策略型路由

本章介绍如何通过 防火墙管理中心 的策略型路由页面来配置 Firewall Threat Defense 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。

策略型路由

策略型路由 (PBR) 扩展了传统路由协议，可增强对流量的控制。它支持根据目标 IP 以外的条件做出路由决策，例如源和目标端口、协议和应用。此外，PBR 可在大规模网络部署中实现安全的特定应用的流量分支。

策略型路由特征

在传统路由中，数据包会根据目的 IP 地址进行路由。在基于目的地的路由系统中，更改特定流量的路由并非易事。策略型路由 (PBR) 扩展并补充了路由协议提供的机制。

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，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型网络部署中众多设备访问应用程序和数据的场景。在大规模部署中，网络流量通常会通过基于路由的 VPN 以加密流量的形式回传到中心服务器。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。解决这些问题需要昂贵且复杂的部署和管理。

策略型路由

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

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。

这些场景演示了基于策略的路由应用：

- **直接互联网访问**：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。分支机构 Firewall Threat Defense 配置了互联网出口点。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。
- **平等访问和源敏感路由**：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。因此在本例中，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。
- **负载共享**：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。

图 *1*: 直接互联网接入场景

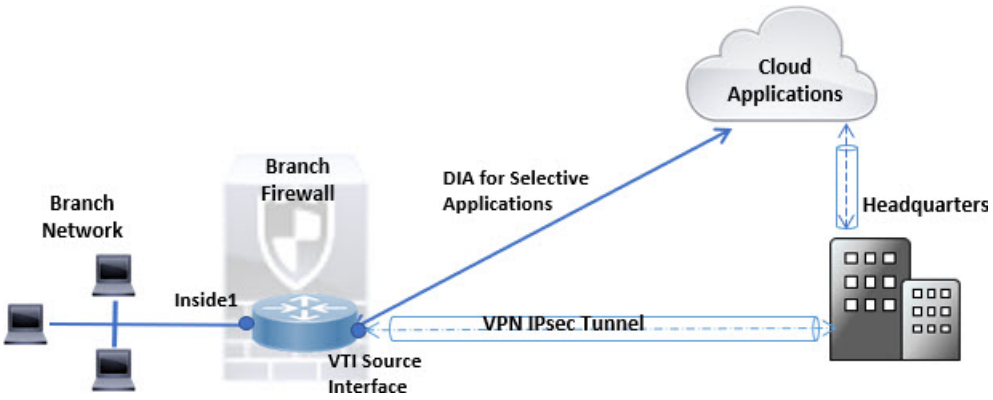
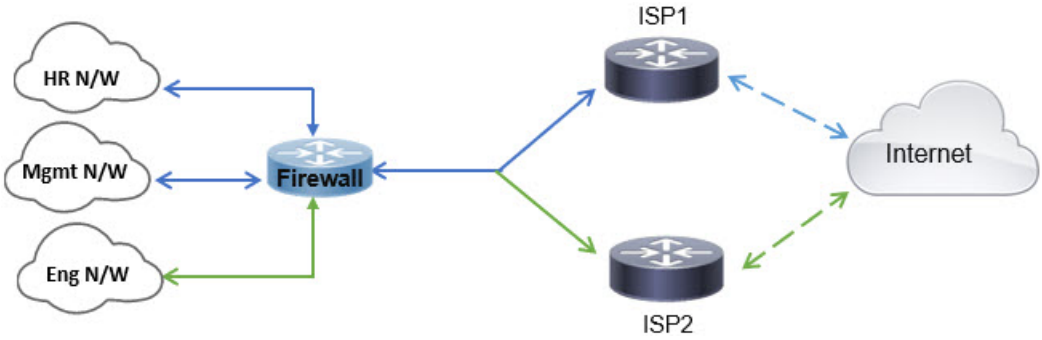


图 2: 平等访问场景



策略型路由的许可证

策略型路由 (PBR) 有特定的许可要求，具体取决于您的配置中使用的功能和服务。

- 所有 PBR 策略功能均受 基础版 Firewall Threat Defense 智能软件许可的支持。
- 如果要为通过 RA VPN 隧道接口来为路由流量配置 Cisco Secure 客户端，则必须拥有 PBR 许可。
- 要在 PBR 策略中使用 ISE，需要 Cisco ISE 许可证。

策略型路由的最佳实践

设备准则

在实施策略型路由时，确保版本兼容性和设备特定配置正确。

- PBR 至 防火墙管理中心 的“策略型路由”页面仅在 7.1 及更高版本的 防火墙管理中心 和 Firewall Threat Defense 设备上受支持。
- 当您将 防火墙管理中心 或 防火墙威胁防御 升级到版本 7.1 及更高版本时，设备中的 PBR 配置将被删除。您必须使用策略型路由页面再次配置 PBR。如果托管设备的版本低于 7.1，则必须使用 FlexConfig 再次配置 PBR，并将部署选项设置为“每次”。
- 在集群设备上，请勿配置基于应用、用户身份和安全组标签 (SGT) 的 PBR 策略，因为集群设备不支持这些策略。
- 在 Cisco Secure Firewall 200 型号设备上，请勿配置基于用户身份或安全组标记 (SGT) 的 PBR 策略，因为这些设备不支持这些策略。

接口准则

为 PBR 策略配置适当的接口类型和设置。

- 仅将全局虚拟路由器中的路由模式接口和非仅管理接口配置为 PBR 策略的入口或出口接口。您不能为该策略配置用户定义的虚拟路由器接口。
- 要在策略中定义的接口必须具有逻辑名称。
- 仅将静态 VTI 配置为出口接口。
- 请勿选择动态 VTI 来配置 PBR 出口接口。

您可以应用 PBR 来管理 IPv4 和 IPv6 流量。

基于应用的 PBR 和 DNS 配置

确保基于应用的 PBR 功能配置正确。

- 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 Firewall Threat Defense 时，应用检测才会成功； DNS 流量不会被加密。
- 您必须配置受信任的 DNS 服务器，应用检测才能成功。

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

策略型路由是一种仅入口功能；系统仅会将 PBR 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

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，在新的内部接口与客户端建立连接之前，PBR 不会处理来自主机的返回流量。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。为防止响应丢失，请在内部接口上配置具有更高度量值的加权静态路由。

基于 HTTP 的路径监控准则

通过适当的接口类型和版本注意事项来配置基于 SSL 的路径监控。

- 仅在物理接口、端口通道接口、子接口和静态隧道接口上配置基于 HTTP 的路径监控。请勿在集群设备上进行配置。
- HTTP 仅使用 IPv4 对应用执行 ping 操作。IPv4 指标同时用于路由和转发 IPv4 和 IPv6 流量。
- Secure Firewall Management Center 7.4 及更高版本默认启用基于 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。

其他准则

请按照以下其他配置注意事项来有效实施 PBR。

- 所有现有的配置限制和路由映射限制仍然有效。

- 在定义策略匹配条件的ACL时，您可以从列表中选择多个预定义的应用程序来形成访问控制条目 (ACE)。在 Firewall Threat Defense 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。但是，您可以创建自定义应用检测器。请参阅为 PBR 创建自定义应用检测器，第 11 页。
- 单播反向路径转发 (uRPF) 会根据路由表而不是 PBR 路由映射来验证接口上接收的数据包的源 IP 地址。启用 uRPF 时，通过 PBR 在接口上接收的数据包将被丢弃，因为它们没有特定路由条目。因此，在使用 PBR 时，请确保禁用 uRPF。

用于确定最佳路径路由的路径监控指标

用于确定最佳路径路由的路径监控指标是一种使用各种监控方法（例如ICMP和HTTP）来收集性能指标并确定最佳路径的动态路由方法。

路径监控方法和操作

PBR 使用静态开销或路径监控（动态指标）来路由其流量。

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 的路径监控方法

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 的路径监控方法

路径监控会计算与接口关联的每个远程对等体的动态指标。在监控多个应用程序并确定分支防火墙策略的最佳路径时，HTTP 比 ICMP 更受青睐，原因如下：

- 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，因此当应用程序服务器 IP 地址更改时，无需更改防火墙配置。

