Cisco Secure Firewall 中安全广域网的使用案例

首次发布日期: 2023 年 4 月 4 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

目录

Full Cisco Trademarks with Software License ?

第 1 章

使用入门 1

关于本出版物 1

Cisco Secure Firewall 1

简化的分支机构概述 2

功能 3

第 2 章

使用动态虚拟隧道接口 (DVTI) 简化分支机构与中心的通信 5

中心辐射型拓扑中基于路由的 VPN 6

优势 6

此使用案例适合您吗？ 6

场景 7

网络拓扑 7

最佳实践 8

前提条件 8

配置基于路由的 VPN 的端到端程序（中心辐射型拓扑） 9

创建基于路由的站点间 VPN 10

配置中心节点的终端 11

配置分支节点的终端 12

在中心节点上配置 OSPF 14

在分支节点上配置 OSPF 16

配置访问控制策略。 18

部署配置 21

验证流经 VPN 隧道的流量 21
在分支节点上配置备份 VTI 接口 24
为主 VTI 接口和辅助 VTI 接口配置 ECMP 区域 26
验证主隧道和辅助隧道 27
基于路由的 VPN 隧道故障排除 30
其他资源 31

第 3 章 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 33
直接互联网接入 33
优势 35
此使用案例适合您吗？ 35
用于直接互联网接入的组件 35
最佳实践 35
前提条件 36
场景 1：不带路径监控的直接互联网访问 36
不带路径监控的网络拓扑-DIA 37
配置不带路径监控的 DIA 的端到端程序 37
配置受信任的 DNS 服务器 39
配置接口优先级 40
创建 ECMP 区域 40
配置等价静态路由 40
为 YouTube 配置扩展 ACL 对象 41
为 WebEx 配置扩展 ACL 对象 42
为 YouTube 配置策略型路由策略 42
为 WebEx 配置策略型路由策略 43
部署配置 44
验证应用流量 44
策略型路由监控和故障排除 46
其他资源 49

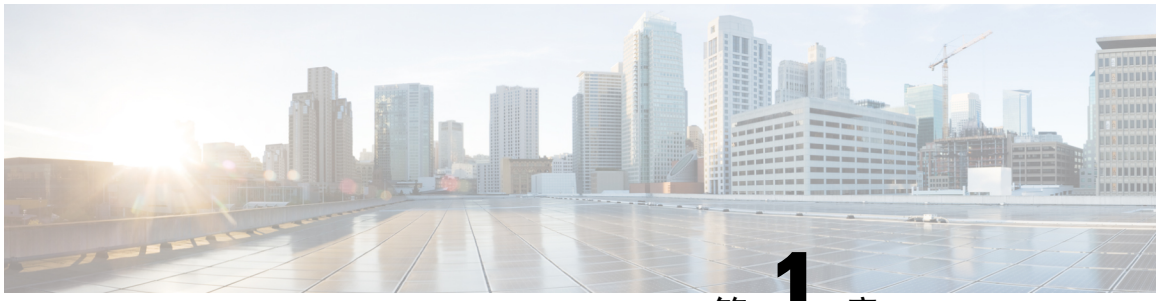
第 4 章 使用带路径监控的直接互联网接入 (DIA) 将应用流量从分支机构路由到互联网 51

直接互联网接入 51
优势 53
此使用案例适合您吗？ 53
用于直接互联网接入的组件 53
最佳实践 53
前提条件 54
场景 2：具有路径监控的直接互联网接入 54
具有路径监控的网络拓扑-DIA 55
使用路径监控来配置 DIA 的端到端步骤 55
配置受信任的 DNS 服务器 57
配置接口优先级 58
配置路径监控设置 58
为 WebEx 配置扩展 ACL 对象 59
为 Webex 配置带路径监控的策略型路由策略 59
部署配置 60
验证应用流量 60
策略型路由监控和故障排除 62
其他资源 65

第 5 章 使用 Umbrella 自动隧道保护互联网流量 67
Cisco Umbrella 自动隧道 67
优势 68
此使用案例适合您吗？ 69
场景 69
网络拓扑 69
SASE Umbrella 隧道的最佳实践 70
配置 Umbrella SASE 隧道的前提条件 70
SASE Umbrella 隧道的最佳实践 71
配置 Umbrella SASE 隧道的前提条件 71
配置 Umbrella 自动隧道的端到端程序 72
为 Umbrella 配置 SASE 隧道 73

配置静态路由 76
为 DNS 和 Web 流量配置扩展 ACL 77
为 DNS 和 Web 流量配置 PBR 策略 78
部署配置 79
验证 SASE Umbrella 隧道部署 79
Umbrella 自动隧道故障排除 84
其他资源 85

第 6 章 为远程员工提供安全连接：使用中的 DIA、Umbrella 自动隧道和 DVTI 87
通过 DIA、Umbrella SASE 自动隧道和 DVTI 增强远程员工的连接性和安全性 87
此使用案例适合您吗？ 87
场景 88
拓扑 88
配置 DIA、Umbrella 自动隧道和 DVTI 的端到端程序 89
其他资源 89



第 1 章

使用入门

本章简要介绍了 Cisco Secure Firewall 的功能以及支持的分支机构和 WAN 功能。

- 关于本出版物，第 1 页
- Cisco Secure Firewall，第 1 页
- 简化的分支机构概述，第 2 页
- 功能，第 3 页

关于本出版物

本指南详细介绍了使用 Cisco Secure Firewall 支持的分支机构和 WAN 功能的主要使用案例。

这些方法并不能满足所有可能的网络需求；相反，它们提供了一些模型，您可以在此基础上构建自己的网络。您可以选择不使用示例中的功能，也可以添加或替换更适合自己需要的功能。

本指南假定您熟悉 Cisco Secure Firewall。有关配置的详细信息，请参阅《Cisco Secure Firewall Management Center 管理指南，7.3》和《Cisco Secure Firewall Management Center 设备配置指南，7.3》。

Cisco Secure Firewall

Cisco Secure Firewall 是一种非常强大的防火墙解决方案，具有 Snort IPS、URL 过滤和恶意软件防御等先进功能。

这一全面的产品通过在物理、私有和公共云环境中执行一致的安全策略，大大简化了威胁防护。

此外，它还能对网络基础设施提供广泛的可见性，从而迅速识别潜在威胁的来源和活动。掌握这些知识后，您就可以及时采取行动，在攻击有机会破坏您的运营之前阻止它们。

除了传统的防火墙功能外，它还提供以下功能：

1. 应用可视性与可控性
2. 用户身份感知和控制
3. 入侵预防和入侵检测

4. SSL/TLS 解密
5. 基于信誉的阻止
6. 文件和恶意软件防护
7. 虚拟专用网络 (VPN)

为了进一步确保网络部署的安全，Cisco Secure Firewall 在后期版本中提供了更多安全功能，例如：

- 加密可视性引擎 (EVE)，可增强加密流量检查，而无需实施完整的中间人 (MITM) 解密。
- 象流检测，用于检测和补救象流（通常大于 1 GB/10 秒的流），避免 CPU 占用率过高和丢包。
- 思科安全动态属性连接器 (CSDAC)，通过利用标记和标签进行策略配置，而不是传统的基于 IP/网络的策略配置，为您的安全策略管理带来灵活性和智能。

简化的分支机构概述

随着组织在多个分支机构扩展其运营，确保安全和简化的连接变得至关重要。部署安全的分支机构网络基础设施涉及复杂的配置和管理流程，如果处理不当，不仅耗时，还容易出现安全漏洞。但是，组织可以通过利用 Cisco Secure Firewall 解决方案来简化分支机构的安全部署，从而克服这些挑战。

在本指南中，我们将探讨使用强大的防火墙解决方案简化安全分支机构部署的概念。通过集成 Cisco Secure Firewall 作为分支网络架构的基础组件，企业可以建立强大的安全基线，同时简化部署流程。这种方法使企业能够执行统一的安全策略，优化流量路由，并确保弹性连接。

Cisco Secure Firewall 支持的一些简化的分支机构和 WAN 功能包括：

- **安全弹性连接：**
  - 总部（中心）和分支机构（分支）之间的基于路由 (VTI) 的 VPN 隧道
  - IPv4 和 IPv6 BGP、IPv4 和 IPv6 OSPFv2/v3 以及 IPv4 EIGRP over VTI
  - 对具有静态或动态 IP 的分支的 DVTI 支持
- **高可用性，网络停机时间接近于零：**
  - 双 ISP 配置
  - 基于应用的接口监控优化路径选择
- **增加可用带宽：**
  - ECMP 支持在多个 ISP 之间实现负载均衡
  - SVTI 的 ECMP 支持
  - 使用 PBR 的基于应用的负载均衡
- **公共云和访客用户的直接互联网接入：**

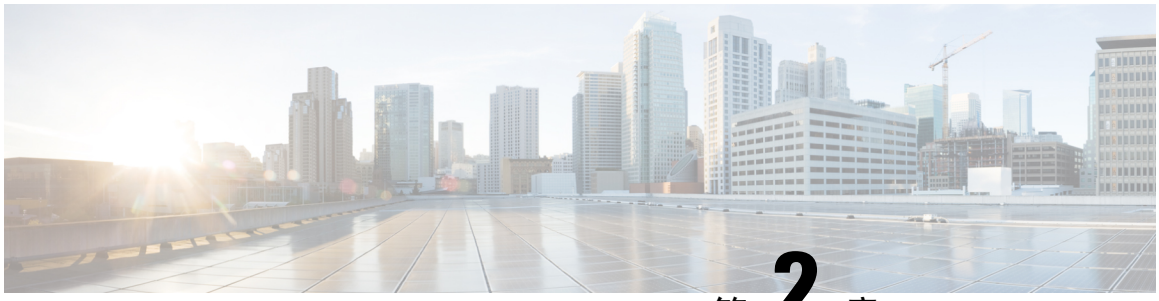
- 使用应用作为匹配条件的策略型路由
- 为 Umbrella 提供本地隧道 ID 支持

- **简化管理：**
  - SASE：Umbrella 自动隧道部署
  - DVTI 中心辐射型拓扑简化

功能

此表列出了一些常用的 WAN 功能

特性	已引入...
VTI 的环回接口支持	版本 7.3
对站点间 VPN 的动态 VTI (DVTI) 支持	版本 7.3
Umbrella 自动隧道	版本 7.3
VTI 支持 IPv4 和 IPv6 BGP、IPv4 和 IPv6 OSPFv2/v3 以及 IPv4 EIGRP	版本 7.3
具有中心辐射型拓扑的基于路由的站点间 VPN	版本 7.2
具有路径监控的策略型路由	版本 7.2
站点间 VPN 监控控制面板	版本 7.1
直接互联网接入/策略型路由	版本 7.1
带 WAN 接口的等价多路径 (ECMP) 区域	版本 7.1
带 VTI 接口的等价多路径 (ECMP) 区域	版本 7.1
备份基于路由的站点间 VPN 的 VTI	版本 7.0
通过站点间 VPN 支持静态 VTI (SVTI)	版本 6.7



第 2 章

使用动态虚拟隧道接口 (DVTI) 简化分支机构与中心的通信

在本章中，我们将深入探讨 DVTI 在中心辐射型拓扑中的实际应用。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。

- 中心辐射型拓扑中基于路由的 VPN，第 6 页
- 优势，第 6 页
- 此使用案例适合您吗？，第 6 页
- 场景，第 7 页
- 网络拓扑，第 7 页
- 最佳实践，第 8 页
- 前提条件，第 8 页
- 配置基于路由的 VPN 的端到端程序（中心辐射型拓扑），第 9 页
- 创建基于路由的站点间 VPN，第 10 页
- 配置中心节点的终端，第 11 页
- 配置分支节点的终端，第 12 页
- 在中心节点上配置 OSPF，第 14 页
- 在分支节点上配置 OSPF，第 16 页
- 配置访问控制策略。，第 18 页
- 部署配置，第 21 页
- 验证流经 VPN 隧道的流量，第 21 页
- 在分支节点上配置备份 VTI 接口，第 24 页
- 为主 VTI 接口和辅助 VTI 接口配置 ECMP 区域，第 26 页
- 验证主隧道和辅助隧道，第 27 页
- 基于路由的 VPN 隧道故障排除，第 30 页
- 其他资源，第 31 页

中心辐射型拓扑中基于路由的 VPN

Cisco Secure Firewall Management Center 支持被称为虚拟隧道接口 (VTI) 的可路由逻辑接口。您可以使用这些接口来应用静态和动态路由策略。在使用 VTI 时，您不必配置静态加密映射访问列表并将其映射到接口。您不再需要跟踪所有远程子网并将其包含在加密映射访问列表中。

您可以在 VTI 的对等体之间创建 VPN 隧道。VTI 可通过将 IPSec 配置文件连接到每个隧道的端部，为基于 VPN 的路由提供支持。VTI 会使用静态或动态路由。威胁防御设备加密或解密来自或到达隧道接口的流量，并根据路由表将其转发。

管理中心支持使用默认设置的站点到站点 VPN 向导来配置 VTI 或基于路由的 VPN。

在中心辐射型拓扑中实施基于路由的 VPN 时，将在中心上配置动态虚拟隧道接口 (DVTI)，在分支上配置静态虚拟隧道接口 (SVTI)。

动态 VTI 会使用虚拟模板来进行 IPsec 接口的动态实例化和管理。虚拟模板会为每个 VPN 会话动态生成独一无二的虚拟访问接口。动态 VTI 支持多个 IPsec 安全关联，并接受分支提议的多个 IPsec 选择器。

Cisco Secure Firewall Threat Defense 支持为基于路由的 (VTI) VPN 配置备份隧道，从而提供链路冗余。当主 VTI（主要隧道）无法路由流量时，VPN 中的流量会通过备用 VTI（辅助隧道）传送。

优势

在中心辐射型拓扑中使用基于 VTI 的 VPN 的优势包括：

1. **简化配置**：VTI 通过提供代表隧道本身的逻辑接口，简化了 VPN 隧道的配置。这样就不需要通常与传统 VPN 设置相关的复杂加密映射或访问列表配置。
2. **简化管理**：它能简化管理大型企业中心辐射型部署的对等体配置。对于在分支上配置的多个静态 VTI，仅在中心上配置一个动态 VTI。
3. **可扩展性**：VTI 可轻松实现可扩展性。添加新的分支不需要在集线器上进行任何其他 VPN 配置。您可能需要根据设置更新 NAT 和路由配置。
4. **动态路由支持**：VTI 支持动态路由协议，例如开放最短路径优先 (OSPF)，从而允许在 VPN 终端之间动态交换路由信息。这样就可以根据实时网络条件做出有效的路由决策。
5. **双 ISP 冗余**：SVTI 支持备份 VTI 隧道。
6. **负载均衡**：SVTI 支持使用 ECMP 对 VPN 流量进行负载均衡。

此使用案例适合您吗？

DVTI 中心辐射型配置的目标受众包括网络架构师、IT 管理员以及负责设计和管理企业网络基础设施的网络专业人员。对于那些希望通过实施集中式中心和连接远程分支站点的安全隧道来优化网络连接、确保数据安全和简化网络管理的人员而言，这种使用案例非常有价值。

场景

一家中型公司在不同城市设有多个分支机构，他们希望建立一个安全高效的网络基础设施，以便将这些分支机构与中央总部连接起来。公司的 IT 管理员 Alice 负责配置和管理网络。

有什么风险？

目前的网络配置需要在每个分支机构和中央总部之间手动配置多个点对点连接。这种方法费时费力，容易出错，而且很难保持所有地点网络设置的一致性。Alice 需要一个能简化配置过程并提供集中控制的解决方案。

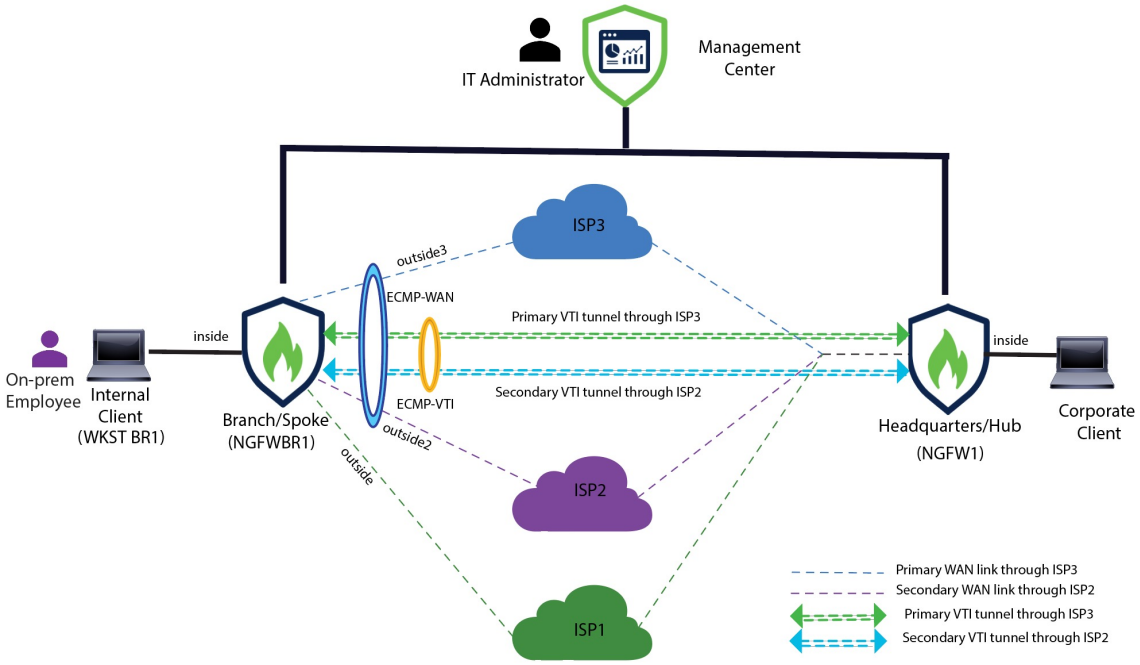
分支机构（分支）和总部（中心）之间基于路由的 VPN 如何解决问题？

1. 集中配置：Alice 实施 DVTI 中心辐射型拓扑，从而在中心进行集中配置和管理。这样就简化了所有地点的网络设置。
2. 动态路由：Alice 设置动态路由协议（如 OSPF），以便自动交换路由信息。无需手动配置静态路由，从而简化了网络管理。
3. 快速调配： 借助 DVTI，Alice 只需配置一个辐条路由器并与中心建立安全隧道，即可快速部署新的分支机构。这简化了调配过程，并支持网络可扩展性。

通过实施 DVTI，Alice 简化了网络配置，实现了集中控制，确保了一致性，并实现了企业网络的高效配置和可扩展性。

网络拓扑

在这种中心辐射型拓扑结构中，威胁防御设备部署在分支机构。在下图中，内部客户端或分支工机构作站被标为 WKST BR，分支机构（分支）威胁防御被标为 NGFWBR1。总部（中心）标记为 NGFW1，并连接到企业网络。在 NGFWBR1 和 NGFW1 之间配置了一个 VPN 通道。在分支节点的主要和辅助静态 VTI 接口上配置 ECMP 区域，以实现 VPN 流量的链路冗余和负载平衡。



最佳实践

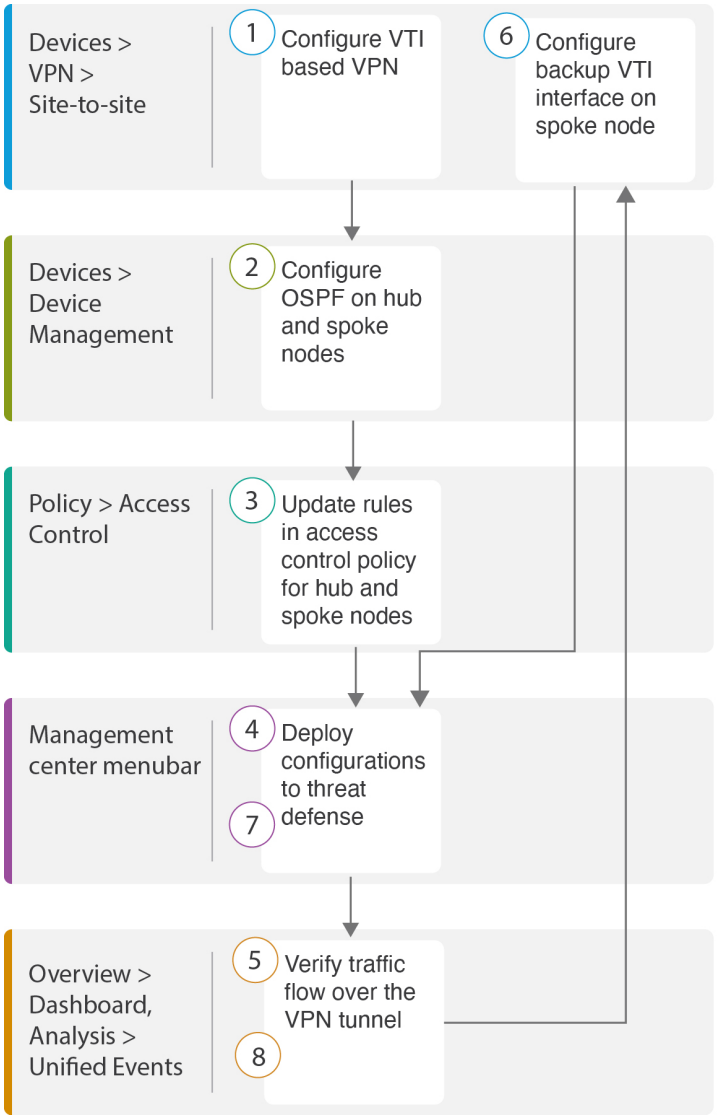
- 确保运行的是 Cisco Secure Firewall Threat Defense 版本 6.7 及更高版本。
- 仅在路由模式中支持 VTI。
- 从环回接口为动态接口配置借用 IP。
- 确保在 VTI 接口上应用访问规则，以控制通过 VTI 的流量。
- 为 SVTI 配置 ECMP 区域，以均衡 VTI 流量负载。

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

配置基于路由的 VPN 的端到端程序（中心辐射型拓扑）

以下流程图说明在 Cisco Secure Firewall Management Center 为中心辐射型拓扑配置基于路由的 VPN 的工作流程。



步骤	说明
1	配置基于 VTI 的 VPN。请参阅 • 创建基于路由的站点间 VPN， 第 10 页 • 配置中心节点的终端， 第 11 页 • 配置分支节点的终端， 第 12 页

步骤	说明
2	在中心和分支节点上配置 OSPF。请参阅 • 在中心节点上配置 OSPF，第 14 页 • 在分支节点上配置 OSPF，第 16 页
3	更新中心和分支节点的访问控制策略中的规则。Updates rules in the access control policy for hub and spoke nodes. 请参阅 配置访问控制策略。，第 18 页。
4	将配置部署到威胁防御。Deploy configuration to threat defense. 请参阅 部署配置，第 21 页。
5	验证通过 VPN 隧道的流量。请参阅 验证流经 VPN 隧道的流量，第 21 页。
6	在分支节点上配置备份 VTI。请参阅 在分支节点上配置备份 VTI 接口，第 24 页。
7	在威胁防御上部署配置。请参阅部署配置，第 21 页。
8	验证通过辅助隧道的流量。请参阅验证主隧道和辅助隧道，第 27 页。

