策略型路由

本章介绍如何配置 ASA 以支持基于策略的路由 (PBR)。以下部分介绍基于策略的路由、PBR 准则和 PBR 配置。

关于策略型路由

传统路由是以目标为基础的，这意味着数据包基于目标 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。使用基于策略的路由 (PBR)，您可以基于非目标网络的条件定义路由 - 通过 PBR，可以基于源地址、源端口、目标地址、目标端口、协议或所有这些的组合来路由流量。

基于策略的路由：

- 用于为差分流量提供服务质量 (QoS)。
- 用于跨低带宽、低成本的永久路径以及高带宽、高成本的交换路径分发交互式和批处理流量。
- 允许互联网运营商及其他组织通过明确定义的网络连接来路由源自各组用户的流量。

基于策略的路由通过在网络边缘对流量进行分类和标记，然后在整个网络中使用 PBR 沿着特定路径路由标记的流量，来实施 QoS。这样，可以将源自不同源的数据包路由至不同网络，甚至在目标不同时亦可以；并且在将多个私有网络互连时，这一点可能很有用。

为什么使用基于策略的路由？

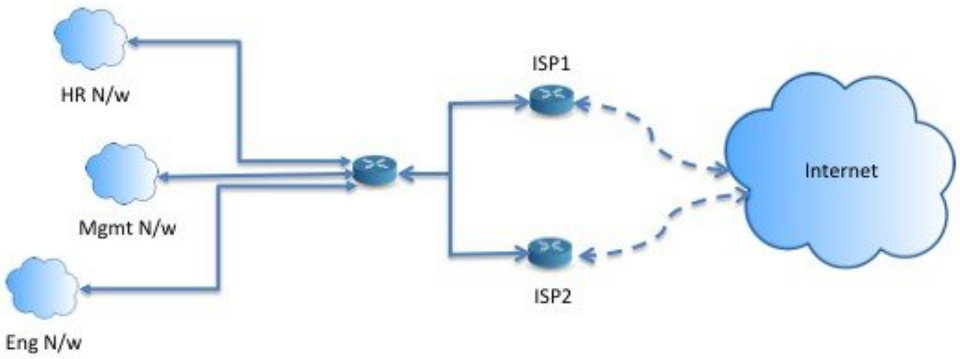
假设一家公司在不同位置之间有两条链路：一条是高带宽、低延迟、较为昂贵的链路，而另一条是低带宽、高延迟、不太昂贵的链路。使用传统路由协议时，高带宽链路将基于通过该链路的带宽和/或延迟（使用 EIGRP 或 OSPF）特性所实现的指标节约而获得大部分（如果不是全部）跨该链路发

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。

基于策略的路由的部分应用为：

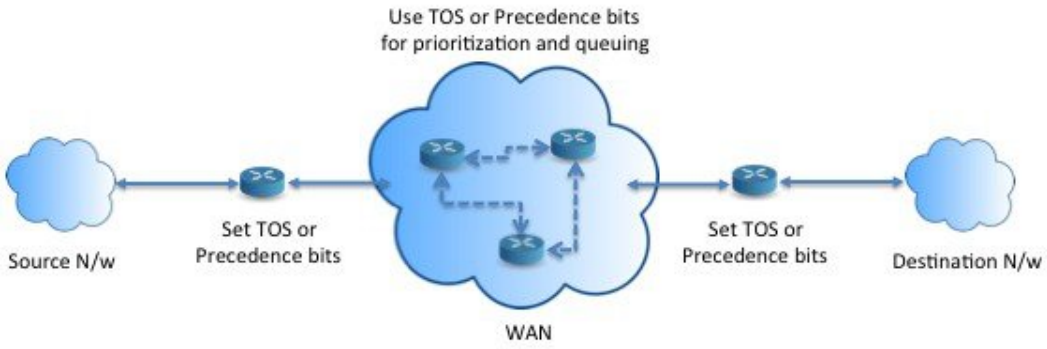
同等访问权限和源敏感路由

在此拓扑中，来自人力资源网络和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，基于策略的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。



