组播

本章介绍如何将 Secure Firewall Threat Defense配置为使用组播路由协议。对于使用虚拟路由的设备，只能为其全局虚拟路由器配置组播，不能为其用户定义的虚拟路由器配置组播。

关于组播路由

组播路由是一种带宽节省技术，通过同时向数千个公司收件人和家庭传送单一信息流来减少流量。使用组播路由的应用包括视频会议、公司通信、远程教育以及软件、股票报价和新闻的分发。

组播路由协议将源流量传递给多个接收者，而不会对源或接收者造成任何额外负担，而且是同类技术当中占用网络带宽最少的。组播数据包通过启用了协议无关组播 (PIM) 及其他支持性组播协议的威胁防御设备 在网络中复制，是目前为止向多个接收者传输数据的最高效方式。

威胁防御设备 支持末节组播路由和 PIM 组播路由。但是，不能在一个 威胁防御设备 上都配置这两种路由。

注释 组播路由同时支持 UDP 和非 UDP 传输。但是，非 UDP 传输没有进行快速路径优化。

IGMP 协议

IP 主机使用互联网组管理协议 (IGMP) 将其组成员身份报告给直连组播路由器。IGMP 用于在特定 LAN 上的一个组播组中动态注册单个主机。主机通过向其本地组播路由器发送 IGMP 消息来识别组

成员身份。在 IGMP 下，路由器监听 IGMP 消息，并定期发出查询以发现特定子网上处于活动状态或非活动状态的组。

IGMP 将组地址（D 类 IP 地址）用作组标识符。主机组地址的范围可以是 224.0.0.0 到 239.255.255.255。地址 224.0.0.0 不分配给任何组。地址 224.0.0.1 分配给子网上的所有系统。地址 224.0.0.2 分配给子网上的所有路由器。

注释 如果在 威胁防御设备上启用组播路由，IGMP V2 将会在所有接口上自动启用。

发送到组播组的查询消息

威胁防御设备发送查询消息，以发现哪些组播组有成员位于与接口连接的网络上。成员以IGMP报告消息作出响应，以表明自己想要接收特定组的组播数据包。查询消息会发送到全系统组播组，该组的地址为 224.0.0.1，生存时间值为 1。

这些消息会定期发送，从而刷新威胁防御设备上存储的成员身份信息。如果威胁防御设备发现组播组中没有本地成员仍与接口相连接，它会停止向连接的网络转发该组的组播数据包，并会向数据包源发送回删除消息。

默认情况下，子网上的 PIM 指定路由器负责发送查询消息。默认情况下，每 125 秒发送一次消息。

默认情况下，更改查询响应时间时，IGMP 查询中通告的最大查询响应时间为 10 秒。如果 威胁防御设备不在此时间内接收对主机查询的响应，它就会删除该组。

末节组播路由

末节组播路由提供动态主机注册并促进组播路由。如果针对末节组播路由进行了配置，威胁防御设备 将用作 IGMP 受托代理。威胁防御设备 将 IGMP 消息转发到上游组播路由器（上游组播路由器设置组播数据的传输），而不是完全参加组播路由。威胁防御设备 在为末节组播路由而配置后，就不能为 PIM 稀疏模式或双向模式而配置。您必须在参与 IGMP 末节组播路由的接口上启用 PIM。

威胁防御设备 同时支持 PIM-SM 和双向 PIM。PIM-SM 是一个组播路由协议，它使用基础单播路由信息库或支持组播的独立路由信息库。该协议会按组播组构建以单个交汇点 (RP) 为根的单向共享树，并且可以选择性地按组播源创建最短路径数。

PIM 组播路由

双向 PIM 是 PIM-SM 的一个变体，用于构建连接组播源和接收器的双向共享树。双向树使用每个组播拓扑链路上运行的专用转发器 (DF) 选择流程构建借助 DF，组播数据从源转发至交汇点 (RP)，然后联通共享树一起发送至接收器，而无需源特定的状态。DF 选择发生在 RP 发现期间，提供至 RP 的默认路由。

注释 如果 威胁防御设备 是 PIM RP，请使用 威胁防御设备 的未被转换的外部地址作为 RP 地址。

PIM 源特定组播支持

威胁防御设备 不支持 PIM 源特定组播 (SSM) 功能和相关配置。不过，威胁防御设备 允许与 SSM 相关的数据包通过，除非将其放置为最后一跳路由器。

SSM 被分类为数据传递机制，适用于一对多应用，如 IPTV。SSM 模型使用“通道”的概念，以 (S,G) 对表示，其中 S 表示源地址，G 表示 SSM 目标地址。通过使用组管理协议（如 IGMPv3）来实现订用通道。一旦SSM获悉某一特定的组播源，它将使接收客户端能直接从该源接收多播流，而不是从共享交汇点 (RP) 接收。SSM 中引入了访问控制机制，提供当前稀疏或疏-密模式实施无法提供的安全增强功能。