创建基于路由的站点间 VPN

您可以在两个节点之间配置基于路由的站点间 VPN。要配置基于 VTI 的 VPN，隧道的两个节点都需要使用虚拟隧道接口。

对于托管分支，您可以配置备份静态 VTI 接口以及主 VTI 接口。

步骤 1 选择**设备 (Devices)** > **VPN** > **站点间 (Site To Site)**。

步骤 2 在**拓扑名称 (Topology Name)** 字段中输入名称 **Corporate-VPN**。

步骤 3 选择**基于路由 (VTI) (Route Based [VTI])** 作为拓扑类型。

步骤 4 配置中心节点的终端。请参阅 配置中心节点的终端，第 11 页。

步骤 5 配置分支节点的终端。请参阅 配置分支节点的终端，第 12 页。

步骤 6 默认设置会别用于 **IKE**、**IPsec** 和**高级 (Advanced)** 选项卡。

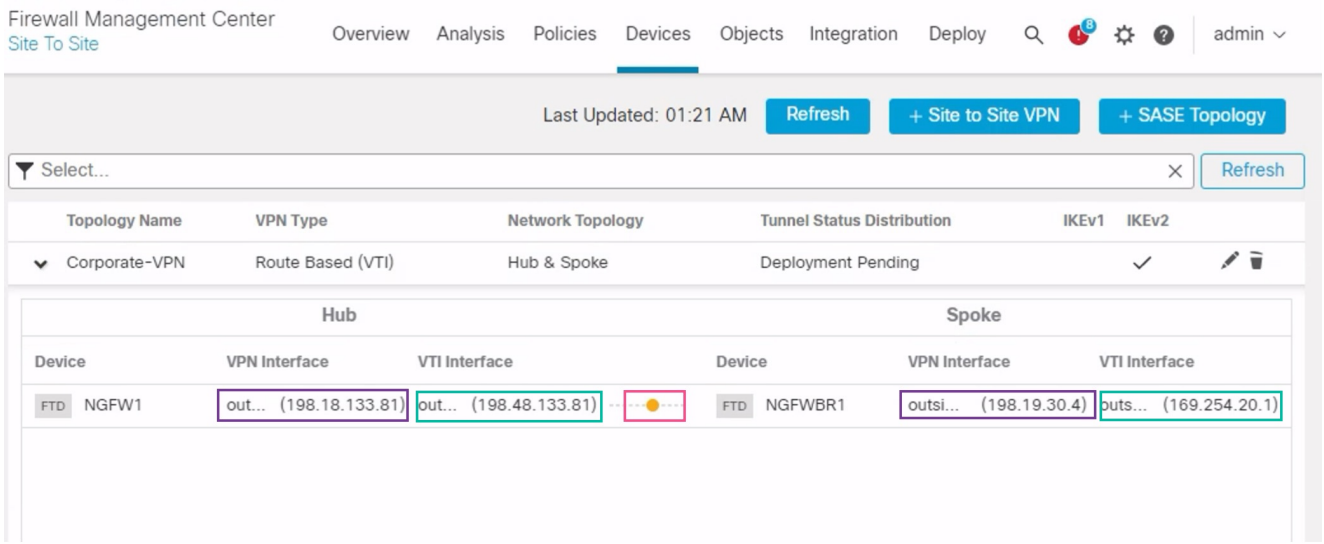
步骤 7 点击**保存 (Save)**。

企业 VPN 拓扑已成功创建。

步骤 8 您可以通过导航至**设备 (Devices)** > **站点间 VPN (Site-to-site VPN)**，在站点间 VPN 列表页面中查看 VPN 拓扑。

注释　　如果没有看到您创建的 VPN 拓扑，请点击**刷新 (Refresh)**。

步骤 9 展开 **Corporate-VPN** 节点以查看拓扑中的所有隧道。它会显示 **NGFW1** 中心和 **NGFWBR1** 分支，以及物理源和 VTI 接口的详细信息。由于配置尚未部署，它会显示**部署待处理 (Deployment Pending)**，并且隧道显示为琥珀色状态。



下一步做什么

在两台设备上配置 VTI 接口和 VTI 隧道后，您必须配置：

- 用于通过 VTI 隧道在设备之间路由 VTI 流量的路由协议。请参阅在中心节点上配置 OSPF，第 14 页和在分支节点上配置 OSPF，第 16 页。
- 用于允许已加密的流量的访问控制规则。请参阅配置访问控制策略。，第 18 页。

配置中心节点的终端

将隧道类型指定为动态并配置相关参数时，管理中心会生成动态虚拟模板。虚拟模板会为每个 VPN 会话动态生成独一无二的虚拟访问接口。

步骤 1 在**中心节点 (Hub Nodes)** 部分中，点击 +。系统将显示**添加终端 (Add Endpoint)** 对话框。

步骤 2 从**设备 (Device)** 下拉列表中选择 **NGFW1** 作为中心。

注释 设备必须使用 7.3 或更高版本的软件。

步骤 3 点击**动态虚拟隧道接口 (Dynamic Virtual Tunnel Interface)** 下拉列表旁边的 + 以添加新的动态 VTI。

系统将显示 **添加虚拟隧道接口** 对话框，其中包含预填充的默认配置。

- **隧道类型 (Tunnel Type)** 会被自动填充为**动态 (Dynamic)**。

- **名称 (Name)** 会自动填充为 *<tunnel_source interface logical name>*+ dynamic_vti +*<tunnel ID>*。例如，**outside_dynamic_vti_1**。
- 默认情况下，**启用 (Enabled)** 复选框处于选中状态。
- **安全区域 (Security Zone)** - 要为此接口定义安全区域，请从下拉列表中选择**新建... (New…)**。在**新安全区域 (New Security Zone)** 对话框中，输入 **Tunnel_Zone** 作为名称并点击**确定 (OK)**。为该隧道接口选择 **Tunnel_Zone** 作为安全区域。
- **模板 ID (Template ID)** 会自动填充 DVTI 接口的唯一 ID。
- **隧道源 (Tunnel Source)** 是作为 DVTI 源的物理接口，默认情况下会被自动填充。在此使用案例中，我们不想为 DVTI 设置明确的隧道源。通过从下拉列表中选择**选择接口 (Select Interface)** 来清除选择。
- 默认情况下，**IPsec 隧道模式 (IPsec Tunnel Mode)** 会被设置为 IPv4。
- **IP 地址 (IP address)** 不能是静态 IP 地址，因为 DVTI 是模板接口。我们建议您从环回接口为动态接口配置借用 IP。要添加环回接口，请点击**借用 IP（未编号 IP）(Borrow IP [IP unnumbered])** 下拉列表旁边的 **+**。在**添加回环接口 (Add Loopback Interface)** 对话框中：

  1. 在**常规 (General)** 选项卡中，在**名称 (Name)** 中输入 **HUB_Tunnel_IP**，并在**环回 ID (Loopback ID)** 中输入 **1**。
  2. 在 **IPv4** 选项卡中，输入 IP 地址 **198.48.133.81/32**。
  3. 点击**确定 (OK)** 以保存环回接口。

  借用 IP 设置为 **环回 1(HUB_Tunnel_IP) (Loopback 1[HUB_Tunnel_IP])**。

点击**确定 (OK)** 以保存 DVTI。系统将显示一条消息，确认 VTI 已成功创建。点击**确定 (OK)**。

动态虚拟隧道接口被设置为 **outside_dynamic_vti_1(198.48.133.81)**。

步骤 4 从**隧道源 (Tunnel Source)** 下拉列表中选择 **GigabitEthernet 0/0 (outside)**。外部接口的 IP 地址 (**198.18.133.81**) 将自动填充到下一个字段中。

步骤 5 展开**高级设置 (Advanced Settings)** 以查看默认设置。

步骤 6 点击**确定 (OK)**。

NGFW1 已被成功配置为中心节点。

配置分支节点的终端

步骤 1 在**分支节点 (Spoke Nodes)** 部分中，点击 **+**。系统将显示**添加终端 (Add Endpoint)** 对话框。

步骤 2 从**设备 (Device)** 下拉列表中选择 **NGFWBR1** 作为中心。

注释 设备必须使用 7.3 或更高版本的软件。

步骤 3 点击**静态虚拟隧道接口 (Static Virtual Tunnel Interface)** 下拉列表旁边的 **+** 以添加新的静态 VTI。

系统将显示 **添加虚拟隧道接口** 对话框，其中包含预填充的默认配置。

- **隧道类型 (Tunnel Type)** 会被自动填充为**静态 (Static)**。
- **名称 (Name)** 会自动填充为 *<tunnel_source interface logical name>*+ static_vti +*<tunnel ID>*。例如，**outside_static_vti_1**。
- 默认情况下，**启用 (Enabled)** 复选框处于选中状态。
- 从“安全区域”(Security Zone) 下拉列表中选择 **Tunnel_Zone**。
- **隧道 ID (Tunnel ID)** 会自动填充值 1。
- 从**隧道源 (Tunnel Source)** 下拉列表中选择 **GigabitEthernet0/4 (outside3)**。从 outside 3 接口旁边的下拉列表中选择 **198.19.30.4** 作为其 IP 地址。
- 默认情况下，**IPsec 隧道模式 (IPsec Tunnel Mode)** 会被设置为 IPv4。
- **IP 地址 (IP address)** 可以是静态 IP 地址或借用 IP 地址。我们建议您从环回接口为静态接口配置借用 IP。要添加环回接口，请点击**借用 IP（未编号 IP）(Borrow IP [IP unnumbered])** 下拉列表旁边的 **+**。在**添加回环接口 (Add Loopback Interface)** 对话框中：
  1. 在**常规 (General)** 选项卡中，在**名称 (Name)** 中输入 **Spoke_Tunnel_IP**，并在**环回 ID (Loopback ID)** 中输入 **1**。
  2. 在 **IPv4** 选项卡中，输入 IP 地址 **169.254.20.1/32**。
  3. 点击**确定 (OK)** 以保存环回接口。

  借用 IP 设置为 **环回 1(Spoke_Tunnel_IP) (Loopback 1[Spoke_Tunnel_IP])**。

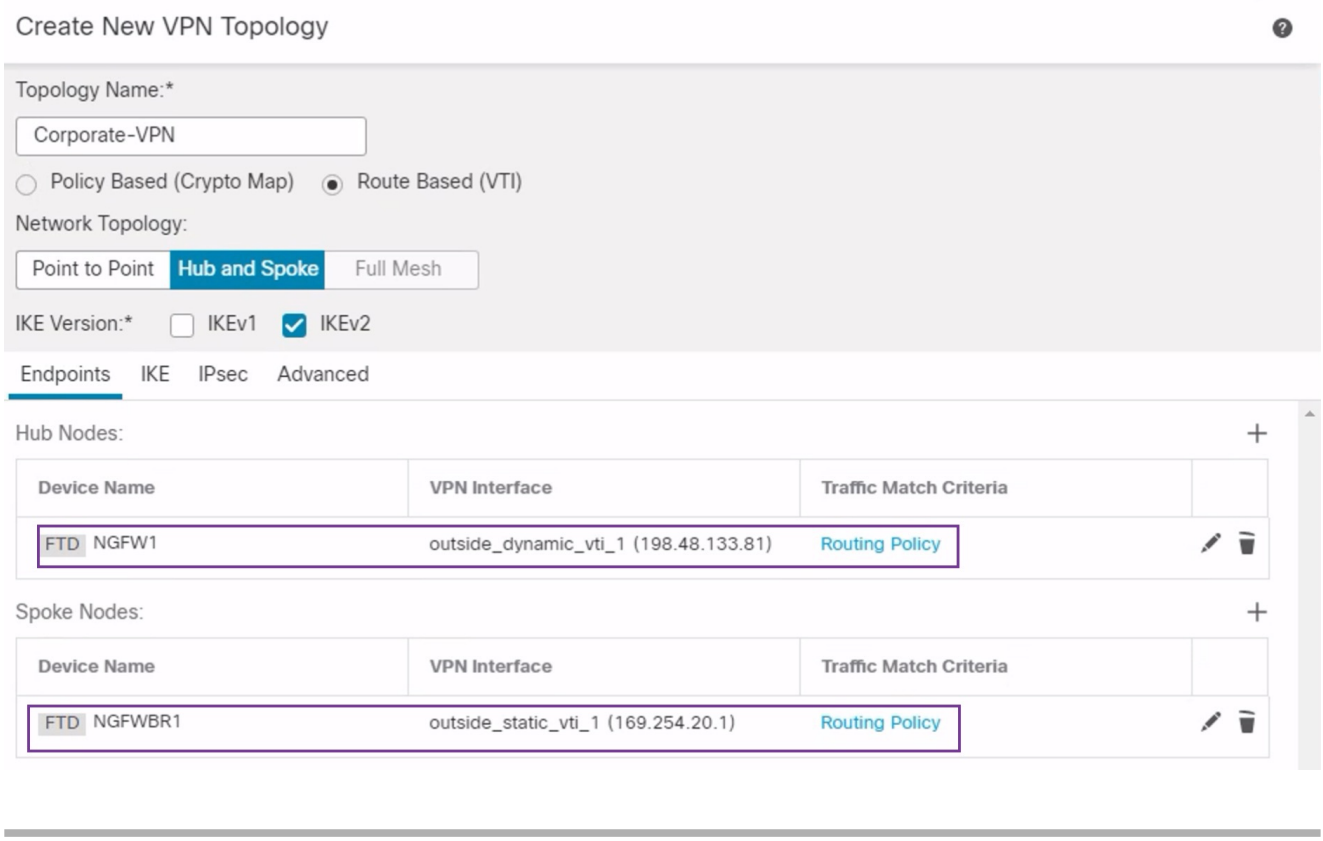
点击**确定 (OK)** 以保存 SVTI。系统将显示一条消息，确认 VTI 已成功创建。点击**确定 (OK)**。

静态虚拟隧道接口设置为 **outside_static_vti_1(169.254.20.1)**。

步骤 4 展开**高级设置 (Advanced Settings)** 以查看默认设置。必须选中两个复选框。

步骤 5 点击**确定 (OK)**。

NGFWBR1 已被成功配置为分支节点。



在中心节点上配置 OSPF

在中心和分支设备之间配置OSPF，以便通过VPN隧道发送流量。作为参考，静态路由是底层网络，在其上建立分支到中心的隧道，并将 OSPF 视为上层网络。

步骤 1 要编辑中心节点，请选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击 NGFW1 节点的 **编辑**（✎）图标。

步骤 2 在**接口 (Interfaces)** 选项卡中，验证之前创建的用作 DVTI 接口 IP 地址的 **Loopback1** 接口。

步骤 3 点击**路由 (Routing)**。

步骤 4 点击左侧面板中的 **OSPF**。

步骤 5 选中**进程 1 (Process 1)** 复选框以启用 OSPF 实例。

步骤 6 点击**接口 (Interface)** 选项卡。

步骤 7 点击 **+添加 (+Add)**。系统将显示 **Add Interface** 对话框。修改以下字段：

- **接口 (Interface)** - 从下拉列表中选择 DVTI 接口 **outside_dynamic_vti_1**。
- **点对点 (Point-to-point)** - 选中复选框以通过 VPN 隧道传输 OSPF 路由。

其余字段使用默认值。

- 点击**确定 (OK)**。

在**接口 (Interface)** 选项卡中为 **outside_dynamic_vti_1** 添加一行。

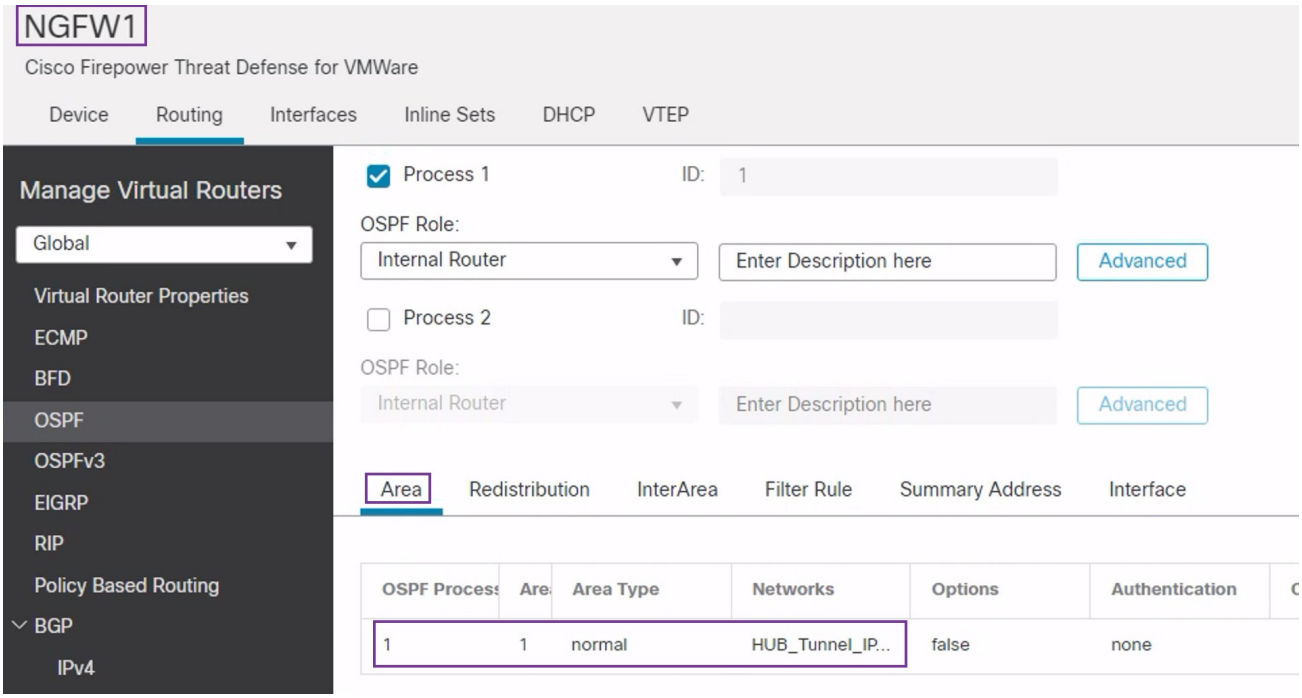
步骤 8 点击**区域 (Area)** 选项卡。

步骤 9 点击 **+添加 (+Add)**。系统将显示 **添加区域 (Add Area)** 对话框。修改以下字段：

- **OSPF 进程 (OSPF Process)** - 选择进程 ID 1。
- **区域 ID (Area ID)** - 确保值为 1。

  其余字段使用默认值。
- **可用网络 (Available Network)** - 要添加要通过隧道通告的网络，请执行以下操作：
  - 要添加新的网络对象，请点击 ＋。输入这些详细信息：
    - **名称 (Name)** - 以 **HUB_Tunnel_IP** 形式输入名称。
    - **网络 (Network)** - 选择**主机 (Host)** 选项，然后输入主机 IP **198.48.133.81**。
    - 点击**保存 (Save)**。
  - 在**可用网络 (Available Network)** 字段的搜索区域中输入**中心 (HUB)**。系统将列出新添加的网络对象 (**HUB_Tunnel_IP**)。选择对象，然后点击**添加 (Add)** 将其添加到**所选网络 (Selected Network)** 列表。
  - 在**可用网络 (Available Network)** 字段的搜索区域中输入**企业 (Corporate)**。系统将列出 **Corporate_LAN** 网络对象。选择对象，然后点击**添加 (Add)** 将其添加到**所选网络 (Selected Network)** 列表。
- 点击**确定 (OK)**。

将在**区域 (Area)** 选项卡中添加一行。



步骤 10 点击**保存 (Save)**，保存中心节点的 OSPF 配置。

在分支节点上配置 OSPF

步骤 1 要编辑分支节点，请选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击 NGFWBR1 节点的 **编辑**（✎）图标。

步骤 2 在**接口 (Interfaces)** 选项卡中：

- 验证之前在分支配置中创建的 **Tunnel1** 接口的详细信息。
- 验证之前创建的用作 Tunnel1 的 IP 地址的 **Loopback1** 接口的详细信息。

步骤 3 点击**路由 (Routing)**。

步骤 4 点击左侧面板中的 **OSPF**。

步骤 5 选中**进程 1 (Process 1)** 复选框以启用 OSPF 实例。

步骤 6 点击**区域 (Area)** 选项卡。

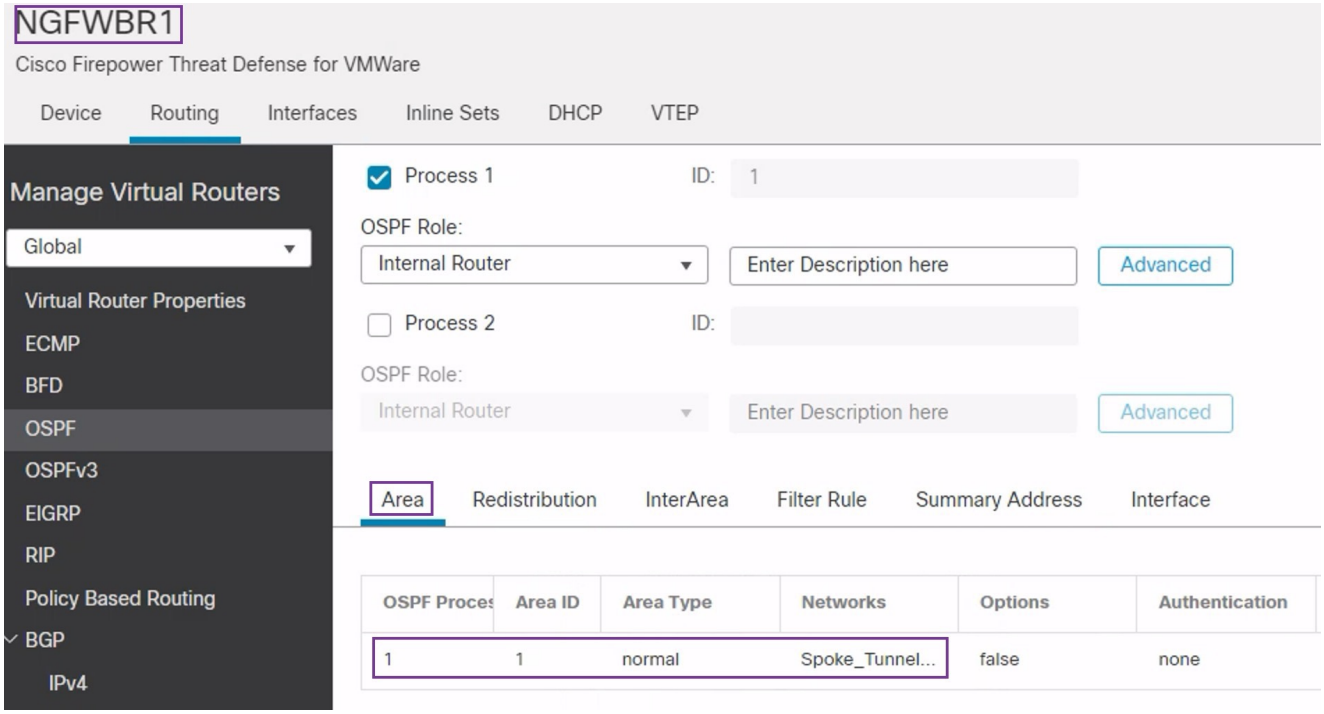
步骤 7 点击 **+添加 (+Add)**。系统将显示 **添加区域 (Add Area)** 对话框。修改以下字段：