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。

用于指标收集的默认监控计时器

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 和路径监控集成

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。

只有在接口上设置了 RTT、抖动、丢包或 MOS 变量时，路径监控功能才会使用动态指标。路径监控对静态指标-接口成本（在接口中设置的成本）不起作用。

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。参阅配置策略型路由策略，第 8 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。仅在检测到域的 DNS 条目后才开始路径监控；配置基于 HTTP 的应用监控时，监控不会立即启动。在获取域的已解析 IP 地址后，路径监控会发送一个 HTTP 请求并接收响应。如果 DNS 为一个域解析出多个 IP 地址，则路径监控探测会使用第一个解析出的 IP 地址来监控应用。路径监控将持续进行，直到 IP 地址发生变化或基于 HTTP 的监控被禁用为止。

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。路径监控会定期向 PBR 发送收集的指标，以便 PBR 可以为来自已配置入口接口的流量做出路由和转发决策。如果在路径监控向 PBR 发送指标之前流量到达，则路由表决定流量流向。一旦指标可用，PBR 会使用它们为后续流量制定路由决策。

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。

管理中心仅在 PBR 配置满足以下条件时才将应用和 NSG 与出口接口关联：

- 匹配 ACL 包含受监控的应用。
- 使用任一接口排序值（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

配置路径监控以收集指定接口上的RTT、抖动、MOS和丢包等指标，以便进行有效的流量管理和路由优化。

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）和接口丢包率）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**页面上，您可以配置接口的路径监控设置，以发送 ICMP 探测或 或 HTTP ping 来收集指标。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 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**— 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 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。

步骤 7 点击**确定 (OK)**。

步骤 8 要保存设置，点击**保存 (Save)**。

路径监控已使用指定设置在接口上配置完毕。系统将根据您的配置使用 ICMP 探测或 HTTP Ping 收集指标，以优化路由路径。

添加路径监控控制面板

添加路径监控控制面板，以便通过预定义的关联和构件管理使用可自定义的显示选项查看路径监控指标。

过程

步骤 1 选择 > **运行状况** > **监控器故障排除** 。

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，所有四个指标和一个附加指标字段均被选中，以构件的形式显示在控制面板中。要排除任何内容，请点击 **删除** (🗑)。

步骤 6 点击**添加控制面板**。

配置策略型路由策略

此任务使您能够配置策略型路由 (PBR)，以根据特定条件来控制流量路由，而不是仅仅依靠路由表来控制流量路由。

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。PBR

Before you begin

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 7 页。

按照这些步骤来配置策略型路由策略：

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)**。

步骤 3 点击**策略型路由**。

在“策略型路由”页面上，您可以查看配置的策略。网格显示入口接口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
您只能从下拉列表中选择属于全局虚拟路由器的逻辑名称的接口。您不能将具有逻辑名称的 VLAN 接口配置为源（入口）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**框中，输入名称，点击**添加**以打开**添加扩展访问列表条目**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。有关创建要与 PBR同步的自定义域的信息，请参阅 为 PBR 创建自定义应用检测器，第 11 页。

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 10 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。默认情况下，设备优先级会被设为 0。PBR优先使用具有最低优先级值的接口来进行流量转发。

- 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* 是按此顺序选择的：*Gig0/2*、*Gig0/3*、*Gig0/1*。流量首先转发到*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 11 页

注释
路由表中必须存在通往所选接口的路由。

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**和 **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。

步骤 8 要保存策略，点击 **保存** 和 **部署**。

Firewall Threat Defense 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 。

为 PBR 创建自定义应用检测器

此任务使您能够创建自定义应用检测器并配置基于应用的PBR 策略，以增强流量控制和路由决策。

自定义应用检测器允许您识别可能未被默认检测方法涵盖的特定应用。然后，这些检测器可用于PBR策略中，以基于应用识别做出路由决策。

过程

步骤 1 为用户定义的应用创建自定义检测器，如 创建用户定义的应用。中所述。

注释
创建用户定义的应用时，请确保从 **标记 (Tag)** 下拉列表中选择 NSG。

步骤 2 通过选择适当的检测器类型和配置方法来定义检测模式。

要手动定义检测模式，请选择 **基本** 检测器类型 (Basic Detector Type) 并继续定义检测模式，如 指定基本检测器中的检测模式中所述。或者，如果要使用 .lua 文件创建检测模式，请选择 **高级** 检测器类型并按照 指定高级检测器中的检测条件中提供的说明进行操作。

步骤 3 激活自定义检测器。

步骤 4 使用自定义应用 ACE 配置 PBR 的ACL 策略（扩展）。

有关创建 ACL 的程序，请参阅 配置扩展 ACL 对象。

步骤 5 在 PBR 策略中，选择与所需转发操作匹配的 ACL。

有关详细操作创建PBR策略，请参阅配置策略型路由策略，第 8 页。

您已成功创建自定义应用检测器并配置了基于应用的PBR 策略。系统现在可以根据您的配置识别自定义应用并应用适当的路由决策。

配置带有自定义应用检测器的 PBR（基本）

此任务使用自定义应用检测器配置PBR 策略，以便使用已定义域的自定义检测器根据特定应用流量模式做出路由决策。

本示例演示了使用特定域的自定义应用检测器配置策略型路由 (PBR)，例如：

- amazon123.com
- flipkart.com
- hamleysonline.com

Before you begin

- 本示例假定您了解配置 PBR 策略和自定义应用检测器的基本步骤。
- 您应已使用逻辑名称来配置入口和出口接口。本示例中，入口接口名为 *Inside1*，而出口接口名为 *eBuy*。

