



配置 FTD 设备

- [接口, on page 2](#)
- [使用 FXOS 同步添加到 Firepower 设备的接口, 第 40 页](#)
- [路由, on page 41](#)
- [对象, on page 48](#)
- [安全策略管理, 第 98 页](#)
- [FDM 策略配置, on page 98](#)
- [虚拟专用网络管理, 第 186 页](#)
- [模板, on page 279](#)
- [FDM 管理 高可用性, on page 287](#)
- [FDM 管理 设备设置, 第 297 页](#)
- [CDO 命令行接口, on page 307](#)
- [批量命令行接口, on page 309](#)
- [用于管理设备的 CLI 宏, on page 313](#)
- [命令行接口文档, on page 317](#)
- [导出 CLI 命令结果, on page 317](#)
- [CDO 公共 API, 第 320 页](#)
- [创建 REST API 宏, on page 320](#)
- [读取、丢弃、检查和部署更改, 第 327 页](#)
- [读取所有设备配置, on page 328](#)
- [将配置更改从 FDM 管理 设备读取到 CDO, on page 329](#)
- [预览和部署所有设备的配置更改, 第 332 页](#)
- [将配置更改从 CDO 部署到 FDM 管理 设备, on page 333](#)
- [将更改部署到设备, on page 333](#)
- [批量部署设备配置, on page 334](#)
- [已计划的自动部署, on page 335](#)
- [检查配置更改, on page 337](#)
- [放弃更改, on page 338](#)
- [设备上的带外更改, on page 339](#)
- [同步 Defense Orchestrator 和设备之间的配置, 第 339 页](#)

- [冲突检测, on page 339](#)
- [自动接受设备的带外更改, on page 340](#)
- [解决配置冲突, on page 341](#)
- [安排设备更改轮询, on page 343](#)
- [安排安全数据库更新, 第 344 页](#)
- [更新 FDM 管理 设备安全数据库, on page 345](#)

接口

您可以使用 Cisco Defense Orchestrator (CDO) 配置和编辑 Firepower 威胁防御 (FTD) 设备上的数据接口或管理/诊断接口。

目前, CDO 只能配置路由接口和网桥组。它不支持配置被动接口。

Firepower 接口配置的指南和限制

使用 思科防御协调器(CDO)配置设备时, 接口配置存在许多局限性。如果您需要以下任意功能, 则必须使用 Firepower 管理中心来配置设备。

防火墙

- 仅支持路由防火墙模式。无法配置透明防火墙模式的接口。
- 只有物理 Firepower 1010 设备支持为交换机端口模式配置的接口。有关详细信息, 请参阅 [FDM 管理 设备的交换机端口模式接口](#)。

被动

- 目前, 思科防御协调器(CDO)未在接口表中识别被动接口模式, 并且您无法配置被动或 ERSPAN 接口。您必须使用 FDM 管理 UI 配置和识别被动接口。

仅 IPS 模式

- 不能将接口配置为内联（在内联集内）或内联分路, 用于仅 IPS 的处理。仅 IPS 模式的接口将绕过许多防火墙检查, 仅支持 IPS 安全策略。相比之下, 防火墙模式接口需要对流量执行防火墙功能, 例如维持流量、跟踪 IP 和 TCP 层的流量状态、IP 分片重组和 TCP 规范化。
- 可选, 您可以根据安全策略, 选择配置该防火墙模式接口的 IPS 功能。

EtherChannel

CDO 支持运行版本 6.5 及更高版本的设备的读取、创建和功能。要创建 Etherchannel 接口, 请参阅 [为 FDM 管理 设备添加 EtherChannel 接口](#)。要创建

- 您最多可以在物理 Firepower 设备上配置 48 个 EtherChannel, 但一次可以活动的接口数量取决于您的设备型号。有关设备特定的限制, 请参阅 [设备特定限制](#)。

- 通道组中的所有接口都必须具有相同的介质类型和容量，并且必须设置为相同的速度和双工模式。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。
- EtherChannel 连接到的设备还必须支持 802.3ad EtherChannel。
- FDM 托管设备不支持带有 VLAN 标记的 LACPDU。如果使用 Cisco IOS `vlan dot1Q tag native` 命令在相邻交换机上启用本地 VLAN 标记，则 FDM 管理设备将会丢弃已标记的 LACPDU。请务必禁用相邻交换机上的本地 VLAN 标记。
- 所有 FDM 管理设备配置均引用 EtherChannel 接口，而不是成员物理接口。



Note 设置为 `portchannels` 的接口仅支持物理接口、冗余接口和子接口作为网桥组成员接口。

网桥组

目前，CDO 支持一个网桥组的配置。要确定您的设备是否支持网桥组，请参阅 [FDM 管理配置中的网桥组兼容性](#) 以了解详细信息。

将接口添加到桥接组时，请记住以下几点：

- 该接口必须具有名称。
- 该接口不能有任何已定义的 IPv4 或 IPv6 地址，无论是静态分配的还是通过 DHCP 获得的。
- BVI 可以将 VLAN 接口或其他路由接口作为成员接口，但不能将两个接口作为单个 BVI 上的成员接口。
- BVI 可以将 VLAN 接口或其他路由接口作为成员接口，但不能将两个接口作为单个 BVI 上的成员接口。
- 接口不能是以太网的点对点协议 (PPPoE)
- 接口不能与安全区域关联（如果它在区域中）。您必须删除该接口的所有 NAT 规则，然后才能将其添加到网桥组。
- 单独启用和禁用成员接口。这样就可以禁用任何未使用的接口，而无需将其从网桥组删除。网桥组本身始终处于启用状态。
- 您可以配置成为网桥组 **成员** 的接口。有关接口要求和创建，请参阅 [配置网桥组](#)。

以太网的点对点协议

- 不能为 IPv4 配置以太网点对点协议 (PPPoE)。如果将互联网接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，且 ISP 使用 PPPoE 为您提供 IP 地址，则您必须使用 FDM 来配置这些设置。

VLAN

要配置 VLAN 接口和 VLAN 成员，请参阅[配置 FDM 管理设备 VLAN](#) 以了解详细信息。要为交换机端口模式配置 VLAN，请参阅[为交换机端口模式配置 FDM 管理设备 VLAN](#) 以了解详细信息。

- 接口必须是物理接口。
- 接口不能是仅管理接口。
- 接口不能与任何其他类型的接口关联，包括 BVI、子接口、另一个 VLAN 接口、EtherChannel 等。
- 接口不能是 BVI 成员或 etherchannel 成员。
- 设备型号支持不同数量的 VLAN 成员。有关详细信息，请参阅[各设备型号的最大 VLAN 成员数量](#)。



Note 要为环境配置 VLAN，请参阅[配置 Firepower VLAN 子接口和 802.1Q 中继](#)。

网络模块卡

可选的网络模块安装仅限于 ASA 5515-X、5525-X、5545-X 和 5555-X 以及 Firepower 2100 系列设备。

- 仅在引导程序期间（即初始安装或重新映像，或在本地/删除管理之间切换时），才会发现网络接口卡。CDO 会为这些接口设置正确的速度和复用默认值。如果将可选网络接口卡替换为更改接口速度/双工选项的卡，而不更改可用接口的总数，则重新启动设备，以便系统识别替换接口的正确速度/双工值。在与设备的 SSH 或控制台会话中，输入 `reboot` 命令。然后，使用 CDO，编辑能够更改的各物理接口，并选择有效的速度和双工选项，因为系统不会自动更正您的原始设置。立即部署更改，确保系统行为正确无误。
- 您无法在 FDM 管理 Secure Firewall 3100 系列设备上启用或禁用网络模块或执行接口的分支在线插入和删除 (OIR)。



Note 将卡更换为接口总数更改的卡，或移除其他对象引用的接口，均可能导致意外问题。如果需要进行此类更改，请先删除待移除接口的所有引用，如安全区成员资格、VPN 连接等。此外，建议您在更改前进行备份。

虚拟 FDM 管理 设备上的接口

- 如果不重新初始化虚拟 FDM 管理 设备，则无法添加或删除接口。您必须在 FDM 管理 设备中执行这些操作。



Note 如果更换的接口具有不同的速率/双工能力，需要重启设备，使系统能够识别新的速率/双工值，步骤如下：在设备的CLI控制台中，输入“重新引导”命令。然后，在 CDO 中，编辑能够更改的各接口，并选择有效的速度和复用选项，因为系统不会自动更正您的原始设置。立即部署更改，确保系统行为正确无误。

各设备型号的最大 VLAN 成员数量

设备型号限制可配置的最大 VLAN 子接口数量。请注意，仅可在数据接口上而不可在管理接口上配置子接口。下表介绍各设备型号的限制。

型号	最大 VLAN 子接口数量
Firepower 1010	60
Firepower 1120	512
Firepower 1140、Firepower 1150	1024
Firepower 2100	1024
Firepower 4100	1024
Firepower 9300	1024
ASA 5508-X	50
ASA 5515-X	100
ASA 5516-X	100
ASA 5525-X	200
ASA 5545-X	300
ASA 5555-X	500
ISA 3000	100

Firepower 数据接口

Cisco Defense Orchestrator (CDO) 支持在 FDM 管理设备上配置路由接口和桥接虚拟接口。

路由接口

每个第 3 层路由接口（或子接口）都需要唯一子网上的一个 IP 地址。通常会将这些接口与交换机、另一个路由器上的端口或 ISP/WAN 网关连接。

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

可以在路由接口上同时配置 IPv4 和 IPv6 地址。请确保配置一条同时适用于 IPv4 和 IPv6 的默认路由。需要使用 Firepower 设备管理器在 FDM 管理设备上执行此任务。有关配置默认路由的信息，请参阅“[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南，版本 xxx](#)”中的[基础知识 > 路由](#)。

网桥组和网桥虚拟接口

网桥组是 FDM 管理设备用于桥接而非路由的一组接口。桥接接口属于桥接组，且所有接口都在同一网络上。桥接组由在网桥网络上有 IP 地址的桥接虚拟接口 (BVI) 表示。包含在网桥组中的接口称为“成员”。

如果指定 BVI，您可以在路由接口和 BVI 之间路由。在这种情况下，BVI 充当成员接口和路由接口之间的网关。如果不指定 BVI，网桥组成员接口上的流量不能离开网桥组。通常，您可以指定该接口，以便将成员接口路由到互联网。

FDM 管理设备仅支持一个网桥组；因此，CDO 只能管理该网桥组，而无法在设备上创建其他网桥组。CDO 只能管理直接安装在硬件上的 FDM 管理设备上的 BVI，而不能管理虚拟 FDM 管理设备实例上的 BVI。

路由模式下网桥组的一种用途是在 FDM 管理设备上而非外部交换机上使用额外接口。您可以将终端直接连接到网桥组成员接口。您还可以连接交换机，以将更多终端添加到与 BVI 相同的网络。

被动接口

被动接口使用交换机 SPAN（交换端口分析器）或镜像端口监控在网络中传输的流量。SPAN 或镜像端口允许从交换机的其他端口复制流量。此功能可以提供网络内的系统可视性，而不会影响网络流量。如果在被动部署中配置系统，系统将不能执行某些操作，例如，阻止流量或流量整形。被动接口无条件接收所有流量，这些接口不会重传接收到的流量。

目前，CDO 对管理 FDM 管理设备上的被动接口提供有限的支持：

- 必须在 FDM 管理设备上配置被动接口。
- 路由接口无法使用 CDO 来更改为被动接口，而被动接口也无法更改为路由接口。
- CDO 不会标识接口表中的被动接口。

相关信息：

- [Firepower 接口的 IPv6 寻址](#)
- [Firepower 接口配置的指南和限制](#)
- [配置物理 Firepower 接口](#)

管理/诊断接口

标记为“管理” (Management) 的物理端口（对于 FDM 管理设备虚拟，则为 Management 0/0 虚拟接口）实际上有两个与其关联的单独接口。

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

（硬件设备。）建议配置管理/诊断接口时，不要将物理端口连接到网络。而是仅配置管理 IP 地址，并把它配置为将数据接口用作从互联网获取更新的网关。然后，打开 HTTPS/SSH 流量（默认情况下启用 HTTPS）的内部接口，并使用内部 IP 地址打开 Firepower 设备管理器。您必须直接在 Firepower 设备管理器上执行此任务。有关说明，请参阅《[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#)》中的“配置管理访问列表”。

对于 FDM 管理设备虚拟，建议的配置是将 Management0/0 连接到与内部接口相同的网络，并将内部接口用作网关。不要为诊断接口配置单独的地址。



Note 有关如何编辑管理接口的特殊说明，请参阅适用于 **Firepower 版本 6.4 或更高版本** 的《[Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#)》。打开指南并导航至 **基础知识 > 接口 > 管理/诊断接口**。管理接口配置应在 Firepower 设备管理器上完成。

接口设置

使用这些主题来配置接口设置。

在 Firepower 接口设置中使用安全区域

可为每个接口分配一个安全区。然后根据区域应用您的安全策略。例如，您可以将内部接口分配到内部区域，而将外部接口分配到外部区域。例如，可以配置访问控制策略，允许流量从内部传到外部，但不允许从外部传入内部。

每个区域都有一个模式，路由或被动模式。该模式与接口模式直接关联。您可以仅向同一模式安全区添加路由和被动接口。

桥接虚拟接口 (BVI) 不会添加到安全区域。仅将成员接口添加到安全区域。

不能将诊断或管理接口包括在区域中。区域只适用于数据接口。

CDO 当前不支持在 ASA 或 FTD 设备上管理、监控或使用虚拟隧道接口 (VTI) 隧道。已配置 VTI 隧道的设备可以被载入 CDO，但它会忽略 VTI 接口。如果安全区域或静态路由引用 VTI，则 CDO 会读取不带 VTI 引用的安全区域和静态路由。即将推出对 VTI 隧道的 CDO 支持。

有关安全区域的详细信息，请参阅[安全区域对象](#)。

将 FDM 管理设备接口分配给安全区域

准备工作

在添加安全区域时，接口存在以下限制：

- 该接口必须具有名称。
- 接口不能是仅管理接口。此选项可在界面的“高级”(Advanced)选项卡中启用和禁用。
- 不能将安全区域分配给网桥组接口。
- 不能将安全区域分配给为交换机端口模式配置的接口。
- CDO 当前不支持在 ASA 或 FDM 管理设备上管理、监控或使用虚拟隧道接口 (VTI) 隧道。已配置 VTI 隧道的设备可以被载入 CDO，但它会忽略 VTI 接口。如果安全区域或静态路由引用 VTI，则 CDO 会读取不带 VTI 引用的安全区域和静态路由。即将推出对 VTI 隧道的 CDO 支持。

将 Firepower 接口分配给安全区域

使用以下程序将安全区域关联到现有接口：

Procedure


步骤 1 登录 CDO。

步骤 2 在导航窗格中，点击**清单 (Inventory)**。

步骤 3 点击**设备 (Devices)**选项卡以查找设备，或点击**模板 (Templates)**选项卡以查找型号设备。

步骤 4 点击**FTD 设备**，然后选择要修改的 FDM 管理设备。

步骤 5 在右侧的**管理 (Management)**窗格中，点击**接口 (Interfaces)**。

步骤 6 选择要向其添加安全区域的接口，然后点击  **编辑 (Edit)**。

步骤 7 使用**安全区 (Security Zone)**下拉菜单并选择要与此接口关联的安全区域。

Note 如果需要，请点击**新建 (Create New)**，从此下拉菜单中创建新的安全区域。

步骤 8 点击**保存 (Save)**。

步骤 9 将配置更改从 CDO 部署到 FDM 管理设备。

相关信息：

- [安全区域对象](#)

- [创建或编辑 Firepower 安全区域对象](#)
- [Firepower 接口配置的指南和限制](#)

在 Firepower 接口设置中使用 Auto-MDI/MDX

对于 RJ-45 接口，默认的自动协商设置还包括 Auto-MDI/MDIX 功能。Auto-MDI/MDIX 在自动协商阶段检测直通电缆时执行内部交叉，从而消除交叉布线的需要。如要启用接口的 Auto-MDI/MDIX，必须将速度或双工设置为自动协商。如果将速度和双工明确设置为固定值，从而禁用了两种设置的自动协商，则 Auto-MDI/MDIX 也将被禁用。对于千兆以太网，当速度和双工被设置为 1000 和全值时，接口始终会自动协商；因此，Auto-MDI/MDIX 始终会启用，且您无法禁用它。

在编辑接口时，可在“高级” (Advanced) 选项卡上配置这些设置。

在 Firepower 接口设置中使用 MAC 地址

您可以手动配置介质访问控制 (MAC) 地址来覆盖默认值。

对于高可用性配置，您可以同时配置接口的主用和备用 MAC 地址。如果主用设备进行故障切换，并且备用设备成为主用设备，则新的主用设备会开始使用主用 MAC 地址，以最大限度地减少网络中断。

在配置接口时，在“高级” (Advanced) 选项卡上配置主用和备用 MAC 地址。

默认 MAC 地址

默认 MAC 地址分配取决于接口类型。

- **物理接口 (Physical interfaces)** - 物理接口使用已刻录的 MAC 地址。
- **子接口 (Subinterfaces)** - 物理接口的所有子接口都使用相同的刻录的 MAC 地址。您可能想为子接口分配唯一的 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一的 MAC 地址分配给子接口会允许唯一的 IPv6 链路本地地址。

在 Firepower 接口设置中使用 MTU 设置

关于 MTU

MTU 会指定 FDM 管理设备可在给定以太网接口上传输的最大帧负载大小。MTU 值是没有以太网报头、VLAN 标记或其他系统开销情况下的帧大小。例如，将 MTU 设置为 1500 时，预期帧大小为 1518 字节（含报头）或 1522 字节（使用 VLAN）。请勿为容纳这些报头而将 MTU 的值设得过高。

路径 MTU 发现

FDM 管理设备支持路径 MTU 发现（如 RFC 1191 中所定义），从而使两个主机之间的网络路径中的所有设备均可协调 MTU，以便它们可以标准化路径中的最低 MTU。

MTU 和分段

对于 IPv4，如果传出 IP 数据包大于指定 MTU，则该数据包将分为 2 帧或更多帧。片段在目标处（有时在中间跃点处）重组，而分片可能会导致性能下降。对于 IPv6，通常不允许对数据包进行分段。因此，IP 数据包大小应在 MTU 大小范围内，以避免分片。

对于 UDP 或 ICMP，应用应将 MTU 考虑在内，以避免分段。



Note 只要有内存空间，FDM 管理设备就可接收大于所配置的 MTU 的帧。

MTU 和巨型帧

MTU 越大，您能发送的数据包越大。加大数据包可能有利于提高网络效率。请参阅以下准则：

- 与流量路径上的 MTU 相匹配：我们建议将所有 FDM 管理设备接口以及流量路径的其他设备接口上的 MTU 设为相同。匹配 MTU 可防止中间设备对数据包进行分片。
- 容纳巨型帧：巨型帧是指大于标准最大值 1522 字节（包括第 2 层报头和 VLAN 报头）的以太网数据包，最大为 9216 字节。MTU 最大可设置为 9198 字节，以容纳巨帧。FDM 管理虚拟的最大值为 9000。



Note 加大 MTU 会为巨型帧分配更多内存，这样可能会限制其他功能（例如访问规则）的最大使用量。如果在 ASA 5500-X 系列设备或 FDM 管理虚拟上将 MTU 增加到默认值 1500 以上，则必须重新启动系统。无需重启 Firepower 2100 系列设备，因为巨帧支持在该设备上始终启用。

默认情况下，在 Firepower 3100 设备上启用巨帧支持。

Firepower 接口的 IPv6 寻址

您可以为 Firepower 物理接口配置两种类型的单播 IPv6 地址。

- **全局 (Global)** - 全局地址是可在公用网络上使用的公用地址。对于桥接组，需要在桥接虚拟接口 (BVI) 上而非每个成员接口上配置全局地址。不能将以下任何地址指定为全局地址。
 - 内部保留的 IPv6 地址：fd00::/56 (fd00:: 至 fd00:0000:0000:00ff:ffff:ffff:ffff:ffff)
 - 未指定的地址，例如 ::/128
 - 环回地址 ::1/128
 - 组播地址，ff00::/8
 - 链路本地地址 fe80::/10

- **链路本地 (Link-local)** - 链路本地地址是只能在直连网络上使用的专用地址。路由器不使用链路本地地址转发数据包；它们仅用于在特定物理网段上通信。链路本地地址可用于地址配置或网络发现功能，例如地址解析和邻居发现。每个接口必须有自己的地址，因为链路本地地址仅在网段中可用，并且会与接口 MAC 地址绑定。

至少需要配置链路本地地址，IPv6 才会起作用。如果配置全局地址，则接口上会自动配置链路本地地址，因此无需另外专门配置链路本地地址。如果不配置全局地址，则需要自动或手动配置链路本地地址。

配置 Firepower 接口

将电缆（以物理方式或虚拟方式）连接到接口接头时，您需要配置该接口。至少需要命名并启用该接口，流量才会通过该接口。如果该接口是网桥组的成员，则只用于接口命名。如果接口是桥接虚拟接口 (BVI)，则需要为 BVI 分配一个 IP 地址。如果要在特定端口上创建 VLAN 子接口（而非单一物理接口），通常要在该子接口（而不是物理接口）上配置 IP 地址。通过 VLAN 子接口，可将一个物理接口划分成多个标记有不同 VLAN ID 的逻辑接口。

接口列表将显示可用的接口及其名称、地址和状态。您可以通过选择接口行并点击“操作” (Actions) 窗格中的 **编辑 (Edit)** 来更改接口的状态（打开或关闭）或编辑接口。列表将基于您的配置显示接口特征。展开接口行以查看子接口或桥接组成员。

相关信息：

- [接口](#)
- [配置物理 Firepower 接口](#)
- [配置高级 Firepower 接口选项, on page 18](#)
- [配置 Firepower VLAN 子接口和 802.1Q 中继](#)
- [为交换机端口模式配置 FDM 管理设备 VLAN](#)

配置物理 Firepower 接口

要启用物理接口，至少必须启用它。您可以常规命名它和配置 IP 地址；然而，如果要创建 VLAN 子接口，或者配置被动模式接口，或者要将接口添加到网桥组，无需配置 IP 寻址。



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

您可以禁用接口，以临时阻止在相连网络中的传输。无需删除该接口的配置。目前，思科防御协调器 (CDO) 只能配置路由接口和网桥组。CDO 会列出被动接口，但不能将其从 CDO 重新配置为主动接口。



Note 注意：CDO 不支持 IPv4 的点对点以太网协议 (PPPoE) 配置。在 FDM 管理设备中配置此选项可能会导致 CDO UI 出现问题；如果必须为设备配置 PPPoE，则必须在 FDM 管理设备中进行适当的更改。

操作步骤

Procedure

步骤 1 在设备和服务 (**Devices & Services**) 页面上，点击要配置其接口的设备，然后点击右侧管理窗格中的接口 (**Interfaces**)。

步骤 2 在“接口” (**Interfaces**) 页面上，选择要配置的物理接口。

步骤 3 在右侧的“操作” (**Actions**) 窗格中，点击编辑 (**Edit**)。

步骤 4 为物理接口指定逻辑名称 (**Logical Name**) 和说明 (**Description**) (可选)。除非配置子接口，否则接口应有名称。

Note 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

步骤 5 选择这两个选项之一：

- 如果要添加子接口：

如果要为此物理接口配置子接口，则可能已完成。点击保存 (**Save**) 并继续配置 [Firepower VLAN 子接口](#) 和 [802.1Q 中继](#)；否则，请继续。

Note 即使在配置子接口时，为接口命名和提供 IP 地址也有效。这不是常规设置，但如果确定符合您的需求，则可以进行配置。

- 如果您不打算添加子接口，请继续[为物理接口配置 IPv4 地址](#)和[为物理接口配置 IPv6 地址](#)中的一个或两个。

为物理接口配置 IPv4 地址



Warning 在配置并保存 DHCP 地址池后，DHCP 地址池将绑定到接口的已配置 IP 地址。如果在配置 DHCP 地址池后编辑接口的子网掩码，则部署到 FDM 管理设备会失败。此外，如果在 FDM 管理控制台中编辑 DHCP 地址池并从 FDM 管理设备读取配置到思科防御协调器中，则读取操作会失败。

Procedure

步骤 1 在“编辑物理接口” (Editing Physical Interface) 对话框中，点击 **IPv4 地址 (IPv4 Address)** 选项卡。

步骤 2 从类型字段中选择以下任一选项：

- **静态 (Static)** - 如果希望分配固定的地址，请选择此选项。对于连接到接口的网络，输入接口的 IP 地址和子网掩码。例如，如果您连接的是 10.100.10.0/24 网络，则可以输入 10.100.10.1/24。确保您输入的地址不是网络 ID 或网络的广播地址，并且该地址尚未在网络上使用。
 - **备用 IP 地址和子网掩码 (Standby IP Address and Subnet Mask)** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。
 - **可选) DHCP 地址池 ([Optional] DHCP Address Pool)** - 输入单个 DHCP 服务器 IP 地址或 IP 地址范围。该 IP 地址范围必须与所选接口位于同一子网上，并且不能包括接口本身的 IP 地址、广播地址或子网地址。指定该池的开始和结束地址，用连字符隔开。要暂时禁用此 DHCP 服务器，请在 [配置 DHCP 服务器](#) 页面的 **DHCP 服务器 (DHCP Servers)** 部分编辑该服务器。
- **动态 (DHCP) (Dynamic [DHCP])** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。如有需要，更改以下选项：
 - **获取默认路由 (Obtain Default Route)** - 是否从 DHCP 服务器获取默认路由。您通常都要选中此选项。
 - **DHCP 路由指标 (DHCP Route Metric)** - 如果从 DHCP 服务器获取默认路由，请输入与获知路由的管理距离，其值介于 1 到 255 之间。

Note 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。

步骤 3 完成后点击**保存 (Save)**，或者继续执行其中一个程序：

- 如果要为此接口分配 IPv6 地址和 IPv4 地址，请“[为物理接口配置 IPv6 地址](#)”。
 - [配置高级 Firepower 接口选项, on page 18](#)。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。
 - 如果您保存了接口并且不想继续使用高级接口选项，请继续[启用物理接口](#)。
-

为物理接口配置 IPv6 地址

Procedure

- 步骤 1** 在“编辑物理接口” (Editing Physical Interface) 对话框中，点击“IPv6 地址” (IPv6 Address) 选项卡。
- 步骤 2 状态 (State)** - 在您未配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请点击状态 (State) 滑块将其启用。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

Note 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

- 步骤 3 地址自动配置 (Address Auto Configuration)** - 选中此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

虽然 RFC 4862 规定为无状态自动配置所配置的主机不发送路由器通告消息，但 FDM 管理设备在这种情况下确实会发送路由器通告消息。选择抑制 RA 可抑制消息，遵从 RFC 要求。

- 步骤 4 抑制 RA (Suppress RA)** - 如果要抑制路由器通告，请选中此复选框。Firepower 威胁防御设备可参与路由器通告，以便相邻设备可动态获知默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息 (ICMPv6 类型 134)。

也会发送路由器通告，以响应路由器请求消息 (ICMPv6 类型 133)。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

对于不希望 Firepower 防御设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望在接口上抑制这些消息。

- 步骤 5 本地链路地址 (Link-Local Address)** - 如果要仅将地址用作链路本地地址，请在链路本地地址字段中输入该地址。本地链路地址在本地网络之外无法访问。在网桥组接口上无法配置本地链路地址。

Note 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feec:6a82。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

- 步骤 6 备用链路本地地址 (Standby Link-Local Address)** - 如果接口连接高可用性设备，请配置此地址。输入此接口所连接的另一台 FDM 管理设备上的接口本地链路地址。

- 步骤 7 静态地址/前缀 (Static Address/Prefix)** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅 [Firepower 接口的 IPv6 寻址](#)。

- 步骤 8 备用 IP 地址 (Standby IP Address)** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

- 步骤 9** 完成后点击保存 (Save)，或者继续执行其中一个程序：

- [配置高级 Firepower 接口选项, on page 18](#)。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。

- 如果您保存了接口并且不想继续使用高级接口选项，请继续[启用物理接口](#)。

启用物理接口

Procedure

- 步骤 1** 选择要启用的接口。
- 步骤 2** 将与接口逻辑名称关联的窗口右上角的**状态 (State)** 滑块滑动到蓝色。
- 步骤 3** 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

配置 Firepower VLAN 子接口和 802.1Q 中继

通过 VLAN 子接口，可将一个物理接口划分成多个标记有不同 VLAN ID 的逻辑接口。带有一个或多个 VLAN 子接口的接口将自动配置为 802.1Q 中继。由于 VLAN 允许您在特定物理接口上将流量分开，所以您可以增加网络中可用的接口数量，而无需增加物理接口或设备。

如果您将物理接口连接到交换机的中继端口，请创建子接口。为交换机中继端口上显示的每个 VLAN 创建子接口。如果您将物理接口连接到交换机的接入端口，创建子接口将没有意义。



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

准备工作

阻止物理接口上的未标记数据包。 如果使用子接口，您通常不想让物理接口传递流量，因为物理接口会传递未标记的数据包。由于必须启用物理接口，才能允许子接口传递流量，所以请确保物理接口不会通过未命名接口传递流量。如果要允许物理接口传递未标记数据包，可以照常命名接口。

操作步骤

Procedure

- 步骤 1** 在导航窗格中，点击**设备和服务 (Devices & Services)**。
- 步骤 2** 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
- 步骤 3** 点击**FTD** 选项卡，然后点击要配置其接口的设备。
- 步骤 4** 点击右侧**管理 (Management)** 窗格中的**接口 (Interfaces)**。
- 步骤 5** 在“接口” (Interfaces) 页面上，选择要配置的物理接口，然后在右侧的“操作” (Actions) 窗格中，点击+ **新建子接口 (+ New Subinterface)**。

请注意，**父接口 (Parent Interface)** 字段显示要为其创建此子接口的物理接口的名称。创建子接口后，父接口则无法更改。

步骤 6 为子接口提供**逻辑名称和说明**（可选）。如果没有逻辑名称，将忽略其余的接口配置。

Note 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

步骤 7 配置 VLAN ID 和子接口 ID:

- **VLAN ID** - 输入 VLAN ID，介于 1 和 4094 之间，用于标记该子接口上的数据包。
- **子接口 ID (Subinterface ID)** - 以整数形式输入介于 1 和 4294967295 之间的子接口 ID。允许的子接口数**各设备型号的最大 VLAN 成员数量**。在创建子接口后，您无法更改子接口 ID。

继续为子接口配置 IPv4 地址 和 为子接口配置 IPv6 地址 。

为子接口配置 IPv4 地址

Procedure

步骤 1 在“添加子接口” (Adding Subinterface) 对话框中，点击 **IPv4 地址 (IPv4 Address)** 选项卡。

步骤 2 从类型字段中选择以下任一选项:

- **静态 (Static)** - 如果希望分配固定的地址，请选择此选项。
对于连接到接口的网络，输入接口的 **IP 地址和子网掩码**。例如，如果您连接的是 10.100.10.0/24 网络，则可以输入 10.100.10.1/24。确保您输入的地址不是网络 ID 或网络的广播地址，并且该地址尚未在网络上使用。
- 仅当在高可用性设备对中使用时，才输入**备用 IP 地址**和子网掩码。
- **动态 (DHCP) (Dynamic [DHCP])** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。如有需要，更改以下选项：
 - **获取默认路由 (Obtain Default Route)** - 是否从 DHCP 服务器获取默认路由。您通常都要选中此选项。
 - **DHCP 路由指标 (DHCP Route Metric)** - 如果从 DHCP 服务器获取默认路由，请输入与获知路由的管理距离，其值介于 1 到 255 之间。

请参阅[配置 DHCP 服务器](#)。

Note 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。

步骤 3 完成后点击**创建 (Create)**，或者继续执行以下程序之一：

- 如果要为此接口分配 IPv6 地址和 IPv4 地址，请继续执行“[为物理接口配置 IPv6 地址](#)”。
- [配置高级 Firepower 接口选项, on page 18](#)。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。
- 如果已创建子接口，请转至[启用物理接口](#)。

为子接口配置 IPv6 地址

Procedure

步骤 1 点击“IPv6 地址” (IPv6 Address) 选项卡。

步骤 2 启用 **IPv6 处理 (Enable IPv6 processing)** - 在不想配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请将状态滑块移至蓝色。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

Note 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

步骤 3 **地址自动配置 (Address Auto Configuration)** - 选中此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

步骤 4 **抑制 RA (Suppress RA)** - 如果要抑制路由器通告，请选中此复选框。Firepower 威胁防御设备可参与路由器通告，以便相邻设备可动态获知默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

也会发送路由器通告，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

对于不希望 Firepower 防御设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望在接口上抑制这些消息。

步骤 5 **本地链路地址 (Link-Local Address)** - 如果要仅将地址用作链路本地地址，请在链路本地地址字段中输入该地址。本地链路地址在本地网络之外无法访问。

Note 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feec:6a82。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

步骤 6 **备用链路本地地址 (Standby Link-Local Address)** - 如果接口连接高可用性设备，请配置此地址。

步骤 7 **静态地址/前缀 (Static Address/Prefix)** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅第 136 页上的“IPv6 地址”。

步骤 8 备用 IP 地址 (Standby IP Address) - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

步骤 9 完成后点击**创建 (Create)**，或者继续执行以下程序之一：

- 点击“高级” (Advanced) 选项卡转到[配置高级 Firepower 接口选项, on page 18](#)。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。
- 如果已创建子接口，请转至[启用物理接口](#)。

启用物理接口

Procedure

步骤 1 要启用子接口，请将子接口的逻辑名称关联的状态滑块滑动到蓝色。

步骤 2 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

配置高级 Firepower 接口选项

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

以下步骤程序假定已定义接口。另外，您还可以在初始编辑或创建接口时编辑这些设置。

此程序及其中的所有步骤都是可选的。

限制：

- 您无法在 Firepower 2100 系列设备上设置管理接口的 MTU、复用或速度。
- 在未命名接口上，MTU 必须 设置为 1500。

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击**FTD** 选项卡，然后点击要配置其接口的设备。

步骤 4 点击右侧**管理 (Management)** 窗格中的 **接口 (Interfaces)**。

步骤 5 在“接口” (Interfaces) 页面上，选择要配置的物理接口，然后在右侧的“操作” (Actions) 窗格中，点击**编辑 (Edit)**。

步骤 6 点击高级选项卡。

步骤 7 启用高可用性监控 (**Enable for HA Monitoring**) 会被自动启用。如果将其启用，当 HA 对决定是否在高可用性配置中故障转移到对等设备时，设备会考虑接口的运行状况。如果不配置高可用性，可忽略此选项。如果不配置接口的名称，也可以忽略此选项。

步骤 8 要将数据接口仅用于管理，请选中**仅管理 (Management Only)**。

仅管理接口不允许直通流量，所以将数据接口设置为**仅管理 (Management Only)**接口的价值微乎其微。不能更改管理/诊断接口的此项设置，它们始终为仅管理。

步骤 9 修改 IPv6 DHCP 设置。

- **启用 DHCP 以获取 IPv6 地址配置** - 是否在 IPv6 路由器通告数据包中设置“托管地址配置” (Managed Address Configuration) 标志。此标志通知 IPv6 自动配置客户端应使用 DHCPv6 来获取相关地址以及派生的无状态自动配置地址。
- **启用 DHCP 以获取 IPv6 非地址配置** - 是否在 IPv6 路由器通告数据包中设置“其他地址配置” (Other Address Configuration) 标志。此标志通知 IPv6 自动配置客户端应使用 DHCPv6 从 DHCPv6 获取其他信息，如 DNS 服务器地址。

步骤 10 配置 **DAD 尝试 (DAD Attempts)** - 接口执行重复地址检测 (DAD) 的频率，介于 0 - 600 之间。默认值为 1。在无状态自动配置过程中，DAD 会验证新单播 IPv6 地址的唯一性，再将地址分配给接口。如果重复地址是接口的链路本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。接口将使用邻居的询求消息来执行重复地址检测。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。

步骤 11 将 MTU (最大传输单位) 更改为所需的值。

默认 MTU 为 1500 字节。您可以指定介于 64 - 9198 (或为 Firepower 威胁防御虚拟指定 9000) 之间的值。如果通常在网络中使用巨帧，请设置一个较大的值。有关详细信息，请参阅[在 Firepower 接口设置中使用 MTU 设置](#)。

Note 如果在 ASA 5500-X 系列设备、ISA 3000 系列设备或 Firepower 威胁防御虚拟上将 MTU 提高到 1500 以上，则必须重新启动设备。登录 CLI 并使用 `reboot` 命令。您无需重启 Firepower 2100 或 Secure Firewall 3100 系列设备，因为在这些设备上会始终启用巨帧支持。

步骤 12 (仅限物理接口)。修改**速度**和**复用**设置。

默认设置为该接口与线路另一端的接口协商最佳复用和速度，但如有必要，您可以强制实施特定的复用或速度。所列的选项仅为接口支持的设置。在网络模块上设置这些选项之前，请阅读[Firepower 接口配置的指南和限制](#)。

- **复用 (Duplex)** - 选择自动、半复用、全复用或默认。当接口支持时，自动为默认值。例如，您不能为 Firepower 2100 或 Secure Firewall 3100 系列设备上的 SFP 接口选择“自动” (Auto)。选择默认表示 Firepower 设备管理器不应尝试配置设置。

任何现有配置将保持不变。

- **速度 (Speed)** - 选择自动可使接口协商速度 (默认值) 或选取特定速度：10 Mbps、100 Mbps、1000 Mbps、10000 Mbps。此外，您还可以选择以下特殊选项：

任何现有配置将保持不变。

接口类型限制了您可以选择的选项。例如，Firepower 2100 系列设备上的 SFP+ 接口仅支持 1000 (1 Gbps) 和 10000 (10 Gbps)，SFP 接口仅支持 1000 (1 Gbps)，而千兆以太网端口不支持 10000 (10 Gbps)。其他设备上的 SPF 接口可能需要设置“不协商”(No Negotiate)。有关接口所支持的选项的信息，请参阅硬件文档。

步骤 13 (可选，建议为子接口和高可用性设备配置。) 配置 MAC 地址。

MAC 地址 (MAC Address) - 采用 H.H.H 格式的介质访问控制，其中 H 是 16 位十六进制数字。例如，您可以将 MAC 地址 00-0C-F1-42-4C-DE 输入为 000C.F142.4CDE。MAC 地址不能设置组播位，即左起第二个十六进制数字不能是奇数。

备用 MAC 地址 (Standby MAC Address) - 用于高可用性。如果主用设备发生故障切换，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

步骤 14 点击创建。

配置网桥组

网桥组是将一个或多个接口分组的虚拟接口。对接口分组的主要原因是创建一组交换接口。如此，就可以将工作站或其他终端设备直接连接到网桥组中所包含的接口。您不需要通过单独的物理交换机来连接这些设备，尽管您也可以将一台交换机连接到某个网桥组成员。

组成员没有 IP 地址。相反，所有成员接口共用桥接虚拟接口 (BVI) 的 IP 地址。如果在 BVI 上启用 IPv6，系统会自动为成员接口分配唯一的链路本地地址。

通常会在网桥组接口 (BVI) 上配置 DHCP 服务器，为通过成员接口连接的任何终端提供 IP 地址。不过，如果愿意的话，您也可以在连接到成员接口的终端上配置静态地址。网桥组中的所有终端都必须具有与网桥组 IP 地址位于同一子网的 IP 地址。



Note ISA 3000 设备预配置了名为 **inside** 的桥接组，其中包括除 **outside** 接口以外的所有数据接口。因此，设备已经预配置了一个端口用于连接到互联网或其他上游网络，而所有其他端口已启用并可用于直接连接终端。如果要将某个内部接口用于新的子网，必须先从 BVI 删除所需接口。

FDM 管理设备仅支持一个网桥组；因此，思科防御协调器只能管理该网桥组，而无法在设备上创建其他网桥组。

在 CDO 上创建网桥组后，在将配置部署到 FDM 管理设备之前，您将不知道网桥组 ID。FDM 管理会分配网桥组 ID，例如 BVI1。如果删除了接口并创建了新的桥接组，则新桥接组的编号会递增，例如 BVI2。

准备工作

指定将成为网桥组 **成员** 的接口。具体而言，每个 **成员** 接口都必须满足以下要求：

- 该接口必须具有名称。

- 接口不能配置为**管理专用**接口。
- 该接口无法被配置为被动模式。
- 接口不能是 EtherChannel 接口或 EtherChannel 子接口。
- 该接口不能有任何已定义的 IPv4 或 IPv6 地址，无论是静态分配的还是通过 DHCP 获得的。如果需从当前正在使用的某个接口删除地址，则可能还需要删除该接口的其他配置，例如静态路由、DHCP 服务器或 NAT 规则，具体视具有地址的接口而定。如果您尝试将具有 IP 地址的接口添加到网桥组，CDO 将向您发出警告。如果继续将接口添加到网桥组，CDO 将从接口配置中删除 IP 地址。
- BVI 可以将 VLAN 接口或其他路由接口作为成员接口，但不能将两个接口作为单个 BVI 上的成员接口。
- 接口不能是以太网的点对点协议 (PPPoE)
- 接口不能与安全区域关联（如果它在区域中）。您必须删除该接口的所有 NAT 规则，然后才能将其添加到网桥组。
- 单独启用和禁用成员接口。这样就可以禁用任何未使用的接口，而无需将其从网桥组删除。网桥组本身始终处于启用状态。
- 集群中不支持网桥组。



Note 在路由模式的 Firepower 2100 设备上，或在具有桥接 ixgbevfc 接口的 VMware 上，网桥组不受支持。

配置桥接组接口的名称并选择桥接组成员

在此程序中，您将为网桥组接口 (BVI) 指定名称，并选择要添加到网桥组的接口：


Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击**FTD** 选项卡，然后选择要为其创建网桥组的设备。

步骤 4 执行以下操作之一：

- 选择 BVI 网桥组，然后在“操作” (Actions) 窗格中点击**编辑 (Edit)**。
- 点击加号按钮 ，然后选择网桥组接口。

Note 您可以创建并配置一个网桥组。如果已经定义了一个网桥组，则应编辑该组而非尝试创建新组。如果需要创建新的网桥组，则必须先删除现有网桥组。

步骤 5 进行以下配置：

- **逻辑名称 (Logical Name)** - 必须为网桥组指定名称。最多可以包含 48 个字符。字母字符必须为小写。例如 inside 或 outside。如果没有名称，将忽略其余的接口配置。

Note 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

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

步骤 6 点击网桥组成员 (**Bridge Group Member**) 选项卡。一个网桥组最多可以包含 64 个接口或子接口。

- 选中接口以将其添加到网桥组。
- 取消选中要从网桥组中删除的接口。

步骤 7 点击保存 (**Save**)。

BVI 现在具有名称和成员接口。继续执行以下任务以配置网桥组接口。您不会为成员接口本身执行以下任务：

- 如果要为 BVI 分配 IPv4 地址，请为 [BVI 配置 IPv4 地址](#)。
- 如果要为 BVI 分配 IPv6 地址，请为 [BVI 配置 IPv6 地址](#)。
- 为网桥组接口 [配置高级接口选项](#)。

为 BVI 配置 IPv4 地址

Procedure

步骤 1 选择要为其创建网桥组的设备。

步骤 2 在接口列表中选择 BVI，然后点击操作窗格中的 **编辑 (Edit)**。

步骤 3 点击“IPv4 地址” (IPv4 Address) 选项卡以配置 IPv4 地址。

步骤 4 从类型字段中选择以下任一选项：

- **静态 (Static)** - 如果希望分配固定的地址，请选择此选项。键入网桥组的 IP 地址和子网掩码。所有连接的终端都将位于此网络中。对于预配置了网桥组的型号而言，BVI “inside” 网络的默认值为 192.168.1.1/24（如 255.255.255.0）。确保该地址尚未在网络中使用。

如果您配置了高可用性，并要监控此接口的高可用性，则还要在同一子网上配置一个备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

Note 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。请参阅配置 DHCP 服务器。

- **动态 (DHCP) (Dynamic [DHCP])** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。网桥组通常不会使用此选项，但是您可以根据需要如此配置。如果您配置高可用性，将不能使用此选项。如有需要，更改以下选项：
 - “路由指标” (Route Metric) - 如果从 DHCP 服务器获取默认路由，则此选项是指与获知路由的管理距离，其值介于 1 到 255 之间。默认值为 1。
 - “获取默认路由” (Obtain Default Route) - 选中此选项以便从 DHCP 服务器获取默认路由。您通常会选择此选项，该选项是默认值。

步骤 5 继续执行以下程序之一：

- 如果要为 BVI 分配 IPv4 地址，请为 [BVI 配置 IPv6 地址](#)。
- 配置高级接口选项。
- 点击 **保存 (Save)** 并将更改部署到 Firepower 设备。有关详细信息，请参阅 [将配置更改从 CDO 部署到 FDM 管理设备](#)。

为 BVI 配置 IPv6 地址

Procedure

步骤 1 点击“IPv6 地址” (IPv6 Address) 选项卡，然后为 BVI 配置 IPv6 地址。

步骤 2 配置 IPv6 地址的以下选项：

步骤 3 启用 **IPv6 处理 (Enable IPv6 processing)** - 在不想配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请将状态滑块滑至蓝色。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

Note 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

步骤 4 抑制 **RA (Suppress RA)** - 是否抑制路由器通告。Firepower 威胁防御设备可参与路由器通告，以便相邻设备可动态获知默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

也会发送路由器通告，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

对于不希望 FTD 设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

步骤 5 **静态地址/前缀 (Static Address/Prefix)** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅“IPv6 地址”。

步骤 6 备用 IP 地址 (Standby IP Address) - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

步骤 7 继续执行以下程序之一：

- 配置高级接口选项。
- 点击**保存 (Save)** 并将更改部署到 Firepower 设备。有关详细信息，请参阅[将配置更改从 CDO 部署到 FDM 管理设备](#)。

配置高级接口选项

请对网桥组 **成员** 接口配置大多数高级选项，不过其中一些选项可用于网桥组接口本身。

Procedure

步骤 1 高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。

步骤 2 点击**确定 (OK)**。

步骤 3 点击**保存 (Save)** 并将更改部署到 Firepower 设备。有关详细信息，请参阅[将配置更改从 CDO 部署到 FDM 管理设备](#)。

What to do next

- 确保已启用您打算使用的所有成员接口。
- 为网桥组配置 DHCP 服务器。请参阅[配置 DHCP 服务器](#)。
- 将成员接口添加到相应的安全区。
- 确保各项策略（例如身份、NAT 和访问策略）可为网桥组和成员接口提供所需的服务。

FDM 管理配置中的网桥组兼容性

在各种配置中，您可以指定接口，有时您将能够指定网桥虚拟接口 (BVI)，而有时您将能够指定网桥组的成员。此表阐述了何时可以使用 BVI，以及何时可以使用成员接口。

Firepower 威胁防御配置类型	可以使用 BVI	可以使用 BVI 成员
DHCP 服务器	是	否
DNS 服务器	是	是
管理访问	是	否
NAT (网络地址转换)	不支持	是

Firepower 威胁防御配置类型	可以使用 BVI	可以使用 BVI 成员
安全区	不支持	是
站点间 VPN 接入点	不支持	是
系统日志服务器	是	否

删除网桥组

删除网桥组时，其成员将变成标准路由接口，并且所有 NAT 规则或安全区成员身份保持不变。可以编辑这些接口为其提供 IP 地址。如果需要创建新的网桥组，则必须先删除现有网桥组。

Procedure

- 步骤 1 在导航窗格中，点击**设备和服务 (Devices & Services)**。
- 步骤 2 点击**设备**选项卡。
- 步骤 3 点击**FTD**选项卡，然后选择要从中删除网桥组的设备。
- 步骤 4 选择 BVI 网桥组，然后在“操作”(Actions)窗格中点击**删除 (Remove)**。
- 步骤 5 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

为 FDM 管理设备添加 EtherChannel 接口

EtherChannel 接口限制

根据设备型号，EtherChannel 可以包含多个同一介质类型和容量的成员接口，并且必须设置为相同的速度和双工模式。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。链路汇聚控制协议 (LACP) 将在两个网络设备之间交换链路汇聚控制协议数据单元 (LACPDU)，进而汇聚接口。

根据物理配置和软件版本，EtherChannel 接口存在诸多限制。有关详细信息，请参阅以下部分。

一般接口限制

- EtherChannel 仅在运行 FDM 管理 版本 6.5 及更高版本的设备上可用。
- 思科防御协调器 支持以下 Firepower 设备上的 EtherChannel 接口配置：1010、1120、1140、1150、2110、2120、2130、2140、3110、3120、3130 和 3140。有关每个设备型号的接口限制，请参阅[设备特定限制](#)。
- 通道组中的所有接口都必须具有相同的介质类型和容量，并且必须设置为相同的速度和双工模式。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。
- EtherChannel 连接到的设备还必须支持 802.3ad EtherChannel。

- FDM 管理设备不支持带有 VLAN 标记的 LACPDU。如果使用 Cisco IOS `vlan dot1Q tag native` 命令在相邻交换机上启用本地 VLAN 标记，则 FDM 管理设备将会丢弃已标记的 LACPDU。请务必禁用相邻交换机上的本地 VLAN 标记。
- 所有 FDM 管理设备配置均引用 EtherChannel 接口，而不是成员物理接口。
- 端口通道接口会被显示为物理接口。

设备特定限制

以下设备具有特定的接口限制：

1000 系列

- Firepower 1010 最多支持 8 个 EtherChannel 接口。
- Firepower 1120、1140、1150 最多支持 12 个 EtherChannel 接口。
- 1000 系列不支持 LACP 快速速率；LACP 始终使用正常速率。此设置不可配置。

2100 系列

- Firepower 2110 和 2120 型号最多支持 12 个 EtherChannel 接口。
- Firepower 2130 和 2140 型号最多支持 16 个 EtherChannel 接口。
- 2100 系列不支持 LACP 快速速率；LACP 始终使用正常速率。此设置不可配置。

Secure Firewall 3100 系列

- 所有 Secure Firewall 3100 型号最多支持 16 个 EtherChannel 接口。
- Secure Firewall 3100 型号支持 LACP 快速速率。
- Secure Firewall 3100 系列型号不支持启用或禁用网络模块，以及接口的分支在线插入和删除 (OIR)。

4100 系列和 9300 系列

- 您无法在 4100 和 9300 系列上创建或配置 EtherChannel。必须在 FXOS 机箱中配置这些设备的 Etherchannel。
- 4100 和 9300 系列上的以太网通道会在 思科防御协调器 中显示为物理接口。

添加 EtherChannel 接口

使用以下程序将 EtherChannel 添加到 FDM 托管设备：



Note 如果要立即创建另一个 EtherChannel，请选中创建另一个 (**Create another**) 复选框，然后点击创建 (**Create**)。

Procedure

- 步骤 1 在导航窗格中，点击清单 (Inventory)。
- 步骤 2 点击设备选项卡。
- 步骤 3 点击 FTD 选项卡，然后选择要将 Etherchannel 添加到的设备。
- 步骤 4 在右侧的管理 (Management) 窗格中，点击接口 (Interfaces)。
- 步骤 5 点击蓝色加号按钮 ，然后选择 EtherChannel。
- 步骤 6 (可选) 输入逻辑名称 (Logical Name)。
- 步骤 7 (可选) 输入说明。
- 步骤 8 输入 EtherChannel ID。

对于 Firepower 1010 系列，请输入一个介于 1 和 8 之间的值。

对于 Firepower 2100、3100、4100 和 9300 系列，请输入一个介于 1 和 48 之间的值。

- 步骤 9 点击链路汇聚控制协议 (Link Aggregation Control Protocol) 的下拉按钮，然后选择以下两个选项之一：
 - **Active (活动)** - 发送和接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。
 - **开 (On)** - EtherChannel 始终开启，并且不使用 LACP。开启的 EtherChannel 只能与另一个开启的 EtherChannel 建立连接。
- 步骤 10 搜索并选择要作为成员包含在 EtherChannel 中的接口。您必须包含至少一个接口。

警告：如果您将 EtherChannel 接口添加为成员，并且该接口已配置了 IP 地址，则 CDO 会删除该成员的 IP 地址。
- 步骤 11 点击创建。

相关信息：

- [编辑或删除 FDM 管理 设备的 EtherChannel 接口](#)
- [将子接口添加到 EtherChannel 接口](#)
- [从 EtherChannel 编辑或删除子接口](#)
- [Firepower 接口配置的指南和限制](#)
- [将 FDM 管理设备接口分配给安全区域](#)
- [为 FDM 管理 设备添加 EtherChannel 接口, on page 25](#)

编辑或删除 FDM 管理 设备的 EtherChannel 接口

使用以下程序修改现有 EtherChannel 接口，或从 FDM 管理 设备中删除 EtherChannel 接口。

编辑 EtherChannel

请注意，EtherChannel 有几个限制，您在修改时必须加以注意。有关详细信息，请参阅[EtherChannel](#)。



Note EtherChannel 必须至少有一个成员。

使用以下程序可编辑现有 EtherChannel：


Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击**FTD**选项卡，然后选择与要修改的 Etherchannel 关联的威胁防御。

步骤 4 在右侧的**管理 (Management)**窗格中，点击**接口 (Interfaces)**。

步骤 5 在**接口 (Interfaces)**页面上，选择要编辑的 EtherChannel 接口。在位于右侧的“操作” (Actions) 窗格中，点击编辑图标 。

步骤 6 修改以下任何项目：

- 逻辑名称。
- 州/省/自治区。
- 说明。
- 安全区域分配。
- 链路汇聚控制协议状态。
- **IPv4**、**IPv6** 或**高级 (Advanced)**选项卡中的 IP 地址配置。
- EtherChannel 成员。

Warning **警告：**如果您将 EtherChannel 接口添加为成员，并且该接口已配置了 IP 地址，则 CDO 会删除该成员的 IP 地址。

步骤 7 点击**保存 (Save)**。

删除 ASA EtherChannel 接口



Note 与高可用性 (HA) 或任何其他配置关联的 EtherChannel 接口。您必须先从所有配置中手动删除 EtherChannel 接口，然后再将其从 CDO 中删除。

使用以下程序从 FDM 管理设备中删除 EtherChannel 接口：

Procedure

- 步骤 1 在导航窗格中，点击清单 (**Inventory**)。
- 步骤 2 点击设备选项卡。
- 步骤 3 点击 **FTD** 选项卡以及与要删除的 Etherchannel 关联的威胁防御。
- 步骤 4 在右侧的管理 (**Management**) 窗格中，点击接口 (**Interfaces**)。
- 步骤 5 在接口 (**Interfaces**) 页面上，选择要编辑的 EtherChannel 接口。在右侧的“操作” (**Actions**) 窗格中，点击删除 (**Remove**)。
- 步骤 6 确认要删除 EtherChannel 接口，然后点击确定 (**OK**)。

将子接口添加到 EtherChannel 接口

EtherChannel 子接口

通过接口 (**Interfaces**) 页面，您可以通过展开每个接口来查看设备的哪些接口具有子接口。这个展开的视图还会显示子接口的唯一逻辑名称、启用/禁用状态、任何关联的安全区域和模式。子接口的接口类型和模式由父接口确定。

一般限制

CDO 不支持以下接口类型的子接口：

- 配置为仅用于管理的接口。
- 为交换机端口模式配置的接口。
- 被动接口。
- VLAN 接口。
- 网桥虚拟接口 (BVI)。
- 已经是另一个 EtherChannel 接口的成员的接口。

您可以为以下对象创建子接口：

- 网桥组成员。
- EtherChannel 接口。
- 物理接口。

将子接口添加到 EtherChannel 接口

使用以下程序将子接口添加到现有接口：



Note 如果要立即创建另一个子接口，请选中创建另一个 (**Create another**) 复选框，然后点击创建 (**Create**)。

Procedure

- 步骤 1 在导航窗格中，点击清单 (**Inventory**)。
- 步骤 2 点击设备选项卡。
- 步骤 3 点击 **FTD** 选项卡，然后选择要将 Etherchannel 添加到的威胁防御。在右侧的“管理” (**Management**) 窗格中，点击接口 (**Interfaces**)。
- 步骤 4 选择要为其分组子接口的接口。在位于右侧的“操作” (**Action**) 窗格中，点击 **+ New Subinterface** 按钮。
- 步骤 5 (可选) 输入逻辑名称 (**Logical Name**)。
- 步骤 6 (可选) 输入说明。
- 步骤 7 (可选) 为子接口分配安全区域。请注意，如果子接口没有逻辑名称，则您无法分配安全区域。
- 步骤 8 输入 VLAN ID。
- 步骤 9 输入 **EtherChannel ID**。使用 1 到 48 之间的值；对于 Firepower 1010 系列，请使用 1 到 8 之间的值。
- 步骤 10 选择 **IPv4**、**IPv6** 或高级 (**Advanced**) 选项卡以配置子接口的 IP 地址。
- 步骤 11 点击创建。

从 EtherChannel 编辑或删除子接口

使用以下程序修改现有子接口，或从 Etherchannel 接口删除子接口。



Note 子接口和 EtherChannel 接口具有一系列可能会影响配置的准则和限制。有关详细信息，请参阅[一般限制](#)。

编辑子接口


使用以下程序编辑与 EtherChannel 接口关联的现有子接口：

Procedure

- 步骤 1 登录 CDO。
- 步骤 2 在导航窗格中，点击清单 (**Inventory**)。
- 步骤 3 点击设备选项卡。
- 步骤 4 点击 **FTD** 选项卡，然后选择与要编辑的 EtherChannel 和子接口关联的威胁防御。

步骤 5 在右侧的**管理 (Management)** 窗格中，点击**接口 (Interfaces)**。

步骤 6 找到并展开子接口所属的 Etherchannel 接口。

步骤 7 选择要编辑的子接口。在位于右侧的“**操作 (Action)**”窗格中，点击编辑图标 。

步骤 8 修改以下任何项目：

- 逻辑名称。
- 州/省/自治区。
- 说明。
- 安全区域分配。
- VLAN ID
- IPv4、IPv6 或高级 (Advanced) 选项卡中的 IP 地址配置。

步骤 9 点击**保存 (Save)**。

从 EtherChannel 中删除子接口

使用以下程序从 EtherChannel 接口删除现有子接口：

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击**FTD** 选项卡，然后选择与要编辑的 EtherChannel 和子接口关联的 威胁防御。在右侧的“**管理 (Management)**”窗格中，点击**接口 (Interfaces)**。

步骤 4 找到并展开子接口所属的 Etherchannel 接口。

步骤 5 选择要删除的子接口。

步骤 6 在右侧的“**操作 (Actions)**”窗格中，点击**删除 (Remove)**。

步骤 7 确认要删除子接口，然后点击**确定 (OK)**。

将接口添加到虚拟 FDM 管理设备

在部署虚拟 FDM 管理设备时，可以将接口分配给虚拟机。然后，在 FDM 管理设备中，使用与配置硬件设备相同的方法配置这些接口。

但是，您无法给虚拟机添加更多虚拟接口，然后让 FDM 来自动识别它们。如果您需要为虚拟 FDM 管理设备配置更多物理接口对等体，那基本上需要重新执行该流程。您可以部署新的虚拟机，也可以使用以下程序。



Caution 要给虚拟机添加接口，您需要完全清除虚拟 FDM 管理配置。配置中唯一保留不变的部分是管理地址和网关设置。

准备工作

在 FDM 管理设备中执行以下操作：

- 检查虚拟 FDM 管理设备配置并记下要在新虚拟机中复制的设置。
- 选择设备 (**Devices**) > 智能许可证 (**Smart License**) > 查看配置 (**View Configuration**) 并禁用所有功能许可证。

Procedure

步骤 1 关闭虚拟 FDM 管理设备。

步骤 2 使用虚拟机软件，将接口添加到虚拟 FDM 管理设备。对于 VMware，默认情况下，虚拟设备使用 e1000（1 千兆位/秒）接口。您还可以使用 vmxnet3 或 ixgbe（10 千兆位/秒）接口

步骤 3 打开虚拟 FDM 管理设备电源。

步骤 4 打开虚拟 FDM 管理设备控制台，删除本地管理器，然后启用本地管理器。删除本地管理器，然后启用本地管理器，重置设备配置，并让系统识别新接口。管理接口配置不会重置。以下 SSH 会话会显示相应命令。

```
> show managers
Managed locally.
> configure manager delete
If you enabled any feature licenses, you must disable them in Firepower Device Manager
before deleting the local manager. Otherwise, those licenses remain assigned to the device
in Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
DCHP Server Disabled
> show managers
No managers configured.
> configure manager local
>
```

步骤 5 打开浏览器并连接到 FDM 管理设备，完成设备安装向导，并配置设备。有关详细说明，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南，版本 xxx》指南中的“完成初始配置”部分。

FDM 管理 设备的交换机端口模式接口

对于各物理 Firepower 1010 接口，可以将其操作设置为防火墙接口或交换机端口。交换机端口使用硬件中的交换功能在第 2 层转发流量。同一 VLAN 上的交换机端口可使用硬件交换互相通信，且流量不受 FDM 管理设备安全策略的限制。接入端口仅接受未标记流量，可以将其分配给单个 VLAN。中继端口接受未标记和已标记流量，且可以属于多个 VLAN。对于已重新映像到版本 6.4 的设备，以太网 1/2 至 1/8 配置为 VLAN 1 上的接入交换机端口；手动升级到版本 6.4（及更高版本）的设备，

以太网配置会在升级之前保留配置。请注意，同一 VLAN 上的交换机端口可使用硬件交换互相通信，且流量不受 FDM 管理 设备安全策略的限制。

访问或中继

配置为交换机端口的物理接口可以分配为接入端口或中继端口。

接入端口仅将流量转发到一个 VLAN，并且仅接受未标记的流量。如果您打算将流量转发到单个主机或设备，我们强烈建议使用此选项。您还必须指定要与接口关联的 VLAN，否则将默认为 VLAN 1。

中继端口将流量转发到多个 VLAN。您必须分配一个 VLAN 接口作为本地中继端口，并至少分配一个 VLAN 作为关联中继端口。最多可以选择 20 个接口与交换机端口接口关联，这使来自不同 VLAN ID 的流量能够通过交换机端口接口。如果未标记流量通过交换机端口，则使用本征 VLAN 接口的 VLAN ID 标记流量。请注意，1002 和 1005 之间的默认光纤分布式数据接口 (FDDI) 和令牌环 ID 不能用于 VLAN ID。

更改端口模式

如果选择为路由模式配置的接口作为 VLAN 成员，CDO 会自动将该接口转换为交换机端口模式，并将该接口默认配置为接入端口。因此，逻辑名称和关联的静态 IP 地址将从接口中删除。

配置限制

请注意以下限制：

- 只有物理 Firepower 1010 设备支持交换机端口模式配置。虚拟 FDM 管理 设备不支持交换机端口模式。
- Firepower 1010 设备最多允许 60 个 VLAN。
- 为交换机端口模式配置的 VLAN 接口必须是未命名的。这意味着 MTU 必须被配置为 1500 字节。
- 您 **不能** 将配置为交换机端口模式的接口删除。您必须手动将接口模式从交换机端口模式更改为已路由模式。
- 为交换机端口模式配置的接口不支持 IP 地址。如果接口当前已在 VPN、DHCP 中引用或配置，或者已与静态路由关联，则 **必须** 手动删除 IP 地址。
- 不能将桥接组接口的任何成员用作交换机端口。
- VLAN 接口的 MTU 必须为 1500 字节。未命名的 VLAN 接口不支持任何其他配置。
- 交换机端口模式不支持以下选项：
 - 诊断接口。
 - 动态、组播、等价多路径 (ECMP) 路由。
 - 被动接口。
 - 端口 etherchannel，或使用作为 etherchannel 成员的接口。

- 子接口。
- 故障切换和状态链路。

高可用性和交换机端口接口

使用高可用性时，不应使用交换机端口功能。由于交换机端口在硬件中运行，因此它们会继续在主用和备用设备上传递流量。高可用性旨在防止流量通过备用设备，但此功能不会扩展到交换机端口。在正常高可用性网络设置中，两台设备上的活动交换机端口将导致网络环路。建议将外部交换机用于任何交换功能。请注意，VLAN 接口可通过故障转移监控，而交换机端口无法通过故障转移监控。



Note 仅可使用防火墙接口作为故障切换链路。

模板中的交换机端口模式配置

您可以使用为交换机端口模式配置的接口创建设备模板。将接口从模板映射到设备时，请注意以下情况：

- 如果模板接口在应用模板之前不包含任何 VLAN 成员，则 CDO 会自动将其映射到具有相同属性的可用设备接口。
- 如果不包含 VLAN 成员的模板接口映射到配置为 N/A 的设备接口，则 CDO 会自动在要应用模板的设备上创建接口
- 如果包含 VLAN 成员的模板接口映射到不存在的设备接口，则应用模板将失败。
- 模板不支持将多个模板接口映射到同一设备接口。
- 模板的管理接口必须映射到设备的管理接口。

配置 FDM 管理设备 VLAN


如果要配置子接口或交换机端口，您必须先配置 VLAN 接口。



Note 一个 FDM 管理设备最多支持 60 个 VLAN 接口。

Procedure

- 步骤 1** 在导航窗格中，点击**清单 (Inventory)**。
- 步骤 2** 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
- 步骤 3** 点击**FTD** 选项卡，然后选择要在其上创建 VLAN 的所需设备。
- 步骤 4** 在右侧的**管理 (Management)** 窗格中，点击**接口 (Interfaces)**。

步骤 5 在接口 (**Interfaces**) 页面上, 点击  按钮。

步骤 6 进行以下配置:

- **父接口 (Parent Interface)** - 父接口是将子接口添加至其中的物理接口。创建子接口后, 父接口则无法更改。
- (可选) **逻辑名称 (Logical Name)** - 设置 VLAN 名称, 最多 48 个字符。字母字符必须为小写。如果不希望在 VLAN 和其他 VLAN 或防火墙接口之间进行路由, 则将 VLAN 接口名称留空。

Note 如果未输入名称, 则必须将**高级选项 (Advanced Options)**中的 MTU 设为 1500。如果将 MTU 更改为 1500 以外的值, 则不得为 VLAN 命名。

- (可选) **说明 (Description)** - 说明最多为 200 个字符, 单行, 不能使用回车。
- (可选) **安全区域 (Security Zone)** - 将子接口分配给安全区域。请注意, 如果子接口没有逻辑名称, 则您无法分配该子接口。您还可以在创建子接口后分配安全区域。有关详细信息, 请参阅在 [Firepower 接口设置中使用安全区域](#)。
- (可选) **VLAN ID** - 输入 VLAN ID, 介于 1 和 4070 之间, 用于标记该子接口上的数据包。

Note 默认情况下会路由 VLAN 接口。如果将此 VLAN 接口添加至网桥组, 则思科防御协调器 (CDO) 会将模式自动更改为 **BridgeGroupMember**。同样, 如果将此 VLAN 接口更改为交换机端口模式, 则 CDO 会自动将模式更改为 **交换机端口 (Switch Port)**。

- (可选) **子接口 ID (Subinterface ID)** - 以整数形式输入介于 1 和 4294967295 之间的子接口 ID。此 ID 附加至接口 ID; 例如 Ethernet1/1.100。方便起见, 您可以匹配 VLAN ID, 但这不是必需的。创建子接口后, 则无法更改该 ID。

步骤 7 点击 **IPv4 地址 (IPv4 Address)** 选项卡, 然后从类型字段中选择以下选项之一:

- **静态 (Static)** - 如果希望分配固定的地址, 请选择此选项。对于连接到接口的网络, 键入接口的 IP 地址和子网掩码。例如, 如果您连接的是 10.100.10.0/24 网络, 则可以输入 10.100.10.1/24。确保该地址尚未在网络中使用。

如果您配置了高可用性, 并要监控此接口的高可用性, 则还要在同一子网上配置一个备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址, 则主用设备无法使用网络测试监控备用接口, 只能跟踪链路状态。

Note 如果为接口配置了 DHCP 服务器, 您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网, 必须先删除 DHCP 服务器或在新子网上配置地址池, 才能保存接口更改。有关详细信息, 请参阅[配置 DHCP 服务器](#)。

- **动态 (DHCP) (Dynamic [DHCP])** - 如果应从网络中的 DHCP 服务器获取地址, 请选择此选项。如果您配置高可用性, 将不能使用此选项。如有需要, 更改以下选项:
 - **路由指标 (Route Metric)** - 如果从 DHCP 服务器获取默认路由, 则此选项是指与获知路由的管理距离, 其值介于 1 到 255 之间。默认值为 1。
 - **获取默认路由 (Obtain Default Route)** - 选中此选项以便从 DHCP 服务器获取默认路由。您通常会选择此选项, 该选项是默认值。

- **DHCP 地址池 (DHCP Address Pool)** - 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。

步骤 8 (可选) 点击 **IPv6 地址 (IPv6 Address)** 选项卡并配置以下内容：

- **状态 (State)** - 在不想配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请将状态滑块滑至蓝色。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

Note 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **地址自动配置 (Address Auto Configuration)** - 选中此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。
- **抑制 RA (Suppress RA)** - 是否抑制路由器通告。威胁防御 可以参与路由器通告，以便邻居设备可以动态获悉默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

也会发送路由器通告，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

对于不希望 FDM 管理设备提供 IPv6 前缀的任何接口（例如外部接口），我们建议抑制接口上的这些消息。

- **静态地址/前缀 (Static Address/Prefix)** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅 [Firepower 接口的 IPv6 寻址](#)。
- **备用 IP 地址 (Standby IP Address)** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

步骤 9 (可选) 点击 **高级 (Advanced)** 选项卡。

- 如果您想让系统在决定是否故障切换到高可用性配置中的对等设备时考虑接口的运行状况，请选择 **启用高可用性监控**。

如果不配置高可用性，可忽略此选项。如果不配置接口的名称，也可以忽略此选项。

- 选择 **仅管理 (Management Only)** 以便将数据接口仅用于管理。

仅管理接口不允许直通流量，所以将数据接口设置为仅管理的价值微乎其微。不能更改管理/诊断接口的此项设置，它们始终为仅管理。

- 修改 IPv6 配置设置。
 - **启用 DHCP 以获取 IPv6 地址配置 (Enable DHCP for IPv6 address configuration)** - 是否在 IPv6 路由器通告数据包中设置“托管地址配置”标志。此标志通知 IPv6 自动配置客户端应使用 DHCPv6 来获取相关地址以及派生的无状态自动配置地址。

- 启用 **DHCP** 以获取 **IPv6 非地址配置 (Enable DHCP for IPv6 non-address configuration)** - 是否在 IPv6 路由器通告数据包中设置“其他地址配置”标志。此标志通知 IPv6 自动配置客户端应使用 DHCPv6 从 DHCPv6 获取其他信息，如 DNS 服务器地址。
- **DAD 尝试 (DAD Attempts)** - 接口执行重复地址检测 (DAD) 的频率，介于 0 - 600 之间。默认值为 1。在无状态自动配置过程中，DAD 会验证新单播 IPv6 地址的唯一性，再将地址分配给接口。如果重复地址是接口的链路本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。接口将使用邻居的询问消息来执行重复地址检测。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。
- 将 **MTU** (最大传输单位) 更改为所需的值。

默认 MTU 为 1500 字节。您可以指定介于 64 - 9198 (或为虚拟 FDM 管理 设备指定 9000，并为 Firepower 4100/9300 指定 9184) 之间的值。如果通常在网络中使用巨帧，请设置一个较大的值。

Note 如果在 ASA 5500-X 系列设备、ISA 3000 系列设备或虚拟 FDM 管理 设备上将 MTU 提高到 1500 以上，则必须重命名 VLAN 并重新启动设备。登录 CLI 并使用 `reboot` 命令。如果设备已为 HA，还须重新启动备用设备。无需重新启动 Firepower 型号，因为巨帧支持在该型号上始终启用。

- (对于子接口和 HA 对为可选) 配置 **MAC 地址 (MAC address)**。

默认情况下，系统对接口使用预烧到网络接口卡 (NIC) 的 MAC 地址。因此，该接口上的所有子接口都使用相同的 MAC 地址，也因此您可能想要为每个子接口创建唯一地址。如果您配置高可用性，建议手动配置主用/备用 MAC 地址。定义 MAC 地址有助于在故障转移时保持网络中的一致性。

- **MAC 地址 (MAC Address)** - 采用 H.H.H 格式的介质访问控制，其中 H 是 16 位十六进制数字。例如，您可以将 MAC 地址 00-0C-F1-42-4C-DE 输入为 000C.F142.4CDE。MAC 地址不能设置组播位，即左起第二个十六进制数字不能是奇数。
- **备用 MAC 地址 (Standby MAC Address)** - 用于 HA 对。如果主用设备发生故障切换，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

步骤 10 如果要为此设备创建另一个子接口，请在完成子接口配置之前选中 **创建另一个 (Create another)**。

步骤 11 (可选) 将弹出窗口右上角的状态滑块从灰色切换为蓝色，以便在创建时激活子接口。

步骤 12 点击 **确定 (OK)**。

步骤 13 立即 [预览和部署所有设备的配置更改](#) 您所做的更改，或等待并一次部署多个更改。

为交换机端口模式配置 FDM 管理 设备 VLAN

在配置之前，请务必阅读交换机端口模式的限制；有关详细信息，请参阅 [FDM 管理 设备的交换机端口模式接口](#)。



Note 您可以随时为物理接口分配或编辑 VLAN 成员。请务必在确认新配置后将更改部署到设备。

为交换机端口模式创建 VLAN 接口

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击**FTD** 选项卡，然后选择要为其配置接口的设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击**接口 (Interfaces)**。

步骤 5 在**接口 (Interfaces)** 页面上，点击  按钮并选择**VLAN 接口 (VLAN Interface)**。

步骤 6 查看**VLAN 成员 (VLAN Members)** 选项卡并选择所需的物理接口。

Note 如果您选择添加引用为接入或本地中继配置的 VLAN 接口的成员，则只能选择一个 VLAN 作为成员。引用为关联中继配置的 VLAN 接口的物理接口最多支持 20 个接口作为成员。

步骤 7 配置 VLAN 接口的其余部分，如[配置 FDM 管理设备 VLAN](#) 中所述。

步骤 8 点击**保存 (Save)**。确认要重置 VLAN 配置并为接口重新分配 IP 地址。

步骤 9 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

为交换机端口模式配置现有物理接口


Procedure

步骤 1 在导航窗格中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击**FTD** 选项卡，然后选择要为其配置接口的设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击**接口 (Interfaces)**。

步骤 5 在**接口 (Interfaces)** 页面上，选择要修改的物理接口。在右侧的“**操作 (Actions)**”窗格中，点击编辑图标 。


步骤 6 为交换机端口模式配置的接口不支持逻辑名称。如果接口具有逻辑名称，请将其删除。

步骤 7 找到**模式 (Mode)** 并使用下拉菜单选择**交换机端口 (Switch Port)**。

步骤 8 为交换机端口模式配置物理接口：

- (可选) 选中**受保护端口 (Protected Port)** 复选框以将此交换机端口设置为受保护端口，因此您可以阻止交换机端口与同一 VLAN 上的其他受保护交换机端口进行通信。在以下情况下，您可能想要防止交换机端口相互之间进行通信：主要从其他 VLAN 访问这些交换机端口上的设备；

您不需要允许 VLAN 间访问；由于病毒感染或其他安全漏洞，您想要将设备相互隔离开。例如，如果具有托管 3 台 Web 服务器的 DMZ，则在您将此选项应用于各交换机端口后，则可以将 Web 服务器相互隔离。内部网络和外部网络均可以与这 3 台网络服务器进行通信，反之亦然，但这些网络服务器相互之间无法进行通信。

- 对于使用类型，请选择访问 (**Access**) 或中继 (**Trunk**)。请参阅 [FDM 管理 设备的交换机端口模式接口](#)，以确定所需的端口类型。
 - 如果选择中继 (**Trunk**)，则您必须选择一个 VLAN 接口作为本地中继 (**Native Trunk**) VLAN 以转发未标记流量，并至少选择一个关联 VLAN (**Associated VLAN**) 以转发标记流量。点击  图标以查看现有物理接口。最多可以选择 20 个 VLAN 接口作为关联的 VLAN。
 - 您可以通过点击新建 VLAN (**Create new VLAN**) 来创建被设为访问模式的新 VLAN 接口。

步骤 9 点击保存 (**Save**)。确认要重置 VLAN 配置并为接口重新分配 IP 地址。

步骤 10 立即 [预览和部署所有设备的配置更改](#) 您所做的更改，或等待并一次部署多个更改。

查看和监控 Firepower 接口


要查看 Firepower 接口，请执行以下步骤：

Procedure

步骤 1 在导航窗格中，点击设备和服 务 (**Devices & Services**)。

步骤 2 点击 设备 (**Devices**) 选项卡以查找设备，或点击 模板 (**Templates**) 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后点击要查看其接口的设备。

步骤 4 在右侧的“管理” (**Management**) 窗格中选择接口 (**Interfaces**) 。

步骤 5 在“接口” (**Interfaces**) 表中选择一个接口

- 如果展开接口行，您就会看到子接口信息。
- 在右侧，您将看到详细的接口信息。

在 CLI 中监控接口

您可以通过使用 SSH 连接到设备并运行下面的命令来查看有关接口的一些基本信息、行为和统计信息。

要使用 SSH 轻松连接到设备，请将要监控的 FDM 管理设备作为 SSH 设备载入，然后使用 CDO 中的 `>_` 命令行接口。

- `show interface` 显示接口统计信息和配置信息。此命令有许多关键字，可用于获取所需的信息。使用 ? 作为关键字可查看可用选项。
- `show ipv6 interface` 显示有关接口的 IPv6 配置信息。
- `show bridge-group` 显示有关桥接虚拟接口 (BVI) 的信息，包括成员信息和 IP 地址。
- `show conn` 显示有关当前通过接口建立的连接的信息。
- `show traffic` 显示有关流经每个接口的流量的统计信息。
- `show ipv6 traffic` 显示有关流经设备的 IPv6 流量的统计信息。
- `show dhcpd` 显示有关接口上的 DHCP 使用情况的统计信息和其他信息，特别是有关接口上配置的 DHCP 服务器的信息。

使用 FXOS 同步添加到 Firepower 设备的接口

在 Firepower 4100 系列或 9300 系列设备上，如果使用 Firepower 可扩展操作系统 (FXOS) 机箱管理器将接口添加到 Firepower 设备，则 思科防御协调器 不会识别该配置更改并报告配置冲突。

要在 CDO 中查看新添加的接口，请执行以下程序：

过程

- 步骤 1** 登录至 FDM 管理 设备。
- 步骤 2** 在 FDM 管理 主页中，点击“接口” (Interfaces) 面板中的**查看所有接口 (View All Interfaces)**。
- 步骤 3** 点击**扫描接口 (Scan Interfaces)** 按钮：



- 步骤 4** 等待接口扫描，然后点击**确定 (OK)**。
- 步骤 5** 将更改部署到 FDM 管理 设备。
- 步骤 6** 以管理员或超级管理员身份登录到 CDO。
- 步骤 7** 在导航窗格中，点击**清单 (Inventory)**。
- 步骤 8** 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
- 步骤 9** 点击**FTD** 选项卡，然后选择具有预期新接口配置的设备。
- 步骤 10** 点击**检查更改 (Check for Changes)**，立即将设备上的配置副本与 CDO 上存储的配置副本进行比较。CDO 将检测接口更改，并在设备的**清单 (Inventory)** 页面上报告“检测到冲突” (Conflict Detected) 状态。
- 步骤 11** 点击**查看冲突 (Review Conflict)**，然后接受带外更改，以便解决检测到的冲突。

路由

所谓路由是指通过网络将信息从源发送到目标的活动。在途中通常会经过至少一个中间节点。路由涉及两个基本活动：确定最佳路由路径和通过网络传输数据包。

通过使用 Cisco Defense Orchestrator (CDO)，您可以为 Firepower 威胁防御 (FTD) 设备定义默认路由和其他静态路由。以下主题介绍路由的基本信息以及如何使用 CDO 在 FDM 管理设备上配置静态路由。

- [关于静态路由和默认路由](#)
- [路由表和路由选择](#)
- [为 FDM 管理设备配置静态路由和默认路由](#)
- [监控路由](#)

关于静态路由和默认路由

要将流量路由到非连接的主机或网络，您必须定义到主机或网络的路由。该定义的路由是静态路由。还要考虑配置一个默认路由。所有流量的默认路由（不是通过其他方式路由到默认网络网关），通常是指下一跳路由器。

相关信息：

- [默认路由](#)
- [静态路由](#)

默认路由

如果您不知道通往某个特定网络的路由，最简单的方法是配置一个默认路由，将所有流量都发送到上游路由器，从而依靠该路由器来为您路由流量。默认路由对网关 IP 地址进行标识，FTD 设备会将您没有定义静态路由的 IP 数据包发送到该地址。默认路由是以 0.0.0.0/0 (IPv4) 或 ::/0 (IPv6) 作为目标 IP 地址的静态路由。

静态路由

静态路由是从一个网络到另一个网络的路由，您可以手动定义并输入到路由表中。在以下情况下，您可能希望使用静态路由：

- 您的网络规模小且稳定，可以轻松管理设备之间的手动添加和更改路由。
- 您的网络使用不受支持的路由器发现协议。
- 不希望流量或 CPU 开销与路由协议相关联。

- 在某些情况下，仅使用默认路由并不足够。默认网关可能无法到达目标网络，因此还必须配置更具体的静态路由。例如，如果默认网关在外部，则默认路由无法将直接流量定向到未直接与 FDM 管理设备连接的任何内部网络。
- 您使用的是不支持动态路由协议的功能。

限制:

- CDO 当前不支持在 ASA 或 FDM 管理设备上管理、监控或使用虚拟隧道接口 (VTI) 隧道。已配置 VTI 隧道的设备可以载入 CDO，但它会忽略 VTI 接口。如果安全区域或静态路由引用 VTI，则 CDO 会读取不带 VTI 引用的安全区域和静态路由。即将推出对 VTI 隧道的 CDO 支持。
- FDM 管理在软件版本 7.0 或更高版本上运行的设备允许配置等价多路径 (ECMP) 流量区域。当 FDM 管理设备载入 CDO 时，它可以读取但不能修改全局 VRF 路由中可用的 ECMP 配置，因为它不允许具有相同指标值的同一目标网络的路由。您可以通过 FDM 创建和修改 ECMP 流量区域，然后再将其读入 CDO。有关 ECMP 的详细信息，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南，版本 7.0 或更高版本》的“路由基础知识和静态路由”一章中的“等价多路径 (ECMP) 路由”部分。

路由表和路由选择

如果 NAT 转换 (xlates) 和规则无法确定传出接口，系统将使用路由表来确定数据包的路径。

路由表中的路由包括一个名为“管理距离”的指标，提供相对于既定路由的优先级。如果某个数据包与多个路由条目匹配，则使用距离最短的路由。直连网络（在接口上定义的网络）的距离为 0，因此始终首选使用此网络。静态路由的默认距离为 1，但您可以使用 1-254 之间的任意距离创建默认距离。

标识具体目标的路由优先于默认路由（即目标为 0.0.0.0/0 或 ::/0 的路由）。

如何填充路由表

可以使用静态定义的路由和直连路由来填充 FDM 管理设备路由表。可以通过多种方式来输入相同的路由。当在路由表中放入同一目标的两条路由时，将按如下确定保留在路由表中的路由：

- 如果两个路由具有不同的网络前缀长度（网络掩码），则会将两个路由都视为唯一并输入到路由表中。然后，由数据包转发逻辑确定使用哪一条路由。

例如，假设在路由表中输入了以下路由：

- 192.168.32.0/24
- 192.168.32.0/19

即使 192.168.32.0/24 路由具有更长的网络前缀，但由于两条路由具有不同的前缀长度（子网掩码），因此均会安装在路由表中。这两条路由被视为不同目标，数据包转发逻辑会确定使用哪条路由。

- 如果在路由表中输入了通向同一目的地的多条路径，则与静态路由一起输入的具有更好度量的路由将被输入到路由表中。

度量是与特定路由关联的值，从最高优先到最低优先进行排序。用于确定度量的参数根据路由协议而异。具有最低指标的路径选择作为最佳路径并安装在路由表中。如果有多个度量相等的通向同一目的地的路径，则会在这些等价路径上进行负载均衡。

相关信息：

- [如何制定转发决策](#)

如何制定转发决策

按以下顺序做出转发决策：

- 使用 NAT 转换 (xlate) 和规则来确定出口接口。如果 NAT 规则无法确定传出接口，系统将使用路由表来确定数据包的路径。
- 如果目的不匹配路由表中的条目，则通过为默认路由指定的接口转发数据包。如果尚未配置默认路由，则会丢弃数据包。
- 如果目的匹配路由表中的单个条目，则通过与该路由关联的接口转发数据包。
- 如果目的匹配路由表中的多个条目，则通过与具有较长网络前缀的路由相关联的接口转发数据包。例如，发往 192.168.32.1 的数据包到达在路由表中拥有以下路由的接口：
 - 192.168.32.0/24 网关 10.1.1.2
 - 192.168.32.0/19 网关 10.1.1.3

在这种情况下，发往 192.168.32.1 的数据包直接发送到 10.1.1.2，因为 192.168.32.1 属于 192.168.32.0/24 网络。它也属于路由表中的其他路由，但 192.168.32.0/24 在路由表中的前缀更长（24 位对比 19 位）。在转发数据包时，较长前缀始终优先于较短的前缀。



Note 即便新的相似连接将因路由中的变化而导致不同行为，现有连接也将继续使用其已建立的接口。

为 FDM 管理 设备配置静态路由和默认路由

在 Firepower 威胁防御 (FTD) 设备上定义静态路由，以告知系统从何处发送的数据包不会绑定至直连到系统接口的网络。

考虑创建默认路由。这是网络 0.0.0.0/0 的路由。如果数据包的传出接口无法由现有 NAT 转换、静态 NAT 规则或其他静态路由确定，则此路由为所发送的数据包定义目的。

如果无法使用默认网关到达所有网络，则可能需要其他静态路由。例如，默认路由通常是外部接口上的上游路由器。如果还有其他未直连到设备的内部网络，并且通过默认网关无法访问它们，则需要对每个此类内部网络使用静态路由。

对于直连到系统接口的网络，无法定义静态路由。系统自动创建这些路由。


操作步骤

Procedure


步骤 1 在导航窗格中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击 **设备 (Devices)** 选项卡以查找设备，或点击 **模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 设备，然后选择要定义静态路由的设备。

步骤 4 在左侧的**管理 (Management)** 窗格中，点击  **路由 (Routing)**。

步骤 5 在静态路由页中，执行以下某项操作：

- 要添加新的静态路由，请点击加号按钮 。
- 点击要编辑的路由的编辑图标。

如果不再需要路由，请点击该路由的垃圾桶图标将其删除。

步骤 6 配置路由属性。

- **协议** - 选择路由是用于 IPv4 还是 IPv6 地址。
- **接口 (Interface)** - 选择要通过其发送流量的接口。通过此接口需能够访问网关地址。
- **网关 (Gateway)** - 选择标识网关 IP 地址的主机网络对象至目标网络。流量将发送至此地址。
- **度量 (Metric)** - 路由的管理距离，该值介于 1 和 254 之间。静态路由的默认值为 1。如果接口和网关之间还有其他路由器，请输入跳数作为管理距离。
管理距离是用于比较路由的参数。数字越小，为该路由指定的优先级越高。连接的路由（直连到设备接口的网络）始终优先于静态路由。
- **目标网络 (Destination Network)** - 选择标识目标网络的网络对象，该目标网络包含在此路由中使用网关的主机。
要定义默认路由，请使用预定义的 any-ipv4 或 any-ipv6 网络对象，或创建一个适用于 0.0.0.0/0 (IPv4) 或 ::/0 (IPv6) 网络的对象。

步骤 7 点击**确定 (OK)**。

步骤 8 立即**预览和部署所有设备的配置更改**您所做的更改，或等待并一次部署多个更改。

静态路由示例

有关此示例中使用的地址，请参阅[静态路由网络图](#)。

目标是创建一个静态路由，它允许将流量返回到目的网络 20.30.1.0/24 中位于 20.30.1.2 的主机。

数据包可以通过任何路径到达目标。当网络接收到接口上的数据包时，它会决定将数据包转发到哪里，以获得到达目标的最佳路由。



Note DMZ 没有静态路由，因为它直接连接到接口。

例如，请考虑以下两个到达目标的路由。

路由 1:

Procedure

步骤 1 数据包返回到外部接口 **209.165.201.0/27**，查找 **20.30.1.2**。

步骤 2 我们将数据包定向到使用**内部**接口到达与目标位于同一网络的网关 192.168.1.2。

步骤 3 然后，通过网络的**网关地址** 20.30.1.1 识别目的网络。

步骤 4 IP 地址 20.30.1.2 与 20.30.1.1 位于同一子网。路由器会将数据包转发到交换机，而交换机会将数据包转发到 20.30.1.2。

Interface:Inside Destination_N/W:20.30.1.0/24 Gateway: 192.168.1.2 Metric: 1

路由 2:

Procedure

步骤 1 数据包返回到外部接口 **209.165.201.0/27**，查找 **20.30.1.2**。

步骤 2 我们将数据包定向到使用**内部**接口到达网关 192.168.50.20，该地址距离目标网络有多跳。

步骤 3 然后，通过网络的**网关地址** 20.30.1.1 识别目的网络。

步骤 4 IP 地址 20.30.1.2 与 20.30.1.0 位于同一子网。路由器会将数据包转发到交换机，而交换机会将数据包转发到 20.30.1.2。

Interface:Inside Destination_N/W:20.30.1.0/24 Gateway: 192.168.50.20 Metric: 100

以下是这些路由的完整添加静态路由表。

Interface	IP Type	Destination Networks	Gateway IP	Metric
inside	IPv4	20.30.1.1 20.30.1.1/32	192.168.1.2 192.168.1.2	1
internal	IPv4	10.20.2.1 10.20.2.1/32	192.168.50.20 192.168.50.20	100