- **OSPF 进程 (OSPF Process)** - 选择进程 ID 1。
- **区域 ID (Area ID)** - 确保值为 1。

  其余字段使用默认值。

- **可用网络 (Available Network)** - 要添加要通过隧道通告的网络，请执行以下操作：
  - 要添加新的网络对象，请点击 ＋。输入这些详细信息：
    - **名称 (Name)** - 以 **Spoke_Tunnel_IP** 形式输入名称。
    - **网络 (Network)** - 选择**主机 (Host)** 选项，然后输入主机 IP **169.254.20.1**。
    - 点击**保存 (Save)**。
  - 在**可用网络 (Available Network)** 字段的搜索区域中输入**分支 (Spoke)**。系统将列出新添加的网络对象 (**Spoke_Tunnel_IP**)。选择对象，然后点击**添加 (Add)** 将其添加到**所选网络 (Selected Network)** 列表。
  - 在**可用网络 (Available Network)** 字段的搜索区域中输入**分支机构 (Branch)**。系统将列出 **Branch_LAN** 网络对象。选择对象，然后点击**添加 (Add)** 将其添加到**所选网络 (Selected Network)** 列表。
- 点击**确定 (OK)**。

将在**区域 (Area)** 选项卡中添加一行。



步骤 8 点击**保存 (Save)**，保存分支节点的 OSPF 配置。

配置访问控制策略。

在继续之前，请确保 **NGFW1** 和 **NGFWBR1** 节点上的 VTI 接口与标记为 **Tunnel_Zone** 的新区域相关联。

导航至**策略 (Policies) > 访问控制 (Access Control)** 以查看访问控制策略。必须为中心和分支更新以下访问控制策略，以允许进出隧道的 VPN 流量。

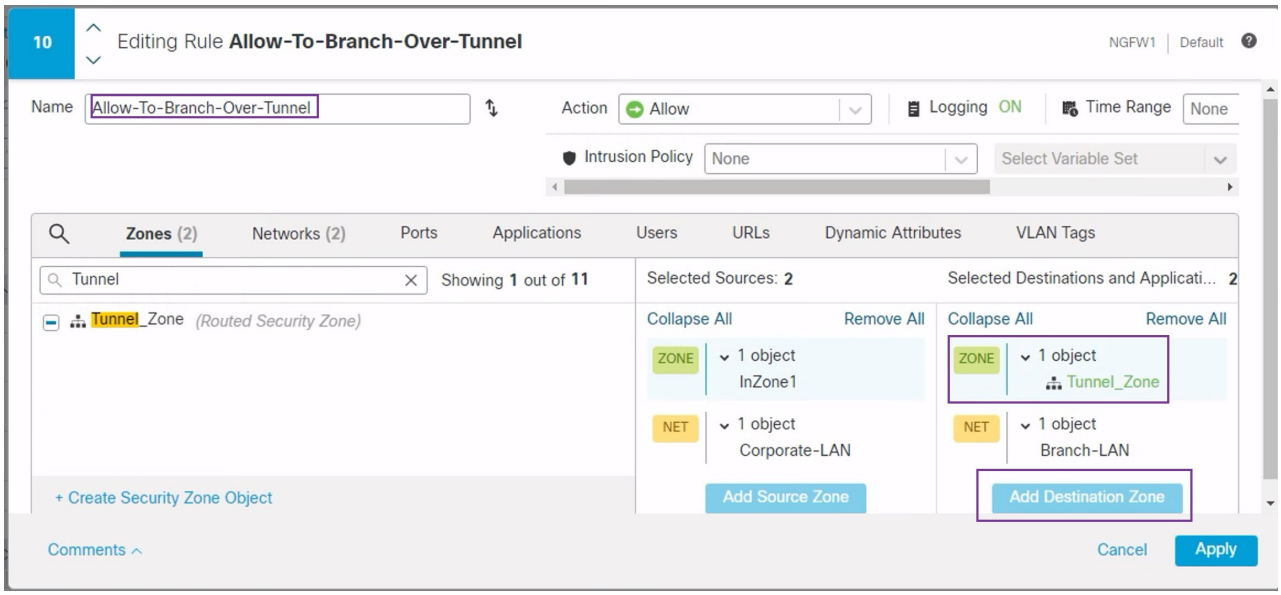
- **NGFW1** - 中心节点 (NGFW1) 的访问控制策略
- **分支机构访问控制** - 分支节点 (NGFWBR1) 的访问控制策略

步骤 1 要编辑中心节点 (NGFW1) AC 策略，请点击 **编辑**（✎） 图标。

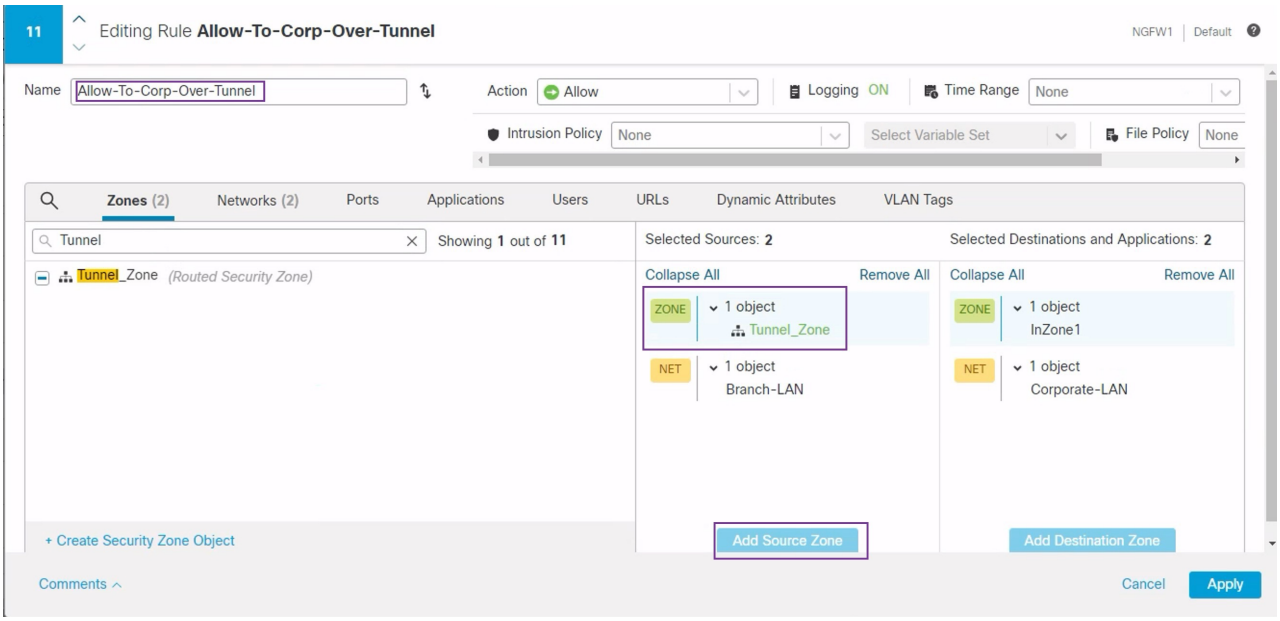
必须为此使用案例修改的现有规则包括：

- **Allow-To-Branch-Over-Tunnel**
- **Allow-To-Corp-Over-Tunnel**

1. 要编辑 **Allow-To-Branch-Over-Tunnel** 策略，请点击 **编辑**（✎） 图标。
2. 在**区域 (Zones)** 选项卡中，搜索 **Tunnel_Zone** 并将其选中，然后点击**添加目标区域 (Add Destination Zone)**。



3. 点击**应用 (Apply)** 保存规则。
4. 要编辑 **Allow-To-Corp-Over-Tunnel** 策略，请点击 **编辑**（✎） 图标。
5. 在**区域 (Zones)** 选项卡中，搜索 **Tunnel_Zone** 并将其选中，然后点击**添加源区域 (Add Source Zone)**。



6. 点击**应用 (Apply)** 保存规则。
7. 验证 NGFW1 中的更新规则。
8. 点击**保存 (Save)** 以保存 AC 策略。
9. 点击**返回访问控制策略管理 (Return to Access Conrol Policy Management)** 以返回策略页面。

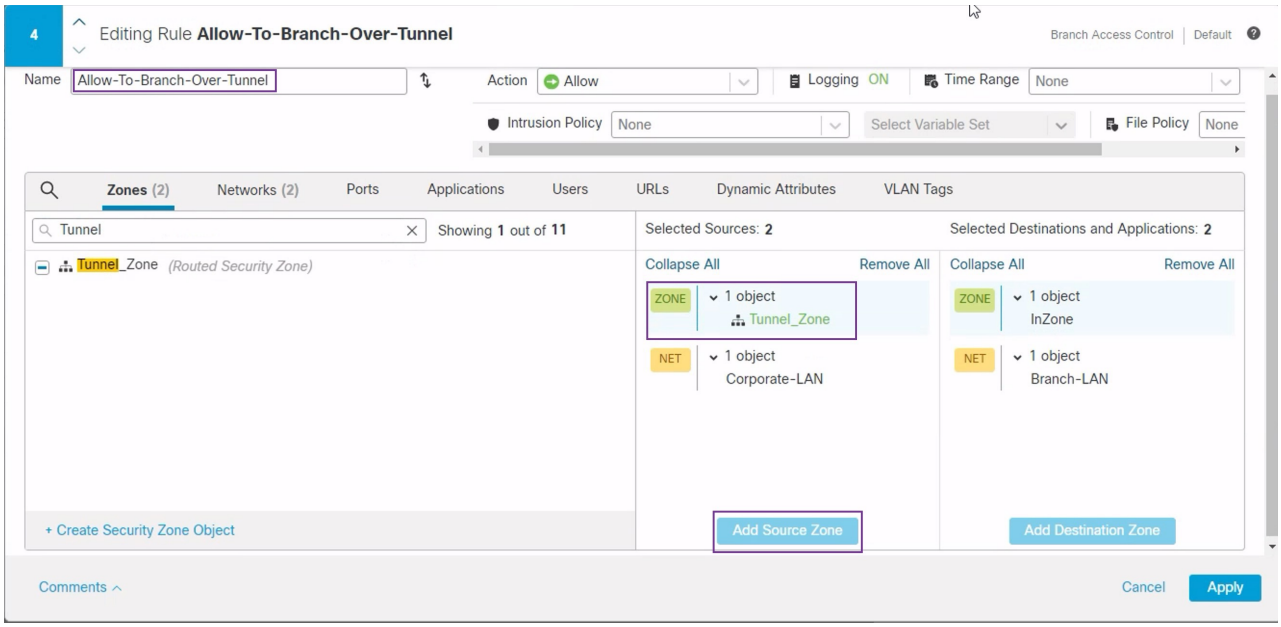
步骤 2 要编辑分支节点 (NGFWBR1) AC 策略，请点击 **编辑**（✎） 图标。

必须为此示例编辑的规则包括：

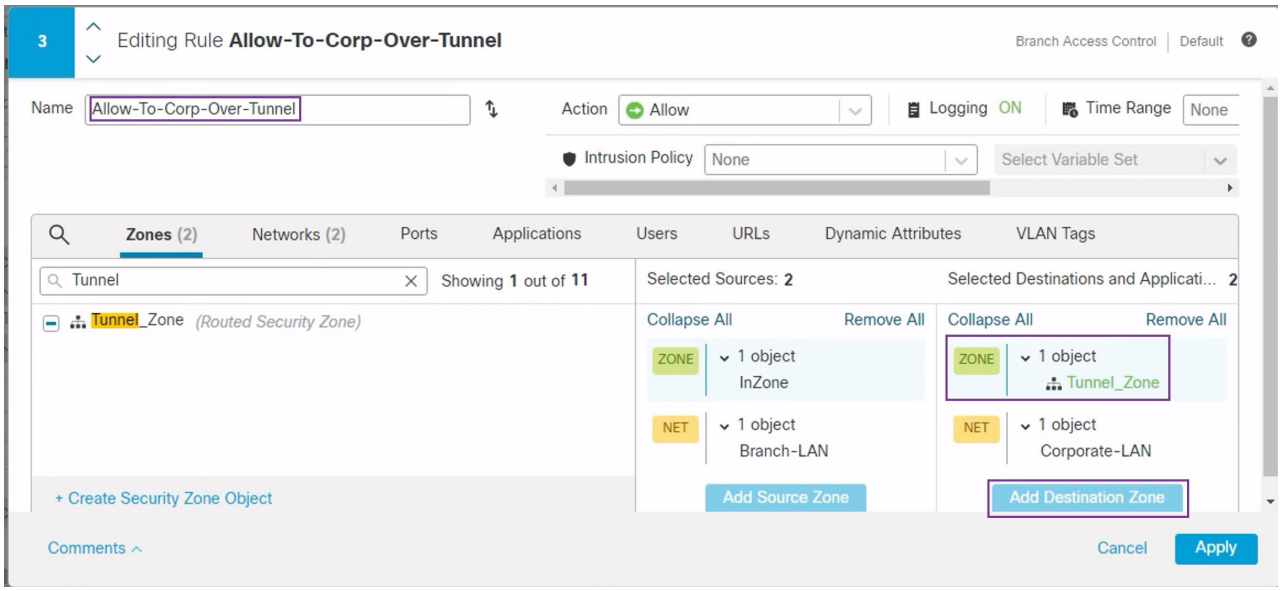
- **Allow-To-Branch-Over-Tunnel**
- **Allow-To-Corp-Over-Tunnel**

1. 要编辑 **Allow-To-Branch-Over-Tunnel** 策略，请点击 **编辑**（✎） 图标。
2. 在**区域 (Zones)** 选项卡中，搜索 **Tunnel_Zone** 并将其选中，然后点击**添加源区域 (Add Source Zone)**。

配置访问控制策略。



3. 点击**应用 (Apply)** 保存规则。
4. 要编辑 **Allow-To-Corp-Over-Tunnel** 策略，请点击 **编辑**（ ）图标。
5. 在**区域 (Zones)** 选项卡中，搜索 **Tunnel_Zone** 并将其选中，然后点击**添加目标区域 (Add Destination Zone)**。



6. 点击**应用 (Apply)** 保存规则。
7. 验证 NGFWBR1 中的更新规则。

8. 点击**保存 (Save)** 以保存 AC 策略。

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)**。这样将显示已准备好部署的设备列表。

步骤 2 选中要部署配置更改的 NGFWBR1 和 NGFW1 旁边的复选框。

步骤 3 点击**部署 (Deploy)**。等待部署在“部署”(Deploy) 对话框中标记为“已完成”(Completed)。

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：

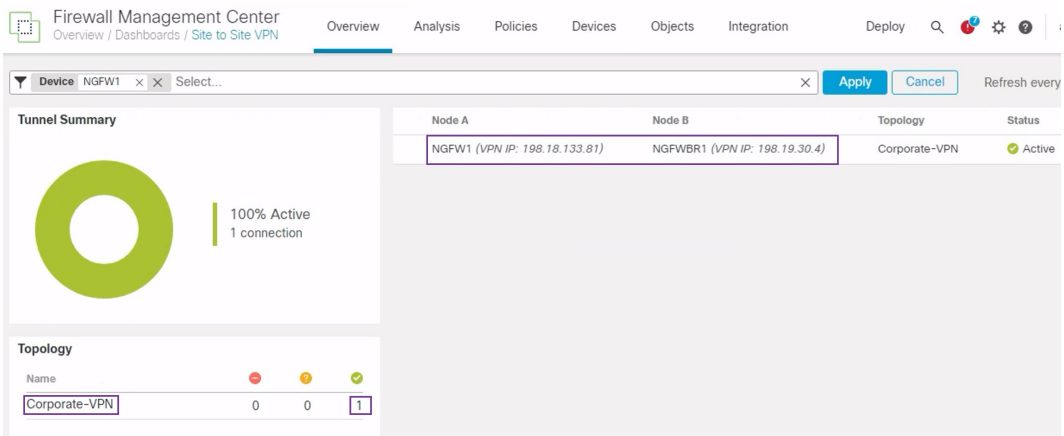
- 继续部署 - 继续部署而无需解决警告情况。如果系统识别错误，则无法继续。
- 关闭 - 退出而不部署。解决错误和警告情况，并尝试重新部署该配置。

验证流经 VPN 隧道的流量

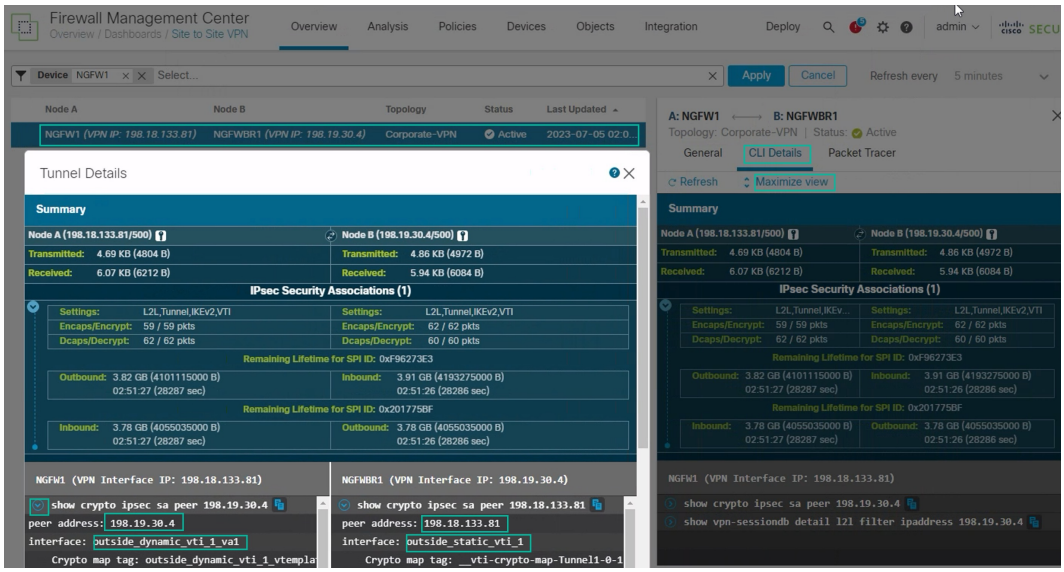
对 VPN 隧道执行以下验证。

- **在站点间 VPN 控制面板上验证隧道状态**

1. 要验证 VPN 隧道是否正常运行，请选择**概述 (Overview)** > **控制面板 (Dashboards)** > **站点间 VPN (Site-to-site VPN)**。

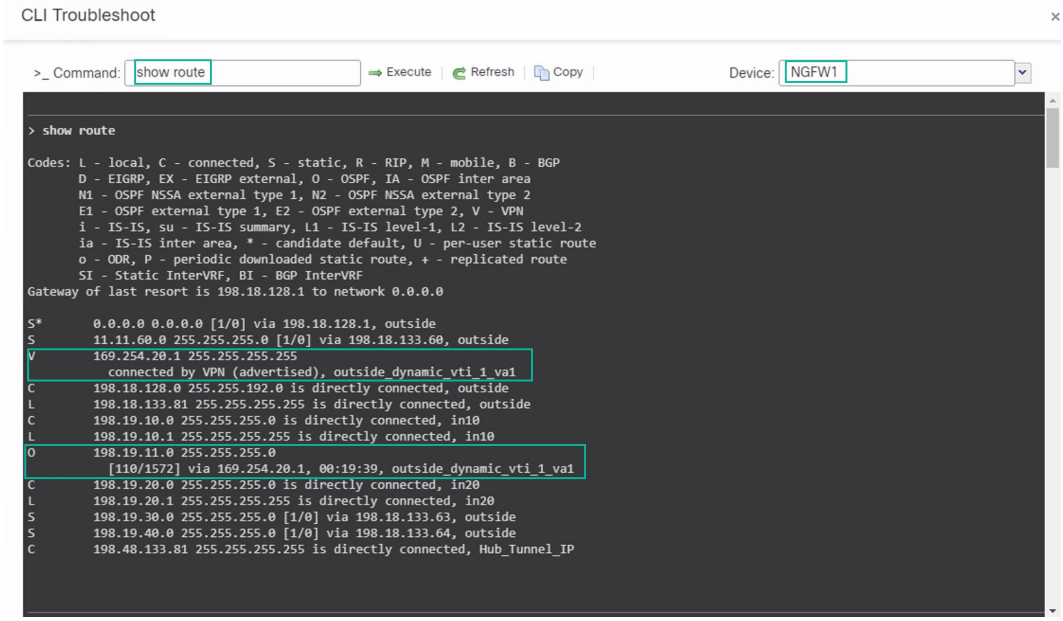


2. 将鼠标光标悬停在 NGFW1 上。NGFW1 旁边会显示**查看完整信息 (View Full Information)** 图标。
3. 点击**查看完整信息 (View Full Information)** 图标。系统将显示包含隧道详细信息和其他操作的侧窗格。
4. 点击侧窗格中的 **CLI 详细信息 (CLI Details)** 选项卡。
5. 点击**最大化视图 (Maximize View)** 以显示包含 IPSec 安全关联详细信息的最大化对话框。
6. 您可以在对话框的下半部分展开 show 命令的 CLI，以查看设备上的 VTI 接口。



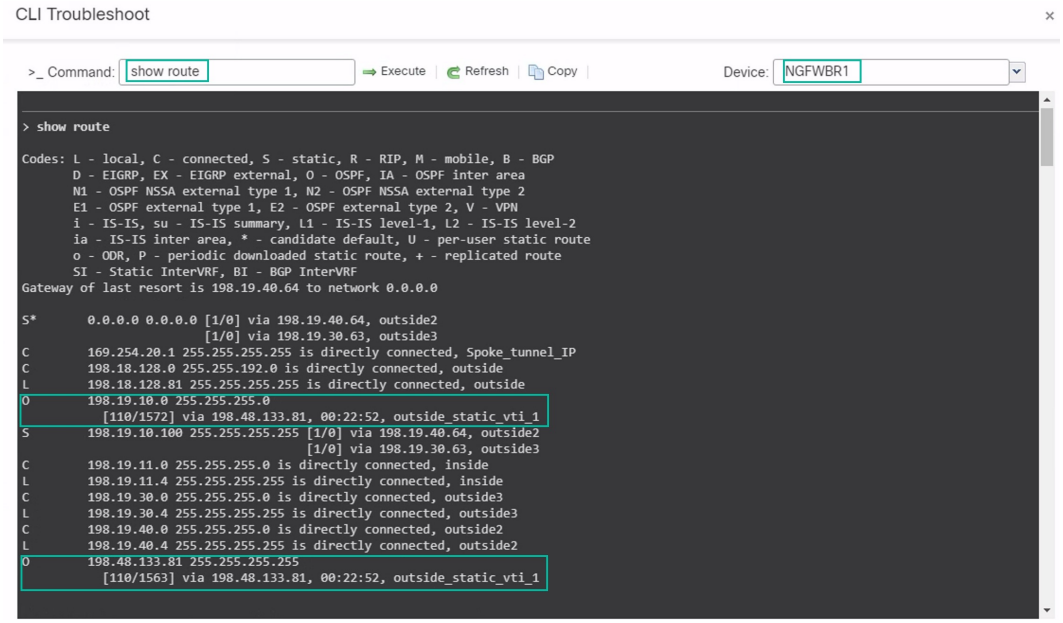
7. 点击**关闭 (Close)** 以终止“隧道详细信息”(Tunnel Details) 窗口。

- **验证中心和分支机构节点上的路由 (Verify Routing on the Hub and Branch Nodes)** - 验证是否已在 **NGFW1** 和 **NGFWBR1** 上正确获知 OSPF 路由。节点：
  1. 依次选择**设备 (Devices)** > **设备管理 (Device Management)**。
  2. 要编辑 NGFW1，请点击 **编辑**（ ） 图标。
  3. 点击**设备 (Device)** 选项卡。
  4. 点击**常规 (General)** 卡中的 **CLI** 按钮。系统将显示 **CLI 故障排除 (CLI Troubleshoot)** 窗口
  5. 在**命令 (Command)** 字段中输入 **show route**，然后点击**执行 (Execute)**。
  6. 查看 NGFW1 节点上的路由，确认分支 的 VTI IP (169.254.20.1) 的 VPN 路由和 Branch_LAN (198.19.11.0/24) 的 OSPF 获知路由，如下图所示。



