使用Catalyst SD-WAN自动隧道配置安全访问以实现安全专用访问

目录

简介

本文档介绍如何使用Catalyst SD-WAN自动隧道配置安全访问以实现安全专用访问。

背景信息

随着组织突破传统的基于周界的网络，安全访问私有资源与保护互联网流量同样重要。应用不再局限于单个数据中心，它们现在跨内部部署环境、公共云和混合架构运行。这一转变要求采用更灵活、更现代的方式进行私有访问。

这正是基于SASE的架构和思科安全访问发挥作用的地方。思科安全接入不依赖于传统VPN集中器和平板网络访问，而是将私有连接作为云交付的服务提供，将VPN即服务(VPNaaS)和零信任网络访问(ZTNA)相结合。

对于网络级专用接入，思科安全接入使用自动化站点间IPsec隧道与SD-WAN集成。这些隧道允许私有流量在安全访问和内部或云网络之间安全流动，同时使安全检查和策略实施集中到云中。从运营角度来看，这消除了部署和维护传统VPN头端的需要，并简化了随环境增长进行的扩展。

在VPNaaS模式中，安全访问充当云中的VPN终端点。SD-WAN通过安全访问处理智能路由和恢复能力，并确保流量在到达私有资源之前受到一致的安全策略的保护和管理。

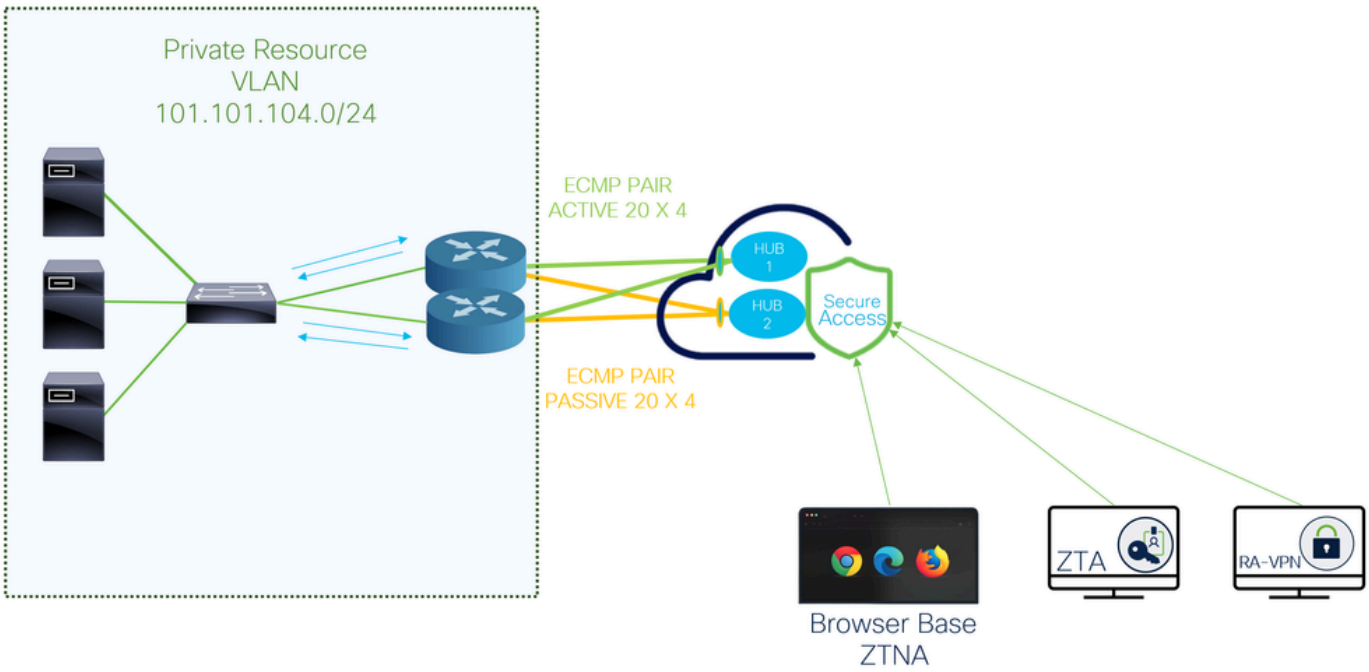
Cisco Secure Access还支持高级站点到站点隧道架构，包括多区域回程。此功能允许组织同时建立到多个安全访问区域的隧道，从而提供地理冗余和更高的可用性。通过连接到不同区域，流量可以在发生区域故障、延迟降低或维护事件时自动进行故障切换。

例如，组织可以建立从其SD-WAN环境到伦敦和德国安全接入区域的站点到站点隧道。两个隧道都保持活动状态，支持跨区域的弹性专用访问，即使一个区域不可用，也可确保连续性。这种多区域设计增强了高可用性，提高了容错能力，并符合企业级可复原性要求。

对于更精细的访问，思科安全访问实施零信任网络访问(ZTNA)模型。ZTNA不是授予用户广泛的网络连接，而是根据身份、设备状态和情景只允许访问特定应用。此方法可显着缩小攻击面，并遵循零信任原则。

通过站点到站点隧道和资源连接器的组合启用ZTNA访问。Resource Connectors是轻量级虚拟设备，用于建立到安全访问的仅出站连接，这意味着私有资源永远不需要直接暴露于互联网。

网络图



先决条件

要求

- 安全访问知识
- Cisco Catalyst SD-WAN Manager版本20.18.2和Cisco IOS XE Catalyst SD-WAN版本17.18.2或更高版本
- 有关路由和交换的中级知识
- ECMP知识
- VPN知识
- 由于此集成基于受控可用性，您需要提交TAC案例以请求在思科安全访问中启用此功能

使用的组件

- 安全访问租户
- Catalyst SD-WAN Manager版本20.18.2和Cisco IOS XE Catalyst SD-WAN版本17.18.2
- Catalyst SD-WAN管理器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

