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

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。

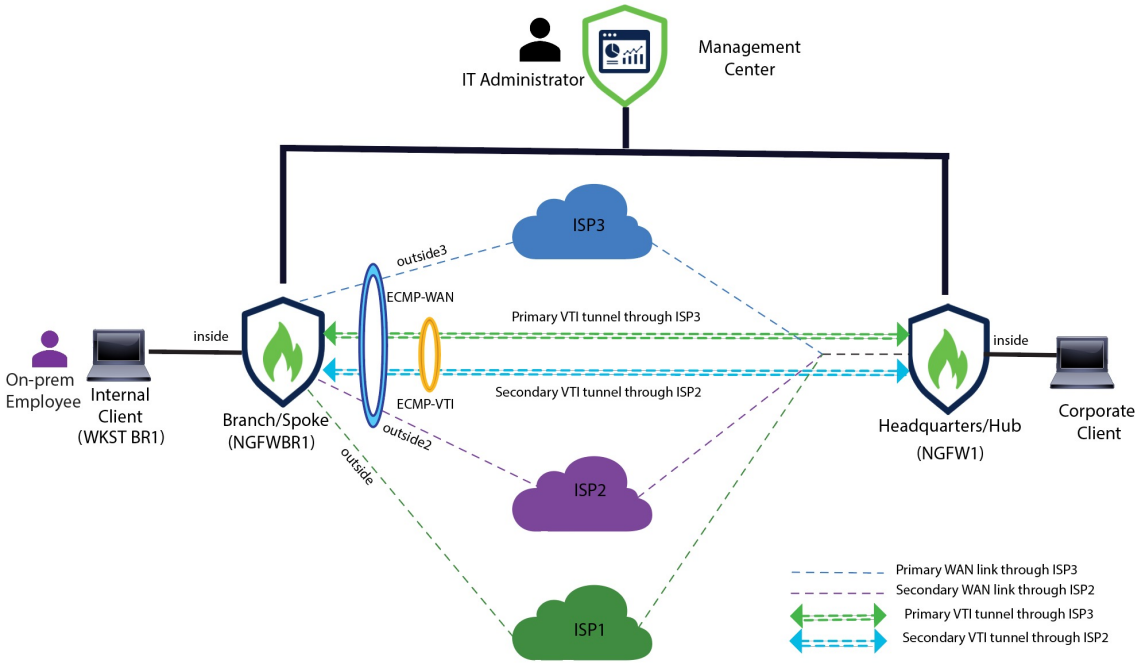
分支机构（分支）和总部（中心）之间基于路由的 VPN 如何解决问题？

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

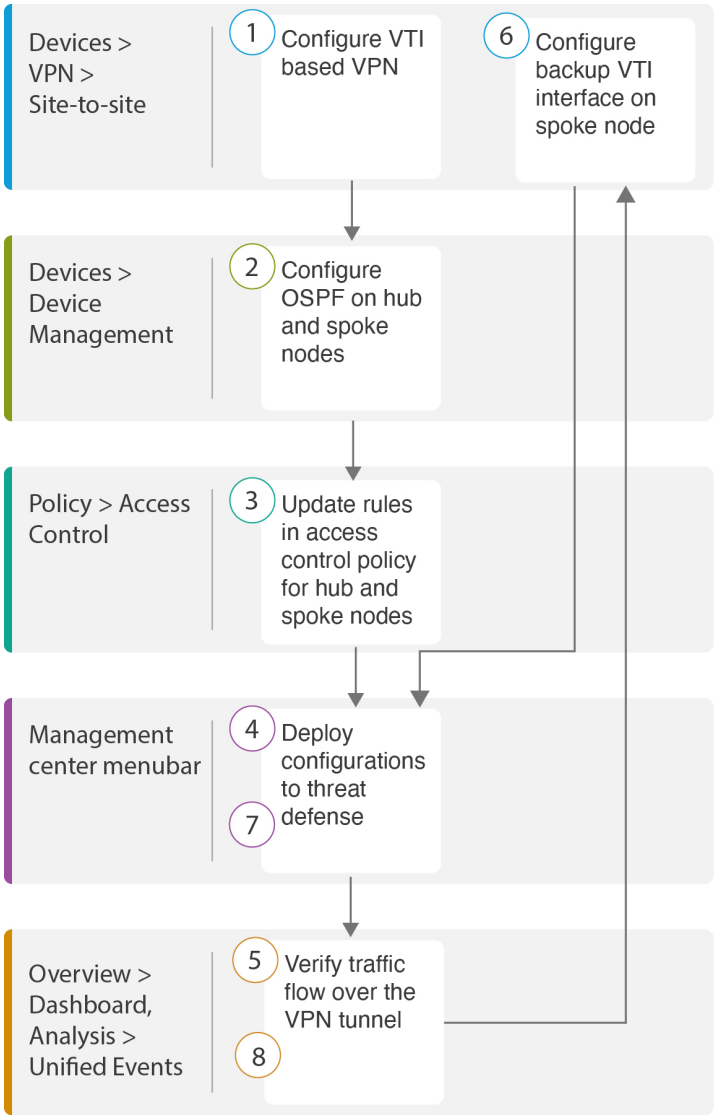
- 确保运行的是 Cisco Secure Firewall Threat Defense 版本 6.7 及更高版本。
- 仅在路由模式中支持 VTI。
- 从环回接口为动态接口配置借用 IP。
- 确保在 VTI 接口上应用访问规则，以控制通过 VTI 的流量。
- 为 SVTI 配置 ECMP 区域，以均衡 VTI 流量负载。

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 6 页 • 配置中心节点的终端， 第 7 页 • 配置分支节点的终端， 第 8 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 10 页 • 在分支节点上配置 OSPF，第 12 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 14 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 17 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 17 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 20 页。
7	在威胁防御上部署配置。请参阅部署配置，第 17 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 23 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 7 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 8 页。