PIM-SSM 与 PIM-SM 不同，前者不使用 RP 或共享树。相反，组播组源地址上的信息将由接收方通过本地接收协议 (IGMPv3) 提供，并且用于直接构建源特定树。

组播双向 PIM

对于有多个源和接收器相互同步交互的网络，以及每个参与者都可以同时成为多播流量的源和接收器的网络而言，多播双向 PIM （例如在视频会议、Webex 会议和分组聊天中）非常有用。当使用 PIM 双向模式时，RP 仅会为共享树创建 (*,G) 条目。没有 (S,G) 条目。这节省了 RP 上的资源，因为这样不用维护每个 (S,G) 条目的状态表。

在 PIM 稀疏模式下，流量仅会沿共享树向下流动。在 PIM 双向模式下，流量沿共享树向上和向下流动。

PIM 双向模式也不使用 PIM 寄存器/寄存器停止机制来向 RP 注册源。每个源随时都可以开始发送到源。当多播数据包到达 RP 时，这些数据包将向下转发到共享树（如果有接收器）或被丢弃（如果没有接收器）。但是，RP 无法告知源停止发送多播流量。

从设计角度看，您必须考虑在网络中放置 RP 的位置，因为该位置应为网络中源和接收器之间的中间位置。

PIM 双向模式没有反向路径转发 (RPF) 检查。相反，它使用指定转发器 (DF) 的概念来防止循环。此 DF 是网段上唯一允许向 RP 发送多播流量的路由器。如果每个网段只有一个路由器转发多播流量，则没有循环。使用以下机制选择 DF：

- 具有最低 RP 指标的路由器是 DF。
- 如果指标相等，则具有最高 IP 地址的路由器将成为 DF。

PIM 自举路由器 (BSR)

PIM 自举路由器 (BSR) 是一个动态交汇点 (RP) 选择模型，它使用候选路由器执行 RP 功能以及中继组的 RP 信息。RP 功能包括 RP 发现并向 RP 提供默认路由。它执行此操作的方式是将一组设备配置为候选 BSR (C-BSR)，它们参与 BSR 选举过程，以从它们自身中选出一个 BSR。选择 BSR 后，配置为候选交汇点 (C-RP) 的设备将开始向选出的 BSR 发送其组映射。然后，BSR 会将组与 RP 的映射信息通过基于跳从 PIM 路由器传送至 PIM 路由器的 BSR 消息发至组播树下的其他所有设备。

此功能提供了一种动态获悉 RP 的方法，这在 RP 可能会定期关闭和启动的大型负载网络中非常重要。

PIM 自举路由器 (BSR) 术语

以下术语经常在 PIM BSR 配置中引用：

- 自举路由器 (BSR) - BSR 通过 PIM 逐跳向其他路由器通告交汇点 (RP) 信息。在多个候选 BSR 中，在选举过程后会选择单个 BSR。此自举路由器的主要目的是将所有候选 RP (C-RP) 通告收集到称为 RP-set 的数据库中，并以 BSR 消息的形式定期（每 60 秒）将此数据库发送到该网络中的其他路由器。
- 自举路由器 (BSR) 消息— BSR 消息会组播到 TTL 为 1 的 All-PIM-Routers 组。收到这些消息的所有 PIM 邻居会将它们重新传输（TTL 同样为 1）到除收到消息的接口之外的所有接口。BSR 消息包含 RP 集合和当前活动 BSR 的 IP 地址。这是 C-RP 了解在何处单播其 C-RP 消息的方式。
- 候选自举路由器 (C-BSR) - 配置为候选 BSR 的某个设备会参与 BSR 选举机制。具有最高优先级的 C-BSR 会被选举作为 BSR。C-BSR 的最高 IP 地址作为决定因素。BSR 选举过程是优先的，例如，如果出现具有更高优先级的新 C-BSR，它会触发新的选举过程。
- 候选交汇点 (C-RP) - RP 作为组播数据源和接收器的交汇场所。配置为 C-RP 的设备会通过单播定期将组播组映射信息直接通告到选举的 BSR。这些消息包含组范围、C-RP 地址和保持时间。当前 BSR 的 IP 地址从网络中所有路由器收到的定期 BSR 消息获取。这样，BSR 可了解当前正在运行且可访问的 RP。

