策略型路由

本章介绍如何通过 管理中心 的策略型路由页面来配置 威胁防御 以支持策略型路由 (PBR)。以下部分介绍策略型路由、PBR 的准则和 PBR 的配置。

关于策略型路由

在传统路由中，数据包会根据目的 IP 地址进行路由。但是，在基于目标的路由系统中更改特定流量的路由是较为困难的。策略型路由 (PBR) 通过扩展和补充路由协议提供的现有机制来增强对路由的控制。

PBR 允许您设置 IP 优先。它还允许为某些流量指定路径，例如高成本链路上的优先级流量。通过 PBR，您可以定义基于目的网络以外的标准的路由，如源端口、目的地址、目的端口、协议、应用程序，或者这些对象的组合。

您可以使用 PBR 根据应用、用户名、组成员身份和安全组关联对网络流量进行分类。此路由方法适用于大量设备访问大型网络部署中的应用和数据的场景。传统上，大型部署具有会将所有网络流量作为基于路由的 VPN 中的加密流量回传到集线器的拓扑。这些拓扑通常会导致诸如数据包延迟、带宽降低和数据丢包等问题。克服这些问题涉及高成本的复杂部署和管理。

PBR 策略让您能够安全地中断指定应用的流量。您可以在 Cisco Secure Firewall Management Center 用户界面中配置 PBR 策略，以允许直接访问应用。

为什么使用策略型路由

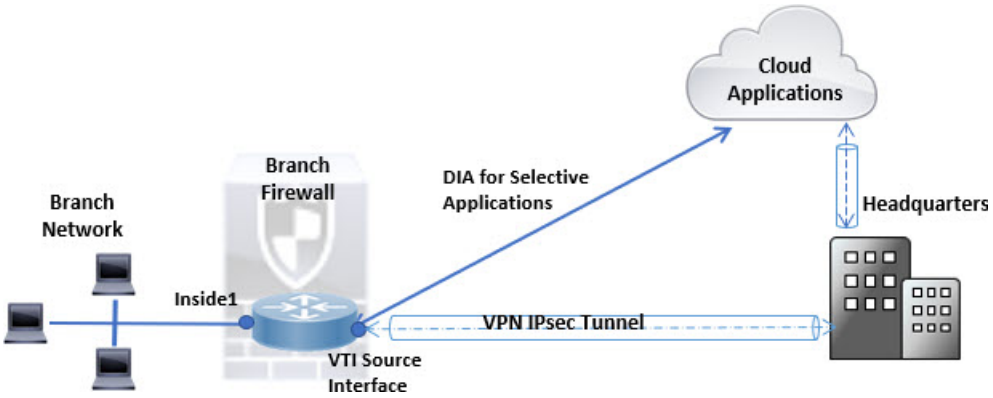
假设一家公司在不同位置之间有两条链路：一条是高带宽、低延迟、较为昂贵的链路，而另一条是低带宽、高延迟、不太昂贵的链路。使用传统路由协议时，高带宽链路将基于通过该链路的带宽、延迟或两者（使用 EIGRP 或 OSPF）特性所实现的指标节约而获得大部分（如果不是全部）跨该链

路发送的流量。通过PBR，您可以通过高带宽/低延迟的链路来路由优先级较高的流量，而通过低带宽/高延迟链路发送其他所有流量。

以下是您可以使用策略型路由的几种场景：

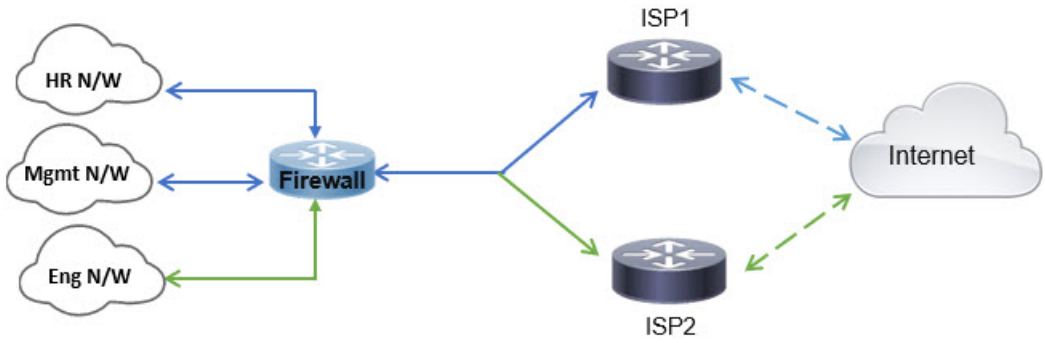
直接互联网接入

在此拓扑中，来自分支机构的应用流量可以被直接路由到互联网，而不是通过连接到总部的VPN隧道。该分支机构 威胁防御 配置了互联网出口点，并在入口接口（内部 *1*）上应用 PBR 策略，以便根据 ACL 中定义的应用、用户身份（用户名和组成员身份）和安全组标记（安全组关联）来识别流量。相应地，流量会通过出口接口直接转发到互联网或 IPsec VPN 隧道。



同等访问权限和源敏感路由

在此拓扑中，来自 HR 和管理管理网络的流量可配置为通过 ISP-1，来自工程网络的流量可配置为通过 ISP-2。因此，策略型路由支持网络管理员提供同等访问权限和源敏感路由，如下所示。



负载分担

除 ECMP 负载均衡提供的动态负载共享功能外，网络管理员现在还可以实施策略来根据流量特征在多个路径之间分发流量。

例如，在同等访问和基于源的路由场景所描绘的拓扑中，管理员可以配置策略型路由来路由从人力资源网络至 ISP1 的流量和从工程网络至 ISP2 的流量，从而实现负载共享。

策略型路由的准则和限制

防火墙模式指导原则

PBR 仅在路由防火墙模式下受支持。

设备准则

- PBR 至 管理中心 的“策略型路由”(Policy Based Routing) 页面仅在 Cisco Secure Firewall Threat Defense 7.1 及更高版本的设备上受支持。虽然 Cisco Secure Firewall Management Center 版本 7.1 支持 7.1 之前版本的 威胁防御，但您无法使用策略型路由页面在此类设备上启用 PBR。
- 仅从 Cisco Secure Firewall Management Center 版本 7.4 以及 Cisco Secure Firewall Threat Defense 版本 7.4 及更高版本的设备上支持使用身份和 SGT 配置 ACL 的PBR 。
- FlexConfig 仅被用于在 管理中心 中为版本 7.1 之前的 威胁防御 配置 PBR。您仍然可以在版本 7.1 前的版本中中使用 FlexConfig 来配置 PBR。
- 不支持在集群设备上配置基于 PBR 策略的应用、用户身份和安全组标记 (SGT)。