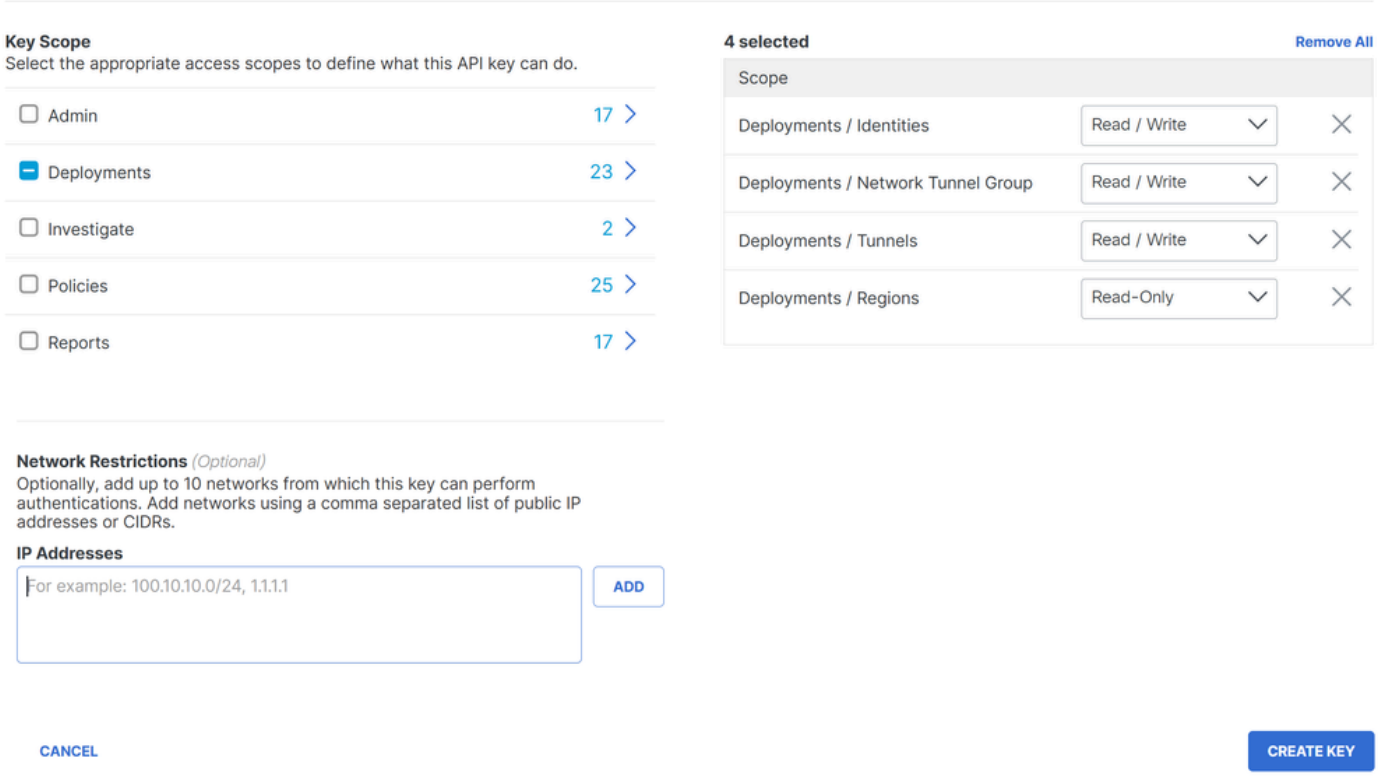
安全访问配置

API创建

要使用Secure Access创建自动隧道，请检查后续步骤：

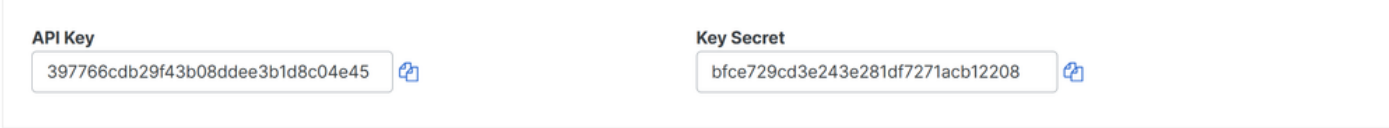
导航到[安全访问控制面板]。

- 点击 Admin > API Keys
- 点击 Add
- 选择下一个选项：
  - Deployments / Network Tunnel Group:读/写
  - Deployments / Tunnels:读/写
  - Deployments / Regions:只读
  - Deployments / Identities:读写
  - Expiry Date:永不过期



注意：或者，最多可添加10个网络，此密钥可以从这些网络执行身份验证。使用逗号分隔的公有IP地址或CIDR列表添加网络。

- 单击CREATE KEY，完成和的API Key创Key Secret。



警告：在点击之前将其复制ACCEPT AND CLOSE;否则，您需要重新创建它们，并删除未复制的。

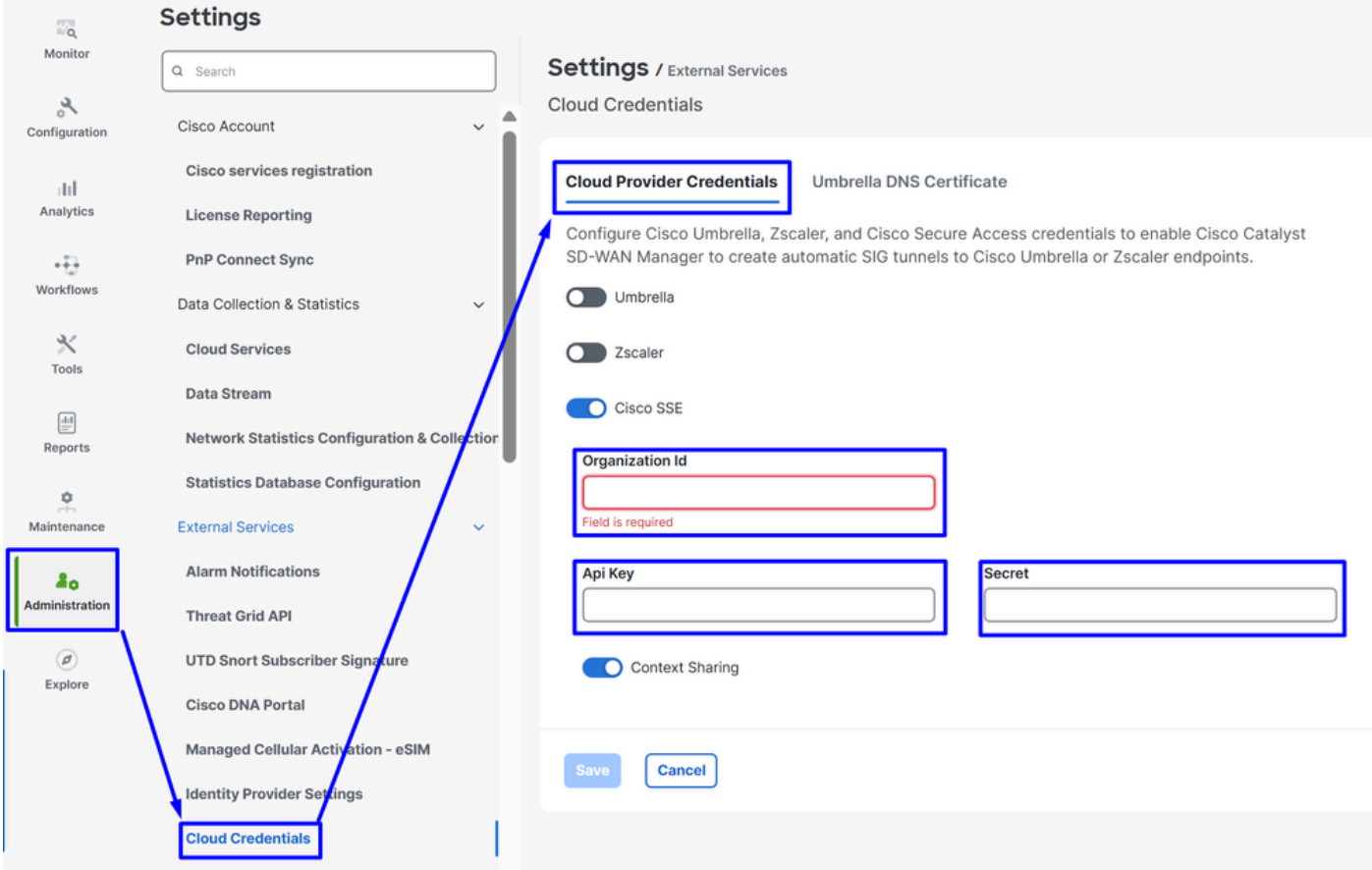
然后单击ACCEPT AND CLOSE。

SD-WAN配置

API集成

导航至Catalyst SD-WAN Manager:

- 单击**Administration**>Settings > Cloud Credentials
- 然后点击Cloud Provider Credentials ，启用Cisco SSE并填充API和组织设置



- **Organization ID**:您可以从SSE控制面板的URL获取https://dashboard.sse.cisco.com/org/xxxxx
- Api Key:从安全访问配置步骤复制它
- Secret：从Secure Access Configuration（安全访问配置）步骤复制它