注释 威胁防御设备 不充当 C-RP，即使 C-RP 是 BSR 流量的强制性要求也是如此。仅路由器可以充当 C-RP。因此，对于 BSR 测试功能，您必须将路由器添加到拓扑。

- BSR 选举机制 - 每个 C-BSR 都会生成包含 BSR 优先级字段的引导程序消息 (BSM)。该域中的路由器会在整个域中泛洪传播 BSM。C-BSR 收到具有比自身优先级更高的 C-BSR 时，会在特定时间内抑制进一步发送 BSM。剩余的单个 C-BSR 会成为选举的 BSR，而且其 BSM 会通知域中的所有其他路由器它是选举的 BSR。

组播组概念

组播基于组概念。任意一组接收者对接收特定数据流表现出兴趣。这样的组没有任何物理边界或地理边界 - 主机可位于互联网上的任何位置。有兴趣接收流向特定组的数据的主机必须使用 IGMP 加入该组。要接收数据流，主机必须是该组的成员。

组播地址

组播地址指定已加入某个组的任意一组 IP 主机，并希望接收发送到此组的流量。

集群

组播路由支持群集。在跨网络 EtherChannel 集群中，在快速路径转发建立之前，控制单元会发送所有的组播数据包和数据包。在建立快速路径转发后，数据单元可能会转发组播数据包。所有数据流

都是全流量。同时还支持末节转发流。由于跨网络 EtherChannel 集群中仅有一台设备接收组播数据包，因此，重定向到控制单元较为常见。

组播路由的要求和必备条件

型号支持

威胁防御

Threat Defense Virtual

支持的域

任意

用户角色

管理员

网络管理员

组播路由指南

防火墙模式

仅在路由防火墙模式下受支持。不支持透明防火墙模式。

IPv6

不支持 IPv6。

组播组

保留 224.0.0.0 和 224.0.0.255 之间的地址范围用于路由协议和其他拓扑发现或维护协议，例如网关发现和组成员报告。因此，不支持来自地址范围 224.0.0/24 的互联网组播路由；为保留地址启用组播路由时，未创建 IGMP 组。

集群

在集群中，对于 IGMP 和 PIM，仅在主设备上支持此功能。

其他规定

- 必须针对入站安全区配置访问控制或预过滤器规则的，以允许流量到达组播主机（如224.1.2.3）。但不能为该规则指定目标安全区，或者不能使其在初始连接验证过程中适用于组播连接。

- 不能禁用配置了 PIM 的接口。如果已在接口上配置 PIM（请参阅 配置 PIM 协议，第 11 页），则禁用组播路由和 PIM 不会删除PIM配置。您必须移除（删除）PIM配置才能禁用接口。
- 流量区域中的接口上不支持 PIM/IGMP 组播路由。
- 请勿将 威胁防御 同时配置为交汇点 (RP) 和第一跳路由器。
- HSRP 备用 IP 地址不参与 PIM 邻居关系。因此，如果通过 HSRP 备用 IP 地址来路由 RP 路由器 IP，则组播路由在 威胁防御 中不起作用。因此，要使组播流量成功通过，请确保 RP 地址的路由不是 HSRP 备用 IP 地址，而是将路由地址配置为接口 IP 地址。

配置 IGMP 功能

IP 主机使用 IGMP 向直接连接的组播路由器报告其组成员身份。IGMP 用于在特定 LAN 上的一个组播组中动态注册单个主机。主机通过向其本地组播路由器发送 IGMP 消息来识别组成员身份。在 IGMP 下，路由器监听 IGMP 消息，并定期发出查询以发现特定子网上处于活动状态或非活动状态的组。

本节介绍如何为逐个接口配置可选的 IGMP 设置。

过程

步骤 1 启用组播路由，第 6 页
步骤 2 配置 IGMP 协议，第 7 页。
步骤 3 配置 IGMP 访问组，第 8 页。
步骤 4 配置 IGMP 静态组，第 9 页。
步骤 5 配置 IGMP 加入组，第 9 页。

启用组播路由

默认情况下，在 威胁防御设备上启用组播路由可以在所有接口上启用 IGMP 和 PIM。IGMP 用于了解直连子网上是否存在组成员。主机通过发送 IGMP 报告消息加入组播组。PIM 用于维护转发表，以转发组播数据报。

注释 组播路由仅支持 UDP 传输层。

下表列出了特定组播表的最大条目数。一旦达到这些限制，系统将会丢弃所有新条目。

- MFIB - 30,000
- IGMP 组 - 30,000

- PIM 路由 - 72,000

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 依次选择**路由** > **组播路由** > **IGMP**。

