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

目录

简介

背景信息

网络图

先决条件

- 要求
- 使用的组件

配置

- 安全访问配置
  - API创建
- SD-WAN配置
  - API集成
  - 配置策略组
- 在SD-WAN中创建自定义绕行FQDN或应用（可选）
- 路由流量

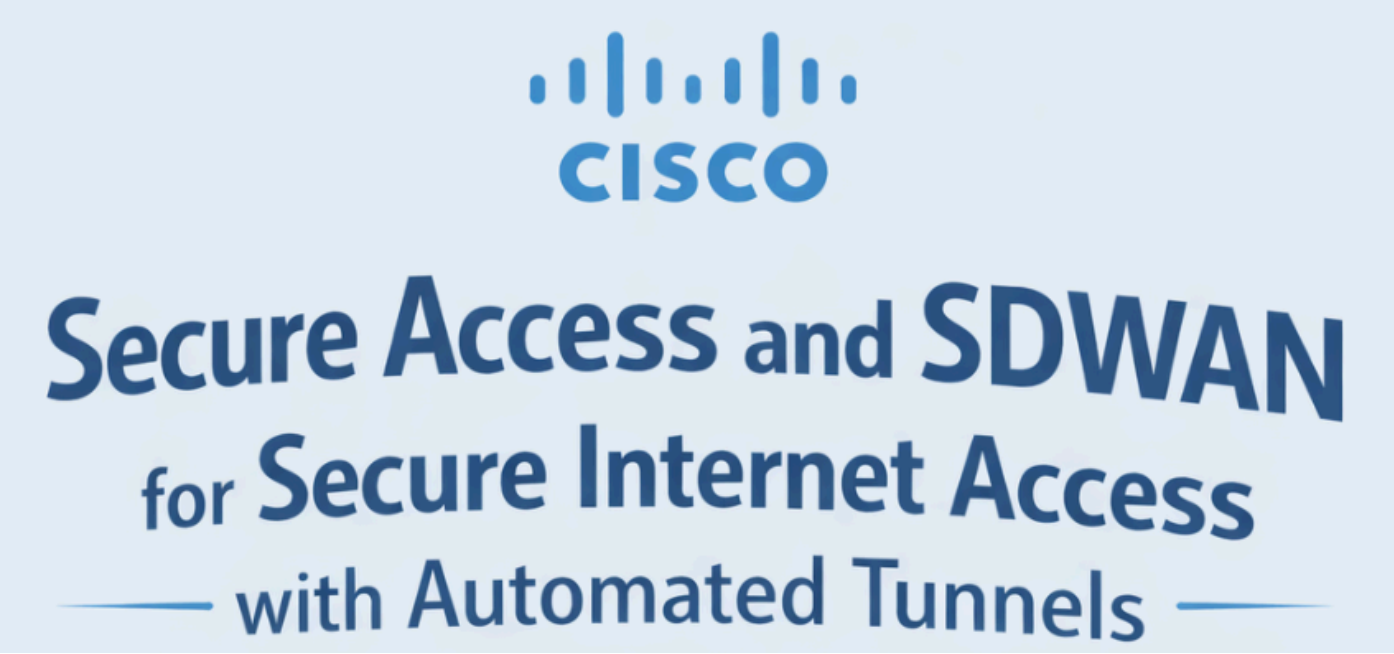
验证

- 安全访问 — 活动搜索
- 安全访问 — 事件
- Catalyst SD-WAN Manager — 网络范围路径分析

相关信息

简介

本文档介绍如何使用SD-WAN自动隧道配置安全访问以实现安全互联网访问。



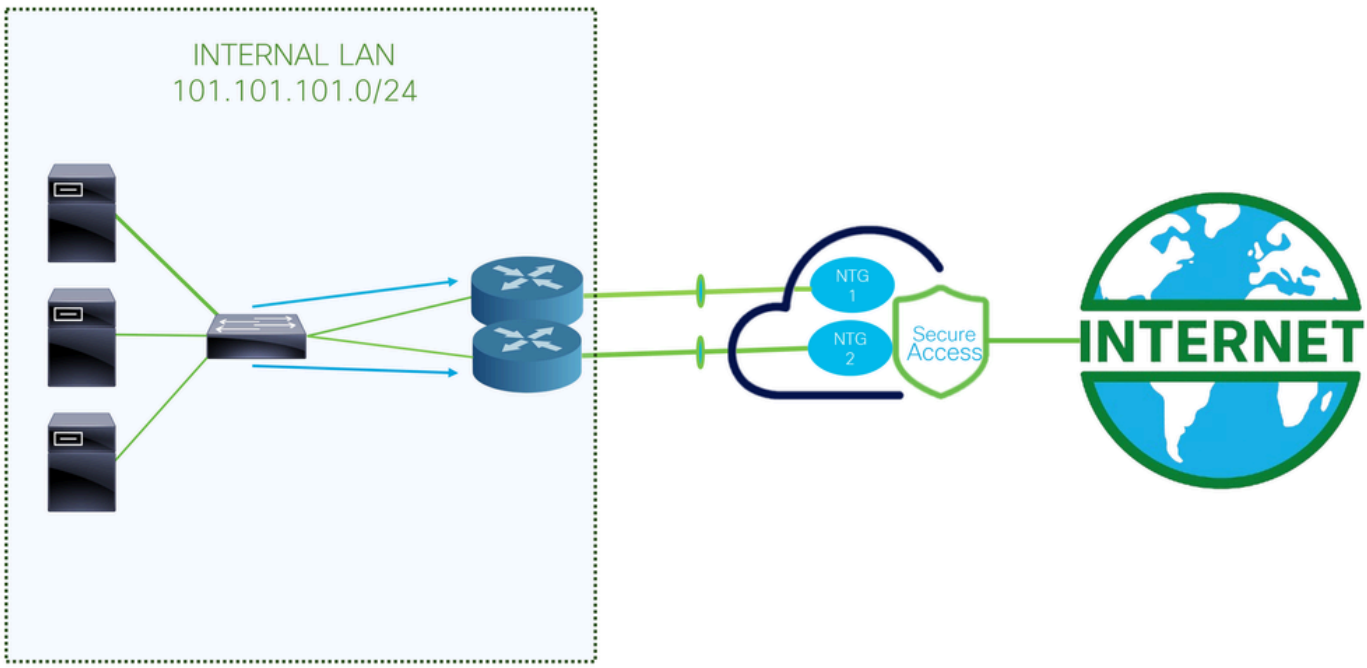
背景信息

随着组织越来越多地采用基于云的应用并支持分布式员工，网络架构必须不断发展以提供安全、可靠且可扩展的资源访问。安全访问服务边缘(SASE)是将网络和安全整合到单个云交付服务的框架，它将SD-WAN功能与高级安全功能(如安全网络网关(SWG)、云访问安全代理(CASB)、DNS层安全、零信任网络访问(ZTNA)或用于安全远程访问的集成VPN相结合。

通过自动隧道将思科安全接入与SD-WAN相集成，使组织能够安全高效地路由互联网流量。SD-WAN提供跨分布式位置的智能路径选择和优化连接，而思科安全访问确保在访问互联网之前，所有流量都根据公司安全策略得到检测和保护。

通过自动化SD-WAN设备和安全访问之间的隧道配置，组织可以简化部署、提高可扩展性并确保用户无论身在何处都能实施一致的安全措施。此集成是现代SASE架构的关键组件，支持分支机构、远程站点和移动用户的安全互联网访问。

网络图



这是用于此配置示例的架构。如您所见，有两台边缘路由器：

如果选择将策略部署到两个不同的设备，则为每个路由器配置一个NTG，并在安全访问端启用NAT。这样，两台路由器可以通过隧道发送来自同一源的流量。通常，这是不允许的；但是，对这些隧道启用NAT选项允许两个边缘路由器发送源自同一源地址的流量。

先决条件

要求

- 安全访问知识
- Cisco Catalyst SD-WAN Manager版本20.15.1和Cisco IOS XE Catalyst SD-WAN版本17.15.1或更高版本
- 有关路由和交换的中级知识
- ECMP知识
- VPN知识

使用的组件

- 安全访问租户
- Catalyst SD-WAN Manager版本20.18.1和Cisco IOS XE Catalyst SD-WAN版本17.18.1
- 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

