配置基本策略

使用以下设置配置基本安全策略：

- 内部和外部接口 - 为内部接口分配静态 IP 地址，并将 DHCP 用作外部接口。
- DHCP 服务器 - 在内部接口上为客户端使用 DHCP 服务器。
- 默认路由 - 通过外部接口添加默认路由。
- NAT - 在外部接口上使用接口 PAT。
- 访问控制 - 允许流量从内部传到外部。

您还可以自定义安全策略，以包括更高级的检查。

- 配置接口，第 1 页
- 配置 DHCP 服务器，第 6 页
- 配置 NAT，第 7 页
- 配置访问控制规则，第 10 页
- 在外部接口上启用 SSH，第 13 页
- 部署配置，第 14 页

配置接口

使用 零接触调配 或 设备管理器 而不是 CLI 进行初始设置时，系统会预配置以下接口：

- 以太网 1/1 - **outside**，IP 地址来自 DHCP、IPv6 自动配置
- VLAN1 - **inside**，192.168.95.1/24
- 默认路由 - 通过外部接口上的 DHCP 获取

如果在向 管理中心 注册之前在 设备管理器 中执行其他特定于接口的配置，则会保留该配置。

如果使用 CLI 进行初始设置，则无需对设备进行预配置。

在两种情况下，您都需要在注册设备后执行其他接口配置。要进行 CLI 初始设置，必须为内部交换机端口添加 VLAN1 接口。其他配置包括根据需要将交换机端口转换为防火墙接口、将接口分配给安全区域以及更改 IP 地址。

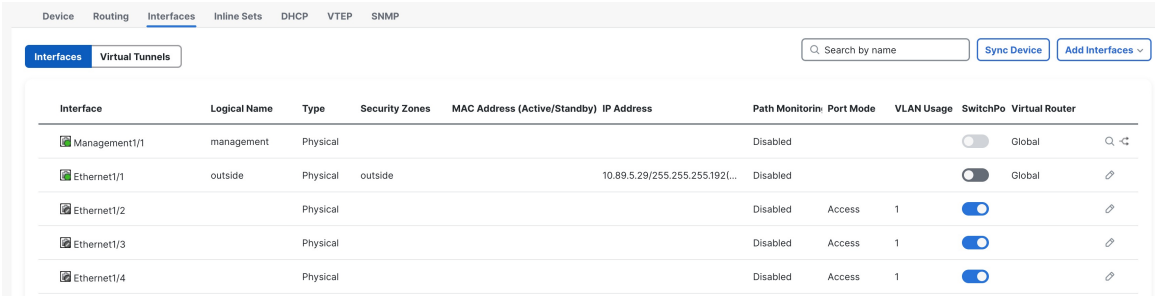
以下示例配置了一个含静态地址的路由模式内部接口 (VLAN1)，以及一个使用 DHCP 的路由模式外部接口（以太网 1/1）。它还会为内部 Web 服务器添加一个 DMZ 接口。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击设备的**编辑** ()。