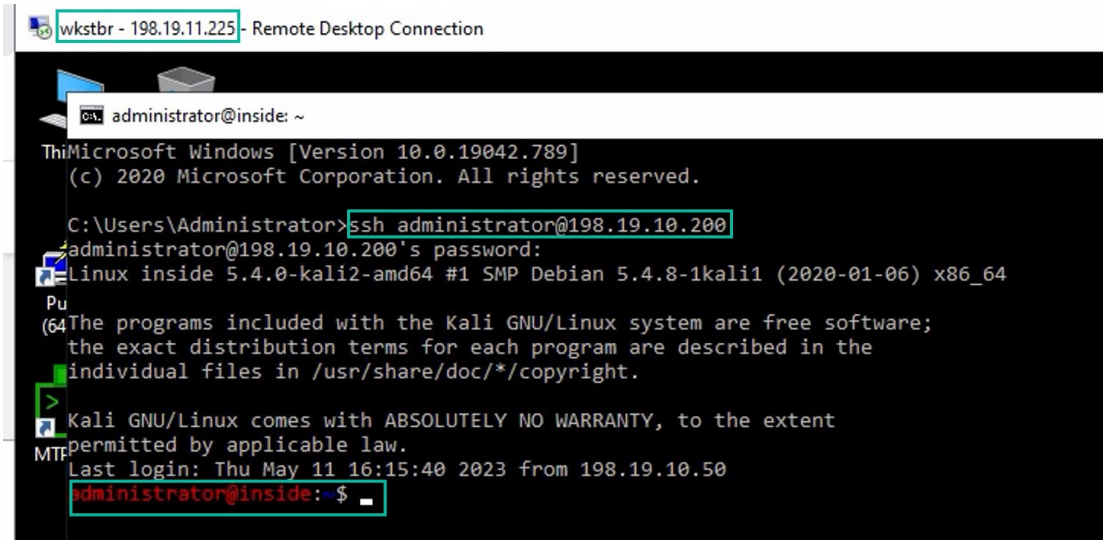
7. 对 NGFWBR1 节点重复步骤 2 至 5。

8. 查看 NGFWBR1 节点上的路由。确认为中心的 VTI IP (198.48.133.81) 和 Corporate_LAN (198.19.10.0/24) 获知的 OSPF 路由，如下图所示。



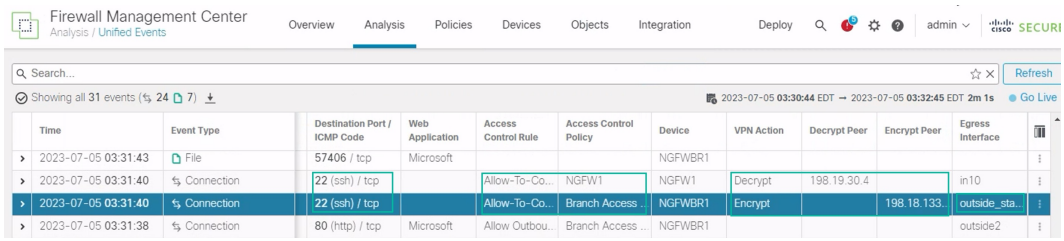
- 验证分支和中心节点背后的受保护网络之间的流量

  登录 WKST BR 工作站 (198.19.11.225)，通过 SSH 连接到 NGFW1 后面的主机 (198.19.10.200)。确保您能够成功通过 SSH 连接到主机。



- 使用统一事件验证分支机构和分支节点之间的连接

1. 选择分析 **(Analysis)** > 统一事件 **(Unified Events)**。
2. 使用列选择器添加**VPN** 操作 **(VPN Action)**、加密对 **(Encrypt Peer)**、解密对 **(Decrypt Peer)** 和入口接口 **(Egress Interface)** 列。
3. 对新列目标端口/**ICMP** 代码 **(Destination Port/ICMP Code)**、访问控制规则 **(Access Control Rule)**、访问控制策略 **(Access Control Policy)** 和设备 **(Device)** 重新排序并调整大小，如下图所示。



4. 要查看与从 **WKST BR** 到企业主机的 SSH 连接相关的事件，请在目标端口/**ICMP** 代码 **(Destination Port/ICMP Code)** 列中选择包含 **22 (ssh/tcp)** 的行。请注意，通过 **outside_static_vti_1** 接口在 **NGFWBR1** 上执行加密操作，然后在 **NGFW1** 上执行解密操作，如上图所示。

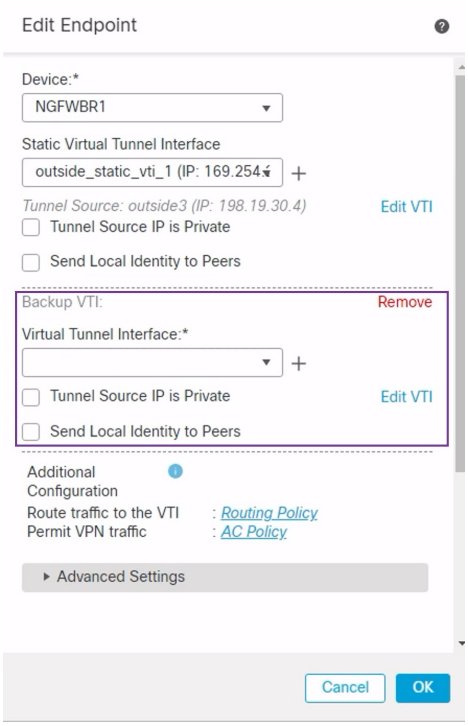
在分支节点上配置备份 VTI 接口

Cisco Secure Firewall Threat Defense 支持为基于路由的 (VTI) VPN 配置备份隧道。当主 VTI 无法路由流量时，VPN 中的流量会通过备用 VTI 传送。

步骤 1 依次选择**设备 (Devices)** > **站点间 VPN (Site-to-site VPN)** 查看已配置的企业 VPN 拓扑，然后点击 **编辑**（✎） 图标。系统将显示“编辑 VPN 拓扑”(Edit VPN Topology) 窗口。

步骤 2 在“分支节点”(Spoke Nodes) 部分中，点击 **NGFWBR1** 节点的 **编辑**（✎） 图标。系统将显示**编辑终端 (Edit Endpoint)** 对话框。

步骤 3 点击**添加备份 VTI (Add Backup VTI)** 链接以添加辅助 VTI 隧道。该链接将显示“备份 VTI”(Backup VTI) 部分。



步骤 4 点击**虚拟隧道接口 (Virtual Tunnel Interface)** 下拉列表旁边的 + 以添加新的 VTI。

系统将显示 **添加虚拟隧道接口** 对话框，其中包含预填充的默认配置。

- **隧道类型 (Tunnel Type)** 会被自动填充为**静态 (Static)**。
- **名称 (Name)** 会自动填充为 *<tunnel_source interface logical name>*+ static_vti +*<tunnel ID>*。例如，**outside_static_vti_2**。
- 默认情况下，**启用 (Enabled)** 复选框处于选中状态。
- 从“安全区域”(Security Zone) 下拉列表中选择 **Tunnel_Zone**。
- **隧道 ID (Tunnel ID)** 会自动填充值 2。
- 从**隧道源 (Tunnel Source)** 下拉列表中选择 **GigabitEthernet0/3 (outside2)**。从 outside 3 接口旁边的下拉列表中选择 **198.19.40.4** 作为其 IP 地址。
- 默认情况下，**IPsec 隧道模式 (IPsec Tunnel Mode)** 会被设置为 IPv4。

- **IP 地址 (IP address)** 可以是静态 IP 地址或借用 IP 地址。我们建议您从环回接口为静态接口配置借用 IP。要添加环回接口，请从下拉列表中点击选择**环回接口 1 (Spoke_Tunnel_IP) (Loopback 1[Spoke_Tunnel_IP])**。

点击**确定 (OK)** 以保存 VTI。系统将显示一条消息，确认 VTI 已成功创建。点击**确定 (OK)**。

备份 VTI 接口设置为 **outside_static_vti_2(169.254.20.1)**。

步骤 5 点击**确定 (OK)** 保存分支配置。

步骤 6 点击**保存 (Save)** 保存 VPN 拓扑。

为主 VTI 接口和辅助 VTI 接口配置 ECMP 区域

在分支节点的主要和辅助静态 VTI 接口上配置 ECMP，以实现链路冗余和 VPN 流量负载平衡。

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**)。

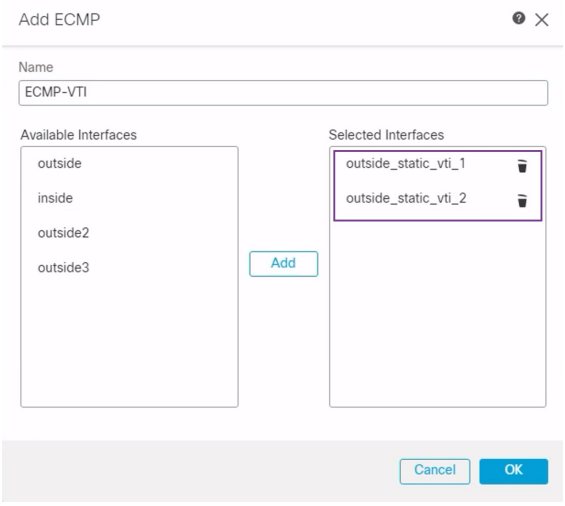
步骤 2 点击 NGFWBR1 接口视图上的**路由 (Routing)** 选项卡。

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-VTI**。

步骤 6 要关联接口，请在**可用接口 (Available Interfaces)** 框下选择接口 **outside_static_vti_1** 和 **outside_static_vti_2**，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。

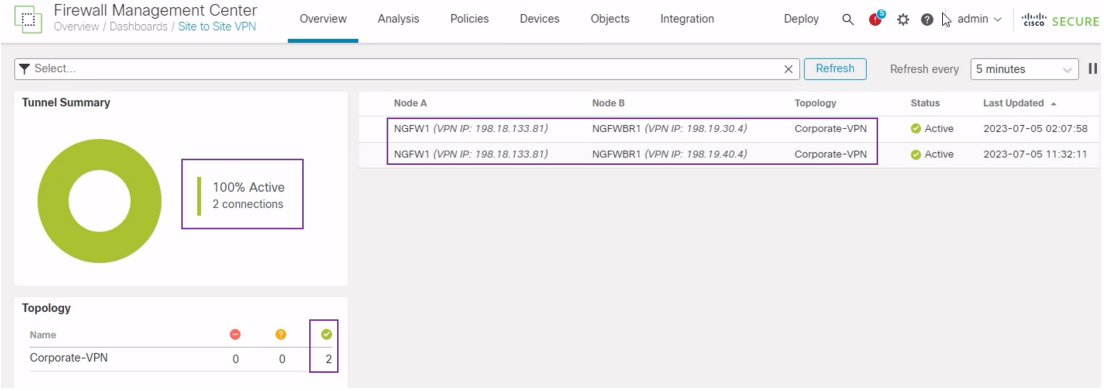
步骤 8 点击**保存 (Save)**。

验证主隧道和辅助隧道

验证分支节点和中心节点之间的主要 VTI 隧道和辅助 VTI 隧道是否都已配置、启动并处于活动状态。

- **在站点间 VPN 控制面板上验证隧道状态**

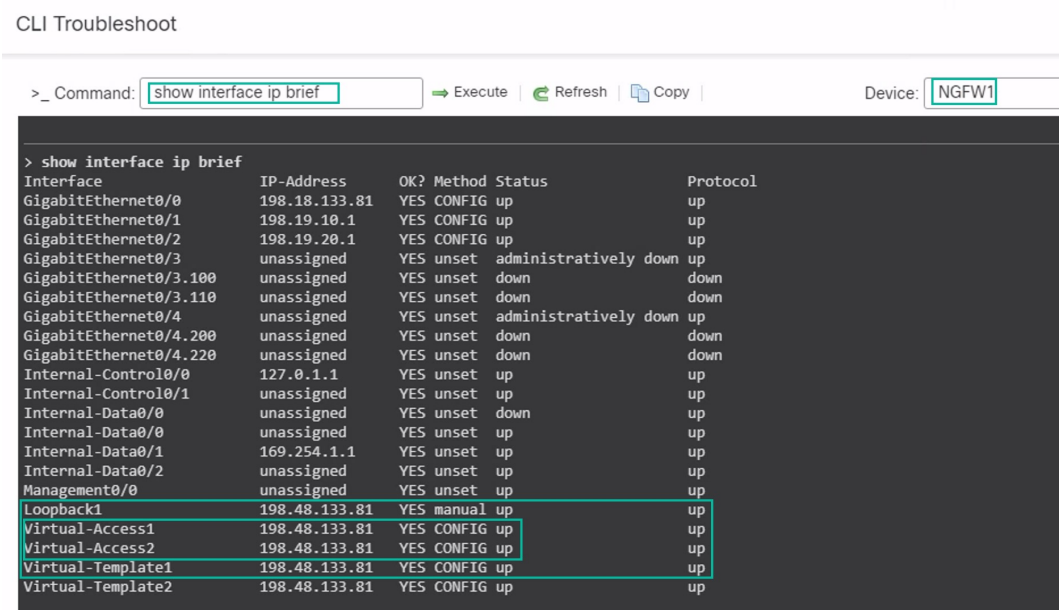
  要验证 VPN 隧道是否正常运行，请选择**概述 (Overview)** > **控制面板 (Dashboards)** > **站点间 VPN (Site-to-site VPN)**。



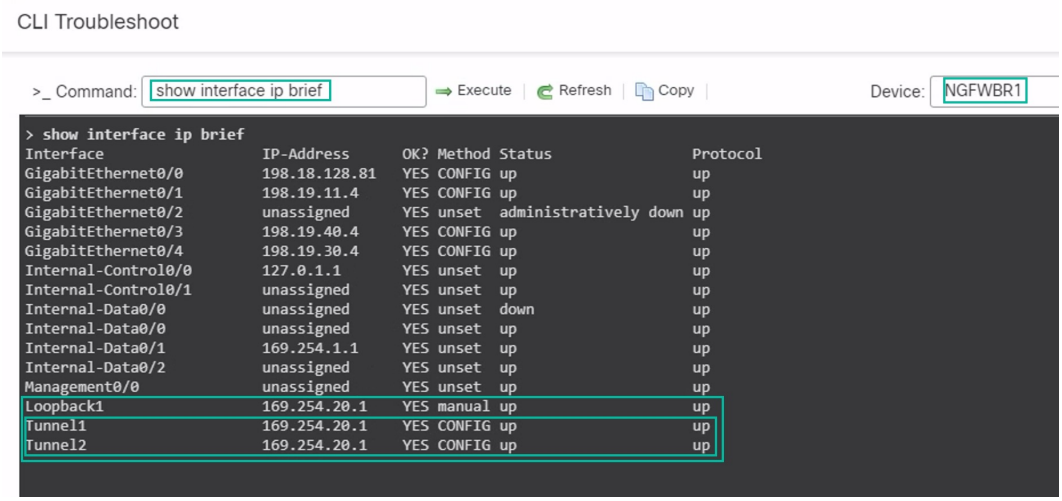
- **验证中心和分支机构节点上的路由**

  1. 依次选择**设备 (Devices)** > **设备管理 (Device Management)**。
  2. 要编辑 NGFW1，请点击编辑图标。
  3. 点击**设备 (Device)** 选项卡。
  4. 点击**常规 (General)** 卡中的 **CLI** 按钮。系统将显示 **CLI 故障排除 (CLI Troubleshoot)** 窗口
  5. 在**命令 (Command)** 字段中输入 **show interface ip brief**，然后点击**执行 (Execute)** 以查看从中心上的 DVTI 创建的动态虚拟接入接口。

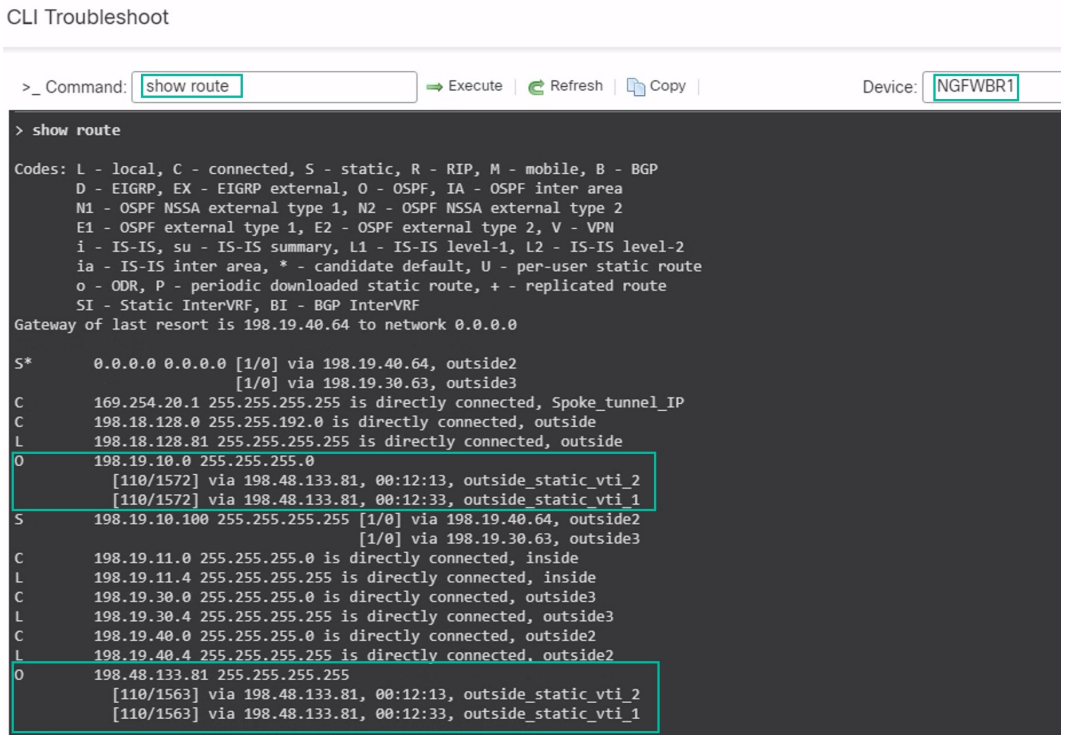
注释 当 **NGFWBR1** 通过辅助 VTI 连接连接到 NGFW1 时，会从同一 DVTI 生成 Virtual-Access2 接口。



6. 对 NGFWBR1 节点重复步骤 2 至 5，以便查看静态 VTI 接口 **Tunnel1** 和 **Tunnel2**，如下图所示。



7. 在**命令 (Command)** 字段中输入 **show route**，然后点击**执行 (Execute)** 以查看添加辅助 VTI 隧道后的路由。



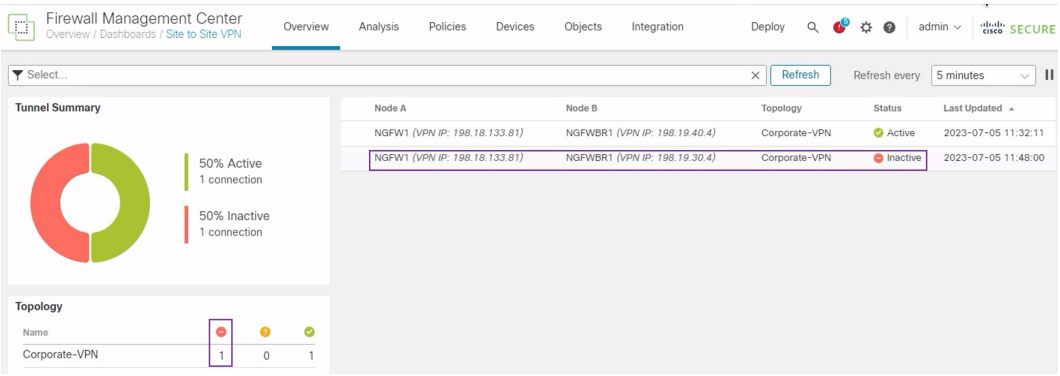
- 请注意，已在主要 (**outside_static_vti_1**) 和辅助 (**outside_static_vti_2**) VTI 上通过 OSPF 获知 **Corporate_LAN** (198.19.10.0/24)。
- 请注意，主 VTI 和辅助 VTI 也已通过 OSPF 获知了 DVTI 隧道 IP (198.48.133.81)。

- **当主隧道关闭时验证到辅助隧道的故障转移**

1. 在本示例中，要验证到辅助隧道的故障转移，可以通过上游设备上的访问控制列表限制来自 outside3 接口的出站流量，或通过关闭用于 Cisco Secure Firewall Threat Defense 的 outside3 接口来诱发丢包来自防火墙管理中心。

注释 关闭接口具有网络侵入性，不得在生产网络中尝试。

2. 在站点间 VPN 控制面板中，主隧道已关闭，如下图所示。



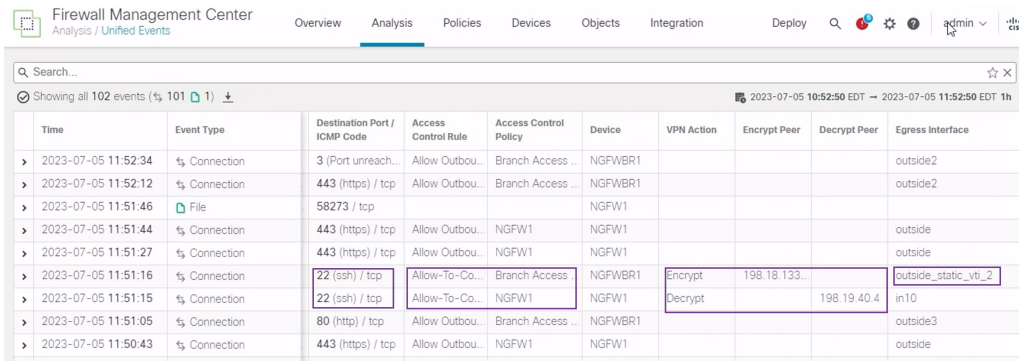
3. 发起从分支机构到中心的流量。登录 WKST BR 工作站，通过 SSH 来访问 NGFW1 后面的主机。确保您能够成功通过 SSH 连接到主机。

4. 使用统一事件查看器验证流量的出口路径：

   1. 选择**分析 (Analysis) > 统一事件 (Unified Events)**。

   2. 使用列选择器添加**VPN 操作 (VPN Action)**、**加密对 (Encrypt Peer)**、**解密对 (Decrypt Peer)** 和**入口接口 (Egress Interface)** 列。

   3. 对新列**目标端口/ICMP 代码 (Destination Port/ICMP Code)**、**访问控制规则 (Access Control Rule)**、**访问控制策略 (Access Control Policy)** 和**设备 (Device)** 重新排序并调整大小，如下图所示。