接口指导原则

- 只有属于全局虚拟路由器的路由接口和非管理专用接口才能被配置为入口或出口接口。
- 用户定义的虚拟路由器不支持 PBR。
- 只能在策略中定义具有逻辑名称的接口。
- 静态 VTI 只能被配置为出口接口。
- 在继续进行配置之前，请确保每个会话的入口和出口流量流经同一面向 ISP 的接口，以避免路由不对称导致的意外行为，尤其是在使用 NAT 和 VPN 时。

IPv6 支持

PBR 支持 IPv6。

基于应用的 PBR 和 DNS 配置

- 基于应用的 PBR 使用 DNS 监听进行应用检测。仅当 DNS 请求以明文格式通过 威胁防御 时，应用检测才会成功； DNS 流量不会被加密。
- 您必须配置信任的 DNS 服务器。

有关配置 DNS 服务器的详细信息，请参阅DNS。

未对输出路由查询应用的 PBR 策略

基于策略的路由是一种仅入口功能；也就是说，它仅会应用于新传入连接的第一个数据包，并在此时选择连接转发支路的出口接口。请注意，如果传入数据包属于现有连接，则不会触发 PBR，或者已应用 NAT，则 NAT 选择出口接口。

PBR 策略不适用于初期流量

注释　初期连接是指源与目标之间尚未完成必要握手的连接。

在添加新的内部接口并使用唯一地址池来创建新的VPN策略时，PBR将应用于与新客户端池的源匹配的外部接口。因此，PBR 会将流量从客户端发送到新接口上的下一跳。但是，PBR 不会涉及从尚未与新内部接口建立连接的主机到客户端的返回流量。因此，从主机到VPN客户端的返回流量（具体而言，VPN 客户端响应）会由于缺少有效路由而被丢弃。必须在内部接口上配置具有更高指标的加权静态路由。

基于 HTTP 的路径监控指南

- 物理接口、端口通道接口、子接口和静态隧道接口支持基于 HTTP 的路径监控。它在集群设备上不受支持。
- 从管理中心配置基于 HTTP 的应用监控的选项仅限于 7.4 威胁防御设备。
- HTTP 仅使用 IPv4 对应用执行 ping 操作。IPv4 指标用于路由和转发 IPv4 和 IPv6 流量。
- 默认情况下， Cisco Secure Firewall Management Center 版本 7.4 启用基于 HTTP 的应用监控。但是，从以前的版本升级时，默认情况下不启用此选项。您必须手动启用它。

其他规定

- 路由映射的所有现有配置限制和局限性都将继续适用。
- 在为策略匹配条件定义ACL时，您可以从预定义应用列表中选择多个应用，以形成访问控制条目 (ACE)。在 威胁防御 中，预定义应用会被作为网络服务对象进行存储，而应用组会作为网络服务组 (NSG) 进行存储。最多可以创建 1024 个此类 NSG。应用或网络服务组会通过第一个数据包分类来检测。目前，您无法添加或修改预定义应用列表。

路径监控

路径监控（在接口上配置）会派生指标，例如往返时间 (RTT)、抖动、平均意见得分 (MOS) 和每个接口的丢包。这些指标会被用于确定路由 PBR 流量的最佳路径。

基于 ICMP 的路径监控

接口上的指标会使用 ICMP 探测消息动态收集到接口的默认网关或指定的远程对等体。

基于 HTTP 的路径监控

路径监控可计算每个接口的多个远程对等体的灵活指标。要通过分支机构防火墙上的策略监控和确定多个应用的最佳路径，由于以下原因，HTTP 优先于 ICMP：

- HTTP-ping 可以派生到服务器的应用层的路径的性能指标，其中应用托管。
- 由于跟踪的是应用域而不是 IP 地址，因此无需在应用服务器 IP 地址更改时更改防火墙配置。

注释 可以在同一接口上同时配置 ICMP 和 HTTP。如果策略中的目的地与任何域 IP 匹配，则使用相应的指标。如果目的地与任何已配置的域都不匹配，则 PBR 将使用 ICMP 中的指标来选择传出接口。

默认监控计时器

对于指标收集和监控，使用以下计时器：

- 接口监控的平均间隔时间为 30 秒。此间隔时间表示探测平均值的频率。
- 接口监控器更新间隔时间为30秒。此时间间隔表示计算所收集的值的平均值并使其可用于PBR以确定最佳路由路径的频率。
- ICMP 的接口监控器探测间隔时间为一秒。此间隔时间表示发送 ICMP ping 的频率。
- HTTP 的应用监控探测间隔为 10 秒。此间隔时间表示发送 HTTP ping 的频率。路径监控使用 HTTP ping 的最后 30 个样本来计算平均指标。

注释 您不能配置或修改任何计时器的间隔时间。

PBR 和路径监控

在 PBR 中，流量通常会根据出口接口上配置的优先级值（接口成本）进行转发。从管理中心版本 7.2，PBR 使用基于 IP 的路径监控来收集出口接口的性能指标（RTT、抖动、丢包和 MOS）。PBR 会使用指标来确定转发流量的最佳路径（出口接口）。路径监控会定期向 PBR 通知其指标已更改的受监控接口。PBR 会从路径监控数据库中检索受监控接口的最新指标值，并更新数据路径。

您必须为接口启用路径监控并配置监控类型。PBR 策略页面允许您为确定路径指定所需的指标。参阅配置基于策略的路由策略，第 7 页。

PBR 和基于 HTTP 的路径监控

从管理中心版本 7.4 开始，可以将 PBR 配置为使用基于 HTTP 的路径监控来收集应用域的性能指标，而不仅仅是一个目的 IP 地址。配置基于 HTTP 的应用监控后，路径监控不会立即开始监控。仅当某个域的 DNS 条目被监听时，它才会开始监控。使用有关域的已解析 IP 的信息，它会分别发送和接收 HTTP 请求和响应。当 DNS 解析单个域的多个 IP 地址时，第一个解析的 IP 地址将用于探测和监控应用。它会继续监控，直到 IP 地址更改或基于 HTTP 的路径监控被禁用。

根据 HTTP 请求和响应持续时间，路径监控计算应用的性能指标。收集的指标会定期转发到 PBR，以便为配置的入口接口产生的流量做出路由和转发决策。如果流量在路径监控可以将其指标发送到 PBR 之前到达，则流量将遵循路由表选择的路径。对于路径监控指标可用后到达的后续流量，PBR 会根据指标应用其路由决策并转发流量。