步骤 2 点击**接口 (Interfaces)**。

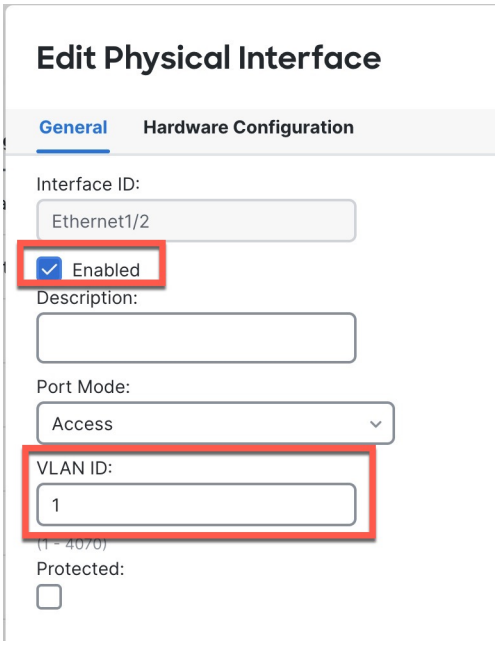
图 *1:* 接口



步骤 3 如果使用 CLI 进行初始设置，请启用交换机端口。

a) 点击交换机端口的 **编辑** ()。

图 *2:* 启用交换机端口

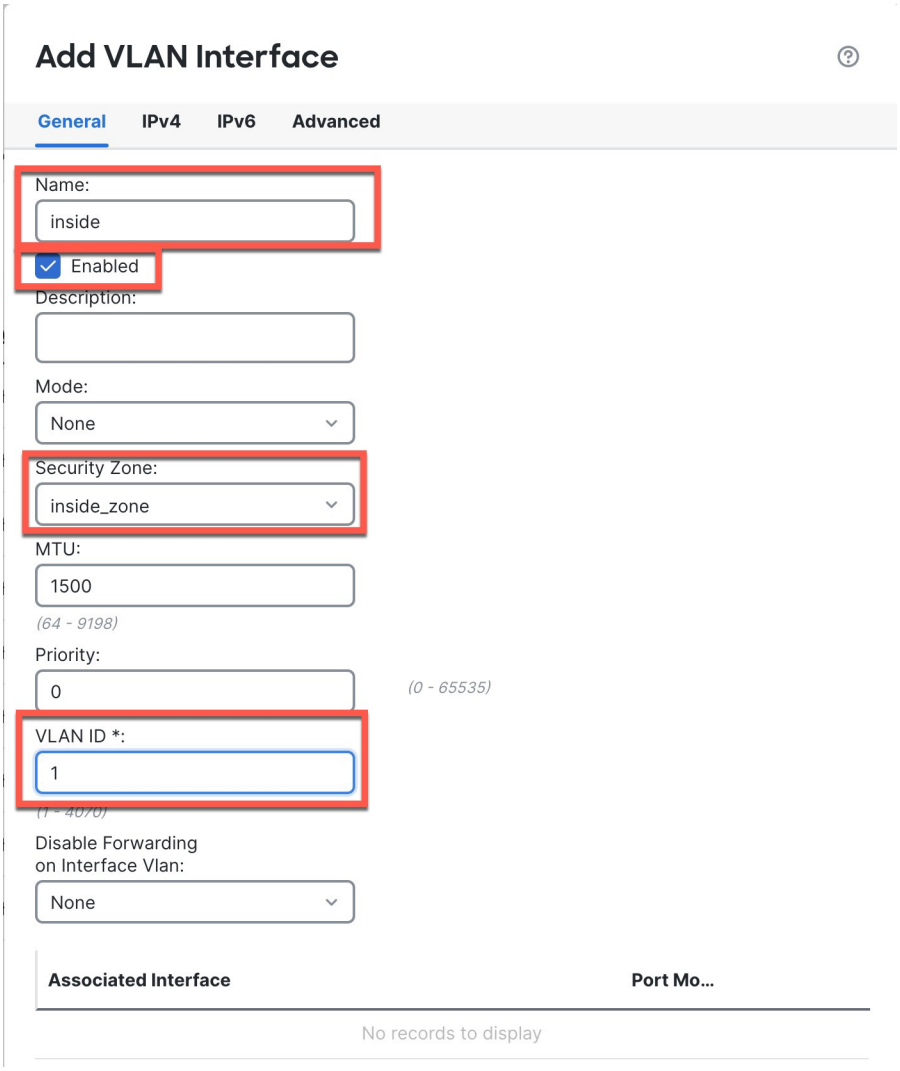


b) 选中**启用**复选框以启用此接口。
c) （可选）更改 VLAN ID；默认值为 1。接下来，您将添加一个 VLAN 接口来匹配此 ID。
d) 点击**确定 (OK)**。

步骤 4 添加（或编辑）**内部** VLAN 接口。

a) 点击**添加接口 (Add Interfaces)** > **VLAN 接口 (VLAN Interface)**；如果此接口已存在，请点击该接口的 **编辑** ()。

图 *3:* 添加 *VLAN* 接口



b) 从**安全区域 (Security Zone)** 下拉列表中选择一个现有的内部安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

例如，添加一个名为 **inside_zone** 的区域。您可以根据区域或组应用安全策略。

如果 VLAN1 已预配置，则其余字段为可选。

c) 输入长度最大为 48 个字符的**名称 (Name)**。

例如，将接口命名为 **inside**。

d) 选中**启用 (Enabled)** 复选框。

e) 将**模式 (Mode)** 保留为**无 (None)**。

f) 将 **VLAN ID** 设置为 **1**。

默认情况下，所有交换机端口都设置为 VLAN 1；如果在此处选择不同的 VLAN ID，还需要编辑每个交换机端口，使其位于新 VLAN ID 所对应的 VLAN 上。

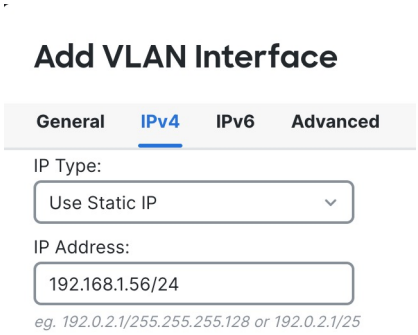
保存接口后，无法更改 VLAN ID；VLAN ID 既是使用的 VLAN 标记，也是您的配置中的接口 ID。

g) 点击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 从下拉列表中选择**使用静态 IP (Use Static IP)**，然后以斜杠表示法输入 IP 地址和子网掩码。

  例如，输入 **192.168.1.56/24**

  图 *4:* 设置内部 *IP* 地址



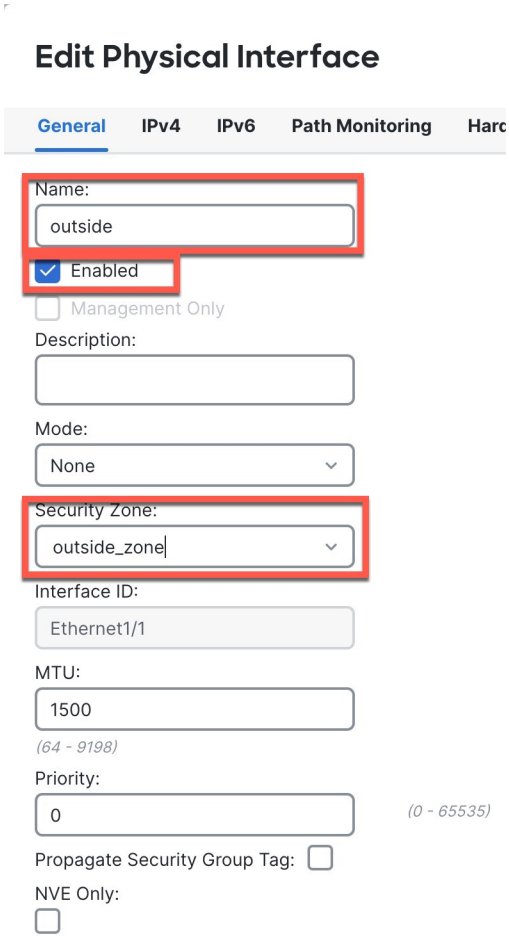
- **IPv6** - 为无状态自动配置选中**自动配置 (Autoconfiguration)** 复选框。

h) 点击**确定 (OK)**。

步骤 5 点击要用于**外部**的以太网 1/1 的 **编辑** (✎)。

系统将显示**一般 (General)** 窗格。

图 *5:* 常规



a) 从**安全区域 (Security Zone)** 下拉列表中选择一个现有的外部安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

