参阅适用于安全事件系统日志消息的 威胁防御 平台设置，第 651 页。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**系统日志** > **日志记录设置**。

步骤 3 启用日志记录并配置基本日志记录设置。

- **启用日志记录** - 为 威胁防御设备启用数据平面系统日志记录。
- **在故障切换备用设备上启用日志记录** - 为 威胁防御设备的备用设备（如果有）启用日志记录。
- **以 EMBLEM 格式发送系统日志** - 为每个日志记录目标启用 EMBLEM 格式日志记录。如果启用 EMBLEM，必须使用 UDP 协议来发布系统日志消息，EMBLEM 与 TCP 不兼容。

  注释 RFC5424 格式的系统日志消息通常显示优先级值（PRI）。但是，在 管理中心中，只有当您启用 Cisco EMBLEM 格式的日志记录时，才会显示受管 威胁防御的系统日志消息中的 PRI 值。有关 PRI 的详细信息，请参阅 RFC5424。

- **发送调试消息作为系统日志** - 将所有调试跟踪输出重定向到系统日志。如果启用了此选项，则控制台中不会显示系统日志消息。因此，要查看调试消息，必须在控制台上启用日志记录并将其配置为调试系统日志消息编号和日志记录级别的目标。使用的系统日志消息编号是 711001。此系统日志的默认日志记录级别为调试。
- **内部缓冲区的内存大小** - 指定在启用了日志记录缓冲区的情况下，将系统日志消息保存到的内部缓冲区的大小。当缓冲区填满时，它将被覆盖。默认值为 4096 字节。范围为 4096 到 52428800。

步骤 4 （可选）通过选中**为 FMC 启用日志记录**复选框启用 VPN 日志记录。从**日志记录级别**下拉列表中选择 VPN 消息的系统日志严重性级别。

有关级别的信息，请参阅严重性级别，第 645 页。

步骤 5 （可选）如果要在覆盖缓冲区之前将日志缓冲区内容保存到 FTP 服务器，请配置该服务器。指定 FTP 服务器信息。

- **FTP 服务器缓冲区回绕** - 要在缓冲区内容被覆盖之前将其保存到 FTP 服务器，请选中此框并在以下字段中输入必要的目标信息。要删除 FTP 配置，请取消选择此选项。

- **IP 地址** - 选择包含 FTP 服务器 IP 地址的主机网络对象。
- **用户名** - 输入连接到 FTP 服务器时要使用的用户名。
- **路径** - 输入相对于 FTP 根目录的路径，缓冲区内容应保存在此处。
- **密码/确认** - 输入并确认用于对访问 FTP 服务器的用户名进行身份验证的密码。

步骤 6 （可选）如果要在覆盖缓冲区之前将日志缓冲区内容保存到闪存，请指定闪存大小。

- **闪存** - 要在缓冲区内容被覆盖之前将其保存到闪存，请选中此框。
- **日志记录所使用的最大闪存大小 (KB)** - 指定用于日志记录的闪存所使用的最大空间（以 KB 为单位）。范围为 4 至 8044176 千字节。
- **要保留的最小可用空间 (KB)** - 指定要在闪存中保留的最小可用空间（以 KB 为单位）。范围为 0 至 8044176 千字节。

步骤 7 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

启用日志记录目标

必须启用日志记录目标才能查看该目标的消息。启用目标时，还必须为该目标指定消息过滤器。

提示 如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则大多数FTD平台设置不适用于这些消息。请参阅适用于安全事件系统日志消息的 威胁防御 平台设置，第 651 页。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**系统日志** > **日志记录目标**。

步骤 3 点击**添加**以启用目标并应用日志记录过滤器，或编辑现有目标。

步骤 4 在**日志记录目标**对话框中，选择目标并配置用于目标的过滤器：

a) 在**日志记录目标**下拉列表中，选择要启用的目标。您可以为每个目标创建一个过滤器：控制台、邮件、内部缓冲区、SNMP 陷阱、SSH 会话和系统日志服务器。

注释 控制台和 SSH 会话日志记录只有在诊断 CLI 中工作。输入 **system support diagnostic-cli**。

b) 在**事件类**中，选择将应用于表中未列出的所有类的过滤器。

您可以配置这些过滤器：

- **基于严重性过滤** - 选择严重性级别。此级别或更高级别的消息将会发送到目标
- **使用事件列表** - 选择定义过滤器的事件列表。在**事件列表 (Event Lists)** 页面上创建这些列表。

- **禁用日志记录** - 阻止消息发送到此目标。

c) 如果要为每个事件类创建过滤器，请点击**添加**以创建新过滤器，或编辑现有过滤器，然后选择事件类和严重性级别以限制该类中的消息。点击**确定**以保存过滤器。

有关事件类的说明，请参阅系统日志消息类，第 646 页。

d) 点击**确定**。

步骤 5 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

将系统日志消息发送给邮件消息

您可以设置以邮件形式发送的系统日志消息收件人列表。

提示 如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则大多数 FTD 平台设置不适用于这些消息。请参阅适用于安全事件系统日志消息的 威胁防御 平台设置，第 651 页。

开始之前

- 在 SMTP 服务器平台设置页面上配置 SMTP 服务器
- 启用日志记录并配置基本设置，第 652 页
- 启用日志记录目标

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**系统日志** > **邮件设置**。

步骤 3 指定用作以邮件形式发送的系统日志消息的源地址的邮件地址。

步骤 4 点击 **Add** 以输入指定的系统日志消息的新邮件地址收件人。

步骤 5 从下拉列表中选择发送给收件人的系统日志消息的严重性级别。

用于目标邮件地址的系统日志消息严重性过滤器会导致发送指定严重性级别和更高严重性级别的消息。有关级别的信息，请参阅严重性级别，第 645 页。

步骤 6 点击**确定 (OK)**。

步骤 7 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

创建自定义事件列表

事件列表是一个自定义筛选器，您可以将其应用于日志记录目标，以控制将哪些消息发送到目标。通常，只根据严重性来筛选目标消息，但可以使用事件列表根据事件类、严重性和消息标识符 (ID) 组合进一步控制要发送的消息。

创建自定义事件列表分为两步。在**事件列表 (Event Lists)** 中创建自定义列表，然后使用事件列表在**日志记录目标 (Logging Destinations)** 中为各种类型的目标定义日志记录筛选。

提示 如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则大多数 FTD 平台设置不适用于这些消息。请参阅适用于安全事件系统日志消息的 威胁防御 平台设置，第 651 页。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**系统日志** > **事件列表**。

步骤 3 配置事件列表。

a) 点击**添加**以添加新列表或编辑现有列表。

b) 在**名称**字段中输入事件列表的名称。不允许使用空格。

c) 要根据严重性或事件类来标识消息，请选择**严重性/事件类**选项卡，并添加或编辑条目。

有关可用类的信息，请参阅系统日志消息类，第 646 页。

有关级别的信息，请参阅严重性级别，第 645 页。

某些事件类在透明模式下不适用于该设备。如果配置了此类选项，将绕过这些选项，不予以部署。

d) 若要通过消息 ID 明确标识消息，请选择**消息 ID (Message ID)**，并添加或编辑 ID。

您可以使用连字符输入 ID 范围，例如 100000-200000。ID 是六位数字。有关初始三位数字如何映射到功能的信息，请参阅系统日志消息类，第 646 页。

有关特定的消息编号，请参阅 Cisco ASA 系列日志消息。

e) 点击**确定**保存事件列表。

步骤 4 点击**日志记录目标 (Logging Destinations)**，然后添加或编辑应使用过滤器的目标。

请参阅启用日志记录目标，第 653 页。

步骤 5 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

限制系统日志消息生成速率

您可以限制按严重性级别或消息ID生成系统日志消息的速率。您可以为每个日志记录级别和每个系统日志消息 ID 指定单独的限制。如果设置冲突，则会优先考虑系统日志消息 ID 限制。

提示 如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则大多数FTD平台设置不适用于这些消息。请参阅适用于安全事件系统日志消息的 威胁防御 平台设置，第 651 页。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**系统日志** > **速率限制**。

步骤 3 要按严重性级别限制邮件生成，请点击**日志记录级别 (Logging Level)** > **添加 (Add)**，然后配置以下选项：

- **日志记录级别** - 您要限制速率的严重性级别。有关级别的信息，请参阅严重性级别，第 645 页。
- **消息数** - 在指定时间段内允许的指定类型的最大消息数。
- **间隔** - 在速率限制计数器重置之前的秒数。

步骤 4 点击**确定**。

步骤 5 要按系统日志消息 ID 限制邮件生成，请点击**系统日志级别 (Syslog Level)** > **添加 (Add)**，然后配置以下选项：

- **系统日志 ID** - 您要限制速率的系统日志消息 ID。有关特定消息编号，请参阅思科 ASA 系列系统日志消息。
- **消息数** - 在指定时间段内允许的指定类型的最大消息数。
- **间隔** - 在速率限制计数器重置之前的秒数。

步骤 6 点击**确定 (OK)**。

步骤 7 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置系统日志设置

可以配置一般系统日志设置，以设置要包括在将被发送到系统日志服务器的系统日志消息中的设备代码；指定是否在每条消息中包括时间戳；指定是否将设备ID包括在消息中；查看和修改消息的严重性级别；以及禁用特定消息的生成。

如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则此页面上的某些设置不适用于这些消息。另请参阅《Cisco Secure Firewall Management Center 管理指南》中的适用于安全事件系统日志消息的威胁防御平台设置。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 依次选择**系统日志** > **系统日志设置**。

步骤 3 在**设备**下拉列表中为系统日志服务器选择要用作文件消息基础的系统日志设备。

默认值为大多数 UNIX 系统期望的 LOCAL4(20)。但是，由于网络设备共享可用设备，因此可能需要为系统日志更改此值。

设施值通常与安全事件无关。

步骤 4 选中**在每个系统日志消息上启用时间戳**复选框, 以包括在系统日志消息中生成消息的日期和时间。

步骤 5 选择系统日志消息的**时间戳格式**：

- 传统 (MMM dd yyyy HH:mm:ss) 格式为系统日志消息的默认格式。

  选择此时间戳格式时，消息不会指示时区，该时区始终为 UTC。

- RFC 5424 (yyyy-MM-ddTHH:mm:ssZ) 使用 RFC 5424 系统日志格式中指定的 ISO 8601 时间戳格式。

  如果选择RFC 5424格式，则会在每个时间戳的末尾附加“Z”，以指示时间戳使用UTC时区。

步骤 6 如果希望向系统日志消息添加设备标识符（它将被放置在消息的开头），则请选中**启用系统日志设备 ID** 复选框，然后选择 ID 的类型。

- **接口** - 使用所选接口的 IP 地址，无论设备通过哪个接口发送消息。选择标识接口的安全区。该区域必须映射到某一接口。
- **用户定义的 ID** - 使用所选的文本字符串（最多 16 个字符）。
- **主机名** - 使用设备的主机名。

步骤 7 使用“系统日志消息”表来更改特定系统日志消息的默认设置。仅当希望更改默认设置时，才需要此表中的配置规则。可以更改分配给消息的严重性，或者可以禁用消息的生成。

默认情况下，将启用 Netflow，并在表中显示条目。

a) 要抑制因 Netflow 而冗余的系统日志消息，请选择 **Netflow 等效系统日志**。

这会将消息作为受抑制的消息添加到该表中。

注释 如果其中任何等效系统日志已经位于该表中，则不会覆盖现有规则。

b) 要添加新规则，请点击**添加 (Add)**。

c) 如果希望更改所选消息编号的配置，则请进入**系统日志 ID** 下拉列表，然后从**日志记录级别**下拉列表中选择新的严重性级别，或者选择**已抑制**以禁用消息的生成。通常不会更改严重性级别并禁用消息，但如果需要，可以对这两个字段进行更改。

d) 点击**确定**以将规则添加到该表中。

步骤 8 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

下一步做什么

- 部署配置更改。

配置系统日志服务器

要配置系统日志服务器，以处理您的系统生成的消息，请执行以下步骤。

如果您希望此系统日志服务器接收连接和入侵事件等安全事件，另请参阅适用于安全事件系统日志消息的 威胁防御 平台设置，第 651 页。

开始之前

- 请参阅日志记录准则，第 649 页中的要求。
- 请确保您的设备可以通过网络访问您的系统日志收集器。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 依次选择**系统日志** > **系统日志服务器**。

步骤 3 如果任何使用 TCP 协议的系统日志服务器关闭，则请选中**在系统日志服务器关闭时允许用户流量传递**复选框，以允许流量。

步骤 4 在**消息队列大小（消息）(Message queue size [messages])** 字段中输入当系统日志服务器繁忙时安全应用上用于存储系统日志消息的队列的大小。最小值为 1 条消息。默认值为 512。指定 0 可允许不限数量的消息排队（受可用块内存约束）。

当消息超过配置的队列大小时，它们会被丢弃并导致系统日志丢失。要确定理想的队列大小，您需要确定可用的块内存。使用 **show blocks** 命令了解当前内存使用率。有关命令及其属性的详细信息，请参阅《*Cisco Secure Firewall ASA* 系列命令参考指南》。如需进一步帮助，请与思科 TAC 联系。

步骤 5 点击 **Add** 以添加新系统日志服务器。

a) 在 **IP 地址**下拉列表中，选择包含系统日志服务器 IP 地址的网络主机对象。

b) 选择协议（TCP 或 UDP），然后输入用于 威胁防御设备与系统日志服务器之间通信的端口号。

UDP 比 TCP 更快，并且在设备上使用的资源更少。

默认 UDP 端口为 514。您必须为 TCP 手动配置端口 1470。任一协议的有效非默认端口值为 1025 至 65535。

c) 选中 **Log messages in Cisco EMBLEM format (UDP only)** 复选框以指定是否记录思科 EMBLEM 格式的消息（仅在选择 UDP 作为协议的情况下才可用）。

注释 RFC5424格式的系统日志消息通常显示优先级值（PRI）。但是，在管理中心中，只有当您启用Cisco EMBLEM格式的日志记录时，才会显示受管 威胁防御 的系统日志消息中的PRI值。有关PRI的详细信息，请参阅RFC5424。

d) 选中**启用安全系统日志**复选框，以使用SSL/TLS over TCP对设备与服务器之间的连接进行加密。

注释 必须选择TCP作为协议才能使用此选项。还必须在 **设备** > **证书** 页面上上传与系统日志服务器通信所需的证书。最后，将该证书从威胁防御设备上传到系统日志服务器，以完成安全关系，并允许其对流量进行解密。设备管理界面不支持 **启用安全系统日志** 选项。

e) 选择**设备管理接口**或**安全区域或指定接口**，以与系统日志服务器通信。

- **设备管理接口**：从管理接口发送系统日志。 我们建议您在配置Snort事件的系统日志时使用此选项。

  注释 **设备管理界面** 选项不支持 **启用安全系统日志** 选项。

- **安全区域或指定接口**：从**可用区域**列表中选择接口，然后点击**添加**。

f) 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

下一步做什么

- 部署配置更改。

配置全局超时

可以设置各种协议的连接和转换插槽的全局空闲超时持续时间。如果插槽在指定的空闲时间内未使用，资源将返回到空闲池。

还可以为设备的控制台会话设置超时。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**超时**。

步骤 3 配置要更改的超时。

对于任何给定的设置，请选择**自定义**来定义您自己的值，选择**默认**将恢复系统默认值。在大多数情况下，最大超时为1193小时。

您可以通过选择**禁用**来禁用某些超时。

- **控制台超时** - 关闭到控制台的连接之前的空闲时间，范围为0 或 5 到 1440 分钟。默认超时时间为 0，表示会话不会超时。如果更改该值，现有的控制台会话将使用原来的超时值。新值仅适用于新连接。
- **转换插槽** - NAT 转换插槽释放前的空闲时间。此持续时间必须为至少 1 分钟。默认值为 3 小时。
- **连接** - 连接插槽释放前的空闲时间。此持续时间必须为至少 5 分钟。默认值为 1 小时。
- **半封闭** - TCP 半闭合连接关闭前的空闲时间。如果同时收到 FIN 和 FIN-ACK，则连接会被认为是半关闭的。如果只看到了 FIN，则常规连接超时适用。最小值为 30 秒。默认值为 10 分钟。
- **UDP** - UDP 连接关闭前的空闲时间。此持续时间必须为至少 1 分钟。默认值为 2 分钟。
- **ICMP** - 通用 ICMP 状态关闭前的空闲时间。默认值（及最小值）是 2 秒。
- **RPC/Sun RPC** - SunRPC 插槽释放前的空闲时间。此持续时间必须为至少 1 分钟。默认值为 10 分钟。

  在基于 Sun RPC 的连接中，当父连接被删除或出现超时时，新的子连接可能不会被视为父-子连接的一部分，因此可以根据策略或系统中设置的规则来评估新的连接。父连接超时后，现有的子连接仅在达到超时值集之前有效。
- **H.225** - H.225 信令连接关闭前的空闲时间。默认值为 1 小时。若要在清除所有调用后立即关闭连接，建议使用超时值 1 秒 (0:0:1)。
- **H.323** - TH.245 (TCP) 和 H.323 (UDP) 媒体连接关闭前的空闲时间。默认值（和最小值）为 5 分钟。由于 H.245 和 H.323 媒体连接上设置的连接标志相同，因此 H.245 (TCP) 连接与 H.323（RTP 和 RTCP）媒体连接共享空闲超时。
- **SIP** - SIP 信令端口连接关闭前的空闲时间。此持续时间必须为至少 5 分钟。默认值为 30 分钟。
- **SIP 媒体** - SIP 媒体端口连接关闭前的空闲时间。此持续时间必须为至少 1 分钟。默认值为 2 分钟。SIP 媒体计时器用于具有 SIP UDP 媒体数据包的 SIP RTP/RTCP，而不是 UDP 非活动超时。
- **SIP 断开连接** - 在 CANCEL 或 BYE 消息未收到 200 OK 的情况下，SIP 会话删除之前的空闲时间，该值介于 0:0:1 至 00:10:0 之间。默认值为 2 分钟 (0:2:0)。
- **SIP 邀请** - PROVISIONAL 响应和媒体转换的针孔关闭前的空闲时间，该值介于 0:1:0 至 00:30:0 之间。默认值为 3 分钟 (0:3:0)。
- **SIP 临时媒体** - SIP 临时媒体连接的超时值，该值介于 1 至 30 分钟之间。默认值为 2 分钟。
- **Floating Connection** - 当某个网络存在具有不同指标的多个路由时，系统会使用连接创建时指标最佳的路由。如果有更好的路由变得可用，则此超时可让连接关闭，以便使用更好的路由重新建立连接。默认值为 0（连接永不超时）。为了可以使用更好的路由，请将超时设置为 0:0:30 至 1193:0:0 之间的值。
- **Xlate PAT** - PAT 转换插槽释放前的空闲时间，该值介于 0:0:30 至 0:5:0 之间。默认值为 30 秒。如果上游路由器拒绝使用释放的 PAT 端口的新连接，您可能会想要增加超时，因为以前的连接在上游设备中可能仍处于开放状态。

- **TCP 代理重组** - 等待重组的缓冲数据包丢弃前的空闲时间，该值介于 0:0:10 到 1193:0:0 之间。默认值为 1 分钟 (0:1:0)。
- **ARP 超时** - ARP 表重建之间的秒数，从 60 到 4294967。默认值为 14,400 秒（4 小时）。

步骤 4 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

为威胁防御配置 NTP 时间同步

使用网络时间协议 (NTP) 服务器同步设备上的时钟设置。建议您将 管理中心 托管的所有 威胁防御 配置为使用同一台 NTP 服务器作为 管理中心。威胁防御 直接从配置的NTP服务器获取时间。如果 威胁防御 配置的NTP服务器由于任何原因无法访问，则会与 管理中心 同步时间。

设备支持 NTPv4。

注释 如果要在 Firepower 4100/9300 机箱上部署 威胁防御，则必须在 Firepower 4100/9300 机箱上配置 NTP，以便智能许可正常运行，并确保设备注册采用正确的时间戳。对于 Firepower 4100/9300 机箱和 管理中心，应使用相同的 NTP 服务器。

开始之前

- 如果您的组织有 威胁防御 可以访问的一个或多个NTP服务器，请在 管理中心 上的**系统 (System)** > **配置 (Configuration)** 页面上为已为时间同步配置的设备使用相同的 NTP 服务器。
- 如果您选择了**仅当为配置 NTP 服务器**管理中心时使用仅通过身份验证的NTP服务器管理中心，则对于您的设备，仅使用配置为通过进行身份验证的NTP服务器。（托管设备将使用与管理中心 相同的 NTP 服务器，但其 NTP 连接将不使用身份验证。）
- 如果您的设备无法访问 NTP 服务器或您的组织没有 NTP 服务器，则必须使用以下程序中讨论的**通过防御中心通过 NTP** 选项。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略。

步骤 2 选择**时间同步 (Time Synchronization)**。

步骤 3 配置以下时钟选项之一：

- **通过 NTP 从防御中心** -（默认）。托管设备从为 管理中心 配置的 NTP 服务器（经过身份验证的 NTP 服务器除外）获取时间，并直接与这些服务器同步时间。但是，如果满足以下任一条件，则托管设备将从 管理中心 同步时间：

- 设备无法访问 管理中心 的 NTP 服务器。
- 管理中心 没有未经身份验证的服务器。

- **通过网络上的 NTP (Via NTP from)**：如果您的 管理中心使用的是网络上的 NTP 服务器，请选择此选项，并输入您在**系统 (System) > 配置 (Configuration) > 时间同步 (Time Synchronization)** 中指定的同一 NTP 服务器的完全限定 DNS 名称（例如 ntp.example.com）或 IPv4 或 IPv6 地址。如果无法访问 NTP 服务器，则 管理中心将充当 NTP 服务器。

步骤 4 点击**保存 (Save)**。

下一步做什么

- 部署配置更改。

为策略应用配置设备时区

默认情况下，系统使用 UTC 时区。要为设备指定不同的时区，请使用此程序。

您指定的时区将仅用于支持此功能的策略中基于时间的策略应用。

注释 从 FMC 7.0 开始，Snort 3 也支持基于时间的 ACL。

过程

步骤 1 依次选择**设备 (Devices)** > **平台设置 (Platform Settings)**，并创建或编辑 威胁防御 策略。

您还可以从 **对象 >对象管理 > 时区** 页面创建时区对象。

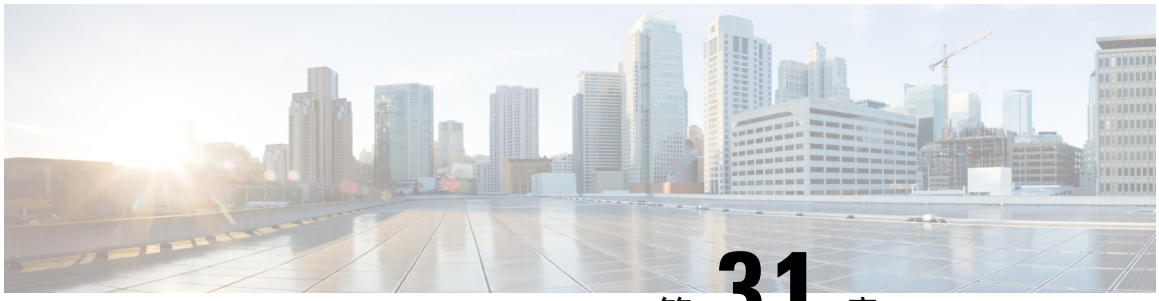
步骤 2 通过点击 +创建新的时区对象。

步骤 3 选择时区。

步骤 4 点击**保存**。

下一步做什么

- 创建时间范围对象，在访问控制和预过滤器规则中选择适用的时间范围，并将父策略分配给与正确时区关联的设备。
- 部署配置更改。



第 31 章

网络地址转换

以下主题介绍网络地址转换 (NAT) 以及在 威胁防御设备上配置网络地址转换的方法。

为何使用 NAT？

IP 网络中的每台计算机和设备都分配了标识主机的唯一 IP 地址。因为缺乏公用 IPv4 地址，所以这些 IP 地址中的大多数都是专用地址，在专用公司网络以外的任何地方都不可路由。RFC 1918 定义可以在内部使用但不应通告的专用 IP 地址：

- 10.0.0.0 到 10.255.255.255
- 172.16.0.0 至 172.31.255.255
- 192.168.0.0 到 192.168.255.255

NAT 的主要功能之一是使专用 IP 网络可以连接到互联网。NAT 用公用 IP 地址替换专用 IP 地址，将内部专用网络中的专用地址转换为可在公用互联网上使用的合法可路由地址。NAT 以此方式保存公用地址，因为它可配置为至少仅将整个网络的一个公用地址向外界通告。

NAT 的其他功能包括：

- 安全 - 隐藏内部 IP 地址可以阻止直接攻击。
- IP 路由解决方案 - 使用 NAT 时不会出现重叠 IP 地址。

- 灵活性 - 可以更改内部 IP 寻址方案，而不影响外部的可用公用地址；例如，对于可以访问互联网的服务器，可以维护供互联网使用的固定 IP 地址，但在内部，可以更改服务器地址。
- 在 IPv4 和 IPv6 之间转换（仅路由模式）- 如果想将 IPv6 网络连接到 IPv4 网络，可以利用 NAT 在两种类型的地址之间转换。

注释 不需要 NAT。如果不为一组给定流量配置 NAT，将不转换这些流量，但会正常应用所有安全策略。

NAT 基础知识

以下主题介绍一些 NAT 基础知识。

NAT 术语

本文档使用以下术语：

- 实际地址/主机/网络/接口 - 实际地址是指在主机上定义的转换前地址。在内部网络访问外部网络时，要转换内部网络的典型 NAT 场景中，内部网络会成为“实际”网络。请注意，您可以转换连接到设备的任何网络，而不是只在网络内部转换。因此，如果配置 NAT 以转换外部地址，“实际”可以是指访问内部网络时的外部网络。
- 映射地址/主机/网络/接口 - 映射地址是指实际地址转换而成的地址。在内部网络访问外部网络时，要转换内部网络的典型 NAT 场景中，外部网络会成为“映射”网络。

注释 在地址转换过程中，不会转换为设备接口配置的 IP 地址。

- 双向发起 - 静态 NAT 允许双向发起连接，意味着可发起到主机的连接和从主机发起连接。
- 源 NAT 和目的 NAT - 对于任何给定数据包，将源 IP 地址和目标 IP 地址与 NAT 规则进行比较，转换/不转换一个或两个地址。对于静态 NAT，规则是双向的，因此，请注意，这整个指南中命令和说明中使用的“源”和“目标”，即便是给定的连接，也可能源自“目标”地址。

NAT 类型

可以使用以下方法实施 NAT：

- 动态 NAT - 按先到先得的方式，将一组实际 IP 地址映射到一组映射 IP 地址（通常较小）。仅实际主机可以发起流量。请参阅动态 NAT，第 685 页。
- 动态端口地址转换 (PAT) - 使用 IP 地址的唯一源端口，将一组实际 IP 地址映射到单一 IP 地址。请参阅动态 PAT，第 690 页。

- 静态 NAT - 实际 IP 地址和映射 IP 地址之间的一致映射。允许发起双向流量。请参阅静态 NAT，第 699 页。
- 身份 NAT - 系统将实际地址静态转换为其本身，基本绕过 NAT。当您想转换一大组地址，但又想豁免一小部分地址时，可能就要这样配置 NAT。请参阅身份 NAT，第 707 页。

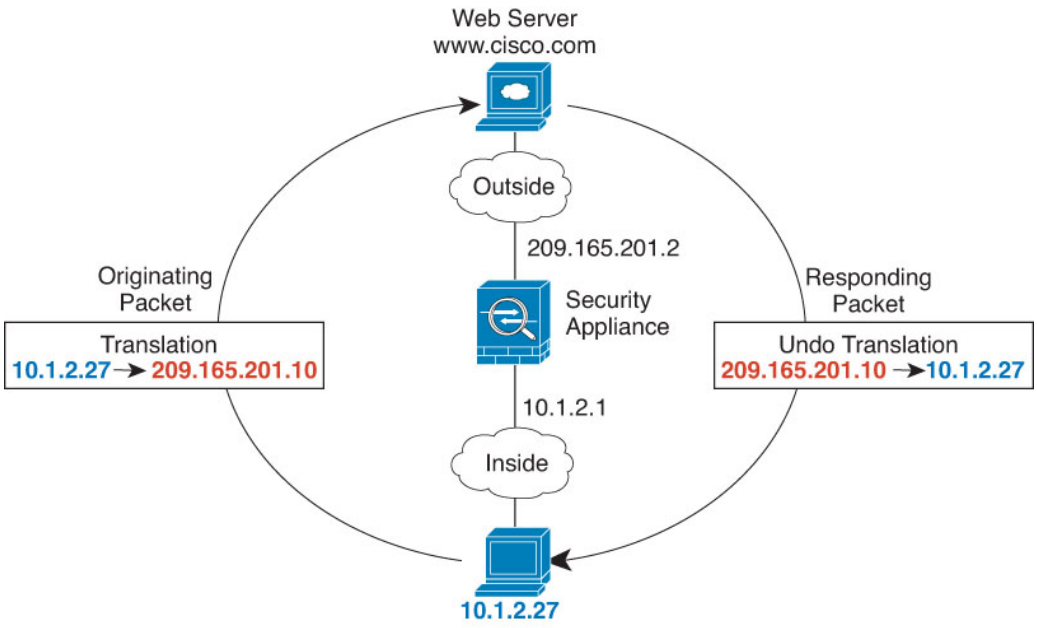
路由和透明防火墙模式下的 NAT

可以在路由和透明防火墙模式下配置 NAT。您不能为在内联、内联分流或被动模式下工作的接口配置 NAT。以下部分介绍每种防火墙模式的典型用法。

路由模式下的 NAT

下图显示路由模式下的一个典型 NAT 示例，专用网络位于内部。

图 *100: NAT* 示例：路由模式



1. 当位于 10.1.2.27 的内部主机向 Web 服务器发送数据包时，数据包的实际源地址 10.1.2.27 会转换为映射地址 209.165.201.10。
2. 当服务器响应时，它会将响应发送到映射地址 209.165.201.10，威胁防御设备 接收数据包，因为威胁防御设备 执行代理 ARP 以认领数据包。
3. 接下来，威胁防御设备 变更从映射地址 209.165.201.10 回到实际地址 10.1.2.27 的转换，然后再发送到主机。

透明模式下或桥接组内的 NAT

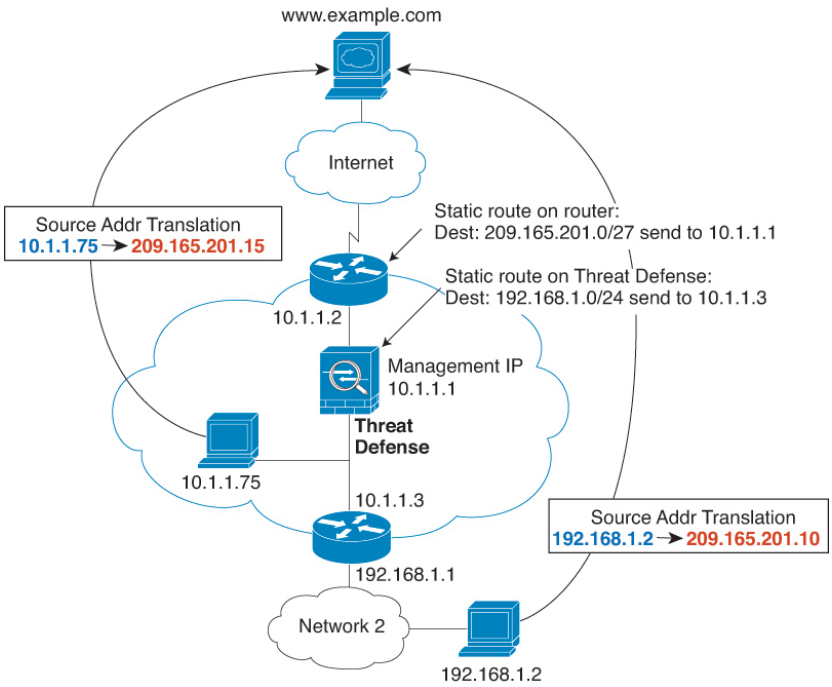
在透明模式下使用NAT可以消除上游或下游路由器为其网络执行NAT的需求。在路由模式下，NAT可以执行与桥接组内类似的功能。

透明模式下的 NAT或在路由模式下同一桥接组的成员之间具有以下要求和局限性：

- 当映射地址是桥接组成员接口时，不能配置接口 PAT，因为没有 IP 地址连接到该接口。
- 不支持 ARP 检测。此外，如果由于某种原因，威胁防御 一端的主机向 威胁防御 另一端的主机发送 ARP 请求，而且发起主机实际地址被映射到同一子网的不同地址，则实际地址在 ARP 请求中依然可见。
- 不支持在 IPv4 和 IPv6 网络之间进行转换。支持在两个 IPv6 网络之间或两个 IPv4 网络之间进行转换。

下图显示透明模式下的典型NAT场景，内部接口和外部接口上的网络相同。在此场景中，透明防火墙执行 NAT 服务，因此上游路由器不必执行 NAT。

图 *101: NAT* 示例：透明模式



1. 当位于 10.1.1.75 的内部主机将数据包发送到 Web 服务器时，数据包的实际源地址 10.1.1.75 被更改为映射地址 209.165.201.15。
2. 当服务器响应时，它将响应发送到映射地址 209.165.201.15，威胁防御 接收数据包，因为上游路由器将此映射网络包含在定向到 威胁防御 管理 IP 地址的静态路由中。
3. 然后，威胁防御 取消映射地址 209.165.201.15 回到实际地址 10.1.1.1.75 的转换。因为实际地址是直接连接的，所以 威胁防御 将实际地址直接发送到主机。

4. 对于主机 192.168.1.2，发生相同流程，但返回流量除外，威胁防御 在其路由表中查询路由，根据 192.168.1.0/24 的 威胁防御 静态路由，将数据包发送到位于 10.1.1.3 的下游路由器。

自动 NAT 和手动 NAT

可以通过以下两种方法实施地址转换：自动 *NAT* 和手动 *NAT*。

我们建议使用自动 NAT，除非您需要手动 NAT 提供的额外功能。自动 NAT 更容易配置，而且可能对应用（例如 IP 语音 [VoIP]）更加可靠。（对于 VoIP，对不属于规则中使用的任何对象的间接地址进行转换可能会失败。）

自动 NAT

配置为网络对象参数的所有 NAT 规则都被视为自动 *NAT* 规则。这是一种为网络对象配置 NAT 的快捷方法。但是，您无法为对象组创建这些规则。

尽管这些规则配置为对象的一部分，但是您通过对象管理器无法看到对象定义中的 NAT 配置。

当数据包进入接口时，系统会根据自动 NAT 规则来检查源和目标 IP 地址。如果进行独立匹配，可根据独立规则转换数据包中的源地址和目标地址。这些规则互不牵连，可以根据流量使用不同的规则组合。

因为规则从未配对，所以不能指定源 A/目的 A 应当有不同于源 A/目的 B 的转换。手动 NAT 用于实现这样的功能：您可以识别单个规则中的源和目标地址。

手动 NAT

手动 NAT 供您在单个规则中同时标识源和目标地址。同时指定源和目标地址，可以让您指定源 A/目的 A 有不同于源 A/目的 B 的转换。

注释 对于静态 NAT，规则是双向的，因此，请注意，这整个指南中命令和说明中使用的“源”和“目标”，即便是给定的连接，也可能源自“目标”地址。例如，如果配置支持端口地址转换的静态 NAT，然后将源地址指定为某台 Telnet 服务器，并且希望进入该 Telnet 服务器的所有流量都将端口从 2323 转换为 23，那么您就必须指定要转换的源端口（实际端口：23，映射端口：2323）。必须指定源端口是因为您已将 Telnet 服务器地址指定为源地址。

目标地址是可选的。如果指定目标地址，可以将其映射到其本身（身份 NAT），也可以将其映射到不同的地址。目的映射始终是静态映射。

比较自动 NAT 和手动 NAT

这两类 NAT 之间的主要差异是：

- 定义实际地址的方法。
  - 自动 NAT - NAT 规则成为网络对象的参数。网络对象 IP 地址用作原始（实际）地址。

- 手动 NAT- 标识实际地址和映射地址的网络对象或网络对象组。在这种情况下，NAT 不是网络对象的参数；网络对象或组是NAT配置的参数。能够使用实际地址的网络对象组意味着手动 NAT 更具可扩展性。

- 实施源和目标 NAT 的方法。
  - 自动 NAT- 每个规则都可应用到数据包的源或目标。因此，可能使用两条规则，一条用于源IP地址，一条用于目标IP地址。这两条规则不能绑在一起对源/目的组合进行特定转换。
  - 手动 NAT- 单一规则可以同时转换源和目标。数据包仅匹配一条规则，且不再检查其他规则。即使您不配置可选目标地址，匹配的数据包仍仅匹配一个 手动 NAT 规则。源和目的绑在一起，使您可以根据源/目的组合进行不同的转换。例如，源 A/目的 A 可以有不同于源 A/目的 B 的转换。

- NAT 规则顺序。
  - 自动 NAT- 在 NAT 表中自动排序。
  - 手动 NAT - 在 NAT 表中手动排序（在自动 NAT 规则之前或之后）。

NAT 规则顺序

自动 NAT 和手动 NAT 规则存储在分为三个部分的单个表中。首先应用第一部分规则，其次是第二部分，最后是第三部分，直到找到匹配项为止。例如，如果在第一部分找到匹配项，则不评估第二部分和第三部分。下表显示每个部分的规则顺序。

表 *75: NAT* 规则表

表部分	规则类型	部分中的规则顺序
第 1 部分	手动 NAT	系统按照在配置中出现的顺序应用第一个匹配的规则。因为会应用第一个匹配规则，所以必须确保具体规则位于更加通用的规则前面，否则无法按预期应用特定规则。默认情况下，手动 NAT 规则会添加到第 1 部分。 “具体规则优先”是指： • 静态规则应放在动态规则前面。 • 包含目的地转换的规则应仅放在具有源转换的规则前面。 如果无法消除重叠规则（其中可能有多个规则基于源或目标地址而应用），请特别注意遵循这些建议。

表部分	规则类型	部分中的规则顺序
第 2 部分	自动 NAT	如果在第 1 部分未找到匹配项，则会按照以下顺序应用第 2 部分的规则： **1.** 静态规则。 **2.** 动态规则。 **在每个规则类型中，遵循以下排序准则：** **1.** 实际 IP 地址数量 - 从最小到最大。例如，带一个地址的对象将在带 10 个地址的对象之前进行评估。 **2.** 如果数量相同，则按从最低到最高的顺序使用 IP 地址编号。例如，10.1.1.0 在 11.1.1.0 之前进行评估。 **3.** 如果使用同一 IP 地址，则按字母数字顺序使用网络对象名称。例如，abracadabra 在 catwoman 之前进行评估。
第 3 部分	手动 NAT	如果仍未找到匹配项，则按照在配置中出现的顺序，应用第三部分规则的第一个匹配项。此部分应当包含最通用的规则。还必须确保此部分的特定规则位于通用规则之前，否则会应用通用规则。

例如，对于第二部分规则，在网络对象中定义以下 IP 地址：

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

结果排序可能是：

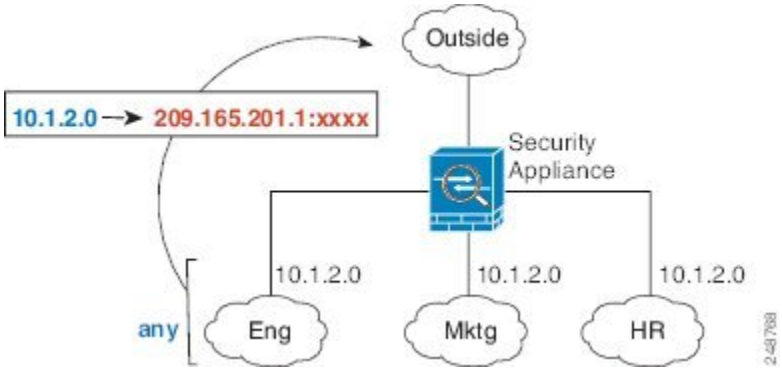
- 192.168.1.1/32（静态）
- 10.1.1.0/24（静态）
- 192.168.1.0/24（静态）
- 172.16.1.0/24（动态）（对象 abc）
- 172.16.1.0/24（动态）（对象 def）
- 192.168.1.0/24（动态）

NAT 接口

除了网桥组成员接口，您可以将NAT规则配置为应用到任何接口（也就是，所有接口），或者也可以标识特定的实际接口和映射接口。还可以为实际地址指定任何接口，为映射地址指定特定接口，反之亦然。

例如，如果在多个接口上使用相同的专用地址，并且在访问外部接口时要将这些地址全部转换到同一全局池，则可能要为实际地址指定任何接口，并且为映射地址指定外部接口。

图 *102:* 指定任何接口



然而，“任何”接口的概念不适用于网桥组成员接口。当指定“任何”接口时，NAT 将排除所有网桥组成员接口。因此，要将NAT应用于网桥组成员，必须指定成员接口。这样可能导致有许多只有一个接口不同的类似规则。您不能为桥接虚拟接口(BVI)本身配置NAT，只能为成员接口配置NAT。

注释 您不能为在内联、内联分流或被动模式下工作的接口配置 NAT。在指定接口时，请通过选择包含该接口的接口对象间接指定。

为 NAT 配置路由

威胁防御 设备需要成为发送到转换（映射）地址的所有数据包的目标。

在发送数据包时，设备使用目标接口（如果指定了接口）或路由表查找（如果未指定接口）来确定出口接口。对于身份 NAT，即使指定了目标接口，您也可以选择使用路由查找。

所需的路由配置类型取决于映射地址的类型，以下主题对此进行了说明。

地址与映射接口在相同的网络中

如果使用与目标（映射）接口在同一网络中的地址，威胁防御设备使用代理ARP应答映射地址的任何 ARP 请求，从而拦截发往映射地址的流量。此解决方案可以简化路由，因为 威胁防御设备 不必成为任何其他网络的网关。如果外部网络包含足够多的空闲地址，并且您正在使用 1:1 转换（例如动态 NAT 或静态 NAT），此解决方案是理想选择。动态 PAT 可显著增加您可以通过少量地址实现的转换数量，因此即使外部网络中的可用地址较少，依然可以使用此方法。对于 PAT，甚至可以使用映射接口的 IP 地址。

注释 如果将映射接口配置为任何接口，而且在与其中一个映射接口相同的网络中指定映射地址，那么如果从其他接口传入对此映射地址的 ARP 请求，则需要在入口接口上为该网络手动配置 ARP 条目，并指定其 MAC 地址。通常，如果该映射接口指定任何接口，则将唯一网络用于此映射地址，避免此类情况发生。在入口接口的**高级**设置中配置 ARP 表。

唯一网络中的地址

如果需要比目标（映射）接口网络上提供的地址更多的地址，则可以识别其他子网中的地址。上游路由器需要对指向 威胁防御设备 的映射地址进行静态路由。

或者，对于路由模式，可以将目标网络上的任何 IP 地址用作网关，为映射地址配置 威胁防御设备 上的静态路由，然后使用路由协议重新分配路由。例如，如果您将NAT用于内部网络(10.1.1.0/24)，并且使用映射 IP 地址 209.165.201.5，则可以为 10.1.1.99 网关配置 209.165.201.5 255.255.255.255（主机地址）的可重新分发静态路由。

对于透明模式，如果直接连接实际主机，则将上游路由器的静态路由配置为指向 威胁防御设备：，指定桥接组IP地址。对于透明模式下的远程主机，在上游路由器上的静态路由中，您也可以指定下游路由器 IP 地址。

与实际地址相同的地址（身份 NAT）

用于身份 NAT 的默认行为已启用代理 ARP，匹配其他静态 NAT 规则。如果需要，可以禁用代理 ARP。如果需要，还可以为常规静态NAT禁用代理ARP，在这种情况下，需要确保上游路由器上有适当的路由。

通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。例如，如果为“任何”IP 地址配置一条大体的身份 NAT 规则，则使代理 ARP 保持启用状态会给直接连接到映射接口的网络上的主机造成问题。在这种情况下，当映射网络上的主机要与同一网络上的其他主机通信时，ARP 请求中的地址匹配 NAT 规则（匹配“任何”地址）。然后，威胁防御设备 将代理地址的 ARP，即使数据包实际上不以 威胁防御设备 为目标。（请注意，即便已设置手动 NAT 规则，也会造成此问题；虽然NAT规则必须匹配源地址和目标地址，但仅会根据“源”地址作出代理ARP决定）。如果在实际主机 ARP 响应之前收到 威胁防御设备 ARP 响应，则流量会错误地发送到 威胁防御设备。

NAT 策略的要求和必备条件

支持的域

任意

用户角色

管理员

访问管理员

网络管理员

NAT 准则

以下主题提供有关实施 NAT 的详细准则。

NAT 防火墙模式指南

在路由和透明防火墙模式下支持 NAT。

不过，在桥接组成员接口（属于桥接组虚拟接口 [BVI] 的接口）上配置 NAT 具有以下局限性：

- 为网桥组的成员配置 NAT 时，需要指定成员接口。您不能为网桥组接口 (BVI) 本身配置 NAT。
- 在桥接组成员接口之间执行 NAT 时，必须指定实际地址和映射地址。不能指定“任意”作为接口。
- 当映射地址是桥接组成员接口时，不能配置接口 PAT，因为没有 IP 地址连接到该接口。
- 当源接口和目标接口是同一网桥组的成员时，不能在 IPv4 和 IPv6 网络 (NAT64/46) 之间进行转换。静态 NAT/PAT 44/66、动态 NAT44/66 和动态 PAT44 是唯一允许的方法；不支持动态 PAT66。但是，您可以在不同网桥组的成员之间，或在网桥组成员（源接口）和标准路由接口（目标接口）之间执行 NAT64/46。

注释 您不能为在内联、内联分流或被动模式下工作的接口配置 NAT。

IPv6 NAT 准则

NAT 支持 IPv6，但有以下准则和限制。

- 对于标准路由模式接口，您还可以在 IPv4 和 IPv6 之间进行转换。
- 对于同一个网桥组的成员接口，不能在 IPv4 和 IPv6 之间进行转换，而只能在两个 IPv6 或两个 IPv4 网络之间进行转换。此限制不适用于接口为不同网桥组成员或一个接口为网桥组成员，另一个为标准路由接口的情况。
- 在同属一个网桥组的接口之间进行转换时，不能将动态 PAT 用于 IPv6 (NAT66)。此限制不适用于接口为不同网桥组成员或一个接口为网桥组成员，另一个为标准路由接口的情况。
- 对于静态 NAT，可以指定一个最大 /64 的 IPv6 子网。不支持更大的子网。
- 将 FTP 和 NAT46 配合使用时，当 IPv4 FTP 客户端连接到 IPv6 FTP 服务器时，客户端必须使用扩展被动模式 (EPSV) 或扩展端口模式 (EPRT)；在使用 IPv6 时，不支持 PASV 和 PORT 命令。

IPv6 NAT 最佳实践

可以使用 NAT 在 IPv6 网络之间转换，以及在 IPv4 和 IPv6 网络之间转换（仅路由模式）。我们推荐以下最佳实践：

- NAT66（IPv6 对 IPv6）- 我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。如果不想允许返回流量，您可以启用单向静态 NAT 规则（仅限于手动 NAT）。
- NAT46（IPv4 对 IPv6）- 我们建议使用静态 NAT。因为 IPv6 地址空间远远大于 IPv4 地址空间，所以可以轻松满足静态转换需求。如果不想允许返回流量，您可以启用单向静态 NAT 规则（仅限于手动 NAT）。转换为 IPv6 子网（/96 或更低）时，默认情况下，生成的映射地址为有嵌入 IPv4 的 IPv6 地址，其中 32 位 IPv4 地址嵌入在 IPv6 前缀后面。例如，如果 IPv6 前缀为 /96 前缀，则 IPv4 地址附在最后的 32 位地址中。例如，如果将 192.168.1.0/24 映射到 201b::0/96，则 192.168.1.4 将被映射到 201b::0.192.168.1.4（通过混合表示法显示）。如果前缀较小（例如 /64），则 IPv4 地址附在前缀的后面，后缀 0 附在 IPv4 地址后面。或者，还能够以网络对网络的方式转换地址，其中第一个 IPv4 地址映射到第一个 IPv6 地址，第二个 IPv4 地址映射到第二个 IPv6，依次类推。
- NAT64（IPv6 到 IPv4）- 可能没有足够的 IPv4 地址来容纳大量的 IPv6 地址。我们建议使用动态 PAT 池提供大量的 IPv4 转换。

对检测到的协议的 NAT 支持

检测打开辅助连接或者在数据包中嵌入 IP 地址的一些应用层协议，以提供以下服务：

- 创建小孔 - 一些应用协议在标准端口或协商的端口上打开辅助 TCP 或 UDP 连接。检测会为这些辅助端口打开小孔，使您无需创建访问控制规则予以允许。
- NAT 重写 - 诸如 FTP 等协议会在数据包数据中嵌入用于辅助连接的 IP 地址和端口，作为协议的一部分。如果 NAT 转换涉及到任一终端，则检测引擎会重写数据包数据以反映嵌入式地址和端口的 NAT 转换。在没有 NAT 重写的情况下，辅助连接不起作用。
- 协议实施 - 一些检测会为检测到的协议实施某种程度的 RFC 一致性。

下表列出了应用 NAT 重写及其 NAT 限制的检测到的协议。当编写包括这些协议的 NAT 规则时，请记住这些限制。此处未列出的协议不应用 NAT 重写。这些检测包括 GTP、HTTP、IMAP、POP、SMTP、SSH 和 SSL。

注释 仅列出的端口支持 NAT 重写。对于其中某些协议，您可以使用网络分析策略将检测扩展到其他端口，但 NAT 重写不会扩展到这些端口。这包括 DCERPC、DNS、FTP 和 Sun RPC 检测。如果在非标准端口上使用这些协议，请勿对连接使用 NAT。

表 *76: NAT* 支持的应用检测

应用	检测到的协议、端口	NAT 限制	创建了小孔
DCERPC	TCP/135	无 NAT64。	是
DNS over UDP	UDP/53	无可用于通过 WINS 进行名称解析的 NAT 支持。	否
ESMTP	TCP/25	无 NAT64。	否
FTP	TCP/21	（集群）无静态 PAT。	是
H.323 H.225（呼叫信令） H.323 RAS	TCP/1720 UDP/1718 对于 RAS， 则为 UDP/1718-1719	（集群）无静态 PAT。 无扩展 PAT。 无 NAT64。	是
ICMP ICMP 错误	ICMP （从不会对定向到设备接口的 ICMP 流量进行检测。）	没有限制。	否
IP 选项	RSVP	无 NAT64。	否
NetBIOS Name Server over IP	UDP/137、138（源端口）	无扩展 PAT。 无 NAT64。	否
RSH	TCP/514	无 PAT。 无 NAT64。 （集群）无静态 PAT。	是
RTSP	TCP/554 （对于 HTTP 隐藏没有任何处理。）	无扩展 PAT。 无 NAT64。 （集群）无静态 PAT。	是
SIP	TCP/5060 UDP/5060	无扩展 PAT。 无 NAT64 或 NAT46。 （集群）无静态 PAT。	是
Skinny (SCCP)	TCP/2000	无扩展 PAT。 无 NAT64、NAT46 或 NAT66。 （集群）无静态 PAT。	是

应用	检测到的协议、端口	NAT 限制	创建了小孔
SQL*Net （版本 1、2）	TCP/1521	无扩展 PAT。 无 NAT64。 （集群）无静态 PAT。	是
Sun RPC	TCP/111 UDP/111	无扩展 PAT。 无 NAT64。	是
TFTP	UDP/69	无 NAT64。 （集群）无静态 PAT。 不转换负载 IP 地址。	是
XDMCP	UDP/177	无扩展 PAT。 无 NAT64。 （集群）无静态 PAT。	是

FQDN 目的准则

您可以使用完全限定域名 (FQDN) 网络对象而不是 IP 地址在手动 NAT 规则中指定转换（映射）目的。例如，您可以基于发往 www.example.com Web 服务器的流量创建规则。

使用 FQDN 时，系统基于返回的地址获取 DNS 解析并编写 NAT 规则。 如果使用多个 DNS 服务器组，则系统会使用过滤器域，并根据过滤器从相应的组请求地址。如果从 DNS 服务器获取多个地址，则使用的地址基于以下条件：

- 如果某个地址与指定接口位于相同的子网上，则使用该地址。如果没有地址位于相同的子网上，则使用返回的第一个地址。
- 转换后的源和转换后的目的的 IP 类型必须匹配。例如，如果转换后的源地址为 IPv6，则 FQDN 对象必须指定 IPv6 作为地址类型。如果转换后的源为 IPv4，则 FQDN 对象可以指定 IPv4 或 IPv4 和 IPv6。在这种情况下，将选择 IPv4 地址。

不能在用于手动 NAT 目的的网络组中包含 FQDN 对象。在 NAT 中，必须单独使用 FQDN 对象，因为只有单个目的主机才适用于此类 NAT 规则。

如果 FQDN 无法解析为 IP 地址，则在获得 DNS 解析之前该规则不起作用。

其他 NAT 准则

- 对于作为网桥组成员的接口，您需要为成员接口编写 NAT 规则。您无法为桥接虚拟接口 (BVI) 本身编写 NAT 规则。

- 您不能为站点间 VPN 中使用的虚拟隧道接口 (VTI) 编写 NAT 规则。为 VTI 的源接口编写规则不会将 NAT 应用于 VPN 隧道。要编写应用于 VTI 上通过隧道传输的 VPN 流量的 NAT 规则，您必须使用“任何”作为接口，而不能明确指定接口名称。
- （仅限于 自动 NAT。）您仅可为给定对象定义单个 NAT 规则，如果要为某个对象配置多个 NAT 规则，则需要创建通过不同名称指定同一 IP 地址的多个对象。
- 如果在接口上定义了 VPN，则接口上的入站 ESP 流量不受 NAT 规则的约束。系统仅允许已建立的 VPN 隧道的 ESP 流量，而丢弃与现有隧道不相关的流量。此限制适用于 ESP 和 UDP 端口 500 和 4500。
- 如果在应用动态 PAT 设备之后的某设备上定义站点间 VPN，以便 UDP 端口 500 和 4500 不是实际使用的端口，必须从 PAT 设备之后的设备发起连接。响应方无法发起安全关联 (SA)，因为不知道正确的端口号。
- 如果更改 NAT 配置，并且不想等待现有转换超时后再使用新 NAT 配置，则可以在设备 CLI 中使用 **clear xlate** 命令清除转换表。然而，清除转换表将断开使用转换的当前所有连接。

  如果创建应应用于现有连接（例如 VPN 隧道）的新 NAT 规则，则需要使用 **clear conn** 来终止连接。然后，尝试重新建立连接应符合 NAT 规则，且连接应正确进行 NAT。

注释 如果删除动态 NAT 或 PAT 规则，然后使用与已删除规则中地址重叠的映射地址添加新规则，则系统将不使用新规则，直至与已删除规则关联的所有连接超时，或已使用 **clear xlate** 或 **clear conn** 命令将这些连接清除。此保护措施确保相同的地址将不分配至多个主机。

- 不能使用同时包含 IPv4 和 IPv6 地址的对象组，对象组只能包括一种类型的地址。
- NAT 中使用的网络对象不能包含超过 131838 个 IP 地址，无论是显式还是隐式包含在地址或子网范围中。将地址空间分成更小的范围，并为较小的对象编写单独的规则。
- （仅限于手动 NAT。）在 NAT 规则中使用 **any** 作为源地址时，“任何”流量（IPv4 与 IPv6）的定义取决于规则。只有数据包为 IPv6 至 IPv6 或 IPv4 至 IPv4，威胁防御设备 才能对数据包执行 NAT；借助此前提条件，威胁防御设备 可确定 NAT 规则中的 **any** 的值。例如，如果配置从“任何”到 IPv6 服务器的规则，且该服务器已从 IPv4 地址映射，则**任何**指“任何 IPv6 流量”。如果配置从“任何”到“任何”的规则，并且将源映射至接口 IPv4 地址，则**任何**指“任何 IPv4 流量”，因为映射的接口地址意味着目标也是 IPv4。
- 可以在多条 NAT 规则中使用同一映射对象或组。
- 映射 IP 地址池不能包括：
  - 映射接口的 IP 地址。如果为该规则指定“任何”接口，则禁止所有接口 IP 地址。对于接口 PAT（仅路由模式），指定接口名称而不是接口地址。
  - 故障转移接口 IP 地址。
  - （透明模式。）管理 IP 地址。
  - （动态 NAT。）启用 VPN 时的备用接口 IP 地址。

- 避免在静态和动态 NAT 策略中使用重叠地址。例如，使用重叠地址，如果 PPTP 的辅助连接命中静态而非动态 xlate，将无法建立 PPTP 连接。
- 无法在 NAT 规则的源地址和远程访问 VPN 地址池中使用重叠地址。
- 如果在规则中指定目标接口，则该接口用作出口接口，而不是在路由表中查找路由。但是，对于身份 NAT，您可以选择改为使用路由查找。
- 如果对用于连接 NFS 服务器的 Sun RPC 流量使用 PAT，请注意，在通过 PAT 方式转换的端口号大于 1024 时，NFS 服务器可能会拒绝连接。NFS 服务器的默认配置是拒绝来自端口号大于 1024 的连接。错误通常为“权限被拒”。 如果不选择将保留端口 (1-1023) 包括在 PAT 池的端口范围内的选项，则系统会映射高于 1024 的端口。您可以通过将 NFS 服务器配置更改为允许所有端口号来避免此问题。
- NAT 仅适用于直通流量。系统生成的流量不进行 NAT。
- 请不要使用大写或小写字母的任意组合来命名网络对象或组 pat-pool。
- 单向选项主要用于测试目的，可能不适用于所有协议。例如，SIP 要求执行协议检查以使用 NAT 转换 SIP 报头，但如果将转换设为单向，则不会发生这种情况。
- 不能在协议无关组播 (PIM) 寄存器的内部负载上使用 NAT。
- (手动 NAT) 为双 ISP 接口设置（使用路由配置中的服务级别协议的主接口和备用接口）编写 NAT 规则时，请勿在规则中指定目标条件。确保主接口的规则在备用接口的规则之前。这允许设备在主 ISP 不可用时根据当前路由状态选择正确的 NAT 目的接口。如果指定目标对象，NAT 规则将始终为其他规则选择主接口。
- 如果您收到不应与为接口定义的 NAT 规则匹配的流量的 ASP drop reason nat-no-xlate-to-pat-pool，请为受影响的流量配置身份 NAT 规则，以便流量可以不经转换地通过。
- 如果为 GRE 隧道终端配置 NAT，则您必须在终端上禁用保持连接，否则将无法建立隧道。终端将保持连接发送到原始地址。

管理 NAT 策略

网络地址转换 (NAT) 会将传入数据包的 IP 地址转换为传出数据包中的其他地址。NAT 的主要功能之一是使专用 IP 网络可以连接到互联网。NAT 用公用 IP 地址替换专用 IP 地址，将内部专用网络中的专用地址转换为可在公用互联网上使用的可路由地址。NAT 会对转换进行跟踪（也称为 xlate），以确保将返回流量定向到正确的未转换主机地址。

开始之前

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

祖先域中的管理员可以将 NAT 策略设为针对后代域中的设备，而后代域可以使用这些策略或者将其替换为自定义本地策略。如果 NAT 策略针对不同后代域中的设备，则后代域中的管理员可以查看有关仅属于其域的目标设备的信息。

过程

步骤 1 选择**设备** > **NAT** 。

步骤 2 管理 NAT 策略：

- 创建 - 点击**新建策略 (New Policy)** 按钮，然后选择**威胁防御 NAT (Threat Defense NAT)**。请参阅创建 NAT 策略，第 678 页。
- 复制 - 点击要复制的策略旁边的 **复制**（）。系统将提示您为副本指定唯一的新名称。该副本包含所有策略规则和配置，但不包含设备分配。
- 报告 - 点击 **报告**（）以获取策略。系统会提示您保存 PDF 报告，其中包括策略属性、设备分配、规则以及对象使用信息。
- 编辑 - 点击要编辑的策略旁边的 **编辑**（）。请参阅配置用于威胁防御的 NAT，第 679 页。
- 删除 - 点击要删除的策略旁边的 **删除**（），然后点击**确定 (OK)**。当系统提示是否继续时，还会告知您是否有其他用户在策略中有未保存的更改。

  注意 将NAT策略部署于受管设备后，就不能从设备删除策略。相反，如果要删除受管设备上已出现的 NAT 规则，则必须部署不带任何规则的 NAT 策略。您也不能删除上一次部署于任何目标设备的策略，即使该策略已过时。要完全删除该策略，必须向目标部署其他策略。

创建 NAT 策略

创建新的NAT策略时，必须至少为其提供一个唯一的名称。虽然在创建策略过程中不需要识别策略目标，但必须执行这个步骤后才能部署策略。如果将不带有规则的NAT策略应用于某台设备，系统会从该设备删除所有 NAT 规则。

过程

步骤 1 选择**设备** > **NAT** 。

步骤 2 从下拉列表中点击**新策略 (New Policy)**，然后为 威胁防御 设备选择**威胁防御 NAT (Threat Defense NAT)**。

Firepower NAT 适用于本文档中未涵盖的较早设备。

步骤 3 在**名称 (Name)** 中输入唯一的名称。

在多域部署中，策略名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的策略名称的冲突。

步骤 4 输入**说明 (Description)**（可选）。

步骤 5 选择要部署策略的设备：

- 从**可用设备 (Available Devices)** 列表中选择一个设备，然后点击**添加到策略 (Add to Policy)**。
- 点击**可用设备 (Available Devices)** 列表中的设备并将其拖移到**所选设备 (Selected Devices)** 列表。
- 点击设备旁边的 **删除**（ ），从**所选设备 (Selected Devices)** 列表中删除设备。

步骤 6 点击**保存 (Save)**。

配置 NAT 策略目标

创建或编辑策略时，可以确定要应用策略的受管设备。可以搜索一系列可用设备和高可用性对，并将其添加到所选设备列表。

过程

步骤 1 选择**设备** > **NAT** 。

步骤 2 点击要修改的 NAT 策略旁边的 **编辑**（ ） 。

如果显示**视图**（ ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击**策略分配**。

步骤 4 执行以下任一操作：

- 要将设备、高可用性对或设备组分配给策略，请在**可用设备 (Available Devices)** 列表中将其选中，然后点击**添加到策略 (Add toPolicy)**。还可以进行拖放。
- 要删除设备分配，请点击**所选设备 (Selected Devices)** 列表中的设备、高可用性对或设备组旁边的 **删除**（ ）。

步骤 5 点击**确定 (OK)**。

配置用于威胁防御的 NAT

网络地址转换可能非常复杂。我们建议规则应尽可能保持简单，以避免出现转换问题和难以进行故障排除的情况。在实施 NAT 之前仔细规划，这非常重要。以下程序说明了规划的基本方法。

NAT 策略为共享策略。您将策略分配给应具有类似 NAT 规则的设备。

策略中的给定规则是否适用于分配的设备由规则中使用的接口对象（安全区域或接口组）来确定。如果接口对象包括设备的一个或多个接口，则规则会部署到设备。因此，通过仔细设计接口对象，您可以配置应用于单个共享策略内的设备子集的规则。适用于“任意”接口对象的规则会部署到所有设备。

如果将某个接口的类型更改为不适用于以具有该接口的设备为目标的NAT策略的类型，策略会将该接口标记为“已删除”。在 NAT 策略中点击**保存 (Save)** 会自动从策略删除接口。

如果设备组需要显著不同的规则，则可以配置多个 NAT 策略。

过程

步骤 1 选择**设备 (Devices)** > **NAT**.

- 点击**新建策略 (New Policy)** > **威胁防御 NAT (Threat Defense NAT)** 以创建新策略。为策略命名，或者为其分配设备，然后点击**保存 (Save)**。

  还可以在以后更改设备分配，只需编辑策略并点击**策略分配 (Policy Assignments)**。

- 点击 **编辑**（ ） 以编辑现有威胁防御 NAT 策略。请注意，该页面还会显示 Firepower NAT 策略，威胁防御 设备不会使用这些策略。

  如果显示**视图**（ ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 2 决定您需要哪些类型的规则。

可以创建动态 NAT、动态 PAT、静态 NAT 和身份 NAT 规则。有关概述，请参阅 NAT 类型，第 664 页。

步骤 3 决定应将哪些规则作为手动或自动 NAT 来实施。

有关这两种实施选项的比较，请参阅自动 NAT 和手动 NAT，第 667 页。

步骤 4 决定哪些规则应该根据设备来自定义。

由于您可以将NAT策略分配给多台设备，因此可以在多台设备上配置单个规则。但是，您可能会具有一些每台设备应有不同解释的规则，或一些仅适用于设备子集的规则。

使用接口对象来控制应在哪些设备上配置规则。然后，在网络对象上使用对象覆盖以自定义每台设备使用的地址。

有关详细信息，请参阅为多个设备自定义 NAT 规则，第 681 页。

步骤 5 遵循以下部分中的说明创建规则。

- 动态 NAT，第 685 页
- 动态 PAT，第 690 页
- 静态 NAT，第 699 页
- 身份 NAT，第 707 页

步骤 6 管理 NAT 策略和规则。

您可以执行以下操作来管理策略及其规则。

- 要编辑策略名称或说明，请在那些字段中点击，键入您的更改，然后在字段之外点击。

- 要查看那些仅适用于特定设备的规则，请点击**按设备过滤 (Filter by Device)** 并选择所需的设备。如果某个设备使用的接口对象包括该设备上的接口，则规则适用于该设备。
- 要查看策略中的任何警告或错误，请点击**显示警告 (Show Warnings)**，，然后选择**设备 (Device)**。警告和错误标记出会对流量产生不利影响或阻碍策略部署的配置。
- 要更改策略所分配到的设备，请点击**策略分配 (Policy Assignments)** 链接并根据需要修改所选设备列表。
- 要更改规则是启用还是禁用，请使用右键点击规则并通过 **State** 命令选择所需的选项。可以暂时禁用一条规则而不使用这些控制来删除规则。
- 要添加规则，请点击**添加规则 (Add Rule)** 按钮。
- 要编辑规则，请点击规则的 **编辑**（）。
- 要删除规则，请点击规则的 **删除**（）。
- 要更改页面上显示的规则数量，请使用**每页行数 (Rows Per Page)** 下拉列表。
- 要选择多个规则以启用、禁用或删除，请点击规则的复选框或标题中的复选框，然后再执行操作。

步骤 7 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

为多个设备自定义 NAT 规则

由于NAT策略已共享，可以将给定策略分配给多个设备。但您最多只可为某个给定对象配置一个自动NAT规则。因此，如果您要根据执行转换的特定设备为对象配置不同的转换，则需要谨慎配置接口对象（安全区域或接口组）和定义转换地址的网络对象覆盖。

接口对象确定在哪些设备上配置规则。网络对象覆盖确定给定设备为该对象使用哪些 IP 地址。

请考虑以下情景：

- FTD-A 和 FTD-B 具有连接到名为“inside”的接口的网络 192.168.1.0/24。
- 在 FTD-A 上，当转至“outside”接口时，您要将所有 192.168.1.0/24 地址转换为 10.100.10.10 - 10.100.10.200 范围内的一个 NAT 池。
- 在 FTD-B 上，当转至“outside”接口时，您要将所有 192.168.1.0/24 地址转换为 10.200.10.10 - 10.200.10.200 范围内的一个 NAT 池。

要实现上述配置，请执行以下操作。虽然此示例规则适用于动态自动 NAT，但您也可以将此方法推广到任何类型的 NAT 规则。

过程

步骤 1 为内部和外部接口创建安全区域。

a) 选择**对象 (Object)** > **对象管理 (Object Management)**。
b) 从目录中选择**接口对象 (Interface Objects)** 并点击**添加 (Add)** > **安全区域 (Security Zone)**。（您可以使用接口组而不是区域。）
c) 配置内部区域属性。
   - **名称 (Name)** - 输入名称，例如，**inside-zone**。
   - **类型 (Type)** - 为路由模式设备选择**路由 (Routed)**，为透明模式选择**交换 (Switched)**。
   - **所选接口 (Selected Interfaces)** - 将 FTD-A/内部和 FTD-B/内部接口添加到所选列表。
d) 点击**保存 (Save)**。
e) 点击**Add (添加)** > **安全区域 (Security Zone)** 并定义外部区域属性。
   - **名称 (Name)** - 输入名称，例如，**outside-zone**。
   - **接口类型 (Interface Type)** - 为路由模式设备选择**路由 (Routed)**，为透明模式选择**交换 (Switched)**。
   - **所选接口 (Selected Interfaces)** - 将 FTD-A/外部和 FTD-B/外部接口添加到所选列表。
f) 点击**保存 (Save)**。

步骤 2 在“对象管理”(Object Management) 页面上为原始内部网络创建网络对象。

a) 从目录中选择**网络 (Network)** 并点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。
b) 配置内部网络属性。
   - **名称 (Name)** - 输入名称，例如，**inside-network**。
   - **网络 (Network)** - 输入网络地址，例如，**192.168.1.0/24**。
c) 点击**保存 (Save)**。

步骤 3 为已转换的 NAT 池创建网络对象并定义覆盖。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。
b) 为 FTD-A 配置 NAT 池属性。
   - **名称 (Name)** - 输入名称，例如，**NAT-pool**。
   - **网络 (Network)** - 输入要包含在 FTD-A 池中的地址范围，例如，**10.100.10.10-10.100.10.200**。
c) 选择**允许覆盖 (Allow Overrides)**。
d) 点击**覆盖 (Overrides)** 标题以打开对象覆盖列表。
e) 点击**添加 (Add)** 以打开“添加对象覆盖”(Add Object Override) 对话框。
f) 选择 FTD-B 和**添加 (Add)** 以将其添加到“所选设备”(Selected Devices) 列表。
g) 点击**覆盖 (Override)** 并将**网络 (Network)** 更改为 **10.200.10.10-10.200.10.200**

h) 点击**添加 (Add)** 以将覆盖添加到设备。

通过定义 FTD-B 的覆盖，每当系统在 FTD-B 上配置此对象时，将使用覆盖值而不是原始对象中定义的值。

i) 点击**保存 (Save)**。

步骤 4 配置 NAT 规则。

a) 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型 (Type)**= 动态。

d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象 (Source Interface Objects)** = 内部区域。
- **目标接口对象 (Destination Interface Objects)** = 外部区域。

注释 接口对象用于控制应在哪些设备上配置规则。由于在本例中区域仅包含 FTD-A 和 FTD-B 的接口，因此即使 NAT 策略分配给其他设备，规则也将仅部署到这两台设备。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源 (Original Source)** = 内部网络对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = NAT 池对象。

f) 点击**保存 (Save)**。

您现在有一条对 FTD-A 和 FTD-B 有不同解释的规则，为每个防火墙保护的内部网络提供唯一转换。

搜索和过滤 NAT 规则表

您可以搜索和过滤NAT规则表，以帮助您查找需要修改或查看的规则。过滤表时，仅显示匹配的规则。请注意，尽管规则编号依次更改为1、2等，但过滤不会更改实际规则编号或规则在表中相对于隐藏规则的位置。过滤只是更改您可以看到的内容，以帮助您找到您感兴趣的规则。

编辑 NAT 策略时，可以使用表上方的字段执行以下类型的搜索/过滤：

- **按设备过滤**-点击 **按设备过滤**，然后选择要查看其规则的设备，然后点击 **确定**。规则是否适用于设备取决于规则的接口限制。如果为源接口或目标接口指定安全区域或接口组，则当设备的至少一个接口位于该区域或组中时，该规则将应用于该设备。如果NAT规则适用于任何源接口和任何目标接口，则它适用于所有设备。

如果您还执行文本或多属性搜索，则结果仅限于所选设备。

要删除此过滤器，请点击 **按设备过滤** 并取消选择设备，或选择 **全部**，然后点击 **确定**。

- **简单文本搜索**-在 **过滤器** 框中，键入字符串，然后按 Enter 键。该字符串将与规则中的所有值进行比较。例如，如果输入“network-object-1”（网络对象的名称），则会获得在源、目标和 PAT 池属性中使用该对象的规则。

  对于网络和端口对象，该字符串还会与规则中使用的对象的内容进行比较。例如，如果 PAT 池对象包括 10.100.10.3-10.100.10.100 范围，则在 10.100.10.3 或 10.100.10.100（或部分 10.100.10）上搜索将包括使用该 PAT 池对象的规则。但是，匹配必须精确：在 10.100.10.5 上搜索将不匹配此 PAT 池对象，即使 IP 地址在对象的 IP 地址范围内。

  要删除过滤器，请点击过滤器框右侧的 **x**。

- **多属性搜索**-如果简单文本搜索提供的结果过多，可以为搜索配置多个值。点击 **过滤器** 框以打开属性列表，然后选择或输入要搜索的属性的字符串，然后点击 **过滤器** 按钮。这些属性与您在 NAT 规则中配置的属性相同。属性已进行 AND 运算，因此过滤后的结果仅包含与您配置的所有属性匹配的规则。

  - 对于二进制属性，例如规则状态（启用/禁用）、是否配置了 PAT 池（启用/禁用）、规则的方向（uni/bi）或规则类型（静态/动态），只需选中或取消选中相应的复选框。如果您不关心属性值，请选中这两个复选框。如果取消选中这两个框，则没有任何规则与过滤器匹配。
  - 对于字符串属性，请键入与该属性相关的完整或部分字符串。这些将是安全区域/接口组、网络对象或端口对象的对象名称。它也可以是网络或端口对象内容，其匹配方式与简单文本搜索相同。

  要删除过滤器，请点击“过滤器”框右侧的 **x**，或点击“过滤器”框以打开下拉列表，然后点击清除按钮。

启用、禁用或删除多个规则

您可以逐一启用或禁用手动 NAT 规则，或者删除任何 NAT 规则。您也可以选择多个规则，并将更改一次性应用于所有规则。由于启用/禁用仅适用于手动NAT，如果您选择了混合规则类型，那么就只能将其删除。

请注意，在启用或禁用规则时，选择一些已启用或禁用的规则并不重要。例如，启用已启用的规则只会让该规则保持启用状态。

过程

步骤 1 选择**设备 (Devices)** > **NAT**，然后编辑**威胁防御 NAT (Threat Defense NAT)** 策略。

步骤 2 （可选。）过滤 NAT 规则，以便找到要更改的规则。

如果您有大型 NAT 策略，过滤特别有用。例如，您可以搜索已禁用的规则以便查找需要启用的规则。

步骤 3 选择要更改的规则。

- 点击规则左列中的复选框，以便选择（或取消选择）单个规则。
- 点击表头中的复选框，以便选择当前显示页面上的所有规则。

在翻页时，您的选择会被保留。但实际上，最好是在转到下一页之前对页面上选择的规则执行操作。

步骤 4 执行所需的操作。如果选择了多个规则，系统会要求您确认操作。

请注意，这些操作也可通过右键点击菜单来执行。

- 要启用所有规则，请点击**选择批量操作 (Select Bulk Action)** > **启用 (Enable)**。
- 要禁用所有规则，请点击**选择批量操作 (Select Bulk Action)** > **禁用 (Disable)**。
- 要删除所有规则，请点击**选择批量操作 (Select Bulk Action)** > **删除 (Delete)**。

动态 NAT

以下主题介绍动态 NAT 以及如何配置动态 NAT。

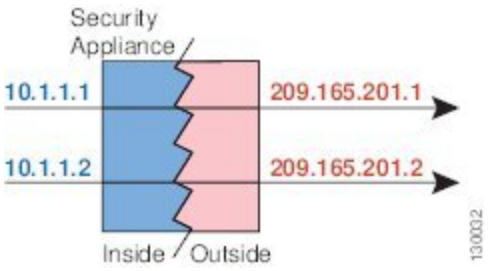
关于动态 NAT

动态NAT将一个实际地址组转换为一个可在目标网络上路由的映射地址池。映射池通常包含少于实际地址组的地址。当您要转换的主机访问目标网络时，NAT会从映射池中为该主机分配IP地址。仅在实际主机发起连接时创建转换。转换仅在连接期间发生，而且转换超时后，给定用户不保持同一IP地址。因此，目标网络上的用户不能向使用动态NAT的主机发起可靠连接，即使访问规则允许该连接。

注释 在转换期间，如果访问规则允许连接转换后主机，远程主机可以发起这种连接。因为地址不可预测，所以与主机的连接不可能发生。然而，在这种情况下，可以依靠访问规则的安全性。

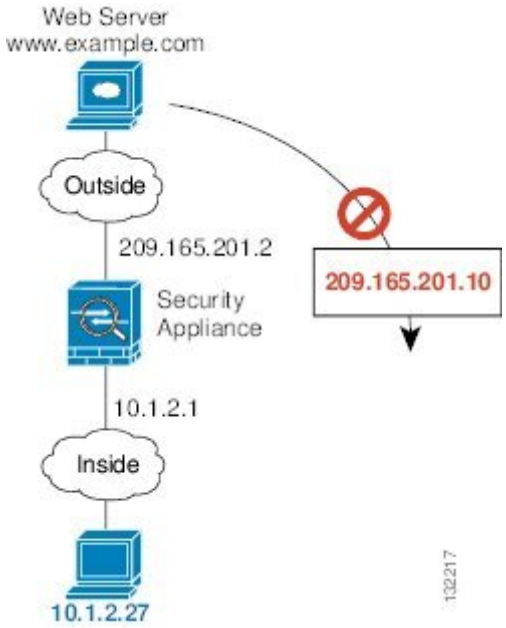
下图显示典型的动态 NAT 场景。仅实际主机可以创建 NAT 会话，允许返回响应流量。

图 *103:* 动态 *NAT*



下图显示一台远程主机尝试发起到映射地址的连接。该地址当前不在转换表中；因此，会丢弃数据包。

图 *104:* 远程主机尝试向映射地址发起连接



动态 NAT 的优缺点

动态 NAT 有以下缺点：

- 如果映射池的地址少于实际组，并且流量数量大于预期，地址可能会用尽。

  如果经常发生这种情况，请使用 PAT 或 PAT 回退方法，因为 PAT 可以使用单一地址的端口提供超过 64,000 次转换。

- 不得不利用映射池中的大量可路由地址，而且可能没有大量的可路由地址可用。

动态 NAT 的优点在于，某些协议不能使用 PAT。PAT 不适用于以下项：

- 没有超载端口的 IP 协议，例如 GRE 0 版本。
- 某些多媒体应用，它们在一个端口上有数据流，在另一个端口上有控制路径，并且不是开放标准。

配置动态自动 NAT

使用动态自动 NAT 规则将地址转换为可在目标网络中路由的其他 IP 地址。

开始之前

选择**对象** > **对象管理**并创建规则中所需的网络对象或组。或者，您可以在定义 NAT 规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机、范围或子网。
- **转换后的源** - 此选项可以是网络对象或组，但不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。如果某个组同时包含范围和主机 IP 地址，则范围将用于动态 NAT，主机 IP 地址将用作 PAT 回退。

过程

步骤 1 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

步骤 2 执行以下操作之一：

- 点击**添加规则 (Add Rule)** 按钮以创建新规则。
- 点击**编辑**（）以编辑现有规则。

右键点击菜单还具有用于剪切、复制、粘贴、插入和删除规则的选项。

步骤 3 配置基本规则选项：

- **NAT 规则** - 选择**自动 NAT 规则**。
- **类型** - 选择**动态**。

步骤 4 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象**、**目标接口对象** - （网桥组成员接口的必选项。）用于识别此 NAT 规则应用的接口的接口对象（安全区域或接口组）。**源**是包含实际接口的对象，流量通过该接口进入设备。**目标**是包含映射接口的对象，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 在 **(General Translation)** 上配置以下选项：

- **原始源** - 包含您要转换的地址的网络对象。
- **转换后的源** - 包含映射地址的网络对象或组。

步骤 6 （可选。）在**高级 (Advanced)** 上选择所需选项：

- **转换与此规则匹配的 DNS 回复** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的DNS回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 760 页。
- **跳转到接口 PAT（目标接口）** - 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。要使用接口的 IPv6 地址，另请勾选 **IPv6** 选项。
- **IPv6** - 是否为接口 PAT 使用目的地接口的 IPv6 地址。

步骤 7 点击**保存**以添加规则。

步骤 8 点击“NAT”页面上的**保存**以保存更改。

配置动态手动 NAT

当自动 NAT 不能满足您的需求时，请使用动态手动 NAT 规则。例如，如果您要根据目标进行不同的转换。动态 NAT 会将地址转换为可在目标网络中路由的其他 IP 地址。

开始之前

依次选择**对象** > **对象管理**，然后创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- **原始源** - 此选项可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定**任何 (Any)**。
- **转换后的源** - 此选项可以是网络对象或组，但不能包含在子网中。如果某个组同时包含范围和主机 IP 地址，则范围将用于动态 NAT，主机 IP 地址将用作 PAT 回退。

如果您要在规则中为**原始目标**和**转换后的目标**配置静态转换，还可以为这些地址创建网络对象。

对于动态 NAT，您还可以对目标执行端口转换。在对象管理器中，请确保有可用于**原始目标端口**和**转换后的目标端口**的端口对象。系统将忽略您指定的源端口。

过程

步骤 1 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

步骤 2 执行以下操作之一：

- 点击**添加规则 (Add Rule)** 按钮以创建新规则。
- 点击**编辑**（ ）以编辑现有规则。

右键点击菜单还具有用于剪切、复制、粘贴、插入和删除规则的选项。

步骤 3 配置基本规则选项：

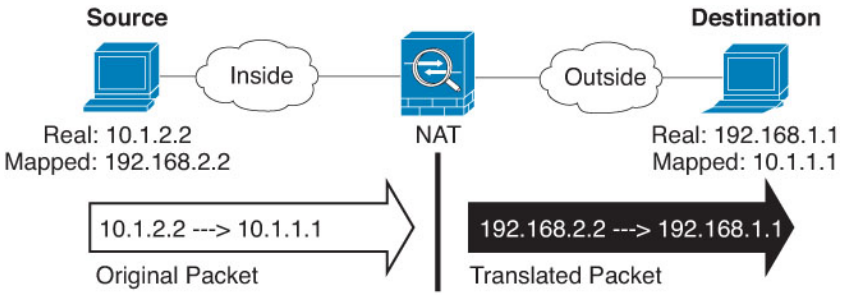
- **NAT 规则** - 选择**手动 NAT 规则**。
- **类型** - 选择**动态**。该设置仅应用于源地址。如果为目标地址定义转换，则该转换始终为静态。
- **启用** - 您是否希望规则处于活动状态。可以随后使用“规则”(Rules) 页面上的右键点击菜单激活或停用该规则。
- **插入** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后）或指定规则的上方或下方。

步骤 4 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象**、**目标接口对象** -（网桥组成员接口的必选项。）用于识别此 NAT 规则应用的接口的接口对象（安全区域或接口组）。**源**是包含实际接口的对象，流量通过该接口进入设备。**目标**是包含映射接口的对象，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 （在**转换**页面上。）确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例。



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

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

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源** - 包含映射地址的网络对象或组。
- **转换后的目标** -（可选。）包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标**选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

步骤 7 （可选。）确定用于服务转换的目标服务端口：**原始目标端口**、**转换后的目标端口**。

动态 NAT 不支持端口转换，因此，请将**原始源端口**和**已转换源端口**字段保留为空。然而，由于目标转换始终为静态，因此可为目标端口执行端口转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

步骤 8 （可选。）在**高级 (Advanced)** 上选择所需选项：

- （仅适用于源转换。）**转换与此规则匹配的 DNS 回复** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的 DNS 回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 760 页。
- **跳转到接口 PAT（目标接口）** - 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。要使用接口的 IPv6 地址，另请勾选 **IPv6** 选项。
- **IPv6** - 是否为接口 PAT 使用目的地接口的 IPv6 地址。

步骤 9 点击**保存**以添加规则。

步骤 10 点击“NAT”页面上的**保存**以保存更改。

动态 PAT

以下主题介绍动态 PAT。

关于动态 PAT

通过将实际地址和源端口转换为映射地址和唯一端口，动态 PAT 可以将多个实际地址转换为单一映射地址。

每个连接都需要单独的转换会话，因为每个连接的源端口都不同。例如，10.1.1.1:1025 需要来自 10.1.1.1:1026 的单独的转换。

下图显示一个典型的动态 PAT 场景。仅实际主机可以创建 NAT 会话，允许返回响应流量。映射地址对于每次转换都是相同的，但端口需要动态分配。

图 *105:* 动态 *PAT*

对于转换持续时间，如果访问规则允许，目标网络上的远程主机可以发起到转换后主机的连接。因为端口地址（实际和映射）不可预测，所以到该主机的连接不可能发生。然而，在这种情况下，可以依靠访问规则的安全性。

在连接过期后，端口转换也将过期。

注释 建议每个接口使用不同的 PAT 池。如果多个接口使用同一池，尤其是用于“任何”接口时，该池将被快速耗尽，且没有端口可用于新的转换。

动态 PAT 的优缺点

通过动态 PAT，可以使用单一映射地址，从而保存可路由地址。甚至可以将 威胁防御设备 接口 IP 地址用作 PAT 地址。

在同属一个网桥组的接口之间进行转换时，不能将动态 PAT 用于 IPv6 (NAT66)。此限制不适用于接口为不同网桥组成员或一个接口为网桥组成员，另一个为标准路由接口的情况。

动态 PAT 不适用于某些数据流不同于控制路径的多媒体应用。有关详细信息，请参阅对检测到的协议的 NAT 支持，第 673 页。

动态 PAT 还可以创建大量显示为来自单一 IP 地址的连接，服务器可能将此流量解释为 DoS 攻击。可以配置一个 PAT 地址池，使用 PAT 地址轮询分配来避免出现这种情况。

PAT 池对象指南

当为 PAT 池创建网络对象时，请遵守以下指导原则。

对于 PAT 池

- 端口会映射到 1024 到 65535 范围内的可用端口。您可以选择包含保留的端口，即 1024 以下的端口，以便让整个端口范围可用于转换。

  在集群中运行时，每个地址的512个端口块会被分配给集群成员，并在这些端口块内进行映射。如果还启用块分配，则会根据块分配大小（其默认值也是 512）来分配端口。

- 如果对 PAT 池启用块分配，则仅在 1024-65535 范围内分配端口块。因此，如果应用需要较低的端口号 (1-1023)，它可能不起作用。例如，请求端口 22 (SSH) 的应用会获得 1024-65535 范围内和分配到主机的块范围内的映射端口。

- 如在两个不同的规则中使用相同的 PAT 池对象，则请确保为每条规则指定相同的选项。例如，如果一条规则指定扩展 PAT，则另一条规则也必须指定扩展 PAT。

- 如果主机拥有现有连接，则来自该主机的后续连接会使用相同的 PAT IP 地址。如果没有可用的端口，这可能会阻止连接。使用轮询选项可避免此问题。

对于 PAT 池的扩展 PAT

- 许多应用检测不支持扩展 PAT。

- 如为动态 PAT 规则启用扩展 PAT，则不能在支持端口转换规则的另一静态 NAT 中使用 PAT 池中的地址作为 PAT 地址。例如，如果 PAT 池包括 10.1.1.1，则无法将 10.1.1.1 作为 PAT 地址创建带端口转换规则的静态 NAT。

- 如使用 PAT 池，并为回退指定接口，则无法指定扩展 PAT。

- 对于使用 ICE 或 TURN 的 VoIP 部署，请勿使用扩展 PAT。ICE 和 TURN 依赖于 PAT 绑定才能对所有目标均保持相同。

- 您不能在集群中的设备上使用扩展 PAT。

- 扩展 PAT 会增加设备上的内存使用率。

对于 PAT 池的轮询

- 如果主机拥有现有连接，并且端口可用，则来自该主机的后续连接将使用相同的 PAT IP 地址。不过，这种“粘性”不能超越故障切换。如果该设备执行故障切换，来自主机的后续连接可能会使用初始 IP 地址。

- 如果在同一接口上混合使用 PAT 池/轮询规则和接口 PAT 规则，IP 地址"粘性"也会受到影响。对于任何给定接口，请选择 PAT 池或接口 PAT；请勿创建竞争 PAT 规则。

- 轮询可能会消耗大量的内存，在与扩展 PAT 组合使用时尤其如此。由于将为每一个映射协议/IP 地址/端口范围创建 NAT 池，因此，轮询会导致大量并发 NAT 池，从而消耗内存。扩展 PAT 甚至将导致更多数量的并发 NAT 池。

配置动态自动 PAT

使用动态自动 PAT 规则可将地址转换为唯一的 IP 地址/端口组合，而不是仅转换为多个 IP 地址。您可以转换为单个地址（目标接口的地址或其他地址），或者使用地址的 PAT 池来提供更多的可能转换。

开始之前

选择**对象** > **对象管理**并创建规则中所需的网络对象或组。或者，您可以在定义 NAT 规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机、范围或子网。
- **转换后的源** - 可通过以下选项指定 PAT 地址：
  - **目标接口** - 要使用目标接口地址，不需要网络对象。
  - **单个 PAT 地址** - 创建包含单个主机的网络对象。
  - **PAT 池** - 创建一个包含范围的网络对象，或创建一个包括主机、范围或这两者的网络对象组。不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。

过程

步骤 1 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

步骤 2 执行以下操作之一：

- 点击**添加规则 (Add Rule)** 按钮以创建新规则。
- 点击**编辑**（ ）以编辑现有规则。

右键点击菜单还具有用于剪切、复制、粘贴、插入和删除规则的选项。

步骤 3 配置基本规则选项：

- **NAT 规则** - 选择**自动 NAT 规则**。
- **类型** - 选择**动态**。

步骤 4 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象**、**目标接口对象** -（网桥组成员接口的必选项。）用于识别此 NAT 规则应用的接口的接口对象（安全区域或接口组）。**源**是包含实际接口的对象，流量通过该接口进入设备。**目标**是包含映射接口的对象，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 在 **(General Translation)** 上配置以下选项：

- **原始源** - 包含您要转换的地址的网络对象。
- **转换后的源** - 以下项之一：
  - （接口 PAT。）要使用目标接口的地址，请选择**目标接口 IP**。您还必须选择特定目标接口对象。要使用接口的 IPv6 地址，还必须在**高级 (Advanced)** 上选择 **IPv6** 选项。跳过配置 PAT 池的步骤。
  - 要使用目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。跳过配置PAT池的步骤。
  - 若要使用 PAT 池，请将**转换后的源**留空。

步骤 6 如果使用的是 PAT 池，请选择 **PAT 池**页面并执行以下操作：

a) 选择**启用 PAT 池 (Enable PAT pool)**。

b) 选择包含 **PAT** > **地址**字段中的池地址的网络对象组。

或者，可以选择**目的接口 IP (Destination Interface IP)**，它是实施接口 PAT 的另一种方法。

c) （可选）根据需要选择以下选项：

- **使用轮询分配** - 以轮询方式分配地址/端口。默认情况下，如果不采用轮询，在使用下一个 PAT 地址之前，将分配 PAT 地址的所有端口。轮询方法分配来自池中每个 PAT 地址的一个地址/端口，然后才返回再次使用第一个地址，接着是第二个地址，以此类推。
- **扩展 PAT 表** - 使用扩展 PAT。通过将目的地地址和端口纳入转换信息，相对于按 IP 地址，扩展 PAT 将按服务使用 65535 个端口。通常，创建 PAT 转换时，不考虑目的地端口和地址，因此限制为每个 PAT 地址 65535 个端口。例如，通过扩展 PAT，您可以创建在访问 192.168.1.7:23 时转到 10.1.1.1:1027 的转换，以及在访问 192.168.1.7:80 时转到 10.1.1.1:1027 的转换。不能将此选项用于接口 PAT 或接口 PAT 回退。
- **扁平端口范围、包括保留端口** - 在分配 TCP/UDP 端口时使用 1024 到 65535 的端口范围作为单个扁平范围。（6.7 以下版本）为转换选择映射端口号时，PAT 使用实际源端口号（若可用）。然而，如果不使用此选项，则当实际端口不可用时，将默认从与实际端口号相同的端口范围选择映射端口：1 到 511、512 到 1023 以及 1024 到 65535。为了避免用尽低端口号范围的端口，请配置此设置。要使用 1 到 65535 的整个范围，另请勾选**包括保留端口 (Include Reserved Ports)** 选项。对于运行版本 6.7 或更高版本的 威胁防御 设备，无论是否选择该选项，始终配置扁平端口范围。您仍可以为这些系统选择**包括保留端口 (Include Reserved Ports)** 选项，并且系统将采用该设置。
- **块分配** - 启用端口块分配。对于运营商级或大规模 PAT，可以为每个主机分配一个端口块，而非由 NAT 每次分配一个端口转换。如果分配端口块，来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中，可根据需要分配更多块。只能在 1024-65535 范围内分配端口块。端口块分配与轮询兼容，但无法将其与扩展 PAT 或不分段端口范围选项一起使用。也无法使用接口 PAT 回退。

步骤 7 （可选。）在**高级 (Advanced)** 上选择所需选项：

- **跳转到接口 PAT（目标接口）** - 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。要使用

接口的 IPv6 地址，另请勾选 **IPv6** 选项。 如果已配置接口 PAT 作为转换后的地址或 PAT 池，则不能选择此选项。

- **IPv6** - 是否为接口 PAT 使用目的地接口的 IPv6 地址。

步骤 8 点击**保存**以添加规则。

步骤 9 点击“NAT”页面上的**保存**以保存更改。

配置动态手动 PAT

当自动 PAT 不能满足您的需求时，请使用动态手动 PAT 规则。例如，如果您要根据目标进行不同的转换。动态 PAT 可将地址转换为唯一的 IP 地址/端口组合，而不是仅转换为多个 IP 地址。您可以转换为单个地址（目标接口的地址或其他地址），或者使用地址的 PAT 池来提供更多的可能转换。

开始之前

依次选择**对象** > **对象管理**，然后创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- **原始源** - 此选项可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定**任何 (Any)**。
- **转换后的源** - 可通过以下选项指定 PAT 地址：
  - **目标接口** - 要使用目标接口地址，不需要网络对象。
  - **单个 PAT 地址** - 创建包含单个主机的网络对象。
  - **PAT 池** - 创建一个包含范围的网络对象，或创建一个包括主机、范围或这两者的网络对象组。不能包含子网。

如果您要在规则中为**原始目标**和**转换后的目标**配置静态转换，还可以为这些地址创建网络对象。

对于动态 NAT，您还可以对目标执行端口转换。在对象管理器中，请确保有可用于**原始目标端口**和**转换后的目标端口**的端口对象。系统将忽略您指定的源端口。

过程

步骤 1 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

步骤 2 执行以下操作之一：

- 点击**添加规则 (Add Rule)** 按钮以创建新规则。
- 点击**编辑**（  ）以编辑现有规则。

右键点击菜单还具有用于剪切、复制、粘贴、插入和删除规则的选项。

步骤 3 配置基本规则选项：

- **NAT 规则** - 选择**手动 NAT 规则**。

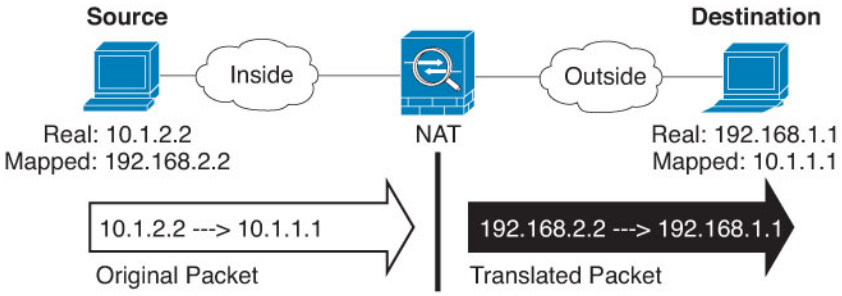
- **类型** - 选择**动态**。该设置仅应用于源地址。如果为目标地址定义转换，则该转换始终为静态。
- **启用** - 您是否希望规则处于活动状态。可以随后使用“规则”(Rules) 页面上的右键点击菜单激活或停用该规则。
- **插入** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后）或指定规则的上方或下方。

步骤 4 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象**、**目标接口对象** - （网桥组成员接口的必选项。）用于识别此 NAT 规则应用的接口的接口对象（安全区域或接口组）。**源**是包含实际接口的对象，流量通过该接口进入设备。**目标**是包含映射接口的对象，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 （在**转换**页面上。）确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例。



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

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

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源** - 以下项之一：
  - （接口 PAT。）要使用目标接口的地址，请选择**目标接口 IP**。您还必须选择特定目标接口对象。要使用接口的 IPv6 地址，还必须在**高级 (Advanced)** 上选择 **IPv6** 选项。跳过配置 PAT 池的步骤。
  - 要使用目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。跳过配置 PAT 池的步骤。
  - 若要使用 PAT 池，请将**转换后的源**留空。

- **转换后的目标** -（可选。）包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标**选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

步骤 7 （可选。）确定用于服务转换的目标服务端口：**原始目标端口**、**转换后的目标端口**。

动态NAT不支持端口转换，因此，请将**原始源端口**和**已转换源端口**字段保留为空。然而，由于目标转换始终为静态，因此可为目标端口执行端口转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

步骤 8 如果使用的是 PAT 池，请选择 **PAT 池**页面并执行以下操作：

a) 选择**启用 PAT 池 (Enable PAT pool)**。

b) 选择包含 **PAT** > **地址**字段中的池地址的网络对象组。

或者，可以选择**目的接口 IP (Destination Interface IP)**，它是实施接口 PAT 的另一种方法。

c) （可选）根据需要选择以下选项：

- **使用轮询分配** - 以轮询方式分配地址/端口。默认情况下，如果不采用轮询，在使用下一个 PAT 地址之前，将分配 PAT 地址的所有端口。轮询方法分配来自池中每个 PAT 地址的一个地址/端口，然后才返回再次使用第一个地址，接着是第二个地址，以此类推。
- **扩展 PAT 表** - 使用扩展 PAT。通过将目的地地址和端口纳入转换信息，相对于按 IP 地址，扩展 PAT 将按服务使用 65535 个端口。通常，创建 PAT 转换时，不考虑目的地端口和地址，因此限制为每个 PAT 地址 65535 个端口。例如，通过扩展 PAT，您可以创建在访问 192.168.1.7:23 时转到 10.1.1.1:1027 的转换，以及在访问 192.168.1.7:80 时转到 10.1.1.1:1027 的转换。不能将此选项用于接口 PAT 或接口 PAT 回退。
- **扁平端口范围**、**包括保留端口** - 在分配 TCP/UDP 端口时使用 1024 到 65535 的端口范围作为单个扁平范围。（6.7 以下版本）为转换选择映射端口号时，PAT 使用实际源端口号（若可用）。然而，如果不使用此选项，则当实际端口不可用时，将默认从与实际端口号相同的端口范围选择映射端口：1 到 511、512 到 1023 以及 1024 到 65535。为了避免用尽低端口号范围的端口，请配置此设置。要使用 1 到 65535 的整个范围，另请勾选**包括保留端口 (Include Reserved Ports)** 选项。对于运行版本 6.7 或更高版本的 威胁防御 设备，无论是否选择该选项，始终配置扁平端口范围。您仍可以为这些系统选择**包括保留端口 (Include Reserved Ports)** 选项，并且系统将采用该设置。
- **块分配** - 启用端口块分配。对于运营商级或大规模 PAT，可以为每个主机分配一个端口块，而非由 NAT 每次分配一个端口转换。如果分配端口块，来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中，可根据需要分配更多块。只能在 1024-65535 范围内分配端口块。端口块分配与轮询兼容，但无法将其与扩展 PAT 或不分段端口范围选项一起使用。也无法使用接口 PAT 回退。

步骤 9 （可选。）在**高级 (Advanced)** 上选择所需选项：

- **跳转到接口 PAT**（**目标接口**） - 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。要使用接口的 IPv6 地址，另请勾选 **IPv6** 选项。
- **IPv6** - 是否为接口 PAT 使用目的地接口的 IPv6 地址。

步骤 10 点击**保存**以添加规则。

步骤 11 点击“NAT”页面上的**保存**以保存更改。

使用端口块分配配置 PAT

对于运营商级或大规模 PAT，您可以为每台主机分配端口块，而无需通过 NAT 一次分配一个端口转换（请参阅 RFC 6888）。如果分配端口块，来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中，可根据需要分配更多块。当使用块中端口的最后一个转换被删除时，系统将释放该块。

分配端口块的主要原因是为了减少日志记录。记录端口块分配，记录连接，但不会记录在端口块中创建的转换。另一方面，这样会使日志分析变得更加复杂。

只能在 1024-65535 范围内分配端口块。因此，如果应用需要较低的端口号 (1-1023)，它可能不起作用。例如，请求端口 22 (SSH) 的应用会获得 1024-65535 范围内和分配到主机的块范围内的映射端口。您可以创建一个单独的 NAT 规则，对于使用低端口号的应用不应用块分配；对于两次 NAT，请确保该规则位于块分配规则之前。

开始之前

NAT 规则的使用说明：

- 您可以包含**使用轮询分配 (Use Round Robin Allocation)** 选项，但无法包含扩展 PAT 唯一性、使用宽范围、包含保留的端口或后退至接口 PAT 的选项。此外，还允许其他源/目标地址和端口信息。
- 同所有 NAT 变更一样，如果要替换现有的规则，必须清除与被替换规则相关的转换，新规则才会生效。可以显式清除它们，也可以静待它们超时。在集群中运行时，您必须在整个集群中全局清除 xlate。

注释 如果要在常规 PAT 和块分配 PAT 规则之间切换，您必须先删除规则，然后再清除转换。然后，您可以创建新的对象 NAT 规则。否则，您将在 **show asp drop** 输出中看到 pat-port-block-state-mismatch 丢弃。

- 对于特定 PAT 池，必须为使用该池的所有规则指定（或不指定）块分配。不能在一个规则中分配块，而在另一个规则中不分配块。重叠的 PAT 池也不能混合块分配设置。此外，该池的静态 NAT 不能与端口转换规则重叠。

过程

步骤 1 （可选。）配置全局 PAT 端口块分配设置。

有一些可以控制端口块分配的全局设置。如果要更改这些选项的默认值，必须配置一个 FlexConfig 对象，并将其添加到 FlexConfig 策略中。

a) 选择**对象** > **对象管理** > **FlexConfig** > **FlexConfig 对象**，然后创建新对象。
b) 配置块分配大小，即每个块中的端口数。

xlate block-allocation size *value*

范围为 32-4096。默认值为 512。使用“no”形式可恢复默认值。

如果不使用默认值，请确保 64,512 能被您所选的大小整除（1024-65535 范围中的端口数)。否则，会出现无法使用的端口。例如，如果指定 100，会有 12 个未使用端口。

c) 配置每个主机可分配的最大块数。

xlate block-allocation maximum-per-host *number*

限制是针对每个协议，因此限制为 4 表示每个主机最多 4 个 UDP 块、4个 TCP 块和 4 个 ICMP 块。范围为 1-8，默认值为 4。使用“no”形式可恢复默认值。

d) （可选。）启用临时系统日志生成。

xlate block-allocation pba-interim-logging *seconds*

默认情况下，系统会在端口块创建和删除操作发生时生成系统日志消息。如果启用临时日志记录，系统会按您指定的时间间隔生成以下消息。这些消息会报告消息生成时所有已分配的活动端口块，包括协议（ICMP、TCP、UDP、源和目标接口与 IP 地址，以及端口块。可以指定 21600 至 604800 秒（6 小时至 7 天）的时间间隔。

%ASA-6-305017: Pba-interim-logging: Active *protocol* block of ports for translation from *real_interface*:*real_host_ip* to *mapped_interface*:*mapped_ip_address*/*start_port_num-end_port_num*

示例：

以下示例将块分配大小设置为 64，将每主机最大数设置为 8，并且每 6 小时启用一次临时日志记录。

```
xlate block-allocation size 64
xlate block-allocation maximum-per-host 8
xlate block-allocation pba-interim-logging 21600
```

e) 在 FlexConfig 对象中选择以下选项：

- **部署** = **每次**
- **类型** = **附加**

f) 点击**保存**以创建 FlexConfig 对象。
g) 选择**设备** > **FlexConfig**，然后创建或编辑分配给需要调整这些设置的设备的 FlexConfig 策略。
h) 在可用对象列表中选择对象，然后点击 > 将其移动至所选的对象列表。
i) 点击**保存**。

您可以点击**预览配置**，选择其中一个目标设备，并验证 xlate 命令是否正确显示。

步骤 2 添加使用 PAT 池端口块分配的 NAT 规则。

a) 依次选择**设备** > **NAT**，并添加或编辑威胁防御 NAT 策略。
b) 添加或编辑 NAT 规则，并至少配置以下选项。

- **类型** = **动态**
- 在 **转换** > **原始源**中，选择定义源地址的对象。
- 在 **PAT 池 (PAT Pool)** 中配置以下选项：
  - 选择**启用 PAT 池**
  - 在 **PAT** > **地址**中选择定义 PAT 池的网络对象。
  - 选择**块分配**选项。

c) 保存对规则和 NAT 策略所做的更改。

静态 NAT

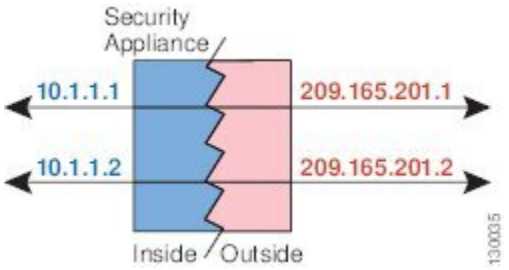
以下主题介绍静态 NAT 以及如何实施静态 NAT。

关于静态 NAT

静态NAT创建实际地址到映射地址的固定转换。因为映射地址对于每个连续连接都是相同的，所以静态NAT允许双向连接发起，即到主机发起和从主机发起（如果有允许这样做的访问规则）。另一方面，通过动态NAT和PAT，每台主机为每次后续转换使用不同的地址或端口，因此，不支持双向发起。

下图显示典型的静态 NAT 场景。转换始终处于活动状态，所以，实际主机和远程主机可以发起连接。

图 *106:* 静态 *NAT*



注释 如果需要，可以禁用双向性。

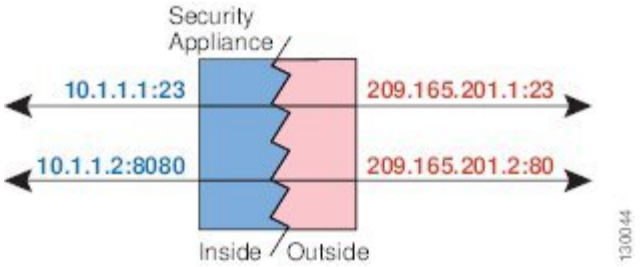
支持端口转换的静态 NAT

支持端口转换的静态 NAT 让您可以指定实际和映射协议及端口。

指定带静态 NAT 的端口时，可以选择将端口和/或 IP 地址映射到同一值或不同值。

下图显示支持端口转换的典型静态NAT场景，其中显示映射到本身的端口和映射到不同值的端口；在这两种情况下，IP 地址映射到不同值。转换始终处于活动状态，所以，转换后主机和远程主机可以发起连接。

图 *107:* 支持端口转换的典型静态 *NAT* 场景



支持端口转换的静态 NAT 规则支持仅访问指定端口的目标 IP 地址。如果您尝试访问其他端口上 NAT 规则未涵盖的的目标 IP 地址，连接将被阻止。此外，对于手动 NAT，如果流量与 NAT 规则的源 IP 地址不匹配，但与目标 IP 地址匹配，流量将被丢弃，不管目标端口为何。因此，您必须为允许发送到目标 IP 地址的所有其他流量添加额外规则。例如，您可以为 IP 地址配置静态 NAT 规则（不含端口规范），并将其放置在端口转换规则后面。

注释 对于需要对辅助信道执行应用检查的应用（例如 FTP 和 VoIP），NAT 会自动转换辅助端口。

下面是使用支持端口转换的静态 NAT 的其他情况。

具有身份端口转换的静态 NAT

可以简化对内部资源的外部访问。例如，如果您有在不同端口上提供服务（例如 FTP、HTTP 和 SMTP）的三个单独的服务器，可以为外部用户提供单个 IP 地址以访问这些服务。然后，可以配置具有身份端口转换的静态NAT，从而根据尝试访问的端口将单个外部IP地址映射到实际服务器的正确 IP 地址。您无需更改端口，因为服务器使用的是标准端口（分别是 21、80 和 25)。

对非标准端口进行端口转换的静态 NAT

还可以利用支持端口转换的静态 NAT 将一个公认端口转换为一个非标准端口，反之亦然。例如，如果内部 Web 服务器使用端口 8080，可以允许外部用户连接到端口 80，然后取消转换到原始端口 8080。同样，要进一步提高安全性，可以告知 Web 用户连接到非标准端口 6785，然后取消转换到端口 80。

具有端口转换的静态接口 NAT

可以配置静态NAT，以将一个实际地址映射到一个接口地址/端口组合。例如，如果要将对设备外部接口的 Telnet 访问重定向至内部主机，则可以将内部主机 IP 地址/端口 23 映射到外部接口地址/端口 23。

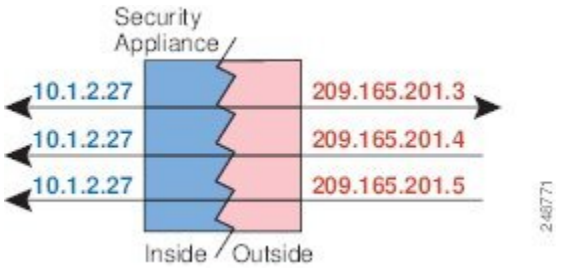
一对多静态 NAT

通常，配置带一对一映射的静态 NAT。然而，在某些情况下，可能要将单一实际地址配置到多个映射地址（一对多）。配置一对多静态 NAT 时，当实际主机发起流量时，它始终使用第一个映射地

址。然而，对于发起到主机的流量，可以发起到任何映射地址的流量，并且不将它们转换为单一实际地址。

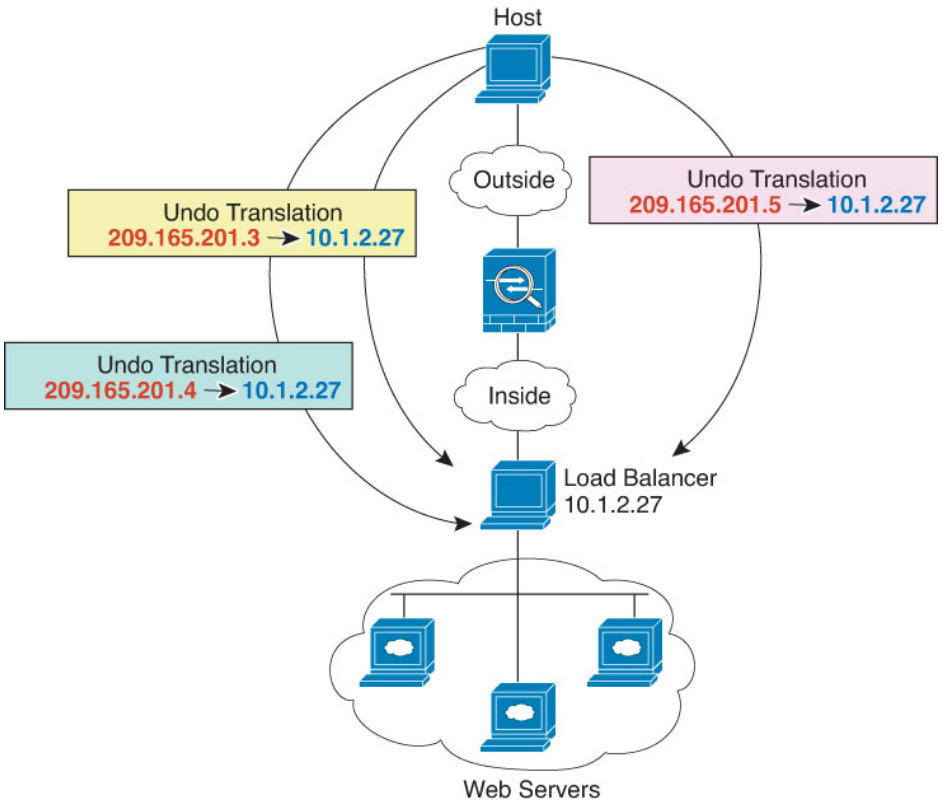
下图显示典型的一对多静态NAT场景。由于实际主机进行的发起的流量始终使用第一个映射地址，因此从技术上说，实际主机 IP/第一个映射 IP 的转换是唯一的双向转换。

图 *108:* 一对多静态 *NAT*



例如，在 10.1.2.27 上有一个负载均衡器。根据请求的 URL，它会将流量重新定向到正确的 Web 服务器。

图 *109:* 一对多静态 *NAT* 示例



其他映射场景（不推荐）

NAT 具有很高的灵活性，允许任何类型的静态映射场景：不仅包括一对一、一对多，还包括少对多、多对少和多对一映射。我们推荐仅使用一对一或一对多映射。其他映射选项可能会导致意外后果。

在功能上，少对多与一对多相同；但是，因为此配置更加复杂，而且实际映射可能不会一目了然，所以我们建议为每个需要一对多配置的实际地址创建该配置。例如，对于少对多场景，少量的实际地址会按顺序映射到多个映射地址（A 到 1、B 到 2、C 到 3）。当映射所有实际地址时，下一个映射地址会映射到第一个实际地址，依此类推，直到映射了所有映射地址为止（A 到 4、B 到 5、C 到 6）。这将导致每个实际地址有多个映射地址。就像一对多配置一样，仅第一个映射是双向的；后续映射可以将流量发起到实际主机，但所有从实际主机发起的流量仅将第一个映射地址用于源。

下图显示典型的少对多静态 NAT 场景。

图 *110:* 少对多静态 *NAT*

对于实际地址多于映射地址的多对少或多对一配置，映射地址会在实际地址用尽之前先用尽。仅最低实际 IP 地址和映射池之间的映射可以导致双向发起。剩余的更高的实际地址可以发起流量，但不能将流量发起到这些地址（由于五元组 [源 IP、目标 IP、源端口、目标端口、协议] 的唯一性，连接的返回流量会定向到正确的实际地址）。

注释 多对少或多对一 NAT 不是 PAT。如果两台实际主机使用同一源端口号，连接到同一外部服务器和同一 TCP 目标端口，并且两台主机转换到同一 IP 地址，那么由于地址冲突（五元组不唯一），将重置两个连接。

下图显示一个典型的多对少静态 NAT 场景。

图 *111:* 多对少静态 *NAT*

我们建议不要这样使用静态规则，而是为需要双向发起的流量创建一对一规则，为其他地址创建动态规则。

配置静态自动 NAT

使用静态自动 NAT 规则将地址转换为可在目标网络中路由的其他 IP 地址。您还可以通过静态 NAT 规则执行端口转换。

开始之前

选择**对象** > **对象管理**并创建规则中所需的网络对象或组。或者，您可以在定义 NAT 规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机、范围或子网。
- **转换后的源** - 可以通过以下选项指定转换后的地址：
  - **目标接口** - 要使用目标接口地址，不需要网络对象。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。
  - **地址** - 创建包含主机、范围或子网的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；其只能包含一种类型。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。

过程

步骤 1 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

步骤 2 执行以下操作之一：

- 点击**添加规则 (Add Rule)** 按钮以创建新规则。
- 点击**编辑**（ ）以编辑现有规则。

右键点击菜单还具有用于剪切、复制、粘贴、插入和删除规则的选项。

步骤 3 配置基本规则选项：

- **NAT 规则** - 选择**自动 NAT 规则**。
- **类型 (Type)** - 选择**静态 (Static)**。

步骤 4 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象**、**目标接口对象** -（网桥组成员接口的必选项。）用于识别此 NAT 规则应用的接口的接口对象（安全区域或接口组）。**源**是包含实际接口的对象，流量通过该接口进入设备。**目标**是包含映射接口的对象，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 在 **(General Translation)** 上配置以下选项：

- **原始源** - 包含您要转换的地址的网络对象。

- **转换后的源** - 以下项之一：
  - 要使用一组地址，请选择**地址**和包含映射地址的网络对象或组。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。
  - （具有端口转换的静态接口NAT。）要使用目标接口的地址，请选择**目标接口IP**。您还必须选择特定目标接口对象。要使用接口的IPv6地址，还必须在**高级 (Advanced)** 上选择 **IPv6** 选项。该选项配置具有端口转换的静态接口NAT：源地址/端口转换为接口的地址和相同的端口号。
- （可选。）**原始端口**、**转换后的端口** - 如果需要转换 TCP 或 UDP 端口，请在**原始端口**中选择协议，并输入原始和转换端口编号。例如，如有必要，可以将 TCP/80 转换为 8080。

步骤 6 （可选。）在**高级 (Advanced)** 上选择所需选项：

- **转换与此规则相匹配的 DNS 应答** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的DNS回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 760 页。 如果您在进行端口转换，则此选项不可用。
- **IPv6** - 是否为接口 PAT 使用目的地接口的 IPv6 地址。
- **网络到网络映射** - 对于 NAT 46，请选择此选项以将第一个 IPv4 地址转换为第一个 IPv6 地址，将第二个 IPv4 地址转换为第二个 IPv6 地址，依此类推。如不使用此选项，则将使用 IPv4 嵌入式方法。对于一对一转换，必须使用此选项。
- **请勿在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。

步骤 7 点击**保存**以添加规则。

步骤 8 点击“NAT”页面上的**保存**以保存更改。

配置静态手动 NAT

当自动 NAT 不能满足您的需求时，请使用静态手动 NAT 规则。例如，如果您要根据目标进行不同的转换。静态 NAT 会将地址转换为可在目标网络中路由的其他 IP 地址。您还可以通过静态 NAT 规则执行端口转换。

开始之前

依次选择**对象** > **对象管理**，然后创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- **原始源** - 此选项可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定**任何 (Any)**。

- **转换后的源** - 可以通过以下选项指定转换后的地址：
  - **目标接口** - 要使用目标接口地址，不需要网络对象。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。
  - **地址** - 创建包主机、范围或子网的网络对象或组。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。

如果要在规则中为**原始目标**和**转换后的目标**地址配置静态转换，则还可以为这些地址创建网络对象。如果只需要配置支持端口转换的目标静态接口 NAT，则可以跳过为目标映射地址添加对象的过程，并在规则中指定接口。

您还可以对源和/或目标执行端口转换。在对象管理器中，确保有可以用于原始端口和转换后的端口的端口对象。

过程

步骤 1 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

步骤 2 执行以下操作之一：

- 点击**添加规则 (Add Rule)** 按钮以创建新规则。
- 点击**编辑**（ ）以编辑现有规则。

右键点击菜单还具有用于剪切、复制、粘贴、插入和删除规则的选项。

步骤 3 配置基本规则选项：

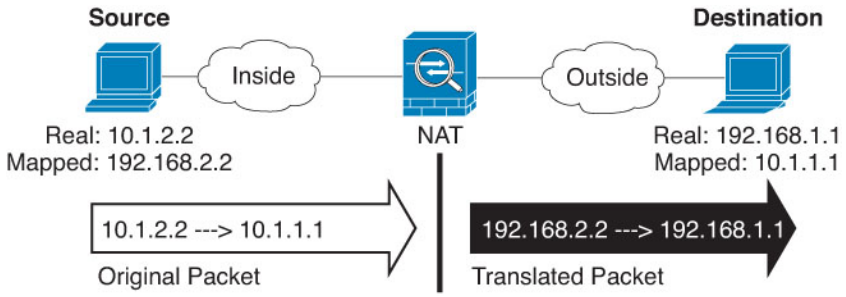
- **NAT 规则** - 选择**手动 NAT 规则**。
- **类型** - 选择**静态**。该设置仅应用于源地址。如果为目标地址定义转换，则该转换始终为静态。
- **启用** - 您是否希望规则处于活动状态。可以随后使用“规则”(Rules) 页面上的右键点击菜单激活或停用该规则。
- **插入** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后）或指定规则的上方或下方。

步骤 4 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象**、**目标接口对象** -（网桥组成员接口的必选项。）用于识别此 NAT 规则应用的接口的接口对象（安全区域或接口组）。**源**是包含实际接口的对象，流量通过该接口进入设备。**目标**是包含映射接口的对象，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 （在**转换**页面上。）确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例。



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

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

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源** - 以下项之一：
  - 要使用一组地址，请选择**地址**和包含映射地址的网络对象或组。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。
  - （具有端口转换的静态接口 NAT。）要使用目标接口的地址，请选择**目标接口 IP**。您还必须选择特定目标接口对象。要使用接口的 IPv6 地址，还必须在**高级 (Advanced)** 上选择 **IPv6** 选项。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。
- **转换后的目标** -（可选。）包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标**选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

步骤 7 （可选。）为服务转换确定源或目的服务端口。

如果要配置支持端口转换的静态 NAT，可以为源和/或目的转换端口。例如，可以在 TCP/80 和 TCP/8080 之间进行转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

- **原始源端口、转换后的源端口** - 定义源地址的端口转换。
- **原始目标端口、转换后的目标端口** - 定义目标地址的端口转换。

步骤 8 （可选。）在**高级 (Advanced)** 上选择所需选项：

- **转换与此规则相匹配的 DNS 应答** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对

于从实际接口传输到映射接口的DNS回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 760 页。 如果您在进行端口转换，则此选项不可用。

- **IPv6** - 是否为接口 PAT 使用目的地接口的 IPv6 地址。
- **网络到网络映射** - 对于 NAT 46，请选择此选项以将第一个 IPv4 地址转换为第一个 IPv6 地址，将第二个 IPv4 地址转换为第二个 IPv6 地址，依此类推。如不使用此选项，则将使用 IPv4 嵌入式方法。对于一对一转换，必须使用此选项。
- **请勿在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。
- **单向** - 选择此选项以阻止目标地址发起流向源地址的流量。单向选项主要用于测试目的，可能不适用于所有协议。例如，SIP 要求执行协议检查以使用 NAT 转换 SIP 报头，但如果将转换设为单向，则不会发生这种情况。

步骤 9 点击**保存**以添加规则。

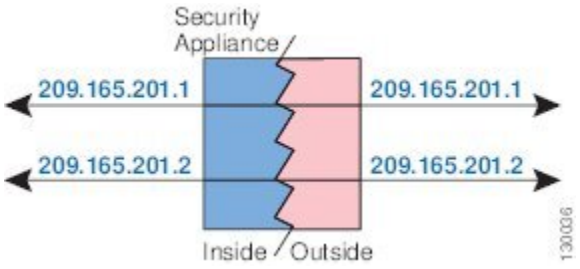
步骤 10 点击“NAT”页面上的**保存**以保存更改。

身份 NAT

可能有一个 NAT 配置，在其中需要将 IP 地址转换为其本身。例如，如果创建一条将 NAT 应用于每个网络的大体的规则，但想使一个网络免于 NAT，则可以创建一条静态 NAT 规则，以将地址转换为其本身。

下图显示典型的身份 NAT 场景。

图 *112: 身份 NAT*



以下主题介绍如何配置身份 NAT。

配置身份自动 NAT

使用静态身份自动 NAT 规则可防止地址转换。即，防止将地址转换为自身。

开始之前

选择**对象** > **对象管理**并创建规则中所需的网络对象或组。或者，您可以在定义 NAT 规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机、范围或子网。
- **转换后的源** - 其内容与原始源对象完全相同的网络对象或组。您可以使用相同的对象。

过程

步骤 1 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

步骤 2 执行以下操作之一：

- 点击**添加规则 (Add Rule)** 按钮以创建新规则。
- 点击**编辑**（ ）以编辑现有规则。

右键点击菜单还具有用于剪切、复制、粘贴、插入和删除规则的选项。

步骤 3 配置基本规则选项：

- **NAT 规则** - 选择**自动 NAT 规则**。
- **类型 (Type)** - 选择**静态 (Static)**。

步骤 4 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象**、**目标接口对象** -（网桥组成员接口的必选项。）用于识别此 NAT 规则应用的接口的接口对象（安全区域或接口组）。**源**是包含实际接口的对象，流量通过该接口进入设备。**目标**是包含映射接口的对象，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 在 **(General Translation)** 上配置以下选项：

- **原始源** - 包含您要转换的地址的网络对象。
- **转换后的源** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。

不要为身份 NAT 配置**原始端口**和**转换后的端口**选项。

步骤 6 （可选。）在**高级 (Advanced)** 上选择所需选项：

- **转换与此规则匹配的 DNS 回复** - 请勿为身份 NAT 配置此选项。
- **IPv6** - 请勿为身份 NAT 配置此选项。
- **网络到网络映射** - 请勿为身份 NAT 配置此选项。
- **不在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。

- **对目标接口执行路由查找** - 如果在为原始源地址和已转换源地址选择同一对象时选择源接口和目标接口，则可以选择此选项，以使系统根据路由表而不是使用在NAT规则中配置的目标接口来确定目标接口。

步骤 7 点击**保存**以添加规则。

步骤 8 点击“NAT”页面上的**保存**以保存更改。

配置身份手动 NAT

当自动 NAT 不能满足您的需求时，请使用静态身份手动 NAT 规则。例如，如果您要根据目标进行不同的转换。使用静态身份 NAT 规则可防止地址转换。即，防止将地址转换为自身。

开始之前

依次选择**对象** > **对象管理**，然后创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- **原始源** - 此选项可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定**任何 (Any)**。
- **转换后的源** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。

如果要在规则中为**原始目标**和**转换后的目标**地址配置静态转换，则还可以为这些地址创建网络对象。如果只需要配置支持端口转换的目标静态接口 NAT，则可以跳过为目标映射地址添加对象的过程，并在规则中指定接口。

您还可以对源和/或目标执行端口转换。在对象管理器中，确保有可以用于原始端口和转换后的端口的端口对象。您可以为身份 NAT 使用相同的对象。

过程

步骤 1 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

步骤 2 执行以下操作之一：

- 点击**添加规则 (Add Rule)** 按钮以创建新规则。
- 点击**编辑**（ ）以编辑现有规则。

右键点击菜单还具有用于剪切、复制、粘贴、插入和删除规则的选项。

步骤 3 配置基本规则选项：

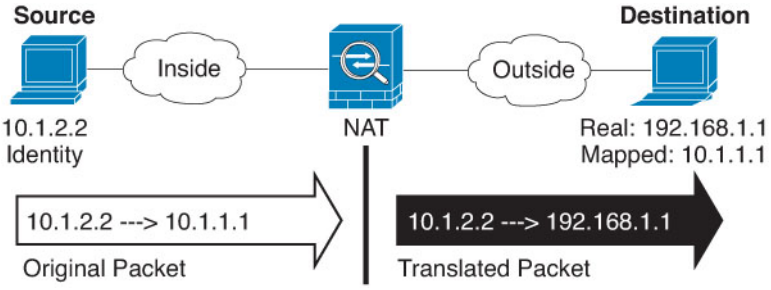
- **NAT 规则** - 选择**手动 NAT 规则**。
- **类型** - 选择**静态**。该设置仅应用于源地址。如果为目标地址定义转换，则该转换始终为静态。
- **启用** - 您是否希望规则处于活动状态。可以随后使用“规则”(Rules) 页面上的右键点击菜单激活或停用该规则。
- **插入** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后）或指定规则的上方或下方。

步骤 4 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象**、**目标接口对象** - （网桥组成员接口的必选项。）用于识别此 NAT 规则应用的接口的接口对象（安全区域或接口组）。**源**是包含实际接口的对象，流量通过该接口进入设备。**目标**是包含映射接口的对象，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例，其中在内部主机上执行身份 NAT，但转换外部主机。



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

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

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。
- **转换后的目标** -（可选。）包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标**选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

步骤 7 （可选。）为服务转换确定源或目的服务端口。

如果要配置支持端口转换的静态 NAT，可以为源和/或目的转换端口。例如，可以在 TCP/80 和 TCP/8080 之间进行转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

- **原始源端口**、**转换后的源端口** - 定义源地址的端口转换。
- **原始目标端口**、**转换后的目标端口** - 定义目标地址的端口转换。

步骤 8 （可选。）在**高级 (Advanced)** 上选择所需选项：

- **转换与此规则匹配的 DNS 回复** - 请勿为身份 NAT 配置此选项。
- **IPv6** - 是否为接口 PAT 使用目的地接口的 IPv6 地址。
- **不在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。
- **对目标接口执行路由查找** - 如果在为原始源地址和已转换源地址选择同一对象时选择源接口和目标接口，则可以选择此选项，以使系统根据路由表而不是使用在NAT规则中配置的目标接口来确定目标接口。
- **单向** - 选择此选项以阻止目标地址发起流向源地址的流量。单向选项主要用于测试目的，可能不适用于所有协议。例如，SIP 要求执行协议检查以使用 NAT 转换 SIP 报头，但如果将转换设为单向，则不会发生这种情况。

步骤 9 点击**保存**以添加规则。

步骤 10 点击“NAT”页面上的**保存**以保存更改。

威胁防御 的 NAT 规则属性

使用网络地址转换 (NAT) 规则将 IP 地址转换为其他 IP 地址。通常使用 NAT 规则将私有地址转换为可公开路由的地址。可以将一个地址转换成另一个地址，或可以使用端口地址转换 (PAT) 将多个地址转换为一个或几个地址，并使用端口号区分源地址。

NAT 规则包括以下基本属性。自动 NAT 和手动 NAT 规则的属性相同，除非另行指明。

NAT 类型

是否要配置**手动 NAT 规则**或**自动 NAT 规则**。自动 NAT 仅转换源地址，不能根据目标地址进行不同的转换。因为自动 NAT 更易于配置，因此除非需要手动 NAT 的附加功能，可以使用自动 NAT。有关两者区别的详细信息，请参阅自动 NAT 和手动 NAT ，第 667 页。

类型

转换规则是**动态**还是**静态**。在实施PAT时，动态转换会自动从地址池中选择映射的地址或地址/端口组合。如果要精确定义映射的地址/端口，请使用静态转换。

启用（仅限手动 NAT。）

您是否希望规则处于活动状态。可以随后使用“规则”(Rules) 页面上的右键点击菜单激活或停用该规则。不能禁用自动 NAT 规则。

插入（仅限手动 NAT。）

要添加规则的位置。可以将其插入类别中（在自动NAT规则之前或之后）或指定规则的上方或下方。

说明（可选。仅手动 NAT。)

规则的用途说明。

以下主题介绍 NAT 规则属性的选项卡。

接口对象 NAT 属性

接口对象（安全区或接口组）定义适用NAT规则的接口。在路由模式下，可将默认值“任何”同时用于源和目标，以适用于所有已分配设备的所有接口。但您通常希望选择特定的源和目标接口。

注释 “任何”接口的概念并不适用于桥接组成员接口。当指定“任何”接口时，NAT 将排除所有网桥组成员接口。因此，要将 NAT 应用于网桥组成员，必须指定成员接口。您不能为桥接虚拟接口 (BVI) 本身配置 NAT，只能为成员接口配置 NAT。

如果选择多个接口对象，则仅当某一已分配的设备上具有包括在所有选定对象中的接口时，才会在该设备上配置NAT规则。例如，如果同时选择了源安全区和目标安全区，则这两个区域必须同时包含一个或多个用于指定设备的接口。

源接口对象、目标接口对象

（网桥组成员接口的必选项。）用于识别此NAT规则应用的接口的接口对象（安全区域或接口组）。**源**是包含实际接口的对象，流量通过该接口进入设备。**目标**是包含映射接口的对象，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

自动 NAT 的转换属性

使用**转换 (Translation)** 上的选项可以定义源地址和映射的转换后的地址。以下属性仅适用于自动 NAT。

原始源（始终为必填项）。

包含您要转换的地址的网络对象。该地址必须是网络对象（而非组），而且可以是主机、范围或子网。

您不能为系统定义的 any-ipv4 或 any-ipv6 对象创建自动 NAT 规则。

转换后的源（通常为必填项）。

您要转换到的映射地址。您在此处选择的选项取决于定义的转换规则类型。

- **动态 NAT** - 包含映射地址的网络对象或组。该地址可以是网络对象或组，但是它不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。如果某个组同时包含范围和主机 IP 地址，则范围将用于动态 NAT，主机 IP 地址将用作 PAT 回退。
- **动态 PAT** - 以下项之一：
  - （接口 PAT。）要使用目标接口的地址，请选择**目标接口 IP**。您还必须选择特定目标接口对象。要使用接口的 IPv6 地址，还必须在**高级 (Advanced)** 上选择 **IPv6** 选项。请勿配置 PAT 池。
  - 要使用目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。请勿配置 PAT 池。

- 要使用 PAT 池，请将**转换后的源**保留为空。在 **PAT 池 (PAT Pool)** 上选择 PAT 池对象。

- **静态 NAT** - 以下项之一：
  - 要使用一组地址，请选择**地址**和包含映射地址的网络对象或组。该对象或组可以包含主机、范围或子网。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。
  - （具有端口转换的静态接口 NAT。）要使用目标接口的地址，请选择**目标接口 IP**。您还必须选择特定目标接口对象。要使用接口的 IPv6 地址，还必须在**高级**选项卡上选择 **IPv6** 选项。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。

- **身份 NAT** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。

原始端口、转换后的端口（仅静态 NAT）。

如果需要转换 TCP 或 UDP 端口，请在**原始端口**中选择协议，并输入原始和转换端口编号。例如，如有必要，可以将 TCP/80 转换为 8080。不要为身份 NAT 配置这些选项。

手动 NAT 的转换属性

使用**转换 (Translation)** 上的选项可以定义源地址和映射的转换后的地址。以下属性仅适用于手动 NAT。所有选项均为可选，除非另行指明。

原始源（始终为必填项）。

包含您要转换的地址的网络对象或组。该地址可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以在规则中指定**任何**。

转换后的源（通常为必填项）。

您要转换到的映射地址。您在此处选择的选项取决于定义的转换规则类型。

- **动态 NAT** - 包含映射地址的网络对象或组。该地址可以是网络对象或组，但是它不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。如果某个组同时包含范围和主机 IP 地址，则范围将用于动态 NAT，主机 IP 地址将用作 PAT 回退。

- **动态 PAT** - 以下项之一：
  - （接口 PAT。）要使用目标接口的地址，请选择**目标接口 IP**。您还必须选择特定目标接口对象。要使用接口的 IPv6 地址，还必须在**高级 (Advanced)** 上选择 **IPv6** 选项。请勿配置 PAT 池。
  - 要使用目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。请勿配置 PAT 池。
  - 要使用 PAT 池，请将**转换后的源**保留为空。在 **PAT 池 (PAT Pool)** 上选择 PAT 池对象。

- **静态 NAT** - 以下项之一：

- 要使用一组地址，请选择**地址**和包含映射地址的网络对象或组。该对象或组可以包含主机、范围或子网。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。
- （具有端口转换的静态接口 NAT。）要使用目标接口的地址，请选择**目标接口 IP**。您还必须选择特定目标接口对象。要使用接口的 IPv6 地址，还必须在**高级**选项卡上选择 **IPv6** 选项。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。

- **身份 NAT** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。

原始目标

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

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

转换目标

包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标**选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

您可以使用指定完全限定域名作为转换目的的网络对象；有关更多信息，请参阅 FQDN 目的准则，第 675 页。

原始源端口、转换后的源端口、原始目标端口、转换后的目标端口

为原始和转换后的数据包定义源和目标服务的端口对象。您可以转换端口，或者选择同一对象以便在没有转换端口的情况下使规则敏感察觉到该服务。在配置服务时请记住以下规则：

- （动态 NAT 或 PAT。）不能对**原始源端口**和**转换后的源端口**进行转换。您可以仅对目标端口进行转换。
- NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

PAT 池 NAT 属性

在配置动态 NAT 时，可以定义一个地址池，以用于使用 **PAT 池**选项卡上的属性的“端口地址转换”。

启用 PAT 池

选择此选项可为 PAT 配置一个地址池。

PAT

用于以下 PAT 池之一的地址：

- **地址** - 定义 PAT 池地址的对象，或者是包括某一范围的网络对象，或者是包含主机、范围或二者的网络对象组。不能包括子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。
- **目标接口 IP** - 指示您希望将目标接口用作 PAT 地址。对于此选项，必须选择某一特定**目标接口对象**；不能将**任何**用作目标接口。这是实施接口 PAT 的另一种方法。

循环法

以轮询方式分配地址/端口。默认情况下，如果不采用轮询，在使用下一个 PAT 地址之前，将分配 PAT 地址的所有端口。轮询方法分配来自池中每个 PAT 地址的一个地址/端口，然后才返回再次使用第一个地址，接着是第二个地址，以此类推。

扩展 PAT 表

使用扩展 PAT。通过将目的地地址和端口纳入转换信息，相对于按 IP 地址，扩展 PAT 将按服务使用 65535 个端口。通常，创建 PAT 转换时，不考虑目的地端口和地址，因此限制为每个 PAT 地址 65535 个端口。例如，通过扩展 PAT，您可以创建在访问 192.168.1.7:23 时转到 10.1.1.1:1027 的转换，以及在访问 192.168.1.7:80 时转到 10.1.1.1:1027 的转换。不能将此选项用于接口 PAT 或接口 PAT 回退。

不分段端口范围；包括保留端口

在分配 TCP/UDP 端口时使用 1024 到 65535 的端口范围作为单个扁平范围。（6.7 以下版本）为转换选择映射端口号时，PAT 使用实际源端口号（若可用）。然而，如果不使用此选项，则当实际端口不可用时，将默认从与实际端口号相同的端口范围选择映射端口：1 到 511、512 到 1023 以及 1024 到 65535。为了避免用尽低端口号范围的端口，请配置此设置。要使用 1 到 65535 的整个范围，另请勾选**包括保留端口 (Include Reserved Ports)** 选项。对于运行版本 6.7 或更高版本的威胁防御设备，无论是否选择该选项，始终配置扁平端口范围。您仍可以为这些系统选择**包括保留端口 (Include Reserved Ports)** 选项，并且系统将采用该设置。

阻止分配

启用端口块分配。对于运营商级或大规模 PAT，可以为每个主机分配一个端口块，而非由 NAT 每次分配一个端口转换。如果分配端口块，来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中，可根据需要分配更多块。只能在 1024-65535 范围内分配端口块。端口块分配与轮询兼容，但无法将其与扩展 PAT 或不分段端口范围选项一起使用。也无法使用接口 PAT 回退。

高级 NAT 属性

在配置 NAT 时，可以在**高级**选项中配置提供专业化服务的属性。所有这些属性都是可选的：仅当需要服务时才对其进行配置。

转换与此规则匹配的 DNS 回复

是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的 DNS 回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 760 页。 如果在静态 NAT 规则中进行端口转换，则此选项不可用。

贯穿到接口 PAT（目标接口）（仅动态 NAT。）

当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。要使用接口的 IPv6 地址，另请勾选 **IPv6** 选项。如果已配置了接口 PAT 配置作为转换的地址，则不能选择此选项。另外，配置 PAT 池时也不能选择此选项。

IPv6

是否为接口 PAT 使用目的地接口的 IPv6 地址。

网络到网络映射（仅静态 NAT）。

对于 NAT 46，请选择此选项以将第一个 IPv4 地址转换为第一个 IPv6 地址，将第二个 IPv4 地址转换为第二个 IPv6 地址，依此类推。如不使用此选项，则将使用 IPv4 嵌入式方法。对于一对一转换，必须使用此选项。

不在目标接口上使用代理 ARP（仅静态 NAT。）

为映射IP地址的传入数据包禁用代理ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理ARP，在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。

对目标接口执行路由查找（仅静态身份 NAT。仅路由模式。）

如果在为原始源地址和已转换源地址选择同一对象时选择源接口和目标接口，则可以选择此选项，以使系统根据路由表而不是使用在 NAT 规则中配置的目标接口来确定目标接口。

单向（仅手动 NAT，仅静态 NAT。）

选择此选项以阻止目标地址发起流向源地址的流量。单向选项主要用于测试目的，可能不适用于所有协议。例如，SIP要求执行协议检查以使用NAT转换SIP报头，但如果将转换设为单向，则不会发生这种情况。

转换 IPv6 网络

当需要在仅 IPv6 网络和仅 IPv4 网络之间传递流量时，需要使用 NAT 在地址类型之间进行转换。即使两个都是 IPv6 网络，您也可能需要对外部网络隐藏内部地址。

对于 IPv6 网络，您可以使用以下转换类型：

- NAT64、NAT46 - 将 IPv6 数据包转换成 IPv4 数据包，反之亦然。您需要定义两个策略，一个用于 IPv6 向 IPv4 的转换，另一个用于 IPv4 向 IPv6 的转换。虽然您可以使用单一 手动 NAT 规则完成此任务，但如果 DNS 服务器位于外部网络，则可能需要重写 DNS 响应。由于在指定了目标的情况下，无法在手动 NAT 规则中启用 DNS 重写，所以最好创建两个自动 NAT 规则。

注释 NAT46 仅支持静态映射。

- NAT66 - 将 IPv6 数据包转换为不同的 IPv6 地址。我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。

注释 NAT64 和 NAT 46 仅可以在标准路由接口上使用。NAT66 可在路由接口和网桥组成员接口上使用。

NAT64/46：将 IPv6 地址转换为 IPv4 地址

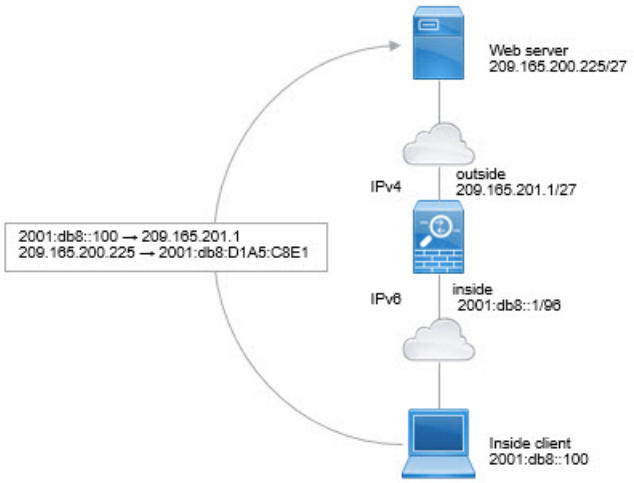
当流量从 IPv6 网络进入仅 IPv4 网络时，您需要将 IPv6 地址转换为 IPv4 地址，并将流量从 Ipv4 返回 IPv6。您需要定义两个地址池，一个 IPv4 地址池用于绑定 IPv4 网络中的 IPv6 地址，另一个 IPv6 地址池用于绑定 IPv6 网络中的 IPv4 地址。

- NAT64 规则的 IPv4 地址池一般较小，通常可能没有足够的地址与 IPv6 客户端地址一对一映射。与动态或静态 NAT 相比，动态 PAT 可以更容易满足可能的大量 IPv6 客户端地址需要。
- NAT46 规则的 IPv6 地址池可以等于或大于要映射的 IPv4 地址数。这允许每个 IPv4 地址映射到不同的 IPv6 地址。NAT46 仅支持静态映射，因此您不能使用动态 PAT。

您需要定义两个策略，一个用于源 IPv6 网络，一个用于目标 IPv4 网络。虽然您可以使用单一 手动 NAT 规则完成此任务，但如果 DNS 服务器位于外部网络，则可能需要重写 DNS 响应。由于在指定了目标的情况下，无法在手动 NAT 规则中启用 DNS 重写，所以最好创建两个自动 NAT 规则。

NAT64/46 示例：内部 IPv6 网络与外部 IPv4 互联网

以下是一个非常简单的示例，假设您具有仅包含 IPv6 的内部网络，且您希望将发送到互联网的流量转换为 IPv4。此示例假定您无需 DNS 转换，以便可以在单个手动 NAT 规则中执行 NAT64 和 NAT46 转换。



在本例中，借助外部接口的 IP 地址，使用动态接口 PAT 将内部 IPv6 网络转换为 IPv4。将外部 IPv4 流量静态转换为 2001:db8::/96 网络中的地址，允许在内部网络中传输。

过程

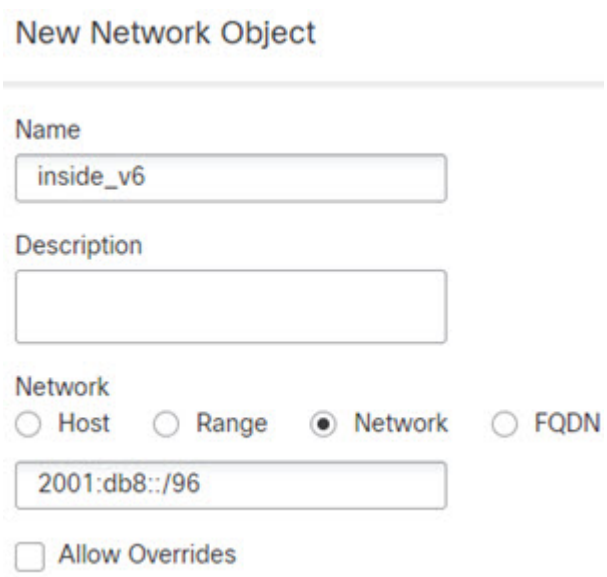
步骤 1 创建定义内部 IPv6 网络的网络对象。

a) 选择**对象** > **对象管理**。

b) 从目录中选择**网络 (Network)** 并点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

c) 定义内部 IPv6 网络。

为网络对象命名（例如，inside_v6），然后输入网络地址 2001:db8::/96。



d) 点击**保存 (Save)**。

步骤 2 创建手动 NAT 规则以将 IPv6 网络转换为 IPv4 并再次返回。

a) 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

- **NAT 规则** = 手动 NAT 规则。
- **类型 (Type)**= 动态。

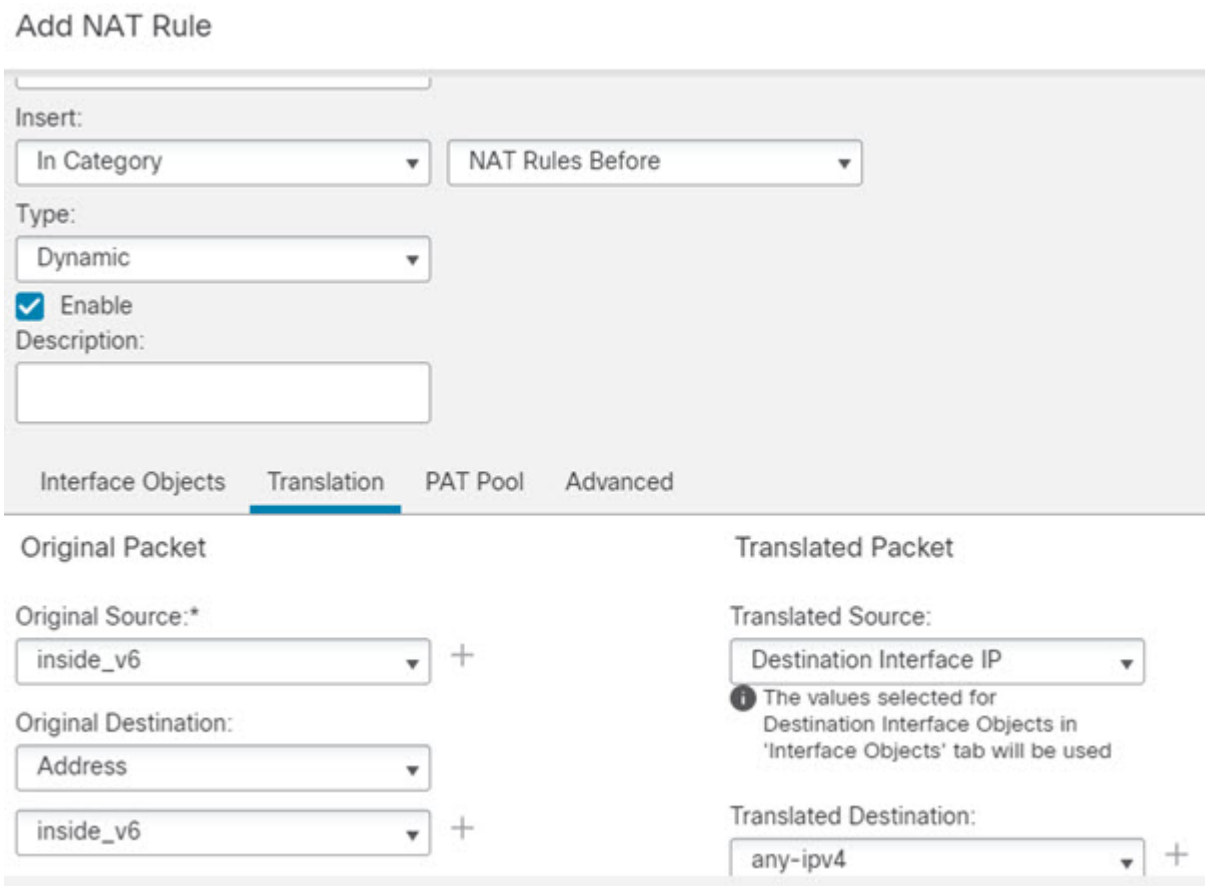
d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = inside_v6 网络对象。
- **已转换的源** = **目标接口 IP**。

- 原始目标 **(Original Destination)** = inside_v6 网络对象。
- 转换后的目标 **(Translated Destination)** = any-ipv4 网络对象。



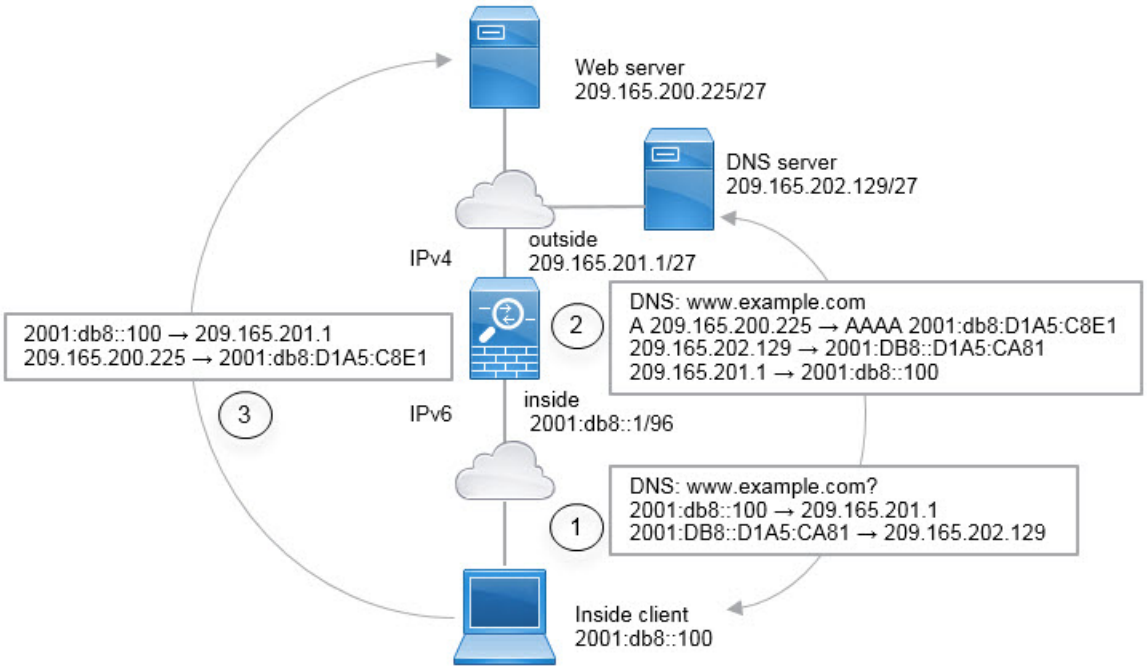
f) 点击**确定**。

使用此规则时，从内部接口上的 2001:db8::/96 子网流向外部接口的任何流量都将接受使用外部接口 IPv4 地址进行的 NAT64 PAT 转换。相反，外部网络中的任何 IPv4 地址到达内部接口，都将使用嵌入式 IPv4 地址方法转换为 2001:db8::/96 网络中的一个地址。

g) 点击 NAT 规则页面上的**保存 (Save)**。

NAT64/46 示例：包含外部 IPv4 互联网和 DNS 转换的内部 IPv6 网络

下面是一个典型的示例：内部网络只支持 IPv6，但外部互联网上有一些内部用户所需的服务只支持 IPv4。



在本例中，借助外部接口的 IP 地址，使用动态接口 PAT 将内部 IPv6 网络转换为 IPv4。将外部 IPv4 流量静态转换为 2001:db8::/96 网络中的地址，允许在内部网络中传输。对 NAT46 规则启用 DNS 重写，使外部 DNS 服务器的回复可以从 A (IPv4) 记录转换为 AAAA (IPv6) 记录，地址也能从 IPv4 地址转换为 IPv6 地址。

当内部 IPv6 网络中地址为 2001:DB8::100 的客户端尝试打开 www.example.com 时，此 Web 请求的典型顺序如下。

1. 客户端的计算机向地址为 2001:DB8::D1A5:CA81 的 DNS 服务器发送 DNS 请求。NAT 规则对 DNS 请求中的源和目的进行以下转换：
   - 2001:DB8::100 转换为 209.165.201.1 上的唯一端口（NAT64 接口 PAT 规则。）
   - 2001:DB8::D1A5:CA81 转换为 209.165.202.129（NAT46 规则。）D1A5:CA81 是 209.165.202.129 的 IPv6 对应物。）
2. DNS 服务器以 A 记录进行响应，指出 www.example.com 位于 209.165.200.225。NAT46 规则（已启用 DNS 重写）将 A 记录转换为 IPv6 对应物 AAAA 记录，并在 AAAA 记录中将 209.165.200.225 转换为 2001:db8:D1A5:C8E1。此外，DNS 响应中的源地址和目标地址未转换：
   - 209.165.202.129 转换为 2001:DB8::D1A5:CA81
   - 209.165.201.1 转换为 2001:db8::100
3. IPv6 客户端现在有 Web 服务器的 IP 地址，于是向位于 2001:db8:D1A5:C8E1 的 www.example.com 发出 HTTP 请求。（D1A5:C8E1 是 209.165.200.225 的 IPv6 对应物。）HTTP 请求中的源和目的进行转换：
   - 2001:DB8::100 转换为 209.156.101.54 上的唯一端口（NAT64 接口 PAT 规则。）

- 2001:db8:D1A5:C8E1 转换为 209.165.200.225（NAT46 规则。）

以下步骤程序介绍了如何配置此示例。

开始之前

确保具有包含用于设备的接口的接口对象（安全区或接口组）。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请依次选择**对象** > **对象管理**，然后选择**接口**。

过程

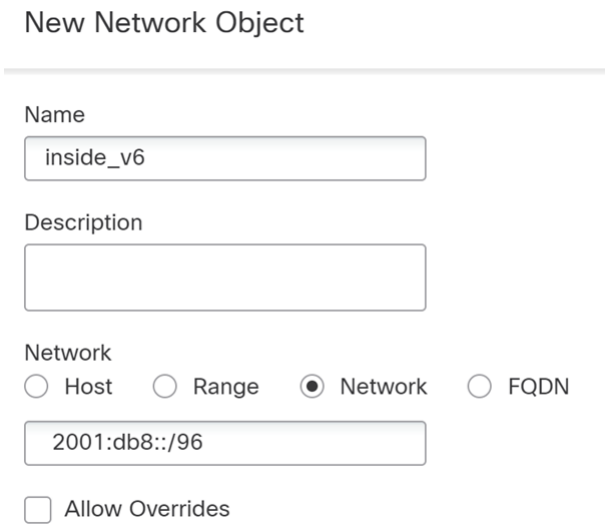
步骤 1 创建定义内部 IPv6 网络和外部 IPv4 网络的网络对象。

a) 选择**对象** > **对象管理**。

b) 从目录中选择**网络 (Network)** 并点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

c) 定义内部 IPv6 网络。

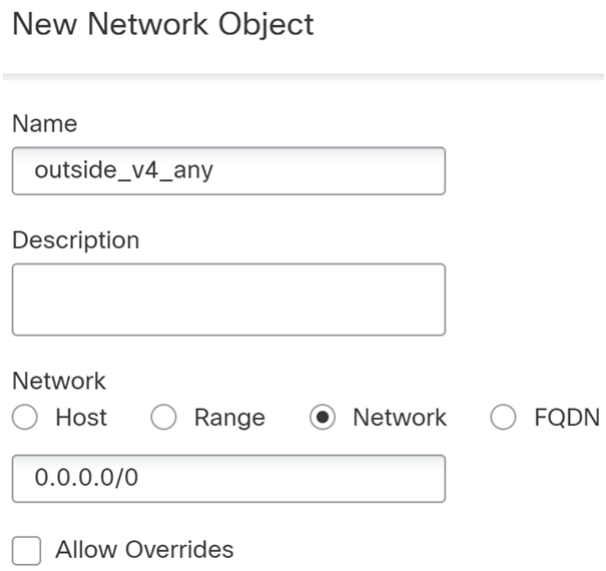
为网络对象命名（例如，inside_v6），然后输入网络地址 2001:db8::/96。



d) 点击**保存 (Save)**。

e) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**并定义外部 IPv4 网络。

为网络对象命名（例如，outside_v4_any），然后输入网络地址 0.0.0.0/0。



f) 点击**保存 (Save)**。

步骤 2 为内部 IPv6 网络配置 NAT64 动态 PAT 规则。

步骤 3 为外部 IPv4 网络配置静态 NAT46 规则。

a) 点击**添加规则**。

b) 配置以下属性：

- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型** = 静态。

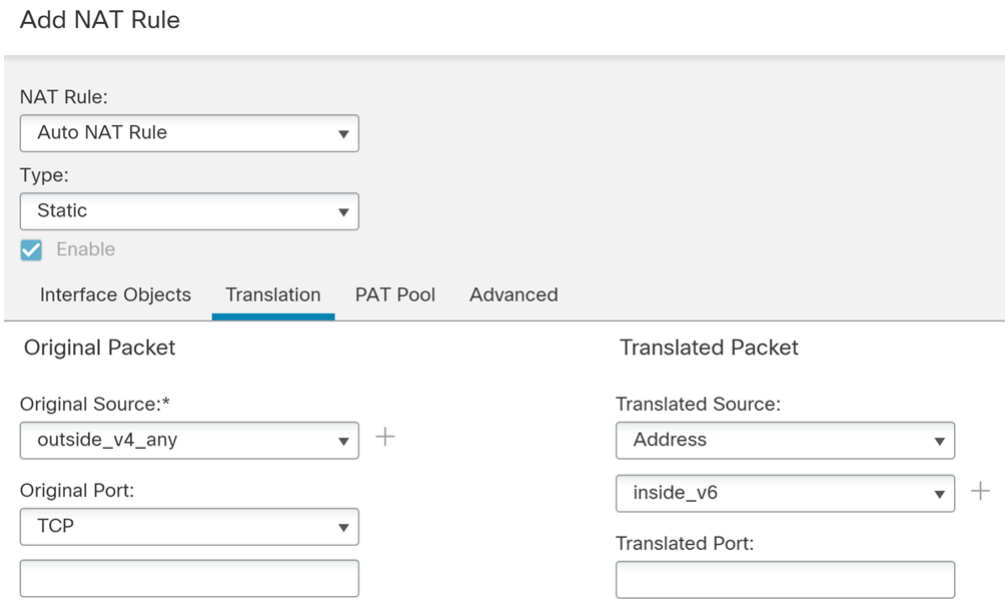
c) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 外部。
- **目标接口对象** = 内部。

d) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = outside_v4_any 网络对象。
- **转换后的源** > **地址 (Translated Source Address)** = inside_v6 网络对象。

e) 在**高级 (Advanced)** 选项卡上，选择**转换与此规则匹配的 DNS 回复 (Translate DNS replies that match this rule)**。



f) 点击**确定**。

使用此规则时，外部网络中的任何 IPv4 地址到达内部接口，都将使用嵌入式 IPv4 地址方法转换为 2001:db8::/96 网络中的一个地址。此外，DNS 响应从 A (IPv4) 记录转换为 AAAA (IPv6) 记录，其地址也从 IPv4 地址转换为 IPv6 地址。

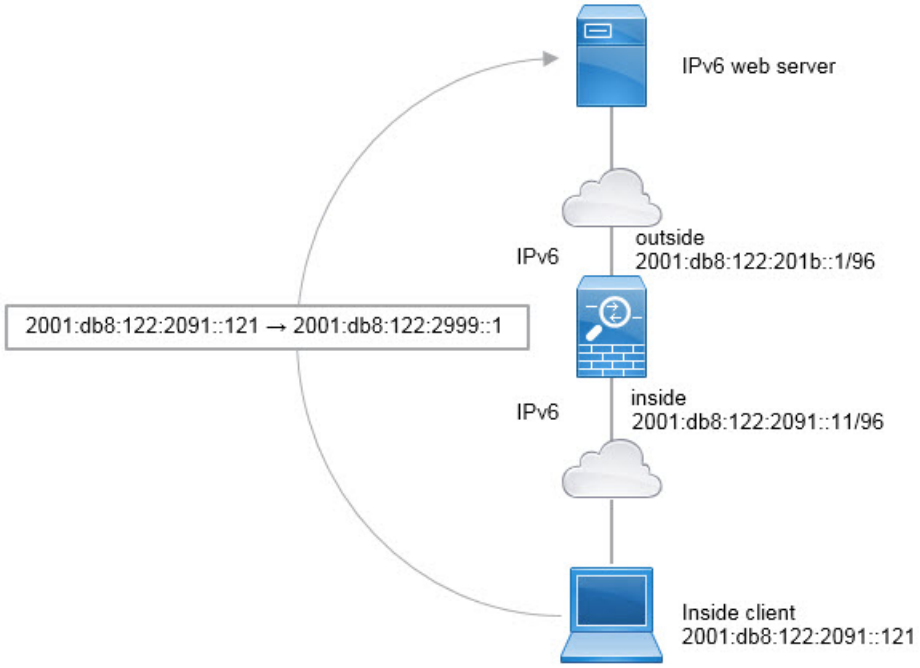
NAT66：将 IPv6 地址转换为不同的 IPv6 地址

当从一个 IPv6 网络进入另一个 IPv6 网络时，您可以将地址转换为外部网络上的不同 IPv6 地址。我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。

因为您不是在不同的地址类型之间转换，所以您需要一个单一的 NAT66 转换规则。使用自动 NAT 可轻松地为这些规则建模。但是，如果不想允许返回流量，您可以仅使用手动 NAT 将静态 NAT 规则设为单向。

NAT66 示例：网络间的静态转换

您可以使用自动 NAT 在 IPv6 地址池之间配置静态转换。以下示例说明如何将 2001:db8:122:2091::/96 网络中的内部地址转换为 2001:db8:122:2999::/96 网络中的外部地址。



开始之前

确保具有包含用于设备的接口的接口对象（安全区或接口组）。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请依次选择**对象** > **对象管理**，然后选择**接口**。

过程

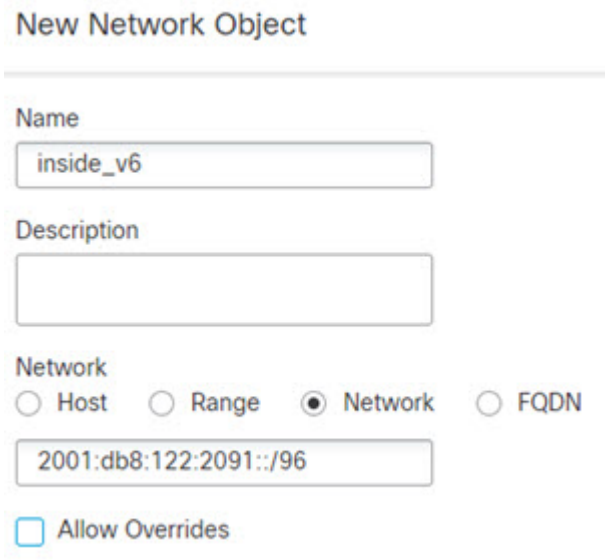
步骤 1 创建定义内部 IPv6 网络和外部 IPv6 NAT 网络的网络对象。

a) 选择**对象** > **对象管理**。

b) 从目录中选择**网络 (Network)** 并点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

c) 定义内部 IPv6 网络。

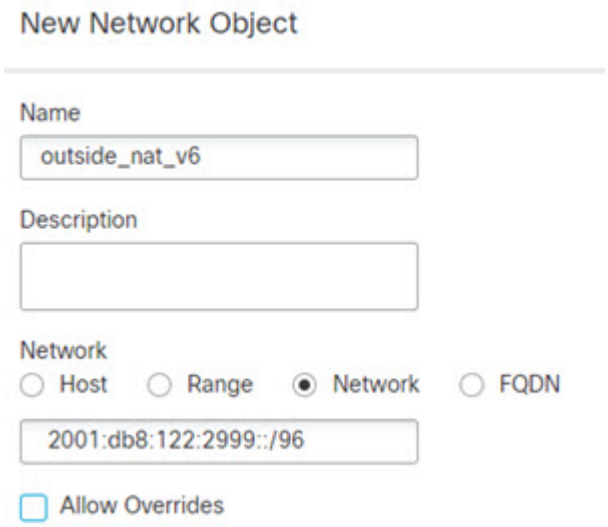
为网络对象命名（例如，inside_v6），然后输入网络地址 2001:db8:122:2091::/96。



d) 点击**保存 (Save)**。

e) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)** 并定义外部 IPv6 NAT 网络。

为网络对象命名（例如，outside_nat_v6），然后输入网络地址 2001:db8:122:2999::/96。



f) 点击**保存 (Save)**。

步骤 2 为内部 IPv6 网络配置静态 NAT 规则。

a) 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

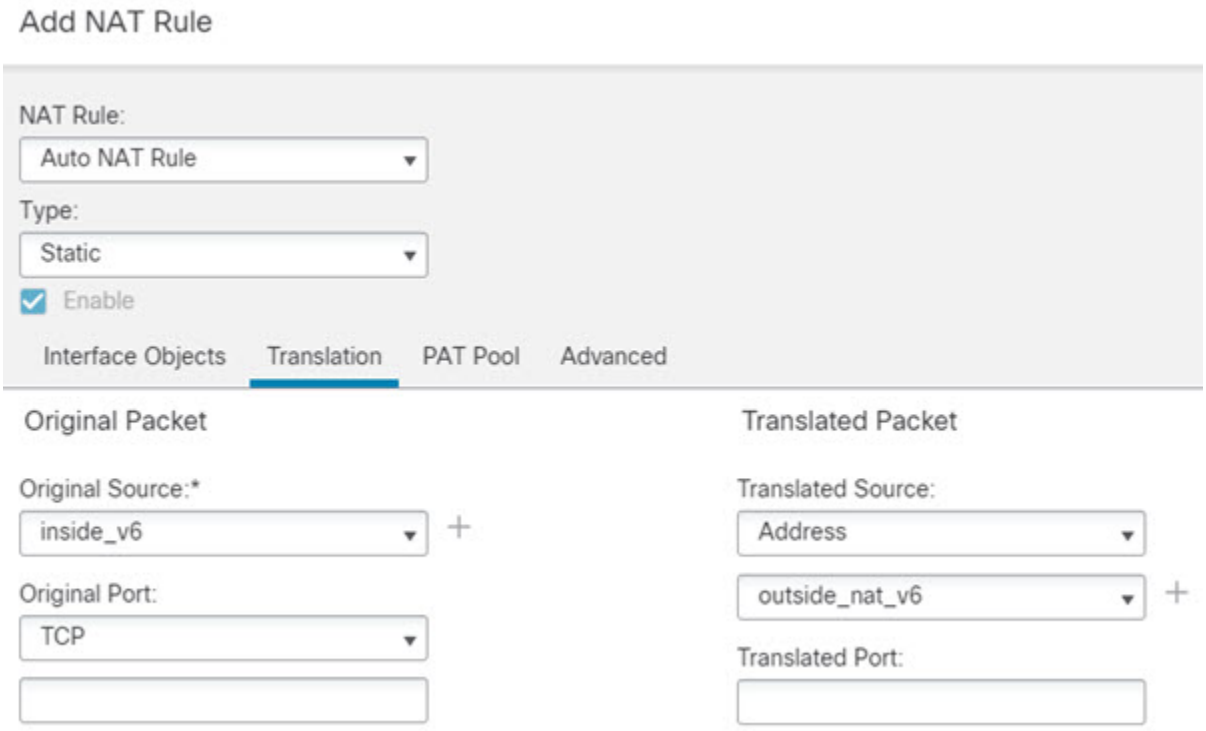
- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型** = 静态。

d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = inside_v6 网络对象。
- **转换后的源** > **地址 (Translated Source Address)** = outside_nat_v6 网络对象。



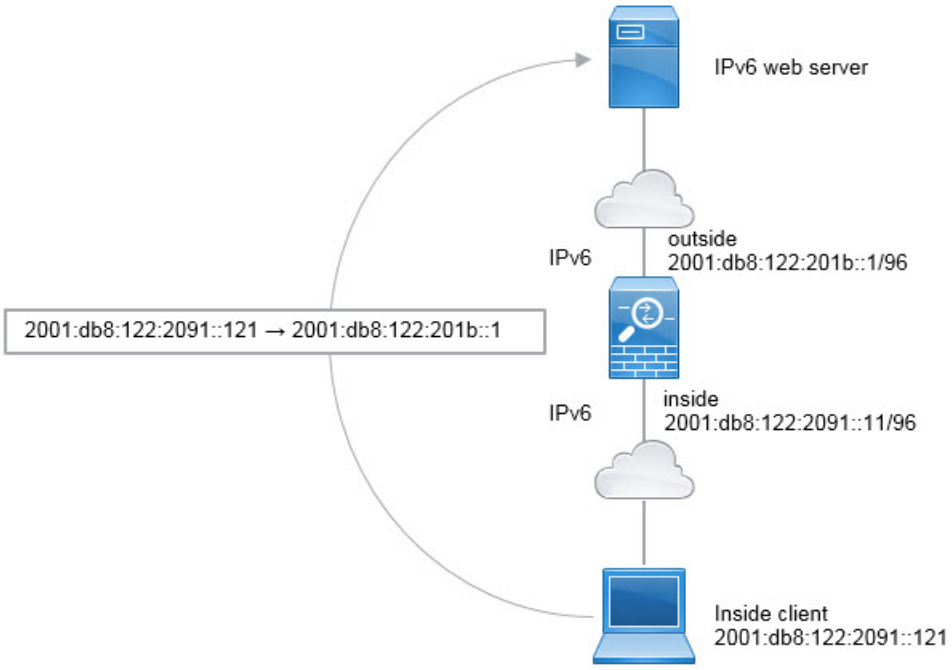
f) 点击**确定**。

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

NAT66 示例：简单 IPv6 接口 PAT

实施 NAT66 的一个简单方法是将内部地址动态分配给外部接口 IPv6 地址上的不同端口。

为 NAT66 配置接口 PAT 规则时，该接口上配置的所有全局地址均用于 PAT 映射。该接口的链路本地地址或站点本地地址不用于 PAT。



开始之前

确保具有包含用于设备的接口的接口对象（安全区或接口组）。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请依次选择**对象** > **对象管理**，然后选择**接口**。

过程

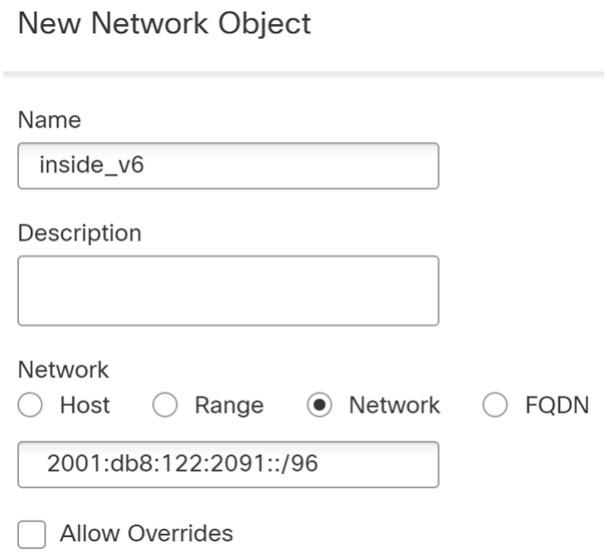
步骤 1 创建定义内部 IPv6 网络的网络对象。

a) 选择**对象** > **对象管理**。

b) 从目录中选择**网络 (Network)** 并点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

c) 定义内部 IPv6 网络。

为网络对象命名（例如，inside_v6），然后输入网络地址 2001:db8:122:2091::/96。



d) 点击**保存 (Save)**。

步骤 2 为内部 IPv6 网络配置动态 PAT 规则。

a) 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型 (Type)**= 动态。

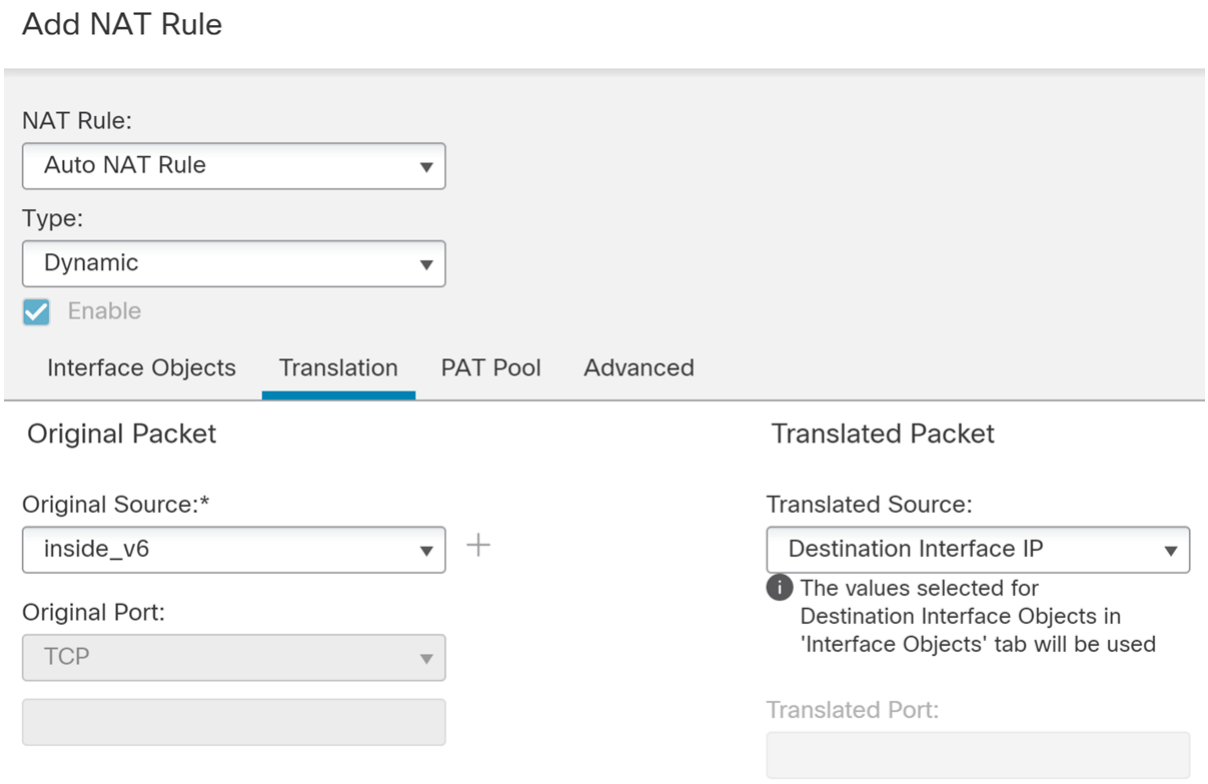
d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = inside_v6 网络对象。
- **已转换的源** = **目标接口 IP**。

f) 在**高级 (Advanced)** 选项卡上，选择 **IPv6**，指示应使用的目标接口 IPv6 地址。



g) 点击 **OK**。

使用此规则，从内部接口的 2001:db8:122:2091::/96 子网到外部接口的任何流量均会通过 NAT66 PAT 转换为为外部接口配置的 IPv6 全局地址之一。

监控 NAT

要对 NAT 连接进行监控和故障排除，请登录设备 CLI 并使用以下命令。

- **show nat** 显示 NAT 规则和每个规则的命中计数。还有其他关键字可用于显示 NAT 的其他方面信息。
- **show xlate** 显示当前处于活动状态的实际 NAT 转换。
- **clear xlate** 允许删除处于活动状态的 NAT 转换。如果更改 NAT 规则，您可能需要删除活动的转换，因为现有连接继续使用旧的转换槽，直到连接结束。清除转换允许系统根据您的新规则，在客户端的下一次连接尝试中为客户端构建新的转换。

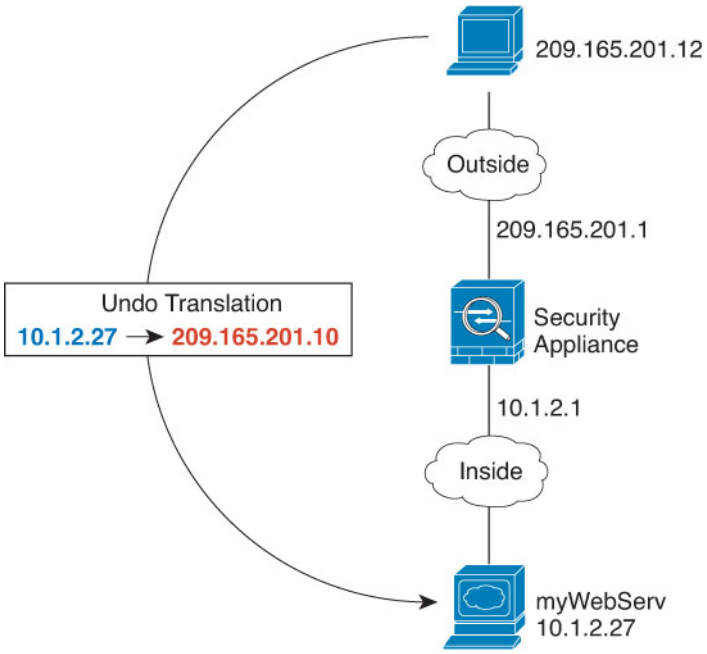
NAT 示例

以下主题提供了在威胁防御设备上配置 NAT 的示例。

提供对内部 Web 服务器的访问权限（静态自动 NAT）

以下示例为内部 Web 服务器执行静态 NAT。实际地址位于专用网络上，因此公共地址是必需的。需要静态 NAT，以便主机能够在固定地址发起到 Web 服务器的流量。

图 *113:* 面向内部 *Web* 服务器的静态 *NAT*



开始之前

确保存在包含保护 Web 服务器的设备接口的接口对象（安全区域或接口组）。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请依次选择**对象** > **对象管理**，然后选择**接口**。

过程

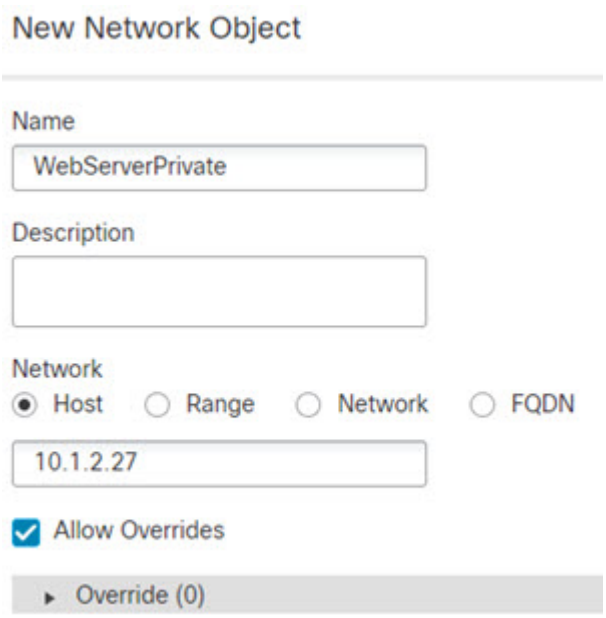
步骤 1 创建定义服务器私有和公共主机地址的网络对象。

a) 选择**对象** > **对象管理**。

b) 从目录中选择**网络 (Network)** 并点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

c) 定义 Web 服务器的私有地址。

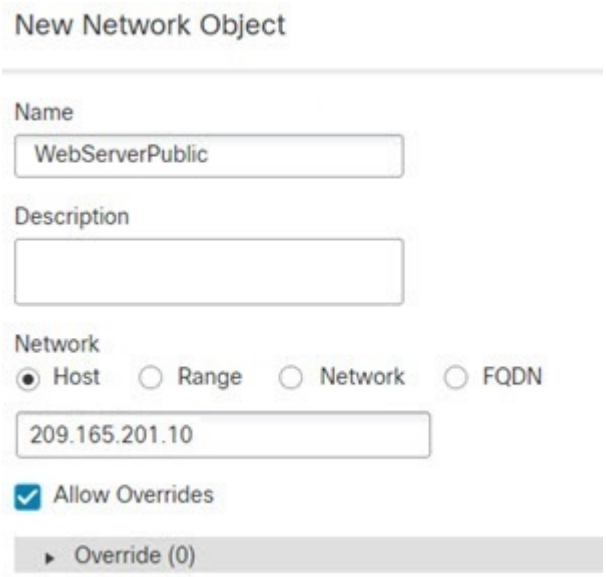
为网络对象命名（例如，WebServerPrivate），然后输入实际主机 IP 地址 10.1.2.27。



d) 点击**保存 (Save)**。

e) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)** 并定义公共地址。

为网络对象命名（例如，WebServerPublic），并输入主机地址 209.165.201.10。



f) 点击**保存 (Save)**。

步骤 2 配置对象的静态 NAT。

a) 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

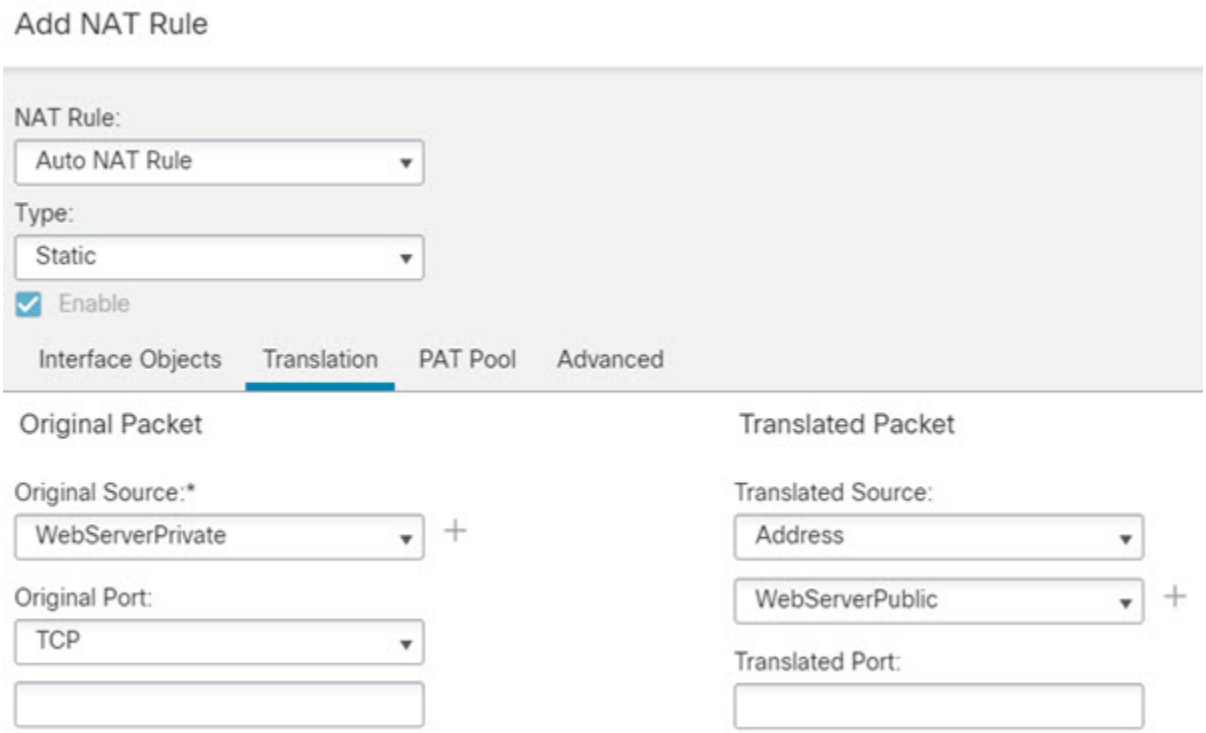
- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型** = 静态。

d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = WebServerPrivate 网络对象。
- **转换后的源 > 地址 (Translated Source Address)** = WebServerPublic 网络对象。



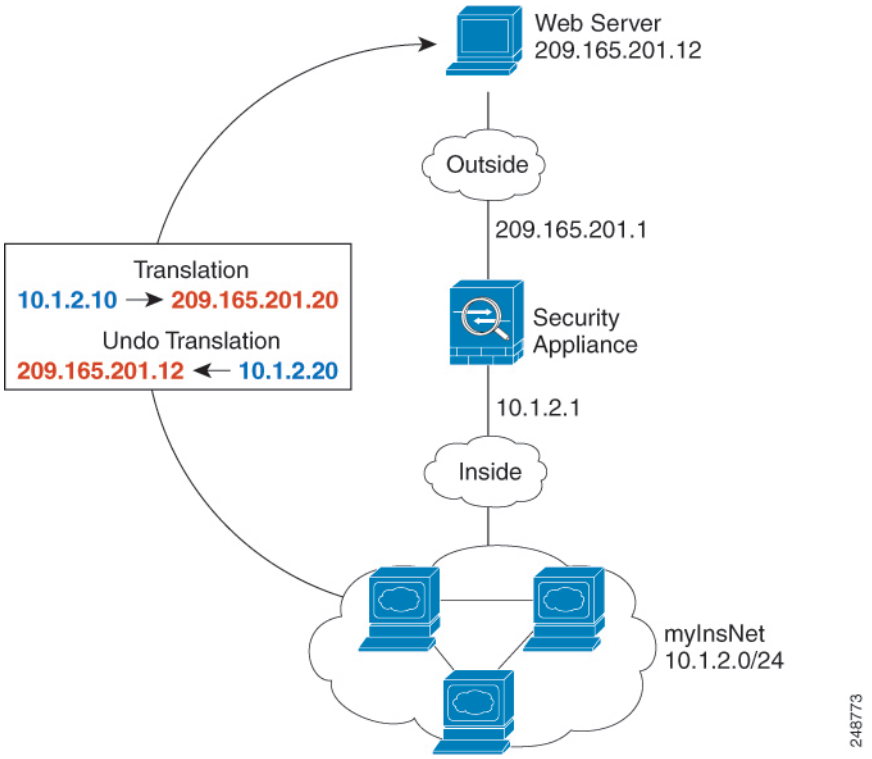
f) 点击**保存 (Save)**。

步骤 3 点击 NAT 规则页面上的**保存**。

面向内部主机的动态自动 NAT 和面向外部 Web 服务器的静态 NAT

当专用网络上的内部用户访问外部 Web 服务器时，以下示例为这些用户配置动态 NAT。此外，当内部用户连接到外部 Web 服务器时，该 Web 服务器地址被转换为显示在内部网络上的地址。

图 *114:* 面向内部 *Web* 服务器的动态 *NAT*，面向外部 *Web* 服务器的静态 *NAT*



开始之前

确保存在包含保护 Web 服务器的设备接口的接口对象（安全区域或接口组）。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请依次选择**对象** > **对象管理**，然后选择**接口**。

过程

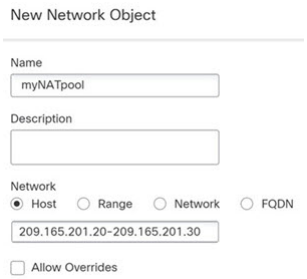
步骤 1 为要向其转换内部地址的动态 NAT 池创建一个网络对象。

a) 选择**对象 (Object)** > **对象管理 (Object Management)**。

b) 从目录中选择**网络 (Network)** 并点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

c) 定义动态 NAT 池。

为网络对象命名（例如，myNATpool），并输入网络地址范围 209.165.201.20-209.165.201.30。

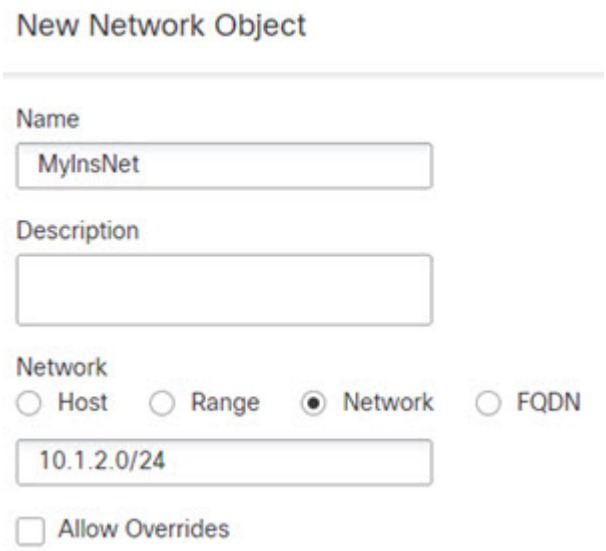


d) 点击**保存 (Save)**。

步骤 2 为内部网络创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，MyInsNet），并输入网络地址 10.1.2.0/24。

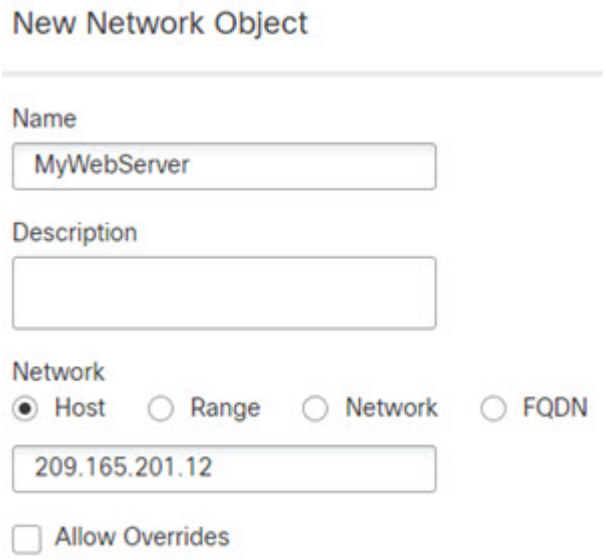


c) 点击**保存 (Save)**。

步骤 3 为外部 Web 服务器创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，MyWebServer），并输入主机地址 209.165.201.12。

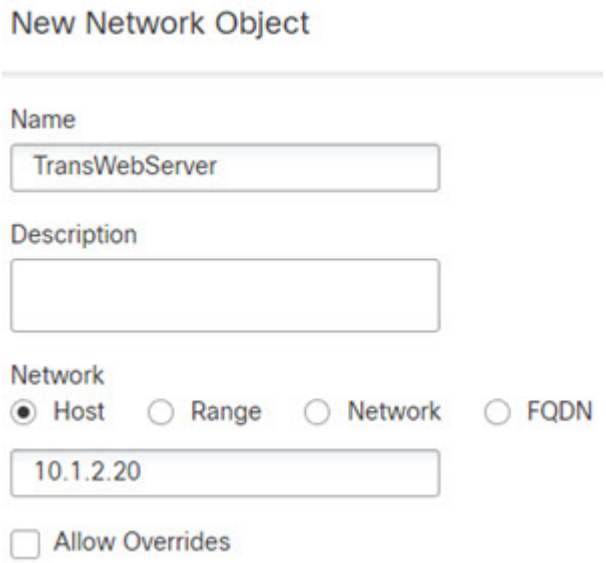


c) 点击**保存 (Save)**。

步骤 4 为转换的 Web 服务器地址创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，TransWebServer），并输入主机地址 10.1.2.20。



c) 点击**保存 (Save)**。

步骤 5 使用动态 NAT 池对象为内部网络配置动态 NAT。

a) 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

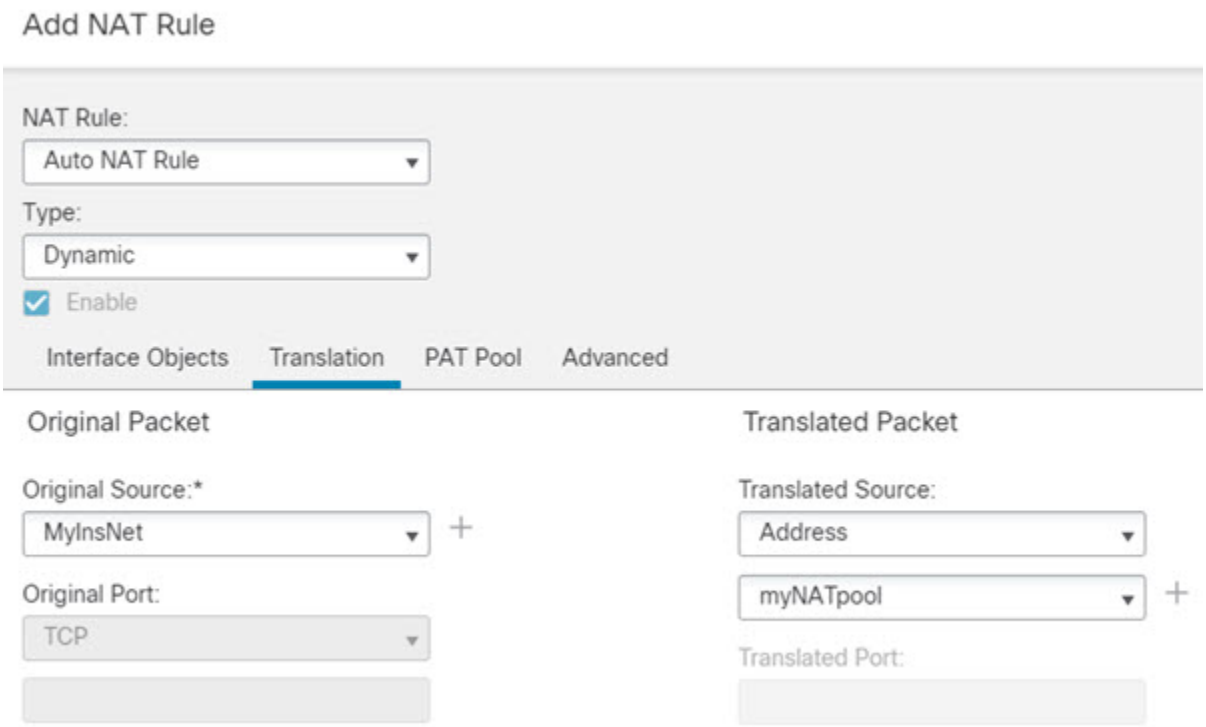
- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型 (Type)**= 动态。

d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = myInsNet 网络对象。
- **转换后的源** > **地址 (Translated Source Address)** = myNATpool 网络组。



f) 点击**保存 (Save)**。

步骤 6 为 Web 服务器配置静态 NAT。

a) 点击**添加规则**。

b) 配置以下属性：

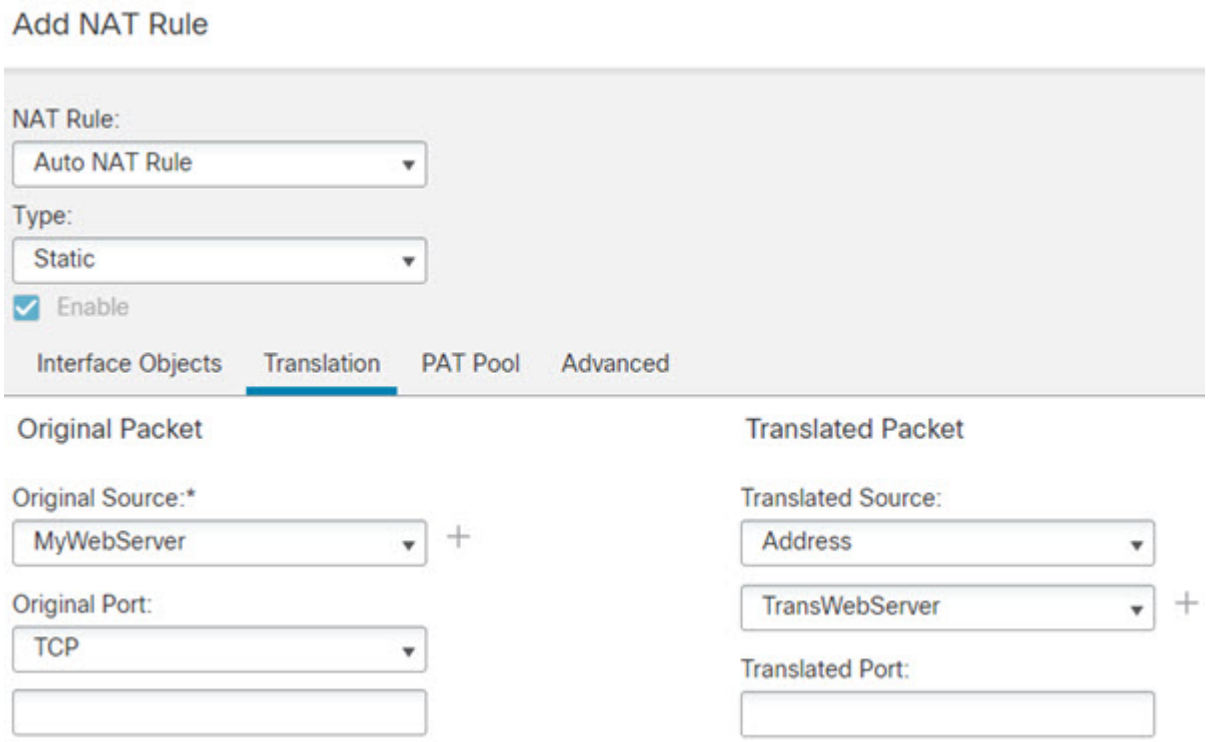
- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型** = 静态。

c) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 外部。
- **目标接口对象** = 内部。

d) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = myWebServer 网络对象。
- **转换后的源** > **地址 (Translated Source Address)** = TransWebServer 网络对象。



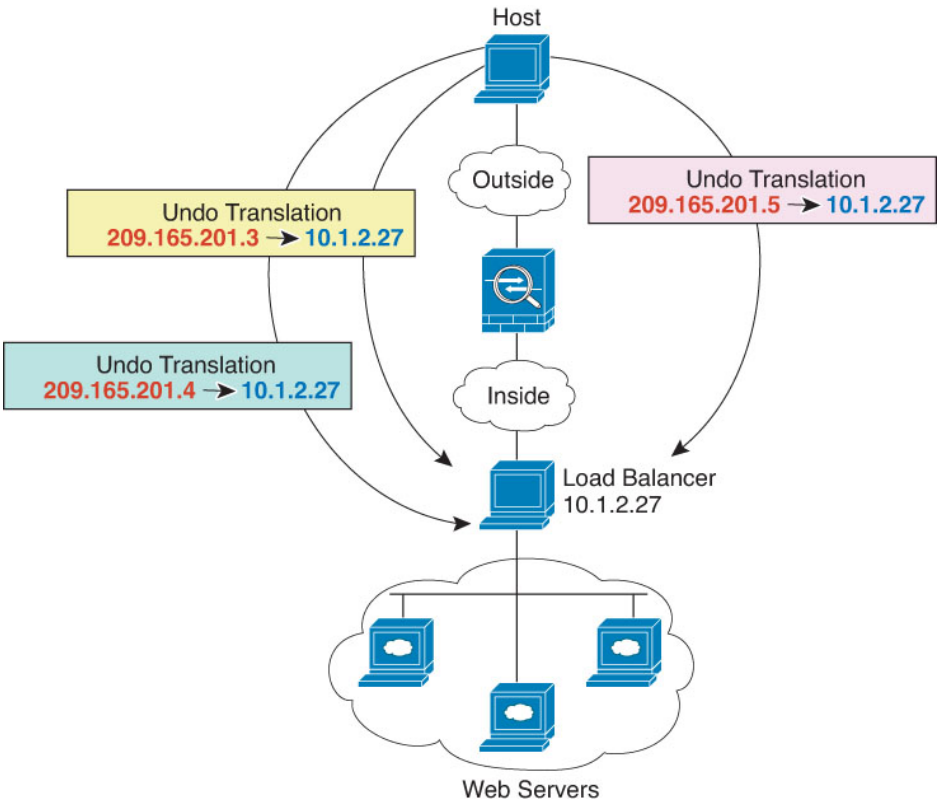
e) 点击**保存 (Save)**。

步骤 7 点击 NAT 规则页面上的**保存**。

具有多个映射地址的内部负载均衡器（静态自动 NAT，一对多）

以下示例显示转换为多个 IP 地址的内部负载均衡器。当外部主机访问其中一个映射 IP 地址时，将该地址反向转换为单一负载均衡器地址。根据请求的URL，它会将流量重新定向到正确的Web服务器。

图 *115:* 内部负载均衡器的一对多静态 *NAT*



开始之前

确保存在包含保护 Web 服务器的设备接口的接口对象（安全区域或接口组）。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请依次选择**对象** > **对象管理**，然后选择**接口**。

过程

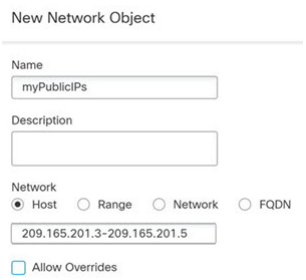
步骤 1 为要向其映射负载均衡器的地址创建网络对象。

a) 选择**对象 (Object)** > **对象管理 (Object Management)**。

b) 从目录中选择**网络 (Network)** 并点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

c) 定义地址。

为网络对象命名（例如，myPublicIPs）并输入网络范围 209.165.201.3-209.165.201.5。

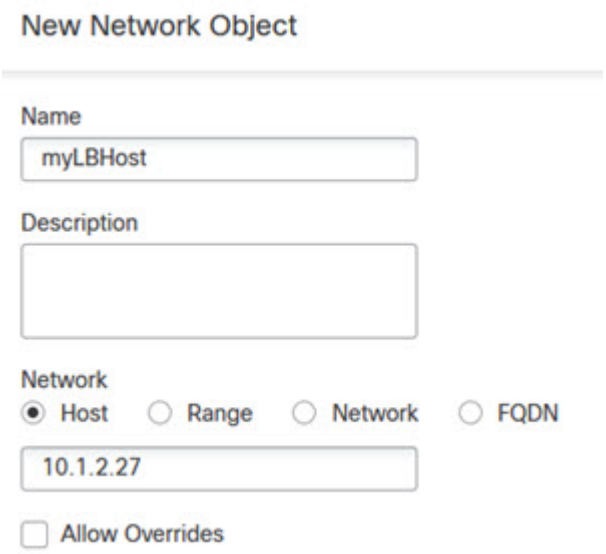


d) 点击**保存 (Save)**。

步骤 2 为负载均衡器创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，myLBHost)，然后输入主机地址 10.1.2.27。



c) 点击**保存 (Save)**。

步骤 3 为负载均衡器配置静态 NAT。

a) 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

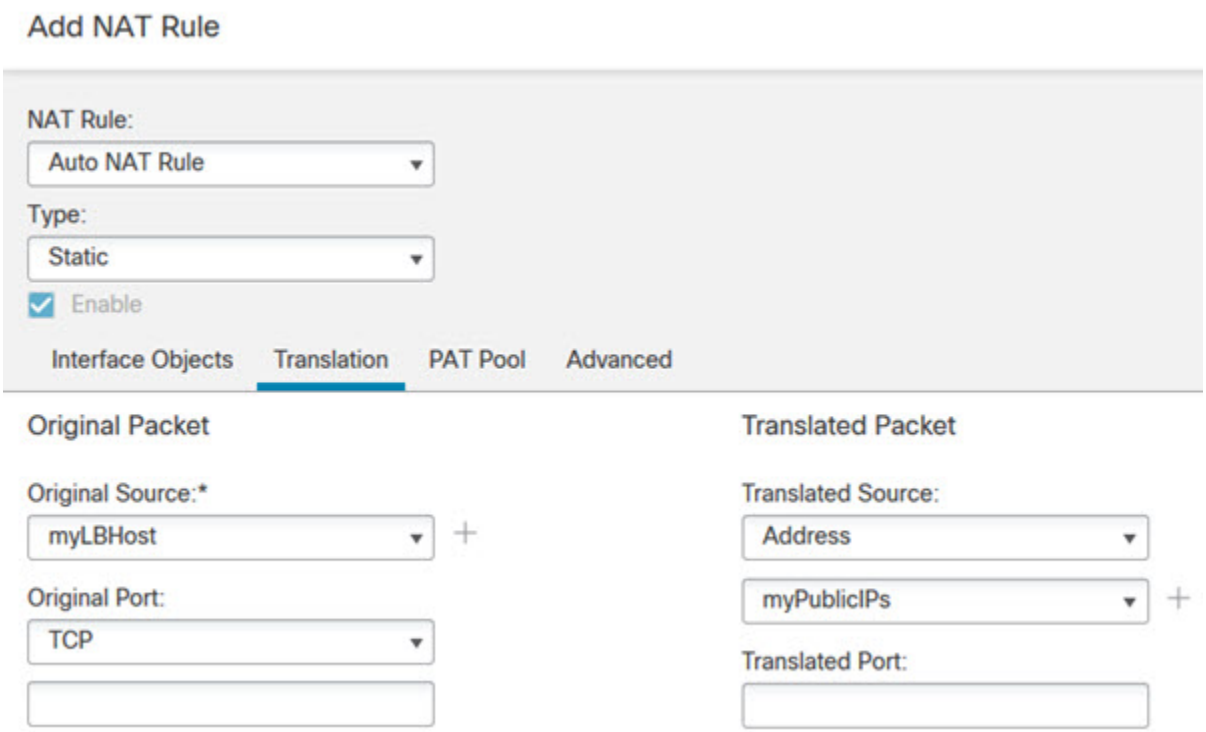
- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型** = 静态。

d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = myLBHost 网络对象。
- **转换后的源 > 地址 (Translated Source Address)** = myPublicIPs 网络组。



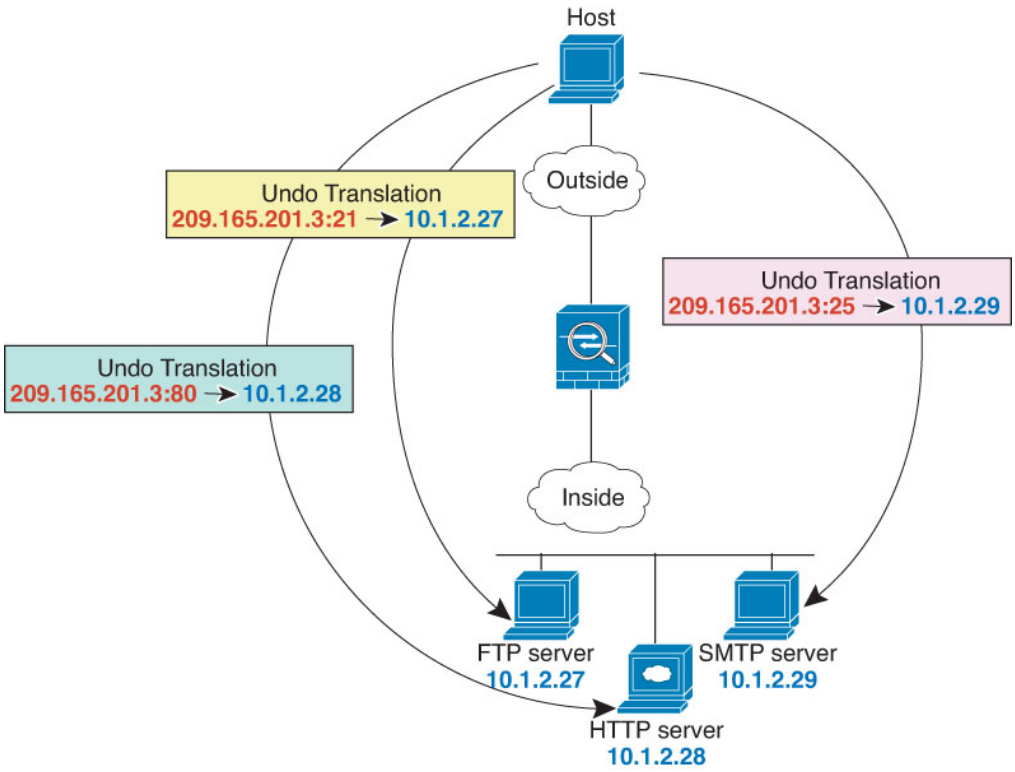
f) 点击**保存 (Save)**。

步骤 4 点击 NAT 规则页面上的**保存**。

FTP、HTTP 和 SMTP 的单个地址（具有端口转换的静态自动 NAT）

以下支持端口转换的静态 NAT 示例为远程用户访问 FTP、HTTP 和 SMTP 提供单一地址。实际上，这些服务器是实际网络上的不同设备，但对于每台服务器，可以指定采用端口转换规则的静态NAT，这些规则使用同一映射 IP 地址和不同端口。

图 *116:* 支持端口转换的静态 *NAT*



开始之前

确保您的接口对象（安全区域或接口组）包含保护服务器的设备的接口。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请依次选择**对象**>**对象管理**，然后选择**接口**。

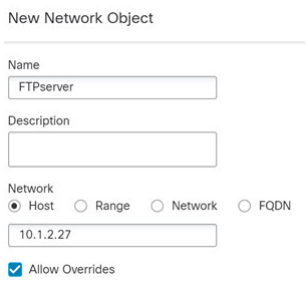
过程

步骤 1 为 FTP 服务器创建网络对象。

a) 选择**对象 (Object)** > **对象管理 (Object Management)**。

b) 从目录中选择**网络 (Network)** 并点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

c) 为网络对象命名（例如，FTPserver），然后输入 FTP 服务器的实际 IP 地址 10.1.2.27。

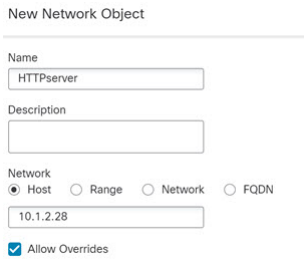


d) 点击**保存 (Save)**。

步骤 2 为 HTTP 服务器创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，HTTPserver)，然后输入主机地址 10.1.2.28。

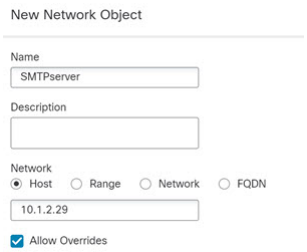


c) 点击**保存 (Save)**。

步骤 3 为 SMTP 服务器创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，SMTPserver)，然后输入主机地址 10.1.2.29。

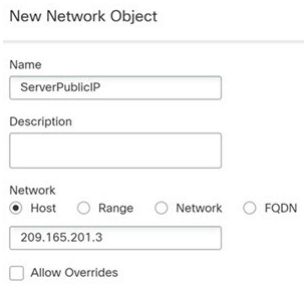


c) 点击**保存 (Save)**。

步骤 4 为用于三台服务器的公共 IP 地址创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，ServerPublicIP），然后输入主机地址 209.165.201.3。



c) 点击**保存 (Save)**。

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

a) 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

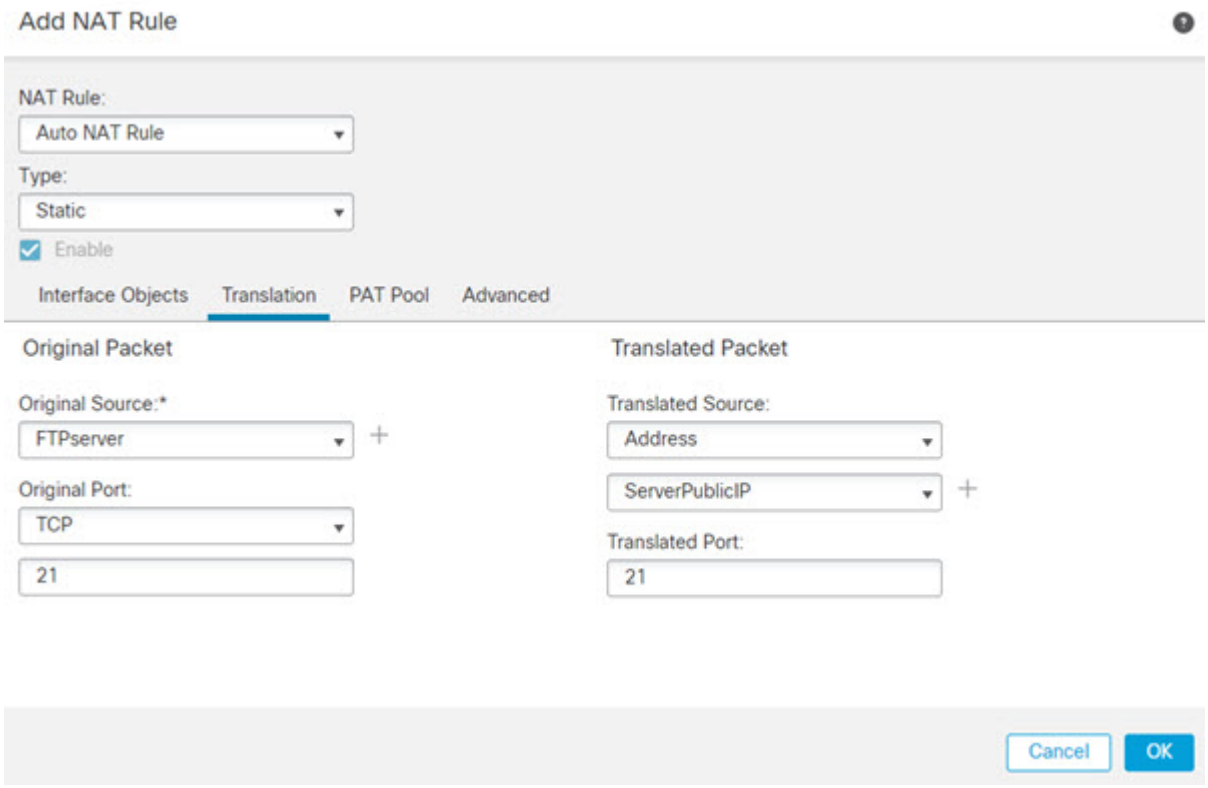
- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型** = 静态。

d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = FTPserver 网络对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = ServerPublicIP 网络对象。
- **原始端口 (Original Port)** > **TCP** = 21。
- **转换后的端口** = 21。



f) 点击**保存 (Save)**。

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

a) 点击**添加规则**。

b) 配置以下属性：

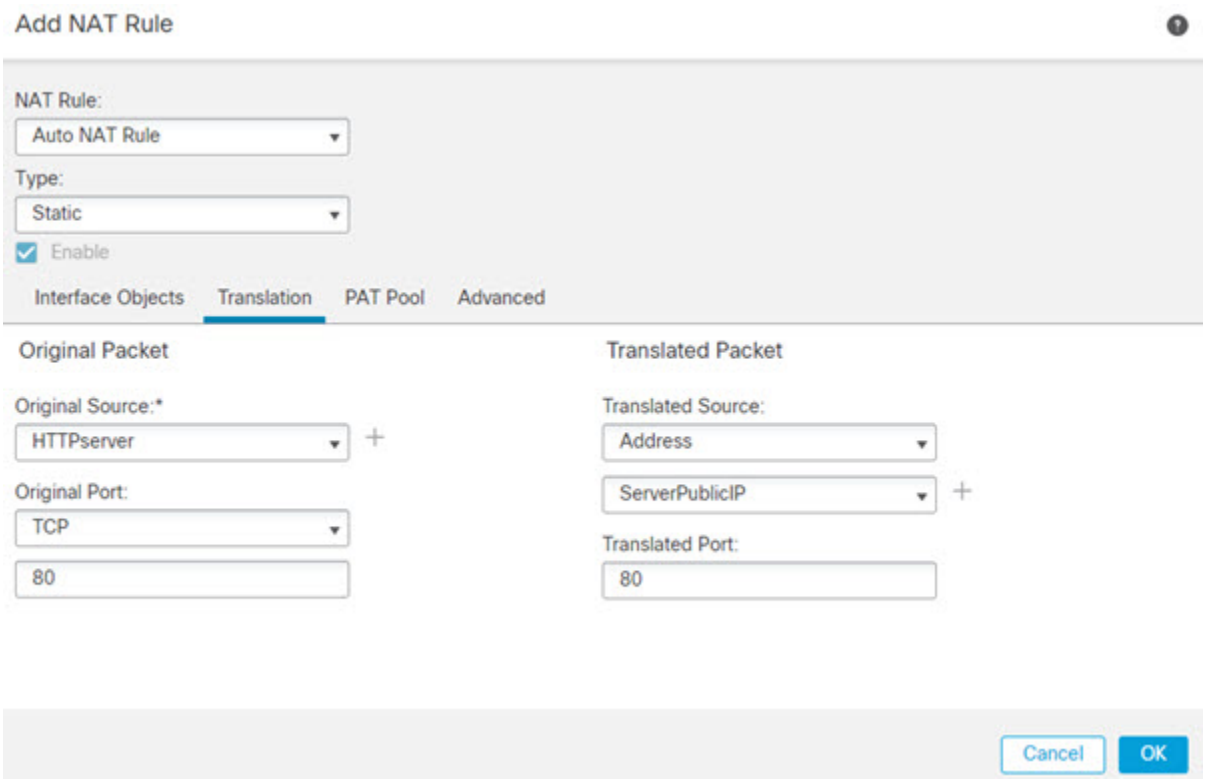
- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型** = 静态。

c) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

d) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = HTTPserver 网络对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = ServerPublicIP 网络对象。
- **原始端口 (Original Port)** > **TCP** = 80。
- **转换后的端口** = 80。



e) 点击**保存 (Save)**。

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

a) 点击**添加规则**。

b) 配置以下属性：

- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。

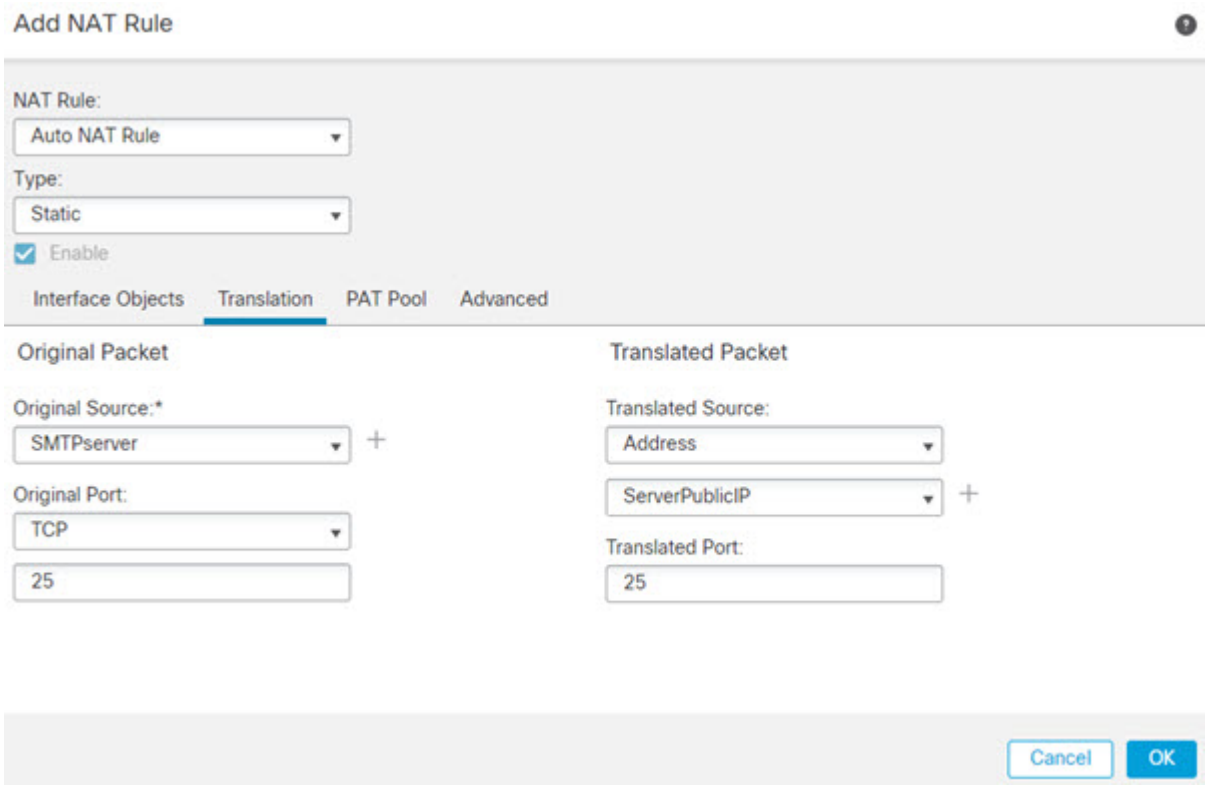
- 类型 = 静态。

c) 在接口对象 **(Interface Objects)** 上配置以下选项：

- 源接口对象 = 内部。
- 目标接口对象 = 外部。

d) 在转换 **(Translation)** 上配置以下选项：

- 原始源 = SMTPserver 网络对象。
- 转换后的源 **(Translated Source)** > 地址 **(Address)** = ServerPublicIP 网络对象。
- 原始端口 **(Original Port)** > **TCP** = 25。
- 转换后的端口 = 25。



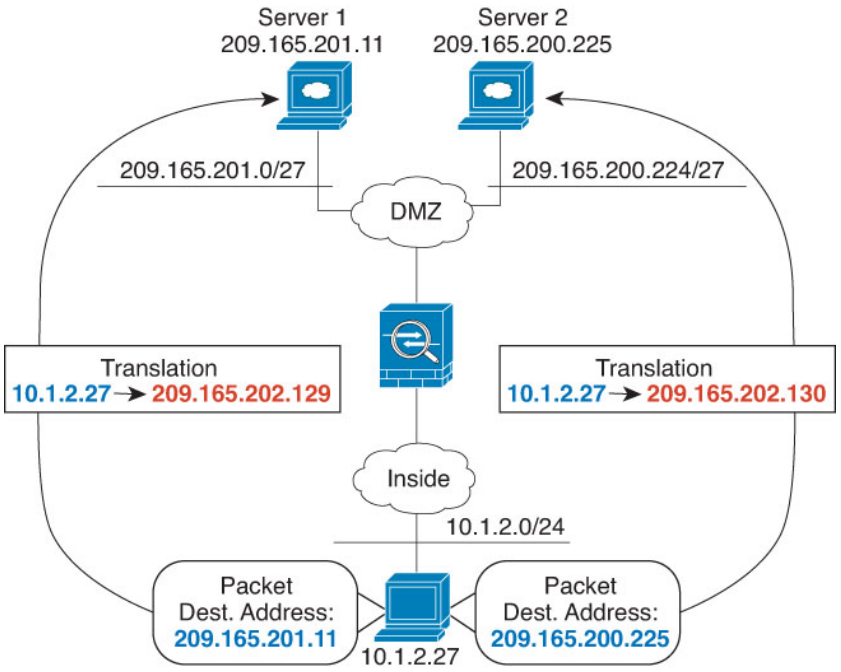
e) 点击保存 **(Save)**。

步骤 8 点击 NAT 规则页面上的保存。

转换因目标而异（动态手动 PAT）

下图显示 10.1.2.0/24 网络上的一台主机正在访问两台不同的服务器。当主机访问位于 209.165.201.11 的服务器时，实际地址将转换为 209.165.202.129:*port*。当主机访问位于 209.165.200.225 的服务器时，实际地址将转换为 209.165.202.130:*port*。

图 *117:* 具有不同目标地址的手动 *NAT*



开始之前

确保具有接口对象（安全区域或接口组），其包含保护服务器的设备的接口。在本例中，我们将假定接口对象是名为**内部**和 **dmz** 的安全区域。要配置接口对象，请选择**对象** > **对象管理**，然后选择**接口**。

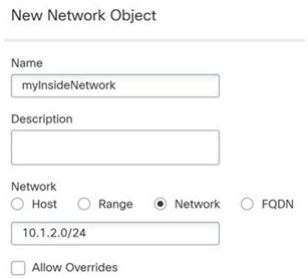
过程

步骤 1 为内部网络创建网络对象。

a) 选择**对象 (Object)** > **对象管理 (Object Management)**。

b) 从目录中选择**网络 (Network)** 并点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

c) 为网络对象命名（例如，myInsideNetwork），然后输入实际网络地址 10.1.2.0/24。



d) 点击**保存 (Save)**。

步骤 2 为 DMZ 网络 1 创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

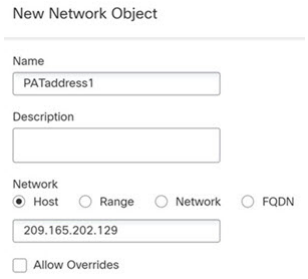
b) 为网络对象命名（例如，DMZnetwork1），然后输入网络地址 209.165.201.0/27（子网掩码为 255.255.255.224）。

c) 点击**保存 (Save)**。

步骤 3 为 DMZ 网络 1 的 PAT 地址创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，PATaddress1），然后输入主机地址 209.165.202.129。

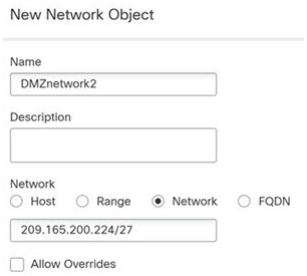


c) 点击**保存 (Save)**。

步骤 4 为 DMZ 网络 2 创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，DMZnetwork2），然后输入网络地址 209.165.200.224/27（子网掩码为 255.255.255.224）。



c) 点击**保存 (Save)**。

步骤 5 为 DMZ 网络 2 的 PAT 地址创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，PATaddress2），然后输入主机地址 209.165.202.130。

c) 点击**保存 (Save)**。

步骤 6 为 DMZ 网络 1 配置动态手动 PAT。

a) 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

- **NAT 规则** = 手动 NAT 规则。
- **类型 (Type)**= 动态。

d) 在**接口对象 (Interface Objects)** 上配置以下选项：

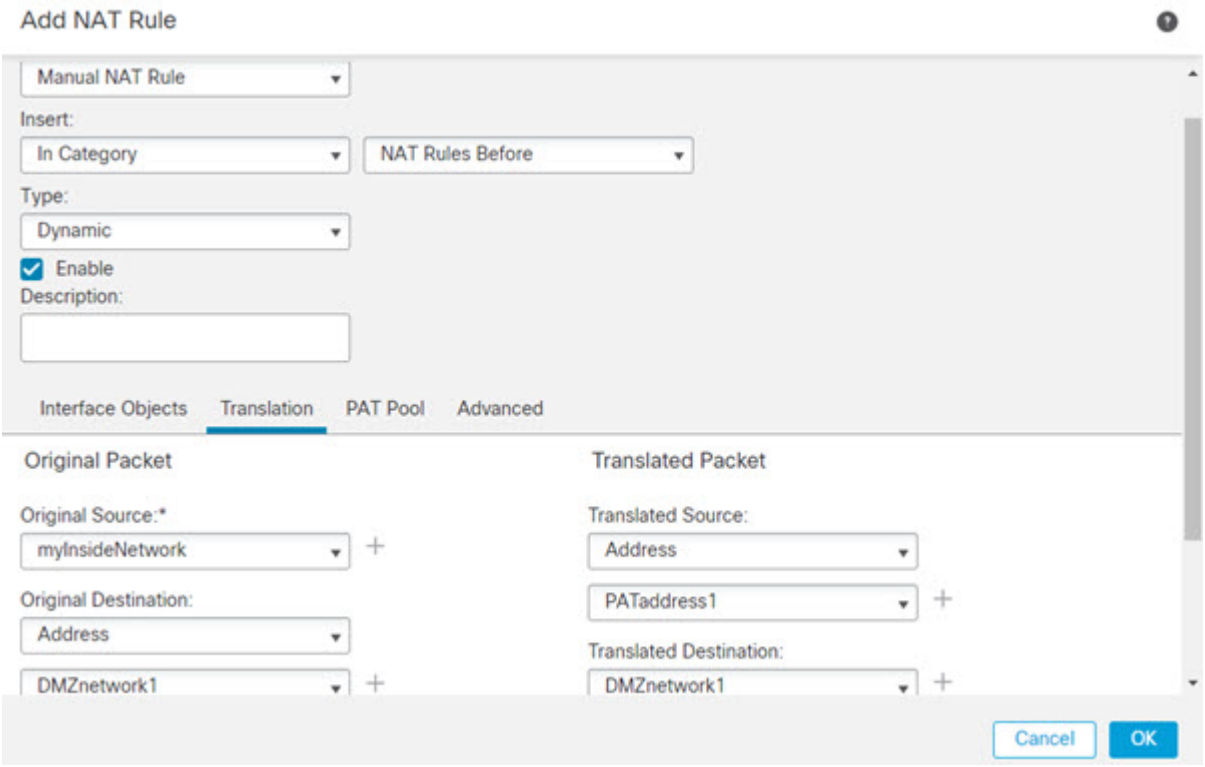
- **源接口对象** = 内部。
- **目的接口对象** = dmz。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = myInsideNetwork 网络对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = PATaddress1 网络对象。
- **原始目标 (Original Destination)** > **地址 (Address)** = DMZnetwork1 网络对象。

- **转换后的目标** = DMZnetwork1 网络对象。

  注释　由于您不需要转换目标地址，因此需要通过为原始目标地址和转换后的目标地址指定相同的地址，从而为其配置身份 NAT。将所有端口字段留空。



f) 点击**保存 (Save)**。

步骤 7 为 DMZ 网络 2 配置动态手动 PAT。

a) 点击**添加规则**。

b) 配置以下属性：

- **NAT 规则** = 手动 NAT 规则。
- **类型 (Type)**= 动态。

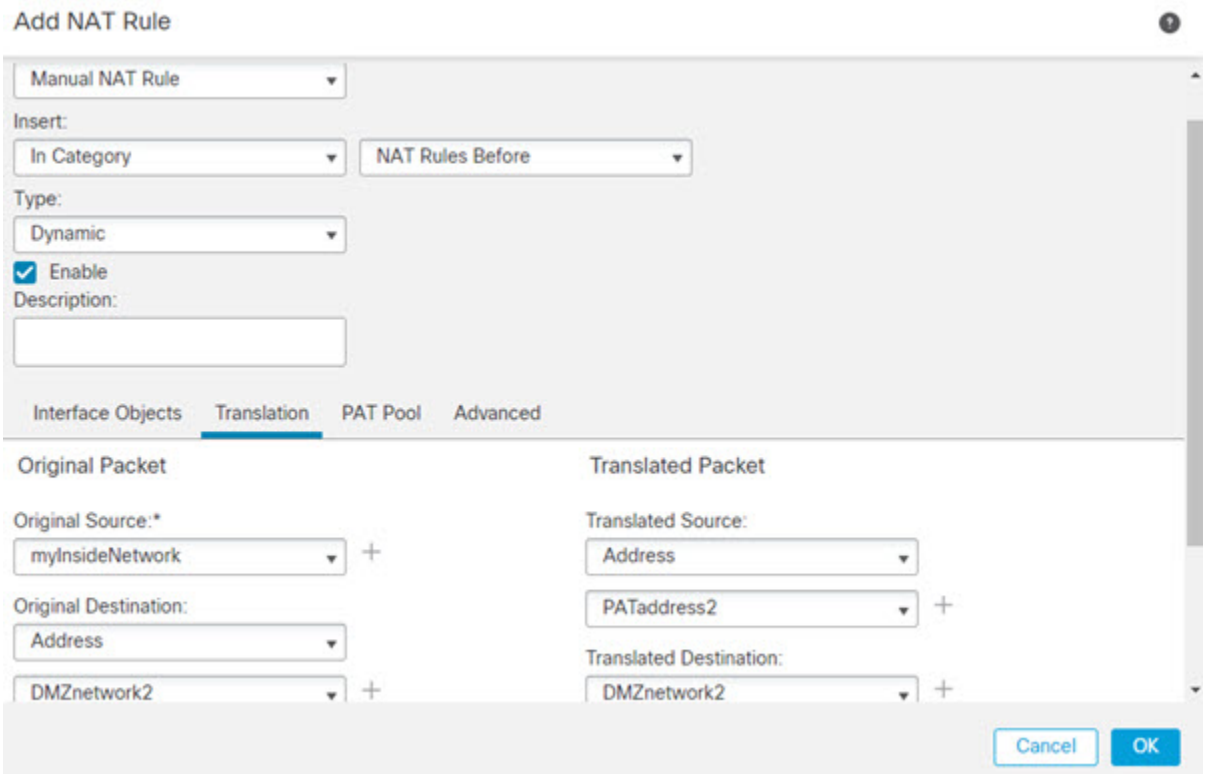
c) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目的接口对象** = dmz。

d) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = myInsideNetwork 网络对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = PATaddress2 网络对象。

- 原始目标 **(Original Destination)** > 地址 **(Address)** = DMZnetwork2 网络对象。
- 转换后的目标 = DMZnetwork2 网络对象。



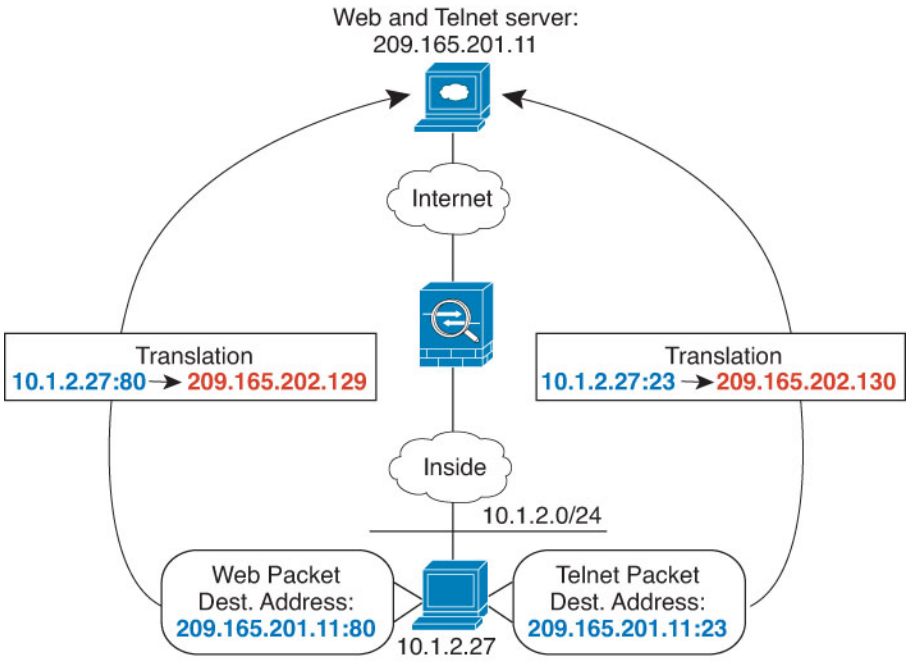
e) 点击保存 **(Save)**。

步骤 8 点击 NAT 规则页面上的保存。

转换因目标地址和端口而异（动态手动 PAT）

下图显示源端口和目标端口的使用情况。10.1.2.0/24 网络上的主机同时因为网络服务和 Telnet 服务访问单个主机。当主机进行 Telnet 服务访问服务器时，实际地址将转换为 209.165.202.129:*port*。当主机进行网络服务访问相同服务器时，真实地址将转换为 209.165.202.130:*port*。

图 *118:* 具有不同目标端口的手动 *NAT*



开始之前

确保具有接口对象（安全区域或接口组），其包含保护服务器的设备的接口。在本例中，我们将假定接口对象是名为**内部**和 **dmz** 的安全区域。要配置接口对象，请选择**对象** > **对象管理**，然后选择**接口**。

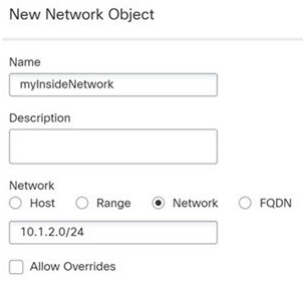
过程

步骤 1 为内部网络创建网络对象。

a) 选择**对象 (Object)** > **对象管理 (Object Management)**。

b) 从目录中选择**网络 (Network)** 并点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

c) 为网络对象命名（例如，myInsideNetwork），然后输入实际网络地址 10.1.2.0/24。



d) 点击**保存 (Save)**。

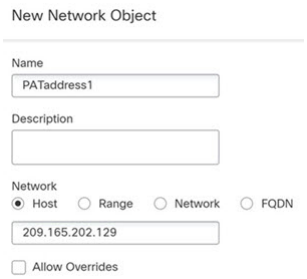
步骤 2 为 Telnet/Web 服务器创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。
b) 为网络对象命名（例如，TelnetWebServer），然后输入主机地址 209.165.201.11。

c) 点击**保存 (Save)**。

步骤 3 使用 Telnet 时为 PAT 地址创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。
b) 为网络对象命名（例如，PATaddress1），然后输入主机地址 209.165.202.129。



c) 点击**保存 (Save)**。

步骤 4 使用 HTTP 时为 PAT 地址创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。
b) 为网络对象命名（例如，PATaddress2），然后输入主机地址 209.165.202.130。

c) 点击**保存 (Save)**。

步骤 5 为 Telnet 访问创建动态手动 PAT。

a) 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。
b) 点击**添加规则**。
c) 配置以下属性：

- **NAT 规则** = 手动 NAT 规则。
- **类型 (Type)**= 动态。

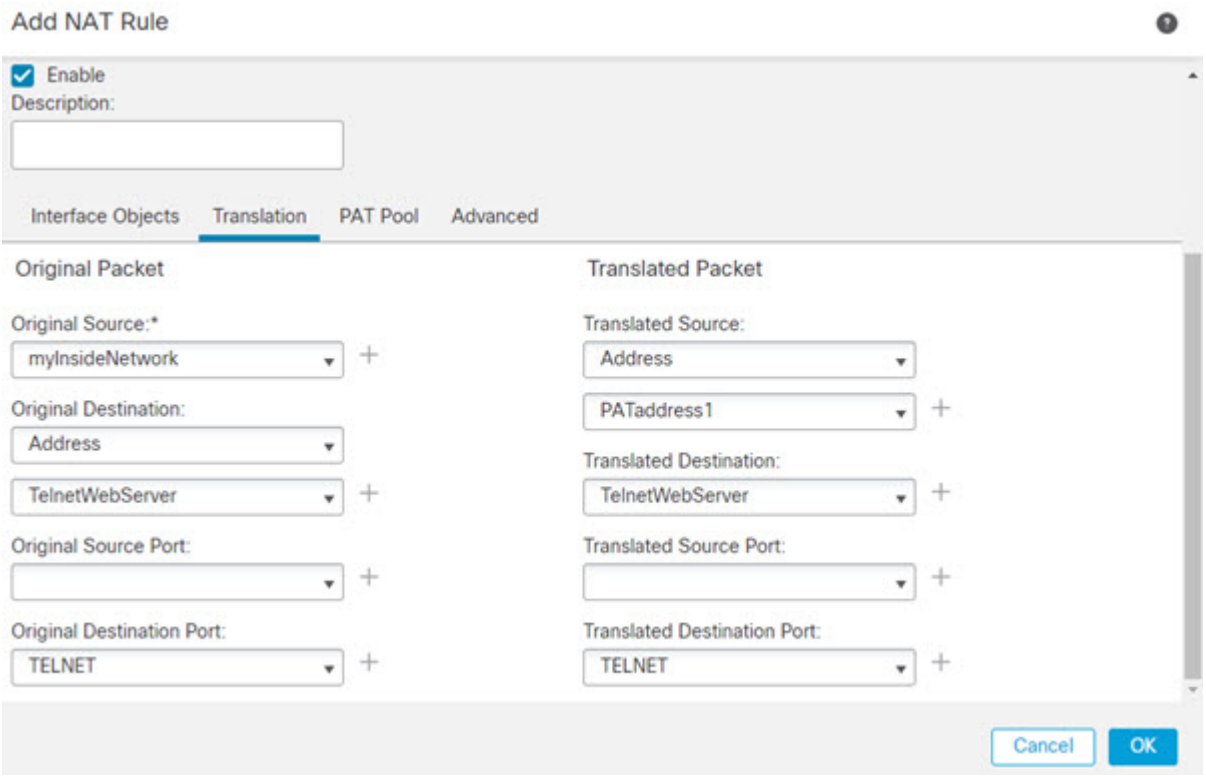
d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目的接口对象** = dmz。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = myInsideNetwork 网络对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = PATaddress1 网络对象。
- **原始目标 (Original Destination)** > **地址 (Address)** = TelnetWebServer 网络对象。
- **转换后的目标** = TelnetWebServer 网络对象。
- **原始目标端口** = TELNET 端口对象（系统定义）。
- **转换后的目标端口** = TELNET 端口对象（系统定义）。

注释 由于您不需要转换目标地址或端口，因此需要通过为原始目标地址和转换后的目标地址指定相同的地址，以及为原始端口和转换后的端口指定相同的端口，从而为它们配置身份 NAT。



f) 点击**保存 (Save)**。

步骤 6 为 Web 访问创建动态手动 PAT。

a) 点击**添加规则**。

b) 配置以下属性：

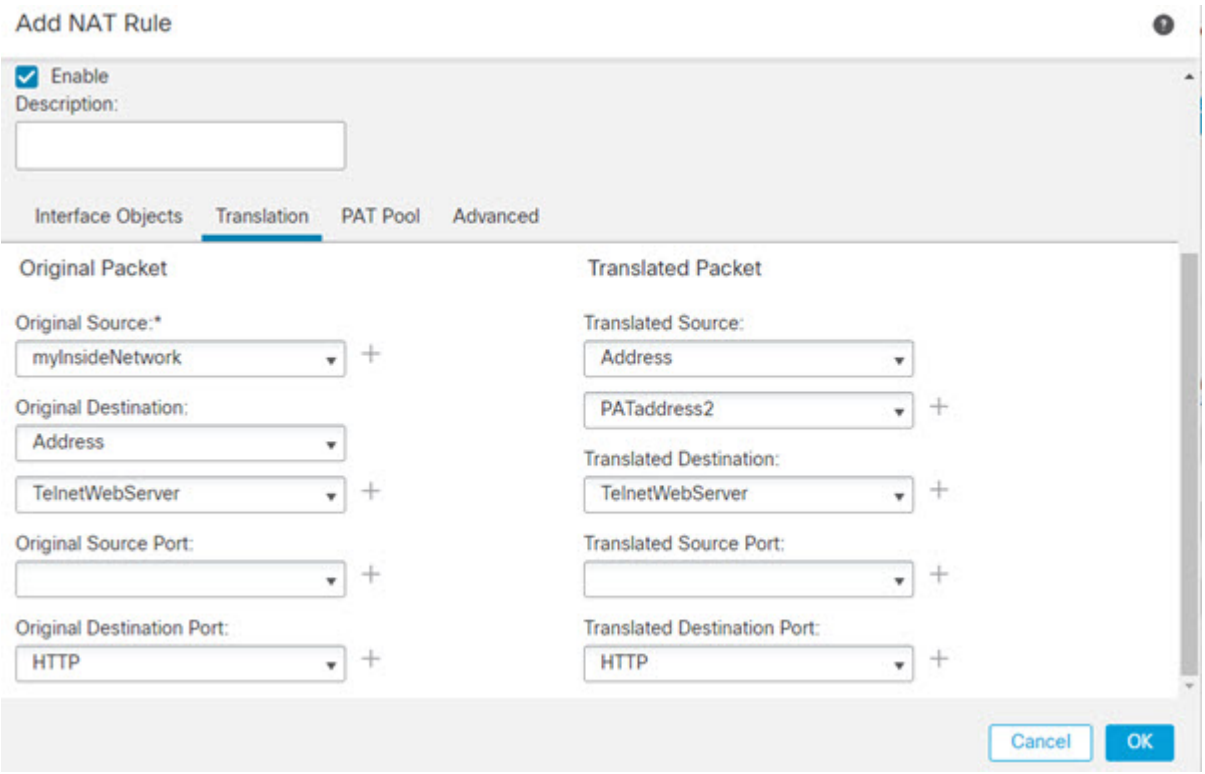
- **NAT 规则** = 手动 NAT 规则。
- **类型 (Type)**= 动态。

c) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目的接口对象** = dmz。

d) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = myInsideNetwork 网络对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = PATaddress2 网络对象。
- **原始目标 (Original Destination)** > **地址 (Address)** = TelnetWebServer 网络对象。
- **转换后的目标** = TelnetWebServer 网络对象。
- **原始目标端口** = HTTP 端口对象（系统定义）。
- **转换后的目标端口** = HTTP 端口对象（系统定义）。



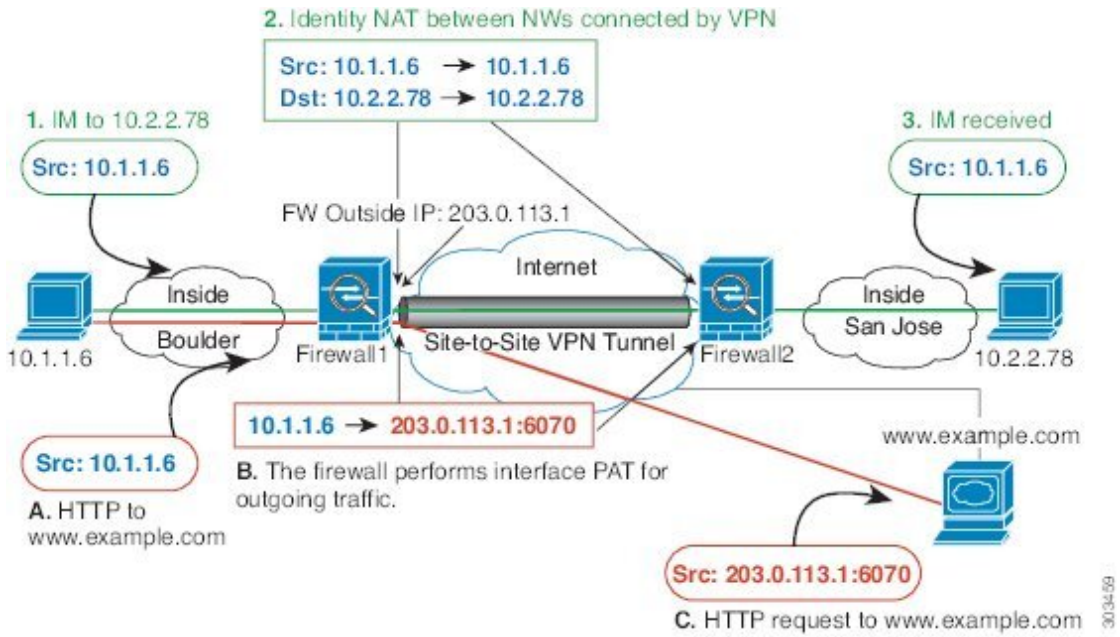
e) 点击**保存 (Save)**。

步骤 7 点击 NAT 规则页面上的**保存**。

NAT 和站点间 VPN

下图显示连接博尔德办公室和圣荷西办公室的站点间隧道。对于要发送到互联网的流量（例如，从博尔德办公室中的 10.1.1.6 到 www.example.com），需要利用 NAT 提供的公用 IP 地址访问互联网。以下示例使用接口 PAT 规则。然而，对于要穿过 VPN 隧道的流量（例如，从博尔德办公室中的 10.1.1.6 到圣荷西办公室中的 10.2.2.78），您不想执行 NAT；您需要通过创建身份 NAT 规则来豁免此流量。身份 NAT 只能将地址转换为其相同的地址。

图 *119:* 用于站点间 *VPN* 的接口 *PAT* 和身份 *NAT*



以下示例说明 Firewall1（博尔德办公室）的配置。

开始之前

确保您有包含VPN中设备接口的接口对象（安全区域或接口组）。在本例中，我们假定接口对象为针对 Firewall1（博尔德办公室）接口的名为 **inside-boulder** 和 **outside-boulder** 的安全区域。要配置接口对象，请选择**对象** > **对象管理**，然后选择**接口**。

过程

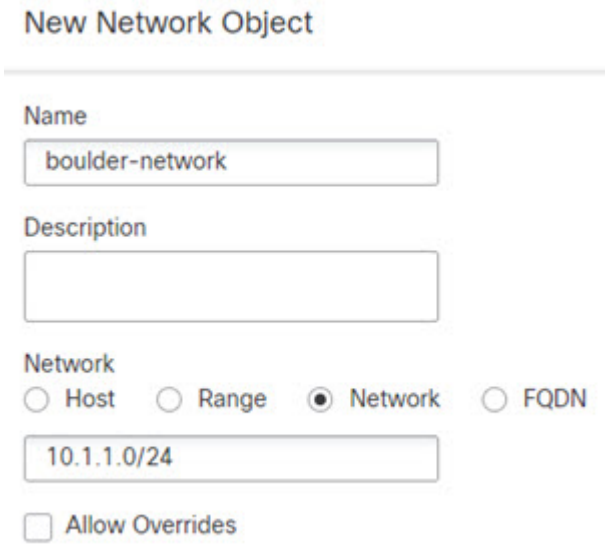
步骤 1 创建对象来定义各种网络。

a) 选择**对象** > **对象管理**。

b) 从目录中选择**网络 (Network)** 并点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

c) 找到博尔德办公室内部网络。

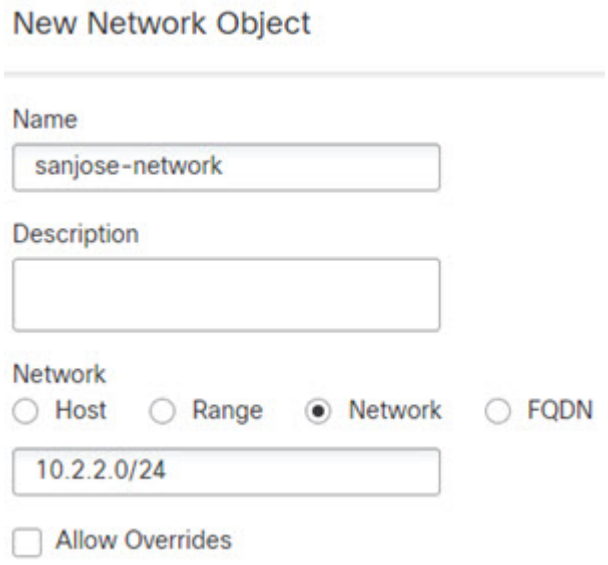
为网络对象命名（例如，boulder-network），然后输入网络地址 10.1.1.0/24。



d) 点击**保存 (Save)**。

e) 点击**添加网络** > **添加对象**，并定义内部圣荷西网络。

为网络对象命名（例如，sanjose-network），然后输入网络地址 10.2.2.0/24。



f) 点击**保存 (Save)**。

步骤 2 在Firewall1（博尔德办公室）上，为博尔德办公室网络配置经过VPN连接到圣荷西办公室时的手动身份 NAT。

a) 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

- **NAT 规则** = 手动 NAT 规则。

- **类型** = 静态。

d) 在**接口对象 (Interface Objects)** 上配置以下选项：

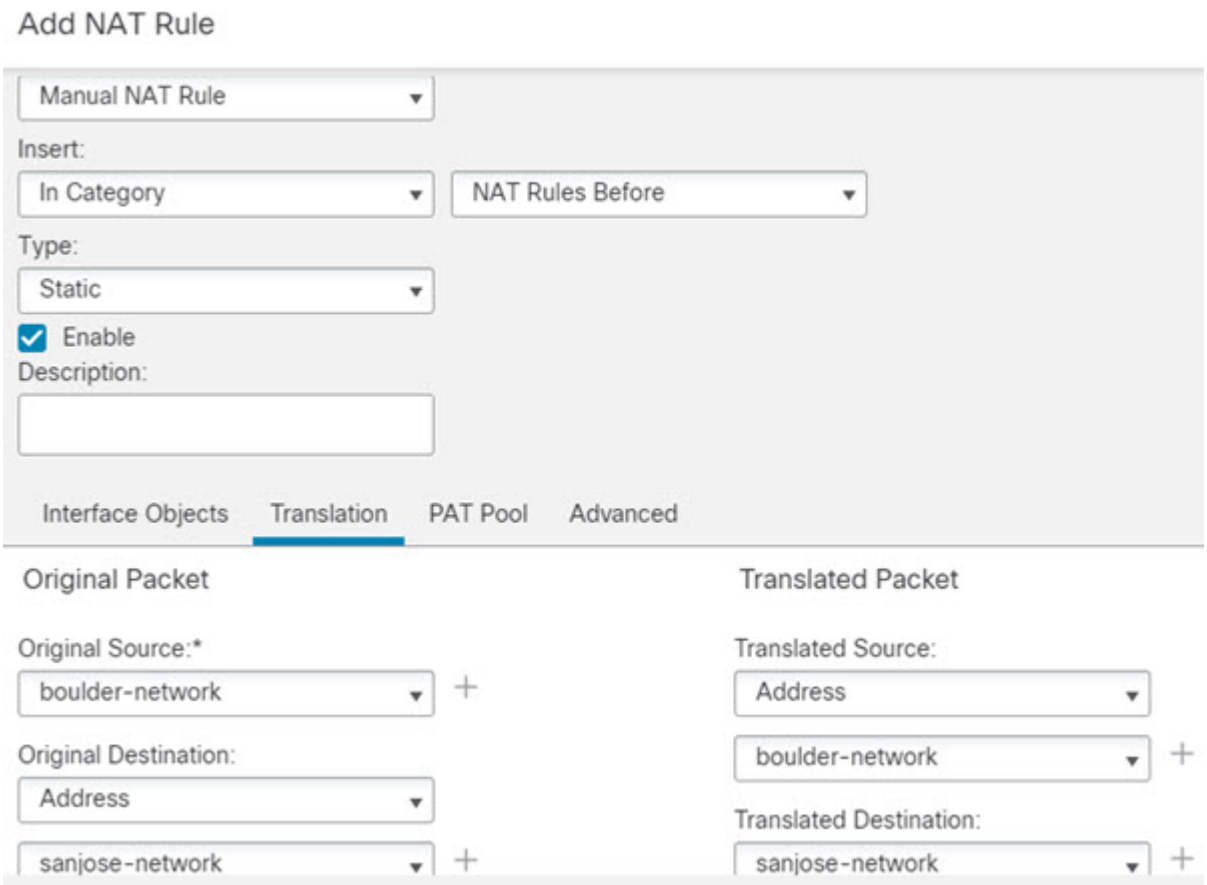
- **源接口对象** = inside-boulder。
- **目标接口对象** = outside-boulder。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = boulder-network 对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = boulder-network 对象。
- **原始目标 (Original Destination)** > **地址 (Address)** = sanjose-network 对象。
- **转换后的目标** = sanjose-network 对象。

  注释 由于您不需要转换目标地址，因此需要通过为原始目标地址和转换后的目标地址指定相同的地址，从而为其配置身份 NAT。将所有端口字段留空。此规则为源和目标配置身份 NAT。

f) 在**高级 (Advanced)** 选项卡中，选择**不在目标接口上使用代理 ARP (Do not proxy ARP on Destination interface)**。



g) 点击**保存 (Save)**。

步骤 3 在Firewall1（博尔德办公室）上，为内部博尔德办公室网络配置接入互联网时的手动动态接口 PAT。

a) 点击**添加规则**。

b) 配置以下属性：

- **NAT 规则** = 手动 NAT 规则。
- **类型** = 动态。
- **插入规则** = 在第一个规则之后的任何位置。由于此规则将应用于所有目的地址，使用 sanjose-network 作为目的的规则必须在此规则之前，否则永远也不会匹配 sanjose-network 规则。默认设置是将新的手动 NAT 规则放到“NAT 规则在自动 NAT 之前”部分的末尾。

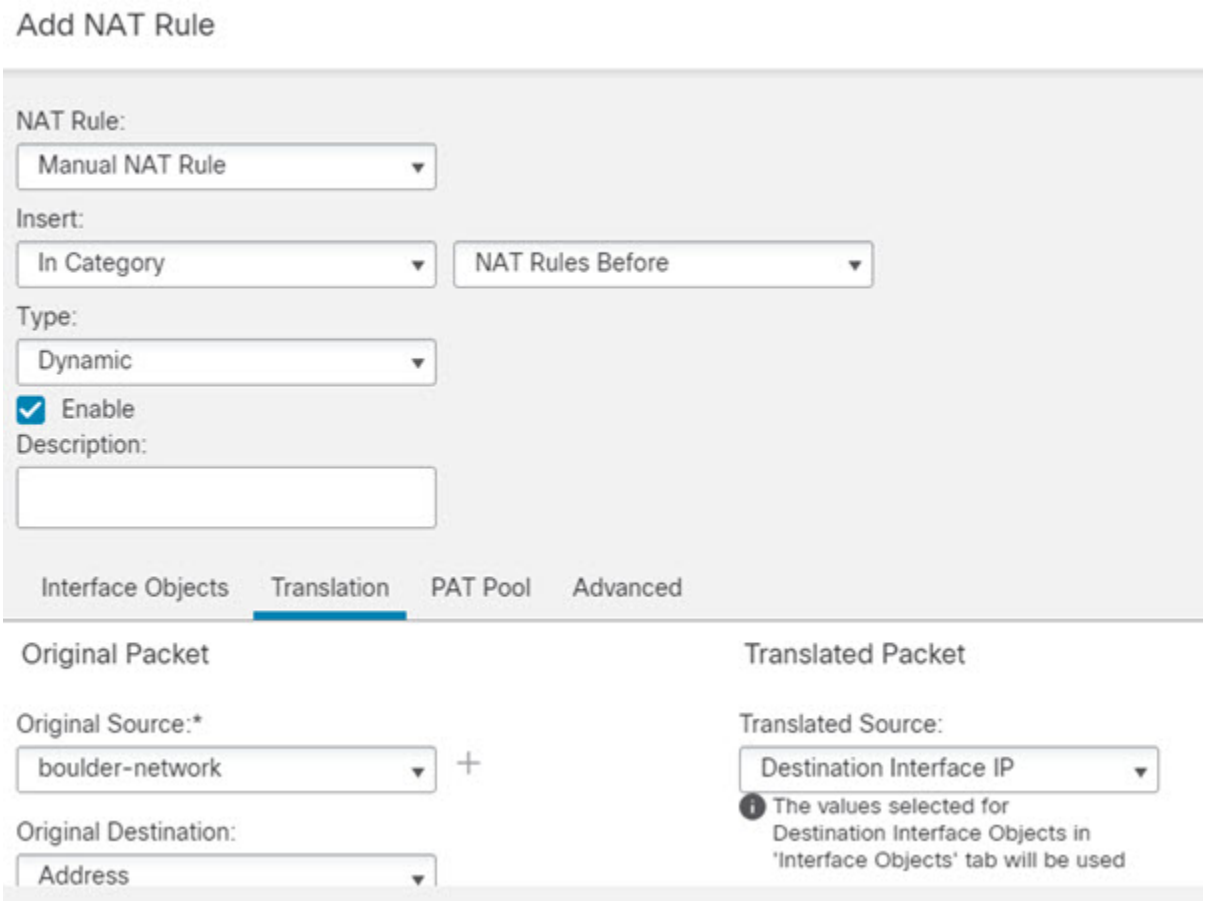
c) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = inside-boulder。
- **目标接口对象** = outside-boulder。

d) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = boulder-network 对象。

- **转换后的源** = **目标接口 IP**。此选项使用目标接口对象中包含的接口来配置接口 PAT。
- **原始目标 (Original Destination)** > **地址 (Address)** = 任意（留空）。
- **转换后的目标** = 任意（留空）。



e) 点击**保存 (Save)**。

步骤 4 如果您也管理着 Firewall2（圣荷西办公室），您可以为该设备配置类似的规则。

- 当目标是 boulder-network 时，手动身份 NAT 规则将用于 sanjose-network。为 Firewall2 内部和外部网络创建新的接口对象。
- 当目标是“任何”时，手动动态接口 PAT 规则将用于 sanjose-network。

使用 NAT 重写 DNS 查询和响应

可能需要配置 威胁防御设备 以修改 DNS 应答，方法是用匹配 NAT 配置的地址替换应答中的地址。配置每条转换规则时，可以配置 DNS 修改。DNS 修改也称为“DNS Doctoring”。

此功能可以重写匹配 NAT 规则的 DNS 查询和应答中的地址（例如，适用于 IPv4 的 A 记录；适用于 IPv6 的 AAAA 记录；或者，适用于逆向 DNS 查询的 PTR 记录）。对于从映射接口穿越到任何其他接口的 DNS 应答，记录会从映射值被重写为实际值。相反，对于从任何接口穿越到映射接口的 DNS 应答，记录会从实际值被重写为映射值。此功能适用于 NAT44、NAT 66、NAT46 和 NAT64。

以下是需要在 NAT 规则上配置 DNS 重写的几种主要情况。

- 规则为 NAT64 或 NAT46，并且 DNS 服务器位于外部网络上。您需要进行 DNS 重写以实现 DNS A 记录（适用于 IPv4）和 AAAA 记录（适用于 IPv6）之间的转换。
- DNS 服务器在外部，客户端在内部，并且客户端使用的一些完全限定域名解析到其他内部主机。
- DNS 服务器在内部并以专用 IP 地址进行响应，客户端在外部，并且客户端访问指向内部托管的服务器的完全限定域名。

DNS 重写限制

以下是 DNS 重写的某些限制：

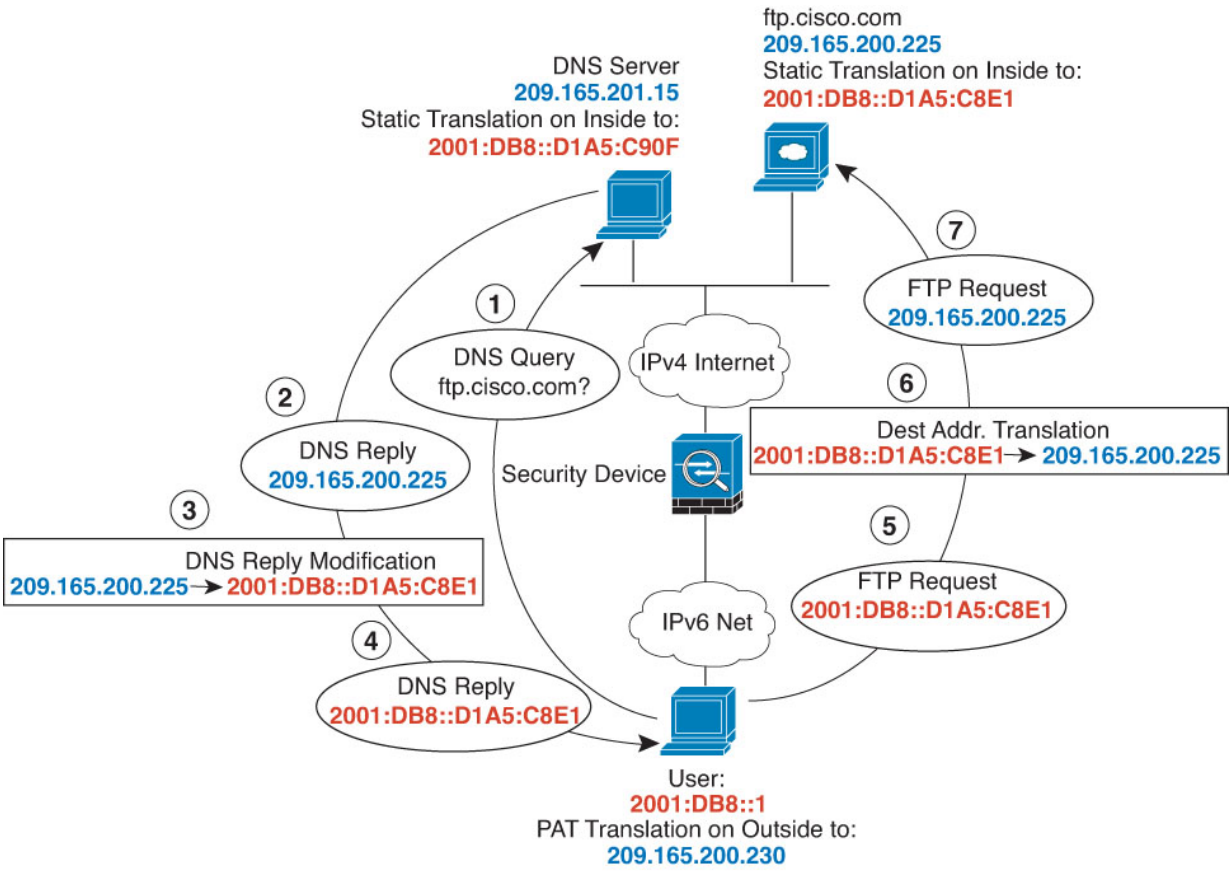
- DNS 重写不适用于 PAT，因为多条 PAT 规则适用于每个 A 或 AAAA 记录，而要使用的 PAT 规则不确定。
- 如果您配置了手动 NAT 规则，当指定了目的地址和源地址时，不能配置 DNS 修改。当流向 A 与 B 时，这类规则可能会有单个地址的不同转换。因此，将精确匹配 DNS 应答中的 IP 地址与正确的两次 NAT 规则相匹配；DNS 应答不包含有关哪个源地址/目标地址组合位于提示 DNS 请求的数据包中的信息。
- 要重写 DNS 查询和响应，您必须启用针对 NAT 规则启用了 DNS NAT 重写的 DNS 应用检查。默认情况下，启用了 DNS NAT 重写的 DNS 检查会全局应用，因此可能无需更改检查配置。
- 实际上，DNS 重写在 xlate 条目而非 NAT 规则上完成。因此，如果没有面向动态规则的 xlate，则不能正确完成重写。静态 NAT 也会出现相同的问题。
- DNS 重写不会重写 DNS 动态更新消息（操作码为 5）。

以下主题提供了 NAT 规则中 DNS 重写的示例。

DNS64 应答修改

下图显示外部 IPv4 网络上的 FTP 服务器和 DNS 服务器。系统有面向外部服务器的静态转换。在这种情况下，当内部 IPv6 用户从 DNS 服务器请求 ftp.cisco.com 的地址时，DNS 服务器将以实际地址 209.165.200.225 作为响应。

由于您希望内部用户使用 ftp.cisco.com 的映射地址（2001:DB8::D1A5:C8E1，其中 D1A5:C8E1 是 209.165.200.225 的 IPv6 对应物），因此需要配置 DNS 回复修改以进行静态转换。本示例还包括面向 DNS 服务器的静态 NAT 转换和面向内部 IPv6 主机的 PAT 规则。



开始之前

确保具有包含用于设备的接口的接口对象（安全区或接口组）。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请依次选择**对象** > **对象管理**，然后选择**接口**。

过程

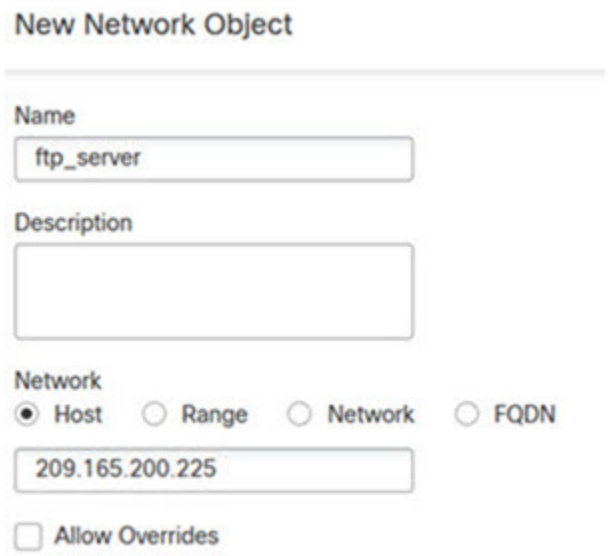
步骤 1 为 FTP 服务器、DNS 服务器、内部网络和 PAT 池创建网络对象。

a) 选择**对象 (Object)** > **对象管理 (Object Management)**。

b) 从目录中选择**网络 (Network)** 并点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

c) 定义实际 FTP 服务器地址。

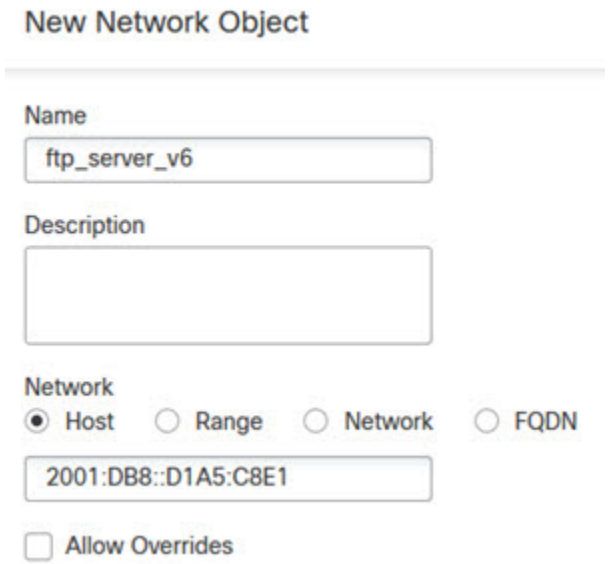
为网络对象命名（例如，ftp_server），然后输入主机地址 209.165.200.225。



d) 点击**保存 (Save)**。

e) 点击**添加网络 > 添加对象**并定义 FTP 服务器的转换后 IPv6 地址。

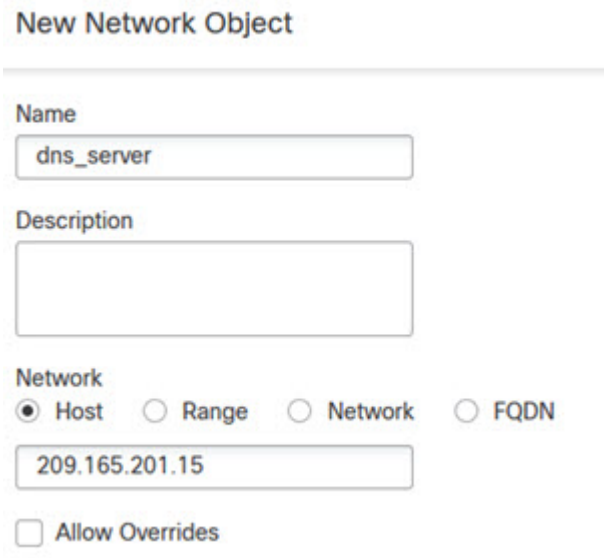
为网络对象命名（例如，ftp_server_v6），然后输入主机地址 2001:DB8::D1A5:C8E1。



f) 点击**保存 (Save)**。

g) 点击**添加网络 > 添加对象**并定义 DNS 服务器的实际地址。

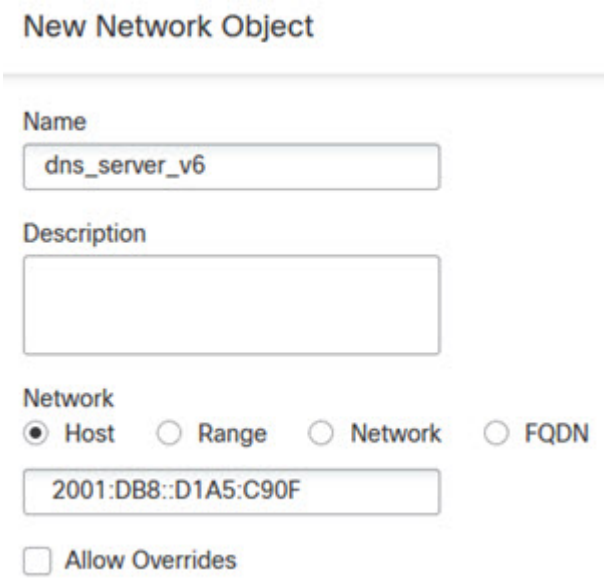
为网络对象命名（例如，dns_server），然后输入主机地址 209.165.201.15。



h) 点击**保存 (Save)**。

i) 点击**添加网络** > **添加对象**并定义 DNS 服务器的转换后 IPv6 地址。

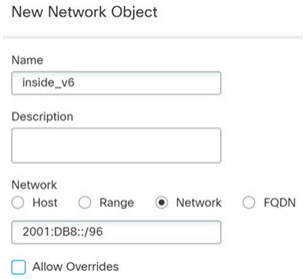
为网络对象命名（例如，dns_server_v6）并输入主机地址 2001:DB8::D1A5:C90F（其中 D1A5:C90F 是 209.165.201.15 的 IPv6 对应项）。



j) 点击**保存 (Save)**。

k) 点击**添加网络** > **添加对象**并定义内部 IPv6 网络。

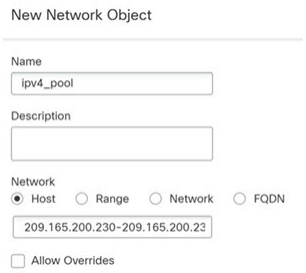
为网络对象命名（例如，inside_v6），然后输入网络地址 2001:DB8::/96。



l) 点击**保存 (Save)**。

m) 点击**添加网络** > **添加对象**并定义内部 IPv6 网络的 IPv4 PAT 池。

为网络对象命名（例如，ipv4_pool），然后输入范围 209.165.200.230-209.165.200.235。



n) 点击**保存 (Save)**。

步骤 2 为 FTP 服务器配置带 DNS 修改的静态 NAT 规则。

a) 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

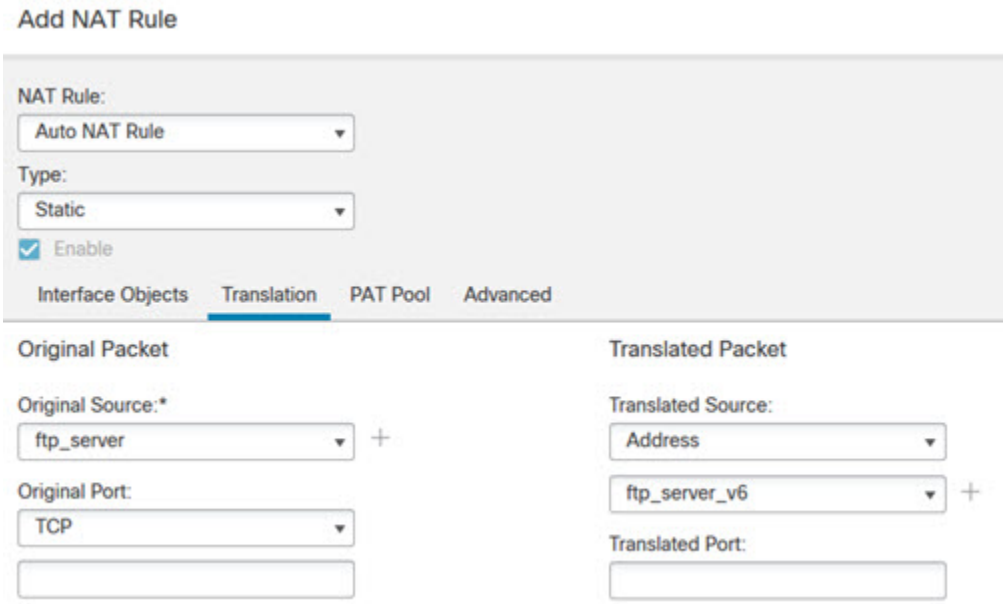
- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型** = 静态。

d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 外部。
- **目标接口对象** = 内部。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = ftp_server 网络对象。
- **转换后的源** > **地址 (Translated Source Address)** = ftp_server_v6 网络对象。



f) 在**高级 (Advanced)** 上，选择以下选项：

- **转换匹配该规则的 DNS 回复**。
- **网到网映射**，因为这是一对一 NAT46 转换。

g) 点击**确定**。

步骤 3 为 DNS 服务器配置静态 NAT 规则。

a) 点击**添加规则**。

b) 配置以下属性：

- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型** = 静态。

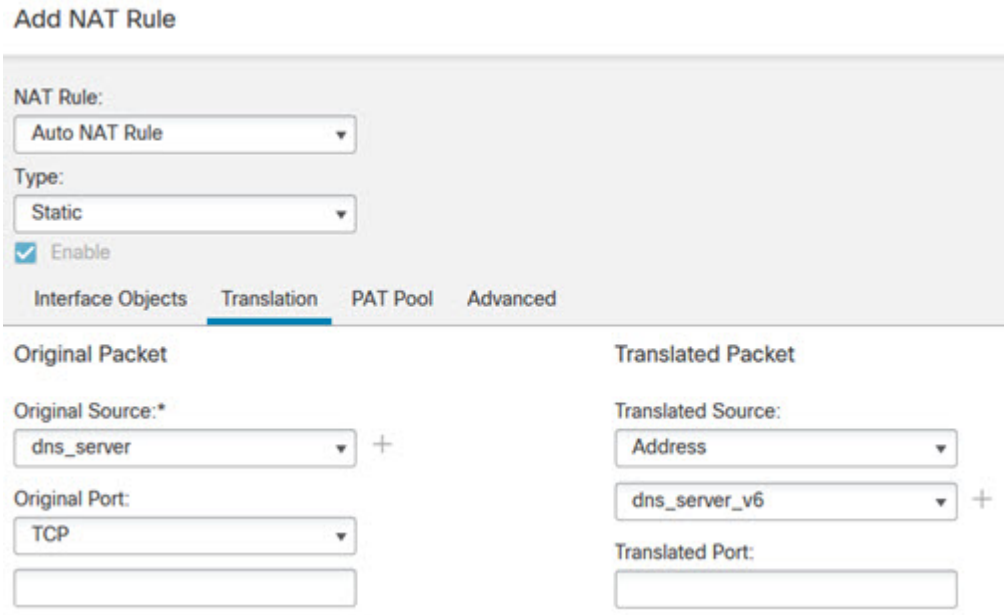
c) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 外部。
- **目标接口对象** = 内部。

d) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = dns_server 网络对象。
- **转换后的源 > 地址 (Translated Source Address)** = dns_server_v6 网络对象。

e) 在**高级 (Advanced)** 上，选择**网到网映射 (Net to Net Mapping)**，因为这是一对一 NAT46 转换。



f) 点击 **OK**。

步骤 4 为内部 IPv6 网络配置具有 PAT 池规则的动态 NAT。

a) 点击**添加规则**。

b) 配置以下属性：

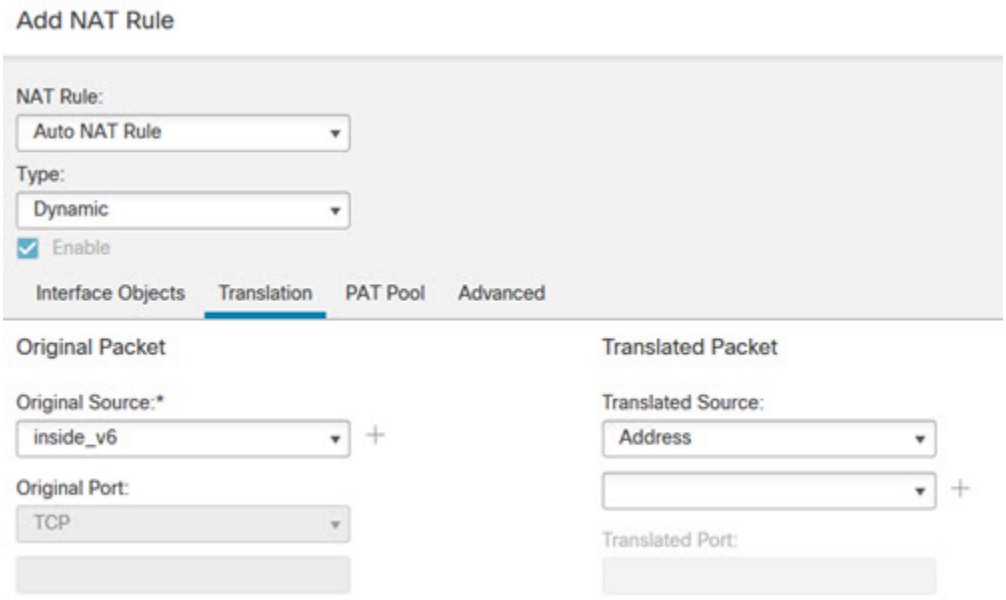
- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型 (Type)**= 动态。

c) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

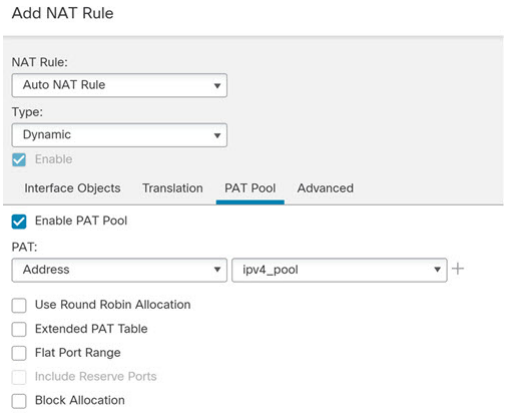
d) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = inside_v6 网络对象。
- **转换后的源** > **地址 (Translated Source Address)** = 将此字段留空。



e) 在 **PAT 池 (PAT Pool)** 中配置以下选项：

- **启用 PAT 池** = 选择此选项。
- **转换后的源** > **地址 (Translated Source Address)** = ipv4_pool 网络对象。



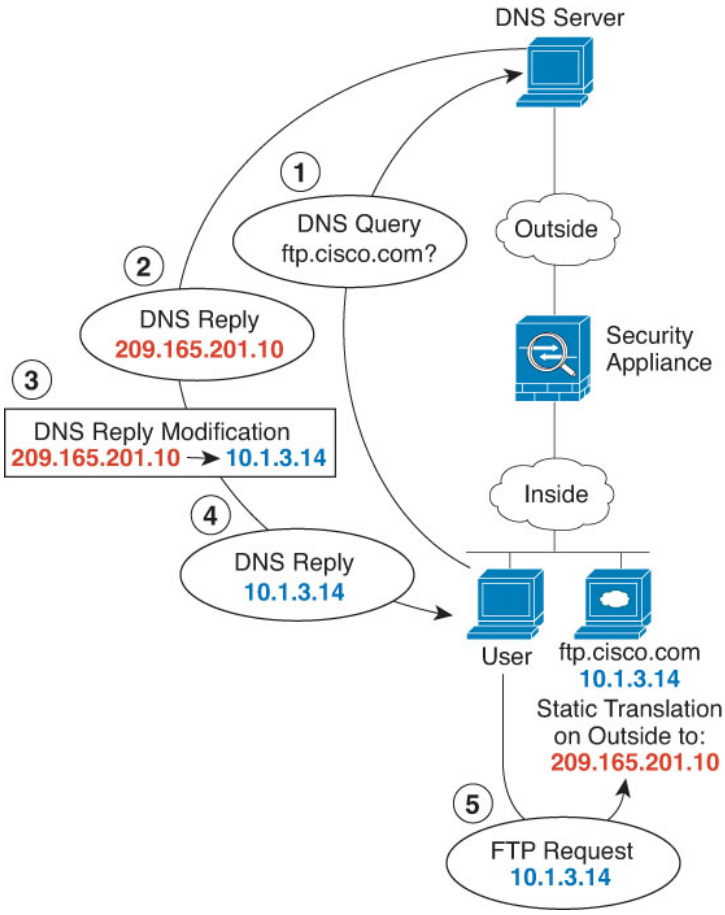
f) 点击**确定 (OK)**。

DNS 回复修改、外部接口上的 DNS 服务器

下图显示可从外部接口访问的 DNS 服务器。服务器 ftp.cisco.com 在内部接口上。将 NAT 配置为将 ftp.cisco.com 实际地址 (10.1.3.14) 静态转换为在外部网络上可见的映射地址 (209.165.201.10)。

在这种情况下，您要在此静态规则上启用 DNS 回复修改，以便使用实际地址访问 ftp.cisco.com 的内部用户可以接收来自 DNS 服务器的实际地址，而不是映射地址。

当内部主机发送对 ftp.cisco.com 的地址的 DNS 请求时，DNS 服务器将以映射地址 (209.165.201.10) 作为回复。系统引用内部服务器的静态规则，并将 DNS 回复中的地址转换为 10.1.3.14。如果不启用 DNS 回复修改，则内部主机尝试将流量发送到 209.165.201.10，而不是直接访问 ftp.cisco.com。



开始之前

确保具有包含用于设备的接口的接口对象（安全区或接口组）。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请依次选择**对象** > **对象管理**，然后选择**接口**。

过程

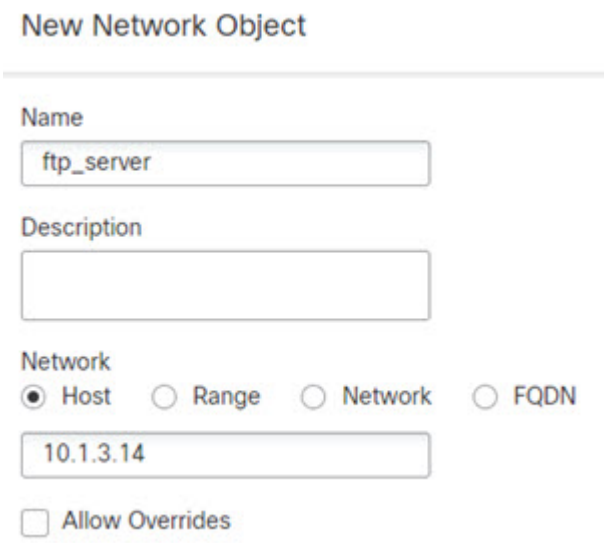
步骤 1 为 FTP 服务器创建网络对象。

a) 选择**对象** > **对象管理**。

b) 从目录中选择**网络 (Network)** 并点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

c) 定义实际 FTP 服务器地址。

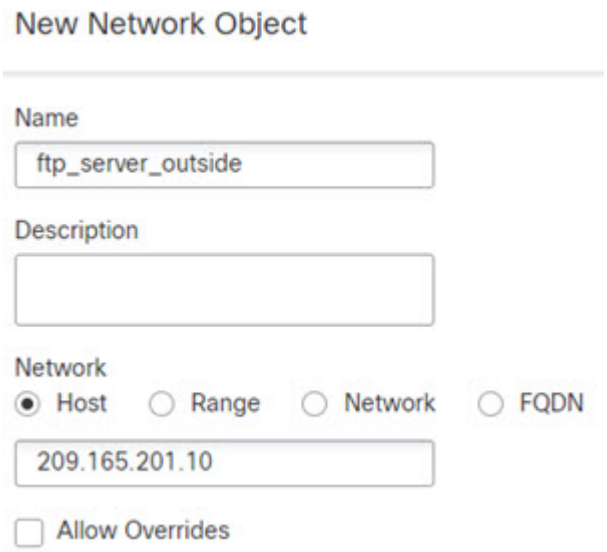
为网络对象命名（例如，ftp_server），然后输入主机地址 10.1.3.14。



d) 点击**保存 (Save)**。

e) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**，然后定义 FTP 服务器的转换后地址。

为网络对象命名（例如，ftp_server_outside），然后输入主机地址 209.165.201.10。



f) 点击**保存 (Save)**。

步骤 2 为 FTP 服务器配置带 DNS 修改的静态 NAT 规则。

a) 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。

- **类型** = 静态。

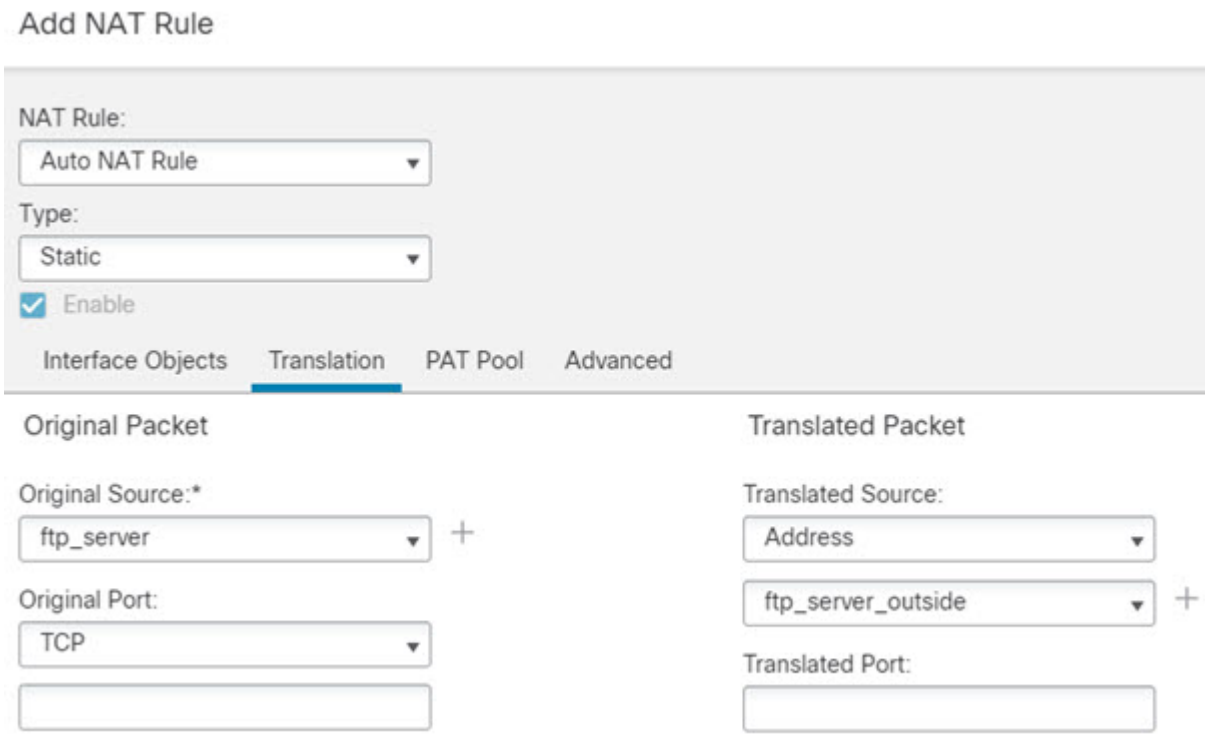
d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = ftp_server 网络对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = ftp_server_outside 网络对象。

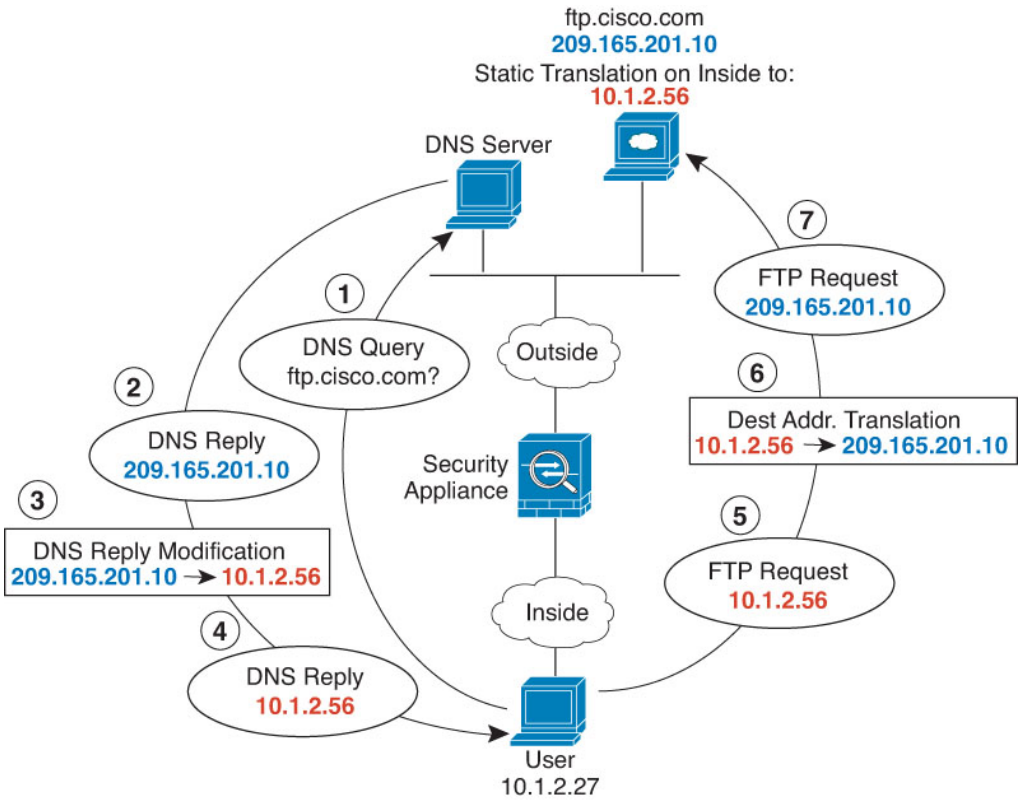
f) 在**高级 (Advanced)** 选项卡上，选择**转换与此规则匹配的 DNS 回复 (Translate DNS replies that match this rule)**。



g) 点击**确定 (OK)**。

DNS 回复修改、主机网络上的 DNS 服务器

下图显示外部网络上的 FTP 服务器和 DNS 服务器。系统有面向外部服务器的静态转换。在这种情况下，当内部用户从 DNS 服务器请求 ftp.cisco.com 的地址时，DNS 服务器将以实际地址 209.165.20.10 作为响应。由于您希望内部用户使用 ftp.cisco.com 的映射地址 (10.1.2.56)，因此需要配置 DNS 回复修改以进行静态转换。



开始之前

确保具有包含用于设备的接口的接口对象（安全区或接口组）。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请依次选择**对象** > **对象管理**，然后选择**接口**。

过程

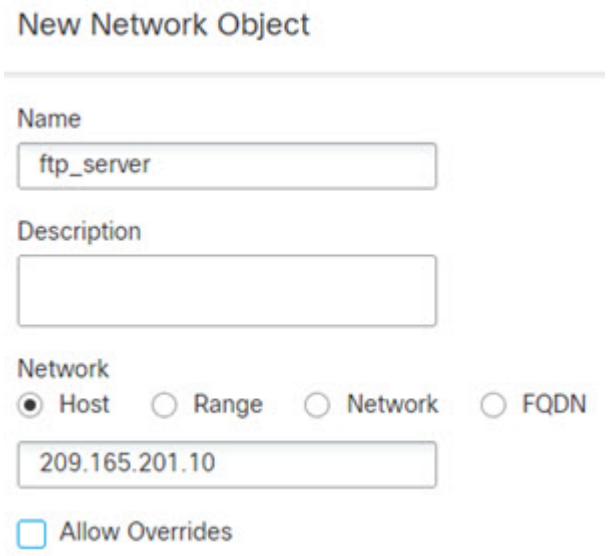
步骤 1 为 FTP 服务器创建网络对象。

a) 选择**对象** > **对象管理**。

b) 从目录中选择**网络 (Network)** 并点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

c) 定义实际 FTP 服务器地址。

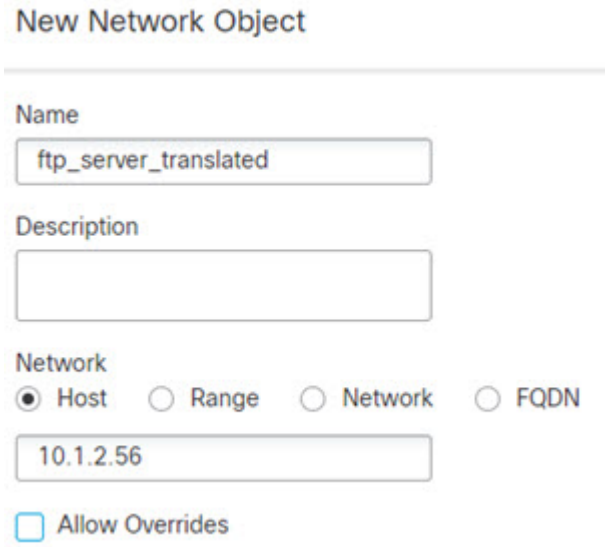
命名网络对象（例如，ftp_server），然后输入主机地址 209.165.201.10。



d) 点击**保存 (Save)**。

e) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**，然后定义 FTP 服务器的转换后地址。

命名网络对象（例如，ftp_server_translated），然后输入主机地址 10.1.2.56。



f) 点击**保存 (Save)**。

步骤 2 为 FTP 服务器配置带 DNS 修改的静态 NAT 规则。

a) 依次选择**设备** > **NAT**，并创建或编辑 威胁防御 NAT 策略。

b) 点击**添加规则**。

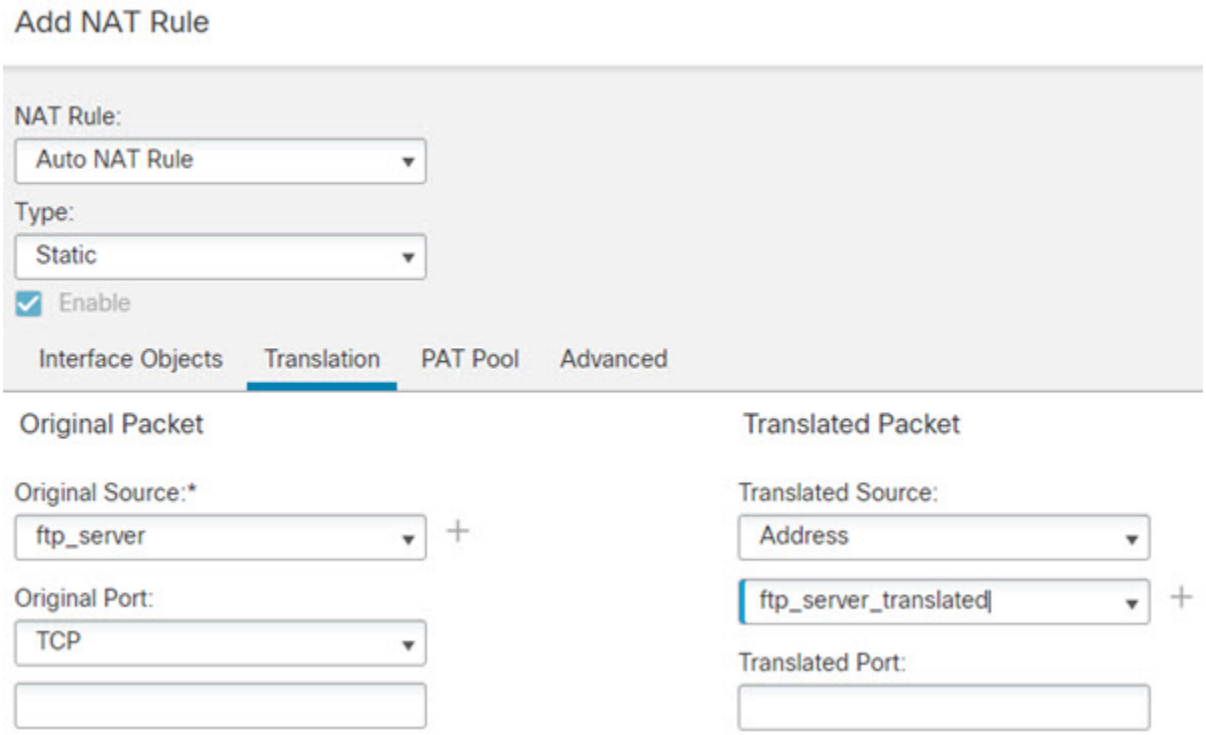
c) 配置以下属性：

- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型** = 静态。

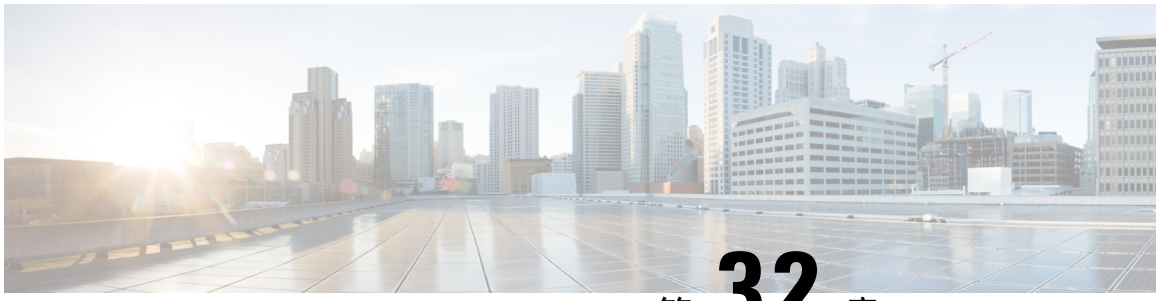
d) 在**接口对象 (Interface Objects)** 上配置以下选项：
   - **源接口对象** = 外部。
   - **目标接口对象** = 内部。

e) 在**转换 (Translation)** 上配置以下选项：
   - **原始源** = ftp_server 网络对象。
   - **转换后的源 > 地址 (Translated Source Address)** = ftp_server_translated 网络对象。

f) 在**高级 (Advanced)** 选项卡上，选择**转换与此规则匹配的 DNS 回复 (Translate DNS replies that match this rule)**。



g) 点击**确定 (OK)**。



第 32 章

思科 ISA 3000 的报警

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

关于报警

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

您可以将报警系统配置为监控以下对象：

- 电源。
- 主温度传感器和辅助温度传感器。
- 报警输入接口。

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

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

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

报警输入接口

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

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

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

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

报警输出接口

您可以将外部报警（如蜂鸣器或灯光）连接到报警输出接口。

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

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

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

系统日志报警

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

要让系统日志报警正常工作，您还必须启用诊断日志记录。选择**设备 (Device)** > **平台设置 (Platform Settings)**，添加或编辑分配给设备的 FTD 平台设置策略，并在**系统日志 (Syslog)** 页面上配置目标和设置。例如，您可以配置系统日志服务器、控制台日志记录或内部缓冲区日志记录。

如果未启用诊断日志记录的目标，报警系统不清楚向何处发送系统日志消息。

SNMP 报警

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

选择**设备 (Device)** > **平台设置 (Platform Settings)**，添加或编辑分配给设备的 FTD 平台设置策略，并在 **SNMP** 页面上启用 SNMP 并配置设置。

报警默认值

下表指定了报警输入接口（触点）、冗余电源和温度的默认值。

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

报警的要求和必备条件

型号支持

ISA 3000 上的 威胁防御。

支持的域

任意

用户角色

管理员

配置 ISA 3000 的报警

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

配置报警输入触点

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

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

过程

步骤 1 创建 FlexConfig 对象以配置警报输入联系人。

a) 选择**对象** > **对象管理**。

b) 从目录中选择 **FlexConfig** > **FlexConfig 对象 (FlexConfig Object)**。

c) 点击**添加 FlexConfig 对象 (Add FlexConfig Object)**，配置以下属性，然后点击**保存 (Save)**。

- **Name** - 对象名称。例如，Configure_Alarm_Contacts。
- **部署 (Deployment)** - 选择**每次 (Everytime)**。您想在每个部署中发送此配置，以确保其保持配置状态。
- **类型 (Type)** - 保留默认值**附加 (Append)**。这些命令会在直接支持的功能的命令之后被发送到设备。
- **对象正文 (Object body)** - 在对象正文中，键入配置警报联系人所需的命令。以下步骤介绍了这些命令。

d) 配置报警触点的说明。

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

例如，要将触点 1 的说明设置为“Door Open”，请输入以下命令：

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

e) 配置报警触点的严重性。

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

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

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

例如，要将触点 1 的严重级别设置为“Major”，请输入以下命令：

```
alarm contact 1 severity major
```

f) 配置报警触点的触发器。

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

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

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

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

```
alarm contact 1 trigger closed
```

g) 配置触发报警触点时采取的操作。

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

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

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

例如，要启用报警输入触点 1 的所有操作，请输入以下命令：

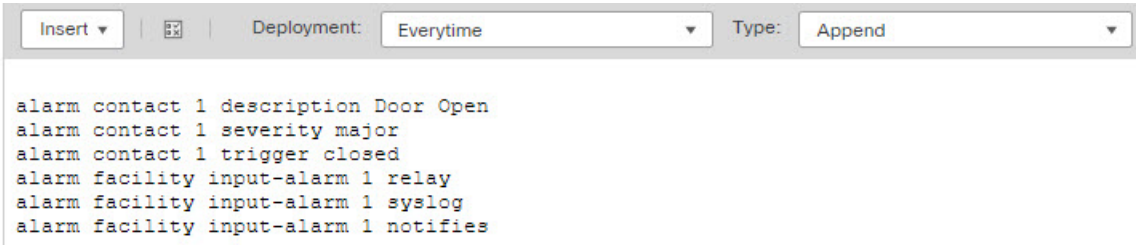
```
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

h) 验证对象正文是否包含您想要的命令。

例如，如果您的模板包含此过程中所示的所有命令示例，则对象正文将包含以下命令：

```
alarm contact 1 description Door Open
alarm contact 1 severity major
alarm contact 1 trigger closed
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

此对象正文应如下所示：



i) 点击**保存 (Save)**。

步骤 2 创建 FlexConfig 策略并将其分配给设备。

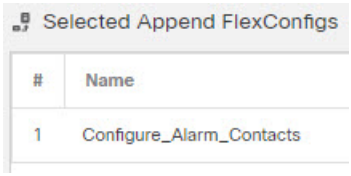
a) 选择**设备 (Devices)** > **FlexConfig**。

b) 点击**新建策略 (New Policy)**，或者如果现有 FlexConfig 策略应分配给（或已分配给）目标设备，则只需编辑该策略。

在创建新的策略时，请在为策略命名的对话框中将目标设备分配给策略。

c) 在目录的 **User Defined** 文件夹中选择警报联系人 FlexConfig 对象，然后点击 **>** 将其添加到策略中。

此对象应被添加到**所选附加 Flexconfig (Selected Appended FlexConfigs)** 列表中。



d) 点击**保存 (Save)**。

e) 如果尚未将所有目标设备分配给策略，请点击“保存”(Save)下面的**策略分配 (Policy Assignments)** 链接并立即进行分配。

f) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择一个已分配的设备。

系统会生成将被发送到设备的配置 CLI 预览。验证从 FlexConfig 对象生成的命令看起来是否正确。这些将在预览结束时显示。请注意，您还会看到通过对托管功能所做的其他更改而生成的命令。对于警报联系人命令，您应该会看到类似如下的内容：

```
###Flex-config Appended CLI ###
alarm contact 1 description Door Open
alarm contact 1 severity major
alarm contact 1 trigger closed
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

步骤 3 部署更改。

由于您已将 FlexConfig 策略分配给设备，因此您始终会收到部署警告，以提醒您有关 FlexConfig 的使用。点击**继续 (Proceed)** 以继续部署。

在部署完成后，您可以检查部署历史记录并查看部署脚本。如果部署失败，这一点尤为重要。请参阅验证部署的配置，第 2020 页。

配置电源报警

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

以下过程说明如何启用双电源模式下，以及如何配置电源报警。

过程

步骤 1 创建 FlexConfig 对象以配置电源警报。

a) 选择**对象** > **对象管理**。

b) 从目录中选择 **FlexConfig** > **FlexConfig 对象 (FlexConfig Object)**。

c) 点击**添加 FlexConfig 对象 (Add FlexConfig Object)**，配置以下属性，然后点击**保存 (Save)**。

- **Name** - 对象名称。例如，Power_Supply_Alarms。
- **部署 (Deployment)** - 选择**每次 (Everytime)**。您想在每个部署中发送此配置，以确保其保持配置状态。
- **类型 (Type)** - 保留默认值**附加 (Append)**。这些命令会在直接支持的功能的命令之后被发送到设备。
- **对象正文 (Object body)** - 在对象正文中，键入配置电源警报所需的命令。以下步骤介绍了这些命令。

d) 启用双电源模式。

power-supply dual

例如：

```
power-supply dual
```

e) 配置触发电源报警时要采取的操作。

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

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

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

例如，要启用电源报警的所有操作，请输入以下命令：

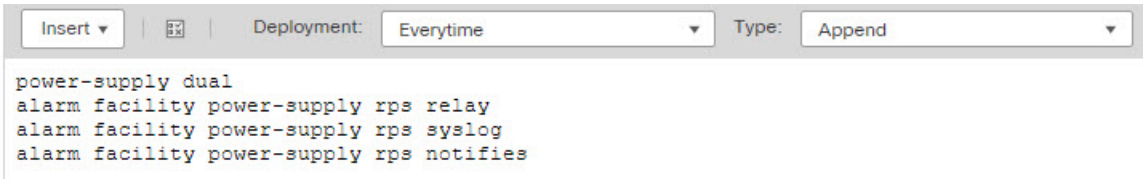
```
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

f) 验证对象正文是否包含您想要的命令。

例如，如果您的模板包含此过程中所示的所有命令示例，则对象正文将包含以下命令：

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

此对象正文应如下所示：



g) 点击**保存 (Save)**。

步骤 2 创建 FlexConfig 策略并将其分配给设备。

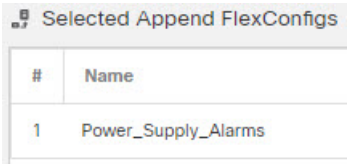
a) 选择**设备 (Devices)** > **FlexConfig**。

b) 点击**新建策略 (New Policy)**，或者如果现有 FlexConfig 策略应分配给（或已分配给）目标设备，则只需编辑该策略。

在创建新的策略时，请在为策略命名的对话框中将目标设备分配给策略。

c) 在目录的 **User Defined** 文件夹中选择电源警报 FlexConfig 对象，然后点击 **>** 将其添加到策略中。

此对象应被添加到**所选附加 Flexconfig (Selected Appended FlexConfigs)** 列表中。



d) 点击**保存 (Save)**。

e) 如果尚未将所有目标设备分配给策略，请点击“保存”(Save)下面的**策略分配 (Policy Assignments)** 链接并立即进行分配。

f) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择一个已分配的设备。

系统会生成将被发送到设备的配置 CLI 预览。验证从 FlexConfig 对象生成的命令看起来是否正确。这些将在预览结束时显示。请注意，您还会看到通过对托管功能所做的其他更改而生成的命令。对于电源警报命令，您应该会看到类似如下的内容：

```
###Flex-config Appended CLI ###
power-supply dual
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

步骤 3 部署更改。

由于您已将 FlexConfig 策略分配给设备，因此您始终会收到部署警告，以提醒您有关 FlexConfig 的使用。点击**继续 (Proceed)** 以继续部署。

在部署完成后，您可以检查部署历史记录并查看部署脚本。如果部署失败，这一点尤为重要。请参阅验证部署的配置，第 2020 页。

配置温度报警

您可以配置基于设备中 CPU 卡温度的警报。

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

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

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

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

因此，在实践中，您应为高温度和低温度仅配置主要设置或仅配置辅助设置。

过程

步骤 1 创建 FlexConfig 对象以配置温度警报。

a) 选择**对象** > **对象管理**。

b) 从目录中选择 **FlexConfig** > **FlexConfig 对象 (FlexConfig Object)**。

c) 点击**添加 FlexConfig 对象 (Add FlexConfig Object)**，配置以下属性，然后点击**保存 (Save)**。

- **Name** - 对象名称。例如，Configure_Temperature_Alarms。
- **部署 (Deployment)** - 选择**每次 (Everytime)**。您想在每个部署中发送此配置，以确保其保持配置状态。

- **类型 (Type)** - 保留默认值**附加 (Append)**。这些命令会在直接支持的功能的命令之后被发送到设备。
- **对象正文 (Object body)** - 在对象正文中，键入配置温度警报所需的命令。以下步骤介绍了这些命令。

d) 配置可接受的温度范围。

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

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

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

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

e) 配置触发温度报警时要采取的操作。

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

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

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

例如，要启用辅助温度报警的所有操作，请输入以下命令：

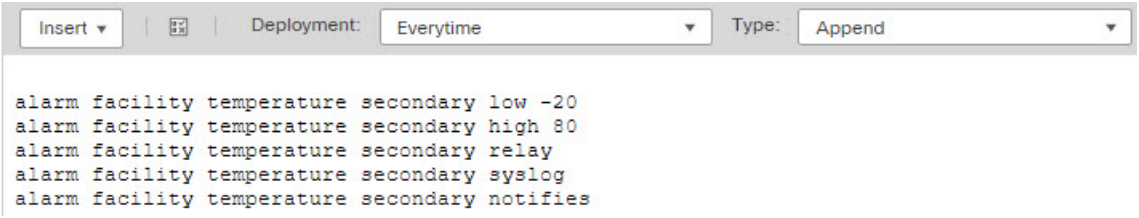
```
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

f) 验证对象正文是否包含您想要的命令。

例如，如果您的模板包含此过程中所示的所有命令示例，则对象正文将包含以下命令：

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

此对象正文应如下所示：



g) 点击**保存 (Save)**。

步骤 2 创建 FlexConfig 策略并将其分配给设备。

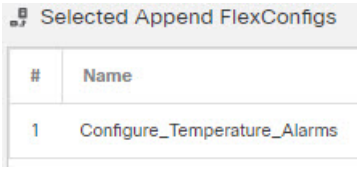
a) 选择**设备 (Devices)** > **FlexConfig**。

b) 点击**新建策略 (New Policy)**，或者如果现有 FlexConfig 策略应分配给（或已分配给）目标设备，则只需编辑该策略。

在创建新的策略时，请在为策略命名的对话框中将目标设备分配给策略。

c) 在目录的 **User Defined** 文件夹中选择温度警报 FlexConfig 对象，然后点击 **>** 将其添加到策略中。

此对象应被添加到**所选附加 Flexconfig (Selected Appended FlexConfigs)** 列表中。



d) 点击**保存 (Save)**。

e) 如果尚未将所有目标设备分配给策略，请点击“保存”(Save)下面的**策略分配 (Policy Assignments)** 链接并立即进行分配。

f) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择一个已分配的设备。

系统会生成将被发送到设备的配置 CLI 预览。验证从 FlexConfig 对象生成的命令看起来是否正确。这些将在预览结束时显示。请注意，您还会看到通过对托管功能所做的其他更改而生成的命令。对于温度警报命令，您应该会看到类似如下的内容：

```
###Flex-config Appended CLI ###
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

步骤 3 部署更改。

由于您已将 FlexConfig 策略分配给设备，因此您始终会收到部署警告，以提醒您有关 FlexConfig 的使用。点击**继续 (Proceed)** 以继续部署。

在部署完成后，您可以检查部署历史记录并查看部署脚本。如果部署失败，这一点尤为重要。请参阅验证部署的配置，第 2020 页。

监控报警

以下主题介绍如何监控和管理报警。

监控报警状态

您可以在 CLI 中使用以下命令监控报警。

- **show alarm settings**

  显示每个可能的报警的当前配置。

- **show environment alarm-contact**

  显示输入报警触点的物理状态信息。

- **show facility-alarm relay**

  显示有关已触发输出中继的报警信息。

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

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

监控报警系统日志消息

根据您配置的报警类型，您可能会看到以下系统日志消息。

双电源报警

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

温度报警

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

- %FTD-6-806001：主要报警 CPU 温度高 *Celsius*
- %FTD-6-806002：CPU 高温主要报警已清除
- %FTD-6-806003：主要报警 CPU 温度低 *Celsius*
- %FTD-6-806004：CPU 低温主要报警已清除
- %FTD-6-806005：辅助报警 CPU 温度高 *Celsius*
- %FTD-6-806006：CPU 高温辅助报警已清除
- %FTD-6-806007：辅助报警 CPU 温度低 *Celsius*

- %FTD-6-806008：CPU 低温辅助报警已清除

报警输入触点报警

在这些报警中，*description* 是您所配置触点的说明。

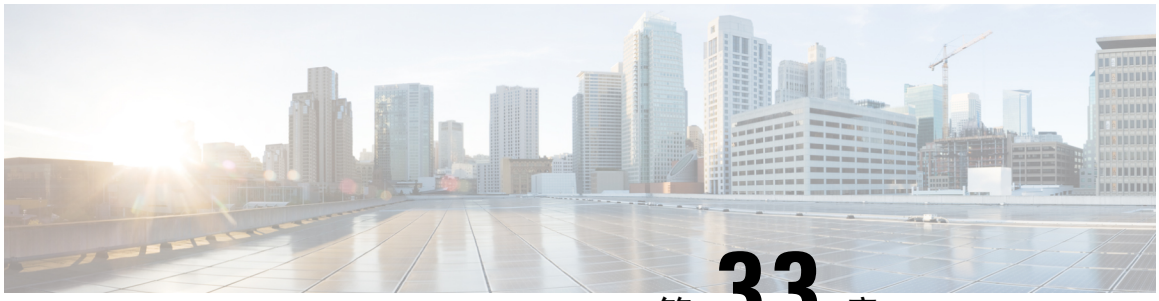
- %FTD-6-806009：与 ALARM_IN_1 *alarm_1_description* 对应的报警已确定
- %FTD-6-806010：与 ALARM_IN_1 *alarm_1_description* 对应的报警已清除
- %FTD-6-806011：与 ALARM_IN_2 *alarm_2_description* 对应的警报已确定
- %FTD-6-806012：与 ALARM_IN_2 *alarm_2_description* 对应的报警已清除

关闭外部报警

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

第 X 部分

路由



第 33 章

静态和默认路由

本章介绍如何在 威胁防御上配置静态路由和默认路由。

关于静态路由和默认路由

要将流量路由到非连接的主机或网络，必须使用静态路由或动态路由定义到主机或网络的路由。通常，您必须配置至少一个静态路由：所有流量的默认路由（不是通过其他方式路由到默认网络网关），通常是指下一跳路由器。

默认路由

最简单的方法是配置一个默认静态路由，将所有流量都发送到上游路由器，从而依靠该路由器来为您路由流量。默认路由对网关 IP 地址进行标识，威胁防御设备将所有不具有已获悉或静态路由的数据包发送到该网关地址。默认静态路由是以 0.0.0.0/0 (IPv4) 或 ::/0 (IPv6) 作为目标 IP 地址的静态路由。

应始终定义一个默认路由。

由于 威胁防御 使用用于数据流量和管理流量的单独路由表，所以，您可以选择配置数据流量的默认路由和管理流量的另一默认路由。请注意，关联设备流量默认使用管理专用或数据路由表，具体取决于类型（请参阅管理流量的路由表，第 801 页），但如果未找到路由，则会退回至其他路由表。默认路由将始终匹配流量，并将阻止退回至其他路由表。在这种情况下，如果接口不在默认路由表中，则必须指定要用于出口流量的接口。诊断接口包含在管理专用表中。特殊管理接口使用单独的 Linux 路由表，并有自己的默认路由。请参阅 **configure network** 命令。

静态路由

在以下情况下，您可能希望使用静态路由：

- 您的网络使用不受支持的路由器发现协议。
- 网络规模较小，并且可以轻松管理静态路由。
- 不希望流量或 CPU 开销与路由协议相关联。
- 在某些情况下，仅使用默认路由并不足够。默认网关可能无法到达目标网络，因此还必须配置更具体的静态路由。例如，如果默认网关在外部，则默认路由无法将直接流量定向到未直接与威胁防御设备连接的任何内部网络。
- 您使用的是不支持动态路由协议的功能。
- 虚拟路由器使用静态路由来创建路由泄漏。路由泄漏使流量从虚拟路由器的接口流向另一个虚拟路由器中的另一个接口。有关详细信息，请参阅互联虚拟路由器，第 808 页。

使用到 null0 接口的路由丢弃不必要的流量

通过访问规则，您可以根据其报头中包含的信息过滤数据包。到null0接口的静态路由是访问规则的补充性解决方案。您可以使用 null0 路由转发不必要或不需要的流量，从而丢弃该流量。

静态 null0 路由具有良好的性能配置文件。您还可以使用静态 null0 路由防止产生路由环路。BGP 可以利用静态 null0 路由进行远程触发黑洞路由。

路由优先级

- 标识具体目标的路由优先于默认路由。
- 当存在通向同一目标的多个路由（静态或动态）时，路由的管理距离即可确定优先级。静态路由设置为 1，因此其通常是优先级最高的路由。
- 当您具有多个管理距离相同的通向同一目标的静态路由时，请参阅等价多路径 (ECMP) 路由，第 802 页。
- 对于来自具有 Tunneled 选项的隧道的新流量，此路由覆盖任何其他已配置或已知悉的默认路由。

透明防火墙模式和网桥组路由

对于源自 威胁防御设备并且通过网桥组成员接口为非直接连接网络定义的流量，需要配置默认路由或静态路由，以使 威胁防御设备了解通过哪个网桥组成员接口发出流量。源自 威胁防御设备 的流量可能包括与系统日志服务器或 SNMP 服务器的通信。如果存在无法通过单个默认路由进行访问的服务器，则必须配置静态路由。对于透明模式，不能将 BVI 指定为网关接口；只能使用成员接口。对于路由模式下的网桥组，必须在静态路由中指定 BVI；不能指定成员接口。有关详细信息，请参阅#unique_889。

静态路由跟踪

使用静态路由的一个问题是，缺乏用于确定路由处于开启还是关闭状态的内在机制。即使下一跳网关变得不可用，这些路由依然保留在路由表中。只有威胁防御设备上的关联接口发生故障时，才会从路由表中删除静态路由。

静态路由跟踪功能提供在主路由发生故障的情况下跟踪静态路由的可用性和安装备用路由的方法。例如，您可以定义一条到 ISP 网关的默认路由和一条到辅助 ISP的备用默认路由，以防主 ISP 不可用。

威胁防御设备 通过将静态路由与 威胁防御设备 使用 ICMP 回应请求监控的目标网络上的监控目标主机相关联来实施静态路由跟踪。如果在指定时间内没有收到回应回复，则主机将被视为关闭，并且会从路由表中删除关联路由。使用具有较高指标的未跟踪备用路由替代已删除的路由。

选择监控目标时，您需要确保它能够响应 ICMP 回应请求。该目标可以是您选择的任何网络对象，但是应考虑使用以下对象：

- ISP 网关（用于支持双 ISP）地址
- 下一跳网关地址（如果您关注网关的可用性）
- 目标网络上的服务器，例如 威胁防御设备 需要与之进行通信的系统日志服务器
- 目标网络上的持久网络对象

注释 可能会在夜间关闭的 PC 不是一个理想选择。

您可以为静态定义的路由或通过 DHCP 或 PPPoE 获取的默认路由配置静态路由跟踪。您只能在配置了路由跟踪的多个接口上启用 PPPoE 客户端。

静态路由的要求和必备条件

型号支持

威胁防御

支持的域

任意

用户角色

管理员

网络管理员

静态和默认路由指南

防火墙模式和网桥组

- 在透明模式下，静态路由必须使用桥接组成员接口作为网关；不能指定 BVI。
- 在路由模式下，必须指定 BVI 作为网关；不能指定成员接口。
- 静态路由跟踪不支持网桥组成员接口或 BVI。

支持的网络地址

- IPv6 不支持静态路由跟踪。
- ASA 不支持 CLASS E 路由。因此，E 类网络不可作为静态路由进行路由。

群集和多情景模式

- 在集群中，仅主设备上支持静态路由跟踪。
- 多情景模式下不支持静态路由跟踪。

网络对象组

配置静态路由时，不能使用一系列网络对象或具有一系列 IP 地址的网络对象组。

ASP 和 RIB 路由条目

在 ASP 路由表中捕获设备上安装的所有路由及其距离。这对于所有静态和动态路由协议都是通用的。在 RIB 表中仅捕获最佳距离路由。

添加静态路由

静态路由用于定义为特定目标网络发送流量的位置。至少应定义一个默认路由。默认路由是以0.0.0.0/0作为目标 IP 地址的静态路由。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置静态路由的虚拟路由器。

步骤 4 选择 **静态路由**。

步骤 5 点击**添加路由**。

步骤 6 点击 **IPv4** 或 **IPv6**，具体取决于要添加的静态路由的类型。

步骤 7 选择此静态路由应用至的**接口**。

对于透明模式，选择网桥组成员接口名称。对于具有网桥组的路由模式，您可以为 BVI 名称选择网桥组成员接口。要将不必要的流量转发到“黑洞”，请选择 **Null0** 接口。

对于使用虚拟路由的设备，您可以选择属于其他虚拟路由器的接口。如果要将流量从此虚拟路由器泄漏到另一个虚拟路由器，可以创建此类静态路由。有关详细信息，请参阅互联虚拟路由器，第 808 页。

步骤 8 在**可用网络**列表中，选择目标网络。

要定义默认路由，请创建一个具有地址 0.0. 0.0/0 的对象，然后在此处选择它。

注释 虽然你可以创建和选择一个包含 IP 地址范围的网络对象组，但 管理中心 不支持在配置静态路由时使用网络对象范围。

步骤 9 在**网关**或 **IPv6 网关**字段中，输入或选择是次路由下一跳的网关路由器。您可以提供 IP 地址或网络/主机对象。当您为虚拟路由器使用静态路由配置泄漏路由时，请勿指定下一跳网关。

步骤 10 在**指标**字段中，输入到目标网络的跳数。有效值范围为 1 到 255；默认值为 1。指标是基于到特定主机所在的网络的跳数对路由的“开销”的一种衡量。跳计数是网络数据包在到达最终目标之前必须遍历的网络数，包括目标网络。指标用于比较不同路由协议之间的路由。静态路由的默认管理距离为 1，这使其优先于动态路由协议所发现的路由，但不优先于直连路由。OSPF 所发现路由的默认管理距离为 110。如果静态路由与动态路由的管理距离相同，则静态路由优先。已连接的路由始终优先于静态路由或动态发现的路由。

步骤 11 （可选） 对于默认路由，选中**隧道**复选框可为 VPN 流量定义单独的默认路由。

如果希望 VPN 流量使用与非 VPN 流量不同的默认路由，可以为 VPN 流量定义单独的默认路由。例如，从VPN连接传入的流量可以轻松定向到内部网络，而来自内部网络的流量可以定向到外部。使用“隧道”选项创建默认路由时，来自终止于无法使用已获悉或静态路由进行路由的设备的隧道的所有流量都会发送到该路由。对于每台设备，您只能配置一条默认的隧道网关。不支持隧道流量的 ECMP。

步骤 12 （仅 IPv4 静态路由）要监控路由可用性，请在**路由跟踪**字段中输入或选择定义监控策略的 SLA（服务级别协议）监控对象的名称。

请参阅SLA 监控器，第 1037 页。

步骤 13 点击**确定**。

路由参考

此部分介绍有关路由如何在 威胁防御 内部运行的基本概念。

确定路径

路由协议使用指标来评估传播数据包的最佳路径。指标是一种测量标准，例如供路由算法用于确定目标的最佳路径的路径带宽。为帮助执行确定路径的过程，路由算法会初始化和维护其中包含路由信息的路由表。路由信息根据所使用的路由算法而异。

路由算法使用各种信息来填充路由表。目标或下一跳关联告知路由器，可以通过将数据包发送到特定路由器（表示通往最终目标的下一跳）来以最优路径到达特定目标。当路由器收到传入数据包时，会检查目标地址并尝试将此地址与下一跳关联。

路由表还包含其他信息，例如有关路径可取性的数据。路由器通过比较指标来确定最佳路由，而这些指标根据所使用的路由算法的设计而异。

路由器互相进行通信，并通过传输各种消息来维护其路由表。路由更新消息是通常由路由表的全部或部分内容组成的消息。通过分析来自所有其他路由器的路由更新，路由器可以构建详细的网络拓扑图。链路状态通告（路由器之间发送的另一种消息）用于告知其他路由器发送方链路的状态。链路信息还可用于构建完整网络拓扑图，以使路由器能够确定通向网络目标的最佳路径。

支持的路由类型

路由器可以使用多种路由类型。威胁防御设备 使用以下路由类型：

- 静态与动态
- 单路径与多路径
- 平面与分层
- 链路状态与距离矢量

静态与动态

静态路由算法实际上是网络管理员建立的表映射。除非网络管理员修改这些映射，否则映射不会发生更改。使用静态路由的算法设计简单，并且在网络流量相对可预测且网络设计相对简单的环境下适用。

由于静态路由系统无法对网络更改作出反应，因此通常被认为不适合大型且不断变化的网络。大多数主要的路由算法为动态路由算法，这些算法通过分析传入路由更新消息来适应变化的网络环境。如果有消息表明网络发生更改，则路由软件会重新计算路由并发出新的路由更新消息。这些消息会渗入网络，促使路由器重新运行其算法并相应地更改其路由表。

可以酌情使用静态路由对动态路由算法进行补充。例如，可以将必备路由器（所有无法路由的数据包都发送到的路由器的默认路由）指定为所有无法路由的数据包的存储库，从而确保所有消息都至少以某种方式进行处理。

单路径与多路径

某些综合路由协议支持指向同一目标的多个路径。与单路径算法不同，这些多路径算法允许流量在多条线路上多路复用。多路径算法的优势在于显著提高吞吐量和可靠性，通常称为负载共享。

平面与分层

某些路由算法在平面空间中运行，而其他算法则使用路由层次结构。在平面路由系统中，路由器是所有其他路由器的对等体。在分层路由系统中，某些路由器形成实际上的路由主干。来自非主干路由器的数据包会传播到主干路由器，在此数据包通过主干进行发送，直至到达目标的大致区域。此时，数据包通过一个或者多个非主干路由器从最后一个主干路由器传播到最终目标。

路由系统通常会指定一些逻辑节点组，称为域、自治系统或区域。在分层系统中，一个域中的一些路由器可以与其他域中的路由器进行通信，而其他路由器只能与其本域中的路由器进行通信。在超大网络中，还可能存在其他分层级别，其中位于最高分层级别的路由器形成路由主干。

分层路由的主要优点在于，它会模仿大多数公司的组织，从而很好地支持这些公司的流量模式。大多数网络通信发生在小型公司组（域）中。由于域内路由器只需知道其域中的其他路由器即可，因此可以简化这些路由器的路由算法，并根据所使用的路由算法相应地减少路由更新流量。

链路状态与距离矢量

链路状态算法（也称最短路径优先算法）将路由信息以泛洪形式发送给互联网络中的所有节点。但是，每条路由器仅发送用于说明其自身链路状态的路由表部分。在链路状态算法中，每条路由器在其路由表中构建整个网络的情景。距离矢量算法（也称为 Bellman-Ford 算法）要求每条路由器仅向其邻居发送其路由表的全部或部分内容。实质上，链路状态算法会四处发送小的更新，而距离矢量算法只将较大的更新发送给相邻路由器。距离矢量算法仅知道其邻居。通常，链路状态算法与OSPF路由协议结合使用。

支持的互联网路由协议

威胁防御设备 支持多种互联网路由协议。本节对每种协议进行简单介绍。

- 增强型内部网关路由协议 (EIGRP)

  EIGRP 是思科专有协议，用于提供与 IGRP 路由器的兼容性和无缝互操作性。通过自动重分发机制，可将 IGRP 路由导入到增强型 IGRP（反之亦然），从而可以将增强型 IGRP 逐渐添加到现有 IGRP 网络。

- 开放最短路径优先 (OSPF)

  OSPF 是由互联网工程任务小组 (IETF) 的内部网关协议 (IGP) 工作小组开发的面向互联网协议 (IP) 网络的路由协议。OSPF 使用链路状态算法构建和计算所有到达已知目标的最短路径。OSPF 区域中的每条路由器包含相同的链路状态数据库，该数据库是由每条路由器可使用的接口和可访问邻居组成的列表。

- 路由信息协议 (RIP)

  RIP 是一种使用跳数作为指标的距离矢量协议。RIP 广泛用于路由全局互联网中的流量，并且是一种内部网关协议 (IGP)，意味着在单个自治系统内执行路由。

- 边界网关协议 (BGP)

  BGP 是一种自治系统间路由协议。BGP 用于交换互联网的路由信息，并且是互联网服务提供商 (ISP) 之间所使用的协议。客户连接到 ISP，然后 ISP 使用 BGP 交换客户路由和 ISP 路由。在自

治系统 (AS) 之间使用 BGP 时，该协议称为外部 BGP (EBGP)。如果运营商使用 BGP 在 AS 内交换路由，则此协议称为内部 BGP (IBGP)。

路由表

威胁防御对数据流量（通过设备）和管理流量（来自设备）使用单独的路由表。本部分介绍路由表的工作原理。有关管理路由表的信息，另请参阅 管理流量的路由表，第 801 页。

路由表的填充方式

威胁防御 路由表可以通过静态定义的路由、直连路由以及动态路由协议发现的路由来填充。由于威胁防御 设备除具有路由表中的静态路由和已连接路由外，还可以运行多条路由协议，因此可通过多种方式发现或输入同一路由。当在路由表中放入同一目标的两条路由时，将按如下确定保留在路由表中的路由：

- 如果两个路由具有不同的网络前缀长度（网络掩码），则会将两个路由都视为唯一并输入到路由表中。然后，由数据包转发逻辑确定使用哪一条路由。

  例如，如果 RIP 和 OSPF 进程发现以下路由：

  - RIP：192.168.32.0/24
  - OSPF：192.168.32.0/19

  即使 OSPF 路由具有更好的管理距离，但由于两条路由具有不同的前缀长度（子网掩码），因此均会安装在路由表中。这两条路由被视为不同目标，数据包转发逻辑会确定使用哪条路由。

- 如果 威胁防御 设备从单个路由协议（例如 RIP）获悉通向同一目标的多条路径，则会在路由表中输入具有更佳指标的路由（由路由协议确定）。

  度量是与特定路由关联的值，从最高优先到最低优先进行排序。用于确定度量的参数根据路由协议而异。具有最低指标的路径选择作为最佳路径并安装在路由表中。如果有多个度量相等的通向同一目的地的路径，则会在这些等价路径上进行负载均衡。

- 如果 威胁防御 设备从多个路由协议获悉目标，则会比较路由的管理距离，并在路由表中输入管理距离较短的路由。

路由的管理距离

您可以更改由路由协议发现或重分发到路由协议中的路由的管理距离。如果来自两个不同路由协议的两条路由具有相同的管理距离，则会将具有较短默认管理距离的路由输入到路由表中。对于EIGRP 和 OSPF 路由，如果 EIGRP 路由和 OSPF 路由具有相同的管理距离，则默认选择 EIGRP 路由。

管理距离是 威胁防御设备在有两个或多个通向同一目标（来自两个不同路由协议）的路由时，用于选择最佳路径的路由参数。由于路由协议具有基于不同于其他协议的算法的度量，因此并非总能够确定通向由不同路由协议生成的同一目的地的两条路由的最佳路径。

每个路由协议使用管理距离值划分优先级。下表显示 威胁防御设备支持的路由协议的默认管理距离值。

表 *77:* 受支持的路由协议的默认管理距离

路由源	默认管理距离
已连接的接口	0
VPN 路由	1
静态路由	1
EIGRP 汇总路由	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
IS-IS	115
RIP	120
EIGRP 外部路由	170
内部和本地 BGP	200
未知	255

管理距离值越小，协议的优先等级越高。例如，如果 威胁防御设备从 OSPF 路由进程（默认管理距离 - 110）和 RIP 路由进程（默认管理距离 - 120）均收到通向特定网络的路由，则 威胁防御设备 会选择 OSPF 路由，因为 OSPF 具有更高的优先级。在这种情况下，路由器会将 OSPF 版本的路由添加到路由表。

VPN 通告路由 (V-Route/RRI)）相当于默认管理距离为 1 的静态路由。但与网络掩码 255.255.255.255 一样，它具有更高的优先级。

在本示例中，如果 OSPF 派生路由的源丢失（例如，由于电源关闭），则 威胁防御设备会使用 RIP 派生路由，直至 OSPF 派生路由再次出现。

管理距离是一项本地设置。例如，如果您更改通过 OSPF 获取的路由的管理距离，那么这种更改只会影响在其上输入该命令的 威胁防御设备的路由表。在路由更新中不会通告管理距离。

管理距离不影响路由进程。路由进程仅通告路由进程已发现或重分发到路由进程中的路由。例如，即使在 路由表中使用 OSPF 路由进程发现的路由，RIP 路由进程也会通告 RIP 路由。

备份动态和浮动静态路由

当由于安装另一条路由而导致初始尝试将路由安装在路由表中失败时，系统会注册备用路由。如果安装在路由表中的路由失败，则路由表维护进程会呼叫已注册备用路由的每个路由协议进程，并请求它们重新在路由表中安装此路由。如果有多个协议为失败路由注册了备用路由，则根据管理距离选择优先路由。

鉴于以上过程，当动态路由协议发现的路由失败时，您可以创建安装在路由表中的浮动静态路由。浮动静态路仅仅是配置有比 威胁防御设备上运行的动态路由协议更大的管理距离的静态路由。当动态路由进程发现的对应路由失败时，会在路由表中安装静态路由。

如何制定转发决策

系统按如下制定转发决策：

- 如果目的不匹配路由表中的条目，则通过为默认路由指定的接口转发数据包。如果尚未配置默认路由，则会丢弃数据包。
- 如果目的匹配路由表中的单个条目，则通过与该路由关联的接口转发数据包。
- 如果目的匹配路由表中的多个条目，则通过与具有较长网络前缀的路由相关联的接口转发数据包。

例如，发往 192.168.32.1 的数据包到达在路由表中拥有以下路由的接口：

- 192.168.32.0/24 网关 10.1.1.2
- 192.168.32.0/19 网关 10.1.1.3

在这种情况下，发往 192.168.32.1 的数据包直接发送到 10.1.1.2，因为 192.168.32.1 属于 192.168.32.0/24 网络。它也属于路由表中的其他路由，但 192.168.32.0/24 在路由表中的前缀最长（24 位对比 19 位）。在转发数据包时，较长前缀始终优先于较短的前缀。

注释 即便新的相似连接将因路由中的变化而导致不同行为，现有连接也将继续使用其已建立的接口。

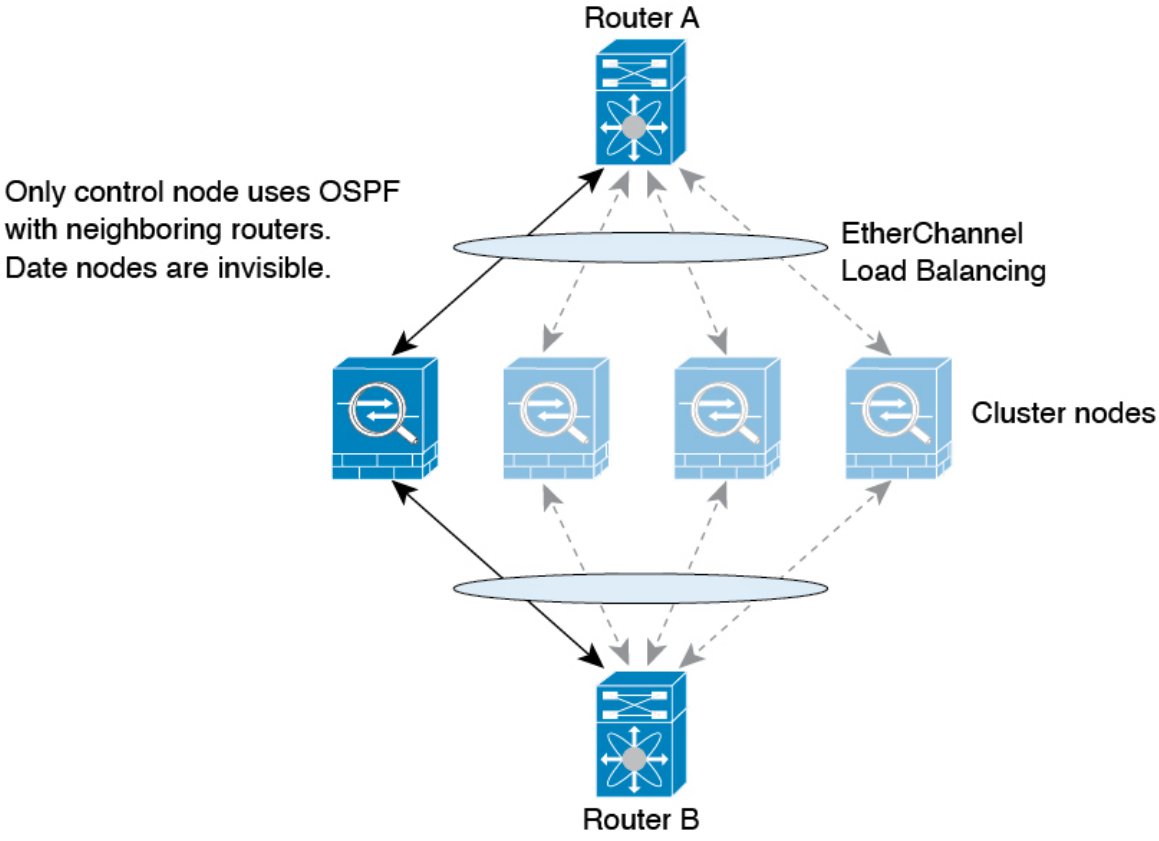
动态路由和高可用性

当主用设备上的路由表发生更改时，在备用设备上同步动态路由。这意味着主用设备上的所有添加、删除或更改都将立即传播到备用设备。如果备用设备在主用/备用就绪 高可用性对中处于活动状态，则它会有与前一个主用设备相同的路由表，因为路由作为 高可用性批量同步和连续复制过程的一部分进行同步。

群集下的动态路由

路由过程仅在控制节点上运行，并且通过控制节点学习路线后复制到数据节点。如果路由数据包到达数据节点，它将重定向到控制节点。

图 *120:* 集群下的动态路由



在数据节点向控制节点学习路线后，每个节点将单独做出转发决策。

OSPF LSA 数据库不会从控制节点同步到数据节点。如果切换了控制节点，邻近路由器将检测到重新启动；切换是不透明的。OSPF 进程将挑选一个 IP 地址作为其路由器 ID。您可以分配一个静态路由器 ID，尽管不要求这样做，但这可以确保整个集群中使用的路由器 ID 一致。请参阅 OSPF 无间断转发功能，解决中断问题。

管理流量的路由表

作为一项标准安全实践，通常需要将管理（关联设备）流量与数据流量分开并隔离。要实现这种隔离，威胁防御为管理专用流量和数据流量使用单独的路由表。单独的路由表意味着您也可以创建用于数据和管理的单独默认路由。

每个路由表的流量类型

关联设备流量始终使用数据路由表。

关联设备流量（根据类型）在默认情况下使用管理专用路由表或数据路由表。如果在默认路由表中找不到匹配项，则会检查其他路由表。

- 管理专用路由表关联设备流量包括 AAA 服务器通信。

- 数据路由表关联设备流量包括 DNS 服务器查找和 DDNS。例外情况是，如果您仅为 DNS 指定诊断接口，则 威胁防御 将仅使用管理专用路由表。

管理专用路由表中包含的接口

管理专用接口包括所有诊断x/x 接口以及您配置为管理专用接口的所有接口。

注释 管理逻辑接口使用自己的 Linux 路由表，该路由表不是 威胁防御 路由查找的一部分。源自管理接口的流量包括管理中心通信、许可通信和数据库更新。另一方面，诊断逻辑接口使用本节所述的管理专用路由表。

回退到其他路由表

如果在默认路由表中找不到匹配项，则会检查其他路由表。

使用非默认路由表

如果您需要传出流量退出默认路由表中不存在的接口，则您可能需要在配置接口时指定接口，而不是依赖于回到另一个表。威胁防御 设备仅检查指定接口的路由。例如，如果您需要通过数据接口与 RADIUS 服务器通信，则在 RADIUS 配置中指定该接口。否则，如果管理专用路由表中具有默认路由，则将匹配默认路由且绝不回退到数据路由表。

动态路由

管理专用路由表支持独立于数据接口路由表的动态路由。给定的动态路由进程必须在管理专用接口或数据接口上运行；不能将两种类型混用。

等价多路径 (ECMP) 路由

威胁防御设备支持等价多路径 (ECMP) 路由。

每个接口最多支持 8 个等价静态或动态路由。例如，您可以在外部接口上配置多个默认路由，指定不同的网关：

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

在这种情况下，流量在外部接口上的 10.1.1.2、10.1.1.3 和 10.1.1.4 之间进行负载均衡。流量基于散列源和目标 IP 地址、传入接口、协议、源与目标端口的算法在 指定网关之间进行分发。

使用流量区域跨多个接口的 ECMP

如果将流量区域配置为包含一组接口，在每个区域中最多可以跨 8 个接口配置最多 8 个等价静态或动态路由。例如，您可以在区域中跨三个接口配置多个默认路由：

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

同样，动态路由协议可以自动配置等价路由。威胁防御设备使用更稳健的负载均衡机制跨接口对流量进行负载均衡。

当某条路由丢失时，设备会将流量无缝移至其他路由。

关于路由映射

在将路由重新分发到OSPF、RIP、EIGRP或BGP路由进程时会使用路由映射。在为OSPF路由进程生成默认路由时也会使用路由映射。路由映射定义了允许将来自指定路由协议的哪些路由重新分发到目标路由进程。

路由映射与广为人知的 ACL 具有许多相同功能。以下是两者共有的一些特征：

- 它们都是单独语句的有序序列，各自具有允许或拒绝结果。ACL 或路由映射的评估包括采用预先确定顺序的列表扫描，以及每条语句匹配条件的评估。一旦找到第一个语句匹配即中止列表扫描，并且会执行与语句匹配相关联的操作。
- 它们是通用机制。条件匹配和匹配解释由它们的应用方式和使用它们的功能决定。应用于不同功能的相同路由映射可能以不同方式进行解释。

以下是路由映射与 ACL 之间的一些差异：

- 路由映射比 ACL 更加灵活，可以根据 ACL 无法验证的条件对路由进行验证。例如，路由映射可以验证路由的类型是否为内部路由。
- 每个ACL按照设计约定以隐式拒绝语句结尾。如果在匹配尝试期间到达路由映射的结尾，则结果取决于路由映射的特定应用。应用于重新分发的路由映射与ACL的行为方式相同：如果路由与路由映射中的任何子句不匹配，则会拒绝路由重新分发，就如同路由映射的结尾包含拒绝语句一样。

Permit 和 Deny 子句

路由映射可以具有permit和deny子句。deny子句可拒绝来自重新分发的路由匹配。您可以使用ACL作为路由映射中的匹配标准。由于 ACL 还有 permit 和 deny 子句，因此数据包与 ACL 匹配时会应用以下规则：

- ACL permit + route map permit：重新分发路由。
- ACL permit + route map deny：重新分发路由。
- ACL deny + route map permit or deny：不匹配 route map 子句，并且对下一个 route-map 子句进行评估。

Match 和 Set 子句值

每个路由映射子句均具有两种类型的值：

- match 值用于选择应将此子句应用于的路由。
- set 值用于修改将重新分发到目标协议的信息。

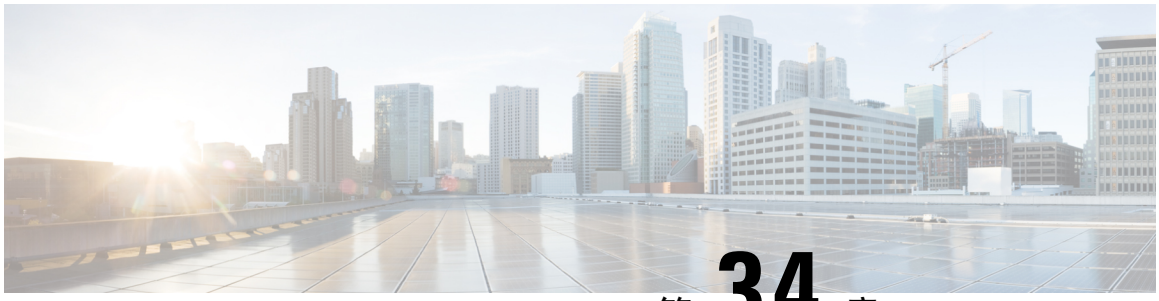
对于要重新分发的每个路由，路由器首先评估路由映射中子句的匹配条件。如果匹配条件成功，则按照permit或deny子句的指示重新分发或拒绝路由，其某些属性可能会通过set命令设置的值修改。如果匹配条件失败，则此子句不适用于路由，软件会根据路由映射中下一个子句继续评估路由。路由映射扫描将继续，直到发现匹配路由的子句或达到路由映射的结尾。

如果存在下列条件中的一个，则每个子句中的 match 值或 set 值可能会缺失或多次重复：

- 如果一个子句中存在多个匹配条目，则对于给定路由而言，所有这些条目必须都符合，该路由才与该子句匹配（也即，为多个 match 命令应用逻辑 AND 算法）。
- 如果一个 match 条目引用了一个条目中的多个对象，那么其中任何一个对象都应匹配（应用逻辑 OR 算法）。
- 如果匹配条目不存在，则所有路由都匹配子句。
- 如果一个 set 条目在 route map permit 子句中不存在，则该路由将被重新分发，而不修改其当前属性。

注释 请勿在 route map deny 子句中配置 set 条目，因为 deny 子句会禁止路由重新分发 - 没有要修改的信息。

没有 match 或 set 条目的 route map 子句需要执行操作。空 permit 子句允许重新分发剩余路由而不进行修改。空deny子句不允许重新分发其他路由（如果路由映射在经过完整扫描后，未发现明确的匹配项，此为默认操作）。



第 34 章

虚拟路由器

本章介绍了关于虚拟路由器的基本概念以及虚拟路由在 Cisco Secure Firewall Threat Defense 中的表现。

关于虚拟路由器和虚拟路由与转发 (VRF)

可以创建多个虚拟路由器来为接口组维护单独的路由表。由于每个虚拟路由器都有自己的路由表，因此您可以完全分隔流经设备的流量。

因此，您可以通过一组通用的网络设备为两个或多个不同的客户提供支持。您还可以使用虚拟路由器为自身网络的元素提供更多隔离，例如，将开发网络与一般用途的企业网络隔离。

虚拟路由器将实施虚拟路由和转发功能的“轻型”版本（或 VRF Lite），它不支持 BGP 的多协议扩展 (MBGP)。

创建虚拟路由器时，您需要为路由器分配接口。您可以将给定接口分配给一个且仅有一个虚拟路由器。然后即可定义静态路由，并为每个虚拟路由器配置路由协议（例如 OSPF 或 BGP）。还可在整个网络中配置单独的路由进程，以便所有参与设备的路由表都使用每个虚拟路由器相同的路由进程和表。使用虚拟路由器，可在同一物理网络上创建逻辑分隔的网络，以确保流经每个虚拟路由器的流量的隐私。

由于路由表独立存在，因此可以在虚拟路由器上使用相同或重叠的地址空间。例如，可以将 192.168.1.0/24 地址空间用于两个独立的虚拟路由器，分别由两个独立物理接口提供支持。

请注意，每个虚拟路由器有单独的管理和数据路由表。例如，如果将管理专用接口分配给虚拟路由器，则该接口的路由表会与分配给虚拟路由器的数据接口分离开来。

虚拟路由器的应用

您可以使用虚拟路由器来隔离共享资源上的网络，以及/或者隔离具有通用安全策略的网络。因此，虚拟路由器可以帮助您实现：

- 通过为每个客户或不同部门提供专用路由表来为客户分离流量。
- 不同部门或网络的通用安全策略管理。
- 不同部门或网络的共享互联网接入。

全局和用户定义的虚拟路由器

全局虚拟路由器

对于具有虚拟路由功能的设备，系统会默认创建一个全局虚拟路由器。系统会将网络中的所有接口分配给全局虚拟路由器。路由接口可以属于用户定义的虚拟路由器或全局虚拟路由器。在将威胁防御升级到具有虚拟路由器功能的版本时，其所有现有路由配置将成为全局虚拟路由器的一部分。

用户定义的虚拟路由器

用户定义的虚拟路由器就是您定义的虚拟路由器。您可以在一台设备上创建多个虚拟路由器。但在任何时候，一个接口都只能分配给一个用户定义的虚拟路由器。虽然用户定义的虚拟路由器支持某些设备功能，但只有少数功能仅在全局虚拟路由器上受支持。用户定义的虚拟路由器支持基于路由的站点间 VPN（静态 VTI）。

支持的功能和监控策略

您只能在全局虚拟路由器上配置以下功能：

- OSPFv3
- RIP
- EIGRP
- IS-IS
- BGPv6
- 组播路由
- 策略型路由 (PBR)

通过管理中心中的 Flex Config 支持 ISIS（请参阅预定义的 FlexConfig 对象，第 2002 页）。只为这些功能配置全局虚拟路由器接口。

DHCP 服务器自动配置会使用从接口获知的 WINS/DNS 服务器。此接口只能是全局虚拟路由器接口。

您可以为每个用户定义的虚拟路由器单独配置以下功能：

- 静态路由及其 SLA 监控器
- OSPFv2
- BGPv4
- 集成的路由与桥接 (IRB)
- SNMP

当查询或与远程系统通信时，系统会使用以下功能（传出流量）。这些功能仅使用全局虚拟路由器中的接口。这意味着，如果为该功能配置了接口，则接口必须属于全局虚拟路由器。作为一条规则，系统无论何时出于管理目的必须查找连接外部服务器的路由，它会在全局虚拟路由器中执行路由查找。

- DNS 服务器用于解析访问控制规则中使用的完全限定名称，或解析 **ping** 命令的名称。如果指定 **any** 作为 DNS 服务器的接口，则系统仅考虑全局虚拟路由器中的接口。
- 用于 VPN 的 AAA 服务器或身份领域。只能在全局虚拟路由器中的接口上配置 VPN。因此，用于 VPN 的外部 AAA 服务器（如 Active Directory）必须可通过全局虚拟路由器中的接口访问。
- 系统日志服务器。

配置策略以感知虚拟路由器

创建虚拟路由器时，该虚拟路由器的路由表会自动与全局虚拟路由器或任何其他虚拟路由器分离开来。但是，安全策略不会自动识别虚拟路由器。

例如，如果编写适用于“任何”源或目标安全区的访问控制规则，则该规则将应用于所有虚拟路由器上的所有接口。这实际上可能正是您所希望得到的结果。例如，可能所有客户都想阻止访问相同系列的令人反感的 URL 类别。

但是，如果需要仅向其中一个虚拟路由器应用策略，则需要创建仅包含来自该单一虚拟路由器的接口的安全区。然后，在安全策略的源和目标条件中使用虚拟路由器限制的安全区。

通过使用其成员身份限制为分配给单个虚拟路由器的接口的安全区，您可以在以下策略中编写虚拟路由器感知规则：

- 访问控制策略。
- 入侵和文件策略。
- SSL 解密策略。
- 身份策略和用户到 IP 地址映射。如果在虚拟路由器中使用重叠地址空间，请确保为每个虚拟路由器创建单独的领域，并在身份策略规则中正确应用。

如果在虚拟路由器中使用重叠地址空间，则应使用安全区确保应用适当的策略。例如，如果在两个单独的虚拟路由器中使用 192.168.1.0/24 地址空间，则指定 192.168.1.0/24 网络的访问控制规则将应用于两个虚拟路由器中的流量。如果这不是期望的结果，您可以通过只为其中一个虚拟路由器指定源/目标安全区来限制该规则的应用。

互联虚拟路由器

静态和动态路由泄漏

您可以配置设备来路由虚拟路由器之间的流量。路由泄漏过程可以通过设置静态路由手动完成，也可以通过 BGP 设置动态完成。

静态路由泄漏

您可以配置静态路由来路由虚拟路由器之间的流量。

例如，如果您在全局虚拟路由器中设有外部接口，则可以在每个其他虚拟路由器中设置静态默认路由，以将流量发送到该外部接口。然后，无法在给定虚拟路由器内路由的任何流量将被发送到全局路由器，以进行后续路由。

虚拟路由器之间的静态路由被称为路由泄漏，这是因为您会将流量泄漏到其他虚拟路由器。泄漏路由（例如，VR1 路由到 VR2）时，可以仅发起从 VR2 到 VR1 的连接。要使流量从 VR1 流向 VR2，必须配置反向路由。当您为另一个虚拟路由器中的接口创建静态路由时，不需要指定网关地址，而只需选择目标接口。

对于虚拟路由器间路由，系统会在源虚拟路由器中查找目标接口。然后，系统会查找目标虚拟路由器中下一跳的MAC地址。因此，目标虚拟路由器必须具有用于目标地址的所选接口的动态（获知）或静态路由。

通过配置将在不同虚拟路由器中使用源接口和目标接口的NAT规则，还允许在虚拟路由器之间路由流量。如果未选择NAT进行路由查找的选项，则每当发生目标转换时，规则就会将流量从目标接口发送到 NATed 地址。但是，目标虚拟路由器应具有一个已转换目标 IP 地址的路由，以便下一跳查找可以取得成功。

虽然NAT规则将流量从一个虚拟路由器泄漏到另一个虚拟路由器，但为了确保正确的路由，建议在这些虚拟路由器之间为转换后的流量配置静态路由泄漏。如果没有路由泄漏，有时该规则可能无法匹配您预期其匹配的流量，并且可能不会应用转换。

虚拟路由不支持级联或路由泄漏链。例如，假设 威胁防御 具有VR1、VR2和VR3虚拟路由器；VR3直接连接到网络 10.1.1.0/24。现在，假设您在 VR1 中通过 VR2 中的接口为网络 10.1.1.0/24 配置了路由泄漏，在 VR2 中通过 VR3 为 10.1.1.0/24 定义了路由泄漏。此路由泄漏链不允许流量从 VR1 跳到 VR2，然后从 VR3 退出。如果存在路由泄漏，路由查找将首先从输入虚拟路由器的路由表确定出口接口，然后查看虚拟路由器的路由表输出，以进行下一跳查找。在上述两次查找中，出口接口应匹配。在本示例中，出口接口不是同一接口，因此流量不会通过。

当目的网络不是上游（传出）VR 的直连子网时，请谨慎使用静态 VRF 间路由。例如，假设有两个 VR - VR1 和 VR2。VR1 处理通过 BGP 或任何动态路由协议从其外部对等体获取默认路由的传出流量，而 VR2 则处理配置了静态 VRF 间默认路由的传入流量，并将 VR1 作为下一跳。当 VR1 丢失来自其对等体的默认路由时，VR2将无法检测到其上游（传出）VR丢失了默认路由，并且仍会向VR1

发送流量，该流量最终将被丢弃，而不会发出通知。在这种情况下，我们建议您通过 BGP 为 VR2 配置动态路由泄漏。

使用 BGP 完成的动态路由泄漏

您可以通过使用路由目标扩展社区将路由从源虚拟路由器（比如VR1）导出到源BGP表，然后将相同的路由目标扩展社区从源 BGP 表导入到目的 BGP 表来实现虚拟路由器间路由泄漏，导入的路由目标扩展社区将由目的虚拟路由器（比如 VR2）使用。您可以使用路由映射来过滤路由。全局虚拟路由器的路由也可以泄漏到用户定义的虚拟路由器，反之亦然。BGP 虚拟路由器间路由泄漏支持 IPv4 和 IPv6 前缀。

有关配置 BGP 路由泄漏的详细信息，请参阅配置 BGP 路由导入/导出设置，第 913 页。

BGP 路由泄漏准则

- 确保递归所需的所有路由均已导入并出现在入口虚拟路由器的路由表中。
- 每个虚拟路由器都支持 ECMP。因此，请不要在不同的虚拟路由器之间配置 ECMP。从不同虚拟路由器导入的重叠前缀无法形成 ECMP。也就是说，当您尝试将具有重叠地址的路由从两个不同的虚拟路由器导入到其他虚拟路由器（全局虚拟路由器或用户定义的虚拟路由器）时，只有一条路由（根据BGP最佳路径算法，是通告的第一个路由）会导入到相应的虚拟路由表中。例如，如果连接到 VR1 的网络 10.10.0.0/24 先通过 BGP 通告到全局虚拟路由器，之后连接到 VR2 的另一个具有相同地址 10.10.0.0/24 的网络也通过 BGP 通告到全局虚拟路由器，则只有 VR1 网络路由会导入到全局虚拟路由表中。
- 用户定义的虚拟路由器不支持 OSPFv3。因此，请不要将 BGPv6 配置为将 OSPFv3 用户定义的虚拟路由器泄漏到全局虚拟路由器。但是，您可以将 BGPv6 配置为通过重新分发将 OSPFv3 全局虚拟路由器路由泄漏到用户定义的虚拟路由器。
- 建议将 VTI 接口、受保护的内部接口（如果 VTI 支持，则为环回接口）保留为同一虚拟路由器的一部分，以防止需要路由泄漏。

重叠 IP 地址

虚拟路由器会创建多个独立的路由表实例，因此可以使用相同或重叠的 IP 地址，而且不会发生冲突。威胁防御 允许同一网络成为两个或多个虚拟路由器的一部分。这涉及到要在接口或虚拟路由器级别应用的多个策略。

除了少数例外，路由功能以及大多数 NGFW 和 IPS 功能都不会受重叠 IP 地址的影响。以下部分介绍具有重叠 IP 地址限制的功能以及摆脱这些限制的建议。

重叠 IP 地址的限制

在多个虚拟路由器中使用重叠 IP 地址时，为确保正确应用策略，您必须修改某些功能的策略或规则。此类功能要求您拆分现有安全区域或根据需要使用新接口组，以便使用更具体的接口。

在使用重叠 IP 地址时，您需要修改以下功能才能正常运行：

- “网络映射”(Network Map) - 修改网络发现策略以排除一些重叠的 IP 网段，以确保没有映射的重叠 IP 地址。
- “身份策略”(Identity Policy) - 身份源来源无法区分虚拟路由器；要摆脱此限制，请在不同领域映射重叠地址空间或虚拟路由器。

对于以下功能，您需要在特定接口上应用规则，才能确保在重叠的 IP 网段上应用不同的策略：

- 访问策略
- 预过滤器策略
- QoS/速率限制
- SSL 策略

重叠 IP 地址的不支持的功能

- AC 策略中基于 ISE SGT 的规则 - 从思科身份服务引擎 (ISE) 下载的静态安全组标签 (SGT) 到 IP 地址的映射不会感知虚拟路由器。如果需要为每个虚拟路由器创建不同的 SGT 映射，请为每个虚拟路由器设置单独的 ISE 系统。如果打算将相同的 IP 地址映射到各个虚拟路由器中的相同 SGT 编号，则无需执行此操作。
- 不支持跨虚拟路由器使用重叠 DHCP 服务器池。
- 事件和分析 - 很多 管理中心 分析依赖于网络映射和身份映射，如果同一 IP 地址属于两个不同的终端主机，则无法区分。因此，当同一设备中存在重叠的 IP 网段但虚拟路由器不同时，这些分析并不准确。

在用户定义的虚拟路由器上配置 SNMP

除了在管理接口和全局虚拟路由器数据接口上支持 SNMP，Cisco Secure Firewall Threat Defense 现在还允许您在用户定义的虚拟路由器上配置 SNMP 主机。

在用户定义的虚拟路由器上配置 SNMP 主机包括以下过程：

1. 启用物理接口并配置以太网设置
2. 创建虚拟路由器
3. 添加 SNMP 主机

注释 SNMP 无法被虚拟路由器感知。因此，在用户定义的虚拟路由器上配置 SNMP 服务器时，请确保网络地址不是重叠 IP 地址。

4. 部署配置更改。在成功部署后，SNMP 轮询和陷阱将通过虚拟路由器接口发送到网络管理站。

按设备型号划分的最大虚拟路由器数量

可以创建的最大虚拟路由器数量取决于设备型号。下表列出了最大限制。您可以通过输入 **show vrf counters** 命令对系统进行复核，该命令显示该平台的用户定义最大虚拟路由器数量（不包括全局虚拟路由器）。下表中的数字包括用户和全局路由器。对于 Firepower 4100/9300，这些数字适用于原生模式。

对于支持多实例功能的平台（例如 Firepower 4100/9300），通过以下方式确定每个容器实例的最大虚拟路由器数：将最大虚拟路由器数除以设备上的核心数，然后乘以分配给该实例的核心数，并四舍五入到最接近的整数。例如，如果平台最多支持 100 个虚拟路由器，并且它有 70 个核心，则每个核心最多支持 1.43 个虚拟路由器（四舍五入为一个）。因此，分配有 6 个核心的实例将支持 8.58 个虚拟路由器（四舍五入为 8 个），分配有 10 个核心的实例将支持 14.3 个虚拟路由器（四舍五入为 14 个）。

设备型号	最大虚拟路由器数量
Firepower 1010	5
Firepower 1120	5
Firepower 1140	10
Firepower 1150	10
Firepower 2110	10
Firepower 2120	20
Firepower 2130	30
Firepower 2140	40
Secure Firewall 3110	15
Secure Firewall 3120	25
Secure Firewall 3130	50
Secure Firewall 3140	100
Firepower 4110	60
Firepower 4112	60
Firepower 4115	80
Firepower 4120	80
Firepower 4125	100
Firepower 4140	100
Firepower 4145	100

设备型号	最大虚拟路由器数量
Firepower 4150	100
Firepower 9300 设备，所有型号	100
Threat Defense Virtual，所有平台	30
ISA 3000	10

相关主题

容器实例的要求和前提条件，第 418 页

虚拟路由器的要求和必备条件

型号支持

威胁防御

支持的域

任意

用户角色

管理员

网络管理员

安全审批人

虚拟路由器的准则和限制

防火墙模式指导原则

虚拟路由器仅在路由防火墙模式下支持。

接口指导原则

- 您可以只能将一个接口分配给一个虚拟路由器。
- 可以为虚拟路由器分配任意数量的接口。
- 只有具有逻辑名称 和 VTI 的路由接口才能被分配给用户定义的虚拟路由器。
- 如果要将虚拟路由器接口更改为非路由模式，请从虚拟路由器中删除该接口，然后再更改其模式。

- 您可以从全局虚拟路由器或其他用户定义的虚拟路由器将接口分配给虚拟路由器。
- 不能将以下接口分配给用户定义的虚拟路由器：
  - 诊断接口。
  - EtherChannel 的成员。
  - 冗余接口的成员。
  - BVI 成员。
- VTI 是基于路由的 VPN。因此，在建立隧道后，必须通过路由控制使用 VTI 进行加密的流量。支持静态路由，以及使用 BGP 的动态路由。
- 属于用户定义的虚拟路由器的接口无法用于站点间或 RA VPN。
- 如果使用正在移动的接口或其虚拟路由器被删除的路由存在于源或目的虚拟路由器表中，请在移动接口或删除虚拟路由器之前删除这些路由。
- 由于为每个虚拟路由器维护了单独的路由表，因此当接口从一个虚拟路由器移至另一个虚拟路由器（无论是全局路由器还是用户定义的路由器）时，系统都会临时删除接口上配置的 IP 地址。接口上的所有现有连接都会被终止。因此，在虚拟路由器之间移动接口会对网络流量产生显著影响。因此，请不要在移动接口之前采取预防措施。

全局虚拟路由器准则

- 已命名但不属于其他虚拟路由器的接口是全局虚拟路由器的一部分。
- 您不能从全局虚拟路由器中删除路由接口。
- 您不能修改全局虚拟路由器。
- 通常，在配置接口后，如果取消注册并重新注册到同一或其他 管理中心，则接口配置会从设备导回。使用虚拟路由器支持时存在一个限制 - 只保留全局虚拟路由器接口的 IP 地址。

集群准则

- 当控制设备链路由于其接口故障而发生故障时，该设备会从全局路由表中删除其接口的所有泄漏路由，然后将非活动连接的静态路由传播到集群的其他设备。这样会导致从其他设备的路由表中删除这些泄漏的路由。这些删除发生在另一台设备成为新的控制设备之前，大约需要 500 毫秒。当另一台设备成为新的控制设备时，这些路由将通过 BGP 融合获知并添加回路由表中。因此，直到融合时间（约一分钟），泄漏的路由才可用于发生路由事件。
- 当集群中发生控制角色更改时，通过 BGP 获知的泄漏路由将通过最佳 ECMP 路径进行更新。但是，仅在 BGP 重新融合计时器过去后（即 210 秒），才会从集群路由表中删除非最佳 ECMP 路径。因此，在 BGP 重新融合计时器到期之前，旧的非最佳 ECMP 路径将继续作为路由事件的首选路由。

其他规定

- 在为虚拟路由器配置 BGP 时，您可以在同一虚拟路由器内重新分发属于不同协议的路由。例如，无法将 OSPF VR2 路由导入到 BGP VR1 中。您只能将 OSPF VR2 重新分发到 BGP VR2，然后在 BGP VR2 和 BGP VR1 之间配置路由泄漏。
- 您不能使用 IPv6 ACL 来过滤路由地图中的路由。只支持前缀列表。
- 安全智能策略 - 安全智能策略不会感知虚拟路由器。如果将 IP 地址、URL 或 DNS 名称添加到阻止列表，则会被所有虚拟路由器阻止。这一限制适用于具有安全区域的接口。
- NAT 规则 - 不要在 NAT 规则中混用接口。在虚拟路由中，如果指定的源和目的接口对象（接口组或安全区）有属于不同虚拟路由器的接口，那么 NAT 规则会将流量从一个虚拟路由器分流到另一个虚拟路由器。NAT 只会在虚拟路由器表中为入站接口执行路由查找。如有必要，请在源虚拟路由器中为目标接口定义静态路由。如果将接口保留为 **any**，则该规则适用于所有接口，而不考虑虚拟路由器成员关系。
- DHCP 中继 - 不支持为 DHCP 中继互连虚拟路由器。例如，如果在 VR1 接口上启用了 DHCP 中继客户端，而在 VR2 接口上启用了 DHCP 中继服务器，则 DHCP 请求将不会被转发到 VR2 接口之外。
- 重新创建已被删除的虚拟路由器 - 如果您重新创建一个在 10 秒内被删除的虚拟路由器，系统将弹出一条错误消息，指出正在删除该虚拟路由器。如果您要连续重新创建已删除的虚拟路由器，请为新的虚拟路由器使用不同的名称。

管理中心 Web 界面 - 路由页面修改

虚拟路由功能不支持用于 威胁防御 6.6 之前的设备和少数设备型号。对于此类不受支持的设备， 管理中心 Web 界面显示的是 管理中心 6.5 或更早版本的“路由”(Routing) 页面。要了解支持使用虚拟路由功能的设备和平台，请参阅按设备型号划分的最大虚拟路由器数量。

您可以在支持设备的路由页面中配置虚拟路由器：

1. 导航至**设备** > **设备管理**，然后编辑虚拟路由器感知设备。
2. 点击**路由 (Routing)** 以进入虚拟路由器页面。

对于使用虚拟路由功能的设备，“路由”(Routing) 页面的左窗格显示以下选项：

- **管理虚拟路由器** - 允许您创建和管理虚拟路由器。
- 虚拟路由协议列表 - 列出可为虚拟路由器配置的路由协议。
- **常规设置** - 允许您配置适用于所有虚拟路由器的 BGP 常规设置。选中**启用 BGP** 复选框可定义其他 BGP 设置。要为虚拟路由器配置其他 BGP 设置，请导航至虚拟路由协议中的 **BGP**。

管理虚拟路由器

当您点击“虚拟路由器”(Virtual Routers) 窗格上的**管理虚拟路由器 (Manage Virtual Routers)** 时，将出现“管理虚拟路由器”(Manage Virtual Routers) 页面。此页面会显示设备和关联接口上的现有虚拟路由器。在此页面中，您可以**添加虚拟路由器**（+）到设备。您还可以**编辑**（✎）和**删除**（🗑）用户定义的虚拟路由器。您无法编辑或删除全局虚拟路由器。您只能**视图**（👁）全局虚拟路由器的详细信息。

创建虚拟路由器

过程

步骤 1 依次选择 **设备** > **设备管理**，并且编辑 威胁防御 设备。

步骤 2 点击**路由**。

步骤 3 点击**管理虚拟路由器**。

步骤 4 请点击 **添加虚拟路由器** （+）。

步骤 5 在“添加虚拟路由器”框中，输入虚拟路由器的名称和说明。

注释 如果您创建一个在10秒内被删除的虚拟路由器，系统将弹出一条错误消息，指出正在删除该虚拟路由器。如果您要连续创建已删除的虚拟路由器，请为新的虚拟路由器使用不同的名称。

步骤 6 点击**确定 (OK)**。

系统将显示“路由”(Routing) 页面，其中显示新创建的虚拟路由器页面。

下一步做什么

- 配置虚拟路由器。

配置虚拟路由器

智能许可证	经典许可证	支持的设备	支持的域	访问权限
任意	不适用	威胁防御 和 Threat Defense Virtual	任意	管理员/网络管理员/安全审批人

您可以为用户定义的虚拟路由器分配接口，并为设备配置路由策略。虽然不能手动为全局虚拟路由器添加或删除接口，但可以为设备接口配置路由策略。

开始之前

- 要为用户定义的虚拟路由器配置路由策略，请添加路由器。请参阅创建虚拟路由器，第 815 页。
- 非虚拟路由设备的所有路由配置设置也可用于全局虚拟路由器。有关设置的信息，请参阅路由参考。
- 用户定义的虚拟路由器只支持有限的路由协议。

过程

步骤 1 在**设备 (Devices)** > **设备管理 (Device Management)** 页面中，编辑虚拟路由器支持的设备。导航至**路由**。有关对路由页面的修改的信息，请参阅 管理中心 Web 界面 - 路由页面修改，第 814 页 。

步骤 2 从下拉列表中，选择所需的虚拟路由器。

步骤 3 在**虚拟路由器属性 (Virtual Router Properties)** 页面中，您可以修改说明。

步骤 4 要添加接口，请在**可用接口**框下选择接口，然后点击**添加**。

请记住以下几点：

- **可用接口**框下仅列出具有逻辑名称的接口。您可以编辑接口并在**接口**中提供逻辑名称。请记住保存更改，以使设置生效。
- 仅全域虚拟路由器可用于分配，**可用接口**框仅列出未分配给任何其他用户定义的虚拟路由器的接口。你可以给虚拟路由器分配物理接口、子接口、冗余接口、网桥组、VTI 和 EtherChannels，但不能分配其成员接口。由于成员接口无法命名，因此无法在虚拟路由中使用。

  您只能将诊断接口 分配给全局虚拟路由器。

步骤 5 要保存设置，点击**保存**。

步骤 6 要为虚拟路由器配置路由策略，请点击各自的名称，打开对应的设置页面：

- **OSPF** - 用户定义的虚拟路由器仅支持 OSPFv2。OSPFv2 的所有其他设置与非虚拟路由器感知接口一样适用，只是**接口**允许您仅选择您正在配置的虚拟路由器的接口。您可以为全局虚拟路由器定义 OSPFv3 和 OSPFv2 路由策略。有关 OSPF 设置的信息，请参阅OSPF，第 863 页。
- **RIP** - 只能为全局虚拟路由器配置 RIP 路由策略。有关 RIP 设置的信息，请参阅RIP，第 917 页。
- **BGP** - 此页面显示您在**设置 (Settings)** 中配置的 BGP 常规设置：
  - 除了路由器 ID 设置外，您无法修改此页面上的任何常规设置。您可以在此页面上进行编辑来覆盖在**设置 (Settings)** 页面中定义的路由器 ID 设置。
  - 要配置其他 BGP IPv4 或 IPv6 设置，必须在**常规设置 (General Settings)** 下的 **BGP** 页面中启用 BGP 选项。
  - 全局路由器和用户定义的虚拟路由器均支持 IPv4 和 IPv6 地址系列的 BGP 配置。

  有关配置 BGP 设置的信息，请参阅BGP，第 899 页。

- **静态路由** - 使用此设置来定义为特定目标网络发送流量的位置。您还可以使用此设置来创建虚拟路由器间静态路由。您可以使用用户定义或全局虚拟路由器的接口创建连接或静态路由的泄漏。**FMC 为接口添加** 前缀，以指示它属于另一个虚拟路由器并可用于路由泄漏。为使路由泄漏成功，请不要指定下一跳网关。

  静态路由表在**已从虚拟路由器泄漏**列中显示其接口用于路由泄漏的虚拟路由器。如果不是路径泄漏，则该列显示 N/A。

  无论静态路由属于哪个虚拟路由器，都会列出 Null0 接口以及与静态路由所属的同一虚拟路由器的接口。

  有关静态路由设置的信息，请参阅静态和默认路由，第 791 页。

- **组播** - 只能为全局虚拟路由器配置组播路由策略。有关组播设置的信息，请参阅组播，第 923 页。

步骤 7 要保存设置，点击**保存**。

下一步做什么

- 修改虚拟路由器。
- 删除虚拟路由器。

修改虚拟路由器

您可以修改虚拟路由器的说明和其他路由策略。

过程

步骤 1 依次选择 **设备** > **设备管理**，并且编辑 威胁防御 设备。

步骤 2 点击**路由**。

步骤 3 点击**管理虚拟路由器**。

所有虚拟路由器以及分配的接口都显示在**虚拟路由器 (Virtual Routers)** 页面中。

步骤 4 要修改虚拟路由器，请点击所需虚拟路由器旁边的 **编辑**（）。

注释 无法修改全局虚拟路由器的常规设置。因此，不能对全局路由器进行编辑；而是提供**视图**（） 来查看设置。

步骤 5 要保存更改，请点击**保存 (Save)**。

下一步做什么

- 删除虚拟路由器。

删除虚拟路由器

开始之前

- 不能删除全局虚拟路由器。因此，删除选项不可用于全局虚拟路由器。
- 您可以一次删除多个虚拟路由器。
- 被删除的虚拟路由器的所有路由策略也被删除。
- 被删除的虚拟路由器的所有接口都移动到全局虚拟路由器。
- 如果接口的移动存在任何限制（例如重叠 IP、路由冲突等），则只有在解决冲突后才能删除路由器。

过程

步骤 1 依次选择 **设备** > **设备管理**，并且编辑 威胁防御 设备。

步骤 2 点击**路由**。

步骤 3 点击**管理虚拟路由器**。

所有虚拟路由器以及映射的接口都显示在**虚拟路由器 (Virtual Routers)** 页面中。

步骤 4 要删除虚拟路由器，请点击所需虚拟路由器旁边的 **删除**（ ）。

步骤 5 要删除多个路由器，请按住 CTRL 键，点击要删除的虚拟路由器。右键点击，然后点击**删除**。

步骤 6 要保存更改，请点击**保存**。

监控虚拟路由器

要对虚拟路由器进行监控和故障排除，请登录设备 CLI 并使用以下命令。

- **show vrf**：显示虚拟路由器及其关联接口的详细信息。
- **show route vrf** <*vrf_name*>：显示虚拟路由器的路由详细信息。
- **show run router bgp all**：显示所有虚拟路由器的 BGP 路由详细信息。
- **show run router bgp vrf** <*vrf_name*>：显示虚拟路由器的 BGP 路由详细信息。

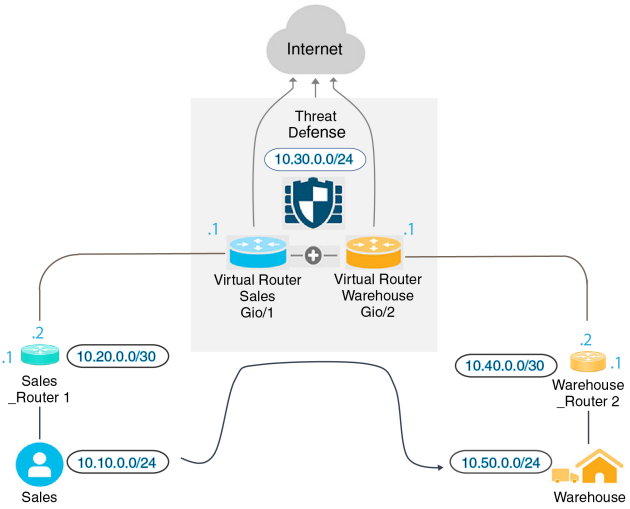
虚拟路由器的配置示例

如何通过虚拟路由器路由到远程服务器

在虚拟路由中，您可以创建多个虚拟路由器来为接口组维护单独的路由表，从而实现网络分离。在某些情况下，您可能需要访问只能通过单独的虚拟路由器访问的服务器。此示例提供了将虚拟路由器互联以访问相距多跳的主机的程序。

例如，假设一家服装公司的销售部成员想要在其工厂单位仓库部门维护的库存中进行查找。在虚拟路由环境中，您需要在目标（仓库部门）与销售部门相距多跳的虚拟路由器之间泄漏路由。路由泄漏是通过添加多跳路由泄漏来完成的，在此过程中，您需要在“销售”虚拟路由器（源）中配置一条通往“仓库”虚拟路由器（目标）中的接口的静态路由。当目标网络相距多跳时，您还需要为“仓库”虚拟路由器配置通往目标网络（即 10.50.0.0/24）的路由。

图 *121:* 互联两个虚拟路由器 - 示例



开始之前

此示例假设您已配置 Sales_Router1，从而将流量从 10.20.0.1/30 接口路由到 10.50.0.5/24。

过程

步骤 1 配置要分给“销售”虚拟路由器的设备的内部接口 (Gi0/1)：

a) 依次选择**设备** > **设备管理** > **接口**。

b) 编辑 Gi0/1 接口：

- **名称** - 本例中为“VR-Sales”。
- 选中**启用**复选框。

- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址** - 输入 10.30.0.1/24。

c) 点击**确定**。
d) 点击**保存**。

步骤 2 配置要分配给“仓库”虚拟路由器的设备的内部接口 (Gi0/2)：

a) 依次选择**设备** > **设备管理** > **接口**。
b) 编辑 Gi0/2 接口：

- **名称** - 本例中为“VR-Warehouse”。
- 选中**启用**复选框。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址** - 将其留空。该系统不允许您使用相同的 IP 地址 (10.30.0.1/24) 配置接口，因为您尚未创建用户定义的虚拟路由器。

c) 点击**确定**。
d) 点击**保存**。

步骤 3 创建“销售”和“仓库”虚拟路由器并分配其接口：

a) 依次选择 **设备** > **设备管理**，并且编辑 威胁防御 设备。
b) 依次选择**路由** > **管理虚拟路由器**。
c) 点击**添加虚拟路由器**并创建“销售”虚拟路由器。
d) 点击**添加虚拟路由器**并创建“仓库”虚拟路由器。
e) 从虚拟路由器下拉列表中选择“销售”，然后在**虚拟路由器属性**中，添加“VR-Sales”作为**选定接口**并保存。
f) 从虚拟路由器下拉列表中选择“仓库”，然后在**虚拟路由器属性**中，添加“VR-Warehouse”作为**选定接口**并保存。

步骤 4 重新访问“VR-Warehouse”接口配置：

a) 依次选择**设备** > **设备管理** > **接口**。
b) 针对“VR-Warehouse”接口点击**编辑**。将 IP 地址指定为 10.30.0.1/24。现在，由于接口分别分配给两个不同的虚拟路由器，因此系统允许您使用“VR-Sales”的同一 IP 地址进行配置。
c) 点击**确定**。
d) 点击**保存**。

步骤 5 为仓库服务器 (10.50.0.0/24) 和仓库网关 (10.40.0.2/30) 创建网络对象：

a) 依次选择**对象** > **对象管理**。
b) 依次选择**添加网络** > **添加对象**：

- **名称** - 本例中为“Warehouse-Server”。
- **网络** - 点击“网络”并输入 10.50.0.0/24。

c) 点击**保存**。

d) 依次选择**添加网络** > **添加对象**：

- **名称** - 本例中为“Warehouse-Gateway”。
- **网络** - 点击“主机”并输入 10.40.0.2。

e) 点击**保存**。

步骤 6 定义指向“VR-Warehouse”接口的“销售”虚拟路由器中的路由泄漏：

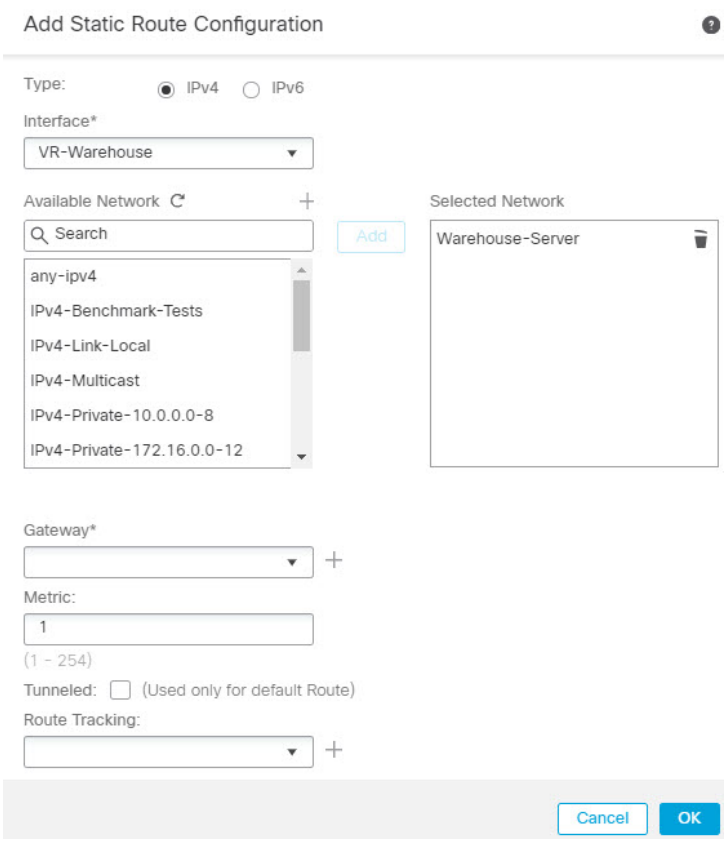
a) 依次选择 **设备** > **设备管理**，并且编辑 威胁防御 设备。

b) 选择**路由**。

c) 从下拉列表中选择“销售”虚拟路由器，然后点击**静态路由**。

d) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口** - 选择“VR-Warehouse”。
- **网络** - 选择 Warehouse-Server 对象。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。



e) 点击**确定**。

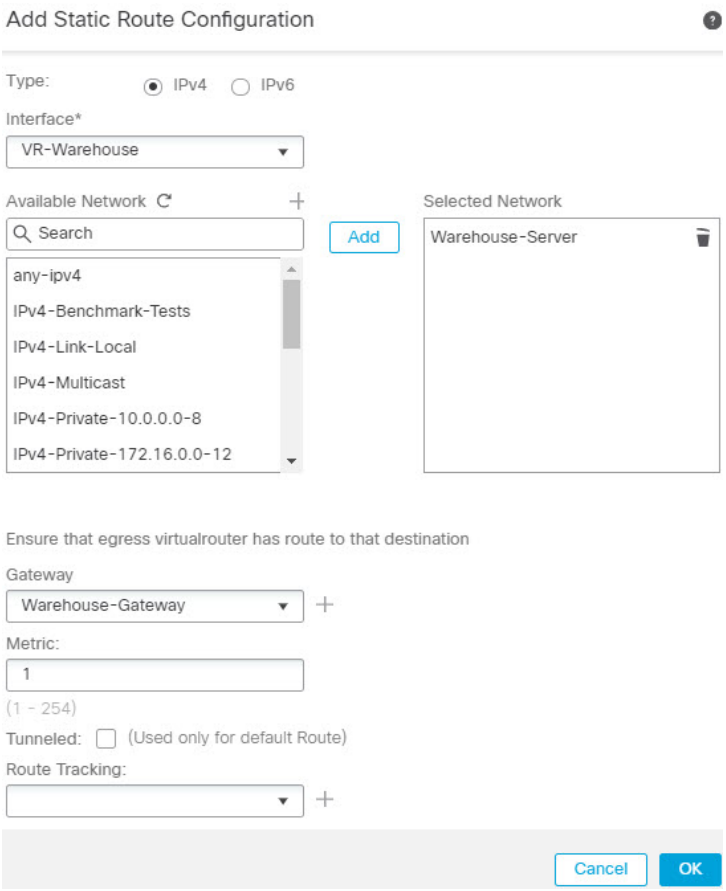
f) 点击**保存**。

步骤 7 在“仓库”虚拟路由器中，定义指向仓库路由器 2 网关的路由：

a) 从下拉列表中选择“仓库”虚拟路由器，然后点击**静态路由**。

b) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口** - 选择“VR-Warehouse”。
- **网络** - 选择 Warehouse-Server 对象。
- **网关**-选择 Warehouse-Gateway 对象。



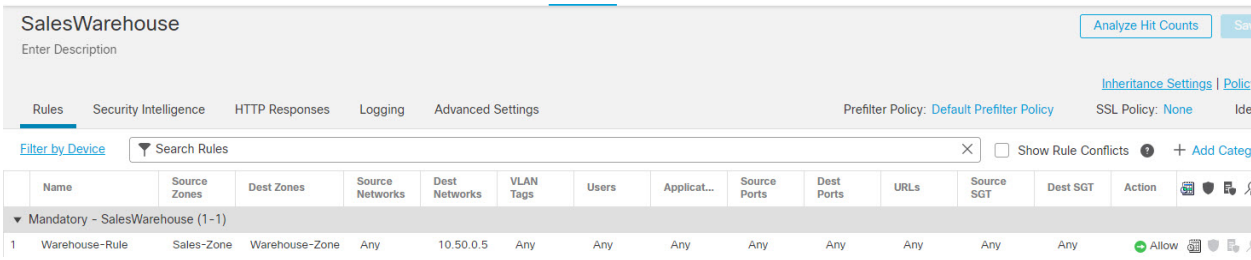
c) 点击**确定**。

d) 点击**保存**。

步骤 8 配置允许访问仓库服务器的访问控制规则。要创建访问控制规则，您需要创建安全区域。使用**对象** > **对象管理** > **接口**。依次选择**添加** > **安全区域**并为“VR-Sales”和“VR-Warehouse”创建安全区域；对于Warehouse-Server 网络对象，创建 Warehouse-Server 接口组（依次选择**添加** > **接口组**）。

步骤 9 依次选择**策略** > **访问控制**并配置访问控制规则，以允许流量从“销售”虚拟路由器中的源接口到流向目的 Warehouse-Server 网络对象的“仓库”虚拟路由器中的目的接口。

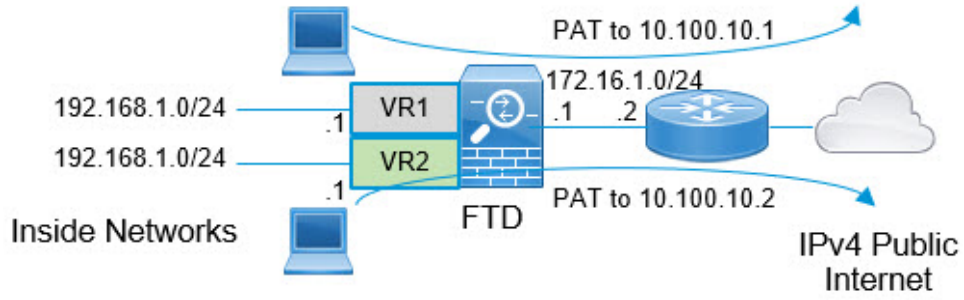
例如，如果“销售”虚拟路由器中的接口位于“销售区域”安全区域中，而“仓库”虚拟路由器中的接口位于“仓库区域”安全区域中，则访问控制规则将如下所述：



如何提供包含重叠地址空间的互联网访问权限

使用虚拟路由器时，您可以为驻留在单独路由器中的多个接口设置相同的网络地址。但是，由于在这些单独的虚拟路由器中路由的 IP 地址相同，因此请使用单独的 NAT/PAT 池为每个接口应用 NAT/PAT 规则，以确保返回流量到达正确的目的地。此示例提供了为管理重叠地址空间而配置虚拟路由器和 NAT/PAT 规则的程序。

例如，FTD 上的接口 vr1-inside 和 vr2-inside 被定义为使用 IP 地址 192.168.1.1/24，从而将终端托管在其在 192.168.1.0/24 网络中的分段上。要允许通过两个使用相同地址空间的虚拟路由器访问互联网，您需要将 NAT 规则分别应用于每个虚拟路由器中的接口，最好使用单独的 NAT 或 PAT 池。可以使用 PAT 将 VR1 中的源地址转换为 10.100.10.1，并将 VR2 中的源地址转换为 10.100.10.2。下图显示了此设置，其中面向互联网的外部接口是全局路由器的一部分。您必须使用明确选择的源接口（vr1-inside 和 vr2-inside）来定义 NAT/PAT 规则 - 使用“任何”作为源接口将使系统无法识别正确源，这是因为两个不同的接口上可能存在相同的 IP 地址。



注释 即使您拥有不使用重叠地址空间的虚拟路由器中的一些接口，也要用源接口定义NAT规则，以便简化故障排除过程，并确保更加清楚地区分来自与互联网绑定的各虚拟路由器之间的流量。

过程

步骤 1 为 VR1 配置设备的内部接口：

a) 依次选择**设备** > **设备管理** > **接口**。

b) 编辑您要分配给 VR1 的接口：

- **名称 (Name)** - 在此示例中为 vr1-inside。
- 选中**启用**复选框。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址 (IP Address)** - 输入 192.168.1.1/24。

c) 点击**确定**。
d) 点击**保存**。

步骤 2 为 VR2 配置设备的内部接口：

a) 依次选择**设备** > **设备管理** > **接口**。
b) 编辑您要分配给 VR2 的接口：

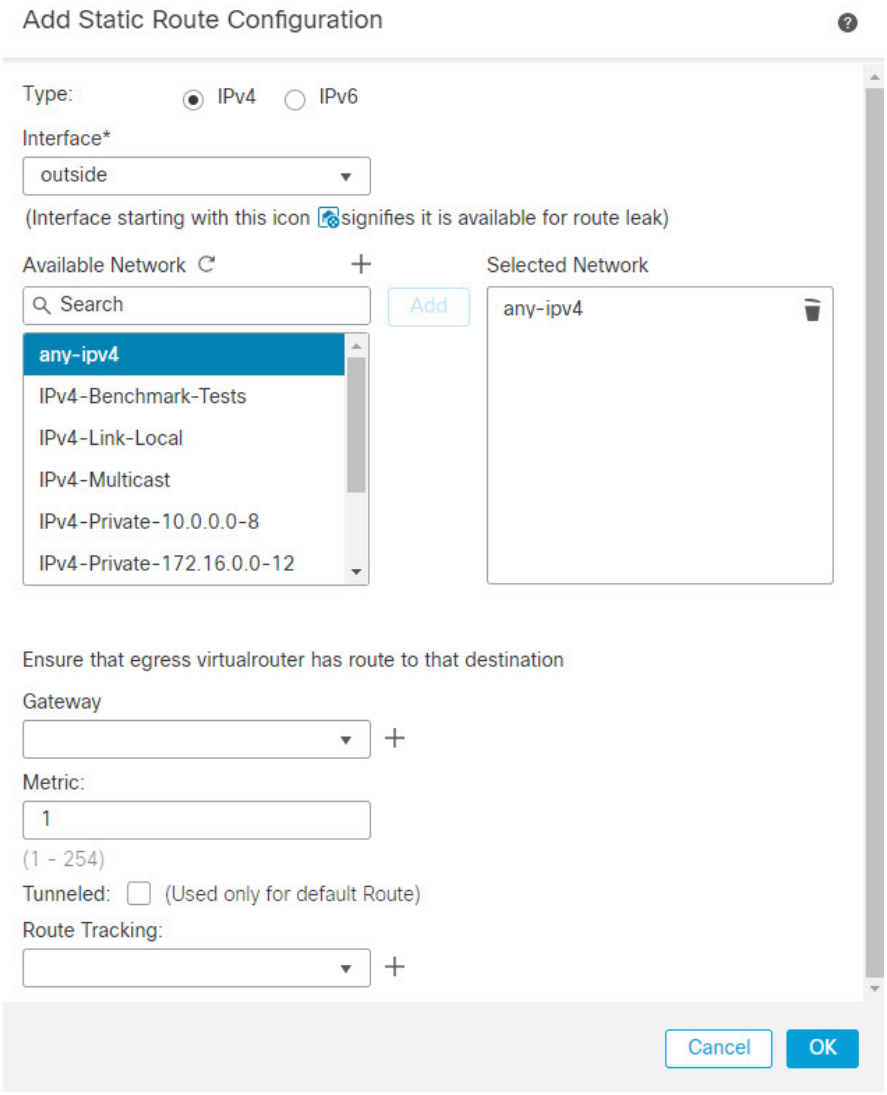
- **名称 (Name)** - 在此示例中为 vr2-inside。
- 选中**启用**复选框。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址** - 将其留空。该系统不允许您使用相同的 IP 地址配置接口，因为您尚未创建用户定义的虚拟路由器。

c) 点击**确定**。
d) 点击**保存**。

步骤 3 配置 VR1 和到外部接口的静态默认路由泄漏：

a) 依次选择**设备** > **设备管理**，然后编辑 FTD 设备。
b) 依次选择**路由** > **管理虚拟路由器**。点击**添加虚拟路由器 (Add Virtual Router)**并创建 VR1。
c) 对于 VR1，在**虚拟路由器属性 (Virtual Router Properties)** 中分配 vr1-inside 并保存。
d) 点击**静态路由 (Static Route)**。
e) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的外部接口。
- **网络 (Network)** - 选择 any-ipv4 对象。这个网络是无法在 VR1 内路由的任何流量的默认路由。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿提供网关。



f) 点击**确定**。

g) 点击**保存**。

步骤 4 配置 VR2 和到外部接口的静态默认路由泄漏：

a) 依次选择**设备** > **设备管理**，然后编辑 FTD 设备。

b) 依次选择**路由** > **管理虚拟路由器**。点击**添加虚拟路由器 (Add Virtual Router)**并创建 VR2。

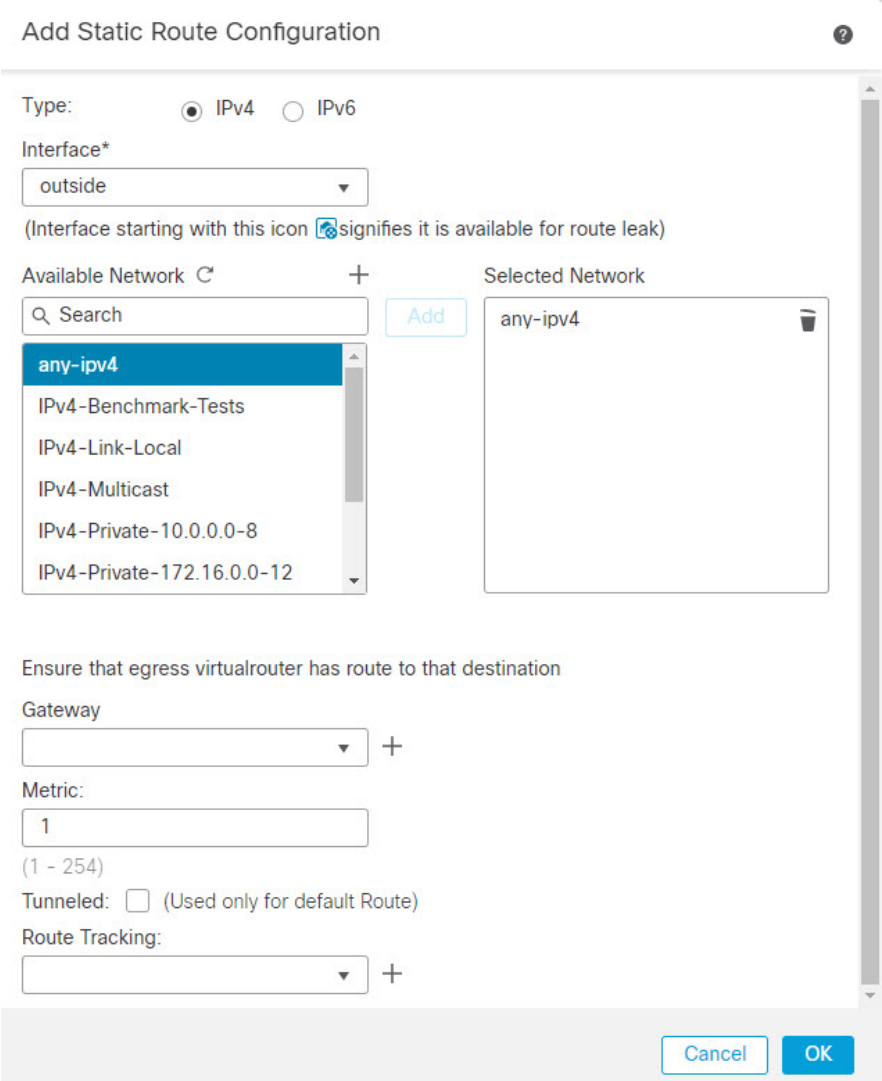
c) 对于 VR2，在**虚拟路由器属性 (Virtual Router Properties)** 中分配 vr2-inside 并保存。

d) 点击**静态路由 (Static Route)**。

e) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的外部接口。
- **网络 (Network)** - 选择 any-ipv4 对象。这个网络是无法在 VR2 内路由的任何流量的默认路由。

- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。



f) 点击**确定**。

g) 点击**保存**。

步骤 5 在全局路由器的外部接口上配置 IPv4 静态默认路由，即 172.16.1.2：

a) 依次选择**设备** > **设备管理**，然后编辑 FTD 设备。

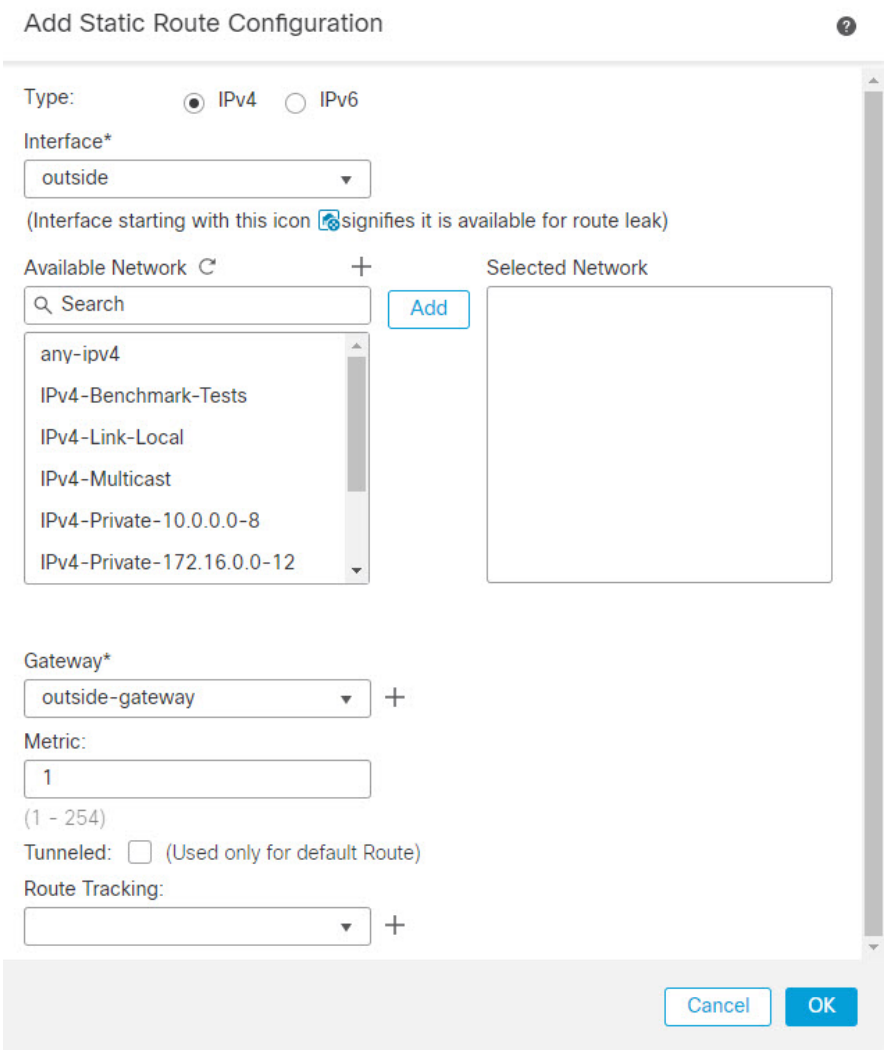
b) 选择**路由 (Routing)** 并编辑全局路由器属性。

c) 点击**静态路由 (Static Route)**。

d) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的外部接口。
- **网络 (Network)** - 选择 any-ipv4 对象。这将是用于任何 IPv4 流量的默认路由。

- **网关 (Gateway)** - 如果已创建，请从下拉列表中选择主机名。如果尚未创建对象，请点击**添加 (Add)**，然后为外部接口上网络链路另一端的网关的 IP 地址（在本例中为 172.16.1.2）定义主机对象。创建对象后，在“网关”(Gateway) 字段中选择该对象。



e) 点击**确定**。

f) 点击**保存**。

步骤 6 重新访问 vr2-inside 接口配置：

a) 依次选择**设备** > **设备管理** > **接口**。

b) 点击 vr2-inside 接口的**编辑 (Edit)**。将 IP 地址指定为 192.168.1.1/24。现在，由于接口分别分配给两个不同的虚拟路由器，因此系统允许您使用 vr1-inside 的相同 IP 地址进行配置。

c) 点击**确定**。

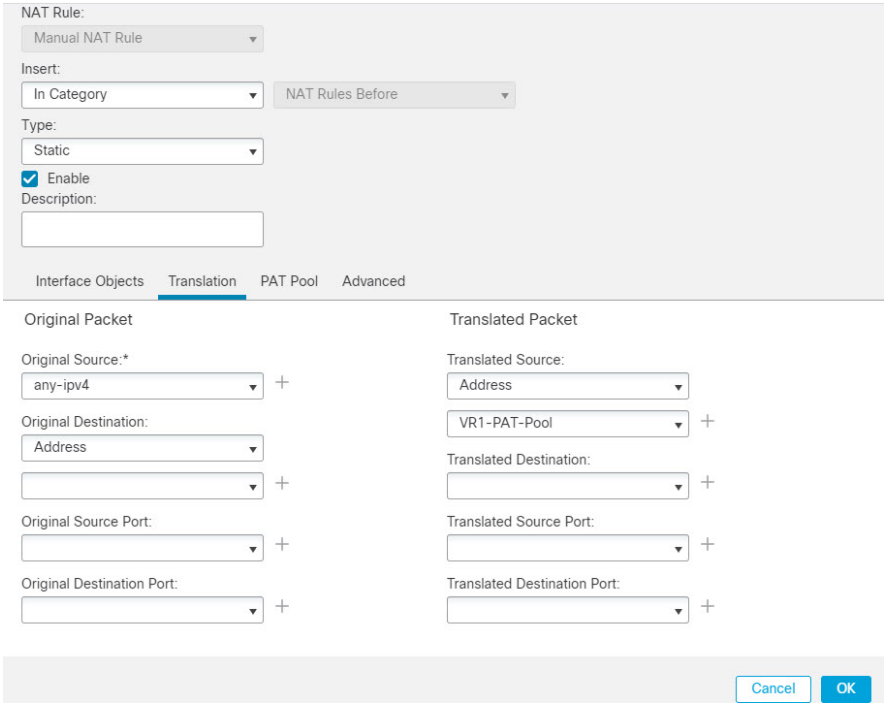
d) 点击**保存**。

步骤 7 创建 NAT 规则，以将 VR1 的 PAT 内-外流量传输到 10.100.10.1。

a) 选择**设备** > **NAT**。

b) 点击**新策略 (New Policy)** > **威胁防御 NAT (Threat Defense NAT)**。
c) 输入 InsideOutsideNATRule 作为 NAT 策略名称，然后选择 FTD 设备。点击**保存 (Save)**。
d) 在 InsideOutsideNATRule 页面中，点击**添加规则 (Add Rule)** 并定义以下内容：

- **NAT 规则 (NAT Rule)** - 选择“手动 NAT 规则”(Manual NAT Rule)。
- **类型 (Type)** - 选择“动态”(Dynamic)。
- **插入 (Insert)** - 如果存在任何动态 NAT 规则，则选择“上方”(Above)。
- 点击 **Enabled**。
- 在**接口对象 (Interface Objects)**中，选择 vr1-interface 对象，然后点击**添加到源 (Add to Source)**（如果对象不可用，请在**对象 (Object)** > **对象管理 (Object Management)** > **接口 (Interface)** 中创建一个对象），然后选择外部作为**添加到目标 (Add to Destination)**。
- 在**转换 (Translation)**中，为**原始源 (Original Source)** 选择 any-ipv4。对于**转换的源 (Translated Source)**，点击**添加 (Add)** 并使用 10.100.10.1 来定义主机对象 VR1-PAT-Pool。选择 VR1-PAT-Pool，如下图所示：



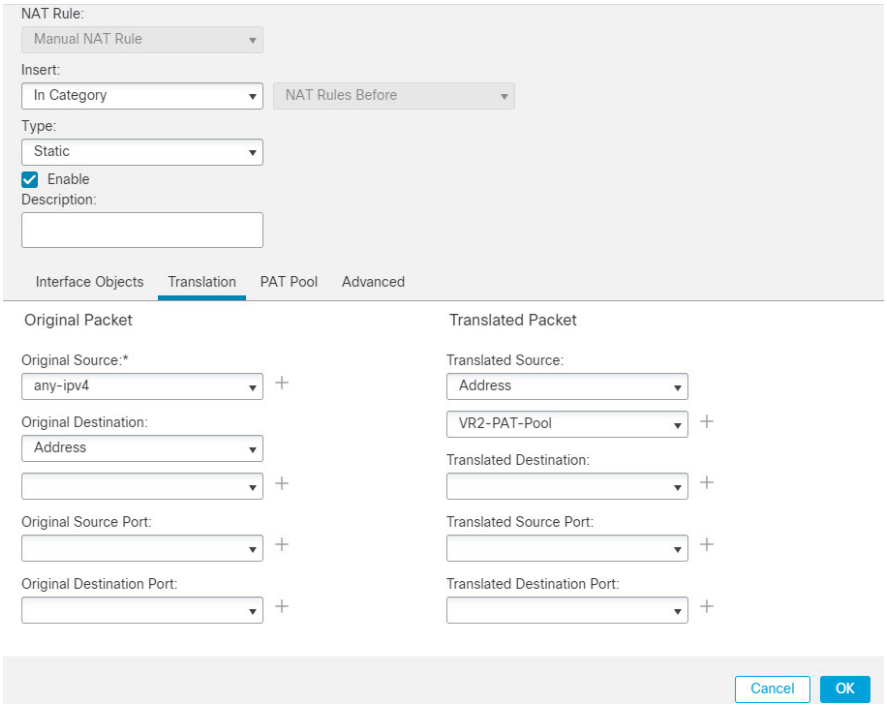
e) 点击**确定**。
f) 点击**保存**。

步骤 8 添加 NAT 规则，以将 VR2 的 PAT 内-外流量传输到 10.100.10.2。

a) 选择**设备** > **NAT**。
b) 编辑 InsideOutsideNATRule 以定义 VR2 NAT 规则：

- **NAT 规则 (NAT Rule)** - 选择“手动 NAT 规则”(Manual NAT Rule)。

- **类型 (Type)** - 选择“动态”(Dynamic)。
- **插入 (Insert)** - 如果存在任何动态 NAT 规则，则选择“上方”(Above)。
- 点击 **Enabled**。
- 在**接口对象 (Interface Objects)**中，选择 vr2-interface 对象，然后点击**添加到源 (Add to Source)**（如果对象不可用，请在**对象 (Object)** > **对象管理 (Object Management)** > **接口 (Interface)** 中创建一个对象），然后选择外部作为**添加到目标 (Add to Destination)**。
- 在**转换 (Translation)**中，为**原始源 (Original Source)** 选择 any-ipv4。对于**转换的源 (Translated Source)**，点击**添加 (Add)** 并使用 10.100.10.2 来定义主机对象 VR2-PAT-Pool。选择 VR2-PAT-Pool，如下图所示：



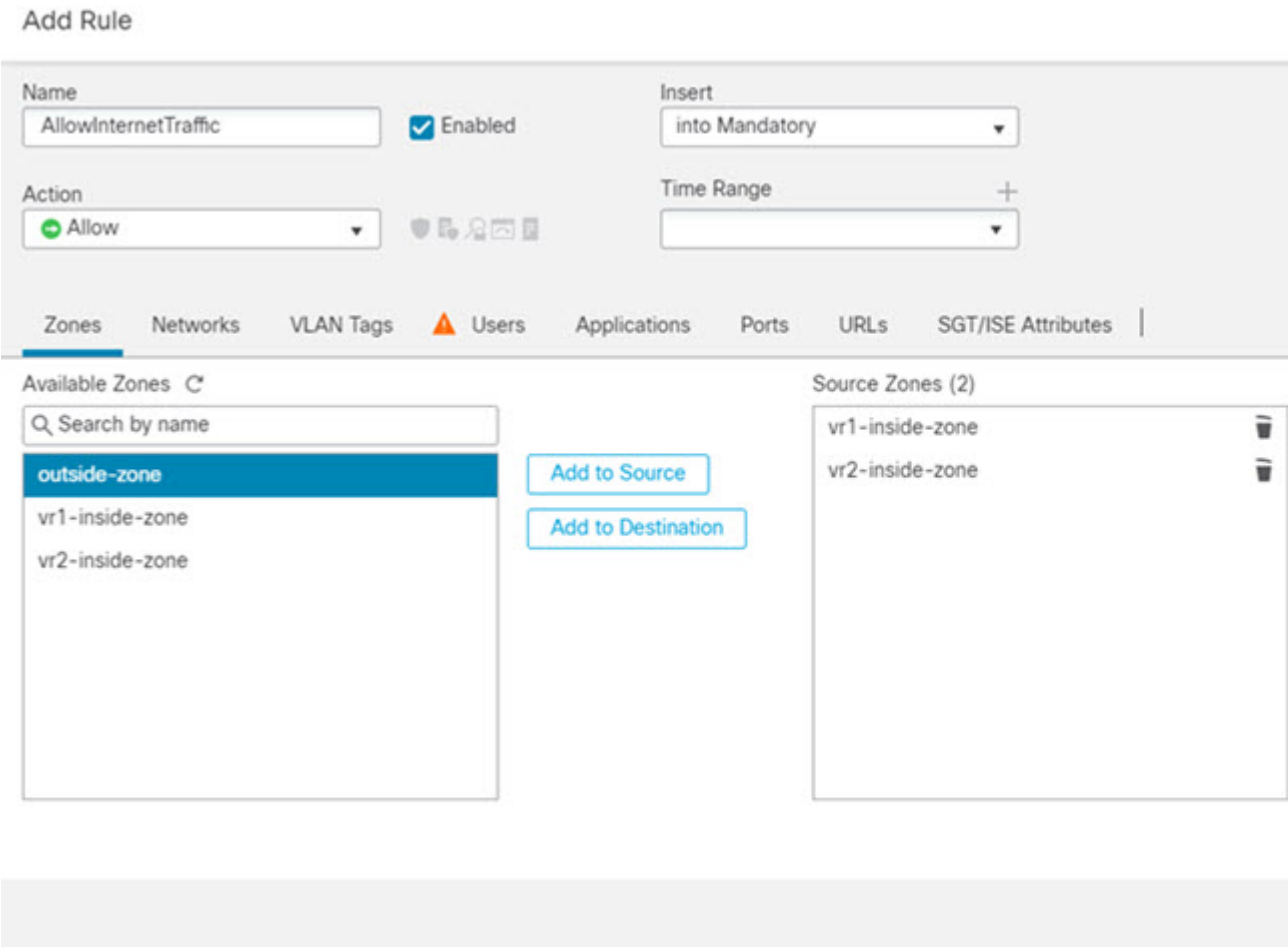
c) 点击**确定**。

d) 点击**保存**。

步骤 9 要配置允许流量从 vr1-inside 和 vr2-inside 接口流向外部接口的访问控制策略，您需要创建安全区域。使用**对象** > **对象管理** > **接口**。选择**添加 (Add)** > **安全区域 (Security Zone)** 并为 vr1-inside、vr2-inside 和外部接口创建安全区域。

步骤 10 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后配置访问控制规则以允许将 vr1-inside-zone 和 vr2- inside-zone 中的流量传输到 outside-zone。

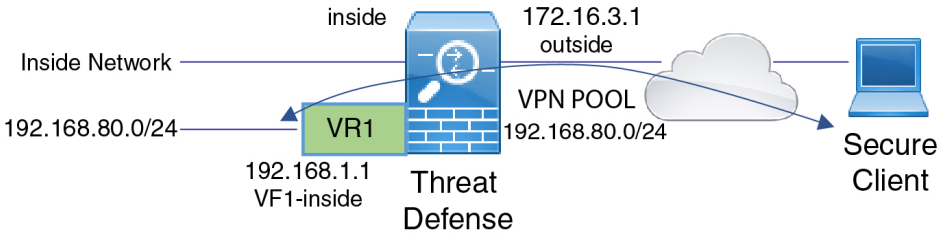
假设您创建了以接口命名的区域，则允许所有流量流向互联网的基本规则将如下所示：您可以将其他参数应用于此访问控制策略：



如何允许对虚拟路由中的内部网络进行 RA VPN 访问

在启用虚拟路由的设备上，只有全局虚拟路由器接口上支持 RA VPN。此示例提供允许 AnyConnect 客户端 用户连接到用户定义的虚拟路由器网络的程序。

在下面的示例中，RA VPN（AnyConnect 客户端）用户连接到地址为 172.16.3.1 的 威胁防御 外部接口，并在 192.168.80.0/24 池中获得 IP 地址。该用户只能访问全局虚拟路由器的内部网络。要允许流量通过用户定义的虚拟路由器 VR1 的网络（即 192.168.1.0/24），请通过在全局和 VR1 上配置静态路由来泄漏路由。



开始之前

此示例假设您已配置 RA VPN，定义虚拟路由器，配置接口并将其分配给相应的虚拟路由器。

过程

步骤 1 配置从全局虚拟路由器到用户自定义 VR1 的路由泄漏。

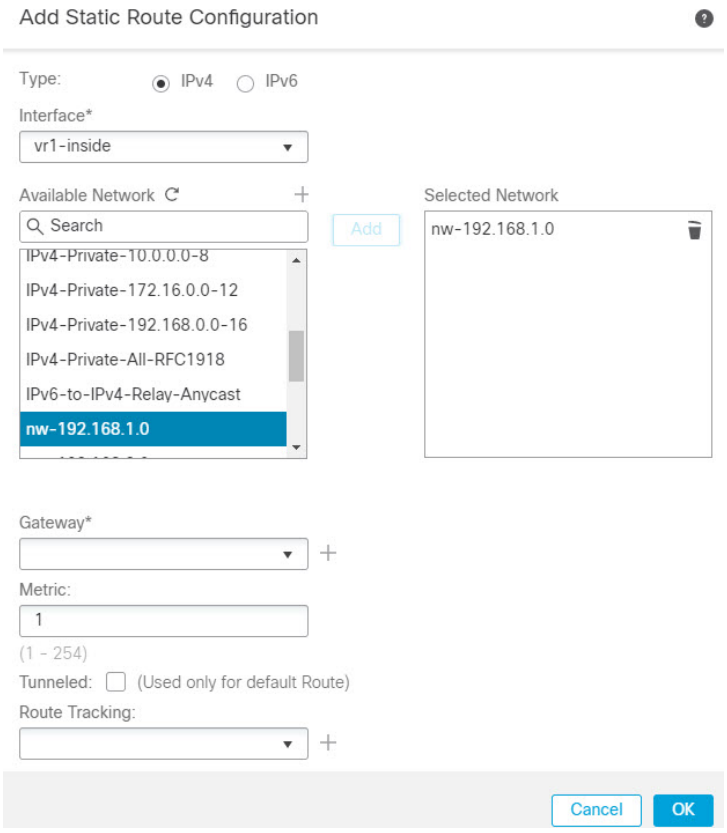
a) 依次选择 **设备** > **设备管理**，并且编辑 威胁防御 设备。

b) 点击**路由**。默认情况下，系统将显示“全局路由属性”(Global routing properties) 页面。

c) 点击**静态路由 (Static Route)**。

d) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择 VR1 内部接口。
- **网络 (Network)** - 选择 VR1 虚拟路由器网络对象。您可以使用**添加对象 (Add Object)** 选项创建一个。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。



此路由泄露允许在 VPN 池中分配 IP 地址的 AnyConnect 客户端 访问 VR1 虚拟路由器中的 192.168.1.0/24 网络。

e) 点击**确定**。

步骤 2 配置从 VR1 到全局虚拟路由器的路由泄漏：

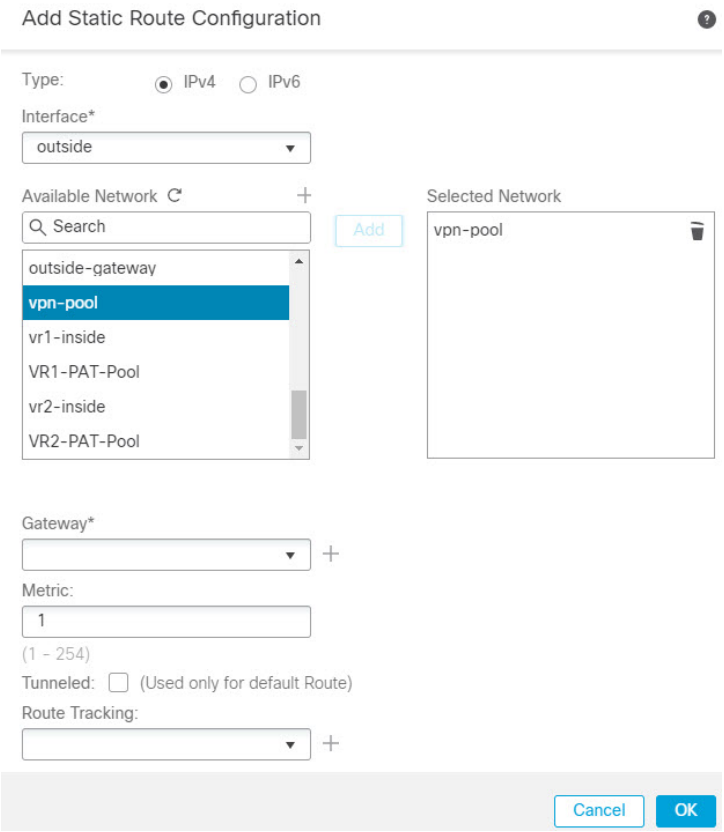
a) 依次选择 **设备** > **设备管理**，并且编辑 威胁防御 设备。

b) 点击**路由 (Routing)**，然后从下拉列表中选择 VR1。

c) 点击**静态路由 (Static Route)**。

d) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的外部接口。
- **网络 (Network)** - 选择全局虚拟路由器网络对象。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。



配置的静态路由允许 192.168.1.0/24 网络 (VR1) 上的终端向在 VPN 池中分配 IP 地址的 AnyConnect 客户端 发起连接。

e) 点击**确定**。

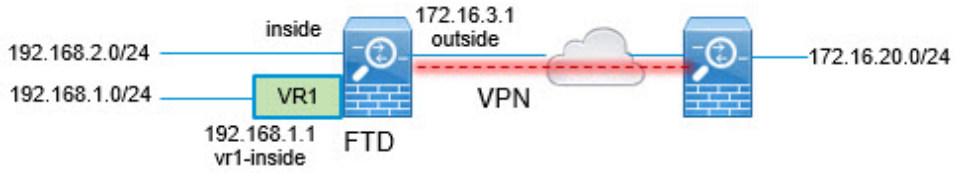
下一步做什么

如果 RA VPN 地址池与用户定义的虚拟路由器中的 IP 地址重叠，则还必须对 IP 地址使用静态 NAT 规则，以启用正确的路由。或者，您可以更改 RA VPN 地址池，以免出现重叠。

如何通过站点间 VPN 保护来自多个虚拟路由器的网络流量

在启用虚拟路由的设备上，只有全局虚拟路由器接口上支持站点间 VPN。您不能在属于用户定义的虚拟路由器的接口上配置它。此示例提供的程序让您能够通过站点间VPN保护来自或到达用户定义的虚拟路由器内的网络的连接。您还需要更新站点间VPN连接，以包括这些用户定义的虚拟路由网络。

我们假设这样一个场景：在分支机构网络和公司总部网络之间配置站点间 VPN；分支机构中的FTD具有虚拟路由器。在这种情况下，站点间 VPN 在 172.16.3.1 的分支机构外部接口上定义。此 VPN 包括内部网络 192.168.2.0/24，而无需进行额外配置，因为内部接口也是全局虚拟路由器的一部分。但是，要为 192.168.1.0/24 网络（其为 VR1 虚拟路由器的一部分）提供站点间 VPN 服务，则必须通过在全局和 VR1 上配置静态路由来泄露路由，并将 VR1 网络加入站点间的 VPN 配置中。



开始之前

此示例假设您已在本地网络 192.168.2.0/24 与外部网络 172.16.20.0/24 之间配置站点间 VPN，定义虚拟路由器，配置接口并将其分配给相应的虚拟路由器。

过程

步骤 1 配置从全局虚拟路由器到用户自定义 VR1 的路由泄漏：

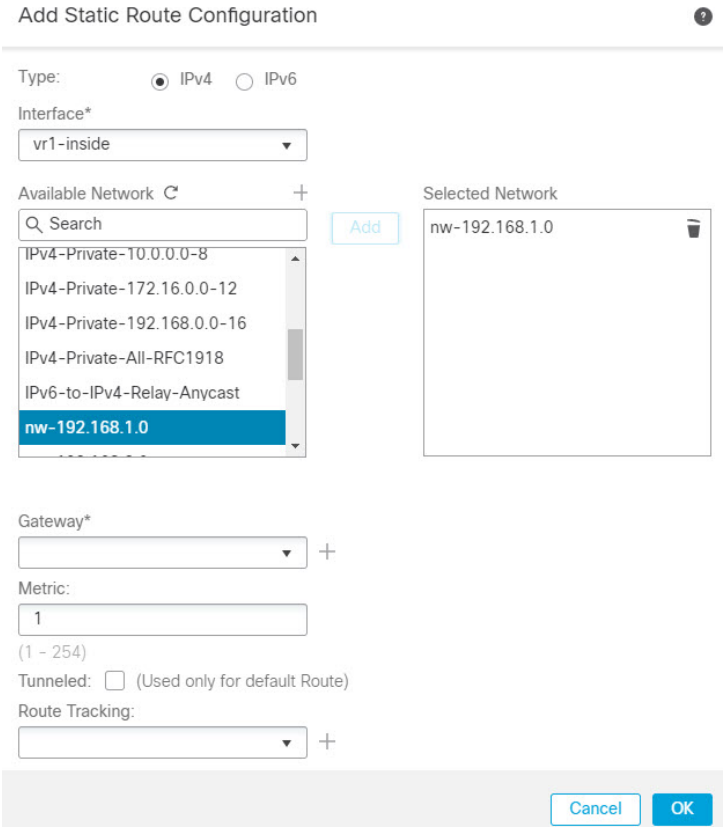
a) 依次选择**设备** > **设备管理**，然后编辑 FTD 设备。

b) 点击**路由**。默认情况下，系统将显示“全局路由属性”(Global routing properties) 页面。

c) 点击**静态路由 (Static Route)**。

d) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择 VR1 内部接口。
- **网络 (Network)** - 选择 VR1 虚拟路由器网络对象。您可以使用**添加对象 (Add Object)** 选项创建一个。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。



此路由泄漏允许受站点间 VPN 的外部（远程）终端保护的终端访问 VR1 虚拟路由器中的 192.168.1.0/24 网络。

e) 点击**确定**。

步骤 2 配置从 VR1 到全局虚拟路由器的路由泄漏：

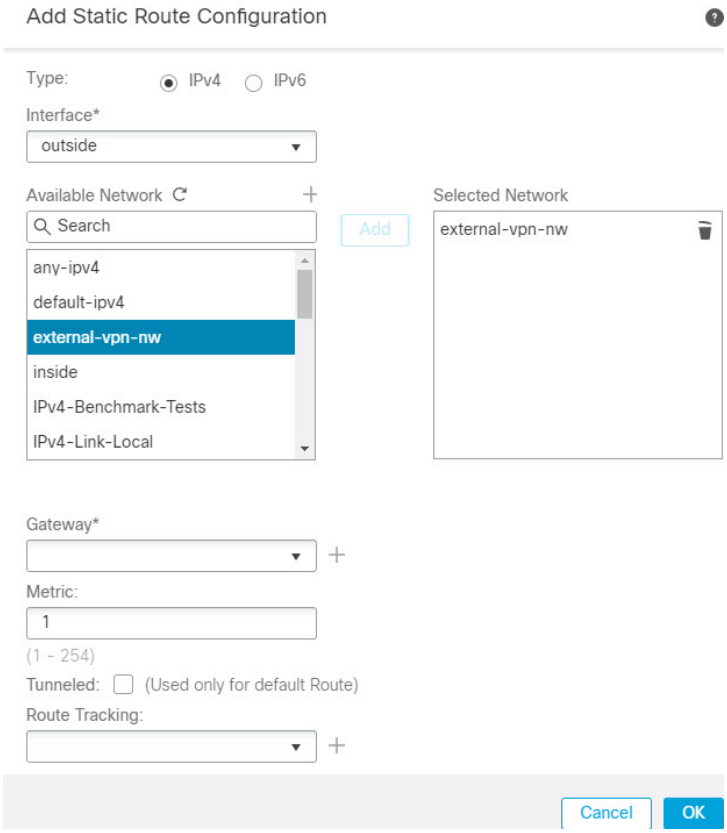
a) 依次选择**设备** > **设备管理**，然后编辑 FTD 设备。

b) 点击**路由 (Routing)**，然后从下拉列表中选择 VR1。

c) 点击**静态路由 (Static Route)**。

d) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的外部接口。
- **网络 (Network)** - 选择全局虚拟路由器网络对象。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。



此静态路由允许 192.168.1.0/24 网络 (VR1) 上的终端发起流经站点间 VPN 隧道的连接。在本示例中，远程终端正在保护 172.16.20.0/24 网络。

e) 点击**确定**。

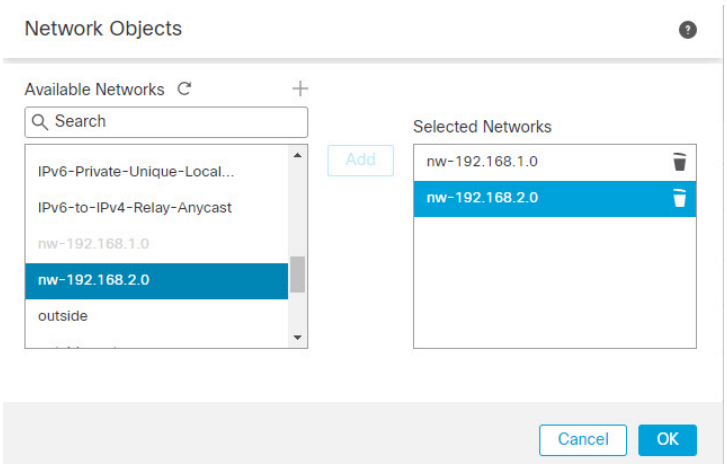
步骤 3 将 192.168.1.0/24 网络添加到站点间 VPN 连接配置文件中：

a) 选择**设备 (Devices)** > **VPN** > **站点间 (Site To Site)**，然后编辑 VPN 拓扑。

b) 在**终端 (Endpoints)** 中，编辑节点 A 终端。

c) 在**编辑终端 (Edit Endpoint)** 的**受保护网络 (Protected Networks)** 字段中，点击**添加新网络对象 (Add New Network Object)**。

d) 添加网络为 192.168.1.0 的 VR1 网络对象：

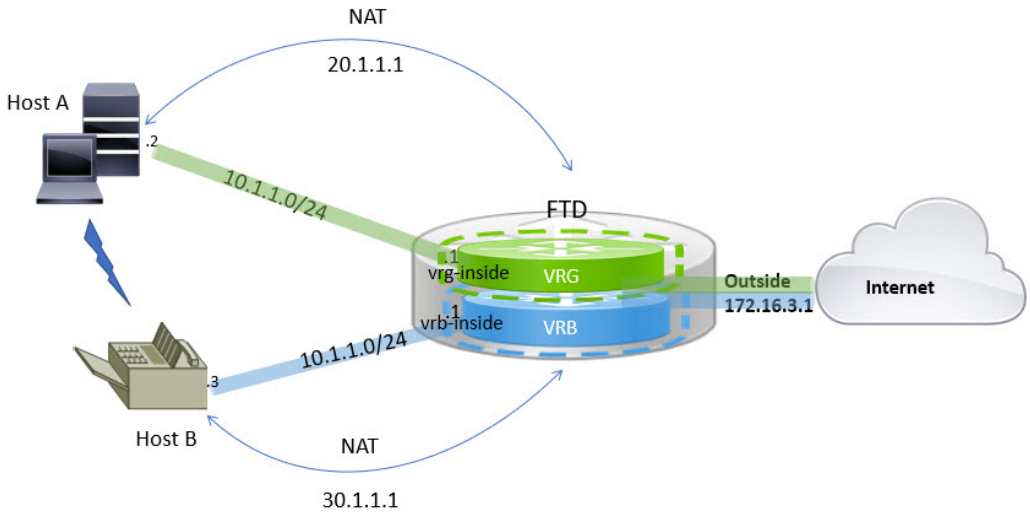


e) 点击**确定 (Ok)** 并保存配置。

如何在虚拟路由中的两个重叠网络主机之间路由流量

您可以在具有相同网络地址的虚拟路由器上配置主机。如果主机想要通信，您可以配置两次 NAT。本示例提供了配置 NAT 规则以管理重叠网络主机的程序。

在下面的示例中，两台主机主机 A 和主机 B 属于不同的虚拟路由器：VRG（接口 vrg-inside）和 VRB（接口 vrb-inside），分别具有相同的子网 10.1.1.0/24。要让两台主机通信，请创建一个 NAT 策略，其中 VRG 主机接口对象将使用映射 NAT 地址 - 20.1.1.1，而 VRB 主机接口对象将使用映射 NAT 地址 - 30.1.1.1。因此，主机 A 会使用 30.1.1.1 与主机 B 通信；主机 B 会使用 20.1.1.1 访问主机 A。



开始之前

此示例假定您已：

- vrg-inside 和 vrb-inside 接口分别与虚拟路由器关联：VRG 和 VRB 以及配置了相同子网地址的 vrg-inside 和 vrb-inside 接口（例如 10.1.1.0/24）。
- 分别使用 vrg-inside 和 vrb-inside 接口创建的接口区域 VRG-Inf、VRB-Inf。
- VRG 中的主机 A，默认网关为 vrg-inside；主机 B 位于 VRB 中，vrb-inside 作为默认网关。

过程

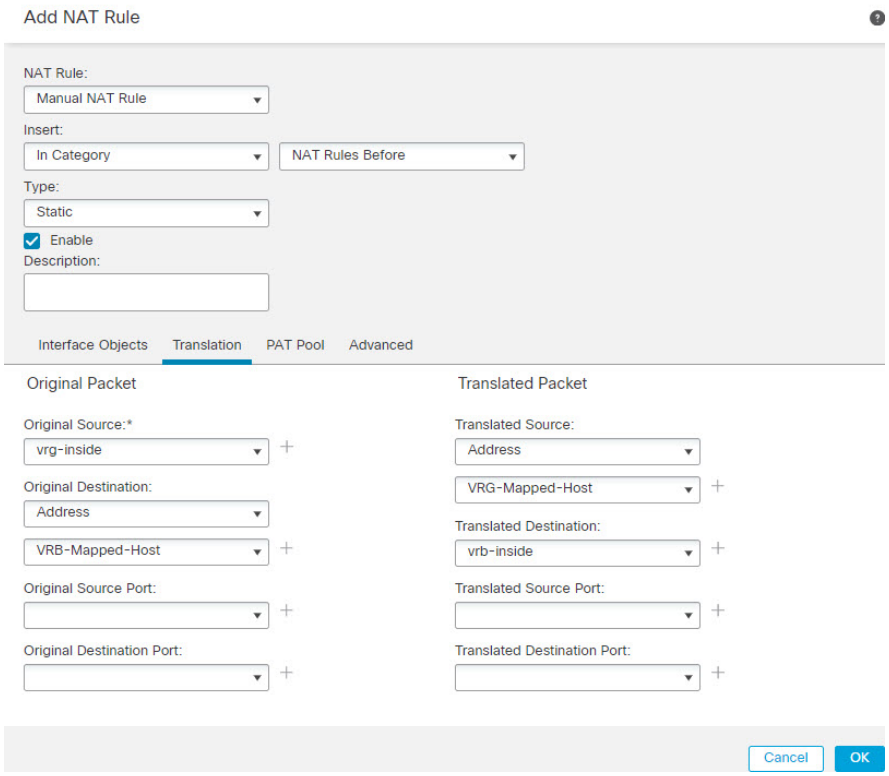
步骤 1 创建 NAT 规则以处理从主机 A 到主机 B 的流量。选择**设备 (Devices)** > **NAT**。

步骤 2 点击**新策略 (New Policy)** > **威胁防御 NAT (Threat Defense NAT)**。

步骤 3 输入 NAT 策略名称，然后选择 FTD 设备。点击**保存 (Save)**。

步骤 4 在 NAT 页面中，点击**添加规则 (Add Rule)** 并定义以下内容：

- **NAT 规则 (NAT Rule)** - 选择“手动 NAT 规则”(Manual NAT Rule)。
- **类型 (Type)** - 选择“静态”(Static)。
- **插入 (Insert)** - 如果存在任何 NAT 规则，则选择“上方”(Above)。
- 点击 **Enabled**。
- 在**接口对象 (Interface Objects)**中，选择 VRG-Inf 对象，然后点击**添加到源 (Add to Source)**（如果对象不可用，请在**对象 (Object)** > **对象管理 (Object Management)** > **接口 (Interface)** 中创建一个对象），然后选择 VRG-Inf 对象并点击**添加到目标 (Add to Destination)**。
- 在**转换 (Translation)** 中选择以下选项：
  - **原始源 (Original Source)**，选择 vrg-inside。
  - **原始目标 (Original Destination)**，点击**添加 (Add)** 并使用 30.1.1.1 定义对象 VRB-Mapped-Host。选择 VRB 映射主机。
  - **转换后的源 (Translated Source)**，，点击**添加 (Add)** 并使用 20.1.1.1 定义对象 VRG-Mapped-Host。选择 VRG 映射主机。
  - **转换后的目标 (Translated Destination)**，选择 vrb-inside，如下图所示：



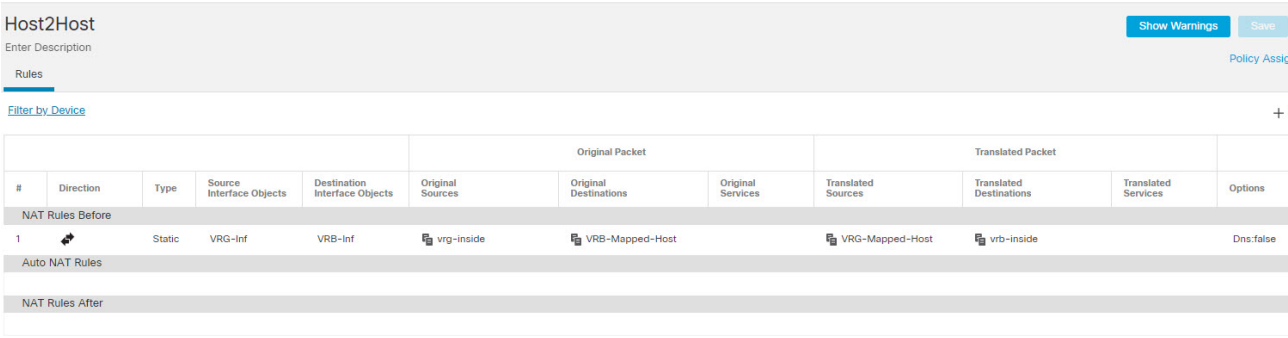
在 FTD 设备上运行 **show nat detail** 命令时，您将看到类似于以下内容的输出：

