OSPF

本章介绍如何将Firewall Threat Defense配置为使用开放式最短路径优先 (OSPF) 路由协议来路由数据、执行身份验证以及重新分发路由信息。

OSPF

本章介绍如何将Firewall Threat Defense配置为使用开放式最短路径优先 (OSPF) 路由协议来路由数据、执行身份验证以及重新分发路由信息。

关于 OSPF

OSPF 是一种使用链路状态而非距离矢量进行路径选择的内部网关路由协议。OSPF 传播链路状态通告而非路由表更新。由于仅交换 LSA 而不是整个路由表，因此 OSPF 网络比 RIP 网络更快收敛。

OSPF 使用链路状态算法构建和计算所有到达已知目标的最短路径。OSPF 区域中的每台路由器包含相同的链路状态数据库，该数据库是由每台路由器可使用的接口和可到达的邻居组成的列表。

相比 RIP，OSPF 具有以下优点：

- OSPF 链路状态数据库更新的发送频率低于 RIP 更新，并且随着过时信息的超时，链路状态数据库即时而非逐步更新。
- 路由决策基于开销，它表明通过特定接口发送数据包所需的开销。Firewall 威胁防御设备 根据链路带宽而非到目标的跃点数计算接口的开销。可以配置开销来指定首选路径。

最短路径优先算法的缺点是需要大量 CPU 周期和内存。

Firewall 威胁防御设备 可以在不同接口集上同时运行 OSPF 协议的两个进程。如果您具有使用相同 IP 地址的接口（NAT 允许这些接口共存，但是 OSPF 不允许重叠地址），则可能要运行两个进程。

或者，可能要在内部运行一个进程，在外部运行另一个进程，并且在两个进程之间重新分发路由的子集。同样，可能需要将专用地址与公用地址分离。

您可以将路由从一个 OSPF 路由进程、RIP 路由进程或从在启用了 OSPF 的接口上配置的静态路由和已连接路由重新分发到另一个 OSPF 路由进程中。

Firewall 威胁防御设备 支持以下 OSPF 功能：

- 区域内、区域间和外部（I 类和 II 类）路由。
- 虚拟链路。
- LSA 泛洪。
- OSPF 数据包身份验证（密码和 MD5 身份验证）。
- 将 Firewall 威胁防御设备 配置为指定路由器或指定备用路由器。Firewall 威胁防御设备 也可以设置为 ABR。
- 末节区域和次末节区域。
- 区域边界路由器 3 类 LSA 筛选。

OSPF 支持 MD5 和明文邻居身份验证。如有可能，应将身份验证与所有路由协议配合使用，因为在 OSPF 和其他协议（如 RIP）之间的路由重新分发可能会被攻击者用于破坏路由信息。

如果使用 NAT，如果 OSPF 是在公共和专用区域上运行，并且如果要求地址过滤，则需要运行两个 OSPF 进程，一个进程对应于公共区域，一个进程对应于专用区域。

在多个区域中具有接口的路由器称为区域边界路由器 (ABR)。充当网关以在使用 OSPF 的路由器与使用其他路由协议的路由器之间重新分发流量的路由器称为自治系统边界路由器 (ASBR)。

ABR 使用 LSA 将有关可用路由的信息发送到其他 OSPF 路由器。使用 ABR 3 类 LSA 筛选，您可以具有单独的以 ASA 作为 ABR 的专用和公共区域。3 类 LSA（区域间路由）可以从一个区域筛选到另一个区域，从而允许您在不通告专用网络即的情况下配合使用 NAT 和 OSPF。

注释 只能筛选 3 类 LSA。如果在专用网络中将 Firewall 威胁防御设备 配置为 ASBR，它将发送描述专用网络的 5 类 LSA，后者会泛洪至整个 AS，包括公共区域。

如果采用 NAT 但 OSPF 仅在公共区域中运行，则可以在专用网络内将到公共网络的路由作为默认或 5 类 AS 外部 LSA 重新分发。但是，需要为受 Firewall 威胁防御设备 保护的专用网络配置静态路由。此外，不应在同一 Firewall 威胁防御设备 接口上混用公用和专用网络。

您可以同时在 Firewall 威胁防御设备 上运行两个 OSPF 路由进程、一个 RIP 路由进程和一个 EIGRP 路由进程。

快速呼叫数据包 OSPF 支持

OSPF 快速呼叫数据包支持功能提供了一种以短于一秒的间隔发送呼叫数据包的配置方式。此类配置在开放式最短路径优先 (OSPF) 网络中会导致更快的收敛。

OSPF 支持快速呼叫数据包的前提条件

OSPF 必须已在网络中进行配置或与快速呼叫数据包 OSPF 支持功能同时配置。

OSPF 呼叫间隔和停顿间隔

OSPF 呼叫数据包是 OSPF 进程向其 OSPF 邻居发送以保持与这些邻居的连接的数据包。呼叫数据包按照可配置间隔（以秒为单位）进行发送。对于以太网链路，默认值为 10 秒；对于非广播链路，默认值为 30 秒。呼叫数据包包含在停顿间隔内为其接收到呼叫数据包的所有邻居的列表。停顿间隔也是可配置间隔（以秒为单位），并且默认为呼叫间隔值的四倍。所有呼叫间隔的值在网络中都必须相同。同样，所有停顿间隔的值在网络中也必须都相同。

这两种间隔通过表明链路可运行来结合用于保持连接。如果路由器在停顿间隔内没有从邻居接收到呼叫数据包，则将声明该邻居关闭。

OSPF 快速呼叫数据包

OSPF 快速呼叫数据包是指按照小于 1 秒的间隔发送的呼叫数据包。要了解快速呼叫数据包，您应已了解 OSPF 呼叫数据包与停顿间隔之间的关系。请参阅 OSPF 呼叫间隔和停顿间隔 ， 第 3 页。

通过使用 ospf dead-interval 命令来获取 OSPF 快速呼叫数据包。停顿间隔设置为 1 秒，并且 hello-multiplier 值设置为在该 1 秒期间要发送的呼叫数据包的数量，从而提供亚秒或“快速”呼叫数据包。

当在接口上配置了快速呼叫数据包时，此接口发出的呼叫数据包中通告的呼叫间隔设置为 0。系统将忽略通过此接口接收到的呼叫数据包中的呼叫间隔。

无论停顿间隔设置为 1 秒（对于快速呼叫数据包）还是设置为任何其他值，它在分片上都必须一致。只要在停顿间隔内发送了至少一个呼叫数据包，呼叫乘数对于整个分片便无需相同。

OSPF 快速呼叫数据包的优势

OSPF 快速呼叫数据包功能的优势是 OSPF 网络将比没有快速呼叫数据包的情况更快收敛。通过此功能，您可以在 1 秒内检测丢失的邻居。它在开放式系统互连 (OSI) 物理层和数据链路层可能未检测到邻居丢失的 LAN 分片中尤其有用。

OSPFv2 与 OSPFv3 之间的实施差异

OSPFv3 不向后兼容 OSPFv2。要使用 OSPF 路由 IPv4 和 IPv6 流量，必须同时运行 OSPFv2 和 OSPFv3。它们会共存但不相互交互。

OSPFv3 提供的其他功能包括：

- 按链路进行协议处理。
- 删除寻址语义。
- 添加泛洪范围。
- 支持每条链路多个实例。

- 使用 IPv6 链路本地地址执行网络发现和其他功能。
- 以前缀和前缀长度表示 LSA。
- 添加两种 LSA 类型。
- 处理未知 LSA 类型。
- 使用 OSPFv3 路由协议流量的 IPsec ESP 标准支持身份验证，如 RFC-4552 所指定。

OSPF 的要求和前提条件

型号支持

Firewall Threat Defense

Firewall Threat Defense Virtual

支持的域

任意

用户角色

管理员

网络管理员

OSPF 准则

防火墙模式准则

OSPF 仅支持路由防火墙模式。OSPF 不支持透明防火墙模式。

准则

OSPFv2 和 OSPFv3 支持状态 。

IPv6 准则

- OSPFv2 不支持 IPv6。
- OSPFv3 支持 IPv6。
- OSPFv3 使用 IPv6 进行身份验证。
- Firewall 威胁防御设备 将 OSPFv3 路由安装到 IPv6 RIB 中，前提是它是最佳路由。

