SD-WAN 功能

本章介绍管理中心支持的 SD-WAN 功能。

SD-WAN 功能概述

软件定义的 WAN (SD-WAN) 解决方案取代了传统的 WAN 路由器，并且不受 WAN 传输技术的影响。SD-WAN 跨多个 WAN 连接提供基于策略的动态应用路径选择，并支持其他服务（例如 WAN 优化和防火墙）的服务链。

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，如果处理不当，不仅耗时，还容易出现配置错误。但是，组织可以通过利用 Cisco Secure Firewall Management Center（管理中心）和 Cisco Secure Firewall Threat Defense（威胁防御）设备来克服这些挑战，实现简化且安全的分支机构部署。

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 SD-WAN 功能包括：

- **简化管理：**
  - SD-WAN 向导
  - SASE：Umbrella 自动隧道部署
  - 动态 VTI (DVTI) 中心辐射型拓扑简化
- **应用感知：**
  - 公共云和访客用户的直接互联网接入 (DIA)
  - 使用应用作为匹配条件的策略型路由 (PBR)

- 为 Umbrella 提供本地隧道 ID 支持

- **增加可用带宽：**
  - ECMP 支持在多个 ISP 之间实现负载均衡和 VTI
  - 使用 PBR 的基于应用的负载均衡
- **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。
- **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 OSPF 以及 IPv4 EIGRP over VTI
  - 对具有静态或动态 IP 的分支的 DVTI 支持

功能

下表列出了一些常用的 SD-WAN 功能：

特性	已引入	更多信息
SD-WAN 向导	版本 7.6	使用 SD-WAN 向导进行安全分支机构网络部署， 第 3 页
SD-WAN 摘要控制面板上的应用监控	版本 7.4.1	Cisco SD-WAN 摘要控制面板
Cisco SD-WAN 摘要控制面板	版本 7.4	Cisco SD-WAN 摘要控制面板
具有用户身份和 SGT 的策略型路由。	版本 7.4	策略型路由
使用 HTTP 路径监控的策略型路由。	版本 7.4	策略型路由
VTI 的环回接口支持	版本 7.3	关于环回接口
对站点间 VPN 的动态 VTI (DVTI) 支持	版本 7.3	动态 VTI
Umbrella 自动隧道	版本 7.3	在 Umbrella 上部署 SASE 隧道

特性	已引入	更多信息
VTI 支持 IPv4 和 IPv6 BGP、IPv4 和 IPv6 OSPF 以及 IPv4 EIGRP	版本 7.3	BGP OSPF EIGRP
具有中心辐射型拓扑的基于路由的站点间 VPN	版本 7.2	创建基于路由的站点间 VPN
具有路径监控的策略型路由	版本 7.2	策略型路由
站点间 VPN 监控控制面板	版本 7.1	监控站点间 VPN
直接互联网接入/策略型路由	版本 7.1	策略型路由
带 WAN 接口的等价多路径 (ECMP) 区域	版本 7.1	ECMP
带 VTI 接口的等价多路径 (ECMP) 区域	版本 7.1	ECMP
备份基于路由的站点间 VPN 的 VTI	版本 7.0	通过备用 VTI 隧道路由流量
通过站点间 VPN 支持静态 VTI (SVTI)	版本 6.7	静态 VTI

使用 SD-WAN 向导进行安全分支机构网络部署

管理中心允许您可以使用新的 SD-WAN 向导轻松配置集中式总部和远程分支机构站点之间的 VPN 隧道和路由配置。

什么是中心和分支？

中心：实现与一个或多个远程分支设备或分支之间的安全VPN连接的设备。中心还充当分支相互通信的网关。

分支：位于远程分支机构的设备，通过VPN连接到中心，以安全地访问中心背后的企业资源。分支通过中心相互通信。

使用 SD-WAN 向导的优势

- 简化并自动化 SD-WAN 网络的 VPN 和路由配置。
- 创建 VPN 隧道，并通过自动执行以下任务来简化配置过程：
  - 生成分支机构的隧道接口。
  - 将 IP 地址分配给这些隧道接口。

  - 为SD-WAN重叠网络配置BGP。这些配置可确保中心和辐射之间的无缝连接，以及通过中心的辐射到辐射之间的无缝连接。

- 提供无缝路由，因为中心充当路由反射器并启用以下功能：
  - 在分支之间提供连接。
  - 根据分支的主用和备用隧道决定最佳路径。
- 要求最少的用户输入。
- 一次轻松添加多个分支机构。
- 提供简单的双 ISP 配置。
- 启用网络扩展。

