

透明或路由防火墙模式

本章介绍如何将防火墙模式设置为路由或透明模式，以及防火墙在各种防火墙模式下的工作方式。

注释 防火墙模式只影响常规的防火墙接口，而不影响仅 IPS 接口，如内联集或被动接口。仅 IPS 接口可以在两种防火墙模式下使用。有关仅 IPS 接口的详细信息，请参阅内联集和被动接口。内嵌集可能是您所熟悉的“透明内联集”，但内联接口类型与本章介绍的透明防火墙模式或防火墙类型接口无关。

- 关于防火墙模式， 第 1 页
- 默认设置， 第 9 页
- 防火墙模式指南， 第 9 页
- 设置防火墙模式， 第 10 页

关于防火墙模式

威胁防御面向普通防火墙接口支持两种防火墙模式：路由防火墙模式和透明防火墙模式。

关于路由防火墙模式

在路由模式中，威胁防御设备被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。

通过集成路由和桥接，您可以使用您用来对网络的多个接口进行分组的“网桥组”，威胁防御设备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。威胁防御设备在 BVI 与正规的路由接口之间进行路由。如果您不需要集群或 EtherChannel 成员接口，则可以考虑使用路由模式而非透明模式。在路由模式下，可以像在透明模式下一样具有一个或多个隔离的网桥组，但也可以使用正常的路由接口进行混合部署。

关于透明防火墙模式

通常情况下，防火墙是一个路由跃点，并充当与其中一个被屏蔽子网连接的主机的默认网关。另一方面，透明防火墙是一个第 2 层防火墙，充当“线缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。但是，与其他防火墙一样，接口之间的访问控制是受控制的，需要进行通常的所有防火墙检查。

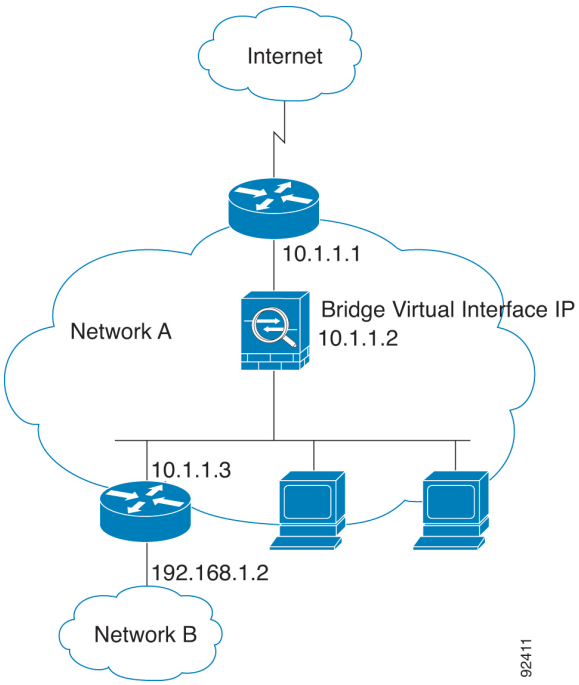
第 2 层连接使用您用来对网络的内部和外部接口进行分组的“网桥组”来实现，威胁防御设备使用桥接技术在接口之间传递流量。每个桥接组包括一个网桥虚拟接口 (BVI)，供您为其分配一个网络 IP 地址。多个网络可以有多个网桥组。在透明模式下，这些网桥组无法相互通信。

在网络中使用透明防火墙

威胁防御设备 在其接口之间连接同一个网络。由于防火墙不是路由跃点，因此可以将透明防火墙轻松引入到现有网络中。

下图显示典型的透明防火墙网络，其中的外部设备与内部设备在同一个子网上。内部路由器和主机显示为与外部路由器直接连接。

图 *1:* 透明防火墙网络



允许路由模式功能通过流量

对于透明防火墙不直接支持的功能，您可以允许流量通过，以便上游和下游路由器能够支持这些功能。例如，通过使用访问规则，可以允许 DHCP 流量（而不是不受支持的 DHCP 中继功能）或组播流量（例如 IP/TV 产生的流量）。还可以通过透明防火墙建立路由协议邻接；可以根据扩访问规则允许 OSPF、RIP、EIGRP 或 BGP 流量通过。同样，诸如 HSRP 或 VRRP 之类的协议也可以通过 威胁防御设备。

