使用直接互联网接入(DIA)将应用流量从分支机构路由到互联网

在本章中，我们将深入探讨直接互联网接入 (DIA) 的实际应用。该使用案例详细介绍了场景、网络拓扑、最佳实践和前提条件。它还为无缝实施提供了全面的端到端程序。

直接互联网接入

数字创新正在改变企业运营、沟通以及与客户互动的方式。这促使新的应用和技术应运而生，以改善协作和客户体验，并要求高带宽和低延迟连接。

传统网络面临的挑战

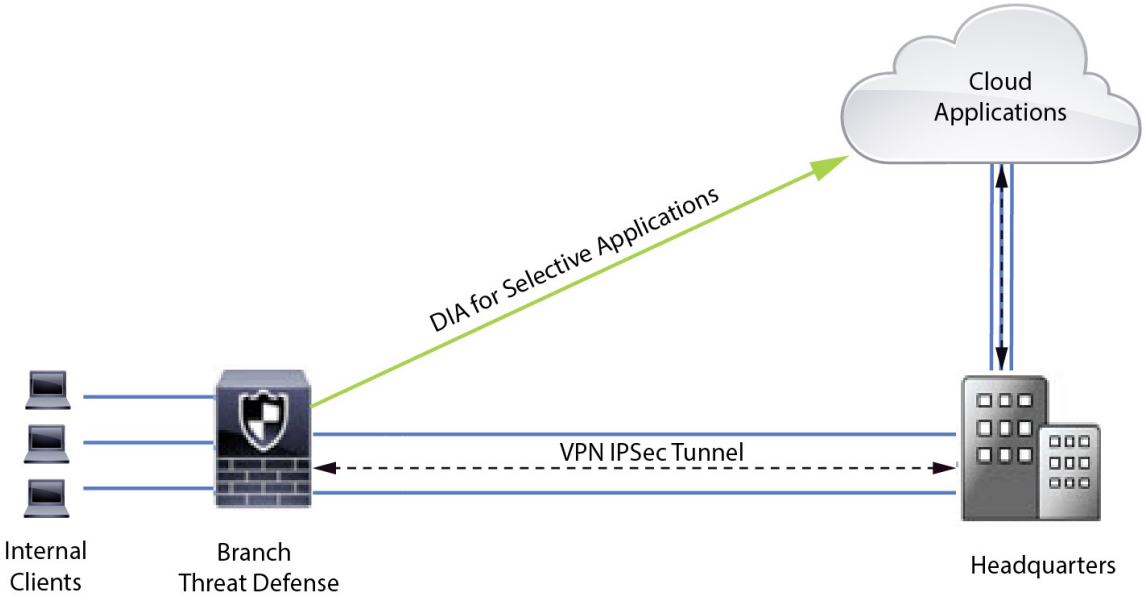
传统上，网络部署会利用中心站点上的边界防火墙来为本地和分支机构用户提供安全访问。这种架构可提供所需的连接，但它会将所有互联网流量作为加密流量通过VPN隧道传输到中心站点，从而导致数据包延迟、丢包和抖动。此外，网络还不断面临着与部署和复杂的网络管理相关的高成本和带宽利用率的挑战。

解决方案

克服这些挑战的方法之一是使用直接互联网接入 (DIA)。DIA 是 Cisco Secure Firewall 的“简化的分支机构”功能的一个组件。DIA 使用策略型路由 (PBR)。DIA 也被称为应用感知路由。

在 DIA 拓扑中，分支机构的应用流量会被直接路由到互联网，从而绕过了通过隧道将互联网流量传输到总部的延迟。分支机构 Cisco Secure Firewall Threat Defense 配置了互联网出口点。PBR 策略被应用于入口接口，以便根据扩展访问控制列表中定义的应用来识别流量。相应地，流量会通过出口接口直接转发到互联网。

图 *1:* 通过特定出口接口直接访问互联网



为什么要使用策略型路由？

您可以使用 PBR 来对指定应用的流量进行分类和安全分离。它还允许您为某些流量指定路径。您可以在 Cisco Secure Firewall Management Center 用户界面中配置 PBR 策略，以便允许直接访问应用。

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。在 Cisco Secure Firewall Management Center 版本 7.2 及更高版本中，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）。PBR 会使用这些指标来确定转发流量的最佳路径（出口接口）。当指标被修改时，路径监控会定期通知 PBR 有关被监控接口的信息。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，为出口接口配置监控类型并配置应用流量，以便利用使用指标值的路径监控。

要了解路径监控，请参阅场景 2：具有路径监控的直接互联网接入。

优势

使用 DIA 的优势包括

- 提高网速并改善分支机构用户体验。
- 降低复杂性，使网络管理更轻松、成本更低。
- 成本效益高，因为它减少了带宽使用量，无需昂贵的硬件。
- 使用实时指标的动态路径选择。
- 保证最佳出口路径，无需人工干预。
- 持续监控链路运行状况和网络状态。
- 提高灵活性，让组织能够快速适应不断变化的业务需求。

