設定Catalyst SD-WAN上的安全存取(SSE)整合併疑難排解

目錄

[簡介](#)

[必要條件](#)

- [需求](#)
- [採用元件](#)

[Cisco Secure Access](#)

[初步配置](#)

- [建立環回介面](#)

[在SSE門戶上配置新的API金鑰](#)

[在Catalyst Manager上配置SSE](#)

- [設定雲憑據](#)
- [使用策略組配置SSE隧道](#)
- [配置策略組](#)

[配置策略組以將流量重定向到SSE](#)

[驗證](#)

- [經理](#)
- [安全訪問控制面板](#)
- [命令線路介面(CLI)命令](#)

簡介

本文檔介紹如何在Catalyst SD-WAN上配置主用 — 主用SSE整合，並指導對其進行故障排除。

必要條件

需求

思科建議您瞭解以下主題：

- 思科軟體定義廣域網路(SD-WAN)
- 配置組
- 策略組

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- C8000V版本17.15.02

- vManage版本20.15.02
- Cisco Secure Access帳戶

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

Cisco Secure Access

思科安全訪問是一種基於雲的安全服務邊緣(SSE)解決方案，可融合多種網路安全服務，從雲交付這些服務以支援混合型員工。Cisco SD-WAN Manager利用REST API從Cisco Secure Access中檢索策略資訊，並將此資訊分發到Cisco IOS XE SD-WAN裝置。這一整合為使用者提供了無縫、透明且安全的直接網際網路接入(DIA)，使使用者能夠從任何裝置安全地連線到網路。

Cisco SSE允許SD-WAN裝置使用IPSec隧道與SSE提供商建立連線。本檔案是供思科安全存取使用者使用的。

初步配置

- 為裝置啟用域查詢：導航到Configuration Groups > System Profile > Global，然後啟用Domain Lookup。

附註：預設情況下，「域查詢」處於禁用狀態。

- 配置DNS:路由器可以在VPN 0上解析DNS並訪問網際網路。
- 配置NAT DIA:建立SSE隧道的路由器上需要存在DIA配置。

建立環回介面

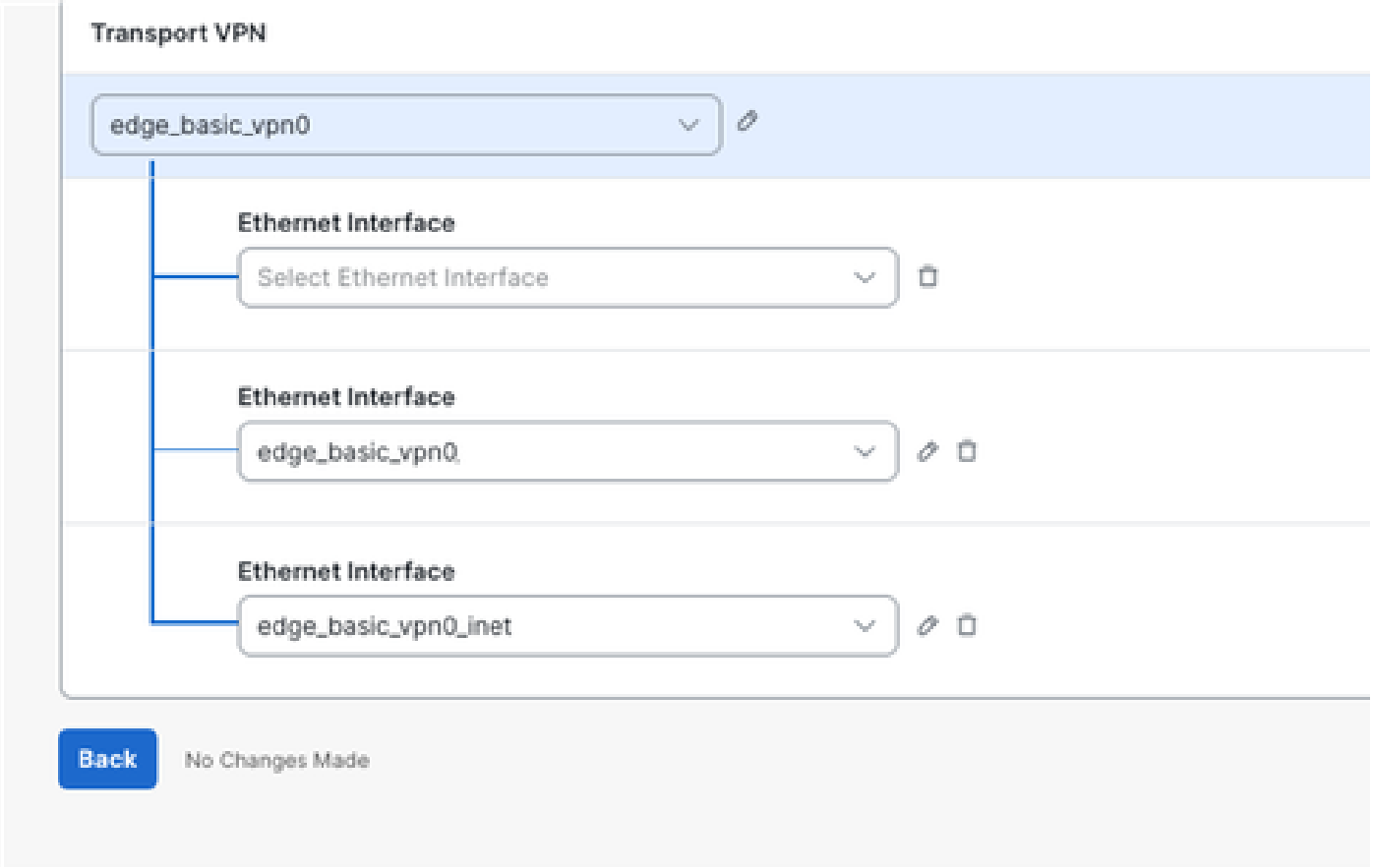
如果主用/主用配置中的兩個隧道連線到同一個目標資料中心，並使用相同的WAN介面作為源，則需要建立兩個環回IP地址。

附註：當使用相同的源和目標配置兩個隧道時，IKEv2會形成由本地ID和遠端ID組成的身份對。預設情況下，本地ID是隧道的源介面的IP地址。此標識對必須是唯一的，不能在兩個隧道之間共用。為防止在IKEv2狀態中出現混淆，每個隧道使用不同的環回介面作為其源。雖然IKE資料包在DIA介面上進行了轉換(NATed)，但本地ID保持不變，並保留原始環回IP地址。

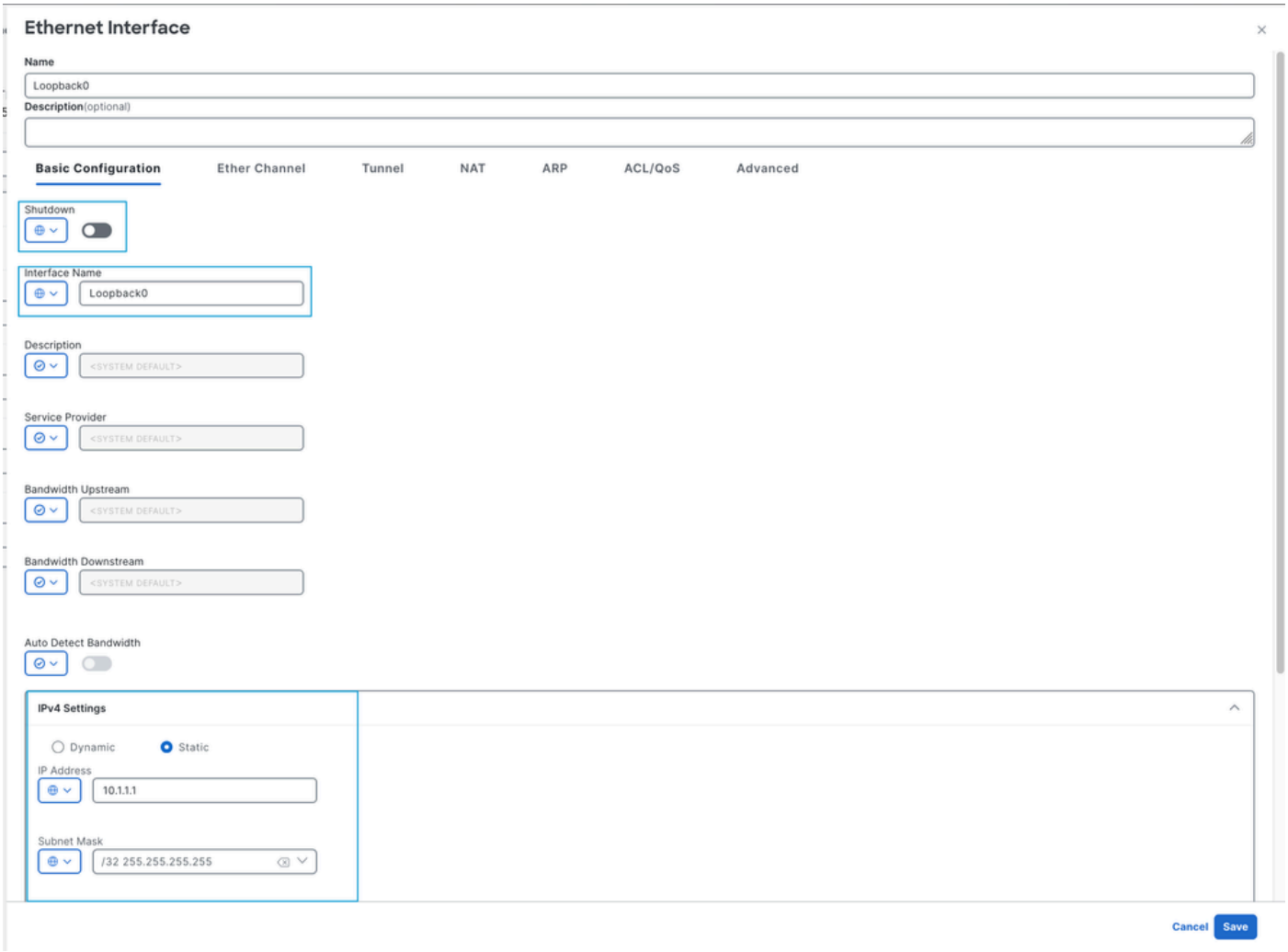
1.導覽至Configuration > Configuration Groups > Configuration Group Name> Transport & Management Profile>按一下Edit.