关于网桥组

网桥组是指 威胁防御设备 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。与任何其他防火墙接口一样，接口之间的访问控制将受控制，并将部署所有普通防火墙检查。

网桥虚拟接口 (BVI)

每个网桥组包括一个网桥虚拟接口 (BVI)。威胁防御设备使用该 BVI IP 地址作为源自网桥组的数据包的源地址。BVI IP 地址必须与网桥组成员接口位于同一子网。BVI 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。

在透明模式下：只有网桥组成员接口会被命名并可以与基于接口的功能配合使用。

在路由模式下：BVI 充当网桥组和其他路由接口之间的网关。要在网桥组/路由接口之间进行路由，必须为 BVI 命名。对于一些基于接口的功能，您可以单独使用 BVI：

- DHCPv4 服务器 - 只有 BVI 支持 DHCPv4 服务器配置。
- 静态路由 - 可以为 BVI 配置静态路由；不能为成员接口配置静态路由。
- 系统日志服务器和其他源自 威胁防御设备的流量 - 当指定系统日志服务器（或 SNMP 服务器，或流量源自 威胁防御设备的其他服务）时，可以指定 BVI 或成员接口。

如果您在路由模式下没有命名 BVI，则 威胁防御设备不会路由网桥组流量。此配置将为网桥组复制透明防火墙模式。如果您不需要集群或 EtherChannel 成员接口，则可以考虑改用路由模式。在路由模式下，可以像在透明模式下一样具有一个或多个隔离的网桥组，但也可以使用正常的路由接口进行混合部署。

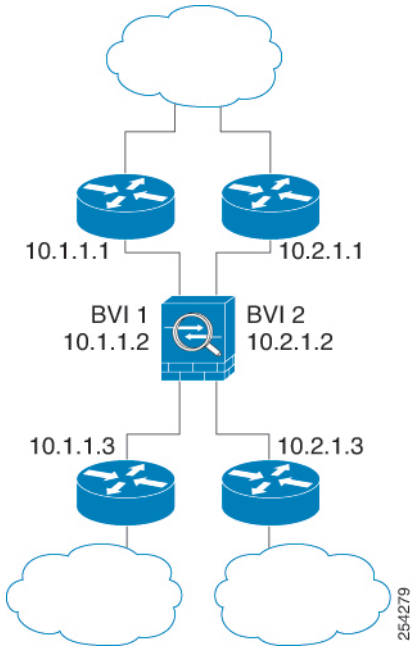
透明防火墙模式下的网桥组

网桥组的流量相互分离；流量不会路由至 威胁防御设备 中的另一个网桥组，并且流量必须退出 威胁防御设备 后才能通过外部路由器路由回 威胁防御设备 中的另一个网桥组。虽然每个网桥组的桥接功能是独立的，但所有网桥组之间可共享很多其他功能。例如，所有网桥组都共享系统日志服务器或 AAA 服务器的配置。

可以在每个网桥组中包含多个接口。有关支持的网桥组和接口的确切数量，请参阅防火墙模式指南，第 9 页。如果您在每个网桥组中使用的接口数超过 2 个，则可以控制同一网络上多个网段之间的通信，而不只是在内部和外部之间的通信。例如，如果您有三个不需要彼此通信的内部网段，则可以将每个网段设置在单独的接口上，并且仅允许它们与外部接口通信。或者，您可以自定义接口之间的访问规则，以根据需要允许任意程度的访问。