此使用案例适合您吗？

本使用案例的目标受众是网络设计工程师、网络运营人员和安全运营人员，他们希望在每个远程站点内实施直接互联网接入，以便从分支机构直接中断本地的互联网流量。

用于直接互联网接入的组件

分支机构防火墙用于 DIA 的一些重要组件包括：

- **受信任的 DNS 服务器** - DIA 功能中的应用检测依赖 DNS 监听来解析应用或一组应用。为确保 DNS 请求不会被恶意 DNS 服务器解析，并确实锁定到所需的 DNS 服务器，管理中心允许您为威胁防御配置受信任的 DNS 服务器。
- **接口优先级** - Cisco Secure Firewall 使用接口优先级来确定最佳互联网路径。优先级越低越好，它决定了特定 ISP 向互联网发送流量时的优先级。管理中心允许您配置威胁防御的接口优先级。
- **网络服务** - 与策略型路由中使用的特定应用关联的对象。此对象是自动创建的。
- **网络服务组 (NSG)** - 网络服务组是防火墙用于根据配置确定路径的一组应用。多个网络服务对象可以是单个 NSG 的一部分。管理中心根据为基于策略路由配置的扩展访问列表来自动生成 NSG。

最佳实践

- 必须运行 7.1 及更高版本的 Cisco Secure Firewall Threat Defense。

- 必须配置受信任的 DNS 服务器，以确保通过受信任的 DNS 服务器执行 DNS 监听，从而支持应用流量。
- 通过威胁防御的 DNS 请求必须采用明文格式且未加密，以允许 DNS 监听来促进 PBR 流。
- 必须配置 ECMP 区域，以实现应用流量的主用/主用负载均衡。
- ECMP 仅在路由防火墙模式下受支持，设备最多可拥有 256 个 ECMP 区域。
- 只能使用路由接口。每个接口只能属于一个 ECMP 区域。
- 确保接口属于正在配置 ECMP 的虚拟路由器。
- ECMP 区域配置中使用的接口必须在接口配置中定义逻辑名称。
- 验证在 Cisco Secure Firewall Threat Defense 上为 PBR 配置的每个 ECMP 区域接口不超过 8 个。
- Cisco Secure Firewall Threat Defense 不能部署在群集中，因为该模式下不支持 PBR。
- 必须为全局虚拟路由器配置 PBR，因为用户定义的虚拟路由器不支持 PBR。
- 确保 PBR 中用于入口和出口的接口是路由接口或非管理专用接口，并且属于全局虚拟路由器。

前提条件

- 使用设备管理器完成威胁防御初始配置
- 将许可证分配到设备
- 为互联网访问添加路由。请参阅添加静态路由
- 配置用于威胁防御的 NAT
- 创建基本访问控制策略

场景 1：不带路径监控的直接互联网访问

Bob 是一位客户经理，Ann 是一位服务中心专家。两人都在一家大公司的分支机构工作。最近，他们在使用 Webex 等网络会议工具和 YouTube 等流媒体平台时遇到了延迟问题。