OSPFv3 Hello 数据包和 GRE

通常，OSPF流量不会通过 GRE 隧道。当 IPv6 上的 OSPFv3 封装在 GRE 内时，安全检查（例如组播目标）的IPv6报头验证失败。由于隐式安全检查验证，数据包被丢弃，因为此数据包具有目标 IPv6 组播。

您可以定义预过滤器规则来绕过GRE流量。但是，使用预过滤器规则，检测引擎不会询问内部数据包。

集群准则

- 不支持 OSPFv3 加密。如果尝试在集群环境中配置 OSPFv3 加密，系统将显示错误消息。
- 在跨接口模式下，仅管理接口上不支持动态路由。
- 在单个接口模式下，确保已作为 OSPFv2 或 OSPFv3 邻居建立控制和数据单元。
- 在单个接口模式下，只能在控制单元共享接口上的两个情景之间建立 OSPFv2 邻接。仅在点对点链路上支持配置静态邻居；因此，在接口上仅允许一个邻居声明。
- 当集群中的控制角色发生变化时，会发生以下行为：
  - 在跨接口模式中，路由器进程仅在控制单元上处于活动状态，在数据单元上处于暂停状态。各集群设备具有同一路由器 ID，因为已从控制单元对配置进行同步。因此，在角色更改过程中，相邻路由器不会注意到集群的路由器 ID 发生的任何更改。
  - 在单个接口模式中，路由器进程在所有单个集群设备上都处于活动状态。各集群设备从已配置的集群池中选择其自己独特的路由器 ID。集群中的控制角色更改不会以任何方式更改路由拓扑。

多协议标签交换 (MPLS) 和 OSPF 准则

如果 MPLS 配置的路由器发送的链路状态 (LS) 更新数据包包含不透明 Type-10 链路状态通告 (LSA)，而且其中包括 MPLS 报头，则身份验证会失败且设备会自动丢弃更新数据包，而不是确认它们。最终，对等路由器将终止邻居关系，因为它没有收到任何确认。

确保在设备上禁用了不间断转发 (NSF)，以确保邻居关系保持稳定：

- 导航到 防火墙管理中心 中的**不间断转发 (Non Stop Forwarding)** 页面（**设备 (Devices)** > **设备管理 (Device Management)**（选择所需的设备） > **路由 (Routing)** > **OSPF** > **高级 (Advanced)** > **不间断转发 (Non Stop Forwarding)**）。

  确保未选中“**不间断转发功能**”复选框。

注释 Firepower 4100/9300 型号在使用 MPLS 时可能具有高延迟，因为它们缺乏跨多个接收队列的负载均衡。

双向和转发检测 (BFD)及 OSPF 准则

- 您可以在 OSPFv2 和 OSPFv3 接口（物理接口、子接口和端口通道）上启用 BFD。
- VTI 隧道、DVTI 隧道、环回接口、交换机端口、VNI、VTEP 和 IRB 接口不支持 BFD。

路由重分布准则

- 支持在 OSPFv2 上重新分配带有 IPv4 前缀列表的路由映射。但是，不支持在 OSPFv3 上重新分配带有 IPv6 前缀列表的路由映射。 使用 OSPF 上的路由映射中的访问列表进行重新分发。
- 在属于 EIGRP 网络的设备上配置 OSPF 时，请确保将 OSPF 路由器配置为标记路由（EIGRP 尚不支持路由标记）。

  将 OSPF 重新分发到 EIGRP 并将 EIGRP 重新分发到 OSPF 时，如果其中一个链路、接口中断，甚至当路由发起方关闭时，就会发生路由环路。为了防止将路由从一个域重新分发回同一域，路由器可以在重新分发时标记属于某个域的路由，并且可以根据相同的标记在远程路由器上过滤这些路由。由于这些路由不会安装到路由表中，因此它们不会重新分发到同一域中。

其他准则

- OSPFv2 和 OSPFv3 在接口上支持多个实例。
- OSPFv3 在非集群环境中通过 ESP 报头支持加密。
- OSPFv3 支持非负载加密。
- OSPFv2 根据 RFC 4811、4812 和 3623 定义分别支持思科 NSF 平稳重启和 IETF NSF 平稳重启机制。
- OSPFv3 根据 RFC 5187 定义支持平稳重启机制。
- 可分发的区域内（类型 1）路由数具有限制。对于这些路由，单一 1 类 LSA 包含所有前缀。由于系统的数据包大小限制为 35 KB，所以 3000 个路由会导致数据包超出该限制。考虑设置 2900 个 1 类路由作为支持的最大数量。
- 对于使用虚拟路由的设备，可以为全局虚拟路由器配置 OSPFv2 和 OSPFv3。但是，只能为用户定义的虚拟路由器配置 OSPFv2。
- 要避免在路由更新大于链路上的最小 MTU 时丢弃由于路由更新而导致的邻接摆动，请确保在链路两端的接口上配置相同的 MTU。
- 如果数据包大小超过 8190，OSPFv3 会放弃 LS 更新。因此，邻接关系将终止。因此，使用“ospfv3 mtu-ignore”命令来配置交换机，以避免邻接关系终止。

配置 OSPFv2

本节介绍配置 OSPFv2 路由进程所涉及的任务。对于使用虚拟路由的设备，可以为用户定义的虚拟路由器配置 OSPFv2。

配置 OSPF 区域、范围和虚拟链路

可以配置多个 OSPF 区域参数，包括设置身份验证、定义末节区域以及将特定成本分配给默认摘要路由。您最多可以启用两个 OSPF 进程实例。每个 OSPF 进程具有其自己的关联区域和网络。身份验证提供基于密码的区域非授权访问防御。

末节区域是有关外部路由的信息未发送到的区域。相反，ABR 生成了到自治系统外部目标的末节区域中的默认外部路由。要利用 OSPF 末节区域支持，必须在末节区域中使用默认路由。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF**。

步骤 5 选中 **过程 1** 的复选框。对于每个 context/virtual router，最多可以启用两个 OSPF 进程实例。您必须选择 OSPF 进程才能配置区域参数。

如果设备使用的是虚拟路由，则 ID 字段会显示为所选虚拟路由器生成的唯一进程 ID。

步骤 6 从下拉列表中选择**OSPF 角色**，然后在下一字段中为其输入说明。这些选项是“内部”、“ABR”、“ASBR” 和 “ABR 和 ASBR”。有关 OSPF 角色的说明，请参阅关于 OSPF，第 1 页。

步骤 7 选择**区域 (Area)** > **添加 (Add)**。

您可以点击 **编辑** ()，或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 8 为每个 OSPF 进程配置以下区域选项：

- **OSPF 进程 (OSPF Process)**- 选择进程 ID。对于使用虚拟路由的设备，下拉列表会列出为所选虚拟路由器生成的唯一进程 ID。
- **区域 ID** - 要汇总其路由的区域的资格。
- **区域类型** - 选择以下选项之一：
  - **普通 (Normal)** -（默认）标准 OSPF 区域。
  - **末节** - 末节区域之外没有任何路由器或区域。末节区域防止自制系统 (AS) 外部 LSA（5 类 LSA）泛洪至末节区域中。创建末节区域时，可以通过取消选中**摘要末节**复选框来防止摘要 LSA（3 类和 4 类）泛洪至该区域中。
  - **NSSA** - 使该区域成为次末节区域 (NSSA)。NSSA 接受 7 类 LSA。您也可以通过取消选中**重新分发** 复选框并选中 **默认信息来源** 复选框来禁用路由重新分发。可以通过取消选中**摘要 NSSA** 复选框来防止摘要 LSA 泛洪至该区域中。
- **指标值** - 用于生成默认路由的指标。默认值为 10。有效十进制值范围为 0 至 16777214。

- **指标类型 (Metric Type)** - 指标类型是与通告到OSPF路由域中的默认路由关联的外部链路类型。可用选项为 1（表示 1 类外部路由）或 2（表示 2 类外部路由）。
- **可用网络** - 选择可用网络之一并点击**添加**，或点击 **添加** (+) 以添加新网络对象。有关添加网络的过程，请参阅网络。
- **身份验证** - 选择 OSPF 身份验证：
  - **无** -（默认）禁用 OSPF 区域身份验证。
  - **密码** - 为区域身份验证提供明文密码，在需要考虑安全性的情景下，建议不要选择此选项。
  - **MD5** - 允许 MD5 身份验证。
- **默认成本** - OSPF 区域的默认开成本，用于确定到目标的最短路径。有效值范围为 0 至 65535。默认值为 1。