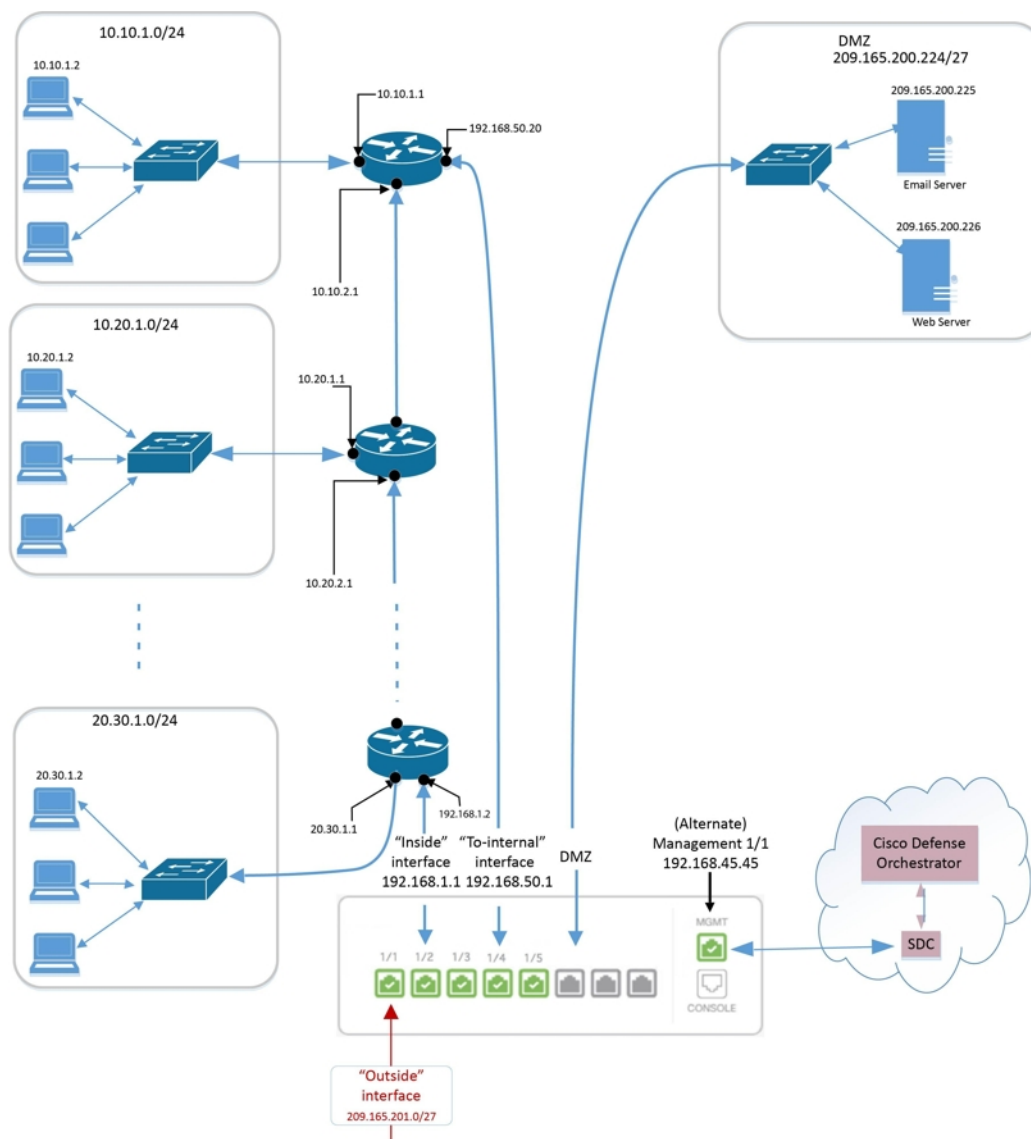
监控路由

要对路由进行监控和故障排除，请打开设备的 防火墙设备管理器 并打开 CLI 控制台，或使用 SSH 登录设备 CLI 并使用以下命令：

- `show route` 显示数据接口的路由表，包括直连网络的路由。
- `show ipv6 route` 显示数据接口的 IPv6 路由表，包括直连网络的路由。
- `show network` 显示虚拟管理接口的配置，包括管理网关。通过虚拟接口路由不由数据接口路由表处理，除非您指定数据接口作为管理网关。
- `show network-static-routes` 显示使用 `configure network static-routes` 命令为虚拟管理接口配置的静态路由。通常不会有任何静态路由，因为在大多数情况下，管理网关足以支持管理路由。这些路由不可用于数据接口上的流量。该命令在 CLI 控制台中不可用。

静态路由网络图

在讨论为 [FDM 管理设备配置静态路由和默认路由](#) 时，我们会参考此网络图：



关于虚拟路由和转发

关于 VRF

虚拟路由和转发 (VRF) 允许一个路由器中存在多个路由表实例。Firepower 版本 6.6 引入了具有默认 VRF 表和用户创建的 VRF 表的功能。单个 VRF 表可以处理多种不同的路由协议，例如 EX、OSPF、BGP、IGRP 等。VRF 表中的每个路由协议都作为一个条目列出。除了处理多种类型的常见路由协议之外，您还可以配置路由协议以引用另一个 VRF 的接口。这使得您可以在不使用多个设备的情况下对网络路径进行分段。

有关详细信息，请参阅[关于虚拟路由器和虚拟路由与转发 \(VRF\)](#)。

思科防御协调器 中的 VRF

此功能是 Firepower 版本 6.6 的新增功能。在将 FDM 管理设备载入 CDO 时，FDM 管理设备的路由页面只会读取并支持设备的全局路由器上定义的 VRF。要在 CDO 中查看全局 VRF，请从 **清单 (Inventory)** 页面中选择设备，然后从窗口右侧的 **管理 (Management)** 窗格中选择 **路由 (Routing)**。您可以在此处查看、修改和删除全局 VRF；请注意，在从 FDM 读取配置时，CDO 会保留 VRF 的名称。


CDO 防火墙设备管理器 不会读取用户定义的虚拟路由器中配置的 VRF。您必须通过 防火墙设备管理器 来创建和管理 VRF 表。

有关全局和用户定义的路由的信息，请参阅《适用于 Firepower 设备管理器版本 7.0 或更高版本的思科 Firepower 威胁防御配置指南》的“虚拟路由器”一章中的“管理虚拟路由器”部分。




对象

对象是可在一个或多个安全策略中使用的信息容器。使用对象可以轻松维护策略一致性。您可以创建单个对象，使用不同的策略，修改对象，然后将该更改传播到使用该对象的每个策略。如果没有对象，则需要单独修改需要进行相同更改的所有策略。

当您载入设备时，会识别该设备使用的所有对象，保存它们，并在“对象” (Objects) 页面上列出它们。CDO 在“对象” (Objects) 页面中，可以编辑现有对象并创建要在安全策略中使用的新对象。

CDO 将多台设备上使用的对象称为 **共享对象**，并在 **对象 (Objects)** 页面中使用此标记  进行标识。

有时，共享对象会产生一些“问题”，并且不再在多个策略或设备之间完美共享：

- **重复对象**是指同一设备上具有不同名称但值相同的两个或多个对象。这些对象通常可用于类似的目的，并供不同的策略使用。重复的对象由此问题图标标识：
- **不一致对象**是指两台或多台设备上具有相同名称但值不同的对象。有时，用户会在不同的配置中创建具有相同名称和内容的对象，但随着时间的推移，这些对象的值会出现分歧，从而造成不一致。不一致的对象由此问题图标标识：
- **未使用的对象**是设备配置中存在但未被其他对象、访问列表或 NAT 规则引用的对象。未使用的对象由此问题图标标识：

您还可以创建在规则或策略中立即使用的对象。您可以创建不与任何规则或策略关联的对象。在规则或策略中使用该未关联的对象时，会创建该对象的副本并使用该副本。CDO

您可以通过导航至对象菜单或在网络策略的详细信息中查看对象来查看对象。CDO

CDO 允许您从一个位置跨受支持的设备管理网络和服务对象。使用，您可以通过以下方式管理对象：CDO

- 根据各种条件搜索和过滤所有对象。[对象过滤器](#)
- 查找设备上的重复、未使用和不一致的对象，并合并、删除或解决这些对象问题。
- 查找未关联的对象，如果未使用，请将其删除。
- 发现跨设备通用的共享对象。


- 在提交更改之前，评估对象更改对一组策略和设备的影响。
- 比较一组对象及其与不同策略和设备的关系。
- 捕获设备在自行激活后使用的对象。CDO

如果您在创建、编辑或读取已载入设备的对象时遇到问题，请参阅以了解详细信息。[对思科防御协调器进行故障排除](#)




对象

对象是可在一个或多个安全策略中使用的信息容器。使用对象可以轻松维护策略一致性。您可以创建单个对象，使用不同的策略，修改对象，然后将该更改传播到使用该对象的每个策略。如果没有对象，则需要单独修改需要进行相同更改的所有策略。

当您载入设备时，会识别该设备使用的所有对象，保存它们，并在“对象”(Objects)页面上列出它们。CDO在“对象”(Objects)页面中，可以编辑现有对象并创建要在安全策略中使用的新对象。

CDO将多台设备上使用的对象称为**共享对象**，并在**对象(Objects)**页面中使用此标记进行标识。

有时，共享对象会产生一些“问题”，并且不再在多个策略或设备之间完美共享：

- **重复对象**是指同一设备上具有不同名称但值相同的两个或多个对象。这些对象通常可用于类似的目的，并供不同的策略使用。重复的对象由此问题图标标识：
- **不一致对象**是指两台或多台设备上具有相同名称但值不同的对象。有时，用户会在不同的配置中创建具有相同名称和内容的对象，但随着时间的推移，这些对象的值会出现分歧，从而造成不一致。不一致的对象由此问题图标标识：
- **未使用的对象**是设备配置中存在但未被其他对象、访问列表或NAT规则引用的对象。未使用的对象由此问题图标标识：

您还可以创建在规则或策略中立即使用的对象。您可以创建不与任何规则或策略关联的对象。在规则或策略中使用该未关联的对象时，会创建该对象的副本并使用该副本。CDO

您可以通过导航至对象菜单或在网络策略的详细信息中查看对象来查看对象。CDO

CDO允许您从一个位置跨受支持的设备管理网络和服务对象。使用，您可以通过以下方式管理对象：CDO

- 根据各种条件搜索和过滤所有对象。[对象过滤器](#)
- 查找设备上的重复、未使用和不一致的对象，并合并、删除或解决这些对象问题。
- 查找未关联的对象，如果未使用，请将其删除。
- 发现跨设备通用的共享对象。
- 在提交更改之前，评估对象更改对一组策略和设备的影响。
- 比较一组对象及其与不同策略和设备的关系。
- 捕获设备在自行激活后使用的对象。CDO

如果您在创建、编辑或读取已载入设备的对象时遇到问题，请参阅以了解详细信息。[对思科防御协调器进行故障排除](#)

对象类型

下表介绍您可以为设备创建和使用 CDO 管理的对象。

Table 1: FDM 托管设备对象类型

对象	说明
应用过滤器	应用过滤器对象定义 IP 连接中使用的应用，或按类型、类别、标记、风险或业务相关性定义应用的过滤器。您可以在策略中使用这些对象而不是使用端口规格来控制流量。
上传 RA AnyConnect 客户端配置文件	AnyConnect 客户端文件对象是文件对象，表示配置中使用的文件，通常适用于远程接入 VPN 策略。可以包含 AnyConnect 客户端配置文件和 AnyConnect 客户端映像文件。
证书过滤器	数字证书是一种用于身份验证的数字识别方式。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。
DNS 组	需要使用 DNS 服务器将完全限定域名 (FQDN) 解析为 IP 地址，例如 www.example.com。您可以为管理和数据接口配置不同的 DNS 组对象。
地理位置	地理位置对象定义托管设备（流量的源或目的）的国家/地区和大洲。您可以在策略中使用这些对象而不是使用 IP 地址来控制流量。
IKEv1 策略	当定义 VPN 连接时，IKEv1 策略对象包含定义 VPN 连接时 IKEv1 策略所需的参数。
IKEv2 策略	当定义 VPN 连接时，IKEv2 策略对象包含定义 VPN 连接时 IKEv2 策略所需的参数。
IKEv1 IPSEC 提议	IPsec 提议对象配置 IKE 第 1 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。
IKEv2 IPSEC 提议	IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。

对象	说明
网络	网络组和网络对象（统称为“网络对象”）定义主机或网络的地址。
安全区	安全区是一组接口。区域将网络划分成网段，帮助您管理流量以及对流量进行分类。
服务	服务对象、服务组和端口组是包含被视为 TCP/IP 协议簇一部分的协议或端口的可重用组件。
SGT 组	SGT 动态对象根据 ISE 分配的 SGT 识别源或目标地址，然后可以与传入流量进行匹配。
系统日志服务器	系统日志服务器对象标识可接收面向连接的消息或诊断系统日志（系统日志）消息的服务器。
URL	使用 URL 对象和组（统称为“URL 对象”）可定义 Web 请求的 URL 或 IP 地址。可以使用这些对象在访问控制策略中执行手动 URL 过滤，或在安全情报策略中进行阻止。

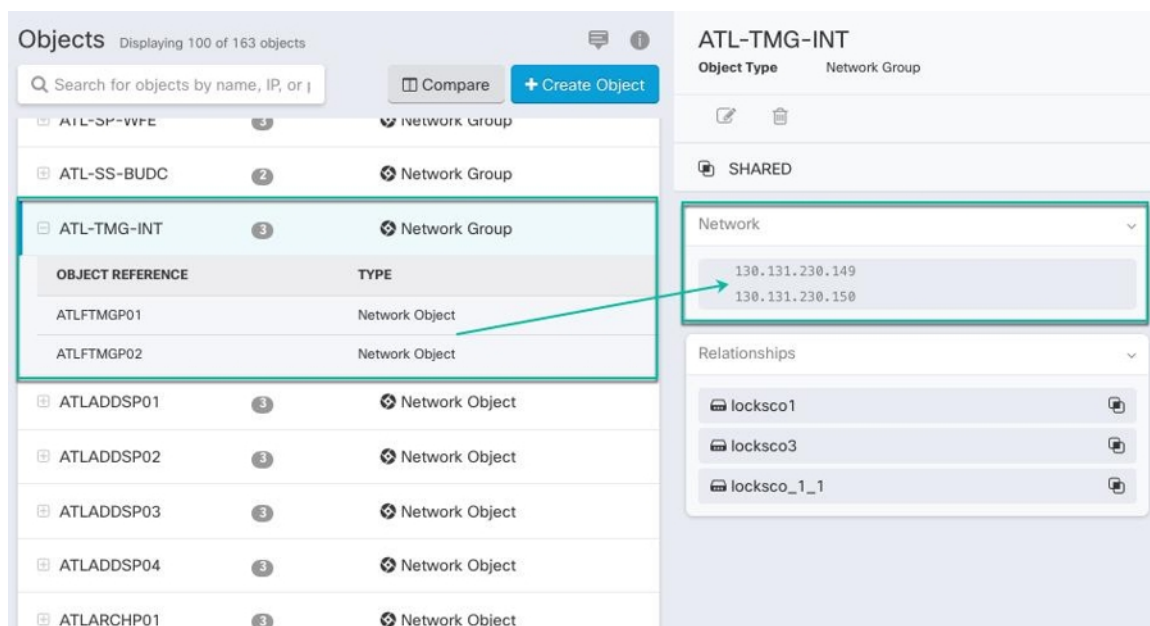
共享对象

Cisco Defense Orchestrator (CDO) 会调用多个设备上具有相同名称和相同内容的对象，即**共享对象**。共享对象由此图标标识



在**对象 (Objects)** 页面上。使用共享对象可以轻松维护策略，因为您可以在一个位置修改对象，并且该更改会影响使用该对象的所有其他策略。如果没有共享对象，则需要单独修改需要进行相同更改的所有策略。

查看共享对象时，CDO 会在对象表中显示该对象的内容。共享对象具有完全相同的内容。CDO 在详细信息窗格中显示对象元素的组合视图或“平面化”视图。请注意，在详细信息窗格中，网络元素被展平为一个简单的列表，而不是直接与命名对象关联。



对象覆盖

对象覆盖允许您覆盖特定设备上共享网络对象的值。CDO 会使用您在配置覆盖时指定的设备的相应值。虽然对象位于两个或多个名称相同但值不同的设备上，但 CDO 不会将其识别为**不一致对象**，因为这些值是作为覆盖值添加的。

您可以创建其定义适用于大多数设备的对象，然后使用覆盖为需要不同定义的几个设备指定对象的修改。您还可以创建需要为所有设备覆盖的对象，但其使用使您能够为所有设备创建单个策略。对象覆盖允许您创建较小的一组在设备间使用的共享策略，而不会失去在各个设备需要时修改策略的能力。

例如，假设您的每个办公室都有一台打印机服务器，并且您创建了一个打印机服务器对象 `print-server`。您的 ACL 中有一条规则，用于拒绝打印机服务器访问互联网。打印机服务器对象有一个您想在办公室之间更改的默认值。您可以使用对象覆盖来实现此目的，并在所有位置保持规则和“`printer-server`”对象的一致性，但它们的值可能不同。

Editing Shared Network Object
✕

Object Name *

Devices

2 Devices ...

Usage

0 Rule Sets ...

Description

printer server object

Default Value ▾

eq ▲ 126.0.1.0 ASAv-99-18 ... ↓

Override Values ▾

Enter a value to add it

Value	Devices	
126.0.2.4	Pasadena-ftd-730-516-... ...	✎ ⬆ 🗑
126.0.1.6	BGL_FTD_7.3 ...	✎ ⬆ 🗑
126.0.1.9	connected_fmc ...	✎ ⬆ 🗑

Cancel Save



Note CDO 允许您覆盖与规则集中的规则关联的对象。在将新对象添加到规则时，只有在将设备附加到规则集并保存更改后，才能覆盖该对象。有关详细信息，请参阅[为设备配置规则集](#)。



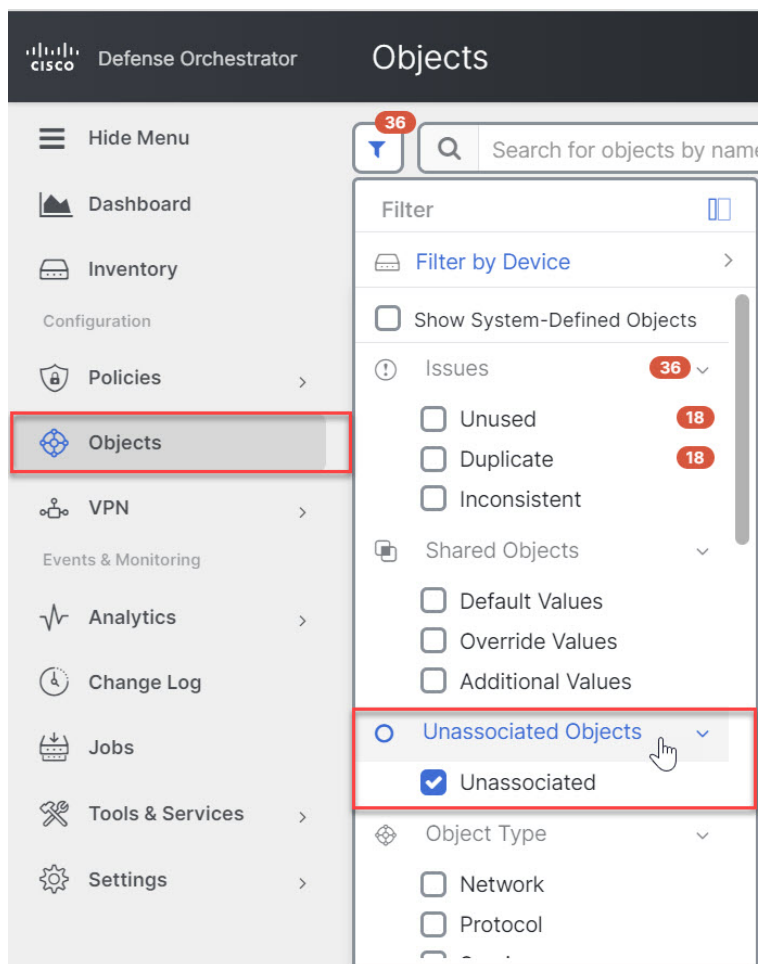
Note 如果存在不一致的对象，您可以将它们合并为一个具有覆盖的共享对象。有关详细信息，请参阅[解决不一致的对象问题](#)。

未关联的对象

您可以创建对象以立即在规则或策略中使用。您还可以创建不与任何规则或策略关联的对象。当您在规则或策略中使用该未关联的对象时，CDO 会创建该对象的副本并使用该副本。原始未关联对象仍保留在可用对象列表中，直到被夜间维护作业删除或您将其删除。

未关联的对象作为副本保留在 CDO 中，以确保在意外删除与对象关联的规则或策略时不会丢失所有配置。

要查看未关联的对象，请点击对象选项卡的左侧窗格，然后选中未关联的复选框。

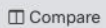


比较对象

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

步骤 2 过滤页面上的对象以查找要比较的对象。

步骤 3 点击**比较按钮**  **Compare**。

步骤 4 最多选择三个要比较的对象。


步骤 5 并排查看屏幕底部的对象。

- 点击“对象详细信息” (Object Details) 标题栏中的向上和向下箭头，可查看更多或更少的对象详细信息。
- 展开或折叠详细信息和关系框以查看更多或更少的信息。

步骤 6（可选）“关系”框显示对象的使用方式。它可能与设备或策略相关联。如果对象与设备关联，您可以点击设备名称，然后点击[查看配置](#)以查看设备的配置。CDO 显示设备的配置文件，并突出显示该对象的条目。

过滤器

您可以在**清单 (Inventory)** 和**对象 (Objects)** 页面上使用许多不同的过滤器来查找要查找的设备和对象。

要过滤，请点击设备和服务、策略和对象选项卡的左侧窗格中的 ：

清单过滤器允许您按设备类型、硬件和软件版本、Snort 版本、配置状态、连接状态、冲突检测以及保护设备连接器和标签进行过滤。您可以应用过滤器在所选设备类型选项卡中查找设备。您可以使用过滤器在所选设备类型选项卡中查找设备。



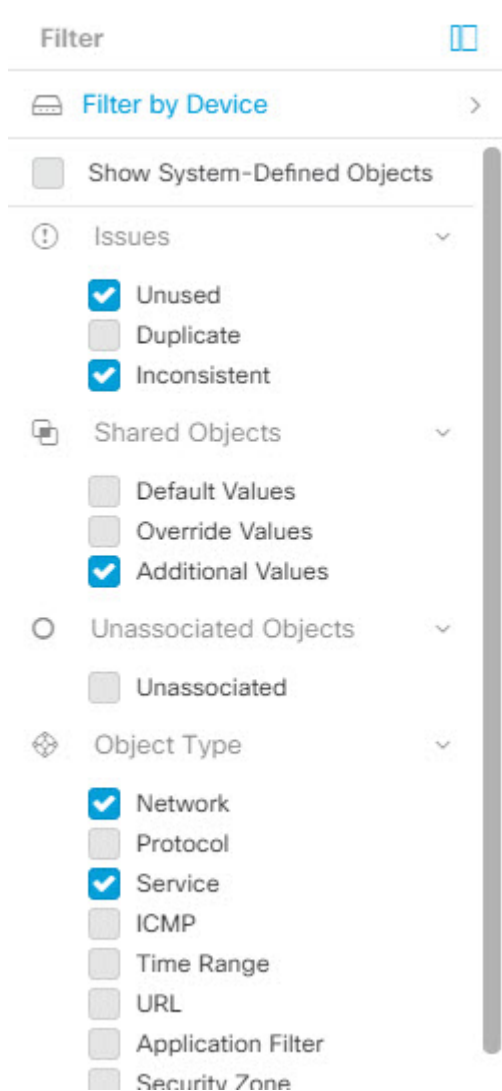
注释 打开 **FTD** 选项卡时，过滤器窗格将提供过滤器，以根据从 CDO 访问设备的管理应用来显示 FDM 管理设备。

- **FDM**：使用 FTD API 或 FDM 管理的设备。
- **FMC-FTD**：通过使用 Firepower 管理中心管理的设备。
- **FTD**：使用 FTD 管理来管理的设备。


对象过滤器允许您按设备、问题类型、共享对象、未关联的对象和对象类型进行过滤。您可以在结果中包含或不包含系统对象。您还可以使用搜索字段在过滤器结果中搜索包含特定名称、IP 地址或端口号的对象。

过滤设备和对象时，您可以组合搜索词来创建多个潜在的搜索策略来查找相关结果。

在以下示例中，过滤器应用于“问题（已使用或不一致）AND 具有其他值的共享对象 AND 类型为网络 OR 服务的对象”。



对象过滤器

要过滤，请点击“对象” (Objects) 选项卡的左侧窗格的 ：

- **所有对象 (All Objects)** - 此过滤器提供您在 CDO 中注册的所有设备中可用的所有对象。此过滤器可用于浏览所有对象，或作为搜索或进一步应用子过滤器的起点。
- **共享对象 (Shared Objects)** - 此快速过滤器显示 CDO 发现的在多台设备上共享的所有对象。
- **按设备排列的对象 (Objects By Device)** - 允许您选择特定设备，以便可以查看在所选设备上找到的对象。

子过滤器 (Sub filters) - 在每个主过滤器中，您可以应用子过滤器以进一步缩小选择范围。这些子过滤器基于对象类型 - 网络、服务、协议等。

此过滤器栏中的选定过滤器将返回与以下条件匹配的对象：

- * 位于两台设备之一上的对象。（点击按设备过滤 (**Filter by Device**) 以指定设备。）AND 是
- * 不一致对象 AND 是
- * 网络 (**Network**) 对象 OR 服务 (**Service**) 对象 AND
- * 包含"组" 在对象命名约定中

由于选中了显示系统对象 (**Show System Objects**)，因此结果将包括系统对象和用户定义的对象。

显示系统对象过滤器

某些设备随附常见服务的预定义对象。这些系统对象很方便，因为它们已经为您创建，您可以在规则和策略中使用它们。对象表中可以有許多系统对象。系统对象无法编辑或删除。


默认情况下，显示系统对象处于关闭状态。要在对象表中显示系统对象，请选中过滤器栏中的显示系统对象 (**Show System Objects**)。要隐藏对象表中的系统对象，请在过滤器栏中保持未选中状态。

如果隐藏系统对象，它们将不会包含在搜索和过滤结果中。如果显示系统对象，它们将包含在对象搜索和过滤结果中。

配置对象过滤器

您可以根据需要过滤任意数量的条件。过滤所依据的类别越多，预期的结果就越少。

Procedure

- 步骤 1** 在左侧的 CDO 导航栏中，点击对象 (**Objects**)并选择一个选项。
- 步骤 2** 点击页面顶部的过滤器图标 ，打开过滤器面板。取消选中任何已选中的过滤器，以确保不会无意中过滤掉任何对象。此外，查看搜索字段并删除可能已在搜索字段中输入的任何文本。
- 步骤 3** 如果要结果限制为在特定设备上找到的结果，请执行以下操作：
 - a. 点击按设备过滤 (**Filter By Device**)。
 - b. 搜索所有设备或点击设备选项卡以仅搜索特定类型的设备。
 - c. 选中要包含在过滤条件中的设备。
 - d. 点击确定 (**OK**)。
- 步骤 4** 选中显示系统对象 (**Show System Objects**) 以在搜索结果中包含系统对象。取消选中显示系统对象 (**Show System Objects**) 可从搜索结果中排除系统对象。
- 步骤 5** 选中要作为过滤依据的对象问题。如果选中多个问题，则选中的任何类别的对象都将包含在过滤器结果中。
- 步骤 6** 如果要查看存在问题但被管理员忽略的对象，请选中已忽略 (**Ignored**) 的问题。
- 步骤 7** 如果要过滤两台或多台设备之间共享的对象，请在共享对象 (**Shared Objects**) 中选中所需的过滤器。
 - 默认值 (**Default Values**): 过滤仅具有默认值的对象。
 - 覆盖值 (**Override Values**): 过滤具有覆盖值的对象。

- **其他值 (Additional Values):** 过滤具有其他值的对象。

步骤 8 如果要过滤不属于任何规则或策略的对象，请选中**未关联 (Unassociated)**。

步骤 9 选中要作为过滤依据的**对象类型 (Object Types)**。

步骤 10 您还可以将对象名称、IP 地址或端口号添加到对象搜索字段，以在过滤结果中查找符合搜索条件的对象。

何时从过滤条件中排除设备

将设备添加到过滤条件时，结果会显示设备上的对象，但不会显示这些对象与其他设备的关系。例如，假设 ObjectA 在 ASA1 和 ASA2 之间共享。如果要过滤对象以查找 ASA1 上的共享对象，则会找到 ObjectA，但“关系”窗格只会显示该对象位于 ASA1 上。

要查看与对象相关的所有设备，请不要在搜索条件中指定设备。按其他条件过滤并添加搜索条件（如果您愿意）。选择 CDO 识别的对象，然后在“关系”窗格中进行查看。您将看到与对象相关的所有设备和策略。

忽略对象

解决具有未使用、重复或不一致问题对象的方法之一是忽略它们。您可以决定，尽管对象未使用、重复或不一致，但该状态存在正当理由，并且您选择不解决对象问题。[解决未使用的对象问题](#)[解决重复对象问题](#)[解决不一致的对象问题](#)在未来的某个时候，您可能希望解析这些被忽略的对象。由于 CDO 在搜索对象问题时不显示已忽略的对象，因此您需要过滤已忽略对象的对象列表，然后对结果执行操作。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

步骤 2 过滤和搜索被忽略的对象。[对象过滤器](#)

步骤 3 在**对象 (Object)**表中，选择要取消忽略的对象。一次可以取消忽略一个对象。

步骤 4 点击详细信息窗格中的取消忽略。

步骤 5 确认您的请求。现在，当您按问题过滤对象时，您应该会找到以前忽略的对象。

删除对象

可以删除单个对象或多个对象。

删除单个对象


**Caution**

如果云交付的防火墙管理中心被部署在您的租户上：

您在 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的云交付的防火墙管理中心网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。


Procedure

- 步骤 1** 在左侧的 CDO 导航栏中，选择**对象 (Objects)**并选择一个选项。
- 步骤 2** 使用对象过滤器和搜索字段找到要删除的对象，然后将其选中。
- 步骤 3** 查看关系窗格。如果在策略或对象组中使用了对象，则在将其从该策略或组中删除之前，无法删除该对象。
- 步骤 4** 点击“操作” (Actions) 窗格中，点击**编辑**图标 .
- 步骤 5** 点击确定，确认要删除对象。
- 步骤 6** [预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

删除一组未使用的对象

当您载入设备并开始解决对象问题时，您会发现许多未使用的对象。一次最多可以删除 50 个未使用的对象。

过程

- 步骤 1** 使用问题过滤器查找未使用的对象。您还可以使用设备过滤器通过选择无设备来查找未与设备关联的对象。过滤对象列表后，系统将显示对象复选框。
- 步骤 2** 选中对象表标题中的全选复选框，以选择过滤器找到的显示在对象表中的所有对象；或者，选中要删除的各个对象的各个复选框。
- 步骤 3** 点击“操作” (Actions) 窗格中，点击**编辑**图标 .
- 步骤 4** 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

网络对象

网络对象 可以包含主机、网络 IP 地址、IP 地址范围、完全限定域名 (FQDN)或用 CIDR 符号表示的子网。**网络组**是添加到组中的网络对象和其他单个地址或子网络的集合。网络对象和网络组用于访问规则、网络策略和 NAT 规则。您可以使用 CDO 创建、更新和删除网络对象和网络组。

Table 2: 网络对象的允许值

设备类型	IPv4 / IPv6	单个地址	地址范围	域名名称	使用 CIDR 表示法的子网。
FTD	IPv4 和 IPv6	是	是	是	是

Table 3: 网络组允许的内容

设备类型	IP 值	网络对象	网络组
FTD	不支持	是	是

跨产品重用网络对象

如果您的 思科防御协调器 租户具有云交付的防火墙管理中心：

在创建 Secure Firewall Threat Defense、FDM 管理 威胁防御、ASA 或 Meraki 网络对象或组时，对象的副本也会被添加到在配置云交付的防火墙管理中心时使用的对象 (Objects) > 其他 FTD 对象 (Other FTD Objects) 页面上的对象列表中。

对任一页面上的网络对象或组所做的更改适用于两个页面上的对象或组实例。从一个页面删除对象也会从另一个页面删除该对象的相应副本。

例外情况：

- 如果云交付的防火墙管理中心已存在同名的网络对象，则不会在思科防御协调器的对象 (Objects) > 其他 FTD 对象 (Other FTD Objects) 页面上复制新的 Secure Firewall Threat Defense、FDM 管理 威胁防御、ASA 或 Meraki 网络对象
- 由本地 Cisco Secure Firewall Management Center 管理的载入 威胁防御 设备中的网络对象和组不会复制到对象 (Objects) > 其他 FTD 对象 (Other FTD Objects) 页面，因此无法在云交付的防火墙管理中心中使用。

请注意，对于已迁移到云交付的防火墙管理中心的本地 Cisco Secure Firewall Management Center 实例，如果在部署到 FTD 设备的策略中使用网络对象和组，它们将被复制到 CDO 对象页面。

- 新租户上会自动启用在 CDO 和云交付的防火墙管理中心之间共享网络对象，但现有租户必须另行请求。如果您的网络对象未与云交付的防火墙管理中心共享，请联系 TAC 以在您的租户上启用这些功能。

查看网络对象

使用 CDO 创建的网络对象以及已载入的设备配置中的 CDO 识别的网络对象会显示在对象页面上。它们标有对象类型。这使您可以按对象类型进行过滤，以快速找到要查找的对象。

在“对象” (Objects) 页面上选择网络对象时，您可在“详细信息” (Details) 窗格中看到该对象的值。“关系” (Relationships) 窗格显示对象是否用于策略中，以及对象存储在什么设备上。

在点击网络组时，您会看到该组的内容。网络组是网络对象为其提供的所有值的综合体。

相关信息：

- [创建或编辑 Firepower 网络对象或网络组](#)

创建或编辑 Firepower 网络对象或网络组

Firepower 网络对象可以包含以 CIDR 表示法表示的主机名、IP 地址或子网地址。**网络组**是在访问规则、网络策略和 NAT 规则中使用的网络对象和网络组的集合。您可以使用思科防御协调器(CDO)来创建、读取、更新和删除网络对象和网络组。

Firepower 网络对象和组可供 ASA、威胁防御、FDM 管理和 Meraki 设备使用。请参阅[跨产品重用网络对象](#)。



Note 如果云交付的防火墙管理中心被部署在您的租户上：

在 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上创建网络对象或组时，对象的副本会自动添加到 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面，反之亦然。



Caution 如果云交付的防火墙管理中心被部署在您的租户上：

您在 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的云交付的防火墙管理中心网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Table 4: 可以添加到网络对象的 IP 地址

设备类型	IPv4 / IPv6	单个地址	地址范围	部分限定域名 (PQDN)	使用 CIDR 表示法的子网。
FirePower	IPv4 / IPv6	是	是	是	是

相关信息：

- [编辑 Firepower 网络对象](#)
- [编辑 Firepower 网络对象](#)
- [向共享网络组添加其他值](#)
- [编辑共享网络组中的其他值](#)

编辑 Firepower 网络对象




Note 如果云交付的防火墙管理中心被部署在您的租户上：

在或对象 (Objects) > FDM 对象 (FDM Objects) 页面上创建网络对象或组时，对象的副本会自动添加到对象 (Objects) > 其他 FTD 对象 (Other FTD Objects) 页面，反之亦然。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击对象 (Objects) > FDM 对象 (FDM Objects)。

步骤 2 点击蓝色加号按钮  以创建新的对象。

步骤 3 点击 FTD > 网络 (Network)。

步骤 4 输入对象名称。

步骤 5 选择创建网络对象。

步骤 6 在值 (Value) 部分中：

- 选择 **eq** 并输入以 CIDR 表示法表示的单个 IP 地址、子网地址或部分限定域名 (PQDN)。
- 选择范围并输入 IP 地址范围。

Note 请勿设置主机位值。如果输入的主机位值不是 0，CDO 会在创建对象时取消设置，因为云交付的防火墙管理中心仅接受未设置主机位的 IPv6 对象。

步骤 7 点击添加 (Add)。

注意：新创建的网络对象不与任何 FDM 管理设备关联，因为它们不属于任何规则或策略。要查看这些对象，请在对象过滤器中选择未关联的对象类别。有关详细信息，请参阅[对象过滤器](#)。在设备的规则或策略中使用未关联的对象后，此类对象将与该设备关联。

创建 Firepower 网络组


网络组可以包含网络对象和网络组。创建新的网络组时，可以按名称、IP 地址、IP 地址范围或 FQDN 搜索现有对象，并将其添加到网络组。如果对象不存在，您可以立即在同一接口中创建该对象并将其添加到网络组。



Note 如果云交付的防火墙管理中心被部署在您的租户上：

在或对象 (Objects) > FDM 对象 (FDM Objects) 页面上创建网络对象或组时，对象的副本会自动添加到对象 (Objects) > 其他 FTD 对象 (Other FTD Objects) 页面，反之亦然。

Procedure

- 步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
- 步骤 2** 点击蓝色加号按钮  以创建新的对象。
- 步骤 3** 点击 **FTD > 网络 (Network)**。
- 步骤 4** 输入 **对象名称**。
- 步骤 5** 选择创建网络组。
- 步骤 6** 在 **值 (Values)** 字段中输入值或名称。当您开始输入时，CDO 会提供与您的条目匹配的对象名称或值。
- 步骤 7** 您可以选择一个显示的现有对象，也可以根据输入的名称或值创建一个新对象。
- 步骤 8** 如果 CDO 找到了匹配项，要选择现有对象，请点击 **添加 (Add)** 将网络对象或网络组添加到新网络组。
- 步骤 9** 如果输入的值或对象不存在，则可以执行以下操作之一：
- 点击 **添加为此名称的新对象 (Add as New Object With This Name)**，以创建具有该名称的新对象。输入一个值，然后点击复选标记将其保存。
 - 点击 **添加为新对象 (Add as New Object)** 以创建一个新对象。对象名称和值相同。输入名称，然后点击复选标记将其保存。
- 即使该值已存在，也可以创建一个新对象。您可以对这些对象进行更改并将它们保存。
- 注意：您可以点击编辑图标修改详细信息。点击“删除”按钮不会删除对象本身；相反，它会将其从网络组中删除。
- 步骤 10** 添加所需的对象后，点击保存以创建新的网络组。
- 步骤 11** [预览和部署所有设备的配置更改](#)。
-

编辑 Firepower 网络对象



Caution 如果云交付的防火墙管理中心被部署在您的租户上：

您在 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的云交付的防火墙管理中心网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure

- 步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的对象。

步骤 3 选择网络对象，然后单击操作 (Actions) 窗格中的编辑图标 。

步骤 4 以在“创建 Firepower 网络组” (Create a Firepower Network Group) 中创建值的相同方式编辑对话框中的值。

Note 单击旁边的删除图标，从网络组中删除对象。

步骤 5 单击保存 (Save)。CDO 会显示将受更改影响的设备。

步骤 6 单击确认 (Confirm) 以完成对对象以及受其影响的任何设备的更改。

编辑 Firepower 网络组



Caution

如果云交付的防火墙管理中心被部署在您的租户上：


您在或对象 (Objects) > FDM 对象 (FDM Objects) 页面上对网络对象和组所做的更改会反映在对象 (Objects) > 其他 FTD 对象 (Other FTD Objects) 页面上的相应的云交付的防火墙管理中心网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure


步骤 1 在左侧的 CDO 导航栏中，单击对象 (Objects) > FDM 对象 (FDM Objects)。

步骤 2 使用对象过滤器和搜索字段找到您要编辑的网络组。

步骤 3 选择网络组，然后单击操作 (Actions) 窗格中的编辑图标 。

步骤 4 如有必要，更改对象名称和说明。

步骤 5 如果要更改已添加到网络组的对象或网络组，请执行以下步骤：

- a. 单击对象名称或网络组旁边的编辑图标可对其进行修改。 
- b. 单击复选标记以保存更改。**注意：**您可以单击删除图标从网络组中删除该值。

步骤 6 如果要向此网络组添加新的网络对象或网络组，必须执行以下步骤：

- a. 在值字段中，输入新值或现有网络对象的名称。当您开始输入时，CDO 会提供与您的条目匹配的对象名称或值。您可以选择一个显示的现有对象，也可以根据输入的名称或值创建一个新对象。
- b. 如果 CDO 找到了匹配项，要选择现有对象，请单击添加 (Add) 将网络对象或网络组添加到新网络组。
- c. 如果输入的值或对象不存在，则可以执行以下操作之一：

- 点击添加为此名称的新对象 (**Add as New Object With This Name**)，以创建具有该名称的新对象。输入一个值，然后点击复选标记将其保存。
- 点击添加为新对象 (**Add as New Object**) 以创建一个新对象。对象名称和值相同。输入名称，然后点击复选标记将其保存。

即使该值已存在，也可以创建一个新对象。您可以对这些对象进行更改并将它们保存。

步骤 7 点击保存 (**Save**)。CDO 显示将受更改影响的策略。

步骤 8 点击确认 (**Confirm**) 以完成对对象以及受其影响的任何设备的更改。

步骤 9 [预览和部署所有设备的配置更改](#)。

添加对象覆盖



注意 如果云交付的防火墙管理中心被部署在您的租户上：

您在 [对象 \(Objects\) > FDM 对象 \(FDM Objects\)](#) 页面上对网络对象和组所做的更改会反映在 [对象 \(Objects\) > 其他 FTD 对象 \(Other FTD Objects\)](#) 页面上的相应的云交付的防火墙管理中心网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

过程

步骤 1 在左侧的 CDO 导航栏中，点击 [对象 \(Objects\) > FDM 对象 \(FDM Objects\)](#)。

步骤 2 使用对象过滤器和搜索字段找到具有要编辑的覆盖的对象。

步骤 3 选择网络对象，然后点击操作 (**Actions**) 窗格中的编辑图标

步骤 4 在覆盖值 (**Override Values**) 对话框中输入值，然后点击 + 添加值 (+ **Add Value**)。

重要事项 要添加的覆盖必须具有与对象所包含的值类型相同。例如，对于网络对象，只能使用网络值而不是主机值来配置覆盖。

步骤 5 看到添加的值后，点击覆盖值 (**Override Values**) 的设备 (**Devices**) 列中的单元格。

步骤 6 点击添加设备 (**Add Devices**)，然后选择要向其添加覆盖的设备。您选择的设备必须包含要向其添加覆盖的对象。

步骤 7 点击保存 (**Save**)。CDO 会显示将受更改影响的设备。

步骤 8 点击确认 (**Confirm**) 以完成对对象以及受其影响的任何设备的覆盖添加。

注释 您可以向一个对象添加多个覆盖。但每次添加覆盖时，都必须选择包含对象的不同设备。

步骤 9 请参阅[对象覆盖](#)，了解有关对象覆盖和[编辑对象覆盖](#)的详细信息以编辑现有覆盖。


编辑对象覆盖

只要设备上存在对象，您就可以修改现有覆盖的值。


Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到具有要编辑的覆盖的对象。

步骤 3 选择带有覆盖的对象，然后点击“操作” (Actions) 窗格中的编辑图标 。

步骤 4 修改覆盖值：

- 点击编辑图标以修改值。
- 在覆盖值 (Override Values) 中点击设备 (Devices) 列，以便分配新设备。您可以选择已分配的设备，然后点击删除覆盖 (Remove Overrides) 以删除该设备上的覆盖。
- 点击覆盖值 (Override Values) 中的  箭头，将其推送并设置为共享对象的默认值。
- 点击要删除的覆盖旁边的删除图标。

步骤 5 点击保存 (Save)。CDO 会显示将受更改影响的设备。

步骤 6 点击确认 (Confirm) 以完成对对象以及受其影响的任何设备的更改。

步骤 7 [预览和部署所有设备的配置更改](#)。

向共享网络组添加其他值

共享网络组中与其关联的所有设备上存在的值被称为“默认值”。CDO 允许您向共享网络组添加“其他值”，并将这些值分配给与该共享网络组关联的某些设备。当 CDO 将更改部署到设备时，它会确定内容并将“默认值”推送到与共享网络组关联的所有设备，而“其他值”只会被推送到指定的设备。

例如，假设您的总部有四台 AD 主服务器，那么这些服务器应可从您的所有站点进行访问。因此，您创建了一个名为“Active-Directory”的对象组，以便用于所有站点。现在，您要为其中一个分支机构再添加两台 AD 服务器。为此，您可以通过将其详细信息添加为对象组“Active-Directory”上该分支机构的特定附加值来执行此操作。这两台服务器不参与确定对象“Active-Directory”是一致的还是共享的。因此，您可从所有站点访问四台 AD 主服务器，但分支机构（具有两台附加服务器）可以访问两台 AD 服务器和四台 AD 主服务器。



Note 如果存在不一致的共享网络组，则您可以将它们合并为具有其他值的单个共享网络组。有关详细信息，请参阅[解决不一致的对象问题](#)。

**Caution**

如果云交付的防火墙管理中心被部署在您的租户上：


您在 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的云交付的防火墙管理中心网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到您要编辑的共享网络组。

步骤 3 点击操作 (**Actions**) 窗格中的编辑图标 。

- **设备 (Devices)** 字段会显示共享网络组所在的设备。
- **使用情况 (Usage)** 字段会显示与共享网络组关联的规则集。
- **默认值 (Default Values)** 字段将指定默认网络对象及其与创建期间提供的共享网络组关联的值。在此字段旁边，您可以看到包含此默认值的设备数量，您可以点击查看其名称和设备类型。您还可以查看与此值关联的规则集。

步骤 4 在 **其他值 (Additional Values)** 字段中输入值或名称。当您开始输入时，CDO 会提供与您的条目匹配的对象名称或值。

步骤 5 您可以选择一个显示的现有对象，也可以根据输入的名称或值创建一个新对象。

步骤 6 如果 CDO 找到了匹配项，要选择现有对象，请点击 **添加 (Add)** 将网络对象或网络组添加到新网络组。

步骤 7 如果输入的值或对象不存在，则可以执行以下操作之一：

- 点击 **添加为此名称的新对象 (Add as New Object With This Name)**，以创建具有该名称的新对象。输入一个值，然后点击复选标记将其保存。
- 点击 **添加为新对象 (Add as New Object)** 以创建一个新对象。对象名称和值相同。输入名称，然后点击复选标记将其保存。

即使该值已存在，也可以创建一个新对象。您可以对这些对象进行更改并将它们保存。

步骤 8 在 **设备 (Devices)** 列中，点击与新添加的对象关联的单元格，然后点击 **添加设备 (Add Devices)**。

步骤 9 选择所需的设备，然后点击 **确定 (OK)**。

步骤 10 点击 **保存 (Save)**。CDO 会显示将受更改影响的设备。

步骤 11 点击 **确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

步骤 12 [预览和部署所有设备的配置更改](#)。

编辑共享网络组中的其他值



Caution 如果云交付的防火墙管理中心被部署在您的租户上:

您在或对象 (Objects) > FDM 对象 (FDM Objects) 页面上对网络对象和组所做的更改会反映在对象 (Objects) > 其他 FTD 对象 (Other FTD Objects) 页面上的相应的云交付的防火墙管理中心网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure

步骤 1 在左侧的 CDO 导航栏中, 点击对象 (Objects) > FDM 对象 (FDM Objects)。

步骤 2 使用对象过滤器和搜索字段找到具有要编辑的覆盖的对象。

步骤 3 点击操作窗格中的编辑图标

步骤 4 修改覆盖值:

- 点击编辑图标以修改值。
- 点击设备 (Devices) 列中的单元格以分配新设备。您可以选择已分配的设备, 然后点击删除覆盖 (Remove Overrides) 以删除该设备上的覆盖。
- 点击默认值 (Default Values) 中的 箭头, 将其设置为共享网络组的其他值。与共享网络组关联的所有设备都会自动分配到该共享网络组。
- 点击覆盖值 (Override Values) 中的 箭头, 将其推送并设置为共享网络组的默认对象。
- 点击旁边的删除图标, 从网络组中删除对象。

步骤 5 点击保存 (Save)。CDO 会显示将受更改影响的设备。

步骤 6 点击确认 (Confirm) 以完成对对象以及受其影响的任何设备的更改。

步骤 7 [预览和部署所有设备的配置更改](#)。

删除网络对象和组

如果云交付的防火墙管理中心被部署在您的租户上:

从或对象 (Objects) > FDM 对象 (FDM Objects) 页面删除网络对象或组都会从对象 (Objects) > 其他 FTD 对象 (Other FTD Objects) 页面中删除复制的对象或组, 反之亦然。

应用过滤器对象

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

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

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



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



Note 当 FDM 托管的 FTD 设备被载入 CDO 时，它会将应用过滤器转换为应用过滤器对象，而不会更改访问规则或 SSL 解密中定义的规则。由于配置更改，设备的配置状态更改为“未同步”，需要从 CDO 进行配置部署。通常，在您手动保存过滤器之前，FDM 不会将应用过滤器转换为应用过滤器对象。

相关信息：

- [创建和编辑 Firepower 应用过滤器对象](#)
- [删除对象](#)

创建和编辑 Firepower 应用过滤器对象

应用过滤器对象允许您以精选应用或由过滤器识别的一组应用为目标。此应用过滤器对象可用于策略中。

创建 Firepower 应用过滤器对象

要创建应用过滤器对象，请执行以下程序：

Procedure

- 步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
- 步骤 2** 点击 **创建对象 > FTD > 应用服务**。
- 步骤 3** 输入对象的 **对象名称** 和 **说明**（后者为可选项）。
- 步骤 4** 点击 **添加过滤器 (Add Filter)**，然后选择要添加到对象的应用程序和过滤器。

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

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

The screenshot shows a 'Filter Applications' dialog box with the following settings:

- Risks:** High, Very High
- Business Relevance:** Very Low, Low
- Types:** Web Application
- Categories:** ad portal
- Tags:** displays ads

Below the filters is a search bar labeled 'Filter the list of applications' with a magnifying glass icon. Below the search bar, it indicates '4 matches' and displays a table:

Application Name	Description
MyWay	Adware and spyware, categorized as an internet browser hijacker.
Olx.pl	Platform to connect local people to buy, sell or exchange used goods and services through their mobile phone or on the web.
PopAds	Advertising network specialized in popunders on the Internet.
PopCash	Advertising platform.

At the bottom right of the dialog box are 'Cancel' and 'OK' buttons.

风险 (Risks): 应用所用的用途可能违反组织安全策略的可能性，从非常低到非常高。

业务相关性 (Business Relevance): 在组织的业务运营环境（非娱乐性）下使用应用的可能性，从非常低到非常高。

类型 (Types): 应用类型。

- **应用协议 (Application Protocol):** 应用协议（例如 HTTP 和 SSH），代表主机之间的通信。
- **客户端协议 (Client Protocol):** 客户端（例如 Web 浏览器和邮件客户端），代表主机上运行的软件。

- **Web 应用 (Web Application):** Web 应用（例如 MPEG 视频和 Facebook），代表 HTTP 流量的内容或请求的 URL。

类别 (Categories): 对应用的一般分类，说明其最基本的功能。

标记 (Tags): 关于应用的其他信息，与类别类似。

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

应用列表 (Applications List) (显示底部): 在从列表上方的选项中选择过滤器时，此列表将进行更新，所以您可查看当前符合过滤器的应用。在计划将过滤器条件添加到规则中时，使用此列表可确认您的过滤器是否针对所需的应用。要将特定应用添加到对象，请从过滤列表中选择它们。选择应用后，过滤器将不再适用。如果您希望过滤器本身作为对象，请勿从列表中选择应用。然后，该对象将代表过滤器识别的应用。

步骤 5 点击确定 (OK)，保存更改。


编辑 Firepower 应用过滤器对象

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的对象。

步骤 3 选择要编辑的对象。

步骤 4 点击“操作” (Actions) 窗格中的编辑图标 。

步骤 5 以在上述过程中创建值的相同方式编辑对话框中的值。

步骤 6 点击保存 (Save)。

步骤 7 CDO 显示将受更改影响的策略。点击 **确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

相关信息:

- [对象](#)
- [对象过滤器](#)
- [删除 Firepower 对象](#)

地理位置对象

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

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

更新地理定位数据库

为了确保使用最新的地理位置数据来过滤流量，思科强烈建议您定期更新地理位置数据库(GeoDB)。目前，这不是您可以使用 Cisco Defense Orchestrator 执行的任务。请参阅《[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#)》的以下部分，了解您的设备正在运行的版本，以了解有关 GeoDB 及其更新方式的详细信息。

- 更新系统数据库和源
- 更新系统数据库

创建和编辑 Firepower 地理位置过滤器对象

您可以在对象页面上或在创建安全策略时单独创建地理位置对象。此程序从对象页面创建地理位置对象。

要创建地理位置对象，请执行以下步骤：

Procedure

- 步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
 - 步骤 2** 点击 **创建对象 (Create Object) > FTD > 地理位置 (Geolocation)**。
 - 步骤 3** 输入对象的 **对象名称** 和 **说明**（后者为可选项）。
 - 步骤 4** 在过滤器栏中，开始键入国家/地区或地区的名称，系统会显示可能的匹配项列表。
 - 步骤 5** 选中要添加到对象的国家/地区或地区。
 - 步骤 6** 点击 **添加**。
-

编辑地理位置对象

Procedure

- 步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
 - 步骤 2** 使用过滤器窗格和搜索字段查找对象。
 - 步骤 3** 在“操作” (Actions) 窗格中，点击 **编辑 (Edit)**。
 - 步骤 4** 您可以更改对象的名称，并向对象添加或删除国家/地区和地区。
 - 步骤 5** 点击 **保存 (Save)**。
 - 步骤 6** 如果有任何设备受到影响，您会收到通知。点击 **Confirm**。
 - 步骤 7** 如果设备或策略受到影响，请打开资产页面并预览并将更改部署到设备。
-

DNS 服务器组对象


域名系统 (DNS) 组定义 DNS 服务器列表和某些相关联的属性。需要使用 DNS 服务器将完全限定域名 (FQDN) 解析为 IP 地址，例如 `www.example.com`。您可以为管理和数据接口配置不同的 DNS 组对象。

FDM 管理设备必须先配置 DNS 服务器，然后才能创建新的 DNS 组对象。您可以将 DNS 服务器添加到思科防御协调器 (CDO) 中的 [配置 DNS 服务器](#)，也可以在防火墙设备管理器中创建 DNS 服务器，然后将 FDM 管理配置同步到 CDO。要在防火墙设备管理器中创建或修改 DNS 服务器设置，请参阅《[思科 Firepower 设备管理器配置指南](#)》，版本 6.4 或更高版本中的 [为数据和管理接口配置 DNS](#)。

创建 DNS 组对象

使用以下程序在 CDO 中创建新的 DNS 组对象：

Procedure

- 步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
- 步骤 2** 点击蓝色加号按钮  以创建新的对象。
- 步骤 3** 点击 FTD DNS 组。 >
- 步骤 4** 输入 **对象名称 (Object Name)**。
- 步骤 5** (可选) 添加说明。
- 步骤 6** 输入 **DNS 服务器** 的 IP 地址。您最多可以添加六个 DNS 服务器；点击添加 DNS 服务器。如果您想要删除服务器地址，请点击删除图标。
Note 列表采用优先顺序：始终使用列表中的第一个服务器，只有当从前面的服务器收不到响应时，才使用后面的服务器。虽然最多可以添加六台服务器，但只有列出的前 3 台服务器将用于管理接口。
- 步骤 7** 输入**域搜索名称 (Domain Search Name)**。此域将被添加到非完全限定的主机名，例如 `serverA` 而不是 `serverA.example.com`。
- 步骤 8** 输入**重试次数**。系统接收不到响应时，重试 DNS 服务器列表的次数，介于 0 和 10 次之间。默认值为 2。此设置仅适用于数据接口上使用的 DNS 组。
- 步骤 9** 输入**超时值**。尝试下一个 DNS 服务器之前要等待的秒数，介于 1 和 30 秒之间。默认值为 2 秒。每次系统重试服务器列表，此超时将加倍。此设置仅适用于数据接口上使用的 DNS 组。
- 步骤 10** 点击**添加**。


编辑 DNS 组对象

您可以编辑在思科防御协调器或防火墙设备管理器中创建的 DNS 组对象。使用以下程序编辑现有的 DNS 组对象：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的 **DNS 组对象**。

步骤 3 选择对象，然后点击 **操作 (Actions)** 窗格中的编辑图标 。

步骤 4 编辑以下任何条目：

- 对象名称。
- 说明。
- DNS 服务器。您可以在此列表中编辑、添加或删除 DNS 服务器。
- 域搜索名称。
- 重试。
- 超时。

步骤 5 点击 **保存 (Save)**。

步骤 6 [预览和部署所有设备的配置更改](#)。

删除 DNS 组对象

使用以下程序从 CDO 中删除 DNS 组对象：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的 **DNS 组对象**。

步骤 3 选择对象，然后点击删除图标 。

步骤 4 确认要删除 DNS 组对象，然后点击确定。

步骤 5 [预览和部署所有设备的配置更改](#)。

将 DNS 组对象添加为 DNS 服务器 FDM 管理

您可以将 DNS 组对象添加为数据接口或管理接口的首选 DNS 组。有关详细信息，请参阅 FDM 托管设备设置。 [FDM 管理 设备设置, on page 297](#)

证书对象

数字证书是一种用于身份验证的数字识别方式。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。

请参阅适用于您的设备的版本的《[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#)》中[可恢复对象](#)一章的关于证书和配置证书部分。

关于证书

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

您可以创建以下类型的证书：

- **内部证书 (Internal certificates)** - 内部身份证书是用于特定系统或主机的证书。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名证书。

系统提供以下预定义内部证书（您可以按原样使用或替换它们）：**DefaultInternalCertificate** 和 **DefaultWebServerCertificate**

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

系统提供以下预定义内部 CA 证书（您可以按原样使用或替换它们）：**NGFW-Default-InternalCA**

- **可信证书颁发机构 (CA) 证书** - 可信的 CA 证书可用于签署其他证书。它是自签名证书，也称为根证书。由另一个 CA 证书颁发的证书称为从属证书。

证书颁发机构 (CA) 是指“签署”证书以确认其真实性，从而确保设备或用户的身份的可信颁发机构。CA 在 PKI（使用公钥或私钥加密以确保安全性）的情景下颁发数字证书。CA 可以是可信的第三方（例如 VeriSign），也可以是组织内建立的私有（内部）CA。CA 负责管理证书请求和颁发数字证书。

系统包括许多从第三方证书颁发机构获取的受信任的 CA 证书。SSL 解密策略可使用这些证书执行解密重新签署操作。

有关详细信息，请参阅《[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#)》中“可重用对象”一章的功能使用的证书类型部分。

功能使用的证书类型

您需要为每个功能创建正确类型的证书。以下功能需要证书。

身份策略（强制网络门户）- 内部证书

(可选。)强制网络门户用于身份策略中。在向设备进行身份验证时，为了标识自己的身份并接收与其用户名关联的 IP 地址，用户必须接受此证书。如果不提供证书，设备将使用自动生成的证书。

SSL 解密策略 - 内部、内部 CA 和受信任 CA 证书。

(必需。)SSL 解密策略将证书用于以下目的：

- 内部证书用于已知的密钥解密规则。
- 在客户端和 FTD 设备之间创建会话时，内部 CA 证书用于解密重签名规则。
- 受信任 CA 证书
 - 在 FTD 设备和服务器之间创建会话时，它们可直接用于解密重签名规则。与其他证书不同，这些证书不能直接在 SSL 解密策略中配置，而是需要上传到系统。系统包括大量受信任 CA 证书，因此，您无需上传任何其他证书。
 - 创建 Active Directory 领域对象并将目录服务器配置为使用加密时。

配置证书

身份策略或 SSL 解密策略中使用的证书必须是 PEM 或 DER 格式的 X509 证书。如果需要，您可以使用 OpenSSL 生成证书、从受信任的证书颁发机构获取证书或创建自签名证书。

使用以下程序配置证书对象：

- [上传内部证书和内部 CA 证书](#)
- [上传受信任的 CA 证书](#)
- [生成自签名的内部证书和内部 CA 证书](#)
- 要查看或编辑证书，请点击证书的编辑图标或视图图标。
- 要删除未引用的证书，请点击证书的垃圾桶图标（删除图标）。请参阅[删除对象](#)。

上传内部证书和内部 CA 证书

内部身份证书是特定系统或主机的证书。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名证书。

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

有关使用这些证书的功能的信息，请参阅[功能使用的证书类型](#)。


操作步骤

此程序通过上传证书文件或将现有证书文本粘贴到文本框中来创建内部证书身份或内部 CA 证书。如果要生成自签名证书，请参阅生成自签名内部证书和内部 CA 证书。[生成自签名的内部证书和内部 CA 证书](#)

要创建内部或内部 CA 证书对象，或者在向策略添加新证书对象时，请执行以下程序：

Procedure

步骤 1 执行以下操作之一：

- 在对象页面中创建证书对象：
 - a. 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
 - b. 点击加号按钮，然后选择 FTD 证书  >
- 将新证书对象添加到策略时，点击创建新对象。

步骤 2 键入证书的名称。该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 3 在步骤 1 中，选择内部证书或内部 CA。