使用 SD-WAN 向导的准则和限制

准则

- 配置两个集线器的 DVTI 时，请确保它们具有相同的 IPsec 隧道模式（IPv4 或 IPv6）。
- 在双中心 SD-WAN 拓扑中，中心可以位于不同的地理位置，并且背后有不同的受保护网络。要确保这些网络之间的直接通信，请确保配置以下内容：
  - 两个中心之间的基于路由的点对点 VPN 拓扑（**设备** > **VPN** > **站点间**，点击**添加** > **基于路由的 VPN**）。
  - 中心之间的动态路由协议（**设备** > **设备管理**，点击设备名称并点击**路由**）。
- 为分支配置 IP 地址池时，请确保执行以下操作：
  - 必须取消选中 **允许过载** 复选框。
  - 如果使用多个池，则其 IP 地址不得重叠。
  - IP 地址不得与辐条上的任何接口重叠。
- 创建安全区域或接口组时，请选择 **接口类型** 作为 **路由**。
- 使用 Spoke 安全区配置访问控制策略，以允许进出 Spoke 的隧道流量。
- 在 ECMP 区域中配置分支设备的静态 VTI，以均衡应用流量负载。如果不配置 ECMP 区域，当主路径发生故障时，其余路径将用作备用路径。请注意，必须在 ECMP 区域中配置分支设备的静态 VTI，而非物理接口。此配置不属于 SD-WAN 向导。
- 在具有分支双 ISP 的 SD-WAN 拓扑中，分支的隧道身份和隧道源必须是唯一的。
- 如果分支设备属于多个 SD-WAN 拓扑，请确保在每个 SD-WAN 拓扑中使用相同的本地社区标记和学习路由社区标记。请注意，本地社区标记和学习路由社区标记必须互不相同。

- 如果设备仅配置了 IPv6 地址，则必须使用具有 IPv4 地址的环回接口或物理接口配置 BGP 路由器 ID（**设备** > **设备管理**，点击**路由** > **常规设置** > **BGP**）。
- 为所有 SD-WAN VPN 拓扑中的所有隧道配置唯一的本地 IKE 身份。
- 确保 SD-WAN 拓扑中的分支设备没有相同的受保护网络。
- 为 SD-WAN 和基于路由的 VPN 使用不同的 DVTI，以避免 IPsec 配置文件冲突和错误。

限制

- 使用 SD-WAN 向导，您最多可以在 SD-WAN 拓扑中配置两个中心。
- 对于每个分支，每个拓扑只能使用一个 WAN 接口。但是，对于双 ISP 设置，您可以使用第二个 WAN 接口配置第二个 SD-WAN 拓扑。有关详细信息，请参阅使用 SD-WAN 向导部署双 ISP 的配置示例，第 10 页。
- SD-WAN 向导不支持以下各项：
  - IKEv1
  - 中心和辐射型不支持集群设备，因为集群设备上不支持 VTI。
  - 外联网中心和辐射点，例如 ASA、思科 IOS、思科 Viptela、Umbrella、Meraki 或供应商设备。

使用 SD-WAN 向导的前提条件。

- 防火墙管理中心 Essentials（以前称为 Base）许可证必须允许导出控制功能。

  选择**系统 (System)** > **许可证 (Licenses)** > **智能许可证 (Smart Licenses)** 以便在 防火墙管理中心 中验证此功能。
- 您必须是管理员用户。
- 中心设备的版本必须为 7.6.0 及更高版本。
- 分支设备的版本必须为 7.3.0 及更高版本。
- 设备必须具有可通过互联网路由的公共 IP 地址。IP 地址可以是静态地址或动态地址。
- 为设备的接口分配适当的逻辑名称和 IP 地址。例如，使用 内部 表示连接到 LAN 的接口，使用 外部 表示连接到互联网或 WAN 的接口。
- 如果使用基于证书的身份验证，则必须在中心和分支中注册证书。
- 配置路由、NAT 和 AC 策略，以确保设备之间的底层连接。

使用 SD-WAN 向导配置 SD-WAN 拓扑

SD-WAN 向导允许您在集中式总部和远程分支机构站点之间轻松配置 VPN 隧道。

开始之前

确保您查看 使用 SD-WAN 向导的前提条件。，第 5 页 和 使用 SD-WAN 向导的准则和限制，第 4 页。

过程

步骤 1 选择 **设备** > **VPN** > **站点间**，然后点击**添加 (Add)**。

步骤 2 在 **拓扑名称** 字段中，输入 SD-WAN VPN 拓扑的名称。

步骤 3 点击 **SD-WAN 拓扑** 单选按钮，然后点击 **创建**。

步骤 4 配置集线器：

a) 点击 **添加集线器**。

b) 从 **设备** 下拉列表中选择中心 。

c) 点击 **动态虚拟隧道接口** 下拉列表旁边的 + 以为中心添加动态 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。然而，您必须配置 **隧道源** 和 **借用 IP 地址**。有关详细信息，请参阅向中心添加动态虚拟隧道接口，第 9 页。

d) 点击**确定**。

e) 在**中心网关 IP 地址**字段，输入中心 VPN 接口的公共 IP 地址或分支所连接的动态 VTI 的隧道源。

如果接口具有静态 IP 地址，则系统会自动填充 IP 地址。如果集线器位于 NAT 设备后面，则必须手动配置 NAT 后的 IP 地址。

f) 从**分支隧道 IP 地址池**下拉列表中选择地址池，或者点击 + 创建池。

添加分支时，向导会自动生成分支隧道接口，并从此 IP 地址池将 IP 地址分配给这些分支接口。

g) 点击 **添加** 以保存中心配置。

h) （可选）要添加辅助中心，请重复步骤 4a 至步骤 4f。

i) 点击**下一步 (Next)**。

步骤 5 配置分支：

点击 **添加** 分支以添加单个分支设备，或点击 **添加分支**（**批量添加**） 以将多个分支添加到您的拓扑。

- 点击 **添加分支**。在 **添加分支** 对话框中，配置以下参数：

  1. 从 **设备** 下拉列表中选择分支。
  2. 从 **VPN 接口** 下拉列表中选择面向 WAN 或面向互联网的物理接口，以与中心建立 VPN 连接。
  3. 选中 **本地隧道 (IKE) 身份** 为此设备到远程对等体的 VPN 隧道启用唯一且可配置的身份。默认情况下，此选项处于已启用状态。