请注意，**NGFWBR1** 上用于 SSH 的出口接口（端口 22）现在显示为辅助接口 (**outside_static_vti_2**)。

基于路由的 VPN 隧道故障排除

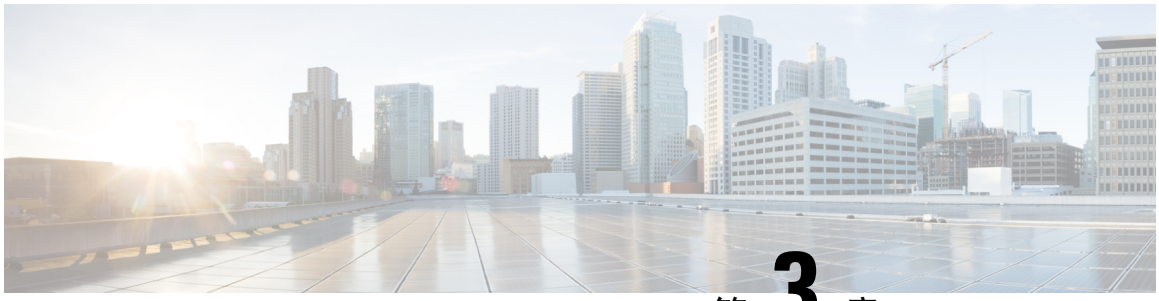
在部署后，使用以下 CLI 调试与 Cisco Secure Firewall Threat Defense 上基于路由的 VPN 隧道相关的问题。

注释 在生产环境中，在威胁防御设备上运行调试命令时要小心谨慎。您可以在设备上设置各种调试级别，这些级别可能会有冗长的输出。

如何...	CLI 命令
为特定对等体启用条件调试	**调试加密条件对等体 <peer-IP>**
调试虚拟隧道接口信息	**debug vti 255**
调试 IKEv2 协议相关事务	**debug crypto ikev2 protocol 255**
调试 IKEv2 平台相关事务	**debug crypto ikev2 platform 255**
调试常见的 IKE 相关事务	**debug crypto ike-common 255**
调试 IPSec 相关事务	**debug crypto ipsec 255**

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



第 3 章

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， 第 33 页
- 优势， 第 35 页
- 此使用案例适合您吗？ ， 第 35 页
- 用于直接互联网接入的组件， 第 35 页
- 最佳实践， 第 35 页
- 前提条件， 第 36 页
- 场景 1：不带路径监控的直接互联网访问， 第 36 页
- 配置受信任的 DNS 服务器， 第 39 页
- 配置接口优先级， 第 40 页
- 创建 ECMP 区域， 第 40 页
- 配置等价静态路由， 第 40 页
- 为 YouTube 配置扩展 ACL 对象， 第 41 页
- 为 WebEx 配置扩展 ACL 对象， 第 42 页
- 为 YouTube 配置策略型路由策略， 第 42 页
- 为 WebEx 配置策略型路由策略， 第 43 页
- 部署配置， 第 44 页
- 验证应用流量， 第 44 页
- 策略型路由监控和故障排除 ， 第 46 页
- 其他资源， 第 49 页

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

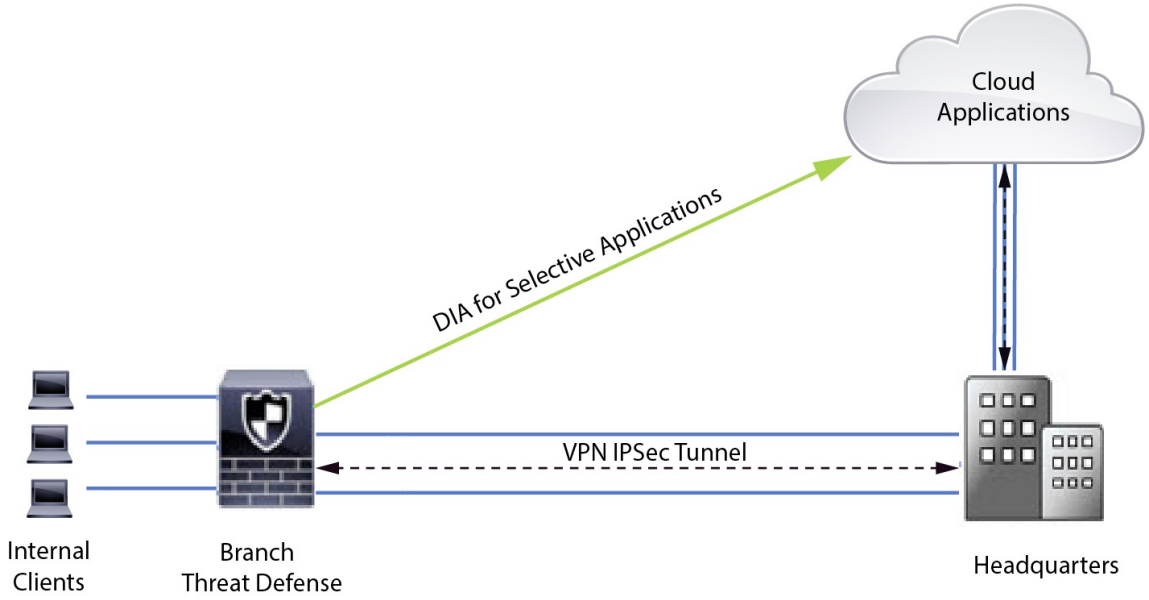
传统上，网络部署会利用中心站点上的边界防火墙来为本地和分支机构用户提供安全访问。这种架构可提供所需的连接，但它会将所有互联网流量作为加密流量通过VPN隧道传输到中心站点，从而导致数据包延迟、丢包和抖动。此外，网络还不断面临着与部署和复杂的网络管理相关的高成本和带宽利用率的挑战。

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 ，第 54 页。

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。

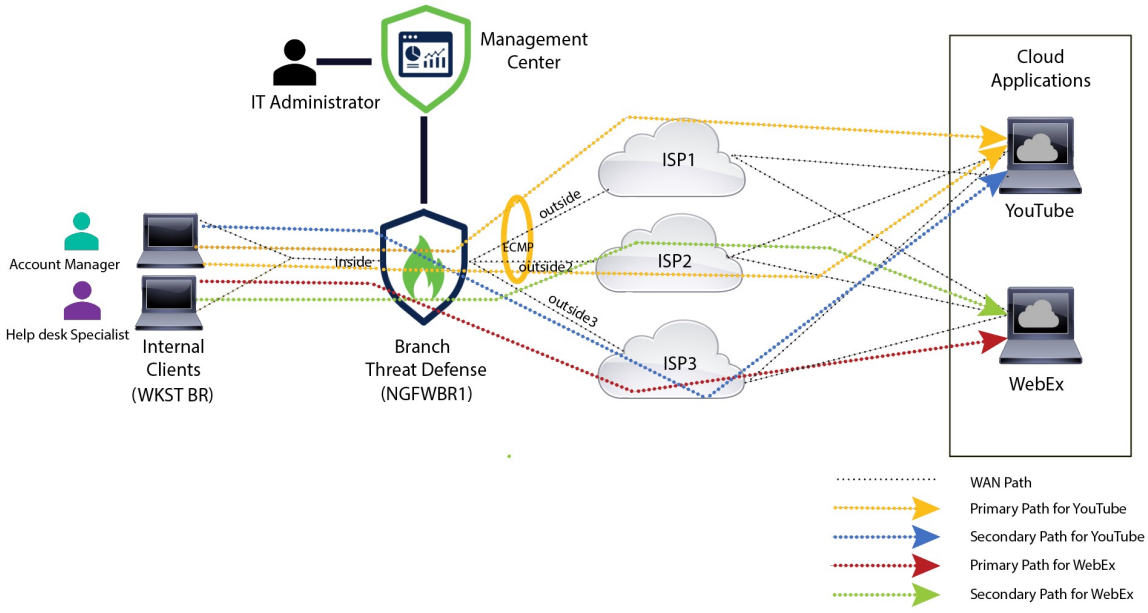
不带路径监控的网络拓扑-DIA

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）

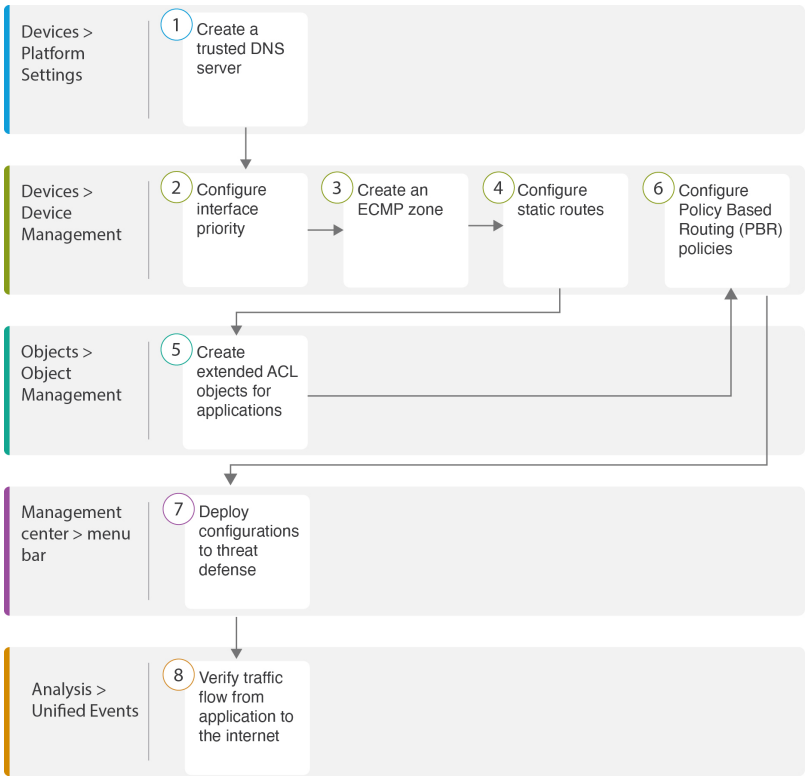


通过 DIA，分支机构防火墙后面的用户就可以访问：

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 39 页。
2	（前提条件）配置接口优先级。请参阅 配置接口优先级， 第 40 页。
3	（前提条件）创建 ECMP 区域。请参阅 创建 ECMP 区域， 第 40 页。
4	（前提条件）配置静态路由。请参阅 配置等价静态路由， 第 40 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 41 页 • 为 WebEx 配置扩展 ACL 对象， 第 42 页
6	为应用配置 PBR 策略。请参阅 • 为 YouTube 配置扩展 ACL 对象， 第 41 页 • 为 YouTube 配置策略型路由策略， 第 42 页
7	在威胁防御上部署配置。请参阅 部署配置， 第 44 页。

步骤	说明
8	验证 YouTube 和 WebEx 流量。请参阅验证应用流量，第 44 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 40 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)**。

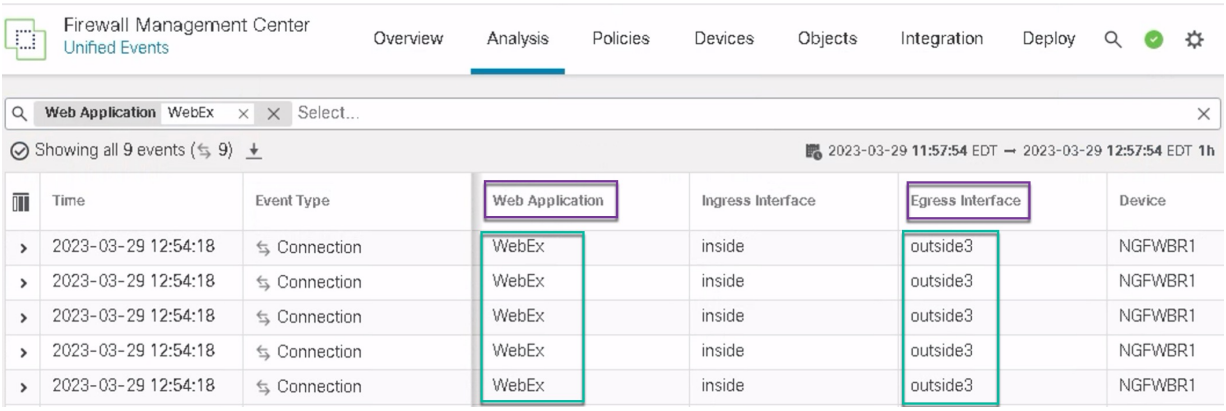
步骤 5 在 **Web 应用 (Web Application)** 过滤器中，输入名称 **YouTube** 并点击**应用 (Apply)**。