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

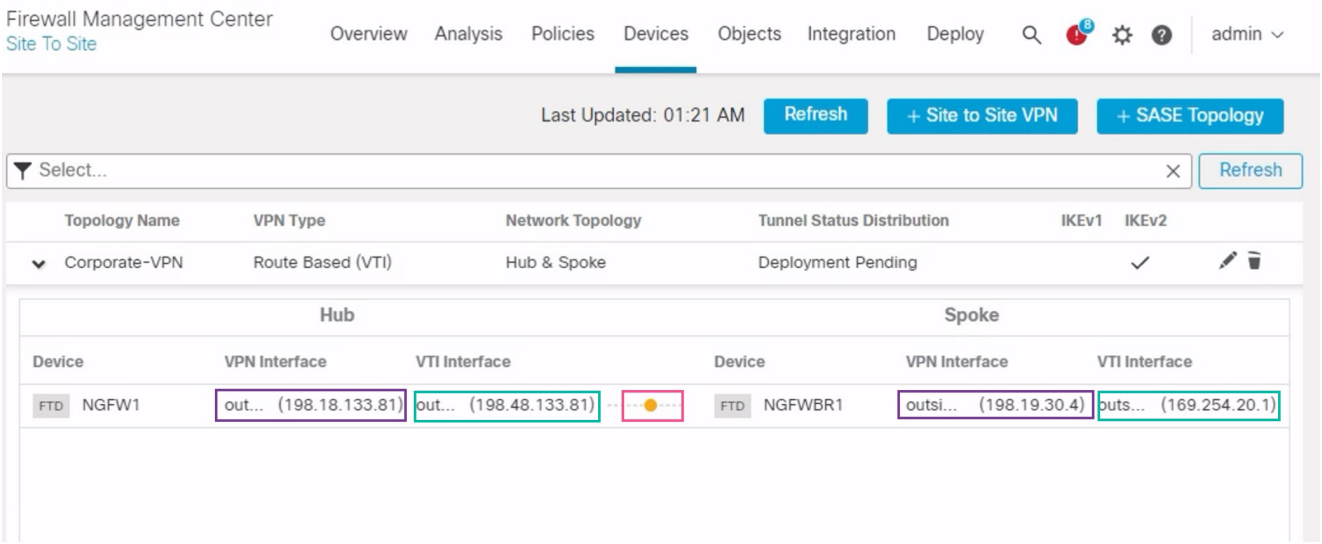
步骤 7 点击**保存 (Save)**。

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 10 页和在分支节点上配置 OSPF，第 12 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 14 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])**。

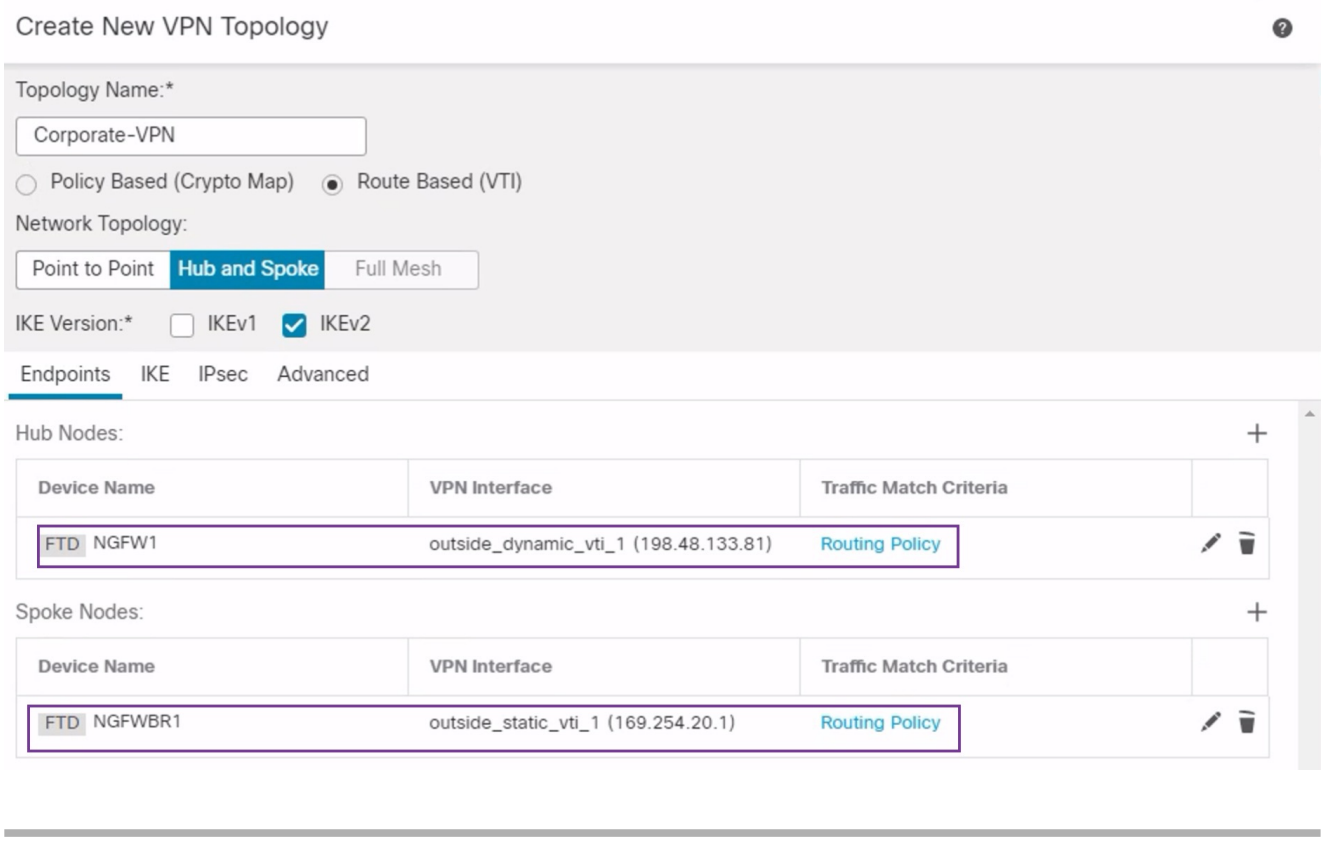
点击**确定 (OK)** 以保存 SVTI。系统将显示一条消息，确认 VTI 已成功创建。点击**确定 (OK)**。