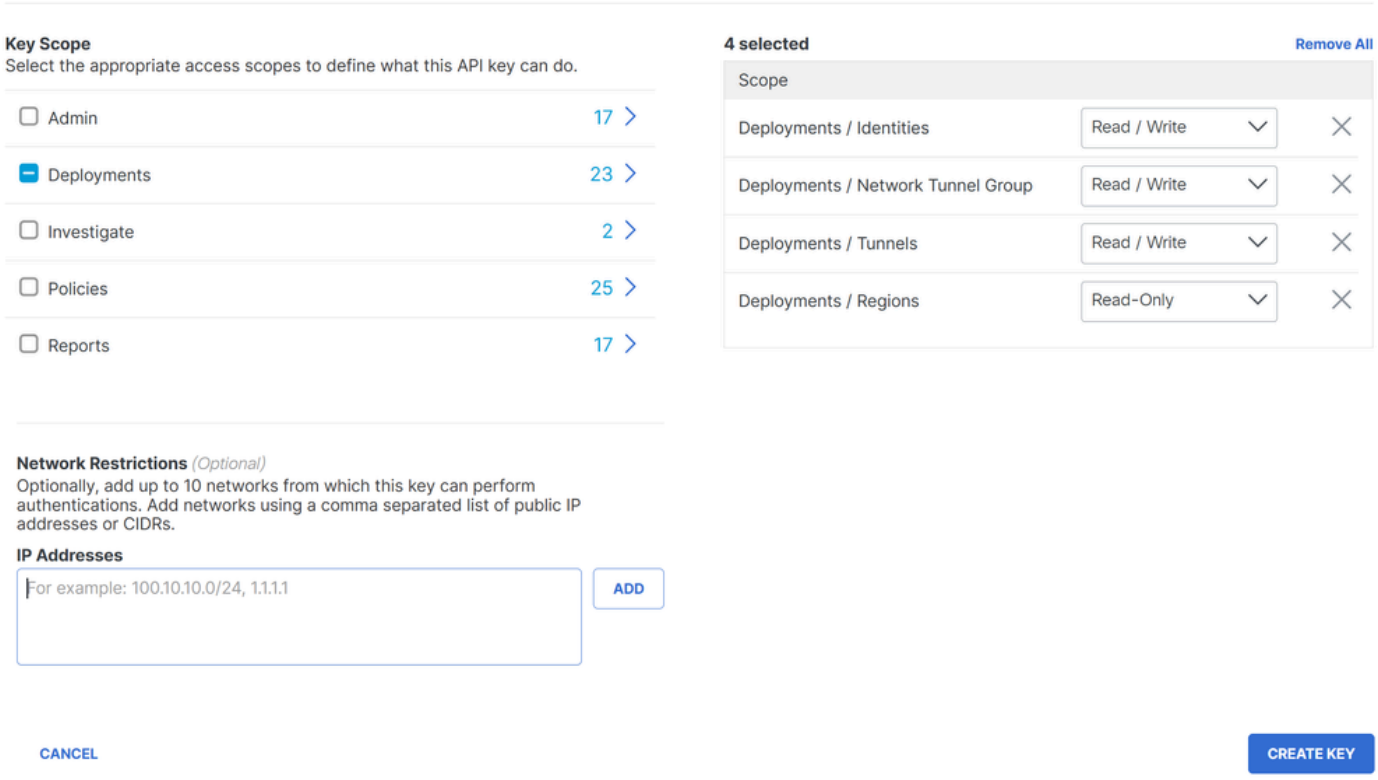
安全访问配置

API创建

要使用Secure Access创建自动隧道，请检查后续步骤：

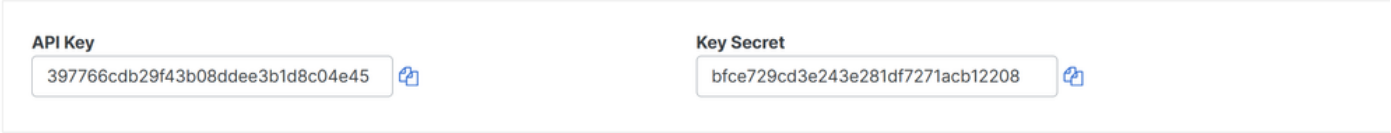
导航到[安全访问控制面板](#)。

- 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。

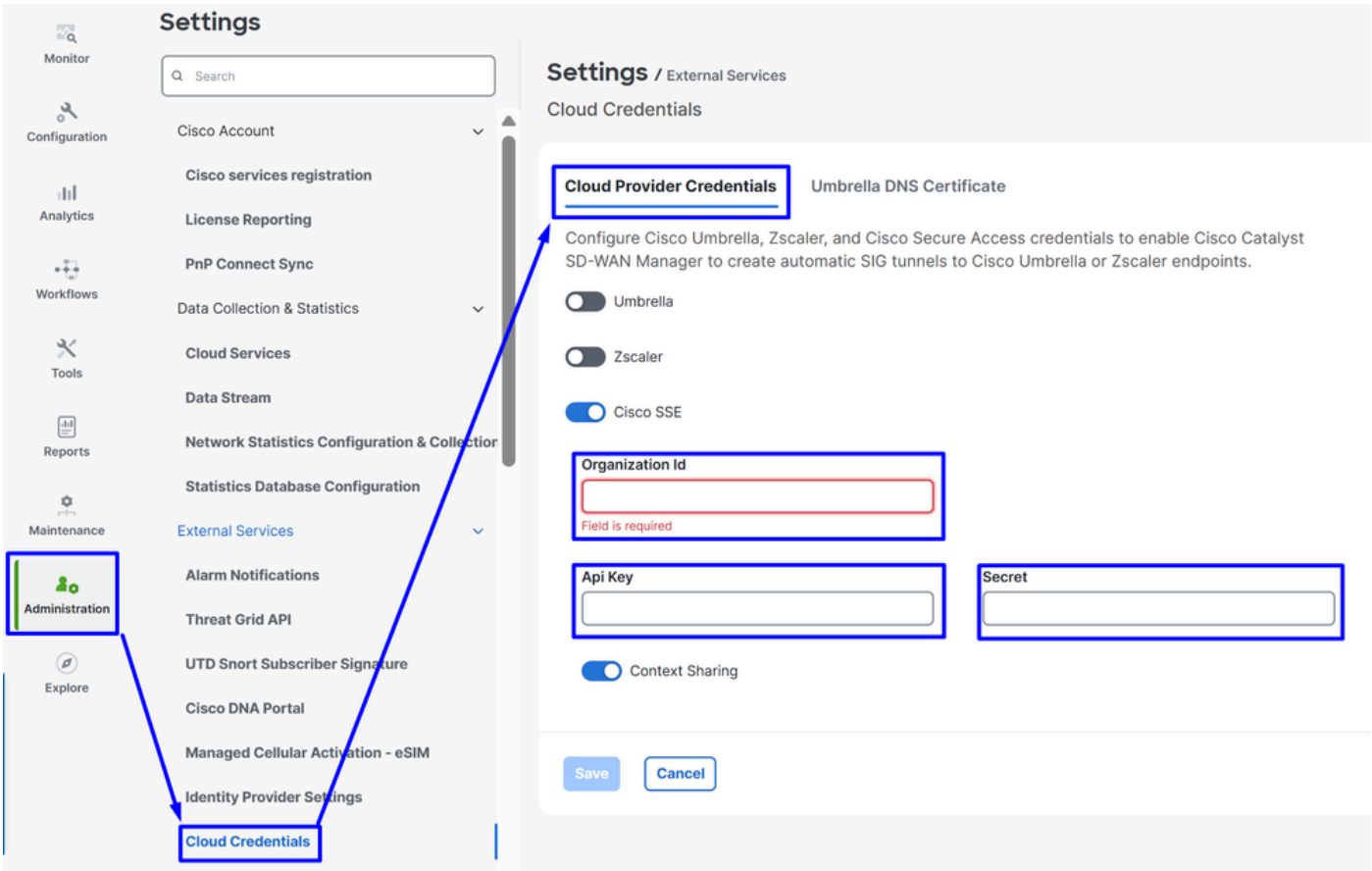
然后单击ACCEPT AND CLOSE。

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

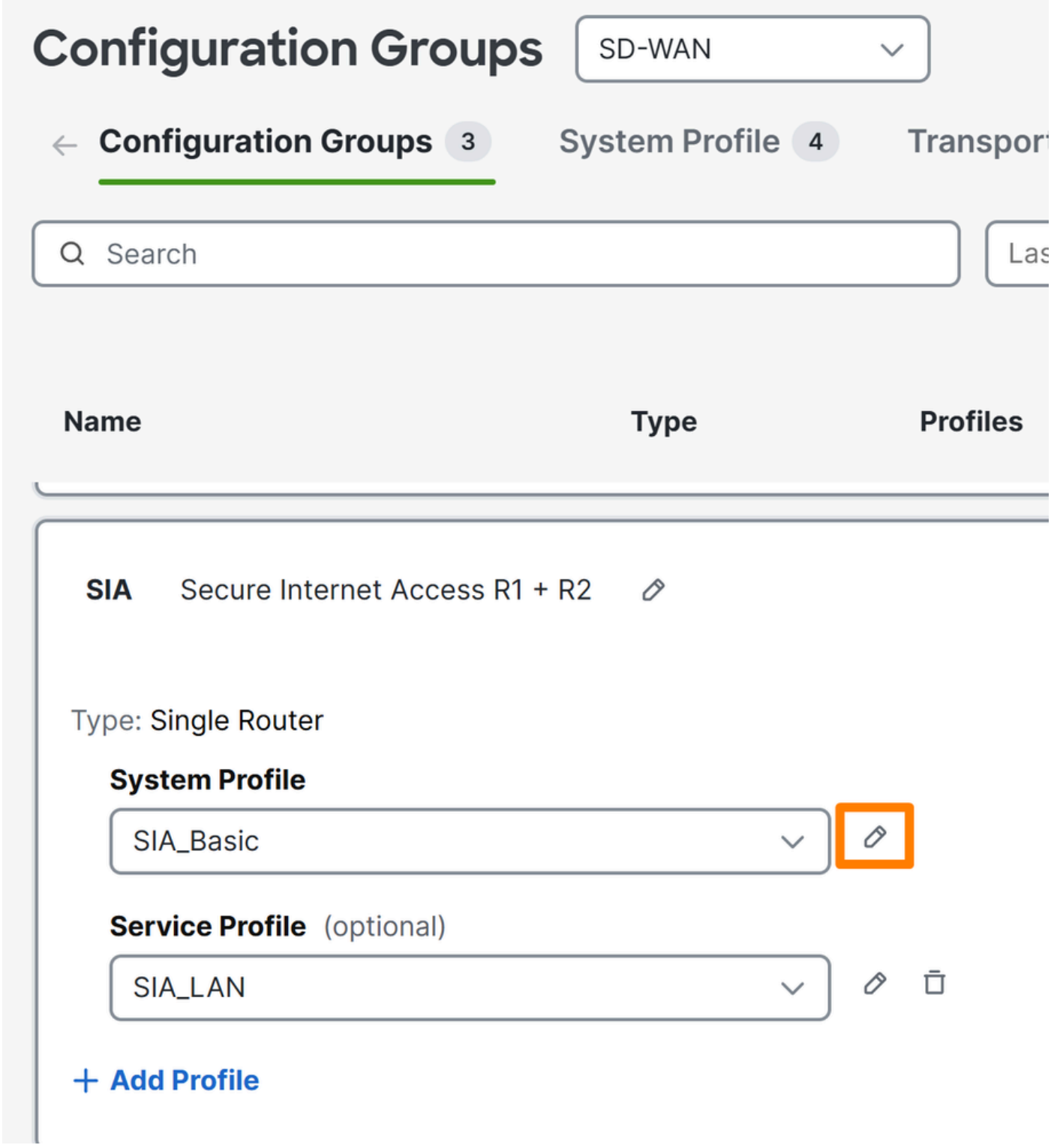
然后，点击按钮Save。



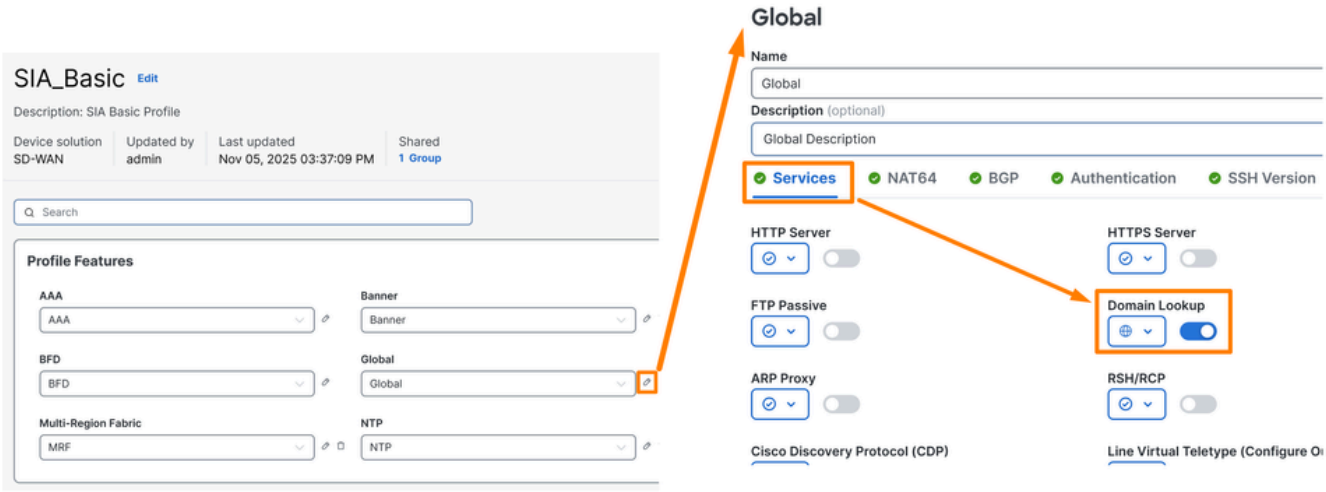
注意：在继续后续步骤之前，您需要确保SD-WAN Manager和Catalyst SD-WAN Edge具有DNS解析和互联网访问。

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



