在Catalyst SD-WAN上配置安全访问(SSE)集成并排除故障

目录

简介

本文档介绍如何在Catalyst SD-WAN上配置主用 — 主用SSE集成，并指导对其进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科软件定义的广域网(SD-WAN)
- 配置组
- 策略组

使用的组件

本文档中的信息基于以下软件和硬件版本：

- C8000V版本17.15.02

- vManage版本20.15.02
- 思科安全访问帐户

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。

思科安全访问

思科安全访问是一种基于云的安全服务边缘(SSE)解决方案，可融合多种网络安全服务，从云交付这些服务以支持混合型员工。Cisco SD-WAN Manager利用REST API从Cisco Secure Access检索策略信息，并将此信息分发到Cisco IOS XE SD-WAN设备。这种集成为用户提供了无缝、透明且安全的直接互联网接入(DIA)，允许用户从任何设备、任何地点、安全地连接。

Cisco SSE允许SD-WAN设备使用IPSec隧道与SSE提供商建立连接。本文档面向思科安全访问的用户。

初步配置

- 为设备启用域查找：导航到配置组 > System Profile > Global并启用域查找。

注意：默认情况下，域查找处于禁用状态。

- 配置 DNS:路由器可以解析DNS并访问VPN 0上的Internet。
- 配置NAT DIA:DIA配置需要存在于创建SSE隧道的路由器上。

创建环回接口

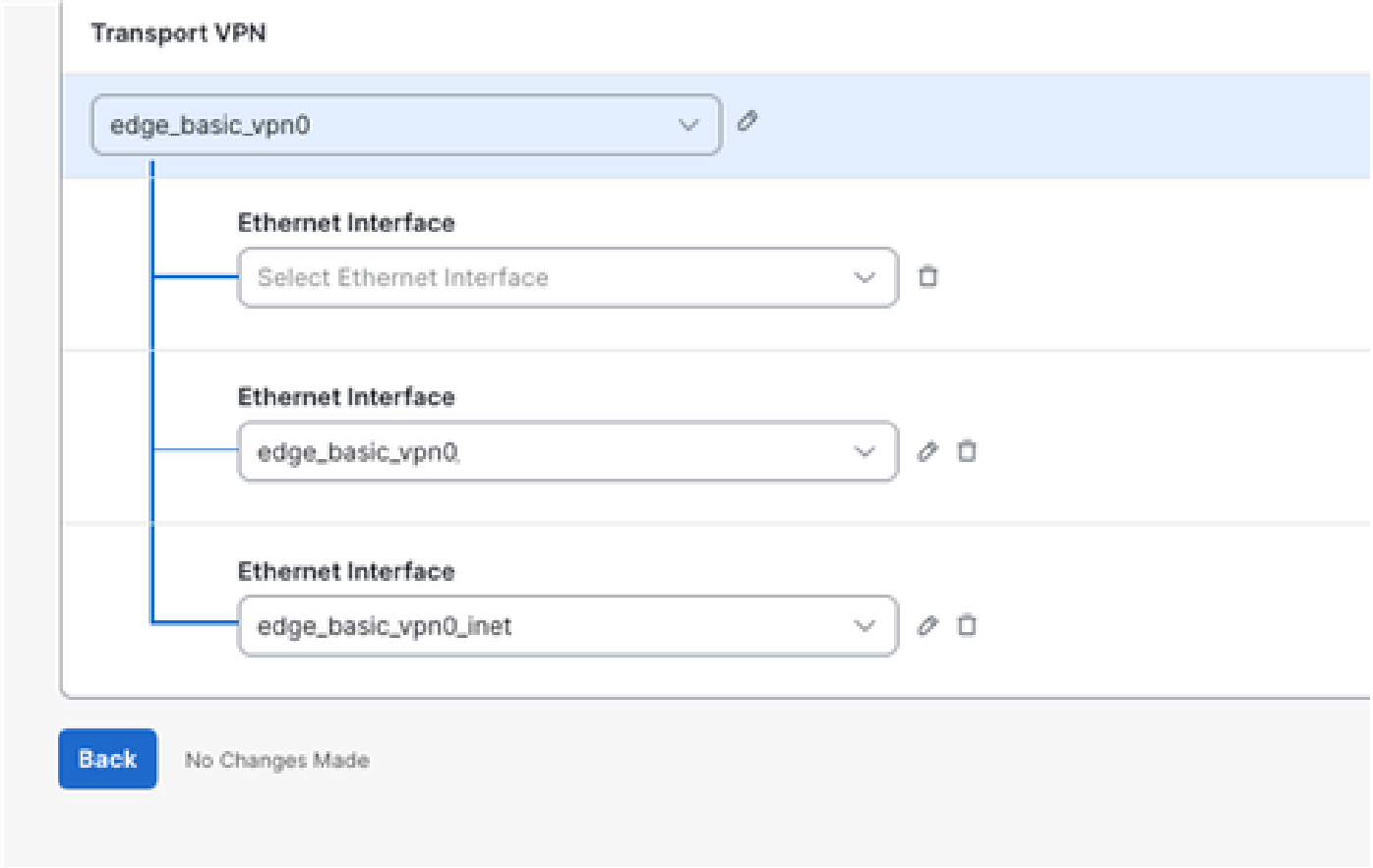
如果主用/主用配置中的两个隧道连接到同一目标数据中心，并且使用相同的WAN接口作为源，则需要创建两个环回IP地址。

注意：当两个隧道配置了相同的源和目标时，IKEv2会形成由本地ID和远程ID组成的身份对。默认情况下，本地ID是隧道的源接口的IP地址。此标识对必须是唯一的，不能在两个隧道之间共享。为防止在IKEv2状态中出现混淆，每个隧道使用不同的环回接口作为其源。虽然IKE数据包在DIA接口上转换(NATed)，但本地ID保持不变，并保留原始环回IP地址。

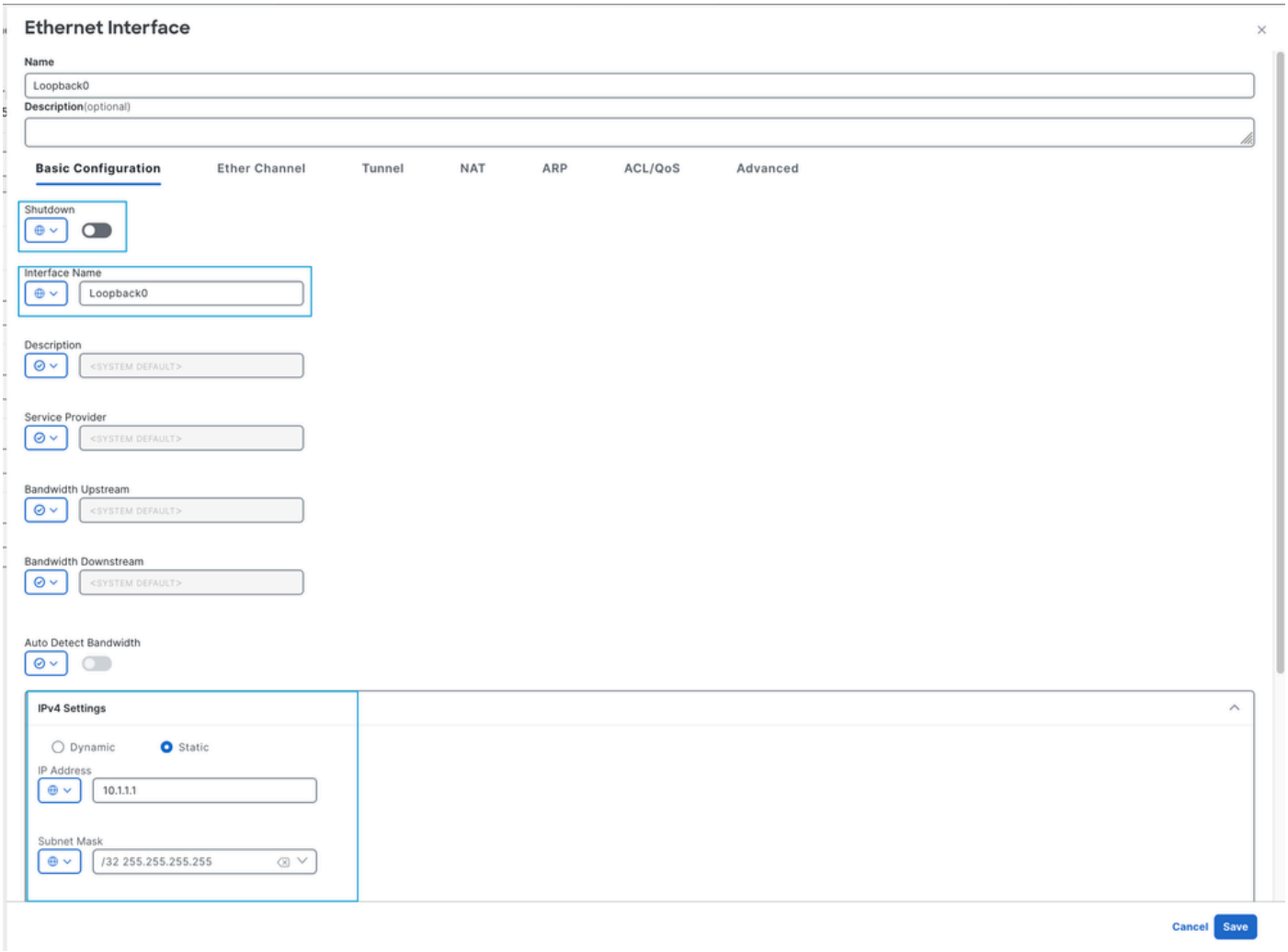
1.导航到配置 > 配置组 > 配置组名称> 传输和管理配置文件 >单击编辑.