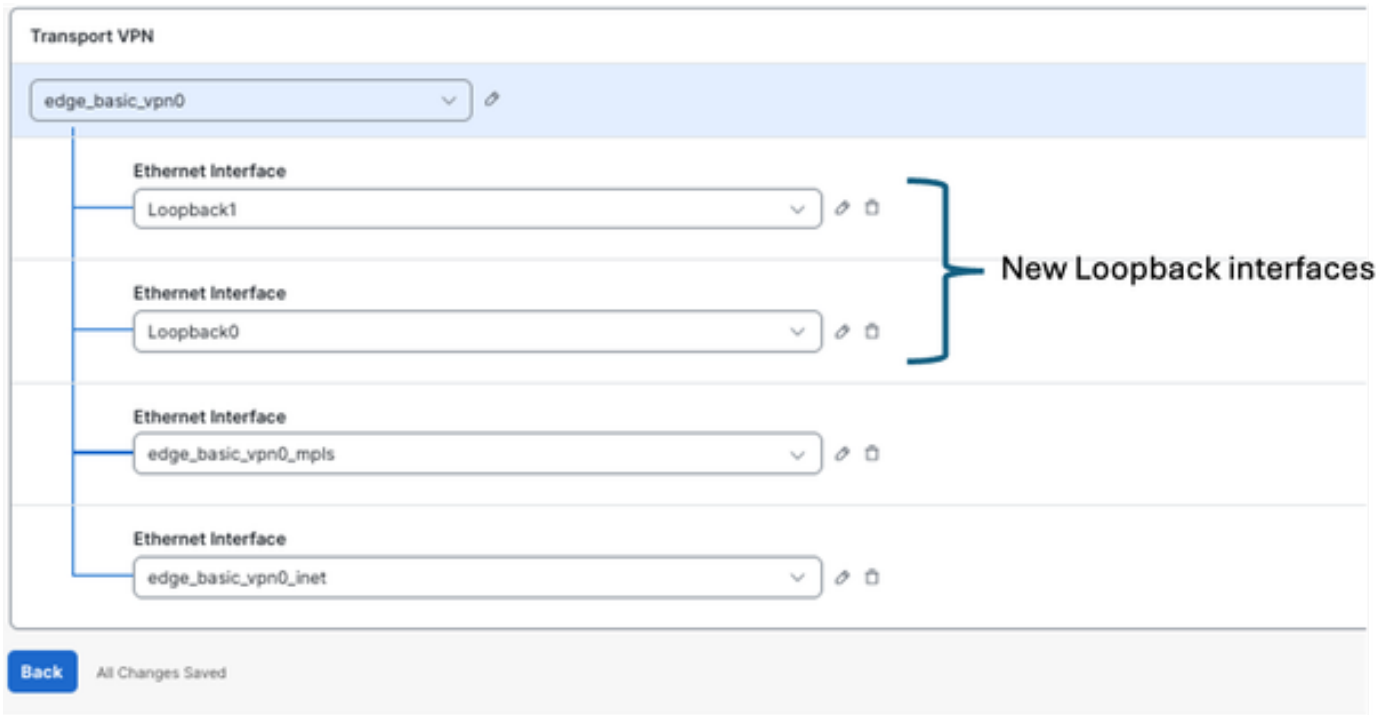
2.按一下傳輸VPN配置文件（主配置檔案）右側的加號(+)。 這將開啟位於最右邊的Add Feature選單。

3.按一下Ethernet Interface。它在傳輸VPN下新增新的Internet介面。



4.使用RFC1918 IPv4位址建立兩個回送介面，如圖中的Loopback0範例。

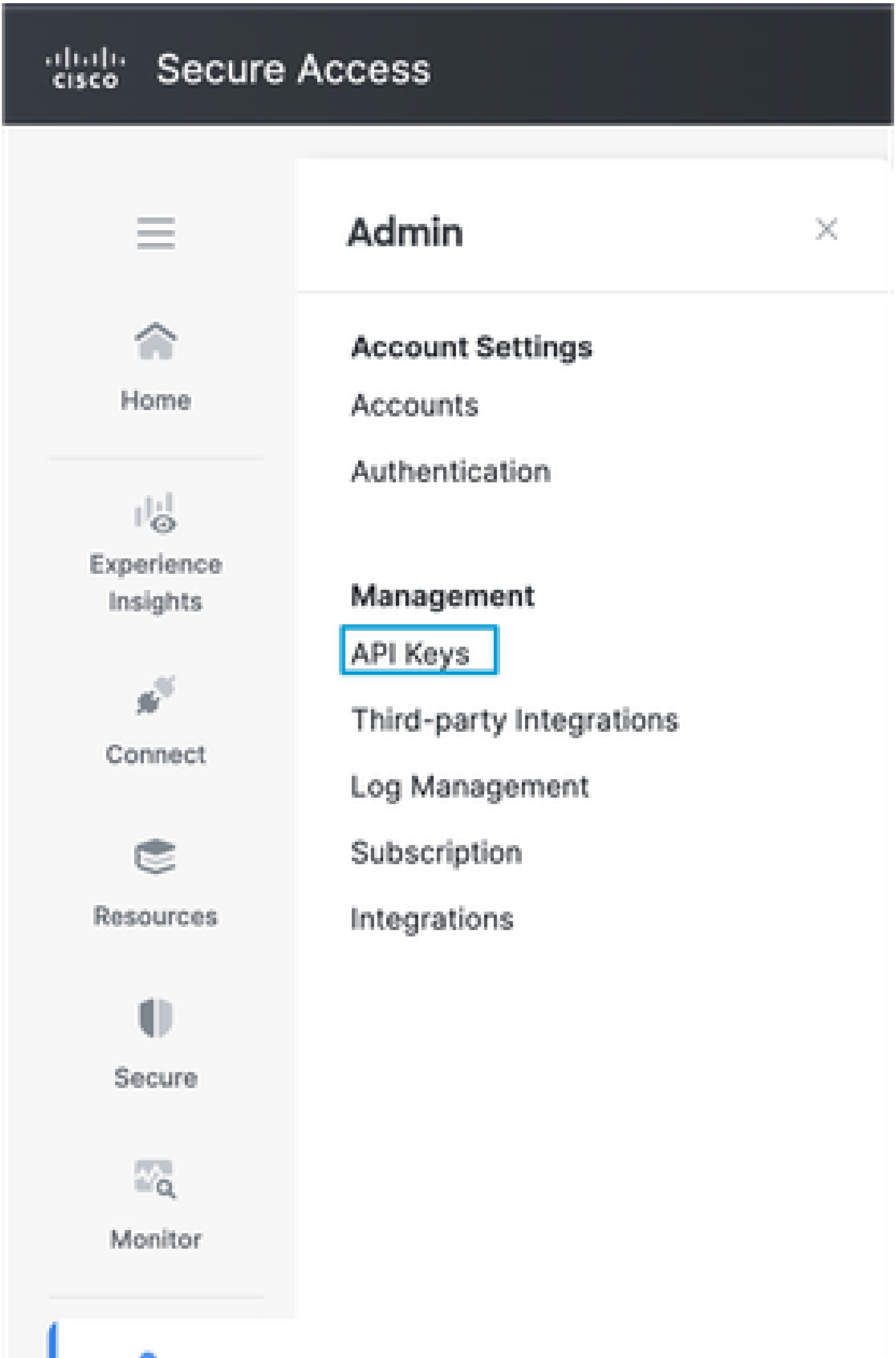




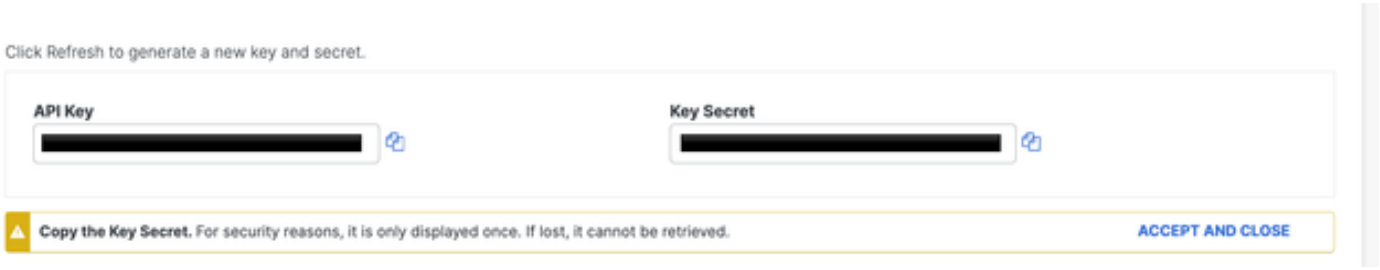
5. 應用環回配置後，繼續將配置更改部署到裝置。請注意，置備狀態從1/1變為0/1。

