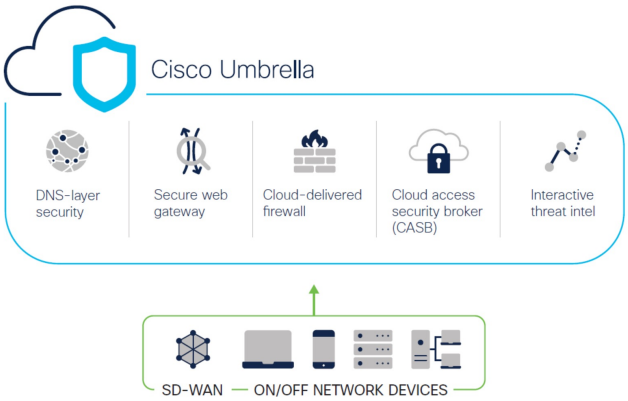
使用 Umbrella 自动隧道保护互联网流量

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

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 *1:* 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。

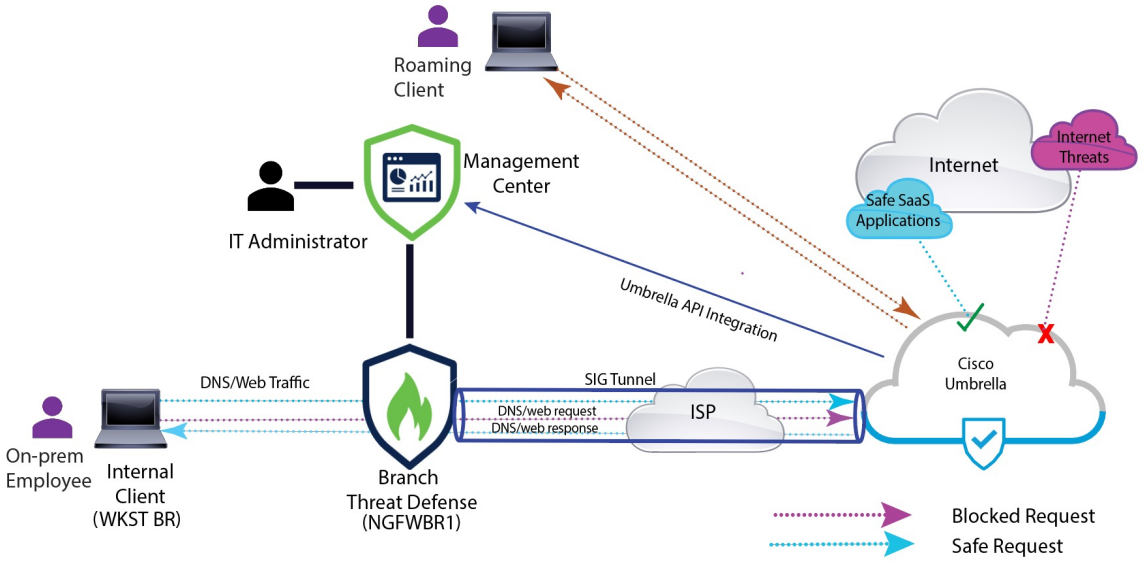
Sally 注意到某些网站现在被防火墙和 Umbrella 阻止了。

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 2: 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