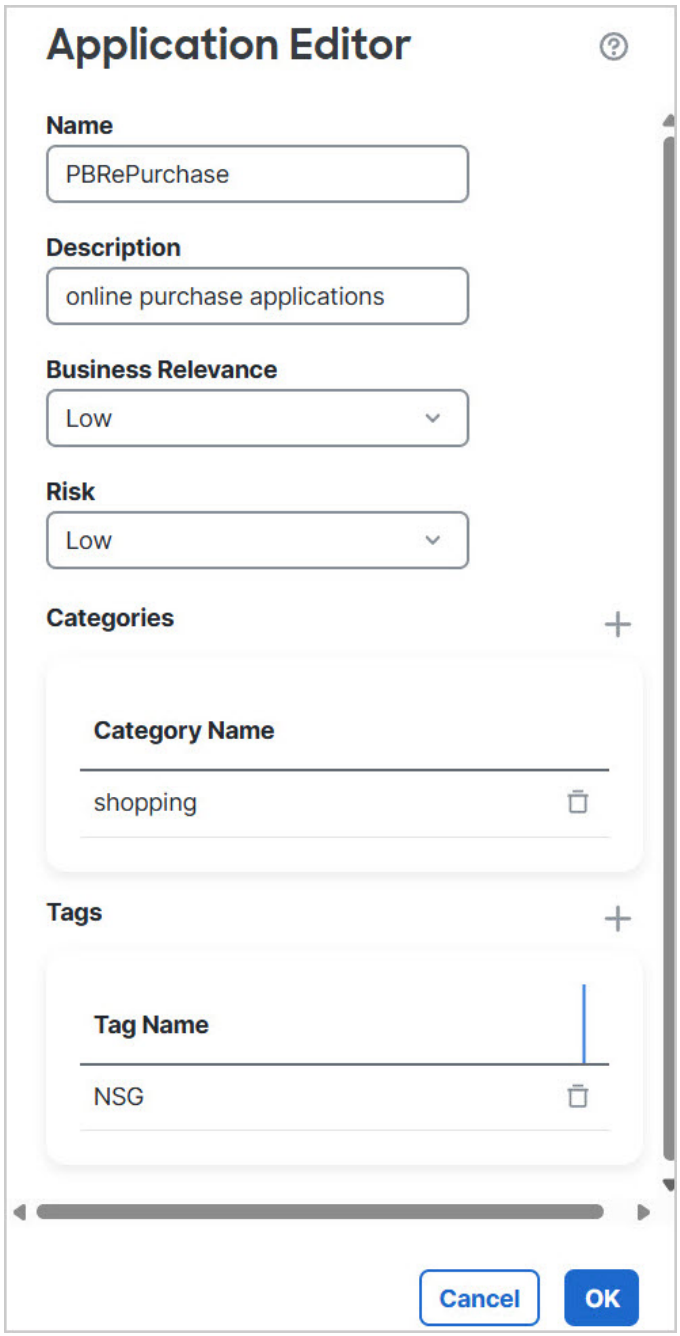
请按照以下步骤使用自定义应用检测器来配置 PBR：

过程

步骤 1 创建自定义检测器 *PBRePurchase*：

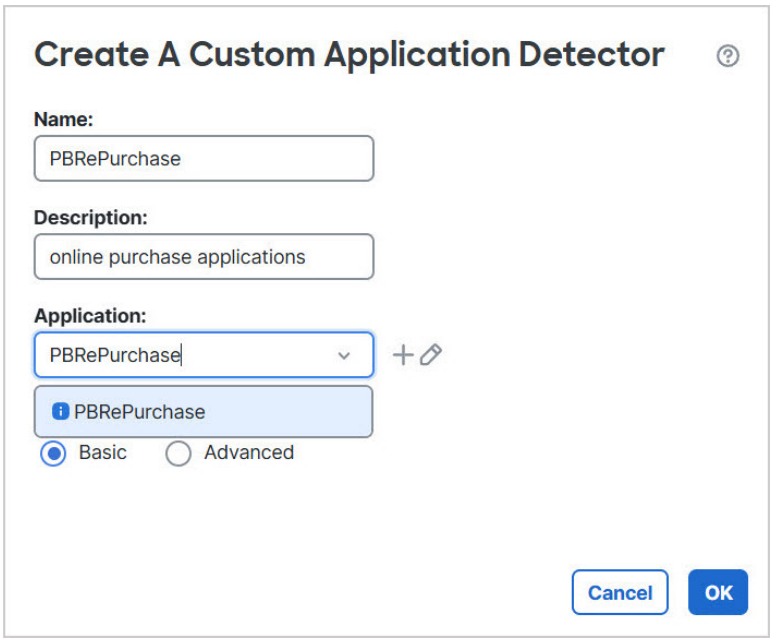
a) 选择 **策略** > **+ 显示更多** > **高级** > **自定义应用检测器**，然后点击**创建自定义检测器**。
b) 在**创建自定义应用检测器**字段中，输入名称（本示例中为 *PBRePurchase*）和说明。
c) 要创建自定义应用，请点击 (+)。
d) 在**应用编辑器**对话框的字段中输入相关值。有关每个字段的详细描述，请参阅创建用户定义的应用。。

注释
要使自定义应用可被 PBR 检测到，请从**标记**下拉列表中选择 **NSG**：



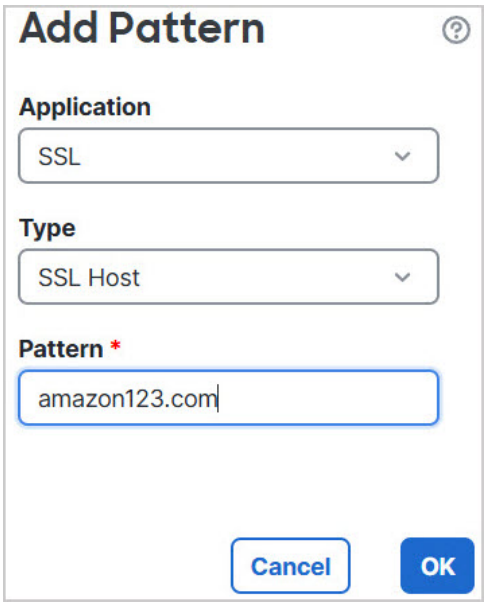
e) 点击**确定**。

f) 从**应用**下拉列表中选择 *PBRePurchase*。



注释
可以在 PBR 策略中使用**基本**或**高级**检测器类型。本示例使用**基本** 检测器类型。

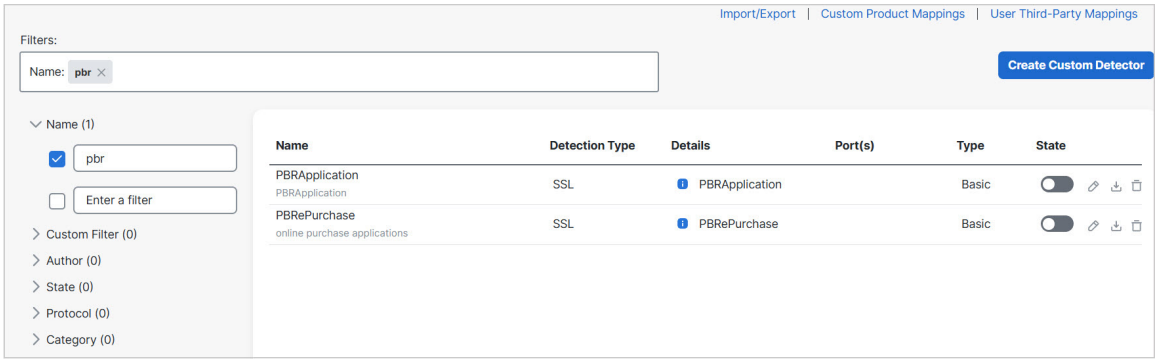
a) 点击**基本**单选按钮，然后点击**确定**。
b) 在**应用检测器**页面上，点击**检测模式**区域中的**添加**按钮以添加模式。
c) 从**应用**下拉列表中，选择 **SSL** 作为协议类型，然后选择适当的模式类型。输入与所选类型匹配的模式字符串（在本例中，输入 *amazon123.com*），然后点击**确定**。