步骤 4 在步骤 2 中，选择上传 (**Upload**) 以上传证书文件。

步骤 5 在步骤 3 的服务器证书 (**Server Certificate**) 区域中，将证书内容粘贴到文本框中，或按照向导中的说明上传证书文件。如果将证书粘贴到文本框中，则证书必须包括 BEGIN CERTIFICATE 和 END CERTIFICATE 两行。例如：

```
-----BEGIN CERTIFICATE-----
MIICMTCCAzoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQvV2lkZ210
(...5 lines removed...)
shGJDReryJQqilHHzrYTWZAYTrD7NQPHutK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZlzM8BpX2Js2yQ3ms30pr8rO+gPCPMCawEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfwCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
v1k3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

步骤 6 在步骤 3 的证书密钥 (**Certificate Key**) 区域中，将密钥内容粘贴到证书密钥文本框中，或者按照向导中的说明上传密钥文件。如果将密钥粘贴到文本框中，则密钥必须包含 BEGIN PRIVATE KEY 或 BEGIN RSA PRIVATE KEY 和 END PRIVATE KEY 或 END PRIVATE KEY 行。

Note 密钥不能加密。

步骤 7 点击添加。

上传受信任的 CA 证书

受信任证书颁发机构 (CA) 证书用于签署其他证书。它是自签名证书，也称为根证书。由另一个 CA 证书颁发的证书称为从属证书。


有关使用这些证书的功能的信息，请参阅[功能使用的证书类型](#)。

受信任 CA 证书可从外部证书颁发机构获取，也可以使用自己的内部 CA 创建（例如通过 OpenSSL 工具生成证书）。然后，使用以下步骤程序上传证书。

操作步骤

Procedure

步骤 1 执行以下操作之一：

- 在对象页面中创建证书对象：
 - a. 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
 - b. 点击加号按钮，然后选择 FTD 证书。  >
- 将新证书对象添加到策略时，点击创建新对象。

步骤 2 键入证书的名称。该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 3 在步骤 1 中，选择外部 CA 证书，然后点击继续。向导前进到步骤 3。

步骤 4 在步骤 3 的证书内容 (**Certificate Contents**) 区域中，将证书内容粘贴到文本框中，或按照向导中的说明上传证书文件。

证书必须遵循以下准则：

- 证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 10.10.10.250 作为 IP 地址，但证书中的地址为 `ad.example.com`，则连接失败。
- 该证书必须为 PEM 或 DER 格式的 X509 证书。
- 您粘贴的证书必须包括 `BEGIN CERTIFICATE` 和 `END CERTIFICATE` 行。例如：

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxZAJBgNV
BAYTA1VTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGZXVzdGluMRQwEgYDVQQKDAx
OTIuMTY4LjEUMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxZDZAN
BgNVBACMBmFlc3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjEwFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIIICiJANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5J1F58AvH82GPKoQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6H0gK1OwXbRvOdkstzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbsCF5rP71fObG9Iu6+u4EfHp/NQv9s9dn5PMffXKieqpuN200jv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

步骤 5 点击添加。

生成自签名的内部证书和内部 CA 证书

内部身份证书是特定系统或主机的证书。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名证书。

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

此外，还可以使用 OpenSSL 创建证书或从受信任的 CA 获取证书，再上传它们。有关详细信息，请参阅[上传内部证书和内部 CA 证书](#)。

有关使用这些证书的功能的信息，请参阅[功能使用的证书类型](#)。



Note 新的自签名证书生成的有效期为 5 年。请务必在证书过期前进行更换。



Warning 升级具有自签名证书的设备可能会遇到问题；有关详细信息，请参阅[检测到新证书](#)。


操作步骤

此程序可通过在向导中输入相应的证书字段值来生成自签名证书。如果要通过上传证书文件来创建内部或内部 CA 证书，请参阅[上传内部和内部 CA 证书](#)。

要生成自签名证书，请执行以下程序：

Procedure

步骤 1 执行以下操作之一：

- 在对象页面中创建证书对象：
 - a. 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
 - b. 点击加号按钮，然后选择 FTD 证书。  >
- 将新证书对象添加到策略时，点击创建新对象。

步骤 2 键入证书的名称。该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 3 在步骤 1 中，选择内部证书或内部 CA。

步骤 4 在步骤 2 中，选择自签名以在此步骤中创建自签名证书。

步骤 5 为证书主题和颁发者信息至少配置以下一项。

- 国家/地区 (Country [C]) - 从下拉列表中选择国家/地区代码。
- 州或省 (ST) (State or Province [ST]) - 证书中包括的州或省。
- 地区或城市 (Locality or City) (L) - 证书中包括的地区，例如城市名称。
- 组织 (O) (Organization [O]) - 要包含在证书中的组织或公司名称。
- 组织单位 (部门) (Organizational Unit [Department]) (OU) - 证书中包含的组织单位名称 (例如部门名称)。
- 公用名 (CN)(Common Name [CN]) - 要包含在证书中的 X.500 公用名。它们可能是设备、网站或其他文本字符串的名称。通常需要有此元素，才能成功进行连接。例如，用于远程访问 VPN 的内部证书中必须包括 CN。

步骤 6 点击添加。

配置 IPsec 提议

IPsec 是设置 VPN 的最安全方法之一。IPsec 在 IP 数据包级别提供数据加密，提供一种基于标准的强大的安全解决方案。使用 IPsec，数据通过隧道在公共网络上传输。隧道是两个对等体之间安全的逻辑通信路径。进入 IPsec 隧道的流量由称为转换集的安全协议和算法组合保护。在 IPsec 安全关联 (SA) 协商期间，对等体搜索在两个对等体处相同的转换集。

根据 IKE 版本 (IKEv1 或 IKEv2)，存在不同的 IPsec 提议对象：

- 当创建 IKEv1 IPsec 提议时，可以选择 IPsec 运行的模式，并定义所需的加密和身份验证类型。您可以为算法选择单一选项。如果要在 VPN 中支持多个组合，请创建和选择多个 IKEv1 IPsec 提议对象。
- 当创建 IKEv2 IPsec 提议时，可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序，并与对等体进行协商，直到找到匹配。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。



Note 我们建议对 IPsec 隧道使用加密和身份验证。

以下主题介绍如何为每个 IKE 版本配置 IPsec 提议：

- [创建和编辑 IKEv1 IPsec 提议对象](#)
- [创建和编辑 IKEv2 IPsec 提议对象](#)

管理 IKEv1 IPsec 提议对象

IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。IKEv1 和 IKEv2 有单独的对象。目前，Cisco Defense Orchestrator (CDO) 支持 IKEv1 IPsec 提议对象。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。



Note 我们建议对 IPsec 隧道使用加密和身份验证。

Related Topics

[创建或编辑 IKEv1 IPsec 提议对象](#)，第 209 页

创建或编辑 IKEv1 IPsec 提议对象


有几个预定义的 IKEv1 IPsec 提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象” (Objects) 页面直接创建和编辑对象。此外，也可以在编辑站点间 VPN 连接中的 IKEv1 IPsec 设置时，点击对象列表中所示的**创建新 IKEv1 提议 (Create New IKEv1 Proposal)** 链接来创建 IKEv1 IPsec 提议对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮 ，然后选择 **FTD > IKEv1 IPsec 提议 (IKEv1 IPsec Proposal)** 以创建新对象。
- 在对象页面中，选择要编辑的 IPsec 方案，然后点击右侧“操作” (Actions) 窗格中的**编辑 (Edit)**。

步骤 3 为新对象输入对象名称。

步骤 4 选择 IKEv1 IPsec 提议对象的运行模式。

- **隧道模式**会封装整个 IP 数据包。IPsec 报头被添加到原始 IP 报头和新的 IP 报头之间。这是默认值。当防火墙对出入位于防火墙后的主机的流量进行保护时，请使用隧道模式。在通过不可信网络（例如互联网）连接的两个防火墙（或其他安全网关）之间，通常采用隧道模式实施常规 IPsec。
- **传输模式**只封装 IP 数据包的上层协议。IPsec 报头被插入到 IP 报头和上层协议报头（例如 TCP）之间。传输模式要求源和目的主机都支持 IPsec，并且只有在隧道的目的对等体是 IP 数据包的最终目的时才可使用。通常只有在保护第 2 层或第 3 层隧道协议（例如 GRE、L2TP 和 DLSW）时，才会使用传输模式。

- 步骤 5** 选择加密 (**Encryption**)提议的 (封装安全协议加密) 算法。有关选项的说明, 请参阅[决定使用哪个加密算法, on page 197](#)。
- 步骤 6** 选择要用于身份验证的 **ESP 散列 (ESP Hash)** 或完整性算法。有关选项的说明, 请参阅[决定使用哪些散列算法, on page 197](#)。
- 步骤 7** 点击添加。

管理 IKEv2 IPsec 提议对象

IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。

当创建 IKEv2 IPsec 提议时, 可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序, 并与对等体进行协商, 直到找到匹配。利用这种排序, 您可以发送单个提议来传达所有允许的组合, 而无需像 IKEv1 一样逐一发送每个允许的组合。

Related Topics

[创建或编辑 IKEv2 IPsec 提议对象](#), 第 210 页

创建或编辑 IKEv2 IPsec 提议对象

有几个预定义的 IKEv2 IPsec 提议。您也可以创建新的提议, 用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects)页面直接创建和编辑对象。此外, 也可以在编辑 VPN 连接中的 IKEv2 IPsec 设置时, 点击对象列表中所指示的创建新 IPsec 提议链接来创建 IKEv2 IPsec 提议对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中, 点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一:

- 点击蓝色加号按钮 , 然后选择 **FTD > IKEv2 IPsec 提议 (IKEv2 IPsec Proposal)** 以创建新对象。
- 在对象页面中, 选择要编辑的 IPsec 方案, 然后点击右侧“操作”(Actions)窗格中的**编辑 (Edit)**。

步骤 3 为新对象输入**对象名称**。

步骤 4 配置 IKEv2 IPsec 方案对象:

- **加密** - 此提议的封装安全协议 (ESP) 加密算法。选择要允许的所有算法。系统与对等体协商, 从最强算法到最弱算法, 直到达成匹配。有关选项的说明, 请参阅[决定使用哪个加密算法, on page 197](#)。

- **完整性散列** - 要用于身份验证的散列或完整性算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅[决定使用哪些散列算法, on page 197](#)。

步骤 5 点击添加。

配置全局 IKE 策略

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。

IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用提议。IKE 提议是一组两个对等体用于保护其之间的协商的算法。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数用于保护后续 IKE 协商。

IKE 策略对象为这些协商定义 IKE 提议。您启用的对象是对等体协商 VPN 连接时使用的对象：不能为每个连接指定不同的 IKE 策略。每个对象的相对优先级确定首先尝试这些策略中的哪一个，数字越小优先级越高。如果协商无法找到两个对等体全都支持的策略，则不建立连接。

要定义全局 IKE 策略，需要为每个 IKE 版本选择启用哪些对象。如果预定义的对象不能满足您的要求，请创建新的策略来执行您的安全策略。

以下步骤说明如何通过“对象” (Objects) 页面配置全局策略。在编辑 VPN 连接时，您还可以点击 IKE 策略设置的编辑，来启用、禁用和创建策略。

以下主题介绍如何为每个 IKE 策略版本配置 IPsec 提议：

- [配置 IKEv1 策略](#)
- [配置 IKEv2 策略](#)

管理 IKEv1 策略

介绍如何创建和编辑 IKEv1 策略。

关于 IKEv1 策略

互联网密钥交换 (IKE) 版本 1 策略对象包含定义 VPN 连接时 IKEv1 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义 IKEv1 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

Related Topics

[创建或编辑 IKEv1 策略](#)，第 205 页

创建或编辑 IKEv1 策略

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。您还可以点击对象列表中所示的**创建新 IKE 策略 (Create New IKEv1 Policy)** 链接，以便在站点间 VPN 连接中编辑 IKEv1 设置时创建 IKEv1 策略对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮 ，然后选择 **FTD > IKEv1 Policy** 策略以创建新的 IKEv1 策略。
- 在对象页面中，选择要编辑的 IKEv1 策略，然后点击右侧“操作” (Actions) 窗格中的 **编辑 (Edit)**。

步骤 3 输入对象名称，最多 128 个字符。

步骤 4 配置 IKEv1 属性。

- **优先级 (Priority)** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **加密** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。有关选项的说明，请参阅“决定使用哪种加密算法”。
- **Diffie-Hellman 组** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。有关选项的解释，请看“决定要使用的 Diffie-Hellman 模数组”。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。
- **身份验证** - 在两个对等体之间使用的身份验证方法。有关详细信息，请参阅[确定使用哪种身份验证方法, on page 199](#)。
 - **预共享密钥** - 使用在每个设备上定义的预共享密钥。在身份验证阶段，此类密钥允许密钥在两个对等体之间共享并由 IKE 使用。如果未使用同一预共享密钥配置对等体，则无法建立 IKE SA。
 - **证书** - 使用对等体的设备身份证书来识别彼此。必须通过在证书颁发机构中注册每个对等体来获取这些证书。还须上传用于签署每个对等体的身份证书的受信任 CA 根证书和中间 CA 证书。对等体可以注册到相同或不同的 CA 中。对于任一对等体，都不能使用自签名证书。

- **散列** - 用于创建消息摘要的散列算法，以确保消息的完整性。有关选项的说明，请参阅 [VPN 中使用的加密和散列算法](#), on page 196。

步骤 5 点击添加。

管理 IKEv2 策略

介绍如何创建和编辑 IKEv2 策略。

关于 IKEv2 策略

互联网密钥交换 (IKE) 版本 2 策略对象包含定义 VPN 连接时 IKEv2 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv2 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

Related Topics

[创建或编辑 IKEv2 策略](#)，第 206 页


创建或编辑 IKEv2 策略

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。您还可以点击对象列表中所示的 **创建新的 IKE 策略** 链接，以便在站点间 VPN 连接中编辑 IKEv1 设置时创建 IKEv1 策略对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮 ，然后选择 **FTD > IKEv2 策略 (IKEv2 Policy)** 以创建新的 IKEv2 策略。
- 在对象页面中，选择要编辑的 IKEv2 策略，然后点击右侧“操作” (Actions) 窗格中的 **编辑 (Edit)**。

步骤 3 输入对象名称 (**object name**)，最多 128 个字符。

步骤 4 配置 IKEv2 属性。

- **优先级 (Priority)** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义参数。数值越低，优先级越高。
- **状态 (State)** - IKE 策略是启用还是禁用状态。点击开关以更改状态。在 IKE 协商期间仅使用启用的策略。
- **加密** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。选择要允许的所有算法，但不能在同一策略中同时包括混合模式 (AES-GCM) 和正常模式选项。（正常模式要

求选择完整性散列，而混合模式禁止选择单独的完整性散列。)系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅[决定使用哪个加密算法, on page 197](#)。

- **Diffie-Hellman 组** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。选择要允许的所有算法。系统与对等体协商，从最强到最弱组，直到达成匹配。有关选项的说明，请参阅[决定要使用的 Diffie-Hellman 模数组, on page 198](#)。
- **完整性散列** - 用于创建消息摘要的散列算法的完整性部分，用于确保消息完整性。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。完整性散列不与 AES-GCM 加密选项一起使用。有关选项的说明，请参阅[VPN 中使用的加密和散列算法, on page 196](#)。
- **伪随机函数 (PRF) 散列 (Pseudo-Random Function [PRF] Hash)** - 散列算法中用作派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法的伪随机函数 (PRF) 部分。在 IKEv1 中，完整性和 PRF 算法不分开，但在 IKEv2 中，可以为这些元素指定不同的算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅[VPN 中使用的加密和散列算法, on page 196](#)。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。

步骤 5 点击添加。

RA VPN 对象

安全区域对象

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

Firepower 系统会在初始配置期间创建以下区域，这些区域显示在 Defense Orchestrator 的对象页面中。您可以编辑区域以添加或移除接口；如果不再使用这些区域，也可以删除它们。

- **inside_zone** - 包括内部接口。此区域用于表示内部网络。
- **outside_zone** - 包括外部接口。此区域用于表示在您控制之外的网络，例如互联网。

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

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

相关信息：

- [创建或编辑 Firepower 安全区域对象](#)
- [将 Firepower 接口分配给安全区域](#)
- [删除对象](#)

创建或编辑 Firepower 安全区域对象

安全区是一组接口。区域将网络划分成网段，帮助您管理流量以及对流量进行分类。您可以定义多个区域，但一个给定接口只能位于一个区域中。有关详细信息，请参阅[安全区域对象](#)。

安全区域对象不与设备关联，除非在该设备的规则中使用该对象。

创建安全区域对象

要创建安全区域对象，请按照以下说明操作：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮 ，然后选择 **FTD > 安全区域 (Security Zone)** 以创建对象。

步骤 3 为对象命名，也可输入说明（可选）。

步骤 4 选择要加入安全区域的的接口。

步骤 5 点击添加。

编辑安全区域对象



自行激活设备后，您会发现至少有两个安全区域，一个是 `inside_zone`，另一个是 `outside_zone`。FDM 管理可以编辑或删除这些区域。要编辑任何安全区域对象，请按照以下说明操作：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 查找要编辑的对象：

- 如果您知道对象的名称，则可以在“对象”页面中进行搜索：
 - 按安全区域过滤列表。

- 在搜索字段中输入对象名称。
- 选择对象。
- 如果您知道对象与设备关联，则可以从“资产”页面开始搜索。
 - 在导航窗格中，点击**清单 (Inventory)**。
 - 点击**设备**选项卡。
 - 点击相应的选项卡。
 - 使用设备过滤器和搜索栏查找您的设备。[过滤器搜索](#)
 - 选择设备。
- 在右侧的“管理” (Management) 窗格中，点击  **对象 (Objects)**。
- 使用对象过滤器和搜索栏查找要查找的对象。 

Note 如果您创建的安全区域对象未与设备策略中的规则关联，则该对象将被视为“未关联”，您将不会在设备的搜索结果中看到该对象。

步骤 3 选择对象。

步骤 4 点击右侧“操作” (Actions) 窗格中的**编辑**图标 。

步骤 5 编辑对象的任何属性后。点击**保存 (Save)**。

步骤 6 点击保存后，您会收到一条消息，说明这些更改将如何影响其他设备。点击**确认 (Confirm)** 以保存更改或点击取消。

服务对象

FirePOWER 服务对象

FTD 服务对象、服务组和端口组是包含被视为 IP 协议簇一部分的协议或端口的可重用组件。

FTD 服务组是服务对象的集合。服务组可能包含一个或多个协议的对象。您可以在安全策略中使用这些对象和组来定义网络流量匹配条件，例如使用访问规则来允许流量传送至特定 TCP 端口。该系统中包括多个针对通用服务的预定义对象。您可以使用策略中的这些对象；但无法编辑或删除系统定义的对象。

Firepower 设备管理器和 Firepower 管理中心将服务对象称为端口对象以及服务组和端口组。

有关详细信息，请参阅[创建和编辑 Firepower 威胁防御服务对象](#)。

协议对象

协议对象是一种包含不太常用或传统协议的服务对象。协议对象由名称和[协议编号](#)来标识。CDO 可识别 ASA 和 Firepower (FDM 管理设备) 配置中的这些对象，并为其提供自己的“协议”过滤器，以便您可以轻松找到它们。

有关详细信息，请参阅[创建和编辑 Firepower 威胁防御服务对象](#)。

ICMP 对象

互联网控制消息协议 (ICMP) 对象是专门用于 ICMP 和 IPv6-ICMP 消息的服务对象。当 ASA 和 Firepower 配置中的这些设备已载入时，CDO 会识别这些对象，并且 CDO 会为其提供自己的“ICMP”过滤器，以便您轻松找到这些对象。

使用 CDO，您可以从 ASA 配置中重命名或删除 ICMP 对象。您可以使用 CDO 在 Firepower 配置中创建、更新和删除 ICMP 和 ICMPv6 对象。



Note 对于 ICMPv6 协议，AWS 不支持选择特定参数。仅支持允许所有 ICMPv6 消息的规则。

有关详细信息，请参阅[创建和编辑 Firepower 威胁防御服务对象](#)。

相关信息：

- [删除对象](#)

创建和编辑 Firepower 服务对象

要创建 Firepower 服务对象，请执行以下步骤：

防火墙设备管理器 (FDM 管理) 服务对象是可重用组件，可指定 TCP/IP 协议和端口。防火墙设备管理器、本地防火墙管理中心和云交付的防火墙管理中心将这些对象称为“端口对象”。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击右侧的蓝色按钮  以创建对象，然后选择 **FTD > 服务 (Service)**。

步骤 3 输入对象名称和说明。

步骤 4 选择创建服务对象 (**Create a service object**)。

步骤 5 点击**服务类型 (Service Type)** 按钮，然后选择要为其创建对象的协议。

步骤 6 按如下方式配置协议：

- **TCP、UDP**

- 选择 **eq**，然后输入端口号或协议名称。例如，您可以输入 80 作为端口号或 HTTP 作为协议名称。

- 您还可以选择范围，然后输入端口号范围，例如 **1 65535**（以涵盖所有端口）。
- **ICMP、IPv6-ICMP**-选择 ICMP 类型。选择 **Any** 类型可应用于所有 ICMP 消息。有关类型和代码的信息，请参阅以下页面：
 - ICMP-<http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml>
 - ICMPv6-<http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml>
- 其他 (**Other**) - 选择所需协议。

步骤 7 点击添加 (**Add**)。


步骤 8 [预览和部署所有设备的配置更改](#)您现在所做的更改，或者等待并一次部署多个更改。

创建 Firepower 服务组

服务组可以由代表一个或多个协议的一个或多个服务对象组成。需要先创建服务对象，然后才能将其添加到组。Firepower 设备管理器和 Firepower 管理中心将这些对象称为“端口对象”。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击右侧的蓝色按钮  以创建对象，然后选择 **FTD > 服务 (Service)**。

步骤 3 输入对象名称和说明。

步骤 4 选择创建服务组 (**Create a service group**)。

步骤 5 通过点击添加对象 (Add Object) 将对象添加到组。

- 点击创建以创建新对象，就像上面创建 Firepower 服务对象中的操作一样。[创建和编辑 Firepower 服务对象](#)
- 点击选择 (Choose) 以将现有服务对象添加到组。重复此步骤以添加更多对象。

步骤 6 将服务对象添加到服务组后，点击添加。


步骤 7 [预览和部署所有设备的配置更改](#)您现在所做的更改，或者等待并一次部署多个更改。

编辑 Firepower 服务对象或服务组

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 过滤对象以查找要编辑的对象，然后在对象表中选择该对象。

步骤 3 在“操作”(Actions)窗格中, 点击编辑 (**Edit**) 。

步骤 4 以在上述过程中创建值的相同方式编辑对话框中的值。

步骤 5 点击保存 (**Save**)。

步骤 6 CDO 显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

步骤 7 [预览和部署所有设备的配置更改](#)您现在所做的更改, 或者等待并一次部署多个更改。

安全组标记组

安全组标记

关于安全组标记

如果使用思科身份服务引擎 (ISE) 定义并使用安全组标记 (SGT) 来对 Cisco TrustSec 网络中的流量进行分类, 则可以编写使用 SGT 作为匹配条件的访问控制规则。因此, 可以基于安全组成员身份阻止或允许访问, 而不是使用 IP 地址。

在 ISE 中, 您可以创建 SGT, 并将主机或网络 IP 地址分配至各标记。如果您将 SGT 分配给用户帐户, SGT 就会被分配给用户流量。将 FDM 管理设备配置为连接到 ISE 服务器并创建 SGT 后, 您可以在思科防御协调器中创建 SGT 组并围绕它们构建访问控制规则。请注意, 您必须先配置 ISE 的 SGT 交换协议 (SXP) 映射, 然后才能将 SGT 关联到 FDM 管理设备。有关详细信息, 请参阅您当前运行的版本的《[思科身份服务引擎管理员指南](#)》中的[安全组标记交换协议](#)。

FDM 管理设备评估 SGT 作为访问控制规则的流量匹配条件时, 会使用以下优先级:

1. 数据包中定义的源 SGT (如有)。使用此技术无法进行目的地匹配。对于数据包中的 SGT, 必须配置网络中的交换机和路由器以添加它们。有关如何实施此方法的信息, 请参阅 ISE 文档。
2. 分配给用户会话的 SGT, 从 ISE 会话目录下载。您需要启用此选项才能侦听此类 SGT 匹配的会话目录信息, 但是, 当您首次创建 ISE 身份源时, 此选项会默认打开。SGT 可以与源或目标相匹配。尽管非必需, 但您通常还会使用 ISE 身份源和 AD 域来设置被动身份验证身份规则, 以收集用户身份信息。
3. 使用 SXP 下载的 SGT-IP 地址映射。如果 IP 地址在 SGT 范围内, 则流量与使用 SGT 的访问控制规则相匹配。SGT 可以与源或目标相匹配。



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

版本支持

CDO 当前在运行 6.5 和更高版本的 FDM 管理 设备上支持 SGT 和 SGT 组。FDM 管理 设备允许您在版本 6.5 及更高版本中配置并连接到 ISE 服务器，但在 6.7 之前版本中不支持在 UI 中配置 SGT。

从 FDM 管理 UI 中，这意味着运行版本 6.5 或更高版本的 FDM 管理 设备可以下载 SGT 的 SXP 映射，但不能手动添加到对象或访问控制规则。要更改运行版本 6.5 或版本 6.6 的设备的 SGT，您必须使用 ISE UI。但是，如果运行版本 6.5 的设备已被载入 思科防御协调器，则可以查看与设备关联的当前 SGT 并创建 SGT 组。

CDO 中的 SGT

安全组标记

SGT 在 CDO 中为只读。您无法在 CDO 中创建或编辑 SGT。要创建 SGT，请参阅当前运行版本的《[思科身份服务引擎管理员指南](#)》。

SGT 组



Note FDM 管理 设备将 SGT 组称作 SGT 动态对象。在 CDO 中，这些标签列表当前被称作 SGT 组。您可以在 CDO 中创建 SGT 组，而无需参考 FDM 管理 设备或 ISE UI。

使用 SGT 组可以根据 ISE 分配的 SGT 来识别源或目标地址。然后，可以将访问控制规则中的对象用于定义流量匹配条件。您无法直接在访问控制规则中使用从 ISE 检索到的信息。相反，您需要创建引用已下载 SGT 信息的 SGT 组。

您的 SGT 组可以引用多个 SGT，因此您可以在适当的情况下根据相关的标记集合应用策略。

要在 CDO 中创建 SGT 组，必须至少已经配置一个 SGT，并为要使用的设备的 FDM 管理 控制台配置来自 ISE 服务器的 SGT 映射。请注意，如果多个 FDM 管理 设备与同一 ISE 服务器关联，则可以将 SGT 或 SGT 组应用于多个设备。如果设备未与 ISE 服务器关联，则不能在访问控制规则中包含 SGT 对象，也不能将 SGT 组应用于该设备配置。

规则中的 SGT 组

SGT 组可被添加到访问控制规则；它们会显示为源或目标网络对象。有关网络如何在规则中工作的详细信息，请参阅 [FDM 管理 访问控制规则中的源和目标条件](#)。

您可以从“对象” (Objects) 页面创建 SGT 组。有关详细信息，请参阅 [创建 SGT 组](#)。

创建 SGT 组

要创建可用于访问控制规则的 SGT 组，请使用以下程序：

Before you begin


在创建安全组标记 (SGT) 组之前，必须配置以下配置或环境：

- FDM 管理 设备必须至少运行版本 6.5。

- 必须配置 ISE 身份源以订用 SXP 映射并启用部署更改。要管理 SXP 映射，请参阅所用版本（版本 6.7 及更高版本）的 [Firepower 设备管理器配置指南](#) 中的在 ISE 中配置安全组和 SXP 发布。
- 所有 SGT 都必须在 ISE 中创建。要创建 SGT，请参阅当前运行版本的《[思科身份服务引擎配置指南](#)》。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮  以创建新的对象。

步骤 3 点击 **FTD > 网络 (Network)**。

步骤 4 输入 **对象名称 (Object Name)**。

步骤 5 （可选）添加说明。

步骤 6 点击 **SGT** 并使用下拉菜单选中要包含在组中的所有适用 SGT。您可以按 SGT 名称对列表进行排序。

步骤 7 点击 **保存 (Save)**。

Note 您无法在 CDO 中创建或编辑 SGT，只能在 SGT 组中添加或删除它们。要创建或编辑 SGT，请参阅当前运行版本的《[思科身份服务引擎配置指南](#)》。


编辑 SGT 组

要编辑 SGT 组，请使用以下程序：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到您要编辑的 SGT 组。

步骤 3 选择 SGT 组，然后点击 **操作 (Actions)** 窗格中的编辑图标 。

步骤 4 修改 SGT 组。编辑与该组关联的名称、说明或 SGT。


步骤 5 点击 **保存 (Save)**。

Note 您无法在 CDO 中创建或编辑 SGT，只能在 SGT 组中添加或删除它们。要创建或编辑 SGT，请参阅当前运行版本的《[思科身份服务引擎配置指南](#)》。

将 SGT 组添加到访问控制规则

要将 SGT 组添加到访问控制规则，请使用以下程序：

Procedure

- 步骤 1 在导航窗格中，点击**清单 (Inventory)**。
- 步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
- 步骤 3 点击 FTD 选项卡，然后选择要向其添加 SGT 组的设备。
- 步骤 4 在**管理 (Management)** 窗格中，选择**策略 (Policy)**。
- 步骤 5 点击源或目标对象的蓝色加号按钮，然后选择 SGT 组。 
- 步骤 6 使用对象过滤器和搜索字段找到您要编辑的 SGT 组。
- 步骤 7 点击**保存 (Save)**。
- 步骤 8 [预览和部署所有设备的配置更改](#)。

Note 如果需要创建其他 SGT 组，请点击创建新对象。填写创建 FTD SGT 组并将 SGT 组添加到规则中提到的必填信息。 [创建 SGT 组](#)


系统日志服务器对象

FDM 管理设备用来存储事件的容量有限。要尽可能提高事件存储量，您可以配置外部服务器。系统日志 (syslog) 服务器对象标识可接收面向连接的消息或诊断 syslog 消息的服务器。如果已为日志收集和分析设置一台系统日志服务器，您可以使用思科防御协调器来创建对象以进行定义并在相关策略中使用这些对象。

创建和编辑系统日志服务器对象

要创建新的系统日志服务器对象，请执行以下步骤：

Procedure

- 步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
- 步骤 2 点击**创建对象 (Create Object)** 按钮 。
- 步骤 3 选择 FDM 管理设备对象类型下方的**系统日志服务器 (Syslog Server)**
- 步骤 4 配置系统日志服务器对象属性：
 - **IP 地址** - 输入系统日志服务器的 IP 地址。
 - **协议类型 (Protocol Type)** - 选择系统日志服务器用于接收消息的协议。如果您选择 TCP，系统可以识别何时系统日志服务器不可用，并停止发送事件，直至服务器再次可用。
 - **端口号 (Port Number)** - 输入要用于系统日志的有效端口号。如果系统日志服务器使用默认端口，请输入 514 作为默认 UDP 端口或 1470 作为默认 TCP 端口。如果服务器不使用默认端口，请输入正确的端口号。端口范围必须介于 1025 至 65535 之间。

- **选择接口**-选择应使用哪个接口发送诊断系统日志消息。连接和入侵事件始终使用管理接口。接口选择决定与系统日志消息关联的 IP 地址。请注意，您只能选择下面列出的选项之一。不能同时选择两者。选择以下选项之一：
 - **数据接口** - 选择用于诊断系统日志消息的数据接口。从生成列表中选择接口。如果可以通过网桥组成员接口访问该服务器，请选择该网桥组接口 (BVI)。如果通过诊断接口（物理管理接口）访问，我们建议您选择管理接口，而不是此选项。您不能选择被动接口。对于连接和入侵系统日志消息，源 IP 地址是管理接口的地址；如果您通过数据接口进行路由，则是网关接口的地址。
 - **管理接口** - 对所有类型的系统日志消息使用虚拟管理接口。源 IP 地址是管理接口的地址；如果您通过数据接口进行路由，则是网关接口的地址。

步骤 5 点击添加 (Add)。

步骤 6 立即 [预览和部署所有设备的配置更改](#) 您所做的更改，或等待并一次部署多个更改。

编辑系统日志服务器对象

要编辑现有的系统日志服务器对象，请执行以下步骤：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 找到所需的系统日志服务器对象并选择它。您可以按系统日志服务器对象类型过滤对象列表。

步骤 3 在“操作” (Actions) 窗格中，点击 **编辑 (Edit)**。

步骤 4 进行所需的编辑，然后点击 **保存 (Save)**。

步骤 5 确认您所做的更改。

步骤 6 立即 [预览和部署所有设备的配置更改](#) 您所做的更改，或等待并一次部署多个更改。

相关信息：

- [删除对象](#)

为安全日志记录分析 (SaaS) 创建系统日志服务器对象

使用要向其发送事件的安全事件连接器 (SEC) 的 IP 地址、TCP 端口或 UDP 端口创建系统日志服务器对象。您将为已载入租户的每个 SEC 创建一个系统日志对象，但您只能将来自一个规则的事件发送到一个代表一个 SEC 的系统日志对象。

前提条件

此任务是更大工作流程的一部分。开始前，请参阅 [为 FDM 管理设备实施安全日志记录分析 \(SaaS\)](#)。

操作步骤

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击创建对象 (**Create Object**) 按钮 。

步骤 3 选择 FDM 管理 设备对象类型下方的系统日志服务器 (**Syslog Server**)。

步骤 4 配置系统日志服务器对象属性。要查找 SEC 的这些属性，请从 CDO 菜单中选择**管理 (Admin) > 安全连接器 (Secure Connectors)**。然后，选择要为其配置系统日志对象的安全事件连接器，并查看右侧的“详细信息”窗格。

- **IP 地址 (IP Address)** - 输入 SEC 的 IP 地址。
- **协议类型** - 选择 TCP 或 UDP。
- **端口号** - 如果您选择了 TCP，请输入端口 10125；如果您选择了 UDP，请输入 10025。
- **选择接口** - 选择配置用于访问 SEC 的接口。

Note FDM 管理 设备支持每个 IP 地址一个系统日志对象，因此您必须在使用 TCP 和 UDP 之间进行选择。

步骤 5 点击添加 (**Add**)。

What to do next

继续步骤 3 [实施安全日志记录分析 \(SaaS\)](#) 并通过[安全事件连接器](#)将事件发送到思科云的现有 [CDO 客户工作流程](#)。

URL 对象

URL 对象和 URL 组由 Firepower 设备使用。使用 URL 对象和组（统称为“URL 对象”）可定义 Web 请求的 URL 或 IP 地址。可以使用这些对象在访问控制策略中执行手动 URL 过滤，或在安全情报策略中进行阻止。URL 对象定义单个 URL 或 IP 地址，而 URL 组可以定义多个 URL 或地址。

准备工作

在创建 URL 对象时，请记住以下要点：

- 如果不包含路径（即 URL 中无 / 字符），则匹配仅基于服务器主机名。如果主机名位于 :// 分隔符之后，或在主机名中的任何点之后，则认为该主机名匹配。例如，ign.com 匹配 ign.com 和 www.ign.com，但不匹配 verisign.com。
- 如果包含一个或多个 / 字符，则整个 URL 字符串将用于子字符串匹配，其中包括服务器名称、路径和任何查询参数。但是，我们建议您不要使用手动 URL 过滤阻止或允许个别网页或部分网

站，因为这样可能会重组服务器并将页面移至新路径。子字符串匹配还可能导致意外匹配，其中 URL 对象中包含的字符串也与非预期服务器上的路径或查询参数中的字符串匹配。

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

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



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

创建或编辑 FDM 管理 URL 对象

URL 对象是指定 URL 或 IP 地址的可重用组件。

要创建 URL 对象，请执行以下步骤：

Procedure

- 步骤 1** 在左侧的 思科防御协调器 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
- 步骤 2** 点击创建对象 **创建对象 (Create Object) > FTD > URL**。
- 步骤 3** 输入对象名称和说明。
- 步骤 4** 选择创建 **URL 对象 (Create a URL object)**。
- 步骤 5** 为对象输入特定 URL 或 IP 地址。
- 步骤 6** 点击添加。

创建 Firepower URL 组


URL 组可以由表示一个或多个 URL 或 IP 地址的一个或多个 URL 对象组成。Firepower 设备管理器和 Firepower 管理中心也将这些对象称为“URL 对象”。

Procedure

- 步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
 - 步骤 2 点击 **创建对象 (Create Object) > FTD > URL**。
 - 步骤 3 输入对象名称和说明。
 - 步骤 4 选择 **创建 URL 组 (Create a URL group)**。
 - 步骤 5 通过点击 **添加对象 (Add Object)**，选择一个对象，然后点击 **选择 (Select)**，添加现有对象。重复此步骤以添加更多对象。
 - 步骤 6 将 URL 对象添加到 URL 组后，点击 **添加**。
-

编辑 Firepower URL 对象或 URL 组

Procedure

- 步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
 - 步骤 2 过滤对象以查找要编辑的对象，然后在对象表中选择该对象。
 - 步骤 3 在详细信息窗格中，点击  以进行编辑。
 - 步骤 4 以在上述过程中创建值的相同方式编辑对话框中的值。
 - 步骤 5 点击 **保存 (Save)**。
 - 步骤 6 CDO 显示将受更改影响的策略。点击 **确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。
-

安全策略管理

安全策略检查网络流量，最终目标是允许流量到达其预定目的地，或者在识别出安全威胁时丢弃该流量。您可以使用 CDO 在许多不同类型的设备上配置安全策略。

- [FDM 策略配置，第 98 页](#)
- [网络地址转换，第 175 页](#)

FDM 策略配置

安全策略检查网络流量，最终目标是允许流量到达其预定目的地，或者在识别出安全威胁时丢弃该流量。使用 CDO 来管理 FDM 管理设备的所有安全策略组件：

FDM 管理 访问控制策略

您可以使用 思科防御协调器 来管理 FDM 管理 设备的访问控制策略。访问控制策略通过根据访问控制规则评估网络流量来控制对网络资源的访问。FDM 管理 设备会按照访问控制规则在访问控制策略中的显示顺序，将其与网络流量进行比较。当访问控制规则中的所有流量条件均为

- 信任 - 允许流量，而无需进行任何类型的进一步检测。
- 允许 - 允许流量，不受策略中的入侵及其他检测设置约束。
- 阻止 - 无条件地丢弃流量。不检测流量。

如果访问控制策略中的任何规则都与网络流量不匹配，则 FDM 管理 设备将采取访问控制规则下面列出的默认操作。

读取 FDM 管理 访问控制策略

Procedure

- 步骤 1 在导航窗格中，点击**清单 (Inventory)**。
- 步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
- 步骤 3 点击 **FTD** 选项卡，然后选择要读取其策略的设备。
- 步骤 4 在右侧的**管理 (Management)** 窗格中，选择 **策略 (Policy)**。
- 步骤 5 要确保您看到整个策略，请点击“过滤器” (Filter) 面板中的**全部显示 (Show All)**。
- 步骤 6 将显示切换规则列，以便查看具有更多或更少列的规则。如果您习惯于查看 FDM 管理设备中的访问控制规则，请切换规则列显示以显示更多列。



以下是如何读取策略中的规则的示例。首先根据规则 1 评估所有流量是否匹配。如果流量与规则 1 匹配，则该规则的操作将应用于流量。源自内部区域的流量，AND 源自非洲或澳大利亚，AND 源自 HTTP 或 HTTPS 端口，AND 到达外部区域，AND 到达奥兰群岛或阿尔巴尼亚，AND 到达任何端口，AND 到达 ABC OR 允许 About.com 从源流向目的地。我们还可以看到，入侵策略和文件策略已应用于规则，并且正在记录规则中的事件。

#	Name	Action	Source			Destination			Layer 7			Users
			Zones	Networks	Ports	Zones	Networks	Ports	Applications	URLs		
1	Allow in...	Allow	inside	Africa Australia	HTTP HTTPS	outside	Aland Islands Albania	Any	ABC About.com	Any	Any	
2	Block o...	Block	outside	Any	Any	inside	Any	Any	Social Net... (Sites with Security...) Gambling (Any Reputation)	Any	Any	

Default Action: Allow

相关信息：

- [配置 FDM 访问控制策略](#)

配置 FDM 访问控制策略

FDM 管理设备有一个策略。该策略的一部分具有访问控制规则。为便于讨论，我们将具有访问控制规则的策略部分称为访问控制策略。载入 FDM 管理设备后，您可以向访问控制策略添加规则或在其中编辑规则。

如果您要载入新的 FDM 管理设备，则导入的策略中可能没有任何规则。在这种情况下，当您打开 FDM 策略页面时，您将看到消息“未找到结果”(No results found)。如果看到该消息，则可以开始将规则添加到 FDM 托管设备策略，然后从 CDO 将其部署到设备。

开始之前的提示


向访问控制规则中添加条件时，请考虑以下提示：




- 您可以在将某些条件添加到规则时为其创建自定义对象。在对话框中查找用于创建自定义对象的链接。
- 您可以为每个规则配置多个条件。要使规则应用于流量，流量必须匹配该规则中的所有条件。例如，可以使用单一规则对特定主机或网络执行 URL 过滤。
- 最多可以为规则中的每个条件添加 50 个标准。匹配某个条件所有条件标准的流量满足该条件。例如，您可以使用单一规则为最多 50 个应用或应用过滤器执行应用控制。因此，单一条件中的项目之间为 OR 关系，但不同条件类型之间（例如，源/目的和应用之间）为 AND 关系。
- 有些功能需要您启用适当的 Firepower 许可证。
- 某些编辑任务可能不需要您进入编辑模式。从策略页面，您可修改规则中的条件，通过点击该条件栏内的 + 按钮，选择弹出对话框中的所需的对象或元素。您也可以点击对象或元素对应的 x，可将其从规则中移除。

创建或编辑 FDM 管理访问控制策略

按照以下程序使用 思科防御协调器 编辑 FDM 管理访问控制策略：

Procedure

- 步骤 1 在导航窗格中，点击**清单 (Inventory)**。
- 步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
- 步骤 3 点击**FTD** 选项卡，然后选择要编辑其策略的访问控制。
- 步骤 4 在右侧的**管理 (Management)** 窗格中，选择  **策略 (Policy)**。
- 步骤 5 执行以下任一操作：

- 要创建新规则，请点击蓝色加号按钮 。
- 要编辑现有规则，请选择该规则，然后点击**操作 (Actions)** 窗格中的编辑图标 。（也可以在不进入编辑模式的情况下内联执行简单编辑。）
- 要删除不再需要的规则，请选择该规则，然后点击“操作” (Actions) 窗格中的删除图标 。
- 要移动策略中的规则，请在访问控制表中选择该规则，然后点击规则行末尾的向上或向下箭头以移动该规则。

在编辑或添加规则时，请继续执行此程序中的其他步骤。

- 步骤 6 在**顺序 (Order)** 字段中，选择规则在策略中的位置。根据规则列表（按数字顺序从 1 到“最后” (last)）评估网络流量。

先匹配的规则先应用，所以您必须确保流量匹配条件标准较具体的规则显示在次之用来匹配流量的较通用条件标准的策略上方。

默认将规则添加到列表的末尾。如果以后要更改规则的位置，请编辑此选项。

- 步骤 7 输入规则名称。可以使用字母数字字符和以下特殊字符：+ . _ -
- 步骤 8 选择规则匹配网络流量时要应用的操作：

- **信任** - 允许流量，而无需进行任何类型的进一步检测。
- **允许** - 允许流量，不受策略中的入侵及其他检测设置约束。
- **阻止** - 无条件地丢弃流量。不检测流量。

- 步骤 9 通过使用以下选项卡的任意属性组合，定义流量匹配标准：

- **源 (Source)** - 点击**源 (Source)** 并添加或删除安全区域（接口）、网络（包括网络、大洲和自定义地理位置）或网络流量来源的端口。默认值为“任意” (Any)。
- **目标 (Destination)** - 点击**目标 (Destination)** 选项卡，然后添加或删除流量到达的安全区域（接口）、网络（包括网络、大洲和自定义地理位置）或端口。默认值为“任意” (Any)。请参阅 [FDM 管理 访问控制规则中的源和目标条件](#)。
- **应用 (Application)** - 点击**应用 (Application)**，然后添加或删除网络应用，或根据类型、类别、标签、风险或业务相关性定义应用的过滤器。默认设置为任何应用。请参阅 [FDM 管理 访问控制规则中的应用条件](#)

- **URL** - 点击 **URL** 选项卡，然后添加或删除 Web 请求的 URL 或 URL 类别。默认设置为任何 URL。请参阅 [FDM 管理 访问控制规则中的 URL 条件](#)，了解如何使用 URL 类别和信誉过滤器来调整该条件。
- **用户 (Users)** - 在规则行中可以看到从 防火墙设备管理器 添加到规则中的 Active Directory 领域对象、特殊身份（身份验证失败、访客、无需身份验证、未知）和用户组，但在 CDO 中尚不可编辑。

Caution 单个用户对象在 CDO 中的访问控制策略规则中不可见。登录到 FDM 管理设备以查看单个用户对象会如何影响访问控制策略规则。

步骤 10 （可选，对于具有“允许” (Allow) 操作的规则）点击 **入侵策略 (Intrusion Policy)** 选项卡，分配入侵检测策略，以检测流量是否存在入侵和漏洞。请参阅 [在 FDM 管理 访问控制规则中选择入侵策略](#)。

a. 要记录入侵策略规则生成的入侵事件，请参阅设备的“[FDM 管理 设备设置](#)”。

步骤 11 （可选，对于具有“允许” (Allow) 操作的规则）点击 **文件策略 (File Policy)** 选项卡，以分配检查包含恶意软件的文件和应阻止的文件的流量的文件策略。请参阅 [FDM 管理 访问控制规则中的文件策略设置](#)。

a. 要记录入侵策略规则生成的文件事件，请参阅设备的“[FDM 管理 设备设置](#)”。

步骤 12 （可选）点击日志记录选项卡以启用日志记录，并收集访问控制规则报告的**连接事件**。

有关日志记录设置的详细信息，请参阅 [FDM 管理 访问控制规则中的日志记录设置](#)。

如果您订用了思科安全分析和日志记录，则可以通过[配置带有 SEC IP 地址和端口的系统日志对象](#)，在 CDO 中配置连接事件并将其发送到安全事件连接器 (SEC)。有关此功能的详细信息，请参阅[思科安全分析和日志记录](#)。您将为已载入租户的每个 SEC 创建一个系统日志对象，但您只能将由一个规则生成的事件发送到一个代表一个 SEC 的系统日志对象。

步骤 13 点击 **保存 (Save)**。您现在已在安全策略中配置了特定的规则。

步骤 14 您现在可以配置整个安全策略的**默认操作**。“默认操作”定义了网络流量与访问控制策略、入侵策略或文件/恶意软件策略中的任何规则都不匹配时会发生的情况。

步骤 15 点击策略的默认操作。

步骤 16 按照上面的步骤 9 配置入侵策略。

步骤 17 配置默认操作生成的日志记录连接事件。

如果您订用了思科安全分析和日志记录，则可以通过[配置带有 SEC IP 地址和端口的系统日志对象](#)，将默认操作生成的事件发送到安全事件连接器 (SEC)。有关此功能的详细信息，请参阅[思科安全分析和日志记录](#)。您将为已载入租户的每个 SEC 创建一个系统日志对象，但您只能将由规则生成的事件发送到一个代表一个 SEC 的系统日志对象。

步骤 18 （可选）对于您创建的任何规则，您可以选择它并在“添加注释” (Add Comments) 字段中添加注释。要了解有关规则注释的详细信息，请参阅[向策略和规则集中的规则添加注释](#)。

步骤 19 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

配置访问策略设置

您可以配置应用于访问策略而不是策略中特定规则的设置。

操作步骤

这些设置适用于整个访问策略，而不是策略中的特定规则。

过程

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击**FTD** 选项卡，然后选择要编辑其策略的访问控制。

步骤 4 在右侧的**管理 (Management)** 窗格中，选择  **策略 (Policy)**。

步骤 5 点击**设置 (Settings)** 图标并配置以下设置：

- **TLS 服务器身份发现 (TLS Server Identity Discovery)** - TLS 1.3 证书已加密。对于使用 TLS 1.3 加密的流量，要匹配使用应用或 URL 过滤的访问规则，系统必须对 TLS 1.3 证书进行解密。建议您启用此选项，以确保将加密连接与正确的访问控制规则进行匹配。此设置仅解密证书；连接保持加密状态。启用此选项即可解密 TLS 1.3 证书；您无需创建相应的 SSL 解密规则。可用于运行 6.7 或更高版本软件的 FDM 管理设备。
- **DNS 流量的信誉实施 (Reputation Enforcement on DNS Traffic)** - 启用此选项可将 URL 过滤类别和信誉规则应用于 DNS 查找请求。如果查找请求中的完全限定域名 (FQDN) 具有要阻止的类别和信誉，系统会阻止 DNS 回复。由于用户未收到 DNS 解析，因此用户无法完成连接。使用此选项可将 URL 类别和信誉过滤应用于非 Web 流量。有关详细信息，请参阅 DNS 请求过滤。适用于运行 7.0 及更高版本软件的 FDM 管理设备。

步骤 6 点击**保存 (Save)**。

关于 TLS 服务器身份发现

通常情况下，TLS 1.3 证书已加密。对于使用 TLS 1.3 加密的流量，要匹配使用应用或 URL 过滤的访问规则，系统必须对 TLS 1.3 证书进行解密。我们建议您启用早期应用检测和 URL 分类，以确保将加密连接与正确的访问控制规则进行匹配。该设置仅解密证书；连接保持加密状态。





Note 此功能当前可用于运行 6.7 或更高版本软件的 FDM 管理设备。

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

- 步骤 3 点击 **FTD** 选项卡，然后选择要编辑其策略的访问控制。
- 步骤 4 在右侧的**管理 (Management)** 窗格中，选择  **策略 (Policy)**。
- 步骤 5 点击设置  按钮。
- 步骤 6 点击 **TLS 服务器身份发现 (TLS Server Identity Discovery)** 旁边的滑块，为加密连接启用早期应用检测和 URL 分类。
- 步骤 7 点击保存 (**Save**)。

复制 FDM 管理 访问控制规则

使用此程序复制访问控制规则，方法是将其从当前位置复制并粘贴到同一策略中的新位置，或者将其粘贴到不同 FDM 管理 设备的策略。您可以将规则粘贴在策略中的其他规则之前或之后，以便规则按其策略中的正确顺序评估该网络流量。

在设备中复制规则

要复制 FDM 管理 设备中的规则，请执行以下程序：

Procedure

- 步骤 1 在导航窗格中，点击**清单 (Inventory)**。
- 步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
- 步骤 3 点击 **FTD** 选项卡，然后选择要编辑其策略的 FDM 管理 设备。
- 步骤 4 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。
- 步骤 5 选择要复制的一个或多个访问控制规则，然后点击右侧**操作 (Actions)** 窗格中的**复制 (Copy)**。
- 步骤 6 在要粘贴规则的策略中，选择复制的规则应在其前面或后面的规则，然后在**操作 (Actions)** 窗格中，点击以下选项之一：
 - **粘贴前 (Paste Before)** 会自动将一个或多个复制的规则粘贴到所选规则上方，以便复制的规则排在其上方。
 - **粘贴后 (Paste After)** 会自动将一个或多个复制的规则粘贴到所选规则的下方，以便复制的规则排在其下方。

可以在任何所需位置多次执行粘贴操作。

Note 在 FDM 管理 设备中粘贴规则时，如果存在具有相同名称的规则，则会将“-Copy”附加到原始名称。如果重命名的名称也存在，则会将“- Copy n”附加到原始名称。例如，“rule name - Copy 2”。

- 步骤 7 立即查看您的更改并将配置更改从 [CDO 部署到 FDM 管理 设备](#)，或者等待并一次部署多个更改。
-

将规则从一个 FDM 管理设备策略复制到另一个 FDM 管理设备策略

将规则从一个 FDM 管理设备策略复制到另一个 FDM 管理设备策略时，与这些规则关联的对象也会被复制到新的 FDM 管理设备。

在粘贴规则时，CDO 会验证某些条件。有关详细信息，请参阅[将规则粘贴到另一个设备时的对象行为](#)。



Important

重要提示：仅当两台设备上的相同软件版本相同时，CDO 才允许您将规则从一台 FDM 管理设备复制到另一台 FDM 管理设备。如果软件版本不同，当您尝试粘贴规则时，系统会显示“规则无法粘贴，因为它们与此设备的版本不兼容” (Rules could not be pasted because they are not compatible with the version of this device)。您可以点击[详细信息 \(Details\)](#) 链接以了解详细信息。

要将规则复制到另一台 FDM 管理设备，请执行以下程序：

Procedure

- 步骤 1 在导航窗格中，点击**清单 (Inventory)**。
- 步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
- 步骤 3 点击**FTD** 选项卡，然后选择要从中复制规则的设备。
- 步骤 4 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。
- 步骤 5 选择要复制的一个或多个访问控制规则，然后点击右侧**操作 (Actions)** 窗格中的**复制 (Copy)**。
- 步骤 6 点击**清单 (Inventory)** 并导航至要将规则复制到的 FDM 管理设备。
- 步骤 7 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。
- 步骤 8 在要粘贴刚才所复制规则的策略中，选择复制的规则应在其前面或后面的规则，然后在**操作 (Actions)** 窗格中，点击**粘贴在前 (Paste Before)** 或**粘贴在后 (Paste After)**。
- 步骤 9 选择要在其周围粘贴复制的规则的任何访问控制规则，然后在**操作 (Actions)** 窗格中点击以下选项之一：
 - **粘贴在前 (Paste Before)** 会自动将一个或多个规则置于所选规则之上，以便复制的规则在所选规则之前评估网络流量。
 - **粘贴在后 (Paste After)** 会在选定规则下自动粘贴一个或多个规则，以便复制的规则在选定规则之后评估网络流量。

可以在任何所需位置多次执行粘贴操作。

Note

在将规则粘贴到另一台 FDM 管理设备时，如果存在具有相同名称的规则，则会将“- Copy”附加到原始名称。如果重命名的名称也存在，则会将“- Copy n”附加到原始名称。例如，“rule name-Copy 2”。

- 步骤 10** 在将规则从一台 FDM 管理设备复制到另一台设备时，目标设备的配置状态 (**Configuration Status**) 将处于“未同步” (Not Synced) 状态。立即查看您的更改并将配置更改从 CDO 部署到 FDM 管理设备，或者等待并一次部署多个更改。

相关信息：

- [移动 FDM 管理 访问控制规则](#)
- [将规则粘贴到另一个设备时的对象行为](#)

移动 FDM 管理 访问控制规则

使用此功能可移动访问控制规则，方法是将其从策略中的当前位置剪切，并将其粘贴到同一策略中的新位置或不同 FDM 管理设备的策略中。您可以将规则粘贴在策略中的其他规则之前或之后，以便规则在策略中按其适当的顺序评估该网络流量。

在设备内移动规则

要在 FDM 管理设备内移动规则，请执行以下程序：

Procedure

- 步骤 1** 在导航窗格中，点击**清单 (Inventory)**。
- 步骤 2** 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
- 步骤 3** 点击**FTD** 选项卡，然后选择您要编辑其策略的 FDM 管理设备。
- 步骤 4** 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。
- 步骤 5** 选择要移动的一个或多个访问控制规则，然后点击右侧“操作” (Actions) 窗格中的**剪切 (Cut)**。您选择的规则将以黄色突出显示。**注意：**如果要取消选择，请选择任何规则，然后点击**复制 (Copy)**。
- 步骤 6** 在要粘贴刚才所剪切规则的策略中，选择剪切的规则应在其前面或后面的规则，然后在**操作 (Actions)** 窗格中，点击以下选项之一：
- **粘贴在前 (Paste Before)** 会自动将一个或多个规则粘贴在所选规则之上，以便剪切的规则在所选规则之前评估网络流量。
 - **粘贴在后 (Paste After)** 会在选定规则下自动粘贴一个或多个规则，以便剪切规则在选定规则之后评估网络流量。

可以在任何所需位置多次执行粘贴操作。

Note 在 FDM 管理设备中粘贴规则时，如果存在具有相同名称的规则，则会将“-Copy”附加到原始名称。如果重命名的名称也存在，则会将“- Copy n”附加到原始名称。例如，“rule name - Copy 2”。

- 步骤 7** 立即查看您的更改并将配置更改从 CDO 部署到 FDM 管理设备，或者等待并一次部署多个更改。
-

将规则从一个 FDM 管理设备策略移至另一个 FDM 管理设备策略

将规则从一个 FDM 管理设备策略移动到另一个 FDM 管理设备策略时，与这些规则关联的对象也会被复制到新的 FDM 管理设备。

在粘贴规则时，CDO 会验证某些条件。有关这些条件的详细信息，请参阅[将规则粘贴到另一个设备时的对象行为](#)。

要将规则移至另一台 FDM 管理设备，请执行以下程序：

Procedure

- 步骤 1 在导航窗格中，点击**清单 (Inventory)**。
- 步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
- 步骤 3 点击**FTD** 选项卡，然后选择要从中复制规则的 FDM 管理设备。
- 步骤 4 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。
- 步骤 5 选择要移动的一个或多个访问控制规则，然后点击右侧**操作 (Actions)** 窗格中的**剪切 (Cut)**。
- 步骤 6 点击**清单 (Inventory)** 并导航至要将一个或多个选定规则移动到的 FDM 管理设备。
- 步骤 7 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。
- 步骤 8 在要粘贴刚才所剪切规则的策略中，选择剪切的规则应在其前面或后面的规则，然后在**操作 (Actions)** 窗格中，点击**粘贴在前 (Paste Before)** 或**粘贴在后 (Paste After)**。

- **粘贴在前 (Paste Before)** 会自动将一个或多个规则置于所选规则之上，以便剪切的规则在所选规则之前评估网络流量。
- **粘贴在后 (Paste After)** 会在选定规则下自动粘贴一个或多个规则，以便剪切规则在选定规则之后评估网络流量。

可以在任何所需位置多次执行粘贴操作。

Note 在 FDM 管理设备中粘贴规则时，如果存在具有相同名称的规则，则会将“- Copy”附加到原始名称。如果重命名的名称也存在，则会将“- Copy n”附加到原始名称。例如，“rule name - Copy 2”。

- 步骤 9 在将规则从一台 FDM 管理设备复制到另一台设备时，源设备和目标设备的**配置状态 (Configuration Status)** 将处于“未同步” (Not Synced) 状态。立即查看您的更改并[将配置更改从 CDO 部署到 FDM 管理设备](#)，或者等待并一次部署多个更改。

相关信息：

- [复制 FDM 管理 访问控制规则](#)
- [将规则粘贴到另一个设备时的对象行为](#)

将规则粘贴到另一个设备时的对象行为

如果您剪切或复制的规则包含对象，并且您将这些规则粘贴到另一个 FDM 管理设备策略中，则当满足以下任何条件时，CDO 会将这些规则中的对象复制到目标 FDM 管理设备：

适用于所有类型的对象（安全区域除外）

- 目的设备不包含对象；在这种情况下，CDO 首先在目标设备中创建对象，然后再粘贴规则。
- 目标设备包含与源设备具有相同名称和相同值的对象。

对于安全区域对象

- 目的设备包含与源设备具有相同名称和相同接口的安全区域对象。
- 目的设备不包含相同的安全区域对象，并且具有在目的设备上使用的接口。
- 目的设备包含安全区域对象，则该对象为空，并且具有在目的设备上使用的接口。

对于具有 **Active Directory (AD)** 领域的对象

- 仅当目标设备上已存在具有相同名称的领域时，CDO 才会使用 Active Directory (AD) 领域对象来粘贴规则。



Important 在以下情况下，粘贴操作会失败：

- 如果两个设备版本之间的漏洞、地理位置、入侵或 URL 数据库存在差异，则 CDO 无法将规则粘贴到目标设备中。您需要在新设备中手动重新创建规则。
- 如果要添加的规则具有包含“仅管理” (management-only) 类型接口的安全区域。

相关信息：

- [复制 FDM 管理 访问控制规则](#)
- [移动 FDM 管理 访问控制规则](#)

FDM 管理 访问控制规则中的源和目标条件

访问规则的“源和目标”标准定义通过其传递流量的安全区（接口）、IP 地址或 IP 地址的国家/地区或大洲（地理位置）或流量中使用的协议和端口。默认设置为任何区域、地址、地理位置、协议和端口。

要修改访问控制规则中的源或目标条件，可以使用 [配置 FDM 访问控制策略](#) 中的程序编辑规则。无需进入编辑模式即可执行简单编辑。在策略页面中，您可以修改规则中的条件，方法是选择规则并点击源或目标条件列中的 + 按钮，然后在弹出对话框中选择新的对象或元素。您也可以点击对象或元素对应的 x，可将其从规则中移除。

您可以通过以下标准来标识规则中要匹配的源和目标。

源区域、目标区域

安全区对象，定义通过其传递流量的接口。可以定义一个或两个条件，也可以不定义任何条件：未指定的任何条件都将应用到任何接口上的流量。

- 要匹配从区域中的接口离开设备的流量，请将该区域添加至目标区域。
- 要匹配从区域中的接口进入设备的流量，请将该区域添加至源区域。
- 如果同时向一条规则添加源区域和目标区域条件，匹配流量必须源自其中一个指定源区域并通过其中一个目标区域流出。

如果应基于流量进入或离开设备的位置来应用规则，请使用此条件。例如，如果要确保到达内部主机的所有流量均进行入侵检测，则应将内部区域选为目标区域，同时将源区域保留为空。要在规则中实施入侵过滤，则规则操作必须为允许，并且必须在该规则中选择入侵策略。



Note 不能在单一规则中搭配使用被动和路由安全区域。此外，被动安全区域只能被指定为源区域，不能作为目标区域。

源网络、目标网络

定义流量的网络地址或位置的网络对象或地理位置。

- 要匹配来自某个 IP 地址或地理位置的流量，请配置源网络。
- 要匹配流向 IP 地址或地理位置的流量，请配置目标网络。
- 如果同时向一条规则添加源网络条件和目标网络条件，匹配流量必须源自其中一个指定 IP 地址并流向其中一个目标 IP 地址。

添加此条件时，可从以下选项卡中进行选择：

- 网络 - 为您要控制的流量选择定义源或目标 IP 地址的网络对象或组。您可以使用通过完全限定域名 (FQDN) 定义地址的对象；通过 DNS 查询确定地址。
- 地理位置 - 选择要基于流量的源或目的国家/地区或大洲控制流量的地理位置。选择大洲将会选择该大洲内的所有国家/地区。除了直接在规则中选择地理位置外，也可以选择您创建的地理位置对象来定义位置。使用地理位置，可以便捷地限制对特定国家/地区的访问，而不需要知道此位置所用的全部潜在 IP 地址。



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

源端口、目标端口/协议

定义流量中所用协议的端口对象。对于 TCP/UDP，这可能包括端口。对于 ICMP，可包括代码和类型。

- 要匹配来自协议或端口的流量，请配置源端口。源端口只能为 TCP/UDP。
- 要匹配流向协议或端口的流量，请配置目标端口/协议。如果仅将目标端口添加至条件，则可以添加使用不同传输协议的端口。ICMP 和其他非 TCP/UDP 规格仅可用于目标端口，不允许用于源端口。
- 要同时匹配来自特定 TCP/UDP 端口的流量和流向特定 TCP/UDP 端口的流量，请配置源端口和目标端口。如果同时将源和目标端口添加至条件，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，您可以匹配从端口 TCP/80 流至端口 TCP/8080 的流量。


FDM 管理 访问控制规则中的 URL 条件

访问控制规则中的 URL 条件对 Web 请求中使用的 URL 或请求的 URL 所属的类别进行定义。对于类别匹配，您还可以指定要允许或阻止的站点的相对信誉。默认设置为允许所有 URL。

URL 类别和信誉可供您快速创建访问控制规则的 URL 标准。例如，您可以阻止所有游戏站点或所有高风险社交网站。如果用户尝试浏览至任何包含该类别和信誉组合的 URL，会话将被阻止。

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

要修改访问控制规则中的 URL 和 URL 类别条件，您可以使用[配置 FDM 访问控制策略](#)中的程序编辑规则。无需进入编辑模式即可执行简单编辑。在策略页面中，您可以修改规则中的 URL 条件，方法是选择规则并点击 URL 条件列中的 + 按钮，然后在弹出对话框中选择新的对象、元素、URL 声誉或 URL 类别。您也可以点击对象或元素对应的 x，可将其从规则中移除。

点击蓝色加号图标 ，选择 URL 对象、组或 URL 类别，然后点击保存 (Save)。如果所需的 URL 对象不存在，可以点击“创建新对象” (Create New Object)。有关 URL 对象的详细信息，请参阅[创建或编辑 FDM URL 对象](#)。

URL 过滤的许可证要求

要使用 URL 过滤，您需要在 FDM 管理设备上启用 URL 许可证。

为规则中使用的 URL 类别指定信誉

默认情况下，规则会以相同的方式处理 URL 类别中的所有 URL。例如，如果您有阻止社交网络 URL 的规则，则无论信誉如何，都将阻止所有这些 URL。您可以调整该设置，以便只阻止高风险社交网络站点。同样，您可以允许 URL 类别中的所有 URL，但高风险站点除外。

使用此程序可对访问控制规则中的 URL 类别使用信誉过滤器：

Procedure

- 步骤 1 在“FTD 策略” (FTD Policy) 页面中，选择要编辑的规则。
- 步骤 2 点击编辑 (Edit)。

- 步骤 3** 点击 **URL** 选项卡。
- 步骤 4** 点击蓝色加号按钮 ，然后选择 URL 类别。
- 步骤 5** 点击将信誉应用于所选的类别 (**Apply Reputation to Selected Categories**) 或您刚刚选择的 URL 类别上的任何信誉 (**Any Reputation**) 链接。
- 步骤 6** 取消选中任何信誉 (**Any Reputation**) 复选框。
- 步骤 7** 按信誉过滤 URL:
- 如果规则具有阻止操作，请将信誉滑块滑动到右侧，以便仅阻止信誉标记为红色的站点。例如，如果将滑块滑动到“具有安全风险的站点” (Sites with Security Risks)，则阻止规则将阻止“具有安全风险的站点” (Sites with Security Risks)、“可疑站点” (Suspicious Sites) 和“高风险站点” (High-Risk sites)，但它会允许来自“公认站点” (Well-known Sites) 和“良性站点” (Benign Sites) 的流量站点。
 - 如果规则具有允许操作，请将信誉滑块滑动到右侧，以便仅允许信誉标记为绿色的站点。例如，如果将滑块滑动到“良性站点” (Benign Sites)，规则将允许来自“公认站点” (Well-Known Sites) 和“良性站点” (Benign Sites) 的流量，但不允许来自“具有安全风险的站点” (Sites with Security Risks)、“可疑站点” (Suspicious Sites) 和“高风险站点” (High-Risk sites)。
- 步骤 8** 点击**保存 (Save)**。
- 步骤 9** 点击 **Select**。
- 步骤 10** 点击**保存 (Save)**。
- 步骤 11** 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

在 FDM 管理 访问控制规则中选择入侵策略

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

入侵策略的许可证和操作要求

- **许可证 (Licenses)** - 要将入侵策略添加到规则，您需要在 FDM 管理 设备上启用 许可证
- **规则操作 (Rule action)** - 您只能对**允许流量**的规则配置入侵策略和文件策略。对于设置为**信任**或**阻止流量**的规则，系统不会执行检测。此外，如果访问控制策略的默认操作是**允许**，则您可以配置入侵策略，但不能配置文件策略。

访问控制规则的可用入侵策略

对于允许流量的访问控制规则，您可以选择以下任一入侵策略来检测流量中是否存在入侵和攻击程序。入侵策略根据模式检查已解码数据包中是否存在攻击，并且可以阻止或修改恶意流量。

策略将按安全性由低到高列出：

- **连接优先于安全** - 此策略适用于连接（即确保能够获取所有资源）优先于网络基础设施安全的组织。此入侵策略启用的规则远远少于“安全优先于连接”策略中启用的规则。仅会启用阻止流量的最重要规则。如果要应用某些入侵保护，但对网络的安全性相当自信，可选择此策略。
- **平衡安全和连接** - 此策略用于平衡整体网络性能和网络基础设施安全性。此策略适合大多数网络。对于要应用入侵防御的大多数情况，可选择此策略。
- **安全性优先于连接** - 此策略适用于网络基础设施安全优先于用户便利性的组织。此入侵策略将启用许多可能会提醒或丢弃合法流量的网络异常入侵规则。如果安全性至上或针对高风险流量，可选择此策略。
- **最大检测** - 此策略适用于网络基础设施安全性比在“安全优先于连接”策略中还要重要、有可能产生更大运营影响的组织。例如，入侵策略将启用大量威胁类别中的规则，包括恶意软件、攻击程序包、旧漏洞和常见漏洞及已知外部攻击程序。如果选择此策略，请仔细评估是否要丢弃过多的合法流量。

相关信息

- [FDM 管理 访问控制策略中的入侵、文件和恶意软件检测](#)

FDM 管理 访问控制规则中的文件策略设置

借助适用于 Firepower 的高级恶意软件保护（适用于 Firepower 的 AMP），可使用文件策略检测恶意软件（或恶意软件）。另外，您还可以使用文件策略执行文件控制，以允许控制特定类型的所有文件，而不考虑文件中是否包含恶意软件。

适用于 Firepower 的 AMP 使用 AMP 云检索网络流量中检测到的潜在恶意软件的处置，并获取本地恶意软件分析和文件预分类更新。管理接口必须可连接互联网，以便访问 AMP 云并搜索恶意软件。当设备检测到符合条件的文件时，它将使用该文件的 SHA-256 散列值来查询 AMP 云中是否存在该文件的处置。可能的处置包括：

- **恶意软件** - AMP 云将文件归类为恶意软件。如果其中的任何文件为恶意软件，存档文件（例如 zip 文件）会被标记为恶意软件。
- **安全** - AMP 云将文件归类为安全，不含恶意软件。如果其中的所有文件都安全，存档文件将会标记为安全。
- **未知** - AMP 云尚未指定该文件的处置。如果其中的任何文件属于未知状态，存档文件会被标记为未知。
- **不可用** - 系统无法通过查询 AMP 云来确定文件的处置。您可能看到很少一部分事件为此处置：这是预期行为。如果您连续看到许多“不可用”事件，请确保管理地址的互联网连接正常运行。

文件策略的许可证和操作要求

许可证 - 要将文件策略添加到规则，您需要在 Firepower 设备管理器上启用两个许可证：

- 许可证
- 恶意软件许可证

规则操作 - 您只能对允许流量的规则配置文件策略。对于设置为信任或阻止流量的规则，系统不会执行检测。此外，如果访问控制策略的默认操作是允许，则您可以配置入侵策略，但不能配置文件策略。

访问控制规则的可用文件策略

- **无** - 不评估传输的文件中是否存在恶意软件，且不阻止特定的文件。对于文件传输受信任或不可能传输文件的规则或您相信自己的应用或 URL 过滤可适当保护网络的规则，请选择此选项。
- **阻止所有恶意软件** - 查询 AMP 云以确定通过网络传输的文件是否包含恶意软件，然后阻止存在威胁的文件。
- **全部执行云查找** - 查询 AMP 云以获取和记录通过网络传输的文件的处置，同时仍允许文件传输。
- **阻止 Office 文档和 PDF 上传、阻止其他恶意软件** - 阻止用户上传 Microsoft Office 文档和 PDF。此外，查询 AMP 云以确定遍历网络的文件是否包含恶意软件，然后阻止存在威胁的文件。
- **阻止 Office 文档上传、阻止其他恶意软件** - 阻止用户上传 Microsoft Office 文档。此外，查询 AMP 云以确定遍历网络的文件是否包含恶意软件，然后阻止存在威胁的文件。

相关信息：

- [在 FDM 管理 访问控制规则中选择入侵策略](#)

FDM 管理 访问控制规则中的日志记录设置

访问控制规则的日志记录设置

访问规则的日志记录设置确定是否对匹配规则的流量发出连接事件。

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



Caution

在拒绝服务 (DoS) 攻击期间记录被阻止的 TCP 连接会影响系统性能并因多个相似事件使数据库不堪重负。在对“阻止”规则启用日志记录之前，请考虑该规则是否监控面向互联网的接口或其他易受 DoS 攻击的接口。

操作步骤

Procedure

步骤 1 [配置 FDM 访问控制策略](#)，然后点击日志记录选项卡。

步骤 2 指定日志操作：

- **在连接开始和结束时记录** - 在连接开始和结束时发出事件。由于连接结束事件包含连接开始事件所含的一切，以及连接期间可能收集的所有信息，所以思科建议不要对允许的流量选择此选项。记录两种事件可能会影响系统性能。但是，这是针对阻止的流量唯一允许的选项。
- **在连接结束时记录** - 如果要在连接结束时启用连接日志记录（建议对允许或受信任的流量执行此操作），请选择此选项。
- **不记录 (Log None)** - 选择此选项，可对规则禁用日志记录。这是默认值。

Note 当访问控制规则调用的入侵策略检测到入侵并生成入侵事件时，系统会在发生入侵的位置自动记录连接终止，无论该规则的日志记录配置如何。对于入侵受阻的连接，连接日志中的连接操作为**阻止**，原因为**入侵阻止**，即使执行入侵检测，也必须使用“允许”规则。

步骤 3 指定将连接事件发送至何处：

如果要将事件副本发送到外部系统日志服务器，请选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，则需要创建一个。有关详细信息，请参阅[创建和编辑系统日志服务器对象](#)。

由于设备中的事件存储受限，所以将事件发送至外部系统日志服务器可供长期存储，并增强您的事件分析。

对于[思科安全分析和日志记录](#)用户：

- 如果通过安全事件连接器 (SEC) 将事件发送到思科云，请[指定 SEC 作为系统日志服务器](#)。然后，您将能够在文件策略和恶意软件策略连接事件旁边看到这些事件。
- 如果不使用 SEC 将事件直接发送到思科云，请指定记录事件的时间（在连接开始或结束时），但不要将 SEC 指定为系统日志服务器。

步骤 4 文件事件

如果要对禁止文件或恶意软件事件启用日志记录，请选中**日志文件 (Log Files)**。只有在规则中选择了文件策略，才能配置此选项。如果对规则选择了文件策略，则该选项默认处于启用状态。我们建议您将此选项保留为已启用。

当系统检测到受禁文件时，它会将以下类型事件之一自动记录到 FDM 管理 内部缓冲区：

- 文件事件，代表检测到或阻止的文件，包括恶意软件文件。
- 恶意软件事件，仅代表检测到或阻止的恶意软件文件。
- 可追溯的恶意软件事件，在之前检测到的文件的恶意软件处置变更时生成。

对于文件受阻的连接，连接记录中的连接操作为阻止，即便要执行文件和恶意软件检测，也必须使用“允许”规则。连接原因是“文件监控”（检测到某种文件类型或恶意软件）或者是“恶意软件阻止”或“文件阻止”（文件被阻止）

步骤 5 点击保存 (Save)。

步骤 6 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

安全组标记

关于安全组标记

如果使用思科身份服务引擎 (ISE) 定义并使用安全组标记 (SGT) 来对 Cisco TrustSec 网络中的流量进行分类，则可以编写使用 SGT 作为匹配条件的访问控制规则。因此，可以基于安全组成员身份阻止或允许访问，而不是使用 IP 地址。

在 ISE 中，您可以创建 SGT，并将主机或网络 IP 地址分配至各标记。如果您将 SGT 分配给用户帐户，SGT 就会被分配给用户流量。将 FDM 管理设备配置为连接到 ISE 服务器并创建 SGT 后，您可以在思科防御协调器中创建 SGT 组并围绕它们构建访问控制规则。请注意，您必须先配置 ISE 的 SGT 交换协议 (SXP) 映射，然后才能将 SGT 关联到 FDM 管理设备。有关详细信息，请参阅您当前运行的版本的《思科身份服务引擎管理员指南》中的安全组标记交换协议。

FDM 管理设备评估 SGT 作为访问控制规则的流量匹配条件时，会使用以下优先级：

1. 数据包中定义的源 SGT（如有）。使用此技术无法进行目的地匹配。对于数据包中的 SGT，必须配置网络中的交换机和路由器以添加它们。有关如何实施此方法的信息，请参阅 ISE 文档。
2. 分配给用户会话的 SGT，从 ISE 会话目录下载。您需要启用此选项才能侦听此类 SGT 匹配的会话目录信息，但是，当您首次创建 ISE 身份源时，此选项会默认打开。SGT 可以与源或目标相匹配。尽管非必需，但您通常还会使用 ISE 身份源和 AD 域来设置被动身份验证身份规则，以收集用户身份信息。
3. 使用 SXP 下载的 SGT-IP 地址映射。如果 IP 地址在 SGT 范围内，则流量与使用 SGT 的访问控制规则相匹配。SGT 可以与源或目标相匹配。



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

版本支持

CDO 当前在运行 6.5 和更高版本的 FDM 管理设备上支持 SGT 和 SGT 组。FDM 管理设备允许您在版本 6.5 及更高版本中配置并连接到 ISE 服务器，但在 6.7 之前版本中不支持在 UI 中配置 SGT。

从 FDM 管理 UI 中，这意味着运行版本 6.5 或更高版本的 FDM 管理设备可以下载 SGT 的 SXP 映射，但不能手动添加到对象或访问控制规则。要更改运行版本 6.5 或版本 6.6 的设备的 SGT，您必须使用 ISE UI。但是，如果运行版本 6.5 的设备已被载入思科防御协调器，则可以查看与设备关联的当前 SGT 并创建 SGT 组。

CDO 中的 SGT

安全组标记

SGT 在 CDO 中为只读。您无法在 CDO 中创建或编辑 SGT。要创建 SGT，请参阅当前运行版本的《思科身份服务引擎管理员指南》。

SGT 组



Note FDM 管理设备将 SGT 组称作 SGT 动态对象。在 CDO 中，这些标签列表当前被称作 SGT 组。您可以在 CDO 中创建 SGT 组，而无需参考 FDM 管理设备或 ISE UI。

使用 SGT 组可以根据 ISE 分配的 SGT 来识别源或目标地址。然后，可以将访问控制规则中的对象用于定义流量匹配条件。您无法直接在访问控制规则中使用从 ISE 检索到的信息。相反，您需要创建引用已下载 SGT 信息的 SGT 组。

您的 SGT 组可以引用多个 SGT，因此您可以在适当的情况下根据相关的标记集合应用策略。

要在 CDO 中创建 SGT 组，必须至少已经配置一个 SGT，并为要使用的设备的 FDM 管理控制台配置来自 ISE 服务器的 SGT 映射。请注意，如果多个 FDM 管理设备与同一 ISE 服务器关联，则可以将 SGT 或 SGT 组应用于多个设备。如果设备未与 ISE 服务器关联，则不能在访问控制规则中包含 SGT 对象，也不能将 SGT 组应用于该设备配置。

规则中的 SGT 组

SGT 组可被添加到访问控制规则；它们会显示为源或目标网络对象。有关网络如何在规则中工作的详细信息，请参阅 [FDM 管理 访问控制规则中的源和目标条件](#)。

您可以从“对象” (Objects) 页面创建 SGT 组。有关详细信息，请参阅 [创建 SGT 组](#)。

创建 SGT 组

要创建可用于访问控制规则的 SGT 组，请使用以下程序：


Before you begin

在创建安全组标记 (SGT) 组之前，必须配置以下配置或环境：

- FDM 管理设备必须至少运行版本 6.5。
- 必须配置 ISE 身份源以订用 SXP 映射并启用部署更改。要管理 SXP 映射，请参阅所用版本（版本 6.7 及更高版本）的 [Firepower 设备管理器配置指南](#) 中的 [在 ISE 中配置安全组和 SXP 发布](#)。
- 所有 SGT 都必须在 ISE 中创建。要创建 SGT，请参阅当前运行版本的 [《思科身份服务引擎配置指南》](#)。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮  以创建新的对象。

步骤 3 点击 **FTD > 网络 (Network)**。

步骤 4 输入 **对象名称 (Object Name)**。

步骤 5 （可选）添加说明。

步骤 6 点击 **SGT** 并使用下拉菜单选中要包含在组中的所有适用 SGT。您可以按 SGT 名称对列表进行排序。

步骤 7 点击 **保存 (Save)**。

Note 您无法在 CDO 中创建或编辑 SGT，只能在 SGT 组中添加或删除它们。要创建或编辑 SGT，请参阅当前运行版本的《[思科身份服务引擎配置指南](#)》。


编辑 SGT 组

要编辑 SGT 组，请使用以下程序：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到您要编辑的 SGT 组。

步骤 3 选择 SGT 组，然后点击 **操作 (Actions)** 窗格中的编辑图标 。

步骤 4 修改 SGT 组。编辑与该组关联的名称、说明或 SGT。

步骤 5 点击 **保存 (Save)**。

Note 您无法在 CDO 中创建或编辑 SGT，只能在 SGT 组中添加或删除它们。要创建或编辑 SGT，请参阅当前运行版本的《[思科身份服务引擎配置指南](#)》。

将 SGT 组添加到访问控制规则

要将 SGT 组添加到访问控制规则，请使用以下程序：


Procedure

步骤 1 在导航窗格中，点击 **清单 (Inventory)**。

步骤 2 点击 **设备 (Devices)** 选项卡以查找设备，或点击 **模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择要向其添加 SGT 组的设备。

步骤 4 在 **管理 (Management)** 窗格中，选择 **策略 (Policy)**。

步骤 5 点击源或目标对象的蓝色加号按钮，然后选择 SGT 组。 

步骤 6 使用对象过滤器和搜索字段找到您要编辑的 SGT 组。

步骤 7 点击 **保存 (Save)**。

步骤 8 [预览和部署所有设备的配置更改](#)。

Note 如果需要创建其他 SGT 组，请点击创建新对象。填写创建 FTD SGT 组并将 SGT 组添加到规则中提到的必填信息。[创建 SGT 组](#)

FDM 管理 访问控制规则中的应用条件

访问规则的“应用”条件对 IP 连接中使用的应用进行定义，或按类型、类别、标记、风险或业务相关性定义应用的过滤器。默认设置为任何应用。

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

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

您可以直接在规则指定应用和过滤器，也可以创建定义这些特征的应用过滤器对象。规格相当，尽管如果要创建复杂规则，使用对象可便于遵守每个条件 50 个项目的系统限制。有关创建应用过滤器对象的详细信息，请参阅[创建和编辑 Firepower 应用过滤器对象](#)。

要修改规则中使用的应用和应用过滤器，可以使用[FDM 管理 访问控制策略](#)中的程序编辑规则。无需进入编辑模式即可执行简单编辑。在策略页面中，您可以修改规则中的应用条件，方法是选择规则并点击应用条件列中的 + 按钮，然后在弹出对话框中选择新的对象或元素。您也可以点击对象或元素对应的 x，可将其从规则中移除。

FDM 管理 访问控制策略中的入侵、文件和恶意软件检测

入侵策略和文件策略共同发挥作用，作为允许流量到达其目标之前的最后一道防线。

- 入侵策略监管系统的入侵防御功能。
- 文件策略监管系统的文件控制和适用于 Firepower 的 AMP 功能。

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

您只能对允许流量的规则配置入侵策略和文件策略。对于设置为信任或阻止流量的规则，系统不会执行检测。此外，如果访问控制策略的默认操作是允许，则您可以配置入侵策略，但不能配置文件策略。

对由访问控制规则处理的任何单个连接，文件检测均发生在入侵检测之前。也就是说，系统不检测文件策略所阻止的文件是否存在入侵。在文件检测中，基于类型的简单阻止优先于恶意软件检测和阻止。文件在会话中得以检测和阻止之前，来自该会话的数据包均可能接受入侵检测。



Note 默认情况下，系统禁用对已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。检测仅适用于未加密的流量。

相关信息：

- [在 FDM 管理 访问控制规则中选择入侵策略](#)
- [FDM 管理 访问控制规则中的文件策略设置](#)

FDM 管理 访问控制规则中的自定义 IPS 策略


不能将同一自定义 IPS 策略的多个实例与单个设备关联。



Note 将 IPS 策略与访问控制规则相关联意味着传递的流量将被提交到深度数据包检查。具有 IPS 策略的访问控制规则唯一受支持的规则操作是**允许 (Allow)**。

使用以下程序将自定义 IPS 策略关联到 FDM 管理 设备：

Procedure

- 步骤 1** 创建自定义 IPS 策略。有关详细信息，请参阅[配置 Firepower 自定义 IPS 策略](#)。
- 步骤 2** 在思科防御协调器 导航窗格中，选择**策略 (Policies)**。点击 **FTD/Meraki/AWS 策略 (FTD / Meraki / AWS Policies)**。
- 步骤 3** 滚动或过滤 FDM 管理 设备策略列表，然后选择要与自定义 IPS 策略关联的策略。
- 步骤 4** 点击蓝色加号按钮 。
- 步骤 5** 在**顺序 (Order)** 字段中，选择规则在策略中的位置。根据规则列表（按数字顺序从 1 到“最后” (last)）评估网络流量。
- 步骤 6** 输入规则名称。可以使用字母数字字符和以下特殊字符：+ . _ -
- 步骤 7** 选择**入侵策略 (Intrusion Policy)** 选项卡。展开下拉菜单以查看所有可用的入侵策略，然后选择所需的自定义 IPS 策略。
- 步骤 8** 使用以下选项卡中的任意属性组合定义流量匹配条件：**源/目标 (Source/Destination)**、**URLs**、**应用 (Applications)** 和**文件策略 (File Policy)**。
- 步骤 9** （可选）点击**日志记录**选项卡以启用日志记录，并收集访问控制规则报告的**连接事件**。
- 步骤 10** 点击**保存 (Save)**。
- 步骤 11** 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

Firepower 威胁防御中的 TLS 服务器身份发现

现在，您可以使用 威胁防御 的独特 TLS 服务器身份发现来对流量执行改进的 URL 过滤和应用控制，从而在环境中实现可控性和精确性。您没有解密流量才能使此功能正常工作。




Note 对服务器身份发现功能的支持仅限于版本 6.7 及更高版本。

启用 TLS 服务器身份发现

使用以下程序为 FDM 管理访问控制策略启用或禁用 TLS 服务器身份发现功能：

Procedure

- 步骤 1** 在导航窗格中，点击**清单 (Inventory)**。
- 步骤 2** 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
- 步骤 3** 点击 **FTD** 选项卡并选择设备。
- 步骤 4** 在位于右侧的**管理 (Management)** 窗格中，选择**策略 (Policy)**。
- 步骤 5** 点击表右上角的访问策略设置齿轮图标 。
- 步骤 6** 滑动开关以启用 TLS 服务器身份发现。
- 步骤 7** 点击**保存 (Save)**。

入侵防御系统

思科 Talos 情报组 (Talos) 实时检测和关联威胁，并维护数十亿个文件的信誉处理情况。思科 IOS 入侵防御系统 (IPS) 是一种内联深度数据包检测功能，通过使用来自 Talos 的威胁情报数据来实时准确识别、分类和丢弃恶意流量，从而缓解网络上的攻击。

思科防御协调器 (CDO) Cisco Defense Orchestrator (CDO) 能够激活并调整运行软件版本 6.4.xx 至 6.6.0.x 和 6.6.1.x 的 FDM 管理设备上的 IPS 功能。



Note CDO 当前不支持版本 6.7 上的 IPS 规则调整。

在 CDO 菜单栏上，导航到**策略 (Policies) > 前面覆盖 (Signature Overrides)** 以执行以下任务：

- 解决跨设备覆盖的不一致问题。
- 查看和隐藏威胁事件。
- 通过更改规则操作来覆盖威胁事件的处理方式。

相关信息：

- [Firepower 入侵策略签名覆盖](#)
- [威胁事件](#)
- [入侵防御系统故障排除](#)

威胁事件

威胁事件报告是在匹配思科 Talos 的入侵策略后已丢弃或已生成警报的流量的报告。在大多数情况下，无需调整 IPS 规则。如有必要，您可以选择通过更改 思科防御协调器 中的匹配规则操作来覆盖事件的处理方式。

请注意“威胁”(Threats)页面的以下行为：

- 显示的威胁事件不是实时的。设备每小时轮询一次，以查找其他威胁事件。
- 未包含在**实时或历史 (Live or Historical)**视图中的威胁事件不属于思科安全分析和日志记录。
- 要查看已隐藏的威胁事件，请点击过滤器图标并选中**查看隐藏 (view hidden)**选项。
- 如果您是**思科安全分析和日志记录**的订户，则您在“威胁事件”(Threat Events)表中看到的事件不包含发送到安全事件连接器的事件。

Procedure

步骤 1 从导航窗格中，选择 **监控 (Monitoring) > 威胁 (Threats)**。您可以**过滤**显示的事件，并按源 IP 地址进行搜索。

步骤 2 点击威胁事件可展开右侧的详细信息面板。

- a) 有关规则的详细信息，请点击规则详细信息 (**Rule Details**) 部分中的 **规则文档 (Rule Document)** URL。
- b) 要隐藏此事件，请选中**隐藏事件 (Hide Events)** 的切换开关。事件处理将按原样继续，但您不会在此处看到它，除非您点击**查看隐藏 (View Hidden)** 或取消隐藏此事件。
- c) 要编辑规则覆盖，请点击**调整规则 (Tune Rule)**。当您在 CDO 中更改规则操作时，覆盖将应用于所有预定义策略。这与 FDM 不同，在 FDM 管理设备中，每个规则可能因政策而异。

Note CDO 提供在运行软件版本 6.4.xx 至 6.6.0.x 和 6.6.1.x 的 FDM 管理设备上调整规则的功能。CDO 当前不支持 FDM 管理版本 6.7 上的规则调整。

- 在**覆盖所有 (Override All)**设备下拉列表中，选择一个操作，然后点击**保存 (Save)**。
 - **丢弃 (Drop)** - 当此规则与流量匹配时，此选择规则创建一个事件同时丢弃连接。使用此操作可加强某些规则的安全性。例如，当 Talos 规则匹配时，即使为访问控制规则指定了“连接优先于安全”策略，指定 Drop 也会提高安全性。
 - **警报 (Alert)** - 当此规则与流量匹配时，此选择创建一个事件但不丢弃连接。“警报”的一个使用案例是流量被阻止，但客户希望允许，并在禁用规则之前查看警报。
 - **已禁用 (Disabled)** - 此选项可防止流量与规则匹配。不生成事件。“禁用”的使用案例是停止报告中的误报，或删除不适用于您的环境的规则，例如，如果您不使用 httpd，则禁用 Apache httpd 规则。
 - **默认 (Default)** - 对于在其中列出的入侵策略，此选项将规则恢复为 Talos 为其分配的默认操作。例如，当您将入侵规则恢复为“默认”时，这可能意味着其操作在“连接优先于安全”策略和“平衡安全性和连接”策略中的“阻止”。

- 要按设备编辑规则覆盖，请选中**高级选项 (Advanced Options)**滑块。此部分显示为每个设备配置的规则操作，您可以通过选中受影响的设备，选择覆盖操作，然后点击**保存 (Save)**来更改规则操作。
- **受影响的设备**不表示源设备。相反，它会显示报告事件的 FDM 管理设备。

Note

- 点击刷新 (🔄) 按钮可刷新根据当前搜索过滤器显示威胁的表。
- 点击导出 (📄) 按钮，将威胁的当前摘要下载到逗号分隔值 (.csv) 文件。您可以在电子表格应用（例如 Microsoft Excel）中打开 .csv 文件，对列表中的项目进行排序和过滤。CDO 会将基本威胁详细信息导出到文件，但时间、来源和设备等附加信息除外。


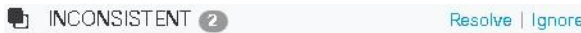
步骤 3 立即**预览和部署所有设备的配置更改**您所做的更改，或等待并一次部署多个更改。

Firepower 入侵策略签名覆盖

在大多数情况下，无需调整任何 IPS 规则。如有必要，您可以选择通过更改 CDO 中的匹配规则操作来覆盖事件的处理方式。CDO 为您提供解决覆盖问题的选项。

管理签名覆盖

Procedure

- 步骤 1** 在主导航栏中，点击**策略 (Policies) > 签名覆盖 (Signature Overrides)**。您可以**过滤**显示的设备 and 策略覆盖策略。您还可以按名称或入侵规则 SID 来搜索入侵策略。
- 步骤 2** 点击策略覆盖策略的名称，以便展开右侧的详细信息面板。
- 步骤 3** 在**问题 (Issues)**窗格中， 标记表示设备之间的覆盖不一致。您可以看到包含受影响设备数量的“不一致” (INCONSISTENT) 字段：
- 要忽略问题**，请点击**忽略 (Ignore)**。这不会更改问题，但会从**问题 (Issues)**列中删除指示器标记。
 - 要解决此问题**，请点击**解决 (Resolve)**。在左侧面板中，选择要比较的策略，然后显示其一致和不一致的覆盖。
 - 要合并策略，请执行以下操作：
 1. 点击**通过合并解决 (Resolve by Merging)** 以便将其合并为一个策略，在其所有设备上采用相同的覆盖。
 2. 点击 **Confirm**。
 - 要重命名策略：
 1. 在策略的部分中，点击**重命名 (Rename)** 并为其指定其他名称。
 2. 点击 **Confirm**。

- 要忽略策略，请执行以下操作：
 1. 在策略的部分中，点击**忽略 (Ignore)**。
 2. 点击 **Confirm**。
- 要忽略所有不一致，请点击**全部忽略 (Ignore All)**。

步骤 4 如果使用 FDM 管理 设备在设备上更改了单个 Talos 入侵规则，您将在**覆盖 (Overrides)** 窗格中看到这些规则。您可以通过点击**调整 (Tune)** 链接并选择覆盖操作来更改入侵规则的覆盖操作。此操作将应用于使用它的所有 Talos 入侵策略中的该规则。请注意，如果您选择恢复默认操作规则（**默认值**），则在环境触发入侵规则之前，您将无法再次调整该规则。

- 连接优先于安全
- 平衡安全和连接
- 安全优先于连接
- 最大检测数

为了在设备之间保持一致，覆盖操作将保存到与入侵覆盖策略关联的每个设备。

以下是覆盖操作的效果：

- **丢弃 (Drop)** - 当此规则与流量匹配时，此选择规则创建一个事件同时丢弃连接。使用此操作可加强某些规则的安全性。例如，当 Talos 规则匹配时，即使为访问控制规则指定了“连接优先于安全”策略，指定 **Drop** 也会提高安全性。
- **警报 (Alert)** - 当此规则与流量匹配时，此选择创建一个事件但不丢弃连接。“警报”的一个使用案例是流量被阻止，但客户希望允许，并在禁用规则之前查看警报。
- **已禁用 (Disabled)** - 此选项可防止流量与规则匹配。不生成事件。“禁用”的使用案例是停止报告中的误报，或删除不适用于您的环境的规则，例如，如果您不使用 httpd，则禁用 Apache httpd 规则。
- **默认 (Default)** - 此选项仅适用于 Talos 入侵策略级别中的规则默认操作。例如，当您将入侵规则恢复为“默认”时，这可能意味着其操作在“连接优先于安全”策略和“平衡安全性和连接”策略中的“阻止”。
- 使用以下选项编辑规则覆盖：
 - **覆盖所有设备 (Override for all devices)** - 此选项可为 CDO 管理的所有设备设置所需的操作。从下拉菜单中选择一个选项。如果规则对于不同的入侵覆盖策略具有不同的覆盖值，则默认情况下，下拉选项为“多个” (Multiple)。
 - **按设备编辑规则覆盖 (Edit rule overrides by device)** - 选中高级选项 (**Advanced Options**) 滑块，然后选择**按设备覆盖 (Overrides by Devices)** 选项卡。此选项显示为每个设备配置的规则操作，您可以通过选中受影响的设备，选择覆盖操作，然后点击**保存 (Save)** 来更改规则操作。

- **按策略编辑规则覆盖 (Edit rule overrides by policy)** - 选中高级选项 (**Advanced Options**) 滑块，然后选择**全部覆盖 (All Overrides)** 选项卡。仅当您的租户配置了多个 IPS 策略时，此部分才适用。您可以从此页面管理所有 IP 策略，包括与多个设备关联的策略。

步骤 5 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

创建签名覆盖

您只能为已在 FTD 设备上触发的 IPS 规则创建签名覆盖。在 CDO 中创建签名覆盖时，覆盖会自动将配置的操作（**丢弃、警报、禁用、默认**）应用于所有策略级别。

Procedure

步骤 1 在主导航栏中，点击**监控 (Monitoring) > 威胁 (Threats)**。

步骤 2 从表中选择一个威胁并将其展开。在“调整操作” (Tune Actions) 窗格中，点击**调整 (Tune)**。

步骤 3 按照 [Firepower 入侵策略签名覆盖](#) 程序的**步骤 4** 中的说明调整规则。

步骤 4 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

删除签名覆盖

Procedure

步骤 1 在主导航栏中，点击**策略 (Policies) > 签名覆盖 (Signature Overrides)**。

步骤 2 点击覆盖的名称，以便展开右侧的详细信息面板。

步骤 3 展开覆盖窗格并选择要删除的覆盖，然后点击**调整 (Tune)**。

步骤 4 将默认操作设置为**默认 (Default)**。

步骤 5 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

自定义 Firepower 入侵防御系统策略

关于自定义 IPS 策略

随着版本 6.7 的推出，改进的 Snort 3 处理引擎允许您使用思科 Talos 情报组 (Talos) 提供的规则来创建和自定义入侵防御系统 (IPS) 策略。最佳实践是根据提供的 Talos 策略模板创建您自己的策略，并在需要调整规则操作时进行更改。



Note 目前，CDO 不支持自定义 IPS 规则。您可以使用 Talos 提供的规则创建和修改自定义 IPS 策略，但不能创建自己的 IPS 规则并将其应用于自定义 IPS 策略。

这些基本模板包含相同的入侵规则（也称为签名）列表，但针对每个规则所采取的操作有所不同。比如，某个规则可能在某个策略中启用，但在另一个策略中却被禁用。又比如，如果您发现某个特定规则为您提供的误报过多，在这种情况下该规则会阻止您不希望阻止的流量，可以禁用该规则而不必切换到安全性较低的入侵策略。也可将其更改为匹配警告，而不丢弃流量。

IPS 策略库模板

这些基本模板包含相同的入侵规则（也称为签名）列表，但针对每个规则所采取的操作有所不同。例如，一条规则在某个策略中可能处于启用状态，但在另一个策略中可能被禁用。有比如，如果您发现某个特定规则为您提供的误报过多，在这种情况下该规则会阻止您不希望阻止的流量，可以禁用该规则而不必切换到安全性较低的入侵策略。也可将其更改为匹配警告，而不丢弃流量。

提供的基本模板是根据您的网络可能需要的保护类型而建议采用的配置。在创建新策略时，您可以使用以下任何模板作为基础：



Caution 请勿修改启用了 Snort 3 的 FDM 管理设备随附的默认 IPS 策略。我们强烈建议根据以下模板来创建新的自定义 IPS 策略，并为新策略使用不同于下面列出的默认 IPS 策略名称的唯一名称。如果您需要对策略进行故障排除，思科 TAC 可以轻松找到自定义策略并恢复为默认策略；这样可以保护您的网络，而不会丢失您的自定义更改。

提供的基本模板是根据您的网络可能需要的保护类型而建议采用的配置。在创建新策略时，您可以使用以下任何模板作为基础：

- **最大检测 (Maximum Detection)** - 此类策略适用于网络基础设施安全比在“安全优先于连接”策略中还要重要、且有可能产生更大运行影响的网络。
- **安全优先于连接 (Security Over Connectivity)** - 这些策略专为网络基础设施安全优先于用户便利性的网络而构建。此入侵策略将启用许多可能会提醒或丢弃合法流量的网络异常入侵规则。
- **平衡安全和连接 (Balanced Security and Connectivity)** - 这些策略专为速度和检测而构建。共同使用时，这些策略充当大多数网络和部署类型的良好起点。
- **连接优先于安全 (Connectivity Over Security)** - 这些策略专为连接（即能够获取所有资源）优先于网络基础设施安全的网络而构建。仅会启用阻止流量的最重要规则。
- **无活动规则 (No Rules Active)** - 默认情况下禁用策略中包含的规则。



Tip **最大检测 (Maximum Detection)** 基础模板需要大量内存和 CPU 才能有效工作。CDO 建议使用此模板将 IPS 策略部署到 2100、4100 或虚拟设备等型号。

随着新的漏洞被发现，Talos 会发布入侵规则更新。这些规则更新可以修改任何思科提供的网络分析或入侵策略，并可提供自动应用于现有规则和策略设置的新的和更新的入侵规则和预处理器规则。规则更新还可能删除现有模板库中的规则，提供新的规则类别，以及修改默认变量集。

IPS 策略模式

默认情况下，所有入侵策略在**防御模式**下运行，以实施 IPS。在防御检测模式下，如果连接与实施流量丢弃操作的入侵规则匹配，则该连接会被主动阻止。

如果想要测试入侵策略对网络的影响，则可以更改为**检测模式**，从而实施入侵检测系统 (IDS)。在此检测模式下，丢弃规则的处理方式类似于报警规则，在这种情况下，系统会通知您匹配的连接，但操作结果变为**将被阻止**，而事实上绝不会阻止连接。

IPS 规则组安全级别

CDO 允许您修改策略中包含的规则组的安全级别。请注意，此安全级别适用于规则组中的所有规则，而不是单个规则。



Note 对规则组的安全级别所做的更改将自动提交，并且无法恢复。您不必点击**保存 (Save)** 即可提交安全级别修改。您必须手动更改安全级别。

IPS 规则操作

随时修改规则组中单个规则或多个规则的操作。IPS 规则可以设置为以下选项：

- **禁用** - 不针对此规则匹配流量。不生成事件。
- **警报** - 当此规则与流量匹配时，创建一个事件但不丢弃连接。
- **丢弃** - 当此规则与流量匹配时，创建一个事件同时丢弃连接。

FDM 模板和自定义 IPS 策略

从启用了 Snort 3 的设备派生的模板只能应用于也启用了 Snort 3 的设备。由于 Snort 2 和 Snort 3 支持和处理的规则存在差异，配置了 Snort 3 的模板无法完全支持和保护配置了 Snort 2 的设备。有关详细信息，请参阅[从 Snort 2 切换到 Snort 3](#)。

如果您碰巧使用 ASA 迁移工具从 ASA 配置创建 FDM 模板，我们**强烈**建议不要配置或取消配置任何 IPS 策略。ASA 设备不支持 Snort 引擎，将 IPS 策略从 ASA 配置迁移到 FDM 管理设备配置可能会导致问题。如果您使用 ASA 迁移工具，我们建议在创建和部署模板后为设备创建自定义 IPS 策略。

有关模板的详细信息，请参阅[FDM 管理 设备模板](#)。

规则集和自定义 IPS 策略

为 Snort 3 配置的设备尚不支持规则集。以下限制适用：

- 不能将规则集附加到支持 Snort 3 的设备。
- 您无法从已安装 Snort 3 的现有设备创建规则集。
- 不能将自定义 IPS 策略与规则集关联。

前提条件

您可以从入侵策略 (**Intrusion policies**) 页面查看可用的 IPS 策略，但如果不满足以下前提条件，则无法创建或修改自定义 IPS 策略：

设备支持

- Firepower 1000 系列
- Firepower 2100 系列
- Firepower 4100 系列
- 带有 AWS 的 威胁防御 virtual
- 带有 Azure 的 威胁防御 virtual

软件支持

s

设备必须至少运行版本 6.7 和 Snort 3。

如果您的设备运行的是 6.7 之前的版本，请升级设备。有关详细信息，请参阅[升级 FDM 托管设备](#)。

如果您的设备运行的是 Snort 2 版本 6.7，请注意，Snort 3.0 中可能不存在 Snort 2.0 中的某些入侵规则。有关详细信息，请参阅[从 Snort 2 切换到 Snort 3](#)。



Note 要了解设备正在运行的软件版本和 Snort 引擎，只需在[清单 \(Inventory\)](#) 页面上找到并选择设备，然后查看[设备详细信息 \(Device Details\)](#)

相关信息：

- [配置 Firepower 自定义 IPS 策略](#)
- [FDM 管理 访问控制规则中的自定义 IPS 策略](#)

配置 Firepower 自定义 IPS 策略

在 CDO 中为 FTD 设备创建或修改自定义 IPS 策略之前，请务必阅读 [自定义 Firepower 入侵防御系统策略](#)。

目前，CDO 不支持自定义 IPS 规则。您可以使用 Talos 提供的规则创建和修改自定义 IPS 策略，但不能创建自己的 IPS 规则并将其应用于自定义 IPS 策略。

如果您在 CDO 中创建或编辑 IPS 策略时遇到问题，请参阅[入侵防御系统故障排除](#)以了解详细信息。