步骤 9 点击**确定 (OK)** 以保存区域配置。

步骤 10 选择**范围 (Range)** > **添加 (Add)**。

- 选择可用网络之一，以及是否进行通告，或者,
- 点击 **添加** (+) 以添加新网络对象。有关添加网络的过程，请参阅网络。

步骤 11 点击**确定 (OK)** 以保存范围配置。

步骤 12 选择**虚拟链路 (Virtual Link)**，点击**添加 (Add)** (+)，并为每个 OSPF 进程配置以下选项：

- **对等体路由器** - 选择对等体路由器的 IP 地址。要添加新的对等体路由器，请点击 **添加** (+)。有关添加网络的过程，请参阅网络。
- **呼叫间隔** - 在接口上发送的呼叫数据包的间隔时间（以秒为单位）。呼叫数据包间隔是将在呼叫数据包中通告的无符号整数。该值对特定网络上的所有路由器和访问服务器必须相同。有效值范围为 1 至 65535。默认值为 10。

  呼叫间隔越小，检测到拓扑更改的速度越快，但会在接口上发送更多流量。
- **传送延迟** - 在接口上发送 LSA 数据包所需的估计时间（以秒为单位）。整数值必须大于零。有效值范围为 1 至 8192。默认值为 1。

  更新数据包中的LSA在传输之前会按此数量递增其自己的年龄。如果在通过链路进行传输之前未添加延迟，则不考虑LSA通过该链路进行传播的时间。分配的值应将接口的传输和传播延迟考虑在内。此设置对于超低速链路意义更大。
- **重新传送间隔** - 属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）：重新传输间隔是连接的网络上任意两个路由器之间的预期往返延迟。该值必须大于预期往返延迟，并且范围可以为 1 至 65535。默认值为 5。

  当一台路由器向其邻居发送LSA时，它将保留该LSA，直至收到确认消息。如果路由器没有接收到确认，则重新发送 LSA。请保守地设置此值，否则可能会产生不必要的重新传输。串行线路和虚拟链路的值应较大。

- **停顿间隔** - 在邻居指示路由器关闭之前呼叫数据包不可见的时间（以秒为单位）。停顿间隔是无符号整数。默认值是呼叫间隔的四倍（或40秒）。对于连接到公用网络的所有路由器和接入服务器，值必须相同。有效值范围为 1 至 65535。
- **身份验证** - 从以下选项中选择 OSPF 虚拟链路身份验证：
  - **无** -（默认）禁用虚拟链路区域身份验证。
  - **区域身份验证** - 使用 MD5 启用区域身份验证。点击**添加**按钮，输入密钥 ID、密钥、确认密钥，然后点击**确定**。
  - **密码** - 为虚拟链路身份验证提供明文密码，在需要考虑安全性的情景下，建议不要选择此选项。
  - **MD5** - 允许 MD5 身份验证。点击**添加**按钮，输入密钥 ID、密钥、确认密钥，然后点击**确定**。

    注释
    确保仅输入数字作为 MD5 密钥 ID。
  - **密钥链** - 允许密钥链身份验证。点击**添加**并创建的密钥链，然后点击**保存**。有关详细操作步骤，请参阅创建密钥链对象。为对等体使用相同的身份验证类型（MD5或密钥链）和密钥 ID 以建立成功的邻接关系。

步骤 13 点击**确定 (OK)** 以保存虚拟链路配置。

步骤 14 点击“路由”页面上的**保存**以保存更改。

下一步做什么

继续配置 OSPF 重新分发。

配置 OSPF 重新分发

Firewall Threat Defense设备可以控制路由在OSPF 路由过程之间的重新分发。将路由从一个路由过程重新分发到 OSPF 路由过程的规则将会显示。可以将 EIGRP、RIP 和 BGP 发现的路由重新分发到 OSPF 路由过程中。还可以将静态路由和已连接路由重新分发到 OSPF 路由过程中。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF**。

步骤 5 从 **OSPF 角色** 下拉列表中，选择角色。

步骤 6 点击 **重新分发** > **添加**。

您可以点击 **编辑** (✎)，或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 7 为每个 OSPF 进程配置以下重新分发选项：

- **OSPF 进程 (OSPF Process)**- 选择进程 ID。对于使用虚拟路由的设备，该下拉列表会显示为所选虚拟路由器生成的唯一进程 ID。
- **路由类型** - 选择下列类型之一：
  - **静态** - 将静态路由重新分发到 OSPF 路由过程。
  - **已连接** - 将已连接路由（通过在接口上启用 IP 地址自动建立的路由）重新分发到 OSPF 路由过程。已连接路由会作为设备的外部路由重新分发。您可以在“可选”列表下选择是否使用子网。
  - **OSPF** - 重新分发来自另一个 OSPF 路由过程（例如内部、外部 1 和 2、NSSA 外部 1 和 2）的路由，或选择是否使用子网。您可以在“可选”列表下选择以下选项。
  - **BGP** - 重新分发来自 BGP 路由过程的路由。添加 AS 编号以及选择是否使用子网。
  - **RIP** - 重新分发来自 RIP 路由过程的路由。您可以在“可选”列表下选择是否使用子网。

    注释
    由于用户定义的虚拟路由器不支持 RIP，因此您无法从 RIP 重新分发路由。

  - **EIGRP**- 重新分发来自 EIGRP 路由进程的路由。添加 AS 编号以及选择是否使用子网。
- **指标值** - 正在分发的路由的指标值。默认值为 10。有效值范围为 0 到 16777214。

  在同一设备上从一个 OSPF 进程重新分发到另一个 OSPF 进程时，如果未指定指标值，则会将指标从一个进程携带至另一个进程。将其他进程重新分发到OSPF进程时，如果未指定指标值，则默认指标为 20。
- **指标类型 (Metric Type)** - 指标类型是与通告到OSPF路由域中的默认路由关联的外部链路类型。可用选项为 1（表示 1 类外部路由）或 2（表示 2 类外部路由）。
- **标签值** - 标签指定附加到 OSPF 本身未使用但可用于在 ASBR 之间传达信息的各外部路由的 32 位十进制值。如果未指定任何内容，则对来自 BGP 和 EGP 的路由使用远程自治系统编号。对于其他协议，将会使用零。有效值为 0 到 4294967295。
- **路由映射** - 检查对于从源路由协议到当前路由协议的路由导入的过滤。如果未指定此参数，则会重新分发所有路由。如果已指定此参数，但未列出路由映射标记，则不会导入任何路由。也可以通过点击 **添加** (+) 来添加新的路由映射。请参阅配置路由映射条目以添加新的路由映射。

步骤 8 点击**确定 (OK)** 以保存重新分发配置。

步骤 9 点击“路由”页上的 **保存**以保存更改。

下一步做什么

继续执行配置 OSPF 区域间过滤，第 11 页。

配置 OSPF 区域间过滤

ABR 类型 3 LSA 过滤扩展了 ABR 的功能，即在不同 OSPF 区域之间运行 OSPF 过滤类型 3 LSA。配置前缀列表后，便会仅将指定的前缀从一个 OSPF 区域发送到另一个 OSPF 区域。所有其他前缀都限用于各自的 OSPF 区域。可以向传入或传出 OSPF 区域的流量或者同时为该区域的传入和传出流量应用此类型的区域过滤。

当前缀列表的多个条目与给定前缀相匹配时，将使用具有最低序列号的条目。为提高效率，可能需要手动为最常用的匹配或拒绝项分配较低的序列号来将其置于列表顶部附近。默认情况下，序列号从 5 开始并以 5 为增量自动生成。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF**。

步骤 5 选择**区域间 (InterArea)** > **添加 (Add)**。

您可以点击 **编辑** ()，或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域间。

步骤 6 为每个 OSPF 进程配置下列区域间过滤选项：

- **OSPF 进程 (OSPF Process)**- 对于使用虚拟路由的设备，下拉列表会列出为所选虚拟路由器生成的唯一进程 ID。
- **区域 ID** - 要汇总其路由的区域。
- **前缀列表** - 前缀的名称。要添加新的前缀列表对象，请参阅步骤 5。
- **流量方向** - 入站或出站。选择 Inbound 以筛选传入 OSPF 区域的 LSA，或者选择 Outbound 以筛选传出 OSPF 区域的 LSA。如果编辑的是现有过滤器条目，则无法修改此设置。