有什么风险？

网络延迟和网络拥塞会降低网络会议和流媒体会话的性能和用户体验。这可能会影响分支机构员工的生产力和效率，从而对整体业务运营造成负面影响。

使用 PBR 的 DIA 如何解决问题？

IT 管理员 Alice 将策略型路由选择与 DIA 结合使用，以减少网络延迟。

直接互联网接入允许分支机构直接访问互联网，而无需通过中央站点或数据中心进行流量路由。这为分支机构用户提供了更直接、更优化的互联网连接，从而减少了延迟。

策略型路由选择将 Webex 和 YouTube 流量分隔在不同的出口接口上。这样确保了流量通过不同的路径，从而减轻单一接口的负担，提高了应用性能。

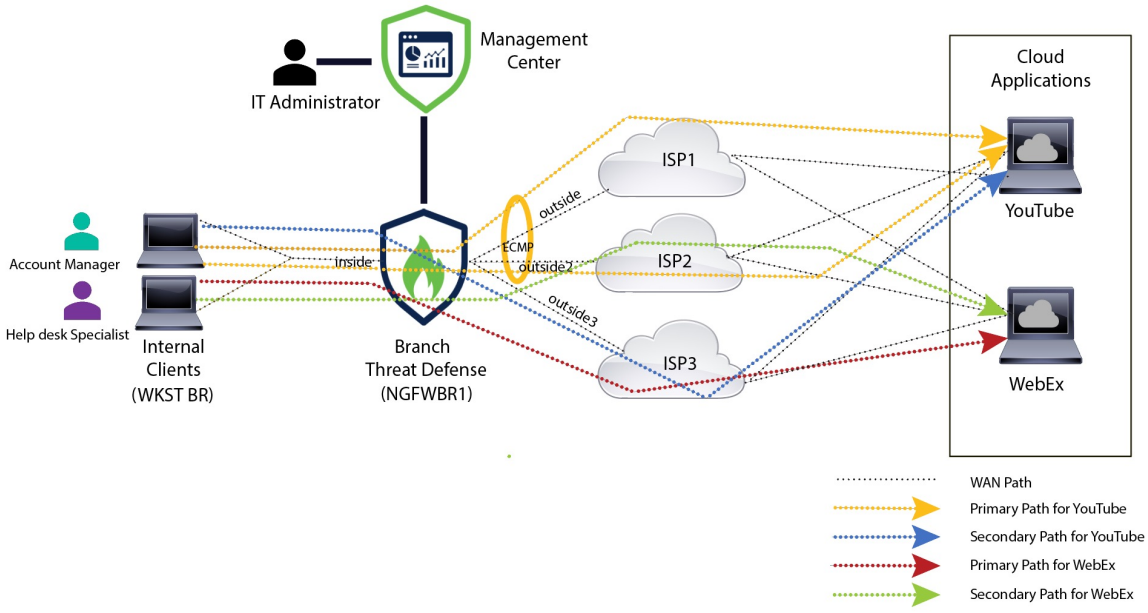
不带路径监控的网络拓扑-DIA

在这种拓扑结构中，威胁防御设备部署在具有三个出口接口的分支机构位置。使用 PBR 为设备配置 DIA。

在下图中，内部客户端或分支机构工作站被标记为 **WKST BR**，而分支机构威胁防御被标记为 **NGFWBR1**。**NGFWBR1** 的入口接口命名为 **inside**，出口接口分别命名为 **outside**、**outside2** 和 **outside3**。

通过配置 ECMP 区域和静态路由，可实现 **outside** 和 **outside2** 接口之间的负载均衡。

图 *2:* 直接互联网访问拓扑（无路径监控）

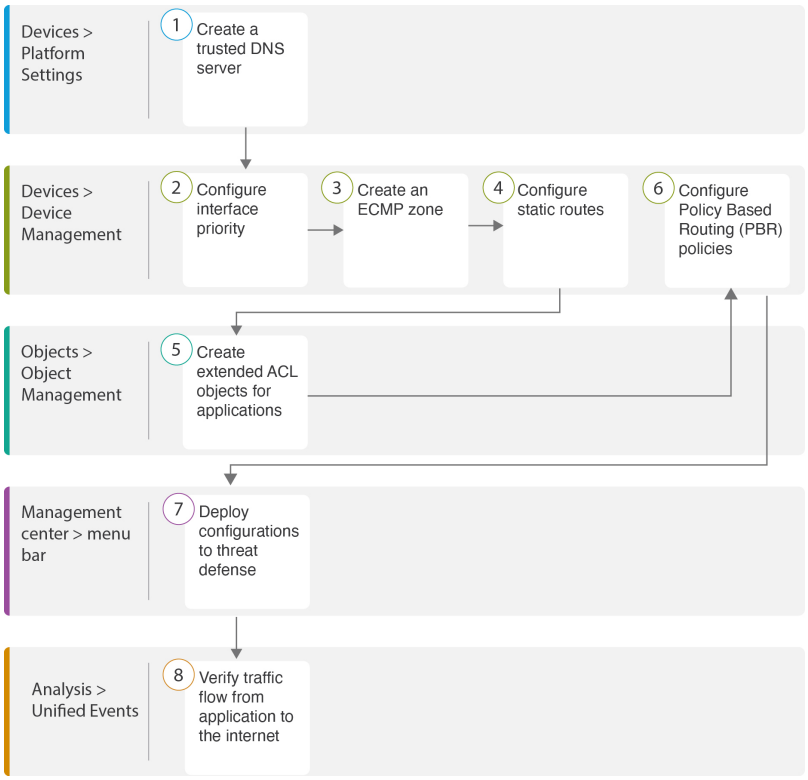


通过 DIA，分支机构防火墙后面的用户就可以访问：

1. 使用两个出口接口（**outside** 和 **outside2**）进行负载均衡的社交媒体应用流量（例如，**YouTube**）。如果两个接口均发生故障，则流量会回退到第三个出口接口 (**outside3**)。
2. 协作应用流量（例如，**WebEx**）通过 **outside3** 接口转发，如果该链路发生故障，流量将通过 **outside2** 接口转发。

配置不带路径监控的 DIA 的端到端程序

以下流程图说明了在 Cisco Secure Firewall Management Center 中配置不带路径监控的 DIA 的工作流程。



步骤	说明
1	（前提条件）配置受信任的 DNS 服务器。请参阅 配置受信任的 DNS 服务器，第 7 页。
2	（前提条件）配置接口优先级。请参阅 配置接口优先级， 第 8 页。
3	（前提条件）创建 ECMP 区域。请参阅 创建 ECMP 区域， 第 8 页。
4	（前提条件）配置静态路由。请参阅 配置等价静态路由， 第 8 页。
5	为应用配置扩展 ACL 对象。请参阅 • 为 YouTube 配置扩展 ACL 对象， 第 9 页 • 为 WebEx 配置扩展 ACL 对象， 第 10 页
6	为应用配置 PBR 策略。请参阅 • 为 YouTube 配置扩展 ACL 对象， 第 9 页 • 为 YouTube 配置策略型路由策略， 第 10 页
7	在威胁防御上部署配置。请参阅 部署配置， 第 12 页。