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。

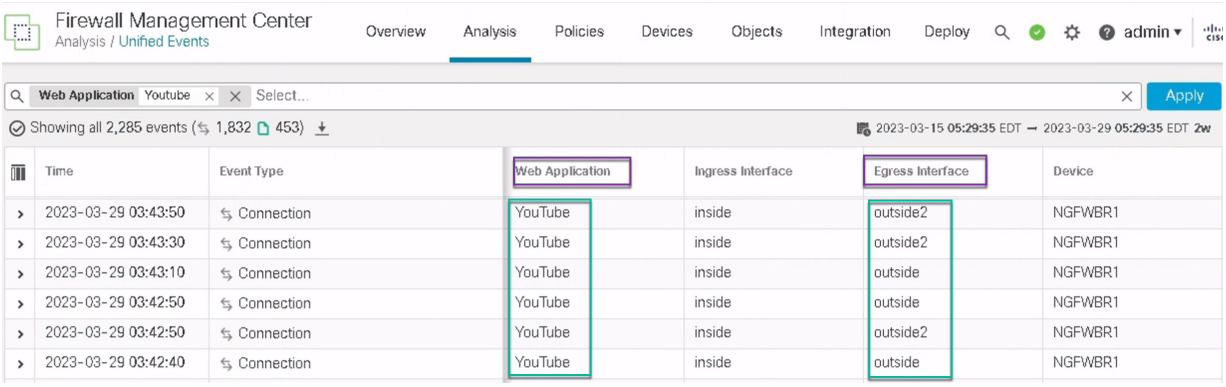
步骤 7 在管理中心中，验证两个应用的流量。

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。

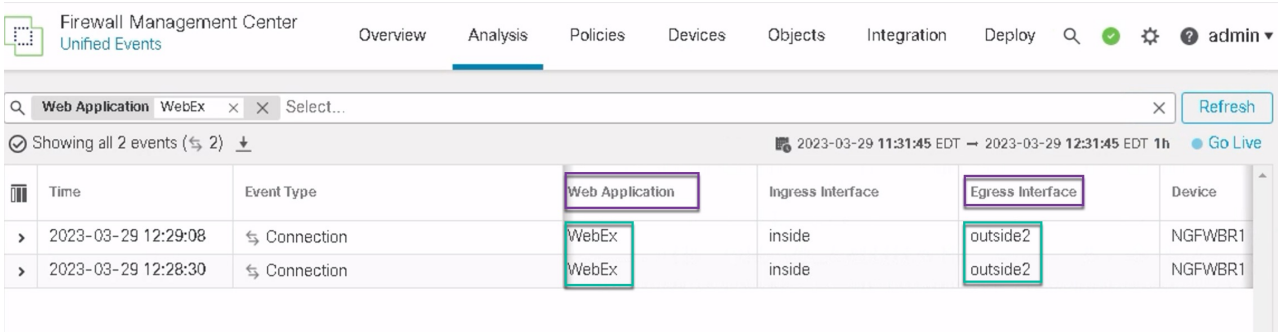


   - **YouTube** 应用流量按照下图所示的配置在 **outside** 和 **outside2** 接口之间进行负载均衡。



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。

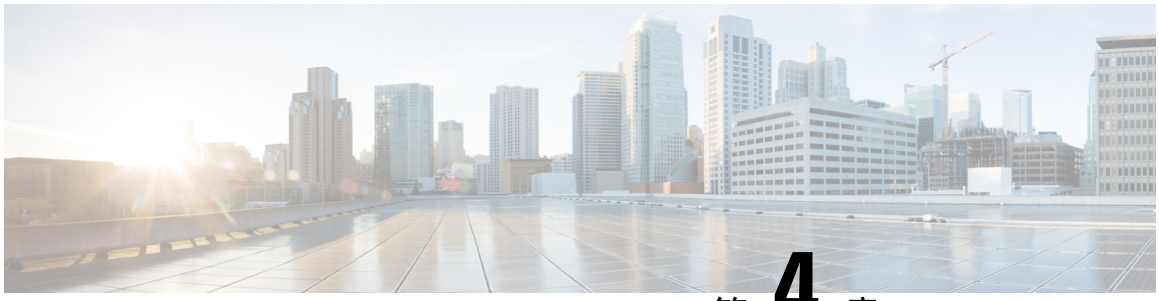
要停止调试过程，请使用以下命令：

```
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



第 4 章

使用带路径监控的直接互联网接入(DIA)将应用流量从分支机构路由到互联网

在本章中，我们将深入探讨具有路径监控的直接互联网接入 (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， 第 51 页
- 优势， 第 53 页
- 此使用案例适合您吗？ ， 第 53 页
- 用于直接互联网接入的组件， 第 53 页
- 最佳实践， 第 53 页
- 前提条件， 第 54 页
- 场景 2：具有路径监控的直接互联网接入， 第 54 页
- 配置受信任的 DNS 服务器， 第 57 页
- 配置接口优先级， 第 58 页
- 配置路径监控设置， 第 58 页
- 为 WebEx 配置扩展 ACL 对象， 第 59 页
- 为 Webex 配置带路径监控的策略型路由策略， 第 59 页
- 部署配置， 第 60 页
- 验证应用流量， 第 60 页
- 策略型路由监控和故障排除 ， 第 62 页
- 其他资源， 第 65 页

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

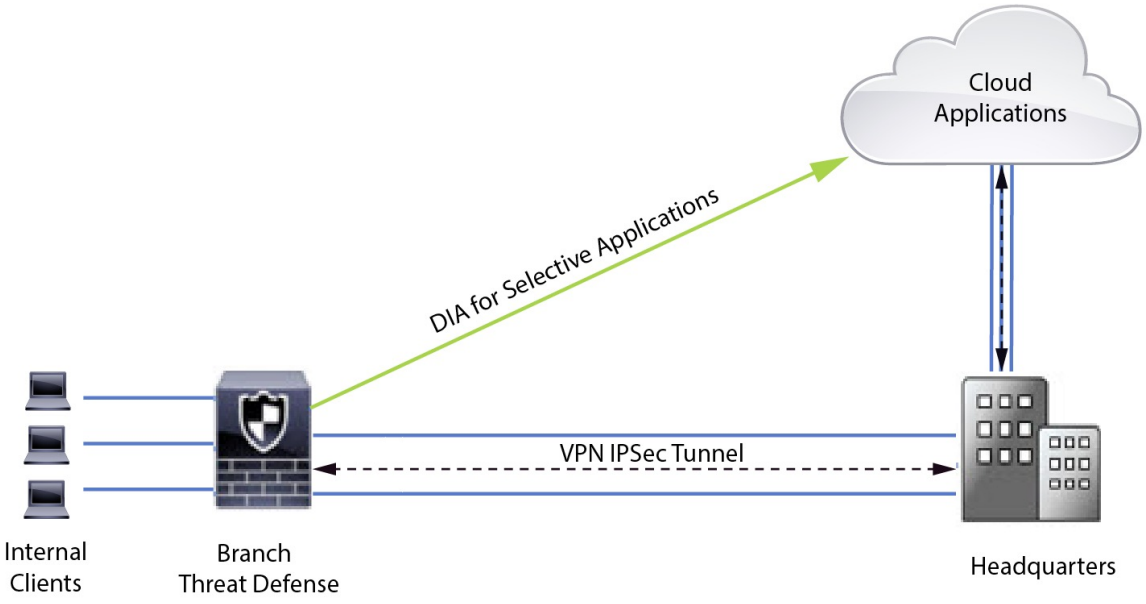
导致数据包延迟、丢包和抖动。此外，网络还不断面临着与部署和复杂的网络管理相关的高成本和带宽利用率的挑战。

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 *3:* 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 ，第 54 页。

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 2：具有路径监控的直接互联网接入

Ann 安是一名服务中心专家，在一家大公司的分公司工作。Ann 在使用 WebEx 时一直遇到连接中断和延迟的问题。

有什么风险？

WebEx 会议依赖于会议主持人和与会者之间的实时数据传输，包括音频和视频流。这种实时数据对网络延迟和丢包很敏感。如果网络出现高丢包率，就会导致音频和视频质量问题，如冻结、滞后或延迟，从而对会议体验造成负面影响。

带有路径监控功能的 PBR 如何解决这一问题？

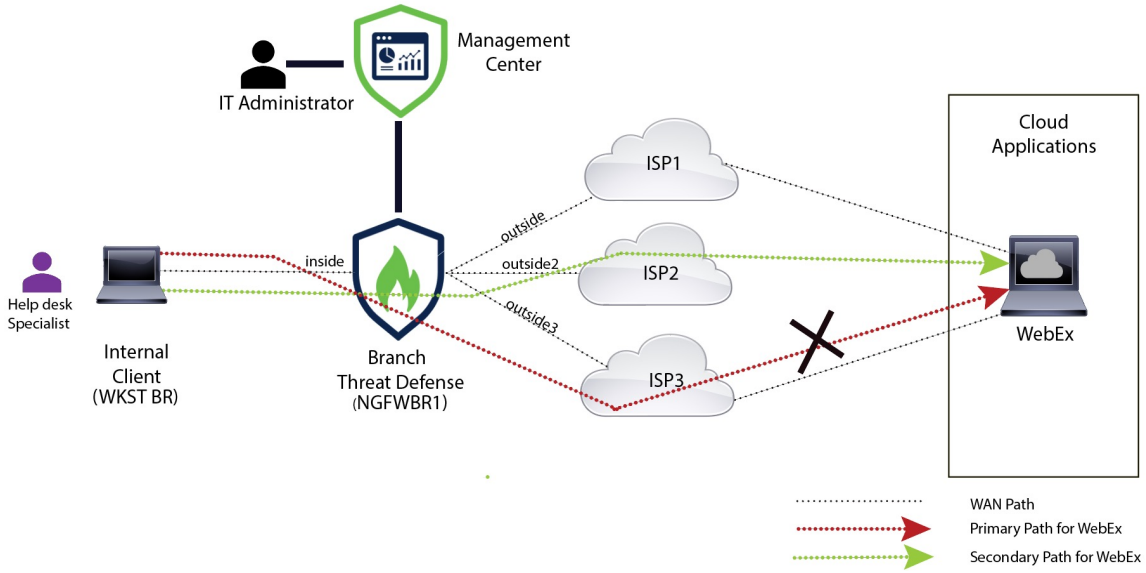
IT 管理员 Alice 使用策略型路由选择和路径监控功能，引导 WebEx 应用程序流量通过出口接口传输到互联网，并将丢包降到最低，从而确保与会者获得最佳的会议体验。

具有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。设备已配置为使用策略型路由直接访问互联网。

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

图 *4:* 直接互联网访问拓扑（带路径监控）



outside2 和 **outside3** 出口接口已启用路径监控。为 WebEx 配置的 PBR 策略可将流量路由到出口接口，并将丢包降到最低。

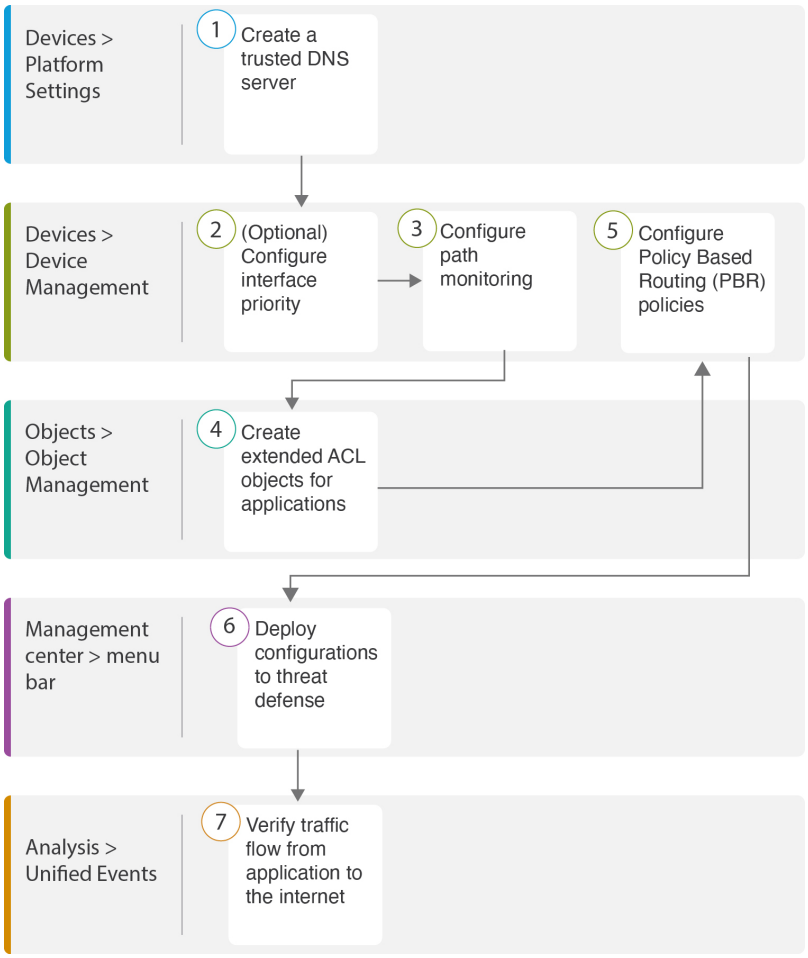
在此场景中，要验证路径监控，可以通过上游设备上的访问控制列表限制来自 **outside3** 接口的出站流量，或通过关闭用于 Cisco Secure Firewall Threat Defense 的 **outside3** 接口来诱发丢包来自防火墙管理中心。

注释 关闭接口具有网络侵入性，不得在生产网络中尝试。

由于丢包，与 **outside3** 接口关联的链路会关闭。协作应用流量通过 **outside2** 接口而不是 **outside3** 接口转发。

使用路径监控来配置 DIA 的端到端步骤

以下流程图说明了在Cisco Secure Firewall Management Center 中配置具有路径监控的 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 39 页。
2	[前提条件（可选）] 配置接口优先级。请参阅 配置接口优先级， 第 40 页。
3	配置路径监控。请参阅 配置路径监控设置， 第 58 页。
4	为应用配置扩展 ACL 对象。请参阅 为 WebEx 配置扩展 ACL 对象， 第 42 页。
5	为应用配置 PBR 策略。请参阅 为 Webex 配置带路径监控的策略型路由策略，第 59 页。
6	在威胁防御上部署配置。请参阅 部署配置， 第 44 页。
7	验证 WebEx 流量。请参阅验证应用流量， 第 44 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)**。

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**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探测。

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击威胁防御设备 (**NGFWBR1**) 的 **编辑**（✎）。

步骤 2 点击要编辑的接口 (**outside**) 的 **编辑**（✎）。

步骤 3 点击 **路径监控 (Path Monitoring)** 选项卡。

步骤 4 选中**启用基于 IP 的路径监控 (Enable IP based Path Monitoring)** 复选框。

步骤 5 从**监控类型 (Monitoring Type)** 下拉列表中，选择相关选项。在本例中，我们使用默认值**接口外的默认路由的下一跳（自动）(Next-hop of default route out of interface [Auto])**。

步骤 6 点击**确定 (OK)**。

步骤 7 对 **outside2** 和 **outside3** 接口重复步骤 2 至 8。

步骤 8 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 Webex 配置带路径监控的策略型路由策略

您可以在“策略型路由选择”页面中配置具有路径监控的 PBR 策略。在本示例中，WebEx 应用流量被转发到了流量损失最小的接口。

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_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**最小丢包率 (Minimal Packet Loss)**。

将流量转发到具有最小丢包的接口。

d) 在**可用接口 (Available Interfaces)** 框中，所有接口都会被列出。从接口列表中，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 8 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)**。

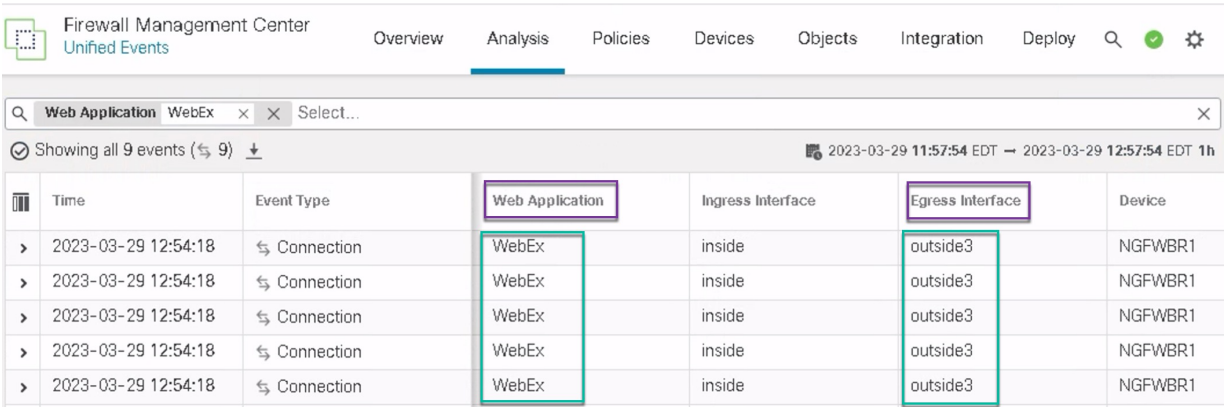
步骤 5 在 **Web 应用 (Web Application)** 过滤器中，输入名称 **YouTube** 并点击**应用 (Apply)**。

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。

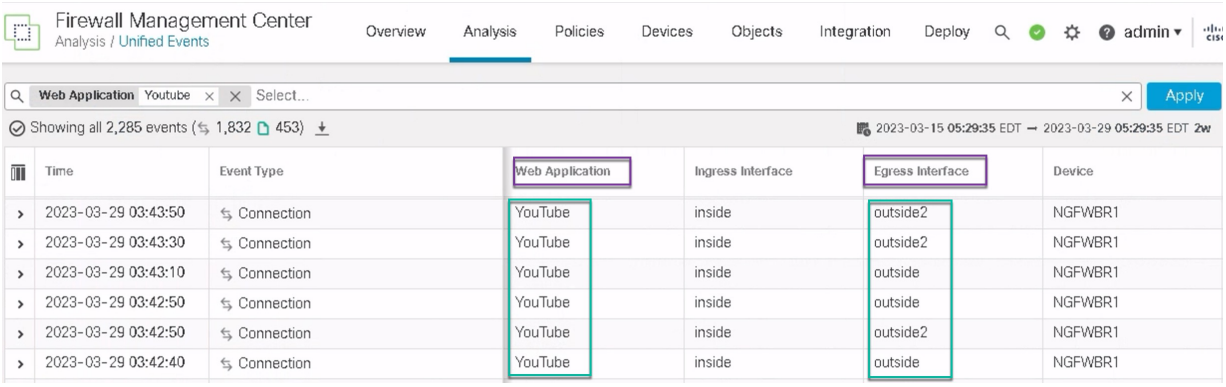
步骤 7 在管理中心中，验证两个应用的流量。

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。

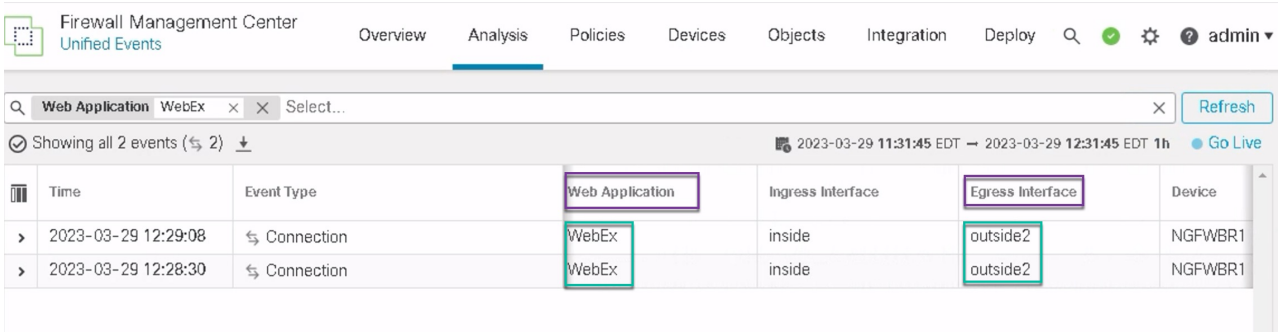


   - **YouTube** 应用流量按照下图所示的配置在 **outside** 和 **outside2** 接口之间进行负载均衡。



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。

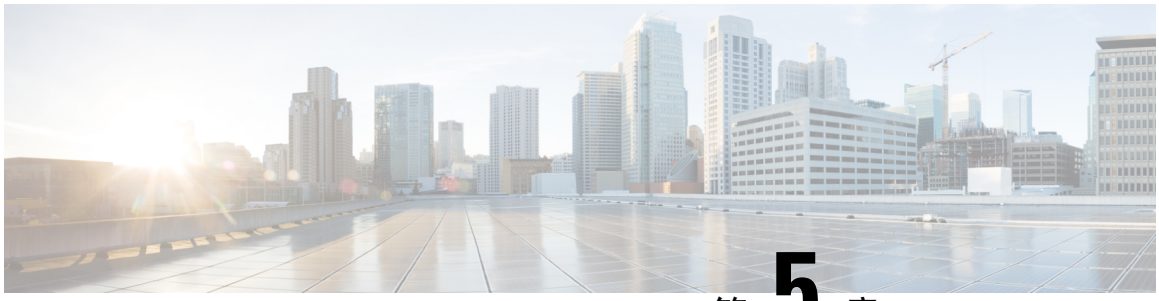
要停止调试过程，请使用以下命令：

```
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



第 5 章

使用 Umbrella 自动隧道保护互联网流量

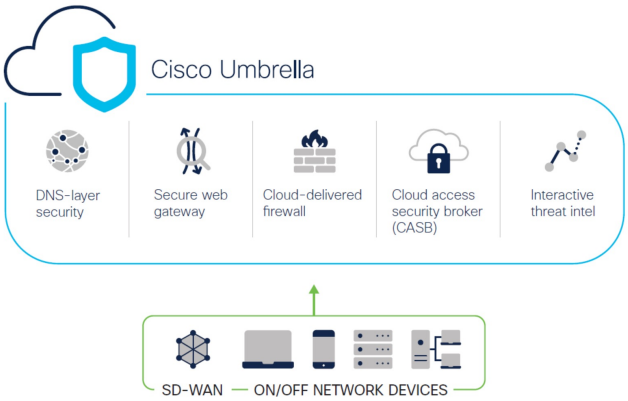
在本章中，我们将深入探讨 Umbrella 自动隧道的实际应用。该使用案例详细介绍了场景、网络拓扑、最佳实践和前提条件。它还为无缝实施提供了全面的端到端程序。

- Cisco Umbrella 自动隧道 ， 第 67 页
- 优势， 第 68 页
- 此使用案例适合您吗？ ， 第 69 页
- 场景， 第 69 页
- 网络拓扑， 第 69 页
- SASE Umbrella 隧道的最佳实践， 第 71 页
- **配置 Umbrella SASE 隧道的前提条件**， 第 71 页
- 配置 Umbrella 自动隧道的端到端程序， 第 72 页
- 为 Umbrella 配置 SASE 隧道， 第 73 页
- 配置静态路由， 第 76 页
- 为 DNS 和 Web 流量配置扩展 ACL， 第 77 页
- 为 DNS 和 Web 流量配置 PBR 策略 ， 第 78 页
- 部署配置， 第 79 页
- 验证 SASE Umbrella 隧道部署， 第 79 页
- Umbrella 自动隧道故障排除 ， 第 84 页
- 其他资源， 第 85 页

Cisco Umbrella 自动隧道

域名系统 (DNS) 是一种经常用于攻击的互联网协议。90% 的恶意软件都会使用 DNS（来源：思科安全研究报告）。然而，许多组织并没有监控 DNS 或使用以 DNS 为重点的安全措施。

图 5: 思科资安防护伞



Cisco Umbrella 是一个基于云的安全互联网网关平台，可提供多层次的互联网威胁防御。Umbrella 集成了 DNS 层安全、云访问安全边界 (CASB) 功能、云交付防火墙和安全 Web 网关，无论分支机构资源如何，都能提供高度可扩展的安全性。在允许或拒绝访问互联网之前，与互联网绑定的流量可以安全地从分支机构自动发送到最近的 Umbrella 点进行检查。

从版本 7.3 开始，Cisco Secure Firewall Management Center 支持 Umbrella 安全互联网网关 (SIG) 集成的自动隧道配置，使网络设备能够将 DNS 和 Web 流量转发到 Umbrella SIG，以便通过 SIG 隧道进行检查和过滤。

在 Cisco Umbrella 中定义的 DNS 和 Web 策略可通过 Cisco Secure Firewall 应用于连接。这使您能够根据请求的域名应用和验证请求。

管理中心提供了一个新的基于向导的简化界面来构建此隧道，从而最大限度地减少防火墙威胁防御和 Cisco Umbrella 上的配置步骤。

管理中心利用 Umbrella API 使用 Cisco Umbrella 连接配置中的参数配置网络隧道。然后，管理中心获取 Umbrella 数据中心列表，并将其显示在用户界面中，以供选择为 SASE 拓扑中的中心。网络隧道部署在威胁防御设备上，并在管理中心完成部署后在 Cisco Umbrella 上自动创建。这有助于为内部用户和漫游用户应用统一的 DNS 和 Web 策略。

优势

使用Cisco Umbrella 保护互联网流量的优势包括：

- 在建立任何连接之前，在DNS层确保用户和应用的安全，从而减少随之而来的数据包处理，加快保护速度。
- 统一 DNS 控制策略适用于混合用户（本地用户和漫游用户）。
- Umbrella 甚至在连接建立之前就能阻止网络请求以及对恶意软件、勒索软件、网络钓鱼和僵尸网络的请求，从而在威胁进入您的网络或终端之前就将其阻止。这会导致您需要补救的感染和警报数量显著减少。
- 无需高级防火墙功能，例如 URL 过滤和 TLS 解密。

- 自动隧道设置只需在管理中心进行最少的配置。
- Umbrella 控制面板上的自动网络隧道配置。

此使用案例适合您吗？

Umbrella SASE 自动隧道配置的目标受众是负责管理和保护企业网络基础设施的 IT 团队、网络管理员和安全专业人员。他们有兴趣探索先进的安全远程访问解决方案，并简化安全隧道的配置和管理。Umbrella SASE 自动隧道配置说明将吸引那些寻求加强网络安全、简化远程连接和改善组织远程员工整体用户体验的人员。

场景

IT 管理员 Alice 负责管理组织的 IT 基础设施并确保其安全。Alice 意识到网络空间的威胁与日俱增，希望采取强有力的安全措施，防止任何潜在的网络攻击，如恶意软件、勒索软件和网络钓鱼。

Sally 是一名在分公司工作的员工，她使用公司的网络访问互联网，从事与工作相关的活动。

有什么风险？

如果没有适当的安全措施，员工可能会在毫不知情的情况下访问恶意网站和下载有害软件，从而危及组织的网络安全和数据隐私。

SIG 集成如何解决问题？

Alice 使用分支机构防火墙和 Cisco Umbrella 实施了双层安全方法。防火墙为网络提供入站安全保护，使其免受基于 Web 和非 Web 的攻击。Umbrella 通过在 DNS 和 Web 层拦截恶意域、IP 和 URL 来提供出站安全性。

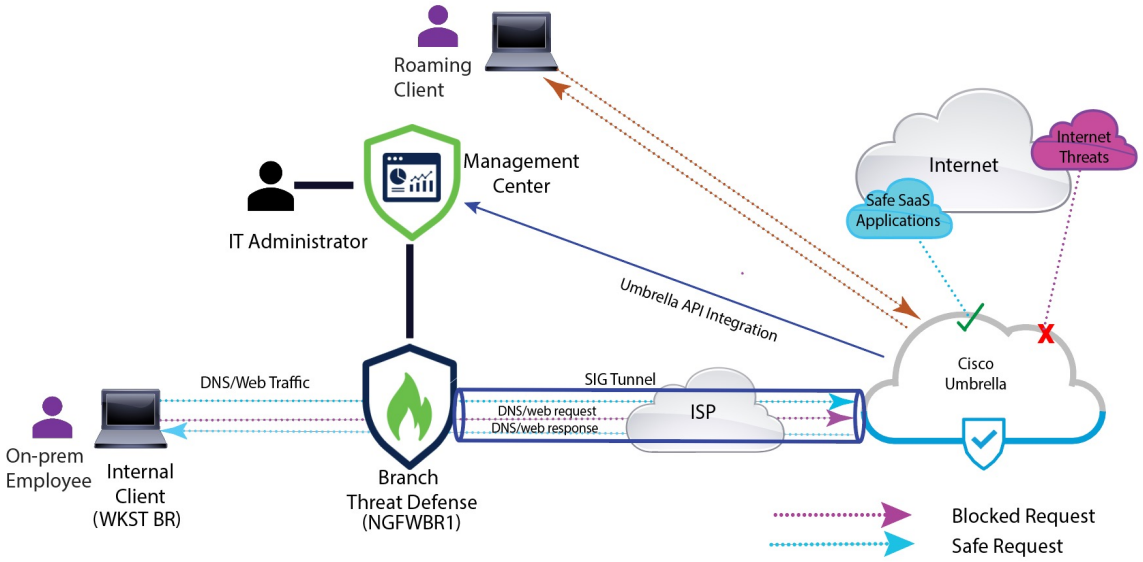
Sally 注意到某些网站现在被防火墙和 Umbrella 阻止了。

企业内部用户和远程用户都不得不在 Umbrella 面板中定义的相同 DNS 和 Web 策略。由于实施了这一解决方案，组织的网络现在更加安全，并能抵御潜在的网络攻击。

网络拓扑

在这种拓扑结构中，威胁防御设备部署在分支机构。在下图中，内部客户端或分支工机构作站被标为 WKST BR，分支机构威胁防御被标为 NGFWBR1。在 NGFWBR1 和 Cisco Umbrella 之间配置了 SIG 自动隧道。

图 *6:* 用于 ***Umbrella*** 自动隧道配置的网络拓扑



所有 DNS 和网络流量都将通过 SIG 隧道发送到 Cisco Umbrella，根据 Umbrella DNS 和网络策略进行验证、允许或阻止。这提供了两层保护，一层由 Cisco Secure Threat Defense 在本地实施，另一层由 Cisco Umbrella 在云端提供。

对于 DNS 流量：

1. 如果 Cisco Umbrella 检测到未分类的域的 DNS 请求，它将查询该域的信誉。
2. 如果域被分类为恶意域，DNS 请求就会被阻止，最终用户就无法访问该网站。
3. 如果域被分类为安全域，DNS 请求就会被解析，最终用户可以访问该网站。

SASE Umbrella 隧道的最佳实践

- 确保在管理中心启用具有出口控制功能的基本许可证。
- 建议将面向互联网的威胁防御接口命名为 **outside** 或以其为前缀。
- 如果 SASE 拓扑的 Umbrella 部署正在运行，请勿编辑或删除该拓扑。
- 要配置备份 Umbrella DC，请使用备份 Umbrella DC 复制具有相同威胁防御终端的相同拓扑。
- 要在威胁防御终端上配置备份接口，请在备份接口上使用 VTI 复制具有相同 Umbrella DC 的相同拓扑。

配置 Umbrella SASE 隧道的前提条件

- 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
- 您必须拥有 Cisco Umbrella 安全互联网网关 (SIG) 基础版订用或 SIG 免费试用版。
- 您必须启用具有出口控制功能的智能许可证帐户，才能从管理中心在 Umbrella 上部署隧道。
- 通过 http://login.umbrella.com Umbrella，获取与 Cisco Umbrella 建立连接所需的信息。确保管理中心可以访问 management.api.umbrella.com。
- 您必须在管理中心注册 Cisco Umbrella 组织，并在 Cisco Umbrella 连接高级设置中配置管理密钥和管理秘密。这将从 Cisco Umbrella 云获取数据中心详细信息。您还必须在思科 Umbrella 连接常规设置中配置组织 ID、网络设备密钥、网络设备密钥和旧版网络设备令牌。

  有关详情，请参阅：

  - 配置 Cisco Umbrella 连接设置
  - 映射管理中心 Umbrella 参数和 Cisco Umbrella API 密钥
- 确保可从威胁防御访问 Umbrella 数据中心。
- 确保威胁防御系统支持基于路由的 VPN，并支持本地隧道 ID（7.1.0 及更高版本）。您可以在管理中心 7.3.0 及更高版本中部署支持本地隧道 ID 的 SASE 隧道。

SASE Umbrella 隧道的最佳实践

- 确保在管理中心启用具有出口控制功能的基本许可证。
- 建议将面向互联网的威胁防御接口命名为 **outside** 或以其为前缀。
- 如果 SASE 拓扑的 Umbrella 部署正在运行，请勿编辑或删除该拓扑。
- 要配置备份 Umbrella DC，请使用备份 Umbrella DC 复制具有相同威胁防御终端的相同拓扑。
- 要在威胁防御终端上配置备份接口，请在备份接口上使用 VTI 复制具有相同 Umbrella DC 的相同拓扑。

配置 Umbrella SASE 隧道的前提条件

- 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

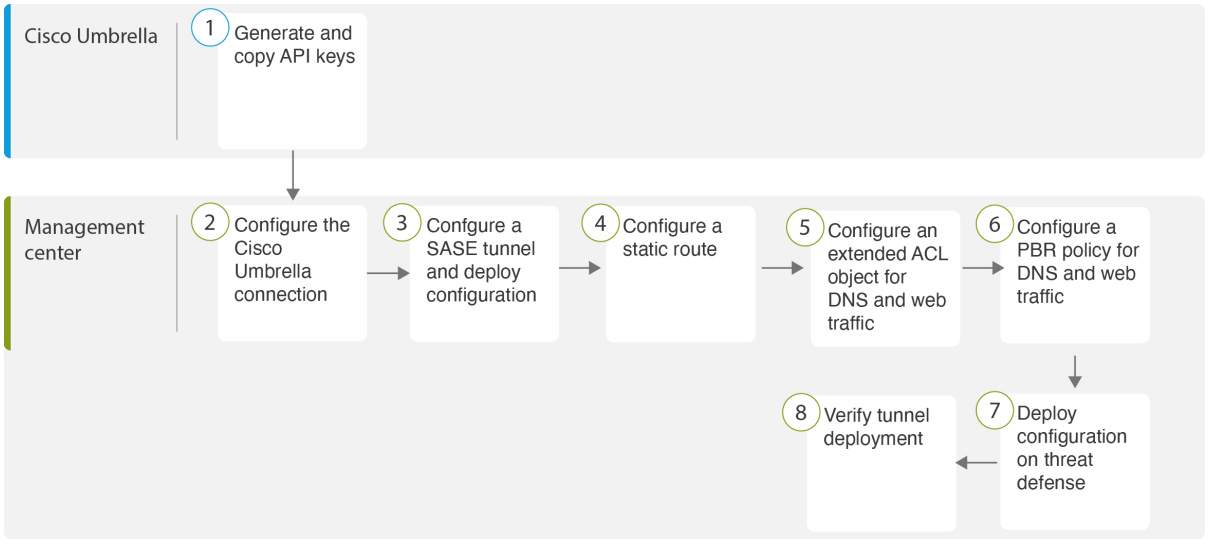
- 创建基本访问控制策略
- 您必须拥有 Cisco Umbrella 安全互联网网关 (SIG) 基础版订用或 SIG 免费试用版。
- 您必须启用具有出口控制功能的智能许可证帐户，才能从管理中心在 Umbrella 上部署隧道。
- 通过 http://login.umbrella.com Umbrella，获取与 Cisco Umbrella 建立连接所需的信息。确保管理中心可以访问 management.api.umbrella.com。
- 您必须在管理中心注册 Cisco Umbrella 组织，并在 Cisco Umbrella 连接高级设置中配置管理密钥和管理秘密。这将从 Cisco Umbrella 云获取数据中心详细信息。您还必须在思科 Umbrella 连接常规设置中配置组织 ID、网络设备密钥、网络设备密钥和旧版网络设备令牌。