步骤 3 选中**启用组播路由**复选框。

选中此复选框可在设备上启用 IP 组播路由。取消选中此复选框将禁用 IP 组播路由。默认情况下，组播已禁用。启用组播路由可在所有接口上启用组播。

您可以逐个接口禁用组播。如果知道特定接口上没有组播接口，并且希望防止 威胁防御设备通过该接口发送主机查询消息，则此操作很有用。

配置 IGMP 协议

您可以为每个接口配置 IGMP 参数，如转发接口、查询消息和时间间隔。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **组播路由** > **IGMP**。

步骤 3 在**协议**上，点击**添加**或**编辑**。

使用**添加 IGMP 参数**对话框将新的 IGMP 参数添加到 威胁防御设备。使用**编辑 IGMP 参数**对话框更改现有参数。

步骤 4 配置以下选项：

- **接口** - 从下拉列表中选择要为其配置 IGMP 协议的接口。
- **启用 IGMP** - 选中该复选框可启用 IGMP。

  注释 如果知道特定接口上没有组播主机，并且想要防止设备通过该接口发送主机查询消息，则在特定接口上禁用 IGMP 很有用。

- **转发接口** - 从下拉列表中选择您要通过其转发 IGMP 消息的特定接口。

  此选项可将 Cisco Secure Firewall Threat Defense设备配置为 IGMP 受托代理，并使其会从连接到一个接口的主机将 IGMP 消息转发到另一个接口上的上游组播路由器。

- **版本** - 选择 IGMP 版本 1 或 2。

  默认情况下，威胁防御设备运行 IGMP 版本 2，这将启用多个附加功能。

注释　子网上所有的组播路由器必须支持同一版本的 IGMP。威胁防御设备不会自动检测 IGMP 版本 1 路由器并切换到版本 1。但是，可以在子网上结合使用 IGMP 版本 1 和版本 2 主机；当存在 IGMP 版本 1 主机时，运行 IGMP 版本 2 的 威胁防御设备可正常工作。

- **查询间隔** - 指定的路由器发送 IGMP 主机查询消息的间隔（以秒为单位）。范围为 1 到 3600。默认值为 125。

  注释　如果 威胁防御 设备不能在指定超时值内在接口上收到查询消息，设备将会成为指定路由器并开始发送查询消息。

- **响应时间** - 在 威胁防御设备删除组之前的间隔（以秒为单位）。范围为 1 到 25。默认值为 10。

  如果 威胁防御设备未在此时间内收到对主机查询的响应，它会删除该组。

- **组限制** - 可在接口上加入的最大主机数。范围为 1 到 500。默认值为 500。

  您可以对每个接口限制 IGMP 成员身份报告造成的 IGMP 状态数量。超出所配置限制的成员身份报告不会输入到 IGMP 缓存中，多余成员身份报告的流量不会转发

- **查询超时** - 在上一请求者停止后，威胁防御设备成为接口请求者之前需经过的时间（以秒为单位）。范围为 60 到 300。默认值为 255。

步骤 5 点击**确定**以保存 IGMP 协议配置。

配置 IGMP 访问组

您可以通过使用访问控制列表控制对组播组的访问。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **组播路由** > **访问组**。

步骤 3 在**访问组 (Access Group)** 上，点击**添加 (Add)** 或**编辑 (Edit)**。

使用**添加 IGMP 访问组参数**对话框可以将新的 IGMP 访问组添加到访问组表中。使用**编辑 IGMP 访问组参数**对话框可更改现有的参数。

步骤 4 配置以下选项：

a) 从**接口**下拉列表中，选择与访问组关联的接口。编辑现有访问组时，不能更改相关的接口。

b) 点击以下选项之一：

- **标准访问列表 (Standard Access List)** - 从**标准访问列表 (Standard Access List)**下拉列表中，选择标准 ACL 或点击 **添加**（+） 以创建新的标准 ACL。请参阅配置标准 ACL 对象了解相关程序。

- **扩展访问列表 (Extended Access List)** - 从**扩展访问列表 (Extended Access List)**下拉列表中，选择扩展 ACL 或点击 **添加**（+）创建新的扩展 ACL。请参阅配置扩展 ACL 对象了解相关程序。

步骤 5 点击**确定**以保存访问组配置。

配置 IGMP 静态组

有时，组成员无法在组中报告其成员身份，或者网络段上没有组的成员，但仍希望将该组的组播流量发送到该网络段。您可以通过配置静态加入的 IGMP 组将该组的组播流量发送到网段。使用此方法时，威胁防御设备不会接受数据包本身，只会转发它们。因此，此方法可用于快速切换。传出接口显示在 IGMP 缓存中，但此接口不是组播组的成员。配置 IGMP 静态组时，请确保 威胁防御 是接口上的目标路由器。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **组播路由** > **IGMP**。