4. 从 **身份类型** 下拉列表中，选择以下选项之一：
   - **密钥 ID**-（默认值）此值自动填充为 *<sd-wan topologyname>_<device_IP_address>*，例如，sdwantopo1_192.168.0.200。您还可以指定您选择的密钥 ID。
   - **邮件 ID**- 指定最多 127 个字符的邮件 ID。
   - **IP 地址**-分支 VPN 接口的 IP 地址。
   - **自动**- 用于预共享密钥身份验证的辐条 VPN 接口的 IP 地址或用于基于证书的身份验证的证书可分辨名称 (DN)。
   - **主机名**-分支的完全限定主机名。
5. 点击 **保存** 以保存分支配置。

- 点击 **添加分支**（**批量添加**）。在 **添加批量分支** 对话框中，配置以下参数：
  1. 从 **可用设备** 列表中选择一个或多个设备，然后点击 **添加** 以将设备移至 **所选设备**。
  2. 使用以下方法之一选择分支的 VPN 接口：
     - 点击 **接口名称模式** 单选按钮，指定一个字符串以匹配分支的互联网或 WAN 接口的逻辑名称，例如，outside*、wan*。

       如果辐射具有多个具有相同模式的接口，则会为拓扑选择与模式匹配的第一个接口。
     - 点击 **安全区域** 单选按钮，从下拉列表中选择具有分支的 VPN 接口的安全区域，或点击 **+** 创建安全区域。
  3. 点击**下一步 (Next)**。

     该向导将验证轮辐是否具有具有指定模式的接口。仅向拓扑添加经过验证的设备。
  4. 点击**添加 (Add)**。
  5. 点击**下一步 (Next)**。

对于每个分支，向导会自动选择集线器的 DVTI 作为隧道源 IP 地址。

注释
如果中心的隧道源 IP 地址是 IPv6 地址，则向导会自动选择分支的所选接口的第一个 IPv6 地址。要编辑分支隧道源的 IPv6 地址，请点击分支旁边的编辑图标，然后选择一个 **IP 地址** 下拉列表中的 IPv6 地址，然后点击 **保存**。

步骤 6 为 SD-WAN 拓扑中的设备配置身份验证设置：

a) **身份验证类型**- 对于设备身份验证，可以使用手动预共享密钥、自动生成的预共享密钥或证书。
   - **预共享手动密钥**-指定此 VPN 连接的预共享密钥。
   - **预共享自动密钥**-（默认值）向导会自动定义此VPN连接的预共享密钥。在 **预共享密钥长度** 字段中指定密钥长度。范围为 1 到 127。

- **证书 (Certificate)** - 当您将证书用作身份验证方法时，对等体从 PKI 基础设施中的 CA 服务器获取数字证书，并适用其相互进行身份验证。

b) 从 **转换集** 下拉列表中选择一个或多个算法。
c) 从 **IKEv2 策略** 下拉列表中选择一个或多个算法。
d) 点击**下一步 (Next)**。

步骤 7 配置 SD-WAN 设置：

此步骤涉及自动生成分支隧道接口，以及重叠网络的 BGP 配置。

a) 从 **分支隧道接口安全区域** 下拉列表中选择一个安全区域，或点击 **+** 以创建一个安全区域，向导会自动将分支的自动生成的静态虚拟隧道接口 (SVTI) 添加到该安全区域。
b) 选中**在 VPN 重叠拓扑上启用 BGP** 复选框以自动执行 BGP 配置，例如覆盖网络隧道接口之间的邻居配置以及来自中心和分支的直接连接的 LAN 接口的基本路由重新分发。
c) 在 **自治系统编号** 字段中，输入自治系统 (AS) 编号。

自治系统 (AS) 编号是具有单一路由策略的网络的唯一编号。BGP 使用 AS 编号标识网络。分支 BGP 邻居配置是根据相应中心的 AS 编号生成的。范围是从 0 到 65536。

- 如果所有中心和辐射点都位于同一区域，则默认情况下，**64512** 是 AS 编号。
- 如果主中心和辅助中心位于不同的区域，则为主中心和分支配置 **64512** 作为 AS 编号，并且为辅助中心配置其他编号。

d) 在 **本地路由的社区标记** 字段，输入用于标记已连接和重新分发的本地路由的 BGP 社区属性。此属性可轻松实现路由过滤。
e) 选中 **重新分发连接的接口** 复选框，从下拉列表中选择一个接口组，或点击 **+** 以创建具有连接的内部或 LAN 接口的接口组，以便在重叠拓扑上重新分发 BGP 路由。
f) 选中 **启用BGP的多路径** 复选框，允许同时使用多个BGP路由到达同一目的地。此选项使BGP能够跨多个链路对流量进行负载均衡。