```
firepower(config-service-object-group)# show nat detail
Manual NAT Policies (Section 1)
1 (2001) to (3001) source static vrg-inside VRG-MAPPED-HOST destination static VRB-MAPPED-HOST
 vrb-inside
translate_hits = 0, untranslate_hits = 0
Source - Origin: 10.1.1.1/24, Translated: 20.1.1.1/24
Destination - Origin: 30.1.1.1/24, Translated: 10.1.1.1/24
```

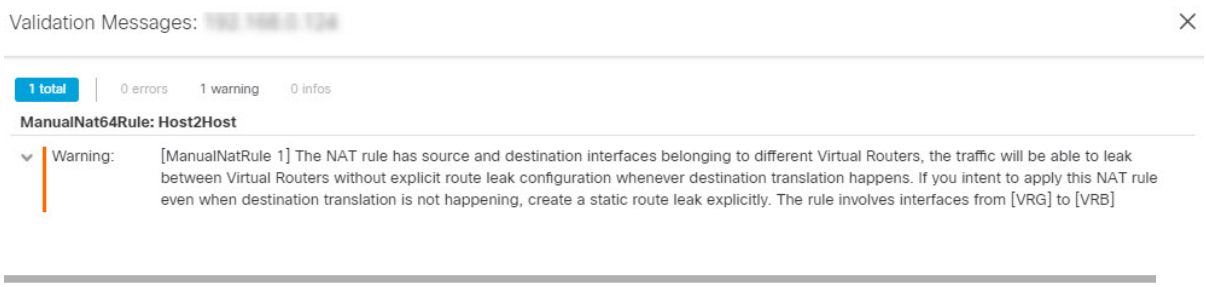
步骤 5 点击**确定**。

步骤 6 点击**保存**。

NAT 规则如下所示：



在部署配置时会出现一条警告消息：

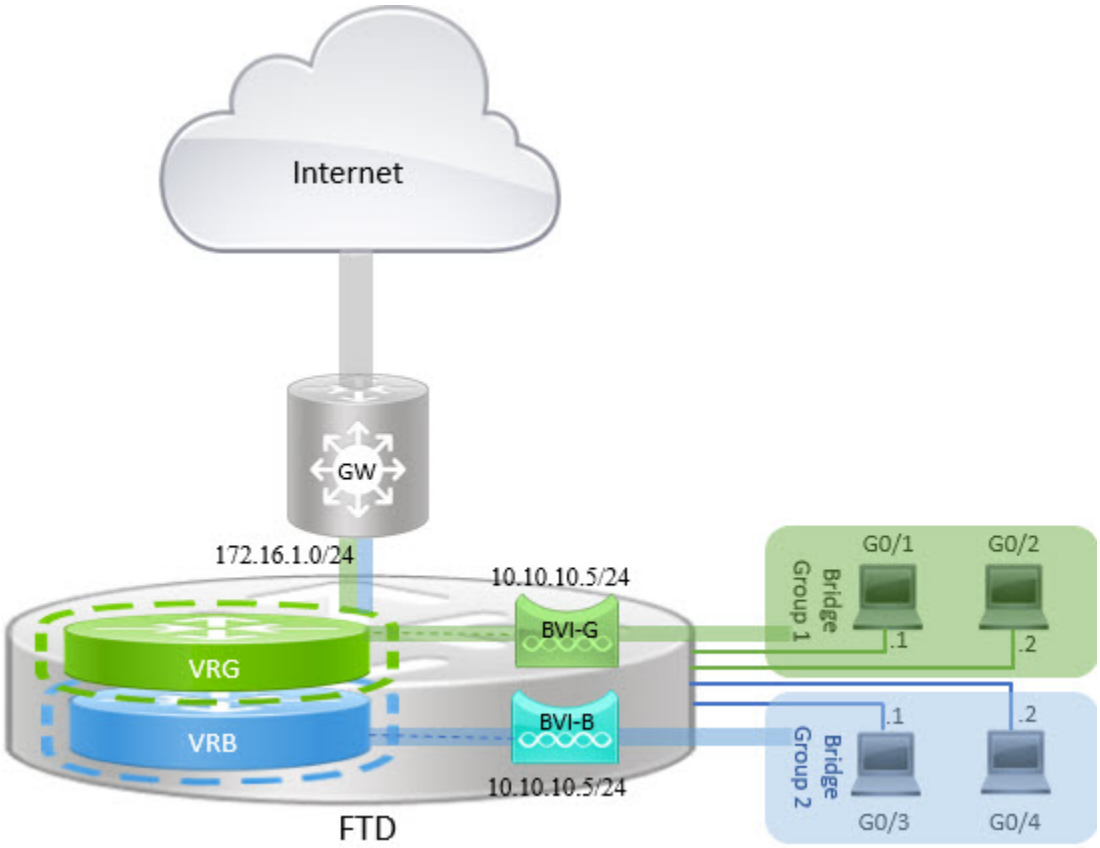


如何使用 BVI 接口在路由防火墙模式下管理重叠网段

您可以在多个重叠网络之间透明地部署单个FTD和/或在同一网络的主机之间部署防火墙。要实现此部署，请按虚拟路由器来配置 BVI。下面介绍了在虚拟路由器中配置 BVI 的程序。

BVI 是路由器内的虚拟接口，其作用类似于普通路由接口。它不支持网桥，但表示路由器内路由接口的可比较网桥组。传入或传出这些桥接接口的所有数据包都会通过 BVI 接口。BVI 的接口编号是虚拟接口所代表的网桥组的编号。

在以下示例中，在 VRG 中配置了 BVI-G，而网桥组 1 是接口 G0/1 和 G0/2 的路由接口。同样，在 VRB 中配置了 BVI-B，网桥组 2 是接口 G0/3 和 G0/4 的路由接口。假设两个 BVI 具有相同的 IP 子网地址，例如 10.10.10.5/24。由于虚拟路由器，网络会在共享资源上被隔离。



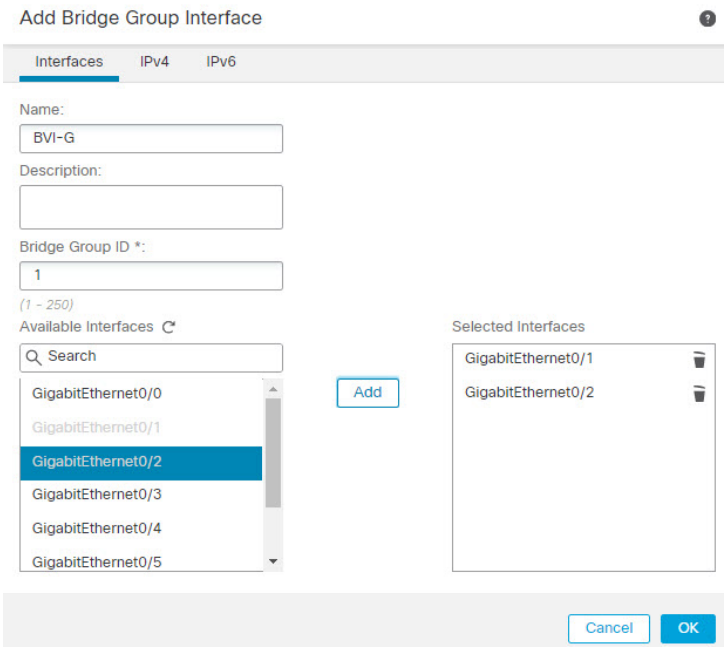
过程

步骤 1 选择**设备** > **设备管理**。编辑所需的设备。

步骤 2 在**接口 (Interfaces)** 中，选择**添加接口 (Add Interfaces)** > **网桥组接口 (Bridge Group Interface)**。

a) 为 BVI-G 输入下列详细信息：

- **名称 (Name)** - 在此示例中，为 BVI-G。
- **网桥组 ID (Bridge Group ID)** - 在本例中为 1。
- **可用接口 (Available Interface)** - 选择接口。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址 (IP Address)** - 输入 10.30.0.1/24。

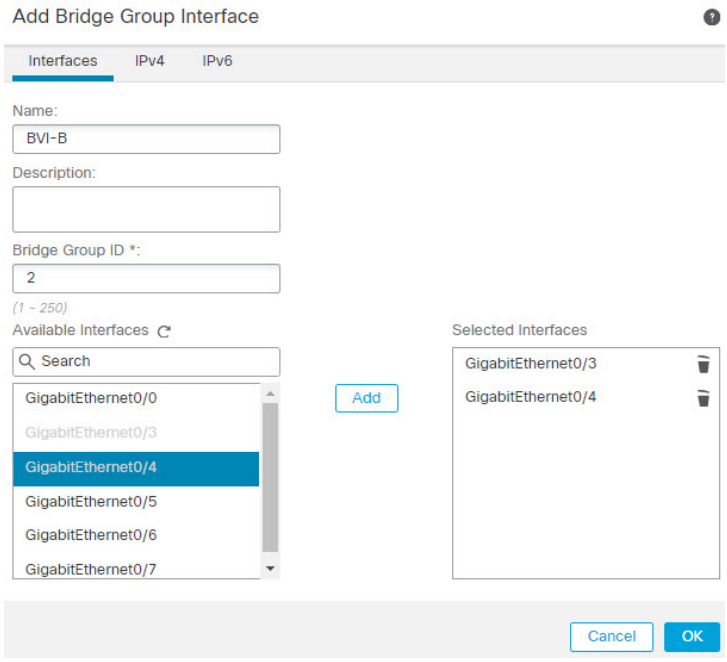


b) 点击**确定**。

c) 点击**保存**。

a) 为 BVI-B 输入下列详细信息：

- **名称 (Name)** - 在此示例中，为 BVI-B。
- **网桥组 ID (Bridge Group ID)** - 在本例中为 2。
- **可用接口 (Available Interface)** - 选择子接口。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址 (IP Address)** - 将此字段留空，因为系统不允许两个接口具有重叠的 IP 地址。您可以重新访问网桥组并在虚拟路由器下对齐后提供相同的 IP 地址。



b) 点击**确定**。

c) 点击**保存**。

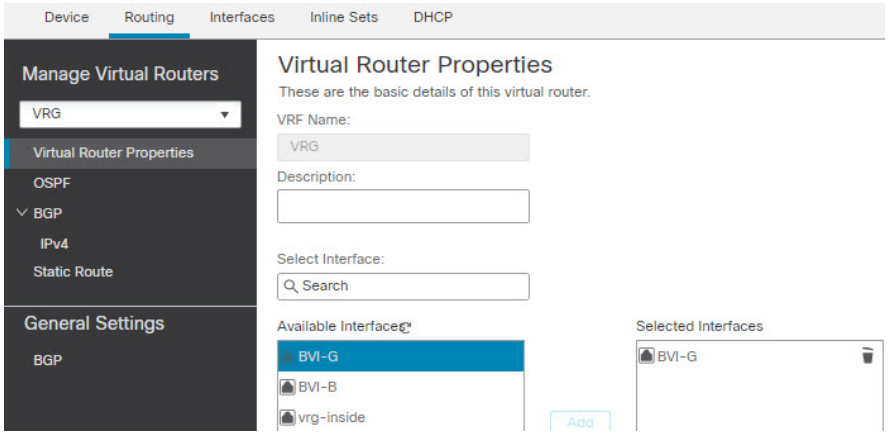
步骤 3 创建虚拟路由器，例如 VRG，然后选择 BVI-G 作为其网络：

a) 选择**设备** > **设备管理**。

b) 编辑设备，然后选择**路由 (Routing)** > **管理虚拟路由器 (Manage Virtual Routers)**。

c) 点击 **Add Virtual Router**。输入虚拟路由器的名称，然后点击**确定 (Ok)**。

d) 在**虚拟路由属性 (Virtual Routing Properties)** 中，选择 **BVI-G**，然后点击**添加 (Add)**。



e) 点击**保存 (Save)**。

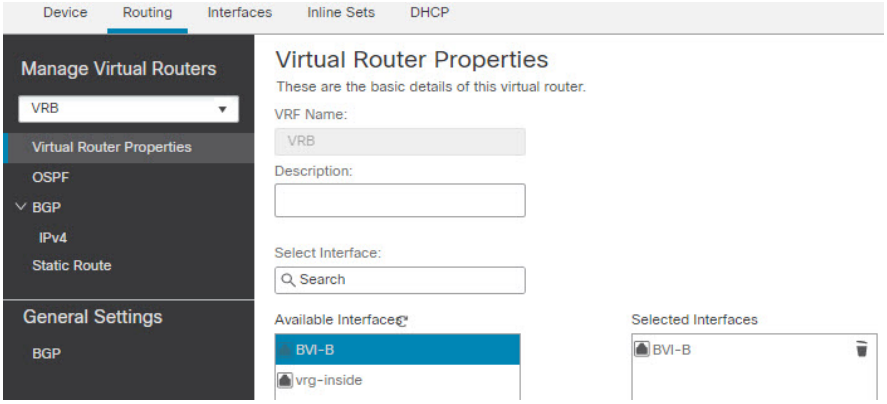
步骤 4 创建虚拟路由器，例如 VRB，然后选择 BVI-B 作为其网络：

a) 选择**设备** > **设备管理**。

b) 编辑设备，然后选择**路由 (Routing)** > **管理虚拟路由器 (Manage Virtual Routers)**。

c) 点击 **Add Virtual Router**。输入虚拟路由器的名称，然后点击**确定 (Ok)**。

d) 在**虚拟路由属性 (Virtual Routing Properties)** 中，选择 **BVI-B**，然后点击**添加 (Add)**。



e) 点击**保存 (Save)**。

步骤 5 重新访问 BVI-B 配置：

a) 依次选择**设备** > **设备管理** > **接口**。

b) 点击 BVI-B 接口的**编辑 (Edit)**。将 IP 地址指定为 10.10.10.5/24。现在，由于接口分别分配给两个不同的虚拟路由器，因此系统允许您使用 BVI-G 的同一 IP 地址进行配置。

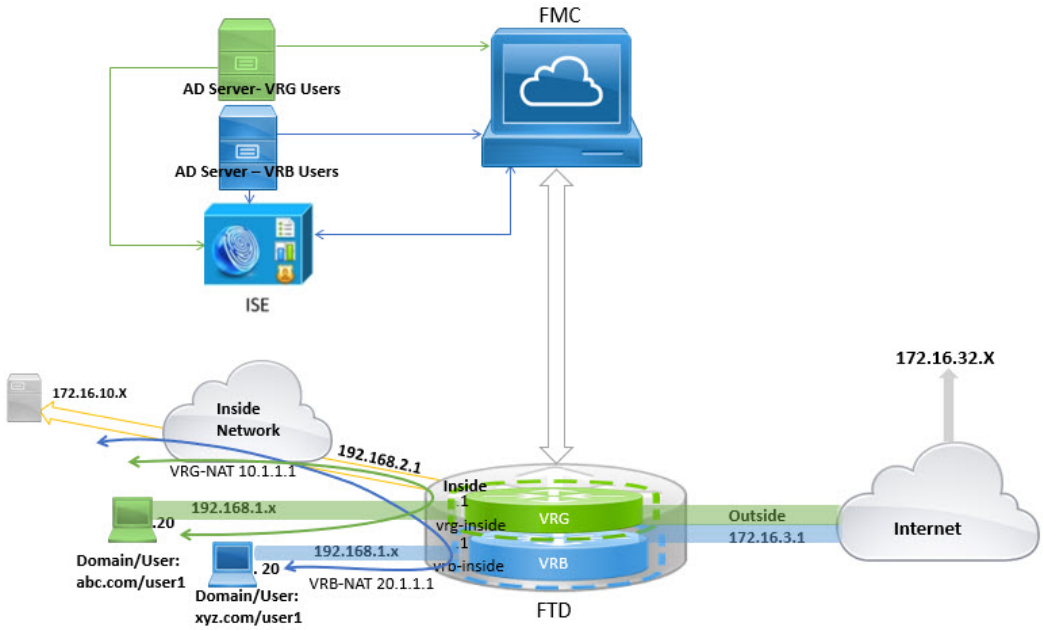
c) 点击**确定**。

d) 点击**保存**。

如果要启用 BVI 间通信，请使用外部路由器作为默认网关。在重叠的 BVI 场景中，如本例所示，使用两次 NAT 外部路由器作为网关来建立 BVI 间流量。为网桥组的成员配置 NAT 时，需要指定成员接口。您不能为网桥组接口 (BVI) 本身配置 NAT。在桥接组成员接口之间执行 NAT 时，必须指定实际地址和映射地址。不能指定“任意”作为接口。

如何使用重叠网络来配置用户身份验证

在虚拟路由中，您可以配置多个具有重叠 IP 和重叠用户的虚拟路由器。在本例中，VRG 和 VRB 是具有重叠 IP - 192.168.1.1/24 的虚拟路由器。两个不同域上的用户也同样位于重叠的网络 IP 192.168.1.20 上。为了让 VRG 和 VRB 用户访问共享服务器 172.16.10.X，可将路由泄漏到全局虚拟路由器。使用源 NAT 来处理重叠 IP。要控制来自 VRG 和 VRB 用户的访问，您必须在 FMC 中设置用户身份验证。FMC 会使用领域、Active Directory、身份源以及身份规则和策略来验证用户身份。由于 FTD 在用户身份验证方面并不发挥直接作用，因此仅通过访问控制策略管理用户访问。要控制来自重叠用户的流量，请使用身份策略和规则来创建访问控制策略。



开始之前

此示例假定您已：

- VRG 和 VRB 用户的两台 AD 服务器。
- 添加了包含两台 AD 服务器的 ISE。

过程

步骤 1 为 VRG 配置设备的内部接口：

a) 依次选择**设备** > **设备管理** > **接口**。

b) 编辑您要分配给 VRG 的接口：

- **名称 (Name)** - 在此示例中为 VRG-inside。
- 选中**启用**复选框。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址 (IP Address)** - 输入 192.168.1.1/24。

c) 点击**确定**。

d) 点击**保存**。

步骤 2 为 VRB 配置设备的内部接口：

a) 依次选择**设备** > **设备管理** > **接口**。

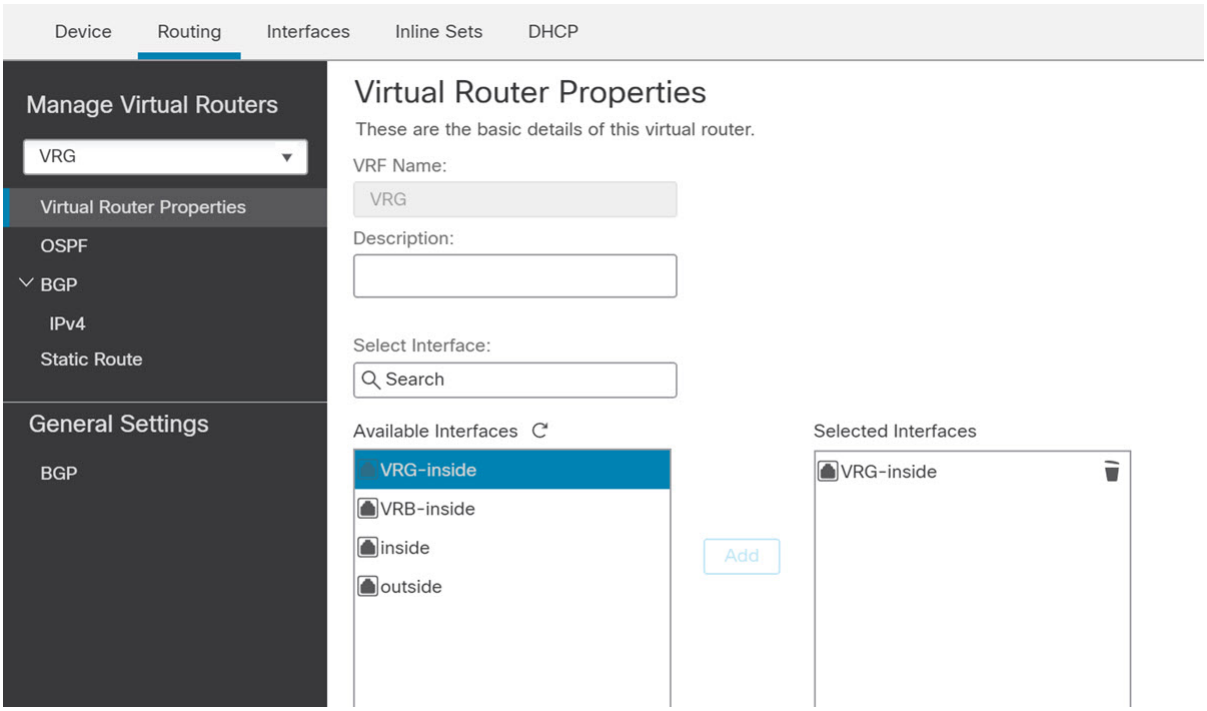
b) 编辑您要分配给 VRB 的接口：

- **名称 (Name)** - 在此示例中为 VRB-inside。
- 选中**启用**复选框。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址** - 将其留空。该系统不允许您使用相同的 IP 地址配置接口，因为您尚未创建用户定义的虚拟路由器。

c) 点击**确定**。
d) 点击**保存**。

步骤 3 将 VRG 和静态默认路由泄漏配置到全局路由器的内部接口，以便 VRG 用户访问通用服务器 172.16.10.1：

a) 依次选择**设备** > **设备管理**，然后编辑 FTD 设备。
b) 依次选择**路由** > **管理虚拟路由器**。点击**添加虚拟路由器 (Add Virtual Router)**并创建 VRG。
c) 对于 VRG，在**虚拟路由器属性 (Virtual Router Properties)** 中分配 VRG-inside 并保存。



d) 点击**静态路由 (Static Route)**。
e) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的内部接口。
- **网络 (Network)** - 选择 any-ipv4 对象。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。

f) 点击**确定**。

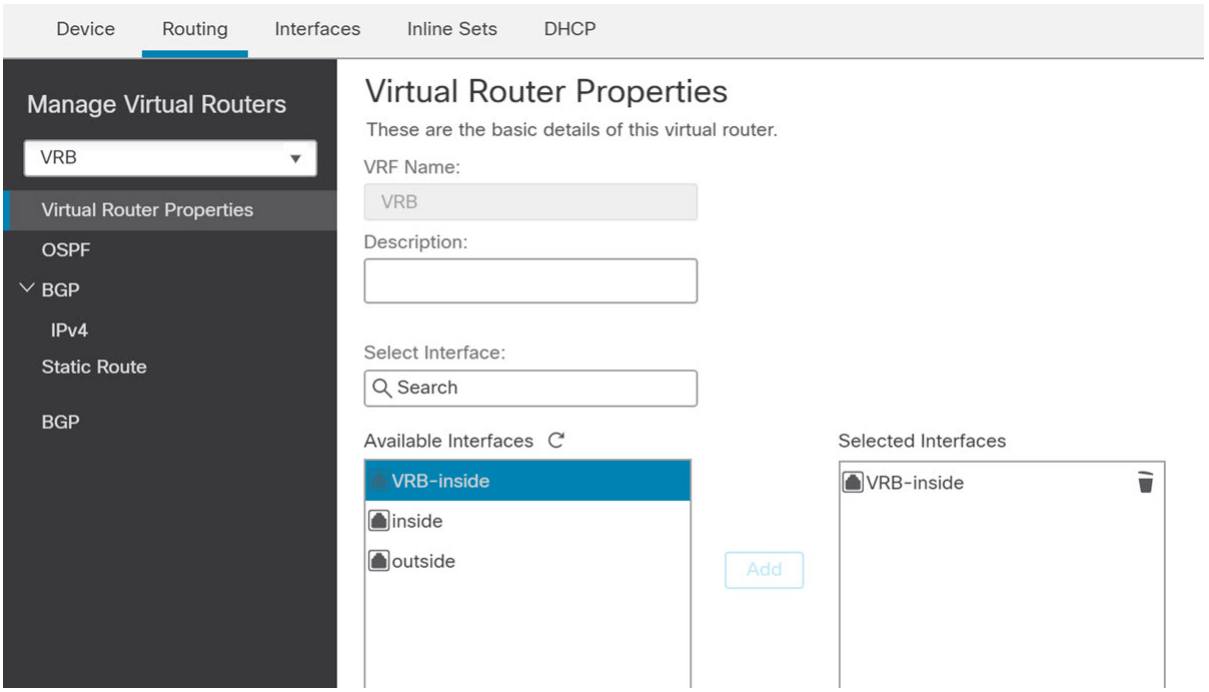
g) 点击**保存**。

步骤 4 将 VRB 和静态默认路由泄漏配置到全局路由器的内部接口，以便 VRB 用户访问共享服务器 172.16.10.x：

a) 依次选择**设备** > **设备管理**，然后编辑 FTD 设备。

b) 依次选择**路由** > **管理虚拟路由器**。点击**添加虚拟路由器 (Add Virtual Router)**并创建 VRB。

c) 对于 VRB，在**虚拟路由器属性 (Virtual Router Properties)** 中分配 VRB-inside 并保存。



d) 点击**静态路由 (Static Route)**。

e) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的内部接口。
- **网络 (Network)** - 选择 any-ipv4 对象。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。

f) 点击**确定**。

g) 点击**保存**。

步骤 5 重新访问 VRB-inside 接口配置：

a) 依次选择**设备** > **设备管理** > **接口**。

b) 点击 VRB-inside 接口的**编辑 (Edit)**。将 IP 地址指定为 192.168.1.1/24。现在，由于接口分别分配给两个不同的虚拟路由器，因此系统允许您使用 VRG-inside 的相同 IP 地址进行配置。

c) 点击**确定**。

d) 点击**保存**。

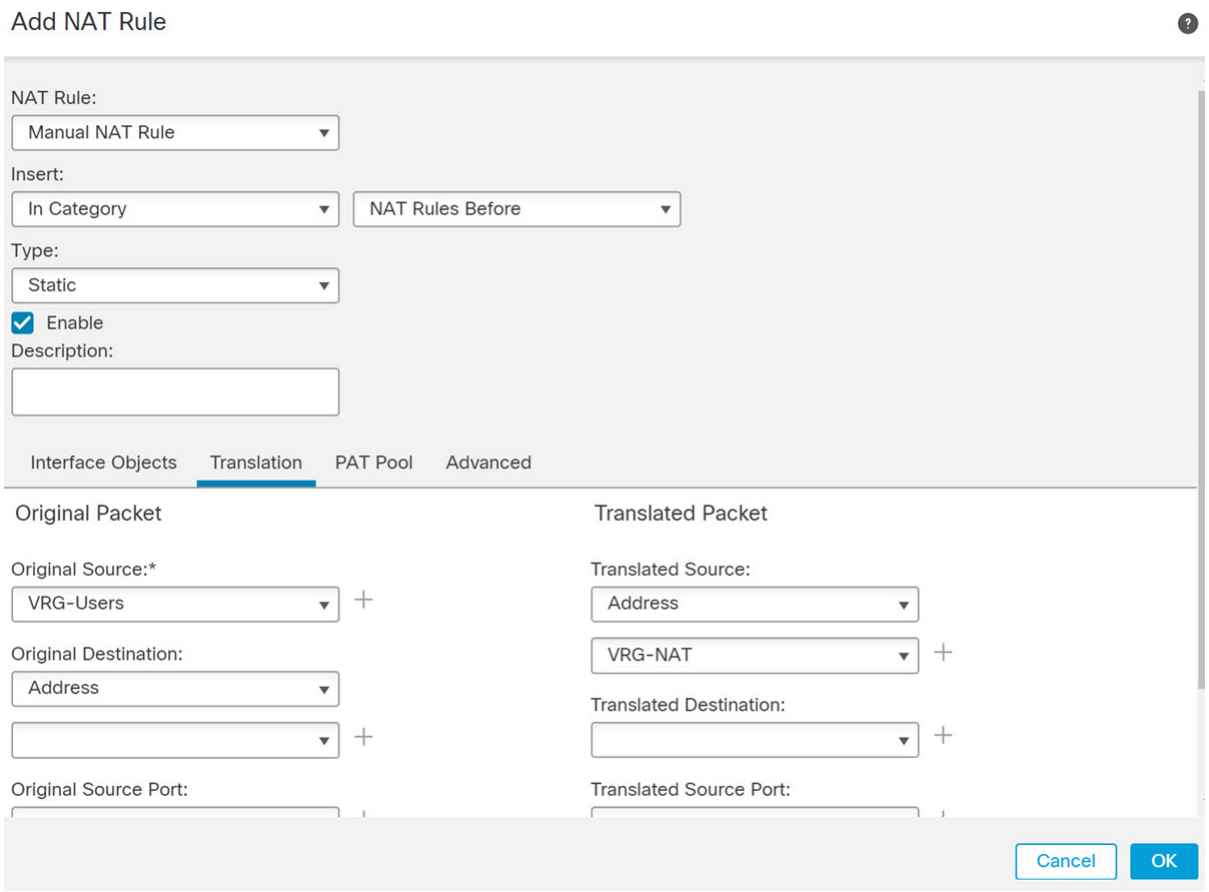
步骤 6 为源对象 VRG 和 VRB 添加 NAT 规则。点击**设备 (Devices)** > **NAT**。

步骤 7 点击**新策略 (New Policy)** > **威胁防御 NAT (Threat Defense NAT)**。

步骤 8 输入 NAT 策略名称，然后选择 FTD 设备。点击**保存 (Save)**。

步骤 9 在 NAT 页面中，点击**添加规则 (Add Rule)** 并为 VRG 定义以下源 NAT：

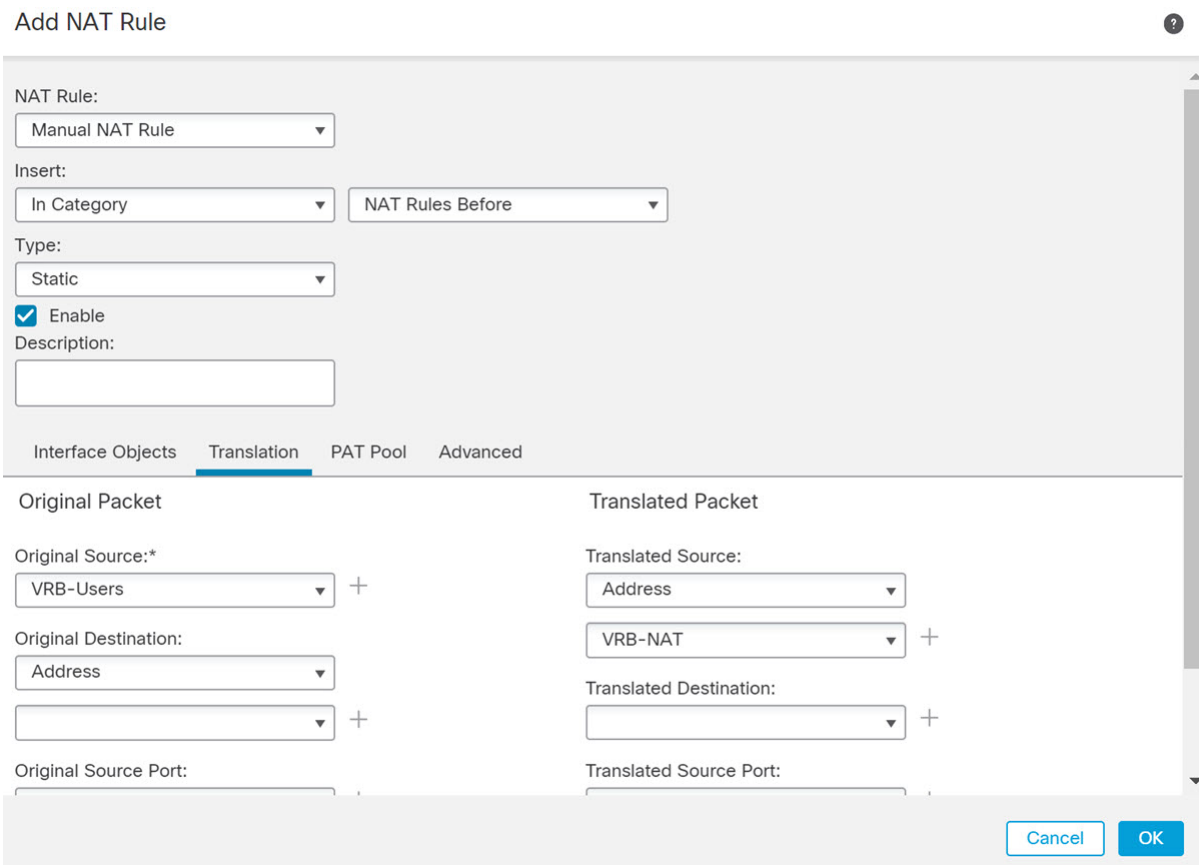
- **NAT 规则 (NAT Rule)** - 选择“手动 NAT 规则”(Manual NAT Rule)。
- **类型 (Type)** - 选择“静态”(Static)。
- **插入 (Insert)** - 如果存在任何 NAT 规则，则选择“上方”(Above)。
- 点击 **Enabled**。
- 在**接口对象 (Interface Objects)**中，选择 VRG-Inside 对象，然后点击**添加到源 (Add to Source)**（如果对象不可用，请在**对象 (Object)** > **对象管理 (Object Management)** > **接口 (Interface)** 中创建一个对象），然后选择 Global-Inside 对象并点击**添加到目标 (Add to Destination)**。
- 在**转换 (Translation)** 中选择以下选项：
  - **原始源 (Original Source)**，选择 VRG-Users。
  - **转换后的源 (Translated Source)**，点击**添加 (Add)**并使用 10.1.1.1 来定义对象 VRG-NAT。选择 VRG-NAT，如下图所示：



步骤 10 点击**确定**。

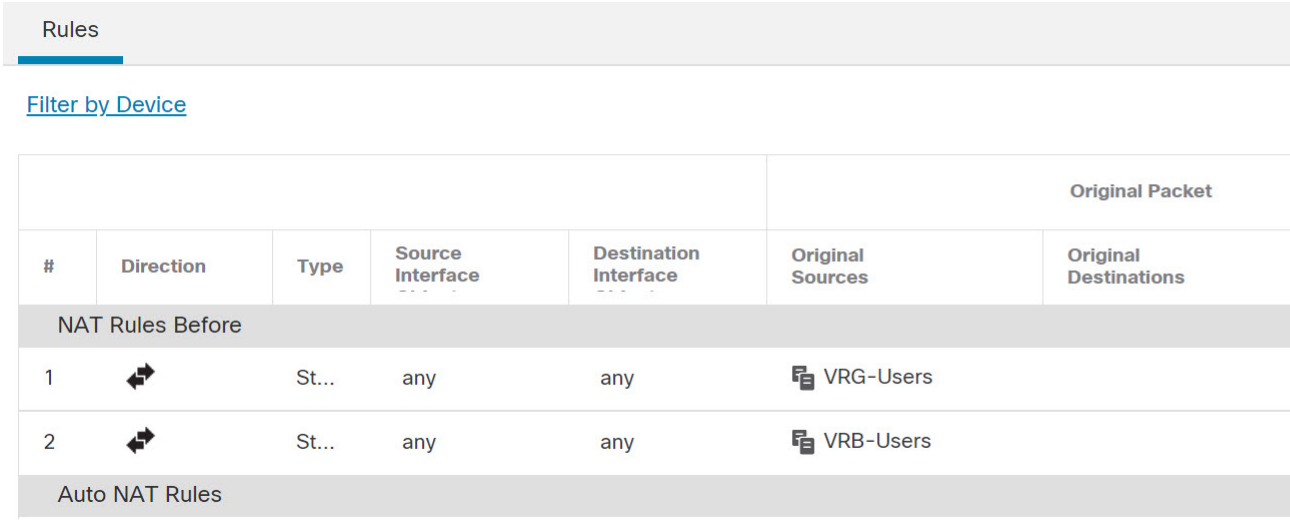
步骤 11 在 NAT 页面中，点击**添加规则 (Add Rule)** 并为 VRB 定义以下源 NAT：

- **NAT 规则 (NAT Rule)** - 选择“手动 NAT 规则”(Manual NAT Rule)。
- **类型 (Type)** - 选择“静态”(Static)。
- **插入 (Insert)** - 如果存在任何 NAT 规则，则选择“上方”(Above)。
- 点击 **Enabled**。
- 在**接口对象 (Interface Objects)**中，选择 VRB-Inside 对象，然后点击**添加到源 (Add to Source)**（如果对象不可用，请在**对象 (Object)** > **对象管理 (Object Management)** > **接口 (Interface)** 中创建一个对象），然后选择 Global-Inside 对象并点击**添加到目标 (Add to Destination)**。
- 在**转换 (Translation)** 中选择以下选项：
  - **原始源 (Original Source)**，选择 VRB-Users。
  - **转换后的源 (Translated Source)**，点击**添加 (Add)**并使用 20.1.1.1 来定义对象 VRB-NAT。选择 VRB-NAT，如下图所示：



步骤 12 点击**保存**。

NAT 规则如下所示：



步骤 13 在 FMC 中为每个 VRG 和 VRB 用户添加两个唯一的 AD 服务器 - 选择**系统 (System)** > **集成 (Integration)** > **领域 (Realms)**。

步骤 14 点击**新建领域 (New Realm)** 并填写字段。有关这些字段的详细信息，请参阅领域字段，第 1818 页。

步骤 15 要控制来自 VRG 和 VRB 用户的访问，请定义 2 个 Active Directory，请参阅领域目录和 同步 字段，第 1822 页请参阅创建 Active Directory 领域和领域目录，第 1816 页

步骤 16 在 FMC 中添加 ISE - 选择**系统 (System)** > **集成 (Integration)** > **身份源 (Identity Sources)**。

步骤 17 点击**身份服务引擎 (Identity Services Engine)** 并填写字段。有关这些字段的详细信息，请参阅如何为无领域的用户控制配置 ISE/ISE-PIC，第 1851 页。

步骤 18 创建身份策略和规则，然后定义访问控制策略，以便控制来自 VRG 和 VRB 的重叠用户的访问。

如何使用 BGP 来互连虚拟路由器

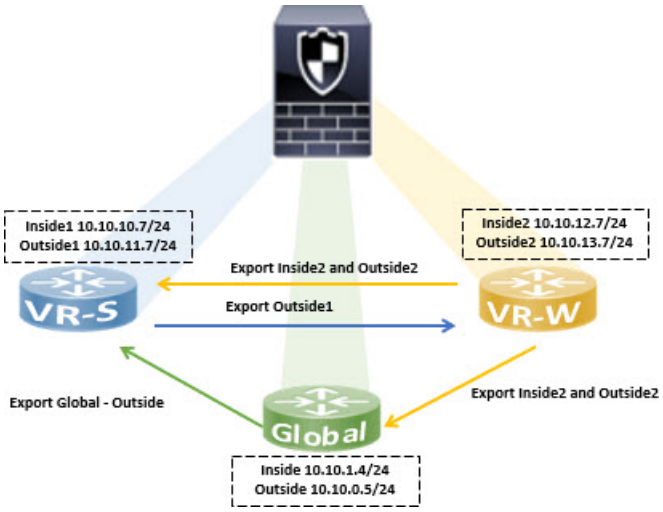
现在，您可以在设备上配置BGP设置，以便在虚拟路由器（全局和用户定义的虚拟路由器）之间泄漏路由。源虚拟路由器的路由目标会被导出到BGP表，而该表又会被导入到目的虚拟路由器。路由地图用于与用户定义的虚拟路由器共享全局虚拟路由，反之亦然。请注意，所有路由到BGP表的导入或导出都在用户定义的虚拟路由器上配置，包括全局虚拟路由。

假设工厂的防火墙设备配置了以下虚拟路由器和接口：

- 全局虚拟路由器配置了内部 (10.10.1.4/24) 和外部 (10.10.0.5/24)
- VR-S（销售）虚拟路由器配置了 Inside1 (10.10.10.7/24) 和 outside1 (10.10.11.7/24)
- VR-W（仓库）虚拟路由器配置了 Inside2 (10.10.12.7/24) 和 outside2 (10.10.13.7/24)

假设您想把仓库 (VR-W) 的路由泄漏给销售 (VR-S) 和全局，并将 VR-S 的外部接口路由到 VR-W。同样，您想把全局路由器的外部接口路由泄漏给销售 (VR-S)。此示例演示了实现路由器互连的 BGP 配置程序：

图 *122:* 使用 *BGP* 设置来互连虚拟路由器



开始之前

- 创建虚拟路由器 - VR-S 和 VR-W。
- 启用 BGP，并为每个虚拟路由器选择配置 BGP 重新分发设置。

过程

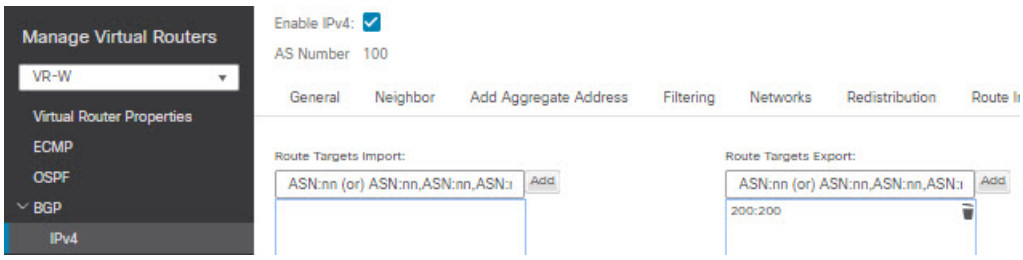
步骤 1 配置 VR-W 以将其带有路由目标的路由导出至 VR-S：

a) 选择**设备 (Devices)** > **设备管理 (Device Management)**，编辑设备，然后点击**路由 (Routing)** 选项卡。

b) 在虚拟路由器下拉列表中选择 VR-W。

c) 点击 **BGP** > **IPv4** > **路由导入/导出 (Route Import/Export)**。

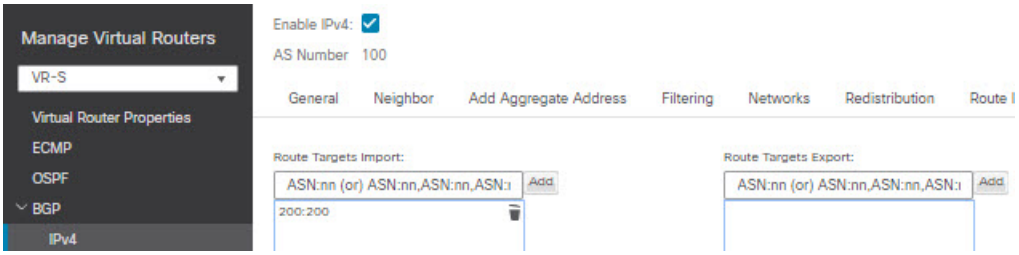
d) 要将 VR-W 路由泄漏到 VR-S，请使用路由目标标记路由，以便将 VR-W 路由导出到其 BGP 表中，并在它上面标记路由目标。在**路由目标导出 (Route Targets Export)** 字段中，输入一个值，例如 *200:200*。点击**添加 (Add)**：



e) 从虚拟路由器下拉列表中选择 VR-S。

f) 点击 **BGP** > **IPv4** > **路由导入/导出 (Route Import/Export)**。

g) 要从 VR-W 接收泄漏的路由，请配置“导入路由目标”(Import Route Target)，以便从（对等体或重新分发的）BGP 表导入标记有路由目标的 VR-W 路由。在**路由目标导入 (Route Targets Import)** 字段中，输入您为 VR-W 配置的相同路由目标值 *200:200*。点击**添加 (Add)**。



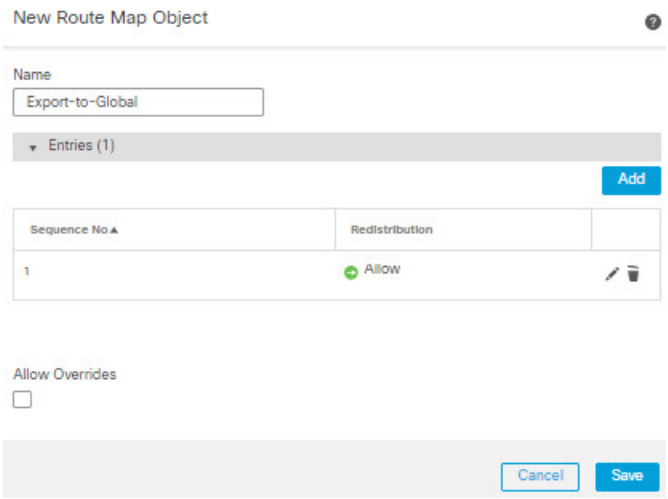
注释 如果要对从 VR-W 泄漏的路由进行条件化，可以在路由映射对象中指定匹配条件，并在**用户虚拟路由器导出路由地图 (User Virtual Router Export Route Map)** 中选择该匹配条件。同样，如果想对要从 BGP 表导入 VR-S 的路由进行条件化，您可以使用**用户虚拟路由器导入路由映射 (User Virtual Router Import Route Map)**。此程序在步骤 3 中进行了介绍。

步骤 2 配置 VR-W 以便将其路由导出到全局虚拟路由器：

a) 您需要创建一个允许将 VR-W 路由导出到全局路由表的路由地图。选择**对象 (Objects)** > **对象管理 (Object Management)** > **路由地图 (Route Map)**。

b) 点击**添加路由地图 (Add Route Map)**，为其命名（如 *Export-to-Global*），然后点击**添加 (Add)**。

c) 指定**序列号 (Sequence Number)**（比如 1），然后从**重新分配 (Redistribution)** 下拉列表选择“运行”(Allow)：

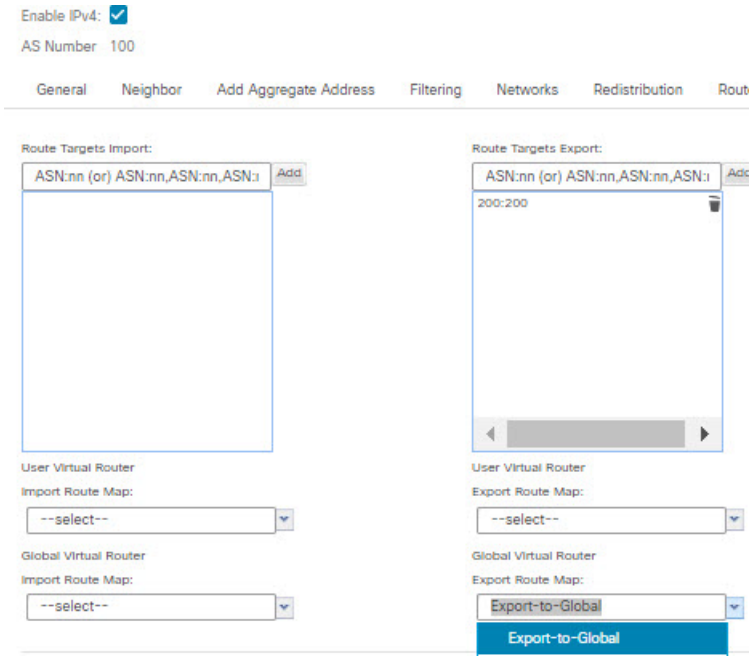


d) 点击**保存 (Save)**。

在本例中，所有 VR-W 路由都会被泄漏到全局路由表。因此，没有为路由映射配置匹配条件。

e) 导航到设备的**路由 (Routing)** 选项卡，然后选择 VR-W。点击 **BGP** > **IPv4** > **路由导入/导出 (Route Import/Export)**。

f) 从全局虚拟路由器导出路由地图 **(Global Virtual Router Export Route Map)** 下拉列表中，选择 Export-to-Global：



步骤 3 要仅将 VR-S 的外部 1 路由泄漏到 VR-W，请执行以下操作：

a) 从虚拟路由器下拉列表中选择 VR-S。

b) 点击 **BGP** > **IPv4** > **路由导入/导出 (Route Import/Export)**。

c) 要将 VR-S 路由泄漏到 VR-W，请使用路由目标标记路由，以便将 VR-S 路由导出到其 BGP 表中，并在它上面标记路由目标。在**路由目标导出 (Route Targets Export)** 字段中，输入一个值，例如 *100:100*。点击**添加 (Add)**。

d) 从虚拟路由器下拉列表中，选择 VR-W，然后选择 **BGP** > **IPv4** > **路由导入/导出 (Route Import/Export)**。

e) 要从 VR-S 接收泄漏的路由，请配置“导入路由目标”(Import Route Target)，以便从（对等体或重新分发的）BGP 表导入标记有路由目标的 VR-S 路由。在**路由目标导入 (Route Targets Import)** 字段中，输入 VR-S 路由目标值 *100:100*。点击**添加 (Add)**。

f) 现在，您需要将 VR-S 的外部 1 路由限制为泄漏到 VR-W。选择**对象 (Objects)** > **对象管理 (Object Management)** > **前缀列表 (Prefix List)** > **IPv4 前缀列表 (IPv4 Prefix List)**。

g) 点击**添加 IPv4 前缀列表 (Add IPv4 Prefix List)**，提供名称（如 *VRS-Outside1-Only*），然后点击**添加 (Add)**。

h) 指定**序列号 (Sequence Number)**（比如 1），然后从**重新分配 (Redistribution)** 下拉列表选择“运行”(Allow)。

i) 输入 VR-S outside1 接口的 IP 地址（前两个八位组）。

j) 点击**保存 (Save)**。

k) 使用带前缀列表的 match 子句来创建路由地图。点击**路由地图 (Route Map)**。点击**添加路由映射 (Add Route Map)**，指定名称（如 *Import-from-VRS*），然后点击**添加 (Add)**。

l) 指定**序列号 (Sequence Number)**（比如 1），然后从**重新分配 (Redistribution)** 下拉列表选择“运行”(Allow)。

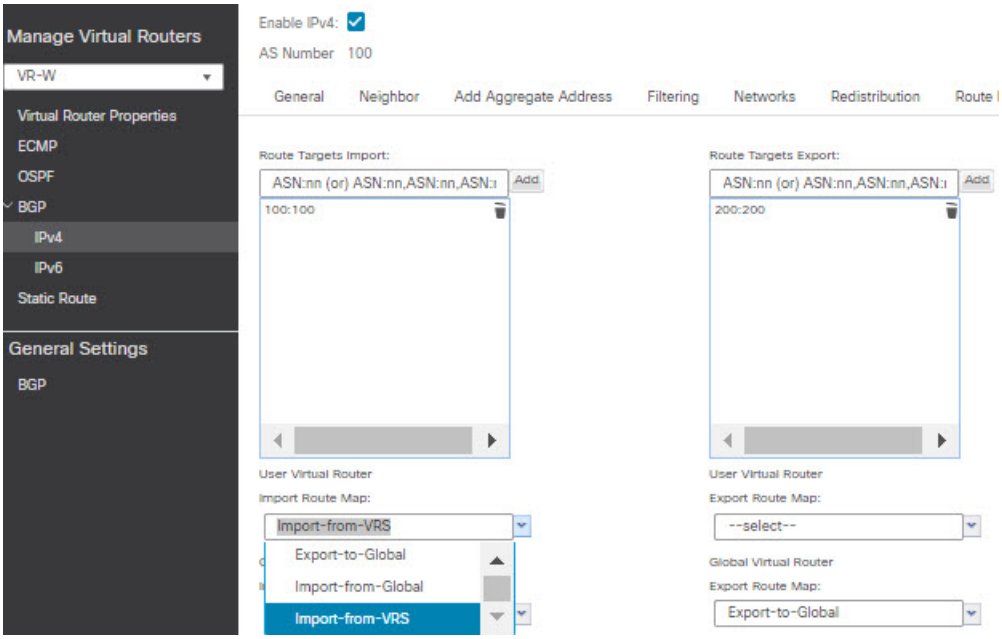
m) 在**匹配子句 (Match Clause)** 选项卡中，点击 **IPv4**。在**地址 (Address)** 选项卡下，点击**前缀列表 (Prefix List)**。

n) 在**可用 IPv4 前缀列表 (Available IPv4 Prefix List)** 下，选择 VRS-Outside1-Only，然后点击**添加 (Add)**。

o) 点击**保存 (Save)**。

p) 导航到设备的**路由 (Routing)** 选项卡，然后选择 VR-W。点击 **BGP** > **IPv4** > **路由导入/导出 (Route Import/Export)**。

q) 从**全局虚拟路由器导入路由地图 (Global Virtual Router Import Route Map)** 下拉列表中，选择 Import-from-VRS：



步骤 4 配置 VR-S 以便导入全局虚拟路由器的外部路由：

注释 要从全局虚拟路由器泄漏路由，您必须分别配置源或目标用户定义的虚拟路由器。因此，在本例中，VR-S 是从全局虚拟路由器的外部接口导入路由的目的路由器。

a) 选择**对象 (Objects)** > **对象管理 (Object Management)** > **前缀列表 (Prefix List)** > **IPv4 前缀列表 (IPv4 Prefix List)**。

b) 点击**添加 IPv4 前缀列表 (Add IPv4 Prefix List)**，提供名称（如 *Global-Outside-Only*），然后点击**添加 (Add)**。

c) 指定**序列号 (Sequence Number)**（比如 1），然后从**重新分配 (Redistribution)** 下拉列表选择“运行”(Allow)。

d) 输入 Global Outside 接口的 IP 地址（前两个八位组）：

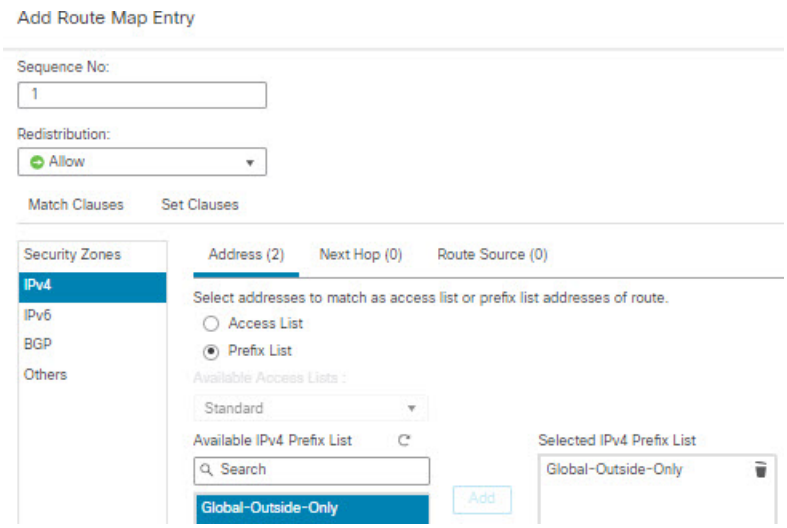
e) 点击保存 **(Save)**。

f) 点击路由地图 **(Route Map)**。点击添加路由映射 **(Add Route Map)**，指定名称（如 *Import-from-Global*），然后点击添加 **(Add)**。

g) 指定序列号 **(Sequence Number)**（比如 1），然后从重新分配 **(Redistribution)** 下拉列表选择“运行”(Allow)。

h) 在匹配子句 **(Match Clause)** 选项卡中，点击 **IPv4**。在地址 **(Address)** 选项卡下，点击前缀列表 **(Prefix List)**。

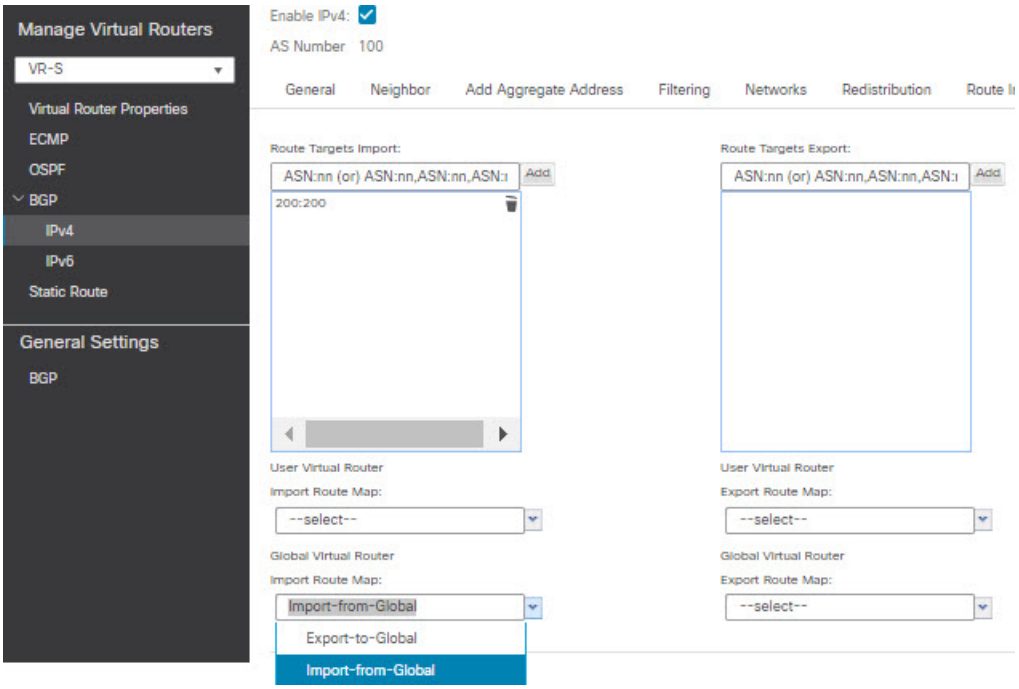
i) 在可用 **IPv4** 前缀列表 **(Available IPv4 Prefix List)** 下，选择 Global-Outside-Only，然后点击添加 **(Add)**。



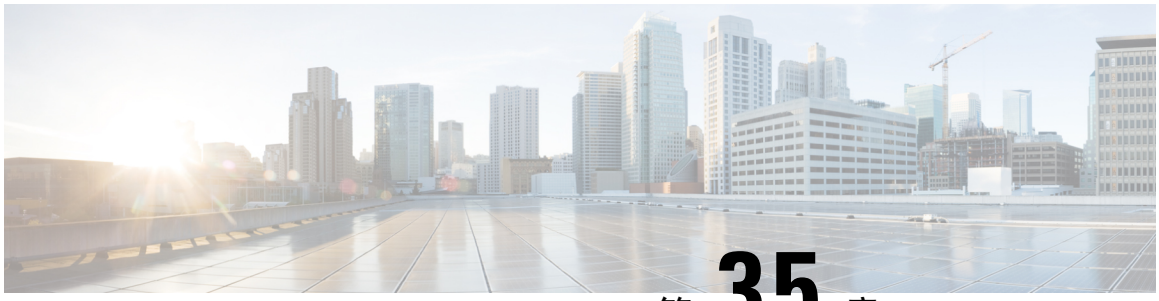
j) 点击保存 **(Save)**。

k) 导航到设备的路由 **(Routing)** 选项卡，然后选择 VR-S。点击 **BGP** > **IPv4** > 路由导入/导出 **(Route Import/Export)**。

l) 从全局虚拟路由器导入路由地图 **(Global Virtual Router Import Route Map)** 下拉列表中，选择 Import-from-Global：



步骤 **5** 保存 **(Save)** 和部署 **(Deploy)**。



第 35 章

ECMP

本章介绍配置等价多路径 (ECMP) 路由的程序，该路由协议用于网络流量负载均衡。

关于 ECMP

Firepower 威胁防御设备支持等价多路径 (ECMP) 路由。您可以将每个虚拟路由器的流量区域配置为包含一组接口。您可以在每个区域中最多跨 8 个接口配置最多 8 个等价静态或动态路由。例如，您可以在区域中跨三个接口配置多个默认路由：

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

ECMP 的准则和限制

防火墙模式指导原则

ECMP 区域仅在路由防火墙模式下支持。

设备准则

- 威胁防御 6.5 及更高版本的设备支持在 管理中心 中配置 ECMP 流量区域：

  - 版本 6.6 及更高版本的 威胁防御 设备支持每个虚拟路由器的 ECMP。但思科 Firepower 1010 不支持虚拟路由。因此，对于 Firepower 1010，您可以将全局接口与 ECMP 相关联。
  - 同样，威胁防御 6.5 版设备不支持虚拟路由，您可以将全局接口与 ECMP 相关联。
- 一台设备最多可以有 256 个 ECMP 区域。

接口指导原则

- 只有路由接口才能与 ECMP 区域相关联。
- 只有具有逻辑名称的接口才能与 ECMP 区域相关联。
- 接口应属于在上面创建 ECMP 的虚拟路由器。
- 每个 ECMP 区域只能关联 8 个接口。
- 接口只能是一个 ECMP 区域的成员。
- 不能从 ECMP 区域中删除与等价静态路由相关联的接口。
- 如果 ECMP 区域的接口具有与其关联的等价静态路由，则您无法删除该区域。
- 对于 7.1 之前的 威胁防御 版本，sVTI 接口不能用于 ECMP 区域。
- 对于 7.1 之前的 威胁防御 版本，站点间 VPN 或远程访问 IPsec-IKEv2 VPN 中不支持 ECMP 区域成员接口。
- 以下接口不能与 ECMP 区域相关联：
  - BVI 接口。
  - EtherChannel 中的成员接口。
  - 故障转移或状态链路接口。
  - 管理专用接口或管理访问接口。
  - 集群控制链路接口。
  - 冗余接口及其成员。
  - VNI。
  - VLAN 接口。
  - 已启用 SSL 的 RA VPN 配置中的接口。

升级指南

升级到 管理中心 7.1 时，现有的 ECMP FlexConfig 不会被部署到设备。因此，要成功部署，您必须在 UI 中将 FlexConfig 流量区域手动迁移到 ECMP。

您可以从 管理中心 UI 为所有 6.5 及更高版本的路由设备创建 ECMP。

其他规定

- DHCP 中继 - 不在与 ECMP 区域关联的接口上启用 DHCP 中继。

管理 ECMP 页面

当您点击“路由”(Routing) 窗格中的 **ECMP** 时，系统将显示与虚拟路由器对应的 ECMP 页面。此页面将显示现有 ECMP 区域以及虚拟路由器的关联接口。在此页面中，您可以将 ECMP 区域添加到虚拟路由器。您还可以 **编辑**（ ） 和 **删除**（ ） ECMP。

您可以执行以下操作：

- 创建 ECMP 区域，第 857 页
- 配置等价静态路由，第 858 页
- 修改 ECMP 区域，第 859 页
- 删除 ECMP 区域，第 860 页

创建 ECMP 区域

ECMP 区域会按虚拟路由器来创建。因此，只有创建 ECMP 的虚拟路由器的接口才能与 ECMP 相关联。

过程

步骤 1 依次选择**设备** > **设备管理**，并且编辑 威胁防御设备。

步骤 2 点击**路由**。

步骤 3 在虚拟路由器下拉列表中，选择要在其中创建 ECMP 区域的虚拟路由器。

您可以在全局虚拟路由器和用户定义的虚拟路由器中创建 ECMP 区域。有关创建虚拟路由器的信息，请参阅创建虚拟路由器，第 815 页。

步骤 4 点击 **ECMP**。

步骤 5 点击**添加 (Add)**。

步骤 6 在**添加 ECMP (Add ECMP)** 框中，输入 ECMP 区域的名称。

注释 路由设备的 ECMP 名称必须是唯一的。

步骤 7 要关联接口，请在**可用接口 (Available Interfaces)**框下选择接口，然后点击**添加 (Add)**。

请记住以下几点：

- 只有属于虚拟路由器的接口可供分配。

- **可用接口**框下仅列出具有逻辑名称的接口。您可以编辑接口并在**接口**中提供逻辑名称。请记住保存更改，以使设置生效。

步骤 8 点击**确定 (OK)**。

ECMP 页面现在会显示新创建的 ECMP。

步骤 9 点击**保存 (Save)** 和**部署 (Deploy)** 以部署配置。

通过为其定义相同的目标和指标值但使用不同的网关，您可以将 ECMP 区域接口与等价静态路由相关联。

下一步做什么

- 配置等价静态路由，第 858 页
- 修改 ECMP 区域，第 859 页
- 删除 ECMP 区域，第 860 页

配置等价静态路由

智能许可证	经典许可证	支持的设备	支持的域	访问权限
任意	不适用	威胁防御和threat defense virtual	任意	管理员/网络管理员/安全审批人

您可以将虚拟路由器的接口（全局和用户定义）分配给设备的 ECMP 区域。

开始之前

- 要为接口配置等价静态路由，请确保将其与 ECMP 区域关联。请参阅创建 ECMP 区域，第 857 页。
- 非 VRF 设备的所有路由配置设置也可用于全局虚拟路由器。
- 如果没有将接口与 ECMP 区域关联，则无法为具有相同目标和指标的接口定义静态路由。

过程

步骤 1 在**设备 (Devices)** > **设备管理 (Device Management)** 页面中，编辑 威胁防御 设备。点击**路由**选项卡。

步骤 2 从下拉列表中，选择其接口与 ECMP 区域相关联的虚拟路由器。

步骤 3 要为接口配置等价静态路由，请点击**静态路由 (Static Route)**。

步骤 4 点击**添加路由 (Add Route)** 以添加新路由，或点击现有路由的 **编辑**（ ）。

步骤 5 从**接口 (Interface)** 下拉列表中，选择属于虚拟路由器的接口和 ECMP 区域。

步骤 6 从**可用网络 (Available Networks)** 框中选择目标网络，然后点击**添加 (Add)**。

步骤 7 输入网络的网关。

步骤 8 输入指标值。它可以是介于 1 和 254 之间的数字。

步骤 9 要保存设置，点击**保存**。

步骤 10 要配置等价静态路由，请重复上述步骤，为同一 ECMP 区域中具有相同目的网络和指标值的另一个接口配置静态路由。请记住提供其他网关。

下一步做什么

- 修改 ECMP 区域，第 859 页
- 删除 ECMP 区域，第 860 页

修改 ECMP 区域

过程

步骤 1 依次选择**设备** > **设备管理**，然后编辑 FTD 设备。

步骤 2 点击**路由**。

步骤 3 点击 **ECMP**。

ECMP 区域及其关联的接口会显示在 **ECMP** 页面中。

步骤 4 要修改 ECMP，请根据所需的 ECMP 点击 **编辑**（）。在**编辑 ECMP (Edit ECMP)** 框中，您可以执行以下操作：

- ECMP 名称 (ECMP Name) - 确保更改的名称对于设备是唯一的。
- 接口 (Interfaces) - 您可以添加或删除接口。您不能包含已与其他 ECMP 关联的接口。此外，您不能删除与等价静态路由关联的接口。

步骤 5 点击**确定 (OK)**。

步骤 6 要保存更改，请点击**保存**。

下一步做什么

- 配置等价静态路由，第 858 页
- 删除 ECMP 区域，第 860 页

删除 ECMP 区域

过程

步骤 1 依次选择**设备** > **设备管理**，然后编辑 FTD 设备。

步骤 2 点击**路由**。

步骤 3 点击 **ECMP**。

ECMP 区域及其关联的接口会显示在 **ECMP** 页面中。

步骤 4 要删除 ECMP 区域，请点击 ECMP 区域旁的 **删除**（ ）。

如果 ECMP 区域的任何接口与等价静态路由关联，则您无法删除该区域。

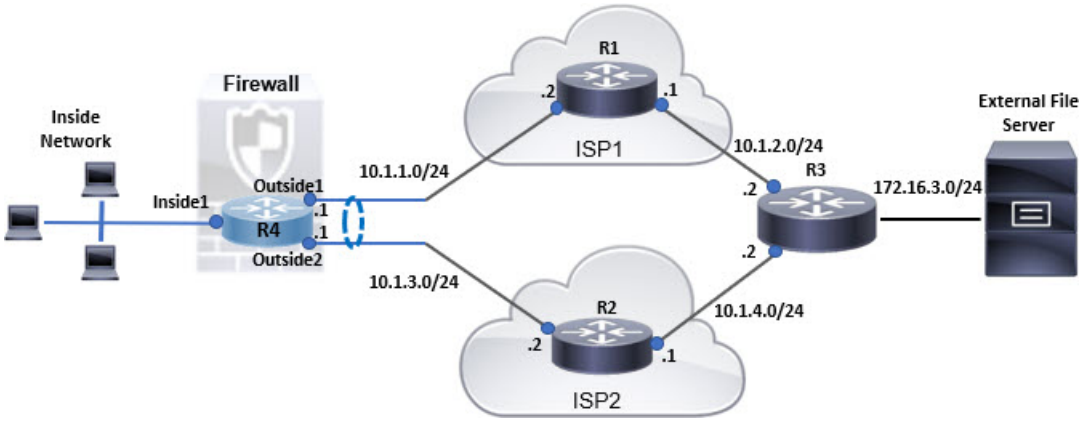
步骤 5 在确认邮件中点击**删除 (Delete)**。

步骤 6 要保存更改，请点击**保存**。

ECMP 的配置示例

此示例演示了如何使用 管理中心 在 威胁防御 上配置 ECMP 区域，以便有效地处理流经设备的流量。如果配置了 ECMP，威胁防御 会维护每个区域的路由表，因此可以在最佳路由中重新路由数据包。因此，ECMP 支持非对称路由、负载均衡并无缝处理丢失的流量。在本例中，R4 会记录到达外部文件服务器的两个路径。

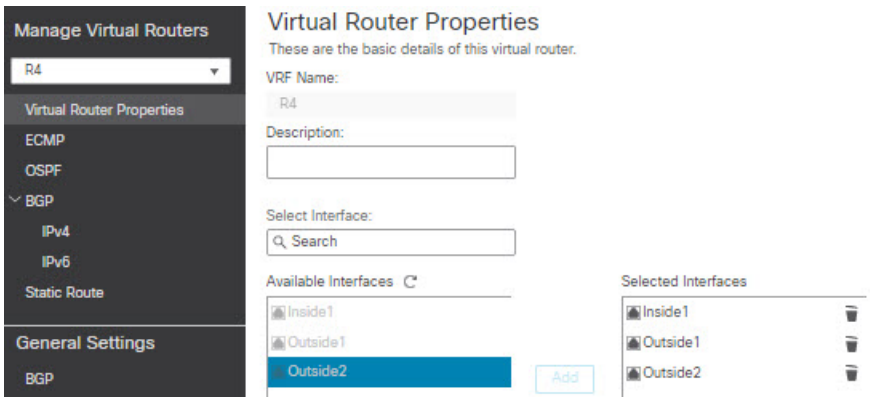
图 *123: ECMP* 的配置示例



过程

步骤 1 创建虚拟路由器 - 包含 *Inside1*、*Outside1* 和 *Outside2* 接口的 *R4*：

图 ***124:*** 配置 ***R4*** 虚拟路由器



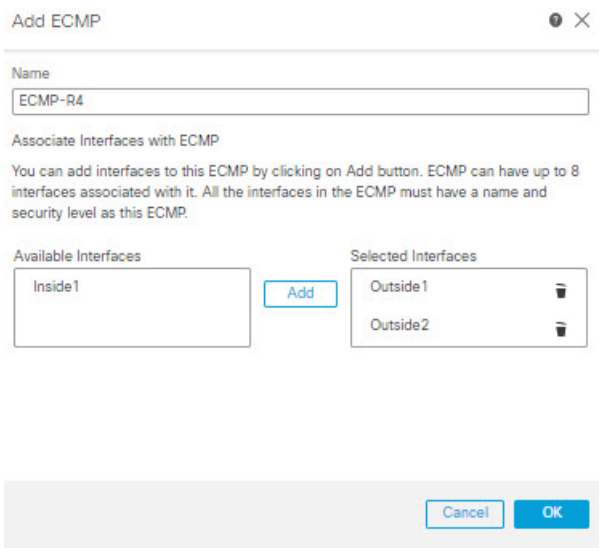
步骤 2 创建 ECMP 区域：

a) 在**路由 (Routing)** 选项卡中，选择 R4 用户定义的虚拟路由器，然后点击 **ECMP**。

b) 点击**添加 (Add)**。

c) 输入 ECMP 名称，然后从**可用接口 (Available Interfaces)** 列表中选择 *Outside1* 和 *Outside2*：

图 ***125:*** 创建 ***ECMP*** 区域



d) 点击**确定 (Ok)**，然后点击**保存 (Save)**。

步骤 3 为区域接口创建静态路由：

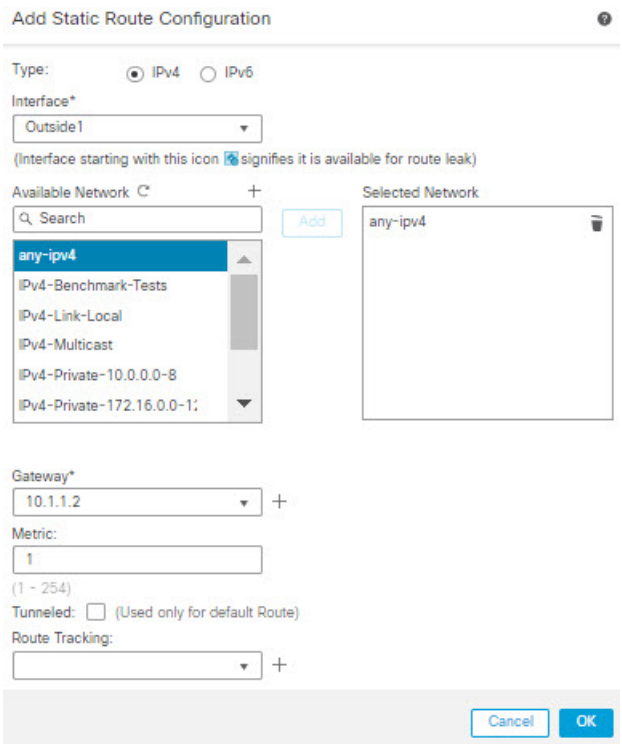
a) 在**路由 (Routing)** 选项卡中，点击**静态路由 (Static Route)**。

b) 在**接口 (Interface)** 下拉列表中，选择 Outside1。

c) 在**可用网络 (Available Network)** 下，选择 any-ipv4，然后点击**添加 (Add)**。

d) 在网关 **(Gateway)** 字段 10.1.1.2 中指定下一跳地址：

图 ***126:*** 为 ***Outside1*** 配置静态路由



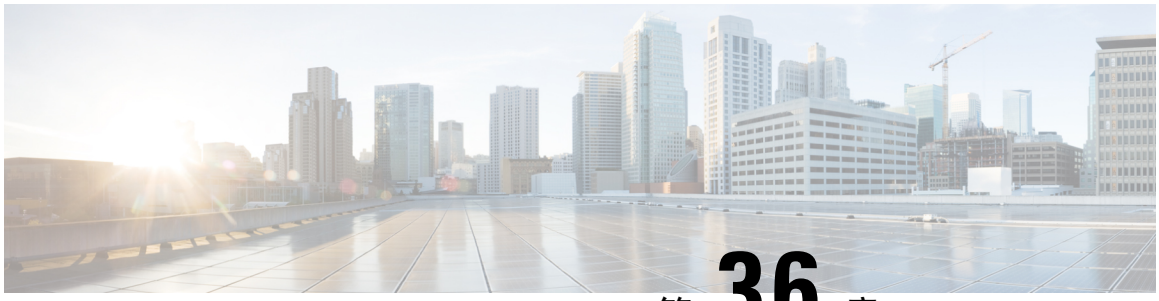
e) 为 Outside2 配置静态路由，重复步骤 3b 到步骤 3d。

确保为静态路由指定相同的指标，但要使用不同的网关：

图 ***127:*** 已配置的 ***ECMP*** 区域接口静态路由

步骤 4 保存 **(Save)** 和部署 **(Deploy)**。

根据 ECMP 算法，到达目的地 R3 的网络数据包会遵循 R4>R1>R3 或 R4>R2>R3。如果 R1>R3 路由丢失，流量将流经 R2，而不会丢弃任何数据包。类似地，虽然数据包是从 *outside1* 发送的，但来自 R3 的响应可被 *outside2* 接收。此外，当网络流量很大时，R4 会在两条路由之间分配流量，从而均衡负载。



第 36 章

OSPF

本章介绍如何将威胁防御配置为使用开放式最短路径优先 (OSPF) 路由协议来路由数据、执行身份验证以及重新分发路由信息。

OSPF

本章介绍如何将威胁防御配置为使用开放式最短路径优先 (OSPF) 路由协议来路由数据、执行身份验证以及重新分发路由信息。

关于 OSPF

OSPF 是一种使用链路状态而非距离矢量进行路径选择的内部网关路由协议。OSPF 传播链路状态通告而非路由表更新。由于仅交换 LSA 而不是整个路由表，因此 OSPF 网络比 RIP 网络更快收敛。

OSPF 使用链路状态算法构建和计算所有到达已知目标的最短路径。OSPF 区域中的每台路由器包含相同的链路状态数据库，该数据库是由每台路由器可使用的接口和可到达的邻居组成的列表。

相比 RIP，OSPF 具有以下优点：

- OSPF 链路状态数据库更新的发送频率低于 RIP 更新，并且随着过时信息的超时，链路状态数据库即时而非逐步更新。
- 路由决策基于开销，它表明通过特定接口发送数据包所需的开销。威胁防御设备 根据链路带宽而非到目标的跃点数计算接口的开销。可以配置开销来指定首选路径。

最短路径优先算法的缺点是需要大量 CPU 周期和内存。

威胁防御设备 可以在不同接口集上同时运行 OSPF 协议的两个进程。如果您具有使用相同 IP 地址的接口（NAT 允许这些接口共存，但是 OSPF 不允许重叠地址），则可能要运行两个进程。或者，可

能要在内部运行一个进程，在外部运行另一个进程，并且在两个进程之间重新分发路由的子集。同样，可能需要将专用地址与公用地址分离。

您可以将路由从一个 OSPF 路由进程、RIP 路由进程或从在启用了 OSPF 的接口上配置的静态路由和已连接路由重新分发到另一个 OSPF 路由进程中。

威胁防御设备 支持以下 OSPF 功能：

- 区域内、区域间和外部（I 类和 II 类）路由。
- 虚拟链路。
- LSA 泛洪。
- OSPF 数据包身份验证（密码和 MD5 身份验证）。
- 将 威胁防御设备 配置为指定路由器或指定备用路由器。威胁防御设备 也可以设置为 ABR。
- 末节区域和次末节区域。
- 区域边界路由器 3 类 LSA 筛选。

OSPF 支持 MD5 和明文邻居身份验证。如有可能，应将身份验证与所有路由协议配合使用，因为在 OSPF 和其他协议（如 RIP）之间的路由重新分发可能会被攻击者用于破坏路由信息。

如果使用 NAT，如果 OSPF 是在公共和专用区域上运行，并且如果要求地址过滤，则需要运行两个 OSPF 进程，一个进程对应于公共区域，一个进程对应于专用区域。

在多个区域中具有接口的路由器称为区域边界路由器 (ABR)。充当网关以在使用 OSPF 的路由器与使用其他路由协议的路由器之间重新分发流量的路由器称为自治系统边界路由器 (ASBR)。

ABR 使用 LSA 将有关可用路由的信息发送到其他 OSPF 路由器。使用 ABR 3 类 LSA 筛选，您可以具有单独的以 ASA 作为 ABR 的专用和公共区域。3 类 LSA（区域间路由）可以从一个区域筛选到另一个区域，从而允许您在不通告专用网络即的情况下配合使用 NAT 和 OSPF。

注释 只能筛选 3 类 LSA。如果在专用网络中将 威胁防御设备 配置为 ASBR，它将发送描述专用网络的 5 类 LSA，后者会泛洪至整个 AS，包括公共区域。

如果采用 NAT 但 OSPF 仅在公共区域中运行，则可以在专用网络内将到公共网络的路由作为默认或 5 类 AS 外部 LSA 重新分发。但是，需要为受 威胁防御设备 保护的专用网络配置静态路由。此外，不应在同一 威胁防御设备 接口上混用公用和专用网络。

您可以同时在 威胁防御设备 上运行两个 OSPF 路由进程、一个 RIP 路由进程和一个 EIGRP 路由进程。

快速呼叫数据包 OSPF 支持

OSPF 快速呼叫数据包支持功能提供了一种以短于一秒的间隔发送呼叫数据包的配置方式。此类配置在开放式最短路径优先 (OSPF) 网络中会导致更快的收敛。

OSPF 支持快速呼叫数据包的必备条件

OSPF 必须已在网络中进行配置或与快速呼叫数据包 OSPF 支持功能同时配置。

OSPF 呼叫间隔和停顿间隔

OSPF 呼叫数据包是 OSPF 进程向其 OSPF 邻居发送以保持与这些邻居的连接的数据包。呼叫数据包按照可配置间隔（以秒为单位）进行发送。对于以太网链路，默认值为10秒；对于非广播链路，默认值为30秒。呼叫数据包包含在停顿间隔内为其接收到呼叫数据包的所有邻居的列表。停顿间隔也是可配置间隔（以秒为单位），并且默认为呼叫间隔值的四倍。所有呼叫间隔的值在网络中都必须相同。同样，所有停顿间隔的值在网络中也必须都相同。

这两种间隔通过表明链路可运行来结合用于保持连接。如果路由器在停顿间隔内没有从邻居接收到呼叫数据包，则将声明该邻居关闭。

OSPF 快速呼叫数据包

OSPF快速呼叫数据包是指按照小于1秒的间隔发送的呼叫数据包。要了解快速呼叫数据包，您应已了解 OSPF 呼叫数据包与停顿间隔之间的关系。请参阅 OSPF 呼叫间隔和停顿间隔，第 865 页。

通过使用 ospf dead-interval 命令来获取 OSPF 快速呼叫数据包。停顿间隔设置为 1 秒，并且 hello-multiplier 值设置为在该1秒期间要发送的呼叫数据包的数量，从而提供亚秒或“快速”呼叫数据包。

当在接口上配置了快速呼叫数据包时，此接口发出的呼叫数据包中通告的呼叫间隔设置为 0。系统将忽略通过此接口接收到的呼叫数据包中的呼叫间隔。

无论停顿间隔设置为1秒（对于快速呼叫数据包）还是设置为任何其他值，它在分片上都必须一致。只要在停顿间隔内发送了至少一个呼叫数据包，呼叫乘数对于整个分片便无需相同。

OSPF 快速呼叫数据包的优势

OSPF快速呼叫数据包功能的优势是OSPF网络将比没有快速呼叫数据包的情况更快收敛。通过此功能，您可以在 1 秒内检测丢失的邻居。它在开放式系统互连 (OSI) 物理层和数据链路层可能未检测到邻居丢失的 LAN 分片中尤其有用。

OSPFv2 与 OSPFv3 之间的实施差异

OSPFv3 不向后兼容 OSPFv2。要使用 OSPF 路由 IPv4 和 IPv6 流量，必须同时运行 OSPFv2 和 OSPFv3。它们会共存但不相互交互。

OSPFv3 提供的其他功能包括：

- 按链路进行协议处理。
- 删除寻址语义。
- 添加泛洪范围。
- 支持每条链路多个实例。

- 使用 IPv6 链路本地地址执行网络发现和其他功能。
- 以前缀和前缀长度表示 LSA。
- 添加两种 LSA 类型。
- 处理未知 LSA 类型。
- 使用 OSPFv3 路由协议流量的 IPsec ESP 标准支持身份验证，如 RFC-4552 所指定。

OSPF 的要求和必备条件

型号支持

威胁防御

Threat Defense Virtual

支持的域

任意

用户角色

管理员

网络管理员

OSPF 指南

防火墙模式准则

OSPF 仅支持路由防火墙模式。OSPF 不支持透明防火墙模式。

高可用性 指南

OSPFv2 和 OSPFv3 支持状态 高可用性。

IPv6 准则

- OSPFv2 不支持 IPv6。
- OSPFv3 支持 IPv6。
- OSPFv3 使用 IPv6 进行身份验证。
- 威胁防御设备 将 OSPFv3 路由安装到 IPv6 RIB 中，前提是它是最佳路由。

OSPFv3 Hello 数据包和 GRE

通常，OSPF流量不会通过 GRE 隧道。当 IPv6 上的 OSPFv3 封装在 GRE 内时，安全检查（例如组播目标）的IPv6报头验证失败。由于隐式安全检查验证，数据包被丢弃，因为此数据包具有目标 IPv6 组播。

您可以定义预过滤器规则来绕过GRE流量。但是，使用预过滤器规则，检测引擎不会询问内部数据包。

集群准则

- 不支持 OSPFv3 加密。如果尝试在集群环境中配置 OSPFv3 加密，系统将显示错误消息。
- 在跨接口模式下，仅管理接口上不支持动态路由。
- 当集群中的控制角色发生变化时，会发生以下行为：
  - 在跨接口模式中，路由器进程仅在控制单元上处于活动状态，在数据单元上处于暂停状态。各集群设备具有同一路由器 ID，因为已从控制单元对配置进行同步。因此，在角色更改过程中，相邻路由器不会注意到集群的路由器 ID 发生的任何更改。

多协议标签交换 (MPLS) 和 OSPF 指南

如果 MPLS 配置的路由器发送的链路状态 (LS) 更新数据包包含不透明 Type-10 链路状态通告 (LSA)，而且其中包括 MPLS 报头，则身份验证会失败且设备会自动丢弃更新数据包，而不是确认它们。最终，对等路由器将终止邻居关系，因为它没有收到任何确认。

确保在设备上禁用了不间断转发 (NSF)，以确保邻居关系保持稳定：

- 导航到 管理中心 中的**不间断转发 (Non Stop Forwarding)** 页面（“设备”(Devices) > “设备管理”(Device Management) [选择所需的设备] > “路由”(Routing) > OSPF > “高级”(Advanced) > 不间断转发 (Non Stop Forwarding)）。

  确保未选中“**不间断转发功能**”复选框。

路由重分布指南

不支持在 OSPFv2 或 OSPFv3 上重新分发具有 IPv4 或 IPv6 前缀列表的路由映射。使用 OSPF 上的连接路由进行重新分发。

其他准则

- OSPFv2 和 OSPFv3 在接口上支持多个实例。
- OSPFv3 在非集群环境中通过 ESP 报头支持加密。
- OSPFv3 支持非负载加密。
- OSPFv2 根据 RFC 4811、4812 和 3623 定义分别支持思科 NSF 平稳重启和 IETF NSF 平稳重启机制。
- OSPFv3 根据 RFC 5187 定义支持平稳重启机制。

- 可分发的区域内（类型 1）路由数具有限制。对于这些路由，单一 1 类 LSA 包含所有前缀。由于系统的数据包大小限制为 35 KB，所以 3000 个路由会导致数据包超出该限制。考虑设置 2900 个 1 类路由作为支持的最大数量。
- 对于使用虚拟路由的设备，可以为全局虚拟路由器配置 OSPFv2 和 OSPFv3。但是，只能为用户定义的虚拟路由器配置 OSPFv2。
- 要避免在路由更新大于链路上的最小 MTU 时丢弃由于路由更新而导致的邻接摆动，请确保在链路两端的接口上配置相同的 MTU。

配置 OSPFv2

本节介绍配置 OSPFv2 路由进程所涉及的任务。对于使用虚拟路由的设备，可以为用户定义的虚拟路由器配置 OSPFv2。

配置 OSPF 区域、范围和虚拟链路

可以配置多个 OSPF 区域参数，包括设置身份验证、定义末节区域以及将特定成本分配给默认摘要路由。您最多可以启用两个 OSPF 进程实例。每个 OSPF 进程具有其自己的关联区域和网络。身份验证提供基于密码的区域非授权访问防御。

末节区域是有关外部路由的信息未发送到的区域。相反，ABR 生成了到自治系统外部目标的末节区域中的默认外部路由。要利用 OSPF 末节区域支持，必须在末节区域中使用默认路由。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF**。

步骤 5 选择**进程 1**。对于每个 context/virtual router，最多可以启用两个 OSPF 进程实例。您必须选择 OSPF 进程才能配置区域参数。

如果设备使用的是虚拟路由，则 ID 字段会显示为所选虚拟路由器生成的唯一进程 ID。

步骤 6 从下拉列表中选择 OSPF 角色，然后在下一字段中为其输入说明。这些选项是“内部”、“ABR”、“ASBR”和“ABR 和 ASBR”。有关 OSPF 角色的说明，请参阅关于 OSPF，第 863 页。

步骤 7 选择**区域 (Area)** > **添加 (Add)**。

您可以点击 **编辑**（ ），或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 8 为每个 OSPF 进程配置以下区域选项：

- **OSPF 进程 (OSPF Process)**- 选择进程 ID。对于使用虚拟路由的设备，下拉列表会列出为所选虚拟路由器生成的唯一进程 ID。

- **区域 ID** - 要汇总其路由的区域的资格。
- **区域类型** - 选择以下选项之一：
  - **普通 (Normal)** -（默认）标准 OSPF 区域。
  - **末节** - 末节区域之外没有任何路由器或区域。末节区域防止自制系统 (AS) 外部 LSA（5 类 LSA）泛洪至末节区域中。创建末节区域时，可以通过取消选中**摘要末节**复选框来防止摘要 LSA（3 类和 4 类）泛洪至该区域中。
  - **NSSA** - 使该区域成为次末节区域 (NSSA)。NSSA 接受 7 类 LSA。您也可以通过取消选中**重新分发**复选框并选中**默认信息来源**复选框来禁用路由重新分发。可以通过取消选中**摘要 NSSA** 复选框来防止摘要 LSA 泛洪至该区域中。
- **指标值** - 用于生成默认路由的指标。默认值为 10。有效十进制值范围为 0 至 16777214。
- **指标类型 (Metric Type)** - 指标类型是与通告到 OSPF 路由域中的默认路由关联的外部链路类型。可用选项为 1（表示 1 类外部路由）或 2（表示 2 类外部路由）。
- **可用网络** - 选择可用网络之一并点击**添加**，或点击 **添加**（+）以添加新网络对象。有关添加网络的过程，请参阅网络，第 997 页。
- **身份验证** - 选择 OSPF 身份验证：
  - **无** -（默认）禁用 OSPF 区域身份验证。
  - **密码** - 为区域身份验证提供明文密码，在需要考虑安全性的情景下，建议不要选择此选项。
  - **MD5** - 允许 MD5 身份验证。
- **默认成本** - OSPF 区域的默认开成本，用于确定到目标的最短路径。有效值范围为 0 至 65535。默认值为 1。

步骤 9 点击**确定**以保存区域配置。

步骤 10 选择**范围 (Range)** > **添加 (Add)**。

- 选择可用网络之一，以及是否进行通告，或者，
- 点击 **添加**（+）以添加新网络对象。有关添加网络的过程，请参阅网络，第 997 页。

步骤 11 点击**确定**以保存范围配置。

步骤 12 选择**虚拟链路 (Virtual Link)**，点击**添加 (Add)**，并为每个 OSPF 进程配置以下选项：

- **对等体路由器** - 选择对等体路由器的 IP 地址。要添加新的对等体路由器，请点击 **添加**（+）。有关添加网络的过程，请参阅网络，第 997 页。
- **呼叫间隔** - 在接口上发送的呼叫数据包的间隔时间（以秒为单位）。呼叫数据包间隔是将在呼叫数据包中通告的无符号整数。该值对特定网络上的所有路由器和访问服务器必须相同。有效值范围为 1 至 65535。默认值为 10。

  呼叫间隔越小，检测到拓扑更改的速度越快，但会在接口上发送更多流量。

- **传送延迟** - 在接口上发送 LSA 数据包所需的估计时间（以秒为单位）。整数值必须大于零。有效值范围为 1 至 8192。默认值为 1。

  更新数据包中的 LSA 在传输之前会按此数量递增其自己的年龄。如果在通过链路进行传输之前未添加延迟，则不考虑 LSA 通过该链路进行传播的时间。分配的值应将接口的传输和传播延迟考虑在内。此设置对于超低速链路意义更大。

- **重新传送间隔** - 属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）：重新传输间隔是连接的网络上任意两个路由器之间的预期往返延迟。该值必须大于预期往返延迟，并且范围可以为 1 至 65535。默认值为 5。

  当一台路由器向其邻居发送 LSA 时，它将保留该 LSA，直至收到确认消息。如果路由器没有接收到确认，则重新发送 LSA。请保守地设置此值，否则可能会产生不必要的重新传输。串行线路和虚拟链路的值应较大。

- **停顿间隔** - 在邻居指示路由器关闭之前呼叫数据包不可见的时间（以秒为单位）。停顿间隔是无符号整数。默认值是呼叫间隔的四倍（或 40 秒）。对于连接到公用网络的所有路由器和接入服务器，值必须相同。有效值范围为 0 至 65535。

- **身份验证** - 从以下选项中选择 OSPF 虚拟链路身份验证：

  - **无** -（默认）禁用虚拟链路区域身份验证。
  - **区域身份验证** - 使用 MD5 启用区域身份验证。点击**添加 (Add)** 按钮，输入密钥 ID、密钥、确认密钥，然后点击**确定 (OK)**。
  - **密码** - 为虚拟链路身份验证提供明文密码，在需要考虑安全性的情景下，建议不要选择此选项。
  - **MD5** - 允许 MD5 身份验证。点击**添加 (Add)** 按钮，输入密钥 ID、密钥、确认密钥，然后点击**确定 (OK)**。

    注释 确保仅输入数字作为 MD5 密钥 ID。

  - **密钥链** - 允许密钥链身份验证。点击**添加 (Add)** 并创建的密钥链，然后点击**保存 (Save)**。有关详细操作步骤，请参阅创建密钥链对象，第 996 页。为对等体使用相同的身份验证类型（MD5 或密钥链）和密钥 ID 以建立成功的邻接关系。

步骤 13 点击**确定**以保存虚拟链路配置。

步骤 14 点击“路由”页面上的**保存**以保存更改。

下一步做什么

继续配置 OSPF 重新分发。

配置 OSPF 重新分发

威胁防御设备可以控制路由在 OSPF 路由过程之间的重新分发。将路由从一个路由过程重新分发到 OSPF 路由过程的规则将会显示。可以将 RIP 和 BGP 发现的路由重新分发到 OSPF 路由过程中。还可以将静态路由和已连接路由重新分发到 OSPF 路由过程中。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF**。

步骤 5 选择**重新分配 (Redistribution)** > **添加 (Add)**。

您可以点击 **编辑**（ ），或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 6 为每个 OSPF 进程配置以下重新分发选项：

- **OSPF 进程 (OSPF Process)**- 选择进程 ID。对于使用虚拟路由的设备，该下拉列表会显示为所选虚拟路由器生成的唯一进程 ID。
- **路由类型** - 选择下列类型之一：
  - **静态** - 将静态路由重新分发到 OSPF 路由过程。
  - **已连接** - 将已连接路由（通过在接口上启用 IP 地址自动建立的路由）重新分发到 OSPF 路由过程。已连接路由会作为设备的外部路由重新分发。您可以在“可选”列表下选择是否使用子网。
  - **OSPF** - 重新分发来自另一个 OSPF 路由过程（例如内部、外部 1 和 2、NSSA 外部 1 和 2）的路由，或选择是否使用子网。您可以在“可选”列表下选择以下选项。
  - **BGP** - 重新分发来自 BGP 路由过程的路由。添加 AS 编号以及选择是否使用子网。
  - **RIP** - 重新分发来自 RIP 路由过程的路由。您可以在“可选”列表下选择是否使用子网。

    注释 由于用户定义的虚拟路由器不支持 RIP，因此您无法从 RIP 重新分发路由。

- **指标值** - 正在分发的路由的指标值。默认值为 10。有效值范围为 0 到 16777214。

  在同一设备上从一个 OSPF 进程重新分发到另一个 OSPF 进程时，如果未指定指标值，则会将指标从一个进程携带至另一个进程。将其他进程重新分发到OSPF进程时，如果未指定指标值，则默认指标为 20。
- **指标类型 (Metric Type)** - 指标类型是与通告到OSPF路由域中的默认路由关联的外部链路类型。可用选项为 1（表示 1 类外部路由）或 2（表示 2 类外部路由）。

- **标签值** - 标签指定附加到 OSPF 本身未使用但可用于在 ASBR 之间传达信息的各外部路由的 32 位十进制值。如果未指定任何内容，则对来自 BGP 和 EGP 的路由使用远程自治系统编号。对于其他协议，将会使用零。有效值为 0 到 4294967295。
- **路由映射** - 检查对于从源路由协议到当前路由协议的路由导入的过滤。如果未指定此参数，则会重新分发所有路由。如果已指定此参数，但未列出路由映射标签，则不会导入任何路由。也可以通过点击 **添加**（+） 来添加新的路由映射。请参阅路由映射以添加新的路由映射。

步骤 7 点击**确定**以保存重新分发配置。

步骤 8 点击“路由”页上的 **保存**以保存更改。

下一步做什么

继续执行配置 OSPF 区域间过滤， 第 872 页。

配置 OSPF 区域间过滤

ABR 类型 3 LSA 过滤扩展了 ABR 的功能，即在不同 OSPF 区域之间运行 OSPF 过滤类型 3 LSA。配置前缀列表后，便会仅将指定的前缀从一个 OSPF 区域发送到另一个 OSPF 区域。所有其他前缀都限用于各自的 OSPF 区域。可以向传入或传出 OSPF 区域的流量或者同时为该区域的传入和传出流量应用此类型的区域过滤。

当前缀列表的多个条目与给定前缀相匹配时，将使用具有最低序列号的条目。为提高效率，可能需要手动为最常用的匹配或拒绝项分配较低的序列号来将其置于列表顶部附近。默认情况下，序列号从 5 开始并以 5 为增量自动生成。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF**。

步骤 5 选择**区域间 (InterArea)** > **添加 (Add)**。

您可以点击 **编辑**（✎），或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域间。

步骤 6 为每个 OSPF 进程配置下列区域间过滤选项：

- **OSPF 进程 (OSPF Process)**- 对于使用虚拟路由的设备，下拉列表会列出为所选虚拟路由器生成的唯一进程 ID。
- **区域 ID** - 要汇总其路由的区域。
- **前缀列表** - 前缀的名称。要添加新的前缀列表对象，请参阅步骤 5。

- **流量方向** - 入站或出站。选择 Inbound 以筛选传入 OSPF 区域的 LSA，或者选择 Outbound 以筛选传出 OSPF 区域的 LSA。如果编辑的是现有过滤器条目，则无法修改此设置。

步骤 7 点击 **添加**（+），然后输入新前缀列表的名称，以及是否允许重写。

配置前缀规则之前，必须先配置前缀列表。

步骤 8 点击**添加**以配置前缀规则，并配置以下参数：

- **操作** - 针对重新分发访问，选择**阻止**或**允许**。
- **序列号** - 路由序列号。默认情况下，序列号从 5 开始并以 5 为增量自动生成。
- **IP 地址** - 以 IP 地址/掩码长度格式指定前缀数字。
- **最小前缀长度** -（可选）最小前缀长度。
- **最大前缀长度** -（可选）最大前缀长度。

步骤 9 点击**确定**以保存区域间过滤配置。

步骤 10 点击“路由”页上的 **保存**以保存更改。

下一步做什么

继续执行配置 OSPF 过滤规则，第 873 页。

配置 OSPF 过滤规则

您可以为每个 OSPF 进程配置 ABR 3 类 LSA 过滤器。ABR 3 类 LSA 过滤器仅允许将指定的前缀从一个区域发送到另一个区域，并会限制其他所有前缀。此类型的区域过滤可以应用在特定 OSPF 区域外、应用到特定 OSPF 区域中，或者同时在相同 OSPF 区域的内外进行应用。OSPF ABR 3 类 LSA 过滤可提高对 OSPF 区域之间路由重新分发的控制。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF**。

步骤 5 选择**过滤规则 (Filter Rule)** > **添加 (Add)**。

您可以点击 **编辑**（✎），或使用右击菜单剪切、复制、粘贴、插入和删除过滤器规则。

步骤 6 为每个 OSPF 进程配置以下过滤规则选项:

- **OSPF 进程 (OSPF Process)**- 对于使用虚拟路由的设备，下拉列表会列出为所选虚拟路由器生成的唯一进程 ID。
- **访问列表**-针对此OSPF进程的访问列表。若要添加新的标准访问列表对象，请点击 **添加**（+）并参阅配置标准 ACL 对象，第 977 页。
- **流量方向** - 为要过滤的流量方向选择 In 或 Out。选择 In 以过滤传入 OSPF 区域的 LSA，或者选择 Out 以过滤传出 OSPF 区域的 LSA。如果编辑的是现有过滤器条目，则无法修改此设置。
- **接口** - 此过滤规则的接口。

步骤 7 点击**确定**保存过滤规则配置。

步骤 8 点击“路由”页上的 **保存**以保存更改。

下一步做什么

继续执行配置 OSPF 汇总地址，第 874 页。

配置 OSPF 汇总地址

将来自其他协议的路由重新分发到 OSPF 中时，将在外部 LSA 中单独通告每个路由。但是，您可以将 威胁防御设备配置为对于为指定网络地址和掩码包含的所有重新分发的路由通告单个路由。此配置可减小 OSPF 链路状态数据库的大小。可以抑制与指定 IP 地址/掩码对相匹配的路由。标签值可用作用于通过路由映射控制重新分发的值。

可以汇总从其他路由协议获知的路由。用于通告汇总的指标是所有较为具体路由的最小指标。汇总路由帮助减小路由表的大小。

对 OSPF 使用汇总路由会导致 OSPF ASBR 将一个外部路由通告为该地址覆盖的所有重新分发的路由的聚合。只能汇总重新分发到 OSPF 中的来自其他路由协议的路由。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF**。

步骤 5 选择**摘要地址 (Summary Address)** > **添加 (Add)**。

可以点击 **编辑**（✎）进行编辑，或者使用右键点击菜单剪切、复制、粘贴、插入和删除汇总地址。

步骤 6 为每个 OSPF 进程配置以下汇总地址选项：

- **OSPF 进程 (OSPF Process)**- 对于使用虚拟路由的设备，下拉列表会列出为所选虚拟路由器生成的唯一进程 ID。

- **可用网络** - 汇总地址的 IP 地址。从“可用网络”(Address) 列表中选择一项然后点击**添加**，或者要添加新网络，请点击 **添加**（+）。有关添加网络的程序，请参阅网络，第 997 页。
- **标记** - 附加到每个外部路由的 32 位十进制值。OSPF 本身未使用此值，但是其可能用于在 ASBR 之间传达信息。
- **通告 (Advertise)** - 通告摘要路由。取消选中此复选框以抑制属于汇总地址的路由。默认情况下，此复选框为选中状态。

步骤 7 点击**确定**以保存汇总地址配置。

步骤 8 点击“路由”页上的 **保存**以保存更改。

下一步做什么

继续执行配置 OSPF 接口和邻居，第 875 页。

配置 OSPF 接口和邻居

如有必要，您可以更改某些特定于接口的 OSPFv2 参数。无需更改其中任何参数，但是以下接口参数在连接的网络中的所有路由器之间必须一致：呼叫间隔、停顿间隔和身份验证密钥。如果配置其中任何参数，请确保网络上所有路由器的配置都具有兼容值。

您需要定义静态 OSPFv2 邻居来通过点对点非广播网络通告 OSPFv2 路由。通过此功能，您可以跨现有 VPN 连接广播 OSPFv2 通告，而不必将通告封装在 GRE 隧道中。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF**。

步骤 5 选择**接口 (Interface)** > **添加 (Add)**。

您可以点击 **编辑**（✎），或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 6 为每个 OSPF 进程配置以下接口选项：

- **接口** - 要配置的接口。

  注释 如果设备使用的是虚拟路由，则此下拉列表只会显示属于路由器的接口。

- **默认成本** - 通过接口发送数据包的成本。默认值为 10。
- **优先级 (Priority)** - 确定网络的指定路由器。有效值范围为 0 到 255。默认值为 1。为此设置输入 0 将使路由器不符合成为指定路由器或备用指定路由器的条件。

当两个路由器连接到网络时，两者均尝试成为指定路由器。具有更高路由器优先级的设备成为指定路由器。如果有绑定，则具有更高路由器ID的路由器成为指定路由器。此设置不适用于配置为点对点接口的接口。

- **MTU 忽略 (MTU Ignore)** - OSPF 检查邻居在公用接口上是否使用的是同一 MTU。在邻居交换 DBD 数据包时会执行此检查。如果DBD数据包中的接收MTU高于传入接口上配置的IP MTU，则不建立 OSPF 邻接。
- **数据库筛选器** - 使用此设置在同步和泛洪过程中筛选传出 LSA 接口默认情况下，OSPF 会在同一区域中的所有接口上泛洪新LSA，但LSA到达的接口除外。在全网状拓扑中，此泛洪可能会浪费带宽并产生过多的链路和 CPU 使用情况。选中此复选框可防止 OSPF 在所选接口上进行 LSA 泛洪。
- **呼叫间隔** - 用于指定在接口上发送的呼叫数据包之间的间隔（以秒为单位）。有效值的范围为 1-8192 秒。默认值为 10 秒。

  呼叫间隔越小，检测到拓扑更改的速度越快，但会在接口上发送更多流量。此值对于特定接口上的所有路由器和接入服务器都必须相同。
- **传输延迟** - 在接口上发送LSA数据包所需的估计时间（以秒为单位）。有效值的范围为1-65535秒。默认值为 1 秒。

  更新数据包中的LSA在传输之前会按此字段指定的量增大其年龄。如果在通过链路进行传输之前未添加延迟，则不考虑LSA通过该链路进行传播的时间。分配的值应将接口的传输和传播延迟考虑在内。此设置对于超低速链路意义更大。
- **重新传送间隔** - 属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）。该时间必须大于连接的网络上任意两个路由器之间的预期往返延迟。有效值的范围为 1 到 65535 秒。默认值为 5 秒。

  当一台路由器向其邻居发送LSA时，它将保留该LSA，直至收到确认消息。如果路由器没有接收到确认，则重新发送 LSA。请保守地设置此值，否则可能会产生不必要的重新传输。串行线路和虚拟链路的值应较大。
- **停顿间隔** - 在邻居表明路由器关闭之前不得查看呼叫数据包的时间段（以秒为单位）：网络上所有节点的值必须相同，范围可以是 1-65535。
- **呼叫乘数** - 指定每秒要发送的呼叫数据包的数量。有效值为 3 – 20.
- **点对点** - 允许您通过 VPN 隧道传输 OSPF 路由。
- **身份验证** - 从以下选项中选择 OSPF 接口身份验证：
  - **无** -（默认）禁用接口身份验证。
  - **区域身份验证** - 使用 MD5 启用接口身份验证。点击**添加 (Add)** 按钮，输入密钥ID、密钥、确认密钥，然后点击**确定 (OK)**。
  - **密码** - 为虚拟链路身份验证提供明文密码，在需要考虑安全性的情景下，建议不要选择此选项。
  - **MD5** - 允许 MD5 身份验证。点击**添加 (Add)** 按钮，输入密钥 ID、密钥、确认密钥，然后点击**确定 (OK)**。

注释　　确保仅输入数字作为 MD5 密钥 ID。

- **密钥链** - 允许密钥链身份验证。点击**添加 (Add)** 并创建的密钥链，然后点击**保存 (Save)**。有关详细操作步骤，请参阅创建密钥链对象，第 996 页。为对等体使用相同的身份验证类型（MD5 或密钥链）和密钥 ID 以建立成功的邻接关系。

- **输入密码** - 配置的密码，如果选择“密码”作为身份验证类型。
- **确认密码 (Confirm Password)** - 确认选择的密码。

步骤 7　选择**邻居 (Neighbor)** > **添加 (Add)**。

您可以点击 **编辑**（✎），或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 8　为每个 OSPF 进程配置以下参数：

- **OSPF 进程** - 选择1或2。
- **邻居 (Neighbor)** - 在下拉列表中选择一个邻居，或点击 **添加**（＋） 以添加新的邻居；输入名称、说明、网络、是否允许重写，然后点击**保存 (Save)**。
- **接口** - 选择与邻居关联的接口。

步骤 9　点击**确定**以保存邻居配置。

步骤 10　点击“路由”页面上的**保存**以保存更改。

配置 OSPF 高级属性

“高级属性”(Advanced Properties) 允许您配置选项，如系统日志消息生成、管理路由距离、LSA 计时器和平稳重启。

平稳重启

威胁防御设备可能会遇到一些已知的故障情况，这些故障情况不应影响跨交换平台转发的数据包。不间断转发 (NSF) 功能允许在恢复路由协议信息的同时沿已知路由继续转发数据。当有计划的无中断软件升级时，此功能非常有用。通过使用 NSF Cisco（RFC 4811 和 RFC 4812）或 NSF IETF (RFC 3623)，您可以在 OSPFv2 上配置平稳重启。

注释　NSF 功能在 HA 模式和集群中也很有用。

配置 NSF 平稳重启功能涉及两个步骤；配置功能和将设备配置为支持 NSF 功能或 NSF 感知。支持NSF 功能的设备可以向邻居表明其自己的重启活动，而支持NSF 感知的设备可以帮助重新启动邻居。

根据某些条件，可以将设备配置为支持 NSF 功能的设备或 NSF 感知的设备：

- 设备可以配置为 NSF 感知的设备，而与其所处的模式无关。

- 设备必须处于 Failover 或 Spanned Etherchannel (L2) 集群模式下才能配置为支持 NSF 功能的设备。
- 为使设备支持NSF功能或NSF感知，应将其配置为能够根据需要处理不透明链路状态通告 (LSA)/本地链路信令 (LLS) 块。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF** > **高级设置 (Advanced Settings)**。

步骤 5 选择**常规 (General)**，然后配置以下选项：

- **路由器 ID** - 为路由器 ID 选择**自动**或 **IP 地址**。如果选择 IP 地址，在“IP 地址”字段中输入 IP 地址。
- **忽略 LSA MOSPF** - 在路由收到不受支持的 LSA 类型 6 组播 OSPF (MOSPF) 数据包时，抑制系统日志消息。
- **RFC 1583 兼容** - 将 RFC 1583 兼容性配置为用于计算摘要路由成本的方法。在启用了 RFC 1583 兼容性的情况下，可能会出现路由环路。禁用它可以防止路由环路的出现。OSPF路由域中的所有 OSPF 路由器都应设置相同的 RFC 兼容性。
- **邻接更改** - 定义将导致发送系统日志消息的邻接更改。

  默认情况下，在OSPF邻居启动或关闭时会生成系统日志消息。您可以将路由器配置为在OSPF邻居关闭时发送一个系统日志消息，并为每个状态发送系统日志。

  - **日志邻接更改** - 使 威胁防御设备每当在 OSPF 邻居启动或关闭时都会发送系统日志消息。默认情况下，此设置处于选中状态。
  - **日志邻接更改详细信息** - 使 威胁防御设备每当在发生任何状态更改时都会发送系统日志消息，而不只是在邻居启动或关闭时发送。默认情况下，此设置处于未选中状态。

- **管理路由距离 (Administrative Route Distance)** - 允许您修改用于为区域间、区域内和外部 IPv6 路由配置管理路由距离的设置。管理路由距离是从 1 至 254 的整数。默认值为 110。
- **LSA 组步调设置** - 指定将 LSA 收集到组中并刷新、校验和或老化的间隔（以秒为单位）。有效值范围为 10 到 1800。默认值为 240。
- **启用默认信息来源** - 选中**启用**复选框可将默认外部路由生成到OSPF路由域中并配置以下选项：
  - **始终通告默认路由** - 确保始终通告默认路由。
  - **指标值 (Metric Value)** - 用于生成默认路由的指标。有效十进制值范围为 0 到 16777214。默认值为 10。

- **指标类型** - 与通告到 OSPFv3 路由域中的默认路由关联的外部链路类型。有效值为 1（1 类外部路由）和 2（2 类外部路由）。默认为 2 类外部路由。
- **路由映射 (RouteMap)** - 选择在路由映射符合条件时生成默认路由的路由过程，或者点击 **添加**（+） 以添加新路由。请参阅路由映射以添加新的路由映射。

步骤 6 点击**确定**以保存常规配置。

步骤 7 选择**非停止转发 (Non Stop Forwarding)**，并为支持 NSF 或识别 NSF 的设备配置 OSPFv2 的思科 NSF 平稳重启：

注释 对于 OSPFv2、思科 NSF 和 IETF NSF，存在两种平稳重启机制。一次只能为 OSPF 实例配置其中一种平稳重启机制。支持NSF 感知的设备既可以配置为思科NSF 助手，也可以配置为 IETF NSF 助手，但是一次只能在思科 NSF 或 IETF NSF 模式中为 OSPF 实例配置支持 NSF 功能的设备。

a) 选中**启用思科非停止转发功能**复选框。
b) （可选）如果需要，请选中**当检测到无法识别 NSF 的邻居设备时取消 NSF 重启**复选框。
c) （可选）确保取消选中**启用思科非停止转发助手模式**复选框，以便在识别 NSF 的设备上禁用助手模式。

步骤 8 为 OSPFv2 配置思科 IETF NSF 平稳重启（支持 NSF 功能的设备或 NSF 感知的设备）。

a) 选中**启用 IETF 非停止转发功能**复选框。
b) 在**平稳重启间隔的长度 (秒)** 字段中，以秒为单位输入重启间隔。默认值为 120 秒。对于低于 30 秒的重启间隔，将终止平稳重启。
c) （可选）确保取消选中**针对助手模式启用 IETF 非停止转发 (NSF)** 复选框，以便在识别 NSF 的设备上禁用 IETF NSF 助手模式。
d) **启用严格链路状态通告检查** - 启用后，它指示助手路由器在以下情况下将终止重新启动路由器的过程：它检测到 LSA 发生会泛洪至重新启动的路由器的更改，或者在发起平稳重启过程时重新启动的路由器的重新传输列表上有已更改的 LSA。
e) **启用 IETF 非停止转发** - 启用非停止转发，这样将允许在状态切换后恢复路由协议信息时，转发数据包以沿已知路由继续。OSPF 使用 OSPF 协议的扩展来从相邻的 OSPF 设备恢复其状态。要进行恢复，相邻的路由器必须支持 NSF 协议扩展，并愿意充当重启设备的“助手”。邻居还必须继续在进行协议状态恢复时将数据流量转发到正在重启的设备。

配置 OSPFv3

本节介绍配置 OSPFv3 路由进程所涉及的任务。对于使用虚拟路由的设备，只能为其全局虚拟路由器配置 OSPFv3，而不能为其用户定义的虚拟路由器配置 RIP。

配置 OSPFv3 区域、路由摘要和虚拟链路

要启用 OSPFv3，您需要创建 OSPFv3 路由进程，创建 OSPFv3 的区域，启用 OSPFv3 的接口，然后将路由重新分发到目标 OSPFv3 路由进程中。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **OSPFv3**。

步骤 3 默认情况下，**启用进程 1** 处于选中状态。您最多可以启用两个 OSPF 进程实例。

步骤 4 从下拉列表中选择 OSPFv3 角色，并为其输入说明。这些选项是“内部”、“ABR”、“ASBR”以及“ABR 和 ASBR”。有关 OSPFv3 角色的说明，请参阅关于 OSPF，第 863 页。

步骤 5 选择**区域 (Area)** > **添加 (Add)**。

您可以点击 **编辑**（✎），或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 6 选择**常规 (General)**，然后为每个 OSPF 进程配置以下选项：

- **区域 ID** - 要汇总其路由的区域。
- **成本** - 汇总路由的指标或开销，它在 OSPF SPF 计算过程中用于确定到达目标的最短路径。有效值范围为 0 到 16777215。
- **类型** - 指定“普通”、“NSSA”或“末节”。如果选择“普通”，则没有其他参数要配置。如果选择“末节”，则可以选择在区域中发送摘要 LSA。如果选择“NSSA”，则可以配置下面的三个选项：
  - **允许将摘要 LSA 发送到该区域** - 允许将摘要 LSA 发送到该区域。
  - **“重新分发”将路由导入到普通和 NSSA 区域** - 允许重新分发以将路由导入到正常区域，而不是末节区域。
  - **默认信息源** - 在 OSPFv3 路由域中生成默认的外部路由。
- **指标** - 用于生成默认路由的指标。默认值为 10。有效十进制值范围为 0 到 16777214。
- **指标类型** - 指标类型是与通告到 OSPFv3 路由域中的默认路由关联的外部链路类型。可用选项为 1（表示 1 类外部路由）或 2（表示 2 类外部路由）。

步骤 7 点击**确定**以保存常规配置。

步骤 8 选择**路由摘要 (Route Summary)** > **添加路由摘要 (Add Route Summary)**。

您可以点击 **编辑**（✎），或使用右键点击菜单剪切、复制、粘贴、插入和删除路由摘要。

步骤 9 为每个 OSPF 进程配置以下路由摘要选项：

- **IPv6 前缀/长度** - IPv6 前缀。要添加新的网络对象，请点击 **添加**（＋）。有关添加网络的过程，请参阅网络，第 997 页。

- **成本** - 汇总路由的指标或开销，它在 OSPF SPF 计算过程中用于确定到达目标的最短路径。有效值范围为 0 到 16777215。
- **通告** - 通告摘要路由。取消选中此复选框以抑制属于汇总地址的路由。默认情况下，此复选框为选中状态。

步骤 10 点击**确定**以保存路由摘要配置。

步骤 11 选择**虚拟链接 (Virtual Link)**，点击**添加虚拟链接 (Add Virtual Link)**，并为每个 OSPF 进程配置以下选项：

- **对等体路由器 ID (Peer RouterID)** - 选择对等体路由器的 IP 地址。要添加新的网络对象，请点击 **添加**（+）。有关添加网络的过程，请参阅网络，第 997 页。
- **TTL 安全** - 启用 TTL 安全检查。hop-count 的值是一个介于 1 到 254 之间的数字。默认值为 1。

  OSPF 发送使用 IP 报头生存时间 (TTL) 值 255 来发送传出数据包，并丢弃 TTL 值小于可配置阈值的传入数据包。由于转发 IP 数据包的每个设备都会使 TTL 递减，因此通过直接（一跳）连接接收的数据包的值为 255。跨越两跳的数据包的值为 254，以此类推。接收阈值根据数据包可能已移动的最大跳数来配置。
- **停顿间隔** - 在邻居指示路由器关闭之前呼叫数据包不可见的时间（以秒为单位）。默认值是呼叫间隔的四倍（或 40 秒）。有效值范围为 1 到 65535。

  停顿间隔是无符号整数。对于连接到公用网络的所有路由器和接入服务器，值必须相同。
- **呼叫间隔** - 在接口上发送的呼叫数据包的间隔时间（以秒为单位）。有效值范围为 1 到 65535。默认值为 10。

  呼叫数据包间隔是将在呼叫数据包中通告的无符号整数。该值对特定网络上的所有路由器和访问服务器必须相同。呼叫间隔越小，检测到拓扑更改的速度越快，但会在接口上发送更多流量。
- **重新传送间隔** - 属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）：重新传输间隔是连接的网络上任意两个路由器之间的预期往返延迟。该值必须大于预期往返延迟，并且范围可以为 1 至 65535。默认值为 5。

  当一台路由器向其邻居发送 LSA 时，它将保留该 LSA，直至收到确认消息。如果路由器没有接收到确认，则重新发送 LSA。请保守地设置此值，否则可能会产生不必要的重新传输。串行线路和虚拟链路的值应较大。
- **传送延迟** - 在接口上发送 LSA 数据包所需的估计时间（以秒为单位）。整数值必须大于零。有效值范围为 1 到 8192。默认值为 1。

  更新数据包中的 LSA 在传输之前会按此数量递增其自己的年龄。如果在通过链路进行传输之前未添加延迟，则不考虑 LSA 通过该链路进行传播的时间。分配的值应将接口的传输和传播延迟考虑在内。此设置对于超低速链路意义更大。

步骤 12 点击**确定**保存虚拟链路配置。

步骤 13 点击“路由”页面上的**保存**以保存更改。

下一步做什么

继续配置 OSPFv3 重新分发。

配置 OSPFv3 重新分发

Cisco Secure Firewall Threat Defense设备可以控制路由在 OSPF 路由过程之间的重新分发。将路由从一个路由过程重新分发到 OSPF 路由过程的规则将会显示。可以将 RIP 和 BGP 发现的路由重新分发到 OSPF 路由过程中。还可以将静态路由和已连接路由重新分发到 OSPF 路由过程中。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **OSPF**。

步骤 3 选择**重新分发 (Redistribution)** 并点击**添加 (Add)**。

您可以点击 **编辑**（ ），或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 4 为每个 OSPF 进程配置以下重新分发选项：

- **源协议** - 从中重新分发路由的源协议。支持的协议为“已连接”、“OSPF”、“静态”和“BGP”。如果选择“OSPF”，则必须在**过程 ID** 字段中输入过程 ID。如果选择“BCP”，则必须在 **AS 编号**字段中添加 AS 编号。
- **指标** - 正在分发的路由的指标值。默认值为 10。有效值范围为 0 到 16777214。

  在同一设备上从一个 OSPF 进程重新分发到另一个 OSPF 进程时，如果未指定指标值，则会将指标从一个进程携带至另一个进程。将其他进程重新分发到OSPF进程时，如果未指定指标值，则默认指标为 20。
- **指标类型 (Metric Type)** - 指标类型是与通告到OSPF路由域中的默认路由关联的外部链路类型。可用选项为 1（表示 1 类外部路由）或 2（表示 2 类外部路由）。
- **标签** - 标签指定附加到 OSPF 本身未使用但可用于在 ASBR 之间传达信息的各外部路由的 32 位十进制值。如果未指定任何内容，则对来自 BGP 和 EGP 的路由使用远程自治系统编号。对于其他协议，将会使用零。有效值为 0 到 4294967295。
- **路由映射** - 选中以过滤从源路由协议到当前路由协议的路由的导入。如果未指定此参数，则会重新分发所有路由。如果已指定此参数，但未列出路由映射标签，则不会导入任何路由。也可以通过点击 **添加**（ ）来添加新的路由映射。请参阅路由映射，第 1022 页了解添加新路由映射的过程。
- **过程 ID** - OSPF 过程 ID，即 1 或 2。

  注释 过程 ID 已启用，OSPFv3 过程正在重新分发由另一个 OSPFv3 过程获悉的路由。
- **匹配** - 启用要重新分发到其他路由域的 OSPF 路由：
  - **内部**，表示特定自治系统的内部路由。

- **外部 1**，表示自治系统的外部路由，但会作为 1 类外部路由导入 OSPFv3。
- **外部 2**，表示自治系统的外部路由，但会作为 2 类外部路由导入 OSPFv3。
- **NSSA 外部 1**，表示自治系统的外部路由，但会在 IPv6 的 NSSA 中作为 1 类外部路由导入到 OSPFv3 中。
- **NSSA 外部 2**，表示自治系统的外部路由，但会在 IPv6 的 NSSA 中作为 2 类外部路由导入到 OSPFv3 中。

步骤 5 点击**确定**以保存重新分发配置。

步骤 6 点击“路由”页上的 **保存**以保存更改。

下一步做什么

继续执行配置 OSPFv3 摘要前缀，第 883 页。

配置 OSPFv3 摘要前缀

您可以配置 威胁防御设备以通告与指定的 IPv6 前缀和掩码对匹配的路由。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **OSPFv3** 。

步骤 3 选择**摘要前缀 (Summary Prefix)** > **添加 (Add)**。

您可以点击 **编辑**（ ），或使用右键点击菜单剪切、复制、粘贴、插入和删除摘要前缀。

步骤 4 为每个 OSPF 进程配置以下摘要前缀选项：

- **IPv6 前缀/长度** - IPv6 前缀和前缀长度标签。从列表中选择一个或点击 **添加**（ ） 以添加新的网络对象。有关添加网络的过程，请参阅网络，第 997 页。
- **通告** - 通告与指定前缀/掩码对匹配的路由。取消选中此复选框以抑制与指定前缀/掩码对匹配的路由。
- （可选）**标记** - 可用作通过路由映射控制重新分发的匹配值的值。

步骤 5 点击**确定**以保存摘要前缀配置。

步骤 6 点击“路由”页上的 **保存**以保存更改。

下一步做什么

继续执行配置 OSPFv3 接口、身份验证和邻居，第 884 页。

配置 OSPFv3 接口、身份验证和邻居

如有必要，您可以更改某些特定于接口的 OSPFv3 参数。无需更改其中任何参数，但是以下接口参数在连接的网络中的所有路由器之间必须一致：hello-interval 和 dead-interval。如果配置其中任何参数，请确保网络上所有路由器的配置都具有兼容值。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **OSPFv3**。

步骤 3 选择**接口 (Interface)** > **添加 (Add)**。

您可以点击**编辑**以进行编辑，或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 4 为每个 OSPFv3 进程配置以下接口选项：

- **接口** - 正在配置的接口。
- **启用 OSPFv3** - 启用 OSPFv3。
- **OSPF 进程** - 选择 1 或 2。
- **区域** - 此进程的区域 ID。
- **实例** - 指定要分配给接口的区域实例 ID。接口只能有一个 OSPFv3 区域。您可以在多个接口上使用同一区域，并且每个接口可以使用不同的区域实例 ID。

步骤 5 选择**属性 (Properties)**，并为每个 OSPFv3 进程配置以下选项：

- **过滤传出链路状态通告** - 过滤到 OSPFv3 接口的传出 LSA。默认情况下，所有传出 LSA 都泛洪至该接口。
- **禁用 MTU 不匹配检测** - 收到 DBD 数据包后，禁用 OSPF MTU 不匹配检测。默认情况下，OSPF MTU 不匹配检测已启用。
- **泛洪减少** - 将普通 LSA 更改为“不老化”LSA，以使它们不会每 3600 秒就出现跨区域泛洪。

  OSPF LSA 每 3600 秒刷新一次。在大型 OSPF 网络中，这可能导致区域间出现大量不必要的 LSA 泛洪。
- **点对点网络** - 允许您通过 VPN 隧道传送 OSPF 路由。当接口配置为点对点非广播时，以下限制适用：
  - 只能为接口定义一个邻居。
  - 需要手动配置邻居。

- 您无需定义指向加密终端的静态路由。
- 如果通过隧道执行的 OSPF 是在接口上运行，则上游路由器的常规 OSPF 不能在同一接口上运行。
- 在指定 OSPF 邻居之前应将加密映射绑定到接口，以确保通过 VPN 隧道传递 OSPF 更新。如果在指定 OSPF 邻居之后将加密映射绑定到接口，请使用 **clear local-host all** 命令清除 OSPF 连接，以便可以通过 VPN 隧道建立 OSPF 邻接。

- **广播** - 指定接口为广播接口。默认情况下，对于以太网接口会选中此复选框。取消选中此复选框以将接口指定为点对点非广播接口。将接口指定为点对点非广播可以通过VPN隧道传输OSPF路由。
- **成本** - 指定在接口上发送数据包的成本。此设置的有效值范围为 0 至 255。默认值为 1。为此设置输入 0 将使路由器不符合成为指定路由器或备用指定路由器的条件。此设置不适用于配置为点对点非广播接口的接口。

  当两个路由器连接到网络时，两者均尝试成为指定路由器。具有更高路由器优先级的设备成为指定路由器。如果有绑定，则具有更高路由器 ID 的路由器成为指定路由器。
- **优先级** - 确定为网络指定的路由器。有效值范围为 0 到 255。
- **死间隔** - 在邻居表明路由器关闭之前不得查看呼叫数据包的时间段（以秒为单位）：该值必须对于同一网络上的所有节点都相同，并且范围可以是 1 至 65535。
- **轮询间隔** - 在与邻居建立邻接关系之前，路由器将发送的 OSPF 数据包之间的时间段（以秒为单位）。路由设备检测到活动邻居，呼叫数据包间隔将从轮询间隔中指定的时间更改为呼叫间隔中指定的时间。有效值的范围为 1 到 65535 秒。
- **重新传送间隔** - 属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）。该时间必须大于连接的网络上任意两个路由器之间的预期往返延迟。有效值的范围为 1 到 65535 秒。默认值为 5 秒。
- **传送延迟** - 在接口上发送链路状态更新数据包所需的估计时间（以秒为单位）。有效值的范围为 1 到 65535 秒。默认值为 1 秒。

步骤 6 点击**确定**以保存属性配置。

步骤 7 选择**身份验证 (Authentication)**，并为每个 OSPFv3 进程配置以下选项：

- **类型** - 身份验证类型。可用选项为 Area、Interface 和 None。None 选项表示未使用身份验证。
- **安全参数索引** - 从 256 到 4294967295 的一个数字。如果选择“接口”作为类型，请配置此选项。
- **身份验证** - 身份验证算法的类型。支持的值为 SHA-1 和 MD5。如果选择“接口”作为类型，请配置此选项。
- **身份验证密钥** - 使用 MD5 身份验证时，密钥长度必须为 32 位十六进制数字（16 字节）。使用 SHA-1 身份验证时，密钥长度必须为 40 位十六进制数字（20 字节）。
- **加密身份验证密钥** - 启用身份验证密钥的加密。

- **包括加密** - 启用加密。
- **加密算法** - 加密算法的类型。支持的值为 DES。NULL 条目表示不加密。如果选择**包括加密**，请配置此选项。
- **加密密钥** - 输入加密密钥。如果选择**包括加密**，请配置此选项。
- **加密密钥** - 使密钥被加密。

步骤 8 点击**确定**以保存身份验证配置。

步骤 9 选择**邻居 (Neighbor)**，点击**添加 (Add)**，并为每个 OSPFv3 进程配置以下选项：

- **链路本地地址** - 静态邻居的 IPv6 地址。
- **成本** - 启用成本。在**成本**字段中输入成本，如果需要通告，请选中**过滤传出链路状态通告**。
- （可选）**轮询间隔** - 启用轮询间隔。以秒为单位输入**优先级**级别和**轮询间隔**。

步骤 10 点击**添加**以添加帐户。

步骤 11 点击**确定**以保存接口配置。

配置 OSPFv3 高级属性

“高级属性”(Advanced Properties) 允许您配置选项，如系统日志消息生成、管理路由距离、被动 OSPFv3 路由、LSA 计时器和平稳重启。

平稳重启

威胁防御设备可能会遇到一些已知的故障情况，这些故障情况不应影响跨交换平台转发的数据包。不间断转发 (NSF) 功能允许在恢复路由协议信息的同时沿已知路由继续转发数据。当有计划的无中断软件升级时，此功能非常有用。您可以使用 graceful-restart (RFC 5187) 在 OSPFv3 上配置平稳重启。

注释 NSF 功能在 HA 模式和集群中也很有用。

配置 NSF 平稳重启功能涉及两个步骤；配置功能和将设备配置为支持 NSF 功能或 NSF 感知。支持NSF功能的设备可以向邻居表明其自己的重启活动，而支持NSF感知的设备可以帮助重新启动邻居。

根据某些条件，可以将设备配置为支持 NSF 功能的设备或 NSF 感知的设备：

- 设备可以配置为 NSF 感知的设备，而与其所处的模式无关。
- 设备必须处于 Failover 或 Spanned Etherchannel (L2) 集群模式下才能配置为支持 NSF 功能的设备。

- 为使设备支持NSF功能或NSF感知，应将其配置为能够根据需要处理不透明链路状态通告(LSA)/本地链路信令 (LLS) 块。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由 (Routing)** > **OSPFv3** > **高级 (Advanced)**。

步骤 3 对于**路由器 ID**，请选择**自动**或 **IP 地址**。如果选择 IP 地址，在“IP 地址”字段中输入 IP 地址。

步骤 4 如果您希望在路由收到不受支持的 LSA 类型 6 组播 OSPF (MOSPF) 数据包时抑制系统日志消息，请选中**忽略 LSA MOSPF** 复选框。

步骤 5 选择**常规 (General)**，然后配置以下选项：

- **邻接更改** - 定义将导致发送系统日志消息的邻接更改。

  默认情况下，在OSPF邻居启动或关闭时会生成系统日志消息。您可以将路由器配置为在OSPF邻居关闭时发送一个系统日志消息，并为每个状态发送系统日志。

  - **邻接更改** - 使 威胁防御设备每当在 OSPF 邻居启动或关闭时都会发送系统日志消息。默认情况下，此设置处于选中状态。
  - **包括详细信息** - 使 威胁防御设备每当在发生任何状态更改时都会发送系统日志消息，而不只是在邻居启动或关闭时发送。默认情况下，此设置处于未选中状态。

- **管理路由距离** - 允许您修改用于为区域间、区域内和外部 IPv6 路由配置管理路由距离的设置。管理路由距离是从 1 至 254 的整数。默认值为 110。
- **默认信息来源** - 选中**启用**复选框可将默认外部路由生成到 OSPFv3 路由域中并配置以下选项：
  - **始终通告** - 将会始终通告默认路由（无论其是否存在）。
  - **指标** - 用于生成默认路由的指标。有效十进制值范围为 0 到 16777214。默认值为 10。
  - **指标类型** - 与通告到 OSPFv3 路由域中的默认路由关联的外部链路类型。有效值为 1（1 类外部路由）和 2（2 类外部路由）。默认为 2 类外部路由。
  - **路由地图 (Route Map)** - 选择在路由映射符合条件时生成默认路由的路由过程，或者点击**添加**（+） 以添加新路由。请参阅路由映射 ， 第 1022 页以添加路由映射。

步骤 6 点击**确定**以保存常规配置。

步骤 7 选择**被动接口 (Passive Interface)**，从“可用接口”(Available Interfaces) 列表中选择要在其上启用被动 OSPFv3 路由的接口，然后点击**添加 (Add)** 将它们移动到“选定的接口”(Selected Interfaces) 列表中。

备用路由帮助控制 OSPFv3 路由信息的通告并禁用在接口上发送和接收 OSPFv3 路由更新。

步骤 8 点击**确定**以保存被动接口配置。

步骤 9 选择**计时器 (Timer)**，并配置以下 LSA 步调设置和 SPF 计算计时器：

- **到达** - 指定前后两次接受从邻居到达的同一 LSA 之间必须经过的最小延迟（以毫秒为单位）。范围是从 0 到 6000,000 毫秒。默认值为 1000 毫秒。
- **泛洪步调设置** - 指定泛洪队列中的 LSA 在两次更新之间定步的时间（以毫秒为单位）。可配置范围是从 5 到 100 毫秒。默认值为 33 毫秒。
- **组步调设置** - 指定将 LSA 收集到组中并刷新、校验和或老化的间隔（以秒为单位）。有效值范围为 10 到 1800。默认值为 240。
- **重新传输步调设置** - 指定重新传输队列中 LSA 设置步调的间隔时间（以毫秒为单位）。可配置范围是从 5 到 200 毫秒。默认值为 66 毫秒。
- **LSA 调速** - 指定生成第一次出现的 LSA 时的延迟（以毫秒为单位）。默认值为 0 毫秒。最小值指定发起同一 LSA 所需的最小延迟（以毫秒为单位）。默认值为 5000 毫秒。最大值指定发起同一 LSA 所需的最大延迟（以毫秒为单位）。默认值为 5000 毫秒。

  注释　对于 LSA 调速，如果最短或最长时间小于第一次出现的值，则 OSPFv3 会自动更正为第一次出现的值。同样，如果指定的最大延迟小于最小延迟，则 OSPFv3 会自动更正为最小延迟值。

- **SPF 调速** - 指定接收对 SPF 计算的更改所需的延迟（以毫秒为单位）。默认值为 5000 毫秒。最小值指定第一次和第二次 SPF 计算之间的延迟（以毫秒为单位）。默认值为 10000 毫秒。最大值指定 SPF 计算的最长等待时间（以毫秒为单位）。默认值为 10000 毫秒。

  注释　对于 SPF 调速，如果最短或最长时间小于第一次出现的值，则 OSPFv3 会自动更正为第一次出现的值。同样，如果指定的最大延迟小于最小延迟，则 OSPFv3 会自动更正为最小延迟值。

步骤 10　点击**确定**以保存 LSA 计时器配置。

步骤 11　选中**非停止转发 (Non Stop Forwarding)**，并选中**启用稳定重启助手 (Enable graceful-restart helper)** 复选框。默认情况下，此复选框处于选中状态。取消选中此复选框将在支持 NSF 感知的设备上禁用平稳重启助手模式。

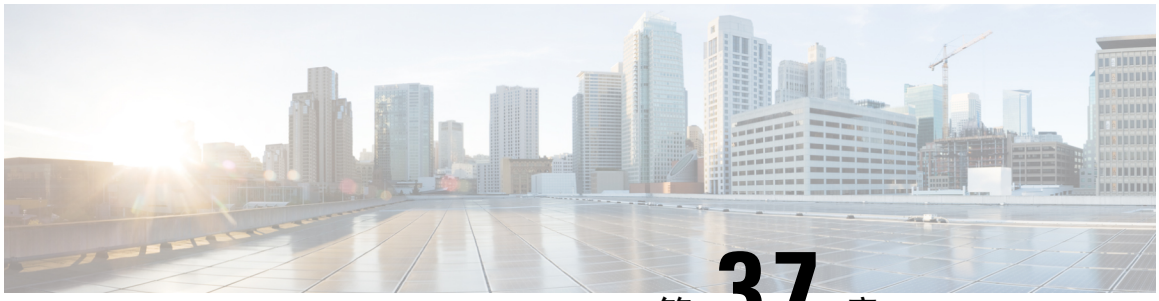
步骤 12　选中**启用链路状态通告**复选框以启用严格链路状态通告检查。

启用后，它指示助手路由器在以下情况下将终止重新启动路由器的过程：它检测到LSA 发生会泛洪至重新启动的路由器的更改，或者在发起平稳重启过程时重新启动的路由器的重新传输列表上有已更改的 LSA。

步骤 13　选中**启用稳定重启 (配置了跨区集群或故障切换时使用)**，然后以秒为单位输入稳定重启间隔。范围为 1-1800。默认值为 120 秒。对于低于 30 秒的重启间隔，将终止平稳重启。

步骤 14　点击**确定**以保存平稳重启配置。

步骤 15　点击“路由”页面上的**保存**以保存更改。



第 37 章

EIGRP

本部分介绍如何使用增强型内部网关路由协议 (EIGRP) 配置 威胁防御，以路由数据、执行身份验证以及重新分发路由信息。

关于 EIGRP 路由

思科开发的增强型内部网关路由协议 (EIGRP) 是 IGRP 的增强版本。与 IGRP 和 RIP 不同，EIGRP 不发送定期路由更新。仅在网络拓扑发生更改时才会发送 EIGRP 更新。将 EIGRP 与其他路由协议区分开来的主要功能包括快速收敛、支持可变长度子网掩码、支持部分更新以及支持多个网络层协议。

运行 EIGRP 的路由器会存储所有邻居路由表，以便可以迅速适应备用路由。如果不存在合适的路由，则EIGRP会查询其邻居以发现备用路由。这些查询会被传播直至找到备用路由为止。EIGRP对可变长度子网掩码功能的支持允许在网络边界自动汇总路由。此外，还可以将EIGRP配置为在任何接口的任何位边界汇总。

EIGRP 不会定期更新。相反，它会在路由指标发生更改时发送部分更新。部分更新的传播是自动绑定的，因此只有需要该信息的路由器才会更新。得益于这两项功能，EIGRP 与 IGRP 相比可显著减少占用的带宽。

要动态地了解直接连接网络上的其他路由器，威胁防御会使用邻居发现。EIGRP 路由器发出组播 Hello 数据包，通告其在网络中的存在状态。当 EIGRP 设备收到来自新邻居的 Hello 数据包时，会将其包含初始化位集的拓扑表发送至邻居。当邻居收到包含初始化位集的拓扑更新时，邻居将其拓扑表发回到设备。

Hello 数据包作为组播消息发出。预期不会对 Hello 消息作出响应。静态定义的邻居不在此规则的范围内。如果手动配置邻居，则 Hello 消息、路由更新和确认将作为单播消息发送。

一旦邻居关系建立后，除非网络拓扑发生更改，否则便不会交换路由更新。邻居关系通过 Hello 数据包来维护。从邻居收到的每个 Hello 数据包均包括保持时间。保持时间是威胁防御预期收到该邻

居的 Hello 数据包的时间。如果设备在保持时间内未收到由该邻居通告的 Hello 数据包，则设备会将该邻居视为不可用。

EIGRP 会使用邻居发现/恢复、可靠传输协议 (RTP) 和扩散更新算法 (DUAL) 进行路由计算。DUAL 将目标的所有路由都保存在拓扑表中，而不只是保存最低成本路由。最低成本路由会插入到路由表中。其他路由则保留在拓扑表中。如果主路由发生故障，可以从可行后继路由中选择另一个路由。后继路由是指用于进行数据包转发的具有到达目标的最低成本路径的邻居路由器。可行性计算可确保路径不是路由环路的一部分。

如果在拓扑表中找不到可行后继路由，则会重新计算路由。在路由重新计算期间，DUAL 会查询 EIGRP 邻居以获取路由。查询会被传播到连续的邻居。如果找不到可行的后继邻居，则会返回不可达消息。

在路由重新计算期间，DUAL 会将路由标记为活动状态。默认情况下，威胁防御会等待三分钟接收来自其邻居的响应。如果设备未收到来自邻居的响应，则会将路由标记为陷入主动状态。系统会删除拓扑表中作为可行性后继路由指向无响应邻居的所有路由。

EIGRP 的要求和必备条件

型号支持

威胁防御

Threat Defense Virtual

支持的域

任意

用户角色

管理员

网络管理员

EIGRP 路由的准则和限制

防火墙模式指导原则

仅支持路由防火墙模式。

设备准则

- 每台设备仅允许有一个 EIGRP 进程。
- 可以通过 威胁防御 6.6 及更高版本上的管理中心 UI 来配置 EIGRP。

接口指导原则

- 只有具有逻辑名称和 IP 地址的路由接口才能与 EIGRP 路由进程相关联。
- 只有属于全局虚拟路由器的接口才能成为 EIGRP 的一部分。EIGRP 可以在全局虚拟路由器中跨路由协议获知、过滤和重新分发路由。
- 仅支持物理、端口通道、冗余、子接口。
- VTI、BVI、VNI 和 EtherChannel 接口不能作为 EIGRP 的一部分。
- 被动接口不能被配置为邻居接口。

IP 地址和网络对象支持

- 仅支持 IPv4 地址。
- 不支持范围、FQDN 和通配符掩码。
- 仅支持标准访问列表对象。

重新分配准则

- 全局虚拟路由器中的 BGP、OSPF 和 RIP 可以重新分配到 EIGRP。
- EIGRP 可以重新分配到全局虚拟路由器中的 BGP、OSPF、RIP、静态和已连接。

部署流程准则

如果要更改已部署 EIGRP 配置的现有 AS 编号，您必须禁用 EIGRP 并进行部署。此步骤将清除威胁防御上已部署的 EIGRP 配置。接下来使用新的 AS 编号重新创建 EIGRP 配置，然后进行部署。因此，此过程可防止由于在威胁防御上部署相同的 EIGRP 配置而导致任何部署失败。

升级指南

如果您升级到版本 7.2 和更新版本具有任何 FlexConfig EIGRP 策略，则管理中心会在部署期间显示警告消息。但是，它不会停止部署过程。但在部署后，要从 UI（**设备**（**编辑**）**(Device [Edit])** > **路由 (Routing)** > **EIGRP**）管理 EIGRP 策略，则必须在 **设备**（**编辑**）**(Device [Edit])** > **路由 (Routing)** > **EIGRP** 页面中重新执行配置，并从 FlexConfig 中删除配置。为了简化该手动过程，引入了命令行迁移工具来将 EIGRP Flex 配置迁移到 EIGRP 路由策略。有关详细信息，请参阅迁移 FlexConfig 策略。

配置 EIGRP

您可以在**路由 (Routing)** 选项卡中启用和配置防火墙设备上的 EIGRP。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 点击**路由**选项卡。

步骤 3 在“全局”(Global) 下，点击 **EIGRP**.

步骤 4 选中**启用 EIGRP (Enable EIGRP)** 复选框以启用 EIGRP 路由进程。

步骤 5 在 **AS 编号**字段中，输入 EIGRP 进程的自治系统 (AS) 编号。AS 编号包含多个自主编号。AS 编号可从 1 到 65535，并且是分配的唯一值，用于在互联网上标识各个网络。

步骤 6 要配置其他 EIGRP 属性，请参阅以下主题：

1. 配置 EIGRP 设置， 第 892 页。
2. 配置 EIGRP 邻居设置， 第 893 页。
3. 配置 EIGRP 过滤器规则设置， 第 893 页。
4. 配置 EIGRP 重新分发设置， 第 894 页。
5. 配置 EIGRP 摘要地址设置， 第 895 页。
6. 配置 EIGRP 接口设置， 第 895 页。
7. 配置 EIGRP 高级设置， 第 896 页。

配置 EIGRP 设置

过程

步骤 1 在 **EIGRP** 页面上，点击**设置 (Setup)** 选项卡。

步骤 2 点击**自动汇总 (Auto Summary)** 复选框，使 EIGRP 能够汇总网络编号边界。

注释 如果存在非连续网络，启用自动汇总这可能会引起路由问题。

步骤 3 在**可用网络/主机 (Available Networks/Hosts)** 框中，点击应参与 EIGRP 路由进程的网络或主机，然后点击**添加 (Add)**。要添加新的网络对象，请点击 **添加**（+）。有关添加网络的过程，请参阅网络， 第 997 页。

步骤 4 要配置被动接口，请点击**被动接口 (Passive Interface)** 复选框。在 EIGRP 中，被动接口既不发送也不接收路由更新。

a) 要将选择性接口指定为被动接口，请点击**选定接口 (Selected Interface)** 单选按钮。在**可用接口 (Available Interfaces)** 框中，选择接口，然后点击**添加 (Add)**。

b) 要将所有接口指定为被动，点击**所有接口 (All Interfaces)** 单选按钮。

步骤 5 点击**确定 (Ok)** 和**保存 (Save)** 以保存这些设置。

配置 EIGRP 邻居设置

您可以为 EIGRP 进程定义静态邻居。在手动定义 EIGRP 邻居时，Hello 数据包会单播至该邻居。

过程

步骤 1 在 **EIGRP** 页面上，点击**邻居 (Neighbors)** 选项卡。

步骤 2 点击**添加 (Add)**。

步骤 3 从**接口 (Interface)** 下拉列表中选择可通过其访问邻居的接口。

步骤 4 从**邻居 (Neighbor)** 下拉列表中选择静态邻居的 IP 地址。要添加网络对象，请点击 **添加**（+）。有关添加网络对象的过程，请参阅网络，第 997 页。

步骤 5 点击**确定 (Ok)** 和**保存 (Save)** 以保存这些设置。

配置 EIGRP 过滤器规则设置

您可以为 EIGRP 路由进程配置路由过滤规则。过滤规则让您能够控制 EIGRP 路由进程接受或通告的路由。

过程

步骤 1 在 **EIGRP** 页面上，点击**过滤器规则 (Filter Rules)** 选项卡。

步骤 2 请点击 **添加**（+）。

步骤 3 在**添加过滤器规则 (Add Filter Rules)** 对话框中，从**过滤器方向 (Filter Direction)** 下拉列表中选择规则的方向：

- 入站 (Inbound) - 规则过滤来自传入 EIGRP 路由更新的默认路由信息。
- 出站 (Outbound) - 规则过滤来自传出 EIGRP 路由更新的默认路由信息。

步骤 4 要选择应用过滤规则的接口，请点击**接口 (Interface)** 单选按钮，然后从下拉列表中选择接口。

步骤 5 要选择应用过滤规则的协议，请点击**协议 (Protocol)** 单选按钮，然后从下拉列表中选择协议 - BGP、RIP、静态、已连接或 OSPF。对于 BGP 和 OSPF 协议，您可以指定相关的进程 ID。

步骤 6 从**访问列表 (Access List)** 下拉列表中选择访问列表。此列表定义了要在路由更新中接收的网络和要抑制的网络。若要添加新的标准访问列表对象，请点击 **添加**（+）并参阅配置标准 ACL 对象，第 977 页了解详细程序。

步骤 7 点击**确定 (Ok)** 和**保存 (Save)** 以保存这些设置。

配置 EIGRP 重新分发设置

您可以定义将来自其他路由协议的路由重新分发到 EIGRP 路由进程的规则

过程

步骤 1 在 **EIGRP** 页面上，点击**重新分配 (Redistribution)** 选项卡。

步骤 2 请点击 **添加**（＋）。

步骤 3 在**添加重新分配 (Add Redistribution)** 对话框中，从**协议 (Protocol)** 下拉列表选择要从其重新分配路由的源协议：

- BGP - 将 BGP 路由进程发现的路由重新分配给 EIGRP。
- RIP - 将 RIP 路由进程发现的路由重新分配给 EIGRP。
- 静态 - 将静态路由重新分布到 EIGRP 路由过程中。位于 network 语句范围内的静态路由会自动重新分发到 EIGRP；不需要为其定义重新分发规则。
- 已连接 - 将已连接路由（通过在接口上启用 IP 地址自动建立的路由）重新分发到 EIGRP 路由进程。位于 network 语句范围内的已连接路由会自动重新分发到 EIGRP；不需要为其定义重新分发规则。
- OSPF - 将由 OSPF 路由进程发现的路由重新分发到 EIGRP。如果选择此协议，则此对话框中的“匹配”(Match) 选项将在**可选 OSPF 重新分配 (Optional OSPF Redistribution)** 下变得可见：
  - 内部 - 特定 AS 的内部路由。
  - External1 - AS 外部的路由，会作为 1 类外部路由导入OSPF。
  - External2 - AS 外部的路由，会作为第 2 类外部路由导入所选进程。
  - Nsaa-External1 - AS 外部的路由，会作为第 1 类外部路由导入所选进程的次末节区域 (NSSA)。
  - Nsaa-External2 - AS 外部的路由，会作为第 2 类外部路由导入所选进程的 (NSSA)。

  注释　当重新分发静态、已连接、RIP 或 BGP 路由时，这些选项不可用。

步骤 4 在**可选指标 (Optional Metrics)** 下输入相关值：

- **带宽 (Bandwidth)** - 路由的最小带宽（以千比特/秒为单位）。有效值范围为 1 到 4294967295。
- **延迟时间 (Delay Time)** - 路由延迟（以十微秒为单位）。有效值范围为 0 到 4294967295。
- **可靠性 (Reliability)** - 数据包成功传输的可能性（以 0 到 255 的数字表示）。值 255 表示 100% 可靠；0 表示不可靠。

- **正在加载 (Loading)** - 路由的有效带宽。有效值范围为 1 到 255。255 表示 100% 加载。
- **MTU** - 路径的最大传输单位允许的最小值。有效值范围为 1 到 65535。

步骤 5 从**路由地图 (Route Map)** 下拉列表中选择要应用于重新分配条目的路由映射。要创建新的路由映射对象，请点击 **添加**（+）。请参阅程序的路由映射以添加新的路由映射。

步骤 6 点击**确定 (Ok)** 和**保存 (Save)** 以保存这些设置。

配置 EIGRP 摘要地址设置

您可以为每个接口配置汇总地址。如果要创建不会出现在网络边界上的汇总地址，或者要在自动路由汇总禁用的情况下在威胁防御上使用汇总地址，则需要手动定义汇总地址。如果路由表中有任何更具体的路由，则 EIGRP 会使用与所有更具体路由的最小值相等的指标来通告汇总地址。

过程

步骤 1 在 **EIGRP** 页面上，点击**汇总地址 (Summary Address)** 选项卡。

步骤 2 点击**添加 (Add)**。

步骤 3 从**接口 (Interface)** 下拉列表中，选择从其通告汇总地址的接口。

步骤 4 从**网络 (Network)** 下拉列表中，选择具有要汇总的特定 IP 地址和网络掩码的网络对象。要添加新的网络，请点击 **添加**（+）。有关添加网络的过程，请参阅网络，第 997 页。

步骤 5 在“管理距离”(Administrative Distance) 字段中，输入汇总路由的管理距离。有效值范围为 1 到 255。

步骤 6 点击**确定 (Ok)** 和**保存 (Save)** 以保存这些设置。

配置 EIGRP 接口设置

您可以在“接口”(Interfaces) 选项卡中配置接口特定的 EIGRP 路由属性。

过程

步骤 1 在 **EIGRP** 页面上，点击**接口 (Interfaces)** 选项卡。

步骤 2 请点击 **添加**（+）。

步骤 3 从**接口 (Interface)** 下拉列表中，选择要应用配置的接口的名称。

步骤 4 在**Hello 间隔 (Hello Interval)** 字段中，输入在接口上发送 EIGRP 呼叫数据包的间隔（以秒为单位）。有效值范围为 1 到 65535。默认值为 5 秒。

步骤 5 在**保持时间 (Hold Time)** 字段中，输入设备在 EIGRP Hello 数据包中进行通告的保持时间。有效值范围为 3 到 65535。默认值为 15 秒。

步骤 6 要在接口上启用 EIGRP 水平分割，请点击**水平分割 (Split Horizon)** 复选框。

步骤 7 在**延迟时间 (Delay Time)** 字段中输入延迟时间，以十微秒为单位。有效值范围为 1 至 16777215。在多情景模式下，设备不支持此选项。

步骤 8 指定身份验证属性的值：

- **启用 MD5 身份验证 (Enable MD5 Authentication)** - 点击此复选框可使用 MD5 散列算法对 EIGRP 数据包进行身份验证。
- **密钥类型 (Key Type)** - 从下拉列表中选择以下任一密钥类型：
  - “无”(None) - 表示无需身份验证。
  - “未加密”(Unencrypted) - 指示要使用的密钥字符串是用于身份验证的明文密码。
  - “已加密”(Encrypted) - 指示要使用的密钥字符串是用于身份验证的加密密码。
  - “身份验证密钥”(Auth Key) - 指示要使用的密钥字符串是 EIGRP 身份验证密钥。
- **密钥 ID (Key ID)** - 用于对 EIGRP 更新进行身份验证的密钥的 ID。输入数字密钥标识符。有效值范围为 0 到 255。
- **密钥 (Key)** - 最多包含 17 个字符的字母数字字符串。对于加密身份验证类型，此字段应至少包含 17 个字符。
- **确认密钥 (Confirm Key)** - 重新输入密钥。

步骤 9 点击**确定 (Ok)** 和**保存 (Save)** 以保存这些设置。

配置 EIGRP 高级设置

您可以配置 EIGRP 高级设置，例如路由器 ID、末节路由和邻接更改。

过程

步骤 1 在 **EIGRP** 页面上，点击**高级 (Advanced)** 选项卡。

步骤 2 在**默认路由器信息 (Default Route Information)** 下，您可以指定 EIGRP 更新中默认路由信息的发送和接收。

- **路由器 ID（IP 地址）(Router ID [IP Address])** - 输入用于标识外部路由的始发路由器的 ID。 如果收到的外部路由具有本地路由器 ID，该路由将被丢弃。要防止出现此问题，请为路由器 ID 指定全局地址。应该为每台 EIGRP 路由器配置一个唯一值。
- **接受默认路由信息 (Accept Default Route Info)** - 点击此复选框可将 EIGRP 配置为接受外部默认路由信息。

- **访问列表 (Access List)** - 从**访问列表 (Access List)** 下拉列表中，指定一个标准访问列表，该列表定义接收默认路由信息时允许的网络和不允许的网络。若要添加新的标准访问列表对象，请点击 **添加**（+） 并参阅配置标准 ACL 对象，第 977 页了解详细程序。

- **发送默认路由信息 (Send Default Route Info)** - 点击此复选框可将 EIGRP 配置为通告外部默认路由信息。
  - **访问列表 (Access List)** - 从**访问列表 (Access List)** 下拉列表中，指定一个标准访问列表，该列表定义发送默认路由信息时允许的网络和不允许的网络。若要添加新的标准访问列表对象，请点击 **添加**（+） 并参阅配置标准 ACL 对象，第 977 页了解详细程序。

步骤 3 在**管理距离 (Administrative Distance)** 下，指定：

- **内部距离 (Internal Distance)** - EIGRP 内部路由的管理距离。内部路由是从同一自主系统中的其他实体学习的路由。有效值范围为 1 到 255。默认值为 90。
- **外部距离 (External Distance)** - EIGRP 外部路由的管理距离。外部路由是为其从自主系统外部的邻居学习最佳路径的路由。有效值范围为 1 到 255。默认值为 170。

步骤 4 在**邻接更改 (Adjacency Changes)** 下，指定：

- **记录邻居更改 (Log Neighbor Changes)** - 点击此复选框可启用 EIGRP 邻居邻接更改的日志记录。
- **记录邻居警告 (Log Neighbor Warnings)** - 点击此复选框可启用 EIGRP 邻居警告消息的日志记录。
- （可选）输入重复的邻居警告消息之间的时间间隔（以秒为单位）。有效值范围为 1 到 65535。系统不会记录在此间隔期间重复出现的警告。

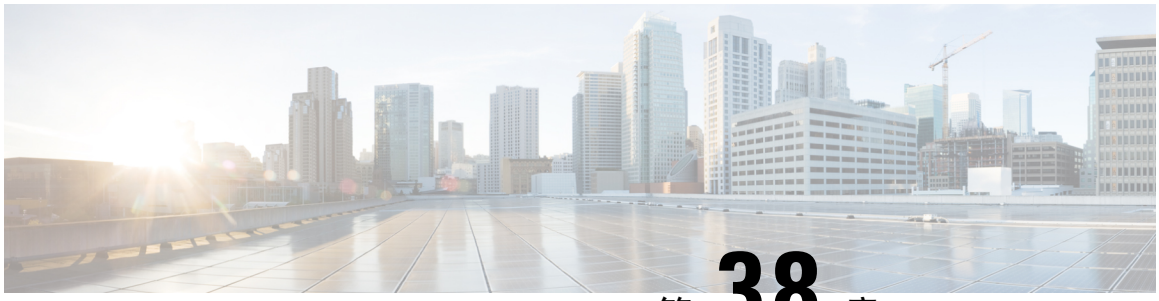
步骤 5 在**末节 (Stub)** 下，要启用设备作为 EIGRP 末节路由进程，请选中以下一个或多个 EIGRP 末节路由进程复选框：

- “仅接收”(Receive only) - 将 EIGRP 末节路由进程配置为接收来自相邻路由器的路由信息，但不向邻居发送路由信息。如果选中此选项，则不能选择任何其他末节路由选项。
- “已连接”(Connected) - 通告已连接路由。
- “已重新分发”(Redistributed) - 通告重新分发的路由。
- “静态”(Static) - 通告静态路由。
- “汇总”(Summary) - 通告汇总路由。

步骤 6 在**默认指标 (Default Metrics)** 下，定义重分布到 EIGRP 路由进程中的路由的默认指标：

- “带宽”(Bandwidth) - 路由的最小带宽（以千比特/秒为单位）。有效值范围为 1 到 4294967295。
- “延迟时间”(Delay Time) - 路由延迟（以十微秒为单位）。有效值范围为 0 到 4294967295。
- “可靠性”(Reliability) - 数据包成功传输的可能性（以 0 到 255 的数字表示）。值 255 表示 100% 可靠；0 表示不可靠。

- “正在加载”(Loading) - 路由的有效带宽。有效值范围为 1 到 255；255 表示已 100% 加载。
- MTU - 路径的最大传输单位允许的最小值，以字节表示。有效值范围为 1 到 65535。



第 38 章

BGP

本节介绍如何配置 威胁防御，以使用边界网关协议 (BGP) 来路由数据、执行身份验证以及重新分发路由信息。

关于 BGP

BGP 是一种外部和内部自主系统路由协议。自治系统是一个或一组接受共同管理并采用共同路由策略的网络。BGP 用于交换互联网的路由信息，并且是互联网运营商 (ISP) 之间所使用的协议。

路由表更改

在 BGP 邻居之间首次建立 TCP 连接时，BGP 邻居会交换完整路由信息。当检测到对路由表所做的更改时，BGP 路由器仅会向其邻居发送已更改的路由。BGP 路由器不会发送定期路由更新，并且 BGP 路由更新仅对到达目标网络的最佳路径进行通告。

注释 系统通过扫描完整的 AS 路径（在 AS_PATH 属性中指定）并检查本地系统的 AS 编号是否未出现在 AS 路径中来完成 AS 环路检测。默认情况下，EBGP 将获知的路由通告给同一对等体，以防止在执行环路检查时 ASA 上出现额外的 CPU 周期，并避免现有传出更新任务中出现延迟。

当存在多个到达某个特定目标的路由时，通过BGP获悉的路由的属性可用于确定到达该目标的最佳路径。这些属性称为 BGP 属性，可在路由选择过程中使用：

- 权重 - 这是思科定义的路由器本地属性。权重属性不会向相邻路由器进行通告。如果路由器获悉有多个到达同一目标的路由，则首选权重最高的路由。

- 本地首选项 - 本地首选项属性用于从本地 AS 中选择出口点。与权重属性不同，本地优先属性在整个本地 AS 中传播。如果有多个来自 AS 的出口点，则使用具有最高本地优先属性的出口点作为特定路由的出口点。
- 多出口鉴别器 - 多出口鉴别器 (MED) 或度量属性可用作对外部 AS 关于进入正在通告此度量的 AS 的首选路径的建议。因为正在接收 MED 的外部 AS 也可能正在使用其他 BGP 属性选择路由，所以它仅作为建议。首选 MED 指标较低的路由。
- 源 - 源属性指示 BGP 获悉某个特定路由的方式。源属性可能具有下面三个可能值中的一个，用于路由选择。
  - IGP - 此路由是源 AS 的内部路由。当使用网络路由器配置命令向 BGP 注入路由时，会设置该值。
  - EGP - 此路由通过外部边界网关协议 (EBGP) 获悉。
  - 不完整 - 路由源未知或通过其他方式获悉。当路由重新分发到 BGP 时，可能会出现源不完整的情况。
- AS_path - 当路由通告通过一个自治系统时，会在按顺序排列的 AS 编号列表中添加 AS 编号，标识路由通告已经穿越的 AS。仅将拥有最短 AS_path 列表的路由添加至 IP 路由表中。
- 下一跳 - EBGP 下一跳属性是用于到达通告路由器的 IP 地址。对于 EBGP 对等体，下一跳地址是对等体之间的连接 IP 地址。对于 IBGP，EBGP 下一跳地址会携带至本地 AS 中。
- 社区 - 社区属性提供一种目标（称为社区）的分组方式，可对社区应用路由决策（例如，接受、首选项和重新分发）。路由映射用于设置社区属性。预定义的社区属性如下：
  - no-export - 不向 EBGP 对等体通告相应路由。
  - no-advertise - 不向任何对等体进行通告。
  - internet - 此路由向互联网社区进行通告；网络中的所有路由器均属于此类型。

何时使用 BGP

客户网络（例如，大学和公司）通常使用 OSPF 等内部网关协议 (IGP) 在其网络内交换路由信息。客户连接到 ISP，然后 ISP 使用 BGP 交换客户路由和 ISP 路由。在自治系统 (AS) 之间使用 BGP 时，该协议称为外部 BGP (EBGP)。如果运营商使用 BGP 在 AS 内交换路由，则此协议称为内部 BGP (IBGP)。

BGP 也可用于通过 IPv6 网络承载有关 IPv6 前缀的路由信息。

BGP 路径选择

BGP 可能会从不同来源接收同一路由的多个通告。BGP 仅选择一个路径作为最佳路径。选择此路径后，BGP 将选定的路径放在 IP 路由表中，并将此路径传播给其邻居。BGP 按显示的顺序使用以下条件为目标选择路径：

- 如果路径指定的下一跳不可访问，则放弃更新。
- 首选权重最高的路径。
- 如果权重相同，则首选具有最高本地优先值的路径。
- 如果本地优先值相同，则首选 BGP 在此路由器上运行所发起的路径。
- 如果未发起路由，则首选 AS_path 最短的路由。
- 如果所有路径的 AS_path 长度相同，则首选源类型最低的路径（其中，IGP 低于 EGP，EGP 低于不完整路径）。
- 如果源代码相同，则首选 MED 属性最低的路径。
- 如果路由的 MED 相同，则首选外部路径而非内部路径。
- 如果路径依然相同，则首选穿过最近的 IGP 邻居的路径。
- 在 BGP 多路径，第 901 页的路由表中确定是否需要安装多个路径。
- 如果两个路径都是外部路径，则首选第一个接收的路径（最早的路径）。
- 首选具有由 BGP 路由器 ID 指定的最低 IP 地址的路径。
- 如果多个路径的发起方或路由器 ID 相同，则首选集群列表长度最短的路径。
- 首选来自最低邻居地址的路径。

BGP 多路径

BGP 多路径允许将多个等成本 BGP 路径的 IP 路由表安装到相同的目标前缀。然后，跨安装的所有路径共享到目标前缀的流量。

这些路径连同最佳路径一起安装在表中，以实现负载共享。BGP 多路径不影响最佳路径选择。例如，路由器仍会根据算法将其中一个路径指定为最佳路径，并将此最佳路径通知其 BGP 对等体。

要想成为多路径的候选对象，指向同一目标的路径需要具有与最佳路径特性相同的以下特性：

- 重量
- 本地优先级
- AS-PATH 长度
- 源代码
- 多出口鉴别器 (MED)
- 以下选项之一：
  - 相邻的 AS 或子 AS（在添加 BGP 多路径之前）
  - AS 路径（在添加 BGP 多路径之后）

某些 BGP 多路径功能对多路径候选对象有一些额外要求：

- 此路径应从外部或联盟外部邻居 (eBGP) 获悉。
- BGP 下一跳的 IGP 指标应等于最佳路径 IGP 指标。

这些是内部 BGP (iBGP) 多路径候选对象的额外要求：

- 此路径应从内部邻居 (eBGP) 获悉。
- BGP 下一跳的 IGP 指标应等于最佳路径 IGP 指标，除非路由器是面向非等成本 iBGP 多路径配置的。

BGP 可将最多 *n* 个最近收到的路径从多路候选对象插入到 IP 路由表中，其中 *n* 是要安装到路由表的路由数，如配置 BGP 多路径时所指定的那样。禁用多路径时的默认值为 1。

对于非等成本的负载平衡，您还可以使用 BGP 链路带宽。

注释 等效的下一自跳将在从 eBGP 中选择的最佳路径上执行，并且是在最佳路径转发至内部对等体之前执行。

BGP 的要求和必备条件

型号支持

威胁防御

Threat Defense Virtual

支持的域

任意

用户角色

管理员

网络管理员

BGP 准则

防火墙模式准则

不支持透明防火墙模式。仅在路由模式下支持 BGP。

IPv6 准则

支持 IPv6。IPv6 地址系列不支持平稳重启。

其他指南

- 系统不会在 CP 路由表中为通过 PPPoE 接收的 IP 地址添加路由条目。BGP 始终查看用于发起 TCP 会话的 CP 路由表，因此 BGP 不会形成 TCP 会话。

  因此，不支持通过 PPPoE 发送 BGP。

- 要避免在路由更新大于链路上的最小 MTU 时丢弃由于路由更新而导致的邻接摆动，请确保在链路两端的接口上配置相同的 MTU。
- 成员设备的 BGP 表未与控制设备表同步。仅其路由表与控制单元路由表同步。

配置 BGP

要配置 BGP，请参阅下列主题：

过程

步骤 1 配置 BGP 基本设置， 第 903 页
步骤 2 配置 BGP 常规设置， 第 905 页
步骤 3 配置 BGP 邻居设置， 第 907 页
步骤 4 配置 BGP 聚合地址设置， 第 910 页
步骤 5 配置 BGPv4 过滤设置， 第 911 页

注释 “过滤”部分仅适用于 IPv4 设置

步骤 6 配置 BGP 网络设置， 第 911 页
步骤 7 配置 BGP 重新分发设置， 第 912 页
步骤 8 配置 BGP 路由注入设置， 第 913 页
步骤 9 配置 BGP 路由导入/导出设置， 第 913 页

配置 BGP 基本设置

可为 BGP 设置很多基本设置。

对于使用虚拟路由的设备，必须在 **BGP** 页面的**常规设置 (General Settings)** 下配置此部分中描述的基本设置。有关详细信息，请参阅 管理中心 Web 界面 - 路由页面修改， 第 814 页。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由**。

步骤 3 （对于虚拟路由器感知设备）在**常规设置**下，点击 **BGP**。

步骤 4 选中**启用 BGP** 复选框以启用 BGP 路由进程。

步骤 5 在 **AS 编号**字段中，输入 BGP 进程的自治系统 (AS) 编号。AS 编号内部包含多个自主编号。AS 编号范围为从 1 至 4294967295，或从 1.0 至 65535.65535。AS 编号是一个唯一分配的值，用于在互联网上标识各个网络。

步骤 6 （可选）从**常规**开始，编辑各项BGP设置。这些设置的默认值适用于大多数情况，但也可以调整它们，以适应您的网络的需求。点击 **编辑** （铅笔）以编辑组中的设置：

a) 在**路由器 ID** 下拉列表中，选择“自动”或“手动”。如果选择了“自动”，则会将 威胁防御设备上的最高级别的 IP 地址用作路由器 ID。要使用固定路由器 ID，请选择“手动”，然后在 **IP 地址**字段中输入一个 IPv4 地址。默认值是自动。对于虚拟路由器感知设备，您可以覆盖**虚拟路由器 (Virtual Routers)** > **BGP** 页面中的路由器 ID 设置。

b) 输入 **AS_PATH 属性中 AS 编号的数量**。AS_PATH 属性是形成供数据包传播的定向路由的源和目标路由器之间的中间 AS 编号序列。有效值介于 1 与 254 之间。默认值为“无”。

c) 选中**记录邻居更改**复选框，启用对 BGP 邻居更改（向上或向下）和重置的日志记录。这有助于解决网络连接问题并衡量网络稳定性。默认情况下，此选项已启用。

d) 选中**使用 TCP 路径 MTU 发现**复选框，使用路径 MTU 确定方法确定两个 IP 主机之间网络路径上的最大传输单位 (MTU) 大小。这可以避免 IP 分片。默认情况下，此选项已启用。

e) 选中**在故障转移时重置会话**复选框，在出现链路故障后立即重置外部 BGP 会话。默认情况下，此选项已启用。

f) 选中**执行第一个 AS 作为对等体的 AS 用于 EBGP 路由**复选框，放弃从未在 AS_PATH 属性中将其 AS 编号列为首个分段的外部 BGP 对等体接收的传入更新。这可以防止错误配置或未经授权的对等体通过通告路由（如同其源自另一个自治系统）来错误定向流量。默认情况下，此选项已启用。

g) 选中**将点分表示法用于 AS 编号**复选框，将完整的二进制 4 字节 AS 编号拆分为两个单词，每个单词 16 位，以点分隔。0-65553 的 AS 编号以十进制数字表示，大于 65535 的 AS 编号使用点分表示法来表示。默认情况下将禁用此复选框。

h) 点击**确定**。

步骤 7 （可选）编辑**最佳路径选择**部分：

a) 为 **默认本地首选项** 输入一个介于 0 与 4294967295 之间的值。默认值为 100。值越大，表示优先级越高。此首选项会发送到本地自治系统中的所有路由器和接入服务器。

b) 选中**允许比较来自不同邻居的 MED** 复选框，允许比较来自不同自治系统中不同邻居的路径的多出口鉴别器 (MED)。默认情况下将禁用此复选框。

c) 选中**比较相同 EBGP 路径的路由器 ID** 复选框，在最佳路径选择过程中，比较从外部 BGP 对等体接收的类似路径，并将最佳路径切换到路由器 ID 最低的路由。默认情况下将禁用此复选框。

d) 选中**在邻居 AS 通告的路径之间选择最佳 MED 路径**复选框，启用从联盟对等体获悉的路径之间的MED比较。仅当路径中没有外部自治系统时，才会比较MED。默认情况下将禁用此复选框。

e) 选中**将缺失 MED 的路径视为最不推荐的路径**复选框，将缺失 MED 的属性视为具有无穷值，从而使此路径成为最不需要使用的路径；因此，缺失 MED 的路径最不优先考虑。默认情况下将禁用此复选框。

f) 点击**确定**。

步骤 8 （可选）编辑**邻居计时器**部分：

a) 在**保持连接时间间隔 (Keep alive interval)** 字段中，输入 BGP 邻居在不发送保持连接消息后保持活动状态的时间间隔。在此 keepalive 时间间隔结束时，如果未发送消息，则声明 BGP 对等体处于失效状态。默认值为 60 秒。

b) 在**保持时间**字段中，输入在发起和配置 BGP 连接期间 BGP 邻居保持活动状态的时间间隔。默认值为 180 秒。指定一个从 0 至 65535 的值。

c) （可选）在**最小保持时间**字段中，输入在发起和配置 BGP 连接期间 BGP 邻居保持活动状态的最小时间间隔。指定一个从 3 至 65535 的值。

注释 保持时间小于 20 秒会增加对等体振荡的可能性。

d) 点击**确定**。

步骤 9 （可选）编辑**无中断重启**部分：

注释 仅当威胁防御设备处于故障转移或跨集群模式下时，此部分才可用。此操作已经完成，以便在处于故障转移设置中的某一设备发生故障时，流量中的数据包不会被丢弃。

a) 选中 **启用无中断重启** 复选框，使 威胁防御 对等体能在状态切换后避免路由抖动。

b) 在**重启时间**字段中，指定在收到BGP开放消息之前，威胁防御对等体删除过时路由的持续时间。默认值为 120 秒。有效值介于 1 至 3600 秒之间。

c) 在 **过时路径时间** 字段中，输入 威胁防御 在从重启 威胁防御 收到记录终止 (EOR) 消息之后，删除过时路由之前等待的持续时间。默认值为 360 秒。有效值介于 1 至 3600 秒之间。

d) 点击**确定 (OK)**。

步骤 10 点击**保存 (Save)**。

步骤 11 要查看 BGP 基本设置，请从虚拟路由器下拉列表中选择所需的路由器，然后点击 **BGP**。

此页面显示在**设置 (Settings)** 页面中配置的基本设置。您可以在此页面上编辑路由器 ID 设置。

步骤 12 要编辑路由器ID设置，请修改 **IP 地址**字段中的 IP 地址。修改后的值会覆盖在 **BGP** 页面中**常规设置 (General Settings)** 下配置的路由器 ID 设置。

配置 BGP 常规设置

配置路由映射、管理路由距离、同步、下一跃点和数据包转发。在大多数情况下，这些设置的默认值都是适当的，但您可以进行调整以适应网络的需要。

过程

步骤 1 在**设备管理 (Device Management)** 页面中，点击**路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4**或 **IPv6**。

注释 用户定义的虚拟路由器不支持使用 IPv6 地址系列的 BGP 配置。因此，如果您选择用户定义的虚拟路由器，则只有 **IPv4** 设置可用。

步骤 4 点击 **General**。

步骤 5 在**常规**选项卡中，更新以下部分：

a) 在**设置**部分中，输入或选择**路由映射**对象，并为 BGP 路由器输入**扫描间隔**，以便进行下一跃点验证。有效值范围为 5 至 60 秒。默认值为 60。点击**确定**。

注释 **路由映射**字段仅适用于 IPv4 设置

b) 在 **路由和同步** 部分中，根据需要更新以下内容，然后点击 **确定**：

- （可选） **生成默认路由** - 选择此选项以配置默认信息来源。
- （可选） **将子网路由汇总至网络级路由** - 选择此选项，以配置子网路由自动汇总至网络级路由。此复选框仅适用于 IPv4 设置。
- （可选） **通告非活动路由** - 选择此选项可通告未安装至路由信息库 (RIB) 中的路由。
- （可选） **在 BGP 和 IGP 系统之间同步** - 选择此选项以启用 BGP 和内部网关协议 (IGP) 系统之间的同步。通常，BGP 发言方不会向外部邻居通告路由，除非路由是本地路由或存在于 IGP 中。使用此功能，自治主系统中的路由器和接入服务器可在 BGP 将某个路由分配给其他自治系统之前获得该路由。
- （可选） **将 iBGP 重新分发至 IGP** - 选择此选项，以将 iBGP 配置为重新分发到内部网关协议 (IGP) 中，例如 OSPF。

c) 在 **管理路由距离** 部分，根据需要更新以下内容，然后点击 **确定**：

- **外部** - 输入外部 BGP 路由的管理距离。从外部自治系统获悉的路由是外部路由。此参数值的范围为 1 至 255。默认值为 20。
- **内部** - 输入内部 BGP 路由的管理距离。从本地自治系统中的对等体获悉的路由是内部路由。此参数值的范围为 1 至 255。默认值为 200。
- **本地** - 输入本地 BGP 路由的管理距离。本地路由是指通过网络路由器显示命令列出的网络，通常作为正在从其他进程重新分发的路由器或网络的后门。此参数值的范围为 1 至 255。默认值为 200。

d) 在**下一跃点**部分中，选择地选中**启用地址跟踪**复选框，以启用 BGP 下一跃点地址跟踪，并输入检查路由表中所安装的更新后下一跃点路由的**延迟间隔**。点击**确定**。

注释 **下一跃点**部分仅适用于 IPv4 设置。

e) 在**在多个路径上转发数据包**部分中，根据需要更新以下内容，并点击**确定**：

- （可选）**路径数** - 指定可以安装在路由表中的边界网关协议路由的最大数量。值的范围是从 1 到 8。默认值为 1。
- （可选）**IBGP 路径数** - 指定可以安装在路由表中的并行内部边界网关协议 (iBGP) 路由的最大数目。值的范围是从 1 到 8。默认值为 1。

步骤 6 点击**保存 (Save)**。

配置 BGP 邻居设置

在交换更新之前，BGP路由器必须与其每个对等体连接。这些对等体称为BGP邻居。使用“邻居”可以定义 BGP IPv4 或 IPv6 邻居及邻居设置。

过程

步骤 1 在“设备管理”页面中，点击**路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4**或 **IPv6**。

步骤 4 点击 **Neighbor**。

步骤 5 点击**添加**以定义 BGP 邻居及邻居设置。

步骤 6 输入 BGP 邻居的 **IP 地址**。此 IP 地址会添加到 BGP 邻居表。在静态 VTI 上配置 BGP IPv6 时，请输入邻居的虚拟隧道 IP 地址。

步骤 7 选择 BGP 邻居**接口**。

注释 **接口**字段仅适用于 IPv6 设置。

步骤 8 在**远程 AS** 字段中，输入 BGP 邻居所属的自治系统。

步骤 9 选中**启用地址**复选框以启用与此BGP邻居的通信。仅当选中“已启用地址”复选框时，才会配置进一步的邻居设置。

步骤 10 （可选）选中**管理性地关闭邻居**复选框，以禁用邻居或对等体组。

步骤 11 （可选）选中**配置平稳重启**复选框，以为此邻居启用BGP平稳重启功能的配置。选择此选项后，必须使用**平稳重启（故障转移/跨区模式）(Graceful restart [failover / spanned mode])** 复选框来指定对此邻居启用还是禁用平稳重启。

注释

- 平稳重启字段仅适用于 IPv4 设置。
- 仅当设备处于HA 模式或配置了 L2 集群（来自同一网络的所有节点）时，才会启用平稳重启。

步骤 12 （可选）选中 **BFD Fallover** 复选框以启用对 BGP 的 BFD 支持的配置。该选择会注册 BGP 邻居以接收来自 BFD 的转发路径检测失败消息。

步骤 13 （可选）输入 BGP 邻居的**说明**。

步骤 14 （可选）在**过滤路由**中，根据需要使用访问列表、路由映射、前缀列表和AS路径过滤器来分发BGP邻居信息。更新以下部分：

a) 输入或选择适当的传入或传出**访问列表**以分发 BGP 邻居信息。

注释 访问列表仅适用于 IPv4 设置。

b) 输入或选择适当的传入或传出**路由映射**，将路由映射应用到传入或传出路由。

c) 输入或选择适当的传入或传出**前缀列表**以分发 BGP 邻居信息。

d) 输入或选择适当的传入或传出 **AS 路径过滤器**以分发 BGP 邻居信息。

e) 选中 **限制允许来自邻居的前缀数量** 复选框，以控制可以从邻居接收的前缀的数量。

- 在**最大前缀数**字段中，输入允许从特定邻居接收的前缀的最大数量。
- 在**阈值级别**字段中，输入路由器开始生成警告消息时所处的（最大值的）百分比。有效值是介于 1 和 100 之间的整数。默认值为 75。

f) 选中 **控制从对等体接收的前缀** 复选框，以指定对从对等体接收的前缀的额外控制。执行以下操作之一：

- 选择**超出前缀限制时终止对等**，以在达到前缀限制时停止 BGP 邻居。在 **Restart interval** 字段中，指定 BGP 邻居重新启动前的间隔。
- 选择**仅在超出前缀限制时发出警报消息**，以在达到最大前缀限制时生成日志消息。此时将不会终止 BGP 邻居。

g) 点击**确定**。

步骤 15 （可选）在**路由**中，指定其他邻居路由参数。继续更新以下内容：

a) 在**通告间隔**字段中，输入前后两次发送 BGP 路由更新的最小间隔（以秒为单位）。有效值介于 1 与 600 之间。

b) 选中**删除传出路由更新中的专用 AS 编号**复选框，以阻止在出站路由上通告专用 AS 编号。

c) 选中**生成默认路由**复选框，以允许本地路由器将默认路由 0.0.0.0 发送到邻居，以用作该邻居的默认路由。在**路由映射**字段中输入或选择允许有条件地注入路由 0.0.0.0 的路由映射。

d) 要添加有条件通告的路由，请点击“添加行”+。在“添加通告路由”对话框中，执行以下操作：

1. 在**通告映射**字段中添加或选择路由映射，如果满足现有映射或非现有映射的条件，则会通告该映射。
2. 选择**现有映射**，然后从“路由映射对象选择器”中选择路由映射。此路由映射与BGP表中的路由进行比较，以确定是否对通告映射路由进行通告。
3. 选择**非现有映射**，然后从“路由映射对象选择器”中选择路由映射。此路由映射与BGP表中的路由进行比较，以确定是否对通告映射路由进行通告。
4. 点击**确定**。

步骤 16 在**计时器**中，选中**设置 BGP 对等体的计时器**复选框，以设置保持连接频率、保持时间和最小保持时间。

- **保持连接间隔 (Keep alive interval)** - 输入 威胁防御 设备向邻居发送保持连接消息的频率（以秒为单位）。有效值介于 0 与 65535 之间。默认值为 60 秒。
- **保持时间**- 威胁防御 设备在未接收到保持连接消息后声明对等体处于失效状态的间隔（以秒为单位）。有效值介于 0 与 65535 之间。默认值为 180 秒。
- **最小保持时间**-（可选）威胁防御设备在未接收到保持连接消息后声明对等体处于失效状态的最小间隔（以秒为单位）。有效值介于 3 与 65535 之间。默认值为 3 秒。

  注释 保持时间小于 20 秒会增加对等体振荡的可能性。

步骤 17 在**高级**中，更新以下内容：

a) （可选）选中**启用身份验证**，以在两个 BGP 对等体之间的 TCP 连接上启用 MD5 身份验证。

1. 从**启用加密类型**下拉列表中选择加密类型。
2. 在 **Password** 字段中输入密码。在**确认**字段中重新输入密码。密码区分大小写，当启用 service password-encryption 命令时，长度最大为 25 个字符；未启用 service password-encryption 命令时，长度最大为 81 个字符。此字符串包含任意字母数字字符，包括空格。

   注释 不能指定 number-space-anything 格式的密码。数字后的空格会导致身份验证失败。

b) （可选）选中**将社区属性发送到此邻居**复选框，以指定应将社区属性发送到 BGP 邻居

c) （可选）选中**使用 FTD 作为此邻居的下一跳**复选框，将路由器配置为 BGP 发言邻居或对等体组的下一跳。

d) 选中**禁用连接验证**复选框可为可通过单跳访问但在环回接口上配置或通过非直接连接 IP 地址配置的 eBGP 对等会话禁用连接验证过程。取消选中（默认设置）时，BGP 路由过程将验证单跳 eBGP 对等会话 (TTL=254) 的连接，以确定 eBGP 对等体在默认情况下是否直接连接到相同的网段。如果对等体没有直连到同一网段，连接验证将阻止建立对等会话。

e) 选择**允许连接未直接连接的邻居**，以接受并尝试建立与未直接连接的网络上的外部对等体的 BGP 连接。（可选）在 **TTL 跳**字段中输入生存时间。有效值介于 1 与 255 之间。或者，选择**到邻居的有限 TTL 跳数**，以确保 BGP 对等会话的安全。在 **TTL hops** 字段中，输入用于分隔 eBGP 对等体的最大跳数。有效值介于 1 与 254 之间。

f) （可选）选中**使用 TCP MTU 路径发现**复选框，为 BGP 会话启用 TCP 传输会话。

g) 从 **TCP 传输模式** 下拉列表中选择 TCP 连接模式。选项包括“默认”、“主动”或“被动”。

h) （可选）输入 BGP 邻居连接的**权重**。

i) 从下拉列表中选择 威胁防御设备将接受的 **BGP 版本**。版本可以设置为“仅限 4”，以强制软件仅对指定邻居使用版本 4。默认使用版本 4，如有要求，可以动态地协商降至版本 2。

步骤 18 仅当考虑进行 AS 迁移时，才更新**迁移**。

注释 在过渡完成后，应删除 AS 迁移自定义。

a) （可选）选中**为从邻居接收的路由自定义 AS 编号**复选框，为从 eBGP 邻居接收的路由自定义 AS_PATH 属性。

b) 在**本地 AS 编号**字段中输入本地自治系统编号。有效值是从 1 到 4294967295 或 1.0 到 65535.65535 之间的任何有效自治系统编号。

c) （可选）选中**不将本地 AS 编号附加到从邻居接收的路由前**复选框，以防止将本地 AS 编号附加到从 eBGP 对等体接收的任何路由前。

d) （可选）选中**将实际 AS 编号替换为从邻居接收的路由中的本地 AS 编号**复选框，将实际自治系统编号替换为 eBGP 更新中的本地自治系统编号。来自本地 BGP 路由过程的自主系统编号不会预置到前面。

e) （可选）选中**接受实际 AS 编号或从邻居接收的路由中的本地 AS 编号**复选框，将 eBGP 邻居配置为使用实际自治系统号（来自本地 BGP 路由过程）或使用本地自治系统编号建立对等会话。

步骤 19 点击**确定 (OK)**。

步骤 20 点击**保存 (Save)**。

配置 BGP 聚合地址设置

BGP邻居存储和交换路由信息，随着配置的BGP发言方的增加，路由信息的量也随之增加。路由聚合是将多个不同路由的属性组合在一起的过程，以便仅通告一个路由。聚合前缀使用无类别域内路由 (CIDR) 原则将相邻的网络合并成一个可在路由表中汇总的无类别 IP 地址集。因此，通告的路由更少。使用“添加/编辑聚合地址”对话框可将特定路由的聚合定义到一个路由中。

过程

步骤 1 编辑 威胁防御 设备时，点击 **路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4**或 **IPv6**。

注释 用户定义的虚拟路由器不支持使用 IPv6 地址系列的 BGP 配置。因此，如果您选择用户定义的虚拟路由器，则只有 **IPv4** 设置可用。

步骤 4 点击**添加汇聚地址 (Add Aggregate Address)**。

步骤 5 在**聚合计时器**字段中，为聚合计时器指定一个值（以秒为单位）。有效值为 0 或介于 6 与 60 之间的任意值。默认值为 30。

步骤 6 点击**添加 (Add)** 并更新**添加聚合地址 (Add Aggregate Address)** 对话框：

a) **网络** - 输入 IPv4 地址或选择所需的网络/主机对象。

b) **属性映射** -（可选）输入或选择用于设置聚合路由属性的路由映射。

c) **通告映射** -（可选）输入或选择用于选择路由的路由映射，以创建 AS_SET 源社区。

d) **隐含映射** -（可选）输入或选择用于选择要隐含的路由的路由映射。

e) **生成 AS 设置路径信息** -（可选）选中该复选框以生成自动系统设置路径信息。

f) **从更新中过滤所有路由** -（可选）选中该复选框可从更新中过滤所有更加特定的路由。

g) 点击**确定 (OK)**。

下一步做什么

- 对于 BGPv4 设置，请继续 配置 BGPv4 过滤设置，第 911 页
- 对于 BGPv6 设置，请继续 配置 BGP 网络设置，第 911 页

配置 BGPv4 过滤设置

过滤设置用于过滤传入的BGP更新中接收的路由或网络。过滤用于限制路由器所获悉或通告的路由信息。

开始之前

过滤仅适用于 BGP IPv4 路由策略。

过程

步骤 1 在“设备管理”页面中，点击**路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4**。

步骤 4 点击 **Filtering**。

步骤 5 点击**添加**并更新**添加过滤器**对话框：

a) **访问列表** - 选择定义在路由更新中要接收和抑制哪些网络的访问控制列表。

b) **方向** -（可选）选择指定是否应将过滤器应用于入站更新或出站更新的方向。

c) **协议** -（可选）选择要过滤的路由进程：“无”、“BGP”、“已连接”、“OSPF”、“RIP”或“静态”。

d) **进程 ID** -（可选）输入 OSPF 路由协议的进程 ID。

e) 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

配置 BGP 网络设置

网络设置用于添加将由BGP路由过程通告的网络，以及将被检查以过滤要通告的网络的路由映射。

过程

步骤 1 在**设备管理 (Device Management)** 页面中，点击**路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4**或 **IPv6**。

注释　用户定义的虚拟路由器不支持使用 IPv6 地址系列的 BGP 配置。因此，如果您选择用户定义的虚拟路由器，则只有 **IPv4** 设置可用。

步骤 4 点击 **Networks**。

步骤 5 点击**添加**并更新**添加网络**对话框：

a) **网络** - 输入将由 BGP 路由过程通告的网络：

b) （可选）**路由映射** - 输入或选择应被检查以过滤要通告的网络的路由映射。如果未指定，则重新分发所有网络。

c) 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

配置 BGP 重新分发设置

重新分发设置可定义将其他路由域中的路由重新分发到 BGP 的条件。

过程

步骤 1 在**设备管理 (Device Management)** 页面中，点击**路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4**或 **IPv6**。

注释　用户定义的虚拟路由器不支持使用 IPv6 地址系列的 BGP 配置。因此，如果您选择用户定义的虚拟路由器，则只有 **IPv4** 设置可用。

步骤 4 点击 **Redistribution**。

步骤 5 点击**添加**并更新**添加重新分发**对话框：

a) **源协议** - 从“源协议”下拉列表中选择要将路由重新分发到 BGP 域所使用的协议。

注释　用户定义的虚拟路由器不支持从 RIP 重新分发流量。

b) **进程 ID** - 输入所选源协议的标识符。应用至 OSPF 协议。对于使用虚拟路由的设备，此下拉列表列出了为您为其配置 BGP 设置的虚拟路由器分配的进程 ID。

c) **指标** -（可选）为重新分配的路由输入一个指标。

d) **路由映射** - 输入或选择应检查的路由映射，以便过滤要重新分发的网络。如果未指定，则重新分发所有网络。

e) **匹配** - 用于将路由从一个路由协议重新分发到另一个路由协议的条件。路由必须与要重新分发的所选条件相匹配。您可以选择以下一个或多个匹配条件。只有在选择 OSPF 作为源协议时，才会启用这些选项。

- 内部
- 外部 1

- 外部 2
- NSSA 外部 1
- NSSA 外部 2

f) 点击**确定**。

配置 BGP 路由注入设置

路由注入设置使您可以定义有条件地注入 BGP 路由表中的路由。

过程

步骤 1 在**设备管理 (Device Management)** 页面中，点击**路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4**或 **IPv6**。

注释 用户定义的虚拟路由器不支持使用 IPv6 地址系列的 BGP 配置。因此，如果您选择用户定义的虚拟路由器，则只有 **IPv4** 设置可用。

步骤 4 点击**路由注入 (Route Injection)**。

步骤 5 点击**添加 (Add)** 并更新**添加路由注入 (Add Route Injection)** 对话框：

a) **注入映射** - 输入或选择指定要注入本地 BGP 路由表的前缀的路由映射。

b) **现有映射** - 输入或选择包含 BGP 发言者将跟踪的前缀的路由映射。

c) **注入的路由将继承聚合路由的属性** - 选择此选项可将注入的路由配置为继承聚合路由的属性。

d) 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

配置 BGP 路由导入/导出设置

在BGP中，可以通过分别使用目的和源虚拟路由器的路由目标扩展社区导入或导出路由来实现虚拟路由器间路由泄漏。您可以使用路由映射来过滤所需的路由目标，而不是泄漏整个路由表。您还可以将全局虚拟路由器的路由泄漏到用户定义的虚拟路由器，反之亦然。

- 您可以将 BGP 配置为使用路由目标扩展社区在两个用户定义的虚拟路由器之间泄漏路由：
  - 使用路由目标导出，使用来自源虚拟路由器的路由目标标记路由。
  - 使用路由目标导入，将与路由目标匹配的路由导入到目的虚拟路由器。

- 或者，您可以分别使用导出或导入路由映射来过滤来自源虚拟路由器或到目的虚拟路由器的路由。您可以通过匹配扩展社区列表来配置路由映射，以过滤路由。同样，您可以通过设置扩展社区路由目标来配置路由映射，以使用路由目标扩展社区标记路由。

- 要将路由从全局虚拟路由器导入到用户定义的虚拟路由器，需要在全局虚拟路由器导入路由映射中指定 IPv4/IPv6 路由映射，以导入到用户定义的虚拟路由器。
- 要将路由从用户定义的虚拟路由器导出到全局虚拟路由器，除了导出路由目标外，还可以指定全局虚拟路由器导出路由映射，以从用户定义的虚拟路由器导出。

BGP 虚拟路由器间路由泄漏支持 IPv4 和 IPv6 前缀。

开始之前

- 创建虚拟路由器。
- 配置 BGP 基本设置。
- 配置 BGP，第 903 页

过程

步骤 1 在“设备管理”页面中，点击**路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4** 或 **IPv6**。

步骤 4 点击**路由导入/导出**。

步骤 5 在**路由目标导入**字段中，输入要与待导入的路由匹配的路由目标扩展社区。在部署时，与此值匹配的目标虚拟路由器的路由将导入到源虚拟路由器的 BGP 表中。

注释
- 路由目标必须采用 **ASN:nn** 格式。
- 您可以以逗号分隔值的形式输入多个路由目标。
- 此值的范围为 0:1 到 65534:65535。

步骤 6 在**路由目标导出**字段中，输入路由目标扩展社区，以使用路由目标值标记源虚拟路由器的路由。部署时，源虚拟路由器的路由使用此值进行标记。

注释
- 路由目标必须采用 **ASN:nn** 格式。
- 您可以以逗号分隔值的形式输入多个路由目标。
- 此值的范围为 0:1 到 65534:65535。

步骤 7 路由映射可帮助您缩小要共享的路由的范围，而不是泄漏整个路由表。路由映射过滤应用于使用指定路由目标值获取的路由列表：

a) （可选）在**用户虚拟路由器**下，从**导入路由映射**下拉列表中选择路由映射，以过滤目的虚拟路由器上的路由。

注释 用户虚拟路由器导入路由映射只有在配置了路由目标导入时才有效。

b) （可选）在**用户虚拟路由器**下，从**导出路由映射**下拉列表中选择路由映射，以在将路由导出到其他虚拟路由器之前过滤源虚拟路由器上的路由。

注释 您可以将路由映射中的 match 和 set 子句与路由目标扩展社区列表一起使用，以根据其他条件进行过滤或使用路由目标社区值标记路由。有关详细信息，请参阅路由映射，第 1022 页

步骤 8 要在用户定义的虚拟路由器和全局虚拟路由器之间共享路由，请在**全局虚拟路由器**下指定路由映射：

a) 要将全局虚拟路由器路由泄漏到用户定义的虚拟路由器，请从**导入路由映射**下拉列表中选择路由映射。将 IPv4 或 IPv6 路由映射导入用户定义的虚拟路由器。

b) 要将用户定义的虚拟路由器路由泄漏到全局虚拟路由器，请从**导出路由映射**下拉列表中选择路由映射。将 IPv4 或 IPv6 路由映射导出到全局虚拟路由器。

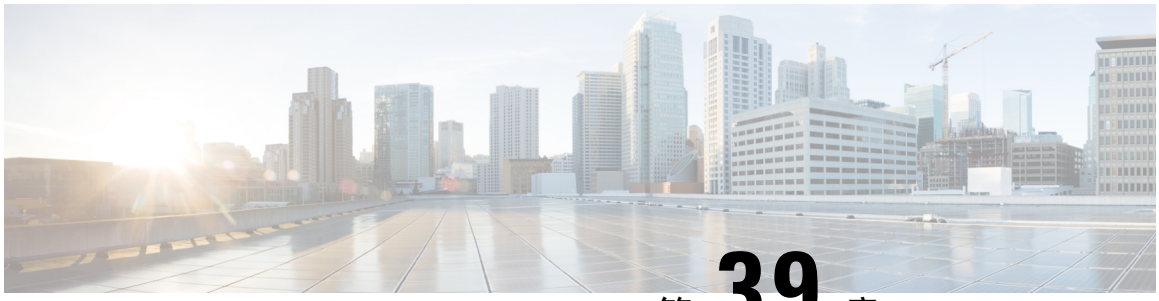
注释 除了指定路由映射之外，您还必须指定导出的路由目标。

注释 您可以使用路由映射对象的 match 子句过滤路由以进行泄漏。有关详细信息，请参阅路由映射，第 1022 页。

步骤 9 按照步骤（步骤 3 到步骤 8）为其他虚拟路由器配置相关的 BGP 路由导入和导出设置。

步骤 10 点击**保存**，然后点击**部署**。

当数据包流入入口虚拟路由器时，BGP 会从具有匹配路由目标值的目的虚拟路由器导入路由，如果还配置了路由映射，则会进一步过滤路由并使用这些路由来识别用于路由数据包的最佳路径路由。



第 39 章

RIP

本章介绍如何配置 威胁防御，以使用路由信息协议 (RIP) 来路由数据、执行身份验证以及重新分发路由信息。对于使用虚拟路由的设备，只能为其全局虚拟路由器配置 RIP，不能为其用户定义的虚拟路由器配置 RIP。

关于 RIP

路由信息协议 (RIP) 是所有路由协议中最常见的协议。RIP 有四基本组成部分：路由更新过程、RIP 路由指标、路由稳定性和路由计时器。支持 RIP 的设备将定期以及在网络拓扑更改时发送路由更新消息。这些 RIP 数据包包括有关设备可到达的网络的信息，以及数据包必须经过才能到达目标地址的路由器或网关的数量。RIP 产生的流量比 OSPF 多，但更易于配置。

RIP 是一种使用跳数作为路径选择指标的距离矢量路由协议。当在某接口上启用 RIP 时，该接口会交换与相邻设备的 RIP 广播，以动态了解和通告路由。

Secure Firewall Threat Defense支持 RIP 版本 1 和 RIP 版本 2。RIP 版本 1 不通过路由更新发送子网掩码。RIP版本2通过路由更新发送子网掩码，并支持可变长度的子网掩码。此外，交换路由更新时，RIP 版本 2 支持邻居身份验证。此身份验证可确保 Secure Firewall Threat Defense从受信任的源接收可靠的路由信息。

RIP比静态路由更有优势，因为初始配置比较简单，并且您不需要在拓扑更改时更新配置。RIP的缺点是网络和处理开销比静态路由大。

路由更新过程

RIP 会定期以及在网络拓扑更改时发送路由更新消息。当路由器接收到包含对某个条目的更改的路由更新时，它将更新其路由表以反映新路由。路径的指标值增加1，而发送器被指示为下一跳。RIP路由器只维护到目标的最佳路由（指标值最低的路由）。更新其路由表后，路由器立即开始传输路由更新，以将此更改通知到其他网络路由器。这些更新独立于RIP路由器发送的定期计划更新发送。

RIP 路由指标

RIP 使用单个路由指标（跃点数）来测量源和目标网络之间的距离。从源到目标的路径中的每个跃点都分配了跃点数值，通常为 1。当路由器接收到包含新的或已更改的目标网络项的路由更新时，路由器会向更新中指示的指标数值增加 1，并将网络输入到路由表中。发送器的 IP 地址被用作下一个跃点。

RIP 稳定性功能

RIP 通过对源到目标的路径中允许的跃点数施加限制，防止无限期地执行路由循环。路径中的最大跃点数量为 15 个。如果路由器接收到包含新项或已更改项的路由更新，并且如果将跃点数增加 1 会导致跃点数无穷大（即 16），则认为网络目标不可访问。此稳定性功能的缺点是，它将 RIP 网络的最大直径限制为少于 16 个跃点。

RIP 具有许多其他路由协议所共有的一些稳定性功能。这些功能旨在提供稳定性，尽管网络拓扑可能会发生快速变化。例如，RIP 实施水平分割和抑制机制，以防止传播不正确的路由信息。

RIP 计时器

RIP 使用多个计时器来调节性能。以下是 RIP 的计时器阶段：

- 更新 - 路由更新计时器会记录定期路由更新之间的时间间隔。这是设备发送路由更新的频率。通常情况下，此间隔设置为30秒，每次计时器复位会随机增加少量的时间。这样做是为了防止由所有路由器同时试图更新邻居而造成的拥塞。
- 无效 - 每个路由表条目都有一个与之关联的路由超时计时器。这是设备自上次收到有效更新以来经过的秒数。路由超时计时器过期后，路由将被标记为无效，但会保留在表中，直到路由刷新计时器过期。此计时器到期后，路由将进入抑制状态。默认值为 3 分钟（180 秒）。
- 抑制 - 抑制周期是指系统在接受处于抑制状态的路由（即已标记为无效的路由）的任何新更新之前等待的秒数。默认值为 3 分钟（180 秒）。
- 刷新 - 路由刷新计时器是指从系统收到上次有效更新到路由被丢弃并从路由表中删除之前所经过的秒数。默认值为 240 秒（4 分钟）。

例如，当相邻路由器上的接口关闭时，系统不会再从相邻路由器接收路由更新。此时，无效和刷新计时器会开始计数。在前 180 秒内，什么都不会发生。180 秒后，无效计时器到期，从而让路由无效，同时抑制计时器启动并将路由额外保持60秒。如果仍然没有关于相邻路由器上的接口状态的更新（即它仍处于关闭状态），则该路由会进入刷新状态，其中系统从上次更新开始总共等待了 240 秒（无效计时器等待了 180 秒，抑制计时器等待了 60 秒），系统将刷新路由。即使相邻路由器的接口立即启动，系统也不会接受路由更新，直到抑制计时器完成剩余的 120 秒。

RIP 的要求和必备条件

型号支持

威胁防御

Threat Defense Virtual

支持的域

任意

用户角色

管理员

网络管理员

RIP 指南

IPv6 准则

不支持 IPv6。

其他准则

以下信息仅适用于 RIP 版本 2：

- 如果适用邻居身份验证，则在为接口提供 RIP 版本 2 更新的所有邻居设备上，身份验证密钥和密钥 ID 都必须相同。
- 通过 RIP 版本 2，Secure Firewall Threat Defense 将使用组播地址 224.0.0.9 传输和接收默认路由更新。在被动模式下，它将在该地址接收路由更新。
- 在接口上配置 RIP 版本 2 时，将在该接口上注册组播地址 224.0.0.9。在从接口上删除 RIP 版本 2 配置时，将取消注册该组播地址。

限制

- Secure Firewall Threat Defense 不能在两个接口之间传递 RIP 更新。
- RIP 版本 1 不支持可变长度的子网掩码。
- RIP 的最大跳数为 15。跳数大于 15 的路由将被视为无法访问。
- 与其他路由协议相比，RIP 融合的速度相对较慢。
- 只能在 Secure Firewall Threat Defense上启用单个 RIP 进程。

配置 RIP

RIP 是一种使用跳数作为路径选项指标的距离矢量路由协议。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由**。

步骤 3 从目录中选择 **RIP**。

步骤 4 选中**启用 RIP (Enable RIP)** 复选框以配置 RIP 设置。

步骤 5 从 **RIP 版本**下拉列表中选择用于发送和接收 RIP 更新的 RIP 版本。

步骤 6 （可选）选择**生成默认路由 (Generate Default Route)** 复选框，以根据您指定的路由映射生成用于分发的默认路由。

a) 在**路由映射**字段中，指定要用于生成默认路由的路由映射名称。
当在**路由映射**字段中指定的路由映射存在时，将生成默认路由 0.0. 0.0/0 以便通过特定接口进行分发。

步骤 7 当发送和接收版本 2 为所选的 RIP 版本时，**启用自动摘要**选项将可用。选中**启用自动摘要**复选框后，将启用自动路由汇总。如果您必须在已断开连接的子网之间执行路由，则禁用自动汇总。当禁用自动汇总时，会通告子网。

注释 RIP 版本 1 始终使用自动汇总，您无法将其禁用。

步骤 8 点击 **Networks**。定义一个或多个用于 RIP 路由的网络。输入 IP 地址，或者输入或选择所需的网络/主机对象。可添加到安全设备配置的网络数量没有限制。属于此命令定义的网络的任何接口都将参与 RIP 路由过程。RIP 路由更新仅通过指定网络上的接口发送和接收。此外，如果未指定接口的网络，则在不会在任何 RIP 更新中通告该接口。

注释 RIP 仅支持 IPv4 对象。

步骤 9 （可选）点击**被动接口 (Passive Interface)**。使用此选项可以指定设备上的被动接口，以及通过扩展指定主动接口。该设备监听被动接口上的 RIP 路由广播，使用该信息填充其路由表，但不在被动接口上广播路由更新。未指定为被动的接口会接收和发送更新。

步骤 10 点击**重新分发 (Redistribution)** 可管理重新分发路由。这些路由将从其他路由进程重新分发到 RIP 路由进程。

a) 点击**添加**以指定重新分发路由。

b) 在**协议**下拉列表中选择要重新分发到 RIP 路由进程中的路由协议。

注释 对于 OSPF 协议，指定进程 ID。类似地，指定 BGP 的 AS 路径。在**协议**下拉列表中选择“已连接”选项时，可以将直接连接的网络重新分发到 RIP 路由进程中。

c) （可选）如果要将 OSPF 路由重新分发到 RIP 路由进程，可以在**匹配**下拉列表中选择要重新分发的特定类型的 OSPF 路由。按住 Ctrl 键并点击以选择多个类型：

- 内部 - 重新分发自治系统 (AS) 内部的路由。
- 外部 1 - 重新分发 AS 外部的类型 1 路由。
- 外部 2 - 重新分发 AS 外部的类型 2 路由。
- NSSA 外部 1 - 重新分发末节区域 (NSSA) 外部的类型 1 路由。
- NSSA 外部 2 - 重新分发 NSSA 外部的类型 2 路由

注释 默认设置为匹配内部、外部 1 和外部 2

d) 在**指标**下拉列表中选择要应用于重新分发的路由的 RIP 指标类型。两个选择包括：
   - 透明 – 使用当前路由指标
   - 指定的值 - 分配特定的指标值。在**指标值**字段中输入一个特定的值（从 0 到 16）。
   - 无 - 不指定指标。不将任何指标值应用于重新分发的路由。

e) （可选）在**路由映射**字段中输入必须满足的路由映射的名称，然后才能将路由重新分发到RIP路由进程中。只有当 IP 地址与路由映射地址列表中的允许语句匹配时，才会重新分发路由。

f) 点击 **OK**。

步骤 11 （可选）点击**过滤 (Filtering)** 以管理 RIP 策略的过滤器。在本部分中，过滤器用于避免通过接口路由更新、控制路由更新中的路由通告、控制路由更新的处理以及过滤路由更新的源。

a) 点击**添加**添加 RIP 选项。

b) 在**流量方向**字段中，选择要过滤的流量类型：入站或出站。

注释 如果流量方向为入站，则只能定义接口过滤器。

c) 通过在**过滤方式 (Filter On)** 字段中进行相应的选择，指定过滤器是基于“接口”(Interface) 还是“路由”(Route)。如果选择“接口”，则输入或选择要过滤其路由更新的接口的名称。如果选择“路由”，则选择路由类型：
   - 静态 - 仅过滤静态路由。
   - 已连接 - 仅过滤连接的路由。
   - OSPF - 仅过滤由指定的 OSPF 进程发现的 OSPFv2 路由。输入要过滤的 OSPF 进程的进程 ID。
   - BGP - 仅过滤由指定的 BGP 进程发现的 BGPv4 路由。输入要过滤的 BGP 进程的 AS 路径。

d) 在**访问列表**字段中，输入或选择定义要在RIP路由通告中允许或删除的网络的一个或多个访问控制列表 (ACL) 的名称。

e) 点击 **OK**。

步骤 12 （可选）点击**广播 (Broadcast)** 以添加或编辑接口配置。使用“广播”(Broadcast)，可以覆盖要按接口发送或接收的全局 RIP 版本。如果要实施身份验证以确保有效的 RIP 更新，则还可以定义每个接口的身份验证参数。

a) 点击**添加**添加接口配置。
b) 在**接口**字段中输入或选择在此设备上定义的接口。
c) 在“发送”选项中，选择相应的框以指定使用 RIP **版本 1** 和/或**版本 2** 发送更新。这些选项使您可以为指定的接口覆盖指定的全局发送版本。
d) 在“接收”选项中，选择相应的框以指定使用 RIP **版本 1** 和/或**版本 2** 接受更新。这些选项使您可以为指定的接口覆盖指定的全局接收版本。
e) 选择此接口上用于 RIP 广播的**身份验证**。

- 无 - 无身份验证
- MD5 - 使用 MD5
- 清除文本 - 使用明文身份验证

如果选择 MD5 或明文，则还必须提供以下身份验证参数。

- 密钥 ID - 身份验证密钥的 ID。有效值为 0 至 255。
- 密钥 - 所选身份验证方法使用的密钥。最多可以包含 16 个字符。
- 确认 - 再次输入身份验证密钥以进行确认

f) 点击**确定 (OK)**。

第 40 章

组播

本章介绍如何将 Secure Firewall Threat Defense配置为使用组播路由协议。对于使用虚拟路由的设备，只能为其全局虚拟路由器配置组播，不能为其用户定义的虚拟路由器配置组播。

关于组播路由

组播路由是一种带宽节省技术，通过同时向数千个公司收件人和家庭传送单一信息流来减少流量。使用组播路由的应用包括视频会议、公司通信、远程教育以及软件、股票报价和新闻的分发。

组播路由协议将源流量传递给多个接收者，而不会对源或接收者造成任何额外负担，而且是同类技术当中占用网络带宽最少的。组播数据包通过启用了协议无关组播 (PIM) 及其他支持性组播协议的威胁防御设备 在网络中复制，是目前为止向多个接收者传输数据的最高效方式。

威胁防御设备 支持末节组播路由和 PIM 组播路由。但是，不能在一个 威胁防御设备 上都配置这两种路由。

注释 组播路由同时支持 UDP 和非 UDP 传输。但是，非 UDP 传输没有进行快速路径优化。

IGMP 协议

IP 主机使用互联网组管理协议 (IGMP) 将其组成员身份报告给直连组播路由器。IGMP 用于在特定 LAN 上的一个组播组中动态注册单个主机。主机通过向其本地组播路由器发送 IGMP 消息来识别组

成员身份。在 IGMP 下，路由器监听 IGMP 消息，并定期发出查询以发现特定子网上处于活动状态或非活动状态的组。

IGMP 将组地址（D 类 IP 地址）用作组标识符。主机组地址的范围可以是 224.0.0.0 到 239.255.255.255。地址 224.0.0.0 不分配给任何组。地址 224.0.0.1 分配给子网上的所有系统。地址 224.0.0.2 分配给子网上的所有路由器。

注释 如果在 威胁防御设备上启用组播路由，IGMP V2 将会在所有接口上自动启用。

发送到组播组的查询消息

威胁防御设备发送查询消息，以发现哪些组播组有成员位于与接口连接的网络上。成员以IGMP报告消息作出响应，以表明自己想要接收特定组的组播数据包。查询消息会发送到全系统组播组，该组的地址为 224.0.0.1，生存时间值为 1。

这些消息会定期发送，从而刷新威胁防御设备上存储的成员身份信息。如果威胁防御设备发现组播组中没有本地成员仍与接口相连接，它会停止向连接的网络转发该组的组播数据包，并会向数据包源发送回删除消息。

默认情况下，子网上的 PIM 指定路由器负责发送查询消息。默认情况下，每 125 秒发送一次消息。

默认情况下，更改查询响应时间时，IGMP 查询中通告的最大查询响应时间为 10 秒。如果 威胁防御设备不在此时间内接收对主机查询的响应，它就会删除该组。

末节组播路由

末节组播路由提供动态主机注册并促进组播路由。如果针对末节组播路由进行了配置，威胁防御设备 将用作 IGMP 受托代理。威胁防御设备 将 IGMP 消息转发到上游组播路由器（上游组播路由器设置组播数据的传输），而不是完全参加组播路由。威胁防御设备 在为末节组播路由而配置后，就不能为 PIM 稀疏模式或双向模式而配置。您必须在参与 IGMP 末节组播路由的接口上启用 PIM。

威胁防御设备 同时支持 PIM-SM 和双向 PIM。PIM-SM 是一个组播路由协议，它使用基础单播路由信息库或支持组播的独立路由信息库。该协议会按组播组构建以单个交汇点 (RP) 为根的单向共享树，并且可以选择性地按组播源创建最短路径数。

PIM 组播路由

双向 PIM 是 PIM-SM 的一个变体，用于构建连接组播源和接收器的双向共享树。双向树使用每个组播拓扑链路上运行的专用转发器 (DF) 选择流程构建借助 DF，组播数据从源转发至交汇点 (RP)，然后联通共享树一起发送至接收器，而无需源特定的状态。DF 选择发生在 RP 发现期间，提供至 RP 的默认路由。

注释 如果 威胁防御设备 是 PIM RP，请使用 威胁防御设备 的未被转换的外部地址作为 RP 地址。

PIM 源特定组播支持

威胁防御设备 不支持 PIM 源特定组播 (SSM) 功能和相关配置。不过，威胁防御设备 允许与 SSM 相关的数据包通过，除非将其放置为最后一跳路由器。

SSM 被分类为数据传递机制，适用于一对多应用，如 IPTV。SSM 模型使用“通道”的概念，以 (S,G) 对表示，其中 S 表示源地址，G 表示 SSM 目标地址。通过使用组管理协议（如 IGMPv3）来实现订用通道。一旦SSM获悉某一特定的组播源，它将使接收客户端能直接从该源接收多播流，而不是从共享交汇点 (RP) 接收。SSM 中引入了访问控制机制，提供当前稀疏或疏-密模式实施无法提供的安全增强功能。

PIM-SSM 与 PIM-SM 不同，前者不使用 RP 或共享树。相反，组播组源地址上的信息将由接收方通过本地接收协议 (IGMPv3) 提供，并且用于直接构建源特定树。

组播双向 PIM

对于有多个源和接收器相互同步交互的网络，以及每个参与者都可以同时成为多播流量的源和接收器的网络而言，多播双向 PIM （例如在视频会议、Webex 会议和分组聊天中）非常有用。当使用 PIM 双向模式时，RP 仅会为共享树创建 (*,G) 条目。没有 (S,G) 条目。这节省了 RP 上的资源，因为这样不用维护每个 (S,G) 条目的状态表。

在 PIM 稀疏模式下，流量仅会沿共享树向下流动。在 PIM 双向模式下，流量沿共享树向上和向下流动。

PIM 双向模式也不使用 PIM 寄存器/寄存器停止机制来向 RP 注册源。每个源随时都可以开始发送到源。当多播数据包到达 RP 时，这些数据包将向下转发到共享树（如果有接收器）或被丢弃（如果没有接收器）。但是，RP 无法告知源停止发送多播流量。

从设计角度看，您必须考虑在网络中放置 RP 的位置，因为该位置应为网络中源和接收器之间的中间位置。

PIM 双向模式没有反向路径转发 (RPF) 检查。相反，它使用指定转发器 (DF) 的概念来防止循环。此 DF 是网段上唯一允许向 RP 发送多播流量的路由器。如果每个网段只有一个路由器转发多播流量，则没有循环。使用以下机制选择 DF：

- 具有最低 RP 指标的路由器是 DF。
- 如果指标相等，则具有最高 IP 地址的路由器将成为 DF。

PIM 自举路由器 (BSR)

PIM 自举路由器 (BSR) 是一个动态交汇点 (RP) 选择模型，它使用候选路由器执行 RP 功能以及中继组的 RP 信息。RP 功能包括 RP 发现并向 RP 提供默认路由。它执行此操作的方式是将一组设备配置为候选 BSR (C-BSR)，它们参与 BSR 选举过程，以从它们自身中选出一个 BSR。选择 BSR 后，配置为候选交汇点 (C-RP) 的设备将开始向选出的 BSR 发送其组映射。然后，BSR 会将组与 RP 的映射信息通过基于跳从 PIM 路由器传送至 PIM 路由器的 BSR 消息发至组播树下的其他所有设备。

此功能提供了一种动态获悉 RP 的方法，这在 RP 可能会定期关闭和启动的大型负载网络中非常重要。

PIM 自举路由器 (BSR) 术语

以下术语经常在 PIM BSR 配置中引用：

- 自举路由器 (BSR) - BSR 通过 PIM 逐跳向其他路由器通告交汇点 (RP) 信息。在多个候选 BSR 中，在选举过程后会选择单个 BSR。此自举路由器的主要目的是将所有候选 RP (C-RP) 通告收集到称为 RP-set 的数据库中，并以 BSR 消息的形式定期（每 60 秒）将此数据库发送到该网络中的其他路由器。
- 自举路由器 (BSR) 消息— BSR 消息会组播到 TTL 为 1 的 All-PIM-Routers 组。收到这些消息的所有 PIM 邻居会将它们重新传输（TTL 同样为 1）到除收到消息的接口之外的所有接口。BSR 消息包含 RP 集合和当前活动 BSR 的 IP 地址。这是 C-RP 了解在何处单播其 C-RP 消息的方式。
- 候选自举路由器 (C-BSR) - 配置为候选 BSR 的某个设备会参与 BSR 选举机制。具有最高优先级的 C-BSR 会被选举作为 BSR。C-BSR 的最高 IP 地址作为决定因素。BSR 选举过程是优先的，例如，如果出现具有更高优先级的新 C-BSR，它会触发新的选举过程。
- 候选交汇点 (C-RP) - RP 作为组播数据源和接收器的交汇场所。配置为 C-RP 的设备会通过单播定期将组播组映射信息直接通告到选举的 BSR。这些消息包含组范围、C-RP 地址和保持时间。当前 BSR 的 IP 地址从网络中所有路由器收到的定期 BSR 消息获取。这样，BSR 可了解当前正在运行且可访问的 RP。

注释 威胁防御设备 不充当 C-RP，即使 C-RP 是 BSR 流量的强制性要求也是如此。仅路由器可以充当 C-RP。因此，对于 BSR 测试功能，您必须将路由器添加到拓扑。

- BSR 选举机制 - 每个 C-BSR 都会生成包含 BSR 优先级字段的引导程序消息 (BSM)。该域中的路由器会在整个域中泛洪传播 BSM。C-BSR 收到具有比自身优先级更高的 C-BSR 时，会在特定时间内抑制进一步发送 BSM。剩余的单个 C-BSR 会成为选举的 BSR，而且其 BSM 会通知域中的所有其他路由器它是选举的 BSR。

组播组概念

组播基于组概念。任意一组接收者对接收特定数据流表现出兴趣。这样的组没有任何物理边界或地理边界 - 主机可位于互联网上的任何位置。有兴趣接收流向特定组的数据的主机必须使用 IGMP 加入该组。要接收数据流，主机必须是该组的成员。

组播地址

组播地址指定已加入某个组的任意一组 IP 主机，并希望接收发送到此组的流量。

集群

组播路由支持群集。在跨网络 EtherChannel 集群中，在快速路径转发建立之前，控制单元会发送所有的组播数据包和数据包。在建立快速路径转发后，数据单元可能会转发组播数据包。所有数据流

都是全流量。同时还支持末节转发流。由于跨网络 EtherChannel 集群中仅有一台设备接收组播数据包，因此，重定向到控制单元较为常见。

组播路由的要求和必备条件

型号支持

威胁防御

Threat Defense Virtual

支持的域

任意

用户角色

管理员

网络管理员

组播路由指南

防火墙模式

仅在路由防火墙模式下受支持。不支持透明防火墙模式。

IPv6

不支持 IPv6。

组播组

保留 224.0.0.0 和 224.0.0.255 之间的地址范围用于路由协议和其他拓扑发现或维护协议，例如网关发现和组成员报告。因此，不支持来自地址范围 224.0.0/24 的互联网组播路由；为保留地址启用组播路由时，未创建 IGMP 组。

集群

在集群中，对于 IGMP 和 PIM，仅在主设备上支持此功能。

其他规定

- 必须针对入站安全区配置访问控制或预过滤器规则的，以允许流量到达组播主机（如224.1.2.3）。但不能为该规则指定目标安全区，或者不能使其在初始连接验证过程中适用于组播连接。

- 不能禁用配置了 PIM 的接口。如果已在接口上配置 PIM（请参阅 配置 PIM 协议，第 933 页），则禁用组播路由和 PIM 不会删除PIM配置。您必须移除（删除）PIM配置才能禁用接口。
- 流量区域中的接口上不支持 PIM/IGMP 组播路由。
- 请勿将 威胁防御 同时配置为交汇点 (RP) 和第一跳路由器。
- HSRP 备用 IP 地址不参与 PIM 邻居关系。因此，如果通过 HSRP 备用 IP 地址来路由 RP 路由器 IP，则组播路由在 威胁防御 中不起作用。因此，要使组播流量成功通过，请确保 RP 地址的路由不是 HSRP 备用 IP 地址，而是将路由地址配置为接口 IP 地址。

配置 IGMP 功能

IP 主机使用 IGMP 向直接连接的组播路由器报告其组成员身份。IGMP 用于在特定 LAN 上的一个组播组中动态注册单个主机。主机通过向其本地组播路由器发送 IGMP 消息来识别组成员身份。在 IGMP 下，路由器监听 IGMP 消息，并定期发出查询以发现特定子网上处于活动状态或非活动状态的组。

本节介绍如何为逐个接口配置可选的 IGMP 设置。

过程

步骤 1 启用组播路由，第 928 页
步骤 2 配置 IGMP 协议，第 929 页。
步骤 3 配置 IGMP 访问组，第 930 页。
步骤 4 配置 IGMP 静态组，第 931 页。
步骤 5 配置 IGMP 加入组，第 931 页。

启用组播路由

默认情况下，在 威胁防御设备上启用组播路由可以在所有接口上启用 IGMP 和 PIM。IGMP 用于了解直连子网上是否存在组成员。主机通过发送 IGMP 报告消息加入组播组。PIM 用于维护转发表，以转发组播数据报。

注释 组播路由仅支持 UDP 传输层。

下表列出了特定组播表的最大条目数。一旦达到这些限制，系统将会丢弃所有新条目。

- MFIB - 30,000
- IGMP 组 - 30,000

- PIM 路由 - 72,000

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 依次选择**路由** > **组播路由** > **IGMP**。

步骤 3 选中**启用组播路由**复选框。

选中此复选框可在设备上启用 IP 组播路由。取消选中此复选框将禁用 IP 组播路由。默认情况下，组播已禁用。启用组播路由可在所有接口上启用组播。

您可以逐个接口禁用组播。如果知道特定接口上没有组播接口，并且希望防止 威胁防御设备通过该接口发送主机查询消息，则此操作很有用。

配置 IGMP 协议

您可以为每个接口配置 IGMP 参数，如转发接口、查询消息和时间间隔。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **组播路由** > **IGMP**。

步骤 3 在**协议**上，点击**添加**或**编辑**。

使用**添加 IGMP 参数**对话框将新的 IGMP 参数添加到 威胁防御设备。使用**编辑 IGMP 参数**对话框更改现有参数。

步骤 4 配置以下选项：

- **接口** - 从下拉列表中选择要为其配置 IGMP 协议的接口。
- **启用 IGMP** - 选中该复选框可启用 IGMP。

  注释 如果知道特定接口上没有组播主机，并且想要防止设备通过该接口发送主机查询消息，则在特定接口上禁用 IGMP 很有用。

- **转发接口** - 从下拉列表中选择您要通过其转发 IGMP 消息的特定接口。

  此选项可将 Cisco Secure Firewall Threat Defense设备配置为 IGMP 受托代理，并使其会从连接到一个接口的主机将 IGMP 消息转发到另一个接口上的上游组播路由器。

- **版本** - 选择 IGMP 版本 1 或 2。

  默认情况下，威胁防御设备运行 IGMP 版本 2，这将启用多个附加功能。

注释 子网上所有的组播路由器必须支持同一版本的 IGMP。威胁防御设备不会自动检测 IGMP 版本 1 路由器并切换到版本 1。但是，可以在子网上结合使用 IGMP 版本 1 和版本 2 主机；当存在 IGMP 版本 1 主机时，运行 IGMP 版本 2 的 威胁防御设备可正常工作。

- **查询间隔** - 指定的路由器发送 IGMP 主机查询消息的间隔（以秒为单位）。范围为 1 到 3600。默认值为 125。

  注释 如果 威胁防御 设备不能在指定超时值内在接口上收到查询消息，设备将会成为指定路由器并开始发送查询消息。

- **响应时间** - 在 威胁防御设备删除组之前的间隔（以秒为单位）。范围为 1 到 25。默认值为 10。

  如果 威胁防御设备未在此时间内收到对主机查询的响应，它会删除该组。

- **组限制** - 可在接口上加入的最大主机数。范围为 1 到 500。默认值为 500。

  您可以对每个接口限制 IGMP 成员身份报告造成的 IGMP 状态数量。超出所配置限制的成员身份报告不会输入到 IGMP 缓存中，多余成员身份报告的流量不会转发

- **查询超时** - 在上一请求者停止后，威胁防御设备成为接口请求者之前需经过的时间（以秒为单位）。范围为 60 到 300。默认值为 255。

步骤 5 点击**确定**以保存 IGMP 协议配置。

配置 IGMP 访问组

您可以通过使用访问控制列表控制对组播组的访问。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **组播路由** > **访问组**。

步骤 3 在**访问组 (Access Group)** 上，点击**添加 (Add)** 或**编辑 (Edit)**。

使用**添加 IGMP 访问组参数**对话框可以将新的 IGMP 访问组添加到访问组表中。使用**编辑 IGMP 访问组参数**对话框可更改现有的参数。

步骤 4 配置以下选项：

a) 从**接口**下拉列表中，选择与访问组关联的接口。编辑现有访问组时，不能更改相关的接口。

b) 点击以下选项之一：

- **标准访问列表 (Standard Access List)** - 从**标准访问列表 (Standard Access List)**下拉列表中，选择标准 ACL 或点击 **添加**（+） 以创建新的标准 ACL。请参阅配置标准 ACL 对象，第 977 页了解相关程序。

- **扩展访问列表 (Extended Access List)** - 从**扩展访问列表 (Extended Access List)**下拉列表中，选择扩展 ACL 或点击 **添加**（+） 创建新的扩展 ACL。请参阅配置扩展 ACL 对象，第 975 页了解相关程序。

步骤 5 点击**确定**以保存访问组配置。

配置 IGMP 静态组

有时，组成员无法在组中报告其成员身份，或者网络段上没有组的成员，但仍希望将该组的组播流量发送到该网络段。您可以通过配置静态加入的 IGMP 组将该组的组播流量发送到网段。使用此方法时，威胁防御设备不会接受数据包本身，只会转发它们。因此，此方法可用于快速切换。传出接口显示在 IGMP 缓存中，但此接口不是组播组的成员。配置 IGMP 静态组时，请确保 威胁防御 是接口上的目标路由器。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **组播路由** > **IGMP**。

步骤 3 在**静态组 (Static Group)** 上，点击**添加 (Add)** 或**编辑 (Edit)**。

使用**添加 IGMP 静态组参数**对话框可以将组播组静态地分配给接口。使用**编辑 IGMP 静态组参数**对话框可以更改现有的静态组分配。

步骤 4 配置以下选项：

- 从**接口**下拉列表中，选择要向其静态分配组播组的接口。如果编辑的是现有条目，则无法更改此值。
- 从**组播组**下拉列表中，选择要为其分配接口的组播组，或点击 **添加**（+） 创建新的组播组。有关过程，请参阅创建网络对象。

步骤 5 点击**确定**以保存静态组配置。

配置 IGMP 加入组

您可以将接口配置成为组播组的成员。配置 威胁防御设备加入组播组会使上游路由器维护该组的组播路由表信息，并保持该组的路径处于活动状态。配置 IGMP 加入组时，请确保 威胁防御 是接口上的目标路由器 (DR)。

注释 如果要将特定组的组播数据包转发给接口，且无需 威胁防御设备将这些数据包接受为该组的一部分，请参阅配置 IGMP 静态组， 第 931 页。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **组播路由** > **IGMP**。

步骤 3 在**加入组 (Join Group)** 上，点击**添加 (Add)** 或**编辑 (Add)**。

使用**添加 IGMP 加入组参数**对话框可以将 威胁防御设备配置为组播组的成员。使用**编辑 IGMP 加入组参数**对话框可更改现有参数。

步骤 4 配置以下选项：

- 从**接口**下拉列表中，选择要作为组播组成员的接口。如果编辑的是现有条目，则无法更改此值。
- 从**加入组 (Join Group)** 下拉列表中，选择要为其分配接口的组播组，或点击**加号**创建新的组播组。有关过程，请参阅创建网络对象。

配置 PIM 功能

路由器使用 PIM 来维护转发表，以便用于转发组播图。如果在 Secure Firewall Threat Defense 上启用组播路由，PIM 和 IGMP 将会在所有接口上自动启用。

注释 PAT 不支持 PIM。PIM 协议不使用端口，PAT 只能与使用端口的协议配合使用。

本节介绍如何配置可选的 PIM 设置。

过程

步骤 1 配置 PIM 协议， 第 933 页

步骤 2 配置 PIM 邻居过滤器， 第 933 页

步骤 3 配置 PIM 双向邻居过滤器， 第 934 页

步骤 4 配置 PIM 交汇点， 第 935 页

步骤 5 配置 PIM 路由树， 第 936 页

步骤 6 配置 PIM 请求筛选器， 第 937 页

步骤 7 配置组播边界过滤器，第 939 页

配置 PIM 协议

可以在特定接口上启用或禁用 PIM。

还可以配置指定的路由器 (DR) 优先级。指定路由器 (DR) 负责将 PIM 注册消息、加入消息和删除消息发送到 RP。如果网段上有多个组播路由器，将会根据 DR 优先级来选择 DR。如果多台设备具有同样的 DR 优先级，则具有最高 IP 地址的设备将会成为 DR。默认情况下，威胁防御设备 的 DR 优先级为 1。

路由器查询消息用于选择 PIM DR。PIM DR 负责发送路由器查询消息。默认情况下，每隔 30 秒发送一次路由器查询消息。此外，威胁防御设备每隔 60 秒发送一次 PIM 加入消息或删除消息。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **组播路由** > **PIM**。

步骤 3 在**协议**上，点击**添加**或**编辑**。

使用**添加 PIM 参数**对话框可以向接口添加新的 PIM 参数。使用**编辑 PIM 参数**对话框可以更改现有的参数。

步骤 4 配置以下选项：

- **接口** - 从下拉列表中，选择要为其配置 PIM 协议的接口。
- **启用 PIM** - 选中该复选框以启用 PIM。
- **DR 优先级** - 所选接口的 DR 值。子网上具有最高 DR 优先级的路由器将成为指定路由器。有效值范围为 0 到 4294967294。默认 DR 优先级为 1。将此值设置为 0 会使 威胁防御 设备接口没有资格成为指定路由器。
- **呼叫间隔** - 接口发送 PIM 呼叫消息的时间间隔（以秒为单位）。范围为 1 到 3600。默认值为 30。
- **加入删除间隔** - 接口发送 PIM 加入和删除通告的间隔（以秒为单位）。范围为 10 到 600。默认值为 60。

步骤 5 点击**确定**以保存 PIM 协议配置。

配置 PIM 邻居过滤器

您可以定义可成为 PIM 邻居的路由器。通过筛选可成为 PIM 邻居的路由器，可以实现以下目的：

- 防止未授权的路由器成为 PIM 邻居。
- 防止连接的末节路由器加入到 PIM。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **多播路由** > **PIM**。

步骤 3 在**邻居过滤器 (Neighbor Filter)** 上，点击**添加 (Add)** 或**编辑 (Edit)**。

使用**添加 PIM 邻居过滤器**对话框将新的 PIM 邻居筛选器添加到接口。使用**编辑 PIM 邻居过滤器**对话框更改现有参数。

步骤 4 配置以下选项：

- 从**接口**下拉列表中，选择要向其添加 PIM 邻居过滤器的接口。
- **标准访问列表 (Standard Access List)** - 从**标准访问列表 (Standard Access List)**下拉列表中，选择标准 ACL 或点击 **添加**（＋） 以创建新的标准 ACL。请参阅配置标准 ACL 对象，第 977 页了解相关程序。

  注释 在**添加标准访问列表条目**对话框上选择**允许**可以使组播组通告通过该接口。选择**阻止**将会禁止指定的组播组通告通过接口。在接口上配置组播边界时，会阻止所有的组播流量通过接口，除非使用邻居过滤器条目允许通过。

步骤 5 点击**确定**保存 PIM 邻居过滤器配置。

配置 PIM 双向邻居过滤器

PIM 双向邻居过滤器是定义可参与指定转发器 (DF) 选择的邻居设备的 ACL。如果接口未配置 PIM 双向邻居过滤器，则没有限制。如果配置了 PIM 双向邻居过滤器，则只有 ACL 允许的邻居可参与 DF 选择过程。

双向 PIM 允许组播路由器保持减少的状态信息。要选择 DF，必须双向启用分片中的所有组播路由器。

如果启用了 PIM 双向邻居过滤器，ACL 允许的路由器将被视为具有双向功能。因此，以下说法均是正确的：

- 如果一个获允许的邻居不支双向模式，将不会发生 DF 选择。
- 如果一个被拒绝的邻居支持双向模式，将不会发生 DF 选择。
- 如果一个被拒绝的邻居不支持双向模式，可能会发生 DF 选择。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**组播路由** > **PIM**。

步骤 3 在**双向邻居过滤器 (Bidirectional Neighbor Filter)** 上，点击**添加 (Add)** 或**编辑 (Edit)**。

使用**添加 PIM 双向邻居过滤器**对话框可以为 PIM 双向邻居过滤器 ACL 创建 ACL 条目。使用**编辑 BFD 双向邻居过滤器**对话框可更改现有的参数。

步骤 4 配置以下选项：

- 从**接口**下拉列表中，选择要配置 PIM 双向邻居过滤器 ACL 条目的接口。
- **标准访问列表 (Standard Access List)** - 从**标准访问列表 (Standard Access List)**下拉列表中，选择标准 ACL 或点击 **添加**（+） 以创建新的标准 ACL。请参阅配置标准 ACL 对象，第 977 页了解相关程序。

  注释 在**添加标准访问列表条目**对话框上选择**允许**可以使指定的设备参与 DR 选择过程。选择**阻止**可阻止指定设备参与 DR 选择过程。

步骤 5 点击**确定**以保存 PIM 双向邻居过滤器配置。

配置 PIM 交汇点

可以将 威胁防御设备配置为用作多个组的 RP。ACL 中指定的组范围确定 PIM RP 组映射。如果未指定 ACL，则一个组的 RP 将应用于整个组播组范围 (224.0.0.0/4)。有关双向 PIM 的更多信息，请参阅组播双向 PIM，第 925 页。

以下限制适用于 RP：

- 一个 RP 地址不能用两次。
- 不能为多个 RP 指定所有组。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 依次选择**路由** > **组播路由** > **PIM**。

步骤 3 在**交汇点 (Rendezvous Points)** 选项卡上，点击**添加 (Add)** 或**编辑 (Edit)**。

使用**添加交汇点**对话框为“交汇点”表创建新条目。使用**编辑交汇点**对话框以更改现有参数。

步骤 4 配置以下选项：

- 从**交汇点 IP 地址 (Rendezvous Point IP address)** 下拉列表中，选择希望添加为 RP 的 IP 地址，或者点击 **添加**（+） 以创建新网络对象。请参阅创建网络对象了解相关程序。
- 如果指定的组播组要在双向模式下运行，请选中 **Use bi-directional forwarding** 复选框。在双向模式下，如果 威胁防御设备接收组播数据包，且没有直连成员或PIM邻居，则会将删除消息发送回源。
- 选择**将此 RP 用于所有组播组 (Use this RP for all Multicast Groups)** 以便将指定的 RP 用于该接口上的所有组播组。
- 选择**将此 RP 用于下面指定的所有组播组 (Use this RP for all Multicast Groups as specified below)**，以指定组播组与指定 RP 一起使用，然后从**标准访问列表 (Standard Access List)** 下拉列表中，选择标准 ACL，或者点击 **添加**（+） 以创建新的标准 ACL。请参阅配置标准 ACL 对象，第 977 页了解相关程序。

步骤 5 点击**确定**以保存交汇点配置。

配置 PIM 路由树

默认情况下，PIM 叶子路由器在第一个数据包从新源到达后会立即加入到最短路径树。此方法可降低延迟，但需要的内存比共享树多。您可以将 威胁防御设备配置为对于所有组播组或仅对于特定组播地址加入到最短路径树或者使用共享树。

最短路径树用于未在 Multicast Groups 表中指定的任何组。“组播组”表显示与共享树配合使用的组播组。表条目按自上而下的顺序进行处理。您可以通过以下方法来创建包含一系列组播组但不包含该系列中特定组的条目：将特定组的拒绝规则放置在表的顶部，并将该系列组播组的允许规则放置在拒绝语句下面。

注释 这种行为称为最短路径状态切换 (SPT)。建议您始终使用“共享树”选项。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **组播路由** > **PIM**。

步骤 3 在**路由树 (Route Tree)** 上，选择路由树的路径：

- 点击**最短路径 (Shortest Path)** 可为所有组播组使用最短路径树。
- 点击**共享树 (Shared Tree)** 可为所有组播组使用共享树。
- 点击**提到的以下组的共享树 (Shared tree for below mentioned group)** 以指定在“组播组”表中指定的组，然后从**标准访问列表 (Standard Access List)** 下拉列表中选择一个标准 ACL 或点击 **添加**（+） 以创建新的标准 ACL。请参阅配置标准 ACL 对象，第 977 页了解相关程序。

步骤 4 点击**确定**以保存路由树配置。

配置 PIM 请求筛选器

当 威胁防御设备作为 RP 时，您可以禁止特定的组播源注册到该设备，以防止未授权的源注册到 RP。您可以定义 威胁防御设备从其接受 PIM 寄存器消息的组播源。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **组播路由** > **PIM**。

步骤 3 在**请求筛选器 (Request Filter)** 上，定义允许在 威胁防御设备充当 RP 时向其注册的组播源：

- 从**筛选 PIM 寄存器消息使用:** 下拉列表中选择**无**、**访问列表**或**路由映射**。
- 如果从下拉列表中选择**访问列表 (Access List)**，请选择扩展 ACL 或点击 **添加**（+） 以创建新的扩展 ACL。请参阅配置扩展 ACL 对象，第 975 页了解相关程序。

  注释　在**添加扩展访问列表项 (Add Extended Access List Entry)** 对话框中，从下拉列表中选择**允许 (Allow)** 以创建允许指定的组播通信的指定源注册到 威胁防御 设备的规则，或选择**阻止 (Block)** 以创建阻止指定的组播通信的指定源注册到设备的规则。

- 如果选择**路由地图 (Route Map)**，请从**路由地图 (Route Map)** 下拉列表中选择一个路由映射，或点击 **添加**（+） 以创建新的路由映射。有关过程请参阅创建网络对象。

步骤 4 点击**确定**以保存请求过滤配置。

将 Cisco Secure Firewall Threat Defense设备配置为候选自举路由器

可将 威胁防御设备配置为候选 BSR。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 依次选择**路由** > **组播路由** > **PIM**。

步骤 3 在**引导程序路由器 (Bootstrap Router)** 上，选中**将此 FTD 配置为候选自举路由器 (C-BSR) (Configure this FTD as a Candidate Bootstrap Router [C-BSR])** 复选框，以执行 C-BSR 设置。

a) 从**接口**下拉列表中，选择 威胁防御设备上要从其派生 BSR 地址以使其成为候选者的接口。

此接口必须使用 PIM 启用。

b) 在**散列掩码长度**字段中，输入将在调用散列函数之前与组地址进行与运算的掩码的长度（最多32位）。所有具有相同种子的组都将散列（对应）到同一RP。例如，如果此值为24，则组地址只有前 24 位起作用。这种情况允许您为多个组获取一个 RP。范围为 0 到 32。

c) 在**优先级**字段中，输入候选 BSR 的优先级。优先选择优先级高的 BSR。如果优先级值相同，则 IP 地址较大的路由器是 BSR。范围为 0 到 255。默认值为 0。

步骤 4 （可选）在**将此 FTD 配置为边界自举路由器 (BSR)** 部分中点击 **添加**（+），选择不会在其上发送或接收 PIM BSR 消息的接口。

- 从**接口**下拉列表中，选择不会在其上发送或接收 PIM BSR 消息的接口。

  RP 或 BSR 通告将被有效过滤，从而隔离两个域的 RP 信息交换。

- 选中**启用边界 BSR**复选框以启用 BSR。

步骤 5 点击**确定**以保存自举路由器配置。

配置组播路由

配置静态组播路由可以将组播流量与单播流量分隔开。例如，如果源和目标之间的路由不支持组播路由，可以通过如下方法来解决这个问题：使用GRE隧道在它们之间配置两个组播设备，并通过该隧道发送组播数据包。

使用 PIM 时，威胁防御设备期望用于接收数据包的接口和用于将单播数据包发送回到源的接口是同一个接口。在某些情况下（例如，绕过不支持组播路由的路由），您可能希望单播数据包和组播数据包使用不同的路径。

静态组播路由不能通告或重分布。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由 (Routing)** > **组播路由 (Multicast Routing)** > **组播路由 (Multicast Routes)** > **添加或编辑 (Add or Edit)**。

使用**添加组播路由**对话框可将新的组播路由添加到 威胁防御设备。使用**编辑组播路由**对话框可更改现有的组播路由。

步骤 3 从**源网络 (Source Network)** 下拉框中，选择一个现有网络或点击 **添加**（+） 以添加新网络。有关过程，请参阅创建网络对象。

步骤 4 要配置接口以转发路由，请点击**接口 (Interface)** 并配置以下选项：

- 从**源接口**下拉列表中，为组播路由选择传入接口。
- 从**输出接口/密集**下拉列表中，选择路由转发到的目标接口。

- 在**距离**字段中，输入组播路由的距离。范围为 0 到 255。

步骤 5 要配置 RPF 地址以转发路由，请点击**地址 (Address)** 并配置以下选项：

- 在 **RPF 地址**字段中，输入组播路由的 IP 地址。
- 在**距离**字段中，输入组播路由的距离，范围为 0 到 255。

步骤 6 点击**确定**以保存组播路由配置。

配置组播边界过滤器

地址范围定义了域边界，从而使具有 IP 地址相同的 RP 的域不会相互泄漏。可在大型域内的子网边界以及域与互联网之间的边界上执行范围界定。

可以在接口上为组播组地址设置管理权限界定的边界过滤器。IANA 已将 239.0.0.0 到 239.255.255.255 的组播地址范围指定为可使用管理性界定的地址。此地址范围可在不同组织管理的域中重复使用。此类地址被视为本地地址，而不是全局唯一地址。

标准ACL定义受影响地址的范围。在设置边界过滤器后，不允许组播数据包从任一方向流经边界。边界过滤器允许同一个组播组地址在不同的管理域中重复使用。

可在使用管理权限界定的边界配置、检查和过滤 Auto-RP 发现消息和通知消息。Auto-RP 数据包中被边界 ACL 拒绝的任意 Auto-RP 组范围通知都会被删除。仅在 Auto-RP 组范围中的所有地址获得边界 ACL 允许的情况下，Auto-RP 组范围通知才可以通过边界过滤器。如果有任何地址未获允许，在 Auto-RP 消息转发前，将会筛选整个组范围并将其从 Auto-RP 消息中删除。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 依次选择**路由** > **组播路由** > **组播边界过滤器**，然后点击**添加**或**编辑**。

使用**添加组播边界过滤器 (Add Multicast Boundary Filter)** 对话框向设备添加新的组播边界过滤器。使用**编辑组播边界过滤器**对话框更改现有参数。

可为使用管理权限界定的组播地址配置组播边界。组播边界限制组播数据包流，并允许在不同的管理域中重复使用相同的组播组地址。在接口上定义了组播边界后，只有过滤器ACL允许的组播流量可通过接口。

步骤 3 从**接口**下拉列表中，选择为其配置组播边界过滤器 ACL 的接口。

步骤 4 从**标准访问列表**下拉列表中，选择要使用的标准 ACL，或者点击 **添加**（+） 创建新的标准 ACL。请参阅配置标准 ACL 对象，第 977 页了解相关程序。

步骤 5 选中**删除 Auto-RP 数据包中被边界拒绝的任意 Auto-RP 组范围通知**复选框，从被边界 ACL 拒绝的源中过滤 Auto-RP 消息。如果未选中此复选框，则将允许所有 Auto-RP 消息通过。

步骤 6 点击**确定**，以保存组播边界过滤器配置。

第 41 章

策略型路由

本章介绍如何通过 管理中心 的策略型路由页面来配置 威胁防御 以支持策略型路由 (PBR)。以下部分介绍策略型路由、PBR 的准则和 PBR 的配置。

关于策略型路由

在传统路由中，数据包会根据目的 IP 地址进行路由。但是，在基于目标的路由系统中更改特定流量的路由是较为困难的。策略型路由 (PBR) 通过扩展和补充路由协议提供的现有机制来增强对路由的控制。

PBR 允许您设置 IP 优先。它还允许为某些流量指定路径，例如高成本链路上的优先级流量。通过 PBR，您可以定义基于目的网络以外的标准的路由，如源端口、目的地址、目的端口、协议、应用程序，或者这些对象的组合。

您可以使用 PBR 根据应用。此路由方法适用于大量设备访问大型网络部署中的应用和数据的场景。传统上，大型部署具有会将所有网络流量作为基于路由的 VPN 中的加密流量回传到集线器的拓扑。这些拓扑通常会导致诸如数据包延迟、带宽降低和数据丢包等问题。克服这些问题涉及高成本的复杂部署和管理。

PBR 策略让您能够安全地中断指定应用的流量。您可以在 Cisco Secure Firewall Management Center 用户界面中配置 PBR 策略，以允许直接访问应用。

为什么使用策略型路由

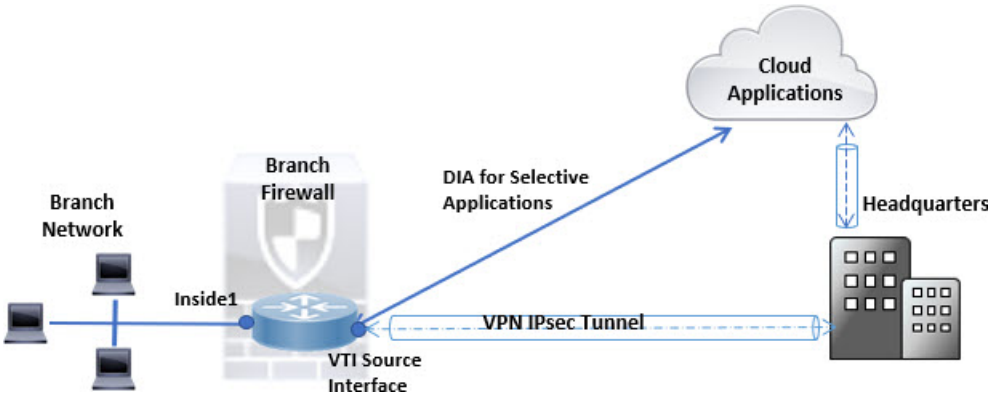
假设一家公司在不同位置之间有两条链路：一条是高带宽、低延迟、较为昂贵的链路，而另一条是低带宽、高延迟、不太昂贵的链路。使用传统路由协议时，高带宽链路将基于通过该链路的带宽、延迟或两者（使用 EIGRP 或 OSPF）特性所实现的指标节约而获得大部分（如果不是全部）跨该链

路发送的流量。通过PBR，您可以通过高带宽/低延迟的链路来路由优先级较高的流量，而通过低带宽/高延迟链路发送其他所有流量。

以下是您可以使用策略型路由的几种场景：

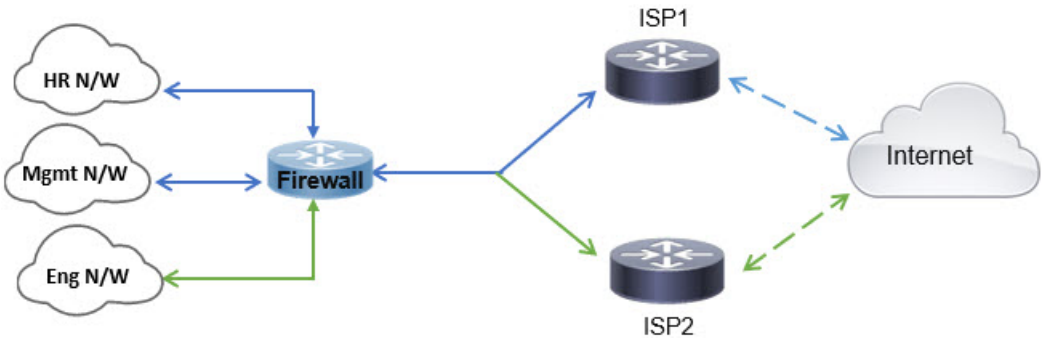
直接互联网接入

在此拓扑中，来自分支机构的应用流量可以被直接路由到互联网，而不是通过连接到总部的VPN隧道。该分支机构 威胁防御 配置了互联网出口点，并在入口接口（内部*1*）上应用PBR 策略，以便根据 ACL 中定义的应用来识别流量。相应地，流量会通过出口接口直接转发到互联网或 IPsec VPN 隧道。



同等访问权限和源敏感路由

在此拓扑中，来自 HR 和管理管理网络的流量可配置为通过 ISP-1，来自工程网络的流量可配置为通过 ISP-2。因此，策略型路由支持网络管理员提供同等访问权限和源敏感路由，如下所示。



负载分担

除 ECMP 负载均衡提供的动态负载共享功能外，网络管理员现在还可以实施策略来根据流量特征在多个路径之间分发流量。

例如，在同等访问和基于源的路由场景所描绘的拓扑中，管理员可以配置策略型路由来路由从人力资源网络至 ISP1 的流量和从工程网络至 ISP2 的流量，从而实现负载共享。

策略型路由的准则和限制

防火墙模式指导原则

PBR 仅在路由防火墙模式下受支持。

设备准则

- PBR 至 管理中心 的“策略型路由”(Policy Based Routing) 页面仅在 Cisco Secure Firewall Threat Defense 7.1 及更高版本的设备上受支持。虽然 Cisco Secure Firewall Management Center 版本 7.1 支持 7.1 之前版本的 威胁防御，但您无法使用策略型路由页面在此类设备上启用 PBR。
- FlexConfig 被用于在 管理中心 中为版本 7.1 之前的 威胁防御 配置 PBR。您仍然可以在所有版本中使用 FlexConfig 来配置 PBR。但是，对于入口接口，不能同时使用 FlexConfig 和 的策略型路由页面进行配置。PBR管理中心
- 不支持在集群设备上配置基于 PBR 策略的应用。

接口指导原则

- 只有属于全局虚拟路由器的路由接口和非管理专用接口才能被配置为入口或出口接口。
- 用户定义的虚拟路由器不支持 PBR。
- 只能在策略中定义具有逻辑名称的接口。
- 静态 VTI 只能被配置为出口接口。
- 在继续进行配置之前，请确保每个会话的入口和出口流量流经同一面向 ISP 的接口，以避免路由不对称导致的意外行为，尤其是在使用 NAT 和 VPN 时。

IPv6 支持

PBR 支持 IPv6。

基于应用的 PBR 和 DNS 配置

- 基于应用的 PBR 使用 DNS 监听进行应用检测。仅当 DNS 请求以明文格式通过 威胁防御 时，应用检测才会成功； DNS 流量不会被加密。
- 您必须配置信任的 DNS 服务器。

有关配置 DNS 服务器的详细信息，请参阅配置 DNS，第 617 页。

PBR 策略不适用于初期流量

注释 初期连接是指源与目标之间尚未完成必要握手的连接。

在添加新的内部接口并使用唯一地址池来创建新的VPN策略时，PBR将应用于与新客户端池的源匹配的外部接口。因此，PBR 会将流量从客户端发送到新接口上的下一跳。但是，PBR 不会涉及从尚未与新内部接口建立连接的主机到客户端的返回流量。因此，从主机到VPN客户端的返回流量（具体而言，VPN 客户端响应）会由于缺少有效路由而被丢弃。必须在内部接口上配置具有更高指标的加权静态路由。

其他规定

- 路由映射的所有现有配置限制和局限性都将继续适用。
- 在为策略匹配条件定义ACL时，您可以从预定义应用列表中选择多个应用，以形成访问控制条目 (ACE)。在 威胁防御 中，预定义应用会被作为网络服务对象进行存储，而应用组会作为网络服务组 (NSG) 进行存储。应用或网络服务组会通过第一个数据包分类来检测。目前，您无法添加或修改预定义应用列表。

路径监控

路径监控（在接口上配置）会派生指标，例如往返时间 (RTT)、抖动、平均意见得分 (MOS) 和每个接口的丢包。这些指标会被用于确定路由 PBR 流量的最佳路径。

接口上的指标会使用 ICMP 探测消息动态收集到接口的默认网关或指定的远程对等体。

默认监控计时器

对于指标收集和监控，使用以下计时器：

- 接口监控的平均间隔时间为 30 秒。此间隔时间表示探测平均值的频率。
- 接口监控器更新间隔时间为30秒。此时间间隔表示计算所收集的值的平均值并使其可用于PBR以确定最佳路由路径的频率。
- ICMP 的接口监控器探测间隔时间为一秒。此间隔时间表示发送 ICMP ping 的频率。

注释 您不能配置或修改任何计时器的间隔时间。

PBR 和路径监控

在 PBR 中，流量通常会根据出口接口上配置的优先级值（接口成本）进行转发。从管理中心版本 7.2，PBR 使用基于 IP 的路径监控来收集出口接口的性能指标（RTT、抖动、丢包和 MOS）。PBR

会使用指标来确定转发流量的最佳路径（出口接口）。路径监控会定期向 PBR 通知其指标已更改的受监控接口。PBR 会从路径监控数据库中检索受监控接口的最新指标值，并更新数据路径。

您必须为接口启用路径监控并配置监控类型。PBR 策略页面允许您为确定路径指定所需的指标。参阅配置基于策略的路由策略，第 946 页。

配置路径监控设置

PBR 策略依靠灵活的指标（例如往返时间（RTT），抖动，平均意见评分（MOS）和接口丢包）来确定流量的最佳路由路径。路径监控收集指定接口上的这些指标。在**接口 (Interfaces)** 页面上，可以使用路径监控设置配置接口，以发送用于指标收集的 ICMP 探测。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 设备的 **编辑**（）。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑**（）。

步骤 3 点击 **路径监控 (Path Monitoring)** 选项卡。

步骤 4 点击 **启用路径监控** 复选框。

步骤 5 从 **监控类型** 下拉列表中，选择相关选项：

- **自动**-将 ICMP 探测发送到接口的 IPv4 默认网关。如果 IPv4 网关不存在，路径监控会将探测发送到接口的 IPv6 默认网关。
- **对等体 IPv4 (Peer IPv4)** - 将 ICMP 探测发送到指定的对等 IPv4 地址（下一跳 IP）以进行监控。如果选择此选项，请在**要监控的对等体 (Peer IP To Monitor)** 字段中输入 IPv4 地址。
- **对等体 (Peer IPv6)** - 将 ICMP 探测发送到指定的对等 IPv6 地址（下一跳 IP）以进行监控。如果选择此选项，请在**要监控的对等体 (Peer IP To Monitor)** 字段中输入 IPv6 地址。
- **自动 IPv4**-将 ICMP 探测发送到接口的默认 IPv4 网关。
- **自动 IPv6**-将 ICMP 探测发送到接口的默认 IPv6 网关。

注释
- 自动选项不适用于 VTI 接口。您必须指定对等体地址。
- 只有一个下一跳被监控到目的地。也就是说，不能为一个接口指定多个对等体地址。

步骤 6 点击 **确认**，要保存设置，点击 **保存**。

配置基于策略的路由策略

您可以通过指定入口接口，匹配条件（扩展访问控制列表）和出口接口，在“策略型路由”页面中配置 PBR 策略。

开始之前

要使用路径监控指标配置出口接口上的流量转发优先级，必须为接口配置路径监控设置。请参阅配置路径监控设置，第 945 页。

过程

步骤 1 依次选择 **设备** > **设备管理**，并且编辑 威胁防御 设备。

步骤 2 点击**路由**。

步骤 3 点击**策略型路由**。

“策略型路由”页面显示配置的策略。网格显示入口接口列表以及策略型路由访问列表和出口接口的组合。

步骤 4 要配置策略，请点击 **添加**。

步骤 5 在 **添加策略型路由** 对话框中，从下拉列表中选择 **入口接口** 。

注释 下拉列表中仅列出具有逻辑名称且属于全局虚拟路由器的接口。

步骤 6 要在策略中指定匹配条件和转发操作，请点击 **添加**。

步骤 7 在 **添加转发操作** 对话框中，执行以下操作：

a) 从 **Match ACL** 下拉列表中，选择扩展访问控制列表对象。您可以预定义 ACL 对象（请参阅配置扩展 ACL 对象，第 975 页）或点击 **添加**（+）图标创建对象。在**新建扩展访问列表对象 (New Extended Access List Object)** 框中，输入名称，点击**添加 (Add)** 以打开**添加扩展访问列表条目 (Add Extended Access List Entry)** 对话框，您可以在其中为 PBR 策略定义网络，端口、或应用匹配条件。

注释 不能在 ACE 中同时定义应用地址和目标地址。

b) 从 **发送至** 下拉列表：

- 要选择配置的接口，请选择 **出口接口**。
- 要指定 IPv4 / IPv6 下一跳地址，请选择 **IP 地址**。继续步骤7.e，第 947 页

c) 如果已选择 **出口接口**，请从 **接口顺序** 下拉列表中选择相关选项：

- **按优先级**-按接口的优先级转发流量。流量首先路由到具有最低优先级值的接口。当接口不可用时，流量会转发到具有下一个最低优先级值的接口。例如，假设 *Gig0/1*、 *Gig0/2*和

Gig0/3 分别配置了优先级值 *0*、*1*和 *2* 。流量被转发到 *Gig0/1*。如果 *Gig0/1* 变得不可用，流量将被转发到 *Gig0/2*。

注释 要配置接口的优先级，请点击策略型路由页面上的**配置接口优先级**。在对话框中，提供接口的优先级编号，然后点击 **保存**。您还可以在 配置路由模式接口中配置接口的优先级。

当所有接口的优先级值相同时，流量在接口之间均衡。

- **按顺序**-按此处指定的接口顺序转发流量。例如，假设 *Gig0/1*、 *Gig0/2*和 *Gig0/3* 是按以下顺序选择的，*Gig0/2*、 *Gig0/3*、 *Gig0/1*。流量先转发到 *Gig0/2*，然后转发到 *Gig0/3*，无论其优先级值如何。
- **按最小抖动**-流量转发到抖动值最低的接口。您需要在接口上启用路径监控，以使 PBR 获取抖动值。
- **按最大平均意见评分**-按流量转发到具有最大平均意见评分（MOS）的接口。您需要在接口上启用路径监控，以便 PBR 获取 MOS 值。
- **按最小往返时间 (By Minimal Round Trip Time)** - 将流量转发到具有最小往返时间 (RTT) 的接口。您需要在接口上启用路径监控，以便 PBR 获取 RTT 值。
- **按最小数据包丢失 (By Minimal Packet Loss)** - 将流量转发到具有最小数据包丢失的接口。您需要在接口上启用路径监控，以使 PBR 获取丢包值。

d) 在 **可用接口框** 中，列出所有接口及其优先级值。从接口列表中，点击 **添加**（⊕）按钮以添加到所选出口接口。继续步骤 7.f，第 947 页

e) 如果选择了 **IP 地址 (IP Address)**，请在 **IPv4 地址 (IPv4 Addresses)** 和 **IPv6 地址 (IPv6 Addresses)** 字段中输入用逗号分隔的 IP 地址。流量根据指定 IP 地址的顺序转发。

f) 点击**保存 (Save)**。

步骤 8 要保存策略，点击 **保存** 和 **部署**。

威胁防御 使用 ACL 来匹配流量，并对流量执行路由操作。典型地，配置指定用于进行匹配的 ACL 的路由映射，然后为该流量指定一个或多个操作。通过使用路径监控，PBR 现在可以选择最佳出口接口来路由流量。最后，将路由映射与接口相关联，在该接口上要对所有传入流量应用 PBR 。

添加路径监控控制面板

要查看路径监控指标，必须将路径监控控制面板添加到设备的“运行状况监控”(Health Monitoring) 页面。

过程

步骤 1 选择**系统 (System)** > **运行状况 (Health)** > **监控 (Monitor)**。

步骤 2 选择设备，然后点击**添加控制面板 (Add Dashboard)**。

步骤 3 在**关联指标 (Correlate Metrics)** 对话框中，从下拉列表中选择**接口 - 路径指标 (Interface - Path Metrics)**。

步骤 4 点击**显示详细信息 (Show Details)** 链接，您可以在其中输入控制面板的自定义名称。默认情况下，系统会选择所有四个指标，以便在控制面板中显示为 Portlet。您可以通过点击**删除**（ ）来排除其中任何一项。

步骤 5 点击**保存 (Save)**。

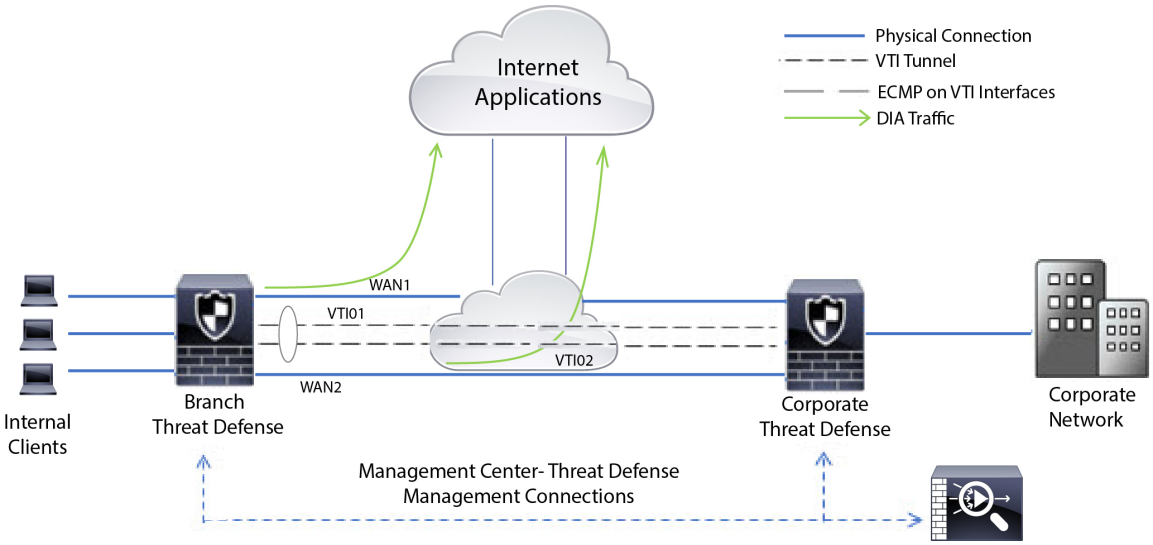
策略型路由的配置示例

假设一个典型的企业网络场景，其中所有分支机构网络流量都通过企业网络的基于路由的 VPN，并在需要时分流到外联网。通过企业网络访问处理日常运营的 Web 应用会导致巨大的网络扩展和维护成本。此示例说明了直接互联网接入的 PBR 配置程序。

下图描述了企业网络的拓扑。分支机构网络通过基于路由的 VPN 连接到企业网络。传统上，公司威胁防御 会被配置为处理分支机构的内部和外部流量。通过 PBR 策略，分支机构 威胁防御 会配置将特定流量路由到 WAN 网络而不是虚拟隧道的策略。其余流量会照常流经基于路由的 VPN。

此示例还说明了如何使用 ECMP 区域来配置 WAN 和 VTI 接口以实现负载均衡。

图 *128:* 在 管理中心 中的分支机构 威胁防御 上配置策略型路由



开始之前

此示例假定您已为 管理中心 中的分支机构 威胁防御 配置 WAN 和 VTI 接口。

过程

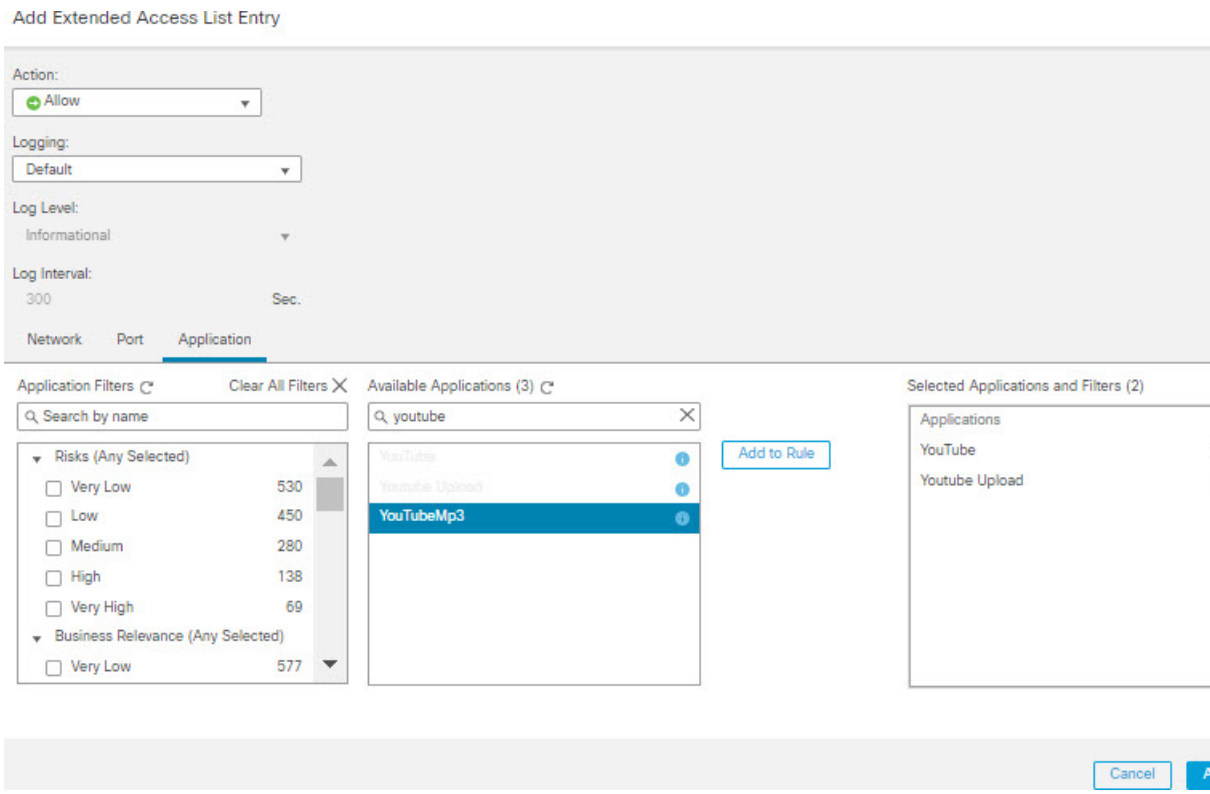
步骤 1 为分支机构 威胁防御 配置策略型路由，选择入口接口：

a) 依次选择 **设备** > **设备管理**，并且编辑 威胁防御 设备。
b) 选择**路由 (Routing)** > **策略型路由 (Policy Based Routing)**，然后在**策略型路由 (Policy Based Routing)** 页面上，点击**添加 (Add)**。
c) 在**添加策略型路由 (Add Policy Based Route)** 对话框中，从**入口接口 (Ingress Interface)** 下拉列表中选择内部 *1 (Inside 1)* 和内部 *2 (Inside 2)*。

步骤 2 指定匹配条件：

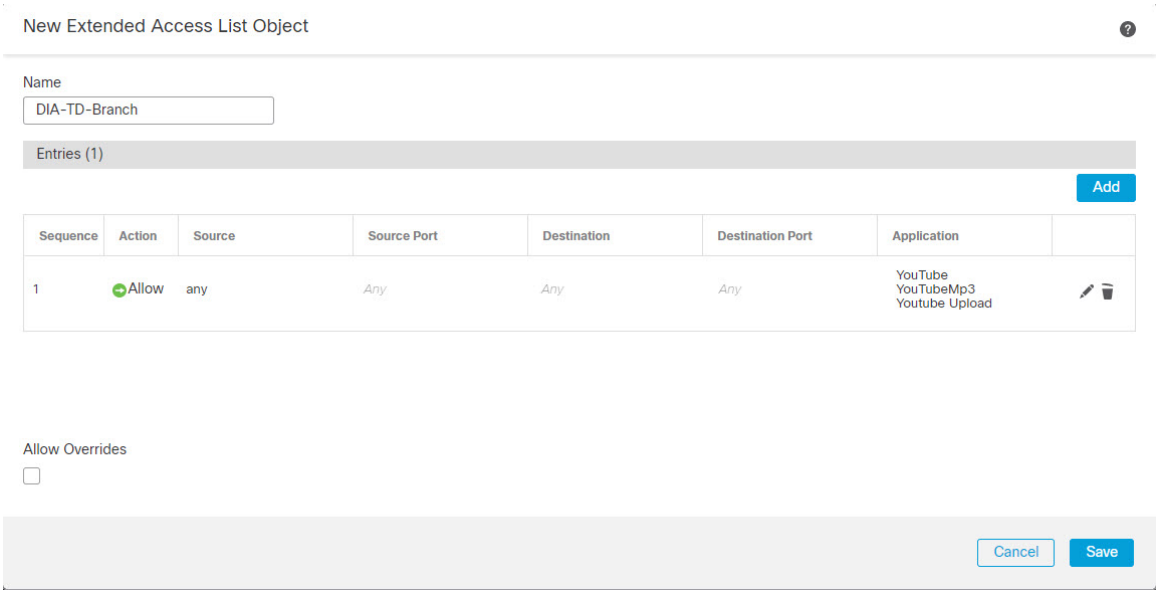
a) 点击**添加 (Add)**。
b) 要定义匹配条件，请点击 **添加**（ ） 按钮。
c) 在**新建扩展访问列表对象 (New Extended Access List Object)** 中，输入 ACL 的名称（例如 *DIA-FTD-Branch*），然后点击**添加 (Add)**。
d) 在**添加扩展访问列表条目 (Add Extended Access List Entry)** 对话框中，从**应用 (Application)** 选项卡中选择所需的基于 Web 的应用：

图 ***129:*** “应用” ***(Applications)*** 选项卡



在 威胁防御 上，ACL 中的应用组被配置为网络服务组，并且每个应用被配置为网络服务对象。

图 *130:* 扩展 *ACL*



e) 点击**保存 (Save)**。

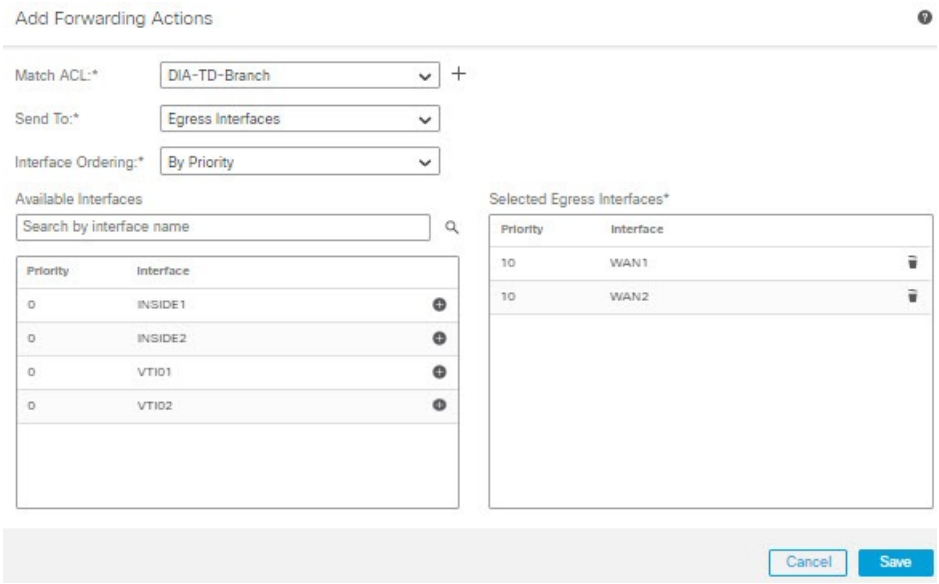
f) 从**匹配 ACL (Match ACL)** 下拉列表中选择 *DIA-FTD-Branch*。

步骤 3 指定出口接口：

a) 从**发送到 (Send To)** 和**接口排序 (Interface Ordering)** 下拉列表中，分别选择“出口接口”(Egress Interfaces) 和“按优先级”(By Priority)。

b) 在 Available Interfaces 下，点击相应接口名称的 按钮以添加 WAN1 和 WAN2：在**可用接口 (Available Interfaces)** 下，再次点击相应接口名称的 ⊕ 按钮以便添加 *WAN1* 和 *WAN2*：

图 *131:* 配置策略型路由



c) 点击**保存 (Save)**。

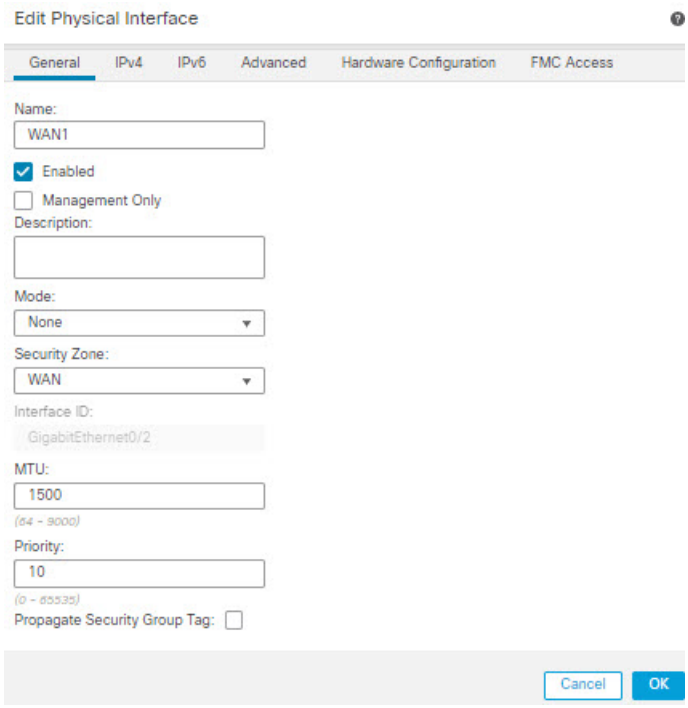
步骤 4 接口优先级配置：

您可以在**编辑物理接口 (Edit Physical Interface)** 页面或**策略型路由 (Policy Based Routing)** 页面（**配置接口优先级**）中设置接口的优先级值。在本示例中，将介绍“编辑物理接口”方法。

a) 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后编辑分支机构 威胁防御。

b) 设置接口的优先级。点击接口的**编辑 (Edit)**，然后输入优先级值：

图 *132:* 设置接口优先级



c) 点击**确定 (Ok)** 和**保存 (Save)**。

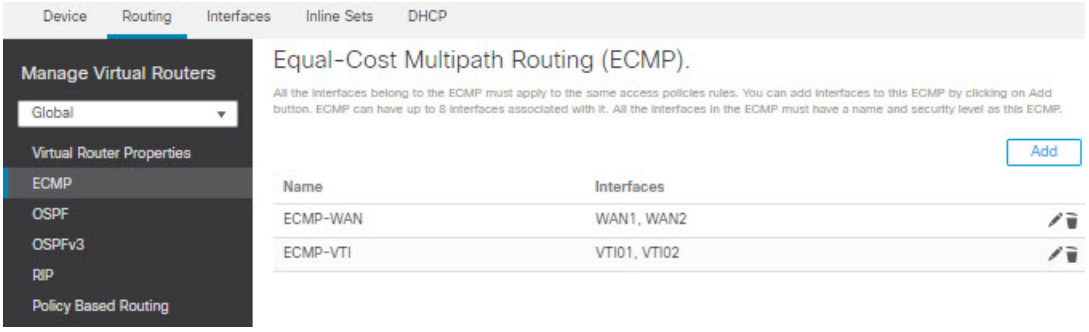
步骤 5 创建用于负载均衡的 ECMP 区域：

a) 在**路由 (Routing)** 页面中，点击 **ECMP**。

b) 要将接口关联到 ECMP 区域，请点击**添加 (Add)**。

c) 选择 *WAN1* 和 *WAN 2*，然后创建一个 ECMP 区域 — *ECMP-WAN*。同样，添加 *VTI01* 和 *VTI02*，然后创建一个 ECMP 区域 — *ECMP-VTI*：

图 *133:* 将接口与 ***ECMP*** 相关联

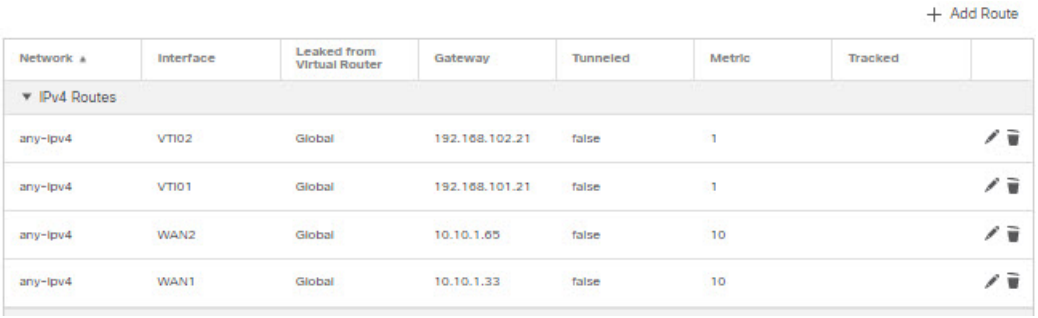


步骤 6 为区域接口配置静态路由以实现负载均衡：

a) 在**路由 (Routing)** 页面中，点击**静态路由 (Static Route)**。

b) 点击**添加 (Add)** 并为 *WAN1*、*WAN2*、*VTI01* 和 *VTI02* 指定静态路由。确保为属于相同 ECMP 区域的接口指定相同的指标值（步骤 5）：

图 *134:* 为 ***ECMP*** 区域接口配置静态路由



注释 确保区域接口具有相同的目的地址和指标，但网关地址不同。

步骤 7 在分支机构 威胁防御 的 WAN 对象上配置受信任的 DNS，以确保流量安全地流向互联网：

a) 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后在分支机构 威胁防御 上创建 DNS 策略。

b) 要指定受信任的 DNS，请点击**编辑 (Edit)** 以编辑策略，然后点击 **DNS**。

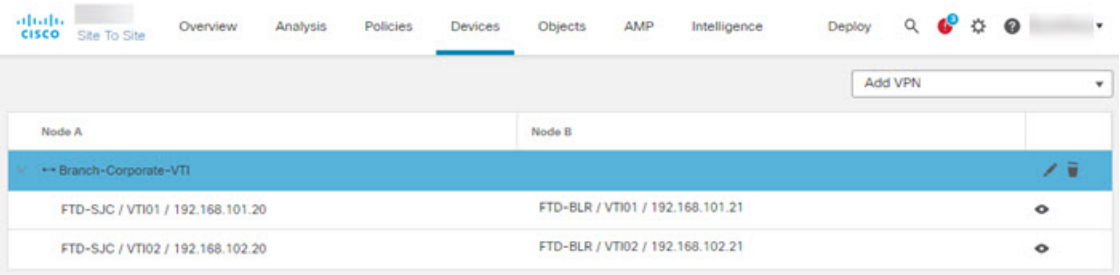
c) 要为 WAN 对象使用的 DNS 解析指定 DNS 服务器，请在 **DNS 设置 (DNS Settings)** 选项卡中提供 DNS 服务器组详细信息，然后从接口对象中选择 WAN。

d) 使用**受信任 DNS 服务器 (Trusted DNS Servers)** 选项卡为 DNS 解析提供您信任的特定 DNS 服务器。

步骤 8 **保存 (Save)** 和**部署 (Deploy)**。

来自分支机构内部网络 *INSIDE1* 或 *INSIDE2* 的任何 *YouTube* 相关访问请求都会被路由到 *WAN1* 或 *WAN2*，因为它们将与 *DIA-FTD-Branch* ACL 匹配。任何其他请求（例如 *google.com*）都会通过在站点间 VPN 设置中配置的 *VTI01* 或 *VTI02* 进行路由：

图 *135:* 站点间 *VPN*



如果配置了 ECMP，就可以无缝地平衡网络流量。

具有路径监控的 PBR 的配置示例

此示例详细介绍了为以下具有灵活指标的应用配置具有路径监控的 PBR：

- 具有抖动的音频或视频敏感应用（例如，WebEx Meetings）。
- 使用 RTT 的基于云的应用（例如 Office365）。
- 具有丢包的基于网络的访问控制（具有特定的源和目标）。

开始之前

1. 此示例假定您知道 PBR 的基本配置步骤。
2. 您已使用逻辑名称来配置入口和出口接口。在本示例中，入口接口命名为 *Inside1*，而出口接口命名为 *ISP01*、*ISP02* 和 *ISP03*。

过程

步骤 1 接口 *ISP01*、*ISP02* 和 *ISP03* 上的路径监控配置：

对于出口接口上的指标收集，您必须在它们上面启用并配置路径监控。

a) 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后编辑 威胁防御。
b) 在**接口 (Interfaces)** 选项卡下，编辑接口（在我们的示例中为 *ISP01*）
c) 点击**路径监控 (Path Monitoring)** 选项卡，选中**启用路径监控 (Enable Path Monitoring)** 复选框，然后指定监控类型（请参阅配置路径监控设置 ， 第 945 页）。
d) 点击**确定 (Ok)** 和**保存 (Save)**。
e) 重复相同的步骤并为 *ISP02* 和 *ISP03* 配置路径监控设置。

步骤 2 为组织 威胁防御 中的分支机构配置策略型路由，选择入口接口：

a) 依次选择 **设备** > **设备管理**，并且编辑 威胁防御 设备。
b) 选择**路由 (Routing)** > **策略型路由 (Policy Based Routing)**，然后在**策略型路由 (Policy Based Routing)** 页面上，点击**添加 (Add)**。

c) 在**添加策略型路由 (Add Policy Based Route)** 对话框中，从**入口接口 (Ingress Interface)** 下拉列表中选择内部 *1 (Inside 1)*。

步骤 3 指定匹配条件：

a) 点击**添加 (Add)**。

b) 要定义匹配条件，请点击 **添加**（ ） 按钮。

c) 在**新建扩展访问列表对象 (New Extended Access List Object)** 中，输入 ACL 的名称（例如 *PBR-WebEx*），然后点击**添加 (Add)**。

d) 在**添加扩展访问列表条目 (Add Extended Access List Entry)** 对话框中，从**应用 (Application)** 选项卡中选择所需的基于 Web 的应用（例如 WebEx 会议）。

记住 在 威胁防御上，ACL 中的应用组被配置为网络服务组，并且每个应用被配置为网络服务对象。

e) 点击**保存 (Save)**。

f) 从**匹配 ACL (Match ACL)** 下拉列表中选择 *PBR-WebEx*。

步骤 4 指定出口接口：

a) 在**发送到 (Send To)** 下拉列表中，选择“出口接口”(Egress Interfaces)。

b) 从**接口排序 (Interface Ordering)** 下拉列表中，选择“按最小抖动”(By Minimal Jitter)。

c) 在**可用接口 (Available Interfaces)** 下，点击相应接口名称对应的 **右箭头**（ ） 按钮，以便添加 *ISP01*、*ISP02* 和 *ISP03*。

d) 点击**保存 (Save)**。

步骤 5 重复步骤 2 和步骤 3，为同一接口 (*Inside1*) 创建 PBR，以便路由 Office365 和基于网络的访问控制流量：

a) 创建匹配条件对象（例如 *PBR-Office365*），然后从**应用 (Application)** 选项卡中选择 Office365 应用。

b) 从**接口排序 (Interface Ordering)** 下拉列表中，选择“按最短往返时间”(By Minimal Round Trip Time)。

c) 指定出口接口 *ISP01*、*ISP02* 和 *ISP03*，然后点击**保存 (Save)**。

d) 现在，创建匹配条件对象（例如 *PBR-networks*），并在**网络 (Network)** 选项卡中指定源接口和目标接口。

e) 从**接口排序 (Interface Ordering)** 下拉列表中，选择“按最小丢包”(By Minimal Packet Loss)。

f) 指定出口接口 *ISP01*、*ISP02* 和 *ISP03*，然后点击**保存 (Save)**。

步骤 6 **保存 (Save)** 和**部署 (Deploy)**。

步骤 7 要查看路径监控指标，请选择**设备 (Devices)** > **设备管理 (Device Management)**，然后在 **更多**（ ） 中点击**运行状况监控 (Health Monitor)**。要查看设备接口的指标详细信息，您必须添加路径指标控制面板。有关详细信息，请参阅添加路径监控控制面板 ， 第 947 页。

WebEx、Office365 和基于网络的 ACL 流量会通过从 *ISP01*、*ISP02* 和 *ISP03* 上收集的指标值得出的最佳路由进行转发。

第 XI 部分

对象和证书

第 42 章

对象管理

本章介绍如何管理可重用对象。

对象简介

为了提高灵活性和 Web 界面的易用性，Firepower 系统会使用命名对象，命名对象是将名称与值相关联的可重用配置。当您要使用该值时，可使用命名对象来替代。系统支持在 Web 界面中的不同位置使用这些对象，包括许多策略和规则、事件搜索、报告、控制面板等等。系统提供许多代表常用配置的预定义对象。

使用对象管理器创建和管理对象。许多使用对象的配置也允许您根据需要即时创建对象。您也可以使用对象管理器进行以下操作：

- 查看使用网络、端口、VLAN 或 URL 对象的策略、设置和其他对象；请参阅查看对象及其使用情况，第 964 页。
- 将对象分组，以用一个配置引用多个对象；请参阅对象组，第 966 页。
- 覆盖所选设备或所选域（在多域部署中）的对象值；请参阅对象覆盖，第 967 页。

编辑在活动策略中使用的对象后，必须重新部署更改的配置，才能使更改生效。您无法删除活动策略正在使用的对象。

注释 当且仅当某个对象用于分配到某个受管设备的策略中时，该对象才会在受管设备上予以配置。如果从分配到给定设备的所有策略中删除某个对象，则该对象也会从下一次部署的设备配置中被删除，对其进行的后续更改不会在设备配置中反映出来。

对象类型

下表列出了您可以在 Firepower 系统中创建的对象，并指示是否可以对每个对象类型进行分组或配置以允许覆盖。

对象类型	是否可分组？	是否允许覆盖？
网络	是	是
端口	是	是
接口： • 安全区 • 接口组	否	否

对象类型	是否可分组？	是否允许覆盖？
隧道区域	否	否
应用过滤器	否	否
VLAN 标记	是	是
外部属性：安全组标记 (SGT) 和动态对象	否	否
URL	是	是
地理定位	否	否
时间范围	否	否
变量集	否	否
安全情报：网络、DNS 和 URL 列表和源	否	否
Sinkhole	否	否
文件列表	否	否
密码套件列表	否	否
可分辨名称	是	否
公钥基础设施 (PKI)： • 内部和受信任 CA • 内部和外部证书	是	否
密钥链	否	是
DNS 服务器组	否	否
SLA 监控器	否	否
前缀列表：IPv4 和 IPv6	否	是
路由映射	否	是
访问列表：标准和扩展	否	是
AS 路径	否	是
社区列表	否	是
策略列表	否	是
FlexConfig：文本和 FlexConfig 对象	否	是

对象和多租户

在多域部署中，您可以在全局域和后代域中创建对象，只能在全局域中创建的安全组标记 (SGT) 对象除外。系统会显示在当前域中创建的对象，您可以对其进行编辑。它还会显示在祖先域中创建的对象，但您无法对其进行编辑，除了安全区域和接口组。

注释 因为安全区域和接口组与在分叶级别配置的设备接口绑定，后代域中的管理员可以查看并编辑在祖先域中创建的区域和组。子域用户可以在祖先区域和组中添加和删除接口，但无法删除或重命名区域/组。

对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

对于支持分组的对象，可以将当前域中的对象与从祖先域中继承的对象分到一组。

对象覆盖允许您定义某些类型对象的设备特定或域特定值，包括网络、端口、VLAN 标记和 URL。在多域部署中，可以为祖先域中的对象定义默认值，但允许后代域中的管理员为该对象添加覆盖值。

对象管理器

可以使用对象管理器创建和管理对象和对象组。

对象管理器每页显示 20 个对象或对象组。如果有超过 20 个任何类型的对象或对象组，请使用位于页面底部的导航链接查看其他页面。您还可以转到特定页或点击 **刷新** （ ） 来刷新视图。

默认情况下，页面会按名称的字母顺序列示对象和对象组。您可以按名称或值对页面上的对象进行过滤。

正在导入对象

对象可以通过逗号分隔值文件导入。一次最多可以导入1000个对象。逗号分隔值文件的内容应依照特定的格式。每种对象类型的格式不同。只能导入几种类型的对象。请参阅下表以了解支持的对象类型以及相应的规则。

对象类型	规则

单个对象	• 列标题必须以大写字母表示。
	• 文件必须包含以下列标题：
	  • 名称
	  • DN
	• 要导入条目，必须同时输入 NAME 和 DN 列条目。
	• 您可以将单个对象直接导入到现有的可分辨名称对象组中。

网络对象	• 列标题必须以大写字母表示。
	• 文件必须包含以下列标题：
	  • 名称
	  • DESCRIPTION
	  • TYPE
	  • 值
	  • 查询
	• 必须提供 NAME 和 VALUE 列条目才能导入主机、范围或网络对象类型的条目。
	• 对于 FQDN 对象，TYPE 列条目必须提及“fqdn”，而 LOOKUP 列条目必须指定为“ipv4”、“ipv6”或“ipv4_ipv6”。
	• 如果 FQDN 对象的 LOOKUP 列条目中未提供内容，则要使用 ipv4_ipv6 字段值来保存该对象。

对象类型	规则

Port	• 列标题必须以大写字母表示。
	• 文件必须包含以下列标题：
	  • 名称
	  • PROTOCOL
	  • PORT
	  • ICMPCODE
	  • ICMPTYPE
	• NAME 列条目为必填。
	• 对于“tcp”和“udp”协议类型，PORT 列条目为必填。
	• 对于“icmp”和“icmp6”协议类型，ICMPCODE 和 ICMPTYPE 列条目为必填。

URL	• 列标题必须以大写字母表示。
	• 文件必须包含以下列标题：
	  • 名称
	  • DESCRIPTION
	  • URL
	• 必须提供 NAME 和 URL 列条目才能导入条目。

VLAN 标签	• 列标题必须以大写字母表示。
	• 文件必须包含以下列标题：
	  • 名称
	  • DESCRIPTION
	  • 标签
	• 必须提供 NAME 和 TAG 列条目才能导入条目。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从左侧窗格中选择以下对象类型之一：

- **可分辨名称 (Distinguished Name)** > **单个对象 (Individual Objects)** >
- **网络对象**
- **端口**
- **URL**
- **VLAN 标签**

步骤 3 从**添加 [对象类型] (Add [Object Type])** 下拉列表中选择**导入对象 (Import Object)**。

注释 如果您在上一步中选择了**单个对象 (Individual Objects)**，请点击**导入 (Import)**。

步骤 4 点击**浏览 (Browse)**。

步骤 5 在系统上找到并选择以逗号分隔的文件。

步骤 6 点击 **Open**。

注释 导入**可分辨名称**对象时，可以选中**将导入的可分辨名称对象添加到下面的对象组 (Add imported Distinguished Name objects to the below object group)** 复选框，然后从下拉框中选择组名称，以将对象直接导入现有的可分辨名称对象组。

步骤 7 点击**导入 (Import)**。

编辑对象

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从列表中选择对象类型；请参阅对象简介，第 958 页。

步骤 3 点击要编辑的对象旁边的 **编辑**（）。

如果显示**视图**（），则表明对象属于祖先域且已配置为不允许覆盖，或者您没有修改对象的权限。

步骤 4 根据需要修改对象设置。

步骤 5 如果编辑的是变量集，请管理变量集中的变量；请参阅管理变量，第 1054 页。

步骤 6 对于可以配置为允许覆盖的对象：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 969 页。只可以为属于当前域的对象更改此设置。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 969 页。

步骤 7 点击**保存 (Save)**。

步骤 8 如果编辑的是变量集，并且该变量集正在被一个访问控制策略使用，请点击**是 (Yes)** 以确认要保存更改。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

查看对象及其使用情况

您可以在“对象管理”(Object Management) 页面上查看对象的使用详细信息。管理中心 为许多对象类型提供此功能。但是，某些对象类型不受支持。

注释 在多域部署中，您可以查看任何其他域中的对象。但是，要查看后代域中的对象使用情况，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 选择以下支持的对象类型之一：

- 访问列表 > 扩展
- 访问列表 > 标准
- AS 路径
- 社区列表
- 接口
- 网络
- 策略列表
- Port
- 前缀列表 > IPv4 前缀列表
- 前缀列表 > IPv6 前缀列表

- 路由映射
- SLA 监控器
- URL
- VLAN 标签

步骤 3 点击对象旁边的 **查找使用情况** （  ） 图标。

“对象使用情况”(Object Usage) 窗口会显示使用对象的所有策略、对象和其他设置的列表。点击列出的任何项目，了解有关对象使用情况的详细信息。对于会用到对象的策略和一些其他设置，您可以点击相应的链接以访问相应的 UI 页面。

过滤对象或对象组

在多域部署中，系统会显示在当前域和祖先域中创建的对象，您可以对其进行过滤。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 在**过滤 (Filter)** 字段中输入过滤器条件。

页面会在您键入内容时进行更新，以显示匹配的项目。

您可以使用以下通配符：

- 星号 (*) 匹配零或重复出现的一个字符。
- 脱字符 (^) 匹配字符串开头的内容。
- 美元符号 ($) 匹配字符串结尾的内容。

步骤 3 选中**显示未使用的对象 (Show Unused Object)** 复选框，以查看系统中任何位置未使用的对象和对象组。

注释
- 如果对象是未使用的对象组的一部分，则该对象会被视为已使用。但是，如果选中**显示未使用的对象 (Show Unused Object)** 复选框，则会显示未使用的对象组。
- **显示未使用的对象 (Show Unused Object)** 复选框仅适用于网络、端口、URL 和 VLAN 标记对象类型。

对象组

将对象分组使得可以引用带有单个配置的多个对象。系统允许在 Web 界面中互用对象和对象组。例如，在任何要使用端口对象的地方，也可以使用端口对象组。

可以将网络、端口、VLAN 标记、URL 和 PKI 对象分组。网络对象组可以嵌套，即您可以将一个网络对象组添加到另一个网络对象组中，最高可达 10 个级别。

相同类型的对象和对象组不能具有相同的名称。在多域部署中，对象组的名称在域层次结构中必须是唯一的。请注意，系统可能会识别出与您在当前域中无法查看的对象组名称的冲突。

编辑策略中使用的对象组（例如，访问控制策略中使用的网络对象组）时，您必须重新部署已更改的配置以使更改生效。

删除组不会删除组中的对象，只会删除对象之间的相关性。此外，您也无法删除活动策略中正在使用的组。例如，无法删除用于已保存访问控制策略中的 VLAN 条件的 VLAN 标记组。

对可重用对象进行分组

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

可以将当前域中的对象与从祖先域中继承的对象分到一组。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 如果要分组的对象类型为**网络 (Network)**、**端口 (Port)**、**URL** 或 **VLAN 标记 (VLAN Tag)**：

a) 从对象类型列表中选择对象类型。

b) 从**添加（对象类型）(Add [Object Type])** 下拉列表中选择**添加组 (Add Group)**。

步骤 3 如果要分组的对象类型为**可分辨名称 (Distinguished Name)**：

a) 展开**可分辨名称 (Distinguished Name)** 节点。

b) 选择**对象组 (Object Groups)**。

c) 点击**添加可分辨名称 (Add Distinguished Name)**。

步骤 4 如果要分组的对象类型为 **PKI**：

a) 展开 **PKI** 节点。

b) 选择以下其中一个选项：

- **内部 CA 证书 (Internal CA Groups)**
- **受信任 CA 证书 (Trusted CA Groups)**
- **内部证书组 (Internal Cert Groups)**
- **外部证书组 (External Cert Groups)**

c) 点击**添加[对象类型]组 (Add [Object Type] Group)**。

步骤 5 在**名称 (Name)** 中输入唯一的名称。

步骤 6 从列表中选择一个或多个对象，然后点击**添加 (Add)**。

您还可以：

- 使用过滤器字段 (**搜索**（）) 可搜索要包括的现有对象，在您键入时，该字段会更新以显示匹配项目。点击搜索字段上方的 **重新加载**（），或点击搜索字段中的 **清除**（） 以清除搜索字符串。
- 如果现有对象不符合您的需要，可点击 **添加**（） 快速创建对象。

步骤 7 或者对于**网络 (Network)**、**端口 (Port)**、**URL** 和 **VLAN 标记 (VLAN Tag)** 组：

- 输入**说明 (Description)**。
- 选中**允许覆盖 (Allow Override)** 复选框，允许对此对象组进行覆盖；请参阅允许对象覆盖，第 969 页。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象组，请部署配置更改；请参阅部署配置更改，第 136 页。

对象覆盖

通过对象覆盖，您可以为对象定义一个备选值，系统将为您指定的设备使用该值。

您可以创建其定义适用于大多数设备的对象，然后使用覆盖为需要不同定义的几个设备指定对象的修改。您还可以创建需要为所有设备覆盖的对象，但其使用使您能够为所有设备创建单个策略。对象覆盖允许您创建较小的一组在设备间使用的共享策略，而不会失去在各个设备需要时修改策略的能力。

例如，您可能想要拒绝 ICMP 流量传送到公司的不同部门，每个部门连接到不同的网络。可以通过定义带有特定规则（包括一个称为“部门网络”的网络对象）的访问控制策略来实现。通过允许覆盖此对象，即可在每个相关设备上创建覆盖，指定该设备所连接的实际网络。

在多域部署中，可以为祖先域中的对象定义默认值，并允许后代域中的管理员为该对象添加覆盖值。例如，托管安全服务提供商 (MSSP) 可以使用单一 管理中心来管理多个客户的网络安全。MSSP 的管理员可以在全局域中定义在所有客户的部署中使用的对象。每个客户的管理员可以登录后代域，为其组织覆盖该对象。这些本地管理员无法查看或影响 MSSP 的其他客户的覆盖值。

您可以将对象覆盖的目标对准特定域。在这种情况下，除非已在设备级覆盖该值，否则系统会将对象覆盖值用于目标域中的所有设备。

在对象管理器中，可以选择可覆盖的对象并为该对象定义设备级或域级覆盖列表。

只能使用具有以下对象类型的对象覆盖：

- 网络
- 端口
- VLAN 标记
- URL
- SLA 监控器
- 前缀列表
- 路由映射
- 访问列表
- AS 路径
- 社区列表
- 策略列表
- PKI 注册
- 密钥链

如果可以覆盖对象，则系统会在对象管理器中为该对象类型显示**覆盖 (Override)** 列。此列的可能值包括：

- 绿色勾选标记 - 表示可为对象创建覆盖且尚未添加任何覆盖
- 红色 X - 表示无法为对象创建覆盖
- 数字 - 表示已添加到该对象的覆盖计数（例如，“2”表示已添加两个覆盖）

管理对象覆盖

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中进行选择；请参阅对象简介，第 958 页。

步骤 3 点击要编辑的对象旁边的 **编辑**（）。

如果显示**视图**（），则表明对象属于祖先域且已配置为不允许覆盖，或者您没有修改对象的权限。

步骤 4 管理对象覆盖：

- 添加 - 添加对象覆盖；请参阅添加对象覆盖，第 969 页。
- 允许 - 允许对象覆盖；请参阅允许对象覆盖，第 969 页。
- 删除 - 在对象编辑器中，点击要删除的覆盖旁边的 **删除**（）。

- 编辑 - 编辑对象覆盖；请参阅编辑对象覆盖 ， 第 970 页。

允许对象覆盖

过程

步骤 1 在对象编辑器中，选中**允许覆盖**复选框。

步骤 2 点击**保存 (Save)**。

下一步做什么

添加对象覆盖值；请参阅添加对象覆盖 ， 第 969 页。

添加对象覆盖

开始之前

允许对象覆盖；请参阅允许对象覆盖 ， 第 969 页。

过程

步骤 1 在对象编辑器中，展开**覆盖**部分。

步骤 2 点击**添加 (Add)**。

步骤 3 在**目标 (Targets)** 中，选择**可用设备和域 (Available Devices and Domains)** 列表中的域或设备，然后点击**添加 (Add)**。

步骤 4 在“覆盖”(Override) 选项卡中，输入**名称**。

步骤 5 输入**说明**（可选）。

步骤 6 输入覆盖值。

示例：

对于网络对象，请输入网络值。

步骤 7 点击**添加 (Add)**。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

编辑对象覆盖

可以修改说明和现有覆盖的值，但不可以修改现有目标列表。相反，您必须添加一个具有新目标的新覆盖，该覆盖将代替现有覆盖。

过程

步骤 1 在对象编辑器中，展开**覆盖 (Override)** 部分。

步骤 2 点击要修改的覆盖旁边的 **编辑**（）。

步骤 3 或者，修改**说明 (Description)**。

步骤 4 修改覆盖值。

步骤 5 点击**保存 (Save)** 保存覆盖。

步骤 6 点击**保存 (Save)** 保存对象。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

AAA 服务器

添加可重用的 AAA 服务器对象。

添加 RADIUS 服务器组

Radius 服务器组对象包含一个或多个对 RADIUS 服务器的引用。这些服务器用于对通过远程接入 VPN 连接登录的用户进行身份验证。

您可以将此对象与 威胁防御 设备一起使用。

开始之前

注释 不能覆盖 Radius 服务器组对象。

过程

步骤 1 选择 **对象** > **对象管理** > **AAA 服务器** > **Radius 服务器组**。

将列出所有当前配置的 Radius 服务器组对象。使用过滤器缩小列表的范围。

步骤 2 选择并编辑列出的 Radius 服务器组对象，或者添加一个新的对象。

参阅RADIUS 服务器选项，第 972 页和RADIUS 服务器组选项，第 971 页以配置此对象。

步骤 3 点击**保存**

RADIUS 服务器组选项

导航路径

对象 > **对象管理** > **AAA 服务器** > **RADIUS 服务器组**。选择并编辑已配置的 RADIUS 服务器组对象，或添加一个新的相应对象。

字段

- **名称**和**说明** - 输入名称，并可选择性地输入说明，以标识此 RADIUS 服务器组对象。
- **组记帐模式** - 将记帐消息发送到组中的 RADIUS 服务器的方法。选择**单个**，记帐消息会发送到组中的单个服务器，这是默认设置。或者，选择 **多个**，记帐消息将同时发送到组中的所有服务器。
- **重试间隔** - 两次尝试与 RADIUS 服务器联系之间的间隔。值范围为 1 秒至 10 秒。
- **领域**（可选）- 指定或选择此 RADIUS 服务器组与之关联的 Active Directory (AD) 领域。然后，在身份策略中选择此领域，以便在确定流量的 VPN 身份验证身份源时访问关联的 RADIUS 服务器组。此领域有效地提供了从身份策略到此 Radius 服务器组的桥接。如果没有与此 RADIUS 服务器组关联的领域，则无法访问 RADIUS 服务器组以确定身份策略中流量的 VPN 身份验证身份源。

注释 如果使用具有用户身份和 RADIUS 作为身份源的远程访问 VPN，则此字段为必填。

- **仅启用授权** - 如果此 RADIUS 服务器组未用于身份验证，但正在用于授权或记帐，请选中此字段以为 RADIUS 服务器组启用仅授权模式。

  在仅授权模式下，无需在 Access-Request 中包含 RADIUS 服务器密码。因此，为各个 RADIUS 服务器配置的密码将被忽略。

- **启用临时帐户更新**和**间隔** - 启用生成 RADIUS 临时记帐更新消息的功能，以便将新分配的 IP 地址通知 RADIUS 服务器。在“间隔”字段中设置定期记帐更新之间的间隔长度（以小时为单位）。有效范围是 1 至 120，默认值为 24。
- **启用动态授权**和**端口** - 为此 RADIUS 服务器组启用 RADIUS 动态授权或授权更改 (CoA) 服务。在**端口**字段中指定用于 RADIUS CoA 请求的侦听端口。有效范围是 1024 至 65535，默认值为 1700。定义后，相应的 RADIUS 服务器组将注册用于 CoA 通知，并侦听相应端口以获取来自思科身份服务引擎 (ISE) 的 CoA 策略更新。

- **RADIUS 服务器** - 请参阅RADIUS 服务器选项，第 972 页。

相关主题

添加 RADIUS 服务器组，第 970 页

RADIUS 服务器选项

导航路径

对象 > **对象管理** > **AAA 服务器** > **Radius 服务器组**。选择并编辑某一已列出的 RADIUS 服务器组对象，或者添加一个新的 RADIUS 服务器组对象。然后在“RADIUS 服务器组”对话框中，选择并编辑某一已列出的 RADIUS 服务器，或者添加一个新的 RADIUS 服务器。

字段

- **IP 地址/主机名** - 标识将要向其发送身份验证请求的 RADIUS 服务器的主机名或 IP 地址的网络对象。只能选择一项，以向“RADIUS 服务器组”列表中添加其他服务器、添加其他 RADIUS 服务器。

注释 设备现在支持 IPv6 IP 地址用于 RADIUS 身份验证。

- **身份验证端口** - 在其上执行 RADIUS 身份验证和授权的端口。默认值为 1812。
- **密钥**和**确认密钥** - 用于在受管设备（客户端）与 RADIUS 服务器之间加密数据的共享密钥。

  该密钥是一个区分大小写的字母数字字符串，最多 127 个字符。允许使用特殊字符。

  在此字段中定义的密钥必须与 RADIUS 服务器上的密钥相匹配。在“确认”字段中再次数据该密钥。
- **记帐端口** - 在其上执行 RADIUS 记帐的端口。默认值为 1813。
- **超时** - 身份验证的会话超时。

注释 RADIUS 双因素身份验证的超时值必须为 60 秒或以上。默认超时值为 10 秒。

- **连接方式** - 使用路由查找或特定接口建立从设备到 RADIUS 服务器的连接。
  - 点击**路由 (Routing)** 单选按钮以使用路由表。
  - 点击**特定接口 (Specific Interface)** 单选按钮，然后从下拉列表中选择一个安全区/接口组或诊断 接口（默认）。。
- **重定向 ACL** - 从列表中选择重定向 ACL 或添加新 ACL。

注释 此为在设备中定义的用于决定重定向流量的ACL名称。此处的重定向ACL名称必须与 ISE 服务器中的 *redirect-acl* 名称相同。在配置 ACL 对象时，请确保对ISE和DNS服务器选择“阻止”操作，并对其余服务器选择“允许”操作。

相关主题

添加 RADIUS 服务器组，第 970 页
RADIUS 服务器组选项，第 971 页

添加单点登录服务器

开始之前

从 SAML 身份提供程序获取以下信息：

- 身份提供程序实体 ID URL
- 登录 URL
- 注销 URL
- 身份提供者证书，并使用 管理中心 Web 界面（**设备 (Devices)** > **证书 (Certificates)**）在 威胁防御 中注册证书

有关详细信息，请参阅配置 SAML 单点登录身份验证，第 1206 页。

过程

步骤 1 依次选择 **对象** > **对象管理** > **AAA服务器** > **单点登录服务器**。

步骤 2 点击 **添加单点登录服务器** 并提供以下详细信息：

- **名称**-SAML 单点登录服务器对象的名称。
- **身份提供程序实体 ID (Identity Provider Entity ID)** - 在 SAML IdP 中定义的用于唯一标识服务提供商的 URL。

  用于提供元数据 XML 的页面的 URL，元数据 XML 说明了 SAML 颁发者将如何响应请求。
- **SSO URL**-用于登录到 SAML 身份提供程序服务器的 URL。
- **注销 URL**-用于注销 SAML 身份提供程序服务器的 URL。
- **基本 URL (Base URL)** - 在身份提供程序身份验证完成后，将用户重定向回 威胁防御 的 URL。这是为 威胁防御 远程访问 VPN 配置的访问接口的 URL。

- **身份提供程序证书 (Identity Provider Certificate)** - 注册到 威胁防御 以验证由 IdP 签名的消息的 IdP 的证书。

  从列表中选择一个标识提供程序证书，或点击添加以创建新的证书注册对象。

  有关详细信息，请参阅管理 威胁防御 证书，第 1078 页。

  您必须在 威胁防御上将所有 Microsoft Azure 注册应用 CA 证书注册为信任点。Microsoft Azure SAML 身份提供程序在 威胁防御上为初始应用配置。所有连接配置文件映射到配置的 MS Azure SAML 身份提供程序。对于每个 MS Azure 应用（默认设置除外），您可以在远程访问 VPN 的连接配置文件配置中选择所需的信任点（CA 证书）。

  有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 1151 页。

- **服务提供商证书 (Service Provider Certificate)** - 威胁防御 证书，用于签署请求并与 IdP 建立信任圈。

  如果您尚未注册内部 威胁防御 证书，请点击 + 添加并注册证书。有关详细信息，请参阅管理 威胁防御 证书，第 1078 页。

- **请求签名**-选择用于对 SAML 单点登录请求签名的加密算法。

  签名从最弱到最强列出：SHA1，SHA256，SHA384，SHA512。选择“无”可禁用加密。

- **请求超时 (Request Timeout)** - 指定用户完成单点登录请求的 SAML 断言有效期。SAML IdP 有两个超时： *NotBefore* 和 *NotOnOrAfter*。威胁防御 会验证其当前时间是否在（下限）*NotBefore* 和（上限）*NotBefore* 加上 *timeout* 和 *NotOnOrAfter* 中的较小者的时间范围内。因此，如果设置的超时长于 IdP 的 *NotOnOrAfter* 超时，则忽略指定的超时，并选择 *NotOnOrAfter* 超时。如果指定超时和 *NotBefore* 超时的总和小于 *NotOnOrAfter* 时间，则 威胁防御 超时会覆盖超时。

  超时范围是 1-7200 秒，默认是 300 秒。

- **启用仅在内部网络上可访问的 IdP (Enable IdP only accessible on Internal Network)** - 如果 SAML IdP 位于内部网络上，请选择此选项。威胁防御 会充当网关，并使用匿名 webvpn 会话在用户和 IdP 之间建立通信。

- **请求 IdP 在登陆重新进行身份验证**-选择此选项以在每次登录时对用户进行身份验证，即使之前的 IdP 会话有效。

- **允许覆盖**-选中此复选框以允许对此单点登录服务器对象进行覆盖。

步骤 3 点击**保存 (Save)**。

相关主题

配置远程访问 VPN 的 AAA 设置，第 1151 页

访问列表

访问列表对象（也称为访问控制列表[ACL]），选择服务将应用到的流量。您可在配置特定功能（例如路由映射，对 威胁防御 设备）时使用这些对象。对于识别为 ACL 所允许的流量，系统会提供服务，而“阻止”流量则会从服务中排除。从服务中排除流量未必意味着完全丢弃该流量。

您可以配置以下类型的 ACL：

- 扩展 - 根据源地址/端口和目标地址/端口识别流量。支持 IPv4 和 IPv6 地址（可以在给定规则中混用）。
- 标准 - 仅根据目标地址识别流量。仅支持 IPv4。

ACL 由一个或多个访问控制条目 (ACE) 或规则组成。ACE 的顺序非常重要。当评估 ACL 以确定数据包是否与“允许的”ACE 匹配时，该数据包会按照条目的列出顺序针对每个 ACE 进行测试。找到匹配项后，不再检查更多 ACE。例如，如果要“允许”10.100.10.1，但是“阻止”10.100.10.0/24 的其余地址，则允许条目必须在阻止条目之前。一般来说，将更具体的规则置于 ACL 的顶部。

与“允许”条目不匹配的数据包被视为受阻止。

以下主题介绍如何配置 ACL 对象。

配置扩展 ACL 对象

当要根据源和目标地址、协议和端口、应用组匹配流量时或者如果流量为IPv6，可使用扩展ACL对象。

过程

步骤 1 依次选择**对象 (Objects)** > **对象管理 (Object Management)** 并从目录中选择**访问控制列表 (Access Control Lists)** > **扩展 (Extended)**。

步骤 2 执行以下操作之一：

- 点击**添加扩展 ACL (Add Extended ACL)** 以创建新对象。
- 点击 **编辑**（ ） 以编辑现有对象。

步骤 3 在“扩展 ACL 对象”(Extended ACL Object) 对话框中，输入对象的名称（不允许使用空格），并配置访问控制条目：

a) 执行以下操作之一：

- 点击**添加 (Add)** 以创建新条目。
- 点击 **编辑**（ ） 以编辑现有条目。

右键点击菜单还包括用于剪切、复制和粘贴条目或者删除这些条目的选项。

b) 选择**操作 (Action)**，是允许（匹配）还是阻止（不匹配）流量标准。

注释 **日志记录 (Logging)**、**日志级别 (Log Level)** 以及**日志间隔 (Log Interval)** 选项仅用于访问规则（附加到接口或全局应用的 ACL）。由于 ACL 对象不用于访问规则，请将这些值保留其默认值。

c) 使用以下任一方法在**网络 (Network)** 选项卡上配置源和目标地址：

- 从“可用”(Available) 列表中选择所需的网络对象或组，然后点击**添加到源 (Add to Source)** 或**添加到目标 (Add to Destination)**。您可以通过点击列表上方的 + 按钮创建新对象。您可以混合使用 IPv4 和 IPv6 地址。
- 在源或目标列表下面的编辑框中输入地址并点击**添加 (Add)**。您可以指定单个主机地址（如 10.100.10.5 或 2001:DB8::0DB8:800:200C:417A）或子网（10.100.10.0/24 或 10.100.10.0 255.255.255.0 格式，或 2001:DB8:0:CD30::/60 这种 IPv6 格式）。

d) 点击**端口 (Port)** 选项卡并使用以下任一方法配置服务。

- 从可用列表中选择所需的端口对象，然后点击 **添加到源** 或 **添加到目标**。您可以通过点击列表上方的 + 按钮创建新对象。对象可以指定 TCP/UDP 端口、ICMP/ICMPv6 消息类型或其他协议（包括“任意”[any]）。但是，通常留空的源端口只接受 TCP/UDP。您无法选择端口组。

  对于TCP/UDP，请注意，如果同时指定了源和目标字段，则必须在两者中使用相同的协议。例如，您不能指定 UDP 源端口和 TCP 目标端口。

- 在源或目标列表下面的编辑框中输入或选择端口或协议并点击**添加 (Add)**。

注释 要获取适用于所有 IP 流量的条目，请选择指定“所有”协议的目标端口对象。

e) 点击 **应用** 选项卡，然后选择要为直接互联网访问策略分组的应用。

重要事项

- 不能为集群设备配置应用。因此，此选项卡不适用于集群设备。
- 仅对策略型路由中的应用使用扩展 ACL。请勿在其他策略中使用它，因为其行为未知且不受支持。

注释

- **可用应用** 列表显示一组固定的预定义应用。此列表是访问控制策略上可用的应用的子集，因为只有第一个数据包（FQDN 终端解析为 IP 地址和端口）可以检测到这些应用。应用定义通过 VDB 更新进行更新，并在后续部署期间推送到 威胁防御 。
- 不支持用户定义的自定义应用或应用组。
- 目前， 管理中心 既不支持用户定义的自定义应用或应用组，也不允许您修改预定义的应用列表。
- 您可以使用应用过滤器下提供的 **应用过滤器** 优化此列表。

f) 选择所需的应用，然后点击 **添加到规则**。

注释
- 请勿在扩展 ACL 对象中配置目标网络和应用。
- 每个访问控制条目中的所选应用（Nertwork 服务对象）组成一个网络服务组 (NSG)，此组部署在 威胁防御上。NSG 用于直接互联网访问，根据与所选应用组的匹配对流量进行分类。

g) 点击**添加 (Add)** 以将条目添加到对象。
h) 如有必要，请点击并拖动条目，以按照规则顺序将其上移或下移到所需位置。

重复该过程以创建或编辑对象中的其他条目。

步骤 4 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 969 页。

步骤 5 点击**保存 (Save)**。

配置标准 ACL 对象

当要仅根据目标 IPv4 地址匹配流量时，请使用标准 ACL 对象。否则，请使用扩展 ACL。

过程

步骤 1 依次选择**对象 (Object)** > **对象管理 (Object Management)** 并从目录中选择**访问控制列表 (Access Control Lists)** > **标准 (Standard)**。

步骤 2 执行以下操作之一：
- 点击**添加标准 ACL (Add Standard ACL)** 以创建新对象。
- 点击 **编辑**（ ） 以编辑现有对象。

步骤 3 在“标准 ACL 对象”(Standard ACL Object) 对话框中，输入对象的名称（不允许使用空格），并配置访问控制条目：

a) 执行以下操作之一：
- 点击**添加 (Add)** 以创建新条目。
- 点击 **编辑**（ ） 以编辑现有条目。

右键点击菜单还包括用于剪切、复制和粘贴条目或者删除这些条目的选项。

b) 对于每个访问控制条目，请配置以下属性：
- **操作 (Action)** - 是允许（匹配）还是阻止（不匹配）流量标准。
- **网络 (Network)** - 添加用于识别流量目标的 IPv4 网络对象或组。

c) 点击**添加 (Add)** 以将条目添加到对象。
d) 如有必要，请点击并拖动条目，以按照规则顺序将其上移或下移到所需位置。

重复该过程以创建或编辑对象中的其他条目。

步骤 4 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 969 页。

步骤 5 点击**保存 (Save)**。

地址池

您可以为 IPv4 和 IPv6 配置 IP 地址池，该地址池可用于 具有 集群 的诊断接口，或 用于 VPN 远程访问配置文件。

过程

步骤 1 选择**对象** > **对象管理** > **地址池** > **IPv4 池**。

步骤 2 点击**添加 IPv4 池**并配置以下字段：

- **名称** - 输入地址池的名称。最多可包含 64 个字符
- **说明** - 为该池添加可选说明。
- **IP 地址** - 输入池中可用地址的范围。在开始地址和结束地址之间使用虚线十进制符号和破折号，例如：10.10.147.100-10.10.147.177。
- **掩码** - 标识此 IP 地址池所属的子网。
- **允许覆盖** - 选中此复选框可启用对象覆盖。点击展开箭头可显示**覆盖**表。您可以通过点击**添加**来添加新的覆盖。有关详细信息，请参阅对象覆盖，第 967 页。

步骤 3 点击**保存**。

步骤 4 点击**添加 IPv6 池**并配置以下字段：

- **名称** - 输入地址池的名称。最多可包含 64 个字符
- **说明** - 为该池添加可选说明。
- **IPv6 地址** - 输入配置的池中可用的第一个 IP 地址和前缀长度（以位为单位）。例如：2001:DB8::1/64。
- **地址数量** - 标识地址池中从开始 IP 地址开始的 IPv6 地址的数量。
- **允许覆盖** - 选中此复选框可启用覆盖。点击展开箭头可显示**覆盖**表。您可以通过点击**添加**来添加新的覆盖。有关详细信息，请参阅对象覆盖，第 967 页。

步骤 5 点击**保存 (Save)**。

应用过滤器

借助系统提供的应用过滤器，您可以根据应用的基本特征（类型、风险、业务关联性、类别和标记）组织应用，从而执行应用控制。您可以在对象管理器中，以系统提供的过滤器的组合为基础或以应用的自定义组合为基础，创建并管理可重复使用的用户定义的应用过滤器。有关详细信息，请参阅应用规则条件，第 607 页。

AS 路径

AS 路径是用于设置 BGP 的必需属性。它是 AS 编号序列，通过其可以访问网络。AS-PATH 是形成供数据包传播的定向路由的源和目标路由器之间的中间 AS 编号序列。相邻自治系统 (ASes) 使用 BGP 交换和更新有关如何到达不同的 AS 前缀的消息。在每个路由器制定有关目标的最佳路由的新本地决策后，它会将该路由或路径信息以及随附的距离指标和路径属性发送到其每个对等体。由于此信息通过网络传播，因此路径沿线的每个路由器会将其唯一 AS 编号预置到 BGP 消息中的 ASes 列表。此列表是路由的AS-PATH。AS-PATH 以及 AS 前缀通过网络为单向传输路由提供特定处理。使用“配置 AS 路径”(Configure AS Path) 页面创建、复制和编辑自治系统 (AS) 路径策略对象。您可以创建 AS 路径对象以在配置路由映射、策略映射、BGP 邻居过滤时使用。AS 路径过滤器使您能够通过使用正则表达式来过滤路由更新消息。

您可以将此对象与 威胁防御 设备一起使用。

过程

步骤 1 依次选择**对象 (Objects)** > **对象管理 (Object Management)** 并从目录中选择 **AS 路径 (AS Path)**。

步骤 2 点击**添加 AS 路径 (Add AS Path)**。

步骤 3 在**名称 (Name)** 字段中输入 AS 路径对象的名称。有效值介于 1 与 500 之间。

步骤 4 点击**新建 AS 路径对象 (New AS Path Object)** 窗口上的**添加 (Add)**。

a) 从**操作 (Action)** 下拉列表中选择“允许”(Allow) 或“阻止”(Block) 选项以指示重新分发访问。

b) 在**正则表达式 (Regular Expression)** 字段中指定用于定义 AS 路径过滤器的正则表达式。

c) 点击**添加 (Add)**。

步骤 5 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 969 页。

步骤 6 点击**保存 (Save)**。

密码套件列表

密码套件列表是由多个密码套件组成的对象。每个预定义密码套件值代表用于协商 SSL 或 TLS 加密会话的一个密码套件。您可以在 SSL 规则中使用密码套件和密码套件列表根据协商 SSL 会话的客户

端和服务器是否使用该加密套件来控制加密流量。如果将密码套件列表添加到 SSL 规则，使用该列表中的任何密码套件协商的 SSL 会话都匹配该规则。

注释 虽然密码套件和密码套件列表在 Web 界面中可使用的位置相同，但不能添加、修改或删除密码套件。

创建密码套件列表

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**密码套件列表 (Cipher Suite List)**。

步骤 3 点击 **Add Cipher Suites**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 从**可用密码 (Available Ciphers)** 列表中选择一个或多个密码套件。

步骤 6 点击 **Add**。

步骤 7 或者，点击**所选密码 (Selected Ciphers)** 列表中要删除的任何密码套件旁边的 **删除**（ ）。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

社区列表

社区是可选的过渡BGP属性。社区是指一组共享某个通用属性的目标。它用于路由标记。BGP社区属性是可分配给特定前缀并通告到其他邻居的数值。社区可用于标记共享通用属性的一组前缀。上游提供商可以使用这些标记应用通用路由策略，例如过滤或分配特定本地首选项或者修改其他属性。使用“配置社区列表”页面创建、复制和编辑社区列表策略对象。您可以创建社区列表对象以在配置路由映射或策略映射时使用。您可以使用社区列表创建要在路由映射的匹配子句中使用的社区组。社区列表是匹配语句的有序列表。目标根据规则进行匹配，直至找到匹配项为止。

您可以将此对象与 威胁防御 设备一起使用。

过程

步骤 1 依次选择**对象** > **对象管理**并从目录中选择**社区列表**。

步骤 2 点击**添加社区列表**。

步骤 3 在**名称**字段中，指定社区列表对象的名称。

步骤 4 点击**新建社区列表对象**窗口上的**添加**。

步骤 5 选择**标准**单选按钮以指示社区规则类型。

标准社区列表用于指定已知的社区和社区编号。

注释 不能在同一社区列表对象中同时具有使用“标准”和使用“扩展”社区规则类型的条目。

a) 从**操作**下拉列表中选择“允许”或“阻止”选项以指示重新分发访问。

b) 在**社区**字段中，指定社区号。有效值可以从 1 到 4294967295 或者从 0:1 到 65534:65535。

c) 选择相应的**路由类型**。

- **互联网** - 选择指定互联网已知社区。系统向所有对等体（内部和外部）通告具有此社区的路由。
- **无通告** - 选择指定不通告已知社区。系统不向任何对等体（内部或外部）通告具有此社区的路由。
- **无导出** - 选择指定不导出已知社区。系统仅向同一自治系统中的对等体或仅向联盟内的其他子自治系统通告具有此社区的路由。不会向外部对等体通告这些路由。

步骤 6 选择**扩展**单选按钮以指示社区规则类型。

扩展的社区列表通过正则表达式用于过滤社区。正则表达式用于指定要与社区属性匹配的模式。

a) 从**操作**下拉列表中选择“允许”或“阻止”选项以指示重新分发访问。

b) 在**表达式**字段中指定正则表达式。

步骤 7 点击**添加 (Add)**。

步骤 8 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖 ， 第 969 页。

步骤 9 点击**保存 (Save)**。

扩展社区

扩展社区是一组更大的共享某个通用属性的目的。BGP 扩展社区列表具有可用于标记共享通用属性的一组前缀的属性。这些标记用在路由映射的 match 子句中，用于过滤路由以实现虚拟路由器之间的路由泄漏。您还可以使用扩展社区列表定义策略列表对象以进行过滤。扩展社区列表是匹配语句的有序列表。路由会根据规则进行匹配，直到找到具有指定路由目标（标准）或正则表达式（扩展）的匹配项。使用“扩展社区”页面创建和编辑扩展社区列表策略对象。

注释 扩展社区列表仅适用于配置路由的导入或导出。

您可以将此对象与 威胁防御 设备一起使用。

过程

步骤 1 依次选择**对象** > **对象管理**，并在目录中选择**社区列表** > **扩展社区**。

步骤 2 点击**添加扩展社区列表**。

步骤 3 在**名称**字段中，指定扩展社区列表对象的名称。名称的长度不能超过 80 个字符。

步骤 4 选择扩展社区规则类型：

- 点击**标准**单选按钮，指定一个或多个路由目标。
- 点击**扩展**单选按钮，指定正则表达式。

注释 在同一个扩展社区列表对象中不能同时具有使用“标准”和“扩展”扩展社区规则类型的条目。

步骤 5 点击**添加 (Add)**。

步骤 6 如果已选择**标准**作为扩展社区规则类型，请指定以下内容：

a) 在**序列号**字段中，输入希望规则执行的顺序。

序列号在列表中必须唯一。

b) 在**操作**下拉列表中，如果要允许具有此处指定的匹配路由目标的路由，请选择**允许**； 如果要拒绝具有在此处指定的匹配路由目标的路由，请选择**阻止**。

c) 在**路由目标**字段中，指定路由目标。

- 您可以在单个条目中添加单个路由目标或一组以逗号分隔的路由目标。例如 *1:2,1:4,1:6*。
- 有效值可以是 1:1 到 65534:65535。
- 一个条目中最多可以包含 8 个路由目标。
- 不能跨多个条目设置多余的路由目标。例如，假设要使用 *1:200,100:100,1:300* 路由目标配置 *seq1*，并使用 *1:300,100:100,1:200* 路由目标配置 *seq2*。这会导致设置多余的路由目标，且无法部署。

步骤 7 如果已选择**扩展**作为扩展社区规则类型，请指定以下内容：

a) 在**序列号**字段中，输入希望规则执行的顺序。

序列号在列表中必须唯一。

b) 在**操作**下拉列表中，如果要允许具有此处指定的匹配正则表达式的路由，请选择**允许**； 如果要拒绝具有此处指定的匹配正则表达式的路由，请选择**阻止**。

c) 在**表达式**字段中指定正则表达式。

- 可以在单个条目中添加单个路由目标或一组以空格分隔的路由目标。例如，*^((16)|(18)):(.)$*。
- 最多可以向一个条目中添加 16 个正则表达式。

- 不能跨多个条目设置多余的正则表达式。例如，假设要使用 *^((16) | (18)):(.)$ ^4_[0-9]*$* 路由目标配置 *seq1*，并使用 *^4_[0-9]*$ ^((16) | (18)):(.)$* 路由目标配置 *seq2*。这会导致设置多余的正则表达式，且无法部署。

有关 BGP 正则表达式的详细信息，请参阅此处。

步骤 8 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 969 页。

步骤 9 点击**保存**。

可以在路由映射对象或策略列表对象的 match 子句中引用扩展社区列表：

- 在路由映射对象中，扩展社区列表的名称显示在**添加路由映射条目** > **Match 子句** > **BGP** > **社区列表** > **添加扩展社区列表**对话框中。有关在路由映射中配置 BGP 设置的详细信息，请参阅路由映射，第 1022 页。
- 在策略列表对象中，扩展社区列表的名称显示在**添加策略列表** > **社区规则** > **添加扩展社区列表**对话框中。有关在策略列表中配置 BGP 设置的详细信息，请参阅策略列表，第 1018 页。

可分辨名称

每个可分辨名称对象代表的公共密钥的使用者或颁发者的可分辨名称。您可在 TLS/SSL 规则中使用可分辨名称对象和对象组根据协商 TLS/SSL 会话的客户端和服务器是否使用将该可分辨名称作为使用者或颁发者的服务器证书来控制加密流量。

（可分辨名称组是现有可分辨名称对象的命名集合。）

可分辨名称可以包含国家/地区代码、公用名、组织和组织单位，但通常只会包含一个公用名。例如，`https://www.cisco.com` 的证书中的公用名为 `cisco.com`。（但情况并非总是这么简单；可分辨名称 (DN) 规则条件，第 1749 页显示了如何查找常用名称。）证书可以包含多个可在规则条件中用作 DN 的使用者可选名称 (SAN)。有关 SAN 的详细信息，请参阅 RFC 5280 第 4.2.1.6 节。

引用通用名称的可分辨名称对象的格式为 `CN=name`。如果添加不带 `CN=` 的 DN 规则条件，系统会在名称前面加上 `CN=`，再保存对象。

如可分辨名称 (DN) 规则条件，第 1749 页中进一步所述，系统尽可能使用服务器名称指示 (SNI) (Server Name Indication [SNI]) 来匹配 TLS/SSL 规则中的 DN。

还可以添加带有下表中列出的每个属性（用逗号隔开）的一个可分辨名称。

表 *78:* 可分辨名称属性

属性	说明	允许的值
选	国家/地区代码	两个字母字符
CN	公用名称	最多 64 个字母数字、斜杠 (/)、连字符 (-)、引号 (")、星号 (*) 字符或空格

属性	说明	允许的值
O	组织	最多 64 个字母数字、斜杠 (/)、连字符 (-)、引号 (")、星号 (*) 字符或空格
OU	组织单位	最多 64 个字母数字、斜杠 (/)、连字符 (-)、引号 (")、星号 (*) 字符或空格

有关 DN 规则条件的重要说明

- 系统首次检测新服务器的加密会话时，DN 数据不可用于 ClientHello 处理，因为这可能会导致首个会话不解密。

  如果服务器请求 TLS 1.3，则 TLS 服务器身份发现的设置可以确保在做出 SSL 策略 决策之前知道服务器证书，从而提供帮助。有关详细信息，请参阅访问控制策略高级设置 ， 第 1271 页。

- 如果还选择了**解密 - 已知密钥 (Derypt - Known Key)** 操作，则无法配置可分辨名称条件。由于该操作要求选择服务器证书来解密流量，因此证书已经与流量相匹配。

通配符示例

可以定义一个或多个星号 (*) 作为属性中的通配符。在通用名称属性中，您可以为每个域名标签定义一个或多个星号。通配符仅在该标签中匹配，但您可以使用通配符定义多个标签。请参阅下表中的示例。

表 *79*: 公用名属性通配符示例

属性	匹配	不匹配
CN=*ample.com	example.com	mail.example.com example.text.com ampleexam.com
CN=exam*.com	example.com	mail.example.com example.text.com ampleexam.com
CN=*xamp*.com	example.com	mail.example.com example.text.com ampleexam.com
CN=*.example.com	mail.example.com	www.myhost.example.com example.com example.text.com ampleexam.com

注释 DN 对象 `CN=amp.cisco.com` 与 `CN=auth.amp.cisco.com` 不匹配，因此我们建议要在这些情况下使用通配符。

有关详细信息和示例，请参阅可分辨名称 (DN) 规则条件，第 1749 页。

相关主题

可分辨名称 (DN) 规则条件，第 1749 页

创建可分辨名称对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开**可分辨名称 (Distinguished Name)** 节点，然后选择**单个对象 (Individual Objects)**。

步骤 3 点击 **Add Distinguished Name**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 在 **DN** 字段中，输入可分辨名称或公用名的值。您有以下选择：

- 如果添加可分辨名称，则可包括可分辨名称，第 983 页中列出的每个属性（以逗号隔开）。
- 如果添加公用名，则可包括多个标签和通配符。

步骤 6 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

DNS 服务器组

域名系统 (DNS) 服务器会将完全限定域名 (FQDN)（例如 www.example.com）解析为 IP 地址。

创建 DNS 服务器组对象

过程

步骤 1 选择**对象 (Object)** > **对象管理 (Object Management)**。

步骤 2 点击网络对象列表中的 **DNS 服务器组**。

步骤 3 点击**添加 DNS 服务器组**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 或者，输入用于附加到非完全限定主机名的**默认域**。

此设置仅用于默认服务器组。

步骤 6 默认的**超时**和**重试次数**值已预填。如有必要，可更改这些值。

- 重试次数 - 系统接收不到响应时，重试 DNS 服务器列表的次数，介于 0 和 10 次之间。默认值为 2。
- 超时 (Timeout) - 尝试下一个 DNS 服务器之前要等待的秒数，介于 1 和 30 秒之间。默认值为 2 秒。每次系统重试服务器列表，此超时将加倍。

步骤 7 输入将属于此组的 **DNS 服务器**，可为 IPv4 或 IPv6 格式的逗号分隔条目。

一个组最多可包含 6 个 DNS 服务器。

步骤 8 点击**保存 (Save)**。

下一步做什么

在 DNS 服务器组中配置的 DNS 服务器应当分配到 DNS 平台设置中的接口对象。有关详细信息，请参阅配置 DNS，第 617 页。

外部属性

动态对象

动态对象是可以使用 IP 或使用 Cisco Secure Dynamic Attributes Connector 来创建的对象，作为一种集成，它允许在 管理中心 访问控制规则中使用来自云网络产品的对象。

有关 dynamic attributes connector 的详细信息，请参阅本指南后面的信息。

动态对象和网络对象之间的差异如下：

- 使用 dynamic attributes connector 创建的动态对象会在创建后立即被推送到 管理中心，并且还会定期更新。
- API 创建的动态对象：
  - 是 IP 地址，有或没有或无类域间路由 (CIDR)，可以在访问控制规则中使用，与网络对象很相似。
  - 不支持完全限定域名或地址范围。
  - 必须使用 API 进行更新。

相关主题

添加或编辑动态对象 ，第 987 页

添加或编辑动态对象

此过程讨论如何添加或编辑动态对象， 动态对象是一组使用 API 的 IP 地址，可以在访问控制规则中使用或不使用无类域间路由 (*CIDR*)，就像网络对象一样。

注释 如果使用 Cisco Secure Dynamic Attributes Connector ，则无需执行此过程，因为它会自动为您创建动态对象。

开始之前

有关使用对象服务 API 为 IP 对象填充地址的信息，请参阅《*Firepower* 管理中心 *REST API* 快速入门指南》。动态对象不需要部署。

过程

步骤 1 点击 **对象** > **对象管理**。

步骤 2 点击**外部属性 (External Attributes)** > **动态对象 (Dynamic Objects)**。

步骤 3 点击**添加动态对象 (Add Dynamic Object)** 或 **编辑**（ ）。

步骤 4 输入对象的**名称**和可选的**说明**。

步骤 5 在**类型 (Type)** 列表中，点击 **IP**。

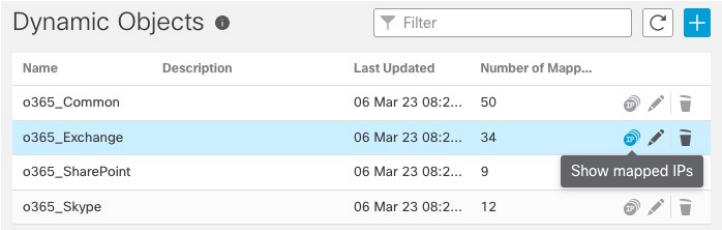
下一步做什么

如有必要，请使用 API 来更新动态对象。不需要部署。

动态对象映射

如果使用 API 或使用 dynamic attributes connector 配置动态对象，则连接器会定期向 管理中心 发送与动态属性过滤器匹配的 IP。

要查看或下载这些 IP 地址的当前列表，请点击**显示映射 ID (Show Mapped IDs)**，如下图所示。



IP 地址随时间动态添加，因此您应考虑定期执行此操作，尤其是在访问控制规则未按预期运行的情况下。

相关主题

- 动态对象 ， 第 986 页

安全组标记

安全组标记 (SGT) 对象指定单个 (SGT) 值。您可以使用规则中的 SGT 对象来控制具有**并非**由思科 ISE 分配的 SGT 属性的流量。您不能分组或覆盖 SGT 对象。

相关主题

从自定义 SGT 自动过渡到 ISE SGT
自定义 SGT 条件
ISE SGT 与自定义 SGT 规则条件

创建安全组标记对象

您只能在全局域中创建这些对象。要在经典设备上使用对象，您必须拥有控制许可证。对于智能许可设备，任何许可证均可。

开始之前

- 禁用 ISE/ISE-PIC 连接。如果使用 ISE/ISE-PIC 作为身份源，则不能创建自定义 SGT 对象。

过程

步骤 1 请点击 **对象** > **对象管理**。

步骤 2 点击**外部属性 (External Attributes)** > **动态对象 (Dynamic Objects)**。

步骤 3 点击**添加安全组标记 (Add Security Group Tag)**。

步骤 4 输入 **Name**。

步骤 5 输入**说明 (Description)**（可选）。

步骤 6 在**标记 (Tag)** 字段中，输入单个 SGT。

步骤 7 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

文件列表

如果使用恶意软件防护，而 AMP 云错误地识别某个文件的处置情况，则您可以将该文件添加到文件列表，以便将来能够更好地检测该文件。这些文件使用 SHA-256 散列值进行指定。每个文件列表最多可以包含 10000 个唯一的 SHA-256 值。

文件列表有两种预定义类别：

干净的列表

如果将某个文件添加到此列表，则系统视为 AMP 云为其分配了干净处置情况。

自定义检测列表

如果将某个文件添加到此列表，则系统视为 AMP 云为其分配了恶意软件处置情况。

在多域部署中，将为每个域呈现一个干净的列表和自定义检测列表。在低层域中，您可以查看但无法修改祖先列表。

由于您手动指定这些列表中包含的文件的阻止行为，系统不会在 AMP 云中查询这些文件的处置情况。您必须配置文件策略中的规则（通过**恶意软件云查找 [Malware Cloud Lookup]** 或**阻止恶意软件 [Block Malware]** 操作）和匹配的文件类型才能计算文件的 SHA 值。

⚠

注意 请**勿**在干净的列表中包含恶意软件。干净的列表会覆盖 AMP 云和自定义检测列表。

文件列表的源文件

可通过上传包含 SHA-256 值和描述的列表的逗号分隔值 (CSV) 源文件将多个 SHA-256 值添加到文件列表。管理中心验证内容并使用有效的 SHA-256 值填充文件列表。

源文件必须为具有 .csv 文件扩展名的简单文本文件。所有标题必须以井号 (#) 开头；标题将被视为注释，不会上传。每个条目都应包含一个 SHA-256 值，后跟说明并以 `LF` 或 `CR+LF` 换行字符结尾。系统将会忽略条目中的任何其他信息。

请注意以下提示：

- 从文件列表删除源文件也会从该文件列表删除所有相关的 SHA-256 散列值。

- 如果成功上传源文件导致文件列表包含超过 10000 个不同的 SHA-256 值，则不能将多个文件上传到该文件列表。
- 上传时，系统会截去描述中超过256个字符的字符，仅保留前256个字符。如果描述包括逗号，必须使用转义字符 (\,)。如果未包含描述，将会改为使用源文件名。
- 所有非重复的SHA-256值都将被添加到文件列表。如果文件列表包含SHA-256值，并且上传了包括该值的源文件，新上传的值不会修改现有SHA-256值。查看与SHA-256值相关的捕获的文件、文件事件或恶意软件事件时，所有威胁名称或描述都来源于单个 SHA-256 值。
- 系统不会在源文件中上传无效的 SHA-256 值。
- 如果多个上传的源文件包括相同 SHA-256 值的条目，系统将使用最新的值。
- 如果源文件包括相同 SHA-256 值的多个条目，系统将使用最后一个。
- 不能在对象管理器中直接编辑源文件。要进行更改，必须首先直接修改源文件，删除系统中的副本，然后上传修改后的源文件。
- 与源文件相关的条目数是指不同的SHA-256值的数量。如果从文件列表删除某个源文件，文件列表包含的 SHA-256 条目总数将会减少等于该源文件中有效条目的数量。

将单个 SHA-256 值添加到文件列表

您必须有此程序的 恶意软件 许可证。

可以提交文件的 SHA-256 值以将其添加到文件列表。不能添加重复的 SHA-256 值。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

开始之前

- 在事件视图中右键点击某个文件或恶意软件事件，在情景菜单中选择**显示全文 (Show Full Text)**，然后复制完整的 SHA-256 值以粘贴到列表中。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**文件列表 (File List)**。

步骤 3 点击要添加文件的干净列表或自定义检测列表旁边的 **编辑**（ ）。

如果显示**视图**（ ），则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 从**添加方式 (Add by)** 下拉列表中选择 `Enter SHA Value`。

步骤 5 在 **Description** 字段中输入源文件的描述。

步骤 6 在 **SHA-256** 字段中输入或粘贴文件的完整值。系统不支持匹配部分值。

步骤 7 点击**添加 (Add)**。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

注释 在部署配置更改后，系统不再查询 AMP 云以查找列表中的文件。

将单个文件上传到文件列表

您必须有此程序的 恶意软件 许可证。

如果要将文件副本添加到文件列表，则可将文件上传到 Cisco Secure Firewall Management Center进行分析；系统会计算文件的 SHA-256 值并将文件添加到列表。系统不对用于 SHA-256 计算的文件大小强制实施任何限制。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**文件列表 (File List)**。

步骤 3 点击要添加文件的干净列表或自定义检测列表旁边的 **编辑**（ ）。

如果显示**视图**（ ），则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 从**添加方式 (Add by)** 下拉菜单中，选择**计算 SHA (Calculate SHA)**。

步骤 5 或者，在**说明 (Description)** 字段中输入文件的说明。如果不输入说明，在上传时文件名将被用作说明。

步骤 6 点击**浏览 (Browse)**，然后选择要上传的文件。

步骤 7 点击**计算并添加 SHA (Calculate and Add SHA)**。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

注释 在部署配置更改后，系统不再查询 AMP 云以查找列表中的文件。

将源文件上传到文件列表

您必须有此程序的 恶意软件 许可证。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 点击 **File List**。

步骤 3 点击要从源文件向其添加值的文件列表旁边的 **编辑**（）。

如果显示**视图**（），则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 从**添加方式 (Add by)** 下拉菜单中，选择 `List of SHAs`。

步骤 5 或者，在**说明 (Description)** 字段中输入源文件的说明。如果不输入说明，系统将会使用文件名。

步骤 6 点击**浏览 (Browse)** 浏览到源文件，然后点击**上传并添加列表 (Upload and Add List)**。

步骤 7 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

注释 在部署策略后，系统不再查询 AMP 云以查找列表中的文件。

编辑文件列表中的 SHA-256 值

您必须有此程序的 恶意软件 许可证。

可以编辑或删除文件列表中的各个 SHA-256 值。请注意，不能在对象管理器中直接编辑源文件。要进行更改，必须首先直接修改源文件，删除系统中的副本，然后上传修改后的源文件。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 点击 **File List**。

步骤 3 点击要修改文件的干净列表或自定义检测列表旁边的 **编辑**（）。

如果显示**视图**（），则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 您可以执行以下操作：

- 点击要更改的 SHA-256 值旁边的 **编辑**（），并根据需要修改 **SHA-256** 或**说明 (Description)** 值。
- 点击要删除的 SHA-256 值旁边的 **删除**（）。

步骤 5 点击**保存 (Save)** 以更新列表中的文件条目。

步骤 6 点击**保存 (Save)** 以保存文件列表。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

注释 在部署配置更改后，系统不再查询 AMP 云以查找列表中的文件。

从文件列表下载源文件

您必须有此程序的 恶意软件 许可证。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**文件列表 (File List)**。

步骤 3 点击要下载源文件的干净列表或自定义检测列表旁边的 **编辑**（）。

如果显示**视图**（），则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 点击要下载的源文件旁边的 **视图**（）。

步骤 5 点击**下载 SHA 列表 (Download SHA List)** 并按照提示保存源文件。

步骤 6 点击 **Close**。

FlexConfig

可以使用 FlexConfig 策略中的 FlexConfig 策略对象为 威胁防御设备上您不能使用 Cisco Secure Firewall Management Center另行配置的功能提供自定义配置。有关 FlexConfig 策略的更多信息，请参阅FlexConfig 策略概述，第 1991 页。

可为 FlexConfig 配置以下类型的对象。

文本对象

文本对象定义了在 FlexConfig 对象中用作变量的自由形式的文本字符串。这些对象可以具有单个值，或是多个值的列表。

有几种预定义文本对象可以用于预定义 FlexConfig 对象。如果使用相关联的 FlexConfig 对象，则只需编辑文本对象的内容，即可自定义 FlexConfig 对象配置给定设备的方式。在编辑预定义对象时，为您配置的每台设备创建设备覆盖，而不是直接更改这些对象的默认值，通常是更好的选择。这有助于避免如果另一个用户希望将同一 FlexConfig 对象用于一组不同的设备可能导致的意外后果。

有关配置文本对象的信息，请参阅配置 FlexConfig 文本对象，第 2016 页。

FlexConfig 对象

FlexConfig 对象包括设备配置命令、变量和脚本语言指令。在配置部署过程中，将处理这些指令，以创建一系列带有自定义参数的配置命令，用于配置目标设备上的特定功能。

这些指令要么是在系统配置常规 管理中心策略和设置中定义的功能之前（预置）进行配置，要么是在此之后（附加）进行配置。必须将任何取决于 Cisco Secure Firewall Management Center配置的对象（例如网络对象）的 FlexConfig 附加到配置部署，否则在所需 FlexConfig 参考所需对象之前，不会配置这些对象。

有关配置 FlexConfig 对象的更多信息，请参阅配置 FlexConfig 对象，第 2012 页。

地理定位

配置的每个地理定位对象代表系统识别为受监控网络上流量的源或目标的一个或多个国家/地区或大洲。可在系统 Web 界面中的不同位置使用地理定位对象，包括访问控制策略、SSL 策略和事件搜索。例如，可编写阻止流向或来自某些国家/地区的流量的访问控制规则。

要确保使用最新信息来过滤网络流量，思科强烈建议您定期更新地理位置数据库 (GeoDB)。

创建地理位置对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**地理位置 (Geolocation)**。

步骤 3 点击 **Add Geolocation**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 选中要包括到地理定位对象中的国家/地区和大洲的相应复选框。选中大洲会选中该大洲的所有国家/地区，以及 GeoDB 更新将来可能添加到该大洲下的所有国家/地区。取消选中大洲下的任意国家/地区会取消选中该大洲。您可以选择国家/地区和大洲的任意组合。

步骤 6 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

接口

每个接口可以被分配给安全区域和/或接口组。然后，根据区域或组应用您的安全策略。例如，您可以将“内部”接口分配到“内部”区域，而将“外部”接口分配到“外部”区域。例如，可以配置访问控制策略，允许流量从内部传到外部，但不允许从外部传入内部。某些策略仅支持安全区域，而其他策略则支持区域和组。

有关接口对象的详细信息，请参阅安全区域和接口组 ， 第 493 页。

要添加接口对象，请参阅创建安全区域和接口组对象 ， 第 496 页。

密钥链

为了增强设备的数据安全和防护，引入了用于对持续时间为 180 天以内的 IGP 对等体进行身份验证的轮换密钥。轮换密钥可阻止任何恶意用户猜测用于路由协议身份验证的密钥，从而保护网络，避免通告错误的路由和重定向流量。频繁更改密钥可降低密钥最终被猜到的风险。在配置提供密钥链的路由协议的身份验证时，请为密钥链中的密钥配置重叠的生存期。这有助于防止由于缺少活动密钥而丢失受密钥保护的通信。轮换密钥仅适用于 OSPFv2 协议。如果密钥生存期到期且未找到活动密钥，则 OSPF 会使用最后一个有效密钥来维持对等体之间的邻接关系。

注释 身份验证仅使用 MD5 加密算法。

密钥生存期

为了维持稳定的通信，每个设备会将密钥链身份验证密钥存储起来，并对某个功能同时使用多个密钥。密钥链管理基于密钥的发送和接受生存期，提供了一种安全机制来处理密钥滚动。设备使用密钥生存期来确定密钥链中的哪些密钥处于活动状态。

密钥链中的每个密钥具有两个生存期：

- 接受生存期 - 设备在与另一设备进行密钥交换期间接受密钥的时间间隔。
- 发送生存期 - 设备在与另一设备进行密钥交换期间发送密钥的时间间隔。

在密钥发送生存期内，设备会将路由更新数据包与密钥一起发送。当发送的密钥不在设备上密钥的接受生存期内时，设备将不会接受来自其他设备的通信。

如果未配置生存期，则相当于配置没有时间线的 MD5 身份验证密钥。

密钥选择

- 当密钥链含有多个有效密钥时，OSPF 会选择生存期最长的密钥。
- 首选具有无限生存期的密钥。
- 如果密钥生存期相同，则首选密钥 ID 较高的密钥。

创建密钥链对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**密钥链**。

步骤 3 点击**添加密钥链**。

步骤 4 在“添加密钥链对象”对话框的**名称**字段中输入密钥链的名称。

该名称必须以下划线或字母开头，后跟字母数字字符或特殊字符（-、_、+、.）。

步骤 5 要向密钥链添加密钥，请点击**添加**。

步骤 6 在**密钥 ID** 字段中指定密钥标识符。

密钥 ID 值可介于 0 到 255 之间。仅在表明无效密钥时使用值 0。

步骤 7 **算法**字段和**密码加密类型**字段分别显示支持的算法和加密类型，即 MD5 和明文。

步骤 8 在**加密密钥字符串**字段中输入密码，然后在**确认加密密钥字符串**字段中重新输入该密码。

- 密码的最大长度可为 80 个字符。
- 密码不能为单个数字或以数字加空格开头。例如，“0 pass”或“1”为无效密码。

步骤 9 要设置设备与其他设备进行密钥交换期间接受/发送密钥的时间间隔，请在**接受生存期**和**发送生存期**字段中提供生存期值：

注释 “日期时间”值默认为 UTC 时区。

结束时间可为持续时间，即接受/发送生存期结束时的绝对时间或永不到期。默认结束时间为日期时间。

以下为开始值和结束值的验证规则：

- 在指定了结束生存期时，开始生存期不可为空值。
- 接受或发送生存期的开始生存期必须早于相应的结束生存期。

步骤 10 点击**添加**。

重复步骤 5 到 10 以创建密钥。为具有重叠生存期的密钥链创建至少两个密钥。这有助于防止由于缺少活动密钥而丢失受密钥保护的通信。

步骤 11 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 969 页。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 969 页。

步骤 12 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

网络

网络对象表示一个或多个 IP 地址。您可以在多个位置使用网络对象和组合，包括访问控制策略、网络变量、身份规则、网络发现规则、事件搜索、报告、身份识别等等。

当配置需要网络对象的选项时，系统会自动过滤列表，以仅显示对于该选项有效的那些对象。例如，某些选项需要主机对象，而其他选项则需要子网。

网络对象可以是以下类型之一：

主机

单个 IP 地址。

IPv4 示例：

209.165.200.225

IPv6 示例：

2001:DB8::0DB8:800:200C:417A 或 2001:DB8:0:0:0DB8:800:200C:417A

范围

IP 地址范围。

IPv4 示例：

209.165.200.225-209.165.200.250

IPv6 示例：

2001:db8:0:cd30::1-2001:db8:0:cd30::1000

网络

地址块，也称为子网。

IPv4 示例：

209.165.200.224/27

IPv6 示例：

2001:DB8:0:CD30::/60

注释 “安全智能”会忽略使用 /0 掩码的 IP 地址块。

FQDN

单个完全限定域名 (FQDN)。您可以将 FQDN 解析限制为仅 IPv4 地址，仅 IPv6 地址或 IPv4 和 IPv6 地址。FQDN 必须以数字或字母开头和结尾。FQDN 中仅允许使用字母、数字和短划线作为内部字符。

例如：