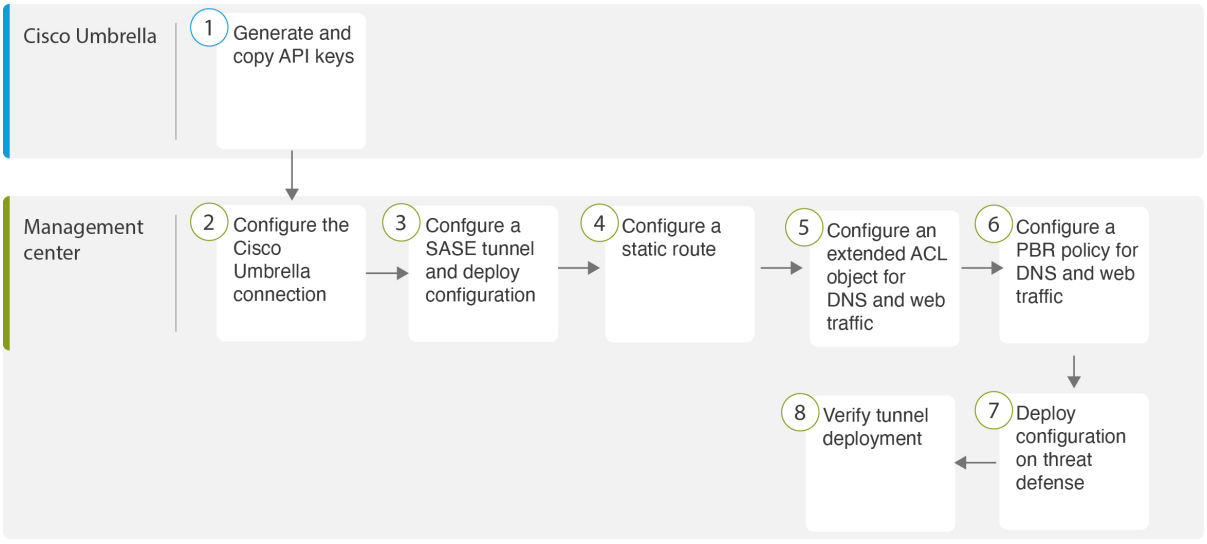
- 创建基本访问控制策略
- 您必须拥有 Cisco Umbrella 安全互联网网关 (SIG) 基础版订用或 SIG 免费试用版。
- 您必须启用具有出口控制功能的智能许可证帐户，才能从管理中心在 Umbrella 上部署隧道。
- 通过 http://login.umbrella.com Umbrella，获取与 Cisco Umbrella 建立连接所需的信息。确保管理中心可以访问 management.api.umbrella.com。
- 您必须在管理中心注册 Cisco Umbrella 组织，并在 Cisco Umbrella 连接高级设置中配置管理密钥和管理秘密。这将从 Cisco 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 7 页。
4	配置静态路由。请参阅 配置静态路由，第 10 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 11 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 12 页
7	在威胁防御上部署配置。请参阅 部署配置。
8	验证隧道部署。请参阅验证 SASE Umbrella 隧道部署，第 13 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 4 页 和 SASE Umbrella 隧道的最佳实践，第 4 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 10 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。

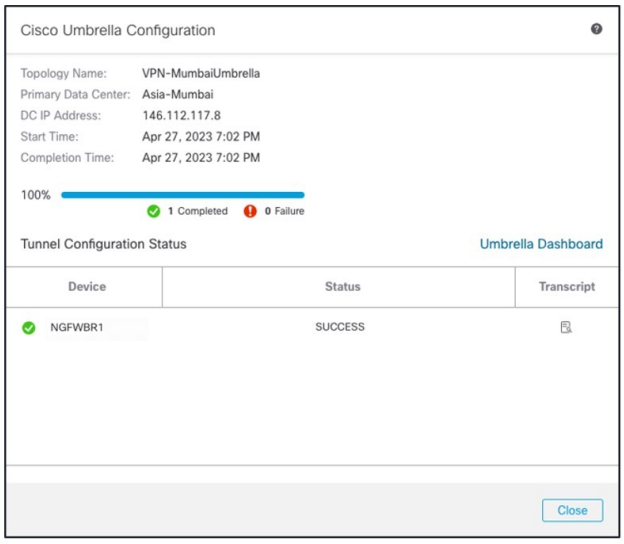
步骤 8 选中**在威胁防御节点上部署配置 (Deploy configuration on threat defense nodes)** 复选框，以触发将网络隧道部署到威胁防御。此部署只会在将隧道部署到 Umbrella 之后进行。威胁防御部署需要本地隧道 ID。