例如，添加一个名为 **outside_zone** 的区域。

您不应更改任何其他基本设置，因为这样做会中断 管理中心 管理连接。

b) 点击**确定 (OK)**。

步骤 6 例如，配置 DMZ 接口以托管 Web 服务器。

a) 单击 **SwitchPort** 列中的滑块，禁用要用于 DMZ 的交换机端口的交换机端口模式（ ）。

b) 点击接口的 **编辑** ( )。

c) 从**安全区域 (Security Zone)** 下拉列表中选择一个现有的 DMZ 安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

例如，添加一个名为 **dmz_zone** 的区域。

d) 输入长度最大为 48 个字符的**名称 (Name)**。

例如，将接口命名为 **dmz**。

e) 选中**启用 (Enabled)** 复选框。
f) 将**模式 (Mode)** 保留为**无 (None)**。
g) 点击 **IPv4** 和/或 **IPv6** 选项卡并配置所需的 IP 地址。
h) 点击**确定 (OK)**。

步骤 7 点击**保存 (Save)**。

配置 DHCP 服务器

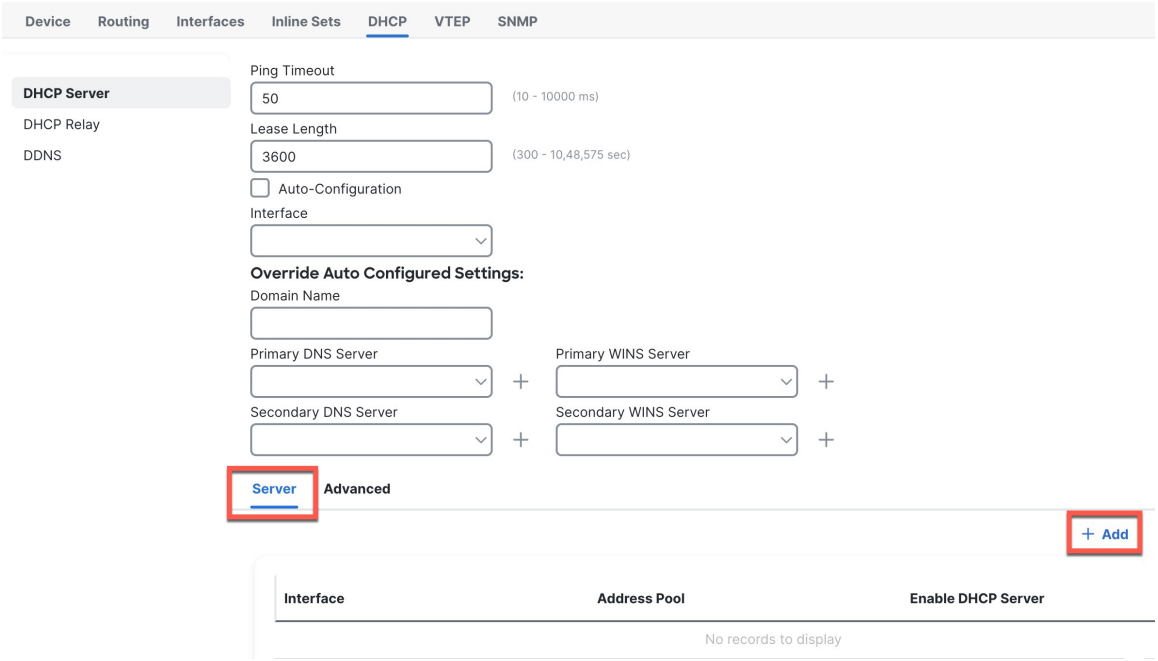
如果希望客户端使用 DHCP 从防火墙获取 IP 地址，请启用 DHCP 服务器。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击设备的**编辑** ()。

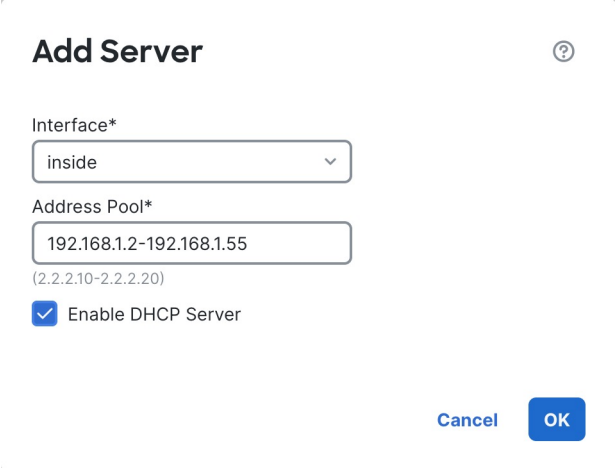
步骤 2 选择 **DHCP** > **DHCP 服务器 (DHCP Server)**。

图 *6: DHCP* 服务器



步骤 3 在**服务器 (Server)** 区域中，点击**添加 (Add)** 并配置以下选项。

图 7: 添加服务器



- **接口 (Interface)** - 从下拉列表中选择接口名称。
- **地址池 (Address Pool)** - 设置 IP 地址的范围。IP 地址必须与选定接口位于相同的子网上，且不能包括接口自身的 IP 地址。
- **启用 DHCP 服务器 (Enable DHCP Server)** - 在所选接口上启用 DHCP 服务器。