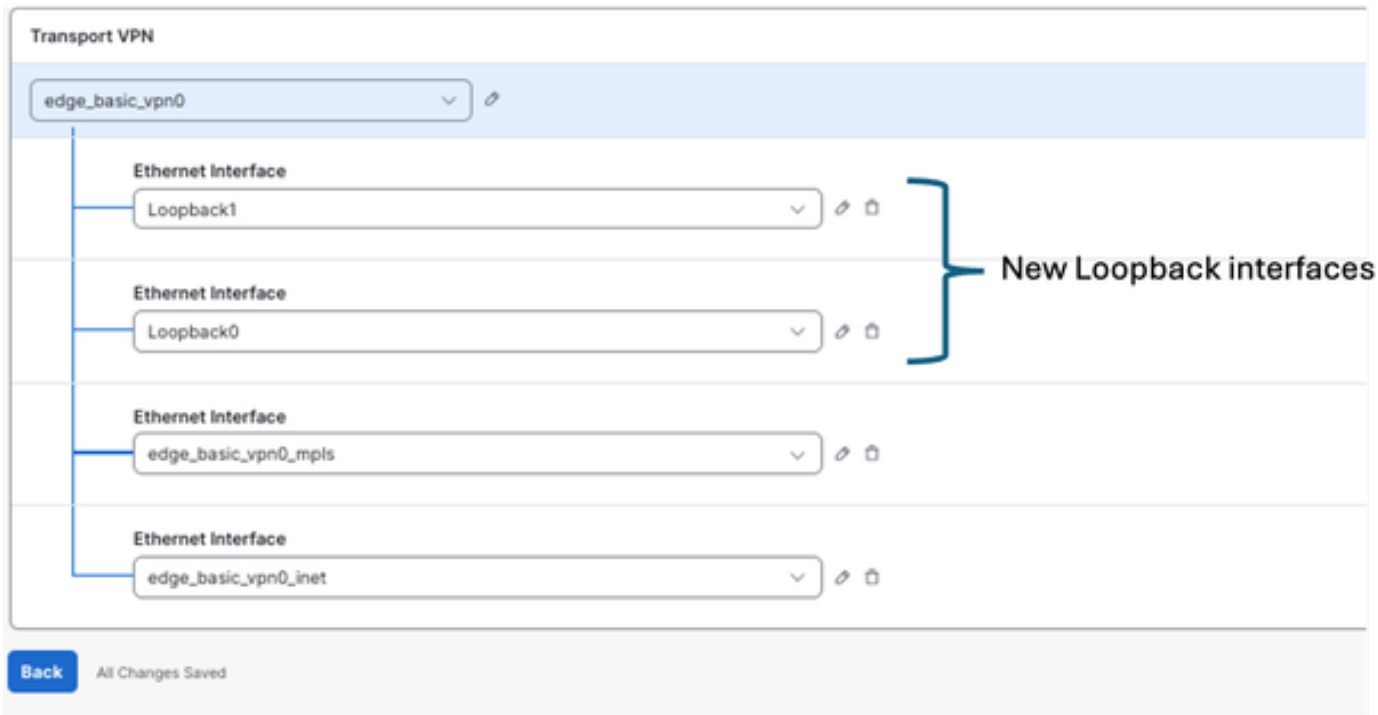
2.点击传输VPN配置文件（主配置文件）右侧的加号(+)。 这将打开位于最右边的Add Featuremenu。

3.单击Ethernet Interface。它在传输VPN下添加新的Internet接口。



4.使用RFC1918 IPv4地址创建两个环回接口，如图中的Loopback0示例。

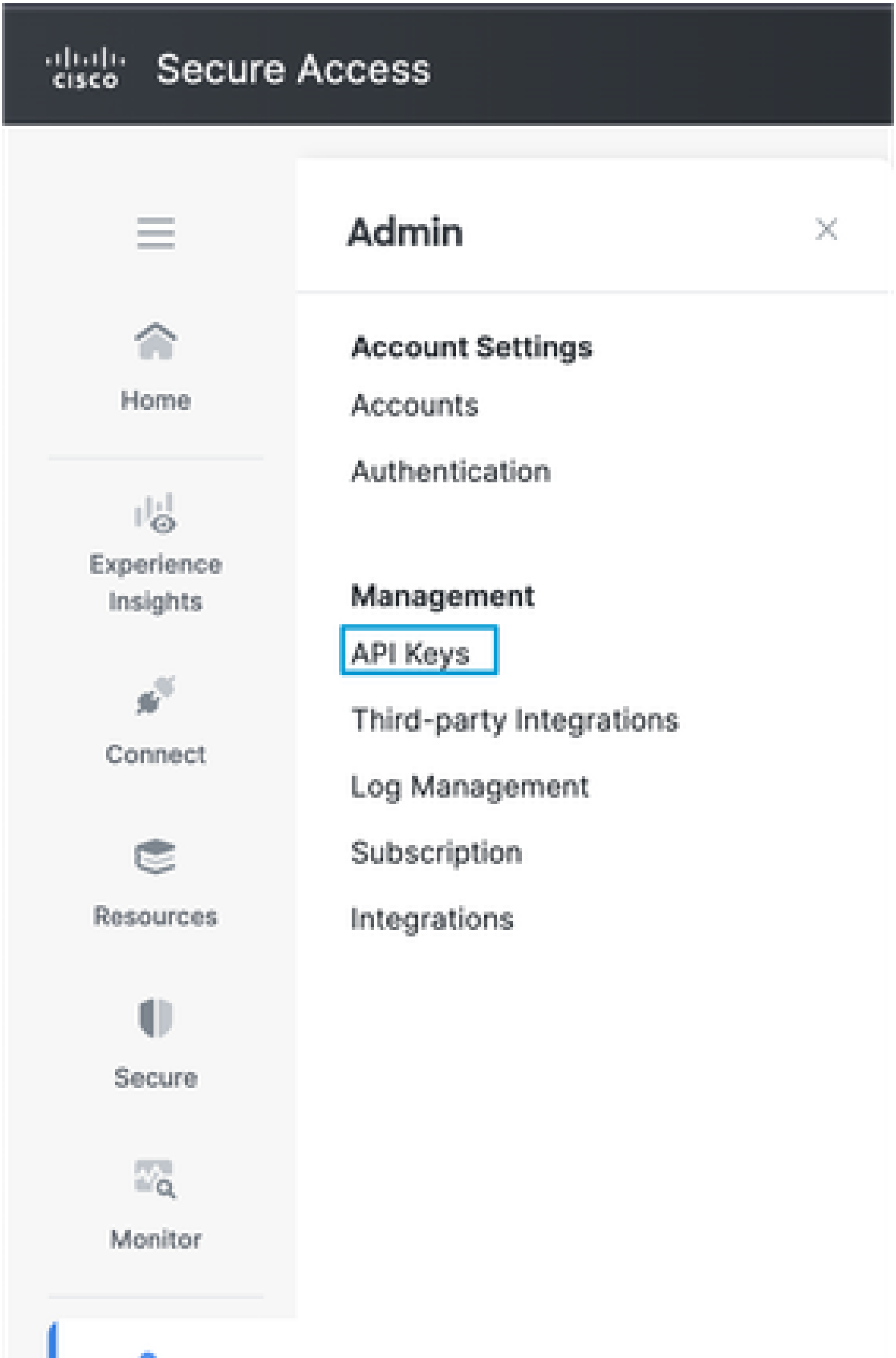




5. 应用环回配置后，继续将配置更改部署到设备。请注意，调配状态从1/1变为0/1。

在SSE门户上配置新的API密钥

1.访问SSE门户https://login.sse.cisco.com/
2.导航到Admin > API Keys


Secure Access
Admin
Account Settings
Accounts
Authentication
Management
API Keys
Third-party Integrations
Log Management
Subscription
Integrations
Home
Experience Insights
Connect
Resources
Secure
Monitor