```
www.example.com
```

注释 您可在访问控制规则和预过滤规则中使用 FQDN 对象， 或手动 NAT 规则，仅限 。规则匹配通过 DNS 查找获取的 FQDN IP 地址。要使用 FQDN 网络对象，请确保已分别在 DNS 服务器组，第 985 页和配置 DNS，第 617 页中配置 DNS 服务器设置和 DNS 平台设置。

您不能在身份规则中使用 FDQN 网络对象。

组

一组网络对象或其他网络对象组。您可以通过将一个网络对象组添加到另一个网络对象组创建嵌套组。最多可以嵌套 10 个级别的组。

网络通配符掩码

您可以从“对象管理”(Object Management) 页面创建和管理通配符掩码对象。

您可以创建具有扩展子网 IP 地址的网络对象。现有网络对象已扩展为支持网络和网络通配符对象。使用通配符掩码的网络对象在网络对象列表页面的**类型 (Type)** 列中列为**网络通配符**。

通配符掩码是不连续的位掩码的 IP 地址。可以使用连续掩码为通配符网络对象创建标准网络对象和不连续的掩码。

IP 地址示例	**网络通配符？**	**对象类型**
192.0.0.0/8	不支持	网络
10.10.0.0/255.255.0.0	不支持	网络
10.10.0.10/255.255.0.255	是	网络通配符
72.0.240.10/255.255.240.255	是	网络通配符

注释 只有在配置以下策略时才允许使用网络通配符对象以及包含网络通配符对象的对象组：

- 预过滤器策略
- 访问控制策略
- NAT 策略

准则和限制

- 要创建网络通配符对象，请在 FMC UI 中依次选择**对象 (Objects)** > **对象管理 (Object Management)** > **网络 (Network)** 并点击**添加网络 (Add Network)**，然后点击**添加对象 (Add Object)**。选择**网络 (Network)** 选项并输入扩展子网掩码形式的值。示例：10.0.10.10/255.255.0.255。
- 支持对象覆盖、组对象支持、组对象覆盖、通配符文本和通配符对象导入。
- 仅 IPv4 地址支持网络通配符对象。
- FMC 和 FTD 7.1 及更高版本可支持网络通配符对象。
- 仅 Snort-3 支持网络通配符对象。

创建网络对象

威胁防御功能历史记录：

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**网络 (Network)**。

步骤 3 从**添加网络 (Add Network)** 下拉菜单中选择**添加对象 (Add Object)**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 输入**说明 (Description)**（可选）。

步骤 6 在**网络**字段中，选择所需选项，然后输入适当的值；请参阅网络，第 997 页。

步骤 7 （仅限 FQDN 对象）从**查找**下拉菜单中选择 DNS 解析以确定是否要将 IPv4 地址、IPv6 地址，或这两个地址与 FQDN 关联。

步骤 8 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 969 页。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 969 页。

步骤 9 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

导入网络对象

有关导入网络对象的详细信息，请参阅正在导入对象，第 960 页。

PKI

用于 SSL 应用的 PKI 对象

PKI 对象代表支持您的部署所需的公钥证书和配对的私钥。内部和可信 CA 对象包括证书颁发机构 (CA) 证书；内部 CA 对象还包括与证书配对的私钥。内部和外部证书对象包括服务器证书；内部证书对象还包括与证书配对的私钥。

如果使用可信证书颁发机构对象和内部证书对象来配置与 ISE/ISE-PIC 的连接，则可使用 ISE/ISE-PIC 作为身份源。

如果使用内部证书对象来配置强制网络门户，在连接到用户的 Web 浏览器时，系统可验证强制网络门户设备的身份。

如果使用可信证书颁发机构对象来配置领域，则可配置与 LDAP 或 AD 服务器的安全连接。

如果在 SSL 规则中使用 PKI 对象，可以匹配使用以下证书加密的流量：

- 外部证书对象中的证书
- 由受信任 CA 对象中的 CA 签名的证书或在 CA 的信任链中的证书

如果在 SSL 规则中使用 PKI 对象，可以解密：

- 传出流量（通过对带有内部 CA 对象的服务器证书进行重签）
- 传入流量（使用内部证书对象中的已知私钥）

可以手动输入证书和密钥信息，上传包含这些信息的文件，在某些情况下，还可以生成新的 CA 证书和私有密钥。

在对象管理器中查看 PKI 对象列表时，系统会将证书的使用者可分辨名称显示为对象值。将指针悬停在该值上可查看证书使用者的完整可分辨名称。要查看其他证书的详细信息，请编辑 PKI 对象。

注释 管理中心和受管设备在保存存储在内部 CA 对象和内部证书对象中的所有私钥之前，会使用随机生成的密钥对它们进行加密。如果上传受密码保护的私钥，设备会使用用户提供的密码对该密钥解密，然后用随机生成的密钥对其加密，再进行保存。

用于证书注册的 PKI 对象

证书注册对象包含创建证书签名请求 (CSR) 以及从指定的证书颁发机构 (CA) 获取身份证书所需的 CA 服务器信息和注册参数。这些活动发生在您的私有密钥基础设施 (PKI) 中。

证书注册对象还可能包括证书撤销信息。有关 PKI、数字证书和证书注册的详细信息，请参阅 PKI 基础设施和数字证书 ，第 1096 页。

内部证书颁发机构对象

配置的每个内部证书颁发机构 (CA) 对象代表组织控制的 CA 的 CA 公共密钥证书。此类对象由对象名称、CA 证书和配对私钥组成。您可以在 SSL 规则中使用内部 CA 对象和组通过使用内部 CA 对服务器证书进行重新签名来解密传出加密流量。

注释 如果在**解密 - 重新签名 (Decrypt - Resign)** SSL 规则中引用内部 CA 对象，且该规则与加密会话相匹配，在协商 SSL 握手时，用户的浏览器可能会警告证书不可信。要避免此问题，请将内部 CA 对象证书添加到受信任根证书的客户端或域列表。

可以通过以下方式创建内部 CA 对象：

- 导入现有基于 RSA 或基于椭圆曲线的 CA 证书和私有密钥
- 生成新的基于 RSA 的自签 CA 证书和私有密钥

- 生成未签名的基于 RSA 的 CA 证书和私有密钥。使用内部 CA 对象之前，必须向另一个 CA 提交证书签名请求 (CSR) 以对证书进行签名。

创建包含签名证书的内部 CA 对象后，可以下载 CA 证书和私钥。系统使用用户提供的密码对下载的证书和私钥进行加密。

无论是系统生成还是用户创建的内部 CA 对象名称，您都只能修改其名称，但不能修改其他对象属性。

不能删除正在使用的内部 CA 对象。此外，在编辑用于 SSL 策略的内部 CA 对象后，相关联的访问控制策略已过时。必须重新部署访问控制策略才能使更改生效。

CA 证书和私钥导入

可以通过导入 X.509 v3 RSA 证书和私有密钥来配置内部 CA 对象。可以上传采用下列其中一种受支持格式编码的文件：

- 可分辨编码规则 (DER)
- 隐私增强电子邮件 (PEM)

如果私有密钥文件受密码保护，您可以提供解密密码。如果证书和密钥采用 PEM 格式编码，还可以复制并粘贴信息。

如果要上传文件，文件中必须包含正确的证书或密钥信息，并且可以相互配对。系统在保存对象前将验证配对。

注释 如果配置具有 **Decrypt - Resign** 操作的规则，除了任何配置的规则条件之外，该规则还根据引用的内部 CA 证书的加密算法类型匹配流量。例如，必须上传一个基于椭圆曲线的 CA 证书，以解密用基于椭圆曲线的算法进行加密的出站流量。

导入 CA 证书和私钥

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开 **PKI** 节点，然后选择**内部 CA (Internal CAs)**。

步骤 3 点击**导入 CA**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 在 **Certificate Data** 字段上方，点击 **Browse** 上传 DER 或 PEM 编码的 X.509 v3 CA 证书文件。

步骤 6 在 **Key** 字段上方，点击 **Browse** 上传 DER、PEM 编码的配对私有密钥文件。

步骤 7 如果上传的文件受密码保护，请选中**已加密，密码为：(Encrypted, and the password is:)** 复选框并输入密码。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

生成新的 CA 证书和私钥

可以通过提供识别信息生成基于 RSA 的自签 CA 证书和私有密钥来配置内部 CA 对象。

生成的 CA 证书有效期为十年。有效期起始日期为生成一周之前。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开 **PKI** 节点，然后选择**内部 CA (Internal CAs)**。

步骤 3 点击**生成 CA (Generate CA)**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 输入标识属性。

步骤 6 点击 **Generate self-signed CA**。

新签名证书

可以通过从 CA 获取签名证书来配置内部 CA 对象。这包括两个步骤：

- 提供识别信息以配置内部 CA 对象。这会生成未签名证书和配对私钥，并创建向您指定的 CA 发出的证书签名请求 (CSR)。
- 在 CA 颁发签名证书后，请上传证书到内部 CA 对象，用以替换未签名证书。

仅当内部 CA 对象包含签名证书时，才能在 SSL 规则中引用该对象。

创建未签名的 CA 证书和 CSR

过程

步骤 1 选择对象 > 对象管理。

步骤 2 展开 **PKI** 节点，然后选择内部 **CA (Internal CAs)**。

步骤 3 点击生成 **CA (Generate CA)**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 输入标识属性。

步骤 6 点击 **Generate CSR**（生成 **CSR**）。

步骤 7 复制 CSR 以将其提交到 CA。

步骤 8 点击 **OK**。

下一步做什么

- 必须上传由 CA 颁发的签名证书，如 中所述 上传为响应 CSR 而颁发的签名证书，第 1004 页

上传为响应 CSR 而颁发的签名证书

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

上传之后，签名证书可在 SSL 规则中引用。

过程

步骤 1 选择对象 > 对象管理。

步骤 2 展开 **PKI** 节点，然后选择内部 **CA (Internal CAs)**。

步骤 3 点击包含等待 CSR 的未签名证书的 CA 对象旁边的 编辑（）。

步骤 4 点击 **Install Certificate**。

步骤 5 点击浏览 **(Browse)** 上传 DER 或 PEM 编码的 X.509 v3 CA 证书文件。

步骤 6 如果上传的文件受密码保护，请选中已加密，密码为：**(Encrypted, and the password is:)** 复选框并输入密码。

步骤 7 点击保存 **(Save)** 以将签名证书上传到 CA 对象。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

CA 证书和私钥下载

可以通过下载包含内部 CA 对象中的证书和密钥信息的文件来备份或传输 CA 证书和配对私钥。

⚠

注意 系统始终将下载的密钥信息存储在安全的位置。

系统在保存密钥信息之前，会使用随机生成的密钥对存储在内部 CA 对象中的私钥进行加密。如果从内部 CA 下载证书和私钥，系统在创建包含证书和私钥信息的文件之前，会首先对这些信息进行解密。然后，您必须提供系统用于加密下载文件的密码。

⚠

注意 作为系统备份一部分下载的私钥将被解密，然后存储在未加密的备份文件中。

下载 CA 证书和私钥

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

可以同时为当前域和祖先域下载 CA 证书。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开 **PKI** 节点，然后选择**内部 CA (Internal CAs)**。

步骤 3 在要下载其证书和私钥的内部 CA 对象旁边，点击 **编辑**（✎）。

在多域部署中，点击 **视图**（👁），为祖先域中的对象下载证书和私钥。

步骤 4 点击**下载**。

步骤 5 在**密码 (Password)** 和**确认密码 (Confirm Password)** 字段中输入加密密码。

步骤 6 点击**确定 (OK)**。

受信任证书颁发机构对象

配置的每个受信任证书颁发机构 (CA) 对象代表属于受信任 CA 的 CA 公钥证书。此类对象由对象名称和 CA 公共密钥证书组成。您可以在以下位置使用外部 CA 对象和组：

- SSL 策略，用于控制使用由受信任 CA 或信任链中的任何 CA 签名的证书加密的流量。

- 领域配置，用于建立与 LDAP 或 AD 服务器的安全连接。
- 您的 ISE/ISE-PIC 连接。为 **pxGrid 服务器 CA (pxGrid Server CA)** 和 **MNT 服务器 CA (MNT Server CA)** 对象选择受信任证书颁发机构对象。

创建受信任 CA 对象后，可以修改名称和添加证书撤销列表 (CRL)，但不能更改其他对象属性。可添加到对象的CRL数量没有限制。要修改已上传到对象的CRL，必须删除该对象并重新创建对象。

注释 在 ISE/ISE-PIC 集成配置中使用对象时，将 CRL 添加到该对象没有任何作用。

不能删除正在使用的可信 CA 对象。此外，在编辑正在使用的受信任 CA 对象后，关联的访问控制策略会过期。必须重新部署访问控制策略才能使更改生效。

受信任的 CA 对象

您可以通过上传 X.509 v3 CA 证书来配置外部 CA 对象。可以上传采用下列其中一种受支持格式编码的文件：

- 可分辨编码规则 (DER)
- 隐私增强电子邮件 (PEM)

如果文件受密码保护，必须提供解密密码。如果证书采用PEM格式编码，还可以复制并粘贴信息。

仅当文件包含适当的证书信息时，才可以上传 CA 证书；系统在保存对象之前会对证书进行验证。

添加受信任 CA 对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开 **PKI** 节点，然后选择**受信任 CA (Trusted CAs)**。

步骤 3 点击 **Add Trusted CAs**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 点击**浏览 (Browse)** 上传 DER 或 PEM 编码的 X.509 v3 CA 证书文件。

步骤 6 如果文件受密码保护，请选中**已加密，密码为：(Encrypted, and the password is:)** 复选框并输入密码。

步骤 7 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

受信任 CA 对象中的证书撤销列表

您可以将 CRL 上传到受信任 CA 对象。如果在 SSL 策略中引用受信任 CA 对象，则可以根据颁发会话加密证书的 CA 随后是否会撤销证书来控制加密流量。可以上传采用下列其中一种受支持格式编码的文件：

- 可分辨编码规则 (DER)
- 隐私增强电子邮件 (PEM)

添加CRL后，可以查看已撤销证书的列表。要修改已上传到对象的CRL，必须删除该对象并重新创建对象。

只能上传包含适当 CRL 的文件。可添加到受信任 CA 对象的 CRL 数量没有限制。但是，每次上传 CRL 之后，必须先保存对象再添加另一个 CRL。

注释 在 ISE/ISE-PIC 集成配置中使用对象时，将 CRL 添加到该对象没有任何作用。

向受信任 CA 对象添加证书撤销列表

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

注释 在 ISE/ISE-PIC 集成配置中使用对象时，将 CRL 添加到该对象没有任何作用。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开 **PKI** 节点，然后选择**受信任 CA (Trusted CAs)**。

步骤 3 点击可信 CA 对象旁边的 **编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击**添加 CRL (Add CRL)** 上传 DER 或 PEM 编码的 CRL 文件。

步骤 5 点击**确定 (OK)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

外部证书对象

您配置的每个外部证书对象都表示一个不属于贵组织的服务器公钥证书。该对象由对象名称和证书组成。可以在 SSL 规则中使用外部证书对象和对象组来控制使用服务器证书加密的流量。例如，您可以上传您信任的自签服务器证书，但不能使用可信 CA 证书进行验证。

您可以通过上传 X.509 v3 服务器证书来配置外部证书对象。可以上传采用下列其中一种受支持格式的文件：

- 可分辨编码规则 (DER)
- 隐私增强电子邮件 (PEM)

仅当文件包含适当的服务器证书信息时，才可以上传文件；系统在保存对象之前会对文件进行验证。如果证书采用 PEM 格式编码，还可以复制并粘贴信息。

添加外部证书对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开 **PKI** 节点，然后选择**外部证书 (External Certs)**。

步骤 3 点击 **Add External Cert**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 在 **Certificate Data** 字段上方，点击 **Browse** 上传 DER 或 PEM 编码的 X.509 v3 服务器证书文件。

步骤 6 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

内部证书对象

您配置的每个内部证书对象都代表一个属于您组织的服务器公共密钥证书。此类对象由对象名称、公共密钥证书和配对私钥组成。您可以在以下位置使用内部证书对象和组：

- SSL 规则，用于通过已知私钥解密传入到您的组织其中一台服务器的流量。
- 您的 ISE/ISE-PIC 连接。为 **MC 服务器证书 (MC Server Certificate)** 字段选择内部证书对象。
- 强制网络门户配置，用于在连接到用户的 Web 浏览器时对强制网络门户设备的身份进行身份验证。为**服务器证书 (Server Certificate)** 字段选择内部证书对象。

可以通过上传基于 X.509 v3 RSA 或基于椭圆曲线的服务器证书和配对的私有密钥来配置内部证书对象。可以上传采用下列其中一种受支持格式的文件：

- 可分辨编码规则 (DER)
- 隐私增强电子邮件 (PEM)

如果文件受密码保护，必须提供解密密码。如果证书和密钥采用 PEM 格式编码，还可以复制并粘贴信息。

如果要上传文件，文件中必须包含正确的证书或密钥信息，并且可以相互配对。系统在保存对象前将验证配对。

创建内部证书对象后，可以修改名称，但不能修改其他对象属性。

不能删除正在使用的内部证书对象。此外，在编辑正在使用的内部证书对象后，关联的访问控制策略会过期。必须重新部署访问控制策略才能使更改生效。

添加内部证书对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开 **PKI** 节点，然后选择**内部证书 (Internal Certs)**。

步骤 3 点击 **Add Internal Cert**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 在 **Certificate Data** 字段上方，点击 **Browse** 上传 DER 或 PEM 编码的 X.509 v3 服务器证书文件。

步骤 6 在 **Key** 字段上方，点击 **Browse** 上传 DER、PEM 编码的配对私有密钥文件。

步骤 7 如果上传的私有密钥文件受密码保护，请选中**已加密，密码为：**复选框并输入密码。

步骤 8 点击**保存 (Save)**。

证书注册对象

通过信任点，您可以管理并跟踪 CA 和证书。信任点表示 CA 或身份对。信任点包括 CA 的身份、CA 特定配置参数，以及与一个注册的身份证书的关联。

证书注册对象包含创建证书签名请求 (CSR) 以及从指定的证书颁发机构 (CA) 获取身份证书所需的 CA 服务器信息和注册参数。这些活动发生在您的私有密钥基础设施 (PKI) 中。

证书注册对象还可能包括证书撤销信息。有关 PKI、数字证书和证书注册的详细信息，请参阅 PKI 基础设施和数字证书 ，第 1096 页。

如何使用 证书注册对象

证书注册对象用于将受管设备注册到PKI基础设施中，并通过执行以下操作在支持VPN连接的设备上创建信任点（CA 对象）：

1. 在证书注册对象中定义用于CA身份验证和注册的参数。指定共享参数，并使用覆盖功能为不同的设备指定唯一的对象设置。
2. 在需要身份证书的每个受管设备上关联并安装此对象。在设备上，它将成为信任点。

   当证书注册对象与某个设备关联并安装至该设备后，证书注册过程会立即开始。对于自签名、SCEP， EST， 和 PKCS12 文件注册类型，此过程将自动执行，这意味着不需要任何额外的管理员操作。手动证书注册需要额外的管理员操作。
3. 在您的 VPN 配置中指定创建的信任点。

管理证书注册对象

要管理证书注册对象，请转至**对象 > 对象管理**，然后从导航窗格中选择 **PKI > 证书注册**。系统将显示以下信息：

- 现有证书注册对象会在**名称**列中列出。

  使用搜索字段（放大镜）过滤列表。
- 每个对象的注册类型显示在**类型**列中。可以使用以下注册方法：
  - **自签名** - 受管设备将生成其自己的自签名根证书。
  - **EST**-设备使用安全传输注册从 CA 获取身份证书。
  - **SCEP** -（默认）简单证书注册协议由设备使用以从 CA 获取身份证书。
  - **手动** - 注册过程由管理员手动执行。
  - **PKCS12 文件** - 在支持 VPN 连接的 Firepower 威胁防御受管设备上导入 PKCS12 文件。PKCS#12、PFX 或 P12 文件将服务器证书、任何中间证书和私钥保存在一个加密文件中。输入**口令**值进行解密。
- **覆盖 (Override)** 列指示对象是允许覆盖（绿色复选标记）还是不允许覆盖（红色的 X）。如果显示一个数字，则它是现有的覆盖数。

  使用“覆盖”选项自定义作为VPN配置一部分的每个设备的对象设置。覆盖将使每个设备的信任点详细信息都是唯一的。通常，在VPN配置中，为每个设备覆盖“公用名”或“使用者”。

  有关覆盖任意类型对象的详细信息和操作步骤，请参阅对象覆盖 ，第 967 页。

- 点击编辑图标（铅笔）可**编辑**之前创建的证书注册对象。只有在注册对象未与任何受管设备关联时，才能进行编辑。请参阅有关编辑证书注册对象的添加说明。您可以对失败的注册对象进行编辑。
- 点击删除图标（垃圾桶）可**删除**之前创建的证书注册对象。如果证书注册对象已与任意受管设备关联，则无法将其删除。

按 **(+) 添加证书注册**打开**添加证书注册**对话框并配置证书注册对象，请参阅添加证书注册对象，第 1011 页。然后在每个受管的前端设备上安装证书。

相关主题

使用自签注册安装证书，第 1081 页
使用 EST 注册安装证书，第 1082 页
使用 SCEP 注册安装证书，第 1082 页
使用手动注册安装证书，第 1084 页
使用 PKCS12 文件安装证书，第 1085 页

添加证书注册对象

您可以将这些对象与 威胁防御 设备一起使用。您必须具有管理员或网络管理员权限才能执行此任务。

过程

步骤 1 打开**添加证书注册**对话框：

- 直接从对象管理打开：在**对象 > 对象管理**屏幕中，从导航窗格中选择 **PKI > 证书注册**，然后按**添加证书注册**。
- 在配置受管设备时：在**设备 > 证书** 屏幕中，选择 **添加 > 添加新证书**，然后为 **证书注册**字段点击 **(+)**。

步骤 2 输入此注册对象的**名称 (Name)** 和**说明 (Description)**（后者为可选项）。

注册完成后，此名称将成为信任点在其关联的受管设备上的名称。

步骤 3 打开 **CA 信息 (CA Information)** 选项卡并选择**注册类型 (Enrollment Type)**。

- **自签名证书** - 作为 CA 的受管设备将生成其自己的自签名根证书。此窗格中不需要其他信息。

  注释 注册自签名证书时，必须在证书参数中指定公用名称 (CN)。

- **EST**-在安全传输协议上注册。指定EST信息。请参阅证书注册对象 EST选项，第 1012 页。
- **SCEP** - （默认）简单证书注册协议。指定 SCEP 信息。请参阅证书注册对象 SCEP 选项，第 1013 页。
- **手动**
  - **仅 CA**-选中此复选框可仅从所选 CA 创建 CA 证书。不会为此证书创建身份证书。

如果不选中此复选框，则CA证书不是强制性的。您可以在没有CA证书的情况下生成CSR并获取身份证书。

- **CA证书**-在框中粘贴CA证书信息。您也可以通过从其他设备复制CA证书来获取该证书。

  如果选择不使用 CA 证书生成 CSR，则可以将此框留空。

- **PKCS12 文件** - 在支持 VPN 连接的 威胁防御受管设备上导入 PKCS12 文件。PKCS#12 或 PFX 文件将服务器证书、中间证书和私钥保存在一个加密文件中。 输入 **口令** 解密值。
- **跳过 CA 证书基本限制中的 CA 标志检查**-如果要跳过检查信任证书中的基本限制扩展和 CA 标志，请选中此复选框。
- **验证使用**-选择在 VPN 连接期间验证证书的选项
  - **IPsec 客户端** - 验证 IPsec 站点间 VPN 连接的客户端证书。
  - **SSL 客户端**-在远程访问 VPN 连接尝试期间验证 SSL 客户端证书。
  - **SSL 服务器**-选择以验证 SSL 服务器证书，例如作为 Cisco Umbrella 服务器证书。

步骤 4 （可选） 打开**证书参数 (Certificate Parameters)** 选项卡并指定证书内容。请参阅证书注册对象 证书参数，第 1014 页。

此类信息会置于证书中，从路由器接收证书的任何一方均可访问这些信息。

步骤 5 （可选） 打开**密钥 (Key)** 选项并指定密钥信息。请参阅证书注册对象 密钥选项，第 1015 页。

步骤 6 （可选） 点击**撤销**选项卡并指定撤销选项：请参阅证书注册对象 撤销选项，第 1017 页。

步骤 7 如有需要，**允许覆盖 (Allow Overrides)** 此对象。有关对象覆盖的完整说明，请参阅对象覆盖，第 967 页。

下一步做什么

关联注册对象并将其安装到某设备上，以在该设备上创建一个信任点。

相关主题

使用自签注册安装证书，第 1081 页
使用 EST 注册安装证书，第 1082 页
使用 SCEP 注册安装证书，第 1082 页
使用手动注册安装证书，第 1084 页
使用 PKCS12 文件安装证书，第 1085 页

证书注册对象 EST选项

Cisco Secure Firewall Management Center 导航路径

对象 > **对象管理**，然后从导航窗格中选择 **PKI** > **Cert 注册**。点击 **(+) 添加 Cert 注册** 来打开 **添加 Cert 注册** 对话框，然后选择 **CA 信息** 选项卡。

字段

注册类型-设置为 **EST**。

注释

- EST 注册类型不支持 EdDSA 密钥。
- 不支持 EST 在证书过期时自动注册设备的功能。

注册 URL (Enrollment URL) - 设备应尝试注册到的 CA 服务器的 URL。

使用 **https://CA_name:port** 形式的 HTTPS URL，其中 *CA_name* 是 CA 服务器的主机 DNS 名称或 IP 地址。 端口 号为必填项。

用户名-用于访问 CA 服务器的用户名。

密码/确认密码-访问 CA 服务器的密码。

指纹-当使用 EST 检索 CA 证书时，您可以为 CA 服务器输入指纹。使用指纹验证 CA 服务器证书的真实性有助于防止未经授权的第三方使用虚假证书替代真证书。输入十六进制格式的 CA 服务器**指纹 (Fingerprint)**。如果您输入的值与证书的指纹不匹配，则证书将被拒绝。通过直接联系服务器获取 CA 的指纹。

源接口-与 CA 服务器交互的接口。默认情况下，显示诊断接口。要将数据接口配置为源接口，请选择相应的安全区域或接口组对象。

忽略 EST 服务器证书验证-默认情况下，EST 服务器证书验证已完成。如果要忽略 FTD 验证 EST 服务器证书，请选中此复选框。

证书注册对象 SCEP 选项

Cisco Secure Firewall Management Center 导航路径

对象 (Objects) > 对象管理 (Object Management)，然后从导航窗格中选择 **PKI > PKI 注册 (PKI Enrollment)**。按 **(+) 添加 PKI 注册 ([+] Add PKI Enrollment)** 打开**添加 PKI 注册 (Add PKI Enrollment)** 对话框，然后选择 **CA 信息 (CA Information)** 选项卡。

字段

注册类型 (Enrollment Type) - 设置为 **SCEP**。

注册 URL (Enrollment URL) - 设备应尝试注册到的 CA 服务器的 URL。

使用 **`http://CA_name:port`** 形式的 HTTP URL，其中 CA_name 是 CA 服务器的主机 DNS 名称或 IP 地址。端口 号为必填项。

注释 如果使用主机名/FQDN 引用 SCEP 服务器，请使用 FlexConfig 对象配置 DNS 服务器。

如果 CA 中的 CA cgi-bin 脚本位置不是默认位置 (/cgi-bin/pkiclient.exe)，则您也必须将非标准脚本位置包含在 http://CA_name:port/script_location 形式的 URL 中，其中 script_location 是 CA 脚本的完整路径。

质询密码/确认密码 (Challenge Password/Confirm Password) - CA 服务器验证设备身份时所使用的密码。您可以通过直接连接 CA 服务器或通过在网络浏览器中输入以下地址获取密码：**`http://URLHostName/certsrv/mscep/mscep.dll`**。从 CA 服务器获取的密码在获取后 60 分钟内有效。因此，创建密码后请务必尽快部署。

重试时间段 (Retry Period) - 各证书请求尝试之间的时间间隔（以分钟为单位）。值可以是 1 到 60 分钟。默认值为 1 分钟。

重试计数 (Retry Count) - 若首次请求后未发出证书，应进行重试的次数。值可以是 1 到 100。默认值为 10。

CA 证书源 (CA Certificate Source) - 指定获取 CA 证书的方式。

- **使用 SCEP 检索**（默认选项，也是唯一受支持的选项）- 使用简单证书注册流程 (SCEP) 从 CA 服务器检索证书。使用 SCEP 在设备和 CA 服务器之间建立连接。在开始注册过程之前，请确保存在从设备到 CA 服务器的路由。

指纹 - 当使用 SCEP 检索 CA 证书时，您可以为 CA 服务器输入指纹。使用指纹验证 CA 服务器证书的真实性有助于防止未经授权的第三方使用虚假证书替代真证书。输入十六进制格式的 CA 服务器**指纹 (Fingerprint)**。如果您输入的值与证书的指纹不匹配，则证书将被拒绝。通过直接连接 CA 服务器或通过在网络浏览器中输入以下地址获取 CA 的指纹：**`http://<URLHostName>/certsrv/mscep/mscep.dll`**。

证书注册对象 证书参数

在发送到 CA 服务器的证书请求中指定其他信息。此类信息会置于证书中，从路由器接收证书的任何一方均可查看这些信息。

Cisco Secure Firewall Management Center 导航路径

对象 (Objects) > 对象管理 (Object Management)，然后从导航窗格中选择 **PKI > PKI 注册 (PKI Enrollment)**。按 **(+) 添加 PKI 注册 ([+] Add PKI Enrollment)** 打开**添加 PKI 注册 (Add PKI Enrollment)** 对话框，然后选择**证书参数 (Certificate Parameters)** 选项卡。

字段

使用标准 LDAP X.500 格式输入所有信息。

- **包含 FQDN (Include FQDN)** - 是否将设备的完全限定域名 (FQDN) 包含在证书请求中。选项如下：
  - **将设备主机名用作 FQDN**
  - **请不要在证书中使用 FQDN**
  - **自定义 FQDN (Custom FQDN)** - 选择此选项，然后在显示的**自定义 FQDN (Custom FQDN)** 字段中指定 FQDN。

- **包含设备的 IP 地址 (Include Device's IP Address)** - 将接口的 IP 地址包含在证书请求中。
- **公用名 (CN)(Common Name [CN])** - 要包含在证书中的 X.500 公用名。

注释 注册自签名证书时，必须在证书参数中指定公用名称 (CN)。

- **组织单位 (OU)** - 要包含在证书中的组织单位名称（例如部门名称）。
- **组织 (O) (Organization [O])** - 要包含在证书中的组织或公司名称。
- **位置 (L) (Locality [L])** - 要包含在证书中的位置。
- **州/省 (ST) (State [ST])** - 要包含在证书中的州或省。
- **国家/地区代码 (C) (County Code [C])** - 要包含在证书中的国家/地区。这些代码符合 ISO 3166 国家/地区缩写规范，例如“US”表示美国。
- **邮件 (E) (Email [E])** - 要包含在证书中的邮件地址。
- **包含设备的序列号 (Include Device’s Serial Number)** - 是否将设备的序列号包含在证书中。CA 使用序列号对证书进行验证，或者之后将证书与特定设备相关联。如有疑问，请含序列号，因为这对调试用途非常有用。

证书注册对象 密钥选项

Cisco Secure Firewall Management Center 导航路径

对象 > 对象管理，然后从导航窗格中选择 **PKI > Cert 注册**。按 **(+) 添加 Cert 注册** 打开 **添加 Cert 注册** 对话框，然后选择 **密钥** 选项卡。

字段

- **密钥类型**-RSA、ECDSA、EdDSA。

注释
- 对于 EST 注册类型，请勿选择 EdDSA 密钥，因为它不受支持。
- EdDSA 仅在站点间 VPN 拓扑中受支持。
- EdDSA 不支持作为远程访问 VPN 的身份证书。

- **密钥名称**-如果要与证书关联的密钥对已存在，则此字段指定该密钥对的名称。如果密钥对不存在，则此字段指定要分配给将在注册期间生成的密钥对的名称。如果您不指定名称，系统将使用完全限定域名 (FQDN) 密钥对。

- **密钥大小 (Key Size)** - 如果密钥对不存在，可定义所需的密钥大小（模数，以位为单位）。建议大小为2048位。模数越大，密钥越安全。但是，生成模数较大的密钥需要更长的时间（模数大于 512 位时需要一分钟或更长时间），而且交换时的处理时间也更长。

重要事项

- 在 管理中心 和 威胁防御 7.0 及更高版本上，您无法使用 RSA 加密算法注册使用 RSA 密钥大小小于 2048 位的密钥和密钥。但是，您可以使用 使用弱加密的 PKI 证书注册 ，以允许使用具有 RSA 加密算法和较小密钥大小的 SHA-1 的证书。
- 对于 威胁防御 7.0，您无法生成大小小于 2048 位的 RSA 密钥，即使启用了弱加密选项也是如此。

- **高级设置** -如果不希望在 IPsec 远程客户端证书的密钥使用和扩展密钥使用扩展中验证值，请选择 **忽略 IPsec 密钥使用** 。您可以抑制对 IPsec 客户端证书的密钥用法检查。默认情况下不启用此选项。

注释 对于站点间 VPN 连接，如果使用 Windows 证书颁发机构（CA），则默认应用策略扩展名为 **IP 安全 IKE 中间**。如果使用此默认设置，则必须为所选对象选择 **忽略 IPsec 密钥使用** 选项。否则，终端无法完成站点间 VPN 连接。

使用弱加密的 PKI 证书注册

SHA-1 散列签名算法和 RSA 密钥大小（小于 2048 位用于认证）在 管理中心 和 威胁防御7.0 及更高版本上不受支持。可以用过RSA密钥（大小小于 2048 位）来注册证书。

要在管理 威胁防御运行低于 7.0 版本的 管理中心 7.0 上覆盖这些限制，您可以在 威胁防御上使用启用弱加密选项。我们不建议允许使用弱加密密钥，因为此类密钥不如具有更大密钥大小的密钥安全。

注释 威胁防御 7.0 或更高版本不支持生成大小小于 2048 位的RSA密钥，即使您允许使用弱加密。

要在设备上启用弱加密，请导航至 **设备 > 证书** 页面。点击针对 威胁防御 设备提供的**启用弱加密**（🔒）按钮。当弱加密选项启用时，按钮更改为 🔓。默认情况下，弱加密选项已禁用。

注释 当由于弱密码使用导致证书注册失败时， 管理中心 会显示警告消息，提示您启用弱加密选项。同样，当您启用启用弱加密按钮时， 管理中心 会在设备上启用弱加密配置之前显示警告消息。

将早期版本升级到 威胁防御 7.0

当您升级到威胁防御 7.0 时，现有证书配置会保留。但是，如果这些证书的 RSA 密钥小于 2048 位，并使用 SHA-1 加密算法，则无法用于建立 VPN 连接。您必须获取 RSA 密钥大小大于 2048 位的证书，或者为 VPN 连接启用允许弱加密选项。

证书注册对象 撤销选项

通过选择和配置相关方法指定是否检查证书的撤销状态。撤销检查默认处于关闭状态，不选中任何一种方法（CRL 或 OCSP）。

Cisco Secure Firewall Management Center 导航路径

对象 (Objects) > 对象管理 (Object Management)，然后从导航窗格中选择 **PKI > PKI 注册 (PKI Enrollment)**。按 **(+) 添加 PKI 注册 ([+] Add PKI Enrollment)** 打开**添加 PKI 注册 (Add PKI Enrollment)** 对话框，然后选择**撤销 (Revocation)** 选项卡。

字段

- **启用证书撤销列表 (Enable Certificate Revocation Lists)** - 选中可启用 CRL 检查。
  - **使用来自证书的 CRL 分发点 (Use CRL distribution point from the certificate)** - 选中可获取来自证书的撤销列表分发 URL。
  - **使用已配置的静态 URL (Use static URL configured)** - 选中可添加静态的预定义的撤销列表分发 URL。然后添加 URL。

    CRL 服务器 URL (CRL Server URL) - 可从中下载 CRL 的 LDAP 服务器的 URL。

    URL 必须以 **`ldap://`**、**`http://`** 或 **`https://`** 开头。在 URL 中包含端口号。

- **启用在线证书状态协议 (Enable Online Certificate Status Protocol) (OCSP)** - 选中可启用 OCSP 检查。

  OCSP 服务器 URL (OCSP Server URL) - 需要进行 OCSP 检查时，用以检查撤销的 OCSP 服务器的 URL。

  URL 必须以 **`http://`** 或 **`https://`** 开头。

- **如果撤销信息无法访问，请考虑证书是否有效 (Consider the certificate valid if revocation information can not be reached)** - 默认处于选中状态。如果您不想允许此操作，请取消选中此字段。

注释 **如果撤销信息无法访问，请考虑证书是否有效 (Consider the certificate valid if revocation information cannot be reached)** 复选框对运行版本 6.5+ 的 威胁防御 设备没有影响。

策略列表

使用“配置策略列表”页面创建、复制和编辑策略列表策略对象。您可以创建策略列表对象以在配置路由映射时使用。当在路径映射中引用策略列表时，将评估并处理此策略列表中的所有匹配语句。通过一个路由映射可以配置两个或更多策略列表。策略列表也可以与任何其他预先存在的匹配共存，并设置在同一路径映射内部、策略列表外部配置的语句。当多个策略列表在路由映射条目中执行匹配时，所有策略列表仅在传入属性上进行匹配。

您可以将此对象与 威胁防御 设备一起使用。

过程

步骤 1 依次选择**对象** > **对象管理**并从目录中选择**策略列表**。

步骤 2 点击**添加策略列表**。

步骤 3 在**名称**字段中输入策略列表对象的名称。对象名称不区分大小写。

步骤 4 从**操作**下拉列表中选择是允许还是阻止匹配条件的访问。

步骤 5 点击**接口**选项卡以分发使其下一跳脱离其中一个指定接口的路由。

在**区域/接口**列表中，添加包含设备可通过其与管理站通信的接口的区域。对于不在区域中的接口，您可以在**所选区域/接口**列表下方的字段中键入接口名称，然后点击**添加**。仅在设备包含所选接口或区域时，系统才会在设备上配置主机。

步骤 6 点击**地址**选项卡以重新分发任何具有标准访问列表或前缀列表允许的目标地址的路由。

选择是否使用**访问列表**或**前缀列表**进行匹配，然后输入或选择要用于匹配的标准访问列表对象或前缀列表对象。

步骤 7 点击**下一跳**选项卡，重新分发具有指定访问列表或前缀列表传递的下一跳路由器地址的任何路由。

选择是否使用**访问列表**或**前缀列表**进行匹配，然后输入或选择要用于匹配的标准访问列表对象或前缀列表对象。

步骤 8 点击**路由源**选项卡，重新分发在访问列表或前缀列表指定的地址由路由器和接入服务器通告的路由。

选择是否使用**访问列表**或**前缀列表**进行匹配，然后输入或选择要用于匹配的标准访问列表对象或前缀列表对象。

步骤 9 点击 **AS 路径**选项卡以匹配 BGP 自治系统路径。如果指定多条 AS 路径，则路由可以匹配任一 AS 路径。

步骤 10 点击**社区规则**选项卡，以支持将BGP社区或扩展社区分别与指定的社区列表对象或扩展社区列表对象相匹配。如果指定多个规则，系统会根据规则验证路由，直到满足某个匹配允许或拒绝条件为止。

a) 要为规则指定社区列表，请点击**选定社区列表**字段中的给定**编辑**（）。社区列表显示在**可用社区列表**下。选择所需列表，点击**添加**，然后点击**确定**。

要使 BGP 社区与指定社区完全匹配，请选中**完全匹配指定社区**复选框。

b) 要添加扩展社区列表，请点击**选定扩展社区列表**字段中的给定**编辑**（）。扩展社区列表显示在**可用扩展社区列表**下。选择所需列表，点击**添加**，然后点击**确定**。

注释 扩展社区列表仅适用于配置路由的导入或导出。

步骤 11 点击**指标与标记**选项卡以匹配路由的指标和安全组标记。

a) 在**指标**字段中输入用于匹配的指标值。可以输入多个以逗号分隔的值。通过此设置可匹配具有指定指标的任何路由。指标值范围可以在 0 到 4294967295 之间。

b) 在**标记**字段中输入用于匹配的标记值。可以输入多个以逗号分隔的值。通过此设置可匹配任何具有指定安全组标记的路由。标记值范围在 0 到 4294967295 之间。

步骤 12 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 969 页。

步骤 13 点击**保存 (Save)**。

端口

端口对象以略有不同的方式代表不同协议：

TCP 和 UDP

代表传输层协议（协议号括在括号内，加上一个可选的关联端口或端口范围）的端口对象。例如：`TCP(6)/22`。

ICMP 和 ICMPv6 (IPv6-ICMP)

代表互联网层协议再加上可选类型和代码的端口对象。例如：`ICMP(1):3:3`。

您可以按类型和代码（如果适用）来限制 ICMP 或 IPV6-ICMP 端口对象。有关 ICMP 类型和代码的详细信息，请参阅：

- http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
- http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml

其他

可以代表不使用端口的其他协议的端口对象。

系统为已知端口提供默认端口对象。您无法修改或删除这些默认对象。除默认对象以外，还可以创建自定义端口对象。

可在系统 Web 界面中的不同位置使用端口对象和对象组，包括访问控制策略、身份规则、网络发现规则、端口变量和事件搜索。例如，如果您的组织使用的自定义客户端使用特定范围的端口并导致系统生成过多误导事件，可以配置网络发现策略来排除对这些端口的监控。

使用端口对象时，请遵循以下准则：

- 不能为访问控制规则中的源端口条件添加除 TCP 或 UDP 以外的任何协议。此外，在规则中设置源端口条件和目标端口条件时，不能混用传输协议。

- 如果要将不受支持的协议添加到用于源端口条件的端口对象组，则在部署配置时使用该协议的规则不会在受管设备上生效。
- 如果创建同时包含 TCP 和 UDP 端口的端口对象，然后将其添加为规则的源端口条件，则不能添加目标端口，反之亦然。

创建端口对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**端口 (Port)**。

步骤 3 从**添加端口 (Add Port)** 下拉列表中选择**添加对象 (Add Object)**。

步骤 4 输入 **Name**。

步骤 5 选择**协议 (Protocol)**。

步骤 6 根据选择的协议，按**端口 (Port)** 进行限制，或者选择 ICMP **类型 (Type)** 和**代码 (Code)**。

可输入 `1` 到 `65535` 之间的端口。使用连字符指定端口范围。如果选择与**所有 (All)** 协议匹配，则必须使用**其他 (Other)** 下拉列表按端口限制对象。

步骤 7 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 969 页。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 969 页。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

导入端口对象

有关导入端口对象的详细信息，请参阅正在导入对象，第 960 页。

前缀列表

您可以为 IPv4 和 IPv6 创建前缀列表对象以在配置路由映射、策略映射、OSPF 过滤或 BGP 邻居过滤时使用。

配置 IPv6 前缀列表

使用“配置 IPv6 前缀列表”(Configure IPv6 Prefix list) 页面创建、复制和编辑前缀列表对象。您可以创建前缀列表对象以在配置路由映射、策略映射、OSPF 过滤或 BGP 邻居过滤时使用。

您可以将此对象与 威胁防御 设备一起使用。

过程

步骤 1 依次选择**对象 (Object)** > **对象管理 (Object Management)** 并从目录中选择**前缀列表 (Prefix Lists)** > **IPv6 前缀列表 (IPv6 Prefix List)**。

步骤 2 点击**添加前缀列表 (Add Prefix List)**。

步骤 3 在**新建前缀列表对象 (New Prefix List Object)** 窗口上的**名称 (Name)** 字段中输入前缀列表对象的名称。

步骤 4 点击**新建前缀列表对象 (New Prefix List Object)** 窗口上的**添加 (Add)**。

步骤 5 从**操作 (Action)** 下拉列表中选择相应的操作（“允许”[Allow] 或“阻止”[Block]），以指示重新分发访问。

步骤 6 在**序列号 (Sequence No.)** 字段中输入用于指示新前缀列表条目在已为此对象配置的前缀列表条目列表中将具有的位置的唯一编号。如果保留为空白，则序列号将默认为比当前使用中的最大序列号大 5。

步骤 7 在 **IP 地址 (IP address)** 字段中指定 IP 地址/掩码长度格式的 IPv6 地址。掩码长度必须是介于 1 和 128 之间的有效值。

步骤 8 在**最小前缀长度 (Minimum Prefix Length)** 中输入最小前缀长度。该值必须大于掩码长度并小于或等于“最大前缀长度”(Maximum Prefix Length)（如果指定）。

步骤 9 在**最大前缀长度 (Maximum Prefix Length)** 字段中输入最大前缀长度。该值必须大于或等于“最小前缀长度”(Minimum Prefix Length)（如果存在），或者大于掩码长度（如果未指定“最小前缀长度”[Minimum Prefix Length]）。

步骤 10 点击**添加 (Add)**。

步骤 11 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖 ， 第 969 页。

步骤 12 点击**保存 (Save)**。

配置 IPv4 前缀列表

使用“配置 IPv4 前缀列表”(Configure IPv4 Prefix list) 页面创建、复制和编辑前缀列表对象。您可以创建前缀列表对象以在配置路由映射、策略映射、OSPF 过滤或 BGP 邻居过滤时使用。

您可以将此对象与 威胁防御 设备一起使用。

过程

步骤 1 依次选择**对象 (Object)** > **对象管理 (Object Management)** 并从目录中选择**前缀列表 (Prefix Lists)** > **IPv4 前缀列表 (IPv4 Prefix List)**。

步骤 2 点击**添加前缀列表 (Add Prefix List)**。

步骤 3 在**新建前缀列表对象 (New Prefix List Object)** 窗口上的**名称 (Name)** 字段中输入前缀列表对象的名称。

步骤 4 点击 **Add**。

步骤 5 从**操作 (Action)** 下拉列表中选择相应的操作（“允许”[Allow] 或“阻止”[Block]），以指示重新分发访问。

步骤 6 在**序列号 (Sequence No.)** 字段中输入用于指示新前缀列表条目在已为此对象配置的前缀列表条目列表中将具有的位置的唯一编号。如果保留为空白，则序列号将默认为比当前使用中的最大序列号大 5。

步骤 7 在 **IP 地址 (IP address)** 字段中指定 IP 地址/掩码长度格式的 IPv4 地址。掩码长度必须是介于 1 和 32 之间的有效值。

步骤 8 在**最小前缀长度 (Minimum Prefix Length)** 中输入最小前缀长度。该值必须大于掩码长度并小于或等于“最大前缀长度”(Maximum Prefix Length)（如果指定）。

步骤 9 在**最大前缀长度 (Maximum Prefix Length)** 字段中输入最大前缀长度。该值必须大于或等于“最小前缀长度”(Minimum Prefix Length)（如果存在），或者大于掩码长度（如果未指定“最小前缀长度”[Minimum Prefix Length]）。

步骤 10 点击**添加 (Add)**。

步骤 11 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 969 页。

步骤 12 点击**保存 (Save)**。

路由映射

在将路由重新分发到任何路由过程中时，将会使用路由映射。在为路由进程生成默认路由时也会使用路由映射。路由映射定义了允许将来自指定路由协议的哪些路由重新分发到目标路由进程。配置路由映射，以创建路由映射对象的新路由映射条目或编辑现有路由映射条目。

您可以将此对象与 威胁防御 设备一起使用。

开始之前

路由映射可以使用其中一个或多个对象；不必添加所有对象。根据需要创建并使用其中任何对象，以配置路由映射。

- 添加 ACL。
- 添加前缀列表。
- 添加 AS 路径。

- 添加社区列表。
- 添加扩展社区列表。

注释 扩展社区列表仅适用于配置路由的导入或导出。

- 添加策略列表。

过程

步骤 1 依次选择**对象** > **对象管理**并从目录中选择**路由映射**。

步骤 2 点击**添加路由映射**。

步骤 3 点击**新建路由映射对象**窗口上的**添加**。

步骤 4 在**序列号**字段中，输入 0 到 65535 之间的数字，该数字指示新路由映射条目在已为此路由映射对象配置的路由映射条目列表中的位置。

注释 建议至少以 10 为间隔对子句进行编号，以便将来想要插入子句时保留编号空间。

步骤 5 从**重新分发**下拉列表中选择相应的操作，即“允许”或“阻止”，以指示重新分发访问。

步骤 6 点击**匹配子句**选项卡以根据在目录中选择的以下条件来匹配（路由/流量）：

- **安全区域** - 根据（入口/出口）接口匹配流量。可以选择区域并添加这些区域，或者键入接口名称并添加这些接口。
- **IPv4** - 根据以下条件匹配 IPv4（路由/流量）；选择该选项卡可定义条件。
  1. 点击**地址**选项卡以根据路由地址来匹配路由。对于 IPv4 地址，请从下拉列表中选择要使用访问列表还是前缀列表进行匹配，然后输入或选择要用于匹配的ACL对象或前缀列表对象。
  2. 点击**下一跳**选项卡以根据路由的下一跳地址来匹配路由。对于 IPv4 地址，请从下拉列表中选择要使用访问列表还是前缀列表进行匹配，然后输入或选择要用于匹配的 ACL 对象或前缀列表对象。
  3. 点击**路由源**选项卡以根据路由的通告源地址来匹配路由。对于 IPv4 地址，请从下拉列表中选择要使用访问列表还是前缀列表进行匹配，然后输入或选择要用于匹配的 ACL 对象或前缀列表对象。
- **IPv6** - 根据路由的路由地址、下一跳地址或通告源地址来匹配 IPv6（路由/流量）。
- **BGP** - 根据以下条件来匹配 BGP（路由/流量）；选择该选项卡可定义条件。
  1. 点击 **AS 路径**选项卡以支持将 BGP 自治系统路径访问列表与指定的路径访问列表相匹配。如果指定多个路径访问列表，则路由可以匹配任一路径访问列表。
  2. 点击**社区列表**选项卡以支持将 BGP 社区或扩展社区分别与指定的社区列表对象或扩展社区列表对象相匹配。

- 要为规则指定社区列表，请点击**选定社区列表**字段中的给定**编辑**（）。社区列表显示在**可用社区列表**下。选择所需列表，点击**添加**，然后点击**确定**。有关如何创建社区列表对象的信息，请参阅社区列表，第 980 页
- 要添加扩展社区列表，请点击**选定扩展社区列表**字段中的给定**编辑**（）。扩展社区列表显示在**可用扩展社区列表**下。选择所需列表，点击**添加**，然后点击**确定**。有关如何创建扩展社区列表对象的信息，请参阅扩展社区，第 981 页。

要使 BGP 社区与指定社区列表对象完全匹配，请选中**完全匹配指定社区**复选框。此选项不适用于扩展社区列表。

注释 如果指定多个规则，系统会根据规则验证路由，直到满足某个匹配允许或拒绝条件为止。出站路由映射中将不会通告与至少一个匹配社区不匹配的路由。

3. 点击**策略列表**选项卡以配置路由映射来评估和处理 BGP 策略。当多个策略列表在路由映射条目中执行匹配时，所有策略列表仅在传入属性上进行匹配。

- **其他** - 根据以下条件来匹配路由或流量。

1. 在**指标路由值**字段中输入要用于匹配的指标值，以支持匹配路由的指标。可以输入多个以逗号分隔的值。通过此设置可匹配具有指定指标的任何路由。指标值范围可以在0到4294967295之间。
2. 在**标签值**字段中输入要用于匹配的标签值。可以输入多个以逗号分隔的值。通过此设置可匹配任何具有指定安全组标记的路由。标记值范围在 0 到 4294967295 之间。
3. 选中相应的**路由类型**选项以启用路由类型匹配。有效路由类型为 External1、External2、Internal、Local、NSSA-External1 和 NSSA-External2。可以从列表中选择多个路由类型。

步骤 7 点击**设置子句**选项卡以根据在目录中选择的以下条件来设置路由/流量：

- **指标值** - 设置“带宽”、所有值或无任何值。

1. 在**带宽**字段中以千位/秒为单位输入指标值或带宽。有效值是范围从 0 到 4294967295 的整数值。
2. 从**指标类型**下拉列表中选择指定目标路由协议的指标类型。有效值为：internal、type-1 或 type-2。

- **BGP 子句** - 根据以下条件设置 BGP 路由；选择该选项卡可定义条件。

1. 点击 **AS 路径**选项卡以修改 BGP 路由的自治系统路径。
    1. 在**预置 AS 路径**字段中输入 AS 路径编号，以将任意自治系统路径字符串预置到 BGP 路由。通常本地 AS 编号预置多次，从而增加自治系统路径长度。如果指定多个 AS 路径编号，则路径可以预置任一 AS 编号。
    2. 在**将最后一个 AS 预置到 AS 路径**字段中输入 AS 路径编号，来为 AS 路径预置最后一个 AS 编号。为 AS 编号输入 1 到 10 之间的值。

3. 选中**将路由标签转换为 AS 路径**复选框以将路由的标签转换为自治系统路径。

2. 点击**社区列表**选项卡以设置社区属性：

   在**特定社区**下：

   1. 点击**无** 单选按钮以从用于传递路由映射的前缀中删除社区属性。
   2. 点击**特定社区**单选按钮以输入社区编号（如果适用）。有效值范围为 1 至 4294967295。
   3. 选中**添加到现有社区**以将社区添加到已经现有的社区。
   4. 选中 **Internet**、**无通告**或**无导出**复选框以使用已知社区之一。

   在**特定扩展社区**下的**路由目标**字段中，输入 *ASN:nn* 格式的路由目标编号：

   - 您可以输入在 1:1 到 65534:65535 范围内的值。

     您可以在单个条目中添加单个路由目标或一组以逗号分隔的路由目标。例如*1:2,1:4,1:6*。
   - 一个条目中最多可以包含 8 个路由目标。
   - 路由映射中不能包含多余的路由目标条目。

3. 点击**其他**选项卡以设置其他属性。

   1. 选中**设置自动标签**复选框以自动计算标签值。
   2. 在**设置本地首选项**字段中输入自治系统路径的首选项值。输入 0 到 4294967295 之间的值。
   3. 在**设置权重**字段中输入路由表的 BGP 权重。输入 0 到 65535 之间的值。
   4. 选择指定 BGP 源代码。有效值为**本地 IGP** 和**不完整**。
   5. 在“IPv4 设置”部分中，指定数据包输出到的下一跳的下一跳 IPv4 地址。它不需要是相邻路由器。如果指定多个 IPv4 地址，则数据包可以在任一 IP 地址输出。

      选择在**前缀列表**下拉列表中指定 IPv4 前缀列表。
   6. 在“IPv6 设置”部分中，指定数据包输出到的下一跳的下一跳 IPv6 地址。它不需要是相邻路由器。如果指定多个 IPv6 地址，则数据包可以在任一 IP 地址输出。

      选择在**前缀列表**下拉列表中指定 IPv6 前缀列表。

步骤 8 点击**添加 (Add)**。

步骤 9 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖 ， 第 969 页。

步骤 10 点击**保存 (Save)**。

安全情报

安全情报功能需要 威胁许可证（适用于 威胁防御 设备）或保护许可证（所有其他设备类型）。

安全情报 列表 和 源 是 IP 地址，域名和 URL 的集合，可用于快速过滤与列表或源上的条目匹配的流量。

- 列表是一个可手动管理的静态集合。
- 源是按一定间隔通过 HTTP 或 HTTPS 更新的动态集合。

安全情报列表/源分组为：

- DNS （域名）
- 网络 （IP 地址）
- URL

系统-提供的源

Cisco 提供以下源作为安全情报对象：

- 安全情报源定期更新来自以下方面的最新威胁情报：Talos
  - Cisco-DNS-and-URL-Intelligence-Feed（在 DNS 列表和源下）
  - Cisco 智能馈送（对于 IP 地址，在网络列表和馈送下）

  虽然无法删除系统提供的源，但可以更改其更新频率（或禁用更新）。
- Cisco-TID-Feed（在网络列表和源下）

  此源不在访问控制策略的“安全情报”选项卡中使用。

  相反，您必须启用并配置 Cisco Secure Firewall 威胁智能导向器 以使用此源，它是 TID 可观察对象数据的集合。

  可以使用此对象来设置将此类数据发布到 TID 元素的频率。

预定义列表：全局阻止列表和全局不阻止列表

系统随附域（DNS）、IP 地址（网络）和 URL 的预定义全局阻止列表和不阻止列表。

这些列表在您填充之前为空。要构建这些列表，请参阅 全局和域安全情报列表，第 1027 页。

默认情况下，访问控制和 DNS 策略使用这些名单作为安全情报的一部分。

自定义源

您可以使用第三方源，或者，利用自定义内部源，您可以在具有多个Cisco Secure Firewall Management Center设备的大型部署中轻松维护企业级阻止列表。

请参阅自定义安全情报源，第 1033 页。

自定义列表

自定义列表可扩充和微调源和全局列表。

请参阅自定义安全情报列表，第 1035 页。

自定义安全情报列表和源使用的地方

- IP 地址和地址块 - 用于访问控制策略的阻止列表和不阻止列表，作为安全情报的一部分。
- 域名 - 用于 DNS 策略的阻止列表和不阻止列表，作为安全情报的一部分。
- URL - 用于访问控制策略的阻止列表和不阻止列表，作为安全情报的一部分。此外，您还可以在访问控制和 QoS 规则中使用 URL 列表，这些规则的分析和处理阶段发生在安全情报之后。

如何修改安全情报对象

要添加或删除阻止列表、不阻止列表、源或 Sinkhole 对象中的条目，请执行以下操作：

对象类型	编辑功能	编辑后是否需要重新部署？
自定义阻止和不阻止列表	使用对象管理器上传新列表和替代列表。	不支持
默认（但自定义填充）阻止列表和不阻止列表：全局、后代和特定域	使用上下文菜单来添加条目或使用对象管理器删除条目。	不支持
系统提供的情报源	使用对象管理器禁用或更改更新频率。	否
自定源	使用对象管理器进行全面修改。	否
Sinkhole	使用对象管理器进行全面修改。	是

全局和域安全情报列表

Firepower管理中心随附空的全局阻止和不阻止列表，您可以随时向网络中的事件立即添加URL，域和 IP 地址。这些列表允许您使用安全情报始终阻止特定连接，或通过安全情报免除特定连接的阻止，从而允许您已配置的其他威胁检测进程对其进行评估。

例如，如果注意到入侵事件中的一组可路由IP地址涉及漏洞攻击尝试，可以立即阻止这些IP地址。虽然更改可能需要几分钟时间才能完成传播，但您无需重新部署。

默认情况下，访问控制和DNS策略使用这些适用于所有安全区域的全局列表。您可以为每个策略选择不使用这些列表。

注释 这些选项仅适用于安全情报。安全情报无法阻止已使用快速路径的流量。同样，安全情报也不会自动将受信任或快速路径匹配流量列入不阻止列表。有关详细信息，请参阅关于安全情报，第1359页。

在多域部署中，可以选择要通过向域列表和全局列表添加项目来实施列入阻止列表或从安全情报阻止中排除操作的 Firepower 系统域；请参阅 安全情报列表和多租户，第 1028 页。

安全情报列表和多租户

在多域部署中，全局域拥有全局阻止列表和不阻止列表。只有全局管理员才可以在全局列表中添加或删除项目。因此，子域用户可以将网络、域名和 URL 列入阻止列表和不阻止列表，多租户则添加：

- 域列表 - 内容只适用于特定子域的阻止列表和不阻止列表。全局列表是全局域的域列表。
- 后代域列表 - 汇聚当前域的后代的域列表的阻止列表和不阻止列表。

域列表

除了能够访问（但不能编辑）全局列表之外，每个子域都具有自己的命名列表，命名列表的内容只应用于该子域。例如，名为 Company A 的子域拥有：

- 域阻止列表-公司 A 和域不阻止列表-公司 A
- DNS 域阻止列表-公司 A，DNS 的域不阻止列表-公司 A
- URL 域阻止列表-公司 A，URL 的域不阻止列表-公司 A

当前或以上域中的任何管理员都可以填充这些列表。您可以用情景菜单将当前及所有后代域中的项目列入阻止列表和不阻止列表。但只有关联域中的管理员可以删除域列表中的项目。

例如，全局管理员可以选择将全局域和公司 A 的域中的相同 IP 地址列入阻止列表，但不能在公司 B 的域中将其列入阻止列表。此操作会将 IP 地址添加到：

- 全局阻止列表（只有全局管理员可以将其删除）
- 域阻止列表 - 公司 A（只有公司 A 管理员可以将其删除）

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

后代域列表

后代域列表是汇聚当前域的后代的域列表的不阻止列表和阻止列表。分叶域没有后代域列表。

后代域列表很有用，因为较高级别的域管理员可以执行通用安全情报设置，但仍允许子域用户将其自己部署中的项目列入阻止列表和不阻止列表。

例如，全局域具有以下后代域列表：

- 后代阻止列表 - 全局、后代不阻止列表 - 全局

- 后代 DNS 阻止列表 - 全局、后代 DNS 不阻止列表 - 全局
- 后代 URL 阻止列表 - 全局、后代 URL 不阻止列表 - 全局

注释 后代域列表不显示在对象管理器中，因为它们是象征性汇聚，不是手动填写列表。它们显示在您可以使用它们的位置：访问控制策略和 DNS 策略。

将条目添加到全局安全情报列表

查看事件和控制面板时，您可以通过将这些事件中显示的 IP 地址、域和 URL 添加到预定义的阻止列表，立即阻止这些流量。

同样，如果安全情报阻止了您希望在安全情报阻止之后由威胁检测进程评估的流量，则可以将事件中的 IP 地址、域和 URL 添加到预定义的“不阻止”列表。

在威胁检测的安全情报阶段，将根据这些列表中的条目评估流量。

有关这些列表的详细信息，请参阅 全局和域安全情报列表，第 1027 页。

开始之前

由于将条目添加到安全情报列表会影响访问控制，因此必须具有以下其中一种角色：

- 管理员
- 角色的组合：网络管理员或访问管理员，加上安全分析师和安全审批人
- 同时具有“修改访问控制策略”(Modify Access Control Policy) 和“将配置部署到设备”(Deploy Configuration to Devices) 权限的自定义角色

如果适用，请验证这些列表是否用于您期望使用它们的策略中。

过程

步骤 1 导航至包含要始终使用安全情报阻止或免于安全情报阻止的 IP 地址、域或 URL 的事件。

步骤 2 右键点击 IP 地址、域或 URL，然后选择相应的选项：

项目类型	上下文菜单选项
IP 地址	将 IP 添加到阻止列表 将 IP 添加到不阻止列表 这些选项将 IP 地址添加到相应的网络列表。
URL	将 URL 添加到 URL 的全局阻止列表 将 URL 添加到 URL 的全局不阻止列表

项目类型	上下文菜单选项
URL 字段中的 URL 域	将域添加到 URL 的全局阻止列表 将域添加到 URL 的全局不阻止列表
DNS 查询字段中的域	将域添加到 DNS 的全局阻止列表 将域添加到 DNS 的全局不阻止列表

下一步做什么

您无需重新部署即可使这些更改生效。

如果要从列表中删除项目，请参阅从全局安全情报列表中删除条目，第 1030 页。

从全局安全情报列表中删除条目

注释

- 在多域部署中，这些列表的名称可能不是“全局”。有关详细信息，请参阅安全情报列表和多租户，第 1028 页。
- 要向这些列表中添加条目，请参阅将条目添加到全局安全情报列表，第 1029 页。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 请点击**安全情报 (Security Intelligence)**。

步骤 3 点击适当的选项：

- **网络列表和源** （对于 IP 地址）
- **DNS 列表和源** （用于域名）
- **URL 列表和源**

步骤 4 点击“全局阻止”(Global Block) 或“全局不阻止”(Global Do-Not-Block) 列表旁边的铅笔。

步骤 5 点击要删除的条目旁边的垃圾桶按钮。

安全情报的列表和源更新

列表和源更新会将现有列表或源文件替换为新文件的内容。现有文件和新文件的内容不会合并。

如果系统下载损坏的源或具有无法识别的条目的源，则系统会继续使用旧源数据（除非是第一次下载）。但是，如果系统可以识别即便源中的一个条目，也会使用其可识别的条目。

默认情况下，各个源每两小时更新一次管理中心，您可以修改频率。管理中心收到的任何更新都会立即传递到托管设备。此外，托管设备每 30 分钟轮询一次 FMC 以了解更改。您无法修改此频率。

在多域部署中，系统提供的源属于全局域，并且只能由该域中的管理员进行修改。您可以修改属于您的域的自定义源的更新频率。

要修改源更新间隔，请参阅更改安全情报源的更新频率，第 1031 页。

更改安全情报源的更新频率

您可以指定 Firepower 管理中心更新安全情报源的间隔。

有关源更新的详细信息，请参阅安全情报的列表和源更新，第 1030 页。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开**安全情报 (Security Intelligence)** 节点，然后选择要更改其频率的源类型。

系统提供的 URL 源与 **DNS 列表和源**下的域源合并。

步骤 3 在要更新的源旁边，点击 **编辑**（）。

如果显示**视图**（），则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 编辑 **Update Frequency**。

步骤 5 点击**保存 (Save)**。

自定义安全情报列表和源

自定义列表和源：要求

列表和源格式

每个列表或源必须是不大于 500 MB 的简单文本文件。列表文件必须包括 .txt 扩展名。每行包括一个条目或注释：一个 IP 地址、一个 URL、一个域名。

提示 可包含的条目数受该文件的最大大小限制。例如，没有注释、平均 URL 长度为 100 个字符（包括 Punycode 或百分比 Unicode 表示和换行符）的 URL 列表可包含 524 万个以上条目。

在 DNS 列表条目中，您可以为域标签指定星号 (*) 通配符。所有标签都与通配符匹配。例如，条目 `www.example.*` 与 `www.example.com` 和 `www.example.co` 均匹配。

如果在源文件中添加注释行，则其必须以井号(#)字符开头。如果上传具有注释的源文件，则系统会在上传期间删除注释。您下载的源文件包含不带注释的所有条目。

源要求

配置源时，可使用 URL 指定位置；但 URL 不能使用 Punycode 编码。

对于 30 分钟或更短的源更新间隔，必须指定 MD5 URL。这可以防止频繁下载未更改的源。如果源服务器未提供 MD5 URL，则必须使用至少 30 分钟的下载间隔。

如果您使用 MD5 校验和，校验和必须存储在仅带有该校验和的简单文本文件中。不支持注释。

URL 列表和源：URL 语法和匹配条件

安全智能URL列表和源（包括全局阻止列表和不阻止列表中的自定义列表和源和条目）可以包括以下内容，它们具有所述的匹配行为：

- 主机名

  例如，**www.example.com**。

- URL

  example.com 匹配 **example.com** 和所有子域，包括 **www.example.com**、**eu.example.com**、**example.com/abc** 和 **www.example.com/def** -- 但不包括 **example.co.uk** 或 **examplexyz.com** 或 **example.com.malicious-site.com**

  您也可以包括整个 URL 路径，例如 **https://www.cisco.com/c/en/us/products/security/firewalls/index.html**

- URL 末尾的斜杠，用于指定精确匹配项

  example.com/ 仅匹配 **example.com**；它不匹配 **www.example.com** 或任何其他 URL。

- 表示 URL 中任何域的通配符 (*)

  星号可以表示由点分隔的完整域字符串，但不能表示部分域字符串，也不能表示URL中第一个斜杠后面的任何部分。

  有效示例：

  - ***.example.com**
  - **www.*.com**
  - **example.***

    （例如，这将匹配 **example.com** 和 **example.org** 和 **example.de**，但不匹配 **example.co.uk**）

  - ***.example.***
  - **example.*/**

  无效示例：

- **example*.com**
- **example.com/***

- IP 地址 (IPv4)

  对于 IPv6 地址，或者要使用范围或 CIDR 表示法，请使用安全智能网络对象。

  您可以包含一个或多个表示八位组的通配符，例如 10.10.10.* 或 10.10.*.*。

另请参阅自定义安全情报列表，第 1035 页。

自定义安全情报源

自定义或第三方安全情报源允许您使用互联网上其他定期更新且信誉良好的不阻止列表和阻止列表来扩充系统提供的情报源。也可以设置内部源；如果要使用一个源列表来更新部署中的多个 Cisco Secure Firewall Management Center 设备，这将会很有用。

注释 您不能通过在安全情报源中使用 /0 网络掩码，将地址块列入阻止列表或不阻止列表。如果要监控或阻止策略所针对的所有流量，请分别使用包含**监控 (Monitor)** 或**阻止 (Block)** 规则操作的访问控制规则，并对**源网络 (Source Networks)** 和**目标网络 (Destination Networks)** 使用默认值 any。

您也可以将系统配置为使用MD5校验和来确定是否下载更新的源。如果校验和自上次系统下载源以来没有更改，则系统无需重新下载该源。您可能希望将MD5校验和用于内部源，尤其是那些很大的内部源。

注释 在下载自定义源时，系统不执行对等 SSL 证书验证，系统也不支持使用证书捆绑包或自签证书来验证远程对等设备。

如果要对系统从互联网更新源的时间进行严格控制，可以禁用该源的自动更新。但是，自动更新可确保获取最新的相关数据。

手动更新安全情报源会更新所有源，包括情报源。

请参阅 自定义列表和源：要求，第 1031 页完成要求

创建安全情报源

您必须拥有 威胁 许可证（适用于 威胁防御 设备）或保护许可证（所有其他设备类型）。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开**安全情报 (Security Intelligence)** 节点，然后选择要添加的源类型。

步骤 3 点击适合您在上方所选源类型的选项：

- 添加网络列表和源（对于 IP 地址）
- 添加 **DNS** 列表和源 **(Add DNS Lists and Feeds)**
- 添加 **URL** 列表和源 **(Add URL Lists and Feeds)**

步骤 4 为源输入**名称 (Name)**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 从**类型 (Type)** 下拉列表中选择**源 (Feed)**。

步骤 6 输入**源 URL (Feed URL)**。

步骤 7 输入 **MD5 URL**。

这用于确定自上次更新以来源内容是否已更改，因此系统不会下载未更改的源。

小于 30 分钟的更新间隔需要 MD5 URL。

如果源服务器未提供 MD5 URL，则必须选择至少 30 分钟的间隔。

步骤 8 选择**更新频率 (Update Frequency)**。

步骤 9 点击**保存 (Save)**。

除非已禁用源更新，否则系统会尝试下载并验证源。

手动更新安全情报源

您必须拥有 威胁 许可证（适用于 威胁防御 设备）或保护许可证（所有其他设备类型）。

开始之前

必须至少将一个设备添加到管理中心。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开**安全情报 (Security Intelligence)** 节点，然后选择源类型。

步骤 3 点击**更新源 (Update Feeds)**，然后确认。

步骤 4 点击 **OK**。

Cisco Secure Firewall Management Center下载和验证源更新后，会将任何更改通知其受管设备。您的部署开始使用更新的源过滤流量。

自定义安全情报列表

安全情报列表是手动上传到系统的IP地址和地址块、URL或域名的简单静态列表。如果要扩充和微调单个Cisco Secure Firewall Management Center的受管设备的源或其中一个全局列表，自定义列表很有用。

例如，如果信誉良好的源错误地阻止对重要资源的访问，但整体来说对组织有用，您即可创建仅包含分类不当的 IP 地址的自定义不阻止列表，而不是从访问控制策略的阻止列表中删除 IP 地址源对象。

注释 您不能通过在安全情报列表中使用 `/0` 网络掩码，将地址块列入阻止列表或不阻止列表。如果要监控或阻止策略所针对的所有流量，请分别使用包含**监控 (Monitor)** 或**阻止 (Block)** 规则操作的访问控制规则，并对**源网络 (Source Networks)** 和**目标网络 (Destination Networks)** 使用默认值 `any`。

有关列表条目格式，请注意以下事项：

- 地址块的网络掩码可以是 `0` 到 `32` 之间或 `0` 到 `128` 之间的整数（分别适用于 IPv4 和 IPv6）。
- 域名中的 Unicode 必须使用 Punycode 格式进行编码，并且不区分大小写。
- 域名中的字符不区分大小写。
- URL 中的 Unicode 应使用百分比编码格式进行编码。
- URL 子目录中的字符区分大小写。
- 以井号 (`#`) 开头的列表条目被视为注释。
- 请参阅 自定义列表和源：要求 ，第 1031 页中的其他格式要求。

有关匹配的列表条目，请注意以下事项：

- 如果在 URL 或 DNS 列表中存在较高级别的域，则系统与子级别域匹配。例如，如果将 `example.com` 添加到 DNS 列表，则系统与 `www.example.com` 和 `test.example.com` 均匹配。
- 系统不对 DNS 或 URL 列表条目执行 DNS 查找（正向或反向）。例如，如果向 URL 列表中添加 `http://192.168.0.2`，并且其解析为 `http://www.example.com`，则系统仅与 `http://192.168.0.2` 匹配，而与 `http://www.example.com` 不匹配。

将新的安全情报列表上传到 Cisco Secure Firewall Management Center

要修改安全情报列表，必须更改源文件并上传新副本。不能使用 Web 界面来修改文件内容。如果您无法访问源文件，可以从系统下载副本。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开**安全情报 (Security Intelligence)** 节点，然后选择列表类型。

步骤 3 点击适合您在上方所选列表的选项：

- **添加网络列表和源**（对于 IP 地址）
- **添加 DNS 列表和源 (Add DNS Lists and Feeds)**
- **添加 URL 列表和源 (Add URL Lists and Feeds)**

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 从**类型 (Type)** 下拉列表中，选择**列表 (List)**。

步骤 6 点击 **Browse** 浏览至列表 `.txt` 文件，然后点击 **Upload**。

步骤 7 点击**保存 (Save)**。

下一步做什么

您无需重新部署这些更改即可生效。如果要从列表中删除条目，请参阅从全局安全情报列表中删除条目，第 1030 页。

更新安全情报列表

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 展开**安全情报 (Security Intelligence)** 节点，然后选择列表类型。

步骤 3 在要更新的列表旁边，点击 **编辑**（ ）。

如果显示**视图**（ ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 如果需要对要编辑的列表保留副本，请点击**下载**，然后按照浏览器的提示将该列表另存为文本文件。

步骤 5 根据需要对列表进行更改。

步骤 6 在“安全情报”弹出窗口中，点击**浏览**以浏览到修改后的列表，然后点击**上传**。

步骤 7 点击**保存 (Save)**。

下一步做什么

您无需重新部署这些更改即可生效。如果要从列表中删除条目，请参阅从全局安全情报列表中删除条目，第 1030 页。

Sinkhole

Sinkhole 对象代表为 Sinkhole 中所有域名提供非可路由地址的 DNS 服务器或没有解析到服务器的 IP 地址。您可以在 DNS 策略规则中引用 Sinkhole 对象，以将匹配流量重定向到 Sinkhole。您必须为对象同时分配 IPv4 地址和 IPv6 地址。

创建 Sinkhole 对象

您必须拥有 威胁 许可证（适用于 威胁防御 设备）或保护许可证（所有其他设备类型）。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择 **Sinkhole**。

步骤 3 点击**添加 Sinkhole (Add Sinkhole)**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 输入 Sinkhole 的 **IPv4 地址 (IPv4 Address)**和 **IPv6 地址 (IPv6 Address)**。

步骤 6 您有以下选择：

- 如果要将流量重定向到 Sinkhole 服务器，请选择**记录与 Sinkhole 的连接 (Log Connections to Sinkhole)**。
- 如果要将流量重定向到非解析 IP 地址，请选择**阻止并记录与 Sinkhole 的连接 (Block and Log Connections to Sinkhole)**。

步骤 7 如果要将危害表现 (IoC) 类型分配给 Sinkhole，请从**类型 (Type)** 下拉列表中选择一种类型。

步骤 8 点击**保存 (Save)**。

SLA 监控器

每个互联网协议服务级别协议 (SLA) 监控器定义受监控地址的连接策略，并跟踪地址路由的可用性。通过发送 ICMP 回应请求并等待响应，定期检查路由的可用性。如果请求超时，路由将从路由表中删除并使用备份路由来替换。SLA 监控作业在部署后立即开始并持续运行，除非您从设备配置移除 SLA 监控器（即，监控器并未过期）。互联网协议服务级别协议 (SLA) 监控器对象用在 IPv4 静态路由策略的“路由跟踪”字段中。IPv6 路由无法选择通过路由跟踪使用 SLA 监控器。

您可以将这些对象与 威胁防御 设备一起使用。

过程

步骤 1 依次选择**对象 (Object)** > **对象管理 (Object Management)** 并从目录中选择 **SLA 监控器 (SLA Monitor)**。

步骤 2 点击**添加 SLA 监控器 (Add SLA Monitor)**。

步骤 3 在**名称 (Name)** 字段中输入对象的名称。

步骤 4 （可选）在**说明**字段中输入对象的说明。

步骤 5 在**频率 (Frequency)** 字段中输入 ICMP 回应请求传输的频率（以秒为单位）。有效值范围为 1 到 604800 秒（7 天）。默认值为 60 秒。

注释 频率不能小于超时值；您必须将频率转换为毫秒才可比较两个值。

步骤 6 在 **SLA 监控器 ID** 字段中输入 SLA 操作的 ID 编号。值范围为 1 到 2147483647。在一个设备上最多可以创建 2000 个 SLA 操作。每个 ID 编号在策略和设备配置中必须是唯一的。

步骤 7 在**阈值**字段中，输入在 ICMP 回应请求之后且在宣告上升阀值之前必须经过的时间（以毫秒为单位）。值的范围为 0 到 2147483647 毫秒。默认值为 5000 毫秒。阈值仅用于指示超过定义值的事件。可以使用这些事件来评估适合的超时值。它不是受监控地址可达性的直接指标。

注释 阈值不应超过超时值。

步骤 8 在**超时 (Timeout)** 字段中，输入 SLA 操作等待 ICMP 回应请求响应的时间量（以毫秒为单位）。值范围为 0 到 604800000 毫秒（7 天）。默认值为 5000 毫秒。如果在此字段中定义的时间内未从受监控地址收到响应，则从路由表中删除静态路由并用备份路由来替换。

注释 超时值不能超过频率值（将频率值转换为毫秒以比较两个数字）。

步骤 9 在**数据大小 (Data Size)** 字段中输入 ICMP 请求数据包负载的大小（以字节为单位）。值范围为 0 到 16384 字节。默认值为 28 字节，它会创建一个总计 64 字节的 ICMP 数据包。请勿将此值设置为高于协议或路径最大传输单位 (PMTU) 允许的最大值。为了实现可达性，可能需要增大默认数据大小，以检测源和目标之间的 PMTU 更改。低 PMTU 会影响会话性能，如果检测到此情况，则可能表示应使用辅助路径。

步骤 10 在 **ToS** 字段中输入在 ICMP 请求数据包的 IP 报头中定义的服务类型 (ToS) 的值。值范围为 0 到 255。默认值为 0。此字段包含延迟、优先级、可靠性等信息。可供网络上其他设备用于策略路由和承诺接入速率等功能。

步骤 11 在**数据包数量 (Number of Packets)** 字段中输入发送的数据包数量。值范围为 1 到 100。默认为 1 个数据包。

注释 如果担心丢包可能会错误地导致 Cisco Secure Firewall Threat Defense设备认为受监控的地址无法访问，则请增加默认数据包数量。

步骤 12 在**受监控的地址 (Monitored Address)** 字段中，输入由 SLA 操作监控其可用性的 IP 地址。

步骤 13 **可用区域**列表同时显示区域和接口组。在**区域/接口**列表中，添加包含设备可通过其与管理站通信的接口的区域或接口组。要指定单个接口，则需要为该接口创建区域或接口组；请参阅创建安全区域和接口组对象，第 496 页。仅在设备包含所选接口或区域时，系统才会在设备上配置主机。

步骤 14 点击**保存 (Save)**。

时间范围

使用时间范围对象定义用于确定规则应用时间的时间段。

注释 从 管理中心 7.0 开始，Snort 3 也支持基于时间的 ACL。

创建时间范围对象

如果希望策略仅在指定的时间范围内应用，请创建一个时间范围对象，然后在策略中指定该对象。请注意，此对象仅适用于 威胁防御 设备。

只能在本主题底部列出的策略类型中指定时间范围对象。

注释 时区表示设备的本地时间，仅用于在支持时间范围的策略中应用时间范围。时区不会更改设备的配置时间。要验证配置，请在 威胁防御 CLI 中，使用 **show time-range timezone** 和 **show time** 命令（请参阅 Cisco Secure Firewall Threat Defense 命令参考 指南）。此外，机箱的时区会覆盖管理中心时区。

开始之前

根据与处理流量的设备关联的时区应用时间范围。默认情况下为 UTC。要更改与设备关联的时区，请转至 **设备 > 平台设置**。

过程

步骤 1 选择**对象 > 对象管理**。

步骤 2 从对象类型列表中，选择**时间范围**。

步骤 3 点击**添加时间范围 (Add Time Range)**。

步骤 4 输入值。

请遵守以下准则：

- 如果您在输入的对象名称周围看到一个红色的错误框，则将光标移到**名称**字段上可查看命名限制。
- 所有时间均为 UTC，除非您在 **设备 > 平台设置**中为设备指定时区。
- 使用 24 小时制时钟输入时间。例如，输入 13:30 表示 13:30。
- 要指定一个连续的范围，例如典型的周末时间（星期五下午 5 点到星期一上午 8 点，包括晚上和夜晚），请选择“范围类型”**范围**。

- 要指定多天的一部分，例如星期一到星期五的上午 8 点到下午 5 点（不包括每日的晚上、夜晚和凌晨），请选择“范围类型”**每日间隔**。
- 您可以在单个对象中最多指定 28 个时间段。
- 要为一天或不同天的不同时间制定多个不连续时间，请创建多个重复间隔。例如，要在标准工作时间以外的所有时间应用策略，请创建一个具有以下两个重复间隔的单个时间范围对象：
  - 星期一到星期五的下午 5 点到上午 8 点的每日间隔，以及
  - 星期五下午 5 点到星期一上午 8 点的范围重复间隔。

步骤 5 点击**保存 (Save)**。

下一步做什么

配置以下任意时间范围：

- 访问控制规则
- 预过滤器规则
- 隧道规则
- VPN 组策略

在 VPN 组策略对象中，使用 **访问时间** 字段指定时间范围对象。有关详细信息，请参阅配置组策略对象，第 1063 页和组策略高级选项，第 1069 页。

时区

要为托管设备指定本地时区，请创建时区对象，并在分配给设备的设备平台设置策略中指定该对象。

该设备本地时间仅用于在支持时间范围的策略（例如访问控制、预过滤器和VPN组策略）中应用规则中的时间范围。如果不为设备分配时区，在这些策略中应用时间范围时，将默认使用 UTC。系统中的任何其他功能都不会使用时区对象中指定的时区。

只有 威胁防御 设备支持时区对象。

注释 从 管理中心 7.0 开始，Snort 3 也支持基于时间的 ACL。

隧道区域

隧道区域代表您为进行特殊分析而明确标记的特定类型的明文、传递隧道。虽然您可以将隧道区域用作某些配置中的接口限制，但它不是接口对象。

有关详细信息，请参阅隧道区域与预过滤 ， 第 1403 页。

URL

重要事项 有关在安全情报配置中使用此选项和类似选项的最佳实践，以及访问控制 和 QoS 策略中的 URL 规则，请参阅 手动 URL 过滤选项 ， 第 1348 页。

URL 对象定义单个 URL 或 IP 地址，而 URL 组对象可以定义多个 URL 或地址。您可在系统 Web 界面中的不同位置使用 URL 对象和对象组，包括访问控制策略和事件搜索。

在创建 URL 对象时，请记住以下要点：

- 如果不包含路径（即 URL 中无 / 字符），则匹配仅基于服务器主机名。如果主机名位于 :// 分隔符之后，或在主机名中的任何点之后，则认为该主机名匹配。例如，ign.com 匹配 ign.com 和 www.ign.com，但不匹配 verisign.com。
- 如果包含一个或多个 / 字符，则整个 URL 字符串将用于子字符串匹配，其中包括服务器名称、路径和任何查询参数。但是，我们建议您不要使用手动URL过滤阻止或允许个别网页或部分网站，因为这样可能会重组服务器并将页面移至新路径。子字符串匹配还可能导致意外匹配，其中 URL 对象中包含的字符串也与非预期服务器上的路径或查询参数中的字符串匹配。
- 系统忽略加密协议（HTTP 与 HTTPS）。换句话说，如果阻止网站，系统将阻止发往该网站的 HTTP 和 HTTPS 流量，除非您使用一个应用条件指定特定协议。在创建 URL 对象时，您不需要指定创建对象时的协议。例如，使用 example.com 而不是 http://example.com。
- 如果您计划使用 URL 对象匹配访问控制规则中的 HTTPS 流量，请使用加密流量时所使用的公钥中的使用者公用名创建该对象。此外，系统会忽略使用者公用名中的子域，因此，不包括子域信息。例如，使用 example.com 而不是 www.example.com。

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

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

创建 URL 对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择 **URL**。

步骤 3 从**添加 URL (Add URL)** 下拉列表中选择**添加对象 (Add Object)**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 输入**说明 (Description)**（可选）。

步骤 6 输入 **URL** 或 IP 地址。

步骤 7 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 969 页。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 969 页。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

变量集

变量代表通常在入侵规则中用来识别源 IP 地址、目标 IP 地址、源端口和目标端口的值。还可以在入侵策略中使用变量表示规则禁止、自适应配置文件和动态规则状态中的 IP 地址。

提示 无论入侵规则中使用的网络变量定义的主机如何，预处理器规则都可以触发事件。

可以使用变量集对变量进行管理、自定义和分组。可以使用系统提供的默认变量集，也可以创建您自己的自定义变量集。可以在任何变量集中修改预定义默认变量，以及添加和修改用户定义的变量。

系统提供的大多数共享对象规则和标准文本规则均使用预定义的默认变量来定义网络和端口号。例如，大部分规则使用变量 `$HOME_NET` 指定受保护网络，使用变量 `$EXTERNAL_NET` 指定未受保护（或外部）网络。此外，专用规则通常会使用其他预定义的变量。例如，检测针对网络服务器的漏洞攻击的规则使用 `$HTTP_SERVERS` 和 `$HTTP_PORTS` 变量。

当变量更准确地反映网络环境时，规则更加有效。至少应修改默认变量集中的的默认变量。通过确保变量（例如 $HOME_NET）正确地定义网络且 $HTTP_SERVERS 包括网络上的所有网络服务器，从而优化处理和监控所有相关系统的可疑活动。

要使用变量，请将变量集链接到与访问控制规则相关的入侵策略或访问控制策略的默认操作。默认情况下，默认设置集链接到访问控制策略使用的所有入侵策略。

将一个变量添加到任意变量集会将其添加到所有变量集；也就是说，每个变量集都是系统中当前配置的所有变量的集合。在任何变量集中，都可以添加用户定义的变量以及自定义任何变量的值。

最初，系统提供由预定义默认值组成的单个默认变量集。默认变量集中的每个变量最初设置为其默认值，对于预定义变量，该默认值是由Talos 情报小组 设置并在规则更新中提供的值。

虽然可以将预定义默认变量保留为所配置的默认值，但思科建议您修改预定义变量的子集。

可以仅使用默认变量集中的变量，但在许多情况下，执行以下操作可得到最大益处：添加一个或多个自定义变量集；在不同变量集中配置不同的变量值；甚至添加新变量。

使用多个变量集时务必谨记，默认变量集中任何变量的当前值决定所有其他变量集中该变量的默认值。

如果选择“对象管理器”(Object Management) 页面上的**变量集 (Variable Sets)**，则对象管理器会列出默认变量集以及您创建的任何自定义变量集。

在全新安装的系统上，默认变量集仅由思科预定义的默认变量组成。

每个变量集都包括系统提供的默认变量以及从任何变量集添加的所有自定义变量。请注意，可以编辑默认变量集，但不能重命名或删除默认变量集。

在多域部署中，系统会为每个子域生成默认变量集。

注意 导入访问控制策略或入侵策略会以导入的默认变量覆盖默认变量集中的现有默认变量。如果现有默认变量集包含不属于导入默认变量集的自定义变量，则会保留该唯一的变量。

相关主题

管理变量，第 1054 页
管理变量集，第 1053 页

入侵策略中的变量集

默认情况下，Firepower 系统会将默认变量集链接到访问控制策略中使用的所有入侵策略。部署使用入侵策略的访问控制策略时，入侵策略中已启用的入侵规则将使用已链接变量集中的变量值。

修改访问控制策略中的入侵策略所使用的自定义变量集时，系统会反映该策略的状态，在 Access Control 页面上将其状态显示为过时。必须重新部署该访问控制策略，才能使变量集的更改生效。修改默认变量集时，系统会将使用入侵策略的所有访问控制策略的状态显示为过时，因此，必须重新部署所有访问控制策略才能使更改生效。

变量

变量属于以下类别之一：

默认变量

Firepower 系统提供的变量。不能重命名或删除默认变量，也不能更改其默认值。但是，可以创建默认变量的自定义版本。

自定义变量

您创建的变量。这些变量可包括：

- 自定义的默认变量

  编辑默认变量的值时，系统会将该变量从“默认变量”(Default Variables) 区域转移到“自定义变量”(Customized Variables) 区域。由于默认变量集中的变量值决定自定义变量集中变量的默认值，因此，自定义默认变量集中的默认变量会修改所有其他变量集中该变量的默认值。

- 用户定义的变量

  您可以添加和删除自己的变量，在不同变量集中自定义这些变量的值，以及将自定义变量重置为默认值。重置用户定义的变量时，该变量保留在“自定义变量”(Customized Variables) 区域。

  用户定义的变量可以是以下类型之一：

  - 网络变量指定网络流量中的主机的 IP 地址。
  - 端口变量指定网络流量中的 TCP 或 UDP 端口，包括这两种端口类型的值 `any`。

例如，如果您创建自定义标准文本规则，您可能还希望添加自己的用户定义的变量，以便更准确地反映流量或作为快捷方式简化规则创建过程。或者，如果创建只检查“隔离区”(DMZ) 中流量的规则，可以创建名为 `$DMZ` 的变量，其值列出已暴露的服务器 IP 地址。这样，在所有为该区域编写的所有规则中都可以使用 `$DMZ` 变量。

高级变量

Firepower 系统在特定情况下提供的变量。这些变量的部署非常有限。

预定义默认变量

默认情况下，Firepower 系统提供一个由预定义默认变量组成的默认变量集。Talos 情报小组 使用规则更新来提供新的和已更新的入侵规则及其他入侵策略元素，包括默认变量。

由于系统提供的许多入侵规则使用预定义默认变量，因此应为这些变量设置适当的值。可以在任何或所有变量集中修改这些默认变量的值，具体取决于如何使用变量集识别网络流量。

⚠

注意 导入访问控制策略或入侵策略会以导入的默认变量覆盖默认变量集中的现有默认变量。如果现有默认变量集包含不属于导入默认变量集的自定义变量，则会保留该唯一的变量。

下表介绍系统提供的变量并指示通常会修改哪些变量。要获得为网络定制自定义变量方面的帮助，请联系专业服务或支持部门。

表 *80:* 系统提供的变量

变量名称	说明	是否修改？
$AIM_SERVERS	定义已知的 AOL Instant Messenger (AIM) 服务器，并用于基于聊天的规则和查找 AIM 漏洞攻击的规则。	不需要。
$DNS_SERVERS	定义域名服务 (DNS) 服务器。如果创建专门影响 DNS 服务器的规则，可以使用 $DNS_SERVERS 变量作为目标或源 IP 地址。	在当前规则集中不需要。
$EXTERNAL_NET	定义 Firepower 系统视为未受保护的网络，并在许多规则中用于定义外部网络。	需要；应该充分定义 $HOME_NET，然后避免将 $HOME_NET 作为 $EXTERNAL_NET 的值。
$FILE_DATA_PORTS	定义非加密端口，用于检测网络数据流中的文件的入侵规则。	不需要。
$FTP_PORTS	定义网络上 FTP 服务器的端口，用于 FTP 服务器漏洞攻击规则。	如果 FTP 服务器使用除默认端口以外的端口，需要修改（可以在 Web 界面中查看默认端口）。
$GTP_PORTS	定义数据包解码器用于提取 GTP（通用分组无线业务 [GPRS] 隧道协议）PDU 中的负载的数据信道端口。	不需要。
$HOME_NET	定义相关入侵策略监控的网络，用于许多定义内部网络的规则。	需要，以便包括内部网络的 IP 地址。
$HTTP_PORTS	定义网络上 Web 服务器的端口，用于 Web 服务器漏洞攻击规则。	如果网络服务器使用除默认端口以外的端口，需要修改（可以在 Web 界面中查看默认端口）。
$HTTP_SERVERS	定义网络上的 Web 服务器。用于 Web 服务器漏洞攻击规则。	如果运行 HTTP 服务器，需要修改。
$ORACLE_PORTS	定义网络上的 Oracle 数据库服务器端口，用于扫描针对 Oracle 数据库的攻击的规则。	如果运行 Oracle 服务器，需要修改。
$SHELLCODE_PORTS	定义希望系统对其扫描外壳代码漏洞的端口，用于检测使用外壳代码的漏洞的规则。	不需要。
$SIP_PORTS	定义网络上 SIP 服务器的端口，用于 SIP 服务器漏洞攻击规则。	不需要。
$SIP_SERVERS	定义网络上的 SIP 服务器，用于针对 SIP 的漏洞攻击的规则。	需要；如果运行 SIP 服务器，应该充分定义 $HOME_NET，然后包括 $HOME_NET 作为 $SIP_SERVERS 的值。

变量名称	说明	是否修改？
$SMTP_SERVERS	定义网络上的 SMTP 服务器，用于解决针对邮件服务器的漏洞的规则。	如果运行 SMTP 服务器，需要修改。
$SNMP_SERVERS	定义网络上的 SNMP 服务器，用于扫描针对 SNMP 服务器的攻击的规则。	如果运行 SNMP 服务器，需要修改。
$SNORT_BPF	识别传统高级变量，仅在 V5.3.0 之前的 Firepower 系统软件版本（后来升级到 V5.3.0 或更高版本）中的系统上存在该变量时，才会显示该变量。	不需要，只能查看或删除此变量。不能对其进行编辑，删除后也不能再恢复。
$SQL_SERVERS	定义网络上的数据库服务器，用于解决针对数据库的漏洞的规则。	如果运行 SQL 服务器，需要修改。
$SSH_PORTS	定义网络上 SSH 服务器的端口，用于 SSH 服务器漏洞攻击规则。	如果 SSH 服务器使用除默认端口以外的端口，需要修改（可以在 Web 界面中查看默认端口）。
$SSH_SERVERS	定义网络上的 SSH 服务器，用于解决针对 SSH 的漏洞的规则。	需要修改；如果运行 SSH 服务器，应该充分定义 $HOME_NET，然后包括 $HOME_NET 作为 $SSH_SERVERS 的值。
$TELNET_SERVERS	定义网络上的已知 Telnet 服务器，用于解决针对 Telnet 的漏洞的规则。	如果运行 Telnet 服务器，需要修改。
$USER_CONF	提供一个通用工具，让您能够配置无法通过网络界面使用的一个或多个功能。 存在冲突或重复的 $USER_CONF 配置会导致系统停止。	不需要，除非功能描述中有指示或在支持人员的指导下进行。

网络变量

网络变量代表可在已在入侵策略、入侵策略规则抑制、动态规则状态和自适应配置文件中启用的入侵规则中使用的 IP 地址。网络变量与网络对象和网络对象组的不同之处在于，网络变量特定于入侵策略和入侵规则，但可以使用网络对象和网络对象组在系统网络界面中的不同位置（包括访问控制策略、网络变量、入侵规则、网络发现规则、事件搜索和报告等）来代表 IP 地址。

可在以下配置中使用网络变量来指定网络上主机的 IP 地址：

- 入侵规则 - 通过入侵规则**源 IP (Source IPs)** 和**目标 IP (Destination IPs)** 报头字段，您可以将数据包检测限于源自或发往特定 IP 地址的数据包。
- 抑制 - 在特定 IP 地址或某个范围的 IP 地址触发入侵规则或预处理器时，通过源或目标入侵规则抑制中的**网络 (Network)** 字段，您可以抑制入侵事件通知。
- 动态规则状态 - 通过源或目标动态规则状态中的**网络 (Network)** 字段，您可以检测在给定时间段内出现入侵规则或预处理器规则的过多匹配项的情况。

- 自适应配置文件 - 启用自适应配置文件更新时，自适应配置文件**网络**字段识别您希望在其中改进被动部署中的数据包分段和 TCP 流的重组的主机。

在本节所述字段中使用变量时，链接至入侵策略的变量集决定使用该入侵策略的访问控制策略处理的网络流量中的变量值。

可以将以下网络配置的任意组合添加到变量：

- 从可用网络列表中选择的网络变量、网络对象和网络对象组的任意组合
- 从“新建变量”(New Variable) 或“编辑变量”(Edit Variable) 页面添加的单个网络对象（这些对象随后可添加到变量以及其他现有和将来的变量）
- 单个文字 IP 地址或地址块

  可以通过逐个添加来列出多个文字 IP 地址和地址块。可以单独列出 IPv4 和 IPv6 地址以及地址块，或者列出它们的任意组合。指定 IPv6 地址时，可使用 RFC 4291 中定义的任意寻址约定。

在任何变量中添加的包含网络的默认值是单词 `any`，它表示任意 IPv4 或 IPv6 地址。已排除网络的默认值为 `none`，它表示无网络。还可以使用文字值指定地址 `::`，以指示包含网络列表中的任何 IPv6 地址，或排除列表中没有 IPv6 地址。

将网络添加到排除列表会使指定的地址和地址块无效。也就是说，可以匹配除了被排除的 IP 地址或地址块以外的所有 IP 地址。

例如，排除文字地址 `192.168.1.1` 会指定除 192.168.1.1 以外的所有 IP 地址，排除 `2001:db8:ca2e::fa4c` 会指定除 2001:db8:ca2e::fa4c 以外的所有 IP 地址。

使用文字网络或可用网络可以排除任意的网络组合。例如，排除文字值 `192.168.1.1` 和 `192.168.1.5` 会包含除 192.168.1.1 或 192.168.1.5 以外的任何 IP 地址。也就是说，系统将此解释为“**既不是** 192.168.1.1 **也不是** 192.168.1.5”，这就会匹配除括号中列出的 IP 地址以外的所有 IP 地址。

添加或编辑网络变量时，请注意以下几点：

- 在逻辑上，不能排除值 `any`，如果排除该值，将表示无地址。例如，不能将具有值 `any` 的变量添加到排除网络列表。
- 网络变量为指定的入侵规则和入侵策略功能识别流量。请注意，无论入侵规则中使用的网络变量定义的主机如何，预处理器规则都可以触发事件。
- 已排除的值必须解析到已包括的值的子集。例如，不能包含地址块 192.168.5.0/24 并排除 192.168.6.0/24。

端口变量

端口变量代表可在入侵策略中启用的入侵规则的**源端口 (Source Port)** 和**目标端口 (Destination Port)** 报头字段中使用的 TCP 和 UDP 端口。端口变量与端口对象和端口变量特定于入侵规则的端口对象组不同。可以为除 TCP 和 UDP 以外的其他协议创建端口对象，还可以在系统 Web 界面中的不同位置使用端口对象，包括端口变量、访问控制策略、网络发现规则和事件搜索。

可以在入侵规则 **Source Port** 和 **Destination Port** 报头字段中使用端口变量来限制仅检查来自或发往特定 TCP 或 UDP 端口的数据包。

在这些字段中使用变量时，链接到与访问控制规则或策略相关的入侵策略的变量集决定部署访问控制策略的网络流量中这些变量的值。

可以将以下端口配置的任意组合添加到变量：

- 端口变量与您从可用端口列表中选择的端口对象的任何组合

  请注意，可用端口的列表不会显示端口对象组，因此您不能将这些端口对象组添加到变量。

- 从“新变量”(New Variable) 或“编辑变量”(Edit Variable) 页面添加的单个端口对象（这些对象随后可添加到变量以及其他现有和将来的变量）

  只有 TCP 和 UDP 端口（包括任一类型的值 `any`）是有效的变量值。如果您使用新的或编辑变量页面以添加不是有效变量值的有效端口对象，则该对象将被添加到系统，但不会显示在可用对象列表中。当您使用对象管理器来编辑变量中使用的端口对象时，只能将其值更改为有效的变量值。

- 单个文字端口值和端口范围

  您必须使用破折号 (-) 分隔端口范围。使用冒号 (:) 指示的端口范围支持向后兼容性，但您不能在您创建的端口变量中使用冒号。

  您可以通过在任何组合中单独添加每个文字端口值和范围，来列出多个文字端口值和范围。

在添加或编辑端口变量时，请注意以下要点：

- 在您添加的任何变量中，包括的端口的默认值为文字 `any`，它表示任何端口或端口范围。排除端口的默认值为 `none`，它表示无端口。

提示 要创建值为 `any` 的变量，请命名并保存该变量，而不要添加具体的值。

- 您不能在逻辑上排除值 `any`，如果排除，这将表示无端口。例如，您不能在将值为 `any` 的变量添加到已排除端口的列表时保存变量集。
- 将端口添加到已排除列表将使指定端口和端口范围无效。即您可以将任何端口与已排除的端口或端口范围进行匹配。
- 已排除的值必须解析到已包括的值的子集。例如，您不能包括端口范围 10-50 并排除端口 60。

高级变量

高级变量让您能够配置通常无法通过网络界面配置的功能。Firepower 系统当前只提供一个高级变量，即 USER_CONF 变量。

USER_CONF

USER_CONF 提供一个通用工具，让您能够配置无法以其他方式通过 Web 界面获得的一个或多个功能。

注意 请**勿**使用高级变量 USER_CONF 来配置入侵策略功能，除非功能描述或支持人员指示您这样做。存在冲突或重复的配置会导致系统停止。

编辑 USER_CONF 时，单行最多总共可输入 4096 个字符；达到该限制后，行会自动换行。可以包含任意数量的有效说明或行，直至达到变量的最大字符长度限制（8192 个字符）或物理限制（例如磁盘空间）。在命令指令中，可以在任何完整参数之后使用反斜线 (\) 续行符。

重置 USER_CONF 会将其清空。

变量重置

在变量集新建或编辑变量页面上，可以将变量重置为默认值。下表总结了重置变量的基本原则。

表 *81:* 变量重置值

要重置的变量类型	所属变量集类型	重置后的值
默认值	默认值	规则更新值
用户定义	默认值	`any`
默认变量或用户定义的变量	自定义	当前默认变量集值（已修改或未修改）

重置自定义变量集中的变量会将其重置为该变量在默认变量集中的当前值。

相反，重置或修改默认变量集中某个变量的值总是会更新所有自定义变量集中该变量的默认值。如果重置图标呈灰色显示，表示不能重置变量，这意味着该变量在该变量集中没有自定义值。除非自定义了自定义变量集中某个变量的值，否则对默认变量集中该变量的更改会更新与该变量集链接的任何入侵策略中使用的值。

注释 理想做法是修改默认变量集中的某个变量，以评估这些更改如何影响使用链接自定义变量集中的该变量的任何入侵策略，尤其是在尚未定制自定义变量集中的变量值时。

将指针悬停在变量集中的**重置图标** 上可查看重置值。当自定义值和重置值相同时，这表示以下其中一种情况属实：

- 您在自定义或默认变量集中，而且在其中添加了值为 `any` 的变量
- 您在自定义变量集中，在其中添加了具有显式值的变量，并且选择了使用配置值作为默认值

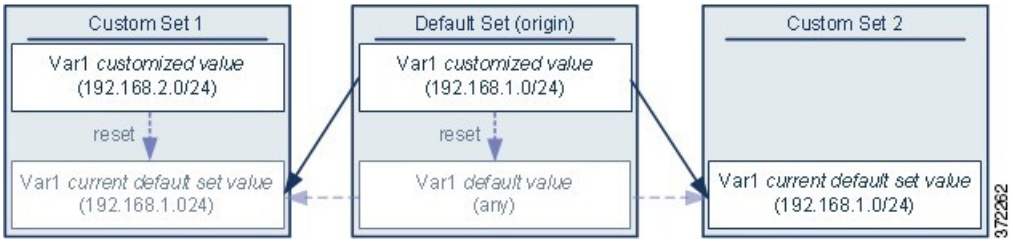
将变量添加到变量集

将变量添加到变量集会将其添加到所有其他变量集。添加自定义变量集中的变量时，必须选择是否使用配置值作为默认变量集中的定制值：

- **如果使用配置值**（例如 192.168.0.0/16），则该变量会被添加到使用配置值作为定制值、默认值为 any 的默认变量集中。由于默认变量集的当前值决定其他变量集的默认值，所以其他自定义变量集的初始默认值为配置值（在本例中为 192.168.0.0/16）。
- **如果不使用配置值**，则该变量将被添加到仅使用默认值 any 的默认变量集中，因此其他自定义变量集的初始默认值将为 any。

示例：将用户定义变量添加到默认变量集

下图说明了将用户定义的变量 Var1（其值为 192.168.1.0/24）添加到默认变量集时发生的变量集交互。



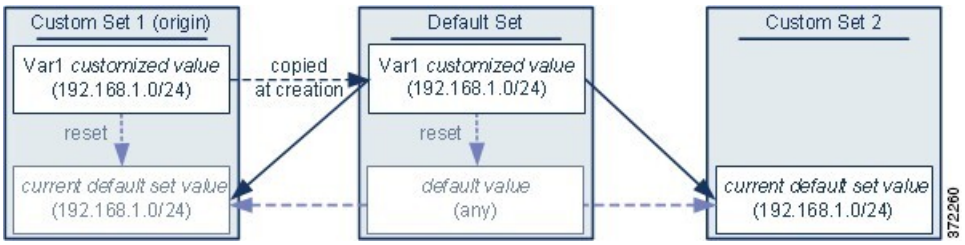
您可以在任何变量集中自定义 Var1 的值。在未自定义 Var1 的自定义变量集 2 中，此变量的值是 192.168.1.0/24。在自定义变量集 1 中，Var1 的自定义值 192.168.2.0/24 覆盖了默认值。重置默认变量集中某个用户定义的变量会将所有变量集中该变量的默认值重置为 any。

须注意的一点是，在本示例中，如果不更新自定义变量集 2 中的 Var1，进一步自定义或重置默认变量集中的 Var1 会导致更新自定义变量集 2 中 Var1 的默认值，从而影响与变量集相关联的所有入侵策略。

请注意，虽然在本示例中未显示，但用户定义的变量和默认变量的变量集交互是相同的，唯一不同的是重置默认变量集中的默认变量会在当前规则更新中将其值重置为由思科配置的值。

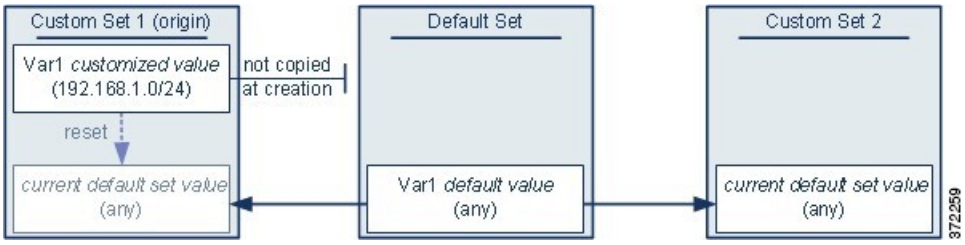
示例：将用户定义变量添加到自定义变量集

以下两个示例说明了将用户定义的变量添加到自定义变量集时变量集之间的交互。保存新变量时，系统会提示您选择是否将配置值用作其他变量集的默认值。在以下示例中，您选择**使用**配置值。



请注意，除了 Var1 来自自定义变量集 1 以外，本示例与以上将 Var1 添加到默认变量集的示例完全相同。将 Var1 的自定义值 192.168.1.0/24 添加到自定义变量集 1 会将该值复制到默认变量集，以作为默认值为 any 的自定义值。之后，Var1 值和交互就像之前将 Var1 添加到默认变量集一样。请记住，与前一个示例一样，进一步自定义或重置默认变量集中的 Var1 会导致更新自定义变量集 2 中 Var1 的默认值，从而影响与变量集相关联的所有入侵策略。

在下一个示例中，像前一个示例一样，将 Var1（其值为 192.168.1.0/24）添加到自定义变量集 1，但选择**不使用** Var1 的配置值作为其他变量集中的默认值。



此方法会将 Var1（其默认值为 any）添加到所有变量集。添加 Var1 后，可以在任何变量集中自定义它的值。此方法的优点是，通过最初不在默认变量集中自定义 Var1，可以降低这样的风险：在默认变量集中自定义此变量的值时，无意中更改了尚未自定义 Var1 的变量集（例如，自定义变量集 2）中的当前值。

嵌套变量

只要嵌套不是循环的，就可以嵌套变量。不支持嵌套的、否定的变量。

有效的嵌套变量

在此示例中，SMTP_SERVERS、HTTP_SERVERS 和 OTHER_SERVERS 是有效的嵌套变量。

变量	类型	包含的网络	排除的网络
SMTP_SERVERS	自定义默认值	10.1.1.1	-
HTTP_SERVERS	自定义默认值	10.1.1.2	-
OTHER_SERVERS	用户定义的变量	10.2.2.0/24	-
HOME_NET	自定义默认值	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

无效的嵌套变量

在本例中，HOME_NET 是一个无效的嵌套变量，因为 HOME_NET 的嵌套是循环的；即，OTHER_SERVERS 的定义包括 HOME_NET，因此您将在其自身中嵌套 HOME_NET。

变量	类型	包含的网络	排除的网络
SMTP_SERVERS	自定义默认值	10.1.1.1	-
HTTP_SERVERS	自定义默认值	10.1.1.2	-

变量	类型	包含的网络	排除的网络
OTHER_SERVERS	用户定义的变量	10.2.2.0/24 HOME_NET	-
HOME_NET	自定义默认值	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

不受支持的嵌套的、否定的变量

由于嵌套的、否定的变量不受支持，因此不能使用本例所示的变量NONCORE_NET来表示受保护网络之外的IP地址。

变量	类型	包含的网络	排除的网络
HOME_NET	自定义默认值	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	-
EXTERNAL_NET	自定义默认值	-	HOME_NET
DMZ_NET	用户定义的变量	10.4.0.0/16	-
NOT_DMZ_NET	用户定义的变量	-	DMZ_NET
NONCORE_NET	用户定义的变量	EXTERNAL_NET NOT_DMZ_NET	-

不受支持的嵌套的、否定的变量的替代方法

作为上述示例的替代方法，您可以通过创建变量NONCORE_NET来表示受保护网络之外的IP地址，如本例所示。

变量	类型	包含的网络	排除的网络
HOME_NET	自定义默认值	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	-
DMZ_NET	用户定义的变量	10.4.0.0/16	-
NONCORE_NET	用户定义的变量	-	HOME_NET DMZ_NET

管理变量集

要使用变量集，您必须拥有 威胁 许可证（适用于 威胁防御 设备）或保护许可证（所有其他设备类型）。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**变量集 (Variable Set)**。

步骤 3 管理变量集：

- 添加 - 如果要添加自定义变量集，请点击**添加变量集 (Add Variable Set)**；请参阅创建变量集，第 1053 页。
- 删除 - 如果要删除自定义变量集，请点击变量集旁边的 **删除**（）），然后点击**是 (Yes)**。不能删除默认变量集或属于祖先域的变量集。

  注释 在删除的变量集中创建的变量不会被删除或以其他方式在其他集合中受影响。

- 编辑 - 如果要编辑变量集，请点击要修改的变量集旁边的 **编辑**（）；请参阅编辑对象，第 963 页。
- 过滤 - 如果要按名称过滤变量集，请开始输入名称；当您键入时，页面会刷新以显示匹配的名称。如果要清除名称过滤，请点击过滤器字段中的 **清除**（）。
- 管理变量 - 要管理变量集中包含的变量，请参阅管理变量，第 1054 页。

创建变量集

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**变量集 (Variable Set)**。

步骤 3 点击**添加变量集 (Add Variable Set)**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 输入**说明 (Description)**（可选）。

步骤 6 管理变量集中的变量；请参阅管理变量，第 1054 页。

步骤 7 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

管理变量

您必须拥有 威胁 许可证（适用于 威胁防御 设备）或保护许可证（所有其他设备类型）。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**变量集 (Variable Set)**。

步骤 3 点击要编辑的变量集旁边的 **编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 管理变量：

- 显示 - 如果要显示变量的完整值，请将指针悬停在变量旁边的**值 (Value)** 列中的值上方。
- 添加 - 如果要添加变量，请点击**添加 (Add)**；请参阅添加变量，第 1055 页。
- 删除 - 点击变量旁边的 **删除**（）。如果自添加变量后已保存变量集，请点击**是 (Yes)** 以确认是否要删除变量。

  不能删除以下变量：

  - 默认变量
  - 入侵规则或其他变量所使用的用户定义的变量
  - 属于祖先域的变量

- 编辑 - 点击要编辑的变量旁边的 **编辑**（）；请参阅编辑变量，第 1056 页。
- 重置 - 如果要将已修改变量重置为其默认值，请点击已修改变量旁边的 **重置** 。如果重置呈灰色显示，则表明以下情况之一成立：

  - 当前值已是默认值。
  - 配置属于祖先域。

  提示 将指针悬停在活动的重置图标上可显示默认值。

步骤 5 点击**保存 (Save)** 以保存变量集。如果变量集正在供访问控制策略使用，请点击**是 (Yes)** 以确认要保存更改。

由于默认变量集中的当前值决定所有其他变量集中的默认值，因此，修改或重置默认变量集中的变量会更改未对该变量默认值进行自定义的那些变量集中的该变量当前值。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

添加变量

您必须拥有 威胁 许可证（适用于 威胁防御 设备）或保护许可证（所有其他设备类型）。

过程

步骤 1 在变量集编辑器中，点击**添加 (Add)**。

步骤 2 在 **Name** 字段中为变量输入一个唯一名称。

步骤 3 从**类型 (Type)** 下拉列表中，选择**网络 (Network)** 或**端口 (Port)**。

步骤 4 为变量指定值：

- 如果要将项目从可用网络或端口列表移动到包含或排除项目列表，可以选择一个或多个项目，然后进行拖放，或者点击**包含 (Include)** 或**排除 (Exclude)**。

  提示 如果网络或端口变量的包含变量列表和排除变量列表中的地址或端口重叠，排除的地址或端口优先。

- 输入一个文字值，然后点击**添加 (Add)**。对于网络变量，可以输入单个 IP 地址或地址块。对于端口变量，可以添加单个端口或端口范围，用连字符(-)隔开上限和下限值。如有需要，可重复此步骤输入多个文字值。
- 如果要从包含或排除列表中删除项目，请点击该项目旁边的 **删除**（ ）。

注释 要包含或排除的项目列表可以包括原义字符串和现有变量、对象及网络对象组（对于网络变量）的任意组合。

步骤 5 点击 **Save** 保存变量。如果是添加自定义变量集中的新变量，可以选择以下选项：

- 点击**是 (Yes)** 添加使用配置值作为默认变量集中的自定义值（进而也是其他自定义变量集中的默认值）的变量。
- 点击**否 (No)** 将变量添加为默认变量集中的默认值 `any`（进而在其他自定义变量集中也使用此默认值）。

步骤 6 点击**保存 (Save)** 以保存变量集。更改保存成功，与该变量集链接的所有访问控制策略均显示为过期状态。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

编辑变量

您必须拥有 威胁 许可证（适用于 威胁防御 设备）或保护许可证（所有其他设备类型）。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

可以同时编辑自定义变量和默认变量。

无法更改现有变量中的**名称 (Name)** 或**类型 (Type)** 值。

过程

步骤 1 在变量集编辑器中，点击要修改的变量旁边的 **编辑**（ ）。

如果显示**视图**（ ），则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 2 修改变量：

- 如果要将项目从可用网络或端口列表移动到包含或排除项目列表，可以选择一个或多个项目，然后进行拖放，或者点击**包含 (Include)** 或**排除 (Exclude)**。

  提示 如果网络或端口变量的包含变量列表和排除变量列表中的地址或端口重叠，排除的地址或端口优先。

- 输入一个文字值，然后点击**添加 (Add)**。对于网络变量，可以输入单个 IP 地址或地址块。对于端口变量，可以添加单个端口或端口范围，用连字符(-)隔开上限和下限值。如有需要，可重复此步骤输入多个文字值。
- 如果要从包含或排除列表中删除项目，请点击该项目旁边的 **删除**（ ）。

注释 要包含或排除的项目列表可以包括原义字符串和现有变量、对象及网络对象组（对于网络变量）的任意组合。

步骤 3 点击 **Save** 保存变量。

步骤 4 点击**保存 (Save)** 以保存变量集。如果变量集正在供访问控制策略使用，请点击**是 (Yes)** 以确认要保存更改。更改保存成功，与该变量集链接的所有访问控制策略均显示为过期状态。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

VLAN 标签

配置的每个 VLAN 标记对象代表一个 VLAN 标记或标记范围。

可以将VLAN标记对象进行分组。组表示多个对象；就此意思而言，在单个对象中使用一系列VLAN标记不被视为组。

可以在系统 Web 界面中的各种位置使用 VLAN 标记对象和组，包括规则和事件搜索。例如，可以编写仅适用于特定 VLAN 的访问控制规则。

创建 VLAN 标记对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中，选择 **VLAN 标记 (VLAN Tag)**。

步骤 3 从**添加 VLAN 标记 (Add VLAN Tag)** 下拉列表中，选择**添加对象 (Add Object)**。

步骤 4 输入 **Name**。

步骤 5 输入 **Description**。

步骤 6 在 **VLAN 标记 (VLAN Tag)** 字段中输入值。使用连字符可指定 VLAN 标记范围。

步骤 7 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖 ， 第 969 页。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖 ， 第 969 页。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

VPN

您可以在 威胁防御 设备上使用以下 VPN 对象。要使用这些对象，您必须具有管理员权限，并且您的智能许可证帐户必须满足导出控制要求。您只能在分叶域中配置这些对象。

威胁防御 IKE 策略

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用提议。IKE 提议是一组两个对等体用于保护其之间的协商的算法。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数用于保护后续 IKE 协商。

对于 IKEv1，IKE 方案包含单个算法集和模数组。您可以创建确保多个优先化的策略来确保至少一个策略与远程对等体的策略匹配。与 IKEv1 不同，在 IKEv2 方案中，您可以在一个策略中选择多个算法和模数组。由于对等体在第 1 阶段协商期间进行选择，因此可创建单个 IKE 方案，但是考虑多个不同的方案，以向最需要的方案提供更高的优先级。对于 IKEv2，策略对象不指定身份验证，其他策略必须定义身份验证要求。

当配置站点间 IPsec VPN 时，需要 IKE 策略。有关详细信息，请参阅VPN，第 1087 页。

配置 IKEv1 策略对象

使用“IKEv1 策略”(IKEv1 Policy) 页面创建、编辑或删除 IKEv1 策略对象。这些策略对象包含 IKEv1 策略所需的参数。

过程

步骤 1 依次选择**对象 (Objects)** > **对象管理 (Object Management)** 并从目录中选择 **VPN** > **IKEv1 策略 (IKEv1 Policy)**。

系统将列出之前配置的策略，包括系统定义的默认值。根据您的访问级别，您可以 **编辑**（）、查看 **视图**（）或 **删除**（）方案。

步骤 2 （可选）选择**添加**（）**添加 IKEv1 策略 (Add IKEv1 Policy)** 以创建新策略对象。

步骤 3 为此策略输入**名称 (Name)**。最多允许 128 个字符。

步骤 4 （可选）为此方案输入**说明 (Description)**。最多允许 1,024 个字符。

步骤 5 在**优先级 (Priority)** 中输入 IKE 策略的优先级值。

当尝试查找常见安全关联 (SA) 时，优先级值可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的第一个策略中选定的参数，它会尝试使用下一个优先级中定义的参数。有效值范围为 1 到 65,535。数值越低，优先级越高。如果将此字段留空，管理中心将分配最低的未分配值，从 1 开始然后为 5，并以 5 为增量继续。

步骤 6 在**加密**中选择加密方法。

在决定为 IKEv1 策略使用哪种加密和散列算法时，您的选择限于对等设备支持的算法。对于 VPN 拓扑中的外部设备，必须选择与两个对等体匹配的算法。对于 IKEv1，选择相关选项之一。 有关选项的完整说明，请参阅决定使用哪个加密算法，第 1094 页。

步骤 7 选择创建消息摘要的**散列 (Hash)** 算法，用于确保消息的完整性。

在决定为IKEv1方案使用哪种加密和散列算法时，您的选择限于受管设备支持的算法。对于VPN拓扑中的外部设备，必须选择与两个对等体匹配的算法。 有关选项的完整说明，请参阅决定使用哪些散列算法，第 1094 页。

步骤 8 设置 **Diffie-Hellman 组**。

用于加密的Diffie-Hellman组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。选择要在 VPN 中允许的组。有关选项的完整说明，请参阅 决定要使用的 Diffie-Hellman 模数组，第 1095 页。

步骤 9 设置安全关联 (SA) 的**持续期限 (Lifetime)**（以秒为单位）。可指定 120 到 2,147,483,647 秒之间的值。默认值为 86400。

当超过持续期限时，SA 到期且必须在两个对等体之间重新协商。通常，持续期限越短（某种程度上），IKE协商越安全。但是，持续期限越长，将来设置IPsec安全关联的速度相比较短持续期限的更快。

步骤 10 设置在两个对等体之间使用的**身份验证方法 (Authentication Method)**。

- **预共享密钥 (Preshared Key)** - 在身份验证阶段，预共享密钥允许密钥在两个对等体之间共享并由 IKE 使用。如果未使用同一预共享密钥配置其中一个参与的对等体，则无法建立 IKE SA。
- **证书 (Certificate)** - 当您将“证书”(Certificate) 用作 VPN 连接的身份验证方法时，对等体从 PKI 基础设施中的 CA 服务器获取数字证书，并用其相互进行身份验证。

注释 在支持IKEv1的VPN拓扑中，所选IKEv1策略对象中指定的**身份验证方法**会成为IKEv1**身份验证类型**设置的默认设置。这些值必须匹配，否则，您的配置将出错。

步骤 11 点击**保存**
IKEv1 策略添加到列表中。

配置 IKEv2 策略对象

使用“IKEv2 策略”(IKEv2 Policy) 对话框来创建、删除和编辑 IKEv2 策略对象。这些策略对象包含 IKEv2 策略所需的参数。

过程

步骤 1 依次选择**对象 (Objects)** > **对象管理 (Object Management)**，然后从目录中选择 **VPN** > **IKEv2 策略 (IKEv2 Policy)**。

系统将列出之前配置的策略，包括系统定义的默认值。根据您的访问级别，您可以**编辑**（）、**视图**（）或**删除**（）策略。

步骤 2 选择**添加**（）**添加 IKEv2 策略 (Add IKEv2 Policy)** 以创建新策略。

步骤 3 为此策略输入**名称 (Name)**。

策略对象的名称。最多允许 128 个字符。

步骤 4 为此策略输入**说明 (Description)**。

策略对象的说明。最多允许 1024 个字符。

步骤 5 输入**优先级 (Priority)**。

IKE 方案的优先级值。当尝试查找常见安全关联 (SA) 时，优先级值可确定两个协商对等体比较的 IKE 方案顺序。如果远程 IPsec 对等体不支持在您的第一个策略中选定的参数，它会尝试使用下一个最低优先级策略中定义的参数。有效值范围为 1 到 65535。数值越低，优先级越高。如果将此字段留空，管理中心将分配最低的未分配值，从 1 开始然后为 5，并以 5 为增量继续。

步骤 6 设置安全关联 (SA) 的**持续期限 (Lifetime)**（以秒为单位）。可指定 120 到 2,147,483,647 秒之间的值。默认值为 86400。

当超过持续期限时，SA 到期且必须在两个对等体之间重新协商。通常，持续期限越短（某种程度上），IKE 协商越安全。但是，持续期限越长，将来设置 IPsec 安全关联的速度相比较短持续期限的更快。

步骤 7 选择 IKE 策略中使用的散列算法的**完整性算法 (Integrity Algorithms)** 部分。散列算法创建消息摘要，它用于确保消息的完整性。

在决定为 IKEv2 方案使用哪种加密和散列算法时，您的选择限于受管设备支持的算法。对于 VPN 拓扑中的外部设备，必须选择与两个对等体匹配的算法。选择要在 VPN 中允许的所有算法。有关选项的完整说明，请参阅决定使用哪些散列算法，第 1094 页。

步骤 8 选择用于建立第 1 阶段 SA（用于保护第 2 阶段协商）的**加密算法 (Encryption Algorithm)**。

在决定为 IKEv2 方案使用哪种加密和散列算法时，您的选择限于受管设备支持的算法。对于 VPN 拓扑中的外部设备，必须选择与两个对等体匹配的算法。选择要在 VPN 中允许的所有算法。 有关选项的完整说明，请参阅决定使用哪个加密算法，第 1094 页。

步骤 9 选择**PRF 算法 (PRF Algorithm)**。

IKE 策略中使用的散列算法的伪随机函数 (PRF) 部分。在 IKEv1 中，完整性和 PRF 算法不分开，但在 IKEv2 中，可以为这些元素指定不同的算法。选择要在 VPN 中允许的所有算法。 有关选项的完整说明，请参阅决定使用哪些散列算法，第 1094 页。

步骤 10 选择并**添加 DH 组 (DH Group)**。

用于加密的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。选择您想要在 VPN 中允许的组。 有关选项的完整说明，请参阅 决定要使用的 Diffie-Hellman 模数组，第 1095 页。

步骤 11 点击**保存**

如果已选择有效的选项组合，则新的 IKEv2 策略会添加到列表中。如果未选择，在会显示错误消息，且必须相应地做出更改，以便成功保存此策略。

威胁防御 IPSec 提议

在配置 VPN 拓扑时，使用 IPsec 方案（或转换集）。在与 ISAKMP 进行 IPsec 安全关联协商期间，对等体同意使用特定方案来保护特定数据流。两个对等体的方案必须相同。

根据 IKE 版本（IKEv1 或 IKEv2），存在不同的 IPsec 方案对象：

- 当创建 IKEv1 IPsec 方案（转换集）对象时，可以选择 IPsec 运行的模式，并定义所需的加密和身份验证类型。您可以为算法选择单一选项。如果要在VPN中支持多个组合，请创建多个IKEv1 IPsec 方案对象。
- 当创建 IKEv2 IPsec 方案对象时，可以选择 VPN 中允许的所有加密和散列算法。在 IKEv2 协商期间，对等体选择其分别支持的最合适选项。

IKEv1 和 IKEv2 IPsec 方案都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

注释 我们建议对 IPsec 隧道使用加密和身份验证。

配置 IKEv1 IPsec 方案对象

过程

步骤 1 依次选择**对象 (Objects)** > **对象管理 (Object Management)**，然后从目录中选择 **VPN** > **IPsec IKev1 方案 (IPsec IKev1 Proposal)**。

系统将列出以前配置的方案，包括系统定义的默认值。根据您的访问级别，您可以 **编辑**（）、查看 **视图**（）或 **删除**（）方案。

步骤 2 选择**添加**（）**添加 IPsec IKEv1 方案 (Add IPsec IKEv1 Proposals)** 以创建新的方案。

步骤 3 为此方案输入**名称 (Name)**

策略对象的名称。最多允许 128 个字符。

步骤 4 为此方案输入**说明 (Description)**。

策略对象的说明。最多允许 1024 个字符。

步骤 5 选择 **ESP 加密**方法。此方案的封装安全协议 (ESP) 加密算法。

对于IKEv1，选择相关选项之一。在决定用于IPsec方案的加密和散列算法时，您的选择仅限于VPN中的设备所支持的算法。 有关选项的完整说明，请参阅决定使用哪个加密算法，第 1094 页。

步骤 6 为 **ESP 散列 (ESP Hash)** 选择一个选项。

有关选项的完整说明，请参阅决定使用哪些散列算法，第 1094 页。

步骤 7 点击**保存**
将新方案添加到列表中。

配置 IKEv2 IPsec 方案对象

过程

步骤 1 依次选择**对象 (Objects)** > **对象管理 (Object Management)**，然后从目录中选择 **VPN** > **IKEv2 IPsec 方案 (IKEv2 IPsec Proposal)**。

系统将列出以前配置的方案，包括系统定义的默认值。根据您的访问级别，可以编辑 **编辑**（）、查看 **视图**（）或删除 **删除**（）方案。

步骤 2 选择**添加**（）**添加 IKEv2 IPsec 方案 (Add IKEv2 IPsec Proposal)** 以创建新的方案。

步骤 3 为此方案输入**名称 (Name)**

策略对象的名称。最多允许 128 个字符。

步骤 4 为此方案输入**说明 (Description)**。

策略对象的说明。最多允许 1024 个字符。

步骤 5 选择要在方案中用于身份验证的 **ESP 散列 (ESP Hash)** 方法、散列或完整性算法。

注释 威胁防御 不支持使用 NULL 加密的 IPSec 隧道。确保不为 IPSec IKEv2 提议选择 NULL 加密。

对于 IKEv2，选择要用于支持 **ESP 散列 (ESP Hash)** 的所有选项。 有关选项的完整说明，请参阅决定使用哪些散列算法，第 1094 页。

步骤 6 选择 **ESP 加密**方法。此方案的封装安全协议 (ESP) 加密算法。

对于 IKEv2，点击“选择”(Select) 以打开一个对话框，在对话框中可以选择要支持的所有选项。在决定用于 IPsec 方案的加密和散列算法时，您的选择仅限于 VPN 中的设备所支持的算法。 有关选项的完整说明，请参阅决定使用哪个加密算法，第 1094 页。

步骤 7 点击**保存**
将新方案添加到列表中。

威胁防御组策略对象

组策略是存储在组策略对象中的一组属性和值对，用于定义远程接入VPN体验。例如，在组策略对象中，可以配置地址、协议和连接设置等常规属性。

在建立VPN隧道时，将确定应用于用户的组策略。RADIUS授权服务器将会分配组策略，或从当前连接配置文件中获取。

注释 威胁防御 上没有任何组策略继承属性。对于用户使用完整的组策略对象。使用登录时 AAA 服务器识别的组策略对象；如果未指定组策略对象，则使用为VPN连接配置的默认组策略。提供的默认组策略可以设置为默认值，但仅在将该策略分配给连接配置文件且用户未识别其他组策略时使用该策略。

要使用组对象，您必须有与您的智能许可证帐户关联的这些 AnyConnect 客户端 许可证之一，并启用了导出控制功能：

- 仅限 AnyConnect VPN
- AnyConnect Plus
- AnyConnect Apex

相关主题

配置组策略对象，第 1063 页

配置组策略对象

请参阅威胁防御组策略对象，第 1062 页。

过程

步骤 1 选择**对象** > **对象管理** > **VPN** > **组策略**。

系统将列出之前配置的策略，包括系统默认值。根据您的访问级别，可以编辑、查看或删除组策略。

步骤 2 点击**添加组策略**或选择要编辑的当前策略。

步骤 3 输入该策略的**名称**，还可以选择输入**说明**。

此名称最多可包含 64 个字符，允许使用空格。说明最多可以有 1,024 个字符。

步骤 4 如组策略常规选项，第 1064 页中所述，为此组策略指定**常规**参数。

步骤 5 如组策略 AnyConnect 客户端 选项，第 1066 页中所述，为此组策略指定 **AnyConnect** 参数。

步骤 6 如组策略高级选项，第 1069 页中所述，为此组策略指定**高级**参数。

步骤 7 点击**保存 (Save)**。

新的策略组将添加到列表中。

下一步做什么

将组策略对象添加到远程接入 VPN 连接配置文件。

组策略常规选项

导航路径

对象 > **对象管理** > **VPN** > **组策略**，点击 点击**添加组策略**或选择要编辑的当前策略。，然后选择**常规**选项卡。

VPN 协议字段

指定应用此组策略时可使用的远程接入 VPN 隧道的类型。**SSL** 或 **IPsec IKEv2**。

IP 地址池

指定根据特定于远程接入 VPN 中用户组的地址池应用的 IPv4 地址分配。对于远程接入 VPN，可以为识别的使用 RADIUS/ISE 进行授权的用户组分配特定地址池中的 IP 地址。通过为特定用户组配置特定的组策略作为“RADIUS 授权”属性 (GroupPolicy/Class)，可以为系统中不知道身份的用户或用户组无缝执行策略实施。例如，您必须为使用这些地址的承包商和策略实施选择一个特定的地址池，以允许他们限制性地访问内部网络。

威胁防御 设备向客户端分配 IPv4 地址池的优先顺序：

1. IPv4 地址池的 RADIUS 属性
2. 组策略的 RADIUS 属性
3. 映射到连接配置文件的组策略中的地址池
4. 连接配置文件中的 IPv4 地址池

关于组策略中使用 IP 地址池的一些限制：

- 不支持 IPv6 地址池。
- 一个组策略中最多可配置六个 IPv4 地址池。
- 修改使用中的地址池时会出现部署失败。在对地址池进行任何更改前，必须注销所有用户。
- 重命名地址池或配置的地址池重叠时，部署可能会失败。您必须删除旧地址池，稍后再部署更改的地址池，以此来部署更改。

  部分故障排除命令：

  - `show ip local pool <address-pool-name>`
  - `show vpn-sessiondb detail anyconnect`
  - `vpn-sessiondb loggoff all noconfirm`

横幅字段

指定登录时要向用户显示的横幅文本。长度最多可以为491个字符。没有默认值。IPsec VPN客户端对于条幅支持完全HTML，但AnyConnect客户端仅支持部分HTML。要确保向远程用户正确显示横幅，请对IPsec客户端使用/n标记，对SSL客户端使用
标记。

DNS/WINS字段

域命名系统(DNS)和Windows Internet命名系统(WINS)服务器。用于AnyConnect客户端名称解析。

- **主DNS服务器**和**辅助DNS服务器** - 选择或创建一个网络对象，定义希望此组使用的DNS服务器的IPv4或IPv6地址。
- **主WINS服务器**和**辅助WINS服务器** - 选择或创建一个网络对象，其中包含希望此组使用的WINS服务器的IP地址。
- **DHCP网络范围**-选择或创建一个网络对象，其中包含一个可路由的IPv4地址，与所需池子在同一子网，但不在池子内。DHCP服务器确定此IP地址所属的子网并从该地址池分配IP地址。如果未正确设置，VPN策略部署将失败。

  如果在连接配置文件中为地址池配置了DHCP服务器，DHCP作用域会标识要用于此组的地址池的子网。DHCP服务器的地址还必须来自此作用域标识的同一个子网。作用域允许您选择DHCP服务器中定义的部分地址池，用于此特定组。

  如未定义网络范围，则DHCP服务器将按地址池配置顺序分配IP地址。它将检查各个池，直到发现未分配的地址为止。

  建议尽可能将接口的IP地址用于路由目的。例如，如果池为10.100.10.2-10.100.10.254，接口地址为10.100.10.1/24，则使用10.100.10.1作为DHCP范围。请不要使用网络编号。DHCP仅可用于IPv4寻址。如果您选择的地址不是接口地址，可能需要为范围地址创建静态路由。

  目前不支持LINK-SELECTION（RFC 3527）和SUBNET-SELECTION（RFC 3011）。
- **默认域** - 默认域的名称。指定顶级域，例如example.com。

拆分隧道字段

拆分隧道引导一些网络流量通过VPN隧道（加密），将剩下的网络流量引导至VPN隧道外部（未加密或“以明文形式”）。

- **IPv4拆分隧道/IPv6拆分隧道** - 默认情况下，不启用拆分隧道。对于IPv4和IPv6，此字段均设置为**允许所有流量通过隧道**。如果保留此设置，来自终端的所有流量都将通过VPN连接。

  要配置拆分隧道，请选择**下面指定的隧道网络**或**排除下面指定的网络**策略。然后为该策略配置访问控制列表。
- **拆分隧道网络列表类型** - 选择所使用的访问列表类型。然后选择或创建**标准访问列表**或**扩展访问列表**。有关详细信息，请参阅访问列表，第975页。
- **DNS请求拆分隧道** - 也称为拆分DNS。配置环境中预期的DNS行为。

默认情况下，不启用拆分 DNS，并将其设置为**按拆分隧道策略发送 DNS 请求**。选择**始终通过隧道发送 DNS 请求**强制将所有 DNS 请求通过隧道发送到专用网络。

要配置拆分 DNS，请选择**仅通过隧道发送指定的域**，然后在**域列表**字段中输入域名列表。这些请求通过拆分隧道解析到专用网络。所有其他名称使用公用DNS服务器进行解析。在域列表中最多输入十个条目，条目之间用逗号分隔。整个字符串的长度不能超过 255 个字符。

相关主题

配置组策略对象，第 1063 页

组策略 AnyConnect 客户端 选项

这些规范适用于 AnyConnect 客户端 VPN 客户端的操作。

导航

对象>**对象管理**>**VPN**>**组策略**。点击**添加组策略**或选择要编辑的当前策略。然后选择 **AnyConnect** 选项卡。

配置文件字段

配置文件-选择或创建包含 AnyConnect 客户端配置文件 的文件对象。有关对象创建详细信息，请参见 文件对象，第 1070 页。

AnyConnect 客户端配置文件 是存储在 XML 文件中的一组配置参数。AnyConnect 客户端 软件使用它来配置出现在客户端用户界面中的连接条目。这些参数（XML 标记）还配置相应设置以启用更多 AnyConnect 客户端 功能。

使用基于 GUI 的 AnyConnect 配置文件编辑器（一个独立的配置工具）来创建 AnyConnect 客户端配置文件。有关详细信息，请参阅相应版本的《Cisco Secure 客户端（包括 AnyConnect）管理员指南》的 *AnyConnect* 配置文件编辑器 一章。

管理配置文件字段

管理 VPN 隧道可提供在终端开启时连接到企业网络，即使最终用户未通过 VPN 连接也是如此。

管理 VPN 配置文件-管理配置文件包含用于在终端上启用和建立管理 VPN 隧道的设置。

独立管理VPN隧道配置文件编辑器可用于创建新的配置文件或修改现有的配置文件。您可以从思科软件下载中心下载配置文件编辑器。

有关添加配置文件的详细信息，请参阅 文件对象，第 1070 页。

客户端模块字段

Cisco 仅限 AnyConnect VPN 通过各种内置模块提供增强的安全性。这些模块提供网络安全，终端流量的网络可视性和网络外漫游保护等服务。每个客户端模块都包含一个客户端配置文件，其中包含根据您的要求的一组自定义配置。

以下 AnyConnect 客户端 模块是可选的，您可以将这些模块配置为在 VPN 用户下载 AnyConnect 时下载 AnyConnect 客户端：

- **AMP 启用程序** - 为终端部署高级恶意软件防护 (AMP) 。
- **DART**-捕获系统日志和其他诊断信息的快照，可将其发送到 Cisco TAC 进行故障排除。
- **ISE 终端安全评估** - 使用 OPSWAT v3 库执行终端安全评估检查，评估终端的合规性。
- **网络访问管理器** -为有线和无线网络访问提供 802.1X（第 2 层）和设备身份验证。
- **网络可视性** -可提升企业管理员执行容量和服务规划、审计、合规性和安全分析的能力。
- **登录前启动 (Start Before Login)** - 通过在 Windows 登录对话框出现之前启动 AnyConnectAnyConnect 客户端，强制用户在登录到 Windows 之前通过 VPN 连接而连接到企业基础设施。
- **Umbrella 漫游安全** -在没有处于活动状态的 VPN 时提供 DNS 层安全。
- **网络安全**-根据定义的安全策略分析网页的元素，允许可接受的内容，并阻止恶意或不可接受的内容。

点击 **添加** 并为每个客户端模块选择以下选项：

- **客户端模块 (Client Module)** - 从列表中选择 AnyConnect 客户端 模块。
- **要下载的配置文件 (Profile to download)** - 选择或创建包含 AnyConnect 客户端配置文件 的文件对象。有关对象创建详细信息，请参见 文件对象，第 1070 页。
- **启用模块下载**-选择启用终端以下载客户端模块以及配置文件。如果未选择，则终端只能下载客户端配置文件。

使用基于 GUI 的 AnyConnect 配置文件编辑器（一个独立的配置工具）来创建每个模块的客户端分析文件 。您可以从 Cisco 软件下载中心下载 AnyConnect 配置文件编辑器 。有关详细信息，请参见相应版本的《思科 AnyConnect 安全移动客户端管理员指南》 中的 *AnyConnect* 配置文件编辑器 一章。

SSL 设置字段

- **SSL 压缩** - 是否启用数据压缩，如果是，则设置要使用的数据压缩方法：Deflate 或 LZS。默认情况下会禁用 SSL 压缩。

  数据压缩加快了传输速率，但也增加了每个用户会话的内存需求和 CPU 使用率。因此，降低了安全设备的总体吞吐量。

- **DTLS 压缩** - 是否使用 LZS 为此组压缩数据报传输层安全 (DTLS) 连接。默认情况下会禁用 DTLS 压缩。
- **MTU 大小 (MTU Size)** - 思科 仅限 AnyConnect VPN 为 SSL VPN 连接建立的最大传输单位 (MTU) 大小。默认值为 1406 字节，有效范围为 576 到 1462 字节。
  - **忽略 DF 位** - 是否忽略需要分片的数据包中的“不分片 (df)”位。允许强制将已设置 DF 位的数据包分片，从而使其能够通过隧道传递。

连接设置字段

- **在 Anyconnect 客户端和 VPN 网关之间启用保持连接消息**。及其**间隔**设置 - 是否在对等体之间交换保持连接消息，以证明它们可用于在隧道中发送和接收数据。默认设置为启用。保持连接消息以设置的时间间隔传输。如果启用，请输入远程客户端在发送 IKE 保持连接数据包之间等待的时间间隔（以秒为单位）。默认间隔为 20 秒，有效范围为 15 到 600 秒。
- **启用失效对等体检测...** 。及其**间隔**设置 - 死对等检测 (DPD) 可确保 VPN 安全网关或 VPN 客户端快速检测到对等体不再响应以及连接失败的情况。默认情况下，会为网关和客户端启用该设置。DPD 消息以设置的时间间隔传输。如果启用，请输入远程客户端在发送 DPD 消息之间等待的时间间隔（以秒为单位）。默认间隔为 30 秒，有效范围为 5 到 3600 秒。
- **启用客户端绕行协议** - 使您可以配置安全网关管理 IPv4 流量（安全网关仅允许 IPv6 流量时）或管理 IPv4 流量（安全网关仅允许 IPv4 流量时）的方式。

  当 AnyConnect 客户端 建立与头端的 VPN 连接时，头端可以为客户端分配 IPv4 和/或 IPv6 地址。如果头端对 AnyConnect 客户端 连接仅分配一个 IPv4 地址或一个 IPv6 地址，则您可以配置 Client Bypass Protocol 以丢弃头端尚未分配 IP 地址（默认、已禁用、未检查）的网络流量，或允许该流量绕过头端并从客户端以未加密或“明文形式”发送（已启用、已检查）。

  例如，假设安全网关只将一个 IPv4 地址分配给 AnyConnect 客户端 连接，且终端为双协议栈。当终端尝试访问 IPv6 地址时，如果禁用客户端旁路协议，则会丢弃 IPv6 流量；但是，如果启用客户端旁路协议，则会从客户端以明文形式发送 IPv6 流量。
- **SSL 重新生成密钥** - 使客户端能够为连接重新生成密钥，重新协商加密密钥和初始化向量，从而提高连接的安全性。默认情况下，此设置处于禁用状态。启用后，可以在指定的时间间隔进行重新协商，对现有隧道重新生成密钥，或通过设置以下字段来创建新隧道：
  - **方法** - 启用 SSL 重新生成密钥时可用。创建**新隧道**（默认）或重新协商**现有隧道**的规范。
  - **间隔** - 启用 SSL 重新生成密钥时可用。设置为 4 分钟的默认值，其范围为 4-10080 分钟（1 周）。
- **客户端防火墙规则** - 使用客户端防火墙规则为 VPN 客户端的平台配置防火墙设置。规则基于诸如源地址、目标地址和协议等条件。扩展访问控制列表构建块对象用于定义流量过滤条件。选择或创建此组策略的扩展 ACL。定义**专用网络规则**以控制流向专用网络的数据，且/或定义**公用网络规则**以控制在已建立的 VPN 隧道之外以“明文”形式传输的数据。

注释 确保 ACL 仅包含 TCP/UDP/ICMP/IP 端口以及“任意”、“任意 IPv4”或“任意 IPv6”类型的源网络。

只有运行 Microsoft Windows 的 VPN 客户端才能使用这些防火墙设置。

自定义属性字段

本部分列出 AnyConnect 客户端 用于配置 Per App VPN，允许或延迟升级和动态分割隧道等功能的 AnyConnect 自定义属性。点击 **添加** 以向组策略添加自定义属性。

1. 选择 **AnyConnect 属性 (AnyConnect Attribute)**：Per App VPN、允许延迟更新或动态分割隧道。
2. 从列表中选择 **自定义属性对象** 。

注释 点击添加（+）以为所选 AnyConnect 属性创建新的自定义属性对象。您还可以在 **对象** > **对象管理** > **VPN** > **自定义属性**中创建自定义属性对象。请参阅添加 AnyConnect 客户端 自定义属性对象，第 1073 页。

3. 点击 **添加** 将属性保存到组策略，然后点击 **保存** 将更改保存到组策略。

相关主题

配置组策略对象，第 1063 页

组策略高级选项

导航路径

对象 > **对象管理** > **VPN** > **组策略**，点击点击**添加组策略**或选择要编辑的当前策略。，然后选择**高级**选项卡。

流量过滤器字段

- **访问列表过滤器** - 这些过滤器包含相应规则来确定是允许还是阻止通过 VPN 连接隧道传输的数据包。规则基于诸如源地址、目标地址和协议等条件。请注意，VPN 过滤器仅适用于初始连接。它不适用于因应用检查操作而打开的辅助连接，例如 SIP 媒体连接。扩展访问控制列表构建块对象用于定义流量过滤条件。选择或创建此组策略的新扩展 ACL。
- **限制 VPN 到 VLAN** - 也称为“VLAN 映射”，此参数指定该组策略应用到的会话的出口 VLAN 接口。ASA 将所有流量从该组转发到所选 VLAN。

  使用此属性向组策略分配 VLAN 以简化访问控制。向此属性赋值是在会话中使用 ACL 过滤流量的替代方法。除默认值（未限制）外，该下拉列表仅显示此 ASA 中配置的 VLAN。允许的值范围为 1 到 4094。

会话设置字段

- **访问时间** - 选择或创建时间范围对象。此对象指定该组策略可用于远程访问用户的时间范围。有关详细信息，请参阅时间范围，第 1039 页。
- **每个用户的同时登录数** - 指定允许某个用户执行的最多同时登录数。默认值为 3。最小值为 0，表示禁止登录并阻止用户访问。允许多个同时连接可能会危害安全性并影响性能。
- **最大连接时间/警报间隔** - 指定最大用户连接时间，以分钟为单位。此时间结束时，系统会终止连接。最小值为 1 分钟)。警报间隔指定在到达最大连接时间以向用户显示消息之前的时间间隔。

- **空闲超时/警报间隔** - 指定此用户的空闲超时时间，以分钟为单位。如果在此时间段内用户连接上没有通信活动，则系统会终止连接。最短时间为 1 分钟。默认值为 30 分钟。警报间隔指定在到达空闲时间以向用户显示消息之前的时间间隔。

相关主题

配置组策略对象，第 1063 页

文件对象

使用“添加文件对象”和“编辑文件对象”对话框可以创建和编辑文件对象。文件对象表示配置中使用的文件，通常适用于远程接入 VPN 策略。它们可以包含 AnyConnect 客户端配置文件和 AnyConnect 客户端映像文件。

还使用独立的配置文件编辑器为每个 AnyConnect 模块和 AnyConnect 客户端 管理 VPN 创建配置文件，并作为 AnyConnect 的一部分部署到管理员定义的终端用户要求和端点上的身份验证策略，他们将预配置的网络配置文件提供给终端用户使用。

在创建文件对象时，管理中心将在其存储库中创建该文件的副本。在创建数据库的备份时，将备份这些文件；如果恢复该数据库，也将恢复这些文件。在将文件复制到 平台以用于文件对象时，请不要将该文件直接复制到文件存储库。

在部署指定文件对象的配置时，会将相关联的文件下载到相应目录中的设备。

您可以针对每个文件点击以下选项之一：

- **下载 (Download)** - 点击下载 AnyConnect 文件。
- **编辑** -修改文件对象详细信息。
- **删除 (Delete)** - 删除 AnyConnect 客户端 文件对象。 在删除文件对象时，不会从文件存储库中删除相关联的文件，而只会删除该对象。

导航路径

对象 (Objects) > **对象管理 (Object Management)** > **VPN** > **AnyConnect 文件 (AnyConnect File)**。

字段

- **名称**-输入文件的名称以识别文件对象；最多可以添加 128 个字符。
- **文件名称**-点击 **浏览** 以选择文件。选择文件时，系统会添加文件名和完整路径。
- **文件类型**-选择与所选文件对应的文件类型。以下文件类型可用：
  - **AnyConnect 客户端映像 (AnyConnect Client Image)** - 当您添加从 Cisco 软件下载中心下载的 AnyConnect 客户端 映像时，请选择此类型。

    您可以将新的或附加的 AnyConnect 客户端 映像与 VPN 策略相关联。您也可以取消关联不受支持的或生命周期终止的客户端程序包。

- **AnyConnect VPN 配置文件 (AnyConnect VPN Profile)** - 为 AnyConnect VPN 配置文件选择此类型。

  使用基于GUI的 AnyConnect 配置文件编辑器（独立配置工具）来创建配置文件。有关详细信息，请参见相应版本的《思科 AnyConnect 安全移动客户端管理员指南》 中的 *AnyConnect* 配置文件编辑器 一章。

- **AnyConnect 管理 VPN 配置文件 (AnyConnect Management VPN Profile)** - 在为 AnyConnect 管理 VPN 隧道添加配置文件时选择此类型。

  从 Cisco 软件下载中心下载 AnyConnect **VPN 管理隧道独立配置文件编辑器**（如果尚未下载），并使用 AnyConnect 管理 VPN 隧道的所需设置创建配置文件。

- **AMP 启用程序服务配置文件 (AMP Enabler Service Profile)** - 该配置文件用于 AnyConnect AMP 启用程序。当远程访问 VPN 用户连接到 VPN 时，AMP 启动器和此配置文件会从 威胁防御 推送到终端。

- **反馈配置文件**-您可以添加客户体验反馈配置文件并选择此类型，以接收有关客户已启用和使用的功能和模块的信息。

- **ISE 终端安全评估配置文件 (ISE Posture Profile)** - 如果要为 AnyConnect ISE 终端安全评估模块添加配置文件，请选择此选项。

- **NAM 服务配置文件**-使用网络访问管理器配置文件编辑器配置和添加 NAM 配置文件。

- **网络可视性服务配置文件 (Network Visibility Service Profile)** - AnyConnect 网络可视性模块的配置文件。您可以使用 NVM 配置文件编辑器创建配置文件。

- **Umbrella 漫游安全配置文件**-如果使用使用配置文件编辑器创建的 .json 文件部署 Umbrella 漫游安全模块，则必须选择此文件类型。

- **网络安全服务配置文件**-在为网络安全模块添加配置文件时选择此文件类型。

- **HostScan 软件包**-添加 HostScan 软件包文件时选择此文件类型。此文件在配置动态访问策略（DAP）时用于收集有关终端上安装的操作系统，防病毒，反间谍软件和防火墙软件的信息。

- **AnyConnect 外部浏览器软件包 (AnyConnect External Browser Package)** - 此文件类型用于为 SAML 单点登录网络身份验证选择外部浏览器软件包文件。

  您可以在新版本的外部软件包文件可用时添加软件包文件。

  有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 1151 页。

- **说明**-添加可选说明。

相关主题

思科 AnyConnect 安全移动客户端 映像，第 1169 页
组策略 AnyConnect 客户端 选项，第 1066 页

证书映射对象

证书映射对象是一组命名的证书匹配规则。这些对象用于在接收的证书和远程接入VPN连接配置文件之间提供关联。连接配置文件和证书映射对象都是远程接入VPN策略的一部分。如果接收的证书与证书映射中包含的规则相匹配，则连接将被“映射”，或者与指定的连接配置文件相关联。规则按优先级顺序排列，并且按照它们在UI中的显示顺序进行匹配。当证书映射对象中的第一个规则产生一个匹配时，匹配结束。

导航

对象 > **对象管理** > **VPN** > **证书映射**

字段

- **名称** - 标识此对象，以便可以从其他配置（如远程接入 VPN）引用该对象。
- **映射条件** - 指定要评估的证书的内容。如果证书认为这些规则满足要求，则用户将被映射到包含此对象的连接配置文件。
  - **组件** - 选择要用于匹配规则的客户端证书的组件。
  - **字段** - 根据客户端证书的使用者或颁发者选择匹配规则的字段。

    如果**字段**设置为替代使用者或扩展密钥用法，则该组件将被冻结为整个字段
  - **运算符** - 为匹配规则选择运算符，如下所示：
    - 等于 - 证书组件必须与输入的值匹配。如果它们不完全匹配，则连接将被拒绝。
    - 包含 - 证书组件必须包含输入的值。如果组件不包含该值，则连接将被拒绝。
    - 不等于 - 证书组件不能等于输入的值。例如，对于一个选定的“国家/地区”证书组件，以及输入的“美国”值，如果客户的“国家/地区”值等于“美国”，则连接将被拒绝。
    - 不包含 - 证书组件不能包含输入的值。例如，对于一个选定的“国家/地区”证书组件，以及输入的“美国”值，如果客户的“国家/地区”值包含“美国”，则连接将被拒绝。
- **值** - 匹配规则的值。输入的值域所选的组件和运算符关联。

相关主题

配置证书映射，第 1172 页

AnyConnect 客户端 自定义属性对象

自定义属性由 AnyConnect 客户端 用于配置 Per App VPN、允许或延迟升级和动态拆分隧道等功能。一个自定义属性有一个类型和一个命名值。先定义属性的类型，然后可以定义此类型的一个或多个命名值。您可以使用 管理中心 来创建 AnyConnect 自定义属性对象，将对象添加到组策略，并将组策略与远程接入 VPN 关联，以启用 VPN 客户端的功能。

威胁防御 使用自定义属性对象支持以下功能：

- **Per App VPN**- Per App VPN 功能可帮助识别 威胁防御 管理员通过 VPN 允许的应用和仅隧道应用。
- **允许或延迟升级** - 延迟升级允许 AnyConnect 客户端 用户延迟 AnyConnect 客户端 升级的下载。如果有客户端更新，您可以配置 AnyConnect 客户端 的属性，以便打开一个询问用户是想要进行更新还是想要延迟升级的对话框。
- **动态拆分隧道 (Dynamic Split Tunneling)** - 通过动态拆分隧道，您可以调配在 VPN 隧道中包含或排除 IP 地址或网络的策略。通过创建自定义属性并将其添加到组策略，可配置动态分割隧道。

有关配置 AnyConnect 客户端 自定义属性的分步说明，请参阅 添加 AnyConnect 客户端 自定义属性对象，第 1073 页 和

有关为某个功能配置特定自定义属性的详细信息，请参阅所用 AnyConnect 客户端 版本的《*Cisco Secure* 客户端（包括 *AnyConnect*）管理员指南》。

相关主题

组策略 AnyConnect 客户端 选项，第 1066 页

添加 AnyConnect 客户端 自定义属性对象

开始之前

在为Per App VPN添加自定义属性对象之前，请确保已完成以下操作：

- Per App VPN 必须通过 MDM 正确配置，并且每个设备都必须注册到 MDM 服务器
- 使用 Cisco AnyConnect 客户端 企业应用选择器工具为每个应用创建 base64 编码字符串。
  1. 从这里下载 Cisco AnyConnect 客户端 企业应用选择器工具。
  2. 打开应用选择工具，然后从左上角的下拉菜单中选择移动平台。
  3. 通过输入友好名称和应用 ID 添加规则；其余字段为可选字段。
  4. 在菜单栏上，点击 **策略 (Policy)**。编码的 base65 规则以其编码格式显示。
  5. 选择并复制策略字符串，并将其保存以供稍后在创建 AnyConnect 客户端 自定义属性对象时使用。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)** > **VPN** > **自定义属性 (Custom Attribute)**。

步骤 2 点击**添加 AnyConnect 自定义属性 (Add AnyConnect Custom Attribute)**。

步骤 3 输入 **名称** 和可选属性的 **说明** 。

步骤 4 从 **AnyConnect 属性 (AnyConnect Attribute)** 下拉列表中选择一个属性：

- **Per App VPN**-选择此选项并在 **属性值** 框中指定 base64 编码的字符串。
- **允许延迟更新**-选择以下选项之一并指定所需的信息以允许或延迟 AnyConnect 客户端 客户端更新：
  - **显示提示直到用户执行操作**-显示提示给 VPN 用户，直到用户选择允许或推迟 VPN 客户端更新。
  - **显示提示直到超时**-选择此选项可显示指定持续时间的提示，并在 **超时** 框中指定持续时间。
  - **不显示提示并采取自动操作**-选择此选项以自动允许或推迟 VPN 更新。
  - **默认操作**-选择在用户不响应时或在您希望配置自动操作而无需用户干预时要采取的默认操作。您可以选择更新 AnyConnect 客户端 客户端或推迟更新。
  - **最低版本**-指定客户端系统上允许或推迟更新的最低 AnyConnect 版本。
- **动态拆分隧道**-选择此选项可在 VPN 隧道中包含或排除 IP 地址或网络。
  - **包含域**-指定将包含在远程访问 VPN 隧道中的域名。
  - **排除域**-指定将从远程访问 VPN 隧道中排除的域名。

步骤 5 选中 **允许覆盖** 复选框，允许对此对象组进行覆盖。

步骤 6 点击**保存**。
自定义属性对象添加到列表中。

下一步做什么

将自定义属性与组策略相关联。请参阅向组策略中添加自定义属性，第 1074 页。

向组策略中添加自定义属性

您必须将 AnyConnect 自定义属性与组策略相关联，才能将其用于远程访问 VPN 连接。您

过程

步骤 1 选择 **对象** > **对象管理** > **VPN** > **组策略**。

步骤 2 添加新的组策略或编辑现有组策略。

步骤 3 点击 **AnyConnect** > **自定义属性 (Custom Attributes)**。

步骤 4 点击**添加 (Add)**。

步骤 5 选择 **AnyConnect 属性 (AnyConnect Attribute)**：Per App VPN、允许延迟更新或动态分割隧道。

步骤 6 从列表中选择 **自定义属性对象** 。

注释 点击添加（+）以为所选 AnyConnect 属性创建新的自定义属性对象。您还可以在 **对象** > **对象管理** > **VPN** > **自定义属性**中创建自定义属性对象。请参阅添加 AnyConnect 客户端自定义属性对象，第 1073 页。

步骤 7 点击 **添加** 将属性保存到组策略，然后点击 **保存** 将更改保存到组策略。

相关主题

组策略 AnyConnect 客户端 选项，第 1066 页

第 43 章

证书

证书的要求和必备条件

支持的域

任意

用户角色

管理员

网络管理员

Cisco Secure Firewall Threat Defense VPN 证书指南和限制

- 如果 PKI 注册对象与某个设备关联并要安装在该设备上，证书注册过程将立即开始。对于自签名和 SCEP 注册类型，此过程将自动执行；它不需要任何额外的管理员操作。手动证书注册需要管理员操作。
- 注册完成后，设备上会出现一个信任点，其名称与 证书注册对象相同。在配置 VPN 身份验证方法时会使用此信任点。

- 威胁防御设备支持使用 Microsoft 证书颁发机构 (CA) 服务和思科自适应安全设备 (ASA) 和思科 IOS 路由器中提供的 CA 服务的证书注册。
- 威胁防御 设备无法配置为证书颁发机构 (CA)。

跨域和设备进行证书管理的指南

- 证书注册可以在子域或父域中完成。
- 当从父域执行注册时，证书注册对象也需要在同一个域中。如果该设备上的信任点在子域中被覆盖，则将在该设备上部署被覆盖的值。
- 当在分叶域中的设备上执行证书注册时，该注册对父域或其他子域是可见的。此外，还可以添加其他证书。
- 当一个叶域被删除时，将自动删除所包含的设备上的证书注册。
- 设备在一个域中注册了证书后，该设备将允许在其他任何域中进行注册。可以在其他域中添加该证书。
- 当您将一台设备从一个域移动到另一个域时，还会相应移动证书。您将收到一个警报，要求您删除这些设备上的注册。

管理 威胁防御 证书

有关数字证书的介绍，请参阅PKI 基础设施和数字证书 ，第 1096 页。

有关用于在受管设备上注册和获取证书的对象的说明，请参阅证书注册对象 ，第 1009 页。

过程

步骤 1 选择**设备** > **证书**。

您可以看到此屏幕上列出的每个设备的以下列：

- **名称**-列出已经与信任点关联的设备。展开设备可查看关联的信任点列表。
- **域**-显示特定域中注册的证书。
- **注册类型**-显示此信任点使用的注册类型。
- **状态**-提供 **CA 证书** 和 **身份证书** 的状态。当 可用时，您可以通过点击放大镜来查看证书内容。

  查看 CA 证书信息时，可以查看颁发 CA 证书的所有证书颁发机构的层次结构。

  如果注册失败，点击状态可显示故障消息。
- 点击右侧的**启用弱密码**，启用证书中的弱密码使用。当您点击切换按钮时，系统会在启用弱密码之前收到警告确认。点击 **是** 以启用弱密码。

注释　当由于弱密码使用导致证书注册失败时，系统会提示您启用弱密码。您可以选择在需要使用弱加密时启用弱密码。

- 附加列列出了用于执行以下任务的图标：
  - **导出证书**-点击以导出并下载证书的副本。您可以选择导出 PKCS12（完整证书链）或 PEM（仅身份证书）格式。

    您必须提供密码才能导出 PKCS12 证书格式，以便稍后导入文件。
  - **重新注册证书**-重新注册现有证书。
  - **刷新证书状态**-刷新证书会将 Firepower 威胁防御设备证书状态同步到 Firepower 管理中心。
  - **删除证书**-删除信任点的所有关联证书。

步骤 2 选择 **(+) 添加**以关联注册对象，并在设备上安装该注册对象。

在证书注册对象与某个设备关联并安装到该设备后，证书注册过程将立即开始。对于自签名和 SCEP 注册类型，此过程将自动执行，这意味着不需要任何额外的管理员操作。手动证书注册需要额外的管理员操作。

注释　在设备上注册证书不会阻止用户界面，并且注册过程将在后台执行，从而使用户能够在其他设备上并行执行证书注册。在同一个用户界面可以监控这些并行操作的进度。各自的图标显示各自的证书注册状态。

相关主题

使用自签注册安装证书 ，第 1081 页
使用 SCEP 注册安装证书，第 1082 页
使用手动注册安装证书，第 1084 页
使用 PKCS12 文件安装证书，第 1085 页

自动更新 CA 捆绑包

您可以将管理中心设置为通过 CLI 命令自动更新 CA 证书。默认情况下，当您安装或升级到版本 7.0.5 时，CA 证书会自动更新。

注释　在仅 IPv6 部署中，CA 证书的自动更新可能会失败，因为某些思科服务器不支持 IPv6。在这种情况下，请使用 **configure cert-update run-now force** 命令强制更新 CA 证书。

过程

步骤 1 使用 SSH 登录 FMC CLI，或者打开 VM 控制台（如果是虚拟的）。

步骤 2 您可以验证本地系统中的 CA 证书是否是最新的：

configure cert-update test

此命令将本地系统上的CA 捆绑包与最新的CA 捆绑包（来自思科服务器）进行比较。如果CA 捆绑包是最新的，则不会执行连接检查，并且会显示测试结果，如下所示：

示例：

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

如果 CA 捆绑包已过期，则对下载的 CA 捆绑包执行连接检查，展示结果。

示例：

当连接检查失败时：

```
> configure cert-update test
Test failed, not able to fully connect.
```

示例：

当连接检查成功时，或者 CA 捆绑包已经是最新的：

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

步骤 3 （可选）要立即更新 CA 捆绑包，请执行以下操作：

configure cert-update run-now

示例：

```
>configure cert-update run-now
Certs have been replaced or was already up to date.
```

执行此命令时，将验证 CA 证书（来自思科服务器）以进行 SSL 连接。如果其中一台思科服务器的 SSL 连接检查失败，该流程也会终止。

示例：

```
> configure cert-update run-now
Certs failed some connection checks.
```

要在连接失败的情况下继续更新，请使用 **force** 关键字。

示例：

```
> configure cert-update run-now force
Certs failed some connection checks, but replace has been forced.
```

步骤 4 如果您不希望自动更新 CA 捆绑包，请禁用配置：

configure cert-update auto-update disable

示例：

```
> configure cert-update auto-update disable
Autoupdate is disabled
```

步骤 5 要重新启用 CA 捆绑包的自动更新：

configure cert-update auto-update enable

示例：

```
> configure cert-update auto-update enable
Autoupdate is enabled and set for every day at 12:18 UTC
```

当您对 CA 证书启用自动更新时，系统将每天在系统定义的时间执行更新流程。

步骤 6 （可选）显示 CA 证书的自动更新状态。

show cert-update

示例：

```
> show cert-update
Autoupdate is enabled and set for every day at 09:34 UTC
CA bundle was last modified 'Thu Sep 15 16:12:35 2022'
```

使用自签注册安装证书

过程

步骤 1 在**设备 > 证书**屏幕上，选择**添加**，以打开**添加新证书**对话框。

步骤 2 从**设备**下拉列表中选择设备。

步骤 3 按照下列方式之一将证书注册对象与此设备关联：

- 从下拉列表中选择“自签名”类型的证书注册对象。
- 点击 **(+)**，以添加新的证书注册对象，请参阅添加证书注册对象 ，第 1011 页。

步骤 4 按**添加**开始自动自签名注册过程。

对于自签名注册类型的信任点， **CA 证书** 状态将始终显示，因为受管设备会充当自己的 CA，而不需要 CA 证书来生成自己的身份证书。

身份证书 (Identity Certificate) 状态会在设备创建自己的自签身份证书时由“进行中”(InProgress) 转变为“可用”(Available)。

步骤 5 点击放大镜可查看为此设备创建的自签身份证书。

下一步做什么

注册完成后，设备上会出现一个信任点，其名称与证书注册对象相同。请在您的“站点到站点”和“远程接入 VPN 身份验证方法”的配置中，使用此信任点。

使用 EST 注册安装证书

开始之前

注释 使用 EST 注册创建受管设备与 CA 服务器之间的直接连接。在开始注册流程之前，请确保您的设备已连接到 CA 服务器。

注释 不支持 EST 在证书过期时自动注册设备的功能。

过程

步骤 1 在 **设备 > 证书** 屏幕上，点击 **添加** 以打开 **添加新证书** 对话框。

步骤 2 从**设备**下拉列表中选择设备。

步骤 3 按照下列方式之一将证书注册对象与此设备关联：

- 从 **认证登记** 下拉列表中选择“手动”类型的证书注册对象。
- 点击 **(+)** 添加新证书注册对象，请参阅添加证书注册对象 ， 第 1011 页。

步骤 4 点击 **添加** 以在设备上注册证书。

身份证书 将在设备使用 EST 从指定的 CA 获取其身份证书后从 进行中 转变为 可用 。有时，可能需要手动刷新才能获取身份证书。

步骤 5 点击放大镜可查看为此设备创建和安装在此设备上的身份证书。

使用 SCEP 注册安装证书

开始之前

注释 使用 SCEP 注册创建受管设备与 CA 服务器之间的直接连接。在开始注册流程之前，请确保您的设备已连接到 CA 服务器。

过程

步骤 1 在**设备 > 证书**屏幕上，选择**添加**，以打开**添加新证书**对话框。

步骤 2 从**设备**下拉列表中选择设备。

步骤 3 按照下列方式之一将证书注册对象与此设备关联：

- 从下拉列表中选择 SCEP 类型的证书注册对象。
- 点击 **(+)**，以添加新的证书注册对象，请参阅添加证书注册对象，第 1011 页。

步骤 4 按**安装**，以开始自动注册过程。

对于 SCEP 注册类型信任点，**CA 证书**状态将在从 CA 服务器获取 CA 证书并安装在设备上后，从“进行中”过渡到“可用”。

身份证书将在设备使用 SCEP 从指定的 CA 获取其身份证书后从进行中转变为可用。有时，可能需要手动刷新才能获取身份证书。

步骤 5 点击放大镜可查看为此设备创建和安装在此设备上的身份证书。

下一步做什么

注册完成后，设备上会出现一个信任点，其名称与证书注册对象相同。请在您的“站点到站点”和“远程接入 VPN 身份验证方法”的配置中，使用此信任点。

使用 EST 注册安装证书

开始之前

注释 使用 EST 注册创建受管设备与 CA 服务器之间的直接连接。在开始注册流程之前，请确保您的设备已连接到 CA 服务器。

注释 不支持 EST 在证书过期时自动注册设备的功能。

过程

步骤 1 在 **设备 > 证书** 屏幕上，点击 **添加** 以打开 **添加新证书** 对话框。

步骤 2 从**设备**下拉列表中选择设备。

步骤 3 按照下列方式之一将证书注册对象与此设备关联：

- 从 **认证登记** 下拉列表中选择“手动”类型的证书注册对象。
- 点击 **(+)** 添加新证书注册对象，请参阅添加证书注册对象 ， 第 1011 页。

步骤 4 点击 **添加** 以在设备上注册证书。

身份证书 将在设备使用 EST 从指定的 CA 获取其身份证书后从 进行中 转变为 可用 。有时，可能需要手动刷新才能获取身份证书。

步骤 5 点击放大镜可查看为此设备创建和安装在此设备上的身份证书。

使用手动注册安装证书

过程

步骤 1 在**设备 > 证书**屏幕上，选择**添加**，以打开**添加新证书**对话框。

步骤 2 从**设备**下拉列表中选择设备。

步骤 3 按照下列方式之一将证书注册对象与此设备关联：

- 从下拉列表中选择“手动”类型的证书注册对象。
- 点击 **(+)**，以添加新的证书注册对象，请参阅添加证书注册对象 ， 第 1011 页。

步骤 4 按**添加**，以开始注册过程。

步骤 5 使用 PKI CA 服务器执行适当的活动，以获取身份证书。

a) 点击 **身份证书** 警告图标以查看和复制 CSR。

b) 使用 PKI CA 服务器执行适当的活动，以使用此 CSR 获取身份证书。

此活动完全独立于 Cisco Secure Firewall Management Center或受管设备。完成后，您将获得受管设备的身份证书。您可以将其放置在文件中。

c) 要完成手动过程，请将获得的身份证书安装到受管设备。

返回到 Cisco Secure Firewall Management Center对话框，并选择**浏览身份证书**以选择身份证书文件。

步骤 6 选择**导入 (Import)** 以导入身份证书。

导入完成时，身份证书状态将为 `Available`。

步骤 7 点击放大镜可查看此设备的**身份证书**。

下一步做什么

注册完成后，设备上会出现一个信任点，其名称与证书注册对象相同。请在您的“站点到站点”和“远程接入 VPN 身份验证方法”的配置中，使用此信任点。

使用 PKCS12 文件安装证书

过程

步骤 1 转至**设备 > 证书**屏幕，然后选择**添加**，以打开**添加新证书**对话框。

步骤 2 从**设备 (Device)** 下拉列表中选择预先配置的受管设备。

步骤 3 按照下列方式之一将证书注册对象与此设备关联：

- 从下拉列表中选择 PKCS 类型的证书注册对象。
- 点击 **(+)** 添加新证书注册对象，请参阅添加证书注册对象，第 1011 页。

步骤 4 按**添加**

CA 证书和身份证书状态会在其在设备上安装 PKCS12 文件时从 `In Progress` 变为 `Available`。

注释 第一次上传 PKCS12 文件时，该文件作为 CertEnrollment 对象的一部分存储在 Firepower 管理中心中。对于因密码错误或部署失败导致的任何失败注册，请重试注册 PKCS12 证书，无需再次上传文件。PKCS12 文件的大小不应超过 24K。

步骤 5 状态转变为可用 `(Available)` 后，请点击放大镜查看此设备的身份证书。

下一步做什么

受管设备上的证书（信任点）的名称与 PKCS#12 文件的名称相同。在 VPN 身份验证配置中使用此证书。

排除 威胁防御 证书问题

请参阅Cisco Secure Firewall Threat Defense VPN 证书指南和限制，第 1077 页确定您的证书注册环境中的变体是否可能导致问题。然后，考虑以下事项：

- 确保存在从设备到 CA 服务器的路由。

  如果在注册对象中给出了 CA 服务器的主机名，请使用 Flex Config 来配置 DNS 以适当方式到达服务器。或者，使用 CA 服务器的 IP 地址。

- 如果您使用的是 Microsoft 2012 CA 服务器，则受管设备不接受默认的 IPsec 模板，必须更改模板。

  请参阅您使用 MS CA 文档时的以下步骤来配置工作模板。

  1. 复制 IPsec（脱机请求）模板。
  2. 在**扩展 (Extensions) > 应用策略 (Application policies)** 中，请选择 *IP* 安全端系统 *(IP security end system)*，而不是 *IP* 安全 *IKE* 中间系统 *(IP security IKE intermediate)*。

3. 设置权限和模板名称。
4. 添加新模板并更改注册表设置以反映新的模板名称。

- 在 管理中心上，您可能会收到与 威胁防御 设备相关的以下运行状况警报：

  ```
  Code - F0853; Description - default Keyring's certificate is invalid, reason: expired
  ```

  在这种情况下，请使用以下命令在 CLISH CLI 中重新生成默认证书：

  ```
  > system support regenerate-security-keyring default
  ```

第 XII 部分

VPN

第 44 章

VPN 概述

虚拟专用网络 (VPN) 连接在使用公共网络（如互联网）的终端之间建立安全隧道。

本章适用于 Cisco Secure Firewall Threat Defense 设备上的 远程访问和 站点间 VPN。它描述了互联网协议安全 (IPsec)、互联网安全关联和密钥管理协议（ISAKMP 或 IKE）以及用于构建站点间 和远程接入 VPN 的 SSL 标准。

VPN 类型

管理中心 支持以下几种类型的 VPN 配置：

- 威胁防御设备上的远程接入 VPN。

  远程接入 VPN 是远程用户和您公司的专用网络之间的安全、加密连接或隧道。连接由 VPN 终端设备组成，该设备是具有VPN客户端功能的工作站或移动设备，以及在企业专用网络边缘的 VPN 前端设备或安全网关。

  Cisco Secure Firewall Threat Defense设备可以配置为通过 管理中心支持 SSL 或 IPsec IKEv2 上的远程接入 VPN。它们作为此功能中的安全网关，将对远程用户进行身份验证、授权访问以及加密数据，以提供与网络的安全连接。由 管理中心管理的其他任何类型的设备都不支持远程接入 VPN 连接。

  Cisco Secure Firewall Threat Defense安全网关支持 AnyConnect 安全移动客户端完整隧道客户端。为远程用户提供安全的 SSL IPsec IKEv2 连接需要此客户端。此客户端为远程用户提供了客户端所带来的好处，而不需要网络管理员在远程计算机上安装和配置客户端，因为它可以在连接时部署到客户端平台。它是终端设备上唯一受支持的客户端。

- 威胁防御设备上的站点间 VPN

  站点间VPN可连接不同地理位置的网络。您可以在托管设备之间以及托管设备与其他符合所有相关标准的思科或第三方对等体之间创建站点间的IPsec连接。这些对等体可以采用内部和外部IPv4和IPv6地址的任意组合。站点间隧道使用 Internet Protocol Security (IPsec) 协议套件和 IKEv1 或 IKEv2 构建。建立 VPN 连接之后，本地网关后台的主机可通过安全 VPN 隧道连接至远程网关后台的主机。

VPN 基础知识

借助隧道，可以使用互联网等公共TCP/IP网络在远程用户与企业专用网络之间创建安全连接。每个安全连接都称为一个隧道。

基于 IPSec 的 VPN 技术通过互联网安全关联和密钥管理协议（ISAKMP 或 IKE）以及 IPSec 隧道标准来建立和管理隧道。ISAKMP 和 IPSec 将完成以下操作：

- 协商隧道参数。
- 建立隧道。
- 验证用户和数据。
- 管理安全密钥。
- 加密和解密数据。
- 管理隧道中的数据传输。
- 作为隧道终端或路由器管理入站和出站数据传输。

VPN 中的设备可用作双向隧道终端。它可以从专用网络接收明文数据包，将其封装，创建隧道，然后发送到隧道的另一端，随后解封并发送到最终目标。它也会从公用网络接收封装数据包，将其解封，然后发送给其在专用网络上的最终目标。

建立站点间 VPN 连接之后，本地网关后的主机可通过安全 VPN 隧道连接至远程网关后的主机。一个连接由以下部分组成：这两个网关的IP地址和主机名、这两个网关后的子网，以及这两个网关用来进行相互身份验证的方法。

互联网密钥交换 (IKE)

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。

IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用提议。

IKE 策略是一组算法，供两个对等体用于保护它们之间的 IKE 协商。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数保护后续 IKE 协商。对于 IKE 版本 1

(IKEv1)，IKE 策略包含单个算法集和模数组。与 IKEv1 不同，在 IKEv2 策略中，您可以选择多个算法和模数组，对等体可以在第 1 阶段协商期间从中进行选择。可创建单个 IKE 策略，尽管您可能需要不同的策略来向最需要的选项赋予更高优先级。对于站点间 VPN，您可以创建单个 IKE 策略。

要定义 IKE 策略，请指定：

- 唯一优先级（1 至 65,543，其中 1 为最高优先级）。
- 一种 IKE 协商加密方法，用于保护数据并确保隐私。
- 散列消息身份验证代码 (HMAC) 方法（在 IKEv2 中称为完整性算法），用于确保发送人身份，以及确保消息在传输过程中未被修改。
- 对于 IKEv2，使用单独的伪随机函数 (PRF) 作为派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法。这些选项与用于散列算法的选项相同。
- Diffie-Hellman 组，用于确定 encryption-key-determination 算法的强度。设备使用此算法派生加密密钥和散列密钥。
- 身份验证方法，用于确保对等体的身份。
- 在更换加密密钥前，设备可使用该加密密钥的时间限制。

当 IKE 协商开始时，发起协商的对等体将其所有策略发送到远程对等体，然后远程对等体按优先级顺序搜索其自己的策略的匹配项。如果 IKE 策略具有相同的加密、散列（完整性和用于 IKEv2 的 PRF）、身份验证和 Diffie-Hellman 值，而且 SA 生命周期小于或等于发送的策略中的生命周期，则它们之间存在匹配。如果生命周期不相同，则应用远程对等体策略中较短的生命周期。默认情况下，Cisco Secure Firewall Management Center会为所有 VPN 终端部署优先级最低的 IKEv1 策略，以确保成功协商。

IPSec

IPsec 是设置 VPN 的最安全方法之一。IPsec 在 IP 数据包级别提供数据加密，提供一种基于标准的强大的安全解决方案。使用 IPsec，数据通过隧道在公共网络上传输。隧道是两个对等体之间安全的逻辑通信路径。进入 IPsec 隧道的流量由安全协议和算法组合保护。

Ipsec 提议策略定义 IPsec 隧道所需的设置。Ipsec 提议是应用于设备上 VPN 接口的一个或多个加密映射的集合。加密映射整合了设置 IPsec 安全关联所需的所有元素，包括：

- 提议（或转换集）是确保 IPsec 隧道中流量安全的安全协议和算法的组合。在 IPsec 安全关联 (SA) 协商期间，对等体搜索在两个对等体上相同的提议。找到后，提议将用于创建一个 SA，以保护该加密映射的访问列表中的数据流，从而保护 VPN 中的流量。IKEv1 和 IKEv2 有单独的 Ipsec 提议。在 IKEv1 提议（或转换集）中，对于每个参数都设置一个值。对于 IKEv2 提议，您可以为单个提议配置多个加密和集成算法。
- 加密映射整合了设置 Ipsec 安全关联 (SA) 所需的所有元素，包括 IPsec 规则、提议、远程对等体以及定义 IPsec SA 所需的其他参数。当两个对等体尝试建立 SA 时，必须至少有一个兼容的加密映射项。

  当未知的远程对等体尝试启动与本地中心的 IPsec 安全关联时，站点间 VPN 中将使用动态加密映射策略。中心不能是安全关联协商的发起者。动态加密策略允许远程对等体与本地中心交换

Ipsec流量，即使中心不知道远程对等体的身份。动态加密映射策略实质上创建了一个没有配置所有参数的加密映射项。稍后将动态配置缺少的参数（作为IPsec协商的结果）以满足远程对等体的要求。

动态加密映射策略适用于中心辐射型以及点对点VPN拓扑。要应用动态加密映射策略，请为拓扑中的一个对等体指定动态IP地址，同时确保在此拓扑上启用动态加密映射。请注意，在全网格 VPN 拓扑中，只能应用静态加密映射策略。

注释 对于 Firepower 威胁防御 (FTD) 上的远程访问和站点间 VPN，同一接口不支持同时使用 IKEv2 动态加密映射。

VPN 数据包流

在威胁防御设备上，默认情况下，不允许任何流量没有显式权限而通过访问控制。VPN隧道流量也不会中继到终端，直到它通过 Snort 为止。传入隧道数据包经过解码后才发送到 Snort 进程。Snort 在加密前将处理传出数据包。

识别 VPN 隧道每个终端节点的受保护网络的访问控制可以确定允许通过 威胁防御设备并访问终端的流量。对于远程接入 VPN 流量，必须将组策略过滤器或访问控制规则配置为允许 VPN 流量。

此外，在隧道关闭时，系统不向公共资源发送隧道流量。

IPsec 流分流

您可以将支持的设备型号配置为使用IPsec数据流分流。初始设置IPsec站点间VPN或远程访问VPN安全关联 (SA) 后，IPsec 连接将被分流到设备中的现场可编程门阵列 (FPGA)，这应该会提高设备性能。

分流操作特别涉及入口上的预解密和解密处理，以及出口上的预加密和加密处理。系统软件处理内部流以应用安全策略。

默认情况下启用 IPsec 数据流分流，并应用于以下设备类型：

- Secure Firewall 3100

IPsec 流分流的限制

不分流以下 IPsec 流：

- IKEv1 隧道。仅 IKEv2 隧道将被分流。IKEv2 支持更强的密码。
- 配置了基于卷的密钥更新的流。
- 已配置压缩的流。
- 传输模式流。仅会分流隧道模式流。

- AH 格式。仅支持 ESP/NAT-T 格式。
- 已配置后分段的流。
- 防重放窗口大小不是 64 位且防重放的流不会被禁用。
- 已启用防火墙过滤器的流。

配置 IPsec 数据流分流

默认情况下，在支持该功能的硬件平台上启用 IPsec 数据流分流。要更改配置，请使用 FlexConfig 实施 **flow-offload-ipsec** 命令。有关命令的详细信息，请参阅 ASA 命令参考。

VPN 许可

没有用于启用 Cisco Secure Firewall Threat Defense VPN 的特定许可，该 VPN 默认情况下是可用的。

管理中心根据智能许可服务器提供的属性，确定是允许还是阻止在 威胁防御 设备上使用强加密。

而控制这一点的，则是您在向思科智能许可证管理器注册时是否选择了允许在设备上使用出口控制功能的选项。如果您使用的是评估许可证，或者您没有启用出口控制功能，则无法使用强加密。

如果你用评估许可证创建了你的VPN配置，并将你的许可证从评估许可证升级为具有出口控制功能的智能许可证，请检查并更新你的加密算法，以加强加密，使 VPN 正常工作。不再支持基于 DES 的加密。

VPN 连接应具有多高的安全性？

由于VPN隧道通常流经公共网络（最可能是互联网），因此您需要对连接进行加密以保护流量。可以使用 IKE 策略和 IPsec 提议定义要应用的加密和其他安全技术。

如果您的设备许可证允许应用较强的加密，则有大量的加密和散列算法以及Diffie-Hellman组供您选择。然而，通常情况下，应用于隧道的加密越强，系统性能越差。您要在安全性和性能之间实现平衡，在提供充分保护的同时不牺牲效率。

我们无法就选择哪些选项提供具体指导。如果您在大型公司或其他组织执行运营，可能已有需要满足的指定标准。如果没有，请花些时间研究各个选项。

下面的主题介绍了几个可用选项。

遵守安全认证要求

许多VPN设置都有允许您遵守各种安全认证标准的选项。查看您的认证要求和可用选项以规划VPN配置。

决定使用哪个加密算法

在决定用于 IKE 策略或 IPsec 提议的加密算法时，您的选择仅限于 VPN 中的设备所支持的算法。

对于 IKEv2，您可以配置多个加密算法。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

对于 IPsec 提议，该算法用于封装安全协议 (ESP)，该协议提供身份验证、加密和防重放服务。ESP 为 IP 协议类型 50。在 IKEv1 IPsec 提议中，算法名称以 ESP- 为前缀。

如果设备许可证符合强加密要求，可以从以下加密算法中选择。如果不符合强加密要求，则只能选择 DES。

注释 如果符合强加密要求，在从评估许可证升级到智能许可证之前，请检查并更新加密算法以实现更强的加密，从而使 VPN 配置正常工作。选择基于 AES 的算法。如果您使用支持强加密的账户注册，则不支持 DES。注册后，在删除对 DES 的所有使用之前，您无法部署更改。

- AES-GCM - （仅 IKEv2。）Galois/Counter 模式中的高级加密标准是提供机密性和数据源身份验证的分组加密操作模式，并且提供比 AES 更高的安全性。AES-GCM 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。密钥越长，其提供的安全性就越高，但性能会随之降低。GCM 是支持 NSA Suite B 所需的 AES 模式。NSA Suite B 是一套加密算法，设备必须支持这套算法才能满足密码强度的联邦标准。.
- AES - 高级加密标准是一种对称密码算法，提供比 DES 更高的安全性，在计算上比 3DES 更高效。AES 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。密钥越长，其提供的安全性就越高，但性能会随之降低。
- DES - 数据加密标准，使用 56 位密钥进行加密，是一种对称密钥块算法。如果您的许可证账户不符合导出控制要求，这将是您唯一的选择。
- Null、ESP-Null - 不使用加密。空加密算法提供不加密的身份验证。这通常仅用于测试目的。但是，它在许多平台上根本不起作用，包括虚拟和 Firepower 2100。

决定使用哪些散列算法

在 IKE 策略中，散列算法创建消息摘要，用于确保消息的完整性。在 IKEv2 中，散列算法分成两个选项，一个用于完整性算法，一个用于伪随机函数 (PRF)。

在 IPsec 提议中，散列算法由封装安全协议 (ESP) 用于身份验证。在 IKEv2 IPsec 提议中，这称为完整性散列。在 IKEv1 IPsec 提议中，算法名称以 ESP- 为前缀，并且还有 -HMAC 后缀（代表“散列方法身份验证代码”）。

对于 IKEv2，您可以配置多个散列算法。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

您可以选择以下散列算法：

- SHA （安全散列算法）- 生成 160 位摘要的标准 SHA (SHA1)。

以下 SHA-2 选项更加安全，可用于 IKEv2 配置。如果要实施 NSA Suite B 加密规范，请选择以下选项之一。

- SHA256 - 指定具有 256 位摘要的安全散列算法 SHA 2。
- SHA384 - 指定具有 384 位摘要的安全散列算法 SHA 2。
- SHA512 - 指定具有 512 位摘要的安全散列算法 SHA 2。

- 空或无（NULL、ESP-NONE） -（仅限 IPsec 提议。）空散列算法；这通常仅用于测试目的。但是，如果选择 AES-GCM 选项之一作为加密算法，则应选择空完整性算法。即使选择非空选项，这些加密标准也会忽略完整性散列。

决定要使用的 Diffie-Hellman 模数组

您可以使用以下 Diffie-Hellman 密钥导出算法生成 IPsec 安全关联 (SA) 密钥。每组具有不同的长度模数。模数越大，安全性越高，但需要的处理时间更长。两个对等体上必须具有一个匹配的模数组。

如果选择 AES 加密，要支持 AES 所需的大型密钥长度，应使用 Diffie-Hellman (DH) 组 5 或更高组。IKEv1 策略不支持下面列出的所有组。

要实施 NSA Suite B 加密规范，请使用 IKEv2 并选择椭圆曲线 Diffie-Hellman (ECDH) 的一个选项：19、20 或 21。使用 2048 位模数的椭圆曲线选项和组较少遭受 Logjam 等攻击。

对于 IKEv2，您可以配置多个组。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

- 14 - Diffie-Hellman 组 14：2048 位模幂算法 (MODP) 组。被认为可以良好地保护 192 位密钥。
- 15 - Diffie-Hellman 组 15：3072 位 MODP 组。
- 16 - Diffie-hellman 组 16：4096 位 MODP 组。
- 19 - Diffie-Hellman 组 19：美国国家标准与技术研究所 (NIST) 256 位椭圆曲线取素数 (ECP) 组。
- 20 - Diffie-Hellman 组 20： NIST 384 位 ECP 组。
- 21 - Diffie-Hellman 组 21： NIST 521 位 ECP 组。
- 31 - Diffie-Hellman 组 31：椭圆曲线 25519 256 位 EC 组。

确定使用哪种身份验证方法

VPN 可用的身份验证方法是预共享密钥和数字证书。

站点间、IKEv1 和 IKEv2 VPN 连接都可以使用这两种方法。

仅使用 SSL 和 IPsec IKEv2 的远程访问仅支持数字证书身份验证。

在身份验证阶段，预共享密钥允许密钥在两个对等体之间共享并由 IKE 使用。必须在每个对等体上配置相同的共享密钥，否则无法建立 IKE SA。

数字证书使用RSA密钥对为IKE密钥管理消息进行签名和加密。证书规定两个对等体之间通信的不可否认性，这意味着可以证明通信已实际发生。使用此身份验证方法时，您需要定义一个公共密钥基础设施 (PKI)，以便对等体可以从证书颁发机构 (CA) 获得数字证书。CA 管理证书请求并向参与网络设备颁发证书，从而为所有参与设备提供集中密钥管理。

预共享密钥不能很好地扩展，使用 CA 可以提高 IPsec 网络的易管理性和可扩展性。使用 CA，不需要在所有加密设备之间配置密钥。相反，每个参与设备都向 CA 注册，并从 CA 请求证书。每个具有其自己的证书和 CA 公共密钥的设备都可以在给定 CA 的域内为其他各个设备进行身份验证。

预共享密钥

预共享密钥使您能够在两个对等体之间共享密钥。 IKE 在身份验证阶段使用此密钥。必须在每个对等体上配置相同的共享密钥，否则无法建立 IKE SA。

要配置预共享密钥，请选择是使用手动还是自动生成的密钥，然后指定IKEv1/IKEv2选项中的密钥。然后，在部署配置时，将在拓扑中的所有设备上配置该密钥。

PKI 基础设施和数字证书

公共密钥基础架构

PKI 为参与的网络设备提供集中密钥管理。它是一组定义的策略、程序和角色，通过生成、验证和撤销公钥证书（通常称为数字证书）支持公钥加密。

在公钥加密中，连接的每个终端均具有包含公钥和私钥的密钥对。密钥对被VPN终端用于消息签名和加密。这对密钥相互补充，用其中一个密钥加密的任何内容都可用另一个密钥解密，保证了连接上数据流的安全性。

生成一个用于签名和加密的通用RSA、ECDSA或EDDSA密钥对，也可以为每种用途生成单独的密钥对。单独的签名和加密密钥有助于降低泄露密钥的风险。SSL 使用密钥进行加密而非签名，但是，IKE 使用密钥进行签名而非加密。通过为每种用途使用单独的密钥，泄露密钥的风险降至最低。

数字证书或标识证书

当将数字证书用作 VPN 连接的身份验证方法时，系统将对等体配置为从证书颁发机构 (CA) 获取数字证书。CA 是“签署”证书以验证其真实性，从而确保设备或用户的身份的可信颁发机构。

作为公共密钥基础设施 (PKI) 的一部分，CA 服务器会管理公共 CA 证书请求并为参与的网络设备颁发证书，此活动称为证书注册。这些数字证书（又称为身份证书）包含：

- 所有者用于身份验证的数字识别信息，例如名称、序列号、公司、部门或 IP 地址。
- 向证书所有者发送和从证书所有者接收加密数据所需要的公钥。
- CA 的安全数字签名。

此外，证书还规定两个对等体之间通信的不可否认性，这意味着它们可以证明通信已实际发生。

证书注册

使用PKI可提高VPN的可管理性和可扩展性，因为您无需配置所有加密设备之间的预共享密钥。您需使用 CA 服务器单独注册每个参与设备，该 CA 服务器明确受信任进行设备身份验证和身份证书的创建。完成注册后，每个参与的对等体将其身份证书发送给另一个对等体，以使用证书中包含的公钥验证身份并建立加密会话。有关注册 威胁防御设备的详细信息，请参阅证书注册对象，第1009页。

证书颁发机构证书

为了验证对等体的证书，每个参与设备都必须从服务器检索CA证书。CA证书用于签署其他证书。它是自签名证书，也称为根证书。此证书包含CA的公钥，用于解密和验证收到的对等体证书的CA数字签名和内容。CA 证书可通过以下方式获得：

- 使用简单证书注册协议（SCEP） 或安全传输注册（EST） 从 CA 服务器检索 CA 的证书
- 从另一个参与的设备手动复制 CA 证书

信任点

完成注册后，会在受管设备上创建信任点。它是 CA 及关联证书的对象代表。信任点包含 CA 的身份、CA 特定的参数，以及与一个已注册身份证书的关联。

PKCS#12 文件

PKCS#12或PFX文件将服务器证书、任何中间证书和私钥保存在一个加密文件中。这种类型的文件可以直接导入到设备中以创建信任点。

撤销检查

CA 还可以为不再参与网络的对等体撤销证书。撤销的证书由联机证书状态协议 (OCSP) 服务器管理，或在存储于 LDAP 服务器上的证书撤销列表 (CRL) 中列出。对等体可以在从其他对等体接受证书之前对证书进行检查。

删除或弃用的散列算法、加密算法和Diffie-Hellman模数组

已删除对不太安全的密码的支持。我们建议您在升级到 威胁防御 6.70 以支持 DH 和加密算法之前更新 VPN 配置，以确保 VPN 正常工作。

更新 IKE 提议和 IPSec 策略以匹配 威胁防御 6.70 中支持的策略，然后再部署配置更改。

从 威胁防御 6.70 开始，以下安全性较低的密码已被删除或弃用：

- 已弃用 IKEv1 和 IKEv2 的 **Diffie-Hellman GROUP 5** 。
- Diffie-Hellman 组 2 和 24 已被删除。
- **加密算法**：3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256 已被删除。

注释 在评估模式下或对不满足强加密导出控制要求的用户继续支持 **DES**。

NULL 在 IKEv2 策略中已已删除，但在 IKEv1 和 IKEv2 IPsec 转换集中仍支持。

VPN 拓扑选项

在创建新的VPN拓扑时，您必须至少为其提供唯一名称，指定拓扑类型，然后选择IKE版本。您可以从三种拓扑类型中进行选择，每种类型都包括一组 VPN 隧道。

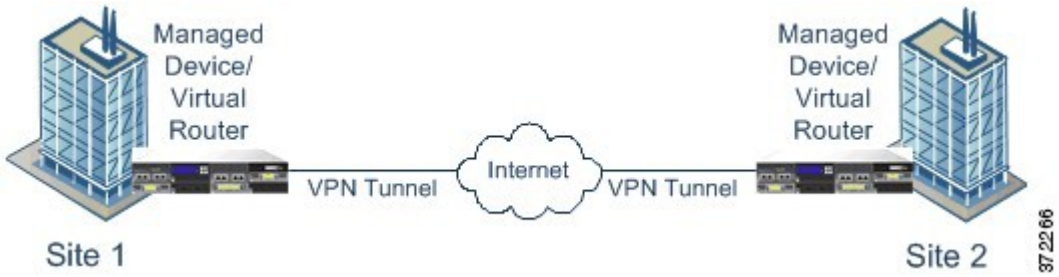
- 点到点 (PTP) 拓扑会在两个终端之间建立 VPN 隧道。
- 中心辐射型拓扑会建立一组 VPN 隧道，将中心终端连接到一组分支终端。
- 全网状拓扑会在一组终端之间建立一组 VPN 隧道。

手动或自动为 VPN 身份验证定义预共享密钥，没有默认密钥。如果选择自动，Cisco Secure Firewall Management Center会生成预共享密钥并将其分配给拓扑中的所有节点。

点对点 VPN 拓扑

在点对点VPN拓扑中，两个终端彼此直接通信。将两个终端配置为对等体设备，任一台设备均可启动安全连接。

下图显示了典型的点对点 VPN 拓扑。

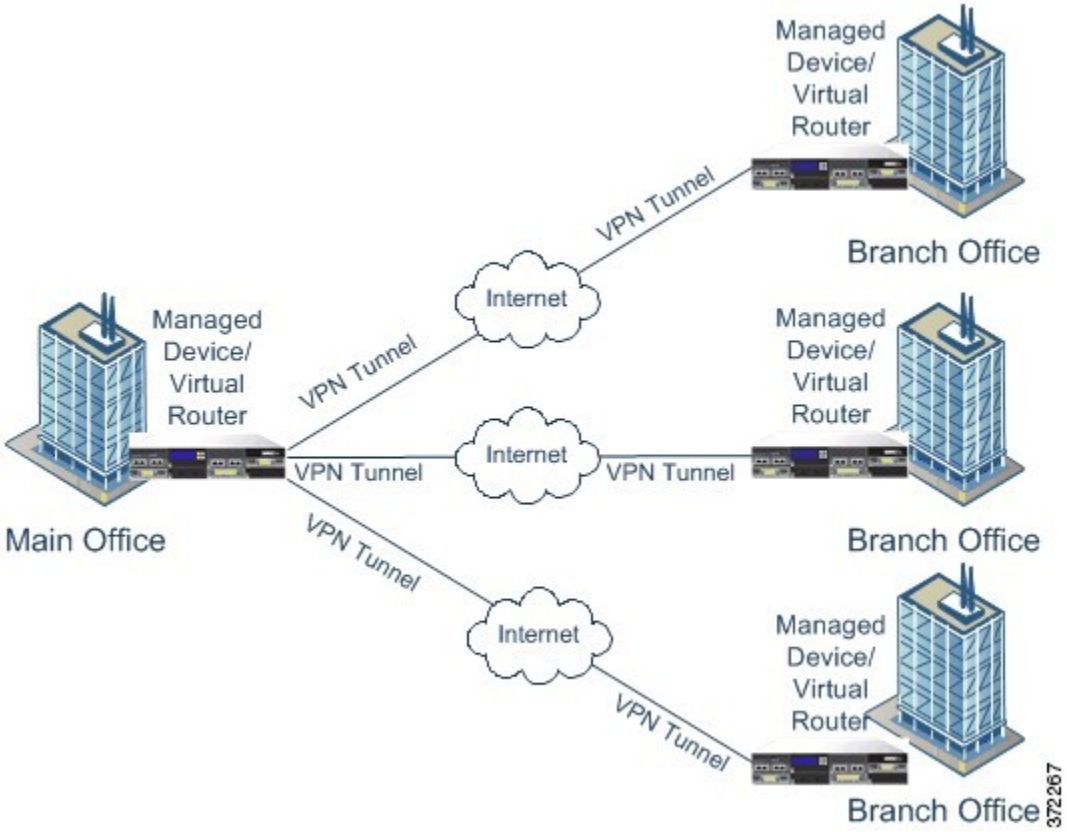


集中星型 VPN 拓扑

在集中星型VPN拓扑中，中心终端（集线器节点）与多个远程终端（辐射节点）连接。集线器节点与每个辐射终端之间的每条连接均为独立VPN隧道。任何辐射节点后台的主机均可通过集线器节点相互通信。

集中星型拓扑通常代表通过互联网或其他第三方网络建立安全连接，将公司总部和分公司相连的VPN。这些部署为所有员工提供对公司网络的受控访问权。通常，集线器节点位于总部。辐射节点位于分支机构并启动大部分流量。

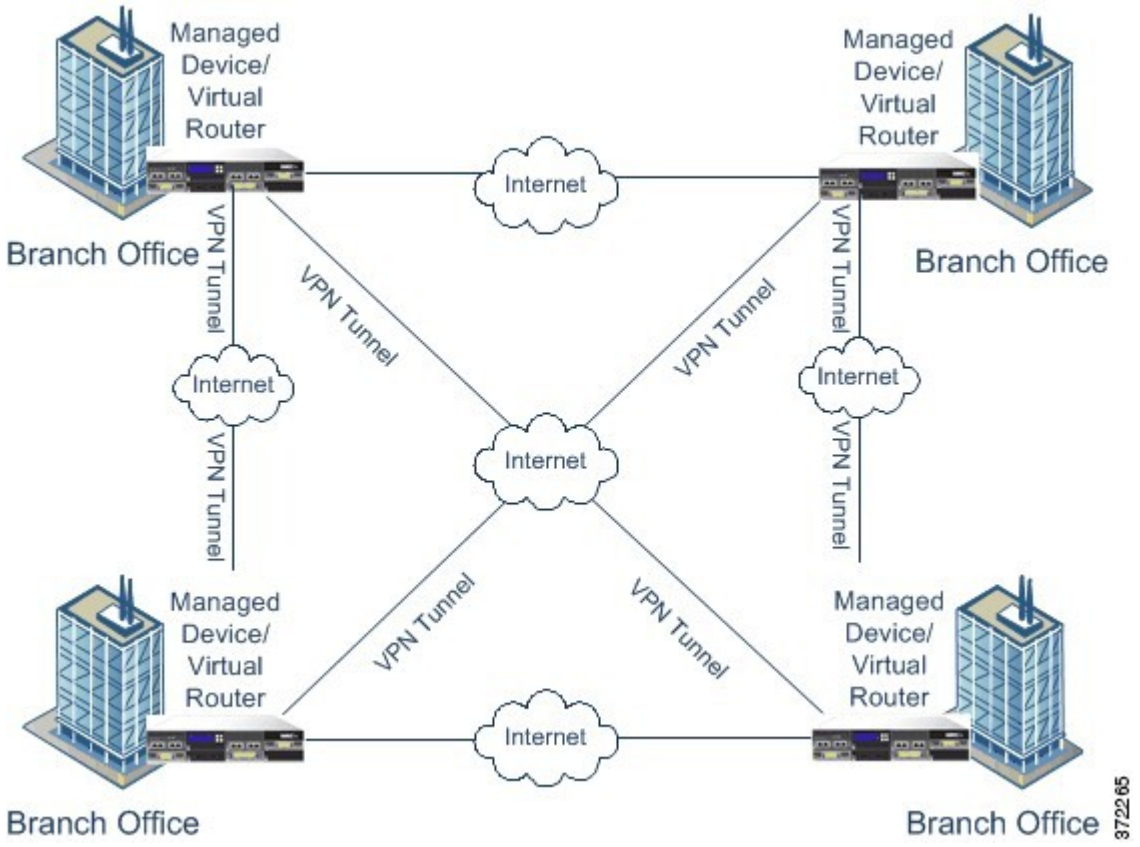
下图显示了典型的集中星型 VPN 拓扑。



全网状 VPN 拓扑

在全网状 VPN 部署中，所有终端均可通过单个 VPN 隧道与每个其他终端进行通信。这种拓扑可提供冗余，以便在某个终端出现故障时，其他终端仍然能够相互通信。它通常代表连接一组分散式分公司地点的 VPN。在此配置中，所部署的支持 VPN 的受管设备数量取决于所需的冗余级别。

以下图表显示了典型的全网状 VPN 拓扑。



隐式拓扑

除了三种主要的VPN拓扑以外，还可通过这些拓扑的组合形式创建其他更复杂的拓扑。具体包括：

- 部分网状结构 - 一种网络结构，其中部分设备按照全网状拓扑加以组织，而其他设备则形成中心辐射型结构，或与某些全网状设备的点对点连接。部分网状结构不能提供全网状拓扑那样的冗余度，但其实施成本相对较低。部分网状拓扑用于连接到全网状主干的外围网络。
- 分层中心辐射型结构 - 一种中心辐射型拓扑网络结构，其中某一设备可在一种或多种拓扑中作为中心设备，而在其他拓扑中作为辐射设备。允许从辐射组到其最直接中心的流量。
- 联合中心辐射型结构 - 两种连接起来形成点对点隧道的拓扑的组合（中心辐射型、点对点或全网状）。例如，联合中心辐射型拓扑可能包含两种中心辐射型拓扑，它们的中心充当点对点拓扑中的对等设备。

第 45 章

站点间 VPN

关于站点间 VPN

Cisco Secure Firewall Threat Defense站点间 VPN 支持以下功能：

- IPsec IKEv1 和 IKEv2 协议。
- 用于身份验证的证书和自动或手动预共享密钥。
- IPv4 和 IPv6。支持内部和外部的所有组合。
- IPsec IKEv2 站点间 VPN 拓扑提供符合安全认证的配置设置。
- 静态和动态接口。
- 支持 管理中心和 威胁防御 HA 环境。
- 当隧道关闭时，VPN 会发出警报。
- 可使用 威胁防御统一 CLI 获得的隧道统计信息。
- 点对点外联网和中心辐射型 VPN 的 IKEv1 和 IKEv2 备份对等体配置。
- “中心辐射型”部署中作为中心的外联网设备。

- 与“点对点”部署中外联网设备配对的托管终端的动态 IP 地址。
- 作为终端的外联网设备的动态 IP 地址。
- “中心辐射型”部署中作为外联网设备的中心。

VPN 拓扑

要创建一个新的站点到站点VPN拓扑，必须为其指定一个唯一名称，指定拓扑类型，选择用于IPsec IKEv1 和/或 IKEv2 的 IKE 版本。此外，确定您的身份验证方法。配置完毕后，可以将拓扑部署到威胁防御设备。Cisco Secure Firewall Management Center仅在 威胁防御设备上配置站点间 VPN。

您可以从三种拓扑类型中进行选择，包括一个或多个 VPN 隧道：

- 点对点 (PTP) 部署在两个终端之间建立 VPN 隧道。
- 中心辐射型部署会建立一组 VPN 隧道，将中心终端连接到一组分支节点。
- 全网状部署会在一组终端之间建立一组 VPN 隧道。

IPsec 和 IKE

在 Cisco Secure Firewall Management Center中，站点间 VPN 是根据分配给 VPN 拓扑的 IKE 策略和 IPsec 建议配置的。策略和建议是定义站点间 VPN 的特性的参数集，例如用于在 IPsec 隧道中保护流量安全的安全协议和算法。可能需要多种策略类型来定义可以分配给 VPN 拓扑的完整配置映像。

身份验证

要对VPN连接进行身份验证，请在拓扑中配置预共享密钥，或在每个设备上配置信任点。预共享密钥允许在两个对等体之间共享安全密钥，该共享密钥在 IKE 身份验证阶段使用。信任点包含 CA 的身份、CA 特定的参数，以及与一个已注册身份证书的关联。

外部网设备

每种拓扑类型都可以包括外部网设备，即不在 管理中心中管理的设备。其中包括：

- Cisco Secure Firewall Management Center 支持但您的组织不负责的思科设备。例如，由您公司内的其他部门管理的网络中的分支，或者与服务提供商或合作伙伴的网络的连接。
- 非思科设备。不能使用 Cisco Secure Firewall Management Center 创建配置以及将配置部署到非思科设备。

将非思科设备或未由 Cisco Secure Firewall Management Center管理的思科设备作为“外联网”设备添加到 VPN 拓扑。此外，还指定每个远程设备的 IP 地址。

Cisco Secure Firewall Threat Defense站点间 VPN 指南和限制

- 只能通过对不在当前域中的终端使用外部网对等体，才能在域之间建立 VPN 连接。
- 不能在域之间移动 VPN 拓扑。

- VPN 中不支持具有“range”选项的网络对象
- Cisco Secure Firewall Threat Defense VPN 只能使用 Firepower 管理备份进行备份。
- Cisco Secure Firewall Threat Defense VPN 当前不支持 PDF 导出和策略比较。
- 对于 Cisco Secure Firewall Threat Defense VPN，没有按隧道或按设备的编辑选项，只能编辑整个拓扑。
- 选择加密 ACL 时，不会对传输模式执行设备接口地址验证。
- 必须为拓扑中的所有节点配置加密 ACL 或受保护的网络。不可在一个节点上为拓扑配置加密 ACL，而在另一个节点上配置受保护的网络。
- 不支持自动镜像 ACE 生成。在任一端，对等设备的镜像 ACE 生成都是手动过程。
- 在使用加密 ACL 时，不支持 VPN 拓扑的隧道运行状况事件。使用加密 ACL 时，不支持中心、辐射和全网状拓扑；仅支持点到点 VPN。
- 只要使用的是 IKE 端口 500/4500，或者有一些 PAT 转换处于活动状态，则无法在同一端口上配置站点间 VPN，因为无法在这些端口上启动服务。
- 隧道状态不会实时更新，但是在 管理中心中以 5 分钟为间隔进行更新。
- 不支持将字符 "（双引号）作为预共享密钥的一部分。如果您在预共享密钥中使用了 "，请确保在升级到 Cisco Secure Firewall Threat Defense 6.30 后更改该字符。
- 站点间 VPN 中支持 ECMP 区域接口。

站点间 VPN 的要求和必备条件

型号支持

威胁防御

支持的域

枝叶

用户角色

管理员

管理站点间 VPN

“站点间 VPN”(Site to Site VPN) 页面提供站点间 VPN 隧道的快照。您可以查看隧道的状态，并根据设备、拓扑或隧道类型来过滤隧道。该页面每页列出20个拓扑，您可以在页面之间导航，以便查看更多拓扑详细信息。您可以点击单个 VPN 拓扑，以便展开并查看终端的详细信息。

开始之前

对于站点间 VPN 的证书身份验证，您必须通过按照证书，第 1077 页中的说明分配信任点来准备设备。

过程

选择**设备 > VPN > 站点到站点**管理您的 Firepower 威胁防御站点间 VPN 配置和部署。

该页面列出了站点间 VPN 拓扑，并使用颜色代码来指示隧道的状态：

- 活动（绿色）- 存在活动的 IPsec 隧道。
- 未知（琥珀色）- 未从设备收到隧道建立事件。
- 关闭（红色）- 不存在活动的 IPsec 隧道。
- 待部署 - 设备上尚未部署拓扑。

从以下选项中选择：

- **刷新 (Refresh)** - 查看 VPN 的更新状态。
- **添加 (Add)** - 创建新的策略型或路由型站点间 VPN。
- **编辑 (Edit)** - 修改现有 VPN 拓扑的设置。

  注释 在最初保存拓扑类型之后，不能对其进行编辑。要更改拓扑类型，应删除该拓扑并新建一个拓扑。

  两个用户不应 同时编辑同一拓扑；然而，Web 界面不会阻止同时编辑。

- **删除 (Delete)** - 要删除 VPN 部署，请点击 **删除**（ ）。
- 部署 - 选择**部署 > 部署**；请参阅部署配置更改，第 136 页。

  注释 一些 VPN 设置仅在部署期间进行验证。请务必确认部署已经成功。

配置策略型站点间 VPN

过程

步骤 1 选择**设备 > VPN > 站点到站点**。然后，选择**添加 VPN > Firepower 威胁防御设备**，或编辑列出的 VPN 拓扑。。

步骤 2 输入唯一的**拓扑名称**。我们建议命名您的拓扑以指示它是一个 威胁防御VPN，并指定其拓扑类型。

步骤 3 点击**策略型（加密映射）(Policy Based [Crypto Map])** 以配置站点间 VPN。

步骤 4 选择此 VPN 的**网络拓扑**。

步骤 5 选择要在 IKE 协商期间使用的 IKE 版本。**IKEv1** 或 **IKEv2**。

默认值是 IKEv2。根据需要选择一个或两个选项；如果拓扑中的任何设备不支持 IKEv2，请选择 IKEv1。

您也可以为点对点外联网 VPN 配置备份对等体。有关详细信息，请参阅威胁防御 VPN 终端选项，第 1105 页。

步骤 6 必需： 通过点击拓扑中每个节点的 **添加**（+），为该 VPN 部署添加终端。

按照威胁防御 VPN 终端选项， 第 1105 页中的描述配置每个终端字段。

- 对于“点到点”，配置**节点 A** 和**节点 B**。
- 对于“中心辐射型”，配置 **中心节点**和**分支节点**
- 对于“全网格”，配置多个**节点**

步骤 7 （可选） 按照描述为该部署指定非默认 IKE 选项 威胁防御 VPN IKE 选项， 第 1109 页

步骤 8 （可选） 按照描述为该部署指定非默认 IPsec 选项 威胁防御 VPN IPSec 选项， 第 1111 页

步骤 9 （可选） 按照威胁防御高级站点间 VPN 部署选项， 第 1113 页中的描述为该部署指定非默认高级选项。

步骤 10 点击**保存 (Save)**。
终端将添加到您的配置中。

下一步做什么

部署配置更改。

注释 一些 VPN 设置仅在部署期间进行验证。请务必确认部署已经成功。

如果您收到 VPN 隧道处于非活动状态的警报，即使 VPN 会话已启动，请按照 VPN 故障排除说明来验证并确保 VPN 处于活动状态。有关详细信息，请参阅 VPN 监控和故障排除 和 VPN 故障排除。

威胁防御 VPN 终端选项

导航路径

设备 > VPN > 站点到站点。然后，**添加 VPN > Firepower 威胁防御设备**，或编辑列出的 VPN 拓扑。打开**终端**选项卡。

字段

设备

为您的部署选择一个终端节点：

- 由此 管理中心管理的 威胁防御设备
- 由此 管理中心管理的 威胁防御高可用性容器
- **外部网**设备，并非由此 管理中心 管理的任意设备（思科或第三方设备）。

设备名称

仅对于外部网设备，为该设备提供一个名称。我们建议其命名可将其识别为非托管设备。

接口

如果选择受管设备作为其终端，请在该受管设备上选择一个接口。

对于“点对点”部署，您还可以配置具有动态接口的终端。具有动态接口的终端只能与外联网设备配对，无法与具有托管设备的终端配对。

您可以在**设备** > **设备管理** > **添加/编辑设备** > **接口**下配置设备接口。

IP 地址

- 如果选择外联网设备（**不**由 管理中心管理的设备），请为终端指定一个 IP 地址。

  对于外联网设备，选择**静态**并指定一个 IP 地址，或选择**动态**以允许动态外联网设备。
- 如果选择托管设备作为终端，则从下拉列表中选择一个 IPv4 地址或多个 IPv6 地址。这些 IP 地址已分配给托管设备上的此接口。
- 拓扑中的所有终端都必须具有相同的 IP 寻址方案。IPv4 隧道可以传输 IPv6 流量，反之亦然。受保护的网络定义隧道流量将使用的寻址方案。
- 如果受管设备是高可用性容器，请从接口列表中进行选择。

此 IP 为私有 IP

如果终端驻留在带网络地址转换 (NAT) 的防火墙后面，请选中此复选框。

注释 仅当对等体由同一个管理中心管理时才使用此选项，如果对等体是外联网设备，则不要使用此选项。

公有 IP 地址

如果选中了**此 IP 为私有 IP** 复选框，请为防火墙指定公共 IP 地址。如果终端为响应方，则必须指定此值。

连接类型

将允许的协商指定为双向、只应答或只发起。受支持的连接类型组合有：

表 *82:* 受支持的连接类型组合

远程节点	中心节点
只发起	只应答
双向	只应答
双向	双向

证书映射

选择预配置的证书映射对象，或点击 **添加**（＋） 以添加证书映射对象。证书地图定义在接收的客户端证书中需要哪些信息才能使其对 VPN 连接有效。有关详细信息，请参阅 证书映射对象，第 1072 页。

受保护网络

注意 中心辐射型拓扑 - 为避免动态加密映射的流量丢弃，请确保不要为两个终端选择任何受保护的网络。

如果受保护的网络配置为任何，则不会在两个终端上生成适用于隧道的加密 ACL。

定义受此 VPN 终端保护的网络。通过选择定义这些网络（受此终端保护的网络）的子网/IP 地址列表来选择网络。点击 **添加**（＋） 可选择可用的网络对象，或添加新的网络对象。请参阅 创建网络对象，第 999 页。访问控制列表会由此处所做的选择生成。

- **子网/IP 地址（网络）(Subnet/IP Address [Network])** - VPN 终端不能有相同的 IP 地址，并且 VPN 终端对中的受保护网络不能重叠。如果一个终端的受保护网络包含 IPv4 或 IPv6 条目，另一个终端的受保护网络必须至少包含一个相同类型的条目（IPv4 或 IPv6）。否则，另一个终端的 IP 地址必须为相同类型，且不会与受保护网络中的条目重叠。（对于 IPv4，使用 /32 CIDR 地址块；对于 IPv6 使用 /128 CIDR 地址块）。如果以上两种检查均失败，则此终端对无效。

注释 默认情况下，Cisco Secure Firewall Management Center 中会启用**启用反向路由注入 (Reverse Route Injection is enabled)**。

子网/IP 地址（网络）(Subnet/IP Address [Network]) 将保持默认选中。

如果已为“受保护的网络”(Protected Networks) 选择任意 *(Any)* 并观察到默认路由流量被丢弃，请禁用反向路由注入。选择 **VPN**> **站点间 (Site to Site)** > 编辑 VPN > **IPsec** > **启用反向路由注入 (Enable Reverse Route Injection)**。部署配置更改，以便从加密映射配置中删除 set reverse-route（反向路由注入），并删除导致反向隧道流量被丢弃的 VPN 通告反向路由。

- **访问列表（扩展）(Access List [Extended])** - 扩展访问列表提供控制此终端可接受的流量类型（例如GRE或OSPF流量）的功能。流量可通过地址或端口加以限制。点击**添加**（+）可添加访问控制列表对象。

注释 访问控制列表仅适用于点对点拓扑。

高级设置

启用动态反向路由注入 (Enable Dynamic Reverse Route Injection) - 反向路由注入 (RRI) 可让路由自动插入到受远程隧道终端保护的网络和主机的路由进程中。仅在成功建立 IPsec 安全关联 (SA) 后才会创建动态 RRI 路由。

注释

- 动态 RRI 仅在 IKEv2 上支持，在 IKEv1 或 IKEv1 + IKEv2 上不支持。
- 只发起对等体、全网状拓扑和外联网对等体不支持动态 RRI。
- 在点对点中，只有一个对等体可以启用动态 RRI。
- 在中心和分支之间，只有一个终端可以启用动态 RRI。
- 动态 RRI 不能与动态加密映射配合使用。

将本地身份发送到对等体 (Send Local Identity to Peers) - 选择此选项可将本地身份信息发送到对等设备。从列表中选择以下**本地身份配置 (Local Identity Configuration)** 之一并配置本地身份：

- **IP 地址 (IP address)** - 对身份使用接口的 IP 地址。
- **自动 (Auto)** - 对预共享密钥使用 IP 地址并对基于证书的连接使用证书 DN。
- **电邮 ID (Email ID)**- 指定要用于身份的邮件 ID。电邮 ID 最多可以包含 127 个字符。
- **主机名 (Hostname)** - 使用完全限定主机名。
- **密钥 ID (Key ID)** - 指定用于身份的密钥 ID。密钥 ID 必须少于 65 个字符。

本地身份用于为每个 IKEv2 隧道配置唯一身份，而不是为所有隧道配置一个全局身份。唯一身份允许 威胁防御 在 NAT 后面有多个 IPsec 隧道，以便连接到思科 Umbrella 安全互联网网关 (SIG)。

有关在 Umbrella 上配置唯一隧道 ID 的信息，请参阅 **Cisco Umbrella SIG 用户指南**。

VPN 过滤器 (VPN Filter) - 从列表中选择扩展访问列表，或点击**添加 (Add)** 以创建新的扩展访问列表对象，以过滤站点间 VPN 流量。

VPN 过滤器使用扩展访问列表来提供额外的安全性并过滤站点间 VPN 数据。通过为 VPN 过滤器选择的扩展访问列表对象，您可以在进入 VPN 隧道之前过滤预加密流量和离开 VPN 隧道的

已解密流量。如果启用了 **sysopt permit-vpn** 选项，将对来自 VPN 隧道的流量绕过访问控制策略规则。如果启用了 **sysopt permit-vpn** 选项，VPN 过滤器有助于识别和过滤站点间 VPN 流量。

注释 只有点对点和中心辐射型拓扑支持 VPN 过滤器。它在网状拓扑上不支持。

对于中心辐射型拓扑，您可以选择覆盖分支终端上的中心 VPN 过滤器，以免需要在特定隧道上启用不同的 VPN 过滤器。

选择**覆盖中心上的 VPN 过滤器 (Override VPN Filter on the Hub)** 选项以覆盖辐射点上的集线器 VPN 过滤器。选择**远程 VPN 过滤器 (Remote VPN Filter)** 扩展访问列表对象或创建要覆盖的访问列表。

注释 对于作为分支的外联网设备，只有**覆盖中心上的 VPN 过滤器 (Override VPN Filter on the Hub)** 选项可用。

有关 sysopt permit-VPN 的详细信息，请参阅威胁防御 高级站点间 VPN 隧道选项，第 1115 页。

威胁防御 VPN IKE 选项

对于您为此拓扑选择的 IKE 版本，请指定 **IKEv1/IKEv2 设置 (IKEv1/IKEv2 Settings)**。

注释 此对话框中的设置适用于整个拓扑、所有隧道和所有受管设备。

导航路径

设备 > VPN > 站点到站点。然后，**添加 VPN > Firepower 威胁防御设备**，或编辑列出的 VPN 拓扑。打开 **IKE** 选项卡。

字段

策略

从预定义列表中选择 IKEv1 或 IKEv2 策略对象，或者创建新的对象以供使用。您可以选择多个 IKEv1 和 IKEv2 策略。

有关详细信息，请参阅 威胁防御 IKE 策略，第 1058 页

身份验证类型

站点间 VPN 支持两种身份验证方法：预共享密钥和证书。有关这两种方法的说明，请参阅确定使用哪种身份验证方法，第 1095 页。

注释 在支持 IKEv1 的 VPN 拓扑中，所选 IKEv1 策略对象中指定的**身份验证方法**会成为 IKEv1 **身份验证类型**设置的默认设置。这些值必须匹配，否则，您的配置将出错。

- **预共享自动密钥 (Pre-shared Automatic Key)** - 管理中心会自动定义此 VPN 的预共享密钥。指定**预共享密钥长度 (Pre-shared Key Length)**，即密钥中的字符数（1-27 个）。

  不支持将字符 "（双引号）作为预共享密钥的一部分。如果您在预共享密钥中使用了 "，请确保在升级到 Cisco Secure Firewall Threat Defense 6.30 或更高版本后更改该字符。

- **预共享手动密钥 (Pre-shared Manual Key)** - 手动分配此 VPN 的预共享密钥。指定**密钥**，然后重新输入以**确认密钥**。

  在为 IKEv2 选择此选项后，将显示**仅执行基于十六进制的预共享密钥 (Enforce hex-based pre-shared key only)** 复选框，如果需要则将其选中。如果已经执行，则必须使用数字 0-9 或 A-F，为该密钥输入一个有效的十六进制值（它是一个 2-256 个字符的偶数）。

- **证书 (Certificate)** - 当您将证书用作 VPN 连接的身份验证方法时，对等体从 PKI 基础设施中的 CA 服务器获取数字证书，并用其相互进行身份验证。

  在**证书 (Certificate)** 字段中，选择预配置的证书注册对象。此注册对象可在托管设备上生成同名的信任点。证书注册对象应与设备关联并安装在设备上，之后注册过程完成，然后会创建一个信任点。

  信任点表示 CA 或身份对。信任点包括 CA 的身份、CA 特定配置参数，以及与一个注册的身份证书的关联。

  在选择此选项之前，请注意以下事项：

  - 确保你已经在拓扑结构中的所有端点上注册了一个证书注册对象 - 证书登记对象包含创建证书签名请求 (CSR) 以及从指定的证书颁发机构 (CA) 获取身份证书所需的 CA 服务器信息和注册参数。证书注册对象用于将受管设备注册到 PKI 基础设施中，并在支持 VPN 连接的设备上创建信任点（CA 对象）。有关创建证书注册对象的说明，请参阅添加证书注册对象，第 1011 页；有关在终端上注册对象的说明，请参阅以下适用内容之一：
    - 使用自签注册安装证书 ，第 1081 页
    - 使用 EST 注册安装证书，第 1082 页
    - 使用 SCEP 注册安装证书，第 1082 页
    - 使用手动注册安装证书，第 1084 页
    - 使用 PKCS12 文件安装证书，第 1085 页

注释 对于站点间 VPN 拓扑，请确保在拓扑中的所有终端中注册相同的证书注册对象。有关详细信息，请参阅下表。

- 请参阅下表，了解不同场景的注册要求。某些场景会要求您覆盖特定设备的证书注册对象。请参阅管理对象覆盖，第 968 页以了解如何覆盖对象。

证书注册类型	所有终端的设备身份证书均来自同一 CA		所有终端的设备身份证书均来自不同 CA
	未在证书注册对象中指定设备特定参数	在证书注册对象中指定了设备特定的参数	
手动	无需覆盖	需要覆盖	需要覆盖
EST	无需覆盖	需要覆盖	需要覆盖
SCEP	无需覆盖	需要覆盖	需要覆盖
PKCS	需要覆盖	需要覆盖	需要覆盖
自签名	不适用	不适用	不适用

- 了解Cisco Secure Firewall Threat Defense VPN 证书指南和限制，第 1077 页中提到的 VPN 证书限制。

注释 如果使用 Windows 证书颁发机构（CA），则默认应用策略扩展名为 **IP 安全 IKE 中间**。如果使用此默认设置，则必须在 **PKI 证书注册 (PKI Certificate Enrollment)** 对话框的**密钥 (Key)** 选项卡的“高级设置”(Advanced Settings) 部分中为所选对象选择**忽略 IPsec 密钥使用 (Ignore IPsec Key Usage)** 选项。否则，终端无法完成站点间 VPN 连接。

威胁防御 VPN IPSec 选项

注释 此对话框中的设置适用于整个拓扑、所有隧道和所有受管设备。

加密映射类型

加密映射整合了设置 IPsec 安全关联 (SA) 所需的所有组件。当两个对等体尝试建立 SA 时，每个对等体均必须至少有一个兼容的加密映射项。IPsec 安全协商使用加密映射条目中定义的提议来保护该加密映射的 IPsec 规则所指定的数据流。为此部署的加密映射选择静态或动态模式：

- **静态** - 在点对点或全网状 VPN 拓扑中使用静态加密映射。
- **动态** - 动态加密映射实质上创建了一个不配置所有参数的加密映射项。稍后将动态配置缺少的参数（作为 IPsec 协商的结果）以满足远程对等体的要求。

  动态加密映射策略适用于中心辐射型以及点对点 VPN 拓扑。要应用这些策略，请为拓扑中的一个对等体指定动态 IP 地址，同时确保在此拓扑上启用动态加密映射。在全网格 VPN 拓扑中，只能应用静态加密映射策略。

IKEv2 模式

仅限于 IPsec IKEv2，请指定将 ESP 加密和身份验证应用于隧道的封装模式。此字段确定原始 IP 数据包的哪个部分已应用 ESP。

- **隧道模式** -（默认）封装模式设置为隧道模式。隧道模式将 ESP 加密和身份验证应用至整个原始 IP 数据包（IP 报头和数据），隐藏最终的源主机和目标地址，并成为新 IP 数据包中的负载。

  隧道模式的主要优势是不需要修改终端系统即可获得IPsec的优势。此模式允许路由器等网络设备用作IPsec代理。也就是说，路由器代表主机执行加密。源路由器加密数据包并将其沿 IPsec 隧道转发。目标路由器解密原始 IP 数据报并将其转发到目标系统。隧道模式还可以防止流量分析；利用隧道模式，攻击者只能确定隧道终端，而无法确定通过隧道传送的数据包的真正源和目标，即使其与隧道终点一样也无法确定。

- **传输首选 (Transport preferred)** - 封装模式设置为传输模式，且可选择在对等体不支持时回退到隧道模式。在传输模式下，仅加密 IP 负载，原始 IP 报头保持不变。因此，管理员必须选择与 VPN 接口 IP 地址相匹配的受保护网络。

  此模式的优势是每个数据包只需增加几个字节并且允许公共网络上的设备查看数据包的最终源和目标。在传输模式下，可以根据 IP 报头中的信息在中间网络上启用特殊处理（例如 QoS）。然而，第 4 层报头将被加密，这就限制了对数据包的检查。

- **传输必要 (Transport required)** - 封装模式设置为仅传输模式，允许回退到隧道模式。如果因一个端点不支持，端点无法成功协商传输模式，将不进行 VPN 连接。

计划书

点击 **编辑**（✎），以便为所选 IKEv1 或 IKEv2 方法指定提议。从可用的 **IKEv1 Ipsec 提议 (IKEv1 IPsec Proposals)** 或 **IKEv2 Ipsec 提议 (IKEv2 IPsec Proposals)** 对象中进行选择，或创建一个新的对象并选择该对象。请阅参配置 IKEv1 IPsec 方案对象，第 1061 页和配置 IKEv2 IPsec 方案对象，第 1062 页了解详情。

启用安全关联 (SA) 强度实施

启用此选项可确保子 IPsec SA 使用的加密算法不比父 IKE SA 更强 (根据密钥中的位数)。

启用反向路由注入

启用反向路由注入 (RRI) 支持静态路由自动插入到受远程隧道终端保护的网络和主机的路由进程中。

启用完全向前保密

是否使用完美前向保密 (PFS) 为每个加密交换生成和使用唯一会话密钥。唯一会话密钥可保护交换免于后续解密，即使整个交换已被记录且攻击者已经获得终端设备使用的预共享或私有密钥。如果选择此选项，也请选择在模数组列表中生成 PFS 会话密钥时使用的 Diffie-Hellman 密钥导出算法。

模块组

用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。 有关选项的完整说明，请参阅 决定要使用的 Diffie-Hellman 模数组，第 1095 页。

生命周期持续时间
安全关联在过期之前存在的秒数。默认值为 28,800 秒。

寿命大小
使用特定安全关联的Ipsec对等体之间在该安全关联到期前可通过的流量（以千字节为单位）。默认值为 4,608,000 千字节。不允许使用无限数据。

ESPv3 设置

验证传入 ICMP 错误消息
选择是否验证通过 IPsec 隧道接收，并发往专用网络上的内部主机的 ICMP 错误消息。

启用“不分段”策略
定义 IPsec 子系统如何处理大型数据包，这些数据包在 IP 报头中设置了不分片 (DF) 位。

策略

- Copy DF bit - 保持 DF 位。
- Clear DF bit - 忽略 DF 位。
- Set DF bit - 设置并使用 DF 位。

启用数据流机密性 (TFC) 数据包
启用虚拟TFC数据包，这些数据包会通过隧道，用于屏蔽流量配置文件。可以使用**Burst**、**Payload Size** 和 **Timeout** 参数生成穿过指定 SA 的随机长度的数据包。

注释 您可以按照任意长度和间隔对 IPsec 安全关联 (SA) 启用虚拟流量机密性 (TFC) 数据包。您必须在启用 TFC 之前设置 IKEv2 IPsec 提议。

启用 TFC 数据包可防止 VPN 隧道处于空闲状态。因此，如果启用了 TFC 数据包，则组策略中配置的 VPN 空闲超时不会按预期工作。

威胁防御高级站点间 VPN 部署选项

以下部分介绍在站点间VPN部署中可以指定的高级选项。这些设置适用于整个拓扑、所有隧道和所有受管设备。

威胁防御 VPN 高级 IKE 选项

高级 > IKE > ISAKAMP 设置

IKE 保持连接

启用或禁用 IKE 保持连接。您可以将此选项设置为 EnableInfinite，以便设备从不会启动保持连接来监控自身。

阈值
指定 IKE 保持连接置信间隔。该间隔是允许对等体在开始保持连接监控之前空闲的秒数。最小间隔值为 10 秒（默认值）；最大间隔值为 3600 秒。

重试间隔
指定在 IKE 保持连接重试之间等待的秒数。默认值为 2 秒；最大值为 10 秒。

发送至对等体的身份：
选择对等体将在 IKE 协商期间用于标识自身的身份：

- **autoOrDN**（默认值）- 按连接类型确定 IKE 协商：用于预共享密钥的 IP 地址或用于证书身份验证的证书 DN（不受支持）。
- **ipAddress** - 使用交换 ISAKMP 身份信息的主机的 IP 地址。
- **hostname** - 使用交换 ISAKMP 身份信息的主机的完全限定域名。此名称包含主机名和域名。

注释 为所有 VPN 连接启用或禁用此选项。

启用激进模式
如果 IP 地址未知，并且 DNS 解析在设备上可能不可用，请选择此协商方法来交换密钥信息。协商基于主机名和域名。

在隧道断开连接时启用通知
当 SA 上接收的入站数据包与该 SA 的流量选择器不匹配时，允许管理员启用或禁用向对等体发送 IKE 通知。默认情况下会禁用发送此通知。

高级 > IKE > IVEv2 安全关联 (SA) 设置

IKE v2 可使用其他会话控制，限制打开的 SA 的数量。默认情况下，打开的 SA 的数量没有限制。

Cookie 质询
是否向对等体设备发送 Cookie 质询，以响应 SA 发起数据包，这可以帮助阻止拒绝服务 (DoS) 攻击。默认情况下，当 50% 的可用 SA 正在协商时使用 Cookie 质询。选择以下选项之一：

- 自定义
- 从不（默认）
- 始终

质询传入 Cookie 的阈值
正在协商的允许的 SA 总数的百分比。这将对未来的任何 SA 协商都触发 Cookie 质询。范围为 0 到 100%。

协商中允许的 SA 数
限制可以随时协商的 SA 的最大数量。如果与 Cookie 质询配合使用，可以配置低于此限制的 Cookie 质询阈值，以便实现有效的交叉检查。

允许的最大 SA 数
限制允许的 IKEv2 连接数。默认值为不受限制。

在隧道断开连接时启用通知
当 SA 上接收的入站数据包与该 SA 的流量选择器不匹配时，允许管理员启用或禁用向对等体发送 IKE 通知。默认情况下禁用发送此通知。

威胁防御 VPN高级 IPsec 选项

高级 > IPsec > IPsec 设置

加密前启用分段
此选项允许流量通过不支持 IP 分片的 NAT 设备。这不影响支持 IP 分片的 NAT 设备的运行。

路径最大传输单元老化
选中以启用“路径最大传输单元 (PMTU) 时效”，即重置安全关联 (SA) 的 PMTU 的间隔时间。

值重置间隔
输入 SA 的 PMTU 值重置为其原始值的分钟数。有效范围是 10 到 30 分钟，默认值为不受限制。

威胁防御 高级站点间 VPN 隧道选项

导航路径

设备 > VPN > 站点到站点，然后，选择**添加 VPN > Firepower 威胁防御设备**，或编辑列出的 VPN 拓扑。打开**高级**选项卡，然后在导航窗格中选择**隧道**。

隧道选项

仅可用于中心辐射型拓扑和全网状拓扑。对于点对点配置，不会显示此部分。

- **使辐射间连接通过中心** - 默认情况下将被禁用。选择此字段将使辐射每一端上的设备将其连接通过中心节点扩展到另一台设备。

NAT 设置

- **保持连接消息穿越** - 选择是否启用 NAT 保持连接消息穿越。NAT 遍历保持连接用于在 VPN 连接的中心和分支之间存在设备（中间设备）并且该设备对 IPsec 流执行 NAT 时，传输保持连接消息时。

  如果选择此选项，请配置在辐射与中间设备之间发送两次保持连接信号（以指示会话处于活动状态）之间的**间隔**（以秒为单位）。此值可以介于 5 到 3600 秒之间。默认值为 20 秒。

VPN 流量访问控制

- **为已解密的流量绕过访问控制策略 (sysopt permit-vpn)** - 默认情况下，威胁防御 会在解密的流量上应用访问控制策略检查。启用此选项可绕过 ACL 检查。威胁防御 仍会将从 AAA 服务器下载的 VPN 过滤器 ACL 和授权 ACL 应用于 VPN 流量。

  启用或禁用所有 VPN 连接的选项。如果禁用此选项，请确保访问控制策略或预过滤器策略允许流量。

证书映射设置

- **使用在终端中配置的证书映射来确定隧道** - 如果启用（选中）此选项，则将通过匹配已收到证书的内容与在终端节点中配置的证书对象的内容，来确定隧道。

- **使用证书 OU 字段来确定隧道** - 如果选择此选项，将指示如果无法根据已配置的映射确定节点（上面的选项），则将使用已收到证书的使用者可分辨名称 (DN) 中组织单位 (OU) 的值来确定隧道。
- **使用 IKE 身份来确定隧道** - 如果选择此选项，将指示如果无法根据规则匹配确定或通过 OU 获取节点（上面的选项），则会根据 phase1 IKE ID 的内容，将基于证书的 IKE 会话映射到隧道。
- **使用对等体 IP 地址来确定隧道** - 如果选择此选项，将指示如果无法根据规则匹配确定或通过 OU 或 IKE ID 方法获取节点（上面的选项），则将使用已建立的对等体 IP 地址。

关于 Virtual Tunnel Interface

管理中心 支持称为虚拟隧道接口 (VTI) 的可路由逻辑接口。VTI 不需要将 IPsec 会话静态映射到物理接口。IPsec 隧道终端与虚拟接口关联。您可以像使用其他接口一样使用这些接口，并应用静态和动态路由策略。在使用 VTI 时，您不必配置静态加密映射访问列表并将其映射到接口。您不再需要跟踪所有远程子网并将其包含在加密映射访问列表中。

作为策略型 VPN 的替代方案，您可以在 VTI 的对等体之间创建 VPN 隧道。VTI 可通过将 IPSec 配置文件连接到每个隧道的端部，为基于 VPN 的路由提供支持。VTI 会使用静态或动态路由。设备加密或解密来自或到达隧道接口的流量，并根据路由表将其转发。这可以简化部署，而且 VTI 通过动态路由协议支持路由型 VPN，还能满足虚拟私有云的诸多要求。管理中心 让您能够从基于密码图的 VPN 配置轻松迁移到基于 VTI 的 VPN。

您可以在 管理中心、威胁防御、设备 REST API 和 设备管理器 中配置路由型 VPN，也可以通过配置静态 VTI 来进行配置。管理中心 支持使用默认设置的站点间 VPN 向导来配置 VTI 或路由型 VPN。使用静态路由或 BGP 加密流量。

您可以创建路由安全区，向其添加 VTI 接口，然后为通过 VTI 隧道为解密的流量控制定义访问控制规则。

您可以在以下对象之间创建基于 VTI 的 VPN：

- 两台 威胁防御 设备。
- 一个威胁防御和公共云。
- 一个威胁防御和另一个具有运营商冗余的威胁防御。
- 一个威胁防御以及任何其他带有 VTI 接口的设备。

有关详细信息，请参阅 静态 VTI，第 1117 页 。

威胁防御功能历史记录

静态 VTI

您可以使用静态 VTI 配置进行站点间连接，其中两个站点之间的隧道会始终在线。对于静态 VTI 接口，您必须将物理接口定义为隧道源。每个设备最多可以关联 1024 个 VTI。要在管理中心创建静态 VTI 接口，请参阅添加 VTI 接口，第 1119 页。

Virtual Tunnel Interfaces 准则和限制

IPv6 支持

- VTI 支持 IPv6。
- 隧道源接口可以有一个 IPv6 地址，并且同样的地址可以用作隧道终端。
- 管理中心 支持以下 VTI IP（或内部网络 IP 版本）与公共 IP 版本的组合：
  - IPv6 over IPv6
  - 基于 IPv6 的 IPv4
  - IPv4 over IPv4
  - 基于 IPv4 的 IPv6
- VTI 支持将静态和动态 IPv6 地址作为隧道源和目的地址。
- 隧道源接口可以有一个 IPv6 地址，并且您可以将隧道终端地址。如果不指定地址， 威胁防御使用列表中的第一个 IPv6 全局地址会被默认为隧道终端。

BGP IPv6 支持

VTI 支持 IPv6 BGP。

多实例和群集

- 多实例中支持 VTI。
- VTI 不支持群集。

防火墙模式

仅在路由模式中支持 VTI。

静态 VTI 的限制

- 仅支持 20 个唯一的 IPSec 配置文件。

- 不支持动态 VTI、OSPF 和 QoS。
- 在策略型路由中，您只能将 VTI 配置为出口接口。

静态VTI 的一般配置准则

- VTI 只有在 IPsec 模式下才可配置。
- 可以将 BGP 或静态路由用于使用这种隧道接口的流量。
- 您最多可以在一台设备上配置 1024 个静态 VTI。在计算 VTI 计数时，请考虑以下事项：
  - 包括 nameif 子接口，以便得出可在设备上配置的 VTI 总数。
  - 您不能在端口通道的成员接口上配置 nameif。因此，隧道计数只会随实际主端口通道接口的数量减少，而不会随其任何成员接口的数量减少。
  - 平台上的 VTI 计数限于该平台上可配置的 VLAN 数量。例如，Firepower 1120 支持 512 个 VLAN，隧道计数为 512 减去配置的物理接口数。
- 如果要在高可用性设置中的设备上配置超过 400 个 VTI，您必须将 45 秒配置为 威胁防御 HA 的设备保持时间。
- VTI 的 MTU 将根据底层物理接口自动设置。
- 静态 VTI 支持 IKE 版本 v1 和 v2，并使用 IPsec 在隧道的源地址与目标地址之间收发数据。
- 如果必须应用 NAT，则将 IKE 和 ESP 数据包封装在 UDP 报头中。
- 无论隧道中的数据流量如何，IKE 和 IPsec 安全关联都将不断重新生成密钥。这可确保 VTI 隧道始终处于活动状态。
- 隧道组名称必须与对等体作为其 IKEv1 或 IKEv2 身份发送的内容相符。
- 对于 LAN 间隧道组中的 IKEv1，仅当隧道身份验证方法为数字证书和/或对等体配置为使用积极模式时，才能使用非 IP 地址的名称。
- 只要加密映射中配置的对等体地址与 VTI 的隧道目的地址不同，VTI 和加密映射配置就可以在同一个物理接口上共存。
- 默认情况下，所有通过 VTI 发送的流量都会被加密。
- 可以在 VTI 接口上应用访问规则来控制通过 VTI 的流量。
- 您可以将 VTI 接口与 ECMP 区域关联，同时配置 ECMP 静态路由以实现以下目的：
  - 负载均衡（主用/主用 VTI）- 连接可以通过任何并行 VTI 隧道进行传输。
  - 无缝连接迁移 - 当 VTI 隧道无法访问时，流会被无缝迁移到同一区域中配置的另一个 VTI 接口。
  - 非对称路由 - 通过一个 VTI 接口转发流量，并通过另一个 VTI 接口配置反向流量。

有关配置 ECMP 的信息，请参阅配置等价静态路由，第 858 页。

备份 VTI 的准则和限制

- 不支持跨隧道故障转移的流恢复能力。例如，明文 TCP 连接在隧道故障切换后丢失，而您需要重新启动故障转移期间发生的任何 FTP 传输。
- 备份 VTI 中不支持证书身份验证。

相关主题

环回接口的准则和限制

创建基于路由的站点间 VPN，第 1121 页

添加 VTI 接口

要配置基于路由的站点间 VPN，您必须在 VTI 隧道的两个节点上的设备上创建 VTI 接口。

过程

步骤 1 选择**设备 > 设备管理**。

步骤 2 点击要创建 VTI 接口的设备旁边的**编辑**图标。

步骤 3 选择**添加接口 (Add Interfaces) > 虚拟隧道接口 (Virtual Tunnel Interface)**。

步骤 4 输入接口的名称和说明。默认情况下，接口处于启用状态。

确保指定的名称不超过 28 个字符。

步骤 5 （可选）从**安全区域 (Security Zone)** 下拉列表中选择一个安全区域，以便以将静态 VTI 接口添加到该区域。

如果要在安全区域的基础上执行流量检查，请将 VTI 接口添加到安全区域并配置访问控制 (AC) 规则。要允许 VPN 流量通过隧道，您需要添加一条将此安全区域作为源区域的 AC 规则。

步骤 6 在**优先级 (Priority)** 字段中输入在多个 VTI 之间对流量进行负载均衡的优先级。

范围是从 0 到 65535。最小的数字具有最高优先级。此选项不适用于动态 VTI。

步骤 7 对于静态 VTI，请在**隧道 ID (Tunnel ID)** 字段中输入 0 到 10413 范围内的唯一隧道 ID。

步骤 8 从**隧道源 (Tunnel Source)** 下拉列表中选择隧道源接口。

VPN 隧道在此接口（物理接口）处终止。从下拉列表中选择接口的 IP 地址。无论 IPsec 隧道模式如何，您都可以选择 IP 地址。如果有多个 IPv6 地址，请选择要用作隧道终端的地址。

步骤 9 在 **IPSec 隧道模式 (IPSec Tunnel Mode)**下，点击 **IPv4** 或 **IPv6** 单选按钮以指定通过 IPsec 隧道的流量类型。

步骤 10 在 **IP 地址 (IP Address)** 字段中，输入要用于隧道终端的 IP 地址和子网。基于路由的 VPN 的两个终端的 VTI IP 地址必须都位于同一子网中。

注释 我们建议使用 169.254.x.x/16 范围内的 IP，不包括 威胁防御 保留范围 (169.254.1.x/24)。此外，请使用 /30 作为网络掩码，以便最好在 VTI 隧道的两端仅使用两个地址。例如，169.254.100.1/30。

步骤 11 点击**确定 (OK)**。

步骤 12 点击**保存 (Save)**。

如何通过备用 VTI 隧道路由流量

Cisco Secure Firewall Threat Defense 支持为基于路由的 (VTI) VPN 配置备份隧道。当主 VTI 无法路由流量时，VPN 中的流量会通过备用 VTI 传送。

您可以在以下场景中部署备份 VTI 隧道：

- 两个对等体都有服务提供商冗余备份。

  在这种情况下有两个物理接口，可充当对等体的两个 VTI 的隧道源。

- 只有一个对等体具有服务提供商冗余备份。

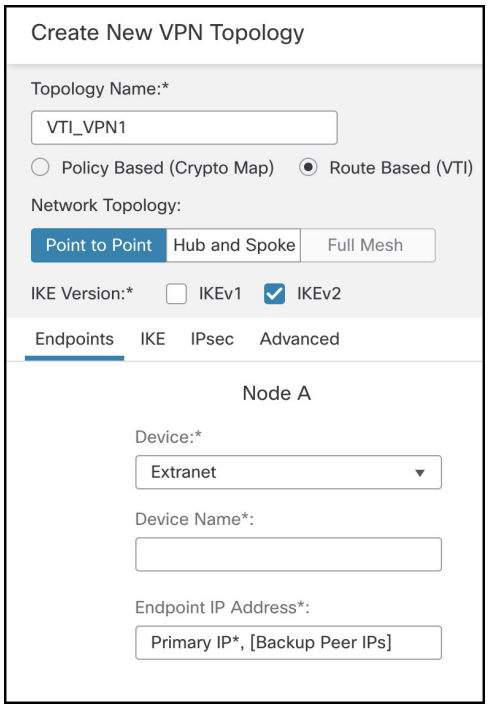
  在这种情况下，只有对等体的一端有一个接口备份，而另一端只有一个隧道源接口。

步骤	相应操作	更多信息
1	查看准则和限制。	Virtual Tunnel Interfaces 准则和限制，第 1117 页
2	创建 VTI 接口。	添加 VTI 接口，第 1119 页
3	在**创建新 VPN 拓扑向导 (Create New VPN Topology)** 的**添加终端 (Add Endpoint)** 对话框中，点击**添加备份 VTI (Add Backup VTI)**，为每个对等体配置相应的备份接口。	• 为点对点拓扑配置终端，第 1122 页 • 为中心辐射型拓扑配置终端，第 1124 页
4	配置路由策略。	• 依次选择 **设备 > 设备管理**，并且编辑威胁防御设备。 • 点击**路由**。
5	配置访问控制策略。	• 选择**策略 (Policies) > 访问控制 (Access Control)**。

配置备份 VTI 隧道的准则

- 对于外联网对等体，您可以在托管的对等体上指定备用接口的隧道源 IP 地址并配置隧道目标 IP。

您可以在**创建新的 VPN 拓扑 (Create New VPN Topology)** 向导的**终端 IP 地址 (Endpoint IP Address)** 字段中指定备份对等体 IP 地址。



- 在配置备份接口后，请为路由流量配置路由策略和访问控制策略。

  虽然主 VTI 和备用 VTI 始终可用，但流量只会通过路由策略中配置的隧道来传输。有关详细信息，请参阅VTI 的其他配置，第 1127 页。

创建基于路由的站点间 VPN

您可以在**点对点**拓扑网络的两个节点之间或在**中心辐射型**拓扑之间配置基于路由的站点间 VPN。对于点对点拓扑，要配置基于 VTI 的 VPN，隧道的两个节点都需要使用虚拟隧道接口。对于中心辐射型拓扑，您需要在具有静态或 VTI 的托管分支上配置虚拟隧道接口。

您可以将外联网设备配置为集线器，并将托管设备配置为分支。您可以配置多个中心和分支，也可以配置备份中心和分支。

- 对于外联网中心和分支，您可以将多个 IP 配置为备份。
- 对于托管分支，您可以配置备份静态 VTI 接口以及主 VTI 接口。

有关 VTI 的详细信息，请参阅关于 Virtual Tunnel Interface，第 1116 页。

过程

步骤 1 选择**设备 (Devices)** > **站点间 (Site To Site)**。

步骤 2 在**添加 VPN (Add VPN)** 下拉菜单中，选择 **Firepower 威胁防御设备 (Firepower Threat Defense Device)**。

步骤 3 选择**添加 (Add)**。

步骤 4 在 **拓扑名称 (Topology Name)** 字段中，输入 VPN 拓扑的名称。

步骤 5 选择**基于路由 (VTI) (Route Based [VTI])** 并执行以下操作之一：

- 选择**点对点 (Point to Point)** 作为网络拓扑。要为路由型**点对点**拓扑配置终端，请参阅为点对点拓扑配置终端，第 1122 页。
- 选择**中心辐射型 (Hub and Spoke)** 作为网络拓扑。要为路由型**中心辐射型**拓扑配置终端，请参阅为中心辐射型拓扑配置终端，第 1124 页。

步骤 6 （可选） 为部署指定 **IKE** 选项，如威胁防御 VPN IKE 选项，第 1109 页中所述。

步骤 7 （可选） 为部署指定 **IPsec** 选项，如威胁防御 VPN IPSec 选项，第 1111 页中所述。

步骤 8 （可选） 为部署指定**高级 (Advanced)** 选项，如威胁防御高级站点间 VPN 部署选项，第 1113 页中所述。

步骤 9 点击**保存 (Save)**。

下一步做什么

在两台设备上配置 VTI 接口和 VTI 隧道后，您必须配置：

- 用于通过 VTI 隧道在设备之间路由 VTI 流量的路由策略。有关详细信息，请参阅VTI 的其他配置，第 1127 页。
- 用于允许已加密的流量的访问控制规则。选择**策略 (Policies)** > **访问控制 (Access Control)**。

为点对点拓扑配置终端

配置以下参数，为**点对点**拓扑节点为路由型站点间 VPN 配置终端：

开始之前

在基于路由的 VPN 中配置点对点拓扑的基本参数，如 创建基于路由的站点间 VPN，第 1121 页 中所述，然后点击**终端 (Endpoints)** 选项卡。

过程

步骤 1 在**节点 A (Node A)** 下，从**设备 (Device)** 下拉菜单中选择要用作 VTI 隧道第一个终端的已注册设备 (威胁防御) 或外联网的名称。

对于外联网对等体，请指定以下参数：

1. 指定设备的名称。
2. 在**终端 IP 地址 (Endpoint IP address)**中输入主 IP 地址。如果配置备份 VTI，请添加一个逗号，然后指定备份 IP 地址。
3. 点击**确定 (OK)**。

为外联网集线器配置上述参数后，请在 **IKE** 选项卡中指定外联网的预共享密钥。

注释 AWS VPC 会将 **AES-GCM-NULL-SHA-LATEST** 作为默认策略。如果远程对等体连接到 AWS VPC，请从**策略 (Policy)** 下拉列表中选择 **AES-GCM-NULL-SHA-LATEST** 以建立 VPN 连接，而无需更改 AWS 中的默认值。

步骤 2 对于已注册的设备，您可以从**虚拟隧道接口 (Virtual Tunnel Interface)** 下拉列表中指定节点 A 的 VTI 接口。

所选隧道接口是节点 A 的源接口，并且它将成为节点 B 的隧道目的接口。

如果要在节点 A 上创建一个新接口，请点击 + 图标并配置字段，如添加 VTI 接口，第 1119 页中所述。

如果要编辑现有 VTI 的配置，请在**虚拟隧道接口 (Virtual Tunnel Interface)** 下拉字段中选择 VTI，然后点击**编辑 VTI (Edit VTI)**。

步骤 3 如果您的节点 A 设备位于 NAT 设备后面，请选中**隧道源 IP 为专用 (Tunnel Source IP is Private)** 复选框。在**隧道源公共 IP 地址 (Tunnel Source Public IP Address)** 字段中，输入隧道源公共 IP 地址。

步骤 4 **将本地身份发送到对等体 (Send Local Identity to Peers)** - 选择此选项可将本地身份信息发送到对等设备。从列表中选择以下**本地身份配置 (Local Identity Configuration)** 之一并配置本地身份：

- **IP 地址 (IP address)** - 对身份使用接口的 IP 地址。
- **自动 (Auto)** - 对预共享密钥使用 IP 地址并对基于证书的连接使用证书 DN。
- **电邮 ID (Email ID)**- 指定要用于身份的邮件 ID。电邮 ID 最多可以包含 127 个字符。
- **主机名 (Hostname)** - 使用完全限定主机名。
- **密钥 ID (Key ID)** - 指定用于身份的密钥 ID。密钥 ID 必须少于 65 个字符。

本地身份用于为每个 IKEv2 隧道配置唯一身份，而不是为所有隧道配置一个全局身份。唯一身份允许 威胁防御 在 NAT 后面有多个 IPsec 隧道，以便连接到思科 Umbrella 安全互联网网关 (SIG)。

有关在 Umbrella 上配置唯一隧道 ID 的信息，请参阅《**Cisco Umbrella SIG 用户指南**》。

步骤 5 （可选）点击**添加备份 VTI (Add Backup VTI)** 以指定其他 VTI 接口作为备份接口。

注释 确保两个拓扑对等体的备份 VTI 具有不同的隧道源。一台设备不能有两个具有相同隧道源和隧道目标的 VTI；因此，请配置唯一的隧道源和隧道目标组合。

虽然虚拟隧道接口是在备用 VTI 下指定的，但路由配置决定了哪个隧道会被用作主隧道或备用隧道。

步骤 6 在**连接类型 (Connection Type)** 下拉菜单中，选择**仅应答 (Answer Only)** 或**双向 (Bidirectional)**。如果已将 IKE 协议版本选择为 IKEv1，则其中一个节点必须为 **仅应答 (Answer Only)**。

仅应答 (Answer Only)：设备只能在对等设备发起连接时做出响应，不能发起任何连接。

双向 (Bidirectional)：设备可以发起或响应连接。这是默认选项。

步骤 7 在**其他配置 (Additional Configuration)** 下，执行以下操作：

- 要将流量路由到 VTI，请点击**路由策略 (Routing Policy)**。管理中心 会显示**设备 (Devices)** > **路由 (Routing)** 页面。

  您可以为 VPN 流量配置静态或 BGP 路由。

- 要允许 VPN 流量，请点击 **AC 策略 (AC Policy)**。管理中心 会显示设备的访问控制策略页面。继续添加用于指定 VTI 安全区域的允许/阻止规则。配置备份 VTI 时，请确保包含与主 VTI 相同的安全区域的备份隧道。AC 策略页面中的备份 VTI 不需要特定的设置。

步骤 8 对节点 B 重复上述程序。

步骤 9 点击**确定 (OK)**。

下一步做什么

- （可选）为部署指定 **IKE** 选项，如威胁防御 VPN IKE 选项，第 1109 页中所述。
- （可选）为部署指定 **IPsec** 选项，如威胁防御 VPN IPSec 选项，第 1111 页中所述。
- （可选）为部署指定 **高级 (Advanced)** 选项，如威胁防御高级站点间 VPN 部署选项，第 1113 页中所述。
- 点击**保存 (Save)**。
- 要将流量路由到 VTI，请选择 **设备 (Devices) > 设备管理 (Device Management)**，编辑威胁防御设备，然后点击**路由 (Routing)** 选项卡。

  您可以为 VPN 流量配置静态，或者使用 BGP 来路由 VPN 流量。

- 要允许 VPN 流量，请选择**策略 (Policies) > 访问控制 (Access Control)**。。添加用于指定 VTI 安全区域的规则。对于备份 VTI，请确保包含与主 VTI 相同的安全区域的备份 VTI。

为中心辐射型拓扑配置终端

配置以下参数，为 **中心辐射型** 拓扑节点配置路由型站点间 VPN 终端：

开始之前

在路由型 VPN 中配置中心辐射型拓扑的基本参数，如创建基于路由的站点间 VPN，第 1121 页中所述，然后点击**终端 (Endpoints)** 选项卡。

过程

步骤 1 添加集线器节点：

a) 在**中心节点 (Hub Nodes)** 下，点击**添加 (+) (Add [+])**。
b) 在**设备名称 (Device Name)** 字段中输入设备名称。
c) 在**终端 IP 地址 (Endpoint IP address)**中，输入主 IP 地址。如果要配置备份中心，请输入一个逗号，然后指定备份 IP 地址。
d) 点击 **IKE** 选项卡并指定外联网上提供的预共享密钥。
e) 点击**确定 (OK)**。

添加分支节点：

- 对于外联网分支，配置参数与集线器类似。
- 对于托管分支节点，请配置类似于点对点节点的参数。

a) 在**分支节点 (Spoke Nodes)** 下，点击**添加 (+) (Add [+])**。
b) 在**设备 (Device)** 下拉菜单中，选择已注册设备的名称 (威胁防御).
c) 指定接口设置：
   - 在**静态虚拟隧道接口 (Static Virtual Tunnel Interface)** 下拉菜单中，选择您在已选为 VTI 终端的 威胁防御 设备上创建的 VTI 接口。
   - 如果要创建新接口，请点击 + 图标并填写相关字段，如添加 VTI 接口，第 1119 页中所述。
   - 如果要编辑现有 VTI 的配置，请在**静态虚拟隧道接口 (Static Virtual Tunnel Interface)** 下拉字段中选择 VTI，然后点击**编辑 VTI (Edit VTI)**。

步骤 2 如果您的终端设备位于 NAT 设备后面，请选中**隧道源 IP 为专用 (Tunnel Source IP is Private)** 复选框。在**隧道源公共 IP 地址 (Tunnel Source Public IP Address)** 字段中，输入隧道源公共 IP 地址。

步骤 3 **将本地身份发送到对等体 (Send Local Identity to Peers)** - 选择此选项可将本地身份信息发送到对等设备。从列表中选择以下**本地身份配置 (Local Identity Configuration)** 之一并配置本地身份：

- **IP 地址 (IP address)** - 对身份使用接口的 IP 地址。
- **自动 (Auto)** - 对预共享密钥使用 IP 地址并对基于证书的连接使用证书 DN。
- **电邮 ID (Email ID)**- 指定要用于身份的邮件 ID。电邮 ID 最多可以包含 127 个字符。
- **主机名 (Hostname)** - 使用完全限定主机名。
- **密钥 ID (Key ID)** - 指定用于身份的密钥 ID。密钥 ID 必须少于 65 个字符。

本地身份用于为每个 IKEv2 隧道配置唯一身份，而不是为所有隧道配置一个全局身份。唯一身份允许 威胁防御 在 NAT 后面有多个 IPsec 隧道，以便连接到 Cisco Umbrella 安全互联网网关 (SIG)。

有关在 Umbrella 上配置唯一隧道 ID 的信息，请参阅 **Cisco Umbrella SIG 用户指南**。

步骤 4 （可选）点击**添加备份 VTI (Add Backup VTI)** 以指定其他 VTI 作为备份接口。

注释 确保两个拓扑对等体均未在同一隧道源上配置备份 VTI。例如，如果对等体 A 的两个 VTI（主和备份）配置了一个隧道源接口，例如 10.10.10.1/30，则对等体 B 的 2 个 VTI 也不能使用一个隧道源 IP，例如 20.20 .20.1/30。

注释 虽然虚拟隧道接口是在备用 VTI 下指定的，但路由配置决定了哪个隧道会被用作主隧道或备用隧道。

可以执行以下操作：

- 要创建新的备份接口，请使用 + 图标。
- 要编辑现有备份 VTI 的配置，请使用**编辑 VTI (Edit VTI)**。

注释 如果设备位于 NAT 设备后面，请选中**隧道源 IP 为专用 (Tunnel Source IP is Private)** 复选框。在**隧道源公共 IP 地址 (Tunnel Source Public IP Address)** 字段中，输入隧道源公共 IP 地址。

步骤 5 展开**高级设置 (Advance Settings)** 并在**连接类型 (Connection Type)** 下拉菜单中选择**仅应答 (Answer Only)** 或**双向 (Bidirectional)**。如果已将 IKE 协议版本选择为 IKEv1，则其中一个节点必须为**仅应答 (Answer Only)**。

步骤 6 对于外联网分支，请指定以下参数：

1. 在**设备名称 (Device Name)** 字段中输入设备名称。
2. 在**终端 IP 地址 (Endpoint IP address)**中，输入主 IP 地址。如果要配置备份 VTI，请输入一个逗号，然后指定备份 IP 地址。
3. 点击 **IKE** 选项卡并指定外联网上提供的预共享密钥。

   注释 AWS VPC 会将 **AES-SHA-SHA-LATEST** 作为默认策略。因此，如果远程对等体连接到 AWS VPC，请从**策略 (Policy)** 下拉列表中选择 **AES-SHA-SHA-LATEST** 以建立 VPN 连接，而无需更改 AWS 中的默认值。

步骤 7 重复上述程序以配置其他分支节点。

步骤 8 点击**确定 (OK)**。

下一步做什么

- （可选）为部署指定 **IKE** 选项，如威胁防御 VPN IKE 选项，第 1109 页中所述。
- （可选）为部署指定 **IPsec** 选项，如威胁防御 VPN IPSec 选项，第 1111 页中所述。
- （可选）为部署指定 **高级 (Advanced)** 选项，如威胁防御高级站点间 VPN 部署选项，第 1113 页中所述。
- 点击**保存 (Save)**。

VTI 的其他配置

在两台设备上配置 VTI 接口和 VTI 隧道后，您必须配置路由策略以通过 VTI 隧道在设备之间路由 VTI 流量。您还必须配置访问控制规则以允许已加密的流量。

VTI 的路由配置

Static Route

在两台设备（两端）上配置静态路由，以便通过 VTI 隧道路由设备之间的流量。

当为VPN配置了备用隧道，请配置具有不同指标的静态路由，以便处理通过备用隧道的流量的故障转移。

在配置静态路由时，请确保配置以下选项：

- **接口 (Interface)** - 选择 VPN 中使用的 VTI 接口。如果是备份隧道，请选择 VPN 中使用的备份 VTI 接口。
- **所选网络 (Selected Network)** - 选择远程对等体的受保护网络（已作为网络对象添加）。
- **网关 (Gateway)** - 选择远程对等体的隧道接口 IP 地址作为网关。对于备用隧道，请选择远程对等体的备用隧道接口 IP 地址作为网关。

有关静态路由的详细信息，请参阅添加静态路由 ， 第 794 页。

边界网关协议 (BGP)

在两台设备上配置 BGP，以便使用以下设置共享路由信息并通过隧道在设备之间路由流量：

1. 在**常规设置 (General Settings)** > **BGP** 下启用 BGP，提供本地设备的 AS 编号，并添加路由器 ID（如果您选择手动）。
2. 在 **BGP** 下，启用 IPv4/IPv6 并在**邻居 (Neighbor)** 选项卡上配置邻居。
   - **IP 地址 (IP Address)** - 将远程对等体的 VTI 接口 IP 地址指定为邻居的 IP 地址。如果为 VPN 配置了备用隧道，则还要添加具有远程对等体的备用 VTI 接口 IP 地址的邻居。
   - **远程 AS (Remote AS)** - 指定远程对等体的 AS 编号。
3. 在**重新分发 (Redistribution)** 选项卡上，将源协议选择为“已连接”(Connected)，以便启用连接的路由重新分发。

有关 BGF 配置的详细信息，请参阅配置 BGP ， 第 903 页。

AC 策略规则

将访问控制规则添加到设备上的访问控制策略，以便允许使用以下设置在 VTI 隧道之间加密流量：

1. 通过“允许”操作来创建规则。
2. 选择本地设备的VTI安全区域作为源区域，然后选择远程对等体的VTI安全区域作为目标区域。

3. 选择远程对等体的VTI安全区域作为源区域，然后选择本地设备的VTI安全区域作为目标区域。

有关配置访问控制规则的详细信息，请参阅创建和编辑访问控制规则，第 1288 页。

注释 配置备份 VTI 时，请确保包含与主 VTI 相同的安全区域的备份隧道。AC 策略页面中的备份 VTI 不需要特定的设置。

监控站点间 VPN

Cisco Secure Firewall Management Center 提供站点间 VPN 隧道的快照以便确定站点间 VPN 隧道的状态。您可以查看对等设备之间的隧道列表以及每个隧道的状态：活动、非活动或无活动数据。您可以根据拓扑结构、设备和状态来过滤表中的数据。监控控制面板中的表格会显示实时数据，您可以配置为按指定的时间间隔来刷新数据。该表显示了基于加密映射的VPN的点对点、中心辐射型以及全网状拓扑。隧道信息还包含路由型 VPN 或虚拟隧道接口 (VTI) 的数据。

您可以使用此数据：

- 确定有问题的 VPN 隧道并进行故障排除。
- 验证站点间 VPN 对等设备之间的连接。
- 监控 VPN 隧道的运行状况，以便在站点间提供不间断的 VPN 连接。

有关配置基于加密映射的站点间 VPN 的信息，请参阅配置策略型站点间 VPN，第 1104 页。

有关 VTI 的信息，请参阅关于 Virtual Tunnel Interface，第 1116 页。

有关 威胁防御 VPN 监控和故障排除的信息，请参阅VPN 监控和故障排除。

准则和限制

- 该表会显示已部署的站点间VPN 的列表。它不会显示已创建但未部署的隧道。
- 该表不会显示有关基于策略的 VPN 和备份 VTI 的备份隧道的信息。
- 对于集群部署，该表不会显示实时数据中的导向器更改。它只会显示部署VPN时存在的导向器信息。只有在更改后重新部署了隧道 AM，导向器更改才会在表中体现出来。

站点间 VPN 监控控制面板

站点间 VPN 监控控制面板显示站点间 VPN 隧道的以下构件：

- **隧道状态表 (Tunnel Status Table)** - 列出使用 管理中心 配置的站点间 VPN 的表
- **隧道状态分布图 (Tunnel Status Distribution Chart)** - 以环状图来显示隧道的聚合状态。
- **拓扑摘要列表 (Topology Summary Listing)** - 按拓扑来汇总的隧道状态。

VPN 隧道的状态

站点间监控控制面板会列出以下状态的 VPN 隧道：

- **非活动 (Inactive)** - 如果所有 IPSec 隧道都关闭，则策略型（基于加密映射）的 VPN 隧道将处于非活动状态。如果 VTI 或 隧道遇到任何配置或连接问题，则该隧道将关闭。
- **活动 (Active)** - 在 管理中心 中，站点间 VPN 是根据分配给 VPN 拓扑的 IKE 策略和 IPsec 建议来配置的。如果 管理中心 在部署后通过隧道识别出需要关注的流量，则策略型 VPN 隧道将处于活动状态。只有当至少有一个 IPsec 隧道正常运行时，IKE 隧道才会正常运行。

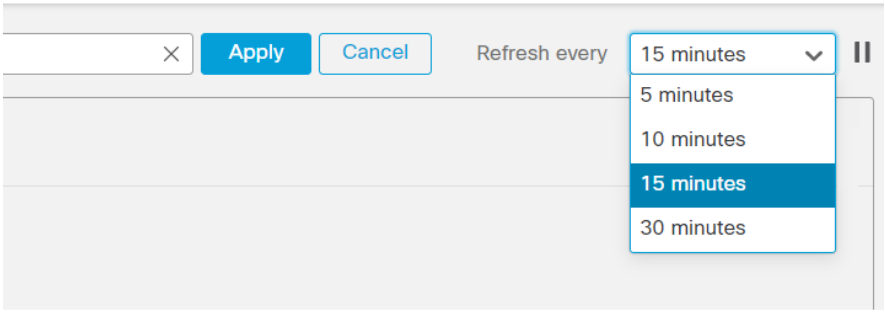
  路由型 VPN (VTI) 隧道不需要所关注的流量处于活动状态。如果它们的配置和部署没有错误，则它们将处于活动状态。
- **无活动数据 (No Active Data)** - 策略型 VPN 隧道会保持“无活动数据”(No Active Data) 状态，直到第一次有流量事件通过隧道。“无活动数据”(No Active Data) 状态还会列出已部署但出错的策略型和路由型 VPN。

自动数据刷新

表中的站点间 VPN 数据会定期刷新。您可以配置为以特定间隔刷新 VPN 监控数据，或者关闭自动数据刷新。

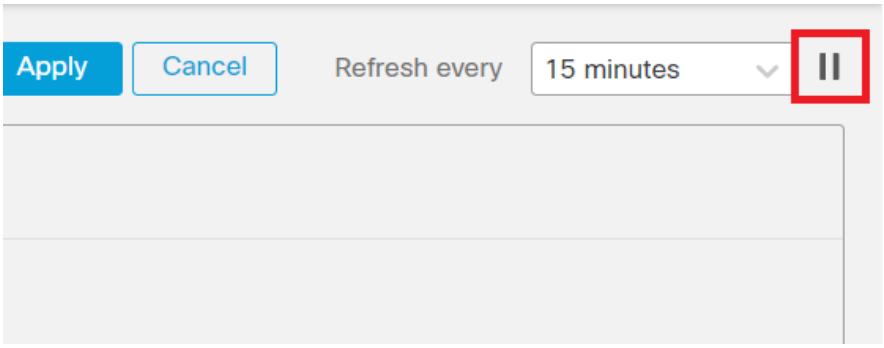
点击**刷新 (Refresh)** 间隔下拉列表，从可用的间隔时间中选择以刷新表中的数据。

图 *136:* 刷新隧道数据



点击**暂停 (Pause)** 可根据需要停止自动数据刷新。您可以点击同一按钮继续刷新隧道数据。

图 *137:* 暂停定期数据刷新



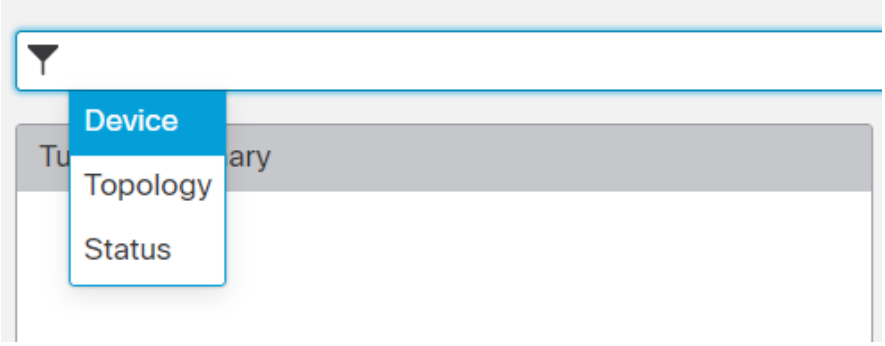
对站点间 VPN 监控数据进行过滤和排序

您可以按拓扑、设备和状态来过滤和查看 VPN 监控表中的数据。

例如，您可以查看特定拓扑中处于关闭状态的隧道。

在过滤器框中点击选择过滤条件，然后指定要过滤的值。

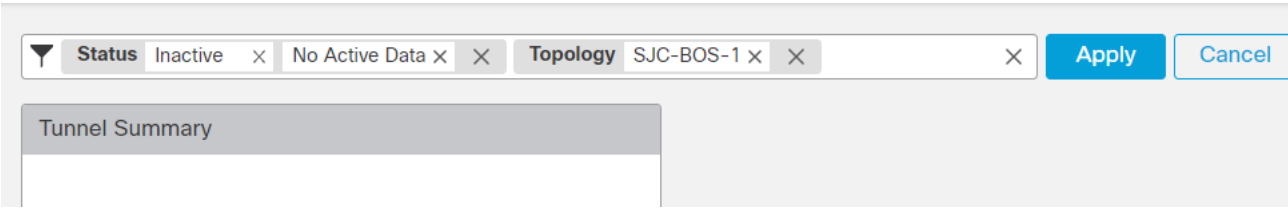
图 *138:* 过滤隧道数据



您可以根据需要使用多个过滤条件来查看数据。

例如，您可以选择只查看处于“开启”(Up) 和“关闭”(Down) 状态的隧道，并忽略处于“未知”(Unknown) 状态的隧道。

图 *139:* 示例：过滤隧道数据



排序数据 (Sort the data) - 要按列对数据进行排序，请点击列标题。

相关主题

关于站点间 VPN，第 1101 页
关于 Virtual Tunnel Interface，第 1116 页

第 46 章

远程访问 VPN

远程访问虚拟专用网络 (VPN) 允许个人用户使用连接到互联网的计算机或其他受支持的设备，从远程位置连接到您的网络。这样，移动员工就可以从家庭网络或公共 Wi-Fi 网络进行连接。

以下主题介绍如何为您的网络配置远程访问 VPN。

Cisco Secure Firewall Threat Defense 远程接入 VPN 概述

Cisco Secure Firewall Threat Defense 提供安全的网关功能，支持远程接入 SSL 和 IPsec-IKEv2 VPN。全隧道客户端， AnyConnect 安全移动客户端，可通过 SSL 和 IPsec-IKEv2 安全地连接远程用户的安全网关。客户端与 威胁防御 设备协商 SSL VPN 连接时，会使用传输层安全 (TLS) 或数据报传输层安全 (DTLS) 进行连接

AnyConnect 是终端设备上通过远程 VPN 连接 威胁防御 设备的唯一受支持客户端。该客户端为远程用户提供了 SSL 或 IPsec-IKEv2 VPN 客户端，而无需网络管理员在远程计算机上安装和配置客户端。连接后，即可从安全网关中部署适用于 Windows、Mac 和 Linux 的 AnyConnect 安全移动客户端。从平台应用程序商店可安装适用于 Apple iOS 和 Android 设备的 AnyConnect 应用程序。

使用 管理中心 中的远程访问 VPN 策略向导可快速而轻松地设置 SSL 和 IPsec-IKEv2 远程访问 VPN 的基本功能。然后，根据需要增强策略配置并将其部署到您的 Cisco Secure Firewall Threat Defense 安全网关设备。

远程接入 VPN 功能

下表介绍了 Cisco Secure Firewall Threat Defense 远程访问 VPN 的功能：

表 *83:* 远程访问 *VPN* 功能

	说明
Cisco Secure Firewall Threat Defense 远程访问 VPN 功能	• 使用 AnyConnect 安全移动客户端 的 SSL 和 IPsec-IKEv2 远程访问。 • Cisco Secure Firewall Management Center 支持所有组合，如 IPv4 隧道上的 IPv6。 • 对 管理中心 和 设备管理器的配置支持。特定于设备的覆盖。 • 支持 Cisco Secure Firewall Management Center 和 威胁防御 HA 环境。 • 支持多个接口和多个 AAA 服务器。 • 使用 RADIUS CoA 或 RADIUS 动态授权提供快速遏制威胁支持。 • 支持 Cisco AnyConnect 安全移动客户端 版本 4.7 或更高版本的 DTLS v1.2 协议。 • AnyConnect 客户端 客户端模块支持远程访问 VPN 连接的其他安全服务。 • VPN 负载均衡。

	说明
AAA 功能	• 使用自签名或 CA 签名的身份证书的服务器身份验证。 • 使用 RADIUS 或 LDAP 或 AD 的基于 AAA 用户名和密码的远程身份验证。 • RADIUS 组和用户授权属性，以及 RADIUS 记帐。 • 提供使用其他 AAA 服务器进行辅助身份验证的双重身份验证支持。 • 使用 VPN 身份的 NGFW 访问控制集成。 • 使用 Cisco Secure Firewall Management Center Web 界面的 LDAP 或 AD 授权属性。 • 支持使用 SAML 2.0 的单一登录。 • 支持使用 Microsoft Azure 的多个身份提供程序信任点，这些信任点可以具有相同实体ID的多个应用，但具有唯一身份证书。
VPN 隧道功能	• 地址分配。 • 分割隧道 • 分割 DNS。 • 客户端防火墙 ACL。 • 最大连接和空闲时间的会话超时。
远程访问 VPN 监控功能	• 新的VPN控制面板构件，按持续时间、客户端应用等各个特性显示 VPN 用户。 • 远程访问VPN事件，包括身份验证信息，如用户名和 OS 平台。 • 使用 威胁防御统一 CLI 提供的隧道统计信息。

AnyConnect 组件

AnyConnect 安全移动客户端 部署

远程接入 VPN 策略可包括 AnyConnect 客户端映像 和 AnyConnect 客户端配置文件 ，以便分发到连接终端。您也可以使用其他方法分发客户端软件。请参阅相应版本的《思科 AnyConnect 安全移动客户端管理员指南》中的部署 *AnyConnect* 一章。

在先前未安装客户端的情况下，远程用户可以在他们的浏览器中输入配置为接受 SSL 或 IPsec-IKEv2 VPN 连接的接口的 IP 地址。除非安全设备被配置为将 http:// 请求重定向到 https://，否则远程用户必须以 https://地址形式输入 URL。在用户输入 URL 后，浏览器将连接该接口并显示登录屏幕。

在用户登录后，如果安全网关将用户识别为需要 VPN 客户端，则会下载与远程计算机的操作系统匹配的客户端。下载后，客户端会自行安装和配置、建立安全连接并在连接停止后自行保留或卸载（取决于安全设备配置）。如果是以前安装的客户端，登录后 威胁防御 安全网关会检查客户端版本，并根据需要进行升级。

AnyConnect 安全移动客户端 操作

当客户端与安全设备协商连接时，客户端将使用传输层安全 (TLS) 以及（可选）或数据报传输层安全 (DTLS) 协议进行连接。DTLS 可避免与某些 SSL 连接关联的延迟和带宽问题，并可提高对于数据包延迟敏感的实时应用的性能。

当 IPsec-IKEv2 VPN 客户端发起到安全网关的连接时，协商包括通过互联网密钥交换 (IKE) 验证设备，然后使用 IKE 扩展身份验证 (Xauth) 进行用户验证。系统会将群组配置文件推送到 VPN 客户端，并创建 IPsec 安全关联 (SA) 来完成 VPN。

AnyConnect 客户端配置文件 和编辑器

AnyConnect 客户端配置文件 是一组以 XML 文件形式存储的配置参数，VPN 客户端使用该文件来配置客户端的操作和外观。这些参数（XML 标记）包括主机名称和地址以及设置，用于启用更多客户端功能。

您可以使用 AnyConnect 配置文件编辑器配置配置文件。此编辑器是一款方便的基于 GUI 的配置工具，作为 AnyConnect 软件包的一部分提供。该程序可独立于 管理中心 而运行。

远程访问 VPN 身份验证

远程接入 VPN 服务器身份验证

Cisco Secure Firewall Threat Defense 安全网关通常使用证书来识别和验证自己到 VPN 客户端终端的连接。

当使用远程访问 VPN 策略向导时，您可以在目标 威胁防御 设备上注册选定的证书。在向导中的**访问和证书**阶段，选择“在目标设备上注册所选的证书对象”选项。证书注册过程将在指定设备上自动执行。完成远程访问 VPN 策略配置时，您可以在设备证书主页下查看已注册证书的状态。该状态清晰指明了证书注册是否成功。您的远程访问 VPN 策略配置现已完成，可以进行部署。

有关如何获得安全网关证书（也称为 PKI 注册）的信息，请参阅 证书，第 1077 页。此章详细说明了如何配置、注册和维护网关证书。

远程接入 VPN 客户端 AAA

对于 SSL 和 IPsec-IKEv2，可只使用用户名和密码、只使用证书或同时使用这两种方法对远程用户进行身份验证。

注释 如果您的部署中正在使用客户端证书，则必须将它们添加到独立于 Cisco Secure Firewall Threat Defense 或 Cisco Secure Firewall Management Center的客户端平台中。不提供 SCEP 或 CA 服务等设施来为客户端填充证书。

AAA 服务器支持使用受管设备作为安全网关来确定用户身份（身份验证）、允许用户执行的操作（授权）以及用户执行的操作（记帐）。AAA 服务器的一些示例有 RADIUS、LDAP/AD、TACACS+ 和 Kerberos.。对于 威胁防御设备上的远程接入 VPN，支持使用 AD、LDAP 和 RADIUS AAA 服务器进行身份验证。

请参阅 了解权限和属性的策略实施 部分以了解更多有关远程接入 VPN 授权的信息。

在添加或编辑远程访问 VPN 策略之前，必须配置要指定的领域和 RADIUS 服务器组。有关详细信息，请参阅创建 Active Directory 领域和领域目录，第 1816 页和添加 RADIUS 服务器组，第 970 页。

如果没有配置 DNS，设备将无法解析 AAA 服务器名称、命名的 URL 和具有 FQDN 或主机名的 CA 服务器，只能解析 IP 地址。

远程用户提供的登录信息由 LDAP 或 AD 领域或 RADIUS 服务器组进行验证。这些实体与 Cisco Secure Firewall Threat Defense 安全网关相集成。

注释 如果用户使用 Active Directory 作为身份验证源通过远程访问 VPN 进行身份验证，则用户必须使用其用户名登录；`domain\username` 或 `username@domain` 格式无效。（Active Directory 将此用户名视为 *logon* 名称，有时也视为 `sAMAccountName`。）有关详细信息，请参阅 MSDN 上的用户命名属性。

如果使用 Radius 进行身份验证，用户可以使用上述任何一种格式登录。

通过 VPN 连接进行身份验证后，远程用户将接受 *VPN* 身份。Cisco Secure Firewall Threat Defense安全网关上的身份策略将使用此 VPN 身份来识别和过滤属于此远程用户的网络流量。

身份策略与访问控制策略相关联，后者用于确定哪些人有权访问网络资源。使用访问控制策略可阻止或允许远程用户访问您的网络资源。

有关详细信息，请参阅 关于身份策略，第 1885 页 和 访问控制策略，第 1259 页 节：

相关主题

配置远程访问 VPN 的 AAA 设置，第 1151 页

了解权限和属性的策略实施

Cisco Secure Firewall Threat Defense设备支持将用户授权属性（也称为用户权利或权限）应用于来自外部身份验证服务器和/或授权 AAA 服务器 (RADIUS) 或 威胁防御设备上的组策略的 VPN 连接。如果 威胁防御设备从与组策略上配置的属性冲突的外部 AAA 服务器接收属性，则来自 AAA 服务器的属性始终优先。

威胁防御设备按照以下顺序应用属性：

1. **外部 AAA 服务器上的用户属性** - 该服务器在用户身份验证和/或授权成功后返回这些属性。
2. **在 Firepower 威胁防御设备上配置的组策略** - 如果 RADIUS 服务器为用户返回 RADIUS Class 属性 IETF-Class-25 (OU=group-policy) 值， 威胁防御 设备会将该用户放在名称相同的组策略中，并实施组策略中该服务器未返回的所有属性。
3. **连接配置文件 (也称为隧道组) 分配的组策略** - 连接配置文件具有该连接的初步设置，包括在进行身份验证前应用于用户的默认组策略。

注释 威胁防御设备不支持从默认组策略 *DfltGrpPolicy* 继承系统默认属性。如果分配给连接配置文件的组策略上的属性没有被用户属性或来自 AAA 服务器的上述组策略所覆盖，则这些属性将用于用户会话。

相关主题

配置远程访问 VPN 的 AAA 设置 ，第 1151 页

了解 AAA 服务器连接

必须能够从 威胁防御 设备访问 LDAP、AD 和 RADIUS AAA 服务器以实现预期目的：仅用户身份处理、仅 VPN 身份验证或这两种活动。AAA 服务器在远程接入 VPN 中被用于以下活动：

- **用户身份处理 (User-identity handling)** - 必须能够通过管理接口访问服务器。

  在 威胁防御 设备上管理接口具有区别于VPN 所使用常规接口的单独路由过程和配置。

- **VPN 身份验证 (VPN authentication)** - 必须能够通过一个常规接口：诊断接口或数据接口来访问服务器。

  对于常规接口，可使用两个路由表。用于诊断接口以及为仅管理而配置的任何其他接口的仅管理路由表，以及用于数据接口的数据路由表。完成路由查找后，首先检查仅管理路由表，然后检查数据路由表。第一个匹配项被选中以连接 AAA 服务器。

注释 如果将 AAA 服务器放在数据接口上，请确保仅管理路由策略与传送至数据接口的流量不匹配。例如，如果存在通过诊断接口的默认路由，流量将永远不会退回到数据路由表。使用 **show route management-only** 和 **show route** 命令验证路由确定。

对于相同AAA服务器上的两种活动，除了使服务器可通过处理用户身份的管理接口访问之外，还要执行下列操作之一，以便为相同的 AAA 服务器提供 VPN 身份验证权限：

- 启用和配置 IP 地址与管理接口位于相同子网的诊断接口，然后配置通过此接口到 AAA 服务器的路由。诊断接口访问将用于 VPN 活动，管理接口访问用于身份处理。

注释 以这种方式配置时，不能将数据接口放在与诊断和管理接口相同的子网中。如果您希望管理接口和数据接口位于同一网络上（例如，当将设备本身用作网关时），将无法使用此解决方案，因为诊断接口必须保持禁用状态。

- 配置通过数据接口到 AAA 服务器的路由。数据接口访问将用于 VPN 活动，管理接口访问用于用户身份处理。

有关不同接口的详细信息，请参阅常规防火墙接口 ， 第 517 页。

部署后，请使用以下 CLI 命令从 威胁防御设备监视和故障排除 AAA 服务器连接：

- **show aaa-server** 显示 AAA 服务器统计信息。
- **show route management-only** 查看仅管理路由表项。
- **show network** 并且 **show network-static-routes** 或者查看管理接口默认路由和静态路由。
- **show route** 查看数据流量路由表项。
- **ping system** 和 **traceroute system** 以验证通过管理接口到 AAA 服务器的路径。
- **ping interface** *ifname* 和 **traceroute** *destination* 验证通过诊断和数据接口到 AAA 服务器的路径。
- **test aaa-server authentication** 和 **test aaa-server authorization** 测试 AAA 服务器上的身份验证和授权。
- **clear aaa-server statistics** *groupname* 或 **clear aaa-server statistics protocol** *protocol* 按组或协议清除 AAA 服务器统计信息。
- **aaa-server** *groupname* **active host** *hostname* 激活发生故障的 AAA 服务器；或 **aaa-server** *groupname* **fail host** *hostname* 使 AAA 服务器发生故障。
- **debug ldap level**、**debug aaa authentication**、 **debug aaa authorization** 和 **debug aaa accounting**。

远程接入 VPN 的许可证要求

威胁防御 许可证

威胁防御 FTD 远程访问 VPN 需要 强加密 和以下 AnyConnect许可证之一：

- AnyConnect Plus
- AnyConnect Apex
- 仅限 AnyConnect VPN

远程接入 VPN 的要求和必备条件

型号支持

威胁防御

支持的域

任意

用户角色

管理员

远程接入 VPN 的准则和限制

远程接入 VPN 策略配置

- 您仅可通过使用向导来添加新的远程访问 VPN 策略。您必须完成整个向导才能创建新的策略；如果在完成向导之前取消，则不会保存任何策略。
- 两个用户必须 不 同时编辑远程访问 VPN 策略，但 Web 界面不会阻止同时编辑。如果发生这种情况，保留最后保存的配置。
- 如果为 Cisco Secure Firewall Threat Defense 设备分配了远程访问 VPN 策略，则无法将该设备从一个域移至另一个域。
- 在集群模式下的 Firepower 9300 和 4100 系列不支持远程访问 VPN 配置。
- 如果存在配置错误的 威胁防御 NAT 规则，远程接入 VPN 连接可能会失败。
- 只要使用的是 IKE 端口 500/4500 或 SSL 端口 443 或有一些 PAT 转换处于活动状态，则无法在同一端口上配置 AnyConnect IPSec-IKEv2 或 SSL 远程访问 VPN，因为无法在这些端口上启动服务。配置远程访问 VPN 之前，不得在 威胁防御 设备上使用这些端口。
- 在使用向导配置远程访问 VPN 时，可以创建内联证书注册对象，但不能使用它们安装身份证书。证书注册对象用于在被配置为远程访问 VPN 网关的 威胁防御设备上生成身份证书。在将远程访问 VPN 配置部署到该设备之前，在该设备上安装身份证书。

  有关如何根据证书注册对象安装身份证书的更多信息，请参阅对象管理器 ，第 960 页。
- ECMP 区域接口可在启用 IPsec 的远程访问 VPN 中使用。

- ECMP 区域接口不能在启用 SSL 的远程访问 VPN 中使用。如果属于安全区域或接口组的所有远程访问 VPN 接口也属于一个或多个 ECMP 区域，则部署远程访问 VPN（启用 SSL）配置会失败。但是，如果只有属于安全区域或接口组的一些远程访问 VPN 接口也属于一个或多个 ECMP 区域，则远程访问 VPN 配置的部署会成功排除这些接口。
- 更改远程访问 VPN 策略配置后，请重新部署对 威胁防御 设备的更改。部署配置更改所需的时间取决于多个因素，例如策略和规则的复杂性，发送到设备的配置的类型和数量以及内存和设备型号。在部署远程访问 VPN 策略更改之前，请查看 部署配置更改的最佳实践，第 128 页。

并发 VPN 会话容量规划（threat defense virtual 型号）

最大并发 VPN 会话数由 threat defense virtual 安装的智能许可授权层管理，并通过速率限制器实施。根据已许可的设备型号，设备上允许的并发远程访问 VPN 会话数量有最大值限制。此限制用于确保系统性能不会降低到不可接受的水平。请使用这些限制进行容量规划。

设备型号	最大并发远程接入 VPN 会话数
Threat Defense Virtual5	50
Threat Defense Virtual10	250
Threat Defense Virtual20	250
Threat Defense Virtual30	250
Threat Defense Virtual50	750
Threat Defense Virtual100	10,000

并发 VPN 会话容量规划 （硬件型号）

最大并发 VPN 会话数受特定于平台的限制约束，而与许可证无关。根据设备型号，设备上允许的并发远程接入 VPN 会话数量有最大值限制。此限制用于确保系统性能不会降低到不可接受的水平。请使用这些限制进行容量规划。

设备型号	最大并发远程接入 VPN 会话数
Firepower 2110	1500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10000

有关其他硬件型号的容量，请联系您的销售代表。

注释 一旦达到每个平台的最大会话限制，威胁防御设备就会拒绝VPN连接。连接通过系统日志消息来拒绝。请参阅系统日志消息指南中的系统日志消息 %ASA-4-113029 和 %ASA-4-113038。有关详细信息，请参阅 Cisco Secure Firewall ASA 系列系统日志消息。

控制 VPN 的密码使用

为防止使用大于 DES 的密码，在 管理中心中的下列位置提供了预部署检查：

设备 (Devices) > **平台设置 (Platform Settings)** > **编辑 (Edit)** > **SSL**。

设备 (Devices) > **VPN** > **远程访问 (Remote Access)** > **编辑 (Edit)** > **高级 (Advanced)** > **IPsec**。

有关 SSL 设置和 IPsec 的详细信息，请参阅 配置 SSL 设置 ， 第 627 页 和 配置远程访问 VPN IPsec/IKEv2 参数 ， 第 1182 页。

身份验证、授权和记帐

在拓扑中的每台设备上配置 DNS，以便使用远程访问 VPN。如果没有 DNS，设备将无法解析 AAA 服务器名称、命名的 URL 和具有 FQDN 或主机名的 CA 服务器；只能解析 IP 地址。

您可以使用**平台设置 (Platform Settings)** 来配置 DNS。有关详细信息，请参阅配置 DNS ， 第 617 页和DNS 服务器组 ， 第 985 页。

客户端证书

如果您的部署中正在使用客户端证书，则必须将它们添加到独立于Cisco Secure Firewall Threat Defense或 Cisco Secure Firewall Management Center的客户端平台中。不提供 SCEP 或 CA 服务等设施来为客户端填充证书。

不支持的 AnyConnect 功能

唯一支持的 VPN 客户端是思科 AnyConnect 安全移动客户端。不支持任何其他客户端或本机 VPN。在 VPN 连接方面不支持无客户端 VPN；它只用于使用 Web 浏览器部署 AnyConnect 客户端 客户端。

在连接到 威胁防御 安全网关时，不支持以下 AnyConnect 功能：

- AnyConnect 定制和本地化支持。威胁防御设备不会配置或部署为这些功能配置 AnyConnect 所需的文件。
- TACACS、Kerberos（KCD 身份验证和 RSA SDI）。
- 浏览器代理。

配置新的远程访问 VPN 连接

本节介绍如何使用 Cisco Secure Firewall Threat Defense 设备作为 VPN 网关和 Cisco AnyConnect 作为 VPN 客户端配置新的远程访问 VPN 策略。

步骤	相应操作	更多信息
1	查看指南前提条件。	远程接入 VPN 的准则和限制，第 1138 页 配置远程接入 VPN 的必备条件，第 1141 页
2	使用向导来添加新的远程访问 VPN 策略。	创建新的远程接入 VPN 策略，第 1142 页
3	更新设备上部署的访问控制策略。	在 Cisco Secure Firewall Threat Defense 设备上更新访问控制策略，第 1143 页
4	（可选）如果在设备上配置了 NAT，请配置 NAT 免除规则。	（可选）配置 NAT 豁免，第 1144 页
5	配置 DNS。	配置 DNS，第 1145 页
6	添加 AnyConnect 客户端 配置文件。	添加 AnyConnect 客户端配置文件 XML 文件，第 1145 页
7	部署远程访问 VPN 策略。	部署配置更改，第 136 页
8	（可选）验证远程访问 VPN 策略配置。	检验配置，第 1147 页

配置远程接入 VPN 的必备条件

- 部署 Cisco Secure Firewall Threat Defense 设备并配置 Cisco Secure Firewall Management Center，以便在启用导出控制功能的情况下管理具有所需许可证的设备。有关详细信息，请参阅VPN 许可，第 1093 页。
- 配置用于为每台充当远程访问 VPN 网关的 威胁防御 设备获取身份证书的证书注册对象。
- 配置供远程接入 VPN 策略使用的 RADIUS 服务器组对象和任何 AD 或 LDAP 领域。
- 确保可以通过 威胁防御设备访问 AAA 服务器，以使远程接入 VPN 配置生效。配置路由（在 **设备 > 设备管理 > 编辑设备 > 路由**）以确保 AAA 服务器连接：

  对于远程接入 VPN 双重身份验证，请确保可以通过 威胁防御访问主身份验证和辅助身份验证服务器，以使双重身份验证配置生效。
- 要启用 威胁防御 远程访问 VPN 功能，购买并启用以下思科 AnyConnect 客户端 许可证之一：AnyConnect Plus、 AnyConnect Apex或 仅限 AnyConnect VPN 。
- 从思科软件下载中心下载最新的 AnyConnect 客户端 映像文件。

  在 Cisco Secure Firewall Management Center Web 界面上，转至**对象 (Objects) > 对象管理 (Object Management) > VPN > AnyConnect 文件 (AnyConnect File)**，然后添加新的 AnyConnect 客户端映像文件。
- 创建一个安全区或接口组，包含用户将访问的网络接口，用于 VPN 连接。请参阅接口，第 995 页。

- 从 Cisco 软件下载中心下载 AnyConnect 配置文件编辑器 以创建 AnyConnect 客户端配置文件。您可以使用独立配置文件编辑器创建新的或修改现有的 AnyConnect配置文件。

创建新的远程接入 VPN 策略

远程访问 VPN 策略向导将指导您快速轻松地设置具备基本功能的远程访问 VPN。您可以根据需要通过指定其他属性来增强策略配置并将其部署到您的 Cisco Secure Firewall Threat Defense安全网关设备。

开始之前

- 确保满足配置远程接入 VPN 的必备条件，第 1141 页中列出的所有必备条件。

过程

步骤 1 选择**设备** > **VPN** > **远程接入**。

步骤 2 点击**添加 (Add)** 使用远程访问 VPN 策略向导来新建具有基本策略配置的远程访问 VPN 策略。

您必须完成整个向导才能创建新的策略；如果在完成向导之前取消，则不会保存策略。

步骤 3 选择目标设备和协议。

您在这里选择的 威胁防御 设备将用作 VPN 客户端用户的远程访问 VPN 网关。

您可以在创建远程访问 VPN 策略或稍后更改设备时选择 威胁防御 设备。请参阅设置远程访问 VPN 策略的目标设备，第 1148 页。

您可以选择 **SSL** 或 **IPSec-IKEv2**，或同时选择两种VPN协议。 威胁防御 支持两种协议通过 VPN 隧道在公共网络上建立安全连接。

注释 威胁防御 不支持使用 NULL 加密的 IPSec 隧道。如果已选择 IPSec-IKEv2，请确保不为 IPSec IKEv2 提议选择 NULL 加密。请参阅配置 IKEv2 IPsec 方案对象，第 1062 页。

有关 SSL 设置，请参阅 配置 SSL 设置 ，第 627 页。

步骤 4 配置 **连接配置文件** 和 **组策略** 设置。

连接配置文件将指定一组参数，用于定义远程用户如何连接到VPN设备。参数包括身份验证的设置和属性、VPN 客户端的地址分配以及组策略。配置远程接入 VPN 策略时，威胁防御设备将提供名为 *DefaultWEBVPNGroup* 的默认连接配置文件。

有关详细信息，请参阅配置连接配置文件设置，第 1149 页。

有关配置的信息，

- AAA 设置，请参阅 配置远程访问 VPN 的 AAA 设置，第 1151 页
- LDAP 属性映射，请参阅 配置 LDAP 属性映射，第 1173 页
- SAML 2.0 单点登录身份验证，请参阅 配置 SAML 单点登录身份验证，第 1206 页

组策略是存储在组策略对象中的一组属性和值对，用于定义远程访问 VPN 体验的 VPN 用户。您可以使用组策略配置用户授权配置文件、IP 地址、AnyConnect 设置、VLAN 映射和用户会话设置等属性。RADIUS 授权服务器将会分配组策略，或从当前连接配置文件中获取。

有关详细信息，请参阅配置组策略，第 1173 页。

步骤 5 选择 VPN 用户将用于连接到远程访问 VPN 的 **AnyConnect 客户端映像**。

AnyConnect 安全移动客户端通过企业资源的全 VPN 调配为远程用户提供到 Cisco Secure Firewall Threat Defense 设备的安全 SSL 或 IPSec (IKEv2) 连接。在 威胁防御设备上部署远程访问 VPN 策略后，VPN用户可以在其浏览器中输入所配置设备接口的IP地址，以下载并安装AnyConnect客户端。

有关配置客户端配置文件和客户端模块的信息，请参阅组策略 AnyConnect 客户端 选项，第 1066 页。

步骤 6 选择**网络接口和身份证书**。

接口对象可对网络分段，帮助您管理和分类流量数据流。安全区域对象只是对接口进行分组。这些组可以跨多个设备；您还可以在单个设备上配置多个区域接口对象。有两种类型的接口对象：

- 安全区域 - 接口只能属于一个安全区域。
- 接口组 - 接口可属于多个接口组（和一个安全区域）。

步骤 7 查看远程访问 VPN 策略配置的**摘要**。

“摘要”页面显示到目前为止已配置的所有远程接入VPN设置，并提供指向在所选设备上部署远程接入 VPN 策略之前需要执行的其他配置的链接。

如有需要，请点击**返回**以更改配置。

步骤 8 点击**完成**，以完成远程接入 VPN 策略的基本配置。

在完成远程访问 VPN 策略向导后，将出现策略列表页面。稍后，设置 DNS 配置，为 VPN 用户配置访问控制，然后启用 NAT 豁免（如有必要），以完成基本远程访问 VPN 策略配置。

在 Cisco Secure Firewall Threat Defense 设备上更新访问控制策略

部署远程访问 VPN 策略之前，必须使用允许目标 Cisco Secure Firewall Threat Defense 设备上的 VPN 流量的规则更新访问控制策略。此规则必须允许来自外部接口的所有流量，其中源设备作为定义的 VPN 池网络，目标设备作为公司网络。

注释 如果在“访问接口”选项卡上选择**为已解密的流量绕过访问控制策略 (sysopt permit-vpn)** 选项，则无需更新远程接入 VPN 的访问控制策略。

启用或禁用所有 VPN 连接的选项。如果禁用此选项，请确保访问控制策略或预过滤器策略允许流量。

有关详细信息，请参阅配置远程访问 VPN 的访问接口，第 1167 页。

开始之前

使用远程接入 VPN 策略向导完成远程接入 VPN 策略配置。

过程

步骤 1 在您的 Cisco Secure Firewall Management Center Web 界面中，选择**策略>访问控制**。

步骤 2 点击要更新的访问控制策略旁边的**编辑 (Edit)**。

步骤 3 请点击 **添加规则**来添加新规则。

步骤 4 指定规则的 **名称** 并选择 **启用**。

步骤 5 选择 **操作**、 **允许** 或 **信任**。

步骤 6 在 **区域** 选项卡上选择以下选项：

a) 从可用区域中选择外部区域，然后点击**添加到源 (Add to Source)**。

b) 从可用区域中选择内部区域，然后点击**添加到目标 (Add to Destination)**。

步骤 7 在 **网络** 选项卡上选择以下选项：

a) 从可用网络中选择内部网络（内部接口和/或公司网络），然后点击 **添加到目标**。

b) 从 **可用网络** 中选择 VPN 地址池网络，然后点击 **添加到源网络**。

步骤 8 配置其他所需的访问控制规则设置，然后点击**添加**。

步骤 9 保存此规则和访问控制策略。

（可选）配置 NAT 豁免

NAT 豁免将豁免转换地址，并允许已转换的主机和远程主机发起与受保护主机的连接。与身份 NAT 一样，请不要限制特定接口上的主机转换；必须对通过所有接口的连接使用 NAT 豁免。但是，借助 NAT 豁免，您可以在确定要转换的实际地址时指定实际地址和目标地址（类似于策略 NAT）。使用静态身份 NAT 以考虑访问列表中的端口。

开始之前

检查部署有远程接入 VPN 策略的目标设备上是否配置了 NAT。如果已在目标设备上启用 NAT，您必须定义 NAT 策略，为 VPN 流量设置豁免。

过程

步骤 1 在您的 Cisco Secure Firewall Management Center Web 界面上，点击**设备** > **NAT**。

步骤 2 选择要更新的 NAT 策略，或点击**新建策略** > **威胁防御 NAT** 以使用允许所有连接的连接的 NAT 规则创建 NAT 策略。

步骤 3 点击**添加规则**，以添加 NAT 规则。

步骤 4 在“添加 NAT 规则”窗口中，选择以下内容：

a) 为“NAT 规则”选择**手动 NAT 规则**。
b) 为“类型”选择**静态**。
c) 点击 **接口对象** ，然后选择源和目标接口对象。

注释 此接口对象必须与在远程访问 VPN 策略中选择的接口相同。

有关详细信息，请参阅配置远程访问 VPN 的访问接口 ，第 1167 页。

a) 点击 **转换** 并选择源和目标网络：
   - **原始源** 和 **转换后的源**
   - **原始目标** 和 **转换后的目标**

步骤 5 在“高级”选项卡中，选择**不在目标接口上使用代理 ARP**。

不在目标接口上使用代理 ARP - 为所映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。

步骤 6 点击**确定 (OK)**。

配置 DNS

在每台 威胁防御设备上配置 DNS，以便使用远程接入 VPN。如果没有 DNS，设备将无法解析 AAA 服务器名称、命名 URL 和具有 FQDN 或主机名的 CA 服务器。它只能解析 IP 地址。

过程

步骤 1 使用“平台设置”配置 DNS 服务器详细信息和域查找接口。有关详细信息，请参阅 配置 DNS ，第 617 页 和 DNS 服务器组 ，第 985 页。

步骤 2 如果可以通过 VNP 网络访问 DNS 服务器，则在组策略中配置拆分隧道，以允许 DNS 流量通过远程接入 VPN 隧道。有关详细信息，请参阅配置组策略对象 ，第 1063 页。

添加 AnyConnect 客户端配置文件 XML 文件

AnyConnect 客户端配置文件 是一组以 XML 文件形式存储的配置参数，客户端使用该文件来配置客户端的操作和外观。这些参数（XML 标记）包括主机名称和地址以及设置，用于启用更多客户端功能。

AnyConnect 客户端配置文件 编辑器是一款基于 GUI 的配置工具，作为 AnyConnect 软件包的一部分提供，您可以使用此编辑器来创建 AnyConnect 客户端配置文件 。该程序可独立于 管理中心 而运

行。有关 AnyConnect 客户端配置文件 编辑器的详细信息，请参阅《思科 AnyConnect 安全移动客户端管理员指南》《》。

开始之前

Cisco Secure Firewall Threat Defense 远程访问 VPN 策略要求将 AnyConnect 客户端配置文件 的任务分配给 VPN 客户端。您可以将客户端配置文件连接到组策略。

您可以从 Cisco 软件下载中心下载 AnyConnect 客户端配置文件 编辑器。

过程

步骤 1 选择**设备 (Devices)** > **远程访问 (Remote Access)**。

步骤 2 点击要编辑的远程接入 VPN 策略旁边的 **编辑** 。

步骤 3 点击要添加的 AnyConnect 客户端 配置文件上的 **编辑** 。

步骤 4 点击**编辑组策略 (Edit Group Policy)**。如果您选择添加新的组策略，请点击**添加 (Add)**。

步骤 5 选择 **AnyConnect** > **配置文件 (Profile)**。

步骤 6 从**客户端配置文件 (Client Profile)** 下拉列表中选择一个配置文件。如果您选择添加新的客户端配置文件，请点击**添加 (Add)** 并执行以下操作：

a) 指定配置文件**名称 (Name)**。

b) 点击**浏览 (Browse)** 并选择 AnyConnect 客户端配置文件 XML 文件。

注释 对于双因素身份验证，也要确保在 AnyConnect 客户端 配置文件中将超时设置为 60 秒或更长。

c) 点击**保存 (Save)**。

步骤 7 保存更改。

（可选）配置分割隧道

拆分隧道不仅允许 VPN 通过安全隧道连接到远程网络，而且允许连接到 VPN 隧道外的网络。如果要允许 VPN 用户在连接到远程访问 VPN 时访问外部网络，则您可以配置分割隧道。要配置拆分隧道列表，必须创建标准访问列表或扩展访问列表。

有关详细信息，请参阅配置组策略 ， 第 1173 页。

过程

步骤 1 选择 **设备** > **远程访问**。

步骤 2 点击要为其配置分割隧道的远程访问 VPN 策略旁边的**编辑 (Edit)**。

步骤 3 在请求的连接配置文件上，点击**编辑 (Edit)**。

步骤 4 点击**添加 (Add)** 以添加组策略，或者点击**编辑组策略 (Edit Group Policy)**。

步骤 5 选择**常规 (General)** > **分割隧道 (Split Tunneling)**。

步骤 6 从 **IPv4 拆分隧道 (IPv4 Split Tunneling)** 或 **IPv6 拆分隧道 (IPv6 Split Tunneling)** 列表中，选择**排除下面指定的网络 (Exclude networks specified below)**；然后选择要从 VPN 流量中排除的网络。

默认设置允许所有流量通过 VPN 隧道。

步骤 7 点击**标准访问列表 (Standard Access List)** 或**扩展访问列表 (Extended Access List)**，然后从下拉列表中选择一个访问列表或添加新的访问列表。

步骤 8 如果您选择添加新的标准或扩展访问列表，请执行以下操作：

a) 为新访问列表指定**名称 (Name)**，然后点击**添加 (Add)**。

b) 从**操作 (Action)** 下拉列表中选择**允许 (Allow)**。

c) 选择允许通过 VPN 隧道的网络流量并点击 **添加**。

步骤 9 保存更改。

相关主题

访问列表，第 975 页

检验配置

过程

步骤 1 在外部网络上的计算机上打开 Web 浏览器。

步骤 2 输入配置 威胁防御 远程访问 VPN 网关的 URL。

步骤 3 提示时，输入用户名和密码，然后点击 **登录**。

注释 如果在系统上安装 AnyConnect，则会自动建立与 VPN 的连接。

如果未安装 AnyConnect，VPN 会提示您下载 AnyConnect。

步骤 4 下载 AnyConnect（如果尚未安装）并连接到 VPN。
AnyConnect 客户端会自行安装。成功进行身份验证后，您将连接到 Cisco Secure Firewall Threat Defense 远程访问 VPN 网关。适用的身份或 QoS 策略根据您的远程访问 VPN 策略配置实施。

创建现有远程接入 VPN 策略的副本

复制现有的远程接入 VPN 策略，以便创建具有所有设置（包括连接配置文件和访问接口）的新策略。然后，您可以将设备分配给新策略，同时根据需要在分配的设备上部署 VPN。

注释 具有远程访问 VPN 只读权限的用户无法创建 VPN 的副本。域中拥有只读权限的用户可以复制远程访问 VPN。

过程

步骤 1 选择设备 > VPN > 远程接入。
步骤 2 点击要复制的策略上的复制 (Copy)。
步骤 3 为新的远程访问 VPN 指定 名称 。
步骤 4 点击确定 (OK)。

下一步做什么

要将设备分配给新策略，请参阅设置远程访问 VPN 策略的目标设备，第 1148 页。

设置远程访问 VPN 策略的目标设备

在创建远程访问 VPN 策略后，您可以将策略分配给威胁防御设备。

过程

步骤 1 选择 设备 > VPN > 远程访问。
步骤 2 点击要编辑的远程接入 VPN 策略旁边的 编辑（） 。
步骤 3 点击策略分配。
步骤 4 执行以下任一操作：

- 要将设备、高可用性对或设备组分配给策略，请在 可用设备 列表中将其选中，然后点击 添加。您还可以拖放可用设备进行选择。
- 要删除设备分配，请点击所选设备 (Selected Devices) 列表中的设备、高可用性对或设备组旁边的 删除（）。

步骤 5 点击确定 (OK)。
步骤 6 点击保存 (Save)。

下一步做什么

- 部署配置更改。

将本地领域与远程接入 VPN 策略相关联

您可以将本地领域与远程访问 VPN 策略相关联，以启用本地用户身份验证。

有关创建和管理领域的信息，请参阅管理领域，第 1836 页。

有关为远程接入 VPN 配置本地用户认证的信息，请参阅配置远程访问 VPN 的 AAA 设置，第 1151 页。

过程

步骤 1 选择 **设备** > **VPN** > **远程访问**。

步骤 2 点击要编辑的远程接入 VPN 策略旁边的 **编辑**（ ）。

步骤 3 点击**本地领域 (Local Realm)** 旁边的链接。

步骤 4 从列表中选择 **本地领域服务器 (Local Realm Server)**，或点击**添加 (Add)** 以添加新的本地领域。

步骤 5 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

下一步做什么

- 部署配置更改。

其他远程访问 VPN 配置

配置连接配置文件设置

远程访问VPN策略包含针对特定设备的连接配置文件。这些策略与创建隧道本身有关，如如何完成AAA，以及如何为VPN客户端分配地址（DHCP或地址池）。它们还包括用户属性，这些属性将在威胁防御设备上配置或从 AAA 服务器上获取的组策略中确定。设备还将提供名为 *DefaultWEBVPNGroup* 的默认连接配置文件。该连接配置文件是使用列表中显示的向导配置的。

如果您决定为不同的VPN用户组授予不同的权限，那么您可以为每个用户组添加特定的连接配置文件，并在远程访问 VPN 策略中维护多个连接配置文件。

过程

步骤 1 选择**设备** > **VPN** > **远程接入**。

步骤 2 在列表中选择现有的远程接入策略，然后点击相应的**编辑**图标。

步骤 3 选择 **连接配置文件 (Connection Profile)**，然后点击 **编辑 (Edit)**。

步骤 4 （可选）如果您选择添加新的连接配置文件，请点击**添加 (Add)**。

步骤 5 配置 VPN 客户端的 IP 地址。
配置 VPN 客户端的 IP 地址，第 1150 页

步骤 6 （可选）更新远程访问 VPN 的 AAA 设置。
配置远程访问 VPN 的 AAA 设置，第 1151 页

步骤 7 （可选）创建或更新别名。
创建或更新连接配置文件的别名，第 1166 页

步骤 8 保存更改。

配置 VPN 客户端的 IP 地址

客户端地址分配提供了一种为远程访问 VPN 用户分配 IP 地址的手段。

您可以配置为从本地 IP 地址池、DHCP 服务器和 AAA 服务器为远程 VPN 客户端分配 IP 地址。首先由 AAA 服务器分配，然后由其他服务器分配。在**高级**选项卡中配置**客户端地址分配**策略，以定义分配标准。仅在连接配置文件的关联组策略或系统默认组策略**DfltGrpPolicy**中未定义 IP 池时，才会使用此连接配置文件中定义的 IP 池。

IPv4 地址池 - SSL VPN 客户端将在连接到 Cisco Secure Firewall Threat Defense设备时收到新 IP 地址。Address Pools 定义远程客户端可以接收的地址范围。选择一个现有的 IP 地址池。可分别为 IPv4 和 IPv6 地址添加最多六个池。

注释 可以使用 Cisco Secure Firewall Management Center中现有 IP 池的 IP 地址，也可以使用**添加**选项创建新池。另外，还可以使用**对象 > 对象管理 > 地址池**路径在 Cisco Secure Firewall Management Center中创建 IP 池。有关详细信息，请参阅地址池，第 978 页。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备 > VPN > 远程接入**。
系统将列出现有的远程接入策略。

步骤 2 选择远程访问 VPN 策略，然后点击 **编辑**。

步骤 3 选择要更新的连接配置文件，然后点击 **编辑 > 客户端地址分配**。

步骤 4 为 **地址池**选择以下选项：

a) 点击 **添加** 以添加 IP 地址，然后选择 **IPv4** 或 **IPv6** 以添加对应的地址池。从可用池中选择 IP 地址池，然后点击 **添加**。

注释 如果在多台 Cisco Secure Firewall Threat Defense 设备之间共享远程访问 VPN 策略，请牢记所有设备都将共享同一地址池，除非使用设备级对象覆盖，将每台设备的全局定义替换为一个唯一地址池。在设备不使用 NAT 的情况下，需要多个唯一地址池，以免重叠地址。

b) 选择 **地址池** 窗口中的 **添加** 图标，以添加新的 IPv4 或 IPv6 地址池。如果选择 IPv4 池，请提供起始和结束 IP 地址。如果选择包括新的 IPv6 地址池，请输入介于范围 1-16384 之间的**地址数量**。在多台设备之间共享对象时，选择**允许覆盖**选项可以避免与 IP 地址冲突。有关详细信息，请参阅地址池，第 978 页。

c) 点击**确定**。

步骤 5 为 **DHCP 服务器**选择以下选项：

注释 只能通过 IPv4 地址配置 DHCP 服务器地址。

a) 指定名称和 DHCP（动态主机配置协议）服务器地址作为网络对象。点击 **添加**，然后从对象列表中选择服务器。点击 **删除** 以删除 DHCP 服务器。

b) 点击 **新对象** 页面中的 **添加** 以添加新网络对象。输入新对象名称、说明、网络，然后选择**允许覆盖**选项（如果适用）。有关更多信息，请参阅创建网络对象，第 999 页和允许对象覆盖，第 969 页。

c) 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

相关主题

配置连接配置文件设置，第 1149 页

配置远程访问 VPN 的 AAA 设置

开始之前

- 确保在终端上部署所需的计算机和用户证书。有关 Cisco Secure Firewall Threat Defense 证书的信息，请参阅管理 威胁防御 证书，第 1078 页管理 VPN 证书。
- 使用所需的证书配置 AnyConnect 配置文件。有关详细信息，请参阅。

过程

步骤 1 选择**设备** > **VPN** > **远程接入**。

步骤 2 在列表中选择现有的远程接入策略，然后点击相应的**编辑**图标。

步骤 3 选择要更新 AAA 设置的连接配置文件，然后点击 **编辑** > **AAA**。

步骤 4 为 **身份验证**选择以下选项：

- **身份验证方法**-确定在允许用户访问网络和网络服务之前对其进行标识的方式这种方法通过要求提供有效的用户凭据（通常是用户名和密码）来控制访问。它也可能包括来自客户端的证书。受支持的身份验证方法有**仅 AAA**、**仅客户端证书**和 **AAA + 客户端证书**。

  何时选择以下**身份验证方法**：

  - **仅 AAA** - 如果选择 **RADIUS** 作为**身份验证服务器**，则授权服务器默认也采用此选择。从下拉列表中选择**记帐服务器**。每当从“身份验证服务器”下拉列表中选择 **AD** 和 **LDAP** 时，必须手动选择 **授权服务器** 和 **记帐服务器** 。

- **SAML**-使用SAML单点登录服务器对每个用户进行身份验证。有关详细信息，请参阅使用SAML 2.0的单点登录身份验证，第1204页。

  覆盖身份提供程序证书-选择此选项可使用连接配置文件或SAML应用特定的IdP证书覆盖SAML提供程序的主身份提供程序证书。从IdP下拉列表中选择证书。

  Microsoft Azure可以为同一实体ID支持多个应用。每个应用（映射到不同的连接配置文件）都需要唯一的证书。如果要在当前连接配置文件中保留单点登录对象的现有实体ID并使用其他IdP证书，则可以选择此选项。

  这启用每个Microsoft Azure SAML身份提供程序支持多个SAML应用。

  主身份证书在单点登录服务器对象中配置。

  有关配置单点登陆服务器对象的详细信息，请参阅添加单点登录服务器，第973页。

  选择您的 **SAML 登录体验** 以配置用于SAML Web身份验证的浏览器：

  - **VPN 客户端嵌入式浏览器**-选择此选项可使用VPN客户端嵌入式浏览器进行Web身份验证。身份验证仅适用于VPN连接。
  - **默认操作系统浏览器**-选择此选项可配置默认操作系统或支持WebAuthN（用于Web身份验证的FIDO2标准）的本地浏览器。此选项启用单点登录(SSO)支持Web身份验证方法，例如生物识别身份验证。

    默认浏览器需要外部浏览器软件包进行Web身份验证。默认情况下配置软件包 默认-外部-浏览器-软件包。您可以通过编辑远程访问 VPN 策略并选择**高级 (Advanced)** > **AnyConnect 客户端映像 (AnyConnect Client Images)** > **软件包文件 (Package File)** 下的文件来更改默认外部浏览器软件包。

    您还可以通过选择添加新的软件包文件。**对象 (Objects)** > **对象管理 (Object Management)** > **VPN** > **AnyConnect 文件 (AnyConnect File)** > **添加 AnyConnect 文件 (Add AnyConnect File)**。

- **仅客户端证书**- 使用客户端证书对每个用户进行身份验证。客户端证书必须在VPN客户端终端上配置。默认情况下，用户名派生自客户端证书字段CN和OU。如果在客户端证书的其他字段中指定了用户名，请使用“主”字段和“辅助”字段来映射适当的字段。

  选择 **启用多个证书身份验证** 以使用计算机和用户证书对VPN客户端进行身份验证。

  如果已启用多个证书身份验证，则可以选择以下证书之一来映射用户名和对VPN用户进行身份验证：

  - **第一个证书**-选择此选项以映射从VPN客户端发送的计算机证书中的用户名。
  - **第二个证书**-选择此选项以映射从客户端发送的用户证书中的用户名。

  注释 如果未启用多证书身份验证，则默认情况下使用用户证书（第二证书）进行身份验证。

  如果选择**映射特定字段**选项（包括客户端证书中的用户名），则**主**字段和**辅助**字段将分别显示默认值：**CN**（**公用名**）和**OU**（**组织单位**）。如果选择**使用整个DN作为用户名**选项，

系统将自动检索用户身份。可分辨名称 (DN) 是由单个字段组成的唯一标识，将用户与连接配置文件匹配时用作标识符。DN 规则用于增强的证书身份验证。

与**映射特定字段**选项相关的“主”字段和“辅助”字段包含以下公用值：

- C（国家/地区）
- CN（公用名）
- DNQ（DN 限定符）
- EA（邮件地址）
- GENQ（代系限定符）
- GN（名字）
- I（首字母）
- L（地区）
- N（名字）
- O（组织）
- OU（组织单位）
- SER（序列号）
- SN（姓氏）
- SP（省）
- T（职务）
- UID（用户 ID）
- UPN（用户主体名称）

- **客户端证书和 AAA**-每个用户都使用客户端证书和 AAA 服务器进行身份验证。选择身份验证所需的证书和 AAA 配置。

  无论选择哪种身份验证方法，选择或取消选择**仅当用户位于授权数据库中时才允许连接**。

- **客户端证书和 SAML**-每个用户都使用客户端证书和 AAA 服务器进行身份验证。选择所需的证书和 SAML 配置以进行身份验证。

  - **允许仅在证书中的用户名与 SAML 相同时允许连接**-仅当证书中的用户名与 SAML 单点登录用户名匹配时，选择仅允许 VPN 连接。
  - **从客户端证书中使用用户名进行授权**-选择从客户端证书中选择用户名进行授权时，必须配置要从客户端证书中选择的字段。

    您可以选择将特定字段映射为用户名，也可以使用整个可分辨名称 (DN) 进行授权：

- **映射特定字段**- 从客户端证书中选择要包含的用户名，则 **主要** 和 **辅助** 字段将分别显示默认值： **CN**（**公用名**） 和 **OU**（**组织单位**） 。
- **使用整个 DN 作为用户名**- 系统将自动检索用户身份用于授权。

您还可以创建动态访问策略 (DAP)，以将用户特定的 SAML 断言属性或用户名与 DAP 证书属性进行匹配。请参阅配置 DAP 的 AAA 标准设置 ， 第 1219 页。

- **身份验证服务器** - 身份验证是在允许用户访问网络和网络服务之前对其进行标识的方式。身份验证需要有效的用户凭证和/或证书。您可以单独使用身份验证功能，也可以将其与授权和记帐功能配合使用。

  如果您已添加服务器或创建身份验证服务器，请从列表中选择身份验证服务器：

  - **LOCAL**-使用来自 威胁防御 的本地数据库进行用户身份验证。
    - **本地领域**-选择本地领域或点击 **添加** 以配置领域。请参阅创建 Active Directory 领域和领域目录 ， 第 1816 页。
  - **领域**-配置 LDAP 或 AD 领域。请参阅创建 Active Directory 领域和领域目录 ， 第 1816 页。
  - **RADIUS 服务器组**-使用 RADIUS 服务器添加 RADIUS 服务器组对象。请参阅添加 RADIUS 服务器组 ， 第 970 页。
  - **单点登录服务器**-为 SAML 身份验证创建单点登录服务器对象。请参阅添加单点登录服务器 ， 第 973 页。

回退到本地身份验证-使用本地数据库对用户进行身份验证，即使 AAA 服务器组不可用，只要已配置本地数据库，即可建立 VPN 隧道。

- **使用辅助身份验证** - 除主身份验证之外，还配置了辅助身份验证，以便为 VPN 会话提供额外的安全保护。辅助身份验证是仅适用于**仅 AAA** 和**客户端证书和 AAA** 身份验证方法。

  辅助身份验证是一项可选功能，该功能要求 VPN 用户在 AnyConnect 登录屏幕上输入两组用户名和密码。您还可以配置为从身份验证服务器或客户端证书预填充辅助用户名。仅当主身份验证和辅助身份验证均成功时，才会授予远程访问 VPN 身份验证。如果任何一个身份验证服务器无法访问或一个身份验证失败，VPN 身份验证将被拒绝。

  必须在配置辅助身份验证前，为辅助用户名和密码配置辅助身份验证服务器组（AAA 服务器）。例如，可以将主身份验证服务器设置为 LDAP 或 Active Directory 领域，将辅助身份验证设置为 RADIUS 服务器。

  注释 默认情况下，无需辅助身份验证。

  身份验证服务器 - 为 VPN 用户提供辅助用户名和密码的辅助身份验证服务器。

  - **回退到本地身份验证**-使用本地数据库对此用户进行身份验证，即使 AAA 服务器组不可用，只要已配置本地数据库，即可建立 VPN 隧道。

  选择 **辅助身份验证的用户名**以下的选项：

- **提示：** 在登录 VPN 网关时，提示用户输入用户名和密码。
- **使用主身份验证用户名：** 用户名从主身份验证服务器获取，用于主身份验证和辅助身份验证；必须输入两个密码。
- **映射客户端证书中的用户名：** 预填充客户端证书中的辅助用户名。

  如果已启用多个证书身份验证，则可以选择以下证书之一：

  - **第一个证书**-选择此选项以映射从 VPN 客户端发送的计算机证书中的用户名。
  - **第二个证书**-选择此选项以映射从客户端发送的用户证书中的用户名。
  - 如果选择**映射特定字段**选项，其中包括来自客户端证书的用户名。则**主**和**辅助**字段将显示默认值：**CN (公用名称)** 和 **OU (组织单位)**。如果选择**使用整个 DN（可分辨名称）作为用户名**选项，系统将自动检索用户身份。

    有关主字段和辅助字段映射的详细信息，请参阅**身份验证方法**说明。
  - **在用户登录窗口预填证书中的用户名 (Prefill username from certificate on user login window)：** 用户通过 AnyConnect VPN 客户端连接时，预填充客户端证书中的辅助用户名。
    - **在登录窗口隐藏用户名：** 辅助用户名是从客户端证书预填充的，但对用户隐藏，确保用户不会修改预填充的用户名。
- **使用 VPN 会话的辅助用户名：** 辅助用户名用于在 VPN 会话期间报告用户活动。

步骤 5 为 **授权**选择以下选项：

- **身份验证服务器**-身份验证完成后，授权将控制对每个经过身份验证的用户都可用的服务和命令。授权通过组合一组描述用户被授权执行的操作、其实际功能和限制的属性来工作。当您不使用授权，则单独的身份验证将为所有经过身份验证的用户提供相同的访问权限。授权需要进行身份验证。

  要了解有关远程访问 VPN 授权工作原理的更多信息，请参阅 了解权限和属性的策略实施，第 1136 页。

  在连接配置文件中配置了 RADIUS 服务器以进行用户授权时，远程访问 VPN 系统管理员可以为用户或用户组配置多个授权属性。在 RADIUS 服务器上配置的授权属性可以特定于用户或用户组。用户通过身份验证后，这些特定的授权属性将被推送到 威胁防御设备。

  注释 从授权服务器获得的 AAA 服务器属性覆盖了之前在组策略或连接配置文件上可能已经配置的属性值。

- 如果需要，请选择**仅当用户位于授权数据库中时才允许连接**。

  启用该选项后，系统检查客户端的用户名必须存在于授权数据库中，才可以成功进行连接。如果授权数据库中不存在该用户名，则连接被拒绝。

- 当您选择领域作为授权服务器时，必须配置 LDAP 属性映射。您可以选择用于身份验证和授权的单个服务器或其他服务器。点击 **配置 LDAP 属性映射** 以添加用于授权的 LDAP属性映射。

  注释 威胁防御 不支持将 SAML 身份提供程序用作授权服务器。如果 SAML 身份提供程序后面的 Active Directory 可通过 管理中心 和 威胁防御 访问，则可以按照以下步骤配置授权：

  - 为 AD 服务器添加领域。请参阅创建 Active Directory 领域和领域目录，第 1816 页。
  - 选择领域对象作为远程访问 VPN 连接配置文件中的授权服务器。
  - 为所选领域配置 LDAP 属性映射。

  有关配置 LDAP 属性映射的信息，请参阅配置 LDAP 属性映射，第 1173 页。

步骤 6 为 **记帐**选择以下选项：

- **记账服务器**-记账用于跟踪用户正在访问的服务和他们正在使用的网络资源量。当激活 AAA 记帐时，网络访问服务器会向 RADIUS 服务器报告用户活动。记账信息包括每个会话的开始和停止时间、用户名、会话时通过设备的字节数、使用的服务以及每个会话的持续时间。然后系统可以分析该数据，以进行网络管理、客户端计费或审核。您可以单独使用记帐功能，也可以将其与身份验证和授权功能配合使用。

  指定将用于对远程访问 VPN 会话进行记帐的 RADIUS 服务器组对象。

步骤 7 选择 **高级设置**以下的选项：

- **从用户名删除领域**- 在将用户名传递到 AAA 服务器之前，选择要从用户名删除领域。例如，如果选择此选项并提供域\用户名，则该域将从用户名中删除，并发送到 AAA 服务器进行身份验证。默认情况下，此选项处于取消选中状态。
- **从用户名删除组**- 在将用户名传递到 AAA 服务器之前，选择要从用户名删除组名称。默认情况下，此选项处于取消选中状态。

  注释 领域是管理域。启用这些选项将允许仅基于用户名进行身份验证。您可以启用这些选项的任意组合。但是，如果服务器无法分析分隔符，则必须选中这两个复选框。

- **密码管理 (Password Management)**：启用远程访问 VPN 用户的密码管理。选择以提前通知密码到期或密码到期的日期。

步骤 8 点击**保存 (Save)**。

相关主题

了解权限和属性的策略实施，第 1136 页
管理领域，第 1836 页

Cisco Secure Firewall Threat Defense 的 RADIUS 服务器属性

威胁防御设备支持将用户授权属性（也称为用户权利或权限）应用到来自外部 RADIUS 服务器的 VPN 连接，这些连接被配置为用于远程接入 VPN 策略中的身份验证和/或授权。

注释 Cisco Secure Firewall Threat Defense 设备支持具有供应商 ID 3076 的属性。

以下用户授权属性由 RADIUS 服务器发送到 威胁防御设备。

- RADIUS 属性 146 和 150 是从 威胁防御设备发送到 RADIUS 服务器，以提出身份验证和请求授权。
- 所有三个属性（146、150 和 151）都是从 威胁防御设备发送到 RADIUS 服务器，以提出开始记账、临时更新和停止请求。

表 *84:* 从 *Cisco Secure Firewall Threat Defense* 发送到 *RADIUS* 服务器的 *RADIUS* 属性

属性	属性编号	语法、类型	单值或多值	说明或值
连接配置文件名称或隧道组名称	146	字符串	单值	1 到 253 个字符
客户端类型	150	整数	单值	2 = AnyConnect 客户端 SSL VPN, 6 = AnyConnect 客户端 IPsec VPN (IKEv2)
会话类型	151	整数	单值	1 = AnyConnect 客户端 SSL VPN, 2 = AnyConnect 客户端 IPsec VPN (IKEv2)

表 *85:* 支持的 *RADIUS* 授权属性

属性名称	威胁防御	属性编号	语法/类型	单值或多值	说明或值
Access-Hours	支持	1	字符串	单值	时间范围的名称，例如工作时间
Access-List-Inbound	支持	86	字符串	单值	这两个访问列表属性都使用 威胁防御 设备 ACL 名称。使用 Smart CLI 扩展访问列表创建 ACL（依次选择**设备 (Device)** > **高级 (Advanced Configuration)** > **Smart CLI** > **(Objects)**）。 此类 ACL 用于控制入站流量（流量进入设备）或出站流量（流量离开 威胁防御
Access-List-Outbound	支持	87	字符串	单值	
Address-Pools	支持	217	字符串	单值	威胁防御 设备上定义的网络对象名称，用作为地址池供客户端连接远程访问 VPN 网。在**对象**页面上定义网络对象。

属性名称	威胁防御	属性编号	语法/类型	单值或多值	说明或值
Allow-Network-Extension-Mode	支持	64	布尔值	单值	0 = 已禁用 1 = 已启用
Authenticated-User-Idle-Timeout	支持	50	整数	单值	1-35791394 分钟
Authorization-DN-Field	支持	67	字符串	单值	可能的值：UID、OU、O、CN、L、SP、C、T、N、GN、SN、I、GENQ、DNQ、SER、use-entire-name
Authorization-Required		66	整数	单值	0 = 否 1 = 是
Authorization-Type	支持	65	整数	单值	0 = 无 1 = RADIUS 2 = LDAP
Banner1	支持	15	字符串	单值	要为思科 VPN 远程访问会话显示的横幅字符IPsec IKEv1、 AnyConnect SSL TLS/DTLS/IKClientless SSL。
Banner2	支持	36	字符串	单值	要为思科 VPN 远程访问会话显示的横幅字符IPsec IKEv1、 AnyConnect SSL TLS/DTLS/IKClientless SSL。如果进行了相应的配置，则I字符串会连接到 Banner1 字符串。
Cisco-IP-Phone-Bypass	支持	51	整数	单值	0 = 已禁用 1 = 已启用
Cisco-LEAP-Bypass	支持	75	整数	单值	0 = 已禁用 1 = 已启用
Client Type	支持	150	整数	单值	1 = 思科 VPN 客户端 (IKEv1) 2 = AnyConnec端 SSL VPN 3 = 无客户端 SSL VPN 4 = 直接理 5 = L2TP/IPsec SSL VPN 6 = AnyConnect IPsec VPN (IKEv2)
Client-Type-Version-Limiting	支持	77	字符串	单值	IPsec VPN 版本号字符串
DHCP-Network-Scope	支持	61	字符串	单值	IP 地址
Extended-Authentication-On-Rekey	支持	122	整数	单值	0 = 已禁用 1 = 已启用
Framed-Interface-Id	支持	96	字符串	单值	分配的 IPv6 接口 ID。与 Framed-IPv6-Prefix用以创建完整的已分配 IPv6 地址。例如：Framed-Interface-ID =1:1:1:1与 Framed-IPv6-P=2001:0db8::/64 组合可提供分配的IP地址2001:0db8::1:1:1:1。

属性名称	威胁防御	属性编号	语法/类型	单值或多值	说明或值
Framed-IPv6-Prefix	支持	97	字符串	单值	分配的 IPv6 前缀和长度。与 Framed-Inter 合以创建完整的已分配 IPv6 地址。例如： 2001:0db8::/64 与 Framed-Interface-Id=1:1: 提供IP地址 2001:0db8::1:1:1:1。通过分配 为/128 的完整 IPv6 地址（例如， Framed-IPv6-Prefix=2001:0db8::1/128）， 属性分配IP地址而不使用 Framed-Interfac
Group-Policy	支持	25	字符串	单值	为远程访问 VPN 会话设置组策略。您可 其中一种格式： • 组策略名称 • OU = 组策略名称 • OU = 组策略名称；
IE-Proxy-Bypass-Local		83	整数	单值	0 = 无 1 = 本地
IE-Proxy-Exception-List		82	字符串	单值	换行符 (\n) 分隔的 DNS 域列表
IE-Proxy-PAC-URL	支持	133	字符串	单值	PAC 地址字符串
IE-Proxy-Server		80	字符串	单值	IP 地址
IE-Proxy-Server-Policy		81	整数	单值	1 = 无修改 2 = 无代理 3 = 自动检测 4 = 使 设置
IKE-KeepAlive-Confidence-Interval	支持	68	整数	单值	10 到 300 秒
IKE-Keepalive-Retry-Interval	支持	84	整数	单值	2 到 10 秒
IKE-Keep-Alives	支持	41	布尔值	单值	0 = 已禁用 1 = 已启用
Intercept-DHCP-Configure-Msg	支持	62	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Allow-Passwd-Store	支持	16	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Authentication		13	整数	单值	0 = 无 1 = RADIUS 2 = LDAP（仅适用于 = NT 域 4 = SDI 5 = 内部 6 = RADIUS 到 Kerberos/Active Directory
IPsec-Auth-On-Rekey	支持	42	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Backup-Server-List	支持	60	字符串	单值	服务器地址（以空格分隔）
IPsec-Backup-Servers	支持	59	字符串	单值	1 = 使用客户端配置的列表 2 = 禁用并清除 表 3 = 使用备份服务器列表

属性名称	威胁防御	属性编号	语法/类型	单值或多值	说明或值
IPsec-Client-Firewall-Filter-Name		57	字符串	单值	指定要作为防火墙策略推送到客户端的过滤器 称
IPsec-Client-Firewall-Filter-Optional	支持	58	整数	单值	0 = 必需 1 = 可选
IPsec-Default-Domain	支持	28	字符串	单值	指定要发送到客户端的单个默认域名（1 到2 符）。
IPsec-IKE-Peer-ID-Check	支持	40	整数	单值	1 = 必需 2 = 如果对等证书支持 3 = 不检查
IPsec-IP-Compression	支持	39	整数	单值	0 = 已禁用 1 = 已启用
IPsec-Mode-Config	支持	31	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Over-UDP	支持	34	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Over-UDP-Port	支持	35	整数	单值	4001 到 49151。默认值为 10000。
IPsec-Required-Client-Firewall-Capability	支持	56	整数	单值	0 = 无 1 = 远程 FW Are-You-There (AYT) 定义 略 2 = 策略推送的 CPP 4 = 来自服务器的策
IPsec-Sec-Association		12	字符串	单值	安全关联的名称
IPsec-Split-DNS-Names	支持	29	字符串	单值	指定要发送到客户端的辅助域名列表（1 到2 符）。
IPsec-Split-Tunneling-Policy	支持	55	整数	单值	0 = 无拆分隧道 1 = 拆分隧道 2 = 允许本地 L
IPsec-Split-Tunnel-List	支持	27	字符串	单值	指定用于描述分割隧道包含列表的网络或 AC 称。
IPsec-Tunnel-Type	支持	30	整数	单值	1 = LAN 到 LAN 2 = 远程访问
IPsec-User-Group-Lock		33	布尔值	单值	0 = 已禁用 1 = 已启用
IPv6-Address-Pools	支持	218	字符串	单值	IP 本地池 IPv6 的名称
IPv6-VPN-Filter	支持	219	字符串	单值	ACL 值
L2TP-Encryption		21	整数	单值	位图： 1 = 需要加密 2 = 40 位 4 = 128 位 8 无状态 15= 40/128 位加密/需要无状态
L2TP-MPPC-Compression		38	整数	单值	0 = 已禁用 1 = 已启用

属性名称	威胁防御	属性编号	语法/类型	单值或多值	说明或值
Member-Of	支持	145	字符串	单值	逗号分隔的字符串，例如： `Engineering, Sales` 可在动态访问策略里使用的管理属性。不 略。
MS-Client-Subnet-Mask	支持	63	布尔值	单值	IP 地址
NAC-Default-ACL		92	字符串		ACL
NAC-Enable		89	整数	单值	0 = 否 1 = 是
NAC-Revalidation-Timer		91	整数	单值	300 到 86400 秒
NAC-Settings	支持	141	字符串	单值	NAC 策略名称
NAC-Status-Query-Timer		90	整数	单值	30 到 1800 秒
Perfect-Forward-Secrecy-Enable	支持	88	布尔值	单值	0 = 否 1 = 是
PPTP-Encryption		20	整数	单值	位图： 1 = 需要加密 2 = 40 位 4 = 128 位 无状态 15= 40/128 位加密/需要无状态
PPTP-MPPC-Compression		37	整数	单值	0 = 已禁用 1 = 已启用
Primary-DNS	支持	5	字符串	单值	IP 地址
Primary-WINS	支持	7	字符串	单值	IP 地址
Privilege-Level	支持	220	整数	单值	介于 0 和 15 之间的整数。
Required-Client- Firewall-Vendor-Code	支持	45	整数	单值	1 = 思科系统（使用思科集成客户端） 2 = 3 = NetworkICE 4 = Sygate 5 = 思科系统 入侵防御安全代理）
Required-Client-Firewall-Description	支持	47	字符串	单值	字符串
Required-Client-Firewall-Product-Code	支持	46	整数	单值	思科系统公司产品： 1 = 思科入侵防御安全代理或思科集成客 Zone Labs 产品： 1 = Zone Alarm 2 = Zon 3 = Zone Labs Integrity NetworkICE 产品： 1 = BlackIce Defende Sygate 产品： 1 = Personal Firewall 2 = P Firewall Pro 3 = 安全代理

属性名称	威胁防御	属性编号	语法/类型	单值或多值	说明或值
Required-Individual-User-Auth	支持	49	整数	单值	0 = 已禁用 1 = 已启用
Require-HW-Client-Auth	支持	48	布尔值	单值	0 = 已禁用 1 = 已启用
Secondary-DNS	支持	6	字符串	单值	IP 地址
Secondary-WINS	支持	8	字符串	单值	IP 地址
SEP-Card-Assignment		9	整数	单值	未使用
Session Subtype	支持	152	整数	单值	0 = 无 1 = 无客户端 2 = 客户端 3 = 仅客户端 Session Subtype 的适用条件是 Session Type (1 性仅具有以下值：1、2、3 和 4。
Session Type	支持	151	整数	单值	0 = 无1 = AnyConnect 客户端 SSL VPN 2 = AnyConnect 客户端 IPSec VPN (IKEv2) 3 = 无 SSL VPN 4 = 无客户端邮件代理5 = 思科 VP 端 (IKEv1) 6 = IKEv1 LAN-LAN 7 = IKEv2 LA 8 = VPN 负载均衡
Simultaneous-Logins	支持	2	整数	单值	0 到 2147483647
Smart-Tunnel	支持	136	字符串	单值	智能隧道的名称
Smart-Tunnel-Auto	支持	138	整数	单值	0 = 已禁用 1 = 已启用 2 = 自动启动
Smart-Tunnel-Auto-Signon-Enable	支持	139	字符串	单值	智能隧道自动登录名称列表（附带域名）
Strip-Realm	支持	135	布尔值	单值	0 = 已禁用 1 = 已启用
SVC-Ask	支持	131	字符串	单值	0 = 已禁用 1 = 已启用 3 = 启用默认服务 5 = 认无客户端 （未使用 2 和 4）
SVC-Ask-Timeout	支持	132	整数	单值	5 到 120 秒
SVC-DPD-Interval-Client	支持	108	整数	单值	0 = 关 5-3600 秒
SVC-DPD-Interval-Gateway	支持	109	整数	单值	0 = 关） 5-3600 秒
SVC-DTLS	支持	123	整数	单值	0 = 错误 1 = 正确
SVC-Keepalive	支持	107	整数	单值	0 = 关 15-600 秒
SVC-Modules	支持	127	字符串	单值	字符串（模块的名称）
SVC-MTU	支持	125	整数	单值	MTU 值 256-1406 字节
SVC-Profiles	支持	128	字符串	单值	字符串（配置文件的名称）

属性名称	威胁防御	属性编号	语法/类型	单值或多值	说明或值
SVC-Rekey-Time	支持	110	整数	单值	0 = 已禁用 1-10080 分钟
Tunnel Group Name	支持	146	字符串	单值	1 到 253 个字符
Tunnel-Group-Lock	支持	85	字符串	单值	隧道组的名称或“none”
Tunneling-Protocols	支持	11	整数	单值	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = I 16 = WebVPN 32 = SVC 64 = IPsec (IKEv 互斥。 0 - 11、16 - 27、32 - 43、48 - 59
Use-Client-Address		17	布尔值	单值	0 = 已禁用 1 = 已启用
VLAN	支持	140	整数	单值	0 到 4094
WebVPN-Access-List	支持	73	字符串	单值	访问列表名称
WebVPN ACL	支持	73	字符串	单值	设备上的 WebVPN ACL 的名称
WebVPN-ActiveX-Relay	支持	137	整数	单值	0 = 已禁用 Otherwise = 已启用
WebVPN-Apply-ACL	支持	102	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Auto-HTTP-Signon	支持	124	字符串	单值	保留
WebVPN-Citrix-Metaframe-Enable	支持	101	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Content-Filter-Parameters	支持	69	整数	单值	1 = Java ActiveX 2 = Java 脚本 4 = 映像 8 的 Cookie
WebVPN-Customization	支持	113	字符串	单值	自定义的名称
WebVPN-Default-Homepage	支持	76	字符串	单值	URL，例如 http://example-example.com
WebVPN-Deny-Message	支持	116	字符串	单值	有效字符串（最多 500 个字符）
WebVPN-Download_Max-Size	支持	157	整数	单值	0x7fffffff
WebVPN-File-Access-Enable	支持	94	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-File-Server-Browsing-Enable	支持	96	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-File-Server-Entry-Enable	支持	95	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	支持	78	字符串	单值	带可选通配符 (*) 的逗号分隔的 DNS/IP *.cisco.com、192.168.1.*、wwwin.cisco.co
WebVPN-Hidden-Shares	支持	126	整数	单值	0 = 无 1 = 可见
WebVPN-Home-Page-Use-Smart-Tunnel	支持	228	布尔值	单值	已启用（如果无客户端主页将通过智能隧

属性名称	威胁防御	属性编号	语法/类型	单值或多值	说明或值
WebVPN-HTML-Filter	支持	69	位图	单值	1 = Java ActiveX 2 = 脚本 4 = 映像 8 = Cook
WebVPN-HTTP-Compression	支持	120	整数	单值	0 = 关 1 = Deflate 压缩
WebVPN-HTTP-Proxy-IP-Address	支持	74	字符串	单值	逗号分隔的 DNS/IP:端口，带 http= 或 https= 前 如 http=10.10.10.10:80、https=11.11.11.11:443
WebVPN-Idle-Timeout-Alert-Interval	支持	148	整数	单值	0 到 30 0 = 已禁用。
WebVPN-Keepalive-Ignore	支持	121	整数	单值	0 到 900
WebVPN-Macro-Substitution	有	223	字符串	单值	无限制。
WebVPN-Macro-Substitution	有	224	字符串	单值	无限制。
WebVPN-Port-Forwarding-Enable	支持	97	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	支持	98	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-HTTP-Proxy	支持	99	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-List	支持	72	字符串	单值	端口转发列表名称
WebVPN-Port-Forwarding-Name	支持	79	字符串	单值	字符串名称（例如，“Corporate-Apps”）。 此文本将替换无客户端门户主页上的默认字 “Application Access”。
WebVPN-Post-Max-Size	支持	159	整数	单值	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	支持	149	整数	单值	0 到 30 0 = 已禁用。
WebVPN Smart-Card-Removal-Disconnect	支持	225	布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-Smart-Tunnel	支持	136	字符串	单值	智能隧道的名称
WebVPN-Smart-Tunnel-Auto-Sign-On	支持	139	字符串	单值	智能隧道自动登录名称列表（附带域名）
WebVPN-Smart-Tunnel-Auto-Start	支持	138	整数	单值	0 = 已禁用 1 = 已启用 2 = 自动启动
WebVPN-Smart-Tunnel-Tunnel-Policy	支持	227	字符串	单值	“e networkname”、“i networkname”或“a 一，其中 networkname 是指智能隧道网络列表 称，e 表示不包含的隧道，i 表示指定的隧道， 所有隧道。
WebVPN-SSL-VPN-Client-Enable	支持	103	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SSL-VPN-Client-Keep- Installation	支持	105	整数	单值	0 = 已禁用 1 = 已启用

属性名称	威胁防御	属性编号	语法/类型	单值或多值	说明或值
WebVPN-SSL-VPN-Client-Required	支持	104	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SSO-Server-Name	支持	114	字符串	单值	有效字符串
WebVPN-Storage-Key	支持	162	字符串	单值	
WebVPN-Storage-Objects	支持	161	字符串	单值	
WebVPN-SVC-Keepalive-Frequency	支持	107	整数	单值	15 到 600 秒，0 = 关闭
WebVPN-SVC-Client-DPD-Frequency	支持	108	整数	单值	5 到 3600 秒，0 = 关闭
WebVPN-SVC-DTLS-Enable	支持	123	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SVC-DTLS-MTU	支持	125	整数	单值	MTU 值为 256 到 1406 个字节。
WebVPN-SVC-Gateway-DPD-Frequency	支持	109	整数	单值	5 到 3600 秒，0 = 关闭
WebVPN-SVC-Rekey-Time	支持	110	整数	单值	4 到 10080 分钟，0 = 关闭
WebVPN-SVC-Rekey-Method	支持	111	整数	单值	0（关闭）、1 (SSL)、2（新隧道）
WebVPN-SVC-Compression	支持	112	整数	单值	0（关闭）、1（Deflate 压缩）
WebVPN-UNIX-Group-ID (GID)	支持	222	整数	单值	有效 UNIX 组 ID
WebVPN-UNIX-User-ID (UID)	支持	221	整数	单值	有效 UNIX 用户 ID
WebVPN-Upload-Max-Size	支持	158	整数	单值	0x7fffffff
WebVPN-URL-Entry-Enable	支持	93	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-URL-List	支持	71	字符串	单值	URL 列表名称
WebVPN-User-Storage	支持	160	字符串	单值	
WebVPN-VDI	支持	163	字符串	单值	设置列表

表 *86:* 发送到 ***Cisco Secure Firewall Threat Defense*** 的 ***RADIUS*** 属性

属性	属性编号	语法、类型	单值或多值	说明或值
Address-Pools	217	字符串	单值	威胁防御 设备上定义的网络对象名称，用于识别将作为地址池供客户端连接远程访问 VPN 时使用的子网。在**对象 (Objects)** 页面上定义网络对象。
Banner1	15	字符串	单值	用户登录时显示的横幅。

属性	属性编号	语法、类型	单值或多值	说明或值
Banner2	36	字符串	单值	用户登录时显示的横幅的第二部分。横幅 2 附加到横幅 1。
可下载 ACL	Cisco-AV-Pair	merge-dacl {before-avpair | after-avpair}		通过 Cisco-AV-Pair 配置来支持。
过滤器 ACL	86, 87	字符串	单值	过滤器 ACL 由 RADIUS 服务器中的 ACL 名称引用。它要求 威胁防御设备上已经存在 ACL 配置，以便可以在 RADIUS 授权期间使用该配置。 86=Access-List-Inbound 87=Access-List-Outbound
Group-Policy	25	字符串	单值	要在连接中使用的组策略。必须在远程访问 VPN **组策略 (Group Policy)** 页面上创建组策略。您可以使用以下其中一种格式： • 组策略名称 • OU = 组策略名称 • OU = 组策略名称；
Simultaneous-Logins	2	整数	单值	允许用户建立的独立并发连接的数量，0 - 2147483647。
VLAN	140	整数	单值	限制用户连接的 VLAN，0 - 4094。还必须在 威胁防御设备的子接口上配置此 VLAN。

您必须将从 ISE 返回的 IE-Proxy-Server-Method 属性的值设置为以下值之一：

- IE_PROXY_METHOD_PACFILE: 8
- IE_PROXY_METHOD_PACFILE_AND_AUTODETECT: 11
- IE_PROXY_METHOD_PACFILE_AND_USE_SERVER: 12
- IE_PROXY_METHOD_PACFILE_AND_AUTODETECT_AND_USE_SERVER: 15

威胁防御 仅当上述值之一用于 IE-Proxy-Server-Method 属性时，才会提供代理设置。

创建或更新连接配置文件的别名

别名包含特定连接配置文件的备用名称或 URL。远程访问 VPN 管理员可以启用或禁用别名和别名 URL。VPN 用户可以在连接到 Cisco Secure Firewall Threat Defense设备时选择别名。可以开启或关闭在此设备上配置的所有连接的别名，以开启或关闭别名显示。您还可以配置别名URL列表，您的终

端在启动远程访问 VPN 连接时可以从该列表中进行选择。如果用户使用别名 URL 进行连接，则系统将使用与别名 URL 匹配的连接配置文件自动记录它们。

过程

步骤 1 选择**设备** > **VPN** > **远程接入**。

步骤 2 点击要修改的策略上的**编辑 (Edit)**。

步骤 3 在要为其创建或更新别名的连接配置文件上点击**编辑 (Edit)**。

步骤 4 点击 **别名**。

步骤 5 要添加别名，请执行以下操作：

a) 点击**别名 (Alias Names)** 下的**添加 (Add)**。
b) 指定 **别名**。
c) 选中每个窗口中的**已启用**复选框以启用别名。
d) 点击**确定**。

步骤 6 要添加别名 URL，请执行以下操作：

a) 点击 **URL 别名 (URL Alias)** 下的**添加 (Add)**。
b) 从列表中选择 **别名 URL** 或创建新的 URL 对象。有关详细信息，请参阅创建 URL 对象，第 1042 页。
c) 选中每个窗口中的**已启用**复选框以启用别名。
d) 点击**确定**。

步骤 7 保存更改。

相关主题

配置连接配置文件设置，第 1149 页

配置远程访问 VPN 的访问接口

访问接口表列出了包含设备接口的接口组和安全区域。它们配置用于远程访问 SSL 或 IPsec IKEv2 VPN 连接。该表显示每个接口组或安全区域的名称、接口使用的接口信任点以及是否启用了数据报传输层安全(DTLS)。

过程

步骤 1 选择**设备** > **VPN** > **远程接入**。

步骤 2 在列表中选择现有的远程接入策略，然后点击相应的**编辑**图标。

步骤 3 点击 **访问接口 (Access Interface)**。

步骤 4 要添加访问接口，请选择 **添加**，并在 **添加访问接口** 窗口中为以下选项指定值：

a) **访问接口** - 选择接口所属的接口组或安全区域。

接口组或安全区域必须是路由类型。远程接入 VPN 连接不支持其他接口类型。

b) 通过选择以下选项将**协议**对象与访问接口关联：

- **启用 IPSet-IKEv2** - 选择此选项可启用 **IKEv2** 设置。
- **启用 SSL** - 选择此选项可启用 **SSL** 设置。
  - 选择**启用数据报传输层安全**。

    选中此选项后，将在接口上启用数据报传输层安全 (DTLS)，并允许 AnyConnect VPN 客户端使用两个同步隧道（一个 SSL 隧道和一个 DTLS 隧道）建立 SSL VPN 连接。

    启用 DTLS 可避免与某些 SSL 连接相关的延迟和带宽问题，并可提高对于数据包延迟敏感的实时应用的性能。

    要配置 SSL 设置以及 TLS 和 DTLS 版本，请参阅 关于 SSL 设置，第 628 页。

    要配置 AnyConnect VPN 客户端的 SSL 设置，请参阅 组策略 AnyConnect 客户端 选项，第 1066 页。
  - 选中 **配置接口特定身份证书** 复选框，然后从下拉列表中选择 **接口身份证书** 。

    如果不选择接口身份证书，则默认使用 **信任点**。

    如果不选择接口身份证书或信任点，则默认使用 **SSL 全局身份证书** 。

c) 点击**确定**以保存更改。

步骤 5 在 **访问设置**下选择以下选项：

- **允许用户选择将登录的连接配置文件**- 如果您有多个连接配置文件，则选择此选项将允许用户在登录期间选择正确的连接配置文件。必须为 **IPsec-IKEv2** VPN 选择此选项。

步骤 6 使用以下选项配置 **SSL 设置**：

- **Web 访问端口号** - 用于 VPN 会话的端口。默认端口为 443。
- **DTLS 端口号** - 要用于 DTLS 连接的 UDP 端口。默认端口为 443。
- **SSL 全域身份证书**-如果未提供 **接口特定身份证书** ，则选定的 **SSL 全局身份证书** 将用于所有关联的接口。

步骤 7 对于 **IPsec-IKEv2 设置**，请从列表中选择 **IKEv2 身份证书** 或添加身份证书。

步骤 8 在 **VPN 流量的访问控制** 部分下，如果要绕过访问控制策略，请选择以下选项：

- **为已解密的流量绕过访问控制策略 (sysopt permit-vpn)** - 默认情况下，已解密流量要经过访问控制策略的检查。启用“为已解密的流量绕过访问控制策略”选项会绕过 ACL 检查，但 VPN 过滤器 ACL 以及从 AAA 服务器下载的身份验证 ACL 仍适用于 VPN 流量。

  注释 如果选择此选项，则无需更新在 Cisco Secure Firewall Threat Defense 设备上更新访问控制策略，第 1143 页中指定的远程接入 VPN 的访问控制策略。

步骤 9 点击**保存**，保存接口更改。

相关主题

接口，第 995 页

配置远程访问 VPN 高级选项

思科 AnyConnect 安全移动客户端 映像

AnyConnect 安全移动客户端 映像

AnyConnect 安全移动客户端通过企业资源的全 VPN 调配为远程用户提供到 威胁防御 设备的安全 SSL 或 IPsec (IKEv2) 连接。如果先前没有安装客户端，远程用户可以输入为在其浏览器中接受无客户端 VPN 连接所配置的接口的 IP 地址，以下载并安装 AnyConnect 客户端。威胁防御设备下载与远程计算机的操作系统匹配的客户端。下载后，客户端安装并建立安全连接。如果先前已安装客户端，当用户进行身份验证时， 威胁防御 设备将检查客户端的版本并在必要情况下升级客户端。

远程访问 VPN 管理员将新的或附加的 AnyConnect 客户端 映像与 VPN 策略相关联。管理员可以取消关联不受支持的或生命周期终止的客户端程序包。

Cisco Secure Firewall Management Center通过使用文件包名称确定操作系统的类型。如果用户重命名文件而不指示操作系统信息，则必须从列表框中选择有效的操作系统类型。

通过访问 Cisco 软件下载中心来下载 AnyConnect 客户端 映像文件。

相关主题

将 AnyConnect 安全移动客户端 映像添加到 Cisco Secure Firewall Management Center，第 1169 页

将 AnyConnect 安全移动客户端 映像添加到 Cisco Secure Firewall Management Center

您可以使用 **AnyConnect 文件**对象将 AnyConnect 安全移动客户端 映像上传到 Cisco Secure Firewall Management Center。有关详细信息，请参阅文件对象，第 1070 页。有关客户端映像的详细信息，请参阅思科 AnyConnect 安全移动客户端 映像，第 1169 页。

过程

步骤 1 选择 **设备 (Devices) > 远程访问 (Remote Access)**，选择并编辑列出的远程访问策略，然后选择**高级 (Advanced)** 选项卡。

步骤 2 点击**添加 (Add)** 以添加 AnyConnect 安全移动客户端 映像。

步骤 3 在 **AnyConnect 映像 (AnyConnect Images)** 对话框的**可用 AnyConnect 映像 (Available AnyConnect Images)**中点击**添加 (Add)**。

步骤 4 为可用的 AnyConnect 映像输入**名称 (Name)** 和**说明 (Description)**（可选）。

步骤 5 点击**浏览 (Browse)**，找到想要上传的客户端映像。

步骤 6 点击**保存 (Save)** 以便将映像上传到 管理中心。

在将客户端映像上传到 Cisco Secure Firewall Management Center 时，会自动显示映像的操作系统信息。

步骤 7 要更改客户端映像的顺序，请点击**显示重新排序按钮 (Show Re-order buttons)**，然后向上或向下移动客户端映像。

相关主题

思科 AnyConnect 安全移动客户端 映像 ，第 1169 页

更新远程接入 VPN 客户端的 AnyConnect 客户端映像

当思科软件下载中心提供新的 AnyConnect 更新时，您可以手动下载软件包并将其添加到远程接入 VPN 策略，以便根据其操作系统在 VPN 客户端系统上升级新的客户端软件包。

开始之前

此部分中的说明可帮助您更新连接 Cisco Secure Firewall Threat Defense VPN 网关的远程接入 VPN 客户端的新 AnyConnect 客户端映像。更新 AnyConnect 映像之前，确保完成以下配置：

- 从思科软件下载中心下载最新的 AnyConnect 映像文件。
- 在 Cisco Secure Firewall Management Center Web 界面上，转至 **对象 (Objects)** > **对象管理 (Object Management)** > **VPN** > **AnyConnect 文件 (AnyConnect File)** ，然后添加新的 AnyConnect 客户端映像文件。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备** > **VPN** > **远程接入**。

步骤 2 点击要编辑的远程访问 VPN 策略旁边的**编辑 (Edit)** 。

步骤 3 点击**高级 (Advanced)** > **AnyConnect 客户端映像 (AnyConnect Client Images)** > **添加 (Add)**。

步骤 4 从**可用的 AnyConnect 映像 (Available AnyConnect Images)** 中选择客户端图像文件，然后点击**添加 (Add)**。

如果未列出所需的客户端映像，点击**添加 (Add)** 浏览并上传映像。

步骤 5 点击**确定 (OK)**。

步骤 6 保存远程访问 VPN 策略。

在部署远程访问 VPN 策略更改之后，新的 AnyConnect 映像将在 Cisco Secure Firewall Threat Defense 设备上更新，该设备配置为远程接入 VPN 网关。当新的 VPN 用户连接到 VPN 网关时，用户将根据客户端系统的操作系统获取要下载的新 AnyConnect 客户端 映像。对于现有 VPN 用户， AnyConnect 客户端 映像将在其下一个 VPN 会话中更新。

将思科 AnyConnect 外部浏览器软件包添加到 Cisco Secure Firewall Management Center

如果您的本地磁盘上有一个 AnyConnect 外部浏览器软件包镜像，请使用此程序将其上传到 Cisco Secure Firewall Management Center。上传外部浏览器软件包后，您可以为远程访问 VPN 连接更新外部浏览器软件包。

您可以使用 **AnyConnect**对象将外部浏览器软件包文件上传到 Cisco Secure Firewall Management Center。有关详细信息，请参阅文件对象，第 1070 页。

要点回顾

- 只能向 威胁防御 设备添加一个外部浏览器软件包。
- 将外部浏览器软件包添加到 管理中心 后，只有在远程接入 VPN 配置中启用外部浏览器后，才会将浏览器推送到 威胁防御。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备 (Devices)** > **远程访问 (Remote Access)**，选择并编辑列出的远程访问策略，然后选择**高级 (Advanced)** 选项卡。

步骤 2 在**AnyConnect 客户端映像 (AnyConnect Client Images)** 页面的 **AnyConnect 外部浏览器软件包 (AnyConnect External Browser Package)** 部分中点击**添加 (Add)**。

步骤 3 输入 AnyConnect 软件包的**名称 (Name)** 和**说明 (Description)**。

步骤 4 点击**浏览 (Browse)** 并找到要上传的外部浏览器软件包文件。

步骤 5 点击**保存 (Save)** 以便将映像上传到 Cisco Secure Firewall Management Center。

注释 如果要使用现有外部浏览器软件包来更新远程访问 VPN 连接，请从**软件包文件 (Package File)** 下拉列表中选择该文件。

步骤 6 保存远程访问 VPN 策略。

相关主题

思科 AnyConnect 安全移动客户端 映像，第 1169 页

远程接入 VPN 地址分配策略

威胁防御设备可以使用 IPv4 或 IPv6 策略将 IP 地址分配给远程接入 VPN 客户端。如已配置多个地址分配方法，则 威胁防御设备将尝试每一个选项，直到找到一个 IP 地址为止。

IPv4 或 IPv6 策略

您可以使用 IPv4 或 IPv6 策略对远程接入 VPN 客户端的 IP 地址进行寻址。首先，您必须尝试使用 IPv4 策略，然后再尝试使用 IPv6 策略。

- **使用授权服务器** - 在每个用户的基础上从外部授权服务器检索地址。如果使用已配置 IP 地址的授权服务器，建议使用此方法。只有基于 RADIUS 的授权服务器支持地址分配。AD/LDAP 则不支持。此方法适用于 IPv4 和 IPv6 分配策略。

- **使用 DHCP** - 从在连接配置文件中配置的 DHCP 服务器获取 IP 地址。您还可以通过在组策略中配置 DHCP 网络范围来定义 DHCP 服务器可以使用的 IP 地址的范围。如果使用 DHCP，则在**对象 > 对象管理 > 网络**窗格中配置服务器。此方法适用于 IPv4 分配策略。

  有关 DHCP 网络范围配置的详细信息，请参阅组策略常规选项，第 1064 页。

- **使用内部地址池** - 内部配置的地址池是分配地址池以进行配置的最简单方法。如果使用此方法，请在**对象 > 对象管理 > 地址池**窗格中创建 IP 地址池，并在连接配置文件中做出相同的选择。此方法适用于 IPv4 和 IPv6 分配策略。

- **允许释放 IP 地址一段时间之后对其重新使用** - 在 IP 地址返回到地址池之后，延迟一段时间方可重新使用。增加延迟有助于防止防火墙在快速重新分配 IP 地址时遇到的问题。默认情况下，延迟设置为零。如果要延长延迟，请输入取值范围为 0 至 480 内的分钟数，以便延迟 IP 地址重新分配。此配置元素适用于 IPv4 分配策略。

相关主题

配置连接配置文件设置，第 1149 页
远程访问 VPN 身份验证，第 1134 页

配置证书映射

通过证书映射，您可以根据证书的字段内容定义匹配连接配置文件的用户证书的规则。证书映射提供安全网关上的证书身份验证。

规则或证书映射在证书映射对象，第 1072 页中定义。

过程

步骤 1 选择**设备 > VPN > 远程接入**。

步骤 2 在列表中选择现有的远程接入策略，然后点击相应的**编辑**图标。

步骤 3 选择 **高级 > 证书映射**。

步骤 4 从**连接配置文件映射的常规设置 (General Settings for Connection Profile Mapping)** 窗格中选择以下选项：

选择是基于优先级的，如果没有找到第一个选择的匹配项，则继续向下匹配列表中的选项。当满足规则时，匹配完成。如果不满足规则，则使用默认的连接配置文件（在底部列出）用于此连接。选择以下任意选项或所有选项，以建立身份验证并确定应映射到客户端的连接配置文件（隧道组）。

- **如果组 URL 和证书映射匹配不同的连接配置文件，则使用组 URL**。
- **使用配置的规则将证书匹配到连接配置文件 (Use the configured rules to match a certificate to a Connection Profile)** - 启用此功能可以使用连接配置文件映射中定义的规则。

注释 配置证书映射意味着采用基于证书的身份验证方法。系统将提示远程用户输入客户端证书，而不考虑配置的身份验证方法。

步骤 5 在**证书到连接配置文件映射 (Certificate to Connection Profile Mapping)** 部分下，点击**添加映射 (Add Mapping)**，以便为此策略创建证书到连接配置文件的映射。

a) 选择或创建**证书映射名称**对象。

b) 选择当满足证书映射对象中的规则时想要使用的**连接配置文件**。

c) 点击**确定 (OK)** 以创建映射。

步骤 6 点击**保存 (Save)**。

配置组策略

组策略是存储在组策略对象中的一组属性和值对，用于定义远程接入VPN体验。例如，在组策略对象中，可以配置地址、协议和连接设置等常规属性。

在建立VPN隧道时，将确定应用于用户的组策略。RADIUS授权服务器将会分配组策略，或从当前连接配置文件中获取。

注释 威胁防御 上没有任何组策略继承属性。对于用户使用完整的组策略对象。使用登录时 AAA 服务器识别的组策略对象；如果未指定组策略对象，则使用为VPN连接配置的默认组策略。提供的默认组策略可以设置为默认值，但仅在将该策略分配给连接配置文件且用户未识别其他组策略时使用该策略。

过程

步骤 1 选择**设备** > **VPN** > **远程接入**。

步骤 2 在列表中选择现有的远程接入策略，然后点击相应的**编辑**图标。

步骤 3 选择**高级 (Advanced)** > **组策略 (Group Policies)** > **添加 (Add)**。

步骤 4 从**可用组策略 (Available Group Policy)** 列表中选择组策略并点击**添加 (Add)**。您可以选择与此远程访问 VPN 策略关联的一个或多个组策略。

步骤 5 点击 **OK** 以完成组策略选择。

步骤 6 保存更改。

相关主题

配置组策略对象 ， 第 1063 页

配置 LDAP 属性映射

LDAP 属性名称将 LDAP 用户或组属性名称映射到 Cisco 可理解的名称。属性映射将 Active Directory（AD）或 LDAP 服务器中存在的属性与 Cisco 属性名称等同起来。您可以将任何标准 LDAP 属性映射到公认的供应商特定属性 (VSA)。您可以将一个或多个 LDAP 属性映射到一个或多个 Cisco LDAP 属性。当 AD 或 LDAP 服务器在远程访问 VPN 连接建立期间向 威胁防御 设备返回身份验证时， 威胁防御 设备可以使用该信息调整 AnyConnect 客户端 如何完成连接。

当您想要为 VPN 用户提供不同的访问权限或 VPN 内容时，您可以在 VPN 服务器上配置不同的 VPN 策略，并根据其凭证将这些策略集分配给每个用户。您可以在 威胁防御 中通过使用 LDAP 属性映射配置 LDAP 授权来实现此目的。要使用 LDAP 将组策略分配给用户，您必须配置映射 LDAP 属性的映射。

LDAP 属性映射包括三个组件：

- **领域 (Realm)** - 指定 LDAP 属性映射的名称；名称根据所选领域生成。
- **属性名称映射 (Attribute Name Map)** - 将 LDAP 用户或组属性名称映射到 Cisco 可理解的名称。
- **属性值映射 (Attribute Value Map)** - 将 LDAP 用户或组属性中的值映射到所选名称映射的 Cisco 属性值.

LDAP 属性映射中使用的组策略将被添加到远程访问 VPN 配置中的组策略列表。从远程访问 VPN 配置中删除组策略也会删除相关的 LDAP 属性映射。

过程

步骤 1 选择**设备** > **VPN** > **远程接入**。

步骤 2 在列表中选择现有的远程接入策略，然后点击相应的**编辑**图标。

步骤 3 点击 **高级** > **LDAP 属性映射**。

步骤 4 点击**添加 (Add)**。

步骤 5 在配置 LDAP 属性映射页面上，选择要配置属性映射的 **领域** 。

步骤 6 点击**添加 (Add)**。

您可以配置多个属性映射。每个属性映射都要求您配置名称映射和值映射。

注释 确保在创建 LDAP 属性映射时遵循以下准则：

- 为 LDAP 属性至少配置一个映射；不允许多个具有相同 LDAP 属性名称的映射。
- 配置至少一个名称映射以创建 LDAP 属性映射。
- 如果属性映射未与远程访问 VPN 配置中的任何连接配置文件关联，您可以删除任何 LDAP 属性映射。
- 对 与 Cisco 和 LDAP 属性名称和值使用 LDAP 属性映射中的正确拼写和大写。

a) 指定 **LDAP 属性名称** ，然后从列表中选择所需的 **Cisco 属性名称** 。

b) 点击 **添加值映射** 并指定 **LDAP 属性值** 和 **Cisco 属性值**。

重复此步骤以添加更多值映射。

步骤 7 点击 **OK** 以完成 LDAP 属性映射配置。

步骤 8 点击 **保存** 以保存对 LDAP 属性映射的更改。

相关主题

配置远程访问 VPN 的 AAA 设置，第 1151 页
了解权限和属性的策略实施，第 1136 页

配置 VPN 负载均衡

关于 VPN 负载均衡

威胁防御 中的 VPN 负载均衡允许您对两台或更多设备进行逻辑分组，并在设备之间平均分配远程接入 VPN 会话。VPN 负载均衡会在负载均衡组中的设备之间共享 AnyConnect 客户端 VPN 会话。

VPN 负载均衡基于简单的流量分配，而不考虑吞吐量或其他因素。VPN 负载均衡组由两台或更多威胁防御 设备组成。一台设备充当导向器，而其他设备是成员设备。组中的设备不需要是完全相同的类型，也不需要具有相同的软件版本和配置。支持远程接入 VPN 的任何 威胁防御 设备都可以加入负载均衡组。 威胁防御 支持使用 AnyConnect AnyConnect SAML 身份验证进行 VPN 负载均衡。

VPN 负载均衡组中的所有主用设备都会承载会话负载。VPN 负载均衡可以将流量定向至组中负载最低的设备，在所有设备之间分配负载。这样可以高效地利用系统资源，提供更高的性能和高可用性。

VPN 负载均衡的组件

以下是 VPN 负载均衡的组件：

- **负载均衡组 (Load-balancing group)** - 由两台或多台 威胁防御 设备组成的虚拟组，用于共享 VPN 会话。

  VPN 负载均衡组可以包含相同版本或混合版本的 威胁防御 设备；但设备必须要支持远程接入 VPN 配置。

  请参阅配置 VPN 负载均衡的组设置，第 1176 页和配置负载均衡的其他设置，第 1177 页。

- **导向器 (Director)** - 由组中的一个设备充当导向器。它会在组中的其他成员之间分配负载，并参与为 VPN 会话提供服务。

  导向器会监控组中的所有设备、追踪每台设备的负载情况，然后相应地分配会话负载。导向器的角色不会与某台物理设备绑定；它可以在设备之间切换。例如，如果当前的导向器发生故障，该组的一台成员设备会接管该角色，立即成为新的导向器。

- **成员 (Members)** - 组中除导向器以外的设备均被称为成员。它们会参与负载均衡并共享远程接入 VPN 连接。

  配置参与设备的设置，第 1177 页。

VPN 负载均衡的必备条件

- **证书 (Certificates)** - 威胁防御 的证书必须包含连接重定向到的导向器和成员的 IP 地址或 FQDN。否则，证书将被视为不可信。证书必须使用使用者替代名称 (SAN) 或通配符证书

- **组 URL (Group URL)** - 在连接配置文件中添加 VPN 负载均衡组 IP 地址的组 URL。指定组 URL，以便用户在登录时无需再选择组。

- **IP 地址池 (IP Address Pool)** - 为成员设备选择唯一的 IP 地址池，并覆盖 管理中心 中每个成员设备的 IP 池。
- 网络地址转换 (NAT) 后面的设备也可以作为负载均衡组的一部分。

VPN 负载均衡准则和限制

- 默认情况下会禁用 VPN 负载均衡。您必须显式启用 VPN 负载均衡。
- 只有协同定位的 威胁防御 设备才能被添加到负载均衡组中。
- 一个负载均衡组必须至少有两台 威胁防御 设备。
- 威胁防御 高可用性的设备可以加入负载均衡组。
- 网络地址转换 (NAT) 后面的设备也可以作为负载均衡组的一部分。
- 当成员或导向器设备发生故障时，该设备提供的远程接入VPN连接会被丢弃。您必须再次启动 VPN 连接。
- 每台设备上的身份证书必须具有使用者替代名称 (SAN) 或通配符。

配置 VPN 负载均衡的组设置

您可以启用VPN负载均衡，并配置适用于负载均衡组所有成员的组设置。在创建组时，您可以配置负载均衡的参与设置。

过程

步骤 1 选择**设备** > **VPN** > **远程接入**。

步骤 2 点击要编辑的远程访问 VPN 策略旁边的**编辑 (Edit)**。

步骤 3 点击**高级 (Advanced)** > **负载均衡 (Load Balancing)**。

步骤 4 点击**启用成员设备之间的负载均衡 (Enable Load balancing between member devices)** 切换按钮以启用负载均衡。
系统将打开**编辑组配置 (Edit Group Configuration)** 页面。组参数适用于负载均衡组下的所有设备。

步骤 5 如果适用，请指定**组 IPv4 地址 (Group IPv4 Address)** 和**组 IPv6 地址 (Group IPv6 Address)**。
此处指定的 IP 地址用于整个负载均衡组，而导向器将为传入 VPN 连接打开此 IP 地址。

步骤 6 为负载均衡组选择**通信接口 (Communication Interface)**。点击**添加 (Add)** 以添加接口组或安全区域。
通信接口是一个专用接口，导向器和成员都会通过该接口共享有关其负载的信息。

步骤 7 输入用于在组中的导向器和成员之间进行通信的 **UDP 端口** 。默认端口为 9023。

步骤 8 启用**IPsec 加密 (IPsec Encryption)**切换按钮，为导向器和成员之间的通信激活 IPsec 加密。
启用加密后会使用预共享密钥在导向器和成员之间建立 IKEv1/IPsec 隧道。

步骤 9 输入用于 IPsec 加密的**加密密钥**。

步骤 10 点击**确定 (OK)**。

配置负载均衡的其他设置

VPN 负载均衡的其他设置包括 FQDN 和 IKEv2 重定向。

过程

步骤 1 选择**设备** > **VPN** > **远程接入**。

步骤 2 点击要编辑的远程访问 VPN 策略旁边的**编辑 (Edit)** 。

步骤 3 点击**高级 (Advanced)** > **负载均衡 (Load Balancing)**。

步骤 4 如果已经完成，打开**启用成员设备之间的负载均衡 (Enable Load balancing between member devices)** 切换按钮以启用负载均衡。

步骤 5 点击**设置**。

步骤 6 打开**将 FQDN 发送到对等设备而不是 IP (Send FQDN to peer devices instead of IP)** 切换按钮以启用使用完全限定域名的重定向。

默认情况下，威胁防御 只会将 VPN 负载均衡重定向中的 IP 地址发给客户端。

步骤 7 选择 **IKEv2 重定向 (IKEv2 Redirect)** 阶段之一：

- **在 SA 身份验证期间重定向**
- **在 SA 初始化期间重定向**

步骤 8 点击**确定**。

步骤 9 保存更改。

配置参与设备的设置

设备参与设置将确定设备如何在 VPN 负载均衡中共享负载。在设备上启用 VPN 负载均衡，并定义设备特定属性，从而配置参与设备。这些值因设备而异。您可以为参与负载均衡的设备提供优先级编号。优先级越高，设备就越有可能成为导向器，而不是其他设备。但您不能选择某个设备作为该组的导向器。

过程

步骤 1 选择**设备** > **VPN** > **远程接入**。

步骤 2 点击要编辑的远程接入 VPN 策略旁边的**编辑 (Edit)**。

步骤 3 点击**高级 (Advanced)** > **负载均衡 (Load Balancing)**。

步骤 4 如果尚未启用负载均衡，打开**启用成员设备之间的负载均衡 (Enable Load balancing between member devices)** 切换按钮以启用负载均衡。

步骤 5 配置**设备参与 (Device Participation)** 设置：

设备参与 (Device Participation) 部分列出了所选远程访问 VPN 配置的目标设备。可以配置这些设备，为分担传入 VPN 会话的负载。

a) 打开**负载均衡 (Load Balancing)** 切换按钮，为设备启用负载均衡，然后点击**编辑 (Edit)**。
b) 输入设备**优先级**。

默认情况下，设备优先级会被设为 5。您可以从 1 到 10 中选择一个数字。

c) 如果设备位于 NAT 之后，请为 VPN 接口 IP 地址指定 **IPv4 NAT** 或 **IPv6 NAT** 地址。
d) 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)** 以保存远程访问 VPN 策略设置。

配置远程接入 VPN 的 IPsec 设置

只有在配置远程接入 VPN 策略时选择 IPsec 作为 VPN 协议时，IPsec 设置才适用。否则，可以使用“编辑访问接口”对话框启用 IKEv2。有关详细信息，请参阅配置远程访问 VPN 的访问接口，第 1167 页。

过程

步骤 1 选择**设备** > **VPN** > **远程接入**。
步骤 2 从可用 VPN 策略列表中，选择要修改其设置的策略。
步骤 3 点击 **Advanced**。

IPsec 设置列表将显示在屏幕左侧的导航窗格中。

步骤 4 使用导航窗格编辑下列 IPsec 选项：

a) **加密映射** -“加密映射”页面列出了在其上启用了 IKEv2 协议的接口组。启用 IKEv2 协议的接口将自动生成加密映射。要编辑加密映射，请参阅配置远程接入 VPN 加密映射，第 1179 页。可在**访问接口 (Access Interface)** 中，为选定的 VPN 策略添加或删除接口组。有关详细信息，请参阅配置远程访问 VPN 的访问接口，第 1167 页。
b) **IKE 策略 (IKE Policy)** - 当 AnyConnect 终端使用 IPsec 协议进行连接时，“IKE 策略”(IKE Policy) 页面将列出适用于所选 VPN 策略的所有 IKE 策略对象。有关详细信息，请参阅 远程接入 VPN 中的 IKE 策略，第 1181 页。要添加新的 IKE 策略，请参阅 配置 IKEv2 策略对象，第 1059 页。威胁防御 仅支持 AnyConnect IKEv2 客户端。不支持第三方标准 IKEv2 客户端。
c) **IPsec/IKEv2 参数** -“IPsec/IKEv2 参数”页面使您可以修改 IKEv2 会话设置、IKEv2 安全关联设置、IPsec 设置和 NAT 透明度设置。有关详细信息，请参阅配置远程访问 VPN IPsec/IKEv2 参数，第 1182 页。

步骤 5 点击**保存 (Save)**。

配置远程接入 VPN 加密映射

对于已启用 IPsec-IKEv2 协议的接口，将自动生成加密映射。可在**访问接口 (Access Interface)** 中，为选定的 VPN 策略添加或删除接口组。有关详细信息，请参阅配置远程访问 VPN 的访问接口，第 1167 页。

过程

步骤 1 选择**设备** > **VPN** > **远程接入**。

步骤 2 从可用 VPN 策略列表中，选择要修改其设置的策略。

步骤 3 点击**高级 (Advanced)** > **加密映射 (Crypto Maps)**，选择表中的一行并点击**编辑 (Edit)** 以编辑加密映射选项。

步骤 4 选择 **IKEv2 IPsec 提议 (IKEv2 IPsec Proposals)** 并选择对指定将使用哪些身份验证和加密算法来保护隧道中的流量安全的集合进行转换。

步骤 5 选择**启用反向路由注入 (Enable Reverse Route Injection)** 以启用静态路由自动插入到受远程隧道终端保护的网络和主机的路由进程中。

步骤 6 选择**启用客户端服务 (Enable Client Services)** 并指定端口号。

客户端服务服务器提供 HTTPS (SSL) 访问，以允许 AnyConnect下载程序接收软件升级、配置文件、本地化和自定义文档、CSD、SCEP 以及客户端所需的其他文件下载。如果选择此选项，请指定客户端服务端口号。如果不启用客户端服务服务器，用户将无法下载 AnyConnect可能需要的任何文件。

注释 您可以使用与在同一设备上运行的 SSL VPN 相同的端口。即使配置了 SSL VPN，您也必须选择此选项，以便通过 SSL 为 IPsec-IKEv2 客户端启用文件下载。

步骤 7 选择**启用完全向前保密 (Enable Perfect Forward Secrecy)**，然后选择**模数组 (Modulus group)**。

使用完美前向保密 (PFS) 为每个加密交换生成和使用唯一会话密钥。唯一会话密钥可保护交换免于后续解密，即使整个交换已被记录且攻击者已经获得终端设备使用的预共享或私有密钥。如果选择此选项，也请选择在**模数组 (Modulus Group)** 列表中生成 PFS 会话密钥时使用的 Diffie-Hellman 密钥导出算法。

模数组是用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。选择要在远程接入 VPN 配置中允许的模数组。

- 1 - Diffie-Hellman 组 1（768 位模数）。
- 2 - Diffie-Hellman 组 2（1024 位模数）。
- 5 - Diffie-Hellman 组 5（1536 位模数，可为 128 为密钥提供较好的保护，但组 14 更好）。如果使用的是 AES 加密，请使用此组（或更高的组）。
- 14 - Diffie-Hellman 组 14（2048 位模数，可为 128 为密钥提供较好的保护）。
- 19 - Diffie-Hellman 组 19（256 位椭圆曲线字段大小）。
- 20 - Diffie-Hellman 组 20（384 位椭圆曲线字段大小）。

- 21 - Diffie-Hellman 组 21（521 位椭圆曲线字段大小）。
- 24 - Diffie-Hellman 组 24（2048 位模数和 256 位素数阶子组）。

步骤 8 指定**生命周期持续时间（秒）(Lifetime Duration [seconds])**。

安全关联 (SA) 的生命周期（以秒为单位）。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，持续期限越短（某种程度上），IKE 协商就越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。

可指定 120 到 2147483647 秒之间的值。默认值为 28800 秒。

步骤 9 指定**生命周期大小（千字节）(Lifetime Size [kbytes])**。

使用特定安全关联的 Ipsec 对等体之间在该安全关联到期前可通过的流量（以千字节为单位）。

可指定 10 到 2147483647 千字节之间的值。默认值为 4,608,000 千字节。没有规范允许使用无限数据。

步骤 10 选择以下 **ESPv3 设置 (ESPv3 Settings)**：

- **验证传入 ICMP 错误消息 (Validate incoming ICMP error messages)** - 选择是否验证通过 IPsec 隧道接收，并发往专用网络上的内部主机的 ICMP 错误消息。
- **启用“不分段”策略 (Enable 'Do Not Fragment' Policy)** - 定义 IPsec 子系统如何处理大型数据包，这些数据包在 IP 报头中设置了不分片 (DF) 位，然后从**策略 (Policy)** 列表选择以下一项。
  - 复制 - 维护 DF 位。
  - 清除 - 忽略 DF 位。
  - 设置 - 设置和使用 DF 位。
- 选择**启用数据流机密性 (TFC) 数据包 (Enable Traffic Flow Confidentiality [TFC] Packets)** - 启用虚拟 TFC 数据包，这些数据包会通过隧道，用于屏蔽流量配置文件。可以使用 **Burst**、**Payload Size** 和 **Timeout** 参数生成穿过指定 SA 的随机长度的数据包。

  注释 启用流量保密性 (TFC) 数据包可防止 VPN 隧道处于空闲状态。因此，如果启用了 TFC 数据包，则组策略中配置的 VPN 空闲超时不会按预期工作。请参阅组策略高级选项，第 1069 页。

  - 突发 - 指定 1 到 16 字节之间的值。
  - 负载大小 - 指定 64 到 1024 字节之间的值。
  - 超时 - 指定 10 到 60 秒之间的值。

步骤 11 点击**确定 (OK)**。

相关主题

接口，第 995 页

远程接入 VPN 中的 IKE 策略

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用提议。IKE 提议是一组两个对等体用于保护其之间的协商的算法。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数用于保护后续 IKE 协商。

注释 威胁防御仅支持将 IKEv2 用于远程接入 VPN。

与 IKEv1 不同，在 IKEv2 方案中，您可以在一个策略中选择多个算法和模数组。由于对等体在第 1 阶段协商期间进行选择，因此可创建单个 IKE 方案，但是考虑创建多个不同的方案，以向最需要的方案提供更高的优先级。对于 IKEv2，策略对象不指定身份验证，其他策略必须定义身份验证要求。

当配置远程接入 IPsec VPN 时，需要 IKE 策略。

配置远程接入 *VPN IKE* 策略

IKE 策略表指定，当 AnyConnect端点使用 IPsec 协议进行连接时适用于所选 VPN 配置的所有 IKE 策略对象。有关详细信息，请参阅远程接入 VPN 中的 IKE 策略，第 1181 页。

注释 威胁防御仅支持用于远程接入 VPN 的 IKEv2。

过程

步骤 1 选择**设备** > **VPN** > **远程接入**。

步骤 2 从可用 VPN 策略列表中，选择要修改其设置的策略。

步骤 3 点击**高级 (Advanced)** > **IKE 策略 (IKE Policy)**。

步骤 4 点击**添加 (Add)** 从可用的 IKEv2 策略中选择，或添加新的 IKEv2 策略并指定以下选项：

- **名称 (Name)** - IKEv2 策略的名称。
- **说明 (Description)** - IKEv2 策略的可选说明
- **优先级** — 当尝试查找常见安全关联 (SA) 时，优先级值可确定两个协商对等体比较的 IKE 策略顺序。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）
- **完整性 (Integrity)** - IKE 策略中使用的散列算法的完整性算法部分。
- **加密 (Encryption)** - 用于建立第 1 阶段 SA（用于保护第 2 阶段协商）的加密算法。

- **PRF 散列 (PRF Hash)** - IKE 策略中使用的散列算法的伪随机函数 (PRF) 部分。在 IKEv2 中，您可以为这些元素指定不同的算法。
- **DH 组 (DH Group)** - 用于加密的 Diffie-Hellman 组。

步骤 5 点击**保存 (Save)**。

配置远程访问 VPN IPsec/IKEv2 参数

过程

步骤 1 选择**设备** > **VPN** > **远程接入**。

步骤 2 从可用 VPN 策略列表中，选择要修改其设置的策略。

步骤 3 点击 **高级** > **IPsec**> **IPsec/IKEv2 参数**。

步骤 4 为 **IKEv2 会话设置**选择以下选项：

- **发送至对等体的身份**-选择对等体将在 IKE 协商期间用于标识自身的身份：
  - **自动**-按连接类型确定 IKE 协商：用于预共享密钥的 IP 地址或用于证书身份验证的证书 DN（不受支持）。
  - **IP 地址**-使用交换 ISAKMP 身份信息的主机的 IP 地址。
  - **主机名称**-使用交换 ISAKMP 身份信息的主机的完全限定域名 (FQDN)。此名称包含主机名和域名。
- **在断联隧道上启用通知**-当 SA 上接收的入站数据包与该 SA 的流量选择器不匹配时，允许管理员启用或禁用向对等体发送 IKE 通知。默认情况下会禁用发送此通知。
- **请勿允许设备重新引导直至所有会话被终止**-选中以支持等待所有活动在系统重启之前自动终止。默认情况下将禁用此复选框。

步骤 5 为 **IKEv2 安全关联 (SA) 设置**选择以下选项：

- **Cookie 质询**-是否向对等体设备发送 Cookie 质询，以响应 SA 发起的数据包，这可以帮助阻止拒绝服务 (DoS) 攻击。默认情况下，当 50% 的可用 SA 正在协商时使用 Cookie 质询。选择以下选项之一：
  - **自定义**-指定 **向质询传入 Cookie 发出挑战的阈值**，这是指允许进行协商的总 SA 数的百分比。这将对未来的任何 SA 协商都触发 Cookie 质询。范围为 0 到 100%。默认为 50%。
  - 始终-始终选择向对等设备发送 cookie 质询。
  - 从不-选择从不向对等设备发送 cookie 质询。
- **允许协商的 SA 数量**-限制可以随时协商的 SA 的最大数量。如果与 Cookie 质询配合使用，可以配置低于此限制的 Cookie 质询阈值，以便实现有效的交叉检查。默认为 100 %。

- **允许的最大 SA 数量**-限制 ASA 上允许的 IKEv2 连接的数量。

步骤 6 为 **IPsec 设置**选择以下选项：

- **解密前启用分片**-此选项允许流量通过不支持 IP 分片的 NAT 设备。这不影响支持 IP 分片的 NAT 设备的运行。
- **路径最大传输单元老化**-选中以启用 PMTU（路径最大传输单元）老化，设置 SA（安全关联）的 PMTU 的间隔。
- **值重置间隔**-输入 SA（安全关联）的 PMTU 值重置为其原始值的分钟数。有效范围是 10 到 30 分钟，默认值为不受限制。

步骤 7 为 **NAT 设置**选择以下选项：

- **保持连接消息穿越** - 选择是否启用 NAT 保持连接消息穿越。NAT 遍历保持连接用于在 VPN 连接的中心和分支之间存在设备（中间设备）并且该设备对 IPsec 流执行 NAT 时，传输保持连接消息时。如果选择此选项，请配置在分支和中间设备之间发送的保持连接信号之间的间隔（以秒为单位），以指示会话处于活动状态。此值可以介于 10 到 3600 秒之间。默认值为 20 秒。
- **间隔**-设置 NAT 保持连接间隔，范围从 10 秒到 3600 秒。默认值为 20 秒。

步骤 8 点击**保存 (Save)**。

配置 AnyConnect 管理 VPN 隧道

只要客户端系统通电，管理 VPN 隧道就会提供与企业网络的连接，而无需 VPN 用户连接到 VPN。这有助于组织通过软件补丁和更新让终端保持最新状态。在建立用户发起的VPN隧道后，管理隧道将断开连接。

本部分提供有关在 威胁防御上配置 AnyConnect 管理 VPN 隧道的信息。使用 管理中心 Web 界面在威胁防御 上配置 AnyConnect 管理隧道需要以下设置：

- 具有基于证书的身份验证和组 URL 的**连接配置文件**。
- **为服务器配置了组 URL 和备份服务器（如果需要）的AnyConnect 管理 VPN 配置文件**。
- 包含管理 VPN 配置文件（其中明确包含网络的分割隧道、客户端绕行协议且无横幅）的**组策略**。

有关配置 AnyConnect 管理 VPN 隧道的详细说明，请参阅 在 威胁防御 上配置 AnyConnect 管理 VPN 隧道 ， 第 1184 页。

AnyConnect 管理 VPN 隧道的要求和前提条件

软件和配置要求

在使用 威胁防御 Web 界面在 管理中心 上配置 AnyConnect 管理隧道之前，请确保您已具备以下条件：

- 确保您使用的是 威胁防御 和 管理中心 版本 6.7.0 或更高版本。
- 下载AnyConnect VPN Webdeploy 软件包 4.7 或更高版本，并将其上传到 威胁防御 远程访问 VPN。
- 确保在连接配置文件中配置证书身份验证。
- 确保未在组策略中配置横幅。
- 检查管理隧道组策略中的分割隧道配置。

证书要求

- 威胁防御 必须具有远程访问 VPN 的有效身份证书，并且 威胁防御 上必须存在来自本地证书颁发机构 (CA) 的根证书。
- 连接到管理 VPN 隧道的终端必须具有有效的身份证书。
- 威胁防御 的身份证书的 CA 证书必须安装在终端上，而终端的 CA 证书必须安装在 威胁防御 上。
- 同一本地 CA 颁发的身份证书必须存在于计算机存储区中。

  证书存储区（适用于 Windows）和/或系统密钥链中（适用于 macOS）。

AnyConnect 管理 VPN 隧道的限制

- AnyConnect 管理 VPN 隧道仅支持证书身份验证，而不支持基于 AAA 的身份验证。
- 不支持公共或专用代理设置。
- 在已连接管理 VPN 隧道时，不支持 AnyConnect 客户端升级和 AnyConnect 模块下载。

在 威胁防御 上配置 AnyConnect 管理 VPN 隧道

过程

步骤 1 使用向导来创建远程访问 VPN 策略配置：

有关配置远程访问 VPN 的信息，请参阅配置新的远程访问 VPN 连接，第 1140 页。

步骤 2 配置管理 VPN 隧道的连接配置文件设置：

注释　建议创建仅用于 AnyConnect 管理 VPN 隧道的新连接配置文件。

a) 编辑已创建的远程访问 VPN 策略。
b) 选择并编辑将用于管理 VPN 隧道的连接配置文件。
c) 点击 **AAA** > **身份验证方法 (Authentication Method)** 并选择**仅限客户端证书 (Client Certificate Only)**。根据需要配置授权和记账设置。
d) 点击连接配置文件的**别名 (Aliases)** 选项卡。
e) 在连接配置文件的 URL 别名和 **URL 别名**下，点击**添加 (+) (Add [+])**。
f) 点击**启用 (Enabled)** 以启用 URL。
g) 点击**确定 (OK)**，然后点击**保存 (Save)** 以保存连接配置文件设置。

有关连接配置文件设置的详细信息，请参阅配置连接配置文件设置，第 1149 页。

步骤 3 使用 **AnyConnect配置文件编辑器来创建管理隧道配置文件：**

a) 从 Cisco 软件下载中心 下载 AnyConnect **VPN 管理隧道独立配置文件编辑器**（如果尚未下载）。
b) 使用 VPN 用户的所需设置来创建管理隧道配置文件并保存文件。
c) 使用您在连接配置文件中配置的组 URL 来配置服务器列表中的服务器。

有关使用配置文件编辑器来创建管理配置文件的详细信息，请参阅《思科 *AnyConnect* 安全移动客户端管理员指南》《》。

步骤 4 创建管理隧道对象：

a) 在 Cisco Secure Firewall Management Center Web 接口上，导航至**对象 (Object)** > **对象管理 (Object Management)** > **VPN** > **AnyConnect 文件 (AnyConnect File)**
b) 点击**添加 AnyConnect 文件 (Add AnyConnect File)**。
c) 指定 AnyConnect 文件的**名称**。
d) 点击**浏览 (Browse)** 并选择已保存的管理隧道配置文件。
e) 点击**文件类型 (File Type)** 下拉列表，然后选择 **AnyConnect 管理 VPN 配置文件 (AnyConnect Management VPN Profile)**。
f) 点击**保存 (Save)**。

注释　您还可以在创建或更新组策略的 AnyConnect 设置时创建管理隧道对象。请参阅组策略 AnyConnect 客户端 选项，第 1066 页。

步骤 5 将管理配置文件与组策略关联并配置组策略设置：

您必须将管理 VPN 配置文件添加到与用于管理隧道 VPN 连接的连接配置文件关联的组策略。当用户连接时，系统会下载管理 VPN 配置文件以及已映射到组策略的用户 VPN 配置文件，从而启用管理 VPN 隧道功能。

注意　**无横幅 (No Banner)**：检查并确保未在组策略设置中配置横幅。您可以在**组策略 (Group Policy)** > **常规设置 (General Settings)** > **横幅 (Banner)** 下检查横幅设置。

a) 编辑为管理 VPN 隧道创建的连接配置文件。
b) 点击**编辑组策略 (Edit Group Policy)** > **AnyConnect** > **管理配置文件 (Management Profile)**。
c) 点击**管理 VPN 配置文件 (Management VPN Profile)** 下拉列表，然后选择您创建的管理配置文件对象。

注释　　您还可以点击 + 并添加新的 AnyConnect 管理 VPN 配置文件对象。

d) 点击**保存 (Save)**。

步骤 6 在组策略中配置分割隧道：

a) 点击**编辑组策略 (Edit Group Policy)** > **常规 (General)** > **分割隧道 (Split Tunneling)**。

b) 从 IPv4 或 IPv6 分割隧道的下拉菜单中，选择**下面指定的隧道网络 (Tunnel networks specified below)**。

c) 选择拆分隧道网络列表类型：**标准访问列表 (Standard Access List)** 或**扩展访问列表 (Extended Access List)**，然后选择所需的访问列表以允许流量通过管理 VPN 隧道。

d) 点击**保存 (Save)**，保存分割隧道设置。

AnyConnect 自定义属性

AnyConnect 管理 VPN 隧道要求分割默认包含隧道配置。如果要在组策略中配置 AnyConnect 自定义属性，以使用分割隧道来部署管理 VPN 隧道，则可以使用 FlexConfig 执行此操作，因为 管理中心 6.7 Web 界面不支持 AnyConnect 自定义属性。

以下是 AnyConnect 自定义属性的示例命令：