步骤 7 点击 **添加** ()，然后输入新前缀列表的名称，以及是否允许重写。

配置前缀规则之前，必须先配置前缀列表。

步骤 8 点击**添加**以配置前缀规则，并配置以下参数：

- **操作** - 针对重新分发访问，选择**阻止**或**允许**。
- **序列号** - 路由序列号。默认情况下，序列号从 5 开始并以 5 为增量自动生成。
- **IP 地址** - 以 IP 地址/掩码长度格式指定前缀数字。

- **最小前缀长度** -（可选）最小前缀长度。
- **最大前缀长度** -（可选）最大前缀长度。

步骤 9 点击**确定 (OK)** 以保存区域间过滤配置。

步骤 10 点击“路由”页上的 **保存**以保存更改。

下一步做什么

继续执行配置 OSPF 过滤规则，第 12 页。

配置 OSPF 过滤规则

您可以为每个 OSPF 进程配置 ABR 3 类 LSA 过滤器。ABR 3 类 LSA 过滤器仅允许将指定的前缀从一个区域发送到另一个区域，并会限制其他所有前缀。此类型的区域过滤可以应用在特定 OSPF 区域外、应用到特定 OSPF 区域中，或者同时在相同 OSPF 区域的内外进行应用。OSPF ABR 3 类 LSA 过滤可提高对 OSPF 区域之间路由重新分发的控制。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF**。

步骤 5 选择**过滤规则 (Filter Rule)** > **添加 (Add)**。

您可以点击 **编辑** (✎)，或使用右击菜单剪切、复制、粘贴、插入和删除过滤器规则。

步骤 6 为每个 OSPF 进程配置以下过滤规则选项:

- **OSPF 进程 (OSPF Process)**- 对于使用虚拟路由的设备，下拉列表会列出为所选虚拟路由器生成的唯一进程 ID。
- **访问列表** - 针对此 OSPF 进程的访问列表。若要添加新的标准访问列表对象，请点击 **添加** (+) 并参阅配置标准 ACL 对象。
- **流量方向** - 为要过滤的流量方向选择 In 或 Out。选择 In 以过滤传入 OSPF 区域的 LSA，或者选择 Out 以过滤传出 OSPF 区域的 LSA。如果编辑的是现有过滤器条目，则无法修改此设置。
- **接口** - 此过滤规则的接口。

步骤 7 点击**确定**保存过滤规则配置。

步骤 8 点击“路由”页上的 **保存**以保存更改。

下一步做什么

继续执行配置 OSPF 汇总地址，第 13 页。

配置 OSPF 汇总地址

将来自其他协议的路由重新分发到 OSPF 中时，将在外部 LSA 中单独通告每个路由。但是，您可以将 Firewall Threat Defense设备配置为对于为指定网络地址和掩码包含的所有重新分发的路由通告单个路由。此配置可减小 OSPF 链路状态数据库的大小。可以抑制与指定 IP 地址/掩码对相匹配的路由。标记值可用作用于通过路由映射控制重新分发的值。

可以汇总从其他路由协议获知的路由。用于通告汇总的指标是所有较为具体路由的最小指标。汇总路由帮助减小路由表的大小。

对 OSPF 使用汇总路由会导致 OSPF ASBR 将一个外部路由通告为该地址覆盖的所有重新分发的路由的聚合。只能汇总重新分发到 OSPF 中的来自其他路由协议的路由。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF**。

步骤 5 选择**摘要地址 (Summary Address)** > **添加 (Add)**。

可以点击 **编辑** (✎) 进行编辑，或者使用右键点击菜单剪切、复制、粘贴、插入和删除汇总地址。

步骤 6 为每个 OSPF 进程配置以下汇总地址选项：

- **OSPF 进程 (OSPF Process)**- 对于使用虚拟路由的设备，下拉列表会列出为所选虚拟路由器生成的唯一进程 ID。
- **可用网络** - 汇总地址的 IP 地址。从“可用网络”(Address) 列表中选择一项然后点击**添加**，或者要添加新网络，请点击 **添加** (+)。有关添加网络的程序，请参阅网络。
- **标记** - 附加到每个外部路由的 32 位十进制值。OSPF 本身未使用此值，但是其可能用于在 ASBR 之间传达信息。
- **通告 (Advertise)** - 通告摘要路由。取消选中此复选框以抑制属于汇总地址的路由。默认情况下，此复选框为选中状态。

步骤 7 点击**确定 (OK)** 以保存汇总地址配置。

步骤 8 点击“路由”页上的 **保存**以保存更改。

下一步做什么

继续执行配置 OSPF 接口和邻居，第 14 页。

配置 OSPF 接口和邻居

如有必要，您可以更改某些特定于接口的 OSPFv2 参数。无需更改其中任何参数，但是以下接口参数在连接的网络中的所有路由器之间必须一致：呼叫间隔、停顿间隔和身份验证密钥。如果配置其中任何参数，请确保网络上所有路由器的配置都具有兼容值。

您需要定义静态 OSPFv2 邻居来通过点对点非广播网络通告 OSPFv2 路由。通过此功能，您可以跨现有 VPN 连接广播 OSPFv2 通告，而不必将通告封装在 GRE 隧道中。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF**。

步骤 5 选择**接口 (Interface)** > **添加 (Add)**。

您可以点击 **编辑** ()，或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 6 为每个 OSPF 进程配置以下接口选项：

- **接口** - 要配置的接口。

  注释
  如果设备使用的是虚拟路由，则此下拉列表只会显示属于路由器的接口。

- **默认成本** - 通过接口发送数据包的成本。默认值为 10。
- **优先级**-为网络指定的路由器。有效值范围为 0 到 255。默认值为 1。为此设置输入 0 将使路由器不符合成为指定路由器或备用指定路由器的条件。

  当两个路由器连接到网络时，两者均尝试成为指定路由器。具有更高路由器优先级的设备成为指定路由器。如果有绑定，则具有更高路由器 ID 的路由器成为指定路由器。此设置不适用于配置为点对点接口的接口。

- **MTU 忽略 (MTU Ignore)** - OSPF 检查邻居在公用接口上是否使用的是同一 MTU。在邻居交换 DBD 数据包时会执行此检查。如果 DBD 数据包中的接收 MTU 高于传入接口上配置的 IP MTU，则不建立 OSPF 邻接。
- **数据库过滤器** - 使用此设置在同步和泛洪过程中筛选传出 LSA 接口默认情况下，OSPF 会在同一区域中的所有接口上泛洪新 LSA，但 LSA 到达的接口除外。在全网状拓扑中，此泛洪可能会浪费带宽并产生过多的链路和 CPU 使用情况。选中此复选框可防止 OSPF 在所选接口上进行 LSA 泛洪。

- **呼叫间隔** - 用于指定在接口上发送的呼叫数据包之间的间隔（以秒为单位）。有效值的范围为 1-8192 秒。默认值为 10 秒。

  呼叫间隔越小，检测到拓扑更改的速度越快，但会在接口上发送更多流量。此值对于特定接口上的所有路由器和接入服务器都必须相同。

- **传输延迟** - 在接口上发送 LSA 数据包所需的估计时间（以秒为单位）。有效值的范围为 1-65535 秒。默认值为 1 秒。

  更新数据包中的 LSA 在传输之前会按此字段指定的量增大其年龄。如果在通过链路进行传输之前未添加延迟，则不考虑 LSA 通过该链路进行传播的时间。分配的值应将接口的传输和传播延迟考虑在内。此设置对于超低速链路意义更大。

- **重新传送间隔** - 属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）。该时间必须大于连接的网络上任意两个路由器之间的预期往返延迟。有效值的范围为 1 到 65535 秒。默认值为 5 秒。

  当一台路由器向其邻居发送 LSA 时，它将保留该 LSA，直至收到确认消息。如果路由器没有接收到确认，则重新发送 LSA。请保守地设置此值，否则可能会产生不必要的重新传输。串行线路和虚拟链路的值应较大。

- **停顿间隔** - 在邻居表明路由器关闭之前不得查看呼叫数据包的时间段（以秒为单位）：网络上所有节点的值必须相同，范围可以是 1-65535。

- **呼叫乘数** - 指定每秒要发送的呼叫数据包的数量。有效值为 3 - 20.

