RIP

本章介绍如何配置 威胁防御，以使用路由信息协议 (RIP) 来路由数据、执行身份验证以及重新分发路由信息。对于使用虚拟路由的设备，只能为其全局虚拟路由器配置 RIP，不能为其用户定义的虚拟路由器配置 RIP。

关于 RIP

路由信息协议 (RIP) 是所有路由协议中最常见的协议。RIP 有四基本组成部分：路由更新过程、RIP 路由指标、路由稳定性和路由计时器。支持 RIP 的设备将定期以及在网络拓扑更改时发送路由更新消息。这些 RIP 数据包包括有关设备可到达的网络的信息，以及数据包必须经过才能到达目标地址的路由器或网关的数量。RIP 产生的流量比 OSPF 多，但更易于配置。

RIP 是一种使用跳数作为路径选择指标的距离矢量路由协议。当在某接口上启用 RIP 时，该接口会交换与相邻设备的 RIP 广播，以动态了解和通告路由。

Cisco Secure Firewall Threat Defense 设备支持 RIP 版本 1 和 RIP 版本 2。RIP 版本 1 不通过路由更新发送子网掩码。RIP 版本 2 通过路由更新发送子网掩码，并支持可变长度的子网掩码。此外，交换路由更新时，RIP 版本 2 支持邻居身份验证。此身份验证可确保 Cisco Secure Firewall Threat Defense 设备从受信任的源接收可靠的路由信息。

RIP 比静态路由更有优势，因为初始配置比较简单，并且您不需要在拓扑更改时更新配置。RIP 的缺点是网络和处理开销比静态路由大。

路由更新过程

RIP 会定期以及在网络拓扑更改时发送路由更新消息。当路由器接收到包含对某个条目的更改的路由更新时，它将更新其路由表以反映新路由。路径的指标值增加 1，而发送器被指示为下一跳。RIP 路由器只维护到目标的最佳路由（指标值最低的路由）。更新其路由表后，路由器立即开始传输路由更新，以将此更改通知到其他网络路由器。这些更新独立于 RIP 路由器发送的定期计划更新发送。

RIP 路由指标

RIP 使用单个路由指标（跃点数）来测量源和目标网络之间的距离。从源到目标的路径中的每个跃点都分配了跃点数值，通常为 1。当路由器接收到包含新的或已更改的目标网络项的路由更新时，路由器会向更新中指示的指标数值增加 1，并将网络输入到路由表中。发送器的 IP 地址被用作下一个跃点。

RIP 稳定性功能

RIP 通过对源到目标的路径中允许的跃点数施加限制，防止无限期地执行路由循环。路径中的最大跃点数量为 15 个。如果路由器接收到包含新项或已更改项的路由更新，并且如果将跃点数增加 1 会导致跃点数无穷大（即 16），则认为网络目标不可访问。此稳定性功能的缺点是，它将 RIP 网络的最大直径限制为少于 16 个跃点。

RIP 具有许多其他路由协议所共有的一些稳定性功能。这些功能旨在提供稳定性，尽管网络拓扑可能会发生快速变化。例如，RIP 实施水平分割和抑制机制，以防止传播不正确的路由信息。

RIP 计时器

RIP 使用多个计时器来调节性能。以下是 RIP 的计时器阶段：

- 更新 - 路由更新计时器会记录定期路由更新之间的时间间隔。这是设备发送路由更新的频率。通常情况下，此间隔设置为30秒，每次计时器复位会随机增加少量的时间。这样做是为了防止由所有路由器同时试图更新邻居而造成的拥塞。
- 无效 - 每个路由表条目都有一个与之关联的路由超时计时器。这是设备自上次收到有效更新以来经过的秒数。路由超时计时器过期后，路由将被标记为无效，但会保留在表中，直到路由刷新计时器过期。此计时器到期后，路由将进入抑制状态。默认值为 3 分钟（180 秒）。
- 抑制 - 抑制周期是指系统在接受处于抑制状态的路由（即已标记为无效的路由）的任何新更新之前等待的秒数。默认值为 3 分钟（180 秒）。
- 刷新 - 路由刷新计时器是指从系统收到上次有效更新到路由被丢弃并从路由表中删除之前所经过的秒数。默认值为 240 秒（4 分钟）。