步骤 3 在**静态组 (Static Group)** 上，点击**添加 (Add)** 或**编辑 (Edit)**。

使用**添加 IGMP 静态组参数**对话框可以将组播组静态地分配给接口。使用**编辑 IGMP 静态组参数**对话框可以更改现有的静态组分配。

步骤 4 配置以下选项：

- 从**接口**下拉列表中，选择要向其静态分配组播组的接口。如果编辑的是现有条目，则无法更改此值。
- 从**组播组**下拉列表中，选择要为其分配接口的组播组，或点击 **添加**（+）创建新的组播组。有关过程，请参阅创建网络对象。

步骤 5 点击**确定**以保存静态组配置。

配置 IGMP 加入组

您可以将接口配置成为组播组的成员。配置 威胁防御设备加入组播组会使上游路由器维护该组的组播路由表信息，并保持该组的路径处于活动状态。配置 IGMP 加入组时，请确保 威胁防御 是接口上的目标路由器 (DR)。

注释 如果要将特定组的组播数据包转发给接口，且无需 威胁防御设备将这些数据包接受为该组的一部分，请参阅配置 IGMP 静态组， 第 9 页。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **组播路由** > **IGMP**。

步骤 3 在**加入组 (Join Group)** 上，点击**添加 (Add)** 或**编辑 (Add)**。

使用**添加 IGMP 加入组参数**对话框可以将 威胁防御设备配置为组播组的成员。使用**编辑 IGMP 加入组参数**对话框可更改现有参数。

步骤 4 配置以下选项：

- 从**接口**下拉列表中，选择要作为组播组成员的接口。如果编辑的是现有条目，则无法更改此值。
- 从**加入组 (Join Group)** 下拉列表中，选择要为其分配接口的组播组，或点击**加号**创建新的组播组。有关过程，请参阅创建网络对象。

配置 PIM 功能

路由器使用 PIM 来维护转发表，以便用于转发组播图。如果在 Secure Firewall Threat Defense 上启用组播路由，PIM 和 IGMP 将会在所有接口上自动启用。

注释 PAT 不支持 PIM。PIM 协议不使用端口，PAT 只能与使用端口的协议配合使用。

本节介绍如何配置可选的 PIM 设置。

过程

步骤 1 配置 PIM 协议， 第 11 页

步骤 2 配置 PIM 邻居过滤器， 第 11 页

步骤 3 配置 PIM 双向邻居过滤器， 第 12 页

步骤 4 配置 PIM 交汇点， 第 13 页

步骤 5 配置 PIM 路由树， 第 14 页

步骤 6 配置 PIM 请求筛选器， 第 15 页

步骤 7 配置组播边界过滤器，第 17 页

配置 PIM 协议

可以在特定接口上启用或禁用 PIM。

还可以配置指定的路由器 (DR) 优先级。指定路由器 (DR) 负责将 PIM 注册消息、加入消息和删除消息发送到 RP。如果网段上有多个组播路由器，将会根据 DR 优先级来选择 DR。如果多台设备具有同样的 DR 优先级，则具有最高 IP 地址的设备将会成为 DR。默认情况下，威胁防御设备 的 DR 优先级为 1。

路由器查询消息用于选择 PIM DR。PIM DR 负责发送路由器查询消息。默认情况下，每隔 30 秒发送一次路由器查询消息。此外，威胁防御设备每隔 60 秒发送一次 PIM 加入消息或删除消息。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **组播路由** > **PIM**。

步骤 3 在**协议**上，点击**添加**或**编辑**。

使用**添加 PIM 参数**对话框可以向接口添加新的 PIM 参数。使用**编辑 PIM 参数**对话框可以更改现有的参数。

步骤 4 配置以下选项：

- **接口** - 从下拉列表中，选择要为其配置 PIM 协议的接口。
- **启用 PIM** - 选中该复选框以启用 PIM。
- **DR 优先级** - 所选接口的 DR 值。子网上具有最高 DR 优先级的路由器将成为指定路由器。有效值范围为 0 到 4294967294。默认 DR 优先级为 1。将此值设置为 0 会使 威胁防御 设备接口没有资格成为指定路由器。
- **呼叫间隔** - 接口发送 PIM 呼叫消息的时间间隔（以秒为单位）。范围为 1 到 3600。默认值为 30。
- **加入删除间隔** - 接口发送 PIM 加入和删除通告的间隔（以秒为单位）。范围为 10 到 600。默认值为 60。

