常规防火墙接口

本章包括常规防火墙 接口配置，包括 EtherChannel、VLAN 子接口、IP 寻址等。

注释 有关 Firepower 4100/9300上的初始接口配置，请参阅配置接口。

常规防火墙接口的要求和前提条件

型号支持

威胁防御

用户角色

- 管理员
- 访问管理员
- 网络管理员

配置 Firepower 1010 交换机端口

可以将各 Firepower 1010 和 Cisco Secure Firewall 1210/1220 接口配置为作为常规防火墙接口或第 2 层硬件交换机端口运行。这部分包括用于启动交换机端口配置的任务，包括启用或禁用交换模式以及创建 VLAN 接口和将它们分配给 VLAN。本节还介绍如何在受支持接口上自定义以太网供电 (PoE)。

关于交换机端口

本节介绍 Firepower 1010 以及 Cisco Secure Firewall 1210/1220 的交换机端口。

了解交换机端口和接口

端口和接口

对于每个物理1010接口，可以将其操作设置为防火墙接口或交换机端口。请参阅以下有关物理接口和端口类型的信息，以及为其分配交换机端口的逻辑 VLAN 接口：

- 物理防火墙接口 - 在路由模式下，这些接口使用已配置的安全策略在第 3 层网络之间转发流量，以应用防火墙和 VPN 服务。 在透明模式下，这些接口是桥接组成员，用于在第 2 层同一网络上的接口之间转发流量，使用已配置的安全策略应用防火墙服务。在路由模式下，还可以将集成路由和桥接与某些接口一起用作桥接组成员，将其他接口用作第 3 层接口。默认情况下，以太网 1/1 接口配置为防火墙接口。 还可以将这些接口配置为仅限 IPS（内联集和被动接口）。
- 物理交换机端口 - 交换机端口使用硬件中的交换功能在第 2 层转发流量。同一 VLAN 上的交换机端口可使用硬件交换互相通信，且流量不受 防火墙威胁防御安全策略的限制。接入端口仅接受未标记流量，可以将其分配给单个 VLAN。中继端口接受未标记和已标记流量，且可以属于多个 VLAN。默认情况下，以太网 1/2 至 1/8 (1010 和 1210) 或以太网 1/2 至 1/10 (1220) 配置为 VLAN 1 上的接入交换机端口。不能将 管理接口配置为交换机端口。
- 逻辑 VLAN 接口 - 这些接口的运行方式与物理防火墙接口相同，但不同的是，无法创建子接口仅 IPS 接口（内联集和被动接口）或 EtherChannel 接口。如果交换机端口需要与另一个网络进行通信，则 防火墙威胁防御 设备将安全策略应用至 VLAN 接口，并路由至另一个逻辑 VLAN 接口或防火墙接口。甚至可以将集成路由和桥接与VLAN接口一起用作桥接组成员。同一VLAN上的交换机端口之间的流量不受安全策略 防火墙威胁防御的限制，但桥接组中 VLAN之间的流量会受到安全策略的限制，因此，可以选择将桥接组和交换机端口进行分层，以在某些分段之间实施安全策略。

以太网供电

PoE 适用于以下端口：

- Firepower 1010 - 使用 IEEE 802.3af (PoE) 和 802.3at (PoE+) 的以太网 1/7 和 1/8，每个端口最高 30 瓦，总功率最高 60 瓦。

- Cisco Secure Firewall 1210CP - 以太网 1/5、1/6、1/7 和 1/8，使用 IEEE 802.3af (PoE)、802.3at (PoE+)和 802.3bt（PoE++ 和 Hi-PoE），每个端口最高 90 瓦，合计最高 120 瓦。

注释 1010E、1210CE 和 1220CX 不支持 PoE。

PoE+ 或更高版本使用链路层发现协议 (LLDP) 来协商功率级别。仅在需要时提供功率。

如果关闭接口，则会禁用设备电源。

Auto-MDI/MDIX 功能

如果是所有交换机口，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。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。

交换机端口准则和限制

高可用性和集群

- 无集群支持。
- 使用高可用性时，不应使用交换机端口功能。由于交换机端口在硬件中运行，因此会继续在主用设备 和备用设备上传输流量。高可用性旨在防止流量通过备用设备，但此功能不会扩展至交换机端口。在正常 高可用性网络设置中，两台设备上的活动交换机端口将导致网络环路。建议将外部交换机用于任何交换功能。请注意，VLAN 接口可通过故障转移监控，而交换机端口无法通过故障转移监控。理论上，您可以将单个交换机端口置于 VLAN 上并成功使用 高可用性，但更简单的设置是改用物理防火墙接口。
- 仅可使用防火墙接口作为故障转移链路。

逻辑 VLAN 接口 (SVI)

- 您可以创建多达 60 个 VLAN 接口。
- 如果还在防火墙接口上使用 VLAN 子接口，则无法使用与逻辑 VLAN 接口相同的 VLAN ID。VLAN 1 保留用于交换机端口的逻辑 VLAN 接口。
- MAC 地址：
  - 路由防火墙模式 - 所有 VLAN 接口共享一个 MAC 地址。确保所有连接的交换机均可支持此方案。如果连接的交换机需要唯一 MAC 地址，可手动分配 MAC 地址。请参阅配置 MAC 地址，第 64 页。
  - 透明防火墙模式 - 每个 VLAN 接口都有唯一的 MAC 地址。如有需要，您可通过手动分配 MAC 地址覆盖生成的 MAC 地址。请参阅配置 MAC 地址，第 64 页。

网桥组

您不能将逻辑 VLAN 接口和物理防火墙接口混合在同一个网桥组中。

VLAN 接口和交换机端口不支持的功能

VLAN 接口和交换机端口不支持：

- 动态路由
- 组播路由
- 等价多路径路由 (ECMP)
- 内联集或被动接口
- EtherChannels-交换机端口不能成为 EtherChannel 的一部分。EtherChannel 中的端口也不支持 PoE。
- 故障转移和状态链路
- 安全组标记 (SGT)

其他准则和限制

- 您最多可以在 Firepower 1010 和 Cisco Secure Firewall 1210/1220上配置 60 个命名接口。
- 不能将 管理接口配置为交换机端口。

默认设置

- 以太网 1/1 是一个防火墙接口。
- 在 1010/1210 上，以太网 1/2 至以太网 1/8 是分配给 VLAN 1 的交换机端口。
- 在 1220 上，以太网 1/2 至以太网 1/10 交换机端口会被分配给 VLAN 1。
- 默认速度和复用 - 默认情况下，速度和复用设置为自动协商。

配置交换机端口和以太网供电

要配置交换机端口和 PoE，请完成以下任务。

启用或禁用交换机端口模式

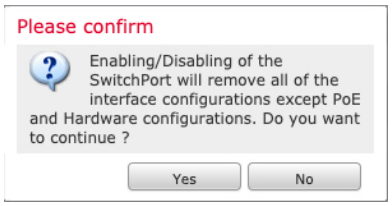
您可以将每个接口单独设置为防火墙接口或交换机端口。默认情况下，以太网 1/1 是防火墙接口，而剩余的以太网接口则配置为交换机端口。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 设备的 **编辑** ()。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击**交换机端口 (SwitchPort)** 列中的滑块，设置交换机端口模式，使其显示为 **滑块已启用** () 或 **滑块已禁用** ()。

默认情况下，交换机端口在 VLAN 1 中会被设为访问模式。您必须手动添加逻辑 VLAN 1 接口（或为这些交换机端口设置的任何 VLAN），以便路由流量并参与 安全策略（请参阅配置 VLAN 接口，第 5 页）。您无法将管理接口设置为交换机端口模式。更改交换机端口模式时，会删除所有不支持的配置：



此外，如果该接口已经启用，系统也会将其禁用。请确保重新启用该接口。

配置 VLAN 接口

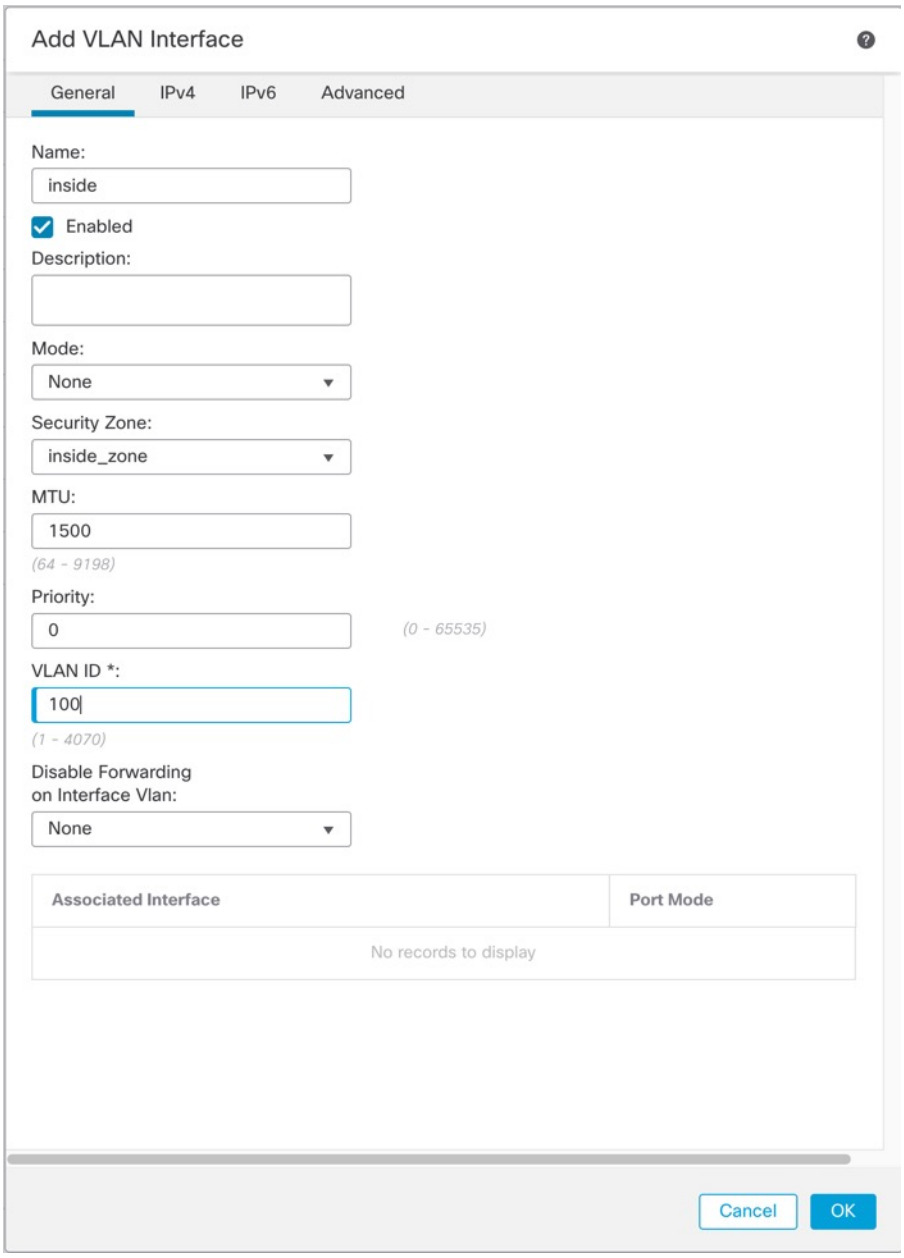
本节介绍如何配置 VLAN 接口以用于关联交换机端口。默认情况下，交换机端口分配给 VLAN1；但是，您必须手动添加逻辑 1 接口（或为这些交换机端口设置的任何 VLAN），以便路由流量并参与 安全策略。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 设备的 **编辑** ()。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击**添加接口 (Add Interfaces)** > **VLAN 接口 (VLAN Interface)**。

步骤 3 在 **常规**上，设置以下 VLAN 特定参数：



如果编辑的是现有 VLAN 接口，则 **关联接口** 表会显示此 VLAN 上的交换机端口。

a) 设置 **VLAN ID**，介于 1 和 4070 之间，不包括 3968 到 4047 范围内的ID（保留供内部使用）。

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。

b) （可选） 为 **接口 VLAN 上的禁用转发** 选择 VLAN ID，以禁用转发到另一个 VLAN。

例如，您有一个 VLAN 分配给外部以供互联网访问，另一个 VLAN 分配给内部企业网络，第三个 VLAN 分配给您的家庭网络。家庭网络无需访问企业网络，因此，您可以禁用家庭 VLAN 上的转发；企业网络可以访问家庭网络，但家庭网络不能访问企业网络。

步骤 4 要完成接口配置，请参阅以下过程之一：

- 配置路由模式接口，第 40 页
- 配置常规网桥组成员接口参数，第 45 页

步骤 5 点击**确定**。

步骤 6 点击**保存**。

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。

将交换机端口配置为接入端口

要将交换机端口分配给单个 VLAN，请将其配置为接入端口。接入端口仅接受未标记流量。启用交换机端口并分配给 VLAN1 的接口如下：

设备型号	交换机端口接口
Firepower 1010 和 Cisco Secure Firewall 1210	以太网 1/2 至以太网 1/8
Cisco Secure Firewall 1220	以太网 1/2 至以太网 1/10

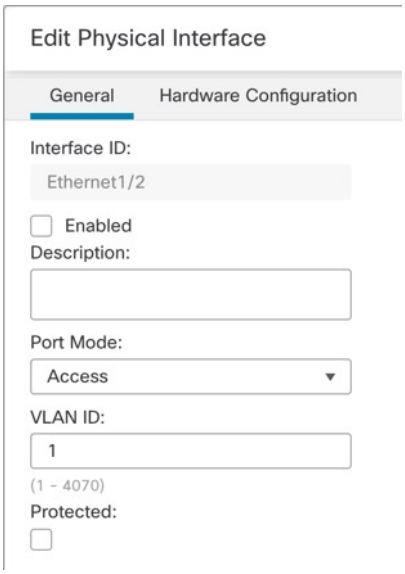
注释 设备不支持在网络中进行环路检测的生成树协议。因此，您必须确保与 的任何连接均不会在网络环路中结束。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 设备的 **编辑** ()。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** ()。

图 *1:* 编辑物理接口



步骤 3 选中**启用**复选框以启用此接口。

步骤 4 （可选） 在**说明**字段中添加说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 5 将**端口模式 (Port Mode)** 设为**访问 (Access)**。

步骤 6 在 **VLAN ID** 字段中，设置此交换机端口的 VLAN，范围介于 1 和 4070 之间。

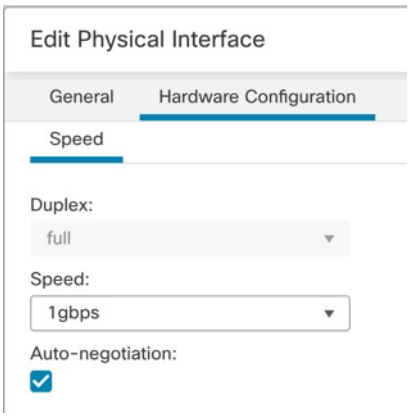
默认的 VLAN ID 为 1。

步骤 7 （可选） 选中**受保护 (Protected)** 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；如出现病毒感染或其他安全漏洞，则需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，当您在交换机端口上启用**受保护 (Protected)** 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。

步骤 8 （可选） 点击**硬件配置 (Hardware Configuration)**，设置双工和速度。

图 *2:* 硬件配置



选中**自动协商 (Auto-negotiation)** 复选框（默认）以自动检测速度和双工。如果取消选中，您可以手动设置速度和双工：

- **复用**—选择 **全** 或 **半**。
- **速度 (Speed)** - 选择 **10mbps**、**100mbps** 或 **1gbps**。

步骤 9 点击**确定**。

步骤 10 点击**保存**。

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。

将交换机端口配置为中继端口

此程序介绍如何创建可以使用 802.1 Q 标记传输多个 VLAN 的中继端口。中继端口接受未标记和标记流量。允许的 VLAN 上的流量通过中继端口保持不变。

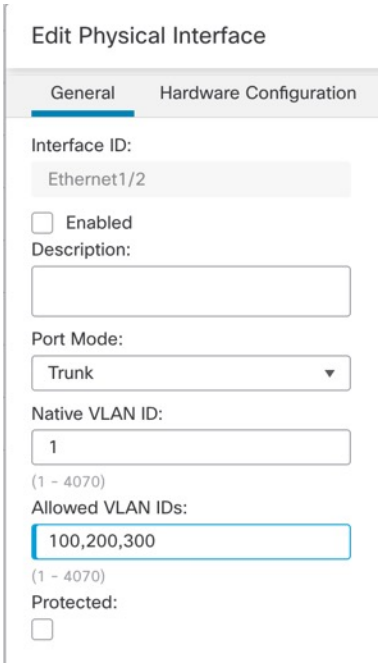
中继端口接收未标记流量后将其标记为本地 VLAN ID，以便 ASA 可以将流量转发至正确交换机端口，或可以将流量路由至另一个防火墙接口。如果 ASA 从中继端口发送本地 VLAN ID 流量，则会删除 VLAN 标记。请务必在另一台交换机上的中继端口上设置相同的本地 VLAN，以便将未标记流量标记至同一 VLAN。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

图 *3:* 设置中继端口模式



步骤 3 选中**启用**复选框以启用此接口。

步骤 4 （可选） 在**说明**字段中添加说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 5 将**端口模式 (Port Mode)** 设为**干线 (Trunk)**。

步骤 6 在**本地 VLAN ID (Native VLAN ID)** 字段中，设置此交换机端口的本地 VLAN，范围介于 1 和 4070 之间。

默认的本地 VLAN ID 为 1。

每个端口只能有一个本地 VLAN，但各端口的本地 VLAN 可以相同也可以不同。

步骤 7 在**允许的 VLAN ID (Allowed VLAN IDs)** 字段中，输入此中继端口的 VLAN，范围介于 1 和 4070 之间。

您可以通过以下方式之一识别最多 20 个ID：

- 单一编号 (n)
- 范围 (n-x)
- 用逗号将编号和范围隔开，例如：

  5,7-10,13,45-100

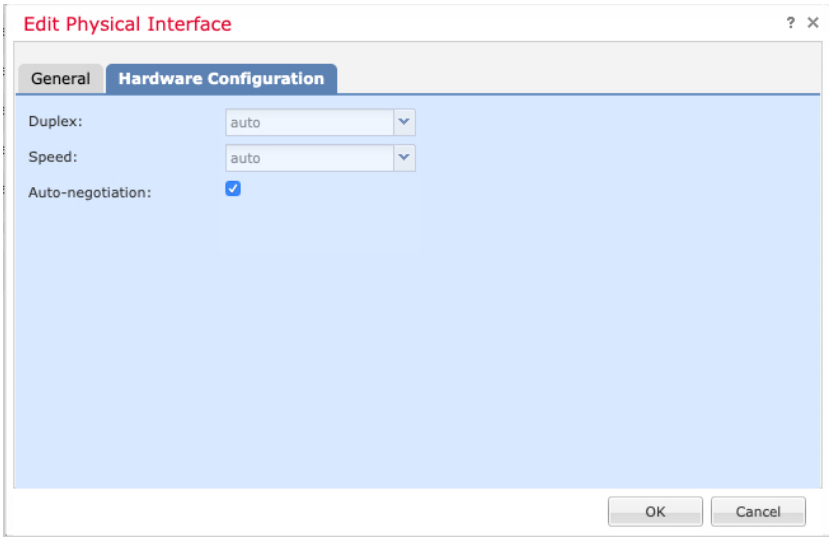
  您可以输入空格而不是逗号。

如果在此字段中包含本地 VLAN，则将忽略该本地 VLAN；从端口发送本地 VLAN 流量时，中继端口始终会删除 VLAN 标记。此外，不会接收仍具有 VLAN 标记的流量。

步骤 8 （可选） 选中**受保护 (Protected)** 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；如出现病毒感染或其他安全漏洞，则需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，当您在交换机端口上启用**受保护 (Protected)** 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。

步骤 9 （可选） 点击**硬件配置 (Hardware Configuration)**，设置双工和速度。



选中**自动协商 (Auto-negotiation)** 复选框（默认）以自动检测速度和双工。如果取消选中，您可以手动设置速度和双工：

- **复用**—选择 **全** 或 **半**。
- **速度 (Speed)** - 选择 **10mbps**、**100mbps** 或 **1gbps**。

步骤 10 点击**确定**。

步骤 11 点击**保存**。

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。

配置以太网供电

以太网供电 (PoE) 端口为 IP 电话或无线接入点等设备供电。默认情况下，PoE 处于启用状态。此过程介绍如何禁用和启用 PoE 以及如何设置可选参数。

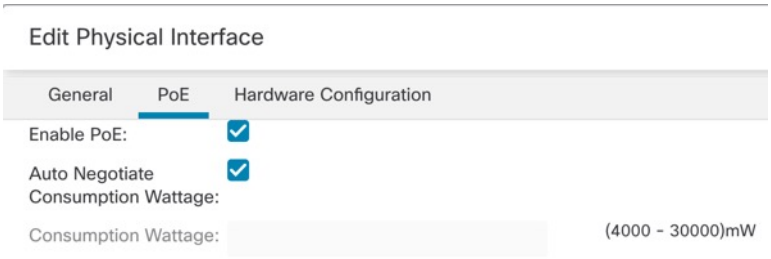
过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 为 Firepower 1010 上的以太网 1/7 或 1/8 或 Cisco Secure Firewall 1210CP 上的以太网 1/5-1/8 的任何接口点击 **编辑** (✎) 。