d) 重复此过程，为自定义域 *flashing.com* 和 *hanleysonline.com* 创建另外两个模式。
e) 点击**保存**。

步骤 2 在应用检测器仪表盘中，使用过滤器搜索刚刚创建的自定义应用检测器。

步骤 3 要启用自定义检测器，请点击相应应用检测器旁边的**状态**切换按钮 ( )。



步骤 4 在显示的对话框中，点击**是**。

应用检测器激活后，将显示成功消息：

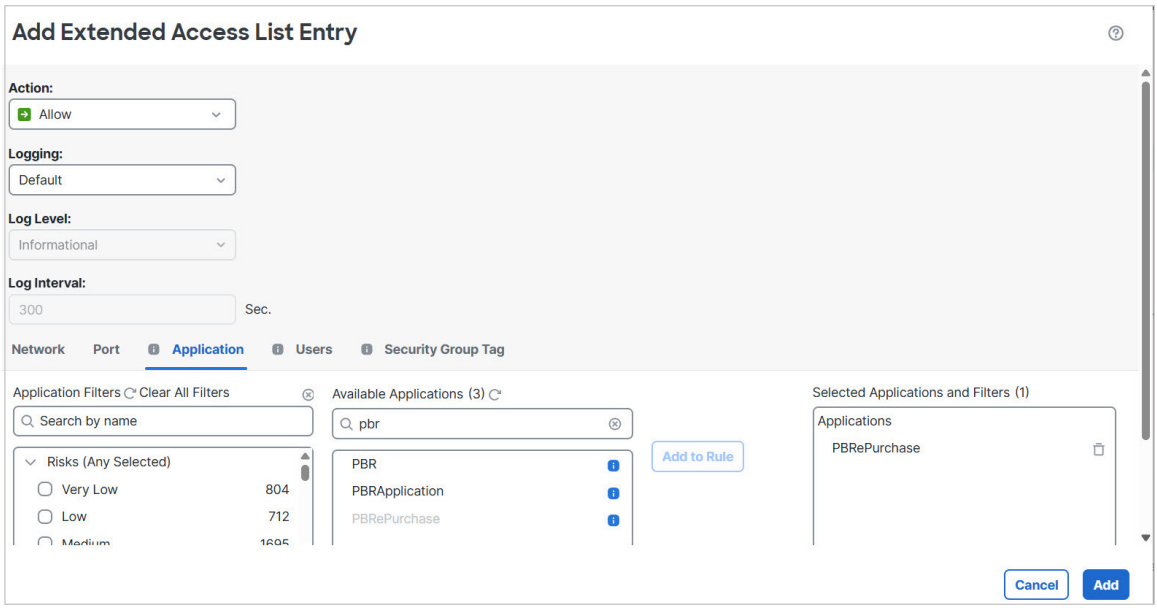
步骤 5 要使用自定义应用检测器创建 ACL 以与 PBR 策略同步：

a) 选择**对象** > **访问列表** > **扩展**。

b) 点击**添加扩展访问列表**。

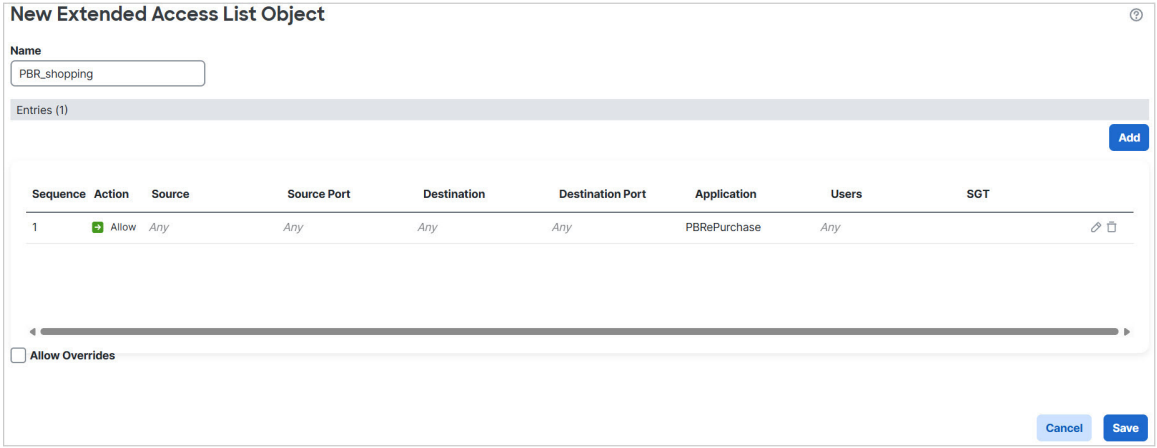
c) 为列表输入名称（例如 *PBR_sending*），然后点击**添加**为列表创建 ACE。

d) 在**添加扩展访问列表条目**对话框中，点击**应用**选项卡，选择应用名称 *PBRePurchase*，然后点击**添加到规则**。



e) 点击添加 **(Add)**。

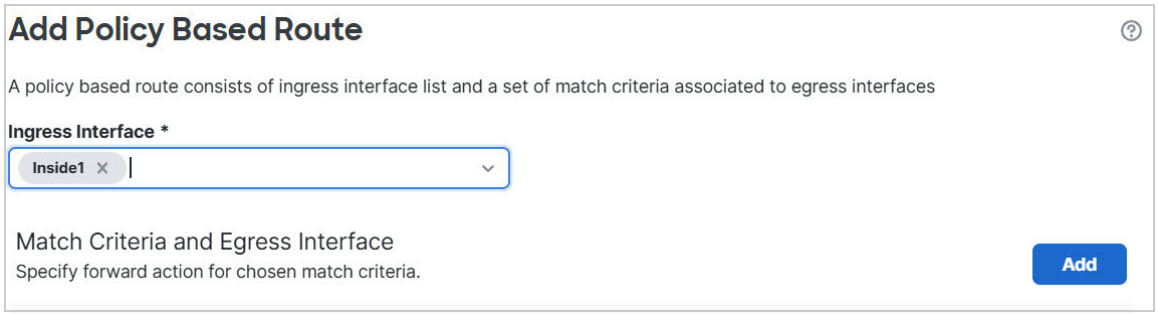
f) 点击保存。



步骤 6 选择路由 > 策略型路由。

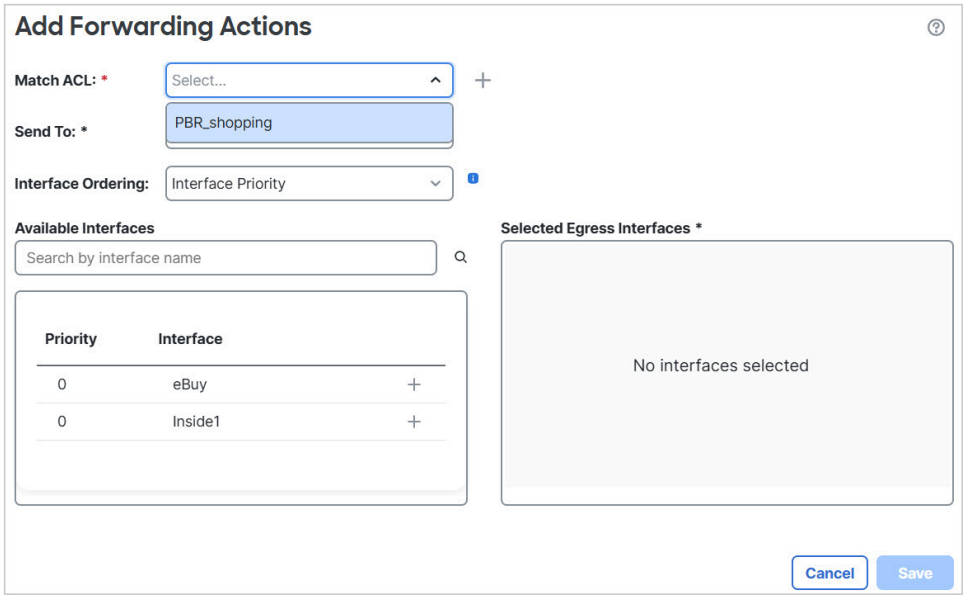
步骤 7 在显示的策略型路由页面上，点击添加。

步骤 8 在添加策略型路由对话框中，从入口接口下拉列表中选择内部 *1*。



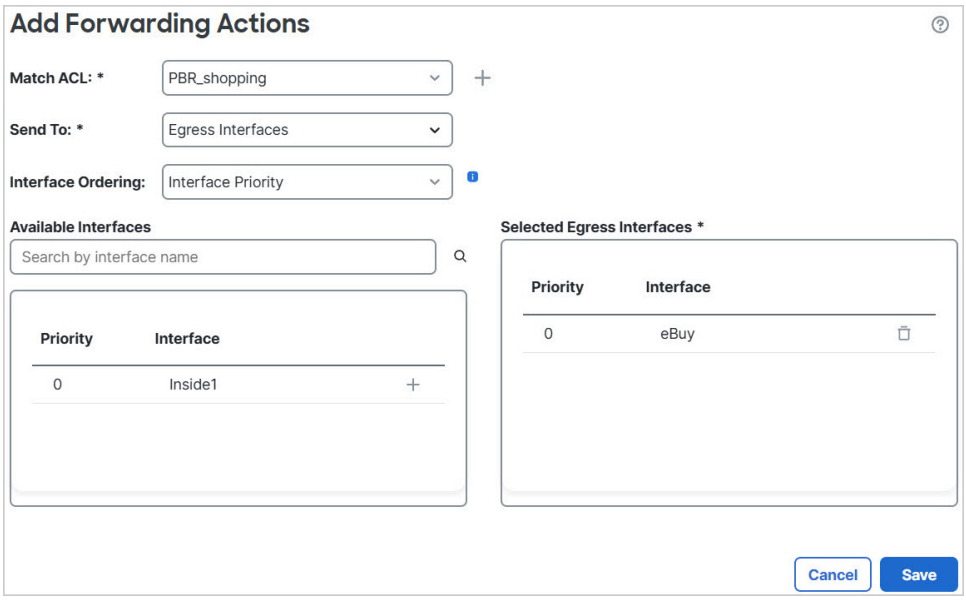
步骤 9 从**匹配 ACL** 下拉列表中，选择已创建的 ACL，在本示例中为 *PBR_sending*。