在SSE門戶上配置新的API金鑰

1.訪問SSE入口網站https://login.sse.cisco.com/
2.導航到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.將API金鑰和金鑰金鑰複製到記事本中，然後選擇ACCEPT AND CLOSE

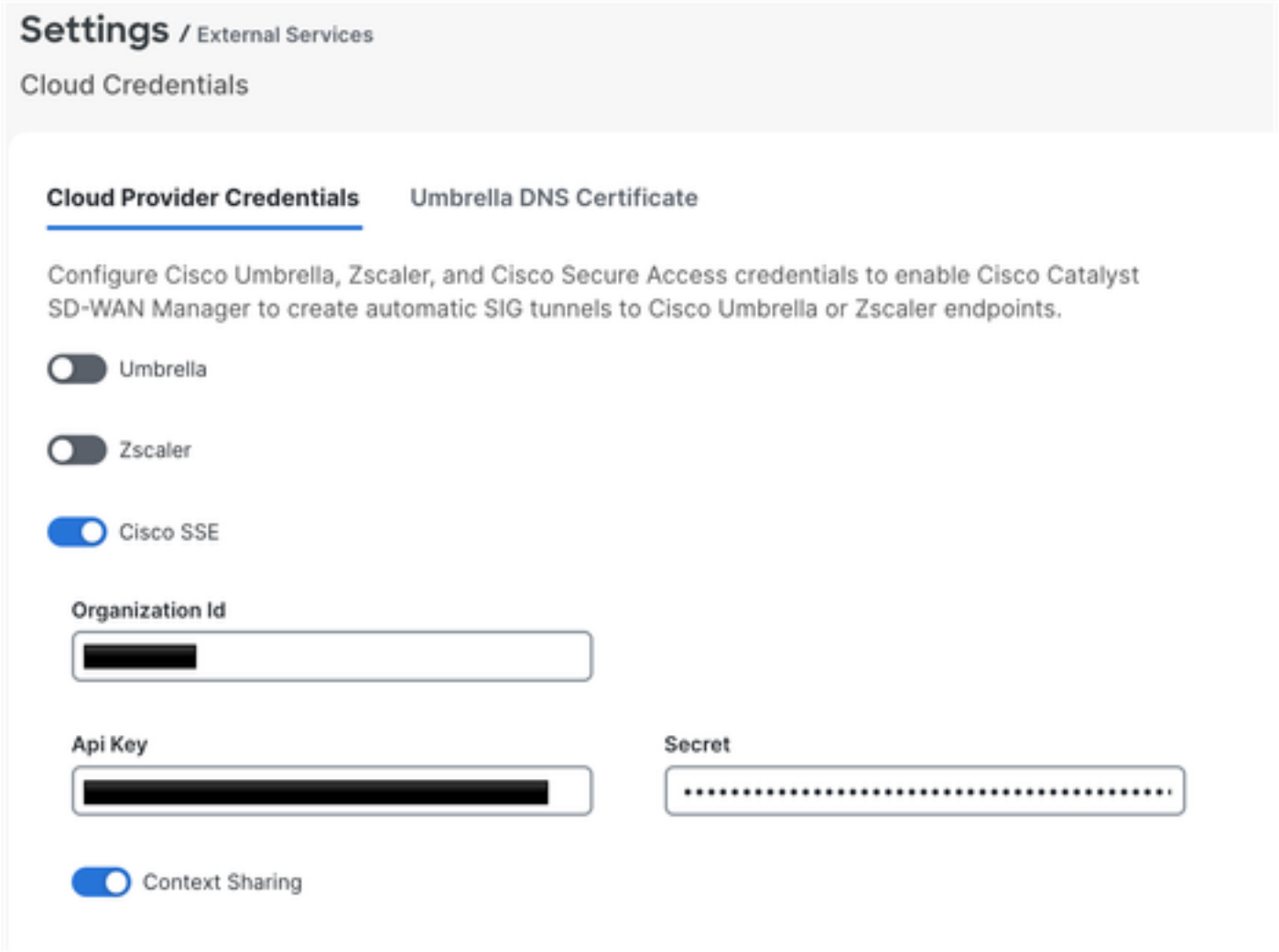


7.在URL https://dashboard.sse.cisco.com/#some-numbers#/admin/apikeys下，#some-numbers#是您的組織ID。也將該資訊複製到您的記事本中。

在Catalyst Manager上配置SSE

設定雲憑據

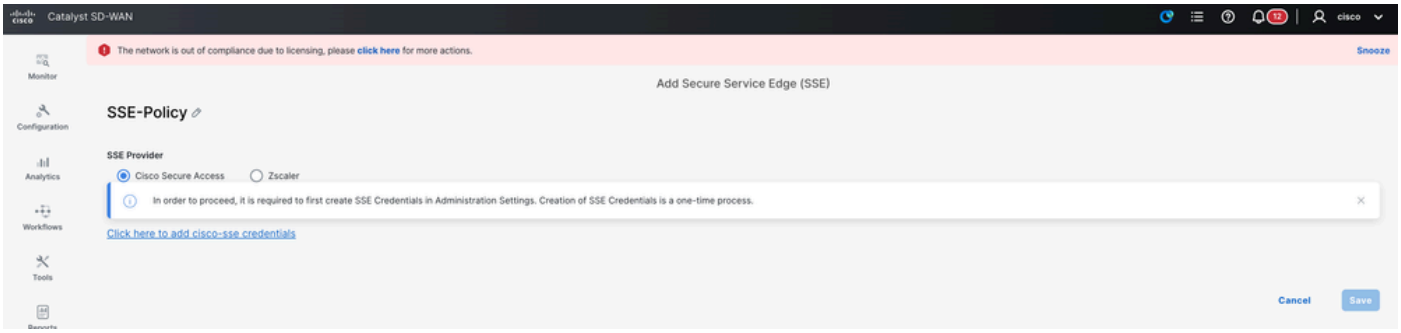
1.導航到管理 > 設定 > 雲憑據 > 雲提供商憑據，然後啟用Cisco Secure Access並輸入詳細資訊。



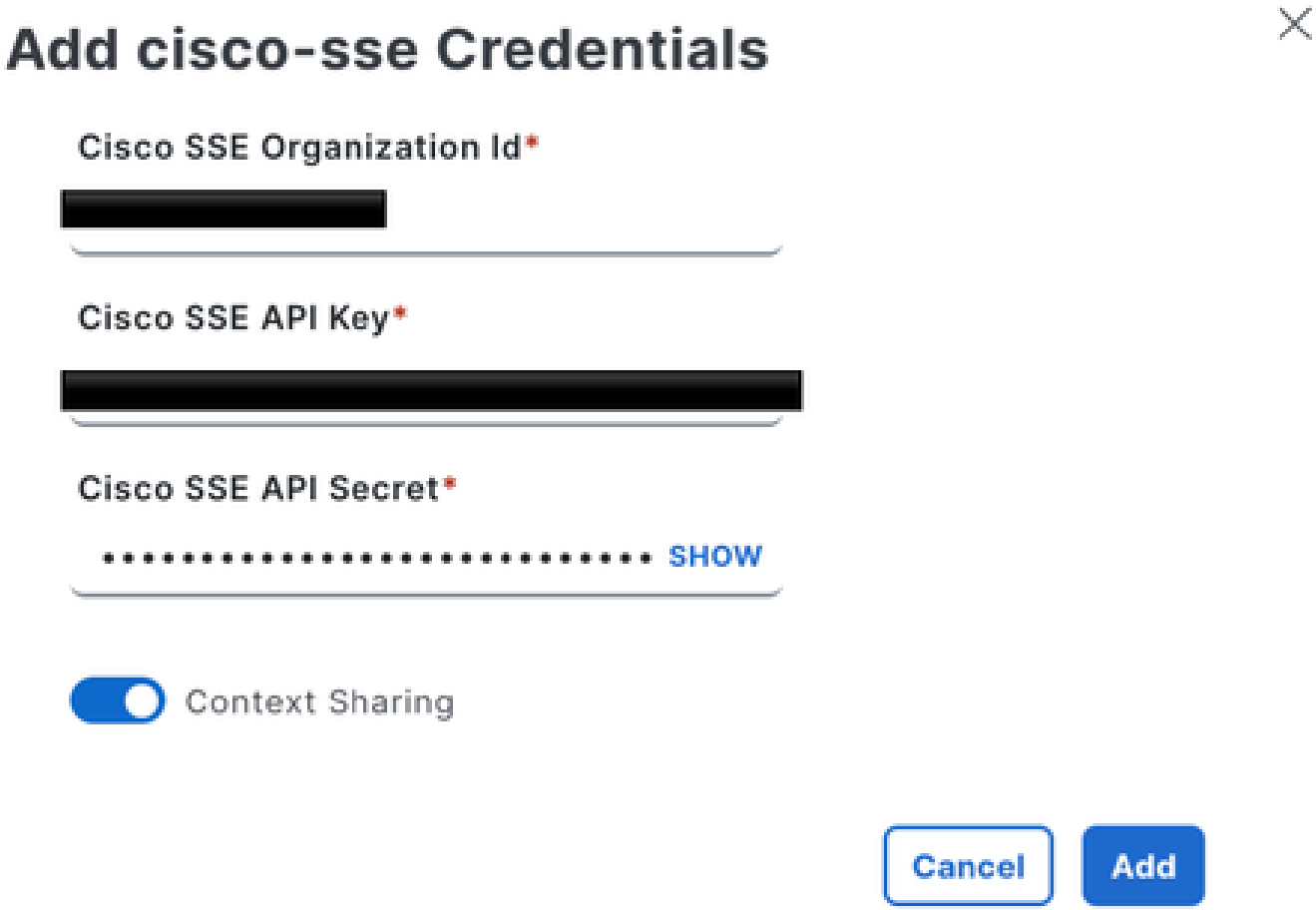
2.可選：您可以啟用上下文共用以增強功能。有關更多資訊，請參閱[關於情景共用的Cisco SSE使用手冊](#).