步骤 3 点击 **PoE**。

图 *4: PoE*



步骤 4 选中**启用 PoE (Enable PoE)** 复选框。

默认情况下，PoE 处于启用状态。

步骤 5 选择自动协商或手动电源。

- **自动协商功耗功率 (Auto Negotiate Consumption Wattage)** - PoE 使用适合受电设备类别的瓦数将电源自动传送至受电设备。防火墙使用 LLDP 进一步协商正确的瓦数。当连接某个类别的设备时，它会被调配到该等级的最大功率，以防需要使用更多电能。例如，如果您添加请求的功率为 12.95W 的 4 类设备，即使它当前没有使用该功率，系统也会为其分配 30W。某些设备可以重新协商电源需求。如果您知道设备需要的电量少于所分配的电量，则可以手动设置**功耗瓦数**，将电量释放给其他设备。
- **功耗瓦数 (Consumption Wattage)** - 取消选中**自动协商功耗功率 (Auto Negotiate Consumption Wattage)** 复选框以手动设置瓦数，从而以毫瓦为单位手动指定范围从 4000 至 30000 (1010) 或 90000 (1210CP) 的瓦数。如果要手动设置瓦数并禁用 LLDP 协商，请使用此选项。对于手动分配，该类别将在 **show power inline** 输出中显示为**不适用 (n/a)**，因为该类别不用于决定功耗。

  使用 **show power inline** 命令查看当前 PoE 状态。

步骤 6 点击**确定**。

步骤 7 点击**保存**。

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。

配置环回接口

本节介绍如何配置环回接口。

关于环回接口

环回接口是一种会模拟物理接口的纯软件接口。此接口可通过多个物理接口在IPv4和IPv6上访问。环回接口有助于克服路径故障；它可以从任何物理接口访问，因此，如果其中一个接口发生故障，您可以从另一个接口访问环回接口。

环回接口可用于：

- AAA
- BGP
- DNS
- HTTP
- ICMP
- IPsec 流量分流 - 仅限 Cisco Secure Firewall 1200、3100 和 4200
- NetFlow
- SNMP
- SSH
- 静态和动态 VTI 隧道
- 系统日志

威胁防御可以使用动态路由协议分发环回地址，也可以在对等设备上配置静态路由，以通过威胁防御的物理接口之一到达环回 IP 地址。不能在指定环回接口的 威胁防御 上配置静态路由。

相关主题

环回接口的准则和限制，第 13 页
配置环回接口，第 14 页

环回接口的准则和限制

防火墙模式

- 仅在路由模式中受支持。

高可用性和集群

- 无集群支持。

其他准则和限制

- 对于从物理接口到环回接口的流量，TCP 序列随机化始终处于禁用状态。

配置环回接口

要为设备添加环回接口：

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 设备的 **编辑** ()。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 从**添加接口 (Add Interfaces)** 下拉列表中，选择**环回接口 (Loopback Interface)**。

步骤 3 在**常规 (General)** 选项卡中，配置以下参数：

a) **名称 (Name)** - 输入环回接口的名称。

b) **启用 (Enabled)** - 选中此复选框可启用环回接口。

c) **环回 ID (Loopback ID)** - 输入介于 1 和 1024 之间的环回 ID。

d) **说明 (Description)** - 输入环回接口的说明。

步骤 4 配置已路由模式的接口参数。请参阅配置路由模式接口，第 40 页。

对流向环回接口的流量进行速率限制

开始之前

您应该对流向环回接口 IP 地址的流量进行速率限制，以防止系统负载过大。您可以向全局服务策略添加连接限制规则。

过程

步骤 1 创建用于标识流向环回接口 IP 地址的流量的扩展访问列表。

a) 选择**对象** > **对象管理** > **访问列表** > **扩展**。

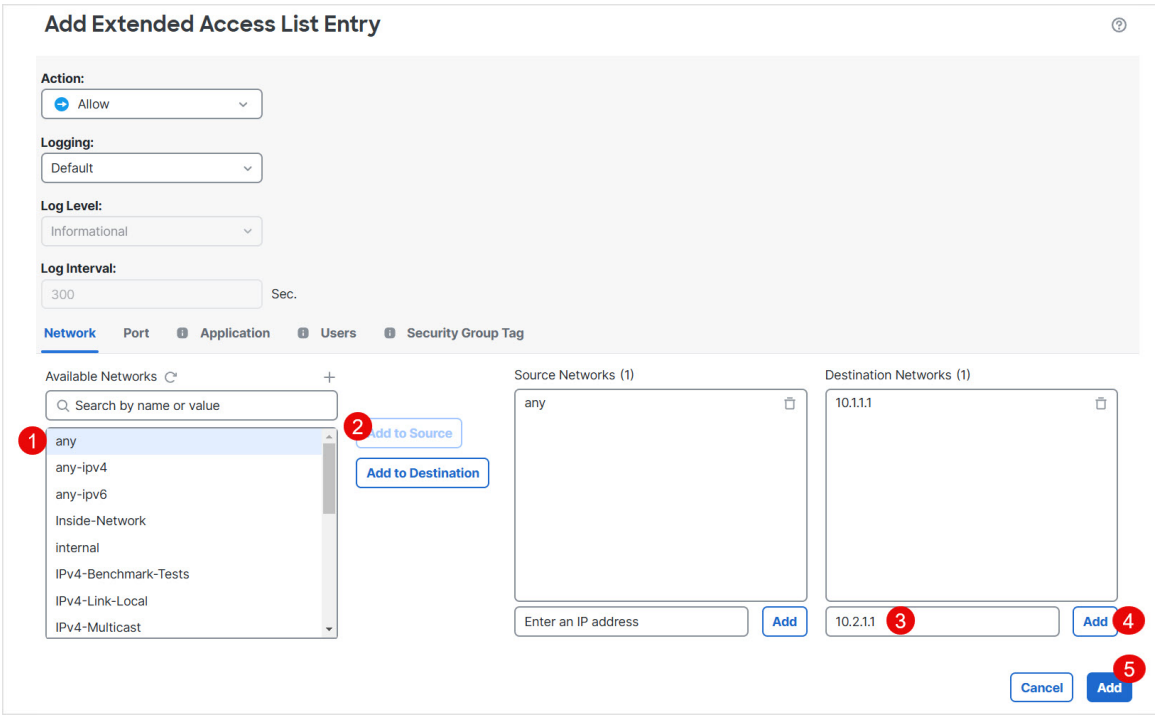
b) 点击 **添加扩展访问列表** 以创建新 ACL。

c) 在 **新建扩展访问列表对象** 对话框中，输入 ACL 的名称（不允许使用空格），然后点击 **添加** 以创建新条目。

图 *5:* 命名 ***ACL*** 并添加条目

d) 在 **网络** 选项卡上配置源地址（任意）和目的地址（环回 IP 地址）。

图 *6:* 源和目标网络

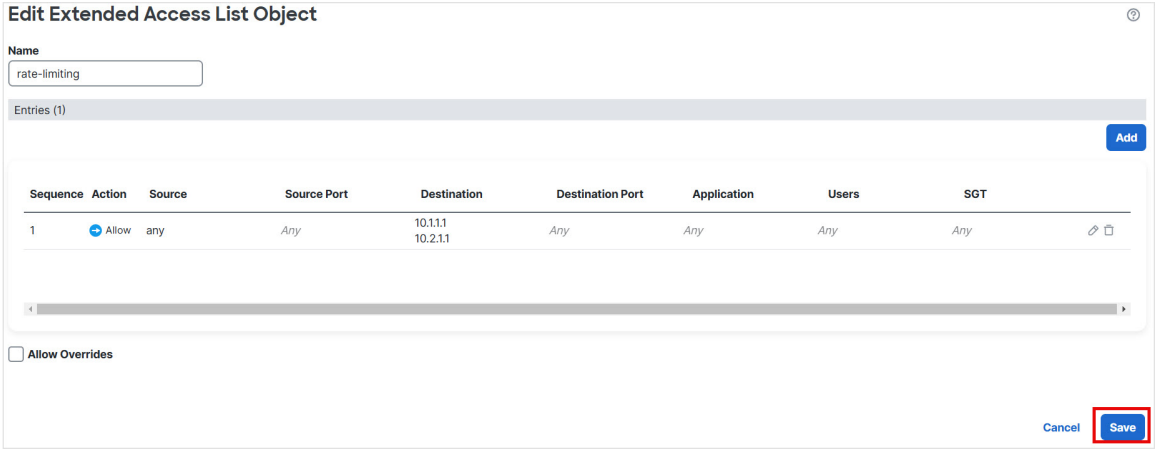


注释
保持默认 **操作** 为 **允许** （匹配），其他设置保持原样。

- 源-从 **可用网络** 列表中选择 **任何**，然后点击 **添加至源**。您还可以通过指定源 IP 地址而不是 **任何**来缩小此访问列表的范围。
- 目标-在 **目标网络** 列表下面的编辑框中输入地址并点击 **添加**。对每个环回接口重复上述操作。

e) 点击 **添加** 以将条目添加至 ACL。
f) 点击 **保存** 以保存 ACL。

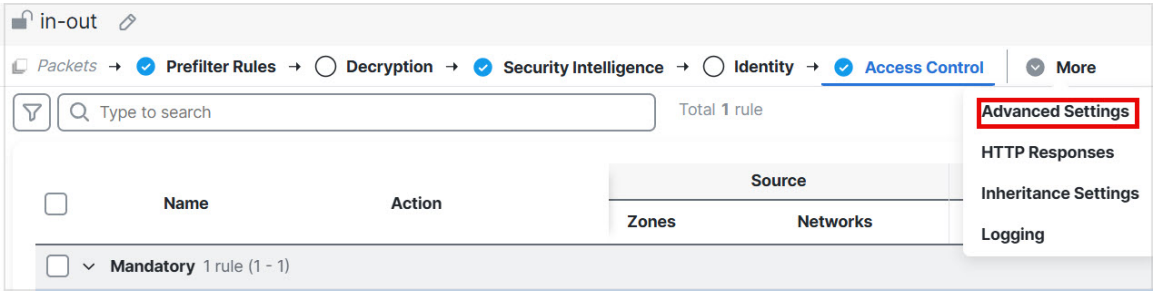
图 *7:* 保存 ***ACL***



步骤 2 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 3 从数据包流末尾的**更多 (More)** 下拉箭头中选择**高级设置 (Advanced Settings)**。

图 *8:* 高级设置

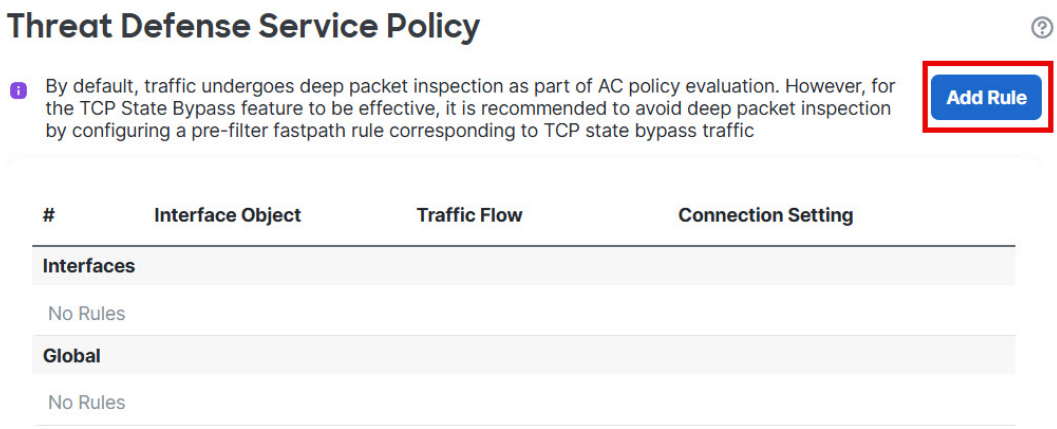


步骤 4 点击**威胁防御服务策略 (Threat Defense Service Policy)** 组中的 **编辑** ()。

图 *9:* 威胁防御服务策略

步骤 5 点击**添加规则**以创建新规则。

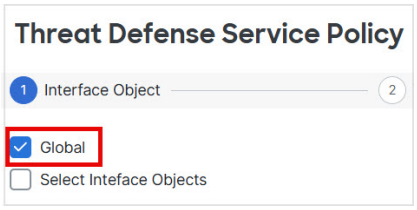
图 *10:* 添加规则



系统将打开服务策略规则向导，逐步指导您完成配置规则的流程。

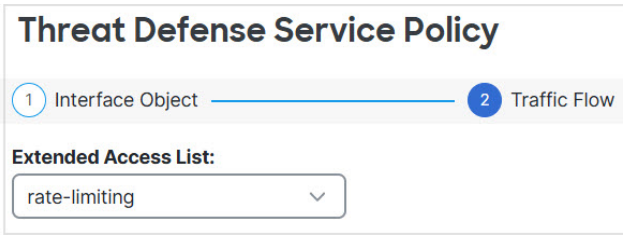
步骤 6 在 **接口对象** 步骤中，点击 **全局** 以创建适用于所有接口的全局规则，然后点击 **下一步**。

图 *11:* 全局策略



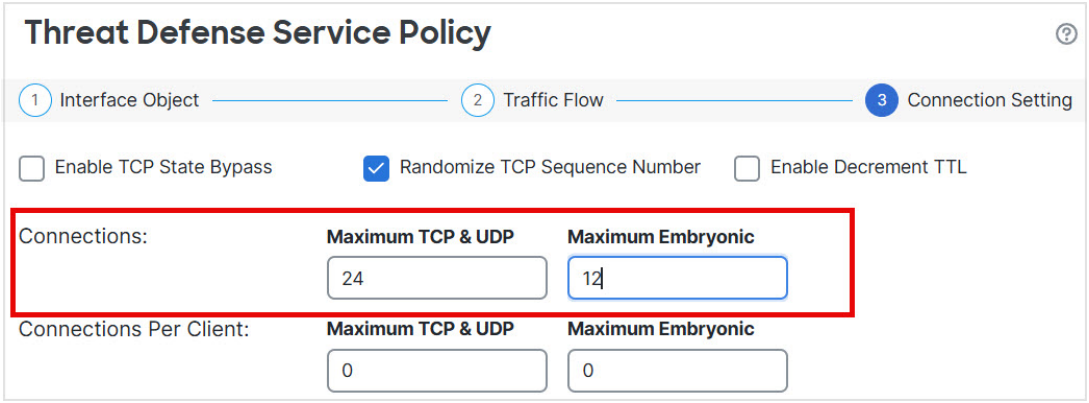
步骤 7 在 **流量** 步骤中，选择您在 步骤 1，第 14 页中创建的扩展访问列表对象，然后点击 **下一步**。

图 *12:* 选择扩展访问列表



步骤 8 在 **连接设置** 步骤中，设置 **连接** 限制。

图 *13:* 设置连接限制



将 **最大 TCP 和 UDP** 连接数设置为环回接口的预期连接数，将 **最大初期** 连接数设置为较低的数字。例如，您可以将其设置为 5/2、10/5 或 1024/512，具体取决于所需的预期环回接口会话。

设置初期连接限制触发 TCP 拦截，从而防止系统受到 DoS 攻击（这种攻击使用 TCP SYN 数据包对接口发起泛洪攻击）。

步骤 9 点击**完成**以保存所做的更改。

步骤 10 点击**确定**。

步骤 11 点击 **高级设置** 窗口中的 **保存** 。

步骤 12 现在您可以将更改部署到受影响的设备。

配置 VLAN 子接口和 802.1Q 中继

通过 VLAN 子接口，您可以将物理接口、冗余接口或 EtherChannel 接口划分为标记有不同 VLAN ID 的多个逻辑接口。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。

VLAN 子接口的准则和限制

型号支持

- Firepower 1010 和 Cisco Secure Firewall 1210/1220 - 交换机端口和 VLAN 接口不支持 VLAN 接口。
- Firepower 1010 和 Cisco Secure Firewall 1210/1220- 无法使用接口 ID 1 或 VLAN ID 1 创建子接口。VLAN 1 保留用于交换机端口的逻辑 VLAN 接口。

高可用性和群集

不能将子接口用于故障切换或状态链路，或用于集群控制链路。多实例模式例外：您可以为这些链路使用 机箱 定义的子接口。

其他准则

- 防止物理接口上的未标记数据包 - 如果使用子接口，则通常表明也不希望物理接口传递流量，因为物理接口会传递未标记的数据包。此属性对冗余接口对中的主用物理接口以及 EtherChannel 链路同样适用。由于必须启用物理接口、冗余接口或 EtherChannel 接口才能使子接口传递流量，请通过不为接口配置名称来确保物理接口、冗余接口或 EtherChannel 接口不传递流量。如果要使物理接口、冗余接口或 EtherChannel 接口传递未标记的数据包，可以照常配置名称。
- 不能在管理接口上配置子接口，无论是在 CLI 中配置的专用管理接口，还是用于管理器访问的数据接口。
- 同一父接口上的所有子接口必须为网桥组成员或路由接口；您无法混合搭配。
- 防火墙威胁防御不支持动态中继协议 (DTP)，因此您必须无条件地将连接的交换机端口配置到中继上。
- 您可能想要为 防火墙威胁防御 上定义的子接口分配唯一 MAC 地址，因为它们使用父接口上相同的固化 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 防火墙威胁防御 上特定实例内发生流量中断。

注释 如果手动分配 MAC 地址，请确保为同一物理接口上的所有子接口分配 MAC 地址，以避免意外行为和中断。

各设备型号的最大 VLAN 子接口数量

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

下表介绍各设备型号的限制。

型号	最大 VLAN 子接口数量
Firepower 1010	60
Firepower 1120	512
Firepower 1140 和 1150	1024
Cisco Secure Firewall 1200	1024
Cisco Secure Firewall 3100、4200	1024

型号	最大 VLAN 子接口数量
Firepower 4100	1024
Firepower 9300	1024
Firewall Threat Defense Virtual	50
ISA 3000	100

添加子接口

向物理接口、冗余接口或 port-channel 接口添加一个或多个子接口。

对于 Firepower 4100/9300，您可以在 FXOS 中配置子接口用于容器实例；请参阅为容器实例添加 VLAN 子接口。这些子接口显示在 防火墙管理中心 接口列表中。您还可以在 防火墙管理中心 中添加子接口，但仅可在未于 FXOS 中定义子接口的父接口上进行操作。

注释 父物理接口会传递未标记的数据包。您可能不想传递未标记的数据包，因此请确保未在安全策略中包括父接口。

过程

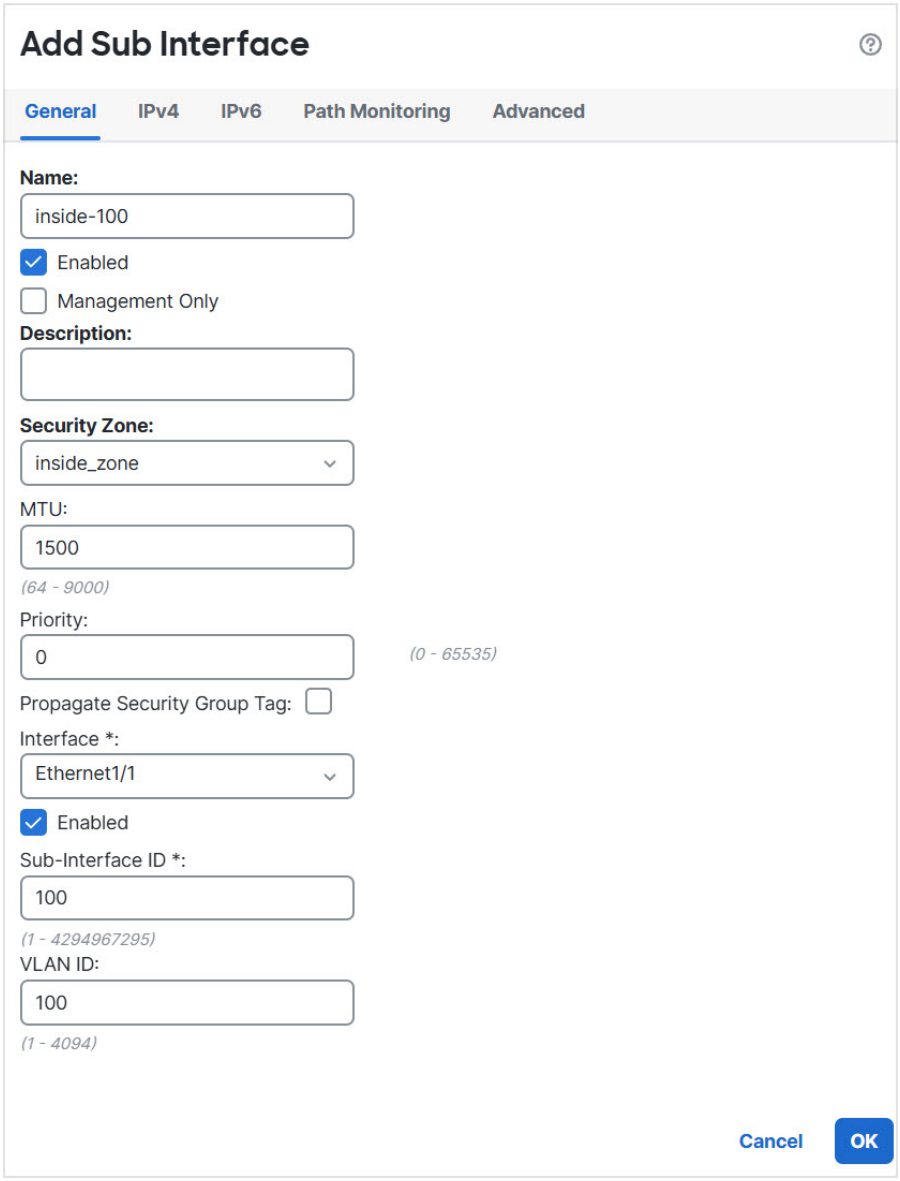
步骤 1 选择 **设备** > **设备管理** 并点击您的 设备的 **编辑** ()。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 根据启用物理接口并配置以太网参数启用父接口。