```
webvpn
 anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed
anyconnect-custom-data ManagementTunnelAllAllowed true true
group-policy MGMT_Tunnel attributes
 anyconnect-custom ManagementTunnelAllAllowed value true
```

步骤 7 部署、验证和监控远程访问 **VPN** 策略：

a) 将管理 VPN 隧道配置部署到 威胁防御。

注释　　客户端系统必须连接到 威胁防御 远程访问 VPN 一次，才能将管理隧道 VPN 配置文件下载到客户端计算机。

b) 您可以在 **AnyConnect 安全移动客户端 (AnyConnect Secure Mobility Client)** > **VPN** > **统计信息 (Statistics)** 中验证 AnyConnect 管理 VPN 隧道。

您还可以使用 **show vpn-sessiondb anyconnect** 命令在 威胁防御 命令提示符后检查管理 VPN 会话详细信息。

c) 在 管理中心 Web 界面上，点击**分析 (Analysis)** 以查看管理隧道会话信息。

相关主题

配置连接配置文件设置，第 1149 页
威胁防御组策略对象，第 1062 页

多证书身份验证

基于多个证书的身份验证能够让 威胁防御 验证计算机或设备的证书，以确保设备是企业发放的设备，此外还可以验证用户的身份证书，以允许在 SSL 或 IKEv2 EAP 阶段使用 AnyConnect 客户端 来进行 VPN 访问。

通过多证书选项，可以同时通过证书对计算机和用户进行证书身份验证。如果未选中此选项，则只能对计算机或用户执行证书身份验证，而不能同时对两者执行证书身份验证。

多重证书身份验证的限制

- 多证书身份验证当前会将证书数量限制为两个。
- AnyConnect 客户端必须指明支持多证书身份验证。如果不是这样，网关将使用其中一种传统身份验证方法，否则连接将失败。AnyConnect 版本 4.4.04030 或更高版本支持基于多证书的身份验证。
- AnyConnect 仅支持基于 RSA 的证书。
- 在 AnyConnect 汇聚身份验证期间，仅支持基于 SHA256、SHA384 和 SHA512 的证书。
- 证书身份验证不能与 SAML 身份验证结合使用。

配置多证书身份验证

开始之前

在配置多证书身份验证之前，请确保配置了用于获取每台 威胁防御 设备的身份证书的证书注册对象。有关详细信息，请参阅证书映射对象，第 1072 页。

过程

步骤 1 选择**设备** > **VPN** > **远程接入**。

步骤 2 选择远程访问 VPN 策略，然后点击 **编辑 (Edit)**。

注释 如果尚未配置远程接入 VPN，请点击**添加 (Add)** 以创建新的远程接入 VPN 策略。

步骤 3 选择并**编辑**连接配置文件，以便配置多证书身份验证。

步骤 4 点击 **AAA** 设置，然后选择**身份验证方法 (Authentication Method)** > **仅客户端证书 (Client Certificate Only)** 或**客户端证书和 AAA (Client Certificate & AAA)**。

注释 如果您选择了客户端证书和 AAA 身份验证方法，请选择**身份验证服务器 (Authentication Server)**

步骤 5 选择**启用多证书身份验证 (Enable multiple certificate authentication)**。

步骤 6 选择一个证书以便**映射客户端证书中的用户名**：

- **第一个证书**-选择此选项以映射从 VPN 客户端发送的计算机证书中的用户名。
- **第二个证书**-选择此选项以映射从客户端发送的用户证书中的用户名。

如果启用仅证书身份验证，从客户端发送的用户名会被用作 VPN 会话用户名。如果启用了 AAA 和证书身份验证，VPN 会话用户名将基于预填充选项。

注释 如果选择**映射特定字段 (Map specific field)** 选项（包括客户端证书中的用户名），则**主 (Primary)** 字段和**辅助 (Secondary)** 字段将分别显示默认值：**CN**（公用名）和 **OU**（组织单位）。

如果选择**使用整个 DN（可分辨名称）作为用户名**选项，系统将自动检索用户身份。可分辨名称 (DN) 是由单个字段组成的唯一标识，可在将用户与连接配置文件匹配时用作标识符。DN 规则用于增强的证书身份验证。

如果您选择了客户证书和 AAA 身份验证，请选择**在用户登录窗口预填证书中的用户名 (Prefill username from certificate on user login window)** 选项，以便在用户通过 AnyConnect VPN 客户端连接时预填充辅助用户名。

- **在登录窗口隐藏用户名：** 辅助用户名是从客户端证书预填充的，但对用户隐藏，确保用户不会修改预填充的用户名。

步骤 7 为远程访问 VPN 配置所需的 AAA 设置和连接配置文件设置。

步骤 8 保存连接配置文件和远程访问 VPN 配置并将其部署在您的 威胁防御 设备上。

相关主题

配置远程访问 VPN 的 AAA 设置，第 1151 页

自定义远程接入 VPN AAA 设置

本节提供有关自定义远程接入 VPN 的 AAA 首选项的信息。有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 1151 页。

通过客户端证书对 VPN 用户进行身份验证

使用向导创建新的远程接入 VPN 策略或稍后编辑策略时，可以使用客户端证书配置远程接入 VPN 身份验证。

开始之前

配置用于为每台充当 VPN 网关的 威胁防御设备获取身份证书的证书注册对象。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备** > **VPN** > **远程接入**。

步骤 2 在远程访问策略，然后点击 **编辑**；或者点击 **添加** 以创建新的远程访问 VPN 策略。

步骤 3 对于新的远程接入VPN策略，请在选择连接配置文件设置时配置身份验证。对于现有配置，选择包含客户端配置文件的连接配置文件，然后点击**编辑**。

步骤 4 点击 **AAA** > **身份验证方法 (Authentication Method)** > **仅限客户端证书 (Client Certificate Only)**。

使用此身份验证方法，用户可以使用客户端证书进行身份验证。必须在VPN客户端终端上配置客户端证书。默认情况下，用户名分别派生自客户端证书字段CN和OU。如果在客户端证书的其他字段中指定了用户名，请使用“主”字段和“辅助”字段来映射适当的字段。

如果选择**映射特定字段**选项，其中包括来自客户端证书的用户名。 **主 (Primary)** 字段和**辅助 (Secondary)** 字段将显示默认值： **CN**（**公用名**） 和 **OU**（**组织单位**）。如果选择**使用整个 DN 作为用户名**选项，系统将自动检索用户身份。可分辨名称(DN)是由单个字段组成的唯一标识，可在将用户与连接配置文件匹配时用作标识符。DN 规则用于增强的证书身份验证。

- 与**映射特定字段 (Map specific field)** 选项相关的“主”(Primary) 和“辅助”(Secondary) 字段包含以下公共值：
  - C（国家/地区）
  - CN（公用名）
  - DNQ（DN 限定符）
  - EA（邮件地址）
  - GENQ（代系限定符）
  - GN（名字）
  - I（首字母）
  - L（地区）
  - N（名字）
  - O（组织）
  - OU（组织单位）
  - SER（序列号）
  - SN（姓氏）
  - SP（省）
  - T（职务）
  - UID（用户 ID）
  - UPN（用户主体名称）
- 无论选择哪种身份验证方法，选择或取消选择**仅当用户位于授权数据库中时才允许连接**。

有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 1151 页。

步骤 5 保存更改。

相关主题

配置连接配置文件设置，第 1149 页

添加证书注册对象，第 1011 页

通过客户端证书和 AAA 服务器配置 VPN 用户身份验证

在配置远程接入VPN身份验证以便同时使用客户端证书和身份验证服务器时，会使用客户端证书验证和 AAA 服务器来完成 VPN 客户端身份验证。

开始之前

- 配置用于为每台充当 VPN 网关的威胁防御设备获取身份证书的证书注册对象。
- 配置在远程访问 VPN 策略配置中使用的 RADIUS 服务器组对象和任何 AD 或 LDAP 领域。
- 确保可以通过 Cisco Secure Firewall Threat Defense设备访问 AAA 服务器，以使远程接入 VPN 配置生效。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择 **设备 (Devices)** > **远程访问 (Remote Access)**。

步骤 2 点击要更新身份验证的远程访问 VPN 策略上的**编辑 (Edit)**，或点击**添加 (Add)** 以新建一个。

步骤 3 如果选择创建新的远程接入 VPN 策略，请在选择连接配置文件设置时配置身份验证。对于现有配置，选择包含客户端配置文件的连接配置文件，然后点击**编辑**。

步骤 4 转到**AAA**，然后从**身份验证方法 (Authentication Method)** 下拉列表中选择**客户端证书和 AAA (Client Certificate & AAA)**。

- 何时选择以下**身份验证方法**：

  客户端证书和 AAA - 完成两种类型的身份验证。

  - **AAA** - 如果选择 **RADIUS** 作为**身份验证服务器**，则授权服务器默认也采用此选择。从下拉列表中选择**记帐服务器**。每当从“身份验证服务器”下拉列表中选择 **AD** 和 **LDAP** 时，都必须手动分别选择**授权服务器**和**记帐服务器**。
  - **客户端证书 (Client Certificate)** - 使用客户端证书对用户进行身份验证。您必须在 VPN 客户端终端上配置客户端证书。默认情况下，用户名分别派生自客户端证书字段 CN 和 OU。如果使用客户端配置文件中的任何其他字段指定了用户名，请使用**主字段 (Primary Field)** 和**辅助字段 (Secondary Field)** 来映射相应的字段。

    如果选择**映射特定字段**选项，其中包括来自客户端证书的用户名。则**主**和**辅助**字段将显示默认值：**CN (公用名称)** 和 **OU (组织单位)**。如果选择**使用整个 DN 作为用户名**选项，系统将自动检索用户身份。可分辨名称 (DN) 是由单个字段组成的唯一标识，可在将用户与连接配置文件匹配时用作标识符。DN 规则用于增强的证书身份验证。

    与**映射特定字段**选项相关的“主”和“辅助”字段包含以下公共值：

    - C（国家/地区）

- CN（公用名）
- DNQ（DN 限定符）
- EA（邮件地址）
- GENQ（代系限定符）
- GN（名字）
- I（首字母）
- L（地区）
- N（名字）
- O（组织）
- OU（组织单位）
- SER（序列号）
- SN（姓氏）
- SP（省）
- T（职务）
- UID（用户 ID）
- UPN（用户主体名称）

- 无论选择哪种身份验证方法，选择或取消选择**仅当用户位于授权数据库中时才允许连接**。

有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 1151 页。

步骤 5 保存更改。

相关主题

配置连接配置文件设置，第 1149 页
添加证书注册对象，第 1011 页

通过 VPN 会话管理密码更改

通过密码管理，远程访问 VPN 策略管理员可以为远程访问 VPN 用户配置密码到期时的通知设置。密码管理在使用身份验证方法“仅 AAA”和“客户端证书和 AAA”的 AAA 设置中可用。有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 1151 页。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择 **设备 (Devices)** > **远程访问 (Remote Access)**。

步骤 2 点击要编辑的远程访问 VPN 策略旁边的**编辑 (Edit)** 。

步骤 3 在包含 AAA 设置的连接配置文件上点击**编辑 (Edit)**。

步骤 4 选择 **AAA** > **高级设置 (Advanced Settings)** >。

步骤 5 选中**启用密码管理 (Enable Password Management)** 复选框并选择以下选项之一：

- 通知用户 - 在密码到期之前；在框中指定天数。
- 在密码到期当天通知用户。

步骤 6 保存更改。

相关主题

配置连接配置文件设置 ， 第 1149 页

向 RADIUS 服务器发送记账记录

远程接入 VPN 中的记账记录有助于 VPN 管理员跟踪用户访问的服务以及他们使用的网络资源量。记账信息包括用户会话的开始和停止时间、用户名、会话时通过设备的字节数、使用的服务以及每个会话的持续时间。

您可以单独使用记帐功能，也可以将其与身份验证和授权功能配合使用。激活 AAA 记账时，网络访问服务器会向所配置的记账服务器报告用户活动。您可以将 RADIUS 服务器配置为记账服务器，以便将所有用户活动信息从 管理中心 发送到 RADIUS 服务器。

注释 您可以在远程接入 VPN AAA 设置中使用相同的 RADIUS 服务器或单独的 RADIUS 服务器进行认证授权和记账。

开始之前

- 使用将向其发送身份验证请求或记账记录的 RADIUS 服务器配置 RADIUS 组对象。有关详细信息，请参阅RADIUS 服务器组选项 ， 第 971 页。
- 确保可从 威胁防御 设备访问 RADIUS 服务器。配置 Cisco Secure Firewall Management Center上的路由（位于**设备** > **设备管理** > **编辑设备** > **路由**） ，以确保 RADIUS 服务器的连接。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备 (Devices)** > **远程访问 (Remote Access)**。

步骤 2 在要配置 RADIUS 服务器的远程访问策略上点击**编辑 (Edit)**，或创建新的远程访问 VPN 策略。

步骤 3 在包含 AAA 设置的连接的配置文件上点击**编辑 (Edit)**，然后选择 **AAA**。

步骤 4 从**记帐服务器 (Accounting Server)** 下拉列表中选择 RADIUS 服务器。

步骤 5 保存更改。

相关主题

配置连接配置文件设置，第 1149 页
配置远程访问 VPN 的 AAA 设置，第 1151 页

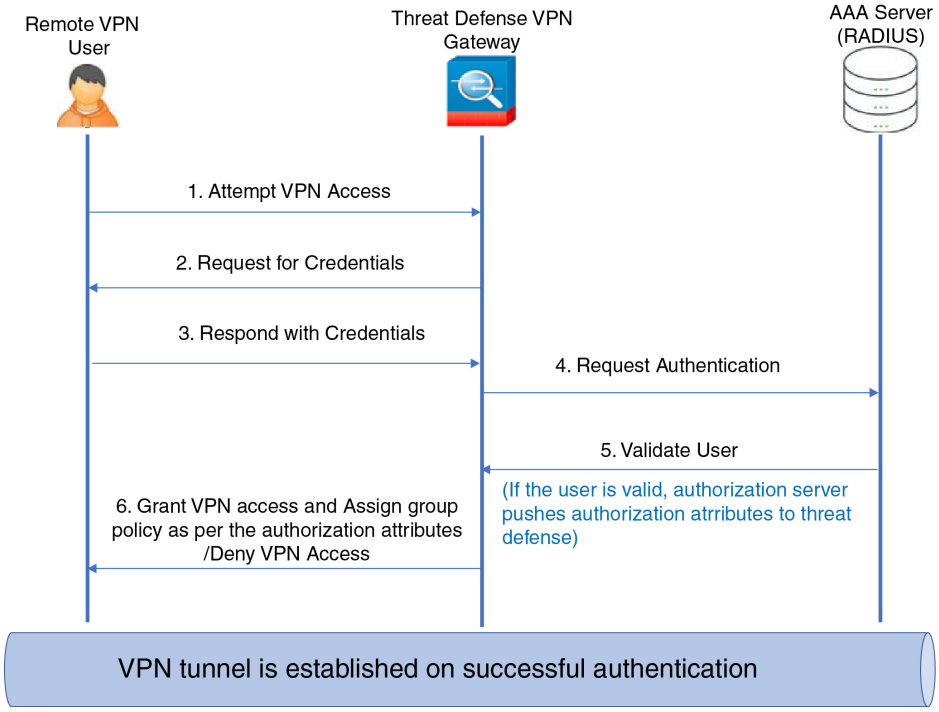
将组策略选择委派给授权服务器

在建立 VPN 隧道时，将确定应用于用户的组策略。您可以在使用向导来创建远程接入 VPN 策略时为连接配置文件选择组策略，也可以稍后再更新连接配置文件的连接策略。但是，您可以配置 AAA (RADIUS) 服务器以分配组策略，或者从当前连接配置文件中获取。如果 威胁防御 设备从与连接配置文件上配置的属性冲突的外部 AAA 服务器接收属性，则来自 AAA 服务器的属性始终优先。

您可以配置 ISE 或 RADIUS 服务器，通过发送 IETF RADIUS 属性 25 并映射到相应的组策略名称来为此用户或用户组设置授权配置文件。您可以为用户或用户组配置特定组策略，以便推送可下载 ACL、设置横幅、限制 VLAN，并配置将 SGT 应用于会话的高级选项。建立 VPN 连接时，这些属性将应用于属于该组的所有用户。

有关更多信息，请参阅《思科身份服务引擎管理员指南》中的“配置标准授权策略”部分和Cisco Secure Firewall Threat Defense 的 RADIUS 服务器属性，第 1157 页。

图 *140: AAA* 服务器的远程接入 *VPN* 组策略选择



相关主题

配置组策略对象，第 1063 页
配置连接配置文件设置，第 1149 页

授权服务器覆盖组策略或其他属性的选择

当远程接入VPN用户连接VPN时，系统会将连接配置文件中配置的组策略和其他属性分配给用户。但是，远程访问 VPN 系统管理员可以通过配置 ISE 或 RADIUS 服务器为用户或用户组设置授权配置文件，将组策略和其他属性的选择委派给授权服务器。用户通过身份验证后，这些特定的授权属性将被推送到 威胁防御设备。

开始之前

确保使用 RADIUS 作为身份验证服务器来配置远程接入 VPN 策略。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备** > **VPN** > **远程接入**。

步骤 2 选择远程访问策略，然后点击 **编辑**。

步骤 3 如果尚未配置，请选择 RADIUS 或 ISE 作为授权服务器。

步骤 4 选择**高级** > **组策略**，并添加所需的组策略。有关组策略对象的详细信息，请参阅配置组策略对象，第 1063 页。

您只可将单个组策略映射到连接配置文件；但是，您可以在远程接入VPN策略中创建多个组策略。可以在 ISE 或 RADIUS 服务器中引用这些组策略，并将其配置为通过在授权服务器中分配授权属性来覆盖连接配置文件中配置的组策略。

步骤 5 在目标 威胁防御设备上部署配置。

步骤 6 在授权服务器上，使用 IP 地址和可下载 ACL 的 RADIUS 属性创建授权配置文件。

在选择用于远程接入VPN的授权服务器中配置组策略后，组策略将覆盖用户通过身份验证后在远程接入 VPN 用户的连接配置文件中配置的组策略。

相关主题

配置组策略对象，第 1063 页

拒绝用户组的 VPN 访问

如果您不希望通过身份验证的用户或用户组使用 VPN，则可以配置组策略以拒绝 VPN 接入。您可以在远程接入VPN策略中配置组策略，并在ISE或RADIUS服务器配置中引用此策略以进行授权。

开始之前

确保已使用远程接入策略向导配置远程接入 VPN，并已为远程接入 VPN 策略配置身份验证设置。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备** > **VPN** > **远程接入**。

步骤 2 选择远程访问策略，然后点击 **编辑**。

步骤 3 选择 **高级** > **组策略**。

步骤 4 选择组策略，点击 **编辑 (Edit)** 或添加新增组策略。

步骤 5 选择**高级** > **会话设置**并将**每用户同时登录数**设置为 0 （零）。
这会阻止用户或用户组连接到 VPN，哪怕只有一次。

步骤 6 点击**保存**以保存组策略，然后保存远程接入 VPN 配置。

步骤 7 配置 ISE 或 RADIUS 服务器，为此用户/用户组设置授权配置文件，以发送 IETF RADIUS 属性 25 并映射到相应的组策略名称。

步骤 8 配置 ISE 或 RADIUS 服务器作为远程访问 VPN 策略中的授权服务器。

步骤 9 保存和部署远程访问 VPN 策略。

相关主题

配置连接配置文件设置，第 1149 页

限制用户组的连接配置文件选择

如果要在用户或用户组上强制实施单个连接配置文件，可以选择禁用连接配置文件，以便用户在使用 AnyConnect VPN 客户端连接时无法选择组别名或 URL。

例如，如果您的组织要为不同的VPN用户组（如移动用户、公司分发的笔记本电脑用户或个人笔记本电脑用户）使用特定配置，则可以配置特定于每个用户组的连接配置文件，并在用户连接VPN时应用适当的连接配置文件。

默认情况下，AnyConnect 客户端将显示在 管理中心 中配置并在 威胁防御 上部署的连接配置文件列表（按连接配置文件名称、别名或别名URL）。如果未配置自定义连接配置文件，AnyConnect将显示 *DefaultWEBVPNGroup* 连接配置文件。使用以下程序实施用户组的单个连接配置文件。

开始之前

- 在 Cisco Secure Firewall Management Center Web 界面中，使用远程接入 VPN 策略向导配置远程接入VPN，将身份验证方法设置为“仅客户端证书”或“客户端证书+AAA”。从证书中选择用户名字段。
- 配置 ISE 或 RADIUS 服务器以进行授权，并将组策略与授权服务器关联。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备** > **VPN** > **远程接入**。

步骤 2 选择远程访问策略，然后点击 **编辑**。

步骤 3 选择 **访问接口** ，然后禁用 **允许用户在登录时选择连接配置文件**。

步骤 4 点击**高级** > **证书映射**。

步骤 5 选择 **使用配置的规则将证书与连接配置文件匹配**。

步骤 6 选择**证书映射名称**，或点击**添加**图标以添加证书规则。

步骤 7 选择**连接配置文件**并点击**确定**。
使用此配置，当用户从AnyConnect连接时，用户将具有映射的连接配置文件，并将进行身份验证以使用 VPN。

相关主题

配置组策略对象 ，第 1063 页
配置连接配置文件设置 ，第 1149 页

更新远程接入 VPN 客户端的 AnyConnect 客户端 配置文件

AnyConnect 客户端 客户端配置文件是一个 XML 文件，其中包含管理员定义的最终用户要求以及作为 AnyConnect的一部分部署在 VPN 客户端系统上的身份验证策略。它使最终用户可以使用预配置的网络配置文件。

您可以使用基于 GUI 的 AnyConnect 配置文件编辑器（一个独立的配置工具）来创建他们。此独立配置文件编辑器可用于创建新的或修改现有的AnyConnect配置文件。您可以从思科软件下载中心下载配置文件编辑器。

有关详细信息，请参见相应版本的《》《思科 AnyConnect 安全移动客户端管理员指南》中的 AnyConnect 配置文件编辑器一章。

开始之前

- 确保已使用远程接入策略向导配置远程接入VPN，并已在威胁防御设备上部署配置。请参阅创建新的远程接入 VPN 策略，第 1142 页。
- 在 Cisco Secure Firewall Management Center Web 界面上，转至**对象 (Objects)** > **对象管理 (Object Management)** > **VPN** > **AnyConnect 文件 (AnyConnect File)**，然后添加新的 AnyConnect 客户端映像。

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备** > **VPN** > **远程接入**。

步骤 2 选择远程访问 VPN 策略，然后点击 **编辑**。

步骤 3 选择包含要编辑的客户端配置文件的连接配置文件，然后点击**编辑**。

步骤 4 点击**编辑组策略 (Edit Group Policy)** > **AnyConnect** > **配置文件 (Profiles)**。

步骤 5 从列表中选择一个客户端配置文件 XML 文件，或者点击**添加 (Add)** 以添加新的客户端配置文件。

步骤 6 保存组策略、连接配置文件，然后保存远程接入 VPN 策略。

步骤 7 部署更改。
客户端配置文件的更改将在 VPN 客户端连接到远程接入 VPN 网关时在 VPN 客户端上进行更新。

相关主题

配置组策略对象，第 1063 页

RADIUS 动态授权

Cisco Secure Firewall Threat Defense 可以使用 RADIUS 服务器进行 VPN 远程接入和防火墙直接转发代理会话的用户授权（按用户使用动态访问控制列表 [ACL] 或 ACL 名称）。要实施动态授权或 RADIUS 授权更改 (RADIUS CoA) 的动态 ACL，您必须配置 RADIUS 服务器以支持它们。在用户尝试进行身份验证时，RADIUS 服务器会向 威胁防御 发送可下载的 ACL 或 ACL 名称。ACL 允许或拒绝访问特定服务。身份验证会话到期时，Cisco Secure Firewall Threat Defense会删除 ACL。

相关主题

添加 RADIUS 服务器组，第 970 页
接口，第 995 页
配置 RADIUS 动态授权，第 1197 页
Cisco Secure Firewall Threat Defense 的 RADIUS 服务器属性，第 1157 页

配置 RADIUS 动态授权

准备工作：

- 如果在 RADIUS 服务器中引用接口，则只能在安全区域或接口组中配置一个接口。

- 启用动态授权的 RADIUS 服务器需要 Cisco Secure Firewall Threat Defense 6.3 或更高版本才能使动态授权生效。
- Cisco Secure Firewall Threat Defense 6.2.3 或更低版本不支持 RADIUS 服务器中的接口选择。在部署期间，接口选项将被忽略。
- 威胁防御 终端安全评估 VPN 不支持通过动态授权或 RADIUS 授权来更改 (CoA) 更改组策略。

表 87: 操作步骤

	相应操作	更多信息
第 1 步	登录 Cisco Secure Firewall Management Center Web 界面。	
第 2 步	使用动态授权配置 RADIUS 服务器对象。	RADIUS 服务器组选项， 第 971 页
第 3 步	通过已启用授权更改 (CoA) 的接口配置到 ISE 服务器的路由，以通过路由或特定接口建立 威胁防御到 RADIUS 服务器的连接。	RADIUS 服务器组选项， 第 971 页 配置用户控制 ISE/ISE-PIC， 第 1858 页
第 4 步	配置远程访问 VPN 策略，选择您通过动态授权创建的 RADIUS 服务器组对象。	创建新的远程接入 VPN 策略， 第 1142 页
第 5 步	使用“平台设置”配置 DNS 服务器详细信息和域查找接口。	配置 DNS， 第 1145 页 DNS 服务器组， 第 985 页
第 6 步	如果可以通过 VNP 网络访问 DNS 服务器，则在组策略中配置拆分隧道，以允许 DNS 流量通过远程接入 VPN 隧道。	配置组策略对象， 第 1063 页
第 7 步	部署配置更改。	部署配置更改， 第 136 页

双因素身份验证

您可以为远程接入VPN配置双因素身份验证。配置了双因素身份验证时，用户必须提供用户名、静态密码，以及一个额外项，如RSA令牌或密码等。双因素身份验证不同于使用第二个身份验证源，双因素是在单个身份验证源中配置的，其与 RSA 服务器的关系绑定到主身份验证源。

Cisco Secure Firewall Threat Defense 支持 RSA 令牌和 Duo Push 身份验证请求，并将任何 RADIUS 或 AD 服务器作为双因素认证过程中的第一因素，向 Duo Mobile 提出第二因素。

配置 RSA 双因素身份验证

关于此任务：

您可以将 RADIUS 或 AD 服务器配置为 RSA 服务器中的身份验证代理，并将 Cisco Secure Firewall Management Center中的服务器用作远程接入 VPN 中的主身份验证源。

使用此方法时，用户必须使用 RADIUS 或 AD 服务器中配置的用户名进行身份验证，并使用一次性临时 RSA 令牌连接密码，用逗号分隔密码和令牌：密码,令牌。

在此配置中，通常会使用单独的 RADIUS 服务器 （例如，Cisco ISE 提供的 RADIUS 服务器) 提供授权服务。将第二个 RADIUS 服务器配置为授权、配置或记账服务器。

准备工作：

在 Cisco Secure Firewall Threat Defense上配置 RADIUS 双因素身份验证之前，请确保完成以下配置：

在 RSA 服务器上

- 将 RADIUS 或 Active Directory 服务器配置为身份验证代理。
- 生成并下载配置 (*sdconf.rec*) 文件。
- 创建令牌配置文件，将令牌分配给用户，并将令牌分发给用户。下载并在远程接入VPN客户端系统上安装令牌。

有关详细信息，请参阅 RSA SecureID 套件文档。

在 ISE 服务器上

- 导入 RSA 服务器上生成的配置 (*sdconf.rec*) 文件。
- 添加 RSA 服务器作为外部身份源并指定共享密钥。

表 *88:* 操作步骤

	相应操作	更多信息
第 1 步	登录 Cisco Secure Firewall Management Center Web 界面。	
第 2 步	创建 RADIUS 服务器组。	RADIUS 服务器组选项， 第 971 页

	相应操作	更多信息
第 3 步	在新 RADIUS 服务器组中创建 RADIUS 服务器对象，将 RADIUS 或 AD 服务器作为主机，超时时间为 60 秒或更长。	RADIUS 服务器组选项，第 971 页 **注释** RADIUS 或 AD 服务器必须与在 RSA 服务器中配置为身份验证代理的服务器相同。 对于双因素身份验证，也要确保在 AnyConnect 客户端配置文件 配置文件 XML 文件中将超时更新为 60 秒或更长。
第 4 步	使用向导配置新的远程接入 VPN 策略，或者编辑现有的远程接入 VPN 策略。	创建新的远程接入 VPN 策略，第 1142 页
第 5 步	选择 RADIUS 作为身份验证服务器，然后选择新创建的 RADIUS 服务器组作为身份验证服务器。	配置远程访问 VPN 的 AAA 设置，第 1151 页
第 7 步	部署配置更改。	部署配置更改，第 136 页

配置 Duo 双因素身份验证

关于此任务：

可以将 Duo RADIUS 服务器配置为主要身份验证源。此方法使用 Duo RADIUS 身份验证代理。（您不能通过 LDAPS 使用与 Duo 云服务的直接连接。）

有关配置 Duo 的详细步骤，请参阅 https://duo.com/docs/cisco-firepower。

然后，配置 Duo，以转发定向到代理服务器的身份验证请求，并将另一台 RADIUS 服务器或 AD 服务器用作第一个身份验证因素，将 Duo 云服务用作第二个因素。

使用此方法时，用户必须使用 Duo 云和 Web 服务器以及关联的 RADIUS 服务器上配置的用户名进行身份验证。用户必须输入 RADIUS 服务器中配置的密码，后跟以下 Duo 代码之一：

- **Duo-passcode**。例如，*my-password*,123456。
- **push**。例如，*my-password*,**push**。使用 push 告知 Duo 向用户应该已经安装并注册的 Duo 移动应用发送推送身份验证。
- **sms**。例如，*my-password*,**sms**。使用 **sms** 告知 Duo 向用户的移动设备发送包含新一批密码的 SMS 消息。使用 **sms** 时，用户的身份验证尝试将会失败。用户必须重新进行身份验证，并输入新密码作为辅助因素。
- **phone**。例如，*my-password*,**phone**。使用**电话**通过电话呼叫来进行身份验证。

有关登录选项及示例的详细信息，请参阅https://guide.duo.com/anyconnect。

准备工作：

在 威胁防御上使用 Duo 身份验证代理配置双因素身份验证之前，确保完成以下配置：

- 在开始部署 Duo 之前，为远程接入 VPN 用户配置有效的主身份验证（RADIUS 或 AD）。
- 在网络中的 Windows 或 Linux 计算机上安装 Duo 代理服务，以将 Duo 与 Cisco Secure Firewall Threat Defense远程接入 VPN 集成。此 Duo 代理服务器也可充当 RADIUS 服务器。

  从以下位置下载并安装最新的 Duo 身份验证代理：

  - **Windows**：https://dl.duosecurity.com/duoauthproxy-latest.exe
  - **Linux**：https://dl.duosecurity.com/duoauthproxy-latest-src.tgz
  - 在 https://duo.com/docs/checksums#duo-authentication-proxy 上验证校验和。

- 配置 Duo 身份验证文件 `authproxy.cfg`。按照 https://duo.com/docs/cisco-firepower#configure-the-proxy 页面上的说明配置身份验证配置设置。

  `authproxy.cfg` 配置文件必须包含 RADIUS 或 ISE 服务器、威胁防御设备的详细信息、Duo 代理服务器详细信息、集成密钥、密钥以及 API 主机详细信息。

- 确保 `authproxy.cfg` 文件中具有正确的 API 主机信息。
- 在 **Duo 安全服务器** > **Duo 管理面板**> **应用** > **思科 ONE RADIUS VPN** 下，在新安装的 Duo 代理服务器中配置其他所需设置，例如辅助身份验证因素。

表 *89:* 操作步骤

	相应操作	更多信息
第 1 步	登录 Cisco Secure Firewall Management Center Web 界面。	
第 2 步	创建 RADIUS 服务器组。	RADIUS 服务器组选项， 第 971 页
第 3 步	在新 RADIUS 服务器组中创建 RADIUS 服务器对象，将 Duo 代理服务器作为主机，超时时间为 60 秒或更长。	RADIUS 服务器选项， 第 972 页 **注释** 对于双因素身份验证，也要确保在 AnyConnect 客户端配置文件 配置文件 XML 文件中将超时更新为 60 秒或更长。
第 4 步	使用向导配置新的远程接入 VPN 策略，或者编辑现有的远程接入 VPN 策略。	创建新的远程接入 VPN 策略， 第 1142 页
第 5 步	选择 RADIUS 作为身份验证服务器，然后选择使用 Duo 代理服务器创建的 RADIUS 服务器组作为身份验证服务器。	配置远程访问 VPN 的 AAA 设置， 第 1151 页

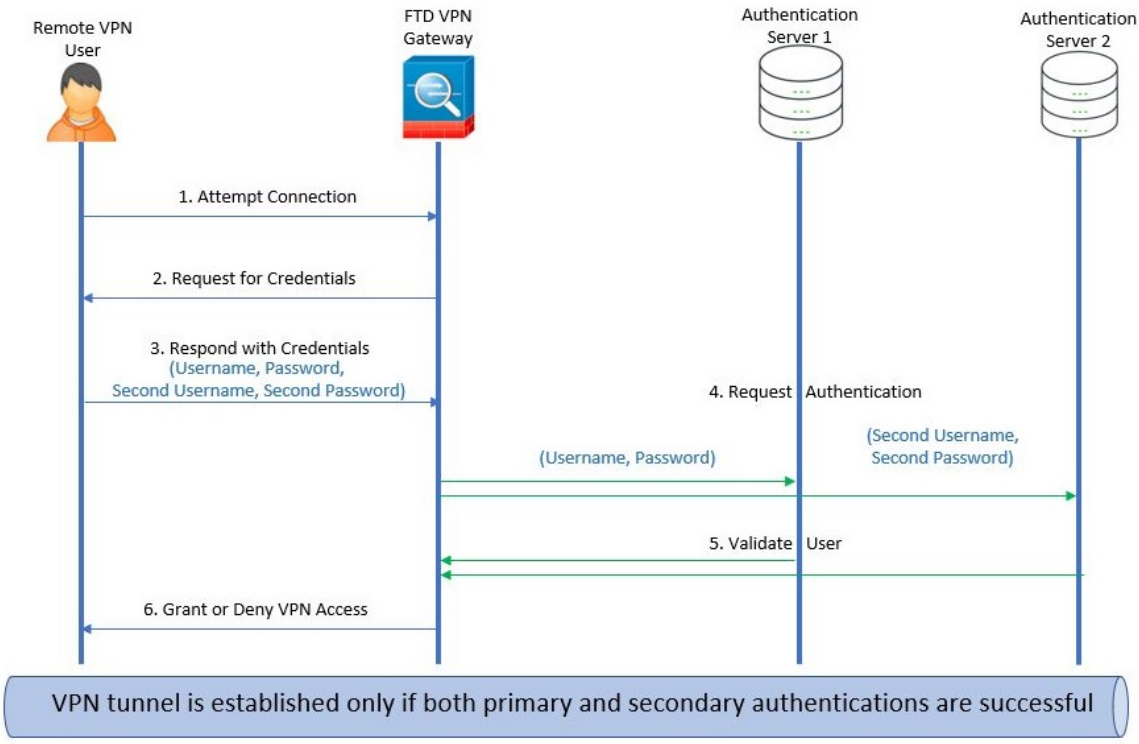
	相应操作	更多信息
第 7 步	部署配置更改。	部署配置更改，第 136 页

辅助身份验证

Cisco Secure Firewall Threat Defense 中的辅助身份验证或双重身份验证，通过使用两个不同的身份验证服务器，为远程访问 VPN 连接额外添加了一层安全性。启用辅助身份验证后， AnyConnect VPN 用户必须提供两组凭证才能登录 VPN 网关。

Cisco Secure Firewall Threat Defense 远程访问 VPN 支持仅 AAA 和客户端证书以及 AAA 身份验证方法的辅助身份验证。

图 *141:* 远程访问 *VPN* 辅助或双重身份验证



相关主题

配置远程访问 VPN 辅助身份验证，第 1202 页

配置远程访问 VPN 辅助身份验证

当远程接入VPN身份验证配置为同时使用客户端证书和身份验证服务器时，使用客户端证书验证和 AAA 服务器完成 VPN 客户端身份验证。

开始之前

- 配置两个身份验证(AAA)服务器-主要和辅助身份验证服务器，以及所需的身份证书。身份验证服务器可以是 RADIUS 服务器以及 AD 或 LDAP 领域。
- 确保可以通过 Cisco Secure Firewall Threat Defense 设备访问 AAA 服务器，以使远程接入访问 VPN 配置生效。配置路由（在 **设备 > 设备管理 > 编辑设备 > 路由**）以确保 AAA 服务器连接：

过程

步骤 1 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备** > **VPN** > **远程接入**。

步骤 2 在远程访问策略，然后点击 **编辑**；或者点击 **添加** 以创建新的远程访问 VPN 策略。

步骤 3 对于新的远程接入VPN策略，请在选择连接配置文件设置时配置身份验证。对于现有配置，选择包含客户端配置文件的连接配置文件，然后点击**编辑**。

步骤 4 点击 **AAA** > **身份验证方式**， **AAA** 或 **客户端证书和 AAA**。

- 何时选择以下**身份验证方法**：

  客户端证书和 AAA-使用客户端证书和 AAA 服务器已完成身份验证。

  - **AAA** - 如果选择 **RADIUS** 作为**身份验证服务器**，则授权服务器默认也采用此选择。从下拉列表中选择**记帐服务器**。每当从“身份验证服务器”下拉列表中选择 **AD** 和 **LDAP** 时，都必须手动分别选择**授权服务器**和**记帐服务器**。
  - 无论选择哪种身份验证方法，选择或取消选择**仅当用户位于授权数据库中时才允许连接**。

- **使用辅助身份验证** - 除主身份验证之外，还配置了辅助身份验证，以便为 VPN 会话提供额外的安全保护。辅助身份验证是仅适用于**仅 AAA** 和**客户端证书和 AAA** 身份验证方法。

  辅助身份验证是一项可选功能，该功能要求 VPN 用户在 AnyConnect 登录屏幕上输入两组用户名和密码。您还可以配置为从身份验证服务器或客户端证书预填充辅助用户名。仅当主身份验证和辅助身份验证均成功时，才会授予远程访问VPN身份验证。如果任何一个身份验证服务器无法访问或一个身份验证失败，VPN 身份验证将被拒绝。

  必须在配置辅助身份验证前，为辅助用户名和密码配置辅助身份验证服务器组（AAA服务器）。例如，可以将主身份验证服务器设置为 LDAP 或 Active Directory 领域，将辅助身份验证设置为 RADIUS 服务器。

  注释 默认情况下，无需辅助身份验证。

  身份验证服务器 - 为 VPN 用户提供辅助用户名和密码的辅助身份验证服务器。

  选择 **辅助身份验证的用户名**以下的选项：

  - **提示**： 在登录 VPN 网关时，提示用户输入用户名和密码。
  - **使用主身份验证用户名**： 用户名从主身份验证服务器获取，用于主身份验证和辅助身份验证；必须输入两个密码。
  - **映射客户端证书中的用户名**： 预填充客户端证书中的辅助用户名。

- 如果选择**映射特定字段**选项，其中包括来自客户端证书的用户名。则**主**和**辅助**字段将显示默认值：**CN (公用名称)** 和 **OU (组织单位)**。如果选择**使用整个 DN（可分辨名称）作为用户名**选项，系统将自动检索用户身份。

  有关主字段和辅助字段映射的详细信息，请参阅**身份验证方法**说明。

- **在用户登录窗口预填证书中的用户名 (Prefill username from certificate on user login window)**：用户通过 AnyConnect VPN 客户端连接时，预填充客户端证书中的辅助用户名。
  - **在登录窗口隐藏用户名**：辅助用户名是从客户端证书预填充的，但对用户隐藏，确保用户不会修改预填充的用户名。

- **使用 VPN 会话的辅助用户名**：辅助用户名用于在 VPN 会话期间报告用户活动。

有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 1151 页。

相关主题

配置连接配置文件设置，第 1149 页

使用 SAML 2.0 的单点登录身份验证

关于 SAML 单点登录身份验证

安全断言标记语言（SAML）是一种开放标准，用于通过用户在其他情景中的会话将其登录到应用中。当用户登录其 Active Directory（AD）域或内联网时，组织已经知道用户的身份。他们使用此身份信息通过使用 SAML 将用户登录到其他应用，例如基于 Web 的应用。单个应用无需存储凭证，用户无需记住和管理单个应用的不同凭证集。SAML 单点登录 (SSO) 通过将用户的身份从一个位置（身份提供程序）传输到另一个位置（服务提供商）来工作。

通过 Cisco Secure Firewall Threat Defense 进行 SAML 单点登录

Cisco Secure Firewall Threat Defense 设备支持使用 AnyConnect 安全移动客户端对远程访问 VPN 连接进行 SAML 2.0 单点登录 (SSO) 身份验证。您需要执行以下操作，才能在 Cisco Secure Firewall Threat Defense上配置 SAML 2.0 SSO：

- **身份提供程序（IdP）**-Duo 访问网关充当身份提供程序以执行用户身份验证并发出断言。
- **服务提供商 (SP)** - 威胁防御 设备充当服务提供商并从身份提供商获取身份验证断言。
- **VPN 客户端** - AnyConnect 安全移动客户端会通过嵌入式浏览器来执行 SAML 2.0 身份验证。

如果您的身份策略与与 SAML 域匹配的 AD 领域相关联，则可以对通过 SAML 身份验证的用户实施访问策略。

SAML 2.0 的准则和限制

- 威胁防御 支持以下 SAML 身份验证签名：
  - 包含 RSA 和 HMAC 的 SHA1
  - 包含 RSA 和 HMAC 的 SHA1
- 威胁防御 支持 SAML 2.0 重定向-POST 绑定，所有 SAML IdP 也支持此功能。
- 威胁防御 仅用作 SAML SP。在网关模式或对等模式下，它不能用作身份提供程序。
- 如果您的身份策略与与 SAML 域匹配的 AD 领域相关联，则可以对通过 SAML 身份验证的用户实施访问策略。
- 不支持在 DAP 评估中使用 SAML 身份验证属性（类似于从 AAA 服务器发送的 RADIUS 身份验证响应中的 RADIUS 属性）。威胁防御 支持对 DAP 策略启用 SAML 的组策略；但是，在使用 SAML 身份验证时，您无法检查用户名属性，因为用户名属性已被 SAML 身份提供程序屏蔽。
- 威胁防御 管理员需要确保 威胁防御 与 SAML IdP 之间的时钟同步，从而正确处理身份验证断言并确保正确的超时行为。
- 威胁防御 管理员有责任在 威胁防御 和 IdP 上维护有效的签名证书，并考虑以下因素：
  - 在 威胁防御 上配置 IdP 时，必须配置 IdP 签名证书。
  - 威胁防御 不会对从 IdP 接收的签名证书执行吊销检查。
- SAML 断言中有 NotBefore 和 NotOnOrAfter 条件。威胁防御 SAML 配置的超时与这两个条件如下交互：
  - 如果 NotBefore 与超时之和早于 NotOnOrAfter，则超时将覆盖 NotOnOrAfter。
  - 如果 NotBefore + 超时晚于 NotOnOrAfter，则 NotOnOrAfter 生效。
  - 如果不存在 NotBefore 属性，威胁防御 将拒绝登录请求。如果不存在 NotOnOrAfter 属性且未设置 SAML 超时，威胁防御 将拒绝登录请求。
- 威胁防御 不适用于使用内部 SAML 的部署中的 Duo，由于在双因素身份验证（推送、代码、密码）的质询/响应期间发生 FQDN 更改，这会强制到客户端代理的 威胁防御 进行身份验证。
- 将 SAML 与 AnyConnect配合使用时，还需遵守这些准则：
  - 在嵌入式浏览器中不允许不受信任的服务器证书。
  - CLI 或 SBL 型号中不支持嵌入式浏览器 SAML 集成。
  - 在网络浏览器中建立的 SAML 身份验证不会与 AnyConnect 共享，反之亦然。
  - 根据具体配置，在使用嵌入式浏览器连接到前端时，会使用各种不同的方法。例如，尽管 AnyConnect 相比于 IPv6 连接更喜欢 IPv4 连接，但嵌入式浏览器可能更喜欢 IPv6，或反之亦然。同样，在尝试代理和收到失败后， AnyConnect 可能会回退到没有代理状态，而嵌入式浏览器在尝试代理并收到失败后可能会停止导航。

- 为了使用 SAML 功能，必须使您的 威胁防御 网络时间协议 (NTP) 服务器与 IdP NTP 服务器同步。
- 使用内部 IdP 登录后，您将无法访问包含 SSO 的内部服务器。
- SAML IdP NameID 属性确定用户的用户名，并且用于授权、记帐和 VPN 会话数据库。

配置 SAML 单点登录身份验证

开始之前

在使用 威胁防御 远程访问 VPN 配置 SAML 单点登录之前，请确保已完成以下操作：

- 使用 Duo 创建帐户。
- 下载并安装 Duo Access 网关。
- 从您的 SAML身份提供程序（Duo）获取以下信息。
  - 身份提供程序实体 ID URL
  - 登录 URL
  - 注销 URL
  - 标识提供程序证书
- 创建 SAML 单点登录服务器对象。有关详细信息，请参阅添加单点登录服务器，第 973 页。

注释 在使用远程访问 VPN 策略向导创建一个新的策略时，您可以在**连接配置文件 (Connection Profile)** 设置中创建一个单点登录服务器对象。

过程

步骤 1 选择**设备** > **VPN** > **远程接入**。

步骤 2 点击要为其配置 SAML 身份验证的远程访问 VPN 策略旁边的**编辑 (Edit)**。如果要创建新策略，请点击**添加 (Add)**。

步骤 3 点击要修改的连接配置文件上的**编辑 (Edit)**。

步骤 4 选择 **AAA** 设置，然后从**身份验证方式 (Authentication Method)** 下拉列表中选择 **SAML**。

步骤 5 选择所需的 SAML 单点登录服务器作为**身份验证服务器**。

步骤 6 配置远程访问 VPN 所需的设置。

步骤 7 在您的 威胁防御 设备上保存和部署远程访问 VPN 策略。

相关主题

配置远程访问 VPN 的 AAA 设置，第 1151 页

配置 SAML 授权

关于 SAML 授权

SAML 授权支持在 AAA 和动态访问策略 (DAP) 框架内的 SAML 断言中提供的用户属性。您可以在身份提供程序上将SAML断言属性配置为名称-值对，然后它们会被解析为字符串。接收的属性可供 DAP 使用，以便在 DAP 记录中定义选择条件时使用这些属性。SAML 断言 *cisco_group_policy* 会被用于确定要应用于 VPN 会话的组策略。

动态访问策略属性表示

在 DAP 表中，DAP 属性按以下格式表示：

```
aaa.saml.name = "value”
```

示例，*aaa.saml.department = ”finance"*

此属性可用于 DAP 选择，如下所示：

```
<attr>
<name>aaa.saml.department</name>
<value>finance</value>
<operation>EQ</operation>
</attr>
```

多值属性

DAP 中也支持多值属性，并且 DAP 表已建立索引：

```
aaa.saml.name.1 = "value”
aaa.saml.name.2 = "value"
```

Active Directory memberOf 属性

Active Directory (AD) memberOf 属性接受与通过 LDAP 查询的处理方式一致的特殊处理。

组名称由 DN 的 CN 属性来表示。

从授权服务器接收的属性示例：

```
memberOf = "CN=FTD-VPN-Group,OU=Users,OU=TechspotUsers,DC=techspot,DC=us"
 memberOf = "CN=Domain Admins,OU=Users,DC=techspot,DC=us”
```

动态访问策略属性：

```
aaa.saml.memberOf.1 = "FTD-VPN-Group”
aaa.saml.memberOf.2 = "Domain Admins"
```

cisco_group_policy 属性的解释

组策略可以通过SAML断言属性来指定。当威胁防御接收到属性“cisco_group_policy”时，相应的值会被用于选择连接组策略

配置 SAML 授权

开始之前

确保您已在服务器（例如 DUO）上配置单点登录，并完成所需的身份提供程序 (IdP) 和服务提供商 (SP) 设置。

有关详细信息，请参阅使用 SAML 2.0 的单点登录身份验证，第 1204 页。

过程

步骤 1 配置单点登录服务器对象（如果尚未配置）。

a) 选择**对象 (Object)** > **对象管理 (Object Management)** > **AAA服务器 (AAA Server)** > **单点登录服务器 (Single Sign-on Server)**。
b) 点击**添加单点登录服务器 (Add Single Sign-on Server)**。
c) 输入单点登录服务器详细信息，然后点击**保存 (Save)**。

有关详细信息，请参阅添加单点登录服务器，第 973 页。

步骤 2 在远程接入 VPN 连接配置文件中配置 SAML 身份验证 。

a) 选择**设备 (Devices)** > **远程访问 (Remote Access)**。
b) 点击要为其配置 SAML 授权或创建新策略的远程访问 VPN 策略上的**编辑 (Edit)**。
c) 编辑所需的连接配置文件，然后选择 **AAA**。
d) 从**身份验证服务器 (Authentication Server)** 下拉列表中选择单点登录服务器对象。
e) 保存远程访问 VPN 配置。

步骤 3 匹配 DAP 策略中的 SAML 条件。

a) 选择 **设备** > **Dynamic Access Policy**。
b) 创建新的 DAP 或编辑现有组。
c) 创建 DAP 记录或编辑现有记录。
d) 点击**AAA 条件 (AAA Criteria)** > **SAML 条件 (SAML Criteria)** > **添加 SAML 条件 (Add SAML Criteria)**。
e) 根据 SSO 服务器返回的 SAML 断言来创建 SAML 条件。

步骤 4 部署远程访问 VPN 配置。

相关主题

配置连接配置文件设置，第 1149 页
威胁防御组策略对象，第 1062 页

远程访问 VPN 示例

如何限制每个用户的 AnyConnect 带宽

本节介绍如何限制 VPN 用户使用 AnyConnect 客户端 到 Cisco Secure Firewall Threat Defense 远程访问 VPN 网关连接时消耗的最大带宽。您可以通过使用 威胁防御策略中的服务质量（QoS）限制最大带宽，以确保单个用户或组或多个用户不会接管整个资源。通过此配置，您可以优先处理关键流量，防止带宽占用和管理网络。如果当流量超出最大速率，威胁防御 会丢弃超额流量。

步骤	相应操作	更多信息
1	创建和设置领域。	创建 Active Directory 领域和领域目录， 第 1816 页
2	为新创建的领域中可用的用户或组创建 QoS 策略和 QoS 规则。	• 请参阅创建 QoS 策略， 第 603 页以创建 QoS 策略。 • 请参阅配置 QoS 规则， 第 604 页以创建 QoS 规则。
3	配置远程访问 VPN 策略，并选择新创建的领域进行用户身份验证。	创建新的远程接入 VPN 策略， 第 1142 页
4	部署远程访问 VPN 策略。	部署配置更改， 第 136 页

如何对基于用户 ID 的访问控制规则使用 VPN 身份

步骤	相应操作	更多信息
1	创建和设置领域。	创建 Active Directory 领域和领域目录， 第 1816 页。
2	创建身份策略并添加身份规则。	• 请参阅创建身份策略， 第 1887 页以创建身份策略。 • 请参阅创建身份规则， 第 1894 页以创建身份规则。
3	将身份策略与访问控制策略相关联。	将其他策略与访问控制相关联， 第 1276 页
4	配置远程访问 VPN 策略，并选择新创建的领域进行用户身份验证。	创建新的远程接入 VPN 策略， 第 1142 页
5	部署远程访问 VPN 策略。	部署配置更改， 第 136 页

配置威胁防御多证书身份验证

基于多证书的身份验证

基于多证书的身份验证允许 威胁防御 验证计算机或设备证书。可以在远程接入 VPN 连接配置文件中为基于证书的身份验证启用多个证书。它可以与 AAA 身份验证结合使用。远程接入 VPN 连接配置文件中的多证书选项允许通过证书同时对计算机和用户进行证书身份验证。除了对用户的身份证书进行身份验证以允许 RA VPN 访问之外，这样还可以确保设备是公司颁发的设备。管理员可以选择是从计算机证书还是用户证书获取会话的用户名。

如果配置了多个基于证书的身份验证，则会从 VPN 客户端获取两个证书：

- **第一个证书 (First Certificate)** - 对终端进行身份验证的计算机证书。
- **第二个证书 (Second Certificate)** - 对 VPN 用户进行身份验证的用户证书。

有关 威胁防御 证书的详细信息，请参阅管理 威胁防御 证书，第 1078 页。

限制

- 多证书身份验证当前会将证书数量限制为两个。
- AnyConnect 仅支持基于 RSA 的证书。
- 在 AnyConnect 汇聚身份验证期间，仅支持基于 SHA256、SHA384 和 SHA512 的证书。
- 证书身份验证不能与 SAML 身份验证结合使用。

从证书预填充用户名

预填充用户名选项允许解析证书中的字段，并将其用于后续AAA身份验证（主和辅助）。在使用两个证书进行身份验证时，管理员可以为预填充功能选择应从中派生的用户名的证书。默认情况下，用于预填充的用户名检索自用户证书（从 AnyConnect接收的第二个证书）。如果启用“仅证书”(Certificate Only) 身份验证方法，预填充的用户名会被用作 VPN 会话用户名。如果启用 AAA 和证书身份验证，VPN 会话用户名将基于预填充选项。

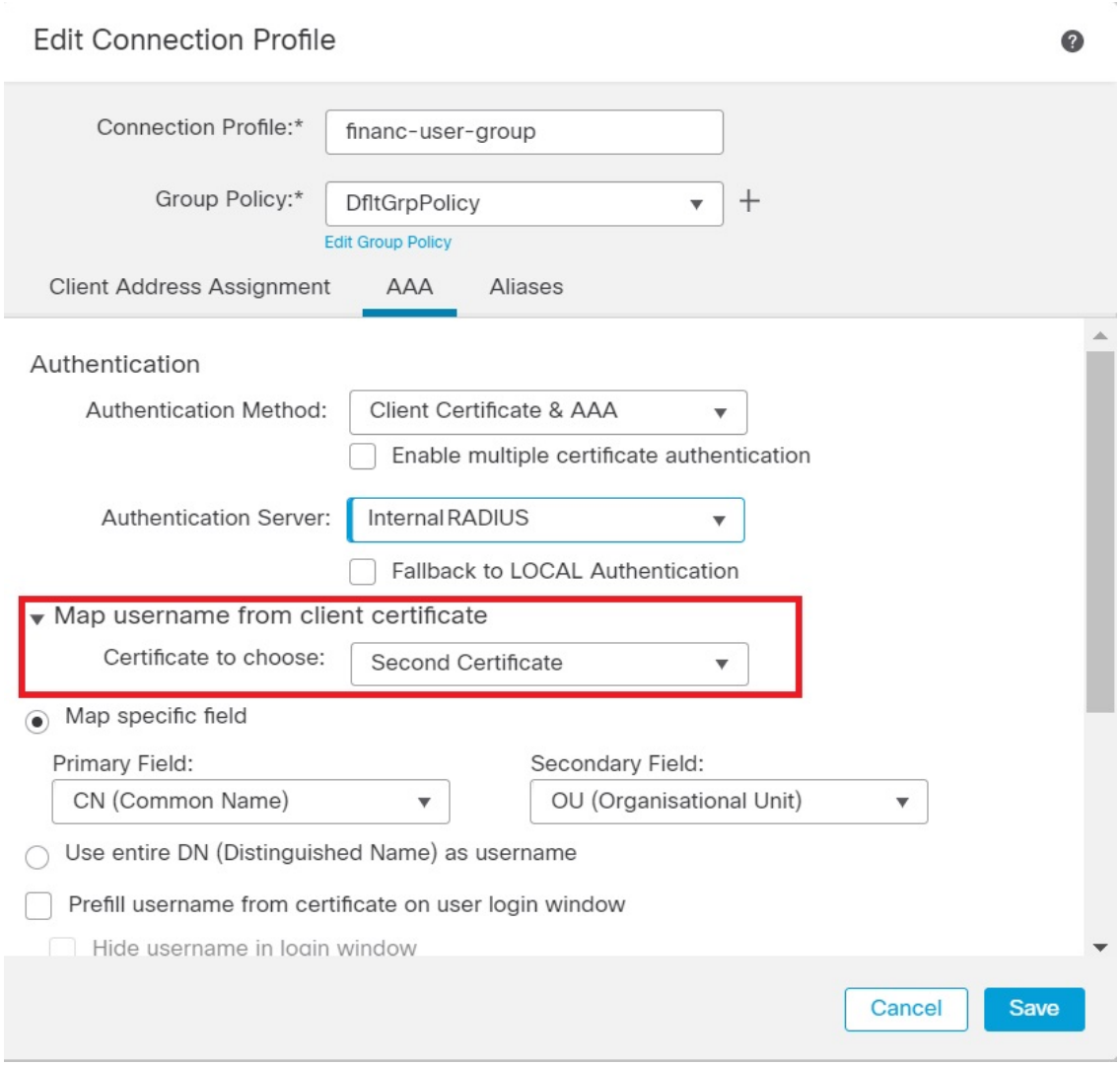
为远程接入 VPN 配置多证书身份验证

1. 在 Cisco Secure Firewall Management Center Web 界面上，选择**设备** > **VPN** > **远程接入**。
2. 编辑现有远程访问策略，或者创建新的策略并进行编辑。

   请参阅创建新的远程接入 VPN 策略，第 1142 页。
3. 选择连接配置文件以配置多证书身份验证，然后点击**编辑 (Edit)**。

   请参阅配置连接配置文件设置，第 1149 页。
4. 选择 **AAA**，然后选择**身份验证方法 (Authentication Method)**：

图 *142:*



- **仅客户端证书** - 使用客户端证书对用户进行身份验证。客户端证书必须在 VPN 客户端终端上配置。默认情况下，用户名分别派生自客户端证书字段 CN 和 OU。如果在客户端证书的其他字段中指定了用户名，请使用“主”(Primary) 和“辅助”(Secondary) 字段来映射适当的字段。
- **客户端证书和 AAA (Client Certificate & AAA)** - 使用 AAA 和客户端证书这两种身份验证类型来对用户进行身份验证。

5. 选择**启用多证书身份验证 (Enable multiple certificate authentication)**。
6. 选择**映射客户端证书中的用户名 (Map username from client certificate)**，然后从**可供选择的证书 (Certificate to choose)** 下拉列表中选择证书，以便从计算机证书或用户证书中选择 VPN 会话的用户名。
   - **第一个证书 (First Certificate)** - 映射计算机证书中的用户名。

- **第二个证书 (Second Certificate)** - 映射用户证书中的用户名，以便对 VPN 用户进行身份验证。

7. 配置所需的连接配置文件设置和远程访问 VPN 设置。
8. 保存连接配置文件和远程访问 VPN 策略。在 威胁防御 上部署远程访问 VPN 策略。

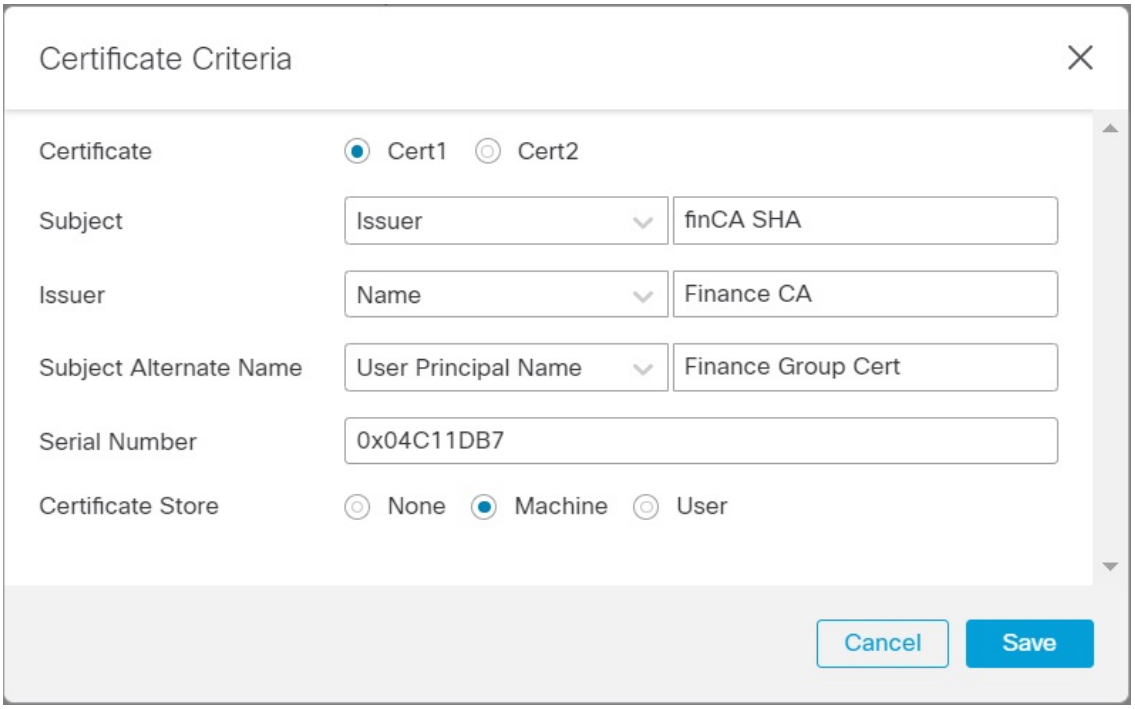
有关远程访问 VPN AAA 设置的信息，请参阅配置远程访问 VPN 的 AAA 设置，第 1151 页。

DAP 中的证书配置

您也可以在 DAP 记录中配置证书条件属性。将在多证书身份验证期间从 VPN 客户端收到的用户和计算机证书加载到动态访问策略 (DAP)，以确保能够根据证书字段配置策略。您可以根据证书字段制定策略决策，该证书用于对该连接尝试进行身份验证。

1. 依次选择**设备 (Devices)** > **动态访问策略 (Dynamic Access Policy)**。
2. 编辑现有 DAP 策略或创建新的 DAP 策略，然后编辑该策略。
3. 选择现有的 DAP 记录，或创建新的 DAP 记录并对其进行编辑。
4. 选择**终端条件 (Endpoint Criteria)** > **证书 (Certificate)**。
5. 选择匹配条件**所有 (All)** 或**任何 (Any)**。
6. 点击**添加 (Add)** 以添加证书属性。

图 *143:*



7. 选择证书 **Cert1** 或 **Cert2**。

8. 选择**使用者 (Subject)** 并指定证书使用者值。
9. 选择**颁发机构 (Issuer)** 并指定证书颁发机构名称。
10. 选择**使用者替代名称 (Subject Alternate Name)**，并为使用者指定替代名称。
11. 指定**序列号 (Serial Number)**。
12. 选择**证书存储区 (Certificate Store)**：无、计算机或用户。

    此选项会添加一个条件来检查在终端上要从中挑选证书的存储区。
13. 点击**保存 (Save)** 以完成证书条件设置。

    配置所需的 DAP 记录设置，然后将 DAP 与远程接入 VPN 关联。

有关 DAP 的详细信息，请参阅动态访问策略 ，第 1215 页。

第 47 章

动态访问策略

动态访问策略(DAP)让您能够配置解决VPN环境动态问题的授权。您可以设置一个与特定用户隧道或会话关联的访问控制属性集合，从而创建动态访问策略。这些属性可解决多重组成员身份和终端安全的问题。

关于 Cisco Secure Firewall Threat Defense 动态访问策略

VPN 网关在动态环境下运行。多个变量可能会影响每个 VPN 连接。例如，频繁更改内联网配置、每个用户在组织中可能有不同的角色，以及使用不同配置和安全级别从远程访问站点尝试登录。相比采用静态配置的网络，授权用户的任务在 VPN 环境中更为复杂。

您可以设置一个与特定用户隧道或会话关联的访问控制属性集合，从而创建动态访问策略。这些属性可解决多重组成员身份和终端安全的问题。威胁防御会根据您定义的策略，为特定的会话向特定用户授予访问权限。 威胁防御 设备会通过从一个或多个 DAP 记录中选择或汇总属性，从而在用户身份验证期间生成 DAP。然后，设备会根据远程设备的终端安全信息，以及经过身份验证的用户的 AAA 授权信息，选择这些 DAP 记录。然后，设备会将 DAP 记录应用至用户隧道或会话。

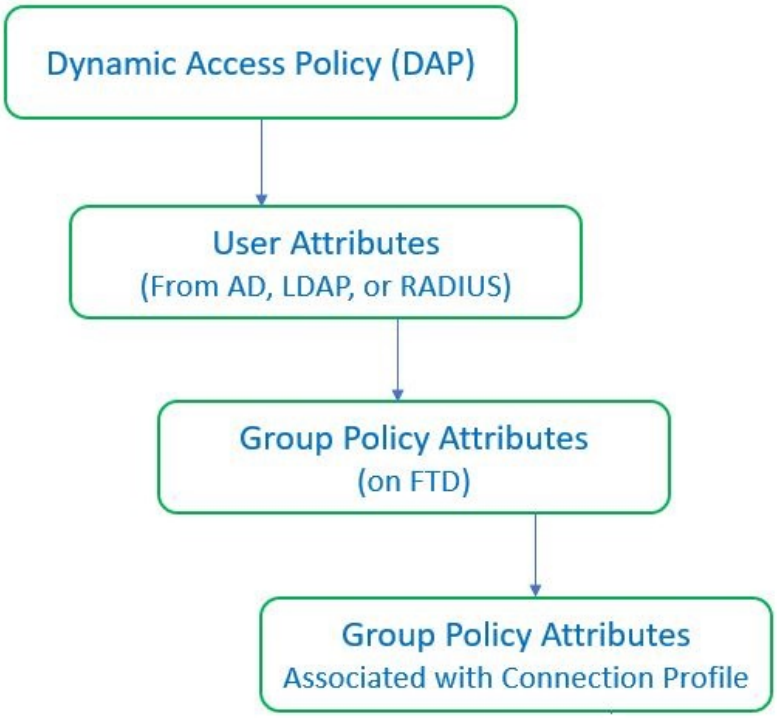
威胁防御 中权限和属性的策略实施层次结构

威胁防御 设备支持将用户授权属性（也称为用户授权或权限）应用到 VPN 连接。从 威胁防御 上的 DAP、外部身份验证服务器和/或授权 AAA 服务器 (RADIUS) 或从 威胁防御 设备上的组策略应用属性。

如果威胁防御设备收到来自所有来源的属性，将会对这些属性进行评估、合并，并将其应用至用户策略。如果来自 DAP、AAA 服务器或组策略的属性之间存在冲突，从 DAP 获得的属性始终会被优先考虑。

威胁防御设备按照以下顺序应用属性：

图 *144:* 策略实施流程



1. **FTD 上的 DAP 属性** - DAP 属性优先于所有其他的属性。
2. **外部 AAA 服务器上的用户属性** - 该服务器在用户身份验证和/或授权成功后返回这些属性。
3. **FTD 上配置的组策略** - 如果 RADIUS 服务器为用户返回 RADIUS 类属性 IETF-Class-25 (OU=group-policy) 值，威胁防御 设备会将该用户放在名称相同的组策略中，并实施组策略中该服务器未返回的所有属性。
4. **连接配置文件 (也称为隧道组) 分配的组策略**- 连接配置文件具有该连接的初步设置，包括在进行身份验证前应用于用户的默认组策略。

注释 威胁防御设备不支持从默认组策略 *DfltGrpPolicy* 继承系统默认属性。对于用户会话，设备会使用您分配给连接配置文件的组策略上的属性，除非它们被来自 AAA 服务器的用户属性或组策略覆盖。

动态访问策略许可

威胁防御必须具有以下AnyConnect 客户端许可证之一：

- AnyConnect Apex
- AnyConnect Plus
- 仅限 AnyConnect VPN

基本许可证必须允许出口控制功能。

动态访问策略的必备条件

表 *90:*

前提条件类型	说明

许可	• 威胁防御 必须至少拥有以下 AnyConnect 客户端 许可证之一：
	  • AnyConnect Apex
	  • AnyConnect Plus
	  • 仅限 AnyConnect VPN
	• 威胁防御 基本许可证必须允许出口控制功能。

配置	有关前提条件的详细信息，请参阅《*Firepower* 管理中心配置指南》中的*Cisco Secure Firewall Threat Defense* 动态访问策略部分。 有关远程访问 VPN 必备条件和配置的详细信息，请参阅《*Firepower* 管理中心配置指南》的 *Cisco Secure Firewall Threat Defense* 远程访问 *VPN* 部分。

动态访问策略的准则与限制

- 只有当AAA服务器被配置为在对远程接入VPN会话进行身份验证或授权时返回正确的属性时，才能匹配 DAP 中的 AAA 属性。

- DAP 支持的最低 AnyConnect 和 HostScan 软件包版本为 4.6。但是强烈建议使用最新版本的 AnyConnect。

配置动态访问策略 (DAP)

创建动态访问策略

开始之前

在配置动态访问策略之前，请确保您拥有 HostScan 软件包。您可以通过 **对象 (Objects)** > **对象管理 (Object Management)** > **VPN** > **AnyConnect 文件 (AnyConnect File)** 来添加 HostScan 文件。

过程

步骤 1 依次选择**设备 (Devices)** > **动态访问策略 (Dynamic Access Policy)** > **创建动态访问策略 (Create Dynamic Access Policy)**。

步骤 2 为 DAP 策略指定**名称 (Name)** 和可选的**说明 (Description)**。

步骤 3 从列表中选择 **HostScan 软件包 (HostScan Package)**。

步骤 4 点击**保存**。

下一步做什么

要配置 DAP 记录，请参阅创建动态访问策略记录

创建动态访问策略记录

动态访问策略 (DAP) 可以包含多个 DAP 记录，您可以在这些记录中配置用户和终端属性。您可以确定 DAP 内的 DAP 记录的优先级，以便 威胁防御 在用户尝试 VPN 连接时选择和排序所需的条件。

过程

步骤 1 依次选择**设备 (Devices)** > **动态访问策略 (Dynamic Access Policy)**。

步骤 2 编辑现有动态访问策略或创建新策略，然后编辑该策略。

步骤 3 指定 DAP 记录的**名称 (Name)**。

步骤 4 为 DAP 记录输入**优先级 (Priority)**。

数值越低，优先级越高。

步骤 5 选择当 DAP 记录匹配时要执行的以下操作之一：

- **继续 (Continue)** - 点击以将访问策略属性应用于会话。
- **终止 (Terminate)** - 选择以终止会话。
- **隔离 (Quarantine)** - 选择以隔离连接。

步骤 6 选中**在条件匹配时显示用户消息 (Display User Message on Criterion Match)** 复选框并添加用户消息。

当 DAP 记录匹配，威胁防御 将此消息显示给用户。

步骤 7 选中**对流量应用网络 ACL (Apply a Network ACL on Traffic)** 复选框，然后从下拉列表中选择访问控制列表。

步骤 8 选中**应用一个或多个 AnyConnect 自定义属性 (Apply one or more AnyConnect Custom Attributes)** 复选框，然后从下拉列表中选择自定义属性对象。

步骤 9 点击**保存 (Save)**。

配置 DAP 的 AAA 标准设置

DAP 可提供一组限定的授权属性，这些属性可覆盖 AAA 提供的属性，从而补充 AAA 服务。威胁防御 会根据用户的 AAA 授权信息和会话的终端安全评估信息选择 DAP 记录。威胁防御 可根据此信息选择多个 DAP 记录，然后将其汇聚以创建 DAP 授权属性。

过程

步骤 1 依次选择**设备 (Devices)** > **动态访问策略 (Dynamic Access Policy)**。

步骤 2 编辑现有 DAP 策略或创建新的 DAP 策略，然后编辑该策略。

步骤 3 选择 DAP 记录或创建新记录，然后编辑 DAP 记录。

步骤 4 点击 **AAA 条件 (AAA Criteria)**。

步骤 5 选择**部分之间匹配条件**之一。

- 任意 (Any) - 匹配任意条件。
- 全部 (All) - 匹配所有条件。
- 无 (None) - 不匹配任何设定的条件。

步骤 6 点击**添加 (Add)** 以添加所需的**思科 VPN 条件**。

思科 VPN 条件包括组策略的属性、分配的 IPv4 地址、分配的 IPv6 地址、连接配置文件、用户名、用户名 2 和所需的 SCEP。

a) 选择属性并指定 **值**。

b) 点击**添加其他条件 (Add another criteria)** 以添加更多条件。

c) 点击**保存 (Save)**。

需要 SCEP

步骤 7 选择 **LDAP 条件**、 **RADIUS 条件**或 **SAML 条件** 并指定 **属性 ID** 和 **值 (**。

步骤 8 点击**保存 (Save)**。

在 DAP 中配置终端属性选择条件

终端属性包含终端系统环境、终端安全评估结果和应用的相关信息。威胁防御 会在会话建立期间动态生成终端属性的集合，并将这些属性存储在与此会话关联的数据库中。每个DAP记录指定终端选择属性，这些属性必须得到满足，威胁防御才能选择将其用于会话。威胁防御仅选择满足每个配置的条件的 DAP 记录。

过程

步骤 1 依次选择**设备 (Devices)** > **动态访问策略 (Dynamic Access Policy)** > **创建动态访问策略 (Create Dynamic Access Policy)**。

步骤 2 编辑 DAP 策略，然后编辑 DAP 记录。

注释 创建 DAP 策略和 DAP 记录（如果尚未创建）。

步骤 3 点击**终端条件 (Endpoint Criteria)** 并配置以下终端条件属性：

注释 您可以创建每个终端属性类型的多个实例。每个 DAP 记录的终端属性数量没有限制。

- 向 DAP 添加 Anti-Malware 终端属性
- 向 DAP 添加设备终端属性
- 向 DAP 添加 AnyConnect终端属性， 第 1222 页
- 向 DAP 添加 NAC 终端属性
- 向 DAP 添加应用属性
- 向 DAP 添加个人防火墙终端属性
- 向 DAP 添加操作系统终端属性
- 向 DAP 添加流程终端属性
- 向 DAP 添加注册表终端属性
- 向 DAP 添加文件终端属性
- 向 DAP 添加证书身份验证属性

步骤 4 点击**保存 (Save)**。

向 DAP 添加 Anti-Malware 终端属性

过程

步骤 1 编辑 DAP 记录，然后选择**终端条件 (Endpoint Criteria)** > **防恶意软件 (Anti-Malware)**。

步骤 2 选择匹配条件**所有 (All)** 或**任何 (Any)**。

步骤 3 点击**添加 (Add)** 以添加防恶意软件属性。

步骤 4 点击**已安装 (Installed)** 以指示安装还是不安装所选终端属性及其附带限定词。

步骤 5 选择**已启用 (Enabled)** 或**已禁用 (Disabled)** 以激活或停用实时恶意软件扫描。

步骤 6 从列表中选择防恶意软件**供应商**的名称。

步骤 7 选择防恶意软件的**产品说明 (Product Description)**。

步骤 8 选择防恶意软件产品的**版本 (Version)**。

步骤 9 指定距离**上次更新 (Last Update)** 的天数。

您可以指明防恶意软件更新时间应小于 (<) 或大于 (>) 您指定的天数。

步骤 10 点击**保存 (Save)**。

向 DAP 添加设备终端属性

过程

步骤 1 编辑 DAP 记录，然后选择**终端条件 (Endpoint Criteria)** > **设备 (Device)**。

步骤 2 选择匹配条件**所有 (All)** 或**任何 (Any)**。

步骤 3 点击**添加 (Add)** 并选择 = 或 ≠ 运算符，以检查属性是否等于或不等于你为以下属性输入的值。

- **主机名 (Host Name)** - 要测试的设备的主机名。此处仅会使用计算机的主机名，而不是完全限定域名 (FQDN)。
- **MAC 地址 (MAC Address)** - 要测试的网络接口卡的 MAC 地址。 地址必须是 xxxx.xxxx.xxxx 格式，其中 x 是十六进制字符。
- **BIOS 序列号 (BIOS Serial Number)** - 要测试的设备的 BIOS 序列号值。此编号格式由制造商指定。
- **端口号 (Port Number)** - 设备的侦听端口号。
- **安全桌面版本 (Secure Desktop Version)** - 在终端上运行的主机扫描映像的版本。
- **OPSWAT 版本 (OPSWAT Version)** - OPSWAT 客户端版本。
- **隐私保护 (Privacy Protection)** - 无、缓存清理器、安全桌面。
- **TCP/UDP 端口号 (TCP/UDP Port Number)** - 您正在测试的处于侦听状态的 TCP 或 UDP 端口。

步骤 4 点击保存 (Save)。

向 DAP 添加 AnyConnect终端属性

过程

步骤 1 编辑 DAP 记录，然后选择终端条件 (Endpoint Criteria) > AnyConnect。

步骤 2 选择匹配条件所有 (All) 或任何 (Any)。

步骤 3 点击添加 (Add) 并选择 = 或 ≠ 运算符，以检查属性是否等于您输入的值。

步骤 4 选择客户端版本 (Client Version) 和平台 (Platform)。

步骤 5 选择平台版本 (Platform Version)，然后指定设备类型 (Device Type) 和设备唯一 ID (Device Unique ID)。

步骤 6 将 MAC 地址添加到 MAC 地址池中。

注释 MAC 地址必须是 XX-XX-XX-XX-XX-XX 格式，其中每个 X 都是十六进制字符。您可以点击添加另一个 MAC 地址 (Add another MAC Address) 以添加更多地址。

步骤 7 点击保存 (Save)。

向 DAP 添加 NAC 终端属性

过程

步骤 1 编辑 DAP 记录，然后选择终端条件 (Endpoint Criteria) > NAC。

步骤 2 选择匹配条件所有 (All) 或任何 (Any)。

步骤 3 点击添加 (Add) 以添加 NAC 属性。

步骤 4 将运算符设置为等于 = 或不等于 ≠ 安全评估状态字符串。在安全评估状态 (Posture Status) 框中输入安全评估标记字符串。

步骤 5 点击保存 (Save)。

向 DAP 添加应用属性

过程

步骤 1 编辑 DAP 记录，然后选择终端条件 (Endpoint Criteria) > 应用 (Application)。

步骤 2 选择匹配条件所有 (All) 或任何 (Any)。

步骤 3 点击**添加 (Add)** 以添加应用属性。

步骤 4 选择等于 (=) 或不等于 (≠) 并指定表明远程访问连接类型的**客户端类型**。

步骤 5 点击**保存 (Save)**。

向 DAP 添加个人防火墙终端属性

过程

步骤 1 编辑 DAP 记录，然后选择**终端条件 (Endpoint Criteria)** > **个人防火墙 (Personal Firewall)**。

步骤 2 选择匹配条件**所有 (All)** 或**任何 (Any)**。

步骤 3 点击**添加 (Add)** 以添加个人防火墙属性。

步骤 4 点击**已安装 (Installed)** 以指示安装还是不安装个人防火墙终端属性及其附带限定词（“名称”/“操作”/“值”列下面的字段）。

步骤 5 选择**启用 (Enabled)** 或**禁用 (Disabled)** 以激活或停用防火墙保护。

步骤 6 从列表中选择防火墙**供应商 (Vendor)** 的名称。

步骤 7 选择防火墙的**产品说明 (Product Description)**。

步骤 8 选择等于 (=) 或不等于 (≠) 运算符，然后选择防恶意软件产品的**版本**。

步骤 9 点击**保存 (Save)**。

向 DAP 添加操作系统终端属性

过程

步骤 1 编辑 DAP 记录，然后选择**终端条件 (Endpoint Criteria)** > **操作系统 (Operating System)**。

步骤 2 选择匹配条件**所有 (All)** 或**任何 (Any)**。

步骤 3 点击**添加 (Add)** 以添加终端属性。

步骤 4 选择等于 (=) 或不等于 (≠) 运算符，然后选择**操作系统 (Operating System)**。

步骤 5 选择等于 (=) 或不等于 (≠) 运算符，然后制定操作系统**版本 (Version)**。

步骤 6 点击**保存 (Save)**。

向 DAP 添加流程终端属性

过程

步骤 1 编辑 DAP 记录，然后选择**终端条件 (Endpoint Criteria)** > **流程 (Process)**。

步骤 2 选择匹配条件**所有 (All)** 或**任何 (Any)**。
步骤 3 点击**添加 (Add)** 以添加流程属性。
步骤 4 选择**存在 (Exists)** 或**不存在 (Does not exist)**。
步骤 5 指定**进程名称 (Process Name)**。
步骤 6 点击**保存 (Save)**。

向 DAP 添加注册表终端属性

扫描注册表终端属性仅适用于 Windows 操作系统。

开始之前

在配置注册表终端属性之前，请为思科安全桌面定义要在 Host Scan 窗口中扫描的注册表项。

过程

步骤 1 编辑 DAP 记录，然后选择**终端条件 (Endpoint Criteria)** > **注册表 (Registry)**。
步骤 2 选择匹配条件**所有 (All)** 或**任何 (Any)**。
步骤 3 点击**添加 (Add)** 以添加注册表属性。
步骤 4 选择注册表的**条目路径 (Entry Path)** 并指定路径。
步骤 5 选择注册表是**存在 (Exists)** 还是**不存在 (Does not Exist)**。
步骤 6 从列表中选择注册表**类型 (Type)**。
步骤 7 选择等于 (=) 或不等于 (≠) 运算符，然后输入注册表项的**值**。
步骤 8 选择**不区分大小写 (Case insensitive)** 以便在扫描时忽略注册表项的大小写。
步骤 9 点击**保存 (Save)**。

向 DAP 添加文件终端属性

过程

步骤 1 编辑 DAP 记录，然后选择**终端条件 (Endpoint Criteria)** > **文件 (File)**。
步骤 2 选择匹配条件**所有 (All)** 或**任何 (Any)**。
步骤 3 点击**添加 (Add)** 以添加文件属性。
步骤 4 指定**文件路径**。
步骤 5 选择**存在 (Exists)** 或**不存在 (Does not Exist)** 以指明文件是否存在。
步骤 6 选择小于 (<) 或大于 (>) 并指定文件的**上次修改 (Last Modified)** 天数。
步骤 7 选择等于 (=) 或不等于 ≠ 运算符，然后输入**校验和 (Checksum)**。

步骤 8 点击**保存 (Save)**。

向 DAP 添加证书身份验证属性

您可以对每个证书编制索引，以便配置的规则可以引用接收到的任何证书。以这些证书字段为基础，您可以配置 DAP 规则来允许或禁止连接尝试。

过程

步骤 1 编辑 DAP 记录，然后选择**终端条件 (Endpoint Criteria)** > **证书 (Certificate)**。

步骤 2 选择匹配条件**所有 (All)** 或**任何 (Any)**。

步骤 3 点击**添加 (Add)** 以添加证书属性。

步骤 4 选择证书 **Cert1** 或 **Cert2**。

步骤 5 选择**使用者 (Subject)** 并指定使用者值。

步骤 6 选择**颁发机构 (Issuer)** 并指定颁发机构值。

步骤 7 选择**使用者替代名称 (Subject Alternate Name)** 并指定使用者值。

步骤 8 指定**序列号 (Serial Number)**。

步骤 9 选择**证书存储区 (Certificate Store)**：无、计算机或用户。

VPN 客户端发送证书存储区信息。

步骤 10 点击**保存 (Save)**。

配置 DAP 的高级设置

您可以使用“高级”(Advanced) 选项卡来添加除 AAA 和端点属性区域中可能存在的选择条件。例如，在您将 威胁防御 配置为使用 AAA 属性（这些属性满足任意、所有指定条件，或者不需要满足指定条件）时，终端属性是累计的，并且必须全部满足。要让安全设备使用一个或另一个终端属性，您必须创建适当的 Lua 逻辑表达式，并在此处输入它们。

过程

步骤 1 依次选择**设备 (Devices)** > **动态访问策略 (Dynamic Access Policy)**。

步骤 2 编辑 DAP 策略，然后编辑 DAP 记录。

注释 创建 DAP 策略和 DAP 记录（如果尚未创建）。

步骤 3 点击**高级 (Advanced)** 选项卡。

步骤 4 选择 **AND** 或 **OR** 作为要在 DAP 配置上使用的匹配条件。

步骤 5 在**用于高级属性匹配的 Lua 脚本 (Lua script for advanced attribute matching)** 字段中添加 Lua 脚本。

步骤 6 点击**保存 (Save)**。

将动态访问策略与远程访问 VPN 关联

您可以将动态访问策略 (DAP) 与远程访问 VPN 策略关联，以便在 VPN 会话身份验证和授权期间匹配动态访问策略属性。您可以在 威胁防御 上部署远程访问 VPN。

过程

步骤 1 选择**设备 (Devices)** > **远程访问 (Remote Access)**。

步骤 2 点击要与动态访问策略关联的远程访问 VPN 策略旁边的**编辑 (Edit)**。

步骤 3 点击远程访问 VPN 中的链接以选择动态访问策略。

步骤 4 从**动态访问策略 (Dynamic Access Policy)** 下拉列表中选择策略，或点击**创建新的动态访问策略 (Create a new Dynamic Access Policy)** 以配置新的动态访问策略。

步骤 5 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)** 以保存远程访问 VPN 策略。

当远程访问 VPN 用户尝试连接时，VPN 会检查配置的动态访问策略记录和属性。VPN 会根据匹配的动态访问策略记录来创建动态访问策略，并对 VPN 会话执行适当的操作。

动态访问策略的历史记录

特性	版本	详细信息
动态访问策略	7.0	引入了此功能。

第 48 章

CDO 中的VPN 监控和故障排除

监控远程访问 VPN 会话

CDO 远程访问监控控制面板可用于查看有关 RA VPN 用户的整合信息，包括用户当前状态、设备类型、客户端应用、用户地理位置信息和连接持续时间。您还可以根据需要断开 RA VPN 会话。

执行以下操作以查看 VPN 会话：

1. 在云交付的防火墙管理中心页面中，点击**返回主页 (Return Home)**。
2. 在 CDO 导航窗格中，点击 **VPN** > **远程访问 VPN 监控 (Remote Access VPN Monitoring)**。

有关详细信息，请参阅监控远程访问虚拟专用网络会话。

系统消息

邮件中心是开始进行故障排除的地方。通过此功能，可以查看持续生成的有关系统活动和状态的消息。要打开消息中心，请点击位于主菜单中**部署 (Deploy)** 按钮正右侧的**系统状态 (System Status)**。

VPN 系统日志

您可以为 威胁防御设备启用系统日志记录（系统日志）。日志记录信息可以帮助您发现并隔离网络或设备配置问题。启用 VPN 日志记录时，这些系统日志将从威胁防御设备发送到Cisco Secure Firewall Management Center进行分析和存档。

所有出现的 VPN 系统日志都具有默认严重性级别“错误”(ERROR) 或更高（除非已更改）。您可以通过威胁防御平台设置来管理 VPN 日志记录。您可以通过编辑目标设备的威胁防御平台设置策略

中的 **VPN 日志记录设置 (VPN Logging Settings)** 来调整消息严重性级别（**平台设置 (Platform Settings)** > **系统日志 (Syslog)** > **日志记录设置 (Logging Setup)**）。有关启用 VPN 日志记录、配置系统日志服务器以及查看系统日志的详细信息，请参阅配置系统日志 ， 第 644 页。

注释 只要您配置了具有站点间或远程访问 VPN 的设备，它就会默认自动启用将 VPN 系统日志发送至 管理中心。

查看 VPN 系统日志

系统捕获事件信息，以帮助您收集有关 VPN 问题源的其他信息。显示的任何 VPN 系统日志都具有默认严重性级别“ERROR”或更高（除非已更改）。默认情况下，行按**时间**列排序。

您必须是枝叶域中的管理员用户才能执行此任务。

开始之前

通过选中 威胁防御平台设备中的**使记录至 FMC** 复选框，启用 VPN 日志记录（**设备** > **平台设置** > **系统日志** > **日志记录设置**）。有关启用 VPN 日志记录、配置系统日志服务器以及查看系统性记录的详细信息，请参阅配置系统日志 ， 第 644 页。

过程

步骤 1 选择**设备** > **VPN** > **故障排除**。

步骤 2 您有以下选择：

- 搜索 - 要过滤当前消息信息，请点击**编辑搜索 (Edit Search)**。
- 查看 - 要查看与视图中所选消息关联的 VPN 详细信息，请点击**查看 (View)**。
- 查看全部 - 要查看视图中所有消息的事件详细信息，请点击**查看全部 (View All)**。
- 删除 - 要从数据库中删除选定的消息，请点击**删除 (Delete)** 或点击**全部删除 (Delete All)** 以删除所有消息。

调试命令

本节介绍如何使用调试命令来帮助您诊断和解决与 VPN 相关的问题。此处介绍的命令并非详尽无遗，本节将根据命令的作用来帮助您诊断 VPN 相关问题。

使用指南

由于调试输出在CPU进程中享有高优先级，因此可导致系统不可用。为此，应仅在对特定问题进行故障排除或与思科 Technical Assistance Center (TAC) 进行故障排除会话时使用 **debug** 命令。此外，最好在网络流量较低和用户较少时使用 **debug** 命令。在这些时段进行调试会减少因 **debug** 命令处理开销增加而影响系统使用的可能性。

您只能在 CLI 会话中查看调试输出。在连接到控制台端口的情况下，或者在诊断 CLI 中，您可以直接查看输出结果（输入 **system support diagnostic-cli**）。此外，您也可以在常规 Firepower Threat Defense CLI 中使用 **show console-output** 命令查看输出结果。

要显示给定功能的调试消息，请使用 **debug** 命令。要禁用调试消息的显示，请使用此命令的 **no** 形式。使用 **no debug all** 关闭所有调试命令。

debug *feature* [*subfeature*] [*level*]
no debug *feature* [*subfeature*]

Syntax Description

feature	指定要为其启用调试的功能。若要查看可用功能，请使用 **debug ?** 命令获取 CLI 帮助。
subfeature	（可选）根据功能，您可以为一项或多项子功能启用调试消息。使用 ? 查看可用的子功能。
级别	（可选）指定调试级别。使用 ? 可查看可用的级别。

Command Default

默认调试级别为 1。

示例

在远程接入 VPN 上运行多个会话时，由于日志的大小，可能会很难进行故障排除。可以使用 **debug webvpn condition** 命令设置过滤器，以便更精确地定位调试进程。

debug webvpn condition { **group** *name* | **p-ipaddress** *ip_address* [{ **subnet** *subnet_mask* | **prefix** *length*}] | **reset** | **user** *name*}

其中：

- **group** *name* 对组策略进行过滤，而不是隧道组或连接配置文件。
- **p-ipaddress** *ip_address* [{**subnet** *subnet_mask* | **prefix** *length*}] 对客户端的公共 IP 地址进行过滤。子网掩码（用于 IPv4）或前缀（用于 IPv6）是可选的。
- **reset** 重置所有过滤器。可以使用 **no debug webvpn condition** 命令关闭特定的过滤器。
- **user** *Name* 按用户名过滤。

如果配置多个条件，则条件是合并的 (AND)，因此只有满足所有条件时才显示调试。

设置条件过滤器后，使用基本 **debug webvpn** 命令打开调试。只设置条件不会启用调试。使用 **show debug** 和 **show webvpn debug-condition** 命令查看调试的当前状态。

下文是在用户 jdoe 上启用条件调试的示例。

```
firepower# debug webvpn condition user jdoe

firepower# show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

```
firepower# debug webvpn
INFO: debug webvpn  enabled at level 1.

firepower# show debug
debug webvpn  enabled at level 1
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

Related Commands

命令	说明
show debug	显示当前活动的调试设置。
undebug	禁用功能调试。此命令与 **no debug** 的效果相同。

调试 aaa

请参阅以下命令以调试配置或身份验证、授权和记帐 (AAA) 设置。

debug *aaa* [*accounting* | *authentication* | *authorization* | *common* | *internal* | *shim* | *url-redirect*]

Syntax Description

aaa	启用对 AAA 的调试。使用 ? 查看可用的子功能。
accounting	（可选）启用 AAA 记帐调试。
authentication	（可选）启用 AAA 身份验证调试。
authorization	（可选）启用 AAA 授权调试。
common	（可选）指定 AAA 通用调试级别。使用 ? 查看可用的级别。
internal	（可选）启用 AAA 内部调试。
shim	（可选）指定 AAA shim 调试级别。使用 ? 查看可用的级别。
url-redirect	（可选）启用 AAA url-redirect 调试。

Command Default

默认调试级别为 1。

Related Commands

命令	说明
show debug aaa	显示 AAA 当前的活动调试设置。
undebug aaa	禁用 AAA 的调试。此命令与 **no debug aaa** 的效果相同。

debug crypto

请参阅以下用于调试与 crypto 相关联的配置或设置的命令。

debug *crypto* [*ca* | *condition* | *engine* | *ike-common* | *ikev1* | *ikev2* | *ipsec* | *ss-apic*]

Syntax Description

crypto	启用对 *crypto* 的调试。使用 ? 查看可用的子功能。
ca	（可选）指定 PKI 调试级别。可以使用 ? 查看可用子功能。
condition	（可选）指定 IPsec/ISAKMP 调试过滤器。可以使用 ? 查看可用过滤器。
engine	（可选）指定 crypto 引擎调试级别。可以使用 ? 查看可用级别。
ike-common	（可选）指定 IKE 常用调试级别。可以使用 ? 查看可用级别。
ikev1	（可选）指定 IKE 版本 1 调试级别。可以使用 ? 查看可用级别。
ikev2	（可选）指定 IKE 版本 2 调试级别。可以使用 ? 查看可用级别。
ipsec	（可选）指定 IPsec 调试级别。使用 ? 可查看可用的级别。
condition	（可选）指定 Crypto 安全套接字 API 调试级别。可以使用 ? 查看可用级别。
vpnclient	（可选）指定 EasyVPN 客户端调试级别。使用 ? 可查看可用的级别。

Command Default

默认调试级别为 1。

Related Commands

命令	说明
show debug crypto	显示当前处于活动状态的适用于 crypto 的调试设置。
undebug crypto	禁用对 crypto 的调试。此命令与 **no debug crypto** 的效果相同。

debug crypto ca

请参阅以下用于调试与 crypto ca 相关联的配置或设置的命令。

debug *crypto ca* [*cluster* | *messages* | *periodic-authentication* | *scep-proxy* | *transactions* | *trustpool*] [*1-255*]

Syntax Description

crypto ca	启用对 *crypto ca* 的调试。使用 ? 查看可用的子功能。
cluster	（可选）指定 PKI 集群调试级别。可以使用 ? 查看可用级别。
cmp	（可选）指定 CMP 交易调试级别。可以使用 ? 查看可用级别。
messages	（可选）指定 PKI 输入/输出消息调试级别。可以使用 ? 查看可用级别。

periodic-authentication	（可选）指定 PKI 周期性身份验证调试级别。可以使用 ? 查看可用级别。
scep-proxy	（可选）指定 SCEP 代理调试级别。可以使用 ? 查看可用级别。
server	（可选）指定本地 CA 服务器调试级别。可以使用 ? 查看可用级别。
transactions	（可选）指定 PKI 交易调试级别。可以使用 ? 查看可用级别。
trustpool	（可选）指定信任池调试级别。使用 ? 查看可用的级别。
1-255	（可选）指定调试级别。

Command Default 默认调试级别为 1。

Related Commands

命令	说明
show debug crypto ca	显示当前处于活动状态的适用于 crypto ca 的调试设置。
undebug	禁用对 crypto ca 的调试。此命令与 **no debug crypto ca** 的效果相同。

debug crypto ikev1

有关与 Internet 密钥交换版本 1 (IKEv1) 相关联的调试配置或设置，请参阅以下命令。

debug *crypto ikev1* ［*timers*］［*1-255*］

Syntax Description

ikev1	启用 *ikev1* 调试。使用 ? 查看可用的子功能。
timers	（可选）启用 IKEv1 计时器调试。
1-255	（可选）指定调试级别。

Command Default 默认调试级别为 1。

Related Commands

命令	说明
show debug crypto ikev1	显示 IKEv1 的当前活动调试设置。
undebug crypto ikev1	禁用 IKEv1 调试。此命令与 **no debug crypto ikev1** 的效果相同。

debug crypto ikev2

有关与 Internet 密钥交换版本 2 (IKEv2) 相关联的调试配置或设置，请参见以下命令。

debug *crypto ikev2* ［*ha* | *platform* | *protocol* | *timers*］

Syntax Description

ikev2	启用调试 *ikev2*。使用 ? 查看可用的子功能。

ha	（可选）指定 IKEv2 HA 调试级别。使用 ? 查看可用的级别。
platform	（可选）指定 IKEv2 平台调试级别。使用 ? 查看可用的级别。
protocol	（可选）指定 IKEv2 协议调试级别。使用 ? 查看可用的级别。
timers	（可选）启用针对 IKEv2 计时器的调试。

Command Default 默认调试级别为 1。

Related Commands

命令	说明
show debug crypto ikev2	显示 IKEv2 的当前活动调试设置。
undebugcrypto ikev2	禁用针对 IKEv2 的调试。此命令与 **no debug crypto ikev2** 的效果相同。

debug crypto ipsec

有关调试与 IPsec 关联的配置或设置的信息，请参阅以下命令。

debug *crypto ipsec* ［*1-255*］

Syntax Description

ipsec	启用对 *ipsec* 的调试要使用 ? 请查看可用的子功能。
1-255	（可选）指定调试级别。

Command Default 默认调试级别为 1。

Related Commands

命令	说明
show debug crypto ipsec	显示 IPsec 的当前活动调试设置。
undebugcrypto ipsec	禁用对 IPsec 的调试。此命令与 **no debug crypto ipsec** 的效果相同。

debug ldap

有关调试与 LDAP 关联的配置或设置的信息（轻量级目录访问协议），请参阅以下命令。

debug *ldap* ［*1-255*］

Syntax Description

ldap	启用对 LDAP 的调试。要使用 ? 请查看可用的子功能。
1-255	（可选）指定调试级别。

Command Default 默认调试级别为 1。

Related Commands

命令	说明
show debug ldap	显示 LDAP 的当前活动调试设置。
undebugldap	禁用对 LDAP 的调试。此命令与 **no debug ldap** 的效果相同。

调试 ssl

请参阅调试与 SSL 会话关联的配置或设置的以下命令。

debug *ssl* [*cipher* | *device*] [*1-255*]

Syntax Description

ssl	启用对 SSL 的调试。使用 ? 查看可用的子功能。
cipher	（可选）指定 SSL 密码调试级别。使用 ? 查看可用的级别。
device	（可选）指定 SSL 设备调试级别。使用 ? 查看可用的级别。
1-255	（可选）指定调试级别。

Command Default

默认调试级别为 1。

Related Commands

命令	说明
show debug ssl	显示 SSL 当前的活动调试设置。
undebug ssl	禁用对 SSL 的调试。此命令与 **no debug ssl** 的效果相同。

debug webvpn

请参阅以下调试与 WebVPN 关联的配置或设置的命令。

debug *webvpn* [*anyconnect* | *chunk* | *cifs* | *citrix* | *compression* | *condition* | *cstp-auth* | *customization* | *failover* | *html* | *javascript* | *kcd* | *listener* | *mus* | *nfs* | *request* | *response* | *saml* | *session* | *task* | *transformation* | *url* | *util* | *xml*]

Syntax Description

webvpn	启用 WebVPN 的调试。使用 ? 可查看可用的子功能。
anyconnect	（可选）指定 WebVPN AnyConnect 调试级别。使用 ? 可查看可用的级别。
chunk	（可选）指定 WebVPN 分块调试级别。使用 ? 可查看可用的级别。
cifs	（可选）指定 WebVPN CIFS 调试级别。使用 ? 可查看可用的级别。
citrix	（可选）指定 WebVPN Citrix 调试级别。使用 ? 可查看可用的级别。
compression	（可选）指定 WebVPN 压缩调试级别。使用 ? 可查看可用的级别。

condition	（可选）指定 WebVPN 过滤条件调试级别。使用 ? 可查看可用的级别。
cstp-auth	（可选）指定 WebVPN CSTP 身份验证调试级别。使用 ? 可查看可用的级别。
customization	（可选）指定 WebVPN 自定义调试级别。使用 ? 可查看可用的级别。
failover	（可选）指定 WebVPN 故障切换调试级别。使用 ? 可查看可用的级别。
html	（可选）指定 WebVPN HTML 调试级别。使用 ? 可查看可用的级别。
javascript	（可选）指定 WebVPN Javascript 调试级别。使用 ? 可查看可用的级别。
kcd	（可选）指定 WebVPN KCD 调试级别。使用 ? 可查看可用的级别。
listener	（可选）指定 WebVPN 侦听程序调试级别。使用 ? 可查看可用的级别。
mus	（可选）指定 WebVPN MUS 调试级别。使用 ? 可查看可用的级别。
nfs	（可选）指定 WebVPN NFS 调试级别。使用 ? 可查看可用的级别。
request	（可选）指定 WebVPN 请求调试级别。使用 ? 可查看可用的级别。
response	（可选）指定 WebVPN 响应调试级别。使用 ? 可查看可用的级别。
saml	（可选）指定 WebVPN SAML 调试级别。使用 ? 可查看可用的级别。
session	（可选）指定 WebVPN 会话调试级别。使用 ? 可查看可用的级别。
task	（可选）指定 WebVPN 任务调试级别。使用 ? 可查看可用的级别。
transformation	（可选）指定 WebVPN 转换调试级别。使用 ? 可查看可用的级别。
url	（可选）指定 WebVPN URL 调试级别。使用 ? 可查看可用的级别。
util	（可选）指定 WebVPN 实用程序调试级别。使用 ? 可查看可用的级别。
xml	（可选）指定 WebVPN XML 调试级别。使用 ? 可查看可用的级别。

Command Default

默认调试级别为 1。

Related Commands

命令	说明
show debug webvpn	显示 WebVPN 的当前活动调试设置。
undebug webvpn	禁用 WebVPN 的调试。此命令与 **no debug webvpn** 的效果相同。

第 XIII 部分

访问控制

第 49 章

访问控制概述

访问控制简介

访问控制是一项基于策略的分层功能，可用于指定、检查和记录（非快速路径）网络流量。

每个受管设备都可作为一个访问控制策略的目标。策略的目标设备收集有关网络流量的数据可用于根据以下内容过滤和控制该流量：

- 简单、易于确定的传输层和网络层特征：源和目标、端口和协议等
- 流量的最新的上下文信息，包括诸如信誉、风险、业务相关性、使用的应用或访问的URL等特征
- 领域、用户、用户组或 ISE 属性
- 自定义安全组标记 (SGT)
- 加密流量的特性；也可以解密此流量以进一步分析
- 未加密或已解密的流量包含禁止的文件、检测到的恶意软件还是入侵尝试
- 时间和日期（在受支持的设备上）

每种类型的流量检查和控制都以提供最大灵活性和性能的方式进行。例如，基于信誉的阻止名单使用简单的源和目标数据，因此，可以在过程的早期阻止禁止的流量。相反，检测和阻止入侵和漏洞则是最后一道防线。

规则简介

各种策略类型（访问控制、SSL、身份等）中的规则对网络流量实行精细控制。系统使用第一个匹配算法按您指定的顺序根据规则评估流量。

虽然这些规则可能包含在策略之间不一致的其他配置，但它们共享许多基本特征和配置机制，包括：

- 条件：规则条件指定每个规则处理的流量。您可以为每个规则配置多个条件。流量必须匹配所有条件才能与规则匹配。
- 操作：规则的操作确定系统如何处理匹配流量。请注意，即使规则没有可供选择的**操作 (Action)**列表，该规则仍然具有关联操作。例如，自定义网络分析规则使用网络分析策略作为其“操作”。 又例如，QoS 规则没有明确的操作，因为所有 QoS 规则都执行同一操作：速率限制流量。
- 位置：规则的位置确定其评估顺序。当使用策略评估流量时，系统按您指定的顺序将流量与规则匹配。通常，系统根据第一个规则（其中所有规则的条件都与流量匹配）处理流量。（用于跟踪和记录的监控规则除外。）适当的规则顺序可减少处理网络流量所需的资源，并防止规则抢占。
- 类别：要组织某些规则类型，您可以在每个父策略中创建自定义规则类别。
- 日志记录：对于许多规则，日志记录设置会监管系统是否以及如何记录规则处理的连接。某些规则（例如身份和网络分析规则）不包括日志记录设置，因为规则既不确定连接的最终处置情况，也不是专门设计为记录连接。 又例如，QoS 规则不包括日志记录设置；只是因为其速率受限，您便无法记录连接。
- 注释：对于某些规则类型，每次保存更改时，可以添加注释。例如，您可为其他用户汇总整体配置，或者当您变更规则和更改的原因时进行记录。

提示 许多策略编辑器中的右键点击菜单提供很多规则管理选项的快捷方式，包括编辑、删除、移动、启用和禁用。

有关详细信息，请参阅讨论您感兴趣的规则的章节（例如，访问控制规则）。

相关主题

配置应用条件和过滤器，第 1294 页
应用控制的最佳实践，第 1248 页

按设备过滤规则

有些策略编辑器允许您按受影响设备过滤您的规则视图。

系统使用规则的接口限制来确定该规则是否影响设备。如果您通过接口限制规则（安全区域或接口组条件），则该规则会影响接口所在的设备。无接口限制的规则会应用于任何接口，因此也会应用于每台设备。

QoS 规则始终受接口限制。

过程

步骤 1 在策略编辑器中，点击**规则 (Rules)**，然后点击**按设备过滤 (Filter by Device)**。
系统将会显示目标设备和设备组列表。

步骤 2 选中一个或多个复选框，以仅显示应用于这些设备或组的规则。或者，选中**全部 (All)** 复选框，以重置和显示所有的规则。

提示 将指针悬停在规则标准上方可查看其值。如果标准代表具有设备特定覆盖的对象，则系统会在您仅按该设备过滤规则列表时显示覆盖值。如果标准代表具有域特定覆盖的对象，则系统会在您按该域中的设备过滤规则列表时显示覆盖值。

步骤 3 点击**确定 (OK)**。

规则和其他策略警告

策略和规则编辑器使用图标来标记可能会对流量分析和流动有不利影响的配置。根据问题，系统可能会在您部署时向您发出警告或完全阻止您进行部署。

提示 将您的鼠标指针悬停在图标之上，即可读取警告、错误或信息文本。

表 *91:* 策略错误图标

图标	说明 (Description)	示例
错误（）	如果规则或配置具有错误，则更正错误之前无法部署，即使禁用任何受影响规则也如此。	在将没有URL过滤许可证的设备设为目标之前，执行基于类别和信誉的URL过滤的规则有效。此时，在规则旁边会显示错误图标，并且在编辑或删除规则、将策略重新设为目标或启用许可证之前，无法进行部署。
警告（  ）	可以部署显示规则或其他警告的策略。然而，标记有警告的不当配置将不起作用。 如果您禁用包含警告的规则，则警告图标将消失。如果在没有纠正潜在问题的情况下启用规则，警告图标将会再次显示。	已占用的规则或由于配置不当而无法与流量相匹配的规则不起作用。这包括使用空对象组的条件、与应用不匹配的应用过滤器、已排除的LDAP用户、无效端口等等。 但是，如果警告图标标记许可错误或型号不匹配，则在更正问题之前无法进行部署。

图标	说明 (Description)	示例
信息（ ）	信息图标传达有关可能影响流量流动的配置的有用信息。这些问题不会阻止您进行部署。	系统可能会跳过根据某些规则来匹配连接的前几个数据包，直至系统识别该连接中的应用或网络流量为止。这样，就可建立连接，以便识别应用和 HTTP 请求。

访问控制策略默认操作

新创建的访问控制策略指导其目标设备使用其默认操作处理所有流量。

在简单的访问控制策略中，默认操作指定目标设备如何处理所有流量。在更复杂的策略中，默认操作处理如下流量：

- 不受智能应用绕行信任
- 不在安全情报阻止列表中
- 未被 SSL 检查阻止（仅限加密流量）
- 与策略中的所有规则均不匹配（“监控”规则除外，这些规则会匹配和记录流量，但不处理或检查流量）。

访问控制策略默认操作可以阻止或信任流量，而不进行进一步检查，或者检查流量以获取入侵和发现数据。

注释 您**不能**对默认操作处理的流量执行文件或恶意软件检查。默认操作处理的连接的日志记录最初处于禁用状态，但是您可以启用该日志记录功能。

如果使用的是策略继承，则最低级别后代的默认操作会确定最终流量处理。尽管访问控制策略可从其基本策略继承其默认操作，但您无法强制执行这一继承。

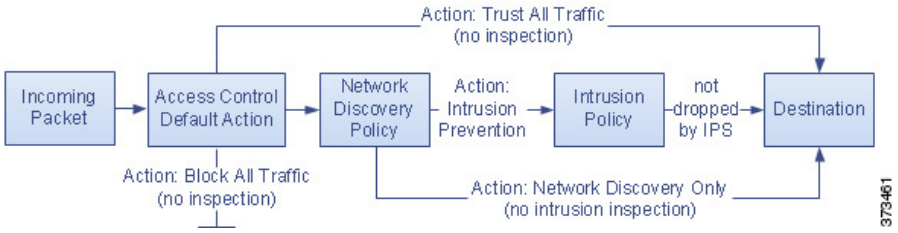
下表介绍了您可以对每个默认操作处理的流量执行的检查类型。

表 *92:* 访问控制策略默认操作

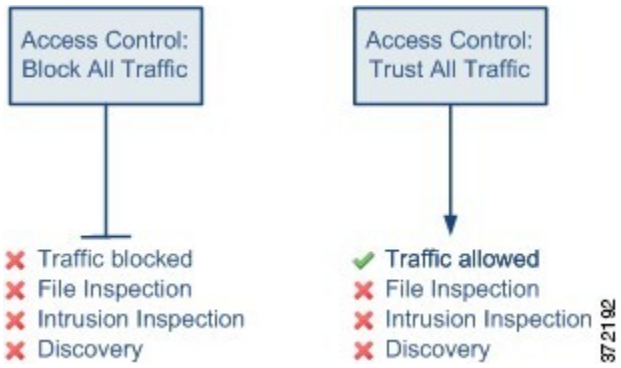
默认操作	对流量的影响	检查类型和策略
访问控制：阻止所有流量	不进一步检查直接阻止	none
访问控制：信任所有流量	信任（允许流向其最终目标，而无需进一步检查）	none
入侵防御	允许，前提是其通过指定的入侵策略	入侵，使用指定的入侵策略和关联变量集，以及 发现，使用网络发现策略

默认操作	对流量的影响	检查类型和策略
仅网络发现	allow	仅发现，使用网络发现策略
继承自基本策略	在基本策略中定义	在基本策略中定义

下图对该表进行了展示。



下图展示了**阻止所有流量 (Block All Traffic)** 和**信任所有流量 (Trust All Traffic)** 默认操作。



下图展示了**入侵防御 (Intrusion Prevention)** 和**仅网络发现 (Network Discovery Only)** 默认操作。

提示 **Network Discovery Only** 的目的是在仅发现部署中提高性能。如果您仅对入侵检测和防御感兴趣，则不同的配置可以禁用发现。

使用文件和入侵策略的深度检测

深度检测会将入侵策略和文件策略用作为允许流量到达其目标之前的最后一道防线。

- 入侵策略监管系统的入侵防御功能。

  有关完整信息，请参阅入侵检测和防御，第 1445 页。

- 文件策略监管系统的文件控制和恶意软件防护 功能。

  有关完整信息，请参阅网络恶意软件防护和文件策略，第 1661 页。

访问控制发生在深度检查之前；访问控制规则和访问控制默认操作确定哪些流量由入侵和文件策略检测。

通过将入侵策略或文件策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要使用入侵策略和/或文件策略检测流量。

在访问控制策略中，您可以将一个入侵策略与每条“允许”(Allow) 和“交互式阻止”(Interactive Block) 规则以及默认操作相关联。每个唯一的入侵策略和变量集**对均**视为一个策略。

要将入侵策略和文件策略与访问控制规则相关联，请参阅：

- 用于执行入侵防御的访问控制规则配置，第 1468 页
- 配置访问控制规则以执行恶意软件保护，第 1669 页

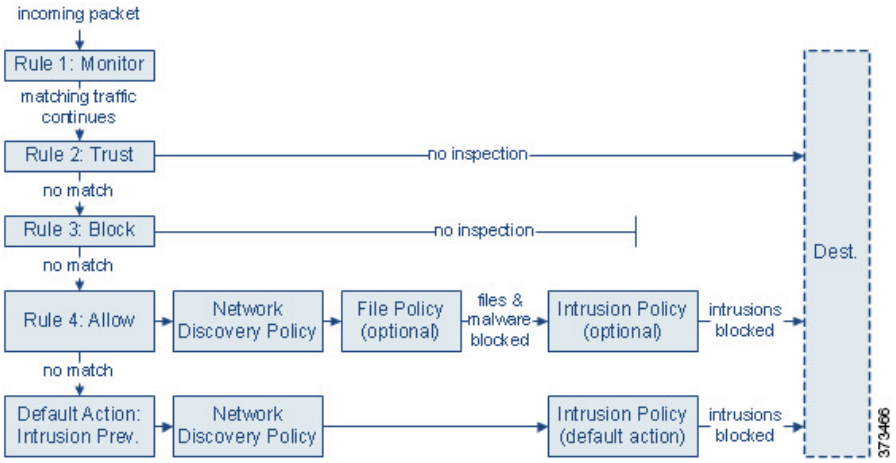
注释 默认情况下，系统禁用对已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。

相关主题

策略如何检查流量是否存在入侵，第 1448 页
文件策略，第 1662 页

使用入侵和文件策略的访问控制流量处理

下图显示一个内联入侵防御和恶意软件防护 部署中的流量，它受包含四种不同类型访问控制规则和默认操作的访问控制策略监管。



在上面的情景中，策略中的前三条访问控制规则 — Monitor、Trust 和 Block — 无法检查匹配的流量。Monitor 规则跟踪和记录但不检查网络流量，因此，系统继续将流量与其他规则进行匹配以确定是允许还是拒绝该流量。（但是，请参阅访问控制规则监控操作，第 1284 页中的重要例外情况和警告。）Trust 和 Block 规则处理匹配流量，无需任何何类型的进一步检查，不匹配的流量继续进入下一条访问控制规则。

策略中的第四个也是最后一条规则（Allow 规则）按照以下顺序调用各种其他策略以检查和处理匹配的流量：

- **发现：网络发现策略** - 首先，网络发现策略检查流量是否存在发现数据。发现是被动分析，并不影响流量的流动。尽管不显式启用发现，但您可以增强或禁用它。但是，允许流量不会自动确保收集发现数据。系统仅对涉及网络发现策略显式监控的 IP 地址的连接进行发现。
- **恶意软件防护 和文件控制：文件策略** - 通过发现功能检查流量后，系统可以检查其是否包含禁止文件和恶意软件。恶意软件防护 将检测并选择性地阻止多种文件中的恶意软件，包括 PDF、Microsoft Office 文档等。如果贵组织不仅要阻止传输恶意软件文件，还要阻止特定类型的所有文件（无论文件是否包含恶意软件），则 *file control* 可供您监控网络流量中特定文件类型的传输，然后阻止或允许文件。
- **入侵防御：入侵策略** - 在文件检查之后，系统可以检查流量中是否存在入侵和漏洞。入侵策略根据模式检查已解码数据包中是否存在攻击，并且可以阻止或修改恶意流量。入侵策略与变量集配对，这使您能够使用指定值准确反映网络环境。
- **目标** - 通过上述所有检查的流量将传递到其目标。

“交互式阻止”(Interactive Block) 规则（未显示在图中）具有与“允许”(Allow) 规则相同的检查选项。因此，您可以在用户通过点击警告页面绕过已阻止网页时检测流量是否存在恶意内容。

在策略中不符合任何访问控制规则的流量，如果有监控以外的操作，则由默认操作来处理。在这种情况下，默认操作是入侵防御操作，只要流量由您指定的入侵策略进行传递，它就允许流量到达其最终目的地。在不同的部署中，您可能有默认操作可以信任或阻止所有流量，而无需进一步检测。请注意，系统可能检测默认操作允许的流量是否存在发现数据和入侵，而不是检测其是否存在受禁文件或恶意软件。您**无法**将文件策略与访问控制默认操作相关联。

注释 有时，当访问控制策略分析某条连接时，系统必须处理该连接中的头几个数据包，**从而让其通过**，然后才能确定哪个访问控制规则（如有）将处理流量。然而，为了让这些数据包不会未经检查就到达目的地，您可以在访问控制策略的高级设置中指定一个入侵策略，以便检查这些数据包并生成入侵事件。

文件和入侵检查顺序

在您的访问控制策略中，您可以将多个 Allow 和 Interactive Block 规则与不同的入侵和文件策略相关联，以使检查配置文件匹配各种流量类型。

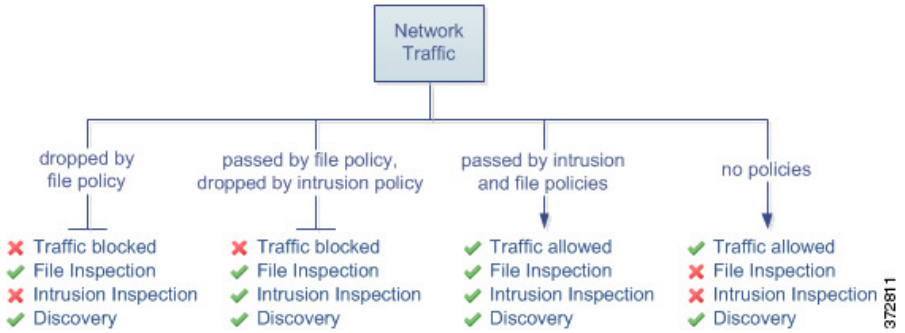
注释 可检测“入侵防御”(Intrusion Prevention) 或“仅网络发现”(Network Discovery Only) 默认操作允许的流量是否存在发现数据和入侵，但不能检测其是否存在受禁文件或恶意软件。您**无法**将文件策略与访问控制默认操作相关联。

您不必在同一规则中同时执行文件和入侵检测。对于符合“允许”(Allow)或“交互式阻止”(Interactive Block) 规则的连接：

- 没有文件策略，数据流取决于入侵策略
- 没有入侵策略，数据流取决于文件策略
- 若以上两者都没有，仅由网络发现检查允许的流量

提示 系统不会对受信任的流量执行任何种类的检测。虽然没有使用入侵或文件策略配置“允许”(Allow) 规则可以放行流量，就像“信任”(Trust) 规则那样，但“允许”(Allow) 规则让您可以对匹配的流量执行发现。

下图说明对符合“允许”(Allow) 或用户绕过的“交互式阻止”(Interactive Block) 访问控制规则的条件的流量执行的检查类型。为简单起见，该图显示入侵策略和/或文件策略与单个访问控制规则关联的情况的流量。



对由访问控制规则处理的任何单个连接，文件检测均发生在入侵检测之前。也就是说，系统不检测文件策略所阻止的文件是否存在入侵。在文件检测中，基于类型的简单阻止优先于恶意软件检测和阻止。

例如，请考虑按照访问控制规则中所定义通常要允许特定网络流量的情况。但是，作为预防措施，您希望阻止下载可执行文件，检测恶意软件的已下载的 PDF 并阻止找到的所有实例，然后对流量执行入侵检测。

您可以使用与自己想要暂时允许通过的流量的特征相匹配的规则创建访问控制策略，然后将其与入侵策略和文件策略相关联。文件策略阻止所有可执行文件的下载，也可检测和阻止包含恶意软件的 PDF：

- 首先，系统根据文件策略中指定的简单类型匹配阻止所有可执行文件的下载。由于会立即遭到阻止，因此这些文件既无法执行恶意软件检查也无法执行入侵检查。
- 接着，系统对下载到网络主机的 PDF 执行恶意软件云查找。具有恶意软件处置情况的任何 PDF 均被阻止，且不接受入侵检查。
- 最后，系统使用与访问控制规则关联的入侵策略检测任何剩余流量，包括文件策略未阻止的文件。

注释 文件在会话中得以检测和阻止之前，来自该会话的数据包均可能接受入侵检测。

访问控制策略继承

此功能在多域部署中尤其有用，您可以嵌套访问控制策略。在这种情况下，每个策略都会继承祖先（或基本）策略的规则和设置。您可以执行此继承，或允许较低级别的策略覆盖其祖先。

访问控制使用基于分层策略的实施。正如创建域层次结构一样，您也可以创建访问控制策略的相应层次结构。后代或子访问控制策略继承其直接父策略或基本策略的规则和设置。该基础策略可能有其子级的父级策略，它从父级策略沿用规则和设置等。

访问控制策略的规则嵌套在其父策略的“强制性”(Mandatory) 规则部分与“默认”(Default) 规则部分之间。这种实施执行来自祖先策略的强制规则，但也允许当前策略写入规则以抢先于来自祖先策略的默认规则。

您可以锁定以下设置，以便在所有后代策略中执行它们。后代策略可以覆盖未锁定的设置。

- 安全情报 - 根据 IP 地址、URL 和域名的最新信誉情报而被允许或阻止的连接。
- HTTP 响应页面 - 在阻止用户的网站请求时显示自定义或系统提供的响应页面。
- 高级设置 - 指定关联的子策略、网络分析设置、性能设置和其他常规选项。

如果使用的是策略继承，则最低级别后代的默认操作会确定最终流量处理。尽管访问控制策略可从祖先策略继承其默认操作，但您无法强制执行这一继承。

策略继承和多租户

访问控制的基于分层策略的实施完善了多租户策略。

在典型的多域部署中，访问控制策略的层次结构与域结构相对应，您将最低级别的访问控制策略应用于受管设备。这种实施支持在较高的域级别选择性地执行访问控制，而低层域管理员可以定制特定部署的具体设置。（要限制后代域中的管理员，您必须使用角色而不能只靠策略继承和实施。）

例如，作为组织的全局域管理员，您可以在全局级别创建访问控制策略。然后，您可以要求所有设备（按功能分为子域）使用该全局级策略作为基本策略。

当子域管理员登录 Cisco Secure Firewall Management Center配置访问控制时，他们可以按原样部署此全局级策略。或者，他们也可以在该全局级策略的界限之内创建和部署后代访问控制策略。

注释 虽然这种最有用的访问控制继承和执行的实施方法可以完善多租户策略，但您也可以在单个域中创建访问控制策略的层次结构。您还可以在任意级别分配和部署访问控制策略。

相关主题

安全情报，第 1359 页
HTTP 响应页面和交互式阻止
访问控制策略的日志记录设置，第 1270 页
访问控制策略高级设置，第 1271 页
管理访问控制策略继承，第 1266 页
选择基本访问控制策略，第 1267 页
继承基本策略的访问控制策略设置，第 1268 页
锁定后代访问控制策略中的设置，第 1268 页
在域中需要访问控制策略，第 1269 页

应用控制的最佳实践

以下主题讨论我们推荐的使用访问控制规则控制应用的最佳实践。

应用控制的建议

请牢记以下应用控制的准则与限制：

确保启用自适应分析

如果未启用（默认状态）自适应分析，访问控制规则将无法执行应用控制。

自动启用应用检测器

如果没有为要检测的应用启用检测器，则系统会为该应用自动启用所有系统提供的检测器。如果不存在检测器，则系统会为该应用启用最新修改的用户定义检测器。

配置策略以检查在识别应用之前必须通过的数据包

在发生以下两种情况之前，系统无法执行应用控制，包括智能应用绕行 (IAB) 和速率限制：

- 客户端与服务器之间建立受监控连接
- 系统识别会话中的应用

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

重要提示！要确保您的系统检查这些初始数据包，请参阅指定策略以处理在流量识别之前通过的数据包，第 2042 页。

如果早期流量与所有其他条件匹配，但应用识别未完成，系统会允许传递数据包，并允许建立连接（或允许 SSL 握手完成）。在系统完成其识别后，系统会将相应的操作应用于剩余会话流量。

注释 服务器必须遵守应用的协议要求，这样系统才能识别该应用。例如，如果您有一台服务器在预期 ACK 时发送保持连接数据包而不是 ACK，则可能无法识别该应用，并且连接将不会匹配基于应用的规则。相反，它将由另一个匹配的规则或默认操作进行处理。这可能意味着您想要允许的连接会被拒绝。如果遇到此问题，并且无法修复服务器以遵循协议标准，则需要编写基于非应用的规则来覆盖该服务器的流量，例如，匹配 IP 地址和端口号。

为 URL 和应用过滤创建单独的规则

尽可能为 URL 和应用过滤创建单独的规则，因为组合应用和 URL 标准可能会导致非预期的结果，特别是对于加密的流量。

包括应用和 URL 标准的规则应位于仅应用或仅 URL 规则前，除非应用+URL 规则作为更一般仅应用或仅 URL 规则的例外。

在应用和其他规则之前应用 URL 规则

为了实现最有效的 URL 匹配，请将包括 URL 条件的规则放在其他规则前面，如果 URL 规则是组织规则，并且其他规则同时满足以下两个条件，则尤其应该如此：

- 它们包括应用条件。
- 将对要检查的流量进行加密。

加密和解密流量的应用控制

系统可识别和过滤已加密和解密的流量：

- 加密流量 - 系统可以检测使用 StartTLS（包括 SMTP、PoP、FTP、Telnet 和 IMAP）加密的应用流量。此外，系统还可以根据 TLS ClientHello 消息中的服务器名称指示或服务器证书中的使用者专有名称值来识别某些加密应用。这些应用附以 `SSL Protocol` 标记；在 SSL 规则中，可以仅选择这些应用。只有在未加密或已解密的流量中才能检测到没有此标记的应用。

- 解密流量 - 系统还会将 `decrypted traffic` 标记分配给系统只能在解密流量中检测到（在加密或未加密流量中无法检测到）的应用。

TLS 服务器身份发现和应用控制

RFC 8446定义的最新版本的传输层安全（TLS）协议 1.3 是许多 Web 服务器提供安全通信的首选协议。由于 TLS 1.3 协议会加密服务器的证书以提高安全性，并且需要使用证书来匹配访问控制规则中的应用和 URL 过滤条件，因此 Firepower 系统提供了一种提取服务器证书而 不 解密整个数据包的方法。

我们强烈建议您为要根据应用或URL 条件匹配的任何流量启用此功能，尤其是在您想要对该流量执行深度检查时。SSL 策略 不需要 SSL 策略，因为在提取服务器证书的过程中不会解密流量。

有关详细信息，请参阅访问控制策略高级设置，第 1271 页。

将应用免于进行主动授权

在身份策略中，可以将某些应用免于主动授权，允许流量继续进行访问控制。这些应用附以 `User-Agent Exclusion` 标记。在身份规则中，仅可以选择这些应用。

处理无负载的应用流量数据包

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

处理推荐应用流量

要处理由 Web 服务器所推荐的流量（如广告流量），请匹配被推荐应用（而非推荐应用）。

控制使用多个协议的应用流量（Skype、Zoho）

某些应用使用多个协议。要控制其流量，请确保访问控制策略能够涵盖所有相关选项。例如：

- Skype - 要控制 Skype 流量，请从**应用过滤器**列表中选择 **Skype** 标记（而不是选择个别应用）。这确保系统可以相同方式检测和控制所有 Skype 流量。
- Zoho - 要控制 Zoho 邮箱，请从“可用应用”列表中同时选择 **Zoho** 和 **Zoho 邮箱**。

内容限制功能支持的搜索引擎

系统仅支持特定搜索引擎的安全搜索过滤。系统将 `safesearch supported` 标记从这些搜索引擎分配给应用流量。

控制规避应用流量

请参阅特定于应用的说明和限制，第 1252 页。

配置应用控制的最佳实践

我们建议如下控制应用对网络的访问：

- 要允许或阻止从安全性较低的网络到安全性较高的网络的应用访问，请执行以下操作：在访问控制规则中使用 **端口** （所选目标端口）条件

  例如，允许从互联网（不太安全）到内部网络（更安全）的 ICMP 流量。

- 要允许或阻止用户组访问应用，请执行以下操作：在访问控制规则上使用 **应用** 条件

  例如，阻止承包商组成员访问 Facebook

注意 未能正确设置访问控制规则可能会导致意外结果，包括允许应阻止的流量。通常，应用控制规则应在访问控制列表中较低，因为与基于 IP 地址的规则相比，匹配这些规则所需的时间更长。

使用 特定 条件（例如网络和 IP 地址）的访问控制规则应在使用一般条件（例如应用）的规则 之前排序。如果您熟悉开放系统互联（OSI）模型，请在概念上使用类似的编号。包含第 1 层、第 2 层和第 3 层（物理、数据链路和网络）条件的规则应首先在访问控制规则中排序。稍后应在访问控制规则中对第 5 层、第 6 层和第 7 层的条件（会话，表示和应用）进行排序。有关 OSI 模型的详细信息，请参阅此 维基百科文章。

下表提供了如何设置访问控制规则的示例：

控制类型	操作 (Action)	区域、网络、VLAN 标记	用户	应用	端口	URL	SGT/ISE 属性	检测、日志记录、注释
当应用使用端口（例如 SSH）时，应用从更安全到不太安全的网络	您的选择（在本例中为 **允许** ）	使用外部接口的目标区域或网络	任意	不设置	可用的端口： **SSH** 添加至 **选定的目标端口**	任意	仅用于 ISE/ISE-PIC。	任意
当应用不使用端口（例如，ICMP）时，应用从更安全到不安全的网络	您的选择（在本例中为 **允许** ）	使用外部接口的目标区域或网络	任意	不设置	选定的目标端口 **协议：ICMP** **类型： 任何**	不设置	仅用于 ISE/ISE-PIC。	任意
用户组的应用访问	您的选择（在本例中为 **Block** ）	您的选择	选择用户组（本例中为承包商组）	选择应用的名称（本例中为 **Facebook** ）	不设置	不设置	仅用于 ISE/ISE-PIC。	您的选择

应用特征

系统使用下表中所述的条件来展示其检测到的每个应用的特征。这些特征用作应用过滤器。

表 *93:* 应用特征

特征	说明 (Description)	示例
类型	应用协议代表主机之间的通信。 客户端代表在主机上运行的软件。 Web 应用代表 HTTP 流量的内容或所请求的 URL。	HTTP 和 SSH 是应用协议。 网络浏览器和邮件客户端是客户端。 MPEG 视频和 Facebook 是网络应用。
风险	应用用于可能违反您的组织安全策略的用途的可能性。	点对点应用的风险通常很高。
业务相关性	应用用于您的组织的业务运营（相对于娱乐目的）的情景中的可能性。	游戏应用的业务相关性通常很低。
类别	说明应用的最基本功能的应用通用分类。每个应用至少属于一个类别。	Facebook 属于社交网络类别。
标签	有关应用的附加信息。应用可以包括任何数量的标记，也可以没有标记。	视频流网络应用通常标记为 `high bandwidth` 和 `displays ads`。

特定于应用的说明和限制

- Office 365 管理员门户：

  限制：如果访问策略在开始和结束时启用了日志记录，第一个数据包将被检测为 Office 365，而连接结束则会被检测为 Office 365 门户管理员用户。这应当不会影响拦截。

- Skype：

  请参阅 应用控制的建议 ， 第 1248 页

- GoToMeeting

  为了完全检测 GoToMeeting，您的规则必须包含以下所有应用：

  - GoToMeeting
  - Citrix Online
  - Citrix GoToMeeting 平台
  - LogMeIn

- STUN

- Zoho：

  请参阅 应用控制的建议，第 1248 页

- 诸如 Bittorrent、Tor、Psiphon 和 Ultrasurf 的规避应用：

  对于规避应用，默认仅检测置信度最高的场景。如果需要对此流量（例如阻止或实施 QoS）采取措施，则可能需要配置效率更高、更为积极的检测。若要如此，请联系 TAC 审查您的配置，因为这些更改可能会导致误报。

- 微信：

  如果您允许微信，则无法选择性地阻止微信媒体。

- RDP（远程桌面协议）：

  如果允许 RDP 应用不允许进行文件传输，请确保 RDP 规则同时包含 TCP 和 UDP 端口 3389。RDP 文件传输会使用 UDP。

访问控制规则的最佳实践

对规则正确进行配置和排序对于构建有效的部署至关重要。以下主题概述了规则性能准则。

注释 当部署配置更改时，系统会将所有规则共同进行评估，并创建目标设备用于评估网络流量的扩展标准集。如果这些标准超过目标设备的资源（物理内存、处理器等），则您无法部署到该设备。

访问控制的一般最佳实践

查看以下要求和一般最佳实践：

- 虽然无需为部署提供许可也可配置系统，但许多功能要求您在部署之前，先启用适当的许可证。
- 在部署访问控制策略时，其规则不会应用于现有连接。现有连接上的流量不受部署的新策略的限制。此外，仅对匹配策略的连接的第一个数据包增加策略命中计数。因此，从命中计数中忽略了可能与策略匹配的现有连接上的流量。要有效应用策略规则，请清除现有连接会话，然后部署策略。
- 为让系统影响流量，必须使用路由接口、交换接口或透明接口或者内联接口对向受管设备部署相关配置。

  有时，系统会阻止您将内联配置部署到被动部署的设备，包括分流模式下的内联设备。

  在其他情况下，策略可成功部署，但尝试使用被动部署的设备阻止或修改流量可能会出现意外结果。例如，由于受阻连接在被动部署中未被阻止，因此系统可为每个受阻连接报告多个连接开始事件。

- 某些功能（包括URL过滤、应用检测、速率限制和智能应用旁路）必须允许某些数据包通过，以便系统识别流量。

  要防止这些数据包未经检查即到达目的地，请参阅 处理在流量识别之前通过的数据包的最佳实践，第 2042 页 和 指定策略以处理在流量识别之前通过的数据包，第 2042 页。

- 您不能对访问控制策略的默认操作处理的流量执行文件或恶意软件检查。
- 某些功能仅在特定设备型号上可用。警告图标和确认对话框会指出不支持的功能。
- 如果您要使用 syslog 或在外部存储事件，请避免在对象名称（例如策略和规则名称）中使用特殊字符。对象名称不应包含特殊字符（例如逗号），接收名称的应用可能将其用作分隔符。
- 默认操作处理的连接的日志记录最初处于禁用状态，但是您可以启用该日志记录功能。
- 访问控制规则的最佳实践，第 1253 页和子主题中详细介绍了创建、排序和实施访问控制规则的最佳实践。

订购规则的最佳实践

一般准则：

- 一般，将必须应用于所有流量的最优先规则靠近策略的顶部放置。
- 特定规则应在一般规则之前，特别当特定规则是一般规则的例外时。

  否则，流量将首先匹配一般规则，而不会命中适用的特定规则。

- 仅基于第 3/4 层标准丢弃流量的规则（如 IP 地址、安全区和端口号）应尽早出现。基于这些条件的规则不需要通过检测来识别匹配的连接。
- 尽可能将特定丢弃规则置于策略顶部附近。这确保了对非预期流量尽可能做出最早的决定。
- URL 过滤、基于应用和基于地理位置的规则以及其他需要检查的规则应位于仅根据第 3/4 层标准（例如 IP 地址、安全区域和端口号）丢弃流量的规则之后，但在规则之前指定文件和入侵策略。
- 将 URL 过滤规则置于应用规则之上，并在应用规则之后加上微应用规则和通用工业协议 (CIP) 子分类应用过滤规则。
- 指定文件策略和入侵策略的规则应位于规则顺序的底部。这些规则需要资源密集型深度检查，并且出于性能原因，您应首先使用强度较低的方法消除尽可能多的威胁，以便最大限度地减少需要深度检查的潜在威胁的数量。
- 始终应根据您的组织的需求对规则进行排序。

以下各节说明了上述准则的例外情况和补充内容。

规则抢占

当一条规则由于评估中排序靠前的规则首先匹配流量而永远无法匹配流量时，会出现规则抢占问题。规则的条件控制其是否会抢占其他规则。在以下示例中，第二条规则无法阻止管理员流量，因为第一条规则会允许该流量：

访问控制规则 1：允许管理员用户
访问控制规则 2：阻止管理员用户

任何类型的规则条件均可以取代后续规则。第一条 SSL 规则中的 VLAN 范围包含第二条规则中的 VLAN，因此第一条规则将抢占第二条规则：

规则 1：不解密 VLAN 22-33
SSL 规则 2：阻止 VLAN 27

在以下示例中，规则 1 匹配所有 VLAN，因为没有配置 VLAN，因此规则 1 会取代尝试匹配 VLAN 2 的规则 2：

访问控制规则 1：允许源网络 10.4.0.0/16
访问控制规则 2：允许源网络 10.4.0.0/16，VLAN 2

规则还会抢占所有已配置条件均相同的相同后续规则：

QoS 规则1：速率限制 VLAN 1 URL www.netflix.com
QoS 规则2：速率限制 VLAN 1 URL www.netflix.com

如有任何条件不同，则后续规则不会被抢占：

QoS 规则1：速率限制 VLAN 1 URL www.netflix.com
QoS 规则2：速率限制 VLAN 2 URL www.netflix.com

示例：对 SSL 规则进行排序以避免抢占

请考虑以下场景，其中受信任CA（好CA）错误地将CA证书颁发给恶意实体（坏CA），但是尚未撤销该证书。您希望使用 SSL 策略来阻止使用由不受信任 CA 颁发的证书加密的流量，但是以其他方式允许受信任 CA 的信任链中的流量。在上传 CA 证书和所有中间 CA 证书后，请配置包含如下排序规则的 SSL 策略：

SSL 规则 1：阻止颁发者 CN=www.badca.com
SSL 规则 2：不解密颁发者 CN=www.goodca.com

如果恢复规则，会首先与受良好CA信任的所有流量相匹配，包括受不良CA信任的流量。由于流量不曾与后续不良 CA 规则相匹配，因此可能会允许而非阻止恶意流量。

规则操作和规则顺序

规则操作确定系统如何处理匹配的流量。通过将不执行也不确保进一步流量处理的规则置于会执行并确保进一步流量处理的资源密集型规则之前来提高性能。然后，系统可以转移可能已另外检查的流量。

以下示例显示在规则集中无任何规则更重要且抢占不是问题的情况下，可能如何在各种策略中对规则进行排序。

如果您的规则包括应用条件，另请参阅配置应用控制的最佳实践，第 1250 页。

最佳顺序：SSL 规则

不仅解密需要资源，进一步分析已解密的流量也同样需要资源。请将用于解密流量的规则放在最后。

注释 某些托管的设备支持对硬件中的 TLS/SSL 流量进行加密和解密，这大大提高了性能。有关详细信息，请参阅TLS 加密加速，第 1717 页。

1. 监控 - 记录匹配连接但不对流量采取任何其他操作的规则。
2. 阻止、阻止并重置 - 阻止流量而不进一步检测的规则
3. 不解密 - 不解密加密流量，从而将加密会话传递到访问控制规则的规则。这些会话的负载不执行深度检查。
4. 解密 - 已知密钥 - 使用已知私钥解密传入流量的规则。
5. 解密 - 重新签名 - 通过对服务器证书重新签名来解密传出流量的规则。

最佳顺序：访问控制规则

入侵、文件和恶意软件检测需要资源，尤其是您使用多个自定义入侵策略和变量集时情况更加如此。请将调用深度检查的访问控制规则放在最后。

1. 监控 - 记录匹配连接但不对流量采取任何其他操作的规则。（但是，请参阅访问控制规则监控操作，第 1284 页中的重要例外情况和警告。）
2. 信任、阻止、阻止并重置 - 处理流量而不进一步检测的规则。请注意，受信任的流量会受到身份策略实施的身份验证要求和速率限制的制约。
3. 允许，交互式阻止（无深度检查）- 不进一步检测流量，但是允许发现的规则。请注意，允许的流量会受到身份策略实施的身份验证要求和速率限制的制约。
4. 允许，交互式阻止（深度检查）- 与对禁止的文件、恶意软件和漏洞执行深度检查的文件或入侵策略关联的规则。

应用规则顺序

如果将包含应用条件的规则移至规则列表中较低的顺序，则更有可能与流量匹配。

使用 特定 条件（例如网络和 IP 地址）的访问控制规则应在使用一般条件（例如应用）的规则 之前排序。如果您熟悉开放系统互联（OSI）模型，请在概念上使用类似的编号。包含第 1 层、第 2 层和第 3 层（物理、数据链路和网络）条件的规则应首先在访问控制规则中排序。稍后应在访问控制规则中对第 5 层、第 6 层和第 7 层的条件（会话，表示和应用）进行排序。有关 OSI 模型的详细信息，请参阅此 维基百科文章。

有关详细信息和示例，请参阅配置应用控制的最佳实践，第 1250 页和应用控制的建议，第 1248 页。

URL 规则顺序

为了实现最有效的 URL 匹配，请将包括 URL 条件的规则放在其他规则前面，如果 URL 规则是组织规则，并且其他规则同时满足以下两个条件，则尤其应该如此：

- 它们包括应用条件。
- 将对要检查的流量进行加密。

如果为规则配置例外，请将例外置于另一条规则之上。

简化和集中规则的最佳实践

简化：不过度配置

最小化单个规则条件。在规则条件中使用尽可能少的单独元素。例如，在网络条件中，使用 IP 地址块，而不是单独的 IP 地址。

如果一个条件足以匹配您想要处理的流量，请不要使用两个条件。使用冗余条件可能会大大扩展已部署的配置，这可能会导致设备性能问题以及集群和高可用性设备重新加入中的意外设备行为。例如：

- 请谨慎使用代表多个接口的安全区域。如果指定源和目标网络作为条件，并且这些条件足以匹配您的目标流量，则无需指定安全区域。
- 例如，如果要将一组内部接口与互联网上的任何目的地进行匹配，则只需使用包含内部接口的源安全区域。不需要网络或目标接口标准。

将元素组合到对象中**不**会提高性能。例如，使用包含 50 个 IP 地址的网络对象，与逐一将这些 IP 地址纳入条件中相比，只能给您带来组织优势，而不是性能优势。

有关应用检测的建议，请参阅配置应用控制的最佳实践，第 1250 页。

集中：更严格地限制资源密集型规则，尤其是按接口限制

尽可能使用规则条件以更严格定义资源密集型规则处理的流量。集中规则很重要的另一原因是，有着广泛条件的规则可能与许多不同类型的流量相匹配，并且可以抢占较为靠后、更为具体的规则。资源密集型规则的示例包括：

- 解密流量的SSL规则-不仅解密，而且进一步分析已解密流量，也都需要资源。缩小集中范围，并尽可能阻止或选择不解密加密流量。

  某些 管理中心 模型在硬件中执行 SSL 加密和解密，这大大提高了性能。有关详细信息，请参阅TLS 加密加速，第 1717 页。

- 调用深度检查的访问控制规则 - 入侵、文件和恶意软件检查需要资源，尤其是您使用多个自定义入侵策略和变量集时情况更是如此。确保只在必要时调用深度检查。

为获得最大性能优势，请按接口限制规则。如果规则排除了某个设备的所有接口，则该规则不影响该设备的性能。

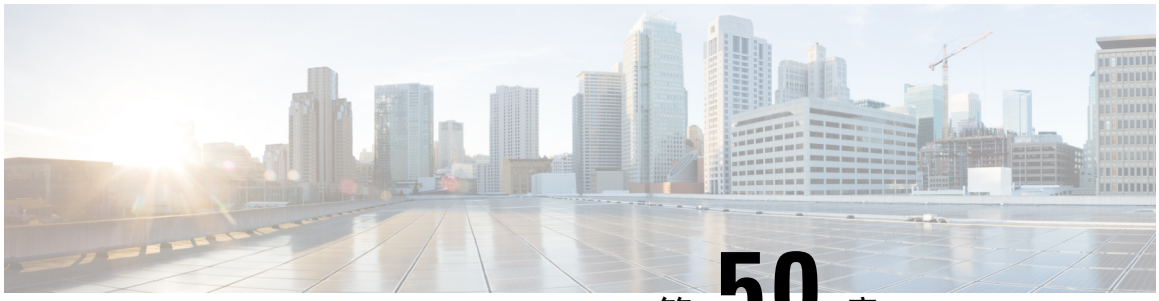
访问控制规则和入侵策略的最大数量

目标设备支持的访问控制规则或入侵策略的最大数量取决于许多因素，包括设备上的策略复杂度、物理内存以及处理器数量。

如果超过了设备支持的最大数量，则您无法部署访问控制策略，且必须重新评估。

入侵策略的准则：

- 在访问控制策略中，您可以将一个入侵策略与每条“允许”(Allow)和“交互式阻止”(Interactive Block)规则以及默认操作相关联。每个唯一的入侵策略和变量集**对均**视为一个策略。
- 您可能希望整合入侵策略或变量集，从而能够将单个入侵策略/变量集对与多个访问控制规则相关联。在某些设备上，您可能会发现只能对所有入侵策略使用单个变量集，甚至对整个设备采用单个入侵策略-变量集对。



第 50 章

访问控制策略

以下主题介绍如何使用访问控制策略：

访问控制策略组件

以下是访问控制策略的主要元素。

名称和描述

每个访问控制策略必须拥有唯一的名称。说明是可选的。

沿用设置

通过策略继承，您可以创建访问控制策略的层次结构。父（或基本）策略定义和执行其后代的默认设置，这对于多域部署尤为有用。

策略的继承设置允许您选择其基本策略。您还可以锁定当前策略中的设置以强制所有后代继承这些设置。后代策略可以覆盖未锁定的设置。

策略分配

每个访问控制策略可识别使用策略的设备。每台设备只能作为一个访问控制策略的目标。在多域部署中，可能需要一个域中的所有设备使用同一基本策略。

规则

访问控制规则提供了一种精细的网络流量处理方法。访问控制策略中的规则从1开始进行编号，包括从祖先策略继承的规则。系统会用升序的规则号码以从上到下的顺序将流量匹配到访问控制规则中。

通常，系统根据第一个访问控制规则（其中所有规则的条件都与流量匹配）处理网络流量。条件可以简单也可以复杂，条件的使用通常取决于某些许可证。

默认操作

默认操作确定系统如何处理和记录不是由任何其他访问控制配置处理的流量。默认操作可以阻止或信任所有流量，而不进行进一步检查，或者检查流量以获取入侵和发现数据。

尽管访问控制策略可从祖先策略继承其默认操作，但您无法强制执行这一继承。

安全情报

安全情报是抵御恶意互联网内容的第一道防线。此功能允许您根据最新的IP地址、URL和域名信誉情报将阻止连接。要确保对重要资源的持续访问，您可以使用自定义不阻止列表条目来覆盖阻止列表条目。

HTTP 响应

在系统阻止用户的网站请求时，您可以显示系统提供的通用响应页面或自定义页面。也可以显示一个警告用户，同时允许他们继续访问初始请求站点的页面。

日志记录

通过访问控制策略日志记录的设置，您可以为当前的访问控制策略配置默认系统日志目标。除非使用所包含规则和策略中的自定义设置显式覆盖系统日志目标设置，否则这些设置适用于访问控制策略以及所有包含在内的 SSL、预过滤器和入侵策略。

高级访问控制选项

高级访问控制策略设置通常只需要进行很小的修改或不需要修改。通常，默认设置就非常适合。可修改的高级设置包括流预处理、SSL 检查、身份和各种性能选项。

系统创建的访问控制策略

根据设备的初始配置，系统提供的策略可以包括：

- “默认访问控制”(Default Access Control) - 阻止所有流量，而不进行进一步检查。
- “默认入侵防御”(Default Intrusion Prevention) - 允许所有流量，但是还会使用“平衡安全性和连接”(Balanced Security and Connectivity) 入侵策略和默认入侵变量集进行检查。
- “默认网络发现”(Default Network Discovery) - 检查时允许发现数据的所有流量，但不允许入侵或漏洞的流量。

访问控制策略的要求和必备条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

管理访问控制策略

您可以编辑系统提供的访问控制策略，并创建自定义访问控制策略。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略** > **访问控制**。

步骤 2 管理访问控制策略：

- 复制 - 点击 **复制**（）。
- 创建 - 点击**新建策略 (New Policy)**；请参阅创建基本访问控制策略，第 1261 页。
- 删除 - 点击 **删除**（）。
- 编辑 - 点击 **编辑**（）；请参阅编辑访问控制策略，第 1262 页
- 锁定或解锁策略 - 请参阅锁定访问控制策略，第 1265 页。
- 继承 - 点击具有后代的策略旁边的**加号**，展开策略层次结构视图。
- 导入/导出 - 点击**导入/导出 (Import/Export)**；请参阅《Cisco Secure Firewall Management Center 管理指南》中的导入/导出。
- 报告 - 点击**报告**（）；请参阅生成当前策略报告，第 149 页。

创建基本访问控制策略

创建新的访问控制策略时，它包含默认操作和设置。创建策略后，您会立即进入编辑会话，以便您可以调整策略以满足您的要求。

过程

步骤 1 选择**策略** > **访问控制**。

步骤 2 点击**新建策略**。

步骤 3 在**名称 (Name)** 和**说明 (Description)**（可选）中输入唯一名称和说明。

步骤 4 或者，从**选择基本策略 (Select Base Policy)** 下拉列表中选择基本策略。

如果已在您的域上执行访问控制策略，则此步骤不为可选步骤。必须选择已执行的策略或其后代之一作为基本策略。

如果您选择基本策略，则基本策略定义默认操作，您无法在此对话框中选择新的操作。日志记录连接由基础策略的默认操作处理。

步骤 5 不选择基本策略时，请指定初始**默认操作**：

- **Block all traffic** 通过 **Access Control: Block All Traffic** 默认操作创建策略。
- **入侵防御 (Intrusion Prevention)** 可以通过**入侵防御：平衡安全性和连接 (Intrusion Prevention: Balanced Security and Connectivity)** 默认操作创建策略，与默认入侵变量集相关联。
- **Network Discovery** 使用默认操作 **Network Discovery Only** 创建策略。

当您选择默认操作时，默认操作处理的连接的日志记录最初处于禁用状态。您可以稍后在编辑策略时启用它。

提示　如果要在默认情况下信任所有流量，或如果已选择基本策略但不想继承默认操作，则可以稍后更改默认操作。

步骤 6 或者，选择要部署策略的**可用设备 (Available Devices)**，然后点击**添加到策略 (Add to Policy)**（或拖放）以添加所选设备。要减少显示的设备，请在 **Search** 字段中键入搜索字符串。

如果要立即部署此策略，则必须执行此步骤。

步骤 7 点击**保存 (Save)**。

新策略将打开以供编辑。您可以向其添加规则，并根据需要进行其他更改。请参阅编辑访问控制策略，第 1262 页。

相关主题

访问控制策略默认操作，第 1242 页
设置访问控制策略的目标设备，第 1269 页

编辑访问控制策略

编辑访问控制策略时，应将其锁定，以确保您的更改不会被同时编辑的其他人覆盖。

您只能编辑在当前域中创建的访问控制策略。此外，不能编辑由祖先访问控制策略锁定的设置。

注释 如果不锁定策略，请考虑以下事项：一个用户一次只能使用一个浏览器窗口编辑一个策略。如果多个用户保存同一个策略，系统会保留最后的更改。为方便起见，系统会显示有关当前正在编辑每条策略的人员（如有任何人）的信息。为保护会话隐私，当策略编辑器30分钟无任何活动后，系统将显示警告。60 分钟后，系统将放弃更改。

过程

步骤 1 选择**策略** > **访问控制**。

步骤 2 点击要编辑的访问控制策略旁边的 **编辑**（ ）。

如果显示**视图**（ ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 或者，点击**尝试新的 UI 布局 (Try New UI Layout)** 以切换到版本 7.2 中引入的用户界面。

这些程序将介绍如何在**旧版 UI**（用户界面）和**新版 UI** 中执行操作。两个接口配置相同的策略，区别仅在于表示。

您可以通过点击**切换到旧版 UI (Switch to Legacy UI)** 来返回旧版 UI。

步骤 4 （**旧版 UI**。）编辑访问控制策略。

提示 您可以通过按住 Shift 键的同时点击或按住 Control 键点击多个规则，然后右键点击并选择“编辑”来一次编辑多个规则。批量编辑可用于启用和禁用规则、选择规则操作以及设置大多数检测和日志记录设置。

设置：

- 名称和说明 - 点击任一字段并输入新信息。
- 默认操作 - 从**默认操作 (Default Action)** 下拉列表中选择一个值。
- 默认操作变量集 - 要更改与**入侵防御**默认操作关联的变量集，请点击 **变量**（ ）。在显示的弹出窗口中，选择新变量集并点击**确定 (OK)**。也可以点击 **编辑**（ ）以在新窗口中编辑所选的变量集。有关详细信息，请参阅管理变量，第 1054 页。
- 默认操作日志记录 - 要配置默认操作所处理的连接的日志记录，请点击 **日志记录**（ ）；请参阅 《Cisco Secure Firewall Management Center 管理指南》中的 日志记录与策略默认操作连接 。
- HTTP 响应 - 要指定当系统阻止网站请求时用户在浏览器中看到的内容，请点击 **HTTP 响应 (HTTP Responses)**；请参阅选择 HTTP 响应页面，第 1351 页。
- 继承：更改基本策略 - 要更改此策略的基本访问控制策略，请点击**继承设置**；请参阅选择基本访问控制策略，第 1267 页。
- 继承：锁定后代域中的设置 - 要在其后代策略中实施此策略的设置，请点击**继承设置**；请参阅锁定后代访问控制策略中的设置，第 1268 页。

- 策略分配：目标 - 要确定此策略所针对的受管设备，请点击**策略分配**；请参阅设置访问控制策略的目标设备，第 1269 页。
- 策略分配：域中需要 - 要在子域中实施此策略，请点击**策略分配**；请参阅在域中需要访问控制策略，第 1269 页。
- 规则 - 要使用入侵和文件策略来管理访问控制规则，以及检查和阻止恶意流量，请点击**规则 (Rules)**；请参阅创建和编辑访问控制规则，第 1288 页。
- 规则冲突 - 要显示规则冲突警告，请启用**显示规则冲突**。当一条规则由于评估中排序靠前的规则首先匹配流量而永远无法匹配流量时，会出现规则冲突问题。因为确定规则冲突会占用很多资源，所以显示它们可能需要一些时间。有关详细信息，请参阅订购规则的最佳实践，第 1254 页。
- 安全情报 - 要立即根据最新信誉情报将连接列入黑入单（阻止），请点击**安全情报 (Security Intelligence)**；请参阅配置安全情报，第 1362 页。
- 高级选项 - 要设置预处理、SSL 检查、身份、性能及其他高级选项，请点击**高级 (Advanced)**；请参阅访问控制策略高级设置，第 1271 页。
- 警告 - 要查看访问控制策略（及其后代和关联策略）中的警告或错误列表，请点击**显示警告 (Show Warnings)**。警告和错误标记出会对流量分析和数据流产生不利影响或阻碍策略部署的配置。如果没有警告，则会显示未出现警告。要查看规则冲突警告，请首先启用**显示规则冲突**。

步骤 5 (**新UI**) 编辑访问控制策略。

提示 您可以通过选中左列中的复选框，然后从搜索框旁边的**选择操作 (Select Action)** 下拉列表中选择要执行的操作，一次对多个规则进行操作。批量编辑可用于启用和禁用、复制、克隆、移动、删除和编辑规则，或查看命中计数或相关事件。

您可以更改以下设置或执行以下操作：

- 名称和说明 - 点击名称旁边的 **编辑**（ ），进行更改，然后点击**保存 (Save)**。
- 默认操作 - 从**默认操作 (Default Action)** 下拉列表中选择一个值。
- 默认操作设置 - 点击 **齿轮**（ ），进行更改，然后点击**确定 (OK)**。您可以配置日志记录设置、外部系统日志服务器或 SNMP 陷阱服务器的位置，以及与入侵防御默认操作关联的变量集。
- 关联的策略 - 要编辑或更改数据包流中的策略，请点击策略名称下方数据包流表示中的策略类型。您可以选择 **预处理规则**、 **SSL**、 **安全情报**和 **身份** 策略。必要时，点击**访问控制 (Access Control)** 以返回访问控制规则。
- 策略分配 - 要标识此策略的目标受管设备，或在子域中实施此策略，请点击**目标：x 设备 (Targeted: x devices)** 链接。
- 规则 - 要使用入侵和文件策略来管理访问控制规则，以及检查和阻止恶意流量，请点击**添加规则 (Add Rule)**，或右击现有规则并选择**编辑 (Edit)** 或其他响应操作。操作也可从每个规则的 **更多**（ ） 按钮获取。请参阅创建和编辑访问控制规则，第 1288 页。

- 布局 - 使用规则列表上方的**网格/表视图 (Grid/Table View)** 图标更改布局。网格视图以易于查看的布局提供彩色编码的对象。表视图提供摘要列表，以便您可以同时查看更多规则。您可以在不影响规则的情况下自由切换视图。
- 列（仅限表视图）- 点击规则列表上方的**显示/隐藏列 (Show/Hide Columns)** 图标，选择要在表中显示的信息。点击**隐藏空列 (Hide Empty Columns)** 以快速删除所有没有信息的列，即您不在任何规则中使用这些条件。点击**恢复为默认值 (Revert to Default)** 以撤消所有自定义设置。
- 命中计数 - 要查看有关与每个规则匹配的连接数的统计信息，请点击**分析命中计数 (Analyze Hit Counts)**。
- 其他设置 - 要更改策略的其他设置，请从数据包流行末尾的**更多 (More)** 下拉箭头中选择以下选项之一。
  - **高级设置 (Advanced Settings)** - 要设置预处理、SSL 检查、身份、性能及其他高级选项。请参阅访问控制策略高级设置，第 1271 页。
  - **HTTP 响应 (HTTP Responses)** - 要指定当系统阻止网站请求时用户在浏览器中看到的内容。请参阅选择 HTTP 响应页面，第 1351 页。
  - **继承设置 (Inheritance Settings)** - 更改此策略的基本访问控制策略，并在其后代策略中实施此策略的设置。请参阅选择基本访问控制策略，第 1267 页和锁定后代访问控制策略中的设置，第 1268 页。
  - **日志记录 (Logging)** - 设置策略的默认日志记录选项。

步骤 6 点击**保存 (Save)**。

下一步做什么

- 部署配置更改。

相关主题

规则和其他策略警告
使用文件和入侵策略的深度检测，第 1244 页

锁定访问控制策略

您可以锁定访问控制策略，以防止其他管理员对其进行编辑。锁定策略可确保在您保存更改之前，如果其他管理员编辑策略并保存更改，您的更改不会失效。在不锁定的情况下，如果多个管理员同时编辑策略，则以保存更改的第一个用户为准，而所有其他用户的更改都会被清除。

该锁用于访问控制策略本身。锁定不适用于策略中所使用的对象。例如，另一个用户可以编辑锁定访问控制策略中所使用的网络对象。在明确解锁策略之前，您的锁定将保持不变，因此您可以稍后注销并返回到您的编辑。

策略被锁定时，其他管理员对该策略具有只读访问权限。但是，其他管理员可以将已锁定的策略分配给托管设备。

开始之前

有权修改访问控制策略的任何用户角色都有权锁定该策略，并且还可以解锁被其他用户锁定的策略。

但是，解锁被其他管理员锁定的策略的能力受以下权限控制：**策略 (Policies)** > **访问控制 (Access Control)** > **访问控制策略 (Access Control Policy)** > **修改访问控制策略 (Modify Access Control Policy)** > **覆盖访问控制策略锁定 (Override Access Control Policy Lock)**。

如果您使用的是自定义角色，则您的组织可能会通过不分配此权限来限制您的解锁能力。如果没有此权限，则只有锁定策略的管理员才能解锁策略。

过程

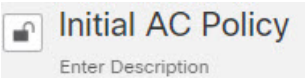
步骤 1 选择**策略** > **访问控制**。

步骤 2 点击要锁定或解锁的访问控制策略旁边的 **编辑**（）。

锁定状态 (Lock Status) 列会显示策略是否已被锁定，如果已锁定，则显示被谁锁定。空单元格表示策略未被锁定。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。否则，它已被其他用户锁定。

步骤 3 点击策略名称旁边的锁定图标可锁定或解锁策略。



如果策略从父策略继承了设置，则在点击锁定图标时必须选择以下选项之一。

- **锁定/解锁此策略 (Lock/Unlock This Policy)** - 锁定或解锁仅适用于此策略。
- **锁定/解锁此策略和层次结构中的父项 (Lock/Unlock This Policy and Parents in the Hierarchy)** - 锁定或解锁此策略和所有父策略。如果父策略已被其他管理员锁定，您将看到一条消息，并且无法锁定该父策略。解锁策略时，如果您具有“覆盖访问控制策略锁定”权限，则会解锁所有父策略，即使它们已被其他用户锁定。

管理访问控制策略继承

继承与使用其他策略作为访问控制策略的基本策略相关。这允许您使用一个策略来定义可应用于多个策略的一些基准特征。要了解继承的工作原理，请参阅访问控制策略继承，第 1247 页。

过程

步骤 1 编辑要更改其继承设置的访问控制策略；请参阅编辑访问控制策略，第 1262 页。

步骤 2 （**旧版 UI**。）管理策略继承：

- 更改基本策略 - 要更改此策略的基本访问控制策略，请点击**继承设置 (Inheritance Settings)**，然后如选择基本访问控制策略， 第 1267 页中所述继续操作。
- 锁定后代策略中的设置 - 要在此策略的所有后代策略中执行其设置，请点击**继承设置 (Inheritance Settings)**，然后如锁定后代访问控制策略中的设置， 第 1268 页中所述继续操作。
- 要求在域中提供 - 要在子域中执行此策略，请点击**策略分配 (Policy Assignment)**，然后如在域中需要访问控制策略， 第 1269 页中所述继续操作。
- 继承基本策略的设置 - 要继承基本访问控制策略的设置，请点击 **安全情报 (Security Intelligence)**、**HTTP 响应 (HTTP Responses)** 或**高级 (Advanced)**，然后如继承基本策略的访问控制策略设置， 第 1268 页中所述继续操作。

步骤 3 （**新 UI**）管理策略继承：

- 更改基本策略 (Change Base Policy) - 要更改基本访问控制策略，请从数据包流行末尾的**更多 (More)** 下拉箭头中选择**继承设置 (Inheritance Settings)**，然后如选择基本访问控制策略， 第 1267 页中所述继续操作。
- 锁定后代策略中的设置 (Lock Settings in Descendants) - 要在此策略的所有后代策略中执行其设置，请从数据包流行末尾的**更多 (More)** 下拉箭头中选择**继承设置 (Inheritance Settings)**，然后如锁定后代访问控制策略中的设置， 第 1268 页中所述继续操作。
- 要求在域中提供 (Required in Domains) - 要在子域中执行此策略，请点击**目标：x 个设备 (Targeted: x devices)** 链接，然后如在域中需要访问控制策略， 第 1269 页中所述继续操作。
- 继承基本策略的设置 (Inherit Settings from Base Policy) - 要继承基本访问控制策略的设置，请点击 **安全情报 (Security Intelligence)**，或从数据包流行末尾的下拉箭头中选择 **HTTP 响应 (HTTP Responses)** 或**高级设置 (Advanced Settings)**，然后如继承基本策略的访问控制策略设置， 第 1268 页中所述继续操作。

选择基本访问控制策略

可以使用一个访问控制策略作为另一个访问控制策略的基础（父级）。默认情况下，子策略从其基本策略继承其设置，但是可以更改未锁定的设置。

当更改当前访问控制策略的基本策略时，系统会使用新基本策略中的任何已锁定的设置来更新当前策略。

过程

步骤 1 在访问控制策略编辑器中，点击**继承设置 (Inheritance Settings)**（**旧 UI (Legacy UI)**）。在**新 UI (New UI)**中，从数据包流行末尾的**更多 (More)** 下拉箭头中选择**继承设置 (Inheritance Settings)**。

步骤 2 从**选择基本策略 (Select Base Policy)** 下拉列表中选择策略。

在多域部署中，在当前域中可能需要访问控制策略。只能选择已执行的策略或其后代之一作为基本策略。

步骤 3 点击**保存 (Save)**。

下一步做什么

- 部署配置更改。

继承基本策略的访问控制策略设置

新的子策略继承其基本策略的许多设置。如果这些设置在基本策略中未锁定，您可以覆盖这些设置。

如果稍后重新继承基本策略的设置，系统会显示基本策略的设置且控件呈灰色。不过，系统会保存所做的覆盖，如果您再次禁用继承，则会恢复覆盖设置。

过程

步骤 1 在访问控制策略编辑器中，点击**安全情报 (Security Intelligence)**、**HTTP 响应 (HTTP Responses)** 或**高级 (Advanced)**（旧 **UI**）.在**新 UI** 中，点击**安全智能 (Security Intelligence)**，或者从数据包流行末尾的**更多 (More)** 下拉箭头中选择 **HTTP 响应 (HTTP Responses)** 或**高级设置 (Advanced Settings)**

步骤 2 选中要继承的每个设置所对应的**继承自基本策略 (Inherit from base policy)** 复选框。

如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。

步骤 3 点击**保存 (Save)**。

下一步做什么

- 部署配置更改。

锁定后代访问控制策略中的设置

锁定访问控制策略中的设置，以便在所有后代策略中执行该设置。后代策略可以覆盖未锁定的设置。

当您锁定设置时，系统会保存后代策略中已经做出的覆盖，以便在您再次解锁设置时可以恢复这些覆盖设置。

过程

步骤 1 在访问控制策略编辑器中，点击**继承设置 (Inheritance Settings)**（旧 **UI (Legacy UI)**）。在**新 UI (New UI)**中，从数据包流行末尾的**更多 (More)** 下拉箭头中选择**继承设置 (Inheritance Settings)**。

步骤 2 在“子策略继承设置”(Child Policy Inheritance Settings) 区域中，选中要锁定的设置。

如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。

步骤 3 点击**确定 (OK)** 保存设置。

步骤 4 点击**保存 (Save)** 保存访问控制策略。

下一步做什么

- 部署配置更改。

在域中需要访问控制策略

您可以要求域中的每个设备都使用相同的基本访问控制策略或其后代策略之一。此程序仅适用于多域部署。

过程

步骤 1 在访问控制策略编辑器中，点击 **策略分配** （旧 **UI**）。在 **新 UI**，点击 **目标： x 设备** 连接。

步骤 2 点击 **在域中需要**。

步骤 3 构建域列表：

- 添加 - 选择要实施当前访问控制策略的域，然后点击**添加 (Add)** 或拖放到所选域列表中。
- 删除 - 点击枝叶域旁边的 **删除**（ ），或者右键点击祖先域并选择 **删除所选项**。
- 搜索 - 在搜索字段中键入搜索字符串。点击 **清除**（ ） 以清除搜索。

步骤 4 点击**确定 (OK)** 以保存域实施设置。

步骤 5 点击**保存 (Save)** 保存访问控制策略。

下一步做什么

- 部署配置更改。

设置访问控制策略的目标设备

访问控制策略指定使用策略的设备。每台设备只能作为一个访问控制策略的目标。在多域部署中，可能需要一个域中的所有设备使用同一基本策略。

过程

步骤 1 在访问控制策略编辑器中，点击 **策略分配** （旧 **UI**）。在 **新 UI**，点击 **目标： x 设备** 连接。

步骤 2 在 **目标设备** 上，建立目标列表：

- 添加 - 选择一个或多个**可用设备 (Available Devices)**，然后点击**添加到策略 (Add to Policy)** 或拖放到**所选设备 (Selected Devices)** 列表。
- 删除 - 点击单个设备旁边的 **删除**（ ），或选择多个设备，点击右键，然后选择 **删除选择**。
- 搜索 - 在搜索字段中键入搜索字符串。点击 **清除**（ ） 以清除搜索。

在**受影响的设备**下，系统会列出其分配的访问控制策略是当前策略子项的设备。对当前策略进行的任何更改都将影响这些设备。

步骤 3 （仅限多域部署。）或者，点击 **域中需要** 以要求您所选的子域中的所有设备使用同一基本策略。

步骤 4 点击**确定 (Ok)** 以保存目标设备设置。

步骤 5 点击**保存 (Save)** 保存访问控制策略。

下一步做什么

- 部署配置更改。

访问控制策略的日志记录设置

您可以为访问控制策略配置默认系统日志目标和系统日志警报。除非使用所包含规则和策略中的自定义设置显式覆盖系统日志目标设置，否则这些设置适用于访问控制策略以及所有包含在内的SSL/TLS解密、预过滤器和入侵策略。

默认操作处理的连接的日志记录最初处于禁用状态。

只有在页面顶部选择通常用于发送系统日志消息的选项后，IPS 和文件和恶意软件设置才会生效。

默认系统日志设置

- **使用特定系统日志警报发送**-如果选择此选项，则会根据 《Cisco Secure Firewall Management Center 管理指南》中 创建系统日志警报响应 的说明配置的所选系统日志警报发送事件。您可以从列表中选择系统日志警报，或通过指定名称、记录主机、端口、设施和严重性来添加警报。有关详细信息，请参阅 《Cisco Secure Firewall Management Center 管理指南》中的 入侵系统日志警报的设施和严重性。此选项适用于所有设备。
- **使用设备上部署的威胁防御平台设置策略中配置的系统日志设置**-如果选择此选项并选择严重性，则系统会将具有所选严重性的连接或入侵事件发送到“平台设置”中配置的系统日志收集器。使用此选项，您可以通过在“平台设置”中配置系统日志配置并重新使用访问控制策略中的设置来统一系统日志配置。本部分中选择的严重性适用于所有连接和入侵事件。默认严重性为警报。

  此选项仅适用于 Cisco Secure Firewall Threat Defense 6.3 及更高版本。

IPS 设置

- **发送 IPS 事件的系统日志消息**-将 IPS 事件作为系统日志消息发送。除非覆盖，否则将使用上面设置的默认值。
- **显示/隐藏覆盖**-如果要使用默认系统日志目标和严重性，请将这些选项留空。否则，可以为 IPS 事件设置不同的系统日志服务器目标，并更改事件的严重性。

文件和恶意软件设置

- **发送文件和恶意软件事件的系统日志消息**-将文件和恶意软件事件作为系统日志消息发送。除非覆盖，否则将使用上面设置的默认值。
- **显示/隐藏覆盖**-如果要使用默认系统日志目标和严重性，请将这些选项留空。否则，可以为文件和恶意软件事件设置不同的系统日志服务器目标，并更改事件的严重性。

访问控制策略高级设置

高级访问控制策略设置通常只需要进行很小的修改或不需要修改。默认设置适用于大多数的部署。请注意，规则更新可能会修改访问控制策略中的许多高级预处理和性能选项，如 《Cisco Secure Firewall Management Center 管理指南》 中 更新入侵规则 所述。

如果显示**视图**（），则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

注意 有关重启 Snort 进程的高级设置修改列表，请参阅部署或激活时重启 Snort 进程的配置，第 146 页，以暂时中断流量检查。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。

常规设置

选项	说明
要在连接事件中存储的最大URL字符数	要自定义您为用户所请求的每个 URL 存储的字符数。 要自定义用户绕过初始阻止后您重新阻止网站前的时长；请参阅为受阻网站设置用户绕过超时，第 1353 页。
允许交互式阻止绕过阻止的时长（秒）	请参阅为受阻网站设置用户绕过超时，第 1353 页。
重试 URL 缓存缺失查询	系统第一次遇到没有本地存储的类别和信誉的URL时，会在云中查找该URL并将结果添加到本地数据存储中，以便在将来更快地处理该 URL。 此设置确定系统需要在云中查找 URL 的类别和信誉时执行的操作。 默认情况下，此设置处于启用状态：系统在检查云的URL信誉和类别时会暂时延迟流量，并使用云判定来处理流量。 如果禁用此设置：当系统遇到不在其本地缓存中的URL时，系统会根据为未分类和无信誉流量配置的规则立即传递和处理流量。 在被动部署中，由于系统无法保留数据包，因此不会重试查询。

选项	说明
启用威胁情报导向器	禁用此选项以停止将 TID 数据发布到配置的设备。
对 DNS 流量启用信誉实施	默认情况下会启用此选项，以提高URL过滤性能和效力。有关详细信息和其他说明，请参阅 DNS 过滤：在 DNS 查找期间识别 URL 信誉和类别 ，第 1347 页 和子主题。
在策略应用期间检测流量	要在部署配置更改时检查流量（除非特定配置需要重新启动 Snort 进程），请确保**在策略应用期间检查流量 (Inspect traffic during policy apply)** 设置为其默认值（已启用）。 启用此选项后，资源需求可能会导致丢弃少量数据包而不进行检查。此外，部署某些配置会重新启动 Snort 进程，这会中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort® 重新启动场景 ，第 143 页。

关联策略

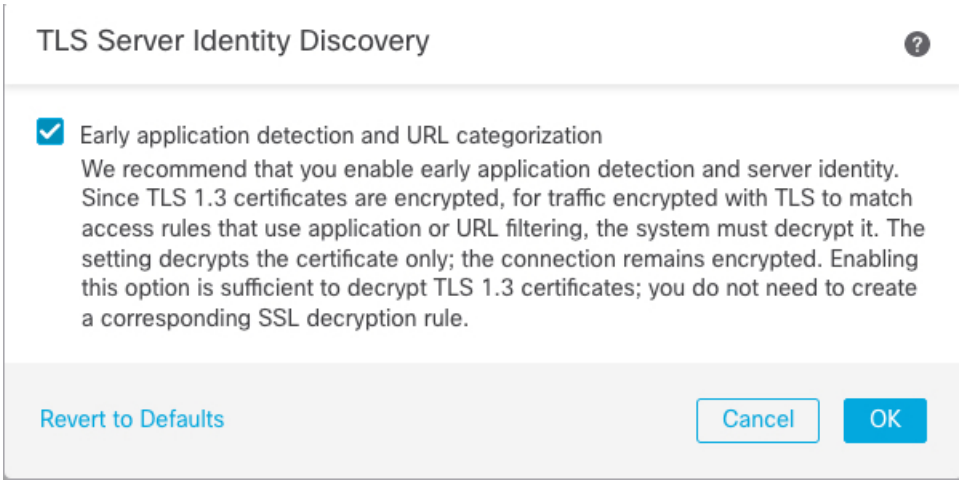
使用高级设置将子策略（解密、身份、预过滤器）与访问控制相关联；请参阅 将其他策略与访问控制相关联 ，第 1276 页。

TLS 服务器身份发现

RFC 8446定义的最新版本的传输层安全（TLS）协议 1.3 是许多 Web 服务器提供安全通信的首选协议。由于 TLS 1.3 协议会加密服务器的证书以提高安全性，并且需要使用证书来匹配访问控制规则中的应用和 URL 过滤条件，因此 Firepower 系统提供了一种提取服务器证书而 不 解密整个数据包的方法。

在为访问控制策略配置高级设置时，可以启用此功能，称为 *TLS* 服务器身份发现。

要启用 TLS 服务器身份发现，请点击 **高级** 选项卡，点击 **编辑**（ ） 以获取设置，然后选择**早期应用检测和 URL 类别**。



我们强烈建议您为要根据应用或URL条件匹配的任何流量启用此功能，尤其是在您想要对该流量执行深度检查时。SSL 策略 不需要 SSL 策略，因为在提取服务器证书的过程中不会解密流量。

注释

- 由于证书是解密的，因此 TLS 服务器身份发现会降低性能，具体取决于硬件平台。
- 内联分路模式或被动模式部署不支持 TLS 服务器身份发现。
- 任何部署到 AWS 的 Cisco Secure Firewall Threat Defense Virtual 都不支持启用 TLS 服务器身份发现。如果您有任何由Cisco Secure Firewall Management Center管理的此类托管设备，则每次设备尝试提取服务器证书时，连接事件 **PROBE_FLOW_DROP_BYPASS_PROXY** 都会增加。

网络分析和入侵策略

高级网络分析和入侵策略设置可供您：

- 指定用于检查数据包的入侵策略和相关变量集，在系统确定如何准确检查该流量之前，这些数据包必须通过。
- 更改访问控制策略的默认网络分析策略，该默认策略监管许多预处理选项。
- 使用自定义网络分析规则和网络分析策略根据特定安全区域、网络和 VLAN 定制预处理选项。

有关详细信息，请参阅网络分析和入侵策略的高级访问控制设置，第 2041 页。

威胁防御服务策略

可以使用威胁防御设备策略将服务应用到特定流量类。例如，可以使用服务策略创建特定于某项TCP应用而非应用于所有TCP应用的超时配置。此策略仅适用于威胁防御设备，对于其他任何设备类型将被忽略。在访问控制规则之后应用服务策略规则。有关详细信息，请参阅服务策略，第1413页。

文件和恶意软件设置

调整文件和恶意软件检测性能和存储，第1695页提供有关文件控制和恶意软件防护的性能选项的信息。

端口威胁检测

Portscan检测器是一种威胁检测机制，旨在帮助您检测和阻止所有类型流量中的端口扫描活动，以保护网络免受最终攻击。可以在允许和拒绝的流量中高效检测 Portscan 流量。。

大象流设置

象流是大型，持续时间长且快速的流，可能会导致Snort核心受到威胁。有两种操作可应用于象流，以减少系统压力、CPU 占用、丢包等。这些操作包括：

- 绕过任何或所有应用-此操作绕过来自 Snort 检测的流。
- Throttle-此操作对象流应用动态速率限制策略（降低 10%）。

智能应用绕行设置

智能应用绕行 (IAB) 是一种专业级配置，指定如果流量超出检查性能和流量阈值的组合，则应用绕行或测试是否要绕行。有关详细信息，请参阅智能应用旁路，第 1431 页。

传输/网络层预处理器设置

高级传输和网络预处理器设置全局应用于会部署访问控制策略的所有网络、区域和 VLAN。可以在访问控制策略中而非网络分析策略中配置这些高级设置。有关详细信息，请参阅高级传输/网络预处理器设置，第 2148 页。

检测增强功能设置

您可以使用高级检测增强功能设置配置自适应配置文件，以便：

- 使用访问控制规则中的文件策略和应用。
- 使用入侵规则中的服务元数据。
- 在被动部署中，根据您的网络主机操作系统改善数据包分片和 TCP 流的重组。

有关详细信息，请参阅自适应配置文件，第 2201 页。

性能设置和基于延迟的性能设置

关于入侵防御性能调整，第 1645 页提供了在您系统分析流量是否存在入侵尝试时如何提高系统性能的信息。

有关特定于基于延迟的性能设置的信息，请参阅数据包和入侵规则延迟阈值配置，第 1650 页。

加密可视性引擎

有关此功能的详细信息，请参阅加密可视性引擎。

加密可视性引擎

加密可视性引擎 (EVE)用于提供对加密会话的更多可视性，而无需对其进行解密。对 TLS 连接的见解源自思科的开源库，该库包含在思科的漏洞数据库 (VDB) 中。库指纹并分析传入的加密会话，并将其与一组已知指纹进行匹配。已知指纹的数据库在思科 VDB 中也可用。

使用访问控制策略的**高级 (Advanced)** 选项卡下的**加密可视性引擎 (EVE) (Encrypted Visibility Engine [EVE])** 切换按钮启用或禁用 EVE。在 管理中心 7.1 中，加密可视性引擎仅用于提供对加密流量的更多可视性。它不会对该流量执行任何操作。

在 管理中心 7.2 中，加密可视性引擎（EVE）具有以下增强功能：

- 要在 管理中心 7.2 上使用 EVE，您的设备上必须具有有效的 威胁 许可证。在没有 威胁 许可证的情况下，策略会显示警告，并且不允许部署。
- 您可以使用从 EVE 派生的信息对流量执行访问控制策略操作。
- Cisco Secure Firewall 7.2 中包含的 VDB 能够以高置信度值将应用分配给 EVE 检测到的某些进程。或者，您可以创建自定义应用检测器，以便：

- 将 EVE 检测到的进程映射到用户定义的新应用。
- 覆盖用于将应用分配给 EVE 检测到的进程的进程置信度的内置值。

  请参阅配置自定义应用检测器，第 1954 页和指定 EVE 进程分配，第 1958 页。

- EVE 可以检测在加密流量中创建客户端 Hello 数据包的客户端的操作系统类型和版本。
- EVE 也支持快速 UDP 互联网连接 (QUIC) 流量的指纹识别和分析。来自客户端 Hello 数据包的服务器名称显示在 **连接事件** 页面的 URL 字段中。

注释 只有运行 Snort 3 的 管理中心管理的设备才支持加密可视性引擎功能。Snort 2 设备， 设备管理器管理的设备或 CDO 不支持此功能。

启用**加密可视性引擎 (Encrypted Visibility Engine)** 切换按钮并部署访问控制策略后，您可以开始通过系统发送实时流量。您可以在“**连接事件**”页面中查看记录的连接事件。要访问连接事件，请在管理中心中转至 **分析 (Analysis)** > **连接 (Connections)** > **事件 (Events)**，然后点击**连接事件表视图 (Table View of Connection Events)** 选项卡。您还可以在 **分析** 菜单下的 **统一事件** 查看器中查看连接事件字段。加密可视化引擎 (Encrypted Visibility Engine) 可以识别发起连接的客户端进程、客户端上的 OS 以及该进程是否包含恶意软件。

在**连接事件 (Connection Events)** 页面中，为 加密可视性引擎 (Encrypted Visibility Engine) 添加了以下列：请注意，您必须明确启用上述列。

- 加密可视性进程名称
- 加密可视性进程置信度分数
- 加密可视性威胁置信度
- 加密可视性威胁置信度分数
- 检测类型

有关这些字段的信息，请参阅 《Cisco Firepower 管理中心管理指南》中 “连接和安全情报事件字段” 的部分。

注释 在“**连接事件**”页面中，如果为进程分配了应用，则“**检测类型**”列会显示 **加密可视化引擎**，表示客户端应用已被 EVE 识别。如果没有为进程名称分配应用， **检测类型** 列会显示 **AppID**，表示识别客户端应用的引擎是 AppID。

您可以在两个控制面板中查看分析信息。在 **概述** > **控制面板** 下，点击 **控制面板**。在 **摘要控制面板** 窗口中，点击 **交换机控制面板** 链接，然后从下拉框中选择 **应用统计信息**。选择 **加密可视性引擎** 选项卡以查看以下两个控制面板：

- **排名靠前的加密可视化引擎发现进程**-显示网络中使用的排名靠前的TLS进程名称和连接计数。您可以点击表中的进程名称，查看 **连接事件** 页面的过滤视图，该视图按进程名称进行过滤。

- **按加密可视化引擎威胁置信度的连接**-按恶意软件置信度级别（非常高，非常低等）显示连接。您可以点击表中的 威胁 置信度级别，查看 ”**连接事件**“ 页面的过滤视图，该视图按置信度级别进行过滤。

在 管理中心 7.2 中，EVE 可以检测 SSL 会话的操作系统类型和版本。操作系统的正常使用（例如运行应用、软件包管理软件等）可以触发操作系统检测。要查看客户端操作系统检测，除了启用 EVE 切换，您还必须在**策略 (Policies)** > **网络发现 (Network Discovery)**下启用 **主机 (Hosts)** 。要查看主机 IP 地址上可能的操作系统的列表，请点击**分析 (Analysis)** > **主机 (Hosts)** > **网络映射 (Network Map)**，然后选择所需的主机。

将其他策略与访问控制相关联

使用访问控制策略的高级设置将以下每一个子策略与该访问控制策略相关联：

- 预过滤器策略 - 使用有限网络（第 4 层）外部报头标准执行早期流量处理。
- SSL 策略 - 用于监控、解密、阻止或允许使用安全套接字层 (SSL) 或传输层安全 (TLS) 加密的应用层协议流量。

注意 仅*Snort 2*。添加或删除 SSL 政策在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。

- 身份策略 - 根据与流量关联的领域和确认方法执行用户身份验证。

开始之前

在将SSL策略与访问控制策略关联之前，请查看访问控制策略高级设置，第 1271 页中有关TLS服务器身份发现的信息。

过程

步骤 1 在访问控制策略编辑器中，点击 **高级** 选项卡 （**旧 UI**）。在 **新 UI**中，从数据包流行末尾的 **更多** 下拉箭头中选择 **高级设置** 。

步骤 2 在相应的“策略设置”区域点击 **编辑**（  ） 。

如果显示**视图**（  ），则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 3 从下拉列表中选择策略。

如果选择用户创建的策略，则可以点击显示的编辑来编辑策略。

步骤 4 点击 **OK**。

步骤 5 点击**保存 (Save)** 保存访问控制策略。

下一步做什么

- 部署配置更改。

相关主题

Snort® 重新启动场景，第 143 页

查看策略命中计数

命中计数表示策略规则或默认操作与连接匹配的次数。策略命中计数只会随匹配策略的连接的第一个数据包递增。您可以使用此信息来确定规则的有效性。只会为应用于威胁防御设备的访问控制和预过滤规则提供命中计数信息。

注释

- 即便是重新启动和升级，计数也会仍然存在。
- 计数会按高可用性对或集群中的每台设备来维护。
- 当设备上正在进行部署或任务时，您将无法从设备获取命中计数信息。
- 您还可以使用 **show rule hits** 命令在设备 CLI 中查看规则命中计数信息。
- 如果已从“访问控制策略”(Access Control Policy) 页面访问“命中计数”(Hit Count) 页面，则无法查看或编辑预过滤器规则，反之亦然。

开始之前

如果使用自定义用户角色，请确保角色包括以下权限：

- 查看设备，以查看命中计数。
- 修改设备，以刷新命中计数。

过程

步骤 1 在访问控制策略或预过滤器策略编辑器中，点击页面右上角的**分析命中计数 (Analyze Hit Counts)**。

步骤 2 在“命中计数”页面上，从**选择设备**下拉列表中选择设备。

如果不是第一次为此设备生成命中计数，最后一次获取的命中计数信息将出现在下拉框旁边。此外，验证**最新部署**时间，以确认最新的策略更改。

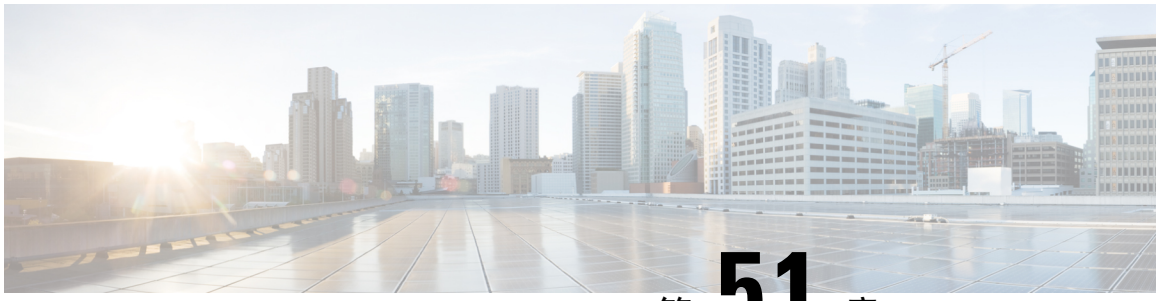
步骤 3 如果您已获得命中计数数据且想要更新的数字，请点击**获取当前命中计数 (Fetch Current Hit Count)** 以获取命中计数数据，或者点击**刷新 (Refresh)**。

步骤 4 查看和分析数据。

可以执行以下操作：

- 点击**预过滤器 (Prefilter)** 或**AC 策略 (AC Policy)**，以便在这些策略的命中计数之间切换。
- 通过在**过滤器规则/策略 (Filter Rules/Policy)** 框中输入搜索字符串来搜索特定规则。
- 通过在**过滤条件 (Filter by)** 字段中选择这些选项，将列表广泛地限制为**命中规则 (Hit Rules)** 或**从不命中规则 (Never Hit Rules)**。在查看命中规则时，您可以通过在**最后时间 (In Last)** 字段中选择一个时间范围（例如，最近 1 天）来进一步限制列表。
- 通过点击 **齿轮**（） 并选择要显示的列来更改显示的列。
- 点击规则名称以对其进行编辑，或点击最后一列中的 **视图**（  ） 以查看规则详细信息。点击规则名称会在策略页面中突出显示它，您可以在该页面中对规则进行编辑。
- 通过右键点击规则并选择**清除命中计数 (Clear Hit Count)**，清除规则的命中计数信息（将其重置为零）。您可以使用 Ctrl+点击来选择多个规则。您无法撤销此操作。
- 通过点击页面左下角的**生成 CSV (Generate CSV)** 来生成页面详细信息的逗号分隔值报告。

步骤 5 点击**关闭**返回策略页面。



第 51 章

访问控制规则

以下主题介绍如何配置访问控制规则：

访问控制规则简介

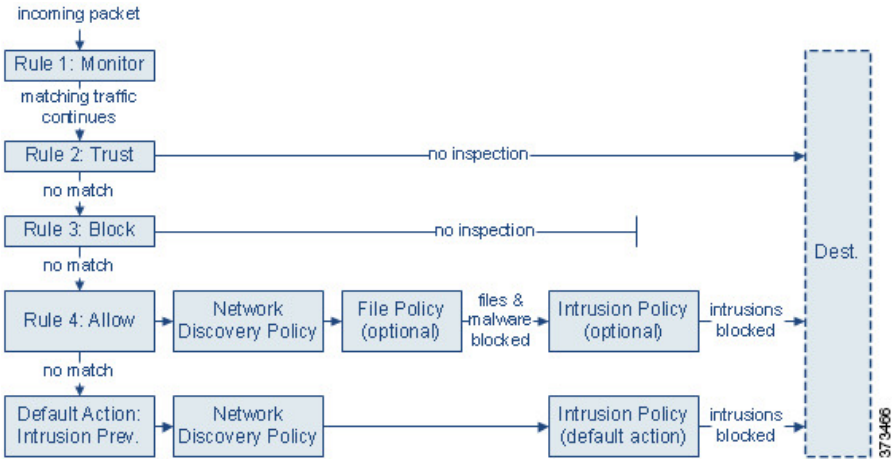
在访问控制策略中，访问控制规则提供在多台受管设备之间处理网络流量的精细方法。

注释 安全情报过滤、解密、用户标识以及某些解码和预处理发生在访问控制规则评估网络流量之前。

系统按您指定的顺序将流量与访问控制规则相匹配。在大多数情况下，系统根据所有规则条件匹配流量的第一个访问控制规则处理网络流量。

每个规则也有操作，确定是否监控、信任、阻止或允许匹配的流量。当您允许流量时，可以指定在流量到达您的资产或退出您的网络之前，系统首先利用入侵或文件策略对其进行检查以阻止任何漏洞攻击、恶意软件或禁止的文件。

以下场景汇总了内联入侵防御部署中访问控制规则评估流量的方式。



在这种情况中，流量评估如下：

- 首先，由**规则 1：监控 (Rule 1: Monitor)** 评估流量。“监控”(Monitor) 规则跟踪和记录网络流量。系统继续根据其他规则匹配流量，以确定允许其通过，还是拒绝。（但是，请参阅访问控制规则监控操作，第 1284 页中的重要例外情况和警告。）
- **规则 2：Trust** 继续评估流量。系统允许匹配的流量传至目标，而无需进一步检查，但此类流量仍会受到身份要求和速率限制的制约。不匹配的流量继续根据下一规则进行评估。
- 第三，由**规则 3：阻止 (Rule 3: Block)** 评估流量。匹配的流量被阻止，无需进一步检测。不匹配的流量继续根据最终规则进行评估。
- **规则 4：允许 (Rule 4: Allow)** 是最终规则。对于此规则，允许匹配的流量；但检测和阻止流量内禁止的文件、恶意软件、入侵和漏洞。系统允许其余未阻止的非恶意流量传至目标，但此类流量仍受到身份要求和速率限制的制约。您可以配置只执行文件检查、入侵检查或两类检查都不执行的“允许”(Allow) 规则。
- **Default Action** 处理不匹配任何规则的所有流量。在此场景下，默认操作在允许非恶意流量通过之前执行入侵防御。在不同的部署中，您可能有默认操作可以信任或阻止所有流量，而无需进一步检测。（您不能对默认操作处理的流量执行文件或恶意软件检测。）

无论是使用访问控制规则还是默认操作，您允许的流量都自动可用于根据网络发现策略检查主机、应用和用户数据。尽管可以增强或禁用发现功能，但不能明确启用该功能。但是，允许流量不会自动确保收集发现数据。系统仅对涉及 IP 地址的连接执行发现功能，根据网络发现策略明确监控这些 IP 地址；此外，对于加密会话，应用发现受到限制。

请注意，当解密配置允许已加密流量通过或者您不配置解密时，访问控制规则处理已加密流量。但是，某些访问控制规则条件需要未加密流量，因此，已加密流量可能匹配的规则更少。此外，默认情况下，系统禁用已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。

访问控制规则管理

访问控制策略编辑器的规则表格让您可以添加、编辑、分类、搜索、过滤、移动、启用、禁用、删除或以其他方式管理当前策略中的访问控制规则。

正确创建和排序访问控制规则是一项复杂的任务，但重要的是构建有效部署。如果不认真规划您的策略，这些规则会抢占其他规则，需要额外的许可证或包含无效配置。为帮助确保系统按预期处理流量，访问控制策略接口具有规则的强大警告和错误反馈系统。

使用搜索栏来过滤访问控制策略规则列表。在新用户界面中，您可以取消选择**仅显示匹配规则 (Show Only Matching Rules)** 选项以查看所有规则。匹配的规则会被突出显示。

对于每个访问控制规则，策略编辑器显示其名称、条件概述、规则操作以及传达规则检测选项或状态的图标。 在新用户界面中，操作和图标位于左侧而不是右侧，并且许多图标不会显示以便让视图更简洁（显示入侵、文件和日志记录，时间范围显示为钟面而不是如下所示的图标）。这些图标代表：

- **时间范围选项**（  ）
- **入侵策略**（）
- **文件策略**（  ）
- **安全搜索**（  ）
- **YouTube EDU**（  ）
- **日志记录**（  ）
- **注释**（  ）
- **警告**（  ）
- **错误**（  ）

已禁用的规则在规则名称后面呈灰色显示并带有相应的标记“（已禁用）”(disabled)。

要创建或编辑规则，请使用访问控制规则编辑器。规则编辑器会因您使用的用户界面而异。

旧版用户界面 - 您可以：

- 在编辑器的上部配置基本属性，如规则的名称、状态、位置和操作。
- 使用编辑器下部左侧的选项卡添加条件。
- 使用下部右侧的选项卡配置检测和日志记录选项，还可以向规则添加注释。为了方便，无论您在查看哪个选项卡，编辑器都列出规则的检测和日志记录选项。

新版用户界面 - 您可以：

- 配置规则名称并选择其在编辑器上部的位置。

- 通过选择编辑器上方或下方的行可以切换到编辑其他规则。
- 使用左侧列表来选择规则操作，并应用入侵策略和变量集、文件策略和时间范围以及顶部的日志记录选项。
- 使用规则名称旁边的选项来选择规则操作，并应用入侵策略和变量集、文件策略和时间范围以及顶部的日志记录选项。
- 使用**源 (Sources)** 和**目标和应用 (Destinations and Applications)** 列来添加匹配条件。
- 在编辑器的底部为规则添加评论。

相关主题

访问控制规则组成部分，第 1282 页
访问控制规则的最佳实践，第 1253 页

访问控制规则组成部分

除唯一名称之外，每个访问控制规则都具有以下基本组件：

状态

默认情况下，规则处于启用状态。如果禁用某规则，系统将不使用该规则并停止为该规则生成警告和错误。

位

系统已对访问控制策略中的规则进行编号，从 1 开始。如果正在使用策略继承，则规则 1 是最外层策略的第一条规则。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。除 Monitor 规则之外，流量匹配的第一个规则是处理该流量的规则。

规则也可属于某个部分和某个类别，其仅有利于组织且不影响规则位置。规则位置跨越部分和类别。

部分和类别

为帮助您组织访问控制规则，每个访问控制策略都有两个系统提供的规则部分：“强制性”(Mandatory) 规则部分和“默认”(Default) 规则部分。要进一步组织访问控制规则，您可以在“强制性”(Mandatory) 和“默认”(Default) 部分中创建自定义规则类别。

如果正在使用策略继承，则当前策略的规则嵌套在其父策略的“强制性”(Mandatory) 规则部分与“默认”(Default) 规则部分之间。

条件

条件指定规则处理的特定流量。条件可以简单也可以复杂；条件的使用通常取决于许可证。

流量必须满足规则中指定的所有条件。例如，如果应用条件指定了 HTTP 而不是 HTTPS，则 URL 类别和信誉条件将不适用于 HTTPS 流量。

适用时间

您可以指定规则适用的日期和时间。

操作

规则操作确定系统如何处理匹配的流量。您可以监控、信任、阻止或允许（执行或无需执行进一步检测）匹配的流量。系统不会对受信任、被阻止或加密的流量进行深度检查。

检查

深度检查选项管理系统如何检查和阻止您意外允许的恶意流量。通过规则允许流量时，可以指定系统先使用入侵或文件策略检测流量以在漏洞、恶意软件或禁止的文件到达您的资产或退出网络之前予以阻止。

日志记录

规则的日志记录设置管理系统保存其处理流量的记录。您可以对匹配规则的流量保存记录。一般来说，您可以在连接开始和/或结束时记录会话。您可以将连接记录到数据库，以及系统日志 (syslog) 或 SNMP 陷阱服务器。

备注

每次保存对访问控制规则所做的更改时，都可以添加注释。

相关主题

访问控制规则的最佳实践，第 1253 页
访问控制规则管理，第 1281 页
创建和编辑访问控制规则，第 1288 页
访问控制规则操作，第 1284 页
访问控制规则条件，第 1290 页
使用文件和入侵策略的深度检测，第 1244 页
访问控制规则注释

访问控制规则顺序

系统已对访问控制策略中的规则进行编号，从 1 开始。系统会用升序的规则号码以从上到下的顺序将流量匹配到访问控制规则中。

在大多数情况下，系统根据所有规则条件匹配流量的第一个访问控制规则处理网络流量。除监控规则，在流量匹配规则后系统不会根据其他优先级较低的规则继续评估流量。

为帮助您组织访问控制规则，每个访问控制策略都有两个系统提供的规则部分：“强制性”(Mandatory) 规则部分和“默认”(Default) 规则部分。要进一步组织，您可以在“强制性”(Mandatory) 和“默认”(Default) 部分中创建自定义规则类别。在创建类别后，无法将其移动，不过可以将其删除、对其重命名，并将规则移入、移出该类别以及在其内部或周围移动。系统跨部分和类别分配规则编号。

如果使用策略继承，则当前策略的规则嵌套在其父策略的“强制性”(Mandatory) 规则部分与“默认”(Default) 规则部分之间。规则 1 是最外层策略（不是当前策略）中的第一条规则，系统跨策略、部分和类别分配规则编号。

允许修改访问控制策略的任何预定义用户角色还允许您在规则类别内部和之间移动和修改访问控制规则。但是，可以创建自定义角色来限制用户移动和修改规则。允许修改访问控制策略的任意用户可以将规则添加到自定义类别，以及无限制的修改其中的规则。

注意 未能正确设置访问控制规则可能会导致意外结果，包括允许应阻止的流量。通常，应用控制规则应在访问控制列表中较低，因为与基于 IP 地址的规则相比，匹配这些规则所需的时间更长。

使用 特定 条件（例如网络和 IP 地址）的访问控制规则应在使用一般条件（例如应用）的规则 之前排序。如果您熟悉开放系统互联（OSI）模型，请在概念上使用类似的编号。包含第 1 层、第 2 层和第 3 层（物理、数据链路和网络）条件的规则应首先在访问控制规则中排序。稍后应在访问控制规则中对第 5 层、第 6 层和第 7 层的条件（会话，表示和应用）进行排序。有关 OSI 模型的详细信息，请参阅此 维基百科文章。

提示 适当的访问控制规则顺序可减少处理网络流量所需的资源并防止规则抢占。尽管您创建的规则对于每个组织和部署来说都是唯一的，但是排序规则时需要遵循几个基本原则，才可优化性能，同时满足您的需求。

相关主题

订购规则的最佳实践 ， 第 1254 页

访问控制规则操作

每个访问控制规则都具有用于确定系统如何处理和记录匹配流量的操作：您可以监控、信任、阻止或允许（执行或无需执行进一步检查）匹配流量。

访问控制策略的 默认操作 会处理不符合任何非 Monitor 访问控制规则条件的流量。

访问控制规则监控操作

监控 (Monitor) 操作不能允许或拒绝流量。相反，它的主要目的是强制连接日志记录，而不会考虑最终如何处理匹配的流量。

如果连接与监控规则匹配，则该连接匹配的下一个非监控规则应确定流量处理和任何进一步检查。如果没有其他匹配的规则，系统应使用默认操作。

但存在一个例外。如果监控规则包含第 7 层条件（例如应用条件），则系统将允许早期数据包通过并建立连接（或完成 SSL 握手）。即使连接应被后续规则阻止，也会发生这种情况；这是因为这些早期数据包不会根据后续规则接受评估。为了使这些数据包不会未经检查就到达目的地，您可以在访问控制策略的高级设置中为此目的指定入侵策略；请参阅在识别流量之前检查通过的数据包 ， 第 2042 页。在系统完成其第 7 层识别后，它就会将相应的操作应用于剩余会话流量。

注意 最佳实践是避免将第 7 层条件放在规则优先级较高的广泛定义的监控规则上，以防止无意中允许流量进入您的网络。此外，如果本地约束的流量与第 3 层部署中的 Monitor 规则相匹配，则该流量可能绕过检查。为确保对流量进行检查，在路由流量的受管设备的高级设备设置中启用 **Inspect Local Router Traffic**。

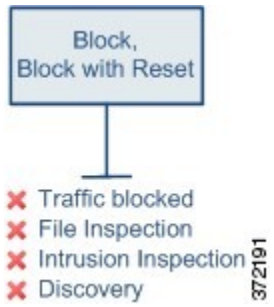
访问控制规则信任操作

信任 (Trust) 操作允许流量通过，无需深度检查或网络发现。受信任的流量仍会受到身份要求和速率限制的制约。

注释 某些协议（例如 FTP 和 SIP）会使用辅助信道，而系统会通过检测过程将其打开。在某些情况下，受信任的流量可以绕过所有检查，并且无法正确打开这些辅助通道。如果遇到此问题，请将信任规则更改为**允许 (Allow)**。

访问控制规则阻止操作

Block 和 **Block with reset** 操作拒绝流量，无需任何类型的进一步检测。



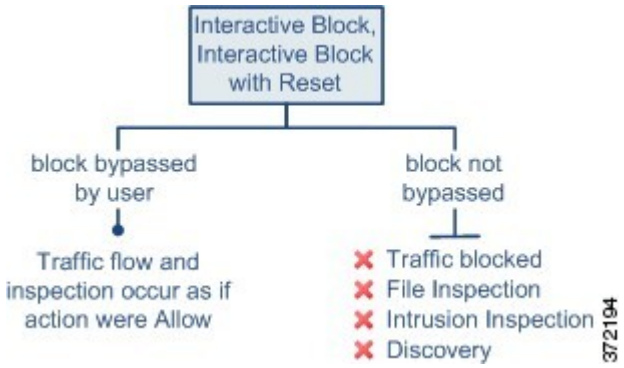
“阻止并重置”规则会重置连接，但 *HTTP* 响应页面遇到的 Web 请求除外。这是因为，如果立即重置连接，则配置为在系统阻止 Web 请求时显示的响应页面将无法显示。有关详细信息，请参阅HTTP 响应页面和交互式阻止。

相关主题

配置 HTTP 响应页面 ， 第 1350 页

访问控制规则交互式阻止操作

交互式阻止和**交互式阻止并重置**操作为 Web 用户提供继续访问其预期目的地的选项。



如果用户绕过阻止，该规则模拟“允许”规则。因此，您可以将交互式阻止规则与文件和入侵策略关联，并且匹配的流量也可用于网络发现。

如果用户未（或无法）绕过阻止，该规则模拟“阻止”规则。匹配流量会被拒绝，无需进一步检测。

请注意，如果启用交互式阻止，则无法重置所有被阻止的连接。这是因为，如果立即重置连接，响应页面将无法显示。使用**交互式阻止并重置**操作，以（通过非交互的方式）阻止并重置所有非 Web 流量，同时仍然为 Web 请求启用交互式阻止。

有关详细信息，请参阅HTTP 响应页面和交互式阻止。

相关主题

TLS/SSL 规则 阻止操作 ，第 1762 页

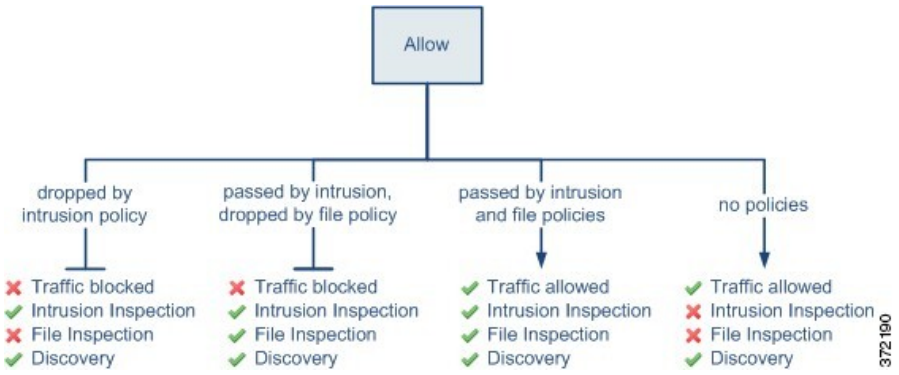
访问控制规则允许操作

允许 (Allow) 操作允许匹配的流量通过，但是仍会受到身份要求和速率限制的制约。

或者，您可以使用深度检查以在未加密或已解密流量到达目的地之前进一步对其进行检查和阻止：

- 您可以使用入侵策略，以便根据入侵检测和防御配置来分析网络流量，并根据配置丢弃恶意数据包。
- 您可使用文件策略执行文件控制。借助文件控制，可以检测和阻止用户通过特定应用协议上传（发送）或下载（接收）特定类型的文件。
- 您还可以使用文件策略执行基于网络的高级恶意软件防护 (AMP)。恶意软件防护 可检测文件中的恶意软件，并根据配置阻止检测到的恶意软件。

下图展示对满足“允许”(Allow) 规则（或用户绕过的“交互式阻止”[Interactive Block] 规则）条件的流量执行的检查类型。请注意，文件检测会在入侵检测之前发生；被阻止文件不会进行入侵相关漏洞检测。



为简单起见，该图显示入侵和文件策略均与访问控制规则相匹配（或都不匹配）的情况下的流量。但是，可以单独配置其中一个策略。如果没有文件策略，流量将由入侵策略确定；如果没有入侵策略，流量将由文件策略确定。

不管入侵或文件策略会检查还是丢弃流量，系统都可以使用网络发现功能进行检查。但是，允许流量不会自动确保发现检查。系统仅对涉及 IP 地址的连接执行发现功能，根据网络发现策略明确监控这些 IP 地址；此外，对于加密会话，应用发现受到限制。

访问控制规则的要求和必备条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

访问控制规则的准则与限制

- 如果编辑正在使用的访问控制规则，则更改不会在部署时应用于已建立的连接。此更新的规则用于根据未来的连接进行匹配。但是，如果系统正在主动检查连接（例如，使用入侵策略），则 会 将更改的匹配或操作条件应用于现有连接。

对于 威胁防御，您可以通过使用 威胁防御 **clear conn** CLI 命令结束已建立的连接，确保您的更改适用于所有当前连接。请注意，你应该只在结束这些连接是可以接受的情况下才这样做，前提是连接的来源将试图重新建立连接，从而与新规则进行适当的匹配。

- 访问规则中的 VLAN 标记仅适用于内联集；它们不能在应用于防火墙接口的访问规则中使用。

管理访问控制规则

以下主题介绍了如何管理访问控制规则。

添加访问控制规则类别

您可以将访问控制策略的“强制性”(Mandatory) 和“默认”(Default) 规则部分划分为自定义类别。在创建类别后，无法将其移动，不过可以将其删除、对其重命名，并将规则移入、移出该类别以及在其内部或周围移动。系统跨部分和类别分配规则编号。

过程

步骤 1 在访问控制策略编辑器中，点击**添加类别 (Add Category)**。

提示　如果您的策略已经包含规则，则可以点击现有规则在该行的空白区域，先设置新类别的位置，然后才能添加。还可以右键点击现有规则并选择 **Insert new category**。

步骤 2 输入 **Name**。

步骤 3 从**插入 (Insert)** 下拉列表中，选择要添加类别的位置：

- 要在某个部分中的所有现有类别下方插入类别，请选择**插入强制性类别 (into Mandatory)** 或**插入默认类别 (into Default)**。
- 要在现有类别上方插入类别，请选择**类别上方 (above category)**，然后选择类别。
- 要在访问控制规则上方或下方插入类别，请选择**规则上方 (above rule)** 或**规则下方 (below rule)**，然后输入现有规则编号。

步骤 4 点击**确定 (OK)**。

步骤 5 点击**保存 (Save)** 保存策略。

创建和编辑访问控制规则

使用访问控制规则将操作应用于特定流量类。规则允许您选择性地允许所需流量并丢弃不需要的流量。

过程

步骤 1 在访问控制策略编辑器中，您有以下选择：

- 要添加新规则，请点击 **Add Rule**。
- 要编辑现有规则，请点击 **编辑**（）（**旧版UI**）。在 **新建 UI**中，右键点击或 **更多**（）菜单中提供 **编辑** 。
- 要编辑多个规则，请按住 Shift 键并点击一系列规则，或按住 Control 键并点击要编辑的多个规则，然后右键点击并选择一个选项。在 **新建 UI中**，使用复选框选择多个规则，然后 从 搜索框旁边的 **选择操作** 列表中选择 **编辑** 或其他操作。

如果规则旁显示**视图**（），则表明规则属于祖先策略，或者您没有修改规则的权限。

步骤 2 如果这是新规则，请输入 **名称**。

步骤 3 （**旧版 UI**。） 配置规则组成部分。

如果批量编辑多个规则，则只有一部分选项可用。

- **已启用** -指定规则是否为已启用。
- 位置 - 指定规则位置；请参阅访问控制规则顺序， 第 1283 页。
- 操作 - 在**操作 (Action)** 中选择规则操作；请参阅访问控制规则操作， 第 1284 页。
- 时间范围-（可选）。对于 威胁防御 设备，请选择规则适用的日期和时间。有关详细信息，请参阅创建时间范围对象， 第 1039 页。
- 条件 - 点击要添加的对应条件。有关详细信息，请参阅 访问控制规则条件， 第 1290 页 。

  注释 访问规则中的 VLAN 标记仅适用于内联集；它们不能在应用于防火墙接口的访问规则中使用。

- 深度检测-（可选）。对于允许和交互组织规则，点击 **入侵策略**（） 或 **文件策略**（） 配置规则的**检查**选项。如果选项呈灰色显示，则表示没有为规则选择此类型的策略。有关详细信息，请参阅访问控制概述， 第 1239 页。
- 内容限制 - 点击 **安全搜索**（） 或 **YouTube EDU**（） 以配置规则编辑器的 **应用** 选项卡上的内容限制设置。如果选项呈灰色显示，则表示对规则禁用内容限制。有关详细信息，请参阅关于内容限制， 第 1439 页。
- 日志记录 - 点击 **日志记录**（） 以指定 **日志记录** 选项。如果选项呈灰色显示，则表示对规则禁用连接日志记录。
- 注释 - 点击注释列中的数值可添加**注释 (Comments)**。编号指示规则已包含的注释数。

步骤 4 （**新建 UI**） 配置规则组成部分。

如果批量编辑多个规则，则只有一部分选项可用。

- 位置 - 指定规则位置；请参阅访问控制规则顺序，第 1283 页。
- 操作 - 在**操作 (Action)** 中选择规则操作；请参阅访问控制规则操作，第 1284 页。
- 深度检测-（可选）。对于允许和交互阻止规则，选择 **入侵策略**，**变量集** 和 **文件策略** 选项。您可以单独应用入侵和文件策略；您不需要同时配置两者。
- 时间范围-（可选）。对于 威胁防御 设备，请选择规则适用的日期和时间。如果不选择选项，则规则始终处于活动状态。有关详细信息，请参阅创建时间范围对象，第 1039 页。
- 日志记录-点击 **日志记录** 可指定连接日志记录和 SNMP 陷阱的选项。
- 条件-点击 **源** 和 **目标** 列中的 + 以添加连接的匹配条件。有关详细信息，请参阅访问控制规则条件，第 1290 页。
- 注释-打开对话框底部的注释列表，输入注释，然后点击 **发布** 添加注释。

步骤 5 点击**确定**以保存该规则。

步骤 6 点击**保存 (Save)** 保存策略。

下一步做什么

如果要部署基于时间的规则，请指定策略分配到的设备的时区。请参阅为策略应用配置设备时区，第 662 页。

部署配置更改。

相关主题

访问控制规则的最佳实践，第 1253 页

访问控制规则条件

规则条件定义要使用每条规则作为目标的连接的特征。精确使用条件来微调规则，以应用于仅应由规则处理的流量。以下主题介绍可使用的匹配条件。

安全/隧道区域规则条件

可以使用安全区域和隧道区域为规则选择流量。

安全区域可对网络进行分段，以通过跨多个设备将接口分组来帮助管理和分类流量。隧道区域允许您识别应作为隧道处理的隧道流量（例如 GRE），而不是将访问控制规则应用于隧道内的封装连接。

您可以使用安全区域按源接口和目标接口控制流量。如果将源区域和目标区域均添加到区域条件中，则匹配流量必须源自其中一个源区域的接口，并通过其中一个目标区域的接口流出，以匹配规则。正如安全区域中的所有接口都必须为同一类型（均为内联、被动、交换或路由），区域条件中使用的所有区域也必须为同一类型。由于被动部署的设备不会传输流量，因此不能使用具有被动接口的区域作为目标区域。

使用隧道区域时，请确保预过滤器策略中有匹配的规则，以将隧道流量与该区域相关联。然后，您可以选择隧道区域作为规则中的源区域；隧道区域不能是目的地。如果没有将隧道重新分区到隧道区域的预过滤器规则，则隧道的访问控制规则将永远不会应用于任何连接。您可以将目标安全区域指定为通过特定接口离开设备的目标隧道。

安全区域注意事项

在决定安全区域标准时，请考虑以下事项：

- 尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。
- 访问控制规则会在设备配置中生成 ACL 条目 (ACE)，以便尽可能提供早期处理和丢弃。如果在规则中指定安全区域，则会为区域中的每个接口创建 ACE，这会大大增加 ACL 的大小。从访问控制规则生成的过大 ACL 可能会影响系统性能。
- 在多域部署中，在祖先域中创建的区域可以包含位于不同域中的设备上的接口。在后代域中配置区域条件时，您的配置仅适用于可以看到的接口。

网络规则条件

网络规则条件是定义流量的网络地址或位置的网络对象或地理位置。

- 要匹配来自某个 IP 地址或地理位置的流量，请将条件添加到源列表。
- 要将流量匹配到某个 IP 地址或地理位置，请将条件添加到目标列表。
- 如果同时向一条规则添加源网络条件和目标网络条件，匹配流量必须源自其中一个指定 IP 地址并流向其中一个目标 IP 地址。

添加此条件时，可从以下选项卡中进行选择：

- **网络** - 为您要控制的流量选择定义源或目标 IP 地址的网络对象或组。您可以使用通过完全限定域名 (FQDN) 定义地址的对象；通过 DNS 查询确定地址。
- **地理位置** - 选择要基于流量的源或目的国家/地区或大洲控制流量的地理位置。选择大洲将会选择该大洲内的所有国家/地区。除了直接在规则中选择地理位置外，也可以选择您创建的地理位置对象来定义位置。使用地理位置，可以便捷地限制对特定国家/地区的访问，而不需要知道此位置所用的全部潜在 IP 地址。

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

网络条件中的原始客户端（过滤代理流量）

对于某些规则，可以根据始发客户端处理代理流量。使用源网络条件指定代理服务器，然后添加原始客户端限制以指定原始客户端 IP 地址。系统将使用数据包的 X-Forwarded-For (XFF)、真实客户端 IP 或自定义的 HTTP 标头报头字段来确定原始客户端 IP。

如果代理的 IP 地址与规则的源网络限制匹配，**并且**原始客户端的 IP 地址与规则的原始客户端限制匹配，则流量与规则匹配。例如，要允许来自特定原始客户端地址的流量，但仅允许其中使用特定代理的流量，请创建三条访问控制规则：

访问控制规则 1：阻止来自特定 IP 地址 (209.165.201.1) 的代理流量

源网络：209.165.201.1
原始客户端网络：无/任意
Action: Block

访问控制规则 2：允许来自同一 IP 地址的代理流量，但只允许其代理服务器为您所选的代理服务器（209.165.200.225 或 209.165.200.238）的流量

源网络：209.165.200.225 和 209.165.200.238
原始客户端网络：209.165.201.1
Action: Allow

访问控制规则 3：阻止来自同一 IP 地址但使用任何其他代理服务器的代理流量。

源网络：任意
原始客户端网络：209.165.201.1
Action: Block

VLAN 标记规则条件

注释 访问规则中的 VLAN 标记仅适用于内联集。带 VLAN 标记的访问规则与防火墙接口上的流量不匹配。

VLAN 规则条件可控制 VLAN 标记的流量，包括 Q-in-Q（堆栈 VLAN）流量。系统使用最内层的 VLAN 标记过滤 VLAN 流量，但不包括预过滤器策略，因为它在其规则中使用最外层的 VLAN 标记。

请注意以下 Q-in-Q 支持：

- Firepower 4100/9300 上的威胁防御 -不支持 Q-in-Q （仅支持一个 VLAN 标记）。
- 所有其他型号上的威胁防御 ：
  - 内联集和被动接口-支持 Q-in-Q，最多2个 VLAN 标记。
  - 防火墙接口-不支持 Q-in-Q （仅支持一个 VLAN 标记）。

可以使用预定义对象构建 VLAN 条件，或手动输入从 1 到 4094 之间的任意 VLAN 标记。使用连字符可指定 VLAN 标记范围。

最多可以指定 50 个 VLAN 条件。

在集群中，如果遇到 VLAN 匹配问题，请编辑访问控制策略高级选项“传输/网络预处理器设置”(Transport/Network Preprocessor Settings)，然后选择**跟踪连接时忽略 VLAN 信头 (Ignore the VLAN header when tracking connections)** 选项。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 VLAN 标记限制此配置可产生意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

用户规则条件

用户规则条件会根据发起连接的用户或用户所属的组来匹配流量。例如，您可以配置阻止规则以禁止财务组中的任何人访问网络资源。

（仅适用于访问控制规则）您必须首先将身份策略与访问控制策略相关联，如将其他策略与访问控制相关联，第 1276 页中所述。

除了为已配置的领域配置用户和组之外，您还可以为以下特殊身份的用户设置策略：

- 身份验证失败：强制网络门户身份验证失败的用户。
- 访客：在强制网络门户中被配置为访客用户的用户。
- 无需身份验证：匹配**无需身份验证 (No Authentication Required)** 规则操作的用户。
- 未知：无法识别的用户；例如，配置的领域未下载的用户。

应用规则条件

系统分析 IP 流量时，可以识别网络上的常用应用并将其分类。这种基于发现的应用感知是应用控制的基础 - 能够控制应用流量。

借助系统提供的应用过滤器，您可以根据应用的基本特征（类型、风险、业务关联性、类别和标记）组织应用，从而执行应用控制。您可以系统提供的过滤器的组合或以应用的自定义组合为基础，创建可重复使用的用户定义过滤器。

对于策略中的每个应用程序规则条件，必须启用至少一个检测器。如果没有为应用启用检测器，则系统会为该应用自动启用所有系统提供的检测器；如果不存在检测器，则系统为该应用启用最新修改的用户定义的检测器。有关应用检测器的详细信息，请参阅应用检测器基础知识，第 1946 页。

您可以使用应用过滤器和单独指定的应用来确保完整覆盖。但是，在订购访问控制规则之前，请了解以下说明。

应用过滤器的优势

应用过滤器可帮助您快速配置应用控制。例如，您可以轻松地使用系统提供的过滤器创建一条访问控制规则，用于识别并阻止所有业务关联性较低的高风险应用。如果用户尝试使用其中一个应用，则系统会阻止会话。

使用应用过滤器可简化策略创建和管理。此方法可保证系统按预期控制应用流量。由于思科经常通过系统和漏洞数据库 (VDB) 更新和添加应用检测器，因此您可确保系统使用最新的检测器监控应用流量。您还可以创建自己的检测器并将特征分配给其检测到的应用，自动将应用添加到现有过滤器。

应用特征

系统使用下表中所述的条件来展示其检测到的每个应用的特征。这些特征用作应用过滤器。

表 *94:* 应用特征

特征	说明 (Description)	示例
类型	应用协议代表主机之间的通信。 客户端代表在主机上运行的软件。 Web 应用代表 HTTP 流量的内容或所请求的 URL。	HTTP 和 SSH 是应用协议。 网络浏览器和邮件客户端是客户端。 MPEG 视频和 Facebook 是网络应用。
风险	应用用于可能违反您的组织安全策略的用途的可能性。	点对点应用的风险通常很高。
业务相关性	应用用于您的组织的业务运营（相对于娱乐目的）的情景中的可能性。	游戏应用的业务相关性通常很低。
类别	说明应用的最基本功能的应用通用分类。每个应用至少属于一个类别。	Facebook 属于社交网络类别。
标签	有关应用的附加信息。应用可以包括任何数量的标记，也可以没有标记。	视频流网络应用通常标记为 `high bandwidth` 和 `displays ads`。

相关主题

配置应用控制的最佳实践，第 1250 页

配置应用条件和过滤器

要构建应用条件或过滤器，请从可用应用列表中选择要控制其流量的应用。或者，可以按照建议使用过滤器限制可用应用。在相同条件下可以使用过滤器和单独指定的应用。

开始之前

- 必须按照配置自适应配置文件，第 2204 页中的说明来启用（其默认状态）自适应分析，以便访问控制规则可以执行应用控制。
- 如果要实施内容限制，请遵循使用访问控制规则执行内容限制，第 1441 页中的程序而不是本程序。
- 对于经典设备型号，您必须拥有控制许可证才能配置这些条件。

过程

步骤 1 调用规则或配置编辑器：

- 访问控制（旧版 UI）、解密、QoS 规则条件 - 在规则编辑器中，点击**应用 (Applications)**。在新的访问控制 UI 中，点击“目标和应用”(Destinations and Applications) 列中的 +，然后点击“应用”(App) 选项卡。
- 身份规则条件 - 在规则编辑器中，点击**领域和设置 (Realm & Settings)** 并启用主动身份验证；请参阅创建身份规则，第 1894 页。

- 应用过滤器 - 在对象管理器的“应用过滤器”(Application Filters) 页面上，添加或编辑应用过滤器。在**名称 (Name)** 中为过滤器提供唯一名称。
- 智能应用绕行 (IAB) - 在访问控制策略编辑器中，点击**高级 (Advanced)** 选项卡，编辑 IAB 设置，然后点击**可绕行的应用和过滤器 (Bypassable Applications and Filters)**。

步骤 2 从**可用应用 (Available Applications)** 列表查找并选择要添加的应用。

要限制**可用应用 (Available Applications)** 中显示的应用，请选择一个或多个**应用过滤器 (Application Filters)** 或搜索单个应用。

提示 点击应用旁边的 **信息**（ ） 以显示摘要信息和互联网搜索链接。**解锁** 标记系统只能在已解密流量中识别的应用。

选择过滤器（单一或组合）时，“可用应用”(Available Applications) 列表会更新为仅显示符合条件的应用。您可以选择系统提供的组合形式的过滤器，但不能选择用户定义的过滤器。

- 针对同一特征选择多个过滤器（风险、业务关联性等）- 应用流量必须仅匹配其中一个过滤器。例如，如果选择中风险和高风险过滤器，则“可用应用”(Available Applications) 列表会显示所有中风险和高风险应用。
- 针对不同应用特征选择过滤器 - 应用流量必须与两个过滤器类型匹配。例如，如果您选择高风险和低业务关联性过滤器，则“可用应用”(Available Applications) 列表仅显示满足这两个条件的应用。

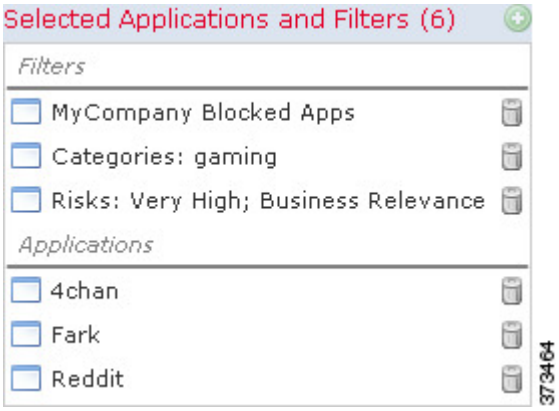
步骤 3 点击**添加到规则 (Add to Rule)**，或进行拖放操作。在新的访问控制 UI 中，点击 **添加应用 (Add Application)**。

提示 在添加更多过滤器和应用之前，点击**清除过滤器 (Clear Filters)** 以清除当前选择。

步骤 4 保存或继续编辑规则或配置。

示例：访问控制规则中的应用条件

下图显示用于阻止以下内容的访问控制规则的应用条件：MyCompany 的用户定义应用过滤器、具有高风险和低业务关联性的所有应用、游戏应用以及一些单独选定的应用。



下一步做什么

- 部署配置更改。

端口、协议和 ICMP 代码规则条件

端口条件根据源和目标端口匹配流量。根据规则类型，“端口”可以表示以下任何一项：

- TCP 和 UDP - 可以根据端口控制 TCP 和 UDP 流量。系统使用括号内的协议号，以及可选的关联端口或端口范围来表示此配置。例如：TCP(6)/22。
- ICMP - 可以根据 ICMP 和 ICMPv6 (IPv6-ICMP) 流量的互联网层协议及可选类型和代码控制该流量。例如：ICMP(1):3:3。
- 协议-您可以借助于未使用端口的其他协议控制流量。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

基于端口的规则的最佳实践

指定端口是目标应用的传统方式。但是，可以将应用配置为使用唯一端口绕过访问控制块。因此，尽可能使用应用过滤条件而不是端口条件来确定流量目标。请注意，应用过滤在预过滤器规则中不可用。

应用过滤也建议用于动态打开单独通道的应用（如 FTP），以实现控制和数据流。使用基于端口的访问控制规则可能会阻止此类应用正确执行，并可能导致阻止所需的连接。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为目标端口条件。

将非 TCP 流量与端口条件相匹配

您可以匹配非基于端口的协议。默认情况下，如果不指定端口条件，则匹配 IP 流量。虽然可以将端口条件配置为与非 TCP 流量相匹配，但有一些限制：

- 访问控制规则 - 对于典型设备，可以通过使用 GRE (47) 协议作为目标端口条件将 GRE 封装的流量与访问控制规则相匹配。对于 GRE 限制的规则，只能添加基于网络的条件：区域、IP 地址、端口和 VLAN 标签。此外，系统使用外部报头将访问控制策略中的**所有**流量与 GRE 限制的规则相匹配。对于 威胁防御设备，请使用预过滤器策略中的隧道规则来控制 GRE 封装的流量。
- SSL 规则 - SSL 规则仅支持 TCP 端口条件。
- IMCP 回应 - 类型设置为 0 的目标 ICMP 端口或类型设置为 129 的目标 ICMPv6 端口仅与主动回应回复相匹配。为应答 ICMP 回应请求而发送的 ICMP 回应回复被忽略。为使某个规则匹配任何 ICMP 回应，请使用 ICMP 类型 8 或 ICMPv6 类型 128。

URL 规则条件

使用 URL 条件控制网络上的用户可以访问的网站。

有关完整信息，请参阅URL 过滤，第 1335 页。

动态属性规则条件

动态属性包括以下内容：

- 动态对象（例如来自 Cisco Secure Dynamic Attributes Connector）

  dynamic attributes connector 让您能够从云提供商收集数据（例如网络和 IP 地址）并将其发送到 Firepower 管理中心，以便将其用于访问控制规则中。。

  有关 dynamic attributes connector 的详细信息，请参阅本指南后面的信息。
- SGT 对象
- 位置 IP 对象
- 设备类型对象
- 终端配置文件对象

动态属性可用作访问控制规则中的源条件和目标条件。使用以下准则：

- 不同类型的对象通过 AND 连接在一起
- 将相似类型的对象一起进行 ORd 运算

例如，如果选择源目标条件 SGT 1、SGT 2 和设备类型 1；如果在 SGT 1 或 SGT 2 上检测到设备类型 1，则规则匹配。

动态对象

动态对象是可以使用 IP 或使用 Cisco Secure Dynamic Attributes Connector 来创建的对象，作为一种集成，它允许在 管理中心 访问控制规则中使用来自云网络产品的对象。

有关 dynamic attributes connector 的详细信息，请参阅本指南后面的信息。

动态对象和网络对象之间的差异如下：

- 使用 dynamic attributes connector 创建的动态对象会在创建后立即被推送到 管理中心，并且还会定期更新。
- API 创建的动态对象：
  - 是 IP 地址，有或没有或无类域间路由 (CIDR)，可以在访问控制规则中使用，与网络对象很相似。
  - 不支持完全限定域名或地址范围。
  - 必须使用 API 进行更新。

相关主题

添加或编辑动态对象 ，第 987 页

时间和日期规则条件

您可以指定连续时间范围或周期性时间段。

例如，规则只能在工作日工作时间或每个周末或节假关闭期间应用。

基于时间的规则基于处理流量的设备的本地时间应用。

基于时间的规则仅在 FTD 设备上受支持。如果将具有基于时间的规则的策略分配给不同类型的设备，则在该设备上会忽略与该规则关联的时间限制。在这种情况下，您将看到警告。

启用和禁用访问控制规则

创建访问控制规则时，默认情况下启用规则。如果您禁用某规则，系统将不用该规则来评估网络流量并停止为该规则生成警告和错误。在查看访问控制策略中的规则列表时，禁用的规则会呈灰色显示，不过，您仍然可以修改它们。

您还可以使用规则编辑器启用或禁用访问控制规则。

过程

步骤 1 在访问控制策略编辑器中，右键点击规则并选择规则状态。

如果规则旁显示**视图**（  ），则表明规则属于祖先策略，或者您没有修改规则的权限。

步骤 2 点击**保存 (Save)**。

下一步做什么

- 部署配置更改。

相关主题

访问控制规则组成部分，第 1282 页

将访问控制规则从一个访问控制策略复制到另一个

您可以将访问控制规则从一个访问控制策略复制到另一个访问控制策略。您可以将规则复制到访问控制策略的**默认 (Default)** 部分或**强制 (Mandatory)** 部分。

已复制规则的所有设置（注释除外）都将保留在粘贴的版本中。但是，复制的规则中会添加一条新注释，其中提及了源访问控制策略。

过程

步骤 1 在访问控制策略编辑器中，选择要复制的规则。

（**旧版 UI**。） 要选择多条规则，请使用 Ctrl + 点击。

（**新用户界面**。）要选择多个规则，请选中每个规则的复选框。

步骤 2 右键点击所选规则，然后选择**复制到 (Copy to)** > **其他策略 (Another policy)**（**旧版 UI (Legacy UI)**）或**复制到其他策略 (Copy to Different Policy)**（**新用户界面 (New UI)**）。

步骤 3 从**访问策略 (Access Policy)** 下拉列表中选择目标访问控制策略。

步骤 4 从**放置规则 (Place Rules)** 下拉列表中，选择要放置所复制规则的位置。

- 要将其定位为**默认 (Default)** 部分中的最后一组规则，请选择**底部（在“默认”部分中） (At the bottom [within the Default section])**。
- 要将其定位为**必填 (Mandatory)** 部分中的第一组规则，请选择**顶部（在“必填”部分中） (At the top [within the Mandatory section])**。

步骤 5 点击**复制 (Copy)**。

下一步做什么

- 部署配置更改。

将访问控制规则移至预过滤器策略

您可以将访问控制规则从访问控制策略移至关联的非默认预过滤器策略。

您必须先将用户定义的预过滤器策略应用于访问控制策略。无法将访问控制规则移至默认的预过滤器策略，因为默认预过滤器策略不能包含规则。

开始之前

请在继续之前注意以下条件：

- 在将访问控制规则移至预过滤器策略时，无法移动访问控制规则中的第 7 层 (L7) 参数。L7 参数会在操作期间被丢弃。
- 在移动规则后，访问控制规则配置中的注释会丢失。但是，移动的规则中会添加一条新注释，其中提及了源访问控制策略。
- 您不能移动将**监控 (Monitor)** 设置为**操作 (Action)** 参数的访问控制规则。
- 移动时，访问控制规则中的**操作 (Action)** 参数将更改为预过滤器规则中的适当操作。要了解访问控制规则中的每个操作，请参阅下表：

访问控制规则中的操作	预过滤器规则中的操作
允许	分析
阻止	阻止
阻止并重置	阻止
交互式阻止	阻止
交互式阻止并重置	阻止
信任	快速路径

- 同样，根据访问控制规则中配置的操作，在移动规则后，日志记录配置会被设置为适当的设置，如下表中所述。

访问控制规则中的操作	在预过滤器规则中启用日志记录配置
允许	未选中任何复选框。
阻止	• 在连接开始时记录 • 事件查看器 • 系统日志服务器 • SNMP 陷阱
阻止并重置	• 在连接开始时记录 • 事件查看器 • 系统日志服务器 • SNMP 陷阱

访问控制规则中的操作	在预过滤器规则中启用日志记录配置
交互式阻止	• 在连接开始时记录 • 事件查看器 • 系统日志服务器 • SNMP 陷阱
交互式阻止并重置	• 在连接开始时记录 • 事件查看器 • 系统日志服务器 • SNMP 陷阱
信任	• 在连接开始时记录 • 在连接结束时记录 • 事件查看器 • 系统日志服务器 • SNMP 陷阱

- 从源策略移动规则时，如果其他用户修改了这些规则，您将看到一条消息。您可以在刷新页面后继续该过程。

过程

步骤 1 在访问控制策略编辑器中，选择要移动的规则。

（**旧版 UI**。） 要选择多条规则，请使用 Ctrl+点击。

（**新用户界面**。）要选择多个规则，请选中每个规则的复选框。

步骤 2 右键点击所选规则，然后选择**移动到其他策略 (Move to another policy)**（**旧版 UI**）或**移动到预过滤策略 (Move to Prefilter Policy)**（**新版 UI**）。

步骤 3 从**放置规则 (Place Rules)** 下拉列表中，选择要放置移动规则的位置：

- 要定位为最后一组规则，请选择**在底部 (At the bottom)**。
- 要定位为第一组规则，请选择**在顶部 (At the top)**。

步骤 4 点击 **移动**。

下一步做什么

- 部署配置更改。

定位访问控制规则

您可以移动访问控制策略中的现有规则，或在所需位置插入新的规则。将某条规则添加或移动到某个类别时，系统会将其置于该类别的末尾。

以下程序介绍如何在编辑规则时移动规则。您还可以执行以下操作：

- （**旧版 UI**。） 通过右键点击规则并选择**插入规则 (Insert Rule)**，在特定位置插入新规则。系统将打开“添加规则”(Add Rule) 对话框，其中包含“插入”(Insert) 菜单和指定的所选规则编号。您可以在规则下方或上方插入规则，并在必要时对规则编号进行更改。
- （**旧版 UI**。） 通过右键点击现有规则，选择**剪切 (Cut)** 或**复制到同一策略 (Copy to Same Policy)**，然后右键点击新位置并选择**粘贴到上方 (Paste Above)** 或**粘贴到下方 (Paste Below)**。复制时，请确保删除旧位置的规则，以避免存在重复的规则。
- （**新 UI**。）将鼠标悬停在现有规则之间的行上，然后点击**添加规则 (Add Rule)** 即可插入新规则。在“添加规则”(Add Rule) 对话框的**插入 (Insert)** 框中选择位置；您可以选择其他规则来调整位置。您还可以从右键点击菜单中选择**在上面添加规则 (Add Rule Above)** 或**在下面添加规则 (Add Rule below)**。
- （**新用户界面**。）通过右键点击规则，选择**复制 (Copy)**，然后右键点击新位置并选择**粘贴到上方 (Paste Above)** 或**粘贴到下方 (Paste Below)**。请确保删除旧位置的规则，以免出现重复的规则。

开始之前

查看访问控制规则的最佳实践，第 1253 页中的规则顺序指南。

过程

步骤 1 在访问控制规则编辑器中，您有以下选择：

- 如果添加的是新规则，请使用**插入 (Insert)** 下拉列表。
- （**旧版 UI**。） 如果编辑的是现有规则，请点击**移动 (Move)**。
- （**新用户界面**。）如果要编辑现有规则，请点击规则名称旁边的**移动规则 (Move Rule)** 图标。

步骤 2 选择要移动或插入规则的位置：

- 选择**插入强制性类别 (into Mandatory)** 或**插入默认类别 (into Default)**。
- 选择**插入强制性类别 (into Mandatory)**，然后选择类别。
- 选择**规则上方**或**规则下方**，然后键入相应的规则编号。在**新 UI (New UI)**，您只用选择规则，而不是键入规则编号。

步骤 3 保存规则。

步骤 4 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改。

将注释添加到访问控制规则

创建或编辑访问控制规则时，可以添加注释。例如，您可为其他用户汇总整体配置，或者当您变更规则和更改的原因时进行记录。您可以显示规则的所有注释列表，以及添加每条注释的用户以及添加注释的日期。

保存规则时，自上次保存所做的所有注释都将变为只读。

要搜索访问控制规则注释，请使用规则列表页面上的“搜索规则”(Search Rules) 栏。

过程

步骤 1 在访问控制规则编辑器中，点击**注释 (Comments)**。

步骤 2 （**旧版 UI**。） 点击**新建注释 (New Comment)**，输入注释，然后点击**确定 (OK)**。您可以在保存规则之前编辑或删除此注释。

步骤 3 （**新 UI**。）输入注释，然后点击**添加备注 (Add Comment)**。您可以在保存规则之前编辑或删除此注释。

步骤 4 保存规则。

访问控制规则的示例

以下主题提供了访问控制规则的示例。

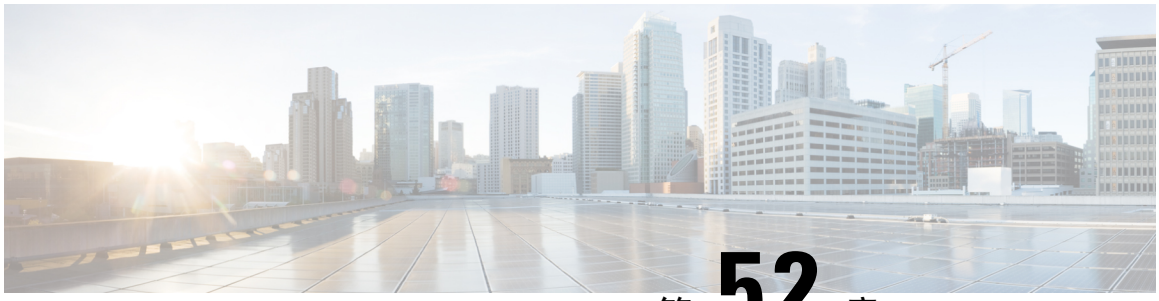
如何使用安全区域来控制访问

假设在某个部署中，您希望主机对互联网具有不受限制的访问权限，但是仍然通过检测传入流量是否存在入侵和恶意软件来保护这些主机。

首先，创建两个安全区域：内部和外部。然后，将一个或多个设备上的接口对分配到这些区域，每个对中的一个接口位于内部区域，另一个接口位于外部区域。在内侧连接至网络的主机代表您的受保护资产。

注释 您不需要将所有内部（或外部）接口分组至单个区域。选择对您的部署和安全策略有意义的分组。

然后，配置访问控制规则，其中目标区域条件设置为“内部”(Internal)。此简单规则与从内部区域中的任何接口传出设备的流量相匹配。要检查匹配流量中是否存在入侵和恶意软件，请选择规则操作**允许 (Allow)**，然后将该规则与入侵和文件策略相关联。



第 52 章

Cisco Secure Dynamic Attributes Connector

以下主题讨论如何配置和使用Cisco Secure Dynamic Attributes Connector。

关于 Cisco Secure Dynamic Attributes Connector

Cisco Secure Dynamic Attributes Connector 让您能够在 Cisco Secure Firewall Management Center (CDO) 访问控制规则中使用来自各种云服务平台的服务标签和类别。

支持的连接器

我们目前支持：

表 *95:* 按 ***Cisco Secure Dynamic Attributes Connector*** 版本和平台列出的受支持连接器列表

CSDAC 版本/平台	AWS	修饰器	GitHub	Google Cloud	Azure	Azure 服务标签	ISE	LDAP	Microsoft Office 365	VMware vCenter
版本 1.1（本地）	是	否	不支持	不支持	是	是	否	不支持	是	是
版本 2.0（本地）	是	不支持	是	是	是	是	否	不支持	是	是
云交付 (思科防御协调器)	是	不支持	是	是	是	是	否	不支持	是	否

有关连接器的详细信息：

- Amazon Web Services (AWS)

  有关更多信息，请参阅 Amazon 文档站点上的标记 AWS 资源等资源。

- GitHub
- Google Cloud

  有关详细信息，请参阅 Google 云文档中的设置环境。

- Microsoft Azure

  有关详情，请参阅 Azure 文档网站上的本页面。

- Microsoft Azure 服务器标签

  有关详细信息，请参阅 Microsoft TechNet 上的虚拟网络服务标签等资源。

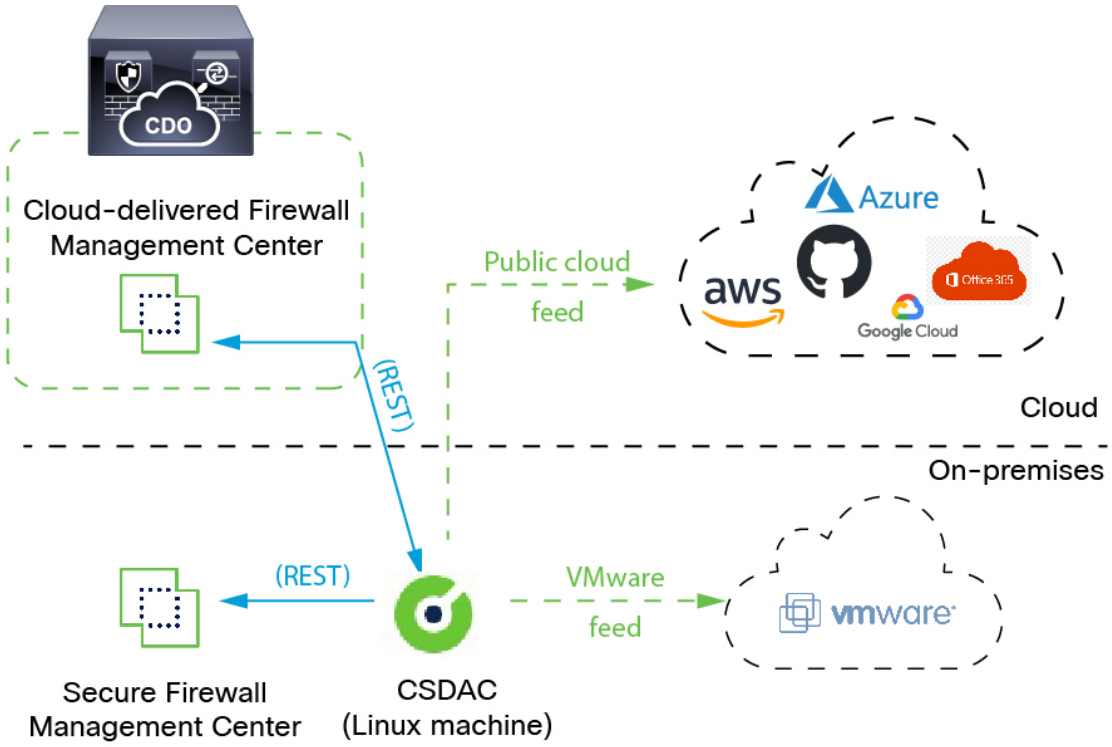
- Office 365

  有关详细信息，请参阅 docs.microsoft.com 上的 Office 365 URL 和 IP 地址范围。

工作原理

由于工作负载的动态性质和 IP 地址重叠的必然性，网络结构（例如 IP 地址）在虚拟、云和容器环境中并不可靠。客户需要根据非网络结构（例如虚拟机名称或安全组）定义策略规则，以便即使 IP 地址或 VLAN 发生更改，防火墙策略也能保持不变。

下图显示了系统的总体运行情况。



1. 连接器包含要查询的标签和容器。

   例如，这些标签通常会定义动态分配的网络和 IP 地址，您无法为其创建访问控制规则。来自连接器的持续源存储在 dynamic attributes connector 上，以便快速访问。

2. 标签信息会保留在您创建动态属性过滤器的 dynamic attributes connector 上，这些过滤器会定义哪些信息必须用于访问控制规则中。

   例如，如果 AWS 为记帐和财务部门虚拟机定义网络，则可以创建仅指定财务网络的动态属性过滤器。

3. dynamic attributes connector 定义的适配器会将这些动态属性过滤器作为动态对象接收，并允许您将它们用于访问控制规则中。

   您可以创建以下类型的适配器：

   - 本地设备的 本地防火墙管理中心。

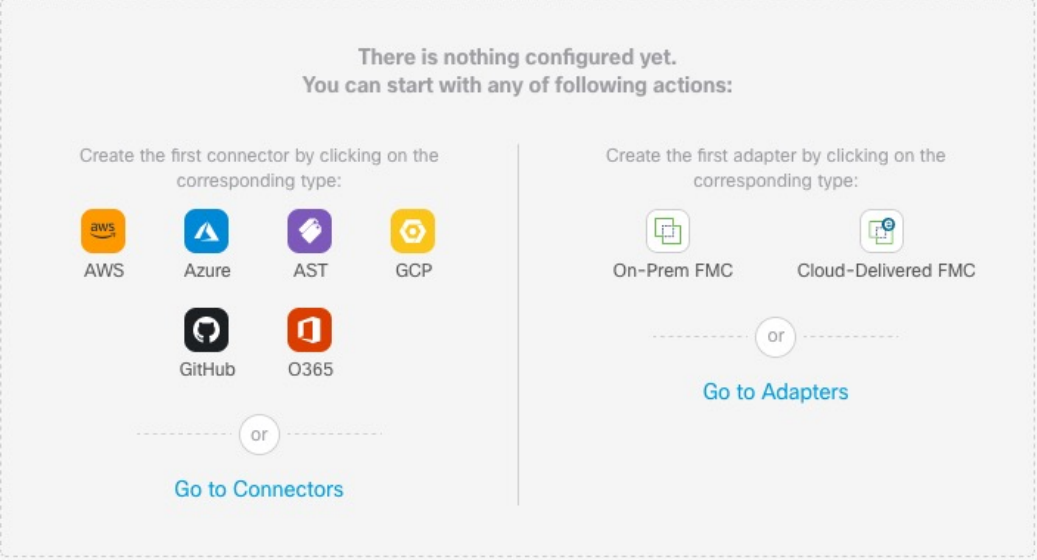
     此类 设备可能由 思科防御协调器 (CDO) 管理，或者它也可能是独立设备。

   - 云交付的防火墙管理中心 适用于 CDO 管理的设备。

关于控制面板

要访问 Cisco Secure Dynamic Attributes Connector 控制面板，请登录 CDO 并点击页面顶部的 **工具和服务 (Tools & Services)** > **动态属性连接 (Dynamic Attributes Connector)** > **控制面板 (Dashboard)**。

Cisco Secure Dynamic Attributes Connector 控制面板页面会显示连接器、适配器和过滤器的状态。以下是未配置系统的控制面板示例：



您可以通过控制面板来执行的操作包括：

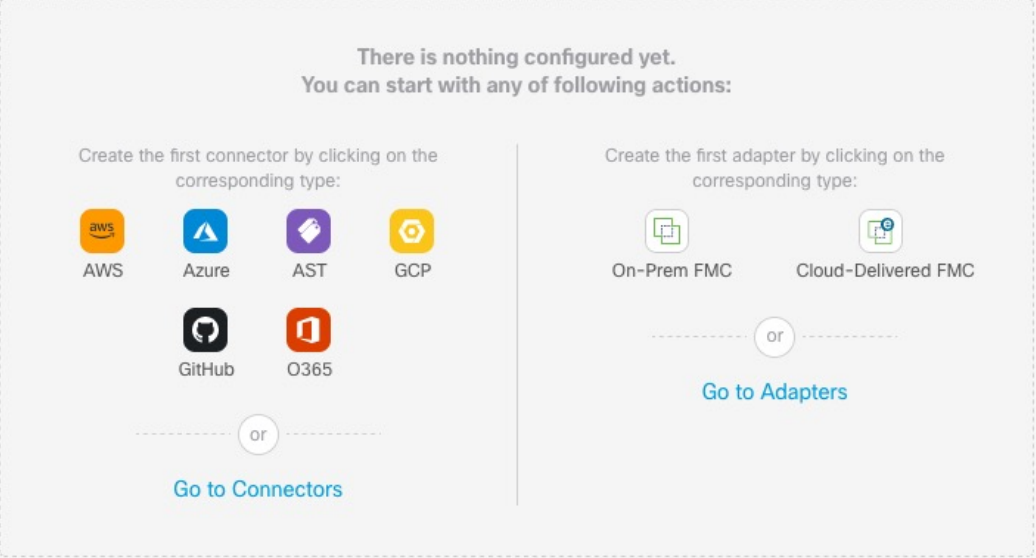
- 添加、编辑和删除连接器、动态属性过滤器和适配器。
- 了解连接器、动态属性过滤器和适配器之间的关系。
- 查看警告和错误。

相关主题

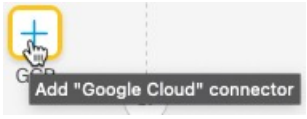
- 未配置系统的控制面板， 第 1308 页
- 已配置系统的控制面板， 第 1309 页
- 添加、编辑或删除连接器， 第 1311 页
- 添加、编辑或删除动态属性过滤器， 第 1312 页
- 添加、编辑或删除适配器， 第 1314 页

未配置系统的控制面板

未配置系统的 Cisco Secure Dynamic Attributes Connector 控制面板页面示例：



控制面板最初显示您可以为系统配置的所有类型的连接器和适配器。您可以执行以下任何操作：

- 将鼠标指针悬停在连接器或适配器上，然后点击 

新建一个。
- 点击**转到连接器 (Go to Connectors)** 以添加、编辑或删除连接器（适用于同时创建、编辑或删除多个连接器）。

  有关详细信息，请参阅创建连接器，第 1315 页。
- 点击**转到适配器 (Go to Adapters)** 以添加、编辑或删除适配器（适用于同时创建、编辑或删除多个适配器）。

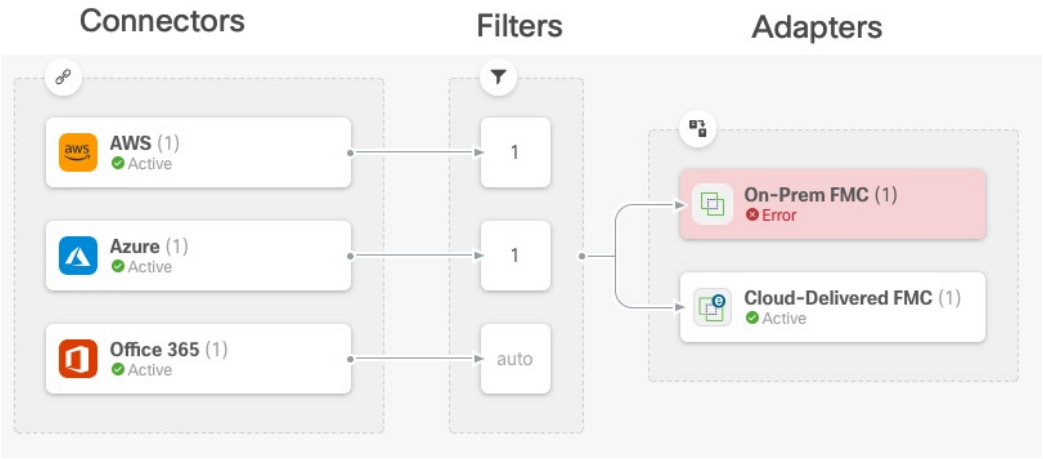
  有关详细信息，请参阅创建适配器，第 1327 页。

相关主题

- 已配置系统的控制面板，第 1309 页
- 添加、编辑或删除连接器，第 1311 页
- 添加、编辑或删除动态属性过滤器，第 1312 页
- 添加、编辑或删除适配器，第 1314 页

已配置系统的控制面板

已配置系统的 Cisco Secure Dynamic Attributes Connector 控制面板页面示例：



控制面板显示以下内容（从左到右）：

“连接器”(Connectors) 列	“过滤器”(Filters) 列	“适配器”(Adapters) 列
连接器列表，其中包含指示每种类型的配置数量的编号。连接器会收集可以发送到已配置适配器的动态属性。动态属性过滤器会指定要发送的数据。 点击 以查看有关所有已配置连接器的详细信息。您还可以点击连接器的名称来添加、编辑或删除连接器；或者查看有关它们的详细信息。有关详细信息，请参阅添加、编辑或删除连接器，第 1311 页。	与每个连接器关联的动态属性过滤器列表，其中带有一个数字，表示每个过滤器与连接器关联的数量。 点击 以查看有关所有已配置过滤器的详细信息。您还可以点击过滤器的名称来添加、编辑或删除过滤器；或者查看有关它们的详细信息。有关详细信息，请参阅添加、编辑或删除动态属性过滤器，第 1312 页。	适配器列表。适配器会使用已配置的动态属性过滤器从已配置的连接器接收动态对象；这些动态对象可用于访问控制策略，而无需部署它们。 点击 以查看有关所有已配置适配器的详细信息。您还可以点击适配器的名称来添加、编辑或删除适配器；或者查看有关它们的详细信息。有关详细信息，请参阅添加、编辑或删除适配器，第 1314 页。

注释 某些连接器（例如 Outlook 365 和 Azure 服务标记）会自动提取可用的动态对象，而无需使用动态属性过滤器。这些连接器在 列中显示为**自动 (Auto)**。

控制面板会指明对象是否可用。控制面板页面会每 15 秒刷新一次，但您可以随时点击页面顶部的**刷新**（ ）来立即刷新。如果问题仍然存在，请检查网络连接。

相关主题

- 添加、编辑或删除连接器，第 1311 页
- 添加、编辑或删除动态属性过滤器，第 1312 页
- 添加、编辑或删除适配器，第 1314 页

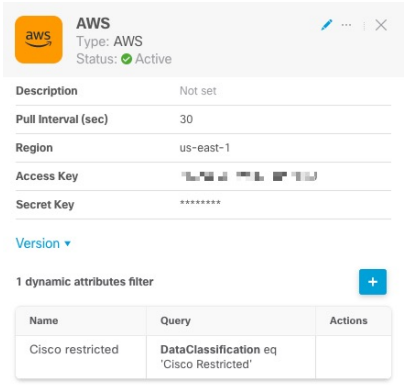
添加、编辑或删除连接器

通过控制面板，您可以查看或编辑连接器。您可以点击连接器的名称以查看该连接器的所有实例，

也可以点击 以查看以下其他选项：

- **转到连接器**可同时查看所有连接器；您可以在此处添加、编辑和删除连接器。
- **添加连接器 (Add Connector)** > **类型**以添加指定类型的连接器。

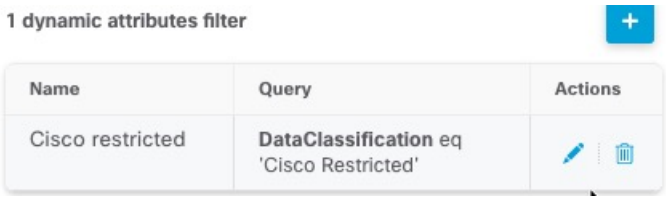
点击连接器列 ( ) 中的任意连接器可显示更多相关信息；示例如下：



您有以下选择：

- 点击 编辑图标 （ ） 以编辑此连接器。
- 点击 更多图标 （ ） 以查看其他选项。
- 点击 关闭面板。
- 点击**版本 (Version)** 以显示 dynamic attributes connector 的版本。如果思科 TAC 需要，您可以选择将版本复制到剪贴板。

通过面板底部的表格，您可以添加动态属性过滤器；或编辑或删除连接器。示例如下：



点击添加图标（ ）以便为此连接器添加动态属性过滤器。有关详细信息，请参阅创建动态属性过滤器，第 1329 页。

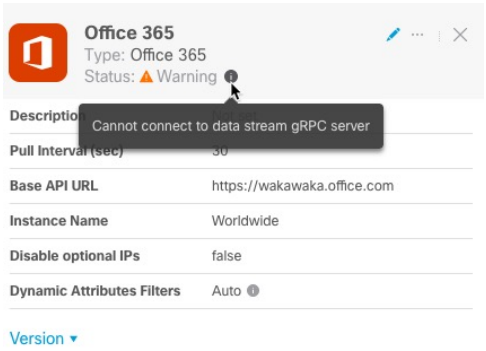
将鼠标指针悬停在“操作”(Actions) 列上，以编辑或删除指示的连接器。

查看错误信息

要查看连接器的错误信息，请执行以下操作：

1. 在控制面板上，点击显示错误的连接器的名称。
2. 在右侧窗格中，点击 **信息** （ ）。

   示例如下。



3. 要解决此问题，请按照创建 Office 365 连接器， 第 1326 页中所述编辑连接器设置。
4. 如果您无法解决问题，请点击**版本 (Version)** 并将版本复制到文本文件。
5. 获取 CDO 租户 ID，如中所述 获取租户 ID， 第 1334 页
6. 向思科 TAC 提供所有这些信息。https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

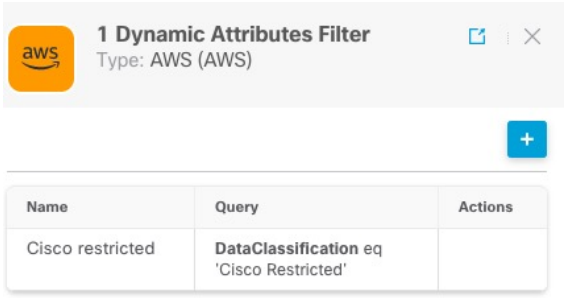
添加、编辑或删除动态属性过滤器

控制面板让您能够添加、编辑或删除动态属性过滤器。您可以点击过滤器的名称以查看该过滤器的所有实例，也可以点击 以查看下列附加选项：

- **转至动态属性过滤器**以查看所有已配置的动态属性过滤器。您可以在此处添加、编辑或删除动态属性过滤器。
- **添加动态属性过滤器**以添加过滤器。

有关添加动态属性过滤器的详细信息，请参阅创建动态属性过滤器， 第 1329 页。

点击过滤器列 ( ) 中的任何适配器以显示有关它的详细信息；如下所示：



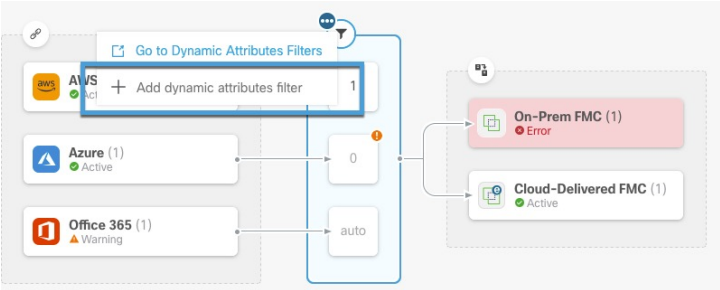
注释 某些连接器（例如 Outlook 365 和 Azure 服务标记）会自动提取可用的动态对象，而无需使用动态属性过滤器。这些连接器在 列中显示为**自动 (Auto)**。

您有以下选择：

- 点击过滤器实例可查看与连接器关联的动态属性过滤器的摘要信息。
- 点击 添加图标 （ ） 以添加新的动态属性过滤器。

  有关详细信息，请参阅创建动态属性过滤器，第 1329 页。
- 在表示指明的连接器没有关联的动态属性过滤器的过滤器列 ( ) 中点击 。如果没有关联的过滤器，连接器将无法向 管理中心 发送任何内容。

  解决此问题的一种方法是点击过滤器列中的 ，然后点击**添加动态属性过滤器 (Add Dynamic Attributes Filter)**。示例如下。



- 点击 以添加、编辑或删除过滤器。
- 点击 关闭面板。

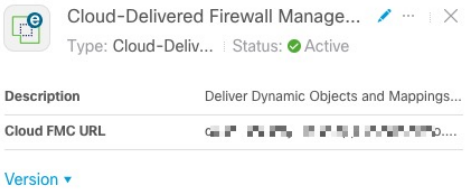
添加、编辑或删除适配器

通过控制面板，您可以查看或编辑适配器。您可以点击适配器的名称以查看该适配器的所有实例，

也可以点击 以查看以下其他选项：

- **转到适配器**以同时查看所有适配器；您可以在此处添加、编辑和删除适配器。
- **添加适配器 (Add Adapter)** > **类型**以添加指定类型的适配器。

点击适配器列 ( ) 中的任何适配器以显示有关它的详细信息；如下所示：



您有以下选择：

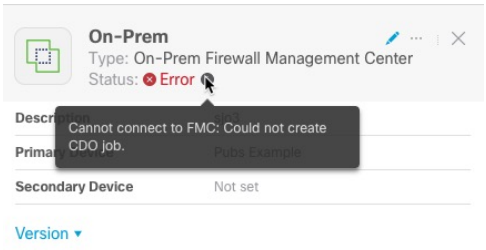
- 点击 编辑图标 （ ） 以编辑此连接器。
- 点击 更多图标 （ ） 以查看其他选项。
- 点击**版本 (Version)** 以显示 dynamic attributes connector 的版本。如果思科 TAC 需要，您可以选择将版本复制到剪贴板。
- 点击 以添加、编辑或删除适配器。您还可以在生成的页面上查看错误详细信息。
- 点击 关闭面板。

查看错误信息

要查看适配器的错误信息，请执行以下操作：

1. 在控制面板上，点击显示了错误的适配器的名称。
2. 在右侧窗格中，点击 **信息** （ ）。

   示例如下。



3. 要解决此错误，请确保 本地防火墙管理中心 已正确载入。有关详细信息，请参阅使用思科防御协调器管理 *FMC* 中的载入 FMC（主题链接）。
4. 如果您无法解决问题，请点击**版本 (Version)** 并将版本复制到文本文件。
5. 获取 CDO 租户 ID，如中所述 获取租户 ID，第 1334 页
6. 向思科 TAC 提供所有这些信息。https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

相关主题

- 创建适配器，第 1327 页

创建连接器

连接器是云服务的接口。连接器从云服务检索网络信息，以便网络信息可用于CDO上的访问控制策略。

我们支持以下内容：

表 *96:* 按 *Cisco Secure Dynamic Attributes Connector* 版本和平台列出的受支持连接器列表

CSDAC 版本/平台	AWS	修饰器	GitHub	Google Cloud	Azure	Azure 服务标签	ISE	LDAP	Microsoft Office 365	VMware vCenter
版本 1.1（本地）	是	否	不支持	不支持	是	是	否	不支持	是	是
版本 2.0（本地）	是	不支持	是	是	是	是	否	不支持	是	是
云交付 (思科防御协调器)	是	不支持	是	是	是	是	否	不支持	是	否

有关详细信息，请参阅以下各节之一：

Amazon Web 服务连接器 - 关于用户权限和导入的数据

Cisco Secure Dynamic Attributes Connector 会将动态属性从 AWS 导入 CDO，以便用于访问控制策略。

动态属性已导入

我们从 AWS 导入以下动态属性：

- 标签，可用于组织 AWS EC2 资源的用户定义的键值对。

  有关更多信息，请参阅 AWS 文档中的标记 EC2 资源

- AWS 中虚拟机的 *IP* 地址。

所需的最低权限

Cisco Secure Dynamic Attributes Connector 要求用户至少具有允许 `ec2:DescribeTags` 和 `ec2:DescribeInstances` 以便能够导入动态属性的策略。

创建对 Cisco Secure Dynamic Attributes Connector 具有最小权限的 AWS 用户

此任务讨论如何设置具有最低权限的服务帐户，以向 CDO 发送动态属性。有关这些属性的列表，请参阅 Amazon Web 服务连接器 - 关于用户权限和导入的数据，第 1315 页。

开始之前

您必须已设置 Amazon Web 服务 (AWS) 帐户。有关执行此操作的更多信息，请参阅 AWS 文档中的此文章。

过程

步骤 1 以具有网络管理员角色的用户身份登录 AWS 控制台。

步骤 2 在控制面板中，点击**安全、身份和合规性 (Security, Identity & Compliance)** > **IAM**。

步骤 3 点击**访问管理 (Access Management)** > **用户 (Users)**。

步骤 4 点击**添加用户 (Add Users)**。

步骤 5 在**用户名 (User Name)** 字段中，输入用于标识用户的名称。

步骤 6 点击**访问密钥 - 编程访问 (Access Key - Programmatic Access)**。

步骤 7 在“设置权限”(Set permissions) 页面中，点击**下一步 (Next)** 而不授予用户任何访问权限；稍后执行此操作。

步骤 8 如果需要，向用户添加标签。

步骤 9 点击**创建用户**。

步骤 10 点击 **Download.csv**，将用户的密钥下载到计算机。

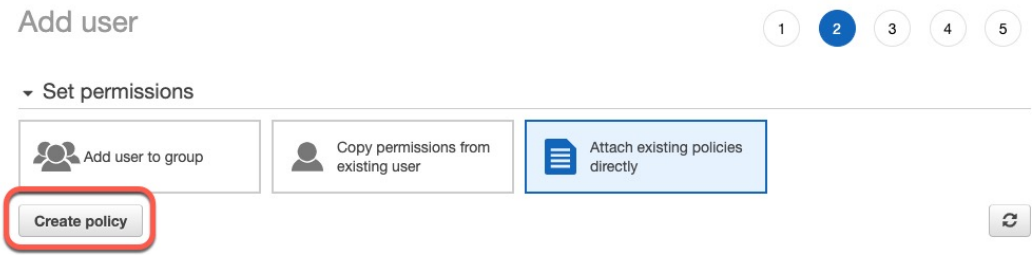
注释 这是您检索用户密钥的唯一机会。

步骤 11 点击**关闭 (Close)**。

步骤 12 在身份和访问管理 (IAM) 页面的左侧列中，点击**访问管理 (Access Management)** > **策略 (Policies)**。

步骤 13 点击**创建策略**。

步骤 14 在“创建策略”(Create Policy) 页面中，点击 **JSON**。



步骤 15 在字段中输入以下策略：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeTags",
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

步骤 16 点击**下一步 (Next)**。

步骤 17 点击**审核 (Review)**。

步骤 18 在“查看策略”(Review Policy) 页面中输入请求的信息，然后点击**创建策略 (Create Policy)**。

步骤 19 在“策略”(Policies) 页面上，在搜索字段中输入全部或部分策略名称，然后按 Enter 键。

步骤 20 点击您刚刚创建的策略。

步骤 21 点击**操作 (Actions)** > **附加 (Attach)**。

步骤 22 如有必要，请在搜索字段中输入全部或部分用户名，然后按 Enter 键。

步骤 23 点击**附加策略 (Attach Policy)**。

下一步做什么

创建 AWS 连接器，第 1317 页。

创建 AWS 连接器

此任务讨论如何配置将数据从 AWS 发送到 CDO 以用于访问控制策略的连接器。

开始之前

创建至少具有创建对 Cisco Secure Dynamic Attributes Connector 具有最小权限的 AWS 用户，第 1316 页中所述权限的用户。

过程

步骤 1 登录CDO。

步骤 2 请点击 **工具和服务 (Tools & Services)** > **动态属性连接器 (Dynamic Attributes Connector)** > **连接器 (Connectors)**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （ ），然后点击连接器名称。
- 编辑连接器：点击编辑图标 （ Edit ）。
- 编辑连接器：点击删除图标 （ Delete ）。

步骤 4 输入以下信息。

值	说明
Name	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 AWS 检索 IP 映射的间隔。
地区	（必需。）输入您的 AWS 区域代码。
访问密钥	（必需。）输入访问密钥。
加密密钥	（必需。）输入加密密钥。

步骤 5 点击**测试 (Test)** 并确保测试成功后再保存连接器。

步骤 6 点击**保存 (Save)**。

步骤 7 确保“状态”(Status) 列中显示**确定 (OK)**。

Azure 连接器 - 关于用户权限和导入的数据

Cisco Secure Dynamic Attributes Connector 会将动态属性从 Azure 导入 CDO，以便用于访问控制策略。

动态属性已导入

我们从 Azure 导入以下动态属性：

- 标签，与资源、资源组和订用关联的键值对。

有关详情，请参阅 Microsoft 文档中的本页面。

- Azure 中虚拟机的 *IP* 地址。

所需的最低权限

Cisco Secure Dynamic Attributes Connector 要求至少具有**读者 (Reader)** 权限的用户才能导入动态属性。

创建对 Cisco Secure Dynamic Attributes Connector 具有最小权限的 Azure 用户

此任务讨论如何设置具有最低权限的服务帐户，以向 CDO 发送动态属性。有关这些属性的列表，请参阅 Azure 连接器 - 关于用户权限和导入的数据， 第 1318 页。

开始之前

您必须已经拥有 Microsoft Azure 帐户。要进行设置，请参阅 Azure 文档站点上的本页面。

过程

步骤 1 以订用所有者的身份登录到 Azure 门户。

步骤 2 点击 **Azure Active Directory**。

步骤 3 查找要设置的应用的 Azure Active Directory 实例。

步骤 4 点击**添加 (Add)** > **应用注册 (App registration)**。

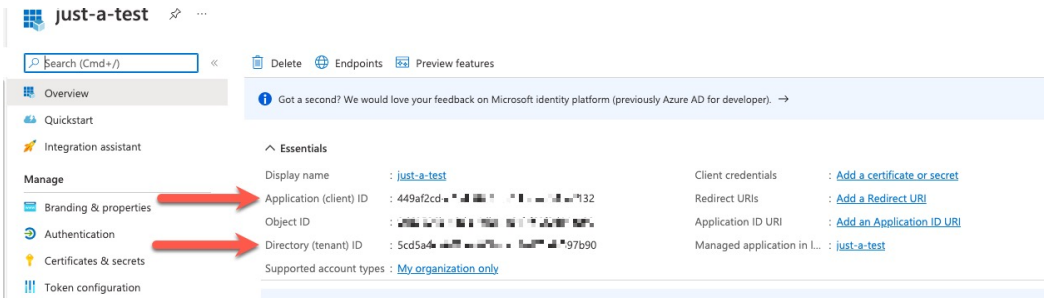
步骤 5 在 **名称 (Name)** 字段中，输入用于标识此应用的名称。

步骤 6 在此页面上输入贵组织所要求的其他信息。

步骤 7 点击**注册 (Register)**。

步骤 8 在下一页上，记录下客户端 ID（也称为应用 *ID*）和租户 ID（也称为目录 *ID*）。

示例如下。



步骤 9 点击**添加证书或密钥 (Add a certificate or secret)**。

步骤 10 点击**新建客户端密钥 (New Client Secret)**。

步骤 11 输入请求的信息，然后点击**添加 (Add)**。

步骤 12 将客户端**值**复制到剪贴板，因为您需要它来设置 Azure 连接器。

步骤 13 返回到 Azure 门户主页面，然后点击**订用 (Subscriptions)**。

步骤 14 将订用 ID 复制到剪贴板。

步骤 15 在订用页面上，点击订用的名称。

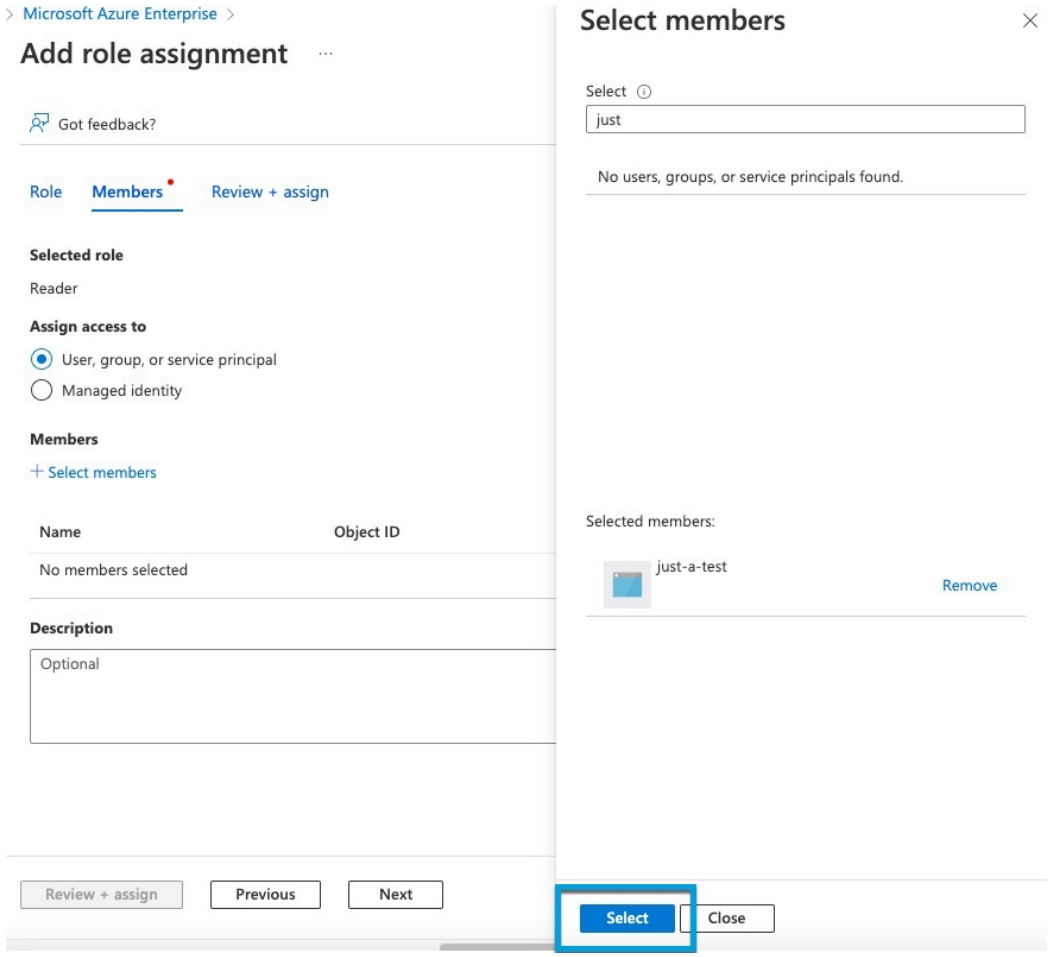
步骤 16 点击**访问控制 (IAM) (Access Control [IAM])**。

步骤 17 点击**添加 (Add)** > **添加角色分配 (Add role assignment)**。

步骤 18 点击**读者 (Reader)**，然后点击**下一步 (Next)**。

步骤 19 点击**选择成员 (Select Members)**。

步骤 20 在页面右侧，点击您注册的应用的名称，然后点击**选择 (Select)**。



步骤 21 点击**查看 + 分配 (Review + Assign)**，然后按照提示完成操作。

下一步做什么

请参阅创建 Azure 连接器，第 1321 页。

创建 Azure 连接器

此任务讨论如何创建从 Azure 向 CDO 发送数据的连接器，以用于访问控制策略中。

开始之前

创建至少具有 创建对 Cisco Secure Dynamic Attributes Connector 具有最小权限的 Azure 用户，第 1319 页 中所述权限的 Azure 用户。

过程

步骤 1 登录CDO。

步骤 2 请点击 **工具和服务 (Tools & Services)** > **动态属性连接器 (Dynamic Attributes Connector)** > **连接器 (Connectors)**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （  ），然后点击连接器名称。
- 编辑连接器：点击编辑图标 （  ）。
- 编辑连接器：点击删除图标 （  ）。

步骤 4 输入以下信息。

值	说明
Name	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 Azure 检索 IP 映射的间隔。
订用 ID	（必需。）输入 Azure 订用 ID。
租户 ID	（必需。）输入租户 ID。
客户端 ID	（必需。）输入您的客户端 ID。
客户端密钥	（必需。）输入您的客户端密钥。

步骤 5 点击**测试 (Test)** 并确保在保存连接器之前显示 **Test connection succeeded**。

步骤 6 点击**保存 (Save)**。

步骤 7 确保“状态”(Status) 列中显示**确定 (OK)**。

创建 Azure 服务标签连接器

本主题讨论了如何为 Azure 服务标签创建到 CDO 的连接器，以供在访问控制策略中使用。Microsoft 会每周更新与这些标记的 IP 地址关联。

有关详细信息，请参阅 Microsoft TechNet 上的虚拟网络服务标签。

过程

步骤 1 登录CDO。

步骤 2 请点击 **工具和服务 (Tools & Services)** > **动态属性连接器 (Dynamic Attributes Connector)** > **连接器 (Connectors)**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （ ），然后点击连接器名称。
- 编辑连接器：点击编辑图标 （ Edit ）。
- 编辑连接器：点击删除图标 （ Delete ）。

步骤 4 输入以下信息。

值	说明
Name	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 Azure 检索 IP 映射的间隔。
订用 ID	（必需。）输入 Azure 订用 ID。
租户 ID	（必需。）输入租户 ID。
客户端 ID	（必需。）输入您的客户端 ID。
客户端密钥	（必需。）输入您的客户端密钥。

步骤 5 点击**测试 (Test)** 并确保在保存连接器之前显示 **Test connection succeeded**。

步骤 6 点击**保存 (Save)**。

步骤 7 确保“状态”(Status) 列中显示**确定 (OK)**。

创建 GitHub 连接器

此部分讨论如何创建将数据发送到 CDO 以用于访问控制策略的 GitHub 连接器。与这些标签关联的 IP 地址由 GitHub 进行维护。您不必创建动态属性过滤器。

有关详细信息，请参阅关于 GitHub 的 IP 地址。

注释 请勿更改 URL，否则将无法检索任何 IP 地址。

过程

步骤 1 登录CDO。

步骤 2 请点击 **工具和服务 (Tools & Services)** > **动态属性连接器 (Dynamic Attributes Connector)** > **连接器 (Connectors)**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （ ），然后点击连接器名称。
- 编辑连接器：点击编辑图标 （ Edit ）。
- 编辑连接器：点击删除图标 （ Delete ）。

步骤 4 输入**名称**和可选说明。

步骤 5 （可选。）在**提取间隔 (Pull Interval)** 字段中，更改动态属性连接器从 GitHub 检索 IP 地址的频率（以秒为单位）。默认值为 21,600 秒（6 小时）。

步骤 6 点击**测试 (Test)** 并确保测试成功后再保存连接器。

步骤 7 点击**保存 (Save)**。

步骤 8 确保“状态”(Status) 列中显示**确定 (OK)**。

Google 云连接器 - 关于用户权限和导入的数据

Cisco Secure Dynamic Attributes Connector 会将动态属性从 Google 云导入 CDO，以便用于访问控制策略。

动态属性已导入

我们会从 Google 云导入以下动态属性：

- 标签，可用于组织 Google 云资源的键值对。

  有关详细信息，请参阅 Google 云文档中的创建和管理标签。

- 网络标记，与组织、文件夹或项目关联的键值对。

有关详细信息，请参阅 Google 云文档中的创建和管理标签。

- Google 云中虚拟机的 *IP* 地址。

所需的最低权限

Cisco Secure Dynamic Attributes Connector 要求至少具有**基本** > **查看者**权限的用户才能导入动态属性。

创建对 Cisco Secure Dynamic Attributes Connector 具有最小权限的 Google 云用户

此任务讨论如何设置具有最低权限的服务帐户，以向 CDO 发送动态属性。有关这些属性的列表，请参阅 Google 云连接器 - 关于用户权限和导入的数据，第 1323 页。

开始之前

您必须已设置 Google 云帐户。有关执行此操作的详细信息，请参阅 Google 云文档中的设置环境。

过程

步骤 1 以所有者角色的用户身份登录您的 Google 云帐户。

步骤 2 点击**IAM 和管理 (IAM & Admin)** > **服务帐户 (Service Accounts)** > **创建服务帐户 (Create Service Account)**。

步骤 3 输入以下信息：

- **服务帐户名称**：用于标识此帐户的名称；例如，**CSDAC**。
- **服务帐户 ID**：应在您输入服务帐户名称后填写唯一值。
- **服务帐户说明**：输入可选说明。

有关服务帐户的详细信息，请参阅 Google 云文档中的了解服务帐户。

步骤 4 点击**创建并继续 (Create and Continue)**。

步骤 5 按照屏幕上的提示操作，直到显示“授予用户对此服务帐户的访问权限”部分。

步骤 6 授予用户**基本** > **查看者**角色。

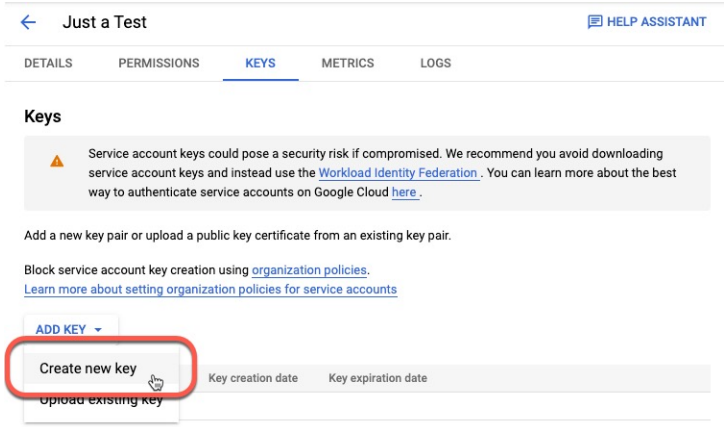
步骤 7 点击**完成 (Done)**。

系统将显示服务帐户列表。

步骤 8 点击您所创建的服务帐户一行末尾的 **更多**（⋮）。

步骤 9 点击**管理密钥 (Manage Keys)**。

步骤 10 点击**添加密钥 (Add Key)** > **创建新密钥 (Create New Key)**。



步骤 11 点击 **JSON**。

步骤 12 点击**创建 (Create)**。

JSON 密钥将下载到您的计算机。

步骤 13 配置 GCP 连接器时，请将密钥放在手边。

下一步做什么

请参阅创建 Google 云连接器，第 1325 页。

创建 Google 云连接器

开始之前

准备好 Google 云 JSON 格式的服务帐户数据；它是设置连接器所必需的。

过程

步骤 1 登录CDO。

步骤 2 请点击 **工具和服务 (Tools & Services)** > **动态属性连接器 (Dynamic Attributes Connector)** > **连接器 (Connectors)**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （ ），然后点击连接器名称。
- 编辑连接器：点击编辑图标 （ Edit ）。
- 编辑连接器：点击删除图标 （ Delete ）。

步骤 4 输入以下信息。

值	说明
Name	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 AWS 检索 IP 映射的间隔。
GCP 区域	（必需。）输入您的 Google 云所在的 GCP 区域。有关详细信息，请参阅 Google 云文档中的区域和地区。
服务帐户	粘贴 Google 云服务帐户的 JSON 代码。

步骤 5 点击**测试 (Test)** 并确保测试成功后再保存连接器。

步骤 6 点击**保存 (Save)**。

步骤 7 确保“状态”(Status) 列中显示**确定 (OK)**。

创建 Office 365 连接器

此任务讨论如何为 Office 365 标记创建连接器，从而将数据发送到 CDO 以便用于访问控制策略。Microsoft 会每周更新与这些标记的 IP 地址关联。您不必创建动态属性过滤器即可使用数据。

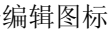
有关详细信息，请参阅 docs.microsoft.com 上的 Office 365 URL 和 IP 地址范围。

过程

步骤 1 登录CDO。

步骤 2 请点击 **工具和服务 (Tools & Services)** > **动态属性连接器 (Dynamic Attributes Connector)** > **连接器 (Connectors)**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （  ），然后点击连接器名称。
- 编辑连接器：点击编辑图标 （  ）。
- 编辑连接器：点击删除图标 （  ）。

步骤 4 输入以下信息。

值	说明
Name	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。

值	说明
提取间隔	（默认为 30 秒。）从 Azure 检索 IP 映射的间隔。
基本 API URL	（必需。）输入要从中检索 Office 365 信息的 URL（如果其与默认值不同）。有关详细信息，请参阅 Microsoft 文档站点上的 Office 365 IP 地址和 URL Web 服务。
实例名称	（必需。）从列表中，点击实例名称。有关详细信息，请参阅 Microsoft 文档站点上的 Office 365 IP 地址和 URL Web 服务。
禁用可选 IP	（必需。）输入 **true** 或 **false**。

步骤 5 点击**保存 (Save)**。

步骤 6 确保“状态”(Status) 列中显示**确定 (OK)**。

创建适配器

适配器 是与 CDO 的安全连接，您可以将来自云对象的网络信息推送到此以用于访问控制策略。

您可以创建以下适配器：

- 本地防火墙管理中心 适用于现场 管理中心 设备。
- 云交付的防火墙管理中心 适用于 CDO 管理的设备。

注释 您必须具有**超级管理员**用户角色才能创建第一个 云交付的防火墙管理中心 适配器。要查看或修改现有适配器，您必须拥有管理员或超级管理员用户角色。

如何创建 本地防火墙管理中心 适配器

本主题讨论了如何创建适配器，以便将动态对象从 dynamic attributes connector 推送 CDO 到。

开始之前

按照使用思科防御协调器来管理安全和网络设备联机帮助中的载入管理中心中所述，将防火墙管理器载入思科防御协调器。

所需的用户角色：

- 超级管理员

过程

步骤 1 登录 CDO。

步骤 2 请点击 工具和服务 > 动态属性连接器 > 适配器。

步骤 3 要添加适配器，请点击 添加图标 （+） > 本地防火墙管理中心。

步骤 4 要编辑或删除适配器，请点击编辑图标 （Edit） 或 删除图标 （Delete ）。

步骤 5 添加或编辑以下信息。

值	说明
Name	（必需。）输入可标识适配器的唯一名称。
说明	适配器的可选说明。
主设备	在列表中点击与您的租户关联的管理中心的 IP 地址。
辅助设备	（可选。）如果您有辅助 本地防火墙管理中心，请在列表中点击其名称。

步骤 6 点击确定 **(OK)**。

如何创建 云交付的防火墙管理中心 适配器

本主题讨论了如何创建适配器，以便将动态对象从 dynamic attributes connector 推送 CDO 到。

开始之前

所需的用户角色：

- 超级管理员

过程

步骤 1 以具有超级管理员角色的用户身份登录 CDO。

步骤 2 请点击 工具和服务 > 动态属性连接器 > 适配器。

步骤 3 要添加适配器，请点击 添加图标 （+） > 云交付的防火墙管理中心。

步骤 4 要编辑或删除适配器，请点击编辑图标 （Edit） 或 删除图标 （Delete ）。

步骤 5 编辑以下信息。

值	说明
Name	（必需。）输入可标识适配器的唯一名称。

值	说明
说明	适配器的可选说明。
云 FMC URL	从列表中，点击您的 云交付的防火墙管理中心 的URL。

步骤 6 点击**测试 (Test)** 并确保测试成功后再保存适配器。

步骤 7 点击**保存 (Save)**。

创建动态属性过滤器

使用 Cisco 安全动态属性连接器定义的动态属性过滤器会在 CDO 中显示为可在访问控制策略中使用的动态对象。例如，您可以将财务部门对 AWS 服务器的访问权限限制为 Microsoft Active Directory 中定义的财务组成员。

注释 您不能为 GitHub、Office 365 或 Azure Service Tags 创建动态属性过滤器。这些类型的云对象会提供自己的 IP 地址。

有关访问控制规则的详细信息，请参阅使用动态属性过滤器来创建访问控制规则，第 1332 页。

开始之前

完成以下所有任务：

- 创建连接器，第 1315 页

过程

步骤 1 登录CDO。

步骤 2 请点击 **工具和服务 (Tools & Services)** > **动态属性连接器 (Dynamic Attributes Connector)** > **动态属性过滤器 (Dynamic Attributes Filters)**。

步骤 3 执行以下任一操作：

- 添加新过滤器：点击添加图标 （ ）
- 编辑过滤器：点击编辑图标 （ Edit ）
- 删除过滤器：点击删除图标 （ Delete ）

步骤 4 输入以下信息。

项目	说明
名称	用于在访问控制策略和 CDO 对象管理器（**外部属性** > **动态对象**）中标识动态过滤器（作为动态对象）的唯一名称。
连接器	在列表中点击要使用的连接器的名称。
查询	• 添加新过滤器：点击添加图标 （） • 编辑过滤器：点击编辑图标 （Edit ） • 删除过滤器：点击删除图标 （Delete ）

步骤 5 要添加或编辑查询，请输入以下信息。

项目	说明
密钥	点击列表中的一个键。密钥会从连接器获取。
操作	点击以下选项之一： • **等于 (Equals)** 会将密钥与值完全匹配。 • **包含 (Contains)** 会将键与值匹配（如果值的任何部分匹配）。
值	点击**任意 (Any)** 或**全部 (All)**，然后点击列表中的一个或多个值。点击**添加其他值 (Add another value)** 以便向查询中添加值。

步骤 6 点击**显示预览 (Show Preview)** 以便显示查询返回的网络或 IP 地址的列表。

步骤 7 完成后，点击**保存 (Save)**。

步骤 8 （可选。）验证 CDO 中的动态对象。

a) 登录 CDO。

b) 请点击 **策略 (策略)** > **FTD 策略 (FTD Policies)**。

c) 点击**对象 (Objects)** > **对象管理器 (Object Manager)**。

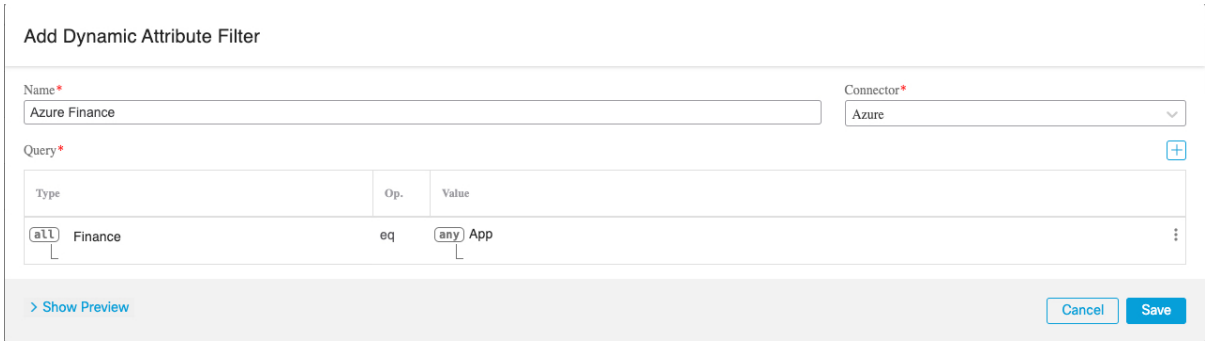
d) 在左侧窗格中，点击**外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**。
您创建的动态属性查询应显示为动态对象。

动态属性过滤器示例

本主题提供了设置动态属性过滤器的一些示例。

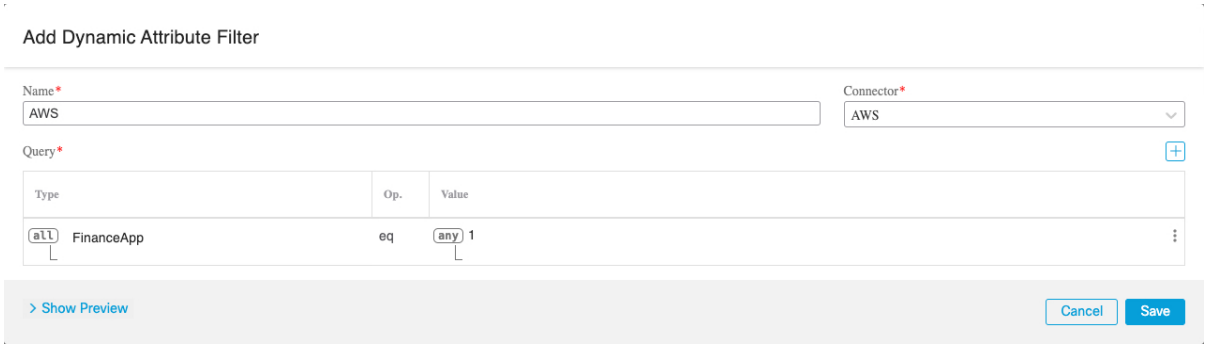
示例：Azure

以下示例显示了一个条件：标记为财务应用的服务器。



示例：AWS

以下示例显示了一个条件：值为 1 的 FinanceApp。



在访问控制策略中使用动态对象

通过 dynamic attributes connector，您可以在访问控制规则中配置动态过滤器（在 CDO 中可视为动态对象）。

关于访问控制规则中的动态对象

在连接器上保存动态属性过滤器后，动态对象会自动从 dynamic attributes connector 推送到定义的 本地防火墙管理中心 或 云交付的防火墙管理中心 适配器。

您可以在访问控制规则的“动态属性”(Dynamic Attributes) 选项卡页面上使用这些动态对象，这类似于使用安全组标记 (SGT) 的方式。您可以将动态对象添加为源或目标属性；例如，在访问控制阻止规则中，您可以将财务动态对象添加为目标属性，以阻止通过匹配规则中其他条件的对象访问财务服务器。

注释 您不能为 GitHub、Office 365 或 Azure Service Tags 创建动态属性过滤器。这些类型的云对象会提供自己的 IP 地址。

使用动态属性过滤器来创建访问控制规则

本主题讨论如何使用动态对象（这些动态对象以您之前创建的动态属性过滤器来命名）创建访问控制规则。

开始之前

创建动态属性过滤器，如创建动态属性过滤器，第 1329 页中所述。

注释 您不能为 GitHub、Office 365 或 Azure Service Tags 创建动态属性过滤器。这些类型的云对象会提供自己的 IP 地址。

过程

步骤 1 登录CDO。

步骤 2 请点击 **策略 (策略)** > **FTD 策略 (FTD Policies)**。

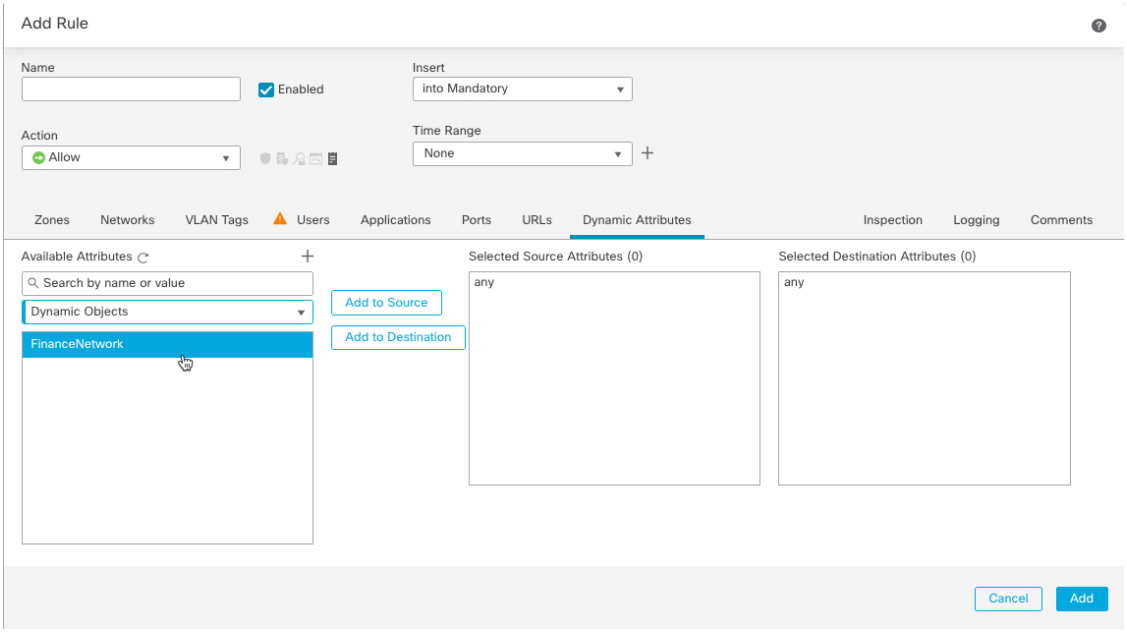
步骤 3 点击访问控制策略旁边的 **编辑**（ ）。

步骤 4 点击**添加规则 (Add Rule)**。

步骤 5 点击**动态属性 (Dynamic Attributes)** 选项卡。

步骤 6 在“可用属性”(Available Attributes) 部分中，点击列表中的**动态对象 (Dynamic Objects)**。

下图显示了一个示例。



前面的示例显示了一个名为 `FinanceNetwork` 的动态对象，该对象对应于 Dynamic Attributes Connector 中创建的动态属性过滤器。

步骤 7 将所需对象添加到源或目标属性。

步骤 8 如果需要，向规则中添加其他条件。

下一步做什么

《思科安全防火墙管理中心设备配置指南》中的“访问控制”一章（章节链接）

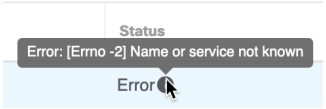
Dynamic Attributes Connector 故障排除

如何对 dynamic attributes connector 进行问题故障排除，包括使用提供的工具。

错误消息故障排除

问题：名称或服务未知错误

当您将鼠标悬停在适配器或连接器的错误条件上时，此错误将显示为工具提示。示例如下；实际可能看起来有所不同。

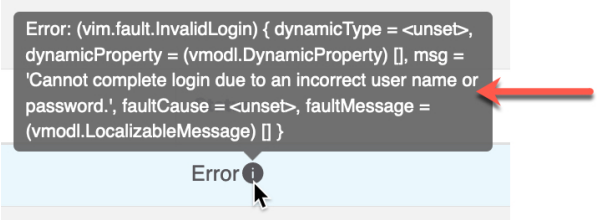


解决方案：编辑连接器或适配器，然后检查：

- 主机名末尾的斜杠
- 验证密码是否正确

问题：用户名或密码不正确

当您将鼠标悬停在连接器的错误条件上时，此错误将显示为工具提示。



解决方案：编辑连接器并更改用户名或密码。

获取租户 ID

如果您需要有关 Cisco Secure Dynamic Attributes Connector 的帮助，则必须向思科 TAC 提供您的租户 ID，这样我们才能查看您的日志。

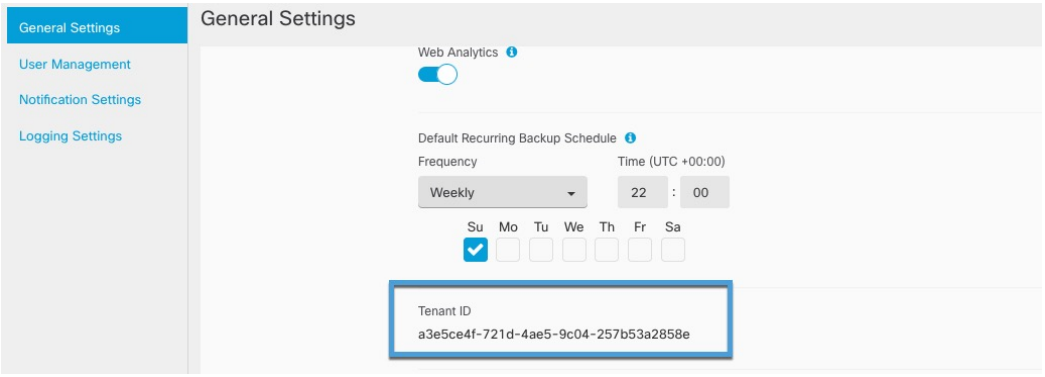
过程

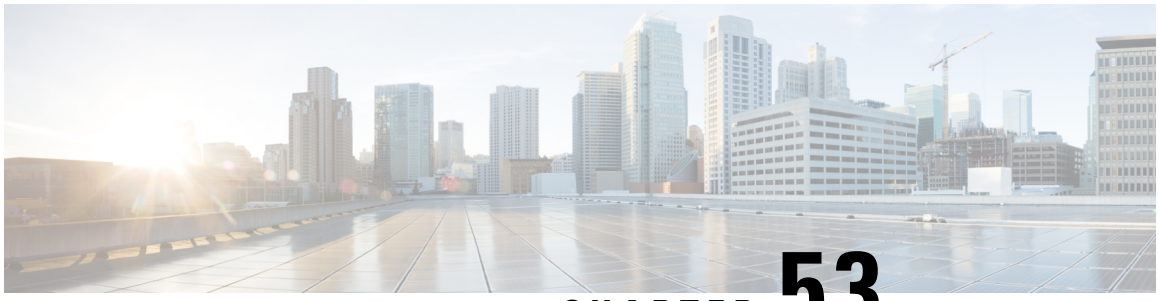
步骤 1 登录CDO。

步骤 2 请点击 **设置 (Settings)** > **常规设置 (General Settings)**。

步骤 3 将您的租户 ID 复制到剪贴板以提供给思科 TAC。

示例如下。





CHAPTER 53

URL 过滤

您可以使用访问控制规则实施 URL 过滤。

URL 过滤概述

使用 URL 过滤功能控制网络上的用户可以访问的网站：

- 基于类别和信誉的 URL 过滤 - 使用 URL 过滤许可证，您可以根据 URL 的一般分类（类别）和风险级别（信誉）控制对网站的访问。这是建议选项。
- 手动 URL 过滤 - 通过任意许可证，可以手动指定单个 URL、URL 组以及 URL 列表和源，以实现对网络流量的精细、自定义控制。有关详细信息，请参阅手动 URL 过滤， 第 1348 页。

另请参阅安全情报， 第 1359 页，用于阻止恶意 URL、域和 IP 地址的类似但不同的功能。

关于使用类别和信誉进行 URL 过滤

通过 URL 过滤许可证，您可以基于所请求 URL 的类别和信誉控制对网站的访问：

- 类别 - URL 的一般分类。例如，ebay.com 属于“拍卖”类别，而 monster.com 属于“职位搜索”类别。

URL 可以属于多个类别。

- 信誉 - URL 被用于可能违反组织安全策略之目的的可能性。信誉的范围从未知风险（第 0 级）或不可信（第 1 级）到信任（第 5 级）。

基于类别和信誉的 URL 过滤的优势

URL 类别和信誉可帮助您快速配置 URL 过滤。例如，您可以使用访问控制来阻止黑客攻击 类别中的不可信 的 URL。 或者，您可以使用 QoS 对来自视频流类别中站点的流量进行速率限制。。也存在基于威胁类型的类别，例如间谍软件和广告软件类别。

使用类别和信誉数据可简化策略创建和管理。此方法可保证系统按预期控制网络流量。由于思科会不断更新有关新 URL 的威胁情报以及现有 URL 的新类别和新风险的信息，因此系统会使用最新信息来过滤所请求的 URL。代表安全威胁的站点或提供不良内容的站点出现和消失的速度可能比您更新和部署新策略的速度要快。

以下是一些系统如何适应的示例：

- 如果某个访问控制规则阻止所有游戏网站，在新域注册并分类为“游戏”时，系统则可以自动阻止这些站点。 同样，如果 QoS 规则对所有视频流站点进行速率限制，则系统可自动限制流向新视频流站点的流量。
- 如果某个访问控制规则阻止所有恶意软件站点，而某个购物页面受到恶意软件感染，系统可以将来自该购物站点的 URL 重新分类为恶意软件站点，并阻止该站点。
- 如果访问控制规则阻止不可信社交网站，但有人在其个人资料页面发布的链接中提供有指向恶意负载的链接，则系统便可以将该页面的信誉从可靠更改为不可信，并阻止该网站。

SSL 策略 “不解密”规则中基于类别的过滤的限制

您可以选择在SSL 策略中包含类别。这些类别也称为 *URL* 过滤，由思科 Talos 智能组更新。更新基于机器学习和人工分析，这些内容可从网站目的地检索，有时也可从其托管和注册信息检索。分类不基于所声明的公司行业、意图或安全性。

注释 不要将 URL 过滤与应用检测混淆，后者依赖于从网站读取数据包来更具体地确定其内容（例如，Facebook Message 或 Salesforce）。有关详细信息，请参阅配置应用控制的最佳实践 ， 第 1250 页。

有关详细信息，请参阅在 URL 过滤中使用类别 ， 第 1341 页。

URL 类别和信誉说明

类别说明

可从https://www.talosintelligence.com/categories中获取每个 URL 类别的说明。

要查看那些类别，请确保点击 **威胁类别** 。

信誉级别说明

转至 https://talosintelligence.com/reputation_center/support 并查看“常见问题”部分。

来自思科云的 URL 过滤数据

添加URL过滤许可证将自动启用启用URL过滤。允许根据网站的一般分类（类别）和风险级别（信誉）来进行流量处理。

添加URL过滤许可证将自动启用启用URL过滤。允许根据网站的一般分类（类别）和风险级别（信誉）来进行流量处理。

当您启用（或重新启用）URL 过滤时， 管理中心 会向思科查询 URL 数据并将数据集推送到托管设备。默认情况下，此数据集的自动更新处于启用状态；我们强烈建议您不要禁用这些更新。

当用户浏览 Web 时，系统使用本地数据集获取类别和信誉信息。当用户浏览到类别和信誉不在本地数据集或之前访问过的网站缓存中的URL时，默认情况下，系统会将其提交到云端进行威胁智能评估，并将结果添加到缓存中。（您可以禁用此云查找；请参阅URL 过滤选项，第 1344 页。）

URL 类别集可能会定期更改。当您收到更改通知时，请检查您的 URL 过滤配置，以确保按预期处理流量。有关详细信息，请参阅如果 URL 类别集发生更改，请执行操作，第 1355 页。

URL 过滤的最佳实践

请记住以下的 URL 过滤的准则和限制：

按照类别和信誉过滤

请按照如何使用类别和信誉配置 URL 过滤，第 1342 页中的相关说明来操作。

配置策略以检查在可以识别 URL 之前必须通过的数据包

在满足以下情况之前，系统无法过滤 URL：

- 客户端与服务器之间建立受监控连接。
- 系统识别会话中的 DNS，HTTP 或 HTTPS 应用。
- 系统识别所请求的域或URL（对于加密会话，从一个非加密的域名、ClientHello消息或服务器证书中获取）。

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

重要提示！要确保您的系统检查否则会通过的这些初始数据包，请参阅在识别流量之前检查通过的数据包，第 2042 页和子主题。

如果早期流量与所有其他规则条件都匹配，但是识别未完成，则系统允许数据包通过并建立连接（或完成 TLS/SSL 握手）。在系统完成其识别后，系统会将相应的规则操作应用于剩余会话流量。

阻止威胁类别

请确保您的策略专门处理威胁类别，以识别已知的恶意站点。除了阻止信誉不佳的站点之外，请执行此操作。

例如，要保护网络免受恶意站点的攻击，必须阻止所有威胁类别。此外，Talos 建议您仅阻止类别为“差”(Poor) 的站点。如果您具有积极的安全状态，可以阻止可疑的信誉，但这可能会导致更多的误报。

有关详细信息，请参阅 URL 类别和信誉说明，第 1336 页中的 URL中的 **威胁类别** 。

URL 条件和规则顺序

- 将 URL 规则置于 必须 命中的所有其他规则之后。
- URL 可以属于多个类别。可以允许一个类别的网站并阻止另一个类别的网站，无论是明确地还是依赖于默认操作。在这种情况下，请确保创建 URL 规则并对其进行排序，从而获得预期效果，具体取决于允许还是阻止应优先。

有关规则的其他指南，请参阅以下主题：访问控制规则的最佳实践，第 1253 页。

未分类或无信誉的 URL

在构建 URL 规则时，首先应选择要匹配的类别。如果您明确选择 **未分类** URL，但不能通过信誉进一步限制。

具有“不受信任”信誉的未分类URL由 **恶意站点** 类别处理。如果要阻止具有任何其他信誉级别的未分类站点（例如“可疑”），则必须阻止所有未分类的站点。

选择类别和信誉级别后，可以选择 **应用到未知信誉**。例如，您可以创建应用于信誉不受信任，可疑和未知的站点的规则。

不能为 URL 手动分配类别和信誉，但在访问控制和 QoS 策略中，可以手动阻止特定 URL。请参阅手动 URL 过滤，第 1348 页。另请参阅争议 URL 类别和信誉，第 1354 页。

针对已加密 Web 网络流量的 URL 过滤

在对加密的 Web 网络流量执行 URL 过滤时，系统将：

- （如果已启用DNS过滤）检查系统之前是否已发现源域或该域在本地信誉数据库中，如果是，则根据域的信誉和类别执行操作。否则，即使已在访问控制策略的高级设置中启用 **重试URL缓存缺失查找** ，系统也会根据您的加密流量配置处理流量。
- 不考虑加密协议；如果规则包含URL条件，但不包含指定协议的应用条件，该规则将同时匹配 HTTPS 和 HTTP 流量。
- 不使用 URL 列表。您必须改用 URL 对象和组。
- 根据用于加密流量的公钥证书中的使用者公用名匹配HTTPS流量，并评估事务期间随时提供的任何其他 URL（包括解密后的 HTTP URL）的信誉。
- 不考虑对象公用名内的子域。

- 不显示被访问控制规则（或任何其他配置）阻止的已加密连接的 HTTP 响应页面；请参阅对 HTTP 响应页面的限制，第 1350 页。

URL 过滤和 TLS 服务器身份发现

RFC 8446定义的最新版本的传输层安全（TLS）协议 1.3 是许多 Web 服务器提供安全通信的首选协议。由于 TLS 1.3 协议会加密服务器的证书以提高安全性，并且需要使用证书来匹配访问控制规则中的应用和 URL 过滤条件，因此 Firepower 系统提供了一种提取服务器证书而 不 解密整个数据包的方法。

访问控制策略高级设置为 TLS 服务器身份发现提供 **早期应用检测和 URL 分类** 选项。

我们强烈建议您为要根据应用或URL条件匹配的任何流量启用此功能，尤其是在您想要对该流量执行深度检查时。SSL 策略 不需要 SSL 策略，因为在提取服务器证书的过程中不会解密流量。

注释

- 由于证书是解密的，因此 TLS 服务器身份发现会降低性能，具体取决于硬件平台。
- 内联分路模式或被动模式部署不支持 TLS 服务器身份发现。
- 任何部署到 AWS 的 Cisco Secure Firewall Threat Defense Virtual 都不支持启用 TLS 服务器身份发现。如果您有任何由Cisco Secure Firewall Management Center管理的此类托管设备，则每次设备尝试提取服务器证书时，连接事件 **PROBE_FLOW_DROP_BYPASS_PROXY** 都会增加。

有关详细信息，请参阅访问控制策略高级设置，第 1271 页。

HTPP/2

系统可从 TLS 证书提取 HTTP/2 URL，但无法从负载进行提取。

手动 URL 过滤

- 使用自定义安全情报列表或源对象指定 URL。请勿使用 URL 对象或直接在规则中输入 URL。有关详细信息，请参阅手动 URL 过滤选项，第 1348 页。
- 如果使用 URL 对象手动过滤特定 URL 或通过直接在规则中输入 URL，请仔细考虑可能会受到影响的其他流量。要确定网络流量是否与URL条件相匹配，系统执行简单的子字符串匹配。如果请求的 URL 与字符串的任何部分匹配，则认为该 URL 匹配。
- 如果使用手动URL过滤创建其他规则的例外情况，请将具有例外情况的特定规则置于本应适用的一般规则之上。

在 URL 中搜索查询参数

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

高可用性部署中的 URL 过滤

有关使用高可用性中的 Firepower 管理中心进行 URL 过滤的指南，请参阅 《Cisco Secure Firewall Management Center 管理指南》 中的 *URL* 过滤和安全情报。

所选设备型号的内存限制

- 内存较少的设备型号在本地存储较少的URL数据，因此系统可能会更频繁地检查云，以确定不在本地数据库中的站点的类别和信誉。

  内存较低的设备包括：

  - Firepower 1010
  - Threat Defense Virtual 配备 8 GB RAM

威胁防御中恢复 TLS 会话的 URL 匹配

在以下条件下使用与 Snort 2 的 URL 匹配：

- 如果没有 TLS 会话恢复且已启用 SSL 策略，或者客户端 Hello 消息包含服务器名称指示 (SNI) 扩展名。
- 如果存在 TLS 会话恢复且未启用 SSL 策略，或者客户端 Hello 消息不包含 SNI 扩展。

过滤 HTTPS 流量

要过滤加密流量，系统将根据 TLS/SSL 握手期间传递的信息确定请求的URL：用于加密流量的公钥证书中的使用者公用名。

HTTPS 过滤与 HTTP 过滤不同，它不考虑使用者公用名称内的子域。在访问控制或 QoS 策略中手动过滤 HTTPS URL 时，不包括子域信息。例如，使用 example.com 而不是 www.example.com。

提示 在SSL 策略中，可以通过定义可分辨名称SSL策略规则条件来处理和解密发送到特定URL的流量。证书的使用者可分辨名称中的公用名属性包含站点的 URL。通过解密 HTTPS 流量，访问控制规则可以评估解密的会话，从而改进 URL 过滤。

按加密协议控制流量

系统在访问控制或 QoS 策略中执行 URL 过滤时，不考虑加密协议（HTTP 与 HTTPS）。对于手动 URL 条件和基于信誉的 URL 条件均会发生此情况。换句话说，URL 过滤以相同方式处理发送到以下网站的流量：

- http://example.com/
- https://example.com/

要配置仅与HTTP或HTTPS流量匹配的规则，请向该规则添加应用条件。例如，可以通过构造两个访问控制规则（每个规则具有应用和URL条件）来允许对某个站点进行HTTP访问，同时禁止HTTP访问。

第一个规则允许 HTTPS 流量到达网站：

操作：允许
应用：HTTPS
URL：example.com

第二个规则阻止对同一网站进行 HTTP 访问：

操作：阻止
应用：HTTP
URL：example.com

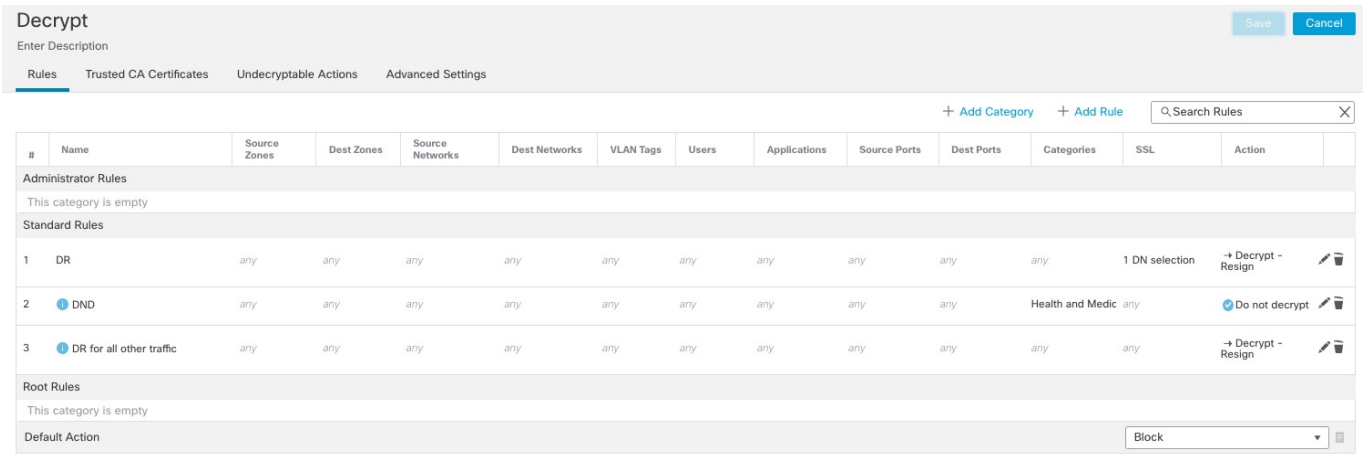
在 URL 过滤中使用类别

“不解密”规则中的类别限制

您可以选择在 SSL 策略中包含类别。这些类别也称为 *URL* 过滤，由思科 Talos 智能组更新。更新基于机器学习和人工分析，这些内容可从网站目的地检索，有时也可从其托管和注册信息检索。分类不基于所声明的公司行业、意图或安全性。虽然我们努力不断更新和改进URL过滤类别，但这并不是一门精确的科学。有些网站根本没有分类，有些网站可能分类不当。

避免在不解密规则中过度使用类别，以避免无故解密流量；例如，“健康和医学”类别包括不会威胁到患者隐私的 WebMD 网站。

以下是一个解密策略示例，它可以阻止解密“健康”和“医学”类别的网站，但允许解密 WebMD 和其他所有内容。有关解密规则的一般信息，请参阅使用 TLS/SSL 解密的准则，第 1732 页。



注释 不要将 URL 过滤与应用检测混淆，后者依赖于从网站读取数据包来更具体地确定其内容（例如，Facebook Message 或 Salesforce）。有关详细信息，请参阅配置应用控制的最佳实践，第 1250 页。

URL 过滤的许可证要求

威胁防御 许可证

- 类别和信誉过滤 - URL 过滤
- 手动过滤 - 无其他许可证。

经典许可证

- 类别和信誉过滤 - URL 过滤
- 手动过滤 - 无其他许可证。

威胁防御设备的 URL 过滤许可证

请参阅《Cisco Secure Firewall Management Center 管理指南》许可证一章中的 *URL* 许可证。

URL 过滤的要求和必备条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

如何使用类别和信誉配置 URL 过滤

	相应操作	更多信息
第 1 步	确保拥有正确的许可证。	将 URL 过滤许可证分配给将过滤 URL 的每个托管设备。

	相应操作	更多信息
第 2 步	确保 Firepower 管理中心可以与云通信以获取 URL 过滤数据。	《Cisco Secure Firewall Management Center 管理指南》中的互联网接入要求 和 通信端口要求 。
第 3 步	了解限制和准则并采取任何必要的措施。	URL 过滤的最佳实践， 第 1337 页
第 4 步	启用 URL 过滤功能。	使用类别和信誉启用 URL 过滤， 第 1343 页
第 5 步	配置规则以按类别和信誉过滤 URL。	配置 URL 条件， 第 1345 页 为了最好地防御恶意站点，您必须按信誉阻止站点，并阻止所有威胁类别中的 URL。 （选件）补充或选择性覆盖基于类别和信誉的 URL 过滤， 第 1349 页
第 6 步	（可选）允许用户能够通过点击忽略警告页面来绕过对网站的阻止。	HTTP 响应页面和交互式阻止
步骤 7	对规则进行排序，使流量首先命中关键规则。	URL 规则顺序， 第 1257 页
第 8 步	（可选）修改与URL过滤相关的高级选项。	通常，除非您有特定的原因需要更改默认值，否则请使用默认值。 有关高级选项的信息，包括以下内容，请参阅访问控制策略高级设置， 第 1271 页。 • **要在连接事件中存储的最大 URL 字符数** • **允许交互式阻止绕过阻止的时长（秒）** • **重试 URL 缓存缺失查询** • **对 DNS 流量启用信誉实施**
步骤 9	部署更改。	部署配置更改， 第 136 页
步骤 10	确保系统按预期接收未来的URL数据更新	配置 URL 过滤运行状况监控器， 第 1354 页
步骤 11	确保您已启用其他功能来保护网络免受恶意站点的攻击	请参阅安全情报， 第 1359 页。

使用类别和信誉启用 URL 过滤

您必须是管理员用户才能执行此任务。

开始之前

按照 如何使用类别和信誉配置 URL 过滤，第 1342 页中所述，完成所有前提条件。

过程

步骤 1 选择**集成** > **其他集成**。

步骤 2 请点击 **云服务**。

步骤 3 配置 URL 过滤选项，第 1344 页。

步骤 4 点击**保存 (Save)**。

URL 过滤选项

添加URL过滤许可证将自动启用启用URL过滤。允许根据网站的一般分类（类别）和风险级别（信誉）来进行流量处理。

当您启用（或重新启用）URL 过滤时， 管理中心 会自动向思科查询 URL 数据并将数据集推送到托管设备。此过程可能需要一些时间。

如果您使用 SSL 规则处理已加密的流量，则另请参阅TLS/SSL 规则 准则和限制，第 1731 页。

启用自动更新

如果**启用自动更新**（默认），则 管理中心 每 30 分钟会检查一次云以获取更新。如果需要严格控制系统联系外部资源的时间，可以禁用自动更新，改为使用调度程序创建定期任务。请参阅在 《Cisco Secure Firewall Management Center 管理指南》中 使用已安排任务自动执行 *URL* 过滤更新 。

立刻更新

点击**立即更新 (Update Now)** 以执行一次性的按需 URL 数据更新。如果有更新正在进行，则不能启动按需更新。虽然每日更新通常是小量更新，但如果距离上一次更新超过五天，新的URL数据最多可能需要 20 分钟才能下载完，具体情况视带宽而定。然后，执行更新也可能最多需要 30 分钟。

向思科云查询未知 URL

当用户浏览的网站的类别和信誉不在本地数据集中时，允许系统将URL提交至云以进行威胁情报评估。默认情况下，此选项已启用。如果不想提交未分类 URL（例如，出于隐私原因），请禁用此选项。但请注意，与未分类 URL 的连接 不会 与使用基于类别或信誉的 URL 条件的规则进行匹配。在这种情况下，您将无法手动对该 URL 指定类别或信誉。

已缓存的 URL 到期

缓存类别和信誉数据使Web浏览速度更快。默认情况下，URL 的缓存数据永不过期，以获得最快的性能。

要尽量减少与过时数据匹配的 URL 实例，可以将缓存中的 URL 设置为过期。要获得更高的威胁数据准确性和通用性，请选择较短的到期时间。经过指定的时间之后，系统将在网络上的用户第一次

访问缓存的 URL 后刷新缓存的 URL。第一个用户看不到刷新的结果，但访问此 URL 的下一个用户将会看到刷新的结果。

配置 URL 条件

通过根据 URL 类别和信誉控制对站点的访问来保护您的网络。

过程

步骤 1 在规则编辑器中，点击 URL 条件的以下：

- 访问控制或 QoS-点击 **URLs**。在新的访问控制 UI 中，从“目标和应用”列中选择此选项。
- SSL-点击 **类别**。

步骤 2 查找并选择要控制的 URL 类别：

在访问控制 或 QoS 规则中，点击 **类别**。

要有效保护网络免受恶意站点的攻击，必须阻止所有威胁类别 URL。此外，Talos 建议您仅阻止类别为“差”(Poor) 的站点。如果您具有积极的安全状态，可以阻止可疑的信誉，但这可能会导致更多的误报。有关威胁类别列表，请参阅 URL 类别和信誉说明，第 1336 页。

请务必点击列表底部的箭头以查看所有可用类别。

步骤 3 （可选）通过选择**信誉 (Reputation)** 来限制 URL 类别。

请注意，如果您明确匹配**未分类**URL，但不能通过信誉进一步限制。选择信誉级别也会将比您选择的级别更高或更低的其他信誉包括在内，具体取决于规则操作：

- 如果规则允许或信任网络流量，则包括级别更低的信誉。例如，如果您将访问控制规则配置为允许良性（4 级），系统还会自动允许受信任（5 级）站点。
- 如果规则对网络流量进行速率限制、解密、阻止或监控，则包括级别更高的信誉。例如，如果将访问控制规则配置为阻止可疑站点（2 级），则系统还会阻止不受信任（1 级）站点。

如果更改规则操作，则系统会自动更改 URL 条件中的信誉级别。

或者，选择 **应用到未知信誉**。

步骤 4 点击 **添加到规则**，或进行拖放操作。在新的访问控制 UI 中，点击 **添加 URL**。

步骤 5 （可选）要在访问控制或 QoS 规则中选择预定义的 URL 对象或 URL 列表和源，请点击 **URL**，选择对象，然后将其添加到目标。

这些对象实施手动 URL 过滤，而不是基于类别的过滤。

步骤 6 保存或继续编辑规则。

示例：访问控制规则中的 URL 条件

下图显示用于阻止以下内容的访问控制规则的 URL 条件：所有具有中性或更差的信誉级别的恶意软件站点、所有不受信任站点以及所有社交站点。

下表总结如何构建该条件。

受阻 URL	类别	信誉
恶意软件站点，无论信誉如何	恶意软件网站	任意
任何不受信任的 URL（1 级）	任意	1 - 不受信任
具有声誉等级为中性或更差 （1 至 3 级）的社交站点	社交网络	3 - 中性

具有 URL 条件的规则

下表列出了支持 URL 条件的规则，以及每个规则类型支持的过滤类型。

规则类型	是否支持类别和信誉过滤？	支持手动过滤？
访问控制	是	是
SSL 策略	是	否；使用可分辨名称条件
QoS	是	是

要在具有**不解密**规则条件的 an SSL 策略 策略中使用 URL 过滤，请参阅在 URL 过滤中使用类别，第 1341 页。

URL 规则顺序

为了实现最有效的 URL 匹配，请将包括 URL 条件的规则放在其他规则前面，如果 URL 规则是组织规则，并且其他规则同时满足以下两个条件，则尤其应该如此：

- 它们包括应用条件。
- 将对要检查的流量进行加密。

如果为规则配置例外，请将例外置于另一条规则之上。

DNS 过滤：在 DNS 查找期间识别 URL 信誉和类别

默认情况下，在每个新访问控制策略的 **高级** 选项卡上启用 **启用对 DNS 流量的信誉实施** 选项。 此选项会轻微修改 URL 过滤行为，并且仅在启用和配置 URL 过滤时适用。

当此选项启用：

- 当浏览器查找域名以获取 IP 地址时，系统会在 URL 事务中尽早评估域类别和信誉
- 加密流量的类别和信誉通常无需解密即可确定

  如果 DNS 过滤无法确定加密流量的 URL，则使用您的加密流量配置处理该流量。

启用 DNS 过滤以在域查找期间识别 URL

默认情况下，在新的访问控制策略中启用DNS过滤。但是，可能需要其他配置才能使此设置生效。

开始之前

- 必须许可、启用和配置使用类别和信誉的 URL 过滤。

  （DNS 过滤不使用 URL 选项卡中的以下设置：URL 组、URL 对象、URL 列表和源，以及输入到“输入 URL”文本框中的 URL。）
- 请参阅 DNS 过滤限制， 第 1347 页中的限制。

过程

步骤 1 在访问控制策略的高级设置中，选择 **对 DNS 流量启用信誉实施**。

步骤 2 在同一策略中，对于配置了 URL 类别和信誉阻止的每个访问控制规则：

- 应用条件 - 如果应用条件不是**任何**（或为空），则将 **DNS** 添加到该列表。其他与 DNS 相关的选项与此目的无关。
- 端口条件 - 如果端口/协议条件不是**任何**（或为空），请添加 **DNS_over_TCP** 和 **DNS_over_UDP**。

步骤 3 保存更改。

下一步做什么

如果您已完成更改：部署配置更改， 第 136 页

DNS 过滤限制

匹配具有**阻止并重置**、**交互式阻止**或**交互式阻止并重置**操作的规则的流量将被视为规则操作为**阻止**。

尝试访问阻止的URL的最终用户会遇到无法解释的无法连接到其页面的情况；连接将旋转，然后超时。

DNS 过滤和事件

由 DNS 过滤生成的连接事件使用以下特别需要关注的字段记录：DNS 查询、URL 类别、URL 信誉和目标端口。DNS 查询字段包含域名；对于 DNS 过滤匹配，URL 字段将为空。目的端口将是 53。

另外：

- 当访问控制规则操作为**允许**或**信任**时，将为同一流量生成两个连接事件，一个用于 DNS 过滤（填充 **DNS 查询 (DNS Query)** 字段），另一个用于 URL 过滤（填充 **URL** 字段）。
- 系统第一次遇到特定 URL 时，您将看到该单个会话的两个事件：一个事件显示 DNS 查询未分类/无信誉，一个事件显示 URL 的实际类别和信誉，这些是在 DNS 期间检索到的使用标准 URL 过滤进行处理时，将查询 和 应用于会话。

手动 URL 过滤

在访问控制和 QoS 规则中，您可以通过手动过滤单个 URL、URL 组 或 URL 列表和源，补充或选择性地覆盖基于类别和信誉的 URL 过滤。

例如，您可使用访问控制阻止不适合您的组织的网站类别。但是，如果该类别包含合适的网站，并且您要为其提供访问权限，则您可以为该站点创建手动的“允许”(Allow) 规则，然后将其置于该类别的“阻止”(Block) 规则之前。

您可以在没有特殊许可证的情况下执行此类 URL 过滤。

SSL 规则不支持手动 URL 过滤；相反，使用可分辨名称条件。

⚠

注意 根据您实施手动 URL 过滤的方式，URL 匹配可能不是您想要的。请参阅手动 URL 过滤选项，第 1348 页。

手动 URL 过滤选项

有几种方法可以指定用于手动 URL 过滤的 URL：

选项	说明
（**最佳实践**） 使用自定义安全情报 URL 列表或源对象。	这是推荐的手动 URL 过滤方法。 您可以创建新列表或源，也可以在访问控制或 QoS 规则中选择现有列表或源。 有关信息，请参阅 自定义安全情报列表和源，第 1031 页 和子主题。

选项	说明
单独或作为组使用 URL 对象。有关 URL 对象的说明，请参阅 URL，第 1041 页。 或 将 URL 直接输入到访问控制规则中。（Web 界面中规则页面上的 **输入URL** 选项。）	如果不包含路径（即 URL 中无 / 字符），则匹配仅基于服务器主机名。如果主机名位于 :// 分隔符之后，或在主机名中的任何点之后，则认为该主机名匹配。例如，ign.com 匹配 ign.com 和 www.ign.com，但不匹配 verisign.com。 如果包含一个或多个 / 字符，则整个 URL 字符串将用于子字符串匹配，其中包括服务器名称、路径和任何查询参数。但是，我们建议您不要使用手动 URL 过滤阻止或允许个别网页或部分网站，因为这样可能会重组服务器并将页面移至新路径。子字符串匹配还可能导致意外匹配，其中 URL 对象中包含的字符串也与非预期服务器上的路径或查询参数中的字符串匹配。 **输入 URL** 选项不支持通配符。

补充或选择性覆盖基于类别和信誉的 URL 过滤

在访问控制或 QoS 规则中，可以使用安全情报 URL 列表和源来补充或指定基于类别和信誉的 URL 过滤规则的例外情况。

重要提示！ 如果您在此过程中配置的列表或源包含基于类别或信誉的规则的例外情况，请按规则顺序将此规则置于这些规则之上。

在 SSL 规则中，使用可分辨名称条件配置并行行为。

开始之前

- 使用类别和信誉配置 URL 过滤请参阅配置 URL 条件，第 1345 页。
- 了解手动 URL 过滤的重要最佳实践。请参阅URL 过滤的最佳实践，第 1337 页和手动 URL 过滤选项，第 1348 页。
- 配置一个或多个包含要用于手动过滤的 URL 的安全情报对象（列表或源）。请参阅自定义安全情报列表和源，第 1031 页。

过程

步骤 1 导航至您将在其中定义规则的访问控制或 QoS 策略。

步骤 2 创建或编辑要在其中添加新条件的规则：

- 如果要补充基于类别或信誉的 URL 过滤规则，请编辑现有规则。
- 如果要覆盖或创建基于类别或信誉的 URL 过滤规则的例外，请创建新规则。

步骤 3 选择您创建的列表或源作为目标 URL 条件。

步骤 4 保存规则。

配置 HTTP 响应页面

作为访问控制的一部分，您可以使用访问控制规则或访问控制策略默认操作配置在系统阻止 Web 请求时要显示的 *HTTP* 响应页面。

所显示的响应页面取决于阻止会话的方式：

- **阻止响应页面**：覆盖用于说明拒绝已被连接的默认浏览器或服务器页面。
- **交互式阻止响应页面**：警告用户，并且还允许其点击按钮（或刷新页面）以加载最初请求的站点。用户在绕过响应页面后可能必须刷新才能加载未加载的页面元素。

如果未选择响应页面，则系统将在没有交互或说明的情况下阻止会话。

对 HTTP 响应页面的限制

响应页面仅适用于访问控制规则/默认操作

系统仅为被访问控制规则或访问控制策略默认操作阻止（或交互式阻止）的未加密连接或解密 HTTP/HTTPS连接显示响应页面。对于被任何其他策略或机制阻止的连接，系统不会显示响应页面。

显示响应页面禁用连接重置

如果重置连接（发送 RST 数据包），系统将无法显示响应页面。如果启用响应页面，系统将优先处理此配置。即使选择**阻止并重置**或**交互式阻止并重置**作为规则操作，系统也会显示响应页面，但不会重置匹配的 Web 连接。要确保重置已阻止的 Web 连接，必须禁用响应页面。

请注意，所有与此规则匹配的非 Web 流量都会被阻止并重置。

没有加密连接的响应页面（必须解密）

对于被访问控制规则（或其他任何配置）阻止的加密连接，系统不会显示响应页面。如果未配置SSL 策略，或者 SSL 策略允许已加密流量通过，则访问控制规则会评估已加密连接。

例如，系统无法解密 HTTP/2 或 SPDY 会话。如果使用以上协议之一加密的网络流量通过访问控制规则评估，则会话被阻止时系统不会显示响应页面。

但是，系统可以为先被 SSL 策略解密然后被访问控制规则或访问控制策略默认操作阻止（或交互式阻止）的连接显示响应页面。在这些情况下，系统会加密响应页面并在重新加密的 SSL 数据流最后发送该页面。

没有"升级"连接的响应页面

如果网络流量由于提升的访问控制规则（放在前面的仅包含简单网络条件的阻止规则）被阻止，系统则不显示响应页面。

没有重新定向连接的响应页面

如果在未指定 “http” 或 “https” 的情况下输入 URL，并且浏览器在端口 80 上发起连接，并且用户点击响应页面，并且该连接随后重定向到端口 443，则用户不会看到第二个交互式响应页面，因为对此 URL 的响应已被缓存。

识别 URL 之前没有响应页面

如果网络流量在系统识别请求的 URL 之前被阻止，则系统不会显示响应页面；请参阅URL 过滤的最佳实践，第 1337 页。

HTTP 响应页面的要求和必备条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

选择 HTTP 响应页面

HTTP 响应页面能否稳定显示取决于页面的网络配置、流量负载和大小。较小的页面更有可能成功显示。

过程

步骤 1 在访问控制策略编辑器中，点击 **HTTP 响应 (HTTP Responses)**。在新 UI 中，从数据包流行末尾的 **更多 (More)** 下拉箭头中选择高级设置。

如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 2 选择**阻止响应页面 (Block Response Page)** 和**交互式阻止响应页面 (Interactive Block Response Page)**：

- “系统提供”(System-provided) - 显示常规响应。点击 **视图**（ ） 可查看此页面的代码。

- “自定义”(Custom)-创建自定义响应页面。屏幕上将显示一个弹出窗口，其中预先填充有系统提供的代码，您可以通过点击 **编辑**（✎）来替换或修改此代码。计数器显示已使用的字符数量。
- “无”(None)-在没有交互或说明的情况下禁用响应页面并阻止会话。要对整个访问控制策略快速禁用交互式阻止，请选择此选项。

步骤 3 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改。

配置对 HTTP 响应页面的交互式阻止

配置交互式阻止时，用户可在看到警告后加载原先请求的站点。用户在绕过响应页面后可能必须刷新才能加载未加载的页面元素。

提示 要对整个访问控制策略快速禁用交互式阻止，既不要显示系统提供的页面，也不要显示自定义页面。然后，系统会阻止所有连接而不交互。

如果用户不绕过交互式阻止，则会拒绝匹配流量而不进行进一步检查。如果用户绕过交互式阻止，则访问控制规则会允许流量，不过，流量仍然可能受到深度检查和阻止。

默认情况下，用户绕行的有效时间为 10 分钟（600 秒），而在在后续访问时不显示警告页面。可以将持续时间设置为长达一年，也可以强制用户每次都绕过阻止。此设置适用于策略中的每条“交互式阻止”规则。不能对每条规则都设置限制。

以交互方式阻止的流量的日志记录选项与允许的流量中的日志记录选项相同，但如果用户不绕过交互式阻止，则系统只能记录连接开始事件。在系统最初警告用户时，它会使用 `Interactive Block` 或 `Interactive Block with reset` 操作标记任何已记录的连接开始事件。如果用户绕过阻止，则为会话记录的其他连接事件具有操作 `Allow`。

配置交互式阻止

以下程序介绍了如何允许用户绕过 URL 过滤规则。

过程

步骤 1 作为访问控制的一部分，请配置与网络流量匹配的访问控制规则；请参阅创建和编辑访问控制规则，第 1288 页：

- 操作 - 将规则操作设置为**交互式阻止 (Interactive Block)** 或**交互式阻止并重置 (Interactive Block with reset)**；请参阅访问控制规则交互式阻止操作，第 1286 页。

- 条件 - 使用 URL 条件指定要进行交互式阻止的网络流量；请参阅URL 条件（URL 过滤）。
- 日志记录 - 假设用户将绕过阻止并相应地选择日志记录选项。
- 检测 - 假设用户将绕过阻止并相应地选择深度检查选项；请参阅访问控制概述， 第 1239 页。

步骤 2 （可选）在访问控制策略 **HTTP 响应 (HTTP Responses)** 上，选择自定义交互式阻止 HTTP 响应页面；请参阅选择 HTTP 响应页面， 第 1351 页。

步骤 3 （可选）在访问控制策略**高级 (Advanced)** 设置中，更改用户绕行超时；请参阅为受阻网站设置用户绕过超时， 第 1353 页。

在用户绕过阻止后，系统允许用户浏览到该页面而不发出警告，直至经过超时期为止。

步骤 4 保存访问控制策略。

步骤 5 部署配置更改。

为受阻网站设置用户绕过超时

以下程序介绍如何设置用户绕过URL过滤阻止后允许浏览的时间。超时到期后，用户必须再次绕过阻止。

过程

步骤 1 点击 **策略** > **访问控制** 并编辑策略。

步骤 2 点击**高级 (Advanced)**。在 新 UI中，从数据包流末尾的 **更多** 下拉箭头中选择 **高级设置** 。

步骤 3 点击常规设置旁边的 **编辑**（ ） 。

如果显示**视图**（ ），则表明设置继承自祖先策略，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 4 在 **Allow an Interactive Block to bypass blocking for (seconds)** 字段中，键入用户绕过到期之前必须经过的秒数。

将此值设置为 0 表示交互式阻止响应显示一次，并且用户绕行永远不会过期。

步骤 5 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改。

配置 URL 过滤运行状况监控器

如果系统在获取或更新 URL 类别和信誉数据时出现问题，以下运行状况策略会发出警报。

- URL 过滤监视器
- 设备中威胁数据更新

要确保按照您希望的方式进行配置，请参阅《Cisco Secure Firewall Management Center 管理指南》中的 运行状况模块 和 配置运行状况监控 。

争议 URL 类别和信誉

如果您不同意 Talos 指定的类别或信誉，可以提交重新评估请求。

开始之前

您将需要思科账户凭证。

过程

步骤 1 在 Firepower 管理中心 Web 界面中，执行以下操作之一：

争议选项的位置	争议选项的路径
云服务配置页面	a. 导航至**系统 > 集成 > 云服务**页面。 b. 选择**争议 URL 类别和信誉**。
手动 URL 查找页面	a. 导航至手动 URL 查找页面：**分析 > 高级 > URL**。 b. 查找所有争议的 URL。 c. 要查看表格行末尾的 **争议** ，请将鼠标悬停在结果列表中的相关条目上，然后点击争议。
URL 连接事件	a. 导航至**分析 > 连接**菜单下的任何页面，此页面包括一个包含 URL 的表。 b. 右键点击 **URL 类别 (URL Category)**或 **URL 信誉 (URL Reputation)** 列（如有需要，请显示隐藏列）中的项目，然后选择一个选项。

Talos 网站将在单独的浏览器窗口中打开。

步骤 2 使用思科凭证登录 Talos 网站。

步骤 3 查看信息并遵循 Talos 页面上的说明。

步骤 4 在 Talos 网站上查找有关如何处理所提交的争议以及期望的响应（如有）的信息。

争议流程与 Firepower 产品无关。

如果 URL 类别集发生更改，请执行操作

URL 类别集可能会偶尔发生更改，以适应新的 Web 趋势和不断发展的使用模式。

这些更改会影响策略和事件。

在计划进行 URL 类别更改之前和之后不久，您将在受更改影响的任何访问控制，SSL 和 QoS 策略的规则列表中以及在您编辑。

在看到这些警报时，您应采取措施。

注释 本主题中描述的对 URL 类别集的更新与简单地在现有类别中添加新的 URL 或对错误分类的 URL 进行重新分类的变化不同。此主题不适用于单个 URL 的类别更改。

过程

步骤 1 如果您在访问控制策略中的规则旁边看到警报，请将鼠标悬停在警报上以查看详细信息。

步骤 2 如果警报提到 URL 类别更改，请编辑规则以查看更多详细信息。

步骤 3 将鼠标悬停在规则对话框中的 URL 或类别上，可查看有关更改类型的一般信息。

步骤 4 如果您在类别旁边看到警报，请点击警报以查看详细信息。

步骤 5 如果您在更改说明中看到“更多信息”链接，请点击该链接以在 Talos 网站上查看有关类别的信息。

或者，查看 URL 类别和信誉说明，第 1336 页链接中的所有类别的列表和说明。

步骤 6 根据更改类型，采取适当的操作：

类别更改的类型	系统将执行的操作	您应该采取的措施
现有类别即将被弃用	还没有。您有几周的时间来更改受影响的规则。 如果您在此期间不执行操作，系统最终将无法重新部署策略。	从包含此类别的所有规则中删除此类别。如果有类似的新类别，请考虑改为使用该类别。
已添加新类别	默认情况下，系统不使用新添加的类别。	考虑为新类别创建新规则。
删除现有类别	类别将以加删除线文本的形式（即，在类别名称上划一条横线）显示在规则中。	您必须先从规则中删除过时类别，然后才能进行部署。

步骤 7 检查您的 SSL 规则（类别）是否存在这些更改，并根据需要执行操作。

步骤 8 检查您的 QoS 规则（URL）是否存在这些更改，并根据需要执行操作。

下一步做什么

部署配置更改。

URL 类别和信誉变更：对事件的影响

- 当URL类别发生更改时，系统在类别更改之前处理的事件将与其原始类别名称相关联，并标记为**传统**。系统在类别更改之后处理的事件将与新类别相关联。

  随着时间的推移，较旧的传统事件将逐渐退出系统。

- 如果在处理 URL 时其没有信誉，则事件查看器中的 URL 信誉列将为空。

URL 过滤故障排除

类别列表中缺少预期的 URL 类别

URL 过滤功能使用的类别集与安全情报功能不同；您期望看到的类别可能是安全情报类别。要查看这些类别，请查看访问控制策略中 **安全情报** 选项卡上的 **URL** 选项卡。

初始数据包不经检查通过

请参阅在识别流量之前检查通过的数据包，第 2042 页以及子主题。

另请参阅DNS 过滤：在 DNS 查找期间识别 URL 信誉和类别，第 1347 页。

运行状况警报：“URL 过滤注册失败”

验证您的 管理中心 和任何代理是否可以连接到思科云。您可能需要以下主题中有关 URL 过滤和 URL 类别的信息：《Cisco Secure Firewall Management Center 管理指南》中的 互联网访问要求 和 通信端口要求 。

如何查找特定 URL 的类别和信誉？

进行手动查找。请参阅《Cisco Secure Firewall Management Center 管理指南》中的查找 *URL* 类别和信誉。

尝试手动查找时出错：“<URL> 云查找失败”

请确保已正确启用此功能。请参阅在 《Cisco Secure Firewall Management Center 管理指南》中 查找 *URL* 类别和信誉 中的前提条件。

似乎根据 URL 类别和信誉对 URL 进行了错误处理

问题：系统无法根据 URL 类别和信誉正确处理 URL。

解决方案：

- 验证与 URL 关联的 URL 类别和信誉是否如您所料。请参阅《Cisco Secure Firewall Management Center 管理指南》中的查找 *URL* 类别和信誉。
- 可以通过URL 过滤选项，第 1344 页（可以使用使用类别和信誉启用 URL 过滤，第 1343 页进行访问）中所述的设置来解决以下问题。
  - URL 缓存可以保存过时信息。请参阅URL 过滤选项，第 1344 页中有关**已缓存的 URL 到期**的信息。
  - 可能无法使用来自云的当前信息更新本地数据集。有关**启用自动更新**设置的信息，请参阅URL 过滤选项，第 1344 页。
  - 系统可以配置为不检查云以获取当前数据。请参阅URL 过滤选项，第 1344 页中有关**向思科云查询未知 URL** 设置的信息。
- 访问控制策略可以配置为将流量传递到 URL，而无需检查云。有关**重试 URL 缓存缺失查找**设置的信息，请参阅访问控制策略高级设置，第 1271 页。
- 另请参阅URL 过滤的最佳实践，第 1337 页。
- 如果使用 SSL 规则处理 URL，请参阅TLS/SSL 规则 准则和限制，第 1731 页和SSL 规则顺序
- 验证是否正在使用您希望处理的访问控制规则处理 URL，并且此规则将执行您希望执行的操作。考虑规则顺序。
- 验证 管理中心上的本地 URL 类别和信誉数据库是否已从云中成功更新，且托管设备是否已从管理中心成功更新。

  这些进程的状态将在运行状况监视器、**URL 过滤监视器**模块和**设备中威胁数据更新**模块中报告。有关详细信息，请参阅 《Cisco Secure Firewall Management Center 管理指南》 中的 运行状况 /

如果要立即更新本地URL类别和信誉数据库，请转至**集成** > **其他集成**，点击**云服务**，然后点击**立即更新 (Update Now)**。有关详细信息，请参阅URL 过滤选项，第 1344 页。

URL 类别或信誉不正确

对于访问控制或 QoS 规则：使用手动过滤，注意规则顺序。请参阅手动 URL 过滤，第 1348 页和配置 URL 条件，第 1345 页。

对于 SSL 规则：不支持手动过滤。改为使用可分辨名称条件。

也请按月 争议 URL 类别和信誉，第 1354 页。

网页加载速度缓慢

可以在安全与性能之间权衡取舍。某些选项：

- 考虑修改**缓存 URL 到期**设置。点击**集成**>**其他集成**，然后选择**云服务**。有关信息，请参阅URL 过滤选项，第 1344 页。
- 考虑在访问控制策略高级设置，第 1271 页中取消选择**重试 URL 缓存缺失查找**设置。

事件不包括 URL 类别和信誉

- 确保已在访问控制策略中包含适用的URL规则，规则处于活动状态，并且策略已部署到相关设备。
- 如果连接在与 URL 规则匹配之前得到处理，则 URL 类别和信誉不会显示在事件中。
- 必须为 URL 类别和信誉配置处理连接的规则。
- 即使已在 SSL 规则的类别选项卡中配置 URL 类别，也必须在访问控制策略的规则中配置 URL 选项卡。

DNS 过滤不起作用

确保您已完成 启用 DNS 过滤以在域查找期间识别 URL ，第 1347 页中的所有前提条件和步骤。

最终用户尝试访问被阻止的 URL，而页面只是旋转和超时

当启用 DNS 过滤且最终用户访问被阻止的 URL 时，页面将旋转但不会加载。最终用户不会收到该页面被阻止的通知。这是当前启用 DNS 过滤时的限制。

请参阅DNS 过滤限制，第 1347 页。

事件包括 URL 类别和信誉，但 URL 字段为空

如果 DNS 查询字段已填充且 URL 字段为空，则在启用 DNS 过滤功能时会出现这种情况。

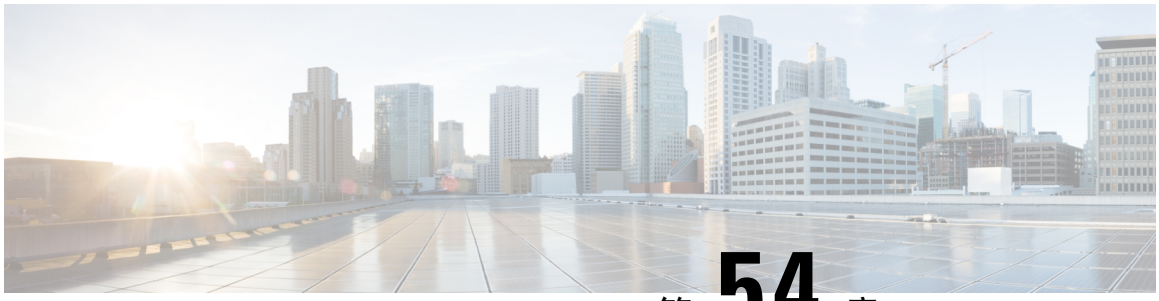
请参阅DNS 过滤和事件，第 1348 页。

为单个事务生成多个事件

单个 Web 事务有时会生成两个连接事件，一个用于 DNS 过滤，另一个用于 URL 过滤。当启用 DNS 过滤并且符合以下条件时，会出现这种情况：

- 流量的访问控制规则操作为“允许”或“信任”。
- 系统首次遇到 URL。

请参阅DNS 过滤和事件，第 1348 页。



第 54 章

安全情报

以下主题提供安全情报的概述，包括用于将流量和基本设置列入阻止名单和允许名单。

关于安全情报

作为防御恶意互联网内容的第一道防线，安全情报使用信誉情报快速阻止与IP地址、URL和域名的连接。这称为 列入安全情报阻止列表。

在系统执行需要更多资源的评估之前，安全情报是访问控制的第一阶段。使用阻止列表通过快速排除不需要检测的流量来提高性能。

注释 不能使用阻止列表阻止快速路径流量。预过滤器评估发生 在安全情报过滤之前。使用快速路径的流量会绕过所有的进一步评估，包括安全情报。

虽然您可以配置自定义阻止列表，但思科提供对定期更新的情报源的访问权限。具有安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的站点出现和消失的速度可能比您更新和部署自定义配置的速度要快。

您可以使用“不阻止”列表和仅监控“阻止”阻止列表细化安全情报阻止列表。这些机制可以使流量免于列入阻止名单，但 **不会** 自动信任匹配流量或对其使用快速路径。 添加到 "不阻止 "列表中的流量或在安全情报阶段被监控的流量会被有意地与其他访问控制进行进一步分析。

相关主题

安全情报，第 1026 页

安全情报的最佳实践

- 配置访问控制策略以阻止由思科提供的安全情报源所检测到的威胁。请参阅配置示例：安全情报阻止，第 1367 页。
- 如果要使用自定义威胁数据来补充思科提供的安全情报源，或手动阻止新出现的威胁：
  - 对于 IP 地址，请使用自定义安全情报列表和源，或者网络对象或组。要创建这些内容，请参阅安全情报，第 1026 页和网络，第 997 页及其子主题。要将其用于安全情报，请参阅配置安全情报，第 1362 页。安全情报策略中使用的网络对象需要 威胁 许可证。
  - 对于 URL 和域，请使用自定义安全情报列表和源，而不是对象或组。请参阅手动 URL 过滤选项，第 1348 页中的详细信息
  - 您还可以将条目从事件添加到阻止列表。请参阅全局和域安全情报列表，第 1027 页。
- 要测试新源或被动部署，请将操作从阻止设为仅监控。请参阅安全情报监控，第 1368 页。
- 如果需要从安全情报阻止中排除特定站点或地址，请参阅覆盖安全情报阻止，第 1368 页。
- 如果您的 Firepower 部署与 SecureX 或相关工具 SecureX 威胁响应（以前称为思科威胁响应或 CTR）集成，并且使用了自定义安全情报列表和源，请务必使用这些列表和源来更新安全服务交换 (SSE)。有关详细信息，请参阅 SSE 联机帮助中有关配置事件自动升级的说明。
- 系统提供的安全情报类别可能会随着时间的推移而发生变化，恕不另行通知；您应该计划定期检查更改，并相应地修改策略。
- 您还应配置URL过滤，这是一项具有单独许可要求的单独功能，旨在进一步防御恶意站点。请参阅URL 过滤，第 1335 页。

安全智能许可证要求

威胁防御 许可证

IPS

经典许可证

保护

安全情报的要求和必备条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

安全情报来源

- 系统-提供的源

  思科提供对定期更新的域名、URL 和 IP 地址的安全情报源的访问权限。有关详细信息，请参阅安全情报，第 1026 页。

- 第三方源

  （可选）可以使用第三方信誉源（通常是 Cisco Secure Firewall Management Center定期从互联网下载的动态列表）补充思科提供的源。请参阅自定义安全情报源，第 1033 页。

- 自定义阻止列表或源（或对象或组）

  使用手动创建的列表或源来阻止特定 IP 地址、URL 或域名（对于 IP 地址，您还可以使用网络对象或组）。

  例如，如果您发现尚未被源阻止的恶意站点或地址，请将这些站点添加到自定义安全情报列表中，并将此自定义列表添加到访问控制策略的“安全情报”(Security Intelligence) 选项卡中的“阻止”列表。如自定义安全情报列表，第 1035 页和配置安全情报，第 1362 页中所述。

  对于 IP 地址，您可以选择使用网络对象而不是列表或源；有关信息，请参阅网络，第 997 页。（对于 URL，强烈建议使用列表和源，而非其他方法。）

- 自定义不阻止列表或源

  优先于特定站点或地址的安全智能阻止。请参阅覆盖安全情报阻止，第 1368 页。

- 全局阻止列表（网络、URL 和 DNS 各一个）

  查看事件时，您可以立即将事件的 IP 地址、URL 或域添加到适用的全局阻止列表，以便安全智能处理来自该源的未来流量。请参阅全局和域安全情报列表，第 1027 页。

- 全局不阻止列表（网络、URL 和 DNS 各一个）

  在查看事件时，如果您不希望安全情报阻止来自该源的未来流量，则可以立即将事件的 IP 地址、URL 或域添加到适用的全局不阻止列表。请参阅全局和域安全情报列表，第 1027 页。

配置安全情报

每个访问控制策略都具有安全情报选项。您可以将网络对象、URL 对象和列表以及安全情报源和列表列入阻止列表或不阻止列表，全部都可通过安全区域进行限制。您还可以将DNS策略与访问控制策略相关联，并将域名列入阻止列表或不阻止列表。

“不阻止列表”中的对象数加上“阻止列表”中的数量不能超过 125 个 网络对象或 32767 个 URL 对象和列表。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

开始之前

- 提示：有关最低配置建议的指南，另请参阅 配置示例：安全情报阻止，第 1367 页。
- 要确保所有选项可供选择，请向管理中心添加至少一个受管设备。
- 在被动部署中，或者如果要将安全情报过滤设置为仅监控，请启用日志记录
- 配置 DNS 策略以对域执行安全情报操作。有关详细信息，请参阅DNS 策略，第 1371 页。

过程

步骤 1 在访问控制策略编辑器中，点击 **安全情报**。

如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 2 您有以下选择：

- 点击 **网络** 以添加网络对象（IP 地址）。

  注释 安全情报策略中使用的网络对象需要 威胁 许可证。

- 点击 **URL** 以添加 URL 对象。

步骤 3 查找要添加到“阻止”或“不阻止”列表的 **可用对象** 。您有以下选择：

- 通过在**按名称或值搜索 (Search by name or value)** 字段中输入内容，搜索可用对象。通过点击 **重新加载**（↻）或 **清除**（✕）来清除搜索字符串。

- 如果现有列表或源不满足需求，请点击 **添加**（+），选择 **新建网络列表** 或 **新建 URL 列表**，然后继续操作，如 创建安全情报源，第 1033 页或将新的安全情报列表上传到 Cisco Secure Firewall Management Center，第 1035 页中所述。
- 如果现有对象不满足需求，请点击 **添加**（+），选择 **新建网络对象** 或**新建 URL 对象**，然后继续操作，如 创建网络对象，第 999 页中所述。

“安全智能”会忽略使用 `/0` 掩码的 IP 地址块。

步骤 4 在**可用对象**中选择一个或多个要添加的可用对象。

步骤 5 （可选）在**可用区域**中选择一个可用区域以按区域约束所选对象。

不能按区域限制系统提供的安全情报列表。

注释 SI的 **Any** 区域列表仅适用于属于安全区域的接口。但是，有一个例外是，如果设备没有与安全区域关联的任何接口，则 **Any** 区域将匹配任何接口。

例如，如果设备上有五个接口，但没有一个接口与安全区域相关联，则将根据设备上所有接口上的流量检查分配给 **Any** 区域的任何 SI 列表。如果将一个接口添加到该设备上的安全区域，它会有效地删除其他四个接口上的 SI 检查，其中 SI 列表的区域设置为 **Any**。如果将其他四个接口添加到安全区域，它们将由附加到 **Any** 区域的 SI 列表进行评估。

步骤 6 点击 **添加到不阻止列表** 或 **添加到阻止列表**，或者点击所选对象并将其拖至任一列表。

要从阻止列表或不阻止列表中删除对象，请点击 **删除**（🗑）。要删除多个对象，请选择这些对象并右键点击 **删除所选项**。

步骤 7 （可选）通过右键点击**阻止列表**下的对象，然后选择**仅监控**（**不阻止**），将列入阻止列表的对象设置为仅监控。

不能将系统提供的全域安全情报列表设置为仅监控。

步骤 8 从 **DNS 策略 (DNS Policy)** 下拉列表中选择 DNS 策略。

步骤 9 点击**保存 (Save)**。

下一步做什么

- 部署配置更改。

相关主题

安全情报，第 1026 页
Snort® 重新启动场景，第 143 页

安全情报选项

使用访问控制策略编辑器中的“安全情报”(Security Intelligence) 选项卡配置网络（IP 地址）和 URL 安全情报，以及将访问控制策略与您在其中为域配置了安全智能的 DNS 策略相关联。

可用对象

可用对象包括：

- 由系统提供的源填充的安全情报类别。

  有关详细信息，请参阅安全情报类别，第 1365 页。

- 由系统提供的全局阻止和不阻止列表。

  有关说明，请参阅安全情报来源，第 1361 页。

- 在“对象”(Object) > “对象管理”(Object Management) > “安全情报”(Security Intelligence) 下创建的安全情报列表和源。

  有关说明，请参阅安全情报来源，第 1361 页。

- 在“对象”(Object) > “对象管理”(Object Management) 下的相应页面上配置的网络和 URL 对象及组。这些对象与上一个项目符号中的安全情报对象有所不同。

  有关网络对象的详细信息，请参阅网络，第 997 页。（对于 URL，请使用安全情报列表或源，而不是对象或组。）

可用区

除系统提供的全局列表之外，您可以按照区域限制安全情报过滤。

例如：为了提高性能，您可能想要锁定执行目标。作为更具体的示例，您可以只阻止处理邮件流量的安全区域的垃圾邮件。

如要在多个区域上实施对象的安全情报过滤，对于每个区域，都必须将对象分别添加至阻止或不组织列表。

DNS 策略

要使用安全情报来匹配 DNS 流量，您必须为安全情报配置选择 DNS 策略。

使用阻止或不阻止列表，或者根据 DNS 列表或源来监控流量还要求您：

- 配置 DNS 安全情报列表和源。请参阅安全情报，第 1026 页。
- 创建 DNS 策略。有关详细信息，请参阅创建基本 DNS 策略，第 1374 页。
- 配置引用 DNS 列表或源的 DNS 规则。有关详细信息，请参阅创建和编辑 DNS 规则，第 1376 页。
- 由于 DNS 策略部署为访问控制策略的一部分，因此必须将两个策略均进行关联。有关详细信息，请参阅DNS 策略部署，第 1384 页。

不阻止列表

请参阅覆盖安全情报阻止，第 1368 页。

要选择列表中的所有对象，请右键点击对象。

阻止列表

请参阅 配置示例：安全情报阻止，第 1367 页 和本章中的其他主题。

有关阻止列表中的视觉指示的说明，请参阅阻止列表图标，第 1366 页。

要选择列表中的所有对象，请右键点击对象。

日志记录

启用安全情报日志记录（默认情况下处于启用状态）会记录由访问控制策略的目标设备处理的所有受阻和受监控的连接。然而，系统不会记录不阻止列表匹配项；对不阻止列表上的连接的日志记录取决于其最终性质。必须首先为阻止列表中的连接启用日志记录，然后才能将该列表中的对象设置为仅监控。

要启用、禁用或查看日志记录设置，请右键点击阻止列表中的对象。

相关主题

全局和域安全情报列表，第 1027 页
安全情报列表和多租户，第 1028 页

安全情报类别

安全情报类别由 安全情报，第 1026 页中所述的系统提供的源确定。

这些类别用于以下位置：

- 访问控制策略的“安全情报”选项卡上的“网络”子选项卡
- 访问控制策略的“安全情报”选项卡上“网络”选项卡旁边的 “URL” 子选项卡
- 在 DNS 策略配置页面的 DNS 选项卡上的 DNS 策略中
- 在流量与上述位置的阻止或监控配置匹配时生成的事件中

注释 如果您的组织使用 Cisco Secure Firewall 威胁智能导向器：查看事件时，您可能会看到指示 TID 已执行操作的类别，例如 `TID URL 阻止`。

类别由 Talos 从云更新，并且此列表可能会独立于 Firepower 版本进行更改。

表 *97:* 思科 *Talos* 情报小组 *(Talos)* 源类别

安全情报类别	说明
攻击者	出站恶意活动已知的活动扫描工具和主机
Banking_fraud	从事与电子银行相关的欺诈活动的网站
Bogon	Bogon 网络和未分配的 IP 地址

安全情报类别	说明
Bots	托管二进制恶意软件丢弃程序的站点
CnC	托管僵尸网络的命令和控制服务器的站点
加密货币挖矿活动	提供对用于挖掘加密货币的池和钱包的远程访问的主机
Dga	用于生成作为与命令和控制服务器的交汇点的大量域名的恶意软件算法
Exploitkit	指定用于识别客户端中的软件漏洞的软件包
High_risk	根据来自安全图的 OpenDNS 预测安全算法进行匹配的域和主机名
IOC	观察到涉及感染指标 (IOC) 的主机
Link_sharing	未经许可共享版权文件的网站
恶意	表现出不一定属于另一种更精细的威胁类别的恶意行为的站点
恶意软件	托管恶意软件二进制或漏洞包的站点
Newly_seen	最近注册或尚未通过遥测发现的域
Open_proxy	允许匿名 Web 浏览的开放代理
Open_relay	已知用于垃圾邮件的开放邮件中继
网络钓鱼	托管网络钓鱼页面的站点
解决方案	主动参与恶意或可疑活动的 IP 地址和 URL
垃圾邮件	已知用于发送垃圾邮件的邮件主机
间谍软件	已知包含、提供或支持间谍软件和广告软件活动的网站
可疑	看似可疑并具有类似于已知恶意软件的特征的文件
Tor_exit_node	已知为 Tor Anonymizer 网络提供出口节点服务的主机

阻止列表图标

以下可视指示器可能会显示在访问控制策略的“安全情报”(Security Intelligence) 选项卡上的阻止列表中：

图标或可视指示灯	说明
阻止图标（  ）	对象被设为阻止。

图标或可视指示灯	说明
监控（）	对象被设为仅监控。 请参阅 安全情报监控，第 1368 页
对象以删除线文本显示	同一对象也位于不阻止列表中，该列表将覆盖该阻止。

配置示例：安全情报阻止

配置访问控制策略以阻止系统定期更新的安全情报源可检测到的所有威胁。

“阻止列表”中的对象数加上“不阻止列表”中的数量不能超过 125 个 网络对象或 32767 个 URL 对象和列表。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

开始之前

- 要确保所有选项可供选择，请向管理中心添加至少一个受管设备。
- 配置 DNS 策略以阻止域的所有安全情报威胁类别。有关详细信息，请参阅DNS 策略，第 1371 页。
- 如果您拥有或将要拥有要阻止的实体的自定义列表，请创建每种类型（URL，DNS，网络）的安全情报对象。请参阅安全情报，第 1026 页。

过程

步骤 1 点击 **策略 (Policies) > 访问控制 (Access Control)**。

步骤 2 创建新的访问控制策略，或者编辑现有策略。

步骤 3 在访问控制策略编辑器中，点击 **安全情报**。

如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 4 点击 **网络** 为 IP 地址添加阻止条件。

a) 在网络列表中向下滚动并选择全局列表下方列出的所有威胁类别。
b) 如果适用，请选择要阻止这些威胁的安全区域。
c) 点击 **添加到阻止列表**。
d) 如果您创建的自定义列表或源具有要阻止的地址，请使用与上述相同的步骤将这些地址添加到阻止列表。

步骤 5 点击 **URL** 以添加 URL 的阻止条件，然后重复您对网络执行的步骤。

步骤 6 从 **DNS 策略**下拉列表中选择 DNS 策略；请参阅DNS 策略概述，第 1371 页。

步骤 7 点击**保存**。

下一步做什么

- 为这些连接启用日志记录
- 部署配置更改。
- 要获得额外保护，请配置 URL 过滤以阻止恶意 URL。请参阅URL 过滤，第 1335 页。

安全情报监控

监控会记录那些本应被安全智能阻止的流量的连接事件，但不会阻止流量。监控对于以下情况尤其有用：

- 在实施源之前对其进行测试。

  考虑一下这样的情况，在使用第三方源实施阻止之前，想要先对该源进行测试。将源设置为仅监控时，系统允许已被阻止的连接，以便系统能对其进行进一步的分析，但是也会记录这些连接中的每一个连接，以供进行评估。

- 被动部署，以优化性能。

  被动部署的受管设备无法影响流量；与将系统配置为阻止流量相比，没有任何优势。此外，因为阻止的连接实际上在被动部署中并未被阻止，因此，系统可能针对每条已阻止连接报告多个连接开始事件。

注释 如已配置，Cisco Secure Firewall 威胁智能导向器 可能会影响所采取的行动（监控或阻止）。

要配置安全智能监控：

按照配置示例：安全情报阻止，第 1367 页中的说明配置安全情报阻止后，右键点击阻止列表中的每个适用对象，然后选择**仅监控 (Monitor-only)**。 不能将系统提供的安全情报列表设置为仅监控。

覆盖安全情报阻止

或者，您可以使用“不阻止”列表来避免特定域、URL 或 IP 地址被安全智能列表或源阻止。

例如，您可以：

- 在信誉良好的安全智能源中覆盖偶尔的误报阻止

- 深入检查特定流量，而不是根据信誉来提前阻止流量
- 根据区域豁免其他受限事务的安全情报阻止

  例如，您可以将分类不当的URL加入“不阻止”列表中，但随后使用您的组织中需要访问这些URL 的人员所使用的安全区域来限制“不阻止”列表对象。这样，只有有业务需要的人员才能访问“不阻止”列表中的 URL。

注释 “不阻止”列表中的条目只是阻止列表中的例外项。通过安全情报策略的任何连接都受访问控制规则的约束。因此，访问控制规则或入侵策略随后可以阻止“不阻止”列表中的条目。您的“不阻止”条目应始终是阻止列表的例外项。

过程

步骤 1 选项 1：将事件中的 IP 地址、URL 或域添加到“全局不阻止列表”。请参阅全局和域安全情报列表，第 1027 页。

步骤 2 选项 2：使用自定义安全智能列表或源。

a) 创建自定义安全智能列表或源。请参阅自定义安全情报列表，第 1035 页或创建安全情报源，第 1033 页。

b) 对于 IP 地址（网络）和 URL：编辑访问控制策略，点击“安全智能”(Security Intelligence)选项卡，然后点击“网络”(Networks) 或“URLs”子选项卡中的自定义列表或源，然后点击**添加到不阻止列表 (Add to Do Not Block List)**。

c) 保存更改。

d) 对于域 (DNS)：请参阅安全情报选项，第 1363 页主题中的“DNS 策略”部分。

e) 部署更改。

安全情报故障排除

请参阅以下有关安全情报故障排除的主题。

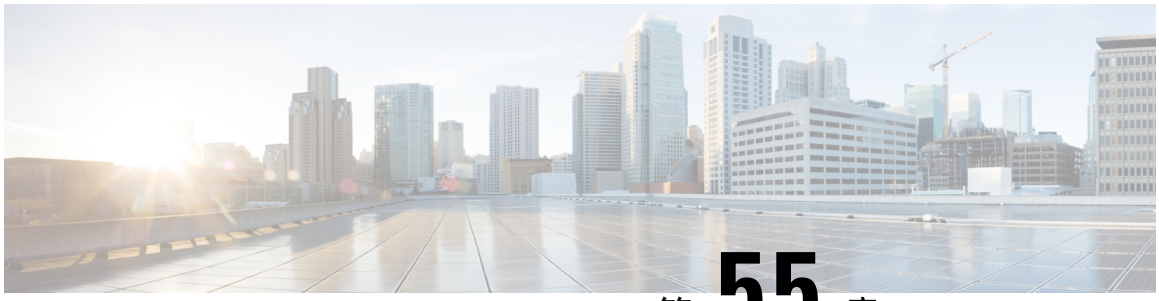
可用选项列表中缺少安全情报类别

症状：在访问控制策略的“安全情报”(Security Intelligence) 选项卡上，“可用选项”(Available Options) 下的“网络”(Networks) 选项卡中不会显示安全情报类别（例如 CnC 或漏洞攻击包）。

原因：

- 在管理中心至少添加一个托管设备之前，这些类别不会显示。您必须添加一个设备才能提取所有 TALOS 源。

- URL 过滤功能使用的类别集与安全情报功能有所不同；；您期望看到的类别可能是 URL 过滤类别。要查看 URL 过滤类别，请查看访问控制规则中的 **URLs** 选项卡。



第 55 章

DNS 策略

以下主题介绍 DNS 策略、DNS 规则，以及向受管设备部署 DNS 策略的方法。

DNS 策略概述

基于DNS的安全智能允许你根据客户端请求的域名，使用安全智能阻止列表来阻止流量。思科提供可用于过滤流量的域名情报，您还可以根据部署配置自定义域名列表和源。

DNS策略阻止列表上的流量会立即被阻止，因此不会受到任何进一步的检查--不是为了入侵、利用、恶意软件等，但也不是为了网络发现。你可以使用安全智能的不阻止列表来覆盖阻止列表并强制评估访问控制规则，而且，在被动部署中建议你使用"仅监控"设置来进行安全智能过滤。这允许系统分析本会被阻止列表阻断的连接，但也会记录与阻止列表的匹配，并生成一个连接结束的安全情报事件。

注释 基于 DNS 的安全情报可能无法为域名实现预期功能，除非 DNS 服务器由于到期删除域缓存条目，或者客户端的 DNS 缓存或本地 DNS 服务器的缓存被清除或已到期。

您可使用 DNS 策略及关联的 DNS 规则配置基于 DNS 的安全情报。要将配置部署到设备，您必须将 DNS 策略与访问控制策略相关联，然后将配置部署到受管设备。

Cisco Umbrella DNS 策略

管理中心中的 Cisco Umbrella DNS 连接有助于将 DNS 查询重定向到Cisco Umbrella。这使 Cisco Umbrella 可以根据域名验证请求是被允许还是被阻止，并对请求应用基于 DNS 的安全策略。如果使用 Cisco Umbrella，则必须配置 Cisco Umbrella 连接，将 DNS 查询重定向到 Cisco Umbrella。

Umbrella 连接器是系统 DNS 检测的一部分。如果现有 DNS 检测策略映射决定根据 DNS 检测设置阻止或丢弃请求，则该请求不会转发至思科 Umbrella。因此，您有两条防线：

- 您的本地 DNS 检测策略
- Cisco Umbrella 基于云的策略

将 DNS 查询请求重定向到思科 Umbrella 时，Umbrella 连接器会添加 EDNS （DNS 扩展机制） 记录。EDNS 记录包括设备标识符信息、 组织 ID 和客户端 IP 地址。基于云的策略可以使用 FQDN 信誉以及这些标准来控制访问。还可以选择使用 DNSCrypt 加密 DNS 请求，以确保用户名和内部 IP 地址的隐私性。

有关如何在管理中心设置 Umbrella DNS 连接器的详细信息，请参阅为 Cisco Secure Firewall Management Center 配置 Umbrella DNS 连接器。

DNS 策略组件

DNS 策略允许您使用阻止列表基于域名阻止连接，或使用“不阻止”列表来免除此类连接的此类阻止。以下列表介绍可在创建 DNS 策略后更改的配置。

名称和描述

每个 DSN 策略必须拥有唯一的名称。说明为可选项。

在多域部署中，策略名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的策略名称的冲突。

规则

规则提供一种基于域名处理网络流量的精细方法。DNS 策略中的规则从 1 开始进行编号。系统按照规则编号的升序顺序自上而下将流量与 DNS 规则相匹配。

创建 DNS 策略时，系统使用默认的全局 DNS 不阻止列表和默认的 DNS 全局阻止列表规则来填充该策略。两个规则均固定到其各自类别中的第一个位置。您无法修改这些规则，但是可以将其禁用。

在多域部署中，系统还会将后代 DNS 不阻止列表和后代 DNS 阻止列表规则添加到后代域中的 NDS 策略。这些规则固定到其各自类别中的第一个位置。

注释 如果为 管理中心启用多租户，则系统组成域的层次结构，包括祖先域和后代域。这些域截然不同并独立于 DNS 管理中所使用的域名。

后代列表包含系统子域用户的阻止或不阻止列表上的域。从祖先域中，您无法查看后代列表的内容。如果您不希望子域用户将域添加到阻止或不阻止列表：

- 禁用后代列表规则，并且
- 使用访问控制策略继承设置执行安全情报

系统按照以下顺序评估规则：

- DNS 规则的全局不阻止列表（如果启用）
- 后代 DNS 不阻止列表规则（如果启用）
- 包含不阻止操作的的规则
- DNS 规则的全局阻止列表（如果启用）
- 后代 DNS 阻止列表规则（如果启用）
- 包含除不阻止以外的操作的规则

通常，系统根据第一个 DNS 规则（其中所有规则的条件都与流量匹配）处理基于 DN 的网络流量。如果没有任何 DNS 规则与流量匹配，则系统根据关联的访问控制策略规则继续评估流量。DNS 规则条件可以简单，也可以复杂。

DNS 策略许可证要求

威胁防御 许可证

IPS

经典许可证

保护

DNS 策略的要求和必备条件

型号支持

任意

支持的域

任意

用户角色

- 管理员

- 访问管理员
- 网络管理员

管理 DNS 和 Umbrella DNS 策略

使用“DNS 策略”(DNS Policy) 页面（**策略** > **访问控制** > **DNS**）管理自定义 DNS 和 Umbrella DNS 策略。

除了您创建的自定义策略之外，系统还提供默认 DNS 策略和默认 Umbrella DNS 策略。默认 DNS 策略会使用默认阻止列表和不阻止列表。您可以编辑并使用系统提供的自定义策略。在多域部署中，默认 DNS 策略使用默认的全局 DNS 阻止列表、全局 DNS 不阻止列表、后代 DNS 阻止列表和后代 DNS 不阻止列表，并且只能在全局域中编辑。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略** > **访问控制** > **DNS**。

步骤 2 要管理 DNS 策略，请执行以下操作：

- 比较 - 要比较 DNS 策略，请点击**比较策略 (Compare Policies)**，然后如比较策略，第 148 页中所述继续操作。
- “复制”(Copy) - 要复制 DNS 策略，请点击 **复制**（  ），然后如编辑 DNS 策略，第 1375 页中所述继续操作。
- “创建”(Create) - 要创建新的 Umbrella DNS 策略，请点击**新建策略 (New Policy)** > **Umbrella DNS 策略 (Umbrella DNS Policy)**，然后如创建 Umbrella DNS 策略，第 1387 页中所述继续操作。
- “删除”(Delete) - 要删除 DSN 或 Umbrella DSN 策略，请点击 **删除**（  ），然后确认要删除策略。
- “编辑”(Edit) - 要修改现有 DNS 策略，请点击 **编辑**（  ），然后如编辑 DNS 策略，第 1375 页中所述继续操作。要修改现有 Umbrella DNS 策略，请点击 **编辑**（），然后如编辑 Cisco Umbrella DNS 策略和规则，第 1387 页中所述继续操作。

创建基本 DNS 策略

当您创建新的 DNS 策略时，它包含默认设置。然后，您必须对其进行编辑以自定义行为。

过程

步骤 1 选择策略 > 访问控制 > **DNS**。

步骤 2 点击添加 **DNS** 策略 **(Add DNS Policy)** > **DNS** 策略 **(DNS Policy)**。

步骤 3 在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。

步骤 4 点击保存 **(Save)**。

下一步做什么

配置策略。请参阅编辑 DNS 策略，第 1375 页。

编辑 DNS 策略

一个用户一次只能使用一个浏览器窗口编辑一个DNS策略。如果多个用户尝试保存同一策略，系统会仅保留第一组保存的更改。

为保护会话隐私，在策略编辑器上 30 分钟未执行任何操作之后，系统将显示警告。在 60 分钟后，系统将放弃更改。

过程

步骤 1 选择策略 > 访问控制 > **DNS**。

步骤 2 点击您要编辑的 DNS 策略旁边的编辑（）。

如果显示视图（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 要编辑 DNS 策略，请执行以下操作：

- 名称和说明 - 要更改名称或说明，请点击相应的字段并键入新信息。
- 规则 - 要添加、分类、启用、禁用或以其他方式管理 DNS 规则，请点击规则 **(Rules)**，然后如创建和编辑 DNS 规则，第 1376 页中所述继续操作。

步骤 4 点击保存 **(Save)**。

下一步做什么

- 或者，进一步配置新策略，如《Cisco Secure Firewall Management Center 管理指南》中的使用安全情报记录连接中所述。
- 部署配置更改；请参阅部署配置更改，第 136 页。

DNS 规则

DNS 规则根据主机请求的域名处理流量。作为安全情报的一部分，此评估发生在所有流量解密之后以及访问控制评估之前。

系统按照您指定的顺序将流量与DNS规则相匹配。在大多数情况下，系统根据第一个DNS规则（其中规则的所有条件都与流量匹配）处理网络流量。

除其唯一名称之外，每个 DNS 规则都具有以下基本组件：

状态

默认情况下，规则处于启用状态。如果您禁用某规则，系统将不用它来评估网络流量并停止为该规则生成警告和错误。

位

DNS 策略中的规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。除 Monitor 规则之外，流量匹配的第一个规则是处理该流量的规则。

条件

条件指定规则处理的特定流量。DNS 规则必须包含 DNS 源或列表条件，还可以按安全区域、网络或 VLAN 匹配流量。

操作

规则的操作确定系统如何处理匹配流量：

- 允许包含**不阻止**操作的流量，需进一步进行访问控制检查。
- 受监控的流量将根据其余有关 DNS 阻止列表的规则进行进一步评估。如果流量不匹配 DNS 阻止列表规则，则将使用访问控制规则进行检查。系统会记录流量的安全情报事件。
- 阻止列表上的流量将被丢弃，无需进一步检查。您还可以返回“找不到域”(Domain Not Found)响应，或将 DNS 查询重定向到 Sinkhole 服务器。

相关主题

关于安全情报，第 1359 页

创建和编辑 DNS 规则

在 DNS 策略中，最多可以向阻止列表和不阻止列表规则中添加总共 32767 个 DNS 列表；即，DNS 策略中的列表数不能超过 32767。

过程

步骤 1 在 DNS 策略编辑器中，可进行以下选择：

- 要添加新规则，请点击**添加 DNS 规则 (Add DNS Rule)**。
- 要编辑现有规则，请点击 **编辑**（）。

步骤 2 输入 **Name**。

步骤 3 配置规则组成部分，或接受默认值：

- 操作 - 在**操作 (Action)** 中选择规则操作；请参阅DNS 规则操作，第 1378 页。
- 条件 - 配置规则的条件；请参阅DNS 规则条件，第 1379 页。
- 已启用 - 指定规则是否为**已启用 (Enabled)**。

步骤 4 点击**保存 (Save)**。

下一步做什么

- 部署配置更改；请参阅部署配置更改，第 136 页。

DNS 规则管理

通过 DNS 策略编辑器的**规则 (Rules)** 选项卡，您可以添加、编辑、移动、启用、禁用、删除或以其他方式管理策略中的 DNS 规则。

对于每个规则，策略编辑器会显示其名称和条件摘要，以及规则操作。其他图标代表 **警告**（）、**错误**（） 和其他重要的 **信息**（）。已禁用的规则在规则名称下方呈灰色显示并带有相应的标记 `(disabled)`。

启用和禁用 DNS 规则

创建DNS规则时，默认情况下会启用规则。如果您禁用某规则，系统将不用该规则来评估网络流量并停止为该规则生成警告和错误。查看DNS策略中的规则列表时，已禁用的规则呈灰色显示，但这些规则仍可以修改。请注意，也可使用 DNS 规则编辑器启用或禁用 DNS 规则。

过程

步骤 1 在 DNS 策略编辑器中，右键点击规则并选择规则状态。

步骤 2 点击**保存 (Save)**。

下一步做什么

- 部署配置更改。

DNS 规则顺序评估

DNS 策略中的规则从 1 开始进行编号。系统按照规则编号的升序顺序自上而下将流量与 DNS 规则相匹配。在大多数情况下，系统根据第一个DNS规则（其中所有规则的条件都与流量相匹配）处理网络流量。

- 对于“监控”(Monitor)规则，系统会记录流量，然后根据优先级较低的DNS黑名单规则继续评估流量。
- 对于“非监控”规则，在流量匹配规则后系统**不会**根据其他优先级较低的DNS规则继续评估流量。

对规则排序时，请注意：

- DNS 的全局不阻止列表 (Do-Not-Block List) 始终排在首位，优先于所有其他规则。
- 后代 DNS 白名单 (Descendant DNS 不阻止列表 (Do-Not-Block Lists) 规则仅在多域部署的非分叶域中显示。它始终排在第二位，且优先于除全局不阻止列表 (Do-Not-Block List) 之外的所有 其他规则。
- “不阻止列表”(Do-Not-Block List)部分优先于“阻止列表”(Block List)部分；不阻止列表规则始终优先于其他规则。
- “全局阻止列表”(Global Block List)始终排在“阻止列表” (Block List)部分的第一个位置，并且优先于所有其他“监控”(Monitor)和“阻止”(Block)列表规则。
- “后代 DNS 阻止列表”(Descendant DNS Block Lists)规则仅在多域部署的非分叶域中显示。它在“阻止列表”(Block List)部分中始终排在第二位，并且优先于除“全局阻止列表”(Global Block List)以外的所有其他“监控”(Monitor)和“阻止”(Block)列表规则。
- “阻止列表”(Block List)部分包含监控和阻止列表规则。
- 首次创建 DNS 规则时，如果分配**不阻止 (Do Not Block)** 操作，系统会将其放在“不阻止列表”(Do-Not-Block List)部分的最后；如果分配任何其他操作，模块会将其放在“阻止列表”(Block List)部分的最后。

可以通过拖放规则来为规则重新排序。

DNS 规则操作

每个 DNS 规则都有确定匹配流量的以下过程的操作：

- 处理 - 首先，规则操作可管理系统是否会根据阻止或不阻止列表来阻止、不阻止或监控符合规则条件的流量。
- 日志记录 - 该规则操作确定何时以及如何记录有关匹配的流量的详细信息

不阻止操作

不阻止 (Do Not Block) 操作将允许流量传递到下一个检查阶段，即访问控制规则。

系统不会记录不阻止列表匹配项。是否记录这些连接取决于其最终的安全状态。

“监控”(Monitor) 操作

监控 (Monitor) 操作旨在强制执行连接日志记录；匹配的流量既不会被立即允许，也不会被阻止。更确切地是，根据其他规则匹配流量以确定允许还是拒绝该流量。所匹配的第一个非“监控”(Monitor) DNS 规则可确定系统是否阻止流量。如果没有其他匹配的规则，流量会进行访问控制评估。

对于 DNS 策略监控的连接，系统会记录连接结束的安全情报和 管理中心数据库的连接事件。

阻止操作

这些操作会阻止流量，无需任何类型的进一步检查：

- **丢弃 (Drop)** 操作会丢弃流量。
- **找不到域 (Domain Not Found)** 操作会针对 DNS 查询返回“不存在的互联网域”响应，防止客户端解析 DNS 请求。
- **Sinkhole** 操作会返回 Sinkhole 对象的 IPv4 或 IPv6 地址以响应 DNS 查询（仅限 A 和 AAAA 记录）。Sinkhole 服务器可以记录或记录并阻止 IP 地址的后续连接。如果配置 **Sinkhole** 操作，还必须配置 Sinkhole 对象。

对于根据**丢弃 (Drop)** 或**找不到域 (Domain Not Found)** 操作而被阻止的连接，系统会记录连接开始的安全情报和连接事件。因为被阻止的流量会被立即拒绝，无需进一步检测，所以，没有要记录的唯一连接终止。

对于根据 **Sinkhole** 操作阻止的连接，日志记录取决于 Sinkhole 对象配置。如果将 Sinkhole 对象配置为仅记录 Sinkhole 连接，则系统会记录后续连接的连接结束的连接事件。如果将 Sinkhole 对象配置为记录并阻止 Sinkhole 连接，则系统会记录后续连接的连接开始的连接事件，然后阻止该连接。

DNS 规则条件

DNS 规则的条件识别该规则处理的流量的类型。条件可以简单，也可以复杂。您必须在 DNS 规则中定义 DNS 源或列表条件。还可以选择按安全区域、网络或 VLAN 控制流量。

将条件添加到 DNS 规则时：

- 如果不为规则配置特定条件，系统将不基于此标准匹配流量。
- 您可以为每个规则配置多个条件。为使规则应用于流量，流量必须匹配规则中的**所有**条件。例如，包含 DNS 源或列表条件和网络条件，但没有 VLAN 标记条件的规则会根据域名以及源或目标评估流量，无论会话采用任何 VLAN 标记。
- 最多可以为规则中的每个条件添加50个标准。匹配**所有**条件的标准的流量满足该条件。例如，您可以使用单一规则根据最多 50 个 DNS 列表和源来阻止流量。

相关主题

安全区域规则条件，第 1380 页
网络规则条件，第 607 页
VLAN 标记规则条件，第 1292 页
DNS 规则条件，第 1381 页

安全区域规则条件

安全区域可对网络进行分段，以通过跨多个设备将接口分组来帮助管理和分类流量。

区域规则条件可根据其源和目标安全区域控制流量。如果将源区域和目标区域均添加到区域条件中，则匹配流量必须源自其中一个源区域的接口，并通过其中一个目标区域的接口流出。

正如区域中的所有接口都必须为同一类型（均为内联、被动、交换或路由），区域条件中使用的所有区域也必须为同一类型。由于被动部署的设备不会传输流量，因此不能使用具有被动接口的区域作为目标区域。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

提示 按区域限制规则是提高系统性能的一种最佳方式。如果规则不适用于通过设备任意接口的流量，则该规则不影响该设备的性能。

安全区域条件和多租户

在多域部署中，在祖先域中创建的区域可以包含位于不同域中的设备上的接口。在后代域中配置区域条件时，您的配置仅适用于可以看到的接口。

网络规则条件

网络规则条件使用内部报头按流量的源和目标 IP 地址来控制流量。使用外部报头的隧道规则具有隧道终端条件而不是网络条件。

您可以使用预定义对象构建网络条件，或手动指定单个 IP 地址或地址块。

注释 您 不能 在身份规则中使用 FDQN 网络对象。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

VLAN 标记规则条件

注释 访问规则中的 VLAN 标记仅适用于内联集。带 VLAN 标记的访问规则与防火墙接口上的流量不匹配。

VLAN 规则条件可控制 VLAN 标记的流量，包括 Q-in-Q（堆栈 VLAN）流量。系统使用最内层的 VLAN 标记过滤 VLAN 流量，但不包括预过滤器策略，因为它在其规则中使用最外层的 VLAN 标记。

请注意以下 Q-in-Q 支持：

- Firepower 4100/9300 上的威胁防御 -不支持 Q-in-Q （仅支持一个 VLAN 标记）。
- 所有其他型号上的威胁防御 ：
  - 内联集和被动接口-支持 Q-in-Q，最多2个 VLAN 标记。
  - 防火墙接口-不支持 Q-in-Q （仅支持一个 VLAN 标记）。

可以使用预定义对象构建 VLAN 条件，或手动输入从 1 到 4094 之间的任意 VLAN 标记。使用连字符可指定 VLAN 标记范围。

最多可以指定 50 个 VLAN 条件。

在集群中，如果遇到 VLAN 匹配问题，请编辑访问控制策略高级选项“传输/网络预处理器设置”(Transport/Network Preprocessor Settings)，然后选择**跟踪连接时忽略 VLAN 信头 (Ignore the VLAN header when tracking connections)** 选项。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 VLAN 标记限制此配置可产生意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

DNS 规则条件

如果 DNS 列表、源或类别包含客户端请求的域名，则 DNS 规则中的 DNS 条件可用于控制流量。您必须在 DNS 规则中定义 DNS 条件。

无论向 DNS 条件中添加全局或自定义阻止还是不阻止列表，系统都会将所配置的规则操作应用于流量。例如，如果向规则中添加全局不阻止列表，并配置**丢弃 (Drop)** 操作，则系统会阻止所有本应被允许进入下一阶段检查的流量。

如何创建 DNS 规则

以下主题讨论如何创建 DNS 规则。

相关主题

根据 DNS 和安全区域控制流量，第 1382 页
根据 DNS 和网络控制流量，第 1382 页
根据 DNS 和 VLAN 控制流量，第 1383 页
根据 DNS 列表或源来控制流量，第 1384 页

根据 DNS 和安全区域控制流量

通过DNS规则中的区域条件，您可以根据其源安全区域来控制流量。安全区域是一个或多个接口的分组，可位于多个设备之间。

过程

步骤 1 在 DNS 规则编辑器中，点击**区域 (Zones)**。

步骤 2 从 **Available Zones** 中查找并选择您想要添加的区域。要搜索需要添加的区域，请点击 **Available Zones** 列表上方的 **Search by name** 提示，然后键入区域名称。该列表会在您键入内容时进行更新，以显示匹配的区域。

步骤 3 点击选择一个区域，或右键点击，然后选择**全选 (Select All)**。

步骤 4 点击**添加到源 (Add to Source)**，或进行拖放操作。

步骤 5 保存或继续编辑规则。

下一步做什么

- 部署配置更改。

根据 DNS 和网络控制流量

DNS 规则中的网络条件可以根据源 IP 地址控制流量。您可以为要控制的流量显式指定源 IP 地址。

过程

步骤 1 在 DNS 规则编辑器中，点击**网络 (Networks)**。

步骤 2 从 **Available Networks** 中查找并选择您想要添加的网络，如下所示：

- 要即时添加可随后添加到条件中的网络对象，请点击**可用网络 (Available Networks)** 列表上方的**添加**（+），然后如创建网络对象，第 999 页中所述继续操作。
- 要搜索要添加的网络对象，请点击**可用网络**列表上方的**按名称或值搜索**提示，然后键入对象名称或对象的其中一个组件的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 3 点击**添加到源 (Add to Source)**，或进行拖放操作。

步骤 4 添加要手动指定的任何源 IP 地址或地址块。点击**源网络 (Source Networks)** 列表下方的**输入 IP 地址 (Enter an IP address)** 提示，然后键入 IP 地址或地址块，并点击**添加 (Add)**。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

步骤 5 保存或继续编辑规则。

下一步做什么

- 部署配置更改。

根据 DNS 和 VLAN 控制流量

通过 DNS 规则中的 VLAN 条件，您可以控制 VLAN 标记流量。系统使用最内部的 VLAN 标记来按照 VLAN 识别数据包。

构建基于 VLAN 的 DNS 规则条件时，可以手动指定 VLAN 标记。或者，也可以使用 VLAN 标记对象配置 VLAN 条件，这些对象可重用，并会将名称与一个或多个 VLAN 标记相关联。

过程

步骤 1 在 DNS 规则编辑器中，选择 **VLAN 标记 (VLAN Tags)**。

步骤 2 查找并选择您要从 **Available VLAN Tags** 添加的 VLAN，如下所述：

- 要即时添加可随后添加到条件中的 VLAN 标记，请点击“可用 VLAN 标记”(Available VLAN Tags) 列表上方的 **添加**（＋） 并继续操作，如创建 VLAN 标记对象，第 1057 页中所述。
- 要搜索将添加的 VLAN 标记对象和组，请点击 **Available VLAN Tags** 列表上方的 **Search by name or value** 提示，然后键入对象的名称或对象中 VLAN 标记的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 3 点击**添加到规则 (Add to Rule)**，或进行拖放操作。

步骤 4 添加要手动指定的任何 VLAN 标记。点击**所选 VLAN 标记 (Selected VLAN Tags)** 列表下方的**输入 VLAN 标记 (Enter a VLAN Tag)** 提示，然后键入 VLAN 标记或范围并点击**添加 (Add)**。您可以指定介于 1 和 4094 之间的任何 VLAN 标记；使用连字符指定 VLAN 标记的范围。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 VLAN 标记限制此配置可产生意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

步骤 5 保存或继续编辑规则。

下一步做什么

- 部署配置更改。

根据 DNS 列表或源来控制流量

过程

步骤 1 在 DNS 规则编辑器中，点击 **DNS**。

步骤 2 从 **DNS 列表和源 (DNS Lists and Feeds)** 中查找并选择要添加的 DNS 列表和源，如下所示：

- 要动态添加可随后添加到条件中的 DNS 列表和源，请点击 **DNS 列表和源 (DNS Lists and Feeds)** 列表上方的 **添加**（+），然后如创建安全情报源，第 1033 页中所述继续操作。
- 要搜索将添加的 DNS 列表、源或类别，请点击 **DNS 列表和源** 列表上方的 **按名称或值搜索** 提示，然后键入对象名称或其中一个对象的组件的值。列表会在您键入内容时进行更新，以显示匹配的对象。
- 有关系统提供的威胁类别的说明，请参阅安全情报类别，第 1365 页。

步骤 3 点击**添加到规则 (Add to Rule)**，或进行拖放操作。

步骤 4 保存或继续编辑规则。

下一步做什么

- 部署配置更改。

DNS 策略部署

完成 DNS 策略配置更新后，您必须将其部署为访问控制配置的一部分。

- 将 DNS 策略与访问控制策略相关联，如配置安全情报，第 1362 页中所述。
- 部署配置更改。

Cisco Umbrella DNS 策略

管理中心中的 Cisco Umbrella DNS 连接有助于将 DNS 查询重定向到Cisco Umbrella。这使 Cisco Umbrella 可以根据域名验证请求是被允许还是被阻止，并对请求应用基于 DNS 的安全策略。如果使用 Cisco Umbrella，则必须配置 Cisco Umbrella 连接，将 DNS 查询重定向到 Cisco Umbrella。

Umbrella 连接器是系统 DNS 检测的一部分。如果现有 DNS 检测策略映射决定根据 DNS 检测设置阻止或丢弃请求，则该请求不会转发至思科 Umbrella。因此，您有两条防线：

- 您的本地 DNS 检测策略
- Cisco Umbrella 基于云的策略

将 DNS 查询请求重定向到思科 Umbrella 时，Umbrella 连接器会添加 EDNS （DNS 扩展机制） 记录。EDNS 记录包括设备标识符信息、 组织 ID 和客户端 IP 地址。基于云的策略可以使用 FQDN 信誉以及这些标准来控制访问。还可以选择使用 DNSCrypt 加密 DNS 请求，以确保用户名和内部 IP 地址的隐私性。

有关如何在管理中心设置 Umbrella DNS 连接器的详细信息，请参阅为 Cisco Secure Firewall Management Center 配置 Umbrella DNS 连接器。

如何将 DNS 请求重定向到 Cisco Umbrella

本节提供使用 管理中心 将 DNS 请求从设备重定向到 Cisco Umbrella 的说明。

步骤	相应操作	更多信息
1	确保您已满足前提条件。	配置 Umbrella DNS 连接器的前提条件， 第 1385 页
2	配置 Cisco Umbrella 连接设置。	配置 Cisco Umbrella 连接设置， 第 1386 页
3	创建 Umbrella DNS 策略	创建 Umbrella DNS 策略， 第 1387 页
4	配置 Umbrella DNS 策略	编辑 Cisco Umbrella DNS 策略和规则， 第 1387 页
5	将 Umbrella DNS 策略与访问控制策略相关联	将 Umbrella DNS 策略与访问控制策略相关联， 第 1388 页

配置 Umbrella DNS 连接器的前提条件

表 *98:* 支持的最低平台

Product	版本
Cisco Secure Firewall Threat Defense	6.6 及更高版本
Cisco Secure Firewall Management Center	7.2 及更高版本

- 在 https://umbrella.cisco.com上建立 Cisco Umbrella 帐户，然后在 http://login.umbrella.com上登录 Umbrella。
- 将 CA 证书从 Cisco Umbrella 服务器导入 管理中心。在 Cisco Umbrella 中，选择**部署 (Deployments)** > **配置 (Configuration)** > **根证书 (Root Certificate)** 并下载证书。

必须导入根证书，才能与思科 Umbrella 注册服务器建立 HTTPS 连接。证书需要受信任才能进行 SSL 服务器验证，这是管理中心中的非默认选项。将设备的证书复制并粘贴到 管理中心（**设备 (Device) > 证书 (Certificates)**）中。

- 在设备上安装证书。
- 从 Umbrella 获取以下数据：
  - 组织 ID
  - 网络设备密钥
  - 网络设备密钥
  - 旧版网络设备令牌
- 确保 管理中心 已连接到互联网。
- 确保已在 管理中心 中启用具有出口控制功能选项的基础许可证。
- 确保配置 DNS 服务器以解析 api.opendns.com。
- 确保 管理中心 可以解析 management.api.umbrella.com 以进行策略配置。
- 配置到 api.opendns.com 的 威胁防御 路由。

配置 Cisco Umbrella 连接设置

思科 Umbrella 连接设置定义了在思科 Umbrella 中注册设备时所需的 API 令牌。

开始之前

使用思科 Umbrella https://umbrella.cisco.com 建立账户，然后通过 https://dashboard.umbrella.com 登录 Umbrella，获取与思科 Umbrella 建立连接所需的信息。

过程

步骤 1 选择**集成 (Integration)** > **其他集成 (Other Integrations)** > **云服务 (Cloud Services)** > **思科 Umbrella 连接 (Cisco Umbrella Connection)**。

步骤 2 获取以下详细信息并将其添加到**常规 (General)** 设置中：

- **组织 ID (Organization ID)** - 在思科 Umbrella 上标识您的组织的唯一编号。每个 Umbrella 组织都是一个单独的 Umbrella 实例，并且有自己的控制面板。组织通过其名称和组织 ID（组织 ID）进行标识。
- **网络设备密钥 (Network Device Key)** - 从思科 Umbrella 获取 Umbrella 策略的密钥。
- **网络设备密钥 (Network Device Secret)** - 从思科 Umbrella 获取 Umbrella 策略的密钥。

- **传统网络设备令牌 (Legacy Network Device Token)** - 通过思科 Umbrella 控制面板颁发 Umbrella 传统网络设备 API 令牌。Umbrella 需要 API 令牌才能注册网络设备。

步骤 3 在**高级 (Advanced)** 下，配置以下可选设置：

- **DNSCrypt 公钥 (DNSCrypt Public Key)** - DNSCrypt 对终端和 DNS 服务器之间的 DNS 查询进行身份验证和加密。要启用 DNScrypt，您可以为证书验证配置 DNScrypt 公钥。密钥是一个 32 字节的十六进制值，预配置为 B735:1140:206F:225d:3E2B:d822:D7FD:691e:A1C3:3cc8:D666:8d0c:BE04:bfab:CA43:FB79，即公钥的 Umbrella 任播服务器。
- **管理密钥 (Management Key)** - 从 Umbrella 云获取 VPN 策略的数据中心详细信息的密钥。
- **管理秘密 (Management Secret)** - 用于从 Umbrella 云获取 VPN 数据中心的秘密。

步骤 4 点击**测试连接 (Test Connection)** - 测试是否可从 管理中心 访问 Cisco Umbrella Cloud。在提供所需的组织 ID 和网络设备详细信息时，您会创建 Umbrella 连接。

步骤 5 点击**保存 (Save)**。

创建 Umbrella DNS 策略

过程

步骤 1 选择**策略** > **访问控制** > **DNS**。

步骤 2 点击**添加 DNS 策略 (Add DNS Policy)** > **Umbrella DNS 策略 (Umbrella DNS Policy)**。

步骤 3 在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。

步骤 4 点击**保存 (Save)**。

下一步做什么

配置策略。请参阅编辑 Cisco Umbrella DNS 策略和规则，第 1387 页。

编辑 Cisco Umbrella DNS 策略和规则

过程

步骤 1 选择**策略** > **访问控制** > **DNS**。

步骤 2 在“DNS 策略”(DNS Policy) 页面上，选择要编辑的 Umbrella DNS 策略，然后点击 **编辑**（）。

刷新 Umbrella 保护策略

如果要从思科 Umbrella 获取最新的 Umbrella 保护策略，请点击**上次更新 Umbrella 保护策略 (Umbrella Protection Policy Last Updated)** 旁边的**刷新 (Refresh)** 图标。

要配置或修改管理中心的 Umbrella 连接设置，请转至**集成 (Integration)** > **其他集成 (Other Integrations)** > **云服务 (Cloud Services)** > **思科 Umbrella 连接 (Cisco Umbrella Connection)**。

步骤 3 在 Cisco Umbrella DNS 策略编辑器中，选择 Umbrella DNS 规则并点击 **编辑**（✎）。

步骤 4 配置规则组成部分，或接受默认值：

- **Umbrella 保护策略 (Umbrella Protection Policy)** - 指定要应用于设备的思科 Umbrella 策略的名称。
- **绕过域 (Bypass Domain)** - 指定 DNS 请求应绕过思科 Umbrella 直接转至所配置的 DNS 服务器的本地域。

  例如，假设允许所有内部连接，可以借助内部 DNS 服务器解析组织域名的所有名称。
- **DNSCrypt** - 启用 DNSCrypt，以便为设备和思科 Umbrella 之间的连接加密。

  启用 DNScrypt 将使用 Umbrella 解析器启动密钥交换线程。密钥交换线程每小时执行与解析器的握手，并使用新密钥来更新设备。由于 DNScrypt 使用 UDP/443，您必须确保用于 DNS 检测的类映射包含该端口。请注意，默认检测类已在 DNS 检测中包括 UDP/443。
- **空闲超时 (Idle Timeout)** - 配置当服务器没有响应时，在删除从客户端至 Umbrella 服务器的连接之前的空闲超时。

步骤 5 点击**保存 (Save)**。

下一步做什么

将 Umbrella DNS 策略与访问控制策略相关联有关详细信息，请参阅将 Umbrella DNS 策略与访问控制策略相关联，第 1388 页。

将 Umbrella DNS 策略与访问控制策略相关联

在设备上部署 Umbrella DNS 策略之前，必须将其与访问控制策略相关联。

过程

步骤 1 选择**策略 (Policies) 访问控制 (Access Control)**，然后选择要编辑的访问策略。

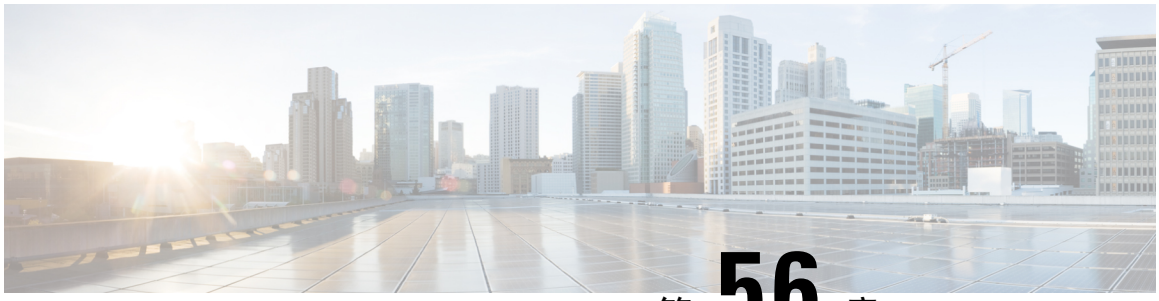
步骤 2 选择**安全智能 (Security Intelligence)**。

步骤 3 从 **Umbrella DNS 策略 (Umbrella DNS Policy)** 下拉列表中选择 Umbrella DNS 策略。

步骤 4 点击**保存 (Save)**。

下一步做什么

部署配置更改；请参阅部署配置更改，第 136 页。



第 56 章

预过滤和预过滤策略

关于预过滤

在系统执行更多资源密集型评估之前，预过滤是访问控制的第一阶段。预过滤非常简单、快速并且可以及早执行。预过滤使用有限的外部报头条件来快速处理流量。将此过滤操作与后续评估进行比较，后续评估使用内部报头并具有更强大的检测功能。

配置预过滤：

- 提高性能 - 越早排除不需要检查的流量，越好。您可以基于隧道的外部封装报头传递隧道为某些类型的明文设置快速路径或加以阻止，而不检查其封装的连接。您还可以为从及早处理中受益的其他任何连接设置快速路径或加以阻止。
- 为封装流量定制深度检查 - 您可以对某些类型的隧道重新分区，以便以后可以使用相同的检查标准处理其封装的连接。重新分区是必要的，因为在预过滤后，访问控制使用内部报头。

关于预过滤策略

预过滤是一种基于策略的功能。要将它分配给设备，请将其分配给分配给该设备的访问控制策略。

策略要素：规则和默认操作

在预过滤策略中，隧道规则、预过滤规则和默认操作处理网络流量：

- 隧道和预过滤规则 - 首先，预过滤策略中的规则按您指定的顺序处理流量。隧道规则只与特定隧道匹配，并支持重新分区。预过滤规则的约束范围更广，不支持重新分区。有关详细信息，请参阅隧道与预过滤器规则，第 1392 页。
- 默认操作（仅限隧道）- 如果隧道不与任何规则匹配，则对隧道应用默认操作。默认操作可以阻止这些隧道，或继续对其单独封装的连接进行访问控制。不能使用默认操作对隧道重新分区。

  没有用于未封装流量的默认操作。如果未封装的连接与任何预过滤规则都不匹配，系统将继续进行访问控制。

连接日志记录

您可以记录被预过滤策略使用快速路径或阻止的连接。

连接事件包含有关记录的连接（包括整个隧道）是否被预过滤以及如何预过滤的信息。您可以在事件视图（工作流）、仪表板和报表中查看此信息，并将其用作关联标准。注意，由于被快速路径和阻止的连接不进行深度检查，因此关联的连接事件包含的信息有限。

默认预过滤策略

每个访问控制策略都有一个关联的预过滤策略。

如果不配置自定义预过滤，系统将使用默认策略。最初，此系统提供的策略将所有流量传递到访问控制的下一阶段。您可以更改策略的默认操作并配置其日志记录选项，但不能向其添加规则或将其删除。

预过滤策略继承和多租户

访问控制使用基于分层的实施，完善了多租户策略。除了其他高级设置之外，您还可以锁定预过滤策略关联，在所有子代访问控制策略中实施该关联。有关详细信息，请参阅访问控制策略继承，第 1247 页。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。默认的预过滤策略属于全局域。

隧道与预过滤器规则

配置隧道规则还是预过滤器规则取决于要匹配的特定流量类型和要执行的操作或进一步分析。

特征	隧道规则	预过滤器规则
主要功能	对明文传递隧道快速使用快速路径、加以阻止或重新分区。	对从早期处理中受益的其他任何连接快速使用快速路径或加以阻止。
封装和端口/协议标准	封装条件只与所选协议上的明文隧道匹配，请参阅封装规则条件，第 1403 页。	与隧道规则相比，端口规则可以使用范围更广泛的端口和协议限制；请参阅端口、协议和 ICMP 代码规则条件，第 609 页。

特征	隧道规则	预过滤器规则
网络标准	隧道终端条件限制要处理的隧道的终端；请参阅网络规则条件，第 607 页。	网络条件限制每个连接中的源主机和目标主机；请参阅网络规则条件，第 607 页。
方向	双向或单向（可配置）。 默认情况下，隧道规则是双向的，这样便于它们处理隧道终端之间的所有流量。	仅单向（不可配置）。 预处理器规则只与源到目标流量匹配。
对会话进行重新分区以便进一步分析	支持，使用隧道区域；请参阅隧道区域与预过滤，第 1403 页。	不支持。

预过滤与访问控制

预过滤和访问控制策略都允许您阻止和信任流量，但预过滤“信任”功能被称为“快速路径”，因为它会跳过更多检查。下表说明了这一点以及预过滤与访问控制之间的其他差异，以帮助您决定是否配置自定义预过滤。

如果不配置自定义预过滤，则只能在访问控制策略中使用早期放置的“阻止”和“信任”规则来接近而非复制预过滤功能。

特征	预过滤	访问控制	有关详细信息，请参阅.....
主要功能	对特定类型的明文、直通隧道快速使用快速路径或加以阻止（请参阅封装规则条件，第 1403 页），或针对其封装的流量定制后续检查。 对从早期处理中受益的其他任何连接使用快速路径或加以阻止。	使用简单或复杂的条件检查和控制所有网络流量，包括情景信息和深度检查结果。	关于预过滤，第 1391 页
实施	预过滤策略。 预过滤策略由访问控制策略调用。	访问控制策略。 访问控制策略是主配置。除了调用子策略，访问控制策略还具有自己的规则。	关于预过滤策略，第 1391 页 将其他策略与访问控制相关联，第 1276 页
访问控制中的序列	首先。 在所有其他访问控制配置之前，系统会将流量与预过滤条件匹配。	-	-

特征	预过滤	访问控制	有关详细信息，请参阅.....
规则操作	更少。 您可以停止进一步检查（快速路径和阻止），或对其余访问控制允许进一步分析（分析）。	更多。 访问控制规则有更广泛的操作，包括监控、深度检查、阻止并重置和交互式阻止。	隧道和预过滤器规则组成部分，第 1399 页 访问控制规则操作，第 1284 页
绕过功能	快速路径规则操作。 在预过滤阶段为流量使用快速路径可绕过所有进一步检查和处理，包括： • 安全情报 • 身份策略强加的身份验证要求 • SSL 解密 • 访问控制规则 • 对数据包负载的深度检验 • 能源成本 • 速率限制	信任规则操作。 访问控制规则信任的流量仅免于深度检查和发现。	访问控制规则简介，第 1279 页
规则条件	限制版。 预过滤策略中的规则使用简单网络条件：IP 地址、VLAN 标记、端口和协议。 对于隧道，隧道终端条件会指定隧道任一端上网络设备的路由接口的 IP 地址。	强健。 访问控制规则使用网络条件，但同时也采用用户、应用、请求的 URL 和数据包负载中可用的其他情景信息。 网络条件指定源和目标主机的 IP 地址。	隧道与预过滤器规则，第 1392 页 预过滤器规则条件，第 1400 页 隧道规则条件，第 1403 页
使用的 IP 报头（隧道处理）	最外层。 使用外部报头使您可以处理整个明文、直通隧道。 对于未封闭的流量，预过滤仍使用“外部”标头 - 在这种情况下，它们是唯一报头。	尽可能在内部。 对于未加密隧道，访问控制作用于其各个封装的连接，而不是作用于整个隧道。	传递隧道和访问控制，第 1395 页
对封装的连接重新分区以进行进一步分析	重新分区隧道传输的流量。 隧道区域允许您对预过滤的封装流量定制后续检查。	使用隧道区域。 访问控制使用在预过滤期间分配的隧道区域。	隧道区域与预过滤，第 1403 页

特征	预过滤	访问控制	有关详细信息，请参阅.....
连接日志记录	仅使用快速路径和阻止的流量。允许的连接仍然可由其他配置进行记录。	任何连接。	
支持的设备	仅限 Cisco Secure Firewall Threat Defense。	All.	—

传递隧道和访问控制

明文（非加密）隧道可以封装多个连接，通常在非连续网络之间流动。这些隧道对通过 IP 网络的路由自定义协议、通过 Ipv4 网络的 IPv6 流量等尤其有用。

外部封装报头指定隧道终端（隧道任一端的网络设备的路由接口）的源 IP 地址和目标 IP 地址。内部负载报头指定封装连接的实际终端的源 IP 地址和目标 IP 地址。

通常，网络安全设备将明文隧道处理为传递流量。也就是说，设备不是隧道终端之一。该设备部署在隧道终端之间，用于监控终端之间流动的流量。

某些网络安全设备（例如运行思科 ASA 软件[而不是 Cisco Secure Firewall Threat Defense]的思科 ASA 防火墙）可使用外部 IP 报头实施安全策略。即使对于明文隧道，这些设备也不能控制或洞察各个封装连接及其负载。

相比之下，Firepower 系统可利用访问控制进行以下操作：

- 外部报头评估 - 首先，预过滤使用外部报头处理流量。可以对此阶段的整个明文、传递隧道进行阻止或使用快速路径。
- 内部报头评估 - 然后，其余访问控制（和 QoS 等其他功能）使用报头最深处可检测的级别确保实现最精细的检测和处理。

  如果传递隧道未加密，则系统会在此阶段对它的各个封装连接执行操作。您必须对隧道进行重新分区（请参阅隧道区域与预过滤，第 1403 页）以对其所有封装连接执行操作。

访问控制无法洞察已加密的传递隧道。例如，访问控制规则会将一个传递 VPN 隧道看做一个连接。系统仅使用其外部封装报头中的信息处理整个隧道。

快速路径预过滤的最佳实践

在预过滤器规则中使用快速路径操作时，匹配的流量会绕过检查并直接通过设备进行传输。请对您可以信任但不会受益于任何可用安全功能的流量使用此操作。

以下类型的流量是快速路径的理想选择。例如，您可以将规则配置为对来自或到达终端或服务器的 IP 地址的任何流量进行快速路径处理。您可以根据使用的端口来进一步限制规则。

- 通过设备的站点间 VPN 流量。也就是说，该设备不是 VPN 拓扑中的终端。
- 扫描程序流量。扫描程序探测可以从入侵策略中创建大量误报响应。

- 语音/视频。
- 备份。
- 流经 威胁防御 设备的管理流量。对管理流量执行深度检查（使用访问控制策略）可能会导致问题。

封装流量处理的最佳实践

本主题讨论以下类型的封装流量的准则：

- 通用路由封装 (GRE)
- 点对点协议 (PPTP)
- IPinIP
- IPv6inIP
- Teredo

了解托管设备的 Snort 版本支持

托管设备使用的检测引擎被称为 Snort。Snort 3 支持的功能比 Snort 2 多。要了解这些因素如何影响网络上的托管设备，您必须了解：

- 您的设备支持哪些版本的 Snort。

  Snort 版本支持可以在《思科 *Firepower*兼容性指南》中关于捆绑组件的部分找到。

- 管理中心 和 威胁防御 软件如何支持 Snort 2 和 Snort 3

  有关 Snort 2 和 Snort 3 的限制，请参阅《Cisco Secure Firewall Management Center Snort 3 配置指南》中的适用于 管理中心 管理的 威胁防御 的 *Snort 3* 的功能限制主题。

GRE v1 和 PPTP 会绕过外部流处理

GRE v1（有时称为状态性 *GRE*）和 PPTP 流量会绕过外部流处理。

IPv6inIP 和 Teredo 支持客流处理，但存在以下限制：

- 会话位于未进行负载均衡的单个隧道上
- 没有 HA 或集群复制
- 不维护主要和辅助流关系
- 不支持预过滤策略白名单和黑名单

GRE v0 序列号字段必须为可选

在网络上发送流量的所有终端都必须发送带有可选序列号字段的GREv0流量；否则，序列号字段会被删除。RFC 1701 和 RFC 2784 都将序列字段指定为可选。

隧道如何与接口配合使用

预过滤器和访问控制策略规则适用于路由、透明、内联集、内联分流和被动接口上的所有隧道类型。

参考资料

有关 GRE 和 PPTP 协议的详细信息，请参阅以下内容：

- RFC 1701、RFC 2784 和 RFC 2890（GRE 协议 v0）
- RFC 2637（PPTP 和 GRE 协议 v1）

预过滤器策略的要求和必备条件

型号支持

威胁防御

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

配置预过滤

要执行自定义预过滤，请配置预过滤策略并将策略分配给访问控制策略。预过滤器策略是通过访问控制策略分配给受管设备的。

一个用户一次只能使用一个浏览器窗口编辑一个策略。如果多个用户保存同一个策略，系统会保留最后的更改。为方便起见，系统会显示有关当前正在编辑每条策略的人员（如有任何人）的信息。为保护会话隐私，当策略编辑器 30 分钟无任何活动后，系统将显示警告。60 分钟后，系统将放弃更改。

过程

步骤 1 选择**策略** > **访问控制** > **预过滤器**。

步骤 2 点击**新建策略 (New Policy)** 以创建自定义预过滤器策略。

新的预过滤器策略不包含规则及“分析所有隧道流量”(Analyze all tunnel traffic) 这一默认操作。它不执行日志记录或隧道重新分区。您也可以 **复制**（） 或 **编辑**（） 现有策略。

步骤 3 配置预过滤器策略的默认操作及其日志记录选项。

- 默认操作 - 为受支持的明文、传递隧道选择默认操作：**分析所有隧道流量 (Analyze all tunnel traffic)**（具有访问控制）或**阻止所有隧道流量 (Block all tunnel traffic)**。
- 默认操作日志记录 - 点击默认操作旁边的 **日志记录**（）。您只能为被阻止的隧道配置默认操作日志记录。

步骤 4 配置隧道规则和预过滤器规则。

在自定义预过滤器策略中，可以按任意顺序使用这两种规则。根据要匹配的具体流量类型和要执行的操作或进一步分析创建规则；请参阅隧道与预过滤器规则，第 1392 页。

注意 使用隧道规则分配隧道区域时应格外小心。在之后进行评估时，重新分区后的隧道中的连接可能与安全区域限制不匹配。有关详细信息，请参阅隧道区域与预过滤，第1403页。

有关配置规则组成部分的详细信息，请参阅 隧道和预过滤器规则组成部分，第 1399 页。

步骤 5 评估规则顺序。要移动规则，请点击并拖动，或使用右键点击菜单进行剪切并粘贴。

正确创建规则并将其排序是一项复杂的任务，但却是构建有效部署的一项重要任务。如果您未缜密地计划，有些规则可能会抢占其他规则，或者包含无效的配置。有关详细信息，请参阅访问控制规则的最佳实践，第 1253 页。

步骤 6 保存预过滤器策略。

步骤 7 对于支持隧道区域限制的配置，请适当处理重新分区后的隧道。

通过将隧道区域用作源区域限制来匹配重新分区后的隧道中的连接。

步骤 8 关联预过滤器策略与部署到受管设备的访问控制策略。

请参阅将其他策略与访问控制相关联，第 1276 页。

步骤 9 部署配置更改。

注释 部署预过滤器策略时，其规则不会应用于现有隧道会话。因此，现有连接上的流量不受部署的新策略的限制。此外，仅对匹配策略的连接的第一个数据包增加策略命中计数。因此，从命中计数中忽略了可能与策略匹配的现有连接上的流量。要有效应用策略规则，请清除现有隧道会话，然后部署策略。

下一步做什么

如果要部署基于时间的规则，请指定策略分配到的设备的时区。请参阅为策略应用配置设备时区，第 662 页。

隧道和预过滤器规则组成部分

状态（启用/禁用）

默认情况下，规则处于启用状态。如果禁用某规则，系统将不使用该规则并停止为该规则生成警告和错误。

位

规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。流量匹配的第一条规则是处理该流量的规则，无论规则是何类型（隧道与预过滤器）。

操作

规则操作确定系统如何处理和记录匹配的流量。

- 快速路径 - 让匹配流量免于进行所有进一步检查和控制，包括访问控制、身份要求和速率限制。对隧道执行快速路径操作可为所有封装连接提供快速路径。
- 阻止 - 阻止匹配流量，不进行任何类型的进一步检查。阻止隧道将阻止所有封装连接。
- 分析 - 允许其余访问控制继续使用内部报头分析流量。即使流量被访问控制和所有相关深度检查放行，也可能会受到速率限制。对于隧道规则，使用“分配隧道区域”(Assign Tunnel Zone) 选项启用重新分区。

方向（仅限隧道规则）

隧道规则的方向用于确定系统源和目标条件：

- 仅从源匹配隧道（单向）- 仅匹配源到目标的流量。匹配流量必须源自其中一个指定的源接口或隧道终端，并通过其中一个目标接口或隧道终端流出。
- 从源和目标匹配隧道（双向）- 同时匹配源到目标的流量和目标到源的流量。其效果与编写两个互为镜像的单向规则相同。

预过滤器规则始终是单向的。

分配隧道区域（仅限隧道规则）

在隧道规则中，分配隧道区域（无论是现有的还是即时创建的）会对匹配隧道进行重新分区。重新分区需要“分析”(Analyze) 操作。

对隧道进行重新分区允许其他配置（例如访问控制策略）识别隧道中所有互相归属的封装连接。通过将隧道的已分配隧道区域用作接口限制，可以针对其封装连接定制检查。有关详细信息，请参阅隧道区域与预过滤，第 1403 页。

⚠

注意 分配隧道区域时应格外小心。在之后进行评估时，重新分区后的隧道中的连接可能与安全区域限制不匹配。请参阅使用隧道区域，第 1404 页，查看隧道区域实施的简要步骤，以及对在不明确处理重新分区流量的情况下进行重新分区的影响的说明。

条件

条件指定规则处理的特定流量。流量必须匹配所有规则条件才能与规则匹配。每种条件类型在规则编辑器中都有自己的选项卡。

您可以使用以下 外部报头 限制预过滤流量。您必须按照封装协议限制隧道规则。

- 接口 -接口规则条件，第 606 页
- 网络（预过滤器规则）/隧道终端（隧道规则）-网络规则条件，第 607 页
- VLAN -VLAN 标记规则条件，第 1292 页
- 端口（预过滤器规则）/封装和端口（隧道规则）-预过滤器规则的端口规则条件，第 1402 页 或 封装规则条件，第 1403 页
- 时间范围-时间和日期规则条件，第 1298 页

日志记录

规则的日志记录设置管理系统保存其处理流量的记录。

在隧道和预过滤器规则中，您可以记录快速路径流量和受阻流量（“快速路径”[Fastpath] 和“阻止”[Block] 操作）。对于需要接受进一步分析（“分析”[Analyze] 操作）的流量，预过滤器策略中的日志记录功能被禁用，但匹配连接可能仍然被其他配置记录下来。日志记录在内部流上执行，而不是在封装流上执行。

备注

每次保存对规则所做的更改时，都可以添加备注。例如，您可为其他用户汇总整体配置，或者当您变更规则和更改的原因时进行记录。

保存规则后，您无法编辑或删除相关备注。

相关主题

访问控制规则的最佳实践，第 1253 页

预过滤器规则条件

通过规则条件，您可以微调预过滤器策略，以您要控制的网络为目标。有关详细信息，请参阅以下各节之一：

接口规则条件

接口规则条件按流量的源接口和目标接口控制流量。

根据规则类型和部署中的设备，您可以使用名为 安全区域 或 接口组 的预定义 接口对象 构建接口条件。接口对象对网络进行分段，以通过跨多个设备将接口分组来帮助管理和分类流量；请参阅接口，第 995 页。

提示 按接口限制规则是提高系统性能的一种最佳方式。如果规则排除了某个设备的所有接口，则该规则不影响该设备的性能。

正如接口对象中的所有接口都必须为同一类型（均为内联、被动、交换、路由或ASA FirePOWER），接口条件中使用的所有接口对象也必须为同一类型。由于被动部署的设备不会传输流量，因此无法在被动部署中按目标接口限制规则。

网络规则条件

网络规则条件使用内部报头按流量的源和目标IP地址来控制流量。使用外部报头的隧道规则具有隧道终端条件而不是网络条件。

您可以使用预定义对象构建网络条件，或手动指定单个 IP 地址或地址块。

注释 您 不能 在身份规则中使用 FDQN 网络对象。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字IP地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

VLAN 标记规则条件

注释 访问规则中的 VLAN 标记仅适用于内联集。带 VLAN 标记的访问规则与防火墙接口上的流量不匹配。

VLAN 规则条件可控制 VLAN 标记的流量，包括 Q-in-Q（堆栈 VLAN）流量。系统使用最内层的 VLAN 标记过滤 VLAN 流量，但不包括预过滤器策略，因为它在其规则中使用最外层的 VLAN 标记。

请注意以下 Q-in-Q 支持：

- Firepower 4100/9300 上的威胁防御 -不支持 Q-in-Q （仅支持一个 VLAN 标记）。

- 所有其他型号上的威胁防御：
  - 内联集和被动接口-支持 Q-in-Q，最多2个 VLAN 标记。
  - 防火墙接口-不支持 Q-in-Q （仅支持一个 VLAN 标记）。

可以使用预定义对象构建 VLAN 条件，或手动输入从 1 到 4094 之间的任意 VLAN 标记。使用连字符可指定 VLAN 标记范围。

最多可以指定 50 个 VLAN 条件。

在集群中，如果遇到 VLAN 匹配问题，请编辑访问控制策略高级选项“传输/网络预处理器设置”(Transport/Network Preprocessor Settings)，然后选择**跟踪连接时忽略 VLAN 信头 (Ignore the VLAN header when tracking connections)** 选项。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 VLAN 标记限制此配置可产生意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

预过滤器规则的端口规则条件

端口条件根据源和目标端口匹配流量。根据规则类型，“端口”可以表示以下任何一项：

- TCP 和 UDP - 可以根据端口控制 TCP 和 UDP 流量。系统使用括号内的协议号，以及可选的关联端口或端口范围来表示此配置。例如：TCP(6)/22。
- ICMP - 可以根据 ICMP 和 ICMPv6 (IPv6-ICMP) 流量的互联网层协议及可选类型和代码控制该流量。例如：ICMP(1):3:3。
- 协议-您可以借助于未使用端口的其他协议控制流量。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为目标端口条件。

将非 TCP 流量与端口条件相匹配

您可以匹配非基于端口的协议。默认情况下，如果不指定端口条件，则匹配 IP 流量。虽然可以配置端口条件以匹配预过滤器规则中的其他协议，但在匹配 GRE、IP in IP、IPv6 in IP 和 Toredo 端口 3544 时，应改为使用隧道规则。

时间和日期规则条件

您可以指定连续时间范围或周期性时间段。

例如，规则只能在工作日工作时间或每个周末或节假关闭期间应用。

基于时间的规则基于处理流量的设备的本地时间应用。

基于时间的规则仅在 FTD 设备上受支持。如果将具有基于时间的规则的策略分配给不同类型的设备，则在该设备上会忽略与该规则关联的时间限制。在这种情况下，您将看到警告。

隧道规则条件

通过规则条件，您可以微调隧道策略，以您要控制的网络为目标。对于隧道规则，您可以使用以下条件：

- **接口对象 (Interface Objects)** - 定义连接所通过的设备接口的安全区域或接口组。请参阅接口规则条件，第 606 页。
- **隧道终端 (Tunnel Endpoints)** - 定义隧道的源和目标 IP 地址的网络对象。
- **VLAN 标记 (VLAN Tags)** - 隧道中最外层的 VLAN 标记。请参阅VLAN 标记规则条件，第 1292 页。
- **封装和端口 (Encapsulation and Ports)** - 隧道的封装协议。请参阅封装规则条件，第 1403 页。
- **时间范围 (Time Range)** - 规则处于活动状态的日期和时间。如果不指定时间范围，规则将始终处于活动状态。请参阅时间和日期规则条件，第 1298 页。

封装规则条件

封装条件特定于隧道规则。

这些条件通过其封装协议控制某些类型的明文、传递隧道。必须先至少选择一个协议进行匹配，然后才能保存规则。您可以选择：

- GRE (47)
- IP-in-IP (4)
- IPv6-in-IP (41)
- Teredo (UDP (17)/3455)

隧道区域与预过滤

隧道区域允许您使用预过滤针对封装连接定制后续流量处理。

由于通常情况下，系统使用报头最深处可检测的级别处理流量，因此这需要用到特殊机制。这可确保尽可能进行最精细的检查。但同时这也意味着，如果传递隧道未加密，系统会对其各个封装连接执行操作；请参阅传递隧道和访问控制，第 1395 页。

隧道区域可解决此问题。在访问控制的第一阶段（预过滤），您可以使用外部报头识别特定类型的明文传递隧道。然后，可通过分配自定义隧道区域对这些隧道进行重新分区。

对隧道进行重新分区允许其他配置（例如访问控制策略）识别隧道中所有互相归属的封装连接。通过将隧道的已分配隧道区域用作接口限制，可以针对其封装连接定制检查。

尽管名称相似，但隧道区域不是安全区域。隧道区域不代表一组接口。将隧道区域理解为在某些情况下替换与封装连接关联的安全区域的标记更为准确。

⚠

注意 对于支持隧道区域限制的配置，重新分区后的隧道中的连接与安全区域限制**不**匹配。例如，在对某个隧道进行重新分区后，访问控制规则可将其封装连接与这些连接新分配的隧道区域相匹配，而不与任何原始安全区域相匹配。

请参阅使用隧道区域，第 1404 页，查看隧道区域实施的简要步骤，以及对在不明确处理重新分区流量的情况下进行重新分区的影响的说明。

支持隧道区域限制的配置

只有访问控制规则支持隧道区域限制。

其他配置均不支持隧道区域限制。例如，您不能使用 QoS 对整个明文隧道进行速率限制，而只能对其单独的封装会话进行速率限制。

使用隧道区域

此操作步骤示例总结了如何对GRE隧道进行重新分区，以便使用隧道区域执行进一步分析。您可以将此示例中描述的概念加以调整并应用到需要根据明文、传递隧道中封装的连接定制流量检查的其他情景中。

设想一种情形，在该情形中，您组织的内部流量流过受信任的安全区域。受信任的安全区域表示部署在不同地方的多个受管设备上的一组接口。您组织的安全策略要求您在对漏洞和恶意软件进行深度检查后允许内部流量。

内部流量有时包含特定终端之间的明文、传递及 GRE 隧道。由于此封装流量的流量配置文件与您“正常”的局间活动（可能为已知且为良性）不同，因此您可以在遵守安全策略的前提下限制对某些封装连接的检查。

在本示例中，部署配置更改后：

- 在受信任区域中检测到的明文、传递和GRE封装隧道各自的封装连接由一组入侵和文件策略评估。
- 受信任区域中的所有其他流量则由另外一组不同的入侵和文件策略评估。

您可以通过对 GRE 隧道进行重新分区来完成这项任务。重新分区可以确保访问控制将 GRE 封装连接与自定义隧道区域（而非其原始的受信任安全区域）关联。鉴于访问控制对封装流量的处理方式，需要进行重新分区；请参阅传递隧道和访问控制，第 1395 页 和 隧道区域与预过滤，第 1403 页。

过程

步骤 1 配置根据封装流量定制深度检查的自定义入侵和文件策略，以及专为非封装流量定制的另外一组入侵和文件策略。

步骤 2 配置自定义预过滤，以便对流过受信任安全区域的 GRE 隧道进行重新分区。

创建自定义预过滤器策略并将其与访问控制关联。在此自定义预过滤器策略中，创建隧道规则（在此示例中，隧道规则为 **GRE_tunnel_rezone**）和对应的隧道区域 (**GRE_tunnel**)。有关详细信息，请参阅配置预过滤，第 1397 页。

表 *99: GRE_tunnel_rezone* 隧道规则

规则组件	说明
接口对象条件	通过将受信任的安全区域同时用作源接口对象和目标接口对象限制来匹配仅内部隧道。
隧道终端条件	为组织中使用的 GRE 隧道指定源终端和目标终端。 默认情况下，隧道规则是双向的。如果不更改**从...匹配隧道 (Match tunnels from...)** 选项，则您将哪些终端指定为源、哪些终端指定为目标都可以。
封装条件	匹配 GRE 流量。
分配隧道区域	创建 **GRE_tunnel** 隧道区域，并将其分配到与规则匹配的隧道。
操作	分析（借助其他访问控制）。

步骤 3 配置访问控制以处理重新分区后的隧道中的连接。

在部署到受管设备的访问控制策略中，配置用于处理重新分区后的流量的规则（在此示例中，规则为 **GRE_inspection**）。有关详细信息，请参阅创建和编辑访问控制规则，第 1288 页。

表 *100: GRE_inspection* 访问控制规则

规则组件	说明
安全区域条件	通过将 GRE_tunnel 安全区域用作源区域限制来匹配重新分区后的隧道。
操作	允许（已启用深度检查） 选择专门用于检查封装内部流量的文件和入侵策略。

注意 如果您跳过此步骤，重新分区后的连接可能会与不受安全区域限制的**任何**访问控制规则匹配。如果重新分区后的连接与任何访问控制规则都不匹配，则由访问控制策略默认操作处理。请确定您想这么做。

步骤 4 配置访问控制以处理流过受信任安全区域的非封装连接。

在同一访问控制策略中，配置用于处理受信任安全区域中未重新分区的流量的规则（在此示例中，规则为 **internal_default_inspection**）。

表 *101: internal_default_inspection* 访问控制规则

规则组件	说明
安全区域条件	通过将受信任的安全区域同时用作源区域和目标区域限制来匹配未重新分区的仅内部流量。
操作	允许（已启用深度检查） 选择专门用于检查非封装内部流量的文件和入侵策略。

步骤 5 评估新访问控制规则相对于预先存在的规则的位置。如有必要，请更改规则顺序。

如果将两个新的访问控制规则放在一起，则哪一个规则放在前面都可以。由于您对GRE隧道进行了重新分区，因此，这两个规则无法相互抢占。

步骤 6 保存所有更改的配置。

下一步做什么

- 部署配置更改。

创建隧道区域

以下步骤介绍如何在对象管理器中创建隧道区域。您还可以在编辑隧道规则时创建区域。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中，选择**隧道区域**。

步骤 3 点击**添加隧道区域**。

步骤 4 输入**名称 (Name)** 和**说明 (Description)**（后者为可选项）。

步骤 5 点击**保存 (Save)**。

下一步做什么

- 在自定义预过滤的过程中，将隧道区域指定为明文直通隧道；请参阅配置预过滤，第 1397 页。

将预过滤器规则移至访问控制策略

您可以将预过滤器规则从预过滤器策略移至关联的访问控制策略。

开始之前

请在继续之前注意以下条件：

- 只能将预过滤器规则移至访问控制策略。无法移动隧道规则。
- 只能将预过滤器规则移至关联的访问控制策略。
- 无法移动已配置接口组的预过滤器规则。
- 移动时，预过滤器规则中的**操作 (Action)** 参数将更改为访问控制规则中的适当操作。要了解预过滤器规则中的每项操作，请参阅下表：

预过滤器规则中的操作	访问控制规则中的操作
分析	允许
阻止	阻止
快速路径	信任

- 同样，根据预过滤器规则中配置的操作，在移动规则后，日志记录配置会被设置为适当的设置，如下表中所述。

预过滤器规则中的操作	访问控制规则中已启用的日志记录配置
分析	未启用任何日志设置。
阻止	• 在连接开始时记录 • 事件查看器 • 系统日志服务器 • SNMP 陷阱
快速路径	• 在连接开始时记录 • 在连接结束时记录 • 事件查看器 • 系统日志服务器 • SNMP 陷阱

- 移动规则后，预过滤器规则配置中的注释会丢失。但是，新注释会被添加到提及源预过滤器策略的移动规则中。
- 从源策略移动规则时，如果其他用户修改了这些规则，则FMC会显示一条消息。您可以在刷新页面后继续该过程。

过程

步骤 1 在预过滤器策略编辑器中，通过点击鼠标左键来选择要移动的规则。

提示　　要选择多个规则，请使用键盘上的 Ctrl (Control) 键。

步骤 2 右键点击所选规则，然后选择**移至另一个策略 (Move to another policy)**。

步骤 3 从**访问策略 (Access Policy)** 下拉列表中选择目标访问控制策略。

步骤 4 从**放置规则 (Place Rules)** 下拉列表中，选择要放置移动规则的位置：

- 要将其定位为**默认 (Default)** 部分中的最后一组规则，请选择**底部（在“默认”部分中） (At the bottom [within the Default section])**。
- 要将其定位为**必填 (Mandatory)** 部分中的第一组规则，请选择**顶部（在“必填”部分中） (At the top [within the Mandatory section])**。

步骤 5 点击 **移动**。

下一步做什么

- 部署配置更改。

预过滤器策略命中计数

命中计数表示为匹配连接触发策略规则的次数。

有关查看预过滤器策略命中计数的完整信息，请参阅查看策略命中计数，第 1277 页。

大型流量分流

在运行 FXOS 的设备上（例如 Firepower 4100/9300 机箱），您配置为通过预过滤器策略进行快速路径的某些流量由硬件（具体而言，在 NIC 中）处理，而不是由您的 威胁防御 软件来处理。分流这些连接流会导致更高的吞吐量和更低的延迟，特别是对于大型文件传输等数据密集型应用。此功能对于数据中心尤为有用。这称为静态数据流分流。

此外，默认情况下，威胁防御 设备会根据其他条件（包括信任）来分流数据流。这称为动态数据流分流。

已分流数据流会继续接收受限的状态检测，例如基础 TCP 标志和选项检查。如有必要，系统可以有选择地将数据包上报至防火墙系统以进行进一步处理。

可以从分流大流量中受益的应用示例如下：

- 高性能计算 (HPC) 研究站点，其中 威胁防御设备部署在存储和高计算站点之间。当一个研究站点使用 NFS 上的 FTP 文件传输或文件同步进行备份时，大量数据流量会影响所有连接。对 NFS 上的 FTP 文件传输或文件同步分流可降低对其他流量的影响。
- 高频交易 (HFT)，其中 威胁防御部署在工作站与交易所之间，主要是出于合规目的。通常无需担心安全问题，但延迟是一个重大问题。

可以分流以下数据流：

- （仅限静态数据流分流。）按预过滤器策略使用快速路径的连接。
- 仅有标准或 802.1Q 标记的以太网帧。
- （仅限动态数据流分流）：
  - 检测引擎认定无需再检测的已检测数据流。这些数据流包括：
    - 由应用“信任”操作且仅基于安全区域、源和目标网络以及端口匹配的访问控制规则处理的流。
    - 未选择使用 an SSL 策略 进行解密的 TLS/SSL 流。
    - 明确受智能应用绕行 (IAB) 策略信任或由于超出数据流绕行阈值而受其信任的数据流。
    - 与文件或入侵策略相匹配而受其信任的数据流。
    - 不再需要检查的任何允许的流。
  - 以下 IPS 预处理器检测的数据流：
    - SSH 和 SMTP。
    - FTP 预处理器辅助连接。
    - 会话初始协议 (SIP) 预处理器辅助连接。
  - 使用关键字的入侵规则（也称为选项）

重要事项 有关上述内容的详细信息、例外情况和限制，请参阅数据流分流限制，第 1410 页。

使用静态数据流分流

要将符合条件的流量卸载到硬件上，请创建应用**快速路径 (Fastpath)** 操作的预过滤器策略规则。为 TCP/UDP 使用预过滤器规则，并为 GRE 使用隧道规则。

(Not recommended.) 要禁用静态数据流分流并将动态数据流分流作为副产品，请使用 FlexConfig 来运行 **no flow-offload enable** 命令。有关此命令的信息，请参阅 https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-command-reference-list.html 上的思科 *ASA* 系列命令参考。

使用动态数据流分流

默认情况下启用动态数据流分流，。

要禁用动态分流，请执行以下操作：