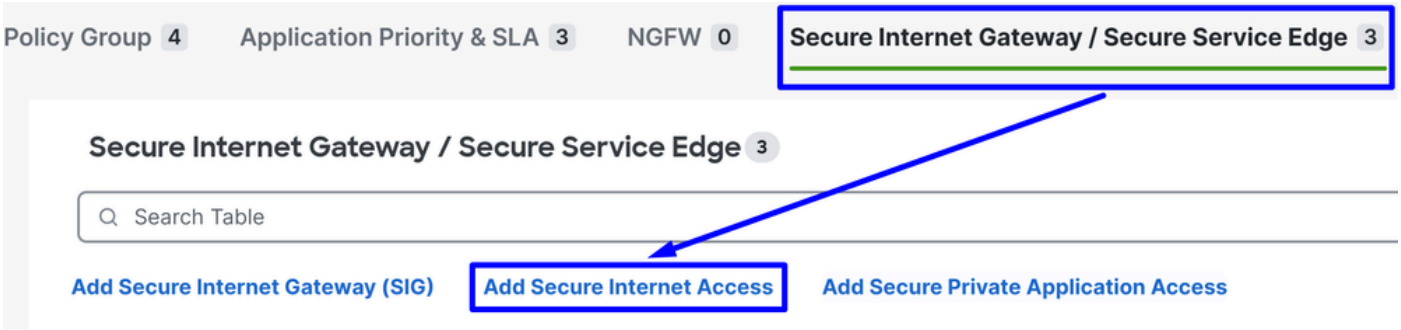
- 然后编辑Global选项，并确保启用选项Domain Resolution



配置策略组

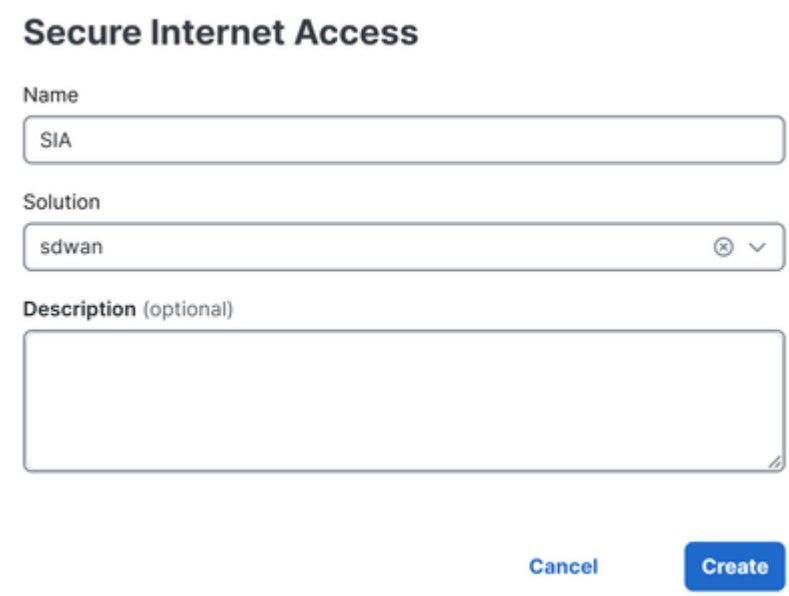
导航到配置>策略组:

- 单击Secure Internet Gateway / Secure Service Edge> *Add Secure Internet Access*

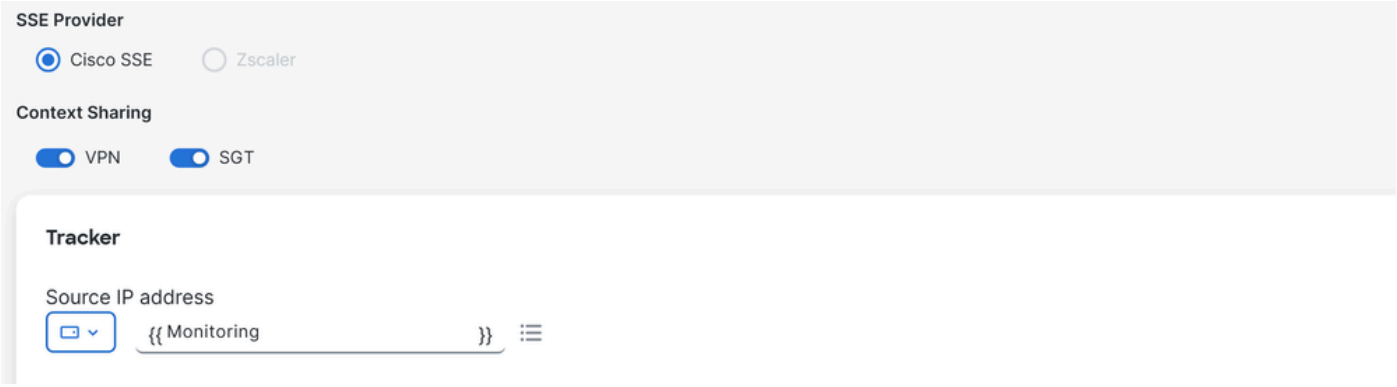


注意：在低于20.18的版本中，此选项称为添加安全服务边缘(SSE)

- 配置名称、解决方案并点击 Create



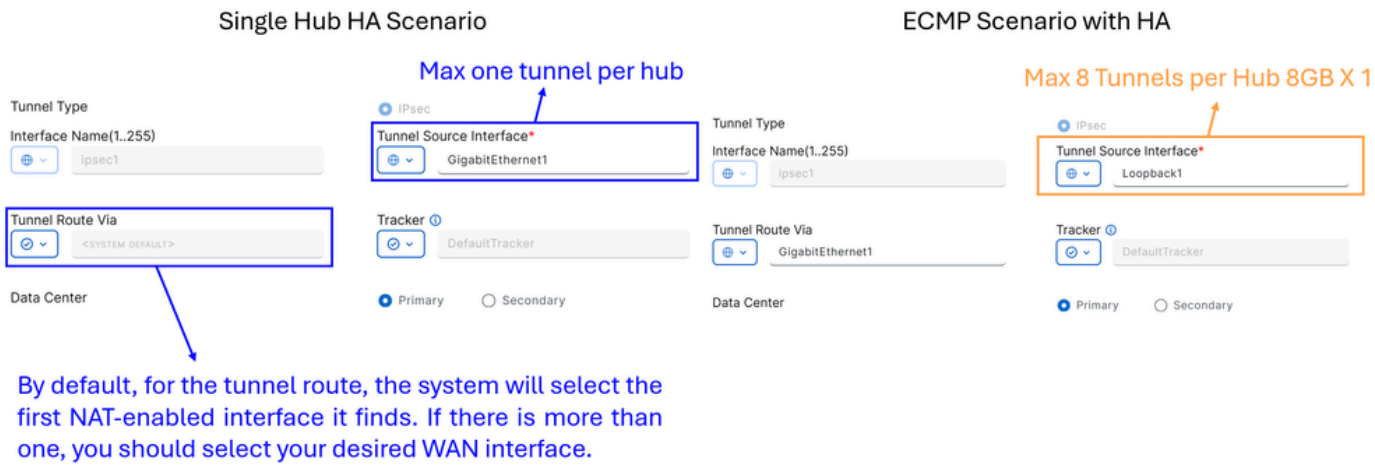
接下来的配置允许您在Catalyst SD-WAN Edge中部署配置后创建隧道：



- SSE Provider:SSE
- Context Sharing:选择VPN或/和SGT取决于您的需求
- Tracker
  - **Source IP Address**:选择Device Specific（这样您就可以按设备修改它，并在部署阶段确定它的使用案例）