步骤 3 点击 **添加接口** > **子接口**。

步骤 4 在 **常规**上，设置以下参数：

图 *14:* 添加子接口



a) **接口** - 选择要将子接口添加到的物理、冗余或端口通道接口。

b) **子接口 ID** - 以整数形式输入介于 1 和 4294967295 之间的子接口 ID。允许的子接口数因平台而异。此 ID 一旦设置便不可更改。

c) **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。

此 VLAN ID 对父接口必须为唯一。

步骤 5 点击**确定**。

步骤 6 点击**保存**。

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。

步骤 7 配置路由或透明模式接口参数。请参阅配置路由模式接口，第 40 页或配置网桥组接口，第 44 页。

配置 VXLAN 接口

本章介绍如何配置虚拟可扩展局域网 (VXLAN) 接口。VXLAN 接口作为第 3 层物理网络之上的第 2 层虚拟网络，可对第 2 层网络进行扩展。

关于 VXLAN 接口

VXLAN 提供与 VLAN 相同的以太网第 2 层网络服务，但其可扩展性和灵活性更为出色。与 VLAN 相比，VXLAN 提供以下优势：

- 可在整个数据中心中灵活部署多租户网段。
- 更高的可扩展性可提供更多的第 2 层网段，最多可达 1600 万个 VXLAN 网段。

本节介绍 VXLAN 如何工作。有关 VXLAN 的详细信息，请参阅 RFC 7348。有关 Geneve 的详细信息，请参阅 RFC 8926。

封装

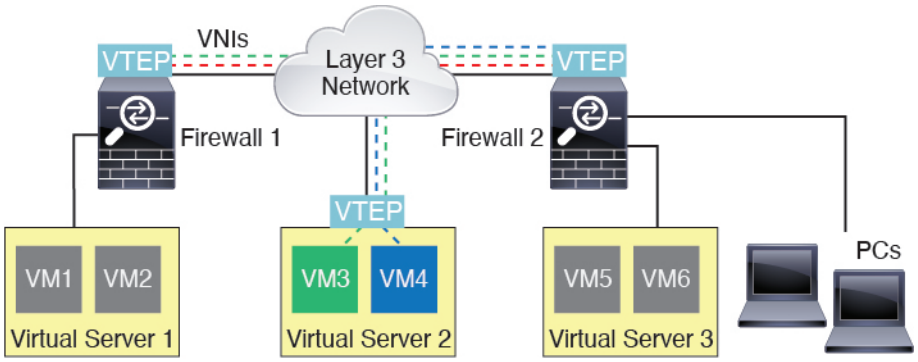
支持两种类型的 VXLAN 封装：

- VXLAN（所有型号）- VXLAN 使用 MAC Address-in-User 数据报协议 (MAC-in-UDP) 的封装方式。原始第 2 层帧已添加 VXLAN 报头，然后放入 UDP-IP 数据包中。
- Geneve（仅限 Firewall Threat Defense Virtual）- Geneve 具有不限于 MAC 地址的灵活内部报头。要在 Amazon Web 服务 (AWS) 网关负载均衡器和设备之间透明路由数据包，以及发送额外信息，则需要使用 Geneve 封装。

VXLAN 隧道端点

VXLAN 隧道终端 (VTEP) 设备执行 VXLAN 封装和解封。每个 VTEP 有两种接口类型：一个或多个虚拟接口称为 VXLAN 网络标识符 (VNI) 接口，您可以向其应用安全策略；以及称为 VTEP 源接口的常规接口，用于为 VTEP 之间的 VNI 接口建立隧道。VTEP 源接口连接到传输 IP 网络，进行 VTEP 至 VTEP 通信。

下图显示两个 和充当第 3 层网络中的 VTEP 的虚拟服务器 2，用于在站点之间扩展 VNI 1、2 和 3 网络。 充当 VXLAN 和非 VXLAN 网络之间的网桥或网关。



VTEP 之间的底层 IP 网络与 VXLAN 重叠无关。封装的数据包根据外部 IP 地址报头路由，该报头具有初始 VTEP（用作源 IP 地址）和终止 VTEP（作为目标 IP 地址）。对于 VXLAN 封装：当远程 VTEP 未知时，目标 IP 地址可以是组播组。在使用 Geneve 时， 仅支持静态对等体。默认情况下，VXLAN 的目标端口是 UDP 端口 4789（用户可配置）。Geneve 的目的端口是 6081。

VTEP 源接口

VTEP 源接口是一个计划要与所有 VNI 接口相关联的常规 接口（物理、EtherChannel 接口，甚至 VLAN 接口）。每个 Firewall Threat Defense Virtual 设备可以配置一个 VTEP 源接口。 由于只能配置一个 VTEP 源接口，因此不能在同一设备上同时配置 VXLAN 和 Geneve 接口。AWS 或 Azure 上的 Firewall Threat Defense Virtual 集群有一个例外，您可以在其中有两个 VTEP 源接口：一个 VXLAN 接口用于集群控制链路，一个 Geneve (AWS) 或 VXLAN (Azure) 接口可用于 AWS 网关负载均衡器。

尽管并未将 VTEP 源接口限制为全部用于传输 VXLAN 流量，但是可以实现该用途。如果需要，可以使用该接口传输常规流量，并将一个安全策略应用于传输此类流量的该接口。但是，对于 VXLAN 流量，必须对 VNI 接口应用所有安全策略。VTEP 接口仅作为物理端口。

在透明防火墙模式下，VTEP 源接口不是 BVI 的一部分，并且类似于对待管理接口的方式，不为该源接口配置 IP 地址。

VNI 接口

VNI 接口类似于 VLAN 接口：它们是虚拟接口，通过使用标记，实现网络流量在给定物理接口上的分离。将安全策略直接应用于每个 VNI 接口。

您智能添加一个 VTEP 接口，并且所有 VNI 接口都与同一 VTEP 接口相关联。AWS 或 Azure上的 Firewall Threat Defense Virtual 集群例外。对于 AWS 集群，您可以在其中有两个 VTEP 源接口：一个 VXLAN 接口用于集群控制链路，一个 Geneve 接口可用于 AWS 网关负载均衡器。对于 Azure 集群，您可以在其中有两个 VTEP 源接口：一个 VXLAN 接口用于集群控制链路，第二个 VXLAN 接口可用于 Azure 网关负载均衡器。

VXLAN 数据包处理

VXLAN

进出 VTEP 源接口的流量取决于 VXLAN 处理，特别是封装或解封。

封装处理包括以下任务：

- VTEP 源接口通过 VXLAN 报头封装内部 MAC 帧。
- UDP 校验和字段设置为零。
- 外部帧源 IP 设置为 VTEP 接口 IP。
- 外部帧目标 IP 通过远程 VTEP IP 查找确定。

解封； 仅在以下条件下解封 VXLAN 数据包：

- VXLAN 数据包是目标端口设置为 4789（用户可配置该值）的 UDP 数据包。
- 入口接口是 VTEP 源接口。
- 入口接口 IP 地址与目标 IP 地址相同。
- VXLAN 数据包格式符合标准。

日内瓦

进出 VTEP 源接口的流量取决于 Geneve 处理，特别是封装或解封。

封装处理包括以下任务：

- VTEP 源接口通过 Geneve 报头封装内部 MAC 帧。
- UDP 校验和字段设置为零。
- 外部帧源 IP 设置为 VTEP 接口 IP。
- 外部帧目标 IP 会被设置为您配置的对等体 IP 地址。

解封；ASA 仅在以下条件下解封 Geneve 数据包：

- VXLAN 数据包是目标端口设置为 6081（用户可配置该值）的 UDP 数据包。
- 入口接口是 VTEP 源接口。
- 入口接口 IP 地址与目标 IP 地址相同。
- Geneve 数据包格式符合标准。

对等体 VTEP

当 将数据包发送到对等体 VTEP 之后的设备时， 需要两条重要的信息：

- 远程设备的目标 MAC 地址
- 对等体 VTEP 的目标 IP 地址

会维护目标 MAC 地址到 VNI 接口的远程 VTEP IP 地址的映射。

VXLAN 对等体

有两种方法使 可以找到此信息：

- 可以在 上静态配置单个对等体 VTEP IP 地址。

  对于 IPv4: 然后， 设备将已封装 VXLAN 的 ARP 广播发送到 VTEP，以获取终端节点 MAC 地址。

  对于 IPv6： 然后向 IPv6 被请求节点的组播地址发送 IPv6 邻居请求消息。对等体 VTEP 以具有其链路本地地址的 IPv6 邻居通告消息作为响应。

- 可以在 上静态配置一组对等体 VTEP IP 地址。

  对于 IPv4: 然后， 设备将已封装 VXLAN 的 ARP 广播发送到 VTEP，以获取终端节点 MAC 地址。

  对于 IPv6： 然后向 IPv6 被请求节点的组播地址发送 IPv6 邻居请求消息。对等体 VTEP 以具有其链路本地地址的 IPv6 邻居通告消息作为响应。

- 可以在每个 VNI 接口（或者总的来说，在 VTEP 上）配置组播组。

  对于 IPv4： 将通过 VTEP 源接口在 IP 组播数据包内发送一个 VXLAN 封装的 ARP 广播数据包。对此 ARP 请求的响应使 可以获取远程终端节点的远程 VTEP IP 地址和目标 MAC 地址。

  对于 IPv6： 通过 VTEP 源接口发送组播侦听程序发现 (MLD) 报告消息，以指示 正在 VTEP 接口上侦听组播地址流量。

  Geneve 不支持此选项。

Geneve 对等体

Firewall Threat Defense Virtual 仅支持静态定义的对等设备。您可以在 AWS 网关负载均衡器上定义 Firewall Threat Defense Virtual 对等体 IP 地址。由于 Firewall Threat Defense Virtual 绝不会向网关负载均衡器发起流量，因此您也不必在 Firewall Threat Defense Virtual 上指定网关负载均衡器 IP 地址；它会在收到 Geneve 流量时获知对等体 IP 地址。Geneve 不支持组播组。

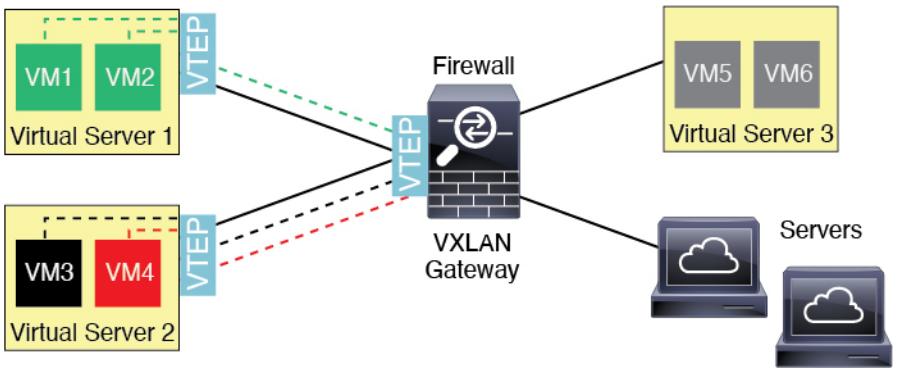
VXLAN 使用案例

本节介绍在 上实施 VXLAN 的使用案例。

VXLAN 网桥或网关概述

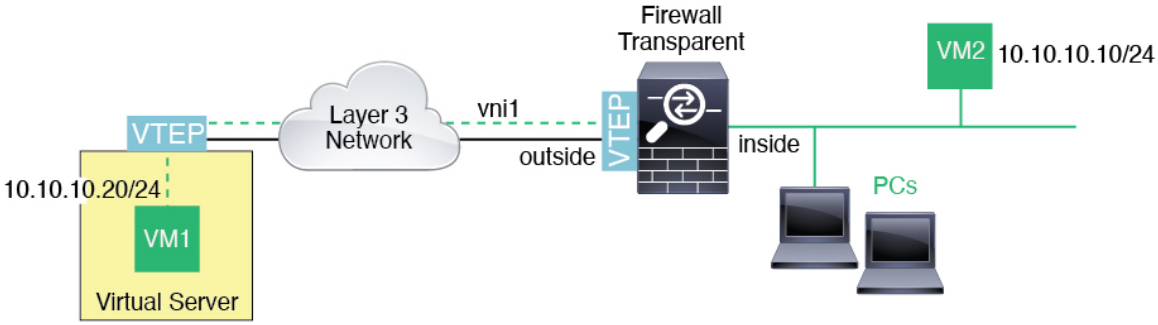
每个 威胁防御 VTEP 都可作为终端节点（例如 VM、服务器和 PC）和 VXLAN 重叠网络之间的网桥或网关。对于通过 VTEP 源接口借助 VXLAN 封装接收的传入帧，威胁防御 去掉 VXLAN 报头，并基于内部以太网帧的目标 MAC 地址，将传入帧转发到连接非 VXLAN 网络的物理接口。

威胁防御 始终会处理 VXLAN 数据包；而不仅仅是在两个其他 VTEP 之间转发未处理的 VXLAN 数据包。



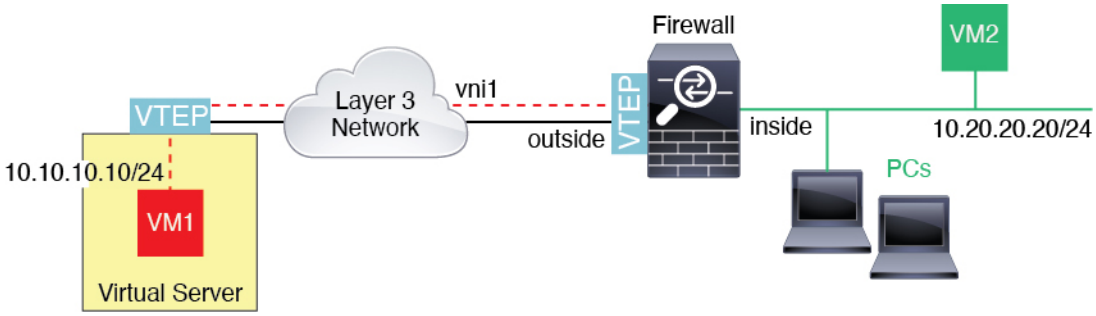
VXLAN 网桥

在使用网桥组（透明防火墙模式或可选的路由模式）时，威胁防御 可以用作 VXLAN 网段与本地网段之间的 VXLAN 网桥（远程），其中二者均位于同一网络中。在这种情况下，网桥组的一个成员是常规接口，而另一个成员是 VNI 接口。



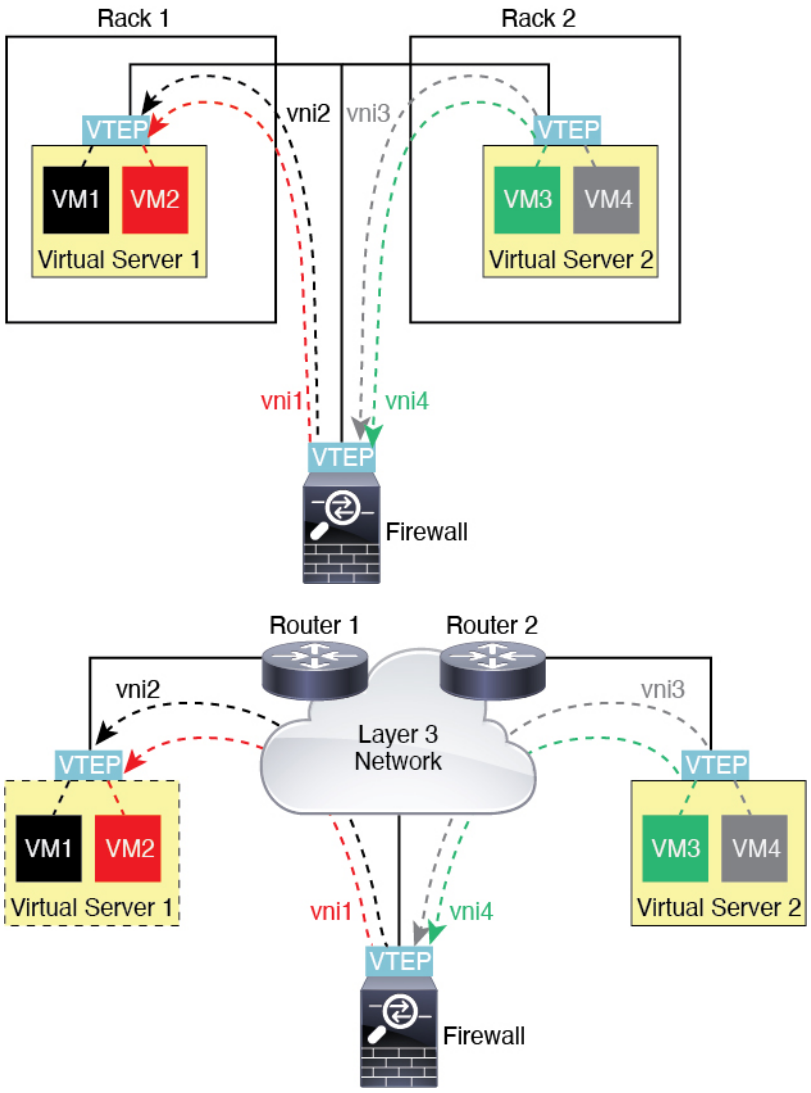
VXLAN 网关（路由模式）

威胁防御 可充当 VXLAN 和非 VXLAN 域之间的路由器，用于连接不同网络上的设备。



VXLAN 域之间的路由器

借助通过 VXLAN 扩展的第 2 层域，虚拟机可以指向一个 威胁防御 作为其网关，即使 威胁防御 位于不同机架中，甚至当 威胁防御 位于第 3 层网络上很远的位置也是如此。



请参阅有关此场景的以下注释：

1. 对于从 VM3 到 VM1 的数据包，目标 MAC 地址为 威胁防御 MAC 地址，因为 威胁防御 是默认网关。
2. 虚拟服务器 2 上的 VTEP 源接口接收来自 VM3 的数据包，然后使用 VNI 3 的 VXLAN 标记封装数据包，并将数据包发送到 威胁防御。
3. 当 威胁防御 接收数据包时，会解封数据包以获得内部帧。
4. 威胁防御 使用内部帧进行路由查找，然后发现目标位于 VNI 2 上。如果尚不具有 VM1 的映射，威胁防御 会在 VNI 2 上的组播组 IP 上发送封装的 ARP 广播。

注释 威胁防御 必须使用动态 VTEP 对等体发现，因为 ASA 在此场景下有多个 VTEP 对等体。

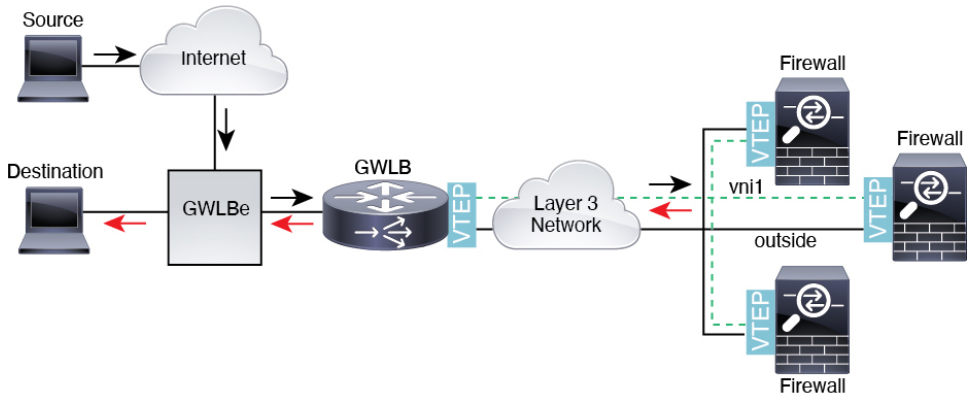
5. 威胁防御 再次使用 VXLAN 标记为 VNI 2 封装数据包，并且将数据包发送到虚拟服务器 1。在封装之前，威胁防御 将内部帧目标 MAC 地址更改为 VM1 的 MAC 地址（威胁防御 可能需要组播封装的 ARP，以获取 VM1 MAC 地址）。
6. 当虚拟服务器 1 接收 VXLAN 数据包时，该虚拟服务器会解封数据包并向 VM1 提供内部帧。

Geneve 单臂代理

注释 这是 Geneve 接口当前唯一支持的使用案例。

AWS 网关负载均衡器结合了透明网络网关和按需分配流量和扩展虚拟设备的负载均衡器。Firewall Threat Defense Virtual 支持具有分布式数据平面的网关负载均衡器集中控制平面（网关负载均衡器终端）。下图显示了从网关负载均衡器终端转发到网关负载均衡器的流量。网关负载均衡器会在多个流量之间进行均衡，这些流量在丢弃流量或将其发送回网关负载均衡器之前对其进行检查（掉头流量）。Firewall Threat Defense Virtual然后，网关负载均衡器会将流量发送回网关负载均衡器终端和目的地。

图 *15: Geneve* 单臂代理



AWS 网关负载均衡器和 Geneve 双臂代理

注释 这是 Geneve 接口唯一支持的使用案例。

Firewall Threat Defense Virtual 在单臂和双臂模式下，支持具有分布式数据平面的网关负载均衡器集中控制平面（网关负载均衡器终端）。下图显示直接转发到目标（互联网）的出站流量（由 Firewall Threat Defense Virtual检查的流量），无需流量跃点到 GWLB 和 GWLB 终端。Firewall Threat Defense Virtual 检查出站流量并执行 NAT，然后丢弃流量或通过 NAT 网关将流量发送回互联网。双臂代理为多 VPC 部署提供通用出口路径。防火墙检查来自多个 VPC 的出站流量，并从单点退出到互联网，使其成为具有成本效益的基础设施解决方案。