- **点对点** - 允许您通过 VPN 隧道传输 OSPF 路由。

- **身份验证** - 从以下选项中选择 OSPF 接口身份验证：

  - **无** -（默认）禁用接口身份验证。
  - **区域身份验证** - 使用 MD5 启用接口身份验证。点击**添加**按钮，输入密钥 ID、密钥、确认密钥，然后点击**确定**。
  - **密码** - 为虚拟链路身份验证提供明文密码，在需要考虑安全性的情景下，建议不要选择此选项。
  - **MD5** - 允许 MD5 身份验证。点击**添加**按钮，输入密钥 ID、密钥、确认密钥，然后点击**确定**。

    注释
    只能为 MD5 密钥标识符输入字母、数字和特殊字符。请勿输入空格；空格在管理中心中会被截断。

  - **密钥链** - 允许密钥链身份验证。点击**添加**并创建的密钥链，然后点击**保存**。有关详细操作步骤，请参阅创建密钥链对象。为对等体使用相同的身份验证类型（MD5 或密钥链）和密钥 ID 以建立成功的邻接关系。

- **启用 BFD**-允许您在此接口上启用 BFD。

- **输入密码** - 配置的密码，如果选择“密码”作为身份验证类型。

- **确认密码 (Confirm Password)** - 确认选择的密码。

步骤 7 选择**邻居 (Neighbor)** > **添加 (Add)**。

您可以点击 **编辑** ()，或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 8 为每个 OSPF 进程配置以下参数：

- **OSPF 进程** - 选择1或2。
- **邻居** - 在下拉列表中选择一个邻居，或点击 **添加** () 以添加新的邻居；输入名称、说明、网络、是否允许重写，然后点击**保存**。
- **接口** - 选择与邻居关联的接口。

步骤 9 点击**确定 (OK)** 以保存邻居配置。

步骤 10 点击“路由”页面上的**保存**以保存更改。

配置 OSPF 高级属性

“高级属性”(Advanced Properties) 允许您配置选项，如系统日志消息生成、管理路由距离、LSA 计时器和平稳重启。

平稳重启

Firewall Threat Defense设备可能会遇到一些已知的故障情况，这些故障情况不应影响跨交换平台转发的数据包。不间断转发 (NSF) 功能允许在恢复路由协议信息的同时沿已知路由继续转发数据。当有计划的无中断软件升级时，此功能非常有用。通过使用NSF Cisco（RFC 4811 和 RFC 4812）或 NSF IETF (RFC 3623)，您可以在 OSPFv2 上配置平稳重启。

注释 NSF 功能在 HA 模式和集群中也很有用。

配置 NSF 平稳重启功能涉及两个步骤；配置功能和将设备配置为支持 NSF 功能或 NSF 感知。支持NSF功能的设备可以向邻居表明其自己的重启活动，而支持NSF感知的设备可以帮助重新启动邻居。

根据某些条件，可以将设备配置为支持 NSF 功能的设备或 NSF 感知的设备：

- 设备可以配置为 NSF 感知的设备，而与其所处的模式无关。
- 设备必须处于 Failover 或 Spanned Etherchannel (L2) 集群模式下才能配置为支持 NSF 功能的设备。
- 为使设备支持NSF功能或NSF感知，应将其配置为能够根据需要处理不透明链路状态通告 (LSA)/本地链路信令 (LLS) 块。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF** > **高级设置**。

步骤 5 选择**常规 (General)**，然后配置以下选项：

- **路由器 ID** - 选择自动或手动（对于非集群和跨区以太网通道模式下的集群显示）或集群池（对于单个接口模式下的集群显示）。如果选择 IP 地址，在邻接字段中输入 IP 地址。如果选择集群池，请在相邻的下拉字段中选择 IPv4 集群池值。有关创建集群池地址的信息，请参阅地址池。
- **忽略 LSA MOSPF** - 在路由收到不受支持的 LSA 类型 6 组播 OSPF (MOSPF) 数据包时，抑制系统日志消息。
- **RFC 1583 兼容** - 将 RFC 1583 兼容性配置为用于计算摘要路由成本的方法。在启用了 RFC 1583 兼容性的情况下，可能会出现路由环路。禁用它可以防止路由环路的出现。OSPF 路由域中的所有 OSPF 路由器都应设置相同的 RFC 兼容性。
- **邻接更改** - 定义将导致发送系统日志消息的邻接更改。

  默认情况下，在 OSPF 邻居启动或关闭时会生成系统日志消息。您可以将路由器配置为在 OSPF 邻居关闭时发送一个系统日志消息，并为每个状态发送系统日志。

  - **日志邻接更改** - 使 Firewall Threat Defense设备每当在 OSPF 邻居启动或关闭时都会发送系统日志消息。默认情况下，此设置处于选中状态。
  - **日志邻接更改详细信息** - 使 Firewall Threat Defense设备每当在发生任何状态更改时都会发送系统日志消息，而不只是在邻居启动或关闭时发送。默认情况下，此设置处于未选中状态。
- **管理路由距离**-允许您修改用于为 **区域间**、 **区域内**和 **外部** IPv6 路由配置管理路由距离的设置。管理路由距离是从 1 至 254 的整数。默认值为 110。
- **LSA 组步调设置** - 指定将 LSA 收集到组中并刷新、校验和或老化的间隔（以秒为单位）。有效值范围为 10 到 1800。默认值为 240。
- **启用默认信息来源** - 选中**启用**复选框可将默认外部路由生成到OSPF 路由域中并配置以下选项：
  - **始终通告默认路由** - 确保始终通告默认路由。
  - **指标值 (Metric Value)** - 用于生成默认路由的指标。有效十进制值范围为 0 到 16777214。默认值为 10。
  - **指标类型** - 与通告到 OSPFv3 路由域中的默认路由关联的外部链路类型。有效值为 1（1 类外部路由）和 2（2 类外部路由）。默认为 2 类外部路由。

- **路由映射 (RouteMap)** - 选择在路由映射符合条件时生成默认路由的路由过程，或者点击 **添加** (+) 以添加新路由。请参阅配置路由映射条目以添加新的路由映射。

步骤 6 点击**确定 (OK)** 以保存常规配置。

步骤 7 选择**非停止转发 (Non Stop Forwarding)**，并为支持 NSF 或识别 NSF 的设备配置 OSPFv2 的思科 NSF 平稳重启：

注释
对于 OSPFv2、思科 NSF 和 IETF NSF，存在两种平稳重启机制。一次只能为 OSPF 实例配置其中一种平稳重启机制。支持 NSF 感知的设备既可以配置为思科 NSF 助手，也可以配置为 IETF NSF 助手，但是一次只能在思科 NSF 或 IETF NSF 模式中为 OSPF 实例配置支持 NSF 功能的设备。

a) 选中**启用思科非停止转发功能**复选框。
b) （可选）如果需要，请选中**当检测到无法识别 NSF 的邻居设备时取消 NSF 重启**复选框。
c) （可选）确保取消选中**启用思科非停止转发助手模式**复选框，以便在识别 NSF 的设备上禁用助手模式。

步骤 8 为 OSPFv2 配置思科 IETF NSF 平稳重启（支持 NSF 功能的设备或 NSF 感知的设备）。

a) 选中**启用 IETF 非停止转发功能**复选框。
b) 在**平稳重启间隔的长度 (秒)** 字段中，以秒为单位输入重启间隔。默认值为 120 秒。对于低于 30 秒的重启间隔，将终止平稳重启。
c) （可选）确保取消选中**针对助手模式启用 IETF 非停止转发 (NSF)** 复选框，以便在识别 NSF 的设备上禁用 IETF NSF 助手模式。
d) **启用严格链路状态通告检查** - 启用后，它指示助手路由器在以下情况下将终止重新启动路由器的过程：它检测到 LSA 发生会泛洪至重新启动的路由器的更改，或者在发起平稳重启过程时重新启动的路由器的重新传输列表上有已更改的 LSA。
e) **启用 IETF 非停止转发** - 启用非停止转发，这样将允许在状态切换后恢复路由协议信息时，转发数据包以沿已知路由继续。OSPF 使用 OSPF 协议的扩展来从相邻的 OSPF 设备恢复其状态。要进行恢复，相邻的路由器必须支持 NSF 协议扩展，并愿意充当重启设备的“助手”。邻居还必须继续在进行协议状态恢复时将数据流量转发到正在重启的设备。