步骤	说明
8	验证 YouTube 和 WebEx 流量。请参阅验证应用流量，第 12 页。

配置受信任的 DNS 服务器

直接互联网接入功能中的应用检测依靠 DNS 监听将应用域映射到 IP，以便检测某个应用或一组应用。为确保 DNS 请求不会被恶意 DNS 服务器解析，并确实锁定到所需的 DNS 服务器，Cisco Secure Firewall Management Center 允许您为 Cisco Secure Firewall Threat Defense 配置受信任的 DNS 服务器。因此，防火墙只会监听流向受信任 DNS 服务器的流量。除了配置受信任的 DNS 服务器之外，您还可以将 DNS 服务器组，DHCP 池，DHCP 中继和 DHCP 客户端中已配置的服务器作为受信任的 DNS 服务器。

您可以使用受信任 DNS 服务器选项卡为 DNS 监听配置受信任 DNS 服务。

注释 对于基于应用的 PBR，必须配置受信任的 DNS 服务器。您还必须确保 DNS 流量以明文格式通过威胁防御（不支持加密 DNS），以便解析域以检测应用。

开始之前

- 确保已创建一个或多个 DNS 服务器组。有关详细信息，请参阅创建 DNS 服务器组对象。
- 确保您已创建用于连接到 DNS 服务器的接口对象。
- 确保受管设备具有适当的静态路由或动态路由来访问 DNS 服务器。

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后编辑威胁防御策略。

步骤 2 点击 **编辑**（ ） 图标。

步骤 3 点击 **DNS**。

步骤 4 要配置受信任的 DNS 服务器，请点击**受信任的 DNS 服务器 (Trusted DNS Servers)** 选项卡。

步骤 5 要从现有主机对象中选择 **DNS_Server**，请在**可用主机对象 (Available Host Objects)** 下使用搜索字段进行搜索，然后点击**添加 (Add)** 将其添加到**所选 DNS 服务器 (Selected DNS Servers)** 列表中。

注释 **DNS_Server** 是本例中配置的 DNS 服务器。

步骤 6 点击**保存 (Save)**。添加的DNS服务器显示在**受信任的 DNS 服务器 (Trusted DNS Servers)** 页面中。

步骤 7 点击**策略分配 (Policy Assignments)**，确保 **NGFWBR1** 已在**所选设备 (Selected Devices)** 列表中。

步骤 8 点击**确定 (OK)** 确认更改。

步骤 9 点击**保存 (Save)** 以写入平台设置的更改。

配置接口优先级

Cisco Secure Firewall Threat Defense 使用接口优先级来确定最佳互联网路径。优先级范围从 0 到 65535，决定了特定 ISP 向互联网发送流量时的优先级。流量将按接口的优先级进行转发。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，流量会被转发到具有下一个较低优先级的接口。例如，假设 outside2 和 outside3 的优先级分别被配置为 10 和 20。流量会被转发到 outside2。如果 outside2 变得不可用，则流量将被转发到 outside3。

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，然后编辑威胁防御设备 (**NGFWBR1**)。

步骤 2 点击 NGFWBR1 接口视图上的**路由 (Routing)** 选项卡。

步骤 3 点击**策略型路由 (Policy Based Routing)**。

步骤 4 点击**配置接口优先级 (Configure Interface Priority)**。

步骤 5 在对话框中，提供接口的优先级编号。

当所有接口的优先级值相同时，流量在接口之间均衡。

步骤 6 点击**保存 (Save)**。

创建 ECMP 区域

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，然后编辑威胁防御设备 (**NGFWBR1**)。

步骤 2 点击 NGFWBR1 接口视图上的**路由 (Routing)** 选项卡。

步骤 3 点击 **ECMP**。

步骤 4 点击**添加 (Add)**。

步骤 5 在**添加 ECMP (Add ECMP)** 框中，输入 ECMP 区域的名称 **ECMP-WAN**。

步骤 6 要关联接口，请在**可用接口 (Available Interfaces)**框下选择接口，然后点击**添加 (Add)**。

步骤 7 点击**确定 (OK)**。

ECMP 页面现在会显示新创建的 ECMP 区域。

步骤 8 点击**保存 (Save)**。

配置等价静态路由

您可以将虚拟路由器的接口（全局和用户定义）分配给设备的 ECMP 区域。

开始之前

- 要为接口配置等价静态路由，请确保将其与 ECMP 区域关联。请参阅创建 ECMP 区域，第 8 页。
- 如果没有将接口与 ECMP 区域关联，则无法为具有相同目标和指标的接口定义静态路由。

步骤 1 从**设备 (Devices)** > **设备管理 (Device Management)** 页面中并编辑威胁防御设备 (**NGFWBR1**)。