Note 您无法删除自定义 IPS 策略的规则组中的规则或对其重新排序。


创建自定义 IPS 策略

按照以下程序使用 Talos 提供的 IPS 规则创建新的自定义 IPS 策略：

Procedure

步骤 1 在 CDO 导航窗格中，点击策略 (Policies)。

步骤 2 选择入侵策略 (Intrusion Policies)。

步骤 3 点击蓝色加号按钮 。

步骤 4 展开基本模板 (Base Template) 的下拉菜单。如果您的设备运行的是版本 7.2 和 Snort 3，则必须展开下拉列表，然后点击选择 (Choose) 以选择模板。如果设备运行的是版本 7.1.x 及更早版本，只需展开下拉菜单并选择以下选项之一即可。以下模板：

- **最大检测 (Maximum Detection)** - 此类策略适用于网络基础设施安全比在“安全优先于连接”策略中还要重要、且有可能产生更大运行影响的网络。

Tip **最大检测 (Maximum Detection)** 基础模板需要大量内存和 CPU 才能有效工作。CDO 建议使用此模板将 IPS 策略部署到 2100、3100、4100 或 威胁防御 virtual 等型号。

- **安全优先于连接 (Security Over Connectivity)** - 这些策略专为网络基础设施安全优先于用户便利性的网络而构建。此入侵策略将启用许多可能会提醒或丢弃合法流量的网络异常入侵规则。
- **平衡安全和连接 (Balanced Security and Connectivity)** - 这些策略专为速度和检测而构建。共同使用时，这些策略充当大多数网络和部署类型的良好起点。
- **连接优先于安全 (Connectivity Over Security)** - 这些策略专为连接（即能够获取所有资源）优先于网络基础设施安全的网络而构建。仅会启用阻止流量的最重要规则。
- **无活动规则 (No Rules Active)** - 默认情况下禁用策略中包含的规则。

步骤 5 输入策略的名称。

我们强烈建议使用与默认基本模板不同的唯一名称。如果您需要对 IPS 策略进行故障排除，思科 TAC 可以轻松找到自定义策略并恢复为默认策略；这样可以保护您的网络，而不会丢失您的自定义更改。

步骤 6 （可选）输入策略说明。

步骤 7 选择 IPS 模式 (IPS Mode)。

- **防御 (Prevention)** - 如果连接与实施流量丢弃操作的入侵规则匹配，则该连接会被主动阻止。

- **检测 (Detection)**- 如果连接匹配其操作为丢弃流量的入侵规则，操作结果将变为**将被阻止 (Would Have Blocked)**，并且不执行任何操作。

步骤 8 点击保存 (Save)。

后续步骤

将 IPS 策略添加到 FDM 管理 设备访问控制规则。有关详细信息，请参阅 [FDM 管理 访问控制规则中的自定义 IPS 策略](#)。

编辑自定义 IPS 策略

如果您已载入具有 IPS 策略的 FDM 管理设备，如果您在 FDM 中创建了 IPS 策略并且 CDO 从已部署的配置中读取该策略，或者您刚刚创建了新的 IPS 策略，则可以编辑现有 IPS 策略。


使用以下程序修改现有自定义 IPS 策略：

Procedure

步骤 1 在 CDO 导航窗格中，点击**策略 (Policies)**。

步骤 2 选择入侵策略 (**Intrusion Policies**)。

步骤 3 确定要编辑的 IPS 策略。点击**编辑 (Edit)**。

步骤 4 从页面顶部，点击编辑图标 。

步骤 5 编辑以下所需的字段：

- 基本模板。
- 名称。
- 说明。
- IPS 模式。

步骤 6 点击保存 (Save)。

步骤 7 立即 [预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

编辑自定义 IPS 策略中的规则组

您可以覆盖规则组中规则的默认操作。使用以下程序编辑规则组中包含的规则

Procedure

步骤 1 在 CDO 导航窗格中，点击策略。

步骤 2 选择入侵策略 (**Intrusion Policies**)。

步骤 3 确定要编辑的 IPS 策略。点击 **编辑 (Edit)**。

步骤 4 从左侧的规则组选项卡中，展开所需的规则组。从展开的列表中选择组。

步骤 5 编辑规则组：

- a) 通过选择安全级别栏来编辑整个规则组的安全级别。手动将安全级别拖至要应用于整个规则组的安全类型。点击 **提交**
- b) 通过展开位于右侧的规则下拉菜单，编辑单个规则的规则操作。
- c) 通过选中所需规则的复选框并展开位于规则表上方的下拉菜单，编辑多个规则的规则操作。此选择会影响所有选定的规则。
- d) 通过选中表的标题行中的复选框并展开位于规则表上方的下拉菜单，编辑所有规则的规则操作。此选择会影响规则组中的所有规则。

步骤 6 点击策略页面顶部的 **保存 (Save)**。

步骤 7 立即 [预览和部署所有设备的配置更改](#) 您所做的更改，或等待并一次部署多个更改。

删除自定义 IPS 策略

使用以下程序从 CDO 中删除自定义 IPS 策略：

Procedure

步骤 1 在 CDO 导航窗格中，点击策略。

步骤 2 选择入侵策略 (**Intrusion Policies**)。

步骤 3 确定要编辑的 IPS 策略。点击删除。

步骤 4 点击 **确定 (OK)** 以删除策略。

步骤 5 立即 [预览和部署所有设备的配置更改](#) 您所做的更改，或等待并一次部署多个更改。

安全情报策略

关于安全智能

通过安全智能策略能够根据源/目标 IP 地址或目标 URL 提前丢弃非必要流量。在使用访问控制策略评估列入受阻列表的流量前，系统会将其丢弃，从而减少系统资源的使用量。

您可以根据以下条件阻止流量：

- **思科 Talos 情报源 (Cisco Talos feeds)** - 思科 Talos 提供对定期更新的安全情报源的访问权限。具有安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的站点出现和消失的速度可能比您更新和部署自定义配置的速度要快。系统定期下载智能源更新，从而提供新的威胁智能，而无需重新部署配置。



Note 默认情况下，思科 Talos 情报源每小时更新一次。您可以更改更新频率，甚至可以根据需要更新源，方法是登录 Firepower 设备管理器并从主页导航：设备 (Device) > 更新 (Updates) > 查看配置 (View Configuration)。

- **网络和 URL 对象 (Network and URL objects)** - 如果您知道要阻止的特定 IP 地址或 URL，则可为其创建对象并将其添加到阻止列表或允许列表。

创建用于 IP 地址（网络）和 URL 的单独阻止和允许列表。

安全情报许可证要求

您必须在 FDM 管理设备上启用许可证才能使用安全智能。


有关详细信息，请参阅《适用于 Firepower 设备管理器的思科 FTD 配置指南》的“安全策略”一章的安全情报源类别部分。

配置 Firepower 安全情报策略


通过安全智能策略能够根据源/目标 IP 地址或目标 URL 提前丢弃非必要流量。所有允许的连接仍会通过访问控制策略进行评估，并且最终可能会被丢弃。您必须启用许可证，才能使用安全智能。

配置 Firepower 安全情报策略

Procedure

- 步骤 1** 在导航窗格中，点击**清单 (Inventory)**。
- 步骤 2** 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
- 步骤 3** 点击**FTD** 选项卡，然后选择要为其创建或编辑安全情报策略的 FDM 管理设备。
- 步骤 4** 在右侧的**管理 (Management)** 窗格中，点击  **策略**。
- 步骤 5** 在 FDM 管理设备策略页面中，点击策略栏中的 **安全情报**。
- 步骤 6** 如果策略未启用，请点击安全情报滑块将其启用，或点击关于安全情报信息框中的**启用 (Enable)**。

Note 您可以通过点击安全情报开关切换到关闭随时禁用策略。配置将被保留，因此，当您再次启用该策略时，无需重新配置。

- 步骤 7** 选择**阻止列表 (Blocked List)** 行。请注意，根据您的表视图，在“网络”、“网络对象”、“网络源”、“URL”、“URL 对象”和“URL 源”列中有加号 。

- 在将网络添加到阻止列表 (**Add Networks to Blocked List**) 对话框和将 URL 对象添加到阻止列表 (**Add URL Object to Blocked List**) 对话框中，可以搜索现有对象或根据需要创建对象。选中要阻止的对象，然后点击**选择 (Select)**。

Note 安全智能会忽略使用 /0 掩码的 IP 地址块。这包括 any-ipv4 和 any-ipv6 网络对象。不得选择将这些对象用于网络阻止操作。

- 在将 URL 对象添加到阻止列表 (Add URL Objects to Blocked List) 和将网络源添加到阻止列表 (Add Network Feeds to Blocked List) 对话框中，选中要阻止的源，然后点击选择 (Select)。您可以通过点击源行末尾的向下箭头来阅读源的说明。如[Firepower 安全情报策略的安全情报源](#)中所描述。

- 步骤 8** 如果您知道在上一步中指定的任何网络组、网络源、URL 对象或 URL 源中包含要对其设置例外的网络、IP 地址或 URL，请点击允许列表 (Allowed List) 行。
- 步骤 9** 为要设置例外的网络、IP 地址和 URL 选择或创建对象。当您点击选择 (Select) 或添加 (Add) 时，它们将被添加到“允许列表” (Allowed List) 行中。
- 步骤 10** (可选) 要记录安全情报策略生成的事件，请执行以下操作：
- 点击日志记录设置  图标来配置日志记录。如果启用了日志记录，系统会记录与阻止列表条目匹配的任意项。系统不记录例外条目的匹配项，但如果被免除的连接与启用日志记录的访问控制规则匹配，您会收到日志消息。
 - 通过点击连接事件日志记录 (Connection Events Logging) 开关启用事件日志记录。
 - 选择发送事件的位置：
 - 点击无 (None) 会将事件保存到 FDM 管理设备。它们在 FDM 事件查看器中显示。FDM 管理设备上的存储空间非常有限。最好通过定义系统日志服务器对象（而不是选择无）将连接事件存储在系统日志服务器上。
 - 点击创建 (Create) 或选择 (Choose) 可创建或选择由系统日志服务器对象表示的系统日志服务器，以向其发送日志记录事件。由于设备中的事件存储受限，所以将事件发送至外部系统日志服务器可供长期存储，并增强您的事件分析。

如果您订用了思科安全分析和日志记录，请使用 [SEC 的 IP 地址和端口](#) 来配置系统日志对象，将事件发送到安全事件连接器。有关此功能的详细信息，请参阅[思科安全分析和日志记录](#)。

- 步骤 11** (可选) 对于您创建的任何规则，您可以选择它并在“添加注释” (Add Comments) 字段中添加注释。要了解有关规则注释的详细信息，请参阅[向策略和规则集中的规则添加注释](#)。
- 步骤 12** 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

对 Firepower 安全情报策略阻止列表进行例外处理

对于在 [配置 Firepower 安全情报策略](#) 中创建的每个阻止列表，您可以创建关联的允许列表。允许列表的唯一目的是豁免阻止出现在阻止列表中的 IP 地址或 URL。也就是说，如果发现需使用且已知安全的地址或 URL 位于在阻止列表上配置的智能源中，则可以将该地址或 URL 添加到允许列表中，使其免于访问。这样，您就不用为了一个地址或 URL 而从阻止列表中删除整个源。

通过安全情报策略后，允许的流量随后会由访问控制策略进行评估。有关允许或丢弃连接的最终决定基于连接匹配的访问控制规则。访问规则还会决定恶意软件检查是否应用于连接。

Firepower 安全情报策略的安全情报源

下表介绍了思科 Talos 源中的可用类别。可以在网络和 URL 阻止列表中输入这些类别。

类别	说明
攻击者	出站恶意活动已知的活动扫描工具和列入组织名单的主机
bogon	Bogon 网络和未分配的 IP 地址。
僵尸	托管二进制恶意软件丢弃程序的站点。
CnC	托管僵尸网络的命令和控制服务器的站点。
dga	用于生成作为与命令和控制服务器的交汇点的大量域名的恶意软件算法。
exploitkit	指定用于识别客户端中的软件漏洞的软件包。
恶意软件	托管恶意软件二进制或漏洞包的站点。
open_proxy	允许匿名 Web 浏览的开放代理。
open_relay	已知用于垃圾邮件的开放邮件中继。
网络钓鱼	托管网络钓鱼页面的站点。
效率低下	主动参与恶意或可疑活动的 IP 地址和 URL。
垃圾邮件	已知用于发送垃圾邮件的邮件主机。
可疑	看似可疑并具有类似于已知恶意软件的特征的文件。
tor_exit_node	Tor 出口节点。

FDM 托管设备身份策略

身份策略概述

使用身份策略从连接中收集用户身份信息。然后，可以在控制面板中基于用户身份查看使用情况，并根据用户或用户组配置访问控制。通过将网络行为、流量和事件直接与单个用户和组相关联，系统可帮助您确定策略违规、攻击或网络漏洞的来源。

例如，可以确定入侵事件所攻击的主机的所有人是谁，并确定是谁发起了内部攻击或端口扫描。此外，还可以确定高带宽用户，以及正在访问不良网站或应用的用户。

然后，您可以根据控制面板中的用户身份来查看使用情况，并根据 Active Directory (AD) 领域对象（与该 AD 上的所有用户匹配）、特殊身份（例如身份验证失败、访客、无需身份验证或未知身份）或用户组。

可以使用以下方法获取用户身份：

- 被动身份验证 - 对所有类型的连接，从其他身份验证服务获取用户身份而不提示输入用户名和密码。
- 主动身份验证 - 提示输入用户名和密码，并根据指定身份源进行身份验证，获取源 IP 地址的用户身份（仅限于 HTTP 连接）。

通过被动身份验证确定用户身份

被动身份验证在收集用户身份信息时不提示用户输入用户名和密码。系统会从您指定的身份源获取映射。

您可以从以下源被动获取用户到 IP 地址的映射：

- 远程访问 VPN 登录。被动身份支持以下用户类型：
 - 在外部验证服务器中定义的用户账户。
 - 在 FDM 管理设备中定义的本地用户账户。
- 思科身份服务引擎 (ISE)；思科身份服务引擎被动身份连接器 (ISE-PIC)。

如果给定用户是通过多个源所识别，则远程访问 VPN 登录身份占优先地位。

通过主动身份验证确定用户身份

身份验证是确认用户身份的行为。

如果 HTTP 流量来自系统没有其用户身份映射的 IP 地址，通过主动身份验证，您可以决定是否针对为系统配置的目录对发起该流量的用户进行身份验证。如果身份验证成功，该 IP 地址则被视为具有该通过身份验证的用户的身份。

如身份验证不成功，用户对网络的访问并不会受阻。为这些用户提供哪些访问权限最终由访问规则决定。

处理未知用户

当您使用 FDM 管理为身份策略配置目录服务器后，FDM 管理会从目录服务器下载用户和组成员信息。Active Directory 信息每 24 小时在午夜刷新一次，或在每次您编辑和保存目录配置时刷新（即使您未进行任何更改）。

如果某用户在活动身份验证身份规则提示时成功进行了身份验证，但该用户的名称不在下载的用户身份信息中，则该用户会被标记为“未知”。您不会在与身份相关的控制面板中看到该用户的 ID，该用户也不会匹配组规则。

但是，系统将应用面向未知用户的任何访问控制规则。例如，如果您阻止未知用户的连接，那么即使这些用户成功进行了身份验证（即目录服务器可识别用户并且密码有效），他们也会被阻止。

因此，当您对目录服务器进行更改（例如添加或删除用户，或更改组成员身份）时，直到系统从目录下载更新之后这些更改才会反映在策略实施中。

如果您不希望每天都等到午夜进行更新，可以通过编辑目录领域信息（登录到 FDM 管理设备并导航至“对象” (Objects) > “身份源” (Identity Sources)，然后编辑领域）。点击确定 (OK)，然后部署更改。系统随即会下载更新。



Note 您可以登录 FDM 管理设备并导航至策略 (Policies) > 访问控制 (Access Control)，点击添加规则 (Add Rule) (+) 按钮，并在“用户” (Users) 选项卡上查看用户列表，从而检查 FDM 管理系统上是否有新的或已删除的用户信息。如果找不到新用户，或者还是可以找到已删除的用户，则系统的信息未更新。

如何实施 Firepower 身份策略

如果要使用 Cisco Defense Orchestrator (CDO) 管理 FDM 管理设备的身份策略，则需要先创建身份源。您可以使用 Defense Orchestrator 配置其余设置。

正确配置后，您将能够看到 FDM 中监控控制面板和事件中的用户名。您还将能够在访问控制和 SSL 解密规则中使用用户身份作为流量匹配条件。



Note 目前，CDO 无法配置实施身份策略所需的某些组件，例如远程接入 VPN 和思科身份服务引擎。这些组件必须在 FDM（设备的本地管理器）中进行配置。以下程序中的某些步骤表明，您必须使用 FDM 配置某些身份组件以实施身份策略。

操作步骤

以下过程概述您必须配置哪些内容才能正常使用身份策略：

Procedure

步骤 1 创建 AD 身份领域。不论您是主动使用用户身份，还是被动使用，都需要配置包含用户身份信息的 Active Directory (AD) 服务器。有关详细信息，请参阅[创建 FTD Active Directory 领域对象](#)。

步骤 2 如果您想要使用被动身份验证身份规则，请使用 **FDM** 来配置被动身份源。

根据您要在设备中实现的服务和网络中可用的服务，您可以配置任何以下内容。

- 远程访问 VPN - 如果您要支持到设备的远程访问 VPN 连接，用户登录可以提供基于 AD 服务器或本地用户（FDM 管理设备中定义的用户）的身份。有关配置远程访问 VPN 的详细信息，请参阅适用于您的设备的版本的[《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》](#)中的“配置远程访问 VPN”一章。
- 思科身份服务引擎 (ISE) 或思科身份服务引擎被动身份连接器 (ISE PIC) - 如果您使用这些产品，您可以将设备配置为 pxGrid 订阅方，并从 ISE 获取用户身份。有关说明，请参阅[《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》](#)的“配置身份服务引擎”一章。

- 步骤 3** 使用 **防御协调器**，启用身份策略并配置被动或主动身份验证。有关详细信息，请参阅[配置身份策略设置](#)。
- 步骤 4** 使用 **防御协调器**，[配置 Firepower 身份策略默认操作](#)。如果您打算仅使用被动身份验证，您可以将默认操作设置为被动身份验证，无需创建特定规则。
- 步骤 5** 使用 **防御协调器**，[配置身份规则](#)。创建将从相关网络收集被动或主动用户身份的规则。
- 步骤 6** （可选）对于您创建的任何规则，您可以选择它并在“添加注释” (Add Comments) 字段中添加注释。要了解有关规则注释的详细信息，请参阅[向策略和规则集中的规则添加注释](#)。
- 步骤 7** 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

配置身份策略

您可以使用身份策略从连接中收集用户身份信息。然后，可以在 FDM 控制面板中基于用户身份查看使用情况，并根据用户或用户组配置访问控制。

下文概述了如何配置通过身份策略获取用户身份所需的元素：

操作步骤

Procedure

- 步骤 1** 在导航窗格中，点击**清单 (Inventory)**。
- 步骤 2** 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
- 步骤 3** 点击 **FTD** 选项卡，选择要为其配置身份策略的设备，然后点击右侧**管理 (Management)** 窗格中的 **策略 (Policy)**。
- 步骤 4** 点击策略栏中的**身份 (Identity)**。
- 步骤 5** 如果尚未启用身份策略，请参阅**被动和主动身份验证**，然后点击**启用 (Enable)**。您正在启用身份策略，而不是被动身份验证策略或主动身份验证策略。策略中的规则将指定主动或被动身份验证。
- 步骤 6** 管理身份策略：

在配置身份设置后，此页面将按顺序列出所有规则。规则依据流量按照从上到下的顺序进行匹配，由第一个匹配项确定要应用的操作。从此页面中可以执行以下操作：

- 要启用或禁用身份策略，请点击身份策略开关。有关详细信息，请参阅[配置身份策略设置](#)。
- 要读取被动身份验证设置，请点击身份栏上**被动身份验证 (Passive Auth)** 标签旁边的按钮。有关详细信息，请参阅[配置身份策略设置](#)。
- 要启用主动身份验证，请点击身份栏上**主动身份验证 (Active Auth)** 标签旁边的按钮。有关详细信息，请参阅[配置身份策略设置](#)。
- 要更改默认操作，请点击默认操作按钮并选择所需的操作。请参阅[配置 Firepower 身份策略默认操作](#)。
- 要移动表中的规则，请选择该规则，然后点击规则表中该规则行末尾的向上或向下箭头。

- 要移动表中的规则，请选择该规则，然后点击规则表中该规则行末尾的向上或向下箭头。
- 要配置规则，请执行以下操作：
 - 要创建新规则，请点击加号  按钮。
 - 要编辑现有规则，请选择该规则，然后点击操作窗格中的编辑 (**Edit**)。也可以选择表中点击某规则属性来编辑该属性。
 - 要删除不再需要的规则，请选择该规则，然后在“操作”窗格中点击删除 (**Remove**)。

有关创建和编辑身份策略的更多信息，请参阅 [配置身份规则](#)。

步骤 7 (可选) 对于您创建的任何规则，您可以选择它并在“添加注释” (Add Comments) 字段中添加注释。要了解有关规则注释的详细信息，请参阅 [向策略和规则集中的规则添加注释](#)。

步骤 8 立即 [预览和部署所有设备的配置更改](#) 您所做的更改，或等待并一次部署多个更改。

配置身份策略设置

要正常使用身份策略，必须配置提供用户身份信息的源。必须配置的设置因配置的规则类型而异，而规则类型可以是被动和/或主动的。




Note 目前，CDO 无法配置实施身份策略所需的某些组件，例如 Active Directory 身份领域、远程访问 VPN 和思科身份服务引擎。这些组件必须在 FDM 中配置，FDM 是 FTD 设备的本地管理器。以下程序中的某些步骤表明，您必须使用 FDM 配置某些身份组件以实施身份策略。

操作步骤

Before you begin

确保目录服务器、FDM 管理设备和客户端之间的时间设置一致。这些设备间的时间偏差可能会导致用户身份验证操作失败。“一致”说明您可以使用不同的时区，但时间相对于这些时区应是相同的；例如，10 AM PST = 1 PM EST。

Procedure

- 步骤 1** 在导航窗格中，点击清单 (**Inventory**)。
- 步骤 2** 点击设备 (**Devices**) 选项卡以查找设备，或点击模板 (**Templates**) 选项卡以查找型号设备。
- 步骤 3** 点击 FTD 选项卡，选择要为其配置身份策略的设备，然后点击右侧管理 (**Management**) 窗格中的策略 (**Policy**)。
- 步骤 4** 通过点击身份切换启用身份策略。或者，您可以点击  按钮，查看被动和主动身份验证的说明，然后点击对话框中的启用 (**Enable**)。

步骤 5 读取被动身份验证设置。 点击身份栏上的被动身份验证 (**Passive Auth**) 按钮。

如果您已使用 Firepower 设备管理器配置远程访问 VPN 或思科身份服务引擎，则被动身份验证按钮显示已启用 (**Enabled**)。


必须配置至少一个被动身份源，才能创建被动身份验证规则。

步骤 6 配置主动身份验证。 如果身份规则要求对用户进行主动身份验证，则该用户将重定向到连接该用户所通过的界面上的强制网络门户，然后系统会提示用户进行身份验证。

- a) 点击身份栏上的主动身份验证 (**Active Auth**) 按钮。
- b) 如果尚未启用 SSL 说明，请点击启用 (**Enable**) 链接。如果您没有看到“启用”链接，请跳至步骤 "c"。

1. 从选择解密重签名证书 (**Select Decrypt Re-Sign Certificate**) 菜单，选择内部 CA 证书，以用于使用重签名证书实施解密的规则。

您可以使用预定义的 **NGFW-Default-InternalCA** 证书，或者点击菜单并选择创建或选择以创建新证书，或者选择已上传到 FDM 管理设备的证书。

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

Note 只有在未配置 SSL 解密策略的情况下，系统才会提示您进行 SSL 解密设置。要在启用身份策略之后更改这些设置，请编辑 SSL 解密策略设置。

2. 点击保存 (**Save**)。

- c) 点击服务器证书 (**Server Certificate**) 菜单以选择在主动身份验证期间提供给用户的内部证书。如果尚未创建所需的证书，请点击创建 (**Create**)。如果用户不上传其浏览器已经信任的证书，则必须接受该证书。
- d) 在端口 (**Port**) 字段中，输入适用于强制网络门户的端口号。默认端口是 885 (TCP)。如果配置了其他端口，则该端口必须在 1025-65535 的范围内。

Note 对于 HTTP Basic、HTTP Response Page 和 NTLM 身份验证方法，通过接口的 IP 地址可将用户重定向到强制网络门户。但对于 HTTP 协商，用户将使用完全限定 DNS 名称 `firewall-hostname.AD-domain-name` 进行重定向。如果想要使用 HTTP Negotiate，还必须更新 DNS 服务器以将此名称映射到您需要进行主动身份验证的所有内部接口的 IP 地址。否则，将无法进行重定向，用户也无法进行身份验证。

- e) 点击保存 (**Save**)。

步骤 7 继续 [配置 Firepower 身份策略默认操作](#)。

配置 Firepower 身份策略默认操作

身份策略会对不匹配任何身份规则的连接实施默认操作。


实际上，不设置规则是策略的有效配置。如果想在所有流量源上使用被动身份验证，只需将被动身份验证配置为默认操作。

操作步骤

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击**FTD** 选项卡，选择要为其配置身份策略的设备，然后点击右侧**管理 (Management)** 窗格中的  **策略 (Policy)**。

步骤 4 点击策略栏中的**身份 (Identity)**。

步骤 5 如果尚未配置身份策略设置，请[配置身份策略设置](#)。

步骤 6 在屏幕底部，点击“默认操作” (Default Action) 按钮，并从以下选项中选择一個：

- **被动身份验证 (Passive Auth)** - 对与任何身份规则都不匹配的连接，将使用所有已配置的被动身份源来确定用户身份。如果不配置任何被动身份源，使用被动身份验证作为默认选择等同于使用“无身份验证”。
- **无身份验证 (No Auth)** - 对与任何身份规则都不匹配的连接，不会确定用户身份。

步骤 7 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

配置身份规则

身份规则确定是否应收集用户身份信息以匹配流量。如果您不想收集用户身份信息以匹配流量，则可以配置“无身份验证”。

请记住，无论规则配置如何，都仅对 HTTP 流量进行主动身份验证。因此，无需创建规则将非 HTTP 流量从主动身份验证中排除。如果您希望获取所有 HTTP 流量的用户身份信息，只需将主动身份验证规则应用于所有源和目的。




Note 而且请记住，身份验证失败对网络访问没有影响。身份策略仅收集用户身份信息。如果要阻止无法进行身份验证的用户访问网络，则必须使用访问规则。

操作步骤

Procedure


步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，选择要为其配置身份策略的设备，然后点击右侧**管理 (Management)** 窗格中的  **策略 (Policy)**。

步骤 4 点击策略栏中的**身份 (Identity)**。

步骤 5 执行以下任一操作：

- 要创建新规则，请点击加号  按钮。要了解身份源对象及其对规则的影响，请参阅[为 FDM 管理 设备配置身份源](#)以了解详细信息。
- 要编辑现有规则，请点击要编辑的规则，然后点击右侧“操作” (Actions) 窗格中的**编辑 (Edit)**。
- 要删除不再需要的规则，请点击要删除的规则，然后在右侧“操作”窗格中点击**删除 (Remove)**。

步骤 6 在**顺序**中，选择要将该规则插入在已排序有序规则列表插入该规则的位置。

先匹配的规则先应用，所以您必须确保流量匹配条件标准较具体的规则显示在次之用来匹配流量的较通用条件标准的策略上方。

默认将规则添加到列表的末尾。如果以后要更改规则的位置，请编辑此选项。

步骤 7 在**名称 (Name)** 中输入规则的名称。

步骤 8 选择 FDM 管理 设备应对匹配项应用的操作，如有必要，还可以选择 **Active Directory (AD)** 身份源。

您必须选择包括用于被动和主动身份验证规则的用户账户的 AD 身份领域。选择以下之一：

- **被动身份验证** - 使用被动身份验证确定用户身份。系统将会显示所有已配置的身份源。此规则会自动使用所有已配置的源。
- **主动身份验证 (Active Auth)**使用主动身份验证确定用户身份。主动身份验证仅适用于 HTTP 流量。如果任何其他类型的流量与要求或允许主动身份验证的身份策略匹配，则不会尝试进行主动身份验证。
- **无身份验证** - 不获取用户身份。基于身份的访问规则不会应用于此流量。这些用户将标记为无需身份验证。

Note 对于**被动身份验证 (Passive Auth)** 和**主动身份验证 (Active Auth)**，您可以选择 AD 领域身份源。如果您没有准备好任何身份源对象，请点击**新建对象 (Create new object)** 以启动身份源对象向导。有关详细信息，请参阅[创建或编辑 Active Directory 领域对象](#)。

步骤 9 （仅主动身份验证。）点击**主动身份验证 (Active authentication)** 选项卡，然后选择您的目录服务器支持的身份验证方法（类型）。

- **HTTP 基本身份验证 (HTTP Basic)** - 使用未加密的 HTTP 基本身份验证连接对用户进行身份验证。用户通过其浏览器的默认身份验证弹出窗口登录网络。这是默认值。
- **NTLM** - 使用 NT LAN Manager (NTLM) 连接对用户进行身份验证。仅当选择了一个 AD 领域时，此选项才可用。用户使用其浏览器的默认身份验证弹出窗口登录网络，不过您可以将 Internet Explorer 和 Firefox 浏览器配置为使用其 Windows 登录域信息以透明方式进行身份验证。该任务在 FDM 中完成，有关说明，请参阅[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南 > 安全策略 > 身份策略 > 启用透明用户身份验证](#)。

- **HTTP 协商** - 允许设备协商用于用户代理（用户发起流量流所用的应用）和 Active Directory 服务器之间的方法。协商有助于使用广受支持的最强方法，顺序为先 NTLM，然后是 Basic 方法。用户通过其浏览器的默认身份验证弹出窗口登录网络。
- **HTTP 响应页面 (HTTP Response Page)**提示用户使用系统提供的网页进行身份验证。这是一种 HTTP Basic 身份验证方法。

Note 对于 HTTP Basic、HTTP Response Page 和 NTLM 身份验证方法，通过接口的 IP 地址可将用户重定向到强制网络门户。但对于 HTTP 协商，用户将使用完全限定 DNS 名称 *firewall-hostname.AD-domain-name* 进行重定向。如果想要使用 HTTP Negotiate，还必须更新 DNS 服务器以将此名称映射到您需要进行主动身份验证的所有内部接口的 IP 地址。否则，将无法进行重定向，用户也无法进行身份验证。

步骤 10 （仅主动身份验证。）选择以访客身份回退 (**Fall Back as Guest**) > 开/关 (**On/Off**)，确定是否将未通过主动身份验证的用户标记为访客用户。


用户有三次机会成功进行身份验证。如果仍不成功，选择此选项可以确定是否标记用户。您可以根据这些值部署访问规则。

- 以访客身份回退 (**Fall Back as Guest**) > 开 (**On**) - 系统将用户标记为“访客” (**Guest**)。
- 以访客身份回退 (**Fall Back as Guest**) > 关 (**Off**) - 用户标记为“访客” (**Guest**)。

步骤 11 在源 (**Source**) 和目标 (**Destination**) 选项卡上为被动身份验证、主动身份验证或无身份验证规则操作定义流量匹配条件。

请记住，仅在使用 HTTP 流量时才会尝试进行主动身份验证。因此，无需为非 HTTP 流量配置无身份验证规则，也无需为任何非 HTTP 流量创建主动身份验证规则。但是，被动身份验证适用于任何类型的流量。

身份规则的源/目标条件定义了流量通过的安全区（接口）、IP 地址或该 IP 地址所在的国家/地区或大洲（地理位置）或是流量中所用的协议和端口。默认设置为任何区域、地址、地理位置、协议和端口。

要修改条件，请点击该条件内的  按钮，选择所需的对象或元素，然后在弹出对话框中点击“确定” (OK)。如果条件需要对象，而所需的对象不存在，您可以点击**创建新对象 (Create New Object)**。

要从条件中删除对象，请将鼠标悬停在对象上，然后点击 X。

可以配置以下流量匹配条件。

源区域、目标区域

安全区对象，定义通过其传递流量的接口。可以定义一个或两个条件，也可以不定义任何条件：未指定的任何条件都将应用到任何接口上的流量。

- 要匹配从区域中的接口离开设备的流量，请将该区域添加至目标区域。
- 要匹配从区域中的接口进入设备的流量，请将该区域添加至源区域。
- 如果同时向一条规则添加源区域和目标区域条件，匹配流量必须源自其中一个指定源区域并通过其中一个目标区域流出。

如果应基于流量进入或离开设备的位置来应用规则，请使用此条件。例如，如果要确保从源自内部网络的所有流量收集用户身份，请选择内部区域作为源区域，同时将目标区域留空。

Note 不能在同一规则中搭配使用被动和路由安全区域。此外，被动安全区域只能被指定为源区域，不能作为目标区域。

源网络、目标网络

定义流量的网络地址或位置的网络对象或地理位置。

- 要匹配来自某个 IP 地址或地理位置的流量，请配置源网络。
- 要匹配流向 IP 地址或地理位置的流量，请配置目标网络。
- 如果同时向一条规则添加源网络条件和目标网络条件，匹配流量必须源自其中一个指定 IP 地址并流向其中一个目标 IP 地址。

添加此条件时，可从以下选项卡中进行选择：

- **网络 (Network)** - 为您要控制的流量选择定义源或目标 IP 地址的网络对象或组。
- **国家/地区/大洲 (Country/Continent)** - 选择要基于流量的源或目的国家/地区或大洲控制流量的地理位置。选择大洲将会选择该大洲内的所有国家/地区。除了直接在规则中选择地理位置外，也可以选择您创建的地理位置对象来定义位置。使用地理位置，可以便捷地限制对特定国家/地区的访问，而不需要知道此位置所用的全部潜在 IP 地址。
- **自定义地理位置 (Custom Geolocation)** - 选择（或创建）具有您指定的国家/地区和大洲的地理位置对象。

Note 为了确保使用最新地理位置数据过滤流量，思科强烈建议您定期更新地理位置数据库 (GeoDB)。有关详细信息，请参阅[更新地理位置数据库](#)。

源端口、目标端口/协议

定义流量中所用协议的端口对象。对于 TCP/UDP，这可能包括端口。

- 要匹配来自协议或端口的流量，请配置源端口。源端口只能为 TCP/UDP。
- 要匹配流向协议或端口的流量，请配置目标端口/协议。
- 要同时匹配来自特定 TCP/UDP 端口的流量和流向特定 TCP/UDP 端口的流量，请配置源端口和目标端口。如果同时将源和目标端口添加至条件，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，您可以匹配从端口 TCP/80 流至端口 TCP/8080 的流量。

步骤 12 点击**保存 (Save)**。

步骤 13 返回**清单 (Inventory)** 页面。

步骤 14 选择已将规则添加到身份策略的设备。

步骤 15 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

SSL 解密策略

某些协议（如 HTTPS）使用安全套接字层 (SSL) 或其后续版本传输层安全性 (TLS) 来加密流量以进行安全传输。由于系统无法检查加密连接，因此，如果要应用可考虑借助更高层流量特性进行访问决策的访问规则，则必须应用 SSL 解密策略将其解密。



Caution 请记住，解密并重新加密流量会增加设备的处理负载，从而降低整体系统性能。

继续讨论以下主题：

- [关于 SSL 解密](#)
- [如何实施和维护 SSL 解密策略](#)
- [配置 SSL 解密策略](#)
- [为已知密钥和重签解密配置证书](#)
- [为解密重签名规则下载 CA 证书](#)
- [SSL 解密问题故障排除](#)

如何实施和维护 SSL 解密策略

您可以使用 SSL 解密策略将加密流量转换为纯文本流量，以便可应用 URL 过滤、入侵和恶意软件控制以及其他需要深度数据包检测的服务。如果策略允许流量通过，则流量在离开设备前会被重新加密。

SSL 解密策略仅适用于加密流量。系统不会根据 SSL 解密规则评估未加密连接。

与其他一些安全策略不同的是，您需要监控并积极维护 SSL 解密策略，这是因为目标服务器上的证书可能会过期甚至发生变更。此外，客户端软件的变更可能会改变解密某些连接的能力，这是因为解密重签名操作无法与中间人攻击区分开来。

以下程序介绍了实施和维护 SSL 解密策略的端到端流程。

操作步骤

Procedure

步骤 1 如果要实施解密重签名规则，请创建所需的内部 CA 证书。

必须使用内部证书颁发机构 (CA) 证书。您有以下选择：由于用户必须信任证书，因此应上传客户端浏览器已配置为可信任的证书，或确保所上传的证书已添加到浏览器信任存储区。

- 创建由设备自身签署的自签名内部 CA 证书。请参阅《[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#)》> 可重用对象 > 证书 > 生成自签名内部和内部 CA 证书。

- 上传由外部受信任 CA 或组织内部 CA 签署的内部 CA 证书和密钥。请参阅《[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#)》>可重用对象>证书>上传内部和内部 CA 证书。

步骤 2 如果要实施解密已知密钥规则，请从各内部服务器收集证书和密钥。

只可将解密已知密钥用于您所控制的服务器，这是因为必须从服务器中获取证书和密钥。上传这些证书和密钥，作为内部证书（而不是内部 CA 证书）。请参阅《[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#)》>可重用对象>证书>上传内部和内部 CA 证书。

步骤 3 配置 SSL 解密策略。

启用该策略时，还需要配置一些基本设置。

步骤 4 配置默认 SSL 解密操作

如有疑问，请选择不解密作为默认操作。在适当的情况下，访问控制策略仍然可以丢弃与默认 SSL 解密规则匹配的流量。

步骤 5 配置 SSL 解密规则。

标识要解密的流量以及要应用的解密类型。

步骤 6 如要配置已知密钥解密，请编辑 SSL 解密策略设置，以加入这些证书。请参阅[为已知密钥和重签解密配置证书](#)。

步骤 7 如有需要，下载用于解密重签名规则的 CA 证书并将其上传到客户端工作站上的浏览器。

有关下载证书并将其分发给客户端的信息，请参阅[为解密重签名规则下载 CA 证书](#)。

步骤 8 定期更新重新签名已知密钥证书。

- 重签名证书 - 在证书过期之前更新此证书。如果通过 Firepower 设备管理器生成证书，则有效期为 5 年。要确定证书何时到期，请从“对象” (Objects) 页面点击证书的查看图标。
- 已知密钥证书 - 对于任何已知密钥解密规则，需要确保已上传目标服务器的当前证书和密钥。只要所支持的服务器上的证书和密钥发生更改，就必须上传新的证书和密钥（作为内部证书）并更新 SSL 解密设置，以使用新证书。

步骤 9 上传外部服务器缺失的受信任 CA 证书。

系统包含各种由第三方颁发的受信任根证书和中间证书。为解密重签名规则协商 FDM 管理设备和目标服务器之间的连接时，需要这些证书。

将根 CA 的信任链中的所有证书都上传到受信任 CA 证书列表中，包括根 CA 证书和所有中间 CA 证书。否则，更难检测由中间 CA 颁发的受信任证书。在“对象” (Objects)>“证书” (Certificates) 页面上上传证书。请参阅《[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#)》>可重用对象>证书>上传受信任的 CA 证书。

关于 SSL 解密

通常情况下，访问控制策略会确定是允许还是阻止网络连接。但是，如果启用 SSL 解密策略，则连接将首先被发送至 SSL 解密策略，以确定应将其解密还是阻止。然后，访问控制策略评估任何未被阻止的连接（无论是否解密），作出最终的允许/阻止决策。



Note 您必须启用 SSL 解密策略，才能在身份策略中实施有效的身份验证规则。如果您启用 SSL 解密来启用身份策略，但不想另外实施 SSL 解密，请在“SSL 解密” (SSL Decryption) 页面中选择“不解密” (Do Not Decrypt) 作为默认操作，并且不要创建其他 SSL 解密规则。身份策略会自动生成所需的任何规则。

以下主题更详细地介绍了加密流量管理和解密。

- [为什么要实施 SSL 解密？](#)
- [自动生成的 SSL 解密规则](#)
- [处理不可解密流量](#)

为什么要实施 SSL 解密？

无法检查 HTTPS 连接等加密流量。许多连接均是合法加密的连接，比如与银行和其他金融机构的连接。许多网站使用加密保护隐私或敏感数据。例如，加密与 Firepower 设备管理器的连接。但是，用户也可能会隐藏加密连接中的不良流量。

通过实施 SSL 解密，可解密和检查连接，确保不含威胁或其他不良流量，然后重新加密后再允许继续连接。（解密流量通过访问控制策略，并根据检查的加密连接特征而不是加密特征匹配规则。）这平衡了应用访问控制策略的需求与用户保护敏感信息的需求。

还可以配置 SSL 解密规则，阻止明确不想要允许其进入网络的加密流量类型。



Caution 请记住，解密并重新加密流量会增加设备的处理负载，从而降低整体系统性能。

可应用于加密流量的操作

配置 SSL 解密规则时，可应用以下主题中所述的操作。这些操作也可用于默认操作（适用于与显示规则不匹配的任何流量）。

- [解密重签名](#)
- [解密已知密钥](#)
- [不解密](#)
- [阻止](#)



Note 通过 SSL 解密策略的任何流量均必须通过访问控制策略。除了 SSL 解密策略中丢弃的流量外，最终的允许或丢弃决定还取决于访问控制策略。

解密重签名

如果选择解密或重签流量，系统将扮演中间人的角色。

例如，用户在浏览器中键入 <https://www.cisco.com>。流量到达 FTD 设备，然后设备使用规则中指定的 CA 证书与用户进行协商，并在用户和 FTD 设备之间建立 SSL 隧道。同时，设备连接至 <https://www.cisco.com>，并在服务器和 FTD 设备之间建立 SSL 隧道。

因此，用户将看到配置用于 SSL 解密规则的 CA 证书，而不是来自 www.cisco.com 的证书。用户必须信任该证书才能完成连接。FTD 设备随后对用户和目标服务器之间的流量执行双向解密/重新加密。



Note 如果客户端不信任用于对服务器证书重新签名的 CA，则会警告用户不应信任该证书。为了避免此情况，请将 CA 证书导入到客户端信任的 CA 库。或者，如果组织拥有专用 PKI，则可以颁发由根 CA（自动受组织中的所有客户端信任）签名的中级 CA 证书，然后将该 CA 证书上传到设备。

如果配置具有“解密重签名” (Decrypt Re-Sign) 操作的规则，则除任何已配置的规则条件外，该规则会根据所引用的内部 CA 证书的签名算法类型来匹配流量。由于您可以选择用于 SSL 解密策略的单个重签名证书，因此可以限制匹配重签规则的流量。

例如，仅当重签名证书是基于 EC 的 CA 证书时，使用椭圆曲线 (EC) 算法加密的出站流量才能匹配解密重签名规则。同样，仅当全局重签名证书为 RSA 时，使用 RSA 算法加密的流量才可与解密重签名规则匹配；即使所有其他配置的规则条件匹配，使用 EC 算法加密的出站流量也与规则不匹配。

解密已知密钥

如果您拥有目标服务器，则可使用已知密钥实现解密。在这种情况下，用户打开 <https://www.cisco.com> 的连接后，用户会看到 www.cisco.com 的实际证书，即使出示证书的是 FTD 设备。



您的组织必须是域和证书的所有者。以 `cisco.com` 为例，让最终用户查看思科证书的唯一可能方式是，您实际拥有域 `cisco.com`（即您是思科系统公司）并拥有由公共 CA 签名的 `cisco.com` 证书。您仅可使用已知密钥对您的组织拥有的站点进行解密。

使用已知密钥进行解密的主要目的是对通往 HTTPS 服务器的流量进行解密，以保护服务器免受外部攻击。如要检查流向外部 HTTPS 站点的客户端流量，由于您不是服务器所有者，所以必须使用解密重签名。



Note 要使用已知密钥解密，必须将服务器证书和密钥上传为内部身份证书，再在 SSL 解密策略设置中将其添加至已知密钥证书。然后，可部署已知密钥解密规则，其中服务器地址为目标地址。有关将证书添加到 SSL 解密策略的信息，请参阅[配置 SSL 解密策略](#)。

不解密

如果选择绕行某些类型的流量的解密，则不会对流量进行任何处理。系统会使加密流量继续进入访问控制策略，根据流量所匹配的访问控制规则对其执行允许或丢弃操作。

阻止

您可以简单地阻止匹配 SSL 解密规则的加密流量。阻止 SSL 解密策略可防止连接到访问控制策略。

阻止 HTTPS 连接后，用户看不到系统默认阻止响应页面。相反，用户会看到浏览器显示安全连接故障的默认页面。错误消息不会指明该站点由于策略而被阻止。相反，错误可能显示为没有通用的加密算法。据此消息，无法明确看出是您有意阻止了该连接。

自动生成的 SSL 解密规则

无论您是否启用 SSL 解密策略，FDM 管理设备都会自动为实施主动身份验证的各身份策略规则生成解密重签名规则。这是为 HTTPS 连接启用主动身份验证的必然要求。

启用 SSL 解密策略后，您可以在“身份策略主动身份验证规则”标题下看到这些规则。这些规则归入 SSL 解密策略顶部。这些规则为只读格式。仅可通过更改身份策略进行更改

处理不可解密流量

有几个特点使得连接不可解密。如果连接具有以下任何特征，则默认操作将应用于该连接，而不管该连接本可能会与哪个规则匹配。如果将“阻止”选作默认操作（而不是“不解密”），则可能会出问题，包括过度丢弃合法流量的问题。

- 压缩会话 - 数据压缩应用于连接。
- SSLv2 会话 - 支持的最低 SSL 版本是 SSLv3。
- 未知密码套件 - 系统无法识别连接的密码套件。
- 不受支持的密码套件 - 系统不支持根据检测到的密码套件进行解密。
- 会话未缓存 - SSL 会话已启用会话重复使用，客户端和服务器使用会话标识符重新建立了该会话，并且系统未缓存该会话标识符。

- 握手错误 - SSL 握手协商期间出错。
- 解密错误 - 解密操作期间出错。
- 被动接口流量 - 被动接口（被动安全区）上的所有流量均无法解密。

SSL 解密策略的许可证要求

使用 SSL 解密策略无需特殊许可证。

但需要 URL 许可证创建将 URL 类别和信誉作为匹配标准的规则。有关配置许可的详细信息，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》> 许可系统 > 启用或禁用可选许可证。

SSL 解密准则

配置和监控 SSL 解密策略时，请注意以下事项：

- 对于与设置为信任或阻止的访问控制规则匹配的任何连接，如果这些规则满足以下条件，则绕过 SSL 解密策略：
 - 将安全区、网络、地理位置和端口仅用作流量匹配条件。
 - 排在任何要求检测的其他规则之前，例如，基于应用或 URL 匹配连接的规则，或允许应用入侵或文件检测的规则。
- 使用 URL 类别匹配时，请注意，有时候站点登录页的类别与站点本身的类别不同。例如，Gmail 的类别是“基于网页的邮件”，而登录页的类别是“互联网门户网站”。要对到这些站点的连接解密，必须在规则中添加这两个类别。
- 如果您有任何主动身份验证规则，将无法禁用 SSL 解密策略。要禁用 SSL 解密策略，您必须禁用身份策略，或者删除任何使用主动身份验证的身份规则。

配置 SSL 解密策略

您可以使用 SSL 解密策略将加密流量转换为纯文本流量，以便可应用 URL 过滤、入侵和恶意软件控制以及其他需要深度数据包检测的服务。如果策略允许流量通过，则流量在离开设备前会被重新加密。

SSL 解密策略仅适用于加密流量。系统不会根据 SSL 解密规则评估未加密连接。



Caution

请记住，解密并重新加密流量会增加设备的处理负载，从而降低整体系统性能。



Note

VPN 隧道在 SSL 解密策略评估之前已解密，因此该策略永远不适用于隧道本身。但是，隧道内的任何加密连接都要通过 SSL 解密策略进行评估。

以下程序介绍了如何配置 SSL 解密策略。有关创建和管理 SSL 解密的端到端流程说明，请参阅 [如何实施和维护 SSL 解密策略](#)。

操作步骤

Before you begin

SSL 解密规则表包含两个部分：

- **身份策略主动身份验证规则** - 如果启用身份策略并创建使用主动身份验证的规则，系统将自动创建使这些策略生效所需的 SSL 解密规则。这些规则始终在您自己创建的 SSL 解密规则之前进行评估。只可通过更改身份策略来间接更改这些规则。
- **SSL 本机规则** - 这些是已经配置的规则。只能将规则添加到此部分。

Procedure

步骤 1 在导航窗格中，点击清单 (**Inventory**)。

步骤 2 点击设备 (**Devices**) 选项卡以查找设备，或点击模板 (**Templates**) 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择要创建 SSL 策略的设备。

步骤 4 点击右侧管理 (**Management**) 窗格中的 **策略 (Policy)**。

步骤 5 点击策略栏中的 **SSL 解密 (SSL Decryption)**。


步骤 6 如果尚未启用该策略，请点击启用 **SSL 解密 (Enable SSL Decryption)** 并按照 [启用 SSL 解密策略](#) 中的说明来配置策略设置。

步骤 7 配置策略的默认操作。最安全的选择是不解密。有关详细信息，请参阅适用于您的设备的版本的《[适用于 Firepower 设备管理器的 Cisco Firepower 威胁防御配置指南](#)》中“安全策略”一章的 **配置默认 SSL 解密操作** 部分。

步骤 8 管理 SSL 解密策略。

在配置 SSL 解密设置后，此页面将按顺序列出所有规则。规则依据流量按照从上到下的顺序进行匹配，由第一个匹配项确定要应用的操作。从此页面中可以执行以下操作：

- 要禁用该策略，请点击 **SSL 解密策略** 开关。可以通过点击启用 **SSL 解密** 重新启用该策略。
- 要编辑策略设置（包括策略中使用的证书列表），请点击 **SSL 工具栏** 上的配置按钮：

。此外，还可以下载与解密重签名规则一起使用的证书，以便将其分发给客户端。请参阅适用于您的设备的版本的《[适用于 Firepower 设备管理器的 Cisco Firepower 威胁防御配置指南](#)》中“安全策略”一章的以下部分：

- 为已知密钥和重签解密配置证书
 - 为解密重签名规则下载 CA 证书
- 要配置规则，请执行以下操作：

- 要创建新规则并记录它生成的事件，请点击蓝色加号按钮 。请参阅[配置 SSL 解密规则](#)。
- 要编辑现有规则，请在规则表中点击该规则，然后点击“操作” (Actions) 窗格中的**编辑 (Edit)**。也可以选择表中点击某规则属性来编辑该属性。
- 要删除不再需要的规则，请在规则表中点击该规则，然后在“操作”窗格中点击**删除 (Remove)**。
- 要移动规则，请将鼠标光标悬停在规则表中。在行的最后，使用向上和向下箭头移动其与规则表的位置。
- (可选) 对于您创建的任何规则，您可以选择它并在“添加注释” (Add Comments) 字段中添加注释。要了解有关规则注释的详细信息，请参阅[向策略和规则集中的规则添加注释](#)。

步骤 9 继续启用 SSL 解密策略。

启用 SSL 解密策略

在可以配置 SSL 解密规则之前，必须启用该策略并配置一些基本设置。以下程序介绍了如何直接启用该策略。此外，还可在启用身份策略时启用该策略。身份策略要求启用 SSL 解密策略。

操作步骤

Before you begin

如果从未设置 SSL 解密策略的版本进行升级，但已使用主动身份验证规则配置身份策略，则 SSL 解密策略已启用。确保已选择要使用的解密重签名证书，并且可以选择启用预定义规则。

查看[配置 SSL 解密策略](#)（如果尚未配置）。

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击**FTD** 选项卡和要为其启用 SSL 解密策略的设备。

步骤 4 点击右侧**管理 (Management)** 窗格中的**策略 (Policy)**。

步骤 5 点击策略栏中的**SSL 解密 (SSL Decryption)**。


步骤 6 点击 SSL 栏中的**SSL 解密 (SSL Decryption)** 开关以启用 SSL 解密策略。

- 如果这是您首次启用该策略，请阅读解密已知密钥和解密重签 SSL 解密的说明，然后点击启用。

- 如果已对策略进行过一次配置然后禁用了策略，则只需使用之前的设置和规则即可再次启动该策略。您可以单击 **SSL 解密配置按钮**  **NGFW-Default-InternalCA** [为已知密钥和重签解密配置证书](#)，并如中所述配置设置。

步骤 7 对于 **选择解密重签名证书**，请选择内部 CA 证书，以用于使用重签名证书实施解密的规则。

您可以使用预定义的 NGFW-Default-InternalCA 证书，也可以使用您创建或上传的证书。如果尚无证书，请点击 **创建 (Create)** 以添加 FDM 管理设备内部 CA 证书。

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

步骤 8 单击 **保存 (Save)**。

步骤 9 继续 [配置默认 SSL 解密操作](#)，以便为策略设置默认操作。

配置默认 SSL 解密操作

如果加密连接没有匹配特定 SSL 解密规则，则由 SSL 解密策略的默认操作来处理。

操作步骤

Before you begin

如果还没有，请查看这些程序并按照其中的程序进行操作：

1. [配置 SSL 解密策略](#)
2. [启用 SSL 解密策略](#)

Procedure

步骤 1 在导航窗格中，单击 **清单 (Inventory)**。

步骤 2 单击 **设备 (Devices)** 选项卡以查找设备，或单击 **模板 (Templates)** 选项卡以查找型号设备。

步骤 3 单击 **FTD** 选项卡，然后选择要为其配置默认 SSL 解密操作的设备。

步骤 4 单击右侧 **管理 (Management)** 窗格中的 **策略 (Policy)**。

步骤 5 单击策略栏中的 **SSL 解密 (SSL Decryption)**。

步骤 6 单击 **默认操作 (Default Action)** 按钮。

步骤 7 选择应用于匹配流量的操作：

- **不解密** - 允许加密连接。然后，访问控制策略将评估加密连接，并根据访问控制规则丢弃或允许该连接。
- **阻止** - 立即丢弃连接。连接将不传递到访问控制策略。

步骤 8 （可选。）针对默认操作配置日志记录。您必须启用日志记录以便从 SSL 解密策略捕获事件。从以下选项中选择：

- **连接结束时** - 在连接结束时生成事件。
 - 将连接事件发送到 (**Send Connection Events To**) - 如果要将事件副本发送至外部系统日志服务器，请选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，请点击创建新系统日志服务器，并创建对象。（要对系统日志服务器禁用日志记录，请从服务器列表中选择“任何”）。

由于设备中的事件存储受限，所以将事件发送至外部系统日志服务器可供长期存储，并增强您的事件分析。

如果订用了思科安全分析和日志记录，请[使用安全事件连接器的 IP 地址和端口来指定或创建系统日志服务器](#)。有关此功能的详细信息，请参阅[思科安全分析和日志记录](#)。

- **无日志记录 (No logging)** - 不生成任何事件。

步骤 9 点击**保存 (Save)**。

步骤 10 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

配置 SSL 解密规则

使用 SSL 解密规则确定如何处理加密连接。SSL 解密策略中的规则按从上到下的顺序进行评估。对流量应用的规则是符合所有流量条件标准的第一个规则。

只可在“SSL 本机规则”部分创建和编辑规则。



Caution 请记住，解密并重新加密流量会增加设备的处理负载，从而降低整体系统性能。



Note 在 SSL 解密策略评估连接之前，系统将对 VPN 连接（站点间和远程访问）流量进行解密。因此，SSL 解密规则永远不会应用于 VPN 连接，且在创建这些规则时不需要考虑 VPN 连接。但是，系统会对 VPN 隧道中使用的所有加密连接进行评估。例如，SSL 解密规则将对通过 RA VPN 连接到内部服务器的 HTTPS 连接进行评估，即使 RA VPN 隧道本身没有接受评估（原因在于其已解密）



操作步骤

Before you begin

如果还没有，请查看[配置 SSL 解密策略](#)、[启用 SSL 解密策略](#)和[配置默认 SSL 解密操作](#)，以配置将向其添加规则的 SSL 解密策略。

如要创建解密已知密钥规则，请确保上传目标服务器的证书和密钥（作为内部证书），并编辑 SSL 解密策略设置，以使用该证书。已知密钥规则通常在该规则目标网络条件中指定目标服务器。有关详细信息，请参阅[为已知密钥和重签解密配置证书](#)。

Procedure

- 步骤 1** 在导航窗格中，点击**清单 (Inventory)**。
- 步骤 2** 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
- 步骤 3** 点击**FTD** 选项卡，然后选择要为其启用 SSL 解密策略的设备。
- 步骤 4** 点击右侧“管理” (Management) 窗格中的**策略 (Policy)**。
- 步骤 5** 点击策略栏中的**SSL 解密 (SSL Decryption)**。
- 步骤 6** 执行以下任一操作：
 - 要创建新规则，请点击蓝色加号  按钮。
 - 要编辑现有规则，请点击规则的编辑图标 。
 - 要删除不再需要的规则，请点击该规则的删除图标 。
- 步骤 7** 在**顺序 (Order)** 中，选择要在规则编号列表中插入规则的位置。


只可将规则插入 SSL 本机规则部分。身份策略主动身份验证规则将根据身份策略自动生成并且为只读形式。

先匹配的规则先应用，所以您必须确保流量匹配条件标准较具体的规则显示在次之用来匹配流量的较通用条件标准的策略上方。

默认将规则添加到列表的末尾。如果以后要更改规则的位置，请编辑此选项。
- 步骤 8** 在**名称 (Name)** 中输入规则的名称。

名称不能包含空格。可以使用字母数字字符和以下特殊字符：+ . _ -
- 步骤 9** 选择应用于匹配流量的操作。有关每个选项的详细讨论，请参阅下列内容：
 - [解密重签名](#)
 - [解密已知密钥](#)
 - [不解密](#)
 - [阻止](#)
- 步骤 10** 使用以下选项卡的任意组合，定义流量匹配标准：
 - **源/目标** - 流量通过的安全区（接口）、IP 地址或该 IP 地址的国家/地区或大洲（地理位置）或者流量中使用的 TCP 端口。默认设置为任何区域、地址、地理位置和 TCP 端口。请参阅 [SSL 解密规则的源/目标条件](#)。
 - **URL** - Web 请求的 URL 类别。默认情况下，进行匹配时不考虑 URL 类别和信誉。请参阅 [SSL 解密规则的 URL 标准](#)。
 - **应用** - 应用或按类型、类别、标记、风险或业务相关性定义应用的过滤器。默认设置为任何加密应用。请参阅 [SSL 解密规则的应用标准](#)。

- **用户** - 用户或用户组。身份策略决定了用户和组的信息是否可用于流量匹配。只有配置身份策略，才能使用此条件标准。请参阅 [SSL 解密规则的用户条件](#)。
- **高级** - 从连接中使用的证书派生的特性，例如 SSL/TLS 版本和证书状态。请参阅 [SSL 解密规则的高级条件](#)。

要修改条件，请点击该条件内的蓝色加号按钮 ，选择所需的对象或元素，然后在弹出对话框中点击**选择 (Select)**。如果条件需要对象，而所需的对象不存在，您可以点击**创建新对象 (Create New Object)**。点击对象或元素对应的 **x**，可将其从策略中移除。

向 SSL 解密规则中添加条件时，请考虑以下提示：

- 您可以为每个规则配置多个条件。要使规则应用于流量，流量必须匹配该规则中的所有条件。例如，可以使用单一规则来基于 URL 类别对流量进行解密。
- 最多可以为规则中的每个条件添加 50 个标准。匹配某个条件所有条件标准的流量满足该条件。例如，您可以使用单一规则为最多 50 个应用或应用过滤器执行应用控制。因此，单一条件中的项目之间为 OR 关系，但不同条件类型之间（例如，源/目的和应用之间）为 AND 关系。
- 匹配 URL 类别需要 URL 许可证。

步骤 11 （可选。）针对规则配置日志记录。

对于与控制面板或事件查看器中包括的规则匹配的流量，必须为其启用日志记录。从以下选项中选择：

- **无日志记录 (No logging)** - 不生成任何事件。
- **将连接事件发送到** - 如果要将事件副本发送至外部系统日志服务器，请选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，请点击**创建 (Create)**并创建对象。（要对系统日志服务器禁用日志记录，请从服务器列表中选择“任何”）。
- **连接结束时** - 在连接结束时生成事件。由于设备中的事件存储受限，所以将事件发送至外部系统日志服务器可供长期存储，并增强您的事件分析。

如果订用了思科安全分析和日志记录，请使用安全事件连接器的 IP 地址和端口来指定或[创建系统日志服务器对象](#)。有关详细信息，请参阅[思科安全分析和日志记录](#)。


步骤 12 点击保存 (Save)。

步骤 13 （可选）对于您创建的任何规则，您可以选择它并在“添加注释” (Add Comments) 字段中添加注释。要了解有关规则注释的详细信息，请参阅[向策略和规则集中的规则添加注释](#)。

步骤 14 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

SSL 解密规则的源/目标条件

SSL 解密规则的源/目标条件定义了流量通过的安全区（接口）、IP 地址或该 IP 地址所在的国家/地区或大洲（地理位置）或是流量中所用的 TCP 端口。默认设置为任何区域、地址、地理位置、协议和任何 TCP 端口。TCP 是与 SSL 解密规则匹配的唯一协议。

要修改条件，请点击该条件内的蓝色按钮 ，选择所需的对象或元素，然后点击**选择 (Select)**。如果条件需要对象，而所需的对象不存在，您可以点击**创建新对象 (Create New Object)**。点击对象或元素对应的 **x**，可将其从策略中移除。

源区域、目标区域

安全区对象，定义通过其传递流量的接口。可以定义一个或两个条件，也可以不定义任何条件：未指定的任何条件都将应用到任何接口上的流量。

- 要匹配从区域中的接口离开设备的流量，请将该区域添加至目标区域。
- 要匹配从区域中的接口进入设备的流量，请将该区域添加至源区域。
- 如果同时向一条规则添加源区域和目标区域条件，匹配流量必须源自其中一个指定源区域并通过其中一个目标区域流出。

如果应基于流量进入或离开设备的位置来应用规则，请使用此条件。例如，如果要确保从外部主机到内部主机的所有流量均被解密，则应将外部区域选为源区域，并将内部区域选为目标区域。

源网络、目标网络

定义流量的网络地址或位置的网络对象或地理位置。

- 要匹配来自某个 IP 地址或地理位置的流量，请配置源网络。
- 要匹配流向 IP 地址或地理位置的流量，请配置目标网络。

如果同时向一条规则添加源网络条件和目标网络条件，匹配流量必须源自其中一个指定 IP 地址并流向其中一个目标 IP 地址。

添加此条件时，可从以下菜单选项中进行选择：

- **网络** - 为您要控制的流量选择定义源或目标 IP 地址的网络对象或组。



Note 对于解密已知密钥规则，请选择使用目标服务器 IP 地址的对象（该对象使用您上传的证书和密钥）。

- **国家/地区/大洲 (Country/Continent)** - 选择要基于流量的源或目的国家/地区或大洲控制流量的地理位置。选择大洲将会选择该大洲内的所有国家/地区。
- **自定义地理位置 (Custom Geolocation)** - 您可以选择您创建的地理位置对象来定义位置。使用地理位置，可以便捷地限制对特定国家/地区的访问，而不需要知道此位置所用的全部潜在 IP 地址。

源端口、目标端口/协议

定义流量中所用协议的端口对象。仅可指定用于 SSL 解密规则的 TCP 协议和端口。

- 要匹配来自 TCP 端口的流量，请配置源端口。
- 要匹配流向 TCP 端口的流量，请配置目标端口/协议。

要同时匹配来自特定 TCP 端口的流量和流向特定 TCP 端口的流量，请配置源端口和目标端口。例如，您可以匹配从端口 TCP/80 流至端口 TCP/8080 的流量。

步骤 10


SSL 解密规则的应用标准

SSL 解密规则的应用标准定义 IP 连接中使用的应用，或定义按类型、类别、标记、风险或业务相关性定义应用的过滤器。默认为任何具有 SSL 协议标记的应用。您无法将 SSL 解密规则与任何未加密应用相匹配。

虽然您可以在规则中指定个别应用，但应用过滤器可简化策略创建和管理。例如，您可以创建一条 SSL 解密规则，用于解密或阻止所有业务相关性较低的高风险应用。如果用户尝试使用这些应用中的任意一个，系统会解密或阻止会话。

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

您可以直接在规则指定应用和过滤器，也可以创建定义这些特征的应用过滤器对象。规格相当，尽管如果要创建复杂规则，使用对象可便于遵守每个条件 50 个项目的系统限制。

要修改应用和过滤器列表，请点击该条件内的  按钮，选择所需的应用程序或应用程序筛选器对象，在弹出的对话框中点击“选择” (Select)，然后点击“保存” (Save)。点击应用、过滤器或对象的 x，可将其从策略中移除。点击另存为过滤器链接，可将尚不是对象的组合条件另存为新应用过滤器对象。

有关应用标准以及如何配置高级过滤器和选择应用的更多信息，请参阅[配置应用过滤器对象](#)。

在 SSL 解密规则中使用应用标准时，请考虑以下提示：

- 系统可以识别使用 StartTLS 进行加密的未加密应用。这包括诸如 SMTPS、POPS、FTPS、TelnetS 和 IMAPS 之类的应用。此外，系统还可以根据 TLS ClientHello 消息中的服务器名称指示或服务器证书使用者可分辨名称值来识别某些加密应用。
- 仅在服务器证书交换后，系统才可识别使用。如果在 SSL 握手期间交换的流量与包含应用条件的 SSL 规则中的所有其他条件相匹配，但是识别未完成，则 SSL 策略允许数据包通过。此行为允许完成握手，以便可以识别应用。在系统完成其识别后，系统将 SSL 规则操作应用于与其应用条件相匹配的剩余会话流量。

步骤 10

SSL 解密规则的 URL 标准

SSL 解密规则的 URL 标准定义了 Web 请求中的 URL 所属的类别。还可以指定要解密、阻止或允许不解密的站点的相对信誉。默认不基于 URL 类别匹配连接。

例如，您可以阻止所有加密的游戏站点或解密所有高风险社交网站。如果用户尝试浏览至任何包含该类别和信誉组合的 URL，会话将被阻止或解密。

要向 SSL 解密规则添加 URL 条件，请执行以下操作：

Procedure

步骤 1 点击 URL 选项卡，将 URL 类别添加到 SSL 解密规则。

步骤 2 搜索并选择要阻止的 URL 类别。

步骤 3 默认情况下，来自您选择的类别的 URL 的流量将由 SSL 解密规则解密，而无论其安全信誉如何。但是，您可以微调规则中的 URL 类别或所有 URL 类别，以便根据信誉从解密中排除某些站点。

- 要微调 URL 中单个类别的信誉，请执行以下操作：

- a. 在选择 URL 类别后，点击该类别。
- b. 取消选中任何信誉 (**Any Reputation**)。
- c. 将绿色滑块向右滑动，选择要从规则中排除的 URL 信誉设置，然后点击**保存 (Save)**。

滑块所覆盖的信誉不受规则影响。例如，如果将绿色滑块滑动到“良性站点”，那么“知名站点”和“良性站点”不会受到所选类别的 SSL 解密规则的影响。被视为具有安全风险、可疑站点和高风险站点的 URL 仍会受到该 URL 类别的规则影响。

- 要微调添加到规则中的所有 URL 类别的信誉，请执行以下操作：

- a. 选择要包含在 SSL 解密规则中的所有类别后，点击**将信誉应用于所选类别 (Apply Reputation to Selected Categories)**。
- b. 取消选中任何信誉 (**Any Reputation**)。
- c. 将绿色滑块向右滑动，选择要从规则中排除的 URL 信誉设置，然后点击**保存 (Save)**。

滑块所覆盖的信誉不受规则影响。例如，如果将绿色滑块滑动到“良性站点”，那么“知名站点”和“良性站点”不会受到全部所选类别的 SSL 解密规则的影响。被视为具有安全风险、可疑站点和高风险站点的 URL 仍会受到全部 URL 类别的规则影响。

步骤 4 点击 **Select**。

步骤 5 点击**保存 (Save)**。

[步骤 10](#)

SSL 解密规则的用户条件

SSL 解密规则的“用户”条件对 IP 连接的用户或用户组进行了定义。只有配置身份策略和相关联的目录服务器，才能在规则中包括用户或用户组条件。

您的身份策略决定是否收集某个特定连接的用户身份。如果建立了身份，则主机的 IP 地址与所识别的用户相关联。因此，源 IP 地址映射到用户的流量将被视为来自该用户。IP 数据包本身不包含用户身份信息，所以此 IP 地址到用户的映射是最接近的近似值。

由于最多可以向规则中添加 50 个用户或组，所以选择组比选择单个用户通常更有意义。例如，您可以创建规则，对从外部网络发往工程组的流量进行解密，并单独创建一个不会对从该组传出的流量

进行解密的规则。然后，要将该规则应用于新工程师，您只需添加将工程师添加到目录服务器的“工程”组即可。

要修改用户列表，请点击该条件内的 + 按钮，并选择所需的用户组，然后点击“选择”(Select)。

步骤 10

SSL 解密规则的高级条件

高级流量匹配标准与根据连接中使用的证书派生的属性有关。您可以配置以下任何或全部选项。

证书属性

如果流量与任何选定属性匹配，则它与相应规则的证书属性选项匹配。您可以配置以下内容：

- **证书状态 (Certificate Status):** 证书无效还是有效。如果您不关心证书状态，请选择任意（默认）。如果满足以下所有条件，证书即视为有效，否则视为无效：
 - 策略信任颁发证书的 CA。
 - 可根据证书的内容对证书的签名进行适当的验证。
 - 颁发者 CA 证书存储在策略的受信任 CA 证书列表中。
 - 策略的受信任 CA 未撤销证书。
 - 当前日期介于证书的有效开始日期和有效期结束日期之间。
- **自签名 (Self-Signed):** 服务器证书是否包含相同的使用者和颁发者可分辨名称。选择以下一个选项：
 - 自签名 - 服务器证书自签名。
 - CA 签名 - 服务器证书由证书颁发机构签名。也就是说，颁发者和使用者不同。
 - 任意 - 不考虑按照匹配标准，证书是否为自签名。

支持的版本

要匹配的 SSL/TLS 版本。该规则适用于仅使用任何选定版本的流量。默认设置是所有版本。可以选择以下版本：SSLv3.0、TLSv1.0、TLSv1.1 和 TLSv1.2。


例如，如果仅希望允许 TLSv1.2 连接，则可创建用于非 TLSv1.2 版本的阻止规则。使用任何未列出版本（例如 SSL v2.0）的流量均由 SSL 解密策略的默认操作处理。

步骤 10

为已知密钥和重签解密配置证书

如果通过重签或使用已知密钥实施解密，则需要确定 SSL 解密规则可以使用的证书。确保所有证书均有效且未过期。

特别是对于已知密钥的解密，需要确保系统拥有要解密连接的各目标服务器的当前证书和密钥。通过解密已知密钥规则，可以使用目标服务器的实际证书和密钥进行解密。因此，必须确保 FDM 管理设备始终拥有当前证书和密钥，否则将无法成功解密。

只要在已知密钥规则中更改目标服务器上的证书或密钥，就要上传新的内部证书和密钥。将上述证书作为内部证书（而不是内部 CA 证书）上传。可以在下列程序中上传证书，也可以转到对象 (Objects) 页面并在此页面中点击  按钮并选择 **FTD > 证书 (Certificate)** 上传。

Procedure

- 步骤 1 在导航窗格中，点击**清单 (Inventory)**。
- 步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
- 步骤 3 点击 **FTD** 选项卡，选择要为其创建 SSL 策略的设备，然后点击右侧管理窗格中的**策略 (Policy)**。
- 步骤 4 点击策略栏中的 **SSL 解密 (SSL Decryption)**。
- 步骤 5 点击 SSL 解密策略栏中的证书按钮 。
- 步骤 6 在 SSL 解密配置对话框中，点击**选择解密重新签名证书 (Select Decrypt Re-Sign Certificate)** 菜单，然后选择或创建内部 CA 证书，以用于利用重签名证书实施解密的规则。您可以使用预定义的 **NGFW-Default-InternalCA** 证书，也可以使用您创建或上传的证书。

如果尚未在客户端浏览器中安装证书，请点击下载按钮  获取副本。有关如何安装证书的信息，请参阅各浏览器文档。另请参阅适用于运行设备的版本的《[适用于 Firepower 设备管理器的 Cisco Firepower 威胁防御配置指南](#)》“安全策略”一章的**下载 CA 证书以进行解密重签名规则**部分。
- 步骤 7 对于使用已知密钥解密的每条规则，上传目标服务器的内部证书和密钥。
- 步骤 8 点击解密已知密钥证书 (**Decrypt Known-Key Certificates**) 下的 。
- 步骤 9 选择内部身份证书，或点击**创建新的内部证书**以便立即上传。
- 步骤 10 点击**保存 (Save)**。
- 步骤 11 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

为解密重签名规则下载 CA 证书

如果决定对流量进行解密，则用户必须拥有加密流程中使用的内部 CA 证书，该证书由使用 TLS/SSL 的应用中被定义为受信任根证书颁发机构所颁发。通常，当生成证书或即使导入证书后，证书不会立即在这些应用中定义为受信任。默认情况下，在大多数网络浏览器中，当用户发送 HTTPS 请求时，他们将看到一条来自客户端应用的警告消息，告知他们网站的安全证书有问题。通常，错误消息表明网站的安全证书并非由受信任证书颁发机构所颁发或网站由未知机构所认证，但该警告可能还表明可能存在中间人攻击。一些其他客户端应用不会向用户显示此警告消息，也不允许用户接受无法识别的证书。

可以通过以下方式为用户提供所需的证书：

通知用户接受根证书

可以通知您组织中的用户，告知其公司的新策略并指示其接受组织提供的根证书作为受信任来源。用户应接受该证书并将其保存在受信任根证书颁发机构存储区，以确保在下次访问该站点时系统不会再次提示。



Note 用户需要接受并信任创建替换证书的 CA 证书。如果仅信任替换服务器证书，用户访问各个不同 HTTPS 站点时将看到警告。

将根证书添加到客户端设备

能够以受信任根证书颁发机构身份将根证书添加到网络上的所有客户端设备。这样，客户端应用将自动接受包含根证书的事务。

可以通过以下方式向用户提供证书：通过邮件发送或将其放在共享站点上，将证书整合到企业工作站映像中并使用应用更新工具将其自动分发给用户。

以下程序介绍了如何下载内部 CA 证书并将其安装在 Windows 客户端上。

操作步骤

该流程因操作系统和浏览器类型的不同而不同。例如，对于 Windows 上运行的 Internet Explorer 和 Chrome 浏览器，可以采用以下流程。（对于 Firefox，请选择工具 (**Tools**) > 选项 (**Options**) > 高级 (**Advanced**) 页面，进行安装。）

系统应显示消息，指示已成功导入。您可能会看到一个中间对话框，警告：如果生成自签名证书而不是从知名第三方证书颁发机构获取证书，则 Windows 无法验证该证书。

此时，可以关闭“证书”和“Internet 选项”对话框。

Procedure

步骤 1 从 Firepower 设备管理器中下载证书。

- a) 在导航窗格中，点击**清单 (Inventory)**。
- b) 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
- c) 点击 **FTD** 选项卡，然后选择存储证书的设备。
- d) 点击右侧“管理” (Management) 窗格中的 **策略 (Policy)**。
- e) 点击策略栏中的 **SSL 解密 (SSL Decryption)**。
- f) 点击 SSL 解密策略栏中的 SSL 解密配置按钮 。
- g) 点击下载按钮 。
- h) 选择一个下载位置，或者更改文件名（但是不要更改扩展名），然后点击保存 (Save)。
- i) 此时可以取消“SSL 解密设置”对话框。

步骤 2 在客户端系统上，在网络浏览器的受信任根证书颁发机构存储区安装证书，或向客户端提供证书，以便用户自行安装。对于不同的浏览器和操作系统，此过程会有所不同。

警告

通过 FDM 管理设备配置的 CA 证书

思科防御协调器可以管理多个设备，但在保存设备配置时保存的其他信息受到限制，这可能会在处理内部 CA 证书时产生一些问题。CDO 不会保存通过 FDM 管理控制台配置的 CA 证书的证书或密钥信息；如果您尝试使用 FDM 管理设备中配置的 CA 证书并将其应用于部署到辅助设备的 SSL 策略，则 CDO 会创建 CA 证书的本地副本，但不会也无法复制密钥信息。因此，CDO 或辅助设备都没有密钥信息，并且无法成功部署 CA 证书。这也意味着 CA 证书的本地副本的下载链接不可用。

我们强烈建议通过 FDM 管理设备为任何其他设备配置单独的 CA 证书，或通过 CDO UI 创建 CA 证书。

规则集

关于规则集

规则集是可与多个 FDM 管理设备共享的访问控制规则的集合。对规则集的规则所做的任何更改都会影响使用此规则集的其他受管设备。FDM 管理设备可以具有设备特定（本地）和共享（规则集）规则。您还可以从 FDM 管理设备中的现有规则创建规则集。



Important “规则集”功能当前可用于运行 FDM 管理设备 [版本 6.5 或更高版本](#) 和更高版本。另请注意，规则集不支持启用 Snort 3 的设备。

以下限制适用：

- 不能将规则集附加到支持 Snort 3 的设备。
- 您无法从已安装 Snort 3 的现有设备创建规则集。
- 不能将自定义 IPS 策略与规则集关联。

复制或移动与规则集关联的规则

可以在规则集中或跨不同规则集复制或移动访问控制规则。此外，您还可以在本地和规则集之间复制或移动规则。有关详细信息，请参阅[复制 FDM 管理访问控制规则](#)和[移动 FDM 管理访问控制规则](#)。

自动检测现有规则集

当您载入设备时，思科防御协调器会自动检测设备上的现有规则集，并尝试将其与设备上的规则进行匹配。成功匹配后，CDO 会自动将规则集附加到新载入的设备。但是，如果设备上的同一组规则有多个规则集匹配项，则不会附加任何规则集，您必须手动分配它们。

为设备配置规则集

按照以下部分来创建和部署规则集：

Procedure

步骤 1 为设备配置规则集。

- a) 创建新的规则集并为其分配规则。
- b) 将对象分配给规则。
- c) 设置规则集的优先级。
- d) 如果需要，更改规则的顺序。

步骤 2 为设备配置规则集。

- a) 将多个设备附加到规则集。
 - b) 查看规则集并将其部署到设备。
-

创建或编辑规则集


您可以创建规则集并向其添加新的访问控制规则。

按照以下程序为多个 FDM 管理设备创建规则集：

Procedure

步骤 1 在导航窗格中，点击策略 (Policies) > FTD 规则集 (FTD Rulesets)。

步骤 2 点击加号  按钮创建新的规则集。

Note 要编辑现有规则集，请选择该规则集，然后点击编辑图标 .

步骤 3 为该规则集输入一个名称，然后点击创建 (Create)。

步骤 4 创建访问控制规则以将其添加到规则集中。有关说明，请参阅[配置 FDM 访问控制策略](#)。

Note 规则集中的访问控制规则不支持用户条件。

步骤 5 在窗口的右上角，选择规则集的优先级 。如果设备未连接到规则集，则可以设置优先级。该选择会影响此规则集中包含的所有规则及其在设备上的处理方式：

- **排名靠前 (Top)** - 在设备上的所有其他规则之前处理规则集。规则排列在规则列表的顶部，并首先进行处理。任何其他规则集都不能优先于此策略中的规则。每个设备只能有一个排名靠前的规则集。
- **排名靠后 (Bottom)** - 规则集在设备上的所有其他规则之后处理。除策略的默认操作外，没有其他规则集可以继承此策略中的规则。每个设备只能有一个排名靠后规则集。默认情况下，优先级会被设为排名靠后 (Bottom)。

本地规则 (Local Rules) 显示设备的所有设备特定规则。

Note 当规则集连接到设备时，无法更改优先级。您必须断开设备并更改优先级。

步骤 6 点击**保存 (Save)**。您可以根据需要创建任意数量的规则。

步骤 7 (可选) 对于您创建的任何规则，您可以选择它并在“添加注释”(Add Comments) 字段中添加注释。要了解有关规则注释的详细信息，请参阅[向策略和规则集中的规则添加注释](#)。

Note


- 即使将设备连接到规则集中，也可以更改规则集中的规则顺序。按照以下程序来更改规则集的优先级：
 - a. 在导航窗格中，点击**策略 (Policies) > 规则集 (Rulesets)**，然后选择要删除的规则集。
 - b. 选择要移动的规则。
 - c. 将光标悬停在规则行内，然后使用**上移 ↑** 或**下移 ↓** 箭头将规则移至所需的顺序。
- CDO 允许您[覆盖与规则集的规则关联的对象](#)。在将新对象添加到规则时，只有在将设备附加到规则集并保存更改后，才能覆盖该对象。

将规则集部署到多个 FDM 管理的设备或模板

您必须将规则集附加到要实施的设备或模板。在查看更改后，您可以在设备上部署配置。在将模板应用于新的 FDM 管理 设备时，模板中包含的规则集将被推送到设备。

有关详细信息，请参阅[使用 FDM 管理 模板的规则集](#)。

在开始之前，请考虑以下信息：

- 您只能将规则集附加到已载入 思科防御协调器 的 FDM 管理 设备。
- 设备只能有一个底部或顶部规则集。
- 从规则集中连接或删除设备后，更改会在 CDO 中暂存但不会部署，并且设备将变为**未同步 (Not Synced)**，表示未与 CDO 同步。点击屏幕右上角的  图标，将更改部署到设备。
- 在连接设备后，与规则集关联的新规则不会覆盖与设备关联的现有规则。

您可以通过两种方式将规则集与设备关联：


- 从“规则集”(Ruleset) 页面将设备添加到规则集。
- 从“设备策略”(Device Policy) 页面向设备添加规则集。

从“规则集”(Ruleset) 页面将设备添加到规则集

Procedure

步骤 1 在导航窗格中，点击**策略 (Policies) > FTD 规则集 (FTD Rulesets)**。

步骤 2 选择要分配给 FTD 设备的规则集，然后在操作 (Actions) 窗格中点击编辑 (Edit)。

步骤 3 在右上角，点击规则集 (Ruleset for) 旁边显示的设备 (Device) 按钮 。

步骤 4 从符合条件的 FTD 设备列表中选择。

步骤 5 当系统确定规则集中的规则与设备特定的规则之间存在重复名称时，在齿轮图标中选择系统要执行的以下操作之一：

- **规则冲突时失败 (Fail on conflicting rules)** (默认选项)：CDO 不会将规则集添加到设备。您需要手动重命名重复的规则，然后添加规则集。
- **重命名冲突规则 (Rename conflicting rules)**：CDO 重命名设备上存在的冲突规则 (本地规则)。

步骤 6 点击保存 (Save)。将规则集附加到设备 (Attached Ruleset to Devices) 向导将关闭。

步骤 7 点击右上角的保存 (Save) 以保存对规则集所做的更改。保存规则集会将更改暂存到 CDO。

Note 每次修改规则集时，都必须点击保存 (Save)。通过执行此操作，所有更改都将被暂存到 CDO。您必须手动部署更改。

步骤 8 点击 Confirm。保存规则集会将更改暂存到 CDO。

步骤 9 [预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。如果您[放弃更改](#)设备上的暂存规则集更改，请参阅[放弃暂存规则集更改的影响](#)。

从“设备策略” (Device Policy) 页面向设备添加规则集


Procedure

步骤 1 在导航窗格中，点击清单 (Inventory)。

步骤 2 点击设备 (Devices) 选项卡以查找设备，或点击模板 (Templates) 选项卡以查找型号设备。

步骤 3 点击 FTD 选项卡，然后从列表中选择所需的设备。

步骤 4 在右侧的管理 (Management) 窗格中，点击策略 (Policy)。

步骤 5 点击窗口右上角出现的  按钮。

步骤 6 选择所需的规则集。

步骤 7 当系统确定规则集中的规则与设备特定的规则之间存在重复名称时，在齿轮图标中选择系统要执行的以下操作之一：

- **规则冲突时失败 (Fail on conflicting rules)** (默认选项)：CDO 不会将规则集添加到设备。您需要手动重命名重复的规则，然后添加规则集。
- **重命名冲突规则 (Rename conflicting rules)**：CDO 重命名设备上存在的冲突规则 (本地规则)。

Note 如果所选设备上没有冲突规则，CDO 会将规则集附加到设备，而不进行任何更改。

步骤 8 点击附加规则集 (Attach Ruleset)。规则集会根据规则集的优先级被添加到设备。

步骤 9 预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。如果您[放弃更改](#)设备上的暂存规则集更改，请参阅[放弃暂存规则集更改的影响](#)。

相关信息：

- [规则集](#)
- [使用 FDM 管理 模板的规则集](#)
- [从所选规则集中分离 FTD 设备](#)
- [删除规则和规则集](#)
- [带外更改对规则集的影响](#)
- [查看规则和规则集](#)
- [创建规则集后更改日志条目](#)
- [从现有设备规则创建规则集](#)

使用 FDM 管理 模板的规则集

思科防御协调器 允许您将规则集分配给 FDM 管理 模板。

- 从具有规则集的 FDM 管理设备创建模板时，CDO 会自动将模板添加到源设备上存在的规则集中。您可以从规则集中管理模板。
- 将包含规则集的模板应用于目标 FDM 管理设备时，CDO 会自动将目标设备添加到规则集，从而从规则集中管理目标设备。
- 将包含规则集的模板应用于已具有不同规则集的目标 FDM 管理设备时，CDO 会从目标设备中删除现有规则集，并添加与该模板关联的新规则集。

有关详细信息，请参阅[将规则集部署到多个 FDM 管理的设备或模板](#)。

相关信息：

- [规则集](#)
- [为设备配置规则集](#)
- [从现有设备规则创建规则集](#)
- [带外更改对规则集的影响](#)
- [查看规则和规则集](#)
- [创建规则集后更改日志条目](#)
- [从所选规则集中分离 FTD 设备](#)
- [删除规则和规则集](#)

从现有设备规则创建规则集

您可以通过选择 FDM 管理设备中的现有规则来创建规则集。

按照以下程序从现有设备规则创建规则集：

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后从列表中选择所需的设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。系统将显示设备的现有规则。

步骤 5 根据您的要求执行以下操作：

- a) 要创建**排名靠前**的规则，请从顶部的第一个规则开始选择连续规则。
- b) 要创建**排名靠后**规则的，请选择包含底部最后一条规则的连续规则。

步骤 6 在右侧的**操作 (Actions)** 窗格中，点击**创建规则集 (Create Ruleset)**。

Note 您的选择必须包含第一个或最后一个规则，**创建规则集 (Create Ruleset)** 链接才能点击。

步骤 7 在**规则集名称 (Ruleset Name)** 字段中指定名称，然后点击**创建 (Create)**。在设备中创建相应的规则集。

您可以使用设备中的其余规则继续创建规则集。

带外更改对规则集的影响

当您使用 FDM 管理设备添加新规则或对现有规则进行更改，并且您已在思科防御协调器中为 FDM 管理设备启用冲突检测时，CDO 会检测到带外更改，并且设备的配置状态显示为**检测到冲突 (Conflict Detected)**。[解决配置冲突](#)。

如果您接受设备更改，CDO 会使用在设备上进行的新更改覆盖最新的配置。将发生以下变化：

- 受更改影响的规则集会失去与设备的关系。
- 与这些规则集关联的规则将转换为本地规则。

如果您拒绝设备更改，CDO 会拒绝新的更改，并将设备上的配置替换为 CDO 中的上次同步配置。

相关信息：

- [规则集](#)
- [为设备配置规则集](#)
- [从现有设备规则创建规则集](#)
- [放弃暂存规则集更改的影响](#)

- [查看规则和规则集](#)
- [创建规则集后更改日志条目](#)
- [从所选规则集中分离 FTD 设备](#)
- [删除规则和规则集](#)

放弃暂存规则集更改的影响

在向规则集添加新规则或使用 CDO 更改与规则集关联的现有规则时，它会将您所做的更改保存到其自己的配置文件副本中。在“部署”到设备之前，这些更改将被视为已在 CDO 上“待处理”。

如果[放弃更改](#)设备上的待定规则集更改，则 CDO 会用存储在设备上的配置完全覆盖设备配置的本地副本。

规则集和关联设备上发生以下更改：

- 受更改影响的规则集会失去与设备的关系。
- 与这些规则集关联的规则将转换为本地规则。
- CDO 会丢弃新的暂存更改并保留设备上的配置。

相关信息：

- [规则集](#)
- [为设备配置规则集](#)
- [从现有设备规则创建规则集](#)
- [带外更改对规则集的影响](#)
- [查看规则和规则集](#)
- [创建规则集后更改日志条目](#)
- [从所选规则集中分离 FTD 设备](#)
- [删除规则和规则集](#)

查看规则和规则集

从设备策略页面查看规则

FDM 管理设备策略页面会显示单个（本地）和共享规则（与规则集关联）。

使用以下程序从策略页面查看 FDM 管理设备规则集：

Procedure

步骤 1 在导航窗格中，点击清单 (Inventory)。

步骤 2 点击设备 (**Devices**) 选项卡以查找设备，或点击模板 (**Templates**) 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择所需的设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。根据所做的配置，您会看到以下规则：

- **排名靠前的规则 (Top Rules)**：显示将在设备上的所有其他规则之前处理的强制共享规则。
- **本地规则 (Local Rules)**：显示将在设备上的强制性规则之后处理的设备特定规则。
- **排名靠后 (Bottom)**：显示将在设备上的所有其他规则之后处理的默认共享规则。

Note 您可以通过转至相应的规则集页面来编辑规则集。

- 在规则集标题的右上角，点击**转到规则集** 。
- 对规则进行所需的更改，然后点击**保存 (Save)**。新的更改会在与规则集关联的所有设备上更新。

查看规则集

规则集 (Rulesets) 页面会显示租户中可用的所有规则集。它还会提供有关与规则集关联的设备的信
息。

使用以下程序可从“规则集” (Rulesets) 页面查看所有规则集：

Procedure

步骤 1 在导航窗格中，点击**策略 (Policies) > 规则集 (Rulesets)**。系统将显示租户中可用的规则。

步骤 2 点击规则集可查看其详细信息。**设备 (Devices)** 列将显示连接到每个规则集的 FTD 设备的数量。

步骤 3 在**管理 (Management)** 窗格中，点击**工作流程 (Workflows)**。此页面将显示您在设备上执行的所有操作。您可以点击**图表 (Diagram)** 以查看工作流程的图示。

搜索规则集

您可以使用**按设备过滤 (Filter by Device)** 过滤器来选择设备，以便查看分配给它们的规则集。

Procedure

步骤 1 在导航窗格中，点击**策略 (Policies) > 规则集 (Rulesets)**。

步骤 2 点击过滤器图标，然后点击**按设备过滤 (Filter by Device)**。

步骤 3 从列表选择一个或多个设备，然后点击**确定 (OK)**。

您可以根据所选的设备来查看规则集。

查看与规则集关联的作业

当您 will 将规则集应用于 FTD 设备或从 FTD 设备中删除它们时，**作业 (Jobs)** 页面会记录操作。它还会确定操作是成功还是失败。

Procedure

步骤 1 在导航窗格中，点击**策略 (Policies) > 规则集 (Rulesets)**。

步骤 2 点击规则集可查看其详细信息。

步骤 3 在**管理 (Management)** 窗格中，点击**作业 (Jobs)**。此页面将显示您在规则集上执行的操作。

创建规则集后更改日志条目

当 CDO 检测到规则集发生更改时，它会为在规则集上执行的每个操作创建一个更改日志条目。

如果点击更改日志条目行中的蓝色**差异 (Diff)** 链接，则会在运行配置文件的上下文中并排对比显示更改。

在下面的示例中，更改日志将显示新规则集的条目，其中三个规则已添加到规则集中。它还会显示有关设置规则集的优先级以及连接到规则集的 FTD 设备的信息。

Feb 25, 2020		
8:43:09 PM	Successfully saved	
8:43:03 PM	Ruleset Modified Ruleset_3	
	DEPLOYED VERSION	PENDING VERSION
	Ruleset	
	#1 Ruleset_3	
	Attached Devices	
	-	"BGL_FTD"
8:42:56 PM	Ruleset Modified Ruleset_3	
	DEPLOYED VERSION	PENDING VERSION
	Ruleset	
	#1 Ruleset_3	
	Apply Position	
	DEFAULT	MANDATORY
8:42:43 PM	Access Rules Added new_rule_3	
8:42:35 PM	Access Rules Added new_rule_2	
8:42:26 PM	Access Rules Added new_rule_1	
Feb 25, 2020 8:42:16 PM	Ruleset_3	Created ruleset Ruleset_3

图中的数字	说明
1	新规则集 “Ruleset_3” 创建于 2020 年 2 月 25 日上午 11:03:18。
2	在规则集中创建了新的访问规则 “new_rule_1”、“new_rule_3” 和 “new_rule_3”。
3	规则集的优先级被设置为 “强制”。
4	规则集被附加到 “BGL_FTD” 设备。
5	规则集更改已保存。

从所选规则集中分离 FTD 设备

使用以下程序从规则集分离设备：

Procedure

- 步骤 1 在导航窗格中，点击策略 (Policies) > 规则集 (Rulesets)。
- 步骤 2 选择您要编辑的规则集，然后点击操作 (Actions) 窗格中的编辑 (Edit) 链接。
- 步骤 3 在右上角，点击规则集 (Ruleset for) 旁边显示的设备 (Device) 按钮。
- 步骤 4 取消选中当前连接到规则集的设备，或点击清除 (Clear) 以立即删除所有设备。
- 步骤 5 点击保存 (Save)。
- 步骤 6 点击右上角窗口中的保存 (Save) 以保存规则集。保存策略会将更改暂存到 CDO。
- 步骤 7 [预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

相关信息：

- [规则集](#)
- [为设备配置规则集](#)
- [从现有设备规则创建规则集](#)
- [带外更改对规则集的影响](#)
- [查看规则和规则集](#)
- [创建规则集后更改日志条目](#)
- [删除规则和规则集](#)

删除规则和规则集

从规则集中删除规则

可以删除规则集中不再需要的规则。

使用以下程序删除规则：

Procedure

步骤 1 在导航窗格中，点击策略 (Policies) > 规则集 (Rulesets)，然后选择规则集。

步骤 2 点击操作 (Actions) 窗格中的编辑 (Edit)。

步骤 3 选择要删除的规则，然后点击操作 (Actions) 下的删除 (Remove)。

步骤 4 点击确定，确认删除。

步骤 5 点击右上角的保存 (Save) 以保存对规则集所做的更改。保存规则集会将更改暂存到 CDO。

步骤 6 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

删除规则集

只有在分离与其关联的所有设备后，才能删除规则集。请参阅从规则集中分离 FTD 设备。[删除规则和规则集, on page 171](#)

使用以下程序删除规则集：

Procedure

步骤 1 在导航窗格中，点击策略 > 规则集，然后选择要删除的规则集。

步骤 2 点击规则集行内的删除 (Remove)。

步骤 3 点击确认以永久删除规则集。

步骤 4 立即[预览和部署所有设备的配置更改](#)您的更改，或等待并一次部署多个更改。

- [规则集](#)
- [为设备配置规则集](#)
- [从所选规则集中分离 FTD 设备](#)

从所选 FDM 的设备中删除规则集

有两种方法可从所选 FTD 设备中删除规则集，但它们的行为略有不同。

- [从所选 FDM 管理设备删除规则集](#)：此功能从所选 FTD 设备删除规则集及其关联的共享规则。

- **取消规则集与所选 FDM 管理设备的关联**：此功能不会删除共享规则。相反，它会将共享规则转换为本地规则。

从所选 FDM 管理设备删除规则集

您可以从所选 FDM 管理设备中删除规则集及其关联的共享规则。规则集也可以从规则集页面[从所选规则集中分离 FTD 设备](#)。


Procedure

- 步骤 1** 在导航窗格中，点击**清单 (Inventory)**。
 - 步骤 2** 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
 - 步骤 3** 点击 **FTD** 选项卡，然后从列表中选择所需的设备。
 - 步骤 4** 点击规则集右上角显示的删除图标。
 - 步骤 5** 点击 **Confirm**。
 - 步骤 6** [预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。
-

取消规则集与所选 FDM 管理设备的关联

如果要将新的设备特定规则添加到 FDM 管理设备中的规则集，则需要将该规则集与 FDM 管理设备取消关联，这会将其关联的共享规则转换为本地规则。然后，您可以将所需的规则添加到本地规则。

Procedure

- 步骤 1** 在导航窗格中，点击**清单 (Inventory)**。
 - 步骤 2** 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
 - 步骤 3** 点击 **FTD** 选项卡，然后从列表中选择所需的设备。
 - 步骤 4** 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。
 - 步骤 5** 点击规则集右上角显示的  图标。
 - 步骤 6** 点击 **Confirm**。
 - 步骤 7** [预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。
-

向策略和规则集中的规则添加注释

您可以向 FDM 管理设备策略中的规则和规则集中的规则添加注释，以记录规则的某些特征。规则注释仅在思科防御协调器上可见；它们永远不会写入 FDM 管理设备，也不会出现在 FDM 中。

在 CDO 中创建并保存注释后，注释会被添加到规则中。由于规则注释只是 CDO 的一项功能，因此创建、更改或删除规则注释并不会将 CDO 中设备的配置状态更改为“未同步” (Not Synced)。您无需将更改从 CDO 写入 FDM 管理设备即可保存规则注释。

可以在设备的策略页面上查看和编辑与 FDM 管理 设备策略中的规则关联的注释。可以在规则集页面上查看和编辑与 FDM 管理 设备规则集中的规则关联的注释。如果规则集被用于策略中，则与规则集中的任何规则关联的任何注释都显示在策略的注释区域中。注释为只读。

如果您在策略、规则集或更改日志中搜索字符串，CDO 将搜索与该字符串的规则关联的注释以及规则的其他属性和值。

在添加或编辑规则的注释时，该操作会记录在更改日志中。由于规则注释只在 CDO 中记录和维护，因此它们会在更改日志中被标记（仅限 CDO 更改）。

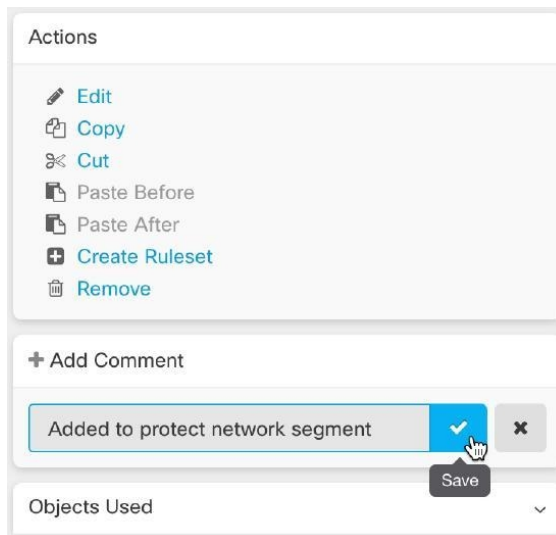


Caution 如果 FDM 管理 设备配置发生带外更改，并且 CDO 将该配置读入其数据库，则与任何规则关联的注释都将被清除。

向规则添加注释

Procedure

- 步骤 1 打开包含您要注释的规则的策略或规则集。
- 步骤 2 选择规则。
- 步骤 3 在规则的“添加注释” (Add Comment) 区域中点击添加注释 (**Add Comment**)。
- 步骤 4 在文本框中添加注释。
- 步骤 5 点击保存 (**Save**)。




编辑政策和规则集中有关规则的注释

编辑策略中的规则注释

使用此程序可编辑 FDM 管理 设备策略中的规则注释。


Procedure

-
- 步骤 1 从 CDO 菜单栏中，选择策略 (Policies) > FTD/Meraki/AWS 策略 (FTD/Meraki/AWS Policies)。
 - 步骤 2 选择包含要添加注释的本地规则的 FDM 管理 设备策略。您无法为策略内的规则集中的规则添加注释。
 - 步骤 3 在“注释” (Comment) 窗格中，点击编辑图标 。
 - 步骤 4 编辑注释并点击“保存” (Save)。您会马上在“注释” (Comment) 区域中看到注释更改。
-

编辑规则集中规则的注释

要查看规则集中规则的注释更改（反映在策略页面上），则必须按特定顺序对注释和规则进行更改。

Procedure

-
- 步骤 1 从 CDO 导航面板中，选择策略 (Policies) > FTD 规则集 (FTD Rulesets)。
 - 步骤 2 选择要为其添加注释的规则。
 - 步骤 3 在“操作” (Actions) 窗格中，点击编辑 (Edit)。
 - 步骤 4 选择规则。
 - 步骤 5 在“注释” (Comment) 窗格中，点击编辑图标 。
 - 步骤 6 编辑注释并点击“保存” (Save)。您会马上在规则集页面的“注释” (Comment) 区域中看到注释更改。
 - 步骤 7 选择要更改的规则，然后在操作窗格中点击编辑 (Edit)。
 - 步骤 8 编辑规则，然后点击蓝色复选按钮以保存更改。
 - 步骤 9 在规则集页面的顶部，点击保存 (Save) 以保存规则集。规则集中该规则的新注释现在将显示在策略页面上。
 - 步骤 10 要查看策略页面中的注释更改，请执行以下操作：
 - a) 从 CDO 菜单栏中，选择策略 (Policies) > FTD/Meraki/AWS 策略 (FTD/Meraki/AWS Policies)。
 - b) 选择包含您刚刚编辑的规则集的 FDM 管理设备策略。
 - c) 选择包含您刚刚编辑的注释的规则。您应该会在“注释” (Comment) 窗格中看到新的注释。
-

网络地址转换

IP 网络中的每台计算机和设备都分配了标识主机的唯一 IP 地址。因为缺乏公用 IPv4 地址，所以这些 IP 地址中的大多数都是专用地址，在专用公司网络以外的任何地方都不可路由。RFC 1918 定义可以在内部使用但不应通告的专用 IP 地址：

- 10.0.0.0 到 10.255.255.255
- 172.16.0.0 至 172.31.255.255
- 192.168.0.0 到 192.168.255.255

网络地址转换 (NAT) 的主要功能之一是使专用 IP 网络可以连接到互联网。NAT 用公用 IP 地址替换专用 IP 地址，将内部专用网络中的专用地址转换为可在公用互联网上使用的合法可路由地址。NAT 以此方式保存公用地址，因为它可配置为至少仅将整个网络的一个公用地址向外界通告。

NAT 的其他功能包括：

- 安全-隐藏内部 IP 地址可以阻止直接攻击。
- IP 路由解决方案-使用 NAT 时不会出现重叠 IP 地址。
- 灵活性-可以更改内部 IP 寻址方案，而不影响外部的可用公用地址；例如，对于可以访问互联网的服务器，可以维护供互联网使用的固定 IP 地址，但在内部，可以更改服务器地址。
- 在 IPv4 和 IPv6 之间转换（仅路由模式）- 如果想将 IPv6 网络连接到 IPv4 网络，可以利用 NAT 在两种类型的地址之间转换。

您可以使用 Cisco Defense Orchestrator 为许多不同的使用案例创建 NAT 规则。使用 NAT 规则向导或以下主题创建不同的 NAT 规则：

NAT 规则的处理顺序

网络对象 NAT 和两次 NAT 规则存储在划分为三部分的单个表中。首先应用第一部分规则，其次是第二部分，最后是第三部分，直到找到匹配项为止。例如，如果在第一部分找到匹配项，则不评估第二部分和第三部分。下表显示每个部分的规则顺序。

Table 5: NAT 规则表

表部分	规则类型	部分中的规则顺序
第 1 部分	两次 NAT (ASA) 手动 NAT (FTD)	系统按照在配置中出现的顺序应用第一个匹配的规则。因为会应用第一个匹配规则，所以必须确保具体规则位于更加通用的规则前面，否则无法按预期应用特定规则。默认情况下，两次 NAT 规则会添加到第 1 部分。

表部分	规则类型	部分中的规则顺序
第 2 部分	网络对象 NAT (ASA) 自动 NAT (FTD)	<p>如果在第 1 部分未找到匹配项，则会按照以下顺序应用第 2 部分的规则：</p> <ol style="list-style-type: none"> 1. 静态规则。 2. 动态规则。 <p>在每个规则类型中，遵循以下排序准则：</p> <ol style="list-style-type: none"> 1. 实际 IP 地址数量“æ”从最小到最大。例如，带一个地址的对象将在带 10 个地址的对象之前进行评估。 2. 如果数量相同，则按从最低到最高的顺序使用 IP 地址编号。例如，10.1.1.0 在 11.1.1.0 之前进行评估。 3. 如果使用同一 IP 地址，则按字母数字顺序使用网络对象名称。例如，先评估对象“Arlington”，然后再评估对象“Detroit”。
第 3 部分	两次 NAT (ASA) 手动 NAT (FTD)	<p>如果仍未找到匹配项，则按照在配置中出现的顺序，应用第三部分规则的第一个匹配项。此部分应当包含最通用的规则。还必须确保此部分的特定规则位于通用规则之前，否则会应用通用规则。</p>

例如，对于第二部分规则，在网络对象中定义以下 IP 地址：

- 192.168.1.0/24（静态）
- 192.168.1.0/24（动态）
- 10.1.1.0/24（静态）
- 192.168.1.1/32（静态）
- 172.16.1.0/24（动态）（对象 Drtroit）
- 172.16.1.0/24（动态）（对象 Arlington）

结果排序可能是：

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

- 172.16.1.0/24 (动态) (对象 Dtrroit)
- 192.168.1.0/24 (动态)

网络地址转换向导

网络地址转换 (NAT) 向导可帮助您在设备上为以下类型的访问创建 NAT 规则:

- 为内部用户启用互联网访问。您可以使用此 NAT 规则允许内部网络上的用户访问互联网。
- 向互联网公开内部服务器。您可以使用此 NAT 规则允许网络外部的人员访问内部 Web 或邮件服务器。

“为内部用户启用互联网访问”的前提条件

在创建 NAT 规则之前, 请收集以下信息:

- 最接近用户的接口; 这通常称为“内部”接口。
- 离您的互联网连接最近的接口; 这通常称为“外部”接口。
- 如果您只想允许特定用户访问互联网, 则需要这些用户的子网地址。

“将内部服务器暴露给互联网”的必备条件

在创建 NAT 规则之前, 请收集以下信息:

- 最接近用户的接口; 这通常称为“内部”接口。
- 离您的互联网连接最近的接口; 这通常称为“外部”接口。
- 要转换为面向互联网的 IP 地址的网络内服务器的 IP 地址。
- 您希望服务器使用的公共 IP 地址。

后续操作

请参阅[使用 NAT 向导创建 NAT 规则, on page 177](#)。

使用 NAT 向导创建 NAT 规则

Before you begin

有关使用 NAT 向导创建 NAT 规则所需的必备条件, 请参阅。[网络地址转换向导, on page 177](#)

Procedure

步骤 1 在 CDO 导航栏中, 点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备, 或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 使用[过滤器](#)和[搜索](#)字段查找要为其创建 NAT 规则的设备。

步骤 5 在详细信息面板的[管理 \(Management\)](#) 区域中，点击 **NAT**  **NAT**。

步骤 6 点击 > NAT 向导。 

步骤 7 回答 NAT 向导问题并按照屏幕上的说明进行操作。

- NAT 向导创建规则。[网络对象](#)从下拉菜单中选择现有对象，或使用创建按钮创建新对象。

 Create...

- 在保存 NAT 规则之前，需要将所有 IP 地址定义为网络对象。

步骤 8 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

NAT 常见使用案例

两次 NAT 和手动 NAT

以下是使用“网络对象 NAT”（也称为“自动 NAT”）可以实现的一些常见任务：

- [启用内部网络上的服务器以使用公共 IP 地址访问互联网，第 178 页](#)
- [使内部网络上的用户能够使用外部接口的公共 IP 地址访问互联网，第 179 页](#)
- [使内部网络上的服务器在公共 IP 地址的特定端口上可用，第 181 页](#)
- [将专用 IP 地址范围转换为公用 IP 地址范围，第 184 页](#)

网络对象 NAT 和自动 NAT

以下是使用“两次 NAT”（也称为“手动 NAT”）可以实现的常见任务：

- [防止在遍历外部接口时转换某个范围的 IP 地址，第 185 页](#)

启用内部网络上的服务器以使用公共 IP 地址访问互联网

使用案例

当您的服务器具有需要从互联网访问的私有 IP 地址，并且您有足够的公共 IP 地址将一个公共 IP 地址转换为私有 IP 地址时，请使用此 NAT 策略。如果您的公共 IP 地址数量有限，请参阅[使内部网络上的服务器可供公共 IP 地址的特定端口上的用户使用（该解决方案可能更合适）](#)。[使内部网络上的服务器在公共 IP 地址的特定端口上可用](#), on page 181


战略

您的服务器具有静态专用 IP 地址，网络外部的用户必须能够访问您的服务器。创建将静态私有 IP 地址转换为静态公共 IP 地址的网络对象 NAT 规则。之后，创建允许来自该公共 IP 地址的流量到达专用 IP 地址的访问策略。最后，将这些更改部署到您的设备。

Before you begin

在开始之前，请创建两个网络对象。将一个对象命名为 `servername_inside`，将另一个对象命名为 `_outside`。`servername_inside` 网络对象应包含服务器的专用 IP 地址。`servername_outside` 网络对象应包含服务器的公共 IP 地址。有关说明，请参阅创建网络对象。[网络对象](#)

Procedure

- 步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。
- 步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。
- 步骤 3 点击设备类型选项卡。
- 步骤 4 选择要为其创建 NAT 规则的设备。
- 步骤 5 点击右侧**管理 (Management)** 窗格中的 **NAT**。
- 步骤 6 点击 > 网络对象 NAT。 
- 步骤 7 在第 1 部分中，键入选择**静态 (Static)**。点击**继续 (Continue)**。
- 步骤 8 在部分 2 中，为源接口选择内部，为目标接口选择外部。点击**继续 (Continue)**。
- 步骤 9 在第 3 部分“数据包”中，执行以下操作：
 - a. 展开 Original Address 菜单，点击 Choose，然后选择 `servername_inside` 对象。
 - b. 展开 Translated Address 菜单，点击 Choose，然后选择 `servername_outside` 对象。
- 步骤 10 跳过第 4 节“高级”。
- 步骤 11 对于 FDM 管理的设备，在部分 5 (Name) 中，为 NAT 规则指定名称。
- 步骤 12 点击**保存 (Save)**。
- 步骤 13 对于，部署网络策略规则，或者对于设备，部署访问控制策略规则，以允许流量从 `servername_inside` 流向 `servername_outside`。ASA/FDM 管理
- 步骤 14 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

使内部网络上的用户能够使用外部接口的公共 IP 地址访问互联网

使用案例


通过共享外部接口的公共地址，允许专用网络中的用户和计算机连接到互联网。

战略

创建端口地址转换 (PAT) 规则，允许专用网络上的所有用户共享设备的外部接口公共 IP 地址。

将私有地址映射到公有地址和端口号后，设备会记录该映射。当收到发往该公共 IP 地址和端口的传入流量时，设备会将其发送回请求它的私有 IP 地址。

Procedure

-
- 步骤 1** 在 CDO 导航栏中，点击**清单 (Inventory)**。
- 步骤 2** 点击**设备** 选项卡以查找设备，或点击**模板** 选项卡以查找型号设备。
- 步骤 3** 点击设备类型选项卡。
- 步骤 4** 选择要为其创建 NAT 规则的设备。
- 步骤 5** 点击右侧**管理 (Management)** 窗格中的 **NAT**。
- 步骤 6** 点击网络对象 NAT。 
- 步骤 7** 在第 1 部分中，键入选择**动态 (Dynamic)**。点击**继续 (Continue)**。
- 步骤 8** 在部分 2 中，为源接口选择 **any**，为目标接口选择 **outside**。点击**继续 (Continue)**。
- 步骤 9** 在第 3 部分“数据包”中，执行以下操作：
- 展开 **Original Address** 菜单，点击 **Choose** 并根据您的网络配置选择 **any-ipv4** 或 **any-ipv6** 对象。
 - 展开 **Translated Address** 菜单，然后从可用列表中选择 **interface**。接口指示使用外部接口的公共地址。
- 步骤 10** 对于 Firepower 威胁防御 (FTD)，在部分 5 中，输入 NAT 规则的名称。
- 步骤 11** 点击**保存 (Save)**。
- 步骤 12** 立即 [预览和部署所有设备的配置更改](#) 您所做的更改，或等待并一次部署多个更改。

的已保存配置文件中的条目 **ASA**

以下是由于此程序而创建并显示在 的已保存配置文件中的条目。ASA



Note 这不适用于设备。FDM 管理

通过此程序创建的对象：