配置 OSPFv3

本节介绍配置 OSPFv3 路由进程所涉及的任务。对于使用虚拟路由的设备，只能为其全局虚拟路由器配置 OSPFv3，而不能为其用户定义的虚拟路由器配置 RIP。

配置 OSPFv3 区域、路由摘要和虚拟链路

要启用 OSPFv3，您需要创建 OSPFv3 路由进程，创建 OSPFv3 的区域，启用 OSPFv3 的接口，然后将路由重新分发到目标 OSPFv3 路由进程中。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由 (Routing)**选项卡。在选项卡的左窗格上，点击 **OSPFv3**。

步骤 3 默认情况下，**启用进程 1** 处于选中状态。您最多可以启用两个 OSPF 进程实例。

步骤 4 从下拉列表中选择OSPFv3 角色，并为其输入说明。这些选项是“内部”、“ABR”、“ASBR”以及“ABR 和 ASBR”。有关 OSPFv3 角色的说明，请参阅关于 OSPF，第 1 页。

步骤 5 选择**区域 (Area)** > **添加 (Add)**。

您可以点击 **编辑** ()，或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 6 选择**常规 (General)**，然后为每个 OSPF 进程配置以下选项：

- **区域 ID** - 要汇总其路由的区域。
- **成本** - 汇总路由的指标或开销，它在 OSPF SPF 计算过程中用于确定到达目标的最短路径。有效值范围为 0 到 16777215。
- **类型** - 指定“普通”、“NSSA”或“末节”。如果选择“普通”，则没有其他参数要配置。如果选择“末节”，则可以选择在区域中发送摘要 LSA。如果选择“NSSA”，则可以配置下面的三个选项：
  - **允许将摘要 LSA 发送到该区域** - 允许将摘要 LSA 发送到该区域。
  - **将路由导入到普通和 NSSA 区域**-允许重新分发以将路由导入到正常区域，而不是末节区域。
  - **默认信息源** - 在 OSPFv3 路由域中生成默认的外部路由。
- **指标** - 用于生成默认路由的指标。默认值为 10。有效十进制值范围为 0 到 16777214。
- **指标类型** - 指标类型是与通告到 OSPFv3 路由域中的默认路由关联的外部链路类型。可用选项为 1（表示 1 类外部路由）或 2（表示 2 类外部路由）。

步骤 7 点击**确定 (OK)** 以保存常规配置。

步骤 8 （不适用于内部 OSPFv3 角色）选择 **路由摘要** > **添加路由摘要**。

您可以点击 **编辑** ()，或使用右键点击菜单剪切、复制、粘贴、插入和删除路由摘要。

步骤 9 为每个 OSPF 进程配置以下路由摘要选项：

- **IPv6 前缀/长度** - IPv6 前缀。要添加新的网络对象，请点击 **添加** ()。有关添加网络的过程，请参阅网络。
- **成本** - 汇总路由的指标或开销，它在 OSPF SPF 计算过程中用于确定到达目标的最短路径。有效值范围为 0 到 16777215。

- **通告** - 通告摘要路由。取消选中此复选框以抑制属于汇总地址的路由。默认情况下，此复选框为选中状态。

步骤 10 点击**确定 (OK)** 以保存路由摘要配置。

步骤 11 （不适用于 OSPFv3 角色）选择**虚拟链接 (Virtual Link)**，点击**添加虚拟链接 (Add Virtual Link)**，并为每个 OSPF 进程配置以下选项：

- **对等体路由器 ID (Peer RouterID)** - 选择对等体路由器的 IP 地址。要添加新的网络对象，请点击 **添加** (+)。有关添加网络的过程，请参阅网络。
- **TTL 安全** - 启用 TTL 安全检查。hop-count 的值是一个介于 1 到 254 之间的数字。默认值为 1。

  OSPF 发送使用 IP 报头生存时间 (TTL) 值 255 来发送传出数据包，并丢弃 TTL 值小于可配置阈值的传入数据包。由于转发 IP 数据包的每个设备都会使 TTL 递减，因此通过直接（一跳）连接接收的数据包的值为 255。跨越两跳的数据包的值为 254，以此类推。接收阈值根据数据包可能已移动的最大跳数来配置。
- **停顿间隔** - 在邻居指示路由器关闭之前呼叫数据包不可见的时间（以秒为单位）。默认值是呼叫间隔的四倍（或 40 秒）。有效值范围为 1 到 65535。

  停顿间隔是无符号整数。对于连接到公用网络的所有路由器和接入服务器，值必须相同。
- **呼叫间隔** - 在接口上发送的呼叫数据包的间隔时间（以秒为单位）。有效值范围为 1 到 65535。默认值为 10。

  呼叫数据包间隔是将在呼叫数据包中通告的无符号整数。该值对特定网络上的所有路由器和访问服务器必须相同。呼叫间隔越小，检测到拓扑更改的速度越快，但会在接口上发送更多流量。
- **重新传送间隔** - 属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）：重新传输间隔是连接的网络上任意两个路由器之间的预期往返延迟。该值必须大于预期往返延迟，并且范围可以为 1 至 65535。默认值为 5。

  当一台路由器向其邻居发送 LSA 时，它将保留该 LSA，直至收到确认消息。如果路由器没有接收到确认，则重新发送 LSA。请保守地设置此值，否则可能会产生不必要的重新传输。串行线路和虚拟链路的值应较大。
- **传送延迟** - 在接口上发送 LSA 数据包所需的估计时间（以秒为单位）。整数值必须大于零。有效值范围为 1 到 8192。默认值为 1。

  更新数据包中的 LSA 在传输之前会按此数量递增其自己的年龄。如果在通过链路进行传输之前未添加延迟，则不考虑 LSA 通过该链路进行传播的时间。分配的值应将接口的传输和传播延迟考虑在内。此设置对于超低速链路意义更大。

步骤 12 点击**确定**保存虚拟链路配置。

步骤 13 点击“路由”页面上的**保存**以保存更改。

下一步做什么

继续配置 OSPFv3 重新分发。

配置 OSPFv3 重新分发

Cisco Secure Firewall Threat Defense设备可以控制路由在 OSPF 路由过程之间的重新分发。将路由从一个路由过程重新分发到 OSPF 路由过程的规则将会显示。可以将 EIGRP、RIP 和 BGP 发现的路由重新分发到 OSPF 路由过程中。还可以将静态路由和已连接路由重新分发到 OSPF 路由过程中。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择**路由** > **OSPF**。

步骤 3 选择**重新分发 (Redistribution)** 并点击**添加 (Add)**。

您可以点击 **编辑** ()，或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 4 为每个 OSPF 进程配置以下重新分发选项：

- **源协议** - 从中重新分发路由的源协议。支持的协议为“已连接”、“静态”、“OSPF”和“BGP”。如果选择“OSPF”，则必须在**过程 ID** 字段中输入过程 ID。如果选择“BGP”，则必须在 **AS 编号**字段中添加 AS 编号。
- **指标** - 正在分发的路由的指标值。默认值为 10。有效值范围为 0 到 16777214。

  在同一设备上从一个 OSPF 进程重新分发到另一个 OSPF 进程时，如果未指定指标值，则会将指标从一个进程携带至另一个进程。将其他进程重新分发到OSPF进程时，如果未指定指标值，则默认指标为 20。
- **指标类型 (Metric Type)** - 指标类型是与通告到OSPF路由域中的默认路由关联的外部链路类型。可用选项为 1（表示 1 类外部路由）或 2（表示 2 类外部路由）。
- **标签** - 标签指定附加到 OSPF 本身未使用但可用于在 ASBR 之间传达信息的各外部路由的 32 位十进制值。如果未指定任何内容，则对来自 BGP 和 EGP 的路由使用远程自治系统编号。对于其他协议，将会使用零。有效值为 0 到 4294967295。
- **路由映射** - 选中以过滤从源路由协议到当前路由协议的路由的导入。如果未指定此参数，则会重新分发所有路由。如果已指定此参数，但未列出路由映射标记，则不会导入任何路由。也可以通过点击 **添加** () 来添加新的路由映射。请参阅路由映射了解添加新路由映射的过程。
- **过程 ID** - OSPF 过程 ID，即 1 或 2。