步骤 2 点击**路由 (Routing)**选项卡。

步骤 3 从下拉列表中，选择其接口与 ECMP 区域相关联的虚拟路由器。

步骤 4 要为接口配置等价静态路由，请点击**静态路由 (Static Route)**。

步骤 5 点击**添加路由 (Add Route)** 以添加新路由，或点击现有路由的 **编辑**（）。

步骤 6 从**接口 (Interface)** 下拉列表中，选择属于虚拟路由器的接口和 ECMP 区域。

步骤 7 从**可用网络 (Available Networks)** 框中选择目标网络，然后点击**添加 (Add)**。

步骤 8 输入网络的网关。

步骤 9 输入指标值。它可以是介于 1 和 254 之间的数字。

步骤 10 要保存设置，点击**保存 (Save)**。

步骤 11 要配置等价静态路由，请重复上述步骤，为同一 ECMP 区域中具有相同目的网络和指标值的另一个接口配置静态路由。请记住提供其他网关。

为 YouTube 配置扩展 ACL 对象

在策略型路由选择功能的帮助下，访问列表被配置为将 YouTube 流量从不同的出口接口引导至互联网。

步骤 1 依次选择**对象 (Objects)** > **对象管理 (Object Management)** 并从目录中选择**访问列表 (Access Lists)** > **扩展 (Extended)**。

步骤 2 点击**添加扩展访问列表 (Add Extended Access List)**，为社交媒体流量创建扩展访问列表。

步骤 3 在“扩展 ACL 对象”(Extended ACL Object) 对话框中，输入对象的名称 (**DIA_SocialMedia**)。

步骤 4 点击**添加 (Add)** 以创建新的扩展访问列表。

步骤 5 配置以下访问控制属性：

1. 选择**操作 (Action)** 以允许（匹配）流量标准。
2. 点击**应用 (Application)** 选项卡，然后在**可用应用 (Available Applications)** 列表中搜索 **YouTube**。
3. 选择 **YouTube**，然后点击**添加到规则 (Add to Rule)**。
4. 点击**添加 (Add)** 以将条目添加到对象。

5. 点击保存 (Save)。

为 WebEx 配置扩展 ACL 对象

在策略型路由选择功能的帮助下，访问列表被配置为将 WebEx 流量从不同的出口接口引导至互联网。

步骤 1 依次选择对象 (Objects) > 对象管理 (Object Management) 并从目录中选择访问列表 (Access Lists) > 扩展 (Extended)。

步骤 2 点击添加扩展访问列表 (Add Extended Access List)，为协作流量创建扩展访问列表。

步骤 3 在“扩展 ACL 对象”(Extended ACL Object) 对话框中，输入对象的名称 (**DIA_Collaboration**)。

步骤 4 点击添加 (Add) 以创建新的扩展访问列表。

步骤 5 配置以下访问控制属性：

1. 选择操作 (Action) 以允许（匹配）流量标准。
2. 点击应用 (Application) 选项卡，然后在可用应用 (Available Applications) 列表中搜索 **Webex**。
3. 选择 **Webex**，然后点击添加到规则 (Add to Rule)。
4. 点击添加 (Add) 以将条目添加到对象。
5. 点击保存 (Save)。

为 YouTube 配置策略型路由策略

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

YouTube 流量在 **outside** 和 **outside2** 之间进行负载均衡，如果两个链路都发生故障，则回退到 **outside3**。

步骤 1 选择设备 (Devices) > 设备管理 (Device Management)，然后编辑威胁防御设备 (**NGFWBR1**)。

步骤 2 点击 NGFWBR1 接口视图上的路由 (Routing) 选项卡。

步骤 3 点击策略型路由 (Policy Based Routing)。

“策略型路由”(Policy Based Routing) 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 (Add)。

步骤 5 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 (Inside)**。

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 (Add)**。

步骤 7 在 **添加转发操作** 对话框中，执行以下操作：

a) 从**匹配 ACL (Match ACL)** 下拉列表中选择 **DIA_SocialMedia**。

b) 要选择配置的接口，请从**发送至 (Send To)** 下拉列表中选择**出口接口 (Egress Interfaces)**。

c) 从**接口排序 (Interface Ordering)** 下拉列表选择**按优先级 (By Priority)**。

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 outside2 和 outside3 的优先级分别被配置为 10 和 20。流量会被转发到 outside2。如果 outside2 变得不可用，则流量将被转发到 outside3。

d) 在 **可用接口框** 中，列出所有接口及其优先级值。点击 **添加**（+） 图标以添加所选的出口接口。

对于我们的场景：

1. 在“可用接口”(Available Interfaces) 中，点击 **outside** 和 **outside2** 接口旁边的 **添加**（+） 图标，将其移至**所选出口接口**。
2. 然后，点击 **outside3** 接口旁边的 **添加**（+） 图标，将其移至**所选出口接口**。

e) 点击**保存 (Save)** 以写入匹配条件的更改。

f) 查看配置，然后点击**保存 (Save)** 以写入策略型路由的所有配置更改。

步骤 8 点击**保存 (Save)**。

为 WebEx 配置策略型路由策略

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

如果主链路发生故障，WebEx 应用流量将路由到 **outside3** 并回退到 **outside2**。

步骤 1 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，然后编辑威胁防御设备 (**NGFWBR1**)。

步骤 2 点击 NGFWBR1 接口视图上的**路由 (Routing)** 选项卡。

步骤 3 点击**策略型路由 (Policy Based Routing)**。

“策略型路由”(Policy Based Routing) 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 要编辑策略，请点击 **编辑**（✎） 图标。