使用策略組配置SSE隧道

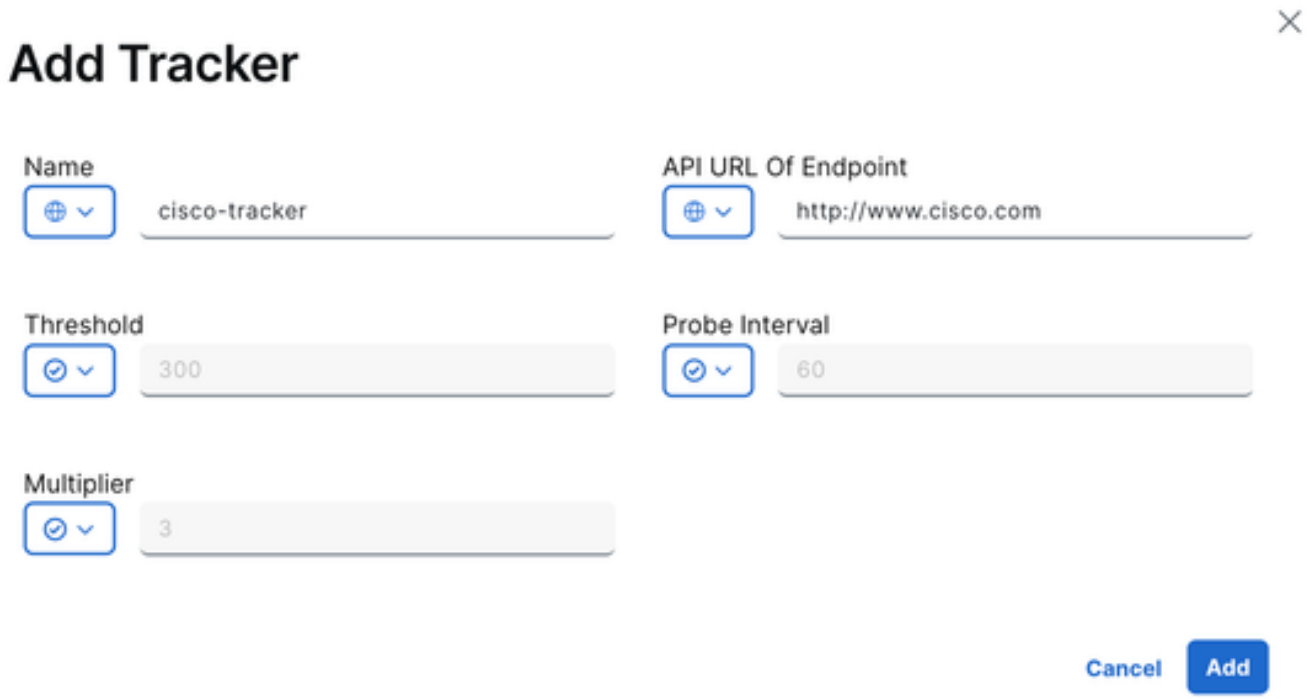
在SD-WAN Manager上，導航至Configuration > Policy Groups > Secure Internet Gateway/Secure Service Edge，然後點選Add Secure Service Edge(SSE)。

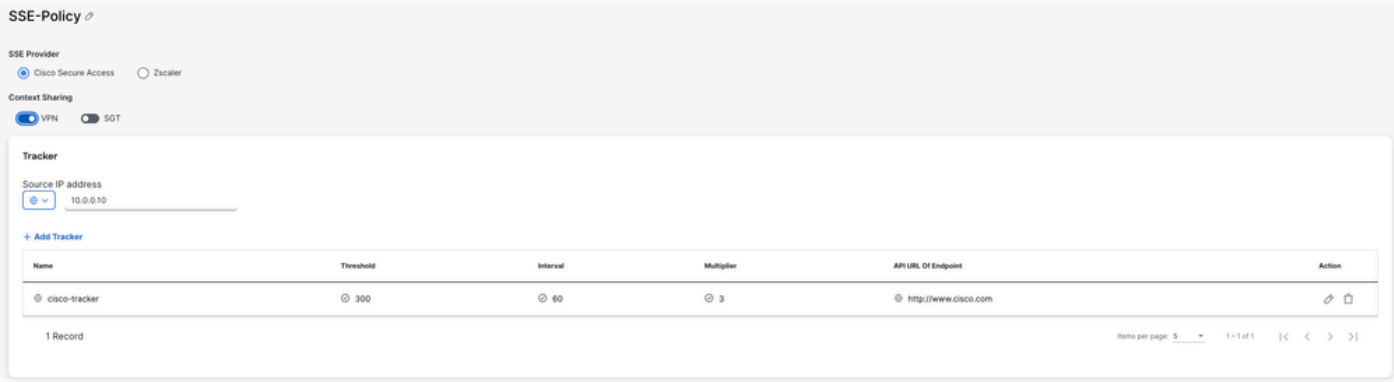


注意:如果尚未配置雲憑據，則可以在此步驟新增它們。如果已配置憑據，則會自動載入這些憑據。



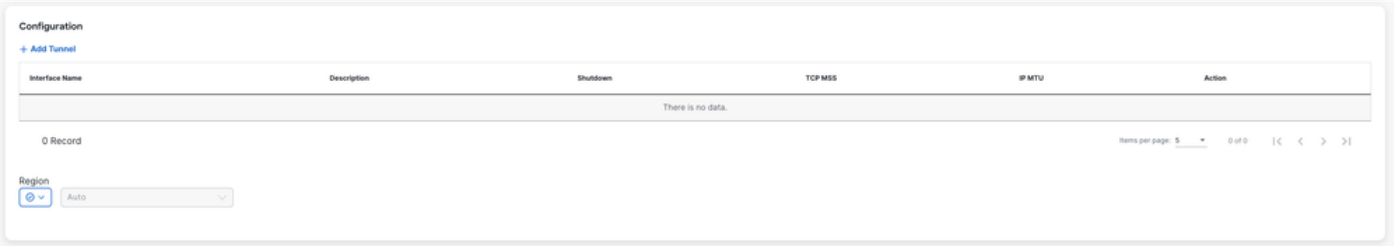
1.配置SSE跟蹤器。在此示例中，跟蹤器URL設定為http://www.cisco.com，並且從其中一個環回介面分配源IP地址。