  注释
  过程 ID 已启用，OSPFv3 过程正在重新分发由另一个 OSPFv3 过程获悉的路由。
- **匹配** - 启用要重新分发到其他路由域的 OSPF 路由：
  - **内部**，表示特定自治系统的内部路由。
  - **外部 1**，表示自治系统的外部路由，但会作为 1 类外部路由导入 OSPFv3。
  - **外部 2**，表示自治系统的外部路由，但会作为 2 类外部路由导入 OSPFv3。

- **NSSA 外部 1**，表示自治系统的外部路由，但会在 IPv6 的 NSSA 中作为 1 类外部路由导入到 OSPFv3 中。
- **NSSA 外部 2**，表示自治系统的外部路由，但会在 IPv6 的 NSSA 中作为 2 类外部路由导入到 OSPFv3 中。

步骤 5 点击**确定 (OK)** 以保存重新分发配置。

步骤 6 点击“路由”页上的 **保存**以保存更改。

下一步做什么

继续执行配置 OSPFv3 摘要前缀 ， 第 22 页。

配置 OSPFv3 摘要前缀

您可以配置 Firewall Threat Defense设备以通告与指定的 IPv6 前缀和掩码对匹配的路由。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择**路由** > **OSPFv3** 。

步骤 3 选择**摘要前缀 (Summary Prefix)** > **添加 (Add)**。

您可以点击 **编辑** ()，或使用右键点击菜单剪切、复制、粘贴、插入和删除摘要前缀。

步骤 4 为每个 OSPF 进程配置以下摘要前缀选项：

- **IPv6 前缀/长度** - IPv6 前缀和前缀长度标签。从列表中选择一个或点击 **添加** () 以添加新的网络对象。有关添加网络的过程，请参阅网络。
- **通告** - 通告与指定前缀/掩码对匹配的路由。取消选中此复选框以抑制与指定前缀/掩码对匹配的路由。
- （可选）**标记** - 可用作通过路由映射控制重新分发的匹配值的值。

步骤 5 点击**确定 (OK)** 以保存摘要前缀配置。

步骤 6 点击“路由”页上的 **保存**以保存更改。

下一步做什么

继续执行配置 OSPFv3 接口、身份验证和邻居 ， 第 23 页。

配置 OSPFv3 接口、身份验证和邻居

如有必要，您可以更改某些特定于接口的 OSPFv3 参数。无需更改其中任何参数，但是以下接口参数在连接的网络中的所有路由器之间必须一致：hello-interval 和 dead-interval。如果配置其中任何参数，请确保网络上所有路由器的配置都具有兼容值。

要与 Nexus 交换机成功实现 OSPFv3 身份验证，请确保您拥有兼容版本的交换机，例如 Nexus 3000、7000 和 9000 系列交换机。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择**路由** > **OSPFv3**。

步骤 3 选择**接口 (Interface)** > **添加 (Add)**。

您可以点击**编辑**以进行编辑，或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 4 为每个 OSPFv3 进程配置以下接口选项：

- **接口** - 正在配置的接口。
- **启用 OSPFv3** - 启用 OSPFv3。
- **OSPF 进程** - 选择 1 或 2。
- **区域** - 此进程的区域 ID。
- **实例** - 指定要分配给接口的区域实例 ID。接口只能有一个 OSPFv3 区域。您可以在多个接口上使用同一区域，并且每个接口可以使用不同的区域实例 ID。

步骤 5 选择**属性 (Properties)**，并为每个 OSPFv3 进程配置以下选项：

- **过滤传出链路状态通告** - 过滤到 OSPFv3 接口的传出 LSA。默认情况下，所有传出 LSA 都泛洪至该接口。
- **禁用 MTU 不匹配检测** - 收到 DBD 数据包后，禁用 OSPF MTU 不匹配检测。默认情况下，OSPF MTU 不匹配检测已启用。
- **泛洪减少** - 将普通 LSA 更改为“不老化”LSA，以使它们不会每 3600 秒就出现跨区域泛洪。

  OSPF LSA 每 3600 秒刷新一次。在大型 OSPF 网络中，这可能导致区域间出现大量不必要的 LSA 泛洪。
- **点对点网络** - 允许您通过 VPN 隧道传送 OSPF 路由。当接口配置为点对点非广播时，以下限制适用：
  - 只能为接口定义一个邻居。
  - 需要手动配置邻居。
  - 您无需定义指向加密终端的静态路由。

- 如果通过隧道执行的 OSPF 是在接口上运行，则上游路由器的常规 OSPF 不能在同一接口上运行。
- 在指定 OSPF 邻居之前应将加密映射绑定到接口，以确保通过 VPN 隧道传递 OSPF 更新。如果在指定 OSPF 邻居之后将加密映射绑定到接口，请使用 **clear local-host all** 命令清除 OSPF 连接，以便可以通过 VPN 隧道建立 OSPF 邻接。

- **广播** - 指定接口为广播接口。默认情况下，对于以太网接口会选中此复选框。取消选中此复选框以将接口指定为点对点非广播接口。将接口指定为点对点非广播可以通过VPN隧道传输OSPF路由。
- **成本** - 指定在接口上发送数据包的成本。此设置的有效值范围为 0 至 255。默认值为 1。为此设置输入 0 将使路由器不符合成为指定路由器或备用指定路由器的条件。此设置不适用于配置为点对点非广播接口的接口。

  当两个路由器连接到网络时，两者均尝试成为指定路由器。具有更高路由器优先级的设备成为指定路由器。如果有绑定，则具有更高路由器 ID 的路由器成为指定路由器。
- **优先级** - 确定为网络指定的路由器。有效值范围为 0 到 255。
- **死间隔** - 在邻居表明路由器关闭之前不得查看呼叫数据包的时间段（以秒为单位）：该值必须对于同一网络上的所有节点都相同，并且范围可以是 1 至 65535。
- **Hello 间隔** - 在与邻居建立邻接关系之前，路由器将发送的 OSPF 数据包之间的时间段（以秒为单位）。路由设备检测到活动邻居，呼叫数据包间隔将从轮询间隔中指定的时间更改为呼叫间隔中指定的时间。有效值的范围为 1 到 65535 秒。
- **重新传送间隔** - 属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）。该时间必须大于连接的网络上任意两个路由器之间的预期往返延迟。有效值的范围为 1 到 65535 秒。默认值为 5 秒。
- **传送延迟** - 在接口上发送链路状态更新数据包所需的估计时间（以秒为单位）。有效值的范围为 1 到 65535 秒。默认值为 1 秒。
- **启用 BFD**-允许您在此接口上启用 BFD。

步骤 6 点击**确定 (OK)** 以保存属性配置。

步骤 7 选择**身份验证 (Authentication)**，并为每个 OSPFv3 进程配置以下选项：

- **类型** - 身份验证类型。可用选项为 Area、Interface 和 None。None 选项表示未使用身份验证。
- **安全参数索引** - 从 256 到 4294967295 的一个数字。如果选择“接口”作为类型，请配置此选项。
- **身份验证** - 身份验证算法的类型。支持的值为 SHA-1 和 MD5。如果选择“接口”作为类型，请配置此选项。
- **身份验证密钥** - 使用 MD5 身份验证时，密钥长度必须为 32 位十六进制数字（16 字节）。使用 SHA-1 身份验证时，密钥长度必须为 40 位十六进制数字（20 字节）。
- **加密身份验证密钥** - 启用身份验证密钥的加密。

- **包括加密** - 启用加密。
- **加密算法** - 加密算法的类型。支持的值为 DES。NULL 条目表示不加密。如果选择**包括加密**，请配置此选项。
- **加密密钥** - 输入加密密钥。密钥长度必须是十六进制字符串。使用 AES-256-CBC 身份验证时，密钥长度必须为 130 位十六进制数字。如果选择**包括加密**，请配置此选项。
- **加密密钥** - 使密钥被加密。