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。

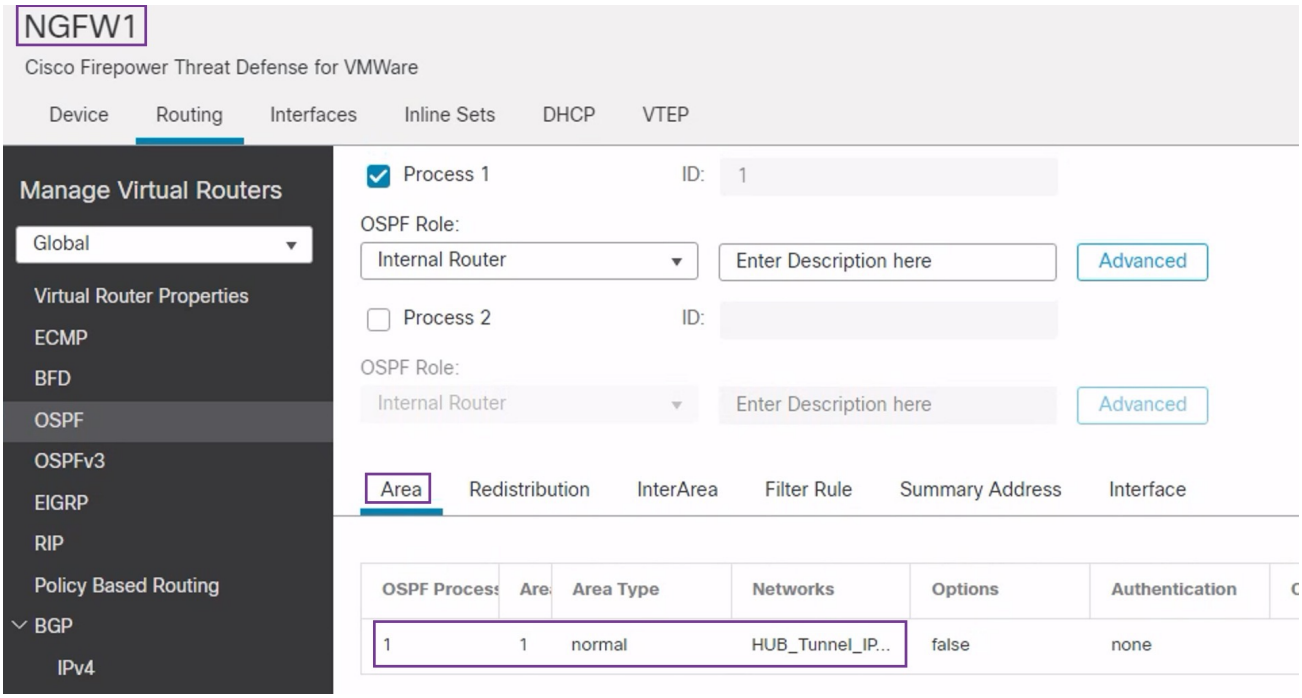
步骤 8 点击**区域 (Area)** 选项卡。

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。

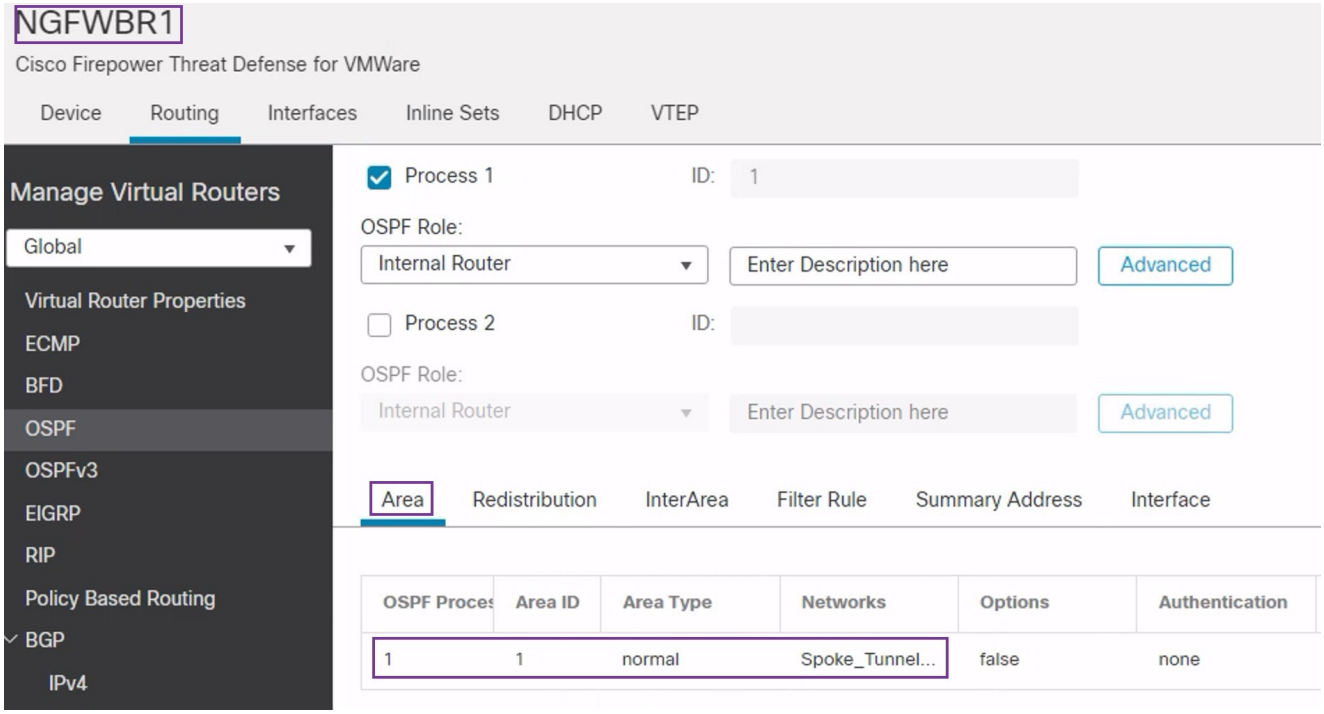
步骤 7 点击 **+添加 (+Add)**。系统将显示 **添加区域 (Add Area)** 对话框。修改以下字段：

- **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。

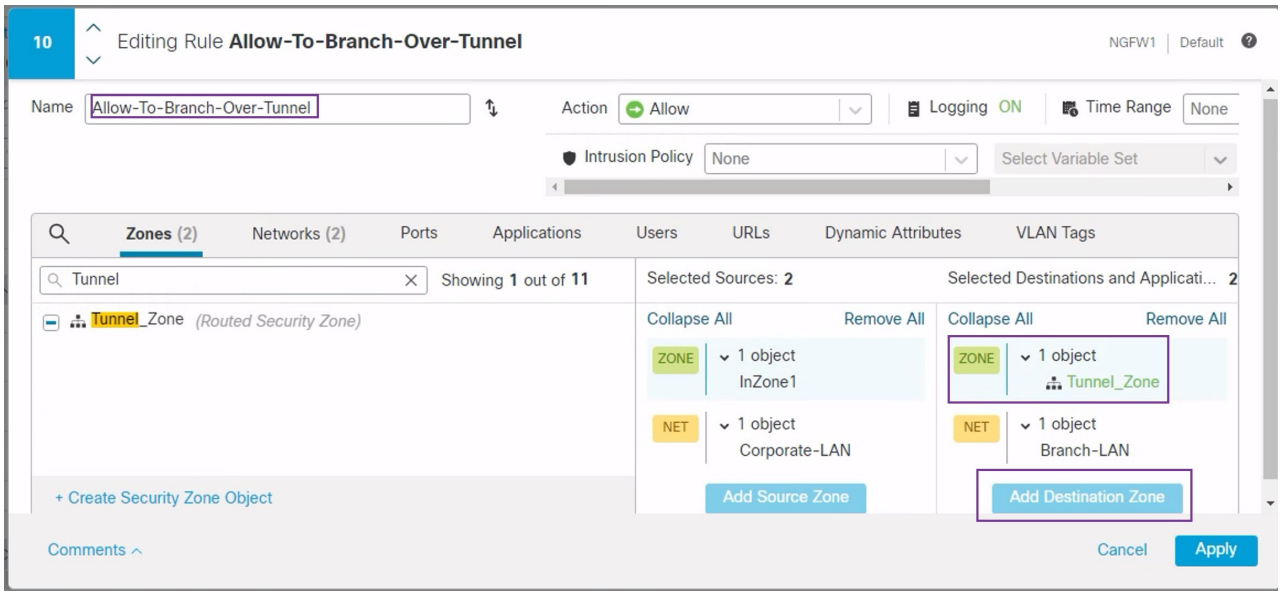
- **NGFW1** - 中心节点 (NGFW1) 的访问控制策略
- **分支机构访问控制** - 分支节点 (NGFWBR1) 的访问控制策略