步骤 5 点击**确定**以保存 PIM 协议配置。

配置 PIM 邻居过滤器

您可以定义可成为 PIM 邻居的路由器。通过筛选可成为 PIM 邻居的路由器，可以实现以下目的：

- 防止未授权的路由器成为 PIM 邻居。
- 防止连接的末节路由器加入到 PIM。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **多播路由** > **PIM**。

步骤 3 在**邻居过滤器 (Neighbor Filter)** 上，点击**添加 (Add)** 或**编辑 (Edit)**。

使用**添加 PIM 邻居过滤器**对话框将新的 PIM 邻居筛选器添加到接口。使用**编辑 PIM 邻居过滤器**对话框更改现有参数。

步骤 4 配置以下选项：

- 从**接口**下拉列表中，选择要向其添加 PIM 邻居过滤器的接口。
- **标准访问列表 (Standard Access List)** - 从**标准访问列表 (Standard Access List)**下拉列表中，选择标准 ACL 或点击 **添加**（+）以创建新的标准 ACL。请参阅配置标准 ACL 对象了解相关程序。

  注释 在**添加标准访问列表条目**对话框上选择**允许**可以使组播组通告通过该接口。选择**阻止**将会禁止指定的组播组通告通过接口。在接口上配置组播边界时，会阻止所有的组播流量通过接口，除非使用邻居过滤器条目允许通过。

步骤 5 点击**确定**保存 PIM 邻居过滤器配置。

配置 PIM 双向邻居过滤器

PIM 双向邻居过滤器是定义可参与指定转发器 (DF) 选择的邻居设备的 ACL。如果接口未配置 PIM 双向邻居过滤器，则没有限制。如果配置了 PIM 双向邻居过滤器，则只有 ACL 允许的邻居可参与 DF 选择过程。

双向 PIM 允许组播路由器保持减少的状态信息。要选择 DF，必须双向启用分片中的所有组播路由器。

如果启用了 PIM 双向邻居过滤器，ACL 允许的路由器将被视为具有双向功能。因此，以下说法均是正确的：

- 如果一个获允许的邻居不支双向模式，将不会发生 DF 选择。
- 如果一个被拒绝的邻居支持双向模式，将不会发生 DF 选择。
- 如果一个被拒绝的邻居不支持双向模式，可能会发生 DF 选择。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**组播路由** > **PIM**。

步骤 3 在**双向邻居过滤器 (Bidirectional Neighbor Filter)** 上，点击**添加 (Add)** 或**编辑 (Edit)**。

使用**添加 PIM 双向邻居过滤器**对话框可以为 PIM 双向邻居过滤器 ACL 创建 ACL 条目。使用**编辑 BFD 双向邻居过滤器**对话框可更改现有的参数。

步骤 4 配置以下选项：

- 从**接口**下拉列表中，选择要配置 PIM 双向邻居过滤器 ACL 条目的接口。
- **标准访问列表 (Standard Access List)** - 从**标准访问列表 (Standard Access List)**下拉列表中，选择标准 ACL 或点击 **添加**（+）以创建新的标准 ACL。请参阅配置标准 ACL 对象了解相关程序。

  注释 在**添加标准访问列表条目**对话框上选择**允许**可以使指定的设备参与 DR 选择过程。选择**阻止**可阻止指定设备参与 DR 选择过程。

步骤 5 点击**确定**以保存 PIM 双向邻居过滤器配置。

配置 PIM 交汇点

可以将 威胁防御设备配置为用作多个组的 RP。ACL 中指定的组范围确定 PIM RP 组映射。如果未指定 ACL，则一个组的 RP 将应用于整个组播组范围 (224.0.0.0/4)。有关双向 PIM 的更多信息，请参阅组播双向 PIM，第 3 页。

以下限制适用于 RP：

- 一个 RP 地址不能用两次。
- 不能为多个 RP 指定所有组。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 依次选择**路由** > **组播路由** > **PIM**。

步骤 3 在**交汇点 (Rendezvous Points)** 选项卡上，点击**添加 (Add)** 或**编辑 (Edit)**。

使用**添加交汇点**对话框为“交汇点”表创建新条目。使用**编辑交汇点**对话框以更改现有参数。

步骤 4 配置以下选项：

- 从**交汇点 IP 地址 (Rendezvous Point IP address)** 下拉列表中，选择希望添加为 RP 的 IP 地址，或者点击 **添加**（+） 以创建新网络对象。请参阅创建网络对象了解相关程序。