请注意，启用此选项后，BGP 多路径仅对分支设备启用。

g) （可选）请选中 **辅助中心在不同的自治系统** 中复选框。仅当此拓扑中有辅助中心时，才会显示此复选框。
h) 在**远程 AS 编号**字段中，输入辅助中心的自治系统 (AS) 编号。
i) 在 **获知路由的社区标记** 字段，输入 BGP 社区属性，用于标记通过 VPN 隧道从其他 SD-WAN 对等体获知的路由。仅当辅助集线器具有不同的AS编号时，才需要对eBGP配置使用此属性。仅当您在 SD-WAN 拓扑中配置了两个中心时，才会显示此字段。
j) 点击**下一步 (Next)**。

步骤 8 点击 **完成** 以保存并验证 SD-WAN 拓扑。

您可以在 **站点间 VPN 摘要** 页面（**设备** > **VPN** > **站点间**）中查看拓扑。将配置部署到所有设备后，您可以在此页面中查看所有隧道的状态。

下一步做什么

- 查看自动生成的分支 SVTI 及其 IP 地址 - 点击分支配置旁的编辑按钮，然后点击 **查看生成的隧道接口**。
- 建议在分支设备的 SVTI 上启用 ECMP。选择 **设备** > **设备管理**，然后点击**路由** > **ECMP**。
- 在中心和辐射点上部署配置。选择**部署**。选择设备并点击**部署**。
- 验证 SD-WAN 拓扑的隧道状态。有关详细信息，请参阅验证 SD-WAN 拓扑的隧道状态，第 15 页。
- 为分支的隧道接口安全区域配置 ACL。选择 **策略** > **访问控制**。
- 建议在中心设备上启用 BGP 多路径。要在中心设备上启用 BGP 多路径，请执行以下操作：
  1. 选择 ECMP**设备** > **设备管理**，然后点击**路由**。
  2. 在**常规设置**下，点击 **BGP**。
  3. 选中**启用 BGP** 复选框以启用 BGP。
  4. 在 **AS 编号**字段中，输入在 SD-WAN 拓扑中配置的 AS 编号。
  5. 点击**保存**。
  6. 在左侧窗格中，选择 **BGP** > **IPv4 或 IPv6**，然后点击**常规**选项卡。
  7. 在**通过多个路径转发数据包**部分中，点击编辑图标。
  8. 配置**路径数量**和 **IBGP 路径数量**的值。建议将这些值配置为 8。
- 有关使用 SD-WAN 向导的配置示例的详细信息，请参阅使用 SD-WAN 向导部署双 ISP 的配置示例，第 10 页
- 在每个分支上，根据 WAN 接口的应用性能指标为应用感知路由或智能路径选择配置 PBR 策略。有关更多信息，请参阅 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。

向中心添加动态虚拟隧道接口

在 SD-WAN 向导中，必须为每个集线器配置 DVTI。DVTI 使用虚拟模板为每个 VPN 会话动态生成独一无二的虚拟访问接口。

开始之前

在 SD-WAN 向导中，点击 **添加集线器**，然后从 **设备** 下拉列表中选择集线器。

过程

步骤 1 点击 **动态虚拟隧道接口 (Dynamic Virtual Tunnel Interface)** 下拉列表旁边的 **+** 以为中心添加 DVTI。

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。

1. **隧道类型**：动态。
2. **名称**: <*tunnel_source_interface_logical name*>_dynamic_vti_<*tunnel_ID*。例如，outside_dynamic_vti_1。
3. **已启用** 复选框：默认选中。
4. **模板 ID**：DVTI 的唯一 ID。
5. **隧道源**：作为 DVTI 源的物理接口，默认情况下会被自动填充。
6. **IPsec 隧道模式**：默认为 IPv4。