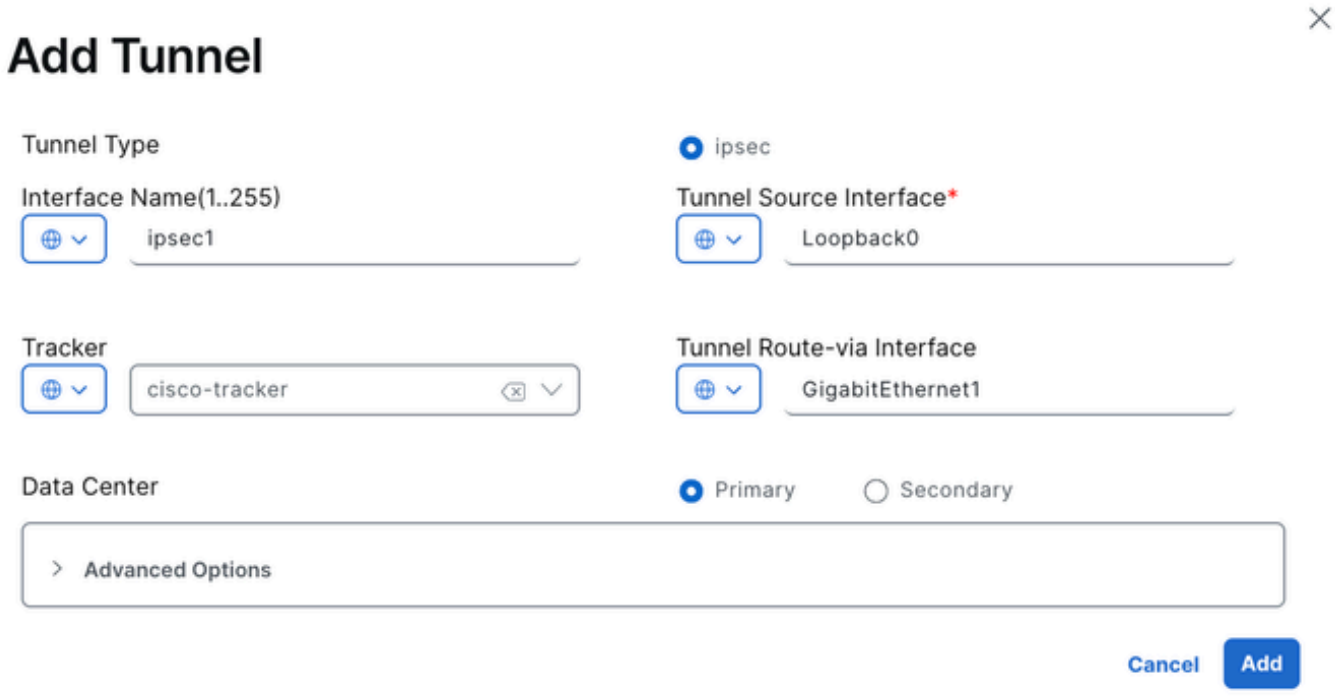


或者，由於配置雲憑據時啟用了上下文共用，因此在本示例中選擇了VPN作為選項。

2.按一下Add Tunnel

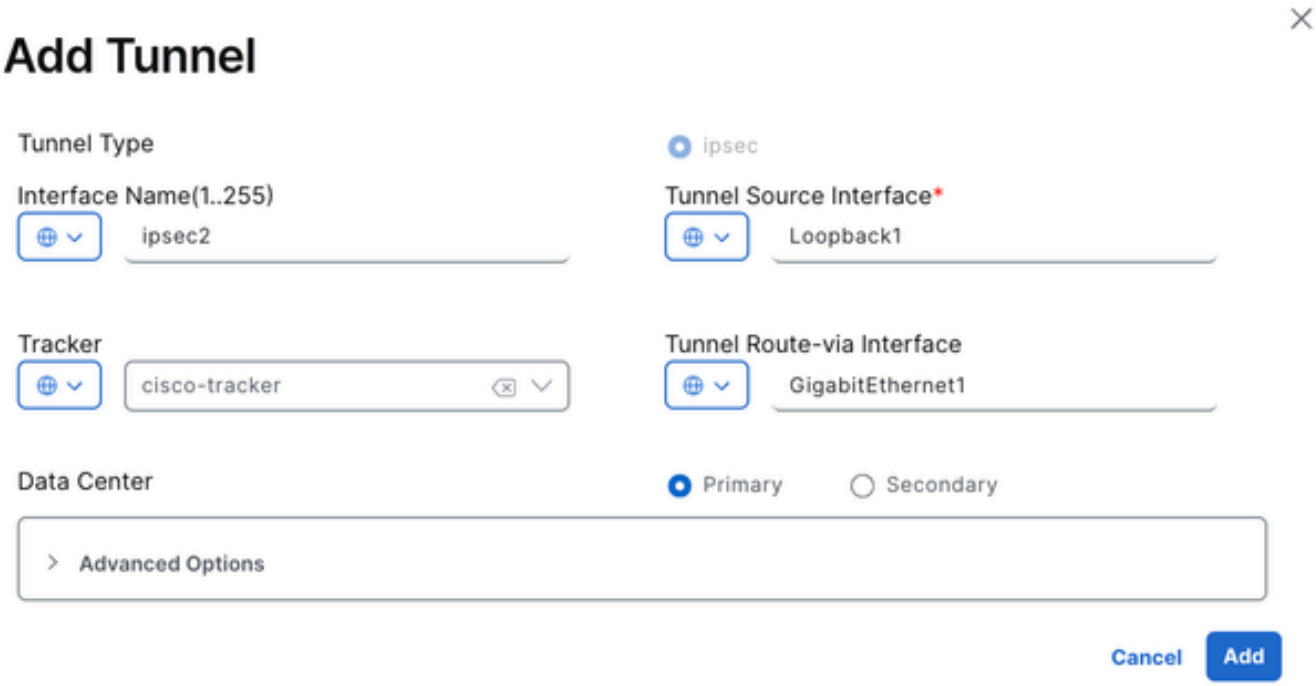


3.在本示例中，Loopback0介面用作隧道源，而GigabitEthernet1介面用作路由流量的WAN介面。



由於在本示例中配置了跟蹤器，因此將設定更改為Global，並且已選擇預配置的cisco-tracker。

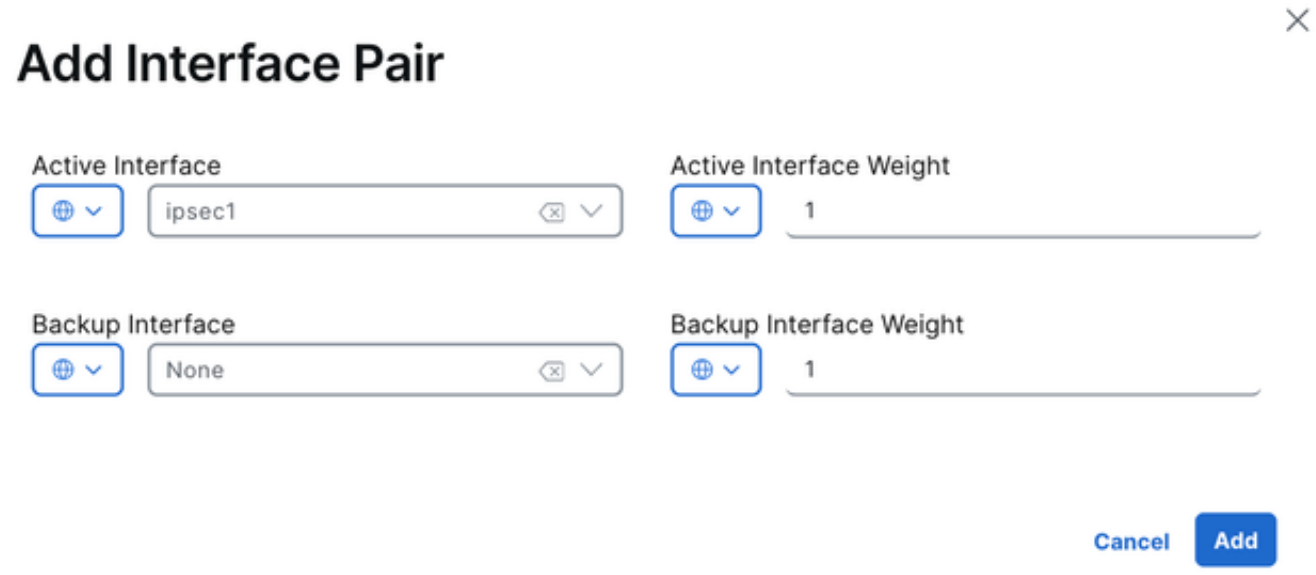
4.對於第二個隧道，使用相同的引數重複相同的步驟，但將介面名稱從ipsec1更改為ipsec2，將源介面名稱更改為Loopback1。