注释 根据策略的匹配 ACL 中的网络服务组，您可以对具有多个 IP 地址的多个域应用 PBR。

在基于 HTTP 的应用路径监控中，仅当 PBR 配置满足以下条件时，管理中心才会将应用/NSG 关联到出口接口：

- 匹配 ACL 包含受监控的应用。
- 使用以下任一接口排序值（度量类型）配置 PBR 策略：
  - 最小抖动
  - 最大平均意见得分
  - 最短往返时间
  - 最小丢包率

配置路径监控设置

PBR 策略依靠灵活的指标（例如往返时间（RTT），抖动，平均意见评分（MOS）和接口丢包）来确定流量的最佳路由路径。路径监控收集指定接口上的这些指标。在**接口 (Interfaces)** 页面上，可以使用路径监控设置配置接口，以发送用于指标收集的 ICMP 探测或 HTTP ping。

过程

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 威胁防御 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 **路径监控 (Path Monitoring)** 选项卡。

步骤 4 要配置基于 ICMP 的接口监控，请点击**启用基于 IP 的监控 (Enable IP based Monitoring)** 复选框。

步骤 5 从 **监控类型** 下拉列表中，选择相关选项：

- **自动**-将 ICMP 探测发送到接口的 IPv4 默认网关。如果 IPv4 网关不存在，路径监控会将探测发送到接口的 IPv6 默认网关。
- **对等体 IPv4 (Peer IPv4)** - 将 ICMP 探测发送到指定的对等 IPv4 地址（下一跳 IP）以进行监控。如果选择此选项，请在**要监控的对等体 (Peer IP To Monitor)** 字段中输入 IPv4 地址。
- **对等体 (Peer IPv6)** - 将 ICMP 探测发送到指定的对等 IPv6 地址（下一跳 IP）以进行监控。如果选择此选项，请在**要监控的对等体 (Peer IP To Monitor)** 字段中输入 IPv6 地址。

- **自动 IPv4**-将 ICMP 探测发送到接口的默认 IPv4 网关。
- **自动 IPv6**-将 ICMP 探测发送到接口的默认 IPv6 网关。

注释
- 自动选项不适用于 VTI 接口。您必须指定对等体地址。
- 只有一个下一跳被监控到目的地。也就是说，不能为一个接口指定多个对等体地址。

步骤 6 默认情况下，**启用基于 HTTP 的应用监控 (Enable HTTP based Application Monitoring)** 复选框处于选中状态。如果此接口配置为策略中的出口接口，则列出在 PBR 策略的匹配 ACL 中选择用于路径监控的所有应用。要禁用基于 HTTP 的接口监控，请清除此复选框。

注释 在升级到管理中心 7.4 期间，默认情况下不会启用**启用基于 HTTP 的应用监控 (Enable HTTP based Application Monitoring)**。您必须选中此复选框才能启用它。

步骤 7 点击 **确认**，要保存设置，点击 **保存**。

配置基于策略的路由策略

您可以通过指定入口接口，匹配条件（扩展访问控制列表）和出口接口，在“策略型路由”(Policy Based Routing) 页面中配置 PBR 策略。

开始之前

要使用路径监控指标配置出口接口上的流量转发优先级，必须为接口配置路径监控设置。请参阅配置路径监控设置，第 6 页。

过程

步骤 1 依次选择 **设备** > **设备管理**，并且编辑 威胁防御 设备。

步骤 2 点击**路由**。

步骤 3 点击**策略型路由**。

“策略型路由”页面显示配置的策略。网格显示入口接口列表以及策略型路由访问列表和出口接口的组合。

步骤 4 要配置策略，请点击 **添加**。

步骤 5 在 **添加策略型路由** 对话框中，从下拉列表中选择 **入口接口** 。

注释 下拉列表中仅列出具有逻辑名称且属于全局虚拟路由器的接口。

步骤 6 要在策略中指定匹配条件和转发操作，请点击 **添加**。

步骤 7 在 **添加转发操作** 对话框中，执行以下操作：

a) 从 **Match ACL** 下拉列表中，选择扩展访问控制列表对象。您可以预定义 ACL 对象（请参阅配置扩展 ACL 对象）或点击 **添加**（＋） 图标创建对象。在**新建扩展访问列表对象 (New Extended Access List Object)** 框中，输入名称，点击**添加 (Add)** 以打开**添加扩展访问列表条目 (Add Extended Access List Entry)** 对话框，您可以在其中为 PBR 策略定义网络，端口、用户身份、SGT 或应用匹配条件。

注释 您可以在 ACE 中定义目的地址或应用/用户身份/SGT。

要选择性地在传入接口上应用 PBR，可以在 ACE 中定义阻止条件。当流量匹配 ACE 的阻止规则时，流量将根据路由表转发到出口接口。

b) 从 **发送至** 下拉列表：

- 要选择配置的接口，请选择 **出口接口**。
- 要指定 IPv4 / IPv6 下一跳地址，请选择 **IP 地址**。继续步骤 7.e，第 8 页

c) 如果已选择 **出口接口**，请从 **接口顺序** 下拉列表中选择相关选项：

- 按**接口优先级 (Interface Priority)** - 按接口的优先级转发流量。流量首先路由到具有最低优先级值的接口。当接口不可用时，流量会转发到具有下一个最低优先级值的接口。例如，假设 *Gig0/1*、 *Gig0/2*和 *Gig0/3* 分别配置了优先级值 *0*、*1*和 *2* 。流量被转发到 *Gig0/1*。如果 *Gig0/1* 变得不可用，流量将被转发到 *Gig0/2*。

  注释 要配置接口的优先级，请点击策略型路由页面上的**配置接口优先级**。在对话框中，提供接口的优先级编号，然后点击 **保存**。您还可以在 接口设置中配置接口的优先级。