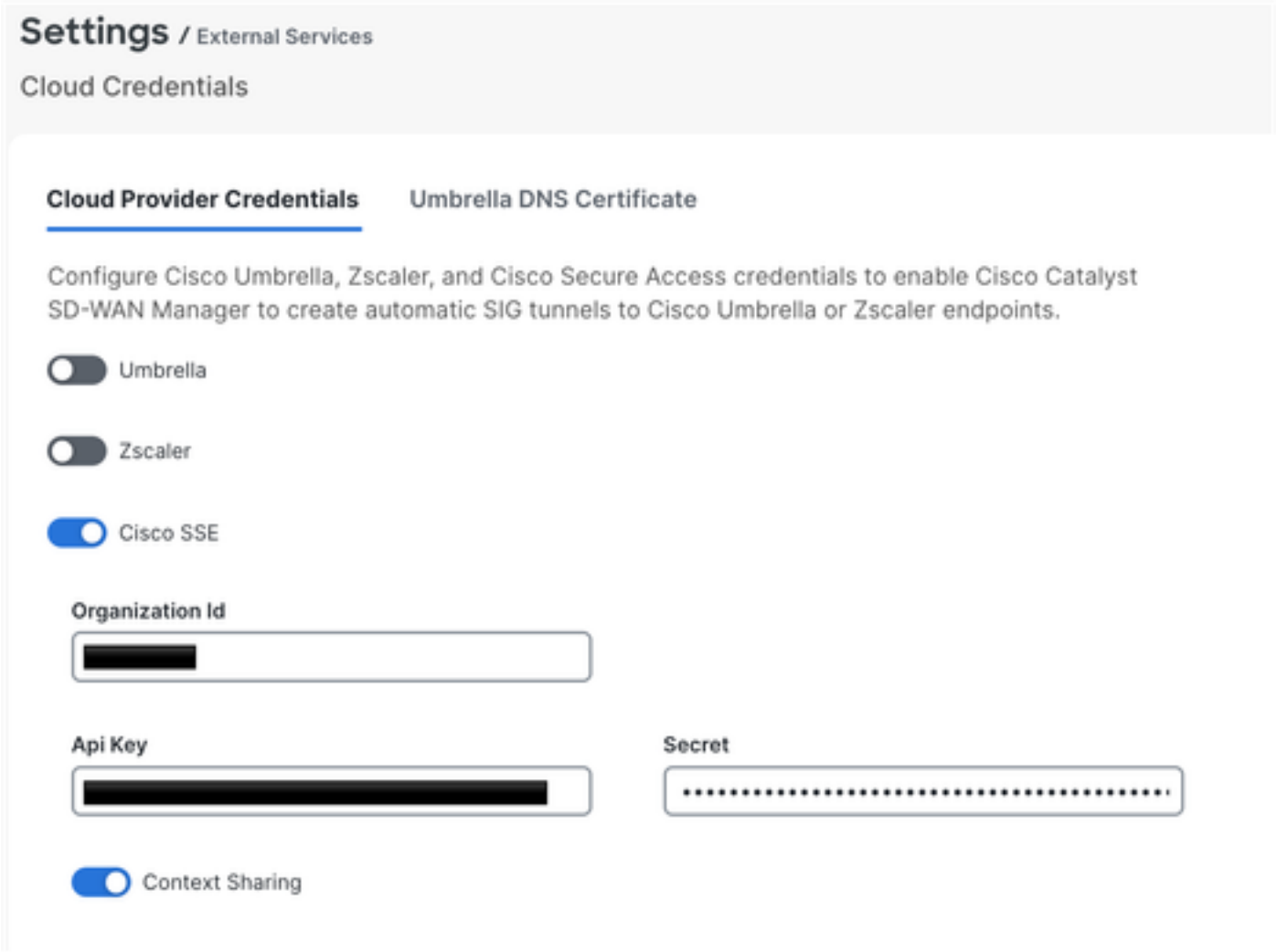
6.将API密钥和密钥密钥复制到记事本中，然后选择ACCEPT AND CLOSE

7.在URL https://dashboard.sse.cisco.com/#some-numbers#/admin/apikey下，#some-numbers#是您的组织ID。同时将这些信息复制到您的记事本中。

在Catalyst Manager上配置SSE

设置云凭据

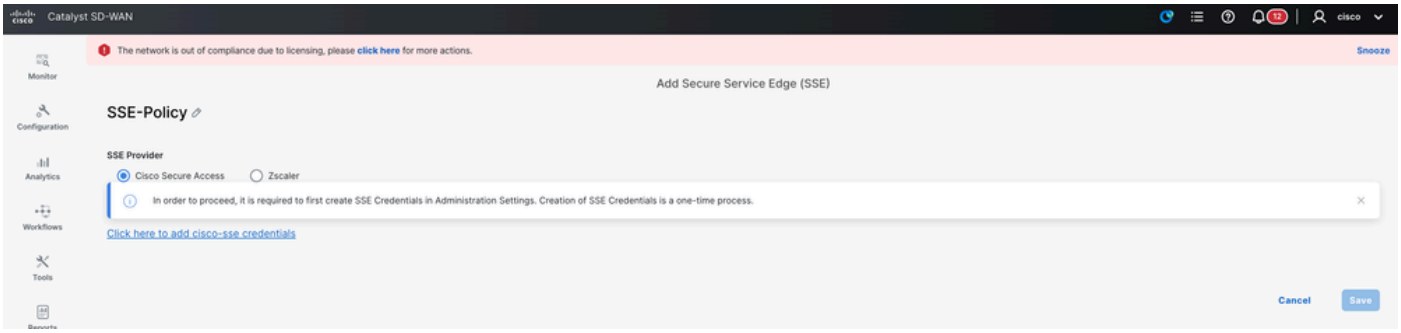
1.导航到管理 > 设置 > 云凭证 > 云提供商凭证，然后启用思科安全访问
并输入详细信息。



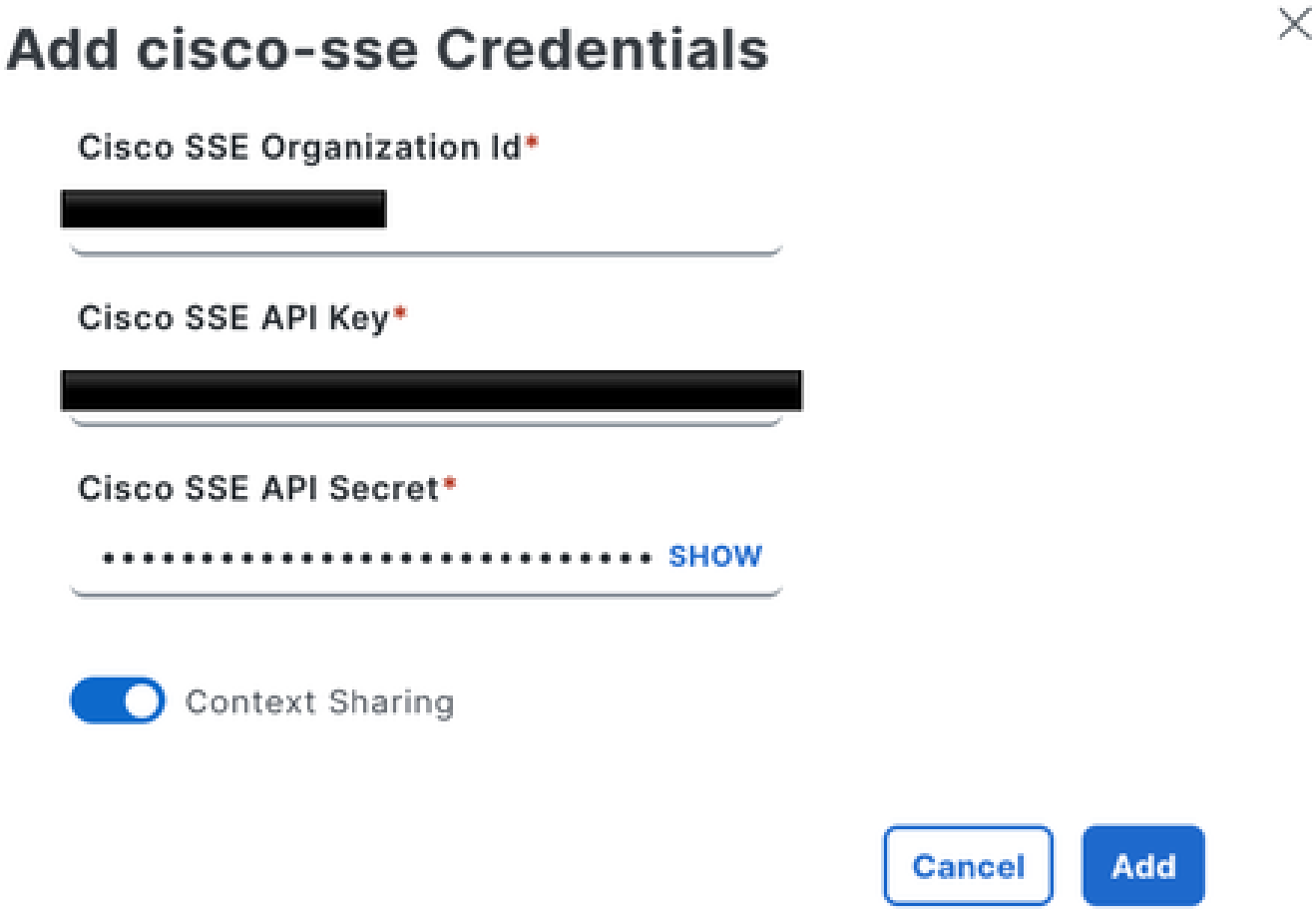
2.可选：您可以启用情景共享以增强功能。有关详细信息，请参阅有关情景共享的Cisco SSE用户指南.