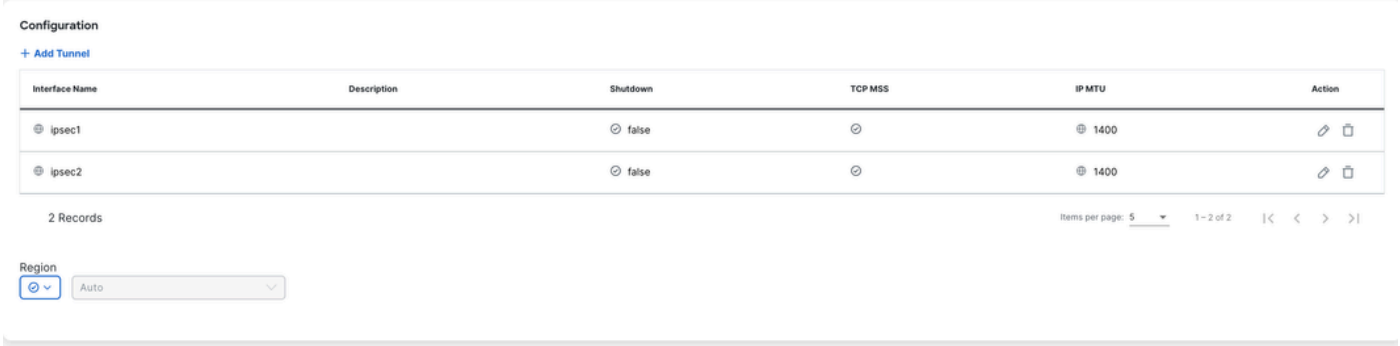
兩個隧道都配置為同時處於活動狀態，沒有備份。

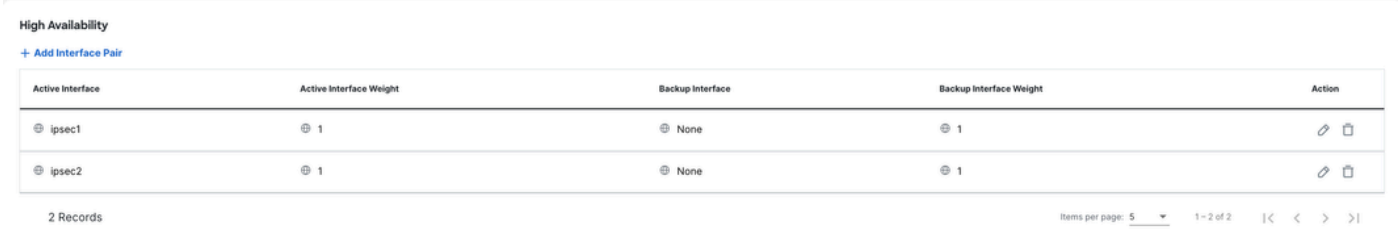
5.按一下「Add Interface Pair」。

6.按一下Add。活動介面設定為ipsec1，但未指定備份介面。



7.對第二個隧道ipsec2重複相同操作。

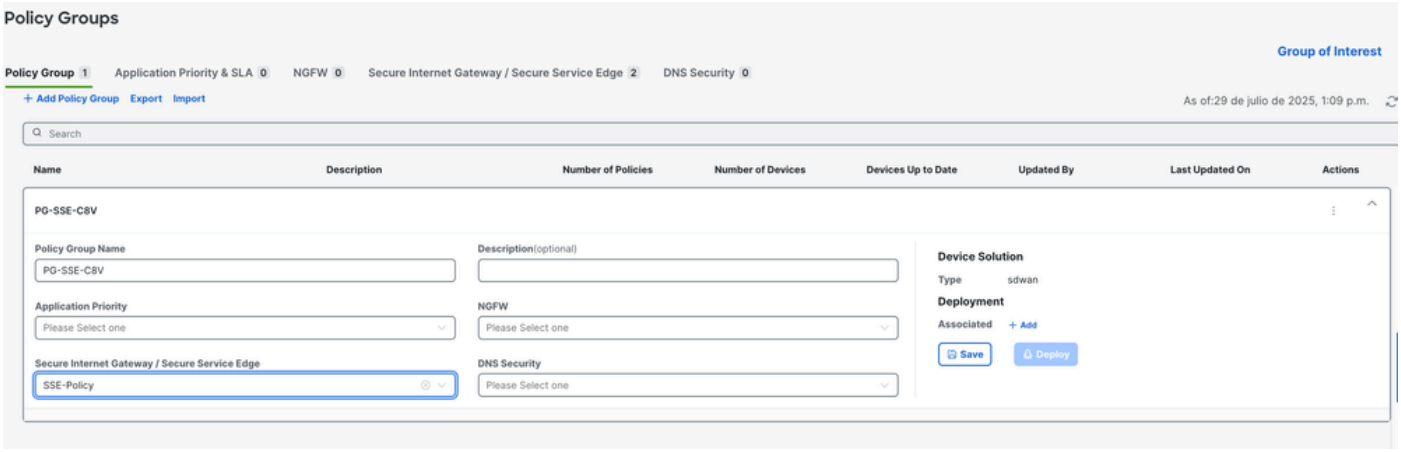




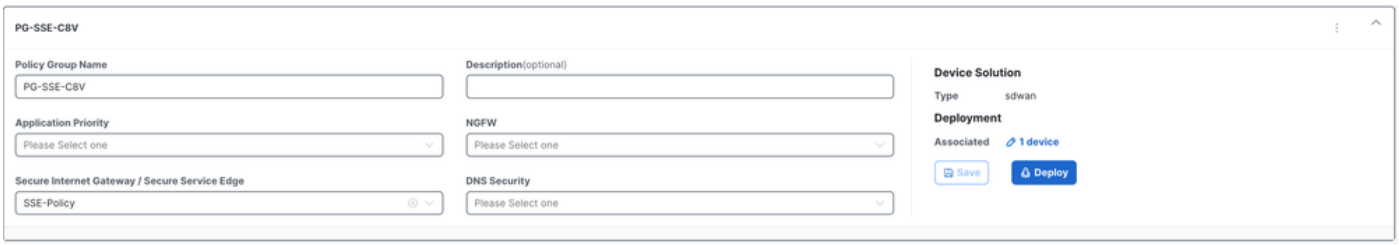
8.儲存配置。

配置策略組

1.您可以只選擇以前在策略組中建立的策略並儲存。



2.裝置與策略組關聯後，繼續部署策略組。

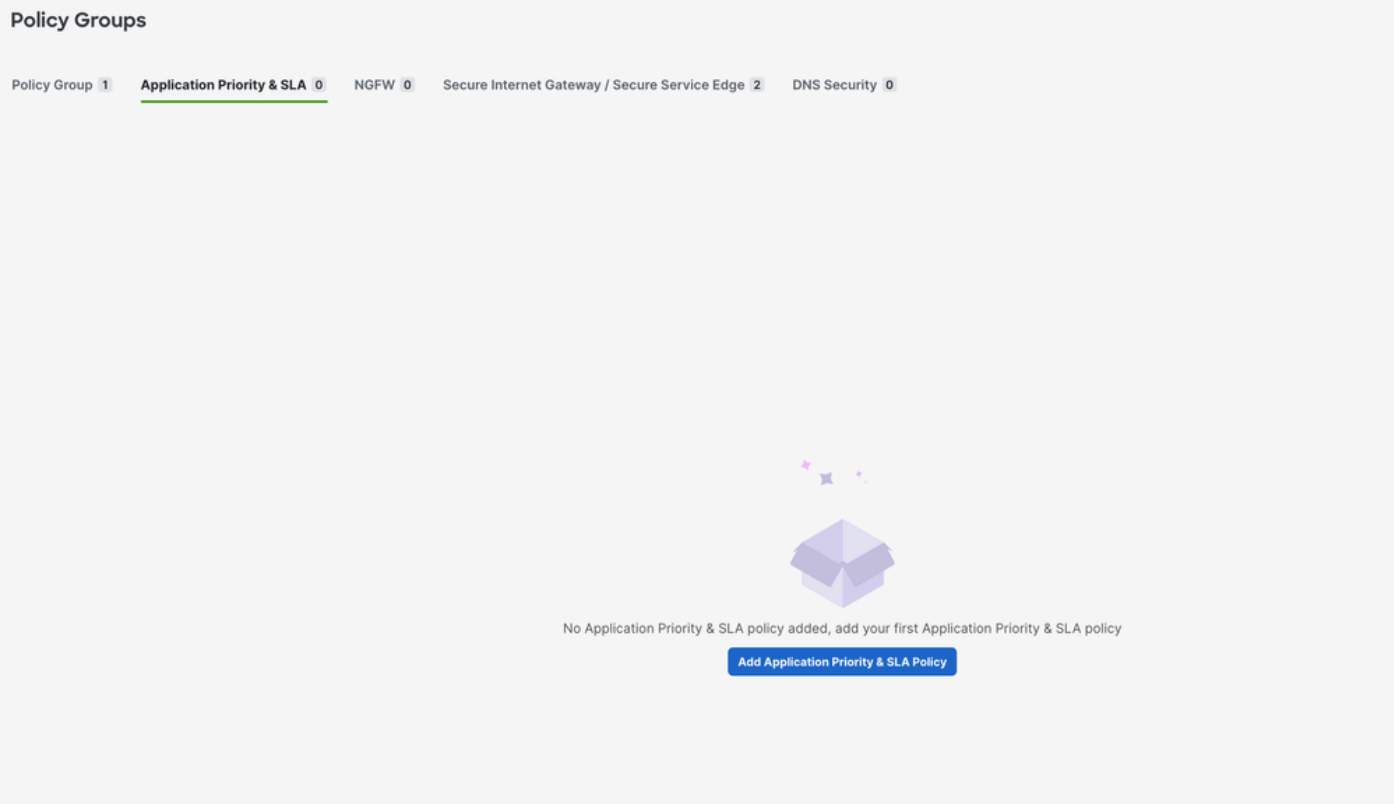


配置策略組以將流量重定向到SSE

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