  当所有接口的优先级值相同时，流量在接口之间均衡。

- 按**顺序 (Order)** - 按此处指定的接口顺序转发流量。例如，假设 *Gig0/1*、 *Gig0/2*和 *Gig0/3* 是按以下顺序选择的，*Gig0/2*、 *Gig0/3*、 *Gig0/1*。流量先转发到 *Gig0/2*，然后转发到 *Gig0/3*，无论其优先级值如何。
- 按**最小抖动 (Minimal Jitter)** - 流量转发到抖动值最低的接口。您需要在接口上启用路径监控，以使 PBR 获取抖动值。
- 按**最大平均意见评分 (Maximum Mean Opinion Score)** - 按流量转发到具有最大平均意见评分（MOS）的接口。您需要在接口上启用路径监控，以便 PBR 获取 MOS 值。
- 按**最小往返时间 (Minimal Round Trip Time)** - 将流量转发到具有最小往返时间 (RTT) 的接口。您需要在接口上启用路径监控，以便 PBR 获取 RTT 值。
- 按**最小数据包丢失 (Minimal Packet Loss)** - 将流量转发到具有最小数据包丢失的接口。您需要在接口上启用路径监控，以使 PBR 获取丢包值。

d) 在 **可用接口框** 中，列出所有接口及其优先级值。从接口列表中，点击 **添加**（⊕） 按钮以添加到所选出口接口。继续步骤 7.k，第 9 页

e) 如果选择了 **IP 地址 (IP Address)**，请在 **IPv4 地址 (IPv4 Addresses)** 和 **IPv6 地址 (IPv6 Addresses)** 字段中输入用逗号分隔的 IP 地址。流量根据指定 IP 地址的顺序转发。

注释　当提供多个下一跳 IP 地址时，将按照指定 IP 地址的顺序转发流量，直至找到有效的可路由下一跳 IP 地址。所配置的下一跳应为直连式。

f) 从**不分段 (Don't Fragment)** 下拉列表中选择“是”(Yes)、“否”(No) 或“无”(None)。如果 DF（不分段）标志设置为是 *(Yes)*，则中间路由器从不执行数据包分段。

g) 要将当前接口指定为默认转发接口，请选中默认接口 (Default Interface) 复选框。

h) **IPv4 设置 (IPv4 Settings)** 和 **IPv6 Settings (IPv6 设置)** 选项卡允许您指定递归和默认设置：

注释　对于路由映射，您只能指定 IPv4 或 IPv6 下一跳设置。

- **递归 (Recursive)** - 只有当在直连子网上找到指定的下一跳地址和默认下一跳地址时，才会应用路由映射配置。但是，您可以使用递归选项，其中的下一跳地址不需要直接连接。在这里，会对下一跳地址进行递归查询，根据路由器的当前路由路径，将匹配的流量转发到该路由条目使用的下一跳中。
- **默认 (Default)** - 如果正常路由查询无法匹配流量，则流量会被转发到此指定的下一跳 IP 地址。

i) 选中**对等体地址 (Peer Address)** 复选框，以便使用下一跳地址作为对等体地址。

注释　您不能同时使用默认下一跳地址和对等体地址配置路由映射。

j) 对于 IPv4 设置，您可以在**验证可用性 (Verify Availability)**下检查路由映射的下一跳是否可用 - 点击 **添加**（＋） 按钮并添加下一跳 IP 地址条目：

- **IP Address** - 输入下一跳 IP 地址。
- **顺序 (Sequence)** - 使用序列号按顺序来评估条目。确保没有输入重复的序列号。有效范围为 1 至 65535。
- **跟踪 (Track)** - 输入有效的 ID。有效范围为 1 至 255。

k) 点击**保存 (Save)**。

步骤 8 要保存策略，点击 **保存** 和 **部署**。

威胁防御 使用 ACL 来匹配流量，并对流量执行路由操作。典型地，配置指定用于进行匹配的 ACL 的路由映射，然后为该流量指定一个或多个操作。通过使用路径监控，PBR 现在可以选择最佳出口接口来路由流量。最后，将路由映射与接口相关联，在该接口上要对所有传入流量应用 PBR 。

添加路径监控控制面板

要查看路径监控指标，必须将路径监控控制面板添加到设备的“运行状况监控”(Health Monitoring) 页面。

过程

步骤 1 选择**系统 (System)** > **运行状况 (Health)** > **监控 (Monitor)**。

步骤 2 选择设备，然后点击 **添加控制面板**。

步骤 3 输入自定义控制面板的名称。

步骤 4 在 **指标** 区域中，点击 **从预定义关联添加** 按钮。

步骤 5 从列表中，点击 **接口 - 路径指标**。

默认情况下，系统会选择所有四个指标，以便在具有额外指标字段的控制面板中显示为 Portlet。您可以通过点击 **删除**（ ） 来排除其中任何一项。

步骤 6 点击 **添加控制面板**。

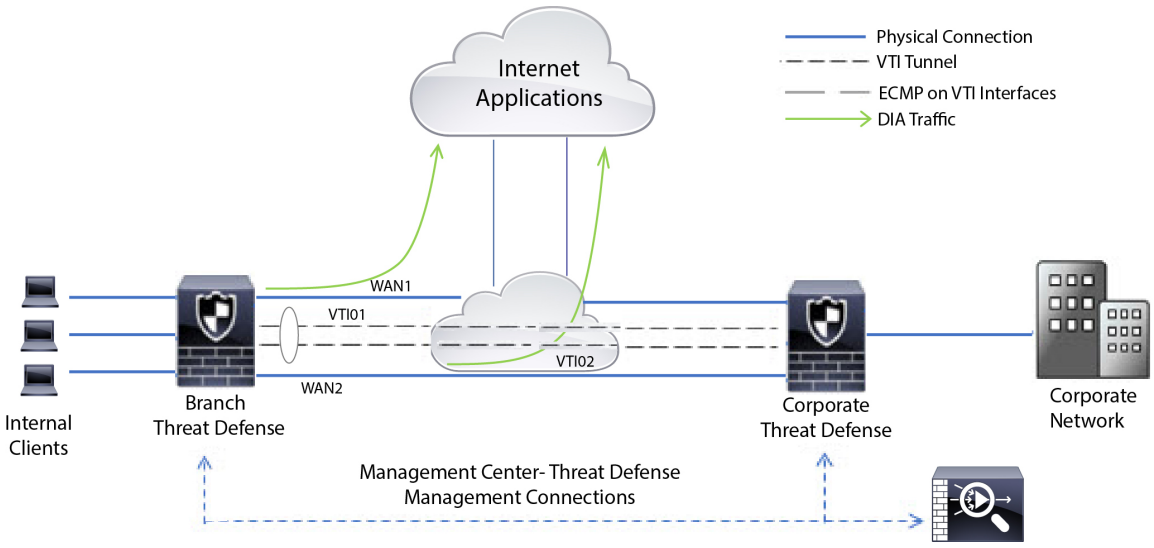
策略型路由的配置示例

假设一个典型的企业网络场景，其中所有分支机构网络流量都通过企业网络的基于路由的 VPN，并在需要时分流到外联网。通过企业网络访问处理日常运营的 Web 应用会导致巨大的网络扩展和维护成本。此示例说明了直接互联网接入的 PBR 配置程序。