在步Configuration骤下，设置隧道：



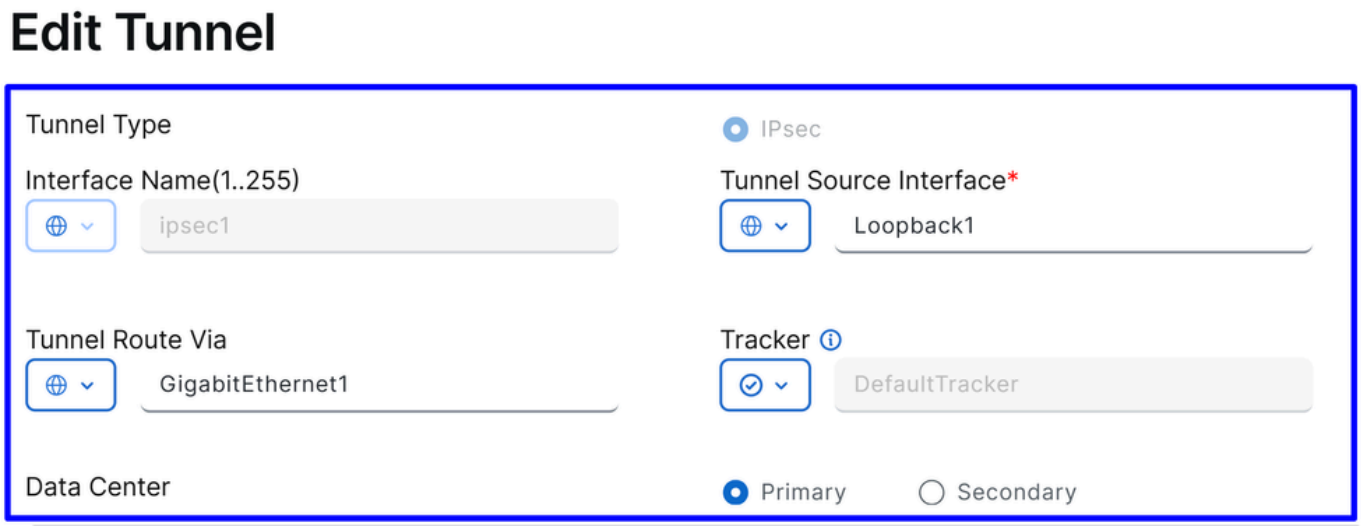


- **Single Hub HA Scenario**:在此方案中，您可以将一个NTG用作主用NTG，将另一个NTG用作被动NTG，从而配置高可用性，每个NTG的最大吞吐量为1 Gbps
- ECMP Scenario with HA:在此方案中，每个集线器最多可以配置8个隧道，每个NTG总共最多支持16个隧道。此设置允许隧道间的吞吐量更高

注意：如果您的网络接口的吞吐量大于1Gbps，并且需要可扩展性，则必须使用环回接口。否则，您可以使用设备上的标准接口。这是为了从安全访问端启用ECMP。

警告：如果要为ECMP方案配置环回接口，必须首先在路由器中使用的策略下在Configuration GroupsTransport & Management Profile > 中设置环回接口。

- 点击Add Tunnel

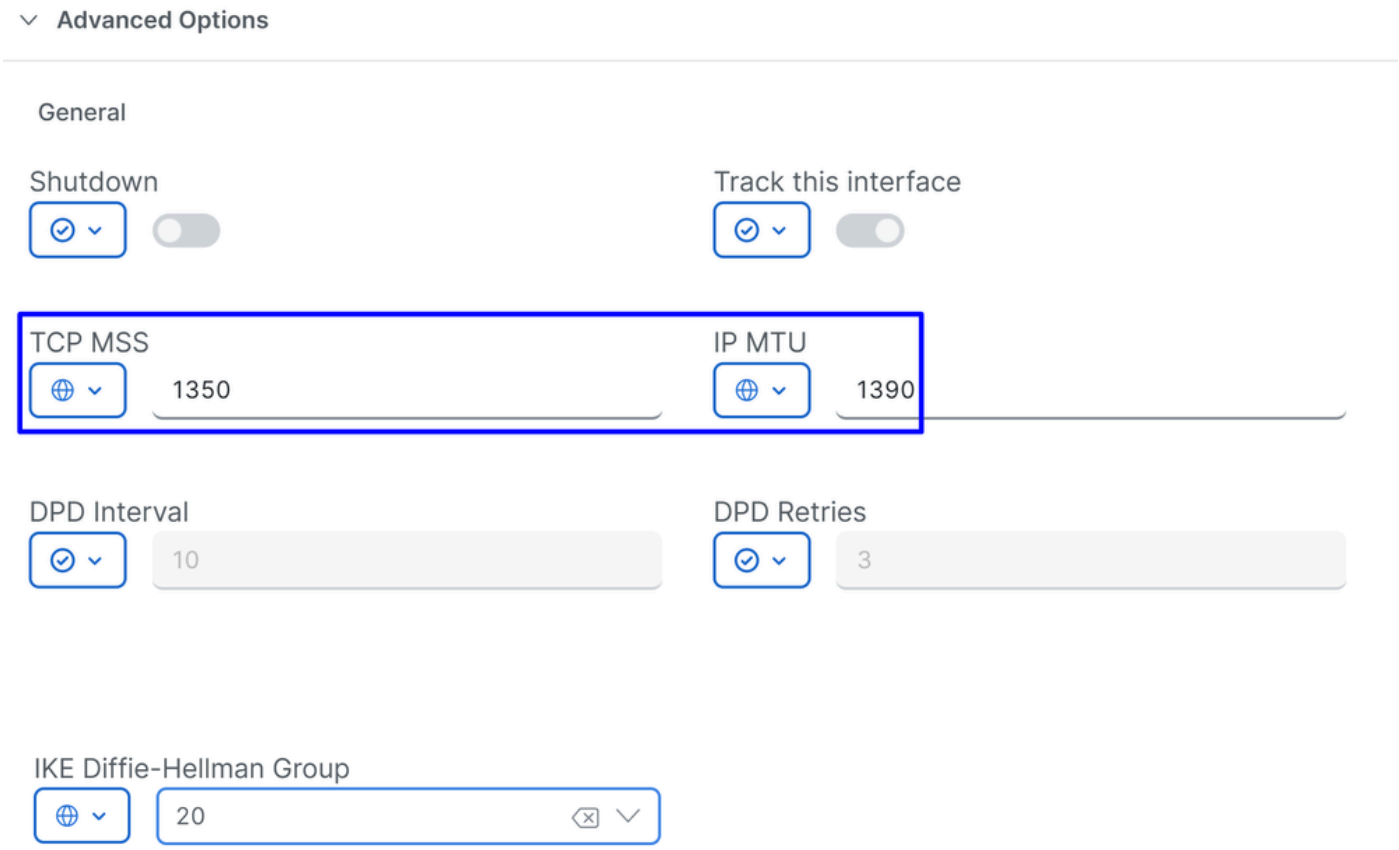


- Interface Name:ipsec1、ipsec2、ipsec3等
- Tunnel Source

Interface:选择Loopback Interfaces或从中建立隧道的特定接口

- **Tunnel Route Via**:如果选择环回，您需要选择要从中路由流量的物理接口。如果不选择环回，此选项显示为灰色，并使用系统创建的第一个启用NAT的接口。如果有多个接口，您必须选择所需的WAN接口
- **Data Center**:这意味着您在Secure Access中建立了连接的中心

隧道配置的下一部分使用思科提供的最佳实践配置隧道。



- TCP MSS:1350
- IP MTU:1390
- IKE Diffie-Hellman Group:20

之后，您必须配置指向辅助数据中心的辅助隧道。

单集线器HA场景



这是使用正常场景部署时的最终结果。

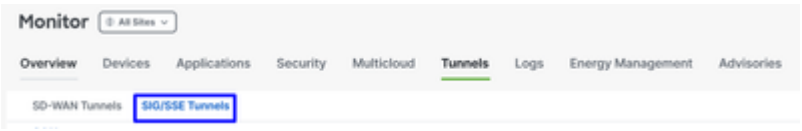
ECMP SCENARIO WITH HA

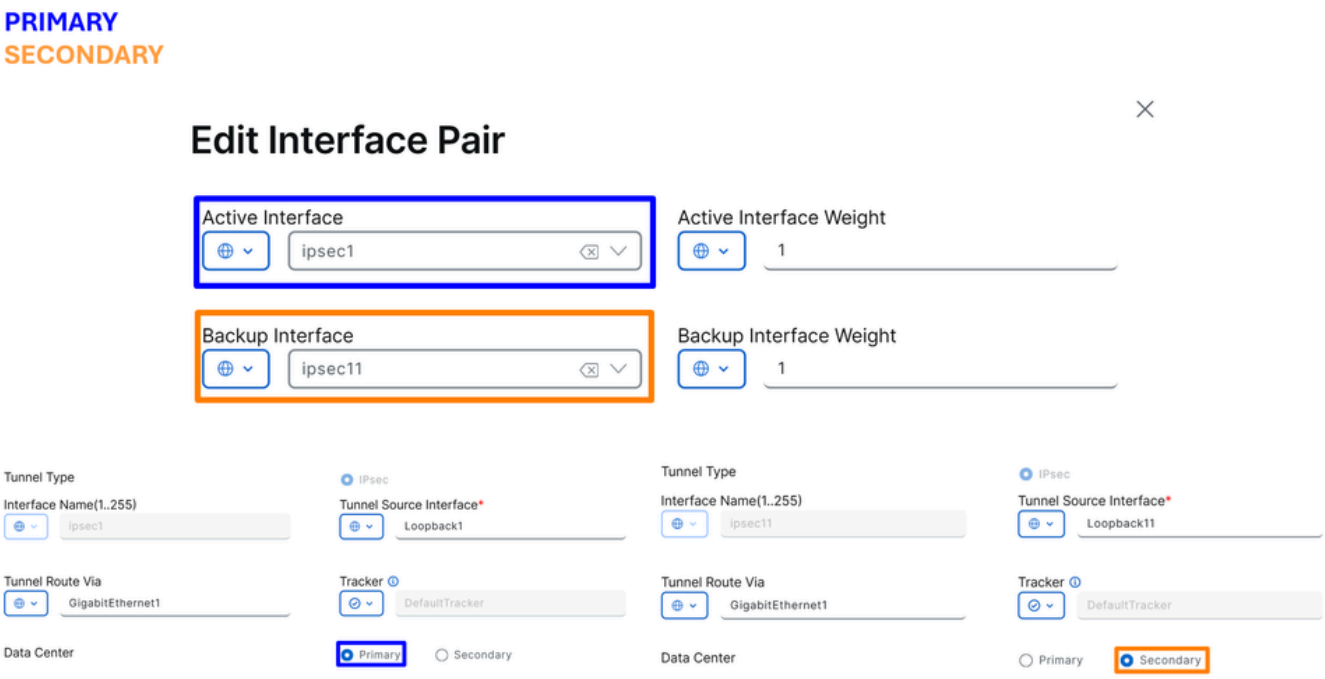
Interface Name	Description	Shutdown	TCP MSS	IP MTU
ipsec1		false	1350	1390
ipsec2		false	1350	1390
ipsec3	PRIMARY HUB	false	1350	1390
ipsec4		false	1350	1390
ipsec5		false	1350	1390
ipsec11		false	1350	1390
ipsec12		false	1350	1390
ipsec13	SECONDARY HUB	false	1350	1390
ipsec14		false	1350	1390
ipsec15		false	1350	1390