```
object network any_network
subnet 0.0.0.0 0.0.0.0
```

此程序创建的 **NAT** 规则：

```
object network any_network
nat (any,outside) dynamic interface
```

使内部网络上的服务器在公共 IP 地址的特定端口上可用

使用案例


如果您只有一个或非常有限的公共 IP 地址，则可以创建一个网络对象 NAT 规则，将绑定到静态 IP 地址和端口的入站流量转换为内部地址。我们提供了适用于特定情况的程序，但您可以将其用作其他受支持应用的模型。

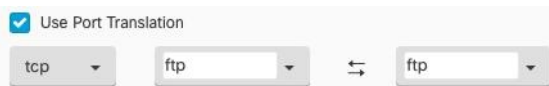
前提条件

在开始之前，请创建三个单独的网络对象，分别用于 FTP、HTTP 和 SMTP 服务器。出于以下程序的考虑，我们将这些对象称为 ftp-server-object、http-server-object 和 smtp-server-object。有关说明，请参阅创建网络对象创建网络对象。[创建或编辑 Firepower 网络对象或网络组](#)

到 FTP 服务器的 NAT 传入 FTP 流量

Procedure

- 步骤 1 在 CDO 导航栏中，点击清单 (**Inventory**)。
- 步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。
- 步骤 3 点击设备类型选项卡。
- 步骤 4 选择要为其创建 NAT 规则的设备。
- 步骤 5 点击右侧**管理 (Management)** 窗格中的 **NAT**。
- 步骤 6 点击 > 网络对象 NAT。 
- 步骤 7 在第 1 部分中，键入选择**静态 (Static)**。点击**继续 (Continue)**。
- 步骤 8 在部分 2 中（**接口**），为源接口选择**内部**，为目标接口选择**外部**。点击**继续 (Continue)**。
- 步骤 9 在第 3 部分**数据包**中，执行以下操作：
 - 展开 **Original Address** 菜单，点击 **Choose**，然后选择 **ftp-server-object**。
 - 展开 **Translated Address** 菜单，点击 **Choose**，然后选择 **Interface**。
 - 选中使用**端口转换 (Use Port Translation)**。
 - 选择 **tcp**、**ftp**、**ftp**。
- 步骤 10 跳过第 4 节**高级**。
- 步骤 11 对于 Firepower 威胁防御 (FTD)，请在第 5 部分**名称**中为 NAT 规则命名。
- 步骤 12 点击**保存 (Save)**。新规则在 NAT 表的**NAT 规则的处理顺序**中创建。



步骤 13 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。


流向 HTTP 服务器的 NAT 传入 HTTP 流量

如果您只有一个或非常有限的公共 IP 地址，则可以创建一个网络对象 NAT 规则，将绑定到静态 IP 地址和端口的入站流量转换为内部地址。我们提供了适用于特定情况的程序，但您可以将其用作其他受支持应用的模型。

Before you begin

在开始之前，为 http 服务器创建网络对象。在本程序中，我们将调用对象 **http-object**。有关说明，请参阅[创建网络对象](#)。

Procedure

- 步骤 1** 在 CDO 导航栏中，点击**清单 (Inventory)**。
- 步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。
- 步骤 3** 点击设备类型选项卡。
- 步骤 4** 选择要为其创建 NAT 规则的设备。
- 步骤 5** 点击右侧**管理 (Management)** 窗格中的 **NAT**。
- 步骤 6** 点击  > **网络对象 NAT**。
- 步骤 7** 在第 1 部分中，键入选择**静态 (Static)**。点击**继续 (Continue)**。
- 步骤 8** 在部分 2 中（接口），为源接口选择**内部**，为目标接口选择**外部**。点击**继续 (Continue)**。
- 步骤 9** 在第 3 部分数据包中，执行以下操作：
 - 展开 Original Address 菜单，点击 **Choose**，然后选择 **http** 对象。
 - 展开 Translated Address 菜单，点击 **Choose**，然后选择 **Interface**。
 - 选中使用端口转换 (**Use Port Translation**)。
 - 选择 **tcp**、**http**、**http**。



- 步骤 10** 跳过第 4 节高级。
- 步骤 11** 对于 Firepower 威胁防御 (FTD)，请在第 5 部分名称中为 NAT 规则命名。
- 步骤 12** 点击**保存 (Save)**。新规则在 NAT 表的[NAT 规则的处理顺序](#)中创建。
- 步骤 13** 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。


到 SMTP 服务器的 NAT 传入 SMTP 流量

如果您只有一个或非常有限的公共 IP 地址，则可以创建一个网络对象 NAT 规则，将绑定到静态 IP 地址和端口的入站流量转换为内部地址。我们提供了适用于特定情况的程序，但您可以将其用作其他受支持应用的模型。

Before you begin

在开始之前，为 SMTP 服务器创建网络对象。在本程序中，我们将调用对象 **smtp-object**。有关说明，请参阅[创建网络对象](#)。

Procedure

- 步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。
- 步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。
- 步骤 3 点击设备类型选项卡。
- 步骤 4 选择要为其创建 NAT 规则的设备。
- 步骤 5 点击右侧**管理 (Management)** 窗格中的 **NAT**。
- 步骤 6 点击  > **网络对象 NAT**。
- 步骤 7 在第 1 部分中，键入选择**静态 (Static)**。点击**继续 (Continue)**。
- 步骤 8 在部分 2 中（接口），为源接口选择**内部**，为目标接口选择**外部**。点击**继续 (Continue)**。
- 步骤 9 在第 3 部分**数据包**中，执行以下操作：
 - 展开 Original Address 菜单，点击 **Choose**，然后选择 **smtp-server-object**。
 - 展开 Translated Address 菜单，点击 **Choose**，然后选择 **Interface**。
 - 选中使用端口转换 (**Use Port Translation**)。
 - 选择 **tcp**、**smtp**、**smtp**。



- 步骤 10 跳过第 4 节高级。
- 步骤 11 对于 Firepower 威胁防御 (FTD)，请在第 5 部分**名称**中为 NAT 规则命名。
- 步骤 12 点击**保存 (Save)**。新规则在 NAT 表的**NAT 规则的处理顺序**中创建。
- 步骤 13 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

将专用 IP 地址范围转换为公用 IP 地址范围

使用案例

如果您有一组特定设备类型或用户类型，需要将其 IP 地址转换为特定范围，以便接收设备（事务另一端的设备）允许流量传入。

将内部地址池转换为外部地址池

Before you begin

为要转换的私有 IP 地址池创建网络对象，并为要将这些私有 IP 地址转换为的公有地址池创建网络对象。



Note 对于 FTD，定义“转换后的地址”池的网络组不能是定义子网的网络对象。ASA

创建这些地址池时，请使用 [Create or Edit ASA Network Objects and Network Groups](#) 使用 [Create or Edit a Firepower Network Object or Network Groups](#) 了解相关说明。[创建或编辑 Firepower 网络对象或网络组](#)

出于以下程序的考虑，我们将私有地址池命名为 `inside_pool`，将公共地址池命名为 `outside_pool`。

Procedure

- 步骤 1 在 CDO 导航栏中，点击 **清单 (Inventory)**。
- 步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。
- 步骤 3 点击设备类型选项卡。
- 步骤 4 选择要为其创建 NAT 规则的设备。
- 步骤 5 点击右侧 **管理 (Management)** 窗格中的 **NAT**。
- 步骤 6 点击 > 网络对象 NAT。 
- 步骤 7 在第 1 部分“类型”中，选择“动态”，然后点击“继续”。
- 步骤 8 在第 2 部分 **接口 (Interfaces)** 中，为源接口选择 **内部**，为目标接口选择 **外部**。点击 **继续 (Continue)**。
- 步骤 9 在部分 3 数据包中，执行以下任务：
 - 对于 Original Address，请点击 **Choose**，然后选择您在上述前提条件部分中创建的 `inside_pool` 网络对象（或网络组）。
 - 对于 Translated Address，点击 **Choose**，然后选择您在上述前提条件部分中创建的 `outside_pool` 网络对象（或网络组）。
- 步骤 10 跳过第 4 节“高级”。
- 步骤 11 对于 Firepower 威胁防御 (FTD)，请在第 5 部分“名称”中为 NAT 规则命名。

步骤 12 点击**保存 (Save)**。

步骤 13 立即 [预览和部署所有设备的配置更改](#) 您所做的更改，或等待并一次部署多个更改。

防止在遍历外部接口时转换某个范围的 IP 地址

使用案例

使用此两次 NAT 使用案例启用站点间 VPN。

策略

您将 IP 地址池转换为自身，以便网络上一个位置的 IP 地址到达另一个位置时保持不变。

创建两次 NAT 规则

Before you begin

创建定义要转换为自身的 IP 地址池的网络对象或网络组。对于 FTD，地址范围可以通过定义子网的网络对象或包含该范围内所有地址的网络组对象来定义。

创建网络对象或网络组时，请使用[创建或编辑 Firepower 网络对象或网络组](#)获取说明。

在以下程序中，我们将调用网络对象或网络组，即站点间 PC 池。

Procedure

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要为其创建 NAT 规则的设备。

步骤 5 点击右侧**管理 (Management)** 窗格中的 **NAT**。

步骤 6 点击  > **两次 NAT (Twice NAT)**。。

步骤 7 在第 1 部分中，键入**选择静态 (Static)**。点击**继续 (Continue)**。

步骤 8 在部分 2 中（**接口**），为源接口选择**内部**，为目标接口选择**外部**。点击**继续 (Continue)**。

步骤 9 在第 3 部分**数据包**中，进行以下更改：

- 展开原始地址菜单，点击**Choose**，然后选择您在先决条件部分中创建的站点到站点 PC 池对象。
- 展开 Translated Address 菜单，点击 **Choose**，然后选择您在前提条件部分中创建的 Site-to-Site-PC-Pool 对象。

步骤 10 跳过第 4 节**高级**。

步骤 11 对于 Firepower 威胁防御 (FTD)，请在第 5 部分**名称**中为 NAT 规则命名。

- 步骤 12** 点击保存 (Save)。
- 步骤 13** 为 ASA 创建一个加密映射。有关创建加密映射的详细信息，请参阅 CLI 手册 3：思科 ASA 系列 VPN CLI 配置指南并查看 LAN 到 LAN IPsec VPN 一章。<https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html>
- 步骤 14** 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

虚拟专用网络管理

虚拟专用网络 (VPN) 连接在使用公共网络（如互联网）的终端之间建立安全隧道。

本节适用于 FDM 托管设备上的远程访问和站点间 VPN。它介绍了在 FTD 上构建站点间 VPN 连接的互联网协议安全 (IPsec) 标准。它还介绍了用于在 ASA FTD 上构建和远程访问 VPN 连接的 SSL 标准。

CDO 支持以下几种类型的 VPN 配置：

- [站点间虚拟专用网络，第 186 页](#)
- [远程访问虚拟专用网络](#)

有关虚拟专用网络的其他信息，请参阅[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#)。

站点间虚拟专用网络

站点间 VPN 隧道可连接不同地理位置的网络。您可以在托管设备之间以及托管设备与其他符合所有相关标准的思科或第三方对等体之间创建站点间的 IPsec 连接。这些对等体可以采用内部和外部 IPv4 和 IPv6 地址的任意组合。站点间隧道使用 Internet Protocol Security (IPsec) 协议套件或网络密钥交换版本 2 (IKEv2) 构建。建立 VPN 连接之后，本地网关后台的主机可通过安全 VPN 隧道连接至远程网关后台的主机。

VPN 拓扑

要创建一个新的站点间 VPN 拓扑，至少必须为其指定一个唯一名称，指定拓扑类型，选择用于 IPsec IKEv1 和/或 IKEv2 的 IKE 版本。配置完毕后，可以将拓扑部署到 FTD。

IPsec 和 IKE

在 CDO 中，站点间 VPN 是根据分配给 VPN 拓扑的 IKE 策略和 IPsec 建议配置的。策略和建议是定义站点到站点 VPN 的特性的参数集，例如用于在 IPsec 隧道中保护流量安全的安全协议和算法。可能需要多种策略类型来定义可以分配给 VPN 拓扑的完整配置映像。

身份验证

要对 VPN 连接进行身份验证，请在每个设备上拓扑中配置预共享密钥。预共享密钥允许在两个对等体之间共享安全密钥，该共享密钥在 IKE 身份验证阶段使用。

虚拟隧道接口 (VTI)

CDO 当前不支持在 FTD 上管理、监控或使用虚拟隧道接口 (VTI) 隧道。已配置 VTI 隧道的设备可以载入 CDO，但它会忽略 VTI 接口。如果安全区域或静态路由引用 VTI，则 CDO 会读取不带 VTI 引用的安全区域和静态路由。即将推出对 VTI 隧道的 CDO 支持。

相关信息：

- [为 FDM 管理 设备配置站点间 VPN, on page 187](#)
- [监控 FDM 管理 设备 站点间虚拟专用网络](#)

为 FDM 管理 设备配置站点间 VPN

思科防御协调器 (CDO) 支持 FDM 管理 设备上的站点间 VPN 功能：

- 支持 IPsec IKEv1 和 IKEv2 协议。
- 用于身份验证的自动或手动预共享密钥。
- IPv4 和 IPv6。支持内部和外部的所有组合。
- IPsec IKEv2 站点间 VPN 拓扑提供符合安全认证的配置设置。
- 静态和动态接口。
- 支持作为终端的外联网设备的动态 IP 地址。

外部网设备

每种拓扑类型都可以包括外部网设备，即不在 CDO 中管理的设备。其中包括：

- CDO 支持但您的组织不负责的思科设备。例如，由您公司内的其他部门管理的网络中的分支，或者与服务提供商或合作伙伴的网络的连接。
- 非托管设备。不能使用 CDO 创建配置以及将配置部署到非托管设备。将非托管设备作为“外联网”设备添加到 VPN 拓扑。此外，还指定每个远程设备的 IP 地址。

配置与动态寻址对等体的站点间 VPN 连接

如果其中一个对等体的 VPN 接口 IP 地址未知或接口从 DHCP 服务器获取其地址，CDO 允许您在对等体之间创建站点间 VPN 连接。预共享密钥、IKE 设置和 IPsec 配置与另一个对等体匹配的任何动态对等体都可以建立站点间 VPN 连接。

假设有两个对等体 A 和 B。静态对等体是其 VPN 接口为固定 IP 地址的设备，而动态对等体是其 VPN 接口为未知 IP 地址或具有临时 IP 地址的设备。

以下使用案例介绍了与动态寻址对等体建立安全站点间 VPN 连接的不同场景：

- A 是静态对等体，而 B 是动态对等体，反之亦然。
- A 是静态对等体，而 B 是具有来自 DHCP 服务器的已解析 IP 地址的动态对等体，反之亦然。您可以选择将 **VPN 绑定到分配的 IP (Bind VPN to the assigned IP)**，以便在静态对等体的 IP 地址和动态对等体的 DHCP 分配的 IP 地址之间建立 VPN 连接。
- A 和 B 是动态的，具有来自 DHCP 服务器的已解析 IP 地址。在这种情况下，必须为至少一个对等体选择将 **VPN 绑定到分配的 IP (Bind VPN to the assigned IP)**，以便在静态对等体的 IP 地址和动态对等体的 DHCP 分配 IP 地址之间建立 VPN 连接。
- A 是动态对等体，而 B 是具有静态或动态 IP 地址的外联网设备。
- A 是具有来自 DHCP 服务器的已解析 IP 地址的动态对等体，而 B 是具有静态或动态 IP 地址的外联网设备。您可以选择将 **VPN 绑定到分配的 IP (Bind VPN to the assigned IP)**，以便在静态对等体的 IP 地址和动态对等体的 DHCP 分配的 IP 地址之间建立 VPN 连接。

**Important**

如果选择将 **VPN 绑定到分配的 IP (Bind VPN to the assigned IP)**，则 VPN 会静态绑定到 DHCP 分配的 IP 地址。但是，在对等体重新启动后，该动态接口就可以接收许多新的 IP 地址。虽然 VPN 隧道会更新新的 IP 地址，但另一个对等体不会使用新的配置来更新。您必须再次部署站点间配置，以便在另一个对等体上实现带外更改。

**Note**

如果使用 防火墙设备管理器 等本地管理器更改了接口的 IP 地址，则 CDO 中该对等体的配置状态会显示“检测到冲突”。当您 **解决配置冲突** 时，其他对等体的配置状态 (**Configuration Status**) 会变成“未同步” (Not Synced) 状态。您必须将 CDO 配置部署到处于“未同步” (Not Synced) 状态的设备。

通常，连接必须由动态对等体发起，因为另一个对等体不知道动态对等体的 IP 地址。当远程对等体尝试建立连接时，另一个对等体会使用预共享密钥、IKE 设置和 IPsec 配置来验证连接。

由于只有在远程对等体发起连接之后才会建立 VPN 连接，因此在连接建立之前，系统会丢弃与允许流量通过 VPN 隧道的访问控制规则匹配的出站流量。这可确保数据不会在未采取适当加密和 VPN 保护措施的情况下离开您的网络。

**Note**

在以下情况下，无法配置站点间 VPN 连接：

- 如果两个对等体都有 DHCP 分配的 IP 地址。
 - **解决方法：** 如果其中一个对等体有从 DHCP 服务器获取的已解析 IP 地址，则可以配置站点间 VPN。在这种情况下，您必须选择将 **VPN 绑定到分配的 IP (Bind VPN to the assigned IP)** 以配置站点间 VPN。
- 如果设备有多个动态对等体连接。

- **解决方法：**您可以通过执行以下步骤来配置站点间 VPN：
 - 考虑三台设备 A、B 和 C。
 - 配置 A（静态对等体）和 B（动态对等体）之间的站点间 VPN 连接。
 - 通过创建外联网设备来配置 A 和 C（动态对等体）之间的 VPN 连接。将 A 的静态 VPN 接口 IP 地址分配给外联网设备，并与 C 建立连接。

FDM 管理站点间 VPN 准则和限制

- CDO 不支持使用 crypto-acl 来设计 S2S VPN 需要关注的流量。它仅支持受保护的流量。
- CDO 当前不支持在 ASA 或 FDM 管理设备上管理、监控或使用虚拟隧道接口 (VTI) 隧道。已配置 VTI 隧道的设备可以载入 CDO，但它会忽略 VTI 接口。如果安全区域或静态路由引用 VTI，则 CDO 会读取不带 VTI 引用的安全区域和静态路由。VTI 隧道的 CDO 支持即将推出。
- 只要使用的是 IKE 端口 500/4500，或者有一些 PAT 转换处于活动状态，则无法在同一端口上配置站点间 VPN，因为无法在这些端口上启动服务。
- 不支持传输模式，仅支持隧道模式。IPsec 隧道模式对整个原始 IP 数据报进行加密，使其成为新 IP 数据包中的负载。当防火墙对出入位于防火墙后的主机的流量进行保护时，请使用隧道模式。在通过不可信网络（例如互联网）连接的两个防火墙（或其他安全网关）之间，通常采用隧道模式实施常规 IPsec。
- 对于此版本，仅支持包含一个或多个 VPN 隧道的 PTP 拓扑。点对点 (PTP) 部署在两个终端之间建立 VPN 隧道。

相关信息：

- [创建站点间 VPN](#)
- [编辑现有 CDO 站点间 VPN](#)
- [VPN 中使用的加密和散列算法](#)
- [使站点间 VPN 流量豁免 NAT](#)

创建站点间 VPN

您可以通过以下两种方法之一创建站点间 VPN：简单配置和高级配置。在简单配置中，默认配置用于建立站点间 VPN 连接。您可以在高级 (**Advanced**) 模式下修改配置。

每种站点间 VPN 拓扑类型都可以包括外部网设备，即不在 CDO 中管理的设备。外部网设备可以是任何设备（思科或第三方设备），并非由 CDO 管理。

对于此版本，仅支持 PTP 拓扑，每个站点间连接包含一个隧道。点对点 (PTP) 部署在两个终端之间建立 VPN 隧道。

相关信息：

- [使用简单配置创建站点间 VPN, on page 190](#)

- [使用高级配置创建站点间 VPN, on page 191](#)
- [为站点间对等体之间的受保护流量配置网络, on page 193](#)

使用简单配置创建站点间 VPN

Procedure

步骤 1 在导航窗格中，选择 **VPN > 站点间 VPN**。

步骤 2 点击蓝色加号  按钮以创建 VPN 隧道。

Note 或者，您可以从 [清单 \(Inventory\)](#) 页面创建站点间 VPN 连接。

- 在导航栏中，点击 [清单 \(Inventory\)](#)。
- 选择要配置的两个 FDM 管理 设备。如果选择外联网设备，请指定外联网设备的 IP 地址。
- 在右侧页面的 [设备操作 \(Device Actions\)](#) 下，点击 [创建站点间 VPN \(Create Site-to-Site VPN\)](#)。

步骤 3 输入唯一的拓扑配置名称。我们建议命名您的拓扑以指示它是一个 FDM 管理 设备 VPN，并指定其拓扑类型。

步骤 4 从“设备” (Devices) 中选择此 VPN 部署的终端设备。

步骤 5 如果您在 [对等体 2 \(Peer 2\)](#) 中选择一个外联网设备，请选择 [静态 \(Static\)](#) 并指定 IP 地址，或者为使用 DHCP 分配 IP 的外联网设备选择 [动态 \(Dynamic\)](#)。IP 地址 (IP Address) 显示静态接口的 IP 地址或为动态接口分配的 DHCP。

步骤 6 为终端设备选择 [VPN 访问接口 \(VPN Access Interface\)](#)。

Note 如果一个或两个终端设备具有动态 IP 地址，请参阅 [配置与动态寻址对等体的站点间 VPN 连接](#) 以获取额外说明。

步骤 7 点击蓝色加号按钮 ，为参与的设备添加受保护的[网络](#)。

步骤 8 (可选) 选择 [NAT 免除 \(NAT Exempt\)](#) 以便从本地 VPN 访问接口的 NAT 策略中免除 VPN 流量。必须为单个对等体手动配置。如果不想将 NAT 规则应用于本地网络，请选择托管本地网络的接口。此选项仅在本地网络驻留在单个路由接口（而非网桥组成员）后时有用。如果本地网络位于多个路由接口或一个或多个网桥组成员之后，则必须手动创建 NAT 豁免规则。有关手动创建所需规则的信息，请参阅 [使站点间 VPN 流量豁免 NAT](#)。

步骤 9 点击 [创建 VPN \(Create VPN\)](#)，然后点击 [完成 \(Finish\)](#)。

步骤 10 执行其他强制性配置。请参阅 [为站点间对等体之间的受保护流量配置网络](#)。

已配置站点间 VPN。

使用高级配置创建站点间 VPN

Procedure


步骤 1 在导航栏上，选择 VPN。

步骤 2 点击蓝色加号  按钮以创建 VPN 隧道。

步骤 3 在对等设备部分中，指定以下设备配置：

- a. 输入唯一的拓扑配置名称。我们建议命名您的拓扑以指示它是一个 FDM 管理设备 VPN，并指定其拓扑类型。
- b. 从“设备” (Devices) 中选择此 VPN 部署的终端设备。
- c. 如果您选择了一个外联网设备，请选择静态 (Static) 并指定 IP 地址，或者为使用 DHCP 分配 IP 的外联网设备选择动态 (Dynamic)。IP 地址 (IP Address) 显示静态接口的 IP 地址或为动态接口分配的 DHCP。
- d. 为终端设备选择 VPN 访问接口 (VPN Access Interface)。

Note 如果一个或两个终端设备具有动态 IP 地址，请参阅[配置与动态寻址对等体的站点间 VPN 连接](#)以获取额外说明。

步骤 4 点击蓝色加号按钮 ，为参与的设备添加受保护的网络。


步骤 5 点击 **Advanced**。


步骤 6 在 **IKE 设置 (IKE Settings)** 部分中，选择要在互联网密钥交换 (IKE) 协商期间使用的 IKE 版本，并指定隐私配置：有关 IKE 策略的详细信息，请参阅[配置全局 IKE 策略](#)。

Note IKE 策略对设备是全局的，并应用于与其关联的所有 VPN 隧道。因此，添加或删除策略会影响此设备参与的所有 VPN 隧道。


- a. 根据需要选择一个或两个选项。


Note 默认情况下，**IKEV 版本 2** 和 **IKEV2 POLICIES** 出于启用状态。

- b. 点击蓝色加号  按钮，然后选择 IKEv2 策略。

点击创建新的 **IKEv2 策略 (Create New IKEv2 Policy)** 以创建新的 IKEv2 策略。或者，您可以转到 CDO 导航栏并点击 **对象 (Objects) > FDM 对象 (FDM Objects)**，然后点击  **> IKEv2 策略 (IKEv2 Policy)**。有关创建新 IKEv2 策略的详细信息，请参阅[配置 IKEv2 策略](#)。要删除现有 IKEv2 策略，请将鼠标悬停在所选的策略上，然后点击 **x** 图标。

- c. 点击 **IKE 版本 1 (IKE Version 1)** 将其启用。

- d. 点击蓝色加号  按钮，然后选择 IKEv1 策略。点击创建新的 **IKEv1 策略 (Create New IKEv1 Policy)** 以创建新的 IKEv1 策略。或者，您可以转到 CDO 导航栏并点击 **对象 (Objects) > FDM 对**

象 (FDM Objects)，然后点击  > **IKEv1 策略 (IKEv1 Policy)**。有关创建新 IKEv1 策略的详细信息，请参阅 [配置 IKEv1 策略](#)。要删除现有 IKEv1 策略，请将鼠标悬停在所选策略上，然后点击 **x** 图标。

- e. 输入参与设备的**预共享密钥**。预共享密钥是在连接中的每个对等体上配置的加密密钥字符串。这些密钥由 IKE 在身份验证阶段使用。
- (IKEv2) **对等体 1 预共享密钥、对等体 2 预共享密钥**：对于 IKEv2，您可以在每个对等体上配置唯一的密钥。输入**预共享密钥 (Pre-shared Key)**。您可以点击**显示覆盖 (Show Override)** 按钮，并为对等体输入适当的预共享。该密钥可以有 1 至 127 个字母数字字符。下表介绍了两个对等体的预共享密钥的用途。

	本地预共享密钥	远程对等预共享密钥
对等体 1	对等体 1 预共享密钥	对等体 2 预共享密钥
对等体 2	对等体 2 预共享密钥	对等体 1 预共享密钥


- (IKEv1) **预共享密钥**：对于 IKEv1，您必须在每个对等体上配置相同的预共享密钥。该密钥可以有 1 至 127 个字母数字字符。在此场景中，对等体 1 和对等体 2 使用相同的预共享密钥加密和解密数据。

- f. 点击下一步。

步骤 7 在 **IPSec 设置 (IPSec Settings)** 部分中，指定 IPSec 配置。相应的 IKEV 提议是否可用，具体取决于在 **IKE 设置** 步骤中所做的选择。

有关 IPSec 设置的详细信息，请参阅 [配置 IPSec 提议](#)。

- a. 点击蓝色加号  按钮，然后选择 IKEv2 提议。要删除现有的 IKEv2 提议，请将鼠标悬停在所选提议上，然后点击 **x** 图标。

Note 点击“创建新的 IKEv2 提议” (Create New IKEv2 Proposal) 以创建新的 IKEv2 提议。或者，您可以转到 CDO 导航栏并点击 **对象 (Objects) > FDM 对象 (FDM Objects)**，然后点击  > **IKEv2 IPSec 提议 (IKEv2 IPSec Proposal)**。

有关创建新 IKEv2 策略的详细信息，请参阅 [为 IKEv2 配置 IPSec 提议](#)。

- b. 选择适用于完全向前保密的 **Diffie-Hellman 组 (Diffie-Hellman Group for Perfect Forward Secrecy)**。有关详细信息，请参阅 [决定要使用的 Diffie-Hellman 模数组](#)。
- c. 点击**创建 VPN**。
- d. 阅读配置，如果满意，请点击**完成 (Finish)**。
- e. 执行其他强制性配置。请参阅 [为站点间对等体之间的受保护流量配置网络](#)。

为站点间对等体之间的受保护流量配置网络

完成站点间连接的配置后，请确保对 VPN 执行以下配置，以便在所有目标设备上运行。

Procedure

步骤 1 配置 AC 策略：

配置 AC 策略，用于允许两个对等体后面的受保护网络之间的双向流量。这些策略可帮助数据包到达预期目的地而不会被丢弃。

Note 您必须为两个对等体上的传入和传出流量创建 AC 策略。

- a. 在左侧的 思科防御协调器 导航栏中，点击**策略 (Policies)** 并选择所需的选项。
- b. 为两个对等体上的传入和传出流量创建策略。有关创建 AC 策略的详细信息，请参阅[配置 FDM 访问控制策略](#)。

以下示例显示了在两个对等体上创建 AC 策略的步骤。

考虑两个 FDM 管理设备 “FTD_BGL_972” 和 “FTD_BGL_973”，它们分别在两个受保护的网路 “boulder-network” 和 “sanjose-network” 之间建立了站点间 VPN 连接。

创建允许传入流量的 AC 策略：

策略 “Permit_incoming_VPN_traffic_from_973” 是在 “FTD_BGL_972” 设备上创建的，用于允许来自对等体 (“FTD_BGL_973”) 的传入流量。

The screenshot shows the 'New Access Rule' configuration window. At the top, there is a close button (X). Below the title, there are fields for 'Order' (set to 1), 'Name' (Permit_incoming_VPN_traffic_from_973), and 'Action' (Allow). Below these are tabs for 'Source/Destination', 'URLs', 'Applications', 'Users', 'Intrusion Policy', 'File Policy', and 'Logging'. The 'Source/Destination' tab is active, showing 'Source' and 'Destination' sections. Under 'Source', there are buttons for '+ ZONES', '+ NETS', and '+ PORTS'. Below these, 'outside_zone' is selected under ZONES, 'sanjose-net...' is selected under NETS, and 'Any' is selected under PORTS. Under 'Destination', there are buttons for '+ ZONES', '+ NETS', and '+ PORTS'. Below these, 'Any' is selected under ZONES, 'boulder-net...' is selected under NETS, and 'Any' is selected under PORTS.

- **源区域 (Source Zone):** 设置产生网络流量的对等设备的区域。在本示例中，流量源自 FTD_BGL_973 并到达 FTD_BGL_972。
- **源网络 (Source Network):** 设置发起网络流量的对等设备的受保护网络。在本例中，流量源自 “sanjose-network”，这是对等设备 (FTD_BGL_973) 背后的受保护网络。
- **目标网络:** 设置网络流量到达的设备的受保护网络。在本例中，流量到达 “boulder-network”，这是对等设备 (FTD_BGL_972) 背后的受保护网络。**注意：**其余字段可以使用默认值 (“任意”)。
- 将**操作 (Action)** 设置为允许 (**Allow**) 以便流量不受策略中的入侵及其他检测设置约束。

创建允许传出流量的 AC 策略：

策略 “Permit_outgoing_VPN_traffic_to_973” 是在 “FTD_BGL_972” 设备上创建的，用于允许向对等体（“FTD_BGL_973”）传出流量。

The screenshot shows the 'New Access Rule' configuration window. At the top, the rule name is 'Permit_outgoing_VPN_traffic_to_973' and the action is 'Allow'. Below this, there are tabs for 'Source/Destination', 'URLs', 'Applications', 'Users', 'Intrusion Policy', 'File Policy', and 'Logging'. The 'Source/Destination' tab is active, showing 'Source' and 'Destination' sections. Under 'Source', there are fields for 'ZONES', 'NETS', and 'PORTS'. The 'NETS' field contains 'boulder-net...'. Under 'Destination', there are fields for 'ZONES', 'NETS', and 'PORTS'. The 'NETS' field contains 'sanjose-net...' and the 'ZONES' field contains 'outside_zone'.

- **源网络 (Source Network):** 设置发起网络流量的对等设备的受保护网络。在本例中，流量源自 “boulder-network”，这是对等设备 (FTD_BGL_972) 背后的受保护网络。
- **目标区域 (Destination Zone):** 设置网络流量到达的对等设备的区域。在本示例中，流量从 FTD_BGL_972 到达并到达 FTD_BGL_973。
- **目标网络 (Destination Network):** 设置网络流量到达的对等体的受保护网络。在本例中，流量到达 “sanjose-network”，这是对等设备 (FTD_BGL_972) 背后的受保护网络。**注意：** 其余字段可以使用默认值（“任意”）。
- 将操作 (**Action**) 设置为允许 (**Allow**) 以便流量不受策略中的入侵及其他检测设置约束。

在一台设备上创建 AC 策略后，您必须在其对等设备上创建类似的策略。

步骤 2 如果在任一对设备上配置了 NAT，则需要手动配置 NAT 豁免规则。请参阅[使站点间 VPN 流量豁免 NAT](#)。

步骤 3 配置每个对等体上接收返回 VPN 流量的路由。有关详细信息，请参阅[为 FDM 管理设备配置静态路由和默认路由](#)。

- 网关 (Gateway)** - 选择标识网关 IP 地址的主机网络对象至目标网络。流量将发送至此地址。
- 接口 (Interface)** - 选择要通过其发送流量的接口。在本例中，流量通过 “外部” 接口发送。
- 目标网络 (Destination Networks)** - 选择一个或多个标识目标网络的网络对象。在本例中，目的地是对等设备 (FTD_BGL_973) 后面的 “sanjose-network”。

在一台设备上配置路由设置后，您必须在其对等设备上配置类似的设置。

编辑现有 CDO 站点间 VPN

默认情况下，使用高级配置向导修改现有站点间 VPN 配置。

Procedure

步骤 1 在导航栏上，选择 **VPN > 站点间 VPN (Site-to-Site VPN)**。

步骤 2 选择要编辑的所需站点间 VPN 隧道。

步骤 3 在操作 (**Actions**) 窗格中，点击 **编辑 (Edit)**。

Note 或者，您可以执行以下操作来编辑配置：

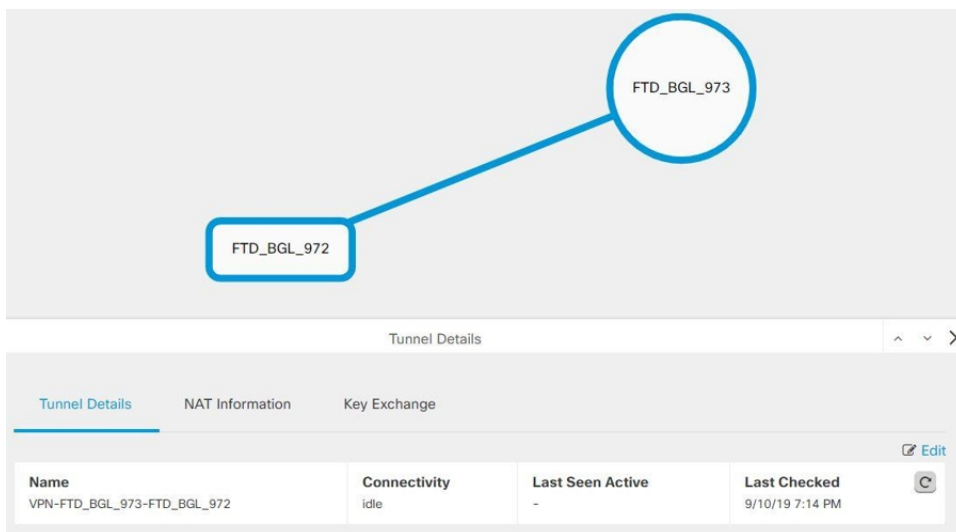
- a. 打开 VPN 页面，然后点击过滤器面板中的**全局视图 (Global View)** 按钮（有关详细信息，请参阅[搜索和过滤器站点间 VPN 隧道](#)）。

系统将显示所有设备上可用的所有站点间 VPN 隧道。

要编辑配置，其中一个对等体必须是 FDM 管理设备。

- b. 通过点击框选择设备。
- c. 点击**查看详细信息 (View details)** 以查看其对等体。
- d. 点击对等设备以查看隧道详细信息。

您可以查看与设备相关的隧道详细信息、NAT 信息和密钥交换信息。





- e. 点击隧道详细信息 (**Tunnel Details**) 中的**编辑 (Edit)**。


步骤 4 在对等设备 (**Peer Devices**) 部分中，您可以修改以下设备配置：配置名称、VPN 访问接口和受保护的网路。

Note 您无法更改参与设备。

步骤 5 在 **IKE 设置 (IKE Settings)** 部分中，您可以修改以下 IKEv2 策略配置：

- a. 点击相应设备的蓝色加号  按钮，然后选择新的 IKEv2 策略。要删除现有 IKEv2 策略，请将鼠标悬停在所选策略上，然后单击 **x** 图标。
- b. 修改参与设备的预共享密钥 (**Pre-Shared Key**)。如果终端设备的预共享密钥不同，请点击蓝色设置  按钮，然后输入设备的相应预共享密钥。
- c. 点击下一步。

步骤 6 在 **IPSec 设置 (IPSec Settings)** 部分中，您可以修改以下 IPSec 配置：

- a. 点击蓝色加号  按钮以选择新的 IKEv2 提议。要删除现有的 IKEv2 提议，请将鼠标悬停在所选提议上，然后单击 **x** 图标。
- b. 选择适用于完全向前保密的 **Diffie-Hellman** 组。
- c. 点击 **编辑 VPN (Edit VPN)**，然后点击 **完成 (Finish)**。

点对点 VPN 将使用您所做的所有更改进行修改和更新。

删除现有 CDO 站点间 VPN

Procedure

步骤 1 在导航栏上，选择 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

步骤 2 选择要删除的所需站点间 VPN 隧道。

步骤 3 在操作 (**Actions**) 窗格中，点击删除 (**Delete**)。

所选站点间 VPN 隧道将被删除。

VPN 中使用的加密和散列算法

由于 VPN 隧道通常流经公共网络（最可能是互联网），因此您需要对连接进行加密以保护流量。可以使用 IKE 策略和 IPsec 提议定义要应用的加密和其他安全技术。

如果您的设备许可证允许应用较强的加密，则有大量的加密和散列算法以及 Diffie-Hellman 组供您选择。然而，通常情况下，应用于隧道的加密越强，系统性能越差。您要在安全性和性能之间实现平衡，在提供充分保护的同时不牺牲效率。

我们无法就选择哪些选项提供具体指导。如果您在大型公司或其他组织执行运营，可能已有需要满足的指定标准。如果没有，请花些时间研究各个选项。

下面的主题介绍了几个可用选项：

决定使用哪个加密算法

在决定用于 IKE 策略或 IPsec 提议的加密算法时，您的选择仅限于 VPN 中的设备所支持的算法。

对于 IKEv2，您可以配置多个加密算法。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

对于 IPsec 提议，该算法用于封装安全协议 (ESP)，该协议提供身份验证、加密和防重放服务。ESP 为 IP 协议类型 50。在 IKEv1 IPsec 提议中，算法名称以 ESP 为前缀。

如果设备许可证符合强加密要求，可以从以下加密算法中选择。如果不符合强加密要求，则只能选择 DES。

- AES-GCM - (仅限 IKEv2。) Galois/Counter 模式中的高级加密标准是提供机密性和数据源身份验证的分组加密操作模式，并且提供比 AES 更高的安全性。AES-GCM 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。密钥越长，其提供的安全性就越高，但性能会随之降低。GCM 是支持 NSA Suite B 所需的 AES 模式。NSA Suite B 是一套加密算法，设备必须支持这套算法才能满足密码强度的联邦标准。
- AES-GMAC - (仅限 IKEv2 IPsec 提议。) 高级加密标准 Galois 消息身份验证代码是仅提供数据源身份验证的分组加密操作模式。它是 AES-GCM 的一个变体，允许在不加密数据的情况下进行数据身份验证。AES-GMAC 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。
- AES - 高级加密标准是一种对称密码算法，提供比 DES 更高的安全性，在计算上比 3DES 更高效。AES 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。密钥越长，其提供的安全性就越高，但性能会随之降低。
- DES - 数据加密标准，使用 56 位密钥进行加密，是一种对称密钥块算法。如果您的许可证账户不符合导出控制要求，这将是您唯一的选择。此算法比 3DES 快且使用的系统资源更少，但安全性也较低。如果不需要很强的数据保密性，并且系统资源或速度存在问题，请选择 DES。
- 3DES - 三重 DES，使用 56 位密钥加密三次，比 DES 更加安全，因其使用不同密钥对每个数据块处理三次。不过，此算法比 DES 使用的系统资源更多且速度更慢。
- NULL - 空加密算法提供不加密的身份验证。这通常仅用于测试目的。

决定使用哪些散列算法

在 IKE 策略中，散列算法创建消息摘要，用于确保消息的完整性。在 IKEv2 中，散列算法分成两个选项，一个用于完整性算法，一个用于伪随机函数 (PRF)。

在 IPsec 提议中，散列算法由封装安全协议 (ESP) 用于身份验证。在 IKEv2 IPsec 提议中，这称为完整性散列。在 IKEv1 IPsec 提议中，算法名称以 ESP- 为前缀，并且还有 -HMAC 后缀（代表“散列方法身份验证代码”）。

对于 IKEv2，您可以配置多个散列算法。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

您可以选择以下散列算法：

- SHA（安全散列算法）- 生成 160 位摘要的标准 SHA (SHA-1)。SHA 抗暴力攻击的能力高于 MD5。但是，它也比 MD5 占用更多资源。对于需要最高级别安全性的实施，请使用 SHA 散列算法。
- 以下 SHA-2 选项更加安全，可用于 IKEv2 配置。如果要实施 NSA Suite B 加密规范，请选择以下选项之一。
 - SHA-256 - 指定具有 256 位摘要的安全散列算法 SHA-2。
 - SHA-384 - 指定具有 384 位摘要的安全散列算法 SHA-2。
 - SHA-512 - 指定具有 512 位摘要的安全散列算法 SHA-2。
- MD5（消息摘要 5）- 生成 128 位的摘要。MD5 能使用更少的处理时间实现比 SHA 更快的整体性能，但 MD5 被认为安全性低于 SHA。
- 空或无（NULL、ESP-NONE）-（仅限 IPsec 提议。）空散列算法；这通常仅用于测试目的。但是，如果选择 AES-GCM/GMAC 选项之一作为加密算法，则应选择空完整性算法。即使选择非空选项，这些加密标准也会忽略完整性散列。

决定要使用的 Diffie-Hellman 模数组

您可以使用以下 Diffie-Hellman 密钥导出算法生成 IPsec 安全关联 (SA) 密钥。每组具有不同的长度模数。模数更大则安全性越高，但需要更多的处理时间。两个对等体上必须具有一个匹配的模数组。

如果选择 AES 加密，要支持 AES 所需的大型密钥长度，应使用 Diffie-Hellman (DH) 组 5 或更高组。IKEv1 策略不支持下面列出的所有组。

要实施 NSA Suite B 加密规范，请使用 IKEv2 并选择椭圆曲线 Diffie-Hellman (ECDH) 的一个选项：19、20 或 21。使用 2048 位模数的椭圆曲线选项和组较少遭受 Logjam 等攻击。

对于 IKEv2，您可以配置多个组。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

- 2 - Diffie-Hellman 组 2：1024 位模幂算法 (MODP) 组。此选项不再是一种良好的保护措施。
- 5 - Diffie-Hellman 组 5：1536 位 MODP 组。曾经被认为可以良好地保护 128 位密钥，如今却不再是一种良好的保护措施。
- 14 - Diffie-Hellman 组 14：2048 位模幂算法 (MODP) 组。被认为可以良好地保护 192 位密钥。
- 19 - Diffie-Hellman 组 19：美国国家标准与技术研究所 (NIST) 256 位椭圆曲线取素数 (ECP) 组。
- 20 - Diffie-Hellman 组 20：NIST 384 位 ECP 组。
- 21 - Diffie-Hellman 组 21：NIST 521 位 ECP 组。
- 24 - Diffie-Hellman 组 24：带 256 位素数阶子组的 2048 位 MODP 组。我们不再建议采用此选项。

确定使用哪种身份验证方法

您可以使用以下方法对站点间 VPN 连接中的对等体进行身份验证。

预共享密钥

预共享密钥是在连接中的每个对等体上配置的加密密钥字符串。这些密钥由 IKE 在身份验证阶段使用。对于 IKEv1，您必须在每个对等体上配置相同的预共享密钥。对于 IKEv2，您可以在每个对等体上配置唯一密钥。

与证书相比，预共享密钥的扩展性相对逊色。如果需要配置大量的站点间 VPN 连接，请使用证书而非预共享密钥。

使站点间 VPN 流量豁免 NAT

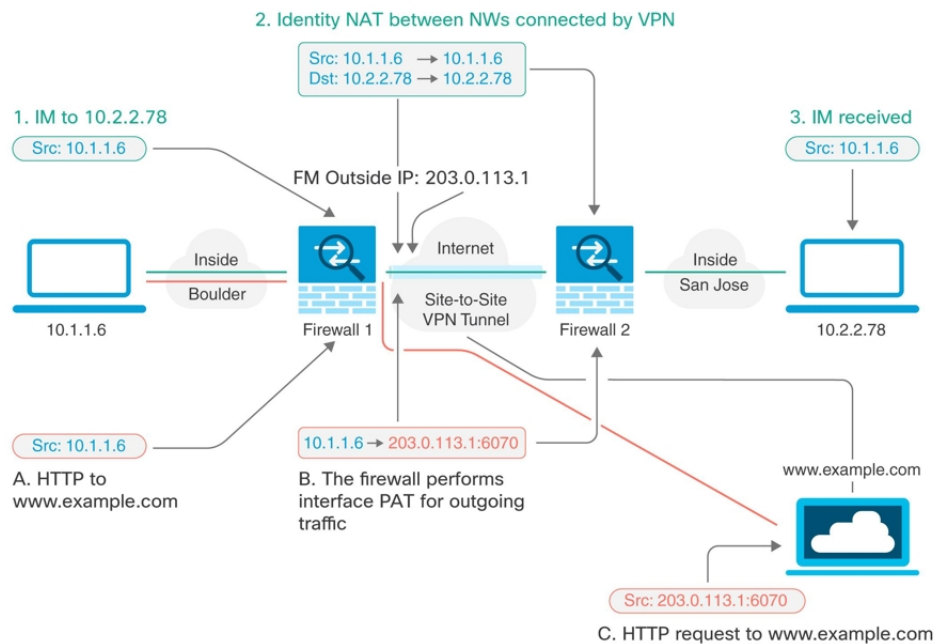
当您在某个接口上定义了站点间 VPN 连接并且还对该接口实施了 NAT 规则时，可以选择使该 VPN 上的流量豁免 NAT 规则。如果 VPN 连接的远端可以处理您的内部地址，则可能要执行此操作。

创建 VPN 连接时，可以选择 **NAT 豁免** 选项自动创建 NAT 豁免规则。不过，此操作仅在通过单个路由接口（而非网桥组成员）连接本地受保护网络时才奏效。相反，如果该连接中的本地网络位于两个或多个路由接口之后或者一个或多个网桥组成员之后，则需要手动配置 NAT 豁免规则。

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

- 如果连接中有多个本地网络，请创建一个网络对象组用于容纳定义这些网络的对象。
- 如果 VPN 中同时包括 IPv4 和 IPv6 网络，请为其各创建一个单独的身份 NAT 规则。

下例显示连接博尔德办公室和圣荷西办公室的站点间隧道。对于要发送到互联网的流量（例如，从博尔德办公室中的 10.1.1.6 到 www.example.com），需要利用 NAT 提供的公用 IP 地址访问互联网。以下示例使用接口端口地址转换 (PAT) 规则。然而，对于要穿过 VPN 隧道的流量（例如，从博尔德办公室中的 10.1.1.6 到圣荷西办公室中的 10.2.2.78），您不想执行 NAT；您需要通过创建身份 NAT 规则来豁免此流量。身份 NAT 将地址转换为其相同的地址。




以下示例说明 Firewall1（博尔德办公室）的配置。该示例假定内部接口是网桥组，因此需要为每个成员接口编写规则。如果有一个或多个路由内部接口，其过程相同。



Note 此示例假定只包括 IPv4 网络。如果该 VPN 还包括 IPv6 网络，请为 IPv6 创建并行规则。请注意，由于无法实施 IPv6 接口 PAT，因此需要使用唯一 IPv6 地址创建主机对象用于 PAT。

Procedure

步骤 1 创建对象来定义各种网络。

- 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
- 点击蓝色加号按钮  以创建新的对象。
- 点击 **FTD > 网络 (Network)**。
- 找到博尔德办公室内部网络。
- 输入对象名称（例如，boulder-network）。
- 选择 **创建网络对象**。
- 在“值”部分：
 - 选择 **eq** 并输入以 CIDR 表示法表示的单个 IP 地址或子网地址。

- 选择 **范围** 并输入 IP 地址范围。例如，输入网络地址 10.1.1.0/24。


Adding FTD Network Object

Object Name
boulder-network

Description
Object description

Create a network group Create a network object



Value
eq ▲ 10.1.1.0/24

- h. 点击添加 (**Add**)。
- i. 点击蓝色加号按钮  以创建新的对象。
- j. 定义内部圣荷西办公室网络。
- k. 输入对象名称（例如，san-jose）。
- l. 选择 **创建网络对象**。
- m. 在“值”部分：
 - 选择 **eq** 并输入以 CIDR 表示法表示的单个 IP 地址或子网地址。


- 选择 **范围** 并输入 IP 地址范围。例如，输入网络地址 10.1.1.0/24。

- n. 点击**添加 (Add)**。

步骤 2 在 Firewall1（博尔德办公室）上，为博尔德办公室网络配置经过 VPN 连接到圣荷西办公室时的手动身份 NAT。

- a. 在 CDO 导航栏中，点击**清单 (Inventory)**。
- b. 使用过滤器查找要为其创建 NAT 规则的设备。
- c. 在详细信息面板的管理区域中，点击 **NAT**  **NAT**。
- d. 点击  **> 两次 NAT**。
 - 在第 1 部分中，选择**静态 (Static)**。点击**继续**。
 - 在部分 2 中，选择源接口 (**Source Interface**) = **inside** 和目标接口 (**Destination Interface**) = **outside**。点击**继续**。
 - 在第 3 部分中，选择原始源地址 (**Source Original Address**) = 'boulder-network' 和 转换后的源地址 (**Source Translated Address**) = 'boulder-network'。
 - 选择 **使用目的**。
 - 选择原始目标地址 (**Destination Original Address**) = 'sanjose-network' 和转换后的源地址 (**Source Translated Address**) = 'sanjose-network'。注意：由于您不需要转换目的地址，因此需要通过为原始目的地址和转换后的目的地址指定相同的地址，从而为其配置身份 NAT。将所有端口字段留空。此规则为源和目标配置身份 NAT。

FTD: FTD_BGL_972 / NAT Rules



Type: Static

Interfaces

Source Interface:

Destination Interface:

ⓘ Select the source interface and destination interface for packets going through this rule.

Packets

Source

Original Address:

Translated Address:

Use Destination

Destination

Original Address:

Translated Address:

Use Service Objects

ⓘ Select the original address and translated address for packets going through this rule.


Advanced

Disable proxy ARP for incoming packets

Use route lookup to determine the egress interface

- 选择为传入数据包禁用代理 ARP (**Disable proxy ARP for incoming packets**)。
- 点击保存 (**Save**)。
- 重复此过程，为每个其他内部接口创建相应规则。

步骤 3 在 Firewall1（博尔德办公室）上，为内部博尔德办公室网络配置接入互联网时的手动动态接口 PAT。
注意：内部接口可能已经配置了将所有 IPv4 流量包括在内的动态接口 PAT 规则，因为初始配置过程中会默认创建这些规则。不过，为完整起见，此处仍显示了这些配置。完成这些步骤之前，请检查是否已经存在将内部接口和网络包括在内的规则，如有则跳过此步骤。

- 点击  > 两次 NAT。
- 在第 1 部分中，选择动态 (**Dynamic**)。点击继续。
- 在部分 2 中，选择源接口 (**Source Interface**) = **inside** 和目标接口 (**Destination Interface**) = **outside**。点击继续。

- d. 在第 3 部分中，选择原始源地址 (Source Original Address) = 'boulder-network' 和转换后的源地址 (Source Translated Address) = 'interface'。

FTD: FTD_BGL_972 / NAT Rules

Cancel Save

GigabitEthernet inside 0/1 0/0 GigabitEthernet outside

Type → Dynamic

Interfaces

Source Interface: inside

Destination Interface: outside

① Select the source interface and the destination interface for packets going through this NAT rule.

Packets

Source

Original Address: boulder-network

Translated Address: interface

① Select the original address and the translated address for packets going through this NAT rule.

Use Destination

Use Service Objects

- e. 点击保存 (Save)。
- f. 重复此过程，为每个其他内部接口创建相应规则。

步骤 4 将配置更改部署到 CDO。有关详细信息，请参阅[将配置更改从 CDO 部署到 FDM 管理设备](#)。

步骤 5 如果您也管理着 Firewall2（圣荷西办公室），您可以为该设备配置类似的规则。

- 当目标是 boulder-network 时，手动身份 NAT 规则将用于 'sanjose-network'。为 Firewall2 内部和外部网络创建新的接口对象。
- 当目标是“任何”时，手动动态接口 PAT 规则将用于 'sanjose-network'。

配置全局 IKE 策略

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。

IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用提议。IKE 提议是一组两个对等体用于保护其之间的协商的算法。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数用于保护后续 IKE 协商。

IKE 策略对象为这些协商定义 IKE 提议。您启用的对象是对等体协商 VPN 连接时使用的对象：不能为每个连接指定不同的 IKE 策略。每个对象的相对优先级确定首先尝试这些策略中的哪一个，数字越小优先级越高。如果协商无法找到两个对等体全都支持的策略，则不建立连接。

要定义全局 IKE 策略，需要为每个 IKE 版本选择启用哪些对象。如果预定义的对象不能满足您的要求，请创建新的策略来执行您的安全策略。

以下步骤说明如何通过“对象”(Objects) 页面配置全局策略。在编辑 VPN 连接时，您还可以点击 IKE 策略设置的编辑，来启用、禁用和创建策略。

以下主题介绍如何为每个 IKE 策略版本配置 IPsec 提议：

- [配置 IKEv1 策略](#)
- [配置 IKEv2 策略](#)

管理 IKEv1 策略

介绍如何创建和编辑 IKEv1 策略。

关于 IKEv1 策略

互联网密钥交换 (IKE) 版本 1 策略对象包含定义 VPN 连接时 IKEv1 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义 IKEv1 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

Related Topics

[创建或编辑 IKEv1 策略](#)，第 205 页

创建或编辑 IKEv1 策略

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。您还可以点击对象列表中所示的**创建新 IKE 策略 (Create New IKEv1 Policy)** 链接，以便在站点间 VPN 连接中编辑 IKEv1 设置时创建 IKEv1 策略对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮 ，然后选择 **FDM > IKEv1 策略 (IKEv1 Policy)** 以创建新的 IKEv1 策略。
- 在对象页面中，选择要编辑的 IKEv1 策略，然后点击右侧“操作”(Actions) 窗格中的 **编辑 (Edit)**。

步骤 3 输入对象名称，最多 128 个字符。

步骤 4 配置 IKEv1 属性。

- **优先级** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **加密** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。有关选项的说明，请参阅“决定使用哪种加密算法”。

- **Diffie-Hellman 组 (Diffie-Hellman Group)** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。有关选项的解释，请看“[决定要使用的 Diffie-Hellman 模数组](#)”。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。
- **身份验证 (Authentication)** - 在两个对等体之间使用的身份验证方法。关于更多信息，请参阅 [确定使用哪种身份验证方法](#)。
 - **预共享密钥** - 使用在每个设备上定义的预共享密钥。在身份验证阶段，此类密钥允许密钥在两个对等体之间共享并由 IKE 使用。如果未使用同一预共享密钥配置对等体，则无法建立 IKE SA。
 - **证书 (Certificate)** - 使用对等体的设备身份证书来识别彼此。必须通过在证书颁发机构中注册每个对等体来获取这些证书。还须上传用于签署每个对等体的身份证书的受信任 CA 根证书和中间 CA 证书。对等体可以注册到相同或不同的 CA 中。对于任一对等体，都不能使用自签证书。
- **散列** - 用于创建消息摘要的散列算法，以确保消息的完整性。有关选项的说明，请参阅 [决定要使用的 Diffie-Hellman 模数组](#)。

步骤 5 点击添加。

管理 IKEv2 策略

介绍如何创建和编辑 IKEv2 策略。

关于 IKEv2 策略

互联网密钥交换 (IKE) 版本 2 策略对象包含定义 VPN 连接时 IKEv2 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv2 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

Related Topics

[创建或编辑 IKEv2 策略](#)，第 206 页


创建或编辑 IKEv2 策略

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。您还可以点击对象列表中所示的 [创建新的 IKE 策略](#) 链接，以便在站点间 VPN 连接中编辑 IKEv1 设置时创建 IKEv1 策略对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮 ，然后选择 **FDM > IKEv2 策略 (IKEv2 Policy)** 以创建新的 IKEv2 策略。
- 在对象页面中，选择要编辑的 IKEv2 策略，然后点击右侧“操作” (Actions) 窗格中的 **编辑 (Edit)**。

步骤 3 输入对象名称 (object name)，最多 128 个字符。

步骤 4 配置 IKEv2 属性。

- **优先级** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **状态** - IKE 策略是启用还是禁用状态。点击开关以更改状态。在 IKE 协商期间仅使用启用的策略。
- **加密 (Encryption)** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。选择要允许的所有算法，但不能在同一策略中同时包括混合模式 (AES-GCM) 和正常模式选项。（正常模式要求选择完整性散列，而混合模式禁止选择单独的完整性散列。）系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅 [决定使用哪个加密算法](#)。
- **Diffie-Hellman 组 (Diffie-Hellman Group)** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。选择要允许的所有算法。系统与对等体协商，从最强到最弱组，直到达成匹配。有关选项的解释，请参阅 [决定要使用的 Diffie-Hellman 模数组](#)。
- **完整性散列 (Integrity Hash)** - 用于创建消息摘要的散列算法的完整性部分，用于确保消息完整性。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。完整性散列不与 AES-GCM 加密选项一起使用。有关选项的说明，请参阅 [决定使用哪些散列算法](#)。
- **伪随机函数 (PRF) 散列 (Pseudo-Random Function [PRF] Hash)** - 散列算法中用作派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法的伪随机函数 (PRF) 部分。在 IKEv1 中，完整性和 PRF 算法不分开，但在 IKEv2 中，可以为这些元素指定不同的算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅 [决定使用哪些散列算法](#)。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。

步骤 5 点击添加。

配置 IPsec 提议

IPsec 是设置 VPN 的最安全方法之一。IPsec 在 IP 数据包级别提供数据加密，提供一种基于标准的强大的安全解决方案。使用 IPsec，数据通过隧道在公共网络上传输。隧道是两个对等体之间安全的逻辑通信路径。进入 IPsec 隧道的流量由称为转换集的安全协议和算法组合保护。在 IPsec 安全关联 (SA) 协商期间，对等体搜索在两个对等体处相同的转换集。

根据 IKE 版本 (IKEv1 或 IKEv2)，存在不同的 IPsec 提议对象：

- 当创建 IKEv1 IPsec 提议时，可以选择 IPsec 运行的模式，并定义所需的加密和身份验证类型。您可以为算法选择单一选项。如果要在 VPN 中支持多个组合，请创建和选择多个 IKEv1 IPsec 提议对象。
- 当创建 IKEv2 IPsec 提议时，可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序，并与对等体进行协商，直到找到匹配。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。



Note 我们建议对 IPsec 隧道使用加密和身份验证。

以下主题介绍如何为每个 IKE 版本配置 IPsec 提议：

- [创建和编辑 IKEv1 IPsec 提议对象](#)
- [创建和编辑 IKEv2 IPsec 提议对象](#)

管理 IKEv1 IPsec 提议对象

IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。IKEv1 和 IKEv2 有单独的对象。目前，Cisco Defense Orchestrator (CDO) 支持 IKEv1 IPsec 提议对象。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。



Note 我们建议对 IPsec 隧道使用加密和身份验证。

Related Topics

[创建或编辑 IKEv1 IPsec 提议对象](#)，第 209 页

创建或编辑 IKEv1 IPsec 提议对象


有几个预定义的 IKEv1 IPsec 提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象” (Objects) 页面直接创建和编辑对象。此外，也可以在编辑站点间 VPN 连接中的 IKEv1 IPsec 设置时，点击对象列表中所示的**创建新 IKEv1 提议 (Create New IKEv1 Proposal)** 链接来创建 IKEv1 IPsec 提议对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮 ，然后选择 **FDM > IKEv1 IPsec 提议 (IKEv1 IPsec Proposal)** 以创建新对象。
- 在对象页面中，选择要编辑的 IPsec 方案，然后点击右侧“操作” (Actions) 窗格中的 **编辑 (Edit)**。

步骤 3 为新对象输入对象名称。

步骤 4 选择 IKEv1 IPsec 提议对象的运行模式。

- **隧道模式**会封装整个 IP 数据包。IPsec 报头被添加到原始 IP 报头和新的 IP 报头之间。这是默认值。当防火墙对出入位于防火墙后的主机的流量进行保护时，请使用隧道模式。在通过不可信网络（例如互联网）连接的两个防火墙（或其他安全网关）之间，通常采用隧道模式实施常规 IPsec。
- **传输模式**只封装 IP 数据包的上层协议。IPsec 报头被插入到 IP 报头和上层协议报头（例如 TCP）之间。传输模式要求源和目的主机都支持 IPsec，并且只有在隧道的目的对等体是 IP 数据包的最最终目的时才可使用。通常只有在保护第 2 层或第 3 层隧道协议（例如 GRE、L2TP 和 DLSW）时，才会使用传输模式。

步骤 5 选择**加密 (Encryption)**提议的（封装安全协议加密）算法。有关选项的说明，请参阅 [决定使用哪个加密算法](#)。

步骤 6 选择要用于身份验证的 **ESP 散列 (ESP Hash)** 或完整性算法。有关选项的说明，请参阅[决定使用哪些散列算法](#)。

步骤 7 点击添加。

管理 IKEv2 IPsec 提议对象

IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。

当创建 IKEv2 IPsec 提议时，可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序，并与对等体进行协商，直到找到匹配。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

Related Topics

[创建或编辑 IKEv2 IPsec 提议对象](#)，第 210 页

创建或编辑 IKEv2 IPsec 提议对象


有几个预定义的 IKEv2 IPsec 提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects)页面直接创建和编辑对象。此外，也可以在编辑 VPN 连接中的 IKEv2 IPsec 设置时，点击对象列表中所指示的创建新 IPsec 提议链接来创建 IKEv2 IPsec 提议对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮 ，然后选择 **FDM > IKEv2 IPsec 提议 (IKEv2 IPsec Proposal)** 以创建新对象。
- 在对象页面中，选择要编辑的 IPsec 方案，然后点击右侧“操作”(Actions)窗格中的 **编辑 (Edit)**。

步骤 3 为新对象输入对象名称。

步骤 4 配置 IKEv2 IPsec 方案对象：

- **加密 (Encryption)** - 此提议的封装安全协议 (ESP) 加密算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅 [决定使用哪个加密算法](#)。
- **完整性散列 (Integrity Hash)** - 要用于身份验证的散列或完整性算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅 [决定使用哪些散列算法](#)。

步骤 5 点击添加。

监控 FDM 管理设备 站点间虚拟专用网络

CDO 允许您在载入的 FDM 管理设备上监控、修改和删除现有或新创建的站点间 VPN 配置。

检查站点间 VPN 隧道连接

使用 **Check Connectivity** 按钮触发对隧道的实时连接检查，以确定隧道当前处于 [搜索和过滤器站点间 VPN 隧道](#)。除非您点击“按需连接检查”按钮，否则将每小时检查一次所有已自行激活设备上可用的所有隧道。

**Note**

- CDO 在 FTD 上运行此连接检查命令，以确定隧道处于活动状态还是空闲状态：