下图显示连接到 威胁防御设备且具有两个网桥组的两个网络。

图 *2:* 具有两个网桥组的透明防火墙网络

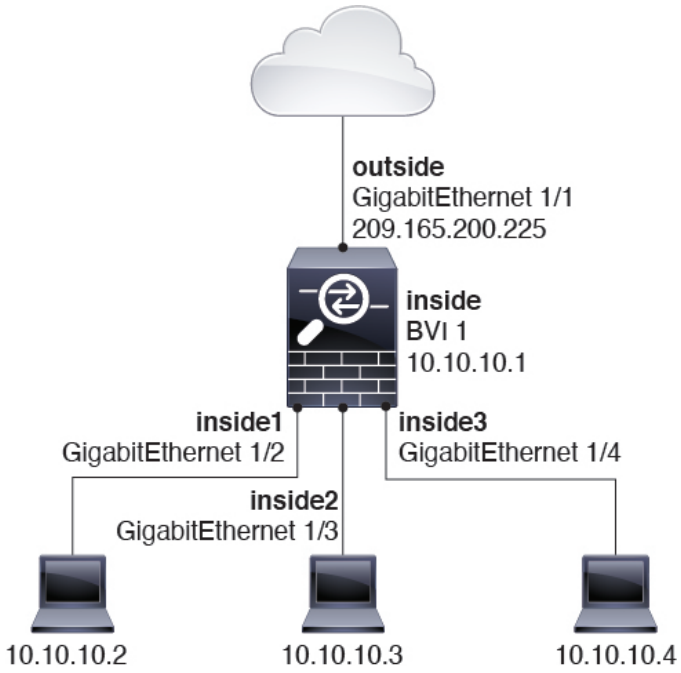


路由防火墙模式下的网桥组

网桥组流量可以路由到其他网桥组或路由接口。您可以选择通过不为网桥组的 BVI 接口分配名称来隔离网桥组流量。如果命名了 BVI，则 BVI 将像其他任何普通接口一样参与路由。

路由模式下网桥组的一种用途是在 威胁防御上而非外部交换机上使用额外接口。例如，某些设备的默认配置包括一个外部接口作为普通接口，还包括分配给内部网桥组的其他接口。由于此网桥组的目的是替换外部交换机，因此您需要配置访问策略，以便所有网桥组接口都可以自由通信。

图 *3:* 具有内部网桥组和外部路由接口的路由防火墙网络



允许第 3 层流量

- 单播 IPv4 和 IPv6 流量需要允许一个访问规则通过网桥组。
- 允许 ARP 双向通过网桥组，而无需访问规则。ARP 流量可通过 ARP 检测进行控制。
- IPv6 邻居发现和路由器请求数据包可以使用访问规则传递。
- 可使用访问规则允许广播和组播流量通过。

允许的 MAC 地址

如果得到您的访问策略的允许，将允许以下目标 MAC 地址通过网桥组（请参阅允许第 3 层流量，第 5 页）。系统会丢弃此列表中未列出的任何 MAC 地址。

- 实际广播目标 MAC 地址等于 FFFF.FFFF.FFFF
- IPv4 组播 MAC 地址的范围是 0100.5E00.0000 至 0100.5EFE.FFFF
- IPv6 组播 MAC 地址的范围是 3333.0000.0000 至 3333.FFFF.FFFF
- BPDU 组播地址等于 0100.0CCC.CCCD

BPDU 处理

为防止环路使用生成树协议，默认情况下允许 BPDU 通过。

默认情况下，BPDU 也会被转发以进行高级检测，这对此类型数据包并无必要，并且有可能导致例如由于检测重启而被阻止的问题发生。我们建议您始终免除对 BPDU 进行高级检测。为此，请使用 FlexConfig 配置信任 BPDU 的 EtherType ACL，并在每个成员接口上免除对其进行高级检测。请参阅 #unique_138。

FlexConfig 对象应部署以下命令，在其中将 <if-name> 替换为接口名称。添加所需数量的 access-group 命令以涵盖设备上的每个网桥组成员接口。您还可以为 ACL 选择其他名称。

```
access-list permit-bpdu ethertype trust bpdu
access-group permit-bpdu in interface <if-name>
```

MAC 地址与路由查找

对于网桥组中的流量，通过执行目标 MAC 地址查找而不是路由查找来确定数据包的传出接口。

但是，路由查找对于以下情况是必要的：

- 源自 威胁防御设备的流量 - 例如，在 威胁防御设备上为发往系统日志服务器所在的远程网络的流量添加一个默认/静态路由。
- IP 语音 (VoIP) 和 TFTP 流量，并且终端至少在一跳之外 - 在 威胁防御设备上为发往成功建立辅助连接的远程终端的流量添加静态路由。威胁防御设备会在访问控制策略中创建一个临时“针孔”以允许辅助连接；由于连接可能会使用一组不同于主连接的 IP 地址，所以 威胁防御设备需要执行路由查找以便在正确的接口上安装针孔。