然后，您需要在安全互联网策略中配置高可用性。



点击Add Interface Pair:



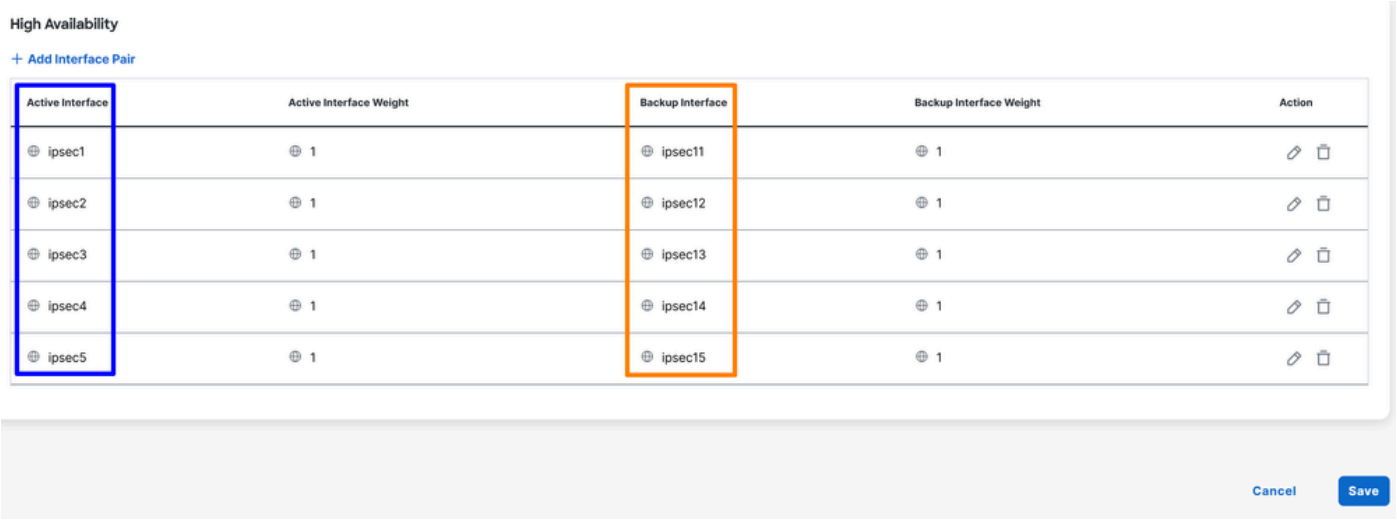


在此步骤中，您需要为正在设置的每个隧道对配置主隧道和辅助隧道。这意味着每个隧道都有自己的备份。请记住，这些隧道被创建为Primary和Secondary，完全是为了此目的。
“Active interface”表示主隧道，而“Backup interface”表示辅助隧道：

- Active Interface:主
- Backup Interface:辅助

警告：如果跳过此步骤，则不会建立隧道，也不会建立从路由器到安全访问的连接。

为隧道配置高可用性后，设置如下图所示。在本指南的实验示例中，HA中显示了五个隧道。可以根据需要调整隧道数。



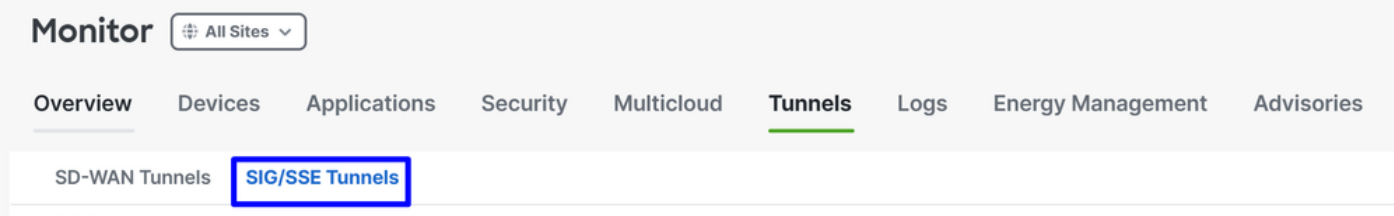
> 注意：最多8个隧道对(16个隧道：可在SD-WAN Catalyst vManage中配置8个主交换和8个辅交换矩阵。Cisco安全接入最多支持10对隧道。

- 点击 Save

此后，如果所有配置都正确，则隧道在SD-WAN管理器和安全访问中显示为UP。

要在SD-WAN中验证，请检查后续步骤：

- 单击Monitor> Tunnels
- 然后单击SIG/SSE Tunnels

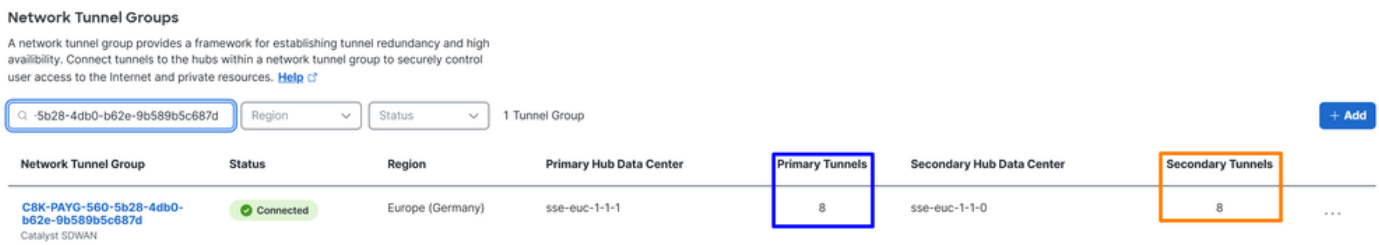


并且您可以看到建立到Cisco Secure Access UP的隧道。

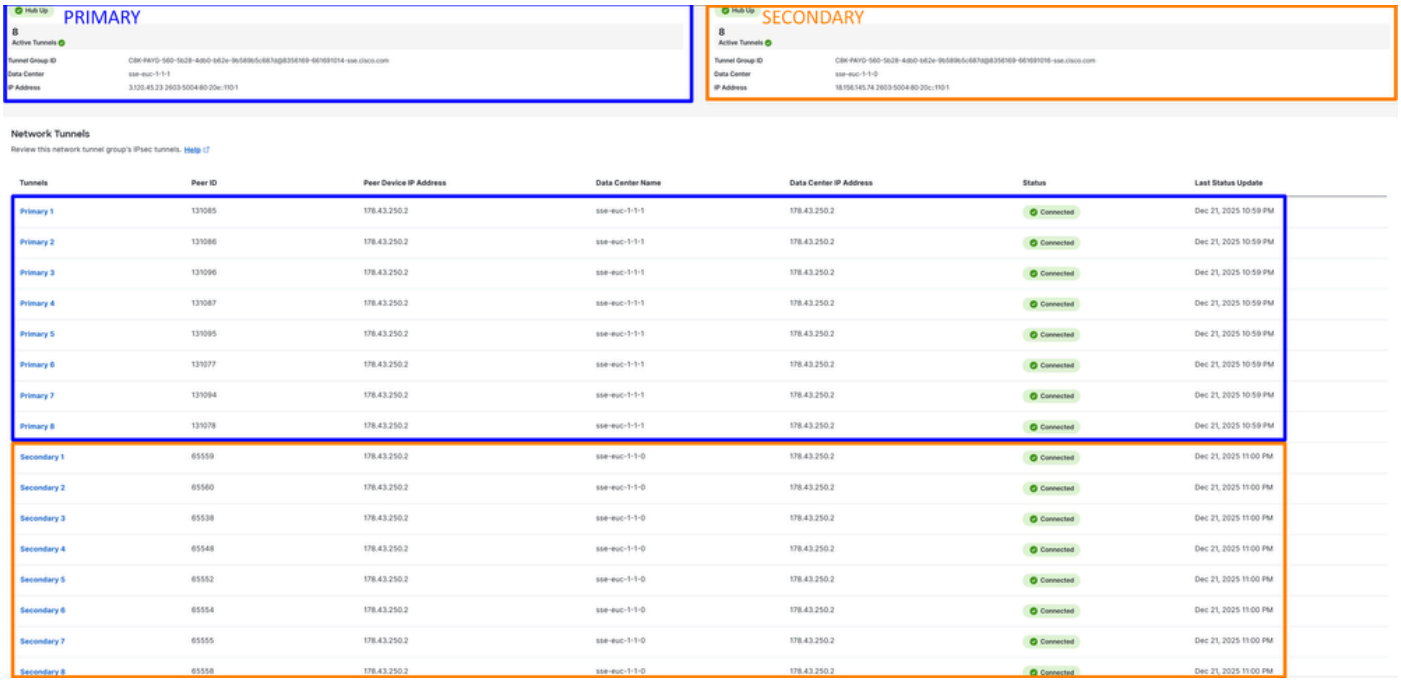
Network Tunnel Group	Tunnel Name	Host Name	Site Name	Tunnel Group ID	Transport Type	Tunnel Type	HA Pair	Provider	Destination Data Center	Tunnel Status(Local)	Tunnel Status(Remote)
		R101-1	SITE_101								
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000001	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000002	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000003	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000004	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000005	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000006	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000007	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000008	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000011	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000012	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000013	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000014	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000015	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000016	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000017	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000018	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up