```
show vpn-sessiondb l2l sort ipaddress
```

- 建模 ASA 设备将始终显示为空闲。

要从 VPN 页面检查隧道连接，请执行以下操作：

Procedure

步骤 1 在主导航栏中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

步骤 2 **搜索和过滤器** 站点间 **VPN 隧道** 站点间 VPN 隧道的隧道列表，然后选择该列表。

步骤 3 在右侧的操作窗格中，点击 **检查连接**。

确定 VPN 问题

CDO 可以识别 ASA FTD 上的 VPN 问题。（此功能尚不适用于 AWS VPC 站点间 VPN 隧道。）本文将介绍以下内容：

- [查找缺少对等体的 VPN 隧道](#)
- [查找存在加密密钥问题的 VPN 对等体](#)
- [查找为隧道定义的不完整或配置错误的访问列表](#)
- [查找隧道配置中的问题](#)

[解决隧道配置问题, on page 213](#)


查找缺少对等体的 VPN 隧道

“缺少 IP 对等体”情况在 ASA 设备上比 FDM 管理设备上更可能发生。


Procedure

步骤 1 在 CDO 导航窗格中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

步骤 2 选择 **表视图 (Table View)**。

步骤 3 通过点击过滤器图标  打开过滤器面板。

步骤 4 检查检测到的问题。


步骤 5 选择每个报告问题  的设备，然后查看右侧的“对等体”窗格。系统将列出一个对等体名称。CDO 报告另一个对等体名称为 “[缺少对等体 IP.]”。

查找存在加密密钥问题的 VPN 对等体

使用此方法查找存在加密密钥问题的 VPN 对等体，例如：

- IKEv1 或 IKEv2 密钥无效、缺失或不匹配
- 过时或低加密隧道


Procedure

-
- 步骤 1** 在 CDO 导航栏中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。
 - 步骤 2** 选择表视图 (**Table View**)。
 - 步骤 3** 通过点击过滤器图标  打开过滤器面板。
 - 步骤 4** 选择每个报告问题的设备，然后查看右侧的“对等体”窗格。▲对等体信息将显示两个对等体。
 - 步骤 5** 点击其中一台设备的查看对等体。
 - 步骤 6** 双击图表视图中报告问题的设备。
 - 步骤 7** 点击底部隧道详细信息面板中的密钥交换。您将能够查看两台设备并从该点诊断关键问题。
-

查找为隧道定义的不完整或配置错误的访问列表

“不完整或配置错误的访问列表”条件只能出现在 ASA 设备上。

Procedure





-
- 步骤 1** 在 CDO 导航栏中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。
 - 步骤 2** 选择表视图 (**Table View**)。
 - 步骤 3** 通过点击过滤器图标  打开过滤器面板。
 - 步骤 4** 选择每个报告问题的设备，然后查看右侧的“对等体”窗格。▲对等体信息显示两个对等体。
 - 步骤 5** 点击其中一台设备的查看对等体。
 - 步骤 6** 双击图表视图中报告问题的设备。
 - 步骤 7** 点击底部隧道详细信息面板中的隧道详细信息。您将看到消息“网络策略：不完整”
-

查找隧道配置中的问题

在以下情况下可能会发生隧道配置错误：

- 当站点间 VPN 接口的 IP 地址更改时，“对等 IP 地址值已更改”。
- 当 VPN 隧道的 IKE 值与另一个 VPN 隧道不匹配时，系统将显示“IKE 值不匹配”消息。

Procedure

- 步骤 1** 在 CDO 导航栏中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。
- 步骤 2** 选择表视图 (**Table View**)。
- 步骤 3** 通过点击过滤器图标  打开过滤器面板。
- 步骤 4** 在隧道问题 (**Tunnel Issues**) 中，点击检测到的问题 (**Detected Issues**) 以查看 VPN 配置报告错误。您可以查看配置报告问题 。
- 步骤 5** 选择 VPN 配置报告问题。
- 步骤 6** 在右侧的对等体窗格中，会显示存在问题的对等体的  图标。将鼠标悬停在  图标上可查看问题和解决方案。

下一步：[解决隧道配置问题](#)。

解决隧道配置问题

此程序尝试解决以下隧道配置问题：


- 当站点间 VPN 接口的 IP 地址更改时，“对等 IP 地址值已更改”。
- 当 VPN 隧道的 IKE 值与另一个 VPN 隧道不匹配时，系统将显示“IKE 值不匹配”消息。

有关详细信息，请参阅[查找隧道配置中的问题](#)。

过程

- 步骤 1** 在 CDO 导航栏中，点击**清单 (Inventory)**。
- 步骤 2** 点击**设备**选项卡。
- 步骤 3** 点击相应的设备类型选项卡，然后选择与报告问题的 VPN 配置关联的设备。
- 步骤 4** 接受设备更改。[解决“检测到冲突”状态，第 342 页](#)
- 步骤 5** 在 CDO 导航窗格中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。
- 步骤 6** 选择报告此问题的 VPN 配置。
- 步骤 7** 点击**操作 (Actions)** 窗格中的**编辑** 图标。
- 步骤 8** 在每个步骤中点击下一步，直到您在步骤 4 中点击完成按钮。
- 步骤 9** [预览和部署所有设备的配置更改，第 332 页](#)。

搜索和过滤器站点间 VPN 隧道

将过滤器边栏  与搜索字段结合使用，可重点搜索 VPN 隧道图中显示的 VPN 隧道。

Procedure

步骤 1 在主导航栏中，导航至 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

步骤 2 点击过滤器图标  可打开过滤器窗格。

步骤 3 使用以下过滤器细化搜索：

- **按设备过滤 (Filter by Device)** - 点击按设备过滤 (**Filter by Device**)，选择设备类型选项卡，然后选中要通过过滤查找的设备。
- **隧道问题 (Tunnel Issues)** - 我们是否检测到隧道的任一端存在问题。存在问题的设备的一些示例可能包括（但不限于）：缺少关联的接口或对等体 IP 地址或访问列表、IKEv1 提议不匹配等。（检测隧道问题尚不适用于 AWS VPC VPN 隧道。）
- **设备/服务 (Devices/Services)** - 按设备类型过滤。
- **状态 (Status)** - 隧道状态可以是活动或空闲。
 - **活动 (Active)** - 存在网络数据包通过 VPN 隧道的开放会话，或者已成功建立会话且尚未超时的会话。活动可以帮助指示隧道处于活动状态和相关性。
 - **空闲 (Idle)** - CDO 无法发现此隧道的开放会话，隧道可能未在使用或此隧道存在问题。
- **已载入 (Onboarded)** - 设备可以由 CDO 管理，也可以不由 CDO 管理（非托管）。
 - **托管 (Managed)** - 按 CDO 管理的设备过滤。
 - **非托管 (Unmanaged)** - 按 CDO 不管理的设备进行过滤。
- **设备类型 (Device Types)** - 隧道的任一端是实时（已连接设备）还是模型设备。

步骤 4 您还可以通过在搜索栏中输入设备名称或 IP 地址来搜索过滤结果。搜索不区分大小写。

载入非托管设备

在载入其中一个对等设备时，CDO 将发现站点间 VPN 隧道。如果第二个对等设备不由 CDO 管理，则您可以过滤 VPN 隧道列表以查找非受管设备并将其载入：

Procedure

步骤 1 在主导航栏中，选择 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

步骤 2 选择表视图 (**Table View**)。

步骤 3 通过点击  打开过滤器面板。

步骤 4 点击非托管 (**Unmanaged**)。

步骤 5 从表中的结果中选择一个隧道。

步骤 6 在右侧的对等体 (Peers) 窗格中，点击载入设备 (Onboard Device)，然后按照屏幕上的说明进行操作。

相关信息：

- [载入设备和服务](#)
- [载入威胁防御设备](#)

查看站点间 VPN 隧道的 IKE 对象详细信息

您可以查看所选隧道的对等体/设备上配置的 IKE 对象的详细信息。这些详细信息根据 IKE 策略对象的优先级显示在层次结构中的树结构中。



Note 外联网设备不显示 IKE 对象详细信息。

Procedure

步骤 1 在左侧 CDO 导航栏中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

步骤 2 在 VPN Tunnels 页面中，点击连接对等体的 VPN 隧道的名称。

步骤 3 在右侧的“关系”下，展开要查看其详细信息的对象。

查看上次成功建立站点间 VPN 隧道的日期

Procedure

步骤 1 [查看站点间 VPN 隧道信息](#)。

步骤 2 点击 **Tunnel Details** 窗格。

步骤 3 查看上次查看的活动字段。

查看站点间 VPN 隧道信息

站点间 VPN 表视图是载入 CDO 的所有设备上可用的所有站点间 VPN 隧道的完整列表。隧道在此列表中仅存在一次。点击表中列出的隧道会在右侧栏中提供一个选项，以直接导航到隧道的对等体以进行进一步调查。

如果 CDO 不管理隧道的两端，您可以点击[载入非托管设备](#)以打开主载入页面并载入非托管对等设备。在 CDO 管理隧道两端的情况下，对等体 2 列包含受管设备的名称。但是，对于 AWS VPC，对等体 2 列包含 VPN 网关的 IP 地址。

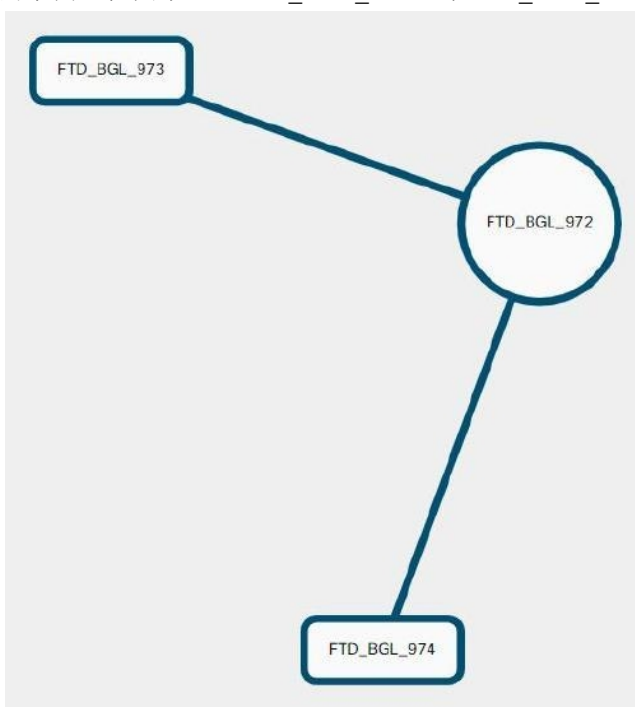
要在表视图中查看站点间 VPN 连接，请执行以下操作：

Procedure

- 步骤 1 在主导航栏中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。
- 步骤 2 点击**表格视图 (Table view)** 按钮。
- 步骤 3 使用[搜索和过滤器站点间 VPN 隧道](#) 以查找特定隧道，或放大大局视图图形以查找要查找的 VPN 网关及其对等体。

站点间 VPN 全局视图

这是全局视图的示例。在图中，“FTD_BGL_972”与 FTD_BGL_973 和 FTD_BGL_974 设备建立了



站点间连接。

Procedure

- 步骤 1 在主导航栏中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。
- 步骤 2 点击**全局视图 (Global view)** 按钮。
- 步骤 3 使用[搜索和过滤器站点间 VPN 隧道](#) 以查找特定隧道，或放大大局视图图形以查找要查找的 VPN 网关及其对等体。
- 步骤 4 选择全局视图中表示的对等体之一。
- 步骤 5 点击**查看详细信息**。
- 步骤 6 点击 VPN 隧道的另一端，CDO 将显示该连接的隧道详细信息、NAT 信息和密钥交换信息：
 - 隧道详细信息 - 显示有关隧道的名称和连接信息。点击刷新图标可更新隧道的连接信息。

- 特定于 AWS 连接的隧道详细信息 - AWS 站点到站点连接的隧道详细信息与其他连接略有不同。对于从 AWS VPC 到 VPN 网关的每个连接，AWS 会创建两个 VPN 隧道。这用于高可用性。
 - 隧道的名称代表您的 VPN 网关所连接的 VPC 的名称。隧道中指定的 IP 地址是您的 VPN 网关获知的 VPC 的 IP 地址。
 - 如果 CDO 连接状态显示为“活动”，则 AWS 隧道状态为“运行”。如果 CDO 连接状态为“非活动”，则 AWS 隧道状态为“关闭”。
- NAT 信息 - 显示正在使用的 NAT 规则类型、原始和转换后的数据包信息，并提供指向 NAT 表的链接以查看该隧道的 NAT 规则。（尚不可用于 AWS VPC 站点间 VPN。）
- 密钥交换 - 显示隧道和密钥交换问题正在使用的加密密钥。（尚不可用于 AWS VPC 站点间 VPN。）

隧道窗格

Tunnels 窗格显示与特定 VPN 网关关联的所有隧道的列表。对于 VPN 网关和 AWS VPC 之间的站点间 VPN 连接，隧道窗格显示从 VPN 网关到 VPC 的所有隧道。由于您的 VPN 网关和 AWS VPC 之间的每个站点间 VPN 连接都有两个隧道，因此您会看到通常用于其他设备的隧道数量的两倍。

VPN 网关详细信息

显示连接到 VPN 网关的对等体的数量以及 VPN 网关的 IP 地址。这仅在“VPN 隧道” (VPN Tunnels) 页面中可见。

对等体窗格

选择站点间 VPN 对等体后，对等体窗格将列出该对中的两台设备，并允许您点击其中一台设备的查看对等体。通过点击查看对等体，您可以看到与该设备关联的任何其他站点到站点对等体。这在“表”视图和“全局”视图中可见。

远程访问虚拟专用网络

远程访问虚拟专用网络 (RA VPN) 允许个人用户使用连接到互联网的计算机或其他受支持的 iOS 或 Android 设备，从远程位置连接到您的网络。这样，移动员工就可以从家庭网络或公共 Wi-Fi 网络进行连接。

RA VPN 配置包括以下组件：

- 连接配置文件：您可以创建远程访问 VPN 连接配置文件，允许用户在外部网络（例如其家庭网络）上时连接到您的内部网络。创建单独的配置文件，以适应不同的身份验证方法。连接配置文件由身份源和组策略组成。

相关信息：

-

- [为 FTD 配置远程访问 VPN](#)

监控远程访问虚拟专用网络会话

远程访问虚拟专用网络 (RA VPN) 为远程用户（如移动用户或远程工作者）提供安全连接。监控这些连接可以让连接和用户会话性能的重要指标变得一目了然。Cisco Defense Orchestrator (CDO) RA VPN 监控功能使您能够快速确定远程接入 VPN 问题是否存在及其存在的位置。然后，您可以应用这些知识并使用网络管理工具来减少或消除网络和用户问题。您还可以根据需要断开远程访问 VPN 会话。


“远程访问虚拟专用监控” (Remote Access Virtual Private Monitoring) 页面提供以下信息：

- 至少过去 90 天内的活动会话和历史会话列表。
- 显示直观的图形视觉效果，让 CDO 管理的所有活动 VPN 前端变得一目了然。
- 实时会话屏幕会显示 CDO 租户中最常用的操作系统和 VPN 连接配置文件。它还会显示平均会话持续时间以及上传和下载的数据。
- 过滤功能可根据设备类型、设备名称、会话长度以及传输和接收的数据量等条件来缩小搜索范围。

相关信息：

- [监控实时 AnyConnect RA VPN 会话, on page 218](#)
- [监控历史 AnyConnect RA VPN 会话, on page 220](#)
- [搜索和过滤 RA VPN 会话](#)
- [自定义 RA VPN 监控视图](#)
- [将 RA VPN 会话导出至 CSV 文件](#)
- [断开 FDM 管理 设备上的活动 RA VPN 会话](#)

监控实时 AnyConnect RA VPN 会话

您可以监控设备上活动 AnyConnect RA VPN 会话的实时数据。这些数据每 10 分钟会自动刷新一次。如果要随时检索最新的会话列表，请点击屏幕右上角显示的重新加载图标 。

开始之前

- 将 RA VPN 前端载入 CDO。
- 确保要监控实时数据的设备的连接状态在清单 (**Inventory**) 页面上为“在线” (Online)。

过程

步骤 1 在 CDO 导航窗格中，点击 **VPN > 远程访问 VPN 监控**。

或者，您可以点击 CDO 主页上的**查看活动远程访问 VPN 会话 (View Active Remote Access VPN Sessions)**，或导航至 **VPN > 远程访问 VPN (Remote Access VPN)** 并点击屏幕右上角的  图标。

步骤 2 点击 **RA VPN**。

步骤 3 点击**实时 (Live)**。

您可以**搜索和过滤 RA VPN 会话**以根据设备类型、会话长度以及上传和下载数据范围等条件来缩小搜索范围。

注释 **数据 TX 和数据 RX** 信息不适用于 FTD。

查看实时数据

实时数据以控制面板和表格形式显示。

面板视图

您必须点击屏幕右上角的**显示图表视图**图标才能查看控制面板。

控制面板提供 CDO 管理的所有活动 VPN 头端的概览视图。

- **明细 (所有设备)**：显示实时会话总数。它还显示了一个分为四个弧长的饼形图。它说明会话数最多的前三台设备的 VPN 会话百分比。剩余的弧长表示其他设备的总和。
- 显示 CDO 租户中最常用的操作系统和 VPN 连接配置文件。
- 显示平均会话持续时间以及上传和下载的数据。
- **按国家/地区排列的活动会话 (Active Sessions by Country)**：显示连接到 RA VPN 前端的用户的位置的交互式热度地图。
 - 用户已连接的国家/地区以逐渐变深的蓝色显示，具体取决于从该国家/地区建立的会话的相对比例 - 蓝色越深表示从该国家/地区建立的会话越多。
 - 地图底部的图例提供了一个比例，表示某个国家/地区的会话数与其所用蓝色阴影之间的相关性。
 - 将鼠标指针悬停在地图上，可查看国家/地区名称以及从该国家/地区建立的活动用户会话总数。
 - 将鼠标指针悬停在表格上，可在地图上看到国家/地区的位置和活动用户会话总数。

表格视图

点击屏幕右上角的**显示表格视图**图标，以表格格式查看数据。

表格形式提供当前连接的 VPN 用户的完整列表。

- **位置列**通过对公共 IP 地址进行地理定位来显示连接到 VPN 头端的所有用户的位置。点击一行可查看用户详细信息。点击左侧窗格中的位置链接时，用户的位置会显示在 Google 地图上。



重要事项 CDO 对实时数据应用标准过滤器，并在控制面板上显示这些数据。仅当显示表格数据时，才能应用新过滤器，因为可视化控制面板视图中不支持自定义过滤器。点击**清除**以删除已应用的所有过滤器。您无法删除标准过滤器。

您可以使用[搜索和过滤 RA VPN 会话](#)功能根据设备类型、会话长度以及上传和下载数据范围等条件来缩小搜索范围。请注意，一次最多可以显示 10,000 个结果。

状态列中带有**活动**标签的绿点表示活动 VPN 用户的会话。

监控历史 AnyConnect RA VPN 会话

您可以监控过去三个月内记录的 AnyConnect RA VPN 会话的历史数据。

开始之前

- 将 RA VPN 前端载入 CDO。

过程

步骤 1 在 CDO 导航窗格中，点击 **VPN > 远程访问 VPN 监控**。

或者，您可以点击 CDO 主页上的**查看活动远程访问 VPN 会话 (View Active Remote Access VPN Sessions)**，或导航至 **VPN > 远程访问 VPN (Remote Access VPN)** 并点击右上角的  图标。

步骤 2 点击 **RA VPN**。

步骤 3 点击**历史 (Historical)**。

CDO 会显示过去三个月内记录的 RA VPN 会话的历史数据。

您可以使用[搜索和过滤 RA VPN 会话](#)功能根据设备类型、会话长度以及上传和下载数据范围等条件来缩小搜索范围。

数据 TX 和**数据 RX** 信息不适用于 FTD。

查看历史数据

历史数据以控制面板和表格形式显示。

面板视图

您必须点击屏幕右上角的“显示图表视图”图标才能查看控制面板。您将看到控制面板视图和表格视图。

控制面板提供 CDO 管理的所有活动 VPN 头端的概览视图。它会提供一个条形图，以便显示过去 24 小时、7 天和 30 天内为所有设备记录的 VPN 会话。您可以从下拉列表中选择持续时间。您可以将鼠标悬停在各个条形上，以查看当天的日期和会话总数。

表格视图

您必须点击屏幕右上角显示的“显示表格视图”图标，才能仅查看表格视图。此表格提供了过去三个月内连接的 VPN 用户的完整列表。

“位置”列通过对公共 IP 地址进行地理定位来显示连接到 VPN 头端的所有用户的位置。点击一行可查看用户详细信息。点击左侧窗格中的位置链接时，用户的位置会显示在 Google 地图上。



重要事项 CDO 对历史数据应用标准过滤器，并将其显示在控制面板上。您只能在显示表格数据时应用新过滤器，因为自定义过滤器不支持控制面板。清除新应用的过滤器会重新启动控制面板（在屏幕上，点击清除可删除手动应用的过滤器）。您无法删除标准过滤器。

您可以使用[搜索和过滤 RA VPN 会话](#)功能根据会话日期和时间范围、会话长度以及上传和下载数据范围等条件来缩小搜索范围。请注意，一次最多可以显示 10,000 个结果。

状态列中带有活动标签的绿点表示活动 VPN 用户的会话。

搜索和过滤 RA VPN 会话

搜索


使用搜索栏功能查找 RA VPN 会话。开始在搜索栏中键入设备名称、IP 地址或序列号，系统将显示符合搜索条件的 RA VPN 会话。搜索不区分大小写。

过滤

使用过滤器边栏可根据会话时间范围、会话长度以及上传和下载数据范围等条件查找 RA VPN 会话。过滤功能可用于实时视图和历史视图。

- **按设备过滤 (Filter by Devices):** 从所有类型 (All Types) 选项卡中选择一个或所有设备以查看所选设备的会话。该窗口还会根据设备的类型来对它们进行分类，并在相应的选项卡下显示它们。
- **会话时间范围 (Sessions Time Range)**（仅适用于历史数据）：查看指定日期和时间范围内的历史会话。请注意，您可以查看过去三个月内记录的数据。
- **会话长度 (Sessions Length):** 根据指定会话的持续时间长度查看会话。设置时间单位（小时、分钟或秒），并通过移动滑块指定最小和最大持续时间。您还可以在提供的字段中指定长度。
- **上传 (TX) (Upload [TX]):** 根据上传或传输到安全网络的指定数据量查看会话。设置单位（GB、MB 或 KB），并通过相应地移动滑块来选择范围。您还可以在可用字段中指定值。
- **下载 (RX) (Download [RX]):** 根据从安全网络下载或接收的指定数据量查看会话。设置单位（GB、MB 或 KB），并通过相应地移动滑块来选择范围。您还可以在可用字段中指定值。

自定义 RA VPN 监控视图

您可以在实时和历史模式下修改 RA VPN 监控视图，以仅包含适用于所需视图的列标题。点击列右侧的列过滤器图标 ，然后选择或取消选择所需的列。

CDO 会在您下次登录 CDO 时记住您的选择。

将 RA VPN 会话导出至 CSV 文件

您可以将一个或多个设备的 RA VPN 会话导出至以逗号来分隔值的 (.csv) 文件。您可以在电子表格应用（例如 Microsoft Excel）中打开 .csv 文件，对列表中的项目进行排序和过滤。这些信息可帮助您分析 RA VPN 会话。每次导出会话时，CDO 都会创建一个新的 .csv 文件，其中创建的文件会在名称中包含日期和时间。


CDO 最多可以将 100,000 个活动会话导出至 CSV 文件。如果来自所有设备的会话总数超过最大限制，则可以使用按设备查看 (View By Device) 过滤器并为各个设备生成报告。

Procedure

步骤 1 在 CDO 导航窗格中，点击 **VPN > 远程访问 VPN 监控 (Remote Access VPN Monitoring)**。

步骤 2 在按设备查看 (View By Devices) 区域中，选择以下选项之一：

- 所有设备 (All Devices)，可从其下面列出的所有设备导出活动会话。
- 点击要导出其会话的设备。

步骤 3 点击右上角的  图标。CDO 会将您在屏幕上看到的规则导出至 .csv 文件。

步骤 4 在电子表格应用中打开 .csv 文件，对结果进行排序和过滤。

断开 FDM 管理 设备上的活动 RA VPN 会话

目前，无法使用 思科防御协调器 接口在 FDM 管理 设备上终止 RA VPN 会话。相反，您可以使用 SSH 连接到 威胁防御 CLI 并断开所需用户的连接。您可以在载入到 CDO 的在线 FDM 管理 设备上执行此任务。

Procedure

步骤 1 登录到 防火墙设备管理器 并使用设备 CLI，如运行设备版本的《[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#)》的“入门”一章的[登录命令行接口 \(CLI\)](#) 部分所述。

步骤 2 执行 `vpn-sessionsdb logoff {name}` 命令并将 **name** 替换为用户名。此命令将终止您指定的用户名的所有会话。

为 FTD 配置远程访问 VPN

CDO 提供直观的用户界面，用于配置新的远程访问虚拟专用网络 (RA VPN)。它还允许您快速轻松地配置 CDO 中的多个设备 RA VPN 连接。FDM 管理 AnyConnect 是终端设备上通过 RA VPN 连接 FDM 管理设备的唯一受支持客户端。

AnyConnect 客户端与 FDM 管理设备协商 SSL VPN 连接时，会使用传输层安全 (TLS) 或数据报传输层安全 (DTLS) 进行连接。DTLS 可避免与某些 SSL 连接关联的延迟和带宽问题，并可提高对于数据包延迟敏感的实时应用的性能。客户端与 FDM 管理设备协商要使用的 TLS/DTLS 版本。如果客户端支持 DTLS，则使用 DTLS。

CDO 支持 FDM 管理设备上的 RA VPN 功能的以下方面：

- 基于 SSL 客户端的远程访问
- IPv4 和 IPv6 寻址
- 跨多台 FDM 管理设备共享 RA VPN 配置



Important

如果自行激活的设备（在软件版本 6.7 或更高版本上运行）包含使用 SAML 服务器作为身份验证源的 RA VPN 配置，则 CDO 不会在连接配置文件中填充 AAA 详细信息，因为它不管理当前版本中的 SAML 服务器对象。FDM 管理因此，您无法从 CDO 管理此类 RA VPN 配置。但是，CDO 会读取 RA VPN 连接配置文件以及关联的受信任 CA 证书和 SAML 服务器对象。

相关信息：

- [使用 RADIUS 和组策略控制用户权限和属性](#)
- [FDM 管理设备的端到端远程接入 VPN 配置过程](#)
 - [下载 AnyConnect 客户端软件包](#)
 - [将 AnyConnect 软件包上传到运行版本 6.4.0 的 FDM 管理设备](#)
 - [将 AnyConnect 软件包上传到运行 FTD 6.5 或更高版本的设备](#) [将 AnyConnect 软件包上传到运行 FDM 管理 6.5 或更高版本的设备](#)
 - [上传 RA AnyConnect 客户端配置文件, on page 269](#)
 - [为 FDM 管理设备配置身份源](#)
 - [创建或编辑 Active Directory 领域对象](#)
 - [创建或编辑 RADIUS 服务器对象或组](#)
 - [创建新的 RA VPN 组策略](#)
 - [创建 RA VPN 配置](#)
 - [配置 RA VPN 连接配置文件](#)
 - [允许流量通过远程访问 VPN](#)

- 在运行版本 6.4.0 的 FDM 管理设备上升级 AnyConnect 软件包
- FDM 管理设备的远程访问 VPN 准则和限制
- 用户如何在 FDM 管理设备上安装 AnyConnect 客户端软件
- 远程访问 VPN 的许可要求
- 各设备型号的最大并发 VPN 会话数量
- RADIUS 授权更改
 - 在 FTD 设备上配置授权更改
- RA VPN 用户的拆分隧道 (Hair Pinning)
- 验证 FDM 管理设备的远程接入 VPN 配置
- 查看设备的远程接入 VPN 配置详细信息FDM 管理

RA VPN 用户的拆分隧道 (Hair Pinning)

本文介绍 RA VPN 的分割隧道。

典型地，在远程接入 VPN 中，您可能希望 VPN 用户通过您的设备访问互联网。但是，您可以允许 VPN 用户在连接到 RA VPN 时访问外部网络。这种技术有时候称为分割隧道或发夹方法。拆分隧道不仅允许 VPN 通过安全隧道连接到远程网络，而且允许连接到 VPN 隧道外的网络。拆分隧道可减少 FTD 设备上的网络负载，并增加外部接口上的带宽。

要配置拆分隧道列表，必须创建标准访问列表或扩展访问列表。按照您的设备版本的《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》中的“虚拟专用网络 (VPN)”一章的如何在外部接口上为远程访问 VPN 用户提供互联网访问部分中所述的说明操作正在运行。

使用 RADIUS 和组策略控制用户权限和属性

本文提供有关从外部 RADIUS 服务器或组策略将属性应用于 RA VPN 连接的信息。

您可以将用户授权属性（也称为用户权利或权限）应用于来自外部 RADIUS 服务器或 FTD 设备上定义的组策略的 RA VPN 连接。如果 FTD 设备从与组策略上配置的属性冲突的外部 AAA 服务器接收属性，则来自 AAA 服务器的属性始终优先。

FTD 设备按照以下顺序应用属性：

Procedure

- 步骤 1** 外部 AAA 服务器上的用户属性 - 该服务器在用户身份验证或授权成功后返回这些属性。
- 步骤 2** 在 FTD 设备上配置的组策略 - 如果 RADIUS 服务器为用户返回 RADIUS CLASS 属性 IETF-Class-25 (OU=group-policy) 值，FTD 设备会将该用户放在名称相同的组策略中，并实施组策略中该服务器未返回的所有属性。

步骤 3 连接配置文件分配的组策略 - 连接配置文件包含该连接的初步设置，包括在进行身份验证前应用于用户的默认组策略。连接至 FTD 设备的所有用户最初都属于此组，这可以提供 AAA 服务器返回的用户属性或分配给用户的组策略中缺失的所有属性。

FTD 设备支持供应商 ID 为 3076 的 RADIUS 属性。如果使用的 RADIUS 服务器没有定义这些属性，您必须手动定义它们。要定义属性，请使用属性名称或编号、类型、值和供应商代码 (3076)。

以下主题根据属性值是在 RADIUS 服务器中定义的还是由系统发送到 RADIUS 服务器的来介绍受支持的属性。

发送到 RADIUS 服务器的属性

RADIUS 属性 146 和 150 由 FDM 管理 发送到 RADIUS 服务器，用于身份验证请求和授权请求。以下所有属性都是由 FDM 管理设备发送到 RADIUS 服务器，用于记账开始请求、临时更新请求和停止请求。

Table 6: 发送到 RADIUS 的属性 *Secure Firewall Threat Defense*

属性	属性	语法、类型	单值或多值	说明或值
客户端类型	150	整数	单值	连接到 VPN 的客户端类型： 2 = AnyConnect 客户端 SSL VPN
会话类型	151	整数	单值	连接类型： 1 = AnyConnect 客户端 SSL VPN
隧道组名称	146	字符串	单值	用于建立会话的连接配置文件名称，如 FDM 管理设备上的定义。此名称可以包含 1-253 个字符。

从 RADIUS 服务器接收的属性

以下用户授权属性由 RADIUS 服务器发送到 FDM 管理设备。

属性	属性编号	语法、类型	单值或多值	说明或值
Access-List-Inbound	86	字符串	单值	这两个访问列表属性都使用 FDM 管理设备上配置的 ACL 名称。使用 Smart CLI 扩展访问列表对象类型在防火墙设备管理器中创建 ACL（登录防火墙设备管理器并选择设备 (Device) > 高级配置 (Advanced Configuration) > Smart CLI > 对象 (Objects) ）。此类 ACL 用于控制进站流量（流量进入 FDM 管理设备）或出站流量（流量离开 FDM 管理设备）。
Access-List-Outbound	87	字符串	单值	
Address-Pools	217	字符串	单值	FDM 管理设备上定义的网络对象名称，用于识别将作为地址池供客户端连接 RA VPN 时使用的子网。在对象 (Objects) 页面上定义网络对象。
Banner1	15	字符串	单值	用户登录时显示的横幅。
Banner2	36	字符串	单值	用户登录时显示的横幅的第二部分。横幅 2 附加到横幅 1。

属性	属性编号	语法、类型	单值或多值	说明或值
Group-Policy	25	字符串	单值	要在连接中使用的组策略。必须在 RA VPN 组策略 (Group Policy) 页面上创建组策略。您可以使用以下其中一种格式： <ul style="list-style-type: none"> • 组策略名称 • OU = 组策略名称 • OU = 组策略名称；
Simultaneous-Logins	2	整数	单值	用户可以建立的独立并发连接的数量，0 - 2147483647。
VLAN	140	整数	单值	限制用户连接的 VLAN，0 - 4094。还必须在 FDM 管理设备的子接口上配置此 VLAN。

双因素身份验证

可以为 RA VPN 配置双因素身份验证。配置了双因素身份验证时，用户必须提供用户名、静态密码，以及一个额外项，如 Duo 密码等。双因素身份验证不同于使用第二个身份验证源，双因素是在单个身份验证源中配置的，其与 Duo 服务器的关系绑定到主身份验证源。例外情况是 Duo LDAP，它将“Duo LDAP 服务器”配置为辅助身份验证源。

- 使用 RADIUS 的 Duo 双因素身份验证，第 227 页
- 使用 LDAP 的 Duo 双因素身份验证，第 232 页

使用 RADIUS 的 Duo 双因素身份验证

可以将 Duo RADIUS 服务器配置为主要身份验证源。此方法使用 Duo RADIUS 身份验证代理。

有关配置 Duo 的详细步骤，请参阅 <https://duo.com/docs/cisco-firepower>。

然后，配置 Duo，以转发定向到代理服务器的身份验证请求，并将另一台 RADIUS 服务器或 Microsoft Active Directory(AD) 服务器用作第一个身份验证因素，将 Duo 云服务用作第二个因素。

使用此方法时，用户必须使用 Duo 身份验证代理和关联的 RADIUS/AD 服务器上配置的用户名，以及 RADIUS/AD 服务器中配置的用户名对应的密码进行身份验证，其后紧随以下其中一个 Duo 代码：

Duo-passcode。例如，*my-password,12345*。

push。例如，*my-password,push*。使用 **push** 告知 Duo 向用户应该已经安装并注册的 Duo 移动应用发送推送身份验证。

sms。例如，*my-password,sms*。使用 **sms** 告知 Duo 向用户的移动设备发送包含新一批密码的 SMS 消息。使用 **sms** 时，用户的身份验证尝试将会失败。用户必须重新进行身份验证，并输入新密码作为辅助因素。

phone。例如，*my-password,phone*。使用 **phone** 告知 Duo 执行电话回叫身份验证。

如果用户名和密码已经过验证，Duo 身份验证代理会联系 Duo 云服务，后者将核实该请求是来自有效配置的代理设备，然后按照指示将临时密码推送到用户的移动设备。当用户接受此密码时，Duo 会将会话标记为已验证，同时 RA VPN 成功创建。

有关详细说明，请参阅[如何使用 Duo RADIUS 配置双因素身份验证](#)，第 228 页

如何使用 Duo RADIUS 配置双因素身份验证

可以将 Duo RADIUS 服务器配置为主要身份验证源。此方法使用 Duo RADIUS 身份验证代理。

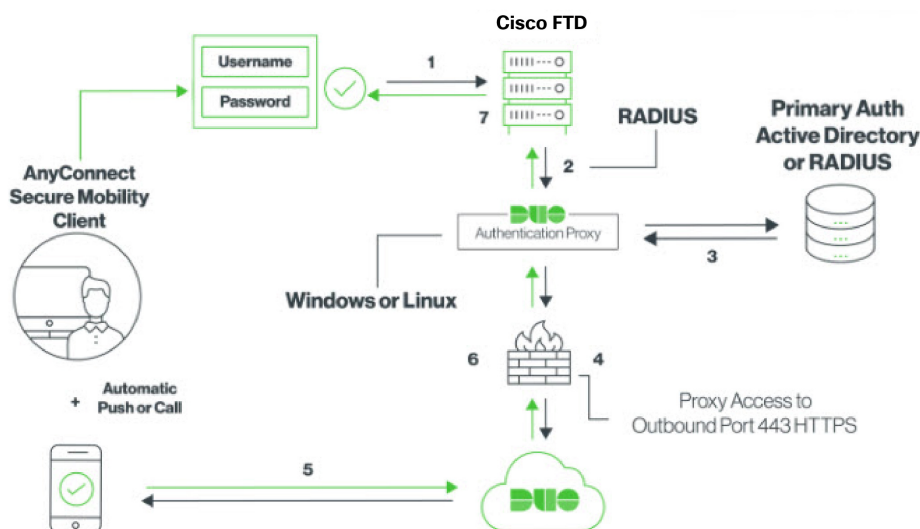
然后，配置 Duo，以转发定向到代理服务器的身份验证请求，并将另一台 RADIUS 服务器或 AD 服务器用作第一个身份验证因素，将 Duo 云服务用作第二个因素。

以下主题详细说明这种类型的高级配置：

- [Duo RADIUS 辅助身份验证系统流程](#)，第 228 页
- [使用 CDO 为 Duo RADIUS 配置设备](#)，第 229 页

Duo RADIUS 辅助身份验证系统流程

以下是系统流程的说明：



1. 用户与设备建立远程接入 VPN 连接，并提供与 RADIUS/AD 服务器关联的用户名、RADIUS/AD 服务器中配置的用户名的密码，后跟其中一个 DUO 代码 Duo-password、push、SMS、或电话。FDM 管理有关更多信息，使用 [RADIUS 的 Duo 双因素身份验证](#)，第 227 页
2. FDM 管理 设备将身份验证请求发送到 Duo 身份验证代理。
3. Duo Authentication 代理使用主身份验证服务器（可能是 Active Directory 或 RADIUS）对此主要身份验证尝试进行身份验证。
4. 如果凭证已通过身份验证，则会通过 TCP 端口 443 与 Duo Security 建立 Duo 身份验证代理连接。
5. 然后，通过推送通知、带密码的短信消息或电话呼叫单独对用户进行身份验证。用户必须成功完成此身份验证。
6. Duo 身份验证代理接收身份验证响应。
7. 如果辅助身份验证成功，则 FDM 管理 设备会与用户的 AnyConnect 客户端建立远程接入 VPN 连接。

配置 Duo RADIUS 辅助身份验证

Duo Authentication 代理使用主身份验证服务器（可能是 Active Directory 或 RADIUS）对此主要身份验证尝试进行身份验证。

创建 Duo 账户

创建 Duo 账户并获取集成密钥、密钥和 API 主机名。

以下是对此过程的概述。有关详细信息，请参阅 [Duo 网站](#)。

过程

-
- 步骤 1 [注册 Duo 账户](#)。
 - 步骤 2 登录到 [Duo 管理面板 \(Duo Admin Panel\)](#) 并导航至应用 (**Applications**)。
 - 步骤 3 点击保护应用 (**Protect an Application**) 并在应用列表中找到 **Cisco Firepower Threat Defense VPN**。
 - 步骤 4 点击保护此应用 (**Protect this Application**) 以获取您的集成密钥、密钥和 API 主机名。配置代理时，您将需要此信息。如需帮助，请参阅《*Duo 入门指南*》<https://duo.com/docs/getting-started>。
 - 步骤 5 安装和配置 Duo 身份验证代理。有关说明，请参阅中的“安装 Duo 身份验证代理”部分。<https://duo.com/docs/cisco-firepower>
 - 步骤 6 启动身份验证代理。有关说明，请参阅中的“启动代理”部分。<https://duo.com/docs/cisco-firepower>
有关在 Duo 中注册新用户的信息，请参阅 <https://duo.com/docs/enrolling-users>。<https://duo.com/docs/enrolling-users>
-

使用 CDO 为 Duo RADIUS 配置设备

过程

步骤 1 配置 FTD Radius 服务器对象。

- a) 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
- b) 点击 **> RA VPN 对象 (ASA 和 FTD) > 身份源** 
- c) 提供名称并将设备类型设置为 FTD。
- d) 选择 Radius 服务器组，然后点击继续。有关详细信息，请参阅中的步骤 6。[创建 RADIUS 服务器组，第 251 页](#)
- e) 在 Radius Server 部分，点击 Add 按钮，然后点击 Create New Radius Server。请参阅[创建 RADIUS 服务器对象，第 250 页](#)

在服务器名称或 IP 地址字段中，输入 Duo 身份验证代理服务器的完全限定主机名或 IP 地址。

Adding FTD RADIUS Server ✕

Object Name Device Type

DuoRadiusServerObject FTD

Description

Object description

1 Identity Source Type **RADIUS Server**

2 Edit Identity Source

Server Name or IP Address	Authentication Port
10.1.10.101	1812
Timeout (seconds) ⓘ	
10	
1 - 300	
Server Secret Key	
....	

RA VPN Only (if this object is used in RA VPN Configuration)

Cancel Add

- f) 将 Duo RADIUS 服务器添加到组后，点击添加以创建新的 Duo RADIUS 服务器组。

步骤 2 将远程接入 VPN 身份验证方法更改为 Duo RADIUS。

- 在 CDO 导航菜单中，点击 VPN > 远程接入 VPN 配置。
- 展开 VPN 配置，然后点击要向其添加 Duo 的连接配置文件。
- 在右侧的操作 (Actions) 窗格中，点击编辑 (Edit)。
- 身份验证类型 (Authentication Type) 可以选择 AAA 或 AAA 和客户端证书 (AAA and Client Certificate)。
- 在“用户身份验证的主身份源” (Primary Identity Source for User Authentication) 列表中，选择您之前创建的服务器组。

- 您通常不需要选择“授权服务器”或“审计服务器”。
- 点击继续 (Continue)。
- 在摘要和说明步骤中，点击完成以保存配置。

步骤 3 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

使用 LDAP 的 Duo 双因素身份验证

您可以将 Duo LDAP 服务器作为辅助身份验证源与作为主要源的 Microsoft Active Directory (AD) 或 RADIUS 服务器结合使用。使用 Duo LDAP 时，辅助身份验证使用 Duo 密码、推送通知或电话呼叫验证主要身份验证。



注释 Duo 双因素身份验证功能在 CDO 中适用于运行 Firepower 威胁版本 6.5 或更高版本的设备。[升级单个 FTD 设备](#)

FTD 设备使用通过端口 TCP/636 的 LDAPS 与 Duo LDAP 通信。

使用此方法时，用户必须使用 AD/RADIUS 服务器和 Duo LDAP 服务器上配置的用户名进行身份验证。系统提示通过 AnyConnect 登录时，用户应在主密码字段中提供 AD/RADIUS 密码，对于辅助密码，可以提供以下选项之一来使用 Duo 进行身份验证。有关更多详细信息，请参阅中的“用于选择因素的第二个密码”部分。<https://guide.duo.com/anyconnect>

- **Duo 密码** - 使用密码进行身份验证，密码将由 Duo Mobile 生成、通过 SMS 发送、由硬件令牌生成或由管理员提供。例如，1234567。
- **推送** - 如果已安装并激活 Duo Mobile 应用，请将登录请求推送至您的手机。查看请求并点击批准以登录。
- **电话** - 使用电话呼叫进行身份验证。
- **短信** - 以短信消息请求 Duo 密码。登录尝试失败。使用新密码重新登录。

有关详细说明，请参阅[如何使用 Duo LDAP 配置双因素身份验证](#)，第 232 页。

如何使用 Duo LDAP 配置双因素身份验证

您可以将 Duo LDAP 服务器作为辅助身份验证源与作为主要源的 Microsoft Active Directory (AD) 或 RADIUS 服务器结合使用。使用 Duo LDAP 时，辅助身份验证使用 Duo 密码、推送通知或电话呼叫验证主要身份验证。

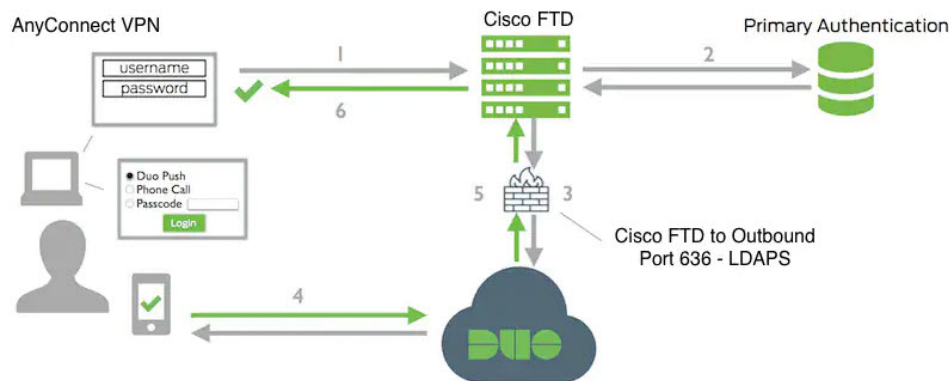
以下主题详细说明这种类型的高级配置：

- [Duo LDAP 辅助身份验证系统流程](#)，第 232 页
- [配置 Duo LDAP 辅助身份验证](#)，第 233 页

Duo LDAP 辅助身份验证系统流程

下图显示的是 威胁防御 如何和 Duo 共同发挥作用，以使用 LDAP 提供双因素身份验证。

以下是系统流程的说明：



1. 用户对 FDM 管理 设备进行远程访问 VPN 连接，并提供用户名和密码。
2. FDM 管理 设备使用主身份验证服务器（可能是 Active Directory 或 RADIUS）对此主要身份验证尝试进行身份验证。
3. 如果主身份验证正常工作， FDM 管理 设备会将辅助身份验证请求发送至 Duo LDAP 服务器。
4. 然后，通过推送通知、带密码的短信消息或电话呼叫单独对用户进行身份验证。用户必须成功完成此身份验证。
5. Duo 响应 FDM 管理 设备，以指示用户是否已成功进行身份验证。
6. 如果辅助身份验证成功，则 FDM 管理 设备会与用户的 AnyConnect 客户端建立远程接入 VPN 连接。

配置 Duo LDAP 辅助身份验证

以下操作步骤介绍配置双因素身份验证的端到端过程，使用 Duo LDAP 作为辅助身份验证源，用于远程访问 VPN。您必须拥有一个 Duo 账户，并从 Duo 获取一些信息，才能完成此配置。

创建 Duo 账户

创建 Duo 账户并获取集成密钥、密钥和 API 主机名。

以下是对此过程的概述。有关详细信息，请参阅 Duo 网站。

过程

步骤 1 注册 Duo 账户。

步骤 2 登录到 Duo 管理面板 (Duo Admin Panel) 并导航至应用 (Applications)。

步骤 3 点击保护应用 (Protect an Application) 并在应用列表中找到 Cisco Firepower Threat Defense VPN。

步骤 4 点击保护此应用 (Protect this Application) 以获取您的集成密钥、密钥和 API 主机名。如需帮助，请参阅《Duo 入门指南》<https://duo.com/docs/getting-started>。

有关在 Duo 中注册新用户的信息，请参阅 <https://duo.com/docs/enrolling-users>。 <https://duo.com/docs/enrolling-users>

将受信任的 CA 证书上传到设备 FDM 管理


FDM 管理设备必须具有验证与 Duo LDAP 服务器的连接所需的可信 CA 证书。您可以直接转至 <https://www.digicert.com/digicert-root-certificates.htm> 并下载 **DigiCertSHA2HighAssuranceServerCA** 或 **DigiCert High Assurance EV Root CA**，然后使用 防火墙设备管理器 (FDM) 将其上传。

过程

- 步骤 1 访问 FDM 管理设备的 防火墙设备管理器 页面，选择 **对象 (Objects) > 证书 (Certificates)**。
 - 步骤 2 点击 **+ > 添加受信任 CA 证书 (Add Trusted CA Certificate)**。
 - 步骤 3 输入证书名称，例如，`DigiCert_High_Assurance_EV_Root_CA`。（不允许使用空格。）
 - 步骤 4 点击 **上传证书 (Upload Certificate)**，然后选择下载的文件。
 - 步骤 5 点击 **确定 (OK)**。
 - 步骤 6 如果尚未将设备载入 思科防御协调器，请将其载入。
 - 步骤 7 [读取所有设备配置](#)。
-

在 CDO 中为 Duo LDAP 配置 FTD

过程

- 步骤 1 创建用于 Duo LDAP 服务器的 Duo LDAP 身份源对象。
 - a) 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
 - b) 点击  以创建一个对象 **> RA VPN 对象 (ASA & FTD) (RA VPN Objects [ASA & FTD]) > 身份源 (Identity Source)**。
 - c) 为对象输入一个名称，例如 `Duo-LDAP-server`。
 - d) 选择设备类型作为 **FTD**。

e) 点击 **Duo LDAP 身份源**，然后点击 **Continue**。

f) 在编辑身份源区域中，提供以下详细信息：

- **API 主机名 (API Hostname)**: 请输入您从 Duo 账户中获取的 API 主机名。主机名应如下所示，X 替换为您的唯一值：API-XXXXXXXXX.DUOSEcurity.COM。无需大写。
- **端口 (Port)**: 请输入用于 LDAPS 的 TCP 端口。这应该是 636，除非 Duo 通知您使用不同端口。请注意，必须确保访问控制列表允许通过此端口流向 Duo LDAP 服务器的流量。
- **超时 (Timeout)**: 请输入连接到 Duo 服务器所采用的超时时间（以秒为单位）。值可以是 1-300 秒。默认值为 120。要使用默认值，请输入 120 或删除该属性行。
- **集成密钥 (Integration Key)**: 请输入从您的 Duo 账户获取的集成密钥。
- **密钥 (Secret Key)**: 输入从您的 Duo 账户获取的密钥。此密钥随后将被屏蔽。
- **用于连接到 Duo 服务器的接口**: 选择用于连接到 Duo 服务器的接口。
 - **通过路由查找解析**: 选择此选项可使用路由表查找正确的路径。有关创建路由表的信息，请参阅路由。
 - **手动选择接口**: 选择此选项并从列表选择一个接口。默认接口为诊断接口，但此操作仅当在接口上配置 IP 地址时有效。注意：确保所选接口存在于要连接到 Duo Server 的同一设备上。
- 点击添加 (**Add**)。

步骤 2（可选）使用 AnyConnect 配置文件编辑器创建配置文件，将身份验证超时值指定为 60 秒或更长时间。

需要为用户提供额外的时间来获取 Duo 密码并完成辅助身份验证。我们建议将此时间设置为至少 60 秒。以下操作步骤介绍如何仅配置身份验证超时，然后将配置文件上传至 FDM 管理设备。如果要更改其他设置，现在就可以进行更改。

- a) 如果尚未执行此操作，请下载并安装 AnyConnect 配置文件编辑器软件包。可以在思科软件中心 (software.cisco.com) 相应 AnyConnect 版本文件夹内找到此软件包。截至我们编制本文件时，基本路径是下载主页 (**Downloads Home**) > **安全 (Security)** > **VPN 和终端安全客户端 (VPN and Endpoint Security Clients)** > **思科 VPN 客户端 (Cisco VPN Clients)** > **AnyConnect 安全移动客户端 (AnyConnect Secure Mobility Client)**。
- b) 打开 AnyConnect VPN 配置文件编辑器。
- c) 在目录中选择首选项 (第 2 部分)，滚动至页面末尾，并将身份验证超时更改为 60 (或更大值)。以下是来自 AnyConnect 4.7 VPN 配置文件编辑器的图像；先前或后续版本可能不同。
- d) 选择文件 (**File**) > 保存 (**Save**)，将配置文件 XML 文件保存至您的工作站，并使用适当名称 (例如，duo-ldap-profile.xml)。
- e) 现在，可以关闭 VPN 配置文件编辑器应用。
- f) 在 CDO 中，[上传 RA AnyConnect 客户端配置文件](#)。

步骤 3 创建组策略，并在策略中选择 AnyConnect 配置文件。

分配给用户的组策略控制连接的许多方面。以下操作步骤介绍如何将配置文件 XML 文件分配到组。有关详细信息，请参阅[创建新的 RA VPN 组策略](#)。

- a) 在左侧的 CDO 导航栏中，点击 **对象 (Objects)** > **FDM 对象 (FDM Objects)**。
- b) 要编辑现有组策略，请使用 **RA VPN 组策略** 过滤器仅查看现有组策略，修改所需的策略并保存。
- c) 要创建新的组策略，请点击 **RA VPN 对象 (ASA 和 FTD) (RA VPN Objects [ASA & FTD])** > **RA VPN 组策略 (RA VPN Group Policy)**。
- d) 在常规 (**General**) 页面上，配置以下属性：
 - **名称 (Name)** - 对于新的配置文件，请输入名称。例如，Duo-LDAP-group。
 - **AnyConnect 客户端配置文件 (AnyConnect Client Profiles)** - 选择您创建的 AnyConnect 客户端配置文件对象。
- e) 点击添加 (**Add**) 以保存对象。
- f) 点击 **VPN** > **远程访问 VPN 配置 (Remote Access VPN Configuration)**。
- g) 点击要更新的远程接入 VPN 配置。
- h) 在右侧的操作窗格中，点击**组策略**。
- i) 点击 + 选择要与 VPN 配置关联的组策略。
- j) 点击**保存**以保存组策略。

步骤 4 创建或编辑用于 Duo-LDAP 辅助身份验证的远程访问 VPN 连接配置文件。

以下操作过程仅介绍将 Duo-LDAP 启用为辅助身份验证源并应用 AnyConnect 客户端配置文件所需执行的密钥更改。对于新连接配置文件，必须配置其余必填字段。对于此操作过程，我们假设您正在编辑现有连接配置文件，而且您必须更改这两个设置。

- a) 在 CDO 导航页面上，点击 **VPN** > **远程接入 VPN 配置**。

- b) 展开远程接入 VPN 配置，然后点击要更新的连接配置文件。
- c) 在右侧的操作 (**Actions**) 窗格中，点击**编辑 (Edit)**。
- d) 在主身份源 (**Primary Identity Source**) 下，配置以下内容：
 - **身份验证类型 (Authentication Type)** - 选择“仅 AAA” (AAA Only) 或“AAA 和客户端证书” (AAA and Client Certificate)。除非使用 AAA，否则无法配置双因素身份验证。
 - **用于用户身份验证的主要身份源 (Primary Identity Source for User Authentication)** - 选择主 Active Directory 或 RADIUS 服务器。请注意，可以选择一个 Duo-LDAP 身份源作为主要源。然而，Duo-LDAP 仅提供身份验证服务，而不提供身份服务，因此，如果将其作为主要身份验证源，则在任何控制面板中都将看不到与 RA VPN 连接关联的用户名，且将无法为这些用户编写访问控制规则。（如有需要，可将回退配置为本地身份源。）
 - **辅助身份源 (Secondary Identity Source)** - 选择 Duo-LDAP 身份源。

注释 如果主身份源和辅助身份源中的用户名相同，我们建议在连接配置文件的高级选项中启用**使用主用户名进行辅助登录**。通过这种方式配置，最终用户可以将单个用户名同时用于主要和辅助身份源。

- e) 点击**继续 (Continue)**。
- f) 在**组策略 (Group Policy)** 页面中，选择您创建或编辑的组策略。

- g) 点击**继续 (Continue)**。
- h) 点击**完成 (Done)**，将更改保存至连接配置文件。

步骤 5 预览和部署所有设备的配置更改，第 332 页。

FDM 管理设备的端到端远程接入 VPN 配置过程

本节提供在载入到CDO的FDM 管理设备上配置远程访问虚拟专用网络 (RA VPN) 的端到端程序。

要为客户端启用远程访问 VPN，需要配置多个单独的项目。以下程序介绍了端到端流程。

Procedure

步骤 1 启用两个许可证。

- 注册设备时，必须使用为受到出口管制的功能启用的智能软件管理器帐户执行此操作。许可证必须符合出口控制要求，然后才能配置远程访问 VPN。您也不能使用评估许可证配置该功能。您购买的 FDM 管理设备会自动附带许可证。许可证涵盖可选许可证未覆盖的所有功能。它是一种永久许可证。设备必须注册到 Firepower 设备管理器。请参阅《思科 Firepower Threat Defense 配置指南》的“许可系统”一章中的注册设备部分，了解您的设备正在运行的版本。
- 许可证。有关详细信息，请参阅[远程访问 VPN 的许可要求](#)。
 - 要启用许可证，请参阅《配置指南》的“许可系统”一章中的启用或禁用可选许可证部分。

步骤 2 配置证书。

对客户端与设备之间的 SSL 连接进行身份验证需要使用证书。您可以将预定义的 DefaultInternalCertificate 用于 VPN，也可以自行创建证书。

如果对用于身份验证的目录领域使用加密连接，则必须上传受信任的 CA 证书。有关证书及其上传方法的详细信息，请参阅[配置证书](#)。

步骤 3 配置用于对远程用户进行身份验证的身份源。

您可以使用以下来源对尝试使用 RA VPN 连接到您的网络的用户进行身份验证。此外，可以使用客户端证书进行身份验证，可单独使用，也可与身份源配合使用。

- Active Directory 身份领域：作为主要身份验证源。在 Active Directory AD 服务器中定义用户帐户。请参阅“配置 AD 身份领域”。请参阅[创建或编辑 Active Directory 领域对象](#)。
- RADIUS 服务器组：充当主要或辅助身份验证源，并用于授权和记账。请参阅[创建或编辑 RADIUS 服务器对象或组](#)。
- 本地身份源（本地用户数据库）：作为主要或回退源。您可以直接在设备上定义用户，不使用外部服务器。如果您使用本地数据库作为回退源，请确保您定义与外部服务器中描述的相同用户名/密码。

Note 您只能直接在 FDM 管理设备上从 Firepower 设备管理器中创建用户帐户。请参阅[配置本地用户](#)。

步骤 4（可选。）创建新的 RA VPN 组策略。

组策略定义用户相关的属性。可以配置组策略，根据组成员身份提供差异化的资源访问权限。或者，可以对所有连接使用默认策略。

步骤 5 创建 RA VPN 配置。

步骤 6 配置 RA VPN 连接配置文件。

步骤 7 预览和部署所有设备的配置更改。

步骤 8 允许流量通过远程访问 VPN。

步骤 9 (可选。) 启用身份策略并配置被动身份验证规则。如果启用被动用户验证，通过远程访问 VPN 登录的用户将显示在控制面板上，他们也可以用作策略中的流量匹配条件。如果不启用被动身份验证，只有当远程访问 VPN 用户匹配主动身份验证策略时，这些用户才可用。必须启用身份策略以在控制面板中获取任何用户名信息，或将其用于流量匹配。请参阅[配置身份策略](#)。



Important 如果使用本地管理器（如 Firepower 设备管理器）更改远程访问 VPN 配置，CDO 中该设备的配置状态 (**Configuration Status**) 将显示“检测到冲突” (Conflict Detected)。请参阅[设备上的带外更改](#)。您可以[解决配置冲突](#)。

What to do next

将 RA VPN 配置下载到设备后，用户可以使用连接到互联网的计算机或其他受支持的 iOS 或 Android 设备从远程位置连接到您的网络。FDM 管理您可以从租户中所有已自行激活的 RA VPN 前端监控实时 AnyConnect 远程访问虚拟专用网络 (RA VPN) 会话。请参阅[监控远程访问虚拟专用网络会话](#)。

下载 AnyConnect 客户端软件包

在配置远程接入 VPN 之前，必须将 AnyConnect 软件包从 <https://software.cisco.com/download/home/283000185> 下载到您的工作站。确保为所需的操作系统下载“AnyConnect 前端部署软件包”。稍后，您可以在定义 VPN 时将软件包上传到 Firepower 威胁防御 (FTD) 设备。

始终下载最新的 AnyConnect 版本，以确保获得最新的功能、漏洞修复和安全补丁。请定期更新设备上的软件包。



Note 您可以为以下每个操作系统 (OS) 上传一个 AnyConnect 软件包：Windows、Mac 和 Linux。无法为特定操作系统类型上传多个版本。

将 AnyConnect 软件包上传到运行版本 6.4.0 的 FDM 管理设备

您可以使用 防火墙设备管理器 API 资源管理器将 AnyConnect 软件包上传到 FDM 管理设备版本 6.4.0。设备上必须至少有一个 AnyConnect 软件包才能创建 RA VPN 连接。

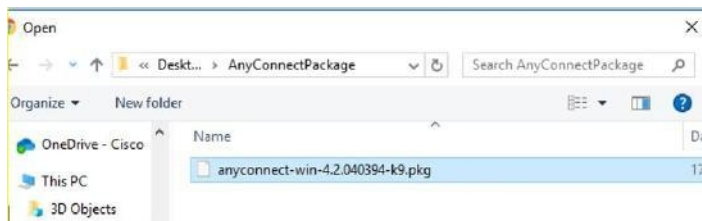


Important 该程序仅适用于 防火墙设备管理器 版本 6.4。如果您使用的是 防火墙设备管理器 版本 6.5 或更高版本，请使用 思科防御协调器 界面来将 [AnyConnect 软件包](#) 上传到运行 [FDM 管理 6.5 或更高版本](#) 的设备。

使用以下程序将 AnyConnect 软件包上传到 防火墙设备管理器 版本 6.4.0:

Procedure

- 步骤 1** 从 <https://software.cisco.com/download/home/283000185> 下载 AnyConnect 软件包。
- 确保您接受 EULA 并具有 K9（加密映像）权限。
 - 为您的操作系统选择“AnyConnect 前端部署软件包”。软件包名称类似于“anyconnect-win-4.7.04056-webdeploy-k9.pkg”。Windows、macOS 和 Linux 有单独的前端 Web 部署软件包。
- 步骤 2** 使用浏览器打开系统主页。例如，<https://ftd.example.com>。
- 步骤 3** 登录至 防火墙设备管理器。
- 步骤 4** 编辑 URL，使其指向 `/#/api-explorer`，例如 <https://ftd.example.com/#/api-explorer>。
- 步骤 5** 向下滚动并点击 Upload /action/uploaddiskfile。 >
- 步骤 6** 在 fileToUpload 字段中，点击 Choose File 并选择所需的 AnyConnect 软件包。您可以一次上传一个软件包。



- 步骤 7** 点击打开 (Open)。
- 步骤 8** 向下滚动并点击试用! (TRY IT OUT!)。等待数据包完全上传。在响应正文中，API 响应按以下格式显示。
- ```
{ "version": null, "name": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
 "fileName": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
 "id": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
 "type": "fileuploadstatus",
 "links": {
 "self":
 "https://ftd.example.com:972/api/fdm/...90d111e9-a361-%20cf32937ce0df.pkg"
 }
}
```
- 记录响应中的软件包的 fileName，因为在执行 POST 操作时必须输入相同的字符串。在本例中，fileName 为 691f47e1-90c7-11e9-a361-79e2452f0c57.pkg。
- 步骤 9** 向上滚动到 威胁防御 REST API 页面顶部，然后点击 **AnyConnectPackageFile > POST /object/anyconnectpackagefiles**。对 API 执行 POST 操作，在负载中提供临时磁盘文件名和软件包文件的操作系统类型。此操作会创建 AnyConnect 软件包文件。
- 步骤 10** 在正文字段中，仅按以下格式输入软件包详细信息：
- ```
{ "platformType": "WINDOWS",
```



```
"diskFileName": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
"type": "anyconnectpackagefile",
"name": "AnyConnectWindowsBGL" }
```

- a. 在 platformType 字段中，输入操作系统平台为 WINDOWS、MACOS 或 LINUX。
- b. 在 diskFileName 字段中，输入您在上传磁盘文件后记录的 fileName。
- c. 在名称 (name) 字段中，输入要用于软件包的名称。
- d. 点击试用！。

在“响应正文”字段中，成功执行 POST 操作后，API 响应将按以下格式显示。

```
{ "version": "ni7xeneslft3p",
  "name": "AnyConnectWindowsBGL",
  "description": null,
  "diskFileName": "41d592e3-90ca-11e9-a361-6d05320a165d.pkg",
  "md5Checksum": "9bbe53dcf92e515d3ce5423048212488",
  "platformType": "WINDOWS",
  "id": "c9c9dfe3-9cd8-11e9-a361-23534f081c43",
  "type": "anyconnectpackagefile",
  "links": { "self":
    " https://>/ftd.example.com:972...1-cf32937ce0df "https://bglgrp1224-pod.cisco.com:972/api/fdm/v3/object/
    anyconnectpackagefiles/7f8248c7-90d1-11e9-a361-cf32937ce0df
  }
}
```

在 防火墙设备管理器 上创建 AnyConnect 软件包。

步骤 11 点击 AnyConnectPackageFile GET /object/anyconnectpackagefiles TRY IT OUT!。 > >

响应正文显示所有 AnyConnect 软件包文件。

示例响应如下所示。

```
{
  "items": [
    {
      "version": "la4nwceqk2sg4",
      "name": "AnyConnectWindowsBGL",
      "description": null,
      "diskFileName": "82f1e362-9cd8-11e9-a361-9758ba07962d.pkg",
      "md5Checksum": "9bbe53dcf92e515d3ce5423048212488",
      "platformType": "WINDOWS",
      "id": "c9c9dfe3-9cd8-11e9-a361-23534f081c43",
      "type": "anyconnectpackagefile",
      "links": {
```

将 AnyConnect 软件包上传到运行 FDM 管理 6.5 或更高版本的设备

```
"self":
  "https://ftd.example.com:972...1-23534f081c43"
}
},
```

步骤 12 为每种操作系统类型上传其他 AnyConnect 软件包。重复步骤 4 到 10。

步骤 13 编辑 URL 以指向网页，例如 <https://ftd.example.com> <https://ftd.example.com/#/api-explorer>

步骤 14 点击网页右上角的部署更改 (**Deploy Changes**) 图标。若有未部署的更改，系统会用圆点高亮显示。

步骤 15 如果您对所做的更改比较满意，可以点击立即部署 (**Deploy Now**) 立即启动作业。窗口将显示部署正在进行。您可以关闭窗口，或等待部署完成。



Note 要从设备中删除软件包，请点击 AnyConnectPackageFile Delete。FDM 管理 > 在 objID 字段中，键入软件包 ID，然后点击试用！

要完成 VPN 连接，您的用户必须在他们的工作站上安装 AnyConnect 客户端软件。有关详细信息，请参阅[用户如何在 FDM 管理设备上安装 AnyConnect 客户端软件, on page 271](#)。

将 AnyConnect 软件包上传到运行 FDM 管理 6.5 或更高版本的设备

如果您使用运行 6.5 或更高版本的 FDM 管理 设备来配置 RA VPN，则可以使用 思科防御协调器 中的 RA VPN 向导将 AnyConnect 软件包上传到设备。在 RA VPN 向导中，必须提供预加载 AnyConnect 软件包的远程 HTTP 或 HTTPS 服务器的 URL。



Note 您也可以使用 FDM API 程序上传 AnyConnect 软件包。将 [AnyConnect 软件包上传到运行版本 6.4.0 的 FDM 管理设备, on page 239](#)

从 CDO 存储库上传 AnyConnect 软件包


远程接入 VPN 配置向导显示 CDO 存储库中每个操作系统的 AnyConnect 软件包，您可以从中选择并上传到设备。确保设备可以访问互联网并进行正确的 DNS 配置。



注释 如果所需的软件包在显示的列表中不可用，或者设备无法访问互联网，则可以使用预加载 AnyConnect 软件包的服务器上传软件包。

过程

步骤 1 点击与操作系统对应的字段，然后选择 AnyConnect 软件包。

步骤 2 点击  以上传软件包。如果校验和不匹配，则 AnyConnect 软件包上传失败。您可以查看设备的工作流程选项卡，了解有关故障的更多详细信息。

准备工作

请确保为所需的操作系统下载“AnyConnect 前端部署软件包”。始终下载最新的 AnyConnect 版本，以确保获得最新的功能、漏洞修复和安全补丁。请定期更新设备上的软件包。



Note 您可以为以下每个操作系统 (OS) 上传一个 AnyConnect 软件包：Windows、Mac 和 Linux。无法为特定操作系统类型上传多个版本。

Procedure

步骤 1 从 <https://software.cisco.com/download/home/283000185> 下载 AnyConnect 软件包。

- 确保您接受 EULA 并具有 K9（加密映像）权限。
- 为您的操作系统选择“AnyConnect 前端部署软件包”。软件包名称类似于“anyconnect-win-4.7.04056-webdeploy-k9.pkg”。有适用于 Windows、macOS 和 Linux 的单独前端软件包。

步骤 2 将 AnyConnect 软件包上传到远程 HTTP 或 HTTPS 服务器。确保存在从 FDM 管理设备到 HTTP 或 HTTPS 服务器的网络路由。

Note 如果要将 AnyConnect 软件包上传到 HTTPS 服务器，请确保执行以下步骤：

- 从防火墙设备管理器上传 FDM 管理设备上该服务器的受信任 CA 证书。要上传证书，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南，版本 XY》“证书”一章中的“上传受信任 CA 证书”部分 <https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html#anchor613>
- 在 HTTPS 服务器上安装受信任的 CA 证书。


步骤 3 远程服务器的 URL 必须是不提示进行身份验证的直接链接。如果 URL 已进行预身份验证，则可以通过指定 RA VPN 向导的 URL 来下载文件。

步骤 4 如果远程服务器 IP 地址经过 NAT，则必须提供远程服务器位置的 NAT 公共 IP 地址。

上传新的 AnyConnect 软件包

使用以下程序将新的 AnyConnect 软件包上传到运行版本 6.5.0 的 FDM 管理设备：

Procedure

- 步骤 1 根据步骤 1-4 创建 RA VPN 配置。[创建 RA VPN 配置, on page 259](#)
- 步骤 2 在检测到的 **AnyConnect 软件包 (AnyConnect Package Detected)** 中, 您可以为 Windows、Mac 和 Linux 终端上传单独的软件包。
- 步骤 3 在相应的平台字段中, 指定预上传与 Windows、Mac 和 Linux 兼容的 AnyConnect 软件包的服务器路径。服务器路径示例: 'http://<ip_address> :port_number/<folder_name>/anyconnect-win-4.8.01090-webdeploy-k9.pkg', 'https:// :port_number/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg'。
- 步骤 4 点击  以上传软件包。CDO 验证路径是否可访问, 以及指定的文件名是否有效。验证成功后, 系统将显示 AnyConnect 软件包的名称。当您为更多设备添加 RA VPN 配置时, 您可以将 AnyConnect 软件包上传到这些设备。FDM 管理
- 步骤 5 点击 **确定 (OK)**。AnyConnect 软件包已添加到 RA VPN 配置中。
- 步骤 6 从第 6 步开始继续创建 RA VPN 配置。[创建 RA VPN 配置, on page 259](#)

What to do next

要完成 VPN 连接, 您的用户必须在他们的工作站上安装 AnyConnect 客户端软件。有关详细信息, 请参阅用户如何在 FTD 上安装 AnyConnect 客户端软件。[用户如何在 FDM 管理设备上安装 AnyConnect 客户端软件, on page 271](#)


替换现有的 AnyConnect 软件包

如果设备上已存在 AnyConnect 软件包, 您可以在 RA VPN 向导中看到它们。您可以在下拉列表中查看操作系统的所有可用 AnyConnect 软件包。您可以从列表中选择现有软件包并将其替换为新软件包, 但不能向列表中添加新软件包。



Note 如果要将现有软件包替换为新软件包, 请确保新的 AnyConnect 软件包已上传到设备可访问的网络上的服务器。FDM 管理

Procedure

- 步骤 1 在左侧的 CDO 导航栏中, 点击 **VPN > 远程访问 VPN (Remote Access VPN)**。
- 步骤 2 选择要修改的 RA VPN 配置, 然后在操作下点击编辑。
- 步骤 3 在“检测到的 AnyConnect 软件包”中, 点击现有 AnyConnect 软件包旁边的图标。☑ 如果操作系统有多个版本的 AnyConnect 软件包, 请从列表中选择要替换的软件包, 然后点击编辑。现有软件包将从相应字段中消失。
- 步骤 4 指定预加载新 AnyConnect 软件包的服务器路径, 然后点击 **上传软件包**。 
- 步骤 5 点击 **确定 (OK)**。新的 AnyConnect 软件包已添加到 RA VPN 配置中。

步骤 6 从第 6 步开始继续创建 RA VPN 配置。[创建 RA VPN 配置, on page 259](#)

删除 AnyConnect 软件包

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **VPN > 远程访问 VPN (Remote Access VPN)**。

步骤 2 选择要修改的 RA VPN 配置，然后在操作下点击编辑。

步骤 3 在“检测到的 AnyConnect 软件包”中，点击要删除的 AnyConnect 软件包旁边的图标。如果某个操作系统有多个版本的 AnyConnect 软件包，请从列表中选择要删除的软件包。现有软件包将从相应字段中消失。

Note 点击取消以停止删除操作并保留现有软件包，


步骤 4 点击**确定 (OK)**。设备的配置状态处于“未同步”状态。

Note 如果要在此阶段撤消删除操作，请转到设备和服务页面，然后点击放弃更改以保留现有的 AnyConnect 软件包。

步骤 5 [预览和部署所有设备的配置更改](#)。

为 FDM 管理 设备配置身份源

身份源（例如 Microsoft AD 领域和 RADIUS 服务器）是为组织内的人员定义用户账户的 AAA 服务器和数据库。身份源信息具有多种用途，例如提供与 IP 地址关联的用户身份，或是对远程访问 VPN 连接或到 思科防御协调器的访问进行身份验证。

点击 **对象 (Objects) > FDM 对象 (FDM Objects)**，然后点击  并选择 **> RA VPN 对象 (ASA 和 FTD) (RA VPN Objects [ASA & FTD]) > 身份源 (Identity Source)** 以创建源。后期配置需要使用身份源的服务时，可以使用这些对象。您可以应用适当的过滤器来搜索现有源并对其进行管理。

Active Directory 领域

Active Directory 可提供用户账户和身份验证信息。将包含 AD 领域的配置部署到 FDM 管理 设备时，CDO 会从 AD 服务器获取用户和组。

您可以将此源用于以下目的：

- 远程访问 VPN，作为主要身份源。您可以配合使用 AD 和 RADIUS 服务器。
- 身份策略，用于主动身份验证，并作为用户身份源用于被动身份验证。
- 身份规则，适用于用户的主动身份验证。

您可以使用用户身份创建访问控制规则。有关详细信息，请参阅[如何实施 Firepower 身份策略](#)。

CDO 每 24 小时请求一次更新的用户组列表。由于最多可以向规则中添加 50 个用户或组，所以选择组比选择单个用户通常更有意义。例如，您可以创建一条规则允许“工程”组访问开发网络，并创建一条后续规则拒绝对该网络的所有其他访问。然后，要将该规则应用于新工程师，您只需添加将工程师添加到目录服务器的“工程”组即可。

CDO 中的 Active Directory 领域

在创建 AD 身份对象时配置 AD 领域。身份源对象向导可帮助确定如何连接到 AD 服务器以及 AD 服务器在网络中的位置。



Note 如果在 CDO 中创建 AD 领域，则在创建附属身份源对象以及将这些对象添加到身份规则时，CDO 会记住 AD 密码。

FDM 中 Active Directory 领域

您可以从 CDO 对象向导指向在 FDM 中创建的 AD 领域对象。请注意，CDO 不会读取在 FDM 中创建的 AD 领域对象的 AD 密码。您必须在 CDO 中手动输入正确的 AD 密码。

要在防火墙设备管理器中配置 AD 领域，请参阅适用于运行设备的版本的《[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#)》中可重用对象一章的**配置 AD 身份领域**部分。

支持的目录服务器

可以使用 Windows Server 2008 和 2012 上的 AD。

请注意以下有关服务器配置的信息：

- 如果要对用户组或组内用户执行用户控制，则必须在目录服务器上配置用户组。如果服务器按照基本对象层次结构组织用户，系统无法执行用户组控制。
- 目录服务器必须使用下表中列出的字段名称，以便系统从该域的服务器中检索用户元数据：

元数据	Active Directory 字段
LDAP 用户名	samaccountname
First name	名称
姓氏	sn
邮箱地址	mail Userprincipalname (如果 mail 没有值)
部门	department distinguishedname (如果 department 没有值)
电话号码	telephonenumber

确定目录基准标识名

配置目录属性时，需要为用户和组指定公共基准标识名(DN)。基准在您的目录服务器中定义，并且会因网络而不同。您必须输入正确的基准，身份策略才能正常使用。如果基准错误，则系统无法确定用户名或组名，进而导致基于身份的策略无法使用。



Note 要获得正确的基准，请咨询目录服务器的管理员。

对于 Active Directory，您可以用域管理员的身份登录 AD 服务器，并按照如下所示在命令提示符后输入 **dsquery** 命令来确定正确的基准：

用户搜索库

输入具有已知用户名（部分或完整）的 **dsquery user** 命令，以确定基准标识名。例如，以下命令使用部分名称 “John*” 返回以 “John.” 开头的所有用户的信息。