步骤 9 点击**保存 (Save)**。

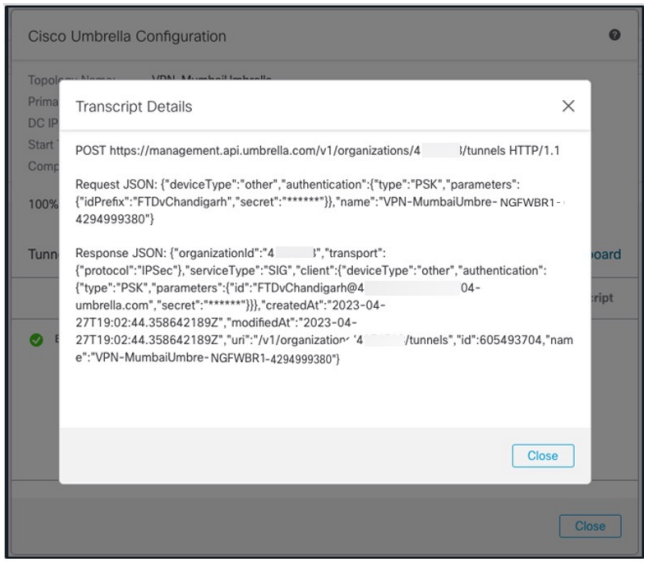
此操作：

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。

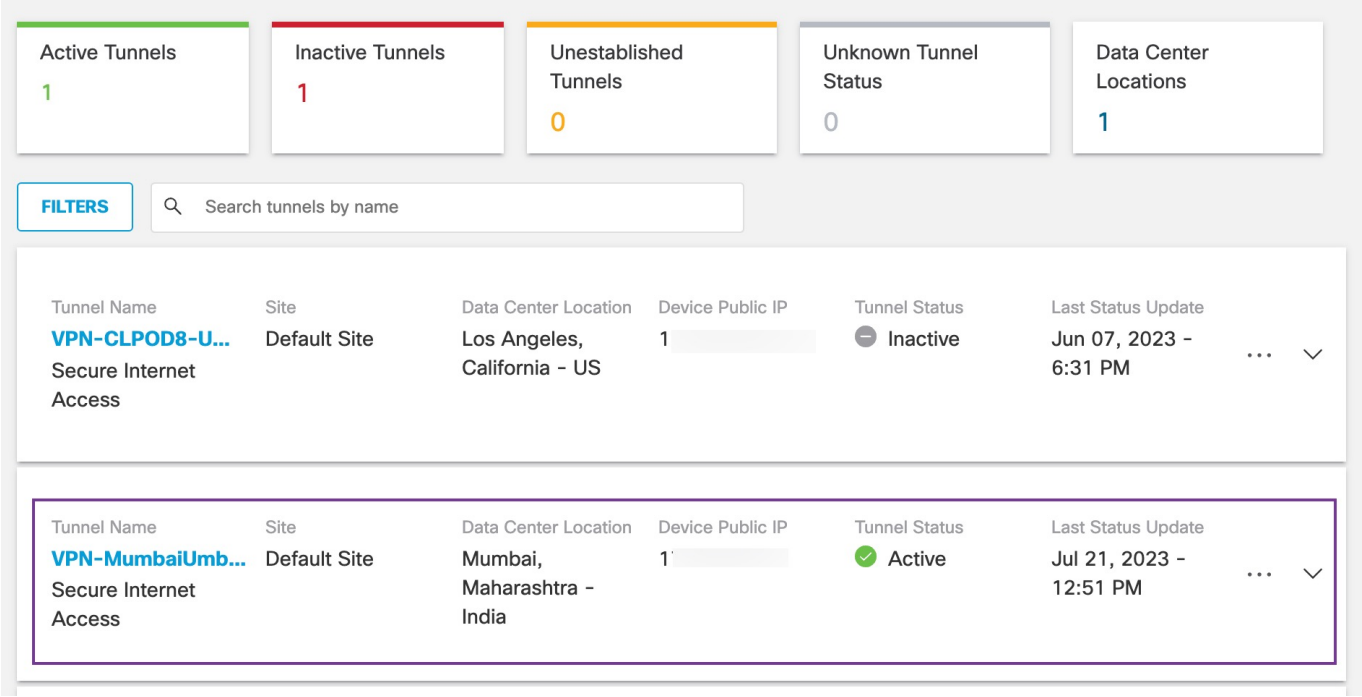
4. 打开 **Cisco Umbrella 配置 (Cisco Umbrella Configuration)** 窗口并显示 Umbrella 上的隧道部署状态。