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

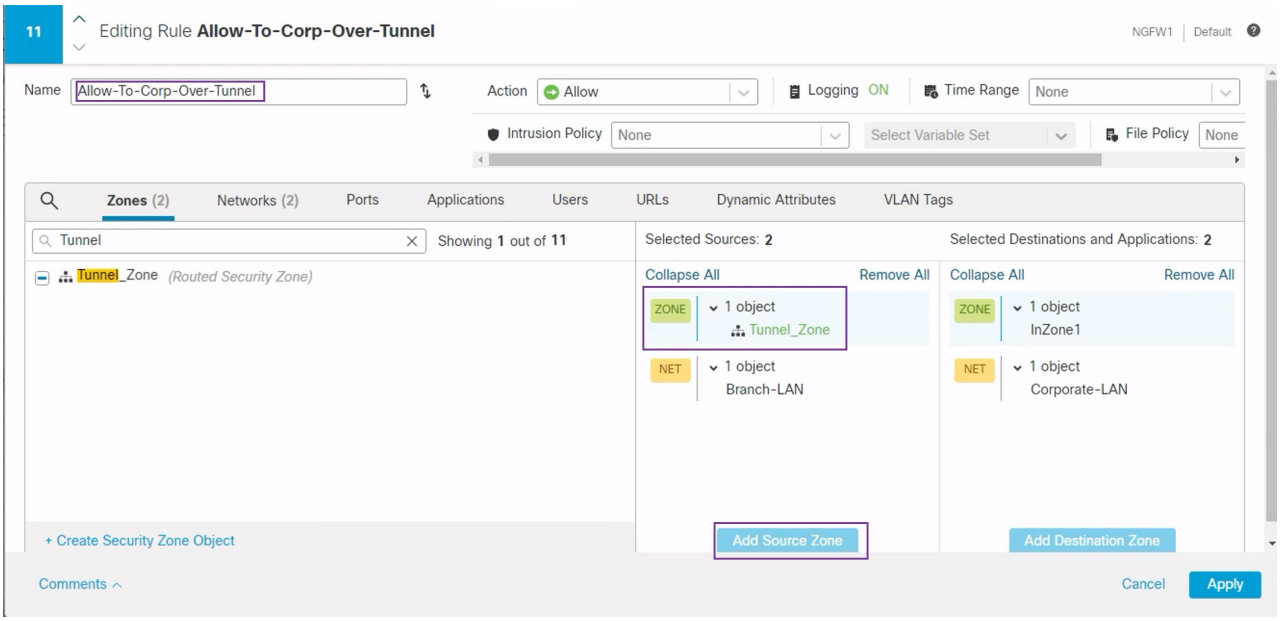
必须为此使用案例修改的现有规则包括：

- **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。

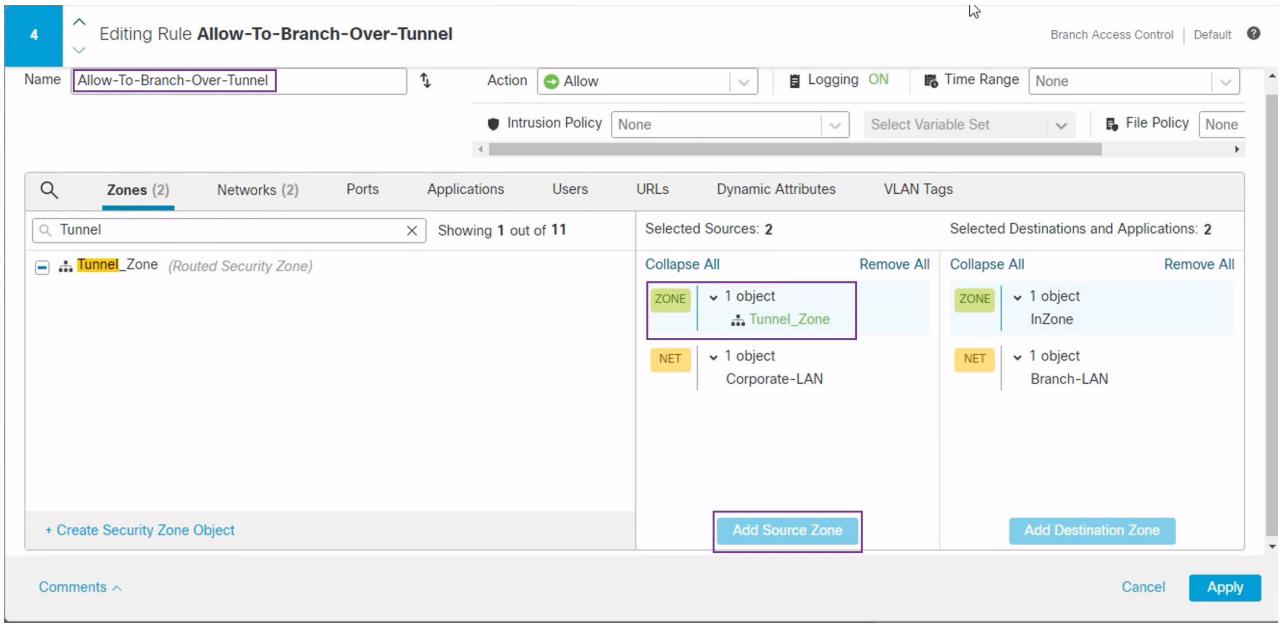
步骤 2 要编辑分支节点 (NGFWBR1) AC 策略，请点击 **编辑**（✎） 图标。