步骤 8 点击**确定 (OK)** 以保存身份验证配置。

步骤 9 选择**邻居 (Neighbor)**，点击**添加 (Add)**，并为每个 OSPFv3 进程配置以下选项：

- **链路本地地址** - 静态邻居的 IPv6 地址。
- **成本** - 启用成本。在**成本**字段中输入成本，如果需要通告，请选中**过滤传出链路状态通告**。
- （可选）**轮询间隔** - 启用轮询间隔。以秒为单位输入**优先级**级别和**轮询间隔**。

步骤 10 点击**添加**以添加帐户。

步骤 11 点击**确定 (OK)** 以保存接口配置。

配置 OSPFv3 高级属性

“高级属性”(Advanced Properties) 允许您配置选项，如系统日志消息生成、管理路由距离、被动 OSPFv3 路由、LSA 计时器和平稳重启。

平稳重启

Firewall Threat Defense设备可能会遇到一些已知的故障情况，这些故障情况不应影响跨交换平台转发的数据包。不间断转发 (NSF) 功能允许在恢复路由协议信息的同时沿已知路由继续转发数据。当有计划的无中断软件升级时，此功能非常有用。您可以使用 graceful-restart (RFC 5187) 在 OSPFv3 上配置平稳重启。

注释 NSF 功能在 HA 模式和集群中也很有用。

配置 NSF 平稳重启功能涉及两个步骤；配置功能和将设备配置为支持 NSF 功能或 NSF 感知。支持NSF功能的设备可以向邻居表明其自己的重启活动，而支持NSF感知的设备可以帮助重新启动邻居。

根据某些条件，可以将设备配置为支持 NSF 功能的设备或 NSF 感知的设备：

- 设备可以配置为 NSF 感知的设备，而与其所处的模式无关。
- 设备必须处于 Failover 或 Spanned Etherchannel (L2) 集群模式下才能配置为支持 NSF 功能的设备。

- 为使设备支持NSF功能或NSF感知，应将其配置为能够根据需要处理不透明链路状态通告(LSA)/本地链路信令 (LLS) 块。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择 **路由** > **OSPFv3** > **高级**。

步骤 3 对于 **路由器 ID**，选择自动或手动（对于非集群和跨区以太网通道模式下的集群显示）或集群池（对于单个接口模式下的集群显示）。如果选择 IP 地址，在 **IP 地址** 字段中输入 IPv6 地址。如果选择集群池，请在 **集群池**下拉列表中选择 IPv6 集群池值。有关创建集群池地址的信息，请参阅地址池。

步骤 4 如果您希望在路由收到不受支持的 LSA 类型 6 组播 OSPF (MOSPF) 数据包时抑制系统日志消息，请选中**忽略 LSA MOSPF** 复选框。

步骤 5 选择**常规 (General)**，然后配置以下选项：

- **邻接更改** - 定义将导致发送系统日志消息的邻接更改。

  默认情况下，在OSPF邻居启动或关闭时会生成系统日志消息。您可以将路由器配置为在OSPF邻居关闭时发送一个系统日志消息，并为每个状态发送系统日志。

  - **邻接更改** - 使 Firewall Threat Defense设备每当在 OSPF 邻居启动或关闭时都会发送系统日志消息。默认情况下，此设置处于选中状态。
  - **包括详细信息** - 使 Firewall Threat Defense设备每当在发生任何状态更改时都会发送系统日志消息，而不只是在邻居启动或关闭时发送。默认情况下，此设置处于未选中状态。

- **管理路由距离** - 允许您修改用于为区域间、区域内和外部 IPv6 路由配置管理路由距离的设置。管理路由距离是从 1 至 254 的整数。默认值为 110。
- **默认信息来源** - 选中**启用**复选框可将默认外部路由生成到 OSPFv3 路由域中并配置以下选项：
  - **始终通告** - 将会始终通告默认路由（无论其是否存在）。
  - **指标** - 用于生成默认路由的指标。有效十进制值范围为 0 到 16777214。默认值为 10。
  - **指标类型** - 与通告到 OSPFv3 路由域中的默认路由关联的外部链路类型。有效值为 1（1 类外部路由）和 2（2 类外部路由）。默认为 2 类外部路由。
  - **路由地图 (Route Map)** - 选择在路由映射符合条件时生成默认路由的路由过程，或者点击**添加** (+) 以添加新路由。请参阅路由映射以添加路由映射。

步骤 6 点击**确定 (OK)** 以保存常规配置。

步骤 7 选择**被动接口 (Passive Interface)**，从“可用接口”(Available Interfaces) 列表中选择要在其上启用被动 OSPFv3 路由的接口，然后点击**添加 (Add)** 将它们移动到“选定的接口”(Selected Interfaces) 列表中。

备用路由帮助控制 OSPFv3 路由信息的通告并禁用在接口上发送和接收 OSPFv3 路由更新。

步骤 8 点击**确定 (OK)** 以保存被动接口配置。

步骤 9 选择**计时器 (Timer)**，并配置以下 LSA 步调设置和 SPF 计算计时器：

- **到达** - 指定前后两次接受从邻居到达的同一 LSA 之间必须经过的最小延迟（以毫秒为单位）。范围是从 0 到 6000,000 毫秒。默认值为 1000 毫秒。
- **泛洪步调设置** - 指定泛洪队列中的 LSA 在两次更新之间定步的时间（以毫秒为单位）。可配置范围是从 5 到 100 毫秒。默认值为 33 毫秒。
- **组步调设置** - 指定将 LSA 收集到组中并刷新、校验和或老化的间隔（以秒为单位）。有效值范围为 10 到 1800。默认值为 240。
- **重新传输步调设置** - 指定重新传输队列中 LSA 设置步调的间隔时间（以毫秒为单位）。可配置范围是从 5 到 200 毫秒。默认值为 66 毫秒。
- **LSA 调速** - 指定生成第一次出现的 LSA 时的延迟（以毫秒为单位）。默认值为 0 毫秒。最小值指定发起同一 LSA 所需的最小延迟（以毫秒为单位）。默认值为 5000 毫秒。最大值指定发起同一 LSA 所需的最大延迟（以毫秒为单位）。默认值为 5000 毫秒。

  注释
  对于 LSA 调速，如果最短或最长时间小于第一次出现的值，则 OSPFv3 会自动更正为第一次出现的值。同样，如果指定的最大延迟小于最小延迟，则 OSPFv3 会自动更正为最小延迟值。

- **SPF 调速** - 指定接收对 SPF 计算的更改所需的延迟（以毫秒为单位）。默认值为 5000 毫秒。最小值指定第一次和第二次 SPF 计算之间的延迟（以毫秒为单位）。默认值为 10000 毫秒。最大值指定 SPF 计算的最长等待时间（以毫秒为单位）。默认值为 10000 毫秒。

  注释
  对于 SPF 调速，如果最短或最长时间小于第一次出现的值，则 OSPFv3 会自动更正为第一次出现的值。同样，如果指定的最大延迟小于最小延迟，则 OSPFv3 会自动更正为最小延迟值。

步骤 10 点击**确定 (OK)** 以保存 LSA 计时器配置。

步骤 11 选中**非停止转发 (Non Stop Forwarding)**，并选中**启用稳定重启助手 (Enable graceful-restart helper)** 复选框。默认情况下，此复选框处于选中状态。取消选中此复选框将在支持 NSF 感知的设备上禁用平稳重启助手模式。

步骤 12 选中**启用链路状态通告**复选框以启用严格链路状态通告检查。

启用后，它指示助手路由器在以下情况下将终止重新启动路由器的过程：它检测到 LSA 发生会泛洪至重新启动的路由器的更改，或者在发起平稳重启过程时重新启动的路由器的重新传输列表上有已更改的 LSA。

步骤 13 选中**启用稳定重启 (配置了跨区集群或故障切换时使用)**，然后以秒为单位输入稳定重启间隔。范围为 1-1800。默认值为 120 秒。对于低于 30 秒的重启间隔，将终止平稳重启。

步骤 14 点击**确定 (OK)** 以保存平稳重启配置。

步骤 15 点击“路由”页面上的**保存**以保存更改。

OSPF 的历史记录

表 *1: OSPF* 的功能历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
OSPF v2 和 v3 的 BFD 支持	7.4	7.4	您可以在 OSPFv2 和 OSPFv3 接口上启用 BFD。 新增/修改的菜单项： • 配置 > 设备设置 > 路由 > **OSPFv2** • 配置 > 设备设置 > 路由 > **OSPFv3**

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。

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。

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。