例如，当相邻路由器上的接口关闭时，系统不会再从相邻路由器接收路由更新。此时，无效和刷新计时器会开始计数。在前 180 秒内，什么都不会发生。180 秒后，无效计时器到期，从而让路由无效，同时抑制计时器启动并将路由额外保持60秒。如果仍然没有关于相邻路由器上的接口状态的更新（即它仍处于关闭状态），则该路由会进入刷新状态，其中系统从上次更新开始总共等待了 240 秒（无效计时器等待了 180 秒，抑制计时器等待了 60 秒），系统将刷新路由。即使相邻路由器的接口立即启动，系统也不会接受路由更新，直到抑制计时器完成剩余的 120 秒。

RIP 的要求和前提条件

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

RIP 准则

IPv6 准则

不支持 IPv6。

其他准则

以下信息仅适用于 RIP 版本 2：

- 如果适用邻居身份验证，则在为接口提供 RIP 版本 2 更新的所有邻居设备上，身份验证密钥和密钥 ID 都必须相同。
- 通过 RIP 版本 2，Cisco Secure Firewall Threat Defense 设备 将使用组播地址 224.0.0.9 传输和接收默认路由更新。在被动模式下，它将在该地址接收路由更新。
- 在接口上配置 RIP 版本 2 时，将在该接口上注册组播地址 224.0.0.9。在从接口上删除 RIP 版本 2 配置时，将取消注册该组播地址。

限制

- Cisco Secure Firewall Threat Defense 设备 不能在两个接口之间传递 RIP 更新。
- RIP 版本 1 不支持可变长度的子网掩码。
- RIP 的最大跳数为 15。跳数大于 15 的路由将被视为无法访问。
- 与其他路由协议相比，RIP 融合的速度相对较慢。
- 只能在 Cisco Secure Firewall Threat Defense 设备上启用单个 RIP 进程。

配置 RIP

RIP 是一种使用跳数作为路径选项指标的距离矢量路由协议。

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**。

步骤 3 从目录中选择 **RIP**。

步骤 4 选中 **启用 RIP** 复选框以配置 RIP 设置。

步骤 5 从 **RIP 版本** 下拉列表中选择用于发送和接收 RIP 更新的 RIP 版本。

步骤 6 （可选）选中 **生成默认路由** 复选框，以根据您指定的路由映射生成用于分发的默认路由。

a) 在**路由映射**字段中，指定要用于生成默认路由的路由映射名称。
当在**路由映射**字段中指定的路由映射存在时，将生成默认路由 0.0. 0.0/0 以便通过特定接口进行分发。

步骤 7 当发送和接收版本 2 为所选的 RIP 版本时，**启用自动摘要**选项将可用。选中 **启用自动摘要** 复选框后，将启用自动路由汇总。如果您必须在已断开连接的子网之间执行路由，则禁用自动汇总。当禁用自动汇总时，会通告子网。

注释
RIP 版本 1 始终使用自动汇总，您无法将其禁用。

步骤 8 点击 **Networks**。定义一个或多个用于 RIP 路由的网络。输入 IP 地址，或者输入或选择所需的网络/主机对象。可添加到安全设备配置的网络数量没有限制。属于此命令定义的网络的任何接口都将参与 RIP 路由过程。RIP 路由更新仅通过指定网络上的接口发送和接收。此外，如果未指定接口的网络，则在不会在任何 RIP 更新中通告该接口。

注释
RIP 仅支持 IPv4 对象。

步骤 9 （可选）点击**被动接口 (Passive Interface)**。使用此选项可以指定设备上的被动接口，以及通过扩展指定主动接口。该设备监听被动接口上的 RIP 路由广播，使用该信息填充其路由表，但不在被动接口上广播路由更新。未指定为被动的接口会接收和发送更新。

步骤 10 点击**重新分发 (Redistribution)** 可管理重新分发路由。这些路由将从其他路由进程重新分发到 RIP 路由进程。

a) 点击**添加**以指定重新分发路由。

b) 在 **协议** 下拉列表中选择要重新分发到 RIP 路由进程中的路由协议。

注释
对于 OSPF 协议，指定进程 ID。类似地，指定 BGP 的 AS 路径。在**协议**下拉列表中选择“已连接”选项时，可以将直接连接的网络重新分发到 RIP 路由进程中。

c) （可选）如果要将OSPF路由重新分发到RIP路由进程，可以在**匹配**下拉列表中选择要重新分发的特定类型的 OSPF 路由。按住 Ctrl 键并点击以选择多个类型：