要在中验证Secure Access，请检查后续步骤：

- 单击Connect> Network Connections



在详细视图中，点击隧道的名称：



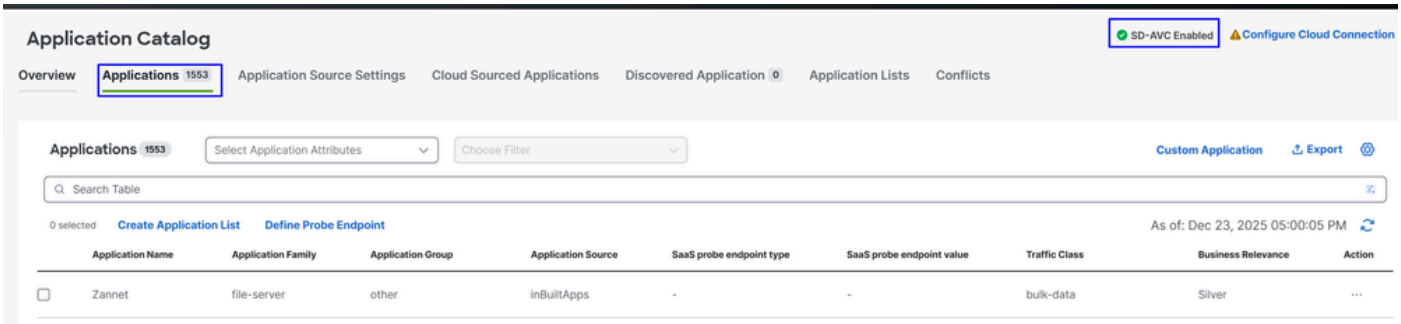
之后，您可以继续步骤， Create your Custom Bypass FQDN or APP in SD-WAN

在SD-WAN中创建自定义绕行FQDN或应用（可选）

在某些特殊使用案例中，您需要创建应用旁路和FQDN或IP，您可以将其应用于路由策略：

导航到SD-WAN Manager门户：

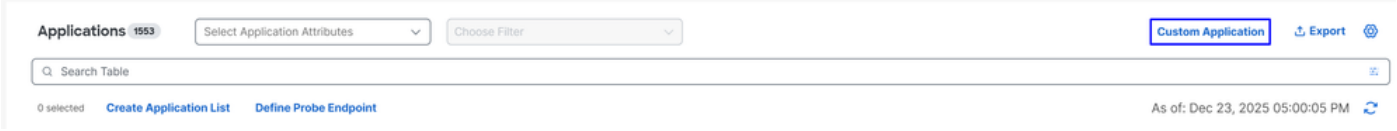
- 单击Configuration> Application Catalog > Applications



提示：如果运行的版本低于20.15，可以在Policy Lists下创建自定义应用

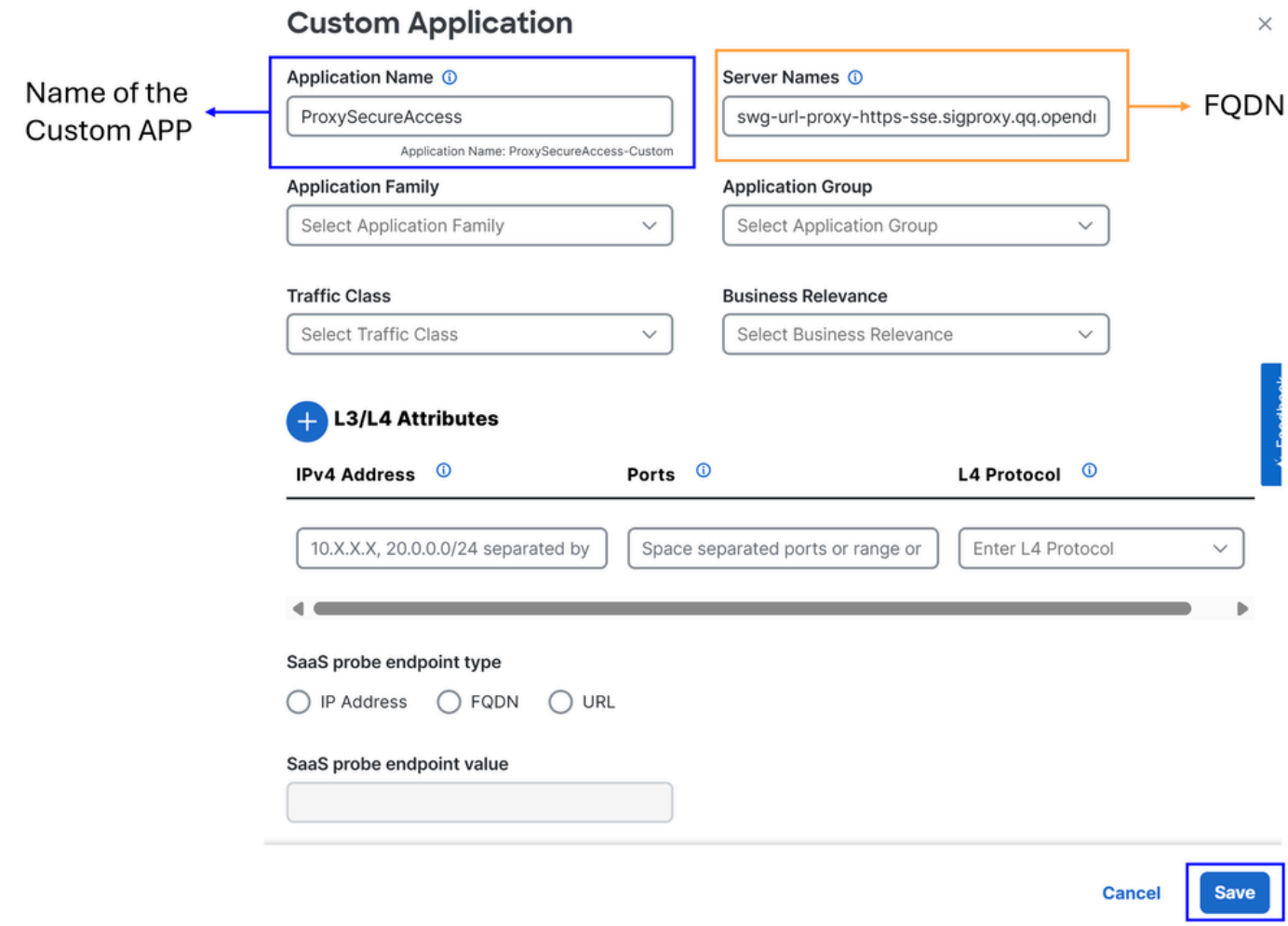
注意：要访问应用目录，必须启用SD-AVC。

- 点击 Custom Application



在此阶段，使用安全客户端 — Umbrella模块SWG FQDN配置基本排除：

ProxySecureAccess

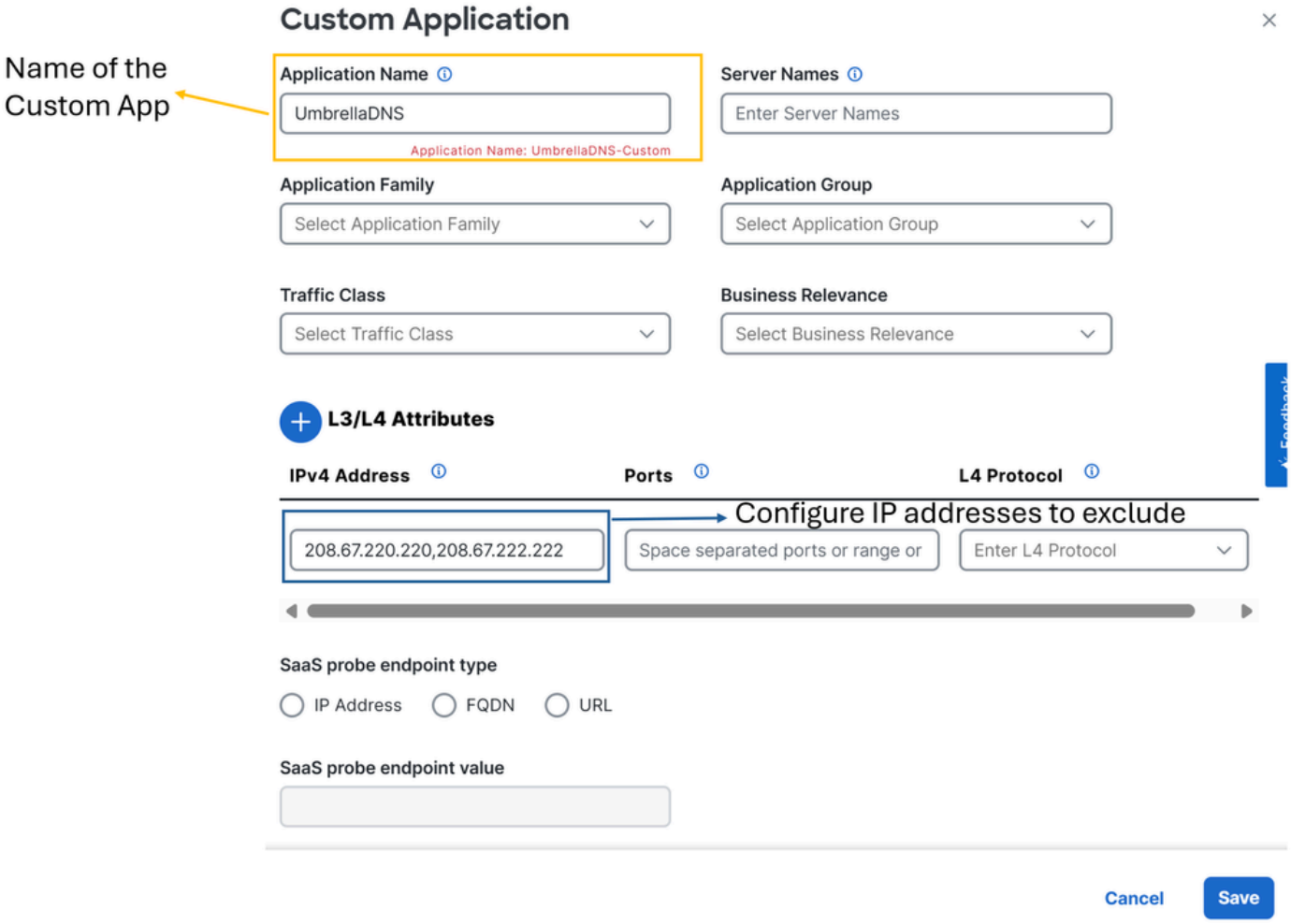


- Server Name:使用您要绕过的FQDN（在本示例中配置了SWG的FQDN）
  - swg-url-proxy-https-sse.sigproxy.qq.op endns.com
  - swg-url-proxy-https-ORGID.sseproxy.qq.op endns.com
- 点击 Save