```
> configure flow-offload dynamic whitelist disable
```

要重新启用动态分流，请执行以下操作：

```
> configure flow-offload dynamic whitelist enable
```

请注意，无论是否配置了预过滤，只有启用静态数据流分流时才会发生动态分流。

数据流分流限制

并非所有数据流都可分流。即使在分流后，在某些情况下可取消对数据流的分流。以下是一些限制条件：

无法分流的数据流

以下数据流类型无法分流。

- 任何不使用 IPv4 寻址的流，例如 IPv6 寻址。
- 除 TCP、UDP 和 GRE 之外的任意协议的数据流。

注释 无法分流 PPTP GRE 连接。

- 被动、内联或内联分流模式下配置的接口上的数据流。仅支持已路由和已交换的接口类型。
- 需要由 Snort 或其他检查引擎检查的数据流。在某些情况下（例如 FTP），虽然无法分流控制通道，但可以分流次要数据通道。
- 在设备上终止的 IPsec 和 TLS/DTLS VPN 连接。
- 需要加密或解密的数据流。例如，由于 an SSL 策略 而解密的连接。
- 路由模式下的组播数据流。如果桥接组中只有两个成员接口，则它们在透明模式下受支持。
- TCP 拦截数据流。
- TCP 状态绕过流。不能在同一流量上配置数据流分流和 TCP 状态绕行。
- 使用安全组标记的数据流。
- 从不同集群节点转发来的逆向数据流（在集群中数据流不对称的情况下）。

- 集群中的集中数据流（如果数据流的所有者不是控制设备）。
- 无法动态分流包含 IP 选项的数据流。

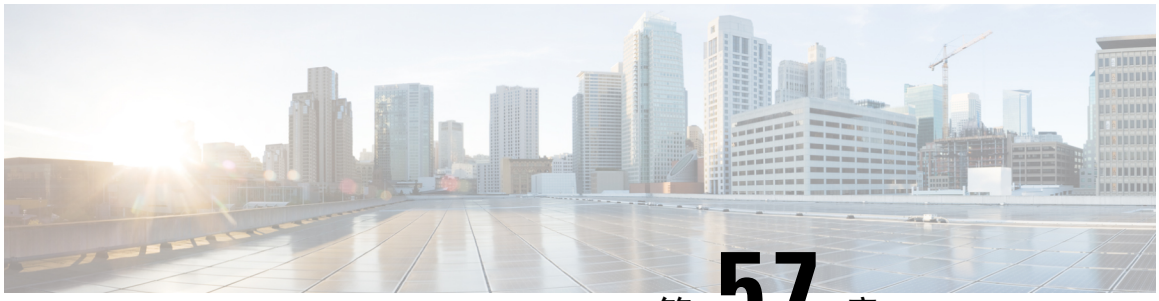
其他限制

- 流分流与死连接检测 (DCD) 不兼容。不要在可分流的连接上配置 DCD。
- 如果多个与数据流分流条件匹配的数据流排队等待同时分流到硬件上的同一位置，则只会分流第一个数据流。其他数据流则会照常处理。这称为冲突。在CLI中使用**show flow-offload flow** 命令显示此情况的统计信息。
- 动态数据流分流会禁用所有 TCP 规范器检查。
- 虽然分流的数据流通过FXOS接口，但这些数据流的统计信息不会显示在逻辑设备接口上。因此，逻辑设备接口计数器和数据包速率不会反映分流流量。

逆向分流的条件

对数据流分流后，如果数据流中的数据包符合以下条件，则将被返回到威胁防御接受进一步处理：

- 数据包包含时间戳以外的 TCP 选项。
- 数据包经过分段。
- 它们会进行等价多路径 (ECMP) 路由，并且入口数据包会从一个接口移至另一个接口。



第 57 章

服务策略

您可以使用 Firepower 威胁防御服务策略将服务应用于特定流量类。例如，可以使用服务策略创建特定于某项 TCP 应用而非应用于所有 TCP 应用的超时配置。服务策略由多个应用于某个接口或全局应用的操作或规则组成。

有关 Firepower 威胁防御服务策略

您可以使用 Firepower 威胁防御服务策略将服务应用于特定流量类。使用服务策略，您不仅仅可以将相同的服务应用于进入设备或给定接口的所有连接。

流量类是接口和扩展访问控制列表(ACL)的组合。ACL“允许”规则确定哪些连接是该类的一部分。ACL 中的任何"被拒绝"流量只是没有应用于其上的服务： 这些连接实际上没有被丢弃。您可以使用 IP 地址和 TCP/UCP 端口根据需要精确识别匹配的连接。

有两种类型的流量类：

- 基于接口的规则 - 如果在服务策略规则中指定安全区域或接口组，则此规则适用于通过作为接口对象一部分的任何接口的 ACL“允许”流量。

  对于指定功能，适用于入口接口的基于接口的规则始终优先于全局规则：如果基于入口接口的规则应用于连接，则忽略任何匹配的全局规则。如果没有适用的入口接口或全局规则，则应用出口接口上的接口服务规则。

- 全局规则 - 这些规则适用于所有接口。如果基于接口的规则不适用于连接，则系统将检查全局规则并将其应用于 ACL“允许”的任何连接。如果没有适用的规则，则连接将继续，而不应用任何服务。

对于指定功能，给定连接只能匹配一个基于接口的流量类或全局流量类。指定接口对象/流量组合最多包含一条规则。

服务策略规则在访问控制规则之后应用。这些服务仅针对您允许的连接进行配置。

服务策略如何与 FlexConfig 和其他功能关联

在版本 6.3(0) 之前，您可以使用 TCP_Embryonic_Conn_Limit 和 TCP_Embryonic_Conn_Timeout 预定义 FlexConfig 对象配置连接相关服务规则。您应该使用 Firepower 威胁防御服务策略删除这些对象并重新配置规则。如果已创建任何自定义 FlexConfig 对象以实施任何连接相关功能（即，**set connection** 命令），则还应删除这些对象并通过服务策略实施这些功能。

由于连接相关服务策略功能被视为与其他服务规则实施功能独立的功能组，因此应该不会遇到流量类重叠的问题。但是，进行以下配置请注意：

- 使用服务策略 CLI 实施 QoS 策略规则。这些规则在基于连接的服务策略规则之前应用。但是，QoS 和连接设置都可以应用于相同或重叠的流量类。
- 您可以使用 FlexConfig 策略来实施自定义应用检测和 NetFlow。使用 **show running-config** 命令检查已配置服务规则的 CLI，包括 **policy-map**、**class-map** 和 **service-policy** 命令。Netflow 和应用检测与 QoS 和连接设置兼容，但是您需要在实施 FlexConfig 之前了解现有配置。在应用检测和 Netflow 之前应用连接设置。

注释 从 Firepower 威胁防御服务策略创建的流量类名为 **class_map_***ACLname*，其中 *ACLname* 是服务策略规则中使用的扩展 ACL 对象的名称。

什么是连接设置？

连接设置包含与管理流量连接相关的各种功能，例如通过 威胁防御 的 TCP 流量。某些功能以组件命名，可以配置这些组件，以提供特定服务。

连接设置包括以下内容：

- **Global timeouts for various protocols** - 所有全局超时均具有默认值，因此，只有在遇到过早失去连接的情况下，才需要更改超时值。配置 Firepower 威胁防御平台策略中的全局超时。依次选择**设备** > **平台设置**。
- **Connection timeouts per traffic class** - 可以使用服务策略覆盖特定流量类型的全局超时。所有流量类超时均具有默认值，因此，无需设置这些超时。
- **Connection limits and TCP Intercept** - 默认情况下，对于可以通过（或到达）威胁防御 的连接数量没有限制。可以使用服务策略规则来设置对特定流量类的限制，以保护服务器免受拒绝服务 (DoS) 攻击。具体而言，可以设置对初期连接（未完成 TCP 握手的连接）的限制，防止 SYN 泛洪攻击。当超过初期限制时，TCP 拦截组件会参与代理连接并确保攻击受到限制。
- **Dead Connection Detection (DCD)** - 如果具有有效但经常空闲的持久连接，以至于这些连接因为超出空闲超时设置而关闭，就可以启用失效连接检测，以识别空闲但有效的连接并且（通过重置其空闲计时器）使之保持活动状态。每当超出空闲时间，DCD 便会探测连接的两侧，了解两侧是否均同意连接是有效的。**show service-policy** 命令输出中包含计数器，以显示来自 DCD 的

活动量。您可以使用 **show conn detail** 命令获取有关发起方和响应方的信息，以及各自发送探测的频率。

- **TCP 序列随机化** - 每个 TCP 连接都有两个初始序列号 (ISN)：一个由客户端生成，一个由服务器生成。默认情况下，威胁防御 随机化入站和出站方向的 TCP SYN 的 ISN。随机化可防止攻击者预测新连接的下一个 ISN 而潜在劫持新会话。可以根据需要按流量类禁用随机化。
- **TCP Normalization** - TCP 规范器可防止异常数据包。可以按流量类配置处理某些数据包异常类型的方式。您可以使用 FlexConfig 策略配置 TCP 规范化。
- **TCP State Bypass** - 如果在网络中使用非对称路由，可以绕过 TCP 状态检查。

服务策略的要求和必备条件

型号支持

威胁防御

支持的域

任意

用户角色

管理员

访问管理员

网络管理员

服务策略准则和限制

- 服务策略仅适用于路由或交换机接口，无论是处于路由模式还是透明模式。这些策略不适用于内联集或被动接口。
- 对于指定接口或全局策略，最多可以有 25 个流量类。具体而言，这意味着对于指定安全区域或接口组，全局策略的服务策略规则不能超过 25 条。但是，对于接口而言，由于同一接口可以同时出现在安全区域和接口组中，因此请注意，实际限制基于接口，而不是基于区域/组。因此，根据所在区域/组的成员资格，您可能无法为每个区域/组设置 25 条规则。
- 对于指定接口对象/流量组合，最多只能包含一条规则。
- 当对配置进行服务策略更改后，所有新连接都将使用新的服务策略。现有连接将继续使用在连接建立时配置的策略。如果希望所有连接立即使用新策略，则需要断开当前连接，以便使用新策略重新连接。在 SSH 或控制台 CLI 会话中，输入 **clear conn** 或 **clear local-host** 命令。

配置威胁防御服务策略

您可以使用威胁防御服务策略将服务应用于特定流量类。例如，可以使用服务策略创建特定于某项 TCP 应用而非应用于所有 TCP 应用的超时配置。服务策略由多个应用于某个接口或全局应用的操作或规则组成。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击要编辑其威胁防御服务策略的访问控制策略的 **编辑**（✎）。

步骤 2 点击**高级 (Advanced)**。

在新 UI 中，从数据包流行末尾的**更多 (More)** 下拉箭头中选择**高级设置 (Advanced Settings)**。

步骤 3 点击**威胁防御服务策略 (Threat Defense Service Policy)** 组中的 **编辑**（✎）。

系统将打开一个对话框，显示现有策略。该策略由有序的规则列表组成，这些规则分为全局规则（适用于所有接口）和基于接口的规则。表格中显示了接口对象和扩展访问控制列表名称（其组合定义规则的流量类）以及所应用的服务。

步骤 4 执行以下任一操作：

- 点击**添加规则**以创建新规则。请参阅配置服务策略规则，第 1416 页。
- 点击**编辑**（✎）以编辑现有规则。请参阅配置服务策略规则，第 1416 页。
- 点击 **删除**（🗑） 以删除规则。
- 点击规则并将其拖动到新位置，以移动规则。您无法在接口和全局列表之间拖动规则，而是必须编辑规则以更改接口/全局设置。列表中与连接匹配的第一条规则将应用于连接。

步骤 5 完成策略编辑后，点击**确定** 。

步骤 6 在**高级 (Advanced)** 选项卡窗口中点击**保存 (Save)**。在您点击保存之前，更改不会被保存。

配置服务策略规则

配置服务策略规则，以将服务应用于特定流量类。

开始之前

转至**对象** > **对象管理** > **访问列表** > **扩展**并创建扩展访问列表，以定义规则适用的流量。此规则适用于与扩展访问列表中的“允许”规则匹配的任何连接。准确定义ACL规则，以便您的服务策略规则仅适用于需要该服务的流量。

如果要创建基于接口的规则，则还必须在已分配的设备上配置接口，并将其添加到安全区域或接口组。

过程

步骤 1 如果您尚未进入“威胁防御服务策略”(Threat Defense Service Policy) 对话框，请选择**策略 (Policies)** > **访问控制 (Access Control)**，编辑访问控制策略，点击**高级 (Advanced)**，然后编辑**威胁防御服务策略 (Threat Defense Service Policy)**。

在新 UI 中，从数据包流行末尾的**更多 (More)** 下拉箭头中选择**高级设置 (Advanced Settings)**。

步骤 2 执行以下任一操作：

- 点击**添加规则**以创建新规则。
- 点击**编辑**（）以编辑现有规则。

系统将打开服务策略规则向导，逐步指导您完成配置规则的流程。

步骤 3 在**接口对象**步骤中，选择用于定义将使用此策略的接口的选项。

- **全局应用** - 选择此选项以创建适用于所有接口的全局规则。
- **选择接口对象** - 选择此选项以创建基于接口的规则。然后，选择包含所需接口的安全区域或接口对象，并点击 > 以将其移到**下一个**选定的列表。系统将在所选对象中包含的每个接口上配置此服务策略规则；而不是在区域/组本身配置此规则。

在满足接口条件后点击。

步骤 4 在**流量传输**步骤中，选择用于定义规则适用的连接的扩展 ACL 对象，然后点击**下一步**。

步骤 5 在**连接设置**步骤中，配置要应用于此流量类的服务。

- **启用 TCP 状态绕行**（仅适用于 TCP 连接）- 实施 TCP 状态绕行。任何检测引擎都不会检查受 TCP 状态绕行影响的连接，它们会绕过所有 TCP 状态检查和 TCP 规范化。有关详细信息，请参阅绕过面向异步路由的 TCP 状态检查（TCP 状态绕行），第 1419 页。

  注释 在进行故障排除或无法解析非对称路由时使用 TCP 状态绕行。此功能将禁用多项安全功能，如果您没有使用狭义定义的流量类正确实施该功能，则可能会导致大量连接。

- **随机生成 TCP 序列号**（仅适用于 TCP 连接）- 启用还是禁用 TCP 序列号随机化。默认情况下启用随机化。有关详细信息，请参阅禁用 TCP 序列随机化，第 1423 页。
- **启用递减 TTL**（仅适用于 TCP 连接）- 减少与类匹配的数据包的生存时间 (TTL)。如果减少生存时间，系统会丢弃 TTL 为 1 的数据包，但会为会话打开一个连接，前提是假设该连接可能包含具有更大 TTL 的数据包。请注意，某些数据包（例如 OSPF hello 数据包）发送时 TTL = 1，因此减去生存时间可能会导致意外后果。

注释 如果希望威胁防御设备显示在跟踪路由中，必须配置递减TTL选项并在平台设置策略中设置ICMP不可达速率限制。请参阅使 威胁防御 设备显示在跟踪路由上，第 1427 页。

- **连接** - 整个类允许的连接数限制。您可以配置以下选项：
  - **最大 TCP 和 UDP 数**（仅适用于 TCP/UDP 连接）- 整个类允许的最大同步 TCP 或 UDP 连接数，该值介于 0 到 2000000 之间。对于 TCP，这仅适用于已建立的连接。默认值为 0，允许无限制连接。由于限制适用于一个类，一台攻击主机可占用所有连接而且使其余所有主机无法与该类匹配。设置每个客户端的限制，以缓解这一问题。
  - **最大初期连接数**（仅适用于 TCP 连接）- 允许的最大同步初期 TCP 连接数（未完成 TCP 握手的连接数），该值介于 0 到 2000000 之间。默认值为 0，允许无限制连接。通过设置非零限制启用 TCP 拦截，从而防止内部系统受到 DoS 攻击（这种攻击使用 TCP SYN 数据包对接口发起泛洪攻击）。另外，请设置每客户端选项，以防止SYN泛洪。有关详细信息，请参阅保护服务器不受 SYN 洪流 DoS 攻击（TCP 拦截），第 1424 页。
- **每个客户端连接数** - 指定客户端（源 IP 地址）的连接数限制。您可以配置以下选项：
  - **最大 TCP 和 UDP 数**（仅适用于 TCP/UDP 连接）- 每个客户端允许的最大同步连接数，该值介于 0 到 2000000 之间。对于 TCP 连接，这包括现有、半开和半闭连接。默认值为 0，允许无限制连接。此选项限制与类匹配的每台主机所允许的最大同步连接数。
  - **最大初期连接数**（仅适用于 TCP 连接）- 每个客户端允许的最大同步初期 TCP 连接数，该值介于 0 到 2000000 之间。默认值为 0，允许无限制连接。有关详细信息，请参阅保护服务器不受 SYN 洪流 DoS 攻击（TCP 拦截），第 1424 页。
- **连接同步 Cookie MSS (Connections Syn Cookie MSS)** - 在达到初期连接限制时为初期连接的 SYN-Cookie 设置服务器最大分段大小 (MSS)，范围为 48 到 65535。默认值为 1380。仅当您为连接和/或每个客户端配置了**最多初期连接次数 (Maximum Embryonic)** 时，此设置才有意义。
- **连接超时** - 要应用于流量类的超时设置。这些超时设置会覆盖平台设置策略中定义的全局超时设置。您可以配置以下内容：
  - **初期连接数**（仅适用于 TCP 连接）- TCP 初期（半开）连接关闭之前的超时时间，该值介于 0:0:5 到 1193:00:00 之间。默认值为 0:0:30。
  - **半闭**（仅适用于 TCP 连接）- 半闭连接关闭之前经过的空闲超时时间，该值介于 0:0:30 到 1193:0:0 之间。默认值为 0:10:0。半闭连接不受失效连接检测 (DCD) 影响。此外，如果取消半闭连接，系统将不发送重置消息。
  - **空闲**（仅适用于 TCP、UDP、ICMP、IP 连接）- 任何协议的已建立连接关闭之前经过的空闲超时时间，该值介于 0:0:1 到 1193:0:0 之间。除非您选择“TCP 状态绕行”选项（其中默认值为 0:2:0），否则默认值为 1:0:0。
  - **超时后重置连接**（仅适用于 TCP 连接）- 是否在空闲连接删除后将 TCP RST 数据包发送到两个终端系统。

- **失效连接检测 (DCD)** - 是否启用失效连接检测 (DCD)。在空闲连接失效前，系统会探测终端主机以确定连接是否有效。如果两台主机均响应，系统会保留连接，否则会释放连接。在透明防火墙模式下运行，必须为终端配置静态路由。您无法在也已分流的连接上配置DCD，因此请勿在预过滤器策略中的快速路径连接上配置 DCD。在 威胁防御 CLI 中使用 **show conn detail** 命令跟踪发起方和响应方发送的 DCD 探测数量。

  配置以下选项：

  - **检测超时** - 每个 DCD 探测器无响应之后发送另一个探测器之前的等待时间（采用 hh:mm:ss 格式），该值介于 0:0:1 到 24:0:0 之间。默认值为 0:0:15。

    对于在集群或高可用性配置中运行的系统，我们建议您不要将间隔设置为小于一分钟(0:1:0)。如果需要在系统之间移动连接，则所需的更改需要花费超过30秒，并且连接可能会在完成更改之前被删除。

  - **检测重试次数** - DCD在宣称连接为失效连接之前可连续失败重试的次数，该值介于1到255之间。默认值为 5。

步骤 6 点击**完成**以保存所做的更改。

此规则将添加到相应列表的底部，即接口或全局。全局规则以自上而下的顺序匹配。接口列表中的规则按自上而下的顺序匹配每个接口对象。请将狭义定义的流量类的规则置于更广泛的规则之上，以确保应用正确的服务。您可以通过拖放操作在每个列表中移动规则。您无法在列表之间移动规则。

绕过面向异步路由的 TCP 状态检查（TCP 状态绕行）

如果网络中有异步路由环境，其中，给定连接的出站和入站流量可以通过两个不同的 威胁防御 设备，则需要在受影响的流量上实施 TCP 状态绕行。

但是，TCP 状态绕行会削弱网络安全性，因此应在非常具体的有限流量类上应用绕行。

以下主题详细介绍该问题和解决方案。

异步路由问题

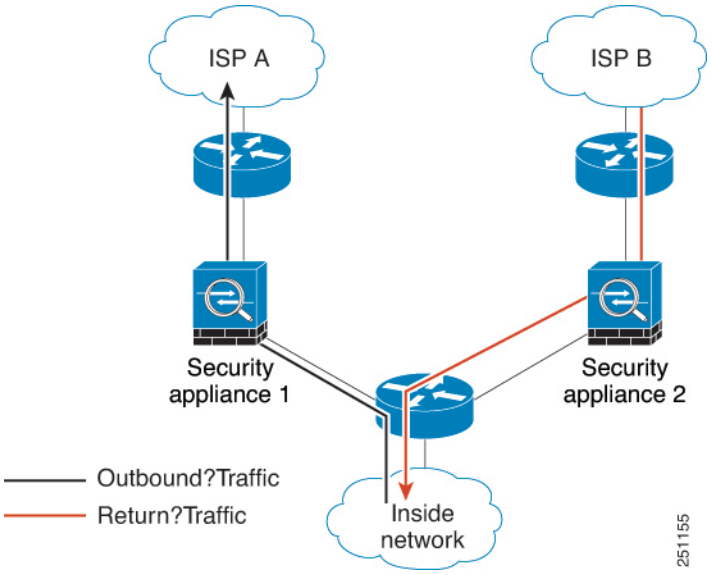
默认情况下，所有经过威胁防御的流量都会使用自适应安全算法检查，并根据安全策略允许通过或予以丢弃。威胁防御 通过检查每个数据包的状态（新连接还是现有连接）并将其分配到会话管理路径（新连接SYN数据包）、快速路径（现有连接）或控制平面路径（高级检测），最大程度地提高防火墙性能。

匹配快速路径中现有连接的TCP数据包，不重新检查安全策略的每个方面即可通过 威胁防御。此功能可最大程度地提高性能。但是，使用SYN数据包在快速路径中建立会话的方法，以及在快速路径中进行的检查（例如 TCP 序列号），可能会阻碍非对称路由解决方案：出站和入站连接流必须通过同一 威胁防御。

例如，有一个新连接传入安全设备 1。SYN 数据包通过会话管理路径，而且连接的条目添加到快速路径表中。如果此连接的后续数据包通过安全设备 1，则这些数据包与快速路径中的该条目匹配，可以通过。但是，如果后续数据包传入安全设备 2，其中没有经过会话管理路径的 SYN 数据包，则

快速路径中没有该连接的条目，数据包将被丢弃。下图显示一个不对称路由示例，其中，出站流量通过一个与入站流量不同的 威胁防御：

图 *145:* 非对称路由



如果在上游路由器中配置了不对称路由，且流量在两个威胁防御之间交替，则可以为特定流量配置 TCP 状态绕行。TCP 状态绕行将改变会话在快速路径中建立的方式，并且禁用快速路径检查。此功能按处理 UDP 连接的大致方式来处理 TCP 流量：当匹配指定网络的非 SYN 数据包进入 威胁防御 时，其中没有快速路径条目，该数据包将通过会话管理路径在快速路径中建立该连接。流量到达快速路径后，将绕过快速路径检查。

有关 TCP 状态绕行的准则和限制

TCP 状态绕行不支持的功能

使用 TCP 状态绕行时不支持以下功能：

- 应用检测 - 检测要求入站和出站流量通过同一 威胁防御，因此不会对 TCP 状态绕行流量应用检测。
- Snort 检测 - 检测要求入站和出站流量通过同一设备。但是，对于 TCP 状态绕行流量，不会自动绕过 Snort 检测。还必须针对您配置 TCP 状态绕行的相同流量类配置预过滤器快速路径规则。
- TCP 拦截、最大初期连接限制、TCP 序列号随机化 - 威胁防御 不跟踪连接的状态，因此不会应用这些功能。
- TCP 标准化 - 禁用 TCP 规范器。
- 状态故障切换。

TCP 状态绕行 NAT 指南

由于转换会话是为每个 威胁防御 单独建立，请务必在两个设备上均为 TCP 状态绕行流量配置静态 NAT。如果使用动态 NAT，则在设备 1 上为会话选择的地址将与在设备 2 上为会话选择的地址不同。

配置 TCP 状态绕行

要在异步路由环境中绕过 TCP 状态检查，请仔细定义适用于受影响主机或仅适用于网络的流量类，然后使用服务策略在流量类上启用 TCP 状态绕行。您还必须为相同的流量配置相应的预过滤器快速路径策略，以确保此流量也绕过检查。

由于绕行会降低网络安全性，请尽可能限制网络应用。

过程

步骤 1 创建定义流量类的扩展 ACL。

例如，要为从 10.1.1.1 到 10.2.2.2 的 TCP 流量定义流量类，请执行以下操作：

a) 选择**对象 (Object)** > **对象管理 (Object Management)**。
b) 从目录中选择**访问列表** > **扩展**。
c) 点击**添加扩展访问列表**。
d) 为对象输入一个**名称**，例如 bypass。
e) 点击**添加**以添加规则。
f) 保持**允许**操作。
g) 在**源**列表下方输入 10.1.1.1 并点击**添加**，然后在**目标**列表下方输入 10.2.2.2 并点击**添加**。
h) 点击**端口 (Port)**，选择**选定源端口 (Selected Source Ports)** 列表下方的 **TCP (6)**，然后点击**添加 (Add)**。不要输入端口号，只需添加 TCP 作为协议，这将覆盖所有端口。
i) 在“扩展访问列表条目”对话框中点击**添加**，以将规则添加到 ACL。
j) 点击“扩展访问列表对象”对话框中的**保存**，以保存 ACL 对象。

步骤 2 配置 TCP 状态绕行服务策略规则。

例如，要为此流量类全局配置 TCP 状态绕行，请执行以下操作：

a) 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后编辑分配给需要此服务的设备的策略。
b) 点击**高级 (Advanced)**，然后点击**威胁防御服务策略 (Threat Defense Service Policy)** 的 **编辑**（）。

   在新 UI 中，从数据包流行末尾的**更多 (More)** 下拉箭头中选择**高级设置 (Advanced Settings)**。

c) 点击**添加规则 (Add Rule)**。
d) 选择**全局应用 (Apply Globally)** > **下一步 (Next)**。
e) 选择为此规则创建的扩展 ACL 对象，然后点击**下一步**。
f) 选择**启用 TCP 状态绕行**。
g) （可选。）调整绕行连接的**空闲**超时。默认值为 2 分钟。
h) 点击**完成**以添加规则。如有必要，将规则拖放到服务策略中的所需位置。

i) 点击**确定**以保存对服务策略所做的更改。

j) 点击**高级 (Advanced)** 中的**保存 (Save)**，以保存对访问控制策略所做的更改。

步骤 3 配置流量类的预过滤器快速路径规则。

不能在预过滤器规则中使用ACL对象，因此您需要直接在预过滤器规则中重新创建流量类，或者通过首先创建定义类的网络对象来创建流量类。

以下程序假定您已经在访问控制策略中附加了预过滤器策略。如果尚未创建预过滤器策略，请转至**策略 (Policies)** > **预过滤器 (Prefilter)**，然后首先创建策略。然后，您可以按照此程序将其附加到访问控制策略并创建规则。

在我们的示例中，此程序为 10.1.1.1 到 10.2.2.2 的 TCP 流量创建快速路径规则。

a) 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后编辑具有 TCP 绕行服务策略规则的策略。

b) 点击**预过滤器策略**链接，该策略位于策略说明的左下方。

c) 在“预过滤器策略”对话框中，选择要分配给设备的策略（如果尚未选择正确的策略）。不要点击“确定”。

由于您无法将规则添加到默认预过滤器策略，因此必须选择自定义策略。

d) 在“预过滤器策略”对话框中，点击**编辑**（）。此操作将打开一个新的浏览器窗口，您可以在其中编辑策略。

e) 点击**添加预过滤器规则**并配置包含以下属性的规则。

- **名称** - 您觉得有意义的任何名称均可，例如 TCPBypass。
- **操作** - 选择**快速路径**。
- **接口对象 (Interface Objects)** - 如果已将 TCP 状态绕行配置为全局规则，则为源和目标接口保留默认值“any”。如果已创建基于接口的规则，则在**源接口对象**列表中选择用于规则的相同接口对象，并将“any”作为目标接口。
- **网络 (Networks)** - 将 10.1.1.1 添加到**源网络 (Source Networks)** 列表中，并将 10.2.2.2 添加到**目标网络 (Destination Networks)** 列表中。您可以使用网络对象或手动添加地址。
- **端口 (Ports)** - 在**选定源端口 (Selected Source Ports)** 下, 选择 TCP(6)，**不要输入端口**，然后点击**添加 (Add)**。这会将规则应用于所有（且仅限）TCP 流量（不考虑 TCP 端口号）。

f) 点击**添加**以将规则添加到预过滤器策略中。

g) 点击**保存**以保存对预过滤器策略所做的更改。

现在您可以关闭预过滤器编辑窗口并返回访问控制策略编辑窗口。

h) 在访问控制策略编辑窗口中，“预过滤器策略”对话框仍处于打开状态。点击**确定**以保存对预过滤器策略分配所做的更改。

i) 如果您做出了更改，则点击访问控制策略上的**保存**以保存已更改的预过滤器策略分配。

现在您可以将更改部署到受影响的设备。

禁用 TCP 序列随机化

每个 TCP 连接都有两个初始序列号 (ISN)：一个由客户端生成，一个由服务器生成。威胁防御设备会为通过入站和出站两个方向的 TCP SYN 随机生成 ISN。

随机化受保护主机的 ISN 可防止攻击者预测新连接的下一个 ISN 而潜在劫持新会话。

可以根据需要禁用 TCP 初始序列号随机化，例如，由于数据混乱。以下是您可能希望禁用随机化的一些情况：

- 如果另一个在线防火墙也随机化初始序列号，则即使此操作不影响流量，两个防火墙也无需执行此操作。
- 如果通过此设备使用 eBGP 多跳，并且 eBGP 对等设备在使用 MD5。随机化会中断 MD5 校验和。
- 如果使用要求 威胁防御设备不为连接随机生成序列号的 WAAS 设备。
- 如果为 ISA 3000 启用硬件旁路，当 ISA 3000 不再是数据路径时的一部分时，TCP 连接将被丢弃。

过程

步骤 1 创建定义流量类的扩展 ACL。

例如，要从任何主机到 10.2.2.2 的 TCP 流量定义流量类，请执行以下操作：

a) 选择**对象 (Object)** > **对象管理 (Object Management)**。
b) 从目录中选择**访问列表** > **扩展**。
c) 点击**添加扩展访问列表**。
d) 为对象输入一个**名称**，例如 preserve-sq-no。
e) 点击**添加**以添加规则。
f) 保持**允许**操作。
g) 将**源**列表留空，在**目标**列表下方输入 10.2.2.2，然后点击**添加**。
h) 点击**端口 (Port)**，选择**选定源端口 (Selected Source Ports)** 列表下方的 **TCP (6)**，然后点击**添加 (Add)**。不要输入端口号，只需添加 TCP 作为协议，这将覆盖所有端口。
i) 在“扩展访问列表条目”对话框中点击**添加**，以将规则添加到 ACL。
j) 点击“扩展访问列表对象”对话框中的**保存**，以保存 ACL 对象。

步骤 2 配置将禁用 TCP 序列号随机化的服务策略规则。

例如，要为此流量类全局禁用随机化，请执行以下操作：

a) 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后编辑分配给需要此服务的设备的策略。
b) 点击**高级 (Advanced)**，然后点击**威胁防御服务策略 (Threat Defense Service Policy)** 的 **编辑**（ ）。

在新 UI 中，从数据包流行末尾的**更多 (More)** 下拉箭头中选择**高级设置 (Advanced Settings)**。

c) 点击**添加规则 (Add Rule)**。
d) 选择**全局应用 (Apply Globally)** > **下一步 (Next)**。
e) 选择为此规则创建的扩展 ACL 对象，然后点击**下一步**。
f) 取消选择**随机生成 TCP 序列号**。
g) （可选。）根据需要调整其他连接选项。
h) 点击**完成**以添加规则。如有必要，将规则拖放到服务策略中的所需位置。
i) 点击**确定**以保存对服务策略所做的更改。
j) 点击**高级 (Advanced)** 中的**保存 (Save)**，以保存对访问控制策略所做的更改。

现在您可以将更改部署到受影响的设备。

服务策略规则示例

以下主题提供服务策略规则示例。

保护服务器不受 SYN 洪流 DoS 攻击（TCP 拦截）

当攻击者将一系列 SYN 数据包发送到主机时，即表示发生 SYN 泛洪拒绝服务 (DoS) 攻击。这些数据包通常来自虚假 IP 地址。SYN 数据包的持续泛洪将使服务器 SYN 队列始终处于充满状态，而无法处理来自合法用户的连接请求。

可以限制初期连接的数量，这样有助于防止SYN泛洪攻击。半开连接是源与目标之间尚未完成必要握手的连接请求。

超过某个连接的初期连接阈值时，威胁防御设备会充当服务器代理，并使用SYN Cookie方法生成对客户端 SYN 请求的 SYN-ACK 响应（有关 SYN Cookie 的详细信息，请参阅维基百科）。当 威胁防御设备收到来自客户端的ACK后，可以对客户端的真实性进行身份验证，并且允许连接到服务器。执行代理的组件称为 TCP 拦截。

设置连接限制可以保护服务器免受 SYN 泛洪攻击。或者，您可以选择启用 TCP 拦截统计信息并监控策略的结果。以下程序介绍端到端流程。

开始之前

- 请确保设置的初期连接限制低于要保护的服务器上的 TCP SYN 积压工作队列。否则，在 SYN 攻击期间，有效客户端将无法访问服务器。为了确定初期限制的合理值，请仔细分析服务器容量、网络和服务器使用情况。
- 根据 Cisco Secure Firewall Threat Defense型号中 CPU 内核数量，由于每个内核管理连接的方式不同，最大并发和正在建立的连接可能超出配置的数量。在最糟糕的情况下，此设备最多允许 n-1 个额外连接和初期连接，其中 n 是内核数量。例如，如果设备型号有 4 个核心，而配置了 6 个并发连接和 4 个初期连接，那么每个类型可能有 3 个额外连接。要确定型号的内核数量，请在设备 CLI 中输入 **show cpu core** 命令。

过程

步骤 1 创建定义流量类的扩展 ACL，该列表是要保护的服务器列表。

例如，要定义流量类以使用 IP 地址 10.1.1.5 和 10.1.1.6 保护 Web 服务器，请执行以下操作：

a) 选择**对象 (Object)** > **对象管理 (Object Management)**。
b) 从目录中选择**访问列表** > **扩展**。
c) 点击**添加扩展访问列表**。
d) 为对象输入一个**名称**，例如，protected-servers。
e) 点击**添加**以添加规则。
f) 保持**允许**操作。
g) 将**源**列表留空，在**目标**列表下方输入 10.1.1.5，然后点击**添加**。
h) 此外，在**目标**列表下方输入 10.1.1.6，然后点击**添加**。
i) 点击**端口 (Port)**，从可用端口列表中选择 **FMC_CONNECTION**，然后点击**添加到目标 (Add to Destination)**。如果您的服务器还支持 HTTPS 连接，还需添加此端口。
j) 在“扩展访问列表条目”对话框中点击**添加**，以将规则添加到 ACL。
k) 点击“扩展访问列表对象”对话框中的**保存**，以保存 ACL 对象。

步骤 2 配置用于设置初期连接限制的服务策略规则。

例如，要将总并发初期连接限制设置为 1000 个并将每客户端的连接限制设置为 50 个，请执行以下操作：

a) 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后编辑分配给需要此服务的设备的策略。
b) 点击**高级 (Advanced)**，然后点击**威胁防御服务策略 (Threat Defense Service Policy)** 的 **编辑**（ ）。

   在新 UI 中，从数据包流行末尾的**更多 (More)** 下拉箭头中选择**高级设置 (Advanced Settings)**。

c) 点击**添加规则 (Add Rule)**。
d) 选择**全局应用 (Apply Globally)** > **下一步 (Next)**。
e) 选择为此规则创建的扩展 ACL 对象，然后点击**下一步**。
f) 为**连接** > **最大初期连接数**输入 1000。
g) 为**每个客户端的连接数** > **最大初期连接数**输入 50。
h) （可选。）根据需要调整其他连接选项。
i) 点击**完成**以添加规则。如有必要，将规则拖放到服务策略中的所需位置。
j) 点击**确定**以保存对服务策略所做的更改。
k) 点击**高级 (Advanced)** 中的**保存 (Save)**，以保存对访问控制策略所做的更改。

步骤 3 （可选。）配置 TCP 拦截统计信息的速率。

TCP 拦截使用以下选项来确定收集统计信息的速率。所有选项都具有默认值，因此如果这些速率符合您的需求，您可以跳过此步骤。

- 速率间隔 - 历史监控窗口的大小，该值介于 1 到 1440 分钟之间。默认值为 30 分钟。在此间隔期间，系统会进行 30 次攻击数量采样。

- 突发速率 - 系统日志消息生成的阈值，该值介于 25 到 2147483647 之间。默认值为每秒 400 条消息。超出突发速率时，设备将生成系统日志消息 733104。
- 平均速率 - 系统日志消息生成的平均速率阈值，该值介于 25 到 2147483647 之间。默认值为每秒 200 条消息。超出平均速率时，设备将生成系统日志消息 733105。

如果要调整这些选项，请执行以下操作：

a) 选择**对象 (Object)** > **对象管理 (Object Management)**。
b) 选择 **FlexConfig** > **文本对象**。
c) 点击 threat_defense_statistics 系统定义对象的 **编辑**（）。
d) 虽然您可以直接更改值，但建议的方法是打开**覆盖**部分，然后点击**添加**以创建设备覆盖。
e) 选择要为其分配服务策略的设备（通过访问控制策略分配），然后点击**添加**以将其移动到所选列表中。
f) 点击**覆盖 (Override)**。
g) 此对象必须有 3 个条目，因此请根据需要点击**计数 (Count)**，直至获得 3 个条目。
h) 按照 1-3 的顺序输入所需的值作为速率间隔、突发速率和平均速率。请参阅对象说明以验证您是否按正确的顺序输入值。
i) 在“对象覆盖”对话框中点击**添加**。
j) 在“编辑文本对象”对话框中点击**保存**。

步骤 4 启用 TCP 拦截统计信息。

您必须配置 FlexConfig 策略以启用 TCP 拦截统计信息。

a) 选择**设备** > **FlexConfig**。
b) 如果已为设备分配策略，请对其进行编辑。否则，请创建新策略并将其分配给受影响的设备。
c) 选择**可用 FlexConfig** 列表中的 **Threat_Detection_Configure** 对象，然后点击 **>>**。此对象将添加到**所选附加 Flexconfig** 列表中。
d) 点击**保存**。
e) （可选。）您可以通过点击**预览配置**并选择其中一个设备来验证是否具有正确的设置。

系统会生成将在下次部署期间写入设备的 CLI 命令。这些命令将包括服务策略所需的命令以及威胁检测统计信息所需的命令。滚动到预览的底部以查看附加的CLI。如果使用默认值，TCP拦截统计信息命令应如下所示（为清晰起见已添加换行符）：

```
###Flex-config Appended CLI ###

threat-detection statistics tcp-intercept rate-interval 30
       burst-rate 400 average-rate 200
```

步骤 5 现在您可以将更改部署到受影响的设备。

步骤 6 使用以下命令从设备 CLI 监控 TCP 拦截统计信息：

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**] - 查看遭受攻击的前 10 台受保护服务器。**all** 关键字显示所有被跟踪服务器的历史数据。**detail** 关键字显示历史采样数据。在速率间隔内，系统会进行 30 次攻击次数采样，因此，在默认的 30 分钟内，每 60 秒收集一次统计信息。

注释　您可以使用 **shun** 命令阻止攻击主机 IP 地址。要删除阻止列表，请使用 **no shun** 命令。

- **clear threat-detection statistics tcp-intercept**- 清除 TCP 拦截统计信息。

示例：

```
hostname(config)# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
---------------------------------------------------------------------------------
1    10.1.1.5:80 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    10.1.1.6:80 inside 10 10 6080 10.0.0.200 (0 secs ago)
```

使 威胁防御 设备显示在跟踪路由上

默认情况下，威胁防御不会在跟踪路由上显示为跃点。要使其显示，您需要递减通过设备的数据包上的生存时间，并增加对 ICMP 不可达消息的速率限制。要实现此目的，必须配置服务策略规则并调整 ICMP 平台设置策略。

注释　如果减少生存时间，系统会丢弃 TTL 为 1 的数据包，但会为会话打开一个连接，前提是假设该连接可能包含具有更大 TTL 的数据包。请注意，某些数据包（例如 OSPF hello 数据包）发送时 TTL = 1，因此减去生存时间可能会导致意外后果。定义流量类时，请注意这些事项。

过程

步骤 1 创建扩展 ACL，以定义要为其启用跟踪路由报告的流量类。

例如，要为所有地址（但不包括 OSPF 流量）定义流量类，请执行以下操作：

a) 选择**对象 (Object)** > **对象管理 (Object Management)**。
b) 从目录中选择**访问列表** > **扩展**。
c) 点击**添加扩展访问列表**。
d) 为对象输入一个**名称**，例如，traceroute-enabled。
e) 点击**添加**以添加规则，从而排除 OSPF。
f) 将操作更改为**阻止 (Block)**，点击**端口 (Port)** 选项卡，选择 **OSPFIGP (89)** 作为**目标端口 (Destination Ports)** 列表下方的协议，然后点击**添加 (Add)** 将此协议添加到所选列表。
g) 在“扩展访问列表条目”对话框中点击**添加**，以将 OSPF 规则添加到 ACL。
h) 点击**添加**以添加规则，从而包含所有其他连接。
i) 保持**允许**操作，并将“源”和“目标”列表留空。

j) 在“扩展访问列表条目”对话框中点击**添加**，以将规则添加到 ACL。

确保 OSPF 拒绝规则优先于“允许所有”规则。如有必要，拖放以移动规则。

k) 点击“扩展访问列表对象”对话框中的**保存**，以保存 ACL 对象。

步骤 2 配置用于递减生存时间值的服务策略规则。

例如，要全局递减生存时间，请执行以下操作：

a) 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后编辑分配给需要此服务的设备的策略。

b) 点击**高级 (Advanced)**，然后点击**威胁防御服务策略 (Threat Defense Service Policy)** 的 **编辑**（）。

在新 UI 中，从数据包流行末尾的**更多 (More)** 下拉箭头中选择**高级设置 (Advanced Settings)**。

c) 点击**添加规则 (Add Rule)**。

d) 选择**全局应用**，然后点击**下一步**。

e) 选择为此规则创建的扩展 ACL 对象，然后点击**下一步**。

f) 选择**启用递减 TTL**。

g) （可选。）根据需要调整其他连接选项。

h) 点击**完成**以添加规则。如有必要，将规则拖放到服务策略中的所需位置。

i) 点击**确定**以保存对服务策略所做的更改。

j) 点击**高级 (Advanced)** 中的**保存 (Save)**，以保存对访问控制策略所做的更改。

现在您可以将更改部署到受影响的设备。

步骤 3 增加 ICMP 不可达消息的速度限制。

a) 选择**设备** > **平台设置**。

b) 如果已为设备分配策略，请对其进行编辑。否则，请创建新的威胁防御平台设置策略并将其分配给受影响的设备。

c) 从目录中选择 **ICMP**。

d) 增加**速率限制**，例如，增加至 50。您可能还希望将**突发大小**增加到 10，以确保在速率限制内生成足够的响应。

您可以将 ICMP 规则表留空，它与此任务无关。

e) 点击**保存**。

步骤 4 现在您可以将更改部署到受影响的设备。

监控服务策略

您可以使用设备 CLI 监控服务策略相关信息。以下是一些有用的命令。

- **show conn** [**detail**]

显示连接信息。详细信息使用标志来表示特殊连接特性。例如，“b”标志表示会对流量应用 TCP 状态绕行。

使用 **detail** 关键字时，您可以查看有关失效连接检测 (DCD) 探测的信息，这会显示发起方和响应方探测连接的频率。例如，对于启用 DCD 的连接，其连接详细信息如下所示：

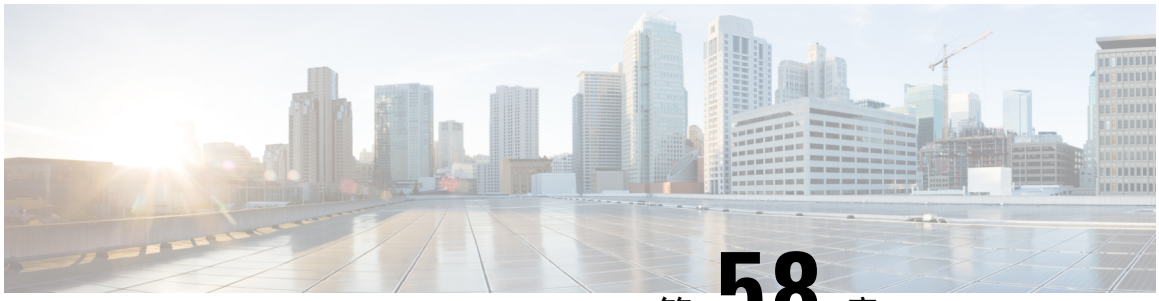
```
TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,
    flags UO , idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828,
cluster sent/rcvd bytes 0/0, owners (0,255)
  Traffic received at interface dmz
        Locally received: 0 (0 byte/s)
  Traffic received at interface inside
        Locally received: 11828 (6 byte/s)
  Initiator: 10.5.4.10, Responder: 10.5.4.11
  DCD probes sent: Initiator 5, Responder 5
```

- **show service-policy**

  显示服务策略统计信息，包括失效连接检测 (DCD) 统计信息。

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**]

  查看遭受攻击的前 10 名受保护服务器。**all** 关键字显示所有被跟踪服务器的历史数据。**detail** 关键字显示历史采样数据。在速率间隔内，系统会进行 30 次攻击次数采样，因此，在默认的 30 分钟内，每 60 秒收集一次统计信息。



第 58 章

智能应用旁路

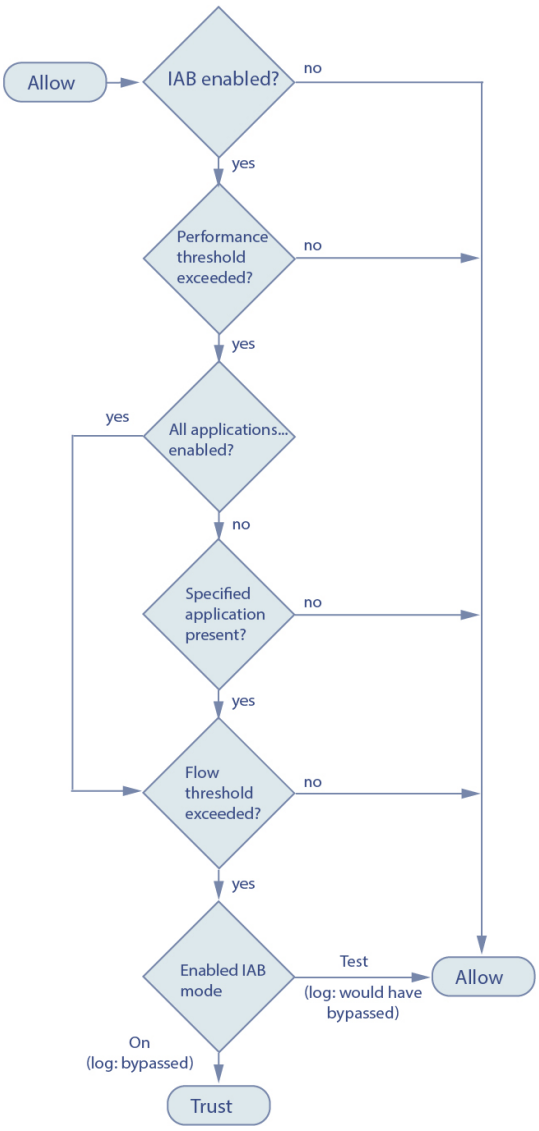
以下主题介绍如何配置访问控制策略以使用智能应用旁路 (IAB)

IAB 简介

IAB 可识别您信任其流经您的网络而无需进一步检查是否超出性能和数据流阈值的应用。例如，如果每次晚间的备份会显著影响系统的性能，您可以配置某些阈值，当超过这些阈值时则信任备份应用产生的流量。（可选）您可以配置 IAB，以便在超过检查性能阈值时，无论应用类型如何，IAB 都信任超过任何流绕行阈值的所有流量。

在对流量进行深度检查之前，系统会对访问控制规则或访问控制策略的默认操作所允许的流量实施 IAB。您可以通过一种测试模式确定是否已超过阈值，如果已超过，则识别出在您实际启用了 IAB 的情况下会被绕过的应用数据流（称为绕行模式）。

下图展示 IAB 决策过程：



IAB 选项

状态

启用或禁用 IAB。

性能采样间隔 (Performance Sample Interval)

指定两次 IAB 性能采样扫描间隔的时间（秒），系统会在此期间收集系统性能指标以与 IAB 性能阈值进行比较。值 **0** 会禁用 IAB。

可绕行应用和过滤器 (Bypassable Applications and Filters)

此功能提供两个互斥的选项：

应用/过滤器
提供您可以在其中指定可绕行应用和应用集（过滤器）的编辑器。请参阅应用规则条件，第 607 页。

包括未识别应用在内的所有应用
超过检查性能阈值时，不管应用类型为何，都信任超过任何流绕行阈值的所有流量。

性能和流阈值

您必须配置至少一个检查性能阈值和一个流绕过阈值。当超过某一性能阈值时，系统会检查流阈值，并且如果超过某一阈值，则信任指定流量。如果您启用了任何一种阈值中的多项，则只能超过每种阈值中的一项。

检查性能阈值提供入侵检查性能限值，如果超过该限值，则会触发流阈值检查。IAB 不使用设置为 **0** 的检查性能阈值。您可以配置一项或多项以下检查性能阈值：

丢弃百分比 (Drop Percentage)

因昂贵入侵规则、文件策略、解压等引起的性能过载导致的数据包丢弃时，丢弃的平均数据包数占总数据包数的百分比。这并不是指入侵规则等正常配置丢弃的数据包数。请注意，当丢弃指定百分比的数据包时，指定大于 1 的整数会激活 IAB。指定 **1** 时，任何从 0 到 1 的百分比都会激活 IAB。这允许少量数据包激活 IAB。

处理器利用率百分比 (Processor Utilization Percentage)

使用的处理器资源的平均百分比。

数据包延迟

平均数据包延迟（微秒）。

流量

系统处理流的速率，以每秒的流数进行测量。请注意，此选项可配置 IAB 以测量流速率，而不是流计数。

流绕行阈值提供流限值，如果超过该限值，则会触发 IAB 信任绕行模式下的可绕行应用流量，或允许应用流量在测试模式下接受进一步检查。IAB 不使用设置为 **0** 的流绕行阈值。您可以配置一项或多项以下流绕行阈值：

单位流字节数 (Bytes per Flow)

一个流可以包含的最大千字节数。

单位流数据包数 (Packets per Flow)

一个流可以包含的最大数据包数。

流持续时间 (Flow Duration)

一个流保持开放的最大秒数。

流速 (Flow Velocity)

最高传输速率（千字节/秒）。

智能应用绕行的要求和必备条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

配置智能应用旁路

⚠

注意 并非所有部署都需要 IAB，而那些需要 IAB 的部署也仅以有限的方式进行使用。除非您具备网络流量（特别是应用流量）和系统性能（包括可预测的性能问题的原因）方面的专业知识，否则不要启用 IAB。在绕行模式下运行 IAB 之前，请确保信任指定的流量不会使您处于风险中。

开始之前

对于经典设备，您必须拥有控制许可证。

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)**，然后点击**智能应用绕行设置 (Intelligent Application Bypass Settings)** 旁边的 **编辑**（✎）。

在新 UI 中，从数据包流行末尾的**更多 (More)** 下拉箭头中选择**高级设置 (Advanced Settings)**。

如果显示**视图**（👁），则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 2 配置 IAB 选项：

- **状态 (State)** - 关闭或打开 IAB，或在测试模式下启用 IAB。
- **性能采样间隔 (Performance Sample Interval)** - 输入 IAB 性能采样扫描之间的间隔时间（以秒为单位）。如果启用 IAB，即使在测试模式下，也请输入非零值。输入 **0** 可禁用 IAB。
- **可绕过的应用和过滤器 (Bypassable Applications and Filters)** - 从以下项中选择：
  - 点击绕过的应用和过滤器数量并指定要绕过其流量的应用；请参阅配置应用条件和过滤器，第 1294 页。
  - 点击**所有应用 (包括未识别的应用)**，以便在超过检查性能阈值时，IAB 信任超过任何流绕行阈值的所有流量，不管应用类型如何都是如此。
- **检查性能阈值 (Inspection Performance Thresholds)** - 点击**配置 (Configure)** 并输入至少一个阈值。
- **流绕行阈值 (Flow Bypass Thresholds)** - 点击**配置 (Configure)** 并输入至少一个阈值。

必须指定至少一个检查性能阈值和一个流绕行阈值；必须超过这两个阈值，IAB 才可信任流量。如果为每种类型输入多个阈值，则仅必须超过每种类型的一个阈值。有关详细信息，请参阅IAB 选项，第 1432 页。

步骤 3 点击**确定 (OK)** 保存 IAB 设置。

步骤 4 点击 **Save** 保存策略。

下一步做什么

- 由于在检测应用之前必须允许一些数据包通过，因此必须配置系统以便检查这些数据包。

  请参阅处理在流量识别之前通过的数据包的最佳实践，第 2042 页和指定策略以处理在流量识别之前通过的数据包，第 2042 页。
- 部署配置更改。

IAB 日志记录和分析

无论是否启用连接日志记录，IAB 都会强制连接结束事件记录已绕过的流和应已绕过的流。连接事件指示在绕行模式下绕过的流或在测试模式下应已绕过的流。基于连接事件的自定义控制面板构件和报告可以显示已绕过和应已绕过的流的长期统计信息。

IAB 连接事件

操作

当**原因 (Reason)** 包括 `Intelligent App Bypass` 时：

`Allow -`

指示已应用的 IAB 配置处于测试模式，并且**应用协议**指定的应用的流量仍可供检查。

Trust -

指示已应用的 IAB 配置处于绕行模式，并且**应用协议**指定的应用的流量受信任，可流经网络而不进行进一步检查。

原因

`Intelligent App Bypass` 指示 IAB 在绕行或测试模式下触发了事件。

应用协议

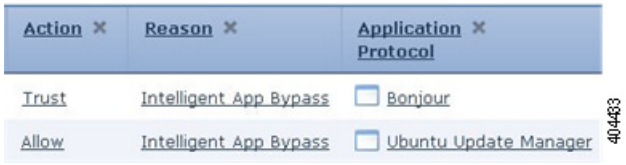
此字段显示触发了事件的应用协议。

示例

在以下截断的图形中，某些字段已省略。该图形显示根据两个单独访问控制策略中的不同 IAB 设置产生的两个连接事件的**操作 (Action)**、**原因 (Reason)** 和**应用协议 (Application Protocol)** 字段。

对于第一个事件，`Trust` 操作指示 IAB 在绕行模式下已启用，并且 Bonjour 协议流量受信任可通过而不进行进一步检查。

对于第二个事件，`Allow` 操作指示 IAB 在测试模式下已启用，因此 Ubuntu 更新管理器流量会接受进一步检查，但如果 IAB 在绕行模式下已启用，则应已绕过该流量。



示例

在以下截断的图形中，某些字段已省略。第二个事件中的流同时按照入侵规则（**原因 [Reason]**：`Intrusion Monitor`）进行绕过（**操作 [Action]**：`Trust`；**原因 [Reason]**：`Intelligent App Bypass`）和检查。`Intrusion Monitor` 原因指示检测到设置为**生成事件 (Generate Events)** 的入侵规则，但在连接过程中未阻止漏洞。在示例中，此情况发生在检测到应用之前。在检测到应用后，IAB 将应用识别为可绕过且受信任的流。

IAB 自定义控制面板构件

可以创建自定义分析控制面板构件以根据连接事件显示长期 IAB 统计信息。创建构件时，请指定以下信息：

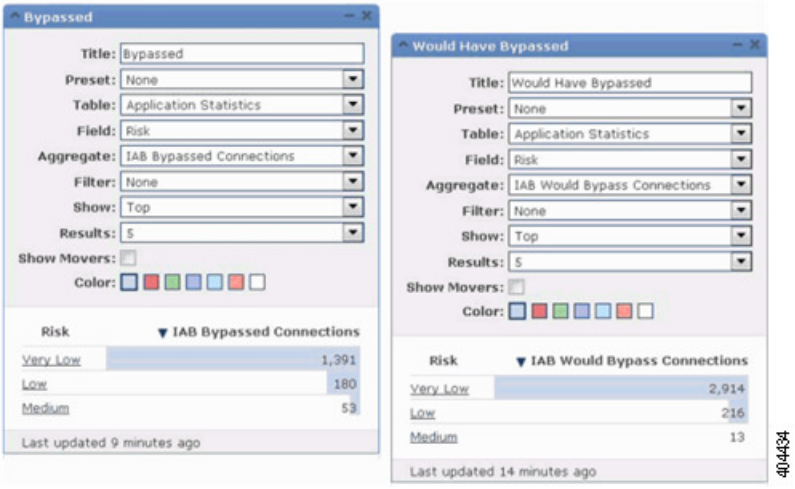
- **预设 (Preset)**：`None`

- **表 (Table)**：`Application Statistics`
- **字段 (Field)**：any
- **汇聚 (Aggregate)**：以下任一：
  - `IAB Bypassed Connections`
  - `IAB Would Bypass Connections`
- **过滤器 (Filter)**：any

示例

在以下自定义分析控制面板构件示例中：

- 已绕过示例显示由于在已部署的访问控制策略中应用指定为可绕过且 IAB 在绕行模式下已启用而绕过的应用流量的统计信息。
- 应已绕过示例显示由于在已部署的访问控制策略中应用指定为可绕过且 IAB 在测试模式下已启用而应已绕过的应用流量的统计信息。.



IAB 自定义报告

可以创建自定义报告以根据连接事件显示长期 IAB 统计信息。创建报告时，请指定以下信息：

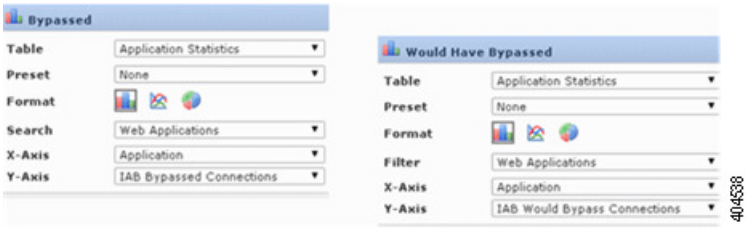
- **表 (Table)**：`Application Statistics`
- **预设 (Preset)**：`None`
- **过滤器 (Filter)**：any
- **X 轴 (X-Axis)**：any
- **Y 轴 (Y-Axis)**：以下任一：

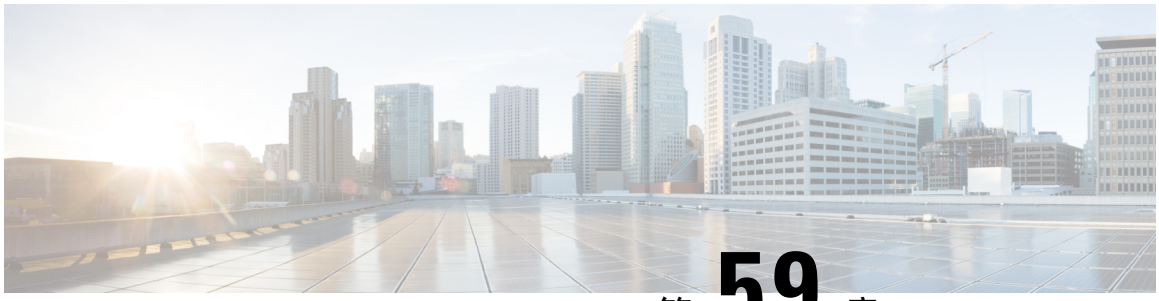
- `IAB Bypassed Connections`
- `IAB Would Bypass Connections`

示例

下图中显示两个缩写的报告示例：

- 已绕过示例显示由于在已部署的访问控制策略中应用指定为可绕过且 IAB 在绕行模式下已启用而绕过的应用流量的统计信息。
- 应已绕过示例显示由于在已部署的访问控制策略中应用指定为可绕过且 IAB 在测试模式下已启用而应已绕过的应用流量的统计信息。





第 59 章

内容限制

以下主题介绍如何将访问控制策略配置为使用内容限制功能：

关于内容限制

主要搜索引擎和内容传递服务提供允许您限制搜索结果和网站内容的功能。例如，学校使用内容限制功能来遵守儿童互联网保护法案 (CIPA)。

当由搜索引擎和内容传递服务实施时，您可以仅针对个别浏览器或用户执行内容限制功能。系统允许您将这些功能扩展到您的整个网络。

该系统允许您执行以下服务：

- 安全搜索 - 许多主要搜索引擎支持此服务，此服务过滤掉被企业、政府和教育环境分类为不允许的限制级成人内容。系统不限制用户访问所支持搜索引擎主页的能力。

您可以使用两种方法配置系统执行这些功能：

方法：访问控制规则
内容限制功能通过请求 URI 中的元素、相关 Cookie 或自定义 HTTP 标头报头元素传达搜索或内容查询的限制状态。您可以将访问控制规则配置为在系统处理流量时修改这些元素。

方法：DNS Sinkhole
对于 Google 搜索，您可以将系统配置为将流量重定向到 Google SafeSearch 虚拟 IP 地址 (VIP)，对安全搜索实施过滤。

下表描述这些执行方法之间的差异。

表 *102:* 内容限制方法的比较

属性	方法：访问控制规则	方法：**DNS Sinkhole**
支持的设备	任意	Cisco Secure Firewall Threat Defense 仅
支持的搜索引擎	规则编辑器的**应用 (Applications)** 选项卡中任何标记 `safesearch supported` 的项目	仅限 Google
支持 YouTube 受限模式	是	是
需要 SSL 策略	是	否
主机必须使用 IPv4	不支持	是
连接事件日志记录	是	是

在确定要使用哪种方法时，请考虑以下限制：

- 访问控制规则方法需要一种 SSL 策略，该策略会影响性能。
- Google SafeSearch VIP 仅支持 IPv4 流量。如果您配置 DNS Sinkhole 来管理 Google 搜索，则受影响的网络上的所有主机必须使用 IPv4。

根据使用的方法，系统会记录连接事件中**原因 (Reason)** 字段的不同值：

- 访问控制规则 - 内容限制 `(Content Restriction)`
- DNS Sinkhole - `DNS 阻止 (DNS Block)`

内容限制的要求和必备条件

型号支持

任意，或如程序中所示。

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

内容限制的准则和限制

- 仅 Snort 2 支持安全搜索。
- YouTube 和 Google 不支持在访问控制规则中实施的 YouTubeEDU 功能。请删除所有配置 YouTubeEDU 的访问控制规则，因为它们实际上不起作用。您还可以删除关联的解密规则。

使用访问控制规则执行内容限制

以下步骤程序介绍了如何配置限制内容的访问控制规则。

注释 在访问控制规则中启用安全搜索或 时，内联规范化会被自动启用。

开始之前

对于经典设备，您必须拥有控制许可证。

过程

步骤 1 创建 SSL策略；请参阅创建基本 SSL 策略， 第 1728 页。

步骤 2 添加用于处理安全搜索 流量的规则：

- 选择**解密 - 重新签名 (Decrypt - Resign)** 作为规则的**操作 (Action)**。
- 在**应用 (Applications)** 中，将所选操作添加到**所选应用和过滤器 (Selected Applications and Filters)** 列表中：
  - 安全搜索 - 添加类别：搜索引擎 (Category: search engine) 过滤器。

步骤 3 为您添加的规则设置规则位置。点击并拖动，或使用右键点击菜单剪切并粘贴。

步骤 4 创建或编辑访问控制策略，并将 SSL 策略与访问控制策略相关联。

有关详细信息，请参阅将其他策略与访问控制相关联， 第 1276 页。

步骤 5 在访问控制策略中，添加用于处理安全搜索和 流量的规则：

- 选择**允许 (Allow)** 作为规则的**操作 (Action)**。
- 在**应用 (Applications)** 中，点击 **安全搜索**（ ） 的图标，然后设置相关选项。
  - 访问控制规则的安全搜索选项， 第 1442 页

- 在**应用 (Applications)** 中，优化**所选应用和过滤器 (Selected Applications and Filters)** 列表中的所选应用。

  在大多数情况下，启用安全搜索 会在**所选应用和过滤器 (Selected Applications and Filters)** 列表中填入适当的值。如果在您启用此功能时，安全搜索 应用已经存在于列表中，则系统不会自动填充列表。如果应用没有按预期填充，请按照以下方式手动添加：

  - 安全搜索 - 添加类别：搜索引擎 (Category: search engine) 过滤器。

有关详细信息，请参阅配置应用条件和过滤器，第 1294 页。

步骤 6 为您添加的访问控制规则设置规则位置。点击并拖动，或使用右键点击菜单剪切并粘贴。

步骤 7 配置系统在阻止受限内容时显示的 HTTP 响应页面；请参阅选择 HTTP 响应页面，第 1351 页。

步骤 8 部署配置更改。

访问控制规则的安全搜索选项

Firepower 系统仅支持特定搜索引擎的安全搜索过滤。有关受支持的搜索引擎的列表，请参阅访问控制规则编辑器的**应用 (Applications)** 选项卡中标记支持安全搜索 (safesearch supported) 的应用。有关不受支持的搜索引擎的列表，请参阅标记不支持安全搜索 (safesearch unsupported) 的应用。

为访问控制规则启用安全搜索时，请设置以下参数：

启用安全搜索
为匹配此规则的流量启用安全搜索过滤。

不受支持的搜索流量
指定在处理来自不受支持的搜索引擎的流量时您希望系统执行的操作。如果您选择**阻止 (Block)** 或**阻止并重置 (Block with Reset)**，还必须配置在系统阻止受限内容时所显示的 HTTP 响应页面；请参阅选择 HTTP 响应页面，第 1351 页。

使用 DNS Sinkhole 执行内容限制

通常，DNS Sinkhole 会将流量定向到特定的目标。此过程描述如何将 DNS Sinkhole 配置为将流量重定向到 Google 安全搜索虚拟 IP 地址 (VIP)，这会强制对 Google 和 YouTube 搜索结果应用内容过滤器。

由于 Google 安全搜索为 VIP 使用单个 IPv4 地址，因此主机必须使用 IPv4 寻址。

⚠

注意 如果您的网络包括代理服务器，则除非您在代理服务器和互联网之间放置 威胁防御设备，否则此内容限制方法无效。

此过程描述了仅对Google搜索实施内容限制。要对其他搜索引擎实施内容限制，请参阅使用访问控制规则执行内容限制，第 1441 页。

开始之前

此程序仅适用于 威胁防御 并需要 威胁 许可证。

过程

步骤 1 通过以下 URL 获得支持的 Google 域列表：https://www.google.com/supported_domains。

步骤 2 在本地计算机上创建自定义 DNS 列表，并添加以下条目：

- 要执行 Google 安全搜索，为每个支持的 Google 域添加一个条目。
- 要实施 YouTube 限制模式，请添加一个“youtube.com”条目。

自定义 DNS 列表必须是文本文件 (.txt) 格式。文本文件的每一行都必须指定一个单独的域名，去掉任何前导句点。例如，支持的域“.google.com”必须显示为“google.com”。

步骤 3 将自定义 DNS 列表上传到 管理中心；请参阅将新的安全情报列表上传到 Cisco Secure Firewall Management Center，第 1035 页。

步骤 4 确定 Google 安全搜索 VIP 的 IPv4 地址。例如，在 forcesafesearch.google.com 上运行 `nslookup`。

步骤 5 为安全搜索 VIP 创建一个 Sinkhole 对象；请参阅创建 Sinkhole 对象，第 1037 页。

为此对象使用以下值：

- IPv4 地址 - 输入安全搜索 VIP 地址。
- IPv6 地址 - 输入 IPv6 环回地址 (`::1`)。
- 记录到 Sinkhole 的连接 - 点击“记录连接” (Log Connections)。
- 类型 - 选择**无**。

步骤 6 创建基本的 DNS 策略；请参见创建基本 DNS 策略，第 1374 页。

步骤 7 为 Sinkhole 添加 DNS 规则；请参阅创建和编辑 DNS 规则，第 1376 页。

对于此规则：

- 选中**已启用 (Enabled)** 复选框。
- 从操作下拉列表中选择 **Sinkhole**。
- 从 **Sinkhole** 下拉列表中选择您创建的 Sinkhole 对象。
- 将您创建的自定义 DNS 列表添加到 **DNS** 上的**所选项目 (Selected Items)** 列表中。
- （可选）在**网络 (Networks)** 中选择一个网络，以将内容约束限制为特定用户。例如，如果要将内容约束限制为学生用户，请将学生分配给不同于教员的子网，并在此规则中指定该子网。

步骤 8 将 DNS 策略与访问控制策略相关联；请参阅将其他策略与访问控制相关联，第 1276 页。

步骤 9 部署配置更改。

第 XIV 部分

入侵检测和防御

第 60 章

网络分析和入侵策略概述

以下主题概述 Snort 检测引擎以及网络分析和入侵策略：

网络分析和入侵策略基础知识

网络分析和入侵策略共同用作 Firepower 系统的入侵检测和防御功能的一部分。

- 术语入侵检测通常是指被动监控并分析网络流量以查找潜在入侵，并存储攻击数据以进行安全分析的过程。这有时称为“IDS”。
- 术语入侵防御包括入侵检测的概念，但是增加了在恶意流量流经网络时对其进行拦截或更改的能力。这有时称为“IPS”。

注释 如果您使用的是 Snort 3 和 SSL 解密或 TLS 服务器身份，则您必须在**预防**模式下配置网络分析策略 (NAP)。当 Snort 3 NAP 处于检测模式时，SSL 功能将不会起作用。

在入侵防御部署中，当系统检测数据包时：

- **网络分析策略**监管如何解码和预处理流量，以便可进一步对其进行评估，尤其适用于可能表明入侵尝试的异常流量。
- **入侵策略**使用入侵和预处理程序规则（有时统称为入侵规则）根据模式检测已解码数据包是否存在攻击。入侵策略与变量集配对，这使您能够使用指定值准确反映网络环境。

网络分析和入侵策略均由父访问控制策略调用，但是在不同时间调用。在系统分析流量时，网络分析（解码和预处理）阶段发生在入侵防御（其他预处理和入侵规则）阶段之前并与其分隔开来。网络分析和入侵策略共同提供广泛且深入的数据包检测。它们可以帮助您检测、提醒和防范可能威胁主机及其数据的可用性、完整性和保密性的网络流量。

Firepower 系统随附若干以类似方式命名的网络分析和入侵策略（例如，“平衡安全性和连接”[Balanced Security and Connectivity]），这些策略是相辅相成的。通过使用系统提供的策略，您可以利用Talos 情报小组 的经验。对于这些策略，Talos 会设置入侵和预处理器规则状态，以及提供预处理器和其他高级设置的初始配置。

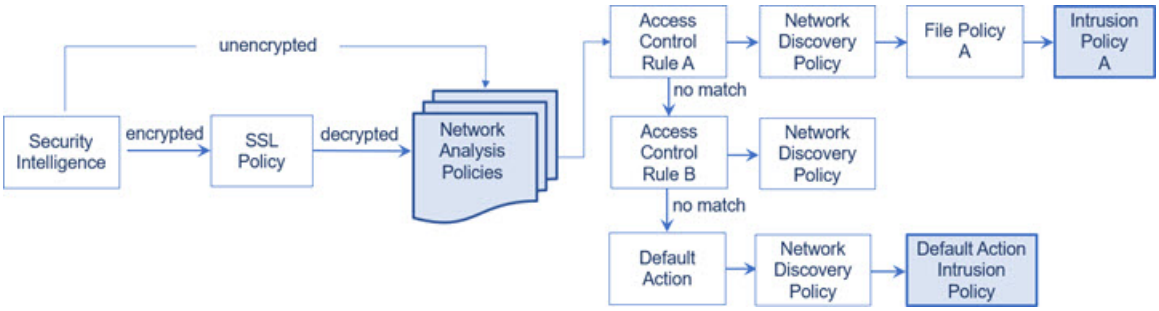
您还可以创建自定义网络分析和入侵策略。您可以调整自定义策略中的设置，以对您最重要的方式检查流量，从而能够提高受管设备的性能以及您有效响应其生成的事件的能力。

您可在网络界面中使用相似的策略编辑器创建、编辑、保存和管理网络分析和入侵策略。在您编辑任一类型的策略时，导航面板显示在网络界面的左侧；右侧显示各种配置页面。

策略如何检查流量是否存在入侵

当系统在访问控制部署过程中分析流量时，网络分析（解码和预处理）阶段发生在入侵防御（入侵规则和高级设置）阶段之前并与其分隔开来。

下图以简化方式显示内联、入侵防御和恶意软件防护 部署中的流量分析顺序。它说明访问控制策略如何调用其他策略来检测流量，以及这些策略的调用顺序。网络分析和入侵策略选择阶段突出显示。



在内联部署中（即，使用路由接口、交换接口、透明接口或内联接口对将相关配置部署到设备），系统可以在图示过程中的几乎任何步骤阻止流量而不进行进一步检查。安全智能、SSL 策略、网络分析策略、文件策略和入侵策略均可以丢弃或修改流量。只有网络发现策略（被动检测数据包）无法影响流量的流动。

类似地，在该过程的每个步骤中，数据包都可能会导致系统生成事件。入侵和预处理程序事件（有时统称为入侵事件）指示数据包或其内容可能表示安全风险。

提示 当您的 SSL 配置允许已加密流量通过，或者您未配置 SSL 检查时，此图未反映访问控制规则处理已加密流量。默认情况下，系统禁用对已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。

请注意，对于单个连接而言，虽然系统在访问控制规则之前选择网络分析策略（如图所示），但是一些预处理（特别是应用层预处理）发生在访问控制规则选择之后。这**不**影响您在自定义网络分析策略中配置预处理的方式。

解码、规范化和预处理：网络分析策略

如果没有解码和预处理，则系统无法适当评估流量是否存在入侵，因为协议差异使得无法进行模式匹配。网络分析策略在以下时机监管这些流量处理任务：

- 在流量由安全智能过滤**之后**
- 在加密流量由可选 SSL 策略解密**之后**
- 在流量可由文件或入侵策略检测**之前**

网络分析策略分阶段监管数据包处理。系统首先通过前三个 TCP/IP 层解码数据包，然后继续规范化、预处理和检测协议异常：

- 数据包解码器将数据包报头和负载转换为可由预处理器并在以后由入侵规则轻松使用的格式。TCP/IP 堆栈的各层从数据链路层开始并持续到网络层和传输层依次解码。数据包解码器还会检测数据包报头中的各种异常行为。
- 在内联部署中，内联规范化预处理程序重新格式化（规范化）流量，以尽量降低攻击者逃避检测的可能性。它会准备数据包以供其他预处理程序和入侵规则进行检测，并且帮助确保系统处理的数据包与网络上主机接收的数据包相同。

注释 在被动部署中，思科建议您在访问控制策略级别启用自适应配置文件更新，而非在网络分析级别配置内联规范化。

- 各种网络层和传输层预处理器检测利用 IP 分段的攻击，执行校验和验证并执行 TCP 和 UDP 会话预处理。

  请注意，一些高级传输和网络预处理程序设置全局适用于由访问控制策略的目标设备处理的所有流量。您在访问控制策略中而不是在网络分析策略中配置这些高级设置。

- 各种应用层协议解码器将特定类型的数据包数据规范化为入侵规则引擎可以分析的格式。通过规范化应用层协议编码，系统可以将相同的内容相关的入侵规则有效地应用于以不同方式表示其数据的数据包，并且获取有意义的结果。
- Modbus、DNP3、CIP 和 s7commplus SCADA 预处理器可检测流量异常并向入侵规则提供数据。监控与数据采集 (SCADA) 协议可监视和控制工业、基础设施以及工厂流程（例如制造、生产、水处理、配电、机场和运输系统等）并从中获取数据。
- 通过若干预处理器，可以检测特定威胁，如 Back Orifice、端口扫描、SYN 泛洪和其他基于速率的攻击。

  请注意，您在入侵策略中配置敏感数据预处理器，该预处理器用于检测敏感数据（例如，ASCII 文本中的信用卡号和社会安全保障号）。

在新建的访问控制策略中，一个默认网络分析策略监管对同一父访问控制策略调用的所有入侵策略的所有流量的预处理。最初，系统使用“平衡安全性和连接”(Balanced Security and Connectivity) 网络分析策略作为默认值，但是，可以将其更改为另一个系统提供的网络分析策略或自定义网络分析策略。在更复杂的部署中，高级用户可以分配自定义网络分析策略以预处理匹配流量，从而根据特定安全区域、网络和 VLAN 定制流量预处理选项。

访问控制规则：入侵策略选择

在初始预处理后，访问控制规则（如果存在）会评估流量。在大多数情况下，数据包匹配的第一条访问控制规则处理该流量；您可以监控、信任、阻止或允许匹配流量。

当使用访问控制规则允许流量时，系统可能按该顺序检查流量是否存在发现数据、恶意软件、受禁文件和入侵。不与任何访问控制规则匹配的流量由访问控制策略的默认操作进行处理，该操作还检查是否存在发现数据和入侵。

注释 所有数据包（**无论**哪个网络分析策略对其进行预处理）均与配置的访问控制规则相匹配，因此可能会由上而下受到入侵策略的检测。

策略如何检查流量是否存在入侵，第 1448 页中的图显示流经内联部署、入侵防御部署和恶意软件防护 部署中设备的流量，如下所示：

- Access Control Rule A 允许匹配流量通过。然后该流量由网络发现策略检查是否存在发现数据，由文件策略 A 检查是否存在受禁文件和恶意软件，最后由入侵策略 A 检查是否存在入侵。
- 访问控制规则 B 也允许匹配流量通过。但是，在此情景中，未检查流量是否存在入侵（或文件或恶意软件），因此没有与规则关联的入侵或文件策略。请注意，默认情况下，您允许通过的流量将由网络发现策略进行检查；您不需要配置此检查。
- 在此情景中，访问控制策略的默认操作允许匹配流量。然后该流量将依次由网络发现策略和入侵策略进行检查。将入侵策略与访问控制规则或默认操作相关联时，可以（但不必）使用其他入侵策略。

图中的示例不包括任何阻止或信任规则，因为系统不检测已阻止或信任的流量。

入侵检查：入侵策略、规则和变量集

在允许流量继续到达其目标之前，可以使用入侵防御作为系统的最后一道防线。入侵策略监管系统如何检测流量是否存在安全违规，并且在内联部署中可以阻止或修改恶意流量。入侵策略的主要功能是管理启用哪些入侵和预处理程序规则以及如何配置它们。

入侵和预处理程序规则

入侵规则是一组指定的关键字和参数，用于检测企图利用网络漏洞的行为；系统使用入侵规则来分析网络流量，以检测其是否与规则中的条件匹配。系统将数据包与每条规则中指定的条件进行比较，如果数据包数据与规则中指定的所有条件都匹配，则触发此规则。

系统包含Talos 情报小组 创建的以下类型的规则：

- 共享对象入侵规则，已编译且无法修改（规则标题信息除外，如源和目标端口及 IP 地址）
- 标准文本入侵规则，可以保存并修改为规则的新自定义实例。
- 预处理程序规则，是指与网络分析策略中的预处理程序和数据包解码器检测选项关联的规则。不能复制或编辑预处理程序规则。默认情况下，大多数预处理器规则是被禁用的；您必须启用它们才可以使用预处理器生成事件并在内联部署中丢弃攻击性数据包。

当系统根据入侵策略处理数据包时，首先，规则优化器会根据传输层、应用协议、受保护网络的方向等条件对子集中所有已激活的规则进行分类。然后，入侵规则引擎选择要应用于每个数据包的相应规则子集。最后，多规则搜索引擎执行三种不同类型的搜索以确定流量是否与规则匹配：

- 协议字段搜索在应用协议的特定字段中查找匹配项。
- 一般内容搜索在数据包负载中查找 ASCII 或二进制字节匹配项。
- 数据包异常搜索查找违反既定协议（而不是包含特定内容）的数据包报头和负载。

在自定义入侵策略中，您可以通过启用和禁用规则以及通过编写和添加自己的标准文本规则来调整检测。还可以遵从思科 的建议，将您的网络中检测到的操作系统、服务器和客户端应用协议与为保护这些资产而特别编写的规则相关联。

变量集

只要系统使用入侵策略来评估流量，它便会使用关联的变量集。变量集中的大多数变量表示入侵规则中常用于识别源和目标 IP 地址及端口的值。您还可以在入侵策略中使用变量表示规则禁止和动态规则状态中的 IP 地址。

系统提供单个由预定义默认变量组成的默认变量集。大多数系统提供的共享对象规则和标准文本规则均使用这些预定义的默认变量来定义网络和端口号。例如，大部分规则使用变量 `$HOME_NET` 指定受保护网络，使用变量 `$EXTERNAL_NET` 指定未受保护（或外部）网络。此外，专用规则通常会使用其他预定义的变量。例如，检测针对网络服务器的漏洞攻击的规则使用 `$HTTP_SERVERS` 和 `$HTTP_PORTS` 变量。

提示 即使您使用系统提供的入侵策略，思科也**强烈**建议修改默认变量集中的关键默认变量。当使用准确反映网络环境的变量时，处理会得以优化，并且系统可以监控相关系统是否存在可疑活动。高级用户可以创建并使用自定义变量集与一个或多个自定义入侵策略配对。

相关主题

预定义默认变量 ，第 1044 页

入侵事件生成

当系统识别可能的入侵时，它会生成入侵或预处理程序事件（有时统称为入侵事件）。受管设备将其事件传输到管理中心，在其中可以查看聚合数据并更好地了解针对网络资产的攻击。在内联部署中，受管设备还可以丢弃或替换已知有害的数据包。

数据库中的每个入侵事件均包括事件报头并包含有关事件名称和分类的信息；源和目标 IP 地址；端口；生成事件的进程；事件的日期和时间，以及有关攻击源及其目标的情景信息。对于基于数据包的事件，系统还会记录一个或多个已触发事件的数据包的已解码数据包报头和负载的副本。

数据包解码器、预处理程序和入侵规则引擎均会导致系统生成事件。例如：

- 如果数据包解码器（在网络分析策略中配置）接收少于 20 字节（没有任何选项或负载的 IP 数据报的大小）的 IP 数据包，解码器将此解释为异常流量。如果之后启用了用于检测数据包的入侵策略中的配套解码器规则，则系统会生成预处理程序事件。
- 如果 IP 分片重组预处理程序遇到一系列重叠的 IP 片段，则预处理程序会将此解释为可能的攻击，当启用了配套预处理程序规则时，系统会生成预处理程序事件。
- 在入侵规则引擎内，大多数标准文本规则和共享对象规则编写为在由数据包触发时会生成入侵事件。

随着数据库累计入侵事件，您可以开始分析潜在攻击。系统为您提供复审入侵事件和评估其在网络环境与安全策略情境中是否重要所需的工具。

系统提供的与自定义的网络分析和入侵策略

创建新的访问控制策略是使用系统管理流量过程中的头几个步骤之一。默认情况下，新创建的访问控制策略调用系统提供的网络分析和入侵策略来检测流量。

下图显示内联的入侵防御部署中新创建的访问控制策略最初如何处理流量。预处理和入侵防御阶段突出显示。

图 *146:* 新的访问控制策略：入侵防御

请注意以下各种操作的方式：

- 默认网络分析策略监管由访问控制策略处理的所有流量的预处理。最初，系统提供的 *Balanced Security and Connectivity* 网络分析策略是默认策略。
- 访问控制策略的默认操作允许由系统提供的 *Balanced Security and Connectivity* 入侵策略确定的所有非恶意流量。由于默认操作允许流量通过，在入侵策略能够检查并可能阻止恶意流量之前，发现功能可以检查流量中的主机、应用和用户数据。
- 策略使用默认的安全情报选项（仅全局阻止列表和非阻止列表），不使用 SSL 解密已加密的流量，并且不使用访问控制规则对网络流量执行特殊处理和检查。

可以采取用于调整入侵防御部署的一个简单步骤是使用系统提供的一组不同的网络分析和入侵策略为作为默认值。Cisco 通过系统提供若干对策略。

或者，您可以通过创建和使用自定义策略来定制入侵防御部署。您可能会发现这些策略中配置的预处理程序选项、入侵规则和其他高级设置无法满足网络的安全需求。通过调整网络分析和入侵策略，可以非常精细地配置系统如何处理网络流量并检测其是否存在入侵。

系统提供的网络分析和入侵策略

思科通过 Firepower 系统提供若干对网络分析和入侵策略。通过使用系统提供的网络分析和入侵策略，您可以利用Talos 情报小组 的经验。对于这些策略，Talos 会提供入侵和预处理器规则状态，以及预处理器和其他高级设置的初始配置。

没有哪一个系统提供的策略能够涵盖所有的网络配置文件、流量组合或防御安全状况。但每个此类策略都涵盖常见情况和网络设置，为提供精细调整的防御策略奠定基础。虽然您可以按原样使用系统提供的策略，但思科强烈建议您将其作为自定义策略的基础，对其进行调整以适合您的网络。

提示 即使您使用系统提供的网络分析和入侵策略，也应该配置系统的入侵变量，以准确反映网络环境。至少应修改默认变量集中的关键默认变量。

随着新的漏洞被发现，Talos 会发布入侵规则更新（也称为 *Snort* 规则更新）。这些规则更新可以修改系统提供的任何网络分析或入侵策略，并且可以提供新的和已更新的入侵规则及预处理程序规则、现有规则的已修改状态，以及已修改的默认策略设置。规则更新还可以从系统提供的策略中删除规则，并且提供新规则类别，以及修改默认变量集。

如果规则更新影响您的部署，则网络界面将受影响的入侵和网络分析策略标记为已过期，并标记其父访问控制策略。您必须重新部署已更新的策略才能使其更改生效。

为方便起见，可以将规则更新配置为自动重新部署受影响的入侵策略（单独或与受影响的访问控制策略组合）。这使您能够轻松、自动保持部署为最新，以防范最近发现的漏洞和入侵。

为了确保获得最新的预处理设置，**必须**重新部署访问控制策略，该策略也会重新部署与当前运行的策略不同的所有关联的 SSL、网络分析和文件策略，同时还可以更新高级预处理和性能选项的默认值。

思科通过 Firepower 系统提供以下网络分析和入侵策略：

“平衡安全和连接”网络分析和入侵策略

这些策略专为速度和检测而构建。共同使用时，这些策略充当大多数组织和部署类型的良好起点。系统在大多数情况下均使用 Balanced Security and Connectivity 策略和设置作为默认值。

Connectivity Over Security 网络分析和入侵策略

这些策略专为连接性（能够获取所有资源）优先于网络基础设施安全性的组织而构建。此入侵策略启用的规则远远少于“安全优先于连接”策略中启用的规则。仅会启用阻止流量的最重要规则。

“安全优先于连接”网络分析和入侵策略

这些策略专为网络基础设施安全性优先于用户便利性的组织而构建。此入侵策略将启用许多可能会提醒或丢弃合法流量的网络异常入侵规则。

“最大检测”网络分析和入侵策略

此类策略适用于网络基础设施安全性比在“安全性优先于连接”(Security Over Connectivity) 策略中还要重要，有可能产生更大运营影响的组织。例如，入侵策略将启用大量威胁类别中的规则，包括恶意软件、攻击程序包、旧漏洞和常见漏洞及已知外部攻击程序。

No Rules Active 入侵策略

在“无活动规则”入侵策略中，所有入侵规则和所有高级设置（除入侵规则阈值外）均已禁用。如果您要创建自己的入侵策略而不是将其基于系统提供的其他策略之一中的已启用规则，可以尝试使用此策略。

注释 根据所选的系统提供的基本策略，该策略的设置有所不同。要查看策略设置，请点击策略旁边的**编辑**图标，然后点击**管理基本策略**链接。

自定义网络分析和入侵策略的优势

您可能会发现系统提供的网络分析和入侵策略中配置的预处理程序选项、入侵规则和其他高级设置不完全满足贵组织的安全需要。

构建自定义策略可以提高环境中系统的性能，并且可以密切关注网络上发生的恶意流量和策略违例。通过创建和调整自定义策略，可以非常精细地配置系统如何处理和检查网络流量是否存在入侵。

所有自定义策略都具有基本策略（也称为基层），用于为策略中所有配置定义默认设置。层是可用于高效管理多个网络分析或入侵策略的构建块。

在大多数情况下，自定义策略基于系统提供的策略，但是可以使用其他自定义策略。不过，所有自定义策略在策略链中都以系统提供的策略作为最终基础。由于规则更新可能会修改系统提供的策略，因此导入规则更新可能会对您产生影响，即使使用自定义策略作为基础也如此。如果规则更新影响部署，则 Web 界面将受影响策略标记为过期。

自定义网络分析策略的优势

默认情况下，一个网络分析策略预处理访问控制策略处理的所有未加密流量。这意味着所有数据包都根据相同设置进行解码和预处理，无论后来使用哪种入侵策略（和因此使用的入侵规则集）对其进行检测。

最初，系统提供的 Balanced Security and Connectivity 网络分析策略是默认策略。调整预处理的一个简单方法是创建并使用自定义网络分析策略作为默认值。

可用的调整选项因预处理程序而异，但是可以调整预处理程序和解码器的一些方法包括：

- 可以禁用不适用于正在监控的流量的预处理程序。例如，HTTP Inspect 预处理程序规范化 HTTP 流量。如果确信网络中没有任何使用 Microsoft 互联网信息服务 (IIS) 的 Web 服务器，则可以禁用查找特定于 IIS 的流量的预处理程序选项，从而减少系统处理开销。

注释 如果禁用自定义网络分析策略中的预处理器，但系统稍后需要使用该预处理器利用已启用的入侵或预处理器规则对数据包进行评估，系统会自动启用并使用预处理器，不过它在网络分析策略 Web 界面中保持禁用。

- 指定端口（如果适用）以关注某些预处理程序的活动。例如，可以确定要对DNS服务器响应或加密 SSL 会话进行监控的其他端口，或者确定解码 telnet、HTTP 和 RPC 流量所在的端口

对于复杂部署的高级用户，可以创建多个网络分析策略，每个策略定制为以不同方式预处理流量。然后，可以配置系统使用这些策略管理使用不同的安全区域、网络或 VLAN 的流量的预处理。

注释 使用自定义网络分析策略（尤其是多个网络分析策略）定制预处理是一个高级任务。由于预处理和入侵检测密切相关，因此，您**必须**注意，要确保允许检测单个数据包的网络分析和入侵策略能够互补。

自定义入侵策略的优势

在新建的初始配置为执行入侵防御的访问控制策略中，默认操作允许所有流量，但是首先会使用系统提供的 Balanced Security and Connectivity 入侵策略对流量进行检测。除非添加访问控制规则或更改默认操作，否则所有流量都由该入侵策略进行检查。

要自定义入侵防御部署，可以创建多个入侵策略，每个策略定制为以不同方式检测流量。然后，使用指定哪个策略检测哪个流量的规则来配置访问控制策略。访问控制规则可能很简单，也可能很复杂，使用多个条件来匹配和检测流量，包括安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL 或用户。

入侵策略的主要功能是管理启用哪些入侵和预处理器规则及其如何配置，如下所示：

- 在每个入侵策略中，应该验证所有适用于环境的规则是否已启用，并且通过禁用不适用于环境的规则来提高性能。在内联部署中，可以指定哪些规则应该丢弃或修改恶意数据包。
- 如果遵从Cisco的建议，则可将您的网络中检测到的操作系统、服务器和客户端应用协议与为保护这些资产而特别编写的规则相关联。
- 您可以修改现有规则并根据需要编写新的标准文本规则，以捕获新的漏洞或强制实施安全策略。

您可能对入侵策略进行的其他自定义包括：

- 敏感数据预处理器检测敏感信息，例如 ASCII 文本格式的信用卡号和社会保障号。请注意，在网络分析策略中配置了用于检测特定威胁（back orifice 攻击、多种端口扫描类型以及尝试以过多流量淹没网络的基于速率的攻击）的其他预处理程序。
- 全局阈值导致系统根据与入侵规则匹配的流量在指定时间段内源自或流向特定地址或地址范围的次数来生成事件。这有助于防止系统被大量事件淹没。
- 禁止入侵事件通知和设置个别规则或全体入侵策略的阈值也可以防止系统被大量事件淹没。
- 除了网络界面中的各种入侵事件视图之外，您还可以启用将日志记录到系统日志工具或者将事件数据发送到 SNMP 陷阱服务器。根据策略，可以指定入侵事件通知限制，设置发送到外部日志记录工具的入侵事件通知，以及配置对入侵事件的外部响应。请注意，除了基于策略的这些警报配置，对于每个规则或规则组，您还可以在入侵事件上全局启用或禁用邮件警报。无论哪个入侵规则处理数据包，都会使用您的邮件警报设置。

自定义策略的限制

由于预处理和入侵检测如此密切相关，因此，您**必须**小心确保自己的配置允许网络网络分析和入侵策略处理和检测单个数据包，以实现互补。

默认情况下，系统使用一个网络分析策略预处理由受管设备使用单个访问控制策略处理的所有流量。下图显示内联的入侵防御部署中新创建的访问控制策略最初如何处理流量。预处理和入侵防御阶段突出显示。

图 *147:* 新的访问控制策略：入侵防御

请留意默认网络分析策略如何监管访问控制策略处理的所有流量的预处理。最初，系统提供的Balanced Security and Connectivity 网络分析策略是默认策略。

调整预处理的一个简单方法是创建并使用自定义网络分析策略作为默认值。但是，如果在自定义网络分析策略中禁用预处理器，但系统需要根据已启用的入侵或预处理器规则评估预处理的数据包，则系统会自动启用并使用该预处理器，尽管其在网络分析策略 Web 界面中保持禁用。

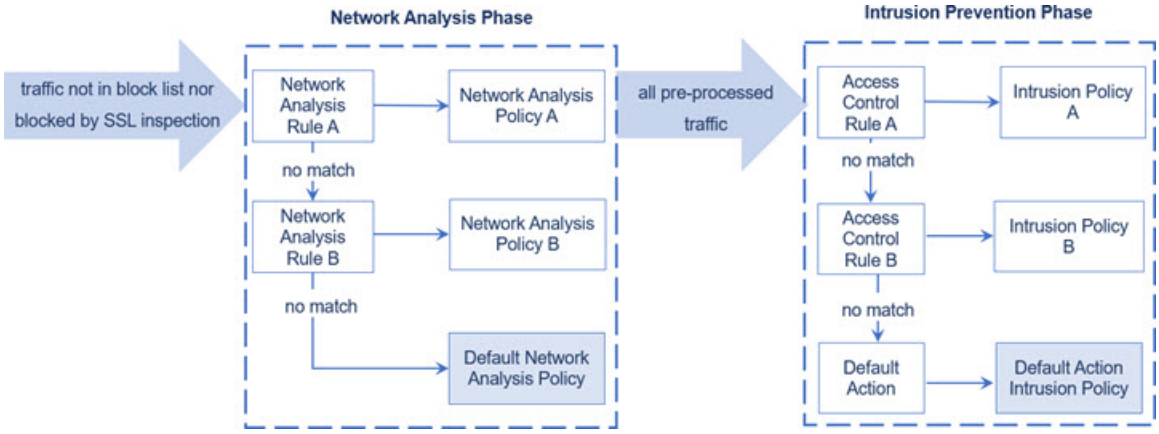
注释 要获取禁用预处理程序的性能优势，您**必须**确保自己的入侵策略均未启用需要该预处理程序的规则。

如果使用多个自定义网络分析策略，则会引起其他问题。对于使用复杂部署的高级用户，可以分配自定义网络分析策略以预处理匹配流量，从而根据特定安全区域、网络和 VLAN 自定义预处理。为此，请向访问控制策略中添加自定义网络分析规则。每条规则均具有关联的网络分析策略，用于监管与该规则匹配的流量的预处理。

提示 可以将网络分析规则配置为访问控制策略中的高级设置。与系统中其他类型的规则不同，网络分析规则调用网络分析策略，而不是被其包含。

系统按规则号由上而下将数据包与任何已配置的网络分析规则相匹配。不与任何网络分析规则相匹配的流量由默认网络分析策略预处理。虽然这使您在预处理流量时具有极大灵活性，但请记住，所有数据包**无论**由哪个网络分析策略进行了预处理，后来都会在各自的进程中与访问控制规则匹配，从而可能会接受入侵策略的检查。换句话说，使用特定网络分析策略预处理数据包**不**保证将通过任何特殊入侵策略检测该数据包。您**必须**仔细配置访问控制策略，以使其调用正确的网络分析和入侵策略来评估特殊数据包。

下图集中细解了网络分析策略（预处理）选择阶段如何在入侵防御（规则）阶段之前发生并与其分隔开来。为简单起见，此图省去了发现和文件/恶意软件检查阶段。它还突出显示默认网络分析和默认操作入侵策略。



在此情景中，访问控制策略配置有两条网络分析规则和一个默认网络分析策略：

- 网络分析规则 A 使用网络分析策略 A 预处理匹配流量。之后，您希望此流量由入侵策略 A 进行检测。
- 网络分析规则 B 使用网络分析策略 B 预处理匹配流量。之后，您希望此流量由入侵策略 B 进行检测。
- 所有剩余流量都使用默认网络分析策略进行预处理。之后，您希望此流量由与访问控制策略的默认操作关联的入侵策略进行检测。

系统在预处理流量之后，可以检测流量是否存在入侵。该图显示具有两条访问控制规则和一个默认操作的访问控制策略：

- 访问控制规则 A 允许匹配流量。然后，流量由入侵策略 A 进行检测。
- 访问控制规则 B 允许匹配流量。然后，流量由入侵策略 B 进行检测。
- 访问控制策略的默认操作允许匹配流量。然后，流量由默认操作的入侵策略进行检测。

每个数据包的处理均由网络分析策略和入侵策略对进行监管，但系统**不**为您协调该对。请考虑以下情景：访问控制策略配置错误，以致网络分析规则 A 和访问控制规则 A 不处理相同流量。例如，您可能希望配对的策略监管特殊安全区域上流量的处理，但是在两条规则的条件中错误地使用不同的区域。这可能会导致错误地预处理流量。因此，使用网络分析规则和自定义策略定制预处理是一项**高级**任务。

请注意，对于单个连接而言，虽然系统在访问控制规则之前选择网络分析策略，但是一些预处理（特别是应用层预处理）发生在访问控制规则选择之后。这**不**影响您在自定义网络分析策略中配置预处理的方式。

网络分析和入侵策略的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

网络分析和入侵策略的要求和必备条件

型号支持

任意。

支持的域

任意

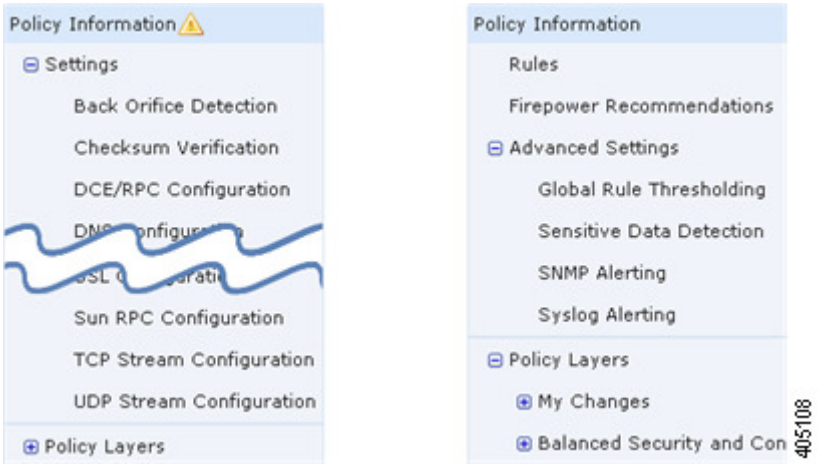
用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

导航面板：网络分析和入侵策略

网络分析和入侵策略使用类似的 Web 界面编辑和保存对其配置进行的更改。

编辑任一类型的策略时，导航面板会出现在网络界面左侧。下图显示网络分析策略（左）和入侵策略（右）的导航面板。



分隔线将导航面板分隔成指向策略设置的链接，可以通过（下方）或不通过（上方）与策略层的直接交互来配置这些设置。要导航到任何设置页面，请在导航面板中点击其名称。某项在导航面板中的浓阴影突出显示当前设置页面。例如，在上方的插图中，“策略信息”页面会显示到导航面板的右侧。

策略信息

“策略信息”页面提供常用设置的配置选项。如以上网络分析策略面板的插图所示，当策略包含未保存的更改时，在导航面板中的**策略信息 (Policy Information)** 旁边会显示**策略更改图标**。保存更改后，该图标消失。

Rules（仅入侵策略）

通过入侵策略中的“规则”(Rules) 页面，您可以为共享对象规则、标准文本规则和预处理器规则配置规则状态和其他设置。

思科 建议（仅入侵策略）

通过入侵策略中的“思科 建议”页面，您可以将在网络上检测到的操作系统、服务器和客户端应用协议与专门编写用于保护这些资产的入侵规则相关联。这样，您就可根据自己的受监控网络的特定需求定制您的入侵策略。

Settings（网络分析策略）和 Advanced Settings（入侵策略）

网络分析策略中的“设置”(Settings) 页面可供您启用或禁用预处理程序以及访问预处理程序配置页面。展开 **Settings** 链接会显示指向策略中所有已启用预处理程序的个别配置页面的子链接。

入侵策略中的Advanced Settings页面可供您启用或禁用高级设置以及访问这些高级设置的配置页面。展开 **Advanced Settings** 链接会显示指向策略中所有已启用高级设置的个别配置页面的子链接。

Policy Layers

“策略层”(Policy Layers) 页面显示构成网络分析或入侵策略的各层的摘要。展开“策略层”(Policy Layers) 链接会显示指向策略中的各层的摘要页面的子链接。展开各层子链接会显示指向层中已启用的所有规则、预处理程序或高级设置的配置页面的进一步子链接。

冲突和更改：网络分析和入侵策略

在编辑网络分析或入侵策略时， **策略更改图标** 显示在导航面板中**策略信息 (Policy Information)** 的旁边以指示策略包含未保存的更改。必须首先保存（或提交）更改，然后系统才会认可这些更改。

注释 保存后，必须部署网络分析或入侵策略，更改才会生效。如果部署策略而不保存，则系统会使用最新保存的配置。

解决编辑冲突

“网络分析策略”页面（**策略 > 访问控制**，然后点击 **网络分析策略**或**策略 > 访问控制 > 入侵**，然后点击 **网络分析策略**）和“入侵策略”页面（**策略 > 访问控制 > 入侵**）显示每个策略是否有未保存的更改，以及有关当前正在编辑策略的用户的信息。思科建议每次仅由一位人员编辑一个策略。如果执行同时编辑，则将产生以下后果：

- 如果在您编辑某条网络分析或入侵策略的同时另一用户也在编辑该策略，并且该用户保存对此策略的更改，则当您提交策略时系统将警告您会覆盖另一用户的更改。
- 如果以同一用户身份通过多个网络界面实例编辑同一网络分析或入侵策略，而且，您保存对一个实例的更改，则无法保存对其他实例的更改。

解析配置依赖关系

为了执行特殊分析，许多预处理程序和入侵规则均要求流量首先以某种方式得以解码或预处理，或者具有其他依存关系。保存网络分析或入侵策略时，系统会自动启用必需的设置，或者警告您已禁用的设置不会影响流量，如下所示：

- 如果已添加 SNMP 规则警报，但未配置 SNMP 告警，则无法保存入侵策略。必须配置 SNMP 告警或禁用规则警报，然后再次保存。
- 如果入侵策略包含已启用的敏感数据规则，但是您尚未启用敏感数据预处理程序，则无法保存该入侵策略。必须允许系统启用预处理程序并保存策略，或者禁用规则并再次保存。
- 如果在网络分析策略中禁用必需的预处理程序，则仍然可以保存该策略。但是，系统会通过已禁用预处理程序的当前设置使用该预处理程序，即使该预处理程序在网络界面中保持禁用亦如此。
- 如果在网络分析策略中禁用内联模式，但是启用内联规范化预处理程序，则仍然可以保存该策略。不过，系统会警告您将忽略规范化设置。禁用内联模式还会导致系统忽略允许预处理程序修改或阻止流量的其他设置，包括校验和验证和基于速率的攻击防御。

提交、丢弃和缓存策略更改

在编辑网络分析或入侵策略时，如果退出策略编辑器而不保存更改，则系统会缓存这些更改。即使注销系统或系统崩溃，仍然会缓存更改。系统缓存可以按照每个用户一个网络分析和一个入侵策略来存储未保存的更改；编辑同一类型的另一个策略之前，必须提交或放弃更改。编辑另一个策略而不保存对第一个策略的更改时，或者导入入侵规则更新时，系统会丢弃缓存的更改。

您可以在网络分析或入侵策略编辑器的“策略信息”(Policy Information) 页面上提交或丢弃策略更改。

在 Cisco Secure Firewall Management Center配置中，您可以控制：

- 是否提示（或要求）您在提交网络分析或入侵策略更改时对其添加注释
- 是否将更改和注释记录到审核日志中

退出网络分析或入侵策略

过程

如果要退出网络分析或入侵策略高级编辑器，您有以下选择：

- 缓存 - 要退出策略和缓存更改，请选择任何菜单或指向另一个页面的其他路径。请在系统提示时点击**离开页面 (Leave page)** 退出，或者点击**停留在页面上 (Stay on page)** 停留在高级编辑器中。
- 放弃 - 要放弃未保存的更改，请点击“策略信息”(Policy Information) 页面上的**放弃更改 (Discard Changes)**，然后点击**确定 (OK)**。
- 保存 - 要保存对策略的更改，请点击“策略信息”(Policy Information) 页面上的**确认更改 (Commit Changes)**。如果出现提示，请输入注释，然后点击**确认 (OK)**。

第 61 章

入侵策略使用入门

以下主题介绍如何开始使用入侵策略：

入侵策略基础知识

入侵策略是已定义的几组入侵检测和防护配置，用于检查流量是否存在安全违规，以及在内联部署中阻止或修改恶意流量。入侵策略供访问控制策略调用，是系统在允许流量到达目标之前的最后一道防线。

每个入侵策略的中心是入侵规则。启用的规则导致系统为匹配规则的流量生成入侵事件（或阻止该流量）。禁用规则将停止该规则的处理。

系统提供几种基本入侵策略，使您可以利用 Talos 情报小组的经验。对于这些策略，Talos 设置入侵和预处理器规则状态（启用或禁用），并提供其他高级设置的初始配置。

提示 系统提供的入侵和网络分析策略具有类似的名称，但包含不同的配置。例如，“平衡安全性和连接”(Balanced Security and Connectivity) 网络分析策略和“平衡安全性和连接”(Balanced Security and Connectivity) 入侵策略共同发挥作用，均可在入侵规则更新中更新。但是，网络分析策略管理的主要是预处理选项，而入侵策略管理的主要是入侵规则。

如果创建自定义入侵策略，您可以：

- 通过启用和禁用规则，以及撰写和添加您自己的规则来调整检测。
- 遵从思科 的建议，将您的网络中检测到的操作系统、服务器和客户端应用协议与为保护这些资产而特别编写的规则相关联。
- 配置各种高级设置，例如，外部警告，敏感数据预处理和全局规则阈值。
- 使用分层作为构建块，以有效地管理多个入侵策略。

在内联部署中，入侵策略可以阻止和修改流量：

- 丢弃规则可以丢弃匹配的数据包和生成入侵事件。要配置入侵或预处理器丢弃规则，请将其状态设置为“丢弃并生成事件”(Drop and Generate Events)。
- 入侵规则可使用 `replace` 关键字来替换恶意内容。

要使入侵规则影响流量，必须正确配置丢弃规则和内容替换规则，以及正确部署内联受管设备，也就是与内联接口集内联。最后，必须启用入侵策略的丢弃行为或 **Drop when Inline** 设置。

当定制入侵策略时，特别是在启用和添加规则时，请记住一些入侵规则要求首先以某种方式对流量进行解码或预处理。在入侵策略检查数据包之前，数据包根据网络分析策略中配置对其进行预处理。如果您禁用一个必需的预处理程序，虽然该预处理程序在网络分析策略 Web 界面中保持禁用，但系统仍自动通过其当前设置使用它。

⚠

注意 由于预处理和入侵检查密切相关，因此用于检查单个数据包的网络分析和入侵策略**必须**相互补充。定制预处理（特别是使用多个自定义网络分析策略）是一个**高级**任务。

在配置自定义入侵策略后，可以在访问控制配置过程中通过以下方式使用该策略：将入侵策略与一个或多个访问控制规则或访问控制策略的默认操作相关联。这会强制系统在某个允许的流量到达最终目的地之前使用入侵策略检查该流量。与入侵策略共同使用的变量集，用于准确地反映您的家庭和外部网络以及网络上的服务器（如果适当）。

请注意，默认情况下，系统禁用加密负载的入侵检查。当加密连接与已配置入侵检查的访问控制规则匹配时，这有助于减少误报和提高性能。

入侵策略的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

入侵策略的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

管理入侵策略

在“入侵策略”页面（**策略** > **访问控制** > **入侵**）上，可以查看当前自定义入侵策略以及下列信息：

- 最近一次修改策略的时间和日期（采用当地时间）以及执行此修改的用户。
- 是否已启用**内联时丢弃 (Drop when Inline)** 设置，该设置允许您在内联部署中丢弃和修改流量。内联部署可以是使用路由、交换或透明接口，或内联接口对部署到设备上的配置。
- 哪些访问控制策略和设备在使用入侵策略检查流量
- 策略是否有未保存的更改，以及有关何人（如果有任何人）当前正在编辑该策略的信息
- 在多域部署中，创建了策略的域

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 管理入侵策略：

- 比较 - 点击**比较策略 (Compare Policies)**；请参阅比较策略，第 148 页。
- 创建 - 点击**创建策略 (Create Policy)**；请参阅：
  - Snort 2 策略的 创建自定义 Snort 2 入侵策略，第 1466 页。
  - 最新版本的《Cisco Secure Firewall Management Center Snort 3 配置指南》中适用于 Snort 3 策略的创建自定义 *Snort 3* 入侵策略主题。

- 删除 - 点击要删除的策略旁边的 **删除**（ ）。如果另一用户在策略中有未保存的更改，则系统会提示您确认并进行通知。点击 **OK** 确认。

  如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

- 编辑 - 选择：
  - **Snort 2 版本 (Snort 2 Version)**；请参阅编辑 Snort 2 入侵策略，第 1467 页。
  - **Snort 3 版本**；请参阅最新版本的《Cisco Secure Firewall Management Center Snort 3 配置指南》中的编辑 *Snort 3* 入侵策略主题。

  如果显示**视图**（ ），则表明配置属于祖先域，或者您没有修改配置的权限。

- 导出 - 如果要导出入侵策略以在其他 Cisco Secure Firewall Management Center 上进行导入，请点击 **YouTube EDU**（ ）；请参阅《Cisco Secure Firewall Management Center 管理指南》中的导出配置。
- 部署 - 选择**部署** > **部署**；请参阅部署配置更改，第 136 页。
- 报告 - 点击**报告**（ ）；请参阅生成当前策略报告，第 149 页。

自定义入侵策略创建

当您创建新的入侵策略时，必须为其提供唯一的名称，指定基本策略并指定丢弃行为。

基本策略定义入侵策略的默认设置。修改新策略中的设置会覆盖（但不会更改）基本策略中的该设置。您可以使用系统提供的策略或自定义策略作为您的基本策略。

创建自定义 Snort 2 入侵策略

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 点击**创建策略**。如果您在另一策略中有未保存的更改，当系统提示您返回“入侵策略”(Intrusion Policy) 页面时，请点击**取消 (Cancel)**。

确保选择**入侵策略 (Intrusion Policies)** 选项卡。

步骤 3 在**名称 (Name)** 和**说明 (Description)**（可选）中输入唯一名称和说明。

步骤 4 选择**监测模式 (Inspection Mode)**。

所选操作确定是入侵规则阻止并发出警报（**防御** 模式）还是仅发出警报（**检测** 模式）。

步骤 5 选择初始**基本策略 (Base Policy)**。

您可以使用系统提供的策略或其他自定义策略作为您的基本策略。

步骤 6 点击**保存 (Save)**。

新策略的设置与其基本策略相同。

相关主题

层中的入侵规则，第 1615 页
冲突和更改：网络分析和入侵策略，第 1459 页

编辑 Snort 2 入侵策略

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 确保选择**入侵策略 (Intrusion Policies)** 选项卡。

步骤 3 点击要配置的入侵策略旁边的 **Snort 2 版本** 。

步骤 4 编辑策略：

- 更改基本策略 - 从**基本策略 (Base Policy)** 下拉列表中选择基本策略；请参阅更改基本策略，第 1610 页。
- 配置高级设置 - 点击导航面板中的**高级设置 (Advanced Settings)**；请参阅入侵策略高级设置，第 1471 页。
- 配置思科 配置 Firepower 建议的入侵规则 - 点击导航面板中的**思科建议 (Cisco Recommendations)**；请参阅生成和应用思科 建议，第 1624 页。
- 丢弃内联部署中的行为 - 选中或取消选中**内联时丢弃 (Drop when Inline)**；请参阅设置内联部署中的丢弃行为，第 1470 页。
- 按建议的规则状态过滤规则 - 生成建议后，点击每个建议类型旁边的**查看 (View)**。点击**查看建议的更改 (View Recommended Changes)** 以查看所有建议。
- 按当前规则状态过滤规则 - 点击每个规则状态类型（生成事件、丢弃和生成事件）旁边的**查看 (View)**；请参阅入侵策略中的入侵规则过滤器，第 1481 页。
- 管理策略层 - 点击导航面板中的**策略层 (Policy Layers)**；请参阅层管理，第 1612 页。
- 管理入侵规则 - 点击**管理规则 (Manage Rules)**；请参阅查看入侵策略中的入侵规则，第 1475 页。
- 查看基本策略中的设置 - 点击**管理基本策略 (Manage Base Policy)**；请参阅基本层，第 1609 页。

步骤 5 要保存自上次策略确认以来在此策略中进行的更改，请选择**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

相关主题

生成和应用思科 建议 ，第 1624 页
配置层中的入侵规则 ，第 1616 页
冲突和更改：网络分析和入侵策略 ，第 1459 页

入侵策略更改

当创建新的入侵策略时，它具有与其基本策略相同的入侵规则和高级设置。

系统为每个用户缓存一个入侵策略。在编辑入侵策略时，如果您选择任何菜单或指向另一页的其他路径，即使您离开此页，更改也会保留在系统缓存中。

用于执行入侵防御的访问控制规则配置

访问控制策略可能有多个与入侵策略相关联的访问控制规则。您可以为任何 Allow 或 Interactive Block 访问控制规则配置入侵检测，这样，您就可在网络中不同类型的流量到达最终目的地之前，使不同的入侵检测配置文件与其匹配。

只要系统使用入侵策略来评估流量，它便会使用关联的变量集。变量集中的变量代表通常在入侵规则中用来识别源 IP 地址、目标 IP 地址、源端口和目标端口的值。您还可以在入侵策略中使用变量表示规则禁止和动态规则状态中的 IP 地址。

提示 即使您使用系统提供的入侵策略，思科也**强烈**建议您配置系统的入侵变量以准确反映您的网络环境。至少，要修改默认变量集中的默认变量。

了解系统提供的入侵策略和自定义入侵策略

思科通过 Firepower 系统提供多种入侵策略。通过使用系统提供的入侵策略，您可以利用 Talos 情报小组 的经验。对于这些策略，Talos 会设置入侵和预处理器规则状态，并提供高级设置的初始配置。可以按现状使用系统提供的策略，也可以将其用作自定义策略的基础。构建自定义策略可以提高系统在您的环境中的性能，并提供网络上发生的恶意流量和策略违规行为的集中视图。

连接和入侵事件日志记录

当访问控制规则调用的入侵策略检测到入侵并生成入侵事件时，它会将此事件保存到 Cisco Secure Firewall Management Center。无论访问控制规则采用何种日志记录配置，系统都会将发生入侵的连接结束自动记录到 Cisco Secure Firewall Management Center数据库。

相关主题

预定义默认变量 ，第 1044 页

访问控制规则配置和入侵策略

请注意，您在单个访问控制策略中可以使用的唯一入侵策略的数量取决于目标设备型号；设备的功能越强大，处理的策略就越多。每个唯一的入侵策略和变量集**对均**视为一个策略。虽然您可以将不同的入侵策略-变量集对与每条“允许”(Allow) 和“交互式阻止”(Interactive Block) 规则（以及默认操作）相关联，但是，如果目标设备没有足够的资源可按照配置执行检测，则无法部署访问控制策略。

配置访问控制规则以执行入侵防御

您必须是管理员，访问管理员或网络管理员用户才能执行此任务。

过程

步骤 1 在访问控制策略编辑器中，创建新规则或编辑现有规则；请参阅访问控制规则组成部分，第 1282 页。

步骤 2 确保规则操作设置为 **Allow**、**Interactive Block** 或 **Interactive Block with reset**。

步骤 3 点击 **检测**。

步骤 4 选择系统提供的或自定义**入侵策略 (Intrusion Policy)**，或选择**无 (None)** 以禁用对与访问控制规则相匹配的流量进行的入侵检查。

步骤 5 如果要更改与入侵策略关联的变量集，请从**变量集 (Variable Set)** 下拉列表中选择值。

步骤 6 点击**保存 (Save)** 保存规则。

步骤 7 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改。

相关主题

变量集，第 1042 页
Snort® 重新启动场景，第 143 页

内联部署中的丢弃行为

如果要评估配置如何在内联部署中起作用（即，使用路由式、交换式或透明接口或内联接口对将相关配置部署到设备），而实际上不影响流量，则可以禁用丢弃行为。在这种情况下，系统生成入侵事件，但不会丢弃触发丢弃规则的数据包。当对结果满意时，可以启用丢弃行为。

请注意，在分流模式下，在被动部署或内联部署中，无论丢弃行为如何，系统都无法影响流量。在被动部署中，设置为**丢弃和生成事件 (Drop and Generate Events)** 的规则与设置为**生成事件 (Generate Events)** 的规则行为完全相同。系统生成入侵事件，但不能丢弃数据包。

注释 假设文件阻止操作导致对数据包的“阻止”或“待处理”文件策略判定，然后在同一数据包上生成 IPS 事件。在这种情况下，即使 IPS 策略处于检测模式 (IDS)，IPS 事件也会被标记为已丢弃，而不是将已丢弃。

注释 要阻止恶意软件通过 FTP 传输，不仅要正确配置恶意软件防护，还必须在访问控制策略的默认入侵策略中启用**内联时丢弃**。

当您查看入侵事件时，工作流可以包括内联结果，以指示流量是否确实已丢弃，或者它是否仅仅应该已丢弃。

设置内联部署中的丢弃行为

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 设置策略的丢弃行为：

- 选中**内联时丢弃 (Drop when Inline)** 复选框，以允许入侵规则影响流量并生成事件。
- 清除**内联时丢弃 (Drop when Inline)** 复选框，以防止入侵规则在生成事件时影响流量。

步骤 4 点击**确认更改 (Commit Changes)** 以保存自上次策略确认后在此策略中做出的更改。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

双系统部署中的丢弃行为

当网络中有两个背靠背连接的系统时，通常可以看到第一个系统丢弃多个事件，并且仍会在第二个系统上记录一次丢弃或“将已丢弃”事件。第一个系统决定到其扫描文件的最后一个数据包时丢弃数据包，而第二个系统还将开展调查并将流量标识为“将被丢弃”。

例如，一个 5 数据包 HTTP GET 请求，其第一个数据包将触发一条规则，被第一个系统阻止，并且仅丢弃最后一个数据包。第二个系统只能收到 4 个数据包，并将丢弃连接，但当第二个系统在其修剪会话的同时最后刷新部分 GET 请求时，由于内联结果，它将触发与“将已丢弃”相同的规则。

入侵策略高级设置

配置入侵策略的高级设置需要特定专业知识。入侵策略的基本策略决定了默认情况下启用哪些高级设置及各自的默认配置。

在入侵策略的导航面板中选择**高级设置 (Advanced Settings)** 时，策略将按类型列出其高级设置。在 Advanced Settings 页面中，您可以启用或禁用入侵策略中的高级设置，以及访问高级设置配置页面。高级设置必须在启用后才能配置。

当禁用高级设置时，子链接和 **Edit** 链接将不显示，但会保留您的配置。请注意，某些入侵策略配置（敏感数据规则、入侵规则的 SNMP 警报）需要启用和正确配置高级设置。

修改高级设置的配置要求了解正在进行的修改及其对网络的潜在影响。

具体威胁检测

敏感数据预处理器检测敏感信息，例如 ASCII 文本格式的信用卡号和社会保障号。

请注意，在网络分析策略中配置了用于检测特定威胁（back orifice 攻击、多种端口扫描类型以及尝试以过多流量淹没网络的基于速率的攻击）的其他预处理程序。

入侵规则阈值

全局规则阈值允许使用阈值来限制系统记录和显示的入侵事件数量，从而可以防止您的系统由于无法应付大量事件而崩溃。

外部响应

除了网络界面中的各种入侵事件视图之外，您还可以启用记录到系统日志 (syslog) 工具或者将事件数据发送到 SNMP 陷阱服务器。根据策略，可以指定入侵事件通知限制，设置发送到外部日志记录工具的入侵事件通知，以及配置对入侵事件的外部响应。

请注意，除了基于策略的这些警报配置，对于每个规则或规则组，您还可以在入侵事件上全局启用或禁用邮件警报。无论哪个入侵规则处理数据包，都会使用您的邮件警报设置。

相关主题

敏感数据检测基础知识，第 1627 页
全局规则阈值基础知识，第 1639 页

优化入侵检测和防御的性能

如果要让 Firepower 系统执行入侵检测和防御，但不需要利用发现数据，则可以通过禁用新发现来优化性能，如下所述。

开始之前

要执行此任务，您必须具有以下用户角色之一：

- 访问控制的管理员、访问管理员或网络管理员。
- 网络发现的管理员或发现管理员。

过程

步骤 1 修改或删除与部署在目标设备的访问控制策略关联的规则。与该设备关联的任何访问控制规则均没有用户、应用或 URL 条件；请参阅创建和编辑访问控制规则，第 1288 页。

步骤 2 从目标设备的网络发现策略中删除所有规则；请参阅配置网络发现规则，第 1968 页。

步骤 3 将已更改的配置部署到目标设备；请参阅部署配置更改，第 136 页。

第 62 章

使用规则调整入侵策略

以下主题介绍如何使用规则调整入侵策略：

入侵规则调整基础知识

您可以使用入侵策略中的“规则”(Rules) 页面为共享对象规则、标准文本规则和预处理器规则配置规则状态和其他设置。

将规则的状态设置为“生成事件”(Generate Events) 或“丢弃并生成事件”(Drop and Generate Events) 即可启用该规则。启用规则后，系统将对与该规则匹配的流量生成事件。禁用规则将停止该规则的处理。您还可以设置入侵策略，以便在内联部署中设置为“丢弃并生成事件”(Drop and Generate Events) 的规则在匹配流量时生成事件并丢弃该匹配流量。在被动部署中，设置为 Drop and Generate Events 的规则仅对匹配的流量生成事件。

您可以对规则进行过滤来显示规则的一个子集，这样就能选择要更改其规则状态或规则设置的确切规则集。

当入侵规则或规则参数要求禁用的预处理器时，系统会自动使用其当前设置，即使其在网络分析策略网络界面中保持禁用状态。

入侵规则类型

入侵规则是系统用于检测利用网络漏洞企图的一组指定关键字和参数。当系统分析网络流量时，它将数据包与每个规则中指定的条件相比较，并在数据包满足规则中指定的所有条件的情况下触发规则。

入侵策略包含：

- 入侵规则，可细分为共享对象规则和标准文本规则
- 预处理器规则，与数据包解码器的检测选项或与 Firepower 系统随附的预处理器相关联

下表总结了这些规则类型的属性：

表 *103:* 入侵规则类型

类型	生成器 ID (GID)	Snort ID (SID)	来源	可以复制？	可以编辑？
共享对象规则	3	低于 1000000	Talos 情报小组	是	有限
标准文本规则	1（全局域或旧式 GID）	低于 1000000	Talos	是	有限
	1000 - 2000（后代域）	1000000 或更高	由用户创建或导入	是	是
预处理器规则	特定于解码器或预处理器	低于 1000000	Talos	否	否
		1000000 或更高	由系统在选项配置期间生成	否	否

无法保存对 Talos 创建的任何规则所做的更改，但是可以将已修改的规则的副本另存为自定义规则。可以修改在规则或规则报头信息中使用的变量（例如源和目标端口及 IP 地址）。在多域部署中，Talos 所创建的规则属于全局域。后代域中的管理员可以保存随后可编辑的规则的本地副本。

对于所创建的规则，Talos 在每个默认入侵策略中分配默认规则状态。大多数预处理器规则在默认情况下已禁用，如果希望系统为预处理器规则生成事件并在内联部署中丢弃违规的数据包，则必须启用这些规则。

入侵规则的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

入侵规则的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

查看入侵策略中的入侵规则

您可以调整规则在入侵策略中的显示方式，并且可按多个条件将规则排序。也可以显示特定规则的详细信息，以便查看规则设置、规则文档和其他规则详情。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中**策略信息 (Policy Information)** 下的**规则 (Rules)**。

步骤 4 查看规则时，您可以执行以下操作：

- 过滤规则，如在入侵策略中设置规则过滤器，第 1486 页中所述。
- 通过点击要按其排序的列顶部的标题对规则进行排序。
- 查看入侵规则的详细信息，如查看入侵规则详细信息，第 1477 页中所述。
- 通过从**策略 (Policy)** 下拉列表中选择一个层来查看不同策略层中的规则。

“入侵规则”页面列

“入侵规则”(Intrusion Rules) 页面在其菜单栏和列标题中使用相同的图标。例如，“规则状态”(Rule State) 菜单使用与“规则状态”(Rule State) 列相同的**生成事件 (Generate Events)** 来列出规则。

表 *104:*“规则”*(Rules)* 页面列

标题	说明
GID	该整数表示规则的生成器 ID (GID)。
SID	该整数表示充当规则唯一标识符的 Snort ID (SID)。 对于自定义规则， SID 为 1000000 或更大值。
消息	此规则生成的事件中包含的消息，亦作为该规则的名称。
Generate Events	规则的规则状态： • **Drop and Generate Events** • **Generate Events** • 已禁用 请注意，与为生成事件而不丢弃流量设置的规则的图标相比，已禁用规则的图标只是暗一些而已。此外，您还可以通过点击规则的规则状态图标来更改规则状态。
思科建议的规则状态	思科 为规则建议的规则状态。
事件过滤	事件过滤器，包括应用于该规则的事件阈值和事件抑制。
动态状态	该规则的动态规则状态，如果发生指定的速率异常则会生效。
错误（  ）	为规则配置的警报（当前仅限 SNMP 警报）。
注释（  ）	向规则添加的注释。

也可以使用层下拉列表切换到策略中其他层的“规则”(Rules) 页面。请注意，除非向策略中添加层，否则下拉列表中列出的唯一可编辑视图是策略的 Rules 页面和最初命名为 `My Changes` 的策略层的 Rules 页面；另请注意，在这些视图其中之一进行更改与在其他视图中进行更改相同。该下拉列表中还会列出只读基本策略的 Rules 页面。

入侵规则详细信息

您可以从“规则详细信息”视图查看规则文档、 Cisco 建议和规则开销。还可以查看和添加特定于规则的功能。

表 *105:* 规则详细信息

项目	说明
摘要	规则摘要。对基于规则的事件，此行将在规则文档包含摘要信息时显示。
规则状态 (Rule State)	规则的当前规则状态。也表示已设置规则状态的层。
思科 建议	如果已生成Cisco建议，则图标表示建议的规则状态；请参阅“入侵规则”页面列，第 1476 页 。如果建议是启用规则，系统还会指出触发该建议的网络资产或配置。
规则开销	规则对系统性能的潜在影响以及规则产生误报的可能性。本地规则没有分配的开销，除非被映射到漏洞。
阈值	当前为此规则设置的阈值，以及用于为该规则添加阈值的工具。
抑制 (Suppressions)	当前为此规则设置的抑制设置，以及用于为该规则添加抑制的工具。
动态状态 (Dynamic State)	当前为此规则设置的基于速率的规则状态，以及用于为该规则添加动态规则状态的工具。
风险通告	为此规则设置的 SNMP 警报，以及用于为此规则添加警报的工具。
备注	向此规则添加的注释，以及用于为该规则添加注释的工具。
文档	当前规则的规则文档，由Talos 情报小组 提供。或者，点击**规则文档**来查看更具体的规则详细信息。

查看入侵规则详细信息

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 在导航窗格中，点击**规则 (Rules)**。

步骤 4 点击要查看其规则详细信息的规则，然后点击页面底部的**显示详细信息 (Show details)**。
屏幕上将显示规则详细信息，如入侵规则详细信息，第 1476 页中所述。

步骤 5 从规则详细信息中，您可以配置：

- 警报 - 请参阅为入侵规则设置 SNMP 警报，第 1480 页。
- 注释 - 请参阅将注释添加到入侵规则，第 1480 页。
- 动态规则状态 - 请参阅从规则详细信息页面设置动态规则状态，第 1479 页。
- 阈值 - 请参阅为入侵规则设置阈值，第 1478 页。

- 抑制 - 请参阅为入侵规则设置抑制，第 1478 页。

为入侵规则设置阈值

您可以在“规则详细信息”(Rule Detail) 页面中为规则设置一个阈值。添加阈值将覆盖该规则的任何现有阈值。

请注意，当输入无效值时，在字段中会显示**恢复**；点击该图标可恢复为该字段的上一个有效值，如果没有先前值，则会清除该字段。

过程

步骤 1 从入侵规则的详细信息中，点击**阈值 (Thresholds)** 旁边的**添加 (Add)**。

步骤 2 从**类型 (Type)** 下拉列表中，选择要设置的阈值的类型：

- 选择**限制 (Limit)** 以将通知限于每个时间段的指定数量的事件实例。
- 选择**阈值 (Threshold)** 以在每个时间段内每次事件实例数达到指定数量时提供通知
- 选择**两者 (Both)** 以在每个时间段内事件实例数达到指定数量后提供一次通知。

步骤 3 从**跟踪方式 (Track By)** 下拉列表中，选择**源 (Source)** 或**目标 (Destination)** 以指示希望按源 IP 地址还是目标 IP 地址跟踪事件实例。

步骤 4 在**计数 (Count)** 字段中，输入要用作阈值的事件实例数。

步骤 5 在**秒 (Seconds)** 字段中，输入用于指定跟踪事件实例的时间段的数字（以秒为单位）。

步骤 6 点击 **OK**。

提示 系统在“事件过滤”列中的规则旁边显示**事件过滤器**。如果向规则中添加多个事件过滤器，系统将注明事件过滤器的数量。

为入侵规则设置抑制

可以为入侵策略中的规则设置一个或多个抑制。

请注意，当键入的值无效时，字段中会显示**恢复 (Revert)**；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清除该字段。

过程

步骤 1 从入侵规则的详细信息中，点击**抑制 (Suppressions)** 旁边的**添加 (Add)**。

步骤 2 从**抑制类型 (Suppression Type)** 下拉列表中，选择下列选项之一：

- 选择**规则 (Rule)** 将完全抑制所选规则的事件。
- 选择**源 (Source)** 将抑制由指定源 IP 地址发出的数据包生成的事件。

- 选择**目标 (Destination)** 将抑制由发往指定目标 IP 地址的数据包生成的事件。

步骤 3 如果为抑制类型选择**源 (Source)** 或**目标 (Destination)**，则在**网络 (Network)** 字段中输入 IP 地址、地址块或由这些值的任意组合组成并以逗号分隔的列表。

如果入侵策略与某个访问控制策略的默认操作相关联，则还可以在默认操作变量集中指定或列出网络变量。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 4 点击 **OK**。

提示 系统将在被抑制规则旁边的“事件过滤”(Event Filtering) 列中的规则旁边显示**事件过滤器 (Event Filter)**。如果向规则中添加多个事件过滤器，过滤器上的数字表示过滤器的数量。

从规则详细信息页面设置动态规则状态

您可以为规则设置一个或多个动态规则状态。列出的第一个动态规则状态具有最高优先级。当两个动态规则状态相冲突时，将执行第一个状态的操作。

动态规则状态为策略特定的。

请注意，当输入无效值时，在字段中会显示**恢复**；点击该图标可恢复为该字段的上一个有效值，如果没有先前值，则会清除该字段。

过程

步骤 1 从入侵规则的详细信息中，点击**动态状态 (Dynamic State)** 旁边的**添加 (Add)**。

步骤 2 从**跟踪方式 (Track By)** 下拉列表中，选择用于指示要如何跟踪规则匹配项的选项：

- 选择**源 (Source)** 将跟踪由特定的一个或一组源地址发出的该规则匹配项的数量。
- 选择**目标 (Destination)** 将跟踪发往特定的一个或一组目标地址的该规则匹配项的数量。
- 选择**规则 (Rule)** 将跟踪该规则的所有匹配项。

步骤 3 如果将**跟踪方式 (Track By)** 设置为**源 (Source)** 或**目标 (Destination)**，请在**网络 (Network)** 字段中输入要跟踪的每台主机的 IP 地址。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 4 在**速率 (Rate)** 旁边，指定每个时间段的规则匹配项数，以设置攻击速率：

- 在**计数 (Count)** 字段中，指定要用作阈值的规则匹配数。
- 在**秒数 (Seconds)** 字段中，指定跟踪攻击的时间段的秒数。

步骤 5 从**新状态 (New State)** 状态下拉列表中，选择满足条件时要采取的新操作。

步骤 6 在**超时 (Timeout)** 字段中输入值。

在超时后，规则将恢复到其原始状态。输入 0 可防止新操作超时。

步骤 7 点击 **OK**。

提示 系统将在“动态状态”()列中的规则旁边显示动态状态。如果向规则中添加多个动态规则状态过滤器，过滤器上的数字表示过滤器的数量。

为入侵规则设置 SNMP 警报

您可以从 Rule Detail 页面为规则设置 SNMP 警报。

过程

从入侵规则的详细信息中，点击**警报 (Alerts)** 旁边的**添加 SNMP 警报 (Add SNMP Alert)**。

提示 系统将在“警报”列中的规则旁边显示警报**错误**（  ）。如果向规则中添加多个警报，则系统将指示警报的数量。

将注释添加到入侵规则

过程

步骤 1 从入侵规则的详细信息中，点击**注释 (Comments)** 旁边的**添加 (Add)**。

步骤 2 在**注释 (Comment)** 字段中，输入规则注释。

步骤 3 点击 **OK**。

提示 系统将并在“注释”(Comments) 列中的规则旁显示**注释**（  ）。如果向规则中添加多个注释，注释上的数字表示注释的数量。

步骤 4 要删除规则注释，请点击规则注释部分的**删除 (Delete)**。仅当缓存的注释具有未提交的入侵策略更改时，才能删除该注释。

下一步做什么

- 部署配置更改。

入侵策略中的入侵规则过滤器

可以按单一条件或按一个或多个条件的组合来过滤 Rules 页面中显示的规则。

规则过滤器关键字可帮助您找到要对其应用规则状态或事件过滤器等规则设置的规则。您可以按关键字进行过滤，同时从“规则”(Rules) 页面的过滤器面板选择所需参数作为关键字的参数。

入侵规则过滤器说明

您所构造的过滤器显示于“过滤器”(Filter) 文本框中。点击过滤器面板中的关键字和关键字参数可以构造过滤器。当选择多个关键字时，系统会使用 AND 逻辑将其组合以创建复合搜索过滤器。例如，如果选择**类别 (Category)** 下的**预处理器 (preprocessor)**，然后选择**规则内容 (Rule Content)** > **GID** 并输入 `116`，则会获得过滤器 `Category: “preprocessor” GID:”116”`，用于检索属于预处理器规则**并且** GID 为 116 的所有规则。

通过 Category、Microsoft Vulnerabilities、Microsoft Worms、Platform Specific、Preprocessor 和 Priority 过滤器组，可以为一个关键字提交多个参数（以逗号分隔）。例如，可以从**类别 (Category)** 中选择 **os-linux** 和 **os-windows** 以生成过滤器 `Category:"os-windows,os-linux"`，用于检索 `os-linux` 类别或 `os-windows` 类别中的任意规则。

要显示过滤器面板，请点击**显示图标**。

要隐藏过滤器面板，请点击**隐藏图标**。

入侵策略规则过滤器构建准则

在大多数情况下，当构建过滤器时，可以使用入侵策略中“规则”(Rules) 页面左侧的过滤器面板选择要使用的关键字/参数。

规则过滤器在过滤器面板中分为不同的规则过滤器组。许多规则过滤器组包含子条件，因此可以更轻松地找到所需的特定规则。有些规则过滤器有多个级别，可展开以向下钻取到各个规则。

过滤器面板中的项有时表示过滤器类型组，有时表示关键字，还有时表示关键字的参数。请注意以下提示：

- 当选择不是关键字的过滤器类型组标题（“规则配置”[Rule Configuration]、“规则内容”[Rule Content]、“平台特定”[Platform Specific] 和“优先级”[Priority]）时，该标题会展开以列出可用关键字。

  通过点击条件列表中的节点来选择关键字时，将显示一个弹出窗口，其中提供要作为过滤条件的参数。

  如果过滤器中已在使用该关键字，则提供的参数将替换该关键字的现有参数。

  例如，如果点击过滤器面板中**规则配置 (Rule Configuration)** > **建议 (Recommendation)** 下的**丢弃并生成事件 (Drop and Generate Events)**，则会将 `Recommendation:"Drop and Generate Events"` 添加到过滤器文本框中。如果随后点击**规则配置** > **建议** 下的**生成事件**，则过滤器会更改为`建议: “生成事件”`。

- 当选择属于关键字的过滤器类型组标题（“类别”[Category]、“分类”[Classifications]、“Microsoft 漏洞”[Microsoft Vulnerabilities]、“Microsoft 蠕虫”[Microsoft Worms]、“优先级”[Priority] 和“规则更新”[Rule Update]）时，该标题会列出可用参数。

  从此类型的组中选择项目时，该参数及其应用到的关键字会立即添加到过滤器中。如果该关键字已经在过滤器中，它将替换与该组对应的关键字的现有参数。

  例如，如果点击过滤器面板中**类别**下的 **os-linux**，则会将 类别：“os-linux”添加到过滤器文本框中。如果随后点击 **Category** 下的 **os-windows**，过滤器将更改为 `Category:"os-windows"`。

- Rule Content 下的 Reference 是关键字，其下方列出的特定引用 ID 类型同样如此。选择任何引用关键字时，会显示一个弹出窗口，其中提供添加到现有过滤器的参数和关键字。如果过滤器中已在使用该关键字，则提供的新参数将替换现有参数。

  例如，如果依次点击过滤器面板中的**规则内容 (Rule Content)** > **引用 (Reference)** > **CVE ID**，系统将显示弹出窗口，提示您提供 CVE ID。如果输入 `2007`，则会将 `CVE:”2007”` 添加到过滤器文本框中。又例如，如果依次点击过滤器面板中的**规则内容 (Rule Content)** > **引用 (Reference)**，系统将显示弹出窗口，提示您提供该引用。如果输入 `2007`，则会将 `Reference:”2007”` 添加到过滤器文本框中。

- 从不同的组中选择规则过滤器关键字时，会将每个过滤器关键字都添加到过滤器中并保留所有现有关键字（除非被同一关键字的新值覆盖）。

  例如，如果点击过滤器面板中**类别**下的 **os-linux**，则会将 类别：“os-linux”添加到过滤器文本框中。如果随后点击 **Microsoft Vulnerabilities** 下的 **MS00-006**，过滤器将更改为 `Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"`。

- 当选择多个关键字时，系统会使用 AND 逻辑将其组合以创建复合搜索过滤器。例如，如果选择**类别 (Category)** 下的**预处理器 (preprocessor)**，然后选择**规则内容 (Rule Content)** > **GID** 并输入 `116`，则会获得过滤器 `Category: “preprocessor” GID:”116”`，用于检索属于预处理器规则**并且** GID 为 116 的所有规则。

- Category、Microsoft Vulnerabilities、Microsoft Worms、Platform Specific 和 Priority 过滤器组可以为一个关键字提交多个参数（以逗号分隔）。例如，可以从**类别 (Category)** 中选择 **os-linux** 和 **os-windows** 以生成过滤器 `Category:"os-windows,app-detect"`，用于检索 `os-linux` 类别或 `os-windows` 类别中的任意规则。

同一规则可以按多个过滤器关键字/参数对进行检索。例如，如果按类别 **dos** 来过滤规则，系统将显示 DOS 思科尝试规则 (SID 1545)，按优先级 **High** 进行过滤亦如此。

注释 Talos 情报小组 可能会使用规则更新机制添加和删除规则过滤器。

请注意，“规则”页面上的规则可以是共享对象规则（生成器 ID 3）或标准文本规则（生成器 ID 1，全局域或旧式 GID；1000-2000，子代域）。下表介绍不同的规则过滤器。

表 *106:* 规则过滤器组

过滤器组	说明	是否支持多个参数？	标题为.....	列表中的项目为.....
规则配置 (Rule Configuration)	根据规则的配置查找规则。	否	一组	关键词
规则内容 (Rule Content)	根据规则的内容查找规则。	否	一组	关键词
类别 (Category)	根据规则编辑器使用的规则类别来查找规则。请注意，本地规则显示于本地子组中。	是	一个关键字	参数
分类 (Classifications)	根据规则生成的事件的数据包显示中所显示的攻击分类来查找规则。	否	一个关键字	参数
Microsoft 漏洞 (Microsoft Vulnerabilities)	根据 Microsoft 公告号查找规则。	是	一个关键字	参数
Microsoft 蠕虫 (Microsoft Worms)	根据影响 Microsoft Windows 主机的特定蠕虫查找规则。	是	一个关键字	参数
平台特定 (Platform Specific)	根据规则与特定操作系统版本的关联性来查找规则。 请注意，规则可能会影响多个操作系统或某个操作系统的多个版本。例如，启用 SID 2260 会影响多个版本的 Mac OS X、IBM AIX 以及其他操作系统。	是	一个关键字	参数 请注意，如果从子列表中选择其中一项，则会向参数添加修饰符。
预处理程序	查找各个预处理器的规则。 请注意，在启用预处理器时，必须启用与预处理器选项相关联的预处理器规则才能生成事件并在内联部署中丢弃攻击性数据包该选项的事件。	是	一组	子组
优先级	根据高、中和低优先级查找规则。 分配给规则的分类将确定该规则的优先级。这些组进一步分为不同的规则类别。请注意，本地规则（即您导入或创建的规则）不会显示在优先级组中。	是	一个关键字	参数 请注意，如果从子列表中选择其中一项，则会向参数添加修饰符。
规则更新 (Rule Update)	查找通过特定规则更新添加或修改的规则。对于每个规则更新，可以查看更新中的所有规则、仅查看更新中导入的新规则或仅查看更新所更改的现有规则。	否	一个关键字	参数

入侵规则配置过滤器

您可以按多个规则配置设置来过滤“规则”(Rules) 页面中列出的规则。例如，如果要查看规则状态与建议的规则状态不匹配的一组规则，可以选择**不匹配建议 (Does not match recommendation)** 来根据规则状态进行过滤。

通过点击条件列表中的节点来选择关键字时，可以提供要作为过滤条件的参数。如果过滤器中已在使用该关键字，则提供的参数将替换该关键字的现有参数。

例如，如果点击过滤器面板中**规则配置 (Rule Configuration)** > **建议 (Recommendation)** 下的**丢弃并生成事件 (Drop and Generate Events)**，则会将 `Recommendation:"Drop and Generate Events"` 添加到过滤器文本框中。如果随后点击**规则配置 (Rule Configuration)** > **建议 (Recommendation)** 下的**生成事件 (Generate Events)**，则过滤器会更改为 `Recommendation:"Generate Events"`。

入侵规则内容过滤器

您可以按多个规则内容项来过滤 Rules 页面中列出的规则。例如，通过搜索规则的 SID 可以快速检索该规则。也可以查找用于检测发往特定目标端口的流量的所有规则。

通过点击条件列表中的节点来选择关键字时，可以提供要作为过滤条件的参数。如果过滤器中已在使用该关键字，则提供的参数将替换该关键字的现有参数。

例如，如果点击过滤器面板中**规则内容**下的 **SID**，系统将显示弹出窗口，提示您提供 SID。如果键入 `1045`，则 `SID:”1045”` 会被添加到过滤器文本框中。如果随即再次点击 **SID** 并将 SID 过滤器更改为 `1044`，过滤器将更改为 `SID:”1044”`。

表 *107:* 规则内容过滤器

以下过滤器	查找符合以下条件的规则
消息	在消息字段中包含所提供的字符串。
SID	具有指定的 SID。
GID	具有指定的 GID。
参考	在引用字段中包含所提供的字符串。您也可以按特定类型的引用和所提供字符串进行过滤。
操作	首先执行 `alert` 或 `pass`。
协议	包含所选协议。
方向	基于规则是否包含指示的方向设置。
源 IP	使用指定的地址或变量作为规则中的源 IP 地址指定。可以按有效 IP 地址、CIDR 块/前缀长度或者使用 `$HOME_NET` 或 `$EXTERNAL_NET` 等变量进行过滤。
目标 IP	使用指定的地址或变量作为规则中的源 IP 地址指定。可以按有效 IP 地址、CIDR 块/前缀长度或者使用 `$HOME_NET` 或 `$EXTERNAL_NET` 等变量进行过滤。

以下过滤器	查找符合以下条件的规则
源端口	包括指定的源端口。端口值必须为 1 到 65535 之间的整数或端口变量。
目的端口	包括指定的目标端口。端口值必须为 1 到 65535 之间的整数或端口变量。
规则开销	具有所选规则开销。
元数据	具有包含匹配的键值对的元数据。例如，键入 `metadata:"service http"` 可查找元数据与 HTTP 应用协议相关的规则。

入侵规则类别

Firepower 系统根据规则检测的流量类型对规则分类。在 Rules 页面中，可以按规则类别过滤，从而可为某个类别中的所有规则设置规则属性。例如，如果网络中没有 Linux 主机，则可以按 **os-linux** 类别过滤，然后禁用表明将禁用整个 **os-linux** 类别的所有规则。

可以将鼠标指针悬停在类别名称上方来显示该类别中的规则数。

注释 Talos 情报小组 可能会使用规则更新机制来添加和删除规则类别。

入侵规则过滤器组件

通过编辑过滤器可以修改您在过滤器面板中点击过滤器时所提供的特定关键字及其参数。“规则”(Rules) 页面中的自定义过滤器的功能与规则编辑器中使用的过滤器类似，但除此之外，您还可以使用在“规则”(Rules) 页面过滤器中提供的任何关键字，使用在过滤器面板中选择过滤器时显示的语法。要确定供今后使用的关键字，请点击右侧过滤器面板中的相应参数。过滤器关键字和参数语法显示在过滤器文本框中。请记住，仅对“类别”和“优先级”过滤器类型支持关键字的多个以逗号分隔的参数。

您可以使用关键字和参数、字符串及带引号的原义字符串，以空格分隔多个过滤条件。过滤器不能包含正则表达式、通配符或任何特殊运算符，例如取反字符 (!)、大于号 (>) 和小于号 (<) 等。当键入的搜索条件没有关键字、关键字的首字母没有大写或者没有用引号将参数引起来时，该搜索将被视为字符串搜索，并搜索类别、消息和 SID 字段中有无指定条件。

除关键字 `gid` 和 `sid` 之外，所有参数和字符串都被视为部分字符串。`gid` 和 `sid` 的参数只会返回完全匹配项。

每个规则过滤器都可以包含一个或多个关键字，其格式如下：

keyword:"*argument*"

其中，keyword 是入侵规则过滤器组中的关键字之一，argument 是要在与该关键字相关的一个或多个特定字段中搜索的字母数字字符串，用双引号引起来且不区分大小写。请注意，键入的关键字应该首字母大写。

除 gid 和 sid 之外，所有关键字的参数都会被视为部分字符串。例如，参数 123 将返回 "12345"、"41235"、"45123" 等。gid 和 sid 的参数只会返回完全匹配项；例如，sid:3080 只会返回结果 SID 3080。

每个规则过滤器还可以包含一个或多个字母数字字符串。字符串将搜索规则的“消息”字段、Snort ID (SID) 和生成器 ID (GID)。例如，字符串 123 会返回规则消息中的 "Lotus123"、"123mania" 等字符串，也会返回 SID 6123、SID 12375 等。使用一个或多个字符串来进行过滤可以搜索部分 SID。

所有字符串都不区分大小写并被视为部分字符串。例如，字符串 ADMIN、admin 或 Admin 中的任意一个都会返回 "admin"、"CFADMIN"、"Administrator" 等等。

用引号将字符串引起来可以返回完全匹配项。例如，用引号引起来的原义字符串 "overflow attempt" 只会返回完全匹配的该字符串，而由 overflow 和 attempt 这两个字符串组成的未加引号的过滤器则会返回 "overflow attempt"、"overflow multipacket attempt"、"overflow with evasion attempt" 等结果。

输入关键字、字符串或这二者的任意组合并以空格分隔可以缩小过滤结果的范围。结果包括符合所有过滤条件的任意规则。

可以按照任意顺序输入多个过滤条件。例如，以下每个过滤器返回的规则相同：

- url:at login attempt cve:200
- login attempt cve:200 url:at
- login cve:200 attempt url:at

入侵规则过滤器的使用

可以从入侵策略中“规则”(Rules) 页面左侧的过滤器面板中选择预定义的过滤器关键字。选择过滤器时，该页面会显示所有匹配的规则，或者指出没有匹配的规则。

您可以对过滤器添加关键字来进一步对其进行限制。输入的任何过滤器都会搜索整个规则数据库并返回所有匹配的规则。当您在页面仍显示上一过滤器的结果时输入过滤器，页面将清空，转而返回新过滤器的结果。

您也可以使用在选择过滤器时提供的相同关键字和参数语法来键入过滤器，或者在选择过滤器后修改其中的参数值。当键入的搜索条件没有关键字、关键字的首字母没有大写或者没有用引号将参数引起来时，该搜索将被视为字符串搜索，并搜索类别、消息和 SID 字段中有无指定条件。

在入侵策略中设置规则过滤器

您可以对 Rules 页面中的规则进行过滤来显示其中一组规则。然后，可以使用任何页面功能，包括选择情景菜单中可用的任何功能。例如，当您需要为某个特定类别中的所有规则设置阈值时，此功能会非常有用。您可以对已过滤或未过滤列表中的规则使用相同的功能。例如，您可以将新的规则状态应用到已过滤或未过滤列表中的规则。

所有过滤器关键字、关键字参数和字符串都不区分大小写。如果点击过滤器中已存在的关键字的参数，则该参数将替换现有的参数。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 使用以下任一方法单独或以组合形式构建过滤器：

- 在**过滤器 (Filter)** 文本框中输入值，然后按 Enter 键。
- 展开任何预定义的关键字。例如，点击**规则配置 (Rule Configuration)**。
- 点击一个关键字，并指定参数值（如果提示）。例如：
  - 在**规则配置 (Rule Configuration)** 下，可以点击**规则状态 (Rule State)**，从下拉列表中选择生成事件 (Generate Events)，然后点击**确定 (OK)**。
  - 在**规则配置 (Rule Configuration)** 下，可以点击**注释 (Comment)**，输入要筛选的注释文本字符串过滤，然后点击**确定 (OK)**。
  - 在**类别 (Category)** 下，可以点击**应用检测 (app-detect)**，系统将其用作参数值。
- 展开关键字，然后点击一个参数值。例如，展开**规则状态 (Rule State)**，然后点击**生成事件 (Generate Events)**。

入侵规则状态

通过入侵规则状态，您可在个别入侵策略中启用或禁用规则，以及指定受监控条件触发该规则时系统采取的操作。

Talos 情报小组 为每个默认策略中的每条入侵规则和预处理器规则设置默认状态。例如，一条规则可能会在 Security over Connectivity 默认策略中启用而在 Connectivity over Security 默认策略中禁用。Talos 有时会使用规则更新来更改默认策略中一条或多条规则的默认状态。如果允许规则更新对基本策略进行更新，则意味着当用于创建策略的默认策略中的默认状态发生更改时，也允许规则更新更改策略中的规则默认状态。但请注意，如果您已经更改了规则状态，规则更新不会覆盖您的更改。

创建入侵规则时，它会继承用于创建策略的默认策略中相应规则的默认状态。

入侵规则状态选项

在入侵策略中，可以将规则的状态设置为以下值：

Generate Events

您希望系统检测特定入侵企图，并在其发现匹配流量时生成入侵事件。当恶意数据包通过网络并触发该规则时，数据包被发送到其目标，系统生成入侵事件。该恶意数据包到达其目标，但是您通过事件日志记录收到通知。

Drop and Generate Events

您希望系统检测特定入侵企图，丢弃包含攻击的数据包，并在其发现匹配流量时生成入侵事件。该恶意数据包永远不会到达其目标，并且您通过事件日志记录收到通知。

请注意，设置为此规则状态的规则在被动部署中生成事件但不丢弃数据包。为使系统丢弃数据包，还必须在入侵策略中启用**内联时丢弃 (Drop when Inline)** 并部署设备内联，并且您必须内联部署设备。

禁用 (Disable)

您不希望系统评估匹配流量。

注释 选择**生成事件 (Generate Events)** 或**丢弃并生成事件 (Drop and Generate Events)** 选项可启用规则。选择**禁用 (Disable)** 会禁用规则。

思科**强烈**建议**不要**启用入侵策略中的所有入侵规则。如果启用所有规则，则您的受管设备的性能可能会下降。相反，应调整规则集，使之与网络环境尽可能匹配。

设置入侵规则状态

入侵规则状态为策略特定的。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

提示 此页面指示已启用规则的总数、设置为“生成事件”的已启用规则的总数，以及设置为“丢弃并生成事件”的总数。另请注意，在被动部署中，设置为 Drop and Generate Events 的规则仅生成事件。

步骤 3 点击导航面板中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择要在其中设置规则状态的一条或多条规则。

步骤 5 选择以下其中一个选项：

- **规则状态** > **生成事件**
- **规则状态** > **丢弃并生成事件**
- **规则状态** > **禁用**

步骤 6 要保存自上次策略提交以来在此策略中进行的更改，请点击导航面板中的**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

入侵策略中的入侵事件通知过滤器

入侵事件的重要性可根据发生频率或者源或目标IP地址而定。在某些情况下，直至事件发生一定次数后您可能才会在意。例如，如果有人企图登录服务器，在其失败达到一定次数之前，您可能不会担心。但在其他情况下，也许只需要发生几次，就能让您知道存在普遍性问题。例如，如果有人对网络服务器发动DoS攻击，可能只需要发生区区数次入侵事件，您就会明白需要解决这种情况。发生数百次相同事件只会让系统不堪重负。

入侵事件阈值

您可以逐个入侵策略为各条规则设置阈值，根据事件在指定时间段内生成的次数来限制系统记录和显示入侵事件的次数。这可以防止因相同事件数量过多而使系统不堪重负。您可以根据共享对象规则、标准文本规则或预处理器规则设置阈值。

入侵事件阈值配置

要设置阈值，请先指定阈值类型。

表 *108:* 阈值选项

选项	说明
限制	为指定时间段内触发规则的指定数量的数据包（由“计数”[Count]参数指定）记录并显示事件。例如，如果将类型设置为**限制 (Limit)**，将**计数 (Count)** 设置为 `10`，并将**秒数 (Seconds)** 设置为 `60`，而同一分钟内有14个数据包触发规则，则系统在显示发生的前10个违反该规则的事件后将停止记录违反该规则的事件。
阈值 (Threshold)	在指定时间段内，当指定数量的数据包（由“计数”[Count]参数指定）触发规则时，记录并显示一个事件。请注意，达到事件阈值计数且系统记录该事件之后，时间计数器将重新开始计数。例如，将类型设置为**阈值 (Threshold)**，将**计数 (Count)** 设置为 `10`，并将**秒数 (Seconds)** 设置为 `60` 时，如果到33秒时规则触发10次，系统将生成一个事件，然后将“秒数”(Seconds) 和“计数”(Count) 计数器重置为0。其后，该规则在接下来25秒内又触发10次。由于计数器在第33秒时已重置为0，因此，系统此时会记录另一个事件。

选项	说明
双向	每个指定时间段在指定数量（计数）的数据包触发规则后记录并显示一次事件。例如，如果将类型设置为**两者 (Both)**，将**计数 (Count)** 设置为 2，并将**秒数 (Seconds)** 设置为 `10`，则事件计数结果如下： • 如果 10 秒内触发规则一次，系统不会生成任何事件（未达到阈值） • 如果 10 秒内触发规则两次，系统将生成一个事件（第二次触发规则时达到阈值） • 如果 10 秒内触发规则四次，系统将生成一个事件（第二次触发规则时达到阈值，忽略其后的事件）

接下来，指定跟踪，从而确定事件阈值是按源 IP 地址计算还是按目标 IP 地址计算。

表 *109:* 阈值 *IP* 选项

选项	说明
来源	按源 IP 地址计算事件实例计数。
目标	按目标 IP 地址计算事件实例计数。

最后，指定用于定义阈值的实例数和时间段。

表 *110:* 阈值实例/时间选项

选项	说明
计数	每个跟踪 IP 地址在每个指定时间段内达到阈值所需的事件实例数量。
秒	计数重置之前经过的秒数。如果将阈值类型设置为**限制 (limit)**，将跟踪设置为**源 IP (Source IP)**，将**计数 (count)** 设置为 `10`，并将**秒数 (seconds)** 设置为 `10`，则系统将记录并显示 10 秒钟内发生的来自指定源端口的前 10 个事件。如果前 10 秒内只发生了 7 个事件，系统将记录并显示这些事件，而如果前 10 秒内发生了 40 个事件，系统将记录并显示 10 个事件，然后在为期 10 秒的时间段过后重新开始计数。

请注意，入侵事件阈值可单独使用，也可与基于速率的攻击防御、`detection_filter` 关键字和入侵事件抑制的任意组合配合使用。

提示 也可以在入侵事件的数据包视图中添加阈值。

相关主题

detection_filter 关键字 ，第 1592 页

添加和修改入侵事件阈值

可以为入侵策略中的一条或多条特定规则设置阈值。也可以单独或同时修改现有阈值设置。可以为每条规则设置一个阈值。添加阈值将覆盖该规则的任何现有阈值。

还可以修改默认应用到与入侵策略关联的所有规则和预处理器生成的事件的全局阈值。

当输入无效值时，字段中会显示**恢复 (Revert)**；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清除该字段。

提示 在有多个 CPU 的受管设备上，全局阈值或单独的阈值可能会导致事件数量高于预期。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航窗格中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择要在其中设置阈值的一条或多条规则。

步骤 5 选择**事件过滤 (Event Filtering)** > **阈值 (Threshold)**。

步骤 6 从**类型 (Type)** 下拉列表中选择阈值类型。

步骤 7 从**跟踪方式 (Track By)** 下拉列表中，选择要按**源 (Source)** 还是**目标 (Destination)** IP 地址跟踪事件实例。

步骤 8 在**计数 (Count)** 字段中输入值。

步骤 9 在**秒数 (Seconds)** 字段中输入值。

步骤 10 点击 **OK**。

提示 系统在“事件过滤”(Event Filtering) 列中的规则旁边显示**事件过滤器 (Event Filter)** 。如果向规则中添加多个事件过滤器，过滤器上的数字表示事件过滤器的数量。

步骤 11 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

相关主题

全局规则阈值基础知识，第 1639 页

查看和删除入侵事件阈值

您可能需要查看或删除一个规则的现有阈值设置。可以使用“规则详细信息”(Rules Details) 视图显示为阈值配置的设置，看其是否适合系统。如果不适合，可以添加新的阈值来覆盖现有值。

请注意，还可以修改全局阈值，它默认应用到入侵策略所记录的所有规则和预处理器生成的事件。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航窗格中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择配置了要查看或删除的阈值的一条或多条规则。

步骤 5 要删除每条所选规则的阈值，请依次选择**事件过滤器 (Event Filtering)** > **删除阀值 (Remove Thresholds)**。

步骤 6 点击 **OK**。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

相关主题

全局规则阈值基础知识，第 1639 页

入侵策略抑制配置

您可以在特定 IP 地址或 IP 地址范围触发特定规则或预处理器时抑制入侵事件通知。这对杜绝误报十分有用。例如，如果邮件服务器传输的数据包看起来像某种特定的漏洞，则可能会在邮件服务器触发该事件时抑制对其发出的事件通知。所有数据包都会触发该规则，但您只会看到真正的攻击事件。

入侵策略抑制类型

请注意，入侵事件抑制可单独使用，也可与基于速率的攻击防御、`detection_filter` 关键字和入侵事件阈值的任意组合配合使用。

提示 可以在入侵事件的数据包视图中添加抑制。在入侵规则编辑器页面（**对象** > **入侵规则**）和任何入侵事件页面（如果该事件由入侵规则触发）上，也可以使用右键点击情景菜单访问抑制设置。

相关主题

detection_filter 关键字 ，第 1592 页

抑制特定规则的入侵事件

您可以在入侵策略中抑制一个或多个规则的入侵事件通知。当某条规则的通知被抑制时，规则会触发，但不会生成事件。可以为一个规则设置一个或多个抑制。列出的第一个抑制的优先级最高。当两个抑制发生冲突时，将执行第一个抑制的操作。

请注意，当输入无效值时，在字段中会显示**恢复 (Revert)**；点击该图标可恢复为该字段的上一个有效值，如果没有先前值，则会清除该字段。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择要为其配置抑制条件的一个或多个规则。

步骤 5 依次选择**事件过滤 (Event Filtering)** > **抑制 (Suppression)**。

步骤 6 选择**抑制类型 (Suppression Type)**。

步骤 7 如果为抑制类型选择了**源 (Source)** 或**目标 (Destination)**，请在**网络 (Network)** 字段中输入要指定为源或目标 IP 地址的 IP 地址、地址块或变量，或者输入由这些值的任意组合组成的逗号分隔列表。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 8 点击 **OK**。

提示 系统将在被抑制规则旁边的“事件过滤”(Event Filtering) 列中的规则旁边显示**事件过滤器 (Event Filter)**。如果向规则中添加多个事件过滤器，过滤器上的数字表示事件过滤器的数量。

步骤 9 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

查看和删除抑制条件

您可能需要查看或删除现有抑制条件。例如，由于某个邮件服务器通常会传输看起来像漏洞的数据包，因此可以抑制由该邮件服务器IP地址发出的数据包的事件通知。如果以后停用该邮件服务器并将此 IP 地址重新分配给其他主机，应删除对该源 IP 地址的抑制条件。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择要查看或删除其抑制的一个或多个规则。

步骤 5 有以下选项可供选择：

- 要删除规则的所有抑制，请依次选择**事件过滤 (Event Filtering)** > **删除抑制 (Remove Suppressions)**。
- 要删除特定抑制设置，请点击规则，然后点击**显示详细信息 (Show details)**。展开抑制设置，然后点击要删除的抑制设置旁边的 **Delete**。

步骤 6 点击 **OK**。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

动态入侵规则状态

基于速率的攻击通过向网络或主机发送过多的流量，企图让网络或主机不堪重负，导致其速度下降或拒绝合法请求。为了应对特定规则出现过多规则匹配项的情况，可以使用基于速率的防御来更改规则的操作。

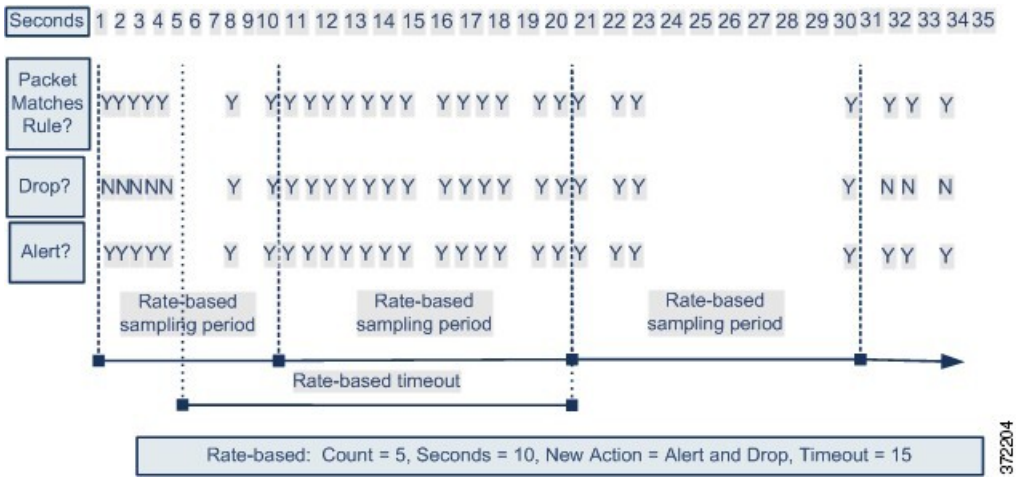
您可以配置入侵策略，使其包含基于速率的过滤器，从而检测指定时间段内出现某条规则匹配项过多的情况。此功能可以用于内联部署的受管设备上，先在指定时间内拦截基于速率的攻击，然后恢复为规则匹配项仅生成事件而不丢弃流量的规则状态。

基于速率的攻击防御可确定异常流量模式，并可将这些流量对合法请求的影响降至最低。您可以识别出发往一个或多个特定目标 IP 地址或者由一个或多个特定源 IP 地址发出的流量中存在的过多规则匹配项。也可以对检测的所有流量中符合特定规则的过多匹配项作出响应。

在某些情况下，您可能不希望将某规则设置为“丢弃并生成事件”(Drop and Generate Events) 状态，因为您不想丢弃与该规则匹配的每个数据包，但同时您又确实希望在指定事件内出现特定频率的匹配项时丢弃与该规则匹配的数据包。动态规则状态可用于配置应该触发规则操作更改的速率、达到该速率时应该改而执行的操作以及新操作应该持续的时间。

下图显示的例子中，攻击者正在尝试访问主机。反复尝试查找密码触发了配置有基于速率的攻击防御的规则。当在 10 秒的时间跨度内发生五次规则匹配之后，基于速率的设置会将规则属性更改为“丢弃并生成事件”(Drop and Generate Events)。新的规则属性在 15 秒之后超时。

请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。如果采样速率高于当前或前一个采样周期的阈值，新操作将继续。只有在采样周期完毕而采样速率低于阈值速率之后，新操作才会恢复为“生成事件”(Generate Events)。



动态入侵规则状态配置

在入侵策略中，可以为任何入侵规则或预处理器规则配置基于速率的过滤器。基于速率的过滤器包含三个组成部分：

- 规则的匹配速率，配置为特定秒数内的规则匹配项数量
- 超过速率时要执行的新操作，可用的操作有三项：“生成事件”(Generate Events)、“丢弃并生成事件”(Drop and Generate Events) 和“禁用”(Disable)。
- 操作的持续时间，配置为超时值

请注意，新操作自开始之后，在到达超时时间之前会一直执行，即使速率在这段时间内降到配置的速率以下亦不会停止。达到超时后，如果速率低于阈值，则规则的操作会恢复到为该规则最初配置的操作。

在内联部署中，可以配置基于速率的攻击防御来临时或永久拦截攻击。如果没有基于速率的配置，设置为“生成事件”(Generate Events) 的规则确实会生成事件，但系统不会丢弃这些规则的数据包。但是，如果攻击流量所匹配的规则配置了基于速率的条件，则基于速率的操作可能会导致系统在该操作处于活动状态的时间内丢弃数据包，即便这些规则最初并未设置为“丢弃并生成事件”(Drop and Generate Events)。

注释 基于速率的操作无法启用禁用的规则，也无法丢弃与禁用的规则匹配的流量。

可以对同一规则定义多个基于速率的过滤器。入侵策略中列出的第一个过滤器优先级最高。请注意，当两个基于速率的过滤器的操作相冲突时，系统将执行第一个基于速率的过滤器的操作。

从规则页面设置动态规则状态

您可以为规则设置一个或多个动态规则状态。列出的第一个动态规则状态具有最高优先级。当两个动态规则状态相冲突时，将执行第一个状态的操作。

动态规则状态为策略特定的。

当输入无效值时，字段中会显示**恢复 (Revert)**；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清除该字段。

注释 动态规则状态无法启用禁用的规则，也无法丢弃与禁用的规则匹配的流量。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航窗格中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择要在其中添加动态规则状态的一条或多条规则。

步骤 5 依次选择**动态状态 (Dynamic State)** > **添加基于速率的规则状态 (Add Rate-Based Rule State)**。

步骤 6 从**跟踪方式 (Track By)** 下拉列表中选择一个值。

步骤 7 如果将 **Track By** 设置为 **Source** 或 **Destination** 时，请在 **Network** 字段中输入要跟踪的每台主机的地址。可以指定单个 IP 地址、地址块、变量或由这些值的任意组合组成并以逗号分隔的列表。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 8 在**速率 (Rate)** 旁边，指定每个时间段的规则匹配项数，以设置攻击速率：

- 在**计数 (Count)** 字段中输入值。
- 在**秒数 (Seconds)** 字段中输入值。

步骤 9 从**新状态 (New State)** 状态下拉列表中，指定满足条件时要采取的新操作。

步骤 10 在**超时 (Timeout)** 字段中输入值。

在超时后，规则将恢复到其原始状态。指定 0 或将**超时 (Timeout)** 字段留空可防止新操作超时。

步骤 11 点击 **OK**。

提示 系统将在“动态状态”(Dynamic State) 列中的规则旁边显示**动态状态** 。如果向规则中添加多个动态规则状态过滤器，过滤器上的数字表示过滤器的数量。

提示 要删除一组规则的所有动态规则设置，请在“规则”(Rules) 页面中选择这些规则，然后依次选择**动态状态 (Dynamic State)** > **删除基于速率的状态 (Remove Rate-Based States)**。也可以从规则的规则详细信息中删除个别基于速率的规则状态过滤器，方法是选择该规则后点击**显示详细信息 (Show details)**，然后点击要删除的基于速率的过滤器旁边的**删除 (Delete)**。

步骤 12 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

添加入侵规则注释

可以向入侵策略中的规则添加注释。按这种方式添加的注释是策略特定的；即添加到一个入侵策略的规则中的注释在其他入侵策略中不可见。添加的任何注释都将显示在该入侵策略的“规则”(Rules) 页面的“规则详细信息”(Rule Details) 视图中。

提交包含注释的入侵策略更改后，点击该规则 Edit 页面中的 **Rule Comment** 也可查看该注释。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择要在其中添加注释的一条或多条规则。

步骤 5 依次选择**注释 (Comments)** > **添加规则注释 (Add Rule Comment)**。

步骤 6 在**注释 (Comment)** 字段中，输入规则注释。

步骤 7 点击 **OK**。

提示 系统将并在“注释”(Comments) 列中的规则旁显示**注释**（  ）。如果向规则中添加多个注释，注释上的数字表示注释的数量。

步骤 8 或者，通过点击注释旁边的**删除 (Delete)** 以删除规则注释。

仅当缓存的注释具有未提交的入侵策略更改时，才能删除该注释。提交入侵策略更改之后，规则注释即是永久性的。

步骤 9 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

第 63 章

自定义入侵规则

以下主题介绍如何使用入侵规则编辑器：

自定义入侵规则概述

入侵规则是系统用于检测利用网络漏洞企图的一组关键字和参数。当系统分析网络流量时，它会将数据包与每条规则中指定的条件进行比较。如果数据包数据与规则中指定的所有条件都匹配，则会触发此规则。如果规则是警报规则，将生成入侵事件。如果是通过规则，将忽略流量。对于内联部署中的丢弃规则，系统将丢弃数据包并生成事件。可以通过Cisco Secure Firewall Management Center或网络界面查看和评估入侵事件。

Firepower 系统提供两种入侵规则：共享对象规则和标准文本规则。Talos 情报小组 可以使用共享对象规则来检测传统的标准文本规则无法检测到的漏洞攻击。您无法创建共享对象规则。在自行编写入侵规则时，您可以创建标准文本规则。

您可以编写自定义标准文本规则，以调整可能出现的事件类型。请注意，虽然本文档有时讨论以检测特定漏洞为目标的规则，但最成功的规则是以检测可能试图利用已知漏洞的流量为目标，而不是以检测特定已知漏洞为目标。通过编写规则和指定规则的事件消息，可以更轻松地识别可能存在攻击和策略逃避行为的流量。

当在自定义入侵策略中启用自定义标准文本规则时，请记住，某些规则关键字和参数要求首先以特定方式对流量进行解码或预处理。本章说明在用于管理预处理的网络分析策略中必须配置的选项。请注意，如果禁用所需的预处理器，系统会自动采用其当前设置使用该预处理器，尽管该预处理器在网络分析策略网络界面中保持禁用状态。

⚠

注意 将编写的入侵规则用于生产环境之前，请务必使用受控网络环境测试这些规则。编写错误的入侵规则可能会严重影响系统性能。

在多域部署中，系统会显示在当前域中创建的规则，您可以对其进行编辑。系统还会显示在祖先域中创建的规则，您不可以对其进行编辑。要查看和编辑在较低域中创建的规则，请切换至该域。 系统提供的入侵规则属于全局域。后代域中的管理员可以创建这些系统规则的本地可编辑副本。

入侵规则编辑器的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

入侵规则编辑器的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

规则剖析

所有标准文本规则均包含两个逻辑部分：规则报头和规则选项。规则报头包含：

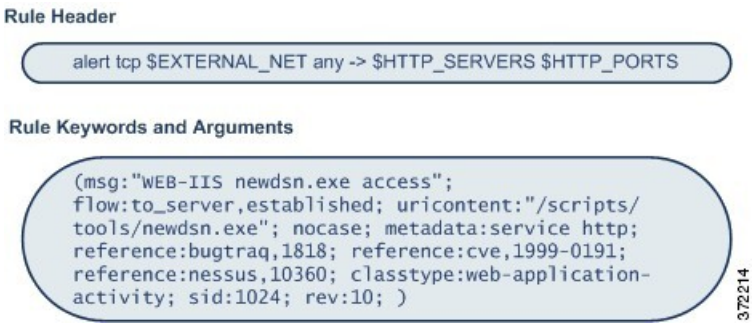
- 规则的操作或类型
- 协议
- 源 IP 地址、目标 IP 地址和子网掩码

- 方向指示符（显示从源到目标的流量流动方向）
- 源端口和目标端口

规则选项部分包含：

- 事件消息
- 关键字及其参数
- 模式（数据包负载必须与之匹配才能触发规则）
- 规范（规定规则引擎应检查数据包的哪些部分）

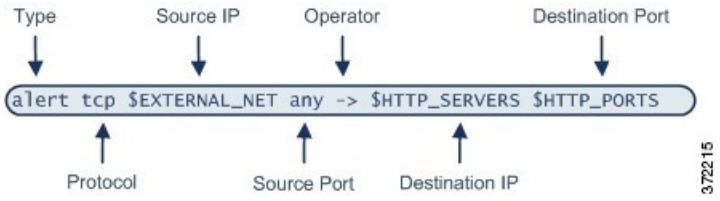
下图说明规则的组成部分：



请注意，括号里的是规则选项部分。入侵规则编辑器提供了一个易于使用的界面来帮助您构建标准文本规则。

入侵规则报头

每个标准文本规则和共享对象规则都有一个包含参数的规则报头。下面说明规则报头的组成部分：



下表介绍了规则报头的上述各个部分。

表 *111:* 规则报头值

规则报头组成部分	示例值	示例值的作用...
操作	`alert`	如果触发，将会生成事件。
协议	`tcp`	仅测试 TCP 流量。
源 IP 地址	`$EXTERNAL_NET`	测试来自不在内部网络上的任何主机的流量。

规则报头组成部分	示例值	示例值的作用...
源端口	any	测试来自发起主机上任何端口的流量。
运算符	->	测试外部流量（流向网络上的 Web 服务器）。
目标 IP 地址：	$HTTP_SERVERS	测试将要传送到内部网络上被指定为 Web 服务器的任何主机的流量。
目标端口	$HTTP_PORTS	测试传送到内部网络上 HTTP 端口的流量。

注释 与大多数入侵规则一样，以上示例使用默认变量。

相关主题

变量集，第 1042 页

入侵规则报头操作

每个规则报头都包含一个用于指定数据包触发规则时系统应采取的操作的参数。操作设置为 *alert* 的规则将会针对触发规则的数据包生成入侵事件并记录该数据包的详细信息。操作设置为 *pass* 的规则不会针对触发规则的数据包生成入侵事件，也不会记录该数据包的详细信息。

注释 在内联部署中，规则状态设置为“丢弃并生成事件”的规则会针对触发规则的数据包生成入侵事件。此外，如果在被动部署中应用丢弃规则，该规则将会充当警报规则。

默认情况下，通过规则会覆盖警报规则。可以创建通过规则来防止符合通过规则中定义的条件的数据包在特定情况下触发警报规则，而无需禁用预警报则。例如，您可能希望使检测尝试作为“匿名”用户登录 FTP 服务器这种情况的规则保持活动状态。但是，如果网络有一个或多个合法的匿名 FTP 服务器，您可以编写并激活一个通过规则，在其中指明匿名用户不会对那些特定服务器触发原始规则。

在入侵规则编辑器中，可以从**操作 (Action)** 列表中选择规则类型。

入侵规则报头协议

在每个规则报头中，必须指定规则检查的流量的协议。可以指定以下网络协议用于分析：

- ICMP（互联网控制消息协议）
- IP（互联网协议）

注释 如果协议设置为 `ip`，系统将忽略入侵规则报头中的端口定义。

- TCP（传输控制协议）
- UDP（用户数据报协议）

请使用**IP**作为协议类型，以检查IANA分配的所有协议（包括TCP、UDP、ICMP、IGMP等等）。

注释 目前不能编写与 IP 负载中下一个报头（例如 TCP 报头）模式匹配的规则。相反，内容匹配从上一个解码的协议开始。要解决这个问题，可以使用规则选项来匹配 TCP 报头中的模式。

在“入侵规则”(Intrusion Rules) 编辑器中，可以从**协议 (Protocol)** 列表中选择协议类型。

相关主题

入侵规则报头协议，第 1502 页

入侵规则报头方向

在规则报头中，可以指定数据包为使规则对其进行检查而必须传播的方向。下表介绍了这些选项。

表 *112:* 规则报头中的方向选项

使用.....	以测试...
定向天线	仅测试从指定源 IP 地址流向指定目标 IP 地址的流量
双向	测试指定的源 IP 地址和目标 IP 地址之间的所有流量

入侵规则报头源和目标 IP 地址

通过将数据包检查限制为仅;对来自或发往特定IP地址的数据包，可以减少系统必须执行的数据包检查工作量。这样做还可以令规则更加具体，并消除规则针对源和目标IP地址未指示可疑行为的数据包进行触发的可能性，从而减少误报。

提示 系统只能识别 IP 地址，不接受源或目标 IP 地址的主机名。

在入侵规则编辑器中，可以在**源 IP (Source IPs)** 和**目标 IP (Destination IPs)** 字段中指定源 IP 地址和目标 IP 地址。

编写标准文本规则时，可以根据自身需求以多种方法指定IPv4和IPv6地址。可以指定单个IP地址、`any`、IP地址列表、CIDR表示法、前缀长度或网络变量。此外，还可以指明要排除的特定IP地址或IP地址集。指定IPv6地址时，可使用RFC 4291中定义的任意寻址约定。

入侵规则中的 IP 地址语法

下表总结了可用于指定源 IP 地址和目标 IP 地址的各种方法。

表 *113:* 源/目标 *IP* 地址语法

指定的对象	使用.....	示例
任意 IP 地址	`any`	`any`
特定 IP 地址	IP 地址 请注意，不能在同一规则中混合使用 IPv4 和 IPv6 源地址和目标地址。	`192.168.1.1` `2001:db8::abcd`
IP 地址列表	使用方括号 (`[]`) 将地址括起来，并使用逗号分隔各个 IP 地址	`[192.168.1.1,192.168.1.15]` `[2001:db8::b3ff, 2001:db8::0202]`
IP 地址块	IPv4 CIDR 块或 IPv6 地址前缀表示法	`192.168.1.0/24` `2001:db8::/32`
除特定 IP 地址或地址集以外的任何项	`!` 字符，后接要否定的 IP 地址	`!192.168.1.15` `!2001:db8::0202:b3ff:fe1e`
IP 地址块中除一个或多个特定 IP 地址以外的任何 IP 地址	在地址块后加上被否定地址或地址块的列表	`[10.0.0/8, !10.2.3.4, !10.1.0.0/16]` `[2001:db8::/32, !2001:db8::8329, !2001:db8::0202]`
网络变量定义的 IP 地址	前面带有 `$` 的大写字母形式的变量名称 请注意，无论入侵规则中使用的网络变量定义的主机如何，预处理器规则都可以触发事件。	`$HOME_NET`
除 IP 地址变量定义的地址以外的所有 IP 地址	前面带有 `!$` 的大写字母形式的变量名称	`!$HOME_NET`

以下描述提供了有关某些 IP 地址输入方法的其他信息。

任意 IP 地址

可以指定 `any` 这个词作为规则的源或目标 IP 地址，以指示 IPv4 或 IPv6 地址。

例如，以下规则在**源 IP** 和**目标 IP** 字段中使用参数 **`any`** 来评估具有 IPv4 或 IPv6 源地址或目标地址的数据包：

```
alert tcp any any -> any any
```

还可以指定 `::` 以指示 IPv6 地址。

多个 IP 地址

可以列出多个 IP 地址，地址之间用逗号分隔，如有需要，还可以用方括号将非否定地址列表括起来，如以下示例所示：

```
[192.168.1.100,192.168.1.103,192.168.1.105]
```

可以单独或以任意组合列出 IPv4 和 IPv6 地址，如以下示例所示：

```
[192.168.1.100,2001:db8::1234,192.168.1.105]
```

请注意，现在不再要求用方括号将 IP 地址列表括起来（旧版软件要求这样做）。另请注意，输入列表时，可以在每个逗号前后添加一个空格。

注释 必须用方括号将否定列表括起来。

也可以使用 IPv4 无类域间路由选择 (CIDR) 表示法或 IPv6 前缀长度来指定地址块。例如：

- 192.168.1.0/24 指定子网掩码为 255.255.255.0 的 192.168.1.0 网络中的 IPv4 地址，即，192.168.1.0 至 192.168.1.255。
- 2001:db8::/32 指定前缀长度为 32 位的 2001:db8:: 网络中的 IPv6 地址，即，2001:db8:: 至 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff。

提示 如果需要指定 IP 地址块，但仅以 CIDR 或前缀长度表示法无法表示出该地址块，可以在 IP 地址列表中使用 CIDR 块和前缀长度。

IP 地址否定

可以使用感叹号 (!) 否定指定 IP 地址。也就是说，可以匹配除指定 IP 地址以外的所有 IP 地址。例如，`!192.168.1.1` 指定除 192.168.1.1 以外的任何 IP 地址，`!2001:db8:ca2e::fa4c` 指定除 2001:db8:ca2e::fa4c 以外的任何 IP 地址。

要否定某个 IP 地址列表，请用方括号将该 IP 地址列表括起来，并在其前面加上 `!`。例如，`![192.168.1.1,192.168.1.5]` 将定义除 192.168.1.1 和 192.168.1.5 以外的任何 IP 地址。

注释 要否定 IP 地址列表，必须使用方括号。

对 IP 地址列表使用否定字符时务必要小心。例如，如果使用 `[!192.168.1.1,!192.168.1.5]` 匹配不是 192.168.1.1 和 192.168.1.5 的任何地址，系统会将此语法解释为“非 192.168.1.1 的任何地址，**或**非 192.168.1.5 的任何地址”。

由于 192.168.1.5 不是 192.168.1.1，且 192.168.1.1 不是 192.168.1.5，因此，这两个 IP 地址都与 `[!192.168.1.1,!192.168.1.5]` 的 IP 地址值匹配；此语法实质上与使用“`any`”相同。

应该使用 `![192.168.1.1,192.168.1.5]`。系统会将此语法为“非 192.168.1.1 且非 192.168.1.5”，这意味着，与方括号中所列地址以外的任何 IP 地址匹配。

请注意，从逻辑上讲，不能对 `any` 进行否定（如果它被否定，将表示无地址）。

相关主题

变量集，第 1042 页

入侵规则报头源和目标端口

在入侵规则编辑器中，可以在**源端口 (Source Port)** 和**目标端口 (Destination Port)** 字段中指定源端口和目标端口。

入侵规则中的端口语法

Firepower 系统使用特定类型的语法来定义规则报头中使用的端口号。

注释 如果协议设置为 `ip`，系统将忽略入侵规则报头中的端口定义。

可以列出多个端口，端口之间用逗号分隔，如以下示例所示：

```
80, 8080, 8138, 8600-9000, !8650-8675
```

或者，以下示例显示如何用方括号将端口列表括起来（先前软件版本中要求如此，但现在不再有此要求）：

```
[80, 8080, 8138, 8600-9000, !8650-8675]
```

请注意，**必须**用方括号将求反端口列表括起来，如以下示例所示：

```
![20, 22, 23]
```

下表总结了可使用的语法：

表 *114:* 源/目标端口语法

指定的对象	使用	示例
任意端口	`any`	`any`
特定端口	端口号	`80`
端口范围	范围内第一个和最后一个端口号之间使用破折号	`80-443`
所有小于或等于指定端口号的端口	在端口号前面加上破折号	`-21`
所有大于或等于指定端口号的端口	在端口号后面加上破折号	`80-`

指定的对象	使用	示例
除特定端口或端口范围以外的所有端口	要求反的端口、端口列表或端口范围前面的 ! 字符 请注意，在逻辑上可以对除 any（如果求反，将指示无端口）以外的所有端口指定使用求反。	`!20`
端口变量定义的所有端口	前面带有 $ 的大写字母形式的变量名称	`$HTTP_PORTS`
除端口变量定义的端口以外的所有端口	前面带有 !$ 的大写字母形式的变量名称	`!$HTTP_PORTS`

入侵事件详细信息

构建标准文本规则时，可以包含说明规则在攻击尝试中检测到的漏洞的情景信息。也可以在其中纳入对漏洞数据库的外部参考，以及定义入侵事件在贵公司中具有的优先级。这样，如果分析师发现入侵事件，他们可随时获取有关优先级、漏洞和已知缓解措施的信息。

消息

可以指定规则触发时以消息形式显示的有意义的文本。这类消息使您可以即时了解规则检测的漏洞的性质。可以使用除花括号 ({}) 以外的所有可打印标准 ASCII 字符。系统将移除将消息完全引起来的引号。

提示 必须指定规则消息。此外，消息不能只包含空白字符、一个或多个引号、一个或多个撇号或者仅由空白字符、引号或撇号组成的任意组合。

要在入侵规则编辑器中定义事件消息，请在**消息 (Message)** 字段中输入事件消息。

分类

对于每个规则，可以指定事件数据包显示中出现的攻击分类。下表列出了每种分类的名称和编号。

表 *115:* 规则分类

编号	分类名称	说明
1	not-suspicious	非可疑流量
2	unknown	未知流量
3	bad-unknown	潜在不良流量
4	attempted-recon	尝试信息泄露
5	successful-recon-limited	信息泄露

编号	分类名称	说明
6	successful-recon-largescale	大规模信息泄露
7	attempted-dos	尝试拒绝服务
8	successful-dos	拒绝服务
9	attempted-user	尝试获取用户权限
10	unsuccessful-user	未成功获取用户权限
11	successful-user	未成功获取用户权限
12	attempted-admin	尝试获取管理员权限
13	successful-admin	成功获取管理员权限
14	rpc-portmap-decode	解码 RPC 查询
15	shellcode-detect	检测到可执行代码
16	string-detect	检测到可疑字符串
17	suspicious-filename-detect	检测到可疑文件名
18	suspicious-login	检测到尝试使用可疑用户名的登录
19	system-call-detect	检测到系统调用
20	tcp-connection	检测到 TCP 连接
21	trojan-activity	检测到网络木马
22	unusual-client-port-connection	客户端使用异常端口
23	network-scan	检测网络扫描
24	denial-of-service	检测拒绝服务攻击
25	non-standard-protocol	检测非标准协议或事件
26	protocol-command-decode	通用协议命令解码
27	web-application-activity	访问可能易受攻击的 Web 应用
28	web-application-attack	Web 应用攻击
29	misc-activity	其他活动
30	misc-attack	其他攻击
31	icmp-event	般 ICMP 事件

编号	分类名称	说明
32	inappropriate-content	检测到不当内容
33	policy-violation	可能违反公司隐私策略
34	default-login-attempt	尝试使用默认用户名和密码登录
35	sdf	敏感数据
36	malware-cnc	已知恶意软件命令和控制流量
37	client-side-exploit	已知客户端攻击尝试
38	file-format	已知的恶意文件或基于文件的攻击

自定义分类

如果您希望事件的数据包显示说明的更多自定义内容由您定义的规则生成，则可以创建自定义分类。

参数	说明
分类名称	分类的名称。如果使用超过 40 个字符，则页面难以读取。不支持以下字符：`<>()\'"&$;` 以及空格字符。
分类说明 (Classification Description)	分类的说明。可使用字母数字字符和空格。不支持以下字符：`<>()\'"&$;`
优先级	高、中或低。

自定义优先级

默认情况下，规则的优先级来源于其事件分类。但是，可以通过向规则中添加 `priority` 关键字并选择高、中或低优先级来覆盖规则的分类优先级。例如，要为检测 Web 应用攻击的规则分配高优先级，请向该规则中添加 `priority` 关键字，并选择**高 (high)** 作为优先级。

自定义参考

可以使用 `reference` 关键字添加对外部网站以及对关于事件的其他信息的参考。添加参考使分析师可以随时获得所需的资源，从而帮助他们确定数据包触发规则的原因。下表列出了一些可提供关于已知漏洞和攻击的数据的外部系统。

表 *116:* 外部攻击识别系统

系统 ID	说明	示例 ID
`bugtraq`	Bugtraq 页面	`8550`
`cve`	常见漏洞和风险 ID	`2020-9607`

系统 ID	说明	示例 ID
mcafee	McAfee 页面	98574
url	网站参考	www.example.com?exploit=14
msb	Microsoft 安全公告	MS11-082
nessus	Nessus 页面	10039
secure-url	安全网站参考 (https://...)	intranet/exploits/exploit=14 请注意，可以对任何安全网站使用 secure-url。

通过输入参考值指定参考，如下所示：

```
id_system,id
```

其中，id_system 是用作前缀的系统，id 是 CVE ID 编号、Arachnids ID 或 URL（不包含 http://）。

例如，要指定 CVE-2020-9607 中记录的 Adobe Acrobat 和 Reader 问题，请输入值：

```
cve,2020-9607
```

向规则添加参考时应注意以下几点：

- 逗号后不能有空格。
- 系统 ID 不能是大写字母。

相关主题

添加自定义分类，第 1510 页
定义事件优先级，第 1511 页
定义事件引用，第 1511 页

添加自定义分类

在多域部署中，系统会显示在当前域创建的自定义分类，您可以设置这些分类的优先级。系统还会显示在祖先域创建的自定义分类，但您无法设置这些分类的优先级。要查看和编辑在较低域中创建的自定义分类，请切换至该域。

过程

步骤 1 当创建或编辑规则时，请从**分类 (Classification)** 下拉列表中选择**编辑分类 (Edit Classifications)**。

如果系统显示**查看分类 (View Classifications)**，则配置属于祖先域，或者您没有修改配置的权限。

步骤 2 输入**分类名称 (Classification Name)** 和**分类说明 (Classification Description)**，如入侵事件详细信息，第 1507 页中所述。

步骤 3 从**优先级 (Priority)** 下拉列表中为分类选择优先级。

步骤 4 点击 **Add**。

步骤 5 点击 **Done**。

定义事件优先级

过程

步骤 1 当创建或编辑规则时，从**检测选项 (Detection Options)** 下拉列表中选择优先级 `(priority)`。

步骤 2 点击**添加选项 (Add Option)**。

步骤 3 从**优先级 (priority)** 下拉列表中选择值。

步骤 4 点击**保存 (Save)**。

定义事件引用

过程

步骤 1 在创建或编辑规则时，从**检测选项 (Detection Options)** 下拉列表中选择 `reference`。

步骤 2 点击**添加选项 (Add Option)**。

步骤 3 在 **reference** 字段中输入值，如入侵事件详细信息，第 1507 页中所述。

步骤 4 点击**保存 (Save)**。

搜索规则

系统提供数千个标准文本规则，并且Talos 情报小组 会在发现新漏洞和攻击时继续添加规则。您可以轻松搜索您想要激活、禁用或编辑的特定规则。

过程

步骤 1 使用以下任一方法访问入侵规则：

- 选择**策略** > **访问控制** > **入侵**。

  点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**，然后点击**规则 (Rules)**。

- 选择**对象** > **入侵规则**。

步骤 2 点击工具栏上的 **Search**。

步骤 3 添加搜索条件。

步骤 4 点击 **Search**。

入侵规则的搜索条件

下表介绍了可用的搜索选项：

表 *117:* 规则搜索条件

选项	说明
签名 ID (Signature ID)	要根据 Snort ID (SID) 搜索单个规则，请输入一个 SID 号。要搜索多个规则，请输入以逗号分隔的 SID 号列表。此字段中最多可输入 80 个字符。
生成器 ID	要搜索标准文本规则，请选择 **1**。要搜索共享对象规则，请选择 **3**。
消息	要搜索带有特殊消息的规则，请在**消息 (Message)** 字段中输入规则消息中的一个字。例如，要搜索 DNS 攻击，可输入 `DNS`；要搜索缓冲区溢出攻击，可输入`溢出 (overflow)`。
协议	要搜索评估特定协议的流量的规则，请选择该协议。如果不选择协议，搜索结果将包含适用于所有协议的规则。
源端口	要搜索检查来自指定端口的数据包的规则，请输入源端口号或端口相关变量。
目标端口	要搜索检查发往特定端口的数据包的规则，请输入目标端口号或端口相关变量。
源 IP	要搜索检查来自指定 IP 地址的数据包的规则，请输入源 IP 地址或 IP 地址相关变量。
目标 IP	要搜索检查发往指定 IP 地址的数据包的规则，请输入目标 IP 地址或 IP 地址相关变量。
关键字	要搜索特定关键字，可以使用关键字搜索选项。可以选择要搜索的关键字并输入关键字值。也可以在关键字值前面加上感叹号 (!) 以匹配任何未指定的值。
类别 (Category)	要搜索特定类别中的规则，请从**类别 (Category)** 列表中选择该类别。
分类 (Classification)	要搜索具有特定分类的规则，请从**分类 (Classification)** 列表中选择该分类名称。
规则状态 (Rule State)	要在特定策略和特定规则状态中搜索规则，请从第一个**规则状态 (Rule State)** 列表中选择策略，并从第二个列表中选择状态，以搜索状态设置为**生成事件 (Generate Events)**、**丢弃并生成事件 (Drop and Generate Events)** 或**已禁用 (Disabled)** 的规则。

入侵规则编辑器页面上的规则过滤

您可以对入侵规则编辑器页面上的规则进行过滤以显示其中一组规则。例如，如果想要修改某个规则或更改其状态，但是难以在成千上万个可用规则中找到该规则，这个过滤功能可能很有用。

当您输入过滤器时，页面将显示至少包含一条匹配规则或消息（如果没有匹配规则）的文件夹。

过滤准则

过滤器可以包含特殊关键字及其参数、字符串和用引号引起来的文字字符串，多个过滤器条件之间用空格隔开。过滤器不能包含正则表达式、通配符或任何特殊运算符，例如取反字符 (!)、大于号 (>) 和小于号 (<) 等。

所有关键字、关键字参数和字符串都不区分大小写。除关键字 `gid` 和 `sid` 之外，所有参数和字符串都被视为部分字符串。`gid` 和 `sid` 的参数只会返回完全匹配项。

您可以在未经过滤的原始页面上展开某个文件夹，如果后续过滤器返回该文件夹中的匹配项，该文件夹将会保持展开。这对于在包含大量规则的文件夹中搜索规则可能有用。

不能使用后续过滤器限制任何过滤器。输入的任何过滤器都会搜索整个规则数据库并返回所有匹配的规则。当您在页面仍显示上一过滤器的结果时输入过滤器，页面将清空，转而返回新过滤器的结果。

您可以对已过滤或未过滤列表中的规则使用相同的功能。例如，可以编辑入侵规则编辑器页面上经过过滤或未经过滤的列表中的规则。您也可以使用该页面上下文菜单中的任何选项。

提示 如果所有子组中的总规则数量很大，过滤所需的时间可能大大增加，因为规则显示在多个类别中，即使唯一规则的总数少很多也是如此。

关键字过滤

每个规则过滤器都可以包含一个或多个关键字，其格式如下：

```
keyword:argument
```

其中，关键字是下表中的其中一个关键字，参数是要在与该关键字相关的一个或多个指定字段中搜索的一个字母数字字符串，不区分大小写。

除 `gid` 和 `sid` 之外，所有关键字的参数都会被视为部分字符串。例如，参数 `123` 将返回 `"12345"`、`"41235"`、`"45123"` 等。`gid` 和 `sid` 的参数只会返回完全匹配项；例如，`sid:3080` 只会返回结果 SID 3080。

提示 使用一个或多个字符串来进行过滤可以搜索部分 SID。

下表介绍了可以用于过滤规则的特定过滤关键字和参数。

表 *118:* 规则过滤器关键字

关键字	说明 (Description)	示例
`arachnids`	根据规则引用中的完整或部分 Arachnids ID 返回一个或多个规则。	`arachnids:181`
`bugtraq`	根据规则引用中的完整或部分 Bugtraq ID 返回一个或多个规则。	`bugtraq:2120`
`cve`	根据规则引用中的完整或部分 CVE 编号返回一个或多个规则。	`cve:2003-0109`
`gid`	参数 `1` 将返回标准文本规则。参数 `3` 将返回共享对象规则。	`gid:3`
`mcafee`	根据规则引用中的完整或部分 McAfee ID 返回一个或多个规则。	`mcafee:10566`
`msg`	根据规则的完整或部分 Message 字段（又称为事件消息）返回一个或多个规则。	`msg:chat`
`nessus`	根据规则引用中的完整或部分 Nessus ID 返回一个或多个规则。	`nessus:10737`
`ref`	根据规则引用或规则 Message 字段中一个完整的字母数字字符串或其一部分返回一个或多个规则。	`ref:MS03-039`
`sid`	返回带有完全匹配的 Snort ID 的规则。	`sid:235`
`url`	根据规则引用中的完整或部分 URL 返回一个或多个规则。	`url:faqs.org`

相关主题

定义事件引用，第 1511 页
入侵事件详细信息，第 1507 页

字符串过滤

每个规则过滤器可以包含一个或多个字母数字字符串。字符串将搜索规则的**消息**字段、Snort ID (SID) 和生成器 ID (GID)。例如，字符串 `123` 会返回规则消息中的 `"Lotus123"`、`"123mania"` 等字符串，也会返回 SID 6123、SID 12375 等。

所有字符串都不区分大小写并被视为部分字符串。例如，字符串 `ADMIN`、`admin` 或 `Admin` 中的任意一个都会返回 `"admin"`、`"CFADMIN"`、`"Administrator"` 等等。

用引号将字符串引起来可以返回完全匹配项。例如，用引号引起来的原义字符串 `"overflow attempt"` 只会返回完全匹配的该字符串，而由 `overflow` 和 `attempt` 这两个字符串组成的未加引号的过滤器则会返回 `"overflow attempt"`、`"overflow multipacket attempt"`、`"overflow with evasion attempt"` 等结果。

相关主题

入侵事件详细信息，第 1507 页

组合关键字和字符串过滤

输入关键字、字符串或这二者的任意组合并以空格分隔可以缩小过滤结果的范围。结果包括符合所有过滤条件的任意规则。

可以按照任意顺序输入多个过滤条件。例如，以下每个过滤器返回的规则相同：

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

过滤规则

在“入侵规则”(Intrusion Rules) 页面上，可以将规则过滤为子集，以便可以更轻松地查找特定规则。然后，可以使用任何页面功能，包括选择情景菜单中可用的任何功能。

规则过滤尤其适用于查找要编辑的特定规则。

过程

步骤 1 使用以下任一方法访问入侵规则：

- 选择**策略** > **访问控制** > **入侵**。

  点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**，然后点击**规则 (Rules)**。

- 选择**对象** > **入侵规则**。

步骤 2 在过滤之前，您有以下选择：

- 展开要展开的任何规则组。某些规则组还具有可展开的子组。

  如果您预计规则可能在某个组中，则在未经过滤的原始页面上展开该组可能有用。如果后续过滤器返回该文件夹中的匹配项，当您点击过滤器 **清除**（✕）返回到未经过滤的原始页面时，该组将会保持展开。

- 从**规则分组方法 (Group Rules By)** 下拉列表中选择其他分组方法。

步骤 3 在**规则分组方法 (Group Rules By)** 列表下的 **过滤器**（🔍） 旁边的文本框中输入过滤器限制。

步骤 4 按下 Enter 键。

注释 通过点击过滤器 **清除**（✕）清除当前已过滤的列表。

入侵规则中的关键字和参数

借助规则语言，可以通过组合关键字来指定规则行为。关键字及其相关值（称为参数）规定系统如何评估规则引擎测试的数据包和数据包相关值。Firepower 系统当前支持允许您执行检查功能（例如内容匹配、协议特定模式匹配和状态特定匹配）的关键字。在每个关键字中最多可以定义 100 个参数，还可以组合任意数量的兼容关键字来创建非常具体的规则。这有助于降低出现误报和漏报的可能性，使您可以重点关注接收到的入侵信息。

请注意，您也可以在被动部署中使用自适应配置文件，以根据规则元数据和主机信息动态调整对特定数据包的主动规则处理。

本节所述的关键字列于规则编辑器中的“检测选项”(Detection Options) 下。

相关主题

关于自适应配置文件 ，第 2201 页

content 和 protected_content 关键字

使用 `content` 关键字或 `protected_content` 关键字可以指定要在数据包中检测的内容。

大多数情况下，应始终在 `content` 或 `protected_content` 关键字后面加上修饰符，指示对内容进行搜索的位置、搜索是否区分大小写及其他选项。

请注意，要使规则触发事件，所有内容匹配必须为真，也就是说，每项内容匹配与其他匹配之间都存在 AND 关系。

另请注意，在内联部署中，可以将规则设置为匹配恶意内容并将其更换为您自定义的等长文本字符串。

content

当使用 `content` 关键字时，规则引擎在数据包负载或数据流中搜索该字符串。例如，如果输入 `/bin/sh` 作为其中一个 `content` 关键字的值，则规则引擎会在数据包负载中搜索字符串 `/bin/sh`。

可以使用 ASCII 字符串、十六进制内容（二进制字节代码）或这两者的组合来匹配内容。可以在关键字值中将十六进制内容放在两条竖线 (|) 之间。例如，可以混合使用十六进制内容和 ASCII 内容，例如，`|90C8 C0FF FFFF|/bin/sh`。

可以在一个规则中指定多项内容匹配。要这样做，请使用 `content` 关键字的其他实例。对于各项内容匹配，可以指明必须在数据包负载或数据流中发现内容匹配才可触发规则。

注意 如果创建的规则只包含一个 `content` 关键字，但没有为该关键字选择 **Not** 选项，可能会使入侵策略无效。

protected_content

protected_content 关键字使您可以在配置规则参数前对搜索内容字符串进行编码。原始规则作者在配置关键字前使用哈希函数（SHA-512、SHA-256 或 MD5）对字符串进行编码。

如果使用 protected_content 关键字而不使用 content 关键字，规则引擎在数据包负载或数据流中搜索字符串的方式并不会改变，且大多数关键字选项将起到预期作用。下表总结了 protected_content 关键字选项与 content 关键字选项存在差异的例外情况。

表 *119: protected_content* 选项例外

选项	说明
散列类型 (Hash Type)	protected_content 规则关键字的新增选项。
区分大小写	不支持
在	不支持
深度	不支持
长度	protected_content 规则关键字的新增选项。
使用快速模式匹配程序 (Use Fast Pattern Matcher)	不支持
仅快速模式匹配程序 (Fast Pattern Matcher Only)	不支持
快速模式匹配程序偏移和长度 (Fast Pattern Matcher Offset and Length)	不支持

思科建议在包含 protected_content 关键字的规则中至少包含一个 content 关键字，以确保规则引擎使用快速模式匹配程序，从而加快处理速度和提高性能。在规则中，content 关键字应置于 protected_content 关键字之前。请注意，如果规则包含至少一个 content 关键字，无论您是否启用 content 关键字的“使用快速模式匹配程序”(Use Fast Pattern Matcher) 参数，规则引擎都会使用快速模式匹配程序。

注意 如果创建的规则只包含一个 protected_content 关键字，但没有为该关键字选择 **Not** 选项，可能会使入侵策略无效。

相关主题

基本 content 和 protected_content 关键字参数 ，第 1517 页
replace 关键字 ，第 1527 页

基本 content 和 protected_content 关键字参数

可以通过修饰 content 或 protected_content 关键字的参数来限制内容搜索的位置以及大小写。配置用于修饰 content 或 protected_content 关键字的选项可以指定要搜索的内容。

区分大小写

注释 配置 protected_content 关键字时不支持此选项。

可以指示规则引擎在搜索 ASCII 字符串内容匹配时忽略大小写。要使搜索不区分大小写，请在指定内容搜索时选择**不区分大小写 (Case Insensitive)**。

散列类型

注释 此选项**仅**对于 protected_content 关键字可配置。

使用**散列类型 (Hash Type)** 下拉列表确定用于编码搜索字符串的散列函数。系统支持对 protected_content 搜索字符串进行 SHA-512、SHA-256 和 MD5 散列处理。如果散列内容的长度与所选的散列类型不匹配，系统将**不**会保存规则。

系统自动选择思科设置的默认值。如果选择了 **Default**，将不会向规则写入特定哈希函数，且系统将假设 SHA-512 为哈希函数。

原始数据

Raw Data 选项指示规则引擎在分析规范化负载数据（由网络分析策略解码）之前分析原始数据包负载，并且此选项不使用参数值。进行规范化之前，可以在分析 telnet 流量时使用此关键字在负载中检查 telnet 协商选项。

不能在同一个 content 或 protected_content 关键字中同时使用 **Raw Data** 选项和任何 HTTP 内容选项。

提示 可以配置 HTTP 检查预处理器 **Client Flow Depth** 和 **Server Flow Depth** 选项，以确定是否在 HTTP 流量中检查原始数据以及检查的原始数据量。

不

选择**不**选项可搜索与指定内容不匹配的内容。如果创建包含已选择**不**选项的 content 或 protected_content 关键字的规则，则必须在该规则中至少包含另一个未选择 **Not** 选项的 content 或 protected_content 关键字。

注意 请勿创建仅包含一个已选择 **Not** 选项的 content 或 protected_content 关键字的规则。否则，可能会使入侵策略无效。

例如，SMTP 规则 1:2541:9 包含三个 content 关键字，其中一个选择了**不匹配 (Not)** 选项。如果移除除选择了**不匹配 (Not)** 选项的关键字以外的其他 content 关键字，基于该规则的自定义规则将无效。将此类规则添加到入侵策略可能会导致该策略失效。

提示 不能对同一个 content 关键字同时选择 **Not** 复选框和 **Use Fast Pattern Matcher** 复选框。

content 和 protected_content 关键字搜索位置

可以使用搜索位置选项指定开始搜索指定内容的位置以及继续搜索的深度。

允许的组合：content 搜索位置参数

可以使用两个 content 位置对指定开始搜索指定内容的位置以及继续搜索的深度，如下所述：

- 同时使用**偏移量 (Offset)** 和**深度 (Depth)** 选项可相对于数据包负载起点进行搜索。
- 同时使用**距离 (Distance)** 和**范围内 (Within)** 可相对于当前搜索位置进行搜索。

如果仅指定选项对中的其中一个选项，系统将会假设另一个选项使用默认值。

不能将**偏移量**和**深度**选项与**距离**和**范围内**选项混合使用。例如，不能将**偏移量 (Offset)** 和**范围内 (Within)** 这两个选项配合使用。可以在规则中使用任意数量的位置选项。

如果未指定位置，系统将假设**偏移量 (Offset)** 和**深度 (Depth)** 选项为默认值；也就是说，将从数据包负载起点开始进行内容搜索，直至数据包终点。

还可以使用现有 byte_extract 变量指定位置选项的值。

提示 可以在规则中使用任意数量的位置选项。

相关主题

byte_extract 关键字，第 1533 页

允许的组合：protected_content 搜索位置参数

将必填的**长度** protected_content 位置选项与**偏移**或**距离**位置选项结合使用，可指定开始搜索指定内容的位置以及继续搜索的深度，如下所示：

- 同时使用**长度 (Length)** 和**偏移 (Offset)** 选项可相对于数据包负载起点搜索受保护字符串。
- 同时使用**长度 (Length)** 和**距离 (Distance)** 选项可相对于当前搜索位置搜索受保护字符串。

提示 不能在单个关键字配置中同时使用**偏移 (Offset)** 和**距离 (Distance)** 选项，但可以在规则内使用任意数量的位置选项。

如果未指定位置，系统将假设使用默认值；也就是说，将从数据包负载起点开始进行内容搜索，直至数据包终点。

还可以使用现有 byte_extract 变量指定位置选项的值。

相关主题

byte_extract 关键字 ，第 1533 页

content 和 protected_content 搜索位置参数

深度

注释 此选项**仅**在配置 content 关键字时可用。

指定最大内容搜索深度（以字节为单位），从偏移量值起点开始计算，如果没有配置偏移量，则从数据包负载起点开始计算。

例如，如果规则的内容值为 cgi-bin/phf，offset 值为 3，depth 值为 22，规则将从字节 3 开始搜索 cgi-bin/phf 字符串内容匹配，并在处理完符合规则报头指定参数的数据包中的 22 个字节（字节 25）后停止。

必须指定一个大于或等于指定内容长度的数值，最多 65535 字节。不能指定值 0。

默认深度是搜索至数据包终点。

距离

指示规则引擎识别在上一次成功内容匹配后出现指定数量字节的后续内容匹配。

由于偏移量计数器从字节 0 开始计算，因此，应指定比所需字节数小 1 的值，以便从上一次成功内容匹配开始继续搜索。例如，如果指定 4，搜索将从第五个字节开始。

可指定 -65535 到 65535 字节之间的值。如果在距离中指定负值，开始搜索的字节可能位于数据包开头以外。所有计算都会将数据包以外的字节考虑在内，尽管搜索实际上从数据包的第一个字节开始。例如，如果数据包当前位置是第五个字节，下一个内容规则选项指定距离值为 -10，内部值为 20，搜索将从负载起点开始，且内部选项将调整为 15。

默认距离是 0，表示继上一次内容匹配之后数据包中的当前位置。

长度

注释 此选项**仅**在配置 protected_content 关键字时可用。

长度 (Length) protected_content 关键字选项表示非散列搜索字符串的长度（以字节为单位）。

例如，如果使用了内容 Sample1 生成安全散列值，请将**长度 (Length)** 值设置为 7。**必须**在该字段中输入一个值。

Offset

指定数据包负载中开始内容搜索的位置与数据包负载起点之间的距离（以字节为单位）。可指定 65535 到 65535 字节之间的值。

由于偏移量计数器从字节 0 开始计算，因此，应指定比所需字节数小 1 的值，以便从数据包负载起点开始继续搜索。例如，如果指定 7，搜索将从第八个字节开始。

默认偏移量是 0，表示数据包起点。

在

注释 此选项仅在配置 `content` 关键字时可用。

范围内 (Within) 选项指明，要触发规则，下一次内容匹配必须发生在上一次成功内容匹配结束之后指定数量的字节内。例如，如果将**范围内 (Within)** 值指定为 `8`，下一次内容匹配必须出现在数据包负载中接下来的八个字节之内，否则将无法满足触发规则的标准。

可以指定一个大于或等于指定内容长度的数值，最多 65535 字节。

范围内 (Within) 的默认设置是搜索至数据包终点。

概述：HTTP content 和 protected_content 关键字参数

通过 HTTP `content` 或 `protected_content` 关键字选项，可以在 HTTP 检查预处理器解码的 HTTP 消息中指定搜索内容匹配项的位置。

以下两个选项搜索 HTTP 响应中的状态字段：

- **HTTP 状态代码**
- **HTTP 状态消息 (HTTP Status Message)**

请注意，尽管规则引擎搜索未规范化的原始状态字段，但这里分别列出这些选项，以方便在下文解释将其他原始 HTTP 字段与规范化 HTTP 字段结合使用时应考虑的限制。

以下五个选项根据情况搜索 HTTP 请求和/或响应中的规范化字段：

- **HTTP URI**
- **HTTP 方法**
- **HTTP 报头 (HTTP Header)**
- **HTTP Cookie**
- **HTTP 客户端正文 (HTTP Client Body)**

以下三个选项根据情况搜索 HTTP 请求和/或响应中的原始（未规范化）非状态字段：

- **HTTP 原始 URI (HTTP Raw URI)**
- **HTTP 原始报头 (HTTP Raw Header)**

- **HTTP 原始 Cookie (HTTP Raw Cookie)**

选择 HTTP `content` 选项时，请遵循以下准则：

- HTTP `content` 选项仅适用于 TCP 流量。
- 为避免对性能造成负面影响，应只选择消息中那些可能出现指定内容的部分。

  例如，如果流量可能包含大型 cookie（例如，购物车消息中的 cookie），可以在 HTTP 报头中搜索指定内容，而不是在 HTTP cookie 中搜索。

- 为利用 HTTP 检查预处理器规范化以及提高性能，所创建的任何 HTTP 相关规则应包含至少一个已选择 **HTTP URI**、**HTTP Method**、**HTTP Header** 或 **HTTP Client Body** 选项的 `content` 或 `protected_content` 关键字。
- 不能将 `replace` 关键字与 HTTP `content` 或 `protected_content` 关键字选项配合使用。

可以指定单个规范化 HTTP 选项或状态字段，或者使用规范化 HTTP 选项与状态字段的任意组合，以指向要匹配的内容区域。但在使用 HTTP 字段选项时，请注意以下限制：

- 不能在同一个 `content` 或 `protected_content` 关键字中同时使用**原始数据 (Raw Data)** 选项和任何 HTTP 选项。
- 不能在同一个 `content` 或 `protected_content` 关键字中同时使用原始 HTTP 字段选项（**HTTP 原始 URI [HTTP Raw URI]**、**HTTP 原始报头 [HTTP Raw Header]** 或 **HTTP 原始 Cookie [HTTP Raw Cookie]**）及其对应的规范化选项（分别是 **HTTP URI**、**HTTP 报头 [HTTP Header]** 或 **HTTP Cookie**）。
- 不能同时选择**使用快速模式匹配程序 (Use Fast Pattern Matcher)** 和以下一个或多个 HTTP 字段选项：

  HTTP 原始 URI (HTTP Raw URI)、**HTTP 原始报头 (HTTP Raw Header)**、**HTTP 原始 Cookie (HTTP Raw Cookie)**、**HTTP Cookie**、**HTTP 方法 (HTTP Method)**、**HTTP 状态消息 (HTTP Status Message)** 或 **HTTP 状态代码 (HTTP Status Code)**

  但是，可以在也使用快速模式匹配程序搜索以下其中一个规范化字段的 `content` 或 `protected_content` 关键字中包含上述选项：

  HTTP URI、**HTTP 报头 (HTTP Header)** 或 **HTTP 客户端正文 (HTTP Client Body)**

  例如，如果选择 **HTTP Cookie**、**HTTP 报头 (HTTP Header)** 和 **使用快速模式匹配程序 (Use Fast Pattern Matcher)**，规则引擎将会在 HTTP cookie 和 HTTP 报头中搜索内容，但快速模式匹配程序仅适用于 HTTP 报头，而不适用于 HTTP cookie。

- 将受限选项和不受限选项结合使用时，快速模式匹配程序将仅搜索您指定的不受限字段，以测试是否要将规则传递到入侵规则编辑器来完成评估，包括受限字段的评估。

相关主题

content 关键字快速模式匹配程序参数 ，第 1525 页

HTTP content 和 protected_content 关键字参数

HTTP URI

选择此选项将会在规范化的请求 URI 字段中搜索内容匹配。

请注意，不能将此选项与 `pcre` 关键字 HTTP URI (U) 选项结合使用来搜索相同的内容。

注释 管道化 HTTP 请求数据包包含多个 URI。如果选择了 **HTTP URI**，且规则引擎检测到管道化 HTTP 请求数据包，规则引擎将会搜索数据包中的所有 URI 以进行内容匹配。

HTTP Raw URI

选择此选项将会在规范化的请求 URI 字段中搜索内容匹配。

请注意，不能将此选项与 `pcre` 关键字 HTTP URI (U) 选项结合使用来搜索相同的内容。

注释 管道化 HTTP 请求数据包包含多个 URI。如果选择了 **HTTP URI**，且规则引擎检测到管道化 HTTP 请求数据包，规则引擎将会搜索数据包中的所有 URI 以进行内容匹配。

HTTP 方法

选择此选项将会在请求方法字段中搜索内容匹配，该字段确定要对 URI 中识别出的资源执行的操作（例如 GET 和 POST）。

HTTP Header

选择此选项将会在 HTTP 请求内的规范化报头字段（cookie 除外）中搜索内容匹配；如果 HTTP 检查预处理器的**检查 HTTP 响应 (Inspect HTTP Responses)** 选项已启用，还会在响应中搜索内容匹配。

请注意，不能将此选项与 `pcre` 关键字 HTTP 报头 (H) 选项结合使用来搜索相同的内容。

HTTP Raw Header

选择此选项将会在 HTTP 请求内的原始报头字段（cookie 除外）中搜索内容匹配；如果 HTTP 检查预处理器的**检查 HTTP 响应 (Inspect HTTP Responses)** 选项已启用，还会在响应中搜索内容匹配。

请注意，不能将此选项与 `pcre` 关键字 HTTP 原始报头 (D) 选项结合使用来搜索相同的内容。

HTTP Cookie

选择此选项将会在规范化 HTTP 客户端请求报头内识别出的任何 cookie 中搜索内容匹配；如果 HTTP 检查预处理器的**检查 HTTP 响应 (Inspect HTTP Responses)** 选项已启用，还会在响应 set-cookie 数据中搜索内容匹配。请注意，系统将消息正文中包含的 cookie 看作正文内容。

若要仅对 cookie 进行内容匹配搜索，必须启用 HTTP 检查预处理器的**检查 HTTP Cookie (Inspect HTTP Cookies)** 选项；否则，规则引擎将搜索包括 cookie 在内的整个报头。

请注意以下提示：

- 不能将此选项与 `pcre` 关键字 HTTP cookie (C) 选项结合使用来搜索相同的内容。
- `Cookie:` 和 `Set-Cookie:` 报头名称、标题行中的前导空格以及终止标题行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。

HTTP Raw Cookie

选择此选项将会在原始 HTTP 客户端请求报头内识别出的任何 cookie 中搜索内容匹配；如果 HTTP 检查预处理器的**检查 HTTP 响应 (Inspect HTTP Responses)** 选项已启用，还会在响应 set-cookie 数据中搜索内容匹配；请注意，系统将消息正文中包含的 cookie 看作正文内容。

若要仅对 cookie 进行内容匹配搜索，必须启用 HTTP 检查预处理器的**检查 HTTP Cookie (Inspect HTTP Cookies)** 选项；否则，规则引擎将搜索包括 cookie 在内的整个报头。

请注意以下提示：

- 不能将此选项与 `pcre` 关键字 HTTP 原始 cookie (K) 选项结合使用来搜索相同的内容。
- `Cookie:` 和 `Set-Cookie:` 报头名称、标题行中的前导空格以及终止标题行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。

HTTP Client Body

选择此选项将会在 HTTP 客户端请求消息正文中搜索内容匹配。

请注意，要使此选项起作用，必须为 HTTP 检查预处理器的**HTTP 客户端正文提取深度 (HTTP Client Body Extraction Depth)** 选项指定一个 0 到 65535 之间的值。

HTTP 状态代码

选择此选项将会在 HTTP 响应的三位数状态代码中搜索内容匹配。

要使此选项能够返回匹配，必须启用 HTTP 检查预处理器的**检查 HTTP 响应 (Inspect HTTP Responses)** 选项。

HTTP Status Message

选择此选项将会在 HTTP 响应中状态代码随附的文字描述中搜索内容匹配。

要使此选项能够返回匹配，必须启用 HTTP 检查预处理器的**检查 HTTP 响应 (Inspect HTTP Responses)** 选项。

相关主题

pcre 修饰符选项，第 1541 页
服务器级别 HTTP 规范化选项，第 2092 页

概述：content 关键字快速模式匹配程序

注释 配置 protected_content 关键字时，这些选项不可用。

快速模式匹配程序快速确定在将数据包传递到规则引擎之前要对哪些规则进行评估。这项初步工作可大大减少用于数据包评估的规则数量，从而提高性能。

默认情况下，快速模式匹配程序会在数据包内搜索规则中指定的最长内容；这样可最大程度地消除不必要的规则评估。以如下规则片段为例：

```
alert tcp any any -> any 80 (msg:"Exploit"; content:"GET";
http_method; nocase; content:"/exploit.cgi"; http_uri;
nocase;)
```

几乎所有 HTTP 客户端请求都包含内容 GET，但是很少会包含内容 /exploit.cgi。使用 GET 作为快速模式内容将会导致规则引擎在大多数情况下评估此规则，但极少会产生匹配。但是，对于大多数客户端 GET 请求，将不会使用 /exploit.cgi 对其进行评估，从而提高性能。

规则引擎仅在快速模式匹配程序检测到指定内容时根据规则评估数据包。例如，如果某个规则中的三个 content 关键字分别指定内容 short、longer 和 longest，快速模式匹配程序将使用内容 longest，并且仅在规则引擎在负载中找到 longest 的情况下对该规则进行评估。

content 关键字快速模式匹配程序参数

Use Fast Pattern Matcher

使用此选项可指定较短的搜索模式以供快速模式匹配程序使用。理想情况下，指定的模式在数据包中被找到的可能性低于最长模式，因此，因此能够更具体地识别所针对的漏洞。

在同一个 content 关键字中选择**使用快速模式匹配程序 (Use Fast Pattern Matcher)** 和其他选项时，请注意以下限制：

- 只能为每个规则指定一次**使用快速模式匹配程序 (Use Fast Pattern Matcher)**。
- 如果同时选择**使用快速模式匹配程序 (Use Fast Pattern Matcher)** 和**不匹配 (Not)**，将不能使用**距离 (Distance)**、**范围内 (Within)**、**偏移 (Offset)** 和**深度 (Depth)**。
- 不能同时选择“快速模式匹配程序”(Use Fast Pattern Matcher) 和以下任何 HTTP 字段选项：

  HTTP 原始 URI (HTTP Raw URI)、**HTTP 原始报头 (HTTP Raw Header)**、**HTTP 原始 Cookie (HTTP Raw Cookie)**、**HTTP Cookie**、**HTTP 方法 (HTTP Method)**、**HTTP 状态消息 (HTTP Status Message)** 或 **HTTP 状态代码 (HTTP Status Code)**

  但是，可以在也使用快速模式匹配程序搜索以下其中一个规范化字段的 content 关键字中包含上述选项：

  HTTP URI、**HTTP 报头 (HTTP Header)** 或 **HTTP 客户端正文 (HTTP Client Body)**

  例如，如果选择 **HTTP Cookie**、**HTTP 报头 (HTTP Header)** 和 **使用快速模式匹配程序 (Use Fast Pattern Matcher)**，规则引擎将会在 HTTP cookie 和 HTTP 报头中搜索内容，但快速模式匹配程序仅适用于 HTTP 报头，而不适用于 HTTP cookie。

请注意，不能在同一个 content 关键字中同时使用原始 HTTP 字段选项（**HTTP 原始 URI [HTTP Raw URI]**、**HTTP 原始报头 [HTTP Raw Header]** 或 **HTTP 原始 Cookie [HTTP Raw Cookie]**）及其对应的规范化选项（分别是 **HTTP URI**、**HTTP 报头 [HTTP Header]** 或 **HTTP Cookie**）。

如果将受限选项和不受限选项结合使用，快速模式匹配程序将仅搜索您指定的不受限字段，以测试是否要将数据包传递到规则引擎以完成评估（包括受限字段的评估）。

- 或者，如果选择**使用快速模式匹配程序 (Use Fast Pattern Matcher)**，还可以选择**仅快速模式匹配程序 (Fast Pattern Matcher Only)** 或**快速模式匹配程序偏移和长度 (Fast Pattern Matcher Offset and Length)** 选项，但不能同时选择这两个选项。
- 检测 Base64 数据时，不能使用快速模式匹配程序。

Fast Pattern Matcher Only

通过此选项，您可以将 content 关键字仅用作快速模式匹配程序选项，而不用作规则选项。如果无需规则引擎评估指定的内容，可以使用此选项来节省资源。例如，假设规则仅要求内容 12345 位于负载中的任何位置。如果快速模式匹配程序检测到该模式，可根据规则中的其他关键字对数据包进行评估。规则引擎无需重新评估数据包来确定其是否包含模式 12345。

如果规则包含其他与指定内容相关的状况，无需使用此选项。例如，如果另一个规则条件尝试确定 abcd 是否出现在 1234 之前，将无需使用此项选项搜索内容 1234。在这种情况下，规则引擎无法确定相对位置，因为选择**仅快速模式匹配程序 (Fast Pattern Matcher Only)** 将会指示规则引擎不搜索指定内容。

使用此选项时请注意以下情况：

- 指定的内容与位置无关，也就是说，该内容可出现在负载中的任何位置；因此，不能使用位置选项（**距离 [Distance]**、**范围内 [Within]**、**偏移 [Offset]**、**深度 [Depth]** 或**快速模式匹配程序偏移和长度 [Fast Pattern Matcher Offset and Length]**）。
- 不能将此选项与**不匹配 (Not)** 结合使用。
- 不能将此选项与**快速模式匹配程序偏移和长度 (Fast Pattern Matcher Offset and Length)** 结合使用。
- 指定的内容将被视为不区分大小写，因为所有模式均以不区分大小写的方式插入到快速模式匹配程序中；系统会自动处理这种情况，因此您无需在选择此选项时选择**不区分大小写 (Case Insensitive)**。
- 不可在使用**仅快速模式匹配程序**选项的 content 关键字后紧接着使用以下关键字（这些关键字设置相对于当前搜索位置的搜索位置）：
  - isdataat
  - pcre
  - content（在选择了**距离 [Distance]** 或**范围内 [Within]** 的情况下）
  - content（在选择了 **HTTP URI** 的情况下）
  - asn1

- byte_jump
- byte_test
- byte_math
- byte_extract
- base64_decode

Fast Pattern Matcher Offset and Length

使用**快速模式匹配程序偏移和长度 (Fast Pattern Matcher Offset and Length)** 选项可指定要搜索的部分内容。如果模式很长，且只需模式的一部分即足以识别出可能是匹配的规则，使用此选项可减少内存消耗。如果快速模式匹配程序选择了某个规则，将会根据该规则评估整个模式。

可以确定快速模式匹配程序要使用的部分，方法是，使用以下语法以字节为单位指定搜索的开始位置（偏移）以及搜索内容的深入度（长度）：

```
offset,length
```

例如，对于以下内容：

```
1234567
```

如果如下指定偏移量和长度字节数：

```
1,5
```

快速模式匹配程序仅搜索内容 `23456`。

请注意，不能将此选项与 **Fast Pattern Matcher Only** 结合使用。

相关主题

概述：HTTP content 和 protected_content 关键字参数，第 1521 页
base64_decode 和 base64_data 关键字，第 1605 页

replace 关键字

可以在内联部署中使用 `replace` 关键字替换指定内容或替换思科 SSL 设备检测到的 SSL 流量中的内容。

要使用 `replace` 关键字，请构建一个使用 `content` 关键字来查找特定字符串的自定义标准文本规则。然后使用 `replace` 关键字指定一个字符串，以替换该内容。替代值和内容值必须是相同长度的字符串。

注释 不能使用 `replace` 关键字替换 `protected_content` 关键字中的散列内容。

或者，可以用引号将替代字符串引起来，以便向后兼容以前的 Firepower 系统 软件版本。如果不加引号，替代字符串将被自动添加到规则，以使规则在语法上正确。要将前引号或后引号纳入为替代文本的一部分，必须使用反斜杠对引号进行转义，如以下示例所示：

```
"replacement text plus \"quotation\" marks""
```

每个规则可包含多个 `replace` 关键字，但只能包含一个 `content` 关键字。仅替代规则发现的内容中的第一个实例。

下面介绍 `replace` 关键字的使用示例：

- 如果系统检测到传入数据包包含漏洞，您可以使用一个无害字符串来替换该恶意字符串。有时，这种方法比单纯地丢弃违规数据包更有效。在某些攻击场景中，攻击者只需重新发送被丢弃的数据包，直至该数据包绕过网络防御或对网络造成泛洪攻击。通过用一个字符串替换另一个字符串，而不是丢弃数据包，可以哄骗攻击者认为已发动针对不易受攻击的目标的攻击。
- 如果您担心侦测攻击试图了解您是否正在运行易受攻击的 Web 服务器版本（示例），可以检测传出的数据包，并将横幅替换为自己的文本。

注释 请确保在要其中使用替换规则的内联入侵规则中将规则状态设置为“生成事件”(Generate Events)；如果将规则设置为“丢弃并生成事件”(Drop and Generate Events)，将会导致数据包被丢弃，进而造成无法替换内容。

在替换字符串的过程中，系统会自动更新数据包校验和，以便目标主机可准确收到该数据包。

请注意，不能将 `replace` 关键字与 HTTP 请求消息的 `content` 关键字选项结合使用。

相关主题

content 和 protected_content 关键字，第 1516 页
概述：HTTP content 和 protected_content 关键字参数，第 1521 页

byte_jump 关键字

`byte_jump` 关键字首先计算指定字节段中定义的字节数，然后在数据包中跳过该数量的字节 - 可以从指定字节段的末尾向前跳，也可以从数据包负载起点或末尾向前跳，还可以从与上一次内容匹配有关的点向前跳，具体取决于指定的选项。这对于具有如下特点的数据包很有用：数据包中的特定字节段说明数据包内变量数据包含的字节数。

下表介绍了 `byte_jump` 关键字所需的参数。

表 *120:* 所需的 *byte_jump* 参数

参数	说明
字节	要从数据包采集的字节数量。 如果不与 DCE/RPC 一起使用，则允许的值为 0 - 10，具有以下限制： • 如果与 `From End` 参数一起使用，则字节数可以是 0。如果 Bytes 为 0，则提取的值为 0。 • 如果指定除 1、2 或 4 以外的字节数，则必须指定数字类型（十六进制、八进制或十进制。） 如果与 DCE/RPC 一起使用，则允许的值为 1、2 和 4。
Offset	从负载开头到开始进行处理之间的字节数。`Offset` 计数器从字节 0 开始计数，因此，应该如下计算 `Offset` 值：用从数据包负载起点或上一次成功内容匹配起向前跳所需的字节数减去 1。 可指定 -65535 到 65535 字节。 您也可以使用现有 `byte_extract` 变量或 `byte_math` 结果指定此参数的值。

下表介绍了可用于定义系统如何解释您为必需参数指定的值的选项。

表 *121:* 其他可选 *byte_jump* 参数

参数	说明
Relative	使偏移量相对于上一次成功内容匹配中找到的上一个模式。
调整	将转换的字节数四舍五入为下一个 32 位边界。
倍数	指明规则引擎应将其与从数据包获取的 `byte_jump` 值相乘的值，以获得最终的 `byte_jump` 值。 也就是说，规则引擎跳过一个与您通过 Multiplier 参数指定的整数相乘的字节数，而不是跳过指定字节段中定义的字节数。
Post Jump Offset	应用其他 `byte_jump` 参数后要向前跳或向后跳的字节数（-65535 到 65535）。选择正值将会向前跳，选择负值将会向后跳。将此字段留空或输入 `0` 将会禁用此字段。 请注意，选择 **DCE/RPC** 参数时，一些 `byte_jump` 参数不适用。
From Beginning	指明规则引擎应从数据包负载起点开始跳过负载中指定的字节数，而不是从数据包的当前位置开始跳。
From End	跳转将从缓冲区最后一个字节后面的字节开始。

参数	说明
Bitmask	将使用 AND 运算符的指定十六进制位掩码应用于从 Bytes 参数提取的字节数。 位掩码可以是 1 到 4 个字节。 结果将按与掩码中的末尾零的数量相等的位数向右位移。

只能指定 **DCE/RPC**、**Endian** 或 **Number Type**。

如果要定义 `byte_jump` 关键字如何计算字节数，则可以选择下表中介绍的参数。如果未选择字节排序参数，规则引擎使用大端字节顺序。

表 *122:* 字节排序 *byte_jump* 参数

参数	说明
大端字节	按大端字节顺序处理数据（大端字节顺序是默认的网络字节顺序）。
小端字节	按小端字节顺序处理数据
DCE/RPC	为 DCE/RPC 预处理器处理的流量指定 `byte_jump` 关键字。 由 DCE/RPC 预处理器确定大端字节顺序或小端字节顺序，**Number Type** 和 **Endian** 参数不适用。 如果启用此参数，还可以将 `byte_jump` 与其他特定 DCE/RPC 关键字结合使用。

使用下表所列的其中一个参数来定义系统如何查看数据包中的字符串。

表 *123:* 数字类型参数

参数	说明
十六进制字符串	使用十六进制格式表示转换的字符串数据。
Decimal String	使用十进制格式表示转换的字符串数据。
Octal String	使用八进制格式表示转换的字符串数据。

例如，如果为 `byte_jump` 设置的值如下：

- Bytes = 4
- Offset = 12
- Relative 已启用
- Align 已启用

规则引擎将会计算自上一次成功内容匹配后显示的 13 个字节当中 4 个字节中描述的数量，并在数据包中向前跳过该数量的字节。例如，如果特定数据包中计算出的 4 个字节是 `00 00 00 1F`，规则引擎

会将它转换为 31。由于指定了 `Align`（指示引擎移到下一个 32 位边界），因此，规则引擎将在数据包中向前跳过 32 个字节。

或者，如果为 `byte_jump` 设置的值如下：

- Bytes = 4
- Offset = 12
- From Beginning 已启用
- Multiplier = 2

规则引擎将会计算在数据包起点后显示的 13 个字节当中 4 个字节中描述的数值。然后，引擎会将该数值乘以 2，以获得将要跳过的字节总数。例如，如果特定数据包中计算出的 4 个字节是 `00 00 00 1F`，规则引擎会将它转换为 31，然后再乘以 2 得到 62。由于启用了 From Beginning，因此，规则引擎会跳过数据包中的前 63 个字节。

相关主题

byte_extract 关键字，第 1533 页
DCE/RPC 关键字，第 1565 页

byte_test 关键字

`byte_test` 关键字根据 Value 参数及其运算符测试指定的字节段。

下表介绍了 `byte_test` 关键字所需的参数。

表 *124:* 所需的 *byte_test* 参数

参数	说明
字节	从数据包进行计算的字节数。 如果不与 DCE/RPC 配合使用，则允许的值为 1 到 10。但是，如果指定除 1、2 或 4 以外的字节数，则必须指定数字类型（十六进制、八进制或十进制。） 如果与 DCE/RPC 一起使用，则允许的值为 1、2 和 4。
值	要测试的值，包括其运算符。 支持的运算符：<、>、=、!、&、^、!>、!<、!=、!& 或 !^。 例如，如果指定 `!1024`，`byte_test` 将会转换该指定数字，且如果该数字不等于 1024，则会生成事件（如果其他所有关键字参数都匹配）。 请注意，! 和 != 等效。 您也可以使用现有 `byte_extract` 变量或 `byte_math` 结果指定此参数的值。

参数	说明
Offset	从负载开头到开始进行处理之间的字节数。偏移量计数器从字节 0 开始计数，因此，应该如下计算 offset 值：用从数据包负载起点或上一次成功内容匹配起向前计算所需的字节数减去 1。 可以使用现有 byte_extract 变量或 byte_math 结果指定此参数的值。

可以用下表中所述的参数进一步定义系统如何使用 byte_test 参数。

表 *125:* 其他可选 *byte_test* 参数

参数	说明
Bitmask	将使用 AND 运算符的指定十六进制位掩码应用于从 Bytes 参数提取的字节数。 位掩码可以是 1 到 4 个字节。 结果将按与掩码中的末尾零的数量相等的位数向右位移。
Relative	使偏移量相对于上一次成功模式匹配。

只能指定 **DCE/RPC**、**字节存储次序 (Endian)** 或**数字类型 (Number Type)**。

要定义 byte_test 关键字如何计算其测试的字节，请从下表中选择参数。如果未选择字节排序参数，规则引擎使用大端字节顺序。

表 *126:* 字节排序 *byte_test* 参数

参数	说明
大端字节	按大端字节顺序处理数据（大端字节顺序是默认的网络字节顺序）。
小端字节	按小端字节顺序处理数据
DCE/RPC	指定 DCE/RPC 预处理器处理的流量的 byte_test 关键字。 由 DCE/RPC 预处理器确定大端字节顺序或小端字节顺序，**Number Type** 和 **Endian** 参数不适用。 如果启用此参数，还可以将 byte_test 与其他特定 DCE/RPC 关键字结合使用。

可以使用下表所列的其中一个参数来定义系统如何在数据包中查看字符串。

表 *127:* 数字类型 *byte-test* 参数

参数	说明
十六进制字符串	使用十六进制格式表示转换的字符串数据。
Decimal String	使用十进制格式表示转换的字符串数据。

参数	说明
Octal String	使用八进制格式表示转换的字符串数据。

例如，如果如下指定 `byte_test` 的值：

- Bytes = 4
- Operator and Value > 128
- Offset = 8
- Relative 已启用

规则引擎计算距离（相对于）上一个成功的内容匹配项 9 个字节的 4 个字节中描述的数值，如果计算的数值大于 128 字节，则会触发规则。

相关主题

byte_extract 关键字，第 1533 页
DCE/RPC 关键字，第 1565 页

byte_extract 关键字

可以使用 `byte_extract` 关键字将数据包中指定数量的字节读取到某个变量中。然后，可以在同一规则中使用该变量作为某些其他检测关键字中特定参数的值。

此参数很有用，例如，可用于从其中的特定字节段描述数据包数据所包含的字节数的数据包提取数据大小。例如，特定字节段可能指出后续数据是由 4 个字节组成；您可以提取 4 个字节的数据大小来作为变量值。

可以使用 `byte_extract` 在一条规则中同时创建多达两个独立变量。可以任意多次地重新定义 `byte_extract` 变量；如果输入变量名称相同但变量定义不同的新的 `byte_extract` 关键字，它将覆盖该变量的上一个定义。

下表介绍 `byte_extract` 关键字所需的参数。

表 128: 所需的 byte_extract 参数

参数	说明
要提取的字节数	要从数据包采集的字节数量。 如果指定除 1、2 或 4 以外的字节数，则必须指定数字类型（十六进制、八进制或十进制。）

参数	说明
偏移	从负载开头到开始提取数据之间的字节数。可指定 -65535 到 65535 字节。偏移量计数器从字节 0 开始计数，因此，计算偏移量值时，应该用向前计算所需的字节数减去 1。例如，指定 7 将会从 8 字节开始向前计算。规则引擎会从数据包负载起点开始向前计算；如果还指定了 **Relative**，规则引擎则会从上一次内容成功匹配后开始向前计算。请注意，如果还指定了 **Relative**，则只能指定负数。 可以使用现有 byte_math 结果来指定此参数的值。
变量名称	用于其他检测关键字的参数中的变量名称。可以指定字母数字字符串，但必须以字母开头。

要进一步定义系统如何查找要提取的数据，可以使用下表中所述的参数。

表 *129:* 其他可选的 *byte_extract* 参数

参数	说明
Multiplier	从数据包提取的值的乘数。可指定 0 到 65535 之间的任意数字。如果未指定乘数，系统将使用默认值 1。
调整	将提取的数值四舍五入为最接近的 2 字节或 4 字节边界。如果也选择了**乘数**，系统会在进行舍入之前应用该乘数。
相对	使**偏移**相对于上一次内容成功匹配的结尾而不是负载起点。
位掩码	使用 AND 运算符将指定的十六进制位掩码应用于从 Bytes to Extract 参数提取的字节。 位掩码可以是 1 到 4 个字节。 结果将按与掩码中的末尾零的数量相等的位数向右位移。

只能指定 **DCE/RPC**、**Endian** 或 **Number Type**。

要定义 byte_extract 关键字如何计算其测试的字节数，可以从下表中选择参数。如果未选择字节排序参数，规则引擎使用大端字节顺序。

表 *130:* 字节排序 *byte_extract* 参数

参数	说明
大端字节	按大端字节顺序处理数据（大端字节顺序是默认的网络字节顺序）。
小端字节	按小端字节顺序处理数据

参数	说明
DCE/RPC	为 DCE/RPC 预处理器处理的流量指定 byte_extract 关键字。 由 DCE/RPC 预处理器确定大端字节顺序或小端字节顺序，**数字类型 (Number Type)** 和**字节存储次序 (Endian)** 参数不适用。 如果启用此参数，还可以将 byte_extract 与其他特定 DCE/RPC 关键字结合使用。

可以指定数字类型来将数据读取为 ASCII 字符串。要定义系统如何在数据包中查看字符串，可选择下表中所述的其中一个参数。

表 *131:* 数字类型 *byte_extract* 参数

参数	说明
十六进制字符串	以十六进制格式读取提取的字符串数据。
十进制字符串	以十进制格式读取提取的字符串数据。
八进制字符串	以八进制格式读取提取的字符串数据。

例如，如果为 byte_extract 指定如下值：

- Bytes to Extract = 4
- Variable Name = var
- Offset = 8
- Relative = enabled

那么，规则引擎会将距离（相对于）上一次内容成功匹配 9 字节的四个字节中描述的数字读取到名为 var 的变量中（然后，您可以在规则中将该数字指定为某些关键字参数的值）。

下表列出了可以在其中指定 byte_extract 关键字中定义的变量的关键字参数。

表 *132:* 接受 *byte_extract* 变量的参数

关键字	参数
content	Depth、Offset、Distance、Within
byte_jump	Offset
byte_test	Offset、Value
byte_math	RValue、Offset
isdataat	Offset

相关主题

DCE/RPC 预处理器，第 2068 页
DCE/RPC 关键字，第 1565 页
基本 content 和 protected_content 关键字参数，第 1517 页
byte_jump 关键字，第 1528 页
byte_test 关键字，第 1531 页
数据包特征，第 1588 页

byte_math 关键字

byte_math 关键字对提取的值和指定值或现有变量执行数学运算，并将结果存储在生成的新变量中。然后，可以使用生成的变量作为其他关键字中的参数。

您可以在规则中使用多个 byte_math 关键字执行多个 byte_math 运算。

下表介绍 byte_math 关键字所需的参数。

表 133: 所需的 *byte_math* 参数

参数	说明
字节	从数据包进行计算的字节数。 如果不与 DCE/RPC 配合使用，则允许的值为 1 到 10： • 当运算符为 +、-、* 或 / 时，Bytes 可以为 1 到 10。 • 当运算符为 << 或 >> 时，Bytes 可以为 1 到 4。 • 如果指定除 1、2 或 4 以外的字节数，则必须指定数字类型（十六进制、八进制或十进制。） 如果与 DCE/RPC 一起使用，则允许的值为 1、2 和 4。
Offset	从负载开头到开始进行处理之间的字节数。offset 计数器在字节 0 处启动，因此请按如下计算 offset 值：将要从数据包负载的开头或（如果指定 Relative）从上次成功内容匹配处向前跳转的字节数减 1。 可指定 -65535 到 65535 字节。 您还可以在此处指定 byte_extract 变量。
运算符	+、-、*、/、<< 或 >>
RValue	运算符后面的值。这可以是从 byte_extract 传递的无符号证书或变量。

参数	说明
Result Variable	byte_math 计算的结果将存储到的变量的名称。可以使用此变量作为其他关键字中的参数。 此值存储为无符号整数。 此变量名称： • 必须使用字母数字字符 • 不得以数字开头 • 可能包含 Microsoft 文件名/变量名称约定支持的特殊字符 • 不能完全由特殊字符组成

下表介绍了可用于定义系统如何解释您为必需参数指定的值的选项。

表 *134:* 其他可选 *byte_math* 参数

参数	说明
Relative	使偏移相对于在上次成功内容匹配中找到的最后一个模式而不是负载开头。
Bitmask	将使用 AND 运算符的指定十六进制位掩码应用于从 Bytes 参数提取的字节数。 位掩码可以是 1 到 4 个字节。 结果将按与掩码中的末尾零的数量相等的位数向右位移。

只能指定 **DCE/RPC**、**Endian** 或 **Number Type**。

如果要定义 byte_math 关键字如何计算字节数，则可以选择下表中介绍的参数。如果未选择字节排序参数，规则引擎使用大端字节顺序。

表 *135:* 字节排序 *byte_math* 参数

参数	说明
大端字节	按大端字节顺序处理数据（大端字节顺序是默认的网络字节顺序）。
小端字节	按小端字节顺序处理数据
DCE/RPC	为 DCE/RPC 预处理器处理的流量指定 byte_math 关键字。 由 DCE/RPC 预处理器确定大端字节顺序或小端字节顺序，**Number Type** 和 **Endian** 参数不适用。 当启用此参数时，还可以将 byte_math 与其他特定 DCE/RPC 关键字结合使用。

使用下表所列的其中一个参数来定义系统如何查看数据包中的字符串。

表 *136:* 数字类型参数

参数	说明
十六进制字符串	表示十六进制格式的字符串数据。
Decimal String	表示十进制格式的字符串数据。
Octal String	表示八进制格式的字符串数据。

例如，如果为 `byte_math` 设置的值如下：

- Bytes = 2
- Offset = 0
- Operator = *
- RValue = height
- Result Variable = area

规则引擎提取数据包中前两个字节中描述的数值，并将其乘以 RValue（使用现有变量 `height`）来创建新变量 `area`。

表 *137:* 接受 *byte_math* 变量的参数

关键字	参数
byte_jump	Offset
byte_test	Offset、Value
byte_extract	Offset
isdataat	Offset

概述：pcre 关键字

`pcre` 关键字使您可以使用兼容 Perl 的正则表达式 (PCRE) 为指定的内容检查数据包负载。使用 PCRE 可避免编写以匹配相同内容的细微变化为目的的多个规则。

搜索可以多种方式显示的内容时，正则表达式很有用。内容可能有不同的属性；在尝试从数据包负载中查找内容时，您会需要考虑其属性。

请注意，入侵规则使用的正则表达式语法是完整正则表达式库的一个子集，并且该库中所用命令的语法在某些方面存在不同之处。使用入侵规则编辑器添加 `pcre` 关键字时，请按以下格式输入完整值：

```
!/pcre/ ismxAEGRBUIPHDMCKSY
```

其中：

- ! 是可选求反（如果要匹配与正则表达式不匹配的模式，请使用此求反）。
- /pcre/ 是兼容 Perl 的正则表达式。
- `ismxAEGRBUIPHDMCKSY` 是修饰符选项的任意组合。

另请注意，在 PCRE 中使用下表所列字符在数据包负载中搜索特定内容时，必须对这些字符进行转义，以使规则引擎能正确地解译这些字符。

表 *138:* 转义的 *PCRE* 字符

必须转义的字符...	使用反斜线...	或使用十六进制代码...
#（散列标记）	\#	\x23
;（分号）	\;	\x3B
|（竖线）	\\|	\x7C
:（冒号）	\:	\x3A

您还可以使用 `m?regex?`，其中 `?` 是除 / 以外的分隔符。如果需要在正则表达式中匹配一个正斜杠，但不想用一个反斜杠来进行转义，可能需要使用此分隔符。例如，可以使用 `m?`regex`?ismxAEGRBUIPHDMCKSY`，其中 regex 是兼容 Perl 的正则表达式，`ismxAEGRBUIPHDMCKSY` 是修饰符选项的任意组合。

提示 或者，可以用引号将兼容 Perl 的正则表达式引起来，例如，pcre_expression 或 “pcre_expression “。这一做法适合习惯使用旧版本的有经验的用户（旧版本要求必须用引号将正则表达式引起来）。在保存规则后显示该规则时，入侵规则编辑器不显示引号。

pcre 语法

`pcre` 关键字接受兼容 Perl 的正则表达式 (PCRE) 标准语法。以下各节介绍这种语法。

提示 尽管本节介绍可用于 PCRE 的基本语法，但您可能想要参阅专门关于 Perl 和 PCRE 的网上参考资料或书籍，以获取更多高级信息。

元字符

元字符是在正则表达式中具有特殊含义的原义字符。在正则表达式中使用元字符时，必须通过在元字符前添加一个反斜杠来对其进行“转义”。

下表举例说明可用于 PCRE 的元字符。

表 *139: PCRE* 元字符

元字符	说明 (Description)	示例
.	匹配除换行符以外的任何字符。如果将 s 用作修饰选项，还将匹配换行符。	abc. 匹配 abcd、abc1、abc# 等等。
*	匹配字符或表达式的零次或多次出现次数。	abc* 匹配 abc、abcc、abccc、abcccccc 等等。
?	匹配字符或表达式的零次或一次出现次数。	abc? 匹配 abc。
+	匹配字符或表达式的一次或多次出现次数。	abc+ 匹配 abc、abcc、abccc、abcccccc 等等。
()	组表达。	(abc)+ 匹配 abc、abcabc、abcabcabc 等等。
{}	为字符或表达式指定匹配项数限制。如果要设置下限和上限，请用逗号将下限和上限隔开。	a{4,6} 匹配 aaaa、aaaaa 或 aaaaaa。 (ab){2} 匹配 abab。
[]	允许定义字符类，并匹配字符集中包含的任意字符或字符组合。	[abc123] 匹配 a、b 或 c 等等。
^	匹配字符串开头的内容。如果在字符类中使用，也可用于否定。	^in 匹配 info 中的“in”，但不匹配 bin 中的“in”。 [^a] 匹配不包含 a 的任何内容。
$	匹配字符串结尾的内容。	ce$ 匹配 announce 中的“ce”，但不匹配 cent 中的“ce”。
|	指示 OR 表达式。	(MAILTO|HELP) 匹配 MAILTO 或 HELP。
\	元字符可用作实际字符，还可用于指定预定义的字符类。	\. 匹配句号，* 匹配星号，\\ 匹配反斜线，依此类推。\d匹配数字字符，\w匹配字母数字字符，依此类推。

字符类

字符类包括字母字符、数字字符、字母数字字符和空白字符。可以用方括号创建自己的字符类，也可以使用预定义类作为不同字符类型的快捷方式。如果不与其他限定符配合使用，一个字符类通常匹配一个数字或字符。

下表举例说明 PCRE 接受的预定义字符类。

表 *140: PCRE* 字符类

字符类	说明	字符类定义
\d	匹配数字字符（“数字”）。	[0-9]
\D	对应不是数字字符的任何字符。	[^0-9]
\w	匹配字母数字字符（“单词”）。	[a-zA-Z0-9_]

字符类	说明	字符类定义
\W	匹配不是字母数字字符的任何字符。	[^a-zA-Z0-9_]
\s	匹配空白字符，包括空格、回车符、制表符、换行符和换页符。	[\r\t\n\f]
\S	匹配不是空白字符的任何字符。	[^ \r\t\n\f]

pcre 修饰符选项

指定 pcre 关键字值中的正则表达式语法后，可以使用修饰选项。这些修饰符执行特定于 Perl、PCRE 和 Snort 的处理功能。修饰符始终按以下格式显示在 PCRE 值的末尾：

```
/pcre/ismxAEGRBUIPHDMCKSY
```

其中，ismxAEGRBUPHMC 可以包括下表中的任何修饰选项。

提示 或者，可以用引号将正则表达式和任何修饰选项引起来，例如“/pcre/ismxAEGRBUIPHDMCKSY”。这一做法适合习惯使用旧版本的有经验的用户（旧版本要求必须用引号将正则表达式引起来）。在保存规则后显示该规则时，入侵规则编辑器不显示引号。

下表介绍了可用于执行 Perl 处理功能的选项。

表 *141: Perl* 相关的后正则表达式选项

选项	说明
i	使正则表达式不区分大小写。
s	点字符 (.) 匹配除换行符和 \n 字符以外的所有字符。可使用 "s" 选项覆盖此选项，这样点字符将匹配所有字符（包括换行符）。
m	默认情况下，一个字符串被视为单行字符，^ 和 $ 分别匹配特定字符串的开头和结尾。如果使用 "m" 代替选项，^ 和 $ 将匹配紧接在缓冲区内所有换行符之前或之后的内容，以及位于缓冲区开头或结尾的内容。
x	忽略可能在这一模式中出现的空格数据字符，除非其为转义字符（前面加有反斜线）或包含在字符类中。

下表介绍了可用于正则表达式之后的 PCRE 修饰符。

表 *142: PCRE* 相关的后正则表达式选项

选项	说明
A	模式必须在字符串开头进行匹配（与在正则表达式中使用 ^ 具有相同的效果）。

选项	说明
E	将 $ 设置为只在目标字符串结尾进行匹配。（如果最后一个字符是换行符，即使没有 E，$ 也会匹配紧接在该字符之前的内容，但不会匹配任何其他换行符之前的内容）。
G	默认情况下，* + 和 ? 是“贪婪”的，这意味着，如果找到两个或更多匹配项，将会选择最长的匹配项。使用 G 字符可使这些字符在后面无问号字符 (?) 的情况下总是选择第一个匹配项。例如，在使用 G 修饰符的构造中，*? +? 和 ?? 将是贪婪字符，而 *、+ 或 ? 在不附带问号的情况下不是贪婪字符。

下表介绍了可用于正则表达式后的 Snort 特定修饰符。

.

表 *143:* 特定于 *Snort* 的后正则表达式修饰符

选项	说明
R	相对于规则引擎上一次找到的匹配项的结尾搜索匹配的内容。
B	在未被预处理器解码的数据中搜索内容（此选项类似于使用带有 content 或 protected_content 关键字的 Raw Data 参数）。
U	在已由 HTTP 检查预处理器解码的规范化 HTTP 请求消息的 URI 中搜索内容。请注意，不能将此选项与 content 或 protected_content 关键字的 **HTTP URI** 选项结合使用来搜索相同的内容。 请注意，管道化 HTTP 请求数据包包含多个 URI。包含 U 选项的 PCRE 表达式使规则引擎仅在管道化 HTTP 请求数据包的第一个 URI 中搜索内容匹配。要搜索数据包中的所有 URI，请使用已选择 **HTTP URI** 的 content 或 protected_content 关键字（可随附或不随附使用 U 选项的 PCRE 表达式）。
I	在已由 HTTP 检查预处理器解码的原始 HTTP 请求消息的 URI 中搜索内容。请注意，不能将此选项与 content 或 protected_content 关键字 **HTTP 原始 URI (HTTP Raw URI)** 选项结合使用来搜索相同的内容
P	在已由 HTTP 检查预处理器解码的规范化 HTTP 请求消息的正文中搜索内容。
H	在已由 HTTP 检查预处理器解码的 HTTP 请求或响应消息的报头（不包括 cookie）中搜索内容。请注意，不能将此选项与 content 或 protected_content 关键字 **HTTP Header** 选项结合使用来搜索相同的内容。
D	在已由 HTTP 检查预处理器解码的原始 HTTP 请求或响应消息的报头（不包括 cookie）中搜索内容。请注意，不能将此选项与 content 或 protected_content 关键字 **HTTP Raw Header** 选项结合使用来搜索相同的内容。
M	在已由 HTTP 检查预处理器解码的规范化 HTTP 请求消息的方法字段中搜索内容；该方法字段确定要对URI中识别出的资源执行的操作（例如，GET、PUT、CONNECT 等）。

选项	说明
选	如果 HTTP 检查预处理器的**检查 HTTP Cookie (Inspect HTTP Cookies)** 选项已启用，将会在 HTTP 请求报头的任何 cookie 中搜索规范化内容；如果该预处理器的**检查 HTTP 响应 (Inspect HTTP Responses)** 选项已启用，还会在 HTTP 响应报头的任何 set-cookie 中搜索规范化内容。如果未启用**检查 HTTP Cookie (Inspect HTTP Cookies)** 选项，将会搜索包括 cookie 或 set-cookie 数据在内的整个报头。 请注意以下提示： • 消息正文中包含的 cookie 将被视为正文内容。 • 不能将此选项与 `content` 或 `protected_content` 关键字 **HTTP Cookie** 选项结合使用来搜索相同的内容。 • `Cookie:` 和 `Set-Cookie:` 报头名称、标题行中的前导空格以及终止标题行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。
K	如果 HTTP 检查预处理器的**检查 HTTP Cookie (Inspect HTTP Cookies)** 选项已启用，将会在 HTTP 请求报头的任何 cookie 中搜索原始内容；如果该预处理器的**检查 HTTP 响应 (Inspect HTTP Responses)** 选项已启用，还会在 HTTP 响应报头的任何 set-cookie 中搜索原始内容。如果未启用**检查 HTTP Cookie (Inspect HTTP Cookies)** 选项，将会搜索包括 cookie 或 set-cookie 数据在内的整个报头。 请注意以下提示： • 消息正文中包含的 cookie 将被视为正文内容。 • 不能将此选项与 `content` 或 `protected_content` 关键字 **HTTP Raw Cookie** 选项结合使用来搜索相同的内容。 • `Cookie:` 和 `Set-Cookie:` 报头名称、标题行中的前导空格以及终止标题行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。
S	搜索 HTTP 响应中的三位数状态代码。
Y	搜索 HTTP 响应中状态代码随附的文字描述。

注释 请勿将U选项与R选项结合使用，否则可能会导致性能问题。此外，请勿将U选项与任何其他HTTP内容选项（I、P、H、D、M、C、K、S 或 Y）结合使用。

相关主题

概述：HTTP content 和 protected_content 关键字参数 ，第 1521 页

pcre 示例关键字值

以下示例显示可为 `pcre` 输入的值，并说明每个示例将会匹配的内容。

- **/feedback[(\d{0,1})]?\.cgi/U**

此示例搜索 feedback 的数据包负载，feedback 后面紧跟着零个或一个数字字符，再紧跟着 .cgi，且仅在 URI 数据中进行搜索。

此示例将匹配：

- feedback.cgi
- feedback1.cgi
- feedback2.cgi
- feedback3.cgi

此示例**不**匹配：

- feedbacka.cgi
- feedback11.cgi
- feedback21.cgi
- feedbackzb.cgi

- **/^ez(\w{3,5})\.cgi/iU**

此示例在字符串开头搜索 ez 的数据包负载，ez 后面跟有一个包含 3 到 5 个字母的单词，该单词后面跟着 .cgi。此搜索不区分大小写，且仅搜索 URI 数据。

此示例将匹配：

- EZBoard.cgi
- ezman.cgi
- ezadmin.cgi
- EZAdmin.cgi

此示例**不**匹配：

- ezez.cgi
- fez.cgi
- abcezboard.cgi
- ezboardman.cgi

- **/mail(file|seek)\.cgi/U**

此示例在 URI 数据中搜索后面跟有 file 或 seek 的 mail 的数据包负载。

此示例将匹配：

- `mailfile.cgi`
- `mailseek.cgi`

此示例不匹配：

- `MailFile.cgi`
- `mailfilefile.cgi`

- **`m?http\\x3a\x2f\x2f.*(\n|\t)+?U`**

此示例跟在任意数量字符后面的 HTTP 请求中为制表符或换行符搜索 URI 内容的数据包负载。此示例使用 `m?`regex`?` 以避免在表达式中使用 `http\:\/\/`。请注意，冒号前面有一个反斜线。

此示例将匹配：

- `http://www.example.com?scriptvar=x&othervar=\n\..\..`
- `http://www.example.com?scriptvar=\t`

此示例不匹配：

- `ftp://ftp.example.com?scriptvar=&othervar=\n\..\..`
- `http://www.example.com?scriptvar=|/bin/sh -i|`

- **`m?http\\x3a\x2f\x2f.*=\|.*\|+?sU`**

此示例为带有任意数量字符（包括换行符）的URL搜索数据包负载，后面跟有一个等号以及包含任意数量字符或空格的竖线。此示例使用 `m?`regex`?` 以避免在表达式中使用 `http\:\/\/`。

此示例将匹配：

- `http://www.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?input=|cat /etc/passwd|`

此示例不匹配：

- `ftp://ftp.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?value=x&input?|cat /etc/passwd|`

- **`/[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}/i`**

此示例为任何 MAC 地址搜索数据包负载。请注意，此示例使用反斜杠对冒号进行转义。

metadata 关键字

您可以使用 `metadata` 关键字向规则中添加自己的描述性信息。您还可以使用具有 `service` 参数的 `metadata` 关键字识别网络流量中的应用和端口。可以使用所添加的信息通过适合需求的方式组织或识别规则，并且可以搜索规则中所添加的信息和有关 `service` 参数的信息。

系统根据参数格式验证元数据：

key value

其中，*key* 和 *value* 提供以空格分隔的组合描述。这是Talos 情报小组 用于向思科提供的规则添加元数据的格式。

也可以使用其他格式：

key = value

例如，通过按如下方式使用类别和子类别，可以使用 *key value* 格式按作者和日期识别规则：

```
author SnortGuru_20050406
```

可以在规则中使用多个 `metadata` 关键字。还可以使用逗号分隔单个 `metadata` 关键字中的多个 *key value* 参数，如以下示例所示：

```
author SnortGuru_20050406, revised_by SnortUser1_20050707,
revised_by SnortUser2_20061003,
revised_by SnortUser1_20070123
```

并非只能使用 *key value* 或 *key=value* 格式；但是，应了解根据这些格式进行验证产生的局限性。

要避免的受限字符

请注意以下字符限制：

- 请勿使用分号 (;) 或冒号 (:)。
- 系统将逗号解释为多个 *key value* 或 *key=value* 参数的分隔符。例如：

  key value,*key value*,*key value*
- 系统将等于 (=) 字符或空格字符解释为 *key* 和 *value* 之间的分隔符。例如：

  key value

  key=value

允许使用所有其他字。

要避免的保留元数据

请避免在 `metadata` 关键字中使用以下单词作为单个参数或作为 *key value* 参数中的 *key*；这些单词保留供 Talos 使用：

```
application
engine
impact_flag
```

```
os
policy
rule-type
rule-flushing
soid
```

注释 如需有关将受限元数据添加到可能不具有预期作用的本地规则方面的帮助，请联系支持部门。

影响级别 1

可以在 `metadata` 关键字中使用以下保留的 *key value* 参数：

```
impact_flag red
```

此 *key value* 参数针对导入的本地规则或使用入侵规则编辑器创建的自定义规则将影响标志设置为红色（级别 1）。

请注意，当 Talos 在思科提供的规则中包含 `impact_flag red` 参数时，Talos 已确定触发该规则的数据包指示源主机或目标主机可能受病毒、特洛伊木马或其他恶意软件的损害。

服务元数据

系统检测在网络中的主机上运行的应用，并将应用协议信息插入网络流量中；无论如何配置发现策略，它都会执行此操作。您可以在 TCP 或 UDP 规则中使用 `metadata` 关键字 `service` 参数来匹配网络流量中的应用协议和端口。您可以在某个规则中组合一个或多个 `service` 应用参数与单个端口参数。

服务应用

可以使用带 `service` 的 `metadata` 关键字作为 *key*，并使用应用作为 *value*，以匹配具备已识别应用协议的数据包。例如，`metadata` 关键字中的以下 *key value* 参数会将规则与 HTTP 流量关联：

```
service http
```

可以识别多个以逗号分隔的应用。例如：

```
service http, service smtp, service ftp
```

注意 如配置自适应配置文件，第 2204 页中所述，**必须**为入侵规则启用（其默认状态）自适应分析，才能使用服务元数据。

下表介绍与 `service` 关键字配合使用的最常见应用值。

注释 如需有关识别表中未列出的应用方面的帮助，请联系支持部门。

表 *144: service* 值

值	说明
cvs	当前版本系统
dcerpc	分布式计算环境/远程过程调用系统
dns	域名系统
finger	Finger 用户信息协议
ftp	文件传输协议
ftp-data	文件传输协议（数据通道）
http	超文本传输协议
imap	互联网消息访问协议
isakmp	互联网安全关联和密钥管理协议
mysql	我的结构化查询语言
netbios-dgm	NetBIOS 数据报服务
netbios-ns	NetBIOS 名称服务
netbios-ssn	NETBIOS 会话服务
nntp	网络新闻传输协议
oracle	Oracle 网络服务
外壳	操作系统外壳
pop2	邮局协议第 2 版
pop3	邮局协议第 3 版
smtp	简单邮件传输协议
snmp	简单网络管理协议
ssh	安全外壳网络协议
sunrpc	Sun 远程过程调用协议
telnet	Telnet 网络协议
tftp	简单文件传输协议
x11	X Window 系统

服务端口

可以使用带 `service` 的 `metadata` 关键字作为 ***key***，并使用指定端口参数作为 ***value***，以定义规则如何与应用结合来匹配端口。

可以指定下表中的任何一个端口值，每条规则一个值。

表 *145: service* 端口值

值	说明
`else-ports` 或 `unknown`	如果符合以下任一条件，则系统将应用规则： • 数据包应用已知，且匹配规则应用。 • 数据包应用未知，且数据包端口匹配规则端口。 当 `service` 指定一个不含端口修饰符的应用协议时，`else-ports` 和 `unknown` 将产生系统使用的默认行为。
`and-ports`	如果数据包应用已知且匹配规则应用，则系统应用规则，并且数据包端口匹配规则报头中的端口。您无法在未指定应用的规则中使用 `and-ports`。
`or-ports`	如果符合以下任何条件，则系统将应用规则： • 数据包应用已知，且匹配规则应用。 • 数据包应用未知，且数据包端口匹配规则端口。 • 数据包应用不匹配规则应用，且数据包端口匹配规则端口。 • 规则未指定应用，且数据包端口匹配规则端口。

请注意以下提示：

- 必须包含带 `service and-ports` 参数的 `service` 应用参数。
- 如果某个规则指定上表中的多个值，则系统将应用该规则中最后出现的一个值。
- 端口和应用参数可以为任何顺序。

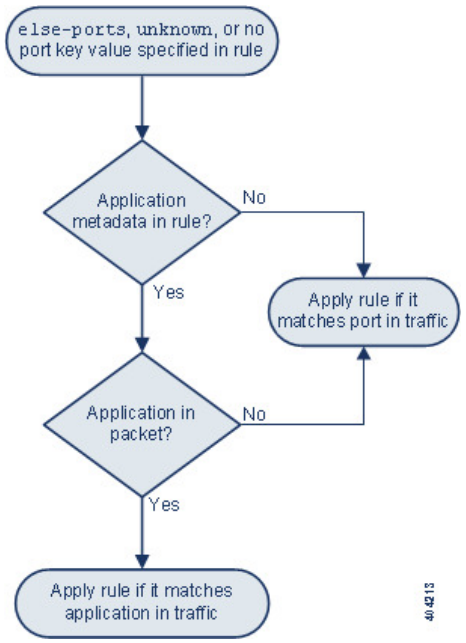
除了 `and-ports` 值，可以包含带或不带一个或多个 `service` 应用参数的 `service` 端口参数。例如：

```
service or-ports, service http, service smtp
```

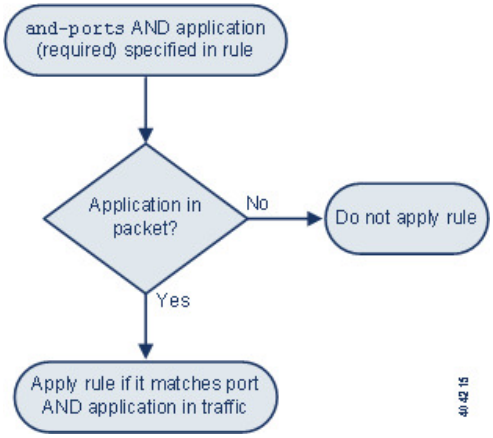
流量中的应用和端口

下图展示了入侵规则支持的应用和端口组合，以及将这些规则限制应用到数据包数据的结果。

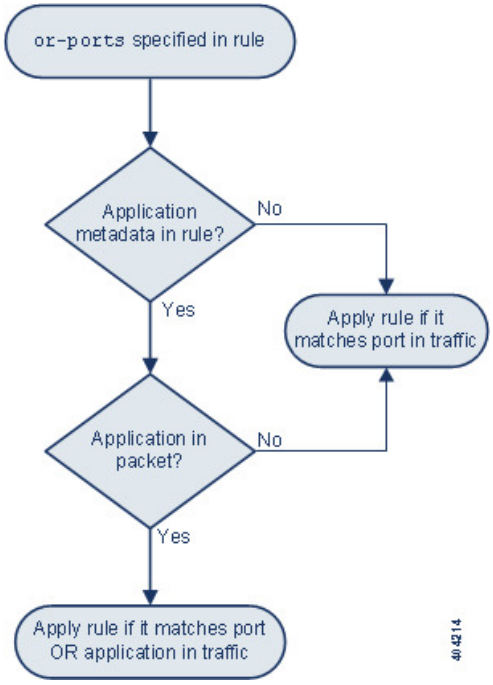
主机应用协议的其他源/目标端口：



主机应用协议和源/目标端口：



主机应用协议或源/目标端口：



示例匹配

以下规则示例使用带 `service` 参数的 `metadata` 关键字，与其匹配和不匹配的数据示例一同显示：

- `alert tcp any any -> any [80,8080] (metadata:service and-ports, service http, service smtp;)`

示例匹配	不匹配示例
• TCP 端口 80 上的 HTTP 流量 • TCP 端口 8080 上的 HTTP 流量 • TCP 端口 80 上的 SMTP 流量 • TCP 端口 8080 上的 SMTP 流量	• 端口 80 或 8080 的 POP3 流量 • 端口 80 或 8080 上的未知应用流量 • 端口 9999 上的 HTTP 流量

- `alert tcp any any -> any [80,8080] (metadata:service or-ports, service http;)`

示例匹配	不匹配示例
• 任意端口上的 HTTP 流量 • 端口 80 上的 SMTP 流量 • 端口 8080 上的 SMTP 流量 • 端口 80 和 8080 上的未知应用流量	• 除 80 或 8080 外的端口上的非 HTTP 和非 SMTP 流量

- 以下任何一规则：
  - `alert tcp any any -> any [80,8080] metadata:service else-ports, service http;)`
  - `alert tcp any any -> any [80,8080] metadata:service unknown, service http;)`
  - `alert tcp any any -> any [80,8080] metadata:service http;)`

示例匹配	不匹配示例
• 任意端口上的 HTTP 流量 • 如果数据包应用未知，则为端口80 • 如果数据包应用未知，则为端口8080	• 端口 80 或 8080 的 SMTP 流量 • 端口 80 或 8080 的 POP3 流量

元数据搜索准则

要搜索使用`metadata`关键字的规则，请在规则搜索页面上选择`metadata`关键字，或者键入元数据的任何部分。例如，可以键入：

- `search`，以显示在其中对 *key* 使用了 `search` 的所有规则。
- `search http`，以显示在其中对 *key* 使用了 `search` 并对 *value* 使用了 `http` 的所有规则。
- `author snortguru`，以显示在其中对 *key* 使用了 `author` 并对 *value* 使用了 `SnortGuru` 的所有规则。
- `author s`，以显示在其中为 *key* 使用了 `author` 并对 *value* 使用了任何词条（例如 `SnortGuru`、`SnortUser1` 或 `SnortUser2`）的所有规则。

提示 如果同时搜索 *key* 和 *value*，应在搜索中使用与规则的 *key value* 参数中使用的相同连接运算符（等号 [=] 或空格字符）；搜索将返回不同的结果，具体取决于 *key* 后面跟的是等号 (=) 还是空格字符。

请注意，无论使用何种格式添加元数据，系统都会将元数据搜索词解释为 *key value* 或 *key=value* 参数的全部或一部分。例如，以下是没有遵循 *key value* 或 *key=value* 格式的有效元数据：

```
ab cd ef gh
```

但是，系统会将此示例中的每个空格解释为 *key* 和 *value* 之间的分隔符。因此，对于并列和单个术语，可以使用以下任何搜索成功查找到包含元数据示例的规则：

```
cd ef
ef gh
ef
```

但是，使用以下搜索不会找到该规则（系统会将其解释为单个 *key value* 参数）：

```
ab ef
```

相关主题

搜索规则，第 1511 页

IP 报头值

可以使用关键字来识别数据包 IP 报头中可能存在的攻击或安全策略违规。

fragbits

`fragbits` 关键字检查 IP 报头中的分片和保留位。可以检查每个数据包的 Reserved 位、More Fragments 位和 Don't Fragment 位的任意组合。

表 *146: Fragbits* 参数值

参数	说明
R	“保留”位
M	“更多分片”位
D	“不分片”位

为进一步改进使用 `fragbits` 关键字的规则，可以在规则的参数值后指定下表中所述的任何运算符。

表 *147: Fragbit* 运算符

运算符	说明
加号 (**+**)	数据包必须匹配所有指定的位。
星号 (*****)	数据包可以匹配任何指定的位。
感叹号 (**!**)	如果未设置任何指定的位，数据包将符合条件。

例如，要生成有关设置了“保留”(Reserved) 位（还可能设置了任何其他位）的数据包的事件，请使用 `R+` 作为 `fragbits` 值。

id

`id` 关键字根据您在此关键字的参数中指定的值测试 IP 报头分片标识字段。某些拒绝服务工具和扫描工具将此字段设置为容易检测的特定数字。例如，在 SID 630（检测 Synscan 端口扫描）中，`id` 设置为 `39426`，这是在扫描仪传输的数据包中用作 ID 号的静态值。

注释 `id` 参数值必须为数字。

ipopts

使用 `IPopts` 关键字可在数据包中搜索指定的 IP 报头选项。下表列出了可用的参数值。

表 *148: IPoption* 参数

参数	说明
rr	记录路由
eol	列表结束
nop	无操作
ts	时间戳
秒	IP 安全选项
lsrr	松散源路由
ssrr	严格源路由
satid	数据流标识符

分析师最经常监视严格和松散源路由，因为这两个选项可能指出欺骗性源 IP 地址。

ip_proto

使用 `ip_proto` 关键字可识别使用指定为关键字值的 IP 协议的数据包。可以为 IP 协议指定 0 到 255 之间的数字。可以将这些协议号与以下运算符结合使用：`<`、`>` 或 `!`。例如，要检查使用非 ICMP 的任何协议的流量，请使用 `!1` 作为 `ip_proto` 关键字的值。也可以在一个规则中多次使用 `ip_proto` 关键字；但请注意，规则引擎会将此关键字的多个实例解释为具有布尔 AND 关系。例如，如果创建一个包含 `ip_proto:!3; ip_proto:!6` 的规则，该规则将忽略使用 GGP 协议和 TCP 协议的流量。

tos

有些网络使用服务类型 (ToS) 值设置在网络上传输的数据包的优先级。使用 `tos` 关键字可根据指定为该关键字的参数的值测试数据包的 IP 报头 ToS 值。对于其 ToS 已设置为指定值且符合规则中规定的其他条件的数据包，使用 `tos` 关键字的规则将会触发。

注释 `tos` 参数值必须为数字。

ToS 字段已在 IP 报头协议中弃用，取而代之的是“差分服务代码点 (DSCP)”(Differentiated Services Code Point [DSCP]) 字段。

ttl

数据包的生存时间 (ttl) 值指明数据包在被丢弃之前可以跳多少次。可以使用 `ttl` 关键字根据指定为关键字参数的值或值范围测试数据包的 IP 报头 ttl 值。将 `ttl` 关键字参数设置为较小的值（例如 0 或

1）可能会有帮助，因为小的生存时间值有时表示跟踪路由或入侵逃避行为。（但请注意，此关键字的相应值取决于受管设备的位置和网络拓扑。）使用以下语法：

- 将 TTL 值设置为 0 到 255 之间的整数。也可以该值前面加上一个等号 (=)（例如，可以指定 `5` 或 `=5`）。
- 使用连字符 (-) 指定 TTL 值的范围（例如，`0-2` 指定 0 到 2 之间的所有值，`-5` 指定 0 到 5 之间的所有值，`5-` 指定 5 到 255 之间的所有值）。
- 使用大于号 (>) 指定 TTL 值大于一个特定值（例如，`>3` 指定大于 3 的所有值）。
- 使用大于或等于号 (>=) 指定 TTL 值大于或等于一个特定值（例如，`>=3` 指定大于或等于 3 的所有值）。
- 使用小于号 (<) 指定 TTL 值小于一个特定值（例如，`<3` 指定小于 3 的所有值）。
- 使用小于或等于号 (<=) 指定 TTL 值小于或等于一个特定值（例如，`<=3` 指定小于或等于 3 的所有值）。

ICMP 报头值

Firepower 系统支持可用于识别 ICMP 数据包报头中的攻击和安全策略违规的关键字。但请注意，存在的预定义规则检测大多数 ICMP 类型和代码。可考虑启用现有规则或者根据现有规则创建本地规则；如果您从头开始构建 ICMP 规则，可能会更快找到符合您需求的规则。

icmp_id 和 icmp_seq

ICMP 识别号和序列号有助于将 ICMP 响应与 ICMP 请求关联起来。在正常流量中，这些值动态地分配给数据包。有些隐蔽通道和分布式拒绝服务 (DDoS) 程序使用静态 ICMP ID 和序列值。使用以下关键字可识别具有静态值的 ICMP 数据包。

关键字	Definition
icmp_id	检查 ICMP 回应请求或应答数据包的 ICMP ID 号。应使用对应于 ICMP ID 号的数值作为 `icmp_id` 关键字的参数。
icmp_seq	`icmp_seq` 关键字检查 ICMP 回应请求或应答数据包的 ICMP 序列。应使用对应于 ICMP 序列号的数值作为 `icmp_seq` 关键字的参数。

itype

使用 `itype` 关键字可查找具有特定 ICMP 消息类型值的数据包。您可以指定有效的 ICMP 类型值或无效的 ICMP 类型值来测试不同类型的流量。例如，攻击者可以将 ICMP 类型值设置为超出范围，从而导致拒绝服务和泛洪攻击。

可以使用小于号 (<) 和大于号 (>) 指定 `itype` 参数值的范围。

例如：

- <35

- >36
- 3<>55

icode

ICMP 消息有时包含代码值，用于在目标不可达的情况下提供有关详细信息。

您可以使用 `icode` 关键字来识别具有特定 ICMP 代码值的数据包。可以指定有效的 ICMP 代码值或无效的 ICMP 代码值来测试不同类型的流量。

可以使用小于号 (<) 和大于号 (>) 指定 `icode` 参数值的范围。

例如：

- 要查找小于 35 的值，请指定 `<35`。
- 要查找大于 36 的值，请指定 `>36`。
- 要查找 3 到 55 之间的值，请指定 `3<>55`。

提示 可以同时使用 `icode` 和 `itype` 关键字来识别与这两者都匹配的流量。例如，要识别包含“ICMP 目标不可达”(ICMP Destination Unreachable) 代码类型和“ICMP 端口不可达”(ICMP Port Unreachable) 代码类型的 ICMP 流量，请指定 3 作为 `itype` 关键字的值（用于“目标不可达”[Destination Unreachable] 类型），并指定 3 作为 `icode` 关键字的值（用于“端口不可达”[Port Unreachable] 类型）。

TCP 报头值和数据流大小

Firepower 系统支持专门用于使用数据包 TCP 报头和 TCP 数据流大小来识别尝试的攻击的关键字。

ack

可以使用 `ack` 关键字将某个值与数据包的 TCP 确认号进行比较。如果数据包的 TCP 确认号与为 `ack` 关键字指定的值相匹配，则会触发规则。

`ack` 参数值必须为数字。

标志

可以使用 `flags` 关键字指定 TCP 标志的任意组合，如果在已检查的数据包中设置此关键字，将触发规则。

注释 在使用 `A+` 作为 `flags` 的值的一般情况下，应转为使用具有 `established` 值的 `flow` 关键字。通常，如果使用标志以确保标志的所有组合均已检测到，应使用具有 `stateless` 值的 `flow` 关键字。

可以检查或忽略下表中所述的 flag 关键字的值。

表 *149: flag* 参数

参数	TCP 标志
Ack	确认数据。
Psh	数据应该在此数据包中发送。
Syn	新的连接。
Urg	包含紧急数据的数据包。
Fin	关闭的连接。
Rst	中止的连接。
CWR	ECN 堵塞窗口已减少。这以前是 R1 参数，仍支持向后兼容。
ECE	ECN 响应。这以前是 R2 参数，仍支持向后兼容。

使用 flags 关键字时，可以使用运算符来指示系统如何匹配多个标志。下表介绍了这些运算符。

表 *150:* 与 *flags* 配合使用的运算符

运算符	说明 (Description)	示例
all	数据包必须包含所有指定的标志。	选择 Urg 和 all 可规定数据包必须包含紧急标志，且可以包含任何其他标志。
any	数据包可包含任何指定的标志。	选择 Ack、Psh 和 any 可规定必须设置 Ack 和/或 Psh 标志才能触发规则，且也可以对数据包设置其他标志。
不	数据包**不得**包含指定的标志集。	选择 Urg 和 not 可规定**不**对会触发此规则的数据包设置紧急标志。

流

可以使用 flow 关键字选择由规则根据会话特征进行的检查的数据包。flow 关键字允许您指定规则应用的流量的方向，从而将规则应用于客户端流量或服务器流量。要指定 flow 关键字如何检查数据包，可以设置要分析的流量的方向、已检查的数据包的状态以及这些数据包是否是重建数据流的一部分。

数据包状态检测发生在规则处理之后。如果要使某个 TCP 规则忽略无状态流量（尚未建立会话情景的流量），必须将 flow 关键字添加到该规则，并为该关键字选择 **Established** 参数。如果要使某个 UDP 规则忽略无状态流量，必须将 flow 关键字添加到该规则，并选择 **Established** 参数和/或方向参数。这样，TCP 或 UDP 规则就会执行数据包状态检查。

如果添加方向参数，规则引擎将只检查具有已建立状态且流向与指定方向匹配的数据包。例如，如果将具有 `established` 参数和 `From Client` 参数的 `flow` 关键字添加到某个规则，且该规则会在检测到 TCP 或 UDP 连接的情况下触发，那么规则引擎将只检查从特定客户端发送的数据包。

提示 为了获得最佳性能，应始终在 TCP 规则或 UDP 会话规则中包含 `flow` 关键字。

下表介绍了可为 `flow` 关键字指定的数据流相关参数：

表 *151:* 状态相关的 *flow* 参数

参数	说明
Established	在已建立连接的情况下触发。
Stateless	无论数据流处理器的状态如何，都会触发。

下表介绍了可为 `flow` 关键字指定的方向选项：

表 *152: flow* 方向参数

参数	说明
到客户端	服务器响应时触发。
到服务器	客户端响应时触发。
自客户端	客户端响应时触发。
自服务器	服务器响应时触发。

请注意，`From Server` 和 `To Client` 执行相同的功能，`To Server` 和 `From Client` 执行相同的功能。这些选项是为了是规则具有上下文和可读性。例如，如果要创建用于检测从服务器向客户端发起的木马攻击的规则，应使用 `From Server`。但是，如果要创建用于检测从客户端向服务器发出的木马攻击的规则，应使用 `From Client`。

下表介绍了可为 `flow` 关键字指定的数据流相关参数：

表 *153:* 数据流相关的 *flow* 参数

参数	说明
忽略流流量	重建流数据包时不触发。
仅流流量	仅在重建流数据包时触发。

例如，可以使用 `To Server, Established, Only Stream Traffic` 作为 `flow` 关键字的值，这样将会检测在建立的会话中从客户端流向服务器并且由数据流预处理器重组的流量。

序列号

使用 `seq` 关键字可指定静态序列号值。序列号与指定参数相匹配的数据包将会触发包含此关键字的规则。虽然此关键字很少使用，但它有助于识别使用生成的具有静态序列号的数据包的攻击和网络扫描。

window

可以使用 `window` 关键字指定感兴趣的 TCP 窗口大小。包含此关键字的规则在遇到具有指定 TCP 窗口大小的数据包时，都会触发。虽然此关键字很少使用，但它有助于识别使用生成的具有静态 TCP 窗口大小的数据包的攻击和网络扫描。

stream_size

可以将 `stream_size` 关键字与数据流预处理器配合使用，以确定 TCP 数据流的大小（以字节为单位），具体格式如下：

```
direction,operator,bytes
```

其中，bytes 是字节数。必须以逗号 (,) 分隔参数中的每个选项。

下表介绍了可为 `stream_size` 关键字指定的不区分大小写的方向选项：

表 *154: stream_size* 关键字定向参数

参数	说明
客户端	当来自客户端的数据流与指定数据流大小相匹配时触发。
server	当来自服务器的数据流与指定数据流大小相匹配时触发。
both	当来自客户端和服务器的流量都与指定数据流大小相匹配时触发。 例如，如果来自客户端的流量大于 200 字节，且来自服务器的流量也大于 200 字节，参数 `both, >, 200` 将会触发。
either	当来自客户端或服务器流量与指定数据流大小相匹配时触发（无论哪一种情况先发生）。 例如，如果来自客户端的流量大于 200 字节，或来自服务器的流量大于 200 字节，参数 `either, >, 200` 将会触发。

下表介绍了可与 `stream_size` 关键字配合使用的运算符：

表 *155: stream_size* 关键字参数运算符

运算符	说明
=	等于
!=	不等于

运算符	说明
>	大于
<	小于
>=	大于或等于
<=	小于或等于

例如，可以使用 `client, >=, 5001216` 作为 `stream_size` 关键字的参数，以检测从客户端发往服务器的且大于或等于 5001216 字节的 TCP 数据流。

stream_reassembly 关键字

如果单个连接上的已检测流量与规则条件相匹配，则可以使用 `stream_reassemble` 关键字为该连接启用或禁用 TCP 流重组。或者，可以在一个规则中多次使用此关键字。

可使用以下语法启用或禁用数据流重组：

```
enable|disable, server|client|both, option, option
```

下表介绍可与 `stream_reassemble` 关键字配合使用的可选参数。

表 *156: stream_reassemble* 可选参数

参数	说明
noalert	无论规则中是否指定任何其他检测选项，都不生成事件。
fastpath	当有匹配时，忽略连接流量的其余部分。

例如，以下规则禁用 TCP 客户端数据流重组，而且不针对在 HTTP 响应中检测到 200 OK 状态代码的连接生成事件：

```
alert tcp any 80 -> any any (flow:to_client, established; content: “200 OK”;
stream_reassemble:disable, client, noalert
```

SSL 关键字

可以使用 SSL 规则关键字调用安全套接字层 (SSL) 预处理器，并从加密会话中的数据包提取有关 SSL 版本和会话状态的信息。

客户机和服务器进行通信以使用 SSL 或安全传输层 (TLS) 建立加密会话时，它们之间会交换握手消息。虽然在会话中传输的数据是加密的，但握手消息没有加密。

SSL 预处理器从特定握手字段提取状态和版本信息。握手中的两个字段分别指明用于加密会话的 SSL 或 TLS 版本以及握手的阶段。

ssl_state

ssl_state 关键字可用于匹配加密会话的状态信息。要同时检查所用的两个或更多 SSL 版本，请在规则中使用多个 ssl_version 关键字。

如果规则使用 ssl_state 关键字，规则引擎将调用 SSL 预处理器来检查流量的 SSL 状态信息。

例如，要检测是否有攻击者试图通过发送具有超长长度和过量数据的 ClientHello 消息来造成服务器缓冲区溢出，可以使用带有 client_hello 参数的 ssl_state 关键字，然后检查异常大的数据包。

可使用逗号分隔列表为 SSL 状态指定多个参数。如果列出多个参数，系统将使用 OR 运算符对这些参数进行评估。例如，如果指定 client_hello 和 server_hello 作为参数，系统将会根据带有 client_hello 或 server_hello 的流量对规则进行评估。

还可以否定任何参数；例如：

```
!client_hello, !unknown
```

为确保连接已达到状态集中的每种状态，应使用具有 ssl_state 规则选项的多个规则。ssl_state 关键字将以下标识符作为参数：

表 *157: ssl_state* 参数

参数	目的
client_hello	当客户端请求加密会话时，匹配消息类型为 ClientHello 的握手消息。
server_hello	当服务器响应客户端的加密会话请求时，匹配消息类型为 ServerHello 的握手消息。
client_keyx	当客户端向服务器发出密钥以确认收到来自服务器的密钥时，匹配消息类型为 ClientKeyExchange 的握手消息。
server_keyx	当客户端向服务器发出密钥以确认收到来自服务器的密钥时，匹配消息类型为 ServerKeyExchange 的握手消息。
unknown	匹配任何握手消息类型。

ssl_version

ssl_version 关键字可用于匹配加密会话的版本信息。如果规则使用 ssl_version 关键字，规则引擎将调用 SSL 预处理器来检查流量的 SSL 版本信息。

例如，如果知道 SSL 2 版本中存在缓冲区溢出漏洞，可以使用带有 sslv2 参数的 ssl_version 关键字来识别使用该 SSL 版本的流量。

可使用逗号分隔列表为 SSL 版本指定多个参数。如果列出多个参数，系统将使用 OR 运算符对这些参数进行评估。例如，如果要识别任何未使用 SSLv2 的加密流量，可以向规则添加 ssl_version:ssl_v3,tls1.0,tls1.1,tls1.2。这样，规则将会评估任何使用 SSL 3 版本、TLS 1.0 版本、TLS 1.1 版本或 TLS 1.2 版本的流量。

ssl_version 关键字将以下 SSL/TLS 版本标识符作为参数：

表 *158: ssl_version* 参数

参数	目的
sslv2	匹配使用安全套接字层 (SSL) 2 版本编码的流量。
sslv3	匹配使用安全套接字层 (SSL) 3 版本编码的流量。
tls1.0	匹配使用传输层安全 (TLS) 1.0 版本编码的流量。
tls1.1	匹配使用传输层安全 (TLS) 1.1 版本编码的流量。
tls1.2	匹配使用传输层安全 (TLS) 1.2 版本编码的流量。

appid 关键字

可以使用 appid 关键字识别数据包中的应用协议、客户端应用或 Web 应用。例如，可以针对据知易受特定漏洞影响的特定应用。

在入侵规则的 appid 关键字中，点击**配置 AppID (Configure AppID)** 以选择一个或多个要检测的应用。

浏览可用应用

首次开始构建条件时，**可用应用 (Available Applications)** 列表不受限制，并且显示系统检测的每个应用（每页 100 个）：

- 要翻页浏览应用，请点击列表下方的箭头。
- 要打开弹出窗口，显示有关应用特性的摘要信息以及可点选的互联网搜索链接，请点击应用旁边的 **信息**（ ）。

使用应用过滤器

为帮助查找要匹配的应用，您可以通过以下方式限制 **Available Applications** 列表：

- 要搜索应用，请点击列表上方的 **Search by name** 提示，然后键入名称。列表会在您键入内容时进行更新，以显示匹配的应用。
- 要通过应用过滤器来限制应用，请使用**应用过滤器 (Application Filters)** 列表。**Available Applications** 列表在您应用过滤器时进行更新。为方便起见，系统使用**解锁图标** 来标记系统只能在解密流量中识别（在加密或未加密流量中无法识别）的应用。

注释 如果您在 Application Filters 列表中选择一个或多个过滤器，并在这种状态下搜索 **Available Applications** 列表，系统会使用 AND 运算将您的选择与搜索过滤出的 **Available Applications** 列表进行组合。

选择应用

要选择单个应用，请选择该应用并点击**添加到规则 (Add to Rule)**。要选择当前受限制视图中的所有应用，请右键点击并选择**全选 (Select All)**。

应用层协议值

虽然预处理器执行应用层协议值的大部分检查和规范化工作，但您仍可以使用各种预处理器选项来检查应用层值。

RPC 关键字

`rpc` 关键字识别 TCP 或 UDP 数据包中的开放网络计算远程过程调用 (ONC RPC) 服务。这使您可以检测尝试识别主机上 RPC 程序的行为。入侵者可以使用 RPC 端口映射程序来确定网络上是否运行着可以利用的任何 RPC 服务。他们还可能尝试访问不使用端口映射程序运行 RPC 的其他端口。下表列出了 `rpc` 关键字接受的参数。

表 *159: rpc* 关键字参数

参数	说明
application	RPC 应用编号
procedure	调用的 RPC 过程
version	RPC 版本

要为 `rpc` 关键字指定参数，请使用以下语法：

```
application,procedure,version
```

其中，application 是 RPC 应用编号，procedure 是 RPC 过程编号，version 是 RPC 版本号。必须指定 `rpc` 关键字的所有参数 - 如果无法指定其中一个参数，请将其替换为星号 (`*`)。

例如，要搜索具有任意程序或版本的 RPC 端口映射程序（以数字 100000 表示的 RPC 应用），可使用 `100000,*,*` 作为参数。

ASN.1 关键字

`asn1` 关键字使您可以解码整个或部分数据包，以查找各种恶意编码。

下表介绍了 `asn1` 关键字的参数。

表 *160: asn.1* 关键字参数

参数	说明
无效位串编码	检测可远程攻击的无效位串编码。

参数	说明
双溢出	检测大于标准缓冲区的双 ASCII 编码。这是 Microsoft Windows 中的一个已知漏洞，但目前不知道哪些服务可能会被利用。
超长长度	检测长度大于提供的参数的 ASN.1 类型。例如，如果将 Oversize Length 设置为 500，任何大于 500 的 ASN.1 类型都会触发规则。
绝对偏移	设置从数据包负载起点算起的绝对偏移量。（请记住，偏移量计数器从字节 0 开始计算。）例如，如果要解码 SNMP 数据包，请将 Absolute Offset 设置为 0，但不设置 Relative Offset。Absolute Offset 可以是正数或负数。
相对偏移	从上一次成功内容匹配、`pcre` 或 `byte_jump` 算起的相对偏移量。要解码紧接在内容“foo”后的 ASN.1 序列，请将 Relative Offset 设置为 0，但不设置 Absolute Offset。Relative Offset 可以是正数或负数。（请记住，偏移量计数器从字节 0 开始计算。）

例如，Microsoft ASN.1 库中存在一个会造成缓冲区溢出的已知漏洞，使得攻击者能够利用包含特制的身份验证数据包的条件。当系统解码 ASN.1 数据时，数据包中的攻击代码可以在具有系统级别权限的主机上执行，或可能导致 DoS 条件。以下规则使用 `asn1` 关键字检测试图利用此漏洞的行为：

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445
(flow:to_server, established; content:"|FF|SMB|73|";
nocase; offset:4; depth:5;
asn1:bitstring_overflow,double_overflow,oversize_length 100,
relative_offset 54;)
```

当有 TCP 流量从 $EXTERNAL_NET 变量中定义的使用任何端口的任何 IP 地址流向 $HOME_NET 变量中定义的使用端口 445 的任何 IP 地址，上述规则将会生成事件。此外，它仅对与服务器之间建立的 TCP 连接执行规则。然后，该规则在特定位置对特定内容进行测试。最后，该规则使用 `asn1` 关键字检测位串编码和双 ASCII 编码，以及确定自上一次成功内容匹配结束以来从 55 字节起算超过 100 字节的 asn.1 类型长度。（请记住，`offset` 计数器从字节 0 开始计算。）

urilen 关键字

可以将 `urilen` 关键字和 HTTP 检查预处理器结合使用，以检查 HTTP 流量中特定长度、小于最大长度、大于最小长度或在指定范围内的 URI。

在 HTTP 检查预处理器对数据包进行规范化和检查后，规则引擎将根据规则评估数据包，并确定 URI 是否与 `urilen` 关键字指定的长度条件相匹配。可以使用此关键字来检测试图利用 URI 长度漏洞的攻击，例如，创建缓冲区溢出，以使攻击者可以在具有系统级别权限的主机上形成 DoS 条件或执行代码。

在规则中使用 `urilen` 关键字时，请注意：

- 实际上，`urilen` 关键字总是与 `flow:established` 关键字以及一个或多个其他关键字结合使用。
- 规则协议始终是 TCP。
- 目标端口始终是 HTTP 端口。

可以使用十进制字节数、小于号 (<) 和大于号 (>) 指定 URI 长度。

例如：

- 指定 `5` 将会检测长度为 5 字节的 URI。
- 指定 `< 5`（用一个空格字符隔开）将会检测长度小于 5 字节的 URI。
- 指定 `> 5`（用一个空格字符隔开）将会检测长度大于 5 字节的 URI。
- 指定 `3 <> 5`（<> 前后各有一个空格字符）将会检测长度为 3 到 5 字节的 URI。

例如，Novell 服务器的监控和诊断实用程序 iMonitor 2.4 版中存在一个已知漏洞，该漏洞来自 eDirectory 8.8 版。包含过长 URI 的一个数据包造成缓冲区溢出，使得攻击者者能够利用包含特制数据包的条件，该数据包可以在具有系统级别权限的主机上执行或可能导致 DoS 条件。以下规则使用 `urilen` 关键字检测试图利用此漏洞的行为：

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:"EXPLOIT eDirectory 8.8 Long URI iMonitor buffer
overflow attempt"; flow:to_server,established;
urilen:> 8192; uricontent:"/nds/"; nocase;
classtype:attempted-admin; sid:x; rev:1;)
```

当有 TCP 流量从 $EXTERNAL_NET 变量中定义的使用任何端口的任何 IP 地址流向 $HOME_NET 变量中定义的使用 $HTTP_PORTS 变量中定义的端口的任何 IP 地址，上述规则将会生成事件。此外，仅针对与服务器之间建立的 TCP 连接根据该规则评估数据包。该规则使用 `urilen` 关键字检测长度超过 8192 字节的任何 URI。最后，该规则在 URI 中搜索不区分大小写的特定内容 `/nds/`。

相关主题

入侵规则报头协议，第 1502 页
入侵规则报头源和目标端口，第 1506 页
预定义默认变量，第 1044 页

DCE/RPC 关键字

下表中描述的三个 DCE/RPC 关键字可用于监控 DCE/RPC 会话流量的漏洞。当系统处理带有这些关键字的规则时，会调用 DCE/RPC 预处理器。

表 *161: DCE/RPC* 关键字

使用.....	使用方式...	要检测的内容...
`dce_iface`	独立	识别特定 DCE/RPC 服务的数据包
`dce_opnum`	在前面加上 `dce_iface`	识别特定 DCE/RPC 服务操作的数据包
`dce_stub_data`	在前面加上 `dce_iface` 和 `dce_opnum`	定义特定操作请求或响应的存根数据

请注意，在上表中，应始终在 `dce_opnum` 前面加上 `dce_iface`，并应始终在 `dce_stub_data` 前面加上 `dce_iface` 和 `dce_opnum`。

也可以将这些 DCE/RPC 关键字与其他规则关键字结合连用。请注意，对于 DCE/RPC 规则，应使用选择了 **DCE/RPC** 参数的 `byte_jump`、`byte_test` 和 `byte_extract` 关键字。

思科建议在包含 DCE/RPC 关键字的规则中至少包含一个 `content` 关键字，以确保规则引擎使用快速模式匹配程序，从而加快处理速度和提高性能。请注意，如果规则包含至少一个 `content` 关键字，无论您是否启用 `content` 关键字的 **Use Fast Pattern Matcher** 参数，规则引擎都会使用快速模式匹配程序。

在以下情况下，可以将 DCE/RPC 版本及相邻报头信息用作匹配的内容：

- 规则不包括其他 `content` 关键字
- 规则包含另一个 `content` 关键字，但 DCE/RPC 版本及相邻信息代表比其他内容更独特的模式

  例如，DCE/RPC 版本及相邻信息更有可能比单个字节的内容更加独特。

应使用以下其中一个版本及相邻信息内容匹配来终止限定规则：

- 对于面向连接的 DCE/RPC 规则，使用内容 `|05 00 00|`（用于 05 主要版本、00 次要版本和请求 PDU [协议数据单元] 类型 00）。
- 对于无连接的 DCE/RPC 规则，使用内容 `|04 00|`（用于 04 版本和请求 PDU 类型 00）。

在这两种情况下，都应将版本及相邻信息的 `content` 关键字放在规则末尾，以调用快速模式匹配程序而不重复 DCE/RPC 预处理器已完成的处理。请注意：将 `content` 关键字放在规则末尾这种做法适用于被用作调用快速模式匹配程序手段的版本内容，对于规则中的其他内容匹配无需这样做。

相关主题

DCE/RPC 预处理器，第 2068 页
content 和 protected_content 关键字，第 1516 页
content 关键字快速模式匹配程序参数，第 1525 页
概述：byte_jump 和 byte_test 关键字
byte_extract 关键字，第 1533 页

dce_iface

可以使用 `dce_iface` 关键字识别特定 DCE/RPC 服务。

或者，还可以将 `dce_iface` 与 `dce_opnum` 和 `dce_stub_data` 关键字结合使用，以进一步限制要检查的 DCE/RPC 流量。

固定的 16 字节通用唯一标识符 (UUID) 用于识别分配给每个 DCE/RPC 服务的应用接口。例如，UUID 4b324fc8-670-01d3-1278-5a47bf6ee188 识别 DCE/RPC lanmanserver 服务（又称为 srvsvc 服务），该服务提供大量用于共享对等网络打印机、文件和 SMB 命名管道的管理功能。DCE/RPC 预处理器使用 UUID 及相关报头值来跟踪 DCE/RPC 会话。

接口 UUID 是由 5 个十六进制字符串（字符串之间用连字符分隔）组成：

```
<4hexbytes>-<2hexbytes>-<2hexbytes>-<2hexbytes>-<6hexbytes>
```

可以通过输入整个 UUID（包括连字符）来指定接口，如以下用于 netlogon 接口的 UUID 中所示：

```
12345678-1234-abcd-ef00-01234567cffb
```

请注意，必须以大端字节顺序指定 UUID 中的前三个字符串。尽管发布的接口列表和协议分析工具通常以正确的字节顺序显示 UUID，但您可能需要在输入前重新排列 UUID 字节顺序。考虑以下所示的信使服务 UUID，在原始 ASCII 文本中，该 UUID 的前三个字符串有时可能会以小端字节顺序显示：

```
f8 91 7b 5a 00 ff d0 11 a9 b2 00 c0 4f b6 e6 fc
```

可以为 dce_iface 关键字指定这个相同的 UUID，方法是先插入连字符，然后以大端字节顺序放置前三个字符串，如下所示：

```
5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc
```

尽管一个 DCE/RPC 会话可能包含发向多个接口的请求，但在一个规则中只能包含一个 dce_iface 关键字。可创建其他规则来检测其他接口。

DCE/RPC 应用接口也有接口版本号。或者，可以指定带有运算符的接口版本，用该操作符指明版本是等于、不等于、小于还是大于指定值。

除了 TCP 分段或 IP 分片外，还可以对面向连接和无连接的 DCE/RPC 进行分片。通常，将任何 DCE/RPC 分片（第一个除外）与指定接口相关联没有任何作用，而且这样做可能导致大量误报。但是，为了提高灵活性，可以根据指定接口对所有分片进行评估。

下表总结了 dce_iface 关键字参数。

表 *162: dce_iface* 参数

参数	说明
接口 UUID (Interface UUID)	UUID（包括连字符），用于识别要在 DCE/RPC 流量中检测的特定服务的应用接口。与指定接口相关的任何请求将匹配接口 UUID。
版本	或者，可以选择应用接口版本号 0 到 65535 和一个操作符，以指明是否检测大于 (>)、小于 (<)、等于 (=) 或不等于 (!) 指定值的版本。
所有分片 (All Fragments)	或者，可以选择匹配与 DCE/RPC 分片相关的所有接口和（如有指定）接口版本。默认情况下，此参数被禁用，表示关键字仅在第一个分片或整个未分片数据包与指定接口相关时才进行匹配。请注意，启用此参数可能会导致误报。

dce_opnum 关键字

可以将 dce_opnum 关键字和 DCE/RPC 预处理器结合使用，以检测识别 DCE/RPC 服务提供的一个或多个特定操作的数据包。

客户端功能调用请求特定服务函数（这些函数在 DCE/RPC 规范中称为操作）。操作编号 (opnum) 用于识别 DCE/RPC 报头中的特定操作。漏洞可能会针对特定操作。

例如，UUID 12345678-1234-abcd-ef00-01234567cffb 识别用于 netlogon 服务的接口；该服务提供几十个不同的操作，其中之一是操作 6，NetrServerPasswordSet 操作。

应该在 dce_opnum 关键字前面加上 dce_iface 关键字，以识别操作的服务。

可以为特定操作指定一个 0 到 65535 之间的十进制值，可以指定一系列由连字符分隔的操作，或者指定逗号分隔的操作和范围列表，其中的操作和范围可按任何顺序排列。

以下任何示例都将指定有效的 netlogon 操作编号：

```
15
15-18
15, 18-20
15, 20-22, 17
15, 18-20, 22, 24-26
```

dce_stub_data 关键字

可以将 dce_stub_data 关键字与 DCE/RPC 预处理器结合使用，以指定无论任何其他规则选项如何，规则引擎都应从存根数据的开头开始检查。紧跟在 dce_stub_data 关键字后面的数据包负载规则选项相对于存根数据缓冲区适用。

DCE/RPC 存根数据提供客户端程序调用和 DCE/RPC 运行时系统之间的接口，这种机制可提供对于 DCE/RPC 至关重要的例程和服务。DCE/RPC 漏洞在 DCE/RPC 数据包的存根数据部分中识别出。由于存根数据与特定的操作或函数调用相关，因此，应始终在 dce_stub_data 前面加上 dce_iface 和 dce_opnum，以识别相关的服务和操作。

dce_stub_data 关键字没有参数。

SIP 关键字

有四个 SIP 关键字可用于监控 SIP 会话流量的漏洞。

请注意，SIP 协议容易受到拒绝服务 (DoS) 攻击。基于速率的攻击防御可能对解决这类攻击的规则有利。

sip_header 关键字

可以使用 sip_header 关键字从提取的 SIP 请求或响应报头开头开始检查，并将检查限制为仅针对报头字段。

sip_header 关键字没有参数。

以下示例规则分片指向 SIP 报头并匹配 CSeq 报头字段：

```
alert udp any any -> any 5060 ( sip_header; content:"CSeq"; )
```

相关主题

动态入侵规则状态，第 1494 页
基于速率的攻击防御，第 2191 页

sip_body 关键字

可以使用 sip_body 关键字在提取的 SIP 请求或响应消息正文开头开始检查，并将检查限制为仅针对消息正文。

sip_body 关键字没有参数。

以下示例规则分片指向 SIP 消息正文，并匹配所提取 SDP 数据的 c（连接信息）字段中的特定 IP 地址：

```
alert udp any any -> any 5060 ( sip_body; content:"c=IN 192.168.12.14"; )
```

请注意，规则不仅限于搜索 SDP 内容。SIP 预处理器将提取整个消息正文并使其可供规则引擎使用。

sip_method 关键字

每个 SIP 请求中的 *method* 字段用于识别请求的目的。可以使用 `sip_method` 关键字测试特定方法的 SIP 请求。使用逗号隔开多种方法。

可以指定以下当前定义的任何 SIP 方法：

```
ack, benotify, bye, cancel, do, info, invite, join, message, notify, options, prack,
publish, quath, refer, register, service, sprack, subscribe, unsubscribe, update
```

方法不区分大小写。可以使用逗号分隔多个方法。

由于可能在将来定义新的 SIP 方法，因此也可以指定自定义方法（即，当前未定义的方法）。RFC 2616 中定义了接受的字段值，该规范允许除控制字符和分隔符（例如 =、(和) ）以外的所有字符。有关被排除分隔符的完整列表，请参阅 RFC 2616。如果系统在流量中遇到指定的自定义方法，它将检查数据包报头，但不检查消息。

系统最多支持 32 种方法，包括 21 种当前定义的方法和 11 种其他方法。系统将忽略您可能配置的任何未定义的方法。请注意，总共有 32 种方法，包括使用**检查方法 (Methods to Check)** SIP 预处理器选项指定的方法。

如果使用否定形式，只能指定一种方法。例如：

```
!invite
```

但请注意，规则中的多个 `sip_method` 关键字与 **AND** 运算相关联。例如，为测试除 `invite` 和 `cancel` 以外的所有提取的方法，将会使用两个否定形式的 `sip_method` 关键字：

```
sip_method: !invite
sip_method: !cancel
```

思科建议在包含 `sip_method` 关键字的规则中至少包含一个 `content` 关键字，以确保规则引擎使用快速模式匹配程序，从而加快处理速度和提高性能。请注意，如果规则包含至少一个 `content` 关键字，无论是否启用 `content` 关键字的**使用快速模式匹配程序 (Use Fast Pattern Matcher)** 参数，规则引擎都会使用快速模式匹配程序。

相关主题

SIP 预处理器选项，第 2108 页
content 和 protected_content 关键字，第 1516 页
content 关键字快速模式匹配程序参数，第 1525 页

sip_stat_code 关键字

每个 SIP 响应中的三位数状态代码指明请求操作的结果。您可以使用 `sip_stat_code` 关键字测试特定状态代码的 SIP 响应。

可以指定一个一位响应型数字（1 到 9）、一个特定的三位数（100 到 999）或者包含这两项的任意组合的逗号分隔列表。如果列表中的任何一个数字与 SIP 响应中的代码相匹配，则列表匹配。

下表介绍了可指定的 SIP 状态代码值。

表 *163: sip_stat_code* 值

要检测的内容...	需指定的内容...	示例	会检测的内容...
特定状态代码	三位数状态代码	189	189
任何以指定一位数开始的三位数代码	一位数	1	1xx；即，100、101、102 等
值列表	以逗号分隔的特定代码与一位数的组合	222, 3	222 以及 300、301、302 等

另请注意，规则引擎不使用快速模式匹配程序搜索用 `sip_stat_code` 关键字指定的值，无论规则是否包含 `content` 关键字。

GTP 关键字

有三个 GSRP 隧道协议 (GTP) 关键字可用于检查 GTP 命令通道的 GTP 版本、消息类型和信息元素。GTP 关键字不可与其他入侵规则关键字（例如 `content` 或 `byte_jump`）结合使用。**必须**在使用 `gtp_info` 或 `gtp_type` 关键字的每个规则中使用 `gtp_version` 关键字。

gtp_version 关键字

可以使用 `gtp_version` 关键字检查 GTP 控制信息以确定 GTP 版本为 0、1 还是 2。

由于不同的 GTP 版本定义不同的信息类型和信息元素，因此，使用 `gtp_type` 或 `gtp_info` 关键字时必须同时使用 `gtp_version`。可以将值指定为 0、1 或 2。

gtp_type 关键字

每条 GTP 消息由一种消息类型标识，消息类型由一个数值和一个字符串组成。可以使用 `gtp_type` 关键字检查特定 GTP 消息类型的流量。由于不同的 GTP 版本定义不同的信息类型和信息元素，因此在使用 `gtp_type` 或 `gtp_info` 关键字时必须同时使用 `gtp_version`。

可以为消息类型指定定义的十进制值，可以指定定义的字符串，或者指定包含这两项的任意组合的逗号分隔列表，如以下示例所示：

```
10, 11, echo_request
```

系统使用 OR 操作来匹配列出的每个值或字符串。值和字符串的列出顺序并不重要。列表中的任何一个值或字符串均与此关键字匹配。如果尝试保存包含无法识别的字符串或超出范围的值的规则，将会出现错误消息。

请注意，下表中不同的 GTP 版本有时会对同一种消息类型使用不同的值。例如，`sgsn_context_request` 这一消息类型在 GTPv0 和 GTPv1 中值是 50，但在 GTPv2 中值是 130。

gtp_type 关键字匹配不同的值，具体取决于数据包中的版本号。在上述示例中，在 GTPv0 或 GTPv1 数据包中，此关键字匹配消息类型值 50，在 GTPv2 数据包中，则匹配值 130。如果数据包中的消息类型值不是在数据包中指定的版本的已知值，此关键字不会匹配数据包。

如果为消息类型指定一个整数，则当关键字中的消息类型与 GTP 数据包中的该值匹配时，关键字将会匹配，无论数据包中指定的版本如何。

下表列出了系统识别出的为每种 GTP 消息类型定义的值和字符串。

表 *164: GTP* 消息类型

值	版本 0	版本 1	版本 2
1	echo_request	echo_request	echo_request
2	echo_response	echo_response	echo_response
3	version_not_supported	version_not_supported	version_not_supported
4	node_alive_request	node_alive_request	不适用
5	node_alive_response	node_alive_response	不适用
6	redirection_request	redirection_request	不适用
7	redirection_response	redirection_response	不适用
16	create_pdp_context_request	create_pdp_context_request	不适用
17	create_pdp_context_response	create_pdp_context_response	不适用
18	update_pdp_context_request	update_pdp_context_request	不适用
19	update_pdp_context_response	update_pdp_context_response	不适用
20	delete_pdp_context_request	delete_pdp_context_request	不适用
21	delete_pdp_context_response	delete_pdp_context_response	不适用
22	create_aa_pdp_context_request	init_pdp_context_activation_request	不适用
23	create_aa_pdp_context_response	init_pdp_context_activation_response	不适用
24	delete_aa_pdp_context_request	不适用	不适用
25	delete_aa_pdp_context_response	不适用	不适用
26	error_indication	error_indication	不适用
27	pdu_notification_request	pdu_notification_request	不适用
28	pdu_notification_response	pdu_notification_response	不适用

值	版本 0	版本 1	版本 2
29	pdu_notification_reject_request	pdu_notification_reject_request	不适用
30	pdu_notification_reject_response	pdu_notification_reject_response	不适用
31	不适用	supported_ext_header_notification	不适用
32	send_routing_info_request	send_routing_info_request	create_session_request
33	send_routing_info_response	send_routing_info_response	create_session_response
34	failure_report_request	failure_report_request	modify_bearer_request
35	failure_report_response	failure_report_response	modify_bearer_response
36	note_ms_present_request	note_ms_present_request	delete_session_request
37	note_ms_present_response	note_ms_present_response	delete_session_response
38	不适用	不适用	change_notification_request
39	不适用	不适用	change_notification_response
48	identification_request	identification_request	不适用
49	identification_response	identification_response	不适用
50	sgsn_context_request	sgsn_context_request	不适用
51	sgsn_context_response	sgsn_context_response	不适用
52	sgsn_context_ack	sgsn_context_ack	不适用
53	不适用	forward_relocation_request	不适用
54	不适用	forward_relocation_response	不适用
55	不适用	forward_relocation_complete	不适用
56	不适用	relocation_cancel_request	不适用
57	不适用	relocation_cancel_response	不适用
58	不适用	forward_srns_contex	不适用
59	不适用	forward_relocation_complete_ack	不适用
60	不适用	forward_srns_contex_ack	不适用
64	不适用	不适用	modify_bearer_command
65	不适用	不适用	modify_bearer_failure_indication

值	版本 0	版本 1	版本 2
66	不适用	不适用	delete_bearer_command
67	不适用	不适用	delete_bearer_failure_indication
68	不适用	不适用	bearer_resource_command
69	不适用	不适用	bearer_resource_failure_indication
70	不适用	ran_info_relay	downlink_failure_indication
71	不适用	不适用	trace_session_activation
72	不适用	不适用	trace_session_deactivation
73	不适用	不适用	stop_paging_indication
95	不适用	不适用	create_bearer_request
96	不适用	mbms_notification_request	create_bearer_response
97	不适用	mbms_notification_response	update_bearer_request
98	不适用	mbms_notification_reject_request	update_bearer_response
99	不适用	mbms_notification_reject_response	delete_bearer_request
100	不适用	create_mbms_context_request	delete_bearer_response
101	不适用	create_mbms_context_response	delete_pdn_request
102	不适用	update_mbms_context_request	delete_pdn_response
103	不适用	update_mbms_context_response	不适用
104	不适用	delete_mbms_context_request	不适用
105	不适用	delete_mbms_context_response	不适用
112	不适用	mbms_register_request	不适用
113	不适用	mbms_register_response	不适用
114	不适用	mbms_deregister_request	不适用
115	不适用	mbms_deregister_response	不适用
116	不适用	mbms_session_start_request	不适用
117	不适用	mbms_session_start_response	不适用
118	不适用	mbms_session_stop_request	不适用

值	版本 0	版本 1	版本 2
119	不适用	mbms_session_stop_response	不适用
120	不适用	mbms_session_update_request	不适用
121	不适用	mbms_session_update_response	不适用
128	不适用	ms_info_change_request	identification_request
129	不适用	ms_info_change_response	identification_response
130	不适用	不适用	sgsn_context_request
131	不适用	不适用	sgsn_context_response
132 个	不适用	不适用	sgsn_context_ack
133	不适用	不适用	forward_relocation_request
134	不适用	不适用	forward_relocation_response
135	不适用	不适用	forward_relocation_complete
136	不适用	不适用	forward_relocation_complete_ack
137	不适用	不适用	forward_access
138	不适用	不适用	forward_access_ack
139	不适用	不适用	relocation_cancel_request
140	不适用	不适用	relocation_cancel_response
141	不适用	不适用	configuration_transfer_tunnel
149	不适用	不适用	detach
150	不适用	不适用	detach_ack
151	不适用	不适用	cs_paging
152	不适用	不适用	ran_info_relay
153	不适用	不适用	alert_mme
154 种	不适用	不适用	alert_mme_ack
155	不适用	不适用	ue_activity
156	不适用	不适用	ue_activity_ack
160	不适用	不适用	create_forward_tunnel_request

值	版本 0	版本 1	版本 2
161	不适用	不适用	create_forward_tunnel_response
162	不适用	不适用	suspend
163	不适用	不适用	suspend_ack
164	不适用	不适用	继续执行
165	不适用	不适用	resume_ack
166	不适用	不适用	create_indirect_forward_tunnel_request
167	不适用	不适用	create_indirect_forward_tunnel_response
168	不适用	不适用	delete_indirect_forward_tunnel_request
169	不适用	不适用	delete_indirect_forward_tunnel_response
170	不适用	不适用	_access_bearer_request
171	不适用	不适用	release_access_bearer_response
176	不适用	不适用	downlink_data
177	不适用	不适用	downlink_data_ack
179	不适用	不适用	pgw_restart
180 个	不适用	不适用	pgw_restart_ack
200	不适用	不适用	update_pdn_request
201	不适用	不适用	update_pdn_response
211	不适用	不适用	modify_access_bearer_request
212	不适用	不适用	modify_access_bearer_response
231	不适用	不适用	mbms_session_start_request
232	不适用	不适用	mbms_session_start_response
233	不适用	不适用	mbms_session_update_request
234	不适用	不适用	mbms_session_update_response
235	不适用	不适用	mbms_session_stop_request
236	不适用	不适用	mbms_session_stop_response
240	data_record_transfer_request	data_record_transfer_request	不适用

值	版本 0	版本 1	版本 2
241	data_record_transfer_response	data_record_transfer_response	不适用
254	不适用	end_marker	不适用
255	pdu	pdu	不适用

gtp_info 关键字

一条 GTP 消息可以包含多个信息元素，其中的每一个元素均由已定义的一个数值和一个字符串来识别。可以使用 `gtp_info` 关键字在指定的信息元素开头开始检查，并将检查限于指定的信息元素。由于不同的 GTP 版本定义不同的消息类型和信息元素，因此在使用此关键字时还必须使用 `gtp_version`。

可以为信息元素指定已定义的十进制值或字符串。可以指定一个值或字符串，也可以在一个规则中使用多个 `gtp_info` 关键字来检查多个信息元素。

如果一条消息包含相同类型的多个信息元素，系统将会全部检查这些元素来进行匹配。如果信息元素按无效顺序出现，将仅检查最后一个实例。

请注意，不同的 GTP 版本有时对同一个信息元素使用不同的值。例如，`cause` 这个信息元素在 GTPv0 和 GTPv1 中值是 1，但在 GTPv2 中值是 2。

`gtp_info` 关键字匹配不同的值，具体取决于数据包中的版本号。在上述示例中，在 GTPv0 或 GTPv1 数据包中，此关键字匹配信息元素值 1，在 GTPv2 数据包中，则匹配值 2。如果数据包中的信息元素值不是在数据包中指定的版本的已知值，此关键字不会匹配数据包。

如果为信息元素指定一个整数，则当关键字中的消息类型与 GTP 数据包中的该值匹配时，关键字将会匹配，无论数据包中指定的版本如何。

下表列出了系统识别出的每个 GTP 信息元素的值和字符串。

表 *165: GTP* 信息元素

值	版本 0	版本 1	版本 2
1	cause	cause	imsi
2	imsi	imsi	cause
3	rai	rai	recovery
4	tlli	tlli	不适用
5	p_tmsi	p_tmsi	不适用
6	qos	不适用	不适用
8	recording_required	recording_required	不适用
9	authentication	authentication	不适用

值	版本 0	版本 1	版本 2
11	map_cause	map_cause	不适用
12	p_tmsi_sig	p_tmsi_sig	不适用
13	ms_validated	ms_validated	不适用
14	recovery	recovery	不适用
15	selection_mode	selection_mode	不适用
16	flow_label_data_1	teid_1	不适用
17	flow_label_signalling	teid_control	不适用
18	flow_label_data_2	teid_2	不适用
19	ms_unreachable	teardown_ind	不适用
20	不适用	nsapi	不适用
21	不适用	ranap	不适用
22	不适用	rab_context	不适用
23	不适用	radio_priority_sms	不适用
24	不适用	radio_priority	不适用
25	不适用	packet_flow_id	不适用
26	不适用	charging_char	不适用
27	不适用	trace_ref	不适用
28	不适用	trace_type	不适用
29	不适用	ms_unreachable	不适用
71	不适用	不适用	apn
72	不适用	不适用	ambr
73	不适用	不适用	ebi
74	不适用	不适用	ip_addr
75	不适用	不适用	mei
76	不适用	不适用	msisdn
77	不适用	不适用	indication

值	版本 0	版本 1	版本 2
78	不适用	不适用	pco
79	不适用	不适用	paa
80	不适用	不适用	bearer_qos
80	不适用	不适用	flow_qos
82	不适用	不适用	rat_type
83	不适用	不适用	serving_network
84	不适用	不适用	bearer_tft
85	不适用	不适用	tad
86	不适用	不适用	uli
87	不适用	不适用	f_teid
88	不适用	不适用	tmsi
89	不适用	不适用	cn_id
90	不适用	不适用	s103pdf
91	不适用	不适用	s1udf
92	不适用	不适用	delay_value
93	不适用	不适用	bearer_context
94	不适用	不适用	charging_id
95	不适用	不适用	charging_char
96	不适用	不适用	trace_info
97	不适用	不适用	bearer_flag
99	不适用	不适用	pdn_type
100	不适用	不适用	pti
101	不适用	不适用	drx_parameter
103	不适用	不适用	gsm_key_tri
104	不适用	不适用	umts_key_cipher_quin
105	不适用	不适用	gsm_key_cipher_quin

值	版本 0	版本 1	版本 2
106	不适用	不适用	umts_key_quin
107	不适用	不适用	eps_quad
108	不适用	不适用	umts_key_quad_quin
109	不适用	不适用	pdn_connection
110	不适用	不适用	pdn_number
111	不适用	不适用	p_tmsi
112	不适用	不适用	p_tmsi_sig
113	不适用	不适用	hop_counter
114	不适用	不适用	ue_time_zone
115	不适用	不适用	trace_ref
116	不适用	不适用	complete_request_msg
117	不适用	不适用	guti
118	不适用	不适用	f_container
119	不适用	不适用	f_cause
120	不适用	不适用	plmn_id
121	不适用	不适用	target_id
123	不适用	不适用	packet_flow_id
124	不适用	不适用	rab_contex
125	不适用	不适用	src_rnc_pdcp
126	不适用	不适用	udp_src_port
127	charge_id	charge_id	apn_restriction
128	end_user_address	end_user_address	selection_mode
129	mm_context	mm_context	src_id
130	pdp_context	pdp_context	不适用
131	apn	apn	change_report_action
132 个	protocol_config	protocol_config	fq_csid

值	版本 0	版本 1	版本 2
133	gsn	gsn	信道
134	msisdn	msisdn	emlpp_pri
135	不适用	qos	node_type
136	不适用	authentication_qu	fqdn
137	不适用	tft	ti
138	不适用	target_id	mbms_session_duration
139	不适用	utran_trans	mbms_service_area
140	不适用	rab_setup	mbms_session_id
141	不适用	ext_header	mbms_flow_id
142	不适用	trigger_id	mbms_ip_multicast
143	不适用	omc_id	mbms_distribution_ack
144 个	不适用	ran_trans	rfsp_index
145	不适用	pdp_context_pri	uci
146	不适用	addi_rab_setup	csg_info
147	不适用	sgsn_number	csg_id
148	不适用	common_flag	cmi
149	不适用	apn_restriction	service_indicator
150	不适用	radio_priority_lcs	detach_type
151	不适用	rat_type	ldn
152	不适用	user_loc_info	node_feature
153	不适用	ms_time_zone	mbms_time_to_transfer
154 种	不适用	imei_sv	throttling
155	不适用	camel	ARP
156	不适用	mbms_ue_context	epc_timer
157	不适用	tmp_mobile_group_id	signalling_priority_indication
158	不适用	rim_routing_addr	tmgi

值	版本 0	版本 1	版本 2
159	不适用	mbms_config	mm_srvcc
160	不适用	mbms_service_area	flags_srvcc
161	不适用	src_rnc_pdcp	nmbr
162	不适用	addi_trace_info	不适用
163	不适用	hop_counter	不适用
164	不适用	plmn_id	不适用
165	不适用	mbms_session_id	不适用
166	不适用	mbms_2g3g_indicator	不适用
167	不适用	enhanced_nsapi	不适用
168	不适用	mbms_session_duration	不适用
169	不适用	addi_mbms_trace_info	不适用
170	不适用	mbms_session_repetition_num	不适用
171	不适用	mbms_time_to_data	不适用
173	不适用	bss	不适用
174	不适用	cell_id	不适用
175	不适用	pdu_num	不适用
177	不适用	mbms_bearer_capab	不适用
178	不适用	rim_routing_disc	不适用
179	不适用	list_pfc	不适用
180 个	不适用	ps_xid	不适用
181	不适用	ms_info_change_report	不适用
182	不适用	direct_tunnel_flags	不适用
183	不适用	correlation_id	不适用
184	不适用	bearer_control_mode	不适用
185	不适用	mbms_flow_id	不适用
186	不适用	mbms_ip_multicast	不适用

值	版本 0	版本 1	版本 2
187	不适用	mbms_distribution_ack	不适用
188	不适用	reliable_inter_rat_handover	不适用
189	不适用	rfsp_index	不适用
190	不适用	fqdn	不适用
191	不适用	evolved_allocation1	不适用
192 个	不适用	evolved_allocation2	不适用
193	不适用	extended_flags	不适用
194	不适用	uci	不适用
195	不适用	csg_info	不适用
196	不适用	csg_id	不适用
197	不适用	cmi	不适用
198	不适用	apn_ambr	不适用
199	不适用	ue_network	不适用
200	不适用	ue_ambr	不适用
201	不适用	apn_ambr_nsapi	不适用
202	不适用	ggsn_backoff_timer	不适用
203	不适用	signalling_priority_indication	不适用
204	不适用	signalling_priority_indication_nsapi	不适用
205	不适用	high_bitrate	不适用
206	不适用	max_mbr	不适用
251	charging_gateway_addr	charging_gateway_addr	不适用
255	private_extension	private_extension	private_extension

SCADA 关键字

规则引擎使用 Modbus、DNP3、CIP 和 S7Commplus 规则来访问某些协议字段。

Modbus 关键字

可以单独使用 Modbus 关键字，也可以将它与其他关键字（例如 `content` 和 `byte_jump` 关键字）结合使用。

modbus_data

可以使用 `modbus_data` 关键字指向 Modbus 请求或响应中 Data 字段的开头。

modbus_func

可以使用 `modbus_func` 关键字来匹配 Modbus 应用层请求或响应报头中的“函数代码”(Function Code) 字段。可以为 Modbus 函数代码指定一个已定义的十进制值或一个已定义的字符串。

下表列出了系统识别出的为 Modbus 函数代码定义的值和字符串。

表 ***166: Modbus*** 函数代码

值	字符串
1	read_coils
2	read_discrete_inputs
3	read_holding_registers
4	read_input_registers
5	write_single_coil
6	write_single_register
7	read_exception_status
8	diagnostics
11	get_comm_event_counter
12	get_comm_event_log
15	write_multiple_coils
16	write_multiple_registers
17	report_slave_id
20	read_file_record
21	write_file_record
22	mask_write_register
23	read_write_multiple_registers
24	read_fifo_queue

值	字符串
43	encapsulated_interface_transport

modbus_unit

可以使用 `modbus_unit` 关键字来匹配 Modbus 请求或响应报头中的 Unit ID 字段。

DNP3 关键字

可以单独使用 DNP3 关键字，也可以将它与其他关键字（例如 `content` 和 `byte_jump` 关键字）结合使用。

dnp3_data

可以使用 `dnp3_data` 关键字指向重组 DNP3 应用层分片的开头。

DNP3 预处理器将链路层帧重组到应用层分片中。`dnp3_data` 关键字指向每个应用层分片的开头；其他规则选项可匹配分片中的重组数据，而无需每 16 个字节分隔数据并添加校验和。

dnp3_func

可以使用 `dnp3_func` 关键字来匹配 DNP3 应用层请求或响应报头中的“函数代码”(Function Code) 字段。可以为 DNP3 函数代码指定一个已定义的十进制值或一个已定义的字符串。

下表列出了系统识别出的为 DNP3 函数代码定义的值和字符串。

表 *167: DNP3* 函数代码

值	字符串
0	confirm
1	read
2	write
3	select
4	operate
5	direct_operate
6	direct_operate_nr
7	immed_freeze
8	immed_freeze_nr
9	freeze_clear
10	freeze_clear_nr
11	freeze_at_time

值	字符串
12	freeze_at_time_nr
13	cold_restart
14	warm_restart
15	initialize_data
16	initialize_appl
17	start_appl
18	stop_appl
19	save_config
20	enable_unsolicited
21	disable_unsolicited
22	assign_class
23	delay_measure
24	record_current_time
25	open_file
26	close_file
27	delete_file
28	get_file_info
29	authenticate_file
30	abort_file
31	activate_config
32	authenticate_req
33	authenticate_err
129	response
130	unsolicited_response
131	authenticate_resp

dnp3_ind

可以使用 `dnp3_ind` 关键字来匹配 DNP3 应用层响应报头中“内部指示”(Internal Indications) 字段中的标志。

可以为单个已知标志或以逗号分隔的标志列表指定字符串，如以下示例所示：

```
class_1_events, class_2_events
```

如果指定多个标志，此关键字将会匹配列表中的任何标志。要检测标志组合，可在一个规则中多次使用 `dnp3_ind` 关键字。

以下列表提供了系统识别出的用于已定义的 DNP3 内部指示标志的字符串语法。

```
class_1_events
class_2_events
class_3_events
need_time
local_control
device_trouble
device_restart
no_func_code_support
object_unknown
parameter_error
event_buffer_overflow
already_executing
config_corrupt
reserved_2
reserved_1
```

dnp3_obj

可以使用 `dnp3_obj` 关键字来匹配请求或响应中的 DNP3 对象报头。

DNP3 数据由一系列不同类型的 DNP3 对象组成，例如模拟输入、二进制输入，等等。每种类型均以组进行识别，例如模拟输入组、二进制输入组等，每个组可由一个十进制值进行识别。每个组中的对象均以对象变体进一步识别，例如 16 位整数、32 位整数、短浮点等，每个这些变体均指定对象的数据格式。每种类型的对象变体也可以十进制值进行识别。

可以通过为对象报头组类型和对象变体类型分别指定一个十进制数值来识别对象报头。这两种类型的组合可定义特定类型的 DNP3 对象。

CIP 和 ENIP 关键字

可以单独使用以下关键字或组合来创建自定义入侵规则，这些规则根据 CIP 预处理器检测的 CIP 和 ENIP 流量识别攻击。对于可配置的关键字，指定在允许的范围内的单个整数。有关详细信息，请参阅CIP 预处理器，第 2141 页。

表 168:

此关键字...	匹配...	范围
`cip_attribute`	CIP 消息中的“对象类/实例属性”字段。指定单个定义的整数值。	0 - 65535
`cip_class`	CIP 消息中的“对象类”字段。指定单个定义的整数值。	0 - 65535

此关键字...	匹配...	范围
cip_conn_path_class	连接路径中的“对象类”。指定单个整数值。	0 - 65535
cip_instance	CIP 消息中的“实例 ID”字段。指定单个整数值。	0 - 4284927295
cip_req	服务请求消息。	不适用
cip_rsp	服务响应消息。	不适用
cip_service	CIP 服务请求消息中的“服务”字段中。指定单个整数值。	0 - 127
cip_status	CIP 服务响应消息中的“状态”字段中。指定单个整数值。	0 - 255
enip_command	EthNet/IP 报头中的命令代码。指定单个整数值。	0 - 65535
enip_req	EthNet/IP 请求消息。	不适用
enip_rsp	EthNet/IP 响应消息。	不适用

S7Commplus 关键字

可以单独使用 S7Commplus 关键字或组合来创建自定义入侵规则，这些规则根据 S7Commplus 预处理器检测的流量识别攻击。对于可配置的关键字，指定在允许的范围内的单个已知值或单个整数。有关详细信息，请参阅S7Commplus 预处理器，第 2144 页。

请注意以下提示：

- 同一规则中的多个 S7commplus 关键字都使用 AND 运算。
- 在同一规则中使用多个 `s7commplus_func` 或 `s7commplus_opcode` 关键字会否定该规则，并且从不会匹配流量。要使用这些关键字搜索多个值，请创建多个规则。

s7commplus_content

在 S7Commplus 入侵规则中使用 `content` 或 `protected_content` 关键字之前，请使用 `s7commplus_content` 关键字将光标定位到数据包负载的开头。有关详细信息，请参阅content 和 protected_content 关键字，第 1516 页。

s7commplus_func

使用 `s7commplus_func` 关键字匹配 S7Commplus 报头中的以下值之一：

- explore
- createobject

- deleteobject
- setvariable
- getlink
- setmultivar
- getmultivar
- beginsequence
- endsequence
- invoke
- getvarsubstr
- 0x0 至 0xFFF

  请注意，数字表达式允许使用其他值。

s7commplus_opcode

使用 `s7commplus_opcode` 关键字匹配 S7Commplus 报头中的以下值之一：

- 请求
- response
- 通知
- response2
- 0x0 至 0xFF

  请注意，数字表达式允许使用其他值。

数据包特征

可以编写只针对具有特定特征的数据包生成事件的规则。

dsize

`dsize` 关键字测试数据包负载大小。使用此关键字时，可以用大于号和小于号（< 和 >）指定值的范围。可以使用以下语法来指定范围：

```
>number_of_bytes
<number_of_bytes
number_of_bytes<>number_of_bytes
```

例如，要表示大于 400 字节的数据包大小，请使用 `>400` 作为 `dtype` 值。要表示小于 500 字节的数据包大小，请使用 `<500`。要指定规则针对介于 400 到 500 字节（包括 400 和 500 字节）的任何数据包触发，请使用 `400<>500`。

⚠

注意 `dsize` 关键字测试未经任何预处理器解码的数据包。

isdataat

`isdataat` 关键字指示规则引擎验证数据是否驻留在负载中的特定位置。

下表列出了可与 `isdataat` 关键字配合使用的参数。

表 *169: isdataat* 参数

参数	类型	说明
偏移	必要	负载中的特定位置。例如，要测试显示在数据包中字节 50 处的数据，需要指定 `50` 作为偏移量值。`!` 修饰符对 `isdataat` 测试的结果进行求反；如果负载中不存在一定的数据量，则会发出警报。 您也可以使用现有 `byte_extract` 变量或 `byte_math` 结果指定此参数的值。
相对	可选	使位置相对于上一次成功内容匹配。指定相对位置时请注意，计数器从字节 0 开始计算，因此，应该如下计算相对位置：用从上一次成功内容匹配起向前计算所需的字节数减去 1。例如，要指定数据必须显示在上一次成功内容匹配后的第九个字节处，需要将相对偏移量指定为 `8`。
原始数据	可选	指定数据在由任何 Firepower 系统预处理器进行解码或应用层规范化之前位于原始数据包负载中。如果上一次内容匹配出现在原始数据包数据中，可以将此参数与 **Relative** 结合使用。

例如，在查找内容 `foo` 的规则搜索中，如果如下指定 `isdataat` 的值：

- Offset = !10
- Relative = enabled

那么，如果规则引擎在负载结束前未能在 `foo` 之后检测到 10 字节，系统将会发出警报。

sameip

`sameip` 关键字测试数据包的源 IP 地址和目标 IP 地址是否相同。此关键字没有参数。

fragoffset

`fragoffset` 关键字测试分片数据包的偏移量。由于某些漏洞（例如，WinNuke 拒绝服务攻击）使用手动生成的具有特定偏移量的数据包分片，因此，此关键字很有用。

例如，要测试分片数据包的偏移量是否为 31337 字节，应指定 `31337` 作为 `fragoffset` 的值。

为 `fragoffset` 关键字指定参数时，可以使用以下运算符。

表 *170: fragoffset* 关键字参数运算符

运算符	说明
!	不
>	大于
<	小于

请注意，不能将非 (!) 运算符与 < 或 > 结合使用。

cvs

`cvs` 关键字测试并发版本系统 (CVS) 流量中是否存在格式不正确的 CVS 条目。攻击者可以使用格式不正确的条目来强制堆溢出，并且在CVS服务器上执行恶意代码。此关键字可用于识别针对两种已知 CVS 漏洞的攻击：CVE-2004-0396（CVS1.11.x 至 1.11.15，以及 CVS1.12.x 至 1.12.7）和 CVS-2004-0414（CVS1.12.x 至 1.12.8，以及 CVS1.11.x 至 1.11.16）。`cvs` 关键字检查格式正确的记录，如果检测到格式不正确的条目，将会发出警报。

规则应包含 CVS 运行所在的端口。此外，应将任何可能出现流量的端口添加到 TCP 策略的数据流重组端口列表，以便为 CVS 会话维护状态。TCP 端口 2401 (`pserver`) 和 514 (`rsh`) 包含在出现数据流重组的客户端端口列表中。但请注意，如果服务器作为 `xinetd` 服务器（即，pserver）运行，它可以在任何 TCP 端口上运行。应将任何非标准端口添加到数据流重组 **Client Ports** 列表中。

相关主题

byte_extract 关键字，第 1533 页
TCP 数据流预处理选项，第 2171 页

活动响应关键字

resp 和 **react** 关键字提供了两种不同的活动响应发起方法。如果数据包触发规则，包含任意一个关键字的入侵规则将发起单一活动响应。活动响应关键字可以发起活动响应，以在响应触发的 TCP 规则时关闭 TCP 连接，或者在响应触发的 UDP 规则时关闭 UDP 会话。请参阅入侵丢弃规则中的活动响应，第 2149 页。出于一些原因，活动响应并不用于取代防火墙；这些原因包括攻击者可能已选择忽略或绕过活动响应。

内联支持活动响应，包括路由部署或透明部署。例如，在内联部署中对 `react` 关键字作出响应时，系统可以为连接的两端将 TCP 重置 (RST) 数据包直接插入到流量中（正常情况下，这样应该会关闭连接）。主动响应不支持或不适合被动部署。

由于活动响应可以回送，因此，系统不允许TCP重置发起TCP重置；这样可防止活动响应出现无穷尽的顺序。此外，为了符合标准做法，系统也不允许ICMP不可达数据包发起ICMP不可达数据包。

可以配置TCP数据流预处理器，使它在入侵规则触发了活动响应后检测TCP连接的其他流量。如果预处理器检测到其他流量，它会将指定最大数量的其他活动响应发送到连接或会话的两端。请参阅高级传输/网络预处理器选项，第 2149 页中的**最大活动响应数**和**最小响应秒数**。

相关主题

入侵丢弃规则中的活动响应，第 2149 页

resp 关键字

可以使用 `resp` 关键字来主动响应 TCP 连接或 UDP 会话，具体取决于在规则报头中指定的是 TCP 还是 UDP 协议。

使用关键字参数可指定数据包方向，以及指定是使用 TCP 重置 (RST) 数据包还是 ICMP 不可达数据包作为活动响应。

可以使用任何 TCP 重置或 ICMP 不可达参数来关闭 TCP 连接。只能使用 ICMP 不可达参数来关闭 UDP 会话。

此外，不同的 TCP 重置参数使得可以将数据包源和/或目标作为活动响应的目标。所有 ICMP 不可达参数都将数据包源作为目标，并且允许指定是使用 ICMP 网络、主机还是端口的不可达数据包，还是同时使用这三者的不可达数据包。

下表列出可与 `resp` 关键字结合使用以明确指定希望 Firepower 系统在规则触发时采取的操作的参数。

表 *171: resp* 参数

参数	说明
reset_source	将 TCP 重置数据包引至发送触发规则的数据包的终端。此外，可以指定 `rst_snd`（为了获得向后兼容性，仍支持使用此参数）。
reset_dest	将 TCP 重置数据包引至触发规则的数据包的预期目标终端。此外，可以指定 `rst_rcv`（为了获得向后兼容性，仍支持使用此参数）。
reset_both	将 TCP 重置数据包引至发送终端和接收终端。此外，可以指定 `rst_all`（为了获得向后兼容性，仍支持使用此参数）。
icmp_net	将 ICMP 网络不可达消息引至发送方。
icmp_host	将 ICMP 主机不可达消息引至发送方。
icmp_port	将 ICMP 端口不可达消息引至发送方。此参数用于终止 UDP 流量。
icmp_all	将以下 ICMP 消息引至发送方： • 网络不可达消息 • 主机无法到达 • 端口无法到达

例如，要将规则配置为会在规则触发时重置连接的两端，可使用 `reset_both` 作为 `resp` 关键字的值。

可以使用逗号分隔列表指定多个参数，如下所示：

```
argument,argument,argument
```

react 关键字

如果数据包触发规则，您可以使用 `react` 关键字将默认 HTML 页面发送到 TCP 连接客户端；发送 HTML 页面后，系统将使用 TCP 重置数据包来发起对连接两端的活动响应`react` 关键字不会对 UDP 流量触发活动响应。

或者，可以指定以下参数：

`msg`

如果数据包触发使用 `msg` 参数的 `react` 规则，HTML 页面将包含规则事件消息。

如果未指定 `msg` 参数，HTML 页面将包含以下消息：

```
You are attempting to access a forbidden site.
Consult your system administrator for details.
```

注释 由于活动响应可以回送，因此，请确保 HTML 响应页面不会触发 `react` 规则；否则，可能会导致活动响应出现无穷尽的顺序。思科建议在生产环境中激活 `react` 规则之前先对其进行广泛测试。

相关主题

规则剖析，第 1500 页

detection_filter 关键字

可以使用 `detection_filter` 关键字来防止某个规则生成事件，除非在指定时间内有指定数量的数据包触发该规则。这样可防止规则过早生成事件。例如，在几秒钟内登录失败两三次可能是预期行为，但在同一时间内出现大量登录尝试可能表示存在蛮力攻击。

`detection_filter` 关键字需要使用参数来定义系统是否跟踪源或目标 IP 地址、满足检测条件多少次后才会触发事件以及持续计数多长时间。

可使用以下语法延迟事件触发：

```
track by_src/by_dst, count count, seconds number_of_seconds
```

`track` 参数指定在计算符合规则检测条件的数据包数量时，是否使用数据包的源或目标 IP 地址。可选择下表中所述的参数值来指定系统如何跟踪事件实例。

表 *172: detection_filter* 跟踪参数

参数	说明
by_src	按源 IP 地址计算检测条件。
by_dst	按目标 IP 地址计算检测条件。

`count` 参数指定要使某个规则生成事件，在指定时间内必须有多少数据包为指定 IP 地址触发该规则。

seconds 参数指定要使某个规则生成事件，必须在多少秒内有指定数量的数据包触发该规则。

假设某个规则在数据包中搜索内容 foo，并将以下参数与 detection_filter 关键字配合使用：

```
track by_src, count 10, seconds 20
```

在此示例中，规则在 20 秒内从来自给定 IP 地址的 10 个数据包中检测到 foo 后才会生成事件。如果系统在头 20 秒内仅检测到有 7 个数据包包含 foo，将不会生成事件。但是，如果在头 20 秒内 foo 出现 40 次，规则将会生成 30 个事件，并在 20 秒后再次进行计数。

比较 threshold 和 detection_filter 关键字

detection_filter 关键字取代已被弃用的 threshold 关键字。但是，为了获得向后兼容性，仍支持使用 threshold 关键字，其作用与您在入侵策略中设置的阈值相同。

detection_filter 关键字是一种检测功能，适合在数据包触发规则前使用。在达到指定的数据包数量之前，规则不会针对触发检测到的数据包生成事件；在内联部署中，如果规则设置为丢弃数据包，在达到指定的数据包数量之前，规则不会丢弃数据包。相反，规则会针对会触发规则且在达到指定数据包数量后出现的数据包生成事件；在内联部署中，如果规则设置为丢弃数据包，规则将会丢弃数据包。

阈值是一种事件通知功能，不会造成检测操作。此功能适合在数据包触发事件后使用。在内联部署中，被设置为丢弃数据包的规则将会丢弃触发其本身的所有数据包，无论规则阈值如何。

请注意，可以在入侵策略中使用使用 detection_filter 关键字与入侵事件阈值、入侵事件抑制和基于速率的攻击防御等功能的任意组合。另请注意，如果启用某个导入的本地规则，而该规则将弃用的 threshold 关键字与某个入侵策略中的入侵事件阈值功能结合起来使用，策略验证将会失败。

相关主题

入侵事件阈值，第 1489 页
入侵策略抑制配置，第 1492 页
从规则页面设置动态规则状态，第 1496 页

tag 关键字

使用 tag 关键字可指示系统记录主机或会话的其他流量。使用 tag 关键字指定要捕获的流量的类型和数量时，可使用以下语法：

```
tagging_type, count, metric, optional_direction
```

以下三个表介绍了其他可用参数。

有两种标记类型可供选择。下表介绍了这两种标记类型。请注意，如果您在入侵规则中仅配置规则报头选项，会话标记参数类型会使系统像记录来自不同会话的数据包一样来记录来自同一个会话的数据包。要将来自同一会话的数据包分组在一起，请在同一入侵规则中配置一个或多个规则选项（例如，flag 关键字或 content 关键字）。

表 *173:* 标记参数

参数	说明
session	记录触发规则的会话中的数据包。
host	记录来自发送触发规则的数据包的主机的数据包。可以添加方向修饰符，以仅记录来自主机 (`src`) 或发送到主机 (`dst`) 的流量。

要指明想要记录的流量数量，请使用以下参数：

表 *174:* 计数参数

参数	说明
count	您想在规则触发后记录的数据包数量或秒数。 此度量单位用指标参数指定（该参数跟在计数参数后面）。

选择下表中所述的其中一个指标，以指明是要按时间还是流量数量进行记录。

⚠

注意 高带宽网络可以每秒查看成千上万个数据包，而且对大量数据包进行标记可能会严重影响性能，因此，请务必根据网络环境调整设置。

表 *175:* 日志记录指标参数

参数	说明
数据包	在规则触发后记录计数指定的数量的数据包。
seconds	在规则触发后在计数指定的秒数内记录流量。

例如，如果带有以下 `tag` 关键字值的规则触发：

```
host, 30, seconds, dst
```

将会记录在接下来的 30 秒内从客户端传输到主机的所有数据包。

flowbits 关键字

可以使用 `flowbits` 关键字为会话分配状态名称。通过根据之前命名的状态分析会话中的后续数据包，系统可以检测在一个会话中跨越多个数据包的攻击，并发出有关警报。

`flowbits` 状态名称是用户定义的标签，将被分配给会话特定部分中的数据包。可以根据数据包内容给数据包分配状态名称标签，以帮助将恶意数据包和那些您不想对其发出警报的数据包区分开。最多可以为每个受管设备定义1024个状态名称。例如，如果要对您知道仅在成功登录后才会出现的恶意数据包发出警报，可以使用 `flowbits` 关键字过滤掉构成初始登录尝试的数据包，这样就能够重点关注恶意数据包。要这样做，首先要创建一个会给具有状态为 `logged_in` 的已建立登录的会话中的

所有数据包分配标签的规则，然后创建另一个包含 flowbits 的规则，用以检查具有您在第一个规则中设置的状态的数据包，并且只对这些数据包采取操作。

可选的组名称用于向状态组添加状态名称。一个状态名称可以属于若干个组。未与组关联的状态并不相互排斥，因此，触发和设置未与组关联的状态的规则不会影响其他同时设置的状态。

flowbits 关键字选项

下表介绍了可用于 flowbits 关键字的运算符、状态和组的各种组合。请注意，状态名称可以包含字母数字字符、句号 (.)、下划线 (_) 和破折号 (-)。

表 176: flowbits 选项

运算符	状态选项	组	说明
set	state_name	可选	为数据包设置某个指定状态。如果定义了某个组，则在该指定的组中设置该状态。
set	state_name&state_name	可选	为数据包设置多个指定状态。如果定义了某个组，则在该指定的组中设置这些状态。
setx	state_name	强制	为数据包在指定组中设置某个指定状态，并取消设置该组中的所有其他状态。
setx	state_name&state_name	强制	为数据包在指定组中设置多个指定状态，并取消设置该组中的所有其他状态。
unset	state_name	没有组	为数据包取消设置某个指定状态。
unset	state_name&state_name	没有组	为数据包取消设置多个指定状态。
unset	all	强制	取消设置指定组中的所有状态。
toggle	state_name	没有组	取消设置某个指定状态（如果已设置），以及设置某个指定状态（如果未设置）。
toggle	state_name&state_name	没有组	取消设置多个指定状态（如果已设置），以及设置多个指定状态（如果未设置）。
toggle	all	强制	取消设置指定组中已设置的所有状态，以及设置指定组中未设置的所有状态。
isset	state_name	没有组	确定是否已在数据包中设置了某个指定状态。
isset	state_name&state_name	没有组	确定是否已在数据包中设置了多个指定状态。
isset	state_name|state_name	没有组	确定是否已在数据包中设置了任何指定状态。

运算符	状态选项	组	说明
isset	any	强制	确定是否已在指定组中设置了任何状态。
isset	all	强制	确定是否已在指定组中设置了所有状态。
isnotset	state_name	没有组	确定是否未在数据包中设置某个指定状态。
isnotset	state_name&state_name	没有组	确定是否未在数据包中设置多个指定状态。
isnotset	state_name|state_name	没有组	确定是否未在数据包中设置任何指定状态。
isnotset	any	强制	确定是否未在数据包中设置任何状态。
isnotset	all	强制	确定是否未在数据包中设置所有状态。
reset	（无状态）	可选	为所有数据包取消设置所有状态。取消设置某个组中的所有状态（如果已指定该组）。
noalert	（无状态）	没有组	可将此运算符与任何其他运算符结合使用，以抑制事件生成。

flowbits 关键字使用准则

使用 flowbits 关键字时，请注意：

- 使用 setx 运算符时，指定的状态只能属于指定的组，而不能属于任何其他组。
- 可以多次定义 setx 运算符，每次用一个实例指定不同的状态和同一个组。
- 如果使用 setx 运算符并指定了某个组，则不能对该指定的组使用 set、toggle 或 unset 运算符。
- isset 和 isnotset 运算符会对指定状态进行评定，无论该状态是否在组中。
- 在保存入侵策略、重新应用入侵策略以及应用访问控制策略期间（不管访问控制策略是引用一个入侵策略还是多个入侵策略），如果启用包含**未**指定组的 isset 或 isnotset 运算符的规则，并且至少有一个影响对应状态名称 flowbits 分配的规则（set、setx、unset、toggle）未启用，那么系统将启用影响对应状态名称 flowbits 分配的所有规则。
- 在保存入侵策略、重新应用入侵策略以及应用访问控制策略期间（不管访问控制策略是引用一个入侵策略还是多个入侵策略），如果启用包含**已**指定组的 isset 或 isnotset 运算符的规则，系统还将启用影响 flowbits 分配（set、setx、unset、toggle）和定义对应组名称的所有规则。

flowbits 关键字示例

本节提供三个使用 flowbits 关键字的示例。

flowbits 关键字示例：使用 state_name 的配置

这是使用 `state_name` 的 flowbits 配置的示例。

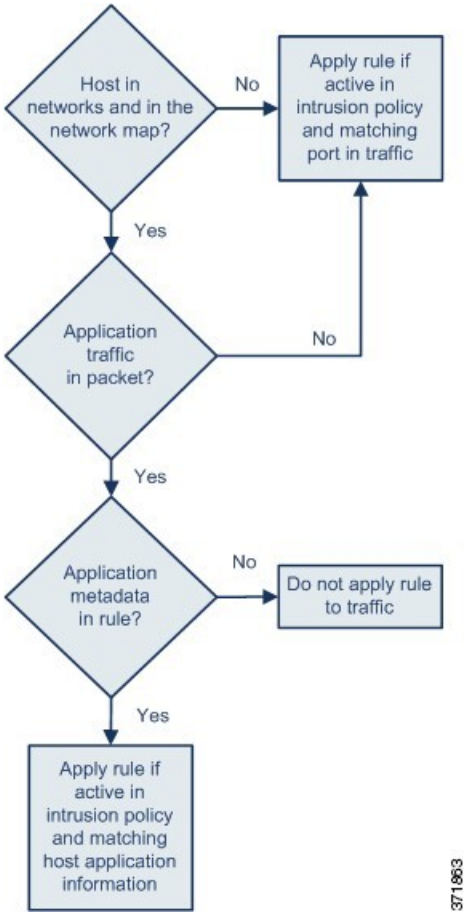
以 CVE ID 2000-0284 中所述的 IMAP 漏洞为例。该漏洞存在于 IMAP 的实现中，尤其是在 LIST、LSUB、RENAME、FIND 和 COPY 命令中。但是，要想利用该漏洞，攻击者必须登录到 IMAP 服务器。由于来自 IMAP 服务器的登录确认及紧随着而来的漏洞必定存在于不同的数据包中，因此，难以构建非基于流量的规则来捕获该漏洞。通过使用 `flowbits` 关键字，可以构建一系列规则来跟踪用户是否登录 IMAP 服务器；如果已登录，则在检测到其中一项攻击时生成事件。如果用户未登录，则攻击不能利用该漏洞，且不会生成事件。

以下两个规则分片说明了此示例。第一个规则分片查找来自 IMAP 服务器的 IMAP 登录确认：

```
alert tcp any 143 -> any any (msg:"IMAP login"; content:"OK

LOGIN"; flowbits:set,logged_in; flowbits:noalert;)
```

下图展示前述规则分片中 `flowbits` 关键字的影响：



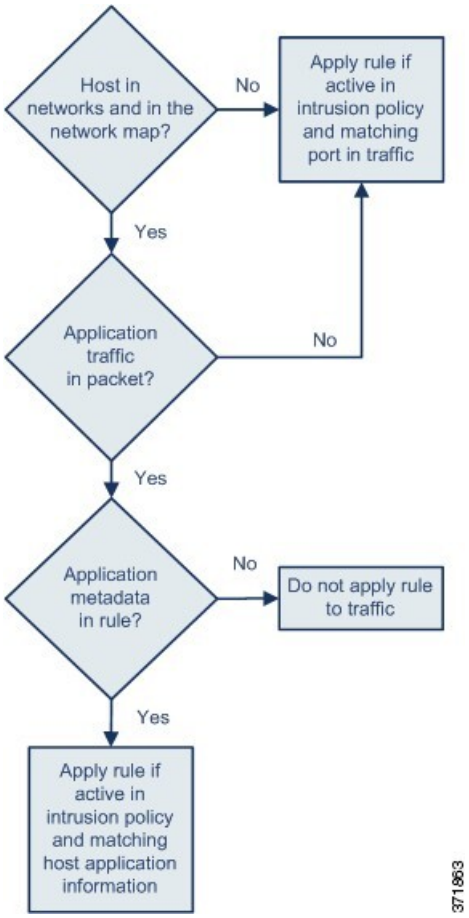
请注意，`flowbits:set` 设置 `logged_in` 状态，`flowbits:noalert` 则抑制警报，因为 IMAP 服务器上可能会出现许多无恶意的登录会话。

以下规则分片查找LIST字符串，但不生成事件，除非由于会话中某个之前的数据包而设置了logged_in状态：

```
alert tcp any any -> any 143 (msg:"IMAP LIST";

content:"LIST"; flowbits:isset,logged_in;)
```

下图展示前述规则分片中 `flowbits` 关键字的影响：



在这种情况下，如果之前的数据包已促使包含第一个分片的规则触发，则包含第二个分片的规则将会触发并生成事件。

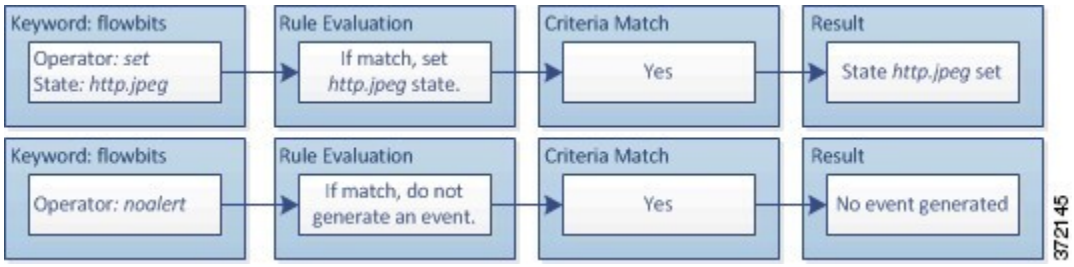
flowbits 关键字示例：导致误报事件的配置

在一个组中包含在不同规则中设置的不同状态名称可防止误报事件；如果后续数据包中的内容与状态不再有效的规则相匹配，就会出现误报事件。以下示例说明不在一个组中包含多个状态名称如何会导致误报。

假设以下三个规则分片在一个会话中按所示的顺序触发：

```
(msg:"JPEG transfer";
content:"image/";pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
?flowbits:set,http.jpeg; flowbits:noalert;)
```

下图展示前述规则分片中 flowbits 关键字的影响：

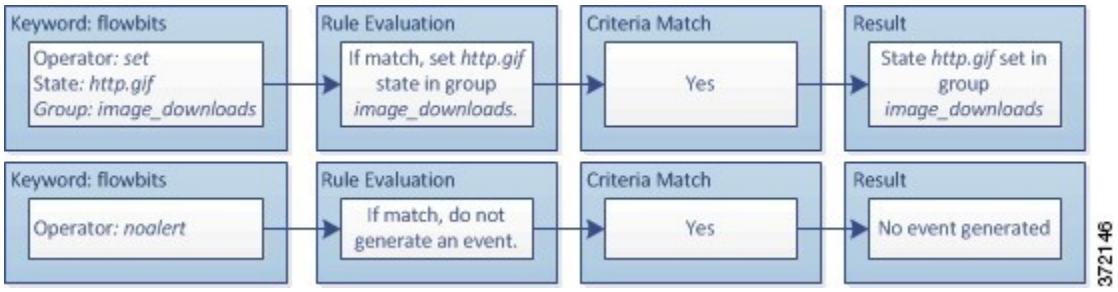


第一个规则分片中的 content 和 pcre 关键字与 JPEG 文件下载相匹配，flowbits:set,http.jpeg 设置 http.jpeg flowbits 状态，flowbits:noalert 阻止规则生成事件。系统不会生成事件，因为该规则的目的是检测文件下载并设置 flowbits 状态；为此，一个或多个伴随规则可以测试状态名称和恶意内容，如果检测到恶意内容，则会生成事件。

以下规则分片检测在上述 JPEG 文件下载之后发生的 GIF 文件下载：

```
(msg:"GIF transfer"; content:"image/";
pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
?flowbits:set,http.jpg,image_downloads; flowbits:noalert;)
```

下图展示前述规则分片中 flowbits 关键字的影响：

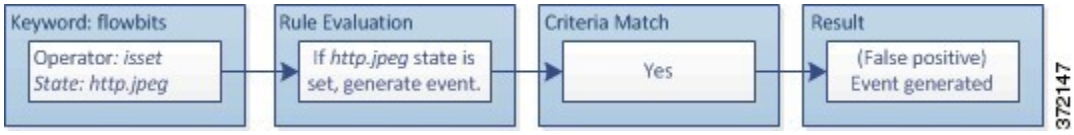


第二个规则中的 content 和 pcre 关键字与 GIF 文件下载相匹配，flowbits:set,http.jpg 设置 http.jpg flowbit 状态，flowbits:noalert 阻止规则生成事件。请注意，仍会设置由第一个规则分片设置的 http.jpeg 状态，即使不再需要使用它；这是因为如果检测到后续 GIF 下载，JPEG 下载必须已终止。

第三个规则分片伴随第一个规则分片出现：

```
(msg:"JPEG exploit";?flowbits:isset,http.jpeg;content:"|FF|";
pcre:"?/\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

下图展示前述规则分片中 flowbits 关键字的影响：



在第三个规则分片中，`flowbits:isset,http.jpeg` 确定是否已设置现在不相关的 `http.jpeg` 状态，`content` 和 `pcre` 则匹配在 JPEG 文件中是恶意的但在 GIF 文件中并非恶意的内容。第三个规则分片会针对 JPEG 文件中不存在漏洞生成误报事件。

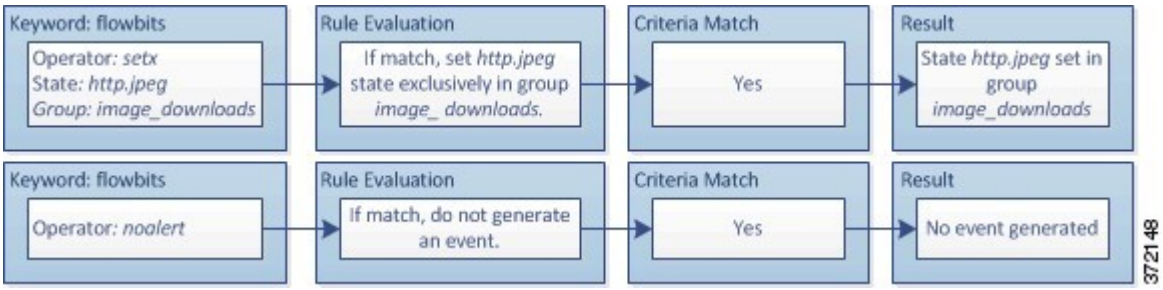
flowbits 关键字示例：防止误报事件的配置

以下示例说明在一个组中包含多个状态名称并使用 `setx` 运算符如何能防止误报。

以下规则分片与上一个规则分片示例大致相同，不同之处是，以下示例的前两个规则将两个不同的状态名称包含在同一个状态组中。

```
(msg:"JPEG transfer";
content:"image/";pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
?flowbits:setx,http.jpeg,image_downloads; flowbits:noalert;)
```

下图展示前述规则分片中 `flowbits` 关键字的影响：

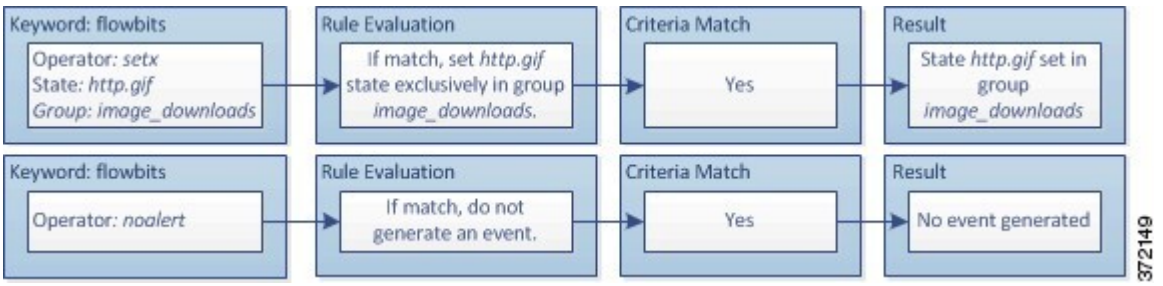


如果第一个规则分片检测到 JPEG 文件下载，`flowbits:setx,http.jpeg,image_downloads` 关键字会将 `flowbits` 状态设置为 `http.jpeg`，并将该状态包含在 `image_downloads` 组中。

然后，下一个规则会后续 GIF 文件下载：

```
(msg:"GIF transfer"; content:"image/";
pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
?flowbits:setx,http.jpg,image_downloads; flowbits:noalert;)
```

下图展示前述规则分片中 `flowbits` 关键字的影响：

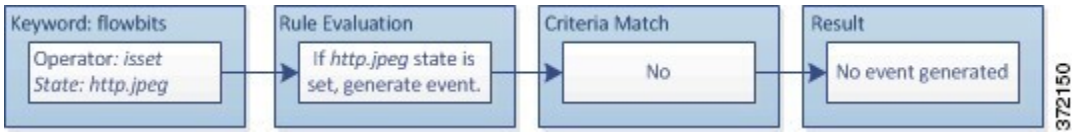


如果第二个规则分片与 GIF 下载相匹配，`flowbits:setx,http.jpg,image_downloads` 关键字将会设置 `http.jpg flowbits` 状态，并取消设置组中的另一个状态 `http.jpeg`。

第三个规则分片不会导致误报：

```
(msg:"JPEG exploit"; ?flowbits:isset,http.jpeg;content:"|FF|";
pcre:"/?\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

下图展示前述规则分片中 `flowbits` 关键字的影响：



由于 `flowbits:isset,http.jpeg` 为假，因此，规则引擎会停止处理规则，且不会生成事件，从而避免误报（即使 GIF 文件中的内容与 JPEG 文件的漏洞内容相匹配）。

http_encode 关键字

您可以使用 `http_encode` 关键字在未经规范化的 HTTP 请求或响应中生成关于编码类型的事件 - 可以是在 HTTP URI 中，在 HTTP 报头的非 cookie 数据中，在 HTTP 请求报头的 cookie 中，或者在 HTTP 响应的 set-cookie 数据中。

必须配置 HTTP 检查预处理器以检查 HTTP 响应和 HTTP cookie，从而使用 `http_encode` 关键字返回规则的匹配项。

此外，您必须在 HTTP 检查预处理器配置中为每个特定编码类型启用解码和警报选项，以使入侵规则中的 `http_encode` 关键字可以触发关于该编码类型的事件。

下表介绍了此选项可在 HTTP URI、报头、cookie 和 set-cookie 中为其生成事件的编码类型。

表 *177: HTTP_encode* 编码类型

编码类型	说明
utf8	如果此编码类型已启用，并可供 HTTP 检查预处理器进行解码，将会在指定位置检测 UTF-8 编码。
double_encode	如果此编码类型已启用，并可供 HTTP 检查预处理器进行解码，将会在指定位置检测双编码。
non_ascii	当检测到非 ASCII 字符但未启用检测到的编码类型时，在指定位置检测非 ASCII 字符。
uencode	如果此编码类型已启用，并可供 HTTP 检查预处理器进行解码，将会在指定位置检测 Microsoft %u 编码。
bare_byte	如果此编码类型已启用，并可供 HTTP 检查预处理器进行解码，将会在指定位置检测裸字节编码。

相关主题

服务器级别 HTTP 规范化选项，第 2092 页
HTTP 检查预处理器，第 2090 页

http_encode 关键字语法

编码位置

指定是要在 HTTP URI、报头还是 cookie（包括 set-cookie）中搜索指定的编码类型。

编码类型

使用以下格式之一指定一个或多个编码类型：

```
encode_type
encode_type|encode_type|encode_type...
```

其中，`encode_type` 是以下其中一项：