  有关详情，请参阅：

  - 配置 Cisco Umbrella 连接设置
  - 映射管理中心 Umbrella 参数和 Cisco Umbrella API 密钥
- 确保可从威胁防御访问 Umbrella 数据中心。
- 确保威胁防御系统支持基于路由的 VPN，并支持本地隧道 ID（7.1.0 及更高版本）。您可以在管理中心 7.3.0 及更高版本中部署支持本地隧道 ID 的 SASE 隧道。

配置 Umbrella 自动隧道的端到端程序

以下流程图说明了在Cisco Secure Firewall Management Center 中配置 SASE 隧道的工作流程。



步骤	说明
1	（前提条件）在 Cisco Umbrella 中生成并复制 API 密钥。请参阅映射管理中心 Umbrella 参数和 Cisco Umbrella API 密钥。

步骤	说明
2	（前提条件）配置 Cisco Umbrella 连接。请参阅配置 Cisco Umbrella 连接设置。
3	创建 SASE 隧道并在威胁防御上部署配置。请参阅 为 Umbrella 配置 SASE 隧道，第 73 页。
4	配置静态路由。请参阅 配置静态路由，第 76 页。
5	为 DNS 和 Web 流量配置扩展 ACL 对象。请参阅 为 DNS 和 Web 流量配置扩展 ACL，第 77 页
6	为 DNS 和 Web 流量配置 PBR 策略。请参阅 为 DNS 和 Web 流量配置 PBR 策略 ，第 78 页
7	在威胁防御上部署配置。请参阅 部署配置，第 21 页。
8	验证隧道部署。请参阅验证 SASE Umbrella 隧道部署，第 79 页。

为 Umbrella 配置 SASE 隧道

开始之前

确保您查看 配置 Umbrella SASE 隧道的前提条件，第 70 页 和 SASE Umbrella 隧道的最佳实践，第 70 页。

步骤 1 登录到管理中心，选择**设备 (Devices) > VPN > 站点间 (Site To Site)**。

步骤 2 点击 **+ SASE 拓扑 (+ SASE Topology)** 以打开 SASE 拓扑向导。

步骤 3 输入唯一的**拓扑名称 (Topology Name)** 在我们的示例中，输入 **VPN-Mumbrella**。

步骤 4 **预共享密钥 (Pre-shared Key)**：此密钥会根据 Umbrella PSK 要求自动生成。

设备和 Cisco Umbrella 分享此密钥，IKEv2 将其用于身份验证。您可以覆盖自动生成的密钥。如果配置此密钥，长度必须介于 16 到 64 个字符之间，至少包含一个大写字母、一个小写字母和一个数字，并且不包含特殊字符。每个拓扑都必须具有唯一的预共享密钥。如果拓扑有多个隧道，则所有隧道都具有相同的预共享密钥。

步骤 5 从 **Umbrella 数据中心 (Umbrella Data center)** 下拉列表中选择数据中心。保护伞数据中心会自动填充区域和 IP 地址。

步骤 6 点击**添加 (Add)**，将威胁防御节点添加为 SASE 拓扑中的终端。

a) 从**设备 (Device)** 下拉列表中选择威胁防御设备 (**NGFWBR1**)。

b) 从 **VPN 接口 (VPN Interface)** 下拉列表选择静态 VTI 接口。

要创建新的静态 VTI 接口（例如 **Outside_static_vti_1**），请点击 **+**。系统将显示 **添加虚拟隧道接口** 对话框，其中包含预填充的默认配置。

- 默认情况下，隧道类型设置为**静态 (Static)**。
- 名称为 <*tunnel_source interface logical name*>+ static_vti +<*tunnel ID*>. 例如，Outside_static_vti_1。
- 默认情况下，隧道已被设为**启用 (Enabled)**。
- 默认情况下，安全区域已被配置为**外部 (Outside)**。
- 隧道 ID 会自动填充一个唯一 ID。
- 隧道源接口会自动填充一个带有“外部”前缀的接口。

  注释 确保隧道源设置为 **GigabitEthernet0/0**

  注释 您也可以将隧道源接口设置为不同的接口。

- 默认情况下，IPsec 隧道模式为 IPv4。
- 未使用的 IP 地址在 169.254.xx/30 专用 IP 地址范围内选取。在我们的示例中，选择了 **169.254.2.1/30**。

  注释 使用 /30 子网时，只有两个 IP 地址可用。第一个 IP 地址是自动隧道 VTI IP，第二个 IP 地址在配置到 Umbrella DC 的静态路由时用作下一跳 IP。在我们的示例中，169.254.2.1 是 VTI IP，169.254.2.2 用于静态路由。请参阅配置静态路由，第 76 页。

- 点击**确定 (OK)**。

从“VPN 接口”(VPN Interface) 下拉列表选择 **outside_static_vti_1**。

c) 在**本地隧道 ID (Local Tunnel ID)** 字段中输入本地隧道 ID 的前缀。

前缀最少包含 8 个字符，最多包含 100 个字符。管理中心在 Umbrella 上部署隧道后，Umbrella 会生成完整的隧道 ID (<*prefix*>@<*umbrella-generated-ID*>-umbrella.com) 。然后，管理中心会检索并更新完整的隧道 ID，并将其部署在威胁防御设备上。每个隧道都有唯一的本地隧道 ID。

d) 点击**保存 (Save)** 以将终端设备添加到拓扑。

步骤 7 点击**下一步 (Next)** 以查看 Umbrella SASE 隧道配置摘要。

- **终端 (Endpoints)** 窗格：显示已配置威胁防御终端的摘要。
- **加密设置 (Encryption Settings)** 窗格：显示 SASE 隧道的加密设置。

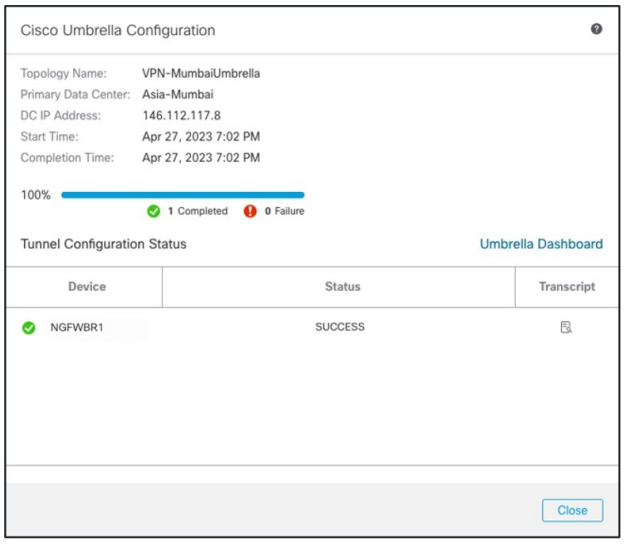
步骤 8 选中**在威胁防御节点上部署配置 (Deploy configuration on threat defense nodes)** 复选框，以触发将网络隧道部署到威胁防御。此部署只会在将隧道部署到 Umbrella 之后进行。威胁防御部署需要本地隧道 ID。

步骤 9 点击**保存 (Save)**。

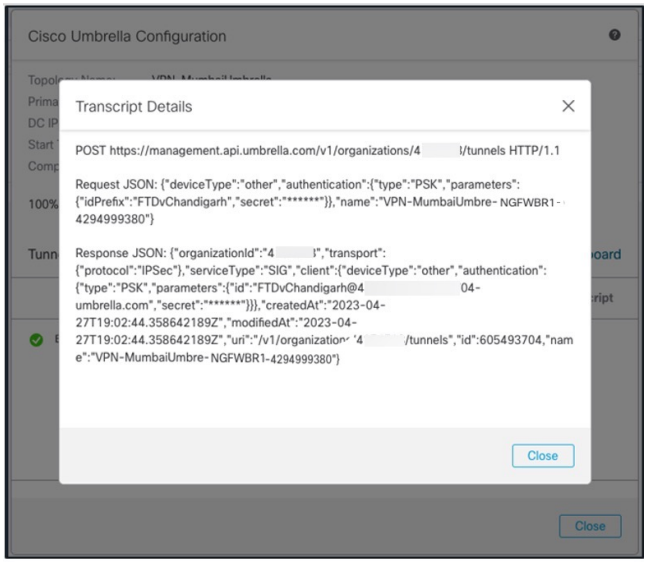
此操作：

1. 在管理中心保存 SASE 拓扑。
2. 为每个威胁防御终端触发部署到 Umbrella 的网络隧道。
3. 如果启用此选项，则会触发将网络隧道部署到威胁防御设备。此操作会提交并部署自上次在设备上部署以来更新的所有配置和策略，包括非 VPN 策略。

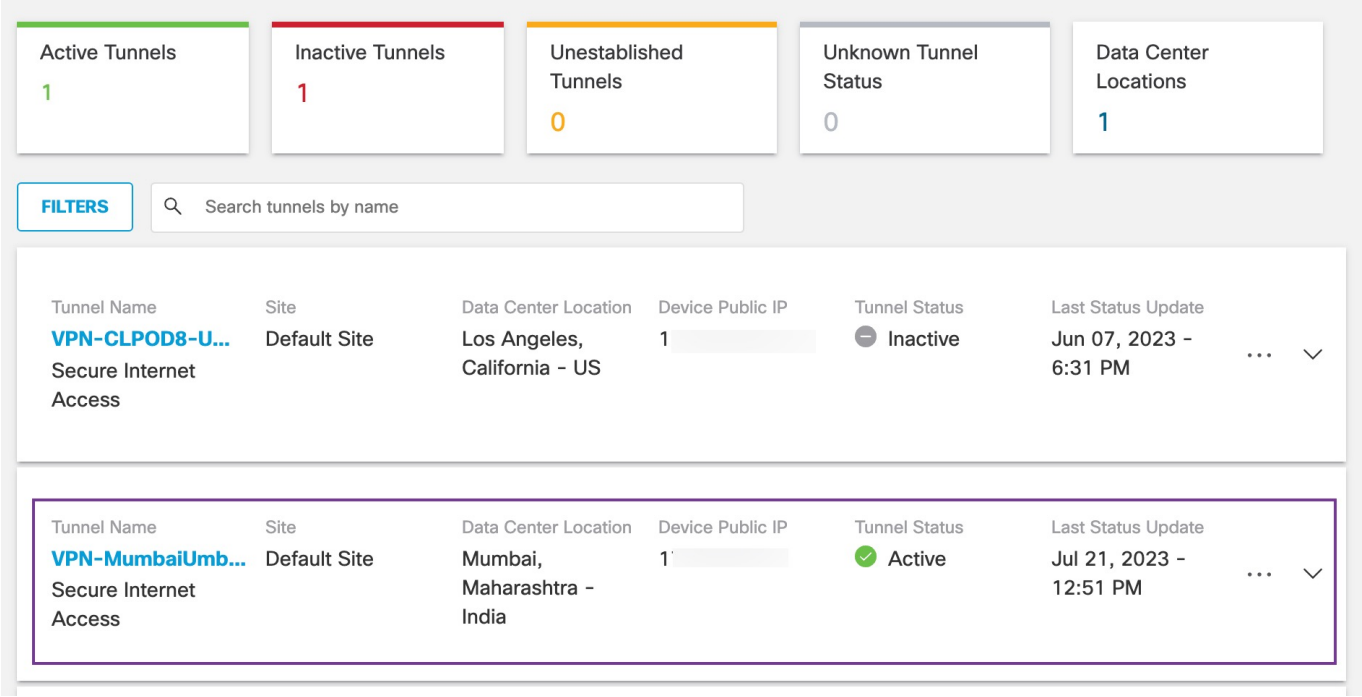
4. 打开 **Cisco Umbrella 配置 (Cisco Umbrella Configuration)** 窗口并显示 Umbrella 上的隧道部署状态。



要查看部署详情，请点击**脚本 (Transcript)** 按钮以查看脚本详情，如 API、请求负载和从 Umbrella 收到的响应。



点击 **Umbrella 控制面板 (Umbrella Dashboard)** 链接，查看 Umbrella 中的“网络隧道”(Network Tunnels) 页面。



下一步做什么

对于要通过 SASE 隧道的流量，请使用特定匹配条件配置 PBR 策略，以通过 VTI 发送流量。

配置静态路由

您必须配置从自动隧道到 Umbrella DC 的静态路由。

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 点击**静态路由 (Static Route)**。

步骤 4 点击**添加路由 (Add Route)** 以添加新路由。

步骤 5 从**接口 (Interface)** 下拉列表中选择 **outside_static_vti_1** 作为接口。

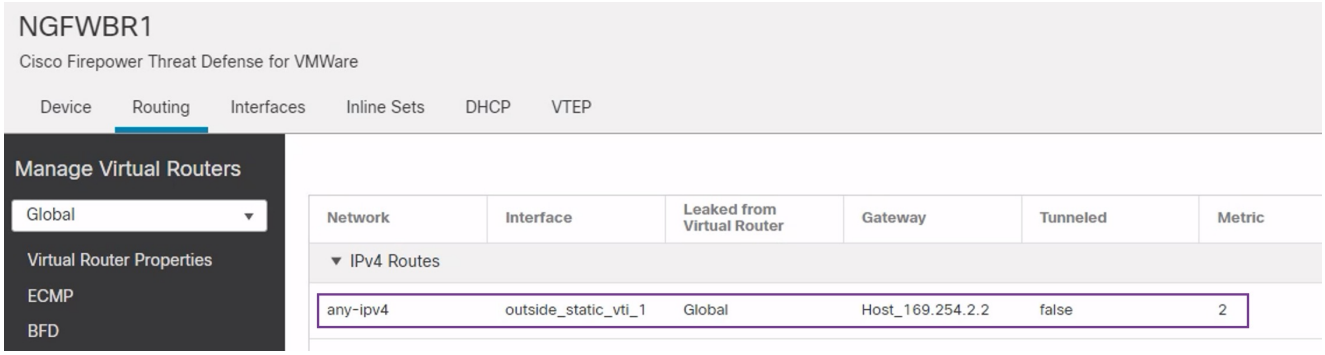
步骤 6 从**可用网络 (Available Networks)** 框中选择 **any-ipv4** 作为目标网络，然后点击**添加 (Add)**。

步骤 7 输入网络的网关。在本例中，输入 **169.254.2.2**。

步骤 8 输入指标值。它可以是介于 1 和 254 之间的数字。在本例中，输入值 2。

步骤 9 要保存设置，点击**保存 (Save)**。

如下图所示创建静态路由。



为 DNS 和 Web 流量配置扩展 ACL

在策略型路由选择功能的帮助下，访问列表被配置为将DNS和网络流量从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 (**LAN_to_Internet**)。

步骤 4 点击**添加 (Add)** 以创建新的扩展访问列表。

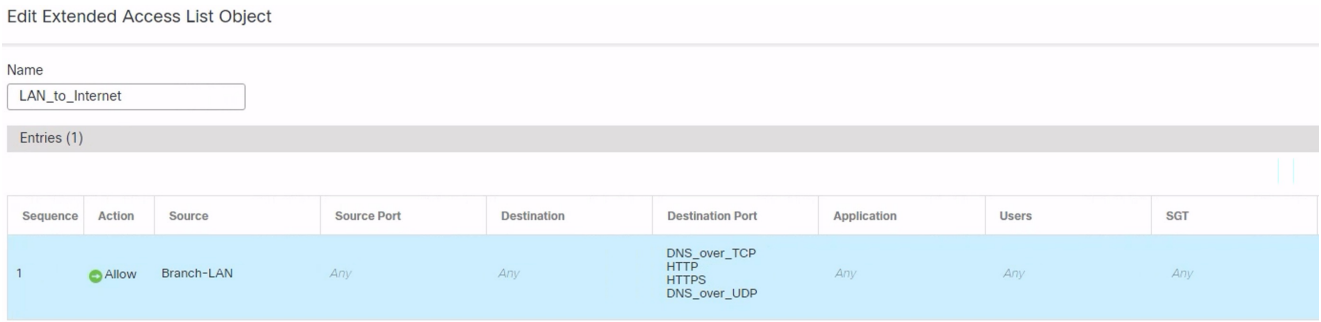
步骤 5 配置以下访问控制属性：

1. 选择**操作 (Action)** 以允许（匹配）流量标准。
2. 点击**端口 (Port)** 选项卡，然后在**可用端口 (Available Ports)** 列表中搜索 **HTTP**、**HTTPS**、**DNS_over_UDP**、**DNS_over_TCP**。
3. 选择端口，然后点击**添加到目标 (Add to Destination)**。
4. 点击**网络 (Network)** 选项卡，然后在**可用网络 (Available Networks)** 列表中搜索分支机构 LAN。

   注释　　在我们的示例中，网络为 **Branch-LAN**。

5. 选择 **Branch-LAN**，然后点击**添加到源 (Add to Source)**。
6. 点击**添加 (Add)** 以将条目添加到对象。
7. 点击**保存 (Save)**。

如下图所示创建 ACL 对象。



为 DNS 和 Web 流量配置 PBR 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DNS和网络流量的出口接口，在“策略型路由”(Policy Based Routing) 页面中配置 PBR 策略。

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 在**添加策略型路由 (Add Policy Based Route)** 对话框中，从下拉列表中选择**入口接口 (Ingress Interface)**。

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 **LAN_to_Internet**。

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)**。

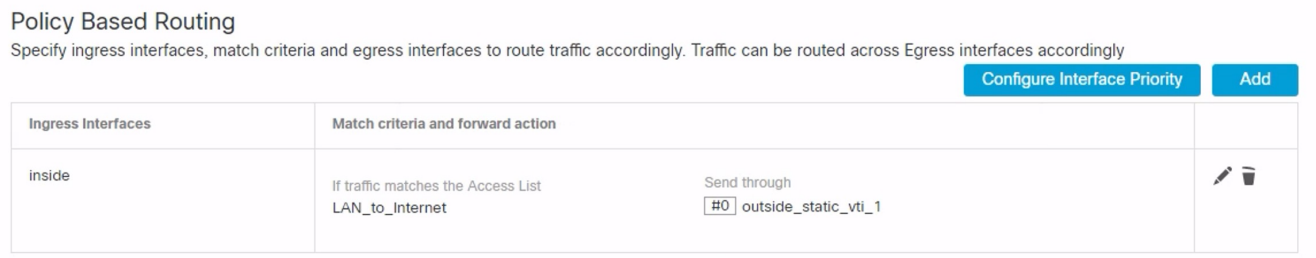
c) 在**可用接口 (Available Interfaces)** 中，点击 **Outside_static_vti_1** 接口旁边的 **添加**（➕） 图标，将其移至**所选出口接口**。

d) 点击**保存 (Save)** 以写入匹配条件的更改。

e) 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)**。

如下图所示创建 PBR 策略。



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)**。这样将显示已准备好部署的设备列表。

步骤 2 选中要部署配置更改的 NGFWBR1 和 NGFW1 旁边的复选框。

步骤 3 点击**部署 (Deploy)**。等待部署在“部署”(Deploy) 对话框中标记为“已完成”(Completed)。

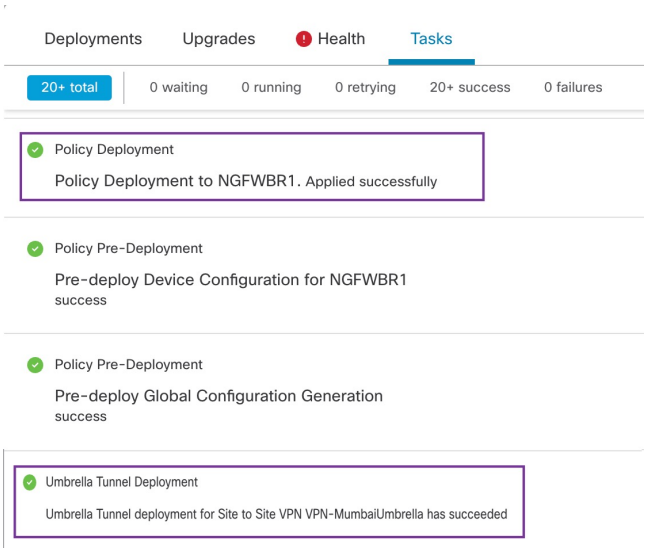
步骤 4 如果系统在要部署的更改中发现错误或警告，则会在**验证错误 (Validation Errors)** 或**验证警告 (Validation Warnings)** 窗口中显示它们。要查看完整的详细信息，请点击“验证错误”(Validation Errors) 或“验证警告”(Validation Warnings) 链接。

有以下选项可供选择：

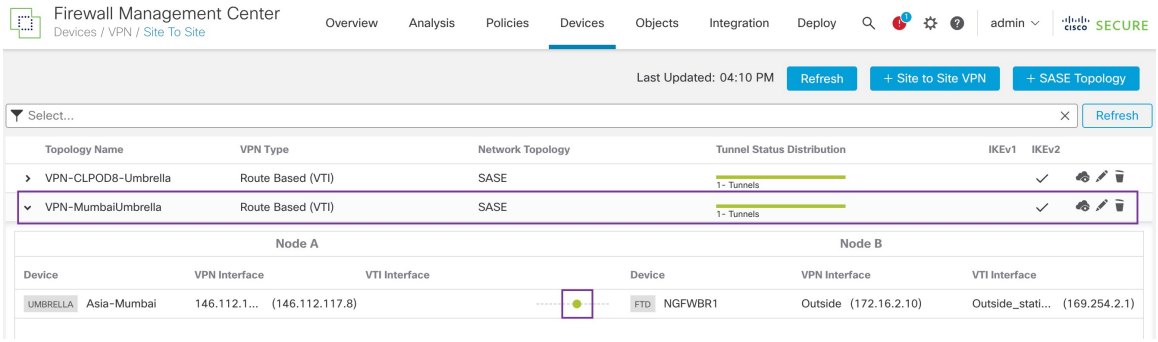
- 继续部署 - 继续部署而无需解决警告情况。如果系统识别错误，则无法继续。
- 关闭 - 退出而不部署。解决错误和警告情况，并尝试重新部署该配置。