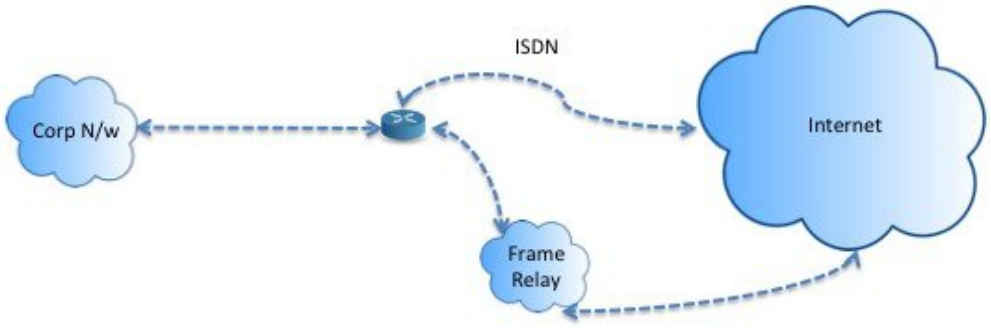
服务质量

通过标记使用基于策略的路由的数据包，网络管理员可以在网络边界对各种服务级别的网络流量进行分类，然后使用优先级、自定义或加权公平排队（如下图所示）在网络核心中实施这些服务级别。此设置无需在主干网络核心中的每个 WAN 接口对流量进行明确分类，从而能够提升网络性能。



成本节约

组织可以通过定义拓扑，将与特定活动关联的批处理流量定向为在短时间内使用较高带宽的高成本链路，并将较低带宽的低成本链路上的基本连接继续用于交互式流量，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，管理员可以配置基于策略的路由来对从人力资源网络至 ISP1 的流量和从工程网络至 ISP2 的流量进行负载共享。

实施 PBR

ASA 使用 ACL 来匹配流量，然后对流量执行路由操作。具体而言，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。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。

注释 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。

基于策略的路由准则

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。

每数据流路由

由于ASA基于每个数据流执行路由，所以会在第一个数据包上应用策略路由，并将生成的路由决策存储在为该数据包创建的数据流中。属于同一连接的所有后续包将简单地与此数据流匹配并正确进行路由。

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。

集群

- 支持集群。
- 在集群情景下，没有静态或动态路由，已启用ip-verify-reverse路径，非对称流量可能会被丢弃。因此，建议禁用 ip-verify-reverse 路径。

IPv6 支持

支持 IPv6

路径监控准则

以下是在接口上配置路径监控的准则：

- 接口必须具有名称。
- 管理专用接口不能配置路径监控。要配置路径监控，必须取消选中**将此接口用于管理**复选框。
- 在透明或多情景系统模式下的设备上不支持路径监控。
- 隧道接口不支持自动监控类型（auto、auto4 和 auto6）。
- 无法为以下接口配置路径监控：
  - BVI
  - 环回
  - DVTI

其他准则

- 所有现有路由映射相关的配置限制和局限性都将继续适用。
- 请勿将包含匹配策略列表的路由映射用于基于策略的路由。match policy-list 仅用于 BGP。

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。

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。

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。

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，第 6 页。

配置路径监控

您可以配置路径监控，以根据网络服务组执行基于策略的路由。要在没有NSG的情况下使用路径监控，可以导航至 **接口** > **编辑** 页面并指定路径监控类型。请参阅 步骤 8。

过程

步骤 1 在 ASDM 中，依次选择 **配置** > **设备设置** > **接口设置** > **接口**。

步骤 2 从 **接口** 下拉列表中选择接口。

步骤 3 在 **可用网络服务组** 复选框中选择网络服务组 (NSG)。要选择多个 NSG，请使用 Ctrl 键并点击所需的 NSG。

步骤 4 点击 **添加** 以添加网络服务组。

步骤 5 点击 **Apply**。

步骤 6 要删除配置，请从 **添加的网络服务组** 复选框中选择 NSG，然后点击 **删除**，然后点击 **应用**。

配置基于策略的路由

路由映射由一个或多个路由映射语句组成。每个语句都有序列号以及 permit 或 deny 子句。每个 route-map 语句都包含 match 和 set 命令。match 命令表示要对数据包应用的匹配条件。set 命令表示要对数据包采取的操作。