图 *16: Geneve* 双臂代理：来自单 *VPC* 的出口流量

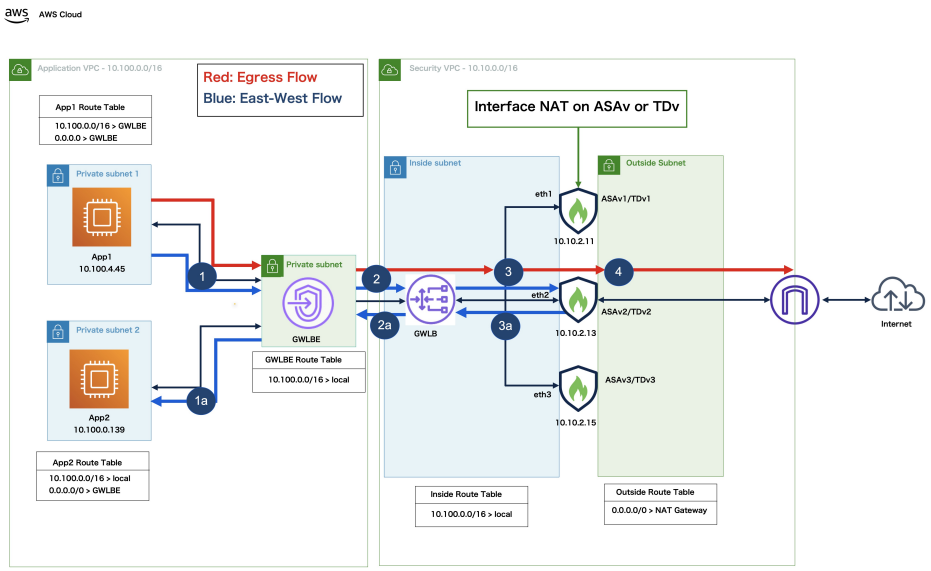
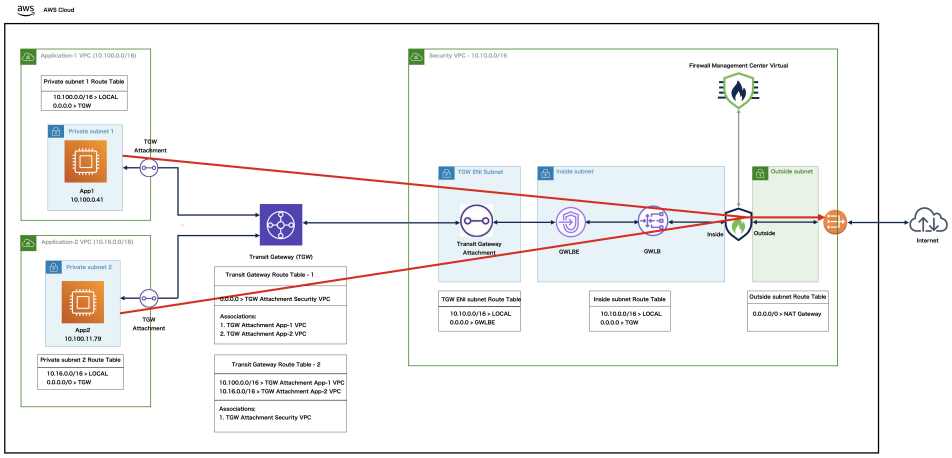


图 *17: Geneve* 双臂代理：来自多个 *VPC* 的出口流量

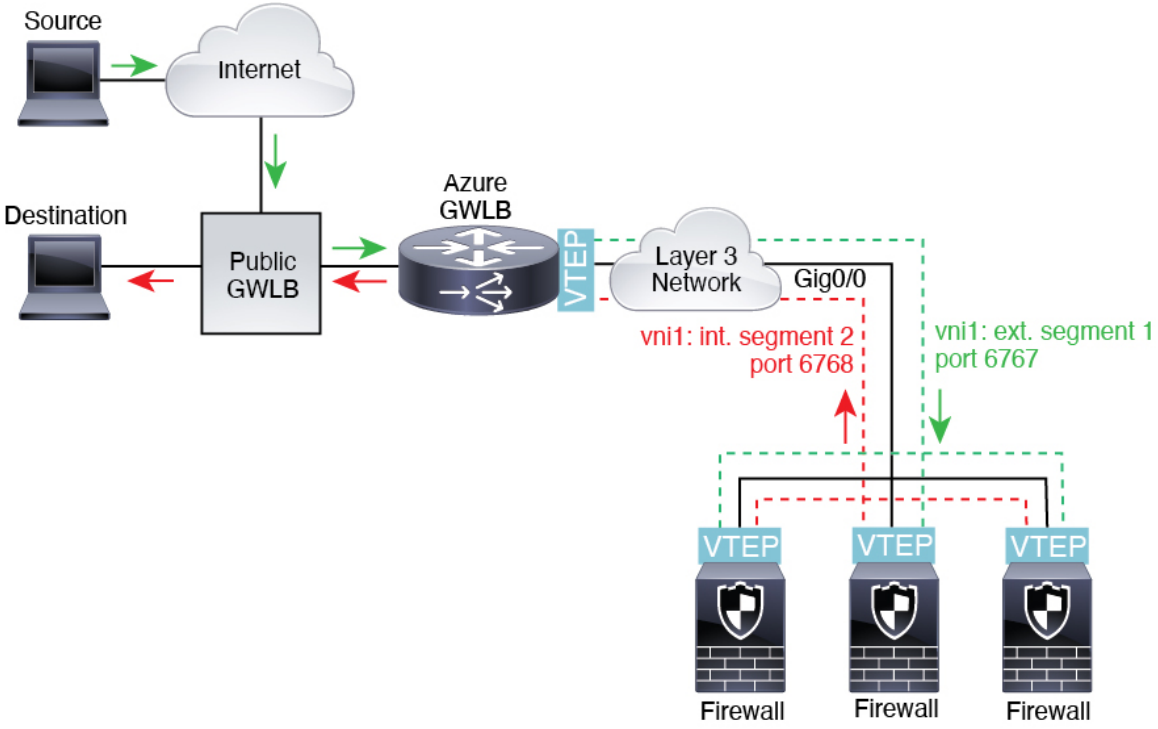


Azure 网关负载均衡器和配对代理

在 Azure 服务链中， Firewall Threat Defense Virtual充当可以拦截互联网和客户服务之间的数据包的透明网关。 Firewall Threat Defense Virtual 通过已配对代理中的 VXLAN 网段在单个 NIC 上定义外部接口和内部接口。

下图显示了从外部 VXLAN 网段上的公共网关负载均衡器转发到 Azure 门户负载均衡器的流量。网关负载均衡器会在多个 Firewall Threat Defense Virtual流量之间进行均衡 ， 这些流量在丢弃流量或将其发送回在内部 VXLAN 部分的网关负载均衡器之前对其进行检查。然后，Azure 网关负载均衡器会将流量发送回公共网关负载均衡器和目的地。

图 *18: Azure* 网关负载均衡器和配对代理



VXLAN 接口的要求和前提条件

型号要求

- 所有型号均支持 VXLAN 封装。
- 以下型号支持 Geneve 封装：
  - Amazon Web 服务 (AWS) 中的 Firewall Threat Defense Virtual
- 以下型号支持 配对代理模式 下的 VXLAN：
  - Firewall Threat Defense Virtual 在 Azure 中
- 不支持将 Firepower 1010 和 Cisco Secure Firewall 1210/1220 交换机端口和 VLAN 接口用作 VTEP 接口。

VXLAN 接口准则

防火墙模式

- Geneve 接口仅在路由防火墙模式下支持。

- 配对代理 VXLAN 接口仅在路由防火墙模式下支持。

IPv6

- VNI 接口支持 IPv4 和 IPv6 流量。
- 对于 VXLAN 封装，VTEP 源接口同时支持 IPv4 和 IPv6。 Firewall Threat Defense Virtual 集群控制链路 VTEP 源接口仅支持 IPv4。

  对于 Geneve，VTEP 源接口仅支持 IPv4。

集群

- 集群在单个接口模式下不支持 VXLAN，但集群控制链路除外（仅限Firewall Threat Defense Virtual）仅跨区以太网通道模式支持 VXLAN。

  例外情况是，AWS 可以使用额外的 Geneve 接口与 GWLB 配合使用，而 Azure 可以使用额外的配对代理 VXLAN 接口与 GWLB 配合使用。

路由

- VNI 接口上仅支持静态路由或策略型路由；动态路由协议不受支持。

VPN

不能为 VPN 配置 VTEP 源接口或将其用作 VTI。

MTU

- VXLAN 封装-如果源接口 MTU 少于 1554 个字节 (IPv4) 或 1574 个字节 (IPv6)，则 会自动将 MTU 提高到 1554 个字节 或 1574 字节。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的 MTU。如果其他设备使用的 MTU 更大，则您应 为 IPv4 将源接口 MTU 设置为网络 MTU＋54 个字节，或者为 IPv6 设置为 +64 个字节。对于 Firewall Threat Defense Virtual，此 MTU 需要您重新启动以启用巨帧保留。
- Geneve 封装 (Geneve encapsulation) - 如果源接口 MTU 少于 1806 个字节， 会自动将 MTU 提高到1806个字节。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的MTU。如果其他设备使用的MTU更大，您应将源接口MTU设置为网络MTU＋306个字节。此 MTU 需要您重新启动以启用巨帧保留。

配置 VXLAN 或 Geneve 接口

您可以配置 VXLAN 或 Geneve 接口。

配置 VXLAN 接口

要配置 VXLAN，请执行下列步骤：

注释 您可以配置 VXLAN 或 Geneve（仅限 Firewall Threat Defense Virtual）。有关 Geneve 接口，请参阅配置 Geneve 接口，第 34 页。

注释 对于 Azure GWLB，在使用 ARM 模板部署 VM 时会配置 VXLAN 接口。您可以在此部分中更改配置。

1. 配置 VTEP 源接口，第 32 页。
2. 配置 VNI 接口，第 33 页。
3. (Azure GWLB) 允许网关负载均衡器运行状况检查，第 36 页。

配置 VTEP 源接口

每个 设备可以配置一个 VTEP 源接口。VTEP 定义为网络虚拟化终端 (NVE)。VXLAN 是默认的封装类型。在 Azure 中，Firewall Threat Defense Virtual 上的集群是个例外，您可以使用一个 VTEP 源接口作为集群控制链路，将另一个 VTEP 源接口用于连接到 Azure GWLB 的数据接口。

过程

步骤 1 如果要指定一组对等 VTEP，请添加具有对等体 IP 地址的网络对象。请参阅创建网络对象。

步骤 2 选择**设备** > **设备管理**。

步骤 3 点击要配置 VXLAN 的设备旁边的 **编辑** (✎)。

步骤 4 （可选） 将源接口指定为仅限 NVE。

在路由模式下，此设置限制此接口上仅允许流向 VXLAN 的流量和常见的管理流量，这种情下此设置是可选的。对于透明防火墙模式，系统会自动启用此设置。

a) 点击**接口 (Interfaces)**。
b) 点击 VTEP 源接口的 **编辑** (✎)。
c) 在**常规 (General)** 页面上，选中**仅限 NVE (NVE Only)** 复选框。

步骤 5 如果尚未显示，点击 **VTEP**。

步骤 6 选中**启用 NVE (Enable NVE)**。

步骤 7 点击**添加 VTEP (Add VTEP)**。

步骤 8 对于**封装类型 (Encapsulation Type)**，请选择 **VxLAN**。

对于 AWS，您可以在 **VxLAN** 和 **Geneve** 之间进行选择。其他平台会自动选择 **VxLAN**。

步骤 9 在**封装端口 (Encapsulation port)** 中输入指定范围内的值。

默认值为 4789。

步骤 10 选择 **VTEP 源接口 (VTEP Source Interface)**。

从设备上的可用物理接口列表中进行选择。如果源接口 MTU 少于 1554 个字节 (IPv4) 或 1574 个字节 (IPv6)，则 防火墙管理中心 会自动将 MTU 提高到 1554 个字节或 1574 字节。

步骤 11 选择**邻居地址 (Neighbor Address)**。可用选项包括：

- **无 (None)** - 未指定邻居地址。
- **对等体 VTEP (Peer VTEP)** - 指定对等体 VTP 地址。
- **对等体组 (Peer Group)** - 指定具有对等体 IP 地址的网络对象。
- **默认组播 (Default Multicast)** - 指定所有相关 VNI 接口的默认组播组。如果每个 VNI 接口未配置组播组，则使用该组。如果配置一个 VNI 接口级别的组，则该组将覆盖此设置。

步骤 12 点击**确定**。

步骤 13 点击**保存**。

步骤 14 配置已路由的接口参数。请参阅配置路由模式接口。

配置 VNI 接口

添加 VNI 接口，将其与 VTEP 源接口相关联，并配置基本的接口参数。

对于 Azure 中的 Firewall Threat Defense Virtual，您可以配置常规 VXLAN 接口，也可以配置配对代理模式 VXLAN 接口，以便与 Azure GWLB 配合使用。配对代理模式是唯一支持的集群模式。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击要配置 VXLAN 的设备旁边的 **编辑** ()。

步骤 3 点击**接口 (Interfaces)**。

步骤 4 点击**添加接口 (Add Interfaces)**，然后选择 **VNI 接口 (VNI Interface)**。

步骤 5 输入接口**名称 (Name)** 和**说明 (Description)**。

步骤 6 从**安全区域 (Security Zone)** 下拉列表中选择一个安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

步骤 7 在指定范围内为**优先级 (Priority)** 字段输入值。默认情况下会选择 0。

步骤 8 输入值介于 1 和 10000 之间的 **VNI ID**。

此 ID 仅为内部接口标识符。

步骤 9 （Azure GWLB 的已配对代理 VXLAN）启用代理配对模式并设置所需的参数。

a) 选中**已配对代理 (Proxy Paired)**。

b) 将**内部端口 (Internal Port)** 设置为 1024 和 65535 之间的值。

c) 将**内部网段 ID (Internal Segment ID)** 设置为 1 和 16777215 之间的值。

d) 将**外部端口 (External Port)** 设置为 1024 和 65535 之间的值。
e) 将**外部网段 ID (External Segment ID)** 设置为 1 和 16777215 之间的值。

步骤 10 （常规 VXLAN）为 **VNI 网段 ID (VNI Segment ID)** 设置为 1 和 16777215 之间值。

网段 ID 用于 VXLAN 标记。

步骤 11 输入**多播组 IP 地址 (Multicast Group IP Address)**。

如果没有为 VNI 接口设置组播组，请使用源自 VTEP 源接口配置的默认组（如果有）。如果手动设置 VTEP 源接口的 VTEP 对等体 IP，则无法为 VNI 接口指定组播组。

步骤 12 选中 **NVE 已映射到 VTEP 接口 (NVE Mapped to VTEP Interface)**。

此选项会将该接口与 VTEP 源接口相关联。

步骤 13 点击**确定**。
步骤 14 点击**保存**以保存接口配置。
步骤 15 配置路由或透明接口参数。请参阅配置路由和透明模式接口，第 37 页。

配置 Geneve 接口

要为 Firewall Threat Defense Virtual 配置 Geneve 接口，请执行以下步骤：

注释 您可以配置 VXLAN 或 Geneve。有关 VXLAN 接口的信息，请参阅配置 VXLAN 接口，第 31 页。

1. 配置 VTEP 源接口，第 34 页。
2. 配置 VNI，第 35 页。
3. 允许网关负载均衡器运行状况检查，第 36 页。

配置 VTEP 源接口

每个 Firewall Threat Defense Virtual 设备可以配置一个 VTEP 源接口。VTEP 定义为网络虚拟化终端 (NVE)。

过程

步骤 1 选择**设备** > **设备管理**。
步骤 2 点击要配置 Geneve 的设备旁边的 **编辑** (✎) 。
步骤 3 点击 **VTEP**。
步骤 4 选中**启用 NVE (Enable NVE)**。
步骤 5 点击**添加 VTEP (Add VTEP)**。

步骤 6 对于**封装类型 (Encapsulation Type)**，请选择 **Geneve**。

步骤 7 在**封装端口 (Encapsulation port)** 中输入指定范围内的值。

我们不建议更改 Geneve 端口；AWS 需要使用端口 6081。

步骤 8 选择 **VTEP 源接口 (VTEP Source Interface)**。

您可以从设备上的可用物理接口列表中进行选择。如果源接口 MTU 少于 1806 个字节，防火墙管理中心 会自动将 MTU 提高到 1806 个字节。

步骤 9 点击**确定**。

步骤 10 点击**保存**。

步骤 11 配置已路由的接口参数。请参阅配置路由模式接口。

配置 VNI

添加 VNI，将其与 (VTEP) 源接口相关联，并配置基本的接口参数。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击要配置 Geneve 的设备旁边的 **编辑** (✎) 。

步骤 3 点击**接口 (Interfaces)**。

步骤 4 点击**添加接口 (Add Interfaces)**，然后选择 **VNI 接口 (VNI Interface)**。

步骤 5 在**名称 (Name)** 和**说明 (Description)** 字段中提供相关信息。

步骤 6 在 **VNI ID** 字段中，输入介于 1 和 10000 之间的值。

注释
此 ID 仅为内部接口标识符。

步骤 7 选中**启用代理 (Enable Proxy)** 复选框。

注释
当设备的 VNI 接口启用 AWS 代理时，不允许配置 NAT。

该选项可启用单臂代理模式或双臂代理模式。单臂代理模式允许流量从进入的同一接口流出（U-turn 流量），而双臂代理模式则使虚拟设备能够对检查到的流量执行 NAT，然后直接将出站流量转发到互联网，而不返回到 GWLB 和 GWLB 端点。如果以后编辑接口，则无法禁用单臂代理模式或双臂代理模式。为此，您需要删除现有接口并创建一个新的 VNI。

此选项仅适用于 Geneve VTEP。

步骤 8 从**代理类型 (Proxy type)** 下拉列表中，选择要为接口启用的代理模式。如果没有为接口指定代理模式，则默认情况下会考虑单臂代理模式。

步骤 9 选择 **NVE 已映射到 VTEP 接口 (NVE Mapped to VTEP Interface)**。

此选项会将该接口与 VTEP 源接口相关联。

步骤 10 点击**确定**。

步骤 11 点击**保存**。

下一步做什么

配置已路由的接口参数。请参阅配置路由模式接口。

允许网关负载均衡器运行状况检查

AWS 或 Azure GWLB 要求设备对运行状况检查进行正确应答。GWLB 只会将流量发送到被视为正常的设备。您必须将 Firewall Threat Defense Virtual 配置为响应 SSH、HTTP 或 HTTPS 运行状况检查。

配置以下方法之一。

过程

步骤 1 配置 SSH。请参阅配置安全外壳

允许来自 GWLB IP 地址的 SSH。GWLB 将尝试与 Firewall Threat Defense Virtual 建立连接，而 Firewall Threat Defense Virtual 的登录提示将被视为运行状况的证明。SSH 登录尝试会在 1 分钟后超时。为了适应此超时，您需要在 GWLB 上配置更长的运行状况检查间隔。

步骤 2 使用支持端口转换的静态接口 NAT 来配置 HTTP(S) 重定向。

您可以将 Firewall Threat Defense Virtual 配置为将运行状况检查重定向到元数据 HTTP(S) 服务器。对于 HTTP(S) 运行状况检查，HTTP(S) 服务器必须使用 200 到 399 范围内的状态代码来回复 GWLB。由于 Firewall Threat Defense Virtual 对同时管理连接的数量存在限制，因此您可以选择将运行状况检查分流到外部服务器。

支持端口转换的静态接口 NAT 允许您将某个端口（例如端口 80）的连接重定向到其他 IP 地址。例如，将来自 GWLB 的 HTTP 数据包转换为 Firewall Threat Defense Virtual 外部接口的目标，使其看起来像是来自目标为 HTTP 服务器的 Firewall Threat Defense Virtual 外部接口。Firewall Threat Defense Virtual 随后会将数据包转发到映射的目标地址。HTTP 服务器会响应 Firewall Threat Defense Virtual 外部接口，然后 Firewall Threat Defense Virtual 会将响应转发回 GWLB。您需要允许从 GWLB 到 HTTP 服务器的流量的访问规则。

a) 在访问规则中允许来自 GWLB 网络的外部接口上的 HTTP(S) 流量。请参阅访问控制规则。

b) 对于 HTTP(S)，请将源 GWLB IP 地址转换为 Firewall Threat Defense Virtual 外部接口 IP 地址；然后将外部接口 IP 地址的目的地转换为 HTTP(S) 服务器 IP 地址。请参阅配置静态手动 NAT。

配置路由和透明模式接口

本部分介绍在路由或透明防火墙模式下为所有型号完成常规接口配置的相关任务。

关于路由和透明模式接口

防火墙模式接口需要对流量执行防火墙功能，例如维持流量、跟踪 IP 和 TCP 层的流量状态、IP 分片重组和 TCP 规范化。另外，您还可以根据安全策略，选择为此流量配置 IPS 功能。

可以配置的防火墙接口类型取决于为设备设置的防火墙模式：路由或透明模式。有关详细信息，请参阅透明或路由防火墙模式。

- 路由模式接口（仅路由防火墙模式）- 要在其间路由的每个接口都在不同的子网中。
- 网桥组接口（路由和透明防火墙模式）- 您可以将网络上的多个接口组合在一起，Firepower 威胁防御设备将使用桥接技术在接口之间传递流量。每个桥接组包括一个网桥虚拟接口 (BVI)，供您为其分配一个网络 IP 地址。 在路由模式下，Firepower 威胁防御设备在 BVI 和常规路由接口之间路由。在透明模式下，每个网桥组都是独立的，相互之间无法通信。