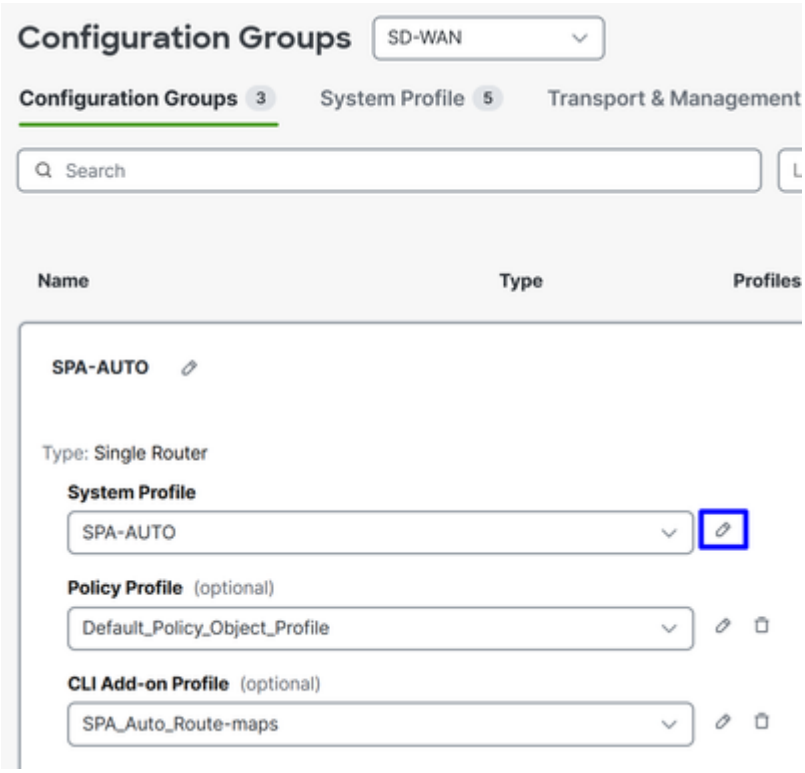
然后，点击按钮Save。

注意：在继续后续步骤之前，您需要确保SD-WAN Manager和Catalyst SD-WAN Edge具有DNS解析和互联网访问。

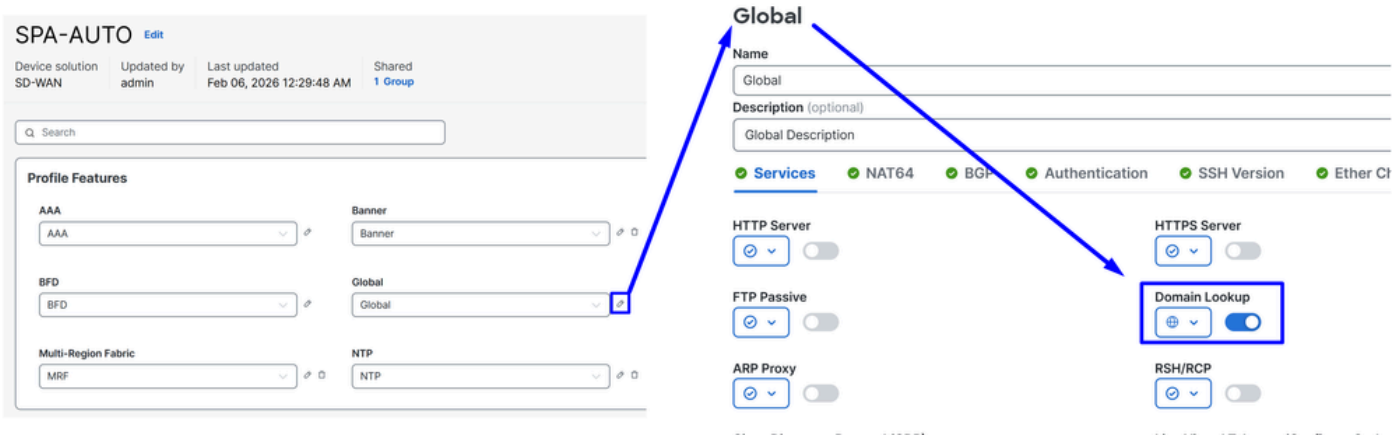
要检查是否启用了DNS查找，请导航至：

- 单击Configuration > Configuration Groups

- 点击边缘设备的配置文件并编辑系统配置文件



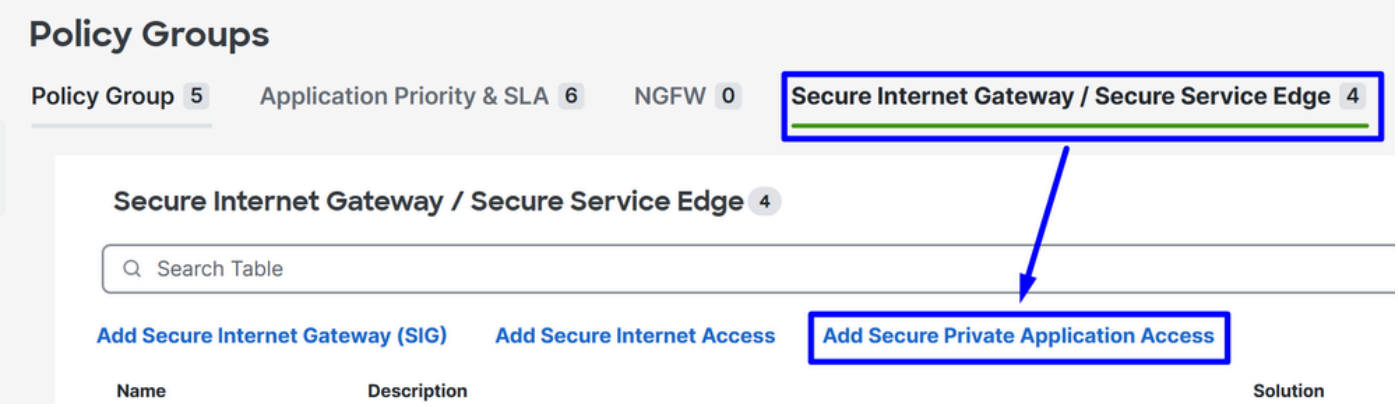
- 然后编辑Global选项，并确保启用选项Domain Resolution



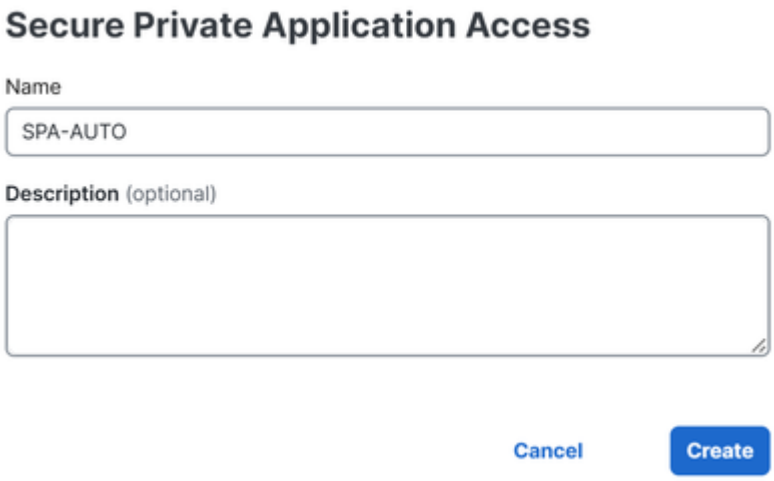
配置策略组

导航到Configuration > Policy Groups:

- 点击Secure Internet Gateway / Secure Service Edge>*Add Secure Private Access*



- 配置名称并单击 Create

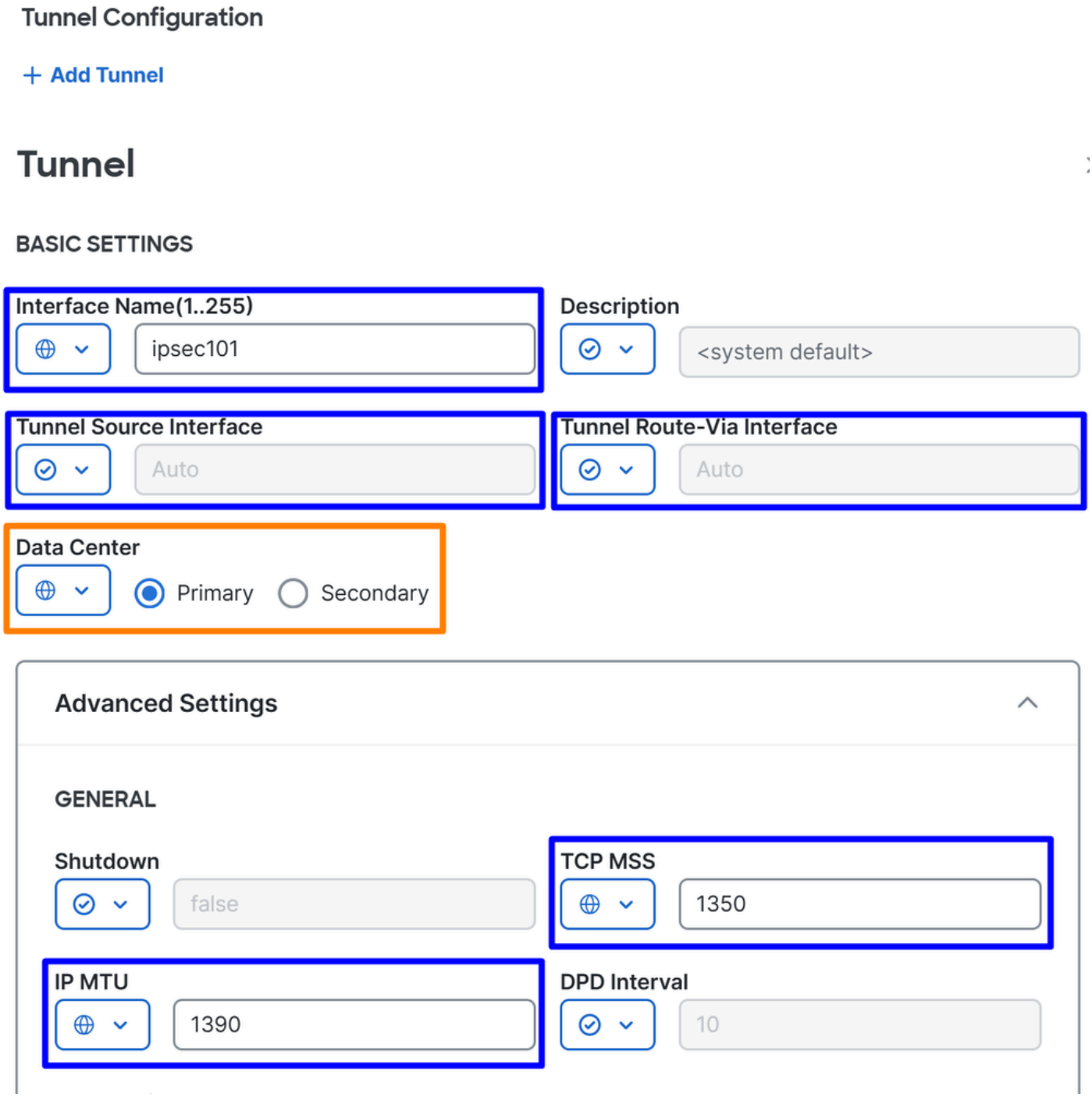


接下来的配置允许您在Catalyst SD-WAN Edge中部署配置后创建隧道：

- Configuration
  - Segment (VPN):选择托管要通过安全访问的应用的VRF
  - Cisco Secure Access Region:选择距离托管应用的SD-WAN集线器或分支机构最近的区域

接下来，定义隧道配置。创建至主要安全访问数据中心的隧道处于活动状态，而创建至辅助安全访问数据中心的隧道则作为备份运行。

在Tunnel Configuration下，单击+ Add Tunnel:



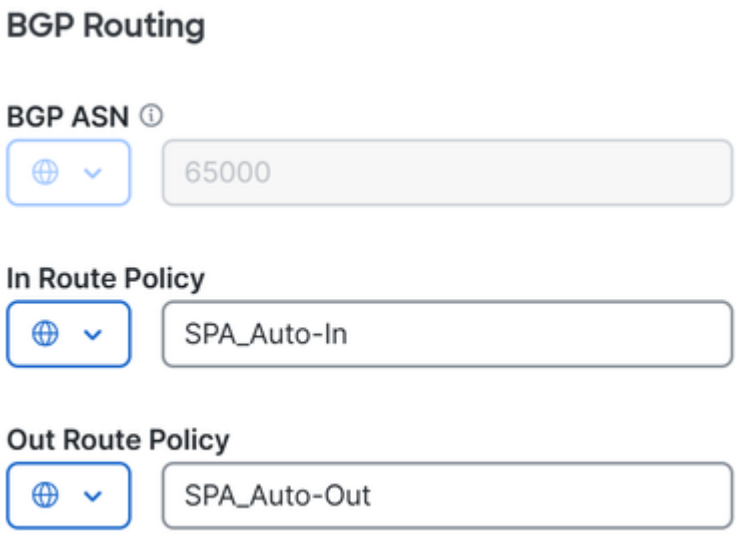
- Tunnel
  - Interface Name：指定隧道名称，每次添加新隧道时都会自动更新该名称
  - Tunnel Source Interface:您无需更改此设置。如果保留为Auto，系统会自动创建带有/31掩码的环回接口。
  - Tunnel Route-Via Interface:无需更改此设置。默认情况下，它使用边缘路由器上的第一个NATed物理WAN接口，但如果需要特定的WAN接口，则可以更改它
  - Data Center：相应选择Primary或Secondary。如果已经配置了主隧道，请选择Secondary。在正常情况下，一个隧道可配置为主隧道，另一个隧道配置为辅助隧道
  - Advanced Settings
    - IP MTU:使用1390
    - TCP MSS:使用1350

注意：如果要创建多个隧道以启用ECMP并增加隧道容量，则可以为每台路由器配置最多10个活动/10个备份隧道。每个NTG提供高达10 × 4 Gbps的带宽。

Interface Name	Description	Tunnel Source Interface	Tunnel Route-Via Interface	Data Center	Action	
ipsec101		Auto	Auto	Primary		
ipsec102		Auto	Auto	Secondary		
ipsec103		Auto	Auto	Primary		
ipsec104		Auto	Auto	Secondary		
ipsec105		Auto	Auto	Primary		
ipsec106		Auto	Auto	Secondary		
ipsec107		Auto	Auto	Primary		
ipsec108		Auto	Auto	Secondary		
ipsec109		Auto	Auto	Primary		MAXIMUM OF 10 TUNNELS PER HUB
ipsec110		Auto	Auto	Secondary		10 x 1 Primary
ipsec111		Auto	Auto	Primary		10 x 1 Secondary
ipsec112		Auto	Auto	Secondary		
ipsec113		Auto	Auto	Primary		
ipsec114		Auto	Auto	Secondary		
ipsec115		Auto	Auto	Primary		
ipsec116		Auto	Auto	Secondary		
ipsec117		Auto	Auto	Primary		
ipsec118		Auto	Auto	Secondary		
ipsec119		Auto	Auto	Primary		
ipsec120		Auto	Auto	Secondary		