- 在路由映射同时配置有 IPv4 和 IPv6 match/set 子句时或在使用了与 IPv4 和 IPv6 流量匹配的统一 ACL 时，将根据目标 IP 版本应用 set 操作。
- 当多个下一跳或接口被配置为 set 操作时，系统将逐个评估所有选项，直到找到有效的可用选项。在已配置的多个选项之间将不进行负载均衡。
- Verify-availability 选项不支持多情景模式。

过程

步骤 1 在 ASDM 中，配置一个或多个标准或扩展 ACL 以识别要对其执行基于策略的路由的流量。请参阅 **Configuration** > **Firewall** > **Advanced** > **ACL Manager**。

步骤 2 依次选择**配置** > **设备设置** > **路由** > **路由图**，然后点击**添加**。

此时将显示 **Add Route Map** 对话框。

步骤 3 输入路由映射名称和序列号。对于可选的其他路由映射语句将使用此同一名称。序列号为ASA评估路由映射的顺序。

步骤 4 点击 **Deny** 或 **Permit**。

此外，ACL 还包括自己的 permit 和 deny 语句。对于路由映射与 ACL 之间的 Permit/Permit 匹配，继续执行基于策略的路由处理。对于 Permit/Deny 匹配，对此路由映射的处理结束并检查其他路由映射。如果结果仍是 Permit/Deny，则使用普通路由表。对于 Deny/Deny 匹配，继续基于策略的路由处理。

步骤 5 点击 **Match Clause** 选项卡以识别您创建的 ACL。

在 **Ipv4** 部分，从下拉菜单中选择 **Access List**，然后从对话框中选择一个或多个标准或扩展 ACL。

注释 确保访问列表不包含任何非活动规则。不能将具有非活动规则的匹配ACL设置为PBR。

如果使用标准ACL，则仅基于目标地址进行匹配。如果使用扩展ACL，可基于源、目标或两者进行匹配。

对于 IPv4 和 IPv6 ACL，使用 IPv4 部分。对于扩展 ACL，可以指定 IPv4、IPv6、身份防火墙或思科 TrustSec 参数。您还可以包括网络服务对象。有关完整语法，请参阅 ASA 命令参考。

步骤 6 点击 **Policy Based Routing** 选项卡以定义用于流量流的策略。

选中以下要为匹配的流量流执行的一个或多个 set 操作：

- **Set PBR next hop address** - 对于 IPv4 和 IPv6，可以配置多个下一跳 IP 地址，在这种情况下将按指定顺序对它们进行评估，直到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，否则不会应用 set 操作。
- **Set default next-hop IP address** - 对于 IPv4 和 IPv6，如果匹配流量的正常路由查询失败，则 ASA 会使用此指定的下一跳 IP 地址转发流量。
- **Recursively find and set next-hop IP address** - 下一跳地址和默认下一跳地址都要求可在直连式子网中找到下一跳。使用此选项时，下一跳地址不需要是直连式。匹配流量不会在下一跳地址上执行递归查询，而是根据路由器中使用的路由路径被转发到该路由条目使用的下一跳中。
- **Configure Next Hop Verifiability** - 验证路由映射的下一 IPv4 跳是否可用。您可以配置 SLA 监控跟踪对象来验证下一跳的可访问性。点击 **Add** 以添加下一跳 IP 地址条目，并指定以下信息。
  - **Sequence Number** - 使用序列号按顺序评估条目。
  - **IP Address** - 输入下一跳 IP 地址。
  - **Tracking Object ID** - 输入有效的 ID。
- **Set interfaces** - 此选项可配置通过其转发匹配流量的接口。您可以配置多个接口，在这种情况下将按指定顺序对它们进行评估，直到找到有效的接口。当指定 **null0** 时，匹配路由映射的所有流量将被丢弃。对于可通过指定接口（静态或动态）路由的目标，必须存在路由。
- **设置子句 > 自适应接口成本** - 此选项位于“设置子句”选项卡上，而不是“**基于策略的路由**”选项卡上。此选项根据接口的成本设置输出接口。点击“**可用接口**”字段并选择应考虑的接口。出口接口从接口列表中选择。如果接口的成本相同，则这是主用-主用配置，数据包在出口接口上进行负载均衡（轮询）。如果成本不同，则选择成本最低的接口。仅当接口处于启用状态时，才会考虑这些接口。
- **Set null0 interface as the default interface** - 如果正常路由查询失败，ASA 将转发流量 null0，并且该流量将被丢弃。
- **Set do-not-fragment bit to either 1or 0** - 选择相应的单选按钮。
- **Set differential service code point (DSCP) value in QoS bits** - 从 IPv4 或 IPv6 下拉列表中选择值。