必须为此示例编辑的规则包括：

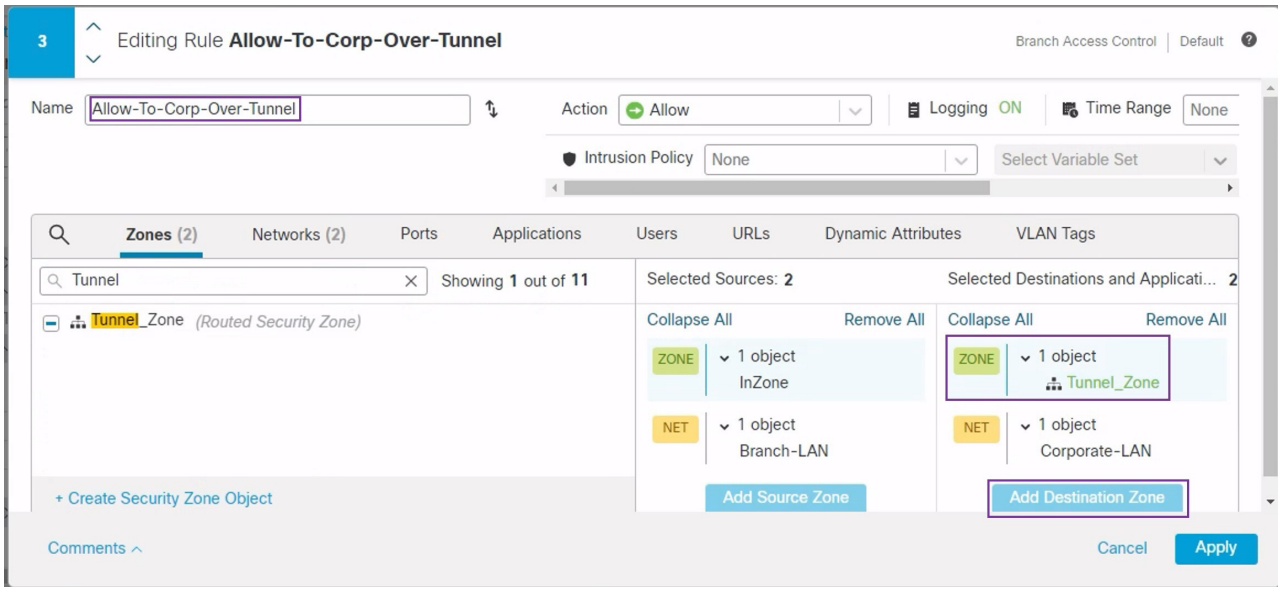
- **Allow-To-Branch-Over-Tunnel**
- **Allow-To-Corp-Over-Tunnel**

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：

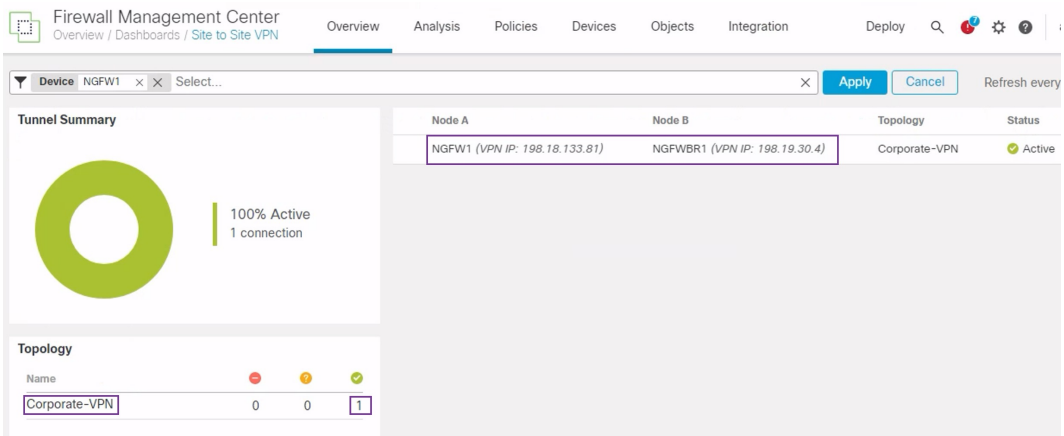
- 继续部署 - 继续部署而无需解决警告情况。如果系统识别错误，则无法继续。
- 关闭 - 退出而不部署。解决错误和警告情况，并尝试重新部署该配置。