注意：使用您的SSE组织编号更改ORGID。

接下来，创建基本排除；在本例中，Umbrella DNS服务器：

UmbrellaDNS



现在您可以继续配置路由策略。

路由流量

在此步骤中，您需要通过隧道路由互联网流量，以通过思科安全访问对其进行保护。在这种情况下，您使用灵活的路由策略，允许我们绕过某些流量，从而有助于防止通过安全访问发送不需要的流量，或避免潜在的错误做法。
首先，定义两种可以使用的路由方法：

- Configuration > Configuration Groups > Service Profile > Service Route:此方法提供到安全访问的路由，但缺乏灵活性。
- **Configuration** > Policy Groups > Application Priority & SLA:此方法在SD-WAN内提供多种路由选项，最重要的是，它允许您绕过特定流量，因此不会通过安全访问发送该流量。

为获得灵活性并与最佳实践保持一致，我们使用以下配置Application Priority & SLA:

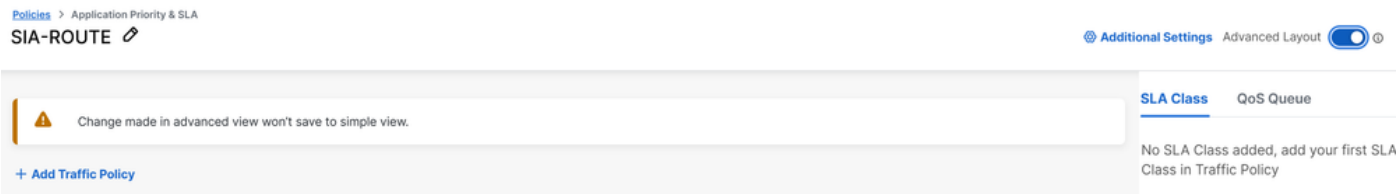
- 点击**Configuration**> Policy Groups > Application Priority & SLA
- 然后单击 Application Priority & SLA Policy



- 配置策略名称，然后点击 Create



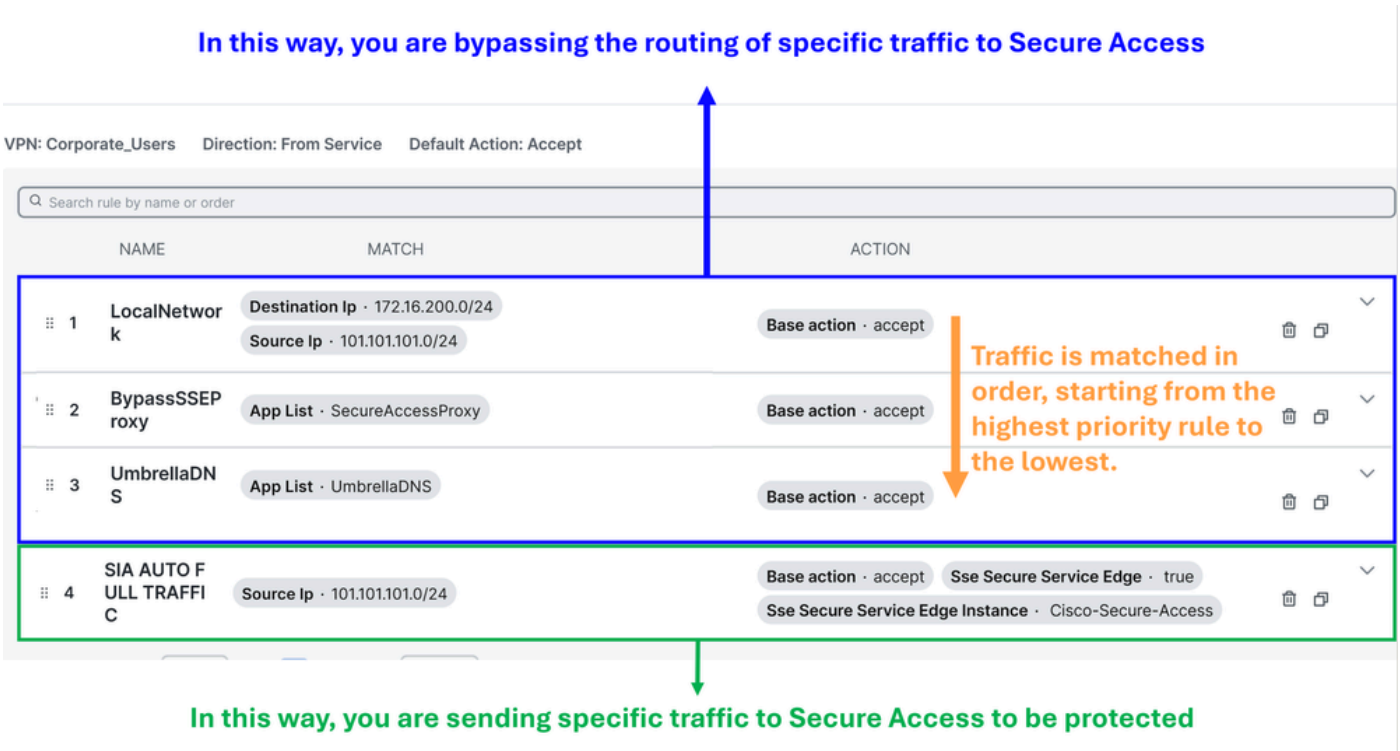
- enable Advanced Layout
- 点击 + Add Traffic Policy





- Policy Name:根据此流量策略列表的目的调整此的名称
- VPN(s):选择从中路由流量的用户的服务VPN
- **Direction**:从服务
- Default action:Accept（接受）

之后，您可以开始创建流量策略：



1. Local Network Policy (Optional):源101.101.101.0/24，目标172.16.200.0/24。此路由可防止网络内流量发送到Cisco安全访问。通常，客户不会这样做，因为在SD-WAN部署中，内部路由通常由分布路由器处理。此配置可确保不会将这些子网之间的内部流量路由到安全访问，具体取决于您的场景是否需要它（可选，取决于您的网络环境）
2. **BypassSSEProxy (Optional)**

:此策略可防止在安全客户端中启用Cisco Umbrella模块且启用SWG的内部计算机将代理流量发送回云。将代理流量再次路由到云不是最佳实践。

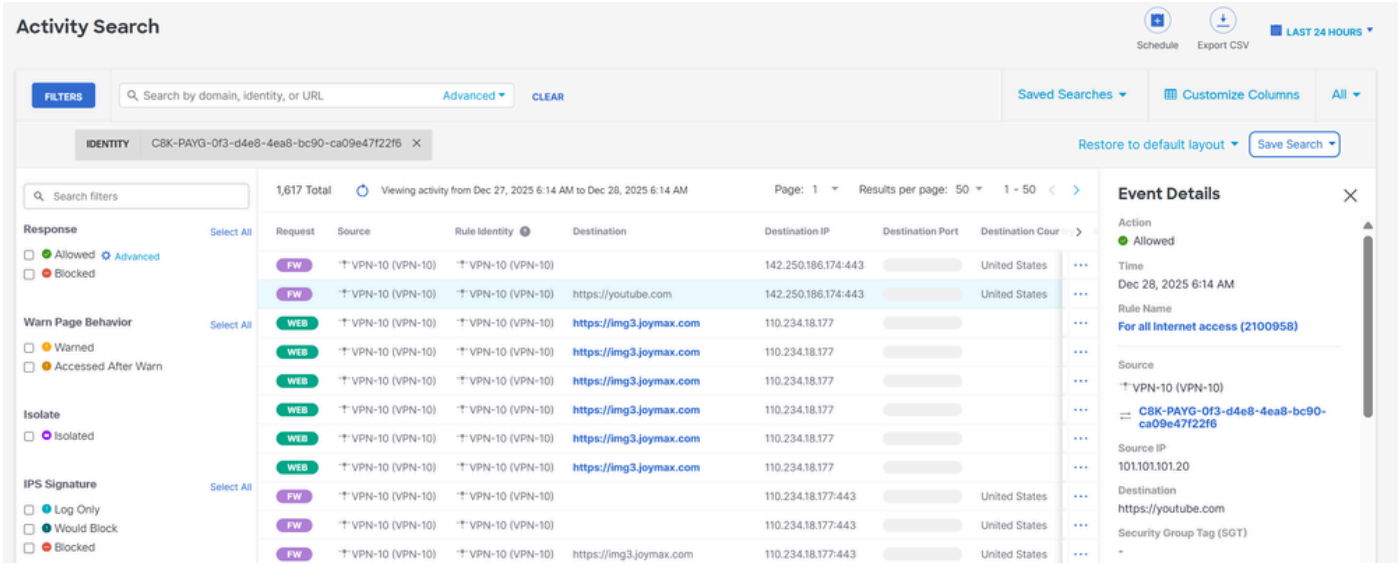
3. UmbrellaDNS (Best Practice):此策略可防止通过隧道发送发往Internet的DNS查询。建议不要通过隧道将DNS查询发送到Umbrella解析器(208.67.222.222,208.67.220.220)。
4. SIA AUTO FULL TRAFFIC:此策略将通过您之前创建的SSE隧道将来自源101.101.101.0/24的所有流量路由到互联网，以确保此流量在云中受到保护。

验证

要验证流量是否已经通过Cisco安全访问泛洪，请导航到Events或Activity Search或Network-Wide Path Insights，然后按您的隧道身份进行过滤：