使用策略组配置SSE隧道

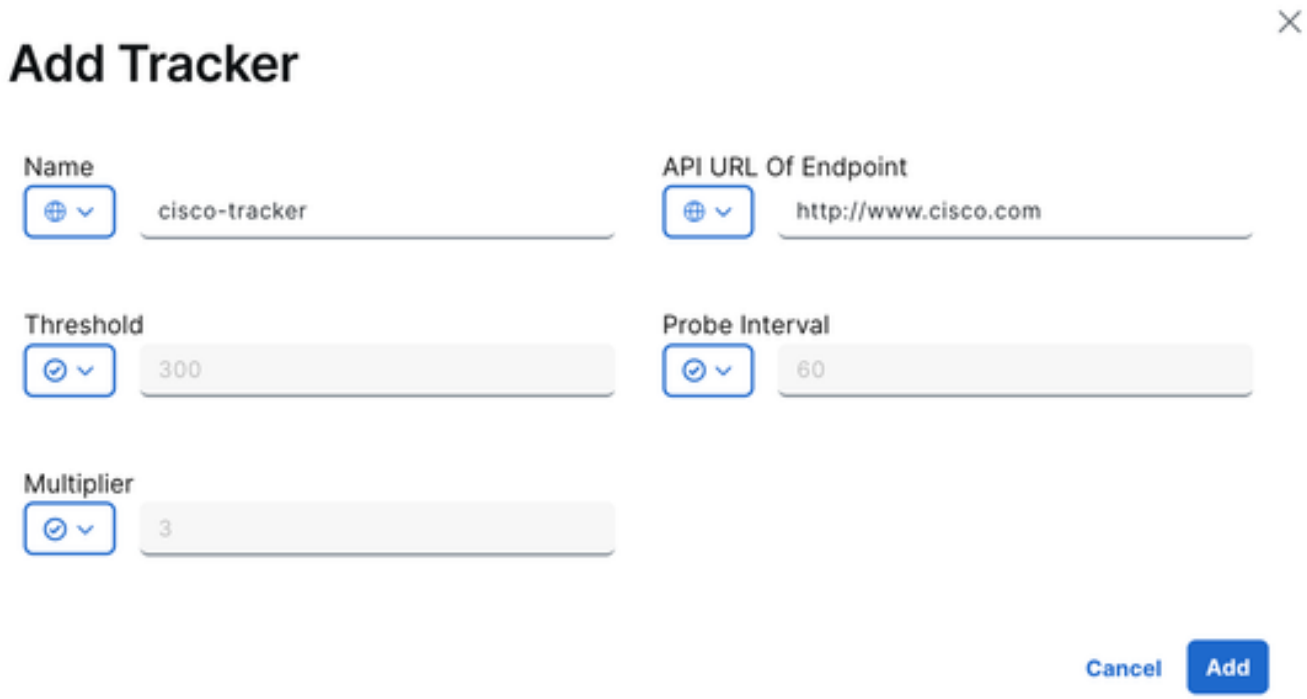
在SD-WAN Manager上，导航到Configuration > Policy Groups > Secure Internet Gateway/Secure Service Edge，然后单击Add Secure Service Edge(SSE)。

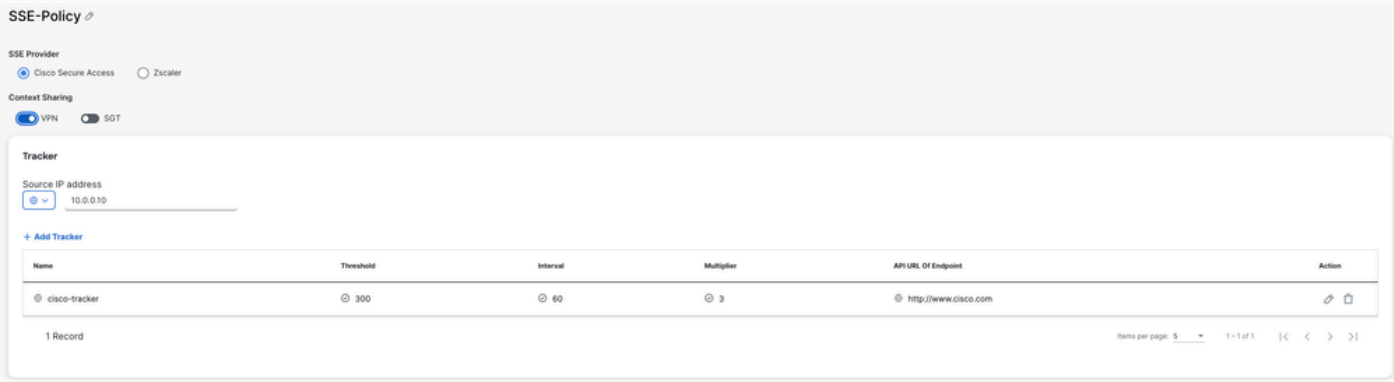


注意:如果尚未配置云凭证，您可以在此步骤添加它们。如果凭证已配置，将自动加载。



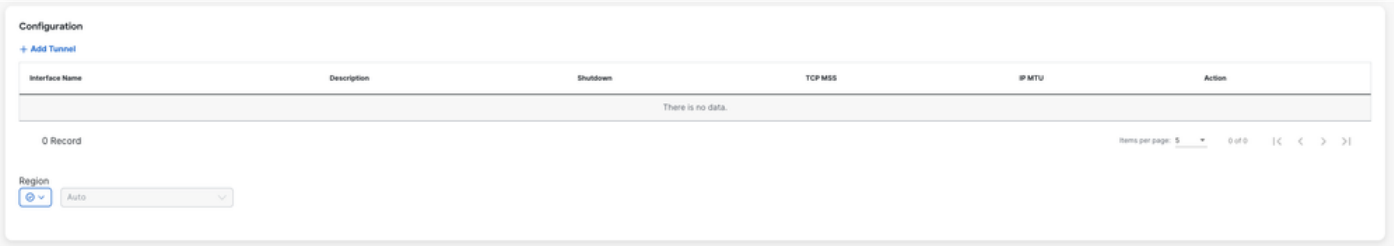
1.配置SSE跟踪器。在本示例中，跟踪器URL设置为http://www.cisco.com，并且从其中一个环回接口分配源IP地址。