双 IP 堆栈（IPv4 和 IPv6）

防火墙威胁防御设备在接口上同时支持 IPv6 和 IPv4 地址。请确保配置一条同时适用于 IPv4 和 IPv6 的默认路由。

31 位子网掩码

对于路由接口，您可以在31位子网上为点对点连接配置IP地址。31位子网只包含2个地址；通常，该子网中的第一个和最后一个地址预留用于网络和广播，因此，不可使用包含 2 个地址的子网。但是，如果您有点对点连接，并且不需要网络或广播地址，则 31 位子网是在 IPv4 中保留地址的有用方式。例如，2 个 防火墙威胁防御 之间的故障转移链路只需要 2 个地址；该链路一端传输的任何数据包始终由另一端接收，无需广播。您还可以拥有运行 SNMP 或系统日志的一个直连管理站。

31 位子网和集群

您可以在跨集群模式，但管理接口和集群控制链路除外。

31 位子网和故障转移

进行故障转移时，如果为 防火墙威胁防御 接口 IP 地址使用 31 位子网，则无法为该接口配置备用 IP 地址，因为没有足够的地址。通常，用于进行故障转移的接口应有一个备用IP地址，以便主设备可以执行接口测试来确保备用接口正常运行。如果没有备用IP地址，防火墙威胁防御无法执行任何网络测试；只能跟踪链路状态。

对于故障转移和可选的独立状态链路（点对点连接），也可以使用 31 位子网。

31 位子网和管理

如果您有直接连接的管理工作站，则对于防火墙威胁防御的SSH或HTTP，或管理工作站上的SNMP或 Syslog，可使用点对点连接。

31 位子网不支持的功能

以下功能不支持 31 位子网：

- 网桥组的 BVI 接口 - 网桥组需要至少 3 个主机地址：BVI 和连接到两个网桥组成员接口的两台主机。您必须使用 /29 子网或更小的子网。
- 组播路由

路由和透明模式接口准则和限制

高可用性、 集群和多实例

- 请勿采用本章中的程序配置故障转移接口。有关详细信息，请参阅高可用性。
- 对于集群接口，请参阅“集群”一章了解要求。
- 对于多实例模式，共享接口不支持用于网桥组成员接口（在透明模式或路由模式下）。
- 在使用高可用性时，则必须为数据接口手动设置 IP 地址和备用地址；不支持 DHCP 和 PPPoE。在**监控接口**区域中的**设备** > **设备管理** > **高可用性**选项卡上设置备用 IP 地址。有关详细信息，请参阅高可用性章节。

IPv6

- 所有接口上都支持 IPv6。
- 只能在透明模式下手动配置 IPv6 地址。
- 防火墙威胁防御设备 不支持 IPv6 任播地址。
- 透明模式、集群或高可用性不支持 DHCPv6 和前缀委派选项。

型号准则

- 对于具有桥接 ixgbevf 接口的 VMware 上的Firewall Threat Defense Virtual，桥接组不受支持。

透明模式和网桥组准则

- 您可以创建最多 250 个桥接组，每个桥接组 64 个接口。
- 各个直连网络必须在同一子网上。
- 防火墙威胁防御设备不支持辅助网络上的流量；只有与 BVI IP 地址相同的网络上的流量才受支持。

- 每个桥接组都需要 BVI 的 IP 地址，以用于管理往返设备的流量和使流量通过 防火墙威胁防御 设备。对于 IPv4 流量，请指定 IPv4 地址。对于 IPv6 流量，请指定 IPv6 地址。
- 您仅可手动配置 Ipv6 地址。
- BVI IP 地址必须与已连接网络位于同一子网上。您不能将该子网设置为主机子网 (255.255.255.255)。
- 不支持将管理接口作为桥接组成员。
- 对于多实例模式，共享接口不支持用于网桥组成员接口（在透明模式或路由模式下）。
- 对于具有桥接 ixgbevf 接口的 VMware 上的 Firewall Threat Defense Virtual ，透明模式不受支持，在路由模式中网桥组不受支持。
- 对于 Firepower 1010 和 Cisco Secure Firewall 1210/20，不能将逻辑 VLAN 接口和物理防火墙接口混合在同一个桥接组中。
- 对于 Firepower 4100/9300，不支持将数据共享接口作为网桥组成员。
- 在透明模式下，必须至少使用 1 个桥接组；数据接口必须属于桥接组。
- 在透明模式下，请勿将 BVI IP 地址指定为所连接设备的默认网关；设备需要将位于 防火墙威胁防御另一端的路由器指定为默认网关。
- 在透明模式下，默认路由（为管理流量提供返回路径所需的路由）仅适用于来自一个桥接组网络的管理流量。这是因为默认路由会指定网桥组中的接口以及网桥组网络上的路由器 IP 地址，而您只能定义一个默认路由。如果您具有来自多个桥接组网络的管理流量，则需要指定常规静态路由来确定预期会发出管理流量的网络。
- Amazon Web 服务、Microsoft Azure、Google Cloud Platform 和 Oracle Cloud Infrastructure 上部署的 Threat Defense Virtual 实例不支持透明模式。
- 在路由模式下，要在桥接组和其他路由接口之间路由，您必须指定 BVI。
- 在路由模式下，防火墙威胁防御 - 不支持将 EtherChannel 接口定义为网桥组成员。 Firepower 4100/9300 上的 Etherchannel 可以是网桥组成员。
- 使用网桥组成员时，不允许双向转发检测 (BFD) 回应数据包通过 防火墙威胁防御。如果 防火墙威胁防御 的一端有两个邻居运行 BFD，则 防火墙威胁防御 会因二者具有相同的源 IP 地址和目标 IP 地址且疑似属于 LAND 攻击而丢弃 BFD 回应数据包。

其他准则和要求

- 防火墙威胁防御 仅支持数据包中的一个 802.1Q 报头，不支持防火墙接口的多个报头（称为 QinQ 支持）。**注意**：对于内联集和被动接口，FTD 在数据包中最多支持 Q-in-Q 两个 802.1Q 报头，但 Firepower 4100/9300 仅支持一个 802.1Q 报头。
- 接口问题（例如频繁的启动/关闭状态更改）会导致浮动连接计时器无法正确应用于通过接口的连接。如果接口状态有问题，可考虑在状态稳定后清除所有连接，以清除无效连接。

配置路由模式接口

此程序介绍如何设置名称、安全区域和 IPv4 地址。

注释 并非所有接口类型都支持所有的字段。

开始之前

- **Firepower 4100/9300**
  1. 配置物理接口
  2. （可选）配置任何特殊接口。
     - 添加 EtherChannel（端口通道）
     - 为容器实例添加 VLAN 子接口 在 FXOS 中
     - 配置环回接口， 第 14 页
     - 添加子接口， 第 20 页 在 防火墙管理中心
     - 配置 VXLAN 接口， 第 31 页

- （可选） **所有其他型号：**
  - 配置 EtherChannel
  - 配置环回接口， 第 14 页
  - 添加子接口， 第 20 页
  - 配置 VXLAN 接口， 第 31 页
  - AWS 上的 Firewall Threat Defense Virtual：配置 Geneve 接口， 第 34 页
  - Firepower 1010 和 Cisco Secure Firewall 1210/1220：配置 VLAN 接口， 第 5 页

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 在**名称**字段中，输入长度最大为 48 个字符的名称。

名称不能以短语“cluster”开头。它保留供内部使用。

步骤 4 选中**启用**复选框以启用此接口。

步骤 5 （可选）将此接口设置为**管理专用**以限制到管理流量的流量；不允许通过设备的流量。

步骤 6 （可选）在**说明**字段中添加说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 7 在**模式 (Mode)** 下拉列表中，选择**无 (None)**。

常规防火墙接口的模式设置为“无”。其他模式用于仅 IPS 接口类型。

步骤 8 从**安全区域 (Security Zone)** 下拉列表中选择一个安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

路由接口是路由类型的接口，只能属于路由类型的区域。

步骤 9 有关 **MTU** 的详细信息，请参阅配置 MTU，第 64 页。

步骤 10 在 **优先级** 字段中，输入一个介于 0 和 65535 之间的数字。

此值在策略型路由配置中使用。优先级用于确定如何跨多个出口接口路由流量。有关详细信息，请参阅配置策略型路由策略。

步骤 11 点击 **Ipv4** 选项卡。要设置 IP 地址，请使用 **IP 类型**下拉列表中的下列选项之一。

高可用性、集群和环回接口仅支持静态 IP 地址配置；不支持 DHCP 和 PPPoE。

- **使用静态 IP** - 输入 IP 地址和子网掩码。对于点对点连接，可以指定 31 位子网掩码（255.255.255.254 或 /31）。在这种情况下，不会为网络或广播地址预留 IP 地址。在此情况下，无法设置备用 IP 地址。对于高可用性，只能使用静态 IP 地址。在 **监控接口** 区域中的 **设备** > **设备管理** > **高可用性**选项卡上设置备用 IP 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。
- **使用 DHCP** - 配置以下可选参数：
  - **使用 DHCP 获取默认路由 (Obtain default route using DHCP)** - 从 DHCP 服务器获取默认路由。
  - **DHCP 路由指标 (DHCP route metric)** - 分配到所获悉路由的管理距离，介于 1 和 255 之间。获悉的路由的默认管理距离为 1。
- **使用 PPPoE** - 如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，请配置以下参数：
  - **VPDN 组名称** - 指定您选择的组名称来表示此连接。
  - **PPPoE 用户名** - 指定 ISP 提供的用户名。
  - **PPPoE 密码/确认密码** - 指定并确认 ISP 提供的密码。
  - **PPP 身份验证** - 选择 **PAP**、**CHAP** 或 **MSCHAP**。

    PAP 在身份验证过程中传递明文用户名和密码，这样并不安全。使用 CHAP 时，客户端可返回加密的 [challenge plus password] 和明文用户名来响应服务器质询。CHAP 比 PAP 更安全，但其不会加密数据。MSCHAP 与 CHAP 类似但更安全，因为服务器只对加密密码进行

存储和比较，而不是像 CHAP 一样存储和比较明文密码。MSCHAP 还可生成密钥，以便 MPPE 进行数据加密。

- **PPPoE 路由指标** - 向获悉的路由分配管理距离。有效值范围为 1 到 255。默认情况下，获悉的路由的默认管理距离为 1。
- **启用路由设置** - 要手动配置 PPPoE IP 地址，请选中此框，然后输入 **IP 地址**。

  如果选中 **启用路由设置** 复选框并将 **IP 地址** 留空，则会应用 **ip address pppoe setroute** 命令，如下例所示：

```
interface GigabitEthernet0/2
nameif inside2_pppoe
cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
security-level 0
pppoe client vpdn group test
pppoe client route distance 10
ip address pppoe setroute
```

- **在闪存中存储用户名和密码** - 在闪存中存储用户名和密码。

  设备将用户名和密码存储在 NVRAM 中的专用位置。

步骤 12 （可选） 要在 **IPv6** 选项卡上配置 IPv6 寻址，请参阅配置 IPv6 寻址，第 48 页。

步骤 13 （可选） 要在**高级**选项卡上手动配置 MAC 地址，请参阅配置 MAC 地址，第 64 页。

步骤 14 （可选） 通过点击 **硬件配置 (Hardware Configuration)** > **速度 (Speed)**，设置复用和速度。

- **复用**—选择 **全** 或 **半**。SFP 接口仅支持 **全** 复用。
- **速度**-选择速度（因型号而异）。（仅限 Cisco Secure Firewall 3100/4200 ）选择 **检测 SFP** 以检测已安装的 SFP 模块的速度并使用适当的速度。复用始终为全复用，并且始终启用自动协商。如果您稍后将网络模块更改为其他型号，并希望速度自动更新，则此选项非常有用。对于 Cisco Secure Firewall 1250，您可以配置的最大接口速度为 2.5gbps。

  注释
  您无法修改 HA 或集群控制链路接口的速度。
- **自动协商**-设置接口以协商速度、链路状态和流量控制。
- **前向纠错模式**-（仅限 Cisco Secure Firewall 3100/4200 ）对于 25 Gbps 及更高的接口，请启用前向纠错 (FEC)。对于 EtherChannel 成员接口，必须先配置 FEC，然后才能将其添加到 EtherChannel。使用**自动 (Auto)** 时选择的设置取决于收发器类型，以及接口是固定接口（内置）还是在网络模块上。

表 *1:* 用于自动设置的默认 *FEC*

收发器类型	固定端口默认 **FEC**（以太网 **1/9** 至 **1/16**）	网络模块默认 **FEC**
25G-SR	Clause 108 RS-FEC	Clause 108 RS-FEC
25G-LR	Clause 108 RS-FEC	Clause 108 RS-FEC

收发器类型	固定端口默认 **FEC**（以太网 **1/9** 至 **1/16**）	网络模块默认 **FEC**
10/25G-CSR	Clause 108 RS-FEC	Clause 74 FC-FEC
25G-AOC*x*M	Clause 74 FC-FEC	Clause 74 FC-FEC
25G-CU2.5/3M	自动协商	自动协商
25G-CU4/5M	自动协商	自动协商
25/50/100G	Clause 91 RS-FEC	Clause 91 RS-FEC

步骤 15 （可选） 在**管理访问 (Manager Access)** 页面上启用数据接口上的 防火墙管理中心 管理器访问。

首次设置 时，您可以从数据接口启用管理器访问。如果要在将 添加到 防火墙管理中心 后启用或禁用管理器访问，请参阅：

- 启用管理器访问：将管理器访问接口从管理更改为数据

  注释
  除非先启动管理器接口从管理到数据接口的迁移，否则无法启用管理器访问。启动迁移后，您可以在**管理器访问 (Manager Access)** 页面上启用管理器访问并成功保存配置。

- 禁用管理器访问：将管理器访问接口从数据更改为管理

如果要将管理器访问接口从一个数据接口更改为另一个数据接口，必须在原始数据接口上禁用管理器访问，但不要禁用接口本身；必须使用原始数据接口执行部署。如果要在新管理器访问接口上使用相同的 IP 地址，可以删除或更改原始接口上的 IP 配置；此更改不应影响部署。如果为新接口使用不同的 IP 地址，则还要更改 防火墙管理中心 中显示的设备 IP 地址；请参阅更新防火墙管理中心中的主机名或 IP 地址。请务必同时更新相关配置，以使用新接口，例如静态路由、DDNS 和 DNS 设置。

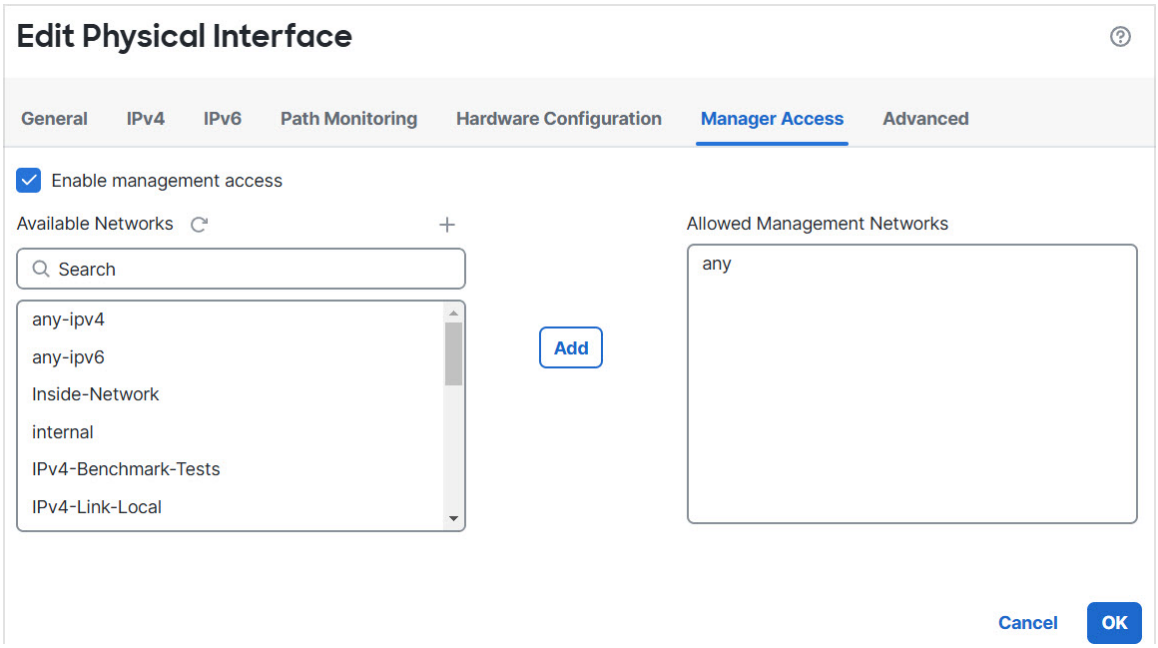
从数据接口进行管理器访问具有以下限制：

- 只能在一个物理数据接口上启用管理器访问。不能使用子接口或 EtherChannel，也不能在管理器访问接口上创建子接口。 您还可以使用 防火墙管理中心 在单个辅助接口上启用管理器访问，以实现冗余。
- 此接口不能是仅管理接口。
- 仅路由防火墙模式，使用路由接口。
- 不支持 PPPoE。如果您的 ISP 需要 PPPoE，则必须在 与 WAN 调制解调器之间放入支持 PPPoE 的路由器。
- 接口只能位于全局 VRF 中。
- 默认不对数据接口启用 SSH，因此必须稍后使用 防火墙管理中心 来启用 SSH。由于管理接口网关将更改为数据接口，因此您也无法启动从远程网络到管理接口的 SSH 会话，除非您使用 **configure network static-routes** 命令为管理接口添加静态路由。对于 Amazon Web 服务上的

Firewall Threat Defense Virtual，控制台端口不可用，因此您应保持对管理接口的 SSH 访问：在继续配置之前为管理添加静态路由。或者，请确保在配置用于管理器访问的数据接口并断开连接之前完成所有 CLI 配置（包括 **configure manager add** 命令）。

- 您不能使用单独的管理接口和仅事件接口。
- 不支持集群技术。在这种情况下，必须使用管理接口。

图 *19:* 管理器访问



- 选中**在此接口上为管理器启用管理 (Enable management on this interface for the manager)** 以便使用此数据接口进行管理，而不是专用管理接口。
- （可选）在**允许的管理网络 (Allowed Management Networks)** 框中，添加要允许管理器访问的网络。默认情况下，允许任何网络。

步骤 16 点击**确定**。

步骤 17 点击**保存**。

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。

配置网桥组接口

网桥组是指 Cisco Secure Firewall Threat Defense 设备网桥（而非路由）的接口组。 网桥组在透明和路由防火墙模式下受支持。有关网桥组的详细信息，请参阅 关于网桥组。

要配置网桥组和关联接口，请执行以下步骤。

配置常规网桥组成员接口参数

此程序描述如何为每个网桥组成员接口设置名称和安全区域。同一网桥组可以包括不同类型的接口：物理接口、子接口、 Firepower 1010 和 Cisco Secure Firewall 1210/1220 VLAN 接口、EtherChannel 接口和冗余接口 。管理接口不受支持。 在路由模式中，不支持 EtherChannels。对于 Firepower 4100/9300，不支持数据共享类型的接口。

开始之前

- **Firepower 4100/9300**
  1. 配置物理接口
  2. （可选）配置任何特殊接口。
     - 添加 EtherChannel（端口通道）
     - 为容器实例添加 VLAN 子接口 在 FXOS 中
     - 添加子接口， 第 20 页 在 防火墙管理中心
- （可选） **所有其他型号**：
  - 配置 EtherChannel
  - 添加子接口， 第 20 页
  - Firepower 1010 和 Cisco Secure Firewall 1210/1220：配置 VLAN 接口， 第 5 页

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 设备的 **编辑** ()。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** ()。

步骤 3 在**名称**字段中，输入长度最大为 48 个字符的名称。

名称不能以短语“cluster”开头。它保留供内部使用。

步骤 4 选中**启用**复选框以启用此接口。

步骤 5 （可选） 将此接口设置为**管理专用**以限制到管理流量的流量；不允许通过设备的流量。

步骤 6 （可选） 在**说明**字段中添加说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 7 在**模式 (Mode)** 下拉列表中，选择**无 (None)**。

常规防火墙接口的模式设置为“无”。其他模式用于仅 IPS 接口类型。在将此接口分配到网桥组后，该模式将显示为**交换**。

步骤 8 从**安全区域 (Security Zone)** 下拉列表中选择一个安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

桥接组成员接口是交换类型的接口，只能属于交换类型的区域。请勿为此接口设置任何 IP 地址设置。您将只设置桥接虚拟接口 (BVI) 的 IP 地址。请注意，BVI 不属于某个区域，您不能将访问控制策略应用到 BVI。

步骤 9 有关 **MTU** 的详细信息，请参阅配置 MTU，第 64 页。

步骤 10 （可选） 通过点击 **硬件配置 (Hardware Configuration)** > **速度 (Speed)**，设置复用和速度。

- **复用**—选择 **全** 或 **半**。SFP 接口仅支持 **全** 复用。
- **速度**-选择速度（因型号而异）。（仅限 Cisco Secure Firewall 3100/4200 ）选择 **检测 SFP** 以检测已安装的 SFP 模块的速度并使用适当的速度。复用始终为全复用，并且始终启用自动协商。如果您稍后将网络模块更改为其他型号，并希望速度自动更新，则此选项非常有用。对于Cisco Secure Firewall 1250，您可以配置的最大接口速度为 2.5gbps。

  注释
  您无法修改 HA 或集群控制链路接口的速度。

- **自动协商**-设置接口以协商速度、链路状态和流量控制。
- **前向纠错模式**-（仅限 Cisco Secure Firewall 3100/4200 ）对于 25 Gbps 及更高的接口，请启用前向纠错 (FEC)。对于 EtherChannel 成员接口，必须先配置 FEC，然后才能将其添加到 EtherChannel。使用**自动 (Auto)** 时选择的设置取决于收发器类型，以及接口是固定接口（内置）还是在网络模块上。