- 如果指定的组播组要在双向模式下运行，请选中 **Use bi-directional forwarding** 复选框。在双向模式下，如果 威胁防御设备接收组播数据包，且没有直连成员或PIM 邻居，则会将删除消息发送回源。
- 选择**将此 RP 用于所有组播组 (Use this RP for all Multicast Groups)** 以便将指定的 RP 用于该接口上的所有组播组。
- 选择**将此 RP 用于下面指定的所有组播组 (Use this RP for all Multicast Groups as specified below)**，以指定组播组与指定 RP 一起使用，然后从**标准访问列表 (Standard Access List)** 下拉列表中，选择标准 ACL，或者点击 **添加**（+）以创建新的标准 ACL。请参阅配置标准 ACL 对象了解相关程序。

步骤 5 点击**确定**以保存交汇点配置。

配置 PIM 路由树

默认情况下，PIM 叶子路由器在第一个数据包从新源到达后会立即加入到最短路径树。此方法可降低延迟，但需要的内存比共享树多。您可以将 威胁防御设备配置为对于所有组播组或仅对于特定组播地址加入到最短路径树或者使用共享树。

最短路径树用于未在 Multicast Groups 表中指定的任何组。“组播组”表显示与共享树配合使用的组播组。表条目按自上而下的顺序进行处理。您可以通过以下方法来创建包含一系列组播组但不包含该系列中特定组的条目：将特定组的拒绝规则放置在表的顶部，并将该系列组播组的允许规则放置在拒绝语句下面。

注释 这种行为称为最短路径状态切换 (SPT)。建议您始终使用“共享树”选项。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **组播路由** > **PIM**。

步骤 3 在**路由树 (Route Tree)** 上，选择路由树的路径：

- 点击**最短路径 (Shortest Path)** 可为所有组播组使用最短路径树。
- 点击**共享树 (Shared Tree)** 可为所有组播组使用共享树。
- 点击**提到的以下组的共享树 (Shared tree for below mentioned group)** 以指定在“组播组”表中指定的组，然后从**标准访问列表 (Standard Access List)** 下拉列表中选择一个标准 ACL 或点击**添加**（+）以创建新的标准 ACL。请参阅配置标准 ACL 对象了解相关程序。

步骤 4 点击**确定**以保存路由树配置。

配置 PIM 请求筛选器

当 威胁防御设备作为 RP 时，您可以禁止特定的组播源注册到该设备，以防止未授权的源注册到 RP。您可以定义 威胁防御设备从其接受 PIM 寄存器消息的组播源。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由** > **组播路由** > **PIM**。

步骤 3 在**请求筛选器 (Request Filter)** 上，定义允许在 威胁防御设备充当 RP 时向其注册的组播源：

- 从**筛选 PIM 寄存器消息使用:** 下拉列表中选择**无**、**访问列表**或**路由映射**。
- 如果从下拉列表中选择**访问列表 (Access List)**，请选择扩展 ACL 或点击 **添加**（+） 以创建新的扩展 ACL。请参阅配置扩展 ACL 对象了解相关程序。

  注释 在**添加扩展访问列表项 (Add Extended Access List Entry)** 对话框中，从下拉列表中选择**允许 (Allow)** 以创建允许指定的组播通信的指定源注册到 威胁防御 设备的规则，或选择**阻止 (Block)** 以创建阻止指定的组播通信的指定源注册到设备的规则。

- 如果选择**路由地图 (Route Map)**，请从**路由地图 (Route Map)** 下拉列表中选择一个路由映射，或点击 **添加**（+） 以创建新的路由映射。有关过程请参阅创建网络对象。

步骤 4 点击**确定**以保存请求过滤配置。

将 Cisco Secure Firewall Threat Defense设备配置为候选自举路由器

可将 威胁防御设备配置为候选 BSR。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 依次选择**路由** > **组播路由** > **PIM**。

步骤 3 在**引导程序路由器 (Bootstrap Router)** 上，选中**将此 FTD 配置为候选自举路由器 (C-BSR) (Configure this FTD as a Candidate Bootstrap Router [C-BSR])** 复选框，以执行 C-BSR 设置。

a) 从**接口**下拉列表中，选择 威胁防御设备上要从其派生 BSR 地址以使其成为候选者的接口。

此接口必须使用 PIM 启用。

b) 在**散列掩码长度**字段中，输入将在调用散列函数之前与组地址进行与运算的掩码的长度（最多32位）。所有具有相同种子的组都将散列（对应）到同一RP。例如，如果此值为24，则组地址只有前 24 位起作用。这种情况允许您为多个组获取一个 RP。范围为 0 到 32。

c) 在**优先级**字段中，输入候选 BSR 的优先级。优先选择优先级高的 BSR。如果优先级值相同，则 IP 地址较大的路由器是 BSR。范围为 0 到 255。默认值为 0。

步骤 4 （可选）在**将此 FTD 配置为边界自举路由器 (BSR)** 部分中点击 **添加**（+），选择不会在其上发送或接收 PIM BSR 消息的接口。