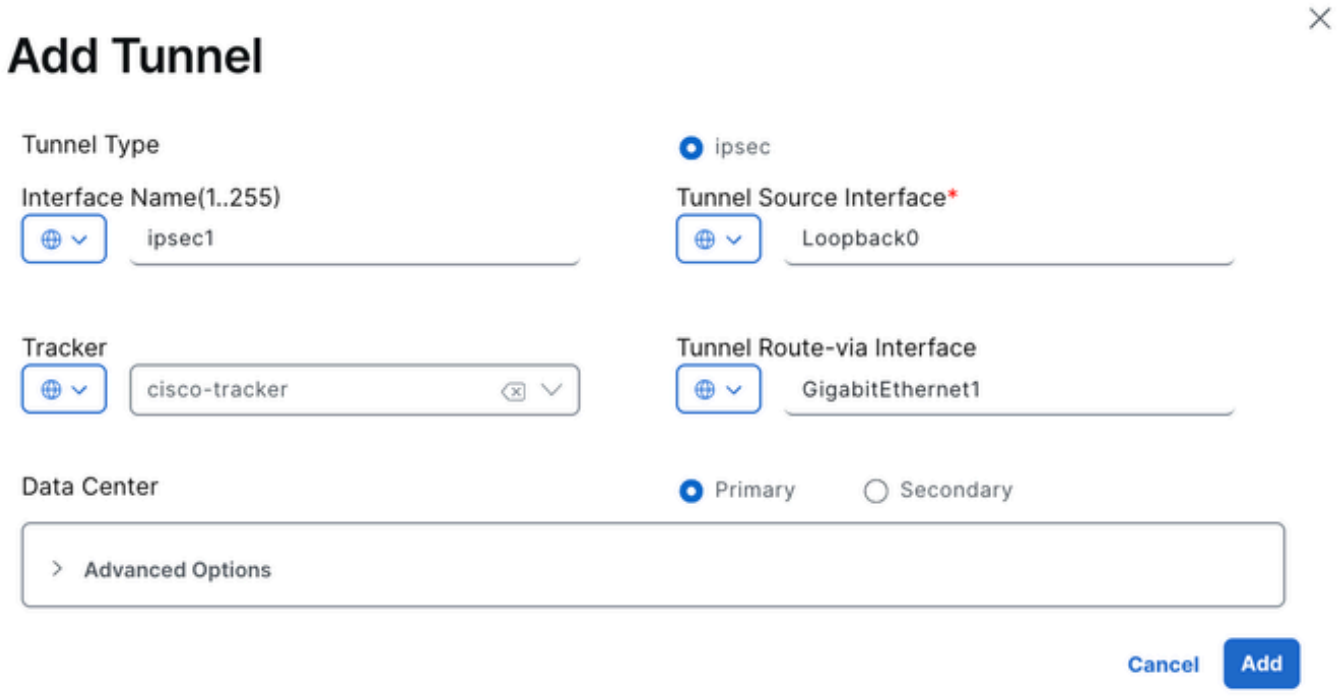


或者，由于配置云凭证时启用了情景共享，因此在本示例中将VPN选作选项。

2.单击Add Tunnel

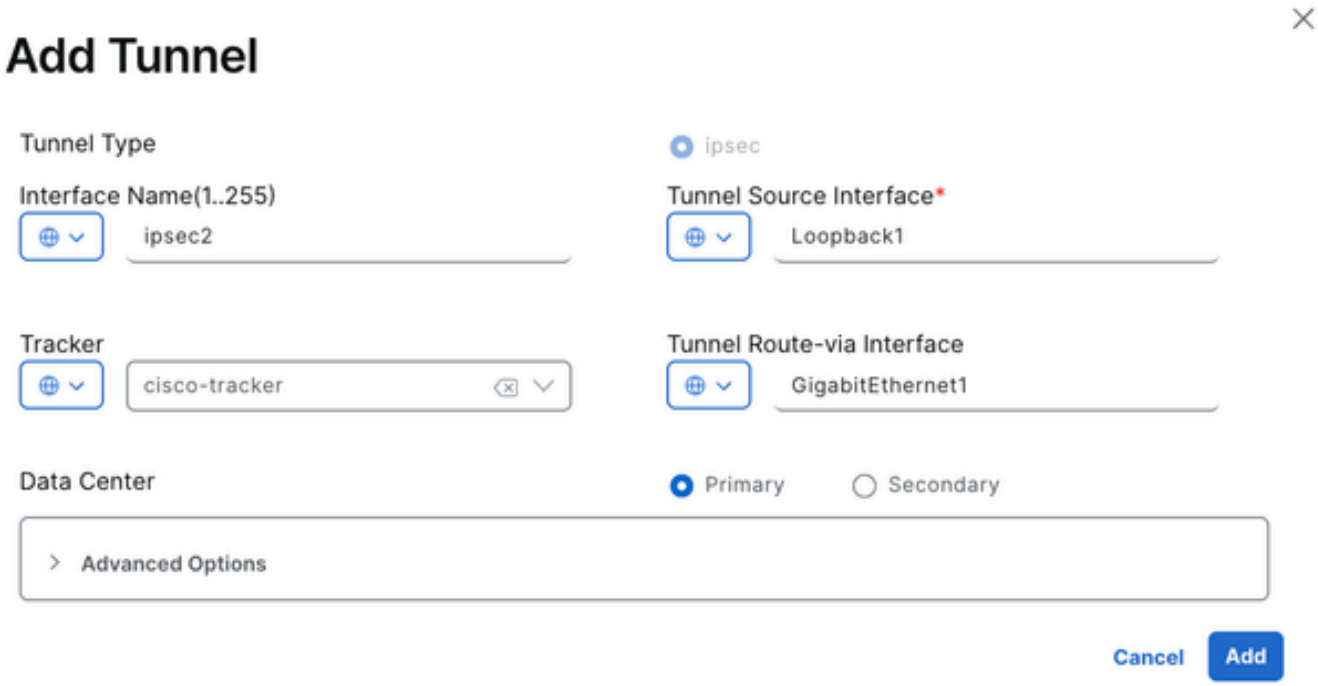


3.在本示例中，Loopback0接口用作隧道源，而GigabitEthernet1接口用作路由流量的WAN接口。



由于在本示例中配置了跟踪器，因此该设置更改为Global，并且已选择预配置的cisco-tracker。

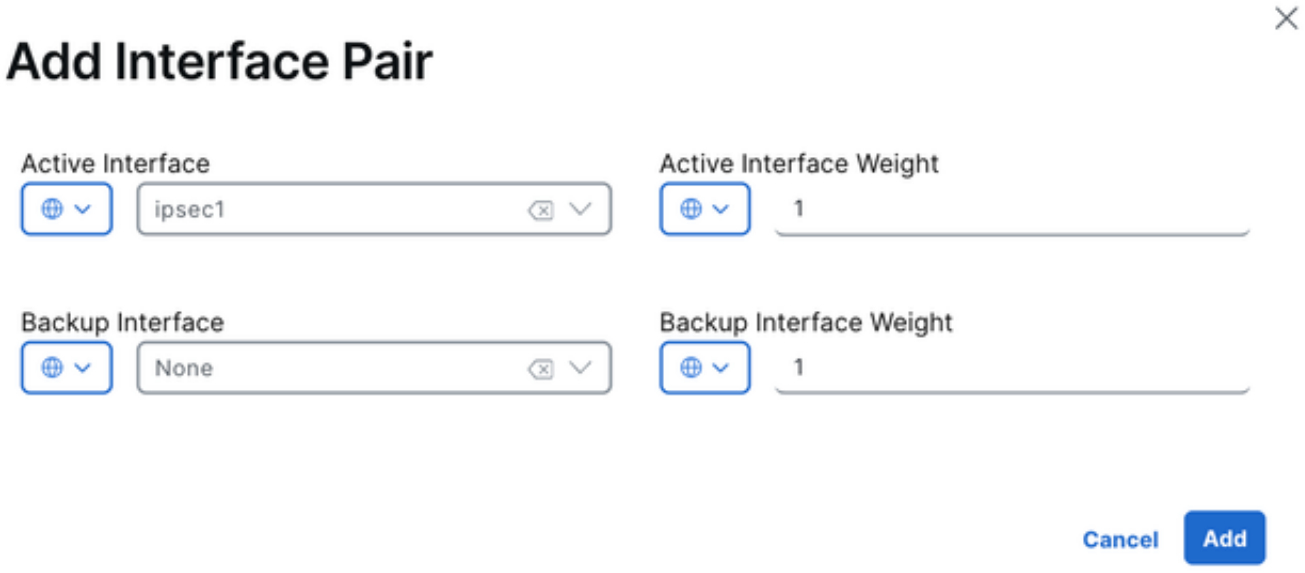
4.对于第二个隧道，使用相同的参数重复相同的步骤，但将Interface Name（接口名称）从ipsec1更改为ipsec2，将Source Interface Name（源接口名称）更改为Loopback1。