  表 *2:* 用于自动设置的默认 *FEC*

收发器类型	固定端口默认 **FEC**（以太网 **1/9** 至 **1/16**）	网络模块默认 **FEC**
25G-SR	Clause 108 RS-FEC	Clause 108 RS-FEC
25G-LR	Clause 108 RS-FEC	Clause 108 RS-FEC
10/25G-CSR	Clause 108 RS-FEC	Clause 74 FC-FEC
25G-AOC*x*M	Clause 74 FC-FEC	Clause 74 FC-FEC
25G-CU2.5/3M	自动协商	自动协商
25G-CU4/5M	自动协商	自动协商
25/50/100G	Clause 91 RS-FEC	Clause 91 RS-FEC

步骤 11 （可选） 要在 **IPv6** 选项卡上配置 IPv6 寻址，请参阅配置 IPv6 寻址，第 48 页。

步骤 12 （可选） 要在**高级**选项卡上手动配置 MAC 地址，请参阅配置 MAC 地址，第 64 页。

步骤 13 点击**确定**。

步骤 14 点击**保存**。

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。

配置网桥虚拟接口 (BVI)

每个网桥组都需要一个您应为其配置 IP 地址的 BVI。 使用此 IP 地址作为源自网桥组的数据包的源地址。BVI IP 地址必须与所连接的网络位于同一子网。对于 IPv4 流量，任何流量的传递都需要使用 BVI IP。对于 IPv6 流量，您必须至少配置链路本地地址以传递流量，但要实现完整功能（包括远程管理和其他管理操作），建议采用全局管理地址。

对于路由模式，如果为 BVI 提供一个名称，则 BVI 将参与路由。如果不提供名称，网桥组在透明防火墙模式下将保持隔离状态。

开始之前

您不能将 BVI 添加到安全区域；因此，不能将访问控制策略应用到 BVI。必须根据其区域将策略应用于网桥组成员接口。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 设备的 **编辑** ()。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 选择**添加接口** > **网桥组接口**。

步骤 3 （路由模式）在**名称**字段中，输入长度最大为 48 个字符的名称。

如果要在网桥组成员之外路由流量，例如路由到外部接口或其他网桥组的成员，则必须为 BVI 命名。该名称不区分大小写。

步骤 4 在**网桥组 ID** 字段中，输入 1 和 250 之间的网桥组 ID。

步骤 5 在**说明**字段中，输入此网桥组的说明。

步骤 6 在**接口**选项卡上，点击某个接口对，然后点击**添加**，以将其移动至**选定的接口**区域。对要使其成为网桥组成员的所有接口重复此步骤。

步骤 7 （透明模式）点击 **IPv4** 选项卡。在 **IP 地址**字段中，输入 IPv4 地址和子网掩码。

请勿为 BVI 分配主机地址（/32 或 255.255.255.255）。此外，请勿使用主机地址不足 3 个（分别用于上游路由器、下游路由器和透明防火墙）的其他子网，例如 /30 子网 (255.255.255.252)。 设备会丢弃传入子网中第一个和最后一个地址或从其传出的所有 ARP 数据包。例如，如果您使用 /30 子网，并从该子网中为上游路由器分配了一个预留地址，那么 设备将丢弃从下游路由器发送至上游路由器的 ARP 请求。

对于高可用性，请在 **监控接口** 区域的 **设备** > **设备管理** > **高可用性** 选项卡中设置备用 IP 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 8 （路由模式）点击 **IPv4** 选项卡。要设置 IP 地址，请使用 **IP 类型**下拉列表中的下列选项之一。

高可用性和集群接口仅支持静态 IP 地址配置；不支持 DHCP。

- **使用静态 IP** - 输入 IP 地址和子网掩码。对于高可用性，只能使用静态 IP 地址。在 **监控接口** 区域中的 **设备** > **设备管理** > **高可用性**选项卡上设置备用 IP 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。
- **使用 DHCP** - 配置以下可选参数：
  - **使用 DHCP 获取默认路由 (Obtain default route using DHCP)** - 从 DHCP 服务器获取默认路由。
  - **DHCP 路由指标 (DHCP route metric)** - 分配到所获悉路由的管理距离，介于 1 和 255 之间。获悉的路由的默认管理距离为 1。

步骤 9 （可选） 请参阅配置 IPv6 寻址，第 48 页配置 Ipv6 寻址。

步骤 10 （可选） 要配置 **ARP** 和 **MAC** 设置，请参阅添加静态 ARP 条目，第 65 页和添加静态 MAC 地址并为网桥组禁用 MAC 学习，第 66 页（仅对于透明模式）。

步骤 11 点击**确定**。

步骤 12 点击**保存**。

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。

配置 IPv6 寻址

本节介绍如何在路由模式和透明模式下配置 IPv6 寻址。

关于 IPv6

本节包括关于 IPv6 的信息。

IPv6 寻址

您可以为 IPv6 配置两种类型的单播地址：

- 全局 - 全局地址是可在公用网络上使用的公用地址。对于网桥组，需要为 BVI（而不必为每个成员接口）配置此地址。还可以为透明模式下的管理接口配置全局 IPv6 地址。
- 链路本地 - 链路本地地址是只能在直连网络上使用的专用地址。路由器不使用链路本地地址转发数据包；它们仅用于在特定物理网段上通信。链路本地地址可用于地址配置或邻居发现功能，例如地址解析。在网桥组中，只有成员接口具有链路本地地址；BVI 没有链路本地地址。

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。对于网桥组成员接口，在 BVI 上配置全局地址时，防火墙威胁防御设备 将为成员接口自动生成链路本地地址。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。

修改的 EUI-64 接口 ID

RFC 3513：互联网协议第 6 版 (IPv6) 寻址架构要求所有单播 IPv6 地址（以二进制值 000 开头的地址除外）的接口标识符部分的长度为 64 位，并以修改的 EUI-64 格式进行构造。防火墙威胁防御设备可为连接到本地链路的主机执行该要求。

在接口上启用此功能时，该接口接收的 IPv6 数据包源地址根据源 MAC 地址进行验证，以确保接口标识符使用修改的 EUI-64 格式。如果 IPv6 数据包不将修改的 EUI - 64 格式用于接口标识符，则会丢弃数据包并生成以下系统日志消息：

```
325003: EUI-64 source address check failed.
```

只有在创建流量时才会执行地址格式验证。不检查来自现有流量的数据包。此外，只能对本地链路上的主机执行地址验证。

配置 IPv6 前缀代理客户端

威胁防御 可以作为 DHPCv6 前缀授权客户端，以便客户端接口（例如连接到电缆调制解调器的外部接口）可以接收一个或多个 IPv6 前缀，然后 威胁防御 可以将这些前缀通过子网分配到其内部接口。

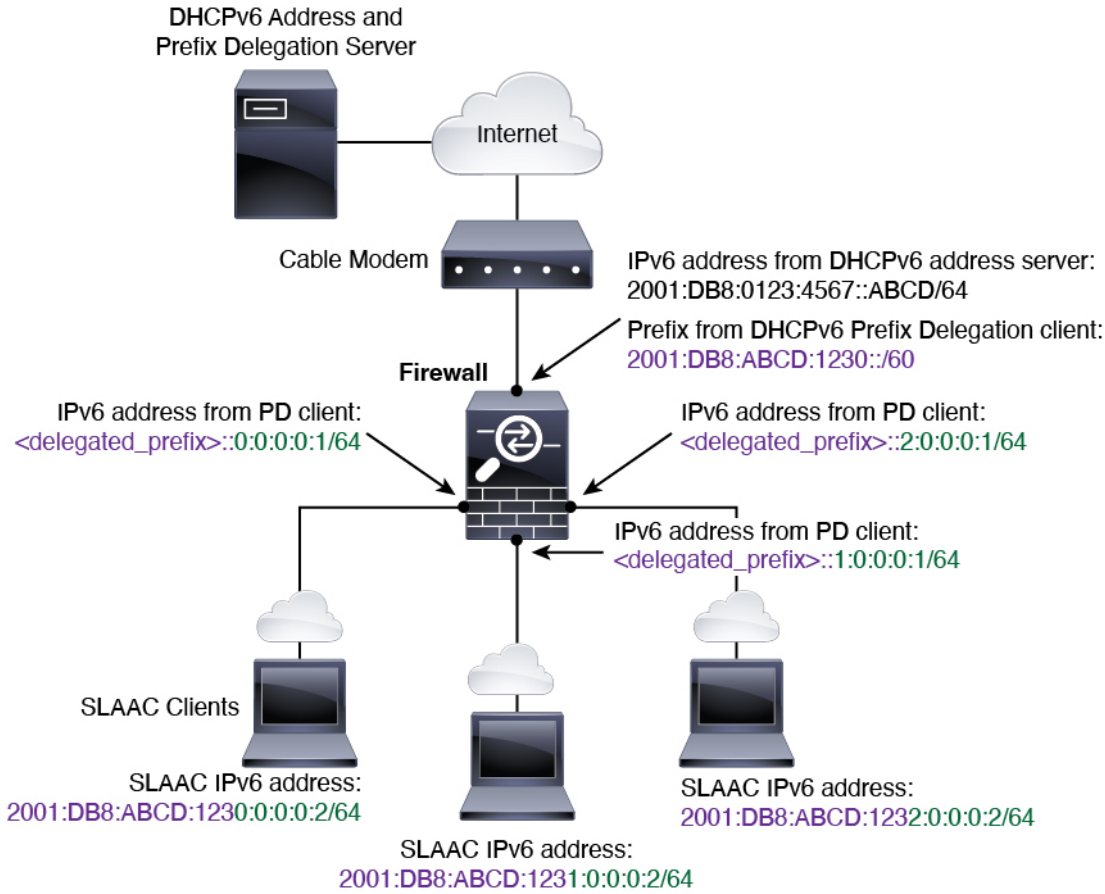
关于 IPv6 前缀授权

威胁防御 可以作为 DHPCv6 前缀授权客户端，以便客户端接口（例如连接到电缆调制解调器的外部接口）可以接收一个或多个 IPv6 前缀，然后 威胁防御 可以将这些前缀通过子网分配到其内部接口。然后，连接到内部接口的主机可以使用无状态地址自动配置 (SLAAC) 获取全局 IPv6 地址。请注意，内部 威胁防御 接口不会依次充当前缀授权服务器；威胁防御 只能向 SLAAC 客户端提供全局 IP 地址。例如，如果路由器连接到 威胁防御，它可以作为 SLAAC 客户端获取其 IP 地址。但是，如果您要为路由器后的网络使用授权的前缀的子网，则必须在路由器的内部接口上手动配置这些地址。

威胁防御 中包括一个轻型 DHCPv6 服务器，以便 SLAAC 客户端在向 威胁防御 发送信息请求 (IR) 数据包时，威胁防御 可以向这些客户端提供 DNS 服务器和域名等信息。威胁防御 仅接受 IR 数据包，不向客户端分配地址。您将通过在客户端上启用 IPv6 自动配置来配置客户端，以便生成自己的 IPv6 地址。在客户端上启用无状态自动配置时，将基于路由器通告消息中接收到的前缀来配置 IPv6 地址；换句话说，根据使用前缀授权收到 威胁防御 的前缀。

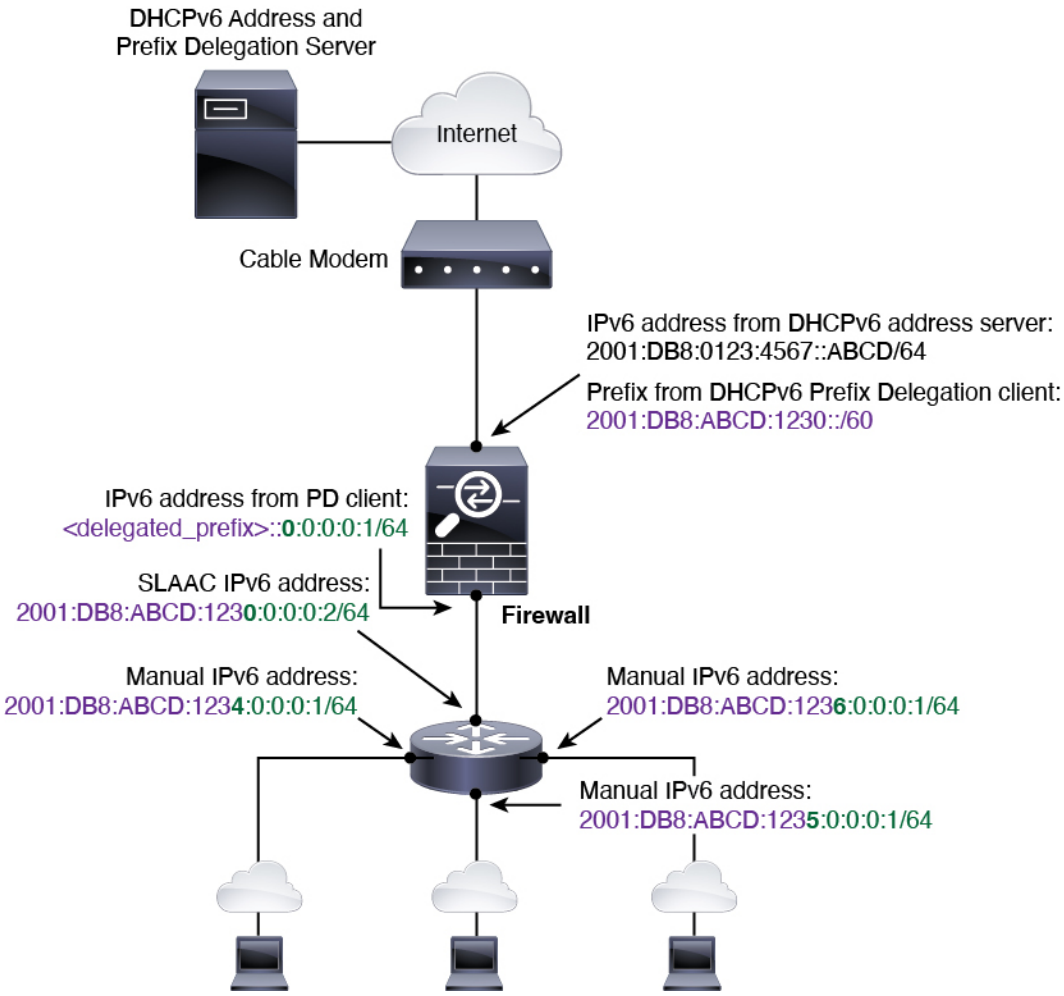
IPv6 前缀授权 */64* 子网示例

以下示例显示使用 DHCPv6 地址客户端在外部接口上接收 IP 地址的 威胁防御。此外，它还会使用 DHCPv6 前缀授权客户端获得一个授权的前缀。威胁防御 将授权的前缀编入 /64 网络的子网，并使用授权的前缀以及手动配置的子网（::0、::1 或 ::2）和每个接口上的 IPv6 地址 (0:0:0:1) 为其内部接口动态分配全局 IPv6 地址。连接至这些内部接口的 SLAAC 客户端将获得每个 /64 子网上的 IPv6 地址。



IPv6 前缀委派 */62* 子网示例

以下示例显示了 威胁防御 将前缀子网划分到 4 个 /62 子网中:2001:DB8:ABCD:123**0**::/62、2001:DB8:ABCD:123**4**::/62、2001:DB8:ABCD:123**8**::/62 和 2001:DB8:ABCD:123**C**::/62。威胁防御 将 2001:DB8:ABCD:1230::/62 上 4 个可用 /64 子网之一用于其内部网络 (::0)。随后您可以手动将其他 /62 子网用于下游路由器。所示的路由器将 2001:DB8:ABCD:1234::/62 上 4 个可用 /64 子网中的 3 个用于其内部接口（::4、::5 和 ::6）。在此情况下，内部路由器接口无法动态获取委派的前缀，因此您需要在 威胁防御 上查看委派的前缀，然后将该前缀用于您的路由器配置。通常，当租约到期时，ISP 会将同一前缀委派给指定客户端，但如果 威胁防御 收到新前缀，则您必须修改路由器配置以使用该新前缀。DHCP 唯一标识符 (DUID) 在重新启动时会保持不变。



启用 IPv6 前缀授权客户端

在一个或多个接口上启用 DHCPv6 前缀代理客户端。 可获取一个或多个可设置子网和分配给内部网络的 IPv6 前缀。通常，在其上启用前缀代理客户端的接口使用 DHCPv6 地址客户端获取其 IP 地址，只有其他 接口才能使用代理前缀衍生的地址。

此功能仅支持路由模式。此功能不支持集群或高可用性。

开始之前

当您使用前缀代理时，必须将 IPv6 邻居发现路由器通告间隔设置为远低于 DHCPv6 服务器分配的前缀的首选有效期，以防 IPv6 流量中断。例如，如果 DHCPv6 服务器将首选前缀代理有效期设置为 300 秒，则您应将 RA 间隔设置为 150 秒。要设置首选有效期，请使用 **show ipv6 general-prefix** 命令。要设置 RA 间隔，请参阅 配置 IPv6 邻居发现， 第 57 页；默认值为 200 秒。

过程

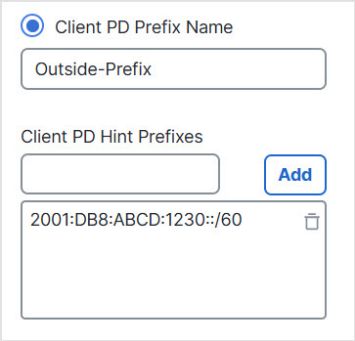
步骤 1 选择 **设备** > **设备管理** 并点击您的 设备的 **编辑** ()。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** ()。

步骤 3 点击 **IPv6** 页面，然后点击 **DHCP**。

步骤 4 点击**客户端 PD 前缀名称 (Client PD Prefix Name)**，然后输入此前缀的名称。

图 *20:* 启用前缀授权客户端



name 最长为 200 个字符。

步骤 5 （可选）在**客户端 PD 提示前缀 (Client PD Hint Prefixes)** 字段中输入前缀和前缀长度，以便向 DHCP 服务器提供有关要接收的委派前缀的一个或多个提示，然后点击**添加 (Add)**。

通常，您需要请求特定的前缀长度（例如 ::/60），或者如果您以前收到过特定前缀并希望确保在租用到期后重新获取该前缀，可以作为提示输入整个前缀。如果输入了多个提示（不同的前缀或长度），则由 DHCP 服务器来决定要尊重的提示或是否尊重提示。

步骤 6 点击**确定**。

步骤 7 点击**保存**。

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。

配置全局 IPv6 地址

要为任何路由模式接口和透明或路由模式 BVI 配置全局 IPv6 地址，请执行以下步骤。

注释 配置全局地址将自动配置链路本地地址，因此无需单独对其进行配置。对于网桥组，在 BVI 上配置全局地址会自动在所有成员接口上配置链路本地地址。

对于在 防火墙威胁防御 上定义的子接口，建议您同样手动设置 MAC 地址，这是因为它们使用父接口上相同的固化 MAC 地址。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，这能够避免 防火墙威胁防御 上特定实例内发生流量中断。请参阅配置 MAC 地址，第 64 页。

开始之前

对于网桥组的 IPv6 邻居发现，您必须使用双向访问规则明确允许邻居请求（ICMPv6 类型 135）和邻居通告（ICMPv6 类型 136）数据包通过 网桥组成员接口。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 点击 **IPv6** 页面。

对于路由模式，**基本 (Basic)** 页面默认处于选中状态。对于透明模式，**地址 (Address)** 页面默认处于选中状态。

步骤 4 （可选） 在**基本 (Basic)** 页面上，选中**启用 IPv6 (Enable IPv6)**。

如果您只想配置链路本地地址，请使用此选项。否则，配置 IPv6 地址将自动启用 IPv6 处理。

步骤 5 使用以下其中一种方法配置全局 IPv6 地址。

要用于故障转移和集群，以及用于环回接口，您必须手动设置 IP 地址。对于集群，也不支持手动配置链路本地地址。

- （路由接口）无状态自动配置 - 选中**自动配置**复选框。

  在接口上启用无状态自动配置时，将基于路由器通告消息中接收到的前缀来配置 IPv6 地址。启用无状态自动配置时，将基于修改的 EUI-64 接口 ID 自动生成接口的链路本地地址。

  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 设备在这种情况下确实会发送路由器通告消息。取消选中**IPv6** > **设置** > **启用 RA** 复选框以抑制邮件。

- 手动配置 - 要手动配置全局 IPv6 地址，请执行以下操作：

  1. 点击**地址 (Address)** 页面并点击 (＋)**添加地址 (Add Address)**。

     系统将显示**添加接口**对话框。

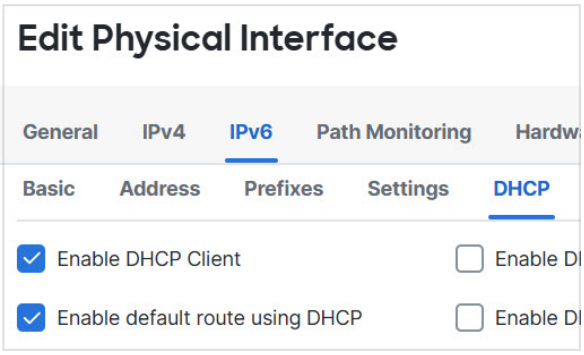
  2. 在**地址**字段中，输入完整全局 IPv6 地址（包括接口 ID），或输入 IPv6 前缀以及 IPv6 前缀长度。（路由模式）如果仅输入前缀，请务必选中**强制 EUI 64** 复选框，以使用修改的 EUI-64

格式生成接口 ID。例如，2001:0DB8::BA98:0:3210/48（完整地址）或 2001:0DB8::/48（前缀，且选中 EUI 64）。

对于高可用性（如果未设置**强制 EUI 64 (Enforce EUI 64)**），请在**设备 (Devices)** > **设备管理 (Device Management)** > **高可用性 (High Availability)** 页面的**受监控接口 (Monitored Interfaces)** 区域中设置备用 IP 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。