步骤 7 点击“**确定**”，然后点击“**应用**”。

步骤 8 依次选择Configuration Device Setup Interface Settings Interfaces，并配置应应用此路由映射来确定出口接口的入口接口。 > > >

a) 选择一个流入接口并点击**编辑 (Edit)**。

b) 在“**路由映射**”中，选择应应用的基于策略的路由映射。
c) 如果您使用的是“**自适应接口成本**”来选择路由映射中的输出接口，请设置接口的“**成本**”。

   值可以是 1-65535。默认值为 0，您可以通过删除此字段中的值进行重置。数值越低，优先级越高。例如，1 的优先级高于 2。

d) 要使 PBR 使用灵活的指标来确定路由数据包的最佳路径，请从**路径监控 (Path Monitoring)** 下拉列表中选择相关的监控类型：

   - **auto** - 将 ICMP 探测发送到接口的 IPv4 默认网关（如果存在 - 与自动 IPv4 相同）。否则，发送到接口的 IPv6 默认网关（与自动 IPv6 相同）。
   - **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，则会启用相邻字段。在字段中输入 IPv4 地址。
   - **ipv6** - 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，则会启用相邻字段。在字段中输入 IPv4 地址。
   - **自动4**-将 ICMP 探测发送到接口的 IPv4 默认网关。
   - **自动6**-将 ICMP 探测发送到接口的默认 IPv6 网关。
   - **无** - 禁用接口的路径监控。

e) 点击 **OK**，然后点击 **Apply**。

基于策略的路由的历史记录

表 *1:* 路由映射的历史记录

功能名称	平台版本	功能信息
通过 HTTP 客户端进行路径监控	9.20(1)	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。基于 HTTP 的路径监控可以使用网络服务组对象在接口上进行配置。 新增/修改的菜单项：**配置 (Configuration)** > **设备设置 (Device Setup)** > **接口设置 (Interface Settings)** > **路径监控 (Path Monitoring)**
PBR 中的路径监控指标。	9.18(1)	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。 新增/修改的菜单项： **配置** > **设备设置** > **接口设置** > **接口**

功能名称	平台版本	功能信息
基于策略的路由	9.4(1)	基于策略的路由 (PBR) 是一种机制，基于该机制，流量可以使用 ACL，通过带有指定 QoS 的特定路径进行路由。基于数据包的第 3 层和第 4 层报头的内容，ACL 可以对流量进行分类。管理员通过此解决方案可向不同的流量提供 QoS，在低带宽、低成本永久路径与高带宽、高成本交换式路径之间分发交互式和批处理流量，并允许互联网运营商和其他组织通过明确定义的互联网连接来路由源自各类用户的流量。 更新了以下屏幕：Configuration > Device Setup > Routing > Route Maps > Policy Based Routing， Configuration > Device Setup > Routing > Interface Settings > Interfaces
为策略型路由提供 IPv6 支持	9.5(1)	策略型路由现在支持 IPv6 地址。 修改了以下菜单项： **配置 > 设备设置 > 路由 > 路由映射 > 添加路由映射 > 基于策略的路由配置 > 设备设置 > 路由 > 路由映射 > 添加路由映射 > 匹配语句**
为策略型路由提供 VXLAN 支持	9.5(1)	现在您可以在 VNI 接口中启用策略型路由。 修改了以下菜单项：**配置 > 设备设置 > 接口设置 > 接口 > 添加/编辑接口 > 常规**
为身份防火墙和思科 TrustSec 提供策略型路由支持	9.5(1)	您可以先配置身份防火墙和思科 TrustSec，然后再在策略型路由的路由图中使用身份防火墙和思科 TrustSec ACL。 修改了以下菜单项：**配置 > 设备设置 > 路由 > 路由映射 > 添加路由映射 > 匹配语句**

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。