下图描述了企业网络的拓扑。分支机构网络通过基于路由的 VPN 连接到企业网络。传统上，公司威胁防御 会被配置为处理分支机构的内部和外部流量。通过 PBR 策略，分支机构 威胁防御 会配置将特定流量路由到 WAN 网络而不是虚拟隧道的策略。其余流量会照常流经基于路由的 VPN。

此示例还说明了如何使用 ECMP 区域来配置 WAN 和 VTI 接口以实现负载均衡。

图 *1:* 在 管理中心 中的分支机构 威胁防御 上配置策略型路由



开始之前

此示例假定您已为 管理中心 中的分支机构 威胁防御 配置 WAN 和 VTI 接口。

过程

步骤 1 为分支机构 威胁防御 配置策略型路由，选择入口接口：

a) 依次选择 **设备** > **设备管理**，并且编辑 威胁防御 设备。

b) 选择**路由 (Routing)** > **策略型路由 (Policy Based Routing)**，然后在**策略型路由 (Policy Based Routing)** 页面上，点击**添加 (Add)**。

c) 在 **添加策略型路由 (Add Policy Based Route)** 对话框中，从 **入口接口 (Ingress Interface)** 下拉列表中选择接口（也就是， 内部 *1 (Inside 1)* 和 内部 *2 (Inside 2)*）。

步骤 2 指定匹配条件：

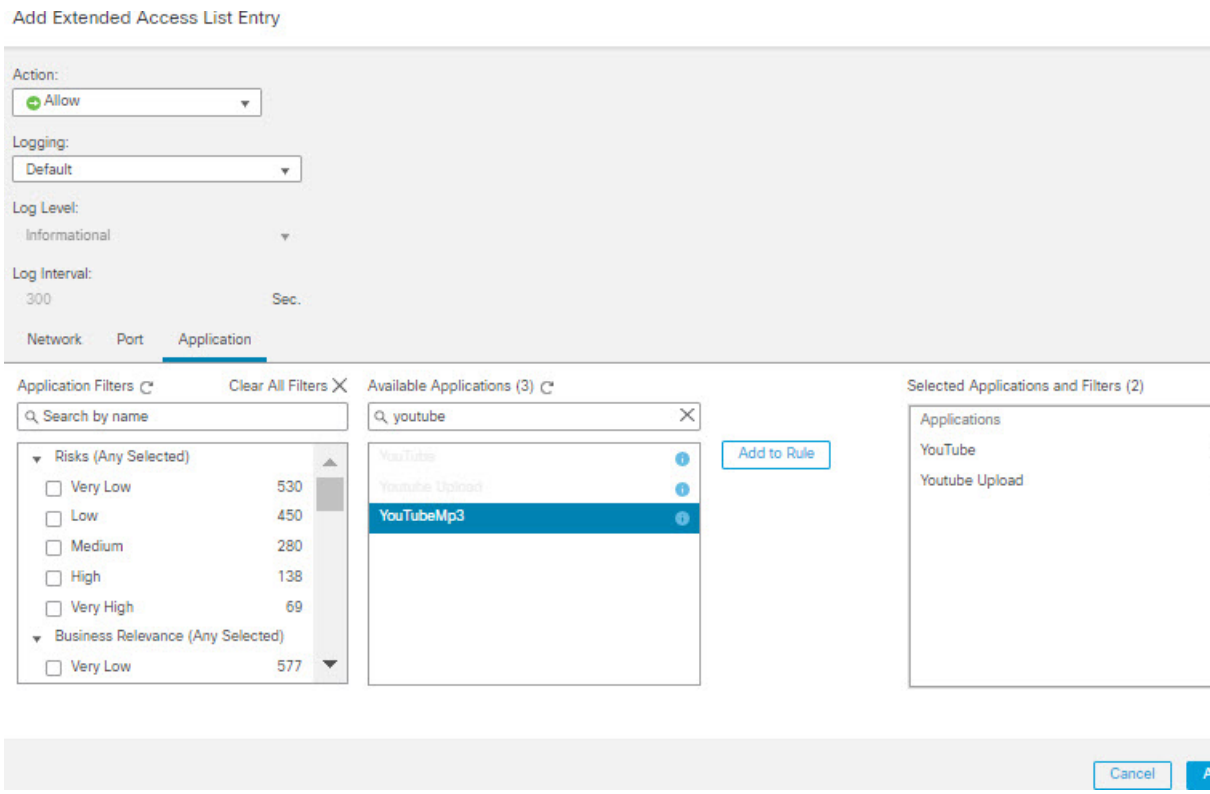
a) 单击**添加**。

b) 要定义匹配条件，请点击 **添加**（+） 按钮。

c) 在**新建扩展访问列表对象 (New Extended Access List Object)** 中，输入 ACL 的名称（例如 *DIA-FTD-Branch*），然后点击**添加 (Add)**。

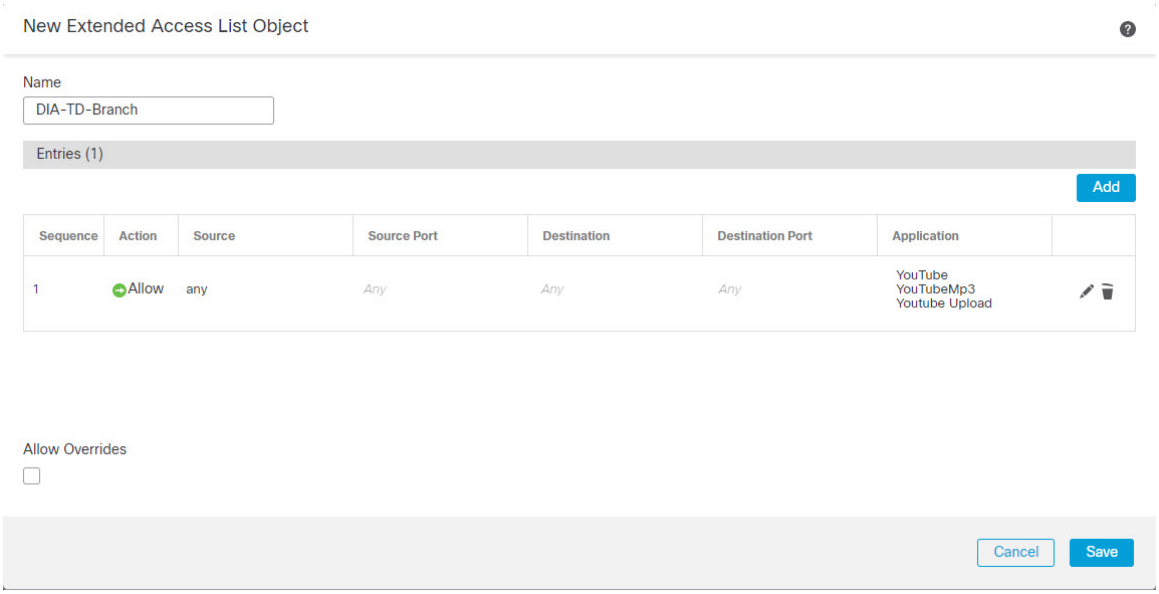
d) 在**添加扩展访问列表条目 (Add Extended Access List Entry)** 对话框中，从**应用 (Application)** 选项卡中选择所需的基于 Web 的应用：