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。

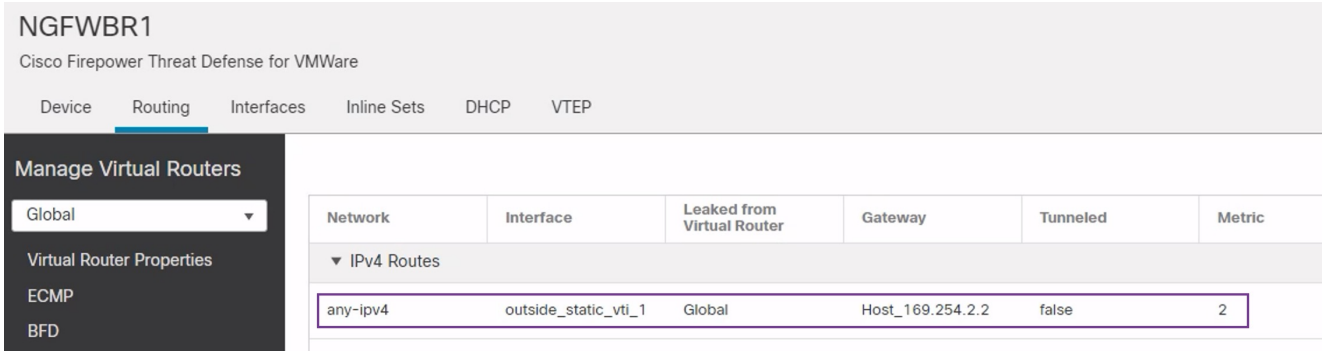
步骤 6 从**可用网络 (Available Networks)** 框中选择 **any-ipv4** 作为目标网络，然后点击**添加 (Add)**。

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。

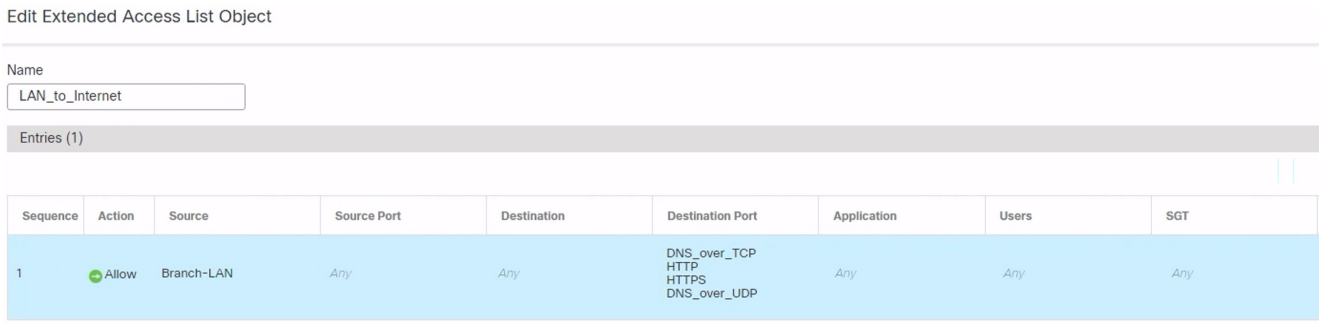
步骤 5 配置以下访问控制属性：

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)**。

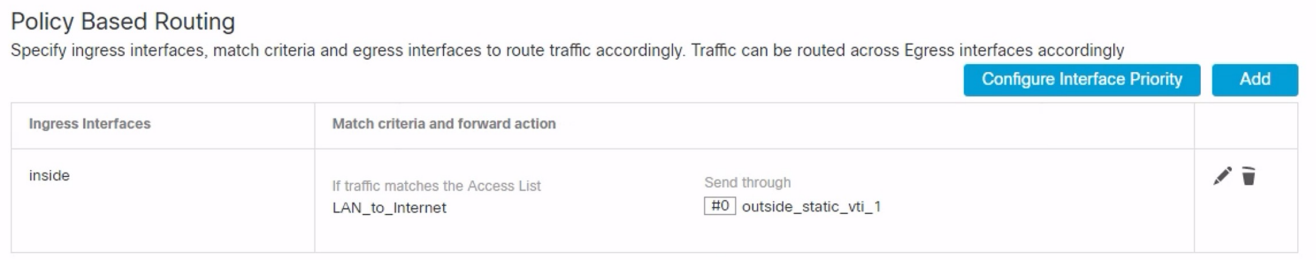
c) 在**可用接口 (Available Interfaces)** 中，点击 **Outside_static_vti_1** 接口旁边的 **添加**（➕） 图标，将其移至**所选出口接口**。