- 从**接口**下拉列表中，选择不会在其上发送或接收 PIM BSR 消息的接口。

  RP 或 BSR 通告将被有效过滤，从而隔离两个域的 RP 信息交换。

- 选中**启用边界 BSR**复选框以启用 BSR。

步骤 5 点击**确定**以保存自举路由器配置。

配置组播路由

配置静态组播路由可以将组播流量与单播流量分隔开。例如，如果源和目标之间的路由不支持组播路由，可以通过如下方法来解决这个问题：使用GRE隧道在它们之间配置两个组播设备，并通过该隧道发送组播数据包。

使用 PIM 时，威胁防御设备期望用于接收数据包的接口和用于将单播数据包发送回到源的接口是同一个接口。在某些情况下（例如，绕过不支持组播路由的路由），您可能希望单播数据包和组播数据包使用不同的路径。

静态组播路由不能通告或重分布。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 选择**路由 (Routing)** > **组播路由 (Multicast Routing)** > **组播路由 (Multicast Routes)** > **添加或编辑 (Add or Edit)**。

使用**添加组播路由**对话框可将新的组播路由添加到 威胁防御设备。使用**编辑组播路由**对话框可更改现有的组播路由。

步骤 3 从**源网络 (Source Network)** 下拉框中，选择一个现有网络或点击 **添加**（+） 以添加新网络。有关过程，请参阅创建网络对象。

步骤 4 要配置接口以转发路由，请点击**接口 (Interface)** 并配置以下选项：

- 从**源接口**下拉列表中，为组播路由选择传入接口。
- 从**输出接口/密集**下拉列表中，选择路由转发到的目标接口。

- 在**距离**字段中，输入组播路由的距离。范围为 0 到 255。

步骤 5 要配置 RPF 地址以转发路由，请点击**地址 (Address)** 并配置以下选项：

- 在 **RPF 地址**字段中，输入组播路由的 IP 地址。
- 在**距离**字段中，输入组播路由的距离，范围为 0 到 255。

步骤 6 点击**确定**以保存组播路由配置。

配置组播边界过滤器

地址范围定义了域边界，从而使具有 IP 地址相同的 RP 的域不会相互泄漏。可在大型域内的子网边界以及域与互联网之间的边界上执行范围界定。

可以在接口上为组播组地址设置管理权限界定的边界过滤器。IANA 已将 239.0.0.0 到 239.255.255.255 的组播地址范围指定为可使用管理性界定的地址。此地址范围可在不同组织管理的域中重复使用。此类地址被视为本地地址，而不是全局唯一地址。

标准ACL定义受影响地址的范围。在设置边界过滤器后，不允许组播数据包从任一方向流经边界。边界过滤器允许同一个组播组地址在不同的管理域中重复使用。

可在使用管理权限界定的边界配置、检查和过滤 Auto-RP 发现消息和通知消息。Auto-RP 数据包中被边界 ACL 拒绝的任意 Auto-RP 组范围通知都会被删除。仅在 Auto-RP 组范围中的所有地址获得边界 ACL 允许的情况下，Auto-RP 组范围通知才可以通过边界过滤器。如果有任何地址未获允许，在 Auto-RP 消息转发前，将会筛选整个组范围并将其从 Auto-RP 消息中删除。

过程

步骤 1 依次选择**设备(Devices)** > **设备管理(Device Management)**，并且编辑 威胁防御 设备。

步骤 2 依次选择**路由** > **组播路由** > **组播边界过滤器**，然后点击**添加**或**编辑**。

使用**添加组播边界过滤器 (Add Multicast Boundary Filter)** 对话框向设备添加新的组播边界过滤器。使用**编辑组播边界过滤器**对话框更改现有参数。

可为使用管理权限界定的组播地址配置组播边界。组播边界限制组播数据包流，并允许在不同的管理域中重复使用相同的组播组地址。在接口上定义了组播边界后，只有过滤器ACL允许的组播流量可通过接口。

步骤 3 从**接口**下拉列表中，选择为其配置组播边界过滤器 ACL 的接口。

步骤 4 从**标准访问列表**下拉列表中，选择要使用的标准 ACL，或者点击 **添加**（+） 创建新的标准 ACL。请参阅配置标准 ACL 对象了解相关程序。

步骤 5 选中**删除 Auto-RP 数据包中被边界拒绝的任意 Auto-RP 组范围通知**复选框，从被边界 ACL 拒绝的源中过滤 Auto-RP 消息。如果未选中此复选框，则将允许所有 Auto-RP 消息通过。

步骤 6 点击**确定**，以保存组播边界过滤器配置。

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。