步骤 2 从 **安全区域** 下拉列表中选择动态 VTI 的安全区域。

步骤 3 从 **借用 IP** 下拉列表中选择物理或环回接口，动态 VTI 接口将继承此 IP 地址。

确保使用不同于隧道源 IP 地址的 IP 地址。我们建议您使用环回 IP 地址。

步骤 4 点击 **确定** 以保存动态 VTI。

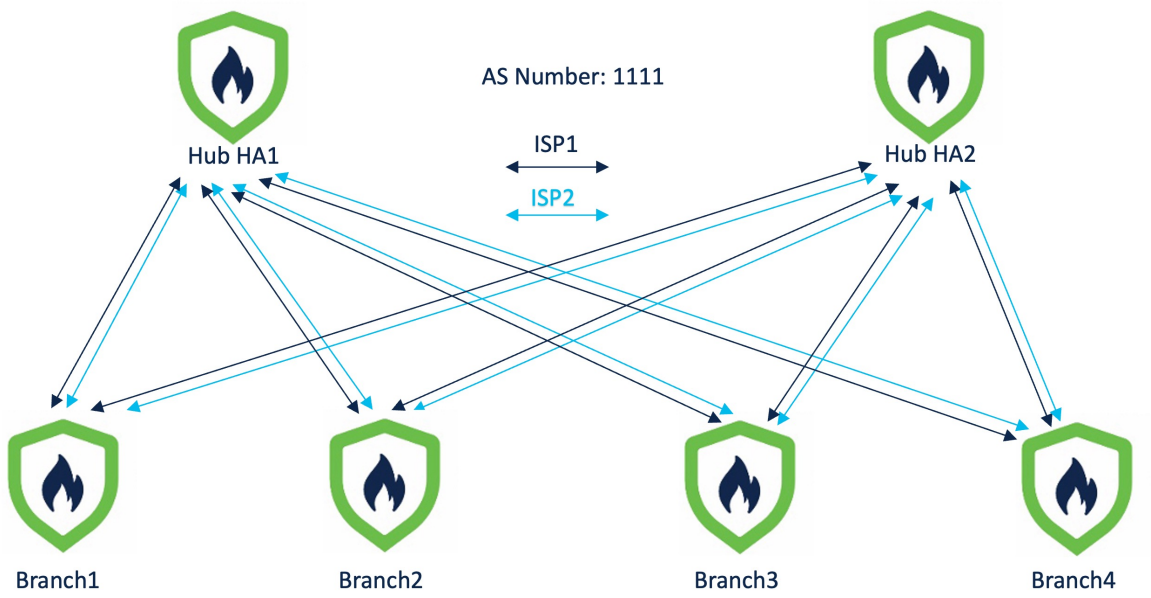
使用 SD-WAN 向导部署双 ISP 的配置示例

双 ISP 部署：同一区域中的两个中心和四个分支

在以下拓扑中，中心和辐射点位于单个区域中，AS 编号为 1111。中心和辐射点使用内部边界网关协议 (iBGP) 作为路由协议来交换路由信息。

- 中心 HA1 和中心 HA2 是总部的中心威胁防御设备。
- Branch1、Branch2、Branch3 和 Branch4 是分支机构的分支威胁防御设备。
- ISP1 是每个分支到 ISP1 的 VPN 接口。
- ISP2 是每个分支到 ISP2 的 VPN 接口。

图 *1:* 双 *ISP* 拓扑具有相同区域的两个中心和四个分支



要配置此拓扑，必须使用 SD-WAN 向导创建以下两个 SD-WAN 拓扑：

SD-WAN 拓扑 1

参数	值
主中心	集线器 HA1
辅助集线器	集线器 HA2
分支	分支1、分之2、分支3、分支4
AS 编号	1111
VPN 接口（分支隧道源）	ISP1
隧道数量	8

SD-WAN 拓扑 1 中的隧道总数为 8。

SD-WAN 拓扑 2

参数	值
主中心	集线器 HA1
辅助集线器	集线器 HA2
分支	分支1、分之2、分支3、分支4

参数	值
AS 编号	1111
VPN 接口（分支隧道源）	ISP2
隧道数量	8

SD-WAN 拓扑 2 中的隧道总数为 8。

此双 ISP 部署的 VPN 隧道总数为 16。

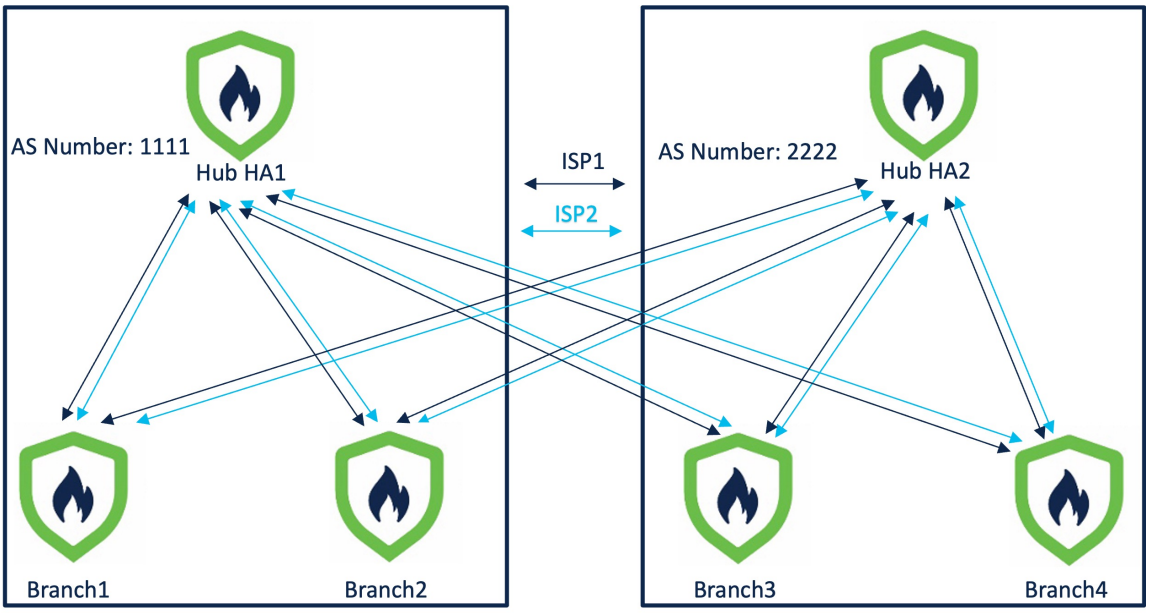
注释 如果集线器位于不同的地理位置，并且背后有不同的受保护网络，为确保这些网络之间的直接通信，请使用基于路由的 VPN 向导在两个集线器之间配置基于点对点路由的 VPN 拓扑。

双 ISP 部署：不同区域中的两个中心和四个分支

在以下双 ISP 拓扑中，集线器位于不同的区域，每个区域都有两个直连辐射点。集线器及其直连分支使用内部边界网关协议 (iBGP) 作为路由协议，而集线器使用外部边界网关协议 (eBGP) 交换路由信息。