```
C:\Users\Administrator>dsquery user -name "John*"
"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"
```

基准 DN 为 “DC=csc-lab,DC=example,DC=com”。

组搜索基准

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

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

组基准 DN 为 “DC=csc-lab,DC=example,DC=com”。

此外，您还可以使用 ADSI Edit 程序浏览 AD 结构 (**Start > Run > adsiedit.msc**)。在 ADSI Edit 中，右键点击任意对象，例如组织单位 (OU)、组或用户，然后选择 **属性查看标识名**。然后，可以复制 DC 值的字符串作为基准。

要验证您是否获得了正确的基准，请执行以下操作：

Procedure

- 步骤 1** 点击目录属性中的 **测试连接 (Test Connection)** 按钮验证连接。解决所有问题后，保存目录属性。
- 步骤 2** 提交对设备的更改。
- 步骤 3** 创建访问规则，选择 **用户** 选项卡，并尝试从目录添加已知的用户和组名称。在您键入内容时，系统会自动填充建议，以匹配包含该目录的领域中的用户和组。如果这些建议显示在一个下拉列表中，则说明系统可以成功查询目录。如果您没有看到建议，而且确定您键入的字符串应显示在用户或组名称中，则需要更正相应的搜索基准。

What to do next

有关详细信息，请参阅[创建或编辑 Active Directory 领域对象](#)。

RADIUS 服务器和组

您可以使用 RADIUS 服务器对管理用户进行身份验证和授权。

配置要使用 RADIUS 服务器的功能时，您应选择 RADIUS 组而不是单个服务器。RADIUS 组所含 RADIUS 服务器是彼此副本的集合。如果一个组具有多个服务器，这些服务器可构成备份服务器链，在其中一台服务器不可用时提供冗余。但即使只有一台服务器，也必须创建包含一个成员的组，以配置功能的 RADIUS 支持。

您可以将此源用于以下目的：

- 远程访问 VPN 用作身份验证、授权和记账的身份源。您可以配合使用 AD 和 RADIUS 服务器。
- 身份策略，作为被动身份源来从远程访问 VPN 登录收集用户身份信息。

有关详细信息，请参阅[创建或编辑 RADIUS 服务器对象或组](#)。

相关信息：

- [创建或编辑 Active Directory 领域对象](#)
- [创建或编辑 RADIUS 服务器对象或组](#)
- [配置身份策略](#)

创建或编辑 Active Directory 领域对象

关于 Active Directory 领域对象


当您创建或编辑身份源对象（例如 AD 领域对象）时，思科防御协调器通过 SDC 将配置请求发送到 FDM 管理设备。然后，FDM 管理设备会与配置的 AD 领域通信。

请注意，CDO 不会读取通过防火墙设备管理器控制台配置的 AD 领域的目录密码。如果使用最初在防火墙设备管理器中创建的 AD 领域对象，则必须手动输入目录密码。

创建 FTD Active Directory 领域对象

使用以下程序创建对象：

Procedure

- 步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
- 步骤 2** 点击，然后点击 RA VPN 对象（ASA 和 FTD）身份源。  >
- 步骤 3** 为对象输入对象名称 (**Object Name**)。
- 步骤 4** 选择设备类型作为 FTD。
- 步骤 5** 在向导的第一部分中，选择 Active Directory 领域作为身份源类型。点击**继续 (Continue)**。

步骤 6 配置基本领域属性。

- **目录用户名、目录密码 (Directory Username, Directory Password)** - 用户的标识名称和密码，该用户具备访问您要检索的用户信息的适当权限。对于 AD，用户不需要更高的权限。您可以在域中指定任何用户。用户名必须是完全限定的；例如， [Administrator@example.com](#)（而不仅仅是 Administrator）。

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

- **基准区别名称 (Base Distinguished Name)** - 用于搜索或查询用户和组信息的目录树，即用户和组的公共父项。例如， cn=users, dc=example, dc=com。
- **AD 主域 (AD Primary Domain)** - 设备应加入的完全限定 AD 域名。例如 example.com。

步骤 7 配置目录服务器属性。

- **主机名/IP 地址 (Hostname/IP Address)** - 目录服务器的主机名或 IP 地址。如果以加密方式连接到服务器，则必须输入完全限定域名，而非 IP 地址。
- **端口 (Port)** - 用于与服务器通信的端口号。默认值为 389。如果选择 LDAPS 作为加密方法，请使用端口 636。
- **加密 (Encryption)** - 要使用加密连接下载用户和组信息，请选择所需的方法 **STARTTLS** 或 **LDAPS**。系统默认为无，也就是说以明文形式下载用户和组信息。
 - **STARTTLS** 将会协商加密方法，并使用目录服务器支持的最强方法。使用端口 389。如果将领域用于远程访问 VPN，则不支持此选项。
 - **LDAPS** 需要基于 SSL 的 LDAP。使用端口 636。
- **受信任 SSL 证书 (Trusted CA Certificate)** - 如果选择加密方法，请上传证书颁发机构 (CA) 证书以便在系统和目录服务器之间启用受信任的连接。如果要使用证书进行身份验证，则证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 10.10.10.250 作为 IP 地址，但证书中的地址为 ad.example.com，则连接失败。

步骤 8 (可选) 使用测试按钮验证配置。

步骤 9 (可选) 点击添加其他配置，将多个 AD 服务器添加到 AD 领域。AD 服务器需要彼此复制并支持相同的 AD 域。因此，与该 AD 领域关联的所有 AD 服务器的基本领域属性（例如目录名称、目录密码和基本可分辨名称）必须相同。

步骤 10 点击添加 (Add)。

步骤 11 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

编辑 FTD Active Directory 领域对象


请注意，在编辑身份源对象时，不能更改身份源类型。您必须创建具有正确类型的新对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的对象。

步骤 3 选择要编辑的对象。

步骤 4 点击操作 (**Actions**) 窗格中的编辑图标 。

步骤 5 在上述过程中创建值的相同方式编辑对话框中的值。展开下面列出的配置栏，以编辑或测试主机名/IP 地址或加密信息。

步骤 6 点击保存 (**Save**)。

步骤 7 CDO 显示将受更改影响的策略。点击确认 (**Confirm**) 以完成对对象和受其影响的任何策略的更改。

步骤 8 立即 [预览和部署所有设备的配置更改](#) 您所做的更改，或等待并一次部署多个更改。

相关信息：

- [创建或编辑 RADIUS 服务器对象或组](#)
- [配置身份策略](#)
- [配置身份规则](#)
- [配置身份策略设置](#)

创建或编辑 RADIUS 服务器对象或组

关于 RADIUS 服务器对象或组

在创建或编辑 RADIUS 服务器对象或一组 RADIUS 服务器对象等身份源对象时，CDO 会通过 SDC 将配置请求发送到 FDM 管理设备。然后，FDM 管理设备会与配置的 AD 领域通信。


创建 RADIUS 服务器对象

RADIUS 服务器提供 AAA（身份验证、授权和记账）服务。

使用以下程序创建对象：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击 ，然后点击 **RA VPN 对象 (ASA & FTD) (RA VPN Objects [ASA & FTD]) > 身份源 (Identity Source)**。

步骤 3 为对象输入对象名称 (**Object name**)。

步骤 4 对于设备类型，请选择 **FTD**。

步骤 5 对于身份源类型，请选择 **RADIUS 服务器**。点击继续 (**Continue**)。

步骤 6 使用以下属性编辑身份源配置：

- **服务器名称或 IP 地址 (Server Name or IP Address)** - 服务器的完全限定主机名 (FQDN) 或 IP 地址。
- **身份验证端口 (Authentication Port)** (可选) - 在其上执行 RADIUS 身份验证和授权的端口。默认值为 1812。
- **超时 (Timeout)** - 系统将请求发送至下一服务器之前等待服务器响应的时长，此为 1-300 秒之间的数值。默认值为 10 秒。
- **输入服务器密钥 (Server Secret Key)** (可选) - 用于加密 Firepower 威胁防御设备和 RADIUS 服务器之间数据的共享密钥。该密钥是一个区分大小写的字母数字字符串，最多 64 个字符，且不含空格。密钥必须以字母数字字符或下划线开头，它可以包含特殊字符：\$ & - _ . + @。字符串必须匹配 RADIUS 服务器上配置的字符串。如果不配置密钥，则不加密连接。

步骤 7 如果您已经为网络配置了 Cisco Identity Services Engine (ISE)，并使用服务器进行远程访问 VPN 授权更改配置，您可以点击**仅限 RA VPN (RA VPN Only)** 链接并配置以下选项。

- **重定向 ACL (Redirect ACL)** - 选择要用于 RA VPN 重定向 ACL 的扩展访问控制列表 (ACL)。如果没有扩展 ACL，则必须从 FDM 管理设备控制台中的 Smart CLI 模板创建所需的扩展 ACL 对象。请参阅适用于运行设备的版本的《[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#)》中“高级配置”一章的**配置智能 CLI 对象**部分。重定向 ACL 的目的是向 ISE 发送初始流量，以便评估客户端安全状态。ACL 应向 ISE 发送 HTTPS 流量，而非已设定发往 ISE 的流量或被定向到域名解析 DNS 服务器的流量。请参阅适用于运行设备的版本的《[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#)》中“虚拟专用网络 (VPN)”一章的**配置授权更改**部分。
- **诊断接口** - 启用此选项将允许系统始终使用“诊断”接口与服务器通信。如果禁用此选项，CDO 将默认使用路由表来确定要使用的接口。

步骤 8 点击**添加 (Add)**。

步骤 9 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。


创建 RADIUS 服务器组

RADIUS 服务器组中包含一个或多个 RADIUS 服务器对象。组中的服务器必须是彼此的备份。这些服务器构成备份服务器链，因此，如果第一台服务器不可用，系统可以尝试列表中的下一个服务器。

使用以下程序创建对象组：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击，然后点击 FTD 身份源。 >

步骤 3 为对象输入**对象名称 (Object name)**。


步骤 4 选择设备类型作为 FTD。

步骤 5 选择 RADIUS 服务器组作为身份源类型。点击**继续 (Continue)**。

步骤 6 使用以下属性编辑身份源配置：

- **断路时间 (Dead Time)** - 只有当所有服务器均发生故障时，才会重新激活故障服务器。断路时间是指最后一台服务器发生故障后，在重新激活所有服务器之前所等待的时间。
- **最大失败尝试次数 (Maximum Failed Attempts)** - 尝试组中下一个服务器之前发送到 RADIUS 服务器的失败请求（即，未收到响应的请求）数。超过最大失败尝试次数时，系统会将服务器标记为故障。对于给定功能，如果您使用本地数据库配置回退方法，并且组中的所有服务器都无法响应，则会将该组视为无法响应，并将尝试回退方法。该服务器组会在断路时间内保持标记为无响应，以确保该时段内其他 AAA 请求不会尝试联系该服务器组，而是立即使用回退方法。
- **动态授权/端口 (Dynamic Authorization/Port)**（可选）- 如果为此 RADIUS 服务器组启用 RADIUS 动态授权或授权更改 (CoA) 服务，该组会注册 CoA 通知并侦听指定的端口，以便使 CoA 策略从 Cisco Identity Services Engine (ISE) 进行更新。仅当您在远程接入 VPN 中结合 ISE 使用此服务器组时，才能启用动态授权。

步骤 7 从下拉菜单中选择支持 RADIUS 服务器的 AD 领域。如果尚未创建 AD 领域，请从下拉菜单中点击创建。

步骤 8 点击添加按钮以添加现有的 RADIUS 服务器对象。 或者，您可以从此窗口创建新的 RADIUS 服务器对象。

Note 优先级添加这些对象，因为列表中的第一个服务器将被使用，直到它停止响应。然后，设备默认为列表中的下一个服务器。FDM 管理

步骤 9 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

编辑 Radius 服务器对象或组


使用以下程序编辑 Radius 服务器对象或 Radius 服务器组：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的对象。

步骤 3 选择要编辑的对象。

步骤 4 点击**操作 (Actions)** 窗格中的编辑图标 。

步骤 5 以在上述过程中创建值的相同方式编辑对话框中的值。要编辑或测试主机名/IP 地址或加密信息，请展开配置栏。

步骤 6 点击**保存 (Save)**。

步骤 7 CDO 显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

步骤 8 立即[预览和部署所有设备的配置更改](#)您所做的更改，或等待并一次部署多个更改。

创建新的 RA VPN 组策略

组策略是一组面向用户的远程接入 VPN 的属性/值对。连接配置文件使用组策略在建立隧道后设置用户连接的条款。通过组策略可将整组属性应用于用户或用户组，而不必为每个用户单独指定每个属性。


系统包含名为“DfltGrpPolicy”的默认组策略。您可以创建其他组策略，以提供您所需的服务。



Note 不能将不一致的组策略对象添加到 RA VPN 配置。在将组策略添加到 RA VPN 配置之前，请解决所有不一致问题。

Procedure

步骤 1 在左侧的 思科防御协调器 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击“加号”  按钮。

步骤 3 点击 **RA VPN 对象 (ASA 和 FTD) (RA VPN Objects [ASA & FTD]) > RA VPN 组策略 (RA VPN Group Policy)**。

步骤 4 输入组策略的名称。此名称最多可包含 64 个字符，允许使用空格。

步骤 5 在 **设备类型 (Device Type)** 下拉列表中，选择 **ASA**。

步骤 6 执行以下任一操作：

- 点击所需的选项卡并配置页面上的属性：
 - [RA VPN 组策略属性](#)
 - [AnyConnect 客户端配置文件, on page 254](#)
 - [会话设置属性, on page 255](#)
 - [地址分配属性, on page 255](#)
 - [分割隧道属性, on page 256](#)
 - [AnyConnect 属性, on page 257](#)
 - [流量过滤器属性, on page 258](#)
 - [Windows 浏览器代理属性, on page 258](#)

步骤 7 点击 **保存 (Save)** 以保存组策略。

RA VPN 组策略属性

组策略的常规属性定义组名称和一些其他基本设置。“名称”属性是唯一必需的属性。

- **DNS 服务器 (DNS Server):** 选择定义连接到 VPN 时，DNS 服务器客户端应用于域名解析的 DNS 服务器组。如果所需的组尚不存在，请点击**创建 DNS 组**并立即创建组。
- **横幅:** 登录时向用户显示的横幅文本或欢迎消息。默认无横幅。最多 496 字符。AnyConnect 客户端支持部分 HTML。为确保向远程用户正确地显示横幅，请使用
 标记表示换行。
- **默认域 (Default Domain):** RA VPN 中用户的默认域名。例如 example.com。此域将被添加到非完全限定的主机名，例如 serverA 而不是 serverA.example.com。
- **AnyConnect 客户端配置文件 (AnyConnect Client Profiles):** 点击 + 并选择要用于该组的 AnyConnect 客户端配置文件。请参阅[上传 RA AnyConnect 客户端配置文件](#)。如果为外部接口（在连接配置文件中）配置的是完全限定域名，则系统将会为您创建默认配置文件。或者，您可上传您的客户端配置文件。使用独立的 AnyConnect 配置文件编辑器创建这些配置文件，您可以从 software.cisco.com 下载和安装该编辑器。如果不选择客户端配置文件，AnyConnect 客户端将为所有选项使用默认值。此列表中的项目是 AnyConnect 客户端配置文件对象，而不是配置文件本身。您可以通过点击下拉列表中的**创建新的 AnyConnect 客户端配置文件 (Create New AnyConnect Client Profile)**，创建（和上传）新配置文件。

AnyConnect 客户端配置文件

运行软件版本 6.7 或更高版本的 防火墙设备管理器 支持此功能。

Cisco AnyConnect VPN 客户端通过各种内置模块提供增强的安全性。这些模块提供网络安全，终端流量的网络可视性和网络外漫游保护等服务。每个客户端模块都包含一个客户端配置文件，其中包含根据您的要求的一组自定义配置。

当 VPN 用户下载 VPN AnyConnect 客户端软件时，您可以选择要下载到客户端的 AnyConnect VPN 配置文件对象和 AnyConnect 模块。

1. 选择或创建 AnyConnect VPN 配置文件对象。请参阅[上传 RA AnyConnect 客户端配置文件, on page 269](#)。除 DART 和“登录前启动”模块外，必须选择 AnyConnect VPN 配置文件对象。
2. 点击添加**Any 链接客户端模块 (Add Any Connect Client Module)**。

以下 AnyConnect 模块是可选的，您可以将这些模块配置为在 VPN AnyConnect 客户端软件时下载：

- **AMP 启用程序 (AMP Enabler)** - 为终端部署高级恶意软件防护 (AMP)。
- **DART** - 捕获系统日志和其他诊断信息的快照并在桌面上创建 .zip 文件，因此您可以便利地将故障排除信息发送到思科 TAC。
- **反馈 (Feedback)** - 提供有关客户已启用和使用的功能和模块的信息。
- **ISE 终端安全评估 (ISE Posture)** - 使用 OPSWAT v3 库执行终端安全评估检查，评估终端的合规性。
- **网络访问管理器 (Network Access Manager)** - 为有线和无线网络访问提供 802.1X（第 2 层）和设备身份验证。

- **网络可视性 (Network Visibility)** - 可提升企业管理员执行容量和服务规划、审计、合规性和安全分析的能力。
- **登录前启动 (Start Before Login)** - 通过在 Windows 登录对话框出现之前启动 AnyConnect, 强制用户在登录到 Windows 之前通过 VPN 连接而连接到企业基础设施。
- **Umbrella 漫游安全 (Umbrella Roaming Security)** - 在没有处于活动状态的 VPN 时提供 DNS 层安全。
- **网络安全 (Web Security)** - 根据定义的安全策略分析网页的元素, 允许可接受的内容, 并阻止恶意或不可接受的内容。

3. 在**客户端模块 (Client Module)**列表中选择 **AnyConnect 模块 (AnyConnect module)**。
4. 在**配置文件 (Profile)**列表中, 选择或创建包含 AnyConnect 客户端配置文件的配置文件对象。
5. 选择**启用模块下载 (Enable Module Download)**以下载客户端模块以及配置文件。如果未选择, 则终端只能下载客户端配置文件。

会话设置属性

组策略会话设置控制用户可以连接到 VPN 的时长和可以创建的独立连接的数量。

- **最长连接时间 (Maximum Connection Time)**: 在不注销和重新连接的情况下, 用户可持续连接到 VPN 的最大时间长度 (以分钟为单位), 范围为 1 到 4473924 或留空。默认值为无限 (留空), 但空闲超时仍适用。
- **连接时间警报间隔 (Connection Time Alert Interval)**: 如果您指定了最大连接时间, 则警报间隔定义, 在达到最长时间之前, 向用户显示即将自动断开连接警告的时间。用户可以选择结束连接并重新连接, 以重新启动计时器。默认值为 1 分钟。可以指定 1 到 30 分钟。
- **空闲时间 (Idle Time)**: VPN 连接在自动关闭之前可以闲置的时间长度 (以分钟为单位), 范围为 1 到 35791394。如果在此时间段内此连接上无通信活动, 则系统会终止连接。默认值为 30 分钟。
- **空闲时间警报间隔 (Idle Time Alert Interval)**: 在达到空闲时间之前, 向用户显示因闲置会话而即将自动断开连接的警报的时间。任何活动都会重置计时器。默认值为 1 分钟。可以指定 1 到 30 分钟。
- **每个用户的同时登录数 (Simultaneous Login Per User)**: 允许用户执行的最多同时登录数。默认值为 3。可以指定 1 到 2147483647 个连接。允许许多同时连接可能会危害安全性并影响性能。

地址分配属性

组策略的地址分配属性定义组的 IP 地址池。此处定义的地址池将覆盖使用此组的任何连接配置文件中定义的池。如果您希望使用连接配置文件中定义的池, 请将这些设置留空。

- **IPv4 地址池 (IPv4 Address Pool)、IPv6 地址池 (IPv6 Address Pool)**: 这些选项定义远程终端的地址池。根据客户端用于建立 VPN 连接的 IP 版本, 从这些池为客户端分配地址。选择一个网络对象, 定义要支持的每个 IP 类型的子网。如果您不想支持该 IP 版本, 则可以空着列表。例

如，可以将 IPv4 池定义为 10.100.10.0/24。地址池不能与外部接口的 IP 地址位于同一子网。可以指定包含最多六个地址池的列表，用于本地地址分配。地址池的指定顺序非常重要。系统按照地址池出现的顺序分配这些地址池中的地址。

- **DHCP 范围 (DHCP Scope):** 如果在连接配置文件中为地址池配置了 DHCP 服务器，DHCP 作用域会标识要用于此组的地址池的子网。DHCP 服务器的地址还必须来自此作用域标识的同一个池。作用域允许您选择 DHCP 服务器中定义的部分地址池，用于此特定组。如未定义网络范围，则 DHCP 服务器将按地址池配置顺序分配 IP 地址。它将检查各个池，直到发现未分配的地址为止。要指定作用域，请选择包含网络号主机地址的网络对象。如果对象尚不存在，请点击**创建新网络**。例如，要告诉 DHCP 服务器使用 192.168.5.0/24 子网池中的地址，请选择指定 192.168.5.0 为主机地址的网络对象。DHCP 仅可用于 IPv4 寻址。

分割隧道属性

组策略的分割隧道属性定义系统如何处理用于内部网络的流量和流向外部的流量。分割隧道引导一些网络流量通过 VPN 隧道（加密），将剩下的网络流量引导至 VPN 隧道外部（未加密或以明文形式）。

- **IPv4 分割隧道 (IPv4 Split Tunneling)、IPv6 分割隧道 (IPv6 Split Tunneling):** 可以根据流量是使用 IPv4 寻址还是 IPv6 寻址来指定不同的选项，但每个流量的选项都相同。如果想要启用分割隧道，指定其中一个要求您选择网络对象的选项。
 - **允许所有流量通过隧道 (Allow all traffic over tunnel):** 不分割隧道。一旦用户建立 RA VPN 连接，用户的所有流量都会通过受保护隧道。这是默认值。这也被视为最安全的选项。
 - **允许指定流量通过隧道 (Allow specified traffic over the tunnel):** 选择定义目标网络和主机地址的网络对象。前往这些目标的所有流量都会通过受保护隧道。客户端会将前往其他目标的流量路由至隧道外部（例如，本地 Wi-Fi 或网络连接）。
 - **排除以下指定网络 (Exclude networks specified below):** 选择定义目标网络或主机地址的网络对象。客户端将前往这些目标的所有流量路由至隧道外部的连接。前往其他目标的流量都会通过隧道。
- **分割 DNS (Split DNS) -** 您可以配置系统通过安全连接发送某些 DNS 请求，同时允许客户端将其他 DNS 请求发送到客户端上配置的 DNS 服务器。您可以配置以下 DNS 行为：
 - **根据分割隧道策略发送 DNS 请求 (Send DNS Request as per split tunnel policy):** 使用此选项时，系统将按照与定义分割隧道选项相同的方式处理 DNS 请求。如果启用分割隧道，则会根据目标地址发送 DNS 请求。如果未启用分割隧道，所有 DNS 请求都会通过受保护的连接。
 - **始终通过隧道发送 DNS 请求 (Always send DNS requests over tunnel):** 如果启用了分割隧道，但想要通过受保护连接将所有 DNS 请求发送到为该组定义的 DNS 服务器上，则可选择此选项。
 - **仅通过隧道发送指定的域 (Send only specified domains over tunnel):** 如果想要让受保护的 DNS 服务器仅解析特定域的地址，则可选择此选项。然后，指定这些域，用逗号分隔域名。例如，example.com, example1.com。如果想要让内部 DNS 服务器解析内部域的名称，同时让外部 DNS 服务器处理所有其他互联网流量，请使用此选项。

AnyConnect 属性

组策略的 AnyConnect 属性定义 AnyConnect 客户端用于远程接入 VPN 连接的某些 SSL 和连接设置。

• SSL 设置

- **启用数据报传输层安全 (DTLS) (Enable Datagram Transport Layer Security [DTLS]):** 是否允许 AnyConnect 客户端使用两个同步隧道: SSL 隧道和 DTLS 隧道。使用 DTLS 可避免某些 SSL 连接带来的延迟和带宽问题, 并可改进对数据包延迟敏感的实时应用的性能。如果不启用 DTLS, AnyConnect 客户端用户在建立 SSL VPN 连接时仅与 SSL 隧道连接。
- **DTLS 压缩 (DTLS Compression):** 是否使用 LZS 为此组压缩数据报传输层安全 (DTLS) 连接。默认情况下会禁用 DTLS 压缩。
- **SSL 压缩 (SSL Compression):** 是否启用数据压缩, 如启用, 则设置要使用的数据压缩方法: Deflate 或 LZS。默认情况下会禁用 SSL 压缩。数据压缩加快了传输速率, 但也增加了每个用户会话的内存需求和 CPU 使用率。因此, SSL 压缩会降低设备的整体吞吐量。
- **SSL 重新生成密钥方法 (SSL Rekey Method)、SSL 重新生成密钥间隔 (SSL Rekey Interval):** 客户端能够为 VPN 连接重新生成密钥, 重新协商加密密钥和初始化向量, 从而提高连接的安全性。选择无可禁用重新生成密钥。要启用重新生成密钥, 请选择**新隧道**来创建新的隧道。(**现有隧道 (Existing Tunnel)** 选项导致的操作与 **新隧道 (New Tunnel)** 的相同。) 如果启用重新生成密钥, 还需设置重新生成密钥间隔, 默认间隔为 4 分钟。可以将间隔设置为 4 到 10080 分钟 (1 周)。

• 连接设置

- **忽略 DF (不分片) 位 (Ignore the DF [Don't Fragment] bit):** 是否忽略需要分片的数据包内的“不分片”(DF) 位。选择此选项会允许强制将已设置 DF 位的数据包分片, 从而使这些数据包能够通过隧道。
- **客户端绕行协议 (Client Bypass Protocol) -** 允许您配置安全网关管理 IPv4 流量 (安全网关仅允许 IPv6 流量时) 或管理 IPv6 流量 (安全网关仅允许 IPv4 流量时) 的方式。

当 AnyConnect 客户端建立与头端的 VPN 连接时, 头端可以为客户端分配 IPv4 和/或 IPv6 地址。如果头端对 AnyConnect 连接仅分配一个 IPv4 地址或一个 IPv6 地址, 则您可以配置 Client Bypass Protocol 以丢弃头端尚未分配 IP 地址 (默认、已禁用、未检查) 的网络流量, 或允许该流量绕过头端并从客户端以未加密或“明文形式”发送 (已启用、已检查)。

例如, 假设安全网关只将一个 IPv4 地址分配给 AnyConnect 连接, 且终端为双协议栈。当终端尝试访问 IPv6 地址时, 如果禁用客户端旁路协议, 则会丢弃 IPv6 流量; 但是, 如果启用客户端旁路协议, 则会从客户端以明文形式发送 IPv6 流量。

- **MTU:** 思科 AnyConnect VPN 客户端为 SSL VPN 连接建立的最大传输单位 (MTU) 大小。默认值为 1406 字节。范围为 576 至 1462 字节。
 - **AnyConnect 和 VPN 网关之间的保持连接消息:** 是否在对等体之间交换保持连接消息, 以证明它们可用于在隧道中发送和接收数据。保持连接消息以设置的时间间隔传输。默认间隔为 20 秒, 有效范围为 15 到 600 秒。

- **网关端 DPD 间隔、客户端 DPD 间隔**：启用失效对等体检测 (DPD)，确保 VPN 网关或 VPN 客户端快速检测对等体不再响应的的时间。您可以单独启用网关或客户端 DPD。发送 DPD 消息的默认间隔为 30 秒。时间间隔可以是 5 到 3600 秒。

流量过滤器属性

组策略的流量过滤器属性定义您想要对分配到该组的用户设置的限制。您可以使用这些属性（而非创建策略规则）根据主机或子网地址和协议或 VLAN 来限制 RA VPN 用户仅可访问特定资源。默认情况下，RA VPN 用户不会受到组策略的限制，可以访问受保护网络上的任何目标。

- **访问列表过滤器 (Access List Filter)**：使用扩展的访问控制列表 (ACL) 限制访问权限。选择 Smart CLI 扩展 ACL 对象。扩展 ACL 允许您基于源地址、目的地址和协议（例如 IP 或 TCP）进行过滤。ACL 评估遵循自上而下、“先匹配的规则先应用”原则，因此，请确保特定规则放在一般规则之前。ACL 末尾不包含隐式 “deny any” 语句，因此如果您想要拒绝对几个子网的访问，同时允许其他访问，请确保在 ACL 末尾加上 “permit any” 规则。由于您无法在编辑扩展的 ACL Smart CLI 对象时创建网络对象，因此您应在编辑组策略之前创建 ACL。否则，您可能需要先创建对象，然后再返回来创建网络对象，最后创建您需要的所有访问控制条目。要创建 ACL，登录 防火墙设备管理器，请转至设备 (Device) > 高级配置 (Advanced Configuration) > 智能 CLI (Smart CLI) > 对象 (Objects)，创建对象，并选择扩展访问列表 (Extended Access List) 作为对象类型。
- **限制 VPN 到 VLAN (Restrict VPN to VLAN)**：也称为“VLAN 映射”，此属性指定该组策略应用到的会话的出口 VLAN 接口。系统将该组中的所有流量都转发到所选 VLAN。使用此属性向组策略分配 VLAN 以简化访问控制。向此属性赋值是在会话中使用 ACL 过滤流量的替代方法。确保您指定了在设备子接口上定义的 VLAN 编号。值的范围为 1 到 4094。

Windows 浏览器代理属性

组策略的 Windows 浏览器代理属性确定用户浏览器上定义的代理是否运行以及如何运行。

可以为 VPN 会话期间浏览器代理选择以下值之一：

- **终端设置无变化 (No change in endpoint settings)**：允许用户配置（或不配置）浏览器代理或 HTTP，并在已配置的情况下使用代理。
- **禁用浏览器代理 (Disable browser proxy)**：不使用为浏览器定义的代理（如有）。浏览器连接不会通过该代理。
- **自动检测设置 (Auto detect settings)**：在客户端设备的浏览器中启用自动代理服务器检测。
- **使用自定义设置 (Use custom settings)**：定义所有客户端设备应对 HTTP 流量使用的代理。配置以下设置：
 - **代理服务器 IP 或主机名 (Proxy Server IP or Hostname)、端口 (Port)**：代理服务器的 IP 地址或主机名，以及代理服务器用于代理连接的端口。主机和端口总共不能超过 100 个字符。
 - **浏览器例外列表 (Browser Proxy Exemption List)**：与例外列表中的主机/端口的连接不通过代理。添加不应使用代理的所有目标的主机/端口值。例如，www.example.com 端口 80。点

击添加代理例外 (Add proxy exemption) 以将项目添加到列表。点击垃圾桶图标可删除项目。整个代理例外列表（包括所有地址和端口）不能超过 255 个字符。

创建 RA VPN 配置

CDO 允许您将一个或多个设备添加到 RA VPN 配置向导，并配置与设备关联的 VPN 接口、访问控制和 NAT 豁免设置。FDM 管理因此，每个 RA VPN 配置都可以在与 RA VPN 配置关联的多个设备之间共享连接配置文件和组策略。FDM 管理此外，您可以通过创建连接配置文件和组策略来增强配置。

您可以载入已配置 RA VPN 设置的设备，也可以载入没有 RA VPN 设置的新设备。FDM 管理当您载入已具有 RA VPN 设置的设备时，CDO 会自动创建“默认 RA VPN 配置”并将设备与此配置相关联。FDM 管理此外，此默认配置可以包含设备上定义的所有连接配置文件对象。



Important

- 不允许在同一远程接入 VPN 配置中添加 ASA 和设备。FDM 管理
- 一台设备不能有多个 RA VPN 配置。FDM 管理

前提条件

在将设备添加到 RA VPN 配置之前，必须满足以下前提条件：FDM 管理

- 确保设备具备以下条件：FDM 管理
 - 有效的思科安全客户端许可证。有关详细信息，请参阅[远程访问 VPN 的许可要求](#)。
 - 对于 FDM 版本 6.4.0，请确保至少已将一个 AnyConnect 软件包预上传到设备。有关详细信息，请参阅将 AnyConnect 软件包上传到 Firepower 威胁防御设备版本 6.4.0。[在运行版本 6.4.0 的 FDM 管理 设备上升级 AnyConnect 软件包, on page 267](#)
 - 对于 FDM 版本 6.5.0 及更高版本，您可以使用 CDO 上传 AnyConnect 软件包。有关详细信息，请参阅将 AnyConnect 软件包上传到 Firepower 威胁防御设备版本 6.5.0。[将 AnyConnect 软件包上传到运行 FDM 管理 6.5 或更高版本的设备, on page 242](#)
 - 没有待处理的配置部署。
- FDM 更改同步到 CDO。
 1. 在左侧的 CDO 导航栏中，点击资产并搜索要同步的一个或多个设备。FDM 管理
 2. 选择一个或多个设备，然后点击检查更改。CDO 与一个或多个设备通信以同步更改。FDM 管理
- RA VPN 配置组策略对象一致。
 - 确保解决所有不一致的组策略对象，因为它们无法添加到 RA VPN 配置中。解决问题或从“对象” (Objects) 页面删除不一致的组策略对象。有关详细信息，请参阅[解决重复对象问题和解决不一致对象问题](#)。[解决重复对象问题](#)[解决不一致的对象问题](#)

- 设备的 RA VPN 组策略与 RA VPN 配置组策略匹配。FDM 管理


操作步骤

Procedure

步骤 1 在左侧的 思科防御协调器 导航栏中，点击 **VPN > 远程访问 VPN 配置 (Remote Access VPN Configuration)**。

步骤 2 点击蓝色加号  按钮以创建 RA VPN 配置。

步骤 3 输入远程访问 VPN 配置的名称。

步骤 4 点击蓝色加号  按钮将 FDM 管理 设备添加到配置。您可以添加设备详细信息并配置与设备关联的网络流量相关权限。

a. 提供以下设备详细信息：

- **设备：**选择要添加的 FDM 管理设备，然后点击 **选择**。

Important 不允许在同一远程接入 VPN 配置中添加 ASA 和 FDM 管理 设备。

- **设备身份证书 (Certificate of Device Identity)：**选择用于建立设备身份的内部证书。在 AnyConnect 客户端与设备进行连接时确定客户端的设备身份。客户端必须接受此证书才能完成安全的 VPN 连接。如果您还没有证书，请点击下拉列表中的 **创建新内部证书 (Create New Internal Certificate)**。请参阅 [生成自签名的内部证书和内部 CA 证书](#)。
- **外部接口 (Outside Interface)：**用户在进行远程访问 VPN 连接时连接的接口。请选择您使用此连接配置文件支持的设备与最终用户之间的任何接口，虽然这通常是外部（面向互联网的）接口。要创建新的子接口，请参阅 [配置 Firepower VLAN 子接口和 802.1Q 中继](#)。
- **外部接口的完全限定域名或 IP (Fully Qualified Domain Name or IP for the Outside Interface)：**接口的名称（例如 `ravpn.example.com`）或必须提供的 IP 地址。如果指定名称，系统可以为您创建一个客户端配置文件。**注意：**您要确保 VPN 中和客户端使用的 DNS 服务器可以将此名称解析为外部接口的 IP 地址。将 FQDN 添加到相关 DNS 服务器。

b. 点击 **继续** 以配置流量权限。

- **为已解密的流量绕过访问控制策略 (sysopt permit-vpn)：**默认情况下，已解密流量要经过访问控制策略的检查。启用此选项可绕过解密流量选项，绕过访问控制策略检查，但从 AAA 服务器下载的 VPN 筛选 ACL 和授权 ACL 仍会应用于 VPN 流量。请注意，如果选择此选项，系统会配置 `sysopt connection permit-vpn` 命令，此为全局设置。这也会影响站点间 VPN 连接的行为。如果不选择此选项，外部用户可能会骗取远程访问 VPN 地址池中的 IP 地址，从而获取访问您网络的权限。这种情况可能会发生，因为您创建的访问控制规则需要允许地址池访问内部资源。如果您使用访问控制规则，请考虑使用用户说明来控制访问，而不是只使用源 IP 地址。选择此选项的弊端在于，VPN 流量将不会被检测，也就是说不会对流量应用入侵和文件保护、URL 过滤或其他高级功能。同时，系统不会生成有关此流量的任何连接事件，且统计控制面板不会反映 VPN 连接。

- **NAT 豁免 (NAT Exempt):** 启用 NAT 豁免，使进出远程访问 VPN 终端的流量免于执行 NAT 转换。如果不豁免 VPN 流量执行 NAT，请确保外部和内部接口的现有 NAT 规则不适用于 RA VPN 地址池。NAT 豁免规则是给定源/目标接口和网络组合的手动静态身份 NAT 规则，但它们不会反映在 NAT 策略中，它们是隐藏起来的。如果启用 NAT 豁免，还必须进行以下配置。
 - **内部接口:** 选择远程用户将要访问的内部网络的接口。所创建的 NAT 规则用于这些接口。
 - **内部网络:** 选择代表远程用户将访问的内部网络的网络对象。网络列表必须包含与您支持的地址池相同的 IP 类型。

步骤 5 点击确定 (OK)。

- 如果您已载入 防火墙设备管理器 版本 6.4.0 设备，则检测到的 **AnyConnect** 软件包会显示设备中可用的 AnyConnect 软件包。
- 如果您已载入 防火墙设备管理器 版本 6.5.0 或更高版本的设备，则必须从预上传 AnyConnect 软件包的服务器添加 AnyConnect 软件包。有关说明，请参阅[将 AnyConnect 软件包上传到运行 FDM 管理 6.5 或更高版本的设备](#)。

步骤 6 点击确定 (OK)。设备已添加到配置中。

What to do next



Note 选择配置，然后在操作下点击相应的操作：

- **Group Policies**，用于添加或删除组策略。
 - 点击 + 选择所需的组策略。要创建新的 RA VPN 组策略，请参阅[创建新的 RA VPN 组策略](#)。
- **删除 (Remove)** 以删除所选的 RA VPN 配置。



修改 RA VPN 配置

您可以修改现有 RA VPN 配置的名称和设备详细信息。

Procedure

选择要修改的配置，然后在操作下点击编辑。

- 如果需要，请修改名称。

- 点击蓝色加号按钮  以添加新设备。
- 点击以在设备上执行以下操作。  FDM 管理
 - 点击编辑以修改现有的 RA VPN 配置。
 - 点击删除以从 RA VPN 配置中删除设备。FDM 管理除组策略外，与该设备关联的所有连接配置文件和 RA VPN 设置都将被删除。您可以从对象页面中明确删除组策略。注意：如果该设备是唯一使用该配置的设备，则无法删除该设备。FDM 管理或者，您可以删除 RA VPN 配置。

您还可以通过键入配置或设备的名称来搜索远程接入 VPN 配置。

相关信息：

- [配置 RA VPN 连接配置文件](#)。
- [预览和部署所有设备的配置更改](#)。
- [允许流量通过远程访问 VPN](#)。

配置 RA VPN 连接配置文件

RA VPN 连接配置文件定义了一些特征，这些特征允许外部用户使用 AnyConnect 客户端与系统创建 VPN 连接。每个配置文件都定义了用于用户身份验证的 AAA 服务器和证书、分配用户 IP 地址的地址池，以及定义各种面向用户的属性的组策略。

如果需要为不同的用户组提供不同的服务，或者有不同的身份验证源，您可以在 RA VPN 配置中创建多个配置文件。例如，如果您的组织与使用不同身份验证服务器的组织合并，您可以为使用这些身份验证服务器的新组创建配置文件。

远程访问 VPN 连接配置文件让您的用户可在外部网络（例如其家庭网络）上时连接到您的内部网络。创建单独的配置文件，以适应不同的身份验证方法。

准备工作

在配置远程访问 (RA) VPN 连接之前：

- 外部接口（作为远程访问 VPN 连接终端的那个外部接口）也不能具有允许 HTTPS 连接的管理访问列表。在配置 RA VPN 之前，从外部接口删除所有 HTTPS 规则。请参阅《[适用于 Firepower 设备管理器版本 X.Y 的思科 Firepower 威胁防御配置指南](#)》的“系统设置”一章中的“配置管理访问列表”部分。
- 创建 RA VPN 配置。请参阅创建 RA VPN 配置。[创建 RA VPN 配置, on page 259](#)

操作步骤

Procedure

- 步骤 1** 在 CDO 导航窗格中，点击 **VPN > 远程访问 VPN 配置 (Remote Access VPN Configuration)**。您可以点击 VPN 配置以查看当前已配置多少连接配置文件和组策略的摘要信息。
- 步骤 2** 点击连接配置文件，然后在右侧边栏中的操作下点击 **添加连接配置文件**。
- 步骤 3** 配置基本连接属性。
- **连接配置文件名称 (Connection Profile Name):** 此连接的名称，最多 50 个字符，不能含空格。例如，MainOffice。
- Note** 您在此输入的名称将是用户在 AnyConnect 客户端的连接列表中看到的名称。选择一个对您的用户来说有意义的名称。
- **组别名、组 URL (Group Alias, Group URL):** 别名包含特定连接配置文件的备用名称或 URL。在连接到 FDM 管理设备时，VPN 用户可以在连接列表中的 AnyConnect 客户端中选择别名。连接配置文件名称会自动添加为组别名。您还可以配置组 URL 列表，在发起远程访问 VPN 连接时您的终端可以从该列表中进行选择。如果用户使用组 URL 进行连接，系统将自动使用与 URL 匹配的连接配置文件。此 URL 供尚未安装 AnyConnect 客户端的客户使用。按需要添加组别名和 URL。在设备上定义的所有连接配置文件中，这些别名和 URL 必须是唯一的。组 URL 必须以 **https://** 开头。
 - 例如，您可能有别名承包商和组 URL <https://ravpn.example.com/contractor>。安装 AnyConnect 客户端后，用户只需在连接的 AnyConnect VPN 下拉列表中选择组别名。
- 步骤 4** 配置主身份源和辅助身份源（可选）。这些选项确定设备如何对远程用户进行身份验证，以启用远程访问 VPN 连接。最简单的方法是仅使用 AAA，然后选择 AD 领域或使用 LocalIdentitySource。根据 **身份验证类型**，您可以使用以下方法：
- **仅 AAA (AAA Only):** 根据用户名和密码对用户进行身份验证和授权。有关详细信息，请参阅 [为连接配置文件配置 AAA](#)。
 - **仅客户端证书 (Client Certificate Only):** 根据客户端设备身份证书进行用户身份验证。有关详细信息，请参阅 [为连接配置文件配置证书身份验证](#)。
 - **AAA 和 ClientCertificate (AAA and ClientCertificate):** 同时使用用户名/密码和客户端设备身份证书。
- 步骤 5** 配置客户端的地址池。地址池定义了远程客户端在建立 VPN 连接时，系统可以分配给它们的 IP 地址。有关详细信息，请参阅 [配置客户端地址池分配](#)。
- 步骤 6** 点击 **继续 (Continue)**。
- 步骤 7** 从列表中选择要用于此配置文件的 **组策略**，然后点击 **选择 (Select)**。组策略在建立隧道后设置用户连接的条款。系统包含名为 DfltGrpPolicy 的默认组策略。您可以创建其他组策略，以提供您所需的服务。
- Note** 如果所需的组策略尚不存在，请在 **对象** 页面上创建组策略，然后将该策略与 RA VPN 配置相关联。有关组策略的详细信息，请参阅 [创建新的 RA VPN 组策略](#)。

步骤 8 点击继续 (Continue)。

步骤 9 审核摘要。首先，验证摘要是否正确。您可以查看最终用户初步安装 AnyConnect 软件需要做什么，



并测试他们是否可以完成 VPN 连接。点击  将这些说明复制到剪贴板，然后分发给您的用户。

步骤 10 点击完成 (Done)。

What to do next

确保 VPN 隧道中允许流量，如 [允许流量通过远程访问 VPN](#) 中所述。

为连接配置文件配置 AAA

身份验证、授权和记账 (AAA) 服务器使用用户名和密码来确认是否允许用户访问远程访问 VPN。如果使用 RADIUS 服务器，则可以区分已验证用户的授权级别，从而提供对受保护资源的差异化访问权限。还可以使用 RADIUS 记账服务来跟踪使用情况。

在配置 AAA 时，您必须配置主身份源。辅助源和备用源是可选的。如果想要实施双重身份验证，请使用辅助源，例如，RSA 令牌或 DUO。

主身份源选项

- **用户身份验证的主身份源 (Primary Identity Source for User Authentication):** 用于对远程用户进行身份验证的主要身份源。必须在此源或可选的回退源中定义最终用户，才能完成 VPN 连接。选择以下一个选项：
 - Active Directory (AD) 身份领域。如果所需的领域尚不存在，请点击 [创建新身份领域](#)。
 - RADIUS 服务器组。
 - LocalIdentitySource (本地用户数据库)：您可以直接在设备上定义用户，而不使用外部服务器。
- **回退本地身份源 (Fallback Local Identity Source):** 如果主要源是一个外部服务器，您可以选择 LocalIdentitySource 作为回退源，以防主服务器不可用。如果使用本地数据库作为回退源，请确保您定义的本地用户名/密码与外部服务器中的定义的用户名/密码相同。
- **删除选项 (Strip options):** 领域是管理域。启用以下选项将允许仅基于用户名进行身份验证。您可以启用这些选项的任意组合。但是，如果服务器无法分析分隔符，则必须选中这两个复选框。
 - **从用户名删除身份源服务器 (Strip Identity Source Server from Username):** 在将用户名传递到 AAA 服务器之前，是否要从用户名删除身份源名称。例如，如果选择此选项且用户输入域用户名作为用户名，则该域将从用户名中删除，并发送到 AAA 服务器进行身份验证。默认情况下，此选项处于取消选中状态。

- **从用户名删除组 (Strip Group from Username):** 在将用户名传递到 AAA 服务器之前，是否要从用户名删除组名称。此选项适用于 username@domain 格式中给定的名称；此选项会剥离域和 @ 符号。默认情况下，此选项处于取消选中状态。

辅助身份源

- **用于用户授权的辅助身份源 (Secondary Identity Source for User Authorization):** 可选的第二个身份源。如果用户成功使用主要源进行身份验证，则系统会提示其使用辅助源进行身份验证。可以选择 AD 领域、RADIUS 服务器组或本地身份源。
- **高级 (Advanced) 选项:** 点击高级 (Advanced) 链接并配置以下选项：
 - **辅助源的备用本地身份源 (Fallback Local Identity Source for Secondary):** 如果辅助源为外部服务器，您可以选择 LocalIdentitySource 作为备用源，以防辅助服务器不可用。如果使用本地数据库作为备用源，请确保您定义的本地用户名/密码与辅助外部服务器中定义的用户名/密码相同。
 - **使用主要用户名进行辅助登录 (Use Primary Username for Secondary Login):** 默认情况下，使用辅助身份源时，系统将提示输入辅助源的用户名和密码。如果选择此选项，系统将提示您输入辅助密码，并使用与主身份源相同的用户名来进行辅助源身份验证。如果您在主身份源和辅助身份源中配置了相同的用户名，请选择此选项。
 - **会话服务器用户名 (Username for Session Server):** 身份验证成功后，用户名将显示在事件和统计控制面板中，用于确定基于用户或组的 SSL 解密和访问控制规则之间的匹配关系，并用于记账。由于使用了两个身份验证源，因此您需要告诉系统是使用主用户名还是辅助用户名作为用户身份。默认情况下，使用主用户名。
 - **密码类型 (Password Type):** 如何获取辅助服务器的密码。默认值为提示，这表明系统将提示用户输入密码。选择主身份源密码，自动使用用户在主服务器中进行身份验证时输入的密码。选择公用密码，为每个用户使用相同的密码，然后在公用密码字段中输入该密码。
 - **授权服务器 (Authorization Server):** 已配置为授权远程访问 VPN 用户的 RADIUS 服务器组。身份验证完成后，授权将控制对每个经过身份验证的用户都可用的服务和命令。授权通过组合一组描述用户被授权执行的操作、其实际功能和限制的属性来工作。如果您不使用授权，则单独的身份验证将为所有经过身份验证的用户提供相同的访问权限。有关配置 RADIUS 进行授权的信息，请参阅使用 RADIUS 和组策略控制用户权限和属性。[使用 RADIUS 和组策略控制用户权限和属性, on page 224](#) 请注意，如果系统从 RADIUS 服务器获取的授权属性与组策略中定义的属性重叠，则 RADIUS 属性将覆盖组策略属性。
 - **记账服务器 (Accounting Server):** (可选。) 用于为远程访问 VPN 会话记账的 RADIUS 服务器组。记账会跟踪用户正在访问的服务以及他们正在使用的网络资源数量。FTD 设备向 RADIUS 服务器报告用户活动。记账信息包括每个会话的开始和停止时间、用户名、会话时通过设备的字节数、使用的服务以及每个会话的持续时间。然后，您可分析该数据，以进行网络管理、客户端计费或审核。您可以单独使用记账功能，也可以将其与身份验证和授权功能配合使用。

为连接配置文件配置证书身份验证



Note 此部分不适用于仅作为 AAA 的身份验证类型。

可以使用客户端设备安装的证书对远程接入 VPN 连接进行身份验证。

使用客户端证书时，仍可以配置辅助身份源、备用源，以及授权和记账服务器。这些是 AAA 选项；有关详细信息，请参阅配置 RA VPN 连接配置文件。[配置 RA VPN 连接配置文件, on page 262](#)

以下是证书特定的属性。您可以为主身份源和辅助身份源单独配置这些属性。配置辅助源为可选操作。

- **从证书中获取的用户名 (Username from Certificate):** 选择以下选项之一：
 - **映射特定字段 (Map Specific Field):** 按照主要字段 (**Primary Field**) 和辅助字段 (**Secondary Field**) 的顺序使用证书元素。默认值为 CN (公用名) 和 OU (组织单位)。选择适用于您的组织的选项。这些字段组合在一起用于提供用户名，此名称用于事件和控制面板中，并出于匹配的目的，在 SSL 解密和访问控制规则中使用。
 - **使用完整 DN (可分辨名称) 作为用户名 (Use entire DN [distinguished name] as username):** 系统自动从 DN 字段派生出用户名。
- **高级选项 (不适用于作为仅客户端证书的身份验证类型):** 点击高级链接并配置以下选项：
 - **在用户登录窗口预填证书中的用户名 (Prefill username from certificate on user login window):** 在提示用户进行身份验证时，是否在用户名字段填写检索到的用户名。
 - **在登录窗口隐藏用户名 (Hide username in login window):** 如果选择预填充 (**Prefill**) 选项，则可以隐藏用户名，这意味着用户无法编辑密码提示中的用户名。

配置客户端地址池分配

系统必须可以通过某种方法向连接到远程访问 VPN 的终端提供 IP 地址。AAA 服务器、DHCP 服务器、组策略中配置的 IP 地址池，或连接配置文件中配置的 IP 地址池可以提供这些地址。系统会按照以上顺序尝试使用这些资源，并在获取一个可用地址后停止尝试，然后将此地址分配给客户端。因此，您可以配置多个选项，以便在并发连接数异常多的情况下，可保障系统能获取地址。

使用下列一个或多个方法配置连接配置文件的地址池。

- **IPv4 地址池和 IPv6 地址池:** 首先，创建最多六个指定子网的网络对象。可以为 IPv4 和 IPv6 单独配置池。然后，在组策略或者连接配置文件的 **IPv4 地址池 (IPv4 Address Pool)** 和 **IPv6 地址池 (IPv6 Address Pool)** 选项中，选择这些对象。无需同时配置 IPv4 和 IPv6，配置您想要支持的寻址方案即可。也不需要同时在组策略和连接配置文件中配置池。组策略会覆盖连接配置文件的设置，因此如果您在组策略中配置了池，则请将连接配置文件中的选项留空。请注意，系统按照您列出的顺序使用地址池。
- **DHCP 服务器 (DHCP Servers):** 首先，使用一个或多个 IPv4 地址范围为 RA VPN 配置 DHCP 服务器（您无法使用 DHCP 配置 IPv6 池）。然后，使用 DHCP 服务器的 IP 地址创建主机网络对象。随后，便可以在连接配置文件的 **DHCP 服务器 (DHCP Servers)** 属性中选择此对象。可

以配置多个 DHCP 服务器。如果 DHCP 服务器有多个地址池，则可以在与连接配置文件关联的组策略中使用 **DHCP 作用域 (DHCP Scope)** 属性，选择要使用的池。使用池的网络地址创建主机网络对象。例如，如果 DHCP 池包含 192.168.15.0/24 和 192.168.16.0/24，将 DHCP 范围设置为 192.168.16.0 可确保从 192.168.16.0/24 子网中选择地址。

允许流量通过远程访问 VPN

可以使用以下方法之一来启用远程访问 VPN 隧道中的流量。

- 配置 **sysopt connection permit-vpn** 命令，此命令会使匹配 VPN 连接的流量免受访问控制策略的限制。此命令的默认值是 **no sysopt connection permit-vpn**，这意味着 VPN 流量的通过还必须获得访问控制策略的允许。外部用户无法在远程访问 VPN 地址池中伪造 IP 地址，因此这种允许 VPN 流量的方法较为安全。但它的缺点是，VPN 流量得不到检测，也就是说不会对流量应用入侵和文件保护、URL 过滤或其他高级功能。同时，系统不会生成有关此流量的任何连接事件，且统计控制面板不会反映 VPN 连接。要配置此命令，请在 RA VPN 配置中选择为 **已解密的流量绕过访问控制策略 (Bypass Access Control policy for decrypted traffic)** 选项。请参阅创建 RA VPN 配置。[创建 RA VPN 配置, on page 259](#)
- 创建访问控制规则以允许来自远程访问 VPN 地址池的连接。此方法可确保对 VPN 流量进行检测，并将高级服务应用于连接。但它的缺点是，有可能造成外部用户伪造 IP 地址，进而获得访问内部网络的权限。请参阅[配置 FDM 访问控制策略](#)。

在运行版本 6.4.0 的 FDM 管理设备上升级 AnyConnect 软件包

您可以使用思科防御协调器升级 FDM 管理设备上可用的 AnyConnect 软件包，以便将其分发给 RA VPN 用户。

以下是升级 AnyConnect 软件包所涉及的主要步骤：

Procedure

步骤 1 使用 防火墙设备管理器 来删除 AnyConnect 软件包并上传该软件包的更高版本。使用其中一种方法来完成此任务。

- 删除旧软件包并从 防火墙设备管理器 UI 上传新软件包。
- 删除旧软件包并从 防火墙设备管理器 API 资源管理器上传新软件包。

步骤 2 将 防火墙设备管理器 更改部署到设备。

步骤 3 将新配置信息读入 CDO。

步骤 4 验证 RA VPN 连接配置文件中的新软件包。

前提条件

- 至少一个具有连接配置文件的 RA VPN 配置已部署到设备。FDM 管理

- 从 <https://software.cisco.com/download/home/283000185> 下载您想要的 AnyConnect 软件包。思科建议升级到最新的可用软件包。

使用 防火墙设备管理器 将所需的 AnyConnect 软件包上传到 Secure Firewall Threat Defense

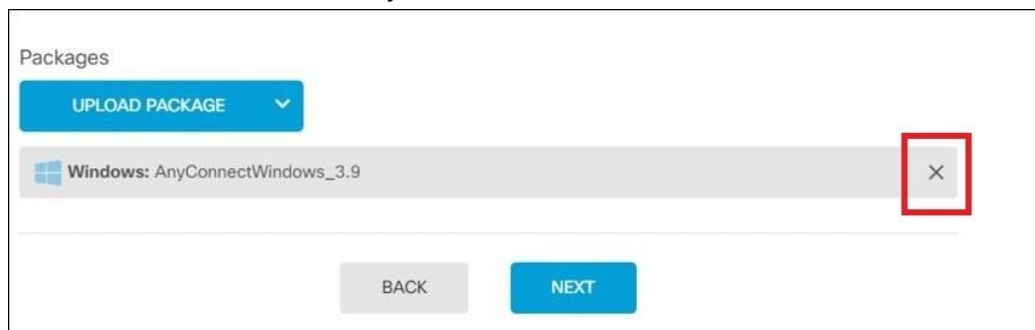
Procedure

- 步骤 1** 使用浏览器打开系统主页。例如，<https://ftd.example.com>。 <https://ftd.example.com/>
- 步骤 2** 登录至 防火墙设备管理器。
- 步骤 3** 在设备 (Device) > 远程访问 VPN (Remote Access VPN) 中点击查看配置 (View Configuration)。该组显示有关当前已配置多少连接配置文件和组策略的摘要信息。

- 步骤 4** 点击查看按钮 () 按钮 (查看 (View) 配置按钮)，打开连接配置文件和连接说明的摘要。

Note 您可以编辑任何一个连接配置文件，以将 AnyConnect 软件包上传到 FDM 管理设备。

- 步骤 5** 点击编辑 (Edit) 按钮以进行更改。
- 步骤 6** 点击下一步，直到显示全局设置屏幕。AnyConnect 软件包会显示 FDM 管理设备上可用的 AnyConnect 软件包。
- 步骤 7** 点击“X”按钮删除要替换的 AnyConnect 软件包。



- 步骤 8** 点击上传软件包，然后点击要上传兼容软件包的操作系统。
- 步骤 9** 选择软件包，然后点击打开 (Open)。您可以在 防火墙设备管理器 UI 上看到正在上传的软件包。
- 步骤 10** 点击完成。配置已保存。

Note 或者，您可以使用 防火墙设备管理器 API 资源管理器删除并上传新的 AnyConnect 软件包。

- 编辑 URL，使其指向 `/#/api-explorer`，例如 <https://ftd.example.com/#/api-explorer>。
- 从 FDM 管理设备中删除软件包，点击 `AnyConnectPackageFile` > 删除 (Delete)。在 objID 字段中，键入软件包 ID，然后点击试用！
- 通过执行将 AnyConnect 软件包上传到 Firepower 威胁防御设备部分中所述的步骤上传新软件包。
将 AnyConnect 软件包上传到运行版本 6.4.0 的 FDM 管理设备, on page 239

- 步骤 11** 点击网页右上角的**部署更改 (Deploy Changes)** 图标。若有未部署的更改，系统会用圆点高亮显示。
- 步骤 12** 如果您对所做的更改比较满意，可以点击**立即部署 (Deploy Now)** 立即启动作业。窗口将显示部署正在进行。您可以关闭窗口，或等待部署完成。

验证 RA VPN 连接配置文件中是否引用了新软件包

Procedure

- 步骤 1** 在左侧的 CDO 导航栏中，点击**清单 (Inventory)**。
- 步骤 2** 点击**设备**选项卡。
- 步骤 3** 点击**FTD** 选项卡，然后选择具有升级的 AnyConnect 软件包的 FTD 设备。此设备将报告冲突。
- 步骤 4** 接受带外更改，以使用设备的运行配置覆盖 CDO 上存储的配置和任何待定更改。有关详细信息，请参阅[解决“检测到冲突”状态](#)。
- 步骤 5** 通过执行以下操作查看新的 AnyConnect 软件包：
- 点击**VPN > 远程访问 VPN (Remote Access VPN)**。
 - 点击与此 FTD 设备关联的 RA VPN 配置。
 - 点击**操作**下的**编辑**。新软件包显示在**设备**下。

上传 RA AnyConnect 客户端配置文件

远程接入 VPN AnyConnect 客户端配置文件是存储在文件中的一组配置参数。这些不同的 AnyConnect 客户端配置文件包含核心客户端 VPN 功能和可选客户端模块网络访问管理器、AMP 启动器、ISE 终端安全评估、网络可视性、客户体验反馈、Umbrella 漫游安全和网络安全的配置设置。

CDO 允许将这些配置文件作为对象上传，以便稍后在组策略中使用。

- **AnyConnect VPN 配置文件 (AnyConnect VPN Profile)** - AnyConnect 客户端配置文件随 AnyConnect 客户端软件一起下载到客户端。这些配置文件定义与客户端相关的诸多选项，例如启动时自动连接和自动重新连接，以及最终用户是否可以更改 AnyConnect 客户端首选项和高级设置中的选项。CDO 支持 XML 文件格式。
- **AMP 启用程序服务配置文件 (AMP Enabler Service Profile)** - 该配置文件用于 AnyConnect AMP 启用程序。当远程访问 VPN 用户连接到 VPN 时，AMP 启动器和此配置文件会从 FDM 管理设备推送到终端。CDO 支持 XML 和 ASP 文件格式。
- **反馈配置文件 (Feedback Profile)** - 您可以添加客户体验反馈配置文件并选择此类型，以接收有关客户已启用和使用的功能和模块的信息。CDO 支持 FSP 文件格式。
- **ISE 终端安全评估配置文件 (ISE Posture Profile)** - 如果要为 AnyConnect ISE 终端安全评估模块添加配置文件，请选择此选项。CDO 支持 XML 和 ISP 文件格式。


- **网络访问管理器服务配置文件 (Network Access Manager Service Profile)** - 使用网络访问管理器配置文件编辑器配置和添加 NAM 配置文件。CDO 支持 XML 和 NSP 文件格式。
- **网络可视性服务配置文件 (Network Access Manager Service Profile)** - AnyConnect 网络可视性模块的配置文件。您可以使用 NVM 配置文件编辑器创建配置文件。CDO 支持 XML 和 NVMSPP 文件格式。
- **Umbrella 漫游安全配置文件 (Umbrella Roaming Security Profile)** - 如果部署 Umbrella 漫游安全模块，则必须选择此文件类型。CDO 支持 XML 和 JSON 文件格式。
- **网络安全服务配置文件 (Web Security Service Profile)** - 在为网络安全模块添加配置文件时选择此文件类型。CDO 支持 XML、WSO 和 WSP 文件格式。

Before you begin

使用适当的基于 GUI AnyConnect 配置文件编辑器创建所需的配置文件。您可以从[思科软件下载中心](#)的 AnyConnect 安全移动客户端类别下载配置文件编辑器，并安装 AnyConnect “配置文件编辑器 - Windows/独立安装程序 (MSI)” (Profile Editor - Windows / Standalone installer [MSI])。配置文件编辑器安装程序包含独立版本的配置文件编辑器。此安装文件仅适用于 Windows，文件名为 anyconnect-profileeditor-win-<version>-k9.msi，其中 <version> 指 AnyConnect 版本。例如，anyconnect-profileeditor-win-4.3.04027-k9.msi。您还必须在安装配置文件编辑器之前安装 Java JRE 1.6（或更高版本）。

除 Umbrella 漫游安全配置文件编辑器外，此软件包包含创建模块所需的所有配置文件编辑器。有关详细信息，请参阅相应版本的《[思科 AnyConnect 安全移动客户端管理员指南](#)》中的 *AnyConnect* 配置文件编辑器一章。从 Umbrella 控制面板单独下载 Umbrella 漫游安全配置文件。有关详细信息，请参阅《[思科 Umbrella 用户指南](#)》中“Umbrella 漫游安全”一章的“从 Umbrella 控制面板下载 AnyConnect 漫游安全配置文件”部分。

Procedure

- 步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
- 步骤 2** 点击“加号”  按钮。
- 步骤 3** 点击 **RA VPN 对象 (ASA 和 FDM) (RA VPN Objects [ASA & FDM]) > AnyConnect 客户端配置文件 (AnyConnect Client Profile)**。
- 步骤 4** 在**对象名称 (Object Name)** 字段中输入 AnyConnect 客户端配置文件名称。
- 步骤 5** 点击**浏览 (Browse)** 并选择使用配置文件编辑器创建的文件。
- 步骤 6** 点击打开上传配置文件。
- 步骤 7** 点击**添加 (Add)** 以添加对象。

相关信息：

- 将客户端模块与 RA VPN 组策略窗口中的 AnyConnect VPN 配置文件关联。请参阅 [创建新的 RA VPN 组策略](#)。



Note 所有 ASA 版本和运行软件版本 6.7 或更高版本的 FDM 都支持客户端模块关联。

FDM 管理 设备的远程访问 VPN 准则和限制

配置 RA VPN 时，请时刻注意以下准则和限制。

- 必须使用 防火墙设备管理器 将 AnyConnect 软件包预加载到运行版本 6.4.0 的 FDM 管理设备。



Note 使用 思科防御协调器 中的远程接入 VPN 配置向导将 AnyConnect 软件包单独上传到运行版本 6.5.0 的 FDM 管理 设备。

- 从 CDO 配置 RA VPN 之前：
 - 从 防火墙设备管理器 为 FDM 管理 设备注册许可证。
 - 通过导出控制从 防火墙设备管理器 启用许可证。
- CDO 不支持扩展访问列表对象。在 防火墙设备管理器 中使用 Smart CLI 配置对象，然后在 VPN 过滤器和授权更改 (CoA) 重定向 ACL 中使用。
- 您从设备创建的模板将不包含 RA VPN 配置。FDM 管理
- IP 池对象和 RADIUS 身份源需要设备特定的覆盖。
- 对于同一个 TCP 端口，无法在同一接口上同时配置 防火墙设备管理器 访问（管理访问列表中的 HTTPS 访问）和 AnyConnect 远程访问 SSL VPN。例如，如果在外部接口上配置远程访问 SSL VPN，则也无法在端口 443 上打开 HTTPS 连接的外部接口。因为无法在 防火墙设备管理器 中配置这些功能所使用的端口，所以无法在同一接口上配置这两项功能。
- 如果您使用 RADIUS 和 RSA 令牌配置双因素身份验证，则在大多数情况下，12 秒的默认身份验证超时太短，无法实现成功的身份验证。通过创建自定义 AnyConnect 客户端配置文件并将其应用到 RA VPN 连接配置文件，来增加身份验证超时值，如 [上传 RA AnyConnect 客户端配置文件, on page 269](#) 中所述。建议身份验证超时时间最短为 60 秒，以使用户有足够的时间进行身份验证并粘贴 RSA 令牌，以及进行令牌往返验证。

用户如何在 FDM 管理设备上安装 AnyConnect 客户端软件

使用 防火墙设备管理器 API 将 AnyConnect 客户端软件包上传到 FDM 管理 设备以分发给用户。请参阅将 AnyConnect 软件包上传到 Firepower 威胁防御设备。 [将 AnyConnect 软件包上传到运行版本 6.4.0 的 FDM 管理设备, on page 239](#)

要完成 VPN 连接，您的用户必须安装 AnyConnect 客户端软件。可以使用现有的软件分发方法直接安装该软件。或者，可以让用户直接从 FDM 管理设备安装 AnyConnect 客户端。



Note 用户必须对其工作站具有管理员权限才能安装软件。

如果您决定让用户一开始从 FDM 管理 设备安装软件，请告知用户执行以下步骤。



Note Android 和 iOS 用户应从相应的应用商店下载 AnyConnect。

Procedure

- 步骤 1** 使用 Web 浏览器，打开 <https://ravpn-address>，其中 *ravpn-address* 是您允许 VPN 连接的外部接口的 IP 地址或主机名。您在配置远程访问 VPN 时确定此接口。系统提示用户登录。
- 步骤 2** 登录到网站。用户使用为远程访问 VPN 配置的目录服务器进行身份验证。登录成功后可继续操作。如果登录成功，系统将确定用户是否已具有所需的 AnyConnect 客户端版本。如果用户的计算机上没有 AnyConnect 客户端，或者客户端的版本较低，系统将自动开始安装 AnyConnect 软件。安装后，AnyConnect 会完成远程接入 VPN 连接。

分发新的 AnyConnect 客户端软件版本

您可以将新版本的 AnyConnect 客户端软件上传到设备，而不删除旧版本。FDM 管理成功上传 AnyConnect 客户端后，您可以删除旧版本。

AnyConnect 客户端在用户建立的下一个 VPN 连接上检测新版本。系统将自动提示用户下载并安装更新的客户端软件。这种自动化可为您和您的客户端简化软件分发。

下图显示了具有适用于 Windows 操作系统的两个版本 AnyConnect 客户端软件（AnyConnectWindows_3.2_BGL 和 AnyConnectWindows_4.2_BGL）的设备示例。FDM 管理

Response Body

```
{
  "items": [
    {
      "version": "nh14yz7tgfgva",
      "name": "AnyConnectWindows_3.2_BGL",
      "description": null,
      "diskFileName": "f3b4daa9-a3b3-11e9-a361-f958979569cd.pkg",
      "md5Checksum": "bf3013d9e8ce52e905ba4bd4495678c0",
      "platformType": "WINDOWS",
      "id": "3f3a329a-a3b4-11e9-a361-338c2bfc8d92",
      "type": "anyconnectpackagefile",
      "links": {
        "self": "https://bg1grp1224-pod.cisco.com:972/api/fdm/v3/object/anyconnectpackagefiles/3f3a329a-a3b4-11e9-a361-338c2bfc8d92"
      }
    },
    {
      "version": "d51dzvydhbn26",
      "name": "AnyConnectWindows_4.2_BGL",
      "description": null,
      "diskFileName": "ae43a4ad-a3b4-11e9-a361-5f4e70129b91.pkg",
      "md5Checksum": "ac1269fd5d172705954f093d56735d76",
    }
  ]
}
```


上传 RA AnyConnect 客户端配置文件

远程接入 VPN AnyConnect 客户端配置文件是存储在文件中的一组配置参数。这些不同的 AnyConnect 客户端配置文件包含核心客户端 VPN 功能和可选客户端模块网络访问管理器、AMP 启动器、ISE 终端安全评估、网络可视性、客户体验反馈、Umbrella 漫游安全和网络安全的配置设置。

CDO 允许将这些配置文件作为对象上传，以便稍后在组策略中使用。


- **AnyConnect VPN 配置文件 (AnyConnect VPN Profile)** - AnyConnect 客户端配置文件随 AnyConnect 客户端软件一起下载到客户端。这些配置文件定义与客户端相关的诸多选项，例如启动时自动连接和自动重新连接，以及最终用户是否可以更改 AnyConnect 客户端首选项和高级设置中的选项。CDO 支持 XML 文件格式。
- **AMP 启用程序服务配置文件 (AMP Enabler Service Profile)** - 该配置文件用于 AnyConnect AMP 启用程序。当远程访问 VPN 用户连接到 VPN 时，AMP 启动器和此配置文件会从 FDM 管理设备推送到终端。CDO 支持 XML 和 ASP 文件格式。
- **反馈配置文件 (Feedback Profile)** - 您可以添加客户体验反馈配置文件并选择此类型，以接收有关客户已启用和使用的功能和模块的信息。CDO 支持 FSP 文件格式。
- **ISE 终端安全评估配置文件 (ISE Posture Profile)** - 如果要为 AnyConnect ISE 终端安全评估模块添加配置文件，请选择此选项。CDO 支持 XML 和 ISP 文件格式。
- **网络访问管理器服务配置文件 (Network Access Manager Service Profile)** - 使用网络访问管理器配置文件编辑器配置和添加 NAM 配置文件。CDO 支持 XML 和 NSP 文件格式。
- **网络可视性服务配置文件 (Network Access Manager Service Profile)** - AnyConnect 网络可视性模块的配置文件。您可以使用 NVM 配置文件编辑器创建配置文件。CDO 支持 XML 和 NVMSPP 文件格式。
- **Umbrella 漫游安全配置文件 (Umbrella Roaming Security Profile)** - 如果部署 Umbrella 漫游安全模块，则必须选择此文件类型。CDO 支持 XML 和 JSON 文件格式。
- **网络安全服务配置文件 (Web Security Service Profile)** - 在为网络安全模块添加配置文件时选择此文件类型。CDO 支持 XML、WSO 和 WSP 文件格式。

Before you begin

使用适当的基于 GUI AnyConnect 配置文件编辑器创建所需的配置文件。您可以从[思科软件下载中心](#)的 AnyConnect 安全移动客户端类别下载配置文件编辑器，并安装 AnyConnect “配置文件编辑器 - Windows/独立安装程序 (MSI)” (Profile Editor - Windows / Standalone installer [MSI])。配置文件编辑器安装程序包含独立版本的配置文件编辑器。此安装文件仅适用于 Windows，文件名为 anyconnect-profileeditor-win-<version>-k9.msi，其中 <version> 指 AnyConnect 版本。例如，anyconnect-profileeditor-win-4.3.04027-k9.msi。您还必须在安装配置文件编辑器之前安装 Java JRE 1.6 (或更高版本)。

除 Umbrella 漫游安全配置文件编辑器外，此软件包包含创建模块所需的所有配置文件编辑器。有关详细信息，请参阅相应版本的《[思科 AnyConnect 安全移动客户端管理员指南](#)》中的 *AnyConnect* 配置文件编辑器一章。从 Umbrella 控制面板单独下载 Umbrella 漫游安全配置文件。有关详细信息，请参阅《[思科 Umbrella 用户指南](#)》中“Umbrella 漫游安全”一章的“从 Umbrella 控制面板下载 AnyConnect 漫游安全配置文件”部分。

Procedure

- 步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
- 步骤 2 点击“加号”  按钮。
- 步骤 3 点击 **RA VPN 对象 (ASA 和 FDM) (RA VPN Objects [ASA & FDM]) > AnyConnect 客户端配置文件 (AnyConnect Client Profile)**。
- 步骤 4 在对象名称 (**Object Name**) 字段中输入 AnyConnect 客户端配置文件名称。
- 步骤 5 点击浏览 (**Browse**) 并选择使用配置文件编辑器创建的文件。
- 步骤 6 点击打开上传配置文件。
- 步骤 7 点击添加 (**Add**) 以添加对象。

相关信息：

- 将客户端模块与 RA VPN 组策略窗口中的 AnyConnect VPN 配置文件关联。请参阅 [创建新的 RA VPN 组策略](#)。



Note 所有 ASA 版本和运行软件版本 6.7 或更高版本的 FDM 都支持客户端模块关联。

远程访问 VPN 的许可要求

从防火墙设备管理器为 FDM 管理设备启用（注册）许可证，以配置 RA VPN 连接。注册设备时，必须使用启用了出口控制功能的智能软件管理器 (SSM) 账户。您也不能使用评估许可证配置该功能。

此外，您必须购买并启用许可证；它可以是以下任何一项：。即使这些许可证被设计为在与基于 ASA 软件的头端一起使用时允许不同的功能集，它们对于 FDM 管理设备都同等处理。

有关从防火墙设备管理器启用许可证的详细信息，请参阅《[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#)》中“远程访问 VPN”一章中的远程访问 VPN 的许可要求部分。

有关详细信息，请参阅《[思科 AnyConnect 订购指南](#)》。

<http://www.cisco.com/c/en/us/product...t-listing.html> 上还提供了其他数据表。

要查看许可证状态，请执行以下操作：

Procedure

- 步骤 1 在左侧的 思科防御协调器 导航栏中，点击 **清单 (Inventory)**。
- 步骤 2 点击 **设备 (Devices)**。
- 步骤 3 点击 **FTD** 选项卡，然后选择所需的设备。

步骤 4 在右侧的设备操作窗格中，点击**管理许可证**。如果许可证有效，则状态显示为**已启用**。

各设备型号的最大并发 VPN 会话数量

根据设备型号，设备上允许的并发远程接入 VPN 会话数量有最大值限制。此限制用于确保系统性能不会降低到不可接受的水平。请使用这些限制进行容量规划。

设备型号	最大并发远程接入 VPN 会话数
Firepower 2110	1,500
Firepower 2120	3,500
Firepower 2130	7500
Firepower 2140	10,000
Firepower 威胁防御虚拟	250

RADIUS 授权更改

RADIUS 更改授权 (CoA) 功能提供了一种机制，可在通过身份验证后更改身份验证、授权和记账 (AAA) 会话的属性。RA VPN 的一个主要挑战是保护 内部网络免遭受攻击终端感染，并在终端受病毒或恶意软件感染时，在终端上采取补救措施来保护终端。有必要在所有阶段（即，在 RA VPN 会话之前、过程中和之后）保护终端和内部网络。RADIUS CoA 功能有助于实现此目标。

如果使用思科身份服务引擎 (ISE) RADIUS 服务器，则可以配置授权更改策略实施。当 AAA 中的用户或用户组的策略发生更改时，ISE 会向 FTD 设备发送 CoA 消息，以重新初始化身份验证并应用新策略。不需要内联安全状态实施点 (IPEP) 来为与 FTD 设备建立的每个 VPN 会话应用访问控制列表 (ACL)。

相关信息：

- [在 FTD 设备上配置授权更改](#)

在 FTD 设备上配置授权更改

大多数授权更改策略是在 ISE 服务器中配置的。但是，您必须将 FTD 设备配置为正确连接到 ISE。

准备工作

如果在任何对象中使用主机名，请确保配置用于数据接口的 DNS 服务器，如《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》“系统设置”一章的“为数据和管理接口配置 DNS”部分中所述。您的设备运行的版本。您通常需要配置 DNS 才能拥有功能齐全的系统。

<https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html>

操作步骤

Procedure

步骤 1 登录至您的 FDM 管理设备的防火墙设备管理器。

步骤 2 配置扩展的访问控制列表 (ACL)，用于将初始连接重定向到 ISE。重定向 ACL 的目的是向 ISE 发送初始流量，以便 ISE 可以评估客户端安全状态。ACL 应向 ISE 发送 HTTPS 流量，而非已设定发往 ISE 的流量或被定向到域名解析 DNS 服务器的流量。重定向 ACL 的示例如下所示：

```
access-list redirect extended deny ip any host<ISE server IP>
```

```
access-list redirect extended deny ip any host<DNS server IP>
```

```
access-list redirect extended deny icmp any any
```

```
access-list redirect extended permit tcp any any eq www
```

但是，请注意，ACL 包含隐式 “deny any any” 作为最后一个访问控制条目 (ACE)。在此示例中，与 TCP 端口 www（即端口 80）匹配的最后一个 ACE 将不会匹配与前 3 个 ACE 匹配的任何流量，因此这些 ACE 是冗余的。您只需使用最后一个 ACE 创建 ACL 即可获得相同的结果。请注意，在重定向 ACL 中，允许和拒绝操作只会确定哪些流量与 ACL 匹配，系统会允许匹配的流量并拒绝不匹配的流量。实际上，系统并不会丢弃任何流量，被拒绝的流量只是未重定向至 ISE。要创建重定向 ACL，您需要配置 Smart CLI 对象。

a. 选择设备 (Device) > 高级配置 (Advanced Configuration) > 智能 CLI (Smart CLI) > 对象 (Objects)。

b. 点击 + 创建新对象。

c. 输入 ACL 的名称。例如，重定向。

d. 对于 CLI 模板，选择扩展访问列表。

e. 在模板正文中进行以下配置：

- configure access-list-entry action = permit
- source-network = any-ipv4
- destination-network = any-ipv4
- configure permit port = any-source
- destination-port = HTTP
- configure logging = disabled

ACE 应如下所示：

Name	Description
redirect	

CLI Template

Extended Access List

Template

```

1 access-list redirect extended
2 configure access-list-entry permit
3 permit network source [any-ipv4] destination [any-ipv4]
4 configure permit port any-source
5 permit port source ANY destination [HTTP]
6 configure logging disabled
7 disabled log set log-level INFORMATIONAL log-interval 300

```

CANCEL OK

f. 点击确定 (OK)。

在下次部署更改时会配置此 ACL。无需在任何其他策略中使用此对象来强制部署。

Note 此 ACL 仅适用于 IPv4。如果您还想要支持 IPv6，除了要为源和目标网络选择 any-ipv6 外，只需再添加一个拥有所有相同属性的 ACE 即可。您还可以添加其他 ACE，以确保前往 ISE 或 DNS 服务器的流量未被重定向。您首先需要创建主机网络对象，以保留这些服务器的 IP 地址。

步骤 3 配置用于动态授权的 RADIUS 服务器组。

按照“创建或编辑 Firepower 威胁防御 RADIUS 服务器对象或组”部分中提供的说明执行以下步骤。
[创建或编辑 RADIUS 服务器对象或组, on page 250](#)

- a. 创建 RADIUS 服务器对象
- b. 创建 RADIUS 服务器组

步骤 4 创建使用此 RADIUS 服务器组的连接配置文件。请参阅[配置 RA VPN 连接配置文件](#)。使用 AAA 身份验证（单独使用或与证书结合使用），并在用户身份验证主身份源、授权和记账选项中选择服务器组。

验证 FDM 管理 设备的远程接入 VPN 配置

在配置远程访问 VPN 并将该配置部署到设备后，请确认是否可以远程连接。

Procedure

步骤 1 在外部网络中，使用 AnyConnect 客户端建立 VPN 连接。使用 Web 浏览器，打开 <https://ravpn-address>，其中 *ravpn-address* 是您允许 VPN 连接的外部接口的 IP 地址或主机名。如有

必要，安装客户端软件并完成连接。请参阅[用户如何在 FDM 管理设备上安装 AnyConnect 客户端软件](#)。如果配置了组 URL，也可尝试这些 URL。

步骤 2 在资产页面中，选择要验证的设备，然后点击设备操作下的命令行界面。

步骤 3 使用 **show vpn-sessiondb** 命令可查看有关当前 VPN 会话的摘要信息。

步骤 4 统计信息应显示您的活动 AnyConnect 客户端会话以及有关累积会话、峰值并发会话数量和非活动会话的信息。以下是该命令的输出示例。

```
> show vpn-sessiondb
-----
VPN Session Summary
-----
Active : Cumulative : Peak Concur : Inactive
-----
AnyConnect Client      :    1 :    49 :    3 :    0
  SSL/TLS/DTLS         :    1 :    49 :    3 :    0
Clientless VPN         :    0 :    1 :    1 :
  Browser              :    0 :    1 :    1 :
-----

Total Active and Inactive :    1          Total Cumulative :    50
Device Total VPN Capacity : 100000
Device Load               :    0%
-----

Tunnels Summary
-----
Active : Cumulative : Peak Concurrent
-----
Clientless              :    0 :    1 :    1
AnyConnect-Parent      :    1 :    49 :    3
SSL-Tunnel              :    1 :    46 :    3
DTLS-Tunnel            :    1 :    46 :    3
-----
Totals                  :    3 :    142
-----

IPv6 Usage Summary
-----
Active : Cumulative : Peak Concurrent
-----
AnyConnect SSL/TLS/DTLS :    :    :
  Tunneled IPv6         :    1 :    20 :    2
-----
```

步骤 5 使用 **show vpn-sessiondb anyconnect** 命令可查看有关当前 AnyConnect VPN 会话的详细信息。详细信息包括使用的加密方式、传输和接收的字节数及其他统计信息。如果使用 VPN 连接，随着您重新发出命令，您应可看到传输/接收的字节数会变化。

```

> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username      : User1|                               Index      : 4820
Assigned IP   : 172.18.0.1                           Public IP   : 192.168.2.20
Assigned IPv6 : 2009::1
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 27731                               Bytes Rx   : 14427
Group Policy  : MyRaVpn|Policy                       Tunnel Group : MyRaVpn
Login Time    : 21:58:10 UTC Mon Apr 10 2017
Duration      : 0h:51m:13s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                                  VLAN       : none
Audt Sess ID  : c0a800fd012d400058ebfff2
Security Grp  : none                                Tunnel Zone : 0

```


查看设备的远程接入 VPN 配置详细信息FDM 管理

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 VPN 远程访问 VPN 配置。 >

步骤 2 点击现有的 VPN 配置对象。

该组显示有关当前已配置多少连接配置文件和组策略的摘要信息。

- 展开 RA VPN 配置以查看与其关联的所有连接配置文件。
 - 点击添加 + 按钮可添加新的连接配置文件。
 - 点击查看按钮()，打开连接配置文件和连接说明的摘要。在操作下，您可以点击编辑以修改更改。
- 您可以点击“操作”下的以下选项之一来执行其他任务：
 - 点击组策略以分配/添加组策略。
 - 点击不再需要的配置对象或连接配置文件，然后点击删除进行删除。

模板

模板提供了开发设备配置文件的首选和通用版本的方法：

- 模板是从现有的基本配置文件创建的。
- 它们支持值参数，以便轻松自定义预期值，包括 IP 地址和端口号。

- 它们可以通过参数替换导出，以便在多个设备之间使用。

相关信息

- [FDM 管理 设备模板, on page 280](#)
 - [配置 FDM 模板, on page 281](#)
 - [将模板应用到 FDM 管理设备, on page 285](#)

FDM 管理 设备模板

关于 FDM 管理 设备模板

思科防御协调器 允许您创建已载入 FDM 管理 设备配置的 FDM 管理 模板。创建模板时，请选择要包含在 FDM 管理 设备模板中的部分（对象、策略、设置、接口和 NAT）。然后，您可以修改该模板并使用它来配置您管理的其他 FDM 管理 设备。FDM 管理 设备模板是促进 FDM 管理 设备之间策略一致性的一种方法。

创建 FDM 管理 设备模板时，您可以选择创建完整或自定义模板：

- 完整的模板包括 FDM FDM 管理 设备配置的所有部分，并将所有内容应用于其他 FDM 管理 设备。
- 自定义模板仅包含您选择的 FDM 管理 设备配置的一个或多个部分，并且仅在其他 FDM 管理 设备上应用该部分及其关联的实体。



Important FDM 管理 模板不包括证书、Radius、AD 和 RA VPN 对象。

如何使用 FDM 管理 设备模板

以下是使用 FDM 管理 设备模板的一些方法：

- 通过应用另一台 FDM 管理 设备的配置模板来配置一台 FDM 管理 设备。您应用的模板可能代表了您要在所有 FDM 管理 设备上使用的“最佳实践”配置。
- 将模板用作一种进行设备配置更改的方法，并在实验环境中模拟这些更改，以便在将这些更改应用于实时 FDM 管理 设备之前测试其功能。
- 在创建模板时，对接口和子接口的属性进行参数化。您可以在应用模板时更改接口和子接口的参数化值。

您将在更改日志中看到的内容

在将模板应用于设备时，该设备的整个配置都会被覆盖。CDO 更改日志会记录由此产生的每个更改。因此，将模板应用于设备后，更改日志条目会变得非常长。

相关信息：

- [配置 FDM 模板](#)
- [应用 FDM 模板](#)

配置 FDM 模板

前提条件

在创建 FDM 管理模板之前，请将您将创建模板的 FDM 管理载入思科防御协调器。您只能从已载入的 FDM 管理设备创建 FDM 管理设备模板。

我们强烈建议使用模板来配置正被添加到环境中的全新 FDM 管理设备。



Note 从 FDM 管理设备创建模板时，RA VPN 对象不会被包含在模板中。

创建 FDM 模板

在创建模板时，如果您选择所有部分，则模板将包括该设备配置的各个方面；管理 IP 地址、接口配置、策略信息等。

如果选择某些部分，自定义模板将包括以下实体。

模板部件	自定义模板中包含的部分
访问规则	包括访问控制规则和这些规则的任何相关实体。例如，对象和接口（带子接口）。
NAT 规则	包括 NAT 规则以及这些 NAT 规则所需的任何相关实体。例如，对象和接口（带子接口）。
设置	包括系统设置以及这些设置所需的任何相关实体。例如，对象和接口（带子接口）。
接口	包括接口和子接口。
对象	包括对象和这些对象所需的任何相关实体。例如，接口和子接口。

使用此程序创建 FDM 管理设备模板：

Procedure

- 步骤 1** 在思科防御协调器导航栏中，点击 **清单 (Inventory)**。
- 步骤 2** 点击**设备**选项卡。
- 步骤 3** 点击 **FTD** 选项卡，然后从列表中选择所需的设备。
- 步骤 4** 使用**过滤器**和**搜索**字段查找要为其创建模板的 FDM 管理设备。

- 步骤 5** 在右侧的设备操作 (**Device Actions**) 窗格中，点击创建模板 (**Create Template**)。名称模板会提供设备上每个部分的计数。它还会显示子接口（如有）的计数。
- 步骤 6** 选择您要在模板中包含的部分。
- 步骤 7** 输入模板的名称。
- 步骤 8** 点击创建模板 (**Create Template**)。
- 步骤 9** 在参数化模板 (**Parameterize Template**) 区域中，您可以执行以下操作：
- 要参数化接口，请将鼠标悬停在与该接口对应的单元格上（直到您看到花括号）并点击。
 - 要参数化子接口，请展开具有子接口的接口，将鼠标悬停在与该子接口对应的单元格上（直到看到花括号）并点击。

您可以参数化以下属性，以便启用每台设备的自定义。

- 逻辑名称
- 状态
- IP 地址/网络掩码

Note 这些属性仅支持每个参数一个值。

- 步骤 10** 点击继续 (**Continue**)。
- 步骤 11** 查看模板和任何参数化。点击完成 (**Done**) 以创建模板。

清单 (Inventory) 页面现在会显示您刚刚创建的 FDM 管理 设备模板。

Note 创建模板后，在**清单 (Inventory)** 窗格中，CDO 会显示相应的模板部件图标，以显示该模板中包含的部件。当您点击设备或将鼠标指针悬停在图标上时，此信息也会显示在**设备详细信息 (Device Details)** 窗格中。

下图显示了一个部件图标示例，用于显示包括“访问规则”、“NAT 规则”和“对象”在内的模板。



编辑 FDM 管理设备模板

使用以下程序来编辑模板参数：

Procedure

- 步骤 1** 在 思科防御协调器 导航栏中，点击 **清单 (Inventory)**。
- 步骤 2** 点击模板 (**Templates**) 选项卡。

步骤 3 点击 **FTD** 选项卡。

步骤 4 使用模型/模板过滤器查找要修改的模板。

步骤 5 在右侧的设备操作 (**Device Actions**) 窗格中，点击**编辑参数 (Edit Parameters)**。

步骤 6 (可选) 通过直接编辑文本框对参数进行任何更改。

步骤 7 点击**保存 (Save)**。

您可以像编辑实时 FDM 管理设备一样编辑 FDM 管理设备模板的其余部分。您可以使用以下配置来编辑 FDM 管理设备模板：

- [FDM 管理 设备设置](#)
- [虚拟专用网络管理](#)
- [创建 RA VPN 配置](#)
- [FDM 策略配置](#)
- [促进策略和配置的一致性](#)

删除 FDM 模板

您可以像从 思科防御协调器 中删除 FDM 管理 设备一样删除 FDM 管理 设备模板：

Procedure

步骤 1 在 CDO 导航栏中，点击 **清单 (Inventory)**。

步骤 2 点击**模板 (Templates)** 选项卡。

步骤 3 点击 **FTD** 选项卡。

步骤 4 使用过滤器和搜索字段查找要删除的 FDM 管理 设备模板。

步骤 5 在设备操作 (**Device Actions**) 窗格中，点击**删除 (Remove)** 。

步骤 6 阅读警告消息，然后点击**确定 (OK)** 以删除模板。

相关信息：

- [FDM 管理 设备模板](#)
- [应用 FDM 模板](#)

应用 FDM 模板

在应用模板之前，您可以通过导航至**清单 (Inventory)** 页面并过滤**模型/模板 (Model/Template)**来识别其内容。思科防御协调器 会显示相应的模板部件图标，以显示该模板中包含的部件。当您点击设备或将鼠标指针悬停在图标上时，此信息也会显示在**设备详细信息 (Device Details)** 窗格中。

您可以通过参数化以下属性来启用每台设备的自定义，这意味着您可以在应用模板时应用设备特定的值：

应用 FDM 管理 设备模板时，可以更改创建模板时配置的接口和子接口的参数化值。

应用整个模板

应用完整的 FDM 管理 设备模板以创建的新 FDM 管理 设备会完全覆盖 FDM 管理 设备上的任何现有配置，包括尚未从 CDO 部署到设备的任何暂存更改。设备上未包含在模板中的任何内容都将丢失。

应用自定义模板

将自定义 FDM 管理 模板应用于其他 FDM 管理 设备将根据模板部分保留或删除现有配置。下表提供在其他 FDM 管理 设备上应用自定义模板后发生的更改。

模板部件	应用自定义模板后
访问规则	<ul style="list-style-type: none"> 自定义模板中的新访问控制规则会覆盖设备上的任何现有访问控制规则。 自定义模板中的新对象和接口（带有子接口）（如有）将应用于设备，而不会删除任何现有对象和接口。
NAT 规则	<ul style="list-style-type: none"> 自定义模板中的新 NAT 规则会覆盖设备上的任何现有 NAT 规则。 自定义模板中的新对象和接口（带有子接口）（如有）将应用于设备，而不会删除任何现有对象和接口。
设置	<ul style="list-style-type: none"> 自定义模板中的新系统设置将应用于设备，而不会删除任何现有系统设置。 自定义模板中的新对象和接口（带有子接口）（如有）将应用于设备，而不会删除任何现有对象和接口。
接口	<ul style="list-style-type: none"> 自定义模板中的新接口和子接口将应用于设备，而不会删除任何现有接口和子接口。 CDO 不允许将模板应用于模板中定义的接口数量超过设备上接口数量的设备。
对象	<ul style="list-style-type: none"> 自定义模板中的新对象将应用于设备，而不会删除任何现有对象。 自定义模板中的新接口和子接口（如有）将应用于设备，而不会删除任何现有接口和子接口。

前提条件

在应用模板之前，必须满足以下条件：

- 使用模板时，请确保您对模板所做的任何更改都已提交，并且模板在清单 (Inventory) 页面上处于“已同步” (Synced) 状态。

- 在使用 FDM 管理设备作为模板时，请确保已部署您打算部署到设备的 CDO 上的任何更改，并且没有尚未部署的防火墙设备管理器控制台更改。设备必须在清单 (Inventory) 页面上显示“已同步” (Synced) 状态。

将模板应用于设备的过程分为三步。

1. [应用整个模板](#)
2. [查看设备和网络设置](#)
3. [将更改部署到设备](#)

将模板应用到 FDM 管理设备



Important 在将更改部署到设备之前，请继续执行下一程序：

[查看设备和网络设置](#)

在应用模板之前，您可以使用更改请求跟踪将跟踪标签应用于更改。[更改请求管理](#)使用以下程序应用 FDM 管理设备模板：

Procedure

步骤 1 (可选) 开始之前，请先创建设备模板，然后再向其应用其他模板。FDM 管理这为您提供了一个配置备份，您可以在需要重新应用设备和网络设置时进行参考。

步骤 2 在 CDO 导航栏中，点击 **清单 (Inventory)**。

步骤 3 点击 **模板 (Templates)** 选项卡。

步骤 4 点击 **FTD** 选项卡。

步骤 5 使用过滤器和搜索字段查找要应用模板的设备或模板。FDM 管理

Note 如果此时更改模板的名称，则会对 DeviceName 应用完整的设备配置或模板。将此更改部署到 DeviceName 将覆盖该设备上运行的整个配置。

步骤 6 在右侧的设备操作 (Actions) 窗格中，点击 **应用模板 (Apply Template)**。

步骤 7 点击选择模板并选择所需的模板，然后点击继续。

步骤 8 您可以配置以下内容，然后点击每个屏幕上显示的继续。

- a. 映射接口：确认或更改模板和设备之间的接口映射。请注意，不能将多个模板接口映射到单个设备接口；如果接口配置不受支持，则无法继续并应用模板。

Note CDO 不允许将模板应用于模板中定义的接口数量超过设备上接口数量的设备。

- b. 填充参数：自定义要应用模板的设备的接口或子接口参数值。

- c. 查看：查看模板配置，并在准备好使用模板中的配置覆盖现有设备配置时点击应用模板。

步骤 9 点击[预览和部署所有设备的配置更改](#) 以查看并部署您所做的更改，或等待并一次部署多个更改。

查看设备和网络设置

创建 FDM 管理 模板时，思科防御协调器 会将整个设备配置复制到模板中。因此，模板中包含原始设备的管理 IP 地址等内容。在将模板应用于设备之前，请查看以下设备和网络设置：

Procedure

步骤 1 查看这些 FDM 管理 设备设置，以确保它们反映新 FDM 管理 设备的正确信息：

- [FDM 管理 设备设置](#)
- [管理接口](#)
- [主机名](#)

步骤 2 查看 [配置 FDM 访问控制策略](#)，确保规则在适当的情况下引用新 FDM 管理 设备的 IP 地址。

步骤 3 查看 `inside_zone` 和 `outside_zone` 安全对象，确保它们引用新 FDM 管理 设备的正确 IP 地址。

步骤 4 查看 NAT 策略，确保它们引用新 FDM 管理 设备的正确 IP 地址。

步骤 5 查看接口配置，确保它们反映新 FDM 管理 设备的正确配置。

将更改部署到设备

立即 [预览和部署所有设备的配置更改](#) 您所做的更改，或等待并一次部署多个更改。

相关信息：

- [FDM 管理 设备模板](#)
- [配置 FDM 模板](#)

将 ASA 配置迁移到 FDM 管理 设备模板



Attention

Firepower 设备管理器 (FDM) 支持和功能仅应要求提供。如果您的租户上尚未启用 防火墙设备管理器 支持，则无法管理或部署到 FDM 管理 设备。向支持团队发送请求以启用此平台。[通过 TAC 打开提交支持请求](#)

思科防御协调器 可帮助您将 ASA 迁移到 FDM 管理 设备。CDO 提供了一个向导来帮助您将 ASA 的运行配置的这些元素迁移到 FDM 管理 模板：

- [访问控制规则 \(ACL\)](#)

- 接口
- 网络地址转换 (NAT) 规则
- 网络对象和网络组对象
- 路由
- 服务对象和服务组对象
- 站点间 VPN

将 ASA 运行配置的这些元素迁移到 FDM 管理 模板后，即可将 FDM 模板应用于由 CDO 管理的新 FDM 管理 设备。FDM 管理 设备采用模板中定义的配置，因此，FDM 管理 设备现在配置了 ASA 运行配置的某些方面。

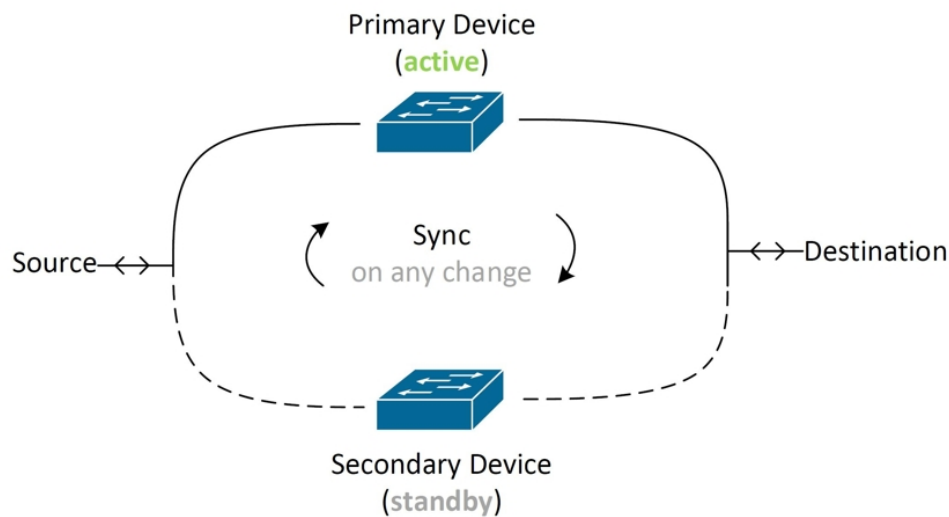
使用此过程不会迁移 ASA 运行配置的其他元素。这些其他元素在 FDM 管理 设备模板中由空值表示。将模板应用于 FDM 管理 设备时，我们会应用迁移到新 FDM 管理 设备的值并忽略空值。无论新 FDM 管理 设备具有哪些其他默认值，它都会保留。我们未迁移的 ASA 运行配置的其他元素将需要在迁移过程之外在 FDM 管理 设备上重新创建。

有关使用 CDO 将 ASA 迁移到 FDM 管理 设备的过程的完整说明，请参阅[使用思科防御协调器将 ASA 迁移到 FDM 托管设备](#)。

FDM 管理 高可用性

关于高可用性

高可用性 (HA) 或故障转移配置可将两台设备连接成主/辅助设置，这样，如果主设备发生故障，辅助设备就会自动接管其任务。配置高可用性（也称为故障切换）需要通过专用故障切换链路和状态链路（可选）相互连接的两台相同的 FDM 管理。系统会对主用设备的运行状况（硬件、接口、软件以及环境状态）进行监控，以便确定是否符合特定的故障切换条件。如果符合这些条件，将执行故障切换。这有助于在设备发生故障的情况下或在设备升级的维护期间让网络保持运行。有关详细信息，请参阅以下相关文章。



这两台设备构成一对主用/备用设备，其中，主设备是主用设备并传递流量。辅助（备用）设备不会主动传递流量，但会使配置和其他状态信息与主用设备同步。这两台设备通过故障转移链路进行通信，以便确定每台设备的运行状态。



Note 当您选择接受 HA 对更改或在部署到 FDM 管理 HA 对时，您将与 HA 对的主用设备通信。这意味着仅从主用设备提取配置和备份。

证书和高可用性对

将证书应用于 FDM 管理 HA 对时，CDO 只会将证书应用于主用设备；只有在部署主用设备时，配置和证书才会与备用设备同步。如果通过 FDM 管理 将新证书应用于主用设备，则主用设备和备用设备可能具有两个不同的证书。这可能会导致故障转移或故障转移历史记录出现问题，以及其他可能的问题。两台设备必须具有相同的证书才能成功运行。如果必须通过 FDM 管理 更改证书，则必须在 HA 对中部署更改并同步证书。

相关信息：

- [用于 FDM 管理 高可用性的故障转移和状态链路](#)
- [FDM 管理 高可用性对要求](#)
- [创建 FDM 管理 高可用性对](#)
- [“高可用性” \(High Availability\) 页面中的 FDM 管理设备](#)
- [中断 FDM 管理 高可用性对](#)
- [FDM 管理 高可用性故障转移历史记录](#)
- [刷新 FDM 管理 高可用性状态](#)

- 在高可用性对上强制执行故障切换 在高可用性对上强制执行故障切换FDM 管理
- 升级 FDM 管理 高可用性对
- 读取、丢弃、检查和部署更改
- 将配置更改从 FDM 管理 设备读取到 CDO
- 将配置更改从 CDO 部署到 FDM 管理 设备

FDM 管理 高可用性对要求

高可用性要求

在创建高可用性 (HA) 对之前，必须满足几个要求。

高可用性的物理和虚拟设备要求

必须满足以下硬软要求：

- 设备的硬件型号必须相同。
- 设备安装的模块必须相同。例如，如果具有可选的网络接口模块，则必须在另一台设备中安装相同的网络模块。
- 设备接口的数量和类型必须相同。
- 要在 思科防御协调器 中创建 HA 对，两台设备都必须配置管理接口。如果设备配置了数据接口，则必须通过 FDM 管理 UI 创建 HA 对，然后将该对载入 CDO。



Note 您不能在 HA 对中使用 FDM 管理 模板。

高可用性的软件要求

物理和虚拟 FDM 管理 设备必须满足以下软件要求：

- 您有两台已在 Defense Orchestrator 中载入的独立 FDM 管理 设备。
- 设备必须运行完全相同的软件版本，也即，主要版本号（第一个）、次要版本号（第二个）以及维护版本号（第三个）都必须相同。您可以在设备详情窗口的清单 (**Inventory**) 页面，或者可以在 CLI 中使用显示版本命令找到版本。



Note 允许连接具有不同版本的设备，但配置不会导入备用设备且故障切换无法使用，直到您将设备升级到同一软件版本。

- 两台设备必须在本地管理器模式下运行，也即，使用 FDM 配置设备。如果您可以在两个系统上登录 FDM，则表示这两台设备是本地管理器模式。您还可以在 CLI 中使用 `show managers` 命令进行验证。
 - 您必须在每台设备中完成初始设置向导，然后再载入 CDO。
 - 每台设备都必须有自己的管理 IP 地址。管理接口的配置在两台设备之间未同步。
 - 设备必须具有相同的 NTP 配置。
 - 不能配置任何接口使用 DHCP 获取地址。也就是说，所有接口都必须有静态 IP 地址。
- 注意：**如果更改任何接口配置，则必须在建立 HA 之前将更改部署到设备。
- 两台设备必须保持同步。如果检测到待处理更改或冲突，请参阅[解决配置冲突](#)和[解决配置冲突](#)以了解详细信息。



Note 当您选择接受 HA 对更改或在部署到 FDM 管理 HA 对时，您将与 HA 对的主用设备通信。这意味着仅从主用设备提取配置和备份。

高可用性的智能许可证要求

物理和虚拟 FDM 管理 设备必须满足以下许可证要求：

- 高可用性对中的两台设备都必须具有注册许可证或评估许可证。如果设备已注册，可以将其注册到不同的思科智能软件管理器账户，但这些账户的出口控制功能设置的状态必须相同，要么都启用这类设置，要么都禁用。但是，如果您已在设备上启用不同的可选许可证，上述设置便不再重要。
- 高可用性对中的两台设备在运行期间必须具有相同的许可证。如果没有足够的许可证，可能会出现一台设备合规，另一台设备不合规的情况。如果您的智能许可证账户不包含足够的购买权利，则您的账户将在您购买正确数量的许可证之前变得不符合要求（即使其中一台设备符合要求）。

请注意，如果设备处于评估模式，您必须确保 CDO 的注册状态在两台设备上相同。您还必须确保选择的思科 Success Network 参与状态相同。对于已注册设备，设置可以在两台设备上不同，但任何已在主（主用）设备上配置的对象将在辅助设备注册或注销。同意在主设备上参与思科成功网络意味着辅助设备上也执行相同操作。

如果将用户注册到存在不同出口控制功能设置的账户，或者尝试创建一个 HA 对，注册其中的一台设备，而将另外一台设备设置为评估模式，则 HA 加入可能会失败。对于出口控制功能，如果您使用不一致的设置配置 IPSec 加密密钥，当您激活 HA 后，两个设备都将变为主用状态。这会影响受支持网段上的路由，且您必须手动断开辅助设备上的 HA 才能消除影响。

HA 的云服务配置

高可用性对中的两台设备都必须启用**将事件发送到思科云 (Send Events to the Cisco Cloud)**。此功能在 FDM UI 中可用。导航至**系统设置 (System Settings)**，然后点击**云服务 (Cloud Services)**以启用此

功能。如果未启用此选项，则无法在 CDO 中形成 HA 对，并且会发生事件描述错误。有关详细信息，请参阅所运行版本的《Firepower 设备管理器配置指南》的[配置云服务](#)一章。

创建 FDM 管理 高可用性对

在 Defense Orchestrator 中创建 FDM 管理 HA 对之前，必须首先载入满足[FDM 管理 高可用性对要求](#)中所述的两个独立 FDM 管理 设备。



Note 要在 CDO 中创建 HA 对，两台设备都必须配置管理接口。如果设备配置了数据接口，则必须通过 FDM 控制台创建 HA 对，然后将该对载入 CDO。

创建 FDM 管理 高可用性对后，默认情况下，主设备处于**主用状态**，辅助设备处于**备用状态**。所有配置更改或部署都通过主设备进行，辅助设备保持备用模式，直到主设备不可用。

请注意，当您选择接受配置更改或部署到 FDM 管理 HA 对时，您将与 HA 对的主用设备通信。对主设备所做的任何更改都通过主设备和辅助设备之间的链路传输。CDO 会部署到主设备并仅接受来自主设备的更改；因此，[清单 \(Inventory\)](#) 页面显示该对的单个条目。部署完成后，主设备会将所有配置更改同步到辅助设备。

类似于 CDO 如何仅与主用设备通信，当您计划或选择备份 FDM 管理 HA 对时，只有主用设备符合备份条件。



Note 如果 HA 设备在创建过程中遇到问题，或者 HA 对未处于正常状态，则必须手动中断 HA 配置，然后才能尝试再次创建该对。

操作步骤

使用以下程序从两个独立 FTD 设备创建 HA 对：

Procedure

步骤 1 在导航栏中，点击[清单 \(Inventory\)](#)。

步骤 2 点击[设备 \(Devices\)](#) 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡并选择要建立为主设备的设备。

Note CDO 不支持使用配置了 DHCP 的设备创建 HA 对。

步骤 4 在“管理” (Management) 窗格中，点击[高可用性 \(High Availability\)](#)。

步骤 5 找到辅助设备的区域并点击[选择设备 \(Select Device\)](#)，然后从符合条件的设备列表选择一个设备。

步骤 6 配置故障转移链路。

a. 点击[物理接口 \(Physical Interface\)](#) 并从下拉菜单中选择接口。

- b. 选择适当的 IP 类型。
- c. 输入主 IP 地址。
- d. 输入辅助 IP 地址。
- e. 输入子网掩码。默认情况下，该值为 24。
- f. 如果适用，请输入有效的 IPSec 加密密钥。

步骤 7 配置状态链路。如果要使用与故障转移链路相同的配置，请选中**与故障转移链路相同 (The same as Failover Link)** 复选框。如果要使用其他配置，请使用以下程序：

- a. 点击**物理接口 (Physical Interface)** 并从下拉菜单中选择接口。请注意，主设备和辅助设备必须具有相同数量的物理接口。
- b. 选择适当的 IP 类型。
- c. 输入主 IP 地址。
- d. 输入辅助 IP 地址。
- e. 输入子网掩码。默认情况下，该值为 24。

步骤 8 在屏幕的右上角点击**创建 (Create)** 以便完成向导。CDO 会立即将您重定向到“高可用性状态” (High Availability Status) 页面。在此页面中，您可以监控 HA 创建的状态。请注意，创建 HA 对后，**清单 (Inventory)** 页面会将该对显示为单行。

步骤 9 [预览和部署所有设备的配置更改](#)您现在所做的更改，或者等待并一次部署多个更改。

“高可用性” (High Availability) 页面中的 FDM 管理设备

高可用性 (HA) 管理页面中的 FDM 管理是 FDM 管理设备的多用途页面。此页面仅适用于已配置为 HA 对的设备。您可以载入 FDM 管理 HA 对，也可以从两台独立 FDM 管理设备创建 FDM 管理 HA 对。

如果从**清单 (Inventory)** 页面选择独立 FDM 管理设备，则此页面将用作创建 HA 对的向导。此时，您必须将两台 FDM 管理设备载入到思科防御协调器才能创建配对。要在 CDO 中创建 FDM 管理 HA 对，请参阅[创建 FDM 管理高可用性对](#)。

如果从**清单 (Inventory)** 页面选择 FDM 管理 HA 对，则此页面将用作概述页面。在这里，您可以查看 HA 配置和故障转移历史记录，以及可操作的项目，例如强制故障转移、编辑故障转移条件以及删除 HA 链路。

高可用性管理页面

要查看“高可用性” (High Availability) 页面，请使用以下程序：

Procedure

- 步骤 1 在导航栏中，点击**清单 (Inventory)**。
- 步骤 2 点击**设备 (Devices)** 选项卡以找到设备。
- 步骤 3 点击**FTD** 选项卡，然后选择独立 FDM 管理设备或 FDM 管理 HA 对的主用 FDM 管理设备。
- 步骤 4 在**管理 (Management)** 窗格中，点击**高可用性 (High Availability)**。

相关信息：

- [FDM 管理 高可用性故障转移历史记录](#)
- [编辑高可用性故障切换条件](#)
- [在高可用性对上强制执行故障切换FDM 管理](#)
- [中断 FDM 管理 高可用性对](#)
- [刷新 FDM 管理 高可用性状态](#)

编辑高可用性故障切换条件

您可以在创建 FTD HA 对后编辑故障转移条件。

Procedure

- 步骤 1 在导航栏中，点击**清单 (Inventory)**。
- 步骤 2 点击**设备 (Devices)** 选项卡以找到设备。
- 步骤 3 点击**FTD** 选项卡，然后选择 FTD HA 对的主用设备。
- 步骤 4 在“管理” (Management)窗格中，点击**高可用性 (High Availability)**。
- 步骤 5 在“故障转移条件” (Failover Criteria) 窗口中，点击**编辑 (Edit)**。
- 步骤 6 进行任何必要的更改，然后点击**保存 (Save)**。
- 步骤 7 [预览和部署所有设备的配置更改](#)您现在所做的更改到主用设备，或等待并一次部署多个更改。

中断 FDM 管理 高可用性对

中断高可用性时，备用设备上的已配置接口将自动禁用。在此过程中，设备可能会遇到流量中断。成功删除 HA 对后，您将从状态页面重定向到“高可用性”页面，您可以在其中选择使用相同的主设备创建另一个 HA 对。



Note 在成功删除高可用性对之前，您无法部署到任一设备。

使用管理接口中断高可用性

中断配置了管理接口的 HA 对时，中断可能需要 10 分钟或更长时间才能完成，并且在此过程中两台设备都会离线。成功删除 HA 配置后，CDO 会在“服务和设备”页面中将两台设备显示为独立设备。

使用数据接口中断高可用性

中断已配置数据接口的 HA 时，中断可能需要 20 分钟或更长时间才能完成，并且两台设备都会离线。删除高可用性配置后，您必须手动重新连接主用设备。

但是，备用设备会保留 HA 配置，并且将无法访问，因为它与主用设备具有相同的配置。您必须在 CDO 外部手动重新配置 IP 接口，然后将设备作为独立设备重新载入。

中断高可用性

使用以下程序删除两台 FDM 管理设备的 HA 配对：

Procedure

- 步骤 1 在导航栏中，点击**清单 (Inventory)**，然后选择 FDM 管理 HA 对的主用设备。
 - 步骤 2 点击**设备**选项卡，找到您的设备。
 - 步骤 3 点击**FTD**选项卡。
 - 步骤 4 在“管理” (Management)窗格中，点击**高可用性 (High Availability)**。
 - 步骤 5 点击**中断高可用性 (Break High Availability)**。
 - 步骤 6 CDO 将删除 HA 配置，两台设备在**清单 (Inventory)**页面中显示为独立设备。
 - 步骤 7 将配置更改从 CDO 部署到 FDM 管理设备，以便将新配置部署到两台设备。
 - 步骤 8 [预览和部署所有设备的配置更改](#)您现在所做的更改到主用设备，或等待并一次部署多个更改。
-

中断带外高可用性

如果使用 FDM 接口中断 FDM 管理 HA 对，则思科防御协调器中 HA 对的配置状态会更改为**检测到冲突 (Conflict Detected)**。中断高可用性后，您必须通过 FDM 管理将更改部署到主设备，然后解决 CDO 中的[解决配置冲突](#)状态。

设备恢复为“已同步” (Synced) 状态后，您可以将 CDO 中所做的配置更改部署到设备。

我们不建议在使用 FDM 管理接口中断高可用性后从 CDO 恢复更改。


相关信息：

- [FDM 管理 高可用性故障转移历史记录](#)
- [刷新 FDM 管理 高可用性状态](#)
- [在高可用性对上强制执行故障切换 FDM 管理](#)
- [读取、丢弃、检查和部署更改](#)

在高可用性对上强制执行故障切换FDM 管理

通过强制故障切换来切换 HA 对中的主用设备和备用设备。FDM 管理请注意，如果您最近将新证书应用于主用设备，并且尚未部署更改，则备用设备会保留原始证书，并且故障切换将失败。主用设备和备用设备必须应用相同的证书。使用以下程序手动强制执行故障切换：

Procedure

- 步骤 1** 在导航栏中，点击**清单 (Inventory)**。
- 步骤 2** 点击 **设备** 选项卡以找到设备。
- 步骤 3** 点击 **FTD** 选项卡。
- 步骤 4** 选择 HA 对的主用设备。FDM 管理
- 步骤 5** 在“管理” (Management)窗格中，点击**高可用性 (High Availability)**。
- 步骤 6** 点击选项图标。 
- 步骤 7** 点击切换模式。主用设备现在处于备用状态，备用设备现在处于活动状态。

相关信息：

- [中断 FDM 管理 高可用性对](#)
- [FDM 管理 高可用性故障转移历史记录](#)
- [刷新 FDM 管理 高可用性状态](#)
- 在高可用性对上强制执行故障切换 [在高可用性对上强制执行故障切换FDM 管理](#)

FDM 管理 高可用性故障转移历史记录

Procedure

- 步骤 1** 在导航栏中，点击**清单 (Inventory)**。
- 步骤 2** 点击 **设备** 选项卡以找到设备。
- 步骤 3** 点击 **FTD** 选项卡。
- 步骤 4** 选择 HA 对的主用设备。FDM 管理
- 步骤 5** 在“管理” (Management)窗格中，点击**高可用性 (High Availability)**。
- 步骤 6** 点击**故障转移历史 (Failover History)**。CDO 会生成一个窗口，其中详细说明自 HA 对形成以来主设备和辅助设备的故障切换历史记录。


Note 故障切换历史记录也会显示在设备对的更改日志中，可从“资产”页面获取。

相关信息：

- [中断 FDM 管理 高可用性对](#)
- [FDM 管理 高可用性故障转移历史记录](#)
- [刷新 FDM 管理 高可用性状态](#)
- [在高可用性对上强制执行故障切换](#) [在高可用性对上强制执行故障切换FDM 管理](#)

刷新 FDM 管理 高可用性状态

Procedure

- 步骤 1** 在导航栏中，点击清单 (Inventory)。
- 步骤 2** 点击 设备 选项卡以找到设备。
- 步骤 3** 点击 FTD 选项卡，然后选择 FDM 管理 设备或 FDM 管理 HA 对。
- 步骤 4** 在 管理 窗格中，点击 高可用性。
- 步骤 5** 点击选项图标。 
- 步骤 6** 点击获取最新状态。CDO 从主设备请求运行状况。

相关信息：

- [中断 FDM 管理 高可用性对](#)
- [FDM 管理 高可用性故障转移历史记录](#)
- [刷新 FDM 管理 高可用性状态](#)
- [在高可用性对上强制执行故障切换](#) [在高可用性对上强制执行故障切换FDM 管理](#)

用于 FDM 管理 高可用性的故障转移和状态链路

故障转移链路和（可选）状态链路

故障转移链路是两台设备之间的专用连接。状态故障转移链路也是专用连接，不过，您可以使用一个故障转移链路作为组合的故障转移/状态链路，也可以创建单独的专用状态链路。如果仅使用故障转移链路，状态信息也会通过该链路：状态故障转移功能不会受到影响。默认情况下，故障转移和状态故障转移链路中的通信是纯文本通信（不加密）。为了增强安全性，您可以通过配置 IPsec 加密密钥对通信加密。

您可以将任何未使用的数据物理接口用作故障转移链路和可选的专用状态链路。但是，您不能选择当前已配置名称或具有子接口的接口。故障转移和状态故障转移链路接口不会被配置为通常的网络接口。这些接口只是为了进行故障转移通信，不能用于直通流量或管理访问。此配置在设备之间是同步的，因此您必须为链路的两端选择相同的端口号。例如，用于故障转移链路的两台设备都使用 GigabitEthernet1/3。



Note FDM 管理 设备用户数据和故障转移链路之间共享接口。

故障转移链路

故障转移对中的两台设备会不断地通过故障转移链路进行通信，以确定每台设备的运行状态和同步配置更改。通过此链接共享以下信息：

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

您可以使用未使用的数据接口（物理接口、冗余接口或 EtherChannel 接口）作为故障转移链路；但不能指定当前配置了名称的接口。请勿使用子接口作为故障转移链路。

故障转移链路接口不会配置为常规网络接口；该接口仅会因为故障转移而存在。该接口只能用于故障转移链路（还用于状态链路）。

状态链接

主用设备使用状态链路将连接状态信息传送到备用设备。这意味着，备用设备可以保持某些类型的连接，而不会影响用户。此信息可在发生故障转移时帮助备用设备保留现有连接。

您可以将专用接口（物理、冗余或 EtherChannel）用于状态链路。对于用作状态链路的 EtherChannel，要阻止无序数据包，仅使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。

对故障转移和状态故障转移链路使用一条链路能够最大程度地节省接口。但是，如果您有一个大型配置和高流量网络，必须考虑对状态链路和故障转移链路使用专用接口。我们建议状态故障转移链路的带宽应匹配设备上数据接口的最大带宽。

FDM 管理 设备设置

配置 FTD 设备的系统设置

使用此程序在单个 FTD 设备上配置设置：

Procedure

步骤 1 打开清单 (Inventory) 页面。

- 步骤 2 点击 **设备** 选项卡，找到您的设备。
- 步骤 3 点击 **FTD** 选项卡，然后选择要配置其设置的设备。
- 步骤 4 在右侧的**管理 (Management)** 窗格中，点击**设置 (Settings)**。
- 步骤 5 点击**系统设置 (System Settings)** 选项卡。
- 步骤 6 编辑这些设备设置：

- [配置管理访问](#)
- [配置日志记录设置](#)
- [配置 DHCP 服务器](#)
- [配置 DNS 服务器](#)
- [主机名](#)
- [配置 NTP 服务器](#)
- [配置 URL 过滤](#)
- [云服务](#)
- [启用或禁用网络分析](#)

配置管理访问

默认情况下，您可以从任何 IP 地址访问设备的管理地址。系统访问仅受用户名和密码的保护。但是，您可以配置访问列表以仅允许来自特定 IP 地址或子网的连接，以进一步加强保护。

您还可以开放数据接口以允许 FDM 管理设备或 SSH 连接至 CLI。然后，无需使用管理地址即可管理设备。例如，您可以允许对外部接口进行管理访问，这样就能远程配置设备。用户名和密码可防止不想要的连接。默认情况下，对数据接口的 HTTPS 管理访问会在内部接口上启用而在外部接口上禁用。对于具有默认“内部”网桥组的设备型号，这意味着可以通过网桥组中的任意数据接口，与网桥组 IP 地址（默认值为 192.168.1.1）建立 FDM 管理设备连接。您可以只在进入设备所通过的接口上开放管理连接。



注意 如果只允许访问特定地址，那么您可能很容易将自己锁定在系统之外。如果删除对当前所用 IP 地址的访问，并且没有“任何”地址条目，则在部署策略时将丢失对系统的访问。在配置访问列表时请注意这一点。

为管理接口创建规则

使用以下程序为管理接口创建规则：

过程

步骤 1 点击“管理接口”(Management Interface)部分中的**新访问权限(New Access)**。

- **Protocol**。选择规则是用于 HTTPS (端口 443) 还是 SSH (端口 22)。
- **允许的网络**。选择定义应该能够访问系统的 IPv4 或 IPv6 网络或主机的网络对象。要指定“任何”地址，请选择 **any-ipv4** (0.0.0.0/0) 和 **any-ipv6**(::/0)。

步骤 2 点击**保存(Save)**。

为数据接口创建规则

使用以下程序为数据接口创建规则：

过程

步骤 1 点击“数据接口”(Data Interface)部分中的**新访问权限(New Access)**。

- **接口**。选择要在其上允许管理访问的接口。
- **Protocol**。选择规则是用于 HTTPS (端口 443)、SSH (端口 22) 还是二者。不能为远程访问 VPN 连接配置文件中使用的接口配置 HTTPS 规则。
- **允许的网络**。选择定义应该能够访问系统的 IPv4 或 IPv6 网络或主机的网络对象。要指定“任何”地址，请选择 **any-ipv4** (0.0.0.0/0) 和 **any-ipv6** (::/0)。

步骤 2 点击**保存(Save)**。

步骤 3 [预览和部署所有设备的配置更改](#)您现在所做的更改，或者等待并一次部署多个更改。


配置日志记录设置

此程序介绍如何启用**诊断(数据)消息**、**文件**和**恶意软件**事件、**入侵**事件和控制台事件的日志记录。由于这些设置，**连接事件**不会被记录。如果在访问规则、安全情报策略或 SSL 解密规则上配置了连接日志记录，则会记录连接事件。

Procedure

步骤 1 [配置 FTD 设备的系统设置](#)。

步骤 2 在“系统设置”(System Settings)页面上，点击设置菜单中的**日志记录(Logging)**。

步骤 3 数据日志记录。将数据日志记录 (**Data Logging**) 滑块滑动到开 (**On**) 以捕获诊断日志记录系统日志消息。点击加号按钮  以指定表示要向其发送事件的系统日志服务器的**系统日志服务器对象**。（此时您还可以创建系统日志服务器对象。）此外，请选择要记录的最低**消息严重性级别**级别。

这会将任何类型的系统日志消息的数据日志记录事件以及您选择的最低严重性级别发送到系统日志服务器。

Note 思科防御协调器 当前不支持为数据日志记录创建自定义日志记录过滤器。为了更好地控制向系统日志服务器发送的消息，我们建议您在 FDM 管理 设备中定义此设置。为此，请登录 FDM 管理 设备，然后导航至**系统设置 (System Settings) > 日志记录设置 (Logging Settings)**。

Tip 如果您是思科安全分析和日志记录客户，请勿启用数据日志记录，除非您将数据日志记录事件转发到**安全事件连接器**之外的系统日志服务器。数据事件（诊断事件）不是流量事件。将数据事件发送到不同的系统日志服务器可以消除 SEC 分析和过滤事件的负担。

步骤 4 文件/恶意软件日志设置。将滑块滑动到开 (**On**) 以捕获**文件事件 (File events)**和**恶意软件事件 (Malware events)**。指定表示要将事件发送到的系统日志服务器的**系统日志服务器对象**。如果尚未创建系统日志服务器对象，也可以在此时创建。

生成的文件和恶意软件事件的严重性级别相同。您选择的最低**消息严重性级别**级别将分配给所有文件和恶意软件事件。

触发任何访问控制规则中的文件或恶意软件策略时，会报告文件和恶意软件事件。这与连接事件不同。请注意，仅当您应用需要和恶意软件许可证的文件或恶意软件策略时，文件/恶意软件事件的系统日志设置才具有相关性。

对于思科安全分析和日志记录用户：

- 如果通过安全事件连接器 (SEC) 将事件发送到思科云，请指定 SEC 作为系统日志服务器。然后，您将能够在文件策略和恶意软件策略连接事件旁边看到这些事件。
- 如果您在没有 SEC 的情况下直接将事件发送到思科云，则无需启用此设置。如果访问控制规则配置为发送连接事件，则会发送文件和恶意软件事件。

步骤 5 入侵日志记录。通过指定表示要将事件发送到的系统日志服务器的**系统日志服务器对象**，将**入侵事件**发送到系统日志服务器。如果尚未创建系统日志服务器对象，也可以在此时创建。

触发任何访问控制规则中的入侵策略时，会报告入侵事件。这与连接事件不同。请注意，仅当您应用需要许可证的入侵策略时，入侵事件的系统日志设置才有意义。

对于思科安全分析和日志记录用户：

- 如果通过安全事件连接器 (SEC) 将事件发送到思科云，请指定 SEC 作为系统日志服务器。然后，您将能够在文件策略和恶意软件策略连接事件旁边看到这些事件。
- 如果您在没有 SEC 的情况下直接将事件发送到思科云，则无需启用此设置。如果访问控制规则配置为发送连接事件，则将入侵事件发送到思科云。

步骤 6 控制台过滤器。将滑块滑动到开 (On)，将数据日志记录（诊断日志记录）事件发送到控制台而不是系统日志服务器。此外，请选择要记录的最低事件严重性级别。这将为任何类型的系统日志消息发送数据日志记录事件，其中包含您选择的严重性级别。

当在 FDM 管理 设备的控制台端口上登录 CLI 时，您会看到这些消息。使用 **show console-output** 命令也可以在其他 FDM 管理 设备接口（包括管理接口）的 SSH 会话中看到这些日志。此外，从主 CLI 中输入 **system support diagnostic-cli** 即可在诊断 CLI 中实时查看这些消息。

步骤 7 点击保存 (Save)。

步骤 8 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

消息 严重性级别

下表列出系统日志消息严重性级别。

级别号	严重性级别	说明
0	应急	系统不可用。
1	警报	需要立即采取措施。
2	严重	严重情况。
3	错误	错误情况。
4	警告	警告情况。
5	通知	正常但重大的情况。
6	信息性	消息仅供参考。
7	调试	消息仅供调试。
Note	FDM管理 设备不会生成严重性级别为零（紧急）的系统日志消息。	

配置 DHCP 服务器

动态主机配置协议 (DHCP) 服务器可为 DHCP 客户端提供网络配置参数，例如 IP 地址。您可以在接口上配置 DHCP 服务器，为连接的网络上的 DHCP 客户端提供配置参数。

IPv4 DHCP 客户端使用广播而非组播地址到达服务器。DHCP 客户端侦听 UDP 端口 68 上的消息。DHCP 服务器侦听 UDP 端口 67 上的消息。DHCP 服务器不支持 BOOTP 请求。

DHCP 客户端必须与启用了服务器的接口位于同一网络内。服务器和客户端之间不能有干预路由器，但可以有交换机。



Caution 不要在已经有 DHCP 服务器运行的网络上配置 DHCP 服务器。这两个服务器间将发生冲突，结果不可预测。

Procedure

步骤 1 该部分有两个区域。一开始，配置区域显示全局参数。DHCP 服务器区域显示已在其上配置服务器的接口、服务器启用情况以及服务器的地址池。

步骤 2 在配置 (**Configuration**) 部分中，配置自动配置和全局设置。

DHCP 自动配置使 DHCP 服务器能为 DHCP 客户端提供从运行于指定接口上的 DHCP 客户端获得的 DNS 服务器、域名和 WINS 服务器信息。通常，如果您是在使用 DHCP 获取地址，则会使用自动配置，但您可以选择通过 DHCP 获取其地址的任何接口。如果无法使用自动配置，可以手动定义所需的选项。

- a. 如果要使用自动配置，请点击启用自动配置 (**Enable Auto Configuration**) 滑块，然后在从接口 (**From Interface**) 下拉列表中选择正在通过 DHCP 获取其地址的接口。
- b. 如果不启用自动配置，或者如果要覆盖任何一个自动配置的设置，请配置以下全局选项。这些设置将发送到托管 DHCP 服务器的所有接口上的 DHCP 客户端。
 1. **主 WINS IP 地址、辅助 WINS IP 地址。** Windows Internet Name Service (WINS) 服务器客户端应该用于 NetBIOS 域名解析的地址。
 2. **主 DNS IP 地址、辅助 DNS IP 地址。** 客户端应该用于域名解析的域名系统 (DNS) 服务器的地址。如果要使用思科 Umbrella DNS 服务器填充 DNS IP 地址字段，请点击应用 **Umbrella 设置 (Apply Umbrella Settings)**。点击该按钮会将正确的 IP 地址载入字段中。
- c. 点击**保存 (Save)**。

步骤 3 在“DHCP 服务器” (DHCP Servers) 部分中编辑现有服务器，或者点击**新建 DHCP 服务器 (New DHCP Server)** 以添加和配置新服务器。

- a. 配置服务器属性：
 1. **启用 DHCP 服务器。** 是否启用服务器。您可以配置服务器，但在做好准备开始使用之前，要一直将其禁用。
 2. **接口。** 选择您为客户端提供 DHCP 地址的接口。接口必须拥有静态 IP 地址；如果要在接口上运行 DHCP 服务器，则不能使用 DHCP 获取接口。对于网桥组，在网桥虚拟接口 (BVI) 上（而不是成员接口上）配置 DHCP 服务器，并且服务器在所有成员接口上运行。您不能在诊断接口上配置 DHCP 服务器，而应在管理接口上配置，它位于**设备 (Device) > 系统设置 (System Settings) > 管理接口 (Management Interface)** 页面中。
 3. **地址池。** 添加 DHCP 服务器的单个 IP 地址或 IP 地址范围。允许服务器为请求地址的客户端提供的 IP 地址的范围（最低至最高）。该 IP 地址范围必须与所选接口位于同一子网上，并且不能包括接口本身的 IP 地址、广播地址或子网地址。指定该池的开始和结束地址，用连字符隔开。例如 10.100.10.12-10.100.10.250。

b. 点击确定 (OK)。

步骤 4 点击保存 (Save)。

步骤 5 [预览和部署所有设备的配置更改](#)您现在所做的更改，或者等待并一次部署多个更改。

配置 DNS 服务器

域名系统 (DNS) 服务器用来将主机名解析到 IP 地址。管理接口用于 DNS 服务器。

Procedure

步骤 1 在主、辅助、第三 DNS IP 地址 (**Primary, Secondary, Tertiary DNS IP Address**) 中，按照首选项顺序输入最多三个 DNS 服务器的 IP 地址。正常情况下，会使用主 DNS 服务器，除非联系不上它，在这种情况下，会尝试使用辅助服务器，最终尝试第三服务器。如果要使用思科 Umbrella DNS 服务器填充 DNS IP 地址字段，请点击应用 **Umbrella 设置 (Apply Umbrella Settings)**。点击该按钮会将正确的 IP 地址载入字段中。

步骤 2 在域搜索名称 (**Domain Search Name**) 中，输入网络的域名，例如 example.com。此域将被附加到非完全限定的主机名，例如 serverA 而不是 serverA.example.com。

步骤 3 点击保存 (Save)。

步骤 4 [预览和部署所有设备的配置更改](#)您现在所做的更改，或者等待并一次部署多个更改。

管理接口

管理接口是一个连接到物理管理端口的虚拟接口。该物理端口名为诊断接口，可在“接口”页面上使用其他物理端口进行配置。在虚拟 FDM 管理设备上，即使两个接口都是虚拟接口，这种双重性也保持不变。

管理接口有两种用途：

- 您可以与该 IP 地址建立 Web 连接和 SSH 连接，并通过该接口配置设备。
- 系统通过此 IP 地址获取智能许可和数据库更新。

如果使用 CLI 安装向导，则在初始系统配置期间，为设备配置管理地址和网关。如果使用 FDM 管理安装向导，管理地址和网关将保留默认值。

如果需要，可以通过 FDM 管理设备来更改这些地址。您还可以在 CLI 中使用 **configure network ipv4 manual** 和 **configure network ipv6 manual** 命令更改管理地址和网关。

您可以定义静态地址，也可以在管理网络中有另一台设备用作 DHCP 服务器时，通过 DHCP 获取地址。默认情况下，管理地址是静态的，而且 DHCP 服务器通常运行在端口（虚拟 FDM 管理设备除外，它没有 DHCP 服务器）。因此，您可以将设备直接连接到管理端口并为工作站获取 DHCP 地址。这种方法可以十分方便地连接和配置设备。



Caution 如果更改当前连接的地址，则当保存更改时，由于这些更改会立即应用，您将丢失对 FDM 管理设备（或 CLI）的访问。您需要重新连接到设备。确保新地址有效且在管理网络中可用。

Procedure

- 步骤 1** 配置管理 IP 地址、网络掩码或 IPv6 前缀，并根据需要配置 IPv4 和/或 IPv6 的网关。必须配置至少一组属性。将一组设置留空将会禁用该寻址方法。
- 步骤 2** 依次选择**类型 > DHCP**，通过 DHCP 或 IPv6 自动配置功能获取地址和网关。但是，如果使用数据接口作为网关，则不能使用 DHCP。在此情况下，必须使用静态地址。
- 步骤 3** 点击**保存 (Save)**。
- 步骤 4** [预览和部署所有设备的配置更改](#)您现在所做的更改，或者等待并一次部署多个更改。

主机名

可以更改设备主机名。

Procedure

- 步骤 1** 在防火墙主机名 (**Firewall Hostname**) 字段中，输入设备的新主机名。
- 步骤 2** 点击**保存 (Save)**。
- 步骤 3** [预览和部署所有设备的配置更改](#)您现在所做的更改，或者等待并一次部署多个更改。

配置 NTP 服务器

配置网络时间协议 (NTP) 服务器才能在系统上设置时间。

Procedure

- 步骤 1** 选择使用您自己的（手动）时间服务器还是思科的时间服务器。
 - **新 NTP 服务器。** 输入您要使用的 NTP 服务器的完全限定域名或 IP 地址。例如 ntp1.example.com 或 10.100.10.10。
 - 使用默认值。
- 步骤 2** 点击 **Save**。

步骤 3 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

配置 URL 过滤

系统从思科综合安全情报 (CSI) 获取 URL 类别和信誉数据库。这些首选项控制数据库更新和系统如何处理类别或信誉未知的 URL。必须启用 URL 过滤许可证，才能设置这些首选项。



Caution 如果您没有 URL 智能许可证，则可以配置 URL 过滤首选项，但需要智能许可证才能部署。在添加 URL 智能许可证之前，系统将阻止您进行部署。

Procedure

步骤 1 启用应用选项：

- 点击**启用自动更新 (Enable Automatic Updates)** 滑块开启以允许系统自动检查和下载更新的 URL 数据，这些数据中包括类别和信誉信息。部署后，FDM 管理设备每 30 分钟检查一次更新。
- 点击**通过 Cisco CSI 查询未知 URL (Query Cisco CSI for Unknown URLs)** 滑块开启以对在本地 URL 过滤数据库中不含类别和信誉数据的 URL，是否通过 Cisco CSI 查询其更新的信息。
- 仅当启用**查询思科 CSI 以获取未知 URL (Query Cisco CSI for Unknown URLs)** 选项时，**URL 生存时间 (URL Time to Live)** 才有效。这决定了为给定 URL 缓存类别和信誉查找值的时间。生存时间到期时，下一个 URL 访问尝试将导致新的类别/信誉查找。更短的时间会产生更准确的 URL 过滤，较长的时间会给未知 URL 带来更好的表现。这是默认选择是**从不 (Never)**。

步骤 2 点击**保存 (Save)**。

步骤 3 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

云服务

使用“云服务”页面管理基于云的服务。



Note 可以在运行软件版本 6.6 及更高版本的 FTD 设备上配置连接到思科成功网络并配置将哪些事件发送到思科云的功能。

连接到思科成功网络

通过启用思科成功网络，可以向思科提供使用信息和统计信息，这对思科为您提供技术支持至关重要。通过此信息，思科还可以改进产品，并使您获悉未使用的可用功能，以便您能够在网络中将产品的价值最大化。

启用连接时，设备将与思科云建立安全连接，以确保设备可以参与思科提供的其他服务（例如技术支持服务、云管理和监控服务）。您的设备将随时建立并维护此安全连接。

准备工作

要启用思科成功网络，必须使用 FDM 管理设备向云注册设备。要注册该设备，请使用思科智能软件管理器（在“智能许可”页面上）注册该设备，或者通过输入注册密钥使用思科防御协调器进行注册。



Attention 如果您在高可用性组的主用设备上启用思科成功网络，也会在备用设备上启用该连接。

Procedure

- 步骤 1** 点击云服务 (Cloud Services) 选项卡。
 - 步骤 2** 点击思科成功网络功能的启用滑块，以根据需要更改设置。
 - 步骤 3** 点击保存 (Save)。
 - 步骤 4** 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。
-

将事件发送至思科云

可以将事件发送至思科云服务器。各种思科云服务均可从这里访问事件。然后，可以使用这些云应用（例如思科威胁响应）来分析事件并评估设备可能遇到的威胁。

准备工作

您必须先向思科智能软件管理器注册设备，然后才能启用此服务。

在美国地区通过 <https://visibility.amp.cisco.com/>，在欧盟地区通过 <https://visibility.amp.cisco.com/>，可以连接至思科威胁响应。您可以在 YouTube 上观看视频 (<http://cs.co/CTRvideos>)，了解此应用的使用方法和优点。有关思科威胁响应与 FTD 结合使用的更多信息，请参阅 <https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html> 处提供的《Firepower 和 CTR 集成指南》。

Procedure

- 步骤 1** 点击云服务 (Cloud Services) 选项卡。
- 步骤 2** 点击发送事件到思科云 (Send Events to the Cisco Cloud) 选项的启用 (Enabled) 滑块，以便根据需要更改设置。

步骤 3 当您启用该服务时，系统会提示您选择要发送到云的事件。

- **文件/恶意软件 (File/Malware)** - 适用于在任何访问控制规则中应用的任何文件策略。
- **入侵事件 (Intrusion Events)** - 适用于在任何访问控制规则中应用的任何入侵策略。
- **连接事件 (Connection Events)** - 适用于已启用日志记录的访问控制规则。选择此选项后，您还可以选择发送所有连接事件，或者只发送高优先级连接事件。高优先级连接事件是指与触发入侵、文件或恶意软件事件的连接相关，或与匹配安全智能阻止策略的连接相关。

步骤 4 点击**保存 (Save)**。

步骤 5 [预览和部署所有设备的配置更改](#)您现在所做的更改，或者等待并一次部署多个更改。

启用或禁用网络分析

启用网络分析可根据页面点击量向思科提供匿名产品使用情况信息。这类信息包括查看的页面、在页面上花费的时间、浏览器版本、产品版本、设备主机名等。此信息可帮助思科确定功能使用模式，帮助思科改进产品。所有使用情况数据均为匿名数据，且不会传输敏感数据。您可以使用 CDO 在所有版本的 FDM 管理设备上配置此功能。

默认启用网络分析。

Procedure

步骤 1 点击 **Web 分析 (Web Analytics)** 选项卡。

步骤 2 点击 **Web 分析 (Web Analytics)** 功能的**启用 (Enable)** 滑块，根据需要更改设置。

步骤 3 点击**保存 (Save)**。

步骤 4 [预览和部署所有设备的配置更改](#)您现在所做的更改，或者等待并一次部署多个更改。

CDO 命令行接口

CDO 为用户提供命令行界面 (CLI)，用于管理、FDM 管理 威胁防御 设备。用户可以将命令发送到单个设备或同时发送到多个设备。

相关信息：

- 有关 FTD CLI 文档，请参阅 [思科 Firepower 威胁防御命令参考](#)。请注意，FDM 管理设备的 CLI 功能有限。这些设备只有以下命令：`show`、`ping`、`traceroute`、`packet-tracer`、`failover` 和 `shutdown`。

使用命令行接口

Procedure

- 步骤 1 打开资产 (**Inventory**) 页面。
- 步骤 2 点击资产表上方的设备按钮。
- 步骤 3 使用设备选项卡和过滤器按钮查找要使用命令行界面 (CLI) 管理的设备。
- 步骤 4 选择设备。
- 步骤 5 在设备操作 (**Device Actions**) 窗格中，点击命令行接口 (**Command Line Interface**)。
- 步骤 6 点击 **命令行接口 (Command Line Interface)**。
- 步骤 7 在命令窗格中输入一个或多个命令，然后点击发送。设备对命令的响应显示在下面的“响应窗格”中。

Note 如果可以运行的命令有限制，则会在命令窗格上方列出这些限制。

Related Topics

[在命令行接口中输入命令](#)

在命令行接口中输入命令

可以在一行中输入单个命令，也可以在多行中依次输入多个命令，CDO 将按顺序执行这些命令。以下示例发送创建三个网络对象和包含这些网络对象的网络对象组的一批命令。ASA