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)。

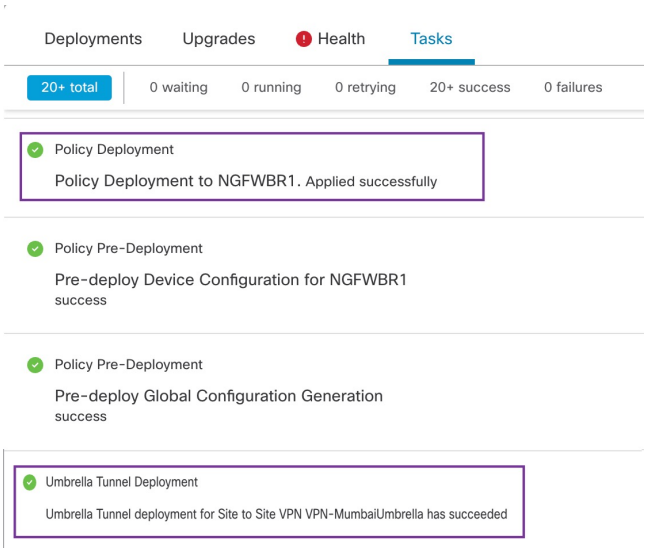
步骤 4 如果系统在要部署的更改中发现错误或警告，则会在**验证错误 (Validation Errors)** 或**验证警告 (Validation Warnings)** 窗口中显示它们。要查看完整的详细信息，请点击“验证错误”(Validation Errors) 或“验证警告”(Validation Warnings) 链接。

有以下选项可供选择：

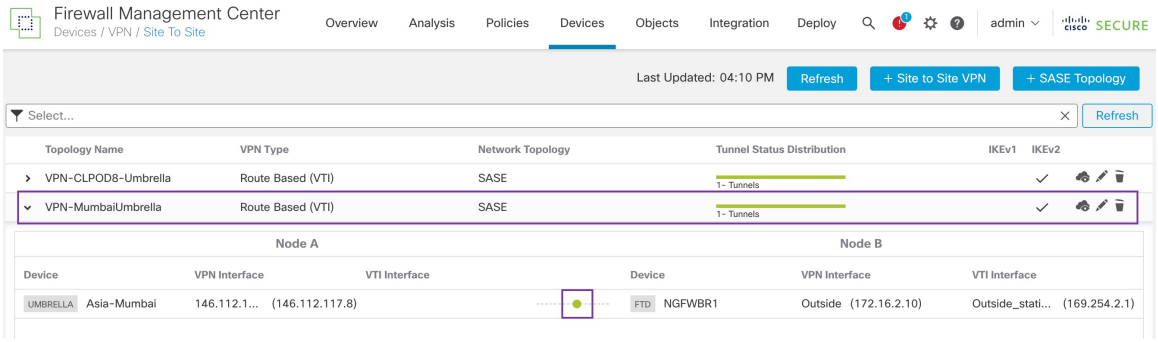
- 继续部署 - 继续部署而无需解决警告情况。如果系统识别错误，则无法继续。
- 关闭 - 退出而不部署。解决错误和警告情况，并尝试重新部署该配置。

验证 SASE Umbrella 隧道部署

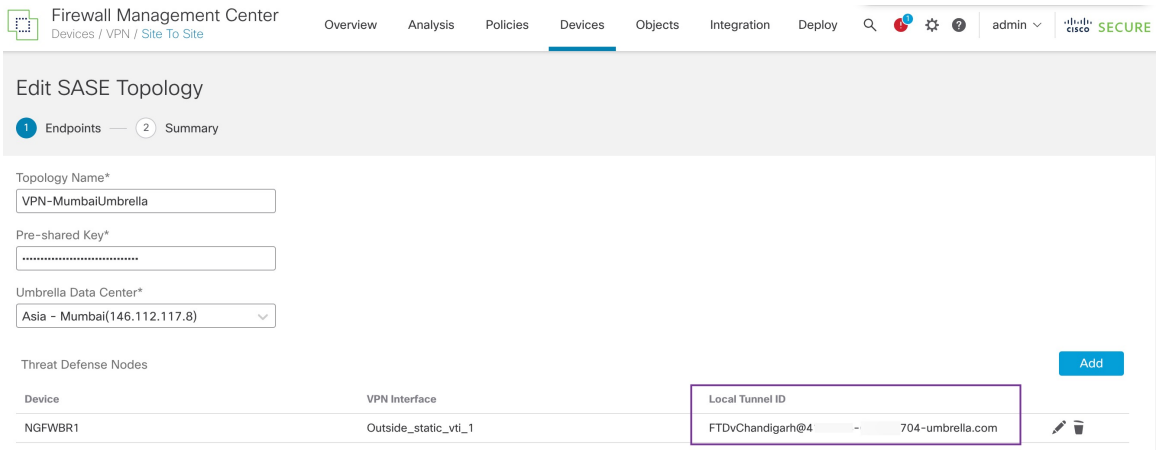
在管理中心，转至**通知 (Notifications)** > **任务 (Tasks)**，查看威胁防御设备 (NGFWBR1) 上的 Umbrella 隧道部署和策略部署状态。