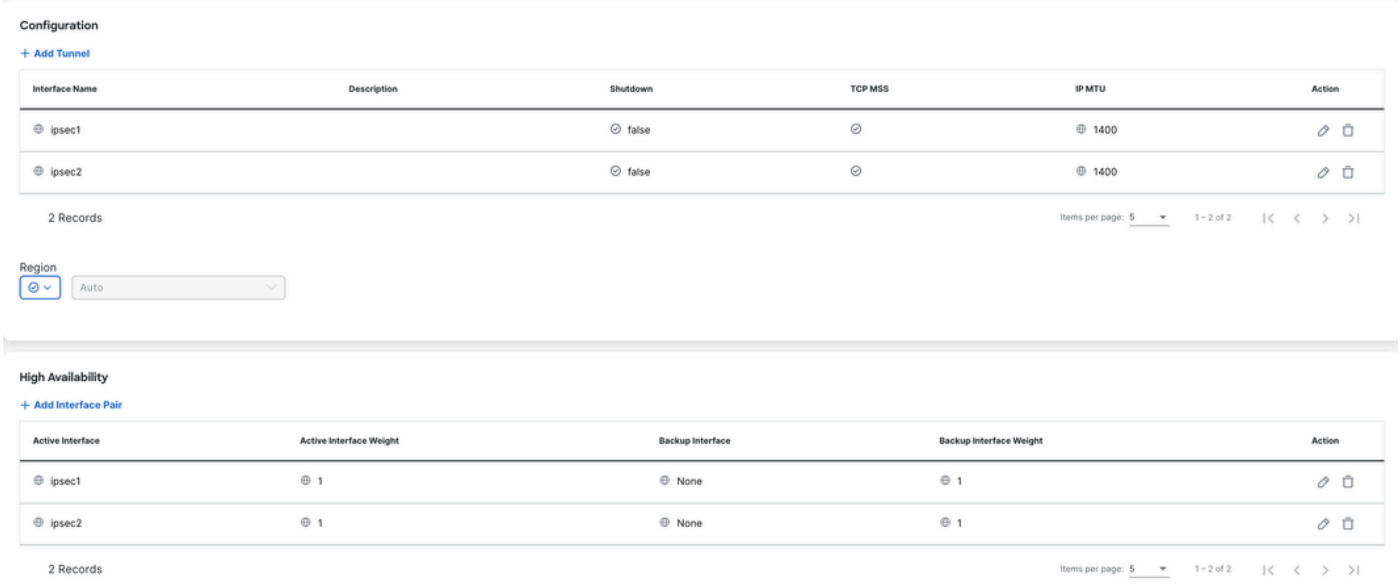
两个隧道都配置为同时处于活动状态，无需备份。

5.单击添加接口对。

6.单击Add。活动接口设置为ipsec1，但未指定备份接口。



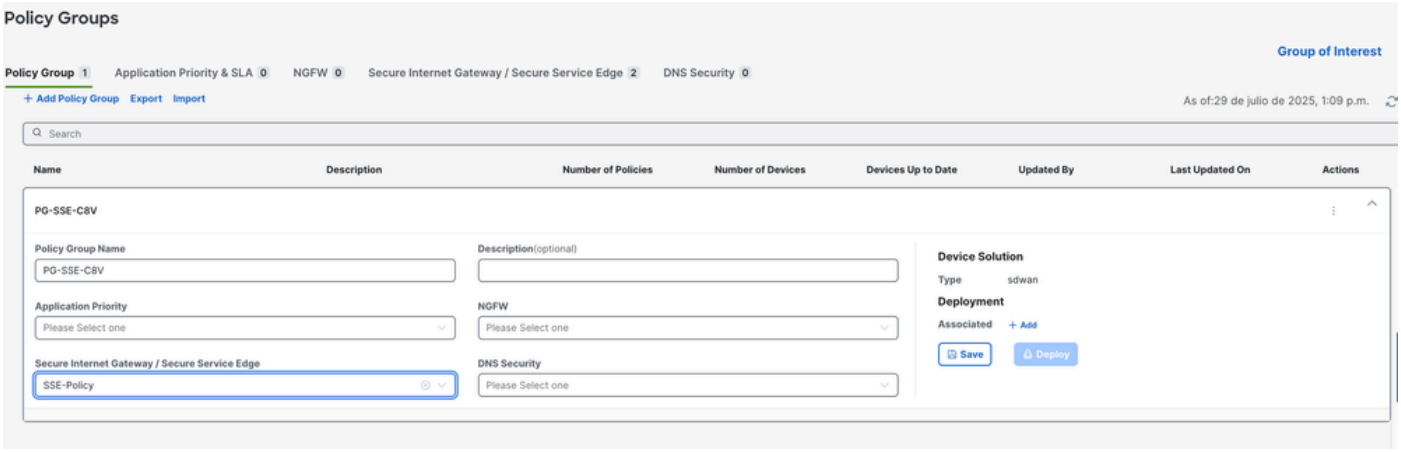
7.对第二个隧道ipsec2重复相同的操作。



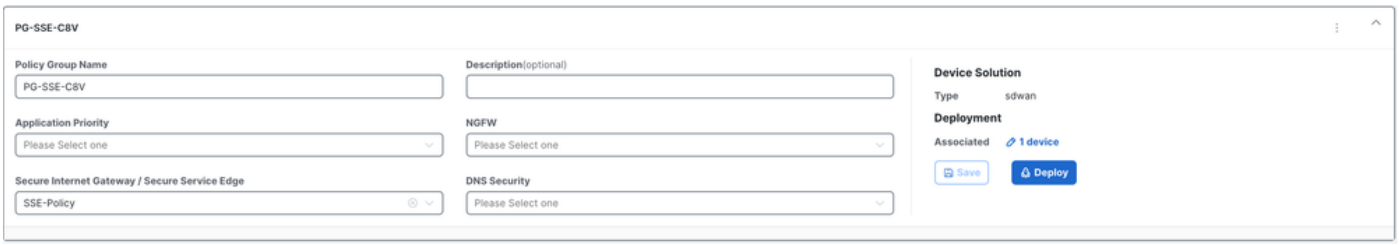
8.保存配置。

配置策略组

1.您可以选择之前在策略组中创建的策略并保存。



2.设备与策略组关联后，继续部署策略组。

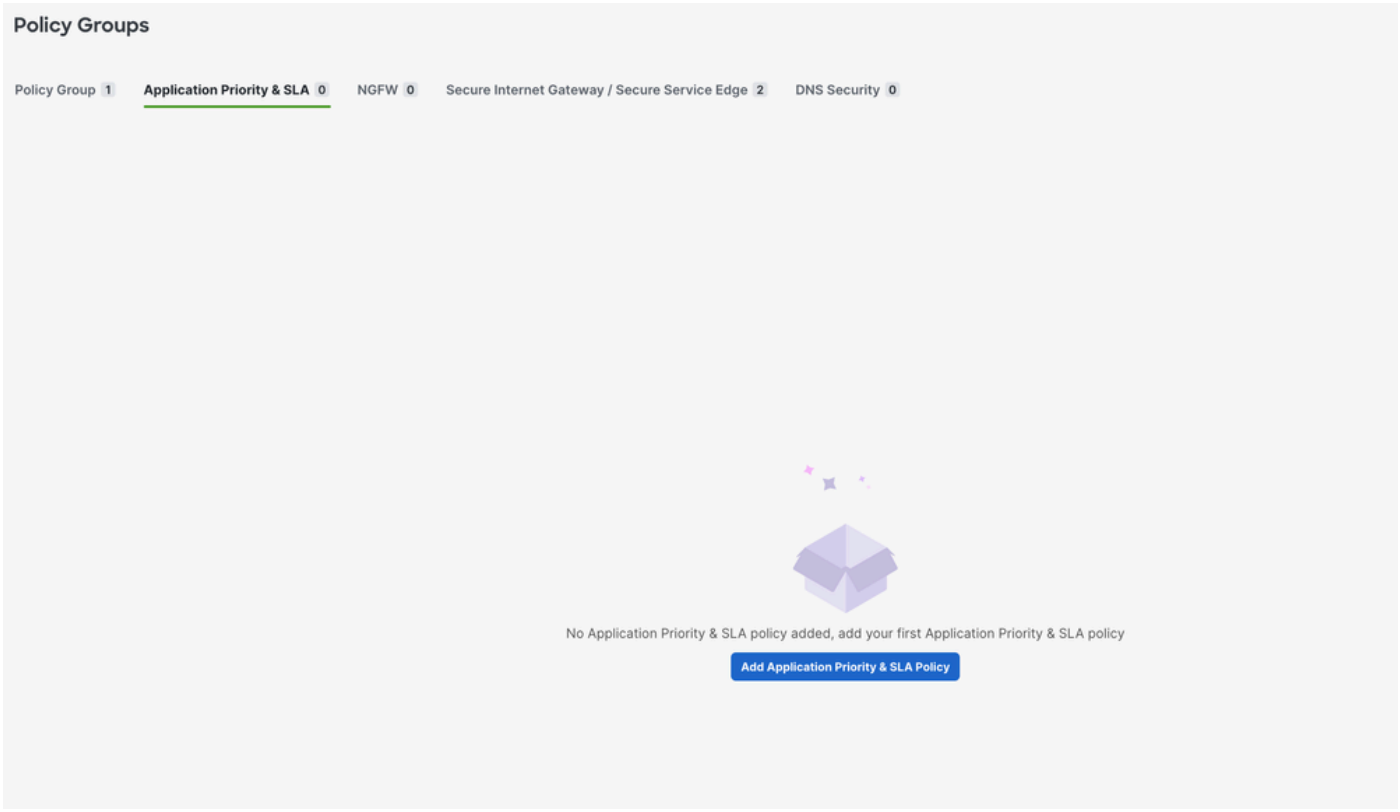


配置策略组以将流量重定向至SSE

1.在SD-WAN Manager上，导航到Configuration > Policy Groups > Application Priority & SLA。