```

> object network email_server_north
  host 192.168.10.2
  object network email_server_south
  host 192.168.20.2
  object network email_server_headquarters
  host 192.168.30.2
  object-group network email_servers_all
  network-object object email_server_north
  network-object object email_server_south
  network-object object email_server_headquarters
  
```

Press Cmd+Enter to send command

输入设备命令：CLI 控制台使用基本 CLI。**FDM 管理**威胁防御不能使用 CLI 控制台进入诊断 CLI、专家模式、FXOS CLI（在使用 FXOS 的型号上）。如果需要进入其他 CLI 模式，请使用 SSH。

使用命令历史记录

发送 CLI 命令后，CDO 会在“命令行界面” (Command Line Interface) 页面的历史记录窗格中记录该命令。您可以重新运行历史记录窗格中保存的命令，或将这些命令用作模板：

Procedure

步骤 1 在资产页面上，选择要配置的设备。

步骤 2 点击 **设备 (Devices)** 选项卡以找到设备。

步骤 3 点击设备类型选项卡。

步骤 4 点击 **>_命令行接口 (>_Command Line Interface)**。

步骤 5 点击时钟图标可展开历史记录窗格（如果尚未展开）。🕒

步骤 6 在历史记录窗格中选择要修改或重新发送的命令。

步骤 7 按原样重新使用命令，或在命令窗格中对其进行编辑，然后点击发送。CDO 在响应窗格中显示命令的结果。

Note CDO 显示 Done! 两种情况下响应窗格中的消息：

- 成功执行命令后。
- 当命令没有要返回的结果时。例如，您可以发出带有正则表达式的 `show` 命令，用于搜索配置条目。如果没有符合正则表达式条件的配置条目，CDO 将返回 Done!。

批量命令行接口

CDO 为用户提供使用命令行接口 (CLI) 管理 Secure Firewall ASA、FDM 管理 威胁防御、SSH、Cisco IOS 和 Cisco Secure Firewall Cloud Native 设备。用户可以将命令发送到单个设备或同时发送到多个同类设备。本节介绍一次向多台设备发送 CLI 命令。

相关信息：

- 对于设备文档，CDO 仅支持基本 FTD CLI。FDM 管理这些设备只有以下命令：`show`、`ping`、`traceroute`、`packet-tracer`、`failover` 和 `shutdown`。

有关 威胁防御 CLI 文档，请参阅 [思科 Firepower 威胁防御命令参考](#)。

批量 CLI 接口



Note CDO 显示 Done!两种情况下的消息:

- 成功执行命令且无错误后。
- 当命令没有要返回的结果时。例如，您可以发出带有正则表达式的 show 命令，用于搜索某个配置条目。如果没有符合正则表达式条件的配置条目，CDO 将返回 Done!。

编号	说明
1	点击时钟可展开或折叠命令历史记录窗格。
2	命令历史记录。发送命令后，CDO 会在此历史记录窗格中记录该命令，以便您可以返回到该窗格，选择并再次运行该命令。
3	命令窗格。在此窗格的提示符后输入命令。
4	<p>响应窗格。CDO 显示设备对命令的响应以及 CDO 消息。如果多个设备的响应相同，则响应窗格会显示消息“显示 X 台设备的响应” (Showing Responses for X devices)。点击 X 设备，CDO 将显示对命令返回相同响应的所有设备。</p> <p>Note CDO 显示 Done!两种情况下的消息:</p> <ul style="list-style-type: none"> • 成功执行命令且无错误后。 • 当命令没有要返回的结果时。例如，您可以发出带有正则表达式的 show 命令，用于搜索某个配置条目。如果没有符合正则表达式条件的配置条目，CDO 将返回 Done!。

编号	说明
5	我的列表选项卡显示您从资产表中选择的设备，并允许您包含或排除要向其发送命令的设备。
6	上图中突出显示的“执行”选项卡显示在历史记录窗格中选择的命令中的设备。在本例中， <code>show run</code> 在历史记录窗格中选择了 <code>grep</code> 用户命令，执行选项卡显示它已发送到 10.82.109.160、10.82.109.181 和 10.82.10.9.187。
7	点击“By Response”（按响应）选项卡将显示命令生成的响应列表。相同的响应组合在一行中。当您在“按响应”选项卡中选择一行时，CDO 会在响应窗格中显示对该命令的响应。
8	点击“按设备”选项卡会显示每个设备的单独响应。点击列表中的其中一个设备，即可查看特定设备对命令的响应。

批量发送命令

Procedure

- 步骤 1 在导航栏中，点击**资产 (Inventory)**。
- 步骤 2 点击**设备 (Devices)** 选项卡以找到设备。
- 步骤 3 选择相应的设备选项卡，然后使用过滤器按钮查找要使用命令行界面配置的设备。
- 步骤 4 选择设备。
- 步骤 5 在**设备操作 (Device Actions)** 窗格中，点击 **>_命令行接口 (>_Command Line Interface)**。
- 步骤 6 您可以在“我的列表”字段中选中或取消选中要向其发送命令的设备。
- 步骤 7 在命令窗格中输入命令，然后点击发送。命令输出显示在响应窗格中，命令记录在更改日志中，命令 CDO 在批量 CLI 窗口的历史记录窗格中记录您的命令。

使用批量命令历史记录

发送批量 CLI 命令后，CDO 会在“批量 CLI”页面历史记录页面中记录该命令。[批量 CLI 接口](#)您可以重新运行历史记录窗格中保存的命令，也可以将这些命令用作模板。历史记录窗格中的命令与运行这些命令的原始设备相关联。

Procedure

- 步骤 1 在导航栏中，点击**资产 (Inventory)**。
- 步骤 2 点击 **设备** 选项卡以找到设备。
- 步骤 3 点击相应的设备类型选项卡，然后点击过滤器图标以查找要配置的设备。

步骤 4 选择设备。

步骤 5 点击 **命令行接口 (Command Line Interface)**。

步骤 6 在“历史记录”窗格中选择要修改或重新发送的命令。请注意，您选择的命令与特定设备相关联，而不一定是您在第一步中选择的设备。

步骤 7 查看我的列表选项卡，确保您要发送的命令将发送到您期望的设备。

步骤 8 在命令窗格中编辑命令，然后点击发送。CDO 在响应窗格中显示命令的结果。

使用批量命令过滤器

运行批量 CLI 命令后，您可以使用“按响应”过滤器和“按设备”过滤器继续配置设备。

按响应过滤器

运行批量命令后，CDO 会使用发送该命令的设备返回的响应列表填充“按响应”选项卡。具有相同响应的设备会合并到一行中。点击“按响应” (By Response) 选项卡中的行会在响应窗格中显示设备的响应。如果响应窗格显示多个设备的响应，则会显示消息“显示 X 台设备的响应”。点击 X 设备，CDO 将显示对命令返回相同响应的所有设备。



要将命令发送到与命令响应关联的设备列表，请执行以下程序：

Procedure

步骤 1 点击 By Response 选项卡中一行中的命令符号。

步骤 2 查看命令窗格中的命令，然后点击发送以重新发送命令，或点击清除以清除命令窗格并输入要发送到设备的新命令，然后点击发送。

步骤 3 查看从命令收到的响应。

步骤 4 如果您确信所选设备上的运行配置文件反映了您的更改，请在命令窗格中键入 `write memory`，然后点击 **Send**。这样会将运行配置保存至启动配置。

按设备过滤器

运行批量命令后，CDO 会使用已发送命令的设备列表填充“执行”选项卡和“按设备”选项卡。点击“按设备” (By Device) 选项卡中的行会显示每个设备的响应。

要在同一设备列表上运行命令，请执行以下程序：

Procedure

- 步骤 1** 点击按设备 (By Device) 选项卡。
- 步骤 2** 点击 > 在这些设备上执行命令。
- 步骤 3** 点击清除以清除命令窗格并输入新命令。
- 步骤 4** 在我的列表窗格中，通过选中或取消选中列表中的单个设备来指定要向其发送命令的设备列表。
- 步骤 5** 点击发送 (Send)。命令的响应会显示在响应窗格中。如果响应窗格显示多个设备的响应，则会显示消息“显示 X 台设备的响应”。点击 X 设备，CDO 将显示对命令返回相同响应的所有设备。
- 步骤 6** 如果您确信所选设备上的运行配置文件反映了您的更改，请在命令窗格中键入 `write memory`，然后点击 Send。

用于管理设备的 CLI 宏

CLI 宏是可以使用的完整形式的 CLI 命令，或者是可以在运行之前修改的 CLI 命令的模板。所有宏都可以在一个或多个 FTD 设备上同时运行。

使用类似模板的 CLI 宏可同时在多台设备上运行相同的命令。CLI 宏可促进设备配置和管理的一致性。使用完全格式的 CLI 宏获取有关设备的信息。您可以立即在 FTD 设备上使用不同的 CLI 宏。

您可以创建 CLI 宏来监控您经常执行的任务。有关详细信息，请参阅[创建 CLI 宏](#)。

CLI 宏是系统定义的或用户定义的。系统定义的宏由 CDO 提供，无法编辑或删除。用户定义的宏由您创建，可以编辑或删除。



Note 只有在设备载入 CDO 后，才能为设备创建宏。

以 ASA 为例，如果要查找其中一个 ASA 上的特定用户，可以运行以下命令：

```
show running-config | grep username
```

运行命令时，您要将 `username` 替换为要搜索的用户的用户名。要使用此命令来创建宏，请使用相同的命令并在用户名周围加上大括号。

```
> show running-config | grep {{username}}
```

您可以随意命名参数。您还可以使用此参数名称创建相同的宏：

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

参数名称可以是描述性的，并且必须使用字母数字字符和下划线。命令语法，在本例中为

```
show running-config | grep
```

命令的一部分，必须对要向其发送命令的设备使用正确的 CLI 语法。

从新命令创建 CLI 宏

Procedure

步骤 1 在创建 CLI 宏之前，请在 CDO 的命令行界面中测试命令，以便确保命令语法正确并返回可靠的结果。

Note


- 对于 FTD 设备，CDO 仅支持可在 FDM 的 CLI 控制台中运行的命令：show、ping、traceroute、packet-tracer、failover、reboot 和 shutdown。有关这些命令的语法的完整说明，请参阅《思科 Firepower 威胁防御命令参考》。


步骤 2 在导航栏中，点击清单 (Inventory)。

步骤 3 点击设备 (Devices) 选项卡以找到设备。

步骤 4 点击相应的设备类型选项卡，然后选择在线和同步的设备。

步骤 5 点击 >_Command Line Interface。

步骤 6 点击 CLI 宏收藏夹星标 ，以查看已经存在的宏。

步骤 7 点击加号按钮 。

步骤 8 请为宏指定唯一的名称。如果需要，请为 CLI 宏提供说明和注释。

步骤 9 在命令 (Command) 字段中输入完整命令。

步骤 10 运行命令时，将要修改的命令部分替换为用大括号括起来的参数名称。

步骤 11 点击创建。您创建的宏可用于该类型的所有设备，而不只是您最初指定的设备。

要运行命令，请参阅[在设备上运行 CLI 宏](#)。

从 CLI 历史记录或现有 CLI 宏创建 CLI 宏

在此程序中，您将从已运行的命令、另一个用户定义的宏或从系统定义的宏创建用户定义的宏。

过程

步骤 1 在导航栏中，点击设备和服务。

注释 如果要从 CLI 历史记录创建用户定义的宏，请选择运行命令的设备。CLI 宏在同一账户上的设备之间共享，但不是 CLI 历史记录。

- 步骤 2** 点击**设备**选项卡。
- 步骤 3** 点击相应的设备类型选项卡，然后选择在线和同步的设备。
- 步骤 4** 点击 **>_命令行接口**。
- 步骤 5** 查找要生成 CLI 宏的命令，然后选择该命令。使用以下方法之一：
- 点击时钟可查看您在该设备上运行的命令。🕒 选择要转换为宏的命令，命令将显示在命令窗格中。
 - 点击 CLI 宏收藏夹星标★，以查看已经存在的宏。选择要更改的用户定义或系统定义的 CLI 宏。命令显示在命令窗格中。
- 步骤 6** 使用命令窗格中的命令，点击 CLI 宏金色星标。🌟 命令现在是新 CLI 宏的基础。
- 步骤 7** 请为宏指定唯一的名称。如果需要，请为 CLI 宏提供说明和注释。
- 步骤 8** 查看命令字段中的命令，并进行所需的更改。
- 步骤 9** 运行命令时，将要修改的命令部分替换为用大括号括起来的参数名称。
- 步骤 10** 点击**创建**。您创建的宏可用于该类型的所有设备，而不只是您最初指定的设备。
- 要运行命令，请参阅[运行 CLI 宏](#)。

运行 CLI 宏

Procedure

- 步骤 1** 在导航栏中，点击**设备和服务**。
- 步骤 2** 点击**设备**选项卡。
- 步骤 3** 点击相应的设备类型选项卡，然后选择一个或多个设备。
- 步骤 4** 点击 **>_命令行接口**。
- 步骤 5** 在命令面板中，点击星号★。
- 步骤 6** 从命令面板中选择 CLI 宏。
- 步骤 7** 使用以下两种方式之一运行宏：
- 如果宏没有要定义的参数，请点击**发送 (Send)**。命令的响应显示在响应窗格中。就行了。
 - 如果宏包含参数，例如下面的配置 DNS 宏，请点击 **>_查看参数**。

```

★ Using Macro: Configure DNS
> dns domain-lookup {{IF_NAME}}
   dns server-group DefaultDNS
   name-server {{IP_ADDR}}
  
```

- 步骤 8** 在“参数”(Parameters)窗格中，在“参数”(Parameters)字段中填写参数的值。

Parameters
✕

Parameters	Payload
IF_NAME <input style="width: 100%;" type="text" value="outside"/>	<pre>dns domain-lookup <u>outside</u> dns server-group DefaultDNS name-server <u>208.67.220.220</u></pre>
IP_ADDR <input style="width: 100%;" type="text" value="208.67.220.220"/>	

步骤 9 点击 **Send**。在 CDO 成功发送命令并更新设备配置后，您会收到消息完成！

- 对于 FTD，会更新设备的活动配置。

步骤 10 发送命令后，您可能会看到消息“某些命令可能已对运行配置进行了更改” (Some commands may have made changes to the running config) 以及两个链接。

⚠ Some commands may have made changes to the running config
 Write to Disk
Dismiss

- 点击**写入磁盘 (Write to Disk)** 会将此命令所做的更改以及运行配置中的任何其他更改保存到设备的启动配置中。
- 点击**消除 (Dismiss)**，可关闭消息。

编辑 CLI 宏

您可以编辑用户定义的 CLI 宏，但不能编辑系统定义的宏。编辑 CLI 宏会更改所有 FTD 设备。宏并非特定于特定设备。

Procedure


- 步骤 1** 在导航栏中，点击 **设备和服务**。
- 步骤 2** 点击**设备选项卡**。
- 步骤 3** 点击适当的设备类型选项卡。
- 步骤 4** 请选择您的设备。
- 步骤 5** 点击 **命令行接口 (Command Line Interface)**。
- 步骤 6** 选择要编辑的用户定义的宏。
- 步骤 7** 点击宏标签中的编辑图标。
- 步骤 8** 在编辑宏对话框中编辑 CLI 宏。
- 步骤 9** 点击**保存 (Save)**。

有关如何运行 CLI 宏的说明，请参阅[运行 CLI 宏](#)。

删除 CLI 宏

您可以删除用户定义的 CLI 宏，但不能删除系统定义的宏。删除 CLI 宏会删除所有设备的宏。宏并非特定于特定设备。

Procedure

- 步骤 1** 在导航栏中，点击 **设备和服务**。
- 步骤 2** 点击**设备**选项卡。
- 步骤 3** 点击适当的设备类型选项卡。
- 步骤 4** 请选择您的设备。
- 步骤 5** 点击 **>_命令行接口 (Command Line Interface)**。
- 步骤 6** 选择要删除的用户定义的 CLI 宏。
- 步骤 7** 点击 CLI 宏标签中的垃圾桶图标 。
- 步骤 8** 确认要删除 CLI 宏。

命令行接口文档

CDO 部分支持 FDM 管理 设备的命令行界面。我们在 CDO 中提供类似终端的接口，供用户以命令和响应形式同时向单个设备和多个设备发送命令。对于 CDO 中不支持的命令，请使用设备 GUI 终端（例如 PuTTY 或 SSH 客户端）访问设备，并参阅[CLI 文档](#)以了解更多命令。

导出 CLI 命令结果


您可以将向独立设备或多个设备发出的 CLI 命令结果导出为逗号分隔值 (.csv) 文件，以便您可以随意过滤和排序其中的信息。您可以导出单个设备或多个设备的 CLI 结果。导出的信息包含以下内容：

- 设备
- 日期
- 用户
- 命令
- 输出

导出 CLI 命令结果

您可以将刚刚在命令窗口中执行的命令的结果导出到 .csv 文件：



Procedure

- 步骤 1** 在导航栏中，点击**设备和服务 (Devices & Services)**。
 - 步骤 2** 点击**设备**选项卡。
 - 步骤 3** 点击适当的设备类型选项卡。
 - 步骤 4** 选择一个或多个设备，使其突出显示。
 - 步骤 5** 在设备的**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。
 - 步骤 6** 在命令行界面窗格中，输入命令并点击发送以向设备发出命令。
 - 步骤 7** 在已输入命令的窗口右侧，点击导出图标。
 - 步骤 8** 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。读取 .csv 文件上的命令输出时，展开所有单元格以查看命令的所有结果。
-

导出 CLI 宏的结果

您可以导出已在命令窗口中执行的宏的结果。使用以下程序可将在一台或多台设备上执行的 CLI 宏的结果导出到 .csv 文件：

Procedure

- 步骤 1** 打开 **设备和服务** 页面。
 - 步骤 2** 点击**设备**选项卡。
 - 步骤 3** 点击适当的设备类型选项卡。
 - 步骤 4** 选择一个或多个设备，使其突出显示。
 - 步骤 5** 在设备的**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。
 - 步骤 6** 在 CLI 窗口的左侧窗格中，选择 CLI 宏收藏夹星型。
 - 步骤 7** 点击要导出的宏命令。填写任何适当的参数，然后点击发送。
 - 步骤 8** 在已输入命令的窗口右侧，点击导出图标。
 - 步骤 9** 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。读取 .csv 文件上的命令输出时，展开所有单元格以查看命令的所有结果。
-

导出 CLI 命令历史记录

使用以下程序将一个或多个设备的 CLI 历史记录导出到 .csv 文件：

Procedure

步骤 1 在导航窗格中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备，使其突出显示。

步骤 5 在设备的“设备操作” (Device Actions) 窗格中，点击**命令行接口 (Command Line Interface)**。

步骤 6 如果历史记录窗格尚未展开，请点击时钟图标将其展开。🕒

步骤 7 在已输入命令的窗口右侧，点击导出图标。📄

步骤 8 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。读取 .csv 文件上的命令输出时，展开所有单元格以查看命令的所有结果。

相关信息：

- [CDO 命令行接口](#)
- [创建 CLI 宏](#)
- [删除 CLI 宏](#)
- [编辑 CLI 宏](#)
- [运行 CLI 宏](#)
- [FTD 命令行接口文档](#)
- [批量命令行接口](#)

导出 CLI 宏列表

您只能导出已在命令窗口中执行的宏。使用以下程序将一个或多个设备的 CLI 宏导出到 .csv 文件：

过程

步骤 1 在导航窗格中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备，使其突出显示。

步骤 5 在设备的“设备操作” (Device Actions) 窗格中，点击 **>_命令行接口 (>_Command Line Interface)**。

步骤 6 在 CLI 窗口的左侧窗格中，选择 CLI 宏收藏夹星型。★

步骤 7 点击要导出的宏命令。填写任何适当的参数，然后点击发送。

步骤 8 在已输入命令的窗口右侧，点击导出图标。📄

步骤 9 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。

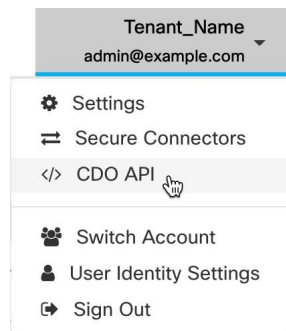
CDO 公共 API

CDO 已发布其公共 API，并为您提供文档、示例和试验场。我们的公共 API 的目标是为您提供一种简单而有效的方法来执行您通常能够在 CDO UI 中执行的许多操作，但在代码中。

要使用此 API，您需要了解 GraphQL。他们的官方指南 () 提供了全面、轻松的阅读。<https://graphql.org/learn/>

要查找完整的架构文档，请转到 GraphQL Playground，然后点击页面右侧的“文档”选项卡。
<https://edge.staging.cdo.cisco.com/api-explorer/playground-samples>

您可以通过从用户菜单中选择来启动 CDO 公共 API。



创建 REST API 宏

使用 API 工具

CDO 提供 API 工具接口来执行 FDM 管理设备具象状态传输 (REST) 应用编程 (API) 请求，以便在 FDM 管理设备上执行高级操作。REST API 使用 JavaScript 对象表示法 (JSON) 格式表示对象。

该接口提供系统定义或用户定义的 API 宏。系统定义的宏由 CDO 提供，无法编辑或删除。用户定义的宏由您创建，可以编辑或删除。您可以使用 Firepower 设备管理器 API Explorer 中支持的所有资源组。



Note CDO 仅支持返回 JSON 的 API 终端。

假定条件

假设您对编程有基本认识并对 REST API 和 JSON 有特定理解。如果您不熟悉这些技术，请首先阅读有关 REST API 的一般指南。

受支持的文档

- 有关详细信息，请参阅《[思科 Firepower 威胁防御 REST API 指南](#)》。
- 您还可以在 [思科 DevNet 站点](#) 上找到参考信息和示例。

支持的 HTTP 方法

仅可使用以下 HTTP 方法。



Important 具有 [只读](#) 角色的用户只能执行 GET 操作。

Attribute	说明
GET	从设备读取数据。
POST	为某种资源创建新对象。例如，使用 POST 方法创建新的网络对象。
PUT	更改现有资源的属性。使用 PUT 时，必须包含整个 JSON 对象。无法选择性地更新对象内的个别属性。例如，使用 PUT 方法修改现有网络对象中包含的地址。
DELETE	删除您或其他用户创建的资源。例如，使用 DELETE 方法删除您不再使用的网络对象。

相关信息：

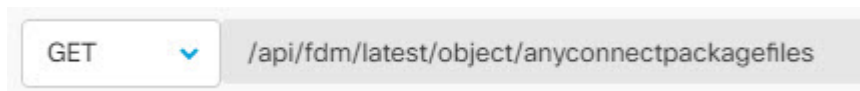
- [如何输入 Secure Firewall Threat Defense REST API 请求](#)
- [关于 FTD REST API 宏](#)
 - [创建 REST API 宏](#)
 - [运行 REST API 宏](#)
 - [编辑 REST API 宏](#)
 - [删除 REST API 宏](#)

如何输入 Secure Firewall Threat Defense REST API 请求

您可以选择 FDM 管理 设备并指定单个命令或执行需要其他参数的命令。

如果要确定 REST API 请求的语法，请登录到设备的 API Explorer 页面，例如 <https://ftd.example.com/#/api-explorer>，然后点击所需的资源组以查看要执行的命令的语法。例如，<https://10.10.5.84/#/api-explorer>。

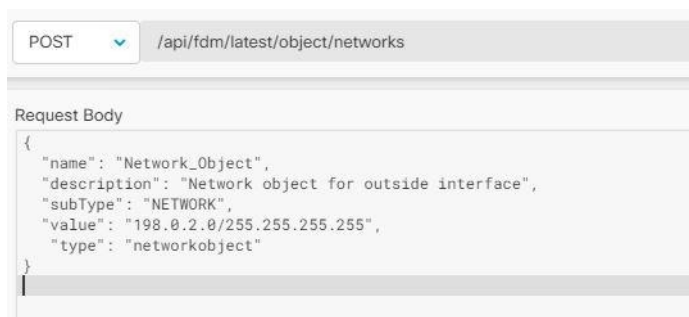
下图显示了 思科防御协调器 中的单个 REST API 请求的示例：



下图显示需要其他参数的 REST API 请求示例。您需要在请求正文 (Request Body) 中手动指定数据。如果要确定命令的语法，请登录设备的 API Explorer 页面。



Note 设备必须处于同步状态才能执行 POST 请求。



Procedure

- 步骤 1 在导航栏中，点击清单 (Inventory)。
- 步骤 2 点击 设备 选项卡以找到设备。
- 步骤 3 点击 FTD 选项卡。
- 步骤 4 选择要使用 REST API 管理的 FDM 管理 设备，然后在右侧的设备操作 (Device Actions) 中，点击 API 工具 (API Tool)。
- 步骤 5 从下拉列表中选择请求方法，然后键入 /api/fdm/latest/，然后键入要执行的命令。如果要执行 POST 或 PUT 命令，请输入请求正文。
- 步骤 6 点击 Send。响应正文 (Response Body) 会显示已执行命令的响应。

Important POST 请求通常会更改设备上的暂存配置。点击在 FDM 中提交更改 (Commit Changes in FDM)，将更改发送到 FDM 管理 设备。

相关信息:

- [使用 API 工具, on page 320](#)
- [关于 FTD REST API 宏](#)
 - [创建 REST API 宏](#)
 - [运行 REST API 宏](#)
 - [编辑 REST API 宏](#)
 - [删除 REST API 宏](#)

关于 FTD REST API 宏

REST API 宏是可以使用的完全格式的 REST API 命令，或者是可以在运行之前修改的 REST API 命令的模板。所有 REST API 宏都可以在一个或多个 FTD 设备上同时运行。

使用类似于模板的 REST API 宏同时在多个设备上运行相同的命令。REST API 宏可提高设备配置和管理的一致性。使用完全格式的 REST API 宏获取有关设备的信息。您可以立即在 FTD 设备上使用不同的 REST API 宏。

您可以为经常执行的任务创建 REST API 宏。有关详细信息，请参阅[创建 REST API 宏](#)。

REST API 宏是系统定义的或用户定义的。系统定义的宏由 CDO 提供，无法编辑或删除。用户定义的宏由您创建，可以编辑或删除。



Note 只有在设备载入 CDO 后，才能为设备创建宏。

相关信息:

- [创建 REST API 宏](#)
- [运行 REST API 宏](#)
- [编辑 REST API 宏](#)
- [删除 REST API 宏](#)

创建 REST API 宏

从新命令创建 REST API 宏


Procedure

- 步骤 1** 在创建 REST API 宏之前，请在 CDO 的 REST API 接口中测试命令，以便确保命令语法正确并返回可靠的结果。

Note 只有在设备载入 CDO 后，才能为设备创建宏。

步骤 2 选择要使用 REST API 管理的 FTD 设备，然后在右侧的设备操作 (**Device Actions**) 中，点击 **API 工具 (API Tool)**。

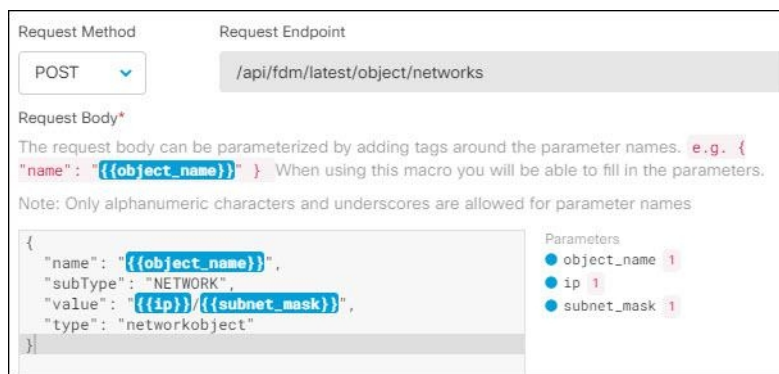
步骤 3 点击 REST API 宏收藏夹星标 ★，以查看已经存在的宏。

步骤 4 点击加号按钮 。

步骤 5 请为宏指定唯一的名称。如果需要，请为 REST API 宏提供说明和注释。

步骤 6 选择请求方法 (**Request Method**)，然后在请求终端 (**Request Endpoint**) 字段中输入终端 URL。有关详细信息，请参阅《[思科 Firepower 威胁防御 REST API 指南](#)》。

步骤 7 运行命令时，将要修改的命令部分替换为用大括号括起来的参数名称。



Request Method: POST

Request Endpoint: /api/fdm/latest/object/networks

Request Body*

The request body can be parameterized by adding tags around the parameter names. e.g. { "name": "{{object_name}}". } When using this macro you will be able to fill in the parameters.

Note: Only alphanumeric characters and underscores are allowed for parameter names

```
{
  "name": "{{object_name}}",
  "subType": "NETWORK",
  "value": "{{ip}}/{{subnet_mask}}",
  "type": "networkobject"
}
```

Parameters

- object_name 1
- ip 1
- subnet_mask 1

步骤 8 点击确定 (**OK**)。您创建的宏可用于该类型的所有设备，而不只是您最初指定的设备。

要运行命令，请参阅[运行 REST API 宏](#)。

从历史记录或现有 REST API 宏创建 REST API 宏

在此程序中，您将从已执行的命令、另一个用户定义的 REST API 宏或从系统定义的宏创建用户定义的宏。


Procedure


步骤 1 选择要使用 REST API 管理的 FDM 管理设备，然后在右侧的设备操作 (**Device Actions**) 中，点击 **API 工具 (API Tool)**。

Note 如果要从 REST API 历史记录创建用户定义的宏，请选择运行命令的设备。REST API 宏会在同一账户上的设备之间共享，但不会共享 REST API 历史记录。

步骤 2 查找要生成 REST API 宏的命令，然后选择该命令。使用以下方法之一：

- 点击时钟可查看您在该设备上运行的命令。🕒 双击选择要转换为宏的命令，命令将显示在命令窗格中。

- 点击 API 宏收藏夹星标 ，以查看已经存在的宏。选择要更改的用户定义或系统定义的 API 宏。命令显示在命令窗格中。

步骤 3 使用命令窗格中的命令，点击 API 宏金色星标 。命令现在是新 API 宏的基础。

步骤 4 请为宏指定唯一的名称。如果需要，请为 API 宏提供说明和注释。

步骤 5 查看命令字段中的命令，并进行所需的更改。

步骤 6 运行命令时，将要修改的命令部分替换为用大括号括起来的参数名称。

步骤 7 点击**创建**。您创建的宏可用于该类型的所有设备，而不只是您最初指定的设备。

要运行命令，请参阅[运行 REST API 宏](#)。

相关信息：

[关于 FTD REST API 宏](#)

运行 REST API 宏


Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

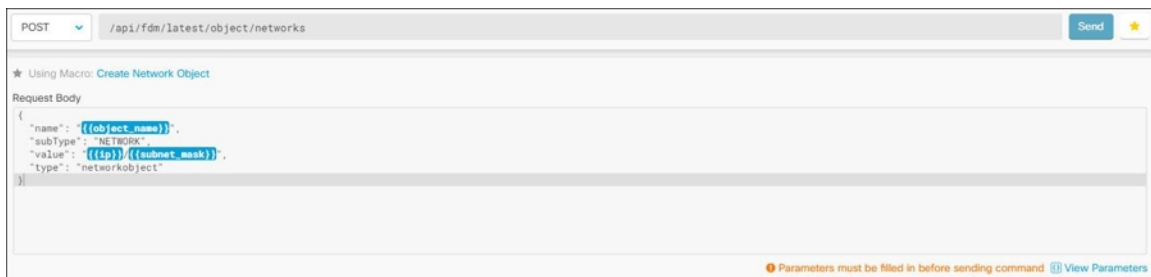
步骤 4 点击右侧设备操作 (**Device Actions**) 窗格中的 **API 工具 (API Tool)**。

步骤 5 在命令面板中，点击星号  查看 REST API 宏。

步骤 6 从命令面板中选择 REST API 宏。

步骤 7 使用以下两种方式之一运行宏：

- 如果宏没有要定义的参数，请点击**发送 (Send)**。命令的响应显示在响应窗格中。就行了。
- 如果宏包含参数，例如下面的“创建网络对象” (Create Network Object) 宏，请点击**查看参数 (View Parameters)**。



步骤 8 在**参数 (Parameters)** 窗格中，在“参数” (Parameters) 字段中填写参数的值。

Parameters
✕

Parameters	Payload
object_name <input style="width: 100%;" type="text" value="DNSObject"/>	<pre style="margin: 0;">{ "name": "DNSObject", "subType": "NETWORK", "value": "192.0.2.1 / 255.255.255.0", "type": "networkObject" }</pre>
ip <input style="width: 100%;" type="text" value="192.0.2.1"/>	
subnet_mask <input style="width: 100%;" type="text" value="255.255.255.0"/>	

Review
Send

步骤 9 点击 **Send**。

Note FTD 设备的活动配置已更新。

相关信息：

[关于 FTD REST API 宏](#)

编辑 REST API 宏

您可以编辑用户定义的 REST API 宏，但不能编辑系统定义的宏。编辑 REST API 宏会更改所有 FDM 管理 设备的宏。宏并非特定于特定设备。

Procedure

步骤 1 在导航栏中，点击清单 (**Inventory**)。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择要使用 REST API 管理的 FDM 管理 设备，然后在右侧的**设备操作 (Device Actions)** 中，点击 **API 工具 (API Tool)**。

步骤 5 选择要编辑的用户定义的宏。

步骤 6 点击宏标签中的编辑图标。

步骤 7 在编辑宏对话框中编辑 REST API 宏。

步骤 8 点击**保存 (Save)**。

有关如何运行 REST API 宏的说明，请参阅[运行 REST API 宏](#)。

相关信息：

[关于 FTD REST API 宏](#)

删除 REST API 宏

您可以删除用户定义的 REST API 宏，但不能删除系统定义的宏。删除 REST API 宏会删除所有设备的宏。宏并非特定于特定设备。

Procedure

- 步骤 1** 在导航栏中，点击**清单 (Inventory)**。
- 步骤 2** 点击 **设备** 选项卡以找到设备。
- 步骤 3** 点击 **FTD** 选项卡。
- 步骤 4** 选择一个设备，然后在右侧的**设备操作 (Device Actions)** 中，点击 **API 工具 (API Tool)**。
- 步骤 5** 选择要删除的用户定义的 REST API 宏。
- 步骤 6** 点击 REST API 宏标签中的垃圾桶图标 。
- 步骤 7** 确认要删除 REST API 宏。

相关信息：

[关于 FTD REST API 宏](#)

读取、丢弃、检查和部署更改

为了管理设备，CDO 必须在其本地数据库中存储自己的设备配置副本。当 CDO 从其管理的设备“读取”配置时，它会获取设备配置的副本并将其保存。CDO 首次和设备载入时读取并保存设备配置的副本。这些选项描述了出于不同目的而读取配置：

- 当设备的配置状态为“未同步”(Not Synced)时，可以使用**放弃更改 (Discard Changes)**。在“未同步”状态下，CDO 上的设备配置有待更改。此选项允许您撤消所有待处理的更改。待处理的更改将被删除，并且 CDO 会使用设备上存储的配置副本覆盖其配置副本。
- **检查更改**。如果设备的配置状态为“已同步”(Synced)，则此操作可用。点击“检查更改”(Checking for Changes)会指示 CDO 将其设备配置副本与设备上存储的配置副本进行比较。如果存在差异，CDO 会立即使用设备上存储的副本覆盖其设备配置副本。
- **审核冲突并接受而不审核**。如果您在设备上启用了**冲突检测 (Conflict Detection)**，CDO 会每 10 分钟检查一次设备上的配置更改。如果设备上存储的配置副本已更改，CDO 会通过显示“检测到冲突”配置状态来通知您。
 - **查看冲突**。点击查看冲突，您可以查看直接在设备上进行的更改，并接受或拒绝这些更改。
 - **接受而不审核**。此操作会使用设备上存储的最新配置副本来覆盖设备配置的 CDO 副本。在执行覆盖操作之前，CDO 不会提示您确认配置的两个副本中的差异。

读取所有是一个批处理操作。您可以选择任何状态的多个设备，然后点击**读取全部 (Read All)**，以使用设备上存储的配置覆盖 CDO 上存储的所有设备的配置。

部署更改

当您更改设备的配置时，CDO 会将您所做的更改保存到自己的配置副本中。在将这些更改部署到设备之前，这些更改在 CDO 上“待处理”。当设备的配置发生更改但尚未部署到设备时，该设备将处于“未同步”配置状态。

待处理的配置更改对通过设备运行的网络流量没有影响。只有在 CDO 将更改部署到设备后，它们才会生效。当 CDO 将更改部署到设备的配置时，它只会覆盖已更改的配置元素。它不会覆盖设备上存储的整个配置文件。可以为单个设备或同时在多个设备上启动部署。



注释 您可以安排部署或定期部署。有关详细信息，请参阅[计划自动部署](#)，第 335 页。

丢弃全部 (Discard All) 选项仅在您点击[预览并部署...\(Preview and Deploy...\)](#)。点击“预览并部署” (Preview and Deploy) 后，CDO 会向您显示 CDO 中待处理更改的预览。点击**丢弃全部 (Discard All)** 会从 CDO 中删除所有待处理的更改，并且不会将任何内容部署到所选设备。与上面的“放弃更改” (Discard Changes) 不同，删除待处理的更改是操作的结束。

读取所有设备配置

如果在 Cisco Defense Orchestrator (CDO) 之外对设备进行配置更改，则存储在 CDO 上的设备配置与其配置的本地副本将不再相同。您可能希望使用设备上存储的配置覆盖 CDO 的设备配置副本，以使配置再次相同。您可以使用[全部读取 \(Read All\)](#) 链接在多台设备上同时执行此任务。

有关 CDO 如何管理设备配置的两个副本的详细信息，请参阅[读取、丢弃、检查和部署更改](#)。

以下是三种配置状态，其中点击[全部读取 \(Read All\)](#) 将使用设备的配置副本覆盖 CDO 的设备配置副本。

- **检测到冲突 (Conflict Detected)** - 如果启用冲突检测，CDO 将每 10 分钟轮询一次其管理的设备，以了解对其配置所做的更改。如果 CDO 发现设备上的配置已更改，则 CDO 会显示设备的“检测到冲突” (Conflict detected) 配置状态。
- **已同步 (Synced)** - 如果设备处于同步状态，并且您点击[全部读取 \(Read All\)](#)，CDO 会立即检查设备以确定是否直接对其配置进行了任何更改。点击[读取全部 \(Read All\)](#) 后，CDO 会确认您是否打算覆盖其设备配置副本，然后 CDO 会执行覆盖。
- **未同步 (Not Synced)** - 如果设备处于未同步状态，并且您点击[全部读取 \(Read All\)](#)，则 CDO 会警告您使用 CDO 对设备的配置进行了待处理的更改，并且继续执行读取操作将删除这些更改，然后覆盖 CDO 的配置副本以及设备上的配置。此读取所有功能，例如[放弃更改](#)。

Procedure

步骤 1 从导航栏中，点击[清单 \(Inventory\)](#)。

步骤 2 点击设备 (**Devices**) 选项卡。

步骤 3 点击适当的设备类型选项卡。

- 步骤 4** （可选）创建[更改请求标签](#)以便在更改日志中轻松识别此批量操作的结果。
- 步骤 5** 选择要保存 CDO 配置的设备。请注意，CDO 仅提供可应用于所有选定设备的操作的命令按钮。
- 步骤 6** 点击[全部读取 \(Read All\)](#)。
- 步骤 7** 如果您选择的任何设备的 CDO 上有配置更改，CDO 会发出警告，并询问您是否要继续执行批量读取配置操作。点击[全部读取 \(Read All\)](#) 以继续。
- 步骤 8** 查看[通知选项卡](#)以了解“全部读取”(Read All)配置操作的进度。如果您想了解有关批量操作中各个操作是如何成功或失败的更多信息，请点击蓝色查看链接，您将被定向到“[作业 \(Jobs\)](#)”页面。
- 步骤 9** 如果您创建并激活了更改请求标签，请记住将其清除，以免无意中将其其他配置更改与此事件关联。

相关信息

- [读取、丢弃、检查和部署更改](#)
- [放弃更改](#)
- [检查配置更改](#)

将配置更改从 FDM 管理 设备读取到 CDO

为什么 Cisco Defense Orchestrator 会读取设备配置？FDM 管理

为了管理 FDM 管理 设备，CDO 必须拥有自己存储的 FDM 管理 设备配置文件副本。当 CDO 从 FDM 管理 设备读取配置时，它会获取 FDM 管理 设备已部署的配置副本并将其保存到自己的数据库中。CDO 首次读取并保存设备配置文件的副本是在设备载入时。有关详细信息，请参[阅读、丢弃、检查和部署更改](#)。

待处理和已部署的更改

直接通过 Firepower 设备管理器 (FDM) 或其 CLI 对设备进行的配置更改在部署之前称为设备上的暂存更改。FDM 管理 FDM 管理 可以编辑或删除已暂存或删除待处理的更改，而不会影响通过 FDM 管理 设备的流量。但是，部署待处理的更改后，它们会由 FDM 管理 设备实施并影响通过设备的流量。

检测到冲突

如果您在设备上启用[冲突检测](#)，则 CDO 会每 10 分钟检查一次配置更改。如果设备上存储的配置副本已更改，CDO 会通过显示“检测到冲突“(Conflict Detected)配置状态来通知您。如果您未启用冲突检测，或者在自动轮询之间的 10 分钟间隔内对设备的配置进行了更改，则点击检查更改会提示 CDO 立即比较设备上的配置副本与配置存储在 CDO 上。您可以选择查看冲突以检查设备配置与保存到 CDO 的配置之间的差异，然后选择放弃更改以删除暂存的更改并恢复为已保存的配置或确认更改。您也可以选择接受而不审核；此选项会获取配置并覆盖当前保存到 CDO 的内容。

放弃更改程序

要丢弃设备的配置更改，请执行以下程序：FDM 管理

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。


步骤 3 点击适当的设备类型选项卡。


步骤 4 选择其配置设置为检测到冲突的设备，并为您提供恢复待处理更改的链接。该消息说明您可以点击链接恢复待处理的更改，也可以使用本地管理器 FDM 登录设备并首先部署更改。您可以使用过滤器查找处于冲突状态的设备。[过滤器](#)

Caution 点击恢复待处理更改链接会立即删除设备上的待处理更改。FDM 管理您没有机会先查看更改。

步骤 5 在点击恢复待处理更改之前，查看 FDM 上的更改：

a. 打开浏览器窗口并输入 `https://< IP_address_of_the_FTD >`。

b. 在 FDM 中查找部署图标。系统将显示一个橙色圆圈，表示有可供部署的更改。

c. 点击  图标并查看待处理的更改：

- 如果可以删除更改，请返回 CDO 并点击“恢复待处理更改”。此时，设备上的配置和 CDO 上的配置副本应该相同。FDM 管理大功告成。
- 如果要将更改部署到设备，请点击立即部署。现在，设备上已部署的配置与 CDO 上存储的配置不同。FDM 管理然后，您可以返回到 CDO 并轮询设备以进行更改。[检查配置更改, on page 337](#)CDO 标识设备上已发生更改，并为您提供查看冲突的机会。FDM 管理请参阅[检测到冲突 - 查看冲突以解决该状态. 冲突检测, on page 339](#)

如果恢复待处理更改失败

CDO 无法恢复对系统数据库和安全源所做的更改。CDO 识别出有待处理的更改，尝试将其恢复，然后失败。要确定恢复失败的原因是数据库更新还是安全源更新，请登录设备的 FDM 控制台。系统

将显示一个橙色圆圈，表示有可供部署的更改。 点击部署按钮以查看待处理的更改，并根据需要部署或丢弃它们。

审核冲突程序

要从设备查看配置更改，请执行以下程序：FDM 管理

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择配置标记为“检测到冲突”的设备，并在右侧的“检测到的冲突”窗格中提供查看冲突的链接。

步骤 5 点击**查看冲突 (Review Conflict)**。

步骤 6 比较呈现给您的两种配置。

步骤 7 采取下列操作之一：

- 点击**接受**，用设备上找到的配置覆盖 CDO 上的最后一个已知配置。注意：存储在 CDO 上的整个配置将被设备上的配置完全覆盖。
- 点击**拒绝**以拒绝在设备上进行的更改，并将其替换为 CDO 上的最后一个已知配置。
- 点击**取消 (Cancel)** 以停止操作。

Note 当设备处于同步状态时，您可以通过点击**检查更改**来提示 CDO 立即检查设备的带外更改。[检查配置更改, on page 337](#)

接受而不审核程序

要接受设备的配置更改而不进行审核，请执行以下程序：FDM 管理

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择配置标记为“检测到冲突” (Conflict Detected) 的设备，并在右侧的“检测到冲突” (Conflict Detected) 窗格中显示接受而不审核的链接。

步骤 5 点击**接受而不审核 (Accept Without Review)**。CDO 接受并覆盖当前配置。

相关信息：

- [读取、丢弃、检查和部署更改](#)
- [冲突检测](#)
- [放弃更改](#)

预览和部署所有设备的配置更改

当您对租户上的设备进行了配置更改，但您尚未部署该更改时，CDO 会通过部署图标上显示一个橙色点来通知您




。受这些更改影响的设备在设备和服务 (Services) 页面中显示“未同步” (Not Synced) 状态。通过点击部署 (Deploy)，您可以查看哪些设备具有待处理的更改，并将更改部署到这些设备。

此部署方法适用于所有受支持的设备。

您可以将此部署方法用于单个配置更改，也可以等待并一次部署多个更改。

过程

- 步骤 1** 在屏幕的右上角，点击部署 (Deploy) 图标 。
- 步骤 2** 选择要部署更改的设备。如果设备有黄色警告三角形，则无法将更改部署到该设备。将鼠标悬停在黄色警告三角形上，了解无法将更改部署到该设备的原因。
- 步骤 3** 选择设备后，您可以在右侧面板中将其展开并预览其特定更改。
- 步骤 4** (可选) 如果要查看有关待处理更改的更多信息，请点击查看详细更改日志 (View Detailed Changelog) 链接以打开与该更改关联的更改日志。点击部署 (Deploy) 图标可返回具有待处理更改的设备 (Devices with Pending Changes) 页面。
- 步骤 5** (可选) 创建更改请求以跟踪更改，而无需离开具有待处理更改的设备 (Devices with Pending Changes) 页面。
- 步骤 6** 点击立即部署 (Deploy Now)，立即将更改部署到您选择的设备。您将在“作业” (Jobs) 托盘的“活动作业” (Active jobs) 指示器中看到进度。
- 步骤 7** (可选) 部署完成后，点击 CDO 导航栏中的作业 (Jobs)。您将看到最近的“部署更改” (Deploy Changes) 作业，其中显示了部署的结果。
- 步骤 8** 如果您创建了更改请求标签，并且没有其他配置更改与之关联，请将其清除。

下一步做什么

- [已计划的自动部署](#)
- [将配置更改从 CDO 部署到 FDM 管理设备，第 333 页](#)
- [部署到 FDM 管理设备后更改日志条目](#)

将配置更改从 CDO 部署到 FDM 管理设备

为什么 CDO 会将更改部署到 FDM 管理设备？

当您使用 CDO 管理和更改设备配置时，CDO 会将您所做的更改保存到自己的配置文件副本中。在部署到设备之前，这些更改将被视为已在 CDO 上暂存。暂存配置更改对通过设备运行的网络流量没有影响。只有在 CDO 将更改部署到设备后，它们才会影响通过设备运行的流量。当 CDO 将更改部署到设备的配置时，它只会覆盖已更改的配置元素。它不会覆盖设备上存储的整个配置文件。

与 CDO 一样，FDM 管理也有待处理更改和已部署更改的概念。FDM 管理设备上的待处理更改相当于 CDO 上的分阶段更改。可以编辑或删除待处理的更改，而不会影响通过 FDM 管理设备的流量。但是，部署待处理的更改后，它们会由 FDM 管理设备实施并影响通过设备的流量。

由于 FDM 托管设备有两步编辑配置文件，因此 CDO 将更改部署到 FDM 管理设备的方式与其管理的其他设备略有不同。CDO 首先将更改部署到 FDM 管理设备，并且更改处于待处理状态。然后，CDO 在设备上部署更改并使其生效。现在，更改已部署，并且会影响通过 FDM 管理设备运行的流量。这适用于独立设备和高可用性 (HA) 设备。

部署可以为单个设备或同时在多个设备上启动。您可以为单个设备安排单独的部署或定期部署。

有两件事会阻止 CDO 将更改部署到 FDM 管理设备：

- FDM 管理设备上是否存在分阶段更改。有关如何解决此状态的详细信息，请参阅[冲突检测](#)。
- 如果部署到 FDM 管理设备的过程发生更改，CDO 不会部署更改。

计划自动部署

您还可以将租户配置为将部署安排到具有[已计划的自动部署](#)的待处理更改。

将更改部署到设备

Procedure

步骤 1 使用 CDO 对设备进行配置更改并保存后，该更改将保存在设备配置的 CDO 实例中。


步骤 2 在导航栏中，点击 **设备和服务**。

步骤 3 点击**设备**选项卡。

步骤 4 点击适当的设备类型选项卡。您应该会看到您所做更改的设备的配置状态现在为“未同步”。

步骤 5 使用以下方法之一部署更改：

- 选择设备，然后在右侧的未同步窗格中，点击预览并部署。在 **Pending Changes** 屏幕上，查看更改。如果您对待定版本感到满意，请点击立即部署。成功部署更改后，您可以查看更改日志以确认刚刚发生的情况。[变更日志](#)

- 点击屏幕右上角的**部署 (Deploy)** 图标 。有关详细信息，请参阅[预览和部署所有设备的配置更改](#), on page 332。

取消更改

如果在将更改从 CDO 部署到设备时，点击取消，则所做的更改不会部署到设备。进程被取消。您所做的更改在 CDO 上仍处于待处理状态，可以在最终将其部署到设备之前进行进一步编辑。FDM 管理

放弃更改

如果在预览更改时点击**全部弃用 (Discard all)**，则您所做的更改以及任何其他用户所做但未部署到设备的任何其他更改都将被删除。在进行任何更改之前，CDO 将其待处理配置恢复为上次读取或部署的配置。

批量部署设备配置

如果您对多个设备进行了更改（例如通过编辑共享对象），则可以一次将这些更改应用到所有受影响的设备：

Procedure


步骤 1 在导航窗格中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。


步骤 4 选择已在 CDO 上进行配置更改的所有设备。这些设备应显示“未同步” (Not Synced) 状态。

步骤 5 使用以下方法之一部署更改：

- 点击屏幕右上角的**部署 (Deploy)** 按钮 。这使您有机会在部署之前查看所选设备上的待处理更改。点击**立即部署 (Deploy Now)** 以部署更改。

Note 如果在有待处理更改的设备 (**Devices with Pending Changes**) 屏幕上看到某个设备旁边显示黄色警告三角形，则无法将更改部署到该设备。将鼠标悬停在警告三角形上，了解有关无法将更改部署到该设备的信息。

- 点击详细信息窗格中的**全部部署 (Deploy All)** 。查看所有警告，然后点击**确定 (OK)**。批量部署会立即开始，无需审核更改。

步骤 6（可选）点击导航栏中的“作业” (Jobs) 图标  以查看批量部署的结果。

相关信息：

- [计划自动部署, on page 335](#)

已计划的自动部署

通过使用 CDO，您可以对其管理的一个或多个设备进行配置更改，然后安排在您方便的时间将更改部署到这些设备。

只有您在“设置” (Settings) 页面的租户设置 (Tenant Settings) 选项卡中 [启用计划自动部署的选项](#) 才能安排部署。一旦启用此选项，您就可以创建、编辑或删除计划部署。计划的部署会在设置的日期和时间部署在 CDO 上保存的所有暂存更改。您还可以在“作业” (Jobs) 页面中查看和删除计划部署。

如果直接对设备进行了尚未[读取、丢弃、检查和部署更改](#)到 CDO 的更改，则将跳过计划的部署，直到该冲突得以解决。“作业” (Jobs) 页面将列出计划部署失败的所有实例。如果[启用计划自动部署的选项 \(Enable the Option to Schedule Automatic Deployments\)](#) 被关闭，则所有计划的部署都将被删除。



Caution

如果您为多台设备安排新的部署，并且其中一些设备已安排了部署，则新的安排部署将覆盖现有的安排部署。



Note

当您创建计划部署时，将按照本地时间来创建计划，而不是设备的时区。计划的部署不会自动调整夏令时。

计划自动部署

部署计划可以是单个事件或周期性事件。您可能会发现定期自动部署是一种将定期部署与维护窗口对齐的便捷方式。请按照以下程序为单个设备安排一次性或周期性部署：



Note

如果为已安排现有部署的设备安排部署，新的安排部署将覆盖现有部署。

Procedure

步骤 1 在导航栏中，点击 [设备和服务](#)。

步骤 2 点击设备选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备。

步骤 5 在设备详细信息窗格中，找到计划的部署选项卡，然后点击计划 (**Schedule**)。

步骤 6 选择应进行部署的时间。

- 对于一次性部署，请点击**一旦开启 (Once on)** 选项以从日历中选择日期和时间。
- 对于周期性部署，请点击**每次 (Every)** 选项。您可以选择每天或每周一次部署。选择部署的日期 (**Day**) 和时间 (**Time**)。

步骤 7 点击保存 (**Save**)。

编辑计划部署

请按照以下程序编辑计划部署：

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击设备选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备。

步骤 5 在设备详细信息 (**Device Details**) 窗格中，找到计划的部署选项卡，然后点击**编辑 (Edit)**。



步骤 6 编辑计划部署的重复周期、日期或时间。

步骤 7 点击保存 (**Save**)。


删除计划部署

请按照以下程序删除计划部署：



Note 如果为多台设备安排部署，然后更改或删除某些设备的安排，则其余设备的原始安排部署将保留。

Procedure

- 步骤 1 在导航栏中，点击 **设备和服务 (Devices & Services)**。
- 步骤 2 点击 **设备** 选项卡。
- 步骤 3 点击适当的设备类型选项卡。
- 步骤 4 选择一个或多个设备。
- 步骤 5 在设备详细信息 (**Device Details**) 窗格中，找到计划的部署选项卡，然后点击 **删除 (Delete)** 

What to do next

- [读取、丢弃、检查和部署更改](#)
- [读取所有设备配置, on page 328](#)
- [将配置更改从 CDO 部署到 FDM 管理 设备, on page 333](#)
- [预览和部署所有设备的配置更改, on page 332](#)

检查配置更改

检查更改以确定设备的配置是否已直接在设备上更改，并且它不再与 CDO 上存储的配置副本相同。当设备处于“已同步” (Synced) 状态时，您将看到此选项。

要检查更改，请执行以下操作：

Procedure

- 步骤 1 在导航栏中，点击 **设备和服务**。
- 步骤 2 点击 **设备** 选项卡。
- 步骤 3 点击适当的设备类型选项卡。
- 步骤 4 选择您怀疑其配置可能已直接在设备上更改的设备。
- 步骤 5 点击右侧“已同步” (Synced) 窗格中的 **检查更改 (Check for Changes)**。
- 步骤 6 以下行为因设备而有细微差别：
 - 对于 FTD 设备，如果设备的配置发生变化，您将收到以下消息：

从设备读取策略。如果设备上有活动的部署，则将在完成后开始读取。

 - 点击 **OK** 继续操作。设备上的配置将覆盖 CDO 上存储的配置。
 - 点击 **取消 (Cancel)** 以取消操作。
 - 对于 设备：

- a. 比较呈现给您的两种配置。点击**继续**。标记为**最后已知的设备配置 (Last Known Device Configuration)**的配置是存储在 CDO 上的配置。标记为**在设备上找到 (Found on Device)**的配置是保存在 ASA 上的配置。
 - b. 选择以下选项中的一种：
 1. **拒绝带外更改**以保留“最后已知的设备配置”(Last Known Device Configuration)。
 2. **接受带外更改**，以使用设备上找到的配置来覆盖 CDO 中存储的设备配置。
 - c. 点击**继续**。
-

放弃更改

如果要“撤消”使用 CDO 对设备配置所做的所有未部署的配置更改，请点击**放弃更改 (Discard Changes)**。在点击**放弃更改 (Discard Changes)**时，CDO 会使用设备上存储的配置完全覆盖设备配置的本地副本。

点击**放弃更改 (Discard Changes)**时，设备的配置状态为**未同步 (Not Synced)**。在放弃更改后，CDO 上的配置副本将与设备上的配置副本相同，CDO 中的配置状态将恢复为“已同步”(Synced)。

要放弃或“撤消”设备的所有未部署的配置更改，请执行以下操作：

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择您已对其进行配置更改的设备。

步骤 5 点击右侧未同步窗格中的**放弃更改 (Discard Changes)**。

- 对于 FDM 管理设备，CDO 会警告您“CDO 上的待处理更改将被丢弃，此设备的 CDO 配置将替换为设备上当前运行的配置”(Pending changes on CDO will be discarded and the CDO configuration for this device will be replaced with the configuration currently running on the device)。点击**继续 (Continue)**以放弃更改。
 - 对于 Meraki 设备 - CDO 会立即删除更改。
 - 对于 AWS 设备 - CDO 会显示您要删除的内容。点击**接受 (Accept)**或**取消 (Cancel)**。
-

设备上的带外更改

带外更改是指在不使用 CDO 的情况下直接在设备上进行的更改。可以使用设备的命令行界面通过 SSH 连接进行这些更改，也可以使用本地管理器（例如适用于 ASA 的自适应安全设备管理器 (ASDM) 或适用于 FDM 管理设备的 FDM）进行这些更改。带外更改会导致 CDO 上存储的设备配置与设备本身上存储的配置之间发生冲突。

检测设备上的带外更改

如果为 ASA、FDM 管理设备或 Cisco IOS 设备启用了冲突检测，CDO 会每 10 分钟检查一次设备，以搜索在 CDO 之外直接对设备配置进行的任何新更改。

如果 CDO 发现未存储在 CDO 上的设备配置更改，则会将该设备的配置状态更改为“检测到冲突”状态。

当 Defense Orchestrator 检测到冲突时，可能出现以下两种情况：

- 直接对设备进行的配置更改尚未保存到 CDO 的数据库中。
- 对于 FDM 管理设备，FDM 管理设备上可能存在尚未部署的“待处理”配置更改。

同步 Defense Orchestrator 和设备之间的配置

关于配置冲突

在“设备和服务”页面上，您可能会看到设备或服务状态为“已同步” (Synced)、 “未同步” (Not Synced) 或 “检测到冲突” (Conflict Detected)。

- 如果设备为**已同步 (Synced)**，Cisco Defense Orchestrator (CDO) 上的配置与设备本地存储的配置相同。
- 如果设备为**未同步 (Not Synced)**，CDO 中存储的配置已更改，现在存储在设备上的配置有所不同。将您的更改从 CDO 部署到设备会更改设备上的配置以匹配 CDO 的版本。
- 在 CDO 之外对设备进行的更改称为**带外更改**。进行带外更改时，如果为设备启用了冲突检测，您会看到设备状态更改为“检测到冲突” (Conflict Detected)。接受带外更改会更改 CDO 上的配置以匹配设备上的配置。

冲突检测

启用冲突检测后，Cisco Defense Orchestrator (CDO) 将按默认间隔轮询设备，以确定是否在 CDO 之外对设备配置进行了更改。如果 CDO 检测到已进行更改，则会将设备的配置状态更改为**检测到冲突 (Conflict Detected)**。在 CDO 之外对设备进行的更改称为“带外”更改。

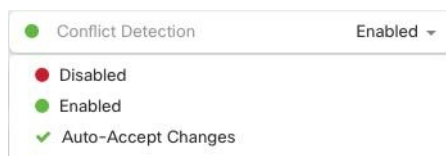
启用此选项后，您可以配置每台设备检测冲突或 OOB 更改的频率。有关详细信息，请参阅[安排设备更改轮询](#), on page 343。

启用冲突检测

启用冲突检测会提醒您在 Defense Orchestrator 之外对设备进行更改。

Procedure

- 步骤 1** 从导航栏中，点击清单 (**Inventory**)。
- 步骤 2** 点击设备选项卡。
- 步骤 3** 选择适当的设备类型选项卡。
- 步骤 4** 选择要启用冲突检测的设备。
- 步骤 5** 在设备表右侧的冲突检测框中，从列表中选择已启用。



自动接受设备的带外更改

您可以通过启用自动接受更改，将 Cisco Defense Orchestrator (CDO) 配置为自动接受直接对受管设备所做的任何更改。不使用 CDO 直接对设备进行的更改称为带外更改。带外更改会在 CDO 上存储的设备配置与设备本身上存储的配置之间产生冲突。

自动接受更改功能是对冲突检测的增强。如果您在设备上启用了自动接受更改，CDO 会每 10 分钟检查一次更改，以确定是否对设备的配置进行了任何带外更改。如果配置发生更改，CDO 会自动更新其本地版本的设备配置，而不会提示您。

如果对 CDO 进行的配置更改尚未部署到设备，则 CDO 不会自动接受配置更改。按照屏幕上的提示确定下一步操作。

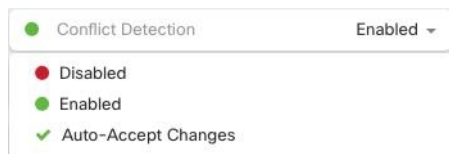
要使用自动接受更改，请先启用租户，以在清单 (**Inventory**) 菜单中显示自动接受选项；然后，您可以为单个设备启用自动接受更改。

如果您希望 CDO 检测带外更改，但为您提供手动接受或拒绝更改的选项，请改为启用 [冲突检测](#), on page 339。

配置自动接受更改

Procedure

- 步骤 1** 使用具有管理员或超级管理员权限的帐户登录 CDO。
- 步骤 2** 从 CDO 菜单中，导航至 **设置 (Settings) > 常规设置 (General Settings)**。
- 步骤 3** 在租户设置区域中，点击切换按钮以启用“自动接受设备更改的选项”。这将使“自动接受更改”菜单选项显示在“资产”页面的“冲突检测”菜单中。
- 步骤 4** 打开“资产”页面，然后选择要自动接受带外更改的设备。
- 步骤 5** 在“冲突检测” (Conflict Detection) 菜单中，选择下拉菜单中的“自动接受更改” (Auto-Accept Changes)。



为租户上的所有设备禁用自动接受更改

Procedure

- 步骤 1** 使用具有管理员或超级管理员权限的帐户登录 CDO。
- 步骤 2** 从 CDO 菜单中，导航至 **设置 (Settings) > 常规设置 (General Settings)**。
- 步骤 3** 在“租户设置”区域中，通过将切换开关向左滑动来禁用“启用自动接受设备更改的选项”，使其显示灰色 X。这将禁用“冲突检测”菜单中的“自动接受更改”选项，并为以下项禁用此功能：租户上的每台设备。

Note 禁用“自动接受”将要求您查看每个设备冲突，然后才能将其接受到 CDO 中。这包括之前配置为自动接受更改的设备。

解决配置冲突

本节提供有关解决设备上发生的配置冲突的信息。

解决“未同步”状态

使用以下程序解决配置状态为“未同步”的设备：

Procedure

步骤 1 在导航栏中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击**设备**选项卡以查找设备，或点击**模板**选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择报告为“未同步”的设备。

步骤 5 在右侧的未同步面板中，选择以下任一选项：

- **预览并部署...** - 如果要配置更改从 CDO 推送到设备，请预览并部署您现在所做的更改，或者等待并一次部署多个更改。[预览和部署所有设备的配置更改, on page 332](#)
 - **放弃更改** - 如果您不想将配置更改从 CDO 推送到设备，或者您想要“撤消”您开始在 CDO 上进行的配置更改。此选项使用设备上存储的运行配置覆盖 CDO 中存储的配置。
-

解决“检测到冲突”状态

CDO 允许您在每个实时设备上启用或禁用冲突检测。如果 [冲突检测, on page 339](#) 已启用，并且在未使用 CDO 的情况下对设备的配置进行了更改，则设备的配置状态将显示为**检测到冲突 (Conflict Detected)**。

要解决“检测到冲突” (Conflict Detected) 状态，请执行以下程序：

Procedure

步骤 1 在导航栏中，点击**设备和服务**。

步骤 2 点击**设备 (Devices)**选项卡以找到设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择报告冲突的设备，然后点击右侧详细信息窗格中的**查看冲突 (Review Conflict)**。

步骤 5 在**设备同步 (Device Sync)**页面中，通过查看突出显示的差异来比较两种配置。

- 标记为“最后一次设备配置” (Last Known Device Configuration) 的面板是存储在 CDO 上的设备配置。
- 标记为“在设备上找到” (Found on Device) 的面板是存储在运行 ASA 配置中的配置。

步骤 6 通过选择以下选项之一来解决冲突：

- **接受设备更改 (Accept Device changes):** 这将使用设备的运行配置覆盖 CDO 上存储的配置 和任何待处理的更改。

Note 由于 CDO 不支持在命令行界面之外部署对 Cisco IOS 设备的更改，因此在解决冲突时，您对 Cisco IOS 设备的唯一选择是选择**接受而不查看 (Accept Without Review)**。

- **拒绝设备更改 (Reject Device Changes):** 这将使用存储在 CDO 上的配置覆盖设备上存储的配置。

Note 所有配置更改（拒绝或接受）都记录在更改日志中。

安排设备更改轮询

如果已启用 [冲突检测](#), on page 339 或从“设置” (Settings) 页面 启用自动接受设备更改的选项 (**Enable the option to auto-accept device changes**)，则 CDO 将按默认间隔轮询设备，以确定是否在 CDO 之外对设备配置进行了更改。您可以自定义 CDO 轮询每台设备更改的频率。这些更改可以应用于多个设备。

如果没有为设备配置选择，则会自动为“租户默认”配置间隔。

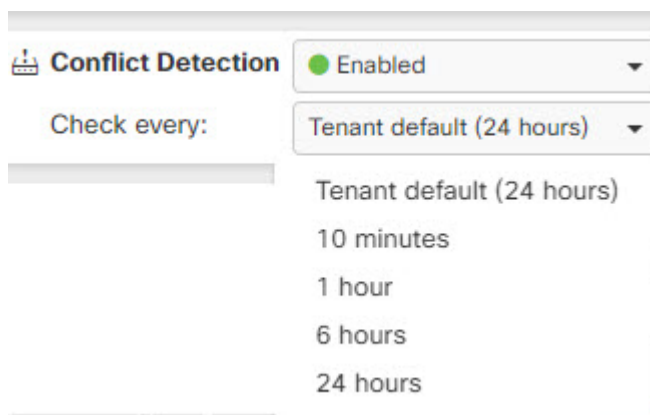


Note 从设备和服 务 (**Devices & Services**) 页面自定义每台设备的间隔会覆盖从常规设置 (**General Settings**) 页面选择作为 [默认冲突检测间隔 \(Default Conflict Detection Interval\)](#) 的轮询间隔。

从设备和服 务 (**Devices & Services**) 页面启用冲突检测 (**Conflict Detection**) 或从“设置” (Settings) 页面选择启用该选项以自动接受设备更改 (**Enable the option to auto-accept device changes**) 后，请使用以下程序来安排您希望 CDO 轮询设备的频率：

Procedure

- 步骤 1** 在导航栏中，点击 **设备和服 务**。
- 步骤 2** 点击 **设备** 选项卡，找到您的设备。
- 步骤 3** 点击设备类型选项卡。
- 步骤 4** 选择要启用冲突检测的设备。
- 步骤 5** 在与冲突检测 (**Conflict Detection**) 相同的区域中，点击**检查间隔 (Check every)** 下拉菜单，然后选择所需的轮询间隔：



安排安全数据库更新

本节提供有关在设备上安排安全数据库更新的信息。

创建计划安全数据库更新

使用以下程序创建一个计划的任务，以检查和更新 FTD 设备的安全数据库：

Procedure

步骤 1 在导航栏中，点击清单 (**Inventory**)。


步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择设备。

步骤 5 在操作 (**Actions**) 窗格中，找到安全数据库更新 (**Security Database Updates**) 部分，然后点击添加 + 按钮。

Note

如果所选设备已存在计划任务，请点击编辑图标  以创建新任务。创建新任务将覆盖现有任务。

步骤 6 使用以下内容配置计划任务：

- **频率 (Frequency)**。选择每天、每周或每月进行更新。
- **时间 (Time)**。选择每天的某个时间。请注意，显示的时间为 UTC。
- **选择天数 (Select Days)**。选择您希望在一周内的哪一天进行更新。

步骤 7 点击保存 (Save)。

设备的配置状态将更改为“正在更新数据库”(Updating Databases)。

编辑计划安全数据库更新

使用以下程序编辑现有的计划任务，以检查和更新 FTD 设备的安全数据库。


Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择设备。

步骤 5 在操作 (**Actions**) 窗格中，找到**安全数据库更新 (Security Database Updates)** 部分，然后点击编辑图标 。

步骤 6 使用以下命令编辑计划任务：

- **频率**。选择每天、每周或每月进行更新。
- **时间 (Time)**。选择每天的某个时间。请注意，显示的时间为 UTC。
- **选择天数 (Select Days)**。选择您希望在一周内的哪一天进行更新。

步骤 7 点击保存 (Save)。

步骤 8 设备的配置状态将更改为“正在更新数据库”(Updating Databases)。

更新 FDM 管理 设备安全数据库

通过更新 FDM 管理 设备上的安全数据库，您将更新以下内容：SRU（入侵规则）、安全情报 (SI)、漏洞数据库 (VDB) 以及地理位置数据库。如果您选择通过 思科防御协调器 UI 来更新安全数据库，请注意，所有提到的数据库都会更新；您无法选择要更新的数据库。

请注意，安全数据库更新无法恢复。



Note 在更新安全数据库时，某些数据包可能会被丢弃或不经检查通过。我们建议您在维护窗口期间安排安全数据库更新。

载入时更新 FDM 管理 设备安全数据库

当您将在 FDM 管理 设备载入 CDO 时，在载入过程中可以启用计划的数据库定期更新。默认情况下，会选中此选项。启用后，CDO 会立即检查并应用任何安全更新，并自动安排设备检查是否有额外更新。在设备载入后，您可以修改计划任务的日期和时间。

我们建议在载入过程中启用自动计划程序，以定期检查和应用安全数据库更新。这样，您的设备将始终保持最新状态。要在载入 FDM 管理 设备时更新安全数据库，请参阅[使用注册密钥载入 FDM 托管设备](#)。



Note 如果使用注册密钥方法载入设备，则不得使用智能许可证来注册设备。我们建议注册许可证。作为替代方法，您可以使用设备的用户名、密码和 IP 地址来载入设备。

载入后更新 FDM 管理 设备安全数据库

在 FDM 管理 设备被载入 CDO 后，您可以通过安排更新来配置设备，以便检查安全数据库更新。您可以通过选择计划更新的设备来随时修改此计划任务。有关详细信息，请参阅[安排安全数据库更新](#)。

工作流程

设备许可证

如果没有许可证，思科防御协调器 将无法更新安全数据库。我们建议您的设备至少具有 Essentials 许可证。FDM 管理

如果您要自行激活没有许可证的设备，这不会阻止 CDO 自行激活设备。相反，设备将遇到“许可证不足”的连接状态。要解决此问题，您必须通过 FDM 管理 设备 UI 应用正确的许可证。



Note 如果您载入 FDM 管理设备并选择计划未来的安全数据库更新，并且设备没有注册的许可证，则 CDO 仍会创建计划任务，但在应用适当的许可证且设备成功同步之前不会触发该任务。

安全数据库更新在 FDM 中待处理

如果您通过 FDM 管理 设备 UI 更新安全数据库，并且您在设备上启用了冲突检测，则 CDO 会将待处理的更新检测为冲突。



Note 如果您载入 FDM 管理 设备并选择安排更新，则 CDO 会在下次部署期间自动更新安全数据库以及对已存储配置的任何其他待处理更改。不必是配置部署

在安全数据库更新期间，设备具有 OOB 更改或暂存更改

如果为具有带外 (OOB) 更改或尚未部署的暂存更改的 FDM 管理 设备安排安全数据库更新，则 CDO 只会检查和更新安全数据库。CDO 不会部署 OOB 或暂存更改。

设备已有更新安全数据库的计划任务

每台设备只能有一个计划任务。如果设备已有更新安全数据库的计划任务，则创建新任务会覆盖该任务。这适用于在 CDO 或 FDM 管理 设备上创建的任务。

没有可用的安全数据库更新

如果没有可用的更新，CDO 不会向设备部署任何内容。

高可用性 (HA) 对的安全数据库更新 FDM 管理

安全数据库更新仅应用于 HA 对的主设备。

相关信息：

- [使用注册密钥载入 FDM 托管设备](#)
- [使用用户名、密码和 IP 地址载入 FDM 管理 设备](#)
- [安排安全数据库更新](#)

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。