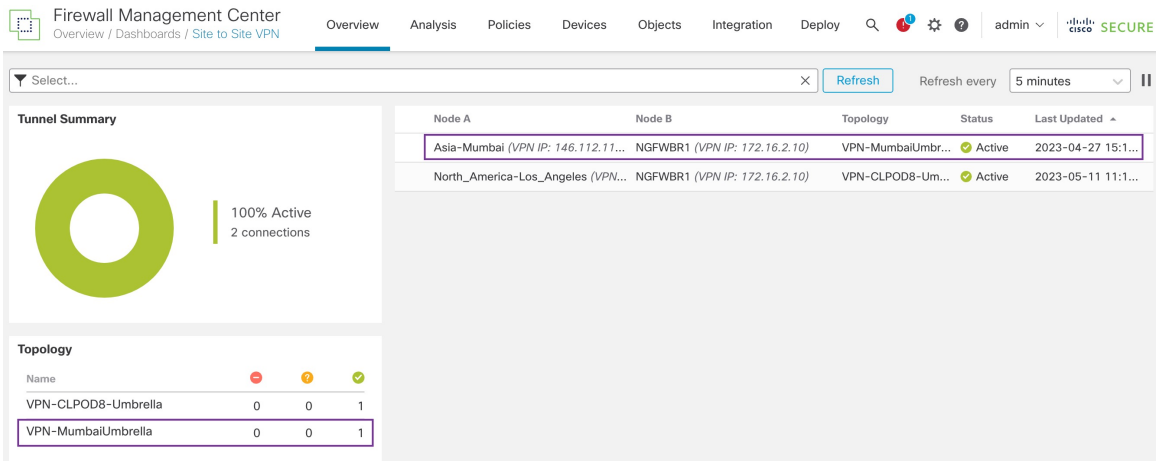
要在管理中心检查 SASE 自动隧道状态，请选择**设备 (Devices) > VPN > 站点间 (Site To Site)**。