```
utf8
double_encode
non_ascii
uencode
bare_byte.
```

请注意，不能同时使用求反 (!) 和 OR (|) 运算符。

http_encode 关键字示例：使用两个 http_endcode 关键字搜索两种编码

以下示例使用同一规则中的两个 `http_encode` 关键字在 HTTP URI 中搜索 UTF-8 AND Microsoft IIS %u 编码：

第一个，`http_encode` 关键字：

- **Encoding Location**：`HTTP URI`
- **Encoding Type**：`utf8`

然后，另一个 `http_encode` 关键字：

- **编码位置 (Encoding Location)**：`HTTP URI`
- **编码类型 (Encoding Type)**：`uencode`

概述：file_type 和 file_group 关键字

`file_type` 和 `file_group` 关键字允许根据文件的类型和版本检测通过 FTP、HTTP、SMTP、IMAP、POP3 和 NetBIOS-ssn (SMB) 传输的文件。请**勿**在单个入侵规则中使用多个 `file_type` 或 `file_group` 关键字。

提示 更新漏洞数据库 (VDB) 可以使入侵规则编辑器获得最新的文件类型、版本和组。

注释 系统不会自动启用预处理器以适应 file_type 和 file_group 关键字。

如果希望流量的 生成事件并在内联部署中丢弃攻击性数据包 与您的 file_type 或 file_group 关键字相匹配，则**必须**启用特定的预处理器。

表 *178: file_type* 和 *file_group* 入侵事件生成

协议	所需的预处理器或预处理器选项
FTP	FTP/Telnet 预处理器和**规范化 TCP 负载**内联规范化预处理器选项
HTTP	在 HTTP 流量中生成入侵事件的 HTTP 检查预处理器
SMTP	在 HTTP 流量中生成入侵事件的 SMTP 预处理器
IMAP	IMAP 预处理器
POP3	POP 预处理器
Netbios-ssn (SMB)	DCE/RPC 预处理器和 **SMB 文件检查 (SMB File Inspection)** DCE/RPC 预处理器选项

相关主题

FTP/Telnet 解码器， 第 2083 页
内联规范化预处理器， 第 2153 页
HTTP 检查预处理器， 第 2090 页
SMTP 预处理器， 第 2120 页
IMAP 预处理器， 第 2114 页
POP 预处理器， 第 2117 页
DCE/RPC 预处理器， 第 2068 页

file_type 和 file_group 关键字

file_type

使用 file_type 关键字可指定在流量中检测到的文件的类型和版本。文件类型参数（例如 **JPEG** 和 **PDF**）用于识别要在流量中查找的文件格式。

注释 请**勿**在同一入侵规则中将 file_type 关键字与另一个 file_type 或 file_group 关键字配合使用。

系统默认选择 **Any Version**，但某些文件类型允许选择版本选项（例如 PDF 版本 **1.7**）来确定要在流量中查找的特定文件类型版本。

file_group

使用 file_group 关键字可选择思科定义的、包含在流量中找到的类似文件类型（例如**多媒体**或**音频**）的组。文件组还包含思科为组中的每种文件类型定义的版本。

注释 请**勿**在同一入侵规则中将 file_group 关键字与另一个 file_group 或 file_type 关键字配合使用。

file_data 关键字

file_data 关键字提供一个指针，该指针作为可用于其他关键字（例如 content、byte_jump、byte_test 和 pcre）的位置参数参考。检测到的流量确定 file_data 关键字指向的数据类型。您可以使用 file_data 关键字来指向以下负载类型的开头：

- HTTP 响应正文

  要检查 HTTP 响应数据包，必须启用 HTTP 检查预处理器，还必须将该预处理器配置为会检查 HTTP 响应。如果 HTTP 检查预处理器检测到 HTTP 响应正文数据，file_data 关键字将会进行匹配。

- 未压缩的 gzip 文件数据

  要检查 HTTP 响应正文中未压缩的 gzip 文件，必须启用 HTTP 检查预处理器，还必须将该预处理器配置为会检查 HTTP 响应以及会解压缩 HTTP 响应正文中的 gzip 压缩文件。有关详细信息，请参阅**检测 HTTP 响应**和**检测压缩数据**服务器级别 HTTP 规范化选项。如果 HTTP 检查预处理器在 HTTP 响应正文中检测到未压缩的 gzip 数据，file_data 关键字将会进行匹配。

- 规范化的 JavaScript

  要检查规范化的 JavaScript 数据，必须启用 HTTP 检查预处理器，还必须将该预处理器配置为检查 HTTP 响应。如果 HTTP 检查预处理器在响应主体数据中检测到 JavaScript，file_data 关键字将会进行匹配。

- SMTP 负载

  要检查 SMTP 负载，必须启用 SMTP 预处理器。如果 SMTP 预处理器检测到 SMTP 数据，file_data 关键字将会进行匹配。

- SMTP、POP 或 IMAP 流量中的编码电子邮件附件

  要检查 SMTP、POP 或 IMAP 流量中的邮件附件，必须分别启用 SMTP、POP 或 IMAP 预处理器或者启用它们的任意组合。然后，必须确保将已启用的每个预处理器配置为会对您想要解码的每种附件编码类型进行解码。可以为每个预处理器配置的附件解码选项是：**Base64 解码深度 (Base64 Decoding Depth)**、**7 位/8 位/二进制解码深度 (7-Bit/8-Bit/Binary Decoding Depth)**、**Quoted-Printable 解码深度 (Quoted-Printable Decoding Depth)** 和 **UUnix-to-Unix 解码深度 (Unix-to-Unix Decoding Depth)**。

  可以在一个规则中使用多个 file_data 关键字。

相关主题

HTTP 检查预处理器，第 2090 页
服务器级别 HTTP 规范化选项，第 2092 页
SMTP 预处理器，第 2120 页
IMAP 预处理器，第 2114 页

pkt_data 关键字

pkt_data 关键字提供一个指针，该指针作为可用于其他关键字（例如 content、byte_jump、byte_test 和 pcre）的位置参数参考。

如果检测到规范化的 FTP、telnet 或 SMTP 流量，pkt_data 关键字将指向规范化数据包负载的开头。如果检测到其他流量，pkt_data 关键字将指向原始 TCP 或 UDP 负载的开头。

必须启用以下规范化选项，系统才会对相应流量进行规范化以供入侵规则进行检测：

- 启用 FTP 和 Telnet 预处理器的**检测 FTP 命令内的 Telnet 转义代码 (Detect Telnet Escape Codes within FTP Commands)** 选项可规范化 FTP 流量以进行检查。
- 启用 FTP 和 Telnet 预处理器的**规范化 (Normalize)** Telnet 选项可规范化 Telnet 流量以进行检查。
- 启用 SMTP 预处理器的**规范化 (Normalize)** 选项可规范化 SMTP 流量以进行检查。

可以在一个规则中使用多个 pkt_data 关键字。

相关主题

客户端级别 FTP 选项，第 2087 页
Telnet 选项，第 2083 页
SMTP 预处理器选项，第 2120 页

base64_decode 和 base64_data 关键字

可以结合使用 base64_decode 和 base64_data 关键字，以指示规则引擎将指定数据作为 Base64 数据进行解码和检查。这可能很有用，例如，对于检查 Base64 编码 HTTP 身份验证请求报头，以及对于检查 HTTP PUT 和 POST 请求中的 Base64 编码数据。

这两个关键字对于编码和检查 HTTP 请求中的 Base64 数据尤其有用。但是，也可以将这两个关键字与像 HTTP 一样使用空格和制表符的任何协议（例如 SMTP）结合使用，以将长的报头行展开为跨越多行。如果协议中不存在这样的行展开（即为“折叠”），检查将在后面不跟有空格或制表符的任何回车符或换行符处结束。

base64_decode

base64_decode 关键字指示规则引擎将数据包数据解码为 Base64 数据。使用可选参数可指定要解码的字节数量以及在数据中的哪个位置开始解码。

可以在一个规则中使用 base64_decode 关键字一次；此关键字必须位于至少一个 base64_data 关键字实例前面。

解码 Base64 数据之前，规则引擎会将跨越多行的已折叠的长报头展开。当规则引擎遇到以下任何情况时，解码将会结束：

- 报头行结尾
- 要解码的指定字节数
- 数据包结尾

下表介绍了可与 `base64_decode` 关键字配合使用的参数。

表 *179:* 可选 *base64_decode* 参数

参数	说明
字节	指定要解码的字节数。如果未指定，解码将持续到报头行结尾或数据包负载结尾（以先到者为准）。可以指定非零的正值。
Offset	确定相对于数据包负载开头的偏移量，如果还指定了 **Relative**，则确定相对于当前检查位置的偏移量。可以指定非零的正值。
Relative	指定相对于当前检查位置的检查。

base64_data

`base64_data` 关键字提供用于检查使用 `base64_decode`关键字进行解码的 Base64 数据的参考。`base64_data` 关键字将检查设置在解码的 Base64 数据开头开始。或者，可以随后使用可用于其他关键字的位置参数（例如 `content` 或 `byte_test`）进一步指定要检查的位置。

使用 `base64_decode` 关键字之后，必须至少使用一次 `base64_data` 关键字；或者，可以多次使用 `base64_data` 以返回到解码的 Base64 数据的开头。

检查 Base64 数据时，请注意：

- 不能使用快速模式匹配程序。
- 如果在规则中使用干预性 HTTP 内容参数中断 Base64 检查，则必须在该规则中插入另一个 `base64_data` 关键字，然后再进一步检查 Base64 数据。

相关主题

概述：HTTP content 和 protected_content 关键字参数 ，第 1521 页
content 关键字快速模式匹配程序参数 ，第 1525 页

第 64 章

入侵和网络分析策略中的层

以下主题介绍如何使用入侵和网络分析策略中的层：

层基础知识

拥有众多受管设备的大型组织可能具有许多入侵策略和网络分析策略来支持不同部门、业务单位或（某些情况下）不同公司的独特需求。两种策略类型中的配置均包含在构建块（称为层）中，可用于高效管理多个策略。

入侵和网络分析策略中的层基本以相同方式工作。您可以创建和编辑任一策略类型，而无需刻意使用层。您也可以修改策略配置；如果您没有向策略中添加用户层，系统会自动将您的更改纳入单个可配置的层（初始名称为 *My Changes*）。您还可以最多添加 200 个层，在其中可以配置设置的任意组合。可以复制、合并、移动和删除用户层，并且最重要的是，可与同一类型的其他策略共享个别用户层。

网络分析和入侵策略层的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

网络分析和入侵策略层的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

层堆栈

层堆栈由以下元素组成：

用户层

用户可配置层可以复制、合并、移动或删除任何用户可配置层，并将任何用户可配置层设置为由同一类型的其他策略共享。此层包括自动生成的层，其最初名为“我的更改”(My Changes)。

内置层

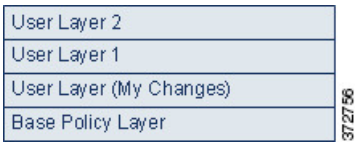
只读基本策略层。此层中的策略可以是系统提供的策略或您创建的自定义策略。

默认情况下，网络分析或入侵策略包括一个基本策略层和一个“我的更改”(My Changes) 层。可以根据需要添加用户层。

每个策略层均包含网络分析策略中所有预处理程序或入侵策略中所有入侵规则和高级设置的完整配置。最低基本策略层包含创建策略时选择的基本策略中的所有设置。较高层中的设置优先于较低层中的相同设置。在某一层中未明确设置的功能从对其进行了明确设置的下一最高层继承其设置。系统会将层平展，也就是说，它在处理网络流量时，仅应用所有设置的累积效果。

提示 可以仅根据基本策略中的默认设置创建入侵或网络分析策略。在创建入侵策略的情况下，如果要根据监控网络的特定需求定制入侵策略，您也可以使用 Firepower 规则陈述建议。

下图显示一个示例层堆栈，除基本策略层和初始My Changes层以外，还包括其他两个用户可配置层 *User Layer 1* 和 *User Layer 2*。请注意，图中添加的每个用户可配置层初始定位为堆栈中的最高层；因此，图中的 User Layer 2 最后添加并位于堆栈中的最高层。



无论是否允许规则更新修改策略，规则更新中的更改都绝不会覆盖您在层中所做的更改。这是因为规则更新中的更改是在基本策略中做出，基本策略会确定基本策略层中的默认设置；您的更改始终在更高层中做出，因此其会覆盖规则更新对基本策略所做出的任何更改。

基本层

入侵或网络分析策略的基本层（也称为基本策略）定义策略中所有配置的默认设置，并且是策略中的最低层。在不添加新层的情况下创建新策略以及更改设置，更改会存储在My Changes层中，并会覆盖（但不会更改）基本策略中的设置。

系统提供的基本策略

Firepower 系统提供若干对网络分析和入侵策略。通过使用系统提供的网络分析和入侵策略，您可以利用Talos 情报小组 的经验。对于这些策略，Talos 会设置入侵和预处理器规则状态，以及提供预处理器和其他高级设置的初始配置。可以按原样使用系统提供的这些策略，也可以将其用作自定义策略的基础。

如果使用系统提供的策略为基础，则导入规则更新可能会修改基本策略中的设置。但是，您可以配置自定义策略，以便系统不会自动对其系统提供的基本策略进行这些更改。这使您能够按照独立于规则更新的计划手动更新系统提供的基本策略。在任一情况下，规则更新对基本策略所做出的更改不会更改或覆盖 My Changes 或任何其他层中的设置。

系统提供的入侵和网络分析策略具有类似的名称，但包含不同的配置。例如，“平衡安全性和连接”(Balanced Security and Connectivity) 网络分析策略和“平衡安全性和连接”(Balanced Security and Connectivity) 入侵策略共同发挥作用，均可在入侵规则更新中更新。

自定义基本策略

您可以使用自定义策略作为基本策略。您可以调整自定义策略中的设置，以对您最重要的方式检查流量，从而能够提高受管设备的性能以及您有效响应其生成的事件的能力。

如果更改用作其他策略的基础的自定义策略，则这些更改会自动用作使用该基础的策略的默认设置。

此外，即使使用自定义基本策略，规则更新也可能会影响您的策略，因为在策略链中，所有策略都将系统提供的策略作为最终基础。如果链中的第一个自定义策略（即使用系统提供的策略作为其基础的策略）允许规则更新修改其基本策略，则您的策略可能会受影响。

无论如何对基本策略进行更改（通过规则更新或在修改用作基本策略的自定义策略时做出更改），都不会更改或覆盖“我的更改”(My Changes) 或任何其他层中的设置。

规则更新对基本策略的影响

导入规则更新时，系统会修改系统提供的入侵策略、访问控制策略和网络分析策略。规则更新可能包括：

- 经过修改的网络分析预处理器设置
- 入侵和访问控制策略中经过修改的高级设置
- 新增和更新的入侵规则
- 经过修改的现有规则状态
- 新的规则类别和默认变量

规则更新还可从系统提供的策略中删除现有规则。

对默认变量和规则类别的更改在系统级别处理。

如果将系统提供的策略用作入侵或网络分析基本策略，您可以允许规则更新修改基本策略，在此情况下，基本策略是系统提供的策略的副本。如果允许规则更新更新基本策略，则新规则更新在基本策略中所做的更改与其对用作基本策略的系统提供的策略所做出的更改相同。如果您未曾对相应的设置进行过修改，则基本策略中的设置会决定策略中的设置。但是，规则更新不会覆盖您在策略中所做出的更改。

如果不允许规则更新修改基本策略，则可以在导入一个或多个规则更新后手动更新基本策略。

无论入侵策略中的规则状态如何或者是否允许规则更新修改基本入侵策略，规则更新始终会删除 Talos 删除的入侵规则。

在将更改重新部署到网络流量之前，当前部署的入侵策略中的规则行为如下：

- 已禁用的入侵规则保持禁用。
- 设置为**生成事件 (Generate Events)** 的规则在触发时继续生成事件。
- 设置为**丢弃并生成事件 (Drop and Generate Events)** 的规则在触发时继续生成事件并丢弃有问题的数据包。

除非同时满足以下两个条件，否则规则更新不会修改自定义基本策略：

- 允许规则更新修改父策略（即用于创建自定义基本策略的策略）的系统提供的基本策略。
- 未曾在父策略中做出将覆盖父策略的基本策略中相应设置的更改。

如果同时满足两个条件，则在保存父策略时，规则更新中的更改会传递到子策略（即，使用自定义基本策略的策略）。

例如，如果规则更新启用以前禁用的入侵规则，并且您未曾修改该规则在父入侵策略中的状态，则在保存父策略时，已修改的规则状态会传递到基本策略。

同样，如果规则更新修改默认预处理程序设置，并且您未曾修改父网络分析策略中的设置，则在保存父策略时，已修改的设置会传递到基本策略。

更改基本策略

可以选择其他系统提供的策略或自定义策略作为基本策略。

可以链接最多五个自定义策略，这五个策略中有四个使用其余四个之一以前创建的策略作为其基本策略；第五个策略必须使用系统提供的策略作为其基础。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击所需的入侵策略行中的 **编辑**（）。

步骤 4 从**基本策略 (Base Policy)** 下拉列表中选择策略。

步骤 5 点击**保存 (Save)**。

下一步做什么

- 部署配置更改。

相关主题

冲突和更改：网络分析和入侵策略，第 1459 页

思科 建议层

当在入侵策略中生成规则状态建议时，可以选择是否根据建议自动修改规则状态。

如下图所示，使用建议的规则状态会在紧挨基本层之上插入一个内置只读思科 建议层。

请注意，此层对于入侵策略是唯一的。

如果您随后选择不使用建议的规则状态，则系统将移除思科 建议层。您无法手动删除该层，但是，您可以通过选择使用或不使用建议的规则状态来添加和移除该层。

添加思科 建议层会在导航面板中的“策略层”(Policy Layers) 下添加一个思科 建议链接。此链接会引导您进入思科 建议层页面的只读视图，在其中您可以只读模式访问“规则”(Rules) 页面的建议过滤视图。

使用建议的规则状态还会在导航面板中的思科 建议链接之下添加“规则”(Rules) 子链接。借助于“规则”(Rules) 子链接，可访问思科 建议层中“规则”(Rules) 页面的只读显示。在此视图中，请注意以下几点：

- 如果状态栏中没有规则状态图标，则从基本策略继承状态。
- 如果这个或其他“规则”(Rules) 页面视图的思科 建议列中没有规则状态图标，则没有适合此规则的建议。

相关主题

根据网络资产定制入侵防护，第 1621 页

层管理

Policy Layers 页面提供网络分析或入侵策略的完整层堆栈的单页摘要。在此页面上，可以添加共享和非共享层，复制、合并、移动和删除层，访问每层的摘要页面，以及访问每层中已启用、禁用和覆盖的配置的配置页面。

对于每层，您均可查看以下信息：

- 层是内置层、共享用户层还是非共享用户层
- 哪些层包含最高（即最有效）预处理程序或高级设置配置（按功能名称）
- 在入侵策略中，在该层中设置了其状态的入侵规则的数量，以及设置为每个规则状态的规则的数量。

“策略层”(Policy Layers) 页面还提供所有已启用预处理器（网络分析）或高级设置（入侵）的实际效果的摘要，并为入侵策略提供入侵规则的实际效果的摘要。

每层的摘要中的功能名称指明在该层中已启用、禁用、覆盖或继承哪些配置，如下所示：

当功能.....	功能名称.....
在层中已启用	以纯文本编写
在层中已禁用	删除
被更高层中的配置覆盖	以斜体文本编写
从更低层继承	不存在

您最多可以向网络分析或入侵策略中添加 200 层。添加的层显示为策略中的最高层。初始状态对于所有功能都为 Inherit，并且在入侵策略中，未设置事件过滤、动态状态或警报规则操作。

在将用户可配置层添加到策略中时，可为该层提供唯一名称。之后，可以更改名称，或者可以在编辑层时添加或修改可视的说明。

您可以复制层，在“用户层”(User Layers) 页面区域中将层上移或下移，或删除用户层，包括初始“我的更改”(My Changes) 层。请注意以下考虑事项：

- 在复制层时，副本显示为最高层。
- 复制共享层会创建初始未共享且之后在选择时可共享的层。
- 不能删除共享层；已启用共享但未曾与其他策略共享的层不是共享层。

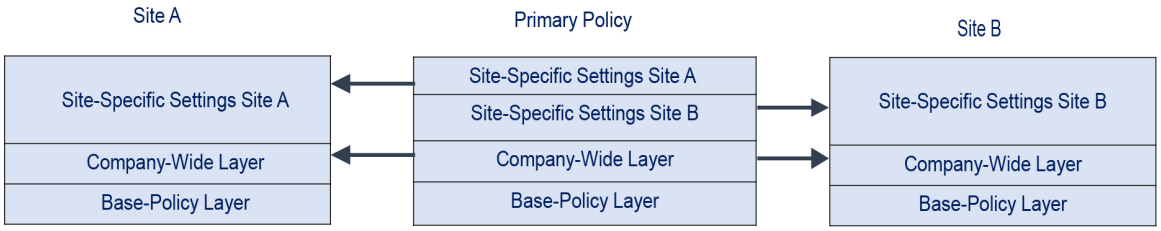
您可以将一个用户可配置层与其正下方的另一个用户可配置层合并。合并层保留任一层特有的所有设置，并且如果两层均包含同一预处理程序、入侵规则或高级设置的设置，则会接受更高层中的设

置。合并层保留更低层的名称。如果在策略中创建的可共享层可以添加到其他策略，则可以将该可共享层正上方的非共享层与该可共享层合并，但是不能将该共享层与其下方的非共享层合并。如果在一个策略中添加的共享层在其他策略中已创建，则可以将该共享层合并到其正下方的非共享层中，所生成的层不再共享；不能将非共享层合并到其下方的共享层中。

共享层

当您在另一策略中创建层后，可以将该层添加到您的策略中并允许其共享，该层即为共享层。可共享的层是您允许共享的层。

下图显示一个主策略示例，您可在其中创建公司范围层，为站点 A 和 B 创建站点特定层，并允许进行共享。然后，将这些层作为共享层添加到站点 A 和 B 的策略中。



主策略中的公司范围层包含适用于站点 A 和 B 的设置。站点特定层包含特定于每个站点的设置。例如，如果使用网络分析策略，则 Site A 在受监控网络上可能没有 Web 服务器，并且不需要 HTTP Inspect 预处理程序的保护或处理开销，但两个站点均可能需要 TCP 数据流预处理。可在与两个站点共享的公司范围层启用 TCP 数据流处理，在与站点 A 共享的站点特定层禁用 HTTP 检查预处理器，在与站点 B 共享的站点特定层启用 HTTP 检查预处理器。通过编辑站点特定策略中的较高层配置，如果需要任何配置调整，您还可以进一步微调每个站点的策略。

示例主策略中的扁平化网络设置不大可能对流量监控有用，但配置和更新站点特定策略所节省的时间使得它成为策略层的一种有用应用。

也可使用许多其他层配置。例如，您可以按公司、部门、网络甚至用户来界定策略层。如果使用入侵策略，则还可以在一层中包含高级设置，在另一层中包含规则设置。

可以将用户可配置层与同一类型（入侵或网络分析）的其他策略共享。在可共享层中修改配置，然后确认更改时，系统会更新共享层的所有策略，并为您提供所有受影响策略的列表。您只能在已创建该层的策略中修改功能配置。

不能对添加到另一个策略的层禁用共享；必须先从另一个策略中删除该层，或者删除另一个策略。

当基本策略是在其中已创建要共享的层的自定义策略时，不能向策略中添加共享层。这样将为策略提供循环依赖。

在多域部署中，可以将来自祖先策略的共享层添加到后代域中的策略。

管理层

过程

步骤 1 在编辑 Snort 2 策略时，点击导航面板中的**策略层 (Policy Layers)**。

步骤 2 可以在“策略层”(Policy Layers) 页面上执行下列任意管理操作：

- 添加其他策略中的共享层 - 点击“用户层”(User Layers) 旁边的添加共享层 **添加**（+），从**添加共享层 (Add Shared Layer)** 下拉列表中选择层，然后点击**确定 (OK)**。
- 添加非共享层 - 点击“用户层”(User Layers) 旁边的添加层 **添加**（+），输入**名称 (Name)**，然后点击**确定 (OK)**。
- 添加或更改层说明 - 点击层旁边的 **编辑**（✎），然后添加或更改**说明 (Description)**。
- 允许与其他策略共享层 - 点击层旁边的 **编辑**（✎），然后清除**共享 (Sharing)** 复选框。
- 更改层名称 - 点击层旁边的 **编辑**（✎），然后更改**名称 (Name)**。
- 复制层 - 点击该层的 **复制**（⧉）。
- 删除层 - 点击该层的 **删除**（🗑），然后点击**确定 (OK)**。
- 合并两层 - 点击两层中上层的 **合并**（⧉），然后点击**确定 (OK)**。
- 移动层 - 点击层摘要中的任何开放区域并将其拖动，直至**位置箭头** 指向该层上方或下方要将该层移到的行。

步骤 3 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

相关主题

冲突和更改：网络分析和入侵策略，第 1459 页

导航层

过程

步骤 1 在编辑 Snort 2 策略时，点击导航面板中的**策略层 (Policy Layers)**。

步骤 2 可以执行下列任意操作以在各层间导航：

- 访问预处理器或高级设置页面 - 如果要访问层级别的预处理器或高级设置配置页面，请点击该层对应的行中的功能名称。配置页面在基本策略和共享层中为只读。
- 访问规则页面 - 如果要访问按规则状态类型过滤的层级别的规则配置页面，请在层摘要中点击**丢弃并生成事件 (Drop and Generate Events)**、**生成事件 (Generate Events)** 或**禁用 (Disabled)**。如果该层不包含设置为所选规则状态的规则，则不会显示任何规则。
- 显示“策略信息”(Policy Information) 页面 - 如果要显示“策略信息”(Policy Information) 页面，请点击导航面板中的**策略摘要 (Policy Summary)**。
- 显示层摘要页面 - 如果要显示某层的摘要页面，请点击该层对应的行中的层名称，或者点击用户层旁边的 **编辑**（）。您也可以点击 **视图**（） 来访问共享层的只读摘要页面。

步骤 3 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

相关主题

冲突和更改：网络分析和入侵策略，第 1459 页

层中的入侵规则

可以在该层的 Rules 页面上查看个别层设置，也可以在 Rules 页面的策略视图中查看所有设置的实际效果。在 Rules 页面的策略视图中修改规则设置时，修改的是策略中的最高用户可配置层。可以在任何 Rules 页面上使用层下拉列表切换到另一层。

下表描述在多个层中配置相同类型设置的效果。

表 *180:* 层规则设置

您可设置	设置类型	所需的操作…
一条	规则状态	覆盖为更低层中的规则设置的规则状态，并忽略在更低层中为该规则配置的所有阈值、抑制、基于速率的规则状态和警报。 如果希望规则从基本策略或更低层继承其状态，请将规则状态设置为 Inherit。请注意，在入侵策略“规则”(Rules) 页面上操作时，不能将规则状态设置为“继承”(Inherit)，因为入侵策略“规则”(Rules) 页面是所有规则设置的实际效果的综合视图。
一条	阈值 SNMP 警报	对于下层中的规则，覆盖相同类型的设置。请注意，对于该层中的规则，设置阈值将改写所有现有阈值。

您可设置	设置类型	所需的操作…
一个或多个	基于抑制率的规则状态	将为每个选定规则累积组合相同类型的设置，直到为规则设置了规则状态的第一层。系统会忽略设定规则状态所在层下方的设置。
一个或多个	注释	向规则中添加注释。注释特定于规则，而非特定于策略或层。您可以在任何层中为规则添加一个或多个注释。

例如，如在一层中将规则状态设置为“丢弃并生成事件”(Drop and Generate Events)，但在上层设置为“已禁用”(Disabled)，则入侵策略的“规则”(Rules) 页面将显示规则已被禁用。

又例如，如果在一层中为规则将基于源的抑制设置为 192.168.1.1，同时也为该规则将基于目标的抑制设置为 192.168.1.2，则“规则”(Rules) 页面显示：累积效应将为源地址 192.168.1.1 和目标地址 192.168.1.2 抑制事件。请注意，抑制和基于速率的规则状态设置将为每个选定规则累积组合相同类型的设置，直到为规则设置了规则状态的第一层。系统会忽略设定规则状态所在层下方的设置。

“规则”(Rules) 页面上特定层的颜色编码表示有效状态位于较高层、较低层还是当前层中，如下所示：

- 红色 - 有效状态位于较高层
- 黄色 - 有效状态位于较低层
- 无光度 - 有效状态位于当前层

由于入侵策略 Rules 页面是所有规则设置的实际效果的综合视图，因此规则状态在此页面上未进行颜色编码。

配置层中的入侵规则

在入侵策略中，可以为任何用户可配置层中的规则设置规则状态、事件过滤、动态状态、警报和规则注释。访问要更改的层后，可按照在入侵策略 Rules 页面上所用的相同方法在该层的 Rules 页面添加设置。

过程

步骤 1 编辑 Snort 2 入侵策略时，展开导航面板中的**策略层 (Policy Layers)**。

步骤 2 展开要修改的策略层。

步骤 3 点击要修改的策略层正下方的 **Rules**。

步骤 4 修改使用规则调整入侵策略，第 1473 页中所述的任意设置。

提示 要从可编辑层删除单项设置，请双击该层“规则”页面上的规则消息，以显示规则详细信息。点击要删除的设置旁边的 **Delete**，然后双击 **OK**。

步骤 5 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

相关主题

冲突和更改：网络分析和入侵策略，第 1459 页

从多个层中删除规则设置

可以从入侵策略中的多个层同时删除特定类型的事件过滤器、动态状态或警报。系统移除所选设置并将规则的剩余设置复制到策略中的最高可编辑层。

系统将向下移除每层中设置的设置类型，直至移除所有设置或遇到为规则设置了规则状态的层。在后一种情况下，系统会从该层中删除设置并停止删除设置类型。

当系统在共享层或在基本策略中遇到该设置类型时，如果策略中的最高层可以编辑，则系统会将该规则的剩余设置和规则状态复制到该可编辑层。否则，如果策略中的最高层是共享层，系统会在该共享层上方创建新的可编辑层，并将该规则的剩余设置和规则状态复制到该可编辑层。

注释 删除从共享层或基本策略派生的规则设置会导致忽略从更低层或基本策略中对该规则做出的任何更改。要停止忽略从更低层或基本策略做出的更改，请在最高层的摘要页面上将规则状态设置为 **Inherit**。

过程

步骤 1 在编辑 Snort 2 入侵策略时，点击导航面板中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

提示 也可为所有层在“规则”(Rules) 页面的层下拉列表中选择**策略 (Policy)**，或在“策略信息”(Policy Information) 页面选择**管理规则 (Manage Rules)**。

步骤 2 选择要从中删除多个设置的规则：

- 选择特定 - 如果要选择特定规则，请选中每条规则旁边的复选框。
- 选择全部 - 如果要选择当前列表中的所有规则，请选中列顶部的复选框。

步骤 3 选择以下选项之一：

- **事件过滤 > 删除阈值**
- **事件过滤 > 删除抑制**
- **动态状态 > 删除基于速率的规则状态**
- **警报 > 删除 SNMP 警报**

注释 删除从共享层或基本策略派生的规则设置会导致忽略从更低层或基本策略中对该规则做出的任何更改。要停止忽略从更低层或基本策略做出的更改，请在最高层的摘要页面上将规则状态设置为 **Inherit**。

步骤 4 点击 **OK**。

步骤 5 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

相关主题

冲突和更改：网络分析和入侵策略，第 1459 页

接受来自自定义基本策略的规则更改

当未曾添加层的自定义网络分析或入侵策略使用另一个自定义策略作为其基本策略时，在以下情况下，必须将规则设置为继承其规则状态：

- 删除为基本策略中的规则设置的事件过滤器、动态状态或 SNMP 警报，以及
- 您希望规则接受在用作基本策略的另一个自定义策略中对其做出的后续更改

过程

步骤 1 编辑 Snort 2 入侵策略时，展开导航面板中的**策略层 (Policy Layers)**。

步骤 2 展开**我的更改 (My Changes)**。

步骤 3 点击**我的更改 (My Changes)** 正下方的**规则 (Rules)** 链接。

步骤 4 选择要接受其设置的规则。有以下选项可供选择：

- 选择特定规则 - 如果要选择特定规则，请选中每条规则旁边的复选框。
- 选择所有规则 - 如果要选择当前列表中的所有规则，请选中列顶部的复选框。

步骤 5 从**规则状态 (Rule State)** 下拉列表选择**继承 (Inherit)**。

步骤 6 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

相关主题

冲突和更改：网络分析和入侵策略，第 1459 页

层中的预处理器和高级设置

您使用类似的机制在网络分析策略中配置预处理程序和在入侵策略中配置高级设置。您可以启用和禁用预处理器（在网络分析设置页面上）和入侵策略高级设置（在入侵策略“高级设置”[Advanced Settings] 页面上）。这些页面还提供所有相关功能的有效状态的摘要。例如，如果网络分析 SSL 预处理器在一层中已禁用但在更高层中已启用，则“设置”(Settings) 页面将其显示为已启用。在这些页面上做出的更改显示在策略的顶层中。请注意，Back Orifice 预处理程序没有用户可配置选项。

您也可以在用户可配置层的摘要页面上启用或禁用预处理程序或高级设置并访问其配置页面。在此页面上，可以修改层名称和说明，并配置是否将该层与同一类型的其他策略共享。可以通过选择导航面板中 **Policy Layers** 下方的层名称来切换到另一层的摘要页面。

启用预处理器或高级设置时，在导航面板中的层名称下方会显示指向该功能的配置页面的子链接，并且在层的摘要页面上的功能旁边会显示 **编辑**（）；在层中禁用该功能或将其设置为“继承”(Inherit) 时，这些图标会消失。

设置预处理器或高级设置的状态（已启用或已禁用）会覆盖更低层中该功能的状态和配置设置。如果希望预处理器或高级设置从基本策略或更低层继承其状态和配置，请将其设置为“**继承**”**(Inherit)**。请注意，当在 Settings 或 Advanced Settings 页面上操作时，无法选择 Inherit。另请注意，如果继承当前启用的功能，则导航面板中的功能子链接和配置页面上的编辑图标不再显示。

系统使用已启用该功能的最高层中的配置。除非明确修改配置，否则系统使用默认配置。例如，如果在一层中启用并修改网络分析 DCE/RPC 预处理程序，并且还在更高层中将其启用但不修改，则系统使用更高层中的默认配置。

每个层摘要页面上的颜色编码指示有效配置位于较高层、较低层还是当前层中，如下所示：

- 红色 - 有效配置位于较高层
- 黄色 - 有效配置位于较低层
- 无光度 - 有效配置位于当前层

由于 Settings 和 Advanced Settings 页面是所有相关设置的综合视图，因此，这些页面不使用颜色编码指明有效配置的位置。

配置层中的预处理器和高级设置

过程

步骤 1 编辑 Snort 2 策略时，请展开导航面板中的**策略层 (Policy Layers)**，然后点击要修改的层的名称。

步骤 2 有以下选项可供选择：

- 更改层**名称 (Name)**。
- 添加或更改**说明 (Description)**。
- 选中或清除**共享 (Sharing)** 复选框以指定层是否可以与其他策略共享。
- 要访问已启用的预处理器/高级设置的配置页面，请点击 **编辑**（ ） 或功能子链接。
- 要禁用当前层中的预处理器/高级设置，请点击功能旁边的**已禁用 (Disabled)**。
- 要启用当前层中的预处理器/高级设置，请点击功能旁边的**已启用 (Enabled)**。
- 要从当前层下方的最高层中的设置继承预处理器/高级设置，请点击**继承 (Inherit)**。

步骤 3 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

相关主题

冲突和更改：网络分析和入侵策略，第 1459 页

第 65 章

根据网络资产定制入侵防护

以下主题介绍如何使用 Cisco 建议规则：

关于思科 建议的规则

可以遵从入侵规则建议，将您的网络中检测到的操作系统、服务器和客户端应用协议与为保护这些资产而特别编写的规则相关联。这样，您就可根据自己的受监控网络的特定需求定制您的入侵策略。

系统为每个入侵策略制定一组单独的建议。它通常会建议标准文本规则和共享对象规则的规则状态更改。但是，它也可建议预处理器和解码器规则的更改。

当生成规则状态建议时，可以使用默认设置或配置高级设置。通过高级设置，可以执行以下操作：

- 重新定义系统监控网络上的哪些主机以查找漏洞
- 影响系统根据规则开销建议哪些规则
- 指定是否生成建议以禁用规则

您还可以选择是要立即使用建议还是在接受之前审核建议（和受影响规则）。

选择使用建议规则状态会向入侵策略中添加只读思科 建议层，并且随后选择不使用建议规则状态会删除该层。

系统不会更改手动设置的规则状态：

- 在生成建议之前手动设置指定规则的状态可防止系统将来修改这些规则的状态。
- 在生成建议之后手动设置指定规则的状态可覆盖这些规则的建议状态。

提示 入侵策略报告可能包含具有与建议状态不同的规则状态的规则列表。

在显示对建议过滤后的 Rules 页面时，或者从导航面板或 Policy Information 页面直接访问 Rules 页面后，可以手动设置规则状态、对规则排序并执行 Rules 页面中的任何其他可用操作，例如抑制规则、设置规则阈值等。

注释 Talos 情报小组 确定系统提供的策略中的各规则的相应状态。如果使用系统提供的策略作为基本策略，并且允许系统将规则设置为思科 建议规则状态，则入侵策略中的规则与思科为网络资产建议的设置相匹配。

建议规则和多租户

系统会为每个枝叶域构建单独的网络映射。在多域部署中，如果您在祖先域的入侵策略中启用此功能，则系统会使用来自所有后代枝叶域的数据生成建议。这可能使得入侵规则针对可能不存在于所有枝叶域的资产进行定制，从而影响性能。

思科 建议的默认设置

当生成思科 建议时，系统会搜索基本策略以查找防范与网络资产关联的漏洞的规则，并识别基本策略中的规则的当前状态。然后，系统会建议规则状态，如果选择如此，则会将规则设置为建议状态。

系统执行以下基本分析来生成建议：

表 *181:* 基于漏洞的规则状态建议

规则是否保护发现的资产？	基本策略规则状态	建议的规则状态
是	禁用	Generate Events
	Generate Events	Generate Events
	Drop and Generate Events	Drop and Generate Events
否	任意	禁用

请注意表中的以下内容：

- 如果某个规则在基本策略中处于禁用状态或设置为“生成事件”，则建议的状态始终是“生成事件”。

  例如，如果基本策略是“无活动规则”，其中的所有规则均处于禁用状态，则不会建议“丢弃并生成事件”。

- 只有对于已在基本策略中设置为“丢弃并生成事件”的规则，才会建议“丢弃并生成事件”。

  如果您要将某个规则设置为“丢弃并生成事件”，且该规则在基本策略中处于禁用状态或已设置为“生成事件”，您必须手动重置该规则的状态。

当生成建议而不更改思科 建议规则的高级设置时，系统会建议更改所发现的整个网络中所有主机的规则状态。

默认情况下，系统仅为低开销或中等开销的规则生成建议，并生成禁用规则的建议。

系统不会为基于使用“影响限定条件”(Impact Qualification) 功能禁用的漏洞的入侵规则建议规则状态。

系统始终建议启用与映射到主机的第三方漏洞相关联的本地规则。

对于未映射的本地规则，系统不会给出状态建议。

相关主题

第三方产品映射，第 1919 页

思科 建议的高级设置

在策略报告中包括建议和规则状态之间的所有差异

默认情况下，入侵策略报告列出策略中已启用的规则，即设置为“生成事件”(Generate Events) 或“丢弃并生成事件”(Drop and Generate Events) 的规则。启用**包括所有差异 (Include all differences)** 选项还会列出其建议状态与已保存状态不同的规则。有关策略报告的信息，请参阅策略报告，第 149 页。

要检查的网络

指定为给出建议而要检查的受监控网络或单独主机。可以指定单个 IP 地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。

指定主机中的地址列表与一个逻辑或运算关联，但逻辑非除外，逻辑非在所有逻辑或运算计算完之后与一个逻辑与运算关联。

如果要根据主机信息动态调整对特定数据包的主动规则处理，也可以启用自适应配置文件。

建议阈值（就规则开销而言）

防止系统推荐或自动启用开销高于您选择的阈值的入侵规则。

开销基于规则对系统性能的潜在影响以及规则产生误报的可能性。允许开销较高的规则通常会得到更多的建议，但会影响系统性能。在“入侵规则”(Intrusion Rules) 页面的规则详细信息视图中，可以查看规则的开销级别。

请注意，系统在给出禁用规则的建议时，不会将规则开销作为一项考虑因素。此外，本地规则没有开销，除非被映射到第三方漏洞。

为开销级别为特定设置的规则生成建议并不会妨碍您使用不同的开销生成建议后再重新为原来的开销设置生成建议。每次为同一规则集生成建议时，无论生成多少次建议或者生成多少不同的开销设置，为每个开销设置获得的规则状态建议都相同。例如，您可以将开销依次设置为中、

高，并最终设置为中来生成建议，如果网络中的主机和应用尚未更改，对于该规则集给出的开销设置为中的两组建议均相同。

接受禁用规则的建议

指定系统是否根据 思科 建议禁用入侵规则。

接受禁用规则的建议会限制规则的覆盖范围。忽略禁用规则的建议会扩大规则的覆盖范围。

相关主题

自适应配置文件更新和思科 建议规则 ，第 2203 页

生成和应用思科 建议

开始或停止使用思科 建议可能需要几分钟的时间，具体取决于网络和入侵规则集的大小。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，如果您在祖先域的入侵策略中启用此功能，则系统会使用来自所有后代枝叶域的数据生成建议。这可能使得入侵规则针对可能不存在于所有枝叶域的资产进行定制，从而影响性能。

开始之前

- 思科 建议具有以下要求：
  - 威胁防御 许可证-IPS
  - 经典许可证-保护
  - 用户角色-管理员 或 入侵管理员 (Intrusion Admin)
- 在开始执行这些步骤之前，请配置网络发现策略。配置网络发现策略以定义内部主机，以便适合思科 建议。请参阅网络发现自定义 ，第 1966 页。

过程

步骤 1 在 Snort 2 入侵策略编辑器的导航窗格中，点击**思科建议 (Cisco Recommendations)**。

步骤 2 （可选）配置高级设置；请参阅思科 建议的高级设置 ，第 1623 页。

步骤 3 生成并应用建议。

- **生成并使用建议**-生成建议并更改规则状态以使其匹配。仅在您从未生成过建议时可用。
- **生成建议**-无论您是否在使用建议，生成新的建议，但不更改规则状态使其匹配。
- **更新建议**-如果您正在使用建议，生成建议并更改规则状态以使其匹配。否则，生成新的建议，但不更改规则状态。
- **使用建议**-更改规则状态以匹配任何未实施的建议。
- **不使用建议**-停止使用建议。如果您在应用建议前手动更改了规则状态，则规则状态会恢复为您为其指定的值。否则，规则状态会恢复为其默认值。

在您生成建议时，系统会显示建议更改的摘要。要查看系统建议更改状态的规则列表，请点击最近建议的规则状态旁边的**查看 (View)**。

步骤 4 评估并调整您实施的建议。

即使您接受大多数思科 建议，也可以通过手动设置规则状态覆盖个别建议；请参阅设置入侵规则状态，第 1488 页。

步骤 5 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

脚本检测

脚本检测可通过部分检测来防止 Snort 过晚阻止入侵失败。在客户端和服务器之间传输 HTML 文件时，这些文件可能会包含用于发起攻击的恶意脚本（例如 JavaScript）。当发现此类恶意脚本时，部分检查允许任何 IPS 规则匹配恶意脚本，并且检查器会通过检查和检测来刷新该数据段。恶意文件永远不会到达其目的地。此功能同时支持 HTTP/1 和 HTTP/2 流量。

默认情况下始终启用此功能。要关闭此功能，请将 **`http_inspect.script_detection=true`** 设为 false。

第 66 章

敏感数据检测

以下主题介绍敏感数据检测及其配置方式：

敏感数据检测基础知识

敏感数据（如社会保障号码、信用卡号码、驾驶证号码等）可能会被有意或无意地在互联网上泄露。系统提供了一种敏感数据预处理器，可在 ASCII 文本中检测和生成关于敏感数据的事件，这在检测意外数据泄露时特别有用。

全局敏感数据检测选项用于控制预处理器的工作方式。可以修改指定以下内容的全局选项：

- 预处理器是否在触发数据包中替换信用卡号或社会保障号的最后四位数
- 网络上的哪些目标主机监控敏感数据
- 单个会话中所有数据类型总共出现多少次会产生事件

具体数据类型确定了在指定目标网络流量中可以针对其进行检测并生成事件的敏感数据。可以为指定以下内容的数据类型选项修改默认设置：

- 某种检测到的数据类型必须达到才能生成单个会话事件的阈值
- 每种数据类型要监控的目标端口
- 每种数据类型要监控的应用协议

可以创建和修改自定义数据类型以检测指定的数据模式。例如，医院可以创建一种数据类型来保护患者编号；再如，大学可以创建一种数据类型来检测具有唯一编号模式的学号。

系统通过将各个数据类型与流量进行比对来检测每个 TCP 会话中的敏感数据。可以为每种数据类型和适用于入侵策略中所有数据类型的全局选项修改默认设置。Firepower 系统提供了常用的预定义数据类型。您也可以创建自定义数据类型。

敏感数据预处理器规则与每种数据类型关联。可通过为数据类型启用相应的预处理器，为每种数据类型启用敏感数据检测和事件生成。配置页面上的链接会将您指向“规则”(Rules) 页面上的敏感数据规则的过滤视图，可以在其中启用和禁用规则以及配置其他规则属性。

保存对入侵策略所做的更改时，如果与数据类型相关的规则已启用且敏感数据检测已禁用，可以选择自动启用敏感数据预处理器。

提示 敏感数据预处理器可以检测使用 FTP 或 HTTP 上传和下载的未加密 Microsoft Word 文件中的敏感数据；之所以可以这样，大概是因为 Word 文件单独分组 ASCII 文本和格式命令的方式。

系统不会检测经过加密的或模糊的敏感数据，也不会检测压缩或编码格式（例如 Base64 编码邮件附件）的敏感数据。例如，系统会检测电话号码 (555)123-4567，但不会检测该号码经过模糊处理的版本，即，每个数字用空格分开，例如 (5 5 5) 1 2 3 - 4 5 6 7，或者通过 HTML 代码介入，例如 (555)-123-4567。但是，系统会检测采用 HTML 代码的号码 (555)-123-4567，在该号码中，没有介入代码中断编号模式。

全局敏感数据检测选项

全局敏感数据选项是特定于策略的并适用于所有数据类型。

掩码

在触发数据包中用 X 替换信用卡号或社会保障号的最后四位数。掩码数字显示在 Web 界面中的入侵事件数据包视图中和下载的数据包中。

网络

指定监控敏感数据的目标主机。可以指定单个 IP 地址、地址块或者 IP 地址和/或地址块的逗号分隔列表。系统会将空白字段解读为任意 (any)，意指任何目标 IP 地址。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

全局阈值 (Global Threshold)

指定在生成全局阈值事件之前，预处理器必须在任何组合中检测的单个会话中所有数据类型出现的总次数。可以指定 1 至 65535 之间的数字。

思科建议将此选项的值设置为大于在策略中启用的任何单个数据类型的最高阈值。

关于全局阈值，请注意：

- 必须启用预处理器规则 139:1 才能检测并生成事件并在内联部署中丢弃攻击性数据包关于数据类型出现次数的事件。
- 在每个会话中，预处理器最多生成一个全局阈值事件。
- 全局阈值事件与具体数据类型事件无关；也就是说，预处理器会在达到全局阈值时生成事件，而不管任何具体数据类型的事件阈值是否达到，反之亦然。

单个敏感数据类型选项

每种自定义数据类型至少必须指定一个事件阈值和至少一个要监控的端口或应用协议。

每种系统提供的预定义数据类型使用一种其他方法无法访问的 `sd_pattern` 关键字来定义用于在流量中进行检测的内置数据模式。您还可以创建自定义数据类型，然后可以使用简单的正则表达式为这些数据类型指定自己的数据模式。

敏感数据类型显示在“敏感数据检测”(Sensitive Data Detection) 功能已启用的所有入侵策略中。系统提供的数据类型显示为只读。对于自定义数据类型，名称和模式字段显示为只读，但是可以将其他选项设置为策略特定的值。

在多域部署中，系统会显示在当前域中创建的敏感数据类型，您可以对其进行编辑。系统还会显示在祖先域中创建的数据类型，您可以通过有限的方式对其进行编辑。对于祖先数据类型，名称和模式字段显示为只读，但是可以将其他选项设置为策略特定的值。

表 *182:* 单个数据类型选项

选项	说明
数据类型	指定数据类型的唯一名称。
阈值	指定系统生成事件时数据类型出现的次数。可以指定 1 至 255 之间的数字。 请注意，在每个会话中，预处理器为检测到的数据类型生成一个事件。另请注意，全局阈值事件与具体数据类型事件无关；也就是说，预处理器会在达到数据类型事件阈值时生成事件，而不管全局事件阈值是否达到，反之亦然。
目标端口 (Destination Ports)	为数据类型指定要监控的目标端口。可以指定单个端口、端口的逗号分隔列表或 `any`（表示任何目标端口）。
应用协议	最多可以为数据类型指定八个要监控的应用协议。必须激活应用检测器来识别要监控的应用协议。 请注意，对于典型设备，此功能需要控制许可证。
模式	指定要检测的模式。此字段仅为自定义数据类型提供。

相关主题

激活和停用检测器，第 1962 页

系统提供的敏感数据类型

每个入侵策略包括用于检测常用数据模式的系统提供的数据类型，例如，信用卡号、邮箱地址、美国电话号码以及带有和不带破折号的美国社会保障号。

每种系统提供的数据类型都与一个生成器 ID (GID) 为 138 的敏感数据预处理器规则相关联。必须启用入侵策略中的关联敏感数据规则才能为要用于策略中的每种数据类型生成事件并在内联部署中丢弃攻击性数据包。

下表介绍每个数据类型并列出了相应的预处理器规则

表 *183:* 系统提供的敏感数据类型

数据类型	说明 (Description)	预处理器规则
信用卡号	匹配 15 位和 16 位数字的 Visa®、MasterCard®、Discover® 和 American Express® 信用卡号（无论是否带正常分隔破折号或空格）；也可以使用 Luhn 算法来验证信用卡校验位。	138:2
邮箱地址	匹配邮箱地址。	138:5
美国电话号码 (U.S. Phone Numbers)	匹配符合 `(\d{3}) ?\d{3}-\d{4}` 模式的美国电话号码。	138:6
不带破折号的美国社会保障号 (U.S. Social Security Numbers Without Dashes)	匹配包含有效的 3 位数区域号码、有效的 2 位数群组号码且不带破折号的 9 位数美国社会保障号。	138:4
带破折号的美国社会保障号 (U.S. Social Security Numbers With Dashes)	匹配包含有效的 3 位数区域号码、有效的 2 位数群组号码且带破折号的 9 位数美国社会保障号。	138:3

为了减少对社会保障号以外的 9 位数号码的误报，预处理器使用一种算法来验证 3 位数区域号码和 2 位数群组号码；在每个社会保障号中，这两组号码位于 4 位数序列号的前面。预处理器可验证 2009 年 11 月之前的社会保障号中的群组号码。

敏感数据检测的许可证要求

威胁防御 许可证

IPS

经典许可证

保护，或如程序中所示。

敏感数据检测的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

配置敏感数据检测

由于敏感数据检测可能会对系统的性能产生重大影响，思科建议遵循以下准则：

- 选择“无活动规则”(No Rules Active) 默认策略作为基本入侵策略。
- 确保在相应的网络分析策略中已启用以下设置：
  - 应用层预处理器 **(Application Layer Preprocessors)** 下的 **FTP** 和 **Telnet** 配置 **(FTP and Telnet Configuration)**。
  - **Transport/Network Layer Preprocessors** 下的 **IP Defragmentation** 和 **TCP Stream Configuration**。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

开始之前

对于典型设备，此程序需要 保护 或 控制 许可证。

过程

步骤 1 选择 **策略** > **访问控制** > **入侵**

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 如果**特定威胁检测 (Specific Threat Detection)** 下的**敏感数据检测 (Sensitive Data Detection)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**敏感数据检测 (Sensitive Data Detection)** 旁边的 **编辑**（）。

步骤 6 有以下选项可供选择：

- 修改全局设置，如全局敏感数据检测选项，第 1628 页中所述。
- 在**目标 (Targets)** 部分中选择数据类型，然后修改数据类型配置，如单个敏感数据类型选项，第 1629 页中所述。
- 如果要检查自定义敏感数据，请创建自定义数据类型；请参阅自定义敏感数据类型，第 1633 页。

步骤 7 为数据类型添加或删除要监控的应用协议；请参阅受监控应用协议和敏感数据，第 1632 页。

注释 要检测 FTP 流量中的敏感数据，必须添加 `Ftp data` 应用协议。

如果需要检测 FTP 流量中的敏感数据，请确保访问控制策略已启用文件策略。

步骤 8 或者，要显示敏感数据预处理器规则，请点击**配置敏感数据检测的规则 (Configure Rules for Sensitive Data Detection)**。

可以启用或禁用所列的任何规则。还可以为 Rules 页面上可用的任何其他操作（例如规则抑制、基于速率的攻击防御，等等）配置敏感数据规则；有关详细信息，请参阅入侵规则类型，第 1474 页。

步骤 9 要保存自上次策略提交以来在此策略中进行的更改，请点击导航面板中的**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在策略中启用敏感数据预处理器规则而未启用敏感数据检测，在保存策略更改时，系统会提示启用敏感数据检测。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 如果要生成入侵事件，请启用敏感数据检测规则 138:2、138:3、138:4、138:5、138:6、138:>999999 或 139:1。有关详细信息，请参阅入侵规则状态，第 1487 页、全局敏感数据检测选项，第 1628 页、系统提供的敏感数据类型，第 1630 页和自定义敏感数据类型，第 1633 页。
- 部署配置更改。

相关主题

特殊情况：FTP 流量中的敏感数据检测，第 1633 页

受监控应用协议和敏感数据

最多可以为每种数据类型指定八个应用协议进行监控。必须为选择的每个应用协议至少启用一个检测器。默认情况下，系统提供的所有检测器均已激活。如果没有为应用协议启用检测器，则系统会

为该应用自动启用所有系统提供的检测器；如果不存在检测器，则系统为该应用启用最新修改的用户定义的检测器。

必须为每种数据类型至少指定一个要监控的应用协议或端口。但是，除了要检测 FTP 流量中的敏感数据的情况之外，思科建议在指定应用协议时指定相应的端口，以便实现最全面覆盖。例如，如果指定 HTTP，还可以配置通用的 HTTP 端口 80。如果网络上的新主机实施 HTTP，系统会在其发现新 HTTP 应用协议的时间间隔内监控端口 80。

如果要检测 FTP 流量中的敏感数据，必须指定 `FTP data` 应用协议；在这种情况下，指定端口号没什么好处。

相关主题

激活和停用检测器，第 1962 页
特殊情况：FTP 流量中的敏感数据检测，第 1633 页

特殊情况：FTP 流量中的敏感数据检测

通常，可通过指定要监控的端口或在部署中指定应用协议来确定要监控敏感数据的流量。

但是，对于检测 FTP 流量中的敏感数据来说，指定端口或应用协议并不足够。在 FTP 应用协议的流量中找到 FTP 流量中的敏感数据，这种情况间歇出现并使用临时端口号，因此难以检测。要检测 FTP 流量中的敏感数据，**必须**在配置中包括以下几项：

- 指定 `FTP 数据 (FTP data)` 应用协议以启用 FTP 流量中的敏感数据检测。

  对于检测 FTP 流量中的敏感数据这种特殊情况，指定 `FTP data` 应用协议不会调用检测功能；而是会调用 FTP/Telnet 预处理器的快速处理功能来检测 FTP 流量中的敏感数据。

- 确保 FTP Data 检测器已启用（默认情况下已启用）。
- 确保配置包括至少一个要监控敏感数据的端口。
- 确保为访问控制策略启用了文件策略。

请注意，不需要指定 FTP 端口（只要检测 FTP 流量中的敏感数据这种罕见情况除外）。大多数敏感数据配置将包括其他端口（例如 HTTP 或邮件端口）。如果只要指定一个 FTP 端口进行监控，思科建议指定 FTP 命令端口 `23`。

相关主题

FTP/Telnet 解码器，第 2083 页
激活和停用检测器，第 1962 页
配置敏感数据检测，第 1631 页

自定义敏感数据类型

创建的每种自定义数据类型还会创建一个敏感数据预处理器规则，该规则的生成器 ID (GID) 为 138，Snort ID (SID) 为大于或等于 1000000（也就是本地规则的 SID）。

必须启用关联的敏感数据规则才能为要用于策略中的每种自定义数据类型启用检测、生成事件并在内联部署中丢弃攻击性数据包。

为了帮助启用敏感数据规则，配置页面上的链接会将您指向入侵策略“规则”(Rules) 页面的过滤视图，其中显示所有系统提供和自定义的敏感数据规则。您还可以通过在入侵策略“规则”(Rules) 页面上选择本地过滤类别，使自定义敏感数据规则与任何自定义本地规则一起显示。请注意，自定义敏感数据规则不会列于入侵规则编辑器页面（**对象** > **入侵规则**）。

创建自定义数据类型后，您可以在系统中的任何入侵策略或多域部署中的当前域中启用该自定义数据类型。要启用自定义数据类型，必须在要用于检测该自定义数据类型事件的任何策略中启用关联敏感数据规则。

自定义敏感数据类型中的数据模式

可使用一组由以下部分组成的简单正则表达式来定义自定义数据类型的数据模式：

- 三个元字符
- 允许将元字符用作原义字符的转义字符
- 六个字符类

元字符是在正则表达式中具有特殊含义的原义字符。

表 *184:* 敏感数据模式元字符

元字符	说明 (Description)	示例
?	匹配前面的字符或转义序列零次或一次；也就是说，前面的字符或转义序列是可选的。	`Colou?r` 匹配 `color` 或 `colour`
{n}	匹配前面的字符或转义序列 n 次。	例如，`\d{2}` 匹配 `55`、`12` 等；`\l{3}` 匹配 `AbC`、`www` 等；`\w{3}` 匹配 `a1B`、25C 等；`x{5}` 匹配 `xxxxx`
\	元字符可用作实际字符，还可用于指定预定义的字符类。	`\?` 匹配问号，`\\` 匹配反斜杠，`\d` 匹配数字字符等

必须将反斜杠用于转义某些字符，这样敏感数据预处理器才能将它们正确解释为原义字符。

表 *185:* 转义敏感数据模式字符

使用的转义字符...	代表的原义字符...
\?	?
\{	{
\}	}
\\	\

在定义自定义敏感数据模式时，可以使用字符类。

表 *186:* 敏感数据模式字符类

字符类	说明	字符类定义
\d	匹配任何 ASCII 数字字符 0-9	0-9
\D	匹配不是 ASCII 数字字符的任何字节	不是 0-9
\l（小写“ell”）	匹配任何 ASCII 字母	a-zA-Z
\L	匹配不是 ASCII 字母的任何字节	不是 a-zA-Z
\w	匹配任何 ASCII 字母数字字符 请注意，与 PCRE 正则表达式不同，此项不包括下划线 (_)。	a-zA-Z0-9
\W	匹配不是 ASCII 字母数字字符的任何字节	不是 a-zA-Z0-9

预处理器将直接输入（而不是作为正则表达式的一部分输入）的字符视为原义字符。例如，数据模式 1234 匹配 `1234`。

以下数据模式示例（用于系统提供的敏感数据规则 138:4）使用转义的数字字符类、乘数和选项说明符元字符、文字破折号 (-) 和左右括号 () 字符来检测美国电话号码：

```
(\d{3}) ?\d{3}-\d{4}
```

创建自定义数据模式时务必谨慎。考虑将下列备选数据模式用于检测电话号码，尽管使用的是有效语法，但可能会导致许多误报：

```
(?\d{3})? ?\d{3}-?\d{4}
```

由于第二个示例结合了可选括号、可选空格和可选破折号，它会在下列所需模式中检测电话号码及其他方面：

- `(555)123-4567`
- `555123-4567`
- `5551234567`

但是，除此之外，第二个示例模式还会检测以下可能无效的模式及其他方面，从而造成误报：

- `(555 1234567`
- `555)123-4567`
- `555) 123-4567`

最后举一个极端的例子（仅作说明用途）：创建一种数据模式，用以在小型企业网络上的所有目标流量中使用一个低事件阈值来检测小写字母 a。这种数据模式可能在短短几分钟内生成数百万的事件，令系统不堪重负。

配置自定义敏感数据类型

在多域部署中，系统会显示在当前域中创建的敏感数据类型，您可以对其进行编辑。系统还会显示在祖先域中创建的数据类型，您可以通过有限的方式对其进行编辑。对于祖先数据类型，名称和模式字段显示为只读，但是可以将其他选项设置为策略特定的值。

如果在任何入侵策略中启用某个数据类型的敏感数据规则，则不能删除该数据类型。

过程

步骤 1 选择 **策略** > **访问控制** > **入侵**

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 如果**特定威胁检测 (Specific Threat Detection)** 下的**敏感数据检测 (Sensitive Data Detection)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**敏感数据检测 (Sensitive Data Detection)** 旁边的 **编辑**（  ）。

步骤 6 点击**数据类型 (Data Types)** 旁边的 **添加**（）。

步骤 7 输入数据类型的名称。

步骤 8 输入要使用此数据类型检测的模式；请参阅自定义敏感数据类型中的数据模式，第 1634 页。

步骤 9 点击 **OK**。

步骤 10 或者，点击数据类型名称，并修改单个敏感数据类型选项，第 1629 页中所述的选项。

步骤 11 或者，通过点击 **删除**（  ） 删除自定义数据类型，然后点击**确定 (OK)** 以确认。

注释 如果在任何入侵规则中启用该数据类型的敏感数据规则，则系统会发出警告，表明不能删除该数据类型。再次尝试删除之前，必须禁用受影响策略中的敏感数据规则；请参阅设置入侵规则状态，第 1488 页。

步骤 12 要保存自上次策略提交以来在此策略中进行的更改，请点击导航面板中的**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 在要使用该数据类型的每个策略中启用关联的自定义敏感数据预处理规则；请参阅设置入侵规则状态，第 1488 页。
- 部署配置更改。

相关主题

编辑自定义敏感数据类型，第 1637 页

编辑自定义敏感数据类型

您可以编辑自定义敏感数据类型中的所有字段。但请注意，当修改名称或模式字段时，这些设置在系统上的所有入侵策略中都会更改。可以将其他选项设置为策略特定值。

在多域部署中，系统会显示在当前域中创建的敏感数据类型，您可以对其进行编辑。系统还会显示在祖先域中创建的数据类型，您可以通过有限的方式对其进行编辑。对于祖先数据类型，名称和模式字段显示为只读，但是可以将其他选项设置为策略特定的值。

过程

步骤 1 选择 **策略 > 访问控制 > 入侵**

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 如果**特定威胁检测 (Specific Threat Detection)** 下的**敏感数据检测 (Sensitive Data Detection)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**敏感数据检测 (Sensitive Data Detection)** 旁边的**编辑 (Edit)**。

步骤 6 在**目标 (Targets)** 部分中，点击自定义数据类型的名称。

步骤 7 点击**编辑数据类型名称和模式 (Edit Data Type Name and Pattern)**。

步骤 8 修改数据类型名称和模式；请参阅自定义敏感数据类型中的数据模式，第 1634 页。

步骤 9 点击 **OK**。

步骤 10 将其余选项设置为策略特定值；请参阅单个敏感数据类型选项，第 1629 页。

步骤 11 要保存自上次策略提交以来在此策略中进行的更改，请点击导航面板中的**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

第 67 章

入侵事件日志记录的全局限制

以下主题介绍如何全局限制入侵事件日志记录：

全局规则阈值基础知识

全局规则阈值为入侵策略记录的事件设置了限制。您可以跨所有流量设置全局规则阈值，用于限制策略在每个指定时间段记录和显示来自特定源地址或目标地址的事件的频率。您还可以根据策略中的共享对象规则、标准文本规则或预处理器规则设置阈值。设置全局阈值后，该阈值将应用于策略中没有特定阈值可覆盖该阈值的每条规则。阈值可以防止因事件数量过多而使系统不堪重负。

每个入侵策略包含一个默认应用于所有入侵规则和预处理器规则的默认全局规则阈值。此默认阈值将发往目标地址的流量的事件数限制为每 60 秒一个事件。

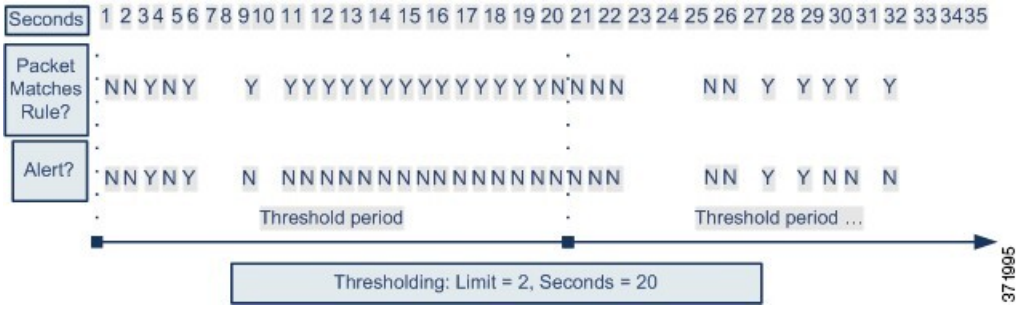
您可以执行以下操作：

- 更改全局阈值。
- 禁用全局阈值。
- 通过为特定规则设置单独的阈值来覆盖全局阈值。

  例如，可将全局限值阈值设置为每 60 秒生成五个事件，然后为 SID 1315 设置每 60 秒生成十个事件的特定阈值。所有其他规则每 60 秒生成的事件不超过五个，但是系统每 60 秒可为 SID 1315 生成多达十个事件。

提示 在有多个 CPU 的受管设备上，全局阈值或单独的阈值可能会导致事件数量高于预期。

下图展示了全局规则阈值的工作方式。在此示例中，系统正受到违反特定规则的攻击。全局限值阈值设置为将每条规则的事件生成频率限制为每 20 秒生成两个事件。请注意，该时间段在 1 秒时开始，在21秒时结束。该时间段结束后，时间周期重新开始，接下来两次规则匹配生成了事件，随后系统在这一时间段内不再生成事件。



全局规则阈值选项

默认阈值将每条规则的事件生成频率限制为对发往同一个目标地址的流量每60秒生成一个事件。全局规则阈值选项的默认值如下：

- **类型 (Type)** -“限制”(Limit)
- **跟踪依据 (Track By)** -“目标”(Destination)
- **计数 (Count)** - 1
- **秒数 (Seconds)** - 60

您可以如下修改这些默认值：

表 *187:* 阈值类型

选项	说明
限制	为指定时间段内触发规则的指定数量的数据包（由 count 参数指定）记录并显示事件。 例如，如果将类型设置为**限制 (Limit)**，将**计数 (Count)** 设置为 `10`，并将**秒数 (Seconds)** 设置为 `60`，而同一分钟内有 14 个数据包触发规则，则系统在显示发生的前 10 个违反该规则的事件后将停止记录违反该规则的事件。
阈值 (Threshold)	在指定时间段内，当指定数量的数据包（由 count 参数指定）触发规则时，记录并显示一个事件。请注意，达到事件阈值计数且系统记录该事件之后，时间计数器将重新开始计数。 例如，将类型设置为**阈值 (Threshold)**，将**计数 (Count)** 设置为 `10`，并将**秒数 (Seconds)** 设置为 `60` 时，如果到 33 秒时规则触发 10 次，系统将生成一个事件，然后将“秒数”(Seconds) 和“计数”(Count) 计数器重置为 `0`。其后，该规则在接下来 25 秒内又触发 10 次。由于计数器在第 33 秒时已重置为 `0`，因此系统此时会再记录一个事件。

选项	说明
双向	每个指定时间段在指定数量（计数）的数据包触发规则后记录并显示一次事件。 例如，如将类型设置为**两者 (Both)**，将**计数 (Count)** 设置为 `2`，将**秒数 (Seconds)** 设置为 `10`，则事件计数结果如下： • 如果 10 秒内触发规则一次，系统不会生成任何事件（未达到阈值） • 如果 10 秒内触发规则两次，系统将生成一个事件（第二次触发规则时达到阈值） • 如果 10 秒内触发规则四次，系统将生成一个事件（第二次触发规则时达到阈值，忽略其后的事件）

跟踪依据 (Track By) 选项确定事件实例计数是按源 IP 地址计算还是按目标 IP 地址计算。

您还可以如下指定用于定义阈值的实例数和时间段：

表 *188:* 阈值实例/时间选项

选项	说明
计数	对于**限制 (Limit)** 阈值，是指每个跟踪 IP 地址或地址范围在每个指定时间段内达到阈值所需的事件实例数。 对于**阀值 (Threshold)** 阈值，是指要用作阈值的规则匹配项的数量。
秒	对于**限制 (Limit)** 阈值，是指组成跟踪攻击的时间段的秒数。 对于**阀值 (Threshold)** 阈值，是指计数重置之前经过的秒数。如果将阈值类型设置为**限制 (Limit)**，将跟踪设置为**源 (Source)**，将**计数 (Count)** 设置为 10，并将**秒数 (Seconds)** 设置为 10，则系统将记录并显示 10 秒钟内发生的来自指定源端口的前 10 个事件。如果前 10 秒内只发生了 7 个事件，系统将记录并显示这些事件，而如果前 10 秒内发生了 40 个事件，系统将记录并显示 10 个事件，然后在为期 10 秒的时间段过后重新开始计数。

相关主题

配置全局阈值，第 1642 页
入侵事件阈值，第 1489 页

全局阈值的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

全局阈值的要求和必备条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

配置全局阈值

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 如果**入侵规则阈值 (Intrusion Rule Thresholds)** 下的**全局规则阈值** （**Global Rule Thresholding**） 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**全局规则阈值 (Global Rule Thresholding)** 旁边的 **编辑**（  ）。

步骤 6 使用**类型 (Type)**，指定在**秒数 (Seconds)** 字段中指定的时间内将应用的阈值类型。

步骤 7 使用**跟踪方式 (Track By)**，请指定跟踪方式。

步骤 8 在**计数 (Count)** 字段中输入值。

步骤 9 在**秒数 (Seconds)** 字段中输入值。

步骤 10 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

相关主题

全局规则阈值选项，第 1640 页
配置层中的入侵规则，第 1616 页
冲突和更改：网络分析和入侵策略，第 1459 页

禁用全局阈值

如果要为特定规则的事件设置阈值而不是将阈值默认应用于每条规则，则可以在最高策略层禁用全局阈值。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择 **策略** > **访问控制** > **入侵**

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 点击**入侵规则阈值 (Intrusion Rule Thresholds)** 下的**全局规则阈值 (Global Rule Thresholding)** 旁边的**已禁用 (Disabled)**。

步骤 5 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

相关主题

冲突和更改：网络分析和入侵策略，第 1459 页
配置层中的入侵规则，第 1616 页

第 68 章

入侵防御性能调整

以下主题介绍如何优化入侵防御性能：

关于入侵防御性能调整

思科提供多项功能，用于提高系统在分析流量中的入侵企图时的性能。您可以执行以下操作：

- 指定事件队列中允许的数据包数量。您还可以在数据流重组前后，启用或禁用对将重建到更大数据流中的数据包进行的检测。
- 覆盖入侵规则中使用的 PCRE 默认匹配和递归限制以检查数据包负载内容。
- 选择使规则引擎在生成多个事件时为每个数据包或数据包流记录多个事件，使您可以收集报告事件之外的信息。
- 在安全和通过数据包及规则延迟阈值将设备延迟保持在可接受水平的需求之间保持平衡。
- 配置设备如何监控和报告其自身性能的基本参数。这样，您可以指定系统更新设备上的性能统计信息的间隔。

可以基于每个访问控制策略配置这些性能设置，他们可应用于该父访问控制策略调用的所有入侵策略。

入侵防御性能调整的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

入侵防御性能调整的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

限制入侵的模式匹配

过程

步骤 1 在访问控制策略编辑器中，点击 **高级**。

在新 UI 中，从数据包流行末尾的下拉箭头中选择**高级设置 (Advanced Settings)**。

步骤 2 点击**性能设置 (Performance Settings)** 旁边的 **编辑**（）。

如果显示**视图**（），则表明设置继承自祖先策略，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 3 点击**性能设置 (Performance Settings)** 弹出窗口中的**模式匹配限制 (Pattern Matching Limits)**。

步骤 4 在**每个数据包要分析的最大模式状态数 (Maximum Pattern States to Analyze Per Packet)** 字段中输入要加入队列的最大事件数的值。

步骤 5 要在 Snort 2 中禁用在数据流重组前后将重建为更大数据流的数据包的检查，请选中**对有待未来重组的流量禁用内容检查 (Disable Content Checks on Traffic Subject to Future Reassembly)** 复选框。重组前后的检测需要更多的处理开销，可能会导致性能下降。

重要事项 在 Snort 3 中，**对未来重组的流量禁用内容检查 (Disable Content Checks on Traffic Subject to Future Reassembly)** 复选框的设置包括：

- 选中 - 表示会在重组前检测 TCP 负载。它包括数据流重组前后的数据包检测。这一过程需要更多的处理开销，并且可能会降低性能。
- 未选中 - 表示在重组后检测 TCP 负载。

步骤 6 点击**确定 (OK)**。

步骤 7 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改。

入侵规则的正则表达式限制覆盖

默认正则表达式限制可确保最低性能级别。覆盖这些限制可能会提高安全性，但也会因允许根据低效的正则表达式对数据包进行评估而严重影响性能。

⚠

注意 除非在撰写入侵规则方面很有经验，并且了解衰减模式的影响，否则，不要覆盖默认的PCRE限制。

表 *189:* 正则表达式限制选项

选项	说明
匹配限制状态 (Match Limit State)	指定是否覆盖**匹配限制 (Match Limit)**。您有以下选择： • 选择**默认值 (Default)**，以使用为**匹配限制 (Match Limit)** 配置的值 • 选择 **Unlimited**，以允许不限次数的尝试 • 选择**自定义 (Custom)**，为**匹配限制 (Match Limit)** 指定 1 或更大的值，或指定 0 以彻底禁用 PCRE 匹配评估
匹配限制 (Match Limit)	指定在与 PCRE 正则表达式中定义的模式进行匹配时的尝试次数。

选项	说明
匹配递归限制状态 (Match Recursion Limit State)	指定是否覆盖**匹配递归限制 (Match Recursion Limit)**。您有以下选择： • 选择**默认值 (Default)**，以使用为**匹配递归限制 (Match Recursion Limit)** 配置的值 • 选择**无限制 (Unlimited)**，以允许进行次数不限的递归 • 选择**自定义 (Custom)**，为**匹配递归限制 (Match Recursion Limit)** 指定 1 或更大的值，或指定 0 以彻底禁用 PCRE 递归 注意：为使**匹配递归限制 (Match Recursion Limit)** 具有意义，其值必须小于**匹配限制 (Match Limit)**。
匹配递归限制 (Match Recursion Limit)	指定在根据数据包静载荷对 PCRE 正则表达式进行评估时的递归次数。

相关主题

概述：pcre 关键字，第 1538 页

覆盖入侵规则的正则表达式限制

过程

步骤 1 在访问控制策略编辑器中，点击 **高级**。

在新 UI 中，从数据包流行末尾的下拉箭头中选择**高级设置 (Advanced Settings)**。

步骤 2 点击**性能设置 (Performance Settings)** 旁边的 **编辑**（）。

如果显示**视图**（），则表明设置继承自祖先策略，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 3 点击**性能设置 (Performance Settings)** 弹出窗口中的**正则表达式限制 (Regular Expression Limits)**。

步骤 4 您可以修改入侵规则的正则表达式限制覆盖，第 1647 页中所述的任何选项。

步骤 5 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改。

每个数据包的入侵事件生成限制

当入侵规则引擎根据规则评估流量时，它会将针对给定数据包或数据包流生成的事件放在事件队列中，然后将队列顶部的事件报告至用户界面。配置入侵事件日志记录限制时，可指定队列中可放置的事件数量及要记录的事件数量，并可选择确定队列中事件顺序的条件。

表 *190:* 入侵事件日志记录限制选项

选项	说明
Maximum Events Stored Per Packet	为给定数据包或数据包流可存储的最多事件数量。
Maximum Events Logged Per Packet	为给定数据包或数据包流记录的事件数量。这不能超过**每个数据包存储的最大事件数量 (Maximum Events Stored Per Packet)** 的值。
事件日志记录的优先排列方式 (Prioritize Event Logging By)	用于确定事件队列内事件排序的值。通过用户界面报告排序最靠前的事件。您可以选择以下选项： • `优先级 (priority)`，按事件的优先级对队列中的事件进行排序。 • `content_length`，按识别出的最长匹配内容对事件进行排序。当事件按内容长度排序时，规则事件始终优先于解码器和预处理程序事件。

限制每个数据包生成的入侵事件

过程

步骤 1 在访问控制策略编辑器中，点击 **高级**。

在新 UI 中，从数据包流行末尾的下拉箭头中选择**高级设置 (Advanced Settings)**。

步骤 2 点击**性能设置 (Performance Settings)** 旁边的 **编辑**（）。

如果显示**视图**（），则表明设置继承自祖先策略，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 3 点击**性能设置 (Performance Settings)** 弹出窗口中的**入侵事件日志记录限制 (Intrusion Event Logging Limits)**。

步骤 4 可以修改每个数据包的入侵事件生成限制，第 1649 页中的任何选项。

步骤 5 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改。

数据包和入侵规则延迟阈值配置

每个访问控制策略都具有基于延迟的设置，这些设置使用阈值来管理数据包和规则处理性能。

数据包延迟阈值用于度量适用的解码器、预处理程序和规则在处理数据包时所需的总时间，并在处理时间超过可配置阈值时停止对数据包的检测。

规则延迟阈值功能可以衡量每个规则处理各个数据包所花费的时间、将超过阈值的规则及一系列相关规则暂停指定的时间（如果处理时间连续超过规则延迟阈值一定次数 [可配置]），以及在暂停到期后恢复规则。

基于延迟的性能设置

默认情况下，系统会从已在系统中部署的最新入侵规则更新中获取基于延迟的性能设置。

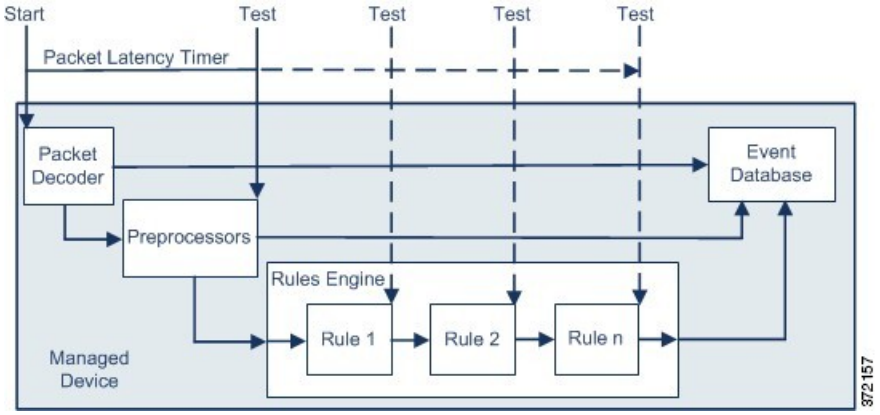
实际应用的延迟设置取决于与访问控制策略关联的网络分析策略 (NAP) 的安全级别。通常，这是指默认 NAP 策略。但是，如果已配置自定义网络分析规则，并且其中任意一个规则指定的 NAP 策略安全级别都高于默认 NAP 策略，则延迟设置取决于自定义规则中安全级别最高的 NAP 策略。如果默认 NAP 策略或任何自定义规则调用自定义 NAP 策略，则评估中使用的安全级别是每个自定义 NAP 策略所基于的系统提供的基本策略。

不论有效阈值和/或网络分析配置直接在策略中继承还是配置，上述情况均成立。

数据包延迟阈值

数据包延迟阈值度量所需时间，而不仅是处理时间，目的是为了更准确地反映规则在处理数据包时实际所需的时间。然而，延迟阈值功能是基于软件实现的延迟管理功能，并不能实施严格的定时功能。

性能与源自延迟阈值的延迟优势的权衡取舍在于未经检查的数据包可能包含攻击。解码器处理开始时，每个数据包的计时器开始计时。计时器会持续计时，直到数据包的所有处理工作结束或处理时间在计时测试点超过阈值。



如上图所示，数据包延迟计时在以下测试点测试：

- 在所有解码器和预处理器的处理完成之后且在规则处理开始之前
- 在每条规则的处理之后

如果处理时间在任何测试点超出阈值，数据包检测将停止。

提示 总的数据包处理时间不包括常规的 TCP 数据流或 IP 分片重组时间。

对于由处理数据包的解码器、预处理器或规则所触发的事件，数据包延迟阈值不会对其产生影响。只有当数据包已完全处理完毕，或当数据包处理因超过了延迟阈值而终止时（以先出现者为准），任何适用的解码器、预处理器或规则才会触发事件。如果丢弃规则在内联部署中检测到入侵，则丢弃规则将触发事件并将数据包丢弃。

注释 只有当数据包的处理因超出数据包延迟阈值而停止后，才会根据规则评估数据包。本可触发事件的规则无法触发该事件，同时，丢弃规则无法丢弃该数据包。

通过停止对要求过长处理时间的数据包进行的检查，数据包延迟阈值可提高被动和内联部署模式下的系统性能，并可缩短内联部署中的延迟。例如，这些性能优势可以在以下情形中发挥出来：

- 无论是被动式部署还是内嵌式部署，多个规则连续检测数据包都需要大量时间
- 对于内联式部署，网络性能不佳（例如，当有人下载超大文件时）期间，数据包处理变慢。

在被动式部署中，停止数据包的处理可能无助于恢复网络性能，这是因为，只不过转至处理下一数据包而已。

数据包延迟阈值说明

默认情况下，用于数据包处理的基于延迟的性能设置会被禁用。您可以选择将其启用。但是，思科建议您不要更改阈值设置的默认值。

仅当您选择指定自定义值时，以下信息才适用。

表 *191:* 数据包延迟阈值选项

选项	说明
阀值（微秒）(Threshold [microseconds])	指定数据包检测停止的时间，以微秒为单位。

启用数据包延迟阈值

过程

步骤 1 在访问控制策略编辑器中，点击 **高级**。

在新 UI 中，从数据包流行末尾的下拉箭头中选择**高级设置 (Advanced Settings)**。

步骤 2 点击**基于延迟的性能设置 (Latency-Based Performance Settings)** 旁边的 **编辑**（）。

如果显示**视图**（），则表明设置继承自祖先策略，或者您没有修改设置的权限。

步骤 3 在**基于延迟的性能设置 (Latency-Based Performance Settings)** 弹出窗口中，点击**数据包处理 (Packet Handling)**。

步骤 4 选中 **Enabled** 复选框。

步骤 5 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改。

配置数据包延迟阈值

默认情况下，用于数据包处理的基于延迟的性能设置会被禁用。您可以选择将其启用。但是，思科建议您不要更改阈值设置的默认值。

过程

步骤 1 在访问控制策略编辑器中，点击 **高级**。

在新 UI 中，从数据包流行末尾的下拉箭头中选择**高级设置 (Advanced Settings)**。

步骤 2 点击**基于延迟的性能设置 (Latency-Based Performance Settings)** 旁边的 **编辑**（）。

系统（） > **监控** > **统计信息**

步骤 3 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 4 在**基于延迟的性能设置 (Latency-Based Performance Settings)** 弹出窗口中，点击**数据包处理 (Packet Handling)**。

系统会默认选择**已安装规则的更新 (Installed Rule Update)**。我们建议使用此默认设置。

显示的值未反映出自动设置。

步骤 5 如果您选择指定自定义值：

- 选中**启用 (Enabled)** 复选框，然后查看数据包延迟阈值说明，第 1651 页以了解最低的**阈值 (Threshold)** 设置。
- 您必须在“数据包处理”(Packet Handling) 选项卡和“规则处理”(Rule Handling) 选项卡中指定自定义值。

步骤 6 点击**确定 (OK)**。

步骤 7 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改。

规则延迟阈值

规则延迟阈值度量所需时间，而不仅是处理时间，目的是为了更准确地反映规则在处理数据包时实际所需的时间。然而，延迟阈值功能是基于软件实现的延迟管理功能，并不能实施严格的定时功能。

性能与源自延迟阈值的延迟优势的权衡取舍在于未经检查的数据包可能包含攻击。计时器测量每次根据一组规则处理数据包所用的处理时间。每当规则处理时间超过指定的规则延迟阈值时，系统将使计数器递增。如果连续超过阈值的次数达到指定数值，则系统将采取以下操作：

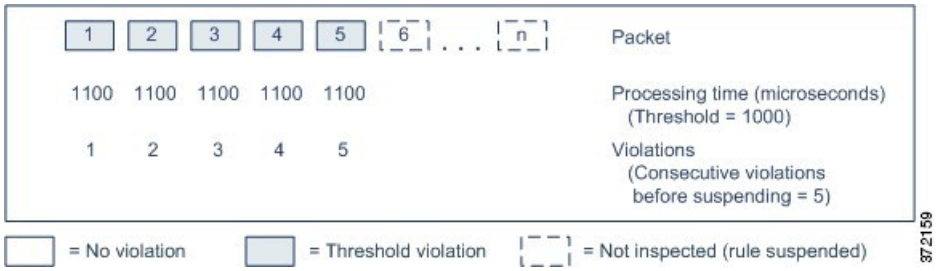
- 在指定时期内暂停规则
- 触发一个事件，指示已暂停规则
- 在暂停到期后重新启用规则
- 触发一个事件，指示已重新启用规则

在已暂停规则组或违反规则的情况不再连续时，系统将使计数器归零。在暂停规则前允许某些连续违反规则的情况，可以使您忽略对性能的影响可以忽略不计的偶然违反规则的情况，转而将重点放在反复超过规则延迟阈值的、更重大的规则影响上。

下面的示例显示了五个连续的规则处理时间，它们并未导致规则暂停。

在上面的示例中，处理前三个数据包中的每个数据包所需的时间都超过了 1000 毫秒的规则延迟阈值，因此违规计数器随着每次违规都会递增。处理第四个数据包并未超过阈值，因此违规计数器复位为零。第五个数据包超过了阈值，因此违规计数器从一重新开始。

下面的示例显示了五个连续的规则处理时间，它们导致了规则暂停。



在第二个示例中，处理五个数据包中的每个数据包所需的时间都超过了1000毫秒的规则延迟阈值。由于对于指定的五次连续违规，每个数据包 1100 毫秒的规则处理时间都超过了 1000 毫秒的阈值，因此该规则组被暂停。不会针对已暂停的规则对任何后续数据包（在该图中表示为数据包 6 至 n）进行检查，直到暂停到期为止。如果在重新启用规则后出现更多数据包，则违规计数器将再次从零开始。

规则延迟阈值处理对处理该数据包的规则所触发的入侵事件没有影响。对于在该数据包中检测到的任何入侵，无论规则处理时间是否超过阈值，规则都会触发事件。如果检测到入侵的规则是内联部署中的丢弃规则，则该数据包将被丢弃。当某一丢弃规则检测到导致该规则被暂停的某一数据包中存在入侵时，该丢弃规则将触发一个入侵事件，该数据包将被丢弃，并且该规则以及所有相关规则都将被暂停。

注释 不会针对已暂停的规则对数据包进行评估。本来能够触发某一事件的规则在被暂停后将无法触发该事件，并且对于丢弃规则，也将无法丢弃数据包。

规则延迟阈值处理可以同时改善被动部署和内联部署中的系统性能，并可通过暂停花费最长时间处理数据包的规则，缩短内联部署中的延迟。不会再次针对已暂停的规则来评估数据包，直到可配置的时间到期为止，为已过载设备提供恢复时间。例如，这些性能优势可以在以下情形中发挥出来：

- 匆忙编写的、大部分未经测试的规则需要大量的处理时间
- 在网络性能较差（如有人下载极大文件）的时段内，将导致数据包检查缓慢

规则延迟阈值说明

默认情况下，数据包和规则处理的基于延迟的性能设置由最新部署的入侵规则更新自动填充，我们建议您不要更改默认设置。

仅当您选择指定自定义值时，本主题中的信息才适用。

如果规则处理数据包时所用时间超过**暂停规则前连续超出阈值的次数 (Consecutive Threshold Violations Before Suspending Rule)** 所指定的连续次数的**阈值 (Threshold)**，则规则延迟阈值就会按**暂停时间 (Suspension Time)** 指定的时间暂停规则。

可启用规则 134:1，当规则已暂停时生成事件；并启用规则 134:2，在启用已暂停规则时生成事件。请参阅入侵规则状态选项，第 1487 页。

表 *192:* 规则延迟阈值选项

选项	说明
阈值 (Threshold)	指定规则在检查数据包时不应超出的时间，以微秒为单位。
暂停规则前连续超出阈值的次数 (Consecutive Threshold Violations Before Suspending Rule)	指定在暂停规则之前，规则可按超过为**阈值 (Threshold)** 设置的时间检查数据包的连续次数。
暂停时间 (Suspension Time)	指定暂停一组规则的秒数。

配置规则延迟阈值

默认情况下，数据包和规则处理的基于延迟的性能设置由最新部署的入侵规则更新自动填充，我们建议您不要更改默认设置。

过程

步骤 1 在访问控制策略编辑器中，点击 **高级**。

在新 UI 中，从数据包流行末尾的下拉箭头中选择**高级设置 (Advanced Settings)**。

步骤 2 点击**基于延迟的性能设置 (Latency-Based Performance Settings)** 旁边的 **编辑**（）。

如果显示**视图**（），则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 3 在**基于延迟的性能设置 (Latency-Based Performance Settings)** 弹出窗口中，点击**规则处理 (Rule Handling)**。

系统会默认选择**已安装规则的更新 (Installed Rule Update)**。我们建议使用此默认设置。

显示的值未反映出自动设置。

步骤 4 如果您选择指定自定义值：

- 可以按规则延迟阈值说明，第 1655 页中所述配置任何选项。
- 您必须在“数据包处理”(Packet Handling) 选项卡和“规则处理”(Rule Handling) 选项卡中指定自定义值。

步骤 5 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)** 保存策略。

下一步做什么

- 如果要生成事件，请启用延迟规则 134:1 和 134:2。有关详细信息，请参阅入侵规则状态选项，第 1487 页。
- 部署配置更改。

入侵性能统计信息日志记录配置

Sample time (seconds) and Minimum number of packets

当过了所指定的性能统计数据更新之间的秒数时，系统验证其已分析的数据包是否到达指定数量。如果到达，则系统更新性能统计数据。否则，系统等待，直到其分析的数据包到达指定的数量。

故障排除选项：日志会话/协议分布 (Troubleshooting Options: Log Session/Protocol Distribution)

支持部门可能要求您在故障排除调用期间记录协议分布、数据包长度和端口统计信息。

⚠

注意 除非有支持人员的指示，否则请勿启用**记录会话/协议分发**。

Troubleshooting Options: Summary

支持部门可能要求您在故障排除调用期间将系统配置为仅在 Snort 进程关闭或重新启动时计算性能统计数据。要启用此选项，也必须启用 **Log Session/Protocol Distribution** 故障排除选项。

⚠

注意 除非有支持人员的指示，否则请勿启用**摘要**。

配置入侵性能统计信息日志记录

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)**，然后点击**性能设置 (Performance Settings)** 旁边的**编辑**（ ）。

在新 UI 中，从数据包流行末尾的下拉箭头中选择**高级设置 (Advanced Settings)**。

如果显示**视图**（ ），则表明设置继承自祖先策略，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 2 点击出现的弹出窗口中的**性能统计信息 (Performance Statistics)**。

步骤 3 如上所述修改 **Sample time** 或 **Minimum number of packets**。

步骤 4 或者，展开 **Troubleshoot Options** 部分并修改这些选项（仅当支持部门要求这样做时）

步骤 5 点击**确定 (OK)**。

下一步做什么

- 部署配置更改。

第 XV 部分

网络恶意软件防护和文件策略

第 69 章

网络恶意软件防护和文件策略

以下主题概述文件控制、文件策略、文件规则、高级恶意软件保护(AMP)、云连接和动态分析连接。

关于网络恶意软件防护和文件策略

要检测和阻止恶意软件，请使用文件策略。您还可以使用文件策略按文件类型来检测和控制流量。

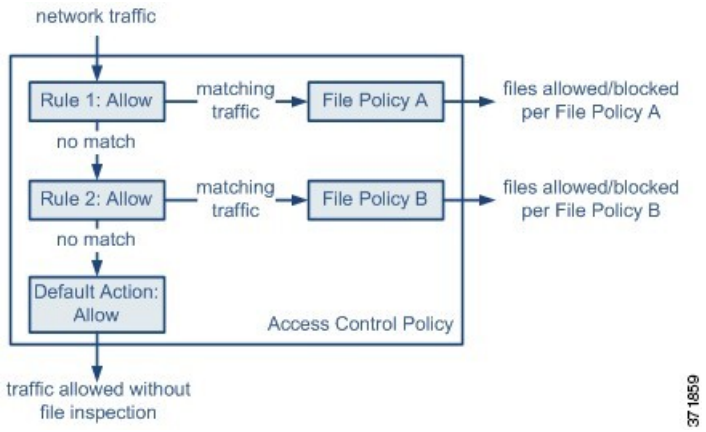
面向 Firepower 的高级恶意软件防护 (AMP) 可以检测、捕获、跟踪、分析、记录并选择性地阻止网络流量中恶意软件的传输。在 Cisco Secure Firewall Management Center Web 界面中，此功能称为恶意软件防护，以前称为面向 *Firepower* 的 *AMP*。思科高级恶意软件保护利用内联部署的托管设备和来自思科云的威胁数据来识别恶意软件。

您可以将文件策略与处理网络流量的访问控制规则作为整体访问控制配置的一部分关联起来。

当系统检测到网络上的恶意软件时，它会生成文件和恶意软件事件。要分析文件和恶意软件事件数据，请参阅《Cisco Secure Firewall Management Center 管理指南》 中的文件/恶意软件事件和网络文件轨迹一章。

文件策略

文件策略是作为整体访问控制配置的一部分供系统用于执行恶意软件保护和文件控制的一组配置。这种关联保证系统在传递流量中与访问控制规则的条件匹配的文件之前，首先检查该文件。在内联部署中，可考虑下图所示的简单访问控制策略。



策略有两个访问控制规则，两者都使用“允许”(Allow)操作并与文件策略关联。策略的默认操作也是允许流量，但不执行文件策略检查。在这种情况下，流量的处理方式如下：

- 与 `Rule 1` 匹配的流量根据 `File Policy A` 进行检查。
- 与 `Rule 1` 不匹配的流量根据 `Rule 2` 进行评估。与 `Rule 2` 匹配的流量根据 `File Policy B` 进行检查。
- 允许与任一规则都不匹配的流量；不能将文件策略与默认操作关联。

通过将不同文件策略与不同访问控制规则相关联，可以精细控制如何识别并阻止网络上传输的文件。

文件策略的要求和必备条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 访问管理员

文件和恶意软件策略许可证要求

要执行此操作	所需许可证	文件规则操作
阻止或允许特定类型的所有文件（例如，阻止all.exe文件）	威胁 （对于 威胁防御 设备） 保护 （适用于传统设备）	允许、阻止、阻止并重置
根据文件包含或可能包含恶意软件的判断，选择性地允许或阻止文件	威胁 （对于 威胁防御 设备） 保护 （适用于传统设备） 恶意软件	恶意软件云查找、阻止恶意软件
存储文件	威胁 （对于 威胁防御 设备） 保护 （适用于传统设备） 恶意软件	选择了 **存储文件** 的任何文件规则操作

有关 恶意软件 许可证的详细信息，请参阅：

- 《Cisco Secure Firewall Management Center 管理指南》中的恶意软件 防御 许可证

文件策略和恶意软件检测的最佳实践

除下述项目外，请按照 如何配置恶意软件防护，第 1666 页 和参考主题中的步骤操作。

文件规则最佳实践

在配置文件规则时，请注意以下准则和限制：

- 配置为在被动部署中阻止文件的规则不会阻止匹配的文件。由于连接继续传输文件，因此如果配置规则以记录连接的开始，则您可能会看到为此连接记录的多个事件。
- 一个策略可以包含多个规则。在创建规则时，请确保没有规则被先前的规则“隐藏”。
- 动态分析支持的文件类型是其他分析类型支持的文件类型的子集。要查看每种分析支持的文件类型，请导航至文件规则配置页面，选择**阻止恶意软件 (Block Malware)** 操作，然后选中所需的复选框。

要确保系统检查所有的文件类型，请为动态分析和其他类型的分析创建单独的规则（在同一策略内）。

- 如果文件规则配置有**恶意软件云查找**或**阻止恶意软件**操作，并且 管理中心无法与 AMP 云建立连接，则系统无法执行任何已配置的规则操作选项，直到恢复连接为止。
- 思科建议启用**重置连接 (Reset Connection)**（适用于**阻止文件 [Block Files]** 和**阻止恶意软件 [Block Malware]** 操作）以防止受阻应用会话保持打开，直到 TCP 连接重置为止。如果不重置连接，则客户端会话会保持打开，直到 TCP 连接重置为止。
- 如果监控大量流量，请**勿**存储所有捕获文件，或者将所有捕获文件提交进行动态分析。否则可能对系统性能产生不利影响。
- 不能对系统检测到的所有文件类型都执行恶意软件分析。从 **Application Protocol**、**Direction of Transfer** 和 **Action** 下拉列表中选择值之后，系统会对文件类型的列表进行约束。

文件检测最佳实践

请考虑文件检测的以下注意事项和限制：

- 如果未启用自适应分析，则访问控制规则无法执行文件控制（包括 AMP）。
- 如果文件与带有应用协议条件的规则相匹配，在系统成功确定该文件的应用协议之后，会生成文件事件。无法识别的文件不生成文件事件。
- FTP 通过不同信道传输命令和数据。在被动或内联分流模式部署中，来自 FTP 数据会话及其控制会话的流量可能不会均衡分摊到同一个内部资源。
- 如果 POP3、POP、SMTP 或 IMAP 会话中文件的所有文件名的总字节数超过 1024，则会话中的文件事件可能无法反映文件名缓冲区填充后检测到的文件的正确文件名。
- 当通过 SMTP 传输基于文本的文件时，某些邮件客户端会将换行符转换为 CRLF 换行符标准。由于基于 MAC 的主机使用回车 (CR) 字符，并且基于 Unix/Linux 的主机使用换行 (LF) 字符，因此，邮件客户端进行的换行可能修改文件的大小。注意某些邮件客户端在处理无法识别的文件类型时默认进行换行。
- 要检测 ISO 文件，请将“限制执行文件类型检测时检查的字节数”选项设置为大于 36870 的值，如文件和恶意软件检测性能和存储选项，第 1693 页中所述。
- 无法检测到某些 .rar 存档中的 .Exe 文件，可能包括 rar5。

文件阻止最佳实践

请考虑文件阻止的以下注意事项和限制：

- 无论使用何种传输协议，如果未检测到文件的文件结尾标记，**Block Malware** 规则或自定义检测列表不会阻止该文件。系统会等待接收整个文件后再阻止文件（如文件结尾标记所指示），并在检测到该标记后阻止文件。

- 如果 FTP 文件传输的文件结尾标记单独从最后一个数据段进行传输，则会阻止该标记，并且 FTP 客户端会指示文件传输失败，但是文件实际上将完整传输到磁盘。
- 具有**阻止文件 (Block Files)** 和**阻止恶意软件 (Block Malware)** 操作的文件规则会阻止通过 HTTP 自动恢复文件下载，方法是在进行初始文件传输尝试后检测到相同的文件、URL、服务器和客户端应用达到 24 小时的情况下阻止新会话。
- 在极少数情况下，如果来自 HTTP 上传会话的流量顺序错误，则系统无法正确重组流量，并因此不会阻止该会话或生成文件事件。
- 如果通过 NetBios-ssn 传输使用**阻止文件 (Block Files)** 规则阻止的文件（例如 SMB 文件传输），则目标主机上可能会显示文件。但是，该文件不可用，原因是在下载启动后阻止了该文件，导致文件传输未完成。
- 如果您创建文件规则来检测或阻止通过 NetBIOS-ssn 传输的文件（例如 SMB 文件传输），系统不会检测正在进行的文件传输。但是，系统会检测部署调用文件策略的访问控制策略后传输的新文件。
- SMB 的多通道功能可以创建 IP 地址相同但端口不同的多个并行会话。对于多通道上的给定事务，文件下载会在未由系统作为单个文件检测的这些会话之间多路复用。
- 系统不会检测单个 TCP 或 SMB 会话中同步传输的文件。
- 在集群环境中，如果现有 SMB 会话因集群角色更改或设备故障而移至新设备，则任何正在传输的文件可能无法得到检测。
- Microsoft Windows 系统之间的一些 SMB 文件传输使用非常高的 TCP 窗口大小来进行快速文件传输。要检测或阻止此类文件传输，建议您增大**网络分析策略 (Network Analysis Policy)** > **TCP 数据流配置 (TCP Stream Configuration)** > **故障排除选项 (Troubleshooting Options)** 下的**最大排队字节数 (Maximum Queued Bytes)** 和**最大排队分段数 (Maximum Queued Segments)** 的值。
- 如果配置了 Firepower 威胁防御高可用性，并且在原始主用设备识别文件时发生故障切换，则文件类型不同步。即使文件策略阻止该文件类型，新的主用设备也会下载该文件。

文件策略最佳实践

在配置文件策略时，请注意以下常规准则和限制：

- 可以将单个文件策略与其操作为**允许 (Allow)**、**交互式阻止 (Interactive Block)** 或**交互式阻止并重置 (Interactive Block with reset)** 的访问控制规则关联。
- 您**不能**使用文件策略检查由访问控制默认操作处理的流量。
- 对于新策略，Web 界面会指出该策略未在使用。如果编辑的是使用中的文件策略，则 Web 界面会告知您使用该文件策略的访问控制策略的数量。在任一情况下，可以点击文本以跳至“访问控制策略”(Access Control Policies) 页面。
- 要使文件阻止起作用，应用于访问控制策略的 NAP 策略必须在保护模式（也称为内联模式）下运行。

- 根据您的配置，您可以在系统首次检测到某个文件时对其进行检查并等待云查找结果，也可以在首次检测到文件时不等待云查找结果即对文件放行。
- 默认情况下，已加密负载的文件检查会被禁用。当已加密连接与已配置文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。

如何配置恶意软件防护

本主题总结设置系统以保护网络免受恶意软件侵害时必须执行的步骤。

过程

步骤 1 规划和准备恶意软件防护， 第 1666 页

步骤 2 配置文件策略， 第 1667 页

步骤 3 将文件策略添加到访问控制配置， 第 1668 页

步骤 4 配置网络发现策略，将文件和恶意软件事件与网络上的主机相关联。

（不要简单地打开网络发现；您必须将其配置为发现网络上的主机，以构建组织的网络映射。）

请参阅网络发现策略， 第 1965 页以及子主题。

步骤 5 将策略部署到受管设备。

请参阅部署配置更改， 第 136 页。

步骤 6 测试您的系统，确保它按预期处理恶意文件。

步骤 7 设置恶意软件防护的维护和监控， 第 1670 页

下一步做什么

- （可选）要进一步增强对网络中恶意软件的检测，请部署和集成思科面向终端的AMP产品。请参阅（可选）面向终端的 AMP 的恶意软件防护， 第 1696 页以及子主题。

规划和准备恶意软件防护

此程序是配置系统以提供恶意软件防护的完整过程中的第一组步骤。

过程

步骤 1 购买和安装许可证。

请参阅 文件和恶意软件策略许可证要求， 第 1663 页 和 《Cisco Secure Firewall Management Center 管理指南》中的 许可证。

步骤 2 了解文件策略和恶意软件防护如何融入您的访问控制计划。

请参阅章节访问控制概述， 第 1239 页。

步骤 3 了解文件分析和恶意软件防护工具。

请参阅文件规则操作， 第 1685 页以及子主题。

也可以考虑 高级和存档文件检查选项， 第 1680 页。

步骤 4 确定您将使用公共云还是私有（本地）云进行恶意软件防护（文件分析和动态分析）。

请参阅恶意软件防护的云连接， 第 1670 页以及子主题。

步骤 5 如果您将使用私有（本地）云进行恶意软件防护：购买、部署和测试这些产品。

有关信息，请联系思科客户代表或授权经销商。

步骤 6 配置防火墙以允许与您选择的云进行通信。

请参阅 《Cisco Secure Firewall Management Center 管理指南》中的 安全、互联网接入和通信端口 。

步骤 7 配置 Firepower 和恶意软件防护云（公共或私有云）之间的连接。

- 有关 AMP 云，请参阅更改 AMP 选项， 第 1675 页。
- 如果您部署了本地 Secure Secure Malware Analytics 设备，请参阅连接到内部动态分析设备， 第 1677 页。（访问公共 Secure Secure Malware Analytics 云不需要配置。）

下一步做什么

继续执行恶意软件防护工作流程的下一步：

请参阅如何配置恶意软件防护， 第 1666 页。

配置文件策略

开始之前

完成恶意软件防护工作流程中到目前为止的任务：

请参阅如何配置恶意软件防护， 第 1666 页。

过程

步骤 1 查看文件策略和文件规则限制。

请参阅文件策略和恶意软件检测的最佳实践 ， 第 1663 页以及子主题。

步骤 2 创建文件策略。

请参阅创建或编辑策略，第 1679 页。

步骤 3 在文件策略中创建规则。

请参阅文件规则，第 1684 页以及子主题。

步骤 4 配置高级选项。

请参阅高级和存档文件检查选项，第 1680 页。

下一步做什么

继续执行恶意软件防护工作流程的下一步：

请参阅如何配置恶意软件防护，第 1666 页。

将文件策略添加到访问控制配置

访问控制策略可能有多个与文件策略相关联的访问控制规则。您可以为任何 Allow 或 Interactive Block 访问控制规则配置文件检测，这样，您就可在网络中不同类型的流量到达其最终目的地之前，将不同的文件和恶意软件检测配置文件与其匹配。

开始之前

完成恶意软件防护工作流程中到目前为止的任务：

请参阅如何配置恶意软件防护，第 1666 页。

过程

步骤 1 查看访问控制政策中的文件策略准则。（这些指南与您之前查看的文件规则和文件策略指南不同。）

查看 文件和入侵检查顺序，第 1246 页。

步骤 2 将文件策略与访问控制策略关联。

请参阅配置访问控制规则以执行恶意软件保护，第 1669 页

步骤 3 将访问控制策略分配给被托管的设备。

请参阅设置访问控制策略的目标设备，第 1269 页。

下一步做什么

继续执行恶意软件防护工作流程的下一步：

请参阅如何配置恶意软件防护，第 1666 页。

配置访问控制规则以执行恶意软件保护

注意 在**检测文件**或**阻止文件**规则中启用启用或禁用**存储文件**，或添加包含**恶意软件云查找**或**阻止恶意软件**文件规则操作与分析选项（**Spero 分析或 MSEXE**、**动态分析**或**本地恶意软件分析**）或存储文件选项（**恶意软件**、**未知**、**清理**或**自定义**）的第一个文件规则，或者删除最后一个这样的文件规则，在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。

注释 当访问控制规则中包含文件策略时，会自动启用内联规范化。有关详细信息，请参阅内联规范化预处理器，第 2153 页。

开始之前

- 如配置自适应配置文件，第 2204 页中所述，为了让访问控制规则执行文件控制（包括 AMP），**必须** 启用（默认状态）自适应分析。
- 您必须是管理员，访问管理员或网络管理员用户才能执行此任务。

过程

步骤 1 在访问控制规则编辑器中（从**策略 (Policies) > 访问控制 (Access Control)**），从**操作 (Action)** 选择**允许 (Allow)**, **交互式阻止 (Interactive Block)** 或**交互式阻止并重置 (Interactive Block with reset)**。

步骤 2 选择**文件策略 (File Policy)** 以检查与访问控制规则相匹配的流量，或选择**无 (None)** 禁用对匹配流量的文件检查。

步骤 3 （可选）通过点击**日志记录 (Logging)** 并取消选中**日志文件 (Log Files)** 为匹配连接禁用文件或恶意软件文件的日志记录。

注释 思科建议您保持启用文件和恶意软件日志记录。

步骤 4 保存规则。

步骤 5 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改。

相关主题

创建或编辑策略，第 1679 页
Snort® 重新启动场景，第 143 页

设置恶意软件防护的维护和监控

持续维护对于保护您的网络至关重要。

开始之前

配置您的系统以保护您的网络免受恶意软件的侵害。

请参阅如何配置恶意软件防护，第 1666 页和引用的程序。

过程

步骤 1 确保您的系统始终具有最新、最有效的保护。

请参阅维护您的系统：更新符合动态分析条件的文件类型，第 1679 页。

步骤 2 为恶意软件相关事件和运行状况监控配置警报。

有关配置 恶意软件防护 警报的信息以及有关以下模块的信息，请参阅《Cisco Secure Firewall Management Center 管理指南》：

- 本地恶意软件分析
- 安全情报
- 设备中威胁数据更新
- 入侵和文件事件率
- 面向 Firepower 的 AMP 状态
- 面向终端的 AMP 状态

下一步做什么

查看恶意软件防护工作流程中的“后续操作”：

请参阅如何配置恶意软件防护，第 1666 页。

恶意软件防护的云连接

为了保护网络免受恶意软件，需要连接到公共云或私有云。

AMP 云

高级恶意软件防护 (AMP) 云是一种 Cisco 托管服务器，它使用大数据分析和持续分析提供系统用于检测和阻止网络中的恶意软件的情报。

AMP 云为由受管设备在网络流量中检测到的潜在恶意软件提供处置情况，并为本地恶意软件分析和文件预分类提供数据更新。

如果您的组织已部署面向终端的 AMP 并且已配置 Firepower 以导入其数据，则系统会从 AMP 云导入这些数据，包括扫描记录、恶意软件检测、隔离和感染指标 (IOC)。

Cisco 提供以下选项，用于从 思科云获取有关已知恶意软件威胁的数据：

- **AMP 公共云**

  您的 Cisco Secure Firewall Management Center 直接与公共 思科云通信。有三个公共 AMP 云，分别位于美国、欧洲和亚洲。

- **AMP 私有云**

  AMP 私有云虚拟设备用作压缩的内部 AMP 云，以及用于连接到公共 AMP 云的匿名代理。有关详细信息，请参阅思科 AMP 私有云，第 1673 页。

  如果与面向终端的 AMP 集成，则 AMPv 会有一些限制。请参阅面向终端的 AMP 和 AMP 私有云，第 1698 页。

动态分析云

- **Secure Secure Malware Analytics 云**

  公共云处理您提交进行动态分析的符合条件的文件，并提供威胁评分和动态分析报告。Firepower 支持 200 个样本/天进行 Secure Secure Malware Analytics 分析。

- **本地 Secure Secure Malware Analytics 设备**

  如果您的组织的安全策略不允许系统发送网络外部的文件，则您可以配置本地设备。此设备不会联系公共 Secure Secure Malware Analytics 云。

  有关详细信息，请参阅动态分析本地设备 (Cisco Secure Secure Malware Analytics)，第 1676 页。

配置与 AMP 和 Secure Secure Malware Analytics 云的连接

- AMP 云连接配置，第 1671 页
- 动态分析连接，第 1676 页

AMP 云连接配置

以下主题介绍不同场景的 AMP 云连接配置：

- 选择 AMP 云，第 1672 页
- 连接到 AMP 私有云，第 1673 页
- 集成 Firepower 和 Cisco Secure EndpointSecure Endpoint，第 1698 页

以下主题也相关：

- 思科 AMP 私有云，第 1673 页
- AMP 云连接的要求和最佳实践，第 1672 页
- 管理与 AMP 云的连接（公共或私有），第 1674 页

AMP 云连接的要求和最佳实践

AMP 云连接的要求

您必须是管理员用户才能设置 AMP 云。

为保证 管理中心 可与 AMP 云通信，请参阅《Cisco Secure Firewall Management Center 管理指南》中安全、互联网接入和通信端口 下的主题。

要使用传统端口进行 AMP 通信，请参阅《Cisco Secure Firewall Management Center 管理指南》 中的通信端口要求。

AMP 和高可用性

高可用性对中的管理中心既不共享云连接，也不共享捕获文件、文件事件和恶意软件事件，但是共享文件策略和相关配置。为确保工作连续性以及检测到的文件的恶意软件处置情况在两个 管理中心 上均相同，则主用和备用 管理中心均必须能够访问云。

在高可用性部署中，必须在 Firepower 管理中心的主用和备用实例上单独配置 AMP 云连接；这些配置是不同步的。

这些要求适用于公共和私有 AMP 云。

AMP 云连接和多租户

在多域部署中，您只能在全局级别配置恶意软件防护连接。每个管理中心只能有一个恶意软件防护连接。

选择 AMP 云

默认情况下，为您的系统配置并启用与美国 (US) AMP 公共云的连接。（此连接会在 Web 界面中显示为 恶意软件防护，有时会显示为面向 Firepower 的 AMP。）您无法删除或禁用 恶意软件防护 云连接，但您可以使用此程序在不同的地理 AMP 云之间切换，或者配置私有云 (AMPv) 连接。

开始之前

- 如果您将使用 AMP 私有云，请参阅连接到 AMP 私有云，第 1673 页而不是本主题。
- 除非 Firepower 与面向终端的 AMP 集成，否则只能配置一个 AMP 云连接。此连接标记为**面向网络的 AMP** 或**面向 Firepower 的 AMP**。
- 如果您已部署面向终端的 AMP，并且想要添加一个或多个 AMP 云以将该应用与 Firepower 集成，请参阅集成 Firepower 和 Cisco Secure EndpointSecure Endpoint，第 1698 页。
- 请参阅AMP 云连接的要求和最佳实践，第 1672 页。

过程

步骤 1 选择集成 (Integration) > AMP > AMP 管理 (AMP Management)。

步骤 2 点击铅笔以编辑现有云连接。

步骤 3 从云名称 (Cloud Name) 下拉列表中，选择离 Cisco Secure Firewall Management Center最近的区域云：

APJC 是指亚太地区/日本/中国。

步骤 4 点击保存。

下一步做什么

- 如果您的部署为高可用性配置，请参阅AMP 云连接的要求和最佳实践，第 1672 页。
- （可选）更改 AMP 选项，第 1675 页。

思科 AMP 私有云

管理中心必须连接到AMP云，才能对在网络流量中检测到的文件进行处置情况查询并接收追溯性恶意软件事件。此云可以是公共云，也可以是私有云。

您的组织可能会担心隐私或安全，以致在受监控网络和 AMP 云之间难以或无法进行频繁或直接连接。在这些情况下，您可以设置一个思科AMP私有云，它是一个思科专有的产品，用作压缩内部版 AMP 云，以及网络与 AMP 云之间的安全中介。将 管理中心连接到 AMP 私有云会禁用到公共 AMP 云的现有直接连接。

所有到 AMP 云的连接均通过 AMP 私有云进行筛选，AMPv 用作匿名代理，以确保受监控网络的安全和隐私。此项筛选包括，对在网络流量中检测到的文件进行处置情况查询、接收追溯性恶意软件事件等等。AMP 私有云不通过外部连接共享任何终端数据。

注释 AMP 私有云既 不 执行动态分析，也不支持匿名检索其他依靠思科综合安全情报 (CSI)（例如，URL 和安全情报过滤）的功能的威胁情报。

有关 AMP 私有云（有时称为“AMPv”）的信息，请参阅 https://www.cisco.com/c/en/us/products/security/fireamp-private-cloud-virtual-appliance/index.html。

连接到 AMP 私有云

开始之前

- 根据该产品的文档中的方向配置思科AMP私有云。在配置过程中，请记下私有云的主机名。配置 管理中心上的连接需要使用此主机名。

- 确保 管理中心 可与 AMP 私有云通信，并确认私有云可访问互联网，以便它可与公有 AMP 云通信。请参阅《Cisco Secure Firewall Management Center 管理指南》中安全、互联网接入和通信端口下的主题。
- 除非您的部署与面向终端的 AMP 集成，否则每个 管理中心 只能有一个 AMP 云连接。此连接标记为 **面向网络的 AMP** 或 **面向 Firepower 的 AMP**。

  如果与面向终端的 AMP 集成，则可以配置多个面向终端的 AMP 云连接。

过程

步骤 1 选择**集成 (Integration)** > **AMP** > **AMP 管理 (AMP Management)**。

步骤 2 点击**添加 AMP 云连接**。

步骤 3 从**云名称 (Cloud Name)** 下拉列表中，选择**私有云 (Private Cloud)**。

步骤 4 输入 **Name**。

此信息显示在 AMP 私有云生成或传输的恶意软件事件中。

步骤 5 在**主机 (Host)** 字段中，输入在设置私有云时配置的私有云主机名。

步骤 6 点击**证书上传路径 (Certificate Upload Path)** 旁边的**浏览 (Browse)**，浏览至私有云的有效 TLS 或 SSL 加密证书的位置。有关详细信息，请参阅 AMP 私有云文档。

步骤 7 如果要将此私有云用于恶意软件防护 和面向终端的 AMP，请选中**用于面向 Firepower 的 AMP** 复选框。

如果配置其他私有云来处理 恶意软件防护 通信，则可以清除此复选框；如果这是唯一的 AMP 私有云连接，则无法清除。

在多域部署中，此复选框仅显示在全局域中。每个 管理中心只能有一个恶意软件防护 连接。

步骤 8 要使用代理与 AMP 私有云进行通信，请选中**使用代理连接 (Use Proxy for Connection)** 复选框。

步骤 9 点击**注册 (Register)**，确认要禁用到 AMP 云的现有直接连接，并最终确认要继续至 AMP 私有云管理控制台以完成注册。

步骤 10 登录管理控制台并完成注册过程。有关进一步说明，请参阅 AMP 私有云文档。

下一步做什么

在高可用性部署中，必须在 Firepower 管理中心的主用和备用实例上单独配置 AMP 云连接；这些配置是不同步的。

管理与 AMP 云的连接（公共或私有）

使用 管理中心管理与用于恶意软件防护 或面向终端的 AMP 或两者的公共和私有 AMP 云的连接。

如果不想再从云接收恶意软件相关信息，则可以删除与公共或私有 AMP 云的连接。请注意，使用面向终端的 AMP 或 AMP 私有云管理控制台注销连接不会从系统中删除连接。注销连接会在 Cisco Secure Firewall Management Center Web 界面上显示失败状态。

您还可以临时禁用连接。当重新启用云连接时，云恢复向系统发送数据，包括禁用期内的已排队数据。

注意 对于已禁用的连接，公共或私有 AMP 云可以存储恶意软件事件和危害表现等，直到重新启用连接。在极少数情况下（例如，事件率超高或连接长时间禁用），云可能无法存储在连接处于禁用状态时生成的所有信息。

在多域部署中，系统会显示在当前域中创建的连接，您可以对其进行编辑。系统还会显示在祖先域中创建的连接，您不可以对其进行管理。要管理较低域中的连接，请切换至该域。每个 管理中心只能具有一个属于全局域的恶意软件防护 连接。

过程

步骤 1 选择**集成 (Integration)** > **AMP** > **AMP 管理 (AMP Management)**。

步骤 2 管理 AMP 云连接：

- 删除 - 点击 **删除**（ ），然后确认选择。
- 启用或禁用 - 点击滑块，然后确认选择。

下一步做什么

在高可用性部署中，必须在 Firepower 管理中心的主用和备用实例上单独配置 AMP 云连接；这些配置是不同步的。

更改 AMP 选项

过程

步骤 1 选择**集成** > **其他集成**。

步骤 2 请点击 **云服务**。

步骤 3 选择选项：

表 *193:* 适用于网络的 *AMP* 的选项

选项	说明
启用自动本地恶意软件检测更新 (Enable Automatic Local Malware Detection Updates)	本地恶意软件检测引擎使用思科提供的签名对文件进行静态分析和预分类。如果启用此选项，则 Cisco Secure Firewall Management Center每 30 分钟检查一次签名更新。

选项	说明
与思科共享恶意软件事件中的 URI (Share URI from Malware Events with Cisco)	系统可以向 AMP 云发送有关网络流量中检测到的文件的信息。此信息包括与被检测的文件相关联的 URI 信息及其 SHA-256 散列值。虽然共享功能是可选的，不过向思科传输此信息对未来的恶意软件识别和跟踪工作有帮助。

步骤 4 点击**保存 (Save)**。

动态分析连接

动态分析的要求

您必须是管理员、访问管理员或网络管理员用户并且在全局域中，才能使用动态分析。

通过适当的许可证，Firepower 系统会自动访问 Secure Secure Malware Analytics 云。

动态分析要求受管设备具有对 Secure Secure Malware Analytics 云或本地 Secure Secure Malware Analytics 设备的端口 443 的直接或代理访问权限。

另请参阅哪些文件符合动态分析的条件？，第 1689 页。

如果您将连接到本地 Secure Secure Malware Analytics 设备，另请参阅连接到内部动态分析设备，第 1677 页中的前提条件。

查看默认动态分析连接

默认情况下，Cisco Secure Firewall Management Center 可以连接到 Secure Secure Malware Analytics 公共云以提交文件并检索报告。您既不能配置也不能删除此连接。

过程

步骤 1 选择**集成 (Integration)** > **AMP** > **动态分析连接 (Dynamic Analysis Connections)**。

步骤 2 请点击 **编辑**（ ）。

注释 有关**集成 (Integration)** > **AMP** > **动态分析连接 (Dynamic Analysis Connections)** 页面上的**关联**（ ）**关联**（ ）的信息，请参阅启用对公共云中动态分析结果的访问权限，第 1678 页。

动态分析本地设备 (Cisco Secure Secure Malware Analytics)

如果您的组织担心提交文件到公共 Secure Secure Malware Analytics 云可能会造成隐私或安全问题，您可以部署内部 Secure Secure Malware Analytics 设备。如同公共云一样，内部设备在沙盒环境下运

行合格文件，然后向系统传回威胁评分和动态分析报告。但是，内部设备不会与公共云或位于您的网络外部的任何其他系统通信。

有关本地 Secure Secure Malware Analytics 设备的详细信息，请参阅https://www.cisco.com/c/en/us/products/security/threat-grid/index.html。

连接到内部动态分析设备

如果在网络上安装内部 Secure Secure Malware Analytics 设备，则可以配置动态分析连接以提交文件并从该设备中检索报告。当配置内部设备动态分析连接时，可将 Cisco Secure Firewall Management Center注册到内部设备。

开始之前

- 设置本地 Secure Secure Malware Analytics 应用。

  可从 https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/tsd-products-support-series-home.html获得应用的说明文档：

  请参阅思科 *Firepower* 兼容性指南。

- 如果您的 Secure Secure Malware Analytics 设备使用自签名公钥证书，请从 Secure Secure Malware Analytics 设备下载证书；有关您的 Secure Secure Malware Analytics 设备信息，请参阅设备管理员指南。

  如果使用证书颁发机构 (CA) 签名的证书，则证书必须满足以下要求：

  - 必须在 Secure Secure Malware Analytics 设备上安装服务器密钥和签名证书。按照 Secure Secure Malware Analytics 设备《管理员指南》中的上传说明进行操作。
  - 如果存在多级 CA 签名链，则所有必需的中间证书和根证书必须包含在 管理中心将上传到的单个文件中。
  - 所有证书都必须采用 PEM 编码。
  - 文件的换行符必须是 UNIX，而不是 DOS。

- 托管设备必须在端口 443 上直接或代理访问 Secure Secure Malware Analytics 设备。

过程

步骤 1 选择**集成 (Integration)** > **AMP** > **动态分析连接 (Dynamic Analysis Connections)**。

步骤 2 点击**添加新连接 (Add New Connection)**。

步骤 3 输入 **Name**。

步骤 4 输入**主机**。

步骤 5 在**证书上传 (Certificate Upload)**旁，点击**浏览 (Browse)** 以上传本地设备的证书。

如果 Secure Secure Malware Analytics 设备将提供自签名证书，请上传您从该设备下载的证书。

如果 Secure Secure Malware Analytics 设备将提供 CA 签名证书，请上传包含证书签名链的文件。

步骤 6 如果要使用已配置的代理建立连接，请选择**在可用时使用代理 (Use Proxy When Available)**。

步骤 7 点击 **Register**。

步骤 8 点击**是 (Yes)** 以显示本地 Secure Secure Malware Analytics 设备登录页面。

步骤 9 将用户名和密码输入到本地 Secure Secure Malware Analytics 设备。

步骤 10 点击 **Sign in**（登录）。

步骤 11 您有以下选择：

- 如果先前将 Cisco Secure Firewall Management Center注册到内部设备，请点击**返回**。
- 如果未注册 Cisco Secure Firewall Management Center，请点击**激活**。

启用对公共云中动态分析结果的访问权限

Secure Secure Malware Analytics 提供的有关已分析文件的报告比 管理中心提供的要详细。如果您的组织有 Secure Secure Malware Analytics 云账户，则您可以直接访问 Secure Secure Malware Analytics 门户，查看有关从受管设备发出的进行分析的文件的其他详细信息。但是，出于隐私方面的考虑，只有提交文件的组织才能查看文件分析详细信息。因此，在查看此信息之前，您必须将管理中心与其托管设备提交的文件相关联。

开始之前

您必须有一个 Secure Secure Malware Analytics 云账户，并准备好您的账户凭证。

过程

步骤 1 选择**集成 (Integration)** > **AMP** > **动态分析连接 (Dynamic Analysis Connections)**。

步骤 2 在 Secure Secure Malware Analytics 云对应的表行中点击 **关联** （  ） 。

将打开一个 Secure Secure Malware Analytics 门户窗口。

步骤 3 登录到 Secure Secure Malware Analytics 云。

步骤 4 点击**提交查询**。

注释 请勿更改**设备 (Devices)** 字段中的默认值。

如果在执行此流程时遇到困难，请与思科 TAC 的 Secure Secure Malware Analytics 代表联系。

此更改最多可能需要 24 小时才能生效。

下一步做什么

激活关联后，请参阅在 《Cisco Secure Firewall Management Center 管理指南》 中 查看思科云中的动态分析结果 。

维护您的系统：更新符合动态分析条件的文件类型

符合动态分析条件的文件类型列表由漏洞数据库 (VDB) 确定，该列表定期更新（但每天不超过一次）。如果您是管理员用户，则可以更新符合动态分析条件的文件类型。

为确保您的系统拥有最新列表：

过程

步骤 1 执行以下操作之一：

- （推荐）请参阅 《Cisco Secure Firewall Management Center 管理指南》中所述的 漏洞数据库更新自动化
- 定期检查新的 VDB 更新，并根据需要 手动更新 *VDB*（如 《Cisco Secure Firewall Management Center 管理指南》 中所述）。

  如果您选择此选项，建议您安排定期提醒来执行此操作。

步骤 2 如果您的文件策略指定单个文件类型，而不是指定**支持动态分析**文件类型类别，请更新您的文件策略以使用新支持的文件类型。

步骤 3 如果符合条件文件类型列表发生更改，请部署到受管设备。

文件策略和文件规则

创建或编辑策略

开始之前

如果要配置恶意软件防护策略，请参阅 配置文件策略，第 1667 页中的所有必要程序。

过程

步骤 1 选择**策略** > **访问控制** > **恶意软件和文件** 。

步骤 2 创建新策略或编辑现有策略。

如果要编辑现有策略： 如果显示**视图**（ ），则表明配置属于祖先域，或者您没有修改配置的权限。

提示 要复制现有文件策略，请点击 **复制**（ ），然后在出现的对话框中为新策略键入唯一名称。然后就可以修改副本。

步骤 3 如创建文件规则，第 1692 页中所述，向文件策略添加一个或多个规则。

步骤 4 或者，也可以选择“高级”，并如 高级和存档文件检查选项，第 1680 页中所述配置高级选项。

步骤 5 保存文件策略。

下一步做什么

- 如果要配置恶意软件防护策略，请参阅 配置文件策略，第 1667 页中的其他所需程序。
- 其他:
  - 如将文件策略添加到访问控制配置，第 1668 页中所述，将该文件策略添加到访问控制规则。
  - 部署配置更改。

高级和存档文件检查选项

文件策略编辑器中的“高级”设置具有以下常规选项：

- **首次文件分析**-选择此选项可在 AMP 云处置处于待定状态时分析首次看到的文件。该文件必须与配置为执行恶意软件云查找和Spero、本地恶意软件或动态分析的规则相匹配。如果取消选择此选项，则会将首次检测到的文件标记为具有“未知”处置情况。
- **启用自定义检测列表** - 阻止自定义检测列表上的文件。
- **启用干净列表**-如果启用，此策略将允许干净列表上的文件。
- **如果 AMP 云处置情况为未知，则根据威胁评分覆盖处置情况**-选择一个选项：
  - 如果您选择 **禁用**， 系统将不会覆盖 AMP 云提供的处置情况。
  - 如果设置了阈值威胁评分，则AMP云判定为“未知”的文件如果其动态分析评分等于或低于阈值，则会被视为恶意软件。
  - 如果选择更低的阈值，请增加被视为恶意软件的文件数。根据文件策略中选择的操作，这可能导致受阻文件数增加。

文件策略编辑器中的“高级”设置具有以下存档文件检查选项：

- **检测存档**-对于大小可达**可存储的最大文件大小**高级访问控制设置的存档文件，启用内容检测。
- **阻止加密的存档** - 阻止包含已加密内容的存档文件。
- **阻止不可检测的存档** - 阻止系统并非因加密原因而无法检测其内容的存档文件。此类文件通常包括损坏的文件，或超过指定的最大存档深度的文件。
- **最大存档深度** - 阻止超过指定深度的嵌套存档文件。此计数中未计入顶级存档文件；深度从 1（第一级嵌套文件）开始。

存档文件

存档文件是包含其他文件的文件，例如 `.zip` 或 `.rar` 文件。

如果存档中的任何单个文件与包含阻止操作的文件规则相匹配，系统将阻止整个存档而非该单个文件。

有关存档文件检查选项的详细信息，请参阅高级和存档文件检查选项，第 1680 页。

可进行检查的存档文件

- **文件类型**

  可检查存档文件类型的完整列表会显示在 FMC Web 接口中的文件规则配置页面上。要查看该页面，请参阅创建文件规则，第 1692 页。

  包含的可检查的文件显示在同一页面上。

- **文件大小**

  您可以检查的存档文件大小可达**可存储的最大文件大小**文件策略高级访问控制设置。

- **嵌套存档**

  存档文件可以包含其他存档文件，而其他存档文件反过来又可以包含所述存档文件。文件嵌套的级别是其存档文件深度。请注意，深度计数中未计入顶级存档文件；深度从 1（第一级嵌套文件）开始。

  系统可以检查最外层存档文件（级别 0）以下的最多三级嵌套文件。您可以将文件策略配置为阻止超过该深度（或指定的较低最大文件深度）的存档文件。

  如果您选择不阻止超过最大存档文件深度 3 的文件，当受监控流量中出现包含某些可提取内容和某些嵌套深度为 3 或更大值的内容的存档文件时，系统仅检查其能够检查的文件并报告相关数据。

  所有适用于未压缩的文件的功能（例如，动态分析和文件存储）也适用于存档文件中的嵌套文件。

- **加密文件**

  您可以将系统配置为阻止内容已加密或无法检查的存档。

- **不会检查的存档**

  如果包含存档文件的流量在安全智能阻止列表或不阻止列表中，或者，如果顶级存档文件的 SHA - 256 值在自定义检测列表中，则系统将不检查该存档文件的内容。

  如果嵌套文件被阻止，则整个存档也将被阻止；但是，如果嵌套文件被允许，则存档不会自动通过（取决于任何其他嵌套文件和特性）。

  无法检测到某些 .rar 存档中的 .Exe 文件，可能包括 rar5。

存档文件处置情况

存档文件处置情况基于分配给存档内文件的处置情况。对于包含已确定的恶意软件文件的**所有**存档，将赋予其 `Malware` 性质。对于不含已确定恶意软件文件的存档，如果其包含任何未知文件，则其性质为 `Unknown`；如果其仅包含安全文件，则其性质为 `Clean`。

表 *194:* 按内容划分的存档文件处置情况

存档文件性质	未知文件数	干净文件数	恶意软件文件数
未知	1 个或更多	任意	0
干净 (Clean)	0	1 个或更多	0
恶意软件 (Malware)	任意	任意	1 或更多

存档文件与其他文件一样可以具有自定义检测 (Custom Detection) 或不可用 (Unavailable) 处置情况（如果符合这些处置情况的条件）。

查看存档内容和详细信息

如果将文件策略配置为检查存档文件内容，当存档文件出现在文件事件、恶意软件事件或捕获的文件中时，您可以使用“分析 > 文件”菜单下页面上表格中的上下文菜单，及网络文件轨迹查看器查看有关存档内文件的信息。

存档的所有文件内容均以表形式列出，同时显示其相关信息的摘要：名称、SHA-256哈希值、类型、类别和存档深度。每个文件旁边都会显示一个网络文件轨迹图标，点击该图标即可查看有关该特定文件的详细信息。

使用自定义列表覆盖文件处置情况

如果文件在AMP云中的处置情况据您所知不正确，您可向覆盖云中处置情况的文件列表中添加该文件的 SHA-256 值：

- 要好像 AMP 云已为文件分配了干净的处置一样对其进行处理，请将文件添加到干净列表。
- 要好像AMP云已为文件分配了恶意软件处置一样对其进行处理，请将文件添加到自定义检测列表。

在后续检测中，设备无需重新评估文件处置情况即可允许或阻止该文件。您可以按文件策略使用干净的列表或自定义检测列表。

注释 要计算文件的SHA-256值，您必须将文件策略中的一条规则配置为对匹配的文件执行恶意软件云查找或阻止恶意软件。

有关在 Firepower 中使用文件列表的完整信息，请参阅文件列表，第 989 页。

或者，如果适用，请使用面向终端的 AMP 的集中文件列表，第 1682 页。

面向终端的 *AMP* 的集中文件列表

如果您的组织已部署面向终端的AMP，则在Firepower查询AMP云获取文件处置情况时，它可以使用在面向终端的 AMP 中创建的阻止名单和允许名单。

要求：

- 您的组织使用的必须是 AMP 公共云。
- 您的组织已部署面向终端的 AMP。
- 您已按照集成 Firepower 和 Cisco Secure EndpointSecure Endpoint，第 1698 页中的程序将 Firepower 系统注册到面向终端的 AMP。

要创建和部署这些列表，请参阅面向终端的 AMP 的相关文档或在线帮助。

注释 在 Firepower 中创建的文件列表会覆盖在面向终端的 AMP 中创建的文件列表。

管理文件策略

“文件策略”(File Policies) 页面显示现有文件策略的列表及其上次修改日期。您可以使用此页面来管理文件策略。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

注释 系统会检查符合动态分析条件的文件类型列表的更新（每天不超过一次）。如果合格文件类型列表更改，这会构成文件策略发生更改；任何使用该文件策略的访问控制策略在部署于任何设备时都会标记为过期。在更新的文件策略可在设备上生效之前，必须先部署策略。请参阅维护您的系统：更新符合动态分析条件的文件类型，第 1679 页。

过程

步骤 1 选择**策略** > **访问控制** > **恶意软件和文件** 。

步骤 2 管理文件策略：

- 比较 - 点击**比较策略 (Compare Policies)**；请参阅比较策略，第 148 页。
- 创建 - 要创建文件策略，请点击**新建文件策略 (New File Policy)**，然后如创建或编辑策略，第 1679 页中所述继续操作。
- 复制 - 要复制文件策略，请点击 **复制**（）。

  如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。
- 删除 - 如果要删除文件策略，请点击 **删除**（），然后按照提示点击**是 (Yes)** 和**确定 (OK)**。

  如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
- 部署 - 选择**部署** > **部署**；请参阅部署配置更改，第 136 页。
- 编辑 - 如果要修改现有文件策略，请点击 **编辑**（）。

- 报告 - 点击**报告**（）；请参阅生成当前策略报告，第 149 页。

文件规则

文件策略（例如父项访问控制策略）包含的规则用于确定系统如何处理与每个规则的条件相符的文件。可以配置单独的文件规则，以对不同的文件类型、应用协议或传输方向采取不同操作。

例如，如果某个文件匹配某个规则，则该规则可以：

- 根据简单的文件类型匹配允许或阻止文件
- 根据处置情况阻止文件（无论评估是否表明它是恶意的）
- 将文件存储到设备（有关信息，请参阅捕获的文件和文件存储，第 1690 页）
- 提交储存的（捕获的）文件以进行本地恶意软件、Spero 或动态分析

此外，文件策略还可以：

- 根据干净的列表或自定义检测列表中的条目自动将文件视为干净的文件或恶意软件
- 在文件的威胁评分超过可配置阈值时将文件视为恶意软件
- 检查存档文件（例如，`.zip` 或 `.rar`）的内容
- 阻止内容已加密，嵌套超过指定的最大存档深度或因其他原因无法检查的存档文件

文件规则组成部分

表 *195:* 文件规则组成部分

文件规则组成部分	说明
应用协议	系统可以检测和检查通过 FTP、HTTP、SMTP、IMAP、POP3 和 NetBIOS-ssn (SMB) 传输的文件。**Any**（默认值）检测 HTTP、SMTP、IMAP、POP3、FTP 和 NetBIOS-ssn (SMB) 流量中的文件。为了提高性能，可以逐个文件规则将文件检测仅限于其中一种应用协议。
传输方向	对于已下载的文件，可以检查通过 FTP、HTTP、IMAP、POP3 和 NetBIOS-ssn (SMB) 传入的流量；对于已上传的文件，可以检查通过 FTP、HTTP、SMTP 和 NetBIOS-ssn (SMB) 传出的流量。 **提示** 无论用户是发送还是接收，使用 **Any** 都可通过多种应用协议检测文件。

文件规则组成部分	说明
文件类别和类型	系统检测各种类型的文件。这些文件类型分为三类：基本类别，包括多媒体（swf 和 mp3）；可执行文件（exe 和 torrent）；以及 PDF。可以配置用于检测个别文件类型或整个类别的文件类型的规则。 例如，可以阻止所有多媒体文件，或者仅阻止 ShockWave Flash (swf) 文件。或者，可以将系统配置为会在用户下载 BitTorrent (torrent) 文件时向您发出警报。 请注意，可执行文件包括可以运行宏和脚本的文件类型，因为它们可能包含恶意软件。 有关系统可以检查的文件类型的列表，请选择**策略 > 访问控制 > 恶意软件和文件**，创建一个临时的新文件策略，然后点击**添加规则**。选择文件类型类别，系统可以检查的文件类型会显示在**文件类型**列表中。 **注释** 频繁触发的文件规则可能会影响系统性能。例如，检测 HTTP 流量（例如 YouTube，用于传输重要的 Flash 内容）中的多媒体文件可能会产生可能生成数量巨大的事件。
文件规则操作	文件规则操作用于确定系统如何处理与规则条件相符的流量。 根据所选操作，您可以配置系统是存储文件还是对文件执行 Spero、本地恶意软件或动态分析。如果选择“阻止”(Block) 操作，还可以配置系统是否还重置受阻连接。 有关这些操作和选项的说明，请参阅文件规则操作，第 1685 页。 文件规则是以规则操作顺序而非数字顺序进行评估。有关详细信息，请参阅文件规则操作：评估顺序，第 1691 页。

文件规则操作

借助文件规则，可以精细控制要对其记录、阻止或扫描恶意软件的文件类型。每个文件规则都有用于确定系统如何处理与规则条件匹配的流量的关联操作。文件策略必须包含一个或多个规则才能生效。您可以在文件策略中使用单独的规则，以对不同的文件类型、应用协议或传输方向采取不同操作。

文件规则操作

- 检测文件规则允许将特定文件类型的检测记录到数据库，同时仍允许其传输。
- 阻止文件规则允许阻止特定文件类型。您可以配置选项，以在阻止文件传输时重置连接并将已捕获的文件存储到受管设备。
- 恶意软件云查找 *(Malware Cloud Lookup)* 规则允许您获取并记录通过网络传输的文件的处置情况，同时仍允许文件传输。

- 阻止恶意软件 *(Block Malware)* 规则允许您计算特定文件类型的 SHA-256 散列值，查询 AMP 云以确定通过网络传输的文件是否包含恶意软件，然后阻止表示为威胁的文件。

文件规则操作选项

根据所选择的操作，有不同的选项：

文件规则操作选项	能否阻止文件？	能否阻止恶意软件？	能否检测文件？	能否进行恶意软件云查找？
MSEXE 的 Spero 分析*	否	是，可以提交可执行文件	否	是，可以提交可执行文件
动态分析*	否	是，可以提交具有未知文件处置情况的可执行文件	否	是，可以提交具有未知文件处置情况的可执行文件
容量处理	否	是	否	是
本地恶意软件分析*	否	是	否	是
重置连接	是（推荐）	是（推荐）	否	否
存储文件	是，可以存储所有匹配的文件类型	是，可以存储与选择的文件性质匹配的文件类型	是，可以存储所有匹配的文件类型	是，可以存储与选择的文件性质匹配的文件类型

* 有关这些选项的完整信息，请参阅恶意软件保护选项（在文件规则操作中），第 1686 页及其子主题。

注意 启用或禁用**检测文件**或**阻止文件**规则中的**存储文件**，或者添加第一条或删除最后一条将**恶意软件云查找**或**阻止恶意软件**文件规则操作与分析选项（**Spero 分析**或 **MSEXE**、**动态分析**或**本地恶意软件分析**）或存储文件选项（**恶意软件**、**未知**、**清理**或**自定义**）、在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。结合起来的文件规则

恶意软件保护选项（在文件规则操作中）

系统运用多种文件检测和分析方法来确定文件是否包含恶意软件。

根据您在文件规则中启用的选项，系统将按顺序使用以下工具检查文件：

1. Spero 分析，第 1688 页 和 AMP 云查找，第 1688 页
2. 本地恶意软件分析，第 1689 页
3. 动态分析，第 1689 页

有关这些工具的比较，请参阅恶意软件防护选项的比较，第 1687 页。

（如果您愿意的话，还可以根据文件类型阻止所有文件。有关详细信息，请参阅按类型阻止所有文件，第 1691 页。）

另请参阅 （可选）面向终端的 AMP 的恶意软件防护，第 1696 页 和子主题中有关思科面向终端的 AMP 产品的信息。

恶意软件防护选项的比较

下表详细介绍每种类型的文件分析的优缺点，以及每种恶意软件防护方法确定文件处置的方式。

分析类型	优点	限制	恶意软件识别
斯佩罗分析	可执行文件的结构分析，将 Spero 签名提交到AMP 云进行分析	没有本地恶意软件分析或动态分析彻底，仅用于可执行文件	仅在明确识别恶意软件时处置情况才会从“未知”(Unknown) 更改为“恶意软件”(Malware)。
本地恶意软件分析	比动态分析消耗的资源少，返回结果更快，尤其当检测到的恶意软件较常见时	分析结果没有动态分析的结果彻底	仅在明确识别恶意软件时处置情况才会从“未知”(Unknown) 更改为“恶意软件”(Malware)。
动态分析	使用 Secure Secure Malware Analytics对未知文件的彻底分析	符合条件的文件将上传到公共云或本地设备。完成分析需要一些时间	威胁评分确定文件的恶意程度。处置情况根据文件策略中配置的威胁评分阈值。
Spero 分析结合本地恶意软件分析	比配置本地恶意软件分析和动态分析消耗的资源少，仍使用 AMP 云资源识别恶意软件	没有动态分析彻底，Spero 分析仅用于可执行文件	仅在明确识别恶意软件时处置情况才会从“未知”(Unknown) 更改为“恶意软件”(Malware)。
Spero 分析结合动态分析	在提交文件和 Spero 签名时使用完整的 AMP 云功能	获取结果的速度没有使用本地恶意软件分析获取结果的速度快	威胁评分根据预分类为可能的恶意软件的文件的动态分析结果更改。处置情况根据文件策略中配置的威胁评分阈值更改，并在 Spero 分析识别恶意软件时从“未知”(Unknown) 更改为“恶意软件”(Malware)。

分析类型	优点	限制	恶意软件识别
本地恶意软件分析结合动态分析	使用两种类型的文件分析使分析结果更彻底	比单独使用任一种分析消耗的资源多	威胁评分根据预分类为可能的恶意软件的文件的动态分析结果更改。处置情况在本地恶意软件分析识别恶意软件时从“未知”(Unknown) 更改为“恶意软件”(Malware)，或根据文件策略中配置的威胁评分阈值更改。
Spero 分析、本地恶意软件分析结合动态分析	分析结果最彻底	运行所有三种类型的文件分析消耗的资源最多	威胁评分根据预分类为可能的恶意软件的文件的动态分析结果更改。处置情况在 Spero 分析或本地恶意软件分析识别恶意软件时从“未知”(Unknown) 更改为“恶意软件”(Malware)，或根据文件策略中配置的威胁评分阈值更改。
（阻止传输指定文件类型的所有文件）	不需要 恶意软件 许可证 （从技术上讲此选项不是恶意软件防护选项。）	合法文件也将被阻止	（不执行任何分析。）

注释 预分类本身并不确定文件的处置情况；它只是确定文件是否符合动态分析条件的一个因素。

Spero 分析

Spero 分析检查结构特征，例如可执行文件中的元数据和报头信息。根据此信息生成 Spero 签名后，若文件是合法可执行文件，则设备会将其提交到 AMP 云中的 Spero 启发式引擎。基于 Spero 签名，Spero 引擎确定文件是否为恶意软件。您还可以配置以下规则：提交文件以进行 Spero 分析，而不将其提交到 AMP 云。

请注意，您无法手动提交文件以进行 Spero 分析。

AMP 云查找

对于符合条件使用高级恶意软件防护进行评估的文件，管理中心执行恶意软件云查找，根据其SHA-256 散列值在 AMP 云中查询文件的处置情况。

为了提高性能，系统会缓存由云返回的处置情况，并为已知文件使用缓存的处置情况而不是查询 AMP 云。有关此缓存的详细信息，请参阅缓存处置情况持久性 ，第 1689 页。

本地恶意软件分析

本地恶意软件分析允许受管设备使用由Talos情报小组 提供的检测规则集，在本地检查可执行文件、PDF、办公文档以及其他类型的文件是否存在最常见的恶意软件类型。由于本地恶意软件分析不需要查询 AMP 云，也不运行该文件，因此节约了时间和系统资源。

如果系统通过本地恶意软件分析识别恶意软件，则它会将现有文件处置情况从“未知”(Unknown) 更改为“恶意软件”(Malware)。然后，系统会生成一个新恶意软件事件。如果系统未识别恶意软件，则它不会将文件处置情况从“未知”(Unknown) 更改为“干净”(Clean)。系统运行本地恶意软件分析后，会缓存 SHA-256 散列值、时间戳以及处置情况等文件信息，以便在特定时间段内再次检测时，系统可以在不进行其他分析的情况下识别恶意软件。有关缓存的详细信息，请参阅缓存处置情况持久性，第 1689 页。

本地恶意软件分析不需要与 Secure Secure Malware Analytics 云建立通信。但是，您必须配置与云的通信，以提交文件以进行动态分析，并将更新下载到本地恶意软件分析规则集。

缓存处置情况持久性

从AMP 云查询返回的处置情况、关联的威胁评分以及本地恶意软件分析分配的处置情况都具有生存时间 (TTL) 值。保持某种处置情况而无更新达到 TTL 值中指定的持续时间后，系统会清除缓存的信息。安全状态及相关的威胁评分具有以下 TTL 值：

- “干净”(Clean) - 4 小时
- “未知”(Unknown) - 1 小时
- “恶意软件”(Malware) - 1 小时

如果对缓存进行查询发现已超时的缓存处置情况，系统会向 本地恶意软件分析数据库和 AMP 云重新查询新的处置情况。

动态分析

您可以将文件策略配置为使用思科的文件分析和威胁情报平台 Secure Secure Malware Analytics （以前称为 Threat Grid）自动提交文件以进行动态分析。

设备将符合条件的文件提交到 Secure Secure Malware Analytics （公共云或本地设备，以您指定的为准），无论设备是否存储文件。

Secure Secure Malware Analytics 在沙盒环境中运行该文件，分析文件的行为以确定该文件是否为恶意文件，然后返回威胁评分，指明文件包含恶意软件的可能性。您可以通过威胁评分查看动态分析摘要报告，该报告包含分配该威胁评分的原因。您还可以查看 Secure Secure Malware Analytics 以查看您的组织提交的文件的详细报告，以及您的组织未提交的文件的有限数据的清理报告。

有关思科 Secure Secure Malware Analytics的详细信息，请参阅 https://www.cisco.com/c/en/us/products/security/threat-grid/index.html

要配置系统以执行动态分析，请参阅 动态分析连接，第 1676 页下面的主题。

哪些文件符合动态分析的条件？

文件是否符合动态分析的条件取决于：

- 文件类型
- 文件大小
- 文件规则的操作

此外：

- 系统只会提交与您配置的文件规则匹配的文件。
- 在发送文件进行分析时，该文件的恶意软件云查找性质必须为“未知”(Unknown) 或“不可用”(Unavailable)。
- 系统必须将文件预分类为潜在的恶意软件。

动态分析和容量处理

在设备无法与云通信或已达到最大提交次数而系统暂时无法将文件提交到云时，容量处理允许您暂时地存储符合动态分析条件的文件。当阻碍条件消除后，系统会提交存储的文件。

一些设备可以将文件存储在设备硬盘驱动器或恶意软件存储包中。另请参阅恶意软件存储包，第 1691 页。

捕获的文件和文件存储

通过文件存储功能，您可以捕获在流量中检测到的选定文件，并自动将文件副本暂时存储至设备硬盘驱动器（如果已安装）或恶意软件存储包内。

在设备捕获文件后，您可以：

- 将捕获文件存储至设备硬盘驱动器中供后期分析使用。
- 将存储的文件下载至本地计算机，以便进一步实施人工分析或存档。
- 手动提交符合条件的捕获文件，以进行 AMP 云查找或动态分析。

请注意，文件存储在设备中之后，如果未来检测到该文件且设备仍存有该文件，则不会再捕获该文件。

注释 在网络上第一次检测到某个文件时，您可以生成代表文件检测情况的文件事件。但如果您的文件规则执行恶意软件云查找，则系统需要额外的时间来查询AMP云并返回处置情况。由于这种延迟，在网络上第二次出现此文件之前，系统无法存储此文件，并且系统可以立即确定此文件的处置情况。

无论系统捕获还是存储文件，您都可以：

- 从“分析“>”文件“>”捕获的文件”审查捕获文件的信息，包括文件是否存储或提交用于动态分析、文件性质和威胁评分，以便迅速查看网络中检测到的恶意软件潜在威胁。
- 查看文件轨迹，确定其如何穿过网络以及哪些主机有副本。
- 向清空列表或自定义检测列表添加文件，以便在未来检测过程中始终将该文件作为清空或恶意软件性质。

您可以在文件策略中配置文件规则，以便捕获并存储特定类型或者具有特定文件性质的文件（如有）。如果将该文件策略与访问控制策略相关联，并将其部署到设备上，则系统将捕获并存储流量中的匹配文件。还可以限制要存储的最小和最大文件大小。

存储的文件不包含在系统备份中。

您可以在“分析”>“文件”>“捕获的文件”下查看捕获的文件信息，并下载副本进行离线分析。

恶意软件存储包

根据您的文件策略配置，设备可能会将大量文件数据存储到硬盘驱动器。您可以在设备中安装一个恶意软件存储包，系统则会将文件存储到该恶意软件存储包，从而使主硬盘驱动器中有更多空间来存储事件和配置文件。系统会定期删除较早的文件。如果设备的主硬盘驱动器没有足够的可用空间，也未安装恶意软件存储包，则无法存储文件。

⚠

注意 请勿尝试在设备中安装非思科提供的硬盘驱动器。安装不受支持的硬盘驱动器可能会损坏设备。恶意软件存储包套件**仅**可从思科购买。如果需要恶意软件存储包方面的帮助，请与技术支持部门联系。有关详细信息，请参阅 《*Firepower* 系统恶意软件存储包指南》。

如果未安装恶意软件存储包，则在配置设备以存储文件时，该设备会将主硬盘驱动器空间的设定部分分配用于存储捕获文件。如果将容量处理配置为暂时存储文件以进行动态分析，则系统会使用相同的硬盘驱动器分配来存储这些文件，直至可以将这些文件重新提交到云。

在设备中安装恶意软件存储包并配置文件存储或容量处理时，该设备会分配整个恶意软件存储包来用于存储这些文件。设备无法在恶意软件存储包中存储任何其他信息。

在分配的用于存储捕获文件的空间容量填满时，系统将删除最早存储的文件，直到分配的空间达到系统定义的阈值。根据存储的文件数量，在系统删除文件后，您可能会看到磁盘已用空间明显下降。

如果在安装恶意软件存储包时，设备已经存储文件，则下次重新启动设备时，存储在主硬盘驱动器上的任何捕获文件或容量处理文件都会移至恶意软件存储包。设备未来存储的文件都将存储至恶意软件存储包。

按类型阻止所有文件

如果您的组织不仅要阻止恶意软件文件的传输，还要阻止某个特定类型的所有文件的传输（无论文件是否包含恶意软件），您可以做到这一点。

系统可以检测恶意软件的所有文件类型以及许多其他文件类型都支持文件控制。这些文件类型分为三类：基本类别，例如多媒体（swf 和 mp3）；可执行文件（exe 和 torrent）；以及 PDF。

从技术上来说，根据类型阻止所有文件不是恶意软件防护功能；它不需要恶意软件许可证，也不会查询 AMP 云。

文件规则操作：评估顺序

文件策略有可能包含针对不同情况的不同操作的多个规则。如果多个规则同时适用于某个特定情况，则将适用本主题中所述的评估顺序。一般来说，简单阻止优先于恶意软件检查和阻止，后者优先于简单检测和日志记录。

文件规则操作的优先顺序为：

- 阻止文件 *(Block Files)*
- 阻止恶意软件
- 恶意软件云查找
- 检测文件

创建文件规则

注意 启用或禁用**存储文件**（在**检测文件**或**阻止文件**规则中），或添加包含**恶意软件云查找**或**阻止恶意软件**文件规则操作与分析选项（**Spero 分析或 MSEXE**、**动态分析**或**本地恶意软件分析**）或存储文件选项（**恶意软件**、**未知**、**清理**或**自定义**）的第一个文件规则，或者删除最后一个这样的文件规则，在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。

开始之前

如果要配置恶意软件防护规则，请参阅配置文件策略，第 1667 页。

过程

步骤 1 在文件策略编辑器中，点击**添加文件规则 (Add File Rule)**。

步骤 2 选择**应用协议 (Application Protocol)** 和**传输方向 (Direction of Transfer)**，如文件规则组成部分，第 1684 页中所述。

步骤 3 选择一个或多个**文件类型**。

显示的文件类型取决于所选的应用协议、传输方向和操作。

可以通过以下方式过滤文件类型列表：

- 在**文件类型类别 (File Type Categories)** 中选择一个或多个文件类型类别，然后点击**所选类别中的所有类型 (All types in selected Categories)**。
- 按名称或说明搜索文件类型。例如，在**搜索名称和说明 (Search name and description)** 字段中键入 **`Windows`** 将会显示 Microsoft Windows 专用文件的列表。

提示 将指针悬停在文件类型上方可查看其描述。

步骤 4 按照文件规则操作，第 1685 页中的描述选择文件规则**操作**，并考虑文件规则操作：评估顺序，第 1691 页。

可用的操作取决于您所安装的许可证。请参阅文件和恶意软件策略许可证要求，第 1663 页。

步骤 5 根据您选择的操作，配置选项：

- 在阻止文件后重置连接
- 存储与规则匹配的文件
- 启用 Spero 分析*
- 启用本地恶意软件分析*
- 启用动态分析*和容量处理

*有关这些选项的信息，请参阅文件规则操作，第 1685 页和恶意软件保护选项（在文件规则操作中），第 1686 页及其子主题。

步骤 6 点击 **Add**。

步骤 7 点击 **Save** 保存策略。

下一步做什么

- 如果要配置恶意软件防护策略，请返回配置文件策略，第 1667 页。
- 部署配置更改。

用于恶意软件防护的访问控制规则日志记录

当系统根据文件策略中的设置检测到受禁文件（包括恶意软件）时，会自动将事件记录到Cisco Secure Firewall Management Center数据库中。如果您不想记录文件或恶意软件事件，则可按每条访问控制规则禁用此日志记录功能。

无论调用访问控制规则的日志记录配置如何，系统均会将关联连接的末端记录到 Cisco Secure Firewall Management Center数据库。

追溯处置情况更改

文件处置情况可以更改。例如，当发现新信息时，AMP 云可以确定先前被视为安全的文件现在被识别为恶意软件，或者正好相反，以前被识别为恶意软件的文件实际上是安全的。如果上周查询过的文件的处置情况发生变化，AMP 云会通知系统，使其在下次检测到该文件进行传输时可以自动采取措施。已更改的处置情况称为追溯性处置情况。

文件和恶意软件检测性能和存储选项

提高文件大小会影响系统的性能。

表 *196:* 高级访问控制文件和恶意软件防护检测选项

字段	说明 (Description)	准则和限制
限制进行文件类型检测时检查的字节数 (Limit the number of bytes inspected when doing file type detection)	指定执行文件类型检测时检查的字节数。	0 - 4294967295 (4GB) 0 可消除限制。 默认值是 TCP 数据包的最大分片大小（1460 个字节）。在大多数情况下，系统可以使用第一个数据包确定常见的文件类型。 要检测 ISO 文件，请输入大于 36870 的值。
Allow file if cloud lookup for Block Malware takes longer than (seconds)	指定进行恶意软件云查找时，没有缓存的处置情况，系统将会保持匹配**阻止恶意软件 (Block Malware)** 规则的文件的最后一个字节的时长。如果该时间过去，系统没有获得处置，文件将会通过。不可用的处置不会被缓存。	0 - 30 秒 如未联系支持部门，请勿将此选项设置为 0。 由于连接故障，思科建议使用默认值以避免阻止流量。
Do not calculate SHA-256 hash values for files larger than (in bytes)	禁止系统存储大于特定大小的文件，对文件进行恶意软件云查找或阻止文件（如果已添加到自定义检测列表）。	0 - 4294967295 (4GB) 0 可消除限制。 该值必须大于或等于**可存储的最大文件大小（字节）**和**用于动态分析测试的最大文件大小（字节）**。

高级文件检查和存储的最小文件大小（字节）	这些设置指定：
	• 系统可以使用以下检测器检测的文件大小：
	  • 斯佩罗分析
	  • 沙盒和预分类
	  • 本地恶意软件分析/ClamAV
	  • 存档检测
	• 系统可以使用文件规则存储的文件大小。
		0 - 10485760 (10MB)
		0 可禁用文件存储。
		必须小于或等于**可存储的最大文件大小（字节）**和**对于文件大小大于以下值的文件，不计算 SHA-256 哈希值（以字节为单位）**。

高级文件检查和存储的最大文件大小（字节）		0 - 10485760 (10MB) 0 可禁用文件存储。 必须大于或等于**可存储的最小文件大小（字节）**，并小于或等于**对于文件大小大于以下值的文件，不计算 SHA-256 哈希值（以字节为单位）**。

字段	说明 (Description)	准则和限制
用于动态分析测试的最小文件大小（字节）**(Minimum file size for dynamic analysis testing [bytes])**	指定系统可以提交到 AMP 云以供动态分析的最小文件大小。	0 - 10485760 (10MB) 必须小于或等于**用于动态分析测试的最大文件大小（字节）**和**对于文件大小大于以下值的文件，不计算 SHA-256 哈希值（以字节为单位）**。 动态分析的文件大小必须位于文件分析的最小值和最大值设置所定义的限制内。 系统会检查 AMP 云以更新可以提交的最小文件大小（一天不超过一次）。如果新的最小值大于当前值，当前值会更新为新的最小值，而且策略会标记为过期。
用于动态分析测试的最大文件大小（字节）**(Maximum file size for dynamic analysis testing (bytes))**	指定系统可以提交到 AMP 云以供动态分析的最大文件大小。	0 - 10485760 (10MB) 必须大于或等于**用于动态分析测试的最小文件大小（字节）**，并小于或等于**对于文件大小大于以下值的文件，不计算 SHA-256 哈希值（以字节为单位）**。 动态分析的文件大小必须位于文件分析的最小值和最大值设置所定义的限制内。 系统会检查 AMP 云以更新可以提交的最大文件大小（一天不超过一次）。如果新的最大值小于当前值，当前值会更新为新的最大值，而且策略会标记为过期。

调整文件和恶意软件检测性能和存储

您必须是管理员，访问管理员或网络管理员用户才能执行此任务。

过程

步骤 1 在访问控制策略编辑器中，点击 **高级设置**。

步骤 2 点击 **文件和恶意软件设置**旁边的 **编辑**（ ）。

如果显示**视图**（ ），则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 3 设置文件和恶意软件检测性能和存储选项，第 1693 页中所述的任何选项。

步骤 4 点击**确定 (OK)**。

步骤 5 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改。

（可选）面向终端的 AMP 的恶意软件防护

思科的面向终端的 AMP 是一款独立的恶意软件防护产品，它可以补充 Firepower 系统提供的恶意软件防护并与您的 Firepower 部署进行集成。

面向终端的 AMP 是思科的企业级高级恶意软件防护解决方案，它在个人用户的终端（计算机和移动设备）上作为轻量级连接器运行，用于发现、了解和阻止高级恶意软件爆发、高级持续威胁和针对性攻击。

面向终端的 AMP 的优势包括：

- 为整个组织配置自定义恶意软件检测策略和配置文件，以及对所有用户的文件执行快速扫描和全面扫描
- 执行恶意软件分析，包括查看热图、详细文件信息、网络文件轨迹和威胁根本原因
- 配置爆发控制的多个方面，包括自动隔离、用于阻止运行非隔离可执行文件的应用阻止，以及排除列表
- 创建自定义保护，根据组策略阻止某些应用的执行，并创建自定义允许的应用列表
- 使用面向终端的 AMP 管理控制台帮助您减轻恶意软件的影响。管理控制台提供稳健灵活的 Web 界面，您可以通过该界面控制面向终端的 AMP 部署的所有方面并管理爆发的所有阶段。

有关面向终端的 AMP 的详细信息，请参阅：

- https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html。
- 面向终端的 AMP 管理控制台中的在线帮助。
- 以下网址中提供的面向终端的 AMP 文档：http://docs.amp.cisco.com。

恶意软件防护比较：Firepower 与面向终端的 AMP

表 *197:* 按检测产品进行比较的高级恶意软件防护差异

特性	Firepower 恶意软件防护（恶意软件防护）	面向终端的 AMP
文件类型检测和阻止方法（文件控制）	在网络流量中，使用访问控制和文件策略	不支持
恶意软件检测和阻止方法	在网络流量中，使用访问控制和文件策略	在单个终端（最终用户计算机和移动设备）上，使用与 AMP 云进行通信的连接器
检查的网络流量	流量传递通过受管设备	无；终端上安装的连接器直接检查文件

特性	Firepower 恶意软件防护（恶意软件防护）	面向终端的 AMP
恶意软件情报数据源	AMP 云（公共或私有）	AMP 云（公共或私有）
恶意软件检测稳健性	有限的文件类型	所有文件类型
恶意软件分析方案	管理中心为基础的分析，以及在 AMP 云中的分析	管理中心为基础的分析，以及面向终端的AMP管理控制台上的其他选项
恶意软件缓解	网络流量中的恶意软件阻止， 管理中心 发起的补救	基于面向终端的 AMP 的隔离和爆发控制方案，管理中心 发起的补救
生成的事件	文件事件、捕获文件、恶意软件事件及追溯性恶意软件事件	恶意软件事件
恶意软件事件中的信息	基本的恶意软件事件信息，以及连接数据（IP 地址、端口和应用协议）	深入的恶意软件事件信息；无连接数据
网络文件轨迹	基于管理中心	管理中心 和面向终端的 AMP 管理控制台均具有网络文件轨迹。两者均很有用。
所需许可证或订用	执行文件控制和所需的许可证 恶意软件防护	面向终端的 AMP 订用。将面向终端的 AMP 数据引入 FMC 无需许可证。

关于将 Firepower 与面向终端的 AMP 进行集成

如果您的组织已部署面向终端的 AMP，您可以选择将该产品与 Firepower 部署进行集成。

与面向终端的 AMP 进行集成不需要专用 Firepower 许可证。

集成 Firepower 和面向终端的 AMP 的优势

将面向终端的 AMP 部署与系统集成具有以下优势：

- 面向终端的 AMP 中配置的集中屏蔽应用和允许应用可确定从 Firepower 发送到 AMP 云用于处置的文件 SHA 的判定。

  请参阅面向终端的 AMP 的集中文件列表，第 1682 页。

- 系统可以将面向终端的 AMP 检测到的恶意软件事件导入到 Cisco Secure Firewall Management Center，这样您便可以管理这些事件以及系统生成的恶意软件事件。这些事件的导入数据包括扫描、恶意软件检测、隔离、阻止的执行和云召回，以及管理中心为其监控的主机显示的感染指标 (IOC)。

- 您可以在面向终端的 AMP 控制台中查看文件轨迹和其他详细信息。

重要事项 如果您使用思科 AMP 私有云虚拟设备 (AMPv)，请参阅 面向终端的 AMP 和 AMP 私有云 ，第 1698 页中的限制。

面向终端的 AMP 和 AMP 私有云

如果您配置思科 AMP 私有云以收集您的网络的 AMP 终端数据，则所有面向终端的 AMP 连接器都会将数据都发送到私有云，然后私有云会将这些数据转发到 Cisco Secure Firewall Management Center。私有云不通过外部连接共享任何终端数据。

如果您的组织已部署 AMP 私有云，则所有到 AMP 云的连接均通过私有云进行筛选，AMPv 用作匿名代理，以确保受监控网络的安全和隐私。这包括导入面向终端的 AMP 数据。私有云不通过外部连接共享任何终端数据。

如果您使用 AMP 私有云，以下集成功能将不可用：

- 使用面向终端的 AMP 中配置的“阻止的应用”和“允许的应用”列表。（这些列表用于阻止或允许文件。）
- Firepower 生成的恶意软件事件在面向终端的 AMP 中的可视性。

您可以配置多个私有云来支持所需的容量。

集成 Firepower 和 Cisco Secure EndpointSecure Endpoint

如果您的组织已部署思科的 Cisco Secure EndpointSecure Endpoint 产品，您可以将该应用与 Firepower 进行集成以实现集成 Firepower 和面向终端的 AMP 的优势 ，第 1697 页中所述的优势。

在与 Cisco Secure EndpointSecure Endpoint集成时，即使已配置了 恶意软件防护 （面向 Firepower 的 AMP）连接，也必须配置 Cisco Secure EndpointSecure Endpoint 连接。您可以配置多个 Cisco Secure EndpointSecure Endpoint 云连接。

注意 在多域部署中，请仅在枝叶级别配置 Cisco Secure EndpointSecure Endpoint，尤其是在枝叶域具有重叠的 IP 空间的情况下。如果多个子域具有 IP-MAC 地址对相同的主机，则系统可能会将 Cisco Secure EndpointSecure Endpoint 生成的恶意软件事件保存到错误的枝叶域，或将 IOC 与错误的主机相关联。

但是，假设您为每个连接使用单独的 Cisco Secure EndpointSecure Endpoint 账户，则您可以在所有域级别配置 Cisco Secure EndpointSecure Endpoint 连接。例如，MSSP 的每个客户端都可能拥有自己的 Cisco Secure EndpointSecure Endpoint 部署。

注释 尚未成功注册到门户的 Cisco Secure EndpointSecure Endpoint 连接不会影响 恶意软件防护。

开始之前

- 您必须是管理员用户才能执行此任务。

- 如果您的部署使用思科 AMP 私有云虚拟设备，请参阅 面向终端的 AMP 和 AMP 私有云，第 1698 页中的限制。
- Cisco Secure EndpointSecure Endpoint 必须在您的网络中正确设置并正常工作。
- 管理中心必须可以直接访问互联网。
- 确保您的 管理中心 和 Cisco Secure EndpointSecure Endpoint 可以互相通信。请参阅《Cisco Secure Firewall Management Center 管理指南》中安全、互联网接入和通信端口下的主题。
- 如果您是在将 Cisco Secure Firewall Management Center恢复为出厂默认设置或还原为先前版本之后连接到 AMP 云，请使用面向终端的 AMP 管理控制台删除先前连接。
- 在此程序期间，您需要使用 Cisco Secure EndpointSecure Endpoint 凭证来登录 Cisco Secure EndpointSecure Endpoint 控制台。

过程

步骤 1 选择**集成 (Integration)** > **AMP** > **AMP 管理 (AMP Management)**。

步骤 2 点击**添加 AMP 云连接**。

步骤 3 从**云名称 (Cloud Name)** 下拉列表中，选择要使用的云：

- AMP 云最接近 Cisco Secure Firewall Management Center的地理位置。

  APJC 是指亚太地区/日本/中国。

- 对于 AMP 私有云 (AMPv)，选择 **私有云**，然后如 思科 AMP 私有云，第 1673 页中所述继续操作。

步骤 4 如果要将此云用于 恶意软件防护 和 Cisco Secure EndpointSecure Endpoint，请选中**用于面向 Firepower 的 AMP** 复选框。

如果配置其他云来处理 恶意软件防护（面向 Firepower 的 AMP）通信，则可以清除此复选框；如果这是唯一的 AMP 云连接，则无法清除。

在多域部署中，此复选框仅显示在全局域中。每个 Cisco Secure Firewall Management Center只能有一个恶意软件防护 连接。

步骤 5 点击 **Register**。

旋转状态图标指示连接处于待处理状态，例如，在 Cisco Secure Firewall Management Center 上配置连接后，但在使用 Cisco Secure EndpointSecure Endpoint 控制台对其进行授权之前。**已拒绝**（ ） 表示云已拒绝连接，或者连接因其他原因而失败。

步骤 6 确认是否要继续访问 Cisco Secure EndpointSecure Endpoint 管理控制台，然后登录管理控制台中。

步骤 7 使用管理控制台，授权 AMP 云以将 Cisco Secure EndpointSecure Endpoint 数据发送到 管理中心。

步骤 8 如果要限制 管理中心 接收的数据，请选择您的组织中要为其接收信息的特定组。

默认情况下，AMP 云发送所有组的数据。要管理组，请在 Cisco Secure EndpointSecure Endpoint 管理控制台上选择 **管理** > **组** 。有关详细信息，请参阅设备管理器联机帮助。

步骤 9 点击**允许 (Allow)** 以启用连接并开始传输数据。

点击**拒绝**会将您返回到 Cisco Secure Firewall Management Center，其中连接标记为已拒绝。如果离开 Cisco Secure EndpointSecure Endpoint 管理控制台上的“应用”页面，并且既未拒绝也未允许连接，则连接在 Cisco Secure Firewall Management Center 的 Web 界面上标记为待处理。运行状况监控器在其中任一情况下**不**提示您连接失败。如果稍后要连接到 AMP 云，请删除失败或待处理的连接，然后重新创建连接。

未完成 Cisco Secure EndpointSecure Endpoint 连接注册不会禁用 恶意软件防护 连接。

步骤 10 要验证连接是否已正确配置，请执行以下操作：

a) 在 **集成 (Integration)** > **AMP** > **AMP 管理 (AMP Management)**页面上，点击**思科 AMP 解决方案类型**列中包括**面向终端的 AMP** 的云名称。
b) 在显示的面向终端的 AMP 控制台窗口中，选择**账户** > **应用**。
c) 验证您的 管理中心在列表中。
d) 在面向终端的 AMP 控制台窗口中，选择**管理** > **计算机**。
e) 验证您的 管理中心在列表中。

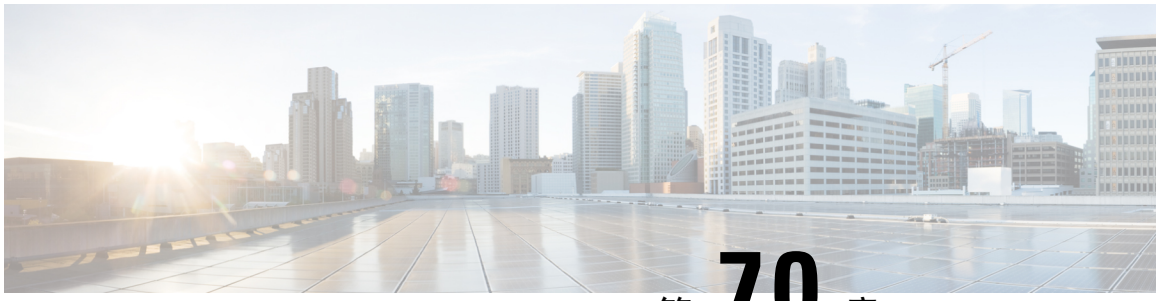
下一步做什么

- 在面向终端的 AMP 控制台窗口中，根据需要配置设置。例如，定义您的管理中心的组成员，并分配策略。有关信息，请参阅面向终端的 AMP 在线帮助或其他文档。
- 在高可用性部署中，必须在 Firepower 管理中心的主用和备用实例上单独配置 AMP 云连接；这些配置是不同步的。
- 如果 管理中心在初始成功连接后无法连接到面向终端的 AMP 门户，或者如果使用 AMP 门户注销了连接，则默认运行状况策略会向您发出警告。

  验证是否在**系统** > **运行状况** > **策略**下启用了**面向终端的 AMP 状态**监控器。

第 XVI 部分

加密流量的处理



第 70 章

流量解密概述

以下主题概述了传输层安全/安全套接字层 (TLS/SSL) 检查，讨论了 TLS/SSL 检查配置的先决条件，并详细介绍了部署场景。

注释 由于 TLS 和 SSL 通常可以互换使用，因此我们使用 *TLS/SSL* 来指示所讨论的任一协议。IETF 已弃用 SSL 协议以支持更安全的 TLS 协议，因此您通常可将 *TLS/SSL* 解读为仅指代 TLS。

但 SSL 策略 是个例外。由于 管理中心 配置选项是 **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**，我们使用术语 *SSL* 策略 ，尽管这些策略是用于定义 TLS 和 SSL 流量的规则。

有关 SSL 和 TLS 协议的更多信息，请参阅 SSL 与 TLS - 差别何在？ 等资源。

流量解密已说明

互联网上的大多数流量都是加密的，并且在大多数情况下您都不希望解密；即使您不这样做，您仍然可以收集有关它的一些信息，并在必要时从网络中阻止它。

您的选择包括：

- 解密流量并对其进行完整的深度检查：
  - 高级恶意软件防护
  - 安全情报
  - 威胁情报导向器
  - 应用检测器

- URL 和类别过滤

- 保持流量加密并设置访问控制和 SSL 策略 以查找并可能阻止：
  - 旧协议版本（例如安全套接字层）
  - 不安全的密码套件
  - 具有高风险和低业务关联性的应用
  - 不可信颁发者的可分辨名称

访问控制策略是一种可调用子策略和其他配置（包括 SSL 策略）的主配置。如果将 SSL 策略与访问控制相关联，则系统会在使用访问控制规则评估加密会话前使用该 SSL 策略对其进行处理。如果没有配置 TLS/SSL或设备不支持，则访问控制规则将处理所有加密流量。

当您的 TLS/SSL配置允许加密流量通过时，访问控制规则也会对其进行处理。但是，某些访问控制规则条件需要未加密流量，因此，已加密流量可能匹配的规则更少。此外，默认情况下，系统禁用已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。

即使策略不需要解密流量，我们也建议将选择性解密作为最佳实践。换句话说，您应该设置一些 TLS/SSL 规则 来查找不需要的应用、密码套件和不安全的协议。这些类型的规则不需要对流量中的数据进行解密，而只用确定流量中是否包含这些不良特征即可。

备注

仅当托管设备处理加密流量时才设置解密规则。TLS/SSL 规则 需要处理可能会影响性能的开销。

只要托管设备启用了 Snort 3，系统就支持解密 TLS 1.3 流量。您可在 SSL 策略 的高级选项中启用 TLS 1.3 解密；有关详细信息，请参阅SSL 策略 高级选项，第 1726 页。

Firepower 系统不支持相互身份验证；也就是说，不能将客户端证书上传到 管理中心 并将其用于**解密 - 重新签名 (Decrypt - Resign)** 或 **解密 - 已知密钥 (Decrypt - Known Key)** TLS/SSL 规则 操作。有关详细信息，请参阅解密和重新签名（传出流量），第1712页和已知密钥解密（传入流量），第1713页。

如果使用 FlexConfig 设置 TCP 最大分段大小 (MSS) 的值，则观察到的 MSS 可能会小于您的设置。有关详细信息，请参阅关于 TCP MSS，第 566 页。

相关主题

TLS/SSL 握手处理，第 1704 页
TLS/SSL 最佳实践，第 1710 页

TLS/SSL 握手处理

在本文档中，术语 *TLS/SSL* 握手表示启动 SSL 协议及其后续协议 TLS 中的加密会话的双向握手。

在内联部署中，Firepower 系统处理可能会修改 ClientHello 消息并用作会话的 TCP 代理服务器的 TLS/SSL 握手。

下图显示了内联部署。

客户端确立与服务器的 TCP 连接后（成功完成 TCP 三向握手后），托管设备会监控 TCP 会话的任何启动加密会话的尝试。TLS/SSL 握手通过使用交换客户端与服务器之间的专门数据包来确立加密会话。在 SSL 和 TLS 协议中，这些专门数据包称为握手消息。握手消息传达客户端和服务器都支持的加密属性：

- ClientHello - 客户端为每个加密属性指定多个受支持的值。
- ServerHello - 服务器为每个加密属性指定一个受支持的值，而 ServerHello 响应会确定安全会话期间系统使用的加密方法。

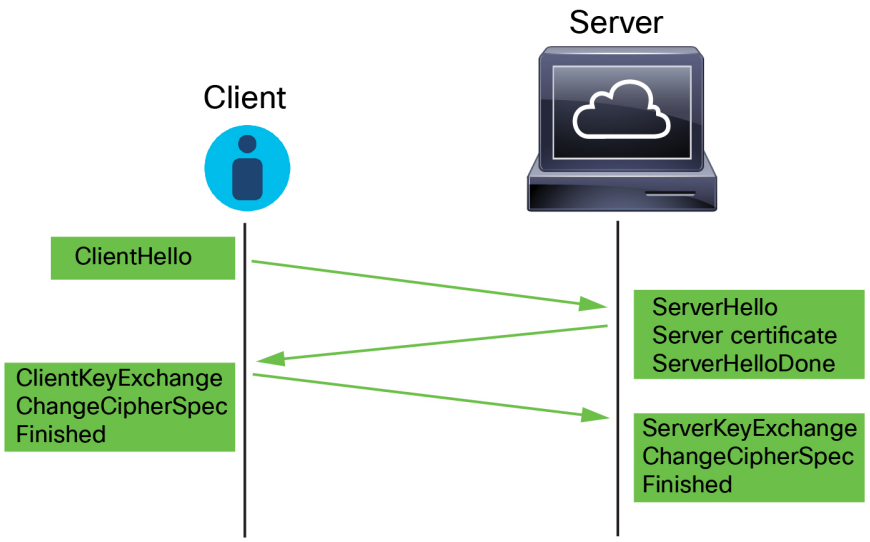
TLS/SSL 握手完成后，受管设备缓存加密会话数据，这允许在不需要完全握手的情况下进行会话恢复。受管设备还缓存服务器证书数据，这允许在使用相同证书的后续会话中更快速地处理握手。

ClientHello 消息的处理

客户端将 ClientHello 消息发送到一台服务器，如果可以建立安全连接，则该服务器将作为数据包的目标。客户端发送信息以启动 TLS/SSL 握手，或者用于响应目标服务器的 ServerHello 消息。

概述

下图显示了一个示例。另请参阅 RFC 8446，第 4 节 。您还可以参考 cheapsslshop.com 上的了解 SSL/TLS 握手协议等资源。



该过程可汇总如下：

1. ClientHello 启动该过程。

ClientHello 消息包含服务器名称指示 (SNI)，其中包含服务器的完全限定域名。

2. 当受管设备处理 ClientHello 消息并将其传输到目标服务器后，服务器会确定其是否支持客户端在该消息中指定的解密属性。如果不支持这些属性，服务器将向客户端发送握手失败警报。如果支持这些属性，服务器将发送 ServerHello 信息。如果商定的密钥交换方法使用证书进行身份验证，则服务器证书消息会紧跟在 ServerHello 消息之后。

   服务器证书包含使用者可选名称 (SAN)，可以具有完全限定的域名和 IP 地址。有关 SAN 的详细信息，请参阅可分辨名称 ，第 983 页。

3. 当受管设备收到这些消息时，会尝试将其与系统上配置的 TLS/SSL 规则相匹配。这些消息包含 ClientHello 消息或会话数据缓存中缺少的信息。具体而言，系统可能会匹配关于 TLS/SSL 规则的可分辨名称、证书状态、密码套件和版本条件的这些消息。

整个过程都会别加密。

数据交换

如果配置 TLS/SSL 解密，则当托管设备收到 ClientHello 消息时，系统会尝试将此消息与进行**解密 - 重新签名 (Decrypt - Resign)** 或**解密 - 已知密钥 (Decrypt - Known Key)** 操作的 TLS/SSL 规则 规则进行匹配。该匹配依赖于来自 ClientHello 消息的数据，以及来自缓存服务器证书数据的数据。可能的数据包括：

表 *198: TLS/SSL* 规则 条件的数据可用性

TLS/SSL 规则 条件	数据所在位置
区域	ClientHello
网络	ClientHello
VLAN Tags	ClientHello
端口	ClientHello
用户	ClientHello
应用	ClientHello（服务器名称指示器扩展）
类别	ClientHello（服务器名称指示器扩展）
证书	服务器证书（可能已缓存）
可分辨名称	服务器证书（可能已缓存）
证书状态	服务器证书（可能已缓存）
Cipher Suites	ServerHello
个版本	ServerHello

注释 仅在具有**阻止**或**阻止并重置**规则操作的规则中使用**密码套件 (Cipher Suite)** 和**版本 (Version)** 规则条件。在具有其他规则操作的规则中使用这些条件可能会干扰系统的 ClientHello 处理，从而导致不可预测的性能。

ClientHello 修改

如果 ClientHello 消息与**解密 - 重新签名 (Decrypt-Resign)** 或 **解密 - 已知密钥 (Decrypt - Known Key)** 规则匹配，则系统会按如下方式修改 ClientHello 消息：

- （仅 TLS 1.2；TLS 1.3 不支持压缩。）压缩方法 - 删除 `compression_methods` 元素（其指定客户端所支持的压缩方法）。系统无法解密压缩的会话。
- 密码套件 - 如果系统不支持密码套件，则从 `cipher_suites` 元素中删除它们。如果系统不支持任何指定的密码套件，则系统将传输原始的未经修改的元素。此修改会减少无法解密的流量的“未知密码套件”(Unknown Cipher Suite) 和“不受支持的密码套件”(Unsupported Cipher Suite) 类型。
- 会话标识符 - 删除 `Session Identifier` 元素和 SessionTicket extension (RFC 5077, sec 3.2) 中任何与缓存会话数据不匹配的值。如果 ClientHello 值与缓存数据相匹配，则中断的会话无需客户端和服务器执行完整的 TLS/SSL 握手操作也可恢复。此修改会增加会话恢复的机会，并减少无法解密的流量的“不缓存会话”(Session Not Cached) 类型。
- 椭圆曲线 - 如果系统不支持椭圆曲线，则从受支持的椭圆曲线扩展中删除它们。如果系统不支持任何指定的椭圆曲线，则受管设备将删除扩展，并从 `cipher_suites` 元素中删除任何相关的密码套件。
- ALPN 扩展 - 删除应用层协议协商 (ALPN) 扩展中不受系统支持的任意值（例如，HTTP/2 协议）。
- 其他扩展 - 删除下次协议协商 (NPN) 和 TLS 通道 ID 扩展。

  目前，具有**解密 - 重新签名**或**解密 - 已知密钥**操作的 TLS/SSL 规则 在 ClientHello 协商期间在本地支持扩展主密钥 (EMS) 扩展，从而实现更安全的通信。EMS 扩展由 RFC 7627 定义。

在系统修改 ClientHello 消息后，它会确定消息是否通过访问控制评估（可能包括深度检测）。如果消息通过评估，则系统会将其传输到目标服务器。

如果 ClientHello 消息与**解密 - 重新签名 (Decrypt-Resign)** 或**解密 - 已知密钥 (Decrypt - Known Key)** 规则不匹配，则系统不会修改消息。然后，它会确定消息是否通过访问控制评估（可能包括深度检查）。如果消息通过检查，则系统会将其传输到目标服务器。

如果流量与**监控**规则条件匹配，则不会修改 ClientHello。

中间人

在 TLS/SSL 握手过程中，客户端和服务器之间无法再进行直接通信，因为在消息修改之后，由客户端和服务器计算的消息身份验证代码 (MAC) 不再匹配。对于所有后续的握手消息（和已建立的加密

会话），托管设备将充当中间人。它创建两个 TLS/SSL 会话，一个是客户端与受管设备之间的会话，一个是受管设备与服务器之间的会话。因此，每个会话包含不同的加密会话详细信息。

注释 系统可以解密的密码套件会频繁更新，且其无法直接对应于您可以在 TLS/SSL 规则 条件中使用的密码套件。有关可解密密码套件的当前列表，请联系思科 TAC。

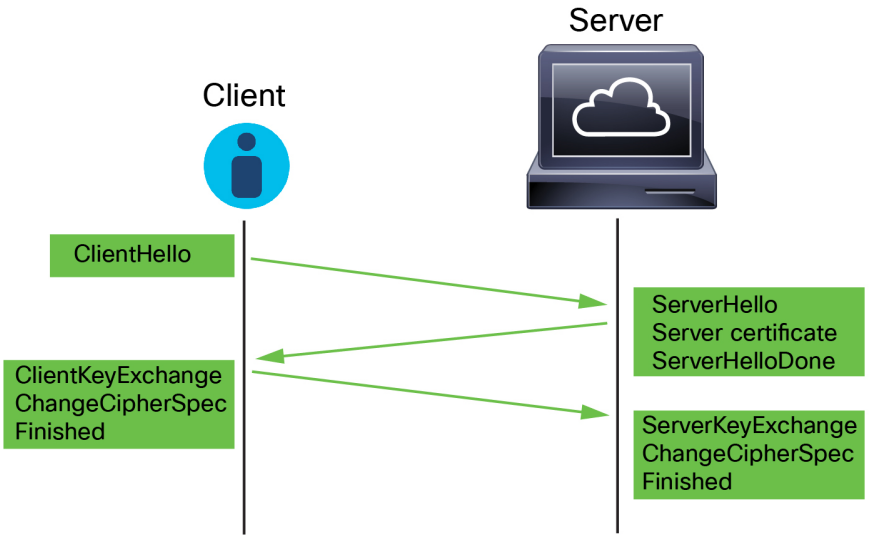
相关主题

无法解密流量的默认处理选项，第 1725 页
ServerHello 和服务器证书消息处理，第 1708 页

ServerHello 和服务器证书消息处理

概述

下图显示了一个示例。另请参阅 RFC 8446，第 4 节 。您还可以参考 cheapsslshop.com 上的了解 SSL/TLS 握手协议等资源。



该过程可汇总如下：

1. ClientHello 启动该过程。

   ClientHello 消息包含服务器名称指示 (SNI)，其中包含服务器的完全限定域名。

2. 当受管设备处理 ClientHello 消息并将其传输到目标服务器后，服务器会确定其是否支持客户端在该消息中指定的解密属性。如果不支持这些属性，服务器将向客户端发送握手失败警报。如果支持这些属性，服务器将发送 ServerHello 信息。如果商定的密钥交换方法使用证书进行身份验证，则服务器证书消息会紧跟在 ServerHello 消息之后。

   服务器证书包含使用者可选名称 (SAN)，可以具有完全限定的域名和 IP 地址。有关 SAN 的详细信息，请参阅可分辨名称，第 983 页。

3. 当受管设备收到这些消息时，会尝试将其与系统上配置的 TLS/SSL 规则相匹配。这些消息包含 ClientHello 消息或会话数据缓存中缺少的信息。具体而言，系统可能会匹配关于 TLS/SSL 规则的可分辨名称、证书状态、密码套件和版本条件的这些消息。

整个过程都会别加密。

TLS/SSL 规则 操作

如果消息与任何 TLS/SSL 规则 都不匹配，托管设备将执行 SSL 策略 默认操作，第 1724 页。

如果消息与属于与访问控制策略关联的 SSL 策略 的规则匹配，则托管设备会根据需要继续：

操作：“监控”(Monitor)

TLS/SSL 握手继续完成。托管设备会跟踪和记录已加密的流量，但不会对其进行解密。

操作：“阻止”(Block) 或“阻止并重置”(Block with reset)

托管设备会阻止 TLS/SSL 会话，并重置 TCP 连接（如已配置）。

操作：“不解密”(Do Not Decrypt)

TLS/SSL 握手继续完成。受管设备不解密 TLS/SSL 会话期间交换的应用数据。

操作：“解密 - 已知密钥”(Derypt - Known Key)

托管设备尝试将服务器证书数据与先前导入管理中心的内部证书对象进行匹配。由于您无法生成内部证书对象，并且您必须拥有其私钥，因此假设您拥有在其上使用已知密钥解密的服务器。

如果此证书与已知证书匹配，则 TLS/SSL 握手将继续完成。受管设备使用上传的私钥解密并重新加密 TLS/SSL 会话期间交换的应用数据。

如果服务器在与客户端的初始连接和后续连接之间更改其证书，则必须在管理中心 中导入新服务器证书，以便用于将来解密连接。

操作：“解密 - 重新签名”(Decrypt - Resign)

托管设备将处理服务器证书消息并使用之前上传或生成的证书颁发机构 (CA) 证书重签服务器证书。TLS/SSL 握手继续完成。托管设备随手会使用上传的私钥解密并重新加密 TLS/SSL 会话期间交换的应用数据。

注释 Firepower 系统不支持相互身份验证；也就是说，不能将客户端证书上传到 管理中心 并将其用于**解密 - 重新签名 (Decrypt - Resign)** 或 **解密 - 已知密钥 (Decrypt - Known Key)** TLS/SSL 规则 操作。有关详细信息，请参阅解密和重新签名（传出流量），第 1712 页和已知密钥解密（传入流量），第 1713 页。

相关主题

ClientHello 消息的处理，第 1705 页

TLS/SSL 最佳实践

本节讨论创建 SSL 策略 和规则时应牢记的信息。

注释 由于 TLS 和 SSL 通常可以互换使用，因此我们使用 *TLS/SSL* 来指示所讨论的任一协议。IETF 已弃用 SSL 协议以支持更安全的 TLS 协议，因此您通常可将 *TLS/SSL* 解读为仅指代 TLS。

但 SSL 策略 是个例外。由于 管理中心 配置选项是 **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**，我们使用术语 *SSL* 策略，尽管这些策略是用于定义 TLS 和 SSL 流量的规则。

有关 SSL 和 TLS 协议的更多信息，请参阅 SSL 与 TLS - 差别何在？等资源。

相关主题

解密案例，第 1710 页
何时解密流量以及何时不解密，第 1711 页
其他 TLS/SSL 规则 操作，第 1713 页
TLS/SSL 规则 组件，第 1714 页
TLS/SSL 规则 顺序评估，第 1715 页
TLS 1.3 解密最佳实践

解密案例

只能允许或阻止通过系统时加密的流量，但不能对其进行深度检查或全面的策略实施（例如入侵防御）。

所有已加密的连接：

- 通过 SSL 策略 发送，以确定是否应解密或阻止它们。

  您还可以配置 TLS/SSL 规则 以阻止您知道不想在网络上传输的类型的加密流量，例如使用非安全 SSL 协议的流量或具有过期或无效证书的流量。

- 如果未被阻止，无论是否解密，流量都要经过访问控制策略，以做出最终的允许或阻止决定。

只有已解密的流量才能利用系统的威胁防御和策略实施功能，例如：

- 高级恶意软件防护
- 安全情报
- 威胁情报导向器
- 应用检测器
- URL 和类别过滤

请记住，解密并重新加密流量会增加设备的处理负载，从而会降低整体系统性能。

我们建议选择性地解密流量，以充分利用访问控制策略和深度检查。

总结：

- 可以通过策略允许或阻止已加密的流量；无法检查已加密的流量
- 已解密的流量受威胁防御和策略实施的约束；可以通过策略允许或阻止已解密的流量

相关主题

使用文件和入侵策略的深度检测，第 1244 页

何时解密流量以及何时不解密

本节提供有关何时应解密流量以及何时应允许其通过加密防火墙的准则。

何时不解密流量

如果是以下情况，则不应对流量进行解密：

- 法律所禁止；例如，某些司法管辖区禁止解密财务信息
- 公司政策所禁止；例如，您的公司可能会禁止解密特权通信
- 隐私法规所禁止
- 使用证书固定（也称为*TLS/SSL*固定）的流量必须保持加密，以防止断开连接

（Snort 2。）如果选择绕行某些类型的流量的解密，则不会对流量进行任何处理。加密流量会首先由 SSL 策略 进行评估，然后进入访问控制策略，在其中做出最终的允许或阻止决策。

（Snort 3。）对于任何符合访问控制规则的“信任”(Trust)、“阻止”(Block)或“阻止并重置”(Block with reset) 的连接，除非流量被预先过滤，否则 SSL 策略 不会被绕过。加密流量会首先由 SSL 策略进行评估，然后进入访问控制策略，在其中做出最终的允许或阻止决策。

加密流量可以在任何 TLS/SSL 规则 条件下被允许或阻止，包括但不限于：

- 证书状态（例如，证书已过期或无效）
- 协议（例如，非安全 SSL 协议）
- 网络（安全区域、IP 地址、VLAN 标记等）
- 确切的 URL 或 URL 类别
- Port
- 用户组

TLS/SSL 规则 为此流量提供**不解密**操作；有关详细信息，请参阅TLS/SSL 规则 不解密操作，第 1761 页。

注释 本主题末尾的相关信息链接解释了规则评估的某些方面是如何运作的。URL 和应用过滤等条件对加密流量存在限制。请确保您了解这些限制。

有关在**不解密**规则中使用 URL 过滤的详细信息，请参阅TLS/SSL 规则 不解密操作，第 1761 页。

何时解密流量

系统的威胁防护和策略实施功能必须在解密所有加密流量后才能发挥作用。如果托管设备允许解密流量（取决于其内存和处理能力），则应解密法律或法规未禁止的流量。如果您必须决定哪些流量要解密，请根据网络上允许流量的风险做出决定。系统提供了一个灵活框架，它会利用规则条件（包括 URL 信誉、密码套件、协议和许多其他因素）来对流量进行分类。

相关主题

解密和重新签名（传出流量），第 1712 页
已知密钥解密（传入流量），第 1713 页
TLS/SSL 规则 准则和限制，第 1731 页
SSL 规则顺序
URL 条件（URL 过滤）
应用规则顺序，第 1256 页
TLS 1.3 解密最佳实践

解密和重新签名（传出流量）

解密 - 重新签名 (Decrypt - Resign) TLS/SSL 规则 操作使系统能够充当中间人，拦截、解密以及（如果允许流量通过）检查和重新加密。**解密 - 重新签名 (Decrypt - Resign)** 规则操作用于传出流量；也就是说，目的服务器在受保护的网络之外。

威胁防御 设备会使用规则中指定的内部证书颁发机构 (CA) 对象来与客户端协商，并在客户端和 威胁防御 设备之间建立 TLS/SSL 隧道。同时，设备连接至目标网站，并在服务器和 威胁防御 设备之间建立 SSL 隧道。

因此，客户端将看到配置用于 TLS/SSL 规则 的 CA 证书，而不是来自目标服务器的证书。客户端必须信任防火墙的证书才能完成连接。威胁防御 设备随后会对客户端和目标服务器之间的流量执行双向解密/重新加密。

前提条件

要使用**解密 - 重新签名 (Decrypt - Resign)** 规则操作，您必须使用 CA 文件和配对的私钥文件创建内部 CA 对象。如果您还没有 CA 和私钥，则可以在系统中生成它们。

注释 Firepower 系统不支持相互身份验证；也就是说，不能将客户端证书上传到 管理中心 并将其用于**解密 - 重新签名 (Decrypt - Resign)** 或 **解密 - 已知密钥 (Decrypt - Known Key)** TLS/SSL 规则 操作。有关详细信息，请参阅解密和重新签名（传出流量），第 1712 页和已知密钥解密（传入流量），第 1713 页。

相关主题

TLS/SSL 规则 解密操作，第 1762 页
外部证书对象，第 1008 页

已知密钥解密（传入流量）

解密 - 已知密钥 (Decrypt - Known Key) TLS/SSL 规则 操作使用服务器的私钥解密流量。**解密 - 已知密钥 (Decrypt - Known Key)** 规则操作用于传入流量；也就是说，目的服务器位于受保护的网络内。

使用已知密钥进行解密的主要目的是保护服务器免受外部攻击。

前提条件

要使用**机密 - 已知密钥 (Decrypt - Known Key)** 规则操作，您必须使用服务器的证书文件和配对的私钥文件来创建内部证书对象。

注释 Firepower 系统不支持相互身份验证；也就是说，不能将客户端证书上传到 管理中心 并将其用于**解密 - 重新签名 (Decrypt - Resign)** 或 **解密 - 已知密钥 (Decrypt - Known Key)** TLS/SSL 规则 操作。有关详细信息，请参阅解密和重新签名（传出流量），第 1712 页和已知密钥解密（传入流量），第 1713 页。

相关主题

已知密钥解密（传入流量），第 1713 页
TLS/SSL 规则 解密操作，第 1762 页
内部证书对象，第 1008 页

其他 TLS/SSL 规则 操作

以下各部分讨论其他 TLS/SSL 规则 操作。

相关主题

TLS/SSL 规则 阻止操作，第 1762 页
TLS/SSL 规则 监控操作，第 1760 页

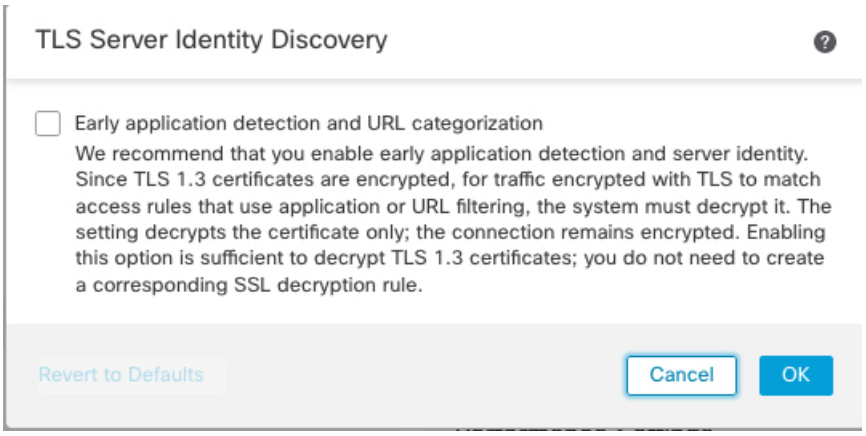
TLS 1.3 服务器身份发现

RFC 8446定义的最新版本的传输层安全（TLS）协议 1.3 是许多 Web 服务器提供安全通信的首选协议。由于 TLS 1.3 协议会加密服务器的证书以提高安全性，并且需要使用证书来匹配访问控制规则中的应用和 URL 过滤条件，因此 Firepower 系统提供了一种提取服务器证书而 不 解密整个数据包的方法。

在为访问控制策略配置高级设置时，可以启用此功能，称为 *TLS* 服务器身份发现。

我们强烈建议您为要根据应用或URL条件匹配的任何流量启用此功能，尤其是在您想要对该流量执行深度检查时。SSL 策略 不需要 SSL 策略，因为在提取服务器证书的过程中不会解密流量。

下图显示在访问控制策略的高级设置中启用 TLS 服务器身份发现的示例。



相关主题

创建基本 SSL 策略，第 1728 页
将其他策略与访问控制相关联，第 1276 页

TLS/SSL 规则 组件

每个 TLS/SSL 规则 都有以下组件。

状态

默认情况下，规则处于启用状态。如果您禁用某规则，系统将不用它来评估网络流量并停止为该规则生成警告和错误。

位

SSL 策略 中的规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。除 Monitor 规则之外，流量匹配的第一个规则是处理该流量的规则。

条件

条件指定规则处理的特定流量。条件可以按安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL、用户、证书、证书使用者或颁发者、证书状态、密码套件或加密协议版本来匹配流量。使用条件取决于目标设备许可证。

操作

规则操作确定系统如何处理匹配的流量。您可以对加密的匹配流量执行监控、允许、阻止或解密操作。解密和允许的加密流量会受到进一步检查。请注意，系统不对被阻止的加密流量执行检查。

日志记录

规则的日志记录设置管理系统保存其处理流量的记录。您可以对匹配规则的流量保存记录。您可以在系统阻止加密会话或允许其未经解密便通过（取决于 SSL 策略中的设置）时记录连接。无论系统

稍后如何处理或检查流量，您都可以强制系统记录其解密的连接，以通过访问控制规则进一步检查。您可以将连接记录到Cisco Secure Firewall Management Center数据库，以及系统日志 (syslog) 或 SNMP 陷阱服务器中。

提示 正确创建 TLS/SSL 规则 并对其排序是一项复杂的任务。如果不认真规划您的策略，这些规则会抢占其他规则，需要额外的许可证或包含无效配置。为帮助确保系统按预期处理流量，SSL 策略接口具有功能强大的规则警告和错误反馈系统。

TLS/SSL 规则 顺序评估

在 SSL 策略 中创建 TLS/SSL 规则 时，您可以使用规则编辑器中的**插入 (Insert)** 列表来指定其位置。SSL 策略 中的 TLS/SSL 规则 会从 1 开始编号。系统按升序规则编号以自上而下的顺序将流量与 TLS/SSL 规则 相匹配。

在大多数情况下，系统根据第一个 TLS/SSL 规则（其中所有规则的条件都与流量相匹配）处理网络流量。除了 Monitor 规则（记录流量，但不影响流量）之外，系统在流量匹配一个规则后，不再继续根据其他低优先级规则评估流量。条件可以简单也可以复杂；可以按安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL、用户、证书、证书可分辨名称、证书状态、密码套件或加密协议版本来控制流量。

每个规则也具有操作，用于确定是使用访问控制监控、阻止还是检测匹配的已加密或已解密流量。请注意，系统不会进一步检查其阻止的加密流量，它会通过访问控制来检查加密流量和无法解密的流量。但是，访问控制规则条件需要未加密流量，因此，已加密流量匹配的规则更少。

使用特定条件（例如网络和 IP 地址）的规则应在使用一般条件（例如应用）的规则之前排序。如果您熟悉开放系统互联（OSI）模型，请在概念上使用类似的编号。包含第 1 层、第 2 层和第 3 层（物理、数据链路和网络）条件的规则应首先在规则中排序。稍后应在规则中对第 5 层、第 6 层和第 7 层的条件（会话，表示和应用）进行排序。有关 OSI 模型的详细信息，请参阅此 维基百科文章。

提示 适当的 TLS/SSL 规则 顺序可减少处理网络流量所需的资源，并防止规则抢占。尽管您创建的规则对于每个组织和部署来说都是唯一的，但是排序规则时需要遵循几个基本原则，才可优化性能，同时满足您的需求。

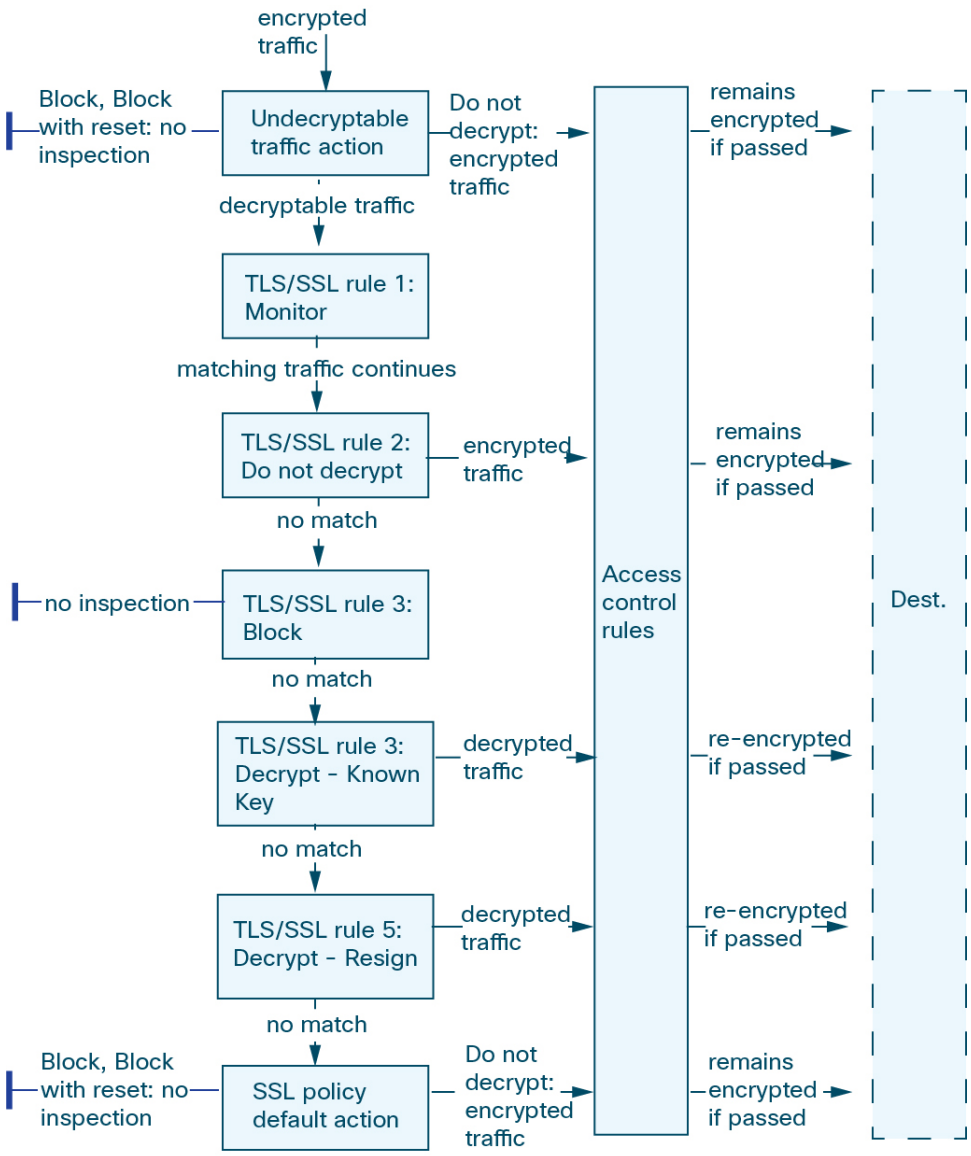
除了按照编号排序规则之外，还可按类别对规则进行分组。默认情况下，系统提供三个类别：管理员、标准和根。您可以添加自定义类别，但是不能删除系统提供的类别或更改类别的顺序。

相关主题

访问控制规则的最佳实践，第 1253 页
无法解密流量的默认处理选项，第 1725 页
SSL 规则顺序

多规则示例

下述场景概括说明了 TLS/SSL 规则在内联部署中处理流量的方式。



在这种情况中，流量评估如下：

- 首先，**Undecryptable Traffic Action** 评估加密流量。对于系统无法解密的流量，系统会将其阻止而不进一步检查，或者使其通过以进行访问控制检查。不匹配的加密流量继续根据下一规则进行评估。
- 其次，使用 **TLS/SSL 规则 1: Monitor** 评估加密流量。Monitor 规则跟踪和记录加密流量，但不对流量做出任何影响。系统继续根据其他规则匹配流量，以确定允许其通过，还是拒绝。
- 第三，使用 **TLS/SSL 规则 2: Do Not Decrypt** 评估加密流量。匹配流量未解密；系统通过访问控制检查此流量，但不执行文件或入侵检测。不匹配的流量继续根据下一规则进行评估。
- 第四，使用 **TLS/SSL 规则 3: Block** 评估加密流量。匹配的流量被阻止，无需进一步检测。不匹配的流量继续根据下一规则进行评估。

- 第五，使用 **TLS/SSL 规则 4: Decrypt - Known Key** 评估加密流量。系统使用您上传的私钥对传入网络的匹配流量进行解密。然后，根据访问控制规则评估解密流量。访问控制规则以相同方式处理已解密和未加密的流量。作为此额外检查的结果，系统可以阻止流量。所有剩余流量将被重新加密，才会被传输到目标。与 TLS/SSL 规则 不匹配的流量会继续根据下一规则进行评估。
- **TLS/SSL 规则 5: Decrypt - Resign** 是最终规则。如果流量与此规则相匹配，则系统使用已上传的 CA 证书对服务器证书重新签名，然后充当中间人解密流量。然后，根据访问控制规则评估解密流量。访问控制规则以相同方式处理已解密和未加密的流量。作为此额外检查的结果，系统可以阻止流量。所有剩余流量将被重新加密，才会被传输到目标。与 SSL 规则不匹配的流量继续根据下一规则进行评估。
- **SSL 策略 Default Action** 会处理与任何 TLS/SSL 规则 不匹配的所有流量。默认操作为以下两种方式之一：阻止加密流量，且不进一步检查；不解密流量而允许传输，以进行访问控制检查。

TLS 加密加速

TLS 加密加速 加快以下操作：

- TLS/SSL 加密和解密。
- VPN，包括TLS/SSL和 IPsec

支持的硬件

以下硬件型号支持 TLS 加密加速：

- Firepower 3100 和 Cisco Secure Firewall Threat Defense
- 采用 Cisco Secure Firewall Threat Defense 的 Firepower 2100
- 采用 Cisco Secure Firewall Threat Defense的 Firepower 4100/9300

  有关 TLS 加密加速Firepower 4100/9300 支持威胁防御 容器实例的信息，请参阅 *FXOS* 配置指南。

所有虚拟设备或除前面所述设备之外的任何硬件上都不支持 TLS 加密加速。

注释 有关 TLS 加密加速 和 4100/9300 的详细信息，请参阅 *FXOS* 配置指南。

以下方不支持的功能 TLS 加密加速

TLS 加密加速不支持的功能包括：

- 启用了 威胁防御 容器实例 的托管设备。

- 如果检测引擎配置为保留连接，并且检测引擎意外出现故障，则 TLS/SSL流量将被丢弃，直到引擎重启。

  此行为受 **configure snort preserve-connection {enable | disable}** 命令控制。

TLS 加密加速 准则和限制

如果受管设备启用了 TLS 加密加速，请记住以下几点。

仅 HTTP 性能

在不对流量进行解密的受管设备上使用 TLS 加密加速可能会影响性能。

联邦信息处理标准 (FIPS)

如果同时启用了 TLS 加密加速 和联邦信息处理标准 (FIPS)，则与以下选项的连接会失败：

- 大小小于 2048 字节的 RSA 密钥
- Rivest 密码 4 (RC4)
- 单一数据加密标准（单一 DES）
- Merkle – Damgard 5 (MD5)
- SSL v3

当您将 管理中心 和受管设备配置为以安全认证合规模式运行时，FIPS 会被启用。在这些模式下运行时，要允许连接，则可配置 Web 浏览器以接受更为安全的选项。

更多详情：

- FIPS 支持的密码：关于 SSL 设置，第 628 页。
- 安全认证合规性模式，第 221 页。
- 通用标准。

TLS 心跳

某些应用使用 RFC6520 定义的传输层安全 (TLS) 和数据报传输层安全 (DTLS) 协议的 *TLS* 心跳扩展。SSL 心跳可用于确认连接是否仍处于活动状态 - 客户端或服务器发送指定字节数的数据，并请求另一方回送响应。如果此过程成功，则发送加密的数据。

当启用 TLS 加密加速的受管设备遇到使用 SSL 检测信号扩展的数据包时，受管设备将执行 SSL 策略 的**无法解密的操作**中**解密错误**的设置所指定的操作：

- 阻止
- 阻止并重置

有关详细信息，请参阅无法解密流量的默认处理选项，第 1725 页。

要确定应用是否正在使用 TLS 心跳，请参阅对 TLS 心跳进行故障排除。

您可以在网络分析策略 (NAP) 中配置**最大心跳长度**，以便确定如何处理 TLS 心跳。有关详细信息，请参阅SSL 预处理器， 第 2129 页。

TLS/SSL 超订用

TLS/SSL 超订用是受管设备过载 TLS/SSL 流量的状态。任何受管设备都可能会遇到 TLS/SSL 超订用，但只有支持 TLS 加密加速的受管设备才提供可配置的方式对其进行处理。

启用了 TLS 加密加速 的受管设备在超订用时，受管设备接收的任何数据包都根据 SSL 策略 的**无法解密的操作**中**握手错误**设置进行处理：

- 继承默认操作
- 不解密
- 阻止
- 阻止并重置

如果 SSL 策略的**无法解密的操作**中**握手错误**的设置为**不解密**，且相关的访问控制策略配置为检查流量，则检查会发生；但是解密不会发生。

如果出现大量超订用，有以下选项可供选择：

- 升级受管设备以提高 TLS/SSL 处理能力。
- 更改您的 SSL 策略，为不具有较高解密优先级的流量添加**不解密**规则。

查看 TLS 加密加速的状态

本主题讨论如何确定是否已启用 TLS 加密加速。

请执行 管理中心 中的下列任务。

过程

步骤 1 登录管理中心。

步骤 2 点击**设备** > **设备管理**。

步骤 3 点击 **编辑**（ ） 以编辑受管设备。

步骤 4 点击**设备 (Device)**页面。TLS 加密加速 状态显示在“常规”(General) 部分中。

如何配置 SSL 策略 和规则

本主题简要概述要在这些策略中配置 SSL 策略和 TLS/SSL 规则而必须完成的任务，以便阻止、监控或允许网络上的 TLS/SSL 流量。

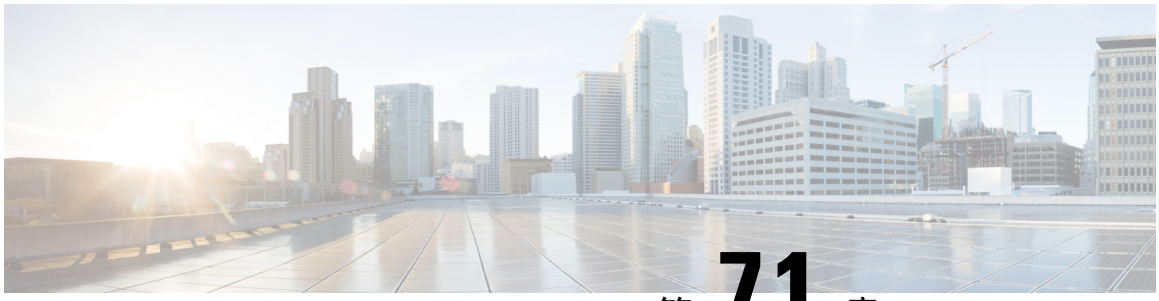
您必须是 管理员、访问管理员 或 网络管理员 才能执行此任务。

过程

	命令或操作	目的
步骤 1	创建an SSL 策略。	An SSL 策略 是一个或多个规则的容器。要使用 an SSL 策略 及其规则进行访问控制，您必须稍后将 SSL 策略 与访问控制策略关联。有关详细信息，请参阅创建基本 SSL 策略，第 1728 页。
步骤 2	为您的 SSL 策略 设置默认操作。	当流量与 SSL 策略 定义的规则不匹配时将采取默认操作。请参阅SSL 策略 默认操作，第 1724 页。
步骤 3	指定应如何处理无法解密的流量。	流量无法解密的原因有很多，包括协议不安全、使用和未知的密码套件，或者在握手或解密错误的情况下。请参阅无法解密流量的默认处理选项，第 1725 页。
步骤 4	对于**解密 - 已知密钥 (Decrypt - Known Key)**（用于解密流向网络中服务器的入站流量）TLS/SSL 规则，请创建内部证书对象。	内部证书对象使用您的服务器的证书和私钥。请参阅内部证书对象，第 1008 页。
步骤 5	对于**解密 - 重新签名 (Decrypt - Resign)**（解密流向网络外部服务器的出站流量）TLS/SSL 规则，请创建内部证书颁发机构 (CA) 对象。	内部 CA 对象会使用 CA 和私钥。请参阅内部证书颁发机构对象，第 1001 页。
步骤 6	创建您的 TLS/SSL 规则。	
步骤 7	将 SSL 策略 与访问控制策略关联。	除非您将 SSL 策略 与访问控制策略相关联，否则它不会起作用。在执行此操作后，您可以选择允许或阻止与访问控制规则匹配的流量并执行其他操作。请参阅将其他策略与访问控制相关联，第 1276 页。
步骤 8	配置访问控制规则，以便允许或阻止已解密的流量。	请参阅访问控制策略组件，第 1259 页。
步骤 9	将访问控制策略部署到托管设备。	在策略生效之前，必须将其部署到托管设备。请参阅部署配置更改，第 136 页。

相关主题

TLS/SSL 规则，第 1731 页



第 71 章

SSL 策略

以下主题概述 SSL 策略 的创建、部署、管理和日志记录。

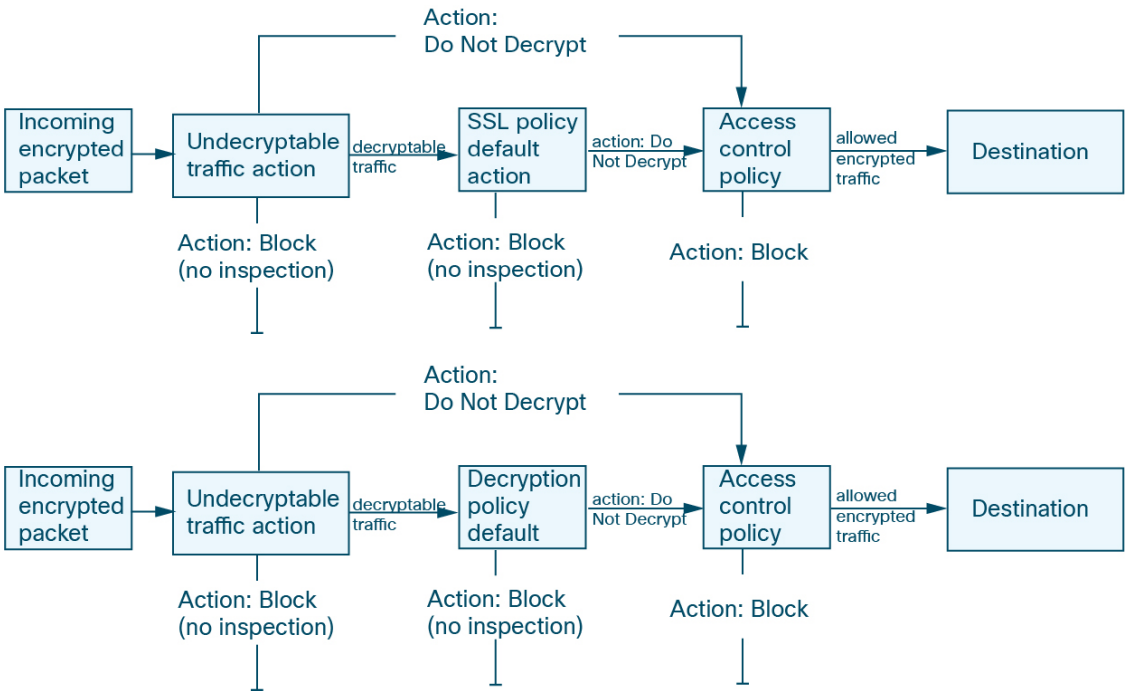
SSL 策略概述

An SSL 策略 确定系统如何处理网络上的加密流量。可以配置一个或多个 SSL 策略，将 an SSL 策略与访问控制策略关联起来，然后将访问控制策略部署到受管设备。当设备检测到 TCP 握手时，访问控制策略首先处理并检查流量。如果它随后识别出通过 TCP 连接建立的 TLS/SSL加密会话，则 SSL 策略将接管、处理和解密已加密的流量。

⚠

注意 仅*Snort 2*。添加或删除构件SSL 策略 在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为， 第 144 页。

最简单的 SSL 策略（如下图所示）引导其部署所在设备，以使用单个默认操作处理加密流量。可将默认操作设置为阻止可解密流量（无需进一步检查），或者使用访问控制检查未解密的可解密流量。然后系统可以允许或阻止已加密的流量。如果设备检测到无法解密的流量，它会阻止该流量，无需进一步检查或不对其进行解密，而是使用访问控制对其进行检查。



更为复杂的 SSL 策略可通过不同的操作处理不同类型无法解密的流量，根据证书颁发机构 (CA) 是否颁发或信任加密证书而控制流量，以及使用 TLS/SSL 规则 规则对已加密流量的日志记录和处理进行精细控制。这些规则可能很简单，也可能很复杂，使用多个条件匹配和检查已加密的流量。

注释 由于 TLS 和 SSL 通常可以互换使用，因此我们使用 *TLS/SSL* 来指示所讨论的任一协议。IETF 已弃用 SSL 协议以支持更安全的 TLS 协议，因此您通常可将 *TLS/SSL* 解读为仅指代 TLS。

但 SSL 策略 是个例外。由于 管理中心 配置选项是 **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**，我们使用术语 *SSL* 策略 ，尽管这些策略是用于定义 TLS 和 SSL 流量的规则。

有关 SSL 和 TLS 协议的更多信息，请参阅 SSL 与 TLS - 差别何在？ 等资源。

相关主题

TLS/SSL 规则 条件 ， 第 1743 页

SSL 策略 默认操作

an SSL 策略的默认操作确定系统如何处理与策略中任何非监控规则都不匹配的可解密的已加密流量。当部署不包含任何 TLS/SSL 规则 规则的 an SSL 策略时，默认操作确定如何处理网络上所有无法解密的流量。请注意，对于默认操作阻止的已加密流量，系统不会执行任何类型的检查。

表 *199: SSL* 策略 默认操作

默认操作	对已加密流量的影响
阻止	阻止 TLS/SSL 会话，无需进一步检查。
阻止并重置	阻止 TLS/SSL 会话并且无需进一步检查，然后重置 TCP 连接。如果流量使用的是像 UDP 一样的无连接协议，请选择此选项。在这种情况下，无连接协议将尝试重新建立连接，直到被重置。 执行此操作时，浏览器中还会显示连接重置错误，以便用户知道连接被阻止。
不解密	使用访问控制检查已加密的流量。

相关主题

创建基本 SSL 策略，第 1728 页

无法解密流量的默认处理选项

表 *200:* 无法解密的流量类型

类型	说明	默认操作	可用操作
压缩的会话	TLS/SSL 会话应用数据压缩方法。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
SSLv2 会话	此会话使用 SSL V2 加密。 请注意，如果 ClientHello 消息为 SSL 2.0，并且已传输流量的剩余部分为 SSL 3.0，则流量可解密。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
未知密码套件	系统无法识别该密码套件。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作

类型	说明	默认操作	可用操作
不支持的密码套件	系统不支持根据检测到的密码套件进行解密。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
会话无法缓存	TLS/SSL 会话已启用会话重复使用，客户端和服务器使用会话标识符重新建立了该会话，并且系统未缓存该会话标识符。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
握手错误	TLS/SSL 握手协商期间出错。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
解密错误	在流量解密时出错。	阻止	阻止 阻止并重置

首次创建 an SSL 策略时，默认情况下将禁用记录默认操作所处理的连接。由于默认操作的日志记录设置也适用于无法解密的流量处理，默认情况下也将禁用记录无法解密的流量操作所处理的连接。

请注意，如果浏览器使用证书锁定验证服务器证书，则无法通过对服务器证书重新签名来解密此流量。有关详细信息，请参阅TLS/SSL 规则 准则和限制，第 1731 页。

相关主题

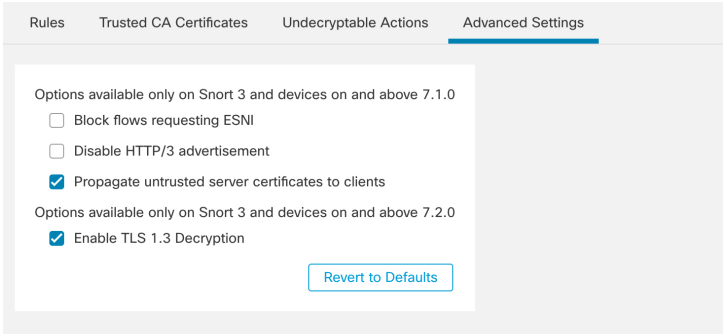
设置无法解密的流量的默认处理，第 1728 页

SSL 策略 高级选项

An SSL 策略 的 **高级设置** 选项卡页面具有适用于为应用策略的 Snort 3 配置的所有受管设备的全局设置。 在运行以下命令的任何受管设备上，这些设置都将被忽略：

- 早于 7.1 的版本
- Snort 2

以下为示例。



阻止请求 ESNI 的流

加密服务器名称指示（ESNI [建议草案的链接]）是客户端告知 TLS 1.3 服务器其请求内容的一种方式。由于 SNI 会被加密，因此您可以选择阻止这些连接，因为系统无法确定服务器是什么。

禁用 HTTP/3 通告

此选项会从 TCP 连接中的 ClientHello 删除 HTTP/3 (RFC 9114)，因为：

- 如 RFC 9114 中所述，HTTP/3 是 QUIC 传输协议的一部分，而不是 TCP 传输协议
- Firepower 系统尚不支持 QUIC
- 阻止这些客户端通告 HTTP/3 提供了对攻击和规避企图的保护。

将不受信任的服务器证书传播到客户端

这仅适用于匹配**解密 - 重新签名 (Decrypt - Resign)** 规则操作的流量。

启用此选项可在服务器证书不受信任的情况下，使用托管设备上的证书颁发机构 (CA) 来替换服务器证书。不受信任的服务器证书是指未在 Cisco Secure Firewall Management Center 中列为受信任 CA 的证书。（**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > **受信任 CA (Trusted CAs)**）。

启用 TLS 1.3 解密

（仅限 Snort 3。）移动滑块可让由 管理中心 管理的 威胁防御 设备能够解密 TLS 1.3 流量。

如果滑块移至禁用位置，则系统仅解密 TLS 1.2 流量。

相关信息

TLS/SSL 规则 最佳实践 ，第 1767 页

SSL 策略 的要求和必备条件

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

创建基本 SSL 策略

要配置 an SSL 策略，您必须为策略提供唯一的名称并指定默认操作。

过程

步骤 1 如果尚未登录，请登录管理中心。
步骤 2 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**。
步骤 3 点击**新建策略**。
步骤 4 在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。
步骤 5 指定**默认操作 (Default Action)**；请参阅SSL 策略 默认操作 ， 第 1724 页。
步骤 6 为默认操作配置日志记录选项，。
步骤 7 点击**保存 (Save)**。

后续操作

- 为无法解密的流量设置默认处理，请参阅设置无法解密的流量的默认处理 ， 第 1728 页。
- 为默认处理无法解密的流量配置日志记录选项。
- 设置高级策略属性：SSL 策略 高级选项 ， 第 1726 页。
- 将 SSL 策略 与访问控制策略相关联，如将其他策略与访问控制相关联 ， 第 1276 页中所述。
- 部署配置更改。

设置无法解密的流量的默认处理

您可以在 SSL 策略 级别设置无法解密的流量操作以处理系统无法解密或检查的某些类型的已加密流量。部署不包含任何 TLS/SSL 规则 的 an SSL 策略 时，无法解密的流量操作确定如何处理网络上的所有无法解密的已加密流量。

视乎无法解密的流量类型，您可以选择：

- 阻止连接。

- 阻止连接，然后重置连接。对于UDP等一直尝试连接直到连接被阻止的无连接协议，最好选择此选项。
- 使用访问控制检查已加密的流量。
- 继承 SSL 策略 的默认操作。

过程

步骤 1 如果尚未登录，请登录管理中心。

步骤 2 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 3 点击 SSL 策略名称旁边的 **编辑**（ ）。

步骤 4 在 SSL 策略 编辑器中，点击**无法解密的操作 (Undecryptable Actions)**。

步骤 5 对于每个字段，请选择要对无法解密的流量类型执行的SSL 策略 的默认操作或其他操作。有关详细信息，请参阅无法解密流量的默认处理选项，第 1725 页和SSL 策略 默认操作，第 1724 页。

步骤 6 点击**保存 (Save)** 保存策略。

下一步做什么

- 为无法解密的流量操作所处理的连接配置默认日志记录。
- 部署配置更改。

管理SSL 策略

在 SSL 策略 编辑器中，您可以：

- 添加、编辑、删除、启用、禁用和整理 TLS/SSL 规则。
- 添加受信任 CA 证书。
- 确定系统无法解密的已加密流量的处理。
- 记录由默认操作和无法解密的流量操作处理的流量。
- 设置高级选项。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

一个用户一次只能使用一个浏览器窗口编辑一个策略。如果多个用户保存同一个策略，系统会保留最后的更改。为方便起见，系统会显示有关当前正在编辑每条策略的人员（如有任何人）的信息。为保护会话隐私，当策略编辑器 30 分钟无任何活动后，系统将显示警告。60 分钟后，系统将放弃更改。

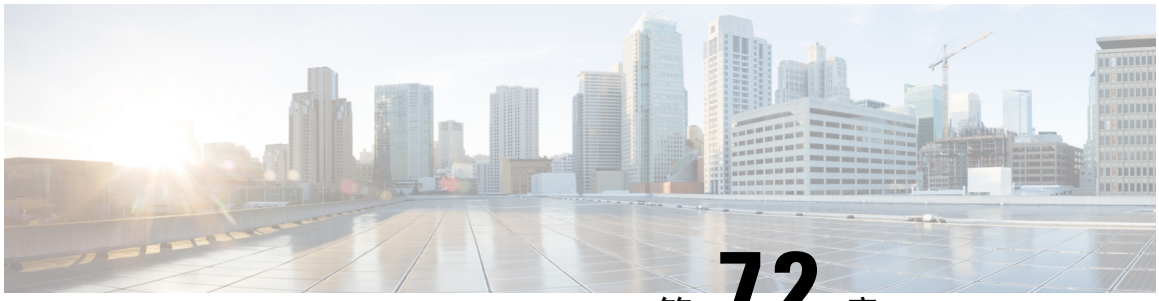
过程

步骤 1 如果尚未登录，请登录管理中心。

步骤 2 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 3 管理 SSL 策略：

- 比较 - 点击**比较策略 (Compare Policies)**；请参阅比较策略，第 148 页。
- 复制 - 点击 **复制**（）。
- 创建 - 点击**新建策略 (New Policy)**；请参阅创建基本 SSL 策略，第 1728 页。
- 删除 - 点击 **删除**（）。 如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
- 报告 - 点击**报告**（）；请参阅生成当前策略报告，第 149 页。
- 编辑 - 点击 **编辑**（）。 如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。
- 要将受信任 CA 证书添加到 SSL 策略，请参阅信任外部证书颁发机构，第 1754 页。
- 要配置您的 SSL 策略 如何处理无法解密的流量，请参阅设置无法解密的流量的默认处理，第 1728 页。
- SSL 策略 高级设置 - 请参阅SSL 策略 高级选项，第 1726 页。
- 导入/导出 - 请参阅Cisco Secure Firewall Management Center 和威胁防御管理网络管理中有关导入和导出配置的部分。
- 要为无法解密的流量处理以及不匹配 SSL 规则的流量记录连接，请参阅《Cisco Secure Firewall Management Center 管理指南》中的使用策略默认操作记录连接 。
- 部署 - 选择**部署** > **部署**；请参阅部署配置更改，第 136 页。



第 72 章

TLS/SSL 规则

以下主题概述了 TLS/SSL 规则 的创建、配置、管理和故障排除：

注释 由于 TLS 和 SSL 通常可以互换使用，因此我们使用 *TLS/SSL* 来指示所讨论的任一协议。IETF 已弃用 SSL 协议以支持更安全的 TLS 协议，因此您通常可将 *TLS/SSL* 解读为仅指代 TLS。

但 SSL 策略 是个例外。由于 管理中心 配置选项是 **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**，我们使用术语 *SSL* 策略 ，尽管这些策略是用于定义 TLS 和 SSL 流量的规则。

有关 SSL 和 TLS 协议的更多信息，请参阅 SSL 与 TLS - 差别何在？等资源。

TLS/SSL 规则概述

TLS/SSL 规则 提供一种精细的方法来跨多台受管设备处理加密流量：阻止流量而不进一步检查；不解密流量并通过访问控制对其进行检查；或者解密流量以进行访问控制分析。

TLS/SSL 规则 准则和限制

在设置 TLS/SSL 规则 时，请记住以下要点。正确配置 TLS/SSL 规则 是一项复杂的任务，但是对于构建用于处理加密流量的有效部署至关重要。许多因素会影响您配置规则的方式，包括您无法控制的特定应用行为。

此外，规则可以互相抢占，需要其他许可证或包含无效配置。周全配置的 SSL 规则还可以减少处理网络流量所需的资源。创建过度复杂的规则和以错误方式对规则进行排序可能会对性能产生不利影响。

有关详细信息，请参阅访问控制规则的最佳实践，第 1253 页。

有关 TLS 加密加速的具体准则，请参阅TLS 加密加速，第 1717 页。

相关主题

规则和其他策略警告
访问控制规则的最佳实践，第 1253 页
使用 TLS/SSL 解密的准则，第 1732 页
TLS/SSL 规则不支持的功能，第 1733 页
TLS/SSL 不解密准则，第 1733 页
TLS/SSL 解密 - 重新签名准则，第 1734 页
TLS/SSL 解密 - 已知密钥准则，第 1736 页
TLS/SSL 阻止准则，第 1737 页
TLS/SSL 证书固定准则，第 1737 页
TLS/SSL 心跳准则，第 1738 页
TLS/SSL 匿名密码套件限制，第 1738 页
TLS/SSL 标准化程序准则，第 1738 页
其他 TLS/SSL 规则 准则，第 1738 页
SSL 规则顺序

使用 TLS/SSL 解密的准则

一般准则

仅当托管设备处理加密流量时，才设置**解密 - 重新签名**或**解密 - 已知密钥**规则。TLS/SSL 规则 需要处理可能会影响性能的开销。

您无法在具有被动或内联分流模式接口的设备上解密流量。

无法解密的流量准则

我们可以确定某些流量不可解密，要么是因为网站本身不可解密，要么是因为该网站使用了 SSL 锁定，这有效地阻止了用户访问其浏览器中没有错误的已解密网站。

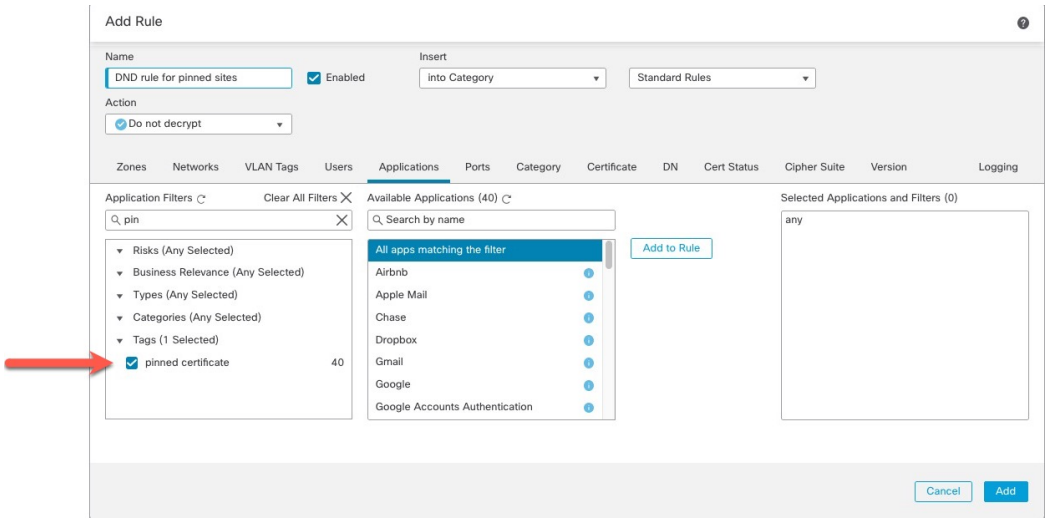
有关证书锁定的详细信息，请参阅关于 TLS/SSL 锁定。

我们维护的这些站点的列表如下：

- 名为 **Cisco-Undecryptable-Sites** 的可分辨名称 (DN) 组
- **已固定证书**应用过滤器

如果您正在解密流量，并且不希望用户在访问这些站点时在其浏览器中看到错误，我们建议您在 TLS/SSL 规则 底部设置**不解密规则**。

设置**已固定证书**应用过滤器的示例如下。



TLS/SSL 规则不支持的功能

不支持 RC4 密码套件

众所周知，Rivest Cipher 4（也称为 *RC4* 或 *ARC4*）密码套件存在漏洞，被认为是不安全的。SSL 策略 会将 RC4 密码套件识别为不受支持；应在策略的**无法解密的操作 (Undecryptable Actions)** 选项卡页面中配置**不支持的密码套件 (Unsupported Cipher Suite)** 操作，以满足您的组织的要求。有关详细信息，请参阅无法解密流量的默认处理选项，第 1725 页。

不支持被动、内联分流模式以及 SPAN 接口

无法在被动、内联分流模式或 SPAN 接口上解密 TLS/SSL 流量。

规则名称中的字符不受支持

请勿在 TLS/SSL 规则 规则名称中使用带重音的字符（例如 Comunicación）；这样做可防止将策略部署到受管设备。

TLS/SSL 不解密准则

如果是以下情况，则不应对流量进行解密：

- 法律所禁止；例如，某些司法管辖区禁止解密财务信息
- 公司政策所禁止；例如，您的公司可能会禁止解密特权通信
- 隐私法规所禁止
- 使用证书固定（也称为*TLS/SSL*固定）的流量必须保持加密，以防止断开连接

加密流量可以在任何 TLS/SSL 规则 条件下被允许或阻止，包括但不限于：

- 证书状态（例如，证书已过期或无效）

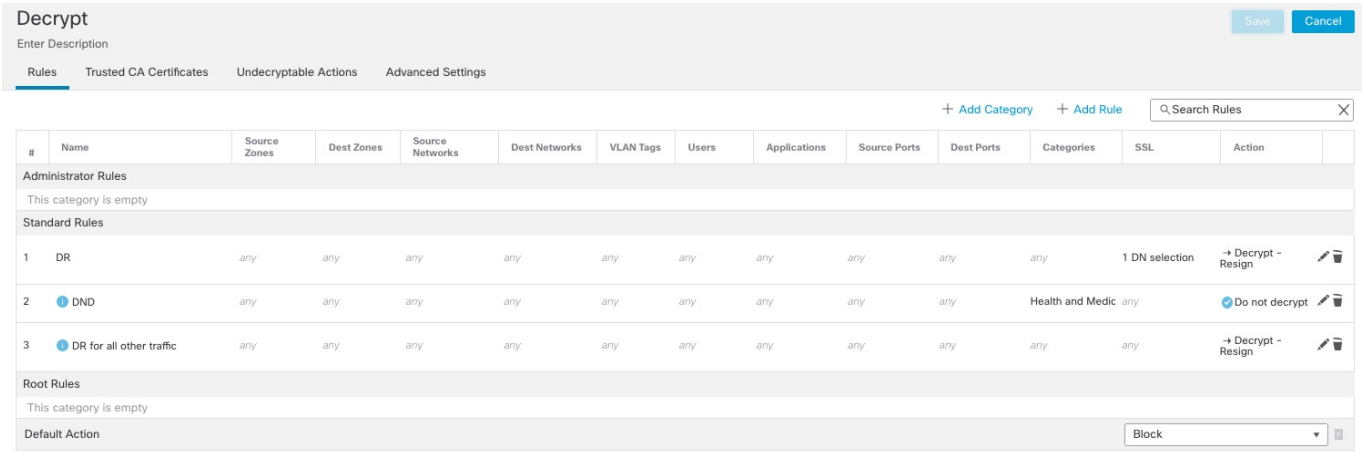
- 协议（例如，非安全 SSL 协议）
- 网络（安全区域、IP 地址、VLAN 标记等）
- 确切的 URL 或 URL 类别
- Port
- 用户组

“不解密”规则中的类别限制

您可以选择在 SSL 策略中包含类别。这些类别也称为 *URL* 过滤，由思科 Talos 智能组更新。更新基于机器学习和人工分析，这些内容可从网站目的地检索，有时也可从其托管和注册信息检索。分类不基于所声明的公司行业、意图或安全性。虽然我们努力不断更新和改进URL过滤类别，但这并不是一门精确的科学。有些网站根本没有分类，有些网站可能分类不当。

避免在不解密规则中过度使用类别，以避免无故解密流量；例如，“健康和医学”类别包括不会威胁到患者隐私的 WebMD 网站。

以下是一个解密策略示例，它可以阻止解密“健康”和“医学”类别的网站，但允许解密 WebMD 和其他所有内容。有关解密规则的一般信息，请参阅使用 TLS/SSL 解密的准则，第 1732 页。



注释 不要将 URL 过滤与应用检测混淆，后者依赖于从网站读取数据包来更具体地确定其内容（例如，Facebook Message 或 Salesforce）。有关详细信息，请参阅配置应用控制的最佳实践，第 1250 页。

TLS/SSL 解密 - 重新签名准则

您可以将一个内部证书颁发机构 (CA) 证书和私钥与**解密 - 重新签名 (Decrypt - Resign)** 操作相关联。如果流量与此规则相匹配，则系统会使用 CA 证书对服务器证书重新签名，然后充当中间人。它创建两个 TLS/SSL 会话，一个是客户端与受管设备之间的会话，一个是受管设备与服务器之间的会话。每个会话包含不同的加密会话详细信息，并且允许系统解密并重新加密流量。

最佳实践

我们的建议如下：

- 使用**解密 - 重新签名 (Decrypt - Resign)** 规则操作解密传出流量，而不是建议使用**解密 - 已知密钥 (Decrypt - Known Key)** 规则操作的传入流量。

  有关**解密 - 已知密钥**的详细信息，请参阅TLS/SSL 解密 - 已知密钥准则，第 1736 页。

- 在设置**机密 - 重新签名 (Decrypt - Resign)** 规则操作时始终选中**仅更换密钥 (Replace Key Only)** 复选框。

  当用户浏览到使用自签名证书的网站时，他们会在 Web 浏览器中看到安全警告，并会意识到自己正在与不安全的站点通信。

  当用户浏览到使用受信任证书的网站时，他们不会看到安全警告。

详情

如果配置具有**Decrypt - Resign**操作的规则，则除任何已配置的规则条件外，该规则会根据所引用的内部 CA 证书的签名算法类型来匹配流量。由于您将一个 CA 证书与 **Decrypt - Resign** 操作相关联，因此无法创建用来解密使用不同签名算法加密的多种类型的传出流量的 TLS/SSL 规则。此外，添加到规则中的任何外部证书对象和密码套件都必须与关联的 CA 证书加密算法类型相匹配。

例如，仅当操作引用基于椭圆曲线 (EC) 的 CA 证书时，使用 EC 算法加密的传出流量才会与**解密 - 重新签名**规则相匹配；必须将基于 EC 的外部证书和密码套件添加到此规则，以创建证书和密码套件规则条件。

同样，引用基于 RSA 的 CA 证书的 **Decrypt - Resign** 规则仅与使用 RSA 算法加密的传出流量相匹配；使用 EC 算法加密的传出流量与该规则不匹配，即使所有其他已配置的规则条件都匹配也如此。

准则和限制

另请注意以下提示：

不支持的匿名密码套件

本质上，匿名密码套件并不用于身份验证，也不使用密钥交换。匿名密码套件的用途有限；有关详细信息，请参阅 RFC 5246，附录 F.1.1.1。（TLS 1.3 已被替换为 RFC 8446 附录 C.5。）

无法在规则中使用**解密 - 重新签名 (Decrypt - Resign)** 或**解密 - 已知密钥 (Derypt - Known Key)** 操作，因为匿名密码套件不用于身份验证。

“解密 - 重新签名”规则操作和证书签名请求

要使用**解密 - 重新签名 (Decrypt - Resign)** 规则操作，应创建证书签名请求 (CSR) 并由受信任的证书颁发机构签名。（您可以使用 FMC 创建 CSR：**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > **内部 CA (Internal CAs)**。）

要在解密 - 重新签名规则中使用，您的证书颁发机构 (CA) 必须至少具有以下扩展名之一：

- **CA: TRUE**

  有关详细信息，请参阅 RFC3280 第 4.2.1.10 节中对基本限制的讨论。

- **KeyUsage=CertSign**

  有关详细信息，请参阅 RFC 5280 第 4.2.1.3 节。

要验证您的 CSR 或 CA 是否至少具有上述扩展名之一，您可以按照 openssl 文档等参考资料中的说明来使用 **openssl** 命令。

这是必要的，因为要使**解密 - 重新签名 (Decrypt - Resign)** 检查工作，SSL 策略 中使用的证书会即时生成证书并对其进行签名，以便充当中间人并代理所有 TLS/SSL 连接。

证书固定

如果客户的浏览器使用证书锁定来验证服务器证书，则无法通过对服务器证书重新签名来解密此流量。要允许此流量，请配置一个 TLS/SSL 规则，将**不解密**操作与服务器证书公用名或可分辨名称相匹配。

不匹配的密码套件

如果尝试使用与证书不匹配的密码套件保存 TLS/SSL 规则，则会显示以下错误。

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

不受信任的证书颁发机构

如果客户端不信任用于对服务器证书重新签名的证书颁发机构 (CA)，则会警告用户不应信任该证书。为了避免此情况，请将 CA 证书导入到客户端信任的 CA 库。或者，如果组织拥有专用 PKI，则可以颁发由根 CA（自动受组织中的所有客户端信任）签名的中级 CA 证书，然后将该 CA 证书上传到设备。

HTTP 代理限制

如果 HTTP 代理位于客户端和受管设备之间，并且客户端和服务器使用 CONNECT HTTP 方法建立隧道化 TLS/SSL 连接，则系统无法解密流量。**Handshake Errors** 无法解密操作将决定系统如何处理此流量。

上传签名的 CA

如果创建内部 CA 对象并选择生成证书签名请求 (CSR)，那么在将签名证书上传到对象之前，会无法对 **Decrypt - Resign** 操作使用此 CA。

不匹配的签名算法

如果配置具有 **Decrypt - Resign** 操作的规则，并且不匹配一个或多个外部证书对象或密码套件的签名算法类型，则策略编辑器在该规则旁边显示**信息**（  ）。如果所有外部证书对象或所有密码套件的签名算法类型不匹配，则策略在该规则旁边显示警告图标**警告**（  ），并且无法部署与 SSL 策略相关联的访问控制策略。

TLS/SSL 解密 - 已知密钥准则

当配置 **Decrypt - Known Key** 操作时，可以将一个或多个服务器证书和配对私钥与该操作相关联。如果流量与规则相匹配，并且用于加密流量的证书与操作的关联证书相匹配，则系统会使用相应的

私钥获取会话加密和解密密钥。由于您必须有权访问私钥，此操作最适合于解密传入到组织控制的服务器的流量。

另请注意以下提示：

不支持的匿名密码套件

本质上，匿名密码套件并不用于身份验证，也不使用密钥交换。匿名密码套件的用途有限；有关详细信息，请参阅 RFC 5246，附录 F.1.1.1。（TLS 1.3 已被替换为 RFC 8446 附录 C.5。）

无法在规则中使用**解密 - 重新签名 (Decrypt - Resign)** 或**解密 - 已知密钥 (Derypt - Known Key)** 操作，因为匿名密码套件不用于身份验证。

无法匹配可分辨名称或证书

创建具有**解密 - 已知密钥 (Decrypt - Known Key)** 操作的 TLS/SSL 规则 时，无法使用**可分辨名称 (Distinguished Name)** 或**证书 (Certificate)** 条件进行匹配。此限制基于这样一种假设：如果此规则与流量相匹配，则证书、使用者 DN 和颁发者 DN 已经与规则的关联证书相匹配。

椭圆曲线数字签名算法 (*ECDSA*) 证书会导致流量被阻止。

（仅启用 TLS 1.3 解密。）如果将 ECDSA 证书与**解密 - 已知密钥 (Decrypt - Known Key)** 规则操作配合使用，则会阻止匹配的流量。要避免这种情况，请将证书与其他类型的证书配合使用。

TLS/SSL 阻止准则

如果解密流量与具有**交互式阻止 (Interactive Block)** 或**交互式阻止并重置 (Interactive Block with reset)** 操作的访问控制规则相匹配，则系统会显示可自定义的响应页面。

如果您在规则中启用了日志记录，则会显示两个连接事件（在**分析 (Analysis)** > **事件 (Events)** > **连接 (Connections)**）：一个事件用于交互式阻止，而另一个事件用于指示用户是否选择继续访问站点。

相关主题

配置 HTTP 响应页面 ， 第 1350 页

TLS/SSL 证书固定准则

某些应用使用称为 *TLS/SSL* 锁定或证书锁定的技术，其在应用自身中嵌入原始服务器证书的指纹。因此，如果您配置具有**解密 - 重签**操作的 TLS/SSL 规则，则应用从受管设备收到重签的证书时，验证会失败且连接会中止。

由于 TLS/SSL 锁定用于避免中间人攻击，因此无法不能将其阻止或绕过。您有以下选择：

- 为排在**解密 - 重签**规则之前的应用创建**不解密**规则。
- 指示用户使用网络浏览器访问应用。

有关规则排序的详细信息，请参阅SSL 规则顺序。

要确定应用是否正在使用 TLS/SSL 锁定，请参阅对 TLS/SSL 锁定进行故障排除。

TLS/SSL 心跳准则

某些应用使用RFC6520定义的传输层安全(TLS)和数据报传输层安全(DTLS)协议的*TLS*心跳扩展。SSL 心跳可用于确认连接是否仍处于活动状态 - 客户端或服务器发送指定字节数的数据，并请求另一方回送响应。如果此过程成功，则发送加密的数据。

您可以在网络分析策略 (NAP) 中配置**最大心跳长度**，以便确定如何处理 TLS 心跳。有关详细信息，请参阅SSL 预处理器，第 2129 页。

有关详细信息，请参阅关于 TLS 心跳。

TLS/SSL 匿名密码套件限制

本质上，匿名密码套件并不用于身份验证，也不使用密钥交换。匿名密码套件的用途有限；有关详细信息，请参阅 RFC 5246，附录 F.1.1.1。（TLS 1.3 已被替换为 RFC 8446 附录 C.5。）

无法在规则中使用**解密 - 重新签名 (Decrypt - Resign)** 或**解密 - 已知密钥 (Derypt - Known Key)** 操作，因为匿名密码套件不用于身份验证。

您可以将匿名密码套件添加到 TLS/SSL 规则 的**密码套件**条件中，但系统会在 ClientHello 处理期间自动删除匿名密码套件。要让系统使用该规则，还必须配置 TLS/SSL 规则 的顺序以阻止 ClientHello 处理。有关详细信息，请参阅SSL 规则顺序。

TLS/SSL 标准化程序准则

如果启用内联规范化预处理器中的**规范化多余负载**选项，则预处理器在规范化解密流量时，可能会丢弃数据包并将其替换为修整过的数据包。这不会结束 TLS/SSL 会话。如果允许流量，则修整过的数据包会作为 TLS/SSL 会话的一部分加密。

其他 TLS/SSL 规则 准则

用户和组

如果向规则中添加用户或组，然后更改领域设置以排除该组或用户，规则将不会生效。（同样适用于禁用领域。）有关领域的更多信息，请参阅创建 Active Directory 领域和领域目录，第 1816 页。

TLS/SSL 规则 中的类别

如果您的 SSL 策略具有**解密 - 重新签名 (Decrypt - Resign)** 操作，但网站不会被解密，请检查与该策略相关的规则的**类别 (Category)** 页面。

在某些情况下，网站重定向到另一个站点进行身份验证或实现其他目的，而重定向的站点可能具有与您正在尝试解密的站点不同的 URL 分类。例如，`gmail.com`（**基于 Web 的电子邮件**类别）将重定向到 `accounts.gmail.com`（**互联网门户**类别）进行身份验证。请务必在 SSL 规则中包含所有相关类别。

注释 为了根据URL类别完全处理流量，您还必须配置URL过滤。请参阅URL 过滤，第 1335 页一章。

查询不在本地数据库中的 URL

如果您创建了一个**解密 - 重签**规则，并且用户浏览到其类别和信誉不在本地数据库中的网站，则数据可能不会被解密。某些网站未分类在本地数据库中，如果未分类，默认情况下不会解密来自这些网站的数据。

您可以通过**系统 (System) > 集成 (Integration) > 云服务** 设置来控制此行为，然后选中**向思科云查询未知 URL (Query Cisco cloud for unknown URLs)**。

有关此选项的详细信息，请参阅《Cisco Secure Firewall Management Center 管理指南》中的思科云。

TLS/SSL 规则 的要求和必备条件

支持的域

任意

用户角色

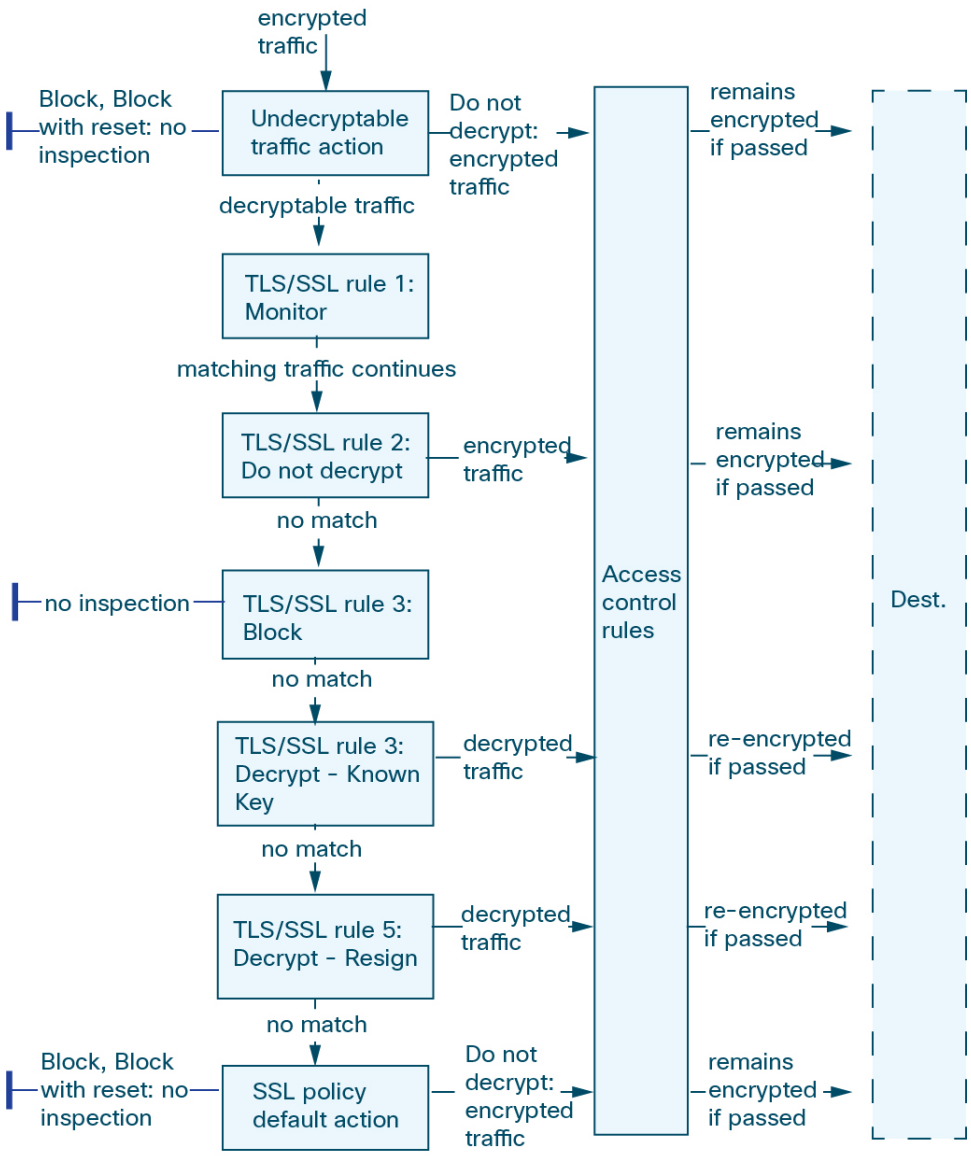
- 管理员
- 访问管理员
- 网络管理员

TLS/SSL 规则流量处理

系统会按照您所指定的顺序将流量与 TLS/SSL 规则规则相匹配。在大多数情况下，系统会根据第一个 TLS/SSL 规则（使用规则的所有条件来匹配流量）来处理加密流量。条件可以简单也可以复杂；可以按安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL、用户、证书、证书可分辨名称、证书状态、密码套件或加密协议版本来控制流量。

每个规则也具有操作，用于确定是使用访问控制监控、阻止还是检测匹配的已加密或已解密流量。请注意，系统不会进一步检查其阻止的加密流量，而是会通过访问控制来检查加密流量和无法解密的流量。但是，某些访问控制规则条件需要未加密流量，因此，已加密流量可能匹配的规则更少。此外，默认情况下，系统禁用已加密负载的入侵和文件检查。

下述场景概括说明了 TLS/SSL 规则在内联部署中处理流量的方式。



在这种情况中，流量评估如下：

- 首先，**Undecryptable Traffic Action** 评估加密流量。对于系统无法解密的流量，系统会将其阻止而不进一步检查，或者使其通过以进行访问控制检查。不匹配的加密流量继续根据下一规则进行评估。
- 其次，使用 **TLS/SSL 规则 1: Monitor** 评估加密流量。Monitor 规则跟踪和记录加密流量，但不对流量做出任何影响。系统继续根据其他规则匹配流量，以确定允许其通过，还是拒绝。
- 第三，使用 **TLS/SSL 规则 2: Do Not Decrypt** 评估加密流量。匹配流量未解密；系统通过访问控制检查此流量，但不执行文件或入侵检测。不匹配的流量继续根据下一规则进行评估。
- 第四，使用 **TLS/SSL 规则 3: Block** 评估加密流量。匹配的流量被阻止，无需进一步检测。不匹配的流量继续根据下一规则进行评估。

- 第五，使用 **TLS/SSL 规则 4: Decrypt - Known Key** 评估加密流量。系统使用您上传的私钥对传入网络的匹配流量进行解密。然后，根据访问控制规则评估解密流量。访问控制规则以相同方式处理已解密和未加密的流量。作为此额外检查的结果，系统可以阻止流量。所有剩余流量将被重新加密，才会被传输到目标。与 TLS/SSL 规则 不匹配的流量会继续根据下一规则进行评估。
- **TLS/SSL 规则 5: Decrypt - Resign** 是最终规则。如果流量与此规则相匹配，则系统使用已上传的 CA 证书对服务器证书重新签名，然后充当中间人解密流量。然后，根据访问控制规则评估解密流量。访问控制规则以相同方式处理已解密和未加密的流量。作为此额外检查的结果，系统可以阻止流量。所有剩余流量将被重新加密，才会被传输到目标。与 SSL 规则不匹配的流量继续根据下一规则进行评估。
- **SSL 策略 Default Action** 会处理与任何 TLS/SSL 规则 不匹配的所有流量。默认操作为以下两种方式之一：阻止加密流量，且不进一步检查；不解密流量而允许传输，以进行访问控制检查。

加密流量检查配置

您必须创建可重用公共密钥基础设施 (PKI) 对象才能基于加密会话特性控制加密流量并解密加密流量。可以在将受信任证书颁发机构 (CA) 证书上传到 an SSL 策略 并创建 TLS/SSL 规则，以及在此过程中创建关联对象时即时添加此信息。不过，提前配置这些对象可降低不正确创建对象的几率。

使用证书和配对密钥解密加密流量

如果通过上传用于会话加密的服务器证书和私钥来配置内部证书对象，则系统可以解密传入的加密流量。如果在包含**解密 - 已知密钥 (Decrypt - Known Key)** 操作的 an SSL 策略 规则中引用该对象并且流量与该规则相匹配，则系统会使用上传的私钥来解密会话。

如果通过上传 CA 证书和私钥来配置内部 CA 对象，则系统还可以解密传出流量。如果在包含**解密 - 重新签名 (Decrypt - Resign)** 操作的 TLS/SSL 规则 规则中引用该对象并且流量与该规则相匹配，则系统会对传递到客户端浏览器的服务器证书重新签名，然后充当中间人来解密会话。您可以选择只替换自签名证书密钥，而不是整个证书，在这种情况下，用户可在浏览器中看到自签名证书密钥通知。

根据加密会话特性控制流量

系统可以根据用于协商会话的密码套件或服务器证书来控制加密流量。您可以从多个不同的可重用对象中选择一个进行配置，并在TLS/SSL规则 条件中参照该对象来匹配流量。下表介绍可以配置的不同类型的可重用对象：

如果配置.....	可以根据是否存在以下内容控制加密流量.....
包含一个或多个密码套件的密码套件列表	用于协商加密会话的密码套件与密码套件列表中的密码套件相匹配
受信任 CA 对象（通过上传组织信任的 CA 证书）	受信任 CA 根据以下情况来确定是否信任用于加密会话的服务器证书： • CA 直接颁发证书 • CA 向颁发服务器证书的中间 CA 颁发证书

如果配置.....	可以根据是否存在以下内容控制加密流量.....
外部证书对象（通过上传服务器证书）	用于加密会话的服务器证书与上传的服务器证书相匹配
包含证书使用者或颁发者可分辨名称的可分辨名称对象	用于加密会话的证书上的主题或颁发者通用名称、国家/地区、组织或组织单位与已配置的可分辨名称相匹配

相关主题

密码套件列表，第 979 页
可分辨名称，第 983 页
PKI，第 1000 页

TLS/SSL 规则 顺序评估

在 SSL 策略 中创建 TLS/SSL 规则 时，您可以使用规则编辑器中的**插入 (Insert)** 列表来指定其位置。SSL 策略 中的 TLS/SSL 规则 会从 1 开始编号。系统按升序规则编号以自上而下的顺序将流量与 TLS/SSL 规则 相匹配。

在大多数情况下，系统根据第一个 TLS/SSL 规则（其中所有规则的条件都与流量相匹配）处理网络流量。除了 Monitor 规则（记录流量，但不影响流量）之外，系统在流量匹配一个规则后，不再继续根据其他低优先级规则评估流量。条件可以简单也可以复杂；可以按安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL、用户、证书、证书可分辨名称、证书状态、密码套件或加密协议版本来控制流量。

每个规则也具有操作，用于确定是使用访问控制监控、阻止还是检测匹配的已加密或已解密流量。请注意，系统不会进一步检查其阻止的加密流量，它会通过访问控制来检查加密流量和无法解密的流量。但是，访问控制规则条件需要未加密流量，因此，已加密流量匹配的规则更少。

使用特定条件（例如网络和 IP 地址）的规则应在使用一般条件（例如应用）的规则之前排序。如果您熟悉开放系统互联（OSI）模型，请在概念上使用类似的编号。包含第 1 层、第 2 层和第 3 层（物理、数据链路和网络）条件的规则应首先在规则中排序。稍后应在规则中对第 5 层、第 6 层和第 7 层的条件（会话，表示和应用）进行排序。有关 OSI 模型的详细信息，请参阅此 维基百科文章。

提示 适当的 TLS/SSL 规则 顺序可减少处理网络流量所需的资源，并防止规则抢占。尽管您创建的规则对于每个组织和部署来说都是唯一的，但是排序规则时需要遵循几个基本原则，才可优化性能，同时满足您的需求。

除了按照编号排序规则之外，还可按类别对规则进行分组。默认情况下，系统提供三个类别：管理员、标准和根。您可以添加自定义类别，但是不能删除系统提供的类别或更改类别的顺序。

相关主题

访问控制规则的最佳实践，第 1253 页
无法解密流量的默认处理选项，第 1725 页
SSL 规则顺序

TLS/SSL 规则 条件

TLS/SSL 规则 的条件识别此规则处理的加密流量的类型。条件可以简单也可以复杂，并且可以指定每个规则有多个条件类型。仅当流量满足规则中的所有条件时，该规则才适用于此流量。

如果不为规则配置特定条件，系统将不基于此标准匹配流量。例如，无论会话 SSL 或 TLS 版本如何，具有证书条件但不具有版本条件的规则根据用于协商会话的服务器证书来评估流量。

每个 TLS/SSL 规则 都具有对匹配的加密流量确定以下处理的关联操作：

- 处理：最重要的是，规则操作管理系统是监控、信任、阻止还是解密与规则条件匹配的加密流量
- 日志记录：规则操作确定何时及如何记录有关匹配的加密流量的详细信息。

您的 TLS/SSL 检查配置会处理、检查并记录解密流量：

- SSL 策略 的无法解密的操作处理系统无法解密的流量。
- 策略的默认操作处理不满足任何非监控器 TLS/SSL 规则 的条件的流量。

当系统阻止或信任加密会话时，可以记录连接事件。无论系统稍后如何处理或检查流量，您都可以强制系统记录其解密的连接，以通过访问控制规则进一步检查。已加密会话的连接日志包含有关加密的详细信息，例如用于加密该会话的证书。您可以仅记录连接结束事件，但是：

- 对于受阻连接（“阻止”、“阻止并重置”），系统会立即结束会话并生成事件
- 对于“不解密”连接，系统在会话结束时生成事件

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

注意 在禁用了 TLS/SSL 解密（即，当访问控制策略不包括 an SSL 策略 时）时添加第一个主动身份验证规则或删除最后一个主动身份验证规则 在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。

请注意，主动身份验证规则具有 **主动身份验证** 规则操作或 **被动身份验证** 规则操作，并且 **如果无法建立被动或 VPN 识别，则使用主动身份验证** 已选中。

相关主题

安全区域规则条件，第 1380 页
网络规则条件，第 607 页
VLAN 标记规则条件，第 1292 页
用户规则条件，第 607 页
应用规则条件，第 607 页
端口规则条件，第 609 页

类别规则条件，第 1747 页
基于服务器证书的 TLS/SSL 规则条件，第 1747 页

安全区域规则条件

安全区域可对网络进行分段，以通过跨多个设备将接口分组来帮助管理和分类流量。

区域规则条件可根据其源和目标安全区域控制流量。如果将源区域和目标区域均添加到区域条件中，则匹配流量必须源自其中一个源区域的接口，并通过其中一个目标区域的接口流出。

正如区域中的所有接口都必须为同一类型（均为内联、被动、交换或路由），区域条件中使用的所有区域也必须为同一类型。由于被动部署的设备不会传输流量，因此不能使用具有被动接口的区域作为目标区域。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

提示 按区域限制规则是提高系统性能的一种最佳方式。如果规则不适用于通过设备任意接口的流量，则该规则不影响该设备的性能。

安全区域条件和多租户

在多域部署中，在祖先域中创建的区域可以包含位于不同域中的设备上的接口。在后代域中配置区域条件时，您的配置仅适用于可以看到的接口。

网络规则条件

网络规则条件使用内部报头按流量的源和目标 IP 地址来控制流量。使用外部报头的隧道规则具有隧道终端条件而不是网络条件。

您可以使用预定义对象构建网络条件，或手动指定单个 IP 地址或地址块。

注释 您 不能 在身份规则中使用 FDQN 网络对象。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

VLAN 标记规则条件

注释 访问规则中的 VLAN 标记仅适用于内联集。带 VLAN 标记的访问规则与防火墙接口上的流量不匹配。

VLAN 规则条件可控制 VLAN 标记的流量，包括 Q-in-Q（堆栈 VLAN）流量。系统使用最内层的 VLAN 标记过滤 VLAN 流量，但不包括预过滤器策略，因为它在其规则中使用最外层的 VLAN 标记。

请注意以下 Q-in-Q 支持：

- Firepower 4100/9300 上的威胁防御 -不支持 Q-in-Q （仅支持一个 VLAN 标记）。
- 所有其他型号上的威胁防御 ：
  - 内联集和被动接口-支持 Q-in-Q，最多2个 VLAN 标记。
  - 防火墙接口-不支持 Q-in-Q （仅支持一个 VLAN 标记）。

可以使用预定义对象构建 VLAN 条件，或手动输入从 1 到 4094 之间的任意 VLAN 标记。使用连字符可指定 VLAN 标记范围。

最多可以指定 50 个 VLAN 条件。

在集群中，如果遇到 VLAN 匹配问题，请编辑访问控制策略高级选项“传输/网络预处理器设置”(Transport/Network Preprocessor Settings)，然后选择**跟踪连接时忽略 VLAN 信头 (Ignore the VLAN header when tracking connections)** 选项。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 VLAN 标记限制此配置可产生意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

用户规则条件

用户规则条件会根据发起连接的用户或用户所属的组来匹配流量。例如，您可以配置阻止规则以禁止财务组中的任何人访问网络资源。

（仅适用于访问控制规则）您必须首先将身份策略与访问控制策略相关联，如将其他策略与访问控制相关联，第 1276 页中所述。

除了为已配置的领域配置用户和组之外，您还可以为以下特殊身份的用户设置策略：

- 身份验证失败：强制网络门户身份验证失败的用户。
- 访客：在强制网络门户中被配置为访客用户的用户。
- 无需身份验证：匹配**无需身份验证 (No Authentication Required)** 规则操作的用户。

- 未知：无法识别的用户；例如，配置的领域未下载的用户。

应用规则条件

系统分析 IP 流量时，可以识别网络上的常用应用并将其分类。这种基于发现的应用感知是应用控制的基础 - 能够控制应用流量。

借助系统提供的应用过滤器，您可以根据应用的基本特征（类型、风险、业务关联性、类别和标记）组织应用，从而执行应用控制。您可以系统提供的过滤器的组合或以应用的自定义组合为基础，创建可重复使用的用户定义过滤器。

对于策略中的每个应用程序规则条件，必须启用至少一个检测器。如果没有为应用启用检测器，则系统会为该应用自动启用所有系统提供的检测器；如果不存在检测器，则系统为该应用启用最新修改的用户定义的检测器。有关应用检测器的详细信息，请参阅应用检测器基础知识，第 1946 页。

您可以使用应用过滤器和单独指定的应用来确保完整覆盖。但是，在订购访问控制规则之前，请了解以下说明。

应用过滤器的优势

应用过滤器可帮助您快速配置应用控制。例如，您可以轻松地使用系统提供的过滤器创建一条访问控制规则，用于识别并阻止所有业务关联性较低的高风险应用。如果用户尝试使用其中一个应用，则系统会阻止会话。

使用应用过滤器可简化策略创建和管理。此方法可保证系统按预期控制应用流量。由于思科经常通过系统和漏洞数据库 (VDB) 更新和添加应用检测器，因此您可确保系统使用最新的检测器监控应用流量。您还可以创建自己的检测器并将特征分配给其检测到的应用，自动将应用添加到现有过滤器。

应用特征

系统使用下表中所述的条件来展示其检测到的每个应用的特征。这些特征用作应用过滤器。

表 *201:* 应用特征

特征	说明 (Description)	示例
类型	应用协议代表主机之间的通信。 客户端代表在主机上运行的软件。 Web 应用代表 HTTP 流量的内容或所请求的 URL。	HTTP 和 SSH 是应用协议。 网络浏览器和邮件客户端是客户端。 MPEG 视频和 Facebook 是网络应用。
风险	应用用于可能违反您的组织安全策略的用途的可能性。	点对点应用的风险通常很高。
业务相关性	应用用于您的组织的业务运营（相对于娱乐目的）的情景中的可能性。	游戏应用的业务相关性通常很低。
类别	说明应用的最基本功能的应用通用分类。每个应用至少属于一个类别。	Facebook 属于社交网络类别。

特征	说明 (Description)	示例
标签	有关应用的附加信息。应用可以包括任何数量的标记，也可以没有标记。	视频流网络应用通常标记为 `high bandwidth` 和 `displays ads`。

相关主题

配置应用控制的最佳实践，第 1250 页

端口规则条件

通过端口条件，您可以按流量的源端口和目标端口控制该流量。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

基于端口的规则的最佳实践

指定端口是目标应用的传统方式。但是，可以将应用配置为使用唯一端口绕过访问控制块。因此，尽可能使用应用过滤条件而不是端口条件来确定流量目标。

应用过滤也建议用于动态打开单独通道的应用（如 FTD），以实现控制和数据流。使用基于端口的访问控制规则可能会阻止此类应用正确执行，并可能导致阻止所需的连接。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为源端口条件。

类别规则条件

您可以选择在SSL 策略中包含类别。这些类别也称为 *URL* 过滤，由思科 Talos 智能组更新。更新基于机器学习和人工分析，这些内容可从网站目的地检索，有时也可从其托管和注册信息检索。分类不基于所声明的公司行业、意图或安全性。

有关详细信息，请参阅URL 过滤概述，第 1335 页。

如果在具有**不解密 (Do Not Decrypt)** 规则操作的规则的 SSL 策略 中使用类别规则条件，请参阅 TBD。

基于服务器证书的 TLS/SSL 规则条件

TLS/SSL 规则可以根据服务器证书特征来处理和解密已加密的流量。您可以根据以下服务器证书属性配置 TLS/SSL 规则：

- 通过可分辨名称，您可以根据颁发服务器证书的 CA 或证书使用者来处理和检查加密流量。根据颁发者可分辨名称，可以根据颁发站点服务器证书的 CA 处理流量。
- 通过 TLS/SSL 规则中的证书条件，可以根据用于对加密流量进行加密的服务器证书来处理和检查该流量。可以配置具有一个或多个证书的条件；如果证书与该条件的任何证书相匹配，则流量与规则相匹配。
- 通过 TLS/SSL 规则中的证书状态条件，可以根据用于对流量加密的服务器证书的状态（包括证书是否有效、已被吊销、已过期、尚未生效、自签署、由可信 CA 签署、证书吊销列表 (CRL) 是否有效；证书中的服务器名称指示 (SNI) 是否与请求中的服务器相匹配）处理和检查加密流量。
- 通过 TLS/SSL 规则中的密码套件条件，可以根据用于协商加密会话的密码套件来处理和检查加密流量。
- 通过 TLS/SSL 规则中的会话条件，可以根据用于加密流量的 SSL 或 TLS 版本来检查加密流量。

要检测规则、证书颁发者或证书持有者中的多个密码套件，可以创建可重用密码套件列表和可分辨名称对象并将其添加到规则中。要检测服务器证书和某些证书状态，必须为规则创建外部证书和外部 CA 对象。

相关主题

证书 TLS/SSL 规则 条件，第 1748 页
证书状态 TLS/SSL 规则 条件，第 1755 页
信任外部证书颁发机构，第 1754 页
按证书状态匹配流量
密码套件 TLS/SSL 规则 条件，第 1757 页
加密协议版本 TLS/SSL 规则条件，第 1760 页

证书 TLS/SSL 规则 条件

构建基于证书的 TLS/SSL 规则条件时，可以上传服务器证书；将证书另存为外部证书对象，该对象可重用并会将名称与服务器证书相关联。或者，可以使用现有外部证书对象和对象组来配置证书条件。

可以根据以下证书可分辨名称特性在外部证书对象或对象组所基于的规则条件中搜索**可用证书 (Available Certificates)** 字段：

- 使用者或颁发者公用名 (CN)，或者 URL 包含在证书的使用者可选名称 (SAN) 中

  用户在浏览器中输入的 URL 与通用名称 (CN) 匹配
- 使用者或颁发者组织 (O)
- 使用者或颁发者组织单位 (OU)

您可以选择根据单个证书规则条件中的多个证书进行匹配；如果用于加密流量的证书与上传的任何证书相匹配，则加密流量与规则相匹配。

在单个证书条件中，可以向**所选证书 (Selected Certificates)** 添加最多 50 个外部证书对象和外部证书对象组。

请注意以下事项：

- 如果还选择**解密 - 已知密钥 (Decrypt - Known Key)** 操作，则无法配置证书条件。由于该操作要求选择服务器证书来解密流量，因此结果是证书已经与流量相匹配。
- 如果使用外部证书对象配置证书条件，则添加到密码套件条件中的任何密码套件或与 **Decrypt - Resign** 操作相关联的内部 CA 对象必须与外部证书的签名算法类型相匹配。例如，如果规则的证书条件引用基于 EC 的服务器证书，则添加的任何密码套件或与 **Decrypt - Resign** 操作相关联的 CA 证书也必须基于 EC。如果在此情况下签名算法类型不匹配，则策略编辑器会在规则旁边显示警告。
- 系统首次检测新服务器的加密会话时，证书数据不可用于 ClientHello 处理，因为这会导致首个会话不解密。在初始会话后，受管设备会缓存服务器证书消息中的数据。对于来自同一个客户端的后续连接，系统可将 ClientHello 消息与使用证书条件的规则进行决定性匹配，并处理消息以最大限度提高解密的可能性。

可分辨名称 (DN) 规则条件

本主题讨论如何在 TLS/SSL 规则 中使用可分辨名称条件。如果您不确定，可以使用 Web 浏览器查找证书的使用者可选名称 (SAN) 和公用名，然后可以将这些值作为可分辨名称条件添加到 TLS/SSL 规则。

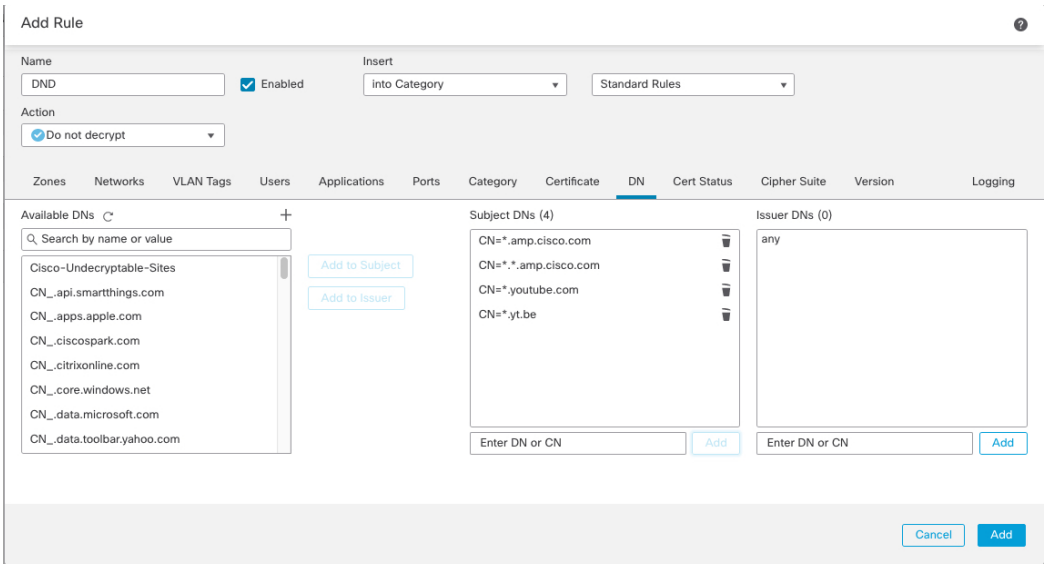
有关 SAN 的详细信息，请参阅 RFC 528 第 4.2.1.6 节。

以下各部分讨论：

- DN 规则匹配示例
- 系统如何使用 SNI 和 SAN
- 如何查找证书的通用名称和使用者可选名称
- 如何添加 DN 规则条件

DN 规则匹配示例

以下是不解密规则中 DN 规则条件的示例。假设您希望确保不解密流向 `amp.cisco.com` 或 YouTube 的流量。那么您可以按如下方式来设置 DN 条件：



前面的 DN 规则条件将与以下 URL 匹配，因此先前被规则阻止的流量会被解密：

- www.amp.cisco.com
- auth.amp.cisco.com
- auth.us.amp.cisco.com
- www.youtube.com
- kids.youtube.com
- www.yt.be

前面的 DN 规则条件与以下任何 URL 都不匹配，因此，流量将不匹配“不解密”(Do Not Decrypt) 规则，但可能匹配同一 SSL 策略 中的任何其他 TLS/SSL 规则。

- amp.cisco.com
- youtube.com
- yt.be

要匹配上述任何主机名，请向规则中添加更多 CN（例如，添加 `CN=yt.be` 就会匹配该 URL。）

系统如何使用 SNI 和 SAN

客户端请求中 URL 的主机名部分是服务器名称指示 (SNI)。客户端会使用 TLS 握手中的 SNI 扩展名来指定要连接的主机名（例如，`auth.amp.cisco.com`）。然后，服务器会选择在单个 IP 地址上托管所有证书时建立连接所需的相应私钥及证书链。

如果证书中的 SNI 与 CN 或 SAN 匹配，则我们会在与规则中列出的 DN 进行比较时使用 SNI。如果没有 SNI 或它与证书不匹配，则我们将在与规则中列出的 DN 进行比较时使用证书的 CN。

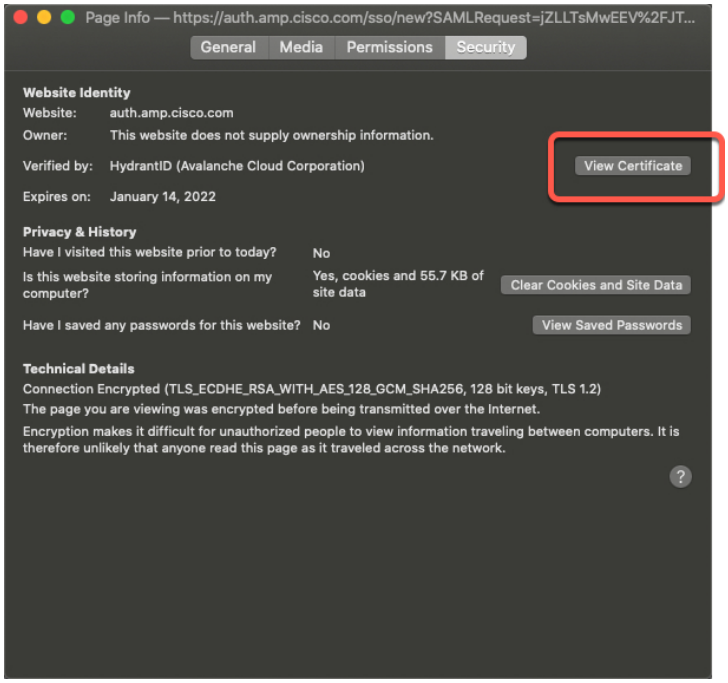
如何查找证书的通用名称和使用者可选名称

要查找任何证书的通用名称，请执行以下步骤。您甚至可以使用这些步骤来查找自签名证书的通用名称和 SAN。

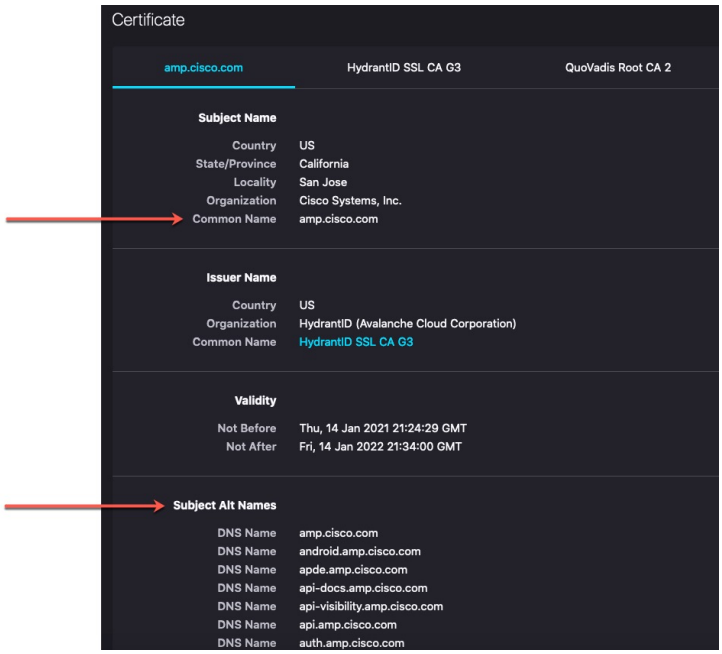
这些步骤适用于 Firefox，但其他浏览器也与之类似。以下程序以 `amp.cisco.com` 为例。

1. 在 Firefox 中浏览到 `amp.cisco.com`。
2. 在浏览器的地址栏中，点击 URL 左侧的 。
3. 点击**连接安全 (Connection secure)** > **更多信息 (More Information)**。

   （对于非安全或自签名证书，请点击**连接不安全 (Connection not secure)** > **详细信息 (More Information)**。）
4. 在页面信息对话框中，点击**查看证书 (View Certificate)**。



5. 下一页显示了证书详细信息。



请注意以下提示：

- `CN=auth.amp.cisco.com`，如果用作 DN 规则条件，则仅与该主机名（即 SNI）匹配。SNI `amp.cisco.com` 不匹配。
- 要匹配尽可能多的域名字段，请使用通配符。

  例如，要匹配 `auth.amp.cisco.com`，请使用 `CN=*.amp.cisco.com`。要匹配 `auth.us.amp.cisco.com`，请使用 `CN=*.*.amp.cisco.com`。

  像 `CN=*.example.com` 这样的 DN 与 `www.example.com` 匹配，但与 `example.com` 不匹配。要匹配两个 SNI，请在规则条件中使用两个 DN。

- 但不要过多使用通配符。例如，DN 对象（例如 `CN=*.google.com`）与大量的 SAN 匹配。使用 DN 对象（例如 `CN=*.youtube.com`）而不是 `CN=*.google.com`，使其与 `www.youtube.com` 等名称匹配。

  您还可以使用与 SAN 匹配的 SNI 变体，例如 `CN=*.youtube.com`、`CN=youtu.be`、`CN=*.yt.be` 等。

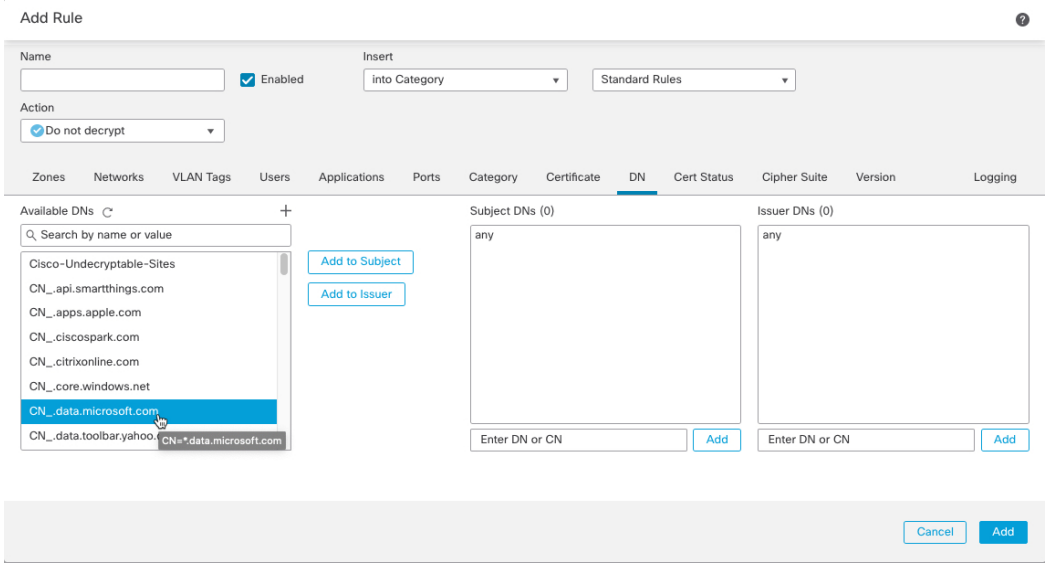
- 自签名证书应以相同的方式工作。您可以通过颁发者 DN 与使用者 DN 是否相同来确认它是否为自签名证书。

如何添加 DN 规则条件

在知道要匹配的 CN 后，请通过以下方式之一编辑 TLS/SSL 规则：

- 使用现有 DN。

  点击 DN 的名称，然后点击**添加到使用者 (Add to Subject)** 或**添加到颁发者 (Add to Issuer)**。（**添加到使用者 (Add to Subject)** 更为常用。）要查看 DN 对象的值，请将鼠标指针悬停在它上面。）

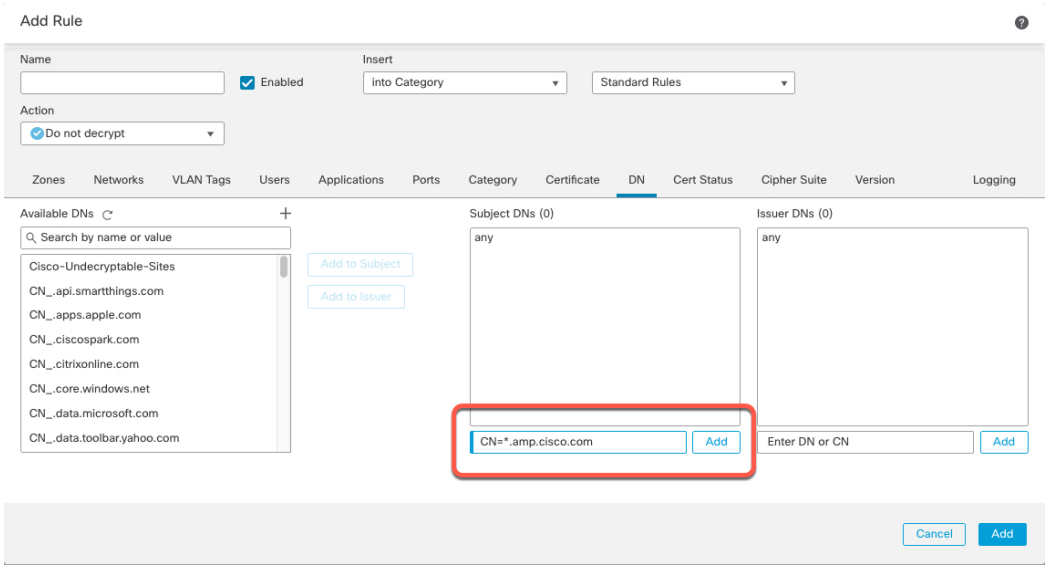


- 创建新的 DN 对象。

  点击可用 DN 右侧的 **添加**（+）。DN 对象必须包含名称和值。

- 直接添加 DN。

  在**使用者 DN (Subject DNs)** 字段或**颁发者 DN (Issuer DNs)** 字段底部的字段中输入 DN。（**使用者 DN (Subject DNs)** 更为常用。）输入 DN 后，点击**添加 (Add)**。



相关主题

可分辨名称，第 983 页

信任外部证书颁发机构

您可以通过向 SSL 策略中添加根 CA 证书和中间 CA 证书来信任 CA，然后使用这些受信任 CA 验证用于加密流量的服务器证书。

如果受信任 CA 证书包含上传的证书撤销列表 (CRL)，则还可以验证受信任 CA 是否已撤销加密证书。

提示 将根 CA 的信任链链中的所有证书都上传到受信任 CA 证书列表中，包括根 CA 证书和所有中间 CA 证书。否则，更难以检测由中间 CA 颁发的受信任证书。此外，如果将证书状态条件配置为根据根颁发者 CA 来信任流量，则可以允许而不解密受信任 CA 的信任链中的所有流量，而不是不必要地将其解密。

有关详细信息，请参阅受信任的 CA 对象，第 1006 页。

注释 创建 an SSL 策略时，策略的**受信任 CA 证书 (Trusted CA Certificate)** 选项卡页面将填充多个受信任 CA 证书，包括添加到 **选择受信任 CA (Select Trusted CAs)** 列表中的 **Cisco-Trusted-Authorities** 组。

过程

步骤 1 如果尚未登录，请登录管理中心。

步骤 2 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 3 点击 SSL 策略 旁边的 **编辑**（ ） 进行编辑。

步骤 4 点击**添加规则 (Add Rule)** 以添加新的 TLS/SSL 规则，或者点击 **编辑**（ ） 以编辑现有的规则。

步骤 5 点击**证书 (Certificates)** 选项卡。

步骤 6 从**可用证书 (Available Certificates)** 中查找要添加的受信任 CA，如下所示：

- 要即时添加可随后添加到条件中的受信任 CA 对象，请点击**可用证书 (Available Certificates)** 列表上方的 **添加**（ ）。
- 要搜索将添加的受信任 CA 对象和组，请点击**可用证书 (Available Certificates)** 列表上方的**按名称或值搜索 (Search by name or value)** 提示，然后键入对象的名称或对象中的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 7 要选择对象，请点击该对象。要选择所有对象，请点击右键，然后选择**全选 (Select All)**。

步骤 8 点击 **Add to Rule**（**添加至规则**）。

提示 您也可以拖放选定对象。

步骤 9 添加或继续编辑规则。

下一步做什么

- 将证书状态 TLS/SSL 规则条件添加到 SSL 规则。有关详细信息，请参阅按证书状态匹配流量。
- 部署配置更改。

证书状态 TLS/SSL 规则 条件

对于配置的每个证书状态 TLS/SSL 规则，您可以根据给定状态存在还是缺失来匹配流量。可以在一个规则条件中选择若干状态，如果证书与任何所选状态相匹配，则规则与流量相匹配。

可以选择根据单个证书状态规则条件中多个证书状态的存在或缺失进行匹配；证书只需匹配其中一个标准即可与规则相匹配。

设置此参数时，应考虑是配置解密规则还是阻止规则。通常情况下，应对阻止规则点击**是**，对解密规则点击**否**。示例：

- 如果要配置**解密 - 重新签名**规则，则默认行为是使用过期的证书解密流量。要更改此行为，请对**过期**点击**否**，以确保不会解密并重签具有过期证书的流量。
- 如果要配置**阻止**规则，则默认行为是允许具有过期证书的流量。要更改此行为，请对**过期**点击**是**，以阻止具有过期证书的流量。

下表介绍系统如何根据加密服务器证书的状态评估加密流量。

表 *202:* 证书状态规则条件标准

状态检查	状态设置为“是”(Yes)	状态设置为“否”(No)
已撤销	策略信任颁发服务器证书的 CA，并且上传到策略的 CA 证书包含用于撤销服务器证书的 CRL。	策略信任颁发服务器证书的 CA，并略的 CA 证书不包含用于撤销证书的
自签名	检测到的服务器证书包含相同的使用者和颁发者可分辨名称。	检测到的服务器证书包含不同的使用可分辨名称。
有效	以下所有情况都成立： • 策略信任颁发证书的 CA。 • 签名则是有效的。 • 颁发者有效。 • 策略的受信任 CA 未撤销证书 • 当前日期介于证书的有效期开始日期和有效期结束日期之间。	至少以下情况之一成立： • 策略不信任颁发证书的 CA。 • 签名无效。 • 颁发者无效。 • 策略中的受信任 CA 已撤销证书 • 当前日期在证书的有效期开始日 • 当前日期在证书的有效期结束日
签名无效	无法根据证书的内容正确验证证书的签名。	根据证书的内容正确验证证书的签名
颁发者无效	颁发者 CA 证书未存储在策略的受信任 CA 证书列表中。	颁发者 CA 证书存储在策略的受信任表中。

状态检查	状态设置为“是”(Yes)	状态设置为“否”(No)
到期	当前日期在证书的有效期结束日期之后。	当前日期在证书的有效期结束日期之前
尚未生效	当前日期在证书的有效期开始日期之前。	当前日期在证书的 Valid From 日期之后
无效的证书	证书无效。至少以下情况之一成立： • 证书扩展名无效或不一致；即，证书扩展名具有无效值（例如，编码不正确）或某些值与其他扩展名不一致。 • 证书无法用于指定用途。 • 已超出基本约束路径长度参数。 有关详细信息，请参阅 RFC 5280 第 4.2.1.9 节。 • 证书的“有效起始日期”或“有效终止日期”值无效。这些日期可以编码为 UTC 时间或通用时间 有关详细信息，请参阅 RFC 5280 第 4.1.2.5 节。 • 无法识别名称限制的格式；例如 RFC 5280 第 4.2.1.10 节中未提及表单的邮件地址格式。这可能是由于扩展名不正确或当前不支持的某些新功能导致的。 遇到了不受支持的名称限制类型。OpenSSL 目前仅支持目录名称、DNS 名称、邮件和 URI 类型。 • 根证书颁发机构不受信任，不可用于指定用途。 • 根证书颁发机构拒绝指定的用途。	证书有效。以下所有情况都成立： • 验证证书扩展名。 • 证书可用于指定用途。 • 基本约束路径长度有效。 • “有效起始日期”和“有效终止日有效。 • 名称限制有效。 • 根证书受信任，可用于指定用途。 • 根证书接受指定的用途。

状态检查	状态设置为“是”(Yes)	状态设置为“否”(No)
无效 CRL	证书撤销列表 (CRL) 的数字签名无效。至少以下情况之一成立： • CRL 的“下次更新”或“上次更新”字段的值无效。 • CRL 尚未生效。 • CRL 已过期。 • 尝试验证 CRL 路径时出错。仅在启用扩展 CRL 检查时才会发生此错误。 • 找不到 CRL。 • 唯一可以找到的CRL 与证书的范围不匹配。	CRL 有效。以下所有情况都成立： • “下次更新”和“上次更新”字 • CRL 日期有效。 • 路径有效。 • 已找到 CRL。 • CRL 与证书的范围相匹配。
服务器不匹配	服务器名称与服务器的服务器名称指示 (SNI) 名称不匹配，这可能表示尝试欺骗服务器名称。	服务器名称与客户端请求访问的服务称匹配。

请注意，即使证书可能匹配多个状态，但是该规则导致仅对流量执行一次操作。

检查颁发或撤销证书的 CA 是否要求将根 CA 证书和中间 CA 证书以及关联的 CRL 作为对象进行上传。然后，将这些受信任 CA 对象添加到 SSL 策略 的受信任 CA 证书列表。

密码套件 TLS/SSL 规则 条件

系统提供可向密码套件规则条件中添加的预定义密码套件。您还可以添加包含多个密码套件的密码套件列表对象。

注释 不能添加新的密码套件。不能修改和删除预定义密码套件。

在单个密码套件条件中，可以向**所选密码套件 (Selected Cipher Suites)** 添加最多 50 个密码套件和密码套件列表。系统支持向密码套件条件添加以下密码套件：

- SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_FIPS_WITH_DES_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DH_Anon_WITH_AES_128_GCM_SHA256
- TLS_DH_Anon_WITH_AES_256_GCM_SHA384
- TLS_DH_Anon_WITH_CAMELLIA_128_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DH_Anon_WITH_CAMELLIA_256_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_NULL_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

- TLS_ECDHE_RSA_WITH_NULL_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

请注意以下提示：

- 如果添加部署不支持的密码套件，则无法部署配置。例如，被动部署不支持使用任何短 Diffie-Hellman (DHE) 或短椭圆曲线 Diffie-Hellman (ECDHE) 密码套件来解密流量。使用这些密码套件创建规则将会阻止部署访问控制策略。
- 如果使用密码套件配置密码套件条件，则添加到证书条件中的任何外部证书对象或与 **Decrypt - Resign** 操作相关联的内部 CA 对象必须与密码套件的签名算法类型相匹配。例如，如果规则的密码套件条件引用基于 EC 的密码套件，则添加的任何服务器证书或与 **Decrypt - Resign** 操作相关联的 CA 证书也必须基于 EC。如果在此情况下签名算法类型不匹配，则策略编辑器会在规则旁边显示警告图标。
- 您可以在 SSL 规则中的**密码套件 (Cipher Suite)** 条件中添加一个匿名密码套件，但请记住：
  - 系统会在 ClientHello 处理期间自动删除匿名密码套件。要让系统使用该规则，还必须配置顺序以阻止 ClientHello 处理。有关详细信息，请参阅SSL 规则顺序。
  - 在该规则中无法使用**解密 - 重新签名 (Decrypt - Resign)** 或**解密 - 已知密钥 (Derypt - Known Key)** 操作，因为系统无法解密使用匿名密码套件加密的流量。

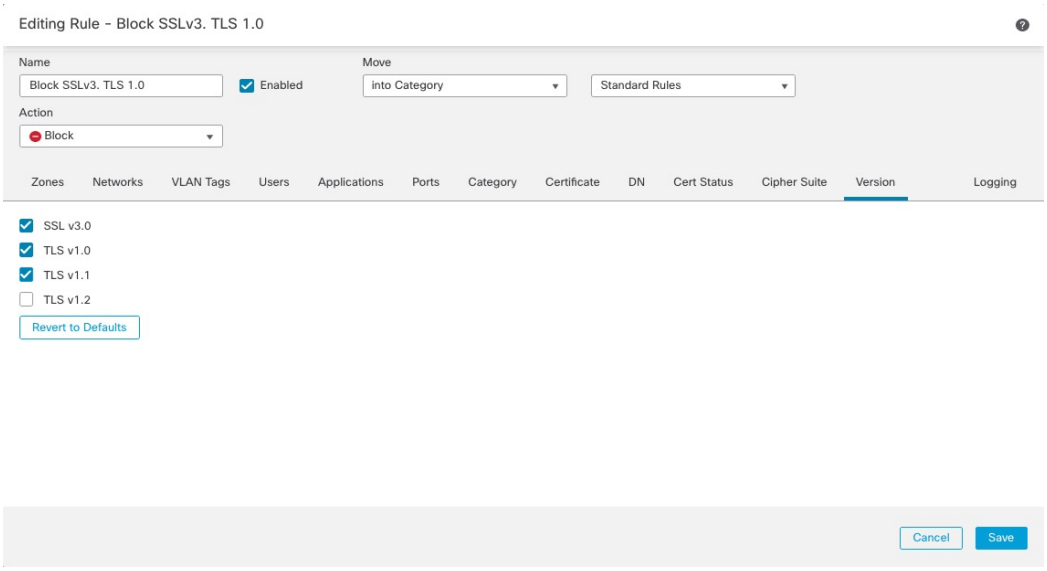
- 指定密码套件作为规则条件时，应该考虑使用 ServerHello 消息中协商的密码套件进行匹配的规则，而不是使用 ClientHello 消息中指定的整个密码套件列表进行匹配的规则。在 ClientHello 处理期间，受管设备从 ClientHello 消息中删除不受支持的密码套件。但如果这会导致所有指定的密码套件被删除，系统会保留原始列表。如果系统保留不受支持的密码套件，后续评估会导致会话不解密。

加密协议版本 TLS/SSL 规则条件

可以选择根据使用 SSL V3.0 或 TLS V1.0、V1.1 或 V1.2 加密的流量进行匹配。默认情况下，在创建规则时会选择所有协议版本；如果选择多个版本，则与任何所选版本相匹配的加密流量都与该规则相匹配。保存规则条件时，必须至少选择一个协议版本。

您无法在版本规则条件中选择 SSL V2.0；系统不支持解密使用 SSL V2.0 加密的流量。可以配置无法解密的操作来允许或阻止此流量而不进一步检查。

例如，要阻止所有 SSL v1.0、TLS v1.0 和 TLS v1.1 流量，请按如下所示设置选项：



TLS/SSL 规则 操作

以下各部分讨论 TLS/SSL 规则 可用的操作。

TLS/SSL 规则 监控操作

监控 (Monitor) 操作不能允许或拒绝流量。相反，它的主要目的是强制连接日志记录，而不会考虑最终如何处理匹配的流量。如果流量与**监控**规则条件匹配，则不会修改 ClientHello 消息。

系统随后会根据其他规则（如果有）来匹配流量，以确定信任、阻止还是解密该流量。所匹配的第一个非“监控”(Monitor) 规则确定流量和任何进一步的检测。如果没有其他匹配的规则，系统使用默认操作。

由于“监控”规则的主要目的是跟踪网络流量，因此系统会自动将受监控流量的连接结束事件记录到 Cisco Secure Firewall Management Center数据库，而无论稍后处理该连接的规则或默认操作的日志记录配置如何。

TLS/SSL 规则 不解密操作

不解密操作会让加密流量通过，以通过访问控制策略的规则和默认操作进行评估。由于某些访问控制规则条件需要未加密的流量，因此该流量可能与较少的规则相匹配。系统无法对加密流量执行深入检查，例如入侵或文件检查。

不解密规则操作的常见原因包括：

- 法律禁止解密 TLS/SSL 流量。
- 确定可以信任的站点。
- 通过检查流量（如 Windows Update）可以中断的站点。
- 使用连接事件查看 TLS/SSL 字段的值。（您无需解密流量即可查看连接事件字段。）。

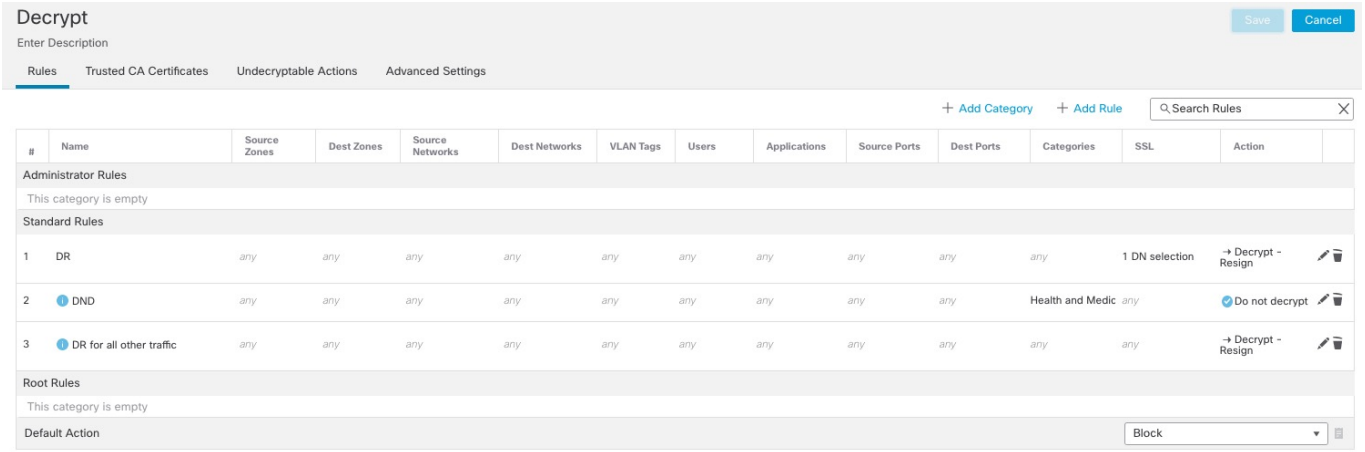
有关详细信息，请参阅无法解密流量的默认处理选项，第 1725 页

“不解密”规则中的类别限制

您可以选择在 SSL 策略中包含类别。这些类别也称为 *URL* 过滤，由思科 Talos 智能组更新。更新基于机器学习和人工分析，这些内容可从网站目的地检索，有时也可从其托管和注册信息检索。分类不基于所声明的公司行业、意图或安全性。虽然我们努力不断更新和改进URL过滤类别，但这并不是一门精确的科学。有些网站根本没有分类，有些网站可能分类不当。

避免在不解密规则中过度使用类别，以避免无故解密流量；例如，“健康和医学”类别包括不会威胁到患者隐私的 WebMD 网站。

以下是一个解密策略示例，它可以阻止解密“健康”和“医学”类别的网站，但允许解密 WebMD 和其他所有内容。有关解密规则的一般信息，请参阅使用 TLS/SSL 解密的准则，第 1732 页。



注释 不要将 URL 过滤与应用检测混淆，后者依赖于从网站读取数据包来更具体地确定其内容（例如，Facebook Message 或 Salesforce）。有关详细信息，请参阅配置应用控制的最佳实践，第 1250 页。

TLS/SSL 规则 阻止操作

系统为您不希望通过系统的流量提供以下 TLS/SSL 规则 操作：

- **阻止 (Block)**，此操作可终止连接，从而导致客户端浏览器出错。

  错误消息不会指明该站点由于策略而被阻止。相反，错误可能显示为没有通用的加密算法。据此消息，无法明确看出是您有意阻止了该连接。

- **阻止并重置 (Block with reset)**，此操作可终止并重置连接，从而导致客户端浏览器出错。

  该错误会指明连接已重置，但未指明具体原因。

提示 在被动或内联（触点模式）部署中不能使用 **阻止 (Block)** 或**阻止并重置 (Block with reset)** 操作，因为设备不会直接检查流量。如果创建具有**阻止 (Block)** 或**阻止并重置 (Block with reset)** 操作的规则，该规则在安全区域条件内包含被动或内联（触点模式）接口，则策略编辑器在该规则旁边显示警告 (⚠)。

TLS/SSL 规则 解密操作

Decrypt - Known Key 和 **Decrypt - Resign** 操作会对加密流量进行解密。系统通过访问控制来检查解密流量。访问控制规则以相同方式处理已解密和未加密的流量，您可以检查该流量来获得发现数据，并检测和阻止入侵、禁止的文件及恶意软件。系统在将允许的流量传递到其目标之前会将其重新加密。

建议使用来自受信任证书颁发机构 (CA) 的证书来解密流量。这可以防止**Invalid Issuer**显示在连接事件的“SSL 证书状态”列中。

有关添加受信任对象的详细信息，请参阅受信任证书颁发机构对象，第 1005 页。

相关主题：TLS 1.3 解密最佳实践。

相关主题

TLS 1.3 解密最佳实践

监控 TLS/SSL 硬件加速

以下主题讨论如何监控 TLS/SSL 状态

信息计数器

如果负载的系统运行良好，您应会看到以下计数器的计数较大。由于跟踪器进程的每个连接有2端，所以您会看到每个连接的这些计数器呈 2 倍增长。PRIV_KEY_RECV 和 SECU_PARAM_RECV 计数器最为重要，并会突出显示。CONTEXT_CREATED 和 CONTEXT_DESTROYED 计数器与加密芯片内存的分配相关。

```
> show counters
Protocol      Counter                          Value   Context
SSLENC        CONTEXT_CREATED                 258225   Summary
SSLENC        CONTEXT_DESTROYED               258225   Summary
TLS_TRK       OPEN_SERVER_SESSION             258225   Summary
TLS_TRK       OPEN_CLIENT_SESSION             258225   Summary
TLS_TRK       UPSTREAM_CLOSE                  516450   Summary
TLS_TRK       DOWNSTREAM_CLOSE                516450   Summary
TLS_TRK       FREE_SESSION                    516450   Summary
TLS_TRK       CACHE_FREE                      516450   Summary
TLS_TRK       PRIV_KEY_RECV                   258225   Summary
TLS_TRK       NO_KEY_ENABLE                   258225   Summary
TLS_TRK       SECU_PARAM_RECV                 516446   Summary
TLS_TRK       DECRYPTED_ALERT                 258222   Summary
TLS_TRK       DECRYPTED_APPLICATION         33568976   Summary
TLS_TRK       ALERT_RX_CNT                    258222   Summary
TLS_TRK       ALERT_RX_WARNING_ALERT          258222   Summary
TLS_TRK       ALERT_RX_CLOSE_NOTIFY           258222   Summary
TCP_PRX       OPEN_SESSION                    516450   Summary
TCP_PRX       FREE_SESSION                    516450   Summary
TCP_PRX       UPSTREAM_CLOSE                  516450   Summary
TCP_PRX       DOWNSTREAM_CLOSE                516450   Summary
TCP_PRX       FREE_CONN                       258222   Summary
TCP_PRX       SERVER_CLEAN_UP                 258222   Summary
TCP_PRX       CLIENT_CLEAN_UP                 258222   Summary
```

警报计数器

我们按照 TLS 1.2 规范实施了以下计数器。FATAL 或 BAD 警报可能表明存在问题；但是，ALERT_RX_CLOSE_NOTIFY 表明正常。

有关详细信息，请参阅 RFC 5246 第 7.2 节。

```
TLS_TRK      ALERT_RX_CNT                              311   Summary
TLS_TRK      ALERT_TX_CNT                                2   Summary
TLS_TRK      ALERT_TX_IN_HANDSHAKE_CNT                   2   Summary
TLS_TRK      ALERT_RX_IN_HANDSHAKE_CNT                   2   Summary
TLS_TRK      ALERT_RX_WARNING_ALERT                    308   Summary
TLS_TRK      ALERT_RX_FATAL_ALERT                        3   Summary
TLS_TRK      ALERT_TX_FATAL_ALERT                        2   Summary
TLS_TRK      ALERT_RX_CLOSE_NOTIFY                     308   Summary
TLS_TRK      ALERT_RX_BAD_RECORD_MAC                     2   Summary
TLS_TRK      ALERT_TX_BAD_RECORD_MAC                     2   Summary
TLS_TRK      ALERT_RX_BAD_CERTIFICATE                    1   Summary
```

错误计数器

这些计数器指示系统错误。这些计数在运行状况正常的系统上应较低。BY_PASS 计数器指示不经解密便直接传递到检测引擎 (Snort) 进程（在软件中运行）或从其传递的数据包。以下示例中列出了一些错误计数器。

值为 0 的计数器不会显示。要查看计数器的完整列表，请使用命令 **show counters description | include TLS_TRK**