- 選擇Add Application Priority & SLA Policy

- 指定策略的名稱。

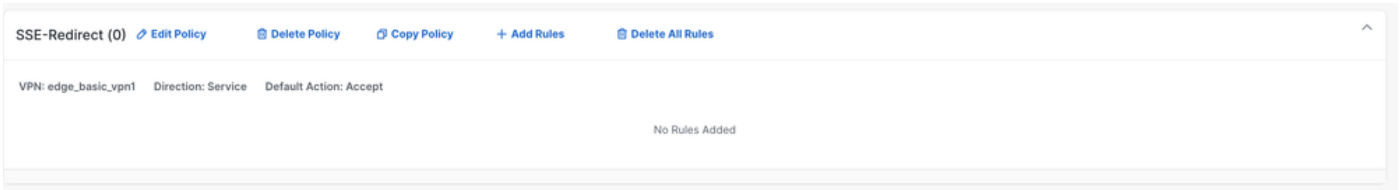


2.顯示新策略後，選擇「高級佈局」切換。

3.選擇Add Traffic Policy List。

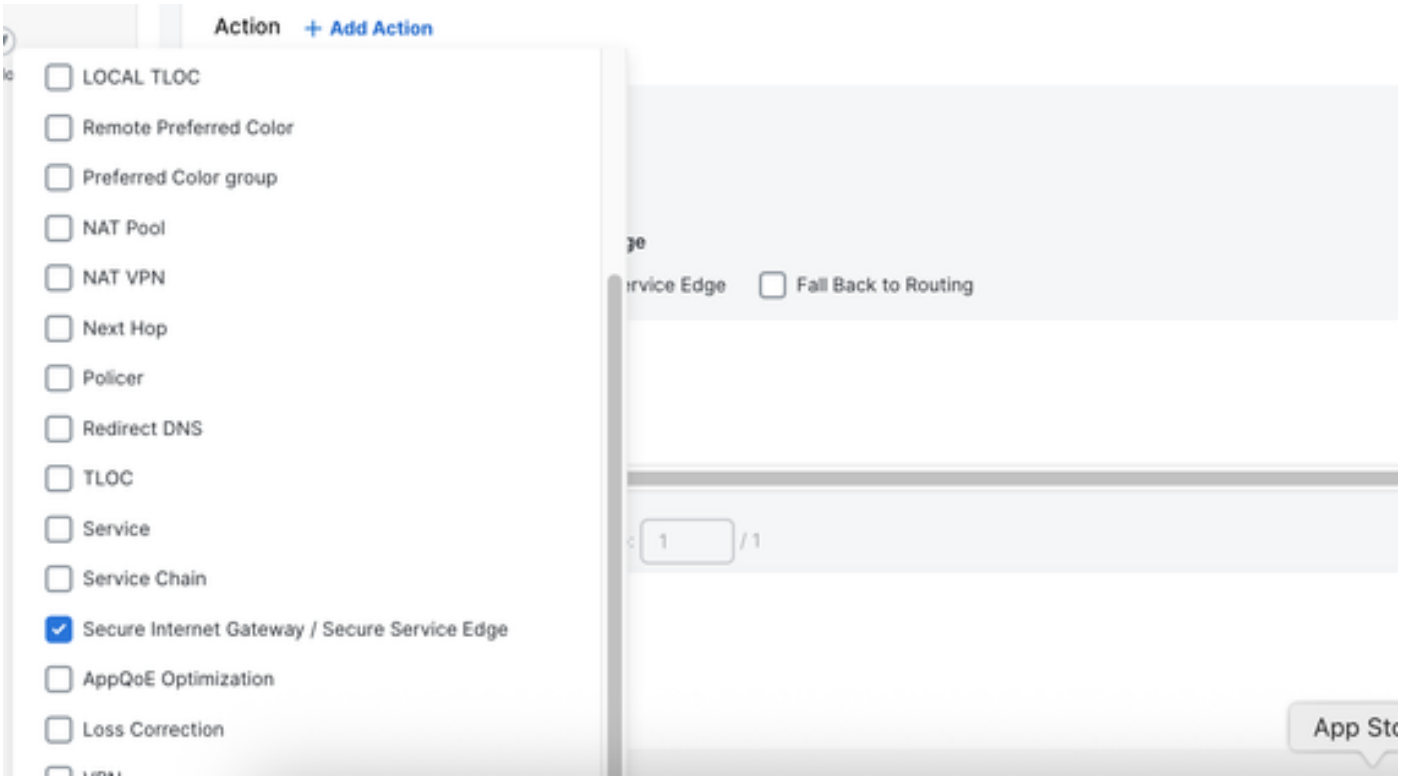
- 配置VPN以將流量重定向到SSE隧道。
- 根據需要設定Direction和Default Action，然後儲存。

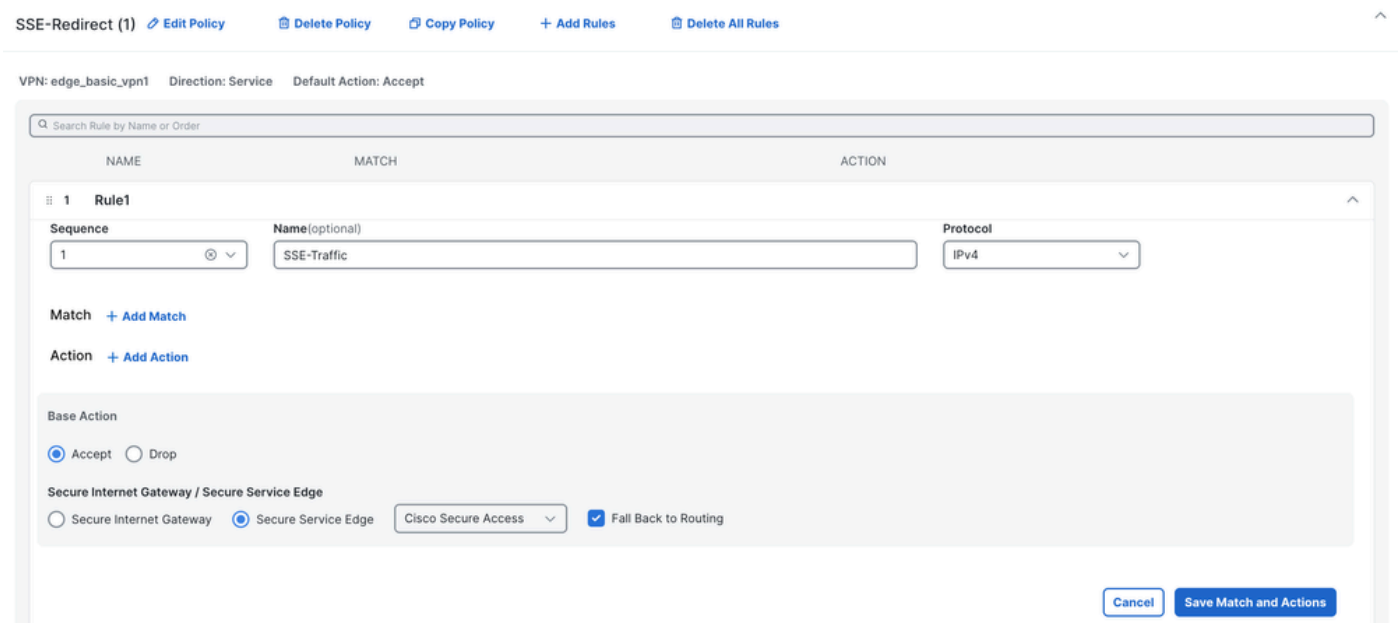
4.選擇+ Add Rule。



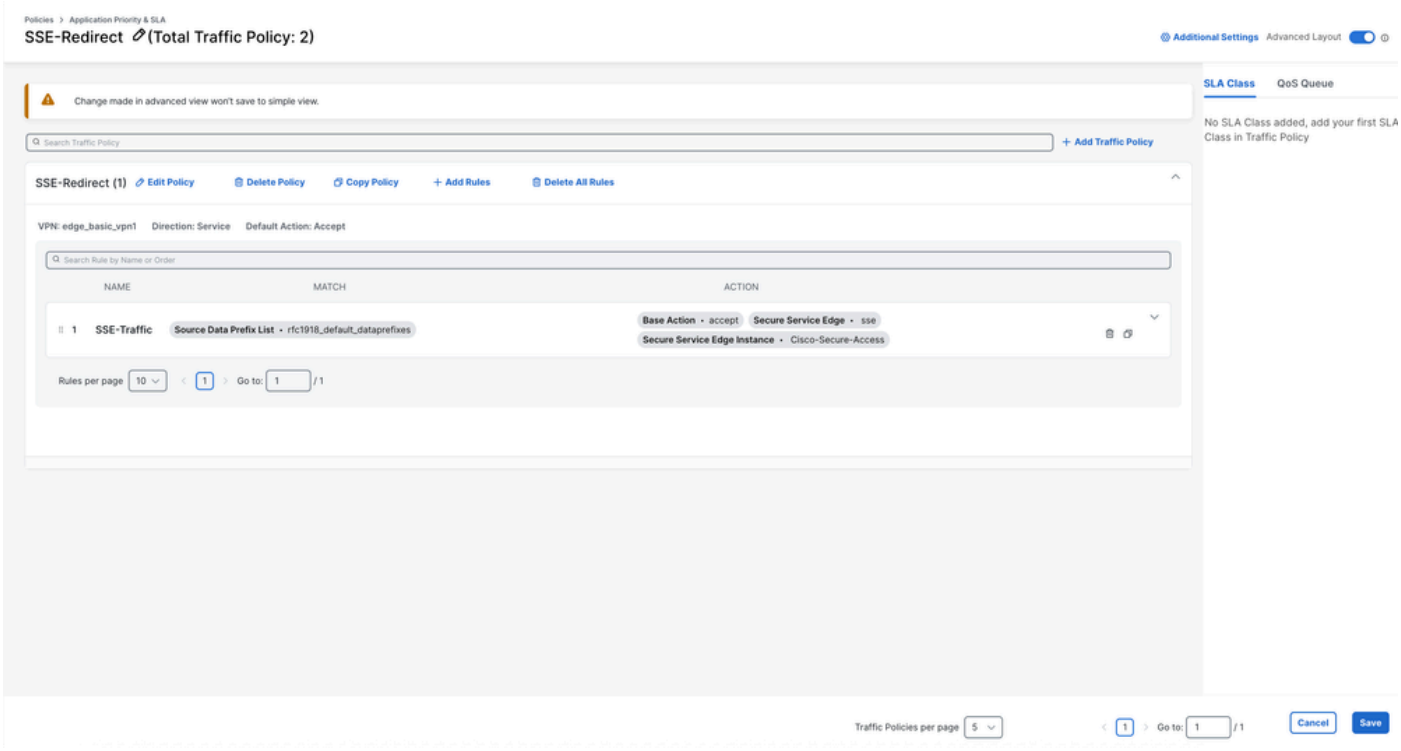
5.配置您的匹配流量標準，將流量重定向到SSE。
6.選擇Accept作為基本操作，然後按一下+ Action。