验证流经 VPN 隧道的流量

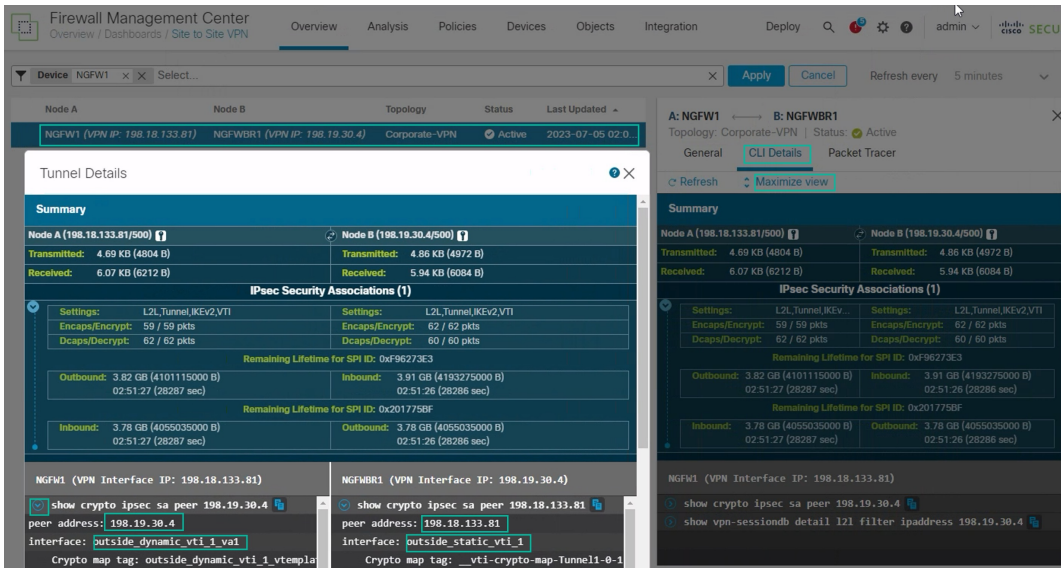
对 VPN 隧道执行以下验证。

- **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)**。

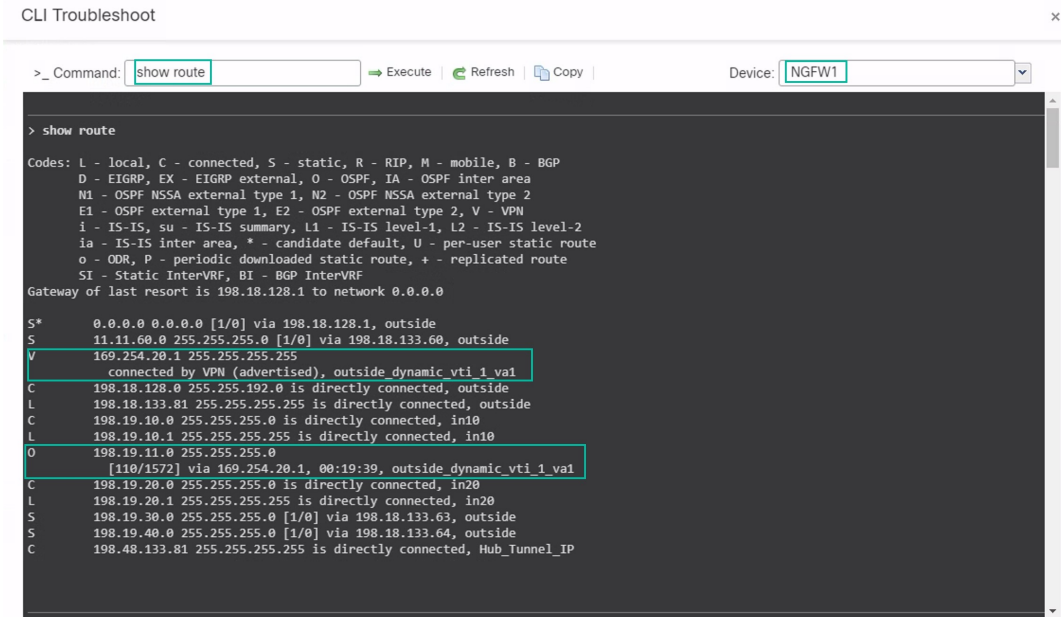


2. 将鼠标光标悬停在 NGFW1 上。NGFW1 旁边会显示**查看完整信息 (View Full Information)** 图标。
3. 点击**查看完整信息 (View Full Information)** 图标。系统将显示包含隧道详细信息和其他操作的侧窗格。
4. 点击侧窗格中的 **CLI 详细信息 (CLI Details)** 选项卡。
5. 点击**最大化视图 (Maximize View)** 以显示包含 IPSec 安全关联详细信息的最大化对话框。
6. 您可以在对话框的下半部分展开 show 命令的 CLI，以查看设备上的 VTI 接口。



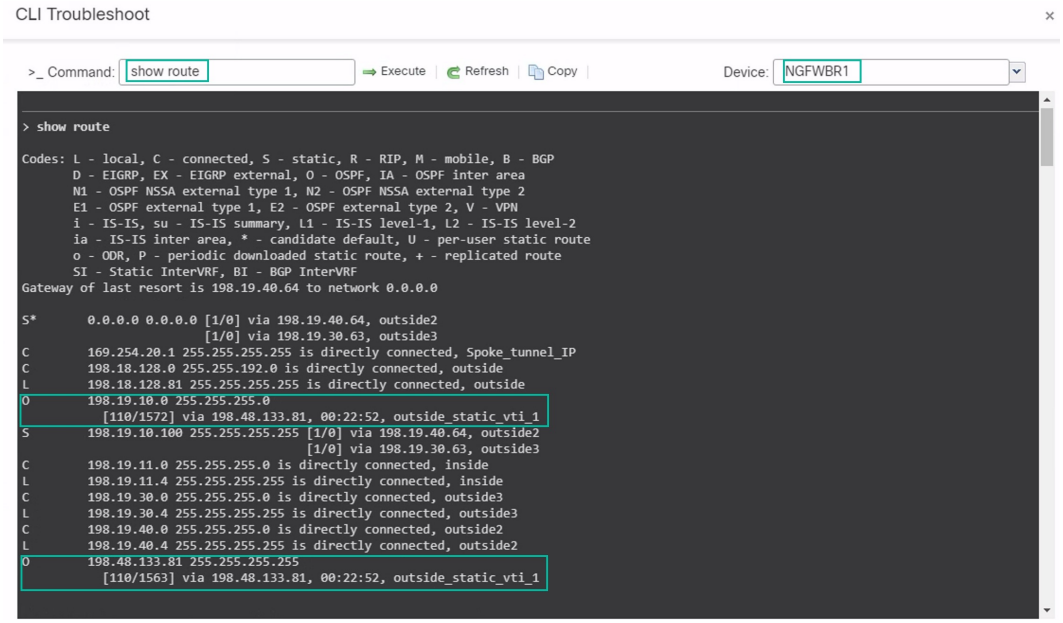
7. 点击**关闭 (Close)** 以终止“隧道详细信息”(Tunnel Details) 窗口。