验证 SASE Umbrella 隧道部署

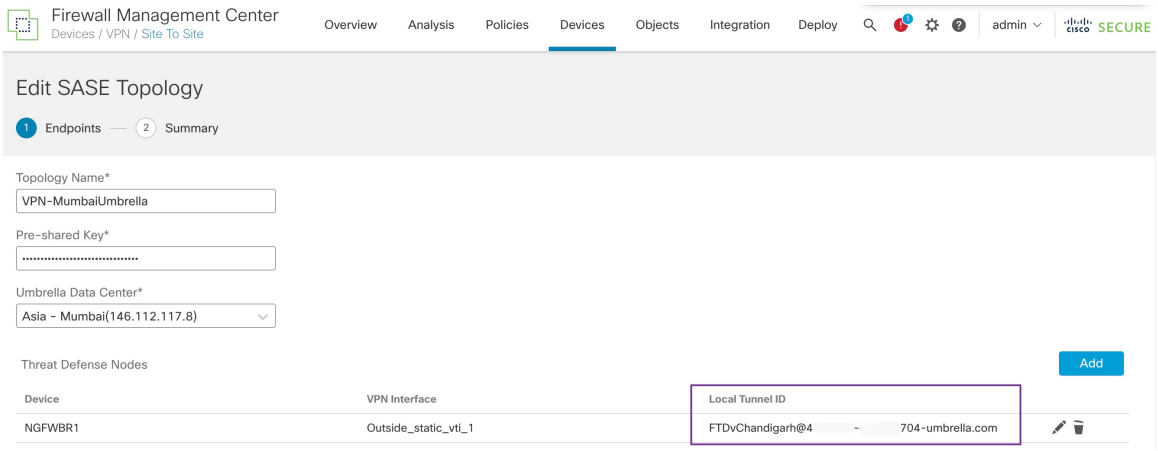
在管理中心，转至**通知 (Notifications)** > **任务 (Tasks)**，查看威胁防御设备 (NGFWBR1) 上的 Umbrella 隧道部署和策略部署状态。



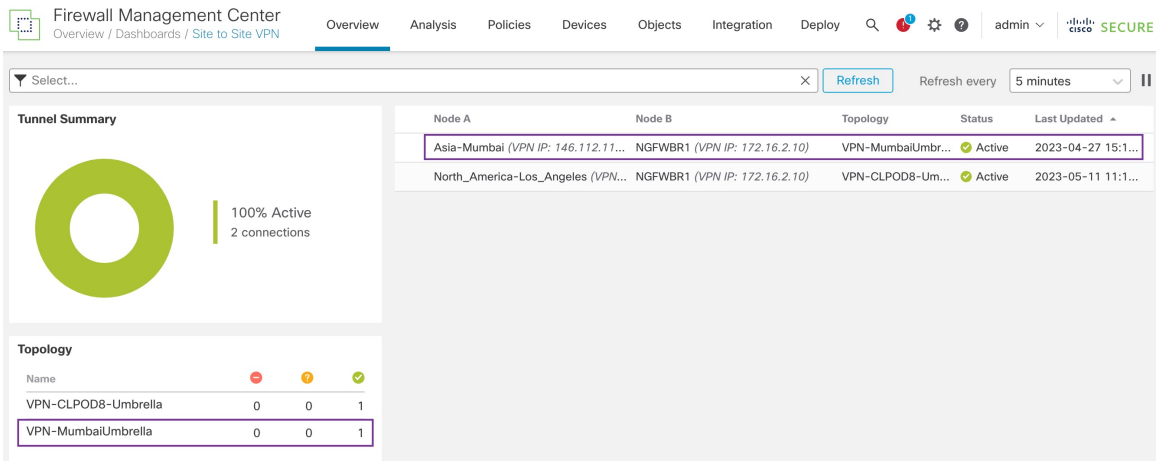
要在管理中心检查 SASE 自动隧道状态，请选择**设备 (Devices) > VPN > 站点间 (Site To Site)**。



要在管理中心检查更新的 SASE 拓扑，请选择**设备 (Devices) > VPN > 站点间 (Site To Site) > 编辑 SASE 拓扑 (Edit SASE Topology)**。本地隧道 ID 会在部署到 Umbrella 后更新。



要在管理中心查看站点间 VPN 控制面板，请选择**概述 (Overview) > 控制面板 (Dashboard) > 站点间 VPN (Site to Site VPN)**。



使用以下 CLI 命令来验证威胁防御中的 SASE Umbrella 隧道：

- 要验证 SASE 隧道的详细信息，请使用以下命令：

```
> show running-config interface tunnel 1
!
interface Tunnel1
 nameif Outside_static_vti_1
 ip address 169.254.2.1 255.255.255.252
 tunnel source interface Outside
 tunnel destination 146.112.117.8
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

- 要验证 IPSec 配置文件和关联的提议，请使用以下命令：

```
> show running-config crypto ipsec
crypto ipsec ikev2 ipsec-proposal CSM_IP_1
 protocol esp encryption aes-gcm-256
 protocol esp integrity sha-256
crypto ipsec profile FMC_IPSEC_PROFILE_1
 set ikev2 ipsec-proposal CSM_IP_1
 set ikev2 local-identity email-id FTDvChandigarh@41xxxxx-xxxxxxxxx-umbrella.com
 set reverse-route
crypto ipsec security-association pmtu-aging infinite
```

- 要验证 IKEV2 策略集，请使用以下命令：

```
> show running-config crypto ikev2
crypto ikev2 policy 15
 encryption aes-gcm-256
 integrity null
 group 20 19
 prf sha256
 lifetime seconds 86400
crypto ikev2 enable Outside
```

- 要验证隧道统计信息（包括发送和接收数据），请使用以下命令：

```
> show vpn-sessiondb l2l
Session Type: LAN-to-LAN
Connection   : 146.112.117.8
Index        : 19                     IP Addr      : 146.112.117.8
Protocol     : IKEv2 IPsecOverNatT
Encryption   : IKEv2: (1)AES-GCM-256  IPsecOverNatT: (1)AES-GCM-256
Hashing      : IKEv2: (1)none  IPsecOverNatT: (1)none
Bytes Tx     : 234                      Bytes Rx     : 446
Login Time   : 19:14:51 UTC Thu Apr 27 2023
Duration     : 0h:55m:16s
Tunnel Zone  : 0
```

- 要检查隧道状态，请使用以下命令：

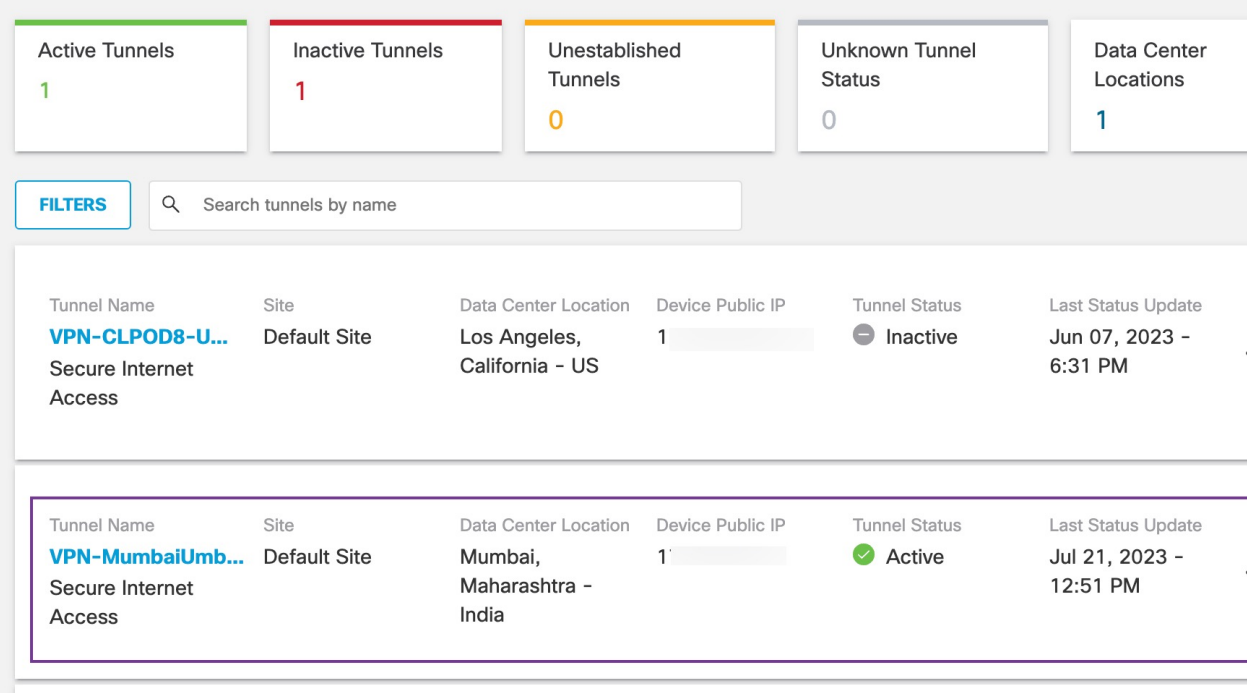
```
> show interface ip brief

Interface                  IP-Address      OK? Method Status                Protocol
Internal-Control0/0        127.0.1.1       YES unset  up                    up
Internal-Control0/1        unassigned      YES unset  up                    up
Internal-Data0/0           unassigned      YES unset  down                  up
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           169.254.1.1     YES unset  up                    up
Internal-Data0/2           unassigned      YES unset  up                    up
Management0/0              203.0.113.130   YES unset  up                    up
TenGigabitEthernet0/0      172.16.2.10     YES manual up                    up
TenGigabitEthernet0/1      172.16.3.10     YES manual up                    up
TenGigabitEthernet0/2      unassigned      YES unset  administratively down up
Tunnel1                    169.254.2.1     YES manual up                    up
```

- 要检查与 VTI 隧道关联的 IPSec SA，请使用以下命令：

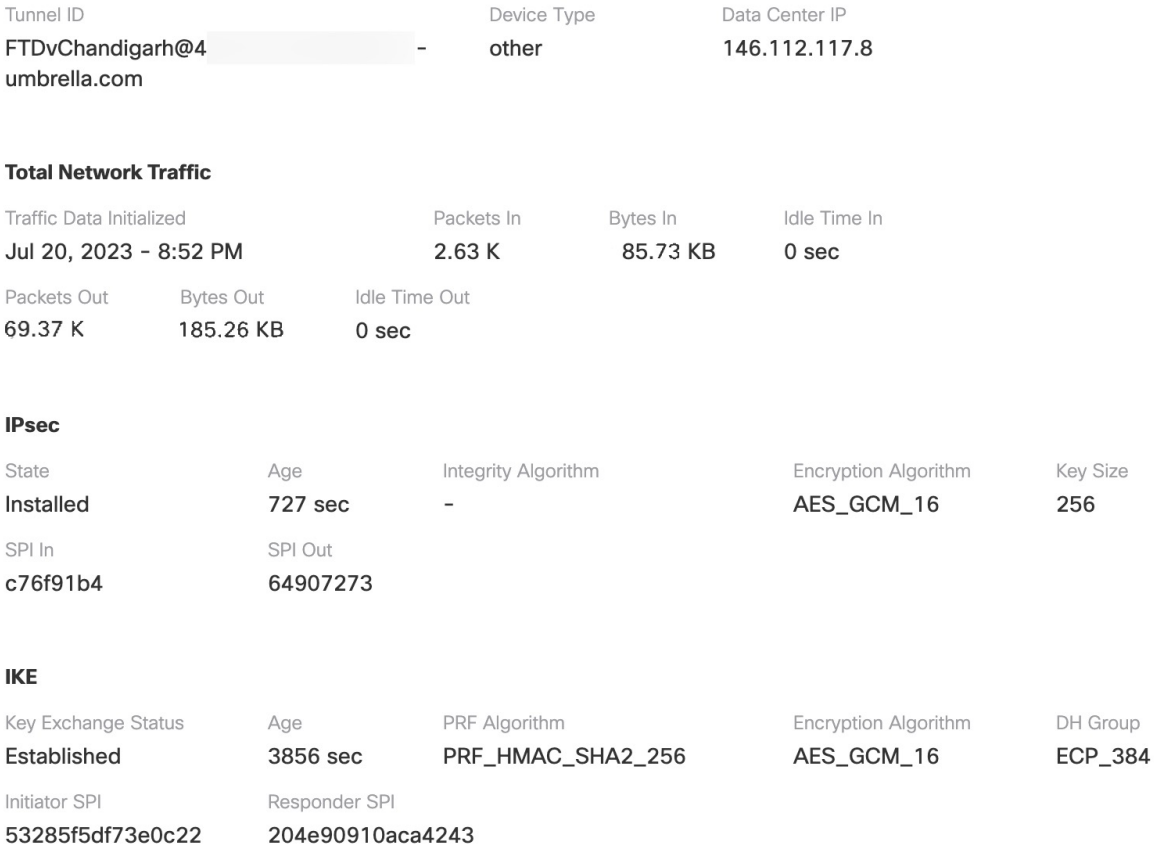
```
> show crypto ipsec sa
interface: outside_static_vti_1
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr:
198.18.128.81

      Protected vrf (ivrf): Global
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer: 146.112.117.8


      #pkts encaps: 705, #pkts encrypt: 705, #pkts digest: 705
      #pkts decaps: 743, #pkts decrypt: 743, #pkts verify: 743
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 705, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

     local crypto endpt.: 198.18.128.81/4500, remote crypto endpt.: 146.112.117.8/4500

      path mtu 1500, ipsec overhead 63(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: C76F91B4
      current inbound spi : 64907273
```

```
inbound esp sas:
  spi: 0x2BF92601 (737748481)
     SA State: active
     transform: esp-aes-gcm-256 esp-null-hmac no compression
     in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, VTI, }
     slot: 0, conn_id: 32, crypto-map: __vti-crypto-map-Tunnel1-0-1
     sa timing: remaining key lifetime (kB/sec): (4331520/27987)
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0x00000000 0x00000001
outbound esp sas:
  spi: 0xCA2DC006 (3391995910)
     SA State: active
     transform: esp-aes-gcm-256 esp-null-hmac no compression
     in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, VTI, }
     slot: 0, conn_id: 32, crypto-map: __vti-crypto-map-Tunnel1-0-1
     sa timing: remaining key lifetime (kB/sec): (4101072/27987)
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0x00000000 0x00000001
```

要在 Umbrella 中查看 SASE 隧道，请登录 Cisco Umbrella 并导航至**部署 (Deployments)** > **核心身份 (Core Identities)** > **网络隧道 (Network Tunnels)**。从威胁防御到 Umbrella 的网络隧道如下图所示。



展开该部分以查看隧道的详细信息。



Umbrella 自动隧道故障排除

在部署后，使用以下 CLI 调试与 Cisco Secure Firewall Threat Defense 上 Umbrella 自动隧道相关的问题。

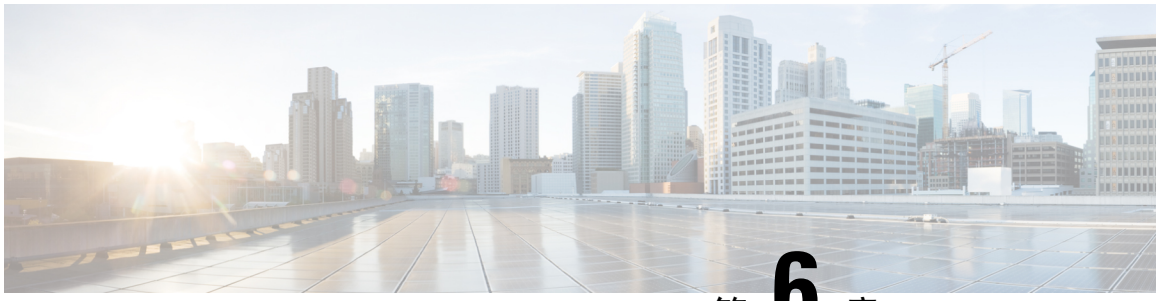
注释 在生产环境中，在威胁防御设备上运行调试命令时要小心谨慎。您可以在设备上设置各种调试级别，这些级别可能会有冗长的输出。

如何...	CLI 命令
为特定对等体启用条件调试	**调试加密条件对等体 <peer-IP>**
调试虚拟隧道接口信息	**debug vti 255**
调试 IKEv2 协议相关事务	**debug crypto ikev2 protocol 255**
调试 IKEv2 平台相关事务	**debug crypto ikev2 platform 255**

如何...	CLI 命令
调试常见的 IKE 相关事务	**debug crypto ike-common 255**
调试 IPSec 相关事务	**debug crypto ipsec 255**

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



第 6 章

为远程员工提供安全连接：使用中的 DIA、Umbrella 自动隧道和 DVTI

在本章中，我们将深入研究 DIA、Umbrella 自动隧道和 DVTI 的实际应用。使用案例详细介绍了场景、网络拓扑和无缝实施的端到端程序。

- 通过 DIA、Umbrella SASE 自动隧道和 DVTI 增强远程员工的连接性和安全性，第 87 页
- 此使用案例适合您吗？，第 87 页
- 场景，第 88 页
- 拓扑，第 88 页
- 配置 DIA、Umbrella 自动隧道和 DVTI 的端到端程序，第 89 页
- 其他资源，第 89 页

通过 DIA、Umbrella SASE 自动隧道和 DVTI 增强远程员工的连接性和安全性

在当今的互联远程办公环境中，企业面临着为其分散的员工提供无缝连接、安全访问和优化性能的挑战。本使用案例探讨了 DIA（直接互联网接入）、Umbrella SASE 自动隧道和 DVTI（动态虚拟隧道接口）技术的实施，以克服网络连接问题，加强协作，保护敏感信息，并让远程用户能够在任何地点都高效地工作。

此使用案例适合您吗？

本使用案例的目标受众是负责管理和保护网络基础设施的 IT 专业人员、网络管理员和决策者，以及希望优化远程员工连接性和安全性的组织。它深入分析了 DIA、Umbrella SASE 自动隧道和 DVTI 技术的实施情况，并重点介绍了这些技术在应对远程员工所面临的挑战方面的优势。

场景

Sally 是一家全球性公司的远程销售代表，该公司非常依赖实时协作和数据访问。她经常出差到不同的客户所在地，但在获取销售数据和与同事沟通方面面临挑战。

有什么风险？

公司现有的网络基础设施无法在多个地点提供无缝连接和安全访问，从而导致延迟、数据不一致和通信中断。

由 DIA、Umbrella 自动隧道和 DVTI 组成的中心辐射型拓扑如何解决问题？

为了应对像 Sally 这样的远程员工所面临的挑战，她的公司使用 DIA、Umbrella SASE 自动隧道和 DVTI 实施了一套全面的解决方案。

1. **DIA**：DIA 让 Sally 能够直接连接到互联网，而无需通过企业网络进行路由。这为她提供了更快、更可靠的互联网接入，让她能够快速访问基于云的应用和服务。它可以从企业网络中分流网络流量，从而减少拥塞并优化性能。
2. **Umbrella 自动隧道**：通过利用 Umbrella 自动隧道配置，无论 Sally 是远程连接还是在分支防火墙后面，Sally 的公司都能确保对流量应用统一的安全策略。它消除了手动配置 VPN 连接的需要，同时也降低了与传统隧道设置相关的复杂性和潜在错误。此技术为 Sally 和组织中的其他远程员工提供简单、方便和更高的安全性
3. **DVTI**：中心辐射型拓扑中的 DVTI 可以在分支机构和企业网络之间动态创建安全的 IPsec 隧道。这些隧道会对数据传输进行加密，确保远程办公时安全访问企业资源。DVTI 还能通过最有效的路径智能路由流量，并提供冗余以实现不间断连接，从而优化网络性能。

通过将 DIA、Umbrella SASE 自动隧道和 DVTI 相结合，Sally 的公司增强了她作为远程员工的连接性、安全性和工作效率。无论身处何地，她都能快速访问云应用，与同事无缝协作，并享受与企业资源安全可靠的连接。集中化的安全管理、网络复杂性的降低以及远程员工活动可视性的提高，都让 IT 团队受益匪浅。

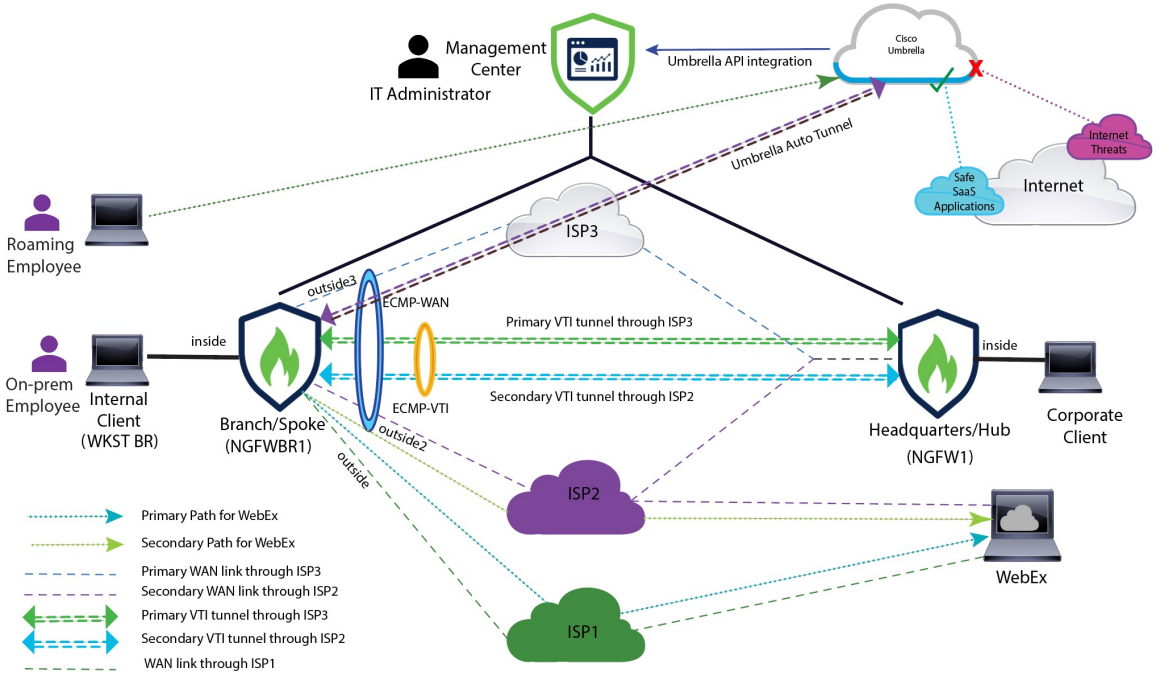
拓扑

在此拓扑中，内部客户端或分支机构工作站被标记为 WKST BR，它与标记为 NGFWBR1 的分支机构威胁防御系统相连。总部威胁防御系统被标记为 NGFW1。企业网络可通过 NGFW1 接入。NGFWBR1 的入口接口命名为 inside，出口接口分别命名为 outside、outside2 和 outside3。

在 NGFWBR1 和 Cisco Umbrella 之间配置了 Umbrella 自动隧道。

所有 DNS 和网络流量都将通过 Umbrella 自动隧道发送到 Cisco Umbrella，根据 Umbrella DNS 和网络策略进行允许或阻止。这提供了两层保护，一层由 Cisco Secure Threat Defense 在本地实施，另一层由 Cisco Umbrella 在云端提供。

对于中心辐射型配置，在 NGFWBR1 和 NGFW1 之间配置了一个 VPN 通道。在分支节点的主要和辅助静态 VTI 接口上配置 ECMP 区域，以实现 VPN 流量的链路冗余和负载平衡。



配置 DIA、Umbrella 自动隧道和 DVTI 的端到端程序

要使用 DIA、Umbrella SASE 自动隧道和 DVTI 配置解决方案，请执行以下操作：

- **配置直接互联网接入：**使用路径监控来配置 DIA 的端到端步骤，第 55 页
- **配置 Umbrella SIG 自动隧道：**配置 Umbrella 自动隧道的端到端程序，第 72 页
- **配置 DVTI 中心辐射型拓扑：**配置基于路由的 VPN 的端到端程序（中心辐射型拓扑），第 9 页

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
YouTube 上的 Secure Firewall 频道	https://www.youtube.com/cisco-netsec

Resource	URL
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。