注意：如果为每台路由器部署多个隧道，请确保传输接口可以保持所有活动隧道的总带宽。例如，如果两个隧道预计每个传输速度最高为1 Gbps，则传输链路必须支持至少2 Gbps的吞吐量。

配置隧道后，继续执行BGP配置。



- **BGP Routing**
  - BGP ASN:指定SD-WAN集线器的AS编号。AS服务64512留用于安全访问，不能使用。有关BGP的详细信息，请参阅
  - In Route Policy:系统使用语句自动创建此入站路由策略deny all，以防止路由问题。必须通过手动修改该路由CLI Add-On Template，才能允许/拒绝相应的路由。
  - Out Route Policy:deny all 系统使用语句创建此出站路由策略以避免路由问题。必须通过手动编辑该策略以允许CLI Add-On Template/拒绝相应的路由。

警告：从2025年11月开始，所有新创建的安全访问组织默认使32644公共ASN组用于网络隧道组中的BGP对等。在2025年11月之前建立的现有组织继续使用之前为64512全访问BGP对等体保留的私有ASN路由。如果私有AS编号64512分配给网络上的设备，则它无法与为对等体（安全访问）BGP AS 64512配置的网络隧道组对等。

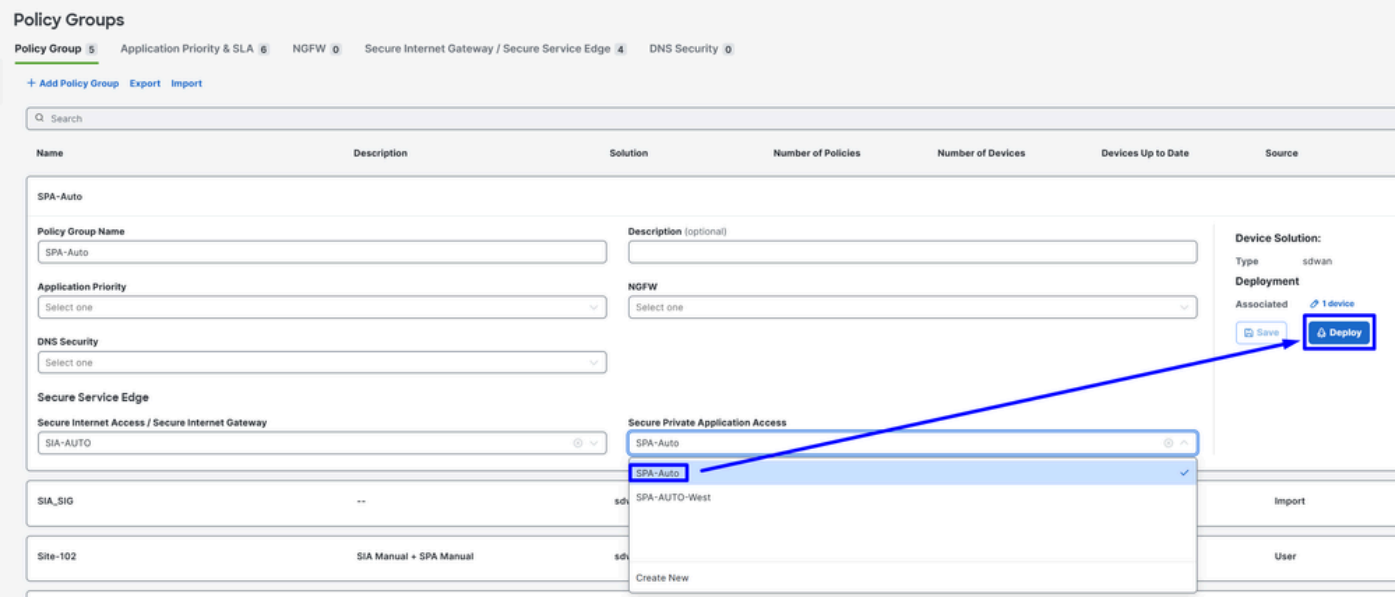
在中BGProute-map创建新策略后，将为每个BGP邻居Deploy自动创建下一个和配Policy Group。

```
route-map SPA_Auto-In deny 65534
 description Default Deny Configured from Secure Private Application Access feature
route-map SPA_Auto-Out deny 65534
 description Default Deny Configured from Secure Private Application Access feature

R104#sh run | s r b
router bgp 65000
bgp log-neighbor-changes
!
address-family ipv4 vrf 10
 neighbor 169.254.0.3 remote-as 64512
 neighbor 169.254.0.3 activate
 neighbor 169.254.0.3 send-community both
 neighbor 169.254.0.3 route-map SPA_Auto-In in
 neighbor 169.254.0.3 route-map SPA_Auto-Out out
 ...
 maximum-paths 32
exit-address-family
```

然后，点击Save，继续执行策略部署以启用隧道。

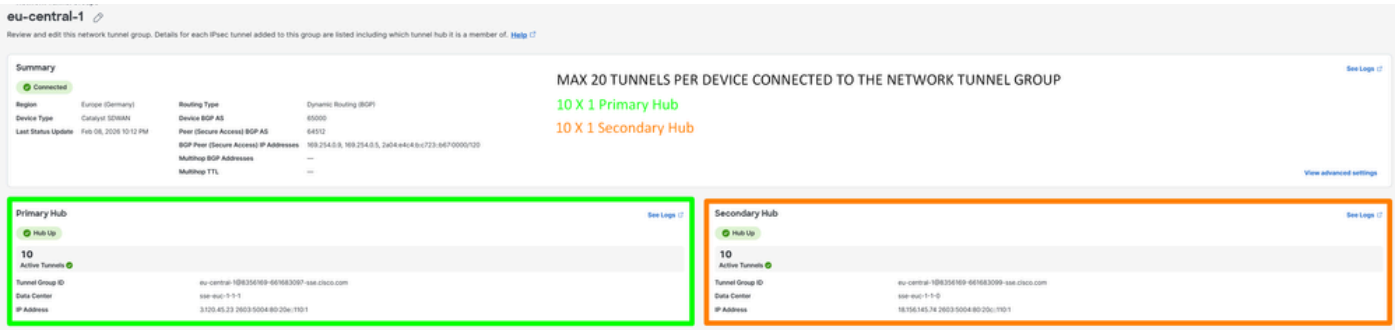
- 单击Configuration> Policy Groups
- 在PolicySecure Service Edge > >下选择，然后单击Secure Private Application Access最近为SPA创建的配置文件。
- 点击Deploy以完成