- **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。



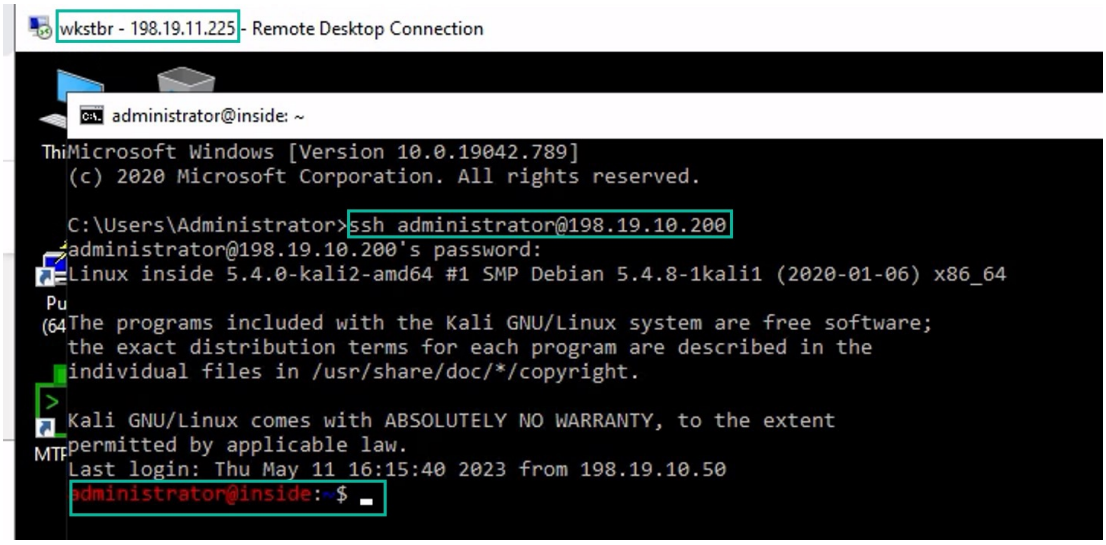
7. 对 NGFWBR1 节点重复步骤 2 至 5。

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。



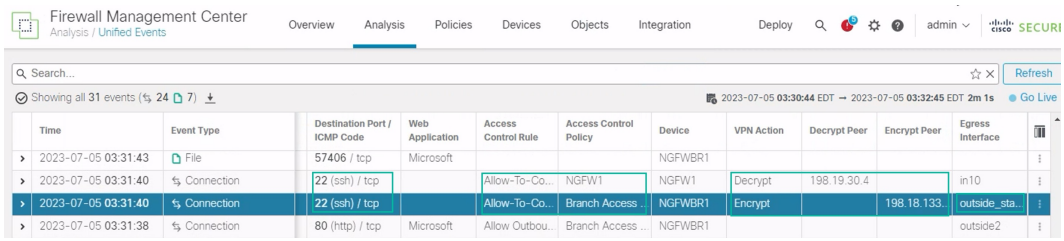
- 验证分支和中心节点背后的受保护网络之间的流量

  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。

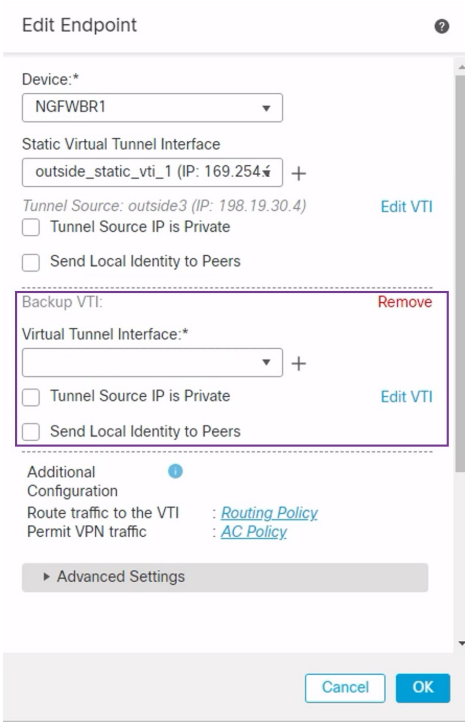
在分支节点上配置备份 VTI 接口

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**)。

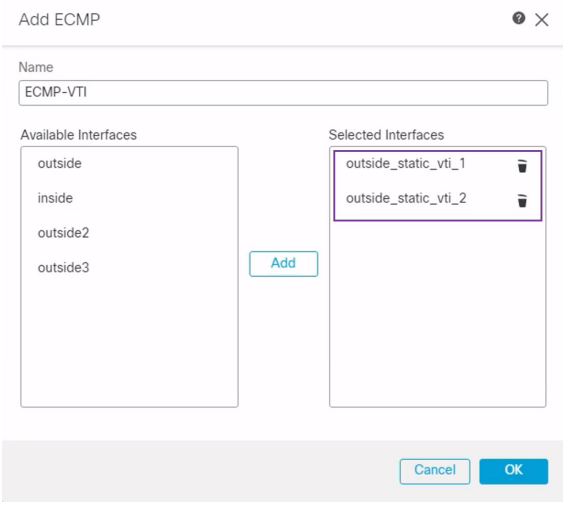
步骤 2 点击 NGFWBR1 接口视图上的**路由 (Routing)** 选项卡。

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。

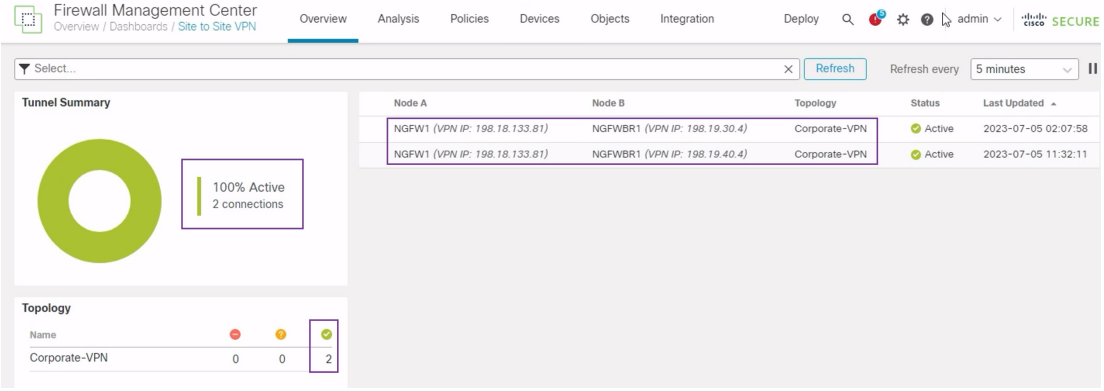
步骤 8 点击**保存 (Save)**。

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**

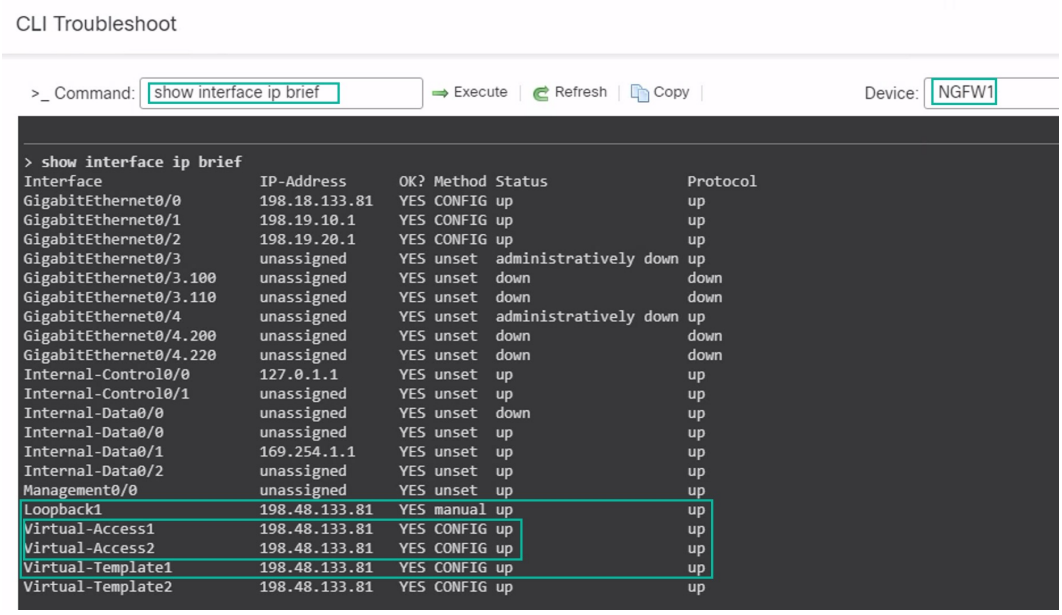
  要验证 VPN 隧道是否正常运行，请选择**概述 (Overview)** > **控制面板 (Dashboards)** > **站点间 VPN (Site-to-site VPN)**。