步骤 5 要在策略中指定匹配条件和转发操作，请点击**添加 (Add)**。

步骤 6 在 **添加转发操作** 对话框中，执行以下操作：

a) 从**匹配 ACL (Match ACL)** 下拉列表中选择 **DIA_Collaboration**。

b) 要选择配置的接口，请从**发送至 (Send To)** 下拉列表中选择**出口接口 (Egress Interfaces)**。

c) 从**接口排序 (Interface Ordering)** 下拉列表中选择**顺序 (Order)**。

流量将按此处指定的接口顺序转发。

d) 在 **可用接口框** 中，列出所有接口及其优先级值。点击 **添加**（+） 图标以添加所选的出口接口。

对于我们的场景：

1. 在“可用接口”(Available Interfaces) 中，点击 **outside3** 接口旁边的 **添加**（+） 图标，将其移至**所选出口接口**。
2. 然后，点击 **outside2** 接口旁边的 **添加**（+） 图标，将其移至**所选出口接口**。

e) 点击**保存 (Save)** 以写入匹配条件的更改。

f) 查看配置，然后点击**保存 (Save)** 以写入策略型路由的所有配置更改。

步骤 7 点击**保存 (Save)**。

部署配置

在完成所有配置后，将其部署到托管设备。

步骤 1 在管理中心菜单栏中，点击**部署 (Deploy)**。

步骤 2 选中要部署配置更改的 NGFWBR1 旁边的复选框。

步骤 3 点击**部署 (Deploy)**。

步骤 4 如果系统在要部署的更改中发现错误或警告，则会在**验证错误 (Validation Errors)** 或**验证警告 (Validation Warnings)** 窗口中显示它们。要查看完整的详细信息，请点击“验证错误”(Validation Errors) 或“验证警告”(Validation Warnings) 链接。

有以下选项可供选择：

- 继续部署 - 继续部署而无需解决警告情况。如果系统识别错误，则无法继续。
- 关闭 - 退出而不部署。解决错误和警告情况，并尝试重新部署该配置。

验证应用流量

步骤 1 在管理中心界面中，选择**分析 (Analysis)** > **统一事件 (Unified Events)**。

步骤 2 使用列选择器通过选择**Web 应用 (Web Application)** 和**入口接口 (Egress Interface)** 来自定义列，然后点击**应用 (Apply)**。

步骤 3 对列重新排序，以方便验证。

步骤 4 在 **Web 应用 (Web Application)** 过滤器中，输入名称 **WebEx** 并点击**应用 (Apply)**。

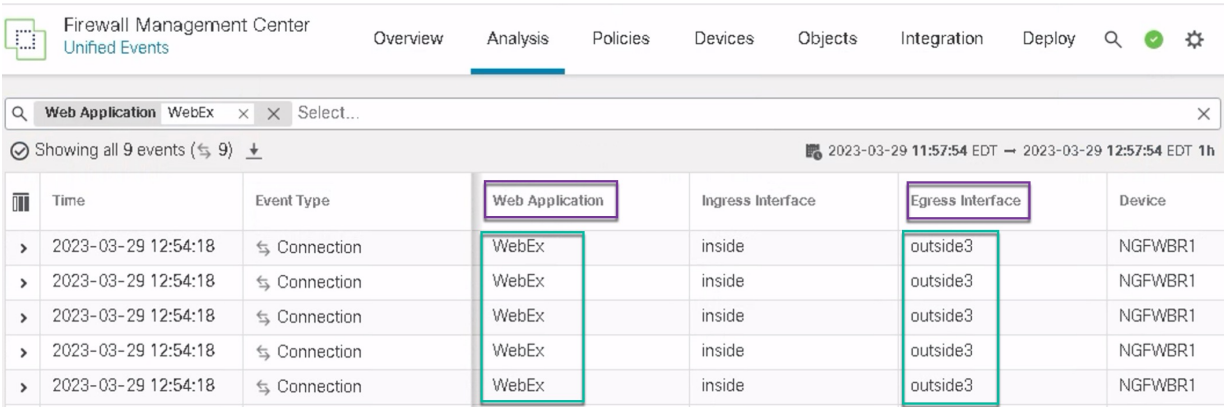
步骤 5 在 **Web 应用 (Web Application)** 过滤器中，输入名称 **YouTube** 并点击**应用 (Apply)**。

步骤 6 在 Cisco Secure Firewall 后面的主机上发起 **YouTube** 和 **WebEx** 应用的流量。在我们的场景中，启动 Google Chrome 浏览器并导航到 https://youtube.com 和分支机构工作站 **WKST BR1** 上不同选项卡中的 https://webex.com。