- 选择Add Application Priority & SLA Policy

- 指定策略的名称。

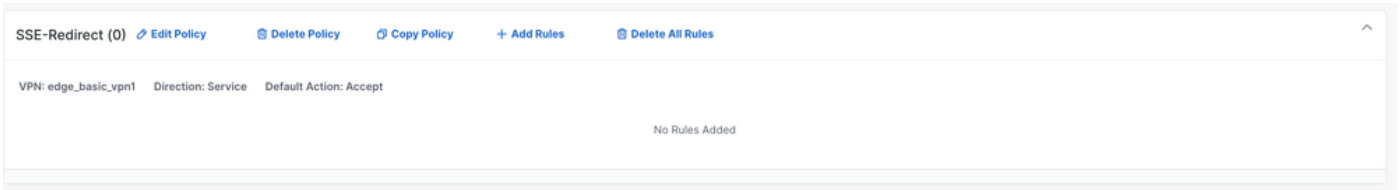


2.显示新策略后，选择“高级布局”切换。

3.选择添加流量策略列表。

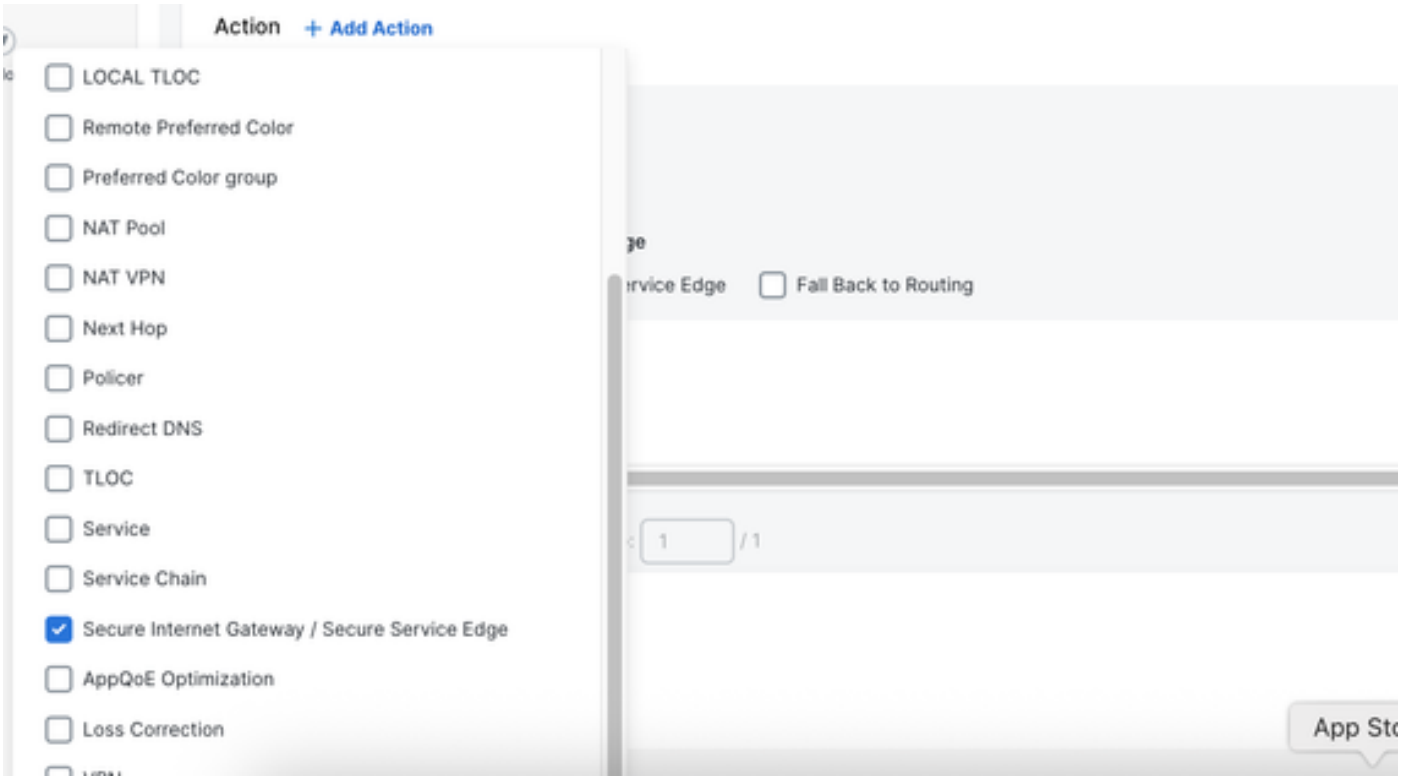
- 配置VPN以将流量重定向到SSE隧道。
- 根据需要设置Direction和Default Action并保存它。

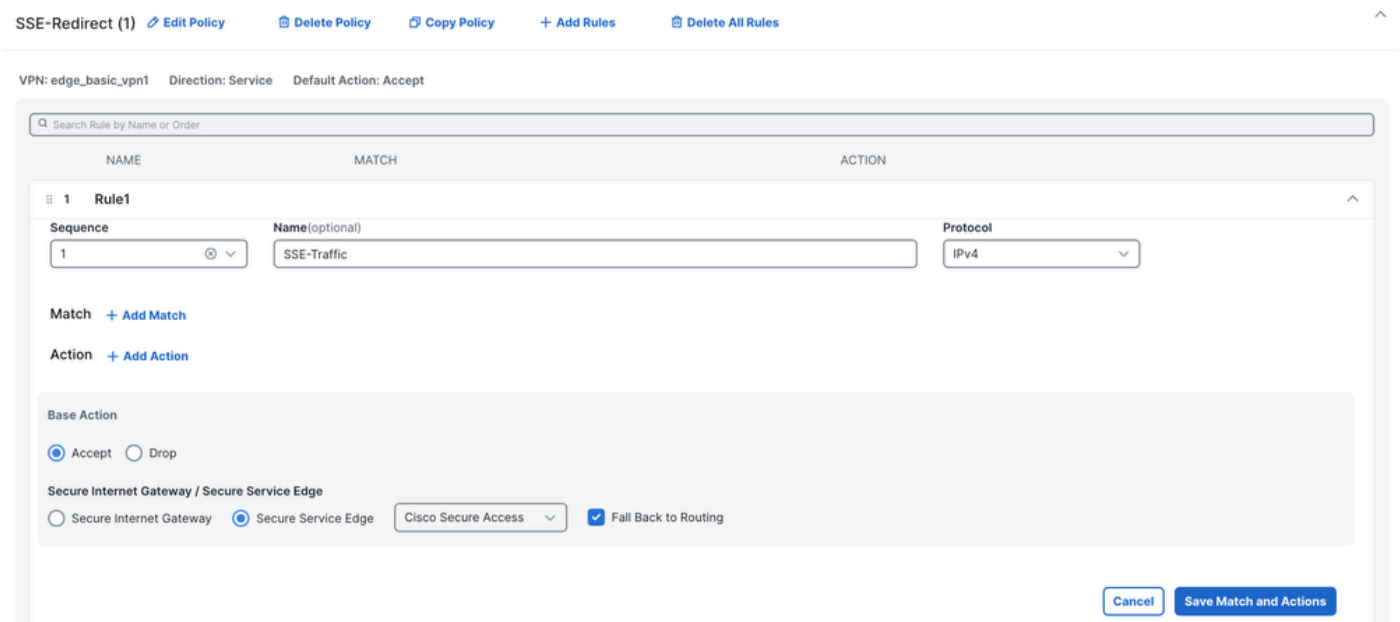
4.选择+ Add Rule。



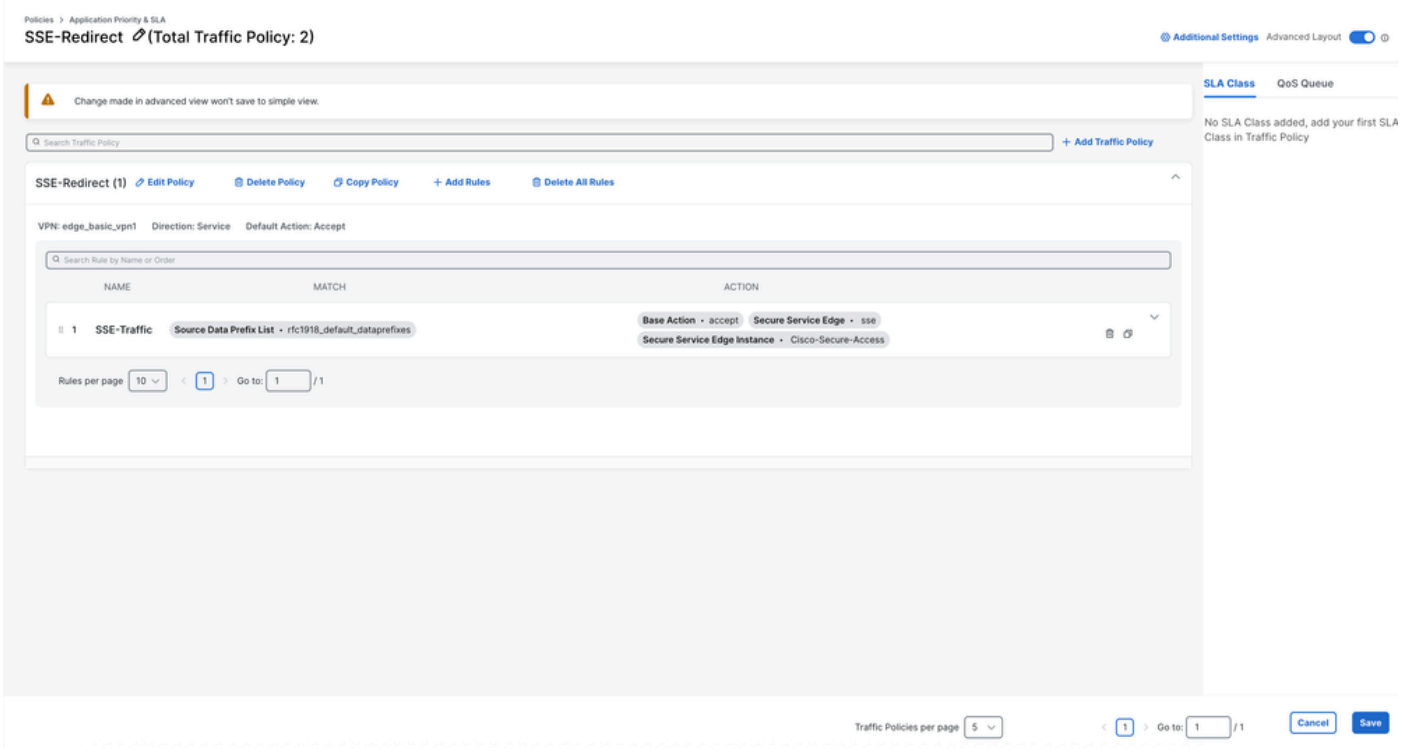
5.配置匹配流量条件，将流量重定向至SSE。
6.选择接受作为基本操作，然后单击+操作。