步骤 4 点击**确定 (OK)**。

步骤 5 点击**保存 (Save)**。

配置 NAT

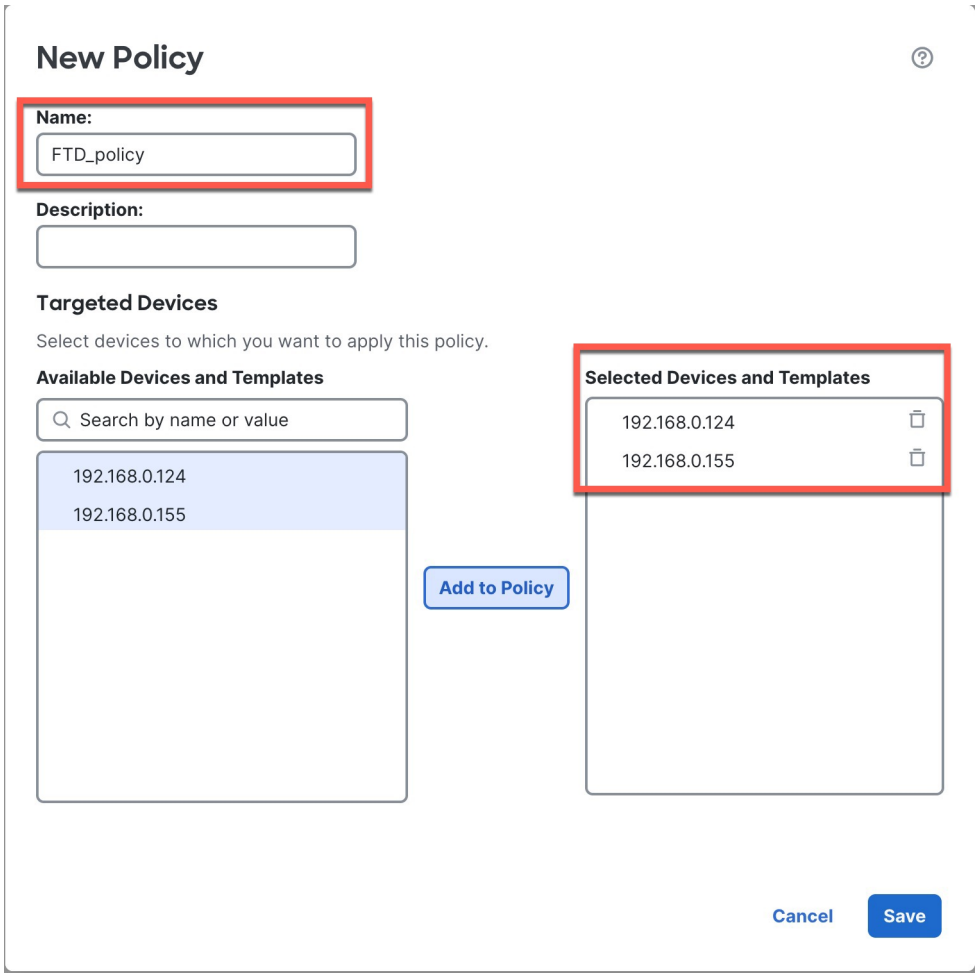
此步骤将为内部客户端创建一条 NAT 规则，以便将内部地址转换为外部接口 IP 地址上的端口。这类 NAT 规则称为接口端口地址转换 *(PAT)*。

过程

步骤 1 选择**设备 (Devices)** > **NAT**，然后点击**新建策略 (New Policy)**。

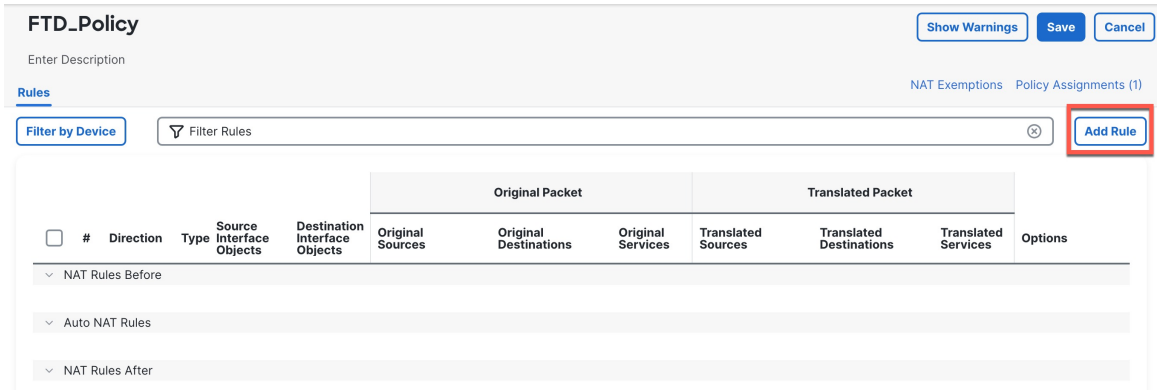
步骤 2 为策略命名，选择要使用策略的设备，然后点击**保存 (Save)**。