```
> show counters
Protocol     Counter                           Value   Context
TCP_PRX      BYPASS_NOT_ENOUGH_MEM              2134   Summary
TLS_TRK      CLOSED_WITH_INBOUND_PACKET            2   Summary
TLS_TRK      ENC_FAIL                             82   Summary
TLS_TRK      DEC_FAIL                            211   Summary
TLS_TRK      DEC_CKE_FAIL                      43194   Summary
TLS_TRK      ENC_CB_FAIL                        4335   Summary
TLS_TRK      DEC_CB_FAIL                         909   Summary
TLS_TRK      DEC_CKE_CB_FAIL                     818   Summary
TLS_TRK      RECORD_PARSE_ERR                    123   Summary
TLS_TRK      IN_ERROR                          44948   Summary
TLS_TRK      ERROR_UPSTREAM_RECORD             43194   Summary
TLS_TRK      INVALID_CONTENT_TYPE                123   Summary
TLS_TRK      DOWNSTREAM_REC_CHK_ERROR            123   Summary
TLS_TRK      DECRYPT_FAIL                      43194   Summary
TLS_TRK      UPSTREAM_BY_PASS                    127   Summary
TLS_TRK      DOWNSTREAM_BY_PASS                  127   Summary
```

重大错误计数器

重大错误计数器表示严重的错误。这些计数器在正常运行的系统中应达到或接近于 0。以下示例列出了重大错误计数器。

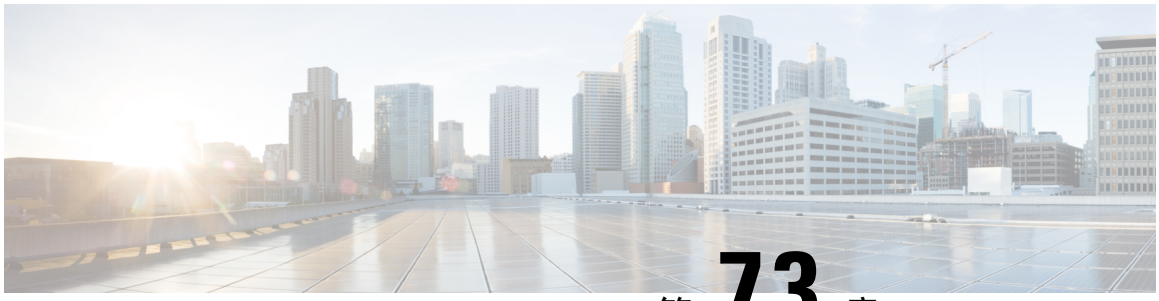
```
> show counters
Protocol     Counter                           Value   Context
CRYPTO       RING_FULL                             1   Summary
CRYPTO       ACCELERATOR_CORE_TIMEOUT              1   Summary
CRYPTO       ACCELERATOR_RESET                     1   Summary
CRYPTO       RSA_PRIVATE_DECRYPT_FAILED            1   Summary
```

RING_FULL 计数器不是重大错误计数器，但表明系统中加密芯片过载的频率。
ACCELERATOR_RESET 计数器指示 TLS 加密加速进程意外失败的次数，该进程意外失败也导致挂

起的操作失败，即您在 ACCELERATOR_CORE_TIMEOUT 和 RSA_PRIVATE_DECRYPT_FAILED 中看到的数字。

如果问题仍未解决，请禁用 TLS 加密加速（ 或 **config hwCrypto disable**）并配合思科 TAC 来解决问题。

注释 您可以使用 **show snort tls-offload** 和 **debug snort tls-offload** 命令进行其他的故障排除。使用 **clear snort tls-offload** 命令可将 **show snort tls-offload** 命令中显示的计数器重置为零。



第 73 章

TLS/SSL 规则 和策略示例

本章以本指南中讨论的概念为基础，提供包含遵循我们的最佳实践和建议的 TLS/SSL 规则 的 SSL 策略具体示例。您应该能够将此示例应用于自己的情况，使其适应您的组织的需求。

简而言之：

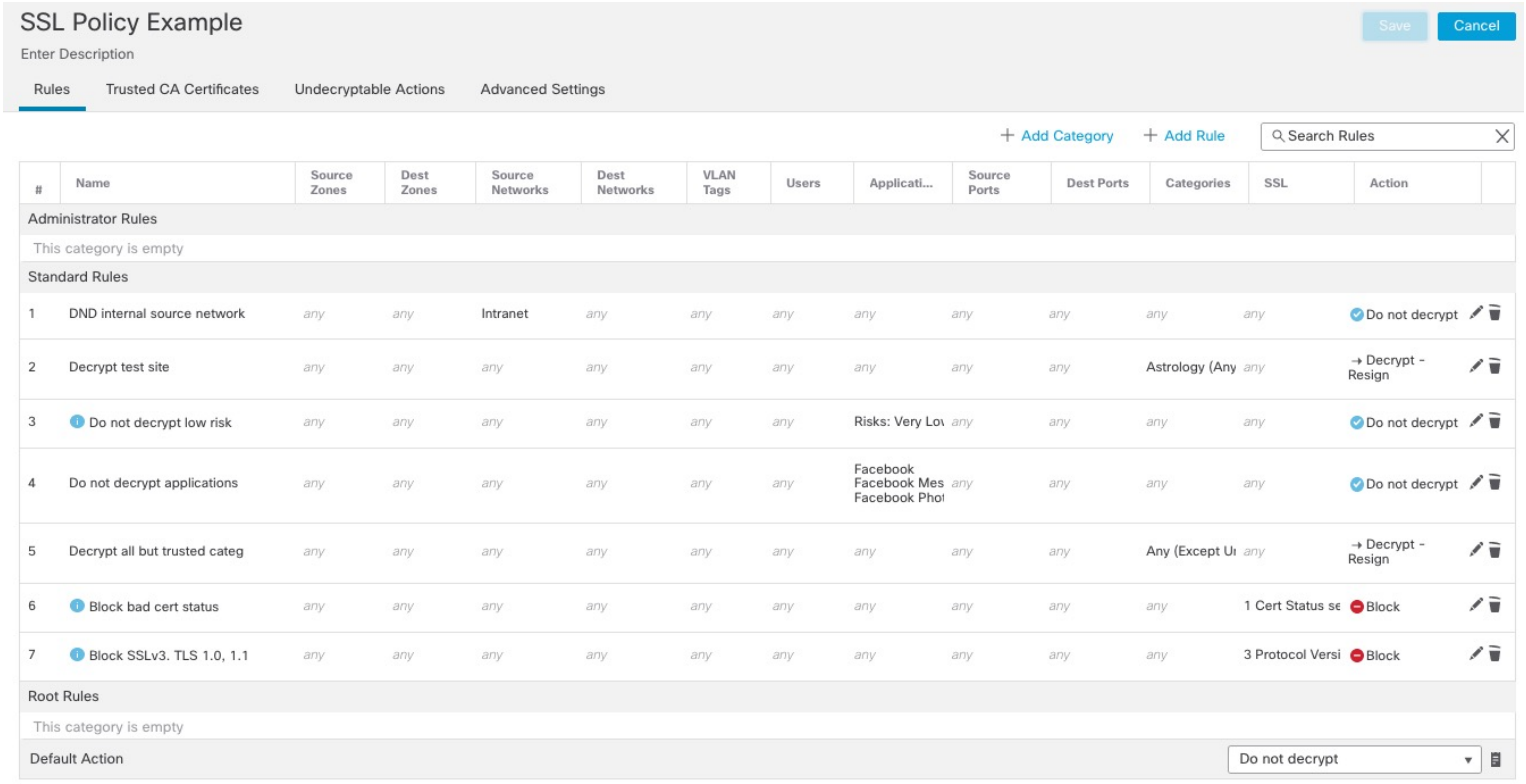
- 对于受信任的流量（例如传输大型压缩服务器备份），可使用预过滤和流量分流完全绕过检查。
- 将可以快速评估的任何 TLS/SSL 规则 规则放在 最前面 ， 例如适用于特定 IP 地址的规则。
- 将需要处理的任何规则、**解密 - 重新签署**规则以及阻止不安全协议版本和密码套件的 TLS/SSL 规则 规则放在 最后 。

- TLS/SSL 规则 最佳实践 ， 第 1767 页
- SSL 策略 逐步指导 ， 第 1770 页

TLS/SSL 规则 最佳实践

本章提供了 TLS/SSL 规则 的一个示例 SSL 策略，用于说明我们的最佳实践和建议。首先，我们将讨论 SSL 和访问控制策略的设置，然后再介绍所有规则以及我们建议以特定方式对其进行排序的原因。

以下是我们将在本章中讨论的 SSL 策略。



使用预过滤器和数据流分流绕过检测

在系统执行更多资源密集型评估之前，预过滤是访问控制的第一阶段。预过滤非常简单、快速并且可以及早执行。预过滤使用有限的外部报头条件来快速处理流量。将此过滤操作与后续评估进行比较，后续评估使用内部报头并具有更强大的检测功能。

配置预过滤：

- 提高性能 - 越早排除不需要检查的流量，越好。您可以基于隧道的外部封装报头传递隧道为某些类型的明文设置快速路径或加以阻止，而不检查其封装的连接。您还可以为从及早处理中受益的其他任何连接设置快速路径或加以阻止。
- 为封装流量定制深度检查 - 您可以对某些类型的隧道重新分区，以便以后可以使用相同的检查标准处理其封装的连接。重新分区是必要的，因为在预过滤后，访问控制使用内部报头。

如果有可用的 Firepower 4100/9300，则可以使用大型流量分流，这种技术可以让受信任的流量绕过检测引擎以获得更好的性能。例如，您可以在数据中心使用它来传输服务器备份。

相关主题

大型流量分流，第 1408 页
预过滤与访问控制，第 1393 页
快速路径预过滤的最佳实践，第 1395 页

不解密最佳实践

记录流量

我们建议不要创建未记录任何内容的**不解密**规则，因为这些规则在托管设备上仍需要处理时间。如果设置了任何类型的 TLS/SSL 规则，请启用日志记录，以便您可以查看匹配的流量。

无法解密的流量准则

我们可以确定某些流量不可解密，要么是因为网站本身不可解密，要么是因为该网站使用了 SSL 锁定，这有效地阻止了用户访问其浏览器中没有错误的已解密网站。

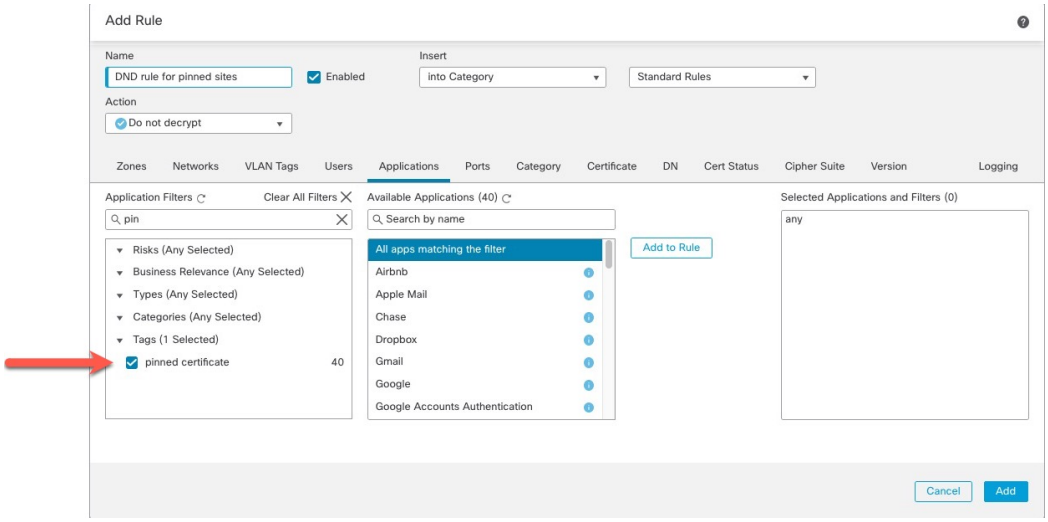
有关证书锁定的详细信息，请参阅关于 TLS/SSL 锁定。

我们维护的这些站点的列表如下：

- 名为 **Cisco-Undecryptable-Sites** 的可分辨名称 (DN) 组
- **已固定证书**应用过滤器

如果您正在解密流量，并且不希望用户在访问这些站点时在其浏览器中看到错误，我们建议您在 TLS/SSL 规则 底部设置**不解密规则**。

设置**已固定证书**应用过滤器的示例如下。



解密 - 重新签名和解密 - 已知密钥最佳实践

本主题讨论**解密 - 重新签名**和**解密 - 已知密钥** TLS/SSL 规则 的最佳实践。

解密 - 使用证书锁定的重新签名最佳实践

某些应用使用称为 *TLS/SSL* 锁定或证书锁定的技术，其在应用自身中嵌入原始服务器证书的指纹。因此，如果您配置具有**解密 - 重签**操作的 TLS/SSL 规则，则应用从受管设备收到重签的证书时，验证会失败且连接会中止。

由于 TLS/SSL 锁定用于避免中间人攻击，因此无法不能将其阻止或绕过。您有以下选择：

- 为排在**解密 - 重签**规则之前的应用创建**不解密**规则。
- 指示用户使用网络浏览器访问应用。

有关证书锁定的详细信息，请参阅关于 TLS/SSL 锁定。

解密 - 已知密钥最佳实践

由于**解密 - 已知密钥**规则操作用于流向内部服务器的流量，因此应始终将目标网络添加到这些规则（ **网络**规则条件）。这样，流量会直接进入服务器所在的网络，从而减少网络上的流量。

优先考虑 TLS/SSL 规则

将数据包的第一部分可以匹配的任何规则放在最前面；例如，引用IP地址的规则（**网络**规则条件）。

TLS/SSL 规则 放在最后

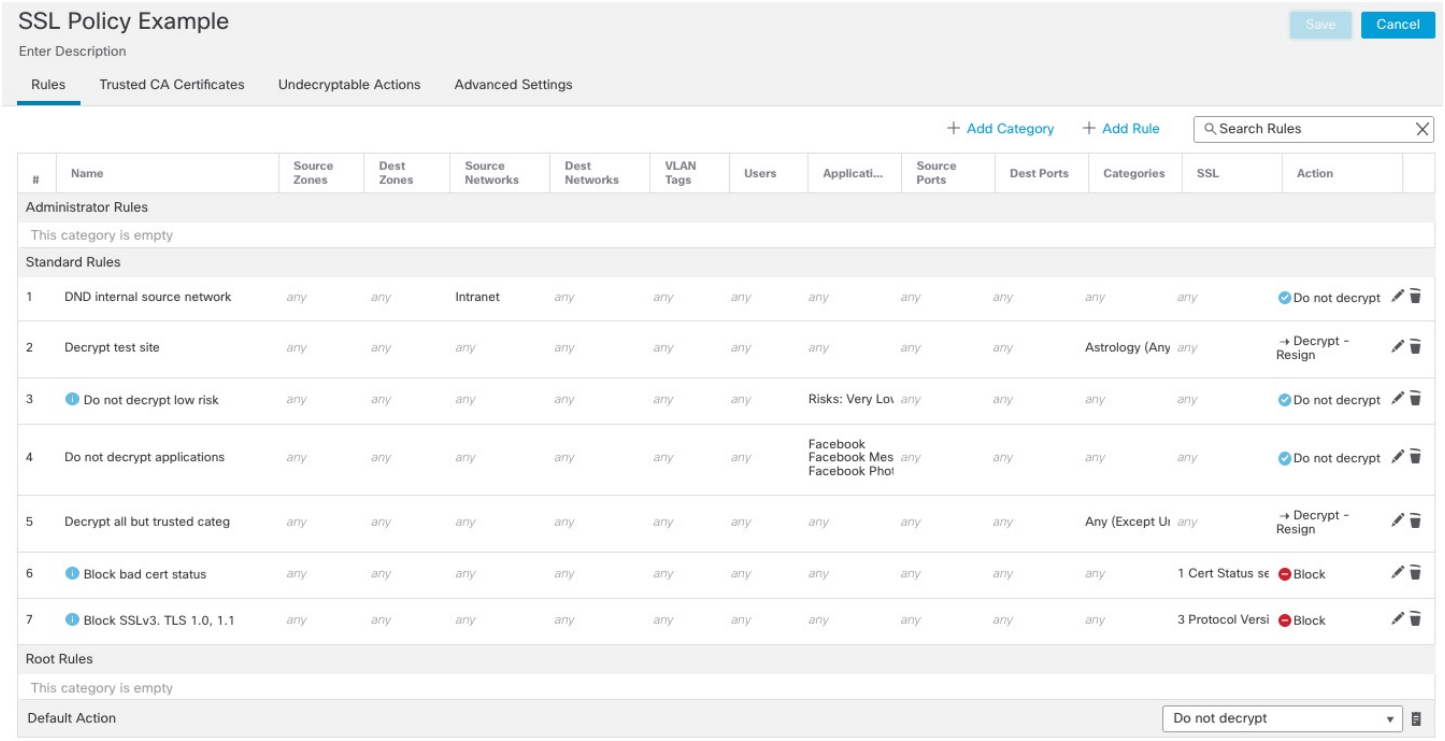
具有以下规则条件的规则应放在最后，因为这些规则要求系统在最长时间内检查流量：

- 应用
- 类别 (Category)
- 证书
- 可分辨名称 (DN)
- 证书状态
- 密码套件
- 版本

SSL 策略 逐步指导

本章提供有关如何使用我们的最佳实践规则来创建 SSL 策略的分步讨论和演练。您将看到 SSL 策略的预览，然后是最佳实践的概要，最后是对策略中规则进行的讨论。

以下是我们将在本章中讨论的 SSL 策略。



有关详细信息，请参阅以下各节之一：

相关主题

建议的策略和规则设置，第 1771 页
要预过滤的流量，第 1775 页
第一条 TLS/SSL 规则：不解密特定流量，第 1775 页
下一条 TLS/SSL 规则：解密特定测试流量，第 1776 页
创建解密 - 类别的重新签名规则，第 1779 页
不解密低风险类别、信誉或应用，第 1777 页
最后的 TLS/SSL 规则：阻止或监控证书和协议版本，第 1780 页

建议的策略和规则设置

我们建议使用以下策略设置：

- SSL 策略：
  - 默认操作：**不解密**。
  - 启用日志记录。
  - 将 **SSL v2 会话 (SSL v2 Session)** 和压缩会话 **(Compressed Session)** 的无法解密的操作 **(Undecryptable Actions)** 同时设置为**阻止 (Block)**。
  - 在策略的高级设置中启用 TLS 1.3 解密。

- TLS/SSL 规则：为每个规则启用日志记录，但具有 **不解密** 规则操作的规则除外。（这取决于您；如要查看有关未解密的流量的信息，请同时启用这些规则的日志记录。）
- 访问控制策略：
  - 将 SSL 策略 与访问控制策略关联。（如果不这样做， SSL 策略 和规则将不会起作用。）
  - 将默认策略操作设为**入侵防御：平衡安全性和连接 (Intrusion Prevention: Balanced Security and Connectivity)**。
  - 启用日志记录。

相关主题

SSL 策略 设置，第 1772 页
TLS/SSL 规则 设置，第 1787 页
访问控制策略设置，第 1773 页

SSL 策略 设置

如何为 SSL 策略配置以下建议的最佳实践设置：

- 默认操作：**不解密**。
- 启用日志记录。
- 将 **SSL v2 会话 (SSL v2 Session)** 和**压缩会话 (Compressed Session)** 的**无法解密的操作 (Undecryptable Actions)** 同时设置为**阻止 (Block)**。
- 在策略的高级设置中启用 TLS 1.3 解密。

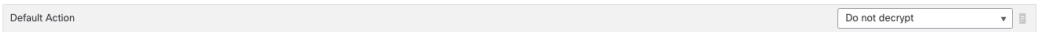
过程

步骤 1 如果尚未登录，请登录Cisco Secure Firewall Management Center。

步骤 2 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 3 点击 SSL 策略 旁边的 **编辑**（）。

步骤 4 从页面底部的**默认操作 (Default Action)** 列表中，点击**不解密 (Do Not Decrypt)**。
下图显示了一个示例。



步骤 5 在行的末尾位置，点击 **日志记录**（）。

步骤 6 选中**在连接结束时记录 (Log at End of Connection)** 复选框。

步骤 7 点击**确定 (OK)**。

步骤 8 点击**保存 (Save)**。

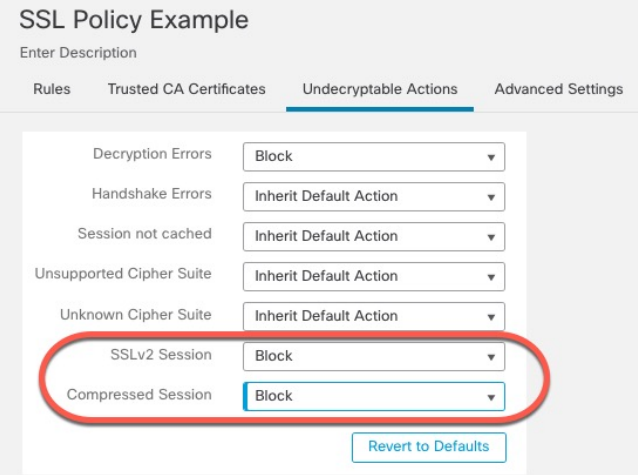
步骤 9 选择**无法解密的操作 (Undecryptable Actions)** 选项卡。

步骤 10 我们建议将 **SSLv2 会话 (SSLv2 Session)** 和**压缩的会话 (Compressed Session)** 的操作设置为**阻止 (Block)**。

您的网络上不应允许 SSL v2，并且不支持压缩的 TLS/SSL 流量，因此您也应阻止该流量。

有关设置每个选项的详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》的部分。

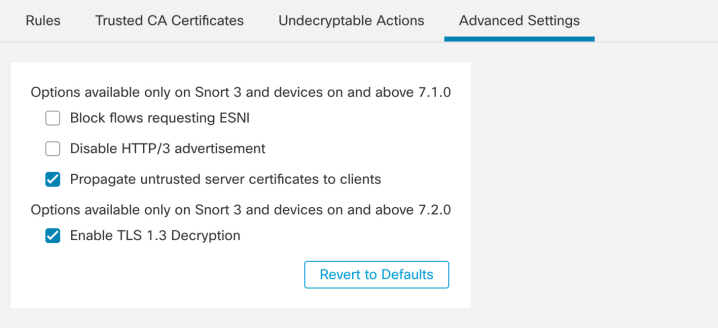
下图显示了一个示例。



步骤 11 点击**高级设置 (Advanced Settings)** 选项卡页面。

步骤 12 选中**启用 TLS 1.3 解密 (Enable TLS 1.3 Decryption)** 复选框。

以下为示例。



步骤 13 在该页面顶部，点击**保存**。

下一步做什么

配置 TLS/SSL 规则 规则并设置每个规则，如TLS/SSL 规则 设置，第 1787 页中所述。

访问控制策略设置

如何为访问控制策略配置以下建议的最佳实践设置：

- 将 SSL 策略 与访问控制策略关联。（如果不这样做， SSL 策略 和规则将不会起作用。）
- 将默认策略操作设为**入侵防御：平衡安全性和连接 (Intrusion Prevention: Balanced Security and Connectivity)**。
- 启用日志记录。

过程

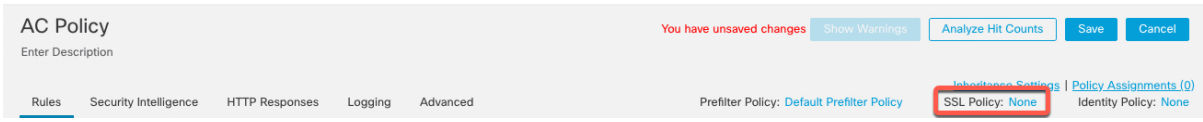
步骤 1 如果尚未登录，请登录Cisco Secure Firewall Management Center。

步骤 2 请点击 **策略** > **访问控制**。

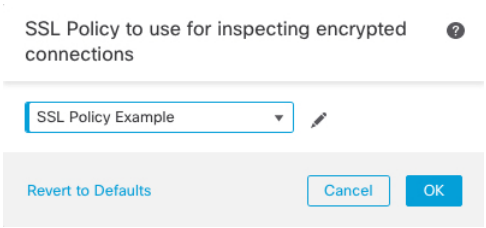
步骤 3 点击访问控制策略旁边的 **编辑**（）。

步骤 4 （如果尚未设置 SSL 策略，可以稍后再执行此操作。）

a) 点击页面顶部 **SSL 策略 (SSL Policy)** 旁边的**无 (None)**，如下图所示。



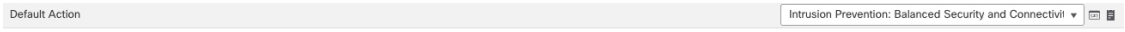
b) 从列表中，点击 SSL 策略的名称。下图显示了一个示例。



c) 点击**确定 (OK)**。

d) 在该页面顶部，点击**保存**。

步骤 5 从页面底部的**默认操作 (Default Action)** 列表中，点击**入侵防御：平衡安全性和连接 (Intrusion Prevention: Balanced Security and Connectivity)**。
下图显示了一个示例。



步骤 6 请点击 **日志记录**（）。

步骤 7 选中**在连接结束时记录 (Log at End of Connection)** 复选框并点击**确定 (OK)**。

步骤 8 点击**保存 (Save)**。

下一步做什么

请参阅TLS/SSL 规则 示例 ， 第 1775 页。

TLS/SSL 规则 示例

本部分提供阐述最佳实践的 TLS/SSL 规则 规则示例。

有关详细信息，请参阅以下各节之一：

相关主题

要预过滤的流量，第 1775 页
第一条 TLS/SSL 规则：不解密特定流量，第 1775 页
下一条 TLS/SSL 规则：解密特定测试流量，第 1776 页
不解密低风险类别、信誉或应用，第 1777 页
创建解密 - 类别的重新签名规则，第 1779 页
最后的 TLS/SSL 规则：阻止或监控证书和协议版本，第 1780 页

要预过滤的流量

在系统执行更多资源密集型评估之前，预过滤是访问控制的第一阶段。与后续评估相比，预过滤简单、快速、及时，它使用内部报头并具有更强大的检测功能。

根据您的安全需求和流量量变曲线，您应该考虑使用预过滤，以便从任何策略和检查中排除以下内容：

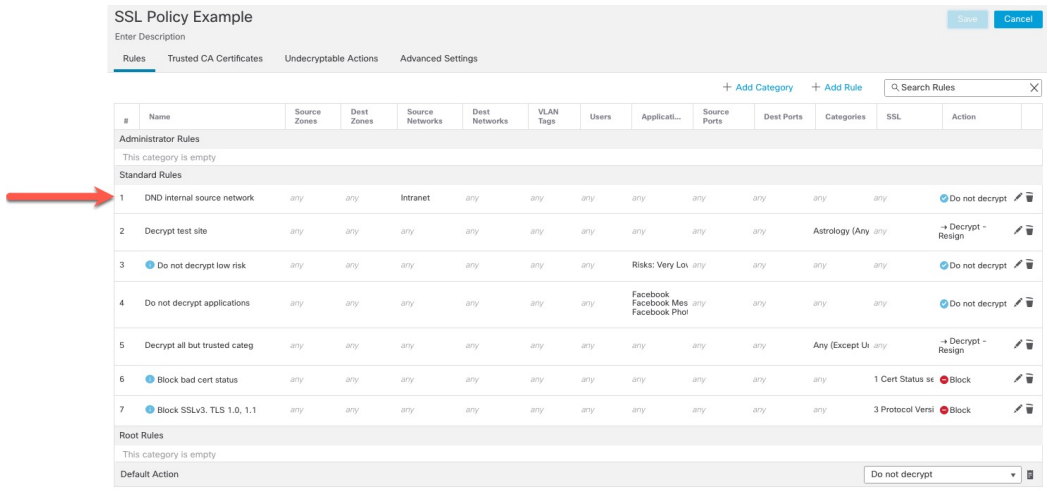
- 常见的办公室内应用，例如 Microsoft Outlook 365
- 大象流，例如服务器备份

相关主题

预过滤与访问控制，第 1393 页
快速路径预过滤的最佳实践，第 1395 页

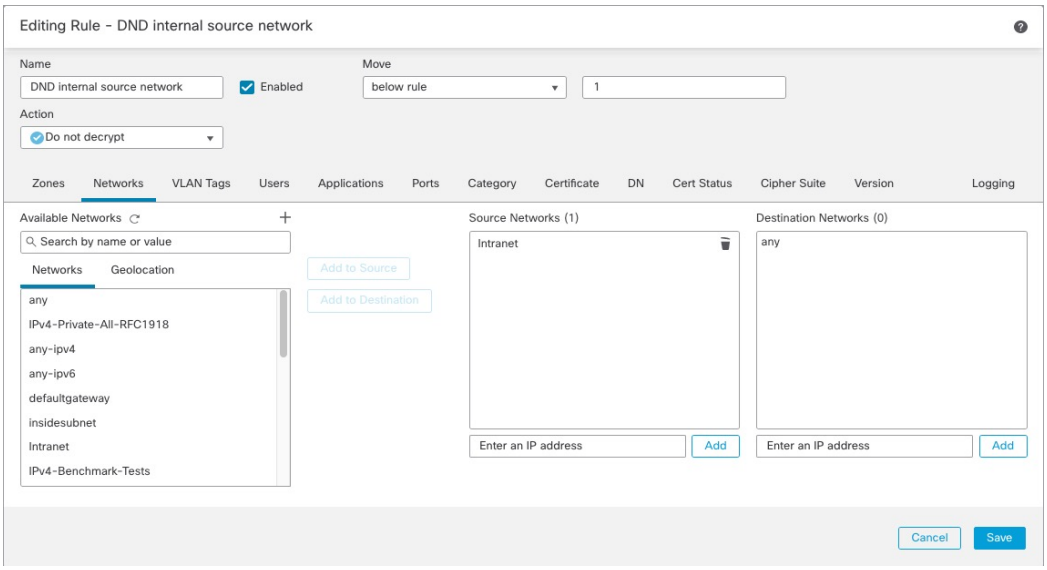
第一条 TLS/SSL 规则：不解密特定流量

示例中的第一条 TLS/SSL 规则 不会解密流向 内部网络（定义为 **intranet**）的流量。**不解密**规则操作会在 ClientHello 期间进行匹配，因此处理速度非常快。



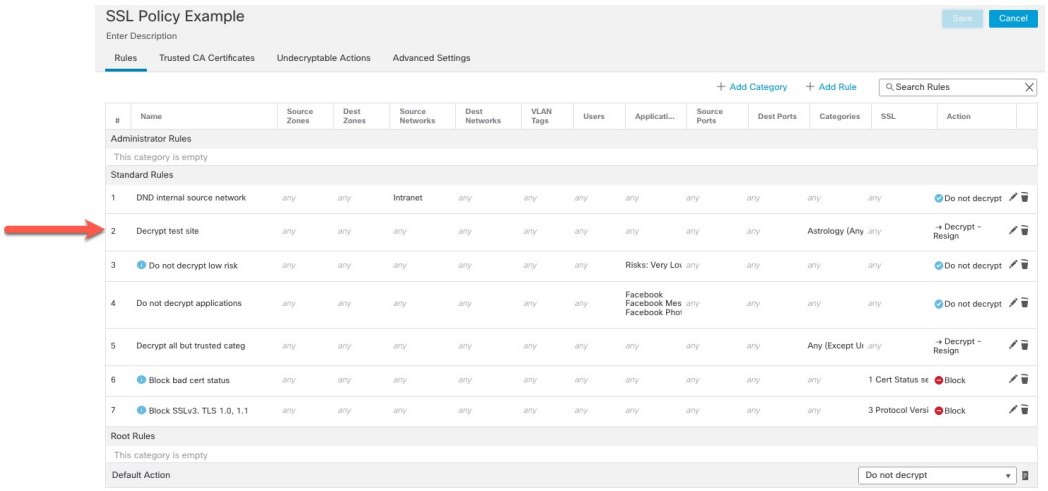
注释 如果您有从内部 DNS 服务器流向内部 DNS 解析器（例如思科 Umbrella 虚拟设备）的流量，则还可以为其添加**不解密规则**。如果内部DNS服务器会执行自己的日志记录，您甚至可以将这些添加到预过滤策略。

但是，我们强烈建议您不要对进入互联网的DNS流量使用**不解密**规则或预过滤，例如互联网根服务器（例如，Active Directory 中内置的 Microsoft 内部 DNS 解析器）。在这些情况下，您应该全面检查流量，甚至考虑阻止它。

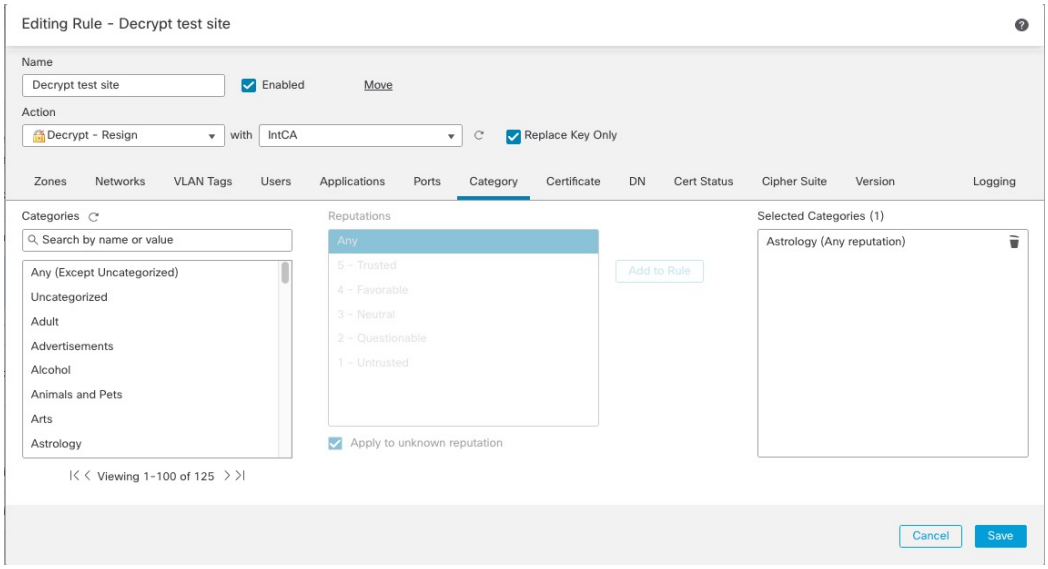


下一条 TLS/SSL 规则：解密特定测试流量

在本例中，下一条规则为可选；使用它来解密和监控有限类型的流量，然后再确定是否允许它在您的网络上使用。



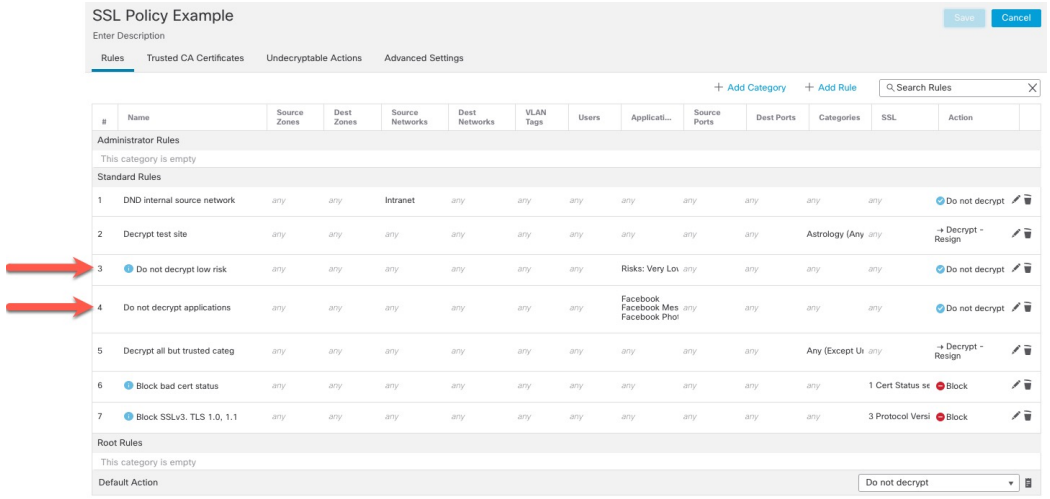
规则详细信息：



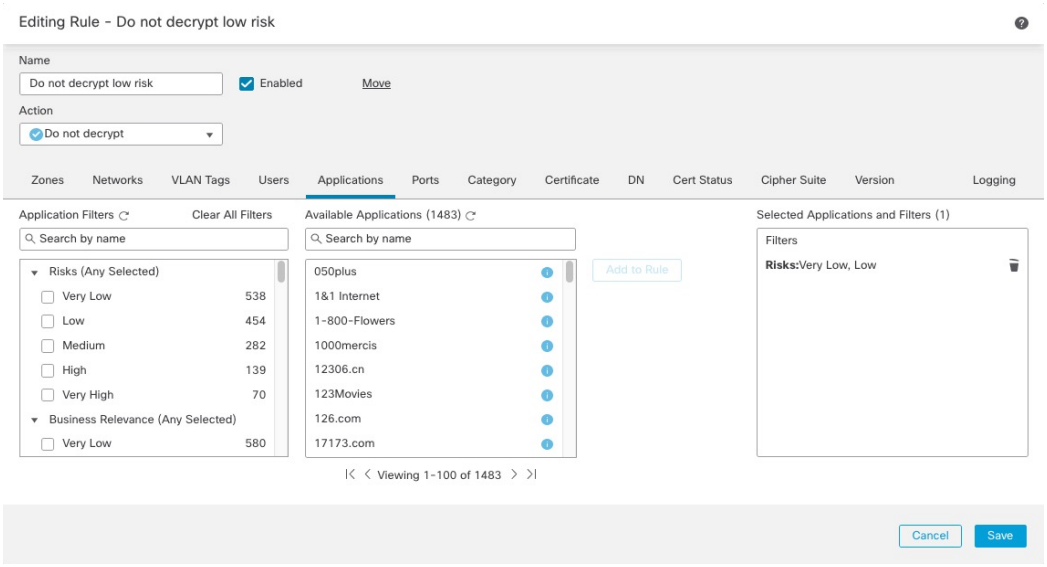
不解密低风险类别、信誉或应用

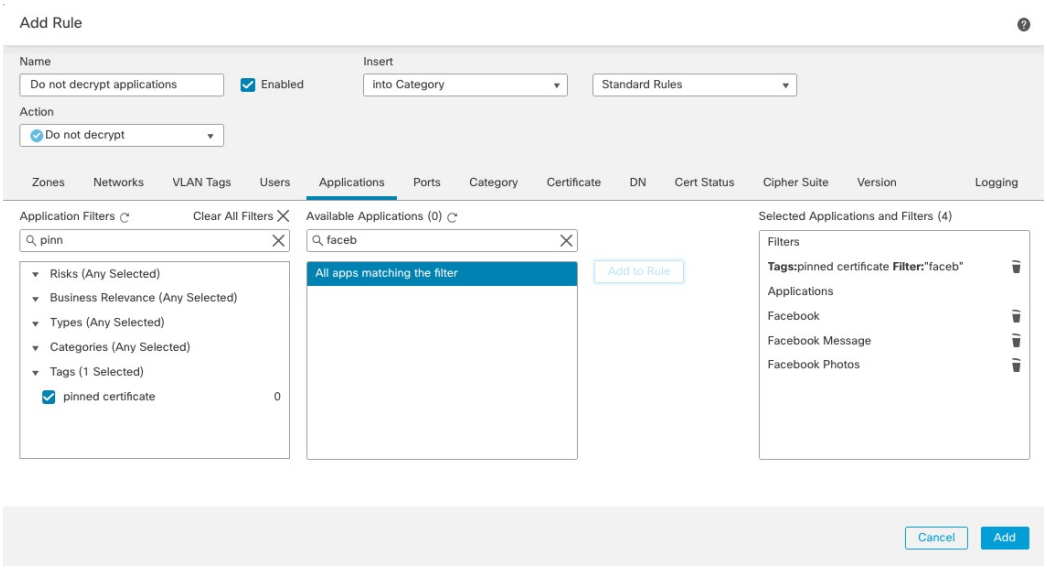
评估网络上的流量，以确定哪些流量与低风险类别、信誉或应用相匹配，并使用**不解密**操作来添加这些规则。将这些规则放在其他更具体的**不解密**规则之后，因为系统需要更多时间来处理流量。

以下为示例。


SSL Policy Example
Enter Description
Save
Cancel
Rules
Trusted CA Certificates
Undecryptable Actions
Advanced Settings
Add Category
Add Rule
Search Rules
Name Source Zones Dest Zones Source Networks Dest Networks VLAN Tags Users Applicati... Source Ports Dest Ports Categories SSL Action
Administrator Rules
This category is empty
Standard Rules
1 DND internal source network Intranet Do not decrypt
2 Decrypt test site Astrology (Any Decrypt - Resign
3 Do not decrypt low risk Risks: Very Lo Do not decrypt
4 Do not decrypt applications Facebook Facebook Mes Facebook Pho Do not decrypt
5 Decrypt all but trusted categ Any (Except Ur Decrypt - Resign
6 Block bad cert status 1 Cert Status se Block
7 Block SSLv3. TLS 1.0, 1.1 3 Protocol Versi Block
Root Rules
This category is empty
Default Action
Do not decrypt

规则详细信息：


Editing Rule - Do not decrypt low risk
Name
Do not decrypt low risk
Enabled
Move
Action
Do not decrypt
Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Logging
Application Filters
Clear All Filters
Search by name
Risks (Any Selected)
Very Low 538
Low 454
Medium 282
High 139
Very High 70
Business Relevance (Any Selected)
Very Low 580
Available Applications (1483)
Search by name
050plus
1&1 Internet
1-800-Flowers
1000mercis
12306.cn
123Movies
126.com
17173.com
Viewing 1-100 of 1483
Add to Rule
Selected Applications and Filters (1)
Filters
Risks:Very Low, Low
Cancel
Save



相关主题

配置应用控制的最佳实践，第 1250 页
应用控制的建议，第 1248 页

创建解密 - 类别的重新签名规则

本主题展示为除未分类站点外的所有站点创建包含 **解密 - 重新签名** 操作的 TLS/SSL 规则 的示例。该规则使用可选的**仅替换密钥 (Replace Key Only)** 选项，我们始终建议将其与**解密 - 重新签名 (Decrypt-Resign)** 规则操作配合使用。

当用户浏览到使用自签名证书的站点时，**仅替换密钥 (Replace Key Only)** 会导致用户在 Web 浏览器中看到安全警告，使用户知道他们正在与不安全的站点通信。

通过将此规则放在底部附近，您可以兼顾两者：您可以解密和（可选）检查流量，同时不会影响性能，就像您将规则放在策略中一样。

过程

步骤 1 如果尚未登录，请登录Cisco Secure Firewall Management Center。

步骤 2 如果尚未执行此操作，请将内部证书颁发机构 (CA) 上传到 Cisco Secure Firewall Management Center（**对象** > **对象管理**，然后 **PKI** > **内部 CA (Internal CAs)**）。

步骤 3 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 4 点击 SSL 策略旁边的 **编辑**（ ）。

步骤 5 点击**添加规则 (Add Rule)**。

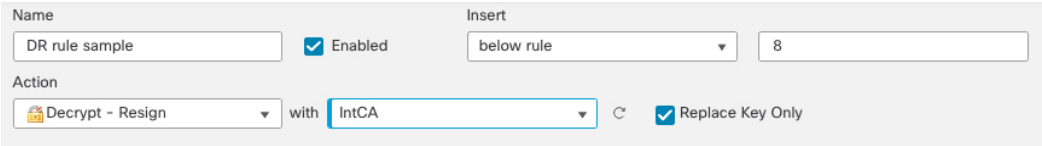
步骤 6 在**名称 (Name)** 字段中，输入用于标识规则的名称。

步骤 7 从**操作 (Action)** 列表中，点击**解密 - 重新签名 (Decrypt - Resign)**。

步骤 8 从**与 (with)** 列表中，点击内部 CA 的名称。

步骤 9 选中**仅替换密钥 (Replace Key Only)** 框。

下图显示了一个示例。



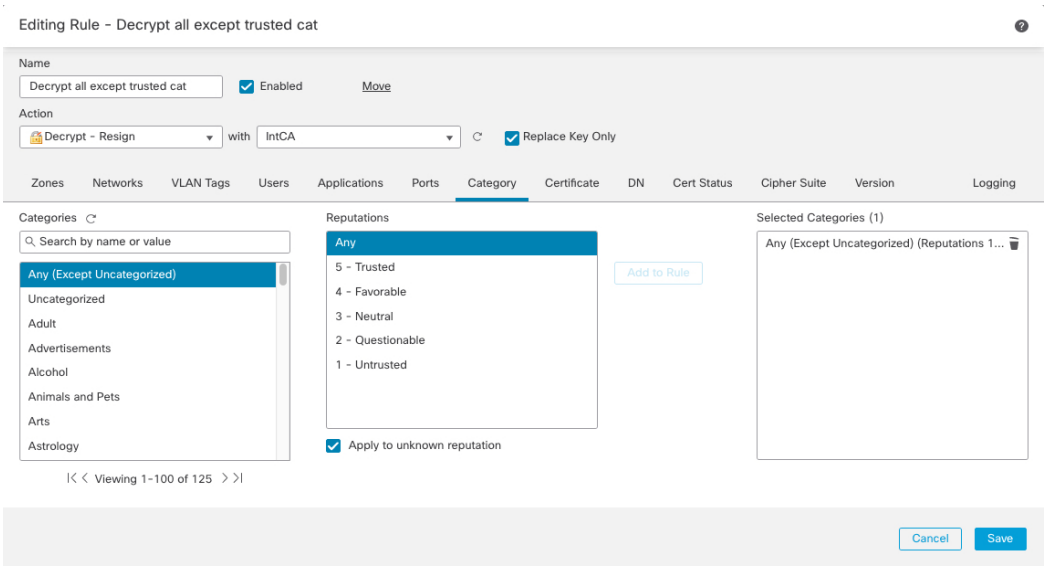
步骤 10 点击**类别 (Category)** 选项卡页面。

步骤 11 从**类别 (Categories)** 列表的顶部，点击**任何（未分类除外）(Any [Except Uncategorized])**。

步骤 12 从**信誉 (Reputations)** 列表中，点击**任意 (Any)**。

步骤 13 点击**添加至规则**。

下图显示了一个示例。

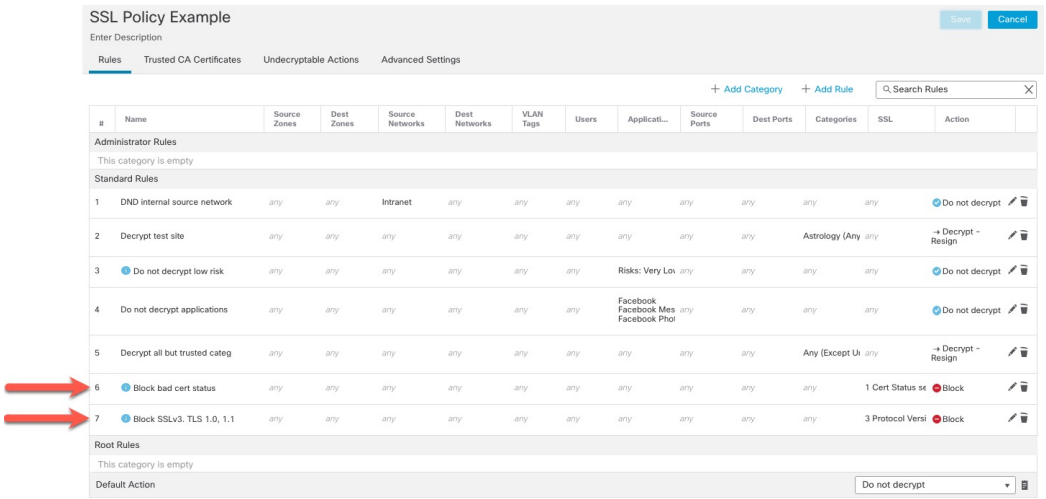


相关主题

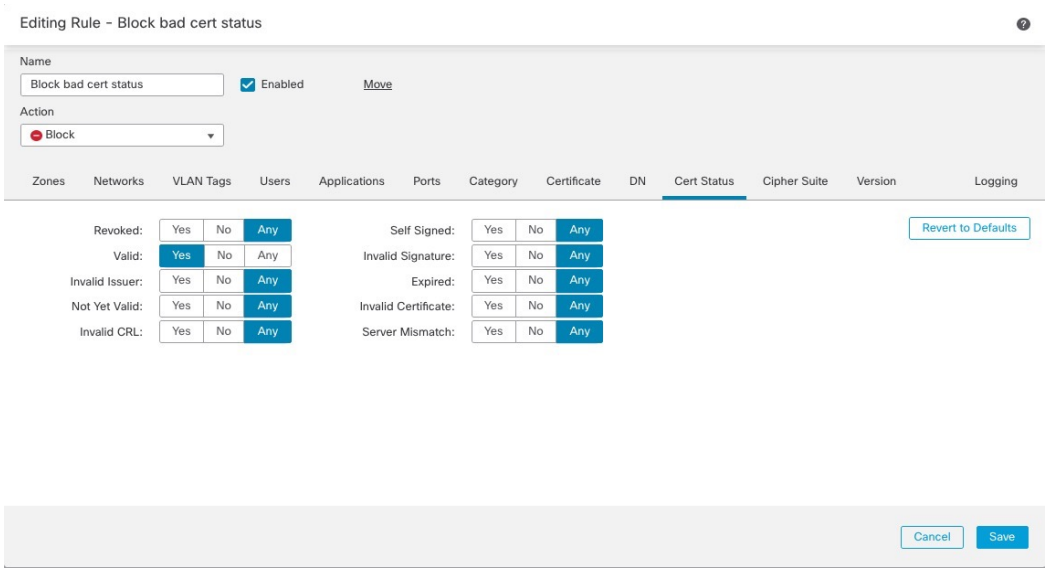
内部证书颁发机构对象，第 1001 页

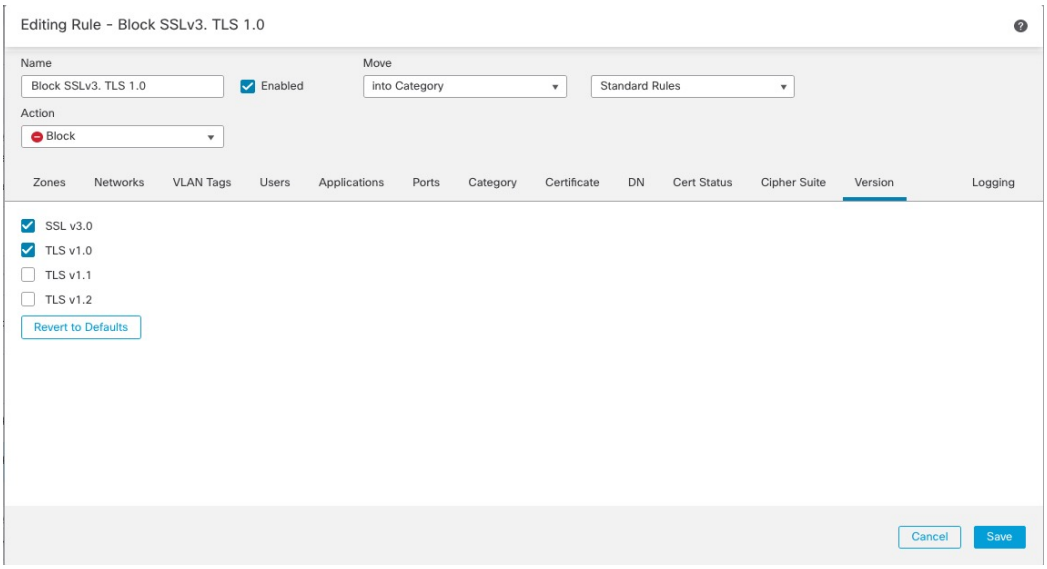
最后的 TLS/SSL 规则：阻止或监控证书和协议版本

由于最后的 TLS/SSL 规则最具体且需要最多的处理，因此它们是监控或阻止不良证书和不安全协议版本的规则。


SSL Policy Example
Enter Description
Save
Cancel
Rules
Trusted CA Certificates
Undecryptable Actions
Advanced Settings
Add Category
Add Rule
Search Rules
Name Source Zones Dest Zones Source Networks Dest Networks VLAN Tags Users Applicati... Source Ports Dest Ports Categories SSL Action
Administrator Rules
This category is empty
Standard Rules
1 DND internal source network Intranet Do not decrypt
2 Decrypt test site Astrology (Any → Decrypt - Resign
3 Do not decrypt low risk Risks: Very Lo Do not decrypt
4 Do not decrypt applications Facebook Facebook Mes Facebook Phot Do not decrypt
5 Decrypt all but trusted categ Any (Except U → Decrypt - Resign
6 Block bad cert status 1 Cert Status se Block
7 Block SSLv3. TLS 1.0, 1.1 3 Protocol Versi Block
Root Rules
This category is empty
Default Action
Do not decrypt

规则详细信息：


Editing Rule - Block bad cert status
Name
Block bad cert status
Enabled
Move
Action
Block
Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Logging
Revoked: Yes No Any
Valid: Yes No Any
Invalid Issuer: Yes No Any
Not Yet Valid: Yes No Any
Invalid CRL: Yes No Any
Self Signed: Yes No Any
Invalid Signature: Yes No Any
Expired: Yes No Any
Invalid Certificate: Yes No Any
Server Mismatch: Yes No Any
Revert to Defaults
Cancel
Save



相关主题

示例： TLS/SSL 规则 监控或阻止证书状态的规则 ， 第 1782 页
示例：用于监控或阻止协议版本的 TLS/SSL 规则 ， 第 1784 页
可选示例：监控或阻止证书可分辨名称的 TLS/SSL 规则 ， 第 1785 页

示例： TLS/SSL 规则 监控或阻止证书状态的规则

由于最后的 TLS/SSL 规则最具体且需要最多的处理，因此它们是监控或阻止不良证书和不安全协议版本的规则。本部分中的示例显示如何按证书状态监控或阻止流量。

注释 仅在具有**阻止**或**阻止并重置**规则操作的规则中使用**密码套件 (Cipher Suite)** 和**版本 (Version)** 规则条件。在具有其他规则操作的规则中使用这些条件可能会干扰系统的 ClientHello 处理，从而导致不可预测的性能。

过程

步骤 1 如果尚未登录，请登录Cisco Secure Firewall Management Center。

步骤 2 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 3 点击 SSL 策略旁边的 **编辑**（）。

步骤 4 点击 TLS/SSL 规则旁的 **编辑**（） 。

步骤 5 点击**添加规则 (Add Rule)**。

步骤 6 在“添加规则”(Add Rule) 对话框中，在**名称 (Name)** 字段中输入规则的名称。

步骤 7 点击**证书状态 (Cert Status)**。

步骤 8 就每个证书状态而言，有以下选项：

- 点击**是 (Yes)** 可根据该证书状态是否存在进行匹配。
- 点击**否 (No)** 可根据该证书状态是否缺失进行匹配。
- 点击**任意 (Any)** 可在匹配规则时跳过条件。换言之，选择**任意**意味着无论证书状态是否存在都与该规则匹配。

步骤 9 从**操作 (Action)** 列表中，点击**监控 (Monitor)** 以仅监控和记录与规则匹配的流量，或点击**阻止 (Block)** 或**阻止并重置 (Block with Reset)** 以阻止流量并选择性地重置连接。

步骤 10 要保存对规则的更改，请点击页面底部的**保存 (Save)**。

步骤 11 要保存对策略的更改，请点击页面顶部的**保存 (Save)**。

示例

组织信任 Verified Authority 证书颁发机构。组织不信任 Spammer Authority 证书颁发机构。系统管理员将 Verified Authority 证书和由 Verified Authority 颁发的中间 CA 证书上传到系统。由于“已验证颁发机构”已撤销它以前颁发的证书，因此系统管理员上传该“已验证颁发机构”提供的 CRL。

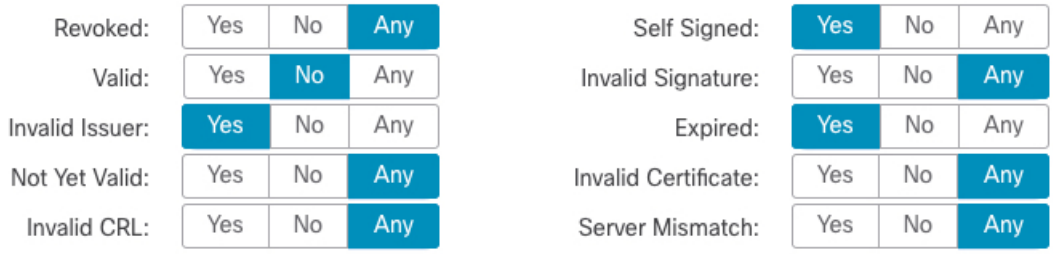
下图说明用于检查有效证书、由“已验证颁发机构”颁发的证书、不在 CRL 上的证书以及仍在有效开始日期和有效结束日期内的证书的证书状态规则条件。受配置原因的影响，未通过访问控制来解密和检查使用这些证书加密的流量。

Revoked:	Yes	No	**Any**	Self Signed:	Yes	No	**Any**
Valid:	**Yes**	No	Any	Invalid Signature:	Yes	No	**Any**
Invalid Issuer:	Yes	No	**Any**	Expired:	Yes	No	**Any**
Not Yet Valid:	Yes	No	**Any**	Invalid Certificate:	Yes	No	**Any**
Invalid CRL:	Yes	No	**Any**	Server Mismatch:	Yes	No	**Any**

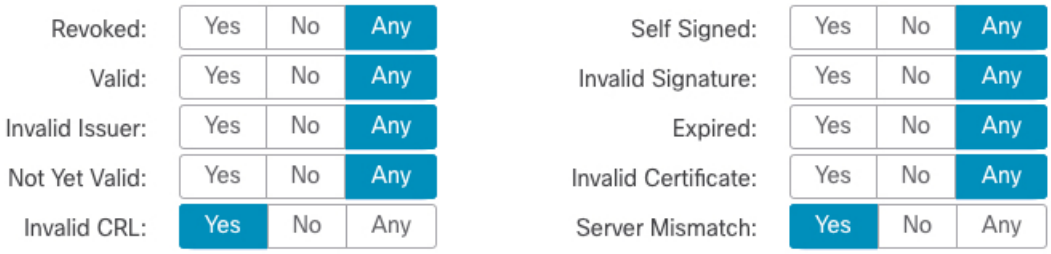
下图显示用于检查状态是否缺失的证书状态规则条件。在此情况下，由于配置原因，它与使用尚未到期的证书加密的流量相匹配并监控该流量。

Revoked:	Yes	No	**Any**	Self Signed:	Yes	No	**Any**
Valid:	Yes	No	**Any**	Invalid Signature:	Yes	No	**Any**
Invalid Issuer:	Yes	No	**Any**	Expired:	Yes	**No**	Any
Not Yet Valid:	Yes	No	**Any**	Invalid Certificate:	Yes	No	**Any**
Invalid CRL:	Yes	No	**Any**	Server Mismatch:	Yes	No	**Any**

在下面的示例中，如果传入流量使用的证书具有无效的颁发者、自签名、已过期且是无效证书，则流量会与此规则条件匹配。



下图展示了一个证书状态规则条件，如果请求的 SNI 与服务器名称匹配或者 CRL 无效，则会与该规则条件匹配。



示例：用于监控或阻止协议版本的 TLS/SSL 规则

本示例显示了如何阻止网络上不再被视为安全的 TLS 和 SSL 协议，例如 TLS 1.0、TLS 1.1 和 SSLv3。包含这些内容是为了让您更详细地了解协议版本规则的工作方式。

您应该从网络中排除不安全的协议，因为它们都可能会被利用。在本例中：

- 您可以使用 SSL 规则上的**版本 (Version)** 页面来阻止某些协议。
- 由于系统会将 SSLv2 视为无法解密，因此您可以对 SSL 策略使用 **无法解密的操作** 来阻止它。
- 同样，由于不支持压缩的 TLS/SSL，因此您也应将其阻止。

注释 仅在具有**阻止**或**阻止并重置**规则操作的规则中使用**密码套件 (Cipher Suite)** 和**版本 (Version)** 规则条件。在具有其他规则操作的规则中使用这些条件可能会干扰系统的 ClientHello 处理，从而导致不可预测的性能。

过程

步骤 1 如果尚未登录，请登录Cisco Secure Firewall Management Center。

步骤 2 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 3 点击 SSL 策略旁边的 **编辑**（✎）。

步骤 4 点击 TLS/SSL 规则旁的 **编辑**（✎）。

步骤 5 点击**添加规则 (Add Rule)**。

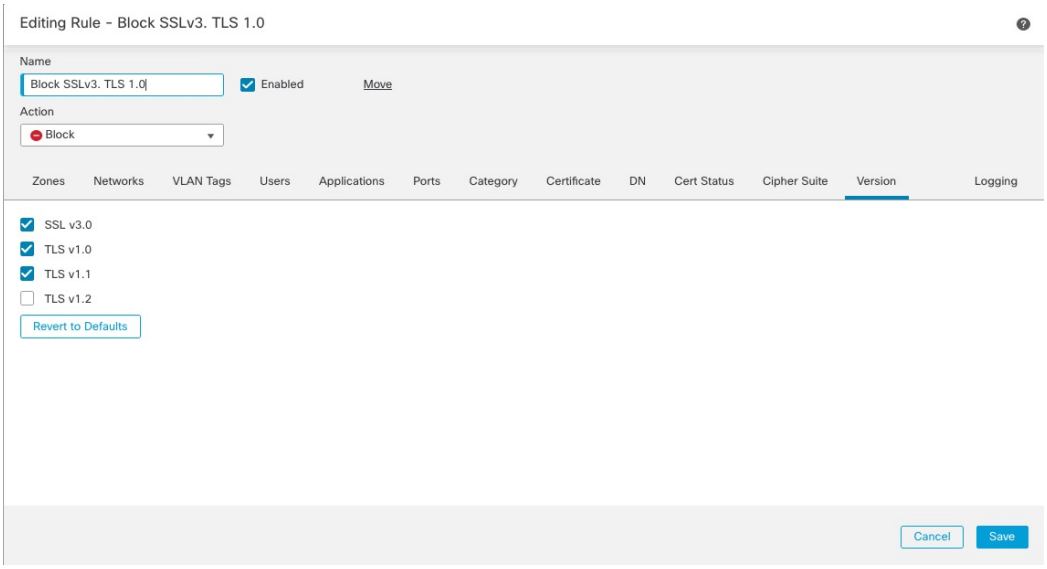
步骤 6 在“添加规则”(Add Rule) 对话框中，在**名称 (Name)** 字段中输入规则的名称。

步骤 7 从**操作 (Action)** 列表中，点击**阻止 (Block)** 或**阻止并重置 (Block with reset)**。

步骤 8 点击**版本 (Version)** 页面。

步骤 9 选中不再安全的协议的复选框，例如 **SSL v3.0**、**TLS 1.0** 和 **TLS 1.1**。取消选中仍被视为安全的任何协议的复选框。

下图显示了一个示例。



步骤 10 根据需要选择其他规则条件。

步骤 11 点击**保存 (Save)**。

可选示例：监控或阻止证书可分辨名称的 TLS/SSL 规则

包含此规则是为了让您了解如何根据服务器证书的可分辨名称来监控或阻止流量。将其包含在内是为了向您提供更多详细信息。

可分辨名称可以包含国家/地区代码、公用名、组织和组织单位，但通常只会包含一个公用名。例如，`https://www.cisco.com` 的证书中的公用名为 `cisco.com`。（但这并非总是那么简单；可分辨名称 (DN) 规则条件，第 1749 页中的可分辨名称规则条件部分介绍了如何查找常用名称。）

客户端请求中 URL 的主机名部分是服务器名称指示 (SNI)。客户端会使用 TLS 握手中的 SNI 扩展名来指定要连接的主机名（例如，`auth.amp.cisco.com`）。然后，服务器会选择在单个 IP 地址上托管所有证书时建立连接所需的相应私钥及证书链。

过程

步骤 1 如果尚未登录，请登录Cisco Secure Firewall Management Center。

步骤 2 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 3 点击 SSL 策略旁边的 **编辑**（）。

步骤 4 点击 TLS/SSL 规则旁的 **编辑**（） 。

步骤 5 点击**添加规则 (Add Rule)**。

步骤 6 在“添加规则”(Add Rule) 对话框中，在**名称 (Name)** 字段中输入规则的名称。

步骤 7 从**操作 (Action)** 列表中，点击**阻止 (Block)** 或**阻止并重置 (Block with reset)**。

步骤 8 点击 **DN**。

步骤 9 从**可用 DN (Available DNs)** 中查找要添加的可分辨名称，如下所示：

- 要即时添加可随后添加到条件中的可分辨名称，请点击**可用 DN (Available DNs)** 列表上方的 **添加**（）。
- 要搜索将添加的可分辨名称对象和组，请点击**可用 DN (Available DNs)** 列表上方的**按名称或值搜索 (Search by name or value)** 提示，然后键入对象的名称或对象中的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 10 要选择对象，请点击该对象。要选择所有对象，请点击右键，然后选择**全选 (Select All)**。

步骤 11 点击**添加到使用者 (Add to Subject)** 或**添加到颁发者 (Add to Issuer)**。

提示 您也可以拖放选定对象。

步骤 12 添加要手动指定的所有文本公用名或可分辨名称。点击**使用者 DN (Subject DNs)** 或**颁发者 DN (Issuer DNs)** 列表下方的**输入 DN 或 CN (Enter DN or CN)** 提示，然后键入公用名或可分辨名称并点击**添加 (Add)**。

虽然您可以将 CN 或 DN 添加到任一列表，但更常见的是将它们添加到**使用者 DN (Subject DNs)** 列表。

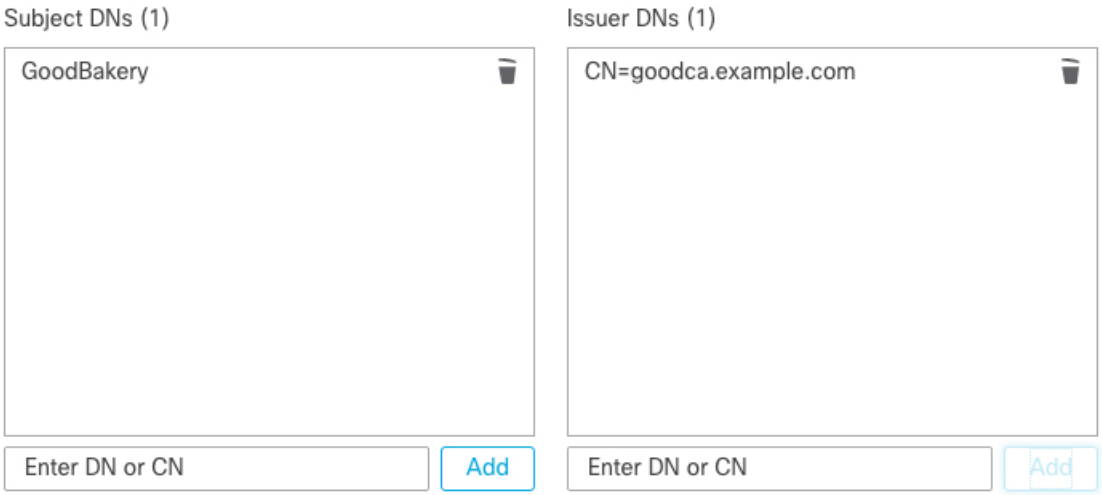
步骤 13 添加或继续编辑规则。

步骤 14 完成后，要保存对规则的更改，请点击页面底部的**保存 (Save)**。

步骤 15 要保存对策略的更改，请点击页面顶部的**保存 (Save)**。

示例

下图显示了用于搜索向 goodbakery.example.com 颁发或由 goodca.example.com 颁发的证书的可分辨名称规则条件。根据访问控制，允许通过这些证书加密的流量。



TLS/SSL 规则 设置

如何为TLS/SSL 规则配置建议的最佳实践设置。

TLS/SSL 规则：为每个规则启用日志记录，但具有 **不解密** 规则操作的规则除外。（这取决于您；如要查看有关未解密的流量的信息，请同时启用这些规则的日志记录。）

过程

步骤 1 如果尚未登录，请登录Cisco Secure Firewall Management Center。

步骤 2 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 3 点击 SSL 策略旁边的 **编辑**（）。

步骤 4 点击 TLS/SSL 规则旁的 **编辑**（） 。

步骤 5 点击**日志记录 (Logging)**选项卡。

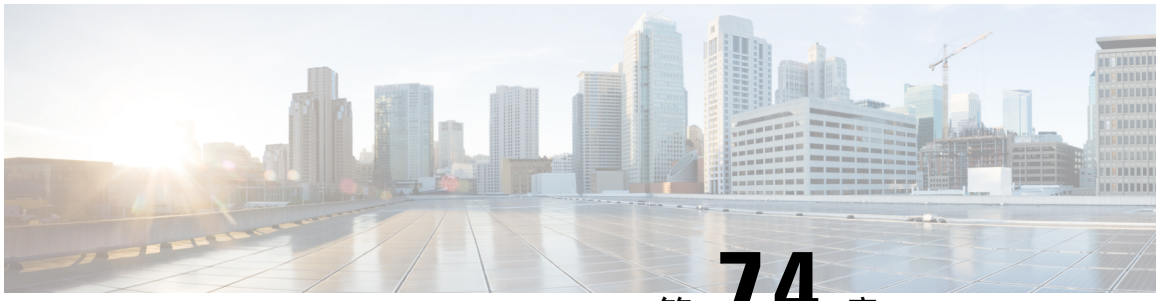
步骤 6 点击**在连接结束时记录 (Log at End of Connection)**。

步骤 7 点击**保存 (Save)**。

步骤 8 点击页面顶部的 **Save**。

第 XVII 部分

用户身份



第 74 章

用户身份概述

以下主题讨论用户身份：

关于用户身份

用户身份信息可以帮助识别政策违规、攻击或网络漏洞的来源，并跟踪它们到具体用户。例如，您可以确定：

- 谁拥有作为影响程度为“易受攻击”（级别 1：红色）的入侵事件的目标的主机。
- 谁发起了内部攻击或端口扫描。
- 谁正在尝试对指定主机进行未经授权的访问。
- 谁正在耗用异常大量的带宽。
- 谁尚未应用关键操作系统更新。
- 谁正在违反公司政策使用即时消息软件或 P2P 文件共享应用。
- 谁与您网络中的每个危害表现相关。

借助这些信息，可以使用 Firepower 系统的其他功能降低风险，执行访问控制以及采取措施防止中断他人的活动。这些功能还可以大大改善审核控制并提高合规性。

在配置用户身份源以收集用户数据后，您可以执行用户感知和用户控制。

相关主题

身份术语，第 1792 页
关于用户身份源，第 1792 页
身份部署，第 1795 页
如何设置身份策略，第 1800 页

身份术语

本主题讨论用户身份和用户控制的常用术语。

用户感知

使用身份源（如或 TS 代理）标识网络中的用户。通过用户感知，您可以从授权（例如 Active Directory）和非授权（基于应用）源中识别用户。要使用 Active Directory 作为身份源，必须配置领域和目录。有关详细信息，请参阅关于用户身份源，第 1792 页。

用户控制

配置与访问控制策略关联的身份策略。（然后，身份策略将作为访问控制子策略引用。）身份策略指定身份源以及（可选）属于该源的用户和组。

通过将身份策略与访问控制策略相关联，可以确定在网络中是监控、信任、阻止还是允许流量中的用户或用户活动。有关详细信息，请参阅访问控制策略，第 1259 页。

授权身份源

验证了用户登录的受信任服务器（例如，Active Directory）。您可以使用从授权登录获取的数据执行用户感知和用户控制。授权用户登录是从被动和主动身份验证中获取：

- 被动身份验证发生在用户通过外部源进行身份验证时。ISE/ISE-PIC 和 TS 代理是 Firepower 系统支持的被动身份验证方法。
- 主动身份验证发生在用户通过预先配置的受管设备进行身份验证时。强制网络门户和远程接入访问 VPN 是 Firepower 系统支持的主动身份验证方法。

非授权身份源

未知或不受信任的服务器已验证用户登录。基于流量的检测是 Firepower 系统唯一支持的未授权身份源。您可以使用从非授权登录获取的数据执行用户感知。

关于用户身份源

下表提供系统支持的用户身份源的简要概述。每个身份源都提供一个用户存储库以获取用户感知。然后，可以使用身份和访问控制策略来控制这些用户。

用户身份源	策略	服务器要求	类型	身份验证类型	用户感知？	用户控制？	有关详细信息，请参阅.....
ISE/ISE-PIC	身份	Microsoft Active Directory	授权登录	无源	是	是	ISE/ISE-PIC 身份源，第 1845 页
TS 代理	身份	Microsoft Windows 终端服务器	授权登录	无源	是	是	终端服务 (TS) 代理身份源，第 1883 页

用户身份源	策略	服务器要求	类型	身份验证类型	用户感知？	用户控制？	有关详细信息，请参阅.....
强制网络门户	身份	OpenLDAP Microsoft Active Directory	授权登录	主用	是	是	强制网络门户身份源，第 1863 页
远程接入 VPN	身份	OpenLDAP 或 Microsoft Active 目录	授权登录	主用	是	是	远程接入 VPN 身份源，第 1879 页
	身份 (Identity)	RADIUS	授权登录	主用	是	否	
基于流量的检测	网络发现	n/a	非授权登录	n/a	是	否	基于流量的检测身份源，第 1974 页

当选择要部署的身份源时，请考虑以下事项：

- 必须使用基于流量的检测来检测非 LDAP 用户登录。
- 必须使用基于流量的检测或强制网络门户来记录失败的登录或身份验证活动。如果登录或身份验证尝试失败，则不会将新用户添加到数据库的用户列表中。
- 强制网络门户身份源需要具有路由接口的受管设备。您不能使用具有强制网络门户的内联（也称为分路模式）接口。

这些身份源的数据存储在 Cisco Secure Firewall Management Center的用户数据库和用户活动数据库中。您可以配置 管理中心服务器用户下载，以将新用户数据定期自动下载到您的数据库中。

在使用所需的身份源配置身份规则之后，必须将每个规则与访问控制策略相关联，并将策略部署到受管设备，策略才能产生效果。有关访问控制策略和部署的详细信息，请参阅将其他策略与访问控制相关联，第 1276 页。

有关用户身份的常规信息，请参阅 关于用户身份，第 1791 页。

用户身份的最佳实践

我们建议您在设置身份策略之前查看以下信息。

- 了解用户限制
- 每个 AD 域创建一个领域
- 运行状况监控
- 使用最新版本的 ISE/ISE-PIC，两种类型的补救
- 6.7 中的用户代理支持丢弃

- 强制网络门户需要路由接口，多个单独的任务

Active Directory、LDAP 和领域

Firepower 系统支持 Active Directory 或 LDAP 进行用户感知和控制。Active Directory 或 LDAP 存储库与 FMC 之间的关联被称为领域。您应为每个 LDAP 服务器或 Active Directory 域创建一个领域。有关支持版本的详细信息，请参阅领域支持的服务器，第 1812 页。

LDAP 支持的唯一用户身份源是强制网络门户。要使用其他身份源（ISE/ISE-PIC 除外），您必须使用 Active Directory。

仅适用于 Active Directory：

- 为每个域控制器创建一个目录。

  有关详细信息，请参阅 创建 Active Directory 领域和领域目录，第 1816 页

- 如果将所有 Active Directory 域和域控制器分别添加为领域和目录，则支持两个域之间存在信任关系的用户和组。

  有关详细信息，请参阅领域和受信任的域，第 1809 页。

代理序列

代理序列 是一个或多个可用于与 LDAP、 Active Directory 或 ISE / ISE-PIC 服务器通信的受管设备。仅当 思科防御协调器 （CDO）无法与 Active Directory 或 ISE / ISE-PIC 服务器通信时，才需要执行此操作。（例如， CDO 可能在公共云中，但 Active Directory 或 ISE / ISE-PIC 可能在私有云中。）

虽然您可以使用一台受管设备作为代理序列，但我们强烈建议您设置两台或更多设备，以便在受管设备无法与 Active Directory 或 ISE / ISE-PIC 通信时，另一台受管设备可以接管。

使用最新版本的 ISE/ISE-PIC

如果您希望使用 ISE/ISE-PIC 身份源，则强烈建议您始终使用最新版本，以确保获得最新的功能和漏洞修复。

pxGrid 2.0（版本 2.6 补丁 6 或更高版本使用；或 2.7 补丁 2 或更高版本）还将 ISE/ISE-PIC 使用的补救从终端保护服务 (EPS) 更改为自适应网络控制 (ANC)。如果升级 ISE/ISE-PIC，您必须将中介策略从 EPS 迁移到 ANC。

有关使用 ISE/ISE-PIC 的更多信息，请参阅ISE/ISE-PIC 指南和限制，第 1847 页。

要设置 ISE/ISE-PIC 身份源，请参阅如何为用户控制配置 ISE/ISE-PIC，第 1850 页。

强制网络门户信息

强制网络门户是唯一可以使用 LDAP 或 Active Directory 的用户身份源。此外，必须将托管设备配置为使用路由接口。

其他准则可在强制网络门户指南和限制，第 1864 页中找到。

设置强制网络门户需要执行多项独立任务。有关详细信息，请参阅如果为用户控制配置强制网络门户，第 1867 页。

TS 代理信息

需要 TS 代理用户身份源来识别 Windows 终端服务器上的用户会话。TS 代理软件必须安装在终端服务器计算机上，如《思科终端服务 *(TS)* 代理指南》中所述。此外，您必须将 TS 代理服务器上的时间与 管理中心上的时间进行同步。

TS 代理数据显示在“用户”(Users)、“用户活动”(User Activity) 和“连接事件”(Connection Event) 表中，并可用于用户感知和用户控制。

有关详细信息，请参阅TS 代理准则，第 1883 页。

将身份策略与访问控制策略相关联

在配置领域、目录和用户身份源后，您必须在身份策略中设置身份规则。要让策略生效，您必须将身份策略与访问控制策略相关联。

有关创建身份策略的详细信息，请参阅创建身份策略，第 1887 页。

有关创建身份规则的详细信息，请参阅创建身份规则，第 1894 页。

要将身份策略与访问控制策略相关联，请参阅将其他策略与访问控制相关联，第 1276 页。

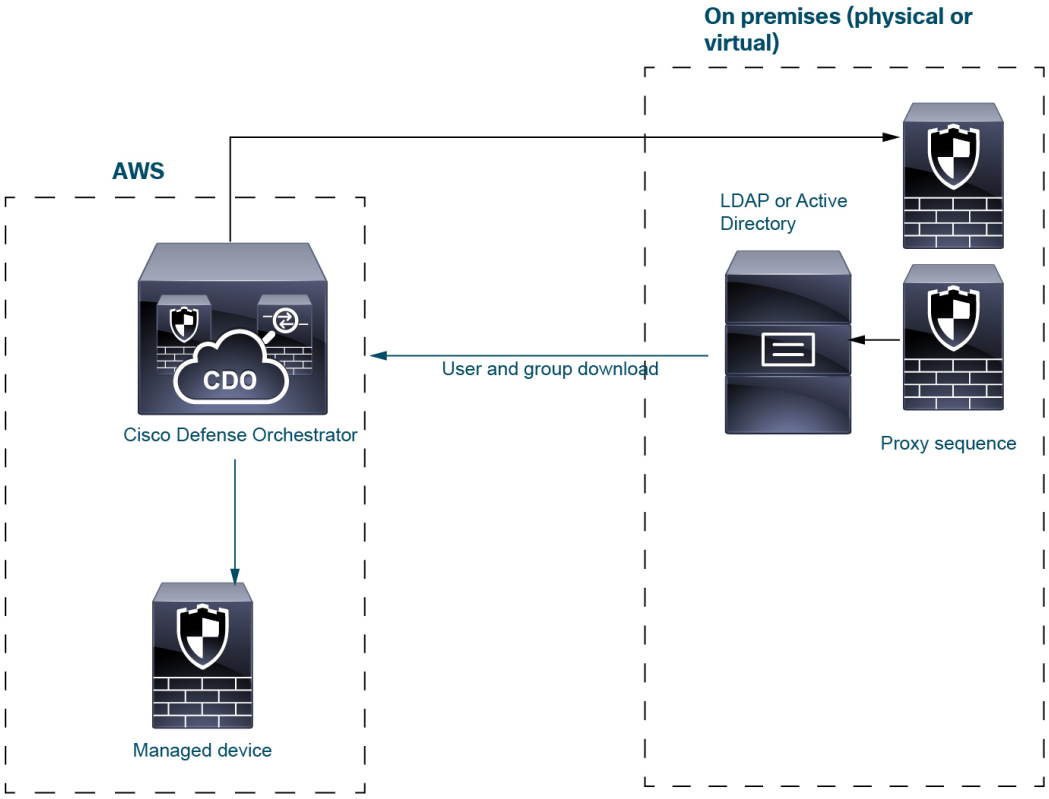
身份部署

系统从任何身份源检测到用户登录的用户数据时，会将登录用户与 管理中心用户数据库中的用户列表进行比对。如果登录用户与现有用户匹配，则登录数据将会分配给该用户。如果登录信息与现有用户不匹配，则会创建新用户，除非登录信息位于 SMTP 流量中。SMTP 流量中不匹配的登录信息将被丢弃。

一旦用户被 管理中心 发现，用户所属的组就会与用户关联。

简单身份部署

本部分中讨论的示例部署基于下图所示的系统。



在上图中，CDO 和一个托管设备会被部署到 AWS，而其他设备位于本地。这些设备可以是物理设备，也可以是虚拟设备；它们只需要能够相互通信。

两个本地托管设备将用作代理序列。您还必须将这些设备添加到 CDO。

代理序列 是一个或多个可用于与 LDAP、 Active Directory 或 ISE / ISE-PIC 服务器通信的受管设备。仅当 思科防御协调器 （CDO）无法与 Active Directory 或 ISE / ISE-PIC 服务器通信时，才需要执行此操作。（例如， CDO 可能在公共云中，但 Active Directory 或 ISE / ISE-PIC 可能在私有云中。）

只有 TS 代理和强制网络门户需要 LDAP 或 Active Directory，如以下段落所述。

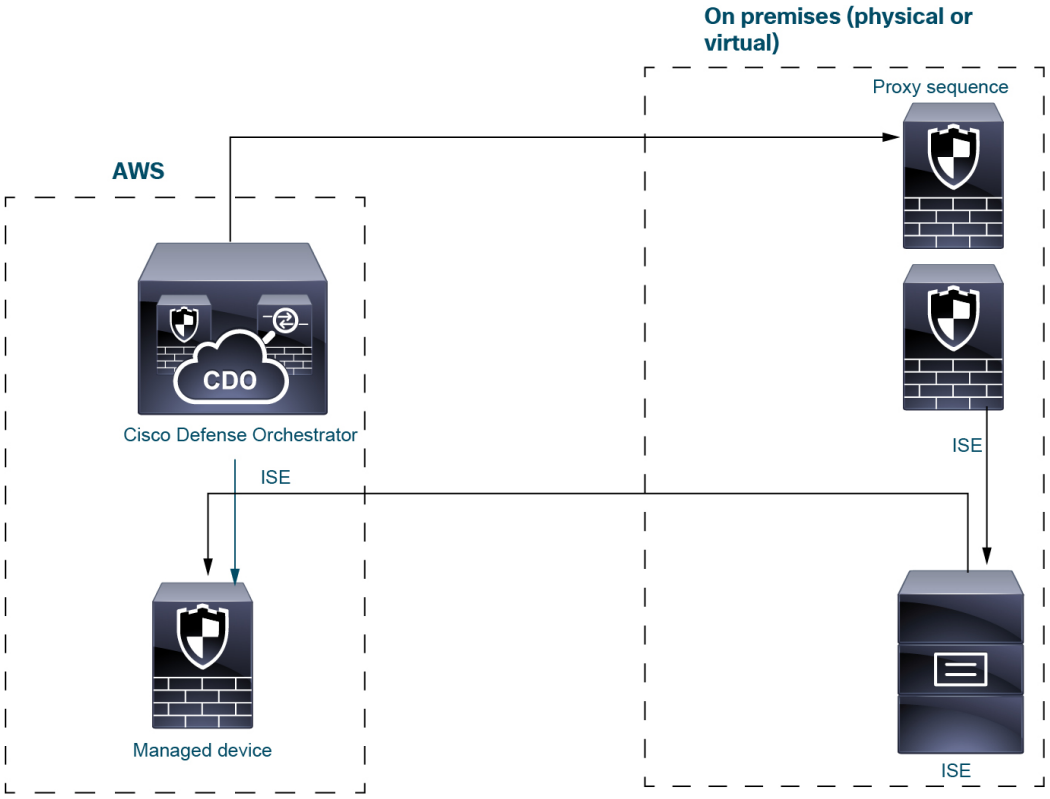
有关设置此类系统的详细信息，请参阅如何设置身份策略，第 1800 页。

ISE/ISE-PIC 身份源

部署 ISE/ISE-PIC 身份源时，如果 CDO 无法直接联系 ISE/ISE-PIC 服务器，CDO 会联系代理序列。用户、组和订用会从 ISE/ISE-PIC 服务器被发送到 AWS 中的托管设备。

您可以选择在 ISE/ISE-PIC 部署中使用 LDAP 服务器，但由于它是可选的，因此并未在下图中显示。

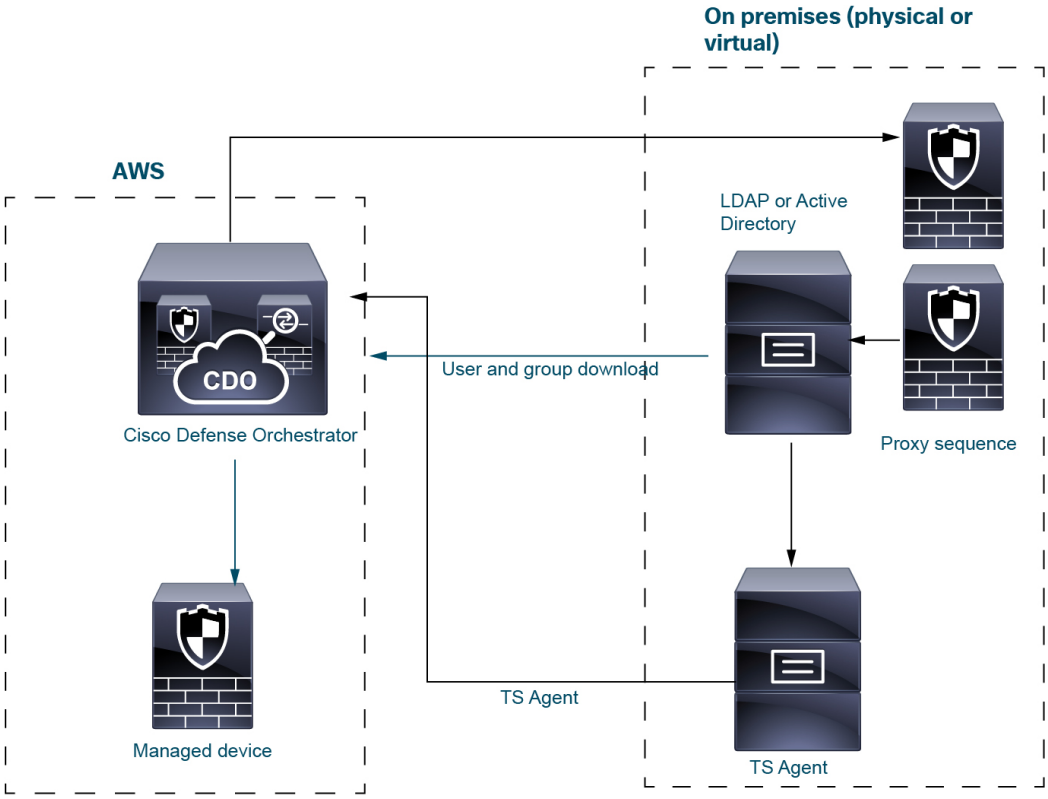
有关 ISE / ISE-PIC 的详细信息，请参阅 ISE/ISE-PIC 身份源，第 1845 页。



TS 代理身份源

终端服务 (TS) 代理软件可在 Microsoft 服务器上运行，并会根据用户登录服务器所用的端口范围来发送 CDO 用户信息。TS 代理会从 LDAP 或 Active Directory 获取用户身份信息，然后将它们发送到 CDO。

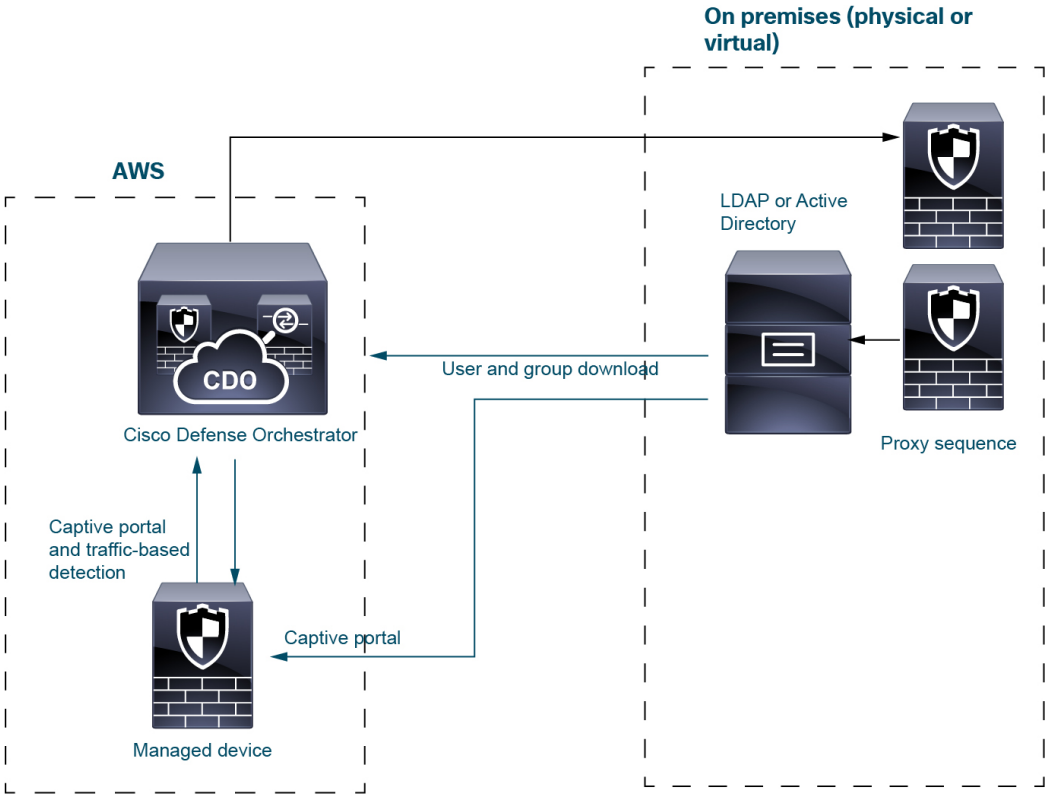
有关 TS 代理身份源的详细信息，请参阅终端服务 (TS) 代理身份源，第 1883 页。



强制网络门户身份源

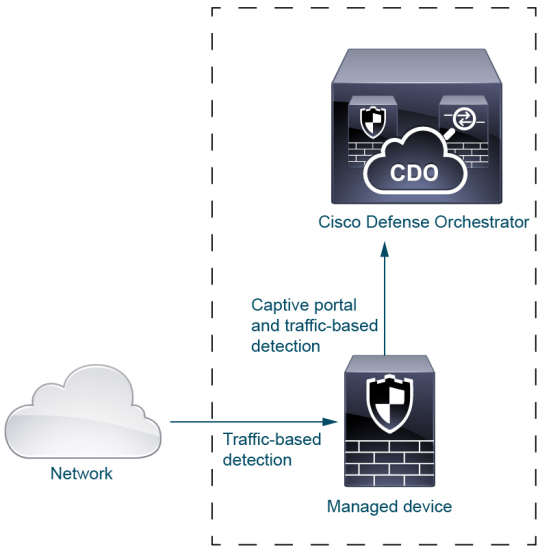
除 Active Directory 外，强制网络门户是唯一也支持 LDAP 的身份源。当用户尝试使用 AWS 中的托管设备通过 IP 地址或主机名来访问网络资源时，就会触发强制网络门户身份源。强制网络门户会使用代理序列从 LDAP 或 Active Directory 获取用户信息，然后将用户信息发送到 CDO。

有关强制网络门户身份源的详细信息，请参阅强制网络门户身份源，第 1863 页。



基于流量的检测

基于流量的检测仅用于检测网络上的应用，因此不需要使用像 Active Directory 这样的用户存储库或代理序列。有关详细信息，请参阅关于主机、应用和用户数据的检测，第 1901 页。



如何设置身份策略

本主题提供了使用任何可用的用户身份源（TS 代理、ISE/ISE-PIC、强制网络门户或远程接入 VPN）设置身份策略的高级概述。

过程

	命令或操作	目的
步骤 1	（可选。）创建代理序列。	代理序列 是一个或多个可用于与 LDAP、Active Directory 或 ISE / ISE-PIC 服务器通信的受管设备。仅当 思科防御协调器（CDO）无法与 Active Directory 或 ISE / ISE-PIC 服务器通信时，才需要执行此操作。（例如，CDO 可能在公共云中，但 Active Directory 或 ISE / ISE-PIC 可能在私有云中。） 虽然您可以使用一台受管设备作为代理序列，但我们强烈建议您设置两台或更多设备，以便在受管设备无法与 Active Directory 或 ISE / ISE-PIC 通信时，另一台受管设备可以接管。 请参阅创建代理序列，第 1814 页。
步骤 2	（可选。）创建领域和目录，林中包含要在用户控制中使用的用户的每个域都要创建一个领域。还为每个域控制器创建一个目录。只有具有相应 管理中心 领域和目录的用户和组才能用于身份策略中。	如果满足以下任一条件，则创建领域、领域目录和代理序列为可选： • 您使用的 SGT ISE 属性条件而不是用户、组、领域、终端位置或终端配置文件条件。 • 您仅使用身份策略来过滤网络流量。 • 仅当您使用 思科防御协调器 (CDO) 且代理序列无法直接与 Active Directory 或 ISE/ISE-PIC 通信时才需要代理序列。 领域是受信任的用户和组存储区，通常是 Microsoft Active Directory 存储库。管理中心会按您指定的间隔时间下载用户和组。您可以包括或排除用户和组来进行下载。 请参阅创建 Active Directory 领域和领域目录，第 1816 页。有关创建领域的选项的详细信息，请参阅领域字段，第 1818 页。 目录是一个 Active Directory 域控制器，它组织有关计算机网络的用户和网络共享的信息。Active Directory 控制器将为该领域提供

	命令或操作	目的
		目录服务。Active Directory 将跨域控制器分发用户和组对象，这些控制器是通过使用目录服务传播相互之间的本地更改的对等体。有关详细信息，请参阅 MSDN 上的 Active Directory 技术规范术语表。 您可以为某个领域指定多个目录，在这种情况下，每个域控制器都按该领域的**目录**选项卡页面上列出的顺序进行查询，以匹配进行用户控制的用户和组凭证。 **注释** 如果您计划配置 SGT ISE 属性条件而不是用户、组、领域、终端位置或终端配置文件条件，则可自行决定是否配置领域或领域序列。
步骤 3	从领域同步用户和组。	要想能够控制用户和组，您必须将它们与管理中心同步。您可以随时将其与用户和组同步，也可以将系统配置为按指定的时间间隔进行同步。 同步用户和组时，可以指定例外；例如，您可以从该领域的所有用户控制中排除“工程”组，也可以从应用于“工程”组的用户控制中排除用户 **joe.smith**。 请参阅 同步用户和组，第 1827 页
步骤 4	（可选。）创建领域序列。	领域序列是一个有序的领域列表，如果用于身份策略中，则会导致系统按指定顺序搜索领域，以查找与规则匹配的用户。请参阅创建领域序列，第 1828 页。
步骤 5	创建检索用户和组数据的方法（身份源）。	设置一个具有其独特配置的身份源，以便能够使用存储在该领域中的数据控制用户和组。身份源包括 TS 代理、网络强制门户或远程 VPN。请参见以下选项之一： • 如果为用户控制配置强制网络门户，第 1867 页 • 配置用户控制 ISE/ISE-PIC，第 1858 页 • 配置用户控制 RA VPN，第 1880 页

	命令或操作	目的
步骤 6	创建身份策略。	身份策略包含一个或多个身份规则，可选择按类别对其进行组织。请参阅创建身份策略，第 1887 页。 **注释** 如果您计划配置 SGT ISE 属性条件而不是用户、组、领域、终端位置或终端配置文件条件；或者，如果您只使用自己的身份策略来过滤网络流量，则可自行决定是否配置领域或领域序列。
步骤 7	创建一个或多个身份规则。	身份规则使您能够指定许多匹配条件，包括身份验证类型、网络区域、网络或地理位置、领域、领域序列等。请参阅创建身份规则，第 1894 页。
步骤 8	请将您身份策略与访问控制策略关联起来。	访问控制策略将会过滤并（可选）检查流量。身份策略必须与访问控制策略相关联方可生效。请参阅将其他策略与访问控制相关联，第 1276 页。
步骤 9	将访问控制策略部署到至少一个受管设备。	要使用策略控制用户活动，必须将该策略部署到客户端所连接到的受管设备。请参阅部署配置更改，第 136 页。
步骤 10	监控用户活动	查看由用户身份源收集的活动会话列表或由用户身份源收集的用户信息列表。。 如果满足以下所有条件，则不需要身份策略： • 您使用 ISE/ISE-PIC 身份源。 • 您未在访问控制策略中使用用户或组。 • 您在访问控制策略中使用安全组标记 (SGT)。有关详细信息，请参阅ISE SGT 与自定义 SGT 规则条件。

相关主题

配置基于流量的用户检测，第 1976 页

用户活动数据库

Cisco Secure Firewall Management Center上的用户活动数据库包含已配置的所有身份源检测或报告的网络上的用户活动记录。系统会在以下情况下记录事件：

- 检测到单独的登录或注销时。
- 检测到新用户时。
- 系统管理员手动删除用户时。
- 系统检测到不在数据库中的用户，但因已达到用户限制而无法添加该用户时。
- 您解决与用户关联的危害表现，或者为用户启用或禁用危害表现规则时。

注释 如果 TS 代理监控与其他被动身份验证身份源（如 ISE/ISE-PIC）相同的用户，则 管理中心 会划分 TS 代理数据的优先级。如果 TS 代理和 ISE 报告来自同一 IP 地址的相同活动，则仅会将 TS 代理数据记录到 管理中心。

可以使用 Cisco Secure Firewall Management Center查看系统检测到的用户活动。（**分析 (Analysis)** > **用户 (Users)** > **用户活动 (User Activity)**。）

用户数据库

Cisco Secure Firewall Management Center中的用户数据库包含所有已配置身份源检测或报告的每个用户的记录。您可以使用从授权源获取的数据进行用户控制。

有关受支持的非授权和授权身份源的详细信息，请参阅关于用户身份源，第 1792 页。

如 用户限制。达到此用户限制后，系统将基于其身份源对以前未检测到的用户数据划分优先级，如下所示：

- 如果新用户来自非授权身份源，则系统不会将该用户添加到数据库。要允许添加新用户，您必须手动或使用数据库清除删除用户。
- 如果新用户来自授权身份源，则系统会删除非活动时间最长的非授权用户，并将新用户添加到数据库。

如果身份源配置为排除特定用户名，则这些用户名的用户活动数据将不会报告给 Cisco Secure Firewall Management Center。这些已排除的用户名仍保留在数据库中，但不与 IP 地址关联。

如果已配置 管理中心高可用性且主连接失败，则在故障切换停机期间无法识别强制网络门户、ISE/ISE-PIC、TS 代理、远程接入 VPN 报告的所有登录，即便以前查看过这些用户并已将他们下载到 管理中心也是如此。无法识别的用户在 管理中心上记录为“未知”(Unknown) 未知用户。停机时间过后，系统将根据身份策略中的规则重新识别和处理“未知”(Unknown) 用户。

注释 如果 TS 代理监控与其他被动身份验证身份源（ISE/ISE-PIC）相同的用户，则 管理中心 会划分 TS 代理数据的优先级。如果 TS 代理和 ISE 报告来自同一 IP 地址的相同活动，则仅会将 TS 代理数据记录到 管理中心。

系统检测到新用户会话时，用户会话数据会保留在用户数据库中，直至出现以下其中一种情形：

- 管理中心 的用户将手动删除用户会话。
- 某个身份源报告该用户会话的注销操作。
- 某个领域结束其**用户会话超时：通过验证的用户**、**用户会话超时：未通过验证的用户**或**用户会话超时：访客用户**设置指定的用户会话。

思科防御协调器主机和用户限制

云交付的防火墙管理中心 主机限制

当在监控网络中检测到与IP地址相关联的活动时，云交付的防火墙管理中心会将主机添加到网络映射，如网络发现策略中所定义。

云交付的防火墙管理中心 可以在其主机数据库中存储最多 600,0000 个主机，但我们的建议如下。

由 **CDO** 管理的设备数量	建议的主机数量
1-50	100,000
51-300	300,000
301-1000	600,000

您无法查看不在网络映射中的主机的情景数据。但是，您可以执行访问控制。例如，您可以对不在网络映射中的主机接收和发出的流量进行应用控制，即使您无法使用合规 allow 名单监控主机的网络合规性。

注释 系统分别从 IP 地址和 MAC 地址识别的主机对仅 MAC 主机进行计数。与一台主机关联的所有 IP 地址均视为一台主机共同计数。

达到主机限制与删除主机

网络发现策略控制在您达到主机限制后检测到新主机时发生的情况；您可以丢弃新主机或替代非活动时间最长的主机。您也可以设置系统在主机处于非活动状态多长时间后将其从网络映射中删除的时间段。虽然您可以从网络映射中手动删除主机、整个子网或所有主机，但如果系统检测到与已删除主机相关的活动，它会重新添加该主机。

在多域部署中，每个分叶域都有自己的网络发现策略。因此，当系统发现新主机时，每个分叶域会管理自己的行为。

思科防御协调器云交付的防火墙管理中心用户限制

用户会在以下情况时被添加到 云交付的防火墙管理中心 用户数据库：

- 从领域下载用户。
- 强制网络门户或 RA-VPN 用户登录。
- 从任何身份源 （例如，TS 代理）检测到用户。

云交付的防火墙管理中心 可以在其主机数据库中存储最多 600,0000 个用户，但我们的建议如下。

由 CDO 管理的设备数量	建议的用户数量
1-50	100,000
51-300	300,000
301-1000	600,000

仅授权用户才能使用访问控制策略进行用户控制。

云交付的防火墙管理中心 可在其用户数据库中存储 600,000 个会话。

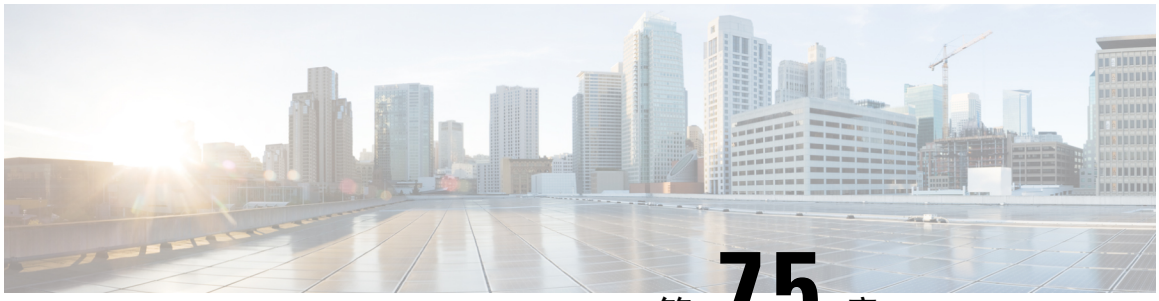
达到限制后，当系统检测到之前未检测到的新用户时，会根据其身份源确定用户数据的优先级：

- 如果新用户来自非授权源，则系统不会将该非授权用户添加到数据库。要允许添加新用户，您必须手动删除用户或清除数据库。
- 如果新用户来自授权身份源，则系统会删除非活动时间最长的非授权用户，并将新授权用户添加到数据库。

  如果只有授权用户，则系统会删除非活动时间最长的授权用户，并将新用户添加到数据库。

故障排除信息可在用户控制故障排除中看到。

提示 请注意，如果使用的是基于流量的检测，则您可按协议限制客户日志记录，以最大程度低减少用户名干扰并保留数据库空间。例如，您可以防止系统添加在 AIM、POP3 和 IMAP 流量中发现的用户，因为您了解此流量来自您不想监控的特定承包商或访客。



第 75 章

领域

以下主题介绍领域和身份策略：

关于领域和领域序列

领域是 Cisco Secure Firewall Management Center 和您监控的服务器上的用户帐户之间的连接。它们可指定该服务器的连接设置和身份验证过滤器设置。领域可以：

- 指定要监控其活动的用户和用户组。
- 查询用户存储库上有关授权用户以及某些非授权用户的用户元数据：通过基于流量的检测而检测到的 POP3 和 IMAP 用户以及通过基于流量的检测、TS 代理/或 ISE/ISE-PIC 而检测到的用户。

领域序列是要在身份策略中使用的两个或更多 Active Directory 领域的排序列表。将领域序列与身份规则关联时，系统会按照领域序列中指定的从第一个到最后的顺序来搜索 Active Directory 域。

您可以将多个域控制器添加为一个领域内的目录，但它们必须共享相同的基本领域信息。领域内的目录必须为专门的 LDAP 或专门的 Active Directory (AD) 服务器。启用领域后，保存的更改将在 管理中心下一次查询服务器时生效。

要执行用户感知，必须为任何一种领域支持的服务器配置一个领域。系统使用这些连接查询服务器上与 POP3 和 IMAP 用户关联的数据，并收集有关通过基于流量的检测发现的 LDAP 用户的数据。

系统使用 POP3 和 IMAP 登录中的邮件地址与 Active Directory 或 OpenLDAP 上的 LDAP 用户相关联。例如，如果受管设备检测到某个用户使用与某个 LDAP 用户相同的邮件地址登录 POP3，则系统会将 LDAP 用户的元数据与该用户关联。

要执行用户控制，可以配置以下任何项目：

- Active Directory服务器或 ISE/ISE-PIC 的领域或领域序列

注释 如果您计划配置 SGT ISE 属性条件而不是用户、组、领域、终端位置或终端配置文件条件；或者，如果您只使用自己的身份策略来过滤网络流量，则可自行决定是否配置 Microsoft AD 领域或领域序列。

- TS 代理的 Microsoft AD 服务器的领域或领域序列
- 对于强制网络门户，则为 LDAP 领域。

  LDAP 不支持领域序列。

关于用户同步

您可以配置领域或领域序列以便在 管理中心 和 LDAP 或 Microsoft AD 服务器之间建立连接，以检索检测到的某些用户的用户和用户组元数据：

- 由强制网络门户进行身份验证或由 ISE/ISE-PIC 报告的 LDAP 和 Microsoft AD 用户。这些元数据可用于用户感知和用户控制。
- 基于流量的检测功能检测到的 POP3 和 IMAP 用户登录（如果这些用户的邮箱地址与 LDAP 或 AD 用户相同）。这些元数据可用于用户感知。

管理中心获取关于每个用户的以下信息和元数据：

- LDAP 用户名
- 名字和姓氏
- 电子邮件地址
- 部门
- 电话号码

重要事项 要以尽可能低的延迟启用 管理中心 ，我们强烈建议您配置一个在地理位置上尽可能靠近 管理中心 的领域目录（即域控制器）。

例如，如果您的 管理中心 位于北美，请配置一个也位于北美的领域目录。

关于用户活动数据

用户活动数据存储在用户活动数据库，而用户身份数据存储在用户数据库。如果访问控制参数范围太宽泛，则 管理中心会获取尽可能多的用户的信息，并报告其无法在消息中心的“任务”选项卡页面中检索的用户数。

要选择性地限制托管设备监控用户感知数据的子网，您可以使用Cisco Secure Firewall Threat Defense命令参考中所述的 **configure identity-subnet-filter** 命令。

注释 即使您从存储库移除系统检测到的用户，管理中心也不会从其用户数据库中移除这些用户；您必须手动删除。但是，在 管理中心下次更新其授权用户列表时，LDAP 更改会反映在访问控制规则中。

领域和受信任的域

在 管理中心中配置 Microsoft Active Directory (AD) 领域 时，该领域与 Microsoft Active Directory 或 LDAP 域 关联。

一组相互信任的 Microsoft Active Directory (AD) 域通常被称为林。此信任关系可使域以不同方式访问彼此的资源。例如，在域 A 中定义的用户帐户可以标记为域 B 中所定义组的成员。

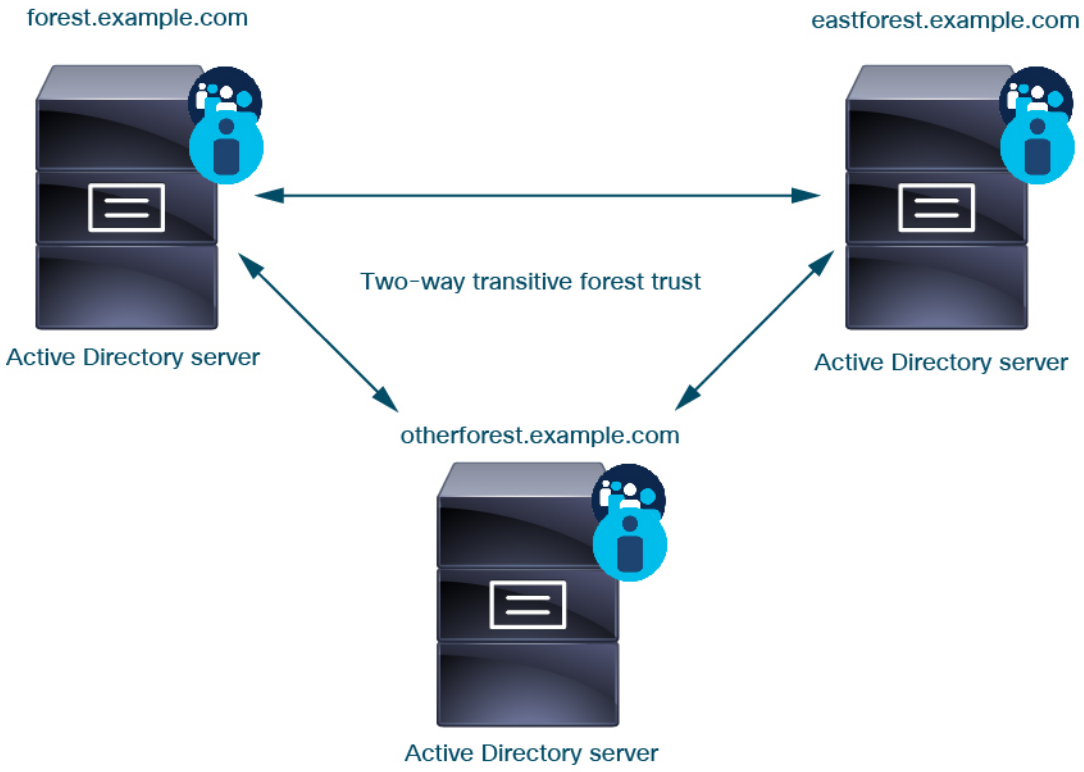
系统和受信任的域

系统支持在信任关系中配置的AD林。有几种类型的信任关系；本指南讨论双向传递森林信任关系。以下简单示例显示两个林： **forest.example.com** 和 **eastforest.example.com**。每个林中的用户和组可以通过另一个林中的 AD 进行身份验证，前提是您以这种方式配置了这些林。

如果您为每个域设置一个领域和每个域控制器一个目录的系统，则系统可以发现最多 100,000 个外部安全主体（用户和组）。如果这些外部安全主体与另一个领域中下载的用户匹配，则可以在访问控制策略中使用它们。

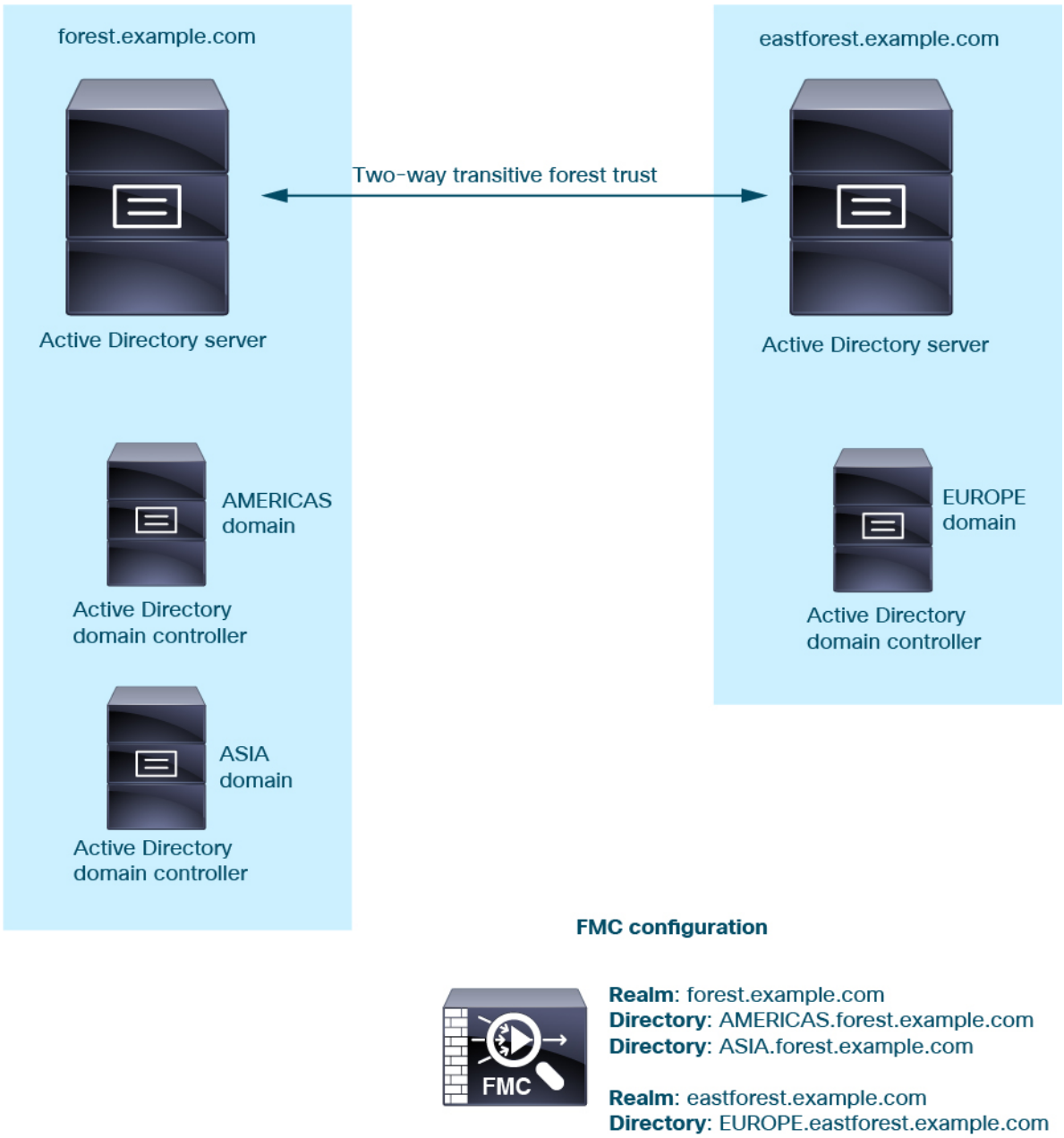
您无需为没有您希望在访问控制策略中使用的用户的任何域配置领域。

继续本示例，假设您有三个 AD 林（其中一个可以是子域或独立林），都设置为双向传递林关系，所有用户和组在所有三个林中以及系统。（如上例所示，必须将所有三个 AD 域设置为领域，并将所有域控制器配置为这些领域中的目录。）



最后，您可以将 管理中心 设置为能够在具有双向传递林信任的双林系统中对用户和组实施身份策略。假设每个林至少有一个域控制器，每个域控制器对不同的用户和组进行身份验证。要使 管理中心 能够在这些用户和组上实施身份策略，必须将每个包含相关用户的域设置为 管理中心 领域，并将每个域控制器设置为相应领域中的 管理中心 目录。

未能正确配置管理中心会阻止某些用户和组在策略中使用。在这种情况下，当您尝试同步用户和组时，您将看到警告。



使用前面的示例，设置 管理中心 如下：

- **forest.example.com** 中包含要使用访问控制策略控制的用户的任何域的领域
  - **AMERICAS.forest.example.com**领域中的目录
  - **ASIA.forest.example.com**领域中的目录
- **eastforest.example.com** 中包含要使用访问控制策略控制的用户的任何域的领域
  - **EUROPE.eastforest.example.com**领域中的目录

注释 管理中心 使用 AD 字段 **msDS-PrincipalName** 来解析引用，以查找每个域控制器中的用户名和组名。**msDS-PrincipalName** 返回 NetBIOS 名称。

领域支持的服务器

可以配置领域以连接到以下类型的服务器（如果这些服务可从 管理中心进行 TCP/IP 访问）：

服务器类型	支持 ISE/ISE-PIC 数据检索？	支持 TS 代理数据检索？	支持强制网络门户数据检索？
Windows 服务器 2012、2016 和 2019 上的 Microsoft Active Directory	是	是	是
Linux 上 的 OpenLDAP	不支持	不支持	是

不支持 将 Active Directory 全局目录服务器作为领域目录。有关全局目录服务器的详细信息，请参阅 learn.microsoft.com 上的 全局目录 。

注释 如果 TS 代理安装在与另一个被动身份验证身份源（ISE/ISE-PIC）共享的 Microsoft Active Directory Windows 服务i去上，则 管理中心 会划分 TS 代理数据的优先级。如果 TS 代理和一个被动身份源通过同一 IP 地址报告活动，则仅会将 TS 代理数据记录到 管理中心。

请注意以下与服务器组配置有关的事项：

- 要对用户组或组内用户执行用户控制，则必须在 LDAP 或 Active Directory 服务器上配置用户组。
- 组名称不能以 **s–** 开头，因为它由 LDAP 在内部使用。

  组名称和组织单位名称都不能包含特殊字符，如星号 (*)、等号 (=) 或反斜线 (\)；否则，这些组或组织单位中的用户不会被下载，也不会可用于身份策略。
- 要配置包含或排除作为服务器上某个子组成员的用户的 Active Directory 领域，请注意，Microsoft 建议在 Windows 服务器 2012 上，Active Directory 每组包含不超过 5000 个用户。有关详细信息，请参阅 MSDN 上的“Active Directory 的最大限制-可扩展性”。

  如果需要，可以修改 Active Directory 服务器配置以增加此默认限制并容纳更多用户。
- 要在您的远程桌面服务环境中唯一识别由服务器报告的用户，则必须配置 Cisco 终端服务 (TS) 代理。在安装并配置后，TS 代理将唯一端口分配给个人用户，因此系统可唯一识别这些用户。（Microsoft将 终端服务 名称更改为 远程桌面服务。）

有关 TS 代理的详细信息，请参阅《思科终端服务 *(TS)* 代理指南》。

支持的服务器对象类和属性名称

领域中的服务器必须使用下表中列出的属性名称，以使 管理中心能够检索服务器中的用户元数据。如果服务器中的属性名称不正确，管理中心将无法使用该属性中的信息来填充其数据库。

表 *203:* 属性名称与 *Cisco Secure Firewall Management Center* 字段的映射

元数据	管理中心属性	LDAP ObjectClass	Active Directory 属性	OpenLDAP 属性
LDAP 用户名	用户名	• 用户 • inetOrgPerson	samaccountname	cn uid
名字	名字		givenname	givenname
姓氏	姓氏		sn	sn
邮箱地址	电子邮件		mail Userprincipalname（如果 mail 没有值）	mail
department	部门		department distinguishedname（如果 department 没有值）	ou
telephone number	电话		telephonenumber	telephonenumber

注释 组的 LDAP ObjectClass 为 `group`、`groupOfNames`（`group-of-names` 适用于 Active Directory）或 `groupOfUniqueNames`。

有关 ObjectClasses 和属性的详细信息，请参阅以下参考资料：

- Microsoft Active Directory：
  - ObjectClasses：MSDN 上的所有类
  - 属性：MSDN 上的所有属性
- OpenLDAP：RFC 4512

领域的许可证要求

威胁防御 许可证

任意

经典许可证

控制

领域的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

创建代理序列

代理序列 是一个或多个可用于与 LDAP、 Active Directory 或 ISE / ISE-PIC 服务器通信的受管设备。仅当 思科防御协调器 （CDO）无法与 Active Directory 或 ISE / ISE-PIC 服务器通信时，才需要执行此操作。（例如， CDO 可能在公共云中，但 Active Directory 或 ISE / ISE-PIC 可能在私有云中。）

虽然您可以使用一台受管设备作为代理序列，但我们强烈建议您设置两台或更多设备，以便在受管设备无法与 Active Directory 或 ISE / ISE-PIC 通信时，另一台受管设备可以接管。

开始之前

您必须至少添加两个受管设备至 CDO，所有这些设备都必须能够与 Active Directory 或 ISE / ISE-PIC 通信。

过程

步骤 1 如果尚未登录，请登录 管理中心。

步骤 2 请点击 **集成** > **其他集成** > **领域** > **代理序列**。

步骤 3 点击 **添加代理序列**。

步骤 4 在 **名称** 字段中输入用于标识代理序列的名称。

步骤 5 （可选。）在**说明**字段中，输入代理序列的说明。

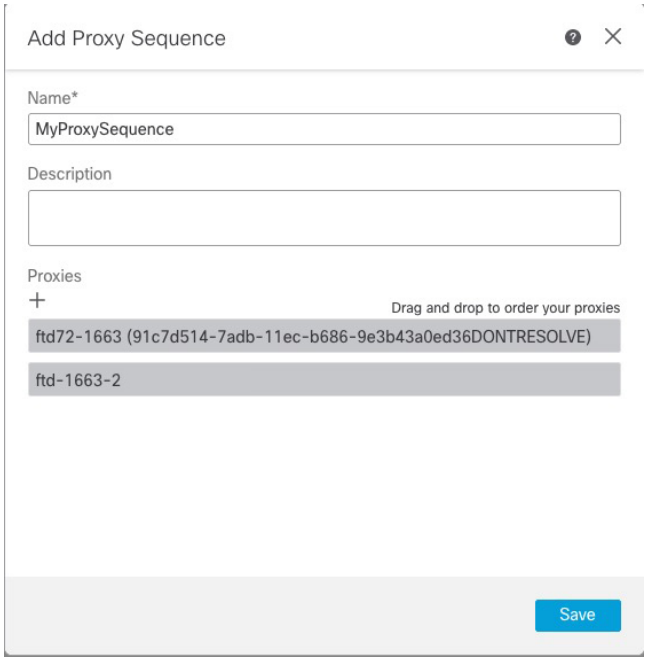
步骤 6 在代理下，点击 **添加**（+）。

步骤 7 点击每个受管设备的名称以添加到序列。

要缩小搜索范围，请在 **过滤器** 字段中输入全部或部分领域名称。

步骤 8 点击**确定**。

步骤 9 在添加代理序列对话框中，按要 CDO 来搜索的顺序拖放代理。
下图显示由两个代理组成的代理序列示例。顶部代理将在底部代理之前搜索用户。两个代理都必须能够与 Active Directory 或 ISE / ISE-PIC 进行通信。



步骤 10 点击**保存**。

下一步做什么

请参阅创建身份策略，第 1887 页。

创建 Active Directory 领域和领域目录

通过以下程序，您可以创建 领域 （ 管理中心 与 Active Directory 目录领域之间的连接）和 目录 （ 管理中心 与 LDAP 服务器或 Active Directory 域控制器之间的连接）。

（推荐。）要从 管理中心 安全连接到 Active Directory 服务器，请先执行以下任务：

- 导出 Active Directory 服务器的根证书， 第 1825 页
- 查找 Active Directory 服务器名称， 第 1825 页

Microsoft 已宣布 Active Directory 服务器将在 2020 年开始实施 LDAP 绑定和 LDAP 签名。Microsoft 将这些作为一项要求，因为在使用默认设置时，Microsoft Windows 中存在一个权限提升漏洞，该漏洞可能允许中间人攻击者将身份验证请求成功转发到 Windows LDAP 服务器。有关详细信息，请参阅 Microsoft 支持站点上的 Windows 2020 LDAP 通道绑定和 LDAP 签名要求 。

有关领域目录配置字段的详细信息，请参阅 领域字段， 第 1818 页 和 领域目录和 同步 字段， 第 1822 页。

配置 管理中心 的跨域信任：设置， 第 1829 页中显示了使用跨域信任设置领域的分步示例。

不支持 将 Active Directory 全局目录服务器作为领域目录。有关全局目录服务器的详细信息，请参阅 learn.microsoft.com 上的 全局目录 。

注释 您必须为每个 Microsoft Active Directory (AD) 领域都指定一个唯一的 **AD 主域**。虽然系统允许对不同 Microsoft AD 领域指定相同的 **AD 主域**，但系统将无法正常运行。发生这种情况，是因为系统会向每个领域的每个用户和每个组都分配一个唯一 ID，因此系统无法明确识别任何特定用户或组。由于系统无法正确识别用户和组，因此会阻止您对多个领域指定相同的 **AD 主域**。发生这种情况，是因为系统会向每个领域的每个用户和每个组都分配一个唯一 ID，因此系统无法明确识别任何特定用户或组。

开始之前

如果您对强制网络门户使用 Kerberos 身份验证，请在开始之前参阅以下部分：Kerberos 身份验证的必备条件， 第 1818 页。

如果使用 思科防御协调器（CDO）管理设备，请首先创建代理序列，如 创建代理序列，第 1814 页中所述

重要事项 要以尽可能低的延迟启用 管理中心，我们强烈建议您配置一个在地理位置上尽可能靠近 管理中心 的领域目录（即域控制器）。

例如，如果您的 管理中心 位于北美，请配置一个也位于北美的领域目录。

过程

步骤 1 登录Cisco Secure Firewall Management Center。

步骤 2 请点击 **集成** > **其他集成** > **领域**。

步骤 3 要创建新的领域，请点击 **添加领域**。

步骤 4 要执行其他任务（如启用、禁用或删除领域），请参阅管理领域，第 1836 页。

步骤 5 按照领域字段，第 1818 页中的描述输入领域信息。

步骤 6 （可选。）从 **代理** 列表中，点击受管设备或代理序列以与 ISE / ISE-PIC 通信（如果 CDO 无法执行此操作）。例如，您的 CDO 可能在公共云中，但 ISE / ISE-PIC 服务器可能在内部内联网上。

步骤 7 在目录服务器配置部分中，输入目录信息，如 领域目录和 同步 字段，第 1822 页中所述。

步骤 8 （可选。）要为此领域配置其他域，请点击 **添加其他目录**。

步骤 9 点击 **配置组和用户**。
输入以下信息：

信息	说明
AD 主域 (AD Primary Domain)	用于需要对用户进行身份验证的 Active Directory 服务器的域。有关其他信息，请参阅领域字段，第 1818 页。
基本 DN (Base DN)	Cisco Secure Firewall Management Center应在其上开始搜索用户数据的服务器上的目录树。
组 DN (Group DN)	Cisco Secure Firewall Management Center 应在其上开始搜索组数据的服务器上的目录树。
代理	从列表中，点击一个或多个受管设备或代理序列。这些设备必须能够与 Active Directory 或 ISE / ISE-PIC 通信，以检索身份策略的用户数据。
加载组	点击以从 Active Directory 服务器加载组。如果未显示组，请在 **AD 主域**、**基本DN**、 和 **组 DN** 字段中输入或编辑信息，然后点击 **加载组**。 有关这些字段的信息，请参阅领域字段，第 1818 页。
可用组部分	通过将组移动到 **包含的组和用户** 或 **排除的组和用户** 列表中，限制要在策略中使用的组。 例如，将一个组移动到 **包含的组和用户** 列表中，仅允许在策略中使用该组。 **排除的组和用户** 中的组及其包含的用户将被排除在用户感知和控制之外。所有其他组和用户 均为 可用。 有关详细信息，请参阅领域目录和 同步 字段，第 1822 页。

步骤 10 点击**领域配置**选项卡。

步骤 11 输入 **组属性**，然后（如果您对强制网络门户使用 Kerberos 身份验证）输入 **AD 加入用户名** 和 **AD 加入密码**。有关详细信息，请参阅领域目录和 同步 字段，第 1822 页。

步骤 12 如果使用 Kerberos 身份验证，请点击 **测试**。如果测试失败，请等待片刻，然后重试。

步骤 13 输入用户会话超时值，以分钟为单位，为 **ISE/ISE-PIC 用户**、**终端服务器代理用户**、**强制网络门户用户**、**出现故障的强制网络门户用户**、和 **访客强制网络门户用户**。

步骤 14 完成配置领域后，点击 **保存 (Save)**。

下一步做什么

- 配置 管理中心 的跨域信任：设置，第 1829 页
- 同步用户和组，第 1827 页
- 编辑、删除、启用或禁用领域；请参阅管理领域，第 1836 页。
- 比较领域，第 1837 页。
- 或者，监控任务状态；请参阅 《Cisco Secure Firewall Management Center 管理指南》中的 查看任务消息 。

Kerberos 身份验证的必备条件

如果使用 Kerberos 对强制网络门户用户进行身份验证，请记住以下几点。

主机名字符限制

如果使用 Kerberos 身份验证，则受管设备的主机名必须少于 15 个字符（这是 Windows 设置的 NetBIOS 限制）；否则，强制网络门户身份验证失败。您在设置设备时设置受管设备主机名。有关详细信息，请参阅 Microsoft 文档网站上的此类文章： Active Directory 中计算机、域、站点和 OU 的命名约定。

DNS 响应字符数限制

DNS 必须向主机名返回 64KB 或更少的响应；否则，测试连接 AD 连接失败。此限制在两个方向上都适用，将在 RFC 6891 第 6.2.5 节中讨论。

领域字段

以下字段用于配置领域。

领域配置字段

这些设置适用于领域中的所有 Active Directory 服务器或域控制器（也称为目录）。

名称

领域的唯一名称。

- 要在身份策略中使用领域，系统需支持字母数字和特殊字符。

- 要在 RA-VPN 配置中使用领域，系统需支持字母数字、连字符 (-)、下划线 (_) 和加号 (+) 字符。

说明

（可选。）输入领域的描述。

类型 (Type)

领域类型， **AD** 表示 Microsoft Active 目录， **LDAP** 表示其他支持的 LDAP 存储库，或 **本地**。有关支持的LDAP存储库的列表，请参阅领域支持的服务器，第 1812 页。您可以使用LDAP存储库对强制网络门户用户进行身份验证；所有其他都需要 Active Directory。

注释 仅强制网络门户支持 LDAP 领域。

领域类型 **LOCAL** 用于配置本地用户设置。LOCAL 领域用于远程访问用户身份验证。

为 LOCAL 领域添加以下本地用户信息：

- **用户名**-用户的名称。
- **密码**-本地用户密码。
- **确认密码**-确认本地用户密码。

注释 **点击添加其他本地用户** 以将更多用户添加到 LOCAL 领域。

您可以在创建领域并为本地用户更新密码后添加更多用户。您还可以创建多个 LOCAL 领域，但不能将其禁用。

AD 主域 (AD Primary Domain)

仅用于 Microsoft Active Directory 领域。用于需要对用户进行身份验证的 Active Directory 服务器的域。

注释 您必须为每个 Microsoft Active Directory (AD) 领域都指定一个唯一的 **AD 主域**。虽然系统允许对不同 Microsoft AD 领域指定相同的 **AD 主域**，但系统将无法正常运行。发生这种情况，是因为系统会向每个领域的每个用户和每个组都分配一个唯一 ID，因此系统无法明确识别任何特定用户或组。由于系统无法正确识别用户和组，因此会阻止您对多个领域指定相同的 **AD 主域**。发生这种情况，是因为系统会向每个领域的每个用户和每个组都分配一个唯一 ID，因此系统无法明确识别任何特定用户或组。

AD 加入用户名和 AD 加入密码 (AD Join Username and AD Join Password)

（在编辑领域时，在 **领域配置** 选项卡页面上可用。）

用于专为 Kerberos 强制网络门户主动身份验证设计的 Microsoft Active Directory 领域，表示具有可在 Active Directory 域中创建域计算机帐户的适当权限的任何 Active Directory 用户的标识用户名和密码。

记住以下几点：

- DNS 必须能够将域名解析为 Active Directory 域控制器的 IP 地址。
- 指定的用户必须能够将计算机加入到 Active Directory 域。
- 用户名必须是完全限定的（例如，**administrator@mydomain.com**，而不是 **administrator**）。

如果选择 **Kerberos**（或 **HTTP 协商**，如果希望 Kerberos 作为选项）作为身份规则中的**身份验证协议**，则必须为您所选的 **领域** 配置 **AD 加入用户名** 和 **AD 加入密码**，才能执行 Kerberos 强制网络门户主动身份验证。

注释 SHA-1 散列算法无法在 Active Directory 服务器上存储密码，因此不应使用。有关详细信息，请参阅参考，例如 Microsoft TechNet 上的将证书颁发机构散列算法从 SHA1 迁移到 SHA2 或 Open Web 应用安全项目网站上的 密码存储备忘单 。

我们建议使用 SHA-256 与 Active Directory 通信。

目录用户名和目录密码 (Directory Username and Directory Password)

为具有检索用户信息的相应权限的用户提供的标识用户名和密码。

请注意以下提示：

- 对于某些版本的 Microsoft Active Directory，可能需要特定权限才能读取用户和组。有关详细信息，请参阅 Microsoft Active Directory 提供的文档。
- 对于 OpenLDAP，用户的访问权限由 OpenLDAP 规范第 8 部分中讨论的 `<level>` 参数确定。用户的 `<level>` 应为 `auth` 或更高。
- 用户名必须是完全限定的（例如，**administrator@mydomain.com**，而不是 **administrator**）。

注释 SHA-1 散列算法无法在 Active Directory 服务器上存储密码，因此不应使用。有关详细信息，请参阅参考，例如 Microsoft TechNet 上的将证书颁发机构散列算法从 SHA1 迁移到 SHA2 或 Open Web 应用安全项目网站上的 密码存储备忘单 。

我们建议使用 SHA-256 与 Active Directory 通信。

基本 DN

（可选。）Cisco Secure Firewall Management Center应在其上开始搜索用户数据的服务器上的目录树。如果未指定 **基本 DN**，则系统会检索可连接到服务器的顶级 DN。

通常，基本可分辨名称 (DN) 具有指示公司域名和运营单位的基础结构。例如，Example 公司的 Security 部门的基础 DN 可能为 **ou=security,dc=example,dc=com**。

组 DN (Group DN)

（可选。）Cisco Secure Firewall Management Center应在其上搜索具有组属性的用户的服务器上的目录树。支持的组属性的列表在支持的服务器对象类和属性名称，第 1813 页中显示。如果未指定 **组 DN**，则系统会检索可连接到服务器的顶级DN。

注释 以下是系统在您的目录服务器中的用户、组和 DN 中 支持 的字符列表。使用除以下字符以外的任何字符可能会导致系统无法下载用户和组。

实体	支持的字符
用户名	**a-z A-Z 0-9 ! # $ % ^ & ( ) _ - { } ' . ~ `**
组名称	**a-z A-Z 0-9 ! # $ % ^ & ( ) _ - { } ' . ~ `**
基础 DN 和组 DN	**a-z A-Z 0-9 ! @ $ % ^ & * ( ) _ - . ~ `**

用户名中的任何位置均不支持空格，包括末尾。

代理

从列表中，点击一个或多个受管设备或代理序列。这些设备必须能够与 Active Directory 或 ISE / ISE-PIC 通信，以检索身份策略的用户数据。

编辑现有领域时，以下字段可用。

用户会话超时

（在编辑领域时，在 **领域配置** 选项卡页面上可用。）

输入用户会话超时前持续的分钟数。在用户登录事件后，默认值为 1440（24 小时）。超时后，用户的会话结束。如果用户继续访问网络，而不再次登录，则 管理中心 会将该用户视为未知（**失败的强制网络门户用户**除外）。

您可以为以下内容设置超时值：

- **用户代理和 ISE/ISE-PIC 用户**：由用户代理或 ISE/ISE-PIC（被动身份验证类型）跟踪的用户的超时。

  您指定的超时值 不 适用于 pxGrid SXP 会话主题订用（例如，目标 SGT 映射）。相反，只要没有来自 ISE 的给定映射的删除或更新消息，会话主题映射就会保留。

  有关 ISE / ISE-PIC 的详细信息，请参阅ISE/ISE-PIC 身份源，第 1845 页。

- **终端服务代理用户**：由 TS 代理（一种被动身份验证类型）跟踪的用户的超时。有关详细信息，请参阅终端服务 (TS) 代理身份源，第 1883 页。

- **强制网络门户用户**：使用强制网络门户（一种主动身份验证类型）成功登录的用户的超时。有关详细信息，请参阅强制网络门户身份源，第 1863 页。

- **失败的强制网络门户用户**：未使用强制网络门户成功登录的用户的超时。您可以配置 管理中心 将用户视为身份验证失败的用户之前的 **最大登录尝试次数** 。可以选择使用访问控制策略为身份验证失败的用户授予对网络的访问权限，如果是这样，此超时值将应用于这些用户。

  有关失败的强制网络门户登录的详细信息，请参阅强制网络门户字段 ， 第 1875 页。

- **访客强制网络门户用户**：以访客用户身份登录到强制网络门户的用户的超时。有关详细信息，请参阅强制网络门户身份源 ， 第 1863 页。

领域目录和 同步 字段

领域目录字段

这些设置适用于领域中的各个服务器（例如 Active Directory 域控制器）。

主机名/IP 地址

Active Directory 域控制器计算机的完全限定主机名。要查找完全限定名称，请参阅 查找 Active Directory 服务器名称 ， 第 1825 页。

如果您使用 Kerberos 对强制网络门户进行身份验证，还请确保您了解以下内容：

如果使用 Kerberos 身份验证，则受管设备的主机名必须少于 15 个字符（这是 Windows 设置的 NetBIOS 限制）；否则，强制网络门户身份验证失败。您在设置设备时设置受管设备主机名。有关详细信息，请参阅 Microsoft 文档网站上的此类文章： Active Directory 中计算机、域、站点和 OU 的命名约定。

DNS 必须向主机名返回 64KB 或更少的响应；否则，测试连接 AD 连接失败。此限制在两个方向上都适用，将在 RFC 6891 第 6.2.5 节中讨论。

端口 (Port)

服务器的端口。

加密

（强烈建议。）要使用的加密方法：

- **STARTTLS** - 加密的 LDAP 连接
- **LDAPS** - 加密的 LDAP 连接
- 无 **(None)** - 未加密的 LDAP 连接（不安全的流量）

要与 Active Directory 服务器安全通信，请参阅 安全地连接到 Active Directory ， 第 1824 页。

CA 证书

用于对服务器进行身份验证的 TLS/SSL 证书。必须配置 **STARTTLS** 或 **LDAPS** 作为 **加密** 类型才能使用 TLS/SSL 证书。

如果使用证书进行身份验证，则证书中的服务器名称必须与服务器**主机名/IP 地址 (Hostname / IP Address)** 匹配。例如，如果将 10.10.10.250 作为 IP 地址，而不是证书中的 **computer1.example.com**，连接会失败。

用于连接目录服务器的接口

点击以下选项之一：

- **通过路由查找进行解析**：使用路由连接到 Active Directory 服务器。
- **选择接口 (Choose an interface)**：选择要连接到 Active Directory 服务器的特定托管接口。

用户 同步 字段

AD 主域 (AD Primary Domain)

仅用于 Microsoft Active Directory 领域。用于需要对用户进行身份验证的 Active Directory 服务器的域。

注释 您必须为每个 Microsoft Active Directory (AD) 领域都指定一个唯一的 **AD 主域**。虽然系统允许对不同 Microsoft AD 领域指定相同的 **AD 主域**，但系统将无法正常运行。发生这种情况，是因为系统会向每个领域的每个用户和每个组都分配一个唯一 ID，因此系统无法明确识别任何特定用户或组。由于系统无法正确识别用户和组，因此会阻止您对多个领域指定相同的 **AD 主域**。发生这种情况，是因为系统会向每个领域的每个用户和每个组都分配一个唯一 ID，因此系统无法明确识别任何特定用户或组。

输入查询以查找用户和组

基本 DN：

（可选。）管理中心应在其上开始搜索用户数据的服务器上的目录树。

通常，基本可分辨名称 (DN) 具有指示公司域名和运营单位的基础结构。例如，Example 公司的 Security 部门的基础 DN 可能为 **ou=security,dc=example,dc=com**。

组 DN：

（可选。）管理中心应在其上搜索具有组属性的用户的服务器上的目录树。支持的组属性的列表在支持的服务器对象类和属性名称，第 1813 页中显示。

注释 组名和组织单位名称都不能包含特殊字符，如星号 (*)、等号 (=) 和后斜线 (\)，因为这些组中的用户不会被下载，也不能用于身份策略。

加载组

让您能够下载要用于用户感知和用户控制的用户和组。

可用组 (Available Groups)、添加以包含 (Add to Include)、添加以排除 (Add to Exclude)

限制可在策略中使用的组。

- 除非将组移至 **包含的组和用户** 或 **排除的组或用户** 字段，否则 **可用组** 字段中显示的组可用于策略。
- 如果您将组移动到 **包含的组和用户** 字段中，只有那些所包含的组和用户被下载，用户数据可用于用户感知和用户控制。
- 如果您将组移动到 **排除的组和用户** 字段中，他们所包含的所有组和用户， 除了 这些被下载并可用于用户认知和用户控制。
- 若要包括来自未包括的组的用户，请在 **用户入侵** 下面的字段中输入用户名，然后点击 **添加**。
- 若要包括来自未包括的组的用户，请在 **用户入侵** 下面的字段中输入用户名，然后点击 **添加**。

注释 使用公式 **R = I - (E+e) + i**计算下载到 管理中心 的用户，其中：

- R 是已下载用户的列表
- I 是包含的组
- E 是排除的组
- e 是排除的用户
- i 是包含的用户

立即同步
点击以将组和用户与 AD 同步。

开始自动 同步 ， 在
输入从 AD下载用户和组的时间和时间间隔。

安全地连接到 Active Directory

要在 Active Directory 服务器和 管理中心 （我们强烈建议）之间创建安全连接，您必须执行以下所有任务：

- 导出 Active Directory 服务器的根证书。
- 将根证书导入 管理中心 作为受信任 CA 证书。
- 查找 Active Directory 服务器的完全限定名称。
- 创建领域目录。

有关详细信息，请参阅以下任务之一。

相关主题

导出 Active Directory 服务器的根证书 ， 第 1825 页

查找 Active Directory 服务器名称，第 1825 页
创建 Active Directory 领域和领域目录，第 1816 页

查找 Active Directory 服务器名称

要在 管理中心中配置领域目录，您必须知道完全限定服务器名称，您可以在后续程序中找到该名称。

开始之前

您必须以具有足够权限查看计算机名称的用户身份登录 Active Directory 服务器。

过程

步骤 1 登录 Active Directory 服务器

步骤 2 点击**开始 (Start)**。

步骤 3 右键点击 **此 PC (This PC)**。

步骤 4 点击**属性**。

步骤 5 点击**高级系统设置 (Advanced System Settings)**。

步骤 6 点击 **计算机名称** 选项卡。

步骤 7 注意 **完整计算机名称**的值。
在 FMC 中配置领域目录时，必须输入此确切名称。

下一步做什么

创建 Active Directory 领域和领域目录，第 1816 页。

相关主题

导出 Active Directory 服务器的根证书，第 1825 页

导出 Active Directory 服务器的根证书

接下来的任务讨论如何导出 Active Directory 服务器的根证书，这是安全连接到 管理中心 以获取用户身份信息所必需的。

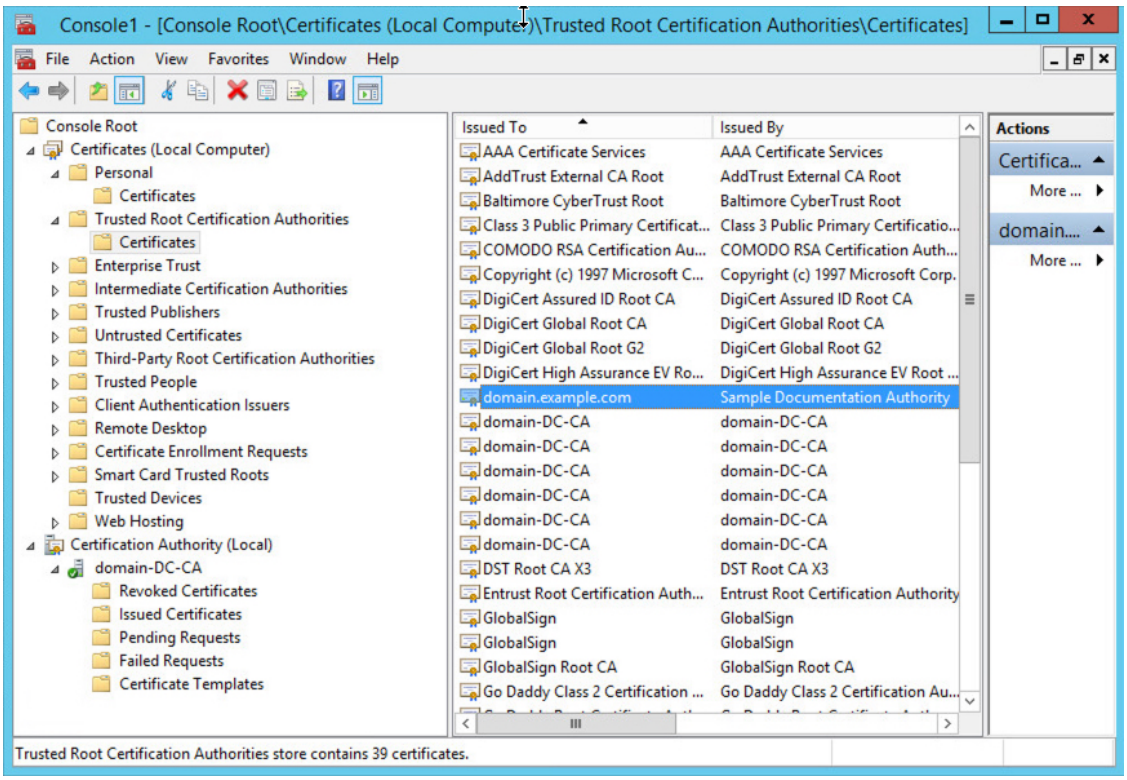
开始之前

您必须知道 Active Directory 服务器的根证书的名称。根证书的名称可能与域的名称相同，或者证书的名称可能不同。后面的程序显示了查找名称的一种方法；可能还有其他方式。

过程

步骤 1 以下是查找 Active Directory 服务器根证书名称的一种方法；有关详细信息，请参阅 Microsoft 文档：

a) 以具有运行 Microsoft 管理控制台权限的用户身份登录 Active Directory 服务器。
b) 点击 **开始** 并输入 **mmc**。
c) 点击 **文件** > **添加/删除 Snap-in**
d) 从左侧窗格的可用管理单元列表中，点击 **证书（本地）**。
e) 点击**添加 (Add)**。
f) 在证书管理单元对话框中，点击 **计算机帐户** 然后点击 **下一步**。
g) 在“选择计算机”对话框中，点击 **本地计算机** 然后点击 **完成**。
h) 仅限 *Windows Server 2012*。重复上述步骤以添加证书颁发机构管理单元。
i) 点击 **控制台根** > **受信任证书颁发机构** > **证书**。
服务器的受信任证书显示在右侧窗格中。下图只是 Windows Server 2012 的示例；您的产品可能看起来有所不同。



步骤 2 使用 **certutil** 命令导出证书。

这只是导出证书的一种方式。这是导出证书的便捷方式，尤其是在您可以运行Web浏览器并从Active Directory 服务器连接到 管理中心 的情况下。

a) 点击 **开始** 并输入 **cmd**。
b) 输入命令 **certutil -ca.cert** 证书-名称。
服务器的证书显示在屏幕上。
c) 将整个证书复制到剪贴板，以 **-----BEGIN CERTIFICATE-----** 开头和以 **-----END CERTIFICATE-----** 结尾（包括这些字符串）。

下一步做什么

将 Active Directory 服务器的证书作为受信任 CA 证书导入 管理中心，如 添加受信任 CA 对象，第 1006 页中所述。

相关主题

查找 Active Directory 服务器名称，第 1825 页

同步用户和组

同步 用户和组意味着 管理中心 查询您为组和这些组中的用户配置的领域和目录。所有用户都可以在身份策略中使用 管理中心 查找。

如果发现问题，您很可能需要添加包含管理中心无法加载的用户和组的领域。有关详细信息，请参阅领域和受信任的域，第 1809 页。

开始之前

为每个 Active Directory 域创建一个 管理中心 领域，并为每个林中的每个 Active 导向器域控制器创建一个 管理中心 目录。请参阅创建 Active Directory 领域和领域目录，第 1816 页。

必须仅为具有要在用户控制中使用的用户的域创建领域。

过程

步骤 1 如果尚未登录，请登录 管理中心。

步骤 2 请点击 **集成** > **其他集成** > **领域**。

步骤 3 点击每个领域旁边的 **下载**（）。

步骤 4 要查看结果，请点击 **同步结果** 选项卡。

“领域”列指示 Active Directory 林中的用户和组同步是否存在问题。查找每个领域旁边的以下指示器。

领域中的指示器列	含义
（无）	所有用户和组同步无错误。无需任何操作。
黄色三角形（）	同步用户和组时出现问题。确保为每个 Active Directory 域添加了一个领域，并为每个 Active Directory 域控制器添加了一个目录。 有关详细信息，请参阅 排除跨域信任故障，第 1841 页。

创建领域序列

通过以下程序，您可以创建领域序列，这是系统在应用身份策略时搜索的领域的有序列表。将领域序列添加到身份规则的方式与添加领域的方式完全相同；区别在于系统在应用身份策略时按领域序列中指定的顺序搜索所有领域。

开始之前

您必须创建并启用至少两个领域，每个领域对应于与 Active Directory 服务器的连接。您无法为 LDAP 领域创建领域序列。

按创建 Active Directory 领域和领域目录，第 1816 页中所述创建领域。

过程

步骤 1 如果尚未登录，请登录 管理中心。

步骤 2 请点击 **集成** > **其他集成** > **领域** > **领域序列**。

步骤 3 点击**添加序列 (Add Sequence)**。

步骤 4 在 **名称** 字段中，输入用于标识领域序列的名称。

步骤 5 （可选。）在 **说明**字段中，输入领域序列的说明。

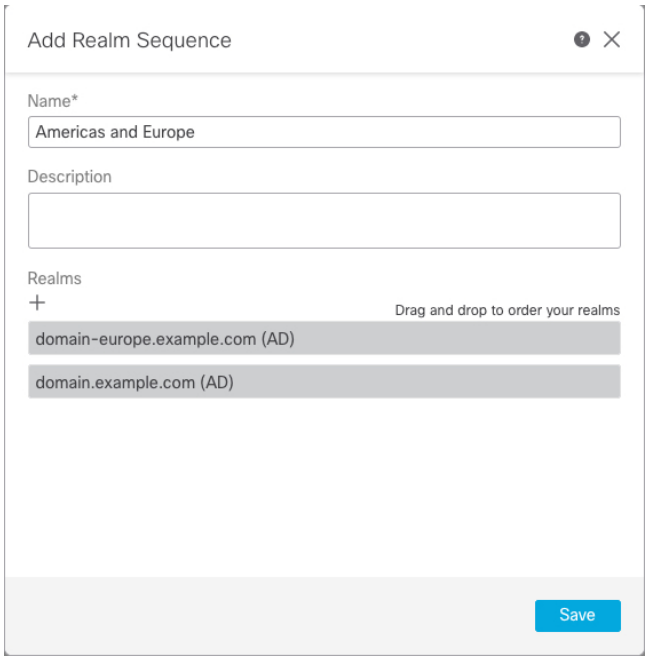
步骤 6 在领域下，点击 **添加**（+）。

步骤 7 点击每个领域的名称以添加到序列。

要缩小搜索范围，请在 **过滤器** 字段中输入全部或部分领域名称。

步骤 8 点击**确定**。

步骤 9 在添加领域序列对话框中，按照您希望系统搜索这些领域的顺序拖放领域。
下图显示由两个领域组成的领域序列的示例。 **domain-europe.example.com** 领域将用于搜索 **domain.example.com** 领域前的用户。



步骤 10 点击保存。

下一步做什么

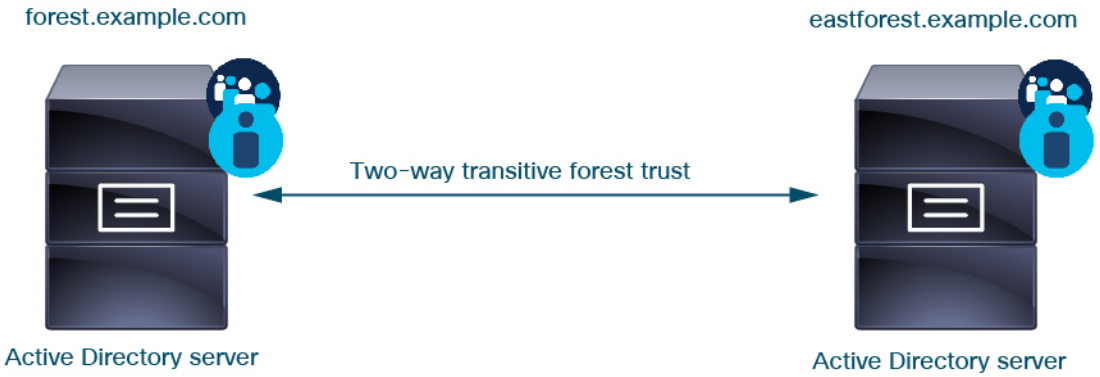
请参阅创建身份策略，第 1887 页。

配置 管理中心 的跨域信任：设置

这是对几个主题的介绍，这些主题将引导您配置 管理中心 使用跨域信任的两个领域。

此分步示例涉及两个林： **forest.example.com** 和 **eastforest.example.com**。配置目录林，以便每个目录林中的某些用户和组可以由另一个目录林中的 Microsoft AD 进行身份验证。

以下是本示例中使用的示例设置。



使用前面的示例，您可以按如下所示设置 管理中心 ：

- **forest.example.com** 中包含要使用访问控制策略控制的用户的任何域的领域和目录
- **eastforest.example.com** 中包含要使用访问控制策略控制的用户的任何域的领域和目录

示例中的每个领域都有一个域控制器，在 管理中心 中配置为目录。本示例中的目录配置如下：

- **forest.example.com**
  - 用户的基本可分辨名称 (DN)： **ou=UsersWest,dc=forest,dc=example,dc=com**
  - 组的基本 DN： **ou=EngineringWest,dc=forest,dc=example,dc=com**
- **eastforest.example.com**
  - 用户的基本 DN： **ou=EastUsers,dc=eastforest,dc=example,dc=com**
  - 组的基本 DN： **ou=EastEngineering,dc=eastforest,dc=example,dc=com**

相关主题

为 Cisco Secure Firewall Management Center 配置跨域信任步骤 1：配置领域和目录 ，第 1830 页

为 Cisco Secure Firewall Management Center 配置跨域信任步骤 1：配置领域和目录

这是分步程序中的第一个任务，解释如何配置 管理中心 来识别在跨域信任关系中配置的 Active Directory 服务器，这是企业组织越来越常见的配置。有关此样本配置的概述，请参阅配置管理中心的跨域信任：设置 ，第 1829 页。

如果您为每个域设置一个领域和每个域控制器一个目录的系统，则系统可以发现最多 100,000 个外部安全主体（用户和组）。如果这些外部安全主体与另一个领域中下载的用户匹配，则可以在访问控制策略中使用它们。

开始之前

您必须在跨域信任关系中配置 Microsoft Active Directory 服务器；有关详细信息，请参阅领域和受信任的域 ， 第 1809 页 。

如果使用 LDAP 对用户进行身份验证，则无法使用此程序。

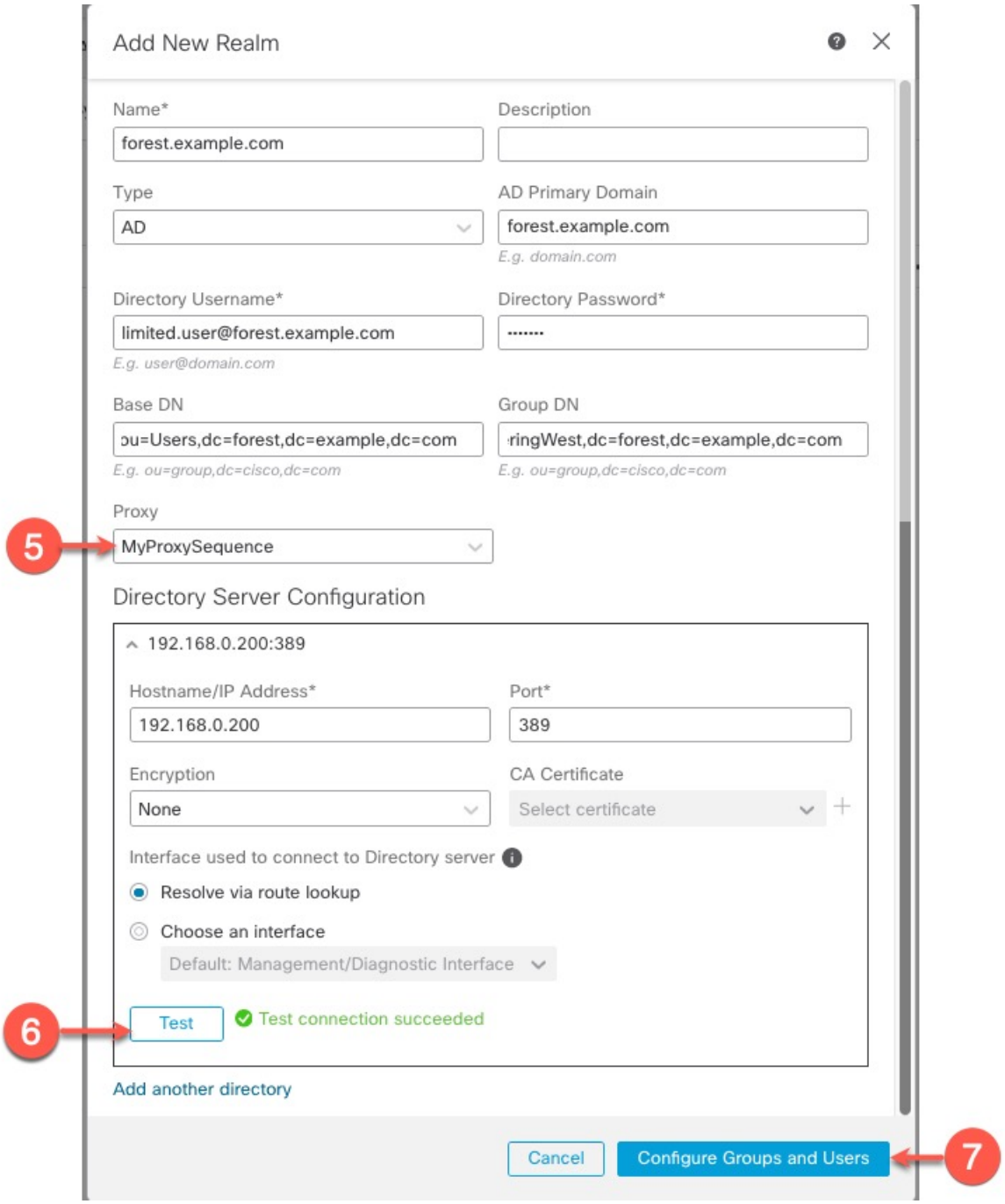
过程

步骤 1 登录管理中心。

步骤 2 请点击 **集成** > **其他集成** > **领域**。

步骤 3 点击**添加领域 (Add Realm)**。

步骤 4 要配置 **forest.example.com**，请输入以下信息。



注释 **目录用户名** 可以是 Active Directory 域中的任何用户；无需特殊权限。

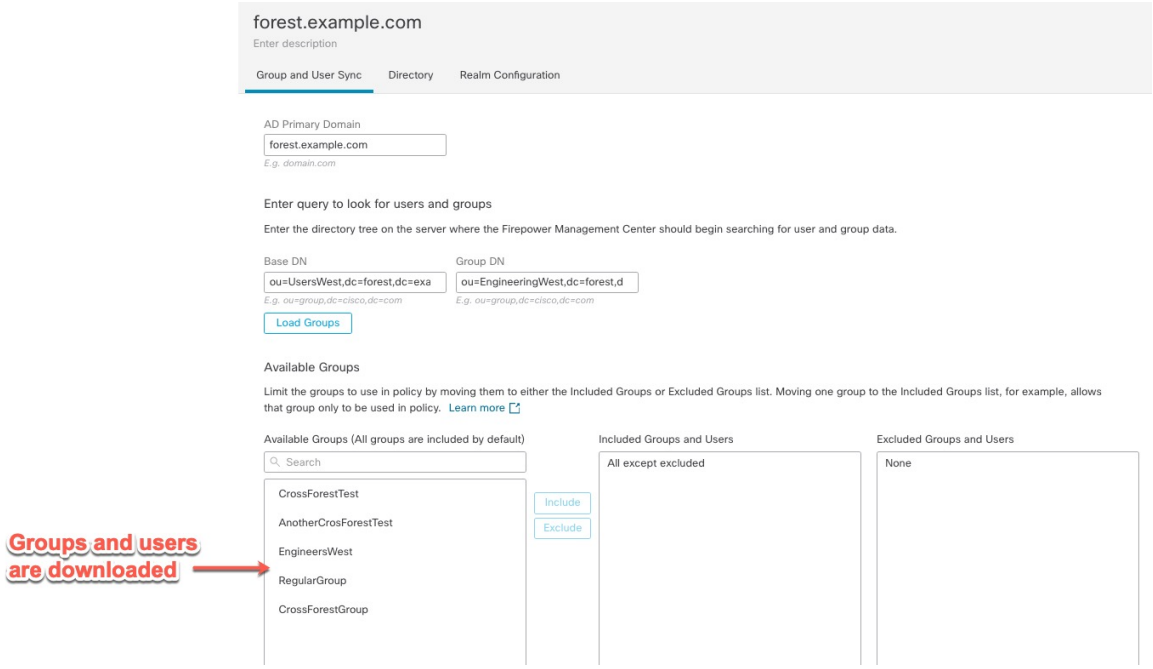
用于连接到目录服务器的接口 可以是可以连接到 Active Directory 服务器的任何接口。

步骤 5 **代理** 是可选的受管设备或代理序列，用于在 CDO 无法执行时与 ISE / ISE-PIC 通信。例如，您的 CDO 可能在公共云中，但 ISE / ISE-PIC 服务器可能在内部内联网上。

步骤 6 点击**测试 (Test)** 并确保测试成功后再继续。

步骤 7 点击 **配置组和用户**。

步骤 8 如果配置成功，则会显示下一页，如下所示。



注释 如果未下载组和用户，请验证 **基本 DN** 和 **组 DN** 字段中的值，然后点击 **加载组**。

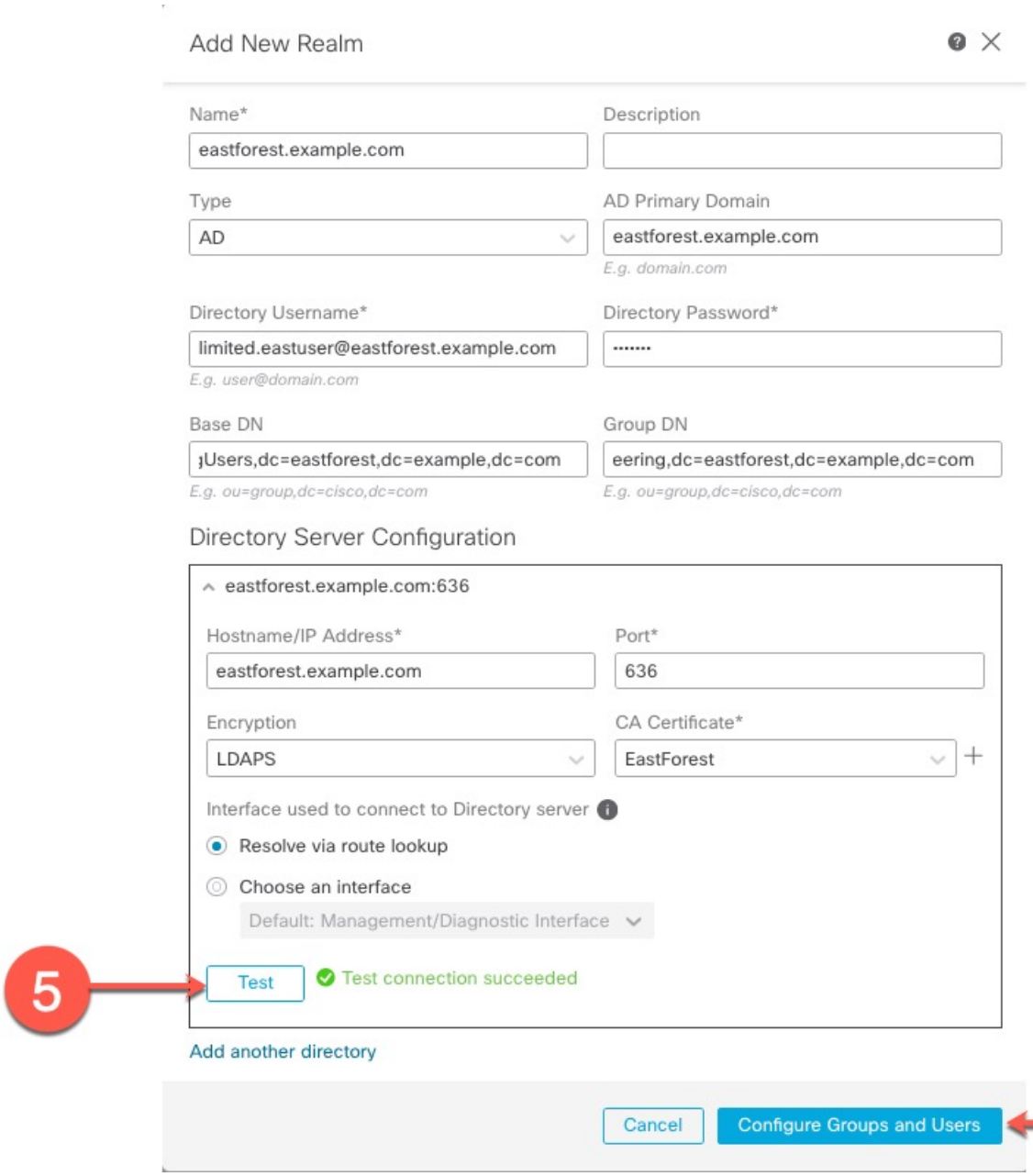
此页面上还有其他可选配置；有关它们的详细信息，请参阅 领域字段，第 1818 页 和 领域目录和 同步 字段，第 1822 页。

步骤 9 如果在此页面或选项卡页面上进行了更改，请点击 **保存**。

步骤 10 请点击 **集成** > **其他集成** > **领域**。

步骤 11 点击**添加领域 (Add Realm)**。

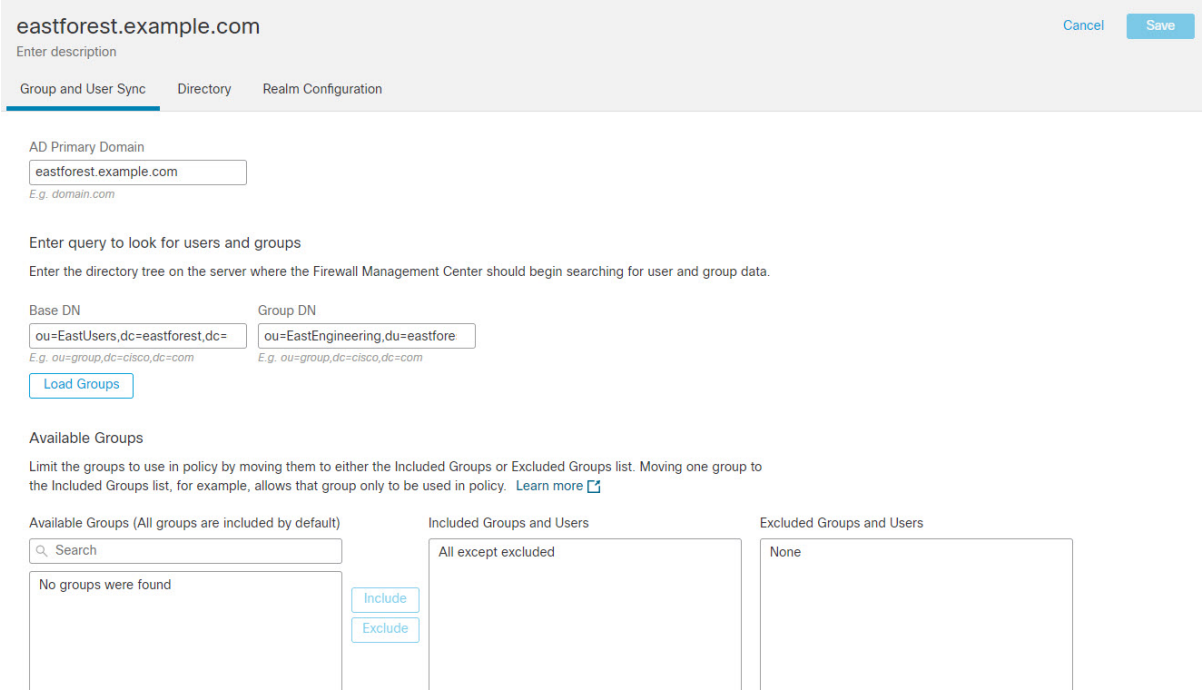
步骤 12 要配置 **eastforest.example.com**，请输入以下信息。



步骤 13 点击**测试 (Test)** 并确保测试成功后再继续。

步骤 14 点击 **配置组和用户**。

步骤 15 如果配置成功，则会显示下一页，如下所示。



相关主题

为跨域信任配置配置 管理中心 步骤 2：同步用户和组，第 1834 页

为跨域信任配置配置 管理中心 步骤 2：同步用户和组

配置两个或多个具有跨域信任关系的 Active Directory 服务器后，必须下载用户和组。该过程会暴露 Active Directory 配置的可能问题（例如，为一个 Active Directory 域而不是为另一个 Active Directory 域下载的组或用户）。

开始之前

确保您已执行 为 Cisco Secure Firewall Management Center 配置跨域信任步骤 1：配置领域和目录，第 1830 页中讨论的任务。

过程

步骤 1 登录管理中心。

步骤 2 请点击 **集成** > **其他集成** > **领域**。

步骤 3 在跨域信任中任何领域行的末尾，点击 （立即下载），然后点击 **是**。

步骤 4 点击 **复选标记**（） （通知） > **任务**。

如果组和用户下载失败，请重试。如果后续尝试失败，请查看您的领域和目录设置，如 领域字段，第 1818 页 和 领域目录和 同步 字段，第 1822 页中所述。

如果您使用的是代理或代理序列，请确保所有受管设备都可以与 Active Directory 或 ISE / ISE-PIC 通信。如果多个受管设备可以与 ISE / ISE-PIC 通信，我们强烈建议您为领域设置代理序列，如 创建代理序列，第 1814 页中所述

步骤 5 请点击 **集成** > **其他集成** > **领域** > **同步结果**。

相关主题

为跨域信任配置 管理中心 步骤 3：解决问题，第 1835 页

为跨域信任配置 管理中心 步骤 3：解决问题

在管理中心中设置跨域信任的最后一步是确保下载的用户和组没有错误。用户和组无法正确下载的一个典型原因是它们所属的领域尚未下载到 管理中心。

本主题讨论如何诊断由于某个域未配置为在域控制器层次结构中查找该组而无法下载一个林中引用的组。

开始之前

过程

步骤 1 如果尚未登录，请登录 管理中心。

步骤 2 请点击 **集成** > **其他集成** > **领域** > **同步结果**。

在领域列中，如果领域名称旁边显示 **黄色三角形**（  ），则您必须解决问题。否则，您的结果配置正确，您可以退出。

步骤 3 从显示问题的领域重新下载用户和组。

a) 点击 **领域** 选项卡。

b) 点击  （立即下载），然后点击 **是**。

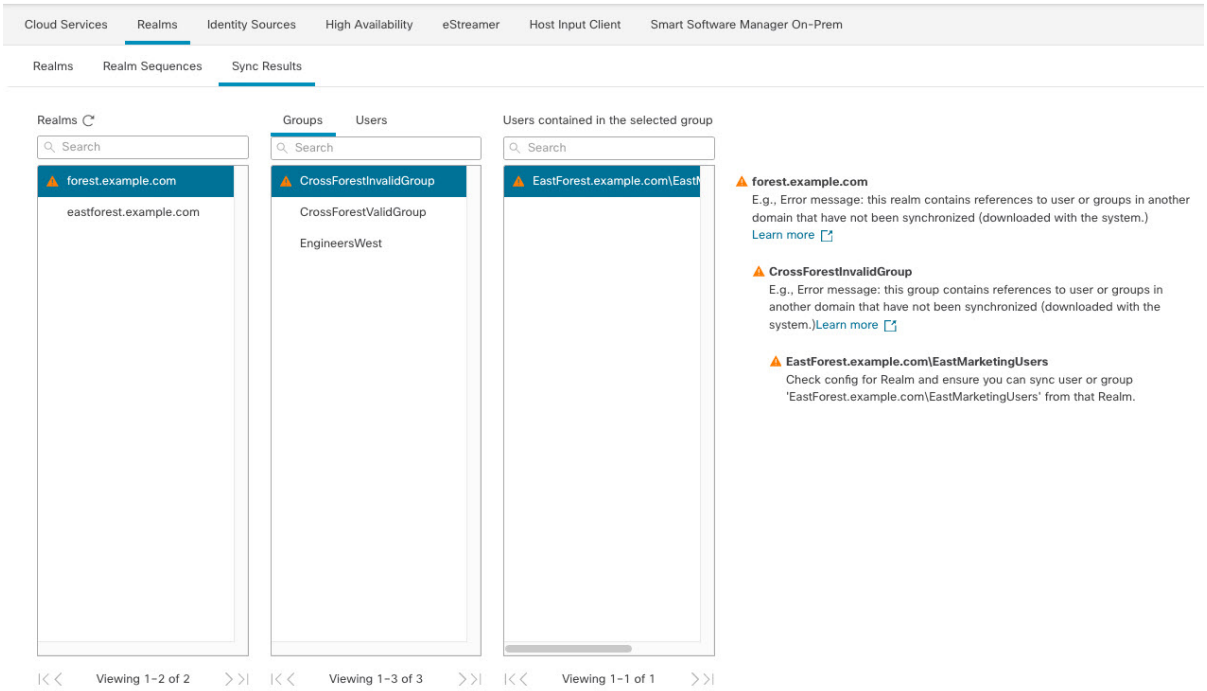
步骤 4 点击 **同步结果** 选项卡页面。

如果“领域”列中显示 **黄色三角形**（  ），请点击存在问题的领域旁边的 **黄色三角形**（  ）。

步骤 5 在中间列中，点击组或用户以查找更多信息。

步骤 6 在组或用户选项卡页面中，点击 **黄色三角形**（  ）以显示更多信息。

右列应显示足够的信息，以便您可以确定问题的来源。



在上述示例中， **forest.example.com** 包括一个跨域组 **CrossForestInvalidGroup** ，其中包含未由 管理中心下载的另一个组 **EastMarketingUsers** 。如果在再次同步 **eastforest.example.com** 领域后，错误未解决，则可能意味着 Active Directory 域控制器不包括 **EastMarketingUsers**。

要解决此问题，您可以：

- 从 **CrossForestInvalidGroup**中删除 **EastMarketingUsers** ， 再次同步 **forest.example.com** 领域，然后重新检查。
- 从 **eastforest.example.com** 领域的 **组 DN** 中删除 **ou=EastEngineering** 值，这会导致 管理中心 从 Active Directory 层次结构的最高级别检索组，进行 **eastforest.example.com**同步并重新检查。

管理领域

本部分讨论如何使用“领域”页上的控件来为领域执行各种维护任务。请注意以下提示：

- 如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
- 如果显示**视图**（ ），则表明配置属于祖先域，或者您没有修改配置的权限。

过程

步骤 1 如果尚未登录，请登录管理中心。

步骤 2 请点击 **集成** > **其他集成** > **领域**。

步骤 3 要删除领域，请点击 **删除**（ ）。

步骤 4 要编辑领域，请点击领域旁边的 **编辑**（ ） 并进行更改，如 创建 Active Directory 领域和领域目录，第 1816 页中所述。

步骤 5 要启用领域，请将**状态**向右滑动；要禁用某个领域，请将其向左滑动。

步骤 6 要下载用户和用户组，请点击 **下载**（ ）。

步骤 7 要复制领域，请点击 **复制**（ ）。

步骤 8 要比较领域，请参阅比较领域，第 1837 页。

比较领域

您必须是 管理员、 访问管理员、 网络管理员或 安全审批人 才能执行此任务。

过程

步骤 1 登录管理中心。

步骤 2 请点击 **集成** > **其他集成** > **领域**。

步骤 3 点击**比较领域 (Compare Realms)**。

步骤 4 从**比较对象**下拉列表中选择**比较领域**。

步骤 5 从**领域 A** 和**领域 B** 下拉列表中选择要比较的领域。

步骤 6 点击 **OK**。

步骤 7 如果要逐一浏览更改，请点击标题栏上方的**上一个**或**下一个**。

步骤 8 （可选。）点击**比较报告**生成领域比较报告。

步骤 9 （可选。）点击**新增比较**生成新的领域比较视图。

领域和用户下载故障排除

如果发现意外的服务器连接行为，请考虑调整领域配置、设备设置或服务器设置。有关其他相关故障排除信息，请参阅：

- 排除 ISE / ISE-PIC 或 Cisco TrustSec 问题，第 1861 页
- TS 代理身份源故障排除，第 1884 页
- 强制网络门户身份源故障排除，第 1877 页
- 远程接入 VPN 身份源故障排除，第 1880 页

- 用户控制故障排除

症状：报告但不下载领域和组

管理中心的运行状况监控器会通知您用户或领域不匹配，其定义为：

- 用户不匹配：系统不下载某个用户而是报告给 管理中心 。

  造成用户不匹配通常是因为该用户属于不予下载至 管理中心。请回顾《Cisco Secure Firewall Management Center 设备配置指南》中介绍的信息。

- 领域不匹配：某个用户登录到某个域，而该域对应 管理中心未知的某个领域。

例如，如果您定义了一个与 管理中心 中名为 **domain.example.com** 的域相对应的领域，但系统报告从名为 **another-domain.example.com**的域进行了登录，这种情况就属于 领域不匹配。 管理中心 将此域中的用户识别为“未知”。

您将不匹配阈值设置为某个百分比，高于此百分比时会触发运行状况警告。示例：

- 如果您使用默认为 50% 的不匹配阈值，则在八个传入会话中有两个不匹配领域（不匹配百分比为 25%）的情况下不会触发任何警告。
- 如果您将不匹配阈值设置为 30%，在五个传入会话中有三个不匹配领域（不匹配百分比为 60%）的情况下则会触发警告。

系统不会对不匹配身份规则的未知用户应用任何策略。（虽然可以对未知用户设置身份规则，但我们建议您正确识别用户和领域，将规则数量保持在最低限度。）

有关详细信息，请参阅检测领域或用户不匹配 ， 第 1840 页。

症状：访问控制策略不匹配组成员

此解决方案适用于与其他 AD 域建立信任关系的 AD 域。在以下讨论中，外部域指用户登录的域之外的域。

如果用户属于受信任的外部域中定义的某个组， 管理中心 则不会跟踪外部域中的成员。例如，请考虑以下情景：

- 域控制器 1 和 2 相互信任
- A 组在域控制器 2 上定义
- 控制器 1 中的用户 `mparvinder` 是 A 组的成员

即使用户 `mparvinder` 在 A 组中，指定 A 组成员身份的 管理中心 访问控制策略规则也不与之匹配。

解决方案：在包含属于 B 组的所有域 1 帐户的域控制器 1 中创建类似的组。更改访问控制策略规则以匹配 A 组或 B 组的任何成员。

症状：访问控制策略与子域成员资格不匹配

如果用户属于母域的子域，Firepower 不跟踪域之间的母/子关系。例如，请考虑以下情景：

- 域 child.parent.com 是域 parent.com 的子域
- 用户 mparvinder 在 child.parent.com 中定义

即使用户 mparvinder 在子域中，与 parent.com 匹配的 Firepower 访问控制策略规则也与 child.parent.com 域中的 mparvinder 不匹配。

解决方案：将访问控制策略规则更改为匹配 parent.com 或 child.parent.com 中的成员。

症状：领域或领域目录测试失败

目录页面上的**测试**按钮将向您输入的主机名或 IP 地址发送 LDAP 查询。如果该查询失败，请检查以下事项：

- 您输入的**主机名**解析到 LDAP 服务器或 Active Directory 域控制器的 IP 地址。
- 您输入的 **IP 地址**无效。

领域配置页面上的 **测试 AD 加入** 按钮将验证以下事项：

- DNS 将 **AD 主域**解析到 LDAP 服务器或 Active Directory 域控制器的 IP 地址。
- **AD 加入用户名**和 **AD 加入密码**正确无误。

  AD 加入用户名必须是完全限定的（例如， **administrator@mydomain.com** ，而不是 **administrator**）。
- 用户有足够的权限在域中创建计算机，并将 管理中心 作为域计算机加入到该域。

症状：在非正常时间发生用户超时

如果您发现系统在非预期时间间隔时执行用户超时，请确认 ISE/ISE-PIC 服务器上的时间与 Cisco Secure Firewall Management Center上的时间是否同步。如果设备不同步，系统可能会在非预期时间间隔时执行用户超时。

如果您发现系统在非预期时间间隔时执行用户超时，请确认 ISE/ISE-PIC 或 TS 代理服务器上的时间与 Cisco Secure Firewall Management Center上的时间是否同步。如果设备不同步，系统可在非预期时间间隔时执行用户超时。

症状：无法下载用户

可能的原因如下：

- 如果您配置的领域**类型**不正确，则将由于系统期望的属性与存储库提供的属性之间不匹配而无法下载用户和组。例如，如果您为 Microsoft Active Directory 领域将**类型**配置为 **LDAP**，则系统期望 uid 属性，而在 Active Directory 上它将被设置为无。（Active Directory 存储库将 sAMAccountName 用于用户 ID。）

  解决方案：适当设置领域**类型**字段：对于 Microsoft Active Directory，设置为 **AD**；对于其他受支持的 LDAP 存储库，设置为 **LDAP**。

- 组或组织单位名称中包含特殊字符的 Active Directory 组中的用户，可能不可用于身份策略规则。例如，如果组或组织单位名称包含字符星号 (*)、等号 (=) 或反斜线 (\)，则这些组中的用户无法下载，并且无法用于身份策略。

  解决方案：从组或组织单位名称中删除特殊字符。

症状：并非一个领域的所有用户都被下载

可能的原因如下：

- 如果尝试下载的用户数超过任何一个领域的最大数量，则下载将在达到最大用户数时停止，同时显示运行状况警报。用户下载限制按 Cisco Secure Firewall Management Center 型号来设置。
- 每个用户都必须是组的成员。不属于任何组的用户不会被下载。

症状：先前未发现的 ISE/ISE-PIC 用户代理用户的用户数据未显示在 Web 界面上

在系统检测到其数据尚未包含在数据库中的 ISE/ISE-PIC 或 TS 代理用户的活动后，系统会从服务器检索其有关信息。在某些情况下，系统需要额外时间来从 Microsoft Windows 服务器成功检索此信息。在数据检索成功之前，ISE/ISE-PIC 或 TS 代理用户发现的活动不显示在 Web 界面中。

请注意，这还可防止系统使用访问控制规则处理用户的流量。

症状：事件中的用户数据为意外

如果您发现用户或用户活动事件包含意外 IP 地址，请检查您的领域。系统不支持为多个领域配置相同的 **AD 主域**值。

症状：源于终端服务器登录的用户未被系统唯一识别

如果部署包括终端服务器，并为连接到该终端服务器的一个或多个服务器配置领域，则必须部署思科终端服务 (TS) 代理以准确报告终端服务器环境中的用户登录。在安装并配置后，TS 代理将唯一端口分配给个人用户，因此系统可在 Web 界面中唯一识别这些用户。

有关 TS 代理的详细信息，请参阅《思科终端服务 *(TS)* 代理指南》。

检测领域或用户不匹配

本部分讨论如何检测领域或用户不匹配，其定义为：

- 用户不匹配：系统不下载某个用户而是报告给 管理中心 。

  造成用户不匹配通常是因为该用户属于不予下载至 管理中心。请回顾《Cisco Secure Firewall Management Center 设备配置指南》中介绍的信息。

- 领域不匹配：某个用户登录到某个域，而该域对应 管理中心未知的某个领域。

有关其他详细信息，请参阅领域和用户下载故障排除 ，第 1837 页。

系统不会对不匹配身份规则的未知用户应用任何策略。（虽然可以对未知用户设置身份规则，但我们建议您正确识别用户和领域，将规则数量保持在最低限度。）

过程

步骤 1 启用领域或用户不匹配检测：

a) 如果尚未登录，请登录 管理中心。
b) 点击 **系统** > **运行状况** > **策略**。
c) 创建新运行状况策略或编辑现有运行状况策略。
d) 在“编辑策略”页面上，设置**策略运行时间间隔**。
这是所有运行状况监控任务的运行频率。
e) 在左侧窗格中，点击**领域**。
f) 输入以下信息：

- **启用**：点击**打开**
- **警告用户匹配阈值百分比**：在运行状况监控器中触发警告的领域不匹配或用户不匹配的百分比。有关详细信息，请参阅领域和用户下载故障排除，第 1837 页。

g) 在页面底部，点击**保存策略并退出**。
h) 如在 《Cisco Secure Firewall Management Center 管理指南》中 运行状况策略 所述，对受管设备应用运行状况策略。

步骤 2 通过以下任意方式查看用户和领域不匹配：

- 如果超出警告阈值，点击 管理中心顶部导航中的 **经过**>**运行状况** 。这将打开运行状况监控器。
- 点击 **系统** > **运行状况** > **监控器**。

步骤 3 在“运行状况监控器”页面上的“显示”列中，展开**领域：域**或**领域：用户**来查看有关不匹配的详细信息。

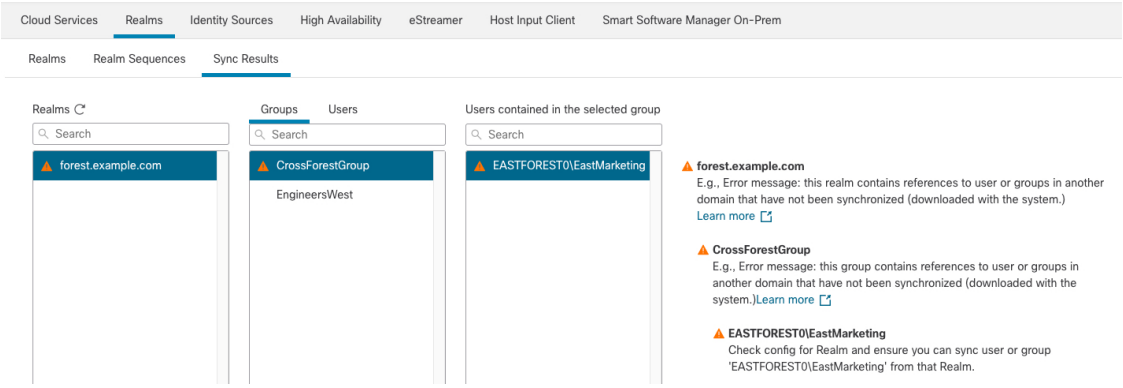
排除跨域信任故障

对跨域信任 管理中心 配置进行故障排除的典型问题包括：

- 不为具有共享组的所有林添加领域或目录。
- 配置领域以排除下载用户，并且这些用户在不同领域的组中被引用。
- 某些临时问题。

了解问题

如果 管理中心 能够将用户和组与您的 Active Directory 目录林同步存在问题，系统将显示“同步结果”选项卡页面，如下所示。



下表介绍如何解释信息。

列	含义
领域	显示系统中配置的所有领域。点击 **刷新** （）以更新领域列表。 **黄色三角形**（）显示来指示领域中的问题。 如果所有用户和组成功同步，则领域旁边不显示任何内容。
组	点击 **组** 以显示领域中的所有组。与领域一样，**黄色三角形**（）显示表示问题。 点击 **黄色三角形**（）查看有关此问题的更多详细信息。
用户	点击 **用户** 以显示按组排序的所有用户。
所选组中包含的用户	显示您在“组”列中选择的组中的所有用户。点击 **黄色三角形**（）可在表的右侧显示更多信息。
包含所选用户的组	显示所选用户所属的所有组。点击 **黄色三角形**（）可在表的右侧显示更多信息。
错误详细信息（显示在表的右侧）。	系统会显示无法同步的 NetBIOS 林名称和组名称。系统无法同步这些用户和组的典型原因如下： • **问题：**包含组和用户的林没有在 管理中心中配置相应的领域。 **解决方案：**如 创建 Active Directory 领域和领域目录，第 1816 页中所述，为包含该组的林添加一个领域。 • **问题：**已将组下从载到 管理中心中排除。 **解决方案：**点击 **领域** 选项卡页面，点击 **编辑**（），然后从 **排除的组和用户** 列表中移动指示的组或用户。

再次尝试下载用户和组

如果问题是临时的，请下载所有领域的用户和组。

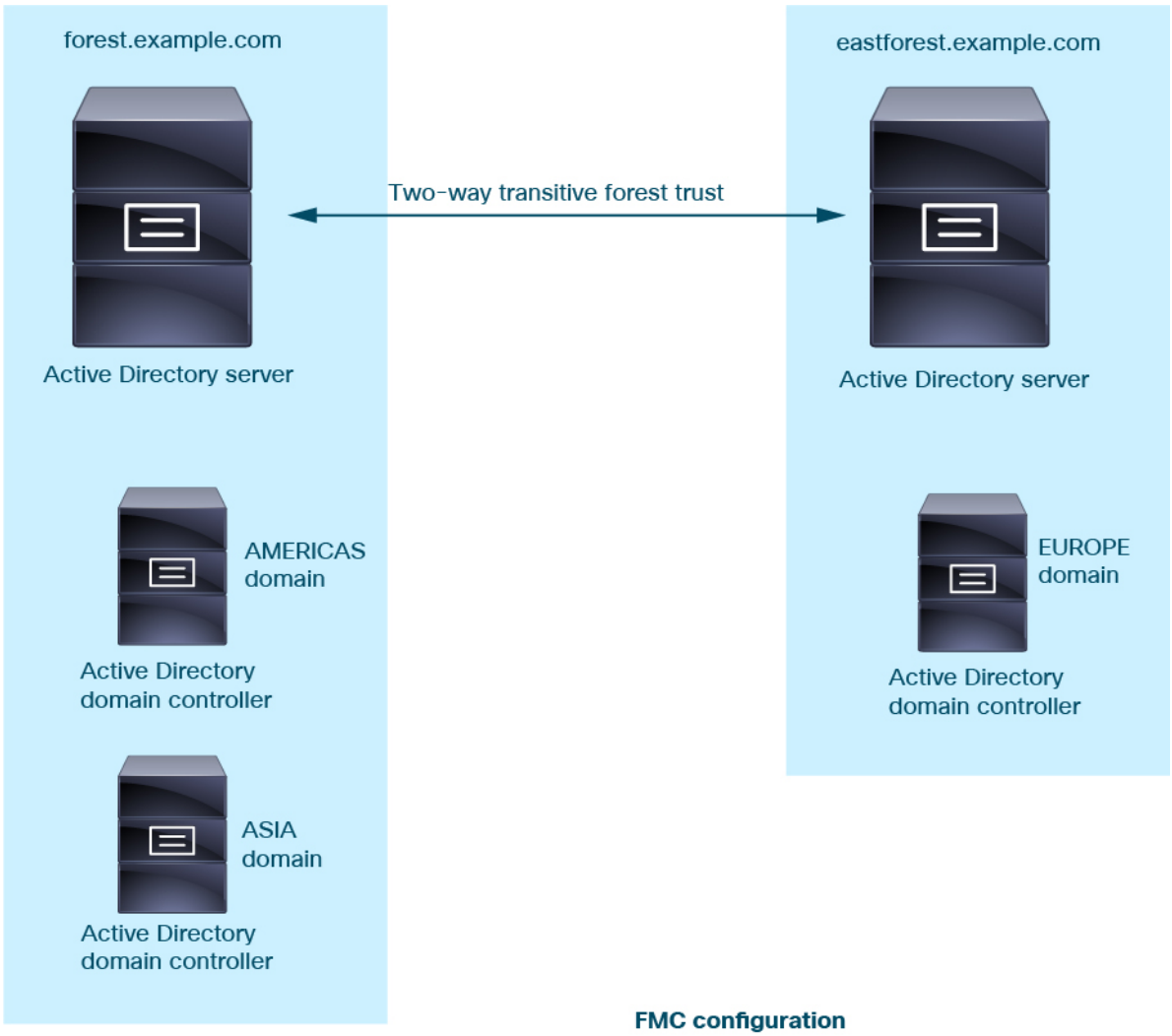
1. 如果尚未登录，请登录 管理中心。
2. 请点击 **集成** > **其他集成** > **领域**。
3. 请点击 **下载**（ ）。
4. 点击 **同步结果** 选项卡页面。
5. 如果“领域”列中的条目未显示指示器，则问题已解决。

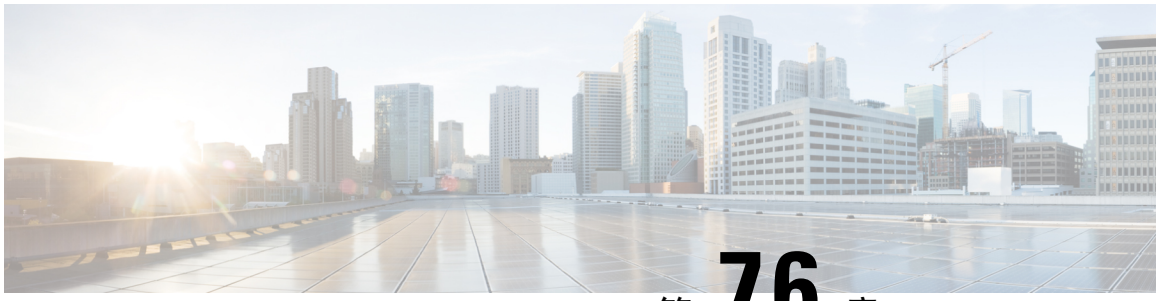
为所有林添加领域

确保已配置：

- 具有要在身份策略中使用的用户的每个林的管理中心 领域。
- 该林中每个域控制器的 管理中心 目录，其中包含要在身份策略中使用的用户。

下图显示了一个示例。


forest.example.com
eastforest.example.com
Two-way transitive forest trust
Active Directory server
Active Directory server
AMERICAS
domain
Active Directory
domain controller
EUROPE
domain
Active Directory
domain controller
ASIA
domain
Active Directory
domain controller
FMC configuration
FMC
Realm: forest.example.com
Directory: AMERICAS.forest.example.com
Directory: ASIA.forest.example.com
Realm: eastforest.example.com
Directory: EUROPE.eastforest.example.com



第 76 章

通过 ISE/ISE-PIC 的用户控制

以下主题介绍如何通过 ISE/ISE-PIC 执行用户感知和用户控制：

ISE/ISE-PIC 身份源

您可以将思科身份服务引擎 (ISE) 或 ISE 被动身份连接器 (ISE-PIC) 部署与 Firepower 系统集成到一起，以便将 ISE/ISE-PIC 用于被动身份验证。

ISE/ISE-PIC 是一个授权身份源，并为使用 Active Directory (AD)、LDAP、RADIUS 或 RSA 进行身份验证的用户提供用户感知数据。此外，您还可以对 Active Directory 用户执行用户控制。ISE/ISE-PIC 不报告 ISE 访客服务用户的失败登录尝试或活动。

注释 Firepower 系统不会解析 IEEE 802.1x 计算机身份验证，但会解析 802.1x 用户身份验证。如果将 802.1x 与 ISE 配合使用，则必须包括用户身份验证。802.1x 计算机身份验证不会向可在策略中使用的 FMC 提供用户身份。

有关 Cisco ISE/ ISE-PIC的详细信息，请参阅 Cisco Identity Services Engine Passive Identity Connector 管理员指南。

注释 我们强烈建议您使用最新版本的ISE/ ISE-PIC 获取最新功能集和最多数量的问题修复程序。

源和目标安全组标记 (SGT) 匹配

如果使用 ISE 定义并使用安全组标记 (SGT) 来对 Cisco TrustSec 网络中的流量进行分类，则可以编写使用 SGT 作为匹配条件的访问控制规则。这允许您可以基于安全组成员身份阻止或允许访问，而不是使用 IP 地址或网络。

匹配 SGT 标签具有以下优势：

- 管理中心 可以从 ISE 订阅安全组标记交换协议 (SXP) 映射。

  ISE 使用 SXP 将 IP 到 SGT 映射数据库传播到受管设备。当您将 管理中心 配置为使用 ISE 服务器时，必须打开该选项才能从 ISE 侦听 SXP 主题。这会导致 管理中心 直接从 ISE 了解安全组标记和映射。然后，FMC 将 SGT 和映射发布到受管设备。

  SXP 主题接收基于 ISE 与其他 SXP 兼容设备（例如交换机）之间通过 SXP 协议获取的静态和动态映射的安全组标记。

  您可以在 ISE 创建安全组标记，并将主机或网络 IP 地址分配至各标记。您还可以将 SGT 分配给用户账户，并将 SGT 分配给用户流量。如果网络中的交换机和路由器配置为执行此操作，则在数据包进入 ISE（Cisco TrustSec 云) 控制的网络时，这些标记会分配给数据包。

  ISE-PIC 不 支持 SXP。

- 管理中心和受管设备可以了解SGT映射，而无需部署其他策略。（换句话说，您可以在不部署访问控制策略的情况下查看 SGT 映射的连接事件。）
- 支持 Cisco TrustSec，使您能够对网络进行分段，以保护关键业务资产。
- 受管设备评估 SGT 作为访问控制规则的流量匹配条件时，会使用以下优先级：

  1. 数据包中定义的源 SGT 标记（如有）。

     对于数据包中的 SGT 标记，必须配置网络中的交换机和路由器以添加它们。有关如何实施此方法的信息，请参阅 ISE 文档。

     对于数据包中的 SGT 标记，必须配置网络中的交换机和路由器以添加它们。有关如何实施此方法的信息，请参阅 ISE 文档。

  2. 分配给用户会话的 SGT，从 ISE 会话目录下载。 SGT 可以与源或目标相匹配。
  3. 使用 SXP 下载的 SGT-IP 地址映射。如果 IP 地址在 SGT 范围内，则流量与使用 SGT 的访问控制规则相匹配。SGT 可以与源或目标相匹配。

示例：

- 在 ISE 中，创建名为 Guest Users 的 SGT 标记并将其与 192.0.2.0/24 网络关联。

  例如，您可以将访客用户用作访问控制规则中的源 SGT 条件，并限制访问您网络的任何人对某些 URL、网站类别或网络的访问。

- 在 ISE 中，创建名为 Restricted Networks 的 SGT 标记并将其与 198.51.100.0/8 网络关联。

  例如，您可以使用“受限网络”作为目标 SGT 规则条件，并阻止来自访客用户和具有未经授权访问网络的用户的其他网络的访问。

相关主题

ISE/ISE-PIC 指南和限制，第 1847 页

ISE/ISE-PIC 的许可证要求

威胁防御 许可证

任意

经典许可证

控制

ISE/ISE-PIC 的要求和必备条件

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

ISE/ISE-PIC 指南和限制

请在配置 ISE/ISE-PIC 时使用本节所讨论的准则。

ISE/ISE-PIC 版本和配置兼容性

您的ISE /ISE-PIC 版本和配置会影响其与 Firepower 的集成和交互，如下所示：

- 我们强烈建议您使用最新版本的 ISE/ ISE-PIC 来获取最新的功能集。
- 同步 ISE/ISE-PIC 服务器和 Cisco Secure Firewall Management Center上的时间。否则，系统可能会以意外间隔执行用户超时。
- 要使用 ISE 或 ISE-PIC 数据实施用户控制，请配置并启用担任 pxGrid 角色的 ISE 服务器的领域，如创建 Active Directory 领域和领域目录，第 1816 页中所述。
- 每个连接到 ISE 服务器的 Cisco Secure Firewall Management Center主机名必须是唯一的；否则，将丢弃与其中一个 Cisco Secure Firewall Management Center的连接。

- 如果将 ISE/ISE-PIC 配置为监控大量用户组，则由于内存限制，系统可能会根据组丢弃用户映射。因此，带有领域或用户条件的规则可能不会按预期执行。

  对于运行版本 6.7 或更高版本的任何设备，您可以选择使用 **configure identity-subnet-filter** 命令限制受管设备监控的子网。有关详细信息，请参阅Cisco Secure Firewall Threat Defense 命令参考。

  或者，您可以配置网络对象并将该对象应用为身份策略中的身份映射过滤器。请参阅创建身份策略，第 1887 页。

有关与此版本的系统兼容的 ISE/ISE-PIC 的特定版本，请参阅 思科 Firepower 兼容性指南。

IPv6 支持

- 兼容版本的 ISE/ISE-PIC 版本 2.x 包括对支持 IPv6 的终端的支持。
- 版本 3.0（补丁 2）及更高版本的 ISE/ISE-PIC 启用 ISE/ISE-PIC 与 管理中心 之间的 IPv6 通信。

代理序列

代理序列 是一个或多个可用于与 LDAP、 Active Directory 或 ISE / ISE-PIC 服务器通信的受管设备。仅当 思科防御协调器 （CDO）无法与 Active Directory 或 ISE / ISE-PIC 服务器通信时，才需要执行此操作。（例如， CDO 可能在公共云中，但 Active Directory 或 ISE / ISE-PIC 可能在私有云中。）

虽然您可以使用一台受管设备作为代理序列，但我们强烈建议您设置两台或更多设备，以便在受管设备无法与 Active Directory 或 ISE / ISE-PIC 通信时，另一台受管设备可以接管。

在 ISE 中批准客户端

在 ISE 服务器与 管理中心 成功建立连接之前，您必须手动在 ISE 中批准客户端。（通常有两个客户端：一个用于连接测试，另一个用于 ISE 代理。）

您还可以按照《思科身份服务引擎管理员指南》中关于管理用户和外部身份源的章节中所述，在 ISE 中启用**自动批准新帐户**。

删除无法访问的会话

如果 ISE/ISE-PIC 中的用户会话被报告为无法访问，则 Cisco Secure Firewall Management Center 会删除该会话，因此具有相同 IP 的其他用户无法匹配不可访问的用户的身份规则。
您可以在 ISE/ISE-PIC 中控制此行为，方法是转至**提供程序 (Providers)** > **终端探测器 (Endpoint Probes)** 并点击以下选项之一：

- **启用 (Enabled)**，ISE/ISE-PIC 将监控终端连接，从而导致 Cisco Secure Firewall Management Center 删除无法访问的用户的会话。
- **禁用 (Disabled)**，可导致 ISE/ISE-PIC 忽略终端连接。

安全组标记 (SGT)

安全组标记 (SGT) 指定受信任网络中的流量源的权限。思科 ISE 和思科 TrustSec 使用称为安全组访问 (SGA) 的功能将 SGT 属性实时应用于进入网络的数据包。这些 SGT 对应于 ISE 或 TrustSec

中的用户分配的安全组。如果将 ISE 配置为身份源，则 Firepower 系统可以使用这些 SGT 过滤流量。

安全组标记可以用于源匹配条件和目标匹配访问控制规则的标准。

注释 要仅使用 ISE SGT 属性标记实施用户控制，则无需为 ISE 服务器配置领域。SGT ISE 属性条件可在具有或不具有关联身份策略的策略中进行配置。

注释 在某些规则中，自定义 SGT 条件可匹配带有非 ISE 分配的 SGT 属性标记的流量。这不属于用户控制，并且仅在不使用 ISE/ISE-PIC 作为身份源时才起作用；请参阅自定义 SGT 条件。

除源 SGT 标记外，要匹配目标 SGT 标记，请执行以下操作：

所需的 ISE 版本： 2.6 补丁 6 或更高版本，2.7 补丁 2 或更高版本

路由器支持：任何支持通过以太网 SGT 内联标记的 Cisco 路由器。有关详细信息，请参阅《Cisco 基于组的策略平台和功能列表》

限制：

- 服务质量（QoS）策略仅使用源 SGT 匹配；它 不 使用目标 SGT 匹配
- RA-VPN 不直接通过 RADIUS 接收 SGT 映射

ISE 和高可用性

当主 ISE / ISE-PIC 服务器发生故障时，会发生以下情况：

由于与 pxGrid v2 集成， 管理中心 已配置 ISE 主机之间的轮询，直到一台主机接受连接。

如果连接丢失， 管理中心 会恢复对连接主机的轮询尝试。

终端位置（或位置 IP）

终端位置属性为 ISE 识别的使用了 ISE 验证用户的网络设备的 IP 地址。

您必须配置和部署身份策略，才能根据**终端位置（位置 IP）**控制流量。

ISE 属性

配置 ISE 连接会使用 ISE 属性数据填充 Cisco Secure Firewall Management Center数据库。对于用户感知和用户控制，可以使用以下 ISE 属性。 SE-PIC 不支持这样做。

终端配置文件（或设备类型）

终端配置文件属性为 ISE 识别的用户终端设备类型。

您必须配置和部署身份策略，才能根据**终端配置文件（设备类型）**控制流量。

如何为用户控制配置 ISE/ISE-PIC

您可以在以下任何配置中使用 ISE/ISE-PIC：

- 具有领域、身份策略和关联的访问控制策略。

  在策略中使用领域来控制用户对网络资源的访问。您仍可以在策略中使用 ISE/ISE-PIC 安全组标记 (SGT) 元数据。

- 仅使用一个访问控制策略。不需要领域或身份策略。

  使用此方法可单独使用 SGT 元数据来控制网络访问。

相关主题

如何在没有领域的情况下配置 ISE，第 1850 页
如何为无领域的用户控制配置 ISE/ISE-PIC，第 1851 页

如何在没有领域的情况下配置 ISE

本主题简要介绍了配置 ISE 以允许或阻止使用 SGT 标记访问网络时所必须完成的任务。

过程

	命令或操作	目的
步骤 1	SGT 匹配：在 ISE 上启用 SXP。	这使 管理中心 能够在 SGT 元数据更改时从 ISE 接收更新。
步骤 2	从 ISE/ISE-PIC 导出系统证书。	在 ISE/ISE-PIC pxGrid、监控 (MNT) 服务器和管理中心之间进行安全连接需要证书。请参阅 从 ISE / ISE-PIC 服务器导出证书以在 管理中心 中使用，第 1855 页
步骤 3	将证书导入 管理中心。	必须按如下方式导入证书： • pxGrid 客户端证书：带密钥 (**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > **内部 CA (Internal CAs)**) 的内部证书 • pxGrid 服务器证书：受信任 CA (**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > **内部证书 (Internal Certs)**) • MNT 证书：受信任 CA

	命令或操作	目的
步骤 4	创建 ISE/ISE-PIC 身份源。	通过 ISE/ISE-PIC 身份源，您可以使用由 ISE/ISE-PIC 提供的安全组标记 (SGT) 控制用户活动。请参阅配置用户控制 ISE/ISE-PIC，第 1858 页。
步骤 5	创建访问控制规则。	访问控制规则指定了在流量与规则条件匹配时要采取的操作（例如，允许或阻止）。您可以将源和目标 SGT 元数据用作访问控制规则中的匹配条件。请参阅访问控制规则简介，第 1279 页。
步骤 6	将访问控制策略部署到托管设备。	在策略生效之前，必须将其部署到托管设备。请参阅部署配置更改，第 136 页。

下一步做什么

从 ISE / ISE-PIC 服务器导出证书以在 管理中心 中使用，第 1855 页

如何为无领域的用户控制配置 ISE/ISE-PIC

开始之前

本主题简要介绍为配置 ISE/ISE-PIC 进行用户控制并允许或阻止用户或组访问网络而必须完成的任务。用户和组可以存储在 领域支持的服务器，第 1812 页 中列出的任何服务器上。

过程

	命令或操作	目的
步骤 1	仅目标 SGT：在 ISE 上启用 SXP。	这使 管理中心 能够在 SGT 元数据更改时从 ISE 接收更新。
步骤 2	从 ISE/ISE-PIC 导出系统证书。	在 ISE/ISE-PIC pxGrid、监控 (MNT) 服务器和 管理中心 之间进行安全连接需要证书。请参阅以下内容： • pxGrid 服务器和 MNT 服务器证书：从 ISE / ISE-PIC 服务器导出证书以在 管理中心 中使用，第 1855 页 • pxGrid 客户端证书：生成自签证书，第 1857 页
步骤 3	将证书导入 管理中心。	必须按如下方式导入证书：

	命令或操作	目的
		• pxGrid 客户端证书：带密钥 (**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > **内部 CA (Internal CAs)**) 的内部证书 • pxGrid 服务器证书：受信任 CA (**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > **内部证书 (Internal Certs)**) • MNT 证书：受信任 CA
步骤 4	（可选。）创建用于该领域以及 ISE/ISE-PIC 的代理序列。	代理序列 是一个或多个可用于与 LDAP、Active Directory 或 ISE / ISE-PIC 服务器通信的受管设备。仅当思科防御协调器（CDO）无法与 Active Directory 或 ISE / ISE-PIC 服务器通信时，才需要执行此操作。（例如，CDO 可能在公共云中，但 Active Directory 或 ISE / ISE-PIC 可能在私有云中。） 虽然您可以使用一台受管设备作为代理序列，但我们强烈建议您设置两台或更多设备，以便在受管设备无法与 Active Directory 或 ISE / ISE-PIC 通信时，另一台受管设备可以接管。
步骤 5	创建领域。	您必须仅创建一个领域来控制所选择的用户和组对网络的访问。 请参阅创建 Active Directory 领域和领域目录，第 1816 页。
步骤 6	下载用户和组并启用领域。	下载用户和组让您能够在访问控制规则中使用它们。请参阅同步用户和组，第 1827 页。
步骤 7	创建 ISE/ISE-PIC 身份源。	通过 ISE/ISE-PIC 身份源，您可以使用由 ISE/ISE-PIC 提供的安全组标记 (SGT) 控制用户活动。请参阅配置用户控制 ISE/ISE-PIC，第 1858 页。
步骤 8	创建身份策略。	身份策略是一个或多个身份规则的容器。请参阅创建身份策略，第 1887 页。
步骤 9	创建身份规则。	身份规则指定了如何使用领域来控制用户和组对网络的访问。请参阅创建身份规则，第 1894 页。

	命令或操作	目的
步骤 10	将身份策略与访问控制策略相关联。	这会让访问控制策略能够使用领域中的用户和组。
步骤 11	创建访问控制规则。	访问控制规则指定了在流量与规则条件匹配时要采取的操作（例如，允许或阻止）。您可以将源和目标SGT元数据用作访问控制规则中的匹配条件。请参阅访问控制规则简介，第 1279 页。
步骤 12	将访问控制策略部署到托管设备。	在策略生效之前，必须将其部署到托管设备。请参阅部署配置更改，第 136 页。

下一步做什么

从 ISE / ISE-PIC 服务器导出证书以在 管理中心 中使用，第 1855 页

配置 ISE/ISE-PIC

以下主题讨论如何配置 ISE/ISE-PIC 服务器，以便与 管理中心 中的身份策略配合使用。

您必须从 ISE/ISE-PIC 服务器导出证书，以使用 管理中心 进行身份验证并发布 SXP 主题，以便使用 ISE 服务器上的安全组标记 (SGT) 来更新 管理中心。

相关主题

在 ISE 中配置安全组和 SXP 发布，第 1853 页
从 ISE / ISE-PIC 服务器导出证书以在 管理中心 中使用，第 1855 页

在 ISE 中配置安全组和 SXP 发布

您必须在思科身份服务引擎 (ISE) 中执行许多配置，才能创建 TrustSec 策略和安全组标记 (SGT)。有关实施 TrustSec 的更完整信息，请参阅 ISE 文档。

以下操作步骤将挑选出必须在 ISE 中配置的核心设置的要点，以便 威胁防御 设备能够下载和应用静态 SGT-IP 地址映射，然后在访问控制规则中用于源 SGT 和目标 SGT 匹配。有关详细信息，请参阅 ISE 文档。

此操作步骤的屏幕截图基于 ISE 2.4。在后续版本中，这些功能的确切路径可能会发生变化，但概念和要求是相同的。虽然建议使用 ISE 2.4 或更高版本（最好是 2.6 或更高版本），但配置应从 ISE 2.2 补丁 1 开始。

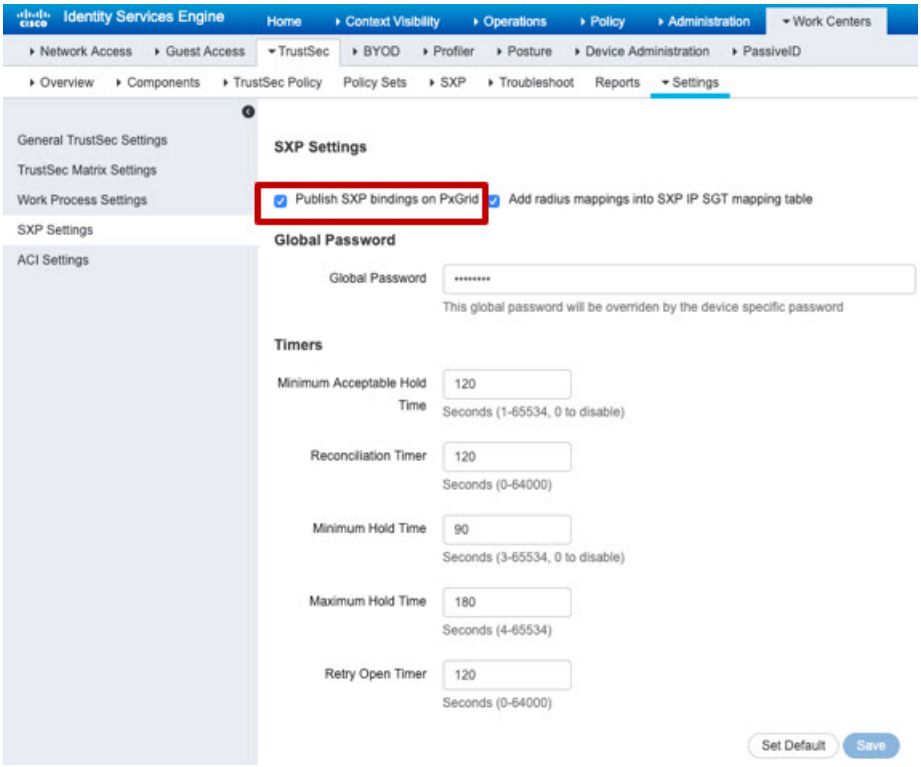
开始之前

您必须拥有 ISE Plus 许可证，才能发布从 SGT 到 IP 地址的静态映射和获取从用户会话到 SGT 的映射，以便 威胁防御 设备可以接收这些映射。

过程

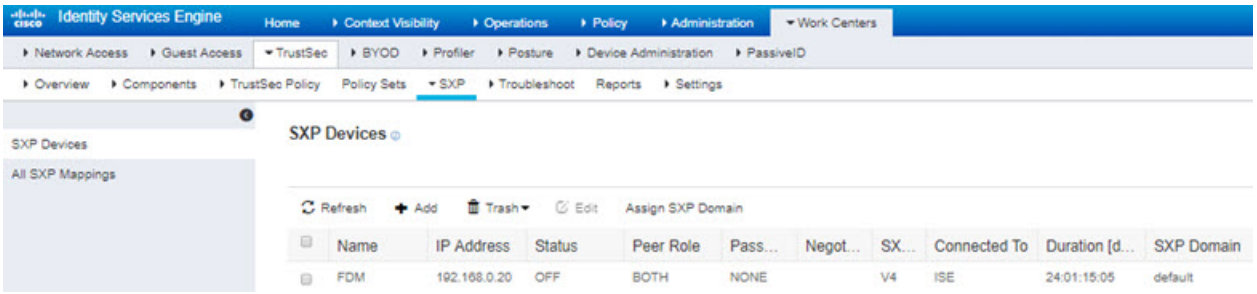
步骤 1 选择工作中心 > **TrustSec** > **设置** > **SXP 设置**，然后选择**在 PxGrid 上发布 SXP 绑定**选项。

选择该选项后，ISE 使用 SXP 发送 SGT 映射。您必须选择此选项， 威胁防御 设备才能“收听”从列表至 SXP 主题等一切内容。必须选择此选项， 威胁防御 设备才能获取静态 SGT-IP 地址映射信息。如果您仅想使用数据包中定义的 SGT 标记或分配给用户会话的 SGT，则没有必要。

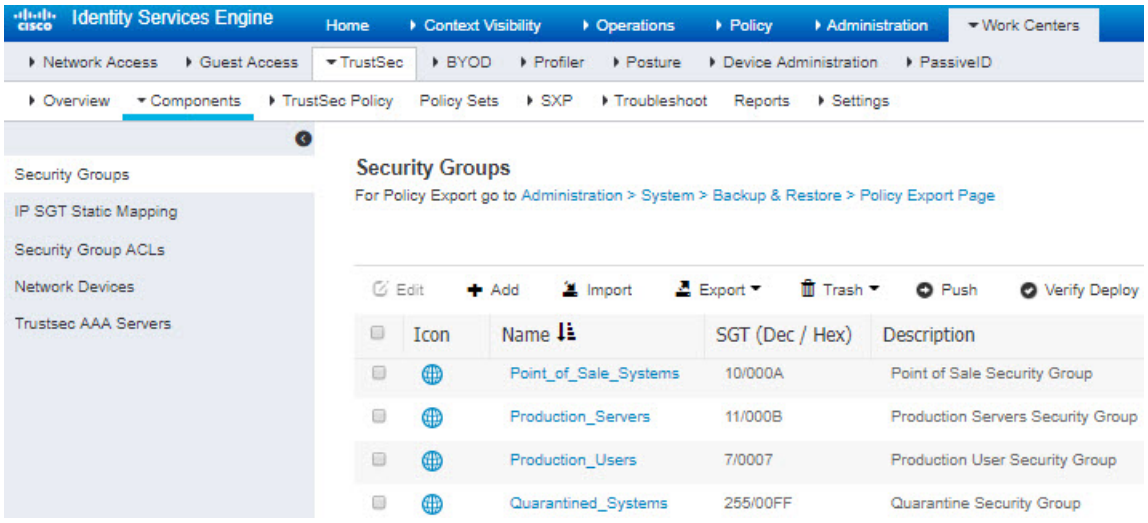


步骤 2 选择工作中心 > **TrustSec** > **SXP** > **SXP 设备**，然后添加设备。

这并不一定是真正的设备，您甚至可以使用 威胁防御 设备的管理 IP 地址。该表只需要至少一台设备来促使 ISE 发布静态 SGT-IP 地址映射。如果您仅想使用数据包中定义的 SGT 标记或分配给用户会话的 SGT，则无需执行此步骤。

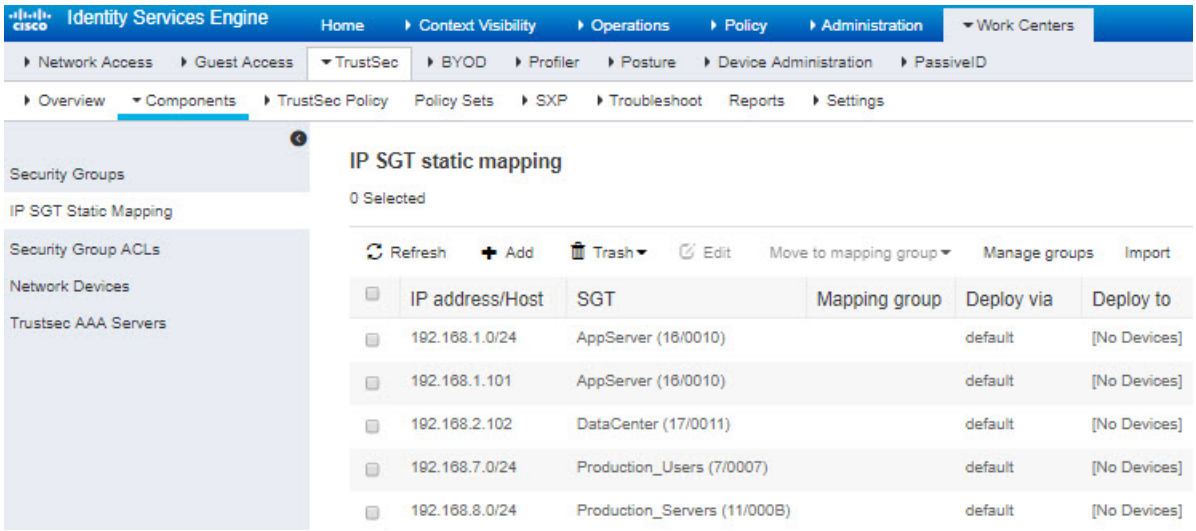


步骤 3 选择工作中心 > **TrustSec** > **组件** > **安全组**并验证是否定义了安全组标记。按需新建。



步骤 4 选择**工作中心** > **TrustSec** > **组件** > **IP SGT 静态映射**，并将主机和网络 IP 地址映射至安全组标记。

如果您仅想使用数据包中定义的 SGT 标记或分配给用户会话的 SGT，则无需执行此步骤。



从 ISE / ISE-PIC 服务器导出证书以在 管理中心 中使用

以下各节介绍如何：

- 从 ISE / ISE-PIC 服务器导出系统证书。

  这些证书是安全连接到 ISE / ISE-PIC 服务器所必需的。您可能需要导出一个或多达三个证书，具体取决于 ISE 系统的设置方式：

  - pxGrid 服务器的一个证书

- 监控（MNT）服务器一个证书
- 一个证书，包括私钥，用于 pxGrid 客户端（即 管理中心）

  与前两个证书不同，这是一个自签名证书。

- 将这些证书导入 管理中心：
  - pxGrid 客户端证书：带密钥 (**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > 内部 **CA (Internal CAs)**) 的内部证书
  - pxGrid 服务器证书：受信任 CA (**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > **内部证书 (Internal Certs)**)
  - MNT 证书：受信任 CA

相关主题

导出系统证书，第 1856 页
导入 ISE/ISE-PIC 证书，第 1857 页

导出系统证书

您可以导出系统证书或某个证书及其关联的专用密钥。如果您导出证书及其私钥以进行备份，如有必要，您以后也可以重新导入此证书与私钥。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

过程

步骤 1 在思科 ISE GUI 中，点击**菜单**图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

步骤 2 选中要导出的证书旁边的复选框，然后点击**导出 (Export)**。

步骤 3 选择是仅导出证书，还是导出证书及其关联的私钥。

提示 由于可能会暴露专用密钥值，我们不建议导出与证书关联的专用密钥。如果您必须导出专用密钥（例如，导出要导入其他思科 ISE 节点以用于节点间通信的通配符系统证书时），请指定专用密钥加密密码。在将此证书导入另一思科 ISE 节点时，必须指定此密码以解密专用密钥。

步骤 4 如果您已选择导出私钥，请输入此密码。此密码至少必须包含 8 个字符。

步骤 5 点击 **Export** 以将证书保存至运行客户端浏览器的文件系统。

如果仅导出证书，证书将以 PEM 的格式进行存储。如果同时导出证书和专用密钥，则证书会导出为 .zip 文件，其中包含 PEM 格式的证书和已加密的专用密钥文件。

生成自签证书

通过生成自签证书添加新的本地证书。思科建议仅采用自签证书，以满足内部测试和评估需求。如果计划在生产环境中部署思科 ISE，尽可能使用 CA 签名证书，确保生产网络中更统一地接受。

注释 如果您使用自签名证书并且必须更改思科 ISE 节点的主机名，请登录思科 ISE 节点的管理门户，删除采用旧主机名的自签证书，然后生成新的自签证书。否则，思科 ISE 会继续使用采用旧主机名的自签证书。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

过程

步骤 1 选择在思科 ISE GUI 中，点击**菜单**图标 (☰) 并选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

要从辅助节点生成自签证书，请选择**管理 (Administration)** > **系统 (System)** > **服务器证书 (Server Certificate)**。

步骤 2 在 ISE-PIC GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **证书 (Certificates)** > **系统证书 (System Certificates)**。

步骤 3 点击**生成自签证书 (Generate Self Signed Certificate)** 并在显示的窗口中输入详细信息。

步骤 4 根据想要对其使用此证书的服务，选中 **Usage** 区域的复选框。

步骤 5 点击**提交 (Submit)** 生成证书。

要从 CLI 重新启动辅助节点，则按给定顺序输入以下命令：

a) **application stop ise**
b) **application start ise**

导入 ISE/ISE-PIC 证书

此步骤为可选。您还可以在创建 ISE/ISE-PIC 身份源时导入 ISE 服务器证书，如配置用户控制 ISE/ISE-PIC，第 1858 页中所述。

开始之前

从 ISE/ISE-PIC 服务器导出证书，如导出系统证书，第 1856 页中所述。证书和密钥必须存在于您登录管理中心 的计算机上。

您必须按如下方式导入证书：

- pxGrid 客户端证书：带密钥 (**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > **内部 CA (Internal CAs)**) 的内部证书
- pxGrid 服务器证书：受信任 CA (**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > **内部证书 (Internal Certs)**)
- MNT 证书：受信任 CA

过程

步骤 1 如果尚未登录，请登录 管理中心。
步骤 2 点击**对象 (Objects)** > **对象管理 (Object Management)**。
步骤 3 展开 **PKI**。
步骤 4 点击 **内部证书**。
步骤 5 点击 **Add Internal Cert**。
步骤 6 按照屏幕上的提示导入证书和私钥。
步骤 7 点击**受信任 CA (Trusted CAs)**。
步骤 8 点击**添加可信 CA**。
步骤 9 按照屏幕上的提示导入 pxGrid 服务器证书。
步骤 10 如有必要，请重复上述步骤，以便导入 MNT 服务器的受信任 CA。

下一步做什么

配置用户控制 ISE/ISE-PIC， 第 1858 页

配置用户控制 ISE/ISE-PIC

以下程序讨论如何配置 ISE/ ISE-PIC 身份源。您必须在全局域中才能执行此任务。

开始之前

- 要从 Microsoft Active Directory 服务器或受支持的 LDAP 服务器获取用户会话，请配置并启用 ISE 服务器的领域（假设为 pxGrid 角色），如 创建 Active Directory 领域和领域目录， 第 1816 页中所述。
- 配置到 ISE 或 ISE-PIC 的连接。有关详细信息，请参阅ISE/ISE-PIC 身份源， 第 1845 页和ISE/ISE-PIC 配置字段， 第 1860 页。
- 要获得 ISE 中定义的所有映射，包括通过 SXP 发布的 SGT 到 IP 地址的映射，请使用以下程序。或者，您可以选择以下选项：

- 要想只使用数据包中的 SGT 信息，而不使用从 ISE 下载的映射，请跳过 创建和编辑访问控制规则，第 1288 页中讨论的步骤。请注意，在这种情况下，您只能使用 SGT 标记作为源条件；这些标记永远不会匹配目标标准。
- 要仅在数据包和用户-IP-地址/SGT 映射中使用 SGT，请不要订阅 ISE 身份源中的 SXP 主题，也不要将 ISE 配置为发布 SXP 映射。您可以将此信息用于源匹配条件和目标匹配条件。

- 从 ISE/ ISE-PIC 服务器导出证书，也可以选择将其导入到 管理中心 中，如 从 ISE / ISE-PIC 服务器导出证书以在 管理中心 中使用，第 1855 页中所述。

过程

步骤 1 登录管理中心。

步骤 2 请点击 **集成** > **其他集成** > **身份源**。

步骤 3 为**服务类型**点击**身份服务引擎**以启用 ISE 连接。

注释 要禁用连接，请点击**无**。

步骤 4 输入**主要主机名/IP 地址**以及**辅助主机名/IP 地址**（后者为可选）。

步骤 5 从 **pxGrid 服务器 CA** 和 **MNT 服务器 CA** 列表中点击相应的证书颁发机构，然后从 **pxGrid 客户端证书** 列表中点击相应的证书。也可以点击 **添加**（＋） 来添加证书。

注释 **pxGrid 客户端证书** 必须包含 **clientAuth** 扩展密钥使用值，或者禁止包含任何扩展密钥使用值。

步骤 6 （可选。）使用 CIDR 块符号输入 **ISE 网络过滤器**。

步骤 7 在“订阅”部分中，选中以下项：

- **会话目录主题**，用于从 ISE 服务器接收 ISE 用户会话信息。
- **SXP 主题**，用于接收来自 ISE 服务器的 SGT 到 IP 映射的更新。要在访问控制规则中使用目标 SGT 标记，需要使用此选项。

步骤 8 （可选。）从 **代理** 列表中，点击受管设备或代理序列。
如果 CDO 无法与您的 ISE / ISE-PIC 服务器通信，您可以选择受管设备或代理序列来执行此操作。例如，您的 CDO 可能在公共云中，但 ISE / ISE-PIC 服务器可能在内部内联网上。

步骤 9 要测试操作，请点击**测试**。

如果测试失败，请点击**其他日志 (Additional Logs)** 以了解有关连接失败的详细信息。

下一步做什么

- 使用创建身份策略，第 1887 页中所述的身份策略指定要控制的用户和其他选项。

- 按将其他策略与访问控制相关联，第 1276 页中所述，将身份规则与可以过滤和选择性检查流量的访问控制策略相关联。
- 将身份和访问控制策略部署到受管设备，如部署配置更改，第 136 页中所述。
- 监控用户活动，。

相关主题

排除 ISE / ISE-PIC 或 Cisco TrustSec 问题，第 1861 页
受信任证书颁发机构对象，第 1005 页
内部证书对象，第 1008 页

ISE/ISE-PIC 配置字段

以下字段用于配置与 /ISE-PIC的连接。

主要和辅助主机名/IP 地址 (Primary and Secondary Host Name/IP Address)

主要和辅助（可选）pxGrid ISE 服务器的主机名或 IP 地址。

您指定的主机名所使用的端口必须可由 ISE 和 管理中心访问。

pxGrid 服务器 CA (pxGrid Server CA)

可信 pxGrid 框架的证书颁发机构。如果部署包括主要和辅助 pxGrid 节点，则两个节点的证书必须由同一证书颁发机构签署。

MNT 服务器 CA (MNT Server CA)

当执行批量下载时 ISE 证书的可信证书颁发机构。如果部署包括主要和辅助 MNT 节点，则两个节点的证书必须由同一证书颁发机构签署。

pxGrid 客户端证书

Cisco Secure Firewall Management Center 必须向 /ISE-PIC 提供的内部证书和密钥，以连接到 /ISE-PIC 或进行批量下载。

注释 **pxGrid 客户端证书** 必须包含 clientAuth 扩展密钥使用值，或者禁止包含任何扩展密钥使用值。

ISE 网络过滤器 (ISE Network Filter)

一个可选过滤器，可以将其设置为限制 ISE 报告给 Cisco Secure Firewall Management Center的数据。如果提供网络过滤器，则 ISE 会报告来自该过滤器中的网络的数据。可通过以下方式指定过滤器：

- 将此字段留空以指定**任意 (any)** 值。
- 使用 CIDR 符号输入单一 IPv4 地址块。
- 使用由逗号分隔的 CIDR 符号输入 IPv4 地址块列表。

注释 无论您的 ISE 是何版本，此版本的系统均不支持使用 IPv6 地址进行过滤。

订用：

会话目录主题：选中此复选框可从 ISE 服务器订阅用户会话信息。包括 SGT 和终端元数据。

SXP 主题：选中此复选框可从 ISE 服务器订阅 SXP 映射。

代理

如果 CDO 无法与 ISE / ISE-PIC 通信，您可以选择选择受管设备或代理序列。例如，您的 CDO 可能在公共云中，但 ISE / ISE-PIC 服务器可能在内部内联网上。

相关主题

受信任证书颁发机构对象，第 1005 页
内部证书对象，第 1008 页

排除 ISE / ISE-PIC 或 Cisco TrustSec 问题

排除 Cisco TrustSec 问题

设备接口可以配置为从 ISE/ ISE-PIC 或从网络上的 Cisco 设备（称为 Cisco TrustSec）传播安全组标记 (SGT)。在设备管理页面（**设备** > **设备管理**）上，在设备重新启动后，选中接口的 **传播安全组标记** 复选框。 如果您不希望接口传播 TrustSec 数据，请取消选中此复选框。

排除 ISE/ ISE-PIC 问题

有关其他相关故障排除信息，请参阅领域和用户下载故障排除，第 1837 页和用户控制故障排除。

如果您遇到 ISE 或 ISE-PIC 连接问题，请检查以下事项：

- 必须启用 ISE 中的 pxGrid 身份映射功能，才能将 ISE 与 Firepower 系统成功集成。
- 当主服务器出现故障时，您必须手动将辅助服务器升级为主服务器；不会进行自动故障切换。
- 在 ISE 服务器与 管理中心 成功建立连接之前，您必须手动在 ISE 中批准客户端。（通常有两个客户端：一个用于连接测试，另一个用于 ISE 代理。）

  您还可以按照 《思科身份服务引擎管理员指南》中"管理用户和外部身份源"的章节中所述，在 ISE 中启用 **自动批准新帐户** 。
- **pxGrid 客户端证书** 必须包含 **clientAuth** 扩展密钥使用值，或者禁止包含任何扩展密钥使用值。
- ISE 服务器上的时间必须与 Cisco Secure Firewall Management Center上的时间同步。如果设备不同步，系统可能会在非预期时间间隔时执行用户超时。
- 如果部署包括主要和辅助 pxGrid 节点，
  - 则两个节点的证书必须由同一个证书颁发机构签名。
  - ISE 服务器和 管理中心必须可以访问主机名使用的端口。

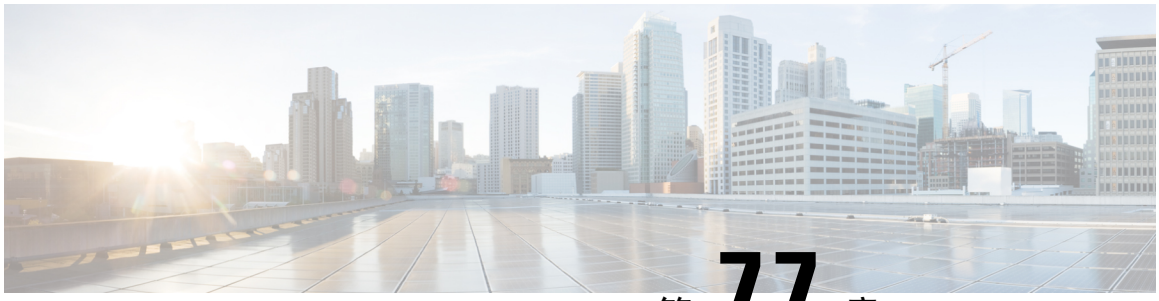
- 如果部署包括主要和辅助 MNT 节点，则两个节点的证书必须由同一证书颁发机构签署。

要从接收 ISE 的用户到 IP 和安全组标记 (SGT) 到 IP 的映射中排除子网，请使用 **configure identity-subnet-filter** {**add** | **remove**} 命令。您通常应对内存较低的受管设备执行此操作，以防止 Snort 身份运行状况监控器内存错误。

如果您遇到 ISE 或 ISE-PIC 报告的用户数据问题，请注意以下事项：

- 系统检测到其数据尚未在数据库中的 ISE 用户的活动后，会从服务器检索其相关信息。ISE 用户发现的活动并非由访问控制规则处理，而且在系统于用户下载中检索到它们的相关信息之前，它们不会显示在 Web 界面中。
- 不能对由 LDAP、RADIUS 或 RSA 域控制器进行身份验证的 ISE 用户执行用户控制。
- 管理中心不会收到 ISE 访客服务用户的用户数据。
- 如果 ISE 与 TS 代理监控的用户相同，则 管理中心 会划分 TS 代理数据的优先级。如果 TS 代理和 ISE 报告来自同一 IP 地址的相同活动，则仅会将 TS 代理数据记录到 管理中心。
- 您的 ISE 版本和配置会影响您在 Firepower 系统中使用 ISE 的方式。有关详细信息，请参阅 ISE/ISE-PIC 身份源，第 1845 页。
- 如果您配置了 管理中心 高可用性并且主管理中心出现故障，请参阅 ISE/ISE-PIC 指南和限制，第 1847 页中有关“ISE 和高可用性”的部分。
- ISE-PIC 不提供 ISE 属性数据。
- ISE-PIC 无法执行 ISE ANC 补救。
- 活动 FTP 会话在事件中显示为**Unknown**用户。此为正常现象，因为在活动 FTP 中，会由服务器（而非客户端）发起连接，而 FTP 服务器则不应具有关联的用户名。有关活动 FTP 的详细信息，请参阅 RFC 959。

如果您遇到支持的功能问题，请参阅 ISE/ISE-PIC 身份源，第 1845 页 了解版本兼容性的详细信息。



第 77 章

通过强制网络门户的用户控制

强制网络门户身份源

强制网络门户是系统支持的授权身份源之一。强制网络门户是一种主动身份验证方法，其中用户可以使用受管设备验证网络登录。

通常使用强制网络门户要求身份验证访问互联网，或者访问受限制的内部资源；可以选择配置对资源的访客访问。在系统对强制网络门户用户进行身份验证后，会根据访问控制规则处理其用户流量。强制网络门户仅会对 HTTP 和 HTTPS 流量执行身份验证。

注释 必须先对 HTTPS 流量进行加密，然后强制网络门户才能执行身份验证。

强制网络门户还记录失败的身份验证尝试。如果尝试失败，则不会将新用户添加到数据库的用户列表中。强制网络门户报告的身份验证活动失败的用户活动类型是**身份验证失败的用户 (Failed Auth User)**。

从强制网络门户获取的身份验证数据可用于用户感知和用户控制。

相关主题

如果为用户控制配置强制网络门户， 第 1867 页

关于主机名重定向

（仅限 Snort 3。）主动身份验证身份规则会使用其配置的接口重定向到强制网络门户端口。由于重定向通常是指向 IP 地址，因此用户会收到不受信任的证书错误，并且由于此行为类似于中间人攻击，因此用户可能不愿意接受不受信任的证书。

为避免此问题，您可以将强制网络门户配置为使用完全限定域名 (FQDN)。使用正确配置的证书时，用户不会收到不受信任的证书错误，并且身份验证将更加无缝，且看起来更加安全。

相关主题

重定向到主机名网络规则条件，第 1890 页

强制网络门户的许可证要求

威胁防御 许可证

任意

经典许可证

控制

强制网络门户的要求和必备条件

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

强制网络门户指南和限制

在身份策略中配置和部署强制网络门户时，来自指定领域的用户会使用 威胁防御 来进行身份验证，以访问您的网络。

注释 如果远程接入VPN用户已通过作为安全网关的受管设备进行主动身份验证，则不会执行强制网络门户主动身份验证，即便身份策略中配置了该验证方式。

需要路由接口

只有配置了路由接口的设备，才能执行强制网络门户主动身份验证。如果要为强制网络门户配置规则，并且您的强制网络门户设备包含内联接口和路由接口，则必须在访问控制策略中配置接口规则条件，以便仅针对设备上的路由接口。

如果访问控制策略引用的身份策略包含一个或多个强制网络门户身份规则，并且您在管理一个或多个配置了路由接口的设备的管理中心上部署策略，则策略部署成功且路由接口执行主动身份验证。

强制网络门户和策略

在身份策略中配置强制网络门户并在身份规则中调用主动身份验证。身份策略与访问控制策略相关联。

您可以在访问控制策略的**主动身份验证**选项卡页面上配置一些强制网络门户身份策略设置，并在与访问控制策略关联的身份规则中配置其余部分。

主动身份验证规则具有**主动身份验证**规则操作或**被动身份验证**规则操作，并且**如果无法建立被动或VPN识别，则使用主动身份验证**已选中。不管上述哪种情况，系统都会透明地启用或禁用 TLS/SSL 解密，从而重启 Snort 进程。

注意 在禁用了 TLS/SSL 解密（即，当访问控制策略不包括 an SSL 策略 时）时添加第一个主动身份验证规则或删除最后一个主动身份验证规则 在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。

当强制网络门户对与身份规则匹配的用户进行身份验证时，Active Directory 或 LDAP 组中尚未下载的任何Microsoft用户都将被识别为“未知”。为避免用户被识别为未知，请将领域配置为下载您希望通过强制网络门户进行身份验证的所有组中的用户。未知用户根据关联的访问控制策略处理；如果访问控制策略配置为阻止未知用户，则会阻止这些用户。

要确保系统下载领域中的所有用户，请确保组位于领域配置的可用组列表中。

有关同步用户和组的详细信息，请参阅同步用户和组，第 1827 页。

强制网络门户要求和限制

请注意以下要求和限制：

- 系统每秒最多支持 20 次强制网络门户登录。
- 对于计入最大登录尝试次数的失败登录尝试，失败登录尝试之间存在最长五分钟的时间限制。该五分钟限制不可配置。

（最大登录尝试次数显示在连接事件中：**分析** > **连接** > **事件**。）

如果失败登录之间的间隔时间超过五分钟，则用户将被重定向到强制网络门户进行身份验证，而不会被指定为登录失败的用户或访客用户，也不会报告给 管理中心。

- 强制网络门户不会协商 TLS v1.0 连接。

  仅支持 TLS v1.1、v1.2 和 TLS 1.3 连接。

- 您不能对强制网络门户使用领域序列。
- 确保用户注销的唯一方法是关闭并重新打开浏览器。除非发生这种情况，否则在某些情况下，用户可以注销强制网络门户，并且能够在不使用同一浏览器再次进行身份验证的情况下访问网络。
- 如果为父域创建了领域，并且受管设备检测到有用户登录到该父域的子域，则受管设备不会检测用户的后续注销。
- 必须允许流量流向计划用于强制网络门户的设备的 IP 地址和端口。
- 要对 HTTPS 流量执行强制网络门户主动身份验证，必须使用 an SSL 策略解密来自要对其进行身份验证的用户的流量。您无法解密受管设备上强制网络门户用户的 Web 浏览器和强制网络门户后台守护程序之间的连接中的流量；此连接用于对强制网络门户用户进行身份验证。
- 要限制允许流经受管设备的非 HTTP 或 HTTPS 流量的量，您应在身份策略的**端口**选项卡页面中输入典型的 HTTP 和 HTTPS 端口。

  受管设备在确定传入请求未使用 HTTP 或 HTTPS 协议时，会将先前未发现的用户从**待定**更改为**未知**。托管设备将用户从**待定**状态更改为其他状态之后，访问控制、服务质量和 SSL 策略便可以应用到该流量。如果您的其他策略不允许非 HTTP 或 HTTPS 流量，则在强制网络门户身份策略上配置端口可以防止允许不需要的流量流经受管设备。

- 当强制网络门户对与身份规则匹配的用户进行身份验证时，Active Directory 或 LDAP 组中尚未下载的任何 Microsoft 用户都将被识别为“未知”。为避免用户被识别为未知，请将领域配置为下载您希望通过强制网络门户进行身份验证的所有组中的用户。未知用户根据关联的访问控制策略处理；如果访问控制策略配置为阻止未知用户，则会阻止这些用户。

  要确保系统下载领域中的所有用户，请确保组位于领域配置的可用组列表中。

  有关详细信息，请参阅同步用户和组 ，第 1827 页。

Kerberos 必备条件

如果使用 Kerberos 身份验证，则受管设备的主机名必须少于 15 个字符（这是 Windows 设置的 NetBIOS 限制）；否则，强制网络门户身份验证失败。您在设置设备时设置受管设备主机名。有关详细信息，请参阅 Microsoft 文档网站上的此类文章： Active Directory 中计算机、域、站点和 OU 的命名约定。

DNS 必须向主机名返回 64KB 或更少的响应；否则，测试连接 AD 连接失败。此限制在两个方向上都适用，将在 RFC 6891 第 6.2.5 节中讨论。

如果为用户控制配置强制网络门户

开始之前

要使用强制网络门户进行主动身份验证，必须设置一个 Microsoft AD 或 LDAP 领域 （但非领域序列）、访问控制策略、一个身份策略、一个 an SSL 策略，并将身份和 SSL 策略 与访问控制策略关联。 最后，必须将这些策略部署到受管设备。此主题介绍这些任务的高度概要。

例如，整个过程从配置强制网络门户第 1 部分：创建网络主体 ， 第 1868 页开始。

首先，请执行以下任务：

- 确认您的 管理中心使用已配置的路由接口管理一台或多台设备。
- 要将加密身份验证用于强制网络门户，要么创建一个 PKI 对象，要么使证书数据和密钥可在用于访问 管理中心的机器上使用。要创建 PKI 对象，请参阅PKI ， 第 1000 页。

过程

步骤 1 按照以下主题中所述，创建并启用 Microsoft AD 领域：

- 创建 Active Directory 领域和领域目录 ， 第 1816 页
- 同步用户和组 ， 第 1827 页

强制网络门户不支持领域序列。

当强制网络门户对与身份规则匹配的用户进行身份验证时，Active Directory 或 LDAP 组中尚未下载的任何 Microsoft 用户都将被识别为“未知”。为避免用户被识别为未知，请将领域配置为下载您希望通过强制网络门户进行身份验证的所有组中的用户。未知用户根据关联的访问控制策略处理；如果访问控制策略配置为阻止未知用户，则会阻止这些用户。

要确保系统下载领域中的所有用户，请确保组位于领域配置的可用组列表中。

有关详细信息，请参阅同步用户和组 ， 第 1827 页。

步骤 2 （可选。）要将强制网络门户重定向到主机而不是 IP 地址，请创建具有关联的受信任证书颁发机构的网络对象。

请参阅配置强制网络门户第 1 部分：创建网络主体 ， 第 1868 页

步骤 3 为强制网络门户创建包含主动身份验证规则的身份策略。

在使用强制网络门户执行身份验证后，该身份策略将在您的领域访问资源内启用所选用户。

有关详细信息，请参阅配置强制网络门户第 2部分：创建身份策略 ， 第 1870 页。

步骤 4 为强制网络门户配置允许强制网络门户端口（默认情况下为 TCP 885）上的流量的访问控制规则。

您可以为要使用的强制网络门户选择任何可用的 TCP 端口。无论选择哪个端口，都必须创建一条允许该端口上的流量的规则。

有关详细信息，请参阅配置强制网络门户第 3 部分：创建 TCP 端口访问控制规则，第 1871 页。

步骤 5 再添加一条访问控制规则，以允许所选领域中的用户使用强制网络门户访问资源。

这样，用户可使用强制网络门户进行身份验证。

有关详细信息，请参阅配置强制网络门户第 4部分：创建用户访问控制规则，第 1872 页。

步骤 6 为**未知**用户配置 an SSL 策略 策略和**解密 - 重签**策略，以使强制网络门户用户能够使用 HTTPS 协议访问网页。

仅当HTTPS流量在流量发送到强制网络门户之前被解密的情况下，强制网络门户才能进行用户身份验证。系统将强制网络门户视为**未知**用户。

有关详细信息，请参阅配置强制网络门户第 5部分：创建 TLS/SSL 解密-重签策略，第 1873 页。

步骤 7 将身份和 SSL 策略 与第 3 步的访问控制策略相关联。

这是最后一步，此后系统即可使用强制网络门户进行用户身份验证。

有关详细信息，请参阅配置强制网络门户第 6 部分：将身份和 SSL 策略 与访问控制策略关联起来，第 1874 页。

下一步做什么

请参阅配置强制网络门户第 1 部分：创建网络主体，第 1868 页。

相关主题

排除强制网络门户中的应用，第 1876 页
PKI，第 1000 页
强制网络门户身份源故障排除，第 1877 页
Snort® 重新启动场景，第 143 页

配置强制网络门户第 1 部分：创建网络主体

开始之前

（仅限 Snort 3。）此任务是可选的。使用 DNS 服务器创建完全限定的主机名（FQDN）。如果您之前从未使用过例如 此类 资源，可以咨询此类资源。在管理中心的其中一个托管服务器上指定路由接口的 IP 地址。

有关网络对象的详细信息，请参阅 重定向到主机名网络规则条件，第 1890 页。

过程

步骤 1 如果尚未这样子，请登录 管理中心。

步骤 2 请点击 **对象** > **对象管理**。

步骤 3 展开 **PKI**。

步骤 4 点击 **内部证书**。

步骤 5 点击 **Add Internal Cert**。

步骤 6 在 **名称** 字段中，输入名称以标识受信任 CA（例如， **`MyCaptivePortal`**）。

步骤 7 在 **证书数据** 字段中，粘贴证书或使用 **浏览** 按钮查找证书。

证书公用名必须与您想要强制网络门户用户进行身份验证的 FDQN 完全匹配。

步骤 8 在 **密钥** 字段中，粘贴证书的私钥或使用 **浏览** 按钮查找证书。

步骤 9 如果证书已加密，请选中 **已加密** 复选框并在相邻字段中输入密码。

步骤 10 点击**保存**。

步骤 11 点击**网络 (Network)**。

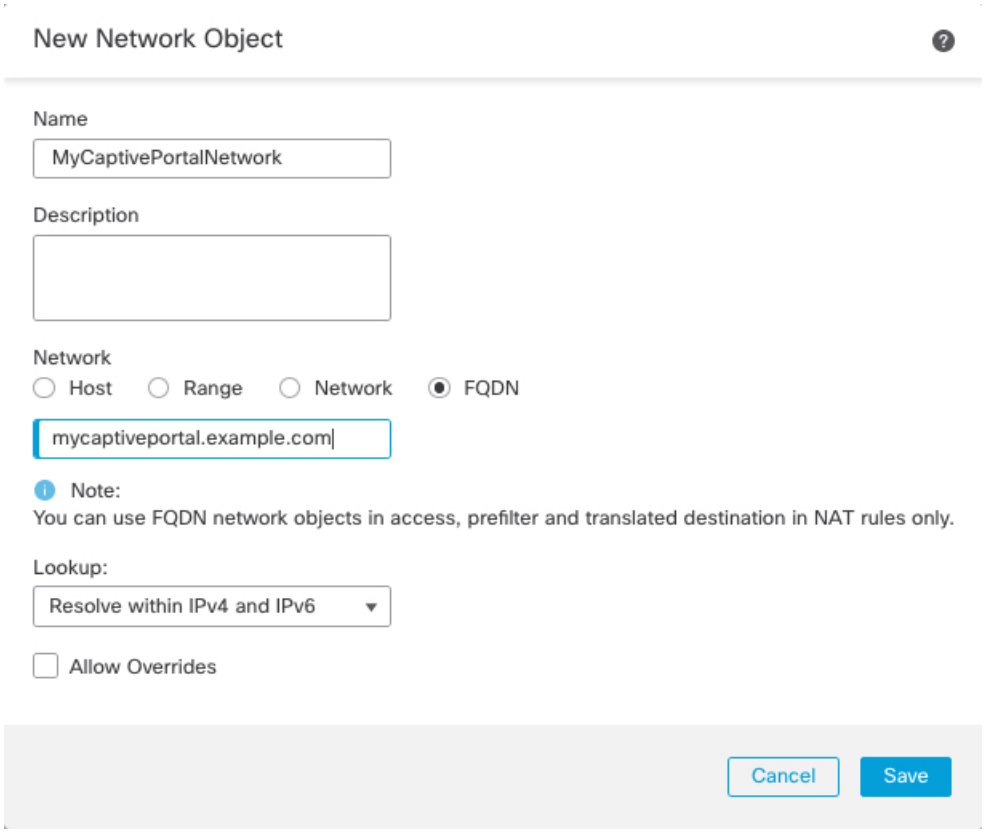
步骤 12 从页面顶部的列表中，点击 **添加对象**。

步骤 13 在 **名称** 字段中，输入名称以标识对象（例如， **`MyCaptivePortalNetwork`**）。

步骤 14 点击 **FDQN** ，然后在字段中输入强制网络门户的FDQN的名称。

步骤 15 点击 **查找**选项。

下图显示了一个示例。



步骤 16 点击**保存 (Save)**。

下一步做什么

配置强制网络门户第 2部分：创建身份策略，第 1870 页

配置强制网络门户第 2部分：创建身份策略

开始之前

此由多个部分组成的程序展示如何使用默认 TCP 端口 885 以及将 管理中心 服务器证书用于强制网络门户和 TLS/SSL 解密来设置强制网络门户。本示例中的每个部分介绍启用强制网络门户来执行主动身份验证所需的一项任务。

如果您遵循此程序中的所有步骤，则可以将强制网络门户配置为供您的域中的用户使用。您可以选择执行在程序的各个部分中介绍的其他任务。

有关完整程序的概述，请参阅如果为用户控制配置强制网络门户，第 1867 页。

过程

步骤 1 如果尚未登录，请登录 管理中心。

步骤 2 依次点击**策略** > **访问控制** > **身份**，然后创建或编辑身份策略。

步骤 3 （可选。）点击**添加类别**，为强制网络门户身份规则添加类别，然后为该类别输入一个**名称**。

步骤 4 点击**主动身份验证 (Active Authentication)**。

步骤 5 从列表中选择适当的 **服务器证书**，或者点击 **添加**（+） 以添加证书。

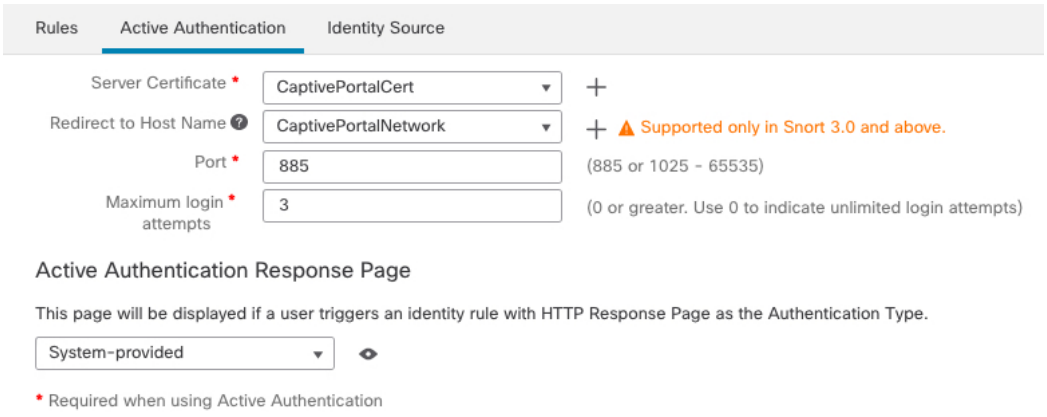
注释 强制网络门户 不 支持使用数字签名算法（DSA）或椭圆曲线数字签名算法（ECDSA）证书。

步骤 6 从 **重定向到主机名** 字段中，点击之前创建的网络对象。

步骤 7 在**端口**字段中输入 **885**，然后指定**最大登录尝试次数**。

步骤 8 （可选。）选择**主动身份验证响应页面**，如强制网络门户字段，第 1875 页中所述。

下图显示了一个示例。



步骤 9 点击**保存 (Save)**。

步骤 10 点击**规则 (Rules)**。

步骤 11 点击 **添加规则** 以添加新的强制网络门户身份策略规则，或者点击 **编辑**（ ） 以编辑现有规则。

步骤 12 为规则输入**名称 (Name)**。

步骤 13 从**操作**列表中，选择**主动身份验证**。

系统仅可对 HTTP 和 HTTPS 流量执行强制网络门户主动身份验证。如果身份规则 **操作** 为 **主动身份验证** （使用强制网络门户），或者如果使用被动身份验证，并将 **领域和设置** 页面上的选项选中为 **如果被动身份验证无法识别用户，则使用主动身份验证**，则请仅使用 TCP 端口约束。

步骤 14 点击 **领域和设置**。

步骤 15 从 **领域** 列表中，选择要用于用户身份验证的领域 。

不支持领域序列。

步骤 16 （可选。）选中**如果身份验证无法识别用户，则识别为访客**。有关详细信息，请参阅强制网络门户字段 ， 第 1875 页。

步骤 17 从列表中选择**身份验证协议**。

步骤 18 （可选。）要豁免强制网络门户中的特定应用流量，请参阅排除强制网络门户中的应用，第 1876 页。

步骤 19 向规则（端口、网络等）添加条件，如身份规则条件 ， 第 1889 页中所述。

步骤 20 点击 **Add**。

步骤 21 在该页面顶部，点击**保存**。

下一步做什么

继续执行配置强制网络门户第 3 部分：创建 TCP 端口访问控制规则 ， 第 1871 页。

配置强制网络门户第 3 部分：创建 TCP 端口访问控制规则

该程序的这一部分显示如何创建访问控制规则，以允许强制网络门户使用 TCP 端口 885（它是强制网络门户的默认端口）与客户端通信。如果您希望，也可以选择另一个端口，但该端口必须与您在配置强制网络门户第 2部分：创建身份策略 ， 第 1870 页中选择的端口匹配。

开始之前

有关整个强制网络门户配置的概述，请参阅如果为用户控制配置强制网络门户 ， 第 1867 页。

过程

步骤 1 如果尚未登录，请登录 管理中心。

步骤 2 如果尚未进行此操作，则请创建强制网络门户证书，如 PKI ， 第 1000 页中所述。

步骤 3 依次点击 **策略** > **访问控制** > **访问控制** 然后创建或编辑访问控制策略。

步骤 4 点击**添加规则**。

步骤 5 为规则输入**名称 (Name)**。

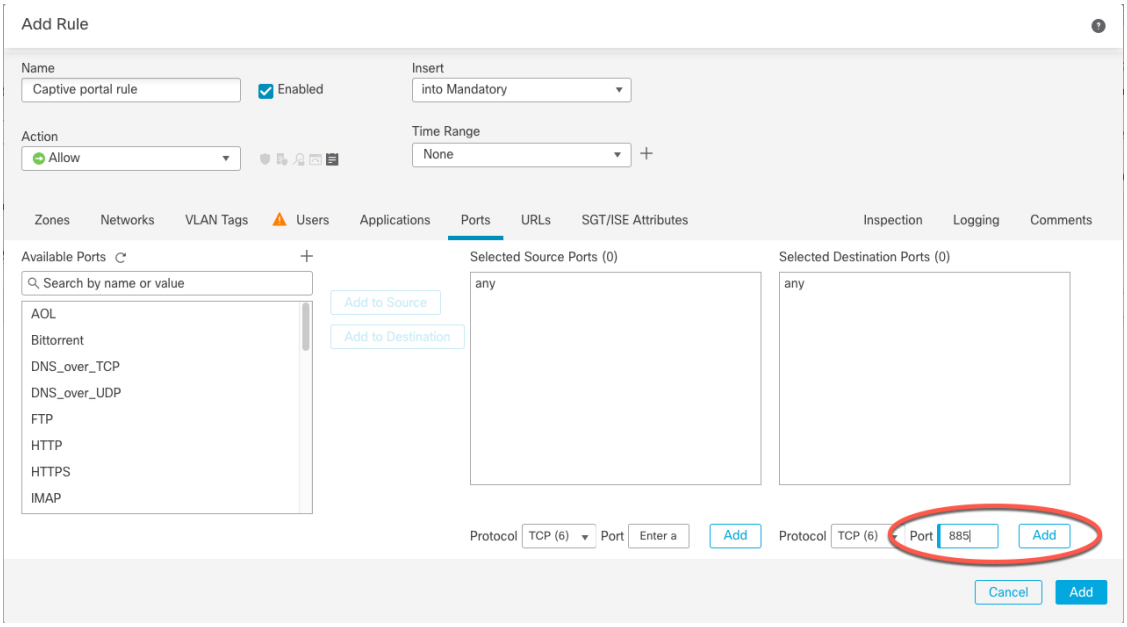
步骤 6 从**操作**列表中选择**允许**。

步骤 7 点击**端口**。

步骤 8 从**所选目标端口**字段下的**协议**列表中，选择 **TCP**。

步骤 9 在**端口**字段中，输入 **885**。

步骤 10 点击**端口**字段旁边的**添加**。
下图显示了一个示例。



步骤 11 点击页面底部的**添加**。

下一步做什么

继续执行配置强制网络门户第 4部分：创建用户访问控制规则 ， 第 1872 页。

配置强制网络门户第 4部分：创建用户访问控制规则

该过程的此部分讨论如何添加访问控制规则，以使领域中的用户能够使用强制网络门户进行身份验证。

开始之前

有关整个强制网络门户配置的概述，请参阅如果为用户控制配置强制网络门户 ， 第 1867 页。

过程

步骤 1 在规则编辑器中，点击**添加规则**。

步骤 2 为规则输入**名称 (Name)**。

步骤 3 从**操作**列表中选择**允许**。

步骤 4 点击“**用户**”。

步骤 5 在**可用领域**列表中，点击要允许的领域。

步骤 6 如果没有显示领域，则请点击 **刷新** （ ）。

步骤 7 在**可用用户**列表中，选择要添加到规则的用户，然后点击**添加到规则**。

步骤 8 （可选。）向访问控制策略添加条件，如身份规则条件，第 1889 页中所述。

步骤 9 点击 **Add**。

步骤 10 在访问控制规则页面上，点击**保存**。

步骤 11 在策略编辑器中，设置规则位置。点击并拖动，或使用右键点击菜单剪切并粘贴。规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。流量匹配的第一条规则是处理该流量的规则。适当的规则顺序可减少处理网络流量所需的资源，并防止规则抢占。

下一步做什么

继续执行配置强制网络门户第 5部分：创建 TLS/SSL 解密-重签策略，第 1873 页。

配置强制网络门户第 5部分：创建 TLS/SSL 解密-重签策略

程序的此部分介绍如何创建an SSL 策略，以在流量到达强制网络门户之前解密和重签流量。强制网络门户仅可对解密的流量进行身份验证。

开始之前

有关整个强制网络门户配置的概述，请参阅如果为用户控制配置强制网络门户，第 1867 页。

过程

步骤 1 如果尚未登录，请登录 管理中心。

步骤 2 如果尚未进行此操作，则请创建证书对象，以TLS/SSL流量进行解密，如PKI，第 1000 页中所述。

步骤 3 依次点击 **策略 (Policies)** > **访问控制 (Access Control)** > **SSL策略** > **访问控制** > **SSL**。

步骤 4 点击**新建策略**。

步骤 5 为策略输入**名称**，然后选择**默认操作**。默认操作将在SSL 策略 默认操作，第 1724 页中讨论。

步骤 6 点击**保存 (Save)**。

步骤 7 点击**添加规则**。

步骤 8 为规则输入**名称 (Name)**。

步骤 9 从**操作**列表中，选择**解密 - 放弃**。

步骤 10 从**使用**列表中，选择 PKI 对象。

步骤 11 点击“**用户**”。

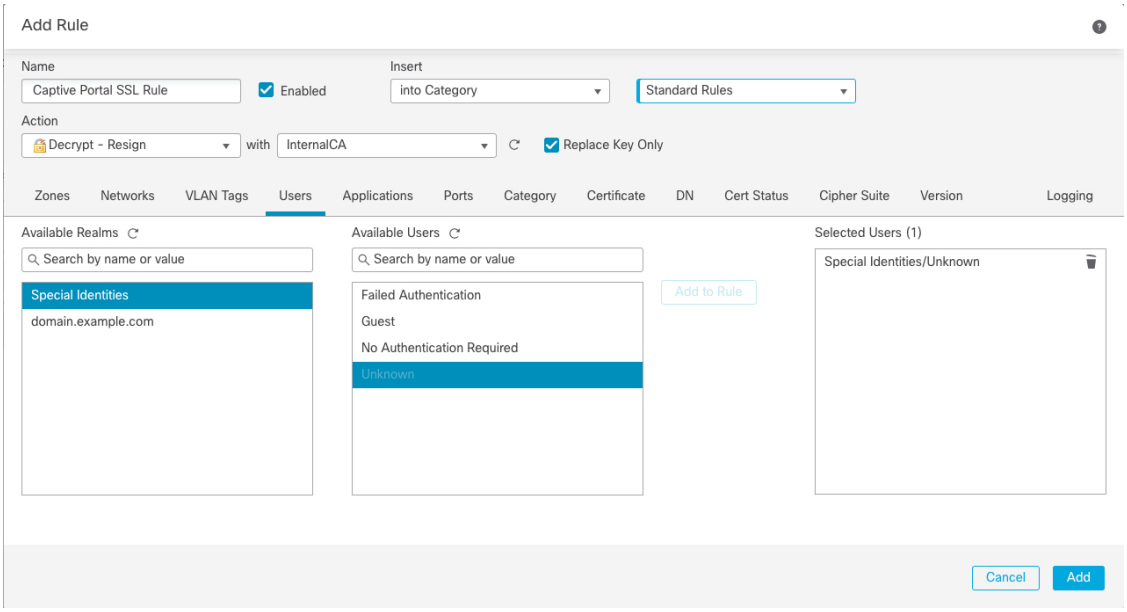
步骤 12 在 **可用领域** 列表上方，点击 **刷新** （ ）。

步骤 13 在**可用领域**列表中，点击**特殊身份**。

步骤 14 在**可用用户**列表中，点击**未知**。

步骤 15 点击**添加至规则**。

下图显示了一个示例。



步骤 16 （可选。）设置其他选项，如TLS/SSL 规则 条件 ， 第 1743 页中所述。

步骤 17 点击 **Add**。

步骤 18 在该页面顶部，点击**保存**。

下一步做什么

继续执行配置强制网络门户第 6 部分：将身份和 SSL 策略 与访问控制策略关联起来 ， 第 1874 页。

配置强制网络门户第 6 部分：将身份和 SSL 策略 与访问控制策略关联起来

该程序的这一部分讨论如何将身份策略和 TLS/SSL **解密 - 重新签名**规则与您先前创建的访问控制规则关联起来。在此之后，用户可以使用强制网络门户进行身份验证。

开始之前

有关整个强制网络门户配置的概述，请参阅如果为用户控制配置强制网络门户 ， 第 1867 页。

过程

步骤 1 点击**策略** > **访问控制** > **访问控制**，然后按照配置强制网络门户第 3 部分：创建 TCP 端口访问控制规则，第 1871 页中所述编辑您创建的访问控制策略。 如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 2 创建新的访问控制策略，或者编辑现有策略。

步骤 3 在该页面顶部，点击**身份策略**旁边的链接。

步骤 4 从该列表中，选择身份策略的名称，然后在该页面顶部，点击**保存**。

步骤 5 重复前面的步骤，以使强制网络门户 SSL 策略与访问控制策略相关联。

步骤 6 如果尚未进行此操作，则请将受管设备作为该策略的目标，如设置访问控制策略的目标设备，第 1269 页中所述。

下一步做什么

- 将身份和访问控制策略部署到受管设备，如部署配置更改，第 136 页中所述。
- 监控用户活动，。

强制网络门户字段

使用以下字段，在身份策略的**主动身份验证**选项卡页面上配置强制网络门户设置。另请参阅身份规则字段，第 1896 页和排除强制网络门户中的应用，第 1876 页。

服务器证书 (Server Certificate)

强制网络门户后台守护程序显示的服务器证书。

注释 强制网络门户 不 支持使用数字签名算法（DSA）或椭圆曲线数字签名算法（ECDSA）证书。

端口

要用于强制网络门户连接的端口号。

最大登录尝试次数 (Maximum login attempts)

系统拒绝用户登录请求前允许的最大失败登录尝试的次数。

主动身份验证响应页面 (Active Authentication Response Page)

要向强制网络门户用户显示的系统提供或自定义 HTTP 响应页面。在身份策略主动身份验证设置中选择**主动身份验证响应页面**后，还必须使用 **HTTP 响应页面**配置一个或更多个身份规则作为**身份验证协议**。

系统提供的 HTTP 响应页面包括**用户名 (Username)** 和**密码 (Password)** 字段，以及用于允许用户以访客身份访问网络的**以访客身份登录 (Login as guest)** 按钮。要显示单点登录方法，请配置自定义 HTTP 响应页面。

选择以下选项：

- 要使用通用响应，请选择**系统提供**。可以点击 **视图**（） 以查看此页面的 HTML 代码。
- 要创建自定义响应，请选择**自定义**。将显示一个具有系统提供的代码的窗口，您可以替换或修改该代码。完成时，保存更改。可以通过点击 **编辑**（） 来编辑自定义页面。

相关主题

内部证书对象，第 1008 页

排除强制网络门户中的应用

您可以选择应用（通过其 HTTP 用户-代理 字符串标识）并免于对它们执行强制网络门户主动身份验证。这允许所选应用的流量在未经身份验证的情况下通过身份策略。

注释 此列表中仅显示带有**用户代理排除标记**的应用。

过程

步骤 1 如果尚未登录，请登录 管理中心。

步骤 2 请点击 **策略** > **访问控制** > **身份** 。

步骤 3 编辑包含强制网络门户规则的身份策略。

步骤 4 在 **领域和设置** 选项卡页面上， 展开**HTTP 用户代理排除**。

- 在第一列中，选中要过滤应用的每个项目旁边的复选框，然后选择一个或多个应用，然后点击**添加到规则**。

  复选框与 ANDed 在一起。

- 要减少显示的过滤器，请在**按名称搜索**字段中键入搜索字符串；这对类别和标记尤其有用。要清除搜索，请点击 **清除**（）。
- 要刷新过滤器列表并清除所有所选过滤器，请点击 **重新加载** （）。

注释 该列表每次显示 100 个应用。

步骤 5 从**可用应用**列表中选择要添加到过滤器的应用：

- 要减少显示的应用，请在**按名称搜索**字段中输入搜索字符串。要清除搜索，请点击**清除**（）。
- 使用位于列表底部的页码可浏览各个可用应用的列表。

- 要刷新应用列表并清除所有所选应用，请点击 **重新加载** （ ）。

步骤 6 添加所选应用以免除外部身份验证。可以点击并拖动，也可以点击**添加到规则 (Add to Rule)**。由此则得到您所选的应用过滤器组合。

下一步做什么

- 继续配置身份规则，如创建身份规则，第 1894 页中所述。

强制网络门户身份源故障排除

有关其他相关故障排除信息，请参阅领域和用户下载故障排除，第 1837 页和用户控制故障排除。

如果您遇到强制网络门户证问题，请检查以下事项：

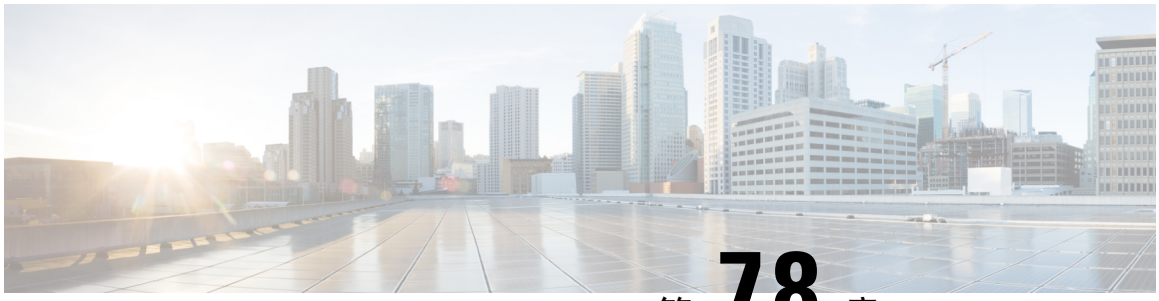
- 强制网络门户托管设备上的时间必须与 管理中心上的时间同步。
- 如果您已配置DNS解析并创建了身份规则来执行**Kerberos**（或**HTTP 协商**，如果希望Kerberos作为选项）强制网络门户，则必须配置 DNS 服务器来解析强制网络门户设备的完全限定域名 (FQDN)。FQDN 必须与您配置 DNS 时提供的主机名匹配。

  有关详细信息，请参阅关于主机名重定向，第 1864 页。
- 如果使用 Kerberos 身份验证，则受管设备的主机名必须少于 15 个字符（这是 Windows 设置的 NetBIOS 限制）；否则，强制网络门户身份验证失败。您在设置设备时设置受管设备主机名。有关详细信息，请参阅 Microsoft 文档网站上的此类文章： Active Directory 中计算机、域、站点和 OU 的命名约定。
- DNS 必须向主机名返回 64KB 或更少的响应；否则，测试连接 AD 连接失败。此限制在两个方向上都适用，将在 RFC 6891 第 6.2.5 节中讨论。
- 如果强制网络门户配置正确，但重定向到 IP 地址或完全限定域名 (FQDN) 失败，请禁用终端安全软件。此类软件可能会干扰重定向。
- 如果您选择**Kerberos**（或**HTTP 协商**，如果您要将Kerberos作为一个选项）作为身份规则的**身份验证类型**，则您选择的**领域**必须配置**AD 加入用户名**和**AD 加入密码**，以便执行Kerberos强制网络门户主动身份验证。
- 如果选择**HTTP 基本身份验证**作为身份规则中的**身份验证类型**，则您的网络上的用户可能不会注意到其会话超时。大多数 Web 浏览器会从 HTTP 基本身份验证登录中缓存凭证，并在旧会话超时后使用这些凭证无缝开始新会话。
- 如果您的管理中心和受管设备之间的连接失败，则无法在停机期间识别设备报告的所有强制网络门户登录，除非以前查看过这些用户并已将他们下载到管理中心。无法识别的用户在管理中心上记录为“未知”(Unknown) 未知用户。停机时间过后，系统将根据身份策略中的规则重新识别和处理“未知”(Unknown) 用户。

- 如果要用于强制网络门户的设备包含内联接口和路由接口，则必须在强制网络门户身份规则中配置区域条件，以便仅针对强制网络门户设备上的路由接口。
- 受管设备的主机名必须少于 15 个字符，Kerberos 身份验证才能成功。
- 确保用户注销的唯一方法是关闭并重新打开浏览器。除非发生这种情况，否则在某些情况下，用户可以注销强制网络门户，并且能够在不使用同一浏览器再次进行身份验证的情况下访问网络。
- 活动 FTP 会话在事件中显示为**Unknown**用户。此为正常现象，因为在活动 FTP 中，会由服务器（而非客户端）发起连接，而 FTP 服务器则不应具有关联的用户名。有关活动 FTP 的详细信息，请参阅 RFC 959。
- 当强制网络门户对与身份规则匹配的用户进行身份验证时，Active Directory 或 LDAP 组中尚未下载的任何 Microsoft 用户都将被识别为“未知”。为避免用户被识别为未知，请将领域配置为下载您希望通过强制网络门户进行身份验证的所有组中的用户。未知用户根据关联的访问控制策略处理；如果访问控制策略配置为阻止未知用户，则会阻止这些用户。

  要确保系统下载领域中的所有用户，请确保组位于领域配置的可用组列表中。

  有关详细信息，请参阅同步用户和组，第 1827 页。



第 78 章

通过远程接入 VPN 的用户控制

以下主题讨论如何通过远程接入 VPN 执行用户感知和用户控制：

远程接入 VPN 身份源

AnyConnect 是终端设备上通过远程 VPN 连接 威胁防御 设备的唯一受支持客户端。

按照创建新的远程接入 VPN 策略，第 1142 页中的描述设置安全 VPN 网关时，您可以为这些用户设置一个身份策略，并将该身份策略与访问控制策略关联，前提是您的用户位于 Active Directory 存储库中。

注释 如果使用具有用户身份和 RADIUS 作为身份源的远程访问 VPN，则必须配置领域（**对象 (Objects) > 对象管理 (Object Management) > AAA 服务器 (AAA Server) > RADIUS 服务器组 (RADIUS Server Group)**）。

远程用户提供的登录信息由 LDAP 或 AD 领域或 RADIUS 服务器组进行验证。这些实体与 Cisco Secure Firewall Threat Defense 安全网关相集成。

注释 如果用户使用 Active Directory 作为身份验证源通过远程访问 VPN 进行身份验证，则用户必须使用其用户名登录；`domain\username` 或 `username@domain` 格式无效。（Active Directory 将此用户名视为 *logon* 名称，有时也视为 `sAMAccountName`。）有关详细信息，请参阅 MSDN 上的用户命名属性。

如果使用 Radius 进行身份验证，用户可以使用上述任何一种格式登录。

通过 VPN 连接进行身份验证后，远程用户将接受 *VPN* 身份。Cisco Secure Firewall Threat Defense安全网关上的身份策略将使用此 VPN 身份来识别和过滤属于此远程用户的网络流量。

身份策略与访问控制策略相关联，后者用于确定哪些人有权访问网络资源。使用访问控制策略可阻止或允许远程用户访问您的网络资源。

相关主题

VPN 概述，第 1089 页
Cisco Secure Firewall Threat Defense 远程接入 VPN 概述，第 1131 页
VPN 基础知识，第 1090 页
远程接入 VPN 功能，第 1132 页
远程接入 VPN 的准则和限制，第 1138 页
创建新的远程接入 VPN 策略，第 1142 页

配置用户控制 RA VPN

开始之前

- 按创建 Active Directory 领域和领域目录，第 1816 页中所述创建领域。
- 要使用身份验证、授权和审核 (AAA)，请按照添加 RADIUS 服务器组，第 970 页中的讨论设置 RADIUS 服务器组。

过程

步骤 1 登录管理中心。

步骤 2 点击**设备** > **VPN** > **远程访问**。

步骤 3 请参阅创建新的远程接入 VPN 策略，第 1142 页。

下一步做什么

- 使用创建身份策略，第 1887 页中所述的身份策略指定要控制的用户和其他选项。
- 按将其他策略与访问控制相关联，第 1276 页中所述，将身份规则与可以过滤和选择性检查流量的访问控制策略相关联。
- 将身份和访问控制策略部署到受管设备，如部署配置更改，第 136 页中所述。
- 按 VPN 会话和用户信息中所述，监视 VPN 用户流量 。

远程接入 VPN 身份源故障排除

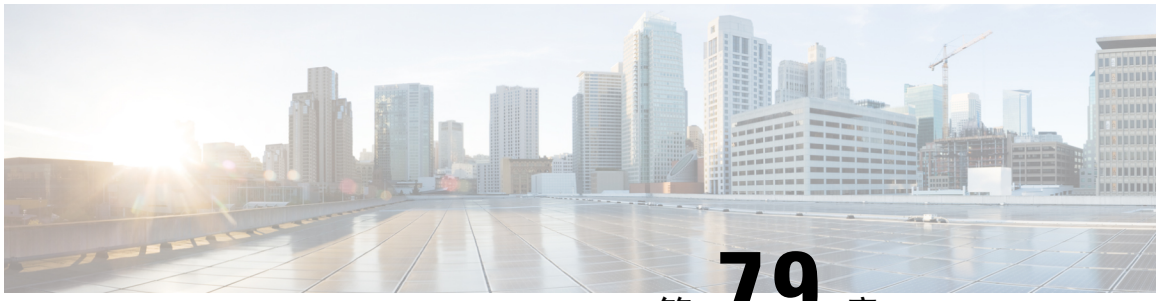
- 有关其他相关故障排除信息，请参阅领域和用户下载故障排除，第 1837 页和用户控制故障排除和VPN 故障排除。

- 如果遇到远程接入 VPN 问题，请检查 管理中心和受管设备之间的连接。如果连接失败，则无法在停机期间识别设备报告的所有远程接入VPN登录，除非以前查看过这些用户并已将他们下载到 管理中心。

  无法识别的用户在 管理中心上记录为未知用户。停机时间过后，系统将根据身份策略中的规则重新识别和处理“未知”用户。

- 受管设备的主机名必须少于 15 个字符，Kerberos 身份验证才能成功。

- 活动 FTP 会话在事件中显示为**Unknown**用户。此为正常现象，因为在活动 FTP 中，会由服务器（而非客户端）发起连接，而 FTP 服务器则不应具有关联的用户名。有关活动 FTP 的详细信息，请参阅 RFC 959。



第 79 章

通过 TS 代理的用户控制

要将 TS 代理用作用户感知和用户控制的身份源，请按照《思科终端服务 (TS) 代理指南》中所述安装和配置 TS 代理软件。

下一步做什么：

- 使用创建身份策略， 第 1887 页中所述的身份策略指定要控制的用户和其他选项。
- 按将其他策略与访问控制相关联，第 1276 页中所述，将身份规则与可以过滤和选择性检查流量的访问控制策略相关联。
- 将身份和访问控制策略部署到受管设备，如部署配置更改， 第 136 页中所述。
- 监控用户活动，。

终端服务 (TS) 代理身份源

TS 代理是一种被动身份验证方式，并且是系统支持的授权身份源之一。Windows 终端服务器执行身份验证，然后 TS 代理将其报告给独立版或高可用性的 管理中心。

当安装在 Windows 终端服务器上时，TS 代理在个人用户登录或注销受监控网络时向其分配唯一端口范围。管理中心使用唯一端口识别系统中的个人用户。您可以使用一个 TS 代理监控一台 Windows 终端服务器上的用户活动，并将加密数据发送到一个 管理中心。

TS 代理不报告失败的登录尝试。从 TS 代理获取的数据可用于用户感知和用户控制。

TS 代理准则

TS 代理需要多步骤配置，并且包括以下内容：

1. 已安装并配置 TS 代理的 Windows 终端服务器。

2. 一个或多个针对服务器所监控用户的身份领域。

在 Microsoft Windows 终端服务器上安装 TS 代理。有关多步骤 TS 代理安装和配置的详细信息以及服务器和 Firepower 系统要求的全面介绍，请参阅《思科终端服务 (TS) 代理指南》。

TS 代理数据显示在“用户”(Users)、“用户活动”(User Activity) 和“连接事件”(Connection Event) 表中，并可用于用户感知和用户控制。

注释 如果 TS 代理监控与其他被动身份验证身份源（ISE/ISE-PIC）相同的用户，则 管理中心 会划分 TS 代理数据的优先级。如果 TS 代理和另一个被动身份源通过同一 IP 地址报告活动，则仅会将 TS 代理数据记录到 管理中心。

通过 TS 代理的用户控制

要将 TS 代理用作用户感知和用户控制的身份源，请按照《思科终端服务 (TS) 代理指南》中所述安装和配置 TS 代理软件。

下一步做什么：

- 使用创建身份策略，第 1887 页中所述的身份策略指定要控制的用户和其他选项。
- 按将其他策略与访问控制相关联，第 1276 页中所述，将身份规则与可以过滤和选择性检查流量的访问控制策略相关联。
- 将身份和访问控制策略部署到受管设备，如部署配置更改，第 136 页中所述。
- 监控用户活动，。

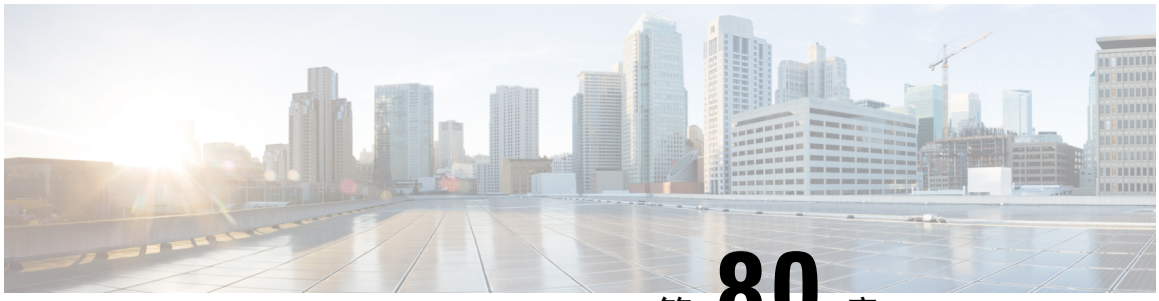
TS 代理身份源故障排除

有关其他相关故障排除信息，请参阅领域和用户下载故障排除，第 1837 页和用户控制故障排除。

如果您遇到 TS 代理与 Firepower 系统的集成问题，请检查以下事项：

- 您必须将 TS 代理服务器上的时间与 管理中心上的时间进行同步。
- 如果 TS 代理监控与其他被动身份验证身份源（ISE/ISE-PIC）相同的用户，则 管理中心 会划分 TS 代理数据的优先级。如果 TS 代理和一个被动身份源通过同一 IP 地址报告活动，则仅会将 TS 代理数据记录到 管理中心。
- 活动 FTP 会话在事件中显示为**Unknown**用户。此为正常现象，因为在活动 FTP 中，会由服务器（而非客户端）发起连接，而 FTP 服务器则不应具有关联的用户名。有关活动 FTP 的详细信息，请参阅 RFC 959。

有关故障排除更多信息，请参阅 《思科终端服务 (TS) 代理指南》。



第 80 章

用户身份策略

以下主题讨论如何创建和管理身份规则及身份策略：

关于身份策略

身份策略包含身份规则。身份规则会将流量集与领域和身份验证方法相关联：被动身份验证、主动身份验证或无身份验证。

除了下面段落提到的例外之外，您必须配置计划使用的领域和身份验证方法，然后才能在身份规则中进行调用：

- 在**系统 (System)** > **集成 (Integration)** > **领域 (Realms)**中，配置身份策略外的领域。有关详细信息，请参阅创建 Active Directory 领域和领域目录， 第 1816 页。
- 在 **系统** > **集成** > **身份源**中，配置 ISE/ISE-PIC 被动身份验证身份源。有关详细信息，请参阅配置用户控制 ISE/ISE-PIC， 第 1858 页。
- 在 Firepower 系统外，配置被动身份验证身份源：TS 代理。有关详细信息，请参阅《思科终端服务 *(TS)* 代理指南》。
- 在身份策略中，配置主动身份验证身份源：强制网络门户。有关详细信息，请参阅如果为用户控制配置强制网络门户， 第 1867 页。
- 您可以在远程接入 VPN 策略中配置远程接入 VPN，即主动身份验证身份源。有关详细信息，请参阅远程访问 VPN 身份验证， 第 1134 页。

向一个身份策略添加多个身份规则后，对规则排序。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。流量匹配的第一个规则是处理该流量的规则。

您可以选择配置身份策略，以按网络对象过滤流量，从而在设备达到或接近其内存限制时限制每个设备监控的网络。设备必须运行 威胁防御 6.7 或更高版本，才能对其应用网络过滤。

配置一个或多个身份策略后，必须将一个身份策略与访问控制策略相关联。当网络上的流量与身份规则中的条件匹配时，系统会将流量与指定领域相关联并使用指定身份源对流量中的用户进行身份验证。

如果不配置身份策略，则系统不会执行用户身份验证。

创建身份策略的例外

如果满足以下所有条件，则不需要身份策略：

- 您使用 ISE/ISE-PIC 身份源。
- 您未在访问控制策略中使用用户或组。
- 您在访问控制策略中使用安全组标记 (SGT)。有关详细信息，请参阅ISE SGT 与自定义 SGT 规则条件。

相关主题

如何设置身份策略 ，第 1800 页

身份策略的许可证要求

威胁防御 许可证

任意

经典许可证

控制

身份策略的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

创建身份策略

开始之前

在访问控制策略内使用领域中的用户和组需要身份策略。创建并启用一个或多个领域，如创建 Active Directory 领域和领域目录， 第 1816 页中所述。

（可选。）如果特定受管设备监控大量用户组，则由于内存限制，系统可能会根据组丢弃用户映射。因此，带有领域或用户条件的规则可能不会按预期执行。如果设备运行的是版本 6.7 或更高版本，您可以将身份规则配置为仅按一个网络或网络组对象监控流量。要创建网络对象，请参阅创建网络对象， 第 999 页。

如果满足以下所有条件，则不需要身份策略：

- 您使用 ISE/ISE-PIC 身份源。
- 您未在访问控制策略中使用用户或组。
- 您在访问控制策略中使用安全组标记 (SGT)。有关详细信息，请参阅ISE SGT 与自定义 SGT 规则条件。

过程

步骤 1 登录管理中心。

步骤 2 点击**策略** > **访问控制** > **身份**，然后点击**新建策略**。

步骤 3 输入**名称 (Name)** 和**说明 (Description)**（后者为可选项）。

步骤 4 点击**保存 (Save)**。

步骤 5 要将规则添加到策略，请点击**添加规则**，如创建身份规则， 第 1894 页中所述。

步骤 6 要创建规则类别，请点击**添加类别**。

步骤 7 要配置强制网络门户主动身份验证，请点击 **主动身份验证**，如配置强制网络门户第 2部分：创建身份策略， 第 1870 页中所述。

步骤 8 （可选。）要按网络对象过滤流量，请点击 **身份源** 选项卡。从列表中，点击要用于过滤此身份策略流量的网络对象。点击 **添加**（+） 以创建新的网络对象。

步骤 9 点击**保存 (Save)** 保存身份策略。

下一步做什么

- 将规则添加到指定要匹配的用户和其他选项的身份策略；请参阅创建身份规则，第 1894 页。
- 将身份策略与访问控制策略相关联，以允许或阻止选定用户访问指定的资源；请参阅将其他策略与访问控制相关联，第 1276 页。
- 将配置更改部署到受管设备；请参阅部署配置更改，第 136 页。

如果您遇到问题，请参阅用户控制故障排除。

相关主题

配置强制网络门户第 2部分：创建身份策略，第 1870 页
创建身份映射过滤器，第 1888 页
强制网络门户字段，第 1875 页
用户控制故障排除

创建身份映射过滤器

身份映射过滤器可用于限制应用身份规则的网络。例如，如果您的 管理中心 管理的FTD 内存有限，则可以限制其监控的网络。

开始之前

执行以下任务：

1. 创建身份策略所需的领域。请参阅创建 Active Directory 领域和领域目录，第 1816 页。
2. 创建身份策略。请参阅创建身份策略，第 1887 页。
3. （可选。）创建网络对象或网络组对象，如创建网络对象，第 999 页中所述。您创建的网络对象或组应定义您希望托管设备在身份策略中监控的网络。

   此步骤为可选，因为您可以在配置身份映射过滤器时创建一个。

过程

步骤 1 登录管理中心。

步骤 2 点击**策略 (Policies)** > **身份 (Identity)**。

步骤 3 请点击 **编辑**（  ）。

步骤 4 点击**身份源 (Identity Source)** 选项卡。

步骤 5 从**身份映射过滤器 (Identity Mapping Filter)** 列表中，点击要用作过滤器的网络对象的名称，或点击**加号**（  ） 以创建新的过滤器。

要创建新的网络对象，请参阅创建网络对象，第 999 页。

步骤 6 点击**保存 (Save)**。

下一步做什么

将身份策略与访问控制策略相关联，如将其他策略与访问控制相关联，第 1276 页中所述。

身份规则条件

通过规则条件，您可以微调身份策略，以您要控制的用户和网络为目标。有关详细信息，请参阅以下各节之一：

相关主题

安全区域规则条件，第 1380 页
网络规则条件，第 607 页
VLAN 标记规则条件，第 1292 页
端口规则条件，第 609 页
领域和设置规则条件，第 1893 页

安全区域规则条件

安全区域可对网络进行分段，以通过跨多个设备将接口分组来帮助管理和分类流量。

区域规则条件可根据其源和目标安全区域控制流量。如果将源区域和目标区域均添加到区域条件中，则匹配流量必须源自其中一个源区域的接口，并通过其中一个目标区域的接口流出。

正如区域中的所有接口都必须为同一类型（均为内联、被动、交换或路由），区域条件中使用的所有区域也必须为同一类型。由于被动部署的设备不会传输流量，因此不能使用具有被动接口的区域作为目标区域。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

提示 按区域限制规则是提高系统性能的一种最佳方式。如果规则不适用于通过设备任意接口的流量，则该规则不影响该设备的性能。

安全区域条件和多租户

在多域部署中，在祖先域中创建的区域可以包含位于不同域中的设备上的接口。在后代域中配置区域条件时，您的配置仅适用于可以看到的接口。

网络规则条件

网络规则条件使用内部报头按流量的源和目标 IP 地址来控制流量。使用外部报头的隧道规则具有隧道终端条件而不是网络条件。

您可以使用预定义对象构建网络条件，或手动指定单个 IP 地址或地址块。

注释 您 不能 在身份规则中使用 FDQN 网络对象。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

重定向到主机名网络规则条件

（仅限 Snort 3.0）—你可以使用一个网络对象，其中包含强制网络门户可用于主动认证请求的接口的完全限定主机名（FQDN）。

FQDN 必须解析为受管设备上接口之一的 IP 地址。通过使用 FQDN，您可以为客户端将识别的主动身份验证分配证书，从而避免用户在被重定向到受管设备的 IP 地址时收到不受信任证书警告。

证书可以在证书的使用者替代名称 (SAN) 中指定一个 FQDN、通配符 FQDN 或多个 FQDN。

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

如果您不提供重定向到主机名 FQDN，HTTP Basic、HTTP 响应页面和 NTLM 身份验证方法会使用接口的 IP 地址将用户重定向到强制网络门户。但对于 HTTP 协商，用户将使用完全限定 DNS 名称 *firewall-hostname*.*directory-server-domain-name*进行重定向。要在不提供重定向到主机名 FQDN 的情况下使用 HTTP 协商，还必须更新 DNS 服务器以将此名称映射到您需要进行主动身份验证的所有内部接口的 IP 地址。否则，将无法进行重定向，用户也无法进行身份验证。

建议您始终提供重定向到主机名 FQDN 以确保行为一致，而无论采用哪种身份验证方法。

VLAN 标记规则条件

注释 访问规则中的 VLAN 标记仅适用于内联集。带 VLAN 标记的访问规则与防火墙接口上的流量不匹配。

VLAN 规则条件可控制 VLAN 标记的流量，包括 Q-in-Q（堆栈 VLAN）流量。系统使用最内层的 VLAN 标记过滤 VLAN 流量，但不包括预过滤器策略，因为它在其规则中使用最外层的 VLAN 标记。

请注意以下 Q-in-Q 支持：

- Firepower 4100/9300 上的威胁防御 -不支持 Q-in-Q （仅支持一个 VLAN 标记）。
- 所有其他型号上的威胁防御 ：
  - 内联集和被动接口-支持 Q-in-Q，最多2个 VLAN 标记。
  - 防火墙接口-不支持 Q-in-Q （仅支持一个 VLAN 标记）。

可以使用预定义对象构建 VLAN 条件，或手动输入从 1 到 4094 之间的任意 VLAN 标记。使用连字符可指定 VLAN 标记范围。

最多可以指定 50 个 VLAN 条件。

在集群中，如果遇到 VLAN 匹配问题，请编辑访问控制策略高级选项“传输/网络预处理器设置”(Transport/Network Preprocessor Settings)，然后选择**跟踪连接时忽略 VLAN 信头 (Ignore the VLAN header when tracking connections)** 选项。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 VLAN 标记限制此配置可产生意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

端口规则条件

通过端口条件，您可以按流量的源端口和目标端口控制该流量。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

基于端口的规则的最佳实践

指定端口是目标应用的传统方式。但是，可以将应用配置为使用唯一端口绕过访问控制块。因此，尽可能使用应用过滤条件而不是端口条件来确定流量目标。

应用过滤也建议用于动态打开单独通道的应用（如 FTD），以实现控制和数据流。使用基于端口的访问控制规则可能会阻止此类应用正确执行，并可能导致阻止所需的连接。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为源端口条件。

端口、协议和 ICMP 代码规则条件

端口条件根据源和目标端口匹配流量。根据规则类型，“端口”可以表示以下任何一项：

- TCP 和 UDP - 可以根据端口控制 TCP 和 UDP 流量。系统使用括号内的协议号，以及可选的关联端口或端口范围来表示此配置。例如：TCP(6)/22。
- ICMP - 可以根据 ICMP 和 ICMPv6 (IPv6-ICMP) 流量的互联网层协议及可选类型和代码控制该流量。例如：ICMP(1):3:3。
- 协议-您可以借助于未使用端口的其他协议控制流量。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

基于端口的规则的最佳实践

指定端口是目标应用的传统方式。但是，可以将应用配置为使用唯一端口绕过访问控制块。因此，尽可能使用应用过滤条件而不是端口条件来确定流量目标。请注意，应用过滤在预过滤器规则中不可用。

应用过滤也建议用于动态打开单独通道的应用（如 FTP），以实现控制和数据流。使用基于端口的访问控制规则可能会阻止此类应用正确执行，并可能导致阻止所需的连接。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为目标端口条件。

将非 TCP 流量与端口条件相匹配

您可以匹配非基于端口的协议。默认情况下，如果不指定端口条件，则匹配 IP 流量。虽然可以将端口条件配置为与非 TCP 流量相匹配，但有一些限制：

- 访问控制规则 - 对于典型设备，可以通过使用 GRE (47) 协议作为目标端口条件将 GRE 封装的流量与访问控制规则相匹配。对于 GRE 限制的规则，只能添加基于网络的条件：区域、IP 地址、端口和 VLAN 标签。此外，系统使用外部报头将访问控制策略中的**所有**流量与 GRE 限制的规则相匹配。对于 威胁防御设备，请使用预过滤器策略中的隧道规则来控制 GRE 封装的流量。
- SSL 规则 - SSL 规则仅支持 TCP 端口条件。
- IMCP 回应 - 类型设置为 0 的目标 ICMP 端口或类型设置为 129 的目标 ICMPv6 端口仅与主动回应回复相匹配。为应答 ICMP 回应请求而发送的 ICMP 回应回复被忽略。为使某个规则匹配任何 ICMP 回应，请使用 ICMP 类型 8 或 ICMPv6 类型 128。

领域和设置规则条件

通过**领域和设置 (Realm & Settings)** 选项卡页面，您可以选择要应用身份规则的领域或领域序列。如果您使用的是强制网络门户，则还可以选择其他选项。

选择领域或领域序列

从**领域 (Realm)** 列表中，点击领域或领域序列。

包含要对其执行指定**操作 (Action)** 的用户的领域或领域序列。必须在选择作为身份规则中的领域或领域序列之前，对领域进行完全配置。

注释 如果启用了 VPN 远程接入，而且您的部署正在使用 RADIUS 服务器组进行 VPN 身份验证，请确保您指定的领域与此 RADIUS 服务器组相关联。

仅主动身份验证：其他选项

如果选择**主动身份验证 (Active Authentication)** 作为身份验证类型，或者选中**如果无法建立被动或 VPN 身份则使用主动身份验证 (Use active authentication if passive or VPN identity cannot be established)** 框，您将看到以下选项。

如果无法建立被动或 VPN 身份，请使用主动身份验证

如果被动身份验证或VPN身份验证无法标识用户，选择此选项将通过强制网络门户主动身份验证来验证用户。您必须在身份策略中配置强制网络门户主动身份验证，才能选择此选项。

如果禁用此选项，没有 VPN 身份或被动身份验证不能标识的用户将被标识为“未知”。

如果身份验证无法识别用户，则识别为特殊身份/访客 (Identify as Special Identities/Guest if authentication cannot identify user)

选择此选项允许执行强制网络门户主动身份验证时而失败指定次数的用户以访客身份访问您的网络。这些用户显示在以其用户名（如果 AD 或 LDAP 服务器中有他们的用户名）或**访客**（如果他们的用户名未知）标识的 管理中心 中。其领域是在身份规则中指定的领域。（默认情况下，失败的登录次数为 3。）

仅当您将**主动身份验证**（即，强制网络门户身份验证）配置为规则**操作**时，才会显示此字段。

身份验证协议

要用于执行强制网络门户主动身份验证的方法。选项因领域、LDAP 或 AD 的类型而有所不同。

- 如果要使用未加密的 HTTP 基本身份验证 (BA) 连接对用户进行身份验证，请选择 **HTTP 基本身份验证**。用户通过其浏览器的默认身份验证弹出窗口登录网络。

  大多数 Web 浏览器会从 HTTP 基本身份验证登录中缓存凭证，并在旧会话超时后使用这些凭证无缝开始新会话。

- 选择 **NTLM** 以使用 NT LAN Manager (NTLM) 连接对用户进行身份验证。仅在选择 AD 领域时，此选项才可用。如果在用户的浏览器中配置了透明身份验证，则该用户自动登录。如果未配置透明身份验证，则用户使用其浏览器的默认身份验证弹出窗口进行登录。
- 选择**Kerberos**以使用Kerberos连接对用户进行身份验证。仅在为已启用安全LDAP (LDAPS)的服务器选择 AD 领域时，此选项才可用。如果在用户的浏览器中配置了透明身份验证，则该用户自动登录。如果未配置透明身份验证，则用户使用其浏览器的默认身份验证弹出窗口进行登录。

注释 您选择的**领域**必须配置**AD 加入用户名**和**AD 加入密码**，才能执行 Kerberos 强制网络门户主动身份验证。

注释 如果您要创建身份规则来执行 Kerberos 强制网络门户，并且已配置了 DNS 解析，则必须配置 DNS 服务器来解析强制网络门户设备的完全限定域名 (FQDN)。FQDN 必须与您配置 DNS 时提供的主机名匹配。

对于 威胁防御 设备，FQDN 必须解析为用于强制网络门户的路由接口的 IP 地址。

- 选择**HTTP 协商**以允许强制网络门户服务器选择“HTTP 基本”、“Kerberos”或“NTLM”进行身份验证连接。仅在选择 AD 领域时，此类型才可用。

注释 您选择的**领域**必须配置**AD 加入用户名**和**AD 加入密码**，这样一来，**HTTP 协商**才能选择 Kerberos 强制网络门户主动身份验证。

注释 如果您要创建身份规则来执行 **HTTP 协商**强制网络门户，并且已配置了 DNS 解析，则必须配置 DNS 服务器来解析强制网络门户设备的完全限定域名 (FQDN)。用于强制网络门户的设备的 FQDN 必须与您配置 DNS 时提供的主机名匹配。

创建身份规则

有关身份规则的配置选项的详细信息，请参阅身份规则字段 ， 第 1896 页。

开始之前

您必须创建并启用领域 或领域序列。

- 创建 Microsoft Active Directory 领域和领域目录，如创建 Active Directory 领域和领域目录，第 1816 页所述。
- 下载用户和组并启用领域，如 同步用户和组，第 1827 页中所述。
- （可选。）按创建领域序列，第 1828 页中所述创建领域序列。

注意 在禁用了 SSL 解密（即，当访问控制策略不包括 SSL 策略时）时添加第一个主动身份验证规则或删除最后一个主动身份验证规则在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。

请注意，主动身份验证规则具有 **主动身份验证** 规则操作或 **被动身份验证** 规则操作，并且 **如果无法建立被动或 VPN 识别，则使用主动身份验证** 已选中。

过程

步骤 1 登录管理中心。

步骤 2 请点击 **策略** > **访问控制** > **身份** 。

步骤 3 点击要将身份规则添加到的身份策略旁边的 **编辑**（ ）。

如果显示**视图**（ ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击**添加规则**。

步骤 5 输入 **Name**。

步骤 6 指定规则是否为 **Enabled**。

步骤 7 要将规则添加到现有类别，请指明要**插入**规则的位置。要添加新类别，请点击**添加类别**。

步骤 8 从列表中选择一个规则**操作**。

步骤 9 如果您正在配置强制网络门户，请参阅如果为用户控制配置强制网络门户，第 1867 页。

步骤 10 （可选）要向身份规则中添加条件，请参阅身份规则条件，第 1889 页。

步骤 11 点击**添加 (Add)**。

步骤 12 在策略编辑器中，设置规则位置。点击并拖动，或使用右键点击菜单剪切并粘贴。规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。流量匹配的第一条规则是处理该流量的规则。适当的规则顺序可减少处理网络流量所需的资源，并防止规则抢占。

步骤 13 点击**保存 (Save)**。

下一步做什么

- 部署配置更改。

身份规则字段

使用以下字段配置身份规则。

启用

启用此选项可启用身份策略中的身份规则。取消选择此选项可禁用身份规则。

操作

指定要对指定领域中的用户执行的身份验证的类型：**被动身份验证**（默认）、**主动身份验证**或**无身份验证**。必须完全配置身份验证方法或身份源，然后再选择其作为身份规则中的操作。

此外，如果启用了 VPN（至少在一台受管设备上配置），远程接入 VPN 会话将通过 VPN 进行主动身份验证。其他会话使用规则操作。这意味着，如果启用了 VPN，会首先确定所有会话的 VPN 身份，而不考虑所选的操作。如果在指定领域发现 VPN 身份，将使用此身份源。不再执行任何其他强制网络门户主动身份验证，即便已选择。

如果未发现 VPN 身份源，该过程将根据指定操作继续。不能将身份策略仅限制为仅使用 VPN 身份验证，因为如果未找到 VPN 身份源，将根据所选的操作应用规则。

⚠

注意 在禁用了 SSL 解密（即，当访问控制策略不包括 SSL 策略时）时添加第一个主动身份验证规则或删除最后一个主动身份验证规则在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。

请注意，主动身份验证规则具有 **主动身份验证** 规则操作或 **被动身份验证** 规则操作，并且 **如果无法建立被动或 VPN 识别，则使用主动身份验证** 已选中。

有关您的 Firepower 系统版本支持哪些被动和主动身份验证方法的信息，请参阅关于用户身份源，第 1792 页。

管理身份策略

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 登录管理中心。

步骤 2 请点击 **策略** > **访问控制** > **身份** 。

步骤 3 要删除策略，请点击 **删除**（🗑）。 如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 要编辑策略，请点击策略旁边的 **编辑**（✎）并进行更改，如创建身份策略，第 1887 页中所述。 如果显示**视图**（👁），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 5 要复制策略，请点击 **复制**（）。

步骤 6 要生成该策略的报告，请点击 **报告**（），如生成当前策略报告，第 149 页中所述。

步骤 7 要比较策略，请参阅比较策略，第 148 页。

步骤 8 要创建用于组织策略的文件夹，请点击**添加类别 (Add Category)**。

下一步做什么

部署配置更改。

管理身份规则

过程

步骤 1 登录管理中心。

步骤 2 请点击 **策略** > **访问控制** > **身份** 。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 如创建身份策略，第 1887 页中所述，要编辑身份规则，请点击 **编辑**（） 并进行更改。

步骤 5 要删除身份规则，请点击 **删除**（）。

步骤 6 要创建规则类别，请点击**添加类别**并选择位置和规则。

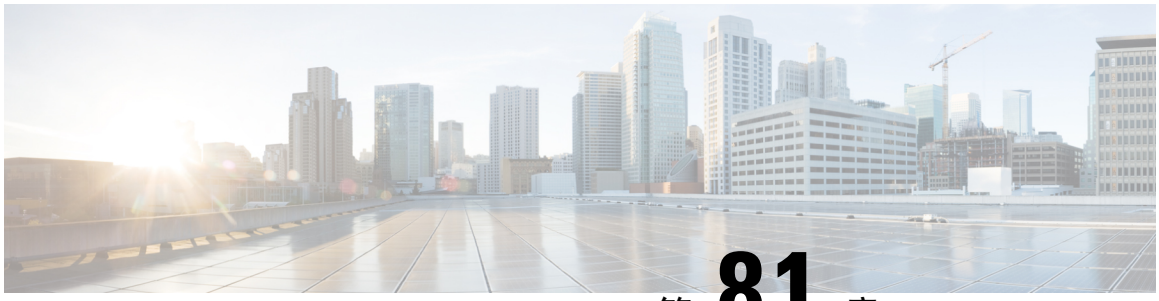
步骤 7 点击**保存 (Save)**。

下一步做什么

- 部署配置更改。

第 XVIII 部分

网络发现



第 81 章

网络发现概述

以下主题讨论网络发现：

关于主机、应用和用户数据的检测

Firepower 系统使用网络发现和身份策略收集网络上流量的主机、应用和用户数据。您可以使用特定类型的发现和身份数据构建全面的网络资产映射，执行调查分析、行为剖析和访问控制并缓解和应对组织最易遭受的漏洞和攻击。

主机和应用数据

主机和应用数据由主机身份源和应用检测器根据网络发现策略中的设置进行收集。受管设备会观察指定网段上的流量。

有关详细信息，请参阅主机和应用检测基础知识，第 1902 页。

用户数据

用户数据由用户身份源根据网络发现和身份策略中的设置进行收集。您可以使用这些数据获取用户感知和用户控制。

有关详细信息，请参阅关于用户身份，第 1791 页。

通过记录发现和身份数据，您可以利用 Firepower 系统中的许多功能，包括：

- 查看网络映射，网络映射是对网络资产和拓扑的详细表示，可通过对主机和网络设备、主机属性、应用协议或漏洞进行分组来查看。
- 执行应用和用户控制，即，使用应用、领域、用户、用户组和ISE属性条件编写访问控制规则。
- 查看主机配置文件，配置文件可完整展示检测到的主机的所有可用信息。
- 查看控制面板，控制面板提供有关网络资产和用户活动的概览及其他功能。
- 查看关于系统记录的发现事件和用户活动的详细信息。
- 将主机及其运行的任何服务器或客户端与它们易受攻击的漏洞关联起来。

这使您能够识别和减少漏洞，评估入侵事件对您的网络的影响，并优化入侵规则状态，以便它们为您的网络资产提供最大的保护

- 在系统生成具有特定影响标志的入侵事件或特定类型的发现事件时，通过邮件、SNMP 陷阱或系统日志向您发出警报
- 监控组织是否遵守允许的 allow操作系统、客户端、应用协议和协议的列表
- 在系统生成发现事件或检测用户活动时，创建具有会触发和生成关联事件的规则的关联策略
- 记录和使用 NetFlow 连接（如果适用）。

主机和应用检测基础知识

您可以配置网络发现策略，以执行主机和应用检测。

有关详细信息，请参阅概述：主机数据收集 ，第 1909 页和概述：应用检测 ，第 1945 页。

操作系统和主机数据被动检测

被动检测是通过分析网络通信量（以及任何导出的NetFlow数据）来填充网络映射的系统默认方法。被动检测提供有关您的网络资产（如操作系统和正在运行的应用）的情景信息。

如果来自受监控主机的流量不提供主机操作系统的确凿证据，则网络映射将显示最有可能的操作系统。例如，由于在 NAT 设备“后面”的主机，NAT 设备可能看起来正在运行多个操作系统。为了做出最可能的决定，系统使用其为每个检测到的操作系统分配的置信值，以及检测到的操作系统之间的确认数据量。

注释 系统在确定时不考虑报告的“unknown”应用和操作系统。

如果被动检测不准确地识别您的网络资产，请考虑更换受管设备。您还可以使用自定义操作系统指纹和自定义应用检测器来增强系统的被动检测功能。或者，您可以使用主用检测，它不基于流量分析，而是允许您使用扫描结果或其他信息源直接更新网络映射。

操作系统和主机数据主动检测

主动检测会将主动源收集的主机信息添加到网络映射。例如，可使用 Nmap 扫描程序主动扫描网络上的目标主机。Nmap 可发现主机上的操作系统和应用。

此外，主机输入功能可用于将主机输入数据主动添加到网络映射。有两种不同类别的主机输入数据：

- 用户输入数据 - 通过 FirePOWER 系统用户界面添加数据。您可以通过此界面修改主机操作系统或应用身份。
- 托管导入输入数据 - 使用命令行实用程序导入的数据。

系统将为每个主动源保留一个身份。如果运行 Nmap 扫描实例，例如，先前的扫描结果将替代为新的扫描结果。然而，如果运行 Nmap 扫描，然后用结果通过命令行导入的客户端的数据替代这些结果，系统将同时保留来自 Nmap 结果的身份以及来自导入客户端的身份。然后，系统会使用网络发现策略中设置的优先级来确定用作当前身份的主动身份。

请注意，用户输入视为一个源，即使其来自不同的源。例如，如果用户 A 通过主机配置文件设置操作系统，然后用户 B 通过主机配置文件更改该定义，用户 B 设置的定义将保留，而用户 A 设置的定义将丢弃。此外，请注意，用户输入会覆盖所有其他的主动源，并会用作当前身份（如果其存在）。

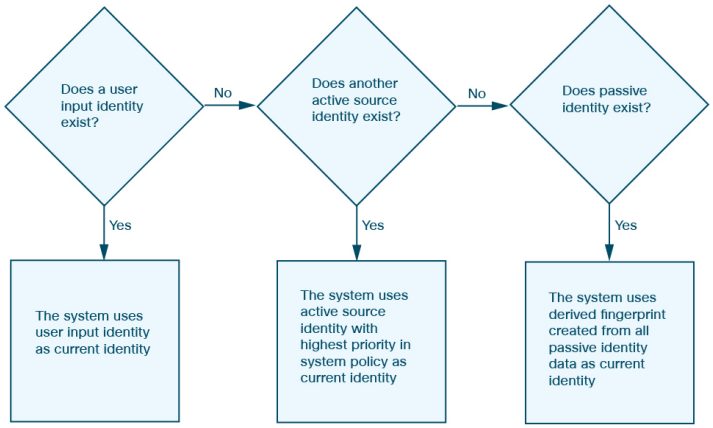
应用和操作系统的当前身份

主机上的应用或操作系统的当前身份是系统发现最有可能正确的身份。

系统会将操作系统或应用的当前身份用于以下用途：

- 分配漏洞至主机
- 影响评估
- 评估针对操作系统标识、主机配置文件合格性以及合规 allow 名单写入的关联规则
- 在工作流程的“主机”(Hosts) 和“服务器”(Servers) 表格视图中进行显示
- 在主机配置文件中进行显示
- 在“发现统计信息”(Discovery Statistics) 页面上计算操作系统和应用统计信息

系统会使用源优先级来确定哪个主动身份应该用作应用或操作系统的当前身份。



例如，如果用户在主机上将操作系统设置为 Windows 2003 Server，则 Windows 2003 Server 为当前身份。针对该主机上的 Windows 2003 Server 漏洞的攻击将被赋予更高的影响，而主机配置文件中为该主机列出的漏洞包括 Windows 2003 Server 漏洞。

对于主机上的操作系统或特定应用，数据库可能保留来自多个源的信息。

如果数据的源拥有最高的源优先级，系统会将操作系统或应用身份视作当前身份。可能的源的优先级顺序如下：

1. 用户

2. 扫描程序和应用（在网络发现策略中设置）

3. 受管设备

4. NetFlow 记录

如果优先级更高的新应用身份拥有的详细信息比当前身份少，则不会覆盖当前应用身份。

此外，如果出现身份冲突，冲突的解决取决于网络发现策略中的设置或者手动解决。

当前用户身份

当系统检测到不同用户多次登录同一主机时，系统将假设某一时刻只有一个用户登录到了某给定主机，并且一个主机的当前用户是最后授权的用户登录。如果只有非授权用户登录用户登录主机，则最后的非授权用户登录用户将被视为当前用户。如果有多个用户通过远程会话登录，则服务器报告的最后用户是报告给 管理中心的用户。

当系统检测到同一用户多次登录到同一主机时，系统会记录用户在特定主机的首次登录并忽略后续的登录。如果单个用户是唯一登录到特定主机的人员，则系统唯一记录的登录为原始登录。

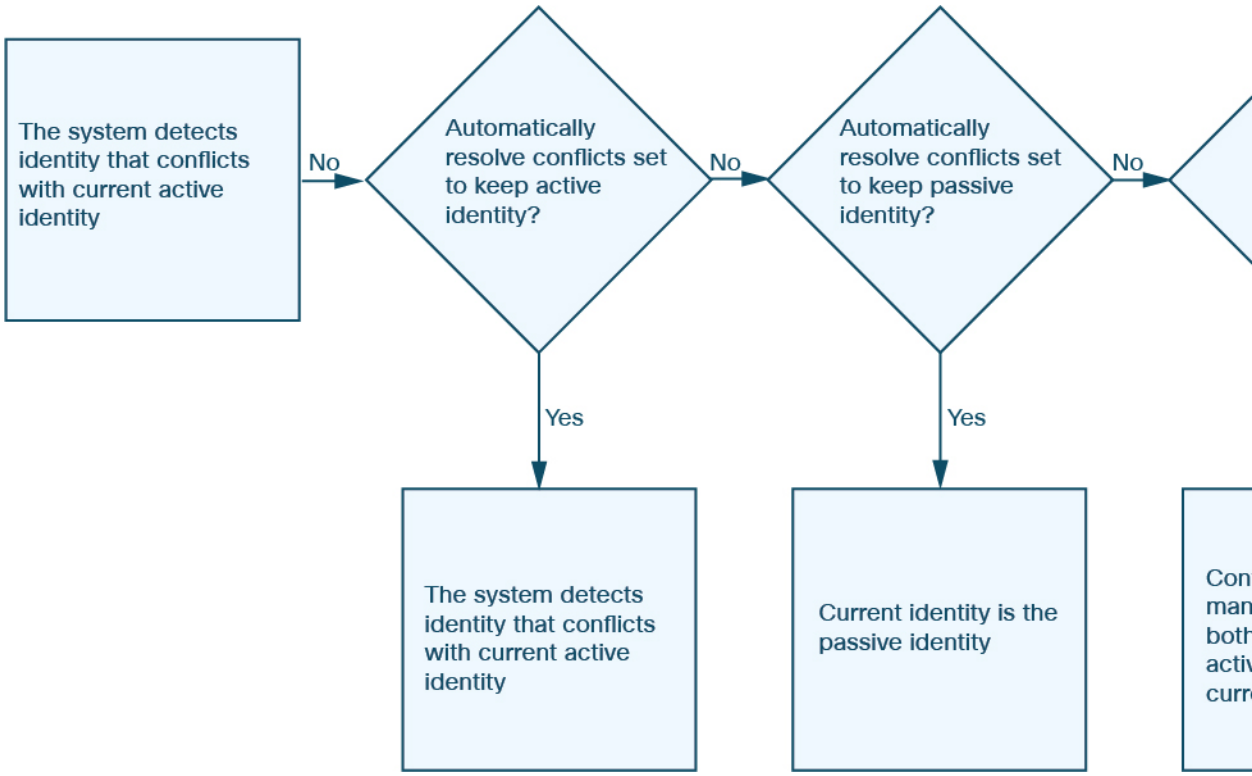
但是，如果另一用户登录到该主机，则系统会记录新的登录。如果原始用户再次登录，系统会记录其新的登录。

应用和操作系统的身份冲突

如果系统报告新的被动身份与当前主动身份和先前报告的被动身份冲突，就会发生身份冲突。例如，如将操作系统先前的被动身份报告为 Windows 2000，则主动身份 Windows XP 成为当前身份。接下来，系统检测到新的被动身份 Ubuntu Linux 8.04.1。身份 Windows XP 和 Ubuntu Linux 发生冲突。

如果主机的操作系统或主机上的某个应用存在身份冲突，系统会将两个冲突的身份均列为当前身份，并将二者用于影响评估，直到冲突解决。

有管理员权限的用户可自动解决身份冲突，只需选择始终使用被动身份或始终使用主动身份。除非禁用身份冲突的自动解决，否则身份冲突始终会自动解决。



有管理员权限的用户还可配置系统，从而在身份冲突发生时生成事件。然后，该用户可设置带有相关性规则的相关策略，规则将Nmap扫描用作相关性响应。如果事件发生，Nmap会扫描主机以获取经过更新的主机操作系统和应用数据。

Netflow 数据

NetFlow 是一款思科 IOS 应用，可以提供有关流经路由器的数据包的统计信息。它在思科网络设备上可用，还可以嵌入到 Juniper、FreeBSD 和 OpenBSD 设备中。

在网络设备上启用 NetFlow 时，设备（NetFlow 缓存）上的数据库会存储通过路由器的数据流的记录。数据流（在系统中称为连接）是数据包序列，代表使用特定端口、协议和应用协议的源主机和目标主机之间的会话。可以将网络设备配置为导出此 NetFlow 数据。在本文档中，通过此方式配置的网络设备称为 *NetFlow* 导出器。

受管设备可以配置为从 NetFlow 导出器收集记录，根据这些记录中的数据生成单向连接结束事件，最后将这些事件发送到 管理中心以记录在连接事件数据库中。您还可以配置网络发现策略，以根据 NetFlow 连接中的信息将主机和应用协议信息添加到数据库。

可以使用这些发现和连接数据补充受管设备直接收集到的数据。这在让 NetFlow 导出器监控受管设备无法监控的网络时尤为有用。

使用 NetFlow 数据的要求

在配置 Firepower 系统以分析 NetFlow 数据之前，必须在计划使用的路由器或其他支持 NetFlow 的设备上启用 NetFlow 功能，并且配置设备以将 NetFlow 数据广播到连接了受管设备传感接口的目标网络。

Firepower 系统可以分析 NetFlow 版本 5 和 NetFlow 版本 9 记录。如果要将数据导出到 Firepower 系统，则 NetFlow 导出器**必须**使用这些版本之一。此外，系统还要求在已导出的 NetFlow 模板和记录中存在特定字段。如果 NetFlow 导出器使用的是可以自定义的版本 9，则**必须**确保已导出的模板和记录按任意顺序包含以下字段：

- IN_BYTES (1)
- IN_PKTS (2)
- PROTOCOL (4)
- TCP_FLAGS (6)
- L4_SRC_PORT (7)
- IPV4_SRC_ADDR (8)
- L4_DST_PORT (11)
- IPV4_DST_ADDR (12)
- LAST_SWITCHED (21)
- FIRST_SWITCHED (22)
- IPV6_SRC_ADDR (27)
- IPV6_DST_ADDR (28)

由于 Firepower 系统使用受管设备分析 NetFlow 数据，因此，部署必须至少包括一个可监控 NetFlow 导出器的受管设备。该受管设备上的至少一个传感接口必须连接到可以收集已导出的 NetFlow 数据的网络。由于受管设备上的感应接口通常不具有 IP 地址，因此系统不支持直接收集 NetFlow 记录。

请注意，在某些网络设备上可用的采样 NetFlow 功能只会收集有关经过设备的数据包子集的 NetFlow 统计信息。尽管启用此功能可以提高网络设备上的 CPU 利用率，但可能会影响收集以供 Firepower 系统分析的 NetFlow 数据。

NetFlow 和受管设备数据之间的差异

NetFlow 数据代表的流量不会被直接分析 。相反，系统会将导出的 NetFlow 记录转换为连接日志以及主机和应用协议数据。

因此，转换后的 NetFlow 数据与受管设备直接收集到的发现数据和连接数据之间存在一些差异。在执行需要以下信息的分析时，应记住这些差异：

- 已检测的连接数量的统计信息
- 操作系统信息以及其他主机相关信息（包括漏洞）

- 应用数据，包括客户端信息、Web 应用信息，以及供应商和版本服务器信息
- 知道连接中哪个主机是发起方，哪个主机是响应方

网络发现策略与访问控制策略

可以使用网络发现策略中的规则来配置 NetFlow 数据收集（包括连接日志记录）。可以将这种数据收集与受管设备（根据访问控制规则进行配置）检测到的连接的连接日志记录进行比较。

连接事件的类型

由于 NetFlow 数据收集与网络而不是访问控制规则相关联，因此您不能非常精细地控制系统记录的 NetFlow 连接。

NetFlow 数据无法生成安全情报事件。

基于 NetFlow 的连接事件只能存储在连接事件数据库中；无法将这些事件发送到系统日志或 SNMP 陷阱服务器。

每个受监控会话生成的连接事件的数量

对于受管设备直接检测到的连接，可将访问控制规则配置为在连接开始和/或结束时记录双向连接事件。

相反，由于导出的 NetFlow 记录包含单向连接数据，因此系统会为其处理的每个 NetFlow 记录生成至少两个连接事件。这也意味着，对于基于 NetFlow 数据的每次连接，摘要的连接数会每次递增 2，从而提供网络上实际发生的快速增长的连接数量。

由于 NetFlow 导出器会以固定间隔输出记录（即使连接仍在继续），因此长期运行的会话可能会导致多个导出的记录，每个记录生成一个连接事件。例如，如果 NetFlow 导出器每 5 分钟导出一次，且特定连接持续 12 分钟，那么系统将会为该会话生成 6 个连接事件：

- 前 5 分钟生成一对事件
- 第二个 5 分钟生成一对事件
- 连接终止时生成最后一对事件

主机和操作系统数据

从 NetFlow 数据添加到网络映射的主机不具有操作系统、NetBIOS 或主机类型（主机与网络设备）信息。但是，可以使用主机输入功能手动设置主机的操作系统身份。

应用数据

对于受管设备直接检测到的连接，系统可以通过检查连接中的数据包来识别应用协议、客户端和 Web 应用。

系统处理 NetFlow 记录时，会使用 `/etc/sf/services` 中的端口关联来推断应用协议身份。不过，这些应用协议不包含供应商或供应商信息，而且连接日志不包含关于会话中使用的客户端或 Web 应用的信息。但是，可以使用主机输入功能手动提供这些信息。

请注意，简单端口关联意味着在非标准端口上运行的应用协议可能不会被识别或被错误识别。此外，如果不存在关联，系统会在连接日志中将应用协议标记为 unknown。

漏洞映射

系统无法将漏洞映射到 NetFlow 导出器监控的主机，除非使用主机输入功能手动设置主机操作系统的身份或应用协议身份。请注意，由于 NetFlow 连接中没有客户端信息，因此您无法将客户端漏洞与根据 NetFlow 数据创建的主机相关联。

连接中发起方和响应方信息

对于受管设备直接检测到的连接，系统可确定哪个主机是发起方（即“源”），哪个主机是响应方（即“目标”）。但是，NetFlow 数据不包含发起方或响应方信息。

当系统处理 NetFlow 记录时，它会根据各主机正在使用的端口以及此类端口是否为公认端口来使用一种算法确定该信息。

- 如果使用的两个端口都是或都不是公认端口，系统会将端口号较小的那个主机视为响应方。
- 如果只有一个主机在使用公认端口，系统会将该主机视为响应方。

为此，公认端口是编号为 1 到 1023 的任意端口，或包含受管设备上 /etc/sf/services 中应用协议信息的任意端口。

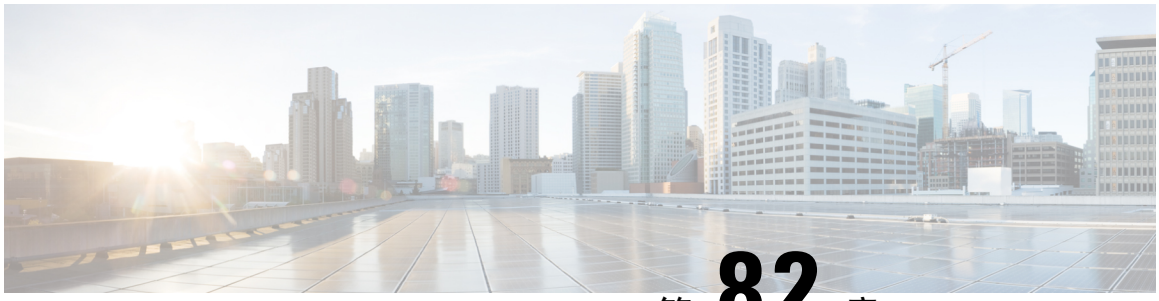
此外，对于由受管设备直接检测到的连接，系统会在对应的连接事件中记录两个字节计数：

- **发起方字节数**字段记录发送的字节数。
- **响应方字节数**字段记录接收的字节数。

基于单向 NetFlow 记录的连接事件只包含一个字节计数（系统分配到**发起方字节数 [Initiator Bytes]** 或**响应方字节数 [Responder Bytes]**），具体取决于基于端口的算法。系统将另一个字段设置为 0。请注意，如果查看 NetFlow 记录的连接摘要（汇聚的连接数据），则这两个字段都可能会填充。

纯 NetFlow 连接事件字段

从 NetFlow 记录生成的连接事件中只存在少量字段。



第 82 章

主机身份源

以下主题提供有关主机身份源的信息：

概述：主机数据收集

由于 Firepower 系统被动监控流经网络的流量，因此，它会根据既定的定义（称为指纹）比较特定数据包报头值以及来自网络流量的其他唯一数据，以确定关于网络上主机的信息，包括：

- 主机（包括网桥、路由器、负载均衡器和 NAT 设备等网络设备）数量和类型
- 基本网络拓扑数据，包括从网络上的发现点到主机的跳数
- 主机上运行的操作系统
- 主机上的应用以及与这些应用关联的用户

如果系统无法识别主机的操作系统，则您可以创建自定义客户端或服务器指纹。系统将使用这些指纹来识别新主机。您可以将指纹映射到漏洞数据库 (VDB) 中的系统，以便在使用自定义指纹识别主机时显示适当的漏洞信息。

注释 除从受监控网络流量中收集主机数据以外，系统还可以从导出的 NetFlow 记录收集主机数据，并且您可以使用 Nmap 扫描和主机输入功能主动添加主机数据。

主机身份源的要求和必备条件

型号支持

任意。

支持的域

任意，但自定义指纹除外，它仅限 枝叶。

用户角色

- 管理员
- 发现管理员，但第三方数据和自定义映射除外。

确定系统可以检测的主机操作系统

要了解系统可以进行指纹识别的确切操作系统，请查看在创建自定义操作系统指纹过程中显示的可用指纹的列表。

过程

步骤 1 选择**策略** > **网络发现**。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。

步骤 3 点击 **Create Custom Fingerprint**。

步骤 4 查看**操作系统漏洞映射**部分的下拉列表中的选项列表。这些选项是系统可以进行指纹识别的操作系统。

下一步做什么

根据需要，请参阅识别主机操作系统 ， 第 1910 页。

识别主机操作系统

如果系统无法正确识别主机的操作系统（例如，操作系统在“主机配置文件”中显示为“未知”，或者识别的操作系统不正确），则请尝试下面的策略。

过程

尝试以下策略之一：

- 检查“网络发现身份冲突设置”。
- 创建主机的自定义指纹。
- 对主机运行 Nmap 扫描。
- 使用主机输入功能将数据导入到网络映射中。
- 手动输入操作系统信息。

自定义指纹

系统包含系统用于识别其检测的每个主机上的操作系统的操作系统指纹。然而，有时系统会因为不存在与操作系统匹配的指纹而无法识别主机操作系统，或者错误地识别主机操作系统。要纠正此问题，可创建自定义指纹，指纹提供未知或识别错误的操作系统所独有的操作系统特征模式，以便提供用于标识的操作系统名称。

如果系统无法匹配主机操作系统，则无法识别主机漏洞，因为系统通过其操作系统指纹为每个主机派生漏洞列表。例如，如果系统检测到运行 Microsoft Windows 的主机，则表明系统存储了 Microsoft Windows 漏洞列表，其根据检测到的 Windows 操作系统将该列表添加至该主机的主机配置文件。

例如，如果网络上有多个运行新试用版 Microsoft Windows 的设备，则系统无法确定操作系统，或无法将漏洞映射到主机。然而，知道系统拥有 Microsoft Windows 的漏洞列表，您可能想要为某个主机创建自定义指纹，以帮助识别运行相同操作系统的其他主机。可将 Microsoft Windows 漏洞列表的映射纳入指纹中，以便将该列表与匹配指纹的每个主机关联。

创建自定义指纹时，管理中心将为运行相同操作系统的任何主机列出与该指纹关联的漏洞集。如果创建的自定义指纹没有任何漏洞映射，则系统将使用该指纹来分配在其中提供的自定义操作系统信息。当系统看到之前检测的主机发出的新流量时，系统用新指纹信息更新主机。首次检测到使用该操作系统的任何新主机时，系统还会使用新的指纹来识别这些主机。

在创建自定义指纹前，应确定主机未被正确识别的原因，从而确定自定义指纹是否为可行的解决方案。

可使用系统创建两种类型的指纹：

- 客户端指纹，这种指纹根据 SYN 数据包识别操作系统，主机连接网络上的另一主机上运行的 TCP 应用时，会发送这种数据包。
- 服务器指纹，这种指纹根据 SYN-ACK 数据包识别操作系统，主机使用这种数据包来响应通向运行的 TCP 应用的传入连接。

注释 如果客户端和服务器指纹均与相同的主机匹配，将会使用客户端指纹。

创建指纹后，必须先将其激活，然后系统才可以将其与主机关联。

相关主题

为客户端创建自定义指纹，第 1914 页
为服务器创建自定义指纹，第 1916 页

管理指纹

指纹创建和激活后，可编辑指纹以便做出更改或添加漏洞映射。

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。如果系统正在等待数据以便创建指纹，将会每 10 秒自动刷新页面，直到指纹已创建。

步骤 3 管理自定义指纹：

- 激活/停用 - 激活或停用指纹，如激活和停用指纹，第 1912 页中所述。
- 创建 - 创建指纹，如为客户端创建自定义指纹，第 1914 页和为服务器创建自定义指纹，第 1916 页中所述。
- 编辑 - 编辑指纹，如编辑活动指纹，第 1913 页和编辑非活动指纹，第 1913 页中所述。
- 删除 - 点击要删除的指纹旁边的 **删除**（  ），并点击**确定 (OK)** 以进行确认。只能删除已停用的指纹。

激活和停用指纹

必须先激活自定义指纹，然后系统才能将其用于识别主机。新指纹激活后，系统会将其用于重新识别先前发现的主机并发现新的主机。

如果想要停止使用指纹，可将其停用。停用指纹后，该指纹就不再可用，但仍可保留其在系统中。停用指纹后，对于使用该指纹的主机，操作系统被标记为未知。如果再次检测到这些主机，并且这些主机与不同的活动指纹匹配，则该活动指纹将对其进行识别。

删除指纹会将其从系统中完全删除。停用指纹后，即可将其删除。

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。

步骤 3 点击要激活或停用的指纹旁边的滑块。

注释 激活选项仅当创建的指纹有效时才可用。如果滑块不可用，请尝试重新创建指纹。

编辑活动指纹

如果指纹处于活动状态，可修改指纹名称、描述、自定义操作系统显示，并向其映射额外的漏洞。

可以修改指纹名称、描述、自定义操作系统显示，并向其映射额外的漏洞。

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**

步骤 3 点击想要编辑的指纹旁的 **编辑**（）。

步骤 4 必要时修改指纹名称、描述和自定义操作系统显示。

步骤 5 如果要删除漏洞映射，请点击页面的**预定义操作系统产品映射 (Pre-Defined OS Product Maps)** 部分中映射旁边的**删除 (Delete)**。

步骤 6 如果要为漏洞映射添加额外的操作系统，请选择**产品 (Product)**，且在适用的情况下，选择**主要版本 (Major Version)**、**次要版本 (Minor Version)**、**修订版本 (Revision Version)**、**内部版本 (Build)**、**补丁 (Patch)** 和**扩展版本 (Extension)**，然后点击**添加操作系统定义 (Add OS Definition)**。

漏洞映射会添加到**预定义操作系统产品映射 (Pre-Defined OS Product Maps)** 列表。

步骤 7 点击**保存 (Save)**。

编辑非活动指纹

如果指纹处于非活动状态，可修改指纹的所有元素，并将其重新提交至 Cisco Secure Firewall Management Center。这包括创建指纹时指定的所有属性，如指纹类型、目标 IP 地址与端口、漏洞映射等。编辑非活动指纹并将其提交时，会将它重新提交至系统，如果指纹是客户端指纹，必须先将流量重新发送至设备，然后才可以将其激活。请注意，对于非活动指纹，仅可选择单一漏洞映射。激活指纹后，可将额外的操作系统和版本映射至其漏洞列表。

过程

步骤 1 选择策略 > 网络发现。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击自定义操作系统 (Custom Operating Systems)。

步骤 3 点击想要编辑的指纹旁的 编辑（）。

步骤 4 请在必要时更改指纹：

- 如果要修改客户端指纹，请参阅为客户端创建自定义指纹，第 1914 页。
- 如果要修改服务器指纹，请参阅为服务器创建自定义指纹，第 1916 页。

步骤 5 点击保存 (Save)。

下一步做什么

- 如已修改客户端指纹，切记将流量从主机发送至收集指纹的设备。

为客户端创建自定义指纹

客户端指纹根据 SYN 数据包识别操作系统，主机连接网络上的另一主机上运行的 TCP 应用时，会发送这种数据包。

如果 管理中心不与受监控的主机直接联系，指定客户端指纹属性时，可以指定管理中心管理的离想要为其设置指纹的主机最近的设备。

开始指纹设置流程之前，获取想要为其设置指纹的主机的以下相关信息：

- 主机与管理中心或用于获取指纹的设备之间的网络跳数。（思科强烈建议将 管理中心或设备直接连接到与主机所连接到的同一子网）。
- 连接至主机所在网络的（管理中心或设备上的）网络接口。
- 主机的实际操作系统供应商、产品和版本。
- 访问主机以便生成客户端流量。

过程

步骤 1 选择策略 > 网络发现。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击自定义操作系统 (Custom Operating Systems)。

步骤 3 点击 **Create Custom Fingerprint**。

步骤 4 从设备下拉列表中，选择要用于收集指纹的 管理中心或设备。

步骤 5 输入**指纹名称 (Fingerprint Name)**。

步骤 6 输入**指纹说明 (Fingerprint Description)**。

步骤 7 从**指纹类型 (Fingerprint Type)** 列表中，选择**客户端 (Client)**。

步骤 8 在**目标 IP 地址 (Target IP Address)** 字段中，输入要为其设置指纹的主机的 IP 地址。

请注意，指纹仅会基于流向和来自您指定的主机IP地址的流量，而不是主机的任何其他IP地址（如果其拥有）。

步骤 9 在**目标距离 (Target Distance)** 字段中，输入主机与之前选择用于收集指纹的设备之间的网络跳数。

注意 此跳数必须是至主机的实际物理网络跳数，与系统检测到的跳数不一定相同。

步骤 10 从**接口 (Interface)** 列表中，选择连接到主机所在网段的网络接口。

注意 由于多个原因，思科建议**不要**将受管设备上的传感接口用于设置指纹。首先，如果传感接口位于 SPAN 端口之上，指纹技术将不起作用。另外，如果使用设备上的传感接口，设备在其收集指纹所花的时间内会停止监控网络。不过，可使用管理接口或任何其他可用网络接口来执行指纹收集。如果不知道哪个接口是设备上的传感接口，请参阅用于设置指纹的特定型号的《安装指南》。

步骤 11 如果要在设置指纹的主机的主机配置文件中显示自定义信息（或者如果要设置指纹的主机不在**操作系统漏洞映射**部分中），请选择**使用自定义操作系统显示**，并对于以下各项提供要显示的值：

- 在**供应商字符串 (Vendor String)** 字段中，输入操作系统的供应商名称。例如，Microsoft Windows 的供应商为 Microsoft。
- 在**产品字符串 (Product String)** 字段中，输入操作系统的产品名称。例如，Microsoft Windows 2000 的产品名称为 Windows。
- 在**版本字符串 (Version String)** 字段中，输入操作系统的版本号。例如，Microsoft Windows 2000 的版本号为 2000。

步骤 12 在“操作系统漏洞映射”(OS Vulnerability Mappings) 部分中，选择要用于漏洞映射的操作系统、产品和版本。

如果要使用指纹来识别匹配主机的漏洞，或者如果不分配自定义的操作系统显示信息，则必须在此部分指定**供应商 (Vendor)** 和**产品 (Product)** 值。

要为所有版本的操作系统映射漏洞，请仅指定**供应商**和**产品**值。

注释 并非**主要版本 (Major Version)**、**次要版本 (Minor Version)**、**修订版本 (Revision Version)**、**内部版本 (Build)**、**补丁 (Patch)** 和**扩展版本 (Extension)** 下拉列表中的所有选项均可应用至选择的操作系统。此外，如果列表中没有显示与想要设置指纹的操作系统匹配的定义，可将这些值留空。请注意，如果不在指纹中创建任何操作系统漏洞映射，则系统无法使用指纹来为指纹识别的主机分配漏洞列表。

示例：

如果想要自定义指纹将 Redhat Linux 9 的漏洞列表分配到匹配主机，请选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为主要版本。

示例：

要添加所有版本的 Palm 操作系统，请从 **供应商**列表中选择 **PalmSource, Inc.**，从**产品**列表中选择 **Palm 操作系统**，并让所有其他列表保持其默认设置。

步骤 13 点击**创建**。

状态会短暂显示 `New`，然后切换至 `Pending`，此状态会保持不变，直到发现匹配指纹的流量。发现流量后，状态会切换至就绪 `(Ready)`。

“自定义指纹”(Custom Fingerprint) 状态页面每隔 10 秒进行刷新，直到其收到来自所述主机的数据。

步骤 14 将指定的 IP 地址用作目标 IP 地址，访问您尝试为其设置指纹的主机，并发起至设备的 TCP 连接。

要创建准确的指纹，收集指纹的设备**必须**发现流量。如果通过交换机进行连接，系统可能不会发现流向系统而不是设备的流量。

示例：

从想要为其设置指纹的主机访问 管理中心的 Web 界面，或者从主机使用 SSH 登录至 管理中心。如果使用的是 SSH，请使用以下命令，其中，localIPv6address 是在步骤 7 中指定的当前已分配到主机的 IPv6 地址，DCmanagementIPv6address 是 管理中心 的管理 IPv6 地址。然后，Custom Fingerprint 页面重新加载，其状态为“就绪”。

```
ssh -b localIPv6address DCmanagementIPv6address
```

下一步做什么

- 激活指纹，如激活和停用指纹 ， 第 1912 页中所述。

为服务器创建自定义指纹

服务器指纹根据 SYN-ACK 数据包识别操作系统，主机使用这种数据包来响应通向运行的 TCP 应用的传入连接。在开始之前，应获取关于想要为其设置指纹的主机的以下信息：

- 主机与用于获取指纹的设备之间的网络跳数。思科强烈建议将设备上不使用的接口直接连接到主机所连接到的相同子网。
- 连接至主机所在网络的（设备上的）网络接口。
- 主机的实际操作系统供应商、产品和版本。
- 未在使用的 IP 地址，并在主机所在网络上得到授权。

提示 如果 管理中心不与受监控的主机直接联系，指定服务器指纹属性时，可以指定离想要为其设置指纹的主机最近的受管设备。

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。

步骤 3 点击 **Create Custom Fingerprint**。

步骤 4 从**设备**列表中，选择要用于收集指纹的 管理中心或受管设备。

步骤 5 输入**指纹名称 (Fingerprint Name)**。

步骤 6 输入**指纹说明 (Fingerprint Description)**。

步骤 7 从**指纹类型 (Fingerprint Type)** 列表中，选择**服务器 (Server)** 以显示服务器指纹选项。

步骤 8 在**目标 IP 地址 (Target IP Address)** 字段中，输入要为其设置指纹的主机的 IP 地址。

请注意，指纹仅会基于流向和来自您指定的主机IP地址的流量，而不是主机的任何其他IP地址（如果其拥有）。

注意 只可以使用运行 5.2 及更高版本的设备捕获 IPv6 指纹。

步骤 9 在**目标距离 (Target Distance)** 字段中，输入主机与之前选择用于收集指纹的设备之间的网络跳数。

注意 此跳数必须是至主机的实际物理网络跳数，与系统检测到的跳数不一定相同。

步骤 10 从**接口 (Interface)** 列表中，选择连接到主机所在网段的网络接口。

注意 由于多个原因，思科建议**不要**将受管设备上的传感接口用于设置指纹。首先，如果传感接口位于 SPAN 端口之上，指纹技术将不起作用。另外，如果使用设备上的传感接口，设备在其收集指纹所花的时间内会停止监控网络。不过，可使用管理接口或任何其他可用网络接口来执行指纹收集。如果不知道哪个接口是设备上的传感接口，请参阅用于设置指纹的特定型号的《安装指南》。

步骤 11 点击**获取活动端口 (Get Active Ports)**。

步骤 12 在**服务器端口**字段中，输入想要设备选择用于收集指纹以便向其发起联系的端口，或者从**获取活动端口**下拉列表选择端口。

可使用主机上已知开放的任何服务器端口（例如，80，如果主机正在运行网络服务器）。

步骤 13 在**源 IP 地址 (Source IP Address)** 字段中，输入应用于尝试与主机通信的 IP 地址。

应使用经授权可在网络上使用，但目前未在使用的源 IP 地址，例如，当前未在使用的 DHCP 池地址。创建指纹时，这可防止临时访问另一离线主机。

创建指纹时，应从网络发现策略的监控中排除该IP地址。否则，网络映射和发现事件视图中将会出现大量关于该 IP 地址代表的主机的不准确信息。

步骤 14 在**源子网掩码 (Source Subnet Mask)** 字段中，输入正在使用的 IP 地址的子网掩码。

步骤 15 如果 **Source Gateway** 字段显示，输入应用于建立至主机的路由的默认网关 IP 地址。

步骤 16 如果要在设置指纹的主机的主机配置文件中显示自定义信息，或者如果要使用的指纹名称在“操作系统定义”(OS Definition) 部分中不存在，则可以在“自定义操作系统显示”(Custom OS Display) 部分中选择**使用自定义操作系统显示 (Use Custom OS Display)**。

对于以下项提供想要在主机配置文件中显示的值：

- 在**供应商字符串 (Vendor String)** 字段中，输入操作系统的供应商名称。例如，Microsoft Windows 的供应商为 Microsoft。
- 在**产品字符串 (Product String)** 字段中，输入操作系统的产品名称。例如，Microsoft Windows 2000 的产品名称为 Windows。
- 在**版本字符串 (Version String)** 字段中，输入操作系统的版本号。例如，Microsoft Windows 2000 的版本号为 2000。

步骤 17 在“操作系统漏洞映射”(OS Vulnerability Mappings) 部分中，选择要用于漏洞映射的操作系统、产品和版本。

如果要使用指纹来识别匹配主机的漏洞，或者如果不分配自定义的操作系统显示信息，则必须在此部分指定供应商和产品名称。

要为所有版本的操作系统映射漏洞，请仅指定供应商和产品名称。

注释 并非**主要版本 (Major Version)**、**次要版本 (Minor Version)**、**修订版本 (Revision Version)**、**内部版本 (Build)**、**补丁 (Patch)** 和**扩展版本 (Extension)** 下拉列表中的所有选项均可应用至选择的操作系统。此外，如果列表中没有显示与想要设置指纹的操作系统匹配的定义，可将这些值留空。请注意，如果不在指纹中创建任何操作系统漏洞映射，则系统无法使用指纹来为指纹识别的主机分配漏洞列表。

示例：

如果想要自定义指纹将 Redhat Linux 9 的漏洞列表分配到匹配主机，请选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为版本。

示例：

要添加所有版本的 Palm 操作系统，请从 **供应商 (Vendor)** 列表中选择 **PalmSource, Inc.**，从**产品 (Product)** 列表中选择 **Palm 操作系统 (Palm OS)**，并让所有其他列表保持其默认设置。

步骤 18 点击**创建**。

“自定义指纹”(Custom Fingerprint) 状态页面每 10 秒刷新一次并应以“就绪”状态重新加载。

注释 如果目标系统在设置指纹的过程中停止响应，状态将会显示错误：无响应 (ERROR: No Response) 消息。如果看到此消息，请再次提交指纹。等待 3 至 5 分钟（时长可能因目标系统而异），点击 **编辑**（）访问“自定义指纹”(Custom Fingerprint) 页面，然后点击**创建 (Create)**。

下一步做什么

- 激活指纹，如激活和停用指纹 ， 第 1912 页中所述。

主机输入数据

您可以通过从第三方导入网络映射数据来扩充网络映射。您还可使用主机输入功能，只需使用 Web 界面修改操作系统或应用身份，或删除应用协议、协议、主机属性或客户端。

系统可协调来自多个源的数据，以确定操作系统或应用的当前身份。

从网络映射中删除受影响的主机后，将会丢弃除第三方漏洞之外的所有数据。有关设置脚本或导入文件的详细信息，请参阅《*Firepower* 系统主机输入 *API* 指南》。

要将已导入数据纳入影响关联中，必须将数据映射至数据库中的操作系统和应用定义。

第三方数据使用要求

可以从网络上的第三方系统导入发现数据。但是，要启用将入侵和发现数据结合使用的功能（例如思科 建议、自适应配置文件或影响评估），应将其中尽可能多的元素映射到对应的定义。考虑对使用第三方数据的以下要求：

- 如果拥有在您的网络资产上有特定数据的第三方系统，则可使用主机输入功能导入该数据。但是，由于第三方可能会以不同的方式命名产品，因此必须将第三方供应商、产品和版本映射到对应的思科产品定义。映射产品后，必须在 管理中心配置中为影响评估启用漏洞映射，以允许影响关联。对于无版本或无供应商的应用协议，需要在 管理中心配置中映射应用协议的漏洞。
- 如果导入来自第三方的修补程序信息，并想要将修补程序修补的所有漏洞标记为无效，则必须将第三方修补程序的名称映射至数据库中的定义。修补程序针对的所有漏洞随后会从添加该修补程序所在的主机中移除。
- 如果导入来自第三方的操作系统和应用协议漏洞，并想将其用于影响关联，则必须将第三方漏洞标识字符串映射至数据库中的漏洞。请注意，尽管许多客户端拥有相关的漏洞，而且客户端用于影响评估，但不能导入和映射第三方客户端漏洞。映射漏洞后，必须在 管理中心配置中为影响评估启用第三方漏洞映射。要使没有供应商或版本信息的应用协议映射到漏洞，管理用户还必须在 管理中心配置中映射应用的漏洞。
- 如果导入应用数据并要将该数据用于影响关联，则必须将每个应用协议的供应商字符串映射到对应的应用协议定义。

相关主题

映射第三方产品，第 1920 页
映射第三方产品修补程序，第 1921 页
映射第三方漏洞，第 1922 页
创建自定义产品映射，第 1923 页

第三方产品映射

如果通过用户输入功能将第三方数据添加至网络映射，则必须将第三方使用的供应商、产品和版本名称映射到思科产品定义。将产品映射到思科定义后，将根据这些定义分配漏洞。

类似地，如果正在导入第三方修补程序信息，如修补程序管理产品，则必须将修补程序的名称映射至适当供应商和产品以及数据库中的相应修补程序。

映射第三方产品

如果从第三方导入数据，则必须将思科产品映射到第三方名称，以分配漏洞并使用该数据执行影响关联。映射产品可以将思科漏洞信息与第三方产品名称关联，这样，系统就可使用该数据执行影响关联。

如果使用主机输入导入功能导入数据，还可以在导入过程中，使用 AddScanResult 函数将第三方产品映射至操作系统和应用漏洞。

例如，如果从将 Apache Tomcat 列为应用的第三方导入数据，并且知道它是该产品的第 6 版，则可以添加第三方映射，其中：

- **供应商名称 (Vendor Name)** 设置为 `Apache`。
- **产品名称 (Product Name)** 设置为 `Tomcat`。
- **Apache** 是从**供应商 (Vendor)** 下拉列表中选择。
- **Tomcat** 是从**产品 (Product)** 下拉列表中选择。
- **6** 是从**版本 (Version)** 下拉列表中选择。

该映射会使 Apache Tomcat 6 的任何漏洞分配到其应用列出了 Apache Tomcat 的主机。

请注意，对于无版本或无供应商的应用，必须在 Cisco Secure Firewall Management Center配置中为应用类型映射漏洞。尽管许多客户端具有关联的漏洞，而且客户端用于影响评估，但不能导入和映射第三方客户端漏洞。

提示 如已在另一 Cisco Secure Firewall Management Center上创建了第三方映射，则将其导出后可导入至此管理中心。然后，可根据自己的需求编辑已导入的映射。

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 点击**用户第三方映射 (User Third-Party Mappings)**。

步骤 3 您有两种选择：

- 创建 - 要创建新的映射集，请点击**创建产品映射集 (Create Product Map Set)**。
- 编辑 - 要编辑现有映射集，请点击要修改的映射集旁边的**编辑**（）。如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 输入**映射集名称 (Mapping Set Name)**。

步骤 5 输入**说明 (Description)**。

步骤 6 您有两种选择：

- 创建 - 要映射第三方产品，请点击**添加产品映射 (Add Product Map)**。
- 编辑 - 要编辑现有第三方产品映射集，请点击要修改的映射集旁边的 **编辑**（）。 如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 7 输入第三方产品使用的**供应商字符串 (Vendor String)**。

步骤 8 输入第三方产品使用的**产品字符串 (Product String)**。

步骤 9 输入第三方产品使用的**版本字符串 (Version String)**。

步骤 10 在“产品映射”部分中，从以下字段为漏洞映射选择要使用的操作系统、产品和版本：**供应商**、**产品**、**主要版本**、**次要版本**、**修订版本**、**内部版本**、**补丁**和**扩展版本** 。

示例：

如果要运行其名称包含第三方字符串的产品的主机使用 Red Hat Linux 9 的漏洞，请选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为版本。

步骤 11 点击**保存 (Save)**。

映射第三方产品修补程序

如果将修补程序名称映射至数据库中一组特定的修补程序，则可从第三方修补程序管理应用中导入数据，并对一组主机应用该修补程序。修补程序名称导入至主机后，对于该主机，系统会将修补程序针对的所有漏洞标记为无效。

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 点击**用户第三方映射 (User Third-Party Mappings)**。

步骤 3 您有两种选择：

- 创建 - 要创建新的映射集，请点击**创建产品映射集 (Create Product Map Set)**。
- 编辑 - 要编辑现有映射集，请点击要修改的映射集旁边的 **编辑**（）。 如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 输入**映射集名称 (Mapping Set Name)**。

步骤 5 输入**说明 (Description)**。

步骤 6 您有两种选择：

- 创建 - 要映射第三方产品，请点击**添加修补程序映射 (Add Fix Map)**。
- 编辑 - 要编辑现有第三方产品映射，请点击映射旁边的 **编辑**（）。 如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 7 在**第三方修补程序名称 (Third-Party Fix Name)** 字段中，输入要映射的修补程序的名称。

步骤 8 在**产品映射 (Product Mappings)** 部分中，从以下字段为修补程序映射选择要使用的操作系统、产品和版本：

- **Vendor**

- **Product**
- 主要版本 **(Major Version)**
- 次要版本 **(Minor Version)**
- 修订版本 **(Revision Version)**
- 构建
- 修补
- 分机

示例：

如果想要映射将 Red Hat Linux 9 的修补程序分配到应用补丁的主机，请选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为版本。

步骤 9 点击 **Save**，以保存修补程序映射。

映射第三方漏洞

要将第三方的漏洞信息添加至VDB，必须将每个导入的漏洞的第三方标识字符串映射至任何现有的SVID、Bugtraq或SID。为漏洞创建映射之后，该映射适用于已导入网络映射中主机的所有漏洞，且可为这些漏洞执行影响关联。

必须为第三方漏洞启用影响关联，才能允许关联发生。对于无版本或无供应商的应用，还必须在Cisco Secure Firewall Management Center配置中为应用类型映射漏洞。

尽管许多客户端拥有关联的漏洞，而且客户端用于影响评估，但不能将第三方客户端漏洞用于影响评估。

提示 如已在另一 Cisco Secure Firewall Management Center上创建了第三方映射，则将其导出后可导入至此管理中心。然后，可根据自己的需求编辑已导入的映射。

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 点击**用户第三方映射 (User Third-Party Mappings)**。

步骤 3 您有两种选择：

- 创建 - 要创建新漏洞集，请点击**创建漏洞映射集 (Create Vulnerability Map Set)**。
- 编辑 - 要编辑现有漏洞集，请点击漏洞集旁边的 **编辑**（）。如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击 **Add Vulnerability Map**。

步骤 5 在**漏洞 ID (Vulnerability ID)** 字段中输入第三方漏洞标识。

步骤 6 输入**漏洞说明 (Vulnerability Description)**。

步骤 7 或者：

- 在 **Snort 漏洞 ID 映射**字段中输入 Snort ID。
- 在 **SVID 映射 (SVID Mappings)** 字段中输入旧版漏洞 ID。
- 在 **Bugtraq 漏洞 ID 映射 (Bugtraq Vulnerability ID Mappings)** 字段中输入 Bugtraq 标识号。

步骤 8 点击**添加**。

相关主题

启用网络发现漏洞影响评估，第 1980 页

自定义产品映射

可以使用产品映射来确保由第三方输入的服务器与适当的思科定义相关联。定义并激活产品映射后，具有映射供应商字符串的受监控主机上的所有服务器或客户端都使用自定义产品映射。为此，您可能想要为网络中带有特定供应商字符串的服务器映射漏洞，而不是显式地为服务器设置供应商、产品和版本。

创建自定义产品映射

如果系统无法将服务器映射到VDB中的供应商和产品，您可以手动创建映射。激活自定义产品映射后，系统会将指定供应商和产品的漏洞映射到出现该供应商字符串的网络映射中的所有服务器。

注释 自定义产品映射将应用于所有出现应用协议的位置，无论应用数据的源为何（如Nmap、主机输入功能或Firepower系统自身）。然而，如果使用主机输入功能导入的数据的第三方漏洞映射与通过自定义产品映射设置的映射发行冲突，则输入出现时，第三方漏洞映射将覆盖自定义产品映射并使用第三方漏洞映射设置。

可创建产品映射列表，然后通过激活或停用每份列表而一次性启用或禁用多个映射。指定将要映射到的供应商后，系统将更新产品列表，以仅包含该供应商提供的产品。

创建自定义产品映射后，必须激活自定义产品映射列表。激活自定义产品映射列表后，系统将更新出现指定供应商字符串的所有服务器。对于通过主机输入功能导入的数据，漏洞将更新，除非已为此服务器显式设置产品映射。

例如，如果贵公司将您的 Apache Tomcat Web 服务器的横幅修改为 `Internal Web Server`，则可将供应商字符串 `Internal Web Server` 映射到供应商 **Apache** 和产品 **Tomcat**，然后激活包含该映射的列表，出现标有 `Internal Web Server` 的服务器的所有主机均拥有数据库中的 Apache Tomcat 漏洞。

提示 可使用此功能将漏洞映至至本地入侵规则，只需将规则的 SID 映射至另一漏洞。

过程

步骤 1 选择策略 > 应用检测器。

步骤 2 点击自定义产品映射 (Custom Product Mappings)

步骤 3 点击 Create Custom Product Mapping List。

步骤 4 输入自定义产品映射列表名称 (Custom Product Mapping List Name)。

步骤 5 点击添加供应商字符串 (Add Vendor String)。

步骤 6 在供应商字符串 (Vendor String) 字段中，输入供应商字符串，该字符串标识应映射到所选供应商和产品值的应用。

步骤 7 从供应商 (Vendor) 下拉列表，选择要映射的供应商。

步骤 8 从产品 (Product) 下拉列表，选择要映射的产品。

步骤 9 点击添加 (Add)，以将已映射的供应商字符串添加到列表。

步骤 10 或者，在必要时，重复第 4 至 8 步，将额外的供应商字符串映射添加至列表。

步骤 11 点击保存 (Save)。

下一步做什么

- 激活自定义产品映射列表。有关详细信息，请参阅激活和停用自定义产品映射 ， 第 1924 页。

编辑自定义产品映射列表

可修改现有自定义产品映射列表，只需添加或移除供应商字符串或更改列表名称。

过程

步骤 1 选择策略 > 应用检测器。

步骤 2 点击自定义产品映射 (Custom Product Mappings)。

步骤 3 点击要编辑的产品映射列表旁边的 编辑（）。

如果显示视图（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 对列表进行更改，如创建自定义产品映射 ， 第 1923 页中所述。

步骤 5 完成后，点击 Save。

激活和停用自定义产品映射

可一次性启用或禁用整个自定义产品映射列表。激活自定义产品映射列表后，该列表上的每个映射均应用所有带有指定供应商字符串的应用，无论是通过受管设备检测到的，还是通过主机输入功能导入的。

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 点击**自定义产品映射 (Custom Product Mappings)**。

步骤 3 点击要激活或停用的自定义产品映射列表旁边的滑块。

如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

配置主机输入客户端

主机输入功能允许您从另一台设备上运行的客户端程序更新 管理中心的网络映射。例如，您可以从网络映射添加或删除主机，或者更新主机操作系统和服务信息。有关详细信息，请参阅《*Firepower* 系统主机输入 *API* 指南》。

只有先从“主机输入客户端”页面将客户端添加到 管理中心的对等数据库，然后才能运行远程客户端。还必须将管理中心生成的身份验证证书复制至客户端。完成这些步骤之后，客户端可连接到管理中心。

在多域部署中，可以在任何域中创建客户端。身份验证证书允许客户端为与客户端证书的域关联的任何分叶域提交网络映射更新。如果您为祖先域创建证书（或如果您的证书域在添加后代域之后成为祖先域），则使用该证书的任何客户端都必须指定每个事务的目标分叶域，如《*Firepower* 系统主机输入 *API* 指南》中所述。

“主机输入客户端”(Host Input Client) 仅显示与当前域关联的客户端，因此，如果您要下载或撤销证书，请切换至创建客户端时所在的域。

此连接使用 TLS 1.2。

过程

步骤 1 选择**集成** > **其他集成**。

步骤 2 点击**主机输入客户端 (Host Input Client)**。

步骤 3 点击 **Create Client**。

步骤 4 在 **Hostname** 字段中，输入运行主机输入客户端的主机的主机名称或 IP 地址。

注释 如果尚未配置 DNS 解析，请使用 IP 地址。

步骤 5 如果要对证书文件进行加密，请在**密码 (Password)** 字段中输入密码。

步骤 6 点击**保存 (Save)**。
主机输入服务将允许主机访问 管理中心上的 8307 端口，并会创建在客户端-服务器身份验证过程中使用的身份验证证书。

步骤 7 点击证书文件旁边的 **下载**（ ）。

步骤 8 将证书文件保存至客户端用于 SSL/TLS 身份验证的目录。

步骤 9 要撤消客户端的访问权限，请点击想要移除的主机旁边的 **删除**（ ）。

Nmap 扫描

Firepower 系统通过对网络上的流量进行被动分析构建网络映射。根据系统的情况，通过这种被动分析获取的信息有时可能并不完整。不过，您可以主动扫描主机，获取完整信息。例如，如果主机有一台服务器在开放端口上运行，但该服务器在系统监控网络期间未收发流量，则系统不会向网络映射添加有关该服务器的信息。但是，如使用主动扫描程序直接扫描主机，则可检测到服务器的存在。

Firepower 系统与用于网络探索和安全审核的开源主动扫描程序 Nmap™ 集成。

使用 Nmap 扫描主机时，系统会：

- 将之前未检测到的开放端口上的服务器添加至该主机配置文件中的服务器列表。主机配置文件在“扫描结果”(Scan Results) 部分列出在已过滤或关闭 TCP 端口或 UDP 端口上检测到的任何服务器。默认情况下，Nmap 扫描 1660 多个 TCP 端口。

  如果系统识别在 Nmap 扫描中已确定的服务器且有对应的服务器定义，系统会将 Nmap 用于该服务器的名称映射至对应的思科服务器定义。

- 然后，将扫描结果与超过1500个已知操作系统指纹进行对比，确定操作系统，并为每个操作系统评分。分配给主机的操作系统是得分最高的操作系统指纹。

  系统会将 Nmap 操作系统名称映射至思科操作系统定义。

- 为添加的服务器和操作系统将漏洞分配至主机。

注意：

- 只有网络映射中存在主机，Nmap 才能将其结果附加至主机配置文件。
- 如果从网络映射中删除主机，则将丢弃该主机的任何 Nmap 扫描结果。

提示 有些扫描选项（例如，端口扫描）会显著增加低带宽网络的负载。请将此类扫描安排在网络使用量较低的时段运行。

有关用于扫描的基础 Nmap 技术的详细信息，请参阅 http://insecure.org/ 上的 Nmap 文档。

Nmap 补救选项

可以创建 Nmap 补救以定义 Nmap 扫描设置。Nmap 补救可用作关联策略中的响应，按需运行，或预定在特定时间运行。

请注意，Nmap提供的服务器和操作系统数据将保持不变，直到您运行另一个Nmap扫描为止。如果计划使用 Nmap 扫描主机以获取操作系统和服务器数据，则可能要设置定期扫描，随时更新任何 Nmap 提供的操作系统和服务器数据。

下表说明可在 Nmap 补救中配置的选项。

表 *204: Nmap* 补救选项

选项	说明	对应的 Nmap 选项
扫描事件中的哪个地址？(Scan Which Address(es) From Event?)	将 Nmap 扫描用作对关联规则的响应时，选择以下其中一个选项以控制扫描事件中的哪个地址，源主机的地址和/或目标主机的地址： • **扫描源地址和目标地址 (Scan Source and Destination Addresses)**，扫描事件中源 IP 地址和目标 IP 地址代表的主机。 • **仅扫描源地址 (Scan Source Address Only)**，扫描事件的源 IP 地址代表的主机。 • **仅扫描目标地址 (Scan Destination Address Only)**，扫描事件的目标 IP 地址代表的主机。	不适用
扫描类型 (Scan Types)	选择 Nmap 如何扫描端口： • **TCP 同步 (TCP Syn)** 扫描可以快速连接到数千个端口，无需使用完整的 TCP 握手。此选项可用于在以下主机上以隐形模式快速扫描，可发起但不完成 TCP 连接：`admin` 帐户拥有原始数据包访问权限的主机，或未运行 IPv6 的主机。如果主机确认在 TCP Syn 扫描中发送的 Syn 数据包，Nmap 会重置连接。 • **TCP 连接 (TCP Connect)** 扫描使用 `connect()` 系统调用，打开穿过主机操作系统的连接。如果 管理中心或受管设备上的 `admin` 用户在主机上没有原始数据包权限，或正在扫描IPv6网络，则可使用“TCP 连接”扫描。换句话说，在无法使用“TCP 同步”(TCP Syn) 扫描的情况下使用此选项。 • **TCP ACK** 扫描发送 ACK 数据包，检查端口是否已被过滤。 • **TCP 窗口 (TCP Window)** 扫描的工作方式与 TCP ACK 扫描相同，但也可确定端口已打开还是关闭。 • **TCP Maimon** 扫描使用 FIN/ACK 探针识别 BSD 派生系统。	**TCP Syn**: `-sS` **TCP Connect**: `-sT` **TCP ACK**: `-sA` **TCP Window**: `-sW` **TCP Maimon**: `-sM`
扫描 UDP 端口 (Scan for UDP ports)	启用此选项，可扫描 UDP 端口以及 TCP 端口。请注意，扫描 UDP 端口可能比较耗时，因此，如果想快速扫描，请避免使用此选项。	`-sU`

选项	说明	对应的 Nmap 选项
使用事件中的端口 (Use Port From Event)	如果计划将补救用作关联政策中的响应，请启用此选项，使补救仅扫描在触发关联响应的事件中指定的端口。 • 选择**打开 (On)** 以扫描关联事件中的端口，而不是在 Nmap 补救配置过程中指定的端口。如果扫描关联事件中的端口，请注意，补救将扫描在 Nmap 补救配置过程中指定的 IP 地址上的端口。这些端口也会添加至补救的动态扫描目标。 • 选择**关闭 (Off)**，仅扫描在 Nmap 补救配置过程中指定的端口。 您也可以控制 Nmap 是否收集关于操作系统和服务器信息的信息。启用**使用事件中的端口 (Use Port From Event)** 选项，可扫描与新服务器关联的端口。	不适用
从报告检测引擎扫描 (Scan from reporting detection engine)	启用此选项，可从报告主机的检测引擎所驻留的设备扫描主机。 • 要从运行报告检测引擎的设备扫描，请选择**打开 (On)**。 • 要从已在补救中配置的设备扫描，请选择**关闭 (Off)**。	不适用
快速端口扫描 (Fast Port Scan)	启用此选项，仅扫描 `nmap-services` 文件中所列的 TCP 端口，而忽略其他端口设置，该文件位于执行扫描设备上的 `/var/sf/nmap/share/nmap/nmap-services` 目录中。请注意，不能同时使用此选项与**端口范围和扫描顺序 (Port Ranges and Scan Order)** 选项。 • 要仅扫描 `nmap-services` 文件中列出的端口，而忽略其他端口设置，请选择**打开 (On)**，该文件可在扫描设置上的 `/var/sf/nmap/share/nmap/nmap-services` 目录中找到。 • 要扫描所有 TCP 端口，请选择**关闭 (Off)**。	`-F`
端口范围和扫描顺序 (Port Ranges and Scan Order)	使用Nmap端口规范语法设置要扫描的特定端口及其扫描顺序。请注意，不能同时使用此选项与**快速端口扫描 (Fast Port Scan)** 选项。	`-p`
探测开放端口以获取供应商和版本信息(Probe open ports for vendor and version information)	启用此选项，可检测服务器供应商和版本信息。如果探测开放端口以获取服务器供应商和版本信息，Nmap将获取其用来识别服务器的服务器数据。然后，它会为该服务器替换思科服务器数据。 • 选择**On**，扫描主机上的开放端口以获取服务器信息，识别服务器厂商和版本。 • 选择**关闭 (Off)**，继续使用主机的思科服务器信息。	`-sV`

选项	说明	对应的 Nmap 选项
服务版本强度 (Service Version Intensity)	选择适用于服务器版本的 Nmap 探针强度。 • 要使用更多探针进行更精确、更长久的扫描，请选择一个较大的数字。 • 要使用更少探针进行不太精确、更加快速的扫描，请选择一个较小的数字。	`--version-intensity` <强度>
检测操作系统 (Detect Operating System)	启用此选项，可检测主机的操作系统信息。 如果配置主机的操作系统检测，Nmap将扫描主机，并使用扫描结果创建每个操作系统的评级，反映操作系统在主机上运行的可能性。 • 选择 **On**，扫描主机获取信息，识别操作系统。 • 选择**关闭 (Off)**，继续使用主机的思科操作系统信息。	`-o`
将所有主机视为在线 (Treat All Hosts As Online)	启用此选项，可跳过主机发现过程，在目标范围内的每台主机上运行端口扫描。请注意，启用此选项时，Nmap 会忽略**主机发现方法 (Host Discovery Method)** 和**主机发现端口列表 (Host Discovery Port List)** 的设置。 • 要跳过主机发现过程，在目标范围中的每台主机上运行端口扫描，请选择**打开 (On)**。 • 要使用**主机发现方法 (Host Discovery Method)** 和**主机发现端口列表 (Host Discovery Port List)** 设置执行主机发现，并跳过任何不可用的主机上的端口扫描，请选择**关闭 (Off)**。	`-PN`

选项	说明	对应的 Nmap 选项
主机发现方法 (Host Discovery Method)	选择此选项，在**主机发现端口列表 (Host Discovery Port List)** 中列出的端口上，为目标范围中的所有主机执行主机发现，或者，如未列出端口，则在适用于主机发现方法的默认端口上执行。 然而，请注意，如也启用**将所有主机视为在线 (Treat All Hosts As Online)**，**主机发现方法 (Host Discovery Method)** 选项不起作用，也不执行主机发现。 选择 Nmap 进行测试以查看主机是否存在且可用时使用的方法： • 如果收到响应，**TCP SYN** 选项将发送设置了 SYN 标记的空 TCP 数据包，并认为主机可用。默认情况下，TCP SYN 扫描端口 80。请注意，TCP SYN 扫描不太可能被设有状态性防火墙规则的防火墙拦截。 • 如果收到响应，**TCP ACK** 选项将发送设置了 ACK 标志的空 TCP 数据包，并认为主机可用。默认情况下，TCP ACK 也扫描端口 80。请注意，TCP ACK 扫描不太可能被设有无状态防火墙规则的防火墙拦截。 • 如果端口不可达响应来自已关闭端口，**UDP** 选项将发送 UDP 数据包，并假设主机可用性。默认情况下，UDP 扫描端口 40125。	**TCP SYN**: `-PS` **TCP ACK**: `-PA` **UDP**: `-PU`
主机发现端口列表 (Host Discovery Port List)	指定在执行主机发现时要扫描的自定义端口列表，用逗号隔开。	主机发现方法端口列表
默认 NSE 脚本 (Default NSE Scripts)	启用此选项，可以运行默认 Nmap 脚本集，执行主机发现以及服务器、操作系统和漏洞检测。请登录 https://nmap.org/nsedoc/categories/default.html，查看默认脚本列表。 • 要运行默认 Nmap 脚本集，请选择**打开 (On)**。 • 要跳过默认 Nmap 脚本集，请选择**关闭 (Off)**。	`-sC`
计时模板 (Timing Template)	选择扫描过程的时间；选择的数字越大，扫描越快、越不全面。	**0**: `T0` (paranoid) **1**: `T1` (sneaky) **2**: `T2` (polite) **3**: `T3` (normal) **4**: `T4` (aggressive) **5**: `T5` (insane)

Nmap 扫描准则

尽管主动扫描可以获取宝贵信息，但过度使用 Nmap 等工具可能会使您的网络资源超载，甚至使重要的主机瘫痪。使用任何主动式扫描工具时，应遵循这些准则创建扫描策略，确保仅扫描需要扫描的主机和端口。

选择适当的扫描目标

配置 Nmap 时，可创建扫描目标以识别要扫描的主机。扫描目标包括一个 IP 地址、CIDR 块或八位字节 IP 地址范围、IP 地址范围或要扫描的 IP 地址或范围列表，以及一台或多台主机上的端口。

可通过以下方式指定目标：

- 对于 IPv6 主机：
  - 确切的 IPv6 地址（例如 `2001:DB8:1::178:ABCD`）
- 对于 IPv4 主机：
  - 精确的 IP 地址（例如，`192.168.1.101`）或 IP 地址列表（用逗号或空格隔开）
  - 使用 CIDR 表示法的 IP 地址块（例如，`192.168.1.0/24` 扫描 192.168.1.1 和 192.168.1.254（含）之间的 254 台主机）
  - 使用八位字节范围寻址的 IP 地址范围（例如，`192.168.0-255.1-254` 扫描 192.168.x.x 范围内的所有地址，但以 .0 和 .255 结尾的地址除外）
  - 使用连字符的 IP 地址范围（例如，`192.168.1.1 - 192.168.1.5` 扫描在 192.168.1.1 和 192.168.1.5（含）之间的六台主机）
  - 地址或范围列表，用逗号或空格隔开（例如，`192.168.1.0/24`，`194.168.1.0/24` 扫描 192.168.1.1 和 192.168.1.254（含）之间的 254 台主机，以及 194.168.1.1 和 194.168.1.254（含）之间的 254 台主机）

Nmap扫描的理想扫描目标包括有系统无法识别的操作系统的主机、有无法识别的服务器的主机，或者最近在网络上检测到的主机。请记住，Nmap 结果不能添加到不存在于网络映射中主机的网络映射。

⚠

注意

- Nmap提供的服务器和操作系统数据将保持不变，直到您运行另一个Nmap扫描为止。如果计划使用 Nmap 来扫描主机，请定期安排扫描。
- 如果从网络映射中删除主机，将丢弃任何 Nmap 扫描结果。
- 请确保您有权限扫描您的目标。使用 Nmap 扫描不属于您或贵公司的主机可能违法。

选择适当端口进行扫描

可为已配置的每个扫描目标选择要扫描的端口。您可以指定各个端口号、端口范围或一系列端口号和端口范围，识别应当在每个目标上扫描的精确端口集。

默认情况下，Nmap 扫描 TCP 端口 1 至端口 1024。如果计划将补救用作关联政策中的响应，则可使补救仅扫描在触发关联响应的事件中指定的端口。如果按需运行补救或将补救作为预定任务加以运行，或者，如不使用来自事件的端口，则可使用其他端口选项确定哪些端口已扫描。可选择仅扫描在 `nmap-services` 文件中列出的 TCP 端口，忽略其他端口设置。除 TCP 端口外，还可扫描 UDP 端口。请注意，扫描UDP端口可能比较耗时，因此，如要快速扫描，请避免使用此选项。为选择要扫描的特定端口或端口范围，请使用 Nmap 端口规范语法识别端口。

设置主机发现选项

在开始主机的端口扫描之前，可决定是否执行主机发现，或者，可假设计划要扫描的所有主机均在线。如果选择不将所有主机视为在线，则可选择要使用的主机发现方法，如果需要，自定义在主机发现过程中扫描的端口列表。主机发现不能从已列出端口探测操作系统或服务器信息；它仅使用特殊端口上的响应确定主机是否活动且可用。如果执行主机发现且主机不可用，Nmap则不扫描该主机上的端口。

示例：使用 Nmap 解析未知操作系统

本示例介绍用于解析未知操作系统的 Nmap 配置。有关 Nmap 配置的完整介绍，请参阅管理 Nmap 扫描 ， 第 1934 页。

如果系统无法确定网络上主机的操作系统，则可使用Nmap主动扫描主机。Nmap使用其通过扫描获取的信息对可能的操作系统进行评级。然后，它使用评级最高的操作系统作为主机操作系统标识。

使用 Nmap 向新主机质询操作系统和服务器信息，会停用系统对已扫描主机的该数据进行的监控。如果使用 Nmap 发现系统标记为拥有未知操作系统的主机的主机操作系统和服务器操作系统，您也许能够识别相似的主机组。然后，可根据其中一个主机组创建自定义指纹，使系统能够根据 Nmap 扫描，将指纹与已知在主机上运行的操作系统相关联。尽可能创建自定义指纹，而不是通过第三方来源（例如，Nmap）输入静态数据，因为自定义指纹允许系统继续监控主机操作系统并按需更新。

在本例中，您将：

1. 配置扫描实例，如添加 Nmap 扫描实例 ， 第 1935 页中所述。
2. 使用以下设置创建 Nmap 补救：
   - 启用 **Use Port From Event**，可扫描与新服务器相关的端口。
   - 启用**检测操作系统 (Detect Operating System)**，可检测主机的操作系统信息。
   - 启用**探测开放端口以了解厂商和版本信息 (Probe open ports for vendor and version information)**，可检测服务器厂商和版本信息。
   - 启用**将所有主机视为在线 (Treat All Hosts as Online)**，因为已知该主机存在。
3. 创建在系统检测到具有未知操作系统的主机时触发的关联规则。该规则应在**发生发现事件**并且**主机的操作系统信息已更改**且符合以下条件时触发：**操作系统名称未知**。

4. 创建包含关联规则的关联策略。
5. 在关联策略中，将第 2 步中创建的 Nmap 补救作为响应添加至第 3 步中创建的规则。
6. 激活关联策略。
7. 清除网络映射上的主机，强制网络发现重新启动，重建网络映射。
8. 一两天后，搜索关联策略生成的事件。分析在主机上检测到的操作系统的Nmap结果，弄清网络上是否有系统无法识别的特殊主机配置。
9. 如果发现未知操作系统的Nmap结果相同的主机，请为其中一台主机创建自定义指纹，并用它识别未来的类似主机。

相关主题

创建 Nmap 补救，第 1938 页
Nmap 扫描结果，第 1941 页
为客户端创建自定义指纹，第 1914 页

示例：使用 Nmap 响应新主机

此示例介绍旨在对新主机作出响应的 Nmap 配置。有关 Nmap 配置的完整介绍，请参阅管理 Nmap 扫描，第 1934 页。

当系统在子网中检测到可能被入侵的新主机时，您可能想扫描该主机，确保获取该主机漏洞的准确信息。

要完成此操作，可创建和激活关联策略，当子网中出现新主机时进行检测，并启动补救以对该主机执行 Nmap 扫描。

为此，将会执行以下操作：

1. 配置扫描实例，如添加 Nmap 扫描实例，第 1935 页中所述。
2. 使用以下设置创建 Nmap 补救：
   - 启用 **Use Port From Event**，可扫描与新服务器相关的端口。
   - 启用**检测操作系统 (Detect Operating System)**，可检测主机的操作系统信息。
   - 启用**探测开放端口以了解厂商和版本信息 (Probe open ports for vendor and version information)**，可检测服务器厂商和版本信息。
   - 启用**将所有主机视为在线 (Treat All Hosts as Online)**，因为已知该主机存在。
3. 创建当系统在特定子网上检测到新主机时触发的关联规则。此规则应在**发生发现事件**并**检测到新主机时**触发。
4. 创建包含关联规则的关联策略。
5. 在关联策略中，将在以前步骤中创建的 Nmap 补救作为响应添加至在第 3 步中创建的规则。
6. 激活关联策略。

7. 收到出现新主机的通知时，检查主机配置文件，以查看Nmap扫描结果并解决适用于该主机的任何漏洞。

激活策略后，可以定期检查补救状态视图（**分析** > **关联** > **状态**）以查看补救启动时间。补救的动态扫描目标应当包括因服务器检测而扫描到的主机的 IP 地址。根据 Nmap 检测到的操作系统和服务器，查看这些主机的主机配置文件，弄清主机上是否存在需要解决的漏洞。

注意 如有大型或动态网络，新主机检测可能太频繁，而无法使用扫描进行响应。为防止资源超载，请避免使用 Nmap 扫描响应频繁发生的事件。另请注意，如果使用 Nmap 向新主机质询操作系统和服务器信息，则会停用思科对已扫描主机的该数据进行的监控。

相关主题

创建 Nmap 补救，第 1938 页

管理 Nmap 扫描

要使用 Nmap 扫描，至少必须配置一个 Nmap 扫描实例和一个 Nmap 补救。是否配置 Nmap 扫描目标可以选择。

过程

步骤 1 配置 Nmap 扫描：

- 如添加 Nmap 扫描实例，第 1935 页中所述，添加 Nmap 扫描实例。
- 如创建 Nmap 补救，第 1938 页中所述，创建 Nmap 补救。
- 或者，也可以如添加 Nmap 扫描目标，第 1936 页中所述，添加 Nmap 扫描目标。

步骤 2 运行 Nmap 扫描：

- 如运行按需 Nmap 扫描，第 1941 页中所述，运行按需 Nmap 扫描。
- 如《Cisco Secure Firewall Management Center 管理指南》的*Nmap* 扫描自动化中所述，配置自动 Nmap 扫描。
- 如《Cisco Secure Firewall Management Center 管理指南》的安排 *Nmap* 扫描中所述，安排自动 Nmap 扫描。

下一步做什么

- 通过查看相关任务，监控正在进行的 Nmap 扫描；请参阅《Cisco Secure Firewall Management Center 管理指南》中的查看任务消息。
- 或者，也可以优化扫描：
  - 如编辑 Nmap 扫描实例，第 1936 页中所述，编辑 Nmap 扫描实例。

- 如编辑 Nmap 扫描目标，第 1937 页中所述，编辑 Nmap 扫描目标。
- 如编辑 Nmap 补救，第 1940 页中所述，编辑 Nmap 补救。

添加 Nmap 扫描实例

可为要用于扫描网络漏洞的每个 Nmap 模块设置独立的扫描实例。可为 Cisco Secure Firewall Management Center上的本地 Nmap 模块以及要用于远程运行扫描的任何设备设置扫描实例。每次扫描的结果始终存储在 管理中心上，可在这里配置扫描，即使是从远程设备运行扫描。为防止意外或恶意扫描关键任务主机，可创建实例黑名单，指出不应通过实例扫描的主机。

不能添加名称与任何现有扫描实例相同的扫描实例。

在多域部署中，系统会显示在当前域中创建的扫描实例，您可以对其进行编辑。系统还会显示在祖先域中创建的扫描实例，您不可以对其进行编辑。要查看和编辑较低域中的扫描实例，请切换至该域。

过程

步骤 1 使用以下任一种方法访问 Nmap 扫描实例列表：

- 选择**策略** > **操作** > **实例**。
- 选择**策略** > **操作** > **扫描程序**。

步骤 2 添加补救：

- 如果通过上述第一种方法访问列表，请找到“添加新实例”(Add a New Instance) 部分，从下拉列表中选择“Nmap 补救”(Nmap Remediation) 模块，然后点击**添加 (Add)**。
- 如果通过上述第二种方法访问该列表，请点击**添加 Nmap 实例 (Add Nmap Instance)**。

步骤 3 输入**实例名称 (Instance Name)**。

步骤 4 输入**说明 (Description)**。

步骤 5 或者，在**豁免的主机 (Exempted hosts)** 字段中，使用以下语法指定任何 绝不应使用此扫描实例扫描的主机或网络：

- 对于 IPv6 主机，精确的 IP 地址（例如，`2001:DB8::fedd:eeff`）
- 对于 IPv4 主机，精确的 IP 地址（例如，`192.168.1.101`）或使用 CIDR 表示法的 IP 地址块（例如，`192.168.1.0/24` 扫描 `192.168.1.1` 和 `192.168.1.254` [含] 之间的 254 台主机）
- 请注意，不能使用感叹号 (!) 否定地址值。

注释 如果明确将黑名单网络中的主机作为扫描目标，该扫描将不运行。

步骤 6 或者，要从远程设备而非管理中心运行扫描，请在**远程设备名称 (Remote Device Name)** 字段中指定设备的 IP 地址或名称，因为它会显示在 管理中心 Web 界面中的设备“信息”(Information) 页面中。

步骤 7 点击**创建**。
系统创建完实例后，以编辑模式显示实例。

步骤 8 或者，将 Nmap 补救添加到实例。为此，请找到实例的“已配置补救”(Configured Remediations) 部分，点击**添加 (Add)**，然后创建补救，如创建 Nmap 补救，第 1938 页中所述。

步骤 9 点击**取消 (Cancel)**，返回实例列表。

注释 如果您通过**扫描程序 (Scanners)** 访问 Nmap 扫描实例列表，系统不会显示您添加的实例，除非您也将补救添加到该实例。要查看尚未添加补救的实例，请使用**实例 (Instances)** 菜单选项访问列表。

编辑 Nmap 扫描实例

当编辑扫描实例时，可以查看、添加和删除与实例关联的补救。不再想使用 Nmap 扫描实例中描述的 Nmap 模块时，请删除该 Nmap 扫描实例。请注意，如果删除扫描实例，也将删除使用该实例的任何补救。

在多域部署中，系统会显示在当前域中创建的扫描实例，您可以对其进行编辑。系统还会显示在祖先域中创建的扫描实例，您不可以对其进行编辑。要查看和编辑较低域中的扫描实例，请切换至该域。

过程

步骤 1 使用以下任一种方法访问 Nmap 扫描实例列表：

- 选择**策略** > **操作** > **实例**。
- 选择**策略** > **操作** > **扫描程序**。

步骤 2 在要编辑的实例旁，点击 **视图**（）。

步骤 3 对扫描实例设置进行更改，如添加 Nmap 扫描实例，第 1935 页中所述。

步骤 4 点击**保存 (Save)**。

步骤 5 点击 **Done**。

下一步做什么

- 或者，将新补救添加到扫描实例；请参阅 创建 Nmap 补救，第 1938 页
- 或者，编辑与实例关联的补救；请参阅编辑 Nmap 补救，第 1940 页。
- 或者，删除与实例关联的补救；请参阅运行按需 Nmap 扫描，第 1941 页。
- 或者，通过点击扫描目标旁边的 **删除**（） 来删除扫描实例。

添加 Nmap 扫描目标

配置 Nmap 模块时，可创建和保存扫描目标，识别想在执行按需或预定扫描时作为扫描目标的主机和端口，从而避免每次构建新扫描目标。扫描目标包括一个或一组要扫描的 IP 地址，以及一台或多

台主机上的端口。对于 Nmap 目标，也可使用 Nmap 八位字节范围寻址或 IP 地址范围。有关 Nmap 八位组范围寻址的详细信息，请参阅 http://insecure.org 上的 Nmap 文档。

注意：

- 扫描包含大量主机的扫描目标可能需要延长的时间。作为一种解决方法，每次仅扫描几台主机。
- Nmap提供的服务器和操作系统数据将保持不变，直到您运行另一个Nmap扫描为止。如果计划使用 Nmap 来扫描主机，请定期安排扫描。如果从网络映射中删除主机，将丢弃任何 Nmap 扫描结果。
- 在多域部署中，系统会显示在当前域中创建的扫描目标，您可以对其进行编辑。系统还会显示在祖先域中创建的扫描目标，您不可以对其进行编辑。要查看和编辑较低域中的扫描目标，请切换至该域。

过程

步骤 1 选择**策略** > **操作** > **扫描程序**。

步骤 2 在工具栏上，点击 **Targets**。

步骤 3 点击 **Create Scan Target**。

步骤 4 在**名称 (Name)** 字段中，输入要用于此扫描目标的名称。

步骤 5 在 **IP 范围 (IP Range)** 文本框中，使用Nmap 扫描准则，第 1931 页中所述的语法指定要扫描的一个或多个主机。

注释 如果在扫描目标中的 IP 地址或范围列表中使用逗号，则保存目标时，逗号将转换为空格。

步骤 6 在**端口 (Ports)** 字段中，指定要扫描的端口。

可使用从 1 到 65535 的值输入以下任意项：

- 端口号
- 用逗号分隔的端口列表
- 用连接号分隔的端口号范围
- 多个用连接号分隔的端口号范围，用逗号分隔

步骤 7 点击**保存 (Save)**。

编辑 Nmap 扫描目标

提示 如果不想使用补救扫描特定 IP 地址，但是该 IP 地址已添加至目标，则可能想编辑补救的动态扫描目标，因为主机参与了启动补救的关联策略违反事件。

如果不再想扫描已在扫描目标中列出的主机，请删除扫描目标。

在多域部署中，系统会显示在当前域中创建的扫描目标，您可以对其进行编辑。系统还会显示在祖先域中创建的扫描目标，您不可以对其进行编辑。要查看和编辑较低域中的扫描目标，请切换至该域。

过程

步骤 1 选择**策略** > **操作** > **扫描程序**。

步骤 2 在工具栏上，点击 **Targets**。

步骤 3 点击要编辑的扫描目标旁边的 **编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 按需进行修改。有关详细信息，请参阅添加 Nmap 扫描目标，第 1936 页。

步骤 5 点击**保存**。

步骤 6 或者，通过点击扫描目标旁边的 **删除**（） 来删除扫描目标。

创建 Nmap 补救

Nmap补救只可以通过将它添加到现有Nmap扫描实例来创建。补救定义了扫描的设置。它可用作关联策略中的响应、按需运行或在指定时间作为预定任务运行。

Nmap提供的服务器和操作系统数据将保持不变，直到您运行另一个Nmap扫描为止。如果计划使用 Nmap 来扫描主机，请定期安排扫描。如果从网络映射中删除主机，将丢弃任何 Nmap 扫描结果。

有关 Nmap 功能的一般信息，请参阅 http://insecure.org 上的 Nmap 文档。

在多域部署中，系统会显示在当前域中创建的 Nmap 补救，您可以对其进行编辑。系统还会显示在祖先域中创建的 Nmap 补救，您不可以对其进行编辑。要查看和编辑较低域中的 Nmap 补救，请切换至该域。

开始之前

- 如添加 Nmap 扫描实例，第 1935 页中所述，添加 Nmap 扫描实例。

过程

步骤 1 选择**策略** > **操作** > **实例**。

步骤 2 点击要添加补救的实例旁边的 **视图**（）。

步骤 3 在“已配置补救”(Configured Remediations) 部分，点击**添加 (Add)**。

步骤 4 输入**补救名称 (Remediation Name)**。

步骤 5 输入**说明 (Description)**。

步骤 6 如果计划使用此补救响应在发生入侵事件、连接事件或用户事件时触发的关联规则，请配置**扫描事件中的哪个地址？(Scan Which Address(es) From Event?)** 选项。

提示 如果计划使用此补救响应在发生发现事件或主机输入事件时触发的关联规则，默认情况下，补救将扫描事件涉及到的主机的 IP 地址；无需配置此选项。

注释 请**勿**为了响应在流量配置文件发生变化时触发的关联规则而分配 Nmap 补救。

步骤 7 配置**扫描类型 (Scan Type)** 选项。

步骤 8 或者，除了 TCP 端口，还要扫描 UDP 端口，请为**扫描 UDP 端口 (Scan for UDP ports)** 选项选择**开启 (On)**。

提示 UDP 端口扫描比 TCP 端口扫描需要更多的时间。要加速扫描，请禁用此选项。

步骤 9 如果计划使用此补救响应关联策略违反事件，请配置**使用事件中的端口 (Use Port From Event)** 选项。

步骤 10 如果计划使用此补救响应关联策略违反事件，并希望使用运行检测引擎来检测事件的设备运行扫描，请配置**从报告检测引擎扫描 (Scan from reporting detection engine)** 选项。

步骤 11 配置**快速端口扫描 (Fast Port Scan)** 选项。

步骤 12 在**端口范围和扫描顺序 (Port Ranges and Scan Order)** 字段中，输入要在默认情况下使用 Nmap 端口规范语法按自己想要的顺序扫描的端口。

使用以下格式：

- 指定从 1 到 65535 的值。
- 使用逗号或空格分隔端口。
- 使用连字符指明端口范围。
- 扫描 TCP 和 UDP 端口时，以 T 作为要扫描的 TCP 端口列表的开端，以 U 作为 UDP 端口列表的开端。

注释 启动补救以响应关联策略违反事件时，**使用事件中的端口 (Use Port From Event)** 选项将覆盖此设置，如第 8 步中所述。

示例：

要扫描 UDP 流量的端口 53 和 111，然后扫描 TCP 流量的端口 21-25，请输入 `U:53,111,T:21-25`。

步骤 13 要探测开放端口以了解服务器厂商和版本信息，请配置**探测开放端口以获取供应商和版本信息 (Probe open ports for vendor and version information)**。

步骤 14 如果选择探测开放端口，请从**服务版本强度 (Service Version Intensity)** 下拉列表中选择一个数字，设置使用的探针数量。

步骤 15 要扫描操作系统信息，请配置**检测操作系统 (Detect Operating System)** 设置。

步骤 16 要确定主机发现是否发生，是否仅针对可用端口运行端口扫描，请配置**将所有主机视为在线 (Treat All Hosts As Online)**。

步骤 17 要设置希望 Nmap 在测试主机可用性时使用的方法，请从**主机发现方法 (Host Discovery Method)** 下拉列表中选择一种方法。

步骤 18 如果要在主机发现过程中扫描自定义端口列表，请在**主机发现端口列表 (Host Discovery Port List)** 字段中输入适合所选主机发现方法的端口列表，用逗号隔开。

步骤 19 配置**默认 NSE 脚本 (Default NSE Scripts)** 选项，控制是否使用默认 Nmap 脚本集进行主机发现以及服务器、操作系统和漏洞发现。

提示 请参阅 http://nmap.org/nsedoc/categories/default.html，获取默认脚本列表。

步骤 20 要设置扫描过程的时间选择，请从**计时模板 (Timing Template)** 下拉列表中选择计时模板编号。

选择的编号越大，速度越快，扫描越不全面；而选择的编号越小，速度越慢，扫描越全面。

步骤 21 点击**创建**。
系统创建完补救后，在编辑模式中显示它。

步骤 22 点击**完成 (Done)** 以返回相关实例。

步骤 23 点击**确定 (OK)** 以返回实例列表。

相关主题

Nmap 补救选项，第 1926 页

编辑 Nmap 补救

对 Nmap 补救所做的更改不会影响正在进行的扫描。新设置将在下一次扫描开始时生效。删除不再需要的 Nmap 补救。

在多域部署中，系统会显示在当前域中创建的 Nmap 补救，您可以对其进行编辑。系统还会显示在祖先域中创建的 Nmap 补救，您不可以对其进行编辑。要查看和编辑较低域中的 Nmap 补救，请切换至该域。

过程

步骤 1 使用以下任一种方法访问 Nmap 扫描实例列表：

- 选择**策略** > **操作** > **实例**。
- 选择**策略** > **操作** > **扫描程序**。

步骤 2 访问要编辑的补救：

- 如果通过上述第一种方法访问列表，请点击相关实例旁的**视图**（  ），然后在要在“已配置补救”部分中编辑的补救旁边再次点击该补救。
- 如果通过上述第二种方法访问列表，请点击要编辑的补救边的**视图**（  ）。

步骤 3 根据需要进行修改，如创建 Nmap 补救，第 1938 页中所述。

步骤 4 如果要保存更改，请点击**保存 (Save)**，或者如果要不保存而直接退出，请点击**完成 (Done)**。

步骤 5 或者，通过点击补救旁边的**删除**（  ）来删除补救。

运行按需 Nmap 扫描

可在需要时启动按需 Namp 扫描。可以通过输入要扫描的 IP 地址和端口或者通过选择现有扫描目标，指定按需扫描目标。

Nmap提供的服务器和操作系统数据将保持不变，直到您运行另一个Nmap扫描为止。如果计划使用 Nmap 来扫描主机，请定期安排扫描。如果从网络映射中删除主机，将丢弃任何 Nmap 扫描结果。

开始之前

- 或者，添加 Nmap 扫描目标；请参阅添加 Nmap 扫描目标 ， 第 1936 页。

过程

步骤 1 选择**策略** > **操作** > **扫描程序**。

步骤 2 在要用于执行扫描的 Nmap 补救旁，点击 **扫描** （ ）。

步骤 3 或者，要使用已保存的扫描目标进行扫描，请从**已保存的目标 (Saved Targets)** 下拉列表中选择目标，然后点击**加载 (Load)**。

步骤 4 在 **IP 范围 (IP Range[s])** 字段中，指定要扫描或修改已加载列表的主机的 IP 地址。

注意：

- 对于带 IPv4 地址的主机，可指定多个 IP 地址，用逗号隔开，或者使用 CIDR 表示法。也可在 IP 地址前面添加感叹号 (!)，否定 IP 地址。
- 对于带 IPv6 地址的主机，请使用精确的 IP 地址。不支持地址范围。

步骤 5 在**端口 (Ports)** 字段中，指定要扫描的端口或修改已加载的列表。

可输入一个端口号、用逗号隔开的端口列表或者用连接号隔开的端口号范围。

步骤 6 在多域部署中，使用**域 (Domain)** 字段指定要执行扫描的分叶域。

步骤 7 点击 **Scan Now**。

下一步做什么

- 或者，监控任务状态；请参阅 《Cisco Secure Firewall Management Center 管理指南》中的 查看任务消息 。

Nmap 扫描结果

您可以监控正在进行的Nmap扫描，导入先前通过 Firepower 系统执行的扫描中的结果或在 Firepower 系统外执行的结果，以及查看和分析扫描结果。

您可查看作为弹出窗口中渲染页面的扫描结果（使用本地 Nmap 模块创建），也可下载原始 XML 格式的 Nmap 结果文件。

您还可在主机配置文件和网络映射中查看由 Nmap 检测到的操作系统和服务器信息。如果主机扫描为已过滤或已关闭端口上的服务器生成服务器信息，或者如果扫描收集无法包含在操作系统信息或服务器部分中的信息，主机配置文件会将这些结果纳入“Nmap 扫描结果”(Nmap Scan Results) 部分。

查看 Nmap 扫描结果

当 Nmap 扫描完成后，可以查看扫描结果表。

可以根据所查找的信息操作结果视图。您在访问扫描结果时看到的页面将随您所使用的工作流程而变化。可使用预定义的工作流程，其中包括扫描结果表视图。还可创建自定义工作流程，仅显示匹配特定需求的信息。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

可在 http://insecure.org 上下载 Nmap 结果，并使用 Nmap 1.01 DTD 查看。

还可清除扫描结果。

过程

步骤 1 选择**策略** > **操作** > **扫描程序**。

步骤 2 在工具栏上，点击**扫描结果 (Scan Results)**。

步骤 3 有以下选项可供选择：

- 调整时间范围，如《Cisco Secure Firewall Management Center 管理指南》中的事件时间限制所述。
- 要使用不同的工作流程，包括自定义工作流程，请按工作流程标题点击 **(switch workflows)** 。
- 要查看作为弹出窗口中页面已渲染的扫描结果，请点击扫描作业旁的**查看**。
- 要保存扫描结果文件的副本，以便在任何文本编辑器中查看原始 XML 代码，请在扫描作业旁点击**下载 (Download)**。
- 要对扫描结果排序，请点击列标题。再次点击列标题以反转排列顺序。
- 要限制显示的列，请在要隐藏的列标题中点击**关闭**（×）。在显示的弹出窗口中，点击**Apply**。

  提示 要隐藏或显示其他列，请选中或清除相应的复选框，然后点击**应用 (Apply)**。要将已禁用列添加回视图中，请点击展开箭头展开搜索限制条件，然后点击**已禁用列 (Disabled Columns)** 下的列名称。

- 要向下展开到工作流程中的下一个页面，请参阅《Cisco Secure Firewall Management Center 管理指南》中的使用向下钻取页面。
- 要配置扫描实例和补救，请点击工具栏中的**扫描工具 (Scanners)** 并参阅管理 Nmap 扫描，第 1934 页。
- 要在工作流程页面之内及在各工作流程页面之间导航，请参阅《Cisco Secure Firewall Management Center 管理指南》中的工作流程页面导航工具。

- 要导航至其他事件视图以查看关联的事件，请从**跳至 (Jump to)** 下拉列表中选择要查看的事件视图的名称。
- 要搜索扫描结果，请在相应字段中输入搜索条件。

相关主题

Nmap 扫描结果字段，第 1943 页

Nmap 扫描结果字段

运行 Nmap 扫描时，管理中心 在数据库中收集扫描结果。下表介绍了扫描结果表中可以查看和搜索的字段。

表 *205:* 扫描结果字段

字段	说明 (Description)
开始时间	生成结果的扫描的开始日期和时间。
结束时间	生成结果的扫描的结束日期和时间。
目标	生成结果的扫描的扫描目标的 IP 地址（或主机名，如果 DNS 解析已启用）。
扫描类型 (Scan Type)	要么是 `Nmap`，要么是第三方扫描工具的名称，指明生成结果的扫描的类型。
扫描模式 (Scan Mode)	生成结果的扫描的模式： • `On Demand` - 来自按需扫描的结果。 • `导入` - 来自不同系统上扫描的结果，和已导入 管理中心的结果。 • `预定 (Scheduled)` - 来自作为预定任务运行的扫描的结果。
结果	扫描的结果。
域	扫描目标的域。此字段只存在于多域部署中。

导入 Nmap 扫描结果

您可以导入在 Firepower 系统外执行的 Nmap 扫描所创建的 XML 结果文件。您还可以导入先前从 Firepower 系统下载的 XML 结果文件。要导入 Nmap 扫描结果，结果文件必须采用 XML 格式，且兼容于 Nmap 1.01 DTD。有关创建 Nmap 结果的详细信息以及 Nmap DTD 的详细信息，请参阅 http://insecure.org 上的 Nmap 文档。

主机必须已存在于网络映射中，然后 Nmap 才能将其结果附加到主机配置文件。

过程

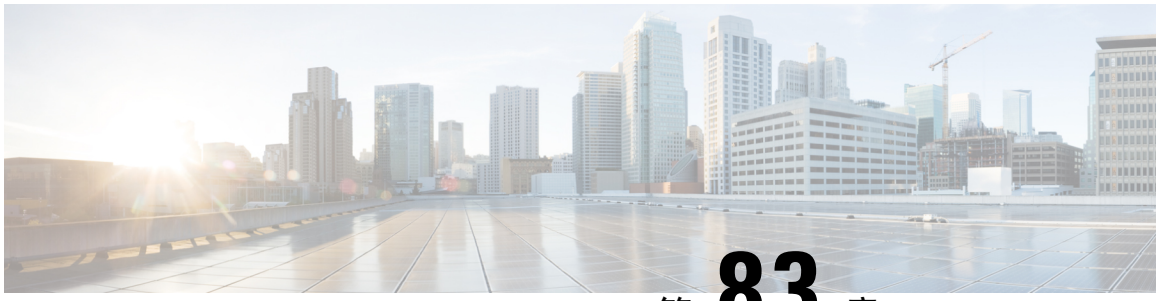
步骤 1 选择策略 > 操作 > 扫描程序。

步骤 2 在工具栏上，点击 **Import Results**。

步骤 3 在多域部署中，从域 **(Domain)** 下拉列表中选择分叶域以指定要存储导入结果的位置。

步骤 4 点击浏览 **(Browse)**，导航至结果文件。

步骤 5 返回“导入结果”(Import Results) 页面后，点击导入 **(Import)**，导入结果。



第 83 章

应用检测

以下主题介绍 Firepower 系统应用检测：

概述：应用检测

当 Firepower 系统分析 IP 流量时，它会尝试识别网络上的常用应用。应用感知对于应用控制至关重要。

系统检测的应用有三种类型：

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

系统根据在检测器中指定的特征识别网络流量中的应用。例如，系统可以通过数据包报头中的ASCII模式识别应用。此外，安全套接字层(SSL)协议检测程序使用安全会话的信息来识别会话中的应用。

在 Firepower 系统中有两个应用检测器来源：

- 系统提供的检测器检测 Web 应用、客户端和应用协议。

系统提供的应用检测器（和操作系统）的可用性取决于 Firepower 系统的版本和已安装的 VDB 版本。版本说明和公告包含关于新的和更新的检测器的信息。也可以导入专业服务开发的各个检测器。

- 自定义应用协议检测器由用户创建并检测 Web 应用、客户端和应用协议。

您还可以通过隐含应用协议检测来检测应用协议，此检测根据对客户端的检测暗示应用协议的存在。

如在网络发现策略中所定义，系统仅识别受监控网络中的主机上运行的应用协议。例如，如果内部主机访问未受监控的远程站点的 FTP 服务器，系统不会将应用协议识别为 FTP。另一方面，如果远程或内部主机访问正受监控主机上的 FTP 服务器，系统能够正确识别应用协议。

如果系统可以识别受监控主机用于连接到未受监控服务器的客户端，则系统会识别客户端的对应应用协议，但是不将该协议添加到网络映射中。请注意，客户端会话必须包括来自要发生应用检测的服务器的响应。

系统会确定其检测到的每个应用的特征；请参阅应用特征，第 1252 页。系统使用这些特征创建应用组，称为应用过滤器。应用过滤器用于执行访问控制以及限制报告和控制面板构件中使用的搜索结果和数据。

您还可以使用导出的 NetFlow 记录、Nmap 主动扫描和主机输入功能补充应用检测器数据。

相关主题

配置应用控制的最佳实践，第 1250 页
应用检测器基础知识，第 1946 页

应用检测器基础知识

Firepower 系统使用应用检测器来识别网络上的常用应用。使用“检测器”页面（**策略 > 应用检测器**）查看检测器列表和自定义检测功能。

是否能修改检测器或更改其状态（活动或非活动）取决于其类型。系统仅使用活动检测器来分析应用流量。

注释 思科提供的检测器可能会随 Firepower 系统和 VDB 更新而更改。有关已更新的检测器的信息，请参阅版本说明和咨询。

注释 对于Firepower应用标识，不会特意列出端口。不会为任何思科应用报告应用的关联端口，因为大多数应用都与端口无关。我们平台的检测功能可以识别在网络中的任何端口运行的服务。

思科提供的内部检测器

内部检测器是一种特殊类别的检测器，适用于客户端、Web 应用和应用协议流量。内部检测器随系统更新一起提供，并且永远在线。

如果应用与旨在检测客户端相关活动的内部检测器匹配且不存在特定客户端检测器，则可以报告通用客户端。

思科提供的客户端检测器

客户端检测器用于检测客户端流量，并且通过VDB或系统更新提供，或由思科专业服务提供用于导入。可以激活和停用客户端检测器。仅当导入客户端检测器后，才可以将其导出。

思科提供的 Web 应用检测器

Web 应用检测器用于检测 HTTP 流量负载中的 Web 应用，并且通过 VDB 或系统更新提供。Web 应用检测器永远在线。

思科提供的应用协议（端口）检测器

基于端口的应用协议检测器使用已知端口识别网络流量。此类检测器通过VDB或系统更新提供，或由思科专业服务提供用于导入。可以激活和停用应用协议检测器，还可查看检测器定义，以便将其用作自定义检测器的基础。

思科提供的应用协议 (Firepower) 检测器

基于 *Firepower* 的应用协议检测器用于使用 Firepower 应用指纹分析网络流量，并且通过 VDB 或系统更新提供。可以激活和停用应用协议检测器。

自定义应用检测器

自定义应用检测器基于模式。它们将检测来自客户端的数据包、Web应用或应用协议流量中的模式。对于已导入检测器和自定义检测器，您将拥有完全控制权。

在 Web 界面中识别应用协议

下表概述了系统如何识别检测到的应用协议：

表 *206:* 系统识别应用协议

标识	说明
应用协议名称	如果应用协议属于以下情况，管理中心将会使用应用协议名称来识别应用协议： • 由系统正确识别出 • 使用 NetFlow 数据识别出，并且 `/etc/sf/services` 中有端口应用协议关联 • 使用主机输入功能手动识别出 • 由 Nmap 或其他活动源识别出

标识	说明
pending	如果系统既不能正确识别也不能错误识别应用，管理中心会将应用协议识别为 pending。 大多数情况下，系统需要收集和分析更多的连接数据才能识别待处理应用。 在应用详细信息表、服务器表和主机配置文件中，只会对在其中检测到（而不是由检测到的客户端或 Web 应用流量推断）特定应用协议流量的应用协议显示 pending 状态。
unknown	在以下情况下，管理中心会将应用协议识别为 unknown： • 应用不匹配系统的任何检测器。 • 应用协议是使用 NetFlow 数据识别出的，但 /etc/sf/services 中没有端口应用协议关联。 • Snort 已关闭会话，但它仍存在于设备中。在这里，流量可以通过防火墙，但不会检测到应用。
空白	已检查检测到的所有可用数据，但没有识别出应用协议。在应用详细信息表、服务器表中和主机配置文件中，对于在其中没有检测到应用协议的非 HTTP 通用客户端数据流量，应用协议留空。

通过客户端检测进行隐含应用协议检测

如果系统可以识别受监控主机用于访问未受监控主机的客户端，管理中心会推断该连接使用与该客户端对应的应用协议。（由于系统仅跟踪监控网络上的应用，因此，连接日志通常不包含有关监控主机用于访问未受监控的服务器的连接的应用协议信息。）

此过程，或隐含应用协议检测，具有以下结果：

- 由于系统不会为这些服务器生成新的 TCP 端口或新的 UDP 端口事件，因此，服务器不会显示在服务器表中。此外，不能将对这些应用协议的检测作为条件来触发事件警报或关联规则。
- 由于应用协议未与主机关联，因此，不能查看主机配置文件中的详细信息，不能设置其服务器身份，也不能使用流量量变曲线或关联规则的主机配置文件限定条件中的信息。此外，系统不会根据此类检测将漏洞与主机关联。

但是，您可以触发有关连接中是否存在应用协议信息的关联事件。还可以使用连接日志中的应用协议信息创建连接跟踪程序和流量量变曲线。

主机限制和发现事件日志记录

如果系统检测到客户端、服务器或网络应用，它会生成发现事件，除非关联的主机已达到客户端、服务器或网络应用的最大数量。

主机配置文件最多为每个主机显示 16 个客户端、100 个服务器和 100 个网络应用。

请注意，依赖于客户端、服务器或网络应用检测的操作不受此限制的影响。例如，经配置要在服务器上触发的访问控制规则仍会记录连接事件。

应用检测的特殊注意事项

SFTP

为了检测 SFTP 流量，同一规则还必须检测 SSH。

Squid

在以下情况下，系统会积极识别 Squid 服务器流量：

- 系统检测从受监控网络上的主机到启用了代理身份验证的 Squid 服务器的连接；或
- 系统检测从受监控网络上的 Squid 代理服务器到目标系统（即，客户端正在其中请求信息或其他资源的目标服务器）的连接。

但是，在以下情况下，系统无法识别 Squid 服务流量：

- 受监控网络上的主机连接到已禁用代理身份验证的 Squid 服务器；或
- Squid 代理服务器被配置为从其 HTTP 响应中移除“通过：”报头字段

SSL 应用检测

系统提供可以使用安全套接字层 (SSL) 会话中的会话信息识别会话中的应用协议、客户端应用或 Web 应用的应用检测器。

如果系统检测到加密连接，它会将该连接标记为通用 HTTPS 连接或更为具体的安全协议，例如 SMTPS（如果适用）。如果系统检测到 SSL 会话，它会将 `SSL client` 添加到该会话的连接事件中的 **客户端 (Client)** 字段。如果识别到会话的 Web 应用，系统会为该流量生成发现事件。

对于 SSL 应用流量，受管设备还可以检测服务器证书中的公用名并将其与 SSL 主机模式的客户端或 Web 应用比对。当系统识别到特定客户端时，会将 `SSL client` 替换为该客户端的名称。

由于 SSL 应用流量已加密，因此系统只能使用证书中的信息（而不是加密数据流中的应用数据）进行标识。为此，SSL 主机模式有时只能识别作为应用编写者的公司，因此同一公司开发的 SSL 应用可能有相同的标识。

在某些情况下，例如 HTTPS 会话是从 HTTP 会话内部发起时，受管设备会从客户端数据包中的客户端证书检测服务器名称。

要启用 SSL 应用标识，必须创建监控响应方流量的访问控制规则。这些规则必须包含适用于 SSL 应用的应用条件或者使用来自 SSL 证书的 URL 的 URL 条件。对于网络发现，响应方 IP 地址不必位于要在网络发现策略中监控的网络上；访问控制策略配置决定是否识别流量。要识别 SSL 应用的检测，您可以在应用检测器列表中或在访问控制规则中添加应用条件时按 `SSL protocol` 标记进行过滤。

推荐的 Web 应用

Web 服务器有时会将流量推荐到其他网站，这些网站通常是广告服务器。为帮助您更好地理解网络上出现的推荐流量的情景，系统在推荐会话的事件的 **Web 应用 (Web Application)** 字段中列出推荐流量的 Web 应用。VDB 包含已知被推荐站点的列表。如果系统检测到来自这些站点之一的流量，会将推荐站点连同该流量的事件一起存储。例如，如果通过Facebook访问的广告实际在Advertising.com上托管，则检测到的 Advertising.com 流量与 Facebook Web 应用关联。系统还可以检测到 HTTP 流量中的推荐 URL，例如当网站提供与另一站点的简单链接时；在这种情况下，推荐 URL 出现在 HTTP Referrer 事件字段。

在事件中，如果存在推荐应用，它将被列为流量的 Web 应用，而 URL 则是被推荐站点的 URL。在上述示例中，用于流量的连接事件的 Web 应用是 Facebook，但 URL 是 Advertising.com。在下列情况下，被推荐的应用可能显示为 Web 应用：未检测到推荐 Web 应用，主机推荐其本身，或者存在推荐链。在控制面板中，Web 应用的连接和字节数包括 Web 应用与该应用推荐的流量关联的会话数。

请注意，如果创建专门针对被推荐流量的规则，应该为被推荐应用（而不是推荐应用）添加条件。例如，要阻止从 Facebook 推荐的 Advertising.com 流量，可以向 Advertising.com 应用的访问控制规则添加应用条件。

Snort 2 和 Snort 3 中的应用检测

在 Snort 2 中，您可以通过访问控制策略中的限制和网络发现策略中的网络过滤器来启用或禁用应用检测。但是，访问控制策略中的限制可以覆盖网络过滤器，同时启用应用检测。例如，如果您在网络发现策略中定义了网络过滤器，并且当访问控制策略具有需要应用检测的限制（例如 SSL、URL SI、DNS SI 等）时，则这些网络发现过滤器会被覆盖，并且所有网络会进行应用检测。Snort 3 不支持此 Snort 2 功能。

注释 Snort 3 现在与 Snort 2 相同，如果 AC 策略中没有其他配置需要 AppID 来监控所有流量，则只会在网络发现策略过滤器中定义的特定网络子网上启用 AppID 检查。

在 Snort 3 中，默认情况下始终为所有网络启用应用检测。要禁用应用检测，请执行以下操作：

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，点击编辑策略并删除应用规则。

步骤 2 选择**策略 (Policies)** > **SSL**，点击删除以删除 SSL 策略。

步骤 3 选择**策略 (Policies)** > **网络发现 (Network Discovery)**，点击删除以删除网络发现策略。

步骤 4 选择**策略 (Policies)** > **访问控制 (Access Control)**，点击编辑策略，然后选择**安全情报 (Security Intelligence)** > **URLs** 选项卡以删除 URL 允许或阻止列表。

步骤 5 由于您无法删除默认 DNS 规则，请选择**策略 (Policies)** > **DNS**，点击编辑并取消选中启用框以禁用 DNS 策略。

步骤 6 在访问控制策略的**高级 (Advanced)** 设置下，禁用启用威胁情报导向器 *(Enable Threat Intelligence Director)* 和对 *DNS* 流量启用信誉实施 *(Enable reputation enforcement on DNS traffic)* 选项。

步骤 7 保存并部署访问控制策略。

应用检测的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 发现管理员

自定义应用检测器

如果在网络上使用自定义应用，您可以创建自定义的 Web 应用、客户端或应用协议检测器，它们可向系统提供识别应用所需的信息。应用检测器的类型由您在**协议 (Protocol)**、**类型 (Type)** 和**方向 (Direction)** 字段中进行的选择确定。

只有客户端会话包含来自服务器的响应器数据包，系统才能开始检测和识别服务器流量中的应用协议。请注意，对于 UDP 流量，系统将响应器数据包的来源指定为服务器。

如果已经在另一管理中心上创建了检测器，可将其导出后，再导入至此管理中心。然后，可根据自己的需求编辑已导入的检测器。您可导出和导入自定义检测器以及思科专业服务提供的检测器。但是，您**无法**导出或导入思科提供的任何其他类型检测器。

自定义应用检测器和用户定义的应用字段

可以使用以下字段配置自定义应用检测器和用户定义的应用。

自定义应用检测器字段：常规

使用以下字段配置基本和高级自定义应用检测器。

应用协议

要检测的应用协议。这可以是系统提供的应用或用户定义的应用。

如果要让应用免于执行主动身份验证（在身份规则中配置），则必须选择或创建带**用户代理排除项 (User-Agent Exclusion)** 标记的应用协议。

说明

应用检测器的说明。

名称

应用检测器的名称。

检测器类型 (Detector Type)

检测器的类型，**基本 (Basic)** 或**高级 (Advanced)**。基本应用检测器是在 Web 界面中作为一系列字段而创建的。高级应用检测器是在外部创建并作为自定义 .lua 文件上传的。

自定义应用检测器字段：检测模式

使用以下字段配置基本自定义应用检测器的检测模式。

方向

检测器应当检查的流量源，包括**客户端 (Client)** 或**服务器 (Server)**。

偏移

以字节为单位表示的在数据包中的位置，从数据包负载起始位置（系统应开始搜索模式的位置）开始。

因为数据包负载从 0 字节开始，请按以下方法计算偏移：将想要从数据包负载起始位置前移的字节数减去 1。例如，要查找数据包的第 5 个位中的模式，请在**偏移 (Offset)** 字段键入 4。

模式

与您选择的**类型 (Type)** 相关联的模式字符串。

端口

检测器应检查流量的端口。

协议

要检测的协议。选择的协议将确定是显示**类型 (Type)** 还是 **URL** 字段。

该协议（以及在某些情况下，您在**类型 [Type]** 和**方向 [Direction]** 字段中的后续选择）将确定您创建的应用检测器类型：Web 应用、客户端或应用协议。

检测器类型 (Detector Type)	协议	类型或方向
Web 应用程序	HTTP	**类型 (Type)** 为**内容类型 (Content Type)** 或 **URL**
	RTMP	任意
	SSL	任意

检测器类型 (Detector Type)	协议	类型或方向
客户端	HTTP	类型 (Type) 为用户代理 (User Agent)
	SIP	任意
	TCP 或 UDP	方向 (Direction) 为客户端 (Client)
应用协议	TCP 或 UDP	方向 (Direction) 为服务器 (Server)

类型

输入的模式字符串类型。您看到的选项由您已选择的协议 (Protocol) 确定。如果已选择 RTMP 作为协议，则系统将显示 **URL** 字段而非类型 (Type) 字段。

注释 如果选择用户代理 (User Agent) 作为类型 (Type)，则系统自动将应用的标记 (Tag) 设为用户代理排除项 (User-Agent Exclusion)。

类型选择	字符串特征
Ascii	字符串使用 ASCII 编码。
公用名	字符串是服务器响应消息中 commonName 字段的值。
内容类型	字符串是服务器响应报头中 content-type 字段的值。
十六进制	字符串使用十六进制表示。
组织单位	字符串是服务器响应消息中 organizationName 字段的值。
SIP 服务器 (SIP Server)	字符串是消息报头中 From 字段的值。
SSL 主机 (SSL Host)	字符串是 ClientHello 消息中 server_name 字段的值。
URL	字符串是一个 URL。 注释 检测器假设输入的字符串是完整的 URL 部分。例如，输入 cisco.com 将匹配 www.cisco.com/support 和 www.cisco.com，但不匹配 www.wearecisco.com。
用户代理	字符串是 GET 请求报头中 user-agent 字段的值。它还可用于 SIP 协议，表示字符串是 SIP 消息报头中 user-agent 字段的值。

URL

来自 RTMP 数据包的 C2 消息内 swfURL 字段的完整 URL 或部分 URL。选择 **RTMP** 作为**协议 (Protocol)** 时，系统将显示此字段而非**类型 (Type)** 字段。

注释 检测器假设输入的字符串是完整的 URL 部分。例如，输入 **cisco.com** 将匹配 **www.cisco.com/support** 和 **www.cisco.com**，但不匹配 **www.wearecisco.com**。

用户定义的应用字段

使用以下字段在基本和高级自定义应用检测器内配置用户定义的应用。

业务相关性

应用被用于您的组织的业务运营中（而不是用于娱乐目的）的可能性：**非常高 (Very High)**、**高 (High)**、**中 (Medium)**、**低 (Low)** 或**非常低 (Very Low)**。选择最能描述应用的选项。

类别

说明应用的最基本功能的应用通用分类。

说明

应用的说明。

名称

应用的名称。

风险

应用被用于违反您的组织安全策略的目的之可能性：**非常高 (Very High)**、**高 (High)**、**中 (Medium)**、**低 (Low)** 或**非常低 (Very Low)**。选择最能描述应用的选项。

标签

提供有关应用的其他信息的一个或多个预定义标记。如果要让应用免于执行主动身份验证（在身份规则中配置），则必须为应用添加**用户代理排除项 (User-Agent Exclusion)** 标记。

配置自定义应用检测器

您可以配置基本或高级自定义应用检测器。

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 点击**创建自定义检测器 (Create Custom Detector)**。

步骤 3 输入**名称 (Name)** 和**说明 (Description)**。

步骤 4 选择 **Application Protocol**。您有以下选择：

- 如果是为现有应用协议创建检测器（例如，如果要检测非标准端口上的特定应用协议），请从下拉列表中选择应用协议。
- 如果是为用户定义的应用创建检测器，请按照创建用户定义的应用，第 1955 页中概述的程序执行操作。

步骤 5 选择**检测器类型 (Detector Type)**。

步骤 6 点击 **OK**。

步骤 7 配置 **检测模式** 或 **检测标准** 或 **加密可视性引擎进程分配**：

- 如果配置的是基本检测器，请指定预设**检测模式 (Detection Patterns)**，如指定基本检测器中的检测模式，第 1956 页中所述。
- 如果配置的是高级检测器，请指定自定义**检测条件 (Detection Criteria)**，如指定高级检测器中的检测条件，第 1957 页中所述。
- 如果要配置加密可视性引擎（EVE）检测器，请指定自定义EVE进程分配，如指定 EVE 进程分配，第 1958 页中所述。

  注意 高级自定义检测器很复杂，且需要具备外部知识才能构建有效的 .lua 文件。错误配置的检测器会对性能或检测能力造成负面影响。

步骤 8 或者，使用**数据包捕获 (Packet Captures)** 测试新检测器，如测试自定义应用协议检测器，第 1959 页中所述。

步骤 9 点击**保存 (Save)**。

注释 如果在访问控制规则中包含该应用，则检测器会自动激活，并且在使用时不能停用。

下一步做什么

- 激活检测器，如激活和停用检测器，第 1962 页中所述。

相关主题

自定义应用检测器和用户定义的应用字段，第 1951 页

创建用户定义的应用

此处创建的应用、类别和标记在访问控制规则以及在应用过滤对象管理器中均可用。

注意 创建用户定义的应用会立即重启 Snort 进程，而无需执行部署过程。系统会提醒您，继续操作会重启 Snort 进程并允许您取消；重启发生在当前域或其任何子域中的任何托管设备上。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。

开始之前

- 开始配置自定义应用协议检测器，如配置自定义应用检测器，第 1954 页中所述。

过程

步骤 1 在 Create Detector 页面上，点击 **Add**。

步骤 2 键入**名称 (Name)**。

步骤 3 键入**说明 (Description)**。

步骤 4 选择**业务关联性**。

步骤 5 选择**风险**。

步骤 6 点击“类别”(Categories) 旁的**添加 (Add)** 以添加类别，并键入新的类别名称，或者从**类别 (Categories)** 下拉列表选择现有类别。

步骤 7 或者，也可以点击"标记"(Tags) 旁的**添加 (Add)** 以添加标记，并键入新的标记名称，或者从**标记 (Tags)** 下拉列表选择现有标记。

步骤 8 点击 **OK**。

下一步做什么

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第 1954 页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

相关主题

自定义应用检测器和用户定义的应用字段，第 1951 页

指定基本检测器中的检测模式

可以配置自定义应用协议检测器以搜索应用协议数据包报头中的特定模式字符串。也可配置检测器，使其搜索多个模式，在这种情况下，应用协议流量必须匹配所有模式，以便检测器主动识别应用协议。

应用协议检测器可使用任何偏移搜索 ASCII 或十六进制模式。

开始之前

- 开始配置自定义应用协议检测器，如配置自定义应用检测器，第 1954 页中所述。

过程

步骤 1 在“创建检测器”(Create Detector) 页面上的“检测模式”(Detection Patterns) 部分中，点击**添加 (Add)**。

步骤 2 在**协议 (Protocol)** 中选择检测器应检查的流量的协议。

步骤 3 在**类型 (Type)** 中指定要检测的模式类型。

步骤 4 键入与指定的**类型 (Type)** 相匹配的**模式字符串 (Pattern String)**。

步骤 5 或者，键入**偏移 (Offset)**（以字节为单位）。

步骤 6 或者，要根据其使用的端口识别应用协议流量，请在**端口**字段中键入 1 到 65535 之间的端口。要使用多个端口，请用逗号分隔它们。

步骤 7 或者，选择**方向 (Direction)**：**客户端 (Client)** 或**服务器 (Server)**。

步骤 8 点击 **OK**。

提示 如果要删除模式，请点击要删除的模式旁边的 **删除**（ ）。

下一步做什么

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第 1954 页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

相关主题

指定高级检测器中的检测条件，第 1957 页

指定高级检测器中的检测条件

注意 高级自定义检测器很复杂，且需要具备外部知识才能构建有效的 .lua 文件。错误配置的检测器会对性能或检测能力造成负面影响。

注意 不要上传来自不可信来源的 .lua 文件。

自定义 .lua 文件包含自定义应用检测器设置。创建自定义 .lua 文件需要具备 lua 编程语言的高级知识和思科的 C-lua API 经验。思科强烈建议使用以下材料来准备 .lua 文件：

- lua 编程语言的第三方说明和参考资料
- 开源检测器开发人员指南： https://www.snort.org/downloads
- OpenAppID Snort 社区资源： http://blog.snort.org/search/label/openappid

注释 系统不支持引用系统调用或文件 I/O 的 .lua 文件。

开始之前

- 开始配置自定义应用协议检测器，如配置自定义应用检测器，第 1954 页中所述。

- 通过下载和学习类似检测器的 .lua 文件，为创建有效的 .lua 文件做准备。有关下载检测器文件的详细信息，请参阅查看或下载检测器详细信息，第 1959 页。
- 创建包含自定义应用检测器设置的有效 .lua 文件。

过程

步骤 1 在高级自定义应用检测器的“创建检测器”(Create Detector) 页面的“检测条件”(Detection Criteria) 部分，点击**添加 (Add)**。

步骤 2 点击**浏览...(Browse...)** 以导航至 **.lua** 文件并将其上传。

步骤 3 点击 **OK**。

下一步做什么

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第 1954 页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

相关主题

指定基本检测器中的检测模式，第 1956 页

指定 EVE 进程分配

您可以配置自己的自定义应用检测器，以将加密可视性引擎 (EVE) 检测到的进程映射到新应用或现有应用。

开始之前

- 开始配置自定义应用协议检测器，如配置自定义应用检测器，第 1954 页中所述。

过程

步骤 1 在“创建检测器”页面上的“加密可视性引擎进程分配”部分中，点击 **添加**。

步骤 2 输入 **进程名称** 和 **最小进程置信度** 值。

注释 您可以在 **进程名称** 字段中输入文本，这区分大小写。该值应与 EVE 检测到的确切进程名称匹配。 **最小进程置信度** 可以是 0 到 100 之间的任何数字。这是连接事件中 **加密可视化进程置信度得分** 字段中显示的数字。

有关 **加密可视化进程置信度得分** 字段的信息，请参阅 《Cisco Firepower 管理中心管理指南》中 “连接和安全情报事件字段” 的部分。

步骤 3 点击**保存**。

步骤 4 在应用检测器列表页面中，激活您创建的检测器。有关详细信息，请参阅激活和停用检测器，第 1962 页。当您激活检测器时，检测器文件会被推送到 FMC 上注册的所有 FTD。

下一步做什么

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第 1954 页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

测试自定义应用协议检测器

如您拥有的数据包捕获 (pcap) 文件包含的数据包带有要检测的应用协议的流量，则可针对该 pcap 文件测试自定义的应用协议检测器。思科建议使用简单、干净的 pcap 文件，没有不必要的流量。

Pcap 文件必须为 256 KB 或更小；如果尝试针对较大的 pcap 文件测试检测器，管理中心会自动将其截断并测试不完整文件。在使用该文件测试检测器之前，必须修复 pcap 中无法确定的校验和。

开始之前

- 配置自定义应用协议检测器，如配置自定义应用检测器，第 1954 页中所述。

过程

步骤 1 在“创建检测器”(Create Detector) 页面上的“数据包捕获”(Packet Captures) 部分，点击**添加 (Add)**。

步骤 2 在弹出式窗口中浏览至 pcap 文件，然后点击**确定 (OK)**。

步骤 3 要针对 pcap 文件的内容测试检测器，点击 pcap 文件旁的评估。系统显示消息，指示测试是否成功。

步骤 4 或者，重复第 1至 3 步，针对额外的 pcap 文件测试检测器。

提示 要删除 pcap 文件，点击想要删除的文件旁的 **删除**（  ） 。

下一步做什么

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第 1954 页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

查看或下载检测器详细信息

可以使用检测器列表来查看应用检测器详细信息（所有检测器）和下载检测器详细信息（仅自定义应用检测器）。

过程

步骤 1 要查看应用检测器详细信息，请执行以下任一操作：

- 参阅 https://www.cisco.com/c/en/us/support/security/defense-center/products-technical-reference-list.html 上提供的相关 VDB 版本的思科 *Firepower* 应用检测器参考
- a. 选择**策略** > **应用检测器**。

  b. 过滤列表以查找特定检测器。

  c. 点击 **信息**（）

步骤 2 要下载自定义应用检测器的检测器详细信息，请点击 **下载**（）。

如果控件呈灰显状态，则表明配置属于祖先域，或者您没有必要的权限。

检测器列表排序

默认情况下，Detectors 页面将按名称以字母顺序列出检测器。列标题旁边的向上或向下箭头表示页面按该列升序或降序排序。

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 点击相应的列标题。

过滤检测器列表

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 展开检测器列表的过滤器组，第 1961 页中所述的其中一个过滤器组并选择过滤器旁边的复选框。要选择组中的所有过滤器，右键点击组名称，然后选择 **Check All**。

步骤 3 如果要移除某个过滤器，请点击 **删除**（）（位于**过滤器 [Filters]** 字段的过滤器名称中）或禁用过滤器列表中的过滤器。要移除组中的所有过滤器，右键点击组名称，然后选择 **Uncheck All**。

步骤 4 如果要移除所有过滤器，请点击已应用至检测器的过滤器列表旁边的**全部清除 (Clear alls)**。

检测器列表的过滤器组

可单独或组合使用多个过滤器组，以过滤检测器列表。

名称

查找名称或描述包含您键入的字符串的检测器。字符串可包含任何字母数字或特殊字符。

自定义过滤器 (Custom Filter)

查找与对象管理页面上创建的自定义应用过滤器匹配的检测器。

作者

按检测器的创建者查找检测器。可按以下内容过滤检测器：

- 创建或导入自定义检测器的任何个别用户
- 思科代表所有思科提供的检测器，单独导入的附加检测器除外（您是自己导入的任何检测器的作者）
- **任何用户 (Any User)**，代表非思科提供的所有检测器

状态

根据检测器的状态（即**活动 [Active]** 或**非活动 [Inactive]**）查找检测器。

类型

根据检测器类型查找检测器，如应用检测器基础知识，第 1946 页中所述。

协议

根据检测器检查的流量协议查找检测器。

类别

根据分配至所检测应用的类别查找检测器。

标签

根据分配至所检测应用的类别查找检测器。

风险 (Risk)

根据分配到所检测应用的风险查找检测器：**非常高 (Very High)**、**高 (High)**、**中 (Medium)**、**低 (Low)** 和**非常低 (Very Low)**。

业务关联性 (Business Relevance)

根据分配至所检测应用的业务关联性查找检测器：**非常高 (Very High)**、**高 (High)**、**中 (Medium)**、**低 (Low)** 和**非常低 (Very Low)**。

导航至其他检测器页面

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 如果要查看下一页，请点击 **右箭头**（ > ）。

步骤 3 如果要查看上一页，请点击 **左箭头**（ < ）。

步骤 4 如果要查看另一页，请键入页码并按 Enter 键。

步骤 5 如果要跳到最后一页，请点击 **右端箭头**（ >| ）。

步骤 6 如果要跳到第一页，请点击 **左端箭头**（ |< ）。

激活和停用检测器

必须激活检测器，然后才能将其用于分析网络流量。默认情况下，思科提供的所有检测器均已激活。

可为每个端口激活多个应用检测器，以补充系统的检测能力。

在策略的访问控制规则中包含应用并部署策略时，如果该应用没有活动检测器，一个或多个检测器将会自动激活。类似地，在已部署策略中使用应用时，如果停用检测器会使该应用没有活动检测器，则不能停用检测器。

提示 为提高性能，请停用任何您不打算使用的应用协议、客户端或 Web 应用检测器。

注意 激活或停用系统或自定义应用检测器会立即重启 Snort 进程，而不会执行部署过程。系统会提醒您，继续操作会重启 Snort 进程并允许您取消；重启发生在当前域或其任何子域中的任何托管设备上。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 点击要激活或停用的检测器旁边的滑块。 如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

注释 其他检测器可能需要某些应用检测器。如果停用其中一个检测器，系统会显示警告表明依赖于它的检测器也已被禁用。

编辑自定义应用检测器

使用以下程序修改自定义应用检测器。

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 点击要修改的检测器旁边的 **编辑**（）。 如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 对检测器进行更改，如配置自定义应用检测器，第 1954 页中所述。

步骤 4 根据检测器的状态，您具有以下保存选择：

- 要保存非活动检测器，请点击**保存 (Save)**。
- 要将非活动检测器另存为新的非活动检测器，请点击**另存为新项目 (Save as New)**。
- 要保存活动检测器并立即开始使用，请点击**保存并重新激活 (Save and Reactivate)**。

  注意 保存和重新激活自定义应用检测器后，无需执行部署过程即可立即重启 Snort 进程。系统会提醒您，继续操作会重启 Snort 进程并允许您取消；重启发生在当前域或其任何子域中的任何托管设备上。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。

- 要将活动检测器另存为新的非活动检测器，请点击**另存为新项目 (Save as New)**。

删除检测器

可以删除自定义检测器以及单独导入的由思科专业服务提供的附加检测器。不能删除思科提供的任何其他检测器，不过可以停用其中许多检测器。

注释 当检测器正在已部署的策略中使用时，不能删除该检测器。

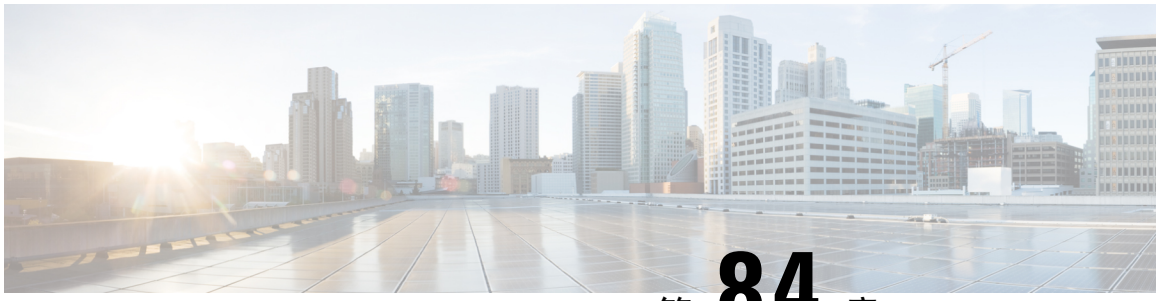
注意 删除已激活的自定义应用检测器将立即重启 Snort 进程，而无需执行部署流程。系统会提醒您，继续操作会重启 Snort 进程并允许您取消；重启发生在当前域或其任何子域中的任何托管设备上。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。

过程

步骤 1 选择**策略** > **应用检测器**。

步骤 2 点击要删除的检测器旁边的 **删除**（ ）。 如果显示**视图**（ ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击**确定 (OK)**。



第 84 章

网络发现策略

以下主题介绍如何创建、配置和管理网络发现策略：

概述：网络发现策略

管理中心上的网络发现策略控制系统如何收集有关组织网络资产以及哪些网段和端口受监控的数据。

在多域部署中，每个分叶域具有独立的网络发现策略。网络发现策略规则和其他设置不能共享、继承或在域之间复制。只要创建新域，系统就会使用默认设置为新域创建网络发现策略。您必须将任何所需自定义应用于新策略。

策略中的发现规则指定系统监控哪些网络和端口来根据流量中的网络数据生成发现数据，以及指定策略部署到的区域。在规则中，您可以配置是否发现主机、应用和非管理用户。可以创建规则来将网络和区域排除在发现范围外。您可以从 NetFlow 导出器配置数据发现，并且限制在网络上发现了用户数据的流量的协议。

网络发现策略包含一个配置为从观察到的所有流量发现应用的默认规则。该规则不排除任何网络、区域或端口，未配置主机和用户发现，并且规则未配置为监控 NetFlow 导出器。当受管设备注册到管理中心时，此策略默认部署到任何受管设备。要开始收集主机或用户数据，必须添加或修改发现规则并将策略重新部署到设备。

如果要调整网络发现范围，可以创建其他发现规则，并修改或移除默认规则。

请记住，每个受管设备的访问控制策略都定义面向该设备允许的流量，以及因此可使用网络发现监控的流量。如果使用访问控制阻止某些流量，则系统无法检查主机、用户和应用活动的该流量。例如，如果访问控制策略阻止对社交网络应用的访问，则系统无法在这些应用上提供任何发现数据。

如果在发现规则中启用基于流量的用户检测，则可以通过使用一组应用协议的流量中的用户登录活动来检测非管理用户。如有需要，可以禁用用于所有规则的特定协议中的发现。禁用某些协议有助于避免达到与 管理中心型号关联的用户限制，从而为来自其他协议的用户保留可用用户计数。

借助高级网络发现设置，可以管理记录哪些数据、如何存储发现数据、哪些危害表现 (IOC) 规则处于活动状态、哪些漏洞映射用于影响评估，以及如果源提供冲突发现数据将会发生什么情况。您还可以添加要监控的主机输入和 NetFlow 导出器的源。

网络发现策略的要求和必备条件

型号支持

任意。

支持的域

枝叶

用户角色

- 管理员
- 发现管理员

网络发现自定义

Firepower 系统收集的有关网络流量的信息对您最有价值，因为系统可以参考该信息来识别网络上最易受攻击和最重要的主机。

例如，如果网络上有多个运行自定义版本的 SuSE Linux 的设备，则系统无法识别操作系统，因此无法将漏洞映射至主机。不过，如果知道系统拥有 SuSE Linux 的漏洞列表，您可能想要为某个主机创建自定义的指纹，以便随后可使用该指纹来识别运行相同操作系统的其他主机。可将 SuSE Linux 漏洞列表的映射纳入指纹中，以便将该列表与匹配指纹的每个主机关联。

系统还允许使用主机输入功能，将来自第三方系统的主机数据直接输入至网络映射。不过，第三方操作系统或应用数据不会自动映射至漏洞信息。如果想要为使用第三方操作系统、服务器和应用协议数据的主机查看漏洞并执行影响关联，必须将来自第三方系统的供应商和版本信息映射至漏洞数据库 (VDB) 中列出的供应商和版本。您也可能想要持续维护主机输入数据。请注意，即使将应用数据映射到 Firepower 系统供应商和版本定义，导入的第三方漏洞也不用于客户端或 Web 应用的影响评估。

如果系统无法识别网络主机上运行的应用协议，则可创建用户定义的应用协议检测器以便系统根据端口或模式识别应用。您还可以导入、激活和停用某些应用检测器，以便进一步自定义 Firepower 系统的应用检测功能。

还可使用 Nmap 主动扫描器的扫描结果替换操作系统和应用数据的检测结果，或者使用第三方漏洞来扩充漏洞列表。系统可以协调来自多个源的数据，从而确定应用的身份。

配置网络发现策略

在多域部署中，每个域具有独立的网络发现策略。如果用户帐户可以管理多个域，请切换至要配置策略的分叶域。

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 配置策略的以下组件：

- 发现规则 - 请参阅配置网络发现规则，第 1968 页。
- 基于流量的用户检测 - 请参阅配置基于流量的用户检测，第 1976 页。
- 高级网络发现选项 - 请参阅配置高级网络发现选项，第 1976 页。
- 自定义操作系统定义（指纹）- 请参阅为客户端创建自定义指纹，第 1914 页和为服务器创建自定义指纹，第 1916 页。

网络发现规则

通过网络发现规则，您可以将为网络映射发现的信息定制为仅包含所需的特定数据。网络发现策略中的规则按顺序接受评估。您可以使用重叠的监控条件创建规则，但这样做可能会影响系统性能。

将主机或网络排除在监控范围外之后，被排除的主机或网络将不会显示在网络映射中，系统也不会为其报告事件。但是，在禁用本地 IP 的主机发现规则时，检测引擎实例会受到更高处理负载的影响，因为它会从每个流重新构建数据，而不是使用现有主机数据。

我们建议将负载均衡器（或负载均衡器上的特定端口）和NAT 设备排除在监控范围外。这些设备可能会创建过量并有误导性的事件，从而填充数据库并使 管理中心过载。例如，受监控的 NAT 设备可能会在短时间内显示其操作系统的多个更新。如果知道负载均衡器和 NAT 设备的 IP 地址，可以将它们排除在监控范围外。

提示 系统可通过检查网络流量识别许多负载均衡器和 NAT 设备。

此外，如果需要创建自定义服务器指纹，应暂时禁止监控用于与正在创建指纹的主机通信的 IP 地址。否则，网络映射和发现事件视图中将会出现大量关于该IP 地址代表的主机的不准确信息。创建指纹后，可以配置策略，以便再次监控该 IP 地址。

思科还建议不监控 NetFlow 导出器和托管设备的相同网段。尽管在理想情况下应使用不重叠的规则来配置网络发现政策，但系统不会丢弃受管设备生成的重复连接日志。但是，不能丢弃受管设备和 NetFlow 导出器均检测到的连接的重复连接日志。

配置网络发现规则

可以配置发现规则，以根据自身需求定制主机和应用数据的发现。

开始之前

- 确保正在为要在其中发现网络数据的流量记录连接。
- 如果要收集导出的 NetFlow 记录，请按照将 NetFlow 导出器添加到网络发现策略，第 1981 页中所述添加 NetFlow Exporter。
- 如果要查看发现性能图，必须在发现规则中启用主机，用户和应用。请注意，这可能会影响性能。

提示 在大多数情况下，思科建议将发现限制在 RFC 1918 中的地址。

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击**添加规则**。

步骤 3 如操作和发现的资产，第 1969 页中所述，为规则设置**操作 (Action)**。

步骤 4 设置可选的发现参数：

- 将规则操作限定于特定网络；请参阅限制受监控网络，第 1970 页。
- 将规则操作限定于特定区域中的流量；请参阅配置网络发现规则中的区域，第 1974 页。
- 将端口排除在监控范围外；请参阅排除网络发现规则中的端口，第 1972 页。
- 为 NetFlow 数据发现配置规则；请参阅配置用于 NetFlow 数据发现的规则，第 1970 页。

步骤 5 点击**保存 (Save)**。

下一步做什么

- 部署配置更改。

操作和发现的资产

配置发现规则时，必须为规则选择操作。规则操作的影响取决于规则是用于从受管设备还是NetFlow导出器发现数据。

下表说明了规则使用这两种方案中指定的操作设置发现的资产。

表 *207:* 发现规则操作

操作 **(Action)**	选项	受管设备	**NetFlow** 导出器
排除	--	将指定网络排除在监控范围外。如果用于连接的源主机或目标主机已被排除在发现范围外，会记录连接，但不会为排除的主机创建发现事件。	将指定网络排除在监控范围外。如果用于连接的源主机或目标主机已被排除在发现范围外，会记录连接，但不会为排除的主机创建发现事件。
Discover	主机数	根据发现事件将主机添加到网络映射。（可选操作；如果启用了用户发现，则为必要操作。）	根据 NetFlow 记录将主机添加到网络映射并记录连接。（必需）
Discover	应用	根据应用检测程序将应用添加到网络映射。请注意，在没有发现应用的情况下，无法发现规则中的主机或用户。（必需）	根据 NetFlow 记录和 `/etc/sf/services` 中的端口应用协议关联将应用协议添加到网络映射。（可选）
Discover	用户	将用户添加到用户表，并根据对网络发现策略中配置的用户协议进行的基于流量的检测记录用户活动。（可选）	n/a
记录 NetFlow 连接	--	n/a	仅记录 NetFlow 连接。不发现主机或应用。

如果要让规则监控受管设备流量，则应用日志记录为必要操作。如果要让规则监控用户，则主机日志记录为必要操作。如果要让规则监控导出的 NetFlow 记录，则您无法将其配置为记录用户，并且记录应用为可选操作。

注释 系统根据网络发现策略中的**操作 (Action)** 设置检测 NetFlow 记录中的连接。系统根据访问控制策略设置检测受管设备中的连接。

受监控网络

发现规则仅可发现流量中发向和来自指定网络中主机的受监控资产。发现规则执行发现的对象是至少有一个 IP 地址在指定网络范围内的连接，并仅对位于受监控网络范围内的 IP 地址生成事件。默认发现规则从所有观察到的流量中发现应用（`0.0.0.0/0` 表示所有 IPv4 流量，`::/0` 表示所有 IPv6 流量）。

如果将规则配置为处理 NetFlow 发现并仅记录连接数据，则系统还会记录发向和来自指定网络中 IP 地址的连接。请注意，网络发现规则是记录 NetFlow 网络连接的唯一方式。

另外，您也可以使用网络对象或对象组指定要监控的网络。

限制受监控网络

每个发现规则必须至少包含一个网络。

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击**添加规则**。

步骤 3 如果还未打开，请点击 **网络**。

步骤 4 或者，将网络对象添加到“可用网络”(Available Networks) 列表，如在配置发现规则期间创建网络对象，第 1971 页中所述。

注释 如果修改网络发现策略中使用的网络对象，则更改对于发现不会生效，直至部署配置更改为止。

步骤 5 指定网络：

- 从**可用网络 (Available Networks)** 列表中选择网络。

  提示 如果网络没有立即显示在列表中，请点击 **重新加载** （）。

- 将 IP 地址输入到“可用网络”(Available Networks) 标签下方的文本框中。

步骤 6 点击 **Add**。

步骤 7 或者，重复前两个步骤以添加其他网络。

步骤 8 点击**保存 (Save)** 以保存所做的更改。

下一步做什么

- 部署配置更改。

配置用于 NetFlow 数据发现的规则

Firepower 系统可以使用来自 NetFlow 导出器的数据生成连接和发现事件，并将主机和应用数据添加到网络映射。

如果选择某个发现规则中的 NetFlow 导出器，该规则将被限制为为指定网络发现 NetFlow 数据。应先选择要监控的 NetFlow 设备，然后再配置规则行为的其他方面，因为在选择 NetFlow 设备时可用规则操作会变化。不能为监控 NetFlow 导出器配置端口排除。

开始之前

- 将支持 NetFlow 的设备添加到网络发现策略；请参阅将 NetFlow 导出器添加到网络发现策略，第 1981 页。

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击**添加规则**。

步骤 3 选择 **NetFlow 设备**。

步骤 4 从 **NetFlow 设备 (NetFlow Device)** 下拉列表中，选择要监控的 NetFlow 导出器的 IP 地址。

步骤 5 指定要让 Firepower 系统受管设备收集的 NetFlow 数据类型：

- 仅连接 - 从操作 (Action) 下拉列表中选择 **Log NetFlow Connections**。
- 主机、应用和连接 - 从操作 (Action) 下拉列表中选择 **Discover**。系统会自动选中**主机 (Hosts)** 复选框并启用连接数据的收集。或者，可以选中**应用 (Application)** 复选框以收集应用数据。

步骤 6 点击**保存 (Save)**。

下一步做什么

- 部署配置更改。

在配置发现规则期间创建网络对象

将新的网络对象添加到可重用网络对象和组列表中，即可将其添加到发现规则中显示的可用网络列表中。

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 在 **网络**中，点击 **添加**。

步骤 3 点击 **可用网络**旁边的 **添加**（+）。

步骤 4 按照创建网络对象，第 999 页中所述创建网络对象。

步骤 5 按照配置网络发现规则，第 1968 页中所述完成添加网络发现规则。

端口排除

可以将特定端口排除在监控范围外，就像将主机排除在监控范围外一样。例如：

- 负载均衡器可在短时间内报告同一端口上的多个应用。可以配置网络发现规则，以便将该端口排除在监控范围外，例如排除处理 Web 场的负载均衡器上的端口 80。
- 组织可以使用采用特定端口范围的自定义客户端。如果来自该客户端的流量生成过多有误导性的事件，可以排除对这些端口的监控。同样，可以决定是否要监控DNS流量。在这种情况下，可以配置规则，使发现策略不监控端口 53。

添加要排除的端口时，可以决定是使用Available Ports列表中的可重用端口对象，将端口直接添加到源或目标排除列表，还是创建新的可重用端口然后将其移至排除列表。

注释 不能排除处理 NetFlow 数据发现的规则中的端口。

排除网络发现规则中的端口

不能排除处理 NetFlow 数据发现的规则中的端口。

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击**添加规则**。

步骤 3 点击 **Port Exclusions**。

步骤 4 或者，将端口对象添加到“可用端口”(Available Ports) 列表，如在配置发现规则期间创建端口对象，第 1973 页中所述。

步骤 5 使用以下任一方法将特定源端口排除在监控范围外：

- 从**可用端口 (Available Ports)** 列表中选择一个或多个端口，然后点击**添加到源 (Add to Source)**。
- 要排除来自特定源端口的流量而不添加端口对象，请在**所选源端口 (Selected Source Ports)** 列表下，选择**协议 (Protocol)**，在**端口 (Port)** 中输入端口号（从 1 到 65535 的值），然后点击**添加 (Add)**。

步骤 6 使用以下任一方法将特定目标端口排除在监控范围外：

- 从**可用端口 (Available Ports)** 列表中选择一个或多个端口，然后点击**添加到目标 (Add to Destination)**。
- 要排除来自特定目标端口的流量而不添加端口对象，请在**所选目标端口 (Selected Destination Ports)** 列表下，选择**协议 (Protocol)**，在**端口 (Port)** 中输入端口号，然后点击**添加 (Add)**。

步骤 7 点击**保存 (Save)** 以保存所做的更改。

下一步做什么

- 部署配置更改。

在配置发现规则期间创建端口对象

将新的端口对象添加到可在Firepower系统中任意位置使用的可重用端口对象和对象组列表，即可将其添加到发现规则中显示的可用端口列表中。

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 在网络中，点击 **添加**。

步骤 3 点击 **Port Exclusions**。

步骤 4 要将端口添加到可用端口列表，请点击 **添加**（+）。

步骤 5 提供**名称 (Name)**。

步骤 6 在 **Protocol** 字段中，指定要排除的流量协议。

步骤 7 在**端口 (Port)** 字段中，输入要排除在监控范围外的端口。

可以指定单个端口、用破折线(-)分隔的一系列端口或者用逗号分隔的端口和端口范围列表。允许的端口值介于 1 到 65535 之间。

步骤 8 点击**保存 (Save)**。

步骤 9 如果添加的端口没有立即显示在列表中，请点击 **刷新**。

下一步做什么

- 部署配置更改。

网络发现规则中的区域

要提高性能，可以配置发现规则，以便规则中的区域包含物理连接到规则中的待监控网络的受管设备上的传感接口。

但是，系统可能并不总是告知您网络配置的更改情况。网络管理员可以通过路由或主机更改修改网络配置而无需告知您，这可能会导致您难以随时了解正确的网络发现策略配置。如果您不知道受管设备上的传感接口如何物理连接到您的网络，请将区域配置保留为默认设置。此默认设置会导致系统将发现规则部署到您的部署中的所有区域。（如果未排除任何区域，则系统会将发现策略部署到所有区域。）

配置网络发现规则中的区域

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击**添加规则**。

步骤 3 点击 **区域**。

步骤 4 从**可用区域 (Available Zones)** 列表中选择一个或多个区域。

步骤 5 点击**保存 (Save)** 以保存所做的更改。

下一步做什么

- 部署配置更改。

基于流量的检测身份源

基于流量的检测是系统唯一支持的未授权身份源。进行配置后，受管设备会检测您指定的网络上的 LDAP、AIM、POP3、IMAP、Oracle、SIP (VoIP)、FTP、HTTP、MDNS 和 SMTP 登录。从基于流量的检测获取的数据仅可用于用户感知。与授权身份源不同，您可在网络发现策略中配置基于流量的检测，如配置基于流量的用户检测 ， 第 1976 页中所述。

请注意以下限制：

- 基于流量的检测仅将用于 LDAP 连接的 Kerberos 登录解释为 LDAP 身份验证。受管设备无法检测使用协议（例如 SSL 或 TLS）的加密 LDAP 身份验证。
- 基于流量的检测只能检测使用 OSCAR 协议的 AIM 登录。无法检测使用 TOC2 的 AIM 登录。
- 基于流量的检测无法限制 SMTP 日志记录。这是因为未根据 SMTP 登录将用户添加到数据库；虽然系统会检测 SMTP 登录，这些登录不会被记录下来，除非数据库中包含已具有匹配邮件地址的用户。

基于流量的检测还会记录失败的登录尝试。如果登录尝试失败，不会将新用户添加到数据库的用户列表中。基于流量的检测功能检测到的登录失败活动的用户活动类型是**登录失败的用户 (Failed User Login)**。

注释 系统无法区分失败和成功的 HTTP 登录。要查看 HTTP 用户信息，您必须在基于流量的检测配置中启用**捕获登录失败尝试 (Capture Failed Login Attempts)**。

注意 使用网络发现策略在部署配置更改时重新启动Snort进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。在 HTTP、FTP 或 MDNS 协议上启用或禁用基于流量的非授权用户检测

基于流量的检测数据

设备使用基于流量的检测功能检测到登录时，它会将以下信息发送到 管理中心（这些信息将被记录为用户活动）：

- 识别出的登录用户名
- 登录时间
- 登录使用的 IP 地址，可能是用户的主机（用于 LDAP、POP3、IMAP 和 AIM 登录）、服务器（用于 HTTP、MDNS、FTP、SMTP 和 Oracle 登录）或会话发起方（用于 SIP 登录）的 IP 地址
- 用户的邮件地址（用于 POP3、IMAP 和 SMTP 登录）
- 检测到登录的设备名称

如果之前已检测到该用户，管理中心会更新该用户的登录历史记录。请注意，管理中心可以使用 POP3 和 IMAP 登录中的邮件地址与 LDAP 用户 关联。举例来说，这意味着如果 管理中心检测到新的 IMAP 登录，且 IMAP 登录中的邮件地址与某个现有 LDAP 用户的邮件地址匹配，则 IMAP 登录不会创建新用户，而是会更新该 LDAP 用户的历史记录。

如果之前从未检测到该用户，管理中心会将该用户添加到用户数据库。唯一的 AIM、SIP 和 Oracle 登录始终会创建新用户记录，因为这些登录事件中没有 管理中心可与其他登录类型关联的数据。

在以下情况下，管理中心**不**会记录用户活动或用户身份：

- 网络发现策略被配置为忽略该登录类型。
- 受管设备检测到 SMTP 登录，但用户数据库不包含之前使用匹配的邮件地址检测到的 LDAP、POP3 或 IMAP 用户

用户数据将被添加到用户表中。

基于流量的检测策略

可以限制在其中发现用户活动的协议，以减少检测到的用户的总数，以便将重点放在可能提供最完整用户信息的用户。限制协议检测有助于最大程度地减少用户名混乱以及预留 管理中心上的存储空间。

当选择基于流量的检测协议时，请注意以下事项：

- 如果通过协议（例如 AIM、POP3 和 IMAP）获取用户名，可能会由于承包商、访客及其他访客的网络访问而引入与组织无关的用户名。

- AIM、Oracle 和 SIP 登录可能会创建外来用户记录。之所以会发生这种情况，是因为这些登录类型没有与系统从 LDAP 服务器获取的任何用户元数据关联，也没有与受管设备会检测的其他类型登录中包含的任何信息关联。因此，管理中心无法将这些用户与其他类型的用户关联。

配置基于流量的用户检测

在网络发现规则中启用基于流量的用户检测时，将会自动启用主机发现。有关基于流量的检测的详细信息，请参阅基于流量的检测身份源，第 1974 页。

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击“**用户**”。

步骤 3 请点击 **编辑**（）。

步骤 4 选中要检测登录的协议的复选框，或取消选中不希望检测登录的协议的复选框。

步骤 5 或者，要记录在 LDAP、POP3、FTP 或 IMAP 流量中检测的失败登录尝试，或捕获 HTTP 登录的用户信息，请启用 **Capture Failed Login Attempts**。

步骤 6 点击**保存 (Save)**。

下一步做什么

⚠

注意 使用网络发现策略在 HTTP、FTP 或 MDNS 协议上启用或禁用基于流量的非授权用户检测将会在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 144 页。

- 配置网络发现规则以发现用户，如配置网络发现规则，第 1968 页中所述。
- 部署配置更改。

配置高级网络发现选项

可以使用网络发现策略的”高级“(Advanced) 来配置策略范围的设置，以指定要检测的事件、发现数据的保留时间长度和更新频率、用于影响关联的漏洞映射，以及如何解决操作系统和服务器身份冲突。此外，还可以添加主机输入源和 NetFlow 导出器，以允许从其他源导入数据。

注释 发现和用户活动事件的数据库事件限制是在系统配置中设置。

过程

步骤 1 选择策略 > 网络发现。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击 **Advanced**。

步骤 3 点击要修改的设置旁边的 编辑（） 或 添加（）：

- “数据存储设置”(Data Storage Settings) - 更新设置，如配置网络发现数据存储，第 1983 页中所述。
- “事件日志记录设置”(Event Logging Settings) - 更新设置，如配置网络发现事件日志记录，第 1984 页中所述。
- “常规设置”(General Settings) - 更新设置，如配置网络发现常规设置，第 1978 页中所述。
- “身份冲突设置”(Identity Conflict Settings) - 更新设置，如配置网络发现身份冲突解决方法，第 1979 页中所述。
- “危害表现设置”(Indications of Compromise Settings) - 更新设置，如启用危害表现规则，第 1981 页中所述。
- “NetFlow 导出器”(NetFlow Exporters) - 更新设置，如将 NetFlow 导出器添加到网络发现策略，第 1981 页中所述。
- “操作系统和服务器身份源”(OS and Server Identity Sources) - 更新设置，如添加网络发现操作系统和服务器身份源，第 1984 页中所述。
- “用于影响评估的漏洞”(Vulnerabilities to use for Impact Assessment) - 更新设置，如启用网络发现漏洞影响评估，第 1980 页中所述。

步骤 4 点击保存 **(Save)**。

下一步做什么

- 部署配置更改。

网络发现常规设置

常规设置控制系统更新网络映射的频率以及是否在发现过程中捕获服务器横幅。

捕获横幅

如果希望系统存储来自通告服务器供应商和版本的网络流量的报头信息（“横幅”），请选中此复选框。这些信息可提供有关收集的信息的其他上下文。可以通过访问服务器详细信息来访问为主机收集的服务器横幅。

更新间隔

系统更新信息（例如，上一次显示任何主机的 IP 地址的时间、使用应用的时间或应用的点击次数）的时间间隔。默认设置为 3600 秒（1 小时）。

请注意，为更新超时设置较小的时间间隔可在主机显示中提供更准确的信息，但会增加生成的网络事件数量。

配置网络发现常规设置

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击 **Advanced**。

步骤 3 点击**常规设置 (General Settings)** 旁边的 **编辑**（ ）。

步骤 4 更新设置，如网络发现常规设置， 第 1977 页中所述。

步骤 5 点击**保存 (Save)** 以保存常规设置。

下一步做什么

- 部署配置更改。

网络发现身份冲突设置

系统通过将操作系统和服务器的指纹与流量模式进行匹配，从而确定在主机上运行的操作系统和应用。为了提供最可靠的操作系统和服务器身份信息，系统会核对来自多个源的指纹信息。

系统使用所有被动数据来推导操作系统身份并分配置信度值。

默认情况下，除非存在身份冲突，否则由扫描工具或第三方应用添加的身份数据会覆盖 Firepower 系统检测到的身份数据。可以使用 Identity Sources 设置按优先级对扫描程序和第三方应用指纹源进行评级。系统为每个源保留一个身份，但只有优先级最高的第三方应用或扫描程序源中的数据可用作当前身份。但请注意，用户输入数据会覆盖扫描程序和第三方应用数据，无论后者的优先级如何。

身份冲突是指系统检测到某个身份与来自“身份源”(Identity Sources) 设置中列出的活动扫描工具或第三方应用源或者来自 Firepower 系统用户的现有身份相冲突。默认情况下，身份冲突不会自动解

决，必须通过主机配置文件，或者通过重新扫描主机或重新添加新的身份数据覆盖被动身份来解决冲突。但是，可以将系统设置为通过保留被动身份或主动身份来自动解决冲突。

Generate Identity Conflict Event

指定在发生身份冲突时系统是否生成事件。

Automatically Resolve Conflicts

从**自动解决冲突 (Automatically Resolve Conflicts)** 下拉列表中，选择以下选项之一：

- **已禁用 (Disabled)**，如果要强制手动解决身份冲突
- **身份**，如果要在发生身份冲突时让系统使用被动指纹
- **保留主动身份 (Keep Active)**，如果要在发生身份冲突时让系统使用来自最高优先级主动源的当前身份

配置网络发现身份冲突解决方法

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击 **Advanced**。

步骤 3 点击**身份冲突设置 (Identity Conflict Settings)** 旁边的 **编辑**（）。

步骤 4 更新“编辑身份冲突设置”(Edit Identity Conflict Settings) 弹出窗口中的设置，如网络发现身份冲突设置，第 1978 页中所述。

步骤 5 点击**保存 (Save)** 以保存身份冲突设置。

下一步做什么

- 部署配置更改。

网络发现漏洞影响评估选项

可以配置系统如何对入侵事件执行关联影响。您具有以下选择：

- 如果要使用基于系统的漏洞信息执行影响关联，请选中**使用网络发现漏洞映射 (Use Network Discovery Vulnerability Mappings)** 复选框。
- 如果要使用第三方漏洞参考执行影响关联，请选中**使用第三方漏洞映射 (Use Third-Party Vulnerability Mappings)** 复选框。有关详细信息，请参阅《*Firepower* 系统主机输入 *API* 指南》。

可以同时选中这两个复选框或选中其中之一。如果系统生成入侵事件，且该事件涉及的主机所拥有的服务器或操作系统包含所选漏洞映射集中的漏洞，则该入侵事件将带有 Vulnerable（级别 1：红色）影响图标。对于没有供应商或版本信息的任何服务器，需要在 管理中心配置中启用漏洞映射。

如果取消选中这两个复选框，入侵事件将**不会**带有 Vulnerable（级别 1：红色）影响图标。

相关主题

映射第三方漏洞，第 1922 页

启用网络发现漏洞影响评估

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击 **Advanced**。

步骤 3 点击**用于影响评估的漏洞 (Vulnerabilities to use for Impact Assessment)** 旁边的 **编辑**（）。

步骤 4 更新“编辑漏洞设置”(Edit Vulnerability Settings) 弹出窗口中的设置，如网络发现漏洞影响评估选项，第 1979 页中所述。

步骤 5 点击**保存 (Save)** 保存漏洞设置。

下一步做什么

- 部署配置更改。

危害表现

系统使用网络发现策略中的 IOC 规则，以确定主机是否可能被恶意手段损害。当主机满足这些系统提供的规则中指定的条件时，系统将使用危害表现 (IOC) 进行标记。相关规则被称为 *IOC* 规则。每条 IOC 规则对应于一种类型的 IOC 标记。*IOC* 标记用于指定可能发生的危害的性质。

当发生以下情况时，管理中心可以标记涉及的主机和用户：

- 通过使用入侵、连接、安全情报和文件或恶意软件事件，系统将收集到的关于受监控网络及其流量的数据相关联，并确定潜在 IOC 已发生。
- 管理中心可通过 AMP 云从面向终端的 AMP 部署导入 IOC 数据。由于这些数据检查主机本身上的活动（例如，单个程序执行的操作），因此，通过这些数据可了解到纯网络数据无法洞察到的可能威胁。为了方便起见，管理中心会自动获取思科从 AMP 云开发的任何新 IOC 标记。

要配置此功能，请参阅启用危害表现规则，第 1981 页。

您还可以针对主机 IOC 数据和合规 allow 名单（决定 IOC 标记的主机）。

要调查和使用标记的 IOC，请参阅《Cisco Secure Firewall Management Center 管理指南》。

启用危害表现规则

要使系统检测和标记危害表现 (IOC)，必须先在网络发现策略中至少激活一个 IOC 规则。每个 IOC 规则对应于一种类型的 IOC 标记，所有 IOC 规则均由思科预定义；您不能创建原始规则。可根据网络和组织需要启用任何或全部规则。例如，如果使用诸如 Microsoft Excel 等软件的主机从未出现在监控网络上，可决定不启用与基于 Excel 的威胁相关的 IOC 标记。

开始之前

由于 IOC 规则根据系统的其他组件以及面向终端的 AMP 提供的数据触发，因此必须为要设置 IOC 标记的 IOC 规则正确许可并配置这些组件。启用与您将启用的 IOC 规则相关联的系统功能，例如入侵检测和防御 (IPS) 及高级恶意软件防护 (AMP)。如果未启用 IOC 规则的关联功能，将不会收集相关数据，规则也将无法触发。

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击 **Advanced**。

步骤 3 点击**危害表现设置 (Indications of Compromise Settings)** 旁边的 **编辑**（ ）。

步骤 4 要关闭或关闭整个 IOC 功能，请点击 **Enable IOC** 旁边的滑块。

步骤 5 要全局启用或禁用个别 IOC 规则，请点击相应规则的**启用 (Enabled)** 列中的滑块。

步骤 6 点击**保存 (Save)** 以保存 IOC 规则设置。

下一步做什么

- 部署配置更改。

将 NetFlow 导出器添加到网络发现策略

开始之前

- 配置计划使用的 NetFlow 导出器，如Netflow 数据，第 1905 页中所述。
- 审核其他 NetFlow 必备条件，如使用 NetFlow 数据的要求，第 1906 页中所述。

过程

步骤 1 选择策略 > 网络发现。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击 **Advanced**。

步骤 3 点击 **NetFlow 设备**旁边的 **添加**（+） 。

步骤 4 在 **IP 地址 (IP Address)** 字段中，输入要使受管设备从中收集 NetFlow 数据的网络设备的 IP 地址。

步骤 5 或者：

- 重复前两个步骤以添加其他 NetFlow 导出器。
- 通过点击 **删除**（🗑）删除 NetFlow 导出器。请记住，如果在发现规则中使用 NetFlow 导出器，必须先删除该规则，然后才能从“高级”(Advanced) 页面中删除设备。

步骤 6 点击**保存 (Save)**。

下一步做什么

- 配置网络发现规则以监控 NetFlow 流量，如配置网络发现规则，第 1968 页中所述。
- 部署配置更改。

网络发现数据存储设置

发现数据存储设置包括主机限制和超时设置。

When Host Limit Reached

Cisco Secure Firewall Management Center可以监控因而存储在网络映射中的主机数取决于其型号。**当达到主机限制时 (When Host Limit Reached)** 选项控制在达到主机限制后检测到新主机时发生的情况。您可以执行以下操作：

丢弃主机

系统丢弃保持非活动状态时间最长的主机，然后添加新主机。这是默认设置。

不插入新主机

系统不跟踪任何新发现的主机。系统仅在主机计数降至低于限制后跟踪新主机，例如，在管理员增大域的主机限制或从网络映射中手动删除主机后，或者，如果系统因主机不活动而将其识别为已超时。

在多域部署中，分叶域共享受监控主机的可用池。要确保每个分叶域都可以填充其网络映射，可以在域的属性中的任何子域级别设置主机限制。由于每个分叶域具有各自的网络发现策略，因此在系统发现新主机时，每个分叶域会监管各自的行为，如下表所述。

表 *208:* 达到多租户的主机限制

设置	已设置域主机限制？	已达到域主机限制	已达到祖先域主机限制
丢弃主机	是	丢弃受限制域中的最旧主机。	丢弃配置为丢弃主机的所有后代分叶域中的最旧主机。 如果无法丢弃任何主机，则不添加主机。
	否	不适用	丢弃配置为丢弃主机以及共享常规池的所有后代分叶域中的最旧主机。
不插入新主机	是/否	不添加主机。	不添加主机。

主机超时 (Host Timeout)

系统因网络映射中的某一主机不活动而丢弃该主机之前经过的时间（以分钟为单位）。默认设置为 10080 分钟（一周）。单个主机 IP 和 MAC 地址可以单独超时，但是，除非主机的所有关联地址都超时，否则该主机不会从网络映射中消失。

要避免主机提前超时，请确保主机超时值大于网络发现策略常规设置中的更新间隔。

服务器超时 (Server Timeout)

系统因网络映射中的某一服务器不活动而丢弃该服务器之前经过的时间（以分钟为单位）。默认设置为 10080 分钟（一周）。

要避免服务器提前超时，请确保服务超时值大于网络发现策略常规设置中的更新间隔。

客户端应用超时 (Client Application Timeout)

系统因网络映射中的某一客户端不活动而丢弃该客户端之前经过的时间（以分钟为单位）。默认设置为 10080 分钟（一周）。

确保客户端超时值大于网络发现策略常规设置中的更新间隔。

相关主题

Firepower 系统主机限制

配置网络发现数据存储

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击 **Advanced**。

步骤 3 点击 **数据存储设置** 旁边的 **编辑**（ ）。

步骤 4 更新“数据存储设置”(Data Storage Settings) 对话框中的设置，如网络发现数据存储设置，第 1982 页中所述。

步骤 5 点击**保存 (Save)** 以保存数据存储设置。

下一步做什么

- 部署配置更改。

配置网络发现事件日志记录

事件日志记录设置控制是否记录发现和主机输入事件。如果不记录事件，则无法在事件视图中检索事件，也不能将事件用于触发关联规则。

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击 **Advanced**。

步骤 3 点击 **事件日志记录设置**旁边的 **编辑**（ ）。

步骤 4 选中或取消选中要在数据库中记录的发现和主机输入事件类型旁边的复选框，。

步骤 5 点击**保存 (Save)** 以保存事件日志记录设置。

下一步做什么

- 部署配置更改。

添加网络发现操作系统和服务器身份源

在网络发现策略的“高级”中，可以添加新的主动源，或更改现有源的优先级或超时设置。

将扫描工具添加到此页面不会添加 Nmap 扫描工具已有的完整集成功能，但允许集成导入的第三方应用或扫描结果。

如果从第三方应用或扫描工具导入数据，请确保将源中的漏洞映射到网络中检测到的漏洞。

过程

步骤 1 选择**策略** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击 **Advanced**。

步骤 3 点击 **操作系统和服务器身份源** 旁边的 **编辑**（ ）。

步骤 4 要添加新源，请点击 **Add Source**。

步骤 5 输入 **Name**。

步骤 6 从下拉列表中选择输入源**类型 (Type)**：

- 如果打算使用 AddScanResult 函数导入扫描结果，请选择**扫描工具 (Scanner)**。
- 如果不打算导入扫描结果，请选择**应用 (Application)**。

步骤 7 要指示从此源将某个身份添加到网络映射到删除该身份之间的持续时间，请从**超时 (Timeout)** 下拉列表中选择**小时数 (Hours)**、**天数 (Days)** 或**周数 (Weeks)**，并输入适当的持续时间。

步骤 8 或者：

- 要升级某个源并使用操作系统和应用身份以支持列表中该源下面的源，请选择该源并点击向上箭头。
- 要降级某个源并且只有列表中该源上面的源没有提供身份时才会使用操作系统和应用身份，请选择改源并点击向下箭头。
- 要删除某个源，请点击该源旁边的 **删除**（ ）。

步骤 9 点击**保存 (Save)** 以保存身份源设置。

下一步做什么

- 部署配置更改。

相关主题

映射第三方漏洞，第 1922 页

对网络发现策略进行故障排除

在对系统的默认检测功能进行任何更改之前，应分析哪些主机未被正确地识别以及原因，以便可以决定实施哪些解决方案。

受管设备是否正确布置？

如果诸如负载均衡器、代理服务器或NAT 设备的网络设备位于受管设备和未识别或错误识别的主机之间，请将受管设备布置在更靠近错误识别的主机的位置，而不是使用自定义指纹技术。思科不建议在这种情况下使用自定义指纹技术。

未识别的操作系统是否拥有唯一的 TCP 堆栈？

如果系统识别的主机错误，应调查主机为何被错误地识别，以便帮助您决定：是创建和激活自定义指纹，还是用 Nmap 或主机输入数据替代发现数据。

⚠

注意 如果遇到错误识别的主机，请在创建自定义指纹之前联系支持代表。

如果主机正在运行的操作系统未被系统默认检测到，并且该操作系统不与检测到的现有操作系统共享识别性 TCP 堆栈特征，则应创建自定义指纹。

例如，如您拥有的 Linux 自定义版本带有系统无法识别的唯一 TCP 堆叠，则创建自定义指纹将让您受益，因为这可使系统识别并继续监控主机，而不必使用扫描结果或第三方数据，进而无需持续自行主动更新这些数据。

请注意，许多开源 Linux 发行版本使用相同的内核，同样，系统将使用 Linux 内核名称来识别它们。如为 Red Hat Linux 系统创建自定义指纹，可能会看到识别为 Red Hat Linux 的其他操作系统（如 Debian Linux、Mandrake Linux、Knoppix 等），因为相同的指纹与多个 Linux 发行版本匹配。

不应在每种情况下都使用指纹。例如，可能对主机的 TCP 堆叠做出了修改，以使其与另一操作系统类似或相同。例如，Apple Mac OS X 主机已修改，使其指纹与 Linux 2.4 主机相同，从而导致系统将其识别为 Linux 2.4 而不是 Mac OS X。如果为 Mac OS X 主机创建自定义指纹，可能会导致所有合法的 Linux 2.4 主机被错误地识别为 Mac OS X 主机。在这种情况下，如果 Nmap 正确地识别主机，应为该主机安排定期的 Nmap 扫描。

如果使用主机输入从第三方系统导入数据，则必须将第三方用于描述服务器和应用协议的供应商、产品和版本字符串映射到这些产品的思科定义。请注意，即使将应用数据映射到 Firepower 系统供应商和版本定义，导入的第三方漏洞也不用于客户端或 Web 应用的影响评估。

系统可以协调来自多个源的数据，以便确定操作系统或应用的当前标识。

对于 Nmap 数据，可安排定期 Nmap 扫描。对于主机输入数据，可定期运行用于导入的 Perl 脚本或命令行实用程序。然而，请注意，主动扫描数据和主机输入数据可能不会随发现数据的频率进行更新。

Firepower 系统能否识别所有应用？

如果主机已由系统正确识别，但有未识别的应用，则可创建用户定义的检测器来向系统提供端口和模式匹配信息以帮助识别应用。

是否已应用可修复漏洞的修补程序？

如果系统已正确识别主机，但未反映已应用的修补，则可使用主机输入功能导入修补程序信息。导入修补程序信息时，必须将修补程序的名称映射至数据库中的修补程序。

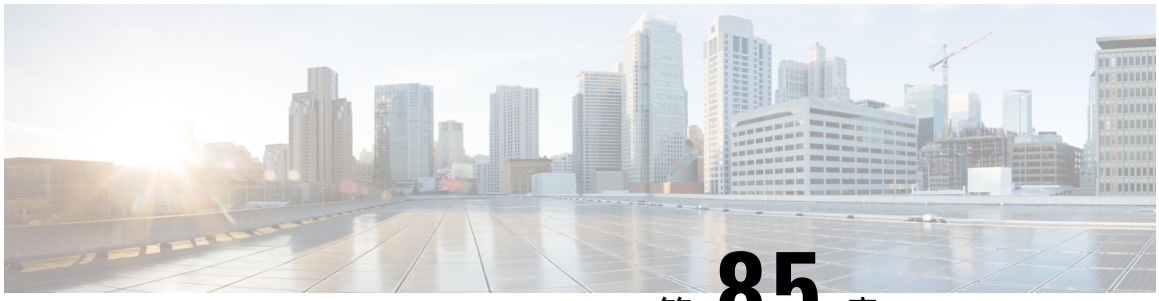
是否要跟踪第三方漏洞？

如果拥有要用于影响关联的第三方系统的漏洞信息，则可将服务器和应用协议的第三方漏洞标识符映射到思科数据库中的漏洞标识符，然后使用主机输入功能导入漏洞。有关使用主机输入功能的详

细信息，请参阅《《*Firepower* 系统主机输入 *API* 指南》》。请注意，即使将应用数据映射到 Firepower 系统供应商和版本定义，导入的第三方漏洞也不用于客户端或 Web 应用的影响评估。

第 XIX 部分

FlexConfig 策略



第 85 章

FlexConfig 策略

以下主题介绍如何配置和部署 FlexConfig 策略。

FlexConfig 策略概述

FlexConfig 策略是 FlexConfig 对象的有序列表的容器。每个对象都包含一系列 Apache Velocity 脚本语言命令（即 ASA 配置命令）和您定义的变量。每个 FlexConfig 对象的内容实质上是一个程序，它生成一系列 ASA 命令，然后将其部署到指定的设备。然后，此命令序列会在 威胁防御设备上配置相关功能。

威胁防御使用 ASA 配置命令实现一些功能，但不是所有功能。没有唯一的一组 威胁防御配置命令。相反，FlexConfig 的要点是允许您配置尚未通过 管理中心策略和设置直接支持的功能。

⚠

注意 思科强烈建议仅具有较强 ASA 背景且自承风险的高级用户使用 FlexConfig 策略。您可以配置不受禁止的任何命令。通过 FlexConfig 启用功能可能会导致配置的其他功能出现意想不到的结果。

您可以联系思科技术支持中心获取有关您已配置的 FlexConfig 策略的支持。思科技术支持中心不代表任何客户设计或编写自定义配置。思科不保证正确的操作或与其他 Firepower 系统功能的互通性。FlexConfig 功能可能随时被摒弃。为获得充分保证的功能支持，您必须等待 管理中心 支持。当有疑问时，请勿使用 FlexConfig 策略。

FlexConfig 策略的建议用法

FlexConfig 有两大主要推荐用途：

- 您正在从 ASA 转换为 威胁防御，并且存在您正在使用（且需要继续使用）的 管理中心 不直接支持的兼容功能。在这种情况下，请在 ASA 上使用 **show running-config** 命令来查看功能配置，并创建 FlexConfig 对象以实施此功能。尝试使用对象的部署设置（一次/每次和追加/预置）以获得正确的设置。通过比较两个设备上的 **show running-config** 输入予以验证。
- 您正在使用 威胁防御，但有一个设置或功能需要配置，例如思科技术援助中心告诉您特定的设置应解决您遇到的特定问题。对于复杂功能，请使用实验室设备测试 FlexConfig，并验证您是否将得到预期行为。

系统包含一组预定义的 FlexConfig 对象，它们代表已测试的配置。如果所需的功能没有由这些对象表示，请首先确定是否可以在标准策略中配置等效功能。例如，访问控制策略包括 ASA 使用单独功能实现的入侵检测和预防、HTTP 和其他类型的协议检查、URL 过滤、应用过滤和访问控制。由于许多功能并未使用 CLI 命令予以配置，因此，您不会看到各策略均显示在 **show running-config** 输出内。

注释 在任何时候，请记住 ASA 和 威胁防御之间不存在一对一重叠关系。请勿尝试在 威胁防御设备上完全重新创建 ASA 配置。您必须仔细测试使用 FlexConfig 配置的各项功能。

FlexConfig 对象中的 CLI 命令

威胁防御 使用 ASA 配置命令配置某些功能。虽然并非所有 ASA 功能都与 威胁防御兼容，但有一些功能可以在 威胁防御 上使用，但不能在 管理中心 策略中进行配置。可以使用 FlexConfig 对象指定配置这些功能所需的 CLI。

如果您决定使用 FlexConfig 手动配置功能，则应根据正确的语法了解和执行这些命令。FlexConfig 策略不验证 CLI 命令语法。有关正确语法和配置 CLI 命令的更多信息，请使用以下 ASA 文档作为参考：

- ASA CLI 配置指南介绍了如何配置功能。指南位于：https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html
- ASA 命令参考提供按命令名称排序的附加信息。参考位于：https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-command-reference-list.html

以下主题介绍了有关配置命令的更多信息。

确定 ASA 软件版本和当前 CLI 配置

由于系统使用 ASA 软件命令配置某些功能，因此需要确定在 威胁防御设备上运行的软件中使用的当前 ASA 版本。此版本号指示用于指导配置功能的 ASA CLI 配置指南。此外，您还应检查当前基于 CLI 的配置，并将其与要实施的 ASA 配置进行比较。

注意，任何 ASA 配置都与 威胁防御 配置有着显著的差异。许多 威胁防御 策略都是在 CLI 之外配置的，因此查看这些命令看不到配置。请勿尝试在 ASA 和 威胁防御 配置之间创建一对一的对应关系。

要查看此信息，请与设备的管理界面建立 SSH 连接，并发出以下命令：

- **show version system** 并查找思科自适应安全装置软件版本号。（如果您通过 Cisco Secure Firewall Management Center CLI 工具发出命令，请忽略 **system** 关键字。）
- **show running-config** 查看当前的 CLI 配置。
- **show running-config all** 包括当前 CLI 配置中的所有默认命令。

也可以使用以下过程在 管理中心中发出这些命令。

过程

步骤 1 选择**系统** > **运行状况** > **监视**。

步骤 2 点击 FlexConfig 策略适用的设备的名称。

您可能需要点击“状态”表中**计数**列中的打开/关闭箭头来查看任何设备。

步骤 3 选择**高级故障排除**。

步骤 4 选择**威胁防御 CLI**。

步骤 5 选择 **show** 作为命令，然后键入**版本**或其他命令之一作为参数。

步骤 6 点击**执行 (Execute)**

对于版本，请搜索思科自适应安全设备软件版本号的输出。

您可以选择输出并按 Ctrl+C 组合键，然后将其粘贴到文本文件中以供日后分析之用。

禁止的 CLI 命令

FlexConfig 的用途是配置在 ASA 设备上可用但无法使用 管理中心在 威胁防御设备上配置的功能。

因此，您无法配置在 管理中心中具有等同功能的 ASA 功能。下表列出的是一些禁止的命令区。

此外，一些 **clear** 命令已被禁止，因为它们与多项托管策略重叠，并且可以删除托管策略的部分配置。

FlexConfig 对象编辑器可防止将被禁止的命令纳入对象中。

禁止的 CLI 命令	说明
AAA	阻止配置。
AAA-Server	阻止配置。
Access-list	阻止高级 ACL、扩展 ACL 和标准 ACL。允许 Ethertype ACL。 可以使用在模板内的对象管理器中定义的标准和扩展ACL对象作为变量。
ARP Inspection	阻止配置。

禁止的 CLI 命令	说明
As-path Object	阻止配置。
Banner	阻止配置。
BGP	阻止配置。
Clock	阻止配置。
Community-list Object	阻止配置。
Copy	阻止配置。
Delete	阻止配置。
DHCP	阻止配置。
Enable Password	阻止配置。
Erase	阻止配置。
Fragment Setting	被阻止，**fragment reassembly**除外。
Fsck	阻止配置。
HTTP	阻止配置。
ICMP	阻止配置。
Interface	仅阻止 **nameif**、**mode**、**shutdown**、**ip address** 和 **mac-address** 命令。
Multicast Routing	阻止配置。
NAT	阻止配置。
Network Object/Object-group	将阻止在 FlexConfig 对象中创建网络对象，但可使用在模板内的对象管理器中定义的网络对象和组作为变量。
NTP	阻止配置。
OSPF/OSPFv3	阻止配置。
pager	阻止配置。
Password Encryption	阻止配置。
Policy-list Object	阻止配置。
Prefix-list Object	阻止配置。

禁止的 CLI 命令	说明
重新加载	不能安排重新加载。系统不使用 **reload** 命令重启系统，它使用的是 **reboot** 命令。
RIP	阻止配置。
Route-Map Object	将阻止 FlexConfig 对象中创建路由映射对象，但可使用在模板内的对象管理器中定义的路由映射对象作为变量。
Service Object/Object-group	将阻止 FlexConfig 对象中创建服务对象，但可使用在模板内的对象管理器中定义的端口对象作为变量。
SNMP	阻止配置。
SSH	阻止配置。
Static Route	阻止配置。
Syslog	阻止配置。
Time Synchronization	阻止配置。
Timeout	阻止配置。
VPN	阻止配置。

模板脚本

您可以使用脚本语言来控制 FlexConfig 对象内的处理。脚本语言指令是 Apache Velocity 1.3.1 模板引擎中支持的命令子集，它是一种支持循环、if/else 语句和变量的基于 Java 的脚本语言。

要了解如何使用该脚本语言，请参阅 http://velocity.apache.org/engine/devel/developer-guide.html 的 *Velocity* 开发人员指南。

FlexConfig 变量

在命令或处理指令的一部分依赖于运行时信息而不是静态信息的情况下，可以在 FlexConfig 对象中使用变量。在部署过程中，变量将替换为基于变量类型从设备的其他配置所获得的字符串：

- 策略对象变量被替换为从 管理中心中定义的对象获取的字符串。
- 系统变量被替换为从设备本身或为其配置的策略中获取的信息。
- 处理脚本命令时，处理变量随策略对象或系统变量的内容一起加载。例如，在循环中将策略对象或系统变量中的一个值通过迭代方式加载到处理变量中，然后使用处理变量组成命令字符串或执行其他操作。这些处理变量在 FlexConfig 对象中的变量列表中不显示。此外，也不要使用 FlexConfig 对象编辑器中的**插入**菜单添加这些变量。

- 密钥变量被替换为 FlexConfig 对象中为该变量定义的单个字符串。

以 $ 字符开头的变量，除以 @ 字符开头的密钥变量变量之外。例如，在下面的命令中 $ifname 是一个策略对象变量，而 @keyname 是一个密钥。

```
interface $ifname
key @keyname
```

注释 第一次插入策略对象或系统变量时，必须通过 FlexConfig 对象编辑器中的**插入**菜单执行操作。此操作可将变量添加到 FlexConfig 对象编辑器底部的**变量**列表中。但您必须在随后的使用中键入变量字符串，即使在使用系统变量时也是如此。如果添加的处理变量没有对象或系统变量赋值，请不要使用**插入**菜单。如果要添加密钥，请始终使用**插入**菜单。密钥变量在变量列表中不显示。

变量是否被解析为单个字符串、字符串列表或值表取决于分配给变量的策略对象或系统变量的类型。（密钥始终解析为单个字符串）。您必须了解返回的内容，以便正确处理变量。

以下主题解释各种类型的变量以及如何处理这些变量。

如何处理变量

在运行时，变量可以解析为单个字符串、相同类型的字符串列表、不同类型的字符串列表或命名值表。此外，解析为多个值的变量的长度可以是确定的，也可以是不定的。您必须了解要返回的内容才能正确处理这些值。

以下是可能出现的主要情况：

单值变量

如果变量始终解析为单个字符串，则在 FlexConfig 脚本中直接使用该变量而不进行修改。

例如，预定义的文本变量 tcpMssBytes 始终解析为单个值（必须为数字）。然后，**Sysopt_basic** FlexConfig 使用 if/then/else 结构根据另一个单值文本变量 tcpMssMinimum 的值设置最大段大小：

```
#if($tcpMssMinimum == "true")
  sysopt connection tcpmss minimum $tcpMssBytes
#else
  sysopt connection tcpmss $tcpMssBytes
#end
```

在此示例中，您将使用 FlexConfig 对象编辑器中的**插入**菜单添加 $tcpMssBytes 的第一个用例，但您可以直接在 #else 行中键入变量。

密钥变量是一种特殊类型的单值变量。对于密钥，始终使用**插入**菜单添加变量，即使是用于第二次和后续的使用。这些变量在 FlexConfig 对象中的变量列表中不显示。

注释 网络对象的策略对象变量也等同于单个 IP 地址规范，即主机地址、网络地址或地址范围。但在这种情况下，您必须清楚需要什么类型的地址，因为 ASA 命令需要特定的地址类型。例如，如果命令需要主机地址，使用指向包含网络地址的对象的网络对象变量将导致部署过程中出错。

多值变量，所有值都具有相同类型

多个策略对象和系统变量解析为同一类型的多个值。例如，指向网络对象组的对象变量解析为组中 IP 地址的列表。同样，系统变量 $SYS_FW_INTERFACE_NAME_LIST 解析为接口名称的列表。

还可以为同一类型的多个值创建文本对象。例如，预定义的文本对象 enableInspectProtocolList 可以包含多个协议名称。

解析为同一类型项目列表的多值变量通常具有不定长度。例如，您无法预先知道命名了设备上的多少个接口，因为用户可以随时配置或取消配置接口。

因此，您通常使用循环来处理同一类型的多值变量。例如，预定义的 FlexConfig **Default_Inspection_Protocol_Enable** 使用 #foreach 循环来遍历 enableInspectProtocolList 对象并处理每个值。