注释
在 Firewall Threat Defense 中，ACL 中的应用组配置为网络服务组。这就是我们将自定义应用标记为 **NSG** 的原因。

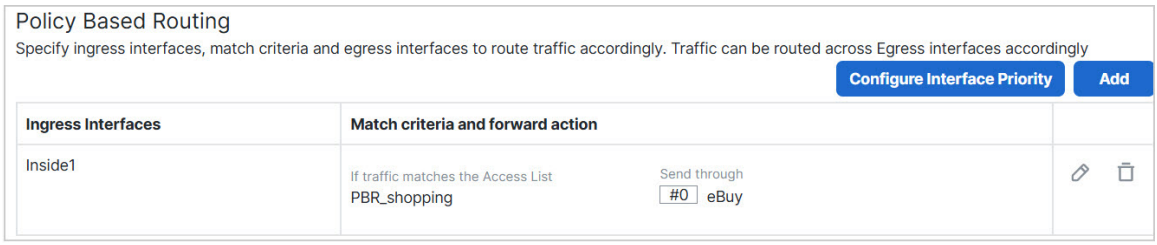


步骤 10 指定出口接口：

a) 在**发送到**下拉列表中，选择**出口接口**。
b) 从**接口排序**下拉列表中选择适当的顺序。
c) 在**可用接口**下，点击相应接口（即 *eBuy*）旁边的（+）。



d) 点击**保存**。



步骤 11 **保存**和**部署**。

使用自定义应用检测器配置和部署了 PBR 策略。与指定域匹配的流量将通过已定义的出口接口进行路由。

配置策略型路由

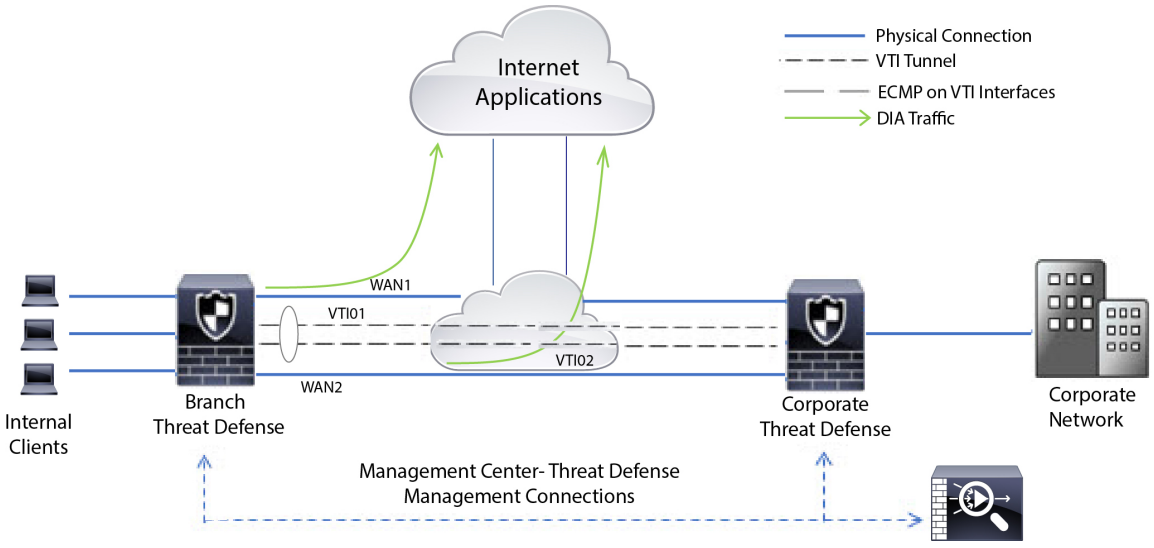
配置 PBR，为特定的基于 Web 的应用启用直连互联网访问，优化流量，并在 WAN 和 VTI 接口之间实现负载均衡。

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。通过企业网络访问支持日常运营的 Web 应用可能会导致网络规模扩大和维护成本增加。本示例说明如何配置 PBR 以实现直接互联网访问。

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 Firewall Threat Defense 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 Firewall Threat Defense 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配置 WAN 和 VTI 接口与 ECMP 区域以实现负载均衡。

图 *3:* 在 防火墙管理中心 中的分支机构 *Firewall Threat Defense* 上配置策略型路由



Before you begin

此示例假定您已为 防火墙管理中心 中的分支机构 Firewall Threat Defense 配置 WAN 和 VTI 接口。

过程

步骤 1 为分支机构 Firewall Threat Defense 配置策略型路由，选择入口接口：

a) 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 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：

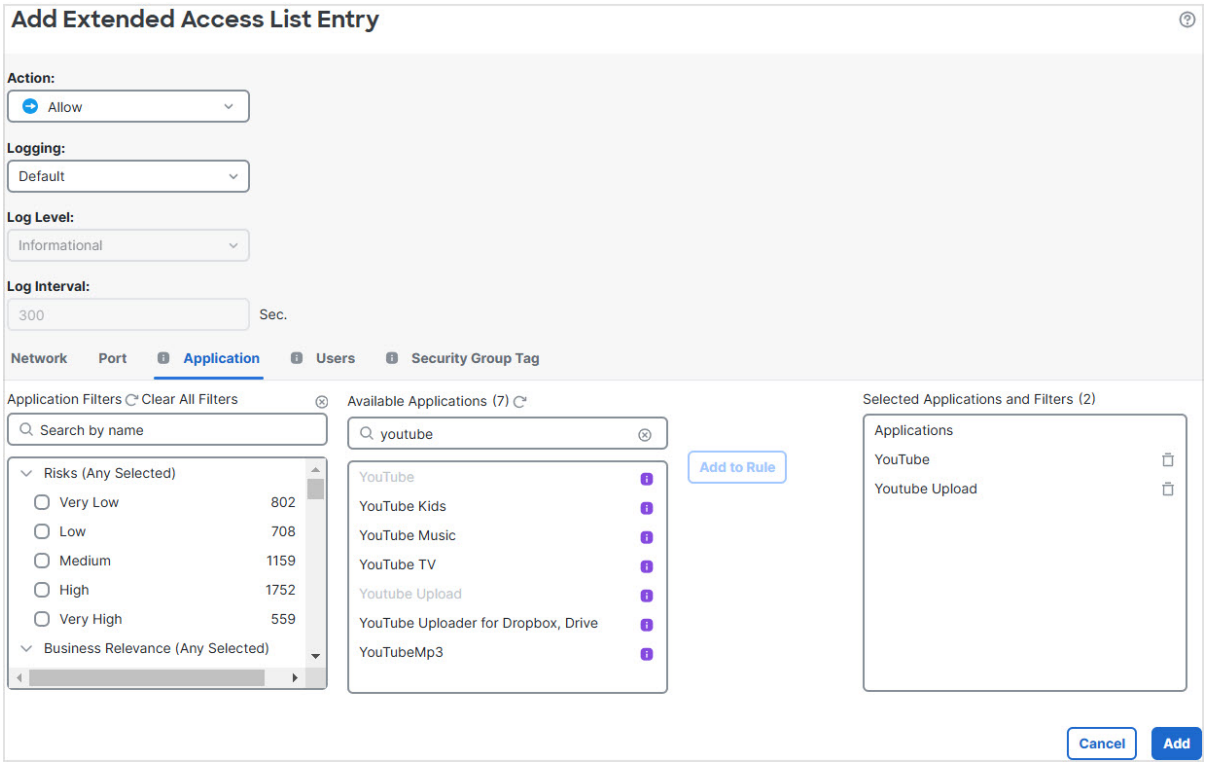
a) 点击**添加 (Add)**。

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**中，输入 ACL 的名称（例如 *DIA-FTD-Branch*），然后点击**添加**。