7.查詢「Secure Internet Gateway/Secure Service Edge」操作，並將其設定為「Secure Service Edge」。



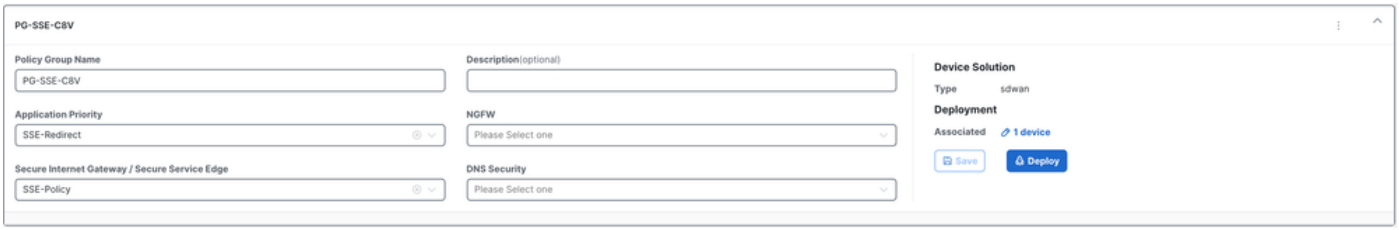


8.按一下儲存匹配和操作



9.按一下Save。

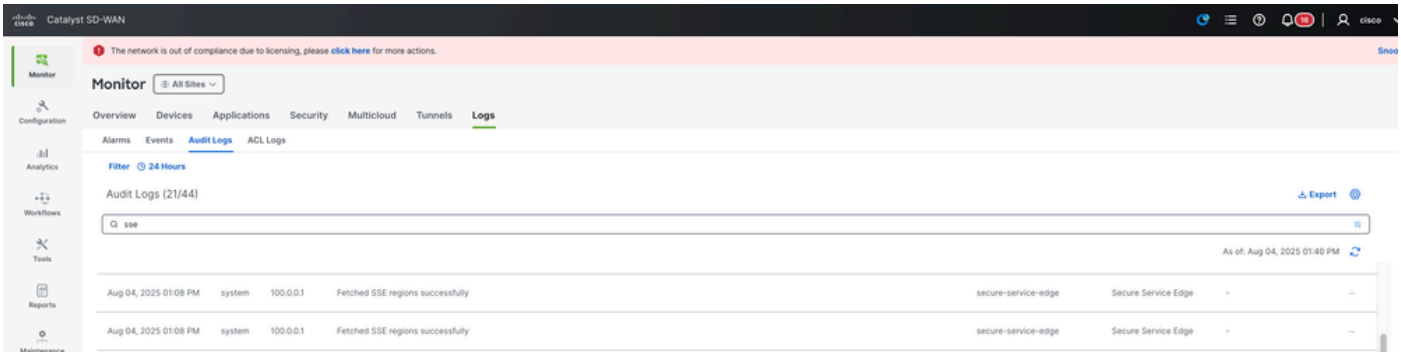
10.導航到Configuration > Policy Groups，然後選擇剛創建的Application Priority策略。儲存，然後部署。



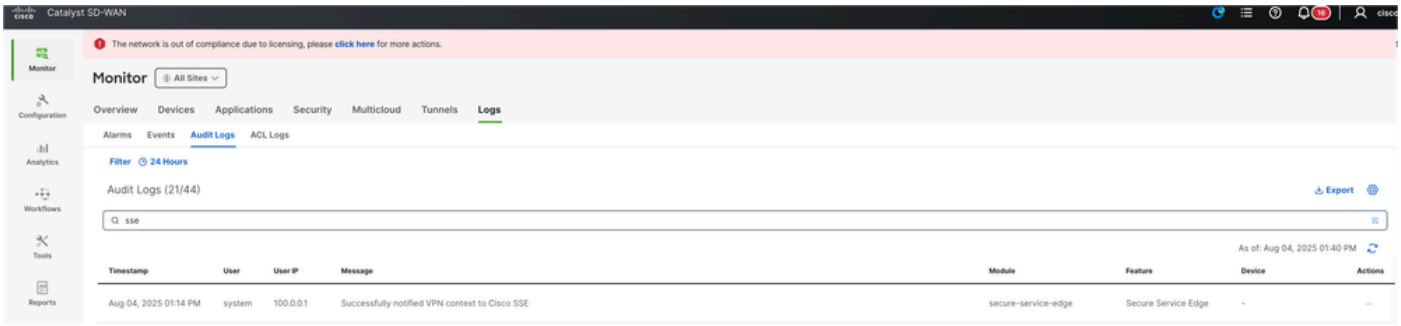
驗證

經理

1.Monitor > Logs > Audit Logs並搜尋「sse」。

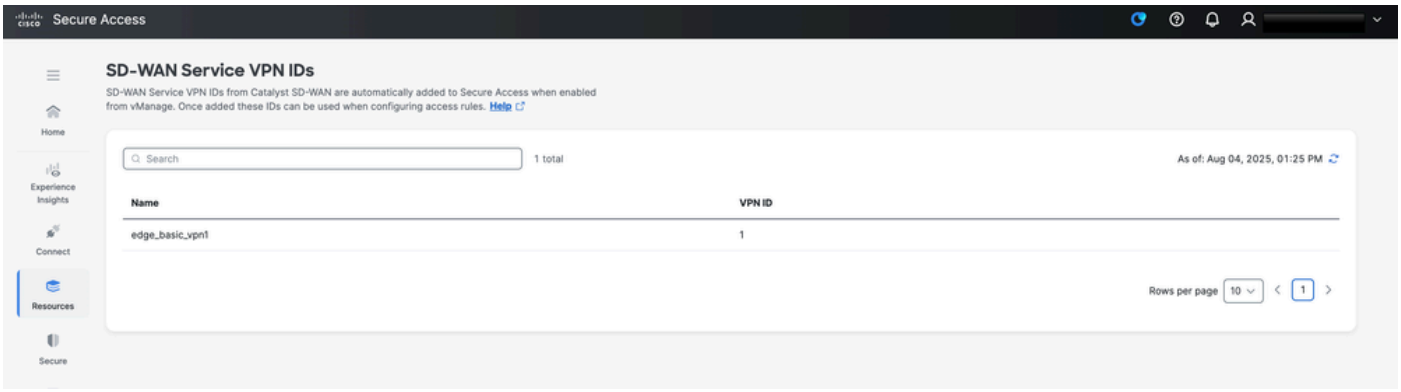


2.您可以通過檢查Manager來驗證是否成功啟用情景共用VPN。



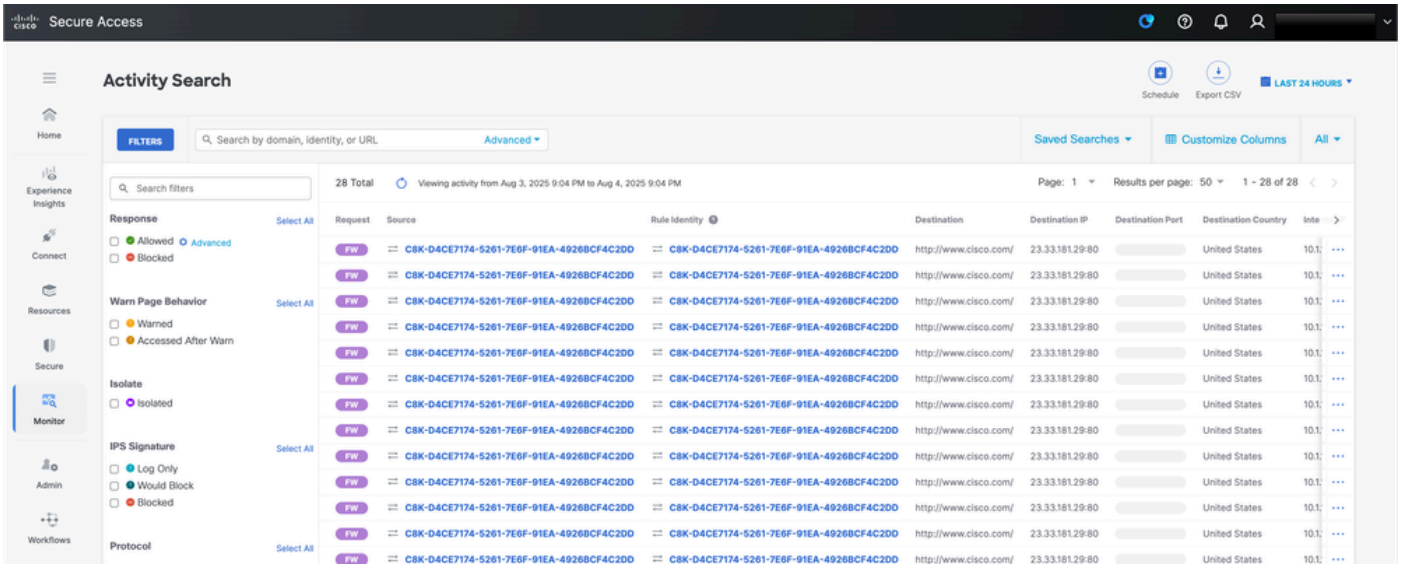
安全訪問控制面板

內容共用
您可以通過檢查SSE控制面板來驗證是否已成功啟用情景共用VPN，Resources > SD-WAN Service VPN ID



通道開啟

當通道開啟且追蹤器對透過通道的流量運作時，您可以導覽至Monitor > Activity Search以驗證這點。在此螢幕上，您會看到通過通道的流量，例如由追蹤器產生的對www.cisco.com的請求。此可視性可確認追蹤器已啟動並主動監控通過通道的流量



命令線路介面(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
```

相關資訊

- 配置情景共用SD-WAN
- 思科安全訪問與SD-Routing整合
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。