- （路由接口）使用 DHCPv6 获取地址 - 要使用 DHCPv6，请执行以下操作：

图 *21:* 启用 *DHCPv6* 客户端



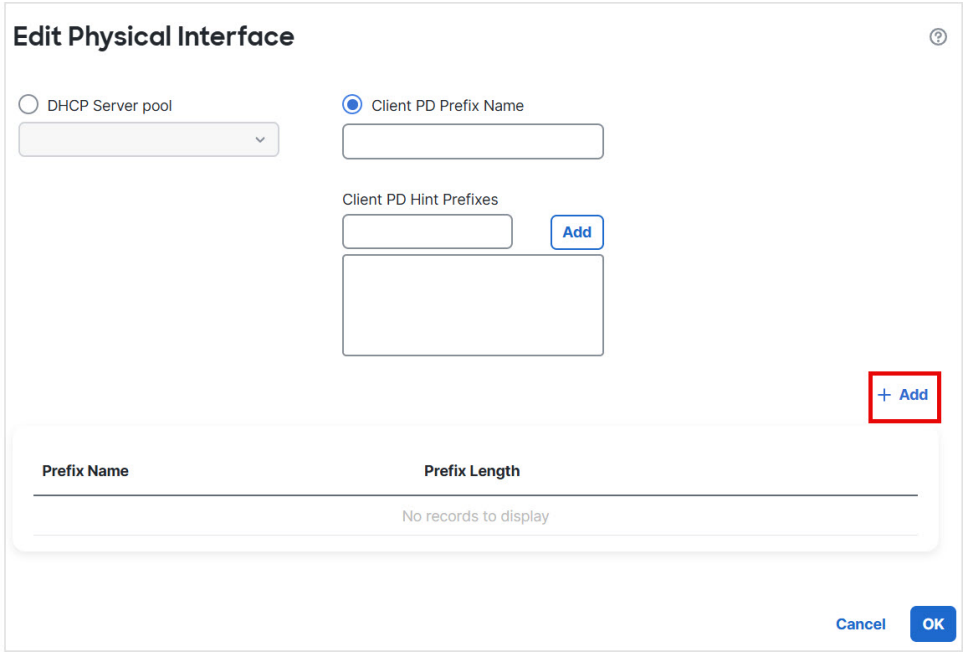
1. 点击 **DHCP** 页面。
2. 选中**启用 DHCP 客户端 (Enable DHCP Client)** 的复选框。
3. （可选）选中**使用 DHCP 启用默认路由 (Enable default route using DHCP)** 复选框，从路由器通告中获取默认路由。

- （路由接口）使用授权前缀 - 要使用授权前缀分配 IPv6 地址，请执行以下操作：

此功能要求 在不同接口上启用 DHCPv6 前缀授权客户端。请参阅启用 IPv6 前缀授权客户端，第 51 页。

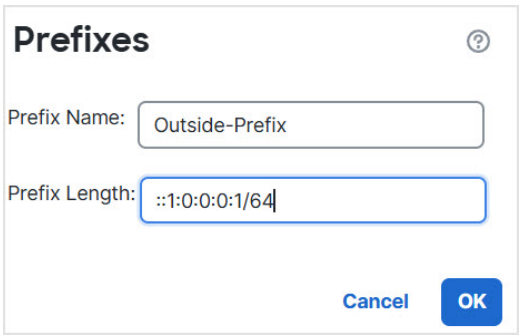
1. 点击 **DHCP** 页面。
2. 请点击 (+)。

图 *22:* 使用授权的前缀



3. 输入您在另一个接口上为前缀委派客户端指定的**前缀名称**（请参阅启用 IPv6 前缀授权客户端，第 51 页）。

图 *23:* 指定前缀名称和地址

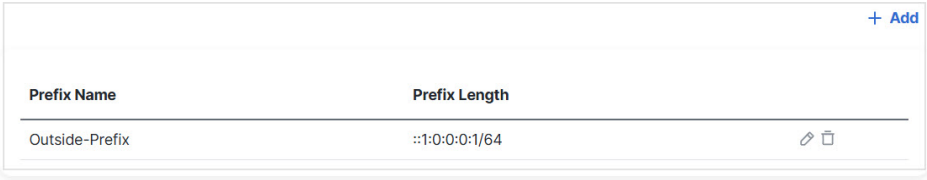


4. 输入 IPv6 地址和**前缀长度**。

   通常情况下，授权的前缀将为 /60 或更小，因此您可以将其作为多个 /64 网络的子网。如果希望连接的客户端支持 SLAAC，则 /64 是受支持的子网长度。您应指定可以完成 /60 子网的地址，例如 ::1:0:0:0:1。在地址前输入 ::，以免前缀小于 /60。例如，如果授权的前缀是 2001:Db8:1234:5670::/60，则分配给该接口的全局 IP 地址是 2001:DB8:1234:5671::1/64。在路由器通告中通告的前缀是 2001:DB8:1234:5671::/64。在本例中，如果前缀小于 /60，则前缀剩余的位将是 0，就如前导 :: 所指示的那样。例如，如果前缀是 2001:DB8:1234::/48，则 IPv6 地址将为 2001:DB8:1234::1:0:0:0:1/64。

5. 点击**确定**。

图 *24:* 前缀授权表



6. 或者，在此接口上启用 DHCPv6 无状态服务器（请参阅启用 DHCPv6 无状态服务器）。如果执行此操作，我们建议您同时选中**为非地址配置启用 DHCP (Enable DHCP for non-address config)** 选项。

步骤 6 对于路由接口，您可以选择在**基本 (Basic)** 页面上设置下列值：

- 要在本地链路上的 IPv6 地址中强制使用修改的 EUI-64 格式的接口标识符，请选中**强制 EUI-64** 复选框。
- 要手动设置链路本地地址，请在**链路本地地址**字段中输入地址。

  链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feee:6a82。如果您不想配置全局地址，且只需配置链路本地地址，则可以选择手动定义链路本地地址。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。

  集群不支持手动链路本地地址。

步骤 7 对于路由接口，您可以选择在 **DHCP** 页面上设置下列值：

- 选中**为地址配置启用 DHCP** 复选框以在 IPv6 路由器通告数据包中设置托管地址配置标志。

  IPv6 路由器通告中的此标志通知 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。

- 选中**为非地址配置启用 DHCP** 复选框以在 IPv6 路由器通告数据包中设置其他地址配置标志。

  IPv6 路由器通告中的此标志通知 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。在使用具有 DHCPv6 前缀委派的 DHCPv6 无状态服务器时使用此选项。

步骤 8 对于路由接口，请参阅配置 IPv6 邻居发现，第 57 页以配置**前缀 (Prefixes)** 和**设置 (Settings)** 页面上的设置。对于 BVI 接口，请参阅**设置 (Settings)** 页面上的以下参数：

- **DAD 尝试次数** - DAD 尝试的最大数，介于 1 和 600 之间。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。此设置可配置当对 IPv6 地址执行 DAD 时，接口上发送的连续邻居请求消息的数量。默认值为 1 次尝试。
- **NS 间隔** - 接口上 Ipv6 邻居请求重新传输之间的间隔，介于 1000 和 3600000 毫秒之间。默认值为 1000 毫秒。
- **可达时间** - 可达性确认事件发生后远程 IPv6 节点被视为可达的时长，介于 0 和 3600000 毫米之间。默认值为 0 毫秒。当该值为 0 时，将发送未确定的可访问时间。由接收设备来设置和跟踪

可访问时间的值。邻居可访问时间可启用检测不可用邻居。配置时间越短，检测不可用邻居的速度就越快，但是，时间缩短却在所有 IPv6 网络设备中占用了更多的 IPv6 网络带宽和处理资源。在正常 IPv6 操作中不建议设置很短的配置时间。

步骤 9 点击**确定**。

步骤 10 点击**保存**。

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。

配置 IPv6 邻居发现

IPv6 邻居发现过程使用 ICMPv6 消息和请求节点组播地址，确定同一网络（本地链路）中邻居的链路层地址、验证邻居的可读性及跟踪相邻路由器。

节点（主机）使用邻居发现确定已知驻留在连接的链路上邻居的链路层地址并快速清除变为无效的缓存值。主机还使用邻居发现查找愿意代表自己转发数据包的邻居路由器。此外，节点使用协议主动跟踪哪些邻居可访问及哪些邻居不可访问，并检测已更改的链路层地址。当路由器或路由器的路径发生故障时，主机会主动搜索起作用的替代项。

开始之前

仅在路由模式下受支持。有关透明模式下支持的 IPv6 邻居设置，请参阅配置全局 IPv6 地址，第 52 页。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 点击 **IPv6**，然后点击**前缀 (Prefixes)**。

步骤 4 （可选） 要配置包含在 IPv6 路由器通告中的 IPv6 前缀，请执行以下步骤：

a) 点击 (+)**添加前缀**。

b) 在**地址**字段中，输入带有前缀长度的 IPv6 地址，或选中**默认**复选框以使用默认前缀。

c) （可选）取消选中**通告**复选框，以指示未通告 IPv6 前缀。对于**默认**前缀，此设置仅适用于 on-link 前缀。除非您取消选中特定 Off-link 前缀的**通告**，否则仍将通告 Off-link 前缀。

d) 选中**关闭链路**复选框以指示指定的前缀已分配给链路。向包含指定前缀的地址发送流量的节点会将目标视为在链路上本地可访问。此前缀不得用于链路上确定。

e) 要使用指定的前缀进行自动配置，请选中**自动配置**复选框。

f) 对于**前缀有效期**，请点击**持续时间**或**到期日期**。

- **持续时间** - 以秒为单位输入前缀的**首选有效期**。此设置是将指定的 IPv6 前缀通告为有效的时间。最大值代表无穷大。有效值为 0 到 4294967295。默认值为 2592000 秒（30 天）。以秒为单位输入前缀的**有效期**。此设置是将指定的 IPv6 前缀通告为首选时间。最大值代表无

穷大。有效值为 0 到 4294967295。默认设置为 604800 秒（七天）。或者，选中**无限 (Infinite)**复选框以设置不受限制的持续时间。

- **到期日期** - 选择**有效**和**首选**日期和时间。

g) 点击**确定**。

步骤 5 点击**设置**。

步骤 6 （可选） 设置介于 1 和 600 之间的 **DAD 尝试次数**最大值。默认值为 1 次尝试。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。

此设置可配置当对 IPv6 地址执行 DAD 时，接口上发送的连续邻居请求消息的数量。

在无状态自动配置过程中，重复地址检测会验证新单播 IPv6 地址的唯一性，再将地址分配给接口。

识别出重复地址后，该地址的状态会设置为 DUPLICATE，且不会使用该地址并生成以下错误消息：

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

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。

步骤 7 （可选） 在 **NS 间隔**字段中配置 IPv6 邻居请求重新传输之间的间隔，介于 1000 和 3600000 毫秒之间。

默认值为 1000 毫秒。

邻居请求消息（ICMPv6 类型 135）由尝试发现本地链路上其他节点的链路层地址的节点在本地链路上发送。在收到邻居请求消息后，目标节点通过在本地链路上发送邻居通告消息（ICPMv6 类型 136）作出应答。

源节点接收邻居通告后，源节点与目标节点即可通信。识别邻居的链路层地址后，邻居请求消息也用于验证邻居的可访问性。当节点要验证邻居的可访问性时，邻居请求消息中的目标地址是邻居的单播地址。

本地链路中一个节点的链路层地址发生变化时，也会发送邻居通告消息。

步骤 8 （可选） 在**可达时间**字段中，配置可达性确认事件发生后远程 IPv6 节点被视为可达的时长，介于 0 和 3600000 毫米之间。

默认值为 0 毫秒。当该值为 0 时，将发送未确定的可访问时间。由接收设备来设置和跟踪可访问时间的值。

邻居可访问时间可启用检测不可用邻居。配置时间越短，检测不可用邻居的速度就越快，但是，时间缩短却在所有 IPv6 网络设备中占用了更多的 IPv6 网络带宽和处理资源。在正常 IPv6 操作中不建议设置很短的配置时间。

步骤 9 （可选） 要禁用路由器通告传输，请取消选中**启用 RA** 复选框。如果启用路由器通告传输，则可以设置 RA 的有效期和间隔。

路由器通告消息（ICMPv6 类型 134）会自动发送，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。

在不希望 提供 IPv6 前缀的所有接口（例如，外部接口）上，您可能想要禁用这些消息。

- **RA 有效期** - 在 IPv6 路由器通告中配置路由器有效期的值，介于 0 和 9000 秒之间。

  默认值为 1800 秒。

- **RA 间隔** - 配置 IPv6 路由器通告传输之间的间隔，介于 3 和 1800 秒之间。

  默认值为 200 秒。

  为防止与其他 IPv6 节点同步，防火墙会随机调整您设置的值（抖动）。

步骤 10 点击**确定**。

步骤 11 点击**保存**。

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。

配置高级接口设置

本部分介绍如何为常规防火墙模式接口配置 MAC 地址，如何设置最大传输单元 (MTU) 以及如何设置其他高级参数。

关于高级接口配置

本节介绍高级接口设置。

关于 MAC 地址

您可以手动分配 MAC 地址以覆盖默认值。 对于容器实例，FXOS 机箱会自动为所有接口生成唯一 MAC 地址。

注释 您可能想要为 防火墙威胁防御 上定义的子接口分配唯一 MAC 地址，因为它们使用父接口上相同的固化 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 防火墙威胁防御 上特定实例内发生流量中断。

注释 对于容器实例，即使您未共享子接口，如果您手动配置 MAC 地址，请确保您为同一父接口上的所有子接口使用唯一 MAC 地址，从而确保分类得当。

默认 MAC 地址

对于本地实例：

默认 MAC 地址分配取决于接口类型。

- 物理接口 - 物理接口使用已刻录的 MAC 地址。
- VLAN 接口 (Firepower 1010 和 Cisco Secure Firewall 1210/1220) -路由防火墙模式： 所有 VLAN 接口均共享一个 MAC 地址。确保所有连接的交换机均可支持此方案。如果连接的交换机需要唯一 MAC 地址，可手动分配 MAC 地址。请参阅配置 MAC 地址，第 64 页。

  透明防火墙模式：各 VLAN 接口均有唯一的 MAC 地址。如有需要，您可通过手动分配 MAC 地址覆盖生成的 MAC 地址。请参阅配置 MAC 地址，第 64 页。
- EtherChannels（Firepower 型号） - 对于 EtherChannel，属于通道组的所有接口均共享同一 MAC 地址。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。端口通道接口使用来自池中的唯一 MAC 地址；接口成员身份不影响 MAC 地址。
- EtherChannel（ASA 型号）- 端口通道接口使用编号最小的通道组接口 MAC 地址作为端口通道 MAC 地址。或者，您可以为端口通道接口配置 MAC 地址。我们建议在组通道接口成员身份更改时，配置唯一的 MAC 地址。如果删除提供端口通道 MAC 地址的接口，则端口通道 MAC 地址会更改为下一个编号最小的接口，从而导致流量中断。
- 子接口（防火墙威胁防御 定义）- 物理接口的所有子接口都使用同一个烧录 MAC 地址。您可能想为子接口分配唯一的 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 防火墙威胁防御 上特定实例内发生流量中断。

对于容器实例：

- 所有接口的 MAC 地址均取自一个 MAC 地址池。对于子接口，如果决定要手动配置 MAC 地址，请确保将唯一 MAC 地址用于同一父接口上的所有子接口，从而确保分类正确。请参阅容器实例接口的自动 MAC 地址。

关于 MTU

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

对于 Geneve，帧中会封装整个以太网数据报，因此新的 IP 数据包更大，需要更大的 MTU：您应该将 ASA VTEP 源接口 MTU 设置为网络 MTU + 306 字节。

路径 MTU 发现

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

默认 MTU

防火墙威胁防御设备 上的默认 MTU 为 1500 字节。该值不包括 18-22 字节的以太网报头、VLAN 标记和其他开销。

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 TCP 数据包，终端通常使用它们的 MTU 来确定 TCP 最大报文段长度（例如，MTU-40）。如果之后添加额外的 TCP 报头，例如对于站点间的 VPN 隧道，则 TCP MSS 可能需要由隧道传输实体向下调整。请参阅关于 TCP MSS，第 61 页。

对于 UDP 或 ICMP，应用应将 MTU 考虑在内，以避免分段。

注释 只要有内存空间，防火墙威胁防御设备 就可接收大于所配置的 MTU 的帧。

MTU 和巨型帧

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

- 与流量路径上的 MTU 相匹配 - 我们建议将所有 防火墙威胁防御接口以及流量路径的其他设备接口上的 MTU 设为相同。匹配 MTU 可防止中间设备对数据包进行分片。
- 容纳巨型帧 - 在启用巨型帧时，MTU 可设置为 9000 字节或更高。最大值取决于型号。

关于 TCP MSS

TCP 最大报文段长度 (MSS) 是 TCP 负载在添加任何 TCP 和 IP 报头前的大小。UDP 数据包不会受到影响。建立连接时，客户端和服务器会在三次握手期间交换 TCP MSS 值。

您可以使用 FlexConfigFlexConfig 策略；默认情况下，最大 TCP MSS 设置为 1380 字节。当 防火墙威胁防御设备 需要增加数据包长度以执行 IPsec VPN 封装时，此设置非常有用。不过，对于非 IPsec 终端，应在 防火墙威胁防御设备 上禁用最大 TCP MSS。

如果设置了 TCP MSS 的最大值，当连接的任一终端请求的 TCP MSS 大于 防火墙威胁防御设备 中设定的值时，防火墙威胁防御设备 会使用 防火墙威胁防御设备 最大值覆盖请求数据包中的TCP MSS。如果主机或服务器没有请求 TCP MSS，防火墙威胁防御设备 会假定采用 RFC 793 的默认值 536 字节 (IPv4) 或 1220 字节 (IPv6)，但不会修改数据包。例如，可以将默认 MTU 保留为 1500 字节。如果主机请求的 MSS 为 1500 减去 TCP 和 IP 报头长度，这会将 MSS 设置为 1460。如果 防火墙威胁防御设备 上的最大TCP MSS 为 1380（默认值），防火墙威胁防御设备 会将 TCP 请求数据包中的MSS 值改为 1380。然后，服务器会发送 1380 字节负载的数据包。然后，防火墙威胁防御设备 可向数据包中增加最多 120 字节的报头，并且仍然符合 1500 的 MTU 大小。

您还可以配置最小 TCP MSS；如果主机或服务器请求一个非常小的 TCP MSS，则 防火墙威胁防御设备 可将该值调高。默认情况下，最小 TCP MSS 未启用。

对于流向设备的流量，包括用于 SSL VPN 连接的流量，此设置不适用。防火墙威胁防御设备 使用 MTU 来推导 TCP MSS：MTU - 40 (IPv4) 或 MTU - 60 (IPv6)。

默认 TCP MSS

默认情况下，防火墙威胁防御设备 上的最大 TCP MSS 是 1380 字节。此默认值符合 VPN 连接的要求（在 VPN 连接中，报头最多可达到 120 字节）；此值在默认 MTU（1500 字节）范围内。

建议的最大 TCP MSS 设置

默认 TCP MSS 假定 防火墙威胁防御设备作为 IPv4 IPsec VPN 终端，并且 MTU 为 1500。当 防火墙威胁防御设备用作 IPv4 IPsec VPN 终端时，它需要为 TCP 和 IP 报头容纳最多 120 个字节。

如果您要更改 MTU 值、使用 IPv6 或不将防火墙威胁防御设备设备用作 IPsec VPN 端点，则应更改 TCP MSS 设置使用 FlexConfig 中的 Sysopt_Basic 对象。

注释 即使您明确设置了 MSS，如果 TLS/SSL 解密或服务器发现等组件需要某个特定 MSS，它也会根据接口 MTU 设置该 MSS 并忽略您设置的 MSS。

请参阅以下准则：

- 正常流量 - 禁用 TCP MSS 限制，并接受在连接终端之间建立的值。由于连接终端一般是从 MTU 获得 TCP MSS，因此非 IPsec 数据包通常符合此 TCP MSS。
- IPv4 IPsec 终端流量 - 将最大 TCP MSS 设置为 MTU - 120。例如，如果使用巨帧并将 MTU 设置为 9000，则需要将 TCP MSS 设置为 8880，以利用新 MTU。
- IPv6 IPsec 终端流量 - 将最大 TCP MSS 设置为 MTU - 140。

网桥组流量的 ARP 检测

默认情况下，桥接组成员之间允许所有 ARP 数据包。可以通过启用 ARP 检测来控制 ARP 数据包的流量。

ARP 检测可防止恶意用户模拟其他主机或路由器（称为 ARP 欺骗）。ARP 欺骗能够启用“中间人”攻击。例如，主机向网关路由器发送 ARP 请求；网关路由器使用网关路由器 MAC 地址进行响应。但是，攻击者使用攻击者 MAC 地址（而不是路由器 MAC 地址）将其他 ARP 响应发送到主机。这样，攻击者即可在所有主机流量转发到路由器之前将其拦截。

ARP 检测确保只要静态 ARP 表中的 MAC 地址和相关 IP 地址正确，攻击者就无法利用攻击者 MAC 地址发送 ARP 响应。

当启用 ARP 检测查时，防火墙威胁防御设备 将所有 ARP 数据包中的 MAC 地址、IP 地址和源接口与 ARP 表中的静态条目进行比较，并执行下列操作：

- 如果 IP 地址、MAC 地址和源接口与 ARP 条目匹配，则数据包可以通过。
- 如果 MAC 地址、IP 地址或接口之间不匹配，则 防火墙威胁防御设备 会丢弃数据包。