图 *8:* 新建策略



策略即已添加 管理中心。您仍然需要为策略添加规则。

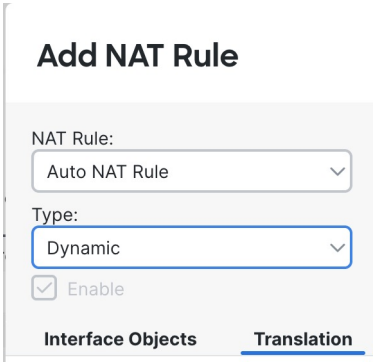
图 *9: NAT* 策略



步骤 3 点击添加规则 **(Add Rule)**。

步骤 4 配置基本规则选项：

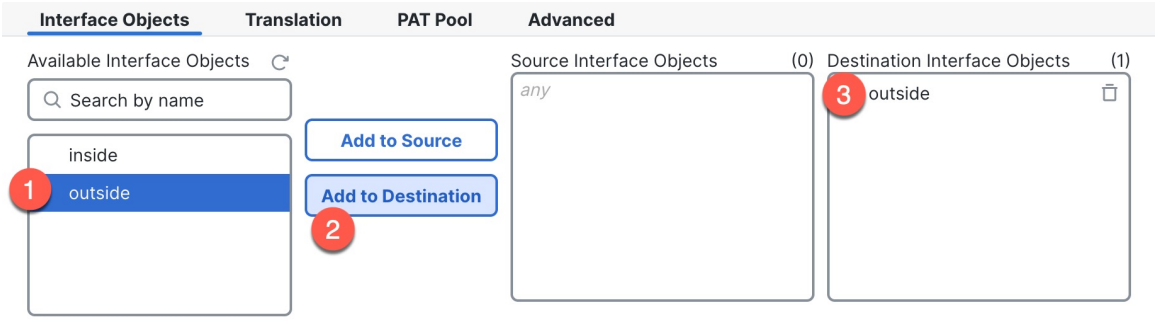
图 *10:* 基本规则选项



- **NAT 规则 (NAT Rule)** - 选择**自动 NAT 规则 (Auto NAT Rule)**。
- **类型 (Type)** - 选择**动态 (Dynamic)**。

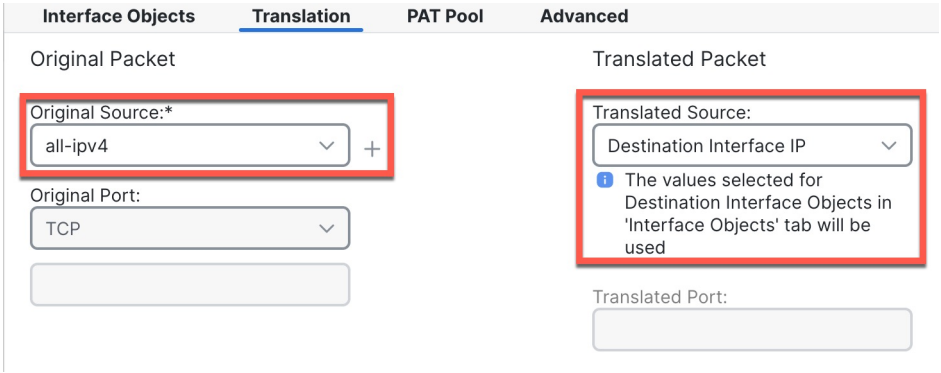
步骤 5 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。