要在中验证Secure Access，请执行以下步骤：

- 点击Connect> Network Connections

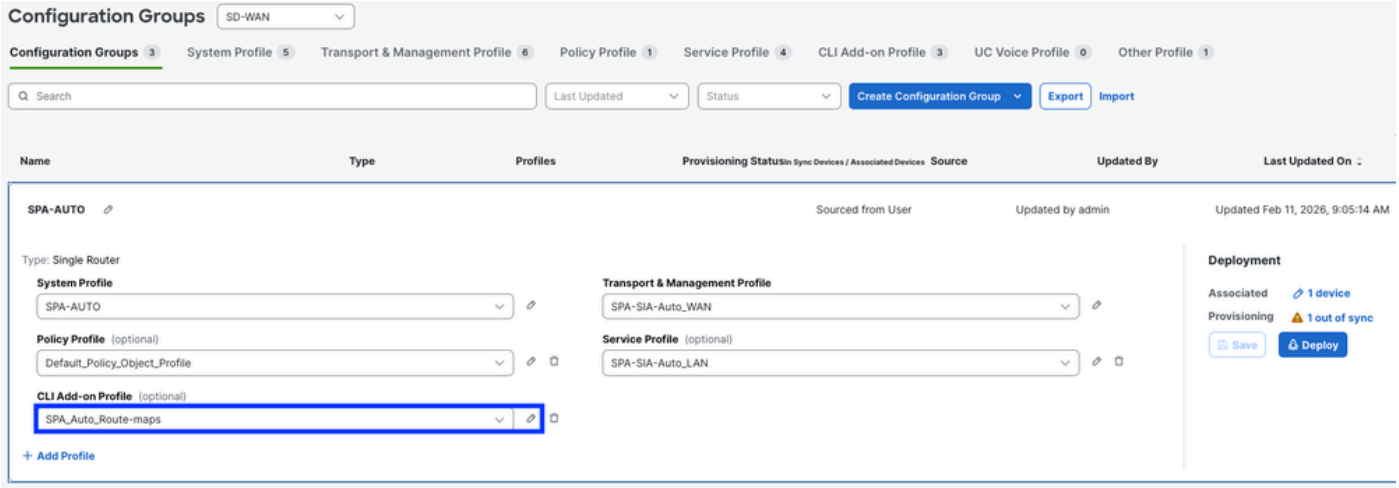
隧道建立



配置路由

导航至Configure> Configuration Groups

- 点击您的Configuration Group，然后创建/编辑 CLI Add-on Profile



要允许BGP路由交换，请使用之前配置的In Route Policy和**Out Route Policy**。 您可以找到路由配置的一个基本CLI Add-On示例。此模板提供了一个起点，必须根据需要进行自定义：

```
ip bgp-community new-format
ip prefix-list ALL-ROUTES seq 5 permit 0.0.0.0/0 le 32

route-map SPA_Auto-In permit 10
match ip address prefix-list ALL-ROUTES
route-map SPA_Auto-In deny 65534
description Default Deny Configured from Secure Private Application Access feature

route-map SPA_Auto-Out permit 10
match ip address prefix-list ALL-ROUTES
description Default Deny Configured from Secure Private Application Access feature
route-map SPA_Auto-Out deny 65534
description Default Deny Configured from Secure Private Application Access feature

router bgp 65000
bgp log-neighbor-changes
!
address-family ipv4 vrf 10
network 172.16.104.0 mask 255.255.255.0
```

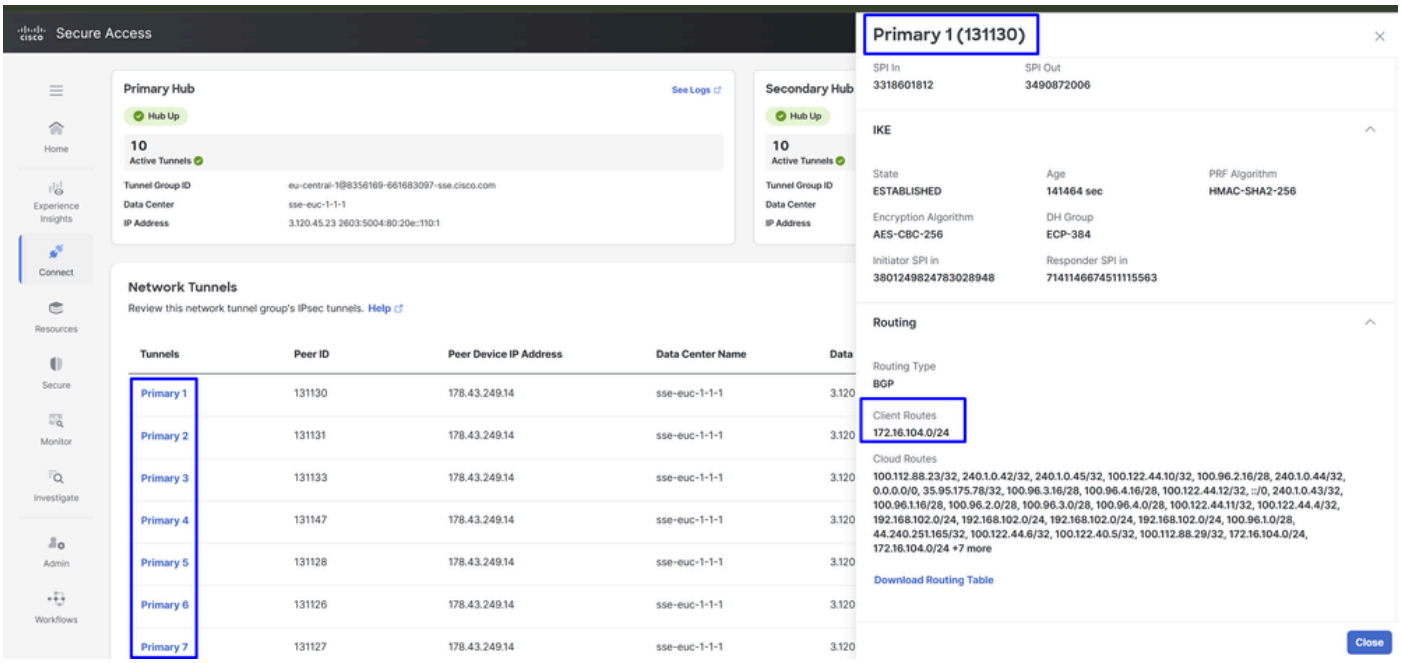
警告：在定义允许通过BGP路由映射传入和传出的网络时，需要仔细规划。如以上示例所示，允许所有路由可能导致意外的路由行为。为实现最佳部署，请在路由映射中仅明确指定必要的网络，以确保路由结果可控制且可预测

现在您可以继续 Deploy the changes

要验证是否在中收到BGP路由Secure Access，请检查后续步骤：

- 单击Connect> Network Connections > Network Tunnel Groupsselect 和NTG名称

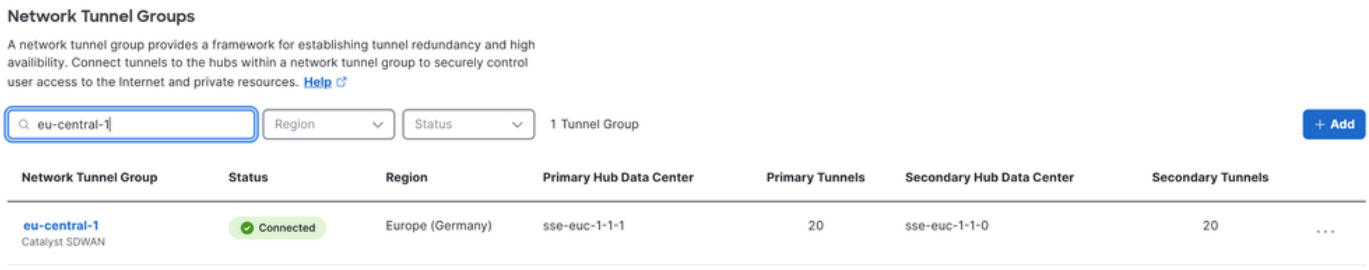
路由建立



注意：在本示例中，企业用户子网172.16.104.0/24通过BGP通告到安全访问。这允许在Catalyst SD-WAN和SSE环境之间正确路由。

同一策略可以应用于Catalyst SD-WAN集线器中的两个WAN边缘，从而产生20个活动隧道和20个备用隧道。隧道总数取决于每个边缘上配置的数量。连接到两个安全接入集线器（集线器1和集线器2）的任何路由器都会在所有已建立的隧道中形成一个ECMP对。