图 *2:*“应用”*(Applications)* 选项卡



在 威胁防御 上，ACL 中的应用组被配置为网络服务组，并且每个应用被配置为网络服务对象。

图 *3:* 扩展 *ACL*



e) 单击**保存**。

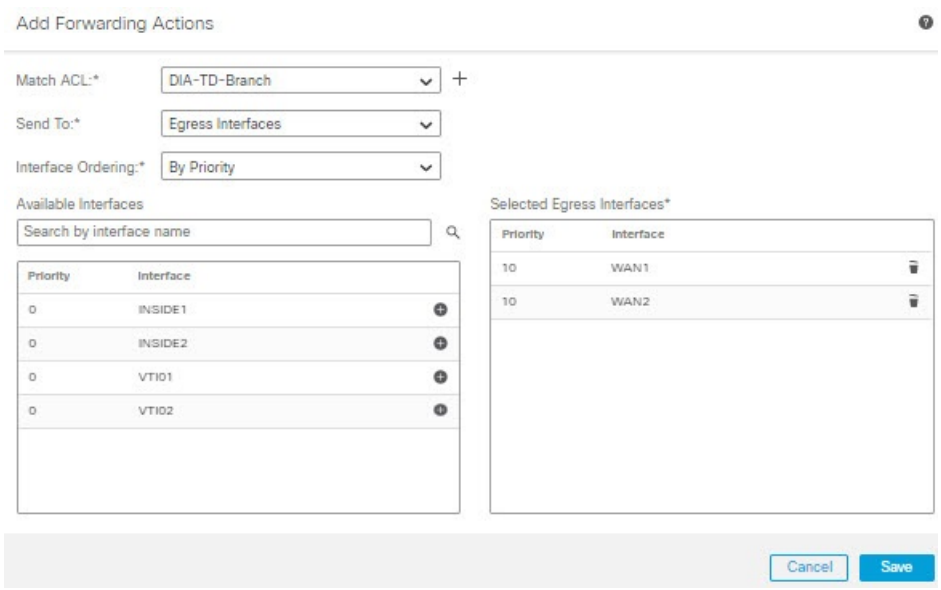
f) 从**匹配 ACL (Match ACL)** 下拉列表中选择 *DIA-FTD-Branch*。

步骤 3 指定出口接口：

a) 从**发送到 (Send To)** 和**接口排序 (Interface Ordering)** 下拉列表中，分别选择“出口接口”(Egress Interfaces) 和“按优先级”(By Priority)。

b) 在 Available Interfaces 下，点击相应接口名称的 按钮以添加 WAN1 和 WAN2：在**可用接口 (Available Interfaces)** 下，再次点击相应接口名称的 ⊕ 按钮以便添加 *WAN1* 和 *WAN2*：

图 *4:* 配置策略型路由



c) 单击**保存**。

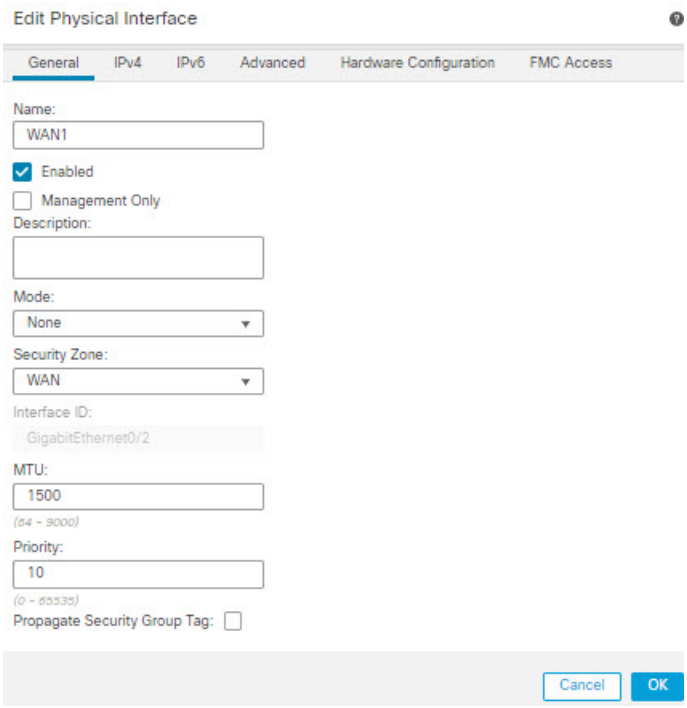
步骤 4 接口优先级配置：

您可以在**编辑物理接口 (Edit Physical Interface)** 页面或**策略型路由 (Policy Based Routing)** 页面（**配置接口优先级**）中设置接口的优先级值。在本示例中，将介绍“编辑物理接口”方法。

a) 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后编辑分支机构 威胁防御。

b) 设置接口的优先级。点击接口的**编辑 (Edit)**，然后输入优先级值：

图 *5:* 设置接口优先级



c) 点击**确定 (Ok)** 和**保存 (Save)**。

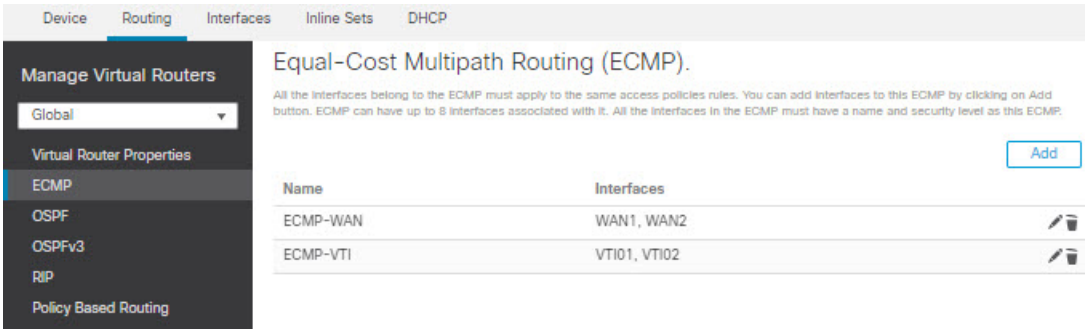
步骤 5 创建用于负载均衡的 ECMP 区域：

a) 在**路由 (Routing)** 页面中，点击 **ECMP**。

b) 要将接口关联到 ECMP 区域，请点击**添加 (Add)**。

c) 选择 *WAN1* 和 *WAN 2*，然后创建一个 ECMP 区域 — *ECMP-WAN*。同样，添加 *VTI01* 和 *VTI02*，然后创建一个 ECMP 区域 — *ECMP-VTI*：