图 *11:* 接口对象



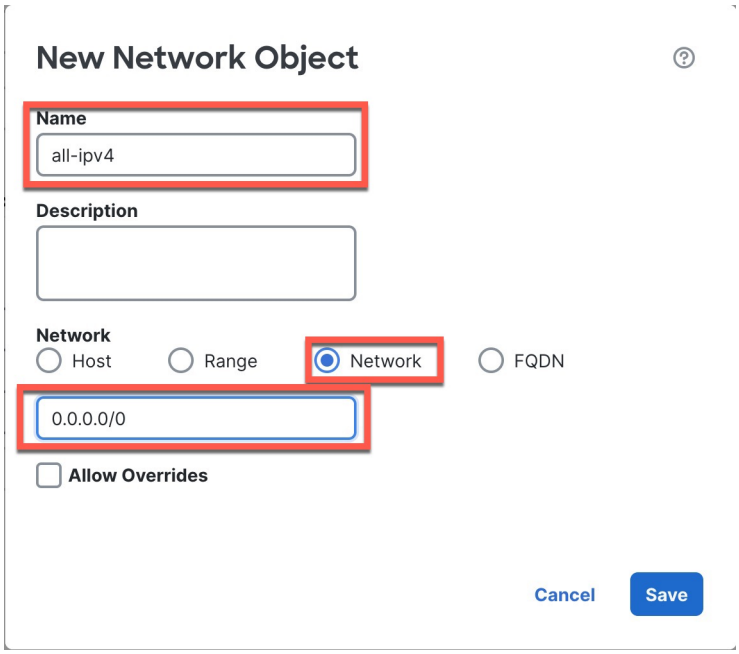
步骤 6 在**转换 (Translation)** 页面上配置以下选项：

图 *12:* 转换



- **原始源**-点击 **添加** (+) 为所有 IPv4 流量添加网络对象 (**0.0.0.0/0**)。

图 *13:* 新的网络对象



注释
您不能使用系统定义的 **any-ipv4** 对象，因为自动 NAT 规则在对象定义过程中添加 NAT，并且您无法编辑系统定义的对象。

- **转换的源 (Translated Source)** - 选择**目标接口 IP (Destination Interface IP)**。

步骤 7 点击**保存 (Save)** 以添加规则。

规则即已保存至 **Rules** 表。

步骤 8 点击 **NAT** 页面上的**保存 (Save)** 以保存更改。

配置访问控制规则

如果您在注册设备时创建了基本的**封锁所有流量**访问控制策略，则需要向策略添加规则以允许流量通过设备。访问控制策略可包括按顺序评估的多个规则。

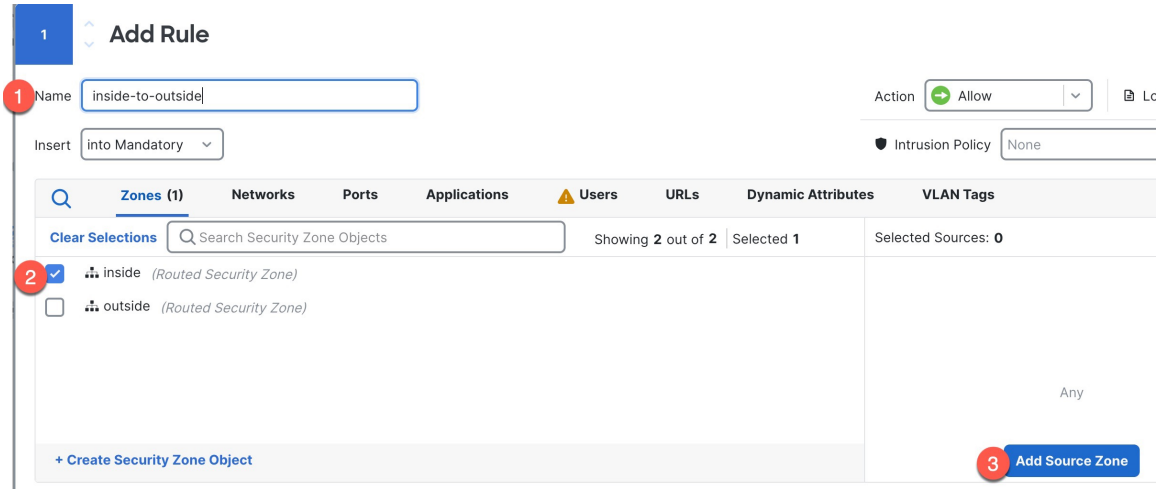
此过程将创建一个访问控制规则，以允许从内部区域到外部区域的所有流量。

过程

步骤 1 选择 **策略** > **访问控制标题** > **访问控制**，然后点击分配给设备的访问控制策略对应的 **编辑** ()。

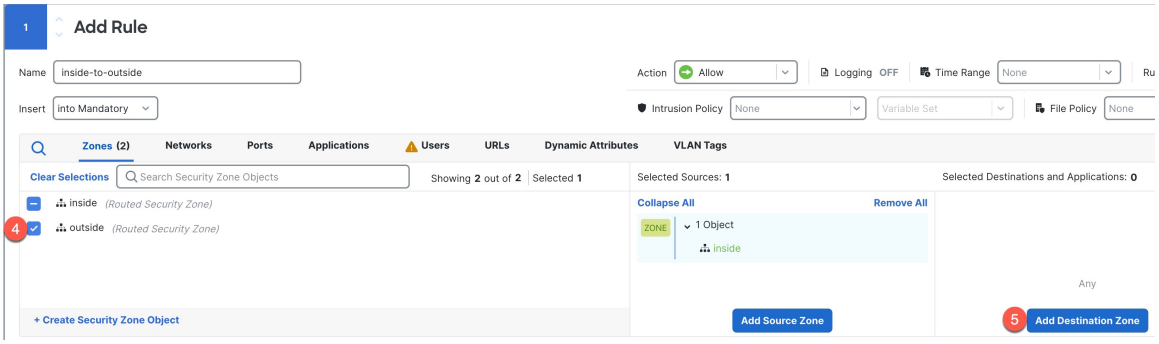
步骤 2 点击**添加规则 (Add Rule)** 并设置以下参数。

图 *14:* 源区域



1. 为此规则命名，例如 **inside-to-outside**。
2. 从**区域 (Zones)** 中选择内部区域
3. 点击**添加源区域 (Add Source Zone)**。

图 *15:* 目标区域



4. 从**区域 (Zones)** 中选择外部区域。
5. 点击**添加目标区域 (Add Destination Zone)**。

其他设置保留原样。

步骤 3 （可选） 点击数据包流程图中的策略类型，以便自定义相关策略。

预过滤器、解密、安全智能和身份策略在访问控制规则之前应用。不需要自定义这些策略，但在了解网络需求后，这些策略可通过快速路由受信任流量（绕过处理）或阻止流量以避免进一步处理，从而提高网络性能。

图 *16:* 在访问控制之前应用政策

- **预过滤器规则** - 默认预过滤器策略通过所有流量，以便其他规则执行操作（分析）。您可以对默认策略进行的唯一更改是**阻止**隧道流量。否则，您可以创建新的预过滤器策略，以便与可以分析（传递）、快速路径（绕过进一步检查）或阻止的访问控制策略关联。

  预过滤功能可在流量到达更远的地方之前，通过拦截或快速路径来处理流量，从而提高性能。在新策略中，您可以添加隧道规则和预过滤器规则。通过隧道规则，您可以对明文（非加密）直通隧道进行快速路由、阻止或重新分区。预过滤器规则可让您快速路由或阻止通过 IP 地址、端口和协议识别的非隧道流量。

  例如，如果知道要阻止网络上的所有 FTP 流量，但不阻止来自管理员的快速 SSH 流量，则可以添加一个新的预过滤器策略。

- **解密** - 默认情况下不应用解密。解密是让网络流量接受深度检查的一种方法。大多数情况下都不要对流量进行解密，只有在法律允许的情况下才能这样做。为了最大限度地保护网络，对于前往关键服务器或来自不信任网段的流量，解密策略可能是一个好主意。

- **安全智能** - （需要 IPS 许可证）默认启用安全智能。安全智能是在将连接传递到访问控制策略进行进一步处理之前应用的另一项针对恶意活动的早期防御措施。安全智能使用信誉情报快速阻止与思科威胁情报组织 Talos 提供的 IP 地址、URL 和域名之间的连接。您可以根据需要添加或删除其他 IP 地址、URL 或域。