- **内部** - 重新分发自治系统 (AS) 内部的路由。
- **外部 1** - 重新分发 AS 外部的类型 1 路由。
- **外部 2** - 重新分发 AS 外部的类型 2 路由。
- **NSSA 外部 1** - 重新分发末节区域 (NSSA) 外部的类型 1 路由。
- **NSSA 外部 2** - 重新分发 NSSA 外部的类型 2 路由

注释
默认设置为匹配内部、外部 1 和外部 2

d) 在**指标**下拉列表中选择要应用于重新分发的路由的 RIP 指标类型。两个选择包括：

- **透明** – 使用当前路由指标
- **指定的值** - 分配特定的指标值。在**指标值**字段中输入一个特定的值（从 0 到 16）。
- **无** - 不指定指标。不将任何指标值应用于重新分发的路由。

注释
无选项仅适用于静态和已连接协议。

e) （可选）在**路由映射**字段中输入必须满足的路由映射的名称，然后才能将路由重新分发到RIP路由进程中。只有当 IP 地址与路由映射地址列表中的允许语句匹配时，才会重新分发路由。要创建新的路由映射对象，请点击**添加**(+)。请参阅程序的配置路由映射条目以添加新的路由映射。

f) 点击**确定 (OK)**。

步骤 11 （可选）点击**过滤 (Filtering)** 以管理 RIP 策略的过滤器。在本部分中，过滤器用于避免通过接口路由更新、控制路由更新中的路由通告、控制路由更新的处理以及过滤路由更新的源。

a) 点击**添加**添加 RIP 选项。

b) 在**流量方向**字段中，选择要过滤的流量类型：入站或出站。

注释
如果流量方向为入站，则只能定义接口过滤器。

c) 通过在**过滤方式 (Filter On)** 字段中进行相应的选择，指定过滤器是基于“接口”(Interface) 还是“路由”(Route)。如果点击 **接口**，则输入或选择要过滤其路由更新的接口的名称。如果点击 **路由**，则选择路由类型：

- **静态** - 仅过滤静态路由。
- **已连接** - 仅过滤连接的路由。
- **OSPF** - 仅过滤由指定的 OSPF 进程发现的 OSPFv2 路由。输入要过滤的 OSPF 进程的进程 ID。
- **BGP** - 仅过滤由指定的 BGP 进程发现的 BGPv4 路由。输入要过滤的 BGP 进程的 AS 路径。

d) 在 **访问列表** 字段中，输入或选择定义要在 RIP 路由通告中允许或删除的网络的一个或多个访问控制列表 (ACL) 的名称。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。

e) 点击**确定 (OK)**。

步骤 12 （可选）点击**广播 (Broadcast)** 以添加或编辑接口配置。使用“广播”，可以覆盖要按接口发送或接收的全局 RIP 版本。如果要实施身份验证以确保有效的 RIP 更新，则还可以定义每个接口的身份验证参数。

a) 点击**添加**添加接口配置。

b) 在 **接口** 字段中输入或选择在此设备上定义的接口。

c) 在“发送”选项中，选择相应的框以指定使用 RIP **版本 1** 和/或**版本 2** 发送更新。这些选项使您可以为指定的接口覆盖指定的全局发送版本。

d) 在“接收”选项中，选择相应的框以指定使用 RIP **版本 1** 和/或**版本 2** 接受更新。这些选项使您可以为指定的接口覆盖指定的全局接收版本。

e) 选择此接口上用于 RIP 广播的**身份验证**。

- **无** - 无身份验证
- **MD5** - 使用 MD5
- **清除文本** - 使用明文身份验证

如果选择 MD5 或明文，则还必须提供以下身份验证参数。

- **密钥 ID** - 身份验证密钥的 ID。有效值为 0 至 255。
- **密钥** - 所选身份验证方法使用的密钥。最多可以包含 16 个字符。
- **确认** - 再次输入身份验证密钥以进行确认

f) 点击**确定 (OK)**。

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。