- 如果 ARP 数据包与静态 ARP 表中的任何条目都不匹配，则可以将 防火墙威胁防御设备 设置为从所有接口向外转发数据包（泛洪），或者丢弃数据包。

注释 即使此参数设置为 flood，专用管理接口也绝不会以泛洪方式传输数据包。

MAC 地址表

当你使用网桥组时，防火墙威胁防御 以与一般网桥或交换机相似的方式获悉和构建 MAC 地址表：当某个设备通过网桥组发送数据包时，防火墙威胁防御 将在其表中添加 MAC 地址。此表将 MAC 地址与源接口相关联，以便防火墙威胁防御可了解如何将要发送到设备的任何数据包从正确的接口发出。由于网桥组成员之间的流量须遵守 防火墙威胁防御 安全策略，因此如果数据包的目标 MAC 地址不在此表中，则 防火墙威胁防御 不会像一般网桥那样以泛洪方式传输所有接口上的原始数据包。相反，它会为直连设备或远程设备生成以下数据包：

- 面向直连设备的数据包 - 防火墙威胁防御 将生成针对目标 IP 地址的 ARP 请求，以使它能了解哪个接口接收 ARP 响应。
- 面向远程设备的数据包 - 防火墙威胁防御将生成一个针对目标 IP 地址的 ping，以使它能了解哪个接口接收 ping 应答。

系统会丢弃原始数据包。

默认设置

- 如果启用 ARP 检测，则默认情况下会以泛洪方式传输不匹配的数据包。
- 动态 MAC 地址表条目的默认超时值为 5 分钟。
- 默认情况下，每个接口会自动获悉进入流量的 MAC 地址，并且 防火墙威胁防御设备 会将对应的条目添加到 MAC 地址表中。

注释 Cisco Secure Firewall Threat Defense 设备 生成重置数据包以重置状态检测引擎拒绝的连接。在这里，数据包的目标 MAC 地址不是根据 ARP 表查找确定的，而是直接从被拒绝的数据包（连接）中获取的。

ARP 检测和 MAC 地址表准则

- ARP 检测仅支持网桥组。
- MAC 地址表配置仅支持网桥组。

配置 MTU

自定义接口上的 MTU，以便实现允许巨型帧等目的。

对于 ISA 3000 和 Firewall Threat Defense Virtual：将 MTU 更改为 1500 字节以上会自动启用巨帧预留。您必须重新启动系统，然后才能使用巨帧。 对于支持集群的 Firewall Threat Defense Virtual，您可以在Day0配置中启用巨帧预留，因此在这种情况下无需重新启动。重新启动后，您将无法禁用巨帧预留。Firewall Threat Defense Virtual 的例外情况是，您可以在 Day0 配置中禁用巨帧预留（如果支持）。如果在内联集中使用接口，则不使用 MTU 设置。但是，巨帧预留设置与内联集相关；巨帧使内嵌接口能够接收多达 9000 字节的数据包。要启用巨帧预留，您必须将任何接口的 MTU 设置为 1500 字节以上。

默认情况下，其他平台上会启用巨帧。

⚠

注意 当部署配置更改时，为数据接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有数据接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于托管设备的型号和接口类型。此警告不适用于 仅管理接口。有关详细信息，请参阅Snort 重启流量行为。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 在 **常规** 选项卡上，设置 **MTU**。最小值和最大值取决于您的平台。

默认值为 1500 字节。

步骤 4 点击**确定**。

步骤 5 点击**保存**。

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。

步骤 6 对于 ISA 3000 和 Firewall Threat Defense Virtual，如果您将 MTU 设置为 1500 字节以上，则请重新启动系统以启用巨帧预留。请参阅关闭或重新启动设备。

配置 MAC 地址

可能需要手动分配 MAC 地址。您还可以通过从添加 **设备** > **设备管理** (**Add**) 下拉列表中选择 **高可用性** 来设置主用和备用 MAC 地址。如果您在两个屏幕中均设置某个接口的 MAC 地址，则**接口** > **高级**选项卡上的地址具有较高优先级。

注释 对于容器实例，即使您未共享子接口，如果您手动配置 MAC 地址，请确保您为同一父接口上的所有子接口使用唯一 MAC 地址，从而确保分类得当。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 点击**高级 (Advanced)** 选项卡。
将选择**信息 (Information)** 选项卡。

步骤 4 （对于单个接口模式下的集群）从下拉列表中选择 MAC 地址池。

您可以根据 地址池添加 MAC 地址池。

步骤 5 （对于其他模式）设置主用和备用 MAC 地址。

a) 在**主用 MAC 地址 (Active MAC Address)** 字段中，输入 H.H.H 格式的 MAC 地址，其中 H 表示 16 位的十六进制数字。

例如，MAC 地址 00-0C-F1-42-4C-DE 将需要输入 000C.F142.4CDE。不得为 MAC 地址设置组播位，即左起第二个十六进制数字不能是奇数。

b) 在**备用 MAC 地址 (Standby MAC Address)** 字段中，输入用于高可用性的 MAC 地址。

如果主用设备发生故障转移，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

步骤 6 点击**确定**。

步骤 7 点击**保存**。

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。

添加静态 ARP 条目

默认情况下，桥接组成员之间允许所有 ARP 数据包。可以通过启用 ARP 检测来控制 ARP 数据包的流量（请参阅ARP 检测）。ARP 检测会对比 ARP 数据包与 ARP 表中的静态 ARP 条目。

对于路由接口，可以输入静态 ARP 条目，但通常动态条目就足够了。对于路由接口，使用 ARP 表向直连主机交付数据包。虽然发件人可根据 IP 地址识别数据包目标，但在以太网上实际交付数据包依赖于以太网 MAC 地址。当路由器或主机希望在直连网络上交付数据包时，它会发送 ARP 请求来寻求与该 IP 地址关联的 MAC 地址，然后根据 ARP 响应将数据包交付到 MAC 地址。主机或路由器可保留 ARP 表，所以不必对需要交付的每个数据包都发送 ARP 请求。只要在网络上发送 ARP 响应，便会动态更新 ARP 表，但如果一段时间未使用条目，则它会超时。如果某个条目错误（例如给定 IP 地址的 MAC 地址改变），该条目需要超时后，才能为其更新新信息。

对于透明模式， 仅对进出 的流量（例如管理流量）使用 ARP 表中的动态 ARP 条目。

开始之前

此屏幕仅适用于指定的接口。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 设备的 **编辑** ()。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** ()。

步骤 3 点击**高级**选项卡，然后点击 **ARP** 选项卡（在透明模式下，称为 **ARP 和 MAC**）。

步骤 4 点击 ()**添加 ARP 配置**。
屏幕上随即会显示**添加 ARP 配置**对话框。

步骤 5 在 **IP 地址**字段中，输入主机的 IP 地址。

步骤 6 在 **MAC 地址**字段中，输入主机的 MAC 地址；例如，00e0.1e4e.3d8b。

步骤 7 要对该地址执行代理 ARP，请选中**启用别名**复选框。

如果 设备收到指定 IP 地址的 ARP 请求，则会使用指定 MAC 地址做出响应。

步骤 8 点击**确定**，然后再次点击**确定**退出“高级”设置。

步骤 9 点击**保存**。

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。

添加静态 MAC 地址并为网桥组禁用 MAC 学习

通常，当来自特定 MAC 地址的流量进入某个接口时，MAC 地址会动态添加到 MAC 地址表中。可以禁用 MAC 地址获悉；然而除非将 MAC 地址静态添加到表中，否则没有流量可以通过 设备。还可以向 MAC 地址表中添加静态 MAC 地址。添加静态条目的一个好处是，可以防止 MAC 欺骗。如果与静态条目具有相同 MAC 地址的客户端尝试向与静态条目不匹配的接口发送流量，则 设备会丢弃这些流量并生成系统消息。当添加静态 ARP 条目时（请参阅添加静态 ARP 条目， 第 65 页），静态 MAC 地址条目会自动添加到 MAC 地址表中。

开始之前

此屏幕仅适用于透明模式下的命名 BVI。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 设备的 **编辑** ()。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** ()。

步骤 3 点击**高级 (Advanced)**选项卡，然后点击 **ARP 和 MAC (ARP and MAC)** 选项卡。

步骤 4 （可选） 通过取消选中**启用 MAC 学习**复选框来禁用 MAC 学习。

步骤 5 要添加静态 MAC 地址，请点击**添加 MAC 配置 (Add MAC Config)**。
此时将显示**添加 MAC 配置**对话框。

步骤 6 在 **MAC 地址 (MAC Address)** 字段中，输入主机的 MAC 地址；例如，00e0.1e4e.3d8b。点击**确定**。

步骤 7 点击**确定 (OK)** 以退出高级设置。

步骤 8 点击**保存**。

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。

设置安全配置参数

本部分介绍如何防止IP欺骗、允许完整分段重组以及覆盖在**平台设置**中的设备级别设置的默认分段设置。

反欺骗

本部分使您可以在接口上启用单播反向路径转发。单播 RPF 根据路由表来确保所有数据包均有与正确的源接口匹配的源 IP 地址，从而避免 IP 欺骗（即数据包使用不正确的源 IP 地址以掩盖其真正来源）。

通常情况下， 设备在确定向何处转发数据包时只查看目标地址。单播 RPF 会指示设备还查找源地址；其因此被称为“反向路径转发”。对于您要允许通过 设备的任何流量，设备路由表必须包括回到源地址的路由。有关详细信息，请参阅 RFC 2267。

例如，对于外部流量， 设备可使用默认路由来满足单播RPF保护。如果流量从外部接口进入，则路由表不知道源地址，而设备使用默认路由将外部接口正确识别为源接口。

如果流量从路由表中包含的已知地址进入外部接口，但与内部接口关联，则 设备会丢弃该数据包。同样，如果流量从未知源地址进入内部接口，则设备会丢弃数据包，因为匹配的路由（默认路由）指示外部接口。

单播 RPF 的实施过程如下：

- ICMP 数据包没有会话，因此要检查每个数据包。
- UDP和TCP有会话，因此初始数据包要求反向路由查找。对于在会话期间到达的后续数据包，使用作为部分会话来维护的现有状态进行检查。系统会检查非初始数据包，以确保它们到达初始数据包使用的同一接口。

每个数据包的分段数

默认情况下，设备允许每个 IP 数据包最多包含 24 个分段，以及最多 200 个等待重组的分段。如果您有定期对数据包进行分段的应用（如 NFS over UDP），可能需要让分段位于您的网络上。但是，如果没有对流量分段的应用，则我们建议您不要允许分段通过 设备。分段的数据包通常用作 DoS 攻击。

分段重组

设备执行以下分段重组过程：

- 系统会收集 IP 分段，直到形成分段集或达到超时间隔。
- 如果分段集形成，则对片段集执行完整性检查。这些检查包括无重叠、无尾部溢出和无链溢出。
- 在 设备处终止的 IP 分段始终会完全重组。
- 如果禁用了**完全分段重组**（默认设置），则分段集会转发到传输层以进一步处理。
- 如果启用了**完全分段重组**，则分段集首先会合并为单个 IP 数据包。然后，该单个 IP 数据包被转发到传输层，以供进一步处理。

开始之前

此屏幕仅适用于指定的接口。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 点击**高级**选项卡，然后点击**安全配置**选项卡。

步骤 4 要启用单播反向路径转发，请选中 **启用反欺骗** 复选框。

步骤 5 要启用完整分段重组，请选中 **允许完整分段重组** 复选框。

步骤 6 要更改每个数据包所允许的分段数，请选中**覆盖默认分段设置**复选框，并设置以下值：

- **大小** - 设置 IP 重组数据库中等待重组的最大数据包数。默认值为 200。将该值设置为 1 会禁用分段。
- **链** - 设置完整 IP 数据包可分成的最大数据包数。默认值为 24 个数据包。
- **超时** - 设置等待整个分段数据包到达的最大秒数。在数据包的第一个分段到达后计时器启动。如果在指定秒数后数据包的分段没有全部抵达，则已收到的数据包的所有分段将被丢弃。默认值为 5 秒。

步骤 7 点击**确定**。

步骤 8 点击**保存**。

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。

常规防火墙接口的历史记录

功能	防火墙管理中心最低版本	最低版本	详细信息
Cisco Secure Firewall 1210CP IEEE 802.3bt 支持（PoE++ 和 Hi-PoE）	7.7.0	7.7.0	请参阅以下与 IEEE 802.3bt 支持相关的改进： • PoE++ 和 Hi-PoE - 每个端口最高 90W。 • 单签名和双签名受电设备 (PD)。 • 电源预算遵循先到先得的原则。 • 功率预算字段已被添加到 **show power inline**。 新增/修改的屏幕：**设备** > **设备管理** > **接口** > **编辑物理接口** > **PoE** 新增/修改的命令：**show power inline**
Cisco Secure Firewall 通过 GWLB 支持 AWS 上的双臂部署模式	7.6	7.6	Cisco Secure Firewall 支持在 AWS 上使用 GWLB 的双臂部署模式。此模式可使防火墙在进行流量检查后，通过互联网网关直接将互联网流量转发到互联网，同时还可执行网络地址转换 (NAT)。
Cisco Secure Firewall 1210/1220 硬件交换机支持	7.6	7.6	Cisco Secure Firewall 1210/1220 支持将各以太网接口设置为交换机端口或防火墙接口
以太网端口 1/5-1/8 上的 Cisco Secure Firewall 1210CP PoE+ 支持	7.6	7.6	Cisco Secure Firewall 1210CP 在以太网端口 1/5-1/8 上支持以太网供电+ (PoE+)。
VXLAN VTEP IPv6 支持	7.4	任意	现在，您可以为 VXLAN VTEP 接口指定 IPv6 地址。Threat Defense Virtual 集群控制链路或 Geneve 封装不支持 IPv6。 新增/修改的屏幕： • **设备** > **设备管理** > **编辑** > **VTEP** > **添加 VTEP** **设备** > **设备管理** > **编辑** > **接口** > **添加接口** > **VNI 接口** 需要 7.4 版本。

功能	防火墙管理中心最低版本	最低版本	详细信息
环回接口支持 BGP 和管理流量	7.4	任意	您可以将环回接口用于： • AAA • BGP • DNS • HTTP • ICMP • IPsec 流分流 • NetFlow • SNMP • SSH • 系统日志 需要 7.4 版本。
VTI 的环回接口支持。	7.3	任意	您现在可以添加环回接口。环回接口有助于克服路径故障。如果接口发生故障，您可以通过分配给环回接口的 IP 地址来访问所有接口。对于 VTI，除了将环回接口设置为源接口外，还添加了支持以从环回接口继承 IP 地址，而不是静态配置的 IP 地址。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **添加接口 (Add Interfaces)** > **添加环回接口 (Add Loopback Interface)**

功能	防火墙管理中心最低版本	最低版本	详细信息
IPv6 DHCP	7.3	任意	现在支持 IPv6 寻址的以下功能： • DHCPv6 地址客户端 - 从 DHCPv6 服务器获取 IPv6 全局地址和可选默认路由。 • DHCPv6 前缀代理客户端 - 从 DHCPv6 服务器获取指定的前缀。然后， 可以使用这些前缀来配置其他 接口地址，以便无状态地址自动配置 (SLAAC) 客户端可以自动配置同一网络上的 IPv6 地址。 • BGP 路由器通告指定的前缀 • DHCPv6 无状态服务器 - 当 SLAAC 客户端向 发送信息请求 (IR) 数据包时， 会向它们提供域名等其他信息。 仅接受 IR 数据包，不向客户端分配地址。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **添加/编辑接口 (Add/Edit Interfaces)** > **IPv6** > **DHCP** • **对象 (Objects)** > **对象管理 (Object Management)** > **DHCP IPv6 池 (DHCP IPv6 Pool)** 新增/修改的命令：**show bgp ipv6 unicast, show ipv6 dhcp, show ipv6 general-prefix**
Firewall Threat Defense Virtual 用于 Azure 网关负载均衡器的已配对代理 VXLAN	7.3	任意	您可以为 Azure 中的 Firewall Threat Defense Virtual 配置配对代理模式 VXLAN 接口，以便与 Azure 网关负载均衡器 (GWLB) 配合使用。 Firewall Threat Defense Virtual 通过已配对代理中的 VXLAN 网段在单个 NIC 上定义外部接口和内部接口。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **接口 (Interfaces)** > **添加接口 (Add Interfaces)** > **VNI 接口 (VNI Interface)** 支持的平台：Azure 中的 Firewall Threat Defense Virtual

功能	防火墙管理中心最低版本	最低版本	详细信息
VXLAN 支持	7.2	任意	添加了 VXLAN 封装支持。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **VTEP** • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **接口 (Interfaces)** > **添加接口 (Add Interfaces)** > **VNI 接口 (VNI Interface)** • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **接口 (Interfaces)** 编辑物理接口 > **General** 支持的平台：全部
Geneve 支持 Firewall Threat Defense Virtual	7.1	任意	为 Firewall Threat Defense Virtual 增加了 Geneve 封装支持，以支持 Amazon Web 服务 (AWS) 网关负载均衡器的单臂代理。AWS 网关负载均衡器将透明网络网关（所有流量都有一个入口和出口点）与负载均衡器相结合，该负载均衡器可分配流量并扩展 Firewall Threat Defense Virtual 以匹配流量需求。 此功能需要使用 Snort 3。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **VTEP** • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **接口 (Interfaces)** > **添加接口 (Add Interfaces)** > **VNI 接口 (VNI Interface)** • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **接口 (Interfaces)** 编辑物理接口 > **General** 支持的平台：AWS 中的 Firewall Threat Defense Virtual

功能	防火墙管理中心最低版本	最低版本	详细信息
31 位子网掩码	7.0	任意	对于路由接口，您可以在 31 位子网上为点对点连接配置 IP 地址。31 位子网只包含 2 个地址；通常，该子网中的第一个和最后一个地址预留用于网络和广播，因此，不可使用包含 2 个地址的子网。但是，如果您有点对点连接，并且不需要网络或广播地址，则 31 位子网是在 IPv4 中保留地址的有用方式。例如，2 个 FTD 之间的故障转移链路只需要 2 个地址；该链路一端传输的任何数据包始终由另一端接收，无需广播。您还可以拥有运行 SNMP 或系统日志的一个直连管理站。网桥组或组播路由的 BVI 不支持此功能。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)**
Firepower 4100/9300 的运行链路状态与物理链路状态之间的同步	6.7	任意	Firepower 4100/9300 机箱现在可以将 运行链路状态与数据接口的物理链路状态同步。目前，只要 FXOS 管理状态为“运行”且物理链路状态为“运行”，接口将处于“运行”状态，而不考虑 应用接口管理状态。如果没有从 同步，数据接口可能在 应用完全上线之前处于“Up”物理状态，或者在您启动 关闭后的一段时间内保持 “Up” 状态。对于内联集，此状态不匹配可能会导致数据包丢失，因为外部路由器可能会在可以处理流量之前开始向 发送流量。该功能默认为禁用状态并可在 FXOS 中按逻辑设备逐一启用。 **注释** 集群、容器实例或具有 Radware vDP 修饰器的 不支持此功能。ASA 也不支持此功能。 新增/修改的 Firepower 机箱管理器屏幕：**逻辑设备** > **启用链路状态** 新增/修改的 FXOS 命令：**set link-state-sync enabled**、**show interface expand detail** 支持的平台：Firepower 4100/9300
Firepower 1010 硬件交换机支持	6.5	任意	Firepower 1010 支持将各以太网接口设置为交换机端口或防火墙接口。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** • **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** • **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **添加 VLAN 接口 (Add VLAN Interface)**

功能	防火墙管理中心最低版本	最低版本	详细信息
Firepower 1010 PoE + 支持以太网 1/7 和以太网 1/8	6.5	任意	在被配置为交换机端口时，Firepower 1010 支持以太网接口 1/7 和 1/8 上的增强型以太网供电+ (PoE+)。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** > **PoE**
用于容器实例的VLAN子接口	6.3.0	任意	要确保灵活使用物理接口，可以在FXOS中创建VLAN子接口，还可以在多个实例之间共享接口。 新增/修改的 Cisco Secure Firewall Management Center菜单项： **设备** > **设备管理** > **编辑** 图标 > **接口** 选项卡 新增/修改的 Cisco Secure Firewall 机箱管理器菜单项： **接口** > **所有接口** > **新增**下拉菜单**子接口** 新增/修改的FXOS 命令：**create subinterface**、**set vlan**、**show interface**、**show subinterface** 支持的平台：Firepower 4100/9300
用于容器实例的数据共享接口	6.3.0	任意	要确保灵活使用物理接口，可以在多个实例之间共享接口。 新增/修改的 Cisco Secure Firewall 机箱管理器菜单项： **接口** > **所有接口** > **类型** 新增/修改的 FXOS 命令：**set port-type data-sharing**、**show interface** 支持的平台：Firepower 4100/9300

功能	防火墙管理中心最低版本	最低版本	详细信息
集成路由和桥接	6.2.0	任意	集成路由和桥接提供了在网桥组和路由接口之间路由的功能。网桥组是指 网桥（而非路由）的接口组。 并非真正的网桥，因为 仍将继续充当防火墙：接口之间实施访问控制，并且部署所有常用防火墙检查。以前，您只能在透明防火墙模式下配置网桥组，而无法在网桥组之间路由。通过此功能，可以在路由防火墙模式下配置网桥组，并在网桥组之间以及网桥组与路由接口之间进行路由。网桥组使用网桥虚拟接口(BVI)作为网桥组的网关，由此参与路由。如果 上还有额外接口可分配给网桥组，集成路由和桥接可提供替代使用外部第 2 层交换机的其他方案。在路由模式下，BVI 可以是已命名接口，并可独立于成员接口参与某些功能，例如访问规则和 DHCP 服务器。 以下功能在透明模式下受支持，但在路由模式下不受支持：集群。以下功能在 BVI 上也不受支持：动态路由和组播路由。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** • **设备** > **设备管理** > **接口** > **添加接口** > **网桥组接口** 支持的平台：Firepower 2100 和 Firewall Threat Defense Virtual 以外的所有平台

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。