  注释
  如果没有 IPS 许可证，即使访问控制策略中显示该策略已启用，也不会部署该策略。

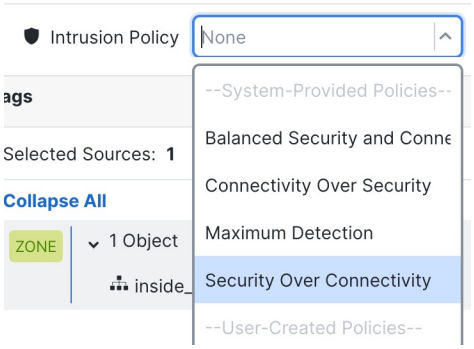
- **身份** - 默认情况下不应用身份。在允许访问控制策略处理流量之前，可以要求用户进行身份验证。

步骤 4 （可选） 添加在访问控制规则之后应用的入侵策略。

入侵策略是一组已定义的入侵检测和防御配置，用于检查流量是否违反安全规定。管理中心 包括许多系统提供的策略，您可以按原样启用或自定义这些策略。此步骤可启用系统提供的策略。

a) 点击**入侵策略 (Intrusion Policy)** 下拉列表。

图 *17:* 系统提供的入侵策略

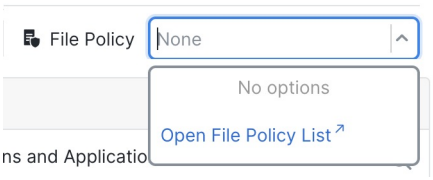


b) 从列表中选择一个系统提供的策略。

步骤 5 （可选） 添加在访问控制规则之后应用的文件策略。

a) 点击**文件策略 (File Policy)** 下拉列表，然后选择现有策略或通过选择**打开文件策略列表 (Open File Policy List)** 添加一个策略。

图 *18:* 文件策略



对于新策略，系统将在单独的选项卡中打开**策略 (Policies)** > **恶意软件和文件 (Malware & File)** 页面。

b) 有关创建策略的详细信息，请参阅《Cisco Secure Firewall 设备管理器配置指南》。

c) 返回**添加规则 (Add Rule)** 页面，从下拉列表中选择新创建的策略。

步骤 6 点击**应用 (Apply)**。

规则即已添加至 **Rules** 表。

步骤 7 点击**保存 (Save)**。

在外部接口上启用 SSH

本部分介绍如何启用与外部接口的 SSH 连接。

默认情况下，您可以使用在初始设置期间为其配置密码的 **admin** 用户。

过程

步骤 1 选择 **设备** > **平台设置**，并创建或编辑 威胁防御 策略。

步骤 2 选择 **SSH 访问 (SSH Access)**。

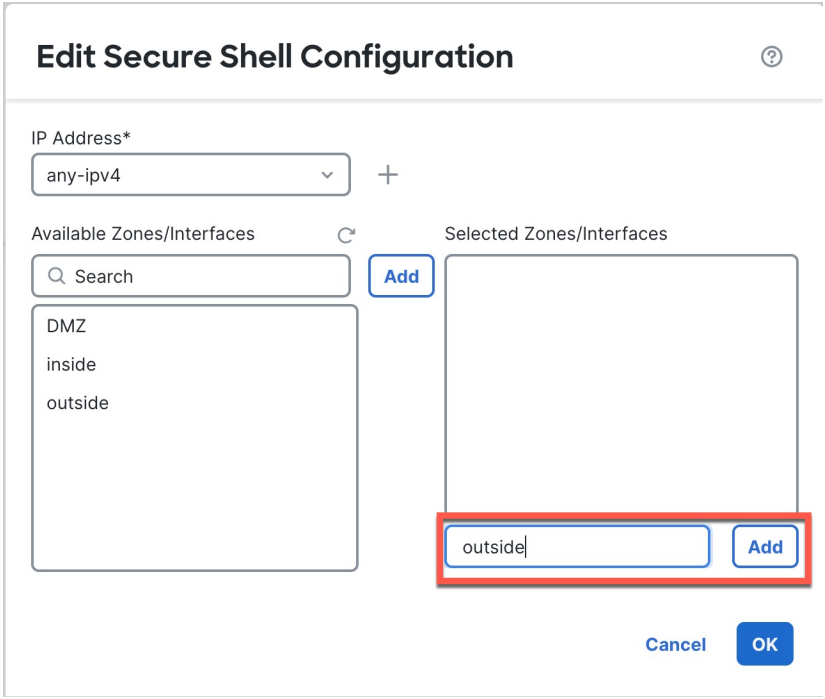
步骤 3 标识允许 SSH 连接的外部接口和 IP 地址。

a) 点击**添加 (Add)** 以添加新规则，或点击**编辑 (Edit)** 以编辑现有规则。

b) 配置规则属性：

- **IP 地址**-用于标识允许建立 HTTPS 连接的主机或网络的网络对象 或组 。从下拉列表中选择一个对象，或者点击 + 以添加新的网络对象。
- **可用区域/接口 (Available Zones/Interfaces)** - 添加外部区域或者在**所选区域/接口 (Selected Zones/Interfaces)** 列表下的字段中键入**外部**接口名称，然后点击**添加 (Add)**。