7.查找Secure Internet Gateway / Secure Service Edge操作并将其设置为Secure Service Edge。



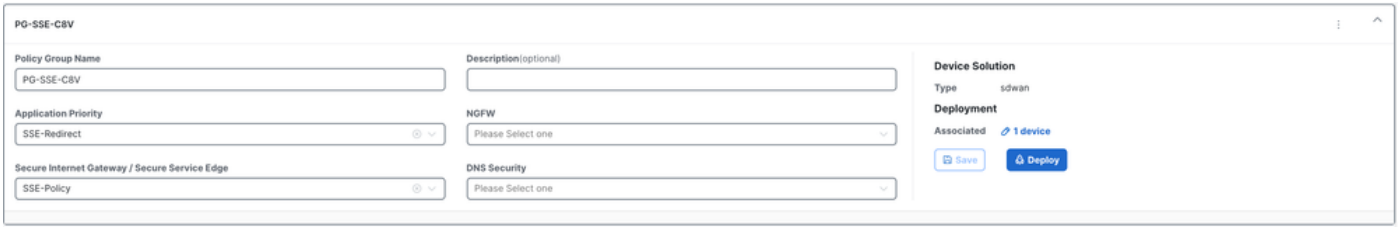


8.单击Save Match and Actions



9.单击保存。

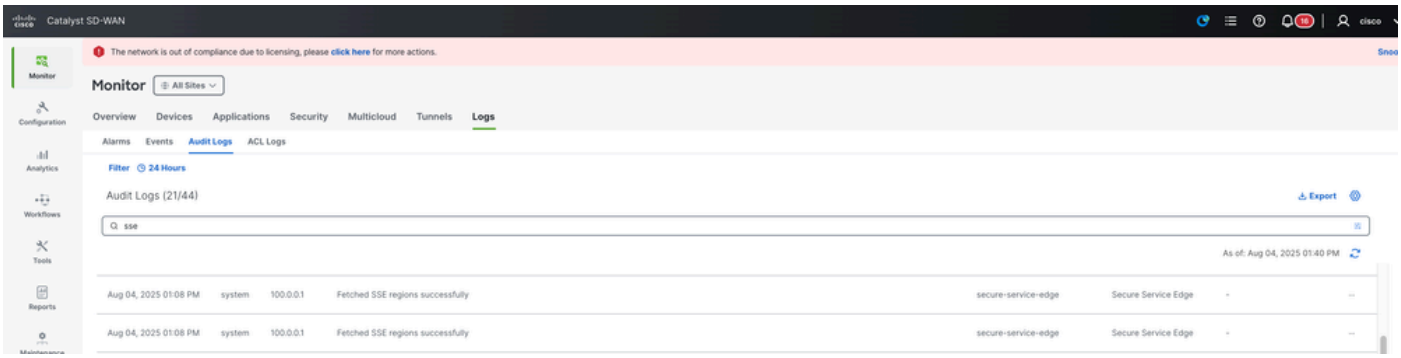
10.导航到配置>策略组，然后选择刚创建的应用优先级策略。保存，然后部署。



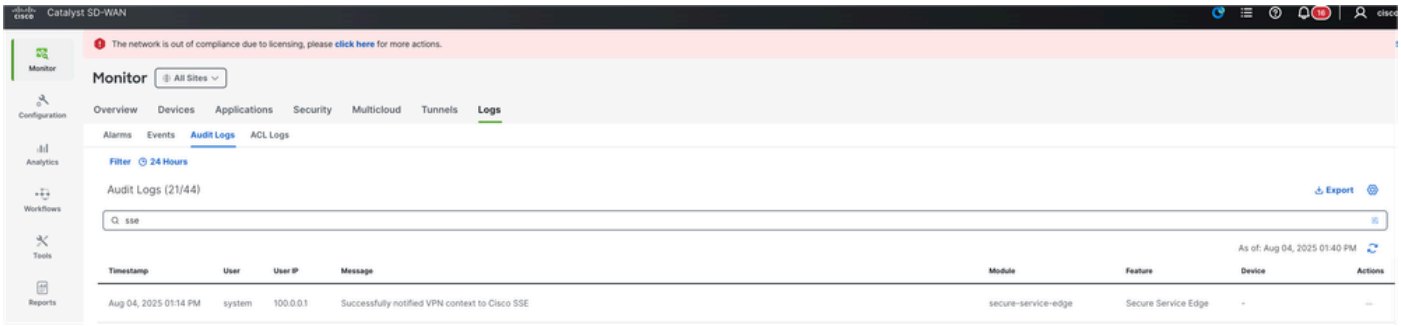
验证

经理

1.Monitor > Logs > Audit Logs并搜索“sse”。

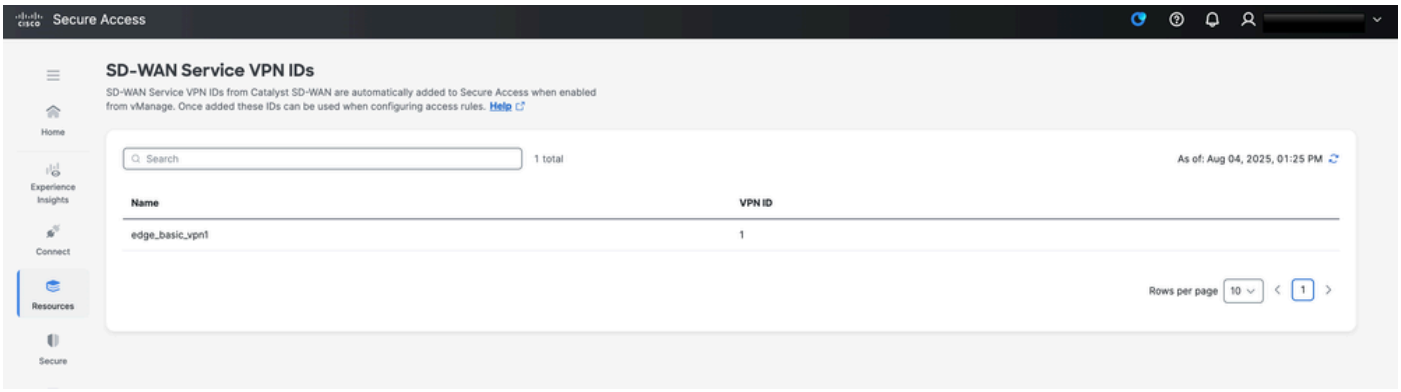


2.您可以通过检查Manager来验证情景共享VPN是否成功启用。



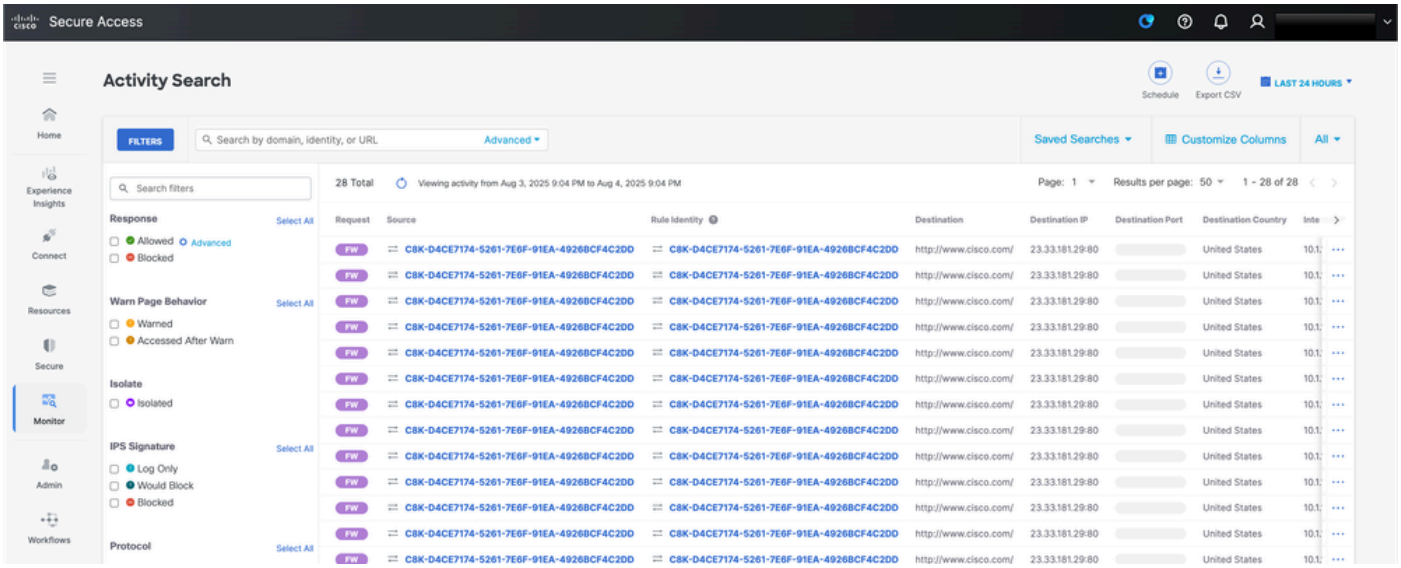
安全访问控制面板

情景共享
您可以通过检查SSE控制面板验证情景共享VPN是否成功启用，Resources > SD-WAN Service VPN IDs



建立隧道

当隧道启动且跟踪器运行且流量流经隧道时，您可以通过导航到监控>活动搜索来验证这一点。在此屏幕上，您会看到通过隧道的流量，例如由跟踪器生成的对www.cisco.com的请求。这种可视性可确认跟踪器已启动并主动监控通过隧道的流量



命令行界面(CLI)命令

<#root>

```
Hub2-SIG#show sse all
**************************************
SSE Instance Cisco-Secure-Access
**************************************
Tunnel name : Tunnel16000001
Site id: 2
Tunnel id: 655184839
SSE tunnel name: C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD
HA role: Active

Local state: Up


Tracker state: Up


Destination Data Center: 44.217.195.188
Tunnel type: IPSEC
Provider name: Cisco Secure Access
Context sharing: CONTEXT_SHARING_SRC_VPN
```

相关信息

- 配置情景共享SD-WAN
- 思科安全访问与SD-Routing集成
- 技术支持和文档 - Cisco Systems

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）。