```
policy-map global_policy
    class inspection_default
    #foreach ( $protocol in $enableInspectProtocolList)
    inspect $protocol
    #end
```

在此示例中，该脚本依次将每个值分配给 $protocol 变量，然后在 ASA **inspect** 命令中使用该变量为该协议启用检测引擎。在这种情况下，您只需键入 $protocol 作为变量名称。您不使用**插入**菜单来添加它，因为您没有将对象或系统值分配给该变量。但是，必须使用**插入**菜单添加 $enableInspectProtocolList。

系统在 #foreach 和 #end 之间循环遍历代码，直到 $enableInspectProtocolList 中没有剩余的值。

多个值变量，值具有不同的类型

可以创建多个值文本对象，但每个值都有不同的用途。例如，预定义的 **netflow_Destination** 文本对象应具有 3 个值，分别表示接口名称、目标 IP 地址和 UDP 端口号。

以这种方式定义的对象应具有确定的值数。否则，它们将很难处理。

使用 get 方法处理这些对象。在对象名称的末尾键入 **.get(*n*)**，并将 *n* 替换为对象中的索引。从 0 开始计数，即使文本对象从 1 开始列出其值亦是如此。

例如，Netflow_Add_Destination 对象使用以下行将 netflow_Destination 中的 3 个值添加到 ASA **flow-export** 命令。

```
flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(1)
$netflow_Destination.get(2)
```

在此示例中，您将使用 FlexConfig 对象编辑器中的**插入**菜单添加 $netflow_Destination 的第一次使用，然后添加 **get(0)**。但您可以直接为 **$netflow_Destination.get(1)** 和 **$netflow_Destination.get(2)** 规范键入该变量。

解析到值表的多个值变量

有些系统变量会返回一个值表。这些变量包括其名称中的 MAP，例如 $SYS_FTD_ROUTED_INTF_MAP_LIST。路由接口映射返回的数据如下所示（为了清楚起见，添加了换行）：

```
[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},

{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=diagnostic}]
```

在上面的示例中，将为 4 个接口返回信息。每个 接口都包括一个指定值表。例如，intf_hardwarare_id 是 接口硬件名称属性的名称，并将返回诸如 GigabitEthernet0/0 的字符串。

这种类型的变量通常长度不确定，因此您需要 使用环路来处理值。但您还需要将属性 名称添加到变量名称中，以指示要检索哪个值。

例如，IS-IS 配置需要在接口配置模式下将 ASA **isis** 命令添加到某一具有逻辑名称的接口。但您可以使用该接口的 硬件名称进入该模式。因此，您需要确定哪些接口具有 逻辑名称，然后仅配置使用其硬件名称的那些接口。预定义了 ISIS_Interface_Configuration 的 FlexConfig 使用 嵌套在环路中的 if/then 结构来进行此操作。在下面的代码中，可以看到 #foreach 脚本命令会将每个接口映射加载到 $intf 变量中， 然后 #if 语句将切断映射 ($intf.intf_logical_name) 中的 intf_logical_name 值，并且如果该值位于 isisIntfList 预定义文本变量中定义的列表中，则请使用 intf_hardwarare_id 值 ($intf.intf_hardwarare_id) 输入接口命令。您需要编辑 isisIntfList 变量以添加要在其上配置 IS-IS 的接口的 名称。

```
#foreach ($intf in $SYS_FTD_ROUTED_INTF_MAP_LIST)
 #if ($isIsIntfList.contains($intf.intf_logical_name))
  interface $intf.intf_hardwarare_id
   isis
   #if ($isIsAddressFamily.contains("ipv6"))
   ipv6 router isis
   #end
 #end
#end
```

如何查看将为设备返回什么变量

评估将会返回什么变量的一种简单方式是创建一个简单的 FlexConfig 对象，该对象除了处理带有注释的变量列表以外，不进行任何其他操作。随后可将该对象分配给某一 FlexConfig 策略，再将该策略分配给某一设备，保存该策略，然后预览该设备的配置。该预览将显示解析出来的值。可以选择预览文本，按 Ctrl+C 键，然后将输出粘贴到文本文件中用于分析。

注释 但不要将此 FlexConfig 部署到设备，因为它不会包含任何有效的配制命令。您将收到部署错误。在获得预览后，请从 FlexConfig 策略中删除该 FlexConfig 对象，然后保存该策略。

例如，可以构建以下 FlexConfig 对象：

```
Following is a network object group variable for the
IPv4-Private-All-RFC1918 object:

$IPv4_Private_addresses

Following is the system variable SYS_FW_MANAGEMENT_IP:

$SYS_FW_MANAGEMENT_IP

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

$SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:

$SYS_FTD_ROUTED_INTF_MAP_LIST

Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

$SYS_FW_INTERFACE_NAME_LIST
```

此对象的 预览可能如下所示（为了清楚起见，添加了换行）：

```
###Flex-config Prepended CLI ###

###CLI generated from managed features ###

###Flex-config Appended CLI ###
Following is an network object group variable for the
IPv4-Private-All-RFC1918 object:

[10.0.0.0, 172.16.0.0, 192.168.0.0]

Following is the system variable SYS_FW_MANAGEMENT_IP:

192.168.0.171

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

[dns, ftp, h323 h225, h323 ras, rsh, rtsp, sqlnet, skinny, sunrpc,
xdmcp, sip, netbios, tftp, icmp, icmp error, ip-options]

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:
```

```
[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},

{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=diagnostic}]

Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

[outside, inside, diagnostic]
```

FlexConfig 策略对象变量

策略对象变量与在对象管理器中配置的特定策略对象关联。在 FlexConfig 对象中插入策略对象变量时，将为该变量提供一个名称，并选择与其关联的对象。

尽管可以为变量提供与关联对象完全相同的名称，但变量本身与关联对象不同。必须使用FlexConfig对象编辑器中的**插入** > **插入策略对象** > **对象类型**菜单首次将该变量添加到 FlexConfig 中的脚本，以建立与该对象的关联。仅键入前面带有 $ 符号的对象的名称不会创建策略对象变量。

您可以创建变量以指向以下类型的对象。确保为每个变量创建正确的对象类型。要创建对象，请转到**对象** > **对象管理**页面。

- **文本对象** - 适用于文本字符串，可以包括 IP 地址、数字和其他自由格式文本，如接口或区域名称。从目录中选择 **FlexConfig** > **文本对象**，然后点击**添加文本对象**。可以将这些对象配置为包含单个值或多个值。这些对象具有高度的灵活性，专用于 FlexConfig 对象。有关详细信息，请参阅配置 FlexConfig 文本对象 ， 第 2016 页。
- **网络** - 适用于 IP 地址。可以使用网络对象或组。从目录中选择**网络**，然后选择**添加网络** > **添加对象**或**添加组**。如果使用组对象，该变量将返回组中每个 IP 地址规范的列表。地址可以是主机、网络或地址范围，具体取决于对象内容。请参阅网络 ， 第 997 页。
- **安全区域** - 适用于安全区域或接口组中的接口。从目录中选择**接口**，然后选择**添加** > **安全区域**或**接口组**。安全区域变量将为正配置的设备返回该区域或组内的接口列表。请参阅接口 ， 第995页。
- **标准的 ACL 对象** - 适用于标准访问控制列表。标准 ACL 变量返回标准 ACL 对象的名称。从目录中选择**访问列表** > **标准**，然后点击**添加标准访问列表对象**。请参阅访问列表 ， 第 975 页。
- **扩展 ACL 对象** - 适用于扩展访问控制列表。扩展 ACL 变量将返回扩展 ACL 对象的名称。从目录中选择**访问列表** > **扩展**，然后点击**添加扩展访问列表对象**。请参阅访问列表 ， 第 975 页。

- **路由映射** - 适用于路由映射对象。路由映射变量将返回路由映射对象的名称。从目录中选择**路由映射**，然后点击**添加路由映射**。请参阅路由映射，第 1022 页。

FlexConfig 系统变量

系统变量会被替换为从设备本身或为其配置的策略中获取的信息。

必须使用 FlexConfig 对象编辑器中的**插入** > **插入系统变量** > **变量名**菜单，第一次就开始将变量添加到 FlexConfig 中的脚本以建立与系统变量的关联。只键入系统变量的名称并前跟 $ 符号不会在 FlexConfig 对象的上下文中创建系统变量。

下表介绍了可用的系统变量。在使用变量之前，检查通常为变量返回的内容；请参阅如何查看将为设备返回什么变量，第 1999 页。

名称	说明
SYS_FW_OS_MODE	设备的操作系统模式。可能的值包括 ROUTED 或 TRANSPARENT。
SYS_FW_OS_MULTIPLICITY	设备在单情景模式还是多情景模式下运行。可能的值包括 SINGLE、MULTI 或 NOT_APPLICABLE。
SYS_FW_MANAGEMENT_IP	设备的管理 IP 地址
SYS_FW_HOST_NAME	设备主机名
SYS_FTD_INTF_POLICY_MAP	以接口名称作为键并将策略映射为值的映射。如果设备上没有定义基于接口的服务策略，则此变量将不返回任何值。
SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST	启用了检查的协议的列表。
SYS_FTD_ROUTED_INTF_MAP_LIST	设备上路由接口映射的列表。每个映射都包含一组与路由接口配置相关的命名值。
SYS_FTD_SWITCHED_INTF_MAP_LIST	设备上交换接口映射的列表。每个映射都包含一组与交换接口配置相关的命名值。
SYS_FTD_INLINE_INTF_MAP_LIST	设备上内联接口映射的列表。每个映射都包含一组与内联集接口配置相关的命名值。
SYS_FTD_PASSIVE_INTF_MAP_LIST	设备上被动接口映射的列表。每个映射都包含一组与被动接口配置相关的命名值。
SYS_FTD_INTF_BVI_MAP_LIST	设备上网桥虚拟接口映射的列表。每个映射都包含一组与 BVI 配置相关的命名值。
SYS_FW_INTERFACE_HARDWARE_ID_LIST	设备上接口硬件名称（如 GigabitEthernet0/0）的列表。
SYS_FW_INTERFACE_NAME_LIST	设备上接口逻辑名称（如内部）的列表。
SYS_FW_INLINE_INTERFACE_NAME_LIST	配置为被动或 ERSPAN 被动的接口的逻辑名称列表。

名称	说明
SYS_FW_NON_INLINE_INTERFACE_NAME_LIST	不属于内联集的接口（如所有路由接口）的逻辑名称列表。

预定义的 FlexConfig 对象

预定义的 FlexConfig 对象为选定功能提供经过测试的配置。如果需要配置这些功能，请使用这些对象，否则无法使用管理中心配置这些功能。

下表列出了可用的对象。记下关联的文本对象。您必须编辑这些文本对象，才能自定义预定义 FlexConfig 对象的行为。文本对象使您可以使用网络和设备所需的 IP 地址和其他属性来自定义配置。

如果需要修改预定义 FlexConfig 对象，请复制该对象，对副本进行更改，然后使用新名称进行保存。不能直接编辑预定义 FlexConfig 对象。

尽管您可以使用 FlexConfig 配置其他基于 ASA 的功能，但这些功能的配置尚未经过测试。如果某个 ASA 功能与您可以在 管理中心策略中配置的内容重叠，请勿尝试通过 FlexConfig 对该功能进行配置。

例如，Snort 检查包括 HTTP 协议，因此不可启用 ASA 式 HTTP 检查。（实际上，您无法将 **http** 添加到 enableInspectProtocolList 对象。在这种情况下，您将被阻止以免错误配置您的设备。）相反，应根据需要配置访问控制策略以执行应用或 URL 过滤，以实施 HTTP 检查要求。

表 *209:* 预定义的 *FlexConfig* 对象

FlexConfig 对象名称	**Description**	关联的文本对象
Default_Inspection_Protocol_Disable	在 global_policy 默认策略映射中禁用协议。	disableInspectProtocolList
Default_Inspection_Protocol_Enable	在 global_policy 默认策略映射中启用协议。	enableInspectProtocolList
DHCPv6_Prefix_Delegation_Configure	为 IPv6 前缀委派配置一个外部接口（前缀委派客户端）和一个内部接口（委派前缀的接收者）。要使用此模板，请对其进行复制并修改变量。	pdoutside、pdinside 还使用系统变量 SYS_FTD_ROUTED_INTF_MAP_LIST
DHCPv6_Prefix_Delegation_UnConfigure	删除 DHCPv6 前缀委派配置。	pdoutside、pdinside 还使用系统变量 SYS_FTD_ROUTED_INTF_MAP_LIST
Inspect_IPv6_Configure	在 global_policy 策略映射中配置 IPv6 检查，从而根据 IPv6 报头内容记录和丢弃流量。	IPv6RoutingHeaderDropLogList、IPv6RoutingHeaderLogList、IPv6RoutingHeaderDropList。
Inspect_IPv6_UnConfigure	清除并禁用 IPv6 检查。	—

FlexConfig 对象名称	Description	关联的文本对象
ISIS_Configure	为 IS-IS 路由配置全局参数。	isIsNet、isIsAddressFamily、isISType
ISIS_Interface_Configuration	接口级别 IS-IS 配置。	isIsAddressFamily、IsIsIntfList 还使用系统变量 SYS_FTD_ROUTED_INTF_MAP_LIST
ISIS_Unconfigure	清除设备上的 IS-IS 路由器配置。	—
ISIS_Unconfigure_All	从设备中清除 IS-IS 路由器配置，包括来自设备接口的路由器分配。	—
Netflow_Add_Destination	创建和配置 Netflow 导出目标。	Netflow_Destinations、netflow_Event_Types
Netflow_Clear_Parameters	恢复 Netflow 导出全局默认设置。	—
Netflow_Delete_Destination	删除 Netflow 导出目标。	Netflow_Destinations、netflow_Event_Types
Netflow_Set_Parameters	为 Netflow 导出设置全局参数。	netflow_Parameters
NGFW_TCP_NORMALIZATION	修改默认 TCP 规范化配置。	—
Policy_Based_Routing	要使用此示例配置，请复制它，修改接口名称，然后使用 r-map-object 文本对象标识对象管理器中的路由映射对象。	—
Policy_Based_Routing_Clear	从设备中清除策略型路由配置。	—
Sysopt_AAA_radius	忽略 RADIUS 记帐响应中的身份验证密钥。	—
Sysopt_AAA_radius_negate	使 Sysopt_AAA_radius 配置失效。	—
Sysopt_basic	配置 sysopt 等待时间、TCP 数据包的最大报文段长度以及详细流量统计信息。	tcpMssMinimum、tcpMssBytes
Sysopt_basic_negate	清除 sysopt_basic 详细流量统计信息、等待时间和 TCP 最大报文段长度。	—
Sysopt_clear_all	从设备中清除所有 sysopt 配置。	—
Sysopt_noproxyarp	配置 noproxy-arp CLI。	使用系统变量 SYS_FW_NON_INLINE_INTF_NAME_LIST
Sysopt_noproxyarp_negate	清除 Sysopt_noproxyarp 配置。	使用系统变量 SYS_FW_NON_INLINE_INTF_NAME_LIST
Sysopt_Preserve_Vpn_Flow	配置 syopt 保留 VPN 流。	—

FlexConfig 对象名称	Description	关联的文本对象
Sysopt_Preserve_Vpn_Flow_negate	清除 Sysopt_Preserve_Vpn_Flow 配置。	—
Sysopt_Reclassify_Vpn	配置 sysopt 重新分类 VPN。	—
Sysopt_Reclassify_Vpn_Negate	否定 sysopt 重新分类 VPN。	—
Threat_Detection_Clear	清除威胁检测 TCP 拦截配置。	—
Threat_Detection_Configure	配置TCP拦截所拦截攻击的威胁检测统计信息。	threat_detection_statistics
Wccp_Configure	此模板提供了一个配置WCCP的示例。	isServiceIdentifier、serviceIdentifier、wccpPassword
Wccp_Configure_Clear	清除 WCCP 配置。	—

弃用的 FlexConfig 对象

下表列出了用于配置您现在可以在 GUI 中本地配置的功能的对象。尽早停止使用这些对象。

表 *210:* 弃用的预定义 *FlexConfig* 对象

弃用的版本	FlexConfig 对象	Description	现在配置在
6.3	Default_DNS_Configure	配置默认 DNS 组，该组定义在数据接口上解析完全限定域名时可以使用的 DNS 服务器。 关联的文本对象：defaultDNSNameServerList、defaultDNSParameters	平台设置。
6.3	DNS_Configure	在非默认 DNS 服务器组中配置 DNS 服务器。复制对象以更改组的名称。	对象管理器中的 **DNS 服务器组**。
6.3	DNS_UnConfigure	删除由 Default_DNS_Configure 和 DNS_Configure 执行的 DNS 服务器配置。如果您更改了 DNS_Configure，则复制该对象以更改 DNS 服务器组名称。	对象管理器中的 **DNS 服务器组**。

弃用的版本	FlexConfig 对象	Description	现在配置在
7.2	Eigrp_Configure	配置 EIGRP 路由 next-hop、auto-summary、router-id、eigrp-stub。 关联的文本对象：eigrpAS、eigrpNetworks、eigrpDisableAutoSummary、eigrpRouterId、eigrpStubReceiveOnly、eigrpStubRedistributed、eigrpStubConnected、eigrpStubStatic、eigrpStubSummary	有关所有 EIGRP 对象，请参阅 EIGRP，第 889 页。 系统允许您部署升级后，但也会警告您重新执行 EIGRP 配置。为了帮助您完成此过程，我们提供了一个命令行迁移工具。
7.2	Eigrp_Interface_Configure	配置 EIGRP 接口身份验证模式、身份验证密钥、呼叫间隔、保持时间、水平分割。 关联的文本对象：eigrpIntfList、eigrpAS、eigrpAuthKey、eigrpAuthKeyId、eigrpHelloInterval、eigrpHoldTime、eigrpDisableSplitHorizon 还使用系统变量 SYS_FTD_ROUTED_INTF_MAP_LIST	
7.2	Eigrp_Unconfigure	从设备中清除自治系统的 EIGRP 配置。	
7.2	Eigrp_Unconfigure_all	清除所有 EIGRP 配置。	
6.3	TCP_Embryonic_Conn_Limit	配置初始连接限制以防止 SYN 泛洪拒绝服务 (DoS) 攻击。 关联的文本对象：tcp_conn_misc、tcp_conn_limit	服务政策。
6.3	TCP_Embryonic_Conn_Timeout	配置初始连接超时以防止 SYN 洪流拒绝服务 (DoS) 攻击。 关联的文本对象：tcp_conn_misc、tcp_conn_timeout	服务政策。

弃用的版本	FlexConfig 对象	Description	现在配置在
7.2	VxLAN_Clear_Nve	从设备中删除使用 VxLAN_Configure_Port_And_Nve 时配置的 NVE 1。	有关所有 VxLAN 对象，请参阅配置 VXLAN 接口，第 536 页。 如果在以前的版本中使用 FlexConfig 配置了 VXLAN 接口，它们将继续工作。实际上，在这种情况下，FlexConfig 优先 - 如果您在 Web 接口中重做 VXLAN 配置，请删除 FlexConfig 设置。
7.2	VxLAN_Clear_Nve_Only	在部署时，清除在接口上配置的 NVE。	
7.2	VxLAN_Configure_Port_And_Nve	配置 VLAN 端口和 NVE 1。 关联的文本对象：vxlan_Port_And_Nve	
7.2	VxLAN_Make_Nve_Only	仅为 NVE 设置接口。 关联的文本对象：vxlan_Nve_Only 还使用系统变量 SYS_FTD_ROUTED_MAP_LIST 和 SYS_FTD_SWITCHED_INTF_MAP_LIST	
7.2	VxLAN_Make_Vni	创建 VNI 接口。部署此项后，您必须先注销设备，然后再重新注册设备，才能正确发现 VNI 接口。 关联的文本对象：vxlan_Vni	

预定义的文本对象

有多种预定义的文本对象。这些对象与预定义的 FlexConfig 对象中使用的变量关联。在大多数情况下，如果您使用关联的 FlexConfig 对象，则必须编辑这些对象才能添加值，否则将在部署过程中出错。尽管其中一些对象包含默认值，但其他一些则为空。

有关编辑文本对象的信息，请参阅配置 FlexConfig 文本对象，第 2016 页。

名称	说明	关联的 FlexConfig 对象
defaultDNSNameServerList （已弃用。）	要在默认 DNS 组中配置的 DNS 服务器 IP 地址。 从版本 6.3 开始，在 Firepower 威胁防御平台设置策略中为数据接口配置 DNS。	Default_DNS_Configure
defaultDNSParameters （已弃用。）	用于控制默认 DNS 服务器组的 DNS 行为的参数。该对象包含单独的条目，依次为重试、超时、过期条目计时器、轮询计时器、域名条目。 从版本 6.3 开始，在 Firepower 威胁防御平台设置策略中为数据接口配置 DNS。	Default_DNS_Configure
disableInspectProtocolList	在默认策略映射 (global_policy) 中禁用协议。	Disable_Default_Inspection_Protocol
dnsNameServerList	要在用户定义的 DNS 组中配置的 DNS 服务器 IP 地址。	DNS_Configure
dnsParameters	用于控制非默认 DNS 服务器组的 DNS 行为的参数。该对象包含单独的条目，依次为重试、超时、域名、域名服务器条目。	DNS_Configure
enableInspectProtocolList	在默认策略映射 (global_policy) 中启用协议。您将不允许添加其检查与 Snort 检查冲突的协议。	Enable_Default_Inspection_Protocol
IPv6RoutingHeaderDropList	要禁止的 IPv6 路由报头类型的列表。IPv6 检查会丢弃包含这些报头的数据包，而不记录此丢弃。	Inspect_IPv6_Configure
IPv6RoutingHeaderDropLogList	要禁止和记录的 IPv6 路由报头类型的列表。IPv6 检查会丢弃包含这些报头的数据包，并发送有关此丢弃的系统日志消息。	Inspect_IPv6_Configure
IPv6RoutingHeaderLogList	要允许但会记录的 IPv6 路由报头类型的列表。IPv6 检查会允许包含这些报头的数据包，并发送有关存在报头的系统日志消息。	Inspect_IPv6_Configure
isIsAddressFamily	IPv4 或 IPv6 地址系列。	ISIS_Configure ISIS_Interface_Configuration
IsIsIntfList	逻辑接口名称的列表。	ISIS_Interface_Configuration

名称	说明	关联的 **FlexConfig** 对象
isIsISType	IS 类型（级别 1、级别 2 或级别 1-2）。	ISIS_Configure
isIsNet	网络实体。	ISIS_Configure
isServiceIdentifier	如果为 false，则使用标准的 **web-cache** 服务标识符。	Wccp_Configure
netflow_Destination	定义单个 Netflow 导出目标的接口、目标和 UDP 端口号。	Netflow_Add_Destination
netflow_Event_Types	将要为目标导出的事件类型定义为以下任意项的子集：**all**、**flow-create**、**flow-defined**、**flow-teardown**、**flow-update**。	Netflow_Add_Destination
netflow_Parameters	提供 Netflow 导出全局设置：活动刷新间隔（流更新事件之间的分钟数）、延迟（以秒为单位的流创建延迟；默认值 0 = 命令不会出现）和以分钟为单位的模板超时速率。	Netflow_Set_Parameters
PrefixDelegationInside	为 DHCPv6 前缀委派配置内部接口。该对象包含多个条目，依次为接口名称、包含前缀长度的 IPv6 后缀以及前缀池名称。	没有，但可以与 DHCPv6_Prefix_Delegation_Configure 副本一起使用。
PrefixDelegationOutside	配置外部 DHCPv6 前缀委派客户端。该对象包括多个条目，依次为接口名称和 IPv6 前缀长度条目	没有，但可以与 DHCPv6_Prefix_Delegation_Configure 副本一起使用。
serviceIdentifier	动态 WCCP 服务标识符编号。	Wccp_Configure
tcp_conn_limit （已弃用。）	用于配置 TCP 初始连接限制的参数。 从版本 6.3 开始，在 Firepower 威胁防御服务策略中配置这些功能，您可以在分配给设备的访问控制策略的“高级”选项卡上找到该策略。	TCP_Embryonic_Conn_Limit
tcp_conn_misc （已弃用。）	用于配置 TCP 初始连接设置的参数。 从版本 6.3 开始，在 Firepower 威胁防御服务策略中配置这些功能，您可以在分配给设备的访问控制策略的“高级”选项卡上找到该策略。	TCP_Embryonic_Conn_Limit、TCP_Embryonic_Conn_Timeout

名称	说明	关联的 FlexConfig 对象
tcp_conn_timeout （已弃用。）	用于配置 TCP 初始连接超时的参数。 从版本 6.3 开始，在 Firepower 威胁防御服务策略中配置这些功能，您可以在分配给设备的访问控制策略的“高级”选项卡上找到该策略。	TCP_Embryonic_Conn_Timeout
tcpMssBytes	最大段大小（以字节为单位）。	Sysopt_basic
tcpMssMinimum	检查是否设置最大段大小 (MSS)，只有此标志为 true 时才设置该值。	Sysopt_basic
threat_detection_statistics	用于 TCP 拦截的威胁检测统计信息的参数。	Threat_Detection_Configure
vxlan_Nve_Only	用于在接口上配置仅 NVE 的参数： • 接口的逻辑名称 • IPv4 地址（对于路由接口而言可选） • Ipv4 网络掩码（对于路由接口而言可选）	VxLAN_Make_Nve_Only
vxlan_Port_And_Nve	用于为 VXLAN 配置端口和 NVE 的参数： • Vxlan 端口 • 源接口（逻辑名称） • 类型（对等体或组播） • 对等体 IP 地址或 default-mcast-grooup	VxLAN_Configure_Port_And_Nve

名称	说明	关联的 FlexConfig 对象
vxlan_Vni	用于创建 VNI 的参数： • 接口编号 (1-10000) • segment-id (1-16777215) • nameif（接口的逻辑名称） • 类型（路由或透明） • IP 地址（如果是路由模式设备时使用）或网桥组编号（如果是透明模式设备时使用） • 网络掩码（如果设备处于路由模式）或未使用	VxLAN_Make_Vni
wccpPassword	WCCP 密码。	Wccp_Configure

FlexConfig 策略的要求和必备条件

型号支持

威胁防御

支持的域

任意

用户角色

管理员

FlexConfig 的指南与限制

- 如果您在 FlexConfig 策略中犯错，系统将回滚包含失败的 FlexConfig 的部署尝试中包含的所有更改。由于部署失败导致的回滚包括了清除配置，因此这可能会中断您的网络。考虑将FlexConfig 更改纳入非营业时间的计时部署中。此外，请考虑隔离部署，使其仅包括 FlexConfig 更改而不包括其他策略更新。
- 使用 VxLAN_Make_VNI 对象时，必须在形成集群或高可用性对之前，将相同的 FlexConfig 部署到该集群或高可用性对中的所有设备。在形成集群或高可用性对之前，管理中心要求VXLAN 接口在所有设备上都匹配。

使用 FlexConfig 策略自定义设备配置

使用 FlexConfig 策略自定义 威胁防御设备的配置。

在使用 FlexConfig 之前，请尝试使用 管理中心中的其他功能配置所需的所有策略和设置。FlexConfig 是一种配置基于 ASA 的与 威胁防御兼容但在 管理中心中不可配置的功能的必备方法。

以下是配置和部署 FlexConfig 策略的端到端过程。

过程

步骤 1 确定要配置的 CLI 命令序列。

如果在 ASA 设备上具有有效的配置，请使用 **show running-config** 获取所需命令的序列。根据需要对接口名称和 IP 地址等项目进行调整。

如果此步骤是面向新功能，最好尝试在实验室设置中的ASA 设备上实现，以验证您具有正确的命令序列。

有关详细信息，请参阅以下主题：

- FlexConfig 策略的建议用法， 第 1991 页
- FlexConfig 对象中的 CLI 命令， 第 1992 页

步骤 2 选择**对象** > **对象管理**，然后从目录中选择 **FlexConfig** > **FlexConfig 对象**。

检查预定义的 FlexConfig 对象，以确定是否能够生成所需的命令。点击 **视图**（  ） 以查看对象内容。如果现有对象接近您所需的内容，请首先复制该对象，然后编辑副本。请参阅预定义的FlexConfig 对象， 第 2002 页。

检查这些对象还可以让您了解 FlexConfig 对象的结构、命令语法和预期顺序。

注释 如果找到要使用的任何对象（直接对象或或是副本），请检查对象底部的“变量”列表。记下变量名称，但全部采用以 SYS 开头的大写字母的变量除外，这些是系统变量。这些变量是您编辑和定义覆盖可能需要的文本对象，尤其是在默认值列显示对象没有值的情况下更是如此。

步骤 3 如果需要创建自己的 FlexConfig 对象，请确定需要哪些变量并创建关联对象。

您需要部署的 CLI 可能包含 IP 地址、接口名称、端口号以及以后可能需要调整的其他参数。这些变量已经与指向包含所需值的变量实现了最好的分隔。对于属于配置一部分，但以后可能会更改的字符串，您可能也需要变量。

此外，还要确定是否要为您将为其分配策略的每个设备使用不同的值。例如，您可能希望在三个设备上配置该功能，但可能需要为其中每个设备在给定命令上指定不同的接口名称或 IP 地址。如果需要为每个设备自定义对象，请确保在创建对象时启用覆盖，然后按设备定义覆盖值。

有关各种类型的变量的解释以及如何在需要时配置相关对象，请参阅下列主题。

- FlexConfig 变量， 第 1995 页
- FlexConfig 策略对象变量， 第 2000 页
- FlexConfig 系统变量， 第 2001 页
- 配置 FlexConfig 文本对象， 第 2016 页

步骤 4 如果使用预定义的 FlexConfig 对象，请编辑用作变量的文本对象。

请参阅配置 FlexConfig 文本对象， 第 2016 页。

步骤 5 （如有必要。）配置 FlexConfig 对象， 第 2012 页。

只有在预定义的对象无法创建对象时，您才需要执行此操作。

步骤 6 配置 FlexConfig 策略， 第 2018 页。

步骤 7 为 FlexConfig 策略设置目标设备， 第 2019 页。

还可以在创建策略时将策略分配给设备。策略必须至少有一个已分配的设备，您才能预览它。

步骤 8 预览 FlexConfig 策略， 第 2019 页。

必须先保存更改，才能预览策略。

验证所生成的命令是否是所预期的，以及所有变量是否都在正确解析。

步骤 9 在菜单栏中选择**部署 (Deploy)** > **部署 (Deployment)**。

步骤 10 选择分配给该策略的设备，然后点击**部署 (Deploy)**。

等待部署完成。

步骤 11 验证部署的配置， 第 2020 页。

步骤 12 （如有必要。）删除使用 FlexConfig 配置的功能， 第 2022 页。

与其他类型的策略不同，仅仅从一台设备取消分配 FlexConfig 可能不会删除相关的配置。如果要删除 FlexConfig 生成的配置，需要遵循上述程序。

如果您要删除某项功能，因为产品目前已支持该功能，另请参阅从 FlexConfig 转换为管理功能， 第 2023 页。

配置 FlexConfig 对象

使用 FlexConfig 对象定义要部署到设备的配置。每个 FlexConfig 策略由一个 FlexConfig 对象列表组成，因此这些对象实质上是由 Apache 速度脚本命令、ASA 软件配置命令和变量组成的代码模块。

有几个可以直接使用的预定义 FlexConfig 对象，或者如果需要编辑这些对象，可以制作对象副本。还可以从头创建自定义对象。FlexConfig 对象的内容可以是从一个简单的命令字符串到复杂 CLI 命令结构的任何内容，复杂CLI命令结构使用变量和脚本命令来部署其内容因设备或部署而异的命令。

还可以在定义 FlexConfig 策略时创建 FlexConfig 策略对象。

开始之前

记住以下几点：

- FlexConfig 对象转换为随后部署到设备的命令。这些命令已在全局配置模式下发出。因此，请不要将 **enable** 和 **configure terminal** 命令作为 FlexConfig 对象的一部分。
- 确定所需的变量类型，并创建所需的任何策略对象。编辑 FlexConfig 对象时，不能为变量创建对象。
- 确保您的命令与设备上的 VPN 或访问控制配置没有任何冲突。
- 如果接口有多组命令，只部署最后一组命令。因此，我们建议您不要使用开始和结束命令来配置接口。有关配置接口的示例，请参阅 ISIS_Interface_Configuration 预定义的 FlexConfig 对象。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择 **FlexConfig** > **FlexConfig 对象**。

步骤 3 执行以下操作之一：

- 点击**添加 FlexConfig 对象**以创建新对象。
- 点击 **编辑**（ ） 以编辑现有对象。
- 点击 **视图**（ ） 可查看预定义对象的内容。
- 如果要编辑预定义对象，请点击 **复制**（ ） 以创建具有相同内容的新对象。

步骤 4 为对象输入**名称**和（可选）说明

步骤 5 在对象正文区域中，输入生成所需配置的命令和说明。

对象内容是生成有效的 ASA 软件命令序列的脚本命令和配置命令序列。威胁防御设备使用 ASA 软件命令来配置某些功能。有关脚本和配置命令的详细信息，请参阅：

- 模板脚本，第 1995 页
- FlexConfig 对象中的 CLI 命令，第 1992 页

您可以使用变量来提供只有在运行时才知道的信息，或者每个设备都不同的信息。您只需键入处理变量，但必须使用**插入**菜单添加与策略对象或系统变量相关联的变量，或者是密钥的变量。有关变量的完整讨论，请参阅FlexConfig 变量，第 1995 页。

- 要插入系统变量，请选择**插入** > **插入系统变量** > **变量名称**。有关这些变量的详细说明，请参阅FlexConfig 系统变量，第 2001 页。
- 要插入策略对象变量，请选择**插入** > **插入策略对象** > **对象类型**，选择适当类型的对象。然后，为变量命名（可以与关联的策略对象同名），选择要与该变量关联的对象，然后点击**保存**。有关这些类型的详细说明，请参阅FlexConfig 策略对象变量，第 2000 页。有关过程的详细信息，请参阅向 FlexConfig 对象添加策略对象变量，第 2015 页。

- 要插入密钥变量，请选择**插入** > **密钥**并定义变量名称和值。有关过程的详细信息，请参阅配置密钥，第 2015 页。

注释 必须使用**插入**菜单来创建新的策略对象或系统变量。但是，对于该变量的后续使用，您必须键入该变量，包括 $。系统变量也是如此：第一次使用变量时，请从**插入**菜单中添加这些变量。然后，键入该变量以供后续使用。如果对系统变量多次使用**插入**菜单，系统变量将多次添加到变量列表中，FlexConfig 将无法验证，这意味着您无法保存更改。对于处理变量（与策略对象或系统变量不关联的变量），只需输入变量即可。如果要添加密钥，请始终使用**插入**菜单。密钥变量在变量列表中不显示。

步骤 6 选择部署频率和类型。

- **部署** - 将对象中的命令部署为**一次**还是**每次**。选择正确选项的唯一方法是测试部署结果。

  通过选择**每次**来开始操作。然后，在将对象附加到FlexConfig 策略后，部署配置。成功部署后，返回 FlexConfig 策略并预览其中一个已分配设备的配置，如预览 FlexConfig 策略，第 2019 页中所述。如果标记为 `###CLI generated from managed features ###` 的部分包含清除或否定对象中命令的命令，且 `###Flex-config Appended CLI ###` 部分包含重新配置此功能的命令，您便可以知道**每次**是正确的选项。

  即使没有看到否定命令，也需对设备配置进行一些细微更改，然后再运行另一个部署。如果成功完成部署，则可以检查部署脚本（请参阅验证部署的配置，第 2020 页）。如果您看到命令再次发出（即使它们已经配置）且没有出错，则可以保留**每次**选项。

  仅当系统在再次发出对象中的命令之前没有首先否定命令，或者部署导致出现特定于命令的错误时，才更改为**一次**。在某些情况下，系统不允许您发出已配置的命令，但这是例外情况。

  一些额外提示：

  - 如果 FlexConfig 对象指向系统托管对象，例如网络或 ACL 对象，请选择**每次**。否则，可能无法部署对象的更新。
  - 如果您在对象中执行的唯一操作是清除配置，请选择**一次**。然后，在下一次部署后从 FlexConfig 策略中删除此对象。

- **类型** - 选择以下一个选项：
  - **追加** -（默认值）。对象中的命令将放在从 管理中心 策略生成的配置的末尾。如果使用策略对象变量（指向从受管对象生成的对象），则必须使用追加。如果为其他策略生成的命令与对象中指定的指令重叠，则应选择此选项，以使您的命令不会被覆盖。这是最安全的选项。
  - **预置** - 对象中的命令放在从 管理中心 策略生成的配置的开始处。通常对清除或否定配置的命令使用预置。

步骤 7 （可选。）点击对象正文上方的 **验证** 以检查脚本的完整性。

点击**保存**时始终验证该对象。无法保存无效对象。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

向 FlexConfig 对象添加策略对象变量

可以向与其他类型的策略对象相关联的 FlexConfig 策略对象中插入变量。在将 FlexConfig 部署到某一设备后，这些变量将解析到相关联对象的名称或内容。

对于首次在 FlexConfig 对象中使用策略对象变量，可以使用以下程序。如果需要再次引用该对象，则请键入该变量（包括 $ 符号）。要了解如何使用这些变量，请参阅如何处理变量，第 1996 页。

过程

步骤 1 依次选择**插入** > **插入策略对象** > **对象类型**，选择适当类型的对象。

步骤 2 输入变量的名称和说明（后者为可选项）。

该名称在 FlexConfig 对象的上下文中必须是唯一的。其中不能包含空格。允许使用跟与变量相关联的对象完全相同的名称。

步骤 3 选择要与变量相关联的对象，然后点击**添加**，以将其移至**选定对象**列表中。

只能使一个变量与一个对象相关联。

注释 对于文本对象，可以根据需要选择任何预定义对象。不过，很多此类对象没有默认值。必须更新这些对象，以直接或以覆盖方式，为将要向其部署 FlexConfig 对象的设备添加所需的值。尝试在不更新这些对象的情况下部署 FlexConfig，通常会导致部署错误。

步骤 4 点击**保存 (Save)**。

该变量将显示在位于 FlexConfig 对象编辑器底部的“变量”列表中。

配置密钥

密钥是要屏蔽其内容的任何单字符串变量，如密码。系统为这些变量提供特殊处理，以帮助您防止敏感信息的散播。

密钥变量不会显示在 FlexConfig 对象中的“变量”列表中。

使用以下过程在 FlexConfig 对象中创建、插入以及以其他方式管理密钥变量。与其他类型的变量不同，您可以在每次需要插入给定的密钥变量时使用**插入**命令。在处理方面，这些变量的行为类似于单值文本对象变量；请参阅单值变量，第 1996 页。

注释 在密钥变量中定义的任何数据都将对用户屏蔽，预览 FlexConfig 策略时除外。此外，如果导出 FlexConfig 策略，则会删除任何密钥变量的内容。导入策略时，需要手动编辑每个密钥变量以输入数据。

过程

步骤 1 编辑 FlexConfig 策略对象时，请选择**插入** > **密钥**。

步骤 2 在“插入密钥”对话框中，执行以下任一操作：

- 要创建新密钥，请点击**添加密钥**，然后填写以下信息并点击**添加**。
  - **密钥名称** - 变量的名称。此名称显示在 FlexConfig 对象中，以 @ 为前缀。
  - **密码**、**确认密码** - 密钥字符串，在键入时用星号进行隐蔽。
- 要在 FlexConfig 对象中插入一个密钥变量，请选中该变量对应的复选框。
- 要编辑密钥变量的值，请点击该变量的 **编辑**（ ）。进行更改并点击**添加**。
- 要删除密钥变量，请点击该变量的 **删除**（ ）。

步骤 3 点击**保存 (Save)**。

配置 FlexConfig 文本对象

将 FlexConfig 对象中的文本对象用作策略对象变量的目标。您可以使用变量来提供只能在运行时获悉或是可能因设备不同而异的信息。在部署过程中，指向文本对象的变量将替换为文本对象的内容。

文本对象可以包含自由格式的字符串，可以是关键字、接口名称、数字、IP 地址等等。内容取决于您在 FlexConfig 脚本中使用这些信息的方式。

在创建或编辑文本对象之前，请准确确定需要的内容。这包括您打算如何处理对象，这将有助于您在创建单字符串或多字符串对象之间做出决定。阅读以下主题：

- FlexConfig 变量， 第 1995 页
- 如何处理变量， 第 1996 页

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择 **lexConfig** > **文本对象**。

步骤 3 执行以下操作之一：

- 点击**添加文本对象**以创建一个新对象。
- 点击 **编辑**（ ） 以编辑现有对象。您可以编辑预定义的文本对象，如果您打算使用预定义的 FlexConfig 对象，则需要这样做。

步骤 4 为对象输入**名称**和（可选）说明。

步骤 5 （仅新对象。）从下拉列表中选择**变量类型**：

- **单个** - 如果对象应包含单个文本字符串。
- **多个** - 如果对象应包含文本字符串列表。

保存对象后，则无法更改变量类型。

步骤 6 如果变量类型为**多个**，则使用向上和向下箭头指定**计数**。

在更改数字时，会在对象中添加或删除行。

步骤 7 向对象添加内容。

您可以在变量号旁边的文本框中点击并键入一个值，也可以为每个将被分配使用此文本对象的 FlexConfig 对象的设备设置设备覆盖。您也可以同时执行这两种方法，在这种情况下，在基本对象中配置的值在给定设备的覆盖不存在的情况下充当默认值。

在编辑预定义对象时，最好使用设备覆盖，这样，对于可能需要在不同 FlexConfig 策略中使用该对象的其他用户来说，系统默认值仍然存在。您所采取的方法取决于组织的要求。

提示 某些预定义对象需要多个值，其中每个值都有特定的用途。仔细阅读说明文本以确定对象中的预期值。在某些情况下，这些说明指定您必须使用覆盖而不是更改基本值。如果是 enableInspectProtocolList，您将无法进入其检测与 Snort 检查不兼容的协议。

如果决定使用覆盖，请执行以下操作。

a) 选择**允许覆盖 (Allow Overrides)**。
b) 展开“覆盖”区域（如果需要），然后点击**添加**。

如果设备已存在覆盖，请点击该覆盖的编辑以更改它。

c) 在“添加对象覆盖”对话框的 **目标** 卡上，选择要为其定义值的设备，然后点击 **添加** 将其移动到“选定设备”列表中。
d) 点击 **覆盖**，根据需要调整 **计数** ，然后在变量字段中点击并键入设备的值。
e) 点击**添加 (Add)**。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 如果活动策略引用您的对象，则部署配置会更改 中的部署配置更改。

配置 FlexConfig 策略

FlexConfig 策略包含 FlexConfig 对象的两个有序列表，一个预置列表和一个附加列表。有关对预置/附加的解释，请参阅配置 FlexConfig 对象，第 2012 页。

FlexConfig 策略是可以分配给多个设备的共享策略。

过程

步骤 1 选择**设备** > **FlexConfig**。

步骤 2 执行以下操作之一：

- 点击**新建策略**创建新的 FlexConfig 策略。系统将提示您输入名称。（可选）选择“可用设备”列表中的设备，然后点击**添加到策略**以分配设备。点击**保存 (Save)**。
- 点击 **编辑**（ ） 以编辑现有策略。可以通过在编辑模式下点击名称或说明来对其进行更改。
- 点击 **复制**（ ）以创建具有相同内容的新策略。系统将提示您输入名称。系统不会为副本保留设备分配。
- 点击删除可删除不再需要的策略。

步骤 3 从**可用 FlexConfig** 列表中选择策略所需的 FlexConfig 对象，然后点击 > 将它们添加到策略中。

对象将根据 FlexConfig 对象中指定的部署类型自动添加到预置或附加列表中。

要删除所选对象，请点击对象旁边的 **删除**（ ） 。

步骤 4 对于每个所选对象，点击该对象旁边 **视图**（ ） 可以标识该对象中使用的变量。

除了系统变量（从 SYS 开始），您需要确保与变量关联的对象不为空。在它们之间没有任何内容的空白或方括号 [] 表示空对象。在部署策略之前，您需要编辑这些对象。

注释 如果使用对象覆盖，则这些值不会显示在此视图中。因此，空的默认值不一定表示您没有使用所需的值更新对象。预览配置将显示变量是否对给定设备正确解析。请参阅预览 FlexConfig 策略，第 2019 页。

步骤 5 点击**保存 (Save)**。

下一步做什么

- 设置策略的目标设备；请参阅为 FlexConfig 策略设置目标设备，第 2019 页。
- 部署配置更改。

为 FlexConfig 策略设置目标设备

创建FlexConfig策略时，可以选择使用该策略的设备。您可以随后更改策略的设备分配，如下所述。

注释 通常，当您从设备取消分配策略时，系统会在下次部署时自动删除关联的配置。但是，由于FlexConfig对象是用于部署自定义命令的脚本，因此只从设备取消分配 FlexConfig 策略不会删除由 FlexConfig 对象配置的命令。如果您打算从设备配置中删除FlexConfig生成的命令，请参阅删除使用 FlexConfig 配置的功能，第 2022 页。

过程

步骤 1 选择**设备** > **FlexConfig** 并编辑 FlexConfig 策略。

步骤 2 点击**策略分配**。

步骤 3 在 **目标设备** 上，建立目标列表：

- 添加 - 选择一个或多个**可用设备**，然后点击**添加到策略**或拖放到**所选设备**列表。可以将策略分配给设备、高可用性对和群集设备。
- 删除 - 点击单个设备旁边的 **删除**（ ），或选择多个设备，点击右键，然后选择 **删除选择**。

步骤 4 点击**确定**，保存选择。

步骤 5 点击**保存**以保存 FlexConfig 策略。

下一步做什么

- 部署配置更改。

预览 FlexConfig 策略

预览 FlexConfig 策略可以查看 FlexConfig 对象如何转换为 CLI 命令。预览将显示从 FlexConfig 对象中使用的脚本和变量为选定设备生成的命令。这些变量基于设备的配置进行解析，因此您可以清楚地了解将部署什么。

使用预览可以查找 FlexConfig 对象中存在的潜在问题。更正对象，直到预览显示预期结果为止。

您必须单独预览每个设备的配置，因为这些变量可以基于设备配置进行不同的解析。

过程

步骤 1 选择**设备** > **FlexConfig** 并编辑 FlexConfig 策略。

步骤 2 如果有任何待保存的更改，请点击**保存**。

预览仅显示最近保存的策略版本中的那些 FlexConfig 对象的结果。必须保存策略才能查看新添加对象的预览。

步骤 3 点击**预览配置**。

步骤 4 从**选择设备**下拉列表中选择设备。

系统从设备和配置的策略中检索信息，并确定将在下次部署到设备时生成哪些 CLI 命令。您可以选择输出并使用 Ctrl+C 将其复制到剪贴板，您可以再次将其粘贴到文本文件中以进行进一步分析。

预览包括以下部分：

- Flex-config 预置 CLI - 这些是由 FlexConfigs 生成、的命令，这些命令。
- 从托管功能生成的CLI - 这些是为在管理中心中配置的策略生成的命令。自上次成功部署到设备后，系统将为新的或更改的策略生成命令。这些命令并不代表实现分配的策略所需的所有命令。本部分中的任何命令都不是从 FlexConfig 对象中生成。
- Flex-config 附加 CLI - 这些是由 FlexConfigs 生成、将被附加到配置的命令。

步骤 5 点击**关闭**以关闭预览对话框。

验证部署的配置

在将 FlexConfig 策略部署到设备后，请验证部署是否成功，以及得到的配置是否是您所预期的。此外，请验证设备是否按预期工作。

过程

步骤 1 要验证部署是否成功，请执行以下操作：

a) 点击菜单栏中的 **系统状态**，即 **部署** 和 **系统** 之间的未命名。

该图标看起来像以下图标中的一个，如果有错误，它可能会包括数字：

- **指示无警告** - 指示系统上不存在任何警告或错误。
- 指示 **一个或多个警告** - 指示系统上存在一个或多个警告而没有错误。
- **指示一个或多个错误** - 指示系统上存在一个或多个错误和任意数量的警告。

b) 在 **部署**上，验证部署是否成功。

c) 要查看更多详细信息，特别是对于失败的部署，请点击**显示历史记录**。

d) 在左侧列的作业列表中选择部署作业。

作业以倒序顺序列出，最近的作业位于列表顶部。

e) 在右侧列中点击设备的 **脚本** 列中的下载。

部署脚本包括发送到设备的命令以及从该设备返回的任何响应。这些响应可以是信息性消息或错误消息。对于失败的部署，请查找指示您通过FlexConfig发送的命令错误的消息。这些错误可帮助您纠正尝试配置这些命令的 FlexConfig 对象中的脚本。

注释 为托管功能发送的命令与从 FlexConfig 策略生成的命令之间没有显著差异。

例如，以下序列显示 管理中心 发送了命令来为 GigabitEthernet0/0 配置外部逻辑名。设备的响应是自动将安全级别设置为0。威胁防御 不会将安全级别用于任何操作。与FlexConfig相关的消息在该脚本的“CLI 应用”部分中。

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

步骤 2 验证部署的配置是否包含预期的命令。

您可以通过与设备的管理 IP 地址建立 SSH 连接来完成此项工作。使用 **show running-config** 命令查看配置。

或者，在 Cisco Secure Firewall Management Center中使用 CLI 工具。

a) 选择**系统** > **运行状况** > **监控**，然后点击设备名称。

您可能需要点击状态表中**计数**列中的打开/关闭箭头来查看任何设备。

b) 点击**高级故障排除**。
c) 点击 **威胁防御 CLI**。
d) 选择 **show** 作为命令，然后键入 **running-config** 作为参数。
e) 点击**执行 (Execute)**

正在运行的配置显示在文本框中。您可以选择配置并按Ctrl+C，然后将其粘贴到文本文件中以供以后分析。

步骤 3 验证设备是否按预期工作。

使用与此功能相关的**show**命令可查看详细信息和统计信息。例如，如果您启用了其他协议检查，则**show service-policy** 命令会提供此信息。要使用的确切命令与功能相关，并且应在您用来了解如何配置此功能的 ASA 配置指南和命令参考中提及。

如果显示统计信息的命令指示数字未发生更改（例如，命中次数、连接计数等），则配置可能有效，但没有意义。如果您知道流量正在通过应在统计中显示的设备，则查找配置中缺少的内容。例如，NAT 或访问规则可能需要丢弃或更改流量，才能对其应用此功能。

您可以从 SSH 会话或通过 管理中心 CLI 工具使用 **show** 命令。

但是，如果您需要使用的 **show** 命令无法直接从 威胁防御 CLI 中获得，则需要与设备建立 SSH 连接才能使用这些命令。在 CLI 中，输入以下命令序列以在诊断 CLI 中进入特权 EXEC 模式。您可以在此处输入这些不受支持的 **show** 命令。

```
> system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password: <press enter, do not enter a password>
firepower#
```

删除使用 FlexConfig 配置的功能

如果您决定需要删除使用 FlexConfig 配置的一组配置命令，则可能需要手动删除该配置。从设备取消分配 FlexConfig 策略可能不会删除所有配置。

要手动删除该配置，请创建新的 FlexConfig 对象以清除或取消配置命令。

开始之前

要确定是否需要手动删除对象生成的部分或全部配置，请执行以下操作：

1. 检查配置预览，如预览 FlexConfig 策略，第 2019 页中所述。如果 `###CLI generated from managed features ###` 部分包含清除或否定命令以删除 FlexConfig 对象中的所有命令，您只需从 FlexConfig 策略中删除此对象，保存并重新部署。
2. 从 FlexConfig 策略中删除对象，保存更改，然后再次预览配置。如果 `###CLI generated from managed features ###` 部分仍不包含所需的清除或否定命令，则必须按照此程序手动删除配置。

过程

步骤 1 要以清除或取消配置命令，选择**对象** > **对象管理**并创建 FlexConfig 对象。

如果某个功能具有可以删除所有配置设置的 **clear** 命令，则使用此命令。例如，预定义的 ISIS_Unconfigure_All 对象就包含一个可以删除所有与 ISIS 相关的配置命令的命令：

```
clear configure router isis
```

如果此功能没有 **clear** 命令，则需要使用每个要删除的命令的 **no** 形式。例如，预定义的 Sysopt_basic_negate 对象将删除通过预定义的 Sysopt_basic 对象配置的命令。

```
no sysopt traffic detailed-statistics

no sysopt connection timewait
```

通常，您将配置一个 FlexConfig 对象，以预置的一次性部署对象形式删除配置。

步骤 2 选择**设备** > **FlexConfig**并创建新的 FlexConfig 策略或编辑现有策略。

如果要保留部署配置命令的 FlexConfig 策略，请创建一个专门用于取消命令的新策略，并将设备分配给该策略。然后，将新的 FlexConfig 对象添加到该策略。

如果要从所有设备中完全删除 FlexConfig 配置对象，只需从现有 FlexConfig 策略中删除这些命令，并将它们替换为取消该配置的对象。

步骤 3 点击**保存**以保存 FlexConfig 策略。

步骤 4 点击**预览配置**并确认清除和取消命令会正确生成。

步骤 5 选择菜单栏中的 **部署** > **部署** ，选择该设备，然后点击 **部署**。

等待部署完成。

步骤 6 验证是否已删除命令。

查看设备上正在运行的配置，以确认这些命令已被删除。有关详细信息，请参阅验证部署的配置，第 2020 页。

步骤 7 编辑 FlexConfig 策略时，点击**策略分配**并删除该设备。（可选）从策略中删除 FlexConfig 对象。

假定 FlexConfig 策略仅删除不需要的配置命令，则在删除完成后无需保留分配给该设备的策略。

但是，如果 FlexConfig 策略保留了您仍希望在设备上配置的选项，请从策略中删除取消对象。不再需要保留它们。

从 FlexConfig 转换为管理功能

每个软件版本都会向产品添加托管功能，也就是您通过在 FlexConfig 外部控制的策略直接配置的功能。这可能会弃用您当前使用的 FlexConfig 命令；您的配置不会自动转换。在升级后，您无法使用新近弃用的命令来分配或创建 FlexConfig 对象。在升级软件后，检查 FlexConfig 策略和对象。

在使用 FlexConfig 配置的功能开始受支持作为托管功能时，您必须从使用 FlexConfig 转换为使用受管功能。在大多数情况下，您现有的 FlexConfig 配置会在升级后继续工作，您仍然可以进行部署。但在某些情况下，使用已弃用的命令可能会导致部署问题。不支持同时在 GUI 和 FlexConfig 中配置功能。

过程

步骤 1 删除 FlexConfig，如删除使用 FlexConfig 配置的功能，第 2022 页中所述。

步骤 2 配置最新支持的托管功能中的设置。

版本说明包含了该版本的新功能列表。

FlexConfig 示例

以下是使用 FlexConfig 的一些示例。

如何配置精确时间协议 (ISA 3000)

精确时间协议 (PTP) 是一种时间同步协议，用于在基于数据包的网络中同步各种设备的时钟。这些设备时钟通常具有不同的精度和稳定性。该协议专为工业联网测量和控制系统设计，而且最适合用于分布式系统，因为其需要极少的带宽和处理开销。

PTP 系统是一个分布式联网系统，包含 PTP 设备和非 PTP 设备的组合。PTP 设备包含常见的时钟、边界时钟和透明时钟。非 PTP 设备包含网络交换机、路由器和其他基础设施设备。

可以将 FTD 设备配置为透明时钟。FTD 设备不会将其时钟与 PTP 时钟同步。FTD 设备将使用 PTP 默认配置文件，如 PTP 时钟上所定义。

配置 PTP 设备时，需要为要一起运行的设备定义一个域编号。因此，可以配置多个 PTP 域，然后将每个非 PTP 设备配置为特定域使用 PTP 时钟。

开始之前

确定设备应使用的 PTP 时钟上配置的域编号。此示例假定 PTP 域编号为 10。另外，确定系统可通过哪些接口到达域中的 PTP 时钟。

以下是 PTP 配置准备：

- 此功能在思科 ISA 3000 设备上不可用。
- 思科 PTP 仅支持组播 PTP 消息。
- PTP 仅可用于 IPv4 网络，不可用于 IPv6 网络。
- 物理以太网数据接口支持 PTP 配置，无论是独立式还是网桥组成员。管理接口、子接口、Etherchannel 接口、桥接虚拟接口 (BVI) 或任何其他虚拟接口均不支持此版本。
- 假如父接口上具有适当的 PTP 配置，则支持 VLAN 子接口上的 PTP 流。
- 必须确保允许 PTP 数据包通过设备。PTP 流量由 UDP 目标端口 319 和 320 以及目标 IP 地址 224.0.1.129 标识，因此允许此流量的任何访问控制规则均应有效。
- 在路由防火墙模式下，必须为 PTP 组播组启用组播路由：此外，如果启用 PTP 的接口**不**在网桥组中，则必须将该接口配置为加入 IGMP 组播组 224.0.1.129。如果物理接口是网桥组成员，则不要将其配置为加入 IGMP 组播组。

过程

步骤 1 （仅路由模式。）启用组播路由，并为接口配置 IGMP 组。

在路由模式下，必须启用组播路由。此外，对于独立物理接口（即非网桥组成员），还必须配置接口以加入 224.0.1.129 IGMP 组。您无法将网桥组成员配置为加入 IGMP 组，但网桥组成员上的 PTP 配置将在没有 IGMP 加入的情况下起效。

对要配置 PTP 的每台设备执行此程序。

注释 记下每个设备上每个面向 PTP 时钟的接口的硬件名称，例如，GigabitEthernet1/1。

a) 选择**设备 (Devices)** > **设备管理 (Device Management)**，并且编辑设备。
b) 点击**路由**。
c) 选择**组播路由 (Multicast Routing)** > **IGMP**。
d) 选中**启用组播路由 (Enable Multicast Routing)** 复选框。
e) 点击**加入组 (Join Group)**。
f) 点击**添加 (Add)**，，然后在添加 IGMP 加入组参数对话框中，配置以下选项，然后点击**确定 (OK)**。

- **接口 (Interface)** - 选择面向 PTP 时钟的独立接口。
- **加入组 (Join Group)** - 点击 **+** 以添加新的网络对象。使用地址 224.0.1.129 来创建主机对象。在配置其他接口时，可直接选择此对象。

对设备上每个面向 PTP 时钟的独立接口重复此步骤。

g) 点击“路由”(Routing) 页面上的**保存 (Save)**。

步骤 2 创建 FlexConfig 对象，以便全局启用 PTP 以及在接口上启用 PTP。

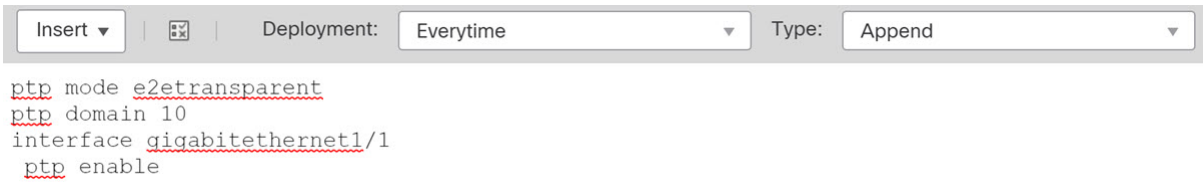
以下程序假定您正在配置的每台设备上的面向 PTP 时钟的接口均相同。如果在不同的设备上使用了不同的接口，则您需要为每个不同的组合创建单独的对象。例如，如果您在设备 A 和 B 上使用 GigabitEthernet1/1，在设备 C 和 D 上使用 GigabitEthernet1/2，在设备 E 和 F 上同时使用 GigabitEthernet1/1 和 1/2，则您需要 3 个单独的 FlexConfig 对象，随后还需要 3 个单独的 FlexConfig 策略（将在下一步中进行说明）。

a) 选择**对象 (Object)** > **对象管理 (Object Management)**。
b) 从目录中选择 **FlexConfig** > **FlexConfig 对象 (FlexConfig Object)**。
c) 点击**添加 FlexConfig 对象 (Add FlexConfig Object)**，配置以下属性，然后点击**保存 (Save)**。

- **Name** - 对象名称。例如，Enable_PTP。
- **部署 (Deployment)** - 选择**每次 (Everytime)**。您想在每个部署中发送此配置，以确保其保持配置状态。
- **类型 (Type)** - 保留默认值**附加 (Append)**。这些命令会在直接支持的功能的命令之后被发送到设备。这样可确保在这些命令之前配置对接口配置所做的任何其他更改。
- **对象正文 (Object body)** - 在对象正文中，键入在每个面向 PTP 时钟的接口上全局配置 PTP 所需的命令。例如，PTP 域 10 的全局配置和 GigabitEthernet1/1 上的接口配置所需的命令如下：

```
ptp mode e2etransparent
ptp domain 10
interface gigabitethernet1/1
 ptp enable
```

此对象正文应如下所示：



步骤 3 创建 FlexConfig 策略并将其分配给设备。

如果为面向 PTP 时钟的接口的不同组合创建了多个 FlexConfig 对象，则需要为每个对象创建单独的 FlexConfig 策略，并根据需要配置的接口将这些策略分配给正确的设备。对每组设备重复以下程序。

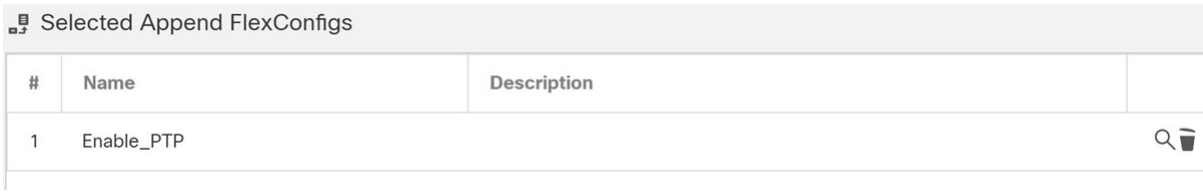
a) 选择**设备** > **FlexConfig**。

b) 点击**新建策略 (New Policy)**，或者如果现有 FlexConfig 策略应分配给（或已分配给）目标设备，则只需编辑该策略。

在创建新的策略时，请在为策略命名的对话框中将目标设备分配给策略。

c) 在目录的 **User Defined** 文件夹中选择 PTP FlexConfig 对象，然后点击 > 将其添加到策略中。

此对象应被添加到**所选附加 Flexconfig (Selected Appended FlexConfigs)** 列表中。



d) 点击**保存 (Save)**。

e) 如果尚未将所有目标设备分配给策略，请点击“保存”(Save)下面的**策略分配 (Policy Assignments)** 链接并立即进行分配。

f) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择一个已分配的设备。

系统会生成将被发送到设备的配置 CLI 预览。验证从 PTP FlexConfig 对象生成的命令看起来是否正确。这些将在预览结束时显示。请注意，您还会看到通过对托管功能所做的其他更改而生成的命令。对于 PTP 命令，您应该会看到类似如下的内容：

```
###Flex-config Appended CLI ###
ptp mode e2etransparent
ptp domain 10
interface gigabitethernet1/1
 ptp enable
```

步骤 4 部署更改。

由于您已将 FlexConfig 策略分配给设备，因此您始终会收到部署警告，以提醒您有关 FlexConfig 的使用。点击**继续 (Proceed)** 以继续部署。

在部署完成后，您可以检查部署历史记录并查看部署脚本。如果部署失败，这一点尤为重要。请参阅验证部署的配置，第 2020 页。

步骤 5 在每台设备上验证 PTP 配置。

从 SSH 或控制台会话到每台设备，验证 PTP 设置：

```
> show ptp clock
 PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
> show ptp port
 PTP PORT DATASET: GigabitEthernet1/1
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 1
  PTP version: 2
  Port state: Enabled

 PTP PORT DATASET: GigabitEthernet1/2
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 2
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/3
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 3
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/4
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 4
  PTP version: 2
  Port state: Disabled
```

如何对电源故障配置自动硬件旁路 (ISA 3000)

您可以启用硬件旁路，使流量在断电期间继续在接口对之间流动。支持的接口对为铜缆接口 GigabitEthernet 1/1 和 1/2 以及 GigabitEthernet 1/3 和 1/4。如果您使用的是光纤以太网型号，则只有铜缆以太网对（GigabitEthernet 1/1 和 1/2）支持硬件旁路。

启用硬件旁路时，流量将在这些接口对之间的第 1 层传递。FTD CLI 会显示接口处于关闭状态。不使用防火墙功能，因此请确保您了解允许流量通过设备的风险。

在 CLI 控制台或 SSH 会话中，使用 **show hardware-bypass** 命令以监控运行状态。

开始之前

要使用硬件旁路：

- 必须将接口对放置在同一网桥组内。
- 必须将接口连接到交换机的接入端口。不能将它们连接到中继端口。

我们建议您通过使用附加到分配给设备的访问控制策略的威胁防御服务策略，来全局禁用 TCP 序列号随机化。默认情况下，ISA 3000 会将通过其的 TCP 连接的初始序列号 (ISN) 重写为随机编号。硬

件旁路激活后，ISA 3000 不再位于数据路径中，也不再转换序列号。接收客户端会收到意外序列号，并丢弃连接，因此需要重新建立 TCP 会话。即便禁用 TCP 序列号随机化后，某些 TCP 连接将也需要重新建立，因为链路在切换期间会临时关闭。

过程

步骤 1 创建 FlexConfig 对象以启用自动旁路。

a) 选择**对象** > **对象管理**。

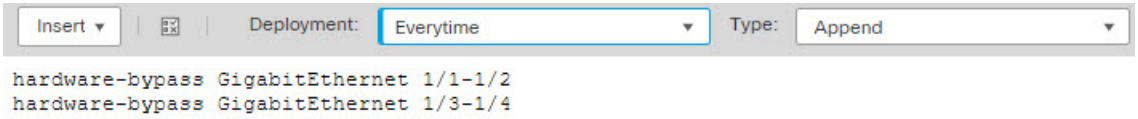
b) 从目录中选择 **FlexConfig** > **FlexConfig 对象 (FlexConfig Object)**。

c) 点击**添加 FlexConfig 对象 (Add FlexConfig Object)**，配置以下属性，然后点击**保存 (Save)**。

- **Name** - 对象名称。例如，Enable_HW-Bypass。
- **部署 (Deployment)** - 选择**每次 (Everytime)**。您想在每个部署中发送此配置，以确保其保持配置状态。
- **类型 (Type)** - 保留默认值**附加 (Append)**。这些命令会在直接支持的功能的命令之后被发送到设备。
- **对象正文 (Object body)** - 在对象正文中，键入启用自动硬件旁路所需的命令。例如，两个可能的接口对所需的命令：

```
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

此对象正文应如下所示：



步骤 2 创建 FlexConfig 策略并将其分配给设备。

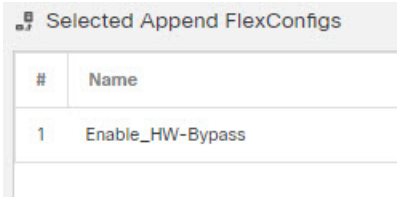
a) 选择**设备 (Devices)** > **FlexConfig**。

b) 点击**新建策略 (New Policy)**，或者如果现有 FlexConfig 策略应分配给（或已分配给）目标设备，则只需编辑该策略。

在创建新的策略时，请在为策略命名的对话框中将目标设备分配给策略。

c) 在目录的 **User Defined** 文件夹中选择硬件旁路 FlexConfig 对象，然后点击 **>** 将其添加到策略中。

此对象应被添加到**所选附加 Flexconfig (Selected Appended FlexConfigs)** 列表中。



d) 点击**保存 (Save)**。

e) 如果尚未将所有目标设备分配给策略，请点击“保存”(Save)下面的**策略分配 (Policy Assignments)**链接并立即进行分配。

f) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择一个已分配的设备。

系统会生成将被发送到设备的配置 CLI 预览。验证从硬件旁路 FlexConfig 对象生成的命令看起来是否正确。这些将在预览结束时显示。请注意，您还会看到通过对托管功能所做的其他更改而生成的命令。对于硬件旁路命令，您应该会看到类似如下的内容：

```
###Flex-config Appended CLI ###
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

步骤 3 部署更改。

由于您已将 FlexConfig 策略分配给设备，因此您始终会收到部署警告，以提醒您有关 FlexConfig 的使用。点击**继续 (Proceed)** 以继续部署。

在部署完成后，您可以检查部署历史记录并查看部署脚本。如果部署失败，这一点尤为重要。请参阅验证部署的配置，第 2020 页。

下一步做什么

如果您要手动调用硬件旁路或手动将其关闭，则需要创建两个 FlexConfig 对象：

- 一个是手动启动绕行，其中包含以下一个或两个命令，具体取决于您是否要为两个对调用绕行：

```
hardware-bypass manual GigabitEthernet 1/1-1/2
hardware-bypass manual GigabitEthernet 1/3-1/4
```

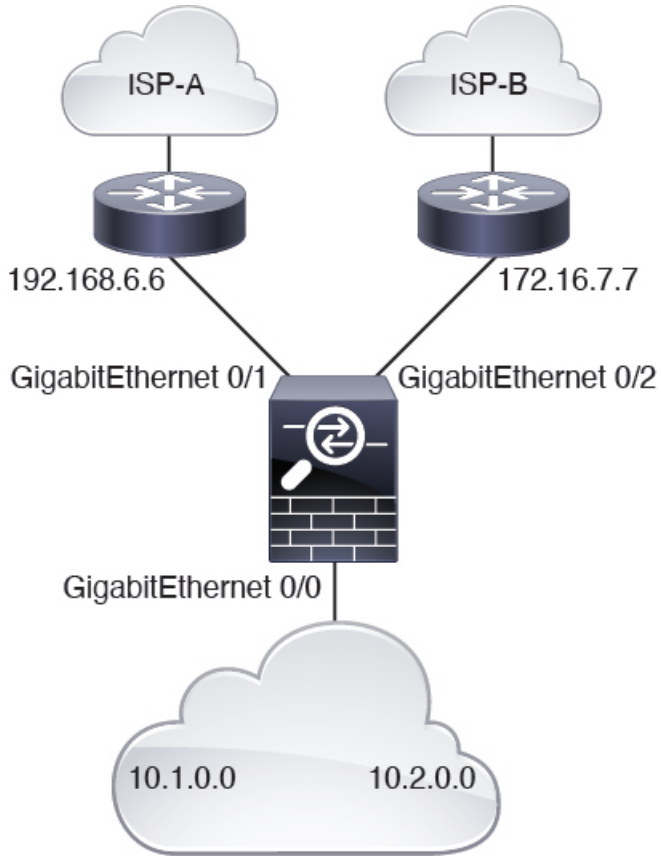
- 另一个是手动关闭旁路，其中包含以下一个或两个命令：

```
no hardware-bypass manual GigabitEthernet 1/1-1/2
no hardware-bypass manual GigabitEthernet 1/3-1/4
```

然后，您需要将一个或另一个对象添加到 FlexConfig 策略中并部署更改，以打开或关闭绕行。您还需要在部署后立即从 FlexConfig 策略中删除该对象。如果您手动调用绕行，则需要重复该过程以再次将其关闭。因此，使用此手动方法需要经常仔细编辑 FlexConfig 策略和其他部署。

如何配置策略型路由

您可以使用 FlexConfig 来实施策略型路由 (PBR) 功能。例如，下图显示了如何根据源 IP 地址在网络之间实现流量负载均衡。在这种情况下，我们将假设 10.1.0.0/16 网络生成高优先级流量，这些流量应通过较高带宽的链路传输到 ISP-A，而 10.2.0.0/16 的优先级较低，应通过较慢、较低的流量传输到 ISP-B 的带宽链路。



开始之前

此程序假定您已按如下方式来配置接口：

- GigabitEthernet0/0。
  - 接口名称：inside
  - IP 地址：10.1.1.1/24
  - 请注意，网络中的其他路由器会使用该接口作为 10.1.0.0/16 和 10.2.0.0/16 地址空间路由的网关。
- GigabitEthernet0/1。
  - 接口名称：outside-1
  - IP 地址：192.168.6.5/24
- GigabitEthernet0/2。
  - 接口名称：outside-2
  - IP 地址：172.16.7.6/24

过程

步骤 1 创建扩展 ACL 对象，以便匹配来自 10.1.0.0/16 和 10.2.0.0/16 地址空间的流量。您必须创建单独的 ACL，因为您将对路由映射中的流量应用不同的操作。

a) 选择**对象** > **对象管理**。

b) 从目录中选择**访问列表 (Access List)** > **扩展 (Extended)**。您必须配置扩展访问列表以便指定流量源地址。

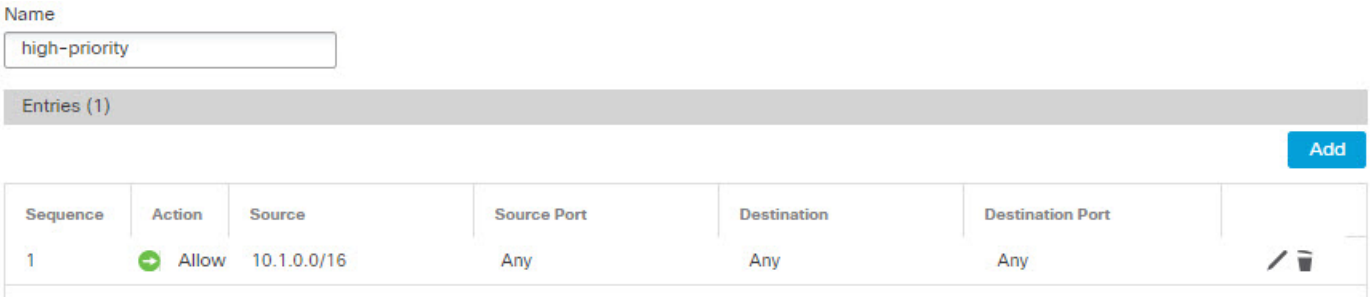
c) 点击**添加扩展访问列表**按钮。

d) 输入访问列表的名称，例如 **high-priority**。

e) 点击**添加 (Add)** 按钮，并为高优先级地址空间创建规则。主要特征如下：

- **操作** - **允许**。
- **源网络 (Source Networks)** - 在列表下方的编辑框中输入 10.1.0.0/16，然后点击**添加 (Add)**。或者，您可以为此网络地址定义网络对象。

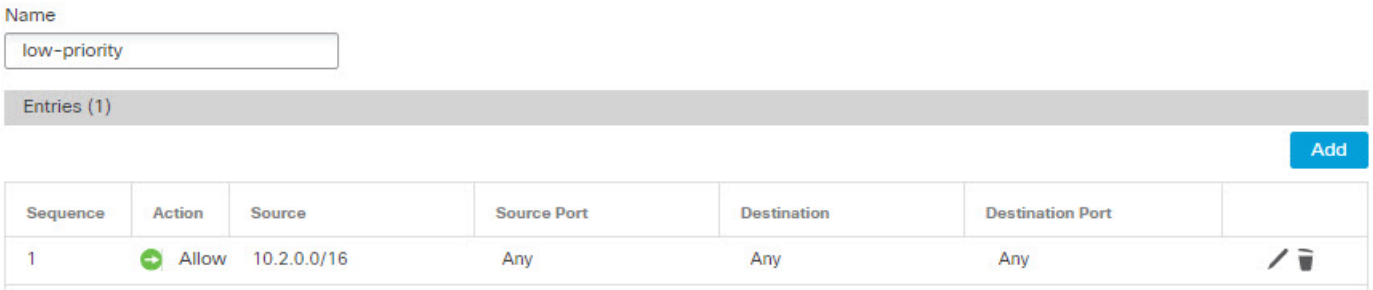
f) 点击对话框底部的**添加 (Add)**。这样会将规则添加到访问列表。



g) 点击**保存 (Save)**。

h) 重复此过程，以便使用以下属性来创建第二个访问列表：

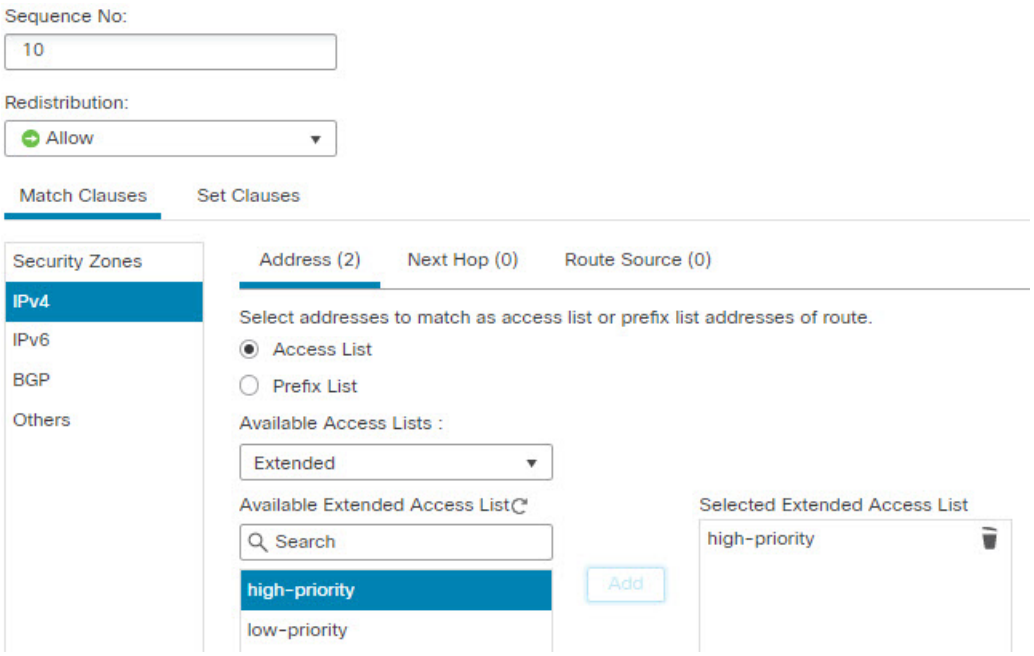
- **名称 (Name)** - **低优先级**。
- **操作** - **允许**。
- **源网络 (Source Networks)** - 在列表下方的编辑框中输入 10.2.0.0/16，然后点击**添加 (Add)**。或者，您可以为此网络地址定义网络对象。



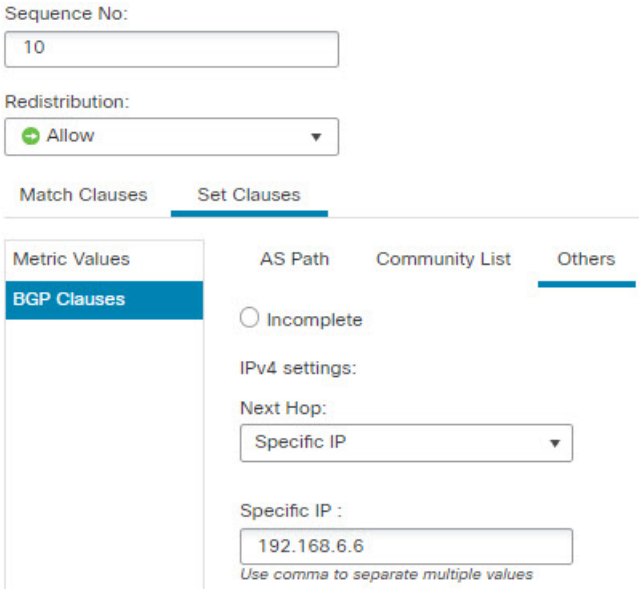
步骤 2 创建用于定义这些地址空间的下一跳地址的路由映射。

a) 仍在对象页面上时，点击目录中的**路由映射 (Route Map)**。
b) 点击**添加路由映射 (Add Route Map)** 按钮。
c) 输入对象的名称，例如 **load-balance**。
d) 点击**添加 (Add)** 并使用以下属性为高优先级流量创建规则：

- **序列号 (Sequence No.)** —**10**。
- **重新分配 (Redistribution)** - **允许 (Allow)**。
- **匹配子句 (Match Clauses)** > **IPv4** > **地址 (Address)** - 选择**访问列表 (Access List)** 单选按钮，然后选择**可用访问列表 (Available Access Lists)** > **扩展 (Extended)**，并将高优先级 ACL 移至所选列表。



- **设置子句 (Set Clauses)** > **BGP 子句 (BGP Clauses)** > **其他 (Others)**- 在 **IPv4 设置 (IPv4 Settings)** > **下一跳 (Next Hop)** 中，选择**特定 IP (Specific IP)**，然后将 ISP-A 的网关 **192.168.6.6** 输入**特定 IP (Specific IP)** 编辑框中。



e) 点击**添加 (Add)**，将规则添加到路由映射。

f) 点击**添加 (Add)** 并使用以下属性为低优先级流量创建规则：

- **序列号- 20**。
- **重新分配 (Redistribution)** - **允许 (Allow)**。
- **匹配子句 (Match Clauses)** > **IPv4** > **地址 (Address)** - 选择**访问列表 (Access List)** 单选按钮，然后选择**可用访问列表 (Available Access Lists)** > **扩展 (Extended)**，并将低优先级 ACL 移至所选列表。
- **设置子句 (Set Clauses)** > **BGP 子句 (BGP Clauses)** > **其他 (Others)**- 在 **IPv4 设置 (IPv4 Settings)** > **下一跳 (Next Hop)** 中，选择**特定 IP (Specific IP)**，然后将 ISP-B 的网关 **172.16.7.7** 输入**特定 IP (Specific IP)** 编辑框中。

g) 点击**添加 (Add)**，将规则添加到路由映射。

h) 点击**保存 (Save)**。

步骤 3 使用路由映射来创建会在内部接口上启用 PBR 的 FlexConfig 对象。

a) 仍在对象页面上时，点击目录中的 **FlexConfig** > **FlexConfig 对象 (FlexConfig Object)**。

b) 找到 Policy_Based_Routing 对象，然后点击 **复制**（  ）。

这是系统定义的对象，但在编辑之前无法使用。它不会指向您可以直接使用路由映射名称进行更新的文本对象。您必须始终为此系统定义的对象创建自定义对象。

c) 点击复制图标时，系统会打开一个包含新对象的对话框，其默认名称为 Policy_Based_Routing_Copy。进行以下基本更改：

- **名称 (Name)** - 输入有意义的名称。例如，如果是为设备 FTD1 配置 PBR，可能是 **PBR_FTD1**.
- **说明 (Description)** - 删除说明或使其对您的目的有意义。
- **部署 (Deployment)** - 保留**一次 (Once)**。
- **类型 (Type)** - 保留**附加 (Append)**。

d) 对象的正文包含以下几行。

```
interface GigabitEthernet0/0
    policy-route route-map $r-map-object
```

请注意，“interface GigabitEthernet0/0”行已被设为为此示例配置正确的接口。如果要将 PBR 应用于其他接口，您需要更正接口硬件名称。

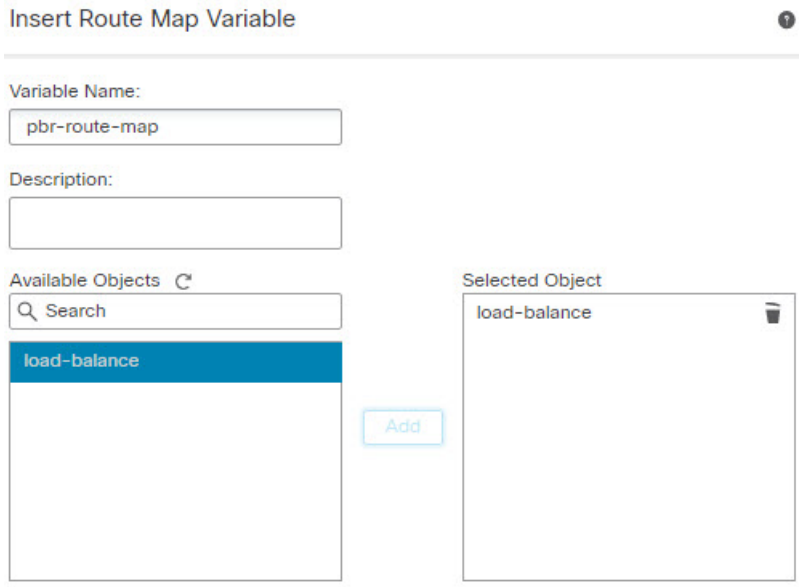
$r-map-object 字符串实际上并非一个真正的变量，它不指向任何内容。您需要替换该字符串。

e) 删除 $r-map-object 字符串，并将光标留在“policy-route route-map”行上，在 route-map 后面留一个空格。

f) 选择**插入 (Insert)** > **插入策略对象 (Insert Policy Object)** > **路由地图 (Route Map)**。

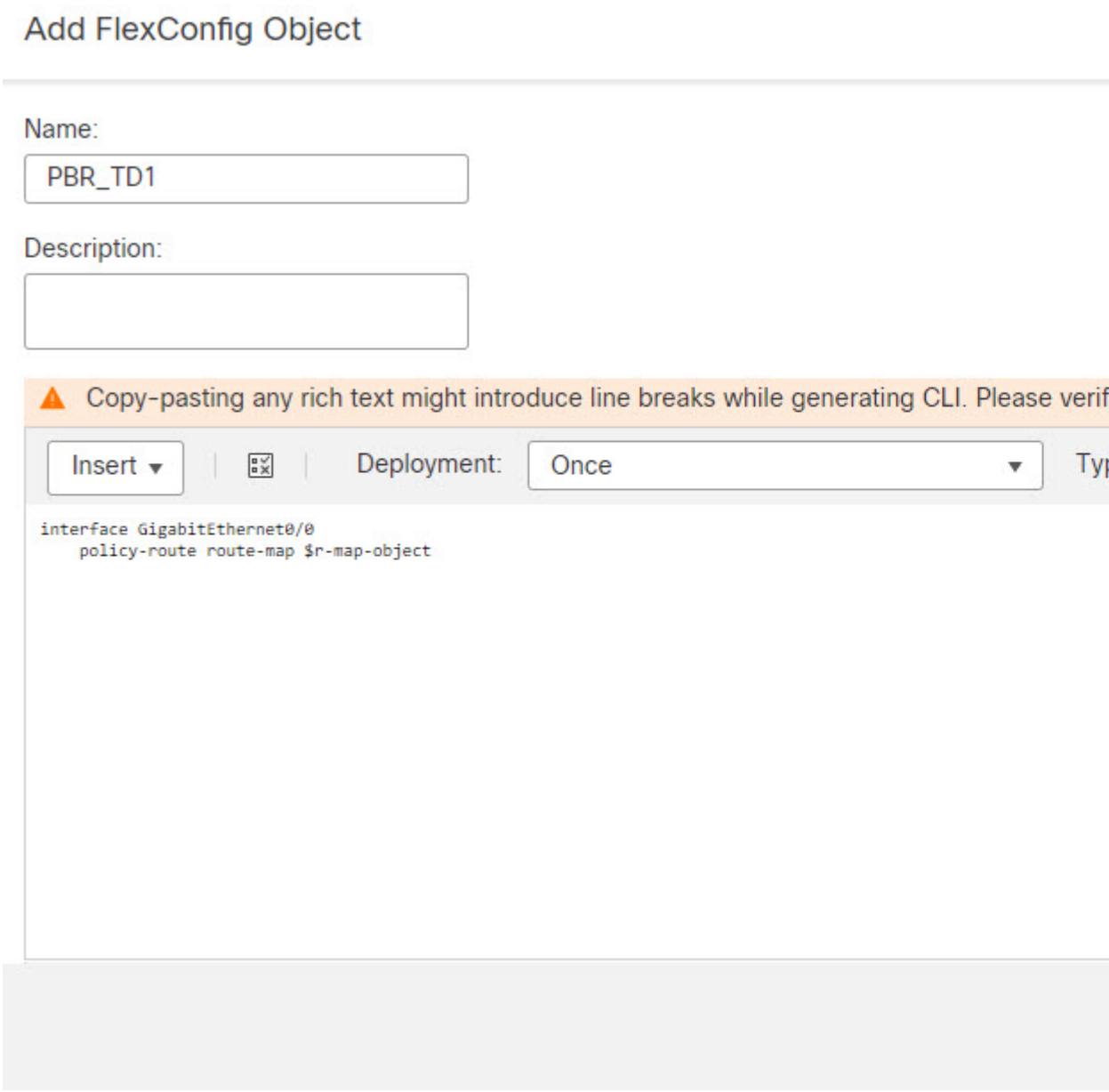
g) 在“路由地图变量”(Route Map Variable) 对话框中，配置以下内容：

- **变量名称 (Variable Name)** - 可以使用任何名称，例如 **pbr-route-map**。
- **选定对象 (Selected Object)** - 将负载均衡路由映射对象从可用列表移至所选列表。



h) 在“路由地图变量”(Route Map Variable) 对话框中点击**保存 (Save)**。

FlexConfig 对象现在应如下所示，而您的变量现在位于对话框底部的变量列表中。



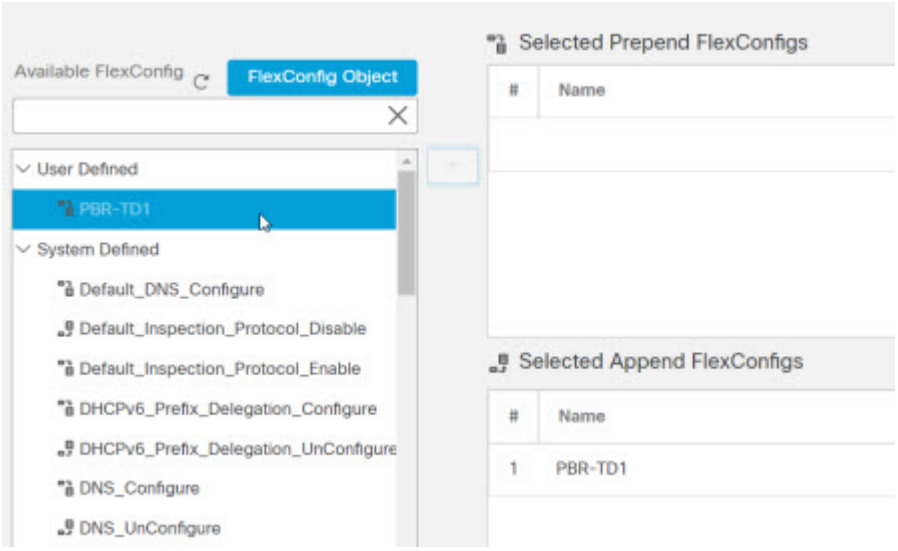
i) 点击**保存 (Save)**。

步骤 4 将 FlexConfig 对象添加到分配给设备的 FlexConfig 策略。

a) 选择 **设备 (Devices)** > **FlexConfig**。

b) 假设您尚未为此设备分配 FlexConfig 策略，请点击**新建策略 (New Policy)**，为策略指定名称并选择 FTD1 设备以向其分配策略，然后点击**保存 (Save)**。

c) 在可用对象列表中的“User Defined”文件夹下查找对象，然后点击 > 将其添加到所选对象列表。



d) 点击**保存 (Save)** 保存策略。

e) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择 FTD1 设备。

预览包括从 FlexConfig 对象和使用配置命令实施的 管理中心 托管配置部分生成的 CLI。它们被分成了多个部分。根据我们在本示例中所执行的操作，将配置以下命令。您可以使用此预览来验证是否达到了预期结果。

```
###Flex-config Prepended CLI ###

###CLI generated from managed features ###
configure session OBJECT
object-group service ProxySG_ExtendedACL_4294969626
 service-object ip
object-group service ProxySG_ExtendedACL_4294969648
 service-object ip
commit noconfirm revert-save
configure session FMC_SESSION_1
access-list high-priority extended permit object-group
      ProxySG_ExtendedACL_4294969626 10.1.0.0 255.255.0.0 any
access-list low-priority extended permit object-group
      ProxySG_ExtendedACL_4294969648 10.2.0.0 255.255.0.0 any
commit noconfirm revert-save
route-map load-balance permit 10
 match ip address high-priority
 set ip next-hop 192.168.6.6
route-map load-balance permit 20
 match ip address low-priority
 set ip next-hop 172.16.7.7


###Flex-config Appended CLI ###
interface GigabitEthernet0/0
    policy-route route-map load-balance
```

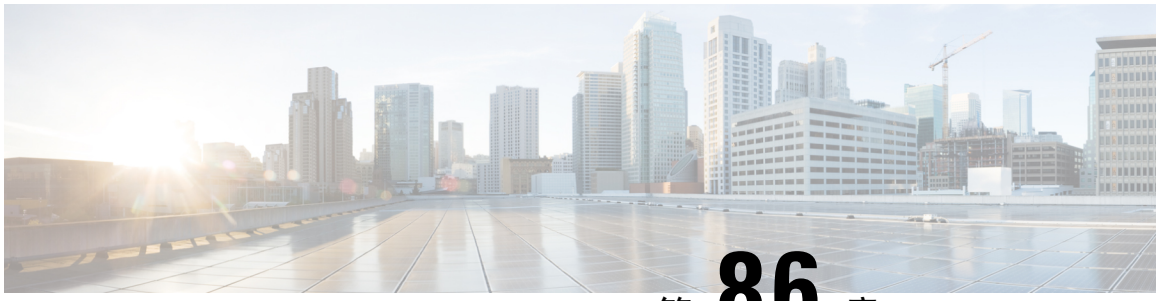
f) 点击**关闭 (Close)** 以关闭预览对话框。

下一步做什么

您现在可以将配置部署到设备。

第 XX 部分

高级网络分析和预处理



第 86 章

网络分析和入侵策略的高级访问控制设置

以下主题介绍如何配置网络分析和入侵策略的高级访问控制设置：

关于网络分析和入侵策略的高级访问控制设置

访问控制策略中的多项高级设置可监管需要特定专门技术才能做出的入侵检测和防御配置。高级设置通常几乎不需要修改，并非在每个部署中都出现。

网络分析和入侵策略的高级访问控制设置的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

在识别流量之前检查通过的数据包

对于某些功能（包括 URL 过滤、应用检测、 速率限制 和智能应用绕行），必须通过几个数据包才能建立连接，并使系统能够识别流量并确定哪个访问控制规则（如果任何）将处理该流量。

您必须明确配置访问控制策略，以检查这些数据包，防止其到达目的地并生成任何事件。请参阅指定策略以处理在流量识别之前通过的数据包，第 2042 页。

一旦系统识别应处理连接的访问控制规则或默认操作后，相应地处理和检测连接中剩余的数据包。

处理在流量识别之前通过的数据包的最佳实践

- 为访问控制策略指定的默认操作不会应用于这些数据包。
- 相反，请使用以下指南为访问控制策略的“高级”设置中的“在 **确定访问控制规则之前使用的入侵策略设置** 选择值。
  - 您可以选择系统创建或自定义入侵策略。例如，您可以选择 **平衡安全和连接**。
  - 出于性能原因，除非您有充分的理由，否则此设置应与访问控制策略的默认操作集匹配。
  - 如果系统不执行入侵检查（例如，在仅发现部署中），请选择 **无活动规则**。系统不会检查这些初始数据包，并且允许它们通过。
  - 默认情况下，此设置使用默认变量集。确保这符合您的用途。有关信息，请参阅变量集，第 1042 页。
  - 与第一个匹配网络分析规则关联的网络分析策略预处理您选择的策略的流量。如果没有网络分析规则，或者无任何网络分析规则匹配，则使用默认网络分析策略。

指定策略以处理在流量识别之前通过的数据包

注释 此设置有时称为 默认入侵策略。（这与访问控制策略的默认操作不同。）

开始之前

查看这些设置的最佳实践。请参阅处理在流量识别之前通过的数据包的最佳实践，第 2042 页。

过程

步骤 1 在访问控制策略编辑器中，点击 **高级**，然后点击 **网络分析** 和 **入侵策略** 旁边的 **编辑**（ ）。

如果显示**视图**（ ），则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 2 从**确定访问控制规则之前使用的入侵策略 (Intrusion Policy used before Access Control rule is determined)** 下拉列表中选择入侵策略。

如果选择用户创建的策略，则可以点击**编辑**（）在新窗口中编辑该策略。无法编辑系统提供的策略。

步骤 3 或者，从**入侵策略变量集 (Intrusion Policy Variable Set)** 下拉列表中选择其他变量集。您还可以点击变量集旁边的**编辑**（）以创建和编辑变量集。如果您未更改变量集，系统会使用默认的变量集。

步骤 4 点击**确定 (OK)**。

步骤 5 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改。

相关主题

变量集，第 1042 页

网络分析策略的高级设置

网络分析策略监管如何解码和预处理流量，以便进一步对其进行评估，特别适用于可能表明入侵尝试的异常流量。此流量预处理发生在安全情报匹配和流量解密之后，但是，发生在入侵策略对数据包进行详细检查之前。默认情况下，系统提供的“平衡安全性和连接”(Balanced Security and Connectivity) 网络分析策略是默认网络分析策略。

提示 系统提供的 Balanced Security and Connectivity 网络分析策略和 Balanced Security and Connectivity 入侵策略共同发挥作用，均可在入侵规则更新中更新。但是，网络分析策略管理的主要是预处理选项，而入侵策略管理的主要是入侵规则。

调整预处理的一个简单方法是创建并使用自定义网络分析策略作为默认值。对于复杂部署的高级用户，可以创建多个网络分析策略，每个策略定制为以不同方式预处理流量。然后，可以配置系统使用这些策略管理使用不同的安全区域、网络或 VLAN 的流量的预处理。

为此，请向访问控制策略中添加自定义网络分析规则。网络分析规则只是指定如何预处理与这些限制条件匹配的流量的一组配置和条件。可在现有访问控制策略的高级选项中创建和编辑网络分析规则。每条规则只属于一个策略。

每条规则均有：

- 一组规则条件，用于识别想要预处理的特定流量
- 一条关联的网络分析策略，想要用来预处理符合所有规则条件的流量

在系统预处理流量时，其将数据包按照规则编号自上而下的顺序与网络分析规则相匹配。不与任何网络分析规则匹配的流量由默认网络分析策略预处理。

设置默认网络分析策略

您可以选择系统或用户创建的策略。

注释 如果禁用预处理器，但是系统需要根据已启用的入侵或预处理器规则评估预处理的数据包，则系统将自动启用和使用预处理器，尽管它在网络分析策略 Web 界面中保持禁用。定制预处理（特别是使用多个自定义网络分析策略）是一个**高级**任务。由于预处理和入侵检测如此密切相关，因此，请**务必**小心确保允许网络和入侵策略检测每个数据包，以实现互补。

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)**，然后点击“网络分析和入侵策略”(Network Analysis and Intrusion Policies) 旁边的 **编辑**（  ）。

如果显示**视图**（  ），则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 2 从 **Default Network Analysis Policy** 下拉列表中，选择一条默认网络分析策略。

如果选择用户创建的策略，则可以点击**编辑**（  ）在新窗口中编辑该策略。无法编辑系统提供的策略。

步骤 3 点击**确定 (OK)**。

步骤 4 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改。

相关主题

自定义策略的限制，第 1456 页

网络分析规则

在访问控制策略的高级设置中，您可以使用网络分析规则定制网络流量的预处理配置。

网络分析规则从 1 开始进行编号。在系统预处理流量时，它将数据包按照升序规则编号自上而下的顺序与网络分析规则相匹配，然后根据所有条件都匹配的第一个规则预处理流量。

您可以向规则中添加区域、网络和 VLAN 标记条件。如果不为规则配置特定条件，系统将不基于此标准匹配流量。例如，一条包含网络条件但不含区域条件的规则根据其源 IP 地址或目标 IP 地址评估流量，不管其进出接口如何。不与任何网络分析规则匹配的流量由默认网络分析策略预处理。

网络分析策略规则条件

通过规则条件，您可以微调网络分析策略，以您要控制的用户和网络为目标。有关详细信息，请参阅以下各节之一：

相关主题

安全区域规则条件，第 1380 页
网络规则条件，第 607 页
VLAN 标记规则条件，第 1292 页

安全区域规则条件

安全区域可对网络进行分段，以通过跨多个设备将接口分组来帮助管理和分类流量。

区域规则条件可根据其源和目标安全区域控制流量。如果将源区域和目标区域均添加到区域条件中，则匹配流量必须源自其中一个源区域的接口，并通过其中一个目标区域的接口流出。

正如区域中的所有接口都必须为同一类型（均为内联、被动、交换或路由），区域条件中使用的所有区域也必须为同一类型。由于被动部署的设备不会传输流量，因此不能使用具有被动接口的区域作为目标区域。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

提示 按区域限制规则是提高系统性能的一种最佳方式。如果规则不适用于通过设备任意接口的流量，则该规则不影响该设备的性能。

安全区域条件和多租户

在多域部署中，在祖先域中创建的区域可以包含位于不同域中的设备上的接口。在后代域中配置区域条件时，您的配置仅适用于可以看到的接口。

网络规则条件

网络规则条件使用内部报头按流量的源和目标 IP 地址来控制流量。使用外部报头的隧道规则具有隧道终端条件而不是网络条件。

您可以使用预定义对象构建网络条件，或手动指定单个 IP 地址或地址块。

注释 您 不能 在身份规则中使用 FDQN 网络对象。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

VLAN 标记规则条件

注释 访问规则中的 VLAN 标记仅适用于内联集。带 VLAN 标记的访问规则与防火墙接口上的流量不匹配。

VLAN 规则条件可控制 VLAN 标记的流量，包括 Q-in-Q（堆栈 VLAN）流量。系统使用最内层的 VLAN 标记过滤 VLAN 流量，但不包括预过滤器策略，因为它在其规则中使用最外层的 VLAN 标记。

请注意以下 Q-in-Q 支持：

- Firepower 4100/9300 上的威胁防御 -不支持 Q-in-Q （仅支持一个 VLAN 标记）。
- 所有其他型号上的威胁防御 ：
  - 内联集和被动接口-支持 Q-in-Q，最多2个 VLAN 标记。
  - 防火墙接口-不支持 Q-in-Q （仅支持一个 VLAN 标记）。

可以使用预定义对象构建 VLAN 条件，或手动输入从 1 到 4094 之间的任意 VLAN 标记。使用连字符可指定 VLAN 标记范围。

最多可以指定 50 个 VLAN 条件。

在集群中，如果遇到 VLAN 匹配问题，请编辑访问控制策略高级选项“传输/网络预处理器设置”(Transport/Network Preprocessor Settings)，然后选择**跟踪连接时忽略 VLAN 信头 (Ignore the VLAN header when tracking connections)** 选项。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 VLAN 标记限制此配置可产生意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

配置网络分析规则

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)**，然后点击“网络分析和入侵策略”(Network Analysis and Intrusion Policies) 旁边的 **编辑**（）。

如果显示**视图**（），则表明设置继承自祖先策略，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

提示 点击**网络分析策略列表 (Network Analysis Policy List)** 以查看和编辑现有自定义网络分析策略。

步骤 2 在 **Network Analysis Rules** 旁，点击指明您所拥有的自定义规则数量的语句。

步骤 3 点击**添加规则**。

步骤 4 通过点击与要添加的条件来配置规则条件。请参阅配置网络分析规则，第 2047 页。

步骤 5 点击**网络分析 (Network Analysis)**，并选择要用于预处理匹配此规则的流量的**网络分析策略 (Network Analysis Policy)**。

点击 **编辑**（），在新窗口中编辑自定义策略。无法编辑系统提供的策略。

步骤 6 点击**添加**。

下一步做什么

- 部署配置更改。

管理网络分析规则

网络分析规则只是指定如何预处理与这些限制条件匹配的流量的一组配置和条件。可在现有访问控制策略的高级选项中创建和编辑网络分析规则。每条规则只属于一个策略。

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)**，然后点击“入侵和网络分析策略”(Intrusion and Network Analysis Policies) 部分旁边的 **编辑**（）。

如果显示**视图**（），则表明设置继承自祖先策略，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 2 在 **Network Analysis Rules** 旁，点击指明您所拥有的自定义规则数量的语句。

步骤 3 编辑您的自定义规则。您有以下选择：

- 要编辑某条规则的条件或更改该规则调用的网络分析策略，请点击该规则旁的 **编辑**（）。

- 要更改某条规则的评估顺序，请点击该规则并将其拖至正确的位置。要选择多条规则，请使用 Shift 和 Ctrl 键。
- 要删除规则，点击规则旁边的 **删除**（ ）。

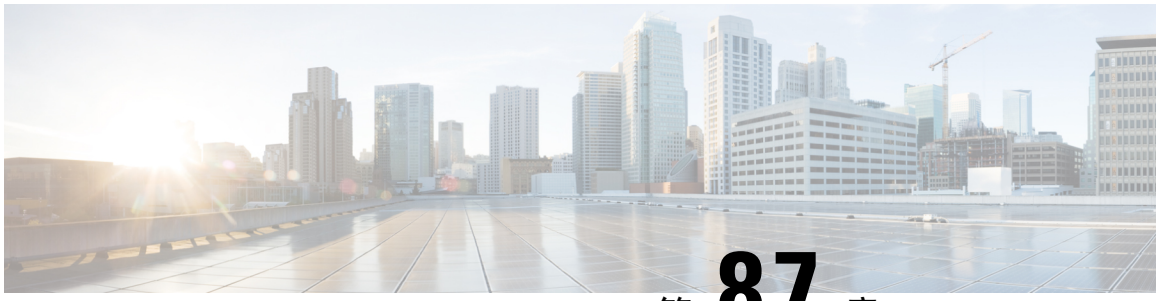
提示 右键点击规则会显示情景菜单，通过该菜单可剪切、复制、粘贴、编辑、删除网络分析规则和添加新的网络分析规则。

步骤 4 点击**确定 (OK)**。

步骤 5 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改。



第 87 章

网络分析策略使用入门

以下主题介绍如何开始使用网络分析策略：

网络分析策略基础知识

网络分析策略管理许多流量预处理选项，并供访问控制策略中的高级设置调用。网络分析相关预处理发生在安全情报匹配和 SSL 解密之后进行，但在入侵或文件检查开始之前进行。

默认情况下，系统使用平衡的安全性和连接性网络分析策略预处理由访问控制策略处理的所有流量。但是，您可以选择不同的默认网络分析策略执行此预处理。为方便您使用，系统提供多种无法修改的网络分析策略供选择，这些策略由Talos情报小组针对安全性和连接的特定平衡专门进行过调整。您也可以用自定义预处理设置创建自定义网络分析策略。

提示 系统提供的入侵和网络分析策略具有类似的名称，但包含不同的配置。例如，“平衡安全性和连接”(Balanced Security and Connectivity) 网络分析策略和“平衡安全性和连接”(Balanced Security and Connectivity) 入侵策略共同发挥作用，均可在入侵规则更新中更新。但是，网络分析策略管理的主要是预处理选项，而入侵策略管理的主要是入侵规则。网络分析和入侵策略相互配合，检查您的流量。

您也可以通过以下方式根据特定安全区域、网络和 VLAN 定制流量预处理选项：创建多个自定义网络分析策略，然后分配它们预处理不同流量。

网络分析策略的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

网络分析策略的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

管理网络分析策略

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 > 访问控制**，然后点击 **网络分析策略**或**策略 > 访问控制 > 入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 管理网络分析策略：

- 比较 - 点击**比较策略 (Compare Policies)**；请参阅比较策略 ， 第 148 页。
- 创建 - 如果要创建新的网络分析策略，请点击**创建策略 (Create Policy)**。

系统将创建两个版本的网络分析策略：**Snort 2 版本**和 **Snort 3 版本**。

- 对于 Snort 2 版本，请按照为 Snort 2 的自定义网络分析策略创建，第 2059 页中所述继续操作。
- 对于 Snort 3 版本，请按照创建网络分析策略，第 2055 页中所述继续操作。

- 删除 - 如果要删除网络分析策略，请点击 **删除**（），然后确认是否要删除策略。如果网络分析策略被访问控制策略引用，则无法删除该网络分析策略。

  如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
- 部署 - 选择**部署** > **部署**；请参阅部署配置更改，第 136 页。
- 编辑 - 如果要编辑现有网络分析策略，请点击 **编辑**（），然后如网络分析策略设置和缓存的更改，第 2061 页中所述继续操作。

  如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。
- 报告 - 点击**报告**（）；请参阅生成当前策略报告，第 149 页。

为 Snort 3 自定义网络分析策略的创建

默认网络分析策略针对典型的网络要求和最佳性能进行了调整。通常，默认网络分析策略足以满足大多数网络要求，您可能不需要自定义策略。但是，当您有特定的网络要求或遇到性能问题时，可以自定义默认网络分析策略。请注意，自定义网络分析策略是一种高级配置，应仅由高级用户或 Cisco 支持人员执行。

Snort 3 的网络分析策略配置是基于 JSON 和 JSO的数据驱动模型。架构基于 OpenAPI 规范，可帮助您了解支持的检查器、设置、设置类型和有效值。Snort 3 检查器是处理数据包的插件（类似于 Snort 2 预处理器）。网络分析策略配置可以 JSON 格式下载。

在 Snort 3 中，检查器和设置列表与 Snort 2 预处理器和设置列表不存在一对一映射。此外， 管理中心 中可用的检查器和设置的数量是 Snort 3 支持的检查器和设置的子集。有关 Snort 3 的详细信息，请参阅https://snort.org/snort3。有关管理中心 中的可用检查器的详细信息，请参阅https://www.cisco.com/go/snort3-inspectors。

注释

- 将 管理中心 升级到 7.0 版本时，在升级后，在 Snort 2 版本的网络分析策略中所做的更改不会迁移到 Snort 3。
- 与入侵策略不同，没有将 Snort 2 网络分析策略设置同步到 Snort 3 的选项。

默认检查器更新

轻量级安全包 (LSP) 更新可能包含新的检查器或对现有检查器配置的整数范围的修改。安装 LSP 后，新的检查器和/或更新的范围将在网络分析策略的 **Snort 3 版本**中的**检查器**下供使用。

绑定检查器

绑定检查器定义必须访问和考虑特定检查器时的流程。当流量与绑定程序检查器中定义的条件匹配时，只有该检查器的值/配置才会生效。例如：

对于 *imap* 检查器，当必须访问时，活页夹定义以下条件。即：

- 服务等于 imap。
- 角色均一致。

如果满足这些条件，则使用类型 imap。

binder

```
185     {
186       "when": {
187         "service": "imap",
188         "role": "any"
189       },
190       "use": {
191         "type": "imap"
192       }
193     },
```

单例检查器

单例检查器包含一个实例。这些检查器不支持添加更多实例，例如多例检查器。单例检查器的设置应用于整个流量，而不是特定的流量段。

例如：

```
{
   "normalizer":{
      "enabled":true,
      "type":"singleton",
      "data":{
         "ip4":{
            "df":true
         }
      }
   }
}
```

多例检查器

多例检查器包含多个实例，您可以根据需要进行配置。这些检查器支持根据特定条件（例如网络、端口和 VLAN）配置设置。一组受支持的设置称为实例。有一个默认实例，您还可以根据特定条件添加其他实例。如果流量与该条件匹配，则应用该实例中的设置。否则，将应用默认实例中的设置。此外，默认实例的名称与检查器的名称相同。

对于多例检查器，当您上传覆盖的检查器配置时，您还需要为 JSON 文件中的每个实例包含/定义匹配的绑定程序条件（必须访问或使用检查器时的条件），否则上传将导致错误。您还可以创建新实例，但请确保为您创建的每个新实例包含绑定程序条件，以避免错误。

例如：

- 修改了默认实例的多例检查器。

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   }
}
```

- 修改默认实例和默认绑定程序的多例检查器。

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   },
   "binder":{
```

```
      "type":"binder",
      "enabled":true,
      "rules":[
         {
            "use":{
               "type":"http_inspect"
            },
            "when":{
               "role":"any",
               "ports":"8080",
               "proto":"tcp",
               "service":"http"
            }
         }
      ]
   }
}
```

- 多例检查器，其中添加了自定义实例和自定义绑定程序。

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect1",
            "data":{
               "response_depth":5000
            }
         }
      ]
   },
   "binder":{
      "type":"binder",
      "enabled":true,
      "rules":[
         {
            "use":{
               "type":"http_inspect",
               "name":"http_inspect1"
            },
            "when":{
               "role":"any",
               "ports":"8080",
               "proto":"tcp",
               "service":"http"
            }
         }
      ]
   }
}
```

网络分析策略映射

对于网络分析策略，Cisco Talos 提供了映射信息，用于为 Snort 3 版本找到对应的 Snort 2 版本的策略。

此映射可确保 Snort 3 版本的策略具有对应的 Snort 2 版本。

查看网络分析策略映射

过程

步骤 1 转至策略 **(Policies)** > 入侵 **(Intrusion)** > 网络分析策略 **(Network Analysis Policies)**。

步骤 2 点击**NAP 映射 (NAP Mapping)**。

步骤 3 展开查看映射 **(View Mappings)** 的箭头。

系统将显示自动映射到 Snort 2 等效策略的 Snort 3 网络分析策略。

步骤 4 点击确定 **(OK)**。

创建网络分析策略

所有 管理中心 现有的网络分析策略均可用于相应的 Snort 2 和 Snort 3 版本。当您创建新的网络分析策略时，会同时创建 Snort 2 版本和 Snort 3 版本。

过程

步骤 1 转至策略 **(Policies)** > 入侵 **(Intrusion)** > 网络分析策略 **(Network Analysis Policies)**。

步骤 2 点击创建策略。

步骤 3 输入名称 **(Name)** 和描述 **(Description)**。

步骤 4 从可用选项中选择检测模式 **(Inspection Mode)** 。

- 检测
- 防御

步骤 5 选择基本策略 **(Base Policy)** ，然后点击保存 **(Save)**。

注释 如果您使用的是 Snort 3 和 SSL 解密或 TLS 服务器身份，请在预防 **(Prevention)** 模式下配置网络分析策略 (NAP)。

新的网络分析策略使用其对应的 **Snort 2 版本**和 **Snort 3 版本**创建。

修改网络分析策略

您可以修改网络分析策略以更改其名称、说明或基本策略。

过程

步骤 1 转至 策略 > 入侵 > 网络分析策略。

步骤 2 点击**编辑 (Edit)** 以更改名称、说明、检测模式或基本策略。

注释 如果编辑网络分析策略名称、说明、基本策略和检测模式，编辑内容将同时应用于Snort 2 和 Snort 3 版本。如果要更改特定版本的检测模式，可以在相应版本的网络分析策略页面中执行此操作。

步骤 3 点击**保存 (Save)**。

自定义网络分析策略

您可以根据自己的要求自定义 Snort 3 版本的网络分析策略。

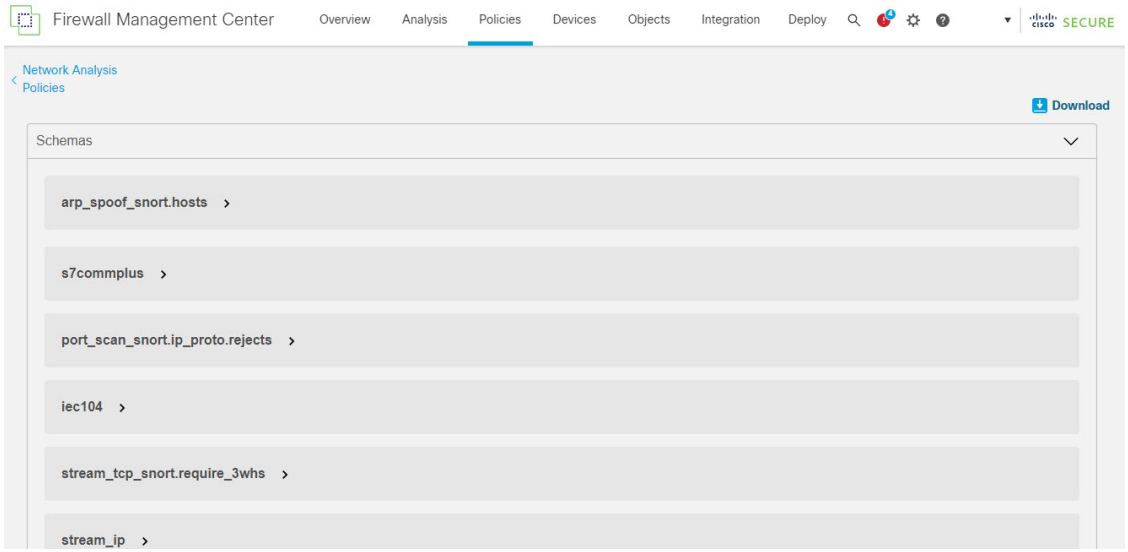
过程

步骤 1 点击网络分析策略的 **Snort 3 版本 (Snort 3 Version)** 中的**操作 (Actions)** 下拉菜单。

系统将显示以下选项：

- 查看架构
- 下载
  - 架构 (Schema)
  - 示例文件/模板
  - 完整配置
  - 覆盖的配置
- 上传
  - 覆盖的配置

步骤 2 点击**查看方案 (View Schema)** 可直接在浏览器中打开方案文件。



步骤 3 在**下载 (Download)** 下，您可以根据需要使用以下选项来下载架构文件、示例文件、完整配置或覆盖配置。

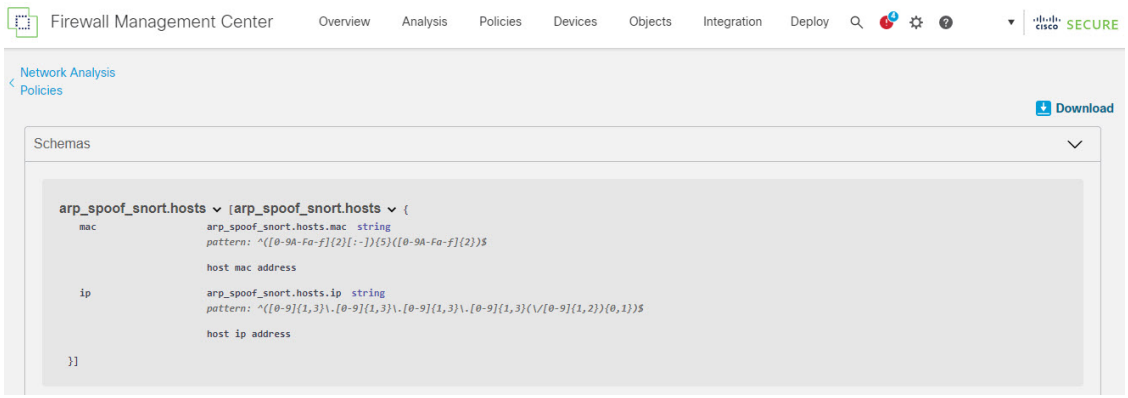
通过这些选项，您可以了解允许的值、范围和模式、现有和默认检查器配置以及覆盖的检查器配置。

a) 点击**架构 (Schema)** 以下载架构文件。

架构文件验证您上传或下载的内容。您可以下载架构文件并使用任何第三方 JSON 编辑器打开它。架构文件可帮助您确定可以为检查器配置的参数及其相应的允许值、范围和要使用的接受模式。

例如，对于 *arp_spoof_snort* 检查器，您可以配置主机。主机包括 *mac* 和 *ip* 地址值。架构文件显示这些值的以下可接受模式。

- **mac** – 模式： `^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$`
- **ip** – 模式：`^([0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}()/[0-9]{1,2}){0,1})$`



您必须根据架构文件中接受的值、范围和模式，才能成功覆盖检查器配置，否则会收到错误消息。

b) 点击**示例文件/模板 (Sample File / Template)** 以使用包含示例配置的预先存在的模板来帮助您配置检查器。

您可以参考示例文件中包含的示例配置，并进行您可能需要的任何更改。有关信息，请参阅。

c) 点击**完整配置 (Full Configuration)** 以将整个检查器配置下载到一个文件中。

您可以下载完整配置来查找所需的信息，而不是单独展开检查器。此文件中提供有关检查器配置的所有信息。

d) 点击**覆盖的配置 (Overridden Configuration)** 以下载已覆盖的检查器配置。

如果尚未覆盖任何检查器配置，则此选项处于禁用状态。当您覆盖检查器配置时，此选项会自动启用，以允许您下载。

步骤 4 要覆盖现有配置，请按照以下步骤操作。

您可以选择使用以下方式覆盖检查器配置。

- 直接在 管理中心上对检查器进行内联编辑。有关如何进行内联编辑的步骤，请参阅 。
- 继续按照当前程序使用**操作 (Actions)** 下拉菜单上传覆盖的配置文件。

如果您选择直接在 管理中心上进行内联编辑，则无需进一步执行当前程序。否则，您必须完全遵循此程序。

a) 在**检查器 (Inspectors)** 下，展开要覆盖其默认配置的所需检查器。

默认配置显示在左侧列中，被覆盖的配置显示在检查器下的右侧列中。

您可能需要通过在搜索栏中输入任何相关文本来搜索检查器。

b) 点击**复制到剪贴板 (Copy to clipboard)** 图标，将默认检查器配置复制到剪贴板。

c) 创建一个 JSON 文件并将默认配置粘贴到其中。

d) 保留要覆盖的检查器配置，并从 JSON 文件中删除所有其他配置和实例。

您还可以使用**示例文件/模板 (Sample File / Template)** 来了解如何覆盖默认配置。这是一个包含 JSON 片段的示例文件，说明如何为 Snort 3 自定义网络分析策略。有关详细信息，请参阅 。

e) 根据需要对检查器配置进行更改。

验证更改并确保它们符合架构文件。对于多例检查器，请确保所有实例的绑定器条件都包含在 JSON 文件中。有关详细信息，请参阅为 Snort 3 自定义网络分析策略的创建，第 2051 页中的 多例检查器 。

f) 如果要复制任何其他默认检查器配置，请将该检查器配置附加到包含覆盖配置的现有文件。

注释 复制的检查器配置必须符合 JSON 标准。

g) 将覆盖的配置文件保存到您的系统。

h) 将覆盖的配置上传到 管理中心 ，如下一步中所述。

步骤 5 在**上传 (Upload)**下，您可以点击**覆盖配置 (Overridden Configuration)** 以上传包含已覆盖配置的 JSON 文件。

注意　仅上传您需要的更改。不应上传整个配置，因为它会使覆盖本质上具有粘性，因此，将不会应用对默认配置的任何后续更改作为 LSP 更新的一部分。

您可以拖放文件，也可以点击浏览到系统中保存的包含覆盖检查器配置的 JSON 文件。

- **合并检查器覆盖 (Merge inspector overrides)** - 如果没有通用检查器，上传文件中的内容会与现有配置合并。如果有通用检查器，则上传文件（用于通用检查器）中的内容优先于之前的内容，并将替换这些检查器的先前配置。
- **替换检查器覆盖 (Replace inspector overrides)** - 删除所有之前的覆盖并替换为上传文件中的新内容。

  注意　由于选择此选项会删除之前的所有覆盖，因此请在使用此选项覆盖配置之前做出明智的决定。

如果在上传覆盖的检查器时发生任何错误，您会在**上传覆盖的配置文件 (Upload Overridden Configuration File)** 弹出窗口中看到错误。您还可以下载存在错误的文件，然后修复错误并重新上传文件。

步骤 6　在**上传覆盖的配置文件 (Upload Overridden Configuration File)** 弹出窗口中，点击**导入 (Import)** 按钮以上传覆盖的检查器配置。

上传覆盖的检查器配置后，您会在检查器旁边看到一个橙色圆圈，表示它是一个覆盖的检查器。

此外，检查器下的**覆盖配置 (Overridden Configuration)** 列会显示覆盖的值。

您还可以使用搜索栏旁边的**仅显示覆盖 (Show Overrides Only)** 复选框查看所有已覆盖的检查器。

注释　确保始终下载**下载 (Download)** 下的 **覆盖配置 (Overridden Configurations)**，然后打开 JSON 文件并将对检查器配置的任何新更改/覆盖附加到此文件。需要执行此操作，以免丢失旧的覆盖配置。

步骤 7　（可选）在进行任何新的检查器配置更改之前，备份系统上的覆盖配置文件。

提示　我们建议您在覆盖检查器配置时不时进行备份。

相关主题

- 将覆盖的配置恢复为默认配置
- 查看具有覆盖的检查器列表
- 自定义网络分析策略配置示例
- 在网络分析策略页面上搜索检查器
- 复制检查器配置

为 Snort 2 的自定义网络分析策略创建

当创建新的网络分析策略时，必须为其提供唯一的名称，指定基本策略并选择内联模式。

基本策略定义网络分析策略的默认设置。修改新策略中的设置会覆盖（但不会更改）基本策略中的该设置。您可以使用系统提供的策略或自定义策略作为您的基本策略。

网络分析策略的内联模式允许预处理器修改（标准化）和丢弃流量，从而使攻击者避开检测的可能性最小化。请注意，在被动部署中，无论内联模式如何设置，系统都无法影响流量传输。

相关主题

基本层，第 1609 页
内联部署中预处理器流量的修改，第 2064 页
创建自定义网络分析策略，第 2060 页
编辑网络分析策略，第 2061 页

创建自定义网络分析策略

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 > 访问控制**，然后点击 **网络分析策略**或**策略 > 访问控制 > 入侵**，然后点击 **网络分析策略**。

注释　如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击**创建策略**。如果在另一策略中有未保存的更改，当系统提示您返回**网络分析策略 (Network Analysis Policy)** 页面时，请点击**取消 (Cancel)**。

步骤 3 在**名称 (Name)** 中输入唯一的名称。

在多域部署中，策略名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的策略名称的冲突。

步骤 4 输入**说明 (Description)**（可选）。

步骤 5 选择初始**基本策略 (Base Policy)**。您可以使用系统提供的策略或自定义策略作为您的基本策略。

注意　在配置自定义 NAP 时，如果选择**最大检测 (Maximum Detection)** 作为**基本策略**，则性能可能会下降。建议在部署到生产环境之前检查并测试此设置。

步骤 6 如果要允许预处理器影响内联部署中的流量，请启用**内联模式 (Inline Mode)**。

步骤 7 要创建策略：

- 点击**创建策略 (Create Policy)**创建新策略并返回**网络分析策略 (Network Analysis Policy)** 页面。新策略的设置与其基本策略相同。
- 点击**创建并编辑策略 (Create and Edit Policy)**，创建策略并在高级网络分析策略编辑器中将其打开进行编辑。

Snort 2 的网络分析策略管理

在“网络分析策略”页面（或**策略 > 访问控制**，然后点击 **网络分析策略**或**策略 > 访问控制 > 入侵**，然后点击 **网络分析策略**）上，可以查看当前的自定义网络分析策略以及以下信息：

- 最近一次修改策略的时间和日期（采用当地时间）以及执行此修改的用户。
- 是否已启用**内联模式 (Inline Mode)** 设置，该设置允许预处理器影响流量
- 哪些访问控制策略和设备使用网络分析策略来预处理流量
- 策略是否有未保存的更改，以及有关何人（如果有任何人）当前正在编辑该策略的信息

除了您创建的自定义策略之外，系统还提供两种自定义策略：初始内联策略和初始被动策略。这两个网络分析策略使用“平衡安全性和连接”(Balanced Security and Connectivity) 网络分析策略作为其基本策略。两者之间的唯一区别在于其内联模式，在内联策略中允许预处理器影响流量，但在被动策略中禁用了该功能。您可以编辑并使用系统提供的这些自定义策略。

请注意，如果您的 Firepower 系统用户帐户的角色被限制为“入侵策略”(Intrusion Policy) 或“修改入侵策略”(Modify Intrusion Policy)，则您可以创建和编辑网络分析策略及入侵策略。

相关主题

创建自定义网络分析策略，第 2060 页
编辑网络分析策略，第 2061 页

网络分析策略设置和缓存的更改

当您创建新的网络分析策略时，它具有与其基本策略相同的设置。

当您定制网络分析策略时，特别是在禁用预处理器时，请记住某些预处理器和入侵规则要求首先以某种方式对流量进行解码或预处理。如果您禁用一个必需的预处理程序，虽然该预处理程序在网络分析策略 Web 界面中保持禁用，但系统仍自动通过其当前设置使用它。

注释 由于预处理和入侵检查密切相关，因此用于检查单个数据包的网络分析和入侵策略**必须**相互补充。定制预处理（特别是使用多个自定义网络分析策略）是一个**高级**任务。

系统为每个用户缓存一条网络分析策略。在编辑网络分析策略时，如果您选择任何菜单或指向另一页的其他路径，即使您离开此页，更改也会保留在系统缓存中。

相关主题

策略如何检查流量是否存在入侵，第 1448 页
自定义策略的限制，第 1456 页

编辑网络分析策略

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略** > **访问控制**，然后点击 **网络分析策略**或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击想要配置的网络分析策略旁的 **编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 编辑网络分析策略：

- 更改基本策略 - 如果要更改基本策略，请从“策略信息”(Policy Information) 页面上的**基本策略 (Base Policy)** 下拉列表中选择一个基本策略。
- 管理策略层 - 如果要管理策略层，请点击导航面板中的**策略层 (Policy Layers)**。
- 修改预处理器 - 如果要启用、禁用或编辑预处理器的设置，请点击导航面板中的**设置 (Settings)**。
- 修改流量 - 如果要允许预处理器修改或丢弃流量，请选中“策略信息”(Policy Information) 页面上的**内联模式 (Inline Mode)** 复选框。
- 查看设置 - 如果要查看基本策略中的设置，请点击“策略信息”(Policy Information) 页面上的**管理基本策略 (Manage Base Policy)**。

步骤 5 要保存自上次策略确认以来在此策略中进行的更改，请选择**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 如果希望预处理器生成事件并在内联部署中丢弃攻击性数据包，请启用该预处理器的规则。有关详细信息，请参阅设置入侵规则状态，第 1488 页。
- 部署配置更改。

相关主题

基本层，第 1609 页
更改基本策略，第 1610 页
Snort 2 的网络分析策略中的预处理器配置，第 2063 页
内联部署中预处理器流量的修改，第 2064 页
管理层，第 1614 页
冲突和更改：网络分析和入侵策略，第 1459 页

Snort 2 的网络分析策略中的预处理器配置

预处理器通过规范化流量和标识协议异常，准备要进行进一步检查的流量。预处理器可以在数据包触发配置的预处理器选项时生成预处理器事件。网络分析策略的基本策略决定了默认情况下启用哪些预处理器及各自的默认配置。

注释 在大多数情况下，配置预处理器要求特定专业知识，并且通常很少需要修改或不需要任何修改。定制预处理（特别是使用多个自定义网络分析策略）是一个**高级**任务。由于预处理和入侵检查密切相关，因此用于检查单个数据包的网络分析和入侵策略**必须**相互补充。

修改预处理器配置要求了解配置及其对网络的潜在影响。

请注意，某些高级传输和网络预处理器设置全局应用于您部署访问控制策略所在的所有网络、区域和 VLAN。可以在访问控制策略中而非网络分析策略中配置这些高级设置。

另请注意，您在入侵策略中配置敏感数据预处理器，用于检测 ASCII 文本形式的信用卡号和社会安全保障号等敏感数据。

相关主题

DCE/RPC 预处理器， 第 2068 页
DNP3 预处理器， 第 2138 页
DNS 预处理器， 第 2079 页
FTP/Telnet 解码器， 第 2083 页
GTP 预处理器， 第 2112 页
HTTP 检查预处理器， 第 2090 页
IMAP 预处理器， 第 2114 页
内联规范化预处理器， 第 2153 页
IP 分片重组预处理器， 第 2160 页
Modbus 预处理器， 第 2136 页
数据包解码器， 第 2164 页
POP 预处理器， 第 2117 页
敏感数据检测基础知识， 第 1627 页
SIP 预处理器， 第 2107 页
SMTP 预处理器， 第 2120 页
SSH 预处理器， 第 2125 页
SSL 预处理器， 第 2129 页
Sun RPC 预处理器， 第 2105 页
TCP 数据流预处理， 第 2169 页
UDP 数据流预处理， 第 2179 页
自定义策略的限制， 第 1456 页

内联部署中预处理器流量的修改

在内联部署中（即，使用路由接口、交换接口、透明接口或内联接口对将相关配置部署到设备），某些预处理器可以修改并阻止流量。例如：

- 内联规范化预处理器将数据包标准化为准备这些数据包，以便由其他预处理器和入侵规则引擎进行分析。您还可以使用预处理器的**允许这些 TCP 选项 (Allow These TCP Options)** 和**阻止无法解析的 TCP 报头异常 (Block Unresolvable TCP Header Anomalies)** 选项阻止某些数据包。
- 系统可以丢弃具有无效校验和的数据包。
- 系统可以丢弃匹配基于速率的攻击防护设置的数据包。

要使网络分析策略中配置的预处理器影响流量，还必须启用并正确配置预处理器，并正确部署内联的受管设备。最后，您必须启用网络分析策略的 **Inline Mode** 设置。

网络分析策略中的预处理器配置说明

当您在网络分析策略的导航面板中选择 **Settings** 时，策略将按类型列出其预处理器。在“设置”(Settings) 页面中，可以启用或禁用网络分析策略中的预处理器，以及访问预处理器配置页面。

必须启用预处理器，这样您才能对其进行配置。当启用预处理器时，该预处理器配置页面的子链接显示在导航面板中**设置 (Settings)** 链接下，并且到配置页的**编辑 (Edit)** 链接显示在“设置”(Settings) 页面上的预处理器旁边。

提示 将预处理器的配置恢复为基本策略中的设置，请点击预处理器配置页面上的**恢复为默认值 (Revert to Defaults)**。出现提示时，请确认您要恢复。

当禁用预处理器时，子链接和**编辑 (Edit)** 链接将不显示，但会保留您的配置。请注意，为了执行其特定分析，许多预处理器和入侵规则要求首先以某种方式对流量进行解码或预处理。如果您禁用一个必需的预处理程序，虽然该预处理程序在网络分析策略网络界面中保持禁用，但系统仍自动通过其当前设置使用它。

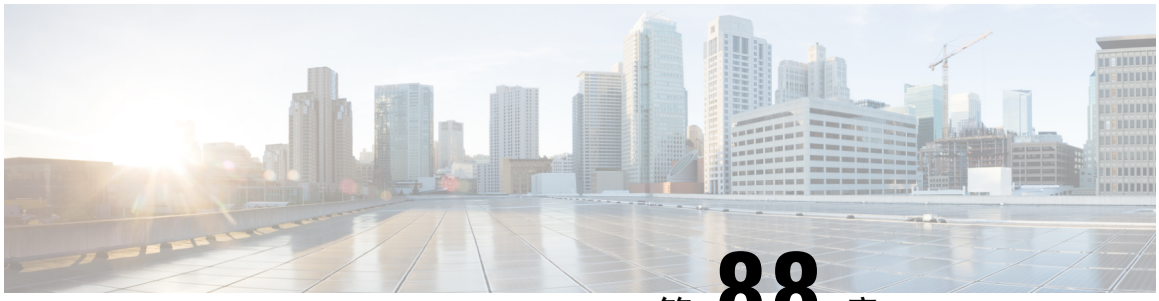
如果要评估配置如何在内联部署中起作用，而不会实际修改流量，您可以禁用内联模式。在被动部署或分路模式的内联部署中，系统无法影响流量，无论内联模式设置如何。

注释 禁用内联模式可能会影响入侵事件性能统计数据图表。在内联部署中启用内联模式时，“入侵事件性能”页面（**概述** > **摘要** > **入侵事件性能**）显示表示已规范化和阻止的数据包的图表。如果禁用内联模式，或者在被动部署中，许多图表显示有关系统应当已规范化或丢弃的流量的数据。

注释 在内联部署中，我们建议您启用内联模式并配置已启用 **Normalize TCP Payload** 选项的内联规范化预处理器。在被动部署中，我们建议您使用 自适应配置文件。

相关主题

高级传输/网络预处理器设置，第 2148 页
校验和验证，第 2151 页
内联规范化预处理器，第 2153 页



第 88 章

应用层预处理器

以下主题介绍应用层预处理器及其配置方法：

应用层预处理器简介

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

应用层协议可以通过多种方式表示相同的数据。Firepower 系统提供应用层协议解码器，这些解码器可将特定类型的数据包数据规范化为入侵规则引擎可以分析的格式。规范化应用层协议编码使得规则引擎可以有效地将相同的内容相关规则应用于其数据以不同方式呈现的数据包，并获得有意义的结果。

当入侵规则或规则参数要求禁用的预处理器时，系统会自动使用其当前设置，即使其在网络分析策略网络界面中保持禁用状态。

请注意，大多数情况下，除非在入侵策略中启用随附预处理器规则，否则预处理器不会生成事件。

应用层预处理器的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

应用层预处理器的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

DCE/RPC 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

DCE/RPC 协议使不同网络主机上的进程可以像在同一主机上一样进行通信。这些进程间通信一般通过 TCP 和 UDP 在主机之间传输。在 TCP 传输中，DCE/RPC 也可以进一步封装在 Windows 服务器消息块 (SMB) 协议或 Samba 中；Samba 是一种在由 Windows 和类似 UNIX 或类似 Linux 操作系统组成的混合环境中用于进程间通信的开源 SMB 实现。此外，网络上的 Windows IIS Web 服务器可能使用 IIS RPC over HTTP，后者通过防火墙向代理 TCP 传输 DCE/RPC 流量提供分布式通信。

请注意，对DCE/RPC预处理器选项和功能的说明包括DCE/RPC的Microsoft实现（又称为MSRPC）；对 SMB 选项和功能的说明涉及 SMB 和 Samba。

虽然大多数 DCE/RPC 漏洞出现在针对 DCE/RPC 服务器（实际上可能是网络上运行 Windows 或 Samba 的任何主机）的 DCE/RPC 客户端请求中，但在服务器响应中也可能出现漏洞。DCE/RPC 预处理器检测封装在TCP、UDP和SMB传输（包括使用版本1 RPC over HTTP的TCP传输DCE/RPC）中的 DCE/RPC 请求和响应。此预处理器分析 DCE/RPC 数据流并检测 DCE/RPC 流量中的异常行为和逃避技术。它还分析 SMB 数据流并检测异常 SMB 行为和逃避技术。

除 IP 分片重组预处理器提供的 IP 分片重组和 TCP 数据流预处理器无缝提供的 TCP 数据流以外，DCE/RPC 预处理器还会将 SMB 分段重组并将 DCE/RPC 分片重组。

最后，DCE/RPC 预处理器会规范化 DCE/RPC 流量，以便规则引擎进行处理。

无连接和面向连接的 DCE/RPC 流量

DCE/RPC 消息符合两种不同的 DCE/RPC 协议数据单元（PDU）之一：

面向连接的 DCE/RPC PDU 协议

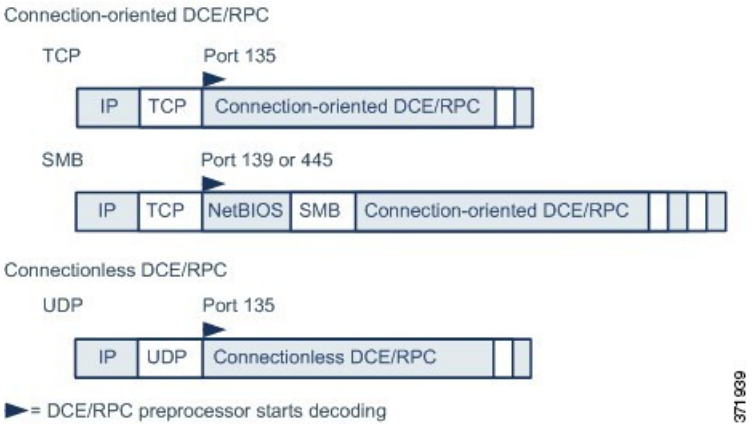
DCE/RPC 预处理器在 TCP、SMB 和 RPC over HTTP 传输中检测面向连接 DCE/RPC。

无连接 DCE/RPC PDU 协议

DCE/RPC 预处理器在 UDP 传输中检测无连接 DCE/RPC。

这两种DCE/RPC PDU协议都有独特的报头和数据特性。例如，面向连接的DCE/RPC的报头长度通常为 24 字节，而无连接 DCE/RPC 的报头长度固定为 80 字节。此外，分片无连接 DCE/RPC 的正确分片顺序不能通过无连接传输处理，而必须通过无连接DCE/RPC报头值提供保证；相比之下，传输协议可确保面向连接 DCE/RPC 的分片顺序正确。DCE/RPC 预处理器使用这些特性及其他特定协议特性监控这两种协议是否存在异常和其他躲避技术，对流量进行解码和分片重组，然后再将流量传送到规则引擎。

下图说明了 DCE/RPC 预处理器开始为不同传输处理 DCE/RPC 流量的点。



对于上图，请注意以下几点：

- 已知 TCP 或 UDP 端口 135 识别 TCP 和 UDP 传输中的 DCE/RPC 流量。

- 图中未包含 RPC over HTTP。

  对于 RPC over HTTP，面向连接 DCE/RPC 在完成 HTTP 初始设置序列后直接通过 TCP 传输（如图所示）。

- DCE/RPC 预处理器通常接收适用于 NetBIOS 会话服务的已知 TCP 端口 139 或以类似方式实现的已知 Windows 端口 445 上的 SMB 流量。

  由于 SMB 具有除传输 DCE/RPC 以外的许多功能，因此，预处理器会首先测试 SMB 流量是否携带 DCE/RPC 流量，如果不是则停止处理，如果是则继续处理。

- IP 封装所有 DCE/RPC 传输。
- TCP 传输所有面向连接 DCE/RPC。
- UDP 传输无连接 DCE/RPC。

DCE/RPC 基于目标的策略

Windows 和 Samba DCE/RPC 的实现有很大不同。例如，在对 DCE/RPC 流量进行分片重组时，所有 Windows 版本都在第一个分片中使用 DCE/RPC 上下文 ID，而所有 Samba 版本都在最后一个分片中使用上下文 ID。再如，Windows Vista 在第一个分片中使用操作编号报头字段来识别特定函数调用，而 Samba 及其他所有 Windows 版本都在最后一个分片中使用操作编号字段。

Windows 和 Samba SMB 的实现也有很大不同。例如，Windows 在与命名管道配合使用时可识别 SMB OPEN 和 READ 命令，而 Samba 不能识别这些命令。

启用 DCE/RPC 预处理器会自动启用默认基于目标的策略。或者，您可以添加将运行不同 Windows 或 Samba 版本的其他主机设为目标的基于目标的策略。默认基于目标的策略适用于未包含在其他基于目标的策略的任何主机。

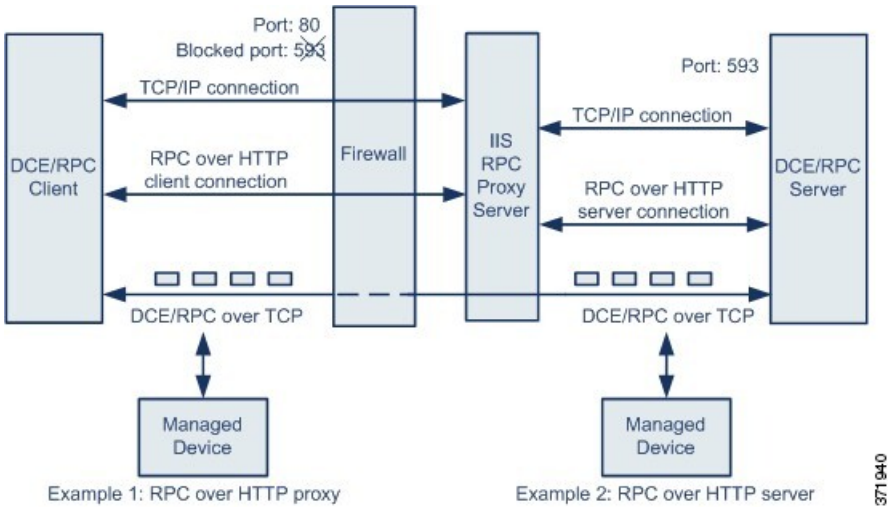
在每个基于目标的策略中，可以：

- 启用一个或多个传输并为每个传输指定检测端口
- 启用并指定自动检测端口
- 设置预处理器，以检测尝试连接到一个或多个所识别的共享 SMB 资源的情况
- 将预处理器配置为检测 SMB 流量中的文件，以及检查检测到的文件中的指定字节数
- 修改应仅由具备 SMB 协议专业知识的用户修改的高级选项；通过该选项，可以将预处理器设置为检测链式 SMB AndX 命令数量超过指定最小数量的情况

除在 DCE/RPC 预处理器中启用 SMB 流量文件检测以外，还可以配置文件策略以选择性地捕获和阻止这些文件，或者将这些文件提交到思科 AMP 云以进行动态分析。在策略中，必须创建具有**操作**为 **Detect Files** 或 **Block Files** 且选定**应用协议**为 **Any** 或 **NetBIOS-ssn (SMB)** 的文件规则。

RPC over HTTP 传输

借助 Microsoft RPC over HTTP，可以引导 DCE/RPC 流量穿过防火墙，如下图所示。DCE/RPC 预处理器检测版本 1 Microsoft RPC over HTTP。



Microsoft IIS 代理服务器和 DCE/RPC 服务器可以位于同一主机上，也可以位于不同的主机上。对于这两种情况，我们提供独立的代理和服务器选项。对于上图，请注意以下几点：

- DCE/RPC 服务器监控端口 593 的 DCE/RPC 客户端流量，但防火墙阻止该端口。

  默认情况下，防火墙通常会阻止端口 593。

- RPC over HTTP 使用已知 HTTP 端口 80（防火墙很可能允许此端口）通过 HTTP 传输 DCE/RPC。
- 在示例 1 中，将会选择 **RPC over HTTP 代理 (RPC over HTTP proxy)** 选项来监控 DCE/RPC 客户端和 Microsoft IIS RPC 代理服务器之间流量。
- 在示例 2 中，如果 Microsoft IIS RPC 代理服务器和 DCE/RPC 服务器位于不同的主机，且设备监控这两个服务器之间的流量，将会选择 **RPC OVER HTTP 服务器 (RPC OVER HTTP SERVER)** 选项。
- RPC over HTTP 完成 DCE/RPC 客户端和服务器代理设置后，流量仅包含通过 TCP 传输的面向连接 DCE/RPC。

DCE/RPC 全局选项

DCE/RPC 预处理器全局选项控制预处理器的工作方式。请注意，除**已达到内存限制 (Memory Cap Reached)** 和 **SMB 会话上自动检测策略 (Auto-Detect Policy on SMB Session)** 这两个选项外，修改这些选项可能会对性能或检测能力造成负面影响。除非您已充分理解此预处理器及其与已启用的 DCE/RPC 规则之间的交互，否则请勿修改这些选项。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

最大分片大小 (Maximum Fragment Size)

当选择**启用分片重组 (Enable Defragmentation)** 时，可指定允许的最大 DCE/RPC 分片长度。预处理器会在分片重组前将较大分片截断成为指定的尺寸以便进行处理，但不会改变实际数据包。空白字段将禁用此选项。

确保**最大分片大小 (Maximum Fragment Size)** 选项大于或等于规则需要检测到的深度。

重组阈值 (Reassembly Threshold)

当选择**启用分片重组 (Enable Defragmentation)** 时，0 表示禁用此选项，或者指定分片 DCE/RPC 最小字节数，并且如果适用，则指定在向规则引擎发送已重组的数据包之前要加入队列的分段 SMB 字节数。值越小，实现早期检测的可能性越高，但可能会对性能造成负面影响。如果启用此选项，应当测试性能所受的影响。

确保**重组阈值 (Reassembly Threshold)** 选项大于或等于规则需要检测到的深度。

启用分片重组 (Enable Defragmentation)

指定是否对 DCE/RPC 流量进行分片重组。当此选项处于禁用状态时，预处理器仍会检测异常并向规则引擎发送 DCE/RPC 数据，但可能会检测不出分片 DCE/RPC 数据中的漏洞。

尽管通过此选项可灵活选择是否对 DCE/RPC 流量进行分片重组，但大多数 DCE/RPC 漏洞都会尝试利用分片隐藏自己。禁用此选项将会忽略大多数已知漏洞，从而造成大量误报。

已达到内存限制 (Memory Cap Reached)

检测达到或超过分配给预处理器的最大内存限制的时间。当达到或超过最大内存上限时，预处理器会释放与造成内存上限事件的会话相关的所有待处理数据并忽略该会话的剩余部分。

您可以启用规则 133:1 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

SMB 会话上自动检测策略 (Auto-Detect Policy on SMB Session)

检测在 SMB `Session Setup AndX` 请求和响应中识别出的 Windows 或 Samba 版本。如果检测到的版本不同于为**策略 (Policy)** 配置选项配置的 Windows 或 Samba 版本，检测到的版本将会仅覆盖为该会话配置的版本。

例如，如果将**策略 (Policy)** 设置为 Windows XP，而预处理器检测到 Windows Vista，则预处理器将对该会话使用 Windows Vista 策略。其他设置仍然有效。

如果 DCE/RPC 传输不是 SMB（即传输协议为 TCP 或 UDP 时），则无法检测到版本，并且策略不能实现自动配置。

要启用此选项，请从下拉列表中选择以下其中一项：

- 选择**客户端 (Client)**，检查该策略类型的服务器到客户端流量。
- 选择**服务器 (Server)**，检查该策略类型的客户端到服务器流量。
- 选择**两者 (Both)**，检查该策略类型的服务器到客户端流量和客户端到服务器流量。

传统 SMB 检测模式 (Legacy SMB Inspection Mode)

如果启用了**传统 SMB 检测模式 (Legacy SMB Inspection Mode)**，则系统只会将 SMB 入侵规则应用于 SMB 版本 1 流量，并将 DCE/RPC 入侵规则应用于使用 SMB 版本 1 作为传输的 DCE/RPC 流量。

如果禁用此选项，系统会将SMB入侵规则应用于使用SMB版本1、2和3的流量，但会将DCE/RPC入侵规则应用于使用 SMB 作为 SMB 版本 1 传输的 DCE/RPC 流量。

相关主题

基本 content 和 protected_content 关键字参数 ，第 1517 页
概述：byte_jump 和 byte_test 关键字

DCE/RPC 基于目标的策略选项

在每个基于目标的策略中，都可以启用一个或多个TCP、UDP、SMB和RPC over HTTP传输。启用传输时，还必须指定一个或多个检测端口（即，已知用于传输 DCE/RPC 流量的端口）。

思科建议使用默认检测端口，这些端口可以是已知端口，也可以是各协议的常用端口。在非默认端口检测到 DCE/RPC 流量的情况下才可以添加端口。

可以在 Windows 基于目标的策略中为一个或多个传输指定任意组合的端口，以便与网络流量匹配，但是，在 Samba 基于目标的策略中只能为 SMB 传输指定端口。

注释 在基于目标的默认策略中必须至少启用一个 DCE/RPC 传输，除非已添加至少启用了一个传输的 DCE/RPC 基于目标的策略。例如，可能要为所有 DCE/RPC 实施指定主机且不将基于目标的默认策略部署到未指定的主机，在此情况下，不会为基于目标的默认策略启用传输。

或者，也可以启用和指定自动检测端口；预处理器会首先对这些端口进行测试，以确定它们是否传输 DCE/RPC 流量，仅在检测到 DCE/RPC 流量的情况下，预处理器才会继续进行处理。

启用自动检测端口时，请确保将端口范围设置为 1024 到 65535，以便覆盖整个临时端口范围。

请注意，仅对于传输检测端口尚未识别的端口才会出现自动检测。

对于“RPC over HTTP 代理自动检测端口”(RPC over HTTP Proxy Auto-Detect Ports) 选项或“SMB 自动检测端口”(SMB Auto-Detect Ports) 选项，不太可能会启用或指定自动检测端口，因为除非是在指定的默认检测端口上，否则任一端口出现流量的可能性极低甚至不可能出现。

每个基于目标的策略都允许指定以下各个选项。如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

网络 (Networks)

要部署DCE/RPC基于目标的服务器策略的主机IP地址。此外，当添加基于目标的策略时，命名“添加目标”(Add Target) 弹出窗口中的**服务器地址 (Server Address)** 字段。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。最多可以配置总共 255 个配置文件，包括默认策略。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字IP地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或 CIDR 块/前缀长度，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如，0.0.0.0/0 或 ::/0）。

策略

目标主机或受监控网段上主机使用的 Windows 或 Samba DCE/RPC 实现。

请注意，可以启用 **Auto-Detect Policy on SMB Session** 全局选项，以便在 DCE/RPC 传输是 SMB 时自动覆盖每个会话的此选项的设置。

SMB Invalid Shares

用于在尝试连接到指定的共享资源时，识别预处理器将检测的一个或多个 SMB 共享资源。您可以在逗号分隔列表中指定多个共享，或者可以将共享用引号引起来（旧版软件要求这样做，但现在不再有此要求），例如：

```
"C$", D$, "admin", private
```

启用 **SMB 端口 (SMB Ports)** 后，预处理器会检测 SMB 流量中的无效共享。

请注意，大多数情况下，对于被识别为无效共享的 Windows 命名的驱动器，应该在其后面附上一个美元符号。例如，将驱动器 C 标识为 C$ 或 "C$"。

另请注意，要检测 SMB 无效共享，还必须启用 **SMB 端口 (SMB Ports)** 或 **SMB 自动检测端口 (SMB Auto-Detect Ports)**。

可以启用规则 133:26 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

SMB Maximum AndX Chain

允许的链式 SMB AndX 命令的最大数量。通常，超过若干链式 AndX 命令即表示存在异常行为，可能代表有躲避行为。指定 1 表示不允许链式命令，指定 0 将会禁止检测链式命令数量。

请注意，预处理器会首先计算链式命令数量，如果随附的 SMB 预处理器规则已启用，并且链式命令数量等于或超过配置的值，预处理器将会生成事件。然后会继续进行处理。

⚠

注意 只有 SMB 协议专业人员可以修改 **SMB Maximum AndX Chains** 选项的设置。

可以启用规则 133:20 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

RPC proxy traffic only

启用 **RPC over HTTP 代理端口 (RPC over HTTP Proxy Ports)** 指示检测到的客户端 RPC over HTTP 流量只是代理流量还是可能包含其他 Web 服务器流量。例如，端口 80 可能传输代理流量和其他网络服务器流量。

此选项处于禁用状态时，将会同时传输代理流量和其他网络服务器流量。例如，如果服务器是专用代理服务器，请启用此选项。启用此选项后，预处理器会测试流量以确定其是否传输DCE/RPC，如果不是，预处理器将会忽略该流量，如果是，则继续进行处理。请注意，仅在已选择**RPC over HTTP 代理端口 (RPC over HTTP Proxy Ports)** 复选框的情况下，此选项才有用。

RPC over HTTP 代理端口 (RPC over HTTP Proxy Ports)

如果受管设备位于 DCE/RPC 客户端与 MicroSoft IIS RPC 代理服务器之间，可以使用此选项对 RPC over HTTP 通过每个指定端口传输的 DCE/RPC 流量启用检测。

启用此选项后，可以添加任意发现DCE/RPC流量的端口，但是这项操作一般并不必要，因为网络服务器通常使用默认端口传输 DCE/RPC 和其他流量。启用此选项后，不可以启用 **RPC over HTTP 代理自动检测端口 (RPC over HTTP Proxy Auto-Detect Ports)**，但如果检测到的客户端 RPC over HTTP 流量仅包含代理流量而不包含其他网络服务器流量，则可以启用**仅 PRC 代理流量 (RPC Proxy Traffic Only)**。

注释 如有可能，很少会选择此选项。

RPC over HTTP Server Ports

当 MicroSoft IIS RPC 代理服务器和 DCE/RPC 服务器位于不同的主机且设备监控这两个服务器之间流量时，对每个指定端口上通过 RPC over HTTP 传输的 DCE/RPC 流量启用检测。

启用此选项后，通常还应启用 **RPC over HTTP 服务器自动检测端口 (RPC over HTTP Server Auto-Detect Ports)**（端口范围介于 1025 到 65535 之间），即使不知道网络上是否存在任何代理网络服务器。请注意，RPC over HTTP 服务器端口有时会重新配置，在这种情况下，应该为此选项将重新配置的服务器端口添加到端口列表。

TCP 端口

对每个指定端口上 TCP 中的 DCE/RPC 流量启用检测。

合法 DCE/RPC 流量和漏洞可能使用多种端口，高于端口 1024 的其他端口很常用。启用此选项后，通常还应启用 **TCP 自动检测端口 (TCP Auto-Detect Ports)**（端口范围介于 1025 到 65535 之间），即使不知道网络上是否存在任何代理网络服务器。

UDP 端口

对每个指定端口上 UDP 中的 DCE/RPC 流量启用检测。

合法 DCE/RPC 流量和漏洞可能使用多种端口，高于端口 1024 的其他端口很常用。启用此选项后，通常还应启用 **UDP 自动检测端口 (UDP Auto-Detect Ports)**（端口范围介于 1025 到 65535 之间）。

SMB 端口 (SMB Ports)

对每个指定端口上 SMB 中的 DCE/RPC 流量启用检测。

可能会出现使用默认检测端口的 SMB 流量。其他端口很少见。通常使用默认设置。

请注意，可以启用 **Auto-Detect Policy on SMB Session** 全局选项，以便在 DCE/RPC 传输是 SMB 时自动覆盖为每个会话的目标策略配置的策略类型。

RPC over HTTP Proxy Auto-Detect Ports

如果受管设备位于 DCE/RPC 客户端与 MicroSoft IIS RPC 代理服务器之间，可以使用此选项对 RPC over HTTP 通过指定端口传输的 DCE/RPC 流量启用自动检测。

启用此选项后，通常需要指定介于 1025 到 65535 之间的端口范围，以覆盖整个临时端口范围。

RPC over HTTP 服务器自动检测端口 (RPC over HTTP Server Auto-Detect Ports)

当 MicroSoft IIS RPC 代理服务器和 DCE/RPC 服务器位于不同的主机且设备监控这两个服务器之间流量时，对指定端口上通过 RPC over HTTP 传输的 DCE/RPC 启用自动检测。

TCP 自动检测端口 (TCP Auto-Detect Ports)

对指定端口上 TCP 中的 DCE/RPC 流量启用自动检测。

UDP 自动检测端口 (UDP Auto-Detect Ports)

对每个指定端口上 UDP 中的 DCE/RPC 流量启用自动检测。

SMB 自动检测端口 (SMB Auto-Detect Ports)

对 SMB 中的 DCE/RPC 流量启用自动检测。

注释 如有可能，很少会选择此选项。

SMB 文件检查 (SMB File Inspection)

启用 SMB 流量检查以检测文件。您有以下选择：

- 选择**关闭 (Off)** 禁用文件检查。
- 选择**仅限 (Only)**，检查文件数据但不检查 SMB 中的 DCE/RPC 流量。选择此选项可以提高文件和 DCE/RPC 流量检查性能。
- 选择**打开 (On)**，检查 SMB 中的文件和 DCE/RPC 流量。选择此选项可能会影响性能。

以下各项不支持 SMB 流量检查：

- 单一 TCP 或 SMB 会话同时传输的文件
- 在多个 TCP 或 SMB 会话之间传输的文件
- 与非连续数据一起传输的文件（例如，协商了消息签名时）
- 与具有相同偏移量的不同数据一起传输的文件（与数据重叠）
- 在远程客户端打开用于编辑并由客户端保存到文件服务器的文件

SMB 文件检查深度 (SMB File Inspection Depth)

如果 **SMB 文件检查 (SMB File Inspection)** 设置为**仅限 (Only)** 或**打开 (On)**，此选项表示在 SMB 流量中检测到文件时检查的字节数。指定以下各项之一：

- 正值
- `0` 以检查整个文件
- `-1` 以禁用文件检查

在此字段中输入小于或等于访问控制策略中“高级”(Advanced)选项卡的“文件和恶意软件设置”(File and Malware Settings) 部分中定义的值。如果为此选项设置的值大于为**限制执行文件类型检测时检查到的字节数 (Limit the number of bytes inspected when doing file type detection)** 定义的值，则系统使用访问控制策略设置作为有效的最大值。

如果 **SMB File Inspection** 设置为 **Off**，此字段将被禁用。

与流量关联的 DCE/RPC 规则

大多数 DCE/RPC 预处理器规则都会针对 SMB、面向连接的 DCE/RPC 或无连接 DCE/RPC 流量中检测到的异常和规避技术触发。下表列出了可为各类流量启用的规则。

表 *211:* 与流量关联的 *DCE/RPC* 规则

交通	预处理器规则 GID:SID
中小企业	133:2 到 133:26，以及 133:48 到 133:59
面向连接的 DCE/RPC	133:27 到 133:39
检测无连接 DCE/RPC	133:40 至 133:43

配置 DCE/RPC 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

要配置DCE/RPC预处理器，可以修改控制预处理器工作方式的全局选项，并指定一个或多个基于目标的服务器策略，从而通过 IP 地址和运行的 Windows 或 Samba 版本识别网络上的 DCE/RPC 服务器。基于目标的策略配置还包括启用传输协议、指定将DCE/RPC流量传输到这些主机的端口以及设置其他服务器特定选项。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

开始之前

- 确认您要在基于目标的自定义策略中识别的网络匹配，或者是其父网络分析策略所处理的网络、区域和 VLAN 的子集。有关详细信息，请参阅网络分析策略的高级设置，第 2043 页。

过程

步骤 1 选择**策略 > 访问控制**，然后点击 **网络分析策略**或**策略 > 访问控制 > 入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击左侧导航面板中的 **Settings**。

步骤 5 如果**应用层预处理器(Application Layer Preprocessors)** 下的 **DCE/RPC 配置 (DCE/RPC Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **DCE/RPC 配置 (DCE/RPC Configuration)** 旁边的 **编辑**（）。

步骤 7 修改**全局设置 (Global Settings)** 部分中的选项；请参阅DCE/RPC 全局选项，第 2071 页。

步骤 8 有以下选项可供选择：

- 添加服务器配置文件 - 点击**服务器 (Server)** 旁边的 **添加**（）。在**服务器地址 (Server Address)** 字段中指定一个或多个 IP 地址，然后点击**确定 (OK)**。
- 删除服务器配置文件 - 点击策略旁边的 **删除**（）。
- 编辑服务器配置文件 - 在**服务器 (Servers)** 下点击配置文件的已配置地址，或者点击**默认值 (default)**。您可以修改**配置 (Configuration)** 部分中的任何设置；请参阅DCE/RPC 基于目标的策略选项，第 2073 页。

步骤 9 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成入侵事件，请启用 DCE/RPC 预处理器规则（GID 132 或 133）。有关详细信息，请参阅设置入侵规则状态，第 1488 页、DCE/RPC 全局选项，第 2071 页、DCE/RPC 基于目标的策略选项，第 2073 页和与流量关联的 DCE/RPC 规则，第 2077 页。
- 部署配置更改。

相关主题

文件和恶意软件检测性能和存储选项，第 1693 页
DCE/RPC 关键字，第 1565 页
管理层，第 1614 页
冲突和更改：网络分析和入侵策略，第 1459 页

DNS 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

DNS 预处理器会检查 DNS 域名服务器响应中是否存在以下具体漏洞：

- RData 文本字段中的溢出尝试
- 过时的 DNS 资源记录类型
- 试验性 DNS 资源记录类型

最常见的 DNS 域称服务器响应类型提供与促成响应的查询中域名对应的一个或多个 IP 地址。其他服务器响应类型提供邮件消息目的地或者可提供从最初查询的服务器无法获得的信息的域名服务器位置等等。

DNS 响应包括：

- 消息报头
- 包含一个或多个请求的问题部分
- 与问题部分中的请求对应的三个部分
  - 回答
  - 权限
  - 其他信息 (Additional Information)。

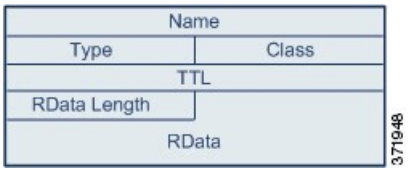
这三个部分中的响应反映域名服务器内保留的资源记录 (RR)。下表将介绍这三个部分。

表 *212: DNS* 域名服务器 *RR* 响应

部分	包含的内容	示例
回答	（可选）为查询提供明确答复的一个或多个资源记录	对应于域名的 IP 地址

部分	包含的内容	示例
权限 (Authority)	（可选）指向授权域名服务器的一个或多个资源记录	用于响应的授权域名服务器的名称
更多信息	（可选）提供与“答案”(Answer) 部分相关的其他信息的一个或多个资源记录	要查询的另一个服务器的 IP 地址

有许多类型的资源记录，全部遵循以下结构：



理论上，任何类型的资源记录均可用于域名服务器响应消息的回答、授权或附加信息部分。DNS 预处理器会检查这三个响应部分中的资源记录是否存在其会检测的漏洞。

“类型”(Type) 和 RData 资源记录字段对于 DNS 预处理器特别重要。“类型”(Type) 字段识别资源记录类型。RData（资源数据）字段提供响应内容。RData 字段的大小和内容因资源记录类型而异。

DNS 消息通常使用 UDP 传输协议，但如果消息类型需要可靠传输或者消息大小超过 UDP 能力，DNS 消息也会使用 TCP。DNS 预处理器会检查 UDP 和 TCP 流量中的 DNS 服务器响应。

DNS 预处理器不会检查在中途恢复的 TCP 会话，如果会话因丢包而丧失状态，DNS 预处理器将会停止检查。

DNS 预处理器选项

端口

此字段指定 DNS 预处理器应为 DNS 服务器响应监控的源端口。使用逗号分隔多个端口。

为 DNS 预处理器配置的典型端口为已知端口 53，DNS 域名服务器对在 UDP 和 TCP 中传输的 DNS 消息使用该端口。

检测 RData 文本字段中的溢出尝试 (Detect Overflow attempts on RData Text fields)

当资源记录类型为 TXT（文本）时，RData 字段为长度可变的 ASCII 文本字段。

如果选择此选项，系统将会检测条目 CVE-2006-3441 在 MITRE 的当前漏洞和风险数据库中识别出的特定漏洞。这是 Microsoft Windows 2000 Service Pack 4、Windows XP Service Pack 1、Windows XP Service Pack 2 和 Windows Server 2003 Service Pack 1 中的已知漏洞。攻击者可以利用该漏洞发送或者导致主机接收恶意域名服务器响应，导致 RData 文本字段长度计算错误，造成缓冲区溢出，最终全面控制主机。

如果网络上可能有主机运行尚未升级纠正该漏洞的操作系统，应该启用此选项。

您可以启用规则131:3生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

检测过时的 DNS RR 类型 (Detect Obsolete DNS RR Types)

RFC 1035 将多种资源记录类型识别为过时类型。由于这些是过时记录类型，因此，某些系统未对其进行说明，可能容易产生漏洞。在正常 DNS 响应中不会遇到这些记录类型，除非故意将网络配置为包含这些记录类型。

可以将系统配置为会检测过时的资源记录类型。下表列出并说明这些记录类型。

表 *213:* 过时的 *DNS* 资源记录类型

RR 类型	代码	说明
3	MD	邮件目的地
4	MF	邮件转发器

您可以启用规则131:1生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

检测试验性 DNS RR 类型 (Detecting Experimental DNS RR Types)

RFC 1035 将多种资源记录类型识别为试验性类型。由于这些是试验性记录类型，因此，某些系统未对其进行说明，可能容易产生漏洞。在正常 DNS 响应中不会遇到这些记录类型，除非故意将网络配置为包含这些记录类型。

可以将系统配置为会检测试验性资源记录类型。下表列出并说明这些记录类型。

表 *214:* 试验性 *DNS* 资源记录类型

RR 类型	代码	说明
7	MB	邮箱域名
8	MG	邮件组成员
9	MR	邮件重命名域名
10	NUL	空资源记录

您可以启用规则131:2生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

配置 DNS 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略** > **访问控制**，然后点击 **网络分析策略**或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **DNS 配置 (DNS Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **DNS 配置 (DNS Configuration)** 旁边的 **编辑**（）。

步骤 7 修改DNS 预处理器选项，第 2080 页中所述的设置。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成入侵事件，请启用 DNS 预处理器规则 (GID 131)。有关详细信息，请参阅设置入侵规则状态，第 1488 页和DNS 预处理器选项，第 2080 页。
- 部署配置更改。

相关主题

入侵和网络分析策略中的层，第 1607 页
冲突和更改：网络分析和入侵策略，第 1459 页

FTP/Telnet 解码器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

FTP/Telnet 解码器会分析 FTP 和 Telnet 数据流，对 FTP 和 Telnet 命令进行规范化，再由规则引擎处理这些命令。

全局 FTP 和 Telnet 选项

可以设置全局选项以确定 FTP/Telnet 解码器是否对数据包执行状态检查或无状态检查，是否检测加密 FTP 或 Telnet 会话，以及是否在遇到加密数据后继续检查数据流。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

状态性检查

如果选择此选项，FTP/Telnet 解码器将会保存状态，提供各个数据包的会话情景，并且仅检查重组的会话。如果清除此选项，将会在没有会话上下文的情况下分析每个数据包。

要检查 FTP 数据传输，必须选择此选项。

检测加密流量 (Detect Encrypted Traffic)

检测加密 Telnet 和 FTP 会话。

您可以启用规则 125:7 和 126:2 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

Continue to Inspect Encrypted Data

指示预处理器在数据流加密后持续检查数据流，以寻找可处理的最终解密数据。

Telnet 选项

可以通过 FTP/Telnet 解码器启用或禁用 Telnet 命令规范化，启用或禁用特定异常情况，以及设置允许的 Are You There (AYT) 攻击阈值。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

端口

指明要实现 Telnet 流量规范化的端口。Telnet 通常连接到 TCP 端口 23。可在此界面列出多个端口，端口之间用逗号分隔。

注意 由于加密流量 (SSL) 无法解码，因此，添加端口 22 (SSH) 可能会产生意外结果。

规范化 (Normalize)

对流向指定端口的 Telnet 流量进行规范化。

检测异常

允许检测没有对应 SE（下级协商终点）的 Telnet SB（下级协商起点）。

Telnet 支持以 SB（下级协商起点）开始并且必须以 SE（下级协商终点）结束的下级协商。但是，Telnet 服务器的某些实现将忽略无对应 SE 的 SB。这是异常行为，可能意味着存在躲避行为。由于 FTP 在控制接口使用 Telnet 协议，因此也容易受此行为影响。

如果在 Telnet 流量中检测到这种异常，可以启用规则 126:3 生成事件，并在内联部署中丢弃恶意数据包；如果在 FTP 命令通道中检测到这种异常，可以启用规则 125:9 生成事件。请参阅设置入侵规则状态，第 1488 页。

Are You There 攻击阈值数 (Are You There Attack Threshold Number)

检测超过指定阈值的连续 AYT 命令数量。思科建议将 AYT 阈值设置为不超过默认值的数值。

可以启用规则 126:1 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

服务器级别 FTP 选项

可以在多个 FTP 服务器上设置解码选项。创建的每个服务器配置文件都包含服务器 IP 地址以及应监控其流量的服务器端口。可以为特定服务器指定需要验证的 FTP 命令和可忽略的 FTP 命令，并可设置最大命令参数长度。还可以设置解码器应针对特定命令验证的具体命令语法，并可设置替代最大命令参数长度。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

网络 (Networks)

使用此选项可指定 FTP 服务器的一个或多个 IP 地址。

可以指定单个 IP 地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。最多可配置 1024 个字符，最多可指定 255 个配置文件（包括默认配置文件）。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

请注意，默认策略中的 default 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或地址块，并且不能在其他策略中将此设置留空或使用地址记法来表示 any（例如，0.0.0.0/0 或 ::/0）。

端口

使用此选项可指定受管设备应监控其流量的 FTP 服务器上的端口。可在此界面列出多个端口，端口之间用逗号分隔。端口 21 是已知的 FTP 流量端口。

文件获取命令 (File Get Commands)

使用此选项可定义用于从服务器向客户端传输文件的 FTP 命令。请勿改变此选项的值，除非支持人员指示执行此操作。

注意 请勿修改**文件获取命令 (File Get Commands)** 字段，除非支持人员指示执行此操作。

文件放置命令 (File Put Commands)

使用此选项可定义用于从客户端向服务器传输文件的 FTP 命令。请勿改变此选项的值，除非支持人员指示执行此操作。

注意 请勿修改**文件放置命令 (File Put Commands)** 字段，除非支持人员指示执行此操作。

附加 FTP 命令 (Additional FTP Commands)

使用此行可指定解码器应检测的其他命令。使用空格隔开其他命令。

可能需要添加的其他命令包括 XPWD、XCWD、XCUP、XMKD 和 XRMD。有关这些命令的详细信息，请参阅网络工作组发布的 RFC775《面向目录的 FTP 命令规范》。

默认最大参数长度 (Default Max Parameter Length)

在未设置替代最大参数长度的情况下，使用此选项可检测命令的最大参数长度。可以根据需要添加尽可能多的替代最大参数长度。

可以启用规则 125:3 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

替代最大参数长度 (Alternate Max Parameter Length)

使用此选项可指定要为其检测其他最大参数长度的命令，并指定这些命令的最大参数长度。点击**添加 (Add)** 可添加行，在添加的行中可指定其他最大参数长度，以便检测特定命令。

检查字符串格式攻击命令 (Check Commands for String Format Attacks)

使用此选项可检查指定命令的字符串格式攻击。

可以启用规则 125:5 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

命令有效性 (Command Validity)

使用此选项可为特定命令输入有效格式。点击 **Add** 可添加命令验证行。

可以启用规则 125:2 和 125:4 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

忽略 FTP 传输 (Ignore FTP Transfers)

使用此选项可禁用除数据传输通道状态检查之外的所有检查，从而提高 FTP 数据传输的性能。

注释 要检查数据传输，必须选择 FTP/Telnet **Stateful Inspection** 全局选项。

检测 FTP 命令内的 Telnet 转义代码 (Detect Telnet Escape Codes within FTP Commands)

使用此选项可检测何时在 FTP 命令通道上使用 Telnet 命令。

可以启用规则 125:1 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

忽略规范化过程中的擦除命令 (Ignore Erase Commands during Normalization)

如果选择了**检测 FTP 命令内的 Telnet 转义代码 (Detect Telnet Escape Codes within FTP Commands)**，使用此选项可在 FTP 流量规范化过程中忽略 Telnet 字符和行擦除命令。此选项的设置应与 FTP 服务器处理 Telnet 擦除命令的方式相匹配。请注意，新 FTP 服务器通常会忽略 Telnet 擦除命令，而旧服务器通常会进行处理。

故障排除选项：记录 FTP 命令验证配置 (Troubleshooting Option: Log FTP Command Validation Configuration)

支持人员可能要求您在故障排除呼叫期间配置系统，以打印为服务器列出的每个 FTP 命令的配置信息。

注意 请勿启用**记录 FTP 命令验证配置 (Log FTP Command Validation Configuration)**，除非支持人员指示执行此操作。

FTP 命令验证语句

为 FTP 命令创建验证语句时，可以通过使用空格隔开参数来指定一组替代参数。还可以在两个参数之间建立二进制 OR 关系，方法是使用竖线 (|) 隔开这两个参数。用方括号 ([]) 引起来的参数是可选参数。用花括号 ({}) 引起来的参数是必要参数。

可以创建 FTP 命令参数验证语句，以验证作为 FTP 通信一部分接收的参数的语法。

下表中列出的任何参数均可用于 FTP 命令参数验证语句中。

表 215: FTP 命令参数

使用的参数	出现的验证
`int`	所代表的参数必须是整数。
`number`	所代表的参数必须是 1 到 255 之间的整数。
`char` _chars	所代表的参数必须是单个字符，并且是 _chars 参数中指定的字符成员。 例如，使用验证语句 `char` SBC 验证定义 `MODE` 的命令有效性会检查 `MODE` 命令的参数是否包含字符 `S`（表示流模式）、字符 `B`（表示阻止模式）或字符 `C`（表示压缩模式）。
`date` _datefmt	如果 _datefmt 包含 `#`，所代表的参数必须是数字。 如果 _datefmt 包含 `C`，所代表的参数必须是字符。 如果 _datefmt 包含文字字符串，所代表的参数必须与文字字符串相匹配。
`string`	所代表的参数必须是字符串。
`host_port`	所代表的参数必须是有效的主机端口说明符（如网络工作组发布的 RFC959《文件传输协议规范》中所规定）。

可以根据需要结合使用上表中的语法来创建参数验证语句，以便在需要验证流量时能够正确验证每个 FTP 命令。

注释 如果要在 TYPE 命令中包含复杂的表达式，应将表达式放在空格之间。此外，应将每个操作数放在空格之间。例如，键入 `char A | B`，而非 `char A|B`。

相关主题

服务器级别 FTP 选项，第 2084 页
FTP 命令验证语句，第 2086 页

客户端级别 FTP 选项

使用这些选项可以配置自定义 FTP 客户端配置文件。如果某选项说明不包括预处理器规则，则该选项不与预处理器规则关联。

网络

使用此选项可指定 FTP 客户端的一个或多个 IP 地址。

可以指定单个 IP 地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。最多可指定 1024 个字符，最多可指定 255 个配置文件（包括默认配置文件）。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或地址块，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如，0.0.0.0/0 或 ::/0）。

最大响应长度 (Max Response Length)

使用此选项可以指定客户端接受的 FTP 命令的最大允许响应长度。这可以检测到基本的缓冲区溢出。

您可以启用规则 125:6 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

检测 FTP 退回尝试 (Detect FTP Bounce Attempts)

使用此选项可检测 FTP 退回攻击。

您可以启用规则 125:8 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

允许 FTP 退回至 (Allow FTP Bounce to)

使用此选项可配置包含附加主机以及这些主机上端口的列表，在这些主机上，FTP PORT 命令不应被视为 FTP 退回攻击。

检测 FTP 命令内的 Telnet 转义代码 (Detect Telnet Escape Codes within FTP Commands)

使用此选项可检测何时在 FTP 命令通道上使用 Telnet 命令。

可以启用规则 125:1 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

忽略规范化过程中的擦除命令 (Ignore Erase Commands During Normalization)

如果选择了**检测 FTP 命令内的 Telnet 转义代码 (Detect Telnet Escape Codes within FTP Commands)**，使用此选项可在 FTP 流量规范化过程中忽略 Telnet 字符和行擦除命令。此选项的设置应与 FTP 客户端处理 Telnet 擦除命令的方式相匹配。请注意，新 FTP 客户端通常会忽略 Telnet 擦除命令，而旧客户端通常会进行处理。

配置 FTP/Telnet 解码器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

可以为 FTP 客户端配置客户端配置文件，以监控来自客户端的 FTP 流量。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

开始之前

- 确认您要在基于目标的自定义策略中识别的任何网络匹配，或者是其父网络分析策略所处理的网络、区域和 VLAN 的子集。有关详细信息，请参阅网络分析策略的高级设置，第 2043 页。

过程

步骤 1 选择**策略 > 访问控制**，然后点击 **网络分析策略**或**策略 > 访问控制 > 入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **FTP 和 Telnet 配置 (FTP and Telnet Configuration)** 已禁用，请点击**已启用 (Enabled)**.。

步骤 6 点击 **FTP 和 Telnet 配置 (FTP and Telnet Configuration)** 旁边的 **编辑**（）。

步骤 7 设置**全局设置 (Global Settings)** 部分中的选项，如全局 FTP 和 Telnet 选项，第 2083 页中所述。

步骤 8 设置 **Telnet 设置 (Telnet Settings)** 部分中的选项，如Telnet 选项，第 2083 页中所述。

步骤 9 管理 FTP 服务器配置文件：

- 添加服务器配置文件 - 点击 **FTP 服务器 (FTP Server)** 旁边的 **添加**（）。在**服务器地址 (Server Address)** 字段中为客户端指定一个或多个 IP 地址，然后点击**确定 (OK)**。可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。最多可指定 1024 个字符，最多可配置 255 个策略（包括默认策略）。
- 编辑服务器配置文件 - 在 **FTP 服务器 (FTP Servers)** 下点击自定义配置文件的已配置地址，或者点击**默认值 (default)**。您可以修改**配置 (Configuration)** 部分中的设置；请参阅服务器级别 FTP 选项，第 2084 页。
- 删除服务器配置文件 - 点击配置文件旁边的 **删除**（）。

步骤 10 管理 FTP 客户端配置文件：

- 添加客户端配置文件 - 点击 **FTP 客户端 (FTP Client)** 旁边的 **添加**（）。在 **Client Address** 字段中为客户端指定一个或多个 IP 地址，然后点击 **OK**。可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。最多可指定 1024 个字符，最多可配置 255 个策略（包括默认策略）。

- 编辑客户端配置文件 - 在 **FTP 客户端 (FTP Client)** 下点击已添加配置文件的已配置地址，或者点击**默认值 (default)**。您可以修改“配置”(Configuration) 页面区域中的设置；请参阅客户端级别 FTP 选项，第 2087 页。
- 删除客户端配置文件 - 点击自定义配置文件旁边的 **删除**（ ）。

步骤 11 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成入侵事件，请启用 FTP 和 Telnet 预处理器规则（GID 125 和 126）。有关详细信息，请参阅设置入侵规则状态，第 1488 页。
- 部署配置更改。

相关主题

管理层，第 1614 页
冲突和更改：网络分析和入侵策略，第 1459 页

HTTP 检查预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

HTTP 检查预处理器负责以下工作：

- 解码和规范化发送到网络上 Web 服务器的 HTTP 请求以及来自该服务器的 HTTP 响应
- 将发送到 Web 服务器的消息分成 URI、非 cookie 报头、cookie 报头、方法和消息正文等组成部分，以提高与 HTTP 相关的入侵规则的性能
- 将从 Web 服务器接收到的消息分成状态代码、状态消息、非 set-cookie 报头、cookie 报头和响应正文等组成部分，以提高与 HTTP 相关的入侵规则的性能
- 检测可能的 URI 编码攻击
- 使规范化数据可用于附加规则处理
- 通过 JavaScript 等恶意脚本检测和预防攻击。

HTTP 流量可以各种格式进行编码，因此规则很难适当地进行检查。HTTP 检查可解码 14 种编码，从而确保 HTTP 流量获得可能的最佳检查。

可以在一个服务器上或者对服务器列表全局配置 HTTP 检查选项。

请注意，预处理器引擎无状态地执行 HTTP 规范化。也就是说，它会逐个数据包进行 HTTP 字符串规范化，并且只能处理已由 TCP 数据流预处理器重组的 HTTP 字符串。

全局 HTTP 规范化选项

为 HTTP 检查预处理器的全局 HTTP 选项用于控制预处理器的工作方式。如果由未指定为网络服务器的端口接收 HTTP 流量，可使用这些选项启用或禁用 HTTP 规范化。

请注意以下提示：

- 如果启用**无限压缩 (Unlimited Decompression)**，提交修改时，**最大压缩数据深度 (Maximum Compressed Data Depth)** 和**最大解压缩数据深度 (Maximum Decompressed Data Depth)** 选项将会自动设置为 65535。
- 当**最大压缩数据深度 (Maximum Compressed Data Depth)** 或**最大解压缩数据深度 (Maximum Decompressed Data Depth)** 的值在以下位置不同时，将会使用最高值：
  - 默认网络分析策略
  - 由同一访问控制策略中的网络分析规则调用的任何其他自定义网络分析策略

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

检测异常 HTTP 服务器 (Detect Anomalous HTTP Servers)

检测发送到未指定为网络服务器的端口或由其接收的 HTTP 流量。

注释 如果启用此选项，请确保在“HTTP 配置”(HTTP Configuration) 页面上的服务器配置文件中列出会接收 HTTP 流量的所有端口。如果不这样做，并且启用此选项以及随附的预处理器规则，则与该服务器之间的正常流量会生成事件。默认的服务器配置文件包含所有通常用于 HTTP 流量的端口，但如果修改了该配置文件，可能需要将这些端口添加到另一个配置文件中，以防止生成事件。

可以启用规则 120:1 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

检测 HTTP 代理服务器 (Detect HTTP Proxy Servers)

检测使用未由**允许 HTTP 代理使用 (Allow HTTP Proxy Use)** 选项定义的代理服务器的 HTTP 流量。

可以启用规则 119:17 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

Maximum Compressed Data Depth

启用 **Inspect Compressed Data**（或者 **Decompress SWF File (LZMA)**、**Decompress SWF File (Deflate)** 或 **Decompress PDF File (Deflate)**）后，设置要解压缩的压缩数据的最大大小。

Maximum Decompressed Data Depth

启用 **Inspect Compressed Data**（或者 **Decompress SWF File (LZMA)**、**Decompress SWF File (Deflate)** 或 **Decompress PDF File (Deflate)**）后，设置规范化解压缩数据的最大大小。

服务器级别 HTTP 规范化选项

可以为监控的每个服务器、全局地为所有服务器或者为服务器列表设置服务器级别选项。此外，可以使用预定义的服务器配置文件来设置这些选项，也可以单独设置它们来满足环境需求。可以使用这些选项或设置这些选项的其中一个默认配置文件来指定要规范化其流量的 HTTP 服务器端口、要规范化的服务器响应负载数量以及要规范化的编码的类型。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

网络 (Networks)

使用此选项可指定一个或多个服务器的 IP 地址。可以指定单个 IP 地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。

除总共最多 255 个配置文件（包括默认配置文件）的限制以外，还可以在 HTTP 服务器列表中包含最多 496 个字符（或大约 26 个条目），并为所有服务器配置文件指定总共最多 256 个地址条目。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或 CIDR 块/前缀长度，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如，0.0.0.0/0 或 ::/0）。

端口

预处理器引擎会对其 HTTP 流量进行规范化的端口。使用逗号分隔多个端口号。

过大的目录长度 (Oversize Dir Length)

检测长度超过指定值的 URL 目录。

当预处理器检测到长于指定长度的 URL 请求时，您可以启用规则 119:15 来生成事件并在内联部署中丢弃攻击性数据包。

客户端流量深度 (Client Flow Depth)

为要在**端口 (Ports)** 中定义的客户端 HTTP 流量中的原始 HTTP 数据包（包括报头和负载数据）中检查的规则指定字节数。如果规则中的 HTTP 内容规则选项检查请求消息的特定部分，客户端流量深度不适用。

可指定以下任意值：

- 正值，检查第一个数据包中的指定字节数。如果第一个数据包包含的字节数小于指定值，则检查整个数据包。请注意，指定值适用于分段和重组的数据包。

  另请注意，值 300 通常表示许多客户端请求报头末尾出现的大尺寸 HTTP Cookie 无需检查。

- 0 将会检查所有客户端流量，包括会话中的多个数据包，在必要时可超出字节上限。请注意，此值可能会影响性能。

- -1 将会忽略所有客户端流量。

服务器流量深度 (Server Flow Depth)

为要在**端口 (Ports)** 中指定的服务器端 HTTP 流量中的原始 HTTP 数据包中检查的规则指定字节数。**Inspect HTTP Responses** 处于禁用状态时，会检查原始报头和负载；**Inspect HTTP Response** 处于启用状态时，仅检查原始响应正文。

服务器流量深度为要在**端口 (Ports)** 中定义的服务器端 HTTP 流量中检查的规则指定会话中原始服务器响应数据的字节数。可以使用此选项来平衡 HTTP 服务器响应数据的性能和检查级别。如果规则中的 HTTP 内容规则选项检查响应消息的特定部分，服务器流量深度不适用。

不同于客户端流量深度，服务器流量深度为要检查的规则指定每个 HTTP 响应而非每个 HTTP 请求数据包的字节数。

可以指定以下任何内容：

- 正值：

  当**检查 HTTP 响应 (Inspect HTTP Responses)** 处于**启用**状态时，仅检查原始 HTTP 响应正文，不会检查非原始 HTTP 报头；当**检查 HTTP 响应 (Inspect HTTP Responses)** 处于启用状态时，还会同时检查解压缩数据。

  当**检查 HTTP 响应 (Inspect HTTP Responses)** 处于**禁用**状态时，会检查原始数据包报头和负载。

  如果会话包含的响应字节数小于指定值，规则将会根据需要在多个数据包中彻底检查给定会话中的所有响应数据包。如果会话包含的响应字节数大于指定值，规则将会根据需要在多个数据包中仅检查该会话中的指定字节数。

  请注意，流量深度值小可能会导致针对**端口 (Ports)** 中定义的服务器端流量的规则出现漏报。大多数这些规则针对的是，可能处于非报头数据的大约前 100 字节中的 HTTP 报头或内容。报头长度通常少于 300 字节，但报头大小可以不同。

  另请注意，指定值适用于分段和重组的数据包。

- 0 将会为**端口 (Ports)** 中定义的所有 HTTP 服务器端流量检查整个数据包（包括超过 65535 字节的会话中的响应数据）。

  请注意，此值可能会影响性能。

- -1：

  当**检查 HTTP 响应 (Inspect HTTP Responses)** 处于**启用**状态时，仅检查原始 HTTP 响应正文，不会检查原始 HTTP 响应正文。

当**检查 HTTP 响应 (Inspect HTTP Responses)** 处于**禁用**状态时，会忽略在**端口 (Ports)** 中定义的所有服务器端流量。

最大报头长度 (Maximum Header Length)

检测 HTTP 请求中长度超过指定最大字节数的报头字段；如果启用了**检查 HTTP 响应 (Inspect HTTP Responses)**，还会对 HTTP 响应执行此项检查。值为 0 将会禁用此选项。指定正值可启用此选项。

您可以启用规则 119:19 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。。

最大报头数 (Maximum Number of Headers)

检测 HTTP 请求中的报头数量超过此设置的情况。值为 0 将会禁用此选项。指定正值可启用此选项。

您可以启用规则 119:20 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。。

最大空格数 (Maximum Number of Spaces)

检测 HTTP 请求的折线中的空格数量等于或超过此设置的情况。值为 0 将会禁用此选项。指定正值可启用此选项。

您可以启用规则 119:26 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。。

HTTP 客户端正文提取深度 (HTTP Client Body Extraction Depth)

指定从 HTTP 客户端请求的消息正文提取的字节数。通过选择 `content` 或 `protected_content` 关键字 **HTTP Client Body** 选项，可以使用入侵规则检查提取的数据。

指定 -1 将会忽略客户端正文。指定 0 将会提取整个客户端正文。请注意，确定要提取的特定字节数可提高系统性能。另请注意，要使 **HTTP 客户端正文 (HTTP Client Body)** 选项在入侵规则中起作用，必须为此选项指定一个大于或等于 0 的值。

小数据块大小 (Small Chunk Size)

指定被认为是小数据块的数据块可包含的最大字节数。指定一个正值。值 0 将会禁用对异常连续小分片的检测。有关详细信息，请参阅**连续小数据块 (Consecutive Small Chunks)** 选项。

连续小数据块 (Consecutive Small Chunks)

指定在使用分块传输编码的客户端流量或服务器流量中，代表异常大数量的连续小数据块的数量。**小数据块大小 (Small Chunk Size)** 选项指定小数据块的最大大小。

例如，将**小数据块大小 (Small Chunk Size)** 设置为 10 并将**连续小数据块 (Consecutive Small Chunks)** 设置为 5，可检测包含 10 个或更少字节的 5 个连续数据块。

对于客户端流量和服务器流量，可分别启用预处理器规则 119:27 和 120:7 针对过多小数据块进行生成事件并在内联部署中丢弃攻击性数据包。如果 **Small Chunk Size** 已启用且此选项设置为 0 或 1，启用这些规则将会对每个指定大小或更小的数据块触发事件。

HTTP 方法 (HTTP Methods)

指定除预期系统会在流量中遇到的 GET 和 POST 以外的 HTTP 请求方法。使用逗号隔开多个值。

入侵规则将 `content` 或 `protected_content` 关键字与 **HTTP Method** 参数配合使用来搜索 HTTP 方法中的内容。如果在流量中遇到 GET、POST 或为此选项配置的方法以外的方法，您可以启用规则 119:31 来生成事件并在内联部署中丢弃攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

无警报 (No Alerts)

当随附的预处理器规则处于启用状态时禁用入侵事件。

注释 此选项**不会**禁用 HTTP 标准文本规则和共享对象规则。

规范化 HTTP 报头 (Normalize HTTP Headers)

当**检查 HTTP 响应 (Inspect HTTP Responses)** 处于启用状态时，启用请求和响应报头中非 cookie 数据的规范化。如果**未**启用**检查 HTTP 响应 (Inspect HTTP Responses)**，则启用请求和响应报头中整个 HTTP 报头（包括 cookie）的规范化。

检查 HTTP Cookie (Inspect HTTP Cookies)

允许从 HTTP 请求报头中提取 cookie。当**检查 HTTP 响应 (Inspect HTTP Responses)** 处于启用状态时，还允许从响应报头提取 set-cookie 数据。当不需要提取 cookie 时，禁用此选项可提高性能。

请注意，`Cookie:` 和 `Set-Cookie:` 报头名称、报头行中的前导空格以及终止报头行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。

HTTP 报头中的规范化 Cookie (Normalize Cookies in HTTP headers)

启用 HTTP 请求报头中 cookie 的规范化。当**检查 HTTP 响应 (Inspect HTTP Responses)** 处于启用状态时，还会启用响应报头中 set-cookie 数据的规范化。必须选择**检查 HTTP Cookie (Inspect HTTP Cookies)** 之后才能选择此选项。

允许 HTTP 代理使用 (Allow HTTP Proxy Use)

允许将受监控的 Web 服务器用作 HTTP 代理。此选项仅用于检查 HTTP 请求。

仅检查 URI (Inspect URI Only)

仅检查规范化 HTTP 请求数据包的 URI 部分。

检查 HTTP 响应 (Inspect HTTP Responses)

启用对 HTTP 响应的延展检查，从而使预处理器不仅会对 HTTP 请求消息进行解码和规范化，还会提取响应字段以供规则引擎进行检查。启用此选项后，系统会提取响应报头、正文、状态代码等；如果还启用了**检查 HTTP Cookie (Inspect HTTP Cookies)**，系统还会提取 set-cookie 数据。

您可以启用规则 120:2 和 120:3 来生成事件并在内联部署中丢弃攻击性数据包，如下所述：

表 *216:* 检查 *HTTP* 响应规则

规则	遇到以下情况时触发...
120:2	出现无效的 HTTP 响应状态代码。
120:3	HTTP 响应不包括内容长度或传输编码。

将 UTF 编码规范化为 UTF-8 (Normalize UTF Encodings to UTF-8)

如果启用了**检查 HTTP 响应 (Inspect HTTP Responses)**，此选项检测 HTTP 响应中的 UTF-16LE、UTF-16BE、UTF-32LE 和 UTF32-BE 编码，并将其规范化为 UTF-8。

当 UTF 规范化失败时，您可以启用规则 120:4 来生成事件并在内联部署中丢弃攻击性数据包。

检查压缩数据 (Inspect Compressed Data)

当**检查 HTTP 响应 (Inspect HTTP Responses)** 已启用时，此选项启用 HTTP 响应正文中的 gzip 和兼容 deflate 的压缩数据的解压，以及对规范化解压缩数据的检查。系统将检查分块和非分块 HTTP 响应数据。系统会根据需要逐一检查多个数据包中的解压缩数据；也就是说，系统不会将来自不同数据包的解压缩数据合并来进行检查。当达到**最大压缩数据深度 (Maximum Compressed Data Depth)** 或**最大解压缩数据深度 (Maximum Decompressed Data Depth)** 中指定的值，或者达到压缩数据末尾时，解压缩将会结束。当达到**服务器流量深度 (Server Flow Depth)** 中指定的值时，对解压缩数据的检查将会结束，除非还选择了**无限制解压缩 (Unlimited Decompression)**。您可以使用 `file_data` 规则关键字来检查解压缩数据。

您可以启用规则 120:6 和 120:24 来生成事件并在内联部署中丢弃攻击性数据包，如下所述：

表 *217:* 检查压缩 *HTTP* 响应规则

规则	遇到以下情况时触发...
120:6	压缩 HTTP 响应的解压缩失败。
120:24	压缩 HTTP 响应的部分解压缩失败。

无限解压

当启用**检查压缩数据 (Inspect Compressed Data)**（或者 **解压缩 SWF 文件 (LZMA) [Decompress SWF File (LZMA)]**、**解压缩 SWF 文件 (Deflate) [Decompress SWF File (Deflate)]** 或**解压缩 PDF 文件 (Deflate) [Decompress PDF File (Deflate)]**）时，会跨多个数据包覆盖**最大压缩数据深度 (Maximum Compressed Data Depth)**；也就是说，此选项支持跨多个数据包无限制解压缩。请注意，启用此选项不会影响单个数据包中的**最大压缩数据深度 (Maximum Compressed Data Depth)** 或**最大解压缩数据深度 (Maximum Decompressed Data Depth)**。另请注意，如果启用此选项，确认修改时**最大压缩数据深度 (Maximum Compressed Data Depth)** 和**最大解压缩数据深度 (Maximum Decompressed Data Depth)** 将会设置为 65535。

规范化 Javascript (Normalize Javascript)

当**检查 HTTP 响应 (Inspect HTTP Responses)** 已启用时，此选项启用对 HTTP 响应正文中 Javascript 的检测和规范化。预处理器会对模糊 JavaScript 数据（例如，unescape 函数、decodeURI 函数和 String.fromCharCode 方法）进行规范化。预处理器会对 unescape、decodeURI 和 decodeURIComponent 函数中的以下编码进行规范化：

- %XX
- %uXXXX
- 0xXX
- \xXX
- \uXXXX

预处理器检测连续空格，并将其规范化为一个空格。此选项处于启用状态时，配置字段允许您指定模糊 Javascript 数据中允许的最大连续空格数量。可输入 1 到 65535 之间的值。值 0 将会禁止生成事件，不管与该字段相关的预处理器规则 (120:10) 是否启用。

预处理器还会对 Javascript 加号 (+) 运算符进行规范化，并使用该运算符连接字符串。

您可以使用 `file_data` 入侵规则关键字使入侵规则指向规范化的 Javascript 数据。

您可以启用规则 120:9、120:10 和 120:11 以生成事件并在内联部署中丢弃攻击性数据包，如下所示：

表 *218:* 规范化 *Javascript* 选项规则

规则	遇到以下情况时触发...
120:9	预处理器内的模糊级别大于或等于 2。
120:10	Javascript 模糊数据中的连续空格数量大于或等于为允许的最大连续空格数量配置的值。
120:11	经转义或编码的数据包含多种类型的编码。

“解压缩 SWF 文件 (LZMA)” (Decompress SWF File [LZMA]) 和“解压缩 SWF 文件 (Deflate)” (Decompress SWF File [Deflate])

启用 **HTTP Inspect Responses** 后，这些选项解压缩位于 HTTP 请求的 HTTP 响应主体中文件的压缩部分。.

注释 您只能解压缩在 HTTP GET 响应中找到的文件的压缩部分。

- **Decompress SWF File (LZMA)** 解压缩 Adobe ShockWave Flash (`.swf`) 文件的 LZMA 兼容压缩部分。

- **Decompress SWF File (Deflate)** 解压缩 Adobe ShockWave Flash (`.swf`) 文件的 deflate 兼容压缩部分。

当达到**最大压缩数据深度 (Maximum Compressed Data Depth)** 或**最大解压缩数据深度 (Maximum Decompressed Data Depth)** 中指定的值，或者达到压缩数据末尾时，解压缩将会结束。当达到**服务器流量深度 (Server Flow Depth)** 中指定的值时，对解压缩数据的检查将会结束，除非还选择了**无限制解压缩 (Unlimited Decompression)**。您可以使用 `file_data` 入侵规则关键字来检查解压缩数据。

您可以启用规则 120:12 和 120:13 以生成事件并在内联部署中丢弃攻击性数据包，如下所示：

表 *219*: 解压缩 *SWF* 文件选项规则

规则	遇到以下情况时触发...
120:12	deflate 文件解压缩失败。
120:13	LZMA 文件解压缩失败。

Decompress PDF File (Deflate)

检查 HTTP 响应 (Inspect HTTP Responses) 处于启用状态时，**解压缩 SWF 文件 (Deflate) (Decompress PDF File [Deflate])** 会解压缩位于 HTTP 请求的 HTTP 响应主体中可移植文档格式 (`.pdf`) 文件的 deflate 兼容压缩部分。系统只能使用 `/FlateDecode` 数据流过滤器解压缩 PDF 文件。不支持其他数据流过滤器（包括 `/FlateDecode /FlateDecode`）。

注释 您只能解压缩在 HTTP GET 响应中找到的文件的压缩部分。

当达到**最大压缩数据深度 (Maximum Compressed Data Depth)** 或**最大解压缩数据深度 (Maximum Decompressed Data Depth)** 中指定的值，或者达到压缩数据末尾时，解压缩将会结束。当达到**服务器流量深度 (Server Flow Depth)** 中指定的值时，对解压缩数据的检查将会结束，除非还选择了**无限制解压缩 (Unlimited Decompression)**。您可以使用 `file_data` 入侵规则关键字来检查解压缩数据。

您可以启用规则 120:14、120:15、120:16 和 120:17 以生成事件并在内联部署中丢弃攻击性数据包，如下所示：

表 *220*: 解压缩 *PDF* 文件 *(Deflate)* 选项规则

规则	遇到以下情况时触发...
120:14	文件解压缩失败。
120:15	由于压缩类型不受支持，文件解压缩失败。
120:16	由于 PDF 数据流过滤器不受支持，文件解压缩失败。
120:17	文件解析失败。

Extract Original Client IP Address

在入侵检查过程中启用原始客户端IP地址的检查。系统从您在**XFF 报头优先级 (XFF Header Priority)**选项中定义的X-Forwarded-For (XFF)、True-Client-IP 或自定义 HTTP 报头提取原始客户端 IP 地址。您可以在入侵事件表中查看提取的原始客户端 IP 地址。

您可以启用规则 119:23、119:29 和 119:30 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。。

XFF Header Priority

指定当 HTTP 请求中存在多个报头时，系统处理原始客户端 IP 报头的顺序。默认情况下，系统会检查 X-Forwarded-For (XFF) 报头，然后检查 True-Client-IP 报头。使用每种报头类型旁边的向上和向下箭头图标调整其优先级。

此选项还允许您指定除 XFF 或 True-Client-IP 以外的原始客户端 IP 报头来进行提取和评估。点击**添加 (Add)**以将自定义报头名称添加到优先级列表中。系统仅支持与 XFF 或 True-Client-IP 报头使用相同语法的自定义报头。

配置此选项时请记住以下几点：

- 在评估原始客户端 IP 地址报头时，系统同时对访问控制和入侵检查使用此优先顺序。
- 如果存在多个原始客户端 IP 报头，则系统仅处理优先级最高的报头。
- XFF 报头包含 IP 地址列表，表示请求所通过的代理服务器。为防止欺骗，系统使用列表中的最后一个 IP 地址（即受信任代理附加的地址）作为原始客户端 IP 地址。

日志 URI (Log URI)

允许从 HTTP 请求数据包提取原始 URI（如果有），并将该 URI 与为会话生成的所有入侵事件相关联。

启用此选项后，可以在入侵事件表视图的“HTTP URI”列中显示提取的 URI 的前 50 个字符。可以在数据包视图中显示完整的 URI（最多 2048 字节）。

日志主机名 (Log Hostname)

允许从 HTTP 请求主机报头中提取主机名（如果有），并将该主机名与为会话生成的所有入侵事件相关联。如果存在多个主机报头，系统将会从第一个报头中提取主机名。

启用此选项后，可以在入侵事件表视图的“HTTP 主机名”(HTTP Hostname) 列中显示提取的主机名的前 50 个字符。可以在数据包视图中显示完整的主机名（最多 256 字节）。

您可以启用规则 119:25 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

请注意，如果启用了规则 119:24，它将在于 HTTP 请求中检测到多个主机报头时触发，而不管该选项的设置为何。

配置文件

指定为 HTTP 流量规范化的编码的类型。系统提供了一个适用于大多数服务器的默认配置文件、适用于 Apache 服务器和 IIS 服务器的若干默认配置文件以及自定义默认设置，您可以对这些设置进行自定义，以满足受监控流量的需求：

- 选择 **All** 将会使用适用于所有服务器的标准默认配置文件。
- 选择 **IIS** 将会使用系统提供的 IIS 配置文件。
- 选择 **Apache** 将会使用系统提供的 Apache 配置文件。
- 选择**自定义 (Custom)** 将会创建您自己的服务器配置文件。

服务器级别 HTTP 规范化编码选项

将 HTTP 服务器级别**配置文件 (Profile)** 选项设置为 `Custom` 时，可以指定为 HTTP 流量规范化的编码类型，并启用 HTTP 预处理器规则以根据包含不同编码类型的流量生成事件。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

ASCII 编码 (ASCII Encoding)

对编码的 ASCII 字符进行解码，并指定规则引擎是否生成关于 ASCII 编码 URI 的事件。

可以启用规则 119:1 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

UTF-8 编码 (UTF-8 Encoding)

对 URI 中的标准 UTF-8 Unicode 序列进行解码。

可以启用规则 119:6 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

Microsoft %U Encoding

对 IIS %u 编码方案进行解码，该编码方案使用 %u，后跟四个字符；其中这四个字符是与 IIS Unicode 代码点相关的十六进制编码值。

提示 合法的客户端很少使用 %u 编码，因此思科建议对使用 %u 编码的 HTTP 流量进行解码。

可以启用规则 119:3 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

裸字节 UTF-8 编码 (Bare Byte UTF-8 Encoding)

对裸字节编码进行解码（这种解码方法使用非 ASCII 字符作为解码 UTF-8 值时的有效值）。

提示 裸字节编码允许用户模拟 IIS 服务器和正确解释非标准编码。思科建议启用此选项，因为合法的客户端不以这种方式编码 UTF-8。

可以启用规则 119:4 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

Microsoft IIS 编码 (Microsoft IIS Encoding)

使用 Unicode 代码点映射进行解码。

提示 思科建议启用此选项，因为它主要出现在攻击和躲避尝试中。

可以启用规则 119:7 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

双重编码 (Double Encoding)

通过在每个进行解码的请求 URI 中形成两条通道，解码 IIS 双编码流量。思科建议启用此选项，因为它通常只存在于攻击情况中。

可以启用规则 119:2 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

多斜杠混淆 (Multi-Slash Obfuscation)

将连续的多个斜杠规范化为一个斜杠。

可以启用规则 119:8 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

IIS 反斜杠混淆 (IIS Backslash Obfuscation)

将反斜线规范化为前斜线。

可以启用规则 119:9 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

目录遍历

对目录遍历和自引用目录进行规范化。如果启用随附的预处理器规则来生成关于此类型流量的事件，可能会产生误报，因为有些网站使用目录遍历来引用文件。

可以启用规则 119:10 和 119:11 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

制表符混淆 (Tab Obfuscation)

规范化有关对空格分隔符使用制表符的非 RFC 标准。Apache 及其他非 IIS Web 服务器在 URL 中使用制表符 (0x09) 作为分隔符。

注释 无论此选项的配置如何，如果制表符前有空格字符 (0x20)，HTTP 检查预处理器都将制表符看作空格。

可以启用规则 119:12 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

RFC 分隔符无效 (Invalid RFC Delimiter)

规范化 URI 数据中的换行符 (\n)。

可以启用规则 119:13 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

Webroot 目录遍历 (Webroot Directory Traversal)

检测穿过 URL 中初始目录的目录遍历。

可以启用规则 119:18 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

制表符 URI 分隔符 (Tab URI Delimiter)

允许使用制表符 (0x09) 作为 URI 的分隔符。Apache、IIS 较新版本以及某些其他 Web 服务器在 URL 中使用制表符作为分隔符。

注释 无论此选项的配置如何，如果制表符前有空格字符 (0x20)，HTTP 检查预处理器都将制表符看作空格。

非 RFC 字符 (Non-RFC characters)

检测在相应字段中添加的并出现在传入或传出 URI 数据中的非 RFC 字符列表。当修改此字段时，请使用代表该字节字符的十六进制格式。如果要配置此选项，在配置此选项时，请小心设置此值。使用很常见的字符可能会使您面临大量事件。

可以启用规则 119:14 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

最大块编码大小 (Max Chunk Encoding Size)

检测 URI 数据中异常大的数据块的大小。

可以启用规则 119:16 和 119:22 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

禁用管道解码 (Disable Pipeline Decoding)

对于管道请求禁用 HTTP 解码。当此选项被禁用时，性能会提升，因为系统不会解码或分析管道中等待的 HTTP 请求，只是使用通用模式匹配对它们进行检测。

非严格 URI 解析 (Non-Strict URI Parsing)

允许非严格的 URI 解析。应仅在接受“GET /index.html abc xo qr \n”格式的非标准 URI 的服务器上使用此选项。使用此选项时，解码器会假定 URI 位于第一个空格与第二个空格之间，即使第二个空格之后没有有效的 HTTP 标识符。

扩展的 ASCII 编码 (Extended ASCII Encoding)

允许解析 HTTP 请求 URI 中的扩展 ASCII 字符。请注意，此选项仅可用于自定义服务器配置文件，在为 Apache、IIS 或所有服务器提供的默认配置文件中不可用。

相关主题

概述：HTTP content 和 protected_content 关键字参数，第 1521 页
file_data 关键字，第 1604 页

配置 HTTP 检查预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

开始之前

- 确认您要在基于目标的自定义策略中识别的任何网络匹配，或者是其父网络分析策略所处理的网络、区域和 VLAN 的子集。有关详细信息，请参阅网络分析策略的高级设置，第 2043 页。

过程

步骤 1 选择**策略 > 访问控制**，然后点击 **网络分析策略**或**策略 > 访问控制 > 入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **HTTP 配置 (HTTP Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **HTTP 配置 (HTTP Configuration)** 旁边的 **编辑**（）。

步骤 7 修改“全局设置”(Global Settings) 页面区域中的选项；请参阅全局 HTTP 规范化选项，第 2091 页。

步骤 8 此时，您有三种选择：

- 添加服务器配置文件 - 点击**服务器 (Servers)** 部分中的 **添加**（）。在**服务器地址**字段中为客户端指定一个或多个 IP 地址，然后点击**确定**。可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。最多可在列表中包含 496 个字符，为所有服务器配置文件总共最多可指定 256 个地址条目，总共最多可创建 255 个配置文件（包括默认配置文件）。
- 编辑服务器配置文件 - 在**服务器 (Servers)** 下点击已添加配置文件的已配置地址，或者点击**默认值 (default)**。您可以修改**配置 (Configuration)** 部分中的任何设置；请参阅服务器级别 HTTP 规范化选项，第 2092 页。如果为**配置文件 (Profile)** 值选择**自定义 (Custom)**，还可以修改服务器级别 HTTP 规范化编码选项，第 2100 页中所述的编码选项。
- 删除服务器配置文件 - 点击自定义配置文件旁边的 **删除**（）。

步骤 9 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果需要生成事件并在内联部署中丢弃攻击性数据包，请启用 HTTP 预处理器规则 (GID 119)。有关详细信息，请参阅设置入侵规则状态，第 1488 页。
- 部署配置更改。

相关主题

管理层，第 1614 页
冲突和更改：网络分析和入侵策略，第 1459 页

其他 HTTP 检查预处理器规则

可以启用下表的 **Preprocessor Rule GID:SID** 列中的规则，为与特定配置选项无关的 HTTP 检查预处理器规则生成事件。

表 *221:* 其他 *HTTP* 检查预处理器规则

预处理器规则 GID:SID	触发场景..
119:21	HTTP 请求报头包含多于一个 `content-length` 字段时。
119:24	HTTP 请求包含多于一个主机报头时。
119:28	HTTP POST 方法既没有 `content-length` 报头，也没有数据块 `transfer-encoding`。
119:32	在流量中遇到 HTTP 0.9 时。请注意，还必须启用“TCP 流配置”(TCP Stream Configuration)。
119:33	HTTP URI 包含非转义空格时。
119:34	TCP 连接包含 24 个或更多管道化 HTTP 请求时。
120:5	HTTP 响应流量中遇到 UTF-7 编码时；UTF-7 应仅在需要 7 位奇偶校验的情况下出现，例如，SMTP 流量。
120:8	`content-length` 或数据库大小无效。
120:18	在客户端请求之前发生 HTTP 服务器响应时。
120:19	HTTP 响应包括多个内容长度时。
120:20	HTTP 响应包括多个内容编码时。
120:25	HTTP 响应包括无效报头折叠时。
120:26	在 HTTP 响应报头之前出现乱码行时。
120:27	HTTP 响应不包括报头尾部时。
120:28	数据块大小无效时，或者数据块大小后跟乱码字符时。

Sun RPC 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

远程过程调用 (RPC) 规范化采用分片 RPC 记录，并将这些记录规范化为单个记录，以便规则引擎可以检查完整的记录。例如，攻击者可能会试图发现运行 RPC `admind` 的端口。某些 UNIX 主机使用 RPC `admind` 执行远程分布式系统任务。如果主机执行的身份验证强度较弱，恶意用户可能会控制远

程管理。Snort ID (SID) 为 575 的标准文本规则 (GID: 1) 会搜索特定位置中的内容，并识别不适当的 `portmap GETPORT` 请求，以此来检测这种攻击。

Sun RPC 预处理器选项

端口

指定要规范化其流量的端口。可在此界面列出多个端口，端口之间用逗号分隔。典型的 RPC 端口为 111 和 32771。如果网络将 RPC 流量发送到其他端口，可考虑添加这些端口。

检测分片 RPC 记录 (Detect fragmented RPC records)

检测 RPC 分片记录。

您可以启用规则 106:1 和 106:5 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

检测一个数据包中的多个记录 (Detect multiple records in one packet)

在每个数据包（或重组数据包）中检测多于一个 RPC 请求。

可以启用规则 106:2生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

检测超出一个分片的片段的记录和

检测超过当前数据包长度的重组分片记录长度。

可以启用规则 106:3生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

检测超过一个数据包长度的单个分片记录

检测部分记录

可以启用规则 106:4生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

配置 Sun RPC 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择策略 > 访问控制，然后点击 网络分析策略或策略 > 访问控制 > 入侵，然后点击 网络分析策略。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **Sun RPC 配置 (Sun RPC Configuration)** 被禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **Sun RPC 配置 (Sun RPC Configuration)** 旁边的 **编辑**（）。

步骤 7 修改Sun RPC 预处理器选项，第 2106 页中所述的设置。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果希望生成事件并在内联部署中丢弃攻击性数据包，则请启用 Sun RPC 预处理器规则 (GID 106)。有关详细信息，请参阅设置入侵规则状态，第 1488 页。
- 部署配置更改。

相关主题

管理层，第 1614 页
冲突和更改：网络分析和入侵策略，第 1459 页

SIP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

会话初始协议 (SIP) 为客户端应用（例如网络电话、多媒体会议、即时消息、网络游戏和文件传输）的一个或多个用户提供一个或多个会话的呼叫建立、修改和取消。每个 SIP 请求中的“方法”(*method*)

字段识别请求的目的，请求 URI 则指定发送请求的目的地。每个 SIP 响应中的状态代码指明请求操作的结果。

使用 SIP 建立呼叫后，实时传输协议 (RTP) 负责随后的音频和视频通信；会话的此部分有时又称为呼叫通道、数据通道或音频/视频数据通道。对于数据通道参数协商、会话公告和会话邀请，RTP 在 SIP 消息正文中使用会话描述协议 (SDP)。

SIP 预处理器负责：

- 解码和分析 SIP 2.0 流量
- 提取包括 SDP 数据（如果有）在内的 SIP 报头和消息正文，并将提取的数据传递给规则引擎，以进行进一步检查
- 在检测到以下条件并且相应的预处理器规则已启用的情况下，将会生成事件：
  - SIP 数据包中存在异常和已知漏洞
  - 调用序列乱序和无效
- 或者，忽略呼叫通道

预处理器会根据在 SDP 消息中识别出的端口来识别 RTP 通道（该消息嵌入在 SIP 消息正文中），但预处理器不提供 RTP 协议检查。

使用 SIP 预处理器时，请注意以下几点：

- UDP 通常传输 SIP 支持的媒体会话。UDP 数据流预处理为 SIP 预处理器提供 SIP 会话跟踪。
- SIP 规则关键字允许您指向 SIP 数据包报头或消息正文，并限制为对特定 SIP 方法或状态代码进行数据包检测。

SIP 预处理器选项

对于以下选项，您可以指定从 1 到 65535 字节的正值或 0，以禁用选项的事件生成（无论是否启用关联规则）。

- **Maximum Request URI Length**
- **Maximum Call ID Length**
- **Maximum Request Name Length**
- **Maximum From Length**
- **Maximum To Length**
- **Maximum Via Length**
- **Maximum Contact Length**
- **Maximum Content Length**

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

端口

指定用于检查 SIP 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口号。

检查方法 (Methods to Check)

指定 SIP 检测方法。可以指定以下当前定义的任何 SIP 方法：

```
ack, benotify, bye, cancel, do, info, invite, join, message,
notify, options, prack, publish, quath, refer, register,
service, sprack, subscribe, unsubscribe, update
```

方法不区分大小写。方法名称可以包含字母字符、数字和下划线字符。不允许任何其他特殊字符。使用逗号隔开多种方法。

由于将来可能会定义新的 SIP 方法，因此，配置可以包含当前未定义的字母字符串。系统最多支持 32 种方法，包括 21 种当前定义的方法和 11 种其他方法。系统将忽略您可能配置的任何未定义的方法。

请注意，除为此选项指定的任何方法外，总共 32 种方法包括入侵规则中使用 `sip_method` 关键字指定的方法。

会话中的最大对话数 (Maximum Dialogs within a Session)

指定数据流会话中允许的最大对话数量。如果创建的对话框数量超过该数量，则最早的对话框会被丢弃，直至对话框数量不超过指定的最大数量。可指定 1 到 4194303 之间的整数。

您可以启用规则 140:27 生成事件并在内联部署中丢弃此选项的攻击性数据包。请参阅设置入侵规则状态，第 1488 页。

最大请求 URL 长度 (Maximum Request URI Length)

指定 Request-URI 报头字段中允许的最大字节数。如果启用了规则 140:3，则更长的“URI”生成事件并在内联部署中丢弃攻击性数据包。请求 URI 字段指明请求的目标路径或目标页面。

最大调用 ID 长度 (Maximum Call ID Length)

指定请求或响应 Call-ID 报头字段中允许的最大字节数。如果启用了规则 140:5，则更长的“调用 ID”生成事件并在内联部署中丢弃攻击性数据包。“调用 ID”字段唯一地识别请求和响应中的 SIP 会话。

最大请求名称长度 (Maximum Request Name Length)

指定请求名称中允许的最大字节数（该名称是CSeq事务标识符中指定的方法的名称）。如果启用了规则 140:7，则更长的“请求名称”生成事件并在内联部署中丢弃攻击性数据包。

最大发件人长度 (Maximum From Length)

指定请求或响应“发件人”(From)报头字段中允许的最大字节数。如果启用了规则140:9，则更长的“发件人”生成事件并在内联部署中丢弃攻击性数据包。“发件人”(From) 字段识别消息发起方。

最大收件人长度 (Maximum To Length)

指定请求或响应“收件人”(To) 报头字段中允许的最大字节数。如果启用了规则 140:11，则更长的“收件人”生成事件并在内联部署中丢弃攻击性数据包。“收件人”(To) 字段识别消息收件人。

最大路径长度 (Maximum Via Length)

指定请求或响应“路径”(Via) 报头字段中允许的最大字节数。如果启用了规则 140:13，则更长的“通过”生成事件并在内联部署中丢弃攻击性数据包。“路径”(Via)字段提供请求的路径，并在响应中提供回执信息。

最大联系人长度 (Maximum Contact Length)

指定请求或响应“联系人”(Contact) 报头字段中允许的最大字节数。如果启用了规则 140:15，则更长的“联系人”生成事件并在内联部署中丢弃攻击性数据包。“联系人”(Contact) 字段提供用以指定与后续消息进行联系的位置的 URI。

最大内容长度 (Maximum Content Length)

指定在请求或响应消息正文的内容中允许的最大字节数。如果启用了规则 140:16，则更长的内容生成事件并在内联部署中丢弃攻击性数据包。

忽略音频/视频数据通道 (Ignore Audio/Video Data Channel)

启用和禁用数据通道流量检查。请注意，如果启用了此选项，预处理器会继续检查其他非数据通道 SIP 流量。

相关主题

SIP 关键字，第 1568 页

配置 SIP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择**策略**>**访问控制**，然后点击 **网络分析策略**或**策略** >**访问控制**>**入侵**，然后点击 **网络分析策略**。

注释　如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **SIP 配置 (SIP Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **SIP 配置 (SIP Configuration)** 旁边的 **编辑**（）。

步骤 7 修改SIP 预处理器选项，第 2108 页中所述的选项。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成事件并在内联部署中丢弃攻击性数据包，请启用 SIP 预处理器规则 (GID 140)。有关详细信息，请参阅设置入侵规则状态，第 1488 页。
- 部署配置更改。

相关主题

管理层，第 1614 页
冲突和更改：网络分析和入侵策略，第 1459 页

其他 SIP 预处理器规则

下表中的 SIP 预处理器规则与特定配置选项无关。与其他 SIP 预处理器规则一样，如果要使这些规则生成事件并在内联部署中丢弃攻击性数据包，必须启用这些规则。

表 *222:* 其他 *SIP* 预处理器规则

预处理器规则 GID:SID	触发场景..
140:1	预处理器监控系统允许的最大 SIP 会话数量。
140:2	必填的 Request_URI 字段在 SIP 请求中为空。
140:4	Call-ID 报头字段在 SIP 请求或响应中为空。
140:6	SIP 请求或响应 CSeq 字段中的序列号值不是小于 231 的 32 位无符号整数。

预处理器规则 GID:SID	触发场景..
140:8	From 报头字段在 SIP 请求或响应中为空。
140:10	To 报头字段在 SIP 请求或响应中为空。
140:12	Via 报头字段在 SIP 请求或响应中为空。
140:14	必填的 Contact 报头字段在 SIP 请求或响应中为空。
140:17	UDP 流量中的单个 SIP 请求或响应数据包包含多条消息。请注意，旧版本 SIP 支持多条消息，但 SIP 2.0 仅在每个数据包中支持一条消息。
140:18	UDP 流量中的 SIP 请求或响应中消息正文的实际长度与 SIP 请求或响应中的 Content-Length 报头字段中指定的值不匹配。
140:19	预处理器无法识别 SIP 响应的 CSeq 字段中的方法名称。
140:20	SIP 服务器不质询经过身份验证的邀请消息。请注意，当有 InviteReplay 计费攻击时，会出现这种情况。
140:21	在设置调用之前，会话信息发生更改。请注意，当有 FakeBusy 计费攻击时，会出现这种情况。
140:22	响应状态代码不是三位数字。
140:23	Content-Type 报头字段未指定内容类型且消息正文包含数据。
140:24	SIP 版本不是1、1.1 或2.0。
140:25	CSeq 报头字段中指定的方法与 SIP 请求中的“方法”字段不匹配。
140:26	预处理器无法识别在 SIP 请求“方法”字段中命名的方法。

GTP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

通用分组无线业务 (GPRS) 隧道协议 (GTP) 实现通过 GTP 核心网络进行通信。GTP 预处理器检测 GTP 流量中的异常，并将命令通道信令消息转发到规则引擎以进行检查。可以使用 `gtp_version`、`gtp_type` 和 `gtp_info` 规则关键字检查 GTP 命令通道流量中是否存在漏洞。

单一配置选项允许为预处理器进行 GTP 命令通道消息检查的端口修改默认设置。

GTP 预处理器规则

如果要下表中所列的 GTP 预处理器规则生成事件并在内联部署中丢弃攻击性数据包，必须启用它们。

表 *223: GTP* 预处理器规则

预处理器规则 GID:SID	说明
143:1	如果预处理器检测到无效的消息长度，将会生成事件。
143:2	如果预处理器检测到无效的信息元素长度，将会生成事件。
143:3	如果预处理器检测到无序的信息元素，将会生成事件。

配置 GTP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

可以使用以下程序修改 GTP 预处理器监控以获取 GTP 命令消息的端口。

过程

步骤 1 选择**策略** > **访问控制**，然后点击 **网络分析策略**或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击左侧导航面板中的 **Settings**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **GTP 命令通道配置 (GTP Command Channel Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **GTP 命令通道配置 (GTP Command Channel Configuration)** 旁边的 **编辑**（）。

步骤 7 输入**端口 (Ports)** 值。

使用逗号分隔多个端口。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要启用入侵事件，请启用 GTP 预处理器规则 (GID 143)。有关详细信息，请参阅设置入侵规则状态，第 1488 页。
- 部署配置更改。

IMAP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

互联网邮件应用协议 (IMAP) 用于从远程 IMAP 服务器检索邮件。IMAP 预处理器检查服务器到客户端的IMAP4流量，如果相关的预处理器规则已启用，还会生成关于异常流量的事件。此预处理器还可以提取和解码客户端到服务器IMAP4流量中的邮件附件，并将附件数据发送到规则引擎。可以在入侵规则中使用 `file_data` 关键字以指向附件数据。

提取和解码涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

IMAP 预处理器选项

请注意，解码（或提取，如果 MIME 邮件附件不要求解码）涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

另请注意，当 **Base64 解码深度 (Base64 Decoding Depth)**、**7 位/8 位/二进制解码深度 (7-Bit/8-Bit/Binary Decoding Depth)**、**Quoted-Printable 解码深度 (Quoted-Printable Decoding Depth)** 或 **Unix-to-Unix 解码深度 (Unix-to-Unix Decoding Depth)** 选项的值在以下设置中不同时，将会使用最高值：

- 默认网络分析策略
- 由同一访问控制策略中的网络分析规则调用的任何其他自定义网络分析策略

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

端口

指定用于检查 IMAP 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口号。

Base64 解码深度 (Base64 Decoding Depth)

指定要从每个 Base64 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码所有 Base64 数据。指定 -1 将会忽略 Base64 数据。

请注意，不能被 4 整除的正值将向上舍入为最接近的 4 的倍数，但值 65533、65534、65535 除外，因为它们将向下舍入为 65532。

当启用此选项时，您可以启用规则 141:4 以在解码失败时生成事件并在内联部署中丢弃攻击性数据包；解码可能会由于不正确的编码或损坏的数据等原因而失败。

7 位/8 位/二进制解码深度 (7-Bit/8-Bit/Binary Decoding Depth)

指定要从每个不要求解码的 MIME 邮件附件中提取的数据的最大字节数。这些附件类型包括 7 位、8 位、二进制以及各种多部分内容类型（例如，纯文本、jpeg 图像、mp3 文件等）。可指定一个正值，或者指定 0 以提取数据包中的所有数据。指定 -1 将会忽略非解码数据。

当启用此选项时，您可以启用规则 141:6 以在提取失败时生成事件并在内联部署中丢弃攻击性数据包；提取可能会由于损坏的数据等原因而失败。

Quoted-Printable 解码深度 (Quoted-Printable Decoding Depth)

指定要从每个 Quoted-Printable (QP) 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码数据包中的所有 QP 编码数据。指定 -1 将会忽略 QP 编码数据。

当启用此选项时，您可以启用规则 141:5 以在解码失败时生成事件并在内联部署中丢弃攻击性数据包；解码可能会由于不正确的编码或损坏的数据等原因而失败。

Unix-to-Unix 解码深度 (Unix-to-Unix Decoding Depth)

指定要从每个 Unix-to-Unix 编码（UuEncode 编码）的邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码数据包中的所有 UuEncode 编码数据。指定 -1 将会忽略 UuEncode 编码数据。

当启用此选项时，您可以启用规则 141:7 以在解码失败时生成事件并在内联部署中丢弃攻击性数据包；解码可能会由于不正确的编码或损坏的数据等原因而失败。

相关主题

file_data 关键字 ，第 1604 页

配置 IMAP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择策略 > 访问控制，然后点击 网络分析策略或策略 > 访问控制 > 入侵，然后点击 网络分析策略。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **IMAP 配置 (IMAP Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **IMAP 配置 (IMAP Configuration)** 旁边的 **编辑**（）。

步骤 7 修改IMAP 预处理器选项，第 2114 页中所述的设置。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要启用入侵事件，请启用 IMAP 预处理器规则 (GID 141)；请参阅设置入侵规则状态，第 1488 页。
- 部署配置更改。

相关主题

入侵和网络分析策略中的层，第 1607 页
冲突和更改：网络分析和入侵策略，第 1459 页

其他 IMAP 预处理器规则

下表中的 IMAP 预处理器规则与特定配置选项无关。与其他 IMAP 预处理器规则一样，如果要使这些规则能够生成事件并在内联部署中丢弃攻击性数据包，则必须启用它们。

表 *224:* 其他 *IMAP* 预处理器规则

预处理器规则 GID:SID	说明
141:1	如果预处理器检测到未在 RFC 3501 中定义的客户端命令，将会生成事件。

预处理器规则 GID:SID	说明
141:2	如果预处理器检测到未在 RFC 3501 中定义的服务器响应，将会生成事件。
141:3	如果预处理器正在使用系统允许的最大内存量，将会生成事件。在这种情况下，预处理将会停止解码，直至内存可用。

POP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

邮局协议 (POP) 用于从远程 POP 邮件服务器检索邮件。POP 预处理器检查服务器到客户端的 POP3 流量，如果相关的预处理器规则已启用，还会生成关于异常流量的事件。此预处理器还可以提取和解码客户端到服务器 POP3 流量中的邮件附件，并将附件数据发送到规则引擎。可以在入侵规则中使用 `file_data` 关键字以指向附件数据。

提取和解码涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

POP 预处理器选项

请注意，解码（或提取，如果 MIME 邮件附件不要求解码）涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

另请注意，当 **Base64 解码深度 (Base64 Decoding Depth)**、**7 位/8 位/二进制解码深度 (7-Bit/8-Bit/Binary Decoding Depth)**、**Quoted-Printable 解码深度 (Quoted-Printable Decoding Depth)** 或 **Unix-to-Unix 解码深度 (Unix-to-Unix Decoding Depth)** 选项的值在以下设置中不同时，将会使用最高值：

- 默认网络分析策略
- 由同一访问控制策略中的网络分析规则调用的任何其他自定义网络分析策略

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

端口

指定用于检查 POP 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口号。

Base64 解码深度 (Base64 Decoding Depth)

指定要从每个 Base64 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码所有 Base64 数据。指定 -1 将会忽略 Base64 数据。

请注意，不能被 4 整除的正值将向上舍入为最接近的 4 的倍数，但值 65533、65534、65535 除外，因为它们将向下舍入为 65532。

启用此选项时，您可以在解码失败时启用规则 142:4 至生成事件并在内联部署中丢弃攻击性数据包，例如，由于解码不正确或数据损坏，解码可能会失败。

7 位/8 位/二进制解码深度 (7-Bit/8-Bit/Binary Decoding Depth)

指定要从每个不要求解码的 MIME 邮件附件中提取的数据的最大字节数。这些附件类型包括 7 位、8 位、二进制以及各种多部分内容类型（例如，纯文本、jpeg 图像、mp3 文件等）。可指定一个正值，或者指定 0 以提取数据包中的所有数据。指定 -1 将会忽略非解码数据。

启用此选项时，您可以在提取失败时启用规则 142:6 至生成事件并在内联部署中丢弃攻击性数据包；例如，由于数据损坏，提取可能会失败。

Quoted-Printable 解码深度 (Quoted-Printable Decoding Depth)

指定要从每个 Quoted-Printable (QP) 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码数据包中的所有 QP 编码数据。指定 -1 将会忽略 QP 编码数据。

启用此选项时，您可以在解码失败时启用规则 142:5 至生成事件并在内联部署中丢弃攻击性数据包；例如，由于解码不正确或数据损坏，解码可能会失败。

Unix-to-Unix 解码深度 (Unix-to-Unix Decoding Depth)

指定要从每个 Unix-to-Unix 编码（UuEncode 编码）的邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码数据包中的所有 UuEncode 编码数据。指定 -1 将会忽略 UuEncode 编码数据。

启用此选项时，您可以在解码失败时启用规则 142:7 到生成事件并在内联部署中丢弃攻击性数据包；例如，由于解码不正确或数据损坏，解码可能会失败。

相关主题

管理层，第 1614 页
冲突和更改：网络分析和入侵策略，第 1459 页
file_data 关键字，第 1604 页

配置 POP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择**策略 > 访问控制**，然后点击 **网络分析策略**或**策略 > 访问控制 > 入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **POP 配置 (POP Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **POP 配置 (POP Configuration)** 旁边的 **编辑**（）。

步骤 7 修改POP 预处理器选项，第 2117 页中所述的设置。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要启用入侵事件，请启用 POP 预处理器规则 (GID 142)。有关详细信息，请参阅设置入侵规则状态，第 1488 页。
- 部署配置更改。

相关主题

管理层，第 1614 页
冲突和更改：网络分析和入侵策略，第 1459 页

其他 POP 预处理器规则

下表中的POP预处理器规则与特定配置选项无关。与其他POP预处理器规则一样，如果您需要它们来生成事件并在内联部署中丢弃攻击性数据包，则必须启用这些规则。

表 *225:* 其他 *POP* 预处理器规则

预处理器规则 GID:SID	说明
142:1	如果预处理器检测到未在 RFC 1939 中定义的客户端命令，将会生成事件。
142:2	如果预处理器检测到未在 RFC 1939 中定义的服务器响应，将会生成事件。
142:3	如果预处理器正在使用系统允许的最大内存量，将会生成事件。在这种情况下，预处理将会停止解码，直至内存可用。

SMTP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

SMTP 预处理器指示规则引擎对 SMTP 命令进行规范化。预处理器还可以提取和解码客户端到服务器流量中的邮件附件，并根据不同的软件版本，提取邮件的文件名、地址和报头数据，以在显示 SMTP 流量触发的入侵事件时提供上下文。

SMTP 预处理器选项

可以启用或禁用规范化，还可以对选项进行配置以控制 SMTP 解码器检测的异常流量类型。

请注意，解码（或提取，如果 MIME 邮件附件不要求解码）涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

另请注意，当 **Base64 解码深度 (Base64 Decoding Depth)**、**7 位/8 位/二进制解码深度 (7-Bit/8-Bit/Binary Decoding Depth)**、**Quoted-Printable 解码深度 (Quoted-Printable Decoding Depth)** 或 **Unix-to-Unix 解码深度 (Unix-to-Unix Decoding Depth)** 选项的值在以下设置中不同时，将会使用最高值：

- 默认网络分析策略
- 由同一访问控制策略中的网络分析规则调用的任何其他自定义网络分析策略

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

端口

指定要规范化其 SMTP 流量的端口。可以指定大于或等于 0 的值。使用逗号分隔多个端口。

状态检查 (Stateful Inspection)

如果选择此选项，SMTP 解码器将会保存状态，提供各个数据包的会话上下文，并且仅检查重组的会话。如果清除此选项，将会在没有会话上下文的情况下分析每个数据包。

规范化 (Normalize)

如果设置为 `All`，将会规范化所有命令。会检查命令后是否有多个空格字符。

如果设置为 `None`，则不会对命令进行规范化。

如果设置为 `Cmds`，将会规范化**自定义命令 (Custom Commands)** 中列出的命令。

自定义命令

如果**规范化 (Normalize)** 设置为 `Cmds`，则会规范化列出的命令。

可在文本框中指定应进行规范化的命令。会检查命令后是否有多个空格字符。

空格 (ASCII 0x20) 和制表符 (ASCII 0x09) 字符被视为是用于规范化目的的空格字符。

忽略数据 (Ignore Data)

不处理邮件数据；仅处理 MIME 邮件报头数据。

忽略 TLS 数据 (Ignore TLS Data)

不处理根据传输层安全协议加密的数据。

无警报 (No Alerts)

当随附的预处理器规则处于启用状态时禁用入侵事件。

检测未知命令 (Detect Unknown Commands)

检测 SMTP 流量中的未知命令。

可以启用规则 124:5，为此选项生成事件并在内联部署中丢弃攻击性数据包。

最大命令行长度 (Max Command Line Len)

检测 SMTP 命令行的长度何时大于此值。指定 0 将不会检测命令行长度。

RFC2821（网络工作组制定的关于简单邮件传输协议的规范）建议将最大命令行长度设置为 512。

可以启用规则 124:1，为此选项生成事件并在内联部署中丢弃攻击性数据包。

最大报头行长度 (Max Header Line Len)

检测 SMTP 数据报头行的长度何时大于此值。指定 0 将不会检测数据报头行长度。

可以启用规则 124:2 和 124:7，为此选项生成事件并在内联部署中丢弃攻击性数据包。

最大响应行长度 (Max Response Line Len)

检测 SMTP 响应行的长度何时大于此值。指定 0 将不会检测响应行长度。

RFC 2821 建议将最大响应行长度设置为 512。

可以启用规则 124:3，为此选项以及**替代最大命令行长度**（如已启用）生成事件并在内联部署中丢弃攻击性数据包。

替代最大命令行长度 (Alt Max Command Line Len)

检测任何指定命令的 SMTP 命令行的长度何时大于此值。指定 0 将不会检测指定命令的命令行长度。为众多命令设置了不同的默认行长度。

此设置将覆盖指定命令的“最大命令行长度”(Max Command Line Len) 设置。

可以启用规则 124:3，为此选项以及**最大响应行长度**（如已启用）生成事件并在内联部署中丢弃攻击性数据包。

无效命令 (Invalid Commands)

检测命令是否是从客户端发出的。

可以启用规则 124:6，为此选项以及**无效命令**生成事件并在内联部署中丢弃攻击性数据包。

有效命令 (Valid Commands)

允许此列表中的命令。

即使此列表为空，预处理器仍允许下列有效命令：ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE SOML STARTTLS TICK TIME TURN TURNME VERB VRFY XADR XAUTH XCIR XEXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR

注释 RCPT TO 和 MAIL FROM 是 SMTP 命令。对这两个命令，预处理器配置分别使用命令名 RCPT 和 MAIL。在代码中，预处理器会将 RCPT 和 MAIL 映射到正确的命令名。

可以启用规则 124:4，为此选项以及**无效命令**（如已配置）生成事件并在内联部署中丢弃攻击性数据包。

数据命令 (Data Commands)

列出以与 SMTP DATA 命令按照 RFC5321 的要求发送数据相同的方法发起数据发送的命令。使用空格分隔多个命令。

二进制数据命令 (Binary Data Commands)

列出以与 BDAT 命令按照 RFC 3030 的要求发送数据类似的方法发起数据发送的命令。使用空格分隔多个命令。

身份验证命令 (Authentication Commands)

列出发起客户端和服务器之间的身份验证交换的命令。使用空格分隔多个命令。

检测 xlink2state (Detect xlink2state)

检测作为 X-Link2State Microsoft Exchange 缓冲区数据溢出攻击的一部分的数据包。在内联部署中，系统还可以丢弃这些数据包。

可以启用规则 124:8，为此选项生成事件并在内联部署中丢弃攻击性数据包。

Base64 解码深度 (Base64 Decoding Depth)

在**忽略数据 (Ignore Data)** 已禁用的情况下，指定要从每个 Base64 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码所有 Base64 数据。指定 -1 将会忽略 Base64 数据。如果选择了**忽略数据 (Ignore Data)**，预处理器将不会对数据进行解码。

请注意，不能被 4 整除的正值将向上舍入为最接近的 4 的倍数，但值 65533、65534、65535 除外，因为它们将向下舍入为 65532。

当启用此选项时，可以启用规则124:10，在解码失败时生成事件并在内联部署中丢弃攻击性数据包；举例来说，解码可能会由于不正确的编码或损坏的数据而失败。

请注意，此选项取代已被弃用的**启用 MIME 解码 (Enable MIME Decoding)** 和**最大 MIME 解码深度 (Maximum MIME Decoding Depth)** 选项，后两个选项由于具有向后兼容性，因此在现有入侵策略中仍受到支持。

7 位/8 位/二进制解码深度 (7-Bit/8-Bit/Binary Decoding Depth)

在**忽略数据 (Ignore Data)** 已禁用的情况下，指定要从每个不要求解码的 MIME 邮件附件中提取的数据的最大字节数。这些附件类型包括7位、8位、二进制以及各种多部分内容类型（例如，纯文本、jpeg 图像、mp3 文件等）。可指定一个正值，或者指定 0 以提取数据包中的所有数据。指定 -1 将会忽略非解码数据。如果选择了**忽略数据 (Ignore Data)**，预处理器将不会提取数据。

Quoted-Printable 解码深度 (Quoted-Printable Decoding Depth)

在**忽略数据 (Ignore Data)** 已禁用的情况下，指定要从每个 Quoted-Printable (QP) 编码的 MIME 邮件附件中提取和解码的最大字节数。

可指定 1 到 65535 字节，或者指定 0 以解码数据包中的所有 QP 编码数据。指定 -1 将会忽略 QP 编码数据。如果选择了**忽略数据 (Ignore Data)**，预处理器将不会对数据进行解码。

当启用此选项时，可以启用规则124:11，在解码失败时生成事件并在内联部署中丢弃攻击性数据包；举例来说，解码可能会由于不正确的编码或损坏的数据而失败。

Unix-to-Unix 解码深度 (Unix-to-Unix Decoding Depth)

在**忽略数据 (Ignore Data)** 已禁用的情况下，指定要从每个 Unix-to-Unix 编码（UuEncode 编码）的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码数据包中的所有 UuEncode 编码数据。指定 -1 将会忽略 UuEncode 编码数据。如果选择了**忽略数据 (Ignore Data)**，预处理器将不会对数据进行解码。

当启用此选项时，可以启用规则124:13，在解码失败时生成事件并在内联部署中丢弃攻击性数据包；举例来说，解码可能会由于不正确的编码或损坏的数据而失败。

记录 MIME 附件名称 (Log MIME Attachment Names)

允许从 MIME Content-Disposition 报头提取 MIME 附件文件名，并将提取的文件名与为会话生成的所有入侵事件相关联。支持多个文件名。

启用此选项后，可以在入侵事件表视图的“邮件附件”(Email Attachment) 列中查看与事件相关的文件名。

记录收件人地址 (Log To Addresses)

允许从 SMTP RCPT TO 命令提取收件人邮件地址，并将提取的收件人地址与为会话生成的所有入侵事件相关联。支持多个收件人。

启用此选项后，可以在入侵事件表视图的“邮件收件人”(Email Recipient) 列中查看与事件相关的收件人。

记录发件人地址 (Log From Addresses)

允许从 SMTP MAIL FROM 命令提取发件人邮件地址，并将提取的发件人地址与为会话生成的所有入侵事件相关联。支持多个发件人地址。

启用此选项后，可以在入侵事件表视图的“邮件发件人”(Email Sender) 列中查看与事件相关的收件人。

记录报头 (Log Headers)

允许提取邮件报头。要提取的字节数取决于为**报头日志深度 (Header Log Depth)** 指定的值。

可以使用 `content` 或 `protected_content` 关键字来编写将邮件报头数据用作模式的入侵规则。还可以在入侵事件数据包视图中查看提取的邮件报头。

报头日志深度 (Header Log Depth)

指定在**记录报头 (Log Headers)** 已启用的情况下要提取的邮件报头的字节数。可指定 0 到 20480 字节。值 0 将会禁用**记录报头 (Log Headers)**。

相关主题

基本 content 和 protected_content 关键字参数，第 1517 页

配置 SMTP 解码

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 > 访问控制**，然后点击 **网络分析策略**或**策略 > 访问控制 > 入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航窗格中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **SMTP 配置 (SMTP Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **SMTP 配置 (SMTP Configuration)** 旁边的 **编辑**（）。

步骤 7 修改SMTP 预处理器选项，第 2120 页中所述的选项。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成事件并在内联部署中丢弃攻击性数据包，请启用 SMTP 预处理器规则 (GID 124)。有关详细信息，请参阅设置入侵规则状态，第 1488 页。
- 部署配置更改。

相关主题

管理层，第 1614 页
冲突和更改：网络分析和入侵策略，第 1459 页

SSH 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

SSH 预处理器检测：

- 质询-响应缓冲区溢出攻击
- CRC-32 攻击
- SecureCRT SSH 客户端缓冲区溢出攻击
- 协议不匹配
- SSH 消息方向不正确
- 任何版本字符串（版本 1 和 2 除外）

密钥交换后，会发生质询-响应缓冲区溢出攻击和 CRC-32 攻击，并会因此进行加密。这两种攻击在身份验证质询之后立即向服务器发送超过 20 KB 的反常态大量负载。CRC-32 攻击仅适用于 SSH 版本 1；质询-响应缓冲区溢出攻击仅适用于 SSH 版本 2。版本字符串在会话开端读取。除版本字符串的差异之外，这两种攻击的处理方式相同。

密钥交换前，如果试图保护连接，会发生 SecureCRT SSH 攻击和协议不匹配攻击。SecureCRT 攻击会向客户端发送过长的协议标识符字符串，从而导致缓冲区溢出。如果非 SSH 客户端应用试图连接到安全 SSH 服务器或者服务器和客户端的版本号不匹配，会出现协议不匹配攻击。

可以将SSH预处理器配置为检查指定端口或端口列表的流量，或者自动检测SSH流量。预处理器将会继续检查SSH流量，直至传递了未超过指定字节数的指定数量的加密数据包，或者直至超过指定数量的数据包中指定的最大字节数。如果超过最大字节数，系统将会假设出现了CRC-32（SSH版本1）攻击或质询-响应缓冲区溢出（SSH版本2）攻击。请注意，预处理器检测时无需配置任何版本字符串值（版本 1 和 2 除外）。

另请注意，SSH 预处理器不处理蛮力攻击。

SSH 预处理器选项

如果发生以下任何一种情况，预处理器将停止检查会话流量：

- 对于某个数量的加密数据包，服务器与客户端之间发生有效交换；连接继续保持。
- 在达到在**服务器无响应时可发送的字节数 (Number of Bytes Sent Without Server Response)** 中设置的值之前，达到要检查的加密数据包数量；假设发生了攻击。

在**待检查的加密数据包数量 (Number of Encrypted Packets to Inspect)** 中设置的数量内的每个有效服务器响应会重置**服务器无响应时可发送的字节数 (Number of Bytes Sent Without Server Response)**，且数据包计数继续进行。

可考虑以下 SSH 预处理器配置示例：

- **服务器端口 (Server Ports)**：22
- **自动检测端口 (Autodetect Ports)**：off
- **协议版本字符串最大长度 (Maximum Length of Protocol Version String)**：80
- **要检查的加密数据包数量 (Number of Encrypted Packets to Inspect)**：25
- **Number of Bytes Sent Without Server Response**：19600
- 所有检测选项均启用。

在本示例中，预处理器仅检查端口 22 的流量。也就是说，自动检测被禁用，因此只检查指定的端口。

此外，如果发生以下任何一种情况，本示例中的预处理器会停止检查流量：

- 客户端发送 25 个加密数据包，这些数据包总共不超过 19600 字节。假设没有发生攻击。
- 客户端发送25个加密数据包，这些数据包总共不超过19600字节。在这种情况下，预处理器可将发生的攻击视为质询-响应缓冲区溢出攻击，因为本示例中的会话为 SSH 版本 2 会话。

本示例中的预处理器还将检测处理流量过程中发生的以下任何情况：

- 服务器溢出，由大于 80 字节的版本字符串触发，表明为 SecureCRT 攻击

- 协议不匹配
- 数据包的传输方向错误

最后，预处理器将自动检测任何版本字符串（版本 1 和 2 除外）。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

服务器端口 (Server Ports)

指定 SSH 预处理器应检查其流量的端口。

可以配置单个端口或端口的逗号分隔列表。

自动检测端口 (Autodetect Ports)

将预处理器设置为会自动检测 SSH 流量。

如果选择此选项，预处理器会检查某个 SSH 版本号的所有流量。如果客户端和服务器数据包均没有包含版本号，预处理器将会停止处理。禁用此选项时，预处理器只会检查在**服务器端口 (Server Ports)**选项中确定的流量。

要检查的加密数据包数量 (Number of Encrypted Packets to Inspect)

指定每个会话待检查的数据流重组加密数据包的数量。

将此选项设置为 0 将允许所有流量通过。

减少待检查的加密数据包的数量可能会导致一些攻击避开检测。增加待检查的加密数据包的数量可能会对性能造成负面影响。

服务器无响应时可发送的字节数 (Number of Bytes Sent Without Server Response)

指定在假设存在质询-响应缓冲区溢出或 CRC-32 攻击之前，SSH 客户端在未获得响应的情况下可以向服务器发送的最大字节数。

如果预处理器对于质询-响应缓冲区溢出或 CRC-32 攻击生成误报，请增加此选项的值。

协议版本字符串的最大长度 (Maximum Length of Protocol Version String)

指定在假设存在 SecureCRT 攻击之前，服务器版本字符串中允许的最大字节数。

检测质询-响应缓冲区溢出攻击 (Detect Challenge-Response Buffer Overflow Attack)

启用或禁用质询-响应缓冲区溢出攻击检测。

您可以启用规则 128:1 为此选项生成事件并在内联部署中丢弃攻击性数据包。请注意，SFTP 会话可偶尔触发规则 128:1。

检测 SSH1 CRC-32 攻击 (Detect SSH1 CRC-32 Attack)

启用或禁用 CRC−-32 攻击检测。

您可以启用规则 128:2 为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测服务器溢出 (Detect Server Overflow)

启用或禁用 SecureCRT SSH 客户端缓冲区溢出攻击检测。

您可以启用规则 128:3 为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测协议不匹配 (Detect Protocol Mismatch)

启用或禁用协议不匹配检测。

您可以启用规则 128:4 为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测错误消息方向 (Detect Bad Message Direction)

允许或禁止检测流量传输方向错误这种情况（即，如果假定的服务器生成客户端流量，或者客户端生成服务器流量）。

您可以启用规则 128:5 为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测给定负载的负载大小不正确 (Detect Payload Size Incorrect for the Given Payload)

允许或禁止检测负载大小不正确的数据包，例如，SSH 数据包中指定的长度与 IP 报头中指定的总长度不一致，或者消息被截断（即，无足够的数据用于整个 SSH 报头）。

您可以启用规则 128:6 为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测错误版本字符串 (Detect Bad Version String)

请注意，启用预处理器后，它在检测时无需配置任何版本字符串（版本 1 和 2 除外）。

您可以启用规则 128:7 为此选项生成事件并在内联部署中丢弃攻击性数据包。

配置 SSH 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择**策略** > **访问控制**，然后点击 **网络分析策略**或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **SSH 配置 (SSH Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **SSH 配置 (SSH Configuration)** 旁边的 **编辑**（）。

步骤 7 修改SSH 预处理器选项，第 2126 页中所述的选项。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要启用入侵事件，请启用 SSH 预处理器规则 (GID 128)。有关详细信息，请参阅设置入侵规则状态，第 1488 页。
- 部署配置更改。

相关主题

管理层，第 1614 页
冲突和更改：网络分析和入侵策略，第 1459 页

SSL 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

SSL 预处理器可供您配置 SSL 检查，从而可以阻止、解密或使用访问控制检查已加密的流量。无论是否配置 SSL 检查，SSL 预处理器也会分析在流量中检测到的 SSL 握手消息，并确定会话何时被加密。系统通过识别已加密流量可以停止对已加密负载执行入侵和文件检查，这有助于减少误报并提高性能。

SSL 预处理器还可以检查已加密流量以检测 Heartbleed 漏洞攻击尝试，并在检测到此类漏洞攻击时生成事件。

会话加密之后，可以暂停检查流量是否存在入侵和恶意软件。如果配置 SSL 检查，则 SSL 预处理器还将确定您可以阻止、解密或使用访问控制进行检查的已加密流量。

使用 SSL 预处理器解密已加密流量无需许可证。所有其他 SSL 预处理器功能（包括暂停检查已加密负载是否存在恶意软件和入侵，并检测 Heartbleed 漏洞攻击）均需要保护许可证。

SSL 预处理的工作原理

如果配置了 SSL 检查，则 SSL 预处理器停止对已加密数据进行入侵和文件检查，然后使用 SSL 策略对已加密流量进行检查。这有助于清除误报。SSL 预处理器在检查 SSL 握手时会维护状态信息，跟踪该会话的状态和 SSL 版本。如果预处理器检测到会话状态已被加密，系统会将该会话的流量标记为“加密”。可将系统配置为在确定会话已加密时停止处理已加密会话中的所有数据包，并在检测到 Heartbleed 漏洞攻击尝试时生成事件。

对于每个数据包，SSL 预处理器都会验证流量是否包含 IP 报头、TCP 报头和 TCP 负载，以及流量发生在指定适用于 SSL 预处理的端口上。对于符合条件的流量，可根据以下情况确定流量是否已加密：

- 系统观察会话中的所有数据包，未启用**服务器端数据受信任 (Server side data is trusted)**，并且会话包含来自服务器和客户端的“已完成”消息以及至少一个来自各端的数据包（包含应用记录但不包含警报记录）。
- 系统遗漏某些流量，未启用**服务器端数据受信任 (Server side data is trusted)**，并且会话至少包含一个来自服务器端和客户端的数据包（包含未使用警报记录应答的应用记录）。
- 系统观察会话中的所有数据包，已启用**服务器端数据受信任 (Server side data is trusted)**，并且会话包含来自客户端的“已完成”消息和至少一个来自客户端的数据包（包含应用记录但不包含警报记录）。
- 系统遗漏某些流量，已启用**服务器端数据受信任 (Server side data is trusted)**，并且会话至少包含一个来自客户端的数据包（包含未使用警报记录应答的应用记录）。

如果选择停止处理加密流量，系统会在将该会话标记为“加密”后忽略其中的后续数据包。

此外，在 SSL 握手期间，预处理器监控检测信号请求和响应。检测到以下对象时，预处理器生成事件。

- 包含大于负载本身的负载长度值的检测信号请求
- 大于“最大检测信号长度”(Max Heartbeat Length) 字段中存储的值的检测信号响应

注释 可向某规则添加 `ssl_state` 和 `ssl_version` 关键字，以便在该规则中使用 SSL 状态或版本信息。

相关主题

SSL 关键字，第 1560 页

SSL 预处理器选项

注释 默认情况下，系统提供的网络分析策略启用 SSL 预处理器。如果预期有已加密流量通过您的网络，思科建议不要在自定义部署中禁用 SSL 预处理器。

如果未配置 SSL 检查，则系统尝试检查已加密流量是否存在恶意软件和入侵，而不对其进行解密。如果启用了 SSL 预处理器，它会检测会话加密的时间。启用 SSL 预处理器后，规则引擎可以调用预处理器来获得 SSL 状态和版本信息。如果在某个入侵策略中启用使用 `ssl_state` 和 `ssl_version` 关键字的规则，则还应在该策略中启用 SSL 预处理器。

端口

指定 SSL 预处理器应监控加密会话流量的端口（用逗号隔开）。只会检查此字段中指定端口的加密流量。

注释 如果 SSL 预处理器检测到指定用于 SSL 监控的端口上有非 SSL 流量，它会尝试将该流量作为 SSL 流量进行解码，然后将其标记为“损坏”。

停止检查加密流量 (Stop inspecting encrypted traffic)

启用或禁止在会话被标记为“加密”后检查会话中的流量。

启用此选项以禁止检查和重组加密的会话。SSL 预处理器会维护会话状态，因此，它可以禁止对会话中所有流量的检查。启用此选项时，系统会验证会话的几个数据包来确保流被加密，然后绕过深度检查。每个绕过的会话会增加 **show snort statistics** 命令的响应中显示的快速转发流计数。此外，由于绕过深度检查，连接事件中的发起方和响应方字节数将会不准确。发起方和响应方字节数小于实际会话的值，因为它只包括 Snort 检查的数据包，而不包括绕过深度检查后的任何数据包。这种行为适用于连接摘要事件和各构件中显示的所有流量值。

如果满足以下两个条件，则系统只会停止检查加密会话中的流量：

- 已启用 SSL 预处理
- 已选择此选项

如果清除此选项，则无法修改**服务器端数据受信任 (Server side data is trusted)** 选项。

服务器端数据受信任 (Server side data is trusted)

当“停止检查加密流量”(Stop inspecting encrypted traffic) 启用时，将支持仅根据客户端流量识别加密流量。

最大检测信号长度 (Max Heartbeat Length)

通过指定数个字节，支持检查 SSL 握手内的检测信号请求和响应以了解是否存在 Heartbleed 漏洞攻击尝试。您可以指定介于 `1` 和 65535 之间的整数，或指定 `0` 禁用该选项。

如果预处理器检测的检测信号请求的负载长度大于实际负载长度且规则 137:3 已启用，或者检测信号响应的大小大于当规则 137:4 已启用时为此选项配置的值，则预处理器生成事件并在内联部署中丢弃攻击性数据包。

配置 SSL 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择策略 > 访问控制，然后点击 网络分析策略或策略 > 访问控制 > 入侵，然后点击 网络分析策略。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **SSL 配置 (SSL Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **SSL 配置 (SSL Configuration)** 旁边的 **编辑**（）。

步骤 7 修改SSL 预处理器选项，第 2130 页中所述的任意设置。

- 在**端口 (Ports)** 字段中输入值。多个值之间用逗号隔开。
- 选中或清除**停止检查加密流量 (Stop inspecting encrypted traffic)** 复选框。
- 如果选中**停止检查加密流量 (Stop inspecting encrypted traffic)**，请选中或清除**服务器端数据受信任 (Server side data is trusted)**。
- 在**最大检测信号长度 (Max Heartbeat Length)** 字段中输入值。

提示 值为 0 将会禁用此选项。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要启用入侵事件，请启用 SSL 预处理器规则 (GID 137)。有关详细信息，请参阅设置入侵规则状态，第 1488 页。
- 部署配置更改。

相关主题

管理层，第 1614 页
冲突和更改：网络分析和入侵策略，第 1459 页

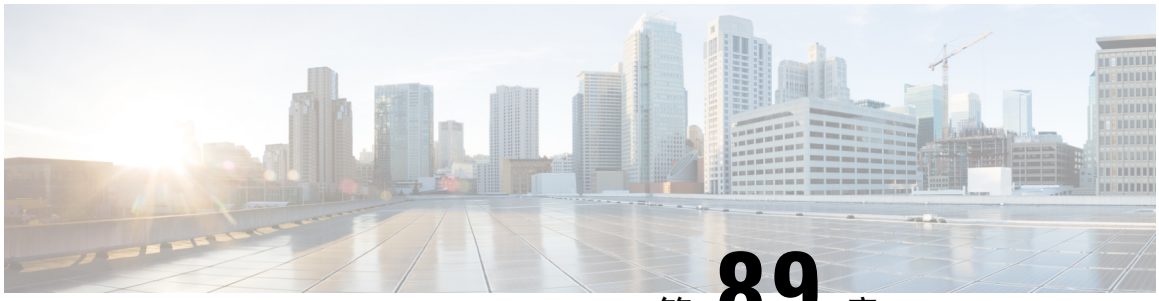
SSL 预处理器规则

如果要生成事件并在内联部署中丢弃攻击性数据包，请启用 SSL 预处理器规则 (GID 137)。

下表说明了可启用的 SSL 预处理器规则。

表 *226: SSL* 预处理器规则

预处理器规则 GID:SID	说明
137:1	在 ServerHello 消息之后检测 ClientHello 消息，此操作无效并被视为异常行为。
137:2	在禁用 SSL 预处理器选项**服务器端数据受信任 (Server side data is trusted)** 时检测没有 ClientHello 消息的 ServerHello 消息，此操作无效并被视为异常行为。
137:3	在 SSL 预处理器选项**最大检测信号长度 (Max Heartbeat Length)** 包含非零值时检测负载长度大于负载本身的检测信号请求，此操作指示尝试利用 Heartbleed 漏洞。
137:4	检测大于 SSL 预处理器选项**最大检测信号长度 (Max Heartbeat Length)** 中指定的非零值的检测信号响应，此操作指示尝试利用 Heartbleed 漏洞。



第 89 章

SCADA 预处理器

以下主题介绍监控和数据采集 (SCADA) 协议的预处理器及其配置方法：

SCADA 预处理器简介

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

监控与数据采集 (SCADA) 协议可监视和控制工业、基础设施以及工厂流程（例如制造、生产、水处理、配电、机场和运输系统等）并从中获取数据。Firepower 系统为可作为网络分析策略一部分进行配置的 Modbus 、分布式网络协议 (DNP3)、通用工业协议 (CIP) 和 S7Commplus SCADA 协议提供预处理器。

如果 Modbus、DNP3、CIP 或 S7Commplus 预处理被禁用，而您启用并部署需要其中一种预处理器的入侵规则，则系统会自动使用所需的预处理器及其当前设置，尽管该预处理器在 Web 界面中对于相应的网络分析策略仍处于禁用状态。

SCADA 预处理器的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

SCADA 预处理器的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

Modbus 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

Modbus 协议由 Modicon 于 1979 年首次发布，是一种广泛使用的 SCADA 协议。Modbus 预处理器可检测 Modbus 流量中的异常，解码 Modbus 协议以供规则引擎进行处理（规则引擎使用 Modbus 关键字来访问某些协议字段）。

单一配置选项允许为预处理器进行 Modbus 流量检查的端口修改默认设置。

相关主题

SCADA 关键字，第 1582 页

Modbus 预处理器端口选项

端口

指定预处理器检查 Modbus 流量的端口。使用逗号分隔多个端口。

配置 Modbus 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

如果您的网络不包含任何支持 Modbus 的设备，则不应该在应用于流量的网络分析策略中启用此预处理器。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 > 访问控制**，然后点击 **网络分析策略**或**策略 > 访问控制 > 入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果 **SCADA 预处理器 (SCADA Preprocessors)** 下的 **Modbus 配置 (Modbus Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **Modbus 配置 (Modbus Configuration)** 旁边的 **编辑**（）。

步骤 7 在**端口 (Ports)** 字段中输入值。

多个值之间用逗号隔开。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成事件并在内联部署中丢弃攻击性数据包，请启用 Modbus 预处理器规则 (GID 144)。有关详细信息，请参阅设置入侵规则状态，第 1488 页和Modbus 预处理器规则，第 2138 页。
- 部署配置更改。

相关主题

管理层，第 1614 页
冲突和更改：网络分析和入侵策略，第 1459 页

Modbus 预处理器规则

如果希望这些规则生成事件并在内联部署中丢弃攻击性数据包，则必须启用下表中的 Modbus 预处理器规则。

表 *227: Modbus* 预处理器规则

预处理器规则 GID:SID	说明
144:1	如果 Modbus 报头中的长度与 Modbus 函数代码所要求的长度不匹配，将会生成事件。 每个 Modbus 函数都有预期的请求和响应格式。如果消息长度与预期格式不匹配，将会生成此事件。
144:2	如果 Modbus 协议 ID 为非零值，将会生成事件。协议 ID 字段用于将其他协议与 Modbus 协议复用。由于预处理器并不处理此类其他协议，因此会生成此事件。
144:3	如果预处理器检测到保留的 Modbus 函数代码，将会生成事件。

DNP3 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

分布式网络协议 (DNP3) 是一种 SCADA 协议，最初开发是为了在发电站之间提供一致的通信。此外，DNP3 还在水务、废弃物、运输和很多其他行业中得到广泛使用。

DNP3 预处理器可检测到 DNP3 流量中的异常，并对 DNP3 协议进行解码以用于按规则引擎进行处理，这将使用 DNP3 关键字来访问某些协议字段。

相关主题

DNP3 关键字，第 1584 页

DNP3 预处理器选项

端口

启用对每个指定端口的 DNP3 流量检查。可以指定单个端口或端口的逗号分隔列表。

记录错误 CRC

验证包含在 DNP3 链路层帧中的校验和。具有无效校验和的帧将被忽略。

可以启用规则 145:1，以便在检测到无效校验和时生成事件并在内联部署中丢弃攻击性数据包。

配置 DNP3 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

如果您的网络不包含任何支持 DNP3 的设备，则不应该在应用于流量的网络分析策略中启用此预处理器。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略** > **访问控制**，然后点击 **网络分析策略**或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（✎）。

如果显示**视图**（👁），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果 **SCADA 预处理器 (SCADA Preprocessors)** 下的 **DNP3 配置 (DNP3 Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **DNP3 配置 (DNP3 Configuration)** 旁边的 **编辑**（✎）。

步骤 7 为**端口数 (Ports)** 输入一个值。

多个值之间用逗号隔开。

步骤 8 选中或清除**记录不良 CRC (Log bad CRCs)** 复选框。

步骤 9 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成事件并在内联部署中丢弃攻击性数据包，请启用 DNP3 预处理器规则 (GID 145)。有关详细信息，请参阅设置入侵规则状态，第 1488 页、DNP3 预处理器选项，第 2139 页和DNP3 预处理器规则，第 2140 页。
- 部署配置更改。

相关主题

管理层，第 1614 页
冲突和更改：网络分析和入侵策略，第 1459 页

DNP3 预处理器规则

如果希望下表中所列的 DNP3 预处理器规则生成事件并在内联部署中丢弃攻击性数据包，必须启用这些规则。

表 *228: DNP3* 预处理器规则

预处理器规则 GID:SID	说明
145:1	在**记录无效 CRC (Log bad CRC)** 已启用的情况下，如果预处理器检测到具有无效校验和的链路层帧，将会生成事件。
145:2	如果预处理器检测到具有无效长度的 DNP3 链路层帧，系统将会生成事件并阻止该数据包。
145:3	如果预处理器检测到具有无效序列号的传输层分段，系统将会生成事件并在重组期间阻止数据包。
145:4	如果需要清除 DNP3 重组缓冲区后才能重组完整的片段，系统将会生成事件。如果在其他分段已加入队列后出现带有 FIR 标志的分段，系统将会发生这种情况。
145:5	如果预处理器检测到使用保留地址的 DNP3 链路层帧，系统将会生成事件。
145:6	如果预处理器检测到使用保留函数代码的 DNP3 请求或响应，系统将会生成事件。

CIP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

通用工业协议 (CIP) 是广泛使用的应用协议，支持工业自动化应用。EtherNet/IP (ENIP) 是基于以太网的网络中使用的 CIP 的实施。

CIP 预处理器检测 TCP 或 UDP 上运行的 CIP 和 ENIP 流量，并将其发送给入侵规则引擎。可以使用自定义入侵规则中的 CIP 和 ENIP 关键字检测 CIP 和 ENIP 流量中的攻击。请参阅 CIP 和 ENIP 关键字。此外，可以指定访问控制规则中的 CIP 和 ENIP 应用条件以控制流量。请参阅配置应用条件和过滤器，第 1294 页。

CIP 预处理器选项

端口

指定用于检查 CIP 和 ENIP 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口号。

注释 必须将默认的 CIP 检测端口 44818 和您列出的任何其他端口添加到 TCP 数据流**对两个端口执行数据流重组**列表。请参阅TCP 数据流预处理选项，第 2171 页和创建自定义网络分析策略，第 2060 页。

默认的无关联超时时间 (秒)

当 CIP 请求消息不包含协议特定超时值，并且达到**每个 TCP 连接上并发无关联请求的最大数 (Maximum number of concurrent unconnected requests per TCP connection)** 时，系统测定此选项指定的消息的秒数。如果计时器过期，则会删除此消息，以便腾出空间来存储未来的请求。可指定 0 到 360 之间的整数。如果指定 0，不具有协议特定超时值的所有流量会首先超时。

每个 TCP 连接上并发无关联请求的最大数

在系统关闭连接之前，可以不用理会的并发请求的数量。可指定 1 到 10000 之间的整数。

每个 TCP 连接上 CIP 连接的最大数

系统允许的每个 TCP 连接上的同步 CIP 连接的最大数。可指定 1 到 10000 之间的整数。

CIP 事件

根据设计，应用检测器检测并且事件查看器显示相同的应用，每个会话一次。CIP 会话可以在不同的数据包中包括多个应用，一个 CIP 数据包可以包含多个应用。CIP 预处理器根据相应的入侵规则处理所有 CIP 和 ENIP 流量。

下表展示在事件视图中显示的 CIP 值。

表 *229: CIP* 事件字段值

事件字段	显示的值
应用协议	CIP 或 ENIP
客户端	CIP 客户端或 ENIP 客户端
Web 应用	检测到的特定应用，即： • 对于允许或监控流量的访问控制规则，会话中检测到的最新应用协议。 配置为记录连接的访问控制规则可能不会为指定的 CIP 应用生成事件，而没 接的访问控制规则可能会为 CIP 应用生成事件。 • 对于阻止流量的访问控制规则，触发此阻止的应用协议。 当访问控制规则阻止 CIP 应用列表时，事件查看器显示检测到的第一个应用

GTP 预处理器规则

如果您希望下表中所列的 CIP 预处理器规则生成事件，必须启用它们。有关启用规则的详细信息，请参阅设置入侵规则状态，第 1488 页。

表 *230: GTP* 预处理器规则

GID:SID	Rule Message
148:1	CIP_MALFORMED
148:2	CIP_NON_CONFORMING
148:3	CIP_CONNECTION_LIMIT
148:4	CIP_REQUEST_LIMIT

配置 CIP 预处理器的准则

配置 CIP 预处理器时，请注意以下事项：

- 必须将默认的 CIP 检测端口 44818 和您列出的任何其他 CIP **端口**添加到 TCP 数据流**对两个端口执行数据流重组**列表。请参阅CIP 预处理器选项，第 2141 页、创建自定义网络分析策略，第 2060 页和TCP 数据流预处理选项，第 2171 页。
- 事件查看器可对 CIP 应用进行特殊处理。请参阅CIP 事件，第 2142 页。
- 我们建议您使用入侵防御操作作为访问控制策略的默认操作。
- CIP 预处理器不支持**访问控制：信任所有流量**的访问控制策略默认操作，此选项可能会产生不需要的行为，包括不丢弃由入侵规则和访问控制规则中所指定的 CIP 应用触发的流量。
- CIP 预处理器不支持**访问控制：阻止所有流量**的访问控制策略默认操作，此选项可能会产生不需要的行为，包括阻止并不想要阻止的 CIP 应用。
- CIP 预处理器不支持 CIP 应用的应用可视性，包括网络发现。
- 要检测 CIP 和 ENIP 应用并将其用在访问控制规则、入侵规则等规则中，必须手动启用相应自定义网络分析策略中的CIP预处理器。请参阅创建自定义网络分析策略，第 2060 页、设置默认网络分析策略和配置网络分析规则，第 2047 页。
- 要丢弃可触发 CIP 预处理器规则和 CIP 入侵规则的流量，请确保在相应入侵策略中已启用**内联时丢弃**。请参阅设置内联部署中的丢弃行为。
- 要使用访问控制规则阻止 CIP 或 ENIP 应用流量，请确保在相应的网络分析策略中已启用内联规范化预处理器及其**内联模式**选项（默认设置）。请参阅创建自定义网络分析策略，第 2060 页、设置默认网络分析策略和内联部署中预处理器流量的修改，第 2064 页。

配置 CIP 预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

开始之前

- 必须将默认的 CIP 检测端口 44818 和任何其他您列出为 CIP **端口**的端口添加到 TCP 数据流**对两个端口执行数据流重组**列表。请参阅CIP 预处理器选项，第 2141 页、创建自定义网络分析策略，第 2060 页和TCP 数据流预处理选项，第 2171 页。
- 熟悉配置 CIP 预处理器的准则，第 2142 页。
- 威胁防御 设备不支持 CIP 预处理器。

过程

步骤 1 选择**策略** > **访问控制**，然后点击 **网络分析策略**或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释　如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果 **SCADA 预处理器** 下的 **CIP 配置**已禁用，请点击**已启用**。

步骤 6 可以修改 CIP 预处理器选项，第 2141 页中所述的任何选项。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果您要生成事件并在内联部署中丢弃攻击性数据包，请启用 CIP 入侵规则和 CIP 预处理器规则 (GID 148)。有关详细信息，请参阅设置入侵规则状态，第 1488 页、GTP 预处理器规则，第 2142 页和CIP 事件，第 2142 页。
- 部署配置更改。

S7Commplus 预处理器

注释　此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

S7Commplus 预处理器可检测 S7Commplus 流量。可以使用自定义入侵规则中的 S7Commplus 关键字检测 S7Commplus 流量中的攻击。请参阅S7Commplus 关键字，第 1587 页。

配置 S7Commplus 预处理器

注释　此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

所有 威胁防御 设备都支持 S7Commplus 预处理器。

过程

步骤 1 选择**策略** > **访问控制**，然后点击 **网络分析策略**或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果 **SCADA 预处理器 (SCADA Preprocessors)** 下的 **S7Commplus 配置 (S7Commplus Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 或者，点击 **S7Commplus 配置 (S7Commplus Configuration)** 旁边的 **编辑**（），然后修改 **s7commplus_ports** 以标识预处理器用于检查 S7Commplus 流量的端口。使用逗号分隔多个端口。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成入侵事件，请启用 S7Commplus 预处理器规则 (GID 149)。有关详细信息，请参阅设置入侵规则状态，第 1488 页
- 部署配置更改。

第 90 章

传输层和网络层预处理器

以下主题介绍传输层和网络层预处理器及其配置方式：

传输层和网络层预处理器简介

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

网络层和传输层预处理器检测对 IP 分片、校验和验证及 TCP 和 UDP 会话预处理加以利用的攻击。在将数据包发送到预处理器之前，数据包解码器将数据包报头和负载转换为便于预处理器和入侵规则引擎使用的格式，并检测数据包报头的各种异常行为。在数据包解码后到将数据包发送到其他预处理器之前这段期间，内联规范化预处理器会对流量进行规范化以便进行内联部署。

当入侵规则或规则参数要求禁用的预处理器时，系统会自动使用其当前设置，即使其在网络分析策略网络界面中保持禁用状态。

传输层和网络层预处理器的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

传输层和网络层预处理器的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

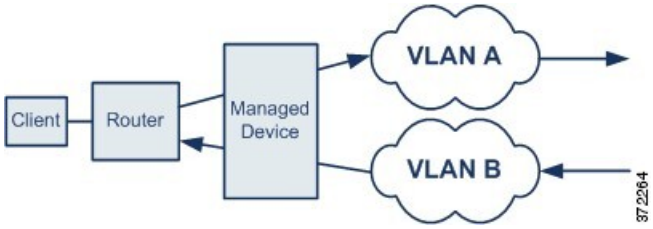
高级传输/网络预处理器设置

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

高级传输和网络预处理器设置全局应用于会部署访问控制策略的所有网络、区域和 VLAN。可以在访问控制策略中而非网络分析策略中配置这些高级设置。

忽略的 VLAN 报头

同一连接中行进方向不同的流量中的 VLAN 标记不同，可能影响流量重组和规则处理。例如，在下图中，同一连接的流量可以通过 VLAN A 进行传输，并通过 VLAN B 进行接收。



您可以将系统配置为忽略 VLAN 报头，从而可以针对您的部署正确处理数据包。

入侵丢弃规则中的活动响应

丢弃规则是指规则状态设置为“丢弃并生成事件”(Drop and Generate Events) 的入侵规则或预处理器。在内联部署中，系统通过丢弃触发数据包并阻止数据包起始的会话来对 TCP 或 UDP 丢弃规则作出响应。

提示 由于在会话方面通常未考虑 UDP 数据流，因此数据流预处理器使用封装 IP 数据报报头中的源和目标 IP 地址字段及 UDP 报头中的端口字段来确定流动方向并识别 UDP 会话。

您可以配置系统来启动一个或多个活动响应，从而在有问题的数据包触发 TCP 或 UDP 丢弃规则时，更精确具体地关闭 TCP 连接或 UDP 会话。您可以在内联部署中使用活动响应，包括路由部署和透明部署。主动响应不适合或不支持被动部署。

要配置活动响应，请执行以下操作：

- 创建或修改 TCP 或 UDP（仅限 **resp** 关键字）入侵规则。请参阅入侵规则报头协议，第 1502 页。
- 为入侵规则添加 **react** 或 **resp** 关键字；请参阅 x活动响应关键字，第 1590 页。
- 或者对于 TCP 连接，可以指定要发送的其他活动响应的最大数量以及活动响应之间等待的秒数；请参阅高级传输/网络预处理器选项，第 2149 页中的**最大活动响应数**和**最小响应秒数**。

当匹配流量触发丢弃规则时，活动响应会关闭会话，如下所示：

- **TCP** - 丢弃触发数据包，并在客户端和服务器流量中插入 TCP 重置 (RST) 数据包。
- **UDP** - 向会话的两端发送 ICMP 不可达数据包。

高级传输/网络预处理器选项

在跟踪连接时忽略 VLAN 报头 (Ignore the VLAN header when tracking connections)

指定在识别流量时是忽略还是包含 VLAN 报头，如下所示：

- 选择此选项时，系统会忽略 VLAN 报头。此设置用于在按不同方向传播的流量中可能检测到同一连接的不同 VLAN 标签的已部署设备

- 当禁用此选项时，系统会包含 VLAN 报头。此设置用于在按不同方向传播的流量中不会检测到同一连接的不同 VLAN 标签的已部署设备。

最大活动响应数

指定每个 TCP 连接的最大活动响应数。如果已启动活动响应的连接上出现其他流量，并且在先前活动响应后流量出现超过**最小响应秒数 (Minimum Response Seconds)**，系统会发送其他活动响应，除非已达到指定的最大数量。设置为 0 会禁用 **resp** 或 **react** 规则触发的其他活动响应。请参阅入侵丢弃规则中的活动响应，第 2149 页和活动响应关键字，第 1590 页。

请注意，无论此选项如何配置，所触发的 **resp** 或 **react** 规则都会启动主动响应。

最小响应秒数 (Minimum Response Seconds)

指定在系统已启动活动响应的连接上的任何其他流量都会产生后续活动响应之前等待的秒数，直至出现**最大活动响应数 (Maximum Active Responses)**。

故障排除选项：会话终止日志记录阈值 (Troubleshooting Options: Session Termination Logging Threshold)

注意 请勿修改“会话终止日志记录阈值”(Session Termination Logging Threshold)，除非支持人员指示执行此操作。

支持人员可能会在故障排除呼叫期间要求您配置系统，以在单个连接超过指定阈值时记录消息。更改此选项的设置会影响性能，应仅在支持人员的指导下进行操作。

此选项指定一个字节数，当会话终止并超过该指定数字时，将会记录消息。

注释 1GB 的上限还受数据流处理分配的受管设备上的内存容量限制。

相关主题

活动响应关键字，第 1590 页

配置高级传输/网络预处理器设置

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

您必须是 管理员、访问管理员 或 网络管理员 才能执行此任务。

过程

步骤 1 在访问控制策略编辑器中，点击 **高级**。

步骤 2 点击“传输/网络层设置”(Transport/Network Layer Settings) 部分旁边的 **编辑**（）。

步骤 3 修改高级传输/网络预处理器选项，第 2149 页中描述的选项，故障排除选项**会话终止日志记录阈值 (Session Termination Logging Threshold)** 除外。

注意 请勿修改**会话终止日志记录阈值 (Session Termination Logging Threshold)**，除非支持人员指示执行此操作。

步骤 4 点击 **OK**。

下一步做什么

- 或者，进一步配置策略，如编辑访问控制策略，第 1262 页中所述。
- 部署配置更改。

校验和验证

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

系统可验证所有协议级校验和，以确保接收完整的 IP、TCP、UDP 和 ICMP 传输，且基本级别的数据包在传输过程中未被篡改或意外修改。校验和使用算法来验证数据包中的协议是否完整。如果系统计算的值与终端主机在数据包中写入的值一致，则认为该数据包未被更改。

禁用校验和验证可能导致您的网络易受插入攻击。请注意，系统不会生成校验和验证事件。在内联部署中，可以将系统配置为丢弃校验和无效的数据包。

校验和验证选项

在被动或内联部署中，可以将以下任何选项设置为**已启用 (Enabled)** 或**已禁用 (Disabled)**；或在内联部署中设置为**丢弃 (Drop)**：

- **ICMP 校验和 (ICMP Checksums)**
- **IP 校验和 (IP Checksums)**
- **TCP 校验和 (TCP Checksums)**
- **UDP 校验和 (UDP Checksums)**

要丢弃恶意数据包，除将选项设置为**丢弃 (Drop)** 以外，还必须在关联网络分析策略中启用**内联模式 (Inline Mode)** 并确保设备为内联部署。

在被动部署中或在分流模式下的内联部署中，将这些选项设置为**丢弃 (Drop)** 与将其设置为**已启用 (Enabled)** 的作用相同。

注意 在 **TCP 校验和 (TCP checksums)** 下， **忽略 (Ignore)** 选项（默认）会绕过或忽略任何已配置的 Snort 规则。

所有校验和验证选项默认为**已启用 (Enabled)**。但是，威胁防御 路由接口和透明接口始终会丢弃 IP 校验和验证失败的数据包。请注意，在将数据包传递到 Snort 进程之前，威胁防御 路由和透明接口会修复带有错误校验和的 UDP 数据包。

相关主题

内联部署中预处理器流量的修改，第 2064 页

验证校验和

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择**策略 > 访问控制**，然后点击 **网络分析策略**或**策略 > 访问控制 > 入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**传输/网络层预处理器 (Transport/Network Layer Preprocessors)** 下的**校验和验证 (Checksum Verification)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击**校验和验证 (Checksum Verification)** 旁边的 **编辑**（）。

步骤 7 修改校验和验证，第 2151 页中所述的选项。

注释 在 **TCP 校验和 (TCP checksums)** 下， **忽略 (Ignore)** 选项（默认）会绕过或忽略任何已配置的 Snort 规则。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 部署配置更改。

相关主题

层管理，第 1612 页
冲突和更改：网络分析和入侵策略，第 1459 页

内联规范化预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

内联规范化预处理器会将流量规范化，从而尽可能降低攻击者在内联部署中得以避开检测的可能性。

注释 为让系统影响流量，必须使用路由接口、交换接口或透明接口或者内联接口对向受管设备部署相关配置。

您可以指定 IPv4、IPv6、ICMPv4、ICMPv6 和 TCP 流量的任意组合的规范化。大多数规范化由内联规范化预处理器逐个数据包执行。但是，TCP 数据流预处理器处理大多数状态相关的数据包和数据流规范化，包括 TCP 负载规范化。

在数据包解码器进行解码后会立即执行内联规范化，直至其他预处理器进行处理。规范化从内数据包层继续执行到外数据包层。

内联规范化预处理器不会生成事件；它准备数据包以供内联部署中的其他预处理器和规则引擎使用。预处理器还有助于确保系统处理的数据包与网络中主机接收的数据包相同。

注释 在内联部署中，我们建议您启用内联模式并配置已启用 **Normalize TCP Payload** 选项的内联规范化预处理器。在被动部署中，我们建议您使用 自适应配置文件。

相关主题

内联部署中预处理器流量的修改，第 2064 页
关于自适应配置文件，第 2201 页

内联规范化选项

Minimum TTL

当**重置 TTL (Reset TTL)** 大于或等于为此选项设置的值时，请指定以下设置：

- 启用**规范化 IPv4 (Normalize IPv4)** 后系统允许“IPv4 生存时间 (TTL)”(IPv4 Time to Live [TTL]) 字段使用的最小值；较小的值会导致将 TTL 的数据包值规范化为针对**重置 TTL (Reset TTL)** 设置的值
- 启用**规范化 IPv6 (Normalize IPv6)** 后系统允许“IPv6 跳数限制”(IPv6 Hop Limit) 字段使用的最小值；较小的值会导致将 TTL 的数据包值规范化为针对**重置 TTL (Reset TTL)** 设置的值

此字段为空时，系统假设值为 1。

注释 对于 威胁防御 路由和透明接口，**最小 TTL** 和**重置 TTL** 选项会被忽略。连接的最大 TTL 由初始数据包中的 TTL 来确定。后续数据包的 TTL 可以减少，但不能增加。系统会将 TTL 重置为该连接之前看到过的最低 TTL。这可以防止 TTL 回避攻击。

当数据包解码**检测协议报头异常**选项已启用时，可以启用解码器规则类别中的以下规则来为此选项生成事件并在内联部署中丢弃攻击性数据包：

- 当系统检测到 TTL 小于指定最小值的 IPv4 数据包时，您可以启用规则 116：428 来触发。
- 当系统检测到跳数限制小于指定最小值的 IPv6 数据包时，您可以启用规则 116：270 来触发。

Reset TTL

如果设置为大于或等于**最小 TTL (Minimum TTL)** 的值，请规范化以下字段：

- IPv4 TTL 字段（如果启用了**规范化 IPv4 [Normalize IPv4]**）
- “IPv6 跳数限制”(IPv6 Hop Limit) 字段（如果启用了**规范化 IPv6 [Normalize IPv6]**）

当数据包值小于**最小 TTL (Minimum TTL)** 时，系统会通过将其 TTL 或“跳数限制”(Hop Limit) 值更改为针对此选项设置的值来规范化数据包。将此字段留空或设置为 0，或设置为小于**最小 TTL (Minimum TTL)** 的任意值会禁用该选项。

规范化 IPv4 (Normalize IPv4)

启用 IPv4 流量规范化。在以下时候，系统还会根据需要规范化 TTL 字段：

- 此选项启用，且
- 为**重置 TTL (Reset TTL)** 设置的值启用 TTL 规范化。

此选项启用时，还可以启用额外的 IPv4 选项。

启用此选项时，系统执行以下基本 IPv4 规范化：

- 将具有多余负载的数据包截断至 IP 报头中指定的数据报长度
- 清除“差分服务 (DS)”(Differentiated Services [DS]) 字段（以前称为“服务类型 (TOS)”(Type of Service [TOS]) 字段）
- 将所有选项八位元设置为 1（“无操作”[No Operation]）

对于 威胁防御 路由和透明接口，此选项会被忽略。威胁防御 设备将丢弃任何包含除任何路由或透明接口上的路由器警报、选项列表结束 (EOOL) 以及无操作 (NOP) 选项之外的 IP 选项的 RSVP 数据包。

规范化不分片位 (Normalize Don't Fragment Bit)

清除“IPv4 标志”(IPv4 Flags) 报头字段的一位“不分片”(Don’t Fragment) 子字段。通过启用此选项，下游路由器可在必要时对数据包进行分片而不是将其丢弃；启用此选项还可以根据要丢弃的构造数据包来防止躲避检测。必须启用**规范化 IPv4 (Normalize IPv4)** 后才可以选择此选项。

规范化保留位 (Normalize Reserved Bit)

清除“IPv4 标志”(IPv4 Flags) 报头字段的一位“保留”(Reserved) 子字段。通常会启用此选项。必须启用**规范化 IPv4 (Normalize IPv4)** 后才可以选择此选项。

规范化 TOS 位 (Normalize TOS Bit)

清除一个字节的“差分服务”(Differentiated Services) 字段（以前称为“服务类型”[Type of Service]）。必须启用**规范化 IPv4 (Normalize IPv4)** 后才可以选择此选项。

规范化多余负载 (Normalize Excess Payload)

将具有多余负载的数据包截断至 IP 报头中指定的数据报长度加上第 2 层（例如以太网）报头，但是不截断为小于最小帧长度。必须启用**规范化 IPv4 (Normalize IPv4)** 后才可以选择此选项。

对于威胁防御路由和透明接口，此选项会被忽略。在这些接口上始终丢弃具有多余负载的数据包。

规范化 IPv6 (Normalize IPv6)

将“逐跳选项”(Hop-by-Hop Options)和“目标选项”(Destination Options) 扩展报头中的所有“选项类型”(Option Type) 字段设置为 00（跳过并继续处理）。此选项处于启用状态并且为**重置 TTL (Reset TTL)** 设置的值会启用跳数限制规范化时，系统还会根据需要规范化 Hop Limit 字段。

规范化 ICMPv4 (Normalize ICMPv4)

清除 ICMPv4 流量中“回应（请求）”(Echo [Request]) 和“回应答复”(Echo Reply) 消息内的 8 位“代码”(Code) 字段。

规范化 ICMPv6 (Normalize ICMPv6)

清除 ICMPv6 流量中“回应（请求）”(Echo [Request]) 和“回应答复”(Echo Reply) 消息内的 8 位“代码”(Code) 字段。

Normalize/Clear Reserved Bits

清除 TCP 报头中的保留位。

规范化/清除选项填充字节 (Normalize/Clear Option Padding Bytes)

清除任何 TCP 选项填充字节。

Clear Urgent Pointer if URG=0

如果未设置紧急 (URG) 控制位，则清除 16 位 TCP 报头 Urgent Pointer 字段。

Clear Urgent Pointer/URG on Empty Payload

如果没有负载，则清除 TCP 报头“紧急指针”(Urgent Pointer) 字段和 URG 控制位。

如果未设置紧急指针则清除 URG (Clear URG if Urgent Pointer is Not Set)

如果未设置紧急指针，则清除 TCP 报头 URG 控制位。

Normalize Urgent Pointer

如果指针大于负载长度，则将两字节的 TCP 报头 Urgent Pointer 字段设置为负载长度。

规范化 TCP 负载 (Normalize TCP Payload)

启用“TCP 数据”(TCP Data) 字段的规范化以确保重传数据的一致性。无法正确重组的所有数据段都会被丢弃。

Remove Data on SYN

如果 TCP 操作系统策略**不是** Mac OS，则移除同步 (SYN) 数据包中的数据。

此选项还会禁用规则 129:2，该规则原本会在 TCP 数据流预处理器**策略**选项未设置为 **Mac OS** 时触发。

Remove Data on RST

从 TCP 重置 (RST) 数据包中删除所有数据。

根据窗口修剪数据 (Trim Data to Window)

将“TCP 数据”(TCP Data) 字段修剪为在“窗口”(Window) 字段中指定的大小。

根据 MSS 修剪数据 (Trim Data to MSS)

如果负载长度大于 MSS，则将 TCP Data 字段修剪为 Maximum Segment Size (MSS)

阻止不可解析的 TCP 报头异常 (Block Unresolvable TCP Header Anomalies)

启用此选项时，系统阻止异常 TCP 数据包，这些数据包在规范化的情况下会无效，并可能受到接收主机的阻止。例如，系统阻止后续传输到已建立的会话上的任何 SYN 数据包。

无论是否启用规则，系统都会丢弃与以下任何 TCP 数据流预处理器规则匹配的任何数据包：

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 至 129:19

Total Blocked Packets 性能图跟踪内联部署中阻止的数据包的数量，并且，在被动部署和轻触模式下的内联部署中，跟踪在内联部署中已阻止的数量。

显式堵塞通知

对显式堵塞通知 (ECN) 标志启用逐个数据包或逐条数据流规范化，如下所示：

- 选择 **Packet** 以逐个数据包清除 ECN 标志（无论协商与否）
- 选择 **Stream** 以逐条数据流清除 ECN 标志（如果未协商 ECN 的使用）

如果选择**数据流 (Stream)**，您还必须确保启用 TCP 数据流预处理器的**需要 TCP 三次握手 (Require TCP 3-Way Handshake)** 选项以进行此规范化。

清除现有 TCP 选项 (Clear Existing TCP Options)

启用**允许这些 TCP 选项 (Allow These TCP Options)**。

允许这些 TCP 选项 (Allow These TCP Options)

禁用您在流量中允许的特定 TCP 选项的规范化。

系统不对您明确允许的选项进行规范化。系统会通过将您未明确允许的选项设置为“无操作”(No Operation)（TCP 选项 1）来规范化这些选项。

由于这些选项常用于实现最佳 TCP 性能，因此无论**允许这些 TCP 选项**的配置如何，系统始终会允许以下选项：

- 最大分片大小 (MSS)
- 窗口比例
- 时间戳 TCP

系统不会自动允许其他不太常用的选项。

您可以通过配置选项关键字和/或选项编号的逗号分隔列表来允许特定选项，如下例所示：

```
sack, echo, 19
```

指定选项关键字等同于指定与该关键字相关的一个或多个 TCP 选项的编号。例如，指定 `sack` 等同于指定 TCP 选项 4（“允许选择性确认 [Selective Acknowledgment Permitted]”）和选项 5（“选择性确认”[Selective Acknowledgment]）。选项关键字不区分大小写。

您还可以指定 `any`，这样将会允许所有 TCP 选项并有效地禁用所有 TCP 选项的规范化。

下表总结了如何指定要允许的 TCP 选项。如果将字段留空，则系统仅允许 MSS、Window Scale 和 Time Stamp 选项。

可指定的内容	以允许.....
sack	TCP 选项 4（“允许选择性确认 [Selective Acknowledgment Permitted]”）和选项 5（“选择性确认”[Selective Acknowledgment]）
echo	TCP 选项 6（“回应请求”[Echo Request]）和选项 7（“回应答复”[Echo Reply]）
partial_order	TCP 选项 9（“允许的偏序连接”[Partial Order Connection Permitted]）和选项 10（“偏序服务配置文件”[Partial Order Service Profile]）
conn_count	TCP 连接计数选项 11 (CC)、选项 12 (CC.New) 和选项 13 (CC.Echo)
alt_checksum	TCP 选项 14（“替代校验和请求”[Alternate Checksum Request]）和选项 15（“替代校验和”[Alternate Checksum]）
md5	TCP 选项 19（“MD5 签名”[MD5 Signature]）
选项编号（2 至 255）	特定选项，包括没有关键字的选项
any	所有 TCP 选项；此设置会有效地禁用 TCP 选项规范化

如果没有为此选项指定 `any`，则规范化会包含以下内容：

- 除 MSS、“窗口比例”(Window Scale)、“时间戳”(Time Stamp) 及任何明确允许的选项以外，所有选项字节都设置为“无操作”(No Operation)（TCP 选项 1）
- 如果时间戳存在但无效，或者有效但未协商，则将时间戳八位元设置为“无操作”(No Operation)
- 如果“时间戳”(Time Stamp) 已协商但不存在，则阻止数据包
- 如果未设置 Acknowledgment (ACK) 控制位，则清除“时间戳回应答复 (TSecr)”(Time Stamp Echo Reply [TSecr]) 选项字段
- 如果未设置 SYN 控制位，则将 MSS 和 Window Scale 选项设置为 No Operation (TCP Option 1)

配置内联规范化

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

开始之前

- 如果要规范化或丢弃恶意数据包，请启用**内联模式 (Inline Mode)**，如内联部署中预处理器流量的修改，第 2064 页中所述。受管设备也必须内联部署。

过程

步骤 1 选择**策略 > 访问控制**，然后点击 **网络分析策略**或**策略 > 访问控制 > 入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**（不是插入符号；点击单词）。

步骤 5 如果**传输/网络层预处理器 (Transport/Network Layer Preprocessors)** 下的**内联规范化 (Inline Normalization)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击**内联规范化 (Inline Normalization)** 旁边的 **编辑**（）。

步骤 7 设置选项，如内联规范化预处理器，第 2153 页中所述。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要让内联规范化的“最小 TTL”(Minimum TTL) 选项生成入侵事件，请启用任一或两个数据包解码器规则：116:429 (IPv4) 和 116:270 (IPv6)。有关详细信息，请参阅设置入侵规则状态，第 1488 页和内联规范化选项，第 2154 页。
- 部署配置更改。

相关主题

层管理，第 1612 页

冲突和更改：网络分析和入侵策略，第 1459 页

IP 分片重组预处理器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

由于 IP 数据报大于最大传输单位 (MTU) 而将其分为两个或多个更小的 IP 数据报，这个过程即为数据报分片。单个 IP 数据报片段可能未包含足够的信息来识别隐藏攻击。攻击者可能尝试通过将攻击数据传输到分片数据包中来躲避检测。在规则引擎对分片的 IP 数据报执行规则之前，IP 分片重组预处理器会重组这些数据报，以便规则可以更适当地识别这些数据包中的攻击。如果分片的数据报无法重组，则不对其执行规则。

IP 分片重组漏洞

启用 IP 分片重组可以帮助您检测针对网络上主机的攻击（例如泪滴 [teardrop] 攻击）和针对系统本身的资源消耗攻击（例如 Jolt2 攻击）。

泪滴攻击利用某些操作系统中在尝试重组重叠 IP 片段时会导致这些操作系统崩溃的漏洞。IP 分片重组预处理器在被启用并配置为识别重叠片段之后，会执行此操作。IP 分片重组预处理器会检测重叠片段攻击（例如泪滴攻击）中的第一批数据包，但对于同一攻击不会检测后续数据包。

Jolt2 攻击会发送同一分片的 IP 数据包的大量副本，以尝试过度使用 IP 分片重组器并导致拒绝服务攻击。内存使用上限会中断此攻击以及 IP 分片重组预处理器中的类似攻击，并在全面检查基础上注重系统自我保护。这样，系统不会因攻击而崩溃，可保持运行，并继续检查网络流量。

不同的操作系统以不同方式重组分片数据包。可以确定主机运行的操作系统的攻击者还可以对恶意数据包进行分片，以便目标主机以特定方式对这些数据包进行重组。由于系统不知道受监控网络上的主机运行的操作系统，因此预处理器可能会不正确地重组和检查数据包，致使漏洞成功躲过检测。要缓解这种攻击，您可以配置分片重组预处理器，使其会针对网络中的每个主机使用适当方法对数据包进行分片重组。

请注意，您也可以在被动部署中使用自适应配置文件，通过数据包中目标主机的主机操作系统信息来为 IP 分片重组预处理器动态选择基于目标的策略。

基于目标的分片重组策略

主机的操作系统使用三个条件来确定当重组数据包时支持的数据包分片。

- 操作系统收到分片的顺序
- 其偏移量（分片与数据包开始位置之间的距离，按字节计算）
- 它与重叠分片相比的开始和结束位置。

虽然每个操作系统都使用这些条件，但是不同的操作系统在重组分片数据包时支持不同的分片。因此，网络中具有不同操作系统的两个主机可能会以完全不同的方式重组同一组重叠分片。

攻击者如果了解其中一个主机的操作系统，可能会尝试通过发送隐藏在重叠数据包片段中的恶意内容来逃避检测并攻击该主机。该数据包经过重组和检查后看似无害，但是由目标主机进行重组后则会包含恶意的漏洞。但是，如果将 IP 分片重组预处理器配置为可感知受监控网段上运行的操作系统，则它会以与目标主机相同的方式重组分片，从而识别攻击。

IP 分片重组选项

您可以选择只是启用或禁用 IP 分片重组；但是，思科建议以更精细的级别指定已启用的 IP 分片重组预处理器的行为。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

可以配置以下全局选项：

预分配分片 (Preallocated Fragments)

预处理器一次可以处理的最大单个分片数量。指定要预分配的片段节点的数量会启用静态内存分配。

注意 处理单个分片会使用大约1550字节的内存。如果预处理器处理单个片段所需的内存超过受管设备的预定允许的内存限制，则设备的内存限制优先。

您可以为每个 IP 分片重组策略配置以下选项：

网络 (Networks)

要对其应用分片重组策略的一个或多个主机的 IP 地址。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。您可以指定总共最多 255 个配置文件（包括默认策略）。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全全局配置。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或 CIDR 块/前缀长度，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如，0.0.0.0/0 或 ::/0）。

策略

要为受监控网段上的主机组使用的分片重组策略。

根据目标主机的操作系统，可以选择七个分片重组策略之一。下表列出了这七个策略以及使用每个策略的操作系统。第一个和最后一个这两个策略名称反映这些策略是否支持原始或后续重叠数据包。

对于 威胁防御 路由和透明接口，此选项会被忽略。

表 *231:* 基于目标的分片重组策略

策略	操作系统
BSD	AIX FreeBSD IRIX VAX/VMS
BSD-right	HP JetDirect
第一页	Mac OS HP-UX
Linux	Linux OpenBSD
最后一页	思科 IOS
Solaris	SunOS
Windows 的 ISE 安全评估代理	Windows 的 ISE 安全评估代理

超时

指定预处理器引擎在重组分片数据包时可用的最长时间（以秒为单位）。如果在指定的时间段内无法重组数据包，则预处理器引擎会停止尝试重组数据包并丢弃接收到的片段。

最小 TTL

指定数据包可具有的可接受最小 TTL 值。此选项检测基于 TTL 的插入攻击。

您可以启用规则 123:11 为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测异常

确定分片问题，例如重叠分片。

对于 威胁防御 路由和透明接口，此选项会被忽略。

您可以通过启用以下规则来为此选项生成事件并在内联部署中丢弃攻击性数据包：

- 123:1 至 123:4
- 123:5（BSD 策略）
- 123:6 至 123:8

重叠限制 (Overlap Limit)

指定在检测到会话中存在所配置数量的重叠片段时，将会停止该会话的分片重组。

必须启用**检测异常 (Detect Anomalies)** 后才可以配置此选项。不指定值将会禁用此选项。值为 0 指定重叠片段的数量不受限制。

对于 威胁防御 路由和透明接口，此选项会被忽略。在这些接口上始终丢弃重叠分片。

您可以启用规则 123:12 为此选项生成事件并在内联部署中丢弃攻击性数据包。

Minimum Fragment Size

指定在检测到小于所配置数量的非最后一个分片时，数据包将被视为恶意。

必须启用**检测异常 (Detect Anomalies)** 后才可以配置此选项。不指定值将会禁用此选项。值 0 表示无限字节数。

您可以启用规则 123:13 为此选项生成事件并在内联部署中丢弃攻击性数据包。

配置 IP 分片重组

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

开始之前

- 确认您要在基于目标的自定义策略中识别的任何网络匹配，或者是其父网络分析策略所处理的网络、区域和 VLAN 的子集。有关详细信息，请参阅网络分析策略的高级设置，第 2043 页。

过程

步骤 1 选择**策略** > **访问控制**，然后点击 **网络分析策略**或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（ ）。

如果显示**视图**（ ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**传输/网络层预处理器 (Transport/Network Layer Preprocessors)** 下的 **IP 分片重组 (IP Defragmentation)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击 **IP 分片重组 (IP Defragmentation)** 旁边的 **编辑**（）。

步骤 7 或者，在**预分配片段 (Preallocated Fragments)** 字段中输入值。

步骤 8 有以下选项可供选择：

- 添加服务器配置文件 - 点击页面左侧**服务器 (Servers)** 旁边的 **添加**（），然后在**主机地址 (Host Address)** 字段中输入值，并点击**确定 (OK)**。可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。可以创建总共 255 个基于目标的策略（包括默认策略）。
- 编辑服务器配置文件 - 点击页面左侧**服务器 (Servers)** 下的已配置地址，或点击**默认 (default)**。
- 删除配置文件 - 点击策略旁边的 **删除**（）。

步骤 9 修改IP 分片重组选项，第 2161 页中所述的选项。

步骤 10 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果希望生成事件并在内联部署中丢弃攻击性数据包，则请启用 IP 解除分段规则 (GID 123)。有关详细信息，请参阅设置入侵规则状态，第 1488 页和IP 分片重组选项，第 2161 页。
- 部署配置更改。

相关主题

层基础知识，第 1607 页
冲突和更改：网络分析和入侵策略，第 1459 页

数据包解码器

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

在将捕获的数据包发送到预处理器之前，系统首先会将数据包发送到数据包解码器。数据包解码器将数据包报头和负载转换为便于预处理器和规则引擎使用的格式。每个堆栈层依次进行解码，从数据链路层开始并继续直至网络层和传输层。

数据包解码器选项

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

解码 GTP 数据通道 (Decode GTP Data Channel)

解码封装的GTP（通用分组无线服务[GPRS]隧道协议）数据通道。默认情况下，解码器在端口3386上解码版本0数据，在端口2152上解码版本1数据。您可以使用默认变量 `GTP_PORTS` 来修改用于识别封装 GTP 流量的端口。

您可以启用规则 116:297 和 116:298 以为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测非标准端口上的 Teredo (Detect Teredo on Non-Standard Ports)

检测 UDP 端口（而非端口 3544）上识别的 IPv6 流量的 Teredo 隧道。

只要 IPv6 流量存在，系统总会检测到 IPv6 流量。默认情况下，IPv6 检测包括 4in6、6in4、6to4 和 6in6 隧道方案；当 UDP 报头指定端口 3544 时，还包括 Teredo 隧道。

在 IPv4 网络中，IPv4 主机可使用 Teredo 协议通过 IPv4 网络地址转换 (NAT) 设备隧道传输 IPv6 流量。Teredo将在IPv4 UDP数据报内封装IPv6数据包，以允许在IPv4 NAT设备后面执行IPv6连接。正常情况下，系统使用 UDP 端口 3544 来识别 Teredo 流量。但是，攻击者可能会使用非标准端口来尝试避开检测。您可以启用**检测非标准端口上的 Terado (Detect Teredo on Non-Standard Ports)**，使系统检查 Teredo 隧道的所有 UDP 负载。

系统仅在外网层使用IPv4时才会执行Teredo解码，并且仅对第一个UDP报头执行Teredo解码。如果由于UDP数据封装在IPv6数据中，导致Teredo IPv6层之后还有一层UDP，规则引擎将使用UDP入侵规则来分析内外 UDP 层。

请注意，**策略-其他 (policy-other)** 规则类别中的入侵规则 12065、12066、12067 和 12068 会检测 Teredo 流量，但不对这些流量进行解码。您可以根据需要在内联部署中使用这些规则丢弃 Teredo 流量；但是，启用**检测非标准端口上的 Terado (Detect Teredo on Non-Standard Ports)** 时，应确保这些规则处于禁用状态或者设置为生成事件而不丢弃流量。

检测多余长度值 (Detect Excessive Length Value)

在数据包报头指定的数据包长度大于实际数据包长度时进行检测。

对于威胁防御路由、透明和内联接口，此选项会被忽略。始终丢弃报头长度过长的数据包。但此选项适用于 威胁防御 内联分流和被动接口。

您可以启用规则 116:6、116:47、116:97 和 116:275 以为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测无效 IP 选项 (Detect Invalid IP Options)

检测无效的 IP 报头选项，以识别使用无效 IP 选项的攻击。例如，有一项针对防火墙的拒绝服务攻击，导致系统冻结。防火墙尝试解析无效的“时间戳”(Timestamp) 和“安全 IP”(Security IP) 选项且未能检查到零长度，导致无法恢复的无限循环。规则引擎将识别零长度选项，并提供相关信息供您通过防火墙缓解攻击。

威胁防御 设备将丢弃任何包含除任何路由或透明接口上的路由器警报、选项列表结束 (EOOL) 以及无操作 (NOP) 选项之外的 IP 选项的 RSVP 数据包。对于内联、内联分流或被动接口，对 IP 选项的处理如上所述。

您可以启用规则 116:4 和 116:5 以为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测试验性 TCP 选项 (Detect Experimental TCP Options)

检测使用试验性 TCP 选项的 TCP 报头。下表介绍了这些选项。

TCP 选项	说明
9	允许的偏序连接
10	偏序服务配置文件
14	替代校验和请求
15	替代校验和数据
18	尾部校验和
20	空间通信协议标准
21	选择性否定确认
22	记录边界 (SCPS)
23	损坏 (SPCS)
24	SNAP
26	TCP 压缩过滤器

由于这些是试验性选项，所以有些系统未使用它们，从而可能遭受攻击。

注释 除上表中列出的试验性选项之外，系统还会考虑选项编号大于 26 的任何试验性 TCP 选项。

您可以启用规则 116:58 以为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测过时 TCP 选项 (Detect Obsolete TCP Options)

检测使用过时 TCP 选项的 TCP 报头。由于这些是过时选项，所以有些系统未使用它们，从而可能遭受攻击。下表介绍了这些选项。

TCP 选项	说明
6	回应
7	回应应答

TCP 选项	说明
16	Skeeter
17	Bubba
19	MD5 签名
25	未分配

您可以启用规则 116:57 以为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测 T/TCP (Detect T/TCP)

检测使用 CC.ECHO 选项的 TCP 报头。CC.ECHO 选项可确认是否正在使用 TCP 事务协议 (T/TCP)。由于 T/TCP 报头选项未被广泛应用，所以有些系统未使用它们，从而可能遭受攻击。

您可以启用规则 116:56 以为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测其他 TCP 选项 (Detect Other TCP Options)

检测其中的无效 TCP 选项未被其他 TCP 解码事件选项检测到的 TCP 报头。例如，此选项会检测长度不正确或长度致使选项数据超出 TCP 报头的 TCP 选项。

对于 威胁防御 路由和透明接口，此选项会被忽略。始终丢弃具有无效 TCP 选项的数据包。

您可以启用规则 116:54、116:55 和 116:59 以为此选项生成事件并在内联部署中丢弃攻击性数据包。

检测协议报头异常 (Detect Protocol Header Anomalies)

检测更具体的 IP 和 TCP 解码器选项未检测到的其他解码错误。例如，解码器可能会检测到格式错误的数据链路协议报头。

对于威胁防御路由、透明和内联接口，此选项会被忽略。始终丢弃报头异常的数据包。但此选项适用于威胁防御内联分流和被动接口。

要为此选项生成事件并在内联部署中丢弃攻击性数据包，可以启用以下任一规则：

GID:SID	在以下情况下生成事件：
116:467	数据包小于用　思科 FabricPath 报头封装的数据包的最小尺寸。
116:468	报头中的思科元数据 (CMD) 字段包含长度小于有效 CMD 报头最小尺寸的报头。CMD 字段与思科 Trustsec 协议相关联。
116:469	报头中的 CMD 字段包含无效字段长度。
116:470	报头中的 CMD 字段包含无效安全组标记 (SGT) 选项类型。
116:471	报头中的 CMD 字段包含具有保留值的 SGT。

您也可以启用与其他数据包解码器选项不关联的任何数据包解码器规则。

相关主题

预定义默认变量，第 1044 页

配置数据包解码

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择**策略** > **访问控制**，然后点击 **网络分析策略**或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**传输/网络层预处理器 (Transport/Network Layer Preprocessors)** 下的**数据包解码 (Packet Decoding)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击**数据包解码 (Packet Decoding)** 旁边的 **编辑**（）。

步骤 7 启用或禁用数据包解码器选项，第 2165 页中所述的选项。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成事件并在内联部署中丢弃攻击性数据包，请启用数据包解码器规则 (GID 116)。有关详细信息，请参阅设置入侵规则状态，第 1488 页和数据包解码器选项，第 2165 页。
- 部署配置更改。

相关主题

层基础知识，第 1607 页
冲突和更改：网络分析和入侵策略，第 1459 页

TCP 数据流预处理

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

TCP 协议定义连接可以处于的各种状态。每个 TCP 连接通过源 IP 地址和目标 IP 地址以及源端口和目标端口进行识别。TCP 一次仅允许存在一个具有相同连接参数值的连接。

状态相关的 TCP 漏洞

如果向入侵规则添加带有 `established` 参数的 `flow` 关键字，则入侵规则引擎会在有状态模式下检查与规则和流指令匹配的数据包。状态模式仅评估通过客户端与服务器之间的合法三次握手建立的TCP会话所包含的流量。

您可以配置系统，以便预处理器对无法识别为已建立的 TCP 会话的一部分的任何 TCP 流量进行检测；但是，对于典型使用不建议此操作，因为事件会使系统迅速过载且不会提供有意义的数据。

stick 和 snot 之类的攻击针对自身使用系统的广泛规则集和数据包检测。这些工具根据基于 Snort 的入侵规则生成数据包，并通过网络发送这些数据包。如果您的规则不包括用于为状态检测配置规则的 `flow` 或 `flowbits` 关键字，则每个数据包将触发规则，进而导致系统过载。您可以通过状态检测来忽略这些数据包，因为它们不是已建立的TCP会话的一部分，而且不提供有意义的信息。执行状态检测时，规则引擎仅检测属于已建立的TCP会话的一部分的那些攻击，从而使分析人员关注这些攻击而不是由 stick 或 snot 攻击导致的事件量。

基于目标的 TCP 策略

不同操作系统以不同方法实施TCP。例如，Windows和其他一些操作系统需要TCP重置段以具有精确的 TCP 序列号来重置会话，而 Linux 和其他操作系统则允许使用一系列序列号。在本示例中，数据流预处理器必须明确了解目标主机会如何根据序列号对重置作出响应。仅当目标主机认为重置有效时，数据流预处理器才会停止跟踪会话，因此，攻击在预处理器停止检查数据流后无法通过发送数据包来躲避检测。在TCP实施中的其他变化包括操作系统是否采用TCP时间戳选项，并且在采用时如何处理时时间戳，以及操作系统接受还是忽略 SYN 数据包中的数据等等方面。

不同操作系统也以不同方式重组重叠的 TCP 数据段。重叠的 TCP 数据段可能会反映未确认的 TCP 流量的正常重传。它们也可能表示攻击者（了解其中一个主机的操作系统）尝试通过发送隐藏在重叠数据段中的恶意内容来躲避检测并利用该主机。但是，您可以将数据流预处理器配置为可感知受监控网段上运行的操作系统，使其以与目标主机相同的方式重组数据段，从而识别攻击。

您可以创建一个或多个 TCP 策略，以根据受监控网段上的不同操作系统定制 TCP 数据流检查和重组。对于每个策略，可识别 13 个操作系统策略之一。您根据需要使用尽可能多的 TCP 策略将每个 TCP 策略绑定到特定 IP 地址或地址块，以识别使用其他操作系统的任意或所有主机。默认 TCP 策略适用于在任何其他TCP策略中未识别的受监控网络上的任何主机，因此无需为默认TCP策略指定 IP 地址或地址块。

请注意，您也可以在被动部署中使用自适应配置文件，通过数据包中目标主机的主机操作系统信息来为 TCP 流预处理器动态选择基于目标的策略。

TCP 数据流重组

数据流预处理器收集和重组属于TCP会话的服务器到客户端通信数据流和/或客户端到服务器通信数据流的一部分的所有数据包。这允许规则引擎将数据流作为单个已重组实体进行检查，而不是仅检查属于指定数据流的一部分的个别数据包。

数据流重组允许规则引擎识别基于数据流的攻击，在检查个别数据包时它可能无法检测此类攻击。您可以根据网络需要指定规则引擎重组哪些通信数据流。例如，在监控网络服务器上的流量时，您可能只希望检查客户端流量，因为您不太可能从自己的网络服务器接收到恶意流量。

在每个 TCP 策略中，您可以指定用于识别要重组的数据流预处理器流量的端口的逗号分隔列表。启用自适应配置文件后，您还可以列出用于识别要重组的流量的服务（以替代端口或端口组合的形式）。

您可以指定端口和/或服务。您可以为客户端端口和/或服务器端口的任意组合指定单独的端口列表。您还可以为客户端服务和/或服务器服务指定单独的服务列表。例如，假设您要重组以下内容：

- 来自客户端的 SMTP（端口 25）流量
- FTP 服务器响应（端口 21）
- 两个方向的 telnet（端口 23）流量

您可以配置以下内容：

- 对于客户端端口，指定 `23 和 25`
- 对于服务器端口，指定 `21 和 23`

或者，您可以配置以下内容：

- 对于客户端端口，指定 `25`
- 对于服务器端口，指定 `21`
- 对于客户端端口和服务器端口，指定 `23`

此外，请参考以下示例，该示例将端口和服务进行组合，并在启用自适应配置文件后有效：

- 对于客户端端口，指定 `23`
- 对于客户端服务，指定 `smtp`
- 对于服务器端口，指定 `21`
- 对于服务器服务，指定 `telnet`

取消一个端口（例如，`!80`）可通过阻止 TCP 数据流预处理器处理该端口的流量来提升性能。

虽然您也可以指定 `all` 作为参数来为所有端口提供重组，但是思科不建议将端口设置为 `all`，因为这样做可能会不必要地增加此预处理器检查的流量并降低性能。

TCP 重组自动透明地包括添加到其他预处理器的端口。但是，如果明确向已添加到其他预处理器配置的 TCP 重组列表中添加端口，则会正常处理这些附加端口。这包括下列预处理器的端口列表：

- FTP/Telnet（服务器级 FTP）
- DCE/RPC
- HTTP 检查
- SMTP
- 会话发起协议
- POP
- IMAP
- SSL

请注意，重组其他流量类型（客户端和/或服务器）会增加资源需求。

TCP 数据流预处理选项

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

可以配置以下全局 TCP 选项：

数据包类型性能提高

支持忽略已启用规则中未指定的所有端口和应用协议的 TCP 流量，但在源端口和目标端口均设置为 `any` 的 TCP 规则具有 `flow` 或 `flowbits` 选项时除外。这种性能改进可能会导致未能检测出某些攻击。

可为每个 TCP 策略配置以下选项：

网络

指定要对其应用 TCP 数据流重组策略的主机 IP 地址。

可以指定单个 IP 地址或地址块。总共最多可以指定 255 个配置文件（包括默认策略）。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或 CIDR 块/前缀长度，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如，0.0.0.0/0 或 ::/0）。

策略

识别一个或多个目标主机的 TCP 策略操作系统。如果选择除 **Mac OS** 以外的其他策略，则系统会从同步 (SYN) 数据包中删除数据并禁用规则 129:2 的事件生成。请注意，启用内联规范化预处理器的 **SYN 时删除数据 (Remove Data on SYN)** 选项也会禁用规则 129:2。

下表列出了操作系统策略以及使用每个策略的主机操作系统。

表 *232: TCP* 操作系统策略

策略	操作系统
第一页	未知的操作系统
最后一页	思科 IOS
BSD	AIX FreeBSD OpenBSD
Linux	Linux 2.4 内核 Linux 2.6 内核
旧 Linux	Linux 2.2 及更低版本的内核
Windows 的 ISE 安全评估代理	Windows 98 Windows NT Windows 2000 Windows XP
Windows 2003	Windows 2003
Windows Vista	Windows Vista
Solaris	Solaris OS SunOS
IRIX	SGI Irix
HPUX	HP-UX 11.0 及更高版本
HPUX 10	HP-UX 10.2 及更高版本
Mac OS	Mac OS 10 (Mac OS X)

提示 当您不知道主机操作系统时，第一个操作系统策略可以提供一些保护。但是，它可能会导致未能检测出某些攻击。如果您知道操作系统，则应该编辑策略以指定正确的操作系统。

Timeout

规则引擎在状态表中保持数据流处于非活动状态的秒数（介于 1 和 86400 之间）。如果数据流在指定时间内未重组，则入侵规则引擎会将其从状态表中删除。

注释 如果受管设备部署在网络流量可能达到设备的带宽限制的网段上，则应该考虑将该值设置为较高的值（例如 600 秒），以降低处理开销。

威胁防御 设备会忽略此选项，而是使用高级访问控制**威胁防御服务策略**中的设置。有关详细信息，请参阅配置服务策略规则，第 1416 页。

最大 TCP 窗口 (Maximum TCP Window)

指定由接收主机指定的所允许的最大 TCP 窗口大小（1 至 1073725440 字节）。值设置为 0 会禁用检查 TCP 窗口大小。

注意 上限是 RFC 允许的最大窗口大小，旨在防止攻击者躲避检测；但是，设置明显过大的最大窗口大小可能导致自愿接受的拒绝服务。

状态检查异常处于启用状态时，可以启用规则 129:6 为此选项生成事件并在内联部署中丢弃攻击性数据包。

重叠限制 (Overlap Limit)

指定在检测到某会话中存在所配置数量（介于 0 [无限制] 和 255 之间）的重叠分片时，针对该会话的分片重组将会停止，并且，如果**状态检查异常 (Stateful Inspection Anomalies)** 以及随附的预处理器规则均处于启用状态，将会生成事件。

您可以启用规则 129:7 来为此选项生成事件并在内联部署中丢弃攻击性数据包。

刷新因数 (Flush Factor)

在内联部署中，指定在经过所配置数量（介于 1 和 2048 之间）的大小未减小的分段后检测到大小减小的分段时，系统会刷新为进行检测而累积的分段数据。值设置为 0 会禁用此分段模式的检测（这可能意味着请求或响应结束）。请注意，必须启用 Inline Normalization **Normalize TCP Payload** 选项才会使此选项生效。

状态检查异常 (Stateful Inspection Anomalies)

检测 TCP 堆栈中的异常行为。启用随附的预处理器规则后，如果 TCP/IP 堆栈编写得不好，可能会生成许多事件。

对于 威胁防御 路由和透明接口，此选项会被忽略。

您可以通过启用以下规则来为此选项生成事件并在内联部署中丢弃攻击性数据包：

- 129:1 至 129:5

- 129:6（仅适用于 Mac OS）
- 129:8 至 129:11
- 129:13 至 129:19

请注意以下提示：

- 为了触发规则 129:6，还必须为**最大 TCP 窗口**配置一个大于 0 的值。
- 为了触发规则 129:9 和 129:10，还必须启用 **TCP 会话劫持**。

TCP 会话劫持

通过针对会话上接收到的后续数据包验证三次握手期间从 TCP 连接两端检测到的硬件 (MAC) 地址来检测 TCP 会话劫持。当一端或另一端的 MAC 地址不匹配时，如果启用了**状态检查异常 (Stateful Inspection Anomalies)** 以及两个对应的预处理器规则之一，系统会生成事件。

对于 威胁防御 路由和透明接口，此选项会被忽略。

您可以启用规则 129:9 和 129:10 来为此选项生成事件并在内联部署中丢弃攻击性数据包。请注意，为了让这些规则中任一个生成事件，还必须启用**状态检查异常 (Stateful Inspection Anomalies)**。

连续小分片 (Consecutive Small Segments)

状态检查异常 (Stateful Inspection Anomalies) 处于启用状态时，可指定允许的连续 TCP 小分片的最大数量（1 至 2048）。值设置为 0 会禁止连续小分片。

此选项必须与**小分片大小 (Small Segment Size)** 选项一起进行设置；您可以同时禁用这两个选项或者将它们都设置为非零值。请注意，在无干预确认的情况下接收多达2000个连续分段，即使每个分段长度为 1 字节，分段数量也会远远超出您通常的预期。

对于 威胁防御 路由和透明接口，此选项会被忽略。

您可以启用规则 129:12 来为此选项生成事件并在内联部署中丢弃攻击性数据包。

小分片大小 (Small Segment Size)

状态检查异常 (Stateful Inspection Anomalies) 处于启用状态时，可指定被视为小分片的 TCP 分片大小（1 至 2048 字节）。值设置为 0 会禁止指定小分片的大小。

对于 威胁防御 路由和透明接口，此选项会被忽略。

此选项必须与**连续小分片 (Consecutive Small Segments)** 选项一起进行设置；您可以同时禁用这两个选项或者将它们都设置为非零值。请注意，一个 2048 字节的 TCP 分段大于普通的 1500 字节的以太网帧。

忽略小分片的端口 (Ports Ignoring Small Segments)

状态检查异常 (Stateful Inspection Anomalies)、**连续小分片 (Consecutive Small Segments)** 和**小分片大小 (Small Segment Size)** 处于启用状态时，可指定一个或多个会忽略小 TCP 分片检测的端口的逗号分隔列表。将此选项留空表示未忽略任何端口。

对于 威胁防御 路由和透明接口，此选项会被忽略。

您可以向列表中添加任何端口，但是列表仅影响TCP策略中的某个**对端口执行数据流重组 (Perform Stream Reassembly on port)** 列表中指定的端口。

需要 TCP 三次握手 (Require TCP 3-Way Handshake)

指定仅在 TCP 三次握手完成时，会话才被视为已建立的会话。禁用此选项可提高性能，防御 SYN 泛洪攻击，并允许在部分异步环境中操作。启用此选项可避免尝试通过发送不属于已建立的 TCP 会话的信息来生成误报的攻击。

您可以启用规则 129:20 来为此选项生成事件并在内联部署中丢弃攻击性数据包。

三次握手超时 (3-Way Handshake Timeout)

指定启用**需要 TCP 三次握手 (Require TCP 3-Way Handshake)** 后必须允许用于完成握手的时间（0 [无限制] 至 86400 秒 [24 小时]）。必须启用**需要 TCP 三次握手 (Require TCP 3-Way Handshake)** 后才能修改此选项的值。

对于 Firepower 软件设备和 威胁防御 内联、内联分流和被动接口，默认值为 0。对于 威胁防御 路由和透明接口，超时始终为 30 秒；此处配置的值会被忽略。

数据包大小性能提升 (Packet Size Performance Boost)

将预处理器设置为在重组缓冲区中不对大数据包进行排队。这种性能改进可能会导致未能检测出某些攻击。禁用此选项可防止使用 1 到 20 字节的小数据包尝试躲避检测。当您肯定所有流量都由超大数据包组成并因此无此类攻击时，可启用此选项。

旧版重组 (Legacy Reassembly)

重组数据包时，将数据流预处理器设置为模拟废弃的数据流 4 预处理器，借此可以将该数据流预处理器重组的事件与基于数据流 4 预处理器重组的相同数据流的事件相比较。

异步网络 (Asynchronous Network)

指定受监控网络是否为异步网络，即，系统只能看到一半流量的网络。启用此选项后，系统不重组 TCP 数据流来提高性能。

对于 威胁防御 路由和透明接口，此选项会被忽略。

对客户端端口执行数据流重组 (Perform Stream Reassembly on Client Ports)

根据连接的客户端的端口启用数据流重组。换句话说，它对目标为网络服务器、邮件服务器或通常由 $HOME_NET 中指定的 IP 地址定义的其他 IP 地址的数据流进行重组。如果您预计客户端会发出恶意流量，请使用此选项。

对于 威胁防御 路由和透明接口，此选项会被忽略。

对客户端服务执行数据流重组 (Perform Stream Reassembly on Client Services)

根据连接的客户端的服务启用数据流重组。如果您预计客户端会发出恶意流量，请使用此选项。

必须为选择的每个客户端服务至少启用一个客户端检测器。默认情况下，思科提供的所有检测器均已激活。如果没有为相关客户端应用启用检测器，则系统会自动为应用启用思科提供的所有检测器；如果不存在任何检测器，则系统会为应用启用最近修改的用户定义的检测器。

此功能需要保护和控制许可证。

对于 威胁防御 路由和透明接口，此选项会被忽略。

对服务器端口执行数据流重组 (Perform Stream Reassembly on Server Ports)

根据连接的服务器端的端口启用数据流重组。换句话说，它对从网络服务器、邮件服务器或通常由 $EXTERNAL_NET 中指定的 IP 地址定义的其他 IP 地址发出的数据流进行重组。当您要监控服务器端攻击时，请使用此选项。您可以通过不指定端口来禁用此选项。

对于 威胁防御 路由和透明接口，此选项会被忽略。

注释 对于服务的全面检查，除了在对服务器端口执行数据流重组字段中添加端口号以外，还要在对服务器服务执行数据流重组字段中添加服务名称。例如，除了在对服务器端口执行数据流重组字段中添加端口号 80 以外，还要在对服务器服务执行数据流重组字段中添加“**HTTP**”服务，以检查 HTTP 服务。

对服务器服务执行数据流重组 (Perform Stream Reassembly on Server Services)

根据连接的服务器端的服务启用数据流重组。当您要监控服务器端攻击时，请使用此选项。您可以通过不指定服务来禁用此选项。

必须至少启用一个检测器。默认情况下，思科提供的所有检测器均已激活。如果没有为服务启用检测器，则系统会自动为相关应用协议启用思科提供的所有检测器；如果不存在任何检测器，则系统会为该应用协议启用最近修改的用户定义的检测器。

此功能需要保护和控制许可证。

对于 威胁防御 路由和透明接口，此选项会被忽略。

对客户端端口和服务器端口执行数据流重组 (Perform Stream Reassembly on Both Ports)

根据连接的客户端和服务器端的端口启用数据流重组。如果您预计相同端口的恶意流量在客户端和服务器之间可能以任一方向传播，请使用此选项。您可以通过不指定端口来禁用此选项。

对于 威胁防御 路由和透明接口，此选项会被忽略。

对客户端服务和服务器服务执行数据流重组 (Perform Stream Reassembly on Both Services)

根据连接的客户端和服务器端的服务启用数据流重组。如果您预计相同服务的恶意流量在客户端和服务器之间可能以任一方向传播，请使用此选项。可以通过不指定服务来禁用此选项。

必须至少启用一个检测器。默认情况下，思科提供的所有检测器均已激活。如果没有为相关客户端应用或应用协议启用检测器，则系统会自动为应用或应用协议启用思科提供的所有检测器；如果不存在任何检测器，则系统会为应用或应用协议启用最近修改的用户定义的检测器。

此功能需要保护和控制许可证。

对于 威胁防御 路由和透明接口，此选项会被忽略。

Troubleshooting Options: Maximum Queued Bytes

支持人员可能会在故障排除呼叫期间要求您指定可以在 TCP 连接的一端排队的数据量。值 0 表示无限字节数。

注意 更改此故障排除选项的设置会影响性能，应仅在支持人员的指导下进行操作。

故障排除选项：最大排队分片数 (Troubleshooting Options: Maximum Queued Segments)

支持人员可能会在故障排除呼叫期间要求您指定可以在 TCP 连接的一端排队的数据段的最大字节数。值 0 表示无限的数据段字节数。

注意 更改此故障排除选项的设置会影响性能，应仅在支持人员的指导下进行操作。

相关主题

激活和停用检测器，第 1962 页
层管理，第 1612 页
冲突和更改：网络分析和入侵策略，第 1459 页

配置 TCP 数据流预处理

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

开始之前

- 确认您要在基于目标的自定义策略中识别的网络匹配，或者是其父网络分析策略所处理的网络、区域和 VLAN 的子集。有关详细信息，请参阅网络分析策略的高级设置，第 2043 页。

过程

步骤 1 选择**策略** > **访问控制**，然后点击 **网络分析策略**或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释　如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击要修改的策略旁边的 **编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击左侧导航面板中的 **Settings**。

步骤 5 如果“传输/网络层预处理器”(Transport/Network Layer Preprocessors) 下的 **TCP 数据流配置 (TCP Stream Configuration)** 设置已禁用，请通过点击**已启用 (Enabled)** 进行启用。

步骤 6 点击 **TCP 数据流配置 (TCP Stream Configuration)** 旁边的 **编辑**（）。

步骤 7 选中或清除**全局设置 (Global Settings)** 部分中的**数据包类型性能提升 (Packet Type Performance Boost)** 复选框。

步骤 8 您可以执行以下操作：

- 添加基于目标的策略 - 点击“目标”(Targets) 部分中的**主机 (Hosts)** 旁边的 **添加**（）。在**主机地址 (Host Address)** 字段中指定一个或多个 IP 地址。可以指定单个 IP 地址或地址块。可以创建总共 255 个基于目标的策略（包括默认策略）。完成后，点击**确定 (OK)**。
- 编辑基于目标的现有策略 - 在**主机 (Hosts)** 下，点击要编辑的策略的地址，或点击默认值以在**默认值 (default)** 中编辑默认配置值。
- 修改 TCP 数据流预处理选项 - 请参阅 TCP 数据流预处理选项，第 2171 页。

  注意　请勿修改**最大排队字节数 (Maximum Queued Bytes)** 或**最大排队分片数 (Maximum Queued Segments)**，除非支持人员指示执行此操作。

  提示　要根据客户端服务和/或服务器服务修改数据流重组设置，请在要修改的字段内点击，或者点击要修改的字段旁边的**编辑 (Edit)**。使用箭头在弹出窗口中的**可用 (Available)** 和**已启用 (Enabled)** 列表之间移动服务，然后点击**确定 (OK)**。

- 删除基于目标的现有策略 - 点击要删除的策略旁边的 **删除**（）。

步骤 9 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成事件并在内联部署中丢弃攻击性数据包，请启用 TCP 流预处理器规则 (GID 129)。有关详细信息，请参阅设置入侵规则状态，第 1488 页和TCP 数据流预处理选项，第 2171 页。
- 部署配置更改。

相关主题

层管理，第 1612 页

冲突和更改：网络分析和入侵策略，第 1459 页

UDP 数据流预处理

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

当规则引擎使用以下任何参数根据包含 `flow` 关键字的 UDP 规则处理数据包时，会发生 UDP 数据流预处理：

- 已建立
- 至客户端
- 自客户端
- 至服务器
- 自服务器

在会话方面通常未考虑 UDP 数据流。UDP 是一个无连接协议，并不提供在两个终端之间建立通信信道、交换数据和关闭该信道的方法。但是，数据流预处理器使用封装 IP 数据报报头中的源和目标 IP 地址字段及 UDP 报头中的端口字段来确定流动方向并识别会话。当超过可配置的计时器时，或者当任一终端收到表明另一个终端不可达或所请求的服务不可用的 ICMP 消息时，会话将会结束。

请注意，系统不生成与 UDP 数据流预处理相关的事件；但是，您可以启用相关数据包解码器规则来检测 UDP 协议报头异常。

相关主题

TCP 报头值和数据流大小，第 1556 页

UDP 数据流预处理选项

超时

指定预处理器在状态表中保持非活动数据流的秒数。如果在指定时间内看不到其他数据报，预处理器会从状态表中删除数据流。

威胁防御 设备会忽略此选项，而是使用高级访问控制**威胁防御服务策略**中的设置。有关详细信息，请参阅配置服务策略规则，第 1416 页。

数据包类型性能提高

将预处理器设为忽略已启用规则中未指定的所有端口和应用协议的 UDP 流量，但在源端口和目标端口均设置为 `any` 的 UDP 规则具有 `flow` 或 `flowbits` 选项时除外。这种性能改进可能会导致未能检测出某些攻击。

配置 UDP 数据流预处理

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择**策略 > 访问控制**，然后点击 **网络分析策略**或**策略 > 访问控制 > 入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**传输/网络层预处理器 (Transport/Network Layer Preprocessors)** 下的 **UDP 数据流配置 (UDP Stream Configuration)** 已禁用，请点击**启用 (Enabled)**。

步骤 6 点击 **UDP 数据流配置 (UDP Stream Configuration)** 旁边的 **编辑**（）。

步骤 7 设置选项，如UDP 数据流预处理选项，第 2179 页中所述。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

下一步做什么

- 如果要生成事件并在内联部署中丢弃攻击性数据包，请启用相关数据包解码器规则 (GID 116)。有关详细信息，请参阅设置入侵规则状态，第 1488 页和数据包解码器，第 2164 页。
- 部署配置更改。

相关主题

层管理，第 1612 页
冲突和更改：网络分析和入侵策略，第 1459 页

第 91 章

具体威胁检测

以下主题介绍如何在网络分析策略中使用预处理器检测特定威胁：

特定威胁检测简介

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

您可以在网络分析策略中使用若干预处理器检测对受监控网络的具体威胁（例如，后洞攻击、若干端口扫描类型和尝试通过大量流量淹没网络的基于速率的攻击）。在启用特定于预处理器的 GID 签名时，Web 上的网络分析策略将显示为已禁用。但是，预处理器将使用可用的默认设置来开启设备。

您还可以使用在入侵规则中配置的敏感数据检测来检测以非安全方式传输的敏感数字数据。

特定威胁检测的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

特定威胁检测的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

Back Orifice 检测

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

Firepower 系统提供用于检测是否存在 Back Orifice 程序的预处理器。此程序可用于获取对 Windows 主机的管理员访问权限。

Back Orifice 检测预处理器

Back Orifice 预处理器为 Back Orifice 神奇 cookie "*!*QWTY?"（位于数据包的前八个字节且使用 XOR 加密）分析 UDP 流量。

Back Orifice 预处理器具有配置页面，但没有配置选项。如果启用此预处理器，则还必须为其启用预处理器规则，以生成事件并在内联部署中丢弃攻击性数据包。

表 233: Back Orifice GID:SID

预处理器规则 GID:SID	说明
105:1	检测到 Back Orifice 流量
105:2	检测到 Back Orifice 客户端流量
105:3	检测到 Back Orifice 服务器流量

预处理器规则 **GID:SID**	说明
105:4	检测到 Back Orifice Snort 缓冲区攻击

检测 Back Orifice

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

过程

步骤 1 选择**策略** > **访问控制**，然后点击 **网络分析策略**或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（ ）。

如果显示**视图**（ ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击导航面板中的**设置 (Settings)**。

步骤 5 如果**特定威胁检测 (Specific Threat Detection)** 下的 **Back Orifice 检测 (Back Orifice Detection)** 已禁用，请点击**已启用 (Enabled)**。

注释 Back Orifice 无用户可配置选项。

步骤 6 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 如果要生成事件并在内联部署中丢弃攻击性数据包，请启用 Back Orifice 检测规则 105:1、105:2、105:3 或 105:4 有关详细信息，请参阅入侵规则状态，第 1487 页和Back Orifice 检测预处理器，第 2182 页。
- 部署配置更改。

端口扫描检测

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

端口扫描是一种通常被攻击者用作攻击前奏的网络侦察形式。在端口扫描中，攻击者将特制的数据包发送到目标主机。通过检查主机响应时所用的数据包，攻击者通常可以直接或通过推理确定主机上的哪些端口是开放的，以及哪种应用协议正在这些端口上运行。

端口扫描本身不算是攻击。事实上，攻击者使用的一些端口扫描技术也可能会被网络上的合法用户使用。思科的端口扫描检测器旨在通过检测活动模式来帮助确定哪些端口扫描可能是恶意的。

注意 设备将跨内部资源进行负载均衡检查。如果端口扫描检测未按预期工作，您可能需要将灵敏度级别配置为**高 (High)**。

我们强烈建议您升级到 Snort 3 并使用版本 7.2.0 中引入的端口扫描功能。有关更多详细信息，请参阅 《Cisco Secure Firewall Management Center Snort 3 配置指南》 和 Snort 3 检查器参考。

端口扫描类型、协议和过滤的灵敏度级别

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

攻击者可能会使用多种方法来探测网络。他们通常使用不同的协议从目标主机获取不同的响应，以期即使某一种协议被阻止，也可以使用另一种。

表 *234:* 协议类型

协议 (Protocol)	说明 (Description)
TCP	检测 TCP 探针，例如 SYN 扫描、ACK 扫描、TCP connect() 扫描和带异常标志组合（如 Xmas tree、FIN 和 NULL）的扫描
UDP	检测 UDP 探针，如零字节 UDP 数据包
ICMP	检测 ICMP 回应请求 (ping)
IP	检测 IP 协议扫描。这些扫描与 TCP 和 UDP 扫描不同，因为攻击者不是查找开放端口，而是尝试去发现目标主机支持哪些 IP 协议。

根据目标主机的数量、扫描主机的数量和扫描的端口数量，端口扫描通常分为四种类型。

表 *235:* 端口扫描类型

类型	说明
端口扫描检测	一对一端口扫描，在这种扫描中，攻击者使用一个或几个主机扫描单个目标主机上的多个端口。 一对一端口扫描具有如下特征： • 扫描主机的数量少 • 扫描单个主机 • 扫描的端口数量多 此选项检测 TCP、UDP 和 IP 端口扫描。
端口扫描	一对多端口清扫，在这种扫描中，攻击者使用一个或几个主机扫描多个目标主机上的单个端口。 端口清扫具有如下特征： • 扫描主机的数量少 • 扫描的主机数量多 • 扫描的唯一端口数量少 此选项检测 TCP、UDP、ICMP 和 IP 端口清扫。
诱骗端口扫描	一对一端口扫描，在这种攻击中，攻击者将伪造的源 IP 地址与真实的扫描 IP 地址混合在一起。 诱骗端口扫描具有如下特征： • 扫描主机的数量多 • 一次扫描的端口数量少 • 扫描的主机为一个（或数量少） 诱骗端口扫描选项检测 TCP、UDP 和 IP 协议端口扫描。

类型	说明
分布式端口扫描	多对一端口扫描，在这种攻击中，多个主机查询单个主机是否有开放端口。 分布式端口扫描具有如下特征： • 扫描主机的数量多 • 一次扫描的端口数量多 • 扫描的主机为一个（或数量少） 分布式端口扫描选项检测 TCP、UDP 和 IP 协议端口扫描。

端口扫描检测器所了解的关于探针的信息主要是基于查看探测主机的否定响应。例如，当 Web 客户端尝试连接到 Web 服务器时，客户端会使用端口 80/tcp 且可以依靠服务器将该端口打开。但是，当攻击者探测服务器时，攻击者事先并不知道该服务器是否提供 Web 服务。当端口扫描检测器看到否定响应（即，ICMP 不可达或 TCP RST 数据包）时，它会将该响应记录为潜在的端口扫描。当目标主机位于设备（例如，过滤否定响应的防火墙或路由器）的另一端时，这个过程更难以执行。在这种情况下，端口扫描检测器可以根据选择的灵敏度级别生成已过滤端口扫描事件。

表 236: 灵敏度级别

级别	说明
低	只检测目标主机的否定响应。选择此级别的灵敏度可抑制误报，但请记住，这样可能会遗漏某些类型的端口扫描（慢速扫描、过滤扫描）。 此级别使用最短的时间窗口进行端口扫描检测。
中等	根据主机的连接数量检测端口扫描，这意味着，可以检测过滤的端口扫描。但是，非常活跃的主机（例如网络地址转换器和代理）可能会生成误报。 请注意，可以将这些活跃主机的 IP 地址添加到**忽略已扫描项 (Ignore Scanned)** 字段以减少此类误报。 此级别使用较长的时间窗口进行端口扫描检测。
高	根据时间窗口检测端口扫描，这意味着，可以检测基于时间的端口扫描。但是，如果使用此选项，应通过在 **Ignore Scanned** 和 **Ignore Scanner** 字段中指定 IP 地址，随时间小心地调整检测器。 此级别使用更长的时间周期进行端口扫描检测。

端口扫描事件生成

当启用端口扫描检测时，必须启用生成器 ID (GID) 为 122 且 Snort ID (SID) 为 1 至 27 的规则，以便检测各种端口扫描和端口清扫。

注释 对于端口扫描连接检测器生成的事件，协议号设置为 255。由于默认情况下端口扫描没有特定协议与之关联，因此，互联网编号分配机构 (IANA) 未将协议号分配给它。IANA 指定 255 作为保留号码，因此，该号码用于端口扫描事件中以指明事件没有关联的协议。

表 *237:* 端口扫描检测 ***SID (GID 122)***

端口扫描类型	协议	灵敏度级别	预处理器规则 **SID**
端口扫描检测	TCP UDP ICMP IP	低 中等或高 低 中等或高 低 中等或高 低 中等或高	1 5 17 21 不生成事件。 不生成事件。 9 13
端口扫描	TCP UDP ICMP IP	低 中等或高 低 中等或高 低 中等或高 低 中等或高	3, 27 7 19 23 25 26 11 15
诱骗端口扫描	TCP UDP ICMP IP	低 中等或高 低 中等或高 低 中等或高 低 中等或高	2 6 18 22 不生成事件。 不生成事件。 10 14

端口扫描类型	协议	灵敏度级别	预处理器规则 SID
分布式端口扫描	TCP UDP ICMP IP	低 中等或高 低 中等或高 低 中等或高 低 中等或高	4 8 20 24 不生成事件。 不生成事件。 12 16

端口扫描事件数据包视图

启用随附的预处理器规则后，端口扫描检测器会生成入侵事件，可以像任何其他事件一样进行查看。但是，数据包视图上显示的信息不同于其他类型的入侵事件。

首先使用入侵事件视图钻取到端口扫描事件的数据包视图。请注意，不能下载端口扫描数据包，因为单个端口扫描事件是基于多个数据包；但是，端口扫描数据包视图提供了所有可用的数据包信息。

对于所有 IP 地址，可点击地址查看上下文菜单并选择 **whois** 以在 IP 地址上执行查找，或者选择 **View Host Profile** 以查看该主机的主机配置文件。

表 *238*: 端口扫描数据包视图

信息	说明
设备	检测事件的设备。
时间	事件发生的时间。
消息	预处理器生成的事件消息。
源 IP	扫描主机的 IP 地址。
目标 IP	被扫描主机的 IP 地址。
优先级计数 (Priority Count)	被扫描主机发出的否定响应（例如，TCP RST 和 ICMP 无法访问）的数量。否定响应的数量越多，优先级计数就越高。
连接计数 (Connection Count)	主机上的活动连接数量。此值对于基于连接的扫描（例如 TCP 和 IP）而言更准确。

信息	说明
IP 计数 (IP Count)	与被扫描主机联系的IP地址变化的次数。例如，如果第一个IP地址是10.1.1.1，第二个 IP 是 10.1.1.2，第三 IP 是 10.1.1.1，那么 IP 计数为 3。 此数字对于活跃的主机（例如代理和 DNS 服务器）而言不太准确。
扫描工具/已扫描 IP 范围 (Scanner/Scanned IP Range)	被扫描主机或扫描主机的IP地址范围，具体取决于扫描类型。对于端口清扫，此字段显示被扫描主机的 IP 范围。对于端口扫描，此字段显示扫描主机的 IP 范围。
端口/协议计数 (Port/Proto Count)	对于 TCP 和 UDP 端口扫描，是指正被扫描的端口变化的次数。例如，如果扫描的第一个端口是 80，扫描的第二个端口是 8080，扫描的第三个端口又是 80，那么端口计数为 3。 对于 IP 协议端口扫描，是指正用于连接至被扫描主机的协议变化的次数。
端口/协议范围 (Port/Proto Range)	对于 TCP 和 UDP 端口扫描，是指被扫描端口的范围。 对于 IP 协议端口扫描，是指已用于尝试连接至扫描的主机的 IP 协议号的范围。
开放端口 (Open Ports)	在被扫描主机上打开的 TCP 端口。此字段仅在端口扫描检测到一个或多个开放端口时显示。

配置端口扫描检测

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

端口扫描检测配置选项可用于精细调整端口扫描检测器如何报告扫描活动。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

过程

步骤 1 选择**策略** > **访问控制**，然后点击 **网络分析策略**或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（ ）。

如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击**设置**。

步骤 5 如果**特定威胁检测 (Specific Threat Detection)** 下的**端口扫描检测 (Portscan Detection)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击**端口扫描检测 (Portscan Detection)** 旁边的 **编辑**（  ）。

步骤 7 在**协议 (Protocol)** 字段中，指定要启用的协议。

注释 必须确保已启用 TCP 数据流处理以在 TCP 上检测扫描，并且确保已启用 UDP 流处理以在 UDP 上检测扫描。

步骤 8 在**扫描类型 (Scan Type)** 字段中，指定要检测的的端口扫描类型。

步骤 9 从**灵敏度级别 (Sensitivity Level)** 列表中选择级别；请参阅端口扫描类型、协议和过滤的灵敏度级别，第 2184 页。

步骤 10 如果要监控特定主机的端口扫描活动迹象，请在**监视 IP (Watch IP)** 字段中输入主机 IP 地址。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。将此字段留空则监视所有网络流量。

步骤 11 如果要忽略作为扫描工具的主机，请在**忽略扫描工具 (Ignore Scanners)** 字段中输入主机 IP 地址。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。

步骤 12 如果要忽略作为扫描对象的主机，请在**忽略已扫描项 (Ignore Scanned)** 字段中输入主机 IP 地址。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。

提示 可使用**忽略扫描工具 (Ignore Scanners)** 和**忽略已扫描项 (Ignore Scanned)** 字段指示在网络上特别活跃的主机。可能需要随时间修改此主机列表。

步骤 13 如果要对中途恢复的会话中断监控，请清除**检测 Ack 扫描 (Detect Ack Scans)** 复选框。

注释 检测中途会话有助于识别ACK扫描，但可能会导致错误事件，特别是在含大流量和丢弃数据包的网络中。

步骤 14 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 如果希望端口扫描检测不同的端口检测和端口端口清扫，则请启用规则 122:1 至 122:27。有关详细信息，请参阅入侵规则状态，第 1487 页和端口扫描事件生成，第 2186 页。
- 部署配置更改。

基于速率的攻击防御

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

基于速率的攻击是取决于连接频率或攻击实施重复次数的攻击。可以使用基于速率的检测标准检测发生的基于速率的攻击，采取应对措施，在攻击停止后返回到常规检测设置。

可以将网络分析策略配置为包括基于速率的过滤器，这种过滤器可检测针对网络中主机的过多活动。可以在内联模式下部署的受管设备上使用此功能，以在指定时间内阻止基于速率的攻击，然后恢复为仅生成事件而不丢弃流量。

SYN 攻击防御选项有助于保护网络主机免受 SYN 泛洪攻击。可以根据在一段时间内看到的数据包数量保护单个主机或整个网络。如果设备采用被动部署，可以生成事件。如果设备采用内联部署，还可以丢弃恶意数据包。超时周期结束后，如果速率条件已停止，将会停止事件生成和数据包丢弃。

例如，您可以配置设置来允许来自任一 IP 地址的最大 SYN 数据包数，并阻止来自该 IP 地址的更多连接达 60 秒。

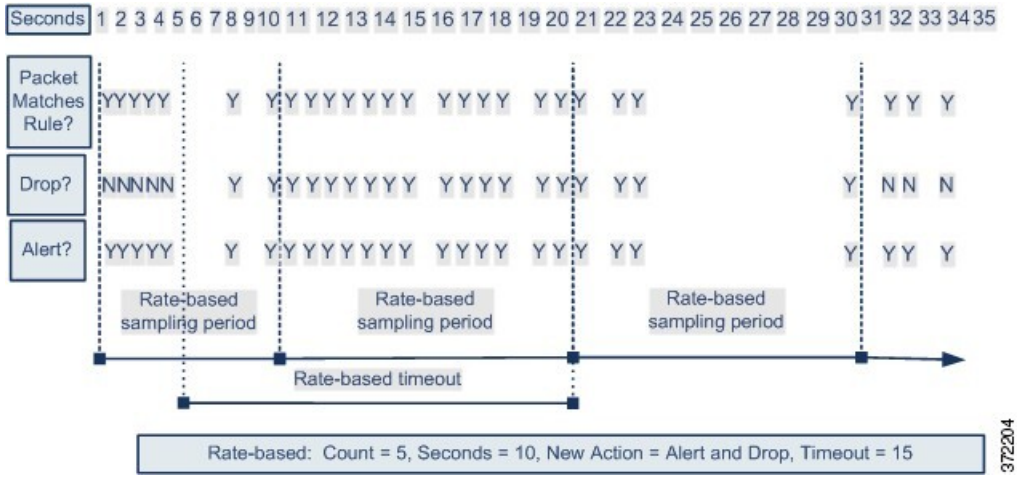
可以限制与网路上主机之间的 TCP/IP 连接，以防止拒绝服务 (DoS) 攻击或用户进行过多活动。当系统检测到与指定 IP 地址成功连接的配置数量或地址范围时，它会对额外连接生成事件。基于速率的事件生成继续进行，直到超时周期结束且未发生速率条件。在内联部署中，可以选择丢弃数据包，直到速率条件超时。

例如，您可以配置设置来允许来自任一 IP 地址的最多 10 个成功同时连接，并阻止来自该 IP 地址的更多连接达 60 秒。

注释 设备将跨内部资源进行负载均衡检查。在配置基于速率的攻击防御时，可以为每个源配置触发率，而不是每个设备。如果基于速率的攻击防御达不到预期，您可能需要降低触发率。如果用户在规定的时间间隔内发送过多的连接尝试，则会触发警报。因此，建议对规则进行速率限制。为了帮助确定正确的速率，请联系支持人员。

下图显示的例子中，攻击者正在尝试访问主机。反复尝试查找密码触发了配置有基于速率的攻击防御的规则。当在 10 秒的时间跨度内发生五次规则匹配之后，基于速率的设置会将规则属性更改为“丢弃并生成事件”(Drop and Generate Events)。新的规则属性在 15 秒之后超时。

请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。如果采样速率高于当前或前一个采样周期的阈值，新操作将继续。在采样速率地区阈值速率的情况下，新操作将恢复为仅在采样期完成后生成事件。



相关主题

动态入侵规则状态，第 1494 页

基于速率的攻击防御示例

关键字 `detection_filter`、阈值和抑制功能提供了其他方式来过滤流量或系统生成的事件。可以单独使用基于速率的攻击防御，也可以将其与阈值、抑制功能或 `detection_filter` 关键字随意组合使用。

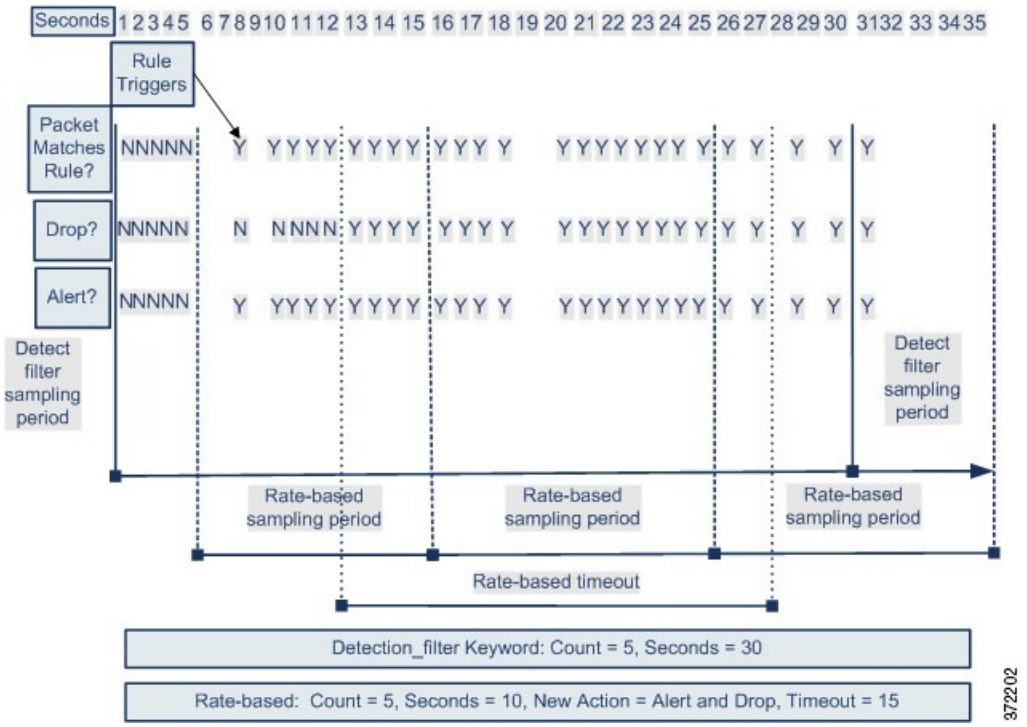
`detection_filter` 关键字、阈值或抑制以及基于速率的条件可能全都适用于同一流量。为规则启用抑制功能后，系统会为指定 IP 地址抑制事件，即使发生基于速率的变化。

detection_filter 关键字示例

下面的示例显示了一个攻击者尝试发动暴力登录攻击。重复尝试查找密码会触发还包含 `detection_filter` 关键字且计数设置为 5 的规则。此规则已配置基于速率的攻击防御。如果在 10 秒内出现五次规则匹配，基于速率的设置会将规则属性更改为“丢弃并生成事件”(Drop and Generate Events) 并保持 20 秒。

如图所示，与规则匹配的前五个数据包不会生成事件，因为在速率超过 `detection_filter` 关键字所指示的速率之前规则不会触发。规则触发后，事件通知开始，但基于速率的标准在再通过五个数据包之前不会触发新操作“丢弃并生成事件”(Drop and Generate Events)。

如果符合基于速率的标准，将会生成事件并会丢弃数据包，直到基于速率的超时周期结束且速率低于阈值。20 秒之后，基于速率的操作超时。请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。由于采样的速率高于之前采样周期的阈值速率，因此发生超时时，基于速率的操作会继续。



请注意，虽然示例未进行描述，但可以将“丢弃并生成事件”(Drop and Generate Events) 规则状态与 `detection_filter` 关键字结合使用，以在规则的匹配速率达到指定速率时开始丢弃流量。确定是否为规则配置基于速率的设置时，请考虑将规则设置为“丢弃并生成事件”(Drop and Generate Events) 和包含 `detection_filter` 关键字是否会获得相同的结果，或者是否要在入侵策略中管理速率和超时设置。

相关主题

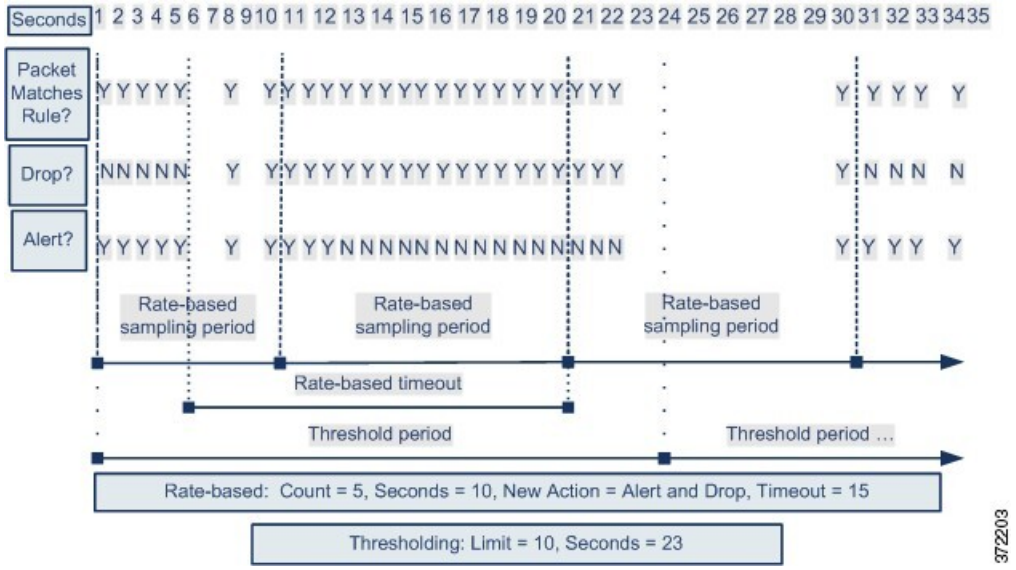
入侵规则状态，第 1487 页

动态规则状态阈值或抑制示例

下面的示例显示了一个攻击者尝试发动暴力登录攻击。反复尝试查找密码将触发一条已经配置了基于速率的攻击预防的规则。如果在10秒内出现五次规则攻击，基于速率的设置会将规则属性更改为“丢弃并生成事件”(Drop and Generate Events) 并保持 15 秒。此外，一个限制阈值还会将该规则可生成的事件数限制为 23 秒内 10 个事件。

如图所示，该规则将为前五个匹配数据包生成事件。五个数据包之后，基于速率的标准会触发新操作“丢弃并生成事件”(Drop and Generate Events)，对于接下来的五个数据包，规则会生成事件且系统会丢弃数据包。第十个数据包之后，已达到极限阈值，因此，对于剩余的数据包，系统不会生成事件，但会丢弃数据包。

请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。如果采样速率高于当前或前一采样期的阈值速率，则新操作将继续。在采样速率地区阈值速率的情况下，新操作将恢复为仅在采样期完成后生成事件。



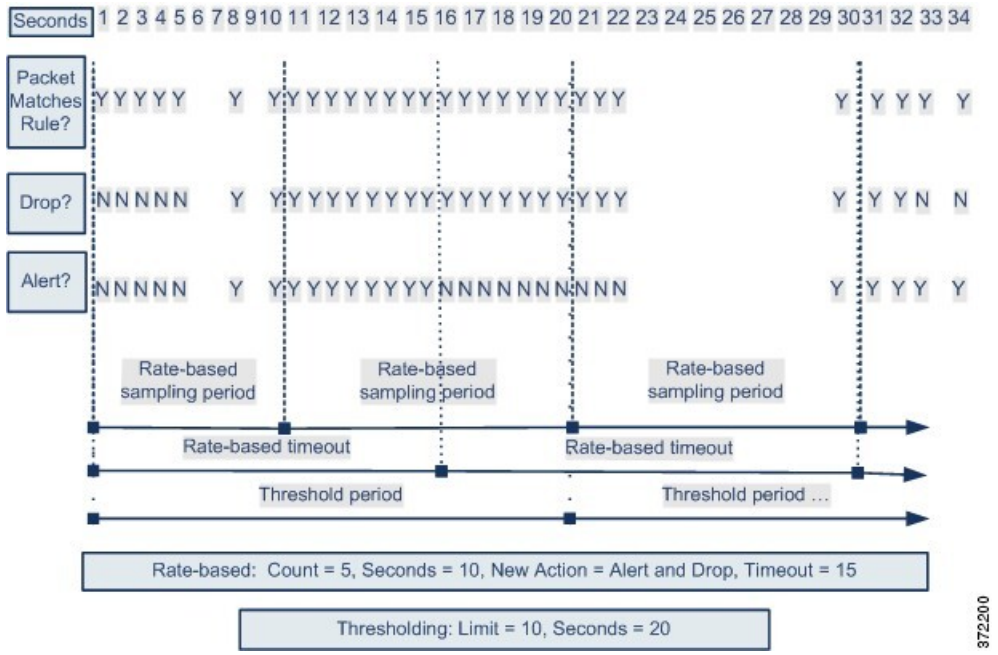
请注意，虽然本例中未显示，但如果在达到阈值后因基于速率的标准而触发新操作，系统会生成一个事件以指示操作变化。因此，例如，对于第 14 个数据包，如果达到极限阈值 10，系统停止生成事件且操作从从“生成事件”(Generate Events) 更改为“丢弃并生成事件”(Drop and Generate Events)，系统会生成第十一个事件以指示操作变化。

整个策略基于速率的检测和阈值或抑制示例

以下示例显示了尝试对网络中的主机进行拒绝服务 (DoS) 攻击的攻击者。许多来自相同源的同步主机连接会触发整个策略的“控制同步连接”设置。如果在10秒内一个源有五个连接，设置会生成事件并丢弃恶意流量。此外，全局极限阈值会在 20 秒内将所有规则或设置可生成的事件数量限制为 10。

如图所示，整个策略的设置会为前十个匹配数据包生成事件并丢弃流量。第十个数据包之后，已达到极限阈值，因此，对于剩余的数据包，不会生成事件，但会丢弃数据包。

请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。如果采样的速率高于当前或之前采样周期的阈值速率，生成事件和丢弃流量这两种基于速率的操作将会继续。基于速率的操作只在采样周期结束后停止，在此情况下采样的速率低于阈值速率。



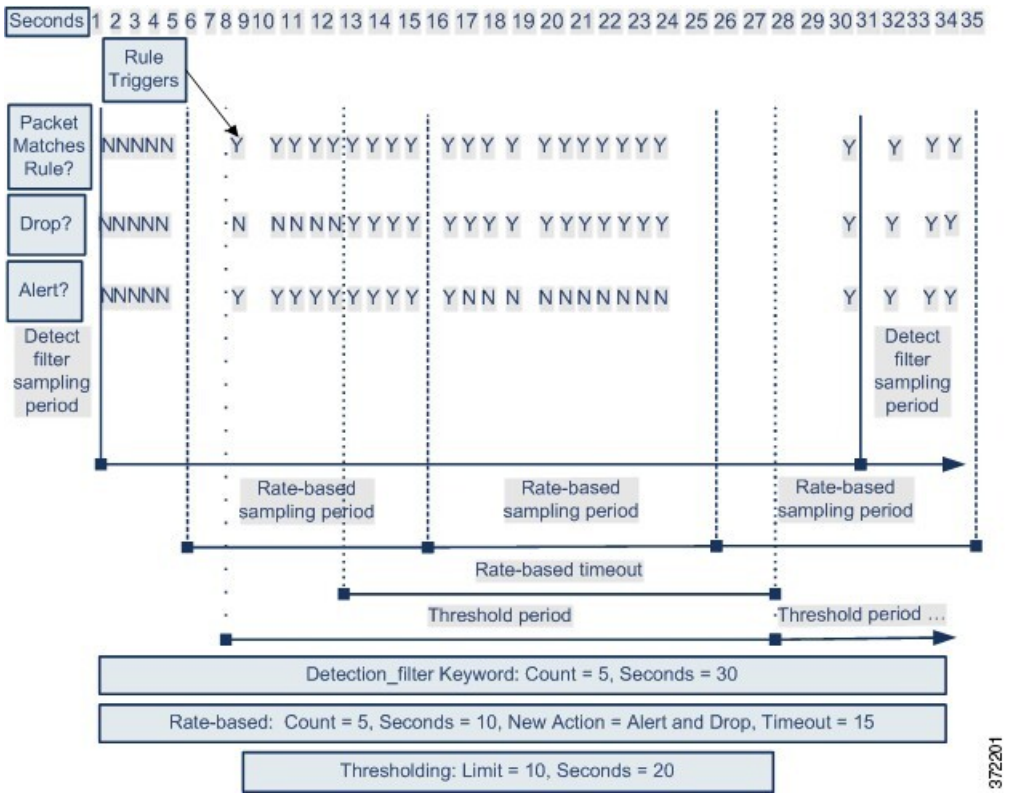
请注意，虽然本例中未显示，但如果在达到阈值后因基于速率的标准而触发新操作，系统会生成一个事件以指示操作变化。因此，例如，对于第 14 个数据包，如果达到极限阈值 10，系统停止生成事件且操作更改为 Drop and Generate Events，系统会生成第十一个事件以指示操作变化。

使用多种过滤方法进行基于速率的检测示例

以下示例显示了尝试强行登录的攻击者，并描述了 `detection_filter` 关键字、基于速率的过滤和阈值功能交互的情况。重复尝试查找密码会触发包括 `detection_filter` 关键字且计数设置为 5 的规则。此规则还具有基于速率的攻击防御设置，如果在 15 秒内出现五次规则匹配，该设置会将规则属性更改为“丢弃并生成事件”(Drop and Generate Events) 并保持 30 秒。此外，极限阈值会在 30 秒内将规则限为 10 个事件。

如图所示，与规则匹配的前五个数据包不会产生事件通知，因为在速率超过 `detection_filter` 关键字所指示的速率之前规则不会触发。规则触发后，事件通知开始，但基于速率的标准在再通过五个数据包之前不会触发新操作“丢弃并生成事件”(Drop and Generate Events)。如果符合基于速率的标准，系统会为数据包 11 至 15 生成事件并丢弃数据包。第十五个数据包之后，已达到极限阈值，因此，对于剩余的数据包，系统不会生成事件，但会丢弃数据包。

请注意，基于速率的超时后，数据包仍会在随后的基于速率的采样周期内丢弃。由于采样的速率高于之前采样周期的阈值速率，新操作将会继续。



基于速率的攻击防御选项和配置

基于速率的攻击防御可确定异常流量模式，并可将这些流量对合法请求的影响降至最低。基于速率的攻击通常具有以下其中一种特征：

- 任何包含与网络主机之间过多不完整连接的流量，表示 SYN 泛洪攻击
- 任何包含与网络主机之间过多完整连接的流量，表示 TCP/IP 连接泛洪攻击
- 在流向特定目标 IP 地址或来自一个或多个特定源 IP 地址的流量中规则匹配过多
- 所有流量中某个特定规则的匹配过多

在网络分析策略中，您可以为整个策略配置 SYN 泛洪或 TCP/IP 连接泛洪检测；在入侵策略中，您可以为单独的入侵或预处理器规则设置基于速率的过滤器。请注意，不能手动将基于速率的过滤器添加到 GID 135 规则或修改其规则状态。GID 为 135 的规则使用客户端作为源值，使用服务器作为目标值。

在启用 **SYN 攻击防御 (SYN Attack Prevention)** 后，如果超过定义的速率条件，则会触发规则 135:1。

在启用**控制同时连接 (Control Simultaneous Connections)** 后，如果超过定义的速率条件，则触发规则 135:2，如果会话关闭或超时，则触发规则 135:3。

注释 设备将跨内部资源进行负载均衡检查。在配置基于速率的攻击防御时，可以为每个源配置触发率，而不是每个设备。如果基于速率的攻击防御达不到预期，您可能需要降低触发率。如果用户在规定的时间间隔内发送过多的连接尝试，则会触发警报。因此，建议对规则进行速率限制。为了帮助确定正确的速率，请联系支持人员。

每个基于速率的过滤器都包含下列几个组成部分：

- 网络地址名称（适用于整个策略或基于规则的源或目标设置）
- 规则的匹配速率，配置为特定秒数内的规则匹配项数量
- 超过该速率时要执行的新操作

  为整个策略设置基于速率的设置时，系统会在其检测到基于速率的攻击时生成事件，并且可以在内联部署中丢弃流量。为具体规则设置基于速率的操作时，有三个可用的操作：Generate Events、Drop and Generate Event 和 Disable。
- 操作的持续时间，配置为超时值

请注意，新操作自开始之后，在到达超时时间之前会一直执行，即使速率在这段时间内降到配置的速率以下亦不会停止。当超时时段结束后，如果速率低于阈值，则规则的操作会恢复到最初为该规则配置的操作。对于整个策略的设置，操作会恢复到流量匹配的每个规则的操作；如果不匹配任何规则，操作会停止。

在内联部署中，可以配置基于速率的攻击防御来临时或永久拦截攻击。在没有基于速率的配置的情况下，设置为“生成事件”(Generate Events) 的规则会创建事件，但系统不会丢弃这些规则的数据包。但是，如果攻击流量所匹配的规则配置了基于速率的条件，则基于速率的操作可能会导致系统在该操作处于活动状态的时间内丢弃数据包，即便这些规则最初并未设置为“丢弃并生成事件”(Drop and Generate Events)。

注释 基于速率的操作无法启用禁用的规则，也无法丢弃与禁用的规则匹配的流量。但是，如果在策略级别设置基于速率的过滤器，则可以在指定时段内生成事件或生成事件并丢弃包含过多SYN数据包或SYN/ACK 交互的流量。

可以对同一规则定义多个基于速率的过滤器。入侵策略中列出的第一个过滤器优先级最高。请注意，当两个基于速率的过滤器操作相冲突时，系统会实施第一个基于速率的过滤器的操作。同样，如果对整个策略设置的基于速率的过滤器与对具体规则设置的基于速率的过滤器相冲突，前者优先。

相关主题

从规则页面设置动态规则状态，第 1496 页

基于速率的攻击防御、检测过滤和阈值或抑制

关键字 `detection_filter` 可防止触发规则，直至在指定时间内出现规则匹配项的阈值数量为止。当规则包括关键字 `detection_filter` 时，系统将跟踪每个超时期间传入的匹配规则中模式的数据包数

量。系统可统计来自特定源 IP 地址或特定目标 IP 地址的规则匹配项的数量。在速率超出规则中的速率后，系统将开始发送该规则的事件通知。

可以使用阈值和抑制来减少过多的事件，方法是限制规则、源或目标的事件通知数量或者抑制该规则的所有通知。您还可以配置适用于没有首要特定阈值的每个规则的全局规则阈值。

如果对规则应用抑制，则系统会为所有适用的 IP 地址抑制该规则的事件通知，即使由于策略范围或规则特定的基于速率的设置而发生基于速率的操作更改也如此。

相关主题

入侵事件阈值，第 1489 页
入侵策略抑制配置，第 1492 页
全局规则阈值基础知识，第 1639 页

配置基于速率的攻击防御

注释 此部分适用于 Snort 2 预处理器。有关 Snort 3 检查器的信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

可以在策略级别配置基于速率的攻击防御以阻止SYN泛洪攻击，也可以阻止来自特定源或到达特定目标的过多连接。

过程

步骤 1 选择**策略 > 访问控制**，然后点击 **网络分析策略**或**策略 > 访问控制 > 入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 点击您要编辑的策略旁边的**编辑**（）。

如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击**设置**。

步骤 5 如果**特定威胁检测 (Specific Threat Detection)** 下的**基于速率的攻击防御 (Rate-Based Attack Prevention)** 已禁用，请点击**已启用 (Enabled)**。

步骤 6 点击**基于速率的攻击防御 (Rate-Based Attack Prevention)** 旁边的 **编辑**（）。

步骤 7 您有两种选择：

- 要防止旨在对主机发起泛洪攻击的不完整连接，请点击 **SYN Attack Prevention** 下的 **Add**。
- 要防止过多连接，请点击 **Control Simultaneous Connections** 下的 **Add**。

步骤 8 指定要跟踪流量的方式：

- 要跟踪来自特定源或一系列源的所有流量，请从**跟踪方式(Track By)**下拉列表中选择**源 (Source)**，然后在**网络 (Network)** 字段中输入单个 IP 地址或地址块。
- 要跟踪到达特定目标或一系列目标的所有流量，请从**跟踪方式 (Track By)** 下拉列表中选择**目标 (Destination)**，然后在**网络 (Network)** 字段中输入单个 IP 地址或地址块。

注释

- 请勿在网络字段中输入 IP 地址 0.0.0.0/0 来监控所有子网或 IP。系统不支持使用此 IP 地址（通常用于识别所有子网或 IP）进行基于速率的攻击预防。
- 系统会单独跟踪**网络 (Network)** 字段中包含的每个 IP 地址的流量。来自超过所配置速率的 IP 地址的流量会带来仅为该 IP 地址生成的事件。例如，进行网络设置时，可将源 CIDR 块设置为 `10.1.0.0/16` 并将系统配置为在有十个同步连接打开时生成事件。如果 10.1.4.21 有八个连接打开，10.1.5.10 有六个连接打开，则系统不会生成事件，因为这两个源地址的打开连接均未达到触发数量。但是，如果 10.1.4.21 有十一个同步连接打开，系统只会为来自 10.1.4.21 的连接生成事件。

  系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

步骤 9 指定速率跟踪设置的触发速率：

- 对于 SYN 攻击配置，在**速率 (Rate)** 字段中输入每个秒数的 SYN 数据包数量。
- 对于同步连接配置，在**计数 (Count)** 字段中输入连接数量。

设备将跨内部资源进行负载均衡检查。在配置基于速率的攻击防御时，可以为每个源配置触发率，而不是每个设备。如果基于速率的攻击防御达不到预期，您可能需要降低触发率。如果用户在规定的时间间隔内发送过多的连接尝试，则会触发警报。因此，建议对规则进行速率限制。为了帮助确定正确的速率，请联系支持人员。

步骤 10 要丢弃与基于速率的攻击防御设置匹配的数据包，请选中**丢弃 (Drop)** 复选框。

步骤 11 在**超时 (Timeout)** 字段中输入时间段，在该时间段结束后将会停止生成针对具有 SYN 的匹配模式或同步连接的流量的事件（如适用，丢弃）。

注意 设置较高的超时值可能会完全阻止连接到内联部署中的某个主机。

步骤 12 点击 **OK**。

步骤 13 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

第 92 章

自适应配置文件

以下主题介绍如何配置自适应配置文件：

关于自适应配置文件

必须启用自适应配置文件才能：

- 执行应用和文件控制，包括恶意软件防护 (AMP)，同时允许入侵规则使用服务元数据。

注意 如配置自适应配置文件，第2204页中所述，为了让访问控制规则执行应用和文件控制（包括恶意软件保护 AMP）并让入侵规则使用服务元数据，**必须**启用（默认状态）自适应分析。

- 在被动部署中，通过启用自适应配置文件更新可根据目标主机上的操作系统对 IP 流量进行重整和重组。

注释 在内联部署中，思科建议您不启用自适应配置文件更新，而是配置已启用**规范化 TCP 负载 (Normalize TCP Payload)** 选项的内联规范化预处理器。

自适应配置文件的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

自适应配置文件的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

自适应配置文件更新

通常，系统使用网络分析策略中的静态设置预处理和分析流量。通过自适应配置文件，系统可以使用由网络发现检测或从第三方导入的主机信息适应处理行为。

配置文件更新（就像可在网络分析策略中手动配置的基于目标的配置文件一样）有助于以与目标主机上操作系统相同的方式对 IP 数据包进行分片重组并重组数据流。然后入侵规则引擎使用与目标主机所用的相同格式分析数据。

手动配置的基于目标的配置文件应用您选择的默认操作系统配置文件，或绑定到特定主机的配置文件。但是，配置文件更新会根据目标主机的主机配置文件中的操作系统切换到相应的操作系统配置文件。

假设您为 10.6.0.0/16 子网配置配置文件更新，并将默认 IP 分片重组基于目标的策略设置为 Linux。配置设置的管理中心中有一个包括 10.6.0.0/16 子网的网络映射。

- 当系统检测到来自主机 A（不在 10.6.0.0/16 子网中）的流量时，它使用基于 Linux 目标的策略重组 IP 分片。
- 当系统检测到来自主机 B（在 10.6.0.0/16 子网中）的流量时，它从网络映射检索主机 B 的操作系统数据。系统使用基于该操作系统的配置文件对传送到主机 B 的流量进行分片重组。

自适应配置文件更新和思科 建议规则

自适应配置文件功能是访问控制策略中的高级设置，它全局应用于由该访问控制策略调用的所有入侵策略。思科 建议的规则功能适用于您在其中配置该功能的各个入侵策略。

与 思科 建议的规则一样，配置文件更新 会将规则中的元数据与主机信息进行比较，确定是否应为某个特定主机应用规则。然而，虽然思科 建议的规则为使用该信息的启用或禁用规则提供建议，但配置文件更新 仍会使用这些信息将特定规则应用于特定流量。

思科Firepower建议的规则需要您的互动才能对规则状态执行建议的更改。另一方面，配置文件更新不会修改入侵规则。基于配置文件更新的规则处理在逐包基础上进行。

此外，思科建议的规则可导致启用禁用的规则。相反，配置文件更新仅影响已在入侵策略中启用的规则的应用。配置文件更新 永远不会更改规则状态。

您可以组合使用配置文件更新和思科建议的规则。当部署入侵策略来确定是否纳入某条规则作为应用备选项时，配置文件更新 会使用该规则的规则状态，您是选择接受还是拒绝建议均反映在该规则状态中。您可以同时使用这两个功能来确保您已启用或禁用每个监测网络中最合适的规则，然后应用对特定流量最为有效的已启用规则。

相关主题

关于思科 建议的规则，第 1621 页

自适应配置文件选项

启用

以下情况需要启用此选项：

- 访问控制规则，以执行应用和文件控制（包括 AMP）
- 入侵规则，以使用服务元数据

默认情况下，此选项已启用。

注释 要在 Snort 3 中启用自适应配置文件，必须同时选择**启用 (Enable)** 和**启用配置文件更新 (Enable Profile Updates)** 选项。

启用配置文件更新

在被动部署中，通过启用配置文件更新可在网络映射中根据主机使用的操作系统的配置文件对 IP 流量进行重整和重组。

对于 Snort 3，如果启用了自适应配置文件，则必须启用此功能。

自适应配置文件 - 属性更新间隔

在启用配置文件更新后，您可以控制网络映射数据从 管理中心同步到其受管设备的频率（以分钟为单位）。系统使用该数据确定处理流量时应使用哪些配置文件。增大此选项的值可提升大型网络的性能。

自适应配置文件 - 网络

或者，启用配置文件更新后，您可以通过将配置文件更新限制在逗号分隔的 IP 地址、地址块和网络变量列表中来提高性能。如果使用网络变量，则系统会为您的访问控制策略使用与默认入侵策略相关联的变量集中的变量值。例如，可以输入：**`192.168.1.101, 192.168.4.0/24, $HOME_NET`**。支持 IPv4 和 IPv6。

默认值 (**`0.0.0.0/0`**) 将自适应配置文件更新应用于所有网络。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。如果启用并执行祖先策略中的配置文件更新，则思科建议您保留默认网络限制 **`0.0.0.0/0`**，或使用网络变量值`any`。此设置将配置文件更新应用于所有子域中的所有受监控主机。

相关主题

在识别流量之前检查通过的数据包，第 2042 页
变量集，第 1042 页

配置自适应配置文件

在被动部署中，思科建议您配置自适应配置文件。在内联部署中，请配置启用**规范化 TCP 负载 (Normalize TCP Payload)** 选项的内联规范化预处理器。

注意 如本程序中所述，为了让访问控制规则执行应用或文件控制（包括 AMP）并让入侵规则使用服务元数据，**必须**启用（默认状态）自适应分析。

开始之前

访问控制策略必须具有启用主机/服务发现的网络发现策略，或者必须从第三方源导入主机数据。

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)**，然后点击“检测增强设置”(Detection Enhancement Settings) 部分旁的 **编辑**（ ）。

如果显示**视图**（ ），则表明设置继承自祖先策略，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 2 如自适应配置文件选项，第 2203 页中所述，设置自适应配置文件。

步骤 3 点击**确定 (OK)**。

步骤 4 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改。

相关主题

内联规范化预处理器，第 2153 页
Snort® 重新启动场景，第 143 页

第 XXI 部分

参考

思科防御协调器平台维护计划

思科防御协调器维护计划

CDO 会每周更新其平台，提供新功能和质量改进。根据此计划，更新可在 3 小时内完成。

大多数情况下，更新会在星期四完成，但如有必要，也可以安排在星期五和星期日进行维护。

表 *239: CDO* 维护时间表

星期	时间 （24 小时制）
星期四	09:00 UTC - 12:00 UTC
星期五	09:00 UTC - 12:00 UTC
星期日	09:00 UTC - 12:00 UTC

在此维护期间，您仍然可以访问您的租户，并且如果您有 云交付的防火墙管理中心，也可以访问该平台。此外，您已载入CDO的设备将继续执行其安全策略。

注释 我们建议您在维护期间不要使用 CDO 来在其管理的设备上部署配置更改。

如果发生阻止 CDO 或 云交付的防火墙管理中心 进行通信的故障，则会尽快在所有受影响的租户上解决该故障，即使并非是在维护时间窗口之内。

云交付的防火墙管理中心维护时间表

在CDO更新云交付的防火墙管理中心环境前大约1周通知在租户上部署了云交付的防火墙管理中心的客户。通过邮件通知租户的超级管理员和管理员用户。CDO还会在其主页上显示一个横幅，通知所有用户即将发布的更新。

在分配给租户区域的维护日的 3 小时维护期内，对租户进行更新最多可能需要 1 小时。在更新租户时，您将无法访问云交付的防火墙管理中心环境，但仍可访问 CDO 的其余部分。

表 *240:* 云交付的防火墙管理中心维护时间表

星期	时间 （**24** 小时制）	地区
星期三	04:00 UTC - 07:00 UTC	欧洲、中东或非洲 (EMEA)
星期三	17:00 UTC - 20:00 UTC	亚太、日本、中国 (APJC)
星期四	09:00 UTC - 12:00 UTC	美国 (US)

使用 CLI 完成 Secure Firewall Threat Defense 设备初始配置

连接到设备的 CLI 以执行初始设置，包括使用安装向导设置管理 IP 地址、网关和其他基本网络设置。确保所有 DNS 和防火墙端口均可访问以进行通信。

专用管理接口是一种具有自己的网络设置的特殊接口。如果您不想使用管理接口，可以使用 CLI 配置数据接口。

Before you begin

此程序适用于以下场景：

- Firepower 1000、 Firepower 2100、 Secure Firewall 3100和 ISA 3000 型号。
- 此配置非常适合使用 CLI 注册密钥自行激活的设备。

Note 请 **勿** 对使用低接触调配进行自行激活的设备使用此配置程序。

Procedure

步骤 1 连接到设备的 CLI，无论从控制台端口还是使用 SSH 至管理接口。如果您打算更改网络设置，我们建议使用控制台端口，以免断开连接。

对于 Firepower 1000、 Firepower 2100、 Secure Firewall 3100 模型：控制台端口连接到 FXOS CLI。SSH 会话直接连接到 威胁防御 CLI。

步骤 2 使用用户名 **admin** 和密码 **Admin123** 登录。

(Firepower 1000/2100, Secure Firewall 3100) 在控制台端口，连接到 FXOS CLI。第一次登录 FXOS 时，系统会提示您更改密码。此密码也用于 SSH 的威胁防御登录。

Note 如果密码已更改，但您不知道，则必须重新映像设备以将密码重置为默认值。有关 重新映像程序的信息，请参阅 《FXOS 故障排除指南》 。有关说明，请参阅 《重新映像指南》 。

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

步骤 3 (Firepower 1000/2100, Secure Firewall 3100) 如果您在控制台端口连接到 FXOS，则连接到 威胁防御 CLI。

connect ftd

Example:

```
firepower# connect ftd
>
```

步骤 4 第一次登录设备时，系统会提示您接受《最终用户许可协议》(EULA)和，如果使用 SSH 连接， 则会提示您更改管理员密码。然后，系统将显示 CLI 设置脚本。

Note 除非清除配置，否则无法重复 CLI 安装向导（例如，通过重新建立映像）。但是，可以稍后在 CLI 中使用 **configure network** 命令更改所有这些设置。请参阅 威胁防御命令参考。

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

Note 即使您在数据接口上启用 威胁防御 访问，也使用管理接口设置。例如，通过数据接口在背板上路由的管理流量将使用管理接口 DNS 服务器解析 FQDN，而非使用数据接口 DNS 服务器。

请参阅以下准则：

- **通过 DHCP 或手动配置 IPv4**？-如果想要使用数据接口而非管理接口进行 威胁防御 访问，请选择 **手动**。虽然您不打算使用管理接口，但必须设置 IP 地址，例如专用地址。如果管理接口设置为 DHCP，则无法配置数据接口用于管理，因为默认路由（必须是 **data-interfaces**，请参阅下一个要点）可能会被接收自 DHCP 服务器的路由覆盖。
- **输入管理接口的 IPv4 默认网关**-如果想要使用数据接口而非管理接口进行 威胁防御 访问，请将网关设置为 **data-interfaces**。此设置将在背板上转发管理流量，因此可路由通过 FMC 访问数据接口。
- **如果您的网络信息已更改，需要重新连接** - 如果您已建立 SSH 连接，但在初始设置时更改了 IP 地址，连接将断开。使用新 IP 地址和密码重新进行连接。控制台连接不会受影响。
- **在本地管理设备**？-输入 **是** 以配置由 云交付的防火墙管理中心 或 Secure Firewall 设备管理器管理的设备。

  在本地管理设备？-输入 **否** 以配置设备进行 本地管理中心管理。
- **配置防火墙模式**？- 建议您在初始配置时设置防火墙模式。在初始设置后更改防火墙模式将会清除正在运行的配置。请注意，只有路由防火墙模式支持数据接口 威胁防御 访问。

步骤 5 (Optional) 配置用于 管理中心 访问的数据接口。

configure network management-data-interface

然后，系统会提示您为数据接口配置基本网络设置。

Note 使用此命令时，应使用控制台端口。如果使用 SSH 访问管理接口，连接可能会断开，您必须重新连接到控制台端口。有关 SSH 用法的详细信息，请参阅下文。

请参阅以下有关使用此命令的详细信息。有关详细信息，请参阅 关于数据接口, on page 21 。

- 如果您要使用数据接口进行管理，则原始管理接口无法使用 DHCP。如果在初始设置期间没有手动设置 IP 地址，则可以使用 **configure network** {**ipv4** | **ipv6**} **manual** 命令立即设置它。如果您尚未将管理接口网关设置为 **data-interfaces**，此命令将立即设置它。
- 当您通过 CDO 为 FTD 管理载入设备时，CDO 会发现并维护接口配置，包括以下设置：接口名称和 IP 地址、网关静态路由、DNS 服务器和 DDNS 服务器。有关 DNS 服务器配置的详细信息，请参阅下文。您可以稍后对访问接口配置进行更改，但要确保更改不会阻止设备或CDO重新建立管理连接。如果管理连接中断，设备将包含 **configure policy rollback** 命令以恢复以前的部署。

- 此命令设置数据接口 DNS 服务器。使用设置脚本（或使用 **configure network dns servers** 命令）设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。

  此外，仅当在初始注册时发现 DNS 服务器， 才会保留本地 DNS 服务器。例如，如果您使用管理接口注册了设备，但随后使用 **configure network management-data-interface** 命令配置数据接口，则必须在 CDO中手动配置所有这些设置（包括 DNS 服务器），以便与设备配置匹配。

- 在通过 CDO 为 FTD 管理载入 威胁防御 后，您可以将该管理接口更改为管理接口或另一数据接口。
- 您在安装向导中设置的 FQDN 将用于此接口。
- 您可以通过命令清除整个设备配置；在恢复场景中可使用此选项，但我们不建议您在初始设置或正常操作中使用它。
- 要禁用数据管理，请输入 **configure network management-data-interface disable** 命令。

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

步骤 6 (Optional) 限制在特定网络上通过数据接口访问 CDO 。

configure network management-data-interface client *ip_address netmask*

默认情况下，允许所有网络。

第 93 章

Cisco Secure Firewall Management Center 命令行参考

本参考介绍 Cisco Secure Firewall Management Center的命令行界面 (CLI)。

注释 有关 Cisco Secure Firewall Threat Defense，请参阅Cisco Secure Firewall Threat Defense 命令参考。

关于 Cisco Secure Firewall Management Center CLI

使用 SSH 登录 管理中心时，可以访问 CLI。虽然我们强烈建议不要这样做，但您可以使用 专家 命令访问 Linux 外壳。

注意 强烈建议您不要访问 Linux 外壳，除非 Cisco TAC 或 Firepower 用户文档明确说明需要这样做。

注意 具有 Linux 外壳访问权限的用户可以获得 root 权限，这将带来安全风险。出于系统安全原因，我们强烈建议：

- 如果您建立外部身份验证，请确保相应地限制具有 Linux 外壳访问权限的用户列表。
- 除了预定义 管理员 用户外，不要建立 Linux 外壳用户。

您 可以使用本附录中所述的命令查看 、对 Cisco Secure Firewall Management Center进行故障排除，以及执行有限的配置操作。

Cisco Secure Firewall Management Center CLI 模式

CLI 包含四种模式。默认模式“CLI 管理”包括用于在 CLI 本身内导航的命令。其余模式包含处理三个不同方面的 Cisco Secure Firewall Management Center功能的命令；这些模式中的命令以模式名称开头：`system`、`show` 或 `configure`。

进入某个模式时，CLI提示符会发生更改以反映当前模式。例如，要显示有关系统组件的版本信息，可在标准 CLI 提示符下输入完整命令：

```
> show version
```

如果您之前进入了 `show` 模式，则可以在显示模式 CLI 提示符下输入不含 `show` 关键字的命令：

```
show> version
```

Cisco Secure Firewall Management Center CLI 管理命令

CLI 管理命令可用于与 CLI 进行交互。这些命令不影响设备的运行。

exit

将 CLI 上下文上移至下一个最高级别的 CLI 上下文。从默认模式发出此命令会使用户注销当前 CLI 会话。

语法

```
exit
```

示例

```
system> exit
>
```

expert

调用 Linux 外壳。

语法

```
expert
```

示例

```
> expert
```

?（问号）

为 CLI 命令和参数显示上下文相关帮助。按照以下说明使用问号 (?) 命令：

- 要为当前 CLI 上下文中可用的命令显示帮助，请在命令提示符处输入问号 (?)。
- 要显示以特定字符集开头的可用命令的列表，请输入缩写命令，再紧接着输入问号 (?)。
- 要为命令的合法参数显示帮助，请在命令提示符处输入问号 (?) 代替参数。

请注意，问号 (?) 不会回送到控制台。

语法

```
?
abbreviated_command ?
command [arguments] ?
```

示例

```
> ?
```

Cisco Secure Firewall Management Center CLI Show 命令

Show 命令提供有关设备状态的信息。这些命令不会更改设备的运行模式，并且运行它们对系统运行的影响极小。

version

显示产品的版本和内部版本。

语法

```
show version
```

示例

```
> show version
```

Cisco Secure Firewall Management Center CLI 配置命令

配置命令可供用户配置和管理系统。这些命令会影响系统的运行。

password

允许当前 CLI 用户更改其密码。

注意 出于系统安全原因，我们强烈建议：除了任何设备上的预定义 **管理** 外，不要建立 Linux 外壳用户。

注释 导出模式不支持 密码 命令。要在安全防火墙系统上重置管理员用户的密码，请参阅 了解更多信息。如果您在专家模式下使用 密码 命令重置管理员密码，我们建议您使用 配置用户管理员密码 命令重新配置密码。重新配置密码后，切换到专家模式，并确保 /opt/cisco/config/db/sam.config 和 /etc/shadow 文件中的 admin 用户的密码散列相同。

发出命令后，CLI 会提示用户其当前（或旧）密码，然后提示用户输入新密码两次。

语法

```
configure password
```

示例

```
> configure password
Changing password for admin.
(current) UNIX password:
New UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Cisco Secure Firewall Management Center CLI 系统命令

系统命令可供用户管理整个系统的文件以及访问控制设置。

generate-troubleshoot

生成供思科进行分析的故障排除数据。

语法

```
system generate-troubleshoot option1 optionN
```

其中，选项是用空格分隔的以下一项或多项：

- ALL：运行以下所有选项。
- SNT：Snort 性能和配置
- PER：硬件性能和日志
- SYS：系统配置、策略和日志
- DES：检测配置、策略和日志
- NET：接口和网络相关数据
- VDB：发现、感知、VDB 数据和日志
- UPG：升级数据和日志
- DBO：所有数据库数据
- LOG：所有日志数据
- NMP：网络映射信息

示例

```
> system generate-troubleshoot VDB NMP
starting /usr/local/sf/bin/sf_troubleshoot.pl…
Please, be patient. This may take several minutes.
The troubleshoot options codes specified are VDB,NMP.
Getting filenames from [usr/local/sf/etc/db_updates/index]
Getting filenames from [usr/local/sf/etc/db_updates/base-6.2.3]
Troubleshooting information successfully created at
/var/common/results-06-14-2018—222027.tar.gz
```

lockdown

移除 专家 命令并访问设备上的 bash shell。

⚠

注意 没有支持部门提供的修复程序，此命令将无法撤销。请谨慎使用。

语法

```
system lockdown
```

示例

```
> system lockdown
```

reboot

重新启动设备。

语法

```
system reboot
```

示例

```
> system reboot
```

restart

重新启动设备应用。

语法

```
system restart
```

示例

```
> system restart
```

shutdown

关闭设备。

语法

```
system shutdown
```

示例

```
> system shutdown
```

第 94 章

安全、互联网接入和通信端口

以下主题提供有关系统安全、互联网接入和通信端口的信息：

安全要求

为了保护Cisco Secure Firewall Management Center，应将其安装在受保护的内部网络中。虽然 管理中心已配置为仅拥有必需的服务和可用端口，但必须确保无法从防火墙外部攻击它（或任何受管设备）。

如果管理中心及其受管设备位于同一个网络，可以将设备的管理接口连接到与管理中心相同的受保护内部网络。这样，就可以安全地从管理中心控制设备。您还可以配置多个管理接口，使管理中心能够管理和隔离来自其他网络上设备的流量。

无论如何部署设备，内部设备通信将始终加密。但是，您仍需采取措施，确保设备之间的通信不会出现中断、阻塞或受到篡改；例如，遭受分布式拒绝服务 (DDoS) 或中间人攻击。

思科云

管理中心 与思科云中的资源进行通信，用于实现以下功能：

- **高级恶意软件防护**

  默认配置的是公共云；要进行更改，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 更改 *AMP* 选项 。

- **URL 筛选**

  有关详细信息，请参阅 *URL* 过滤 一章。

- **Cisco Umbrella 连接**

有关详细信息，请参阅Cisco Umbrella DNS 策略 ， 第 1372 页。

互联网接入要求

默认情况下，系统配置为通过 443/tcp (HTTPS) 端口和 80/tcp (HTTP) 端口连接到互联网。如果您不希望设备直接接入互联网，则可以配置代理服务器。对于许多功能，您的位置可以确定系统访问哪些资源。

大多数情况下，它是可接入互联网的 管理中心。高可用性对中的两个 管理中心 均应可以接入互联网。根据功能，有时两个对等体均可以接入互联网，而有时只有活动对等体才可以接入互联网。

有时托管设备也可以接入互联网。例如，如果恶意软件防护配置使用动态分析，则受管设备会将文件直接提交到 Secure Secure Malware Analytics 云。或者，您也可以将设备同步到外部 NTP 服务器。

此外，除非您禁用 Web 分析跟踪，否则浏览器可能会与 Google Web 分析服务器通信，以向思科发送非个人可识别的使用数据。

表 *241:* 互联网接入要求

功能	原因	管理中心 高可用性	Resource
恶意软件防护	恶意软件云查找。	两个对等体均执行查找。	请参阅正确的 Cisco Secure Endpoint 和恶意软件分析操作所需的服务器地址。
	下载签名更新以进行文件预分类和本地恶意软件分析。	活动对等体执行下载，并同步到备用对等体。	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	提交文件以进行动态分析（受管设备）。 查询动态分析结果 (管理中心)。	两个对等体均查询动态分析报告。	fmc.api.threatgrid.com fmc.api.threatgrid.eu
面向终端的AMP集成	从 AMP 云接收由面向终端的 AMP 检测到的恶意软件事件。 显示由面向终端的 AMP 中的系统检测到的恶意软件事件。 使用在面向终端的 AMP 中创建的集中式文件阻止名单和允许名单覆盖 AMP 云中的处置情况。	两个对等体均接收事件。 您还必须在两个对等体上配置云连接（配置不会同步）。	请参阅正确的 Cisco Secure Endpoint 和恶意软件分析操作所需的服务器地址。
安全情报	下载安全智能源。	活动对等体执行下载，并同步到备用对等体。	intelligence.sourcefire.com

功能	原因	管理中心 高可用性	Resource
URL 筛选	下载 URL 类别和信誉数据。 手动查询（查找）URL类别和信誉数据。 查询未分类的 URL。	活动对等体执行下载，并同步到备用对等体。	URL： • regsvc.sco.cisco.com • est.sco.cisco.com • updates-talos.sco.cisco.com • updates.ironport.com IPV4 块： • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 IPV6 块： • 2a04:e4c7:ffff::/48 • 2a04:e4c7:fffe::/48
思科智能许可	与思科智能软件管理器通信。	活动对等体执行通信。	tools.cisco.com:443 www.cisco.com
思科成功网络	传输使用信息和统计信息。	活动对等体执行通信。	api-sse.cisco.com:8989 dex.sse.itd.cisco.com dex.eu.sse.itd.cisco.com
思科支持诊断结果	接受授权请求并传输使用信息和统计信息。	活动对等体执行通信。	api-sse.cisco.com:8989
系统更新	直接将更新从思科下载到管理中心： • 系统软件 • 入侵规则 • 漏洞数据库 (VDB) • 地理位置数据库 (GeoDB)	更新活动对等体上的入侵规则、VDB 和 GeoDB，然后再同步到备用对等体。 在每个对等体上单独升级系统软件。	cisco.com sourcefire.com
SecureX 威胁响应集成	请参阅相应的集成指南。		

功能	原因	管理中心 高可用性	Resource
时间同步	同步部署中的时间。 代理服务器不支持。	使用外部 NTP 服务器的任何设备均必须接入互联网。	0.sourcefire.pool.ntp.org 1.sourcefire.pool.ntp.org 2.sourcefire.pool.ntp.org 3.sourcefire.pool.ntp.org
RSS 源	在控制面板上显示思科威胁研究博客。	显示RSS源的任何设备均必须接入互联网。	blog.talosintelligence.com blogs.cisco.com feeds.feedburner.com
Whois	请求外部主机的 whois 信息。 代理服务器不支持。	请求 whois 信息的任何设备均必须接入互联网。	whois 客户端会尝试猜出要查询的正确服务器。如果猜不出，则使用： • NIC 句柄：whois.networksolutions.com • IPv4 地址和网络名称：whois.arin.net

通信端口要求

管理中心 和托管设备在 8305/tcp 端口上使用双向、SSL 加密的通信通道进行通信。此端口 必须 保持开放，以进行基本通信。

其他端口允许安全管理，并访问特定功能所需的外部资源。一般来说，除非启用或配置相关功能，否则，功能相关的端口会保持关闭。在了解此操作对部署的影响之前，请勿更改或关闭已打开的端口。

表 *242:* 通信端口要求

端口	协议/功能	平台	方向	详细信息
53/tcp 53/udp	DNS		发送	DNS
67/udp 68/udp	DHCP		发送	DHCP
123/udp	NTP		发送	同步时间。
162/udp	SNMP		发送	发送 SNMP 警报至远程陷阱服务器。

端口	协议/功能	平台	方向	详细信息
389/tcp 636/tcp	LDAP		发送	与 LDAP 服务器通信以进行外部身份验证。 获取检测到的 LDAP 用户元数据（仅限管理中心）。 可配置。
443/tcp	HTTPS	管理中心	接收	如果您使用本地安全设备连接器载入 管理中心，则允许端口 443 上的入站连接。
443/tcp	HTPS	管理中心	出站	如果使用云连接器将 管理中心 载入 CDO，则允许来自端口 443 的出站流量。
443/tcp	HTPS	管理中心	出站	如果使用 SecureX 载入管理中心，则允许端口 443 的出站连接。
443/tcp	HTTPS		发送	发送和接收来自互联网的数据。
514/udp	系统日志（警报）		发送	向远程系统日志服务器发送警报。
1812/udp 1813/udp	RADIUS		发送	与 RADIUS 服务器通信以进行外部身份验证和记账。 可配置。
8305/tcp	设备通信		双向	在同一部署中的设备之间安全地进行通信。 可配置。如果更改此端口，必须为部署中的所有设备更改此端口。建议保留默认值。

相关主题

添加 CDO的 LDAP 外部身份验证对象，第 164 页
添加 CDO的 RADIUS 外部身份验证对象，第 170 页

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。