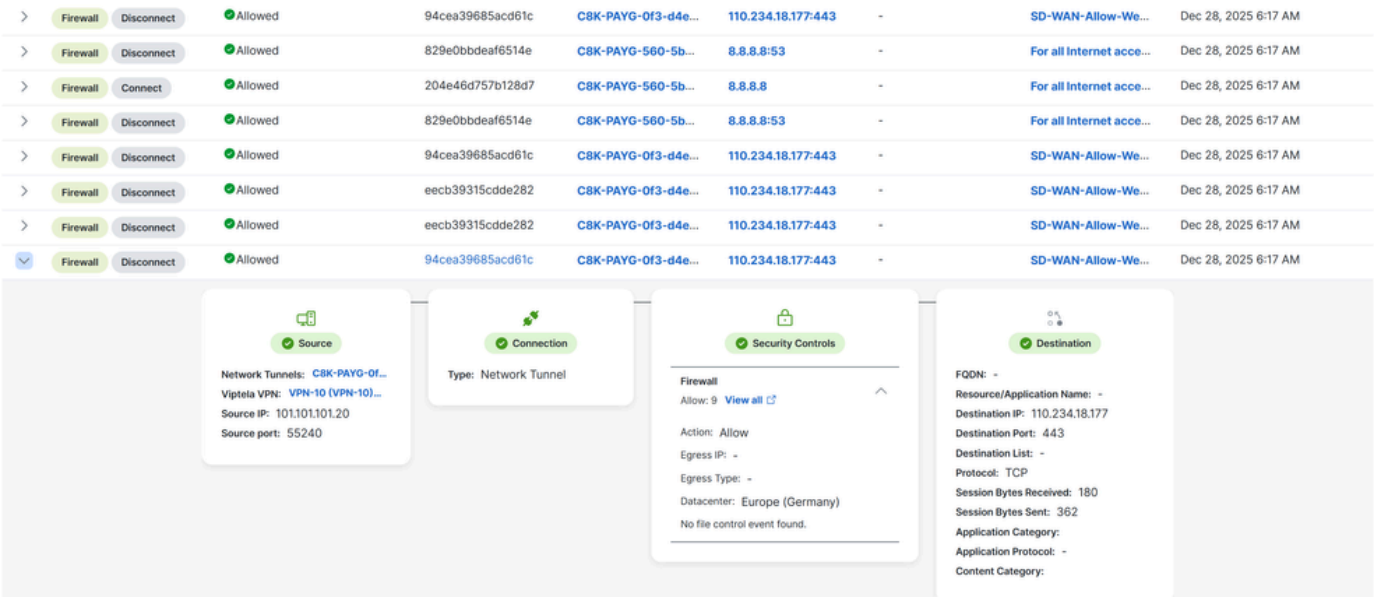
安全访问 — 活动搜索

导航至Monitor>Activity Search:



安全访问 — 事件

导航至Monitor>Events:

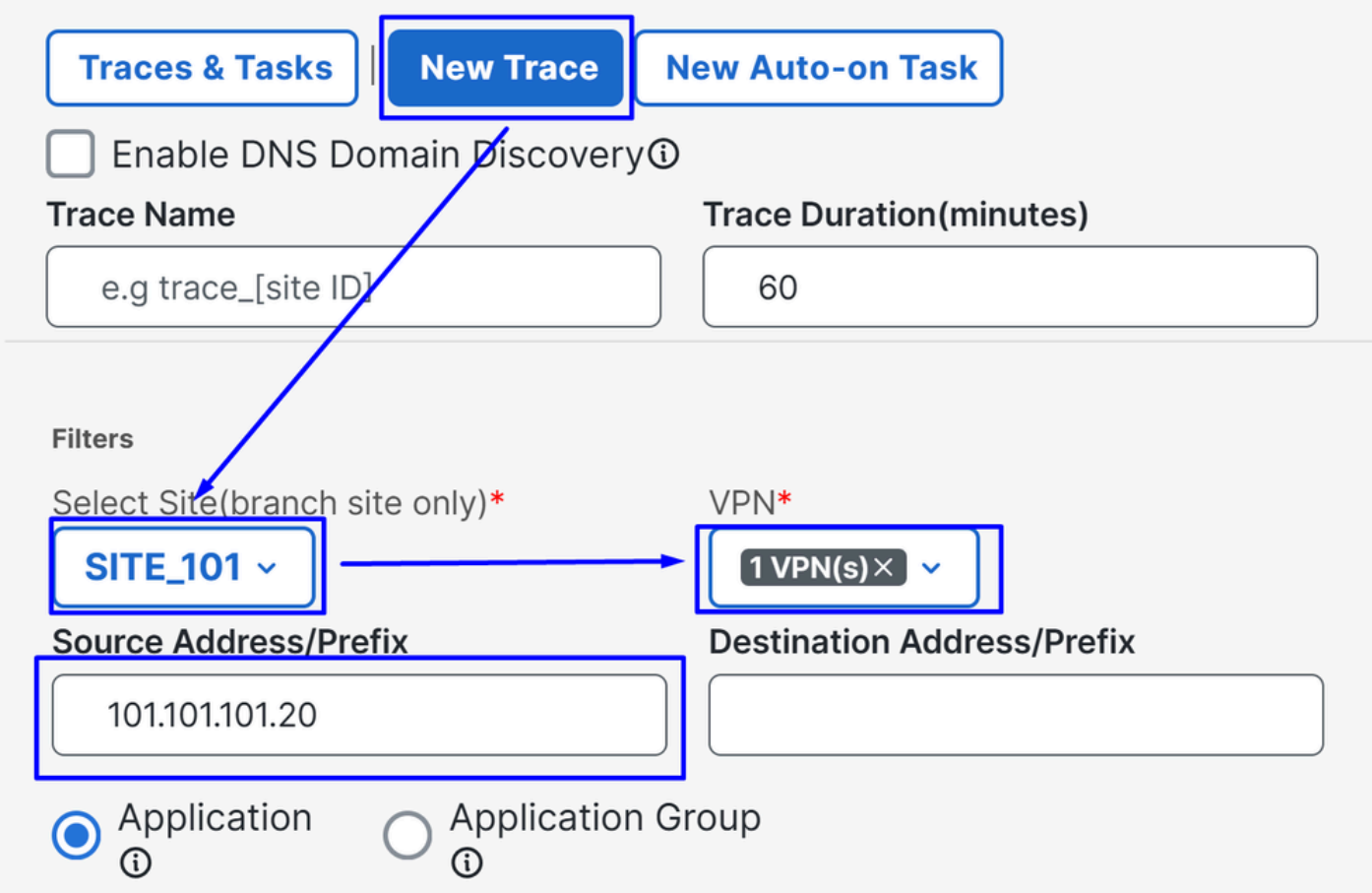


注意：确保您的默认策略已启用日志记录，默认情况下已禁用。

Catalyst SD-WAN Manager — 网络范围路径分析

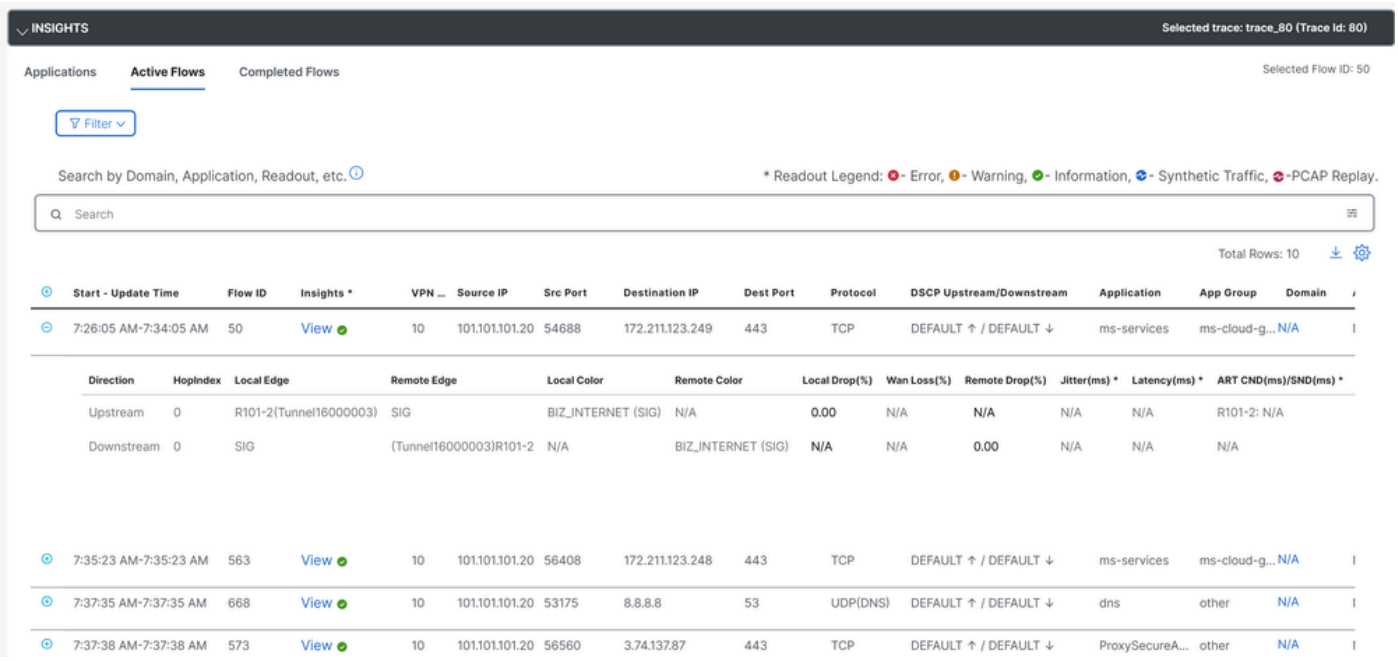
导航至Catalyst SD-WAN Manager:

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



- Site:选择您的流量从哪个站点消失
- VPN:选择您的流量从哪个子网中丢失的VPN ID
- Source:将IP置于空白位置以过滤由和选择过滤的所Site有流VPN量

然后，在Insights中，您可以看到通过隧道泛洪的流量和流向安全访问的流量类型：



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
- 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）。