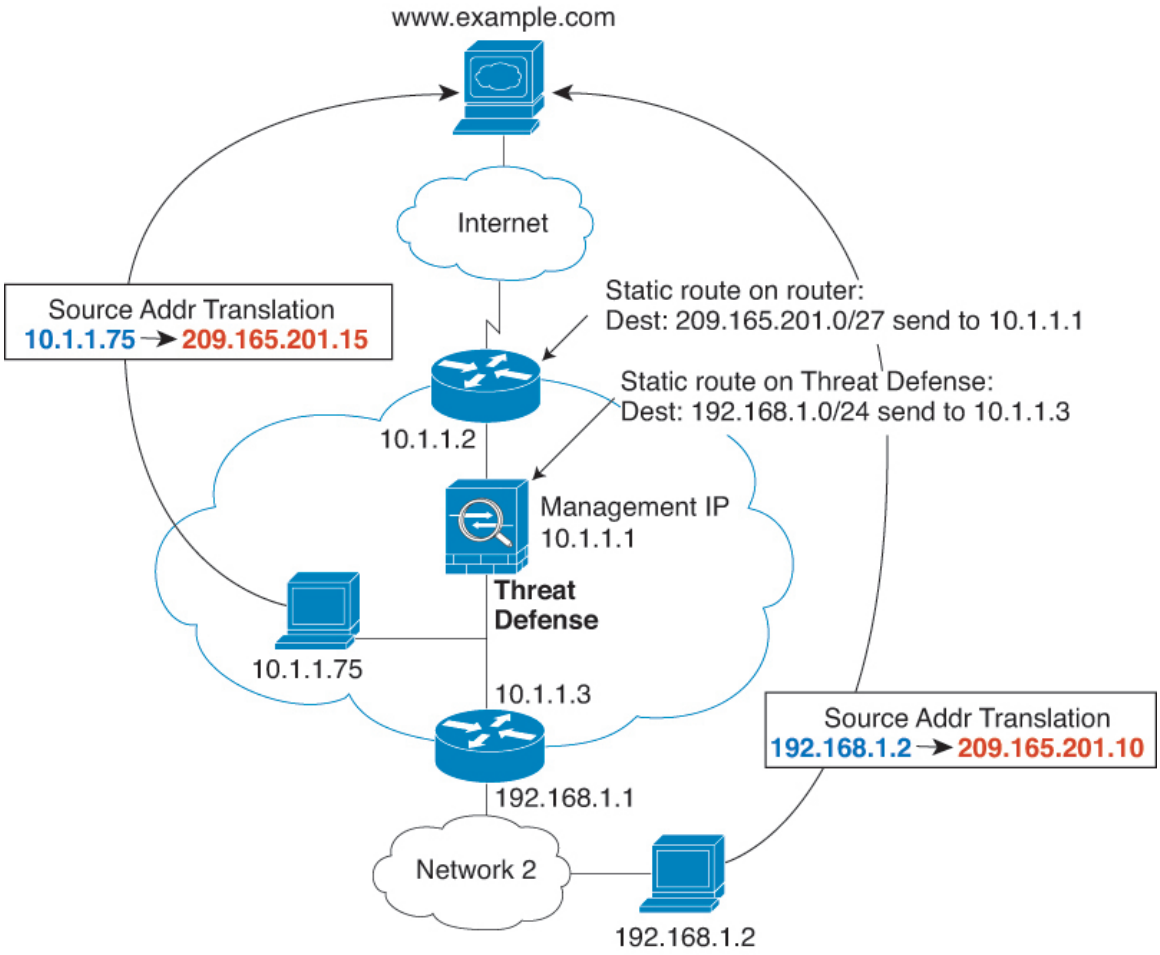
  受影响的应用包括：

  - H.323
  - RTSP
  - SIP
  - Skinny (SCCP)
  - SQL*Net
  - SunRPC
  - TFTP

- 威胁防御设备对其执行 NAT 的至少一跳开外的流量 - 在 威胁防御设备上为发往远程网络的流量配置静态路由。您还需要在上游路由器上为要发送到 威胁防御设备的已映射地址的流量配置静态路由。

  此路由要求也适用 NAT 的 VoIP 和 DNS 的嵌入式 IP 地址，这些嵌入式 IP 地址都必须至少在一跳之外。威胁防御设备需要识别正确的出口接口，以便可以执行转换。

图 *4: NAT* 示例：网桥组中的 *NAT*



透明模式下网桥组不支持的功能

下表列出了在透明模式下网桥组中不受支持的功能。

表 *1:* 在透明模式下不支持的功能

特性	说明
动态 DNS	-
DHCP 中继	透明防火墙可作为 DHCPv4 服务器，但它不支持 DHCP 中继。不需要使用 DHCP 中继，因为可使用两个访问规则来允许 DHCP 流量通过：一个规则用于允许从内部接口向外部发送 DCHP 请求；另一个用于允许来自另一个方向的服务器的应答。