- 中心 HA1 和中心 HA2 是总部的中心威胁防御设备。
- Branch1、Branch2、Branch3 和 Branch4 是分支机构的分支威胁防御设备。
- HQ1、Branch1 和 Branch2 位于一个区域，AS 编号为 1111。
- HQ2、Branch3 和 Branch4 位于一个区域，AS 编号为 2222。
- ISP1 是每个分支到 ISP1 的 VPN 接口。
- ISP2 是每个分支到 ISP2 的 VPN 接口。

图 2: 双 *ISP* 拓扑具有不同区域的两个中心和四个分支



要配置此拓扑，必须使用 SD-WAN 向导创建以下四个 SD-WAN 拓扑：

SD-WAN 拓扑 1

参数	值
主中心	集线器 HA1
辅助集线器	集线器 HA2
分支	分支机构 1 和 分支机构 2
AS 编号	1111
辅助 AS 编号	2222
VPN 接口（分支隧道源）	ISP1

SD-WAN 拓扑 1 中的隧道数量为 4。

SD-WAN 拓扑 2

参数	值
主中心	集线器 HA1
辅助集线器	集线器 HA2
分支	分支机构 1 和 分支机构 2

参数	值
AS 编号	1111
辅助 AS 编号	2222
VPN 接口（分支隧道源）	ISP2

SD-WAN 拓扑 2 中的隧道数量为 4。

SD-WAN 拓扑 3

参数	值
主中心	集线器 HA2
辅助集线器	集线器 HA1
分支	分支机构 3 和分支机构 4
AS 编号	2222
辅助 AS 编号	1111
VPN 接口（分支隧道源）	ISP1

SD-WAN 拓扑 3 中的隧道数量为 4。

SD-WAN 拓扑 4

参数	值
主中心	集线器 HA2
辅助集线器	集线器 HA1
分支	分支机构 3 和分支机构 4
AS 编号	2222
辅助 AS 编号	1111
VPN 接口（分支隧道源）	ISP2

SD-WAN 拓扑 4 中的隧道数量是 4。

此双 ISP 部署的 VPN 隧道总数为 16。

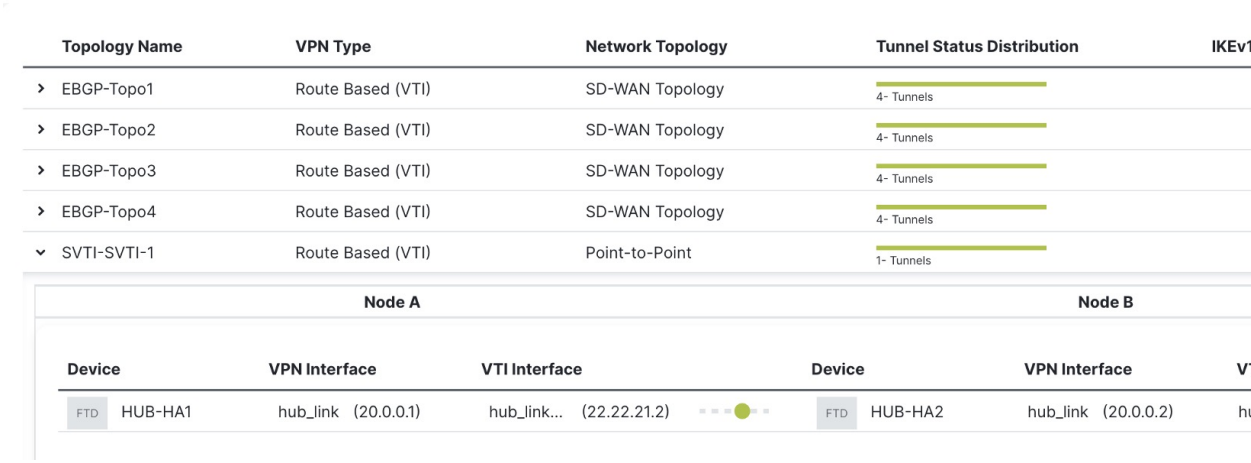
注释 如果集线器位于不同的地理位置，并且背后有不同的受保护网络，为确保这些网络之间的直接通信，请使用基于路由的 VPN 向导在两个集线器之间配置基于点对点路由的 VPN 拓扑。