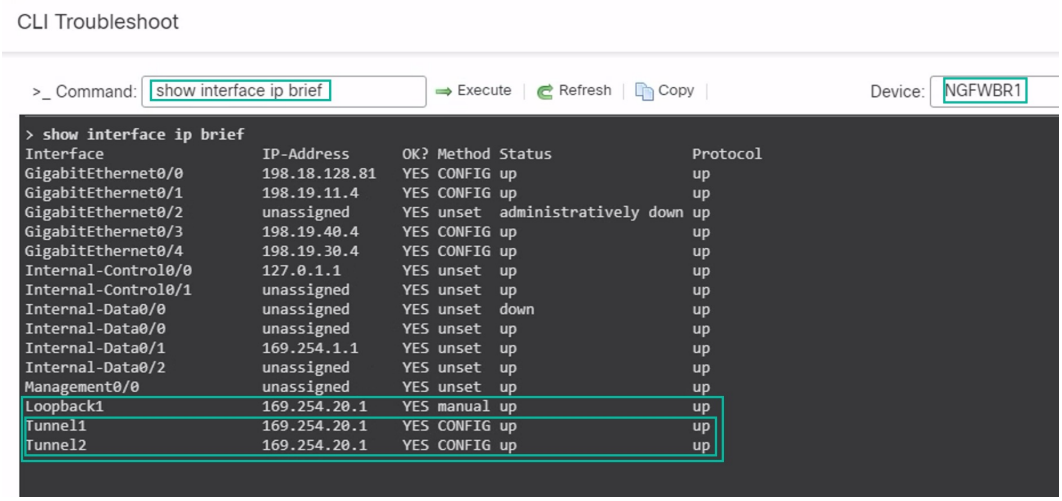
- **验证中心和分支机构节点上的路由**

  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。

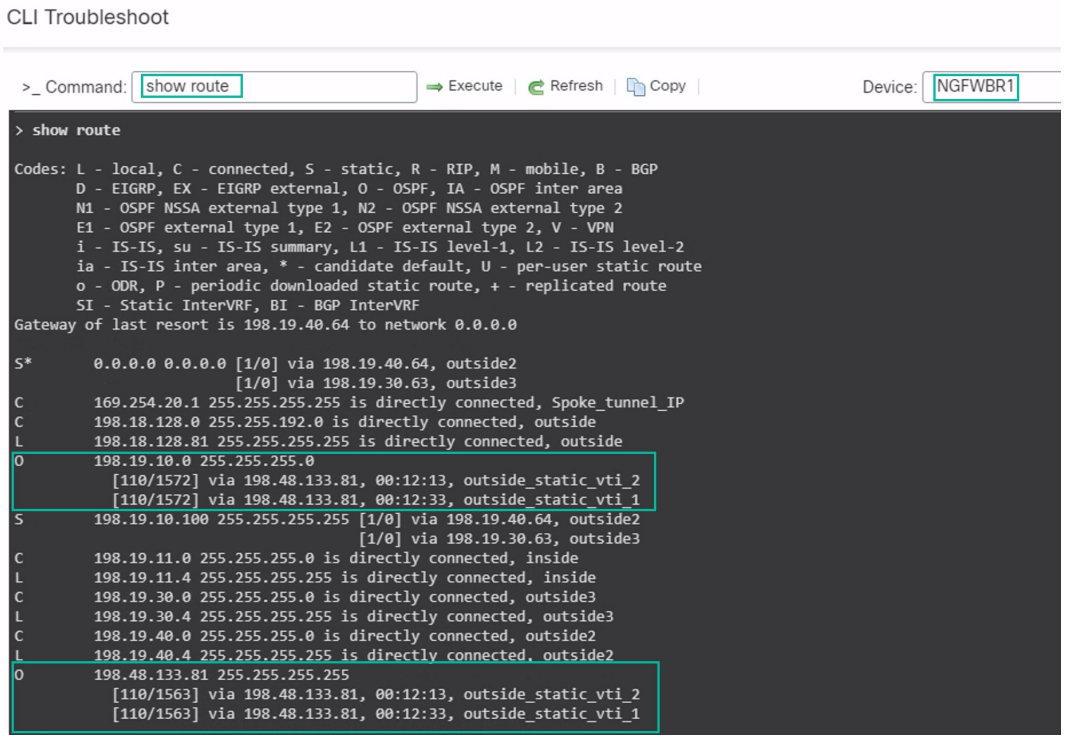
注释 当 **NGFWBR1** 通过辅助 VTI 连接连接到 NGFW1 时，会从同一 DVTI 生成 Virtual-Access2 接口。



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。



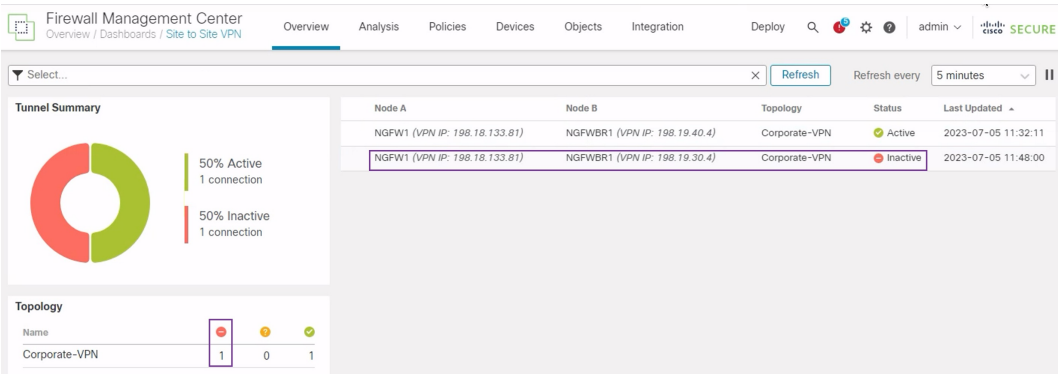
- 请注意，已在主要 (**outside_static_vti_1**) 和辅助 (**outside_static_vti_2**) VTI 上通过 OSPF 获知 **Corporate_LAN** (198.19.10.0/24)。
- 请注意，主 VTI 和辅助 VTI 也已通过 OSPF 获知了 DVTI 隧道 IP (198.48.133.81)。

- **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。



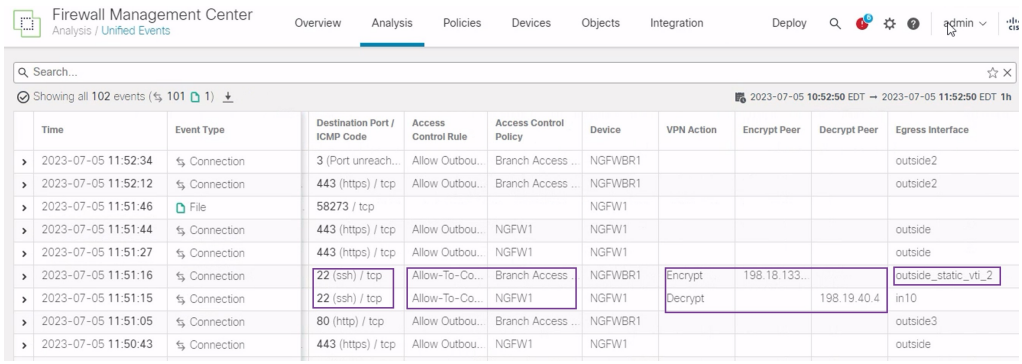
3. 发起从分支机构到中心的流量。登录 WKST BR 工作站，通过 SSH 来访问 NGFW1 后面的主机。确保您能够成功通过 SSH 连接到主机。

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

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。