图 *19:* 在外部接口上启用 ***SSH***



c) 点击**确定 (OK)**。

步骤 4 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

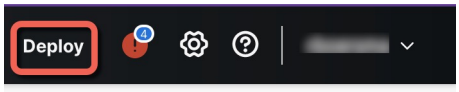
部署配置

将配置更改部署到设备；在部署之前，您的所有更改都不会在设备上生效。

过程

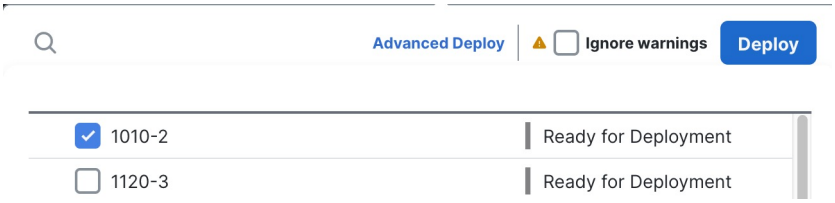
步骤 1 点击右上方的**部署 (Deploy)**。

图 *20:* 部署



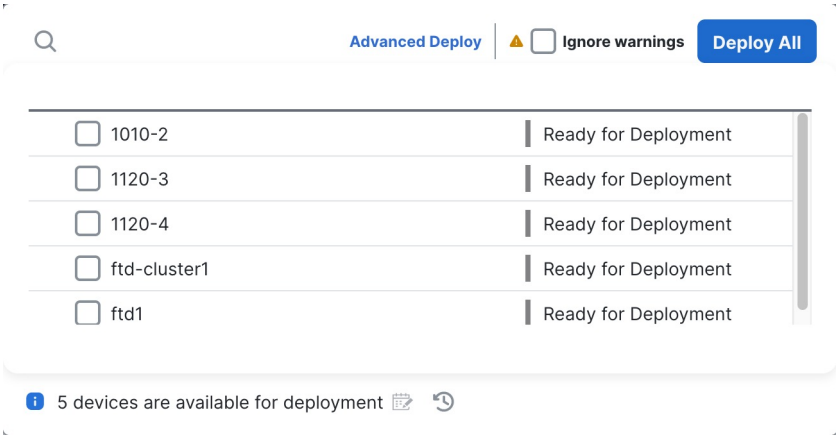
步骤 2 要快速部署，请选中特定设备，然后点击**部署 (Deploy)**。

图 *21:* 部署所选



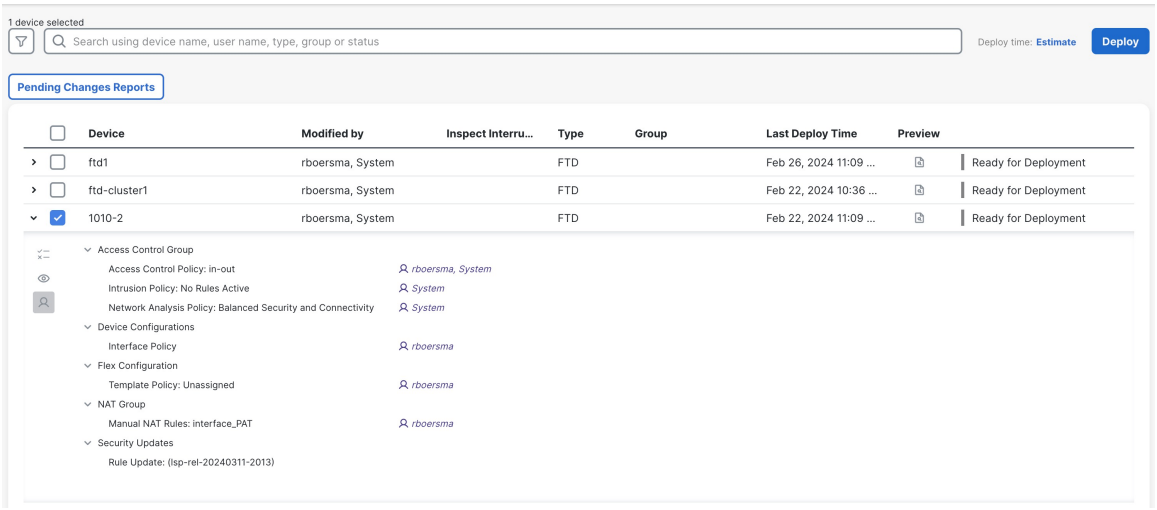
或者，点击**全部部署 (Deploy All)** 以部署到所有设备。

图 *22:* 全部部署



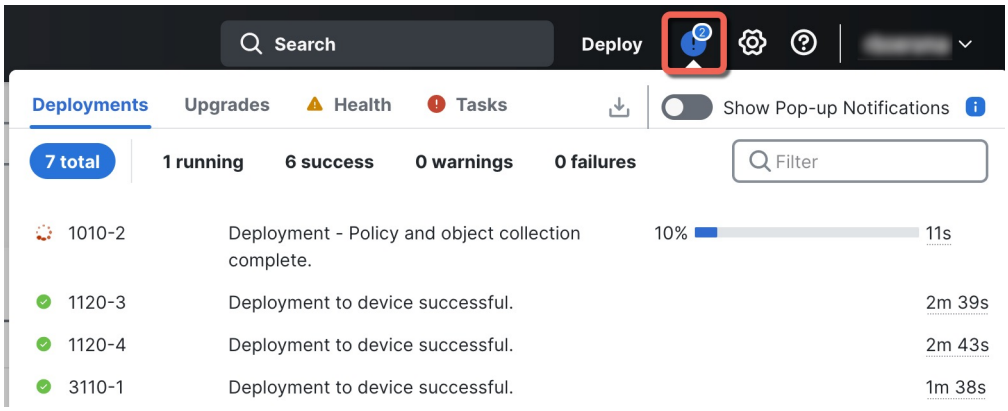
否则，对于其他部署选项，请点击**高级部署 (Advanced Deploy)**。

图 *23:* 高级部署



步骤 3 确保部署成功。点击菜单栏中**部署 (Deploy)** 按钮右侧的图标可以查看部署状态。

图 *24:* 部署状态


Search
Deploy
Deployments
Upgrades
Health
Tasks
Show Pop-up Notifications
7 total
1 running
6 success
0 warnings
0 failures
Filter
1010-2
Deployment - Policy and object collection complete.
10%
11s
1120-3
Deployment to device successful.
2m 39s
1120-4
Deployment to device successful.
2m 43s
3110-1
Deployment to device successful.
1m 38s

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。