特性	说明
动态路由协议	但是，对于网桥组成员接口，可以为 威胁防御设备上发起的流量添加静态路由。您还可以使用访问规则来允许动态路由协议通过 威胁防御设备。
组播 IP 路由	通过在访问规则中允许组播流量，可以允许组播流量通过 威胁防御设备。
QoS	-
针对直通流量终止 VPN	透明防火墙仅支持在网桥组成员接口上使用站点间的VPN隧道传输管理连接。它不会针对通过 威胁防御设备 的流量终止 VPN 连接。您可以使用访问规则允许 VPN 流量通过 ASA，但它不会终止非管理连接。

路由模式下网桥组不支持的功能

下表列出了在路由模式下网桥组中不支持的功能。

表 *2:* 路由模式下不受支持的功能

特性	说明
EtherChannel 成员接口	仅支持物理接口、冗余接口和子接口作为网桥组成员接口。 诊断 接口也不受支持。
集群	集群中不支持网桥组。
动态 DNS	-
DHCP 中继	路由防火墙可以作为 DHCPv4 服务器，但它不支持在 BVI 或网桥组成员接口上使用 DHCP 中继。
动态路由协议	但您可以为 BVI 添加静态路由。您还可以使用访问规则来允许动态路由协议通过 威胁防御设备。非网桥组接口支持动态路由。
组播 IP 路由	通过在访问规则中允许组播流量，可以允许组播流量通过 威胁防御设备。非网桥组接口支持组播路由。
QoS	非网桥组接口支持 QoS。
针对直通流量终止 VPN	您无法终止 BVI 上的 VPN 连接。非网桥组接口支持 VPN。 网桥组成员接口仅支持将站点间VPN隧道用于管理连接。它不会针对通过 威胁防御设备 的流量终止 VPN 连接。您可以使用访问规则通过网桥组传递 VPN 流量，但它不会终止非管理连接。

默认设置

网桥组默认设置

默认情况下，所有 ARP 数据包都在网桥组内通过。

防火墙模式指南

桥接组指南（透明和路由模式）

- 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。
- 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 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 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 2100 系列，在路由模式下不支持网桥组。
- 对于 Firepower 1010，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 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。
- 在透明模式下，诊断接口不支持 PPPoE。

- Amazon Web 服务、Microsoft Azure、Google Cloud Platform 和 Oracle Cloud Infrastructure 上部署的威胁防御虚拟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，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 威胁防御。如果 威胁防御 的一端有两个邻居运行 BFD，则 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。

设置防火墙模式

智能许可证	经典许可证	支持的设备	支持的域	访问权限
任意	不适用	威胁防御	任意	管理员 访问管理员 网络管理员

在 CLI 中执行初始系统设置时，可以设置防火墙模式。我们建议在安装过程中设置防火墙模式，因为更改防火墙模式会清除您的配置，以确保不存在不兼容的设置。如果以后需要更改防火墙模式，则必须从 CLI 中执行此操作。

过程

步骤 1 从管理中心注销 威胁防御设备。

撤销设备之前，不能更改防火墙模式。

a) 选择**设备** > **设备管理**。
b) 从受管设备列表中选择设备。
c) 删除设备（点击垃圾桶），确认并等待系统删除设备。

步骤 2 访问 威胁防御设备 CLI，首选使用控制台端口。

如果您使用 SSH 连接到诊断接口，则更改模式会清除您的接口配置，并断开连接。此时，您应改为连接到管理接口。

步骤 3 更改防火墙模式：

configure firewall [**routed** | **transparent**]

示例：

```
> configure firewall transparent
This will destroy the current interface configurations, are you sure that you want to
proceed? [y/N] y
The firewall mode was changed successfully.
```

步骤 4 向 管理中心重新注册：

configure manager add {*hostname* | *ip_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

其中：

- {*hostname* | *ip_address* | **DONTRESOLVE** }指定 管理中心 的完全限定主机名或 IP 地址。如果 管理中心不是直接可寻址的，请使用 **DONTRESOLVE**。
- *reg_key* 是向 管理中心 注册设备所需的唯一字母数字注册密钥。
- *nat_id* 是在 管理中心与设备之间的注册流程中使用的可选字母数字字符串。如果主机名设置为 **DONTRESOLVE**，此项为必填项。

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。