图 *6:* 将接口与 ***ECMP*** 相关联

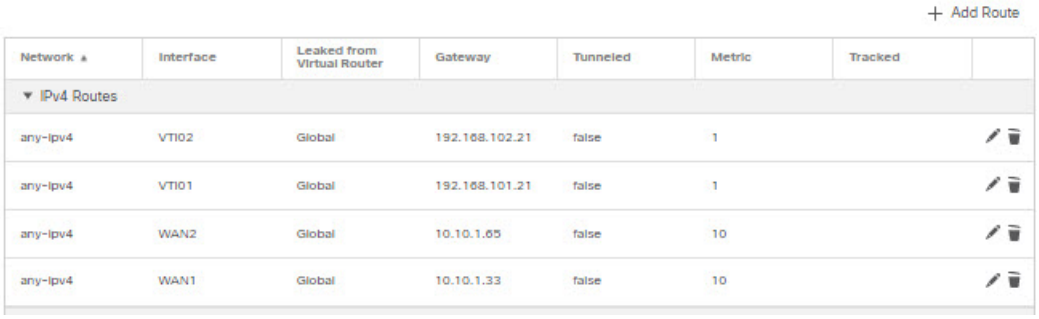


步骤 6 为区域接口配置静态路由以实现负载均衡：

a) 在**路由 (Routing)** 页面中，点击**静态路由 (Static Route)**。

b) 点击**添加 (Add)** 并为 *WAN1*、*WAN2*、*VTI01* 和 *VTI02* 指定静态路由。确保为属于相同 ECMP 区域的接口指定相同的指标值（步骤 5）：

图 *7:* 为 ***ECMP*** 区域接口配置静态路由



注释 确保区域接口具有相同的目的地址和指标，但网关地址不同。

步骤 7 在分支机构 威胁防御 的 WAN 对象上配置受信任的 DNS，以确保流量安全地流向互联网：

a) 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后在分支机构 威胁防御 上创建 DNS 策略。

b) 要指定受信任的 DNS，请点击**编辑 (Edit)** 以编辑策略，然后点击 **DNS**。

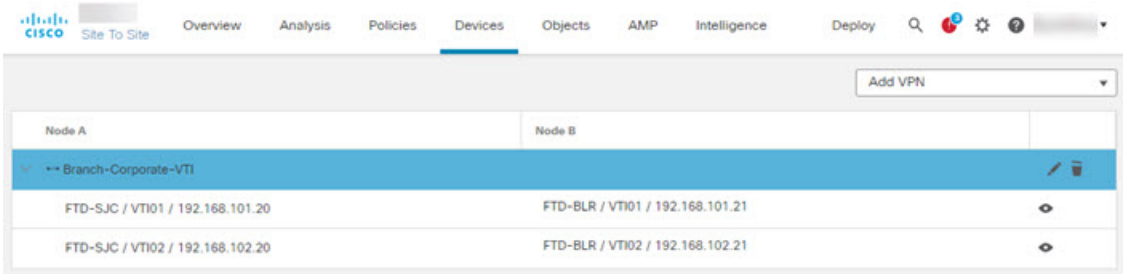
c) 要为 WAN 对象使用的 DNS 解析指定 DNS 服务器，请在 **DNS 设置 (DNS Settings)** 选项卡中提供 DNS 服务器组详细信息，然后从接口对象中选择 WAN。

d) 使用**受信任 DNS 服务器 (Trusted DNS Servers)** 选项卡为 DNS 解析提供您信任的特定 DNS 服务器。

步骤 8 **保存 (Save)** 和**部署 (Deploy)**。

来自分支机构内部网络 *INSIDE1* 或 *INSIDE2* 的任何 *YouTube* 相关访问请求都会被路由到 *WAN1* 或 *WAN2*，因为它们将与 *DIA-FTD-Branch* ACL 匹配。任何其他请求（例如 *google.com*）都会通过在站点间 VPN 设置中配置的 *VTI01* 或 *VTI02* 进行路由：

图 *8:* 站点间 ***VPN***



如果配置了 ECMP，就可以无缝地平衡网络流量。

具有路径监控的 PBR 的配置示例

此示例详细介绍了为以下具有灵活指标的应用配置具有路径监控的 PBR：

- 具有抖动的音频或视频敏感应用（例如，WebEx Meetings）。

- 使用 RTT 的基于云的应用（例如 Office365）。
- 具有丢包的基于网络的访问控制（具有特定的源和目标）。

开始之前

1. 此示例假定您知道 PBR 的基本配置步骤。
2. 您已使用逻辑名称来配置入口和出口接口。在本示例中，入口接口命名为 *Inside1*，而出口接口命名为 *ISP01*、*ISP02* 和 *ISP03*。

过程

步骤 1 接口 *ISP01*、*ISP02* 和 *ISP03* 上的路径监控配置：

对于出口接口上的指标收集，您必须在它们上面启用并配置路径监控。

a) 选择 **设备** > **设备管理**，然后编辑 威胁防御。
b) 在**接口 (Interfaces)** 选项卡下，编辑接口（在我们的示例中为 *ISP01*）
c) 点击**路径监控 (Path Monitoring)** 选项卡，选中**启用路径监控 (Enable Path Monitoring)** 复选框，然后指定监控类型（请参阅配置路径监控设置，第 6 页）。
d) 点击**确定 (Ok)** 和**保存 (Save)**。
e) 重复相同的步骤并为 *ISP02* 和 *ISP03* 配置路径监控设置。