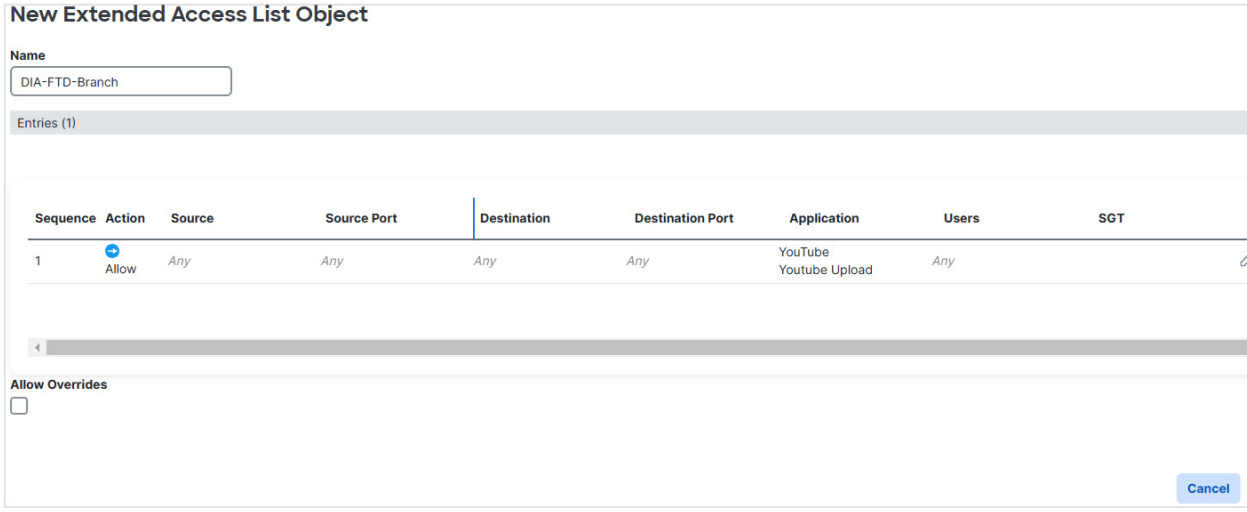
d) 在**添加扩展访问列表条目 (Add Extended Access List Entry)** 对话框中，从**应用 (Application)** 选项卡中选择所需的基于 Web 的应用：

图 *4:*“应用”选项卡



在 Firewall Threat Defense 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 *5:* 扩展 *ACL*



e) 点击**保存**。

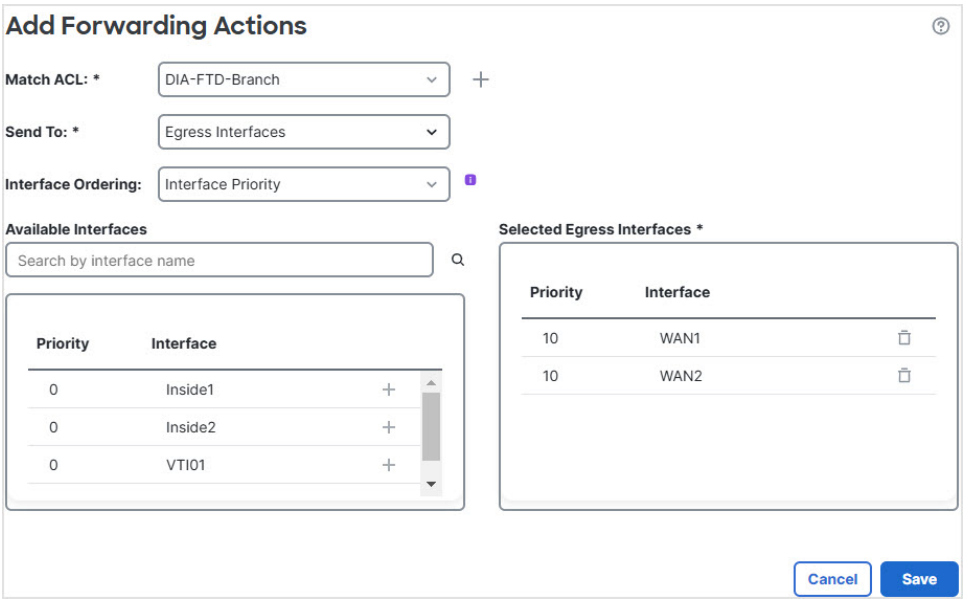
f) 从**匹配 ACL (Match ACL)** 下拉列表中选择 *DIA-FTD-Branch*。

步骤 3 指定出口接口：

a) 从**发送到 (Send To)** 和**和接口排序 (Interface Ordering)** 下拉列表中，分别选择“出口接口”(Egress Interfaces) 和“接口优先级”(Interface 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 *6:* 配置策略型路由



c) 点击**保存**。

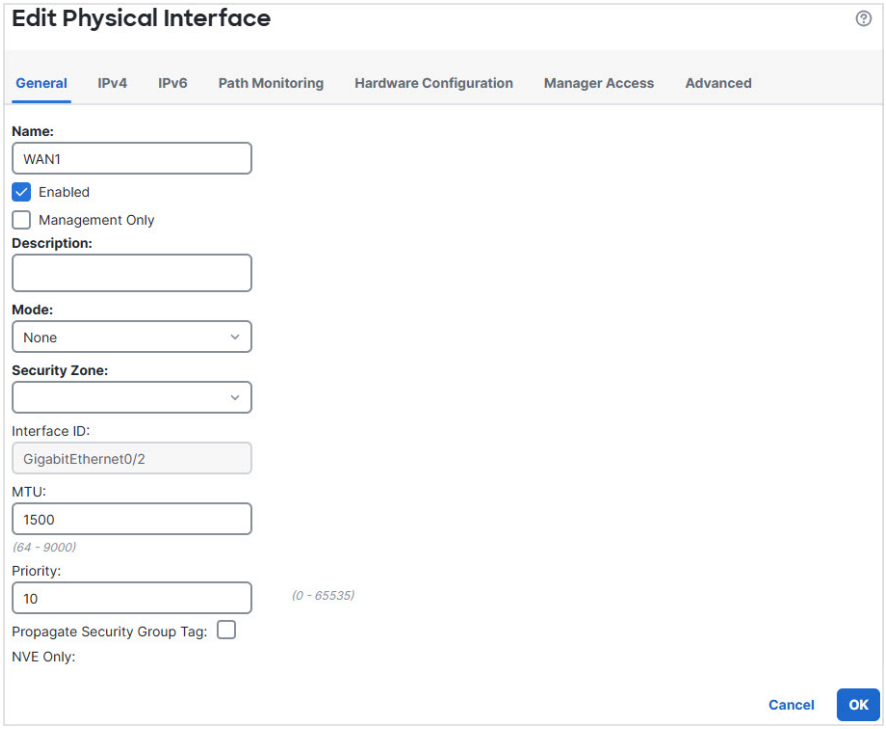
步骤 4 配置接口优先级

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** > **设备管理**，然后编辑分支 Firewall Threat Defense。

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 *7:* 设置接口优先级



c) 点击**确定** 和**保存**。

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*：

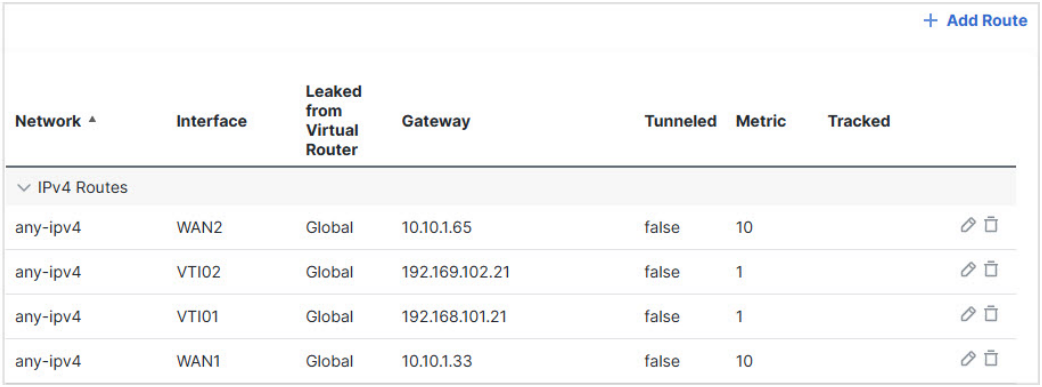
图 *8:* 将接口与 ***ECMP*** 区域相关联

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 *9:* 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 Firewall Threat Defense 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** > **平台设置**，然后在分支 Firewall Threat Defense 上创建 DNS 策略。
b) 要指定受信任的 DNS，请编辑策略，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 点击**保存**，然后点击**部署**。

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。

如果配置了 ECMP，就可以无缝地平衡网络流量。

配置具有路径监控的 PBR

配置具有路径监控的 PBR，通过基于性能指标（例如抖动、往返时间和丢包）动态选择最佳出口接口来优化应用流量路由。

本示例描述了如何为以下应用配置具有路径监控的 PBR，并使用灵活的指标：

- 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）。

Before you begin

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*。

按照以下步骤配置具有路径监控的 PBR：

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 Firewall Threat Defense。
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 7 页）。
d) 点击**确定** 和**保存**。
e) 重复这些步骤以便为 *ISP02* 和 *ISP03* 配置路径监控设置。