例如，如果Catalyst SD-WAN Edge 1有10个隧道，而Catalyst SD-WAN Edge 2有10个隧道，则Secure Access将在20个活动隧道中形成ECMP。此行为同样适用于辅助SSE集线器。

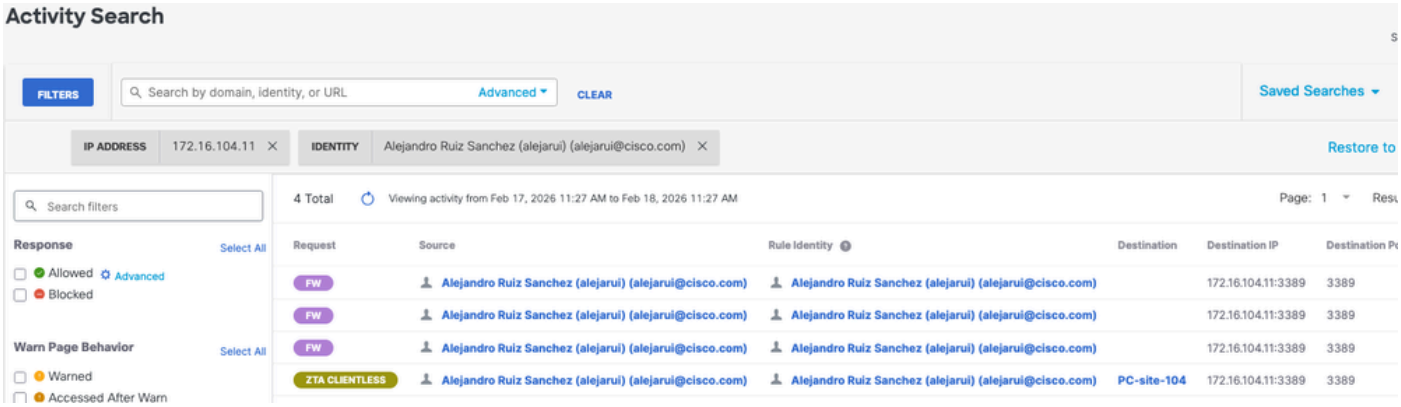


验证

要验证流量是否通过Cisco安全访问，请导航到Events或Activity Search，然Network-Wide Path Insights后按隧道身份过滤：

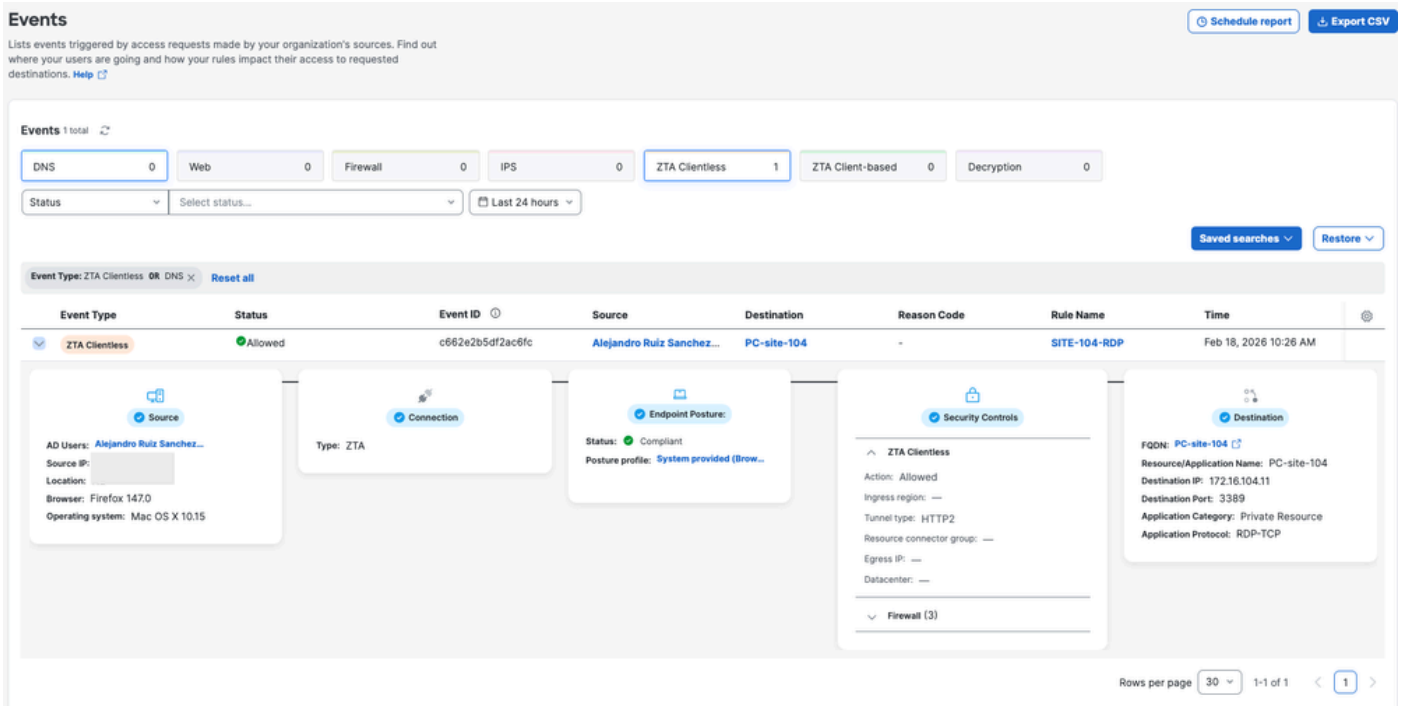
安全访问 — 活动搜索

导航至Monitor>Activity Search：



安全访问 — 事件

导航至Monitor>Events:

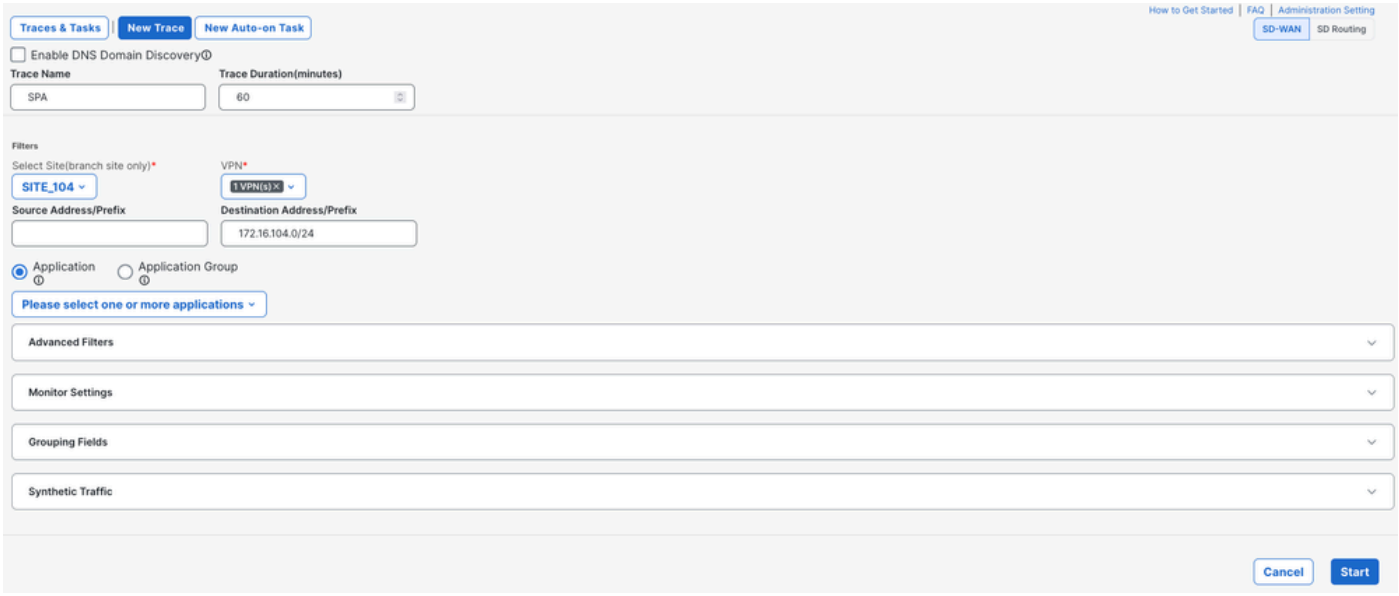


注意：确保您的默认策略已启用日志记录，默认情况下已禁用。

Catalyst SD-WAN Manager — 网络范围路径分析

导航至Catalyst SD-WAN Manager:

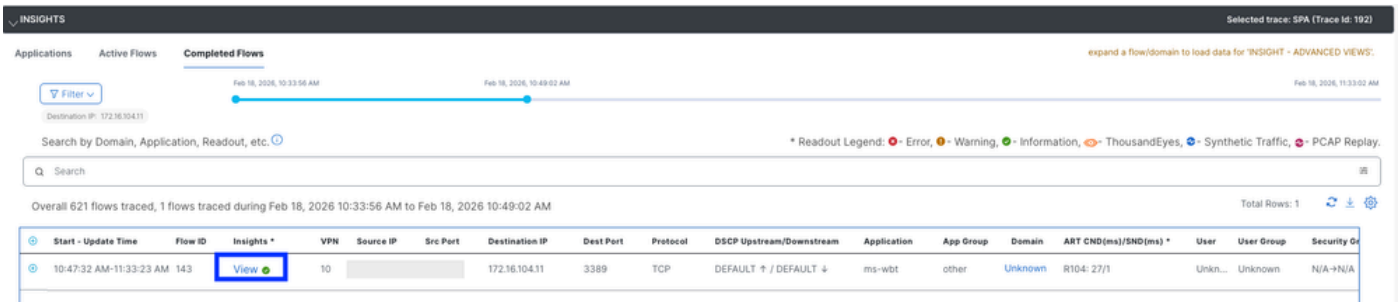
- 点击Tools> Network-Wide Path Insights
- 点击 New Trace



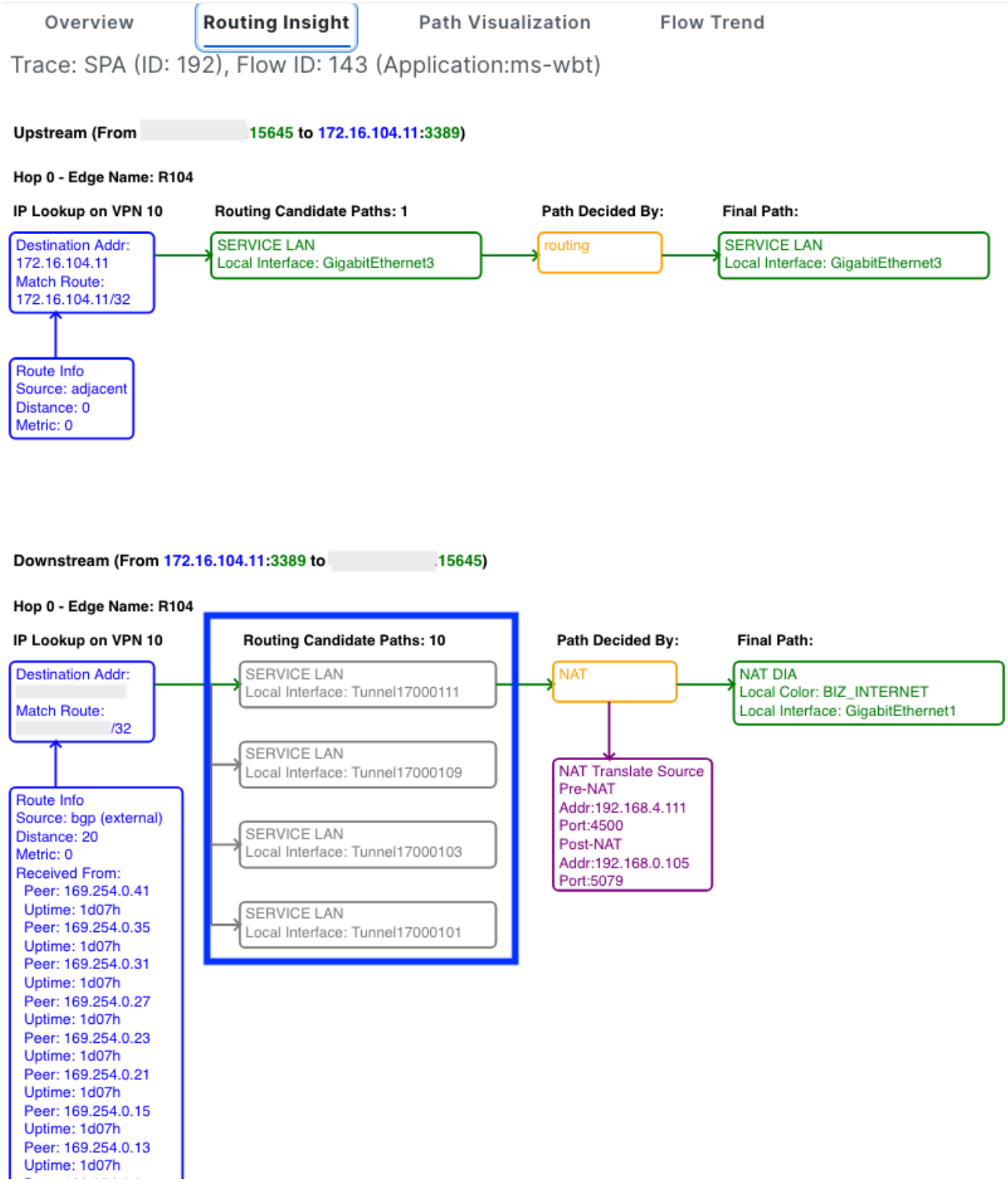
- Trace Name:（可选）指定跟踪名称
- Site:选择私有资源所在的站点
- VPN:选择专用资源所在的VPN ID
- Source/Destination Address:（可选）输入IP或将其保留为空白，以捕获根据和选择过滤的所Site有VPN流量

启动跟踪

找到流量并点击见解列上的查看



routing Insights列显示候选路径并显示用于安全访问的IPSec隧道



相关信息

- 思科技术支持和下载
- 思科安全访问帮助中心
- Cisco SASE设计指南
- 使用SD-WAN自动隧道配置安全访问，以实现安全的互联网访问
- Cisco Catalyst SD-WAN安全配置指南，Cisco IOS XE Catalyst SD-WAN版本17.x

- Cisco SASE解决方案：与思科安全访问集成的Cisco Catalyst SD-WAN概览

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。