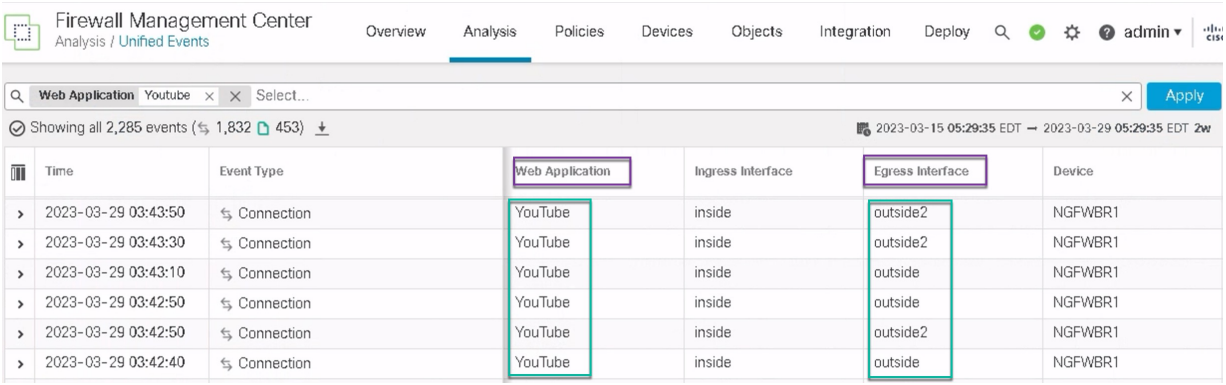
步骤 7 在管理中心中，验证两个应用的流量。

1. 对于不带路径监控的 DIA：

   - **WebEx** 应用流量按照下图所示的配置通过 **outside3** 接口发出。

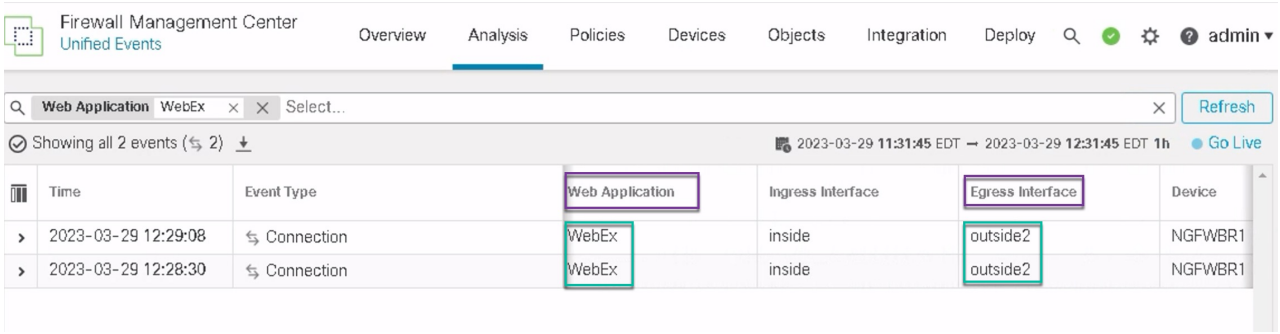


   - **YouTube** 应用流量按照下图所示的配置在 **outside** 和 **outside2** 接口之间进行负载均衡。



2. 对于带有路径监控的 DIA：

   WebEx 应用流量通过 **outside2** 接口发出，因为 **outside3** 接口上存在丢包，如下图所示。



策略型路由监控和故障排除

部署后，使用以下 CLI 监控和排除与 Cisco Secure Firewall Threat Defense 上策略型路由相关的问题。

如何...	CLI 命令
登录 Cisco Secure Firewall Threat Defense Lina CLI	**system support diagnostic-cli**
查看在部署期间从管理中心推送到威胁防御的预定义网络服务对象	• **show object network-service** • **show object network-service detail**
查看与配置的应用相关的特定网络服务对象 (NSG)	• **show object id YouTube** • **show object id WebEx**
验证推送到 Cisco Secure Firewall 的网络服务组 (NSG)	**show run object-group network-service**
查看与策略型路由关联的路由映射	**show run route-map**
验证接口配置详细信息，例如接口名称和接口优先级	**show run interface**
验证受信任的 DNS 服务器配置	**show dns**
确定流量所采用的路径	**debug policy-route** **重要事项** 运行调试命令时要谨慎，尤其是在生产环境中，因为它可能会根据流量产生冗长的输出。
停止调试路由	**undebug all**

要查看预定义的网络服务对象，请使用以下命令：

```
ngfwbr1# show object network-service
object network-service "ADrive" dynamic
 description Online file storage and backup.
 app-id 17
 domain adrive.com (bid=0) ip (hitcnt=0)
object network-service "Amazon" dynamic
 description Online retailer of books and most other goods.
 app-id 24
 domain amazon.com (bid=0) ip (hitcnt=0)
 domain amazon.jobs (bid=0) ip (hitcnt=0)
 domain amazon.in (bid=0) ip (hitcnt=0)
.
.
.
output snipped
.
.
.
object network-service "Logitech" dynamic
 description Company develops Computer peripherals and accessories.
 app-id 4671
 domain logitech.com (bid=0) ip (hitcnt=0)
object network-service "Lenovo" dynamic
 description Company manufactures/markets computers, software and related services.
 app-id 4672
 domain lenovo.com (bid=0) ip (hitcnt=0)
 domain lenovo.com.cn (bid=0) ip (hitcnt=0)
 domain lenovomm.com (bid=0) ip (hitcnt=0)
ngfwbr1#
```