步骤 2 为组织 Firewall Threat Defense 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 Firewall Threat Defense 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) 点击**添加 (Add)**。
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** 对话框中，从**应用**选项卡中选择基于 Web 的必要应用（例如 WebEx 会议）。

记住
在 Firewall Threat Defense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) 点击**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) 点击**保存**。

步骤 5 重复步骤 2 和步骤 3，为 *Inside1* 接口创建 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**。
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**。

步骤 6 点击**保存**，然后点击**部署**。

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 8 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。

用于监控 PBR 的有用 CLI

从 Firewall Threat Defense 设备 CLI 运行本主题中所述的监控命令。

接口配置

要查看设备的接口配置，请运行 `show run interface` 命令：

```
> show run interface
!
interface Ethernetl/l
 description Outside ispl handoff
 nameif outside1
 security-level 0
 zone-member ECMP-WAN
 ip address dhcp setroute
 policy-route cost 10
 policy-route path-monitoring 8.8.8.8
 policy-route path-monitoring object-group network-service FMC_NSG_4295470581 policy-route
 path-monitoring object-group network-service FMC_NSG_4295470600
!
interface Ethernet1/2
 description Outside isp2 handoff
 nameif outside2
 security-level 0
```

```
 zone-member ECMP-WAN
 ip address 192.133.243.240 255.255.255.192
 policy-route cost 20
 policy-route path-monitoring 8.8.8.8
 policy-route path-monitoring object-group network-service FMC_NSG_4295470581 policy-route
 path-monitoring object-group network-service FMC_NSG_4295470600
!
```

DNS 配置

基于应用的路由仅使用受信任的 DNS 服务器来解析域。要查看设备的 DNS 配置，请运行 `show run DNS` 命令：

```
> show run dns
DNS server-group DefaultDNS
dns trusted-source 10.100.0.5
dns trusted-source 10.200.0.5
```

路由地图配置

当您在设备上配置PBR时，管理中心会自动生成路由映射并将其应用到指定入口接口。要查看设备的路由映射，请运行 `show run route-map` 命令：

```
> show run route-map
!
route-map FMC_VPN_CONNECTED_DIST_RMAP_1000 permit 10
 match interface inside-employee
 set community 1000
!
route-map FMC GENERATED PBR 1729024850865 permit 5
 match ip address Cloud-storage-apps-acl
  set adaptive-intertace cost outside1 outside2

!
route-map FMC_GENERATED PBR 1729024850865 permit 10
match ip address Social-media-apps-acl
set adaptive-interface rtt outsidel outside2

!
route-map FMC GENERATED PBR 1729024850865 permit 15
match ip address Conferencing-apps-acl
set adaptive-interface jitter outside1 outside2

!
route-map FMC_GENERATED_PBR_1729024850865 permit 20
match ip address Corp-internal-apps-acl
set adaptive-interface cost outsidel_static_vti_1 outside2_static_vti_4
```

访问列表和网络服务组配置

应用到入口接口的路由映射可以引用扩展访问控制列表。要查看 PBR 的访问列表的详细信息，请运行 `show run access list <access list_name>` 命令：

```
> show run access-list Cloud-storage-apps-acl
access-list Cloud-storage-apps-acl extended permit ip any object-group-network-service
FMC_NSG_4295470562
```

网络服务对象和对象组在扩展访问控制列表中进行配置，并在策型路由路由地图和访问控制组中引用。要查看 NSG 配置，请运行 `show object-group network-service <network-service-groups-name>` 命令。*network-service-groups-name* 派生自上述访问列表的 show 命令。

```
> show object-group network-service FMC_NSG_4295470562
 object-group network-servire FMC_NSG_4295470562 (id=@xfdff0000)
 network-service-member "Box" dynamic
 description File storage and transfer site.
 app-id 1326
 domain box.com (bid=436735707) ip (hitcnt=0)
 domain boxcloud.com (bid=436924171) ip (hitcnt=0)
 domain box.net (bid=437080553) ip (hitcnt=0)
 domain box.org (bid=437174273) ip (hitcnt=0)
 domain boxcdn.net (bid=437272231) ip (hitcnt=0)
 domain boxrelay.com (bid=437481703) ip (hitcnt=0)
 domain boxenterprise.net (bid=437626005) ip {hitcnt=0)
 domain boxinvestorrelations.com (bid=437672765) ip (hitcnt=0)
 domain segment-box.com (bid=437886771) ip (hitcnt=0)
 domain box-corp.com (bid=437924995) ip (hitcnt=0)
 domain boxcn.net (bid=438072833) ip (hitcnt=0)
network-service-member "Dropbox" dynamic
 description Cloud based tile storage.
 app-id 125
 domain dropbox.com (bid=24259639) ip (hitcnt=0)
 domain cfl.dropboxstatic.com (bid=24495525) ip (hitcnt=0)
 domain dl.dropboxusercontent.com (bid=24596237) ip (hitcnt=0)
 domain dropboxapi.com (bid=24694467) ip (hitcnt=0)
 domain dropboxbusiness.com (bid=24859859) ip (hitcnt=0)
 domain dropboxcaptcha.com (bid=25008145) ip {hitcnt=0)
 domain dropbox-dns.com (bid=25087753) ip (hitcnt=0)
 domain dropboxer.net (bid=25236751) ip (hitcnt=0)
 domain dropboxusercontent.com (bid=25324335) ip (hitcnt=0)
 domain getdropbox.com (bid=25437501) ip (hitcnt=0)
 domain cloudon.com (bid=25580229) ip (hitcnt=0)
```

路径监控配置

要查看在出口接口上收集的路径监控指标，请运行 `show path-monitor` 命令：

```
> show path-monitor
Interface: outside2 (Ethernetl/2)
Remote peer: 8.8.8.8
    Remote peer reachable: Yes
    RTT average: 9138 microsecondes) Jitter: 1093 microsecond(s)
    Packet loss: 0% MOS: 4.39
    Last updated: 12 second(s) ago
Interface: outside2 (Ethernetl/2)
Remote NSG: FMC_NSG_4295470581
    Network Service: Facebook Domain name: fbsbx.com Remote peer reachable: Yes
    RTT average: 17460 microsecond(s) Jitter: 911 microseconde)
    Packet loss: 0%
    MOS: 4.39
    Last updated: 12 second(s) ago

    Network Service: Facebook
    Domain name: facebook.net
    Remote peer reachable: Yes
    RTT average: 17444 microsecondes)
    Jitter: 836 microsecondes)
    Packet loss: 0%
    MOS: 4.39
    Last updated: 12 second(s) ago
```

```
    Network Service: Instagram
    Domain name: instagram.com Remote peer reachable: Yes
    RTT average: 17576 microsecondes)
    Jitter: 429 microsecondes)
    Packet loss: 0%
    MOS: 4.39
    Last updated: 12 secondes) ago

Interface: outside2 (Ethernetl/2)
Remote NSG: FMC_NSG_4295470600
    Network Service: WebEx
    Domain name: webex.com Remote peer reachable: Yes RTT average: 18537 microsecond(s)
Jitter: 318 microseconde)
    Packet loss: 0%
    MOS: 4.39
    Last updated: 12 second(s) ago
    Network Service: Zoom Domain name: zoom.com Remote peer reachable: Yes
    RTT average: 98196 microsecond(s) Jitter: 4120 microseconde)
    Packet loss: 0%
    MOS: 4.34
    Last updated: 12 second(s) ago
```