验证 SD-WAN 拓扑的隧道状态

在站点间 VPN 摘要页面上验证隧道状态

要验证 SD-WAN 拓扑的 VPN 隧道是否已启动，请选择**设备** > **VPN** > **站点间**。

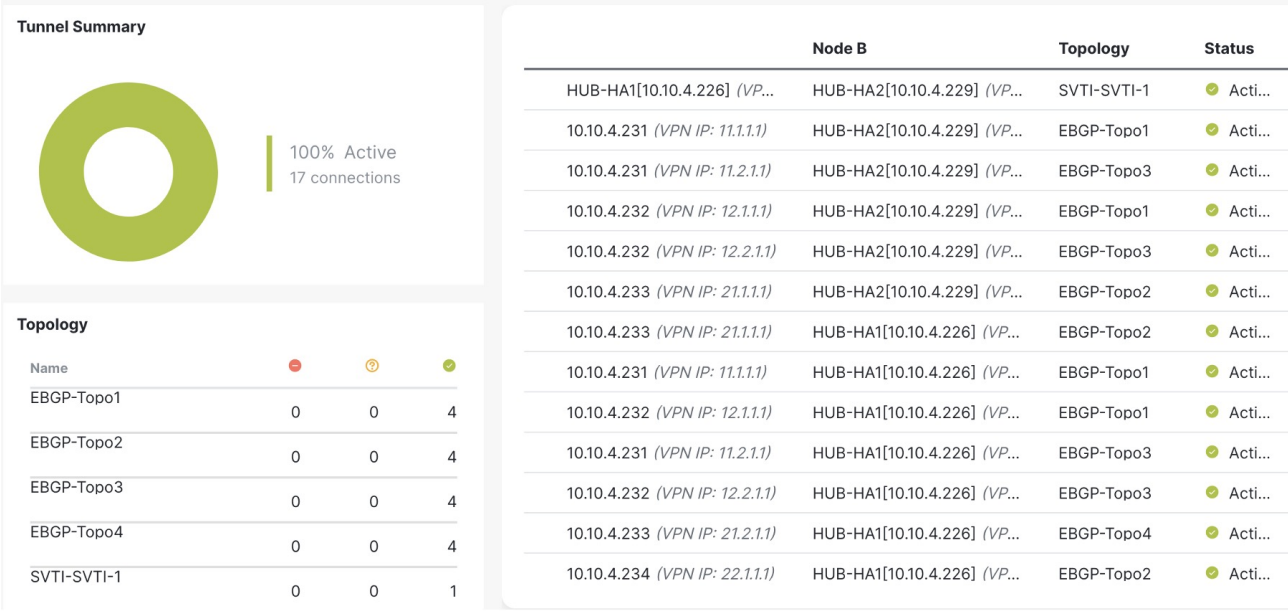
以下是五个 SD-WAN 拓扑，其中两个中心和四个分支位于不同的区域，连接到双 ISP：



在站点间 VPN 控制面板上验证隧道状态

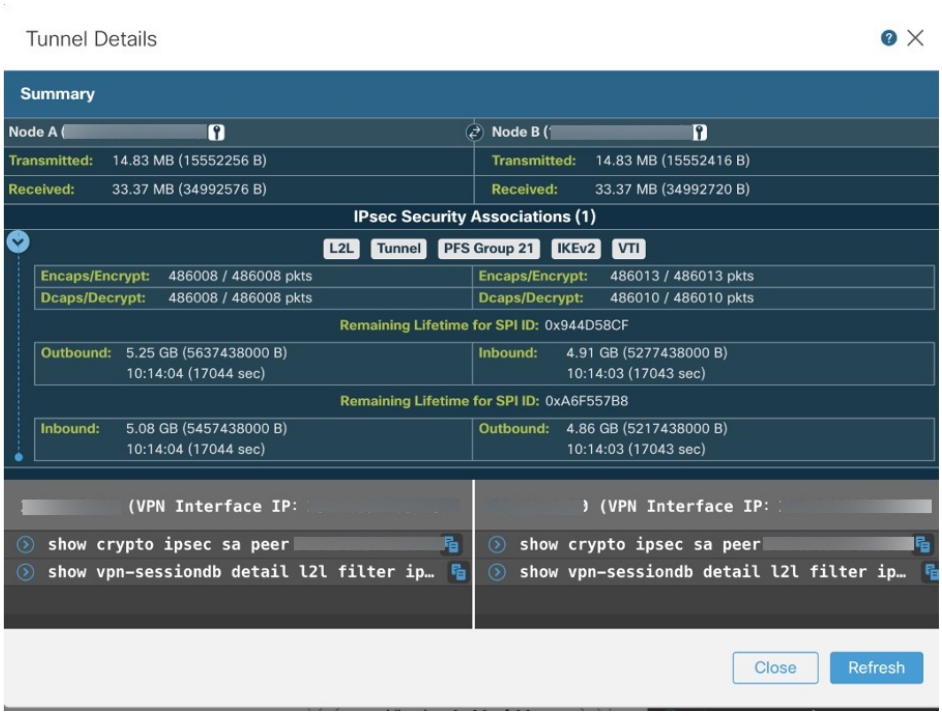
要查看 SD-WAN VPN 隧道的详细信息，请选择**概述** > **控制面板** > **站点间 VPN**。

以下是 SD-WAN 拓扑的 VPN 隧道，其中两个中心和四个分支位于不同的区域，连接到双 ISP：



要查看每个 VPN 隧道的更多详细信息，请执行以下操作：

1. 将鼠标悬停在隧道上。
2. 点击 **查看完整信息** (👁) 图标。系统将显示包含隧道详细信息和更多操作的窗格。
3. 点击侧窗格中的 **CLI 详细信息** 选项卡，查看 IPsec 安全关联的 show 命令和详细信息。