步骤 2 为组织 威胁防御 中的分支机构配置策略型路由，选择入口接口：

a) 依次选择 **设备** > **设备管理**，并且编辑 威胁防御 设备。
b) 选择**路由 (Routing)** > **策略型路由 (Policy Based Routing)**，然后在**策略型路由 (Policy Based Routing)** 页面上，点击**添加 (Add)**。
c) 在**添加策略型路由 (Add Policy Based Route)** 对话框中，从**入口接口 (Ingress Interface)** 下拉列表中选择内部 *1 (Inside 1)*。

步骤 3 指定匹配条件：

a) 单击**添加**。
b) 要定义匹配条件，请点击 **添加**（＋） 按钮。
c) 在**新建扩展访问列表对象 (New Extended Access List Object)** 中，输入 ACL 的名称（例如 *PBR-WebEx*），然后点击**添加 (Add)**。
d) 在**添加扩展访问列表条目 (Add Extended Access List Entry)** 对话框中，从**应用 (Application)** 选项卡中选择所需的基于 Web 的应用（例如 WebEx 会议）。

   记住 在 威胁防御上，ACL 中的应用组被配置为网络服务组，并且每个应用被配置为网络服务对象。

e) 单击**保存**。
f) 从**匹配 ACL (Match ACL)** 下拉列表中选择 *PBR-WebEx*。

步骤 4 指定出口接口：

a) 在**发送到 (Send To)** 下拉列表中，选择“出口接口”(Egress Interfaces)。
b) 从**接口排序 (Interface Ordering)** 下拉列表中，选择“按最小抖动”(By Minimal Jitter)。
c) 在**可用接口 (Available Interfaces)** 下，点击相应接口名称对应的 **右箭头**（ > ） 按钮，以便添加 *ISP01*、*ISP02* 和 *ISP03*。
d) 单击**保存**。

步骤 5 重复步骤 2 和步骤 3，为同一接口 (*Inside1*) 创建 PBR，以便路由 Office365 和基于网络的访问控制流量：

a) 创建匹配条件对象（例如 *PBR-Office365*），然后从**应用 (Application)** 选项卡中选择 Office365 应用。
b) 从**接口排序 (Interface Ordering)** 下拉列表中，选择“按最短往返时间”(By Minimal Round Trip Time)。
c) 指定出口接口 *ISP01*、*ISP02* 和 *ISP03*，然后点击**保存 (Save)**。
d) 现在，创建匹配条件对象（例如 *PBR-networks*），并在**网络 (Network)** 选项卡中指定源接口和目标接口。
e) 从**接口排序 (Interface Ordering)** 下拉列表中，选择“按最小丢包”(By Minimal Packet Loss)。
f) 指定出口接口 *ISP01*、*ISP02* 和 *ISP03*，然后点击**保存 (Save)**。

步骤 6 **保存 (Save)** 和**部署 (Deploy)**。

步骤 7 要查看路径监控指标，请选择**设备 (Devices)** > **设备管理 (Device Management)**，然后在 **更多**（ ⋮ ） 中点击**运行状况监控 (Health Monitor)**。要查看设备接口的指标详细信息，您必须添加路径指标控制面板。有关详细信息，请参阅添加路径监控控制面板 ， 第 9 页。

WebEx、Office365 和基于网络的 ACL 流量会通过从 *ISP01*、*ISP02* 和 *ISP03*上收集的指标值得出的最佳路由进行转发。

Cisco Secure Firewall Threat Defense 中策略型路由的历史记录

特性	Version	最低 威胁防御	详细信息
基于身份和 SGT 的 PBR 策略	7.4	任意	现在，您可以根据用户和用户组以及 PBR 策略中的 SGT 对网络流量进行分类。您可以在定义 PBR 策略的扩展 ACL 时选择身份和 SGT 对象。 新增/修改的屏幕： 扩展访问列表对象中添加的新选项卡，用于配置基于策略的路由策略：**对象** > **对象管理** > **访问控制列表** > **添加扩展** 页面， **用户** 和 **安全组标签**。 支持的平台： 威胁防御

特性	Version	最低 威胁防御	详细信息
基于 HTTP 的路径监控	7.4	任意	PBR 现在可以使用通过应用域上的 HTTP 客户端进行路径监控收集的性能指标（RTT、抖动、丢包和 MOS），而不是特定目标 IP 上的指标。默认情况下，为接口启用基于 HTTP 的应用监控选项。您可以使用匹配 ACL 配置 PBR 策略，该 ACL 具有用于确定路径的受监控应用和指标类型。 新增/修改的屏幕： 接口页面中用于启用路径监控的新选项： **设备** > **设备管理** > **编辑接口** > **路径监控** > **启用基于 HTTP 的应用监控** 复选框。
双 WAN/ISP 威胁防御管理支持	7.3	任意	在启用双 WAN 的威胁防御中，配置了一个数据接口来与管理中心进行通信。现在提供了对配置辅助数据接口的支持，以便在主数据接口发生故障时维持通信通道。管理中心会自动配置 PBR，以根据优先级和 SLA 指标将 SF 隧道流量从 *tapnlp*（内部）接口路由到其中一个可用的数据接口。 无新建/修改的屏幕。但是，添加了部署验证。
PBR 路由映射的下一跳设置	7.3	任意	您可以在启用数据包转发操作的同时，为 PBR 路由映射配置下一跳。 新增/修改的屏幕： 添加/编辑转发操作页面中用于配置出口接口的新字段：**设备管理 (Device Management)** > **路由 (Routing)** > **策略型路由 (Policy Based Routing)** > **添加转发操作 (Add Forwarding Actions)** 页面。
PBR 和路径监控	7.2	任意	PBR 使用路径监控来收集出口接口的性能指标（RTT、抖动、丢包和 MOS）。您必须为接口启用路径监控并配置监控类型。您可以通过路径确定所需的指标来配置 PBR 策略。 新增/修改的屏幕： 接口页面中用于启用路径监控的新选项卡：**设备 (Devices)** > **设备管理 (Device Management)** > **编辑接口 (Edit Interfaces)** > **路径监控 (Path Monitoring)** 选项卡。
策略型路由 (PBR)	7.1	任意	引入了通过 管理中心 策略型路由，以根据应用对网络流量进行分类。您可以定义 PBR 策略并在入口接口上对其进行配置。您可以指定匹配条件和出口接口。与 ACL 列表匹配的网络流量会根据策略中配置的优先级或顺序来通过出口接口进行转发。 新增/修改的屏幕： 用于配置策略型路由策略的新策略页面：**设备 (Devices)** > **设备管理 (Device Management)** > **路由 (Routing)** > **策略型路由 (Policy Based Routing)** 页面。 支持的平台： 威胁防御

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。