对PBR进行故障排除

当数据包被丢弃时，此任务可以通过验证路由、监控指标和验证接口选择来调试 PBR 配置。

当 PBR 未按预期工作时，您需要系统地验证包括路由映射、路径监控和接口选择在内的配置组件，以确定数据包的根本原因。

Before you begin

当数据包被丢弃时，请按照以下步骤来排除 PBR 配置故障：

过程

步骤 1 在相应的表中使用 show route 或 show ipv6 route 命令，检查是否存在进行递归解析的所有必要路由。

除非使用正确的路由更新参与 PBR 中接口的路由映射，否则 PBR 将无法按预期工作。

步骤 2 通过使用 **show running-config interface** 命令来显示路径监控用于监控指标的远程地址。

示例：

```
interface GigabitEthernet0/0
nameif outside_0
security-level 0
zone-member ecmp-zone
ip address 20.0.0.3 255.255.255.0 -> This is egress interface "show running-config" output,
 the monitored address and cost metric value is determined in this output.
policy-route cost 1
policy-route path-monitoring
20.0.0.4
!
int GigabitEthernet 0/3
!
interface GigabitEthernet0/3
nameif outside_3
```

```
security-level 0
ip address 11.1.1.2 255.255.255.0 -> This is ingress interface "show running-config" output,
 the specific route-map will be used by PBR to determine the next route.
policy-route route-map rtt-tes
```

此命令通过发送 ICMP 数据包或 HTTP ping 显示路径监控的受监控地址和开销指标值。

步骤 3 检查 **show path-monitoring** 和 **show run route-map** 输出是否存在丢包。

示例：

```
ciscoasa(config)# show path-monitoring
Interface: outside_0  -> The remote address used for ICMP monitoring
Remote peer: 20.0.0.4
Version: 6223
Remote peer reachable: Yes -> If this value turns "No", then the ICMPv4/v6 packet is not
reaching the required remote address.
RTT average: 1920 microsecond(s)
Jitter: 394 microsecond(s)
Packet loss: 0%
MOS: 4.40
Last updated: 17 second(s) ago -> The data should be updated by path monitoring after every
 30 seconds. The 'show route-map' would show the
updated metric values.
Interface: outside_2
Remote peer: 40.0.0.4
Version: 6223
Remote peer reachable: Yes
RTT average: 1935 microsecond(s)
Jitter: 433 microsecond(s)
Packet loss: 0%
MOS: 4.40
Last updated: 17 second(s) ago
```

示例：

```
ciscoasa(config)# show route-map
route-map rtt-test, permit, sequence 10
Match clauses:
Set clauses:
adaptive-interface rtt outside_0 (1920) outside_2 (1935) outside_1 (1971) -> Displays the
metric type (rtt) that is used by the policy route to select the adequate interface to send
 the packet. The interface list where cost of each interface is given. As the metric type
is "rtt" and considering the minimum rtt value, the "outside_0" interface route will be
selected by PBR.
route-map mos-test, permit, sequence 10
Match clauses:
Set clauses:
adaptive-interface mos outside_0 (378) outside_1 (390) outside_2 (440) - > As the metric
type is "mos", considering the maximum value of mos, the "outside_2" interface will be
selected by PBR.
```

指标类型（丢失、rtt、抖动、成本）应选择具有最小指标值的接口进行路由。

指标类型“MOS”应选择具有最大指标值的接口进行路由。

步骤 4 使用 **packet-tracer** 命令根据 PBR 中定义的指标类型验证接口选择。

示例：

```
packet-tracer input <interface> icmp <src ip address> 8 0 <dst ip
address> detailed
Phase: 3
Type: PBR-LOOKUP
Subtype: policy-route
```

```
Result: ALLOW
Elapsed time: 60656 ns
Config:
route-map rtt-test permit 10
match ip address allow_101_1_1_2
set adaptive-interface rtt outside_0 outside_2
Additional Information:
Matched route-map rtt-test, sequence 10, permit
Found next-hop 40.0.0.4 using egress ifc outside_2 -> PBR selects the adequate interface
from adaptiveinterface list given in "rtt-test" route-map.
```

步骤 5 使用类似 **debug policy-route** 命令的 **packet-tracer** 命令。

当 PBR 成功选择路由后，数据包跟踪器输出将如下所示：

```
pbr: policy based route lookup called for 101.1.1.1/0 to 101.1.1.2/0 proto 1 sub_proto 8
received on
interface outside_3, NSGs, nsg_id=none
pbr: First matching rule from ACL(-1)
pbr: route map rtt-test, sequence 10, permit; proceed with policy routing
pbr: policy based routing applied; egress_ifc = outside_2 : next_hop = 20.0.0.4
```

当 PBR 无法找到适当的路由时，它会回退到正常路由查找，数据包跟踪器输出如下所示：

```
pbr: policy based route lookup called for 100.1.1.1/0 to 100.1.1.2/0 proto 1 sub_proto 8
received on interface outside_3, NSGs, nsg_id=none
pbr: First matching rule from ACL(-1)
pbr: route map mos-test, sequence 10, permit; proceed with policy routing
pbr: no route to 100.1.1.2 on adaptive-interface outside_2
pbr: no route to 100.1.1.2 on adaptive-interface outside_1
pbr: no route to 100.1.1.2 on adaptive-interface outside_0
pbr: policy based routing could not be applied; proceeding with normal route lookup
```

当受监控的远程地址断开，并且路径监控将该地址的**远程对等体可访问**标记为**否**时，PBR 会显示日志，以从自适应接口列表中排除该接口。

```
pbr: policy based route lookup called for 100.1.1.1/0 to 101.1.1.2/0 proto 1 sub_proto 8
received on
interface outside_3, NSGs, nsg_id=none
pbr: First matching rule from ACL(-1)
pbr: route map rtt-test, sequence 10, permit; proceed with policy routing
pbr: Path Monitoring Ifc Down : adaptive-interface outside_1 Excluded from PBR routing
pbr: policy based routing applied; egress_ifc = outside_2 : next_hop = 40.0.0.4
```

注释
当接口在路径监控模块中报告为可访问时，该接口就符合自适应 PBR 路由的条件。

策略型路由的历史记录

本参考提供了全面的历史记录表，总结了思科 Secure Firewall Management Center 各版本中策略型路由功能的介绍和演变，支持快速跟踪功能的可用性和变更。

表 *1:* 历史记录表

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
PBR 中的自定义应用检测器支持	10.0.0	10.0.0	通过使用高级检测器类型选项，可以使用包含检测器模式的 .lua 文件创建自定义检测器。创建的自定义检测器模式然后可以在基于应用的PBR策略的扩展 ACL 中使用。 新增/修改的屏幕：未添加新的或修改的屏幕。
PBR 中的自定义应用检测器支持	7.7	7.7	现在可以创建具有自定义应用域的PBR策略。用户定义的域创建为自定义检测器模式，可以在基于应用的 PBR 策略的扩展 ACL 中使用。 新增/修改的屏幕：未添加新的或修改的屏幕。
基于身份和 SGT 的 PBR 策略	7.4.0	7.4.0	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，用于配置策略型路由策略：**对象 (Objects)** > **对象管理 (Object Management)** > **访问控制列表 (Access Control Lists)** > **添加扩展 (Add Extended)** 页面，**用户 (Users)** 和 **安全组标记 (Security Group Tag)**。
基于 HTTP 的路径监控	7.4.0	7.2.0	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 (Devices)** > **设备管理 (Device Management)** > **编辑接口 (Edit Interfaces)** > **路径监控 (Path Monitoring)** > **启用基于 HTTP 的应用监控 (Enable HTTP based Application Monitoring)** 复选框。
双 WAN/ISP 威胁防御管理支持	7.3.0	7.3.0	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。
PBR 路由映射的下一跳设置	7.3.0	7.1.0	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。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
PBR 和路径监控	7.2.0	7.2.0	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。
从 FMC Web 界面配置策略型路由。	7.1.0	7.1.0	**升级影响。升级后重新设置 FlexConfig**。 您现在可以从 FMC Web 界面配置策略型路由 (PBR)。您可以根据应用对网络流量进行分类，并实施直接互联网接入 (DIA) 以将流量从分支机构部署发送到互联网。您可以定义PBR策略并在入口接口上进行配置，从而指定匹配条件和出口接口。根据策略中配置的优先级或顺序，通过出口接口转发与访问控制策略匹配的网络流量。 此功能需要 FMC 和设备上的版本 7.1+。将 FMC 升级到版本 7.1+ 时，将删除现有的策略型路由 FlexConfig。将设备升级到版本 7.1+ 后，请在 FMC Web 界面中重新执行策略型路由配置。对于未升级到版本 7.1+ 的设备，请重做 FlexConfig 并将其配置为“每次”部署。 新增/修改的屏幕： **设备** > **设备管理** > **路由** > **策略型路由**

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。