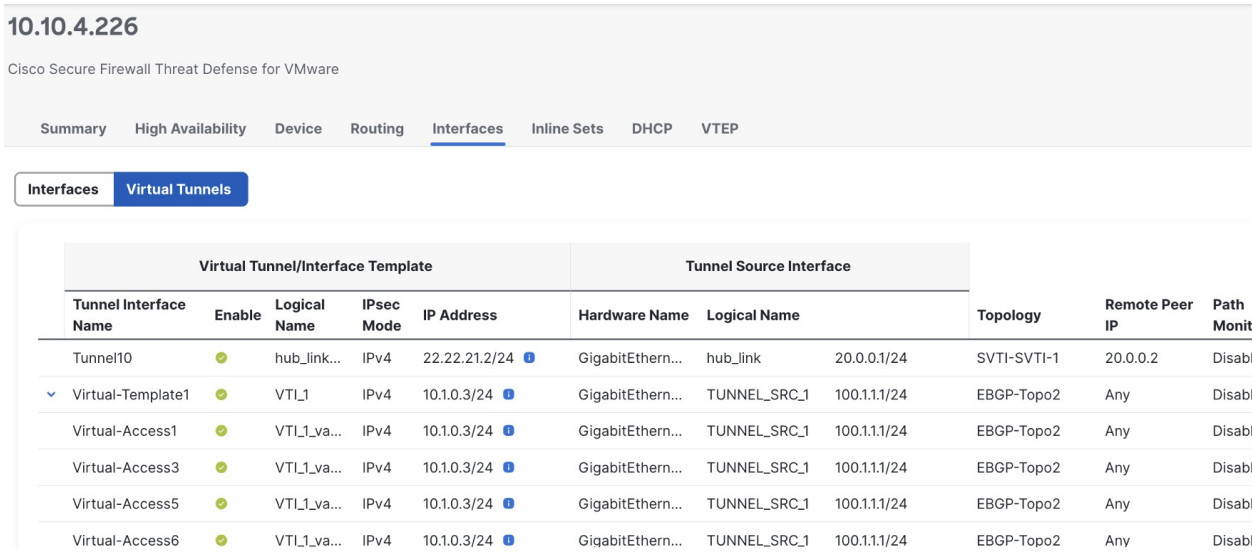
查看设备的虚拟隧道接口

要查看中心的动态 VTI 和分支的静态 VTI，请执行以下操作：

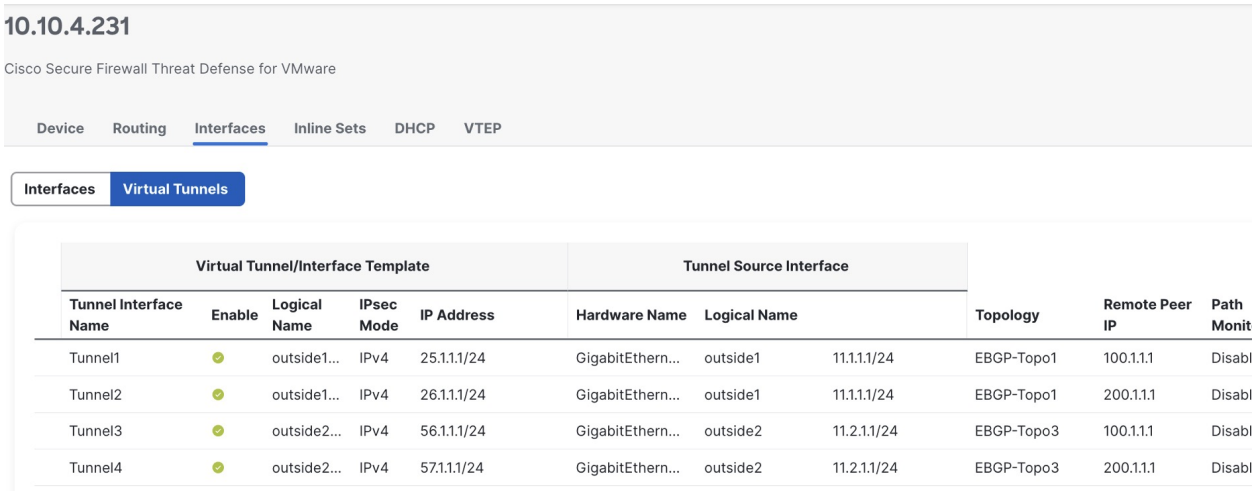
1. 选择**设备** > **设备管理**。
2. 点击中心或分支设备的编辑图标。
3. 点击**接口 (Interface)** 选项卡。
4. 点击**虚拟隧道 (Virtual Tunnels)** 选项卡。

   您可以查看每个 VTI 的详细信息，如名称、IP 地址、IPsec 模式、隧道源接口详细信息、拓扑结构和远程对等 IP。

下图显示了集线器的 DVTI 动态创建的虚拟接入接口示例：



下图显示了 SD-WAN 向导在轮辐上创建的静态隧道虚拟接口 (SVTI) 的示例：



SD-WAN 向导从中心的 IP 地址池将 IP 地址分配给这些隧道接口。

验证中心和分支上的路由

要验证 SD-WAN 拓扑的中心和辐射点的 BGP 配置，请执行以下操作：

1. 选择**设备** > **设备管理**。
2. 点击中心或分支设备的编辑图标。
3. 点击**设备 (Device)** 选项卡。
4. 点击 **常规 (General)** 卡中的 **CLI** 。系统将显示 **CLI 故障排除 (CLI Troubleshoot)** 窗口。
5. 在 **命令** 字段中输入以下命令，然后点击 **执行**：
   - **show route**
   - **show bgp summary**

SD-WAN 功能的使用案例

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。