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：

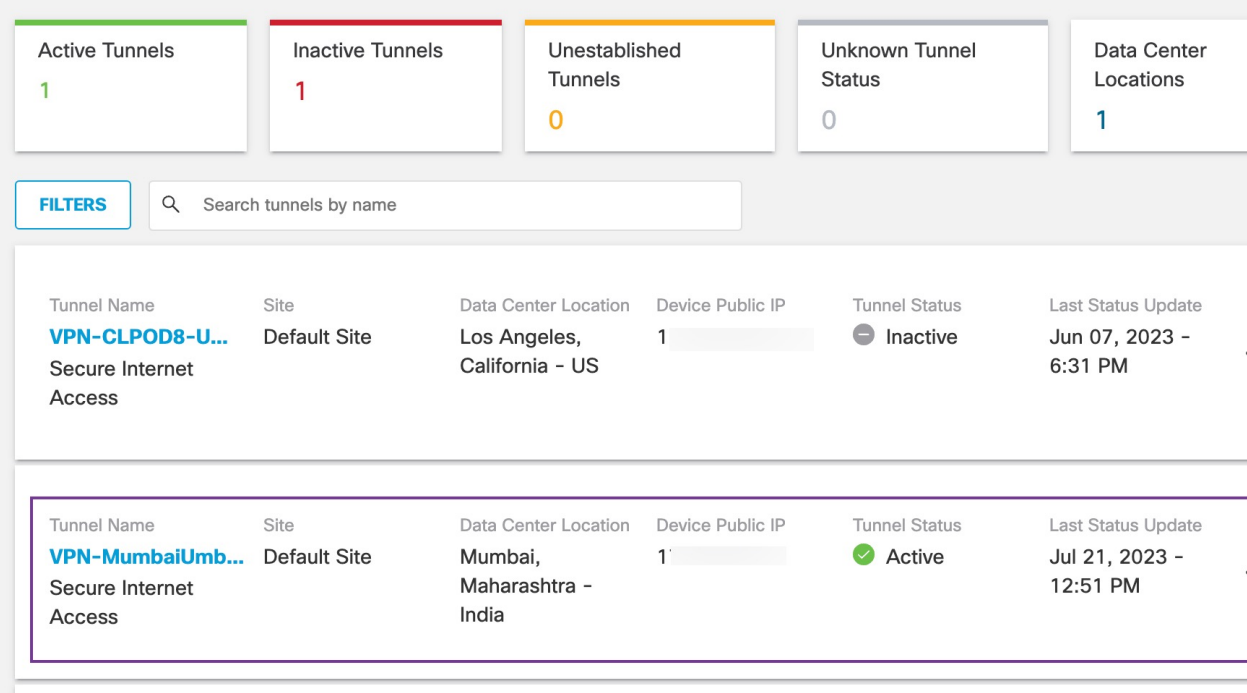
```
> show interface ip brief

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：

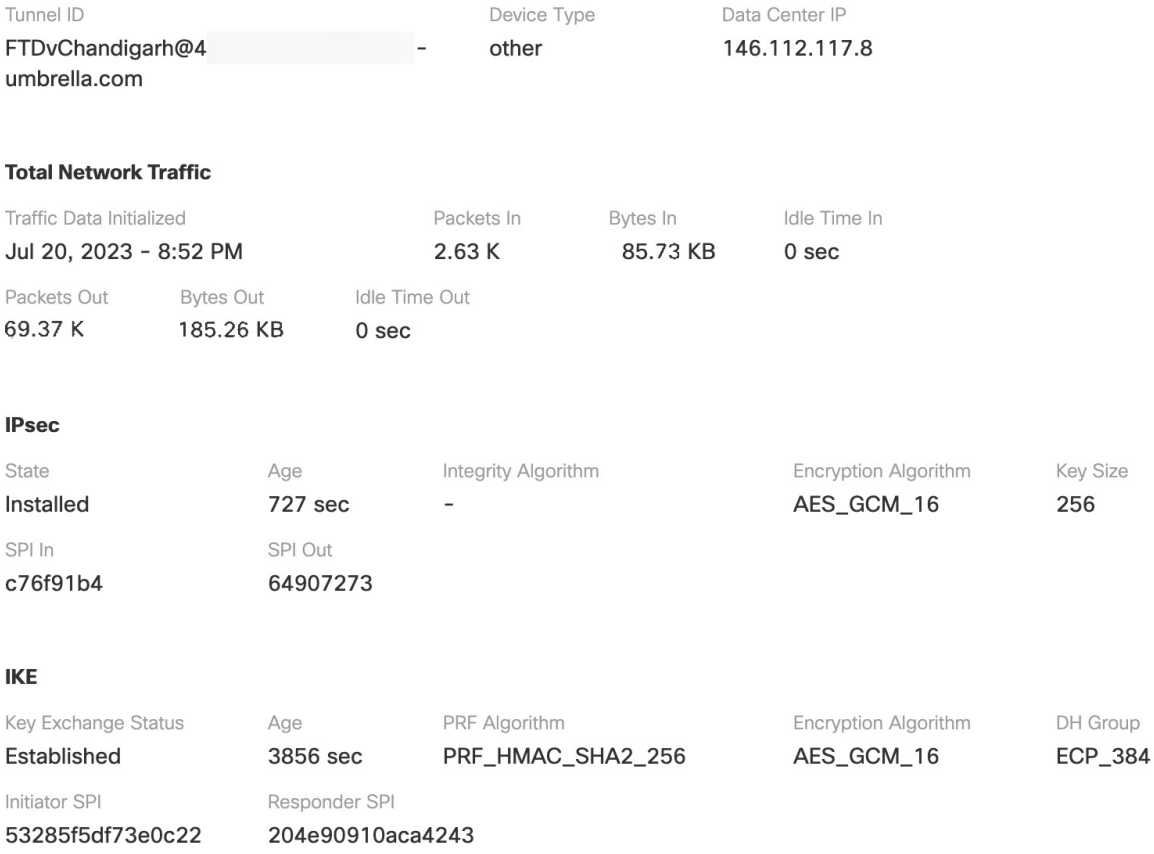
```
> show crypto ipsec sa
interface: outside_static_vti_1
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr:
198.18.128.81

      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

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。