要查看特定网络服务对象（例如 YouTube 和 WebEx），请使用以下命令：

```
ngfwbr1# show object id YouTube
object network-service "YouTube" dynamic
 description A video-sharing website on which users can upload, share, and view videos.
 app-id 929
 domain youtubei.googleapis.com (bid=592729) ip (hitcnt=0)
 domain yt3.ggpht.com (bid=709809) ip (hitcnt=102)
 domain youtube.com (bid=830871) ip (hitcnt=101)
 domain ytimg.com (bid=1035543) ip (hitcnt=93)
 domain googlevideo.com (bid=1148165) ip (hitcnt=466)
 domain youtu.be (bid=1247981) ip (hitcnt=0)
ngfwbr1# show object id WebEx
object network-service "WebEx" dynamic
 description Cisco's online meeting and web conferencing application.
 app-id 905
 domain files-prod-us-east-2.webexcontent.com (bid=182837) ip (hitcnt=0)
 domain webex.com (bid=290507) ip (hitcnt=30)
 domain avatar-prod-us-east-2.webexcontent.com (bid=452667) ip (hitcnt=0)
ngfwbr1#
```

要验证 NSG 是否已推送到威胁防御，请使用以下命令：

```
ngfwbr1# show run object-group network-service
object-group network-service FMC_NSG_292057776181
 network-service-member "WebEx"
object-group network-service FMC_NSG_292057776200
 network-service-member "YouTube"
ngfwbr1#
```

要验证与 PBR 关联的路由映射，请使用以下命令：

```
ngfwbr1# show run route-map
!
route-map FMC_GENERATED_PBR_1678091359817 permit 5
```

```
 match ip address DIA_Collaboration
 set interface outside3 outside2

!
route-map FMC_GENERATED_PBR_1678091359817 permit 10
 match ip address DIA_SocialMedia
 set adaptive-interface cost outside outside2 outside3
!
ngfwbr1#
```

要验证接口配置和接口优先级详细信息，请使用以下命令：

```
ngfwbr1# show run interface
!
interface GigabitEthernet0/0
 nameif outside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
  zone-member ECMP-WAN
 ip address 198.18.128.81 255.255.192.0
 policy-route cost 10
!
interface GigabitEthernet0/1
 nameif inside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 198.19.11.4 255.255.255.0
 policy-route route-map FMC_GENERATED_PBR_1678091359817
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 nameif outside2
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 zone-member ECMP-WAN
 ip address 198.19.40.4 255.255.255.0
 policy-route cost 10
!
interface GigabitEthernet0/4
 nameif outside3
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 198.19.30.4 255.255.255.0
 policy-route cost 20
!
interface Management0/0
 management-only
 nameif diagnostic
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
```

```
 security-level 0
 no ip address
ngfwbr1#
```

要验证受信任的 DNS 配置，请使用以下命令：

```
ngfwbr1# show dns

DNS Trusted Source enabled for DHCP Server Configured
DNS Trusted Source enabled for DHCP Client Learned
DNS Trusted Source enabled for DHCP Relay Learned
DNS Trusted Source enabled for DNS Server Configured
DNS Trusted Source not enabled for Trust-any
DNS Trusted Source: Type: IPs : Interface : Idle/Timeout (sec)
    DNS Server Configured: 198.19.10.100: <ifc-not-specified> : N/A
Trusted Source Configured: 198.19.10.100: <ifc-not-specified> : N/A
DNS snooping IP cache: 0 in use, 37 most used
Address                                 Idle(sec) Timeout(sec) Hit-count          Branch(es)
ngfwbr1#
```

要调试策略路由，请使用以下命令：

```
ngfwbr1# debug policy-route
debug policy-route  enabled at level 1
ngfwbr1# pbr: policy based route lookup called for 198.19.11.225/58119 to 198.19.10.100/53
 proto 17 sub_proto 0 received on interface inside, NSGs, nsg_id=none
pbr: no route policy found; skip to normal route lookup
.
output-snipped
.
pbr: policy based route lookup called for 198.19.11.225/61482 to 63.140.48.151/443 proto 6
 sub_proto 0 received on interface inside
                                                                , NSGs, nsg_id=1
pbr: First matching rule from ACL(2)
pbr: route map FMC_GENERATED_PBR_1678091359817, sequence 5, permit; proceed with policy
routing
pbr: evaluating interface outside3
pbr: policy based routing applied; egress_ifc = outside3 : next_hop = 198.19.30.63

ngfwbr1#
```

上面的调试示例适用于 WebEx 流量。请注意，在 PBR 将路由路径更改为 outside2 接口之前，流量将通过 outside3 接口进行路由。

要停止调试过程，请使用以下命令：

```
ngfwbr1# undebug all
```

其他资源

Resource	URL
Cisco Secure Firewall Threat Defense 版本说明	https://www.cisco.com/go/firewall-release-notes
所有新的和已弃用的功能	http://www.cisco.com/go/whatsnew-fmc
Cisco.com 上的 Secure Firewall 主页	http://www.cisco.com/go/firewall
Cisco.com 上的文档	http://www.cisco.com/go/firewall-docs

Resource	URL
YouTube 上的 Secure Firewall 频道	https://www.youtube.com/cisco-netsec
Secure Firewall 基本版	https://secure.cisco.com/secure-firewall

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。