Catalyst SD-WANでのSecure Access(SSE)統合の設定とトラブルシューティング

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

シスコセキュアアクセス

事前設定

- ループバックインターフェイスの作成

SSEポータルでの新しいAPIキーの設定

Catalyst ManagerでのSSEの設定

- クラウド資格情報の設定
- ポリシーグループによるSSEトンネルの設定
- ポリシーグループの設定

SSEにトラフィックをリダイレクトするためのポリシーグループの設定

確認

- マネージャ
- セキュアアクセスダッシュボード
- コマンドラインインターフェイス(CLI)コマンド

はじめに

このドキュメントでは、Catalyst SD-WANでアクティブ – アクティブSSE統合を設定する方法と、そのトラブルシューティングについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Software-Defined Wide Area Network(SD-WAN)
- 構成グループ
- ポリシーグループ

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- C8000Vバージョン17.15.02
- vManageバージョン20.15.02

- Cisco Secure Accessアカウント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

シスコセキュアアクセス

Cisco Secure Accessは、複数のネットワークセキュリティサービスを統合するクラウドベースのセキュリティサービスエッジ(SSE)ソリューションであり、クラウドからサービスを提供してハイブリッドワークフォースをサポートします。Cisco SD-WAN ManagerはREST APIを利用してCisco Secure Accessからポリシー情報を取得し、その情報をCisco IOS XE SD-WANデバイスに配信します。この統合により、シームレスで透過的、かつ安全なDirect Internet Access(DIA)がユーザに提供され、ユーザは任意のデバイスからどこからでも安全に接続できるようになります。

Cisco SSEにより、SD-WANデバイスはIPSecトンネルを使用してSSEプロバイダーとの接続を確立できます。このドキュメントは、Cisco Secure Accessのユーザを対象としています。

事前設定

- デバイスのドメインルックアップを有効にする：Configuration Groups > System Profile > Globalの順に移動し、ドメインルックアップを有効にします。

注：デフォルトでは、ドメインルックアップは無効です。

- DNSの設定：ルータはDNSを解決して、VPN 0上のインターネットにアクセスできます。
- NAT DIAの設定：DIAの設定は、SSEトンネルが作成されるルータ上に存在している必要があります。

ループバックインターフェイスの作成

アクティブ/アクティブ設定の両方のトンネルが同じ宛先データセンターに接続し、送信元として同じWANインターフェイスを使用する場合、2つのループバックIPアドレスを作成する必要があります。

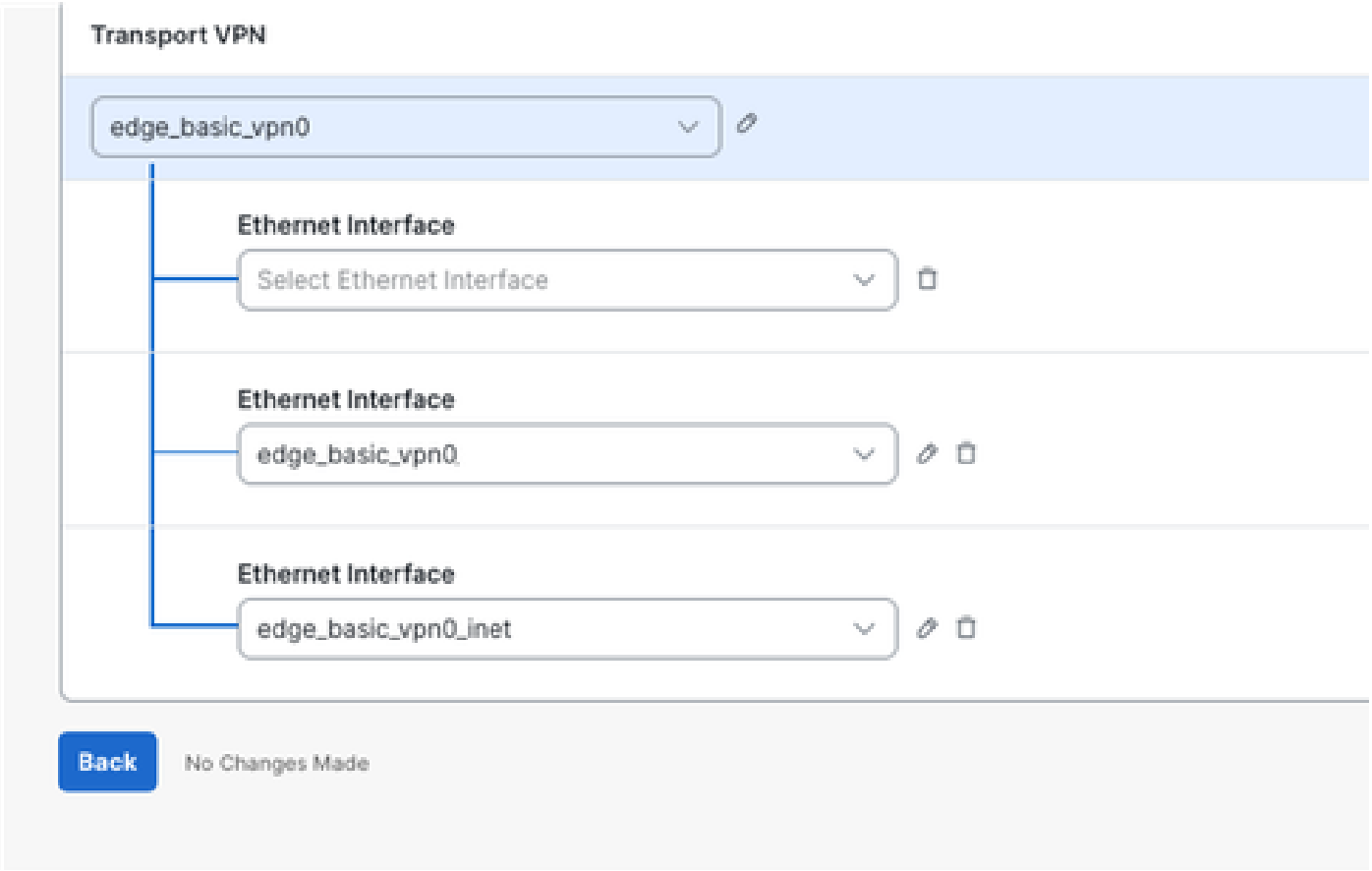
注:2つのトンネルが同じ送信元と宛先で設定されている場合、IKEv2はローカルIDとリモートIDで構成されるIDペアを形成します。デフォルトでは、ローカルIDはトンネルの送信元インターフェイスのIPアドレスです。 このIDペアは一意である必要があり、2つのトンネル間で共有することはできません。 IKEv2状態の混乱を防ぐために、各トンネルは異なるループバックインターフェイスを送信元として使用します。DIAインターフェイスではIKEパケッ

トが変換(NAT)されますが、ローカルIDは変更されず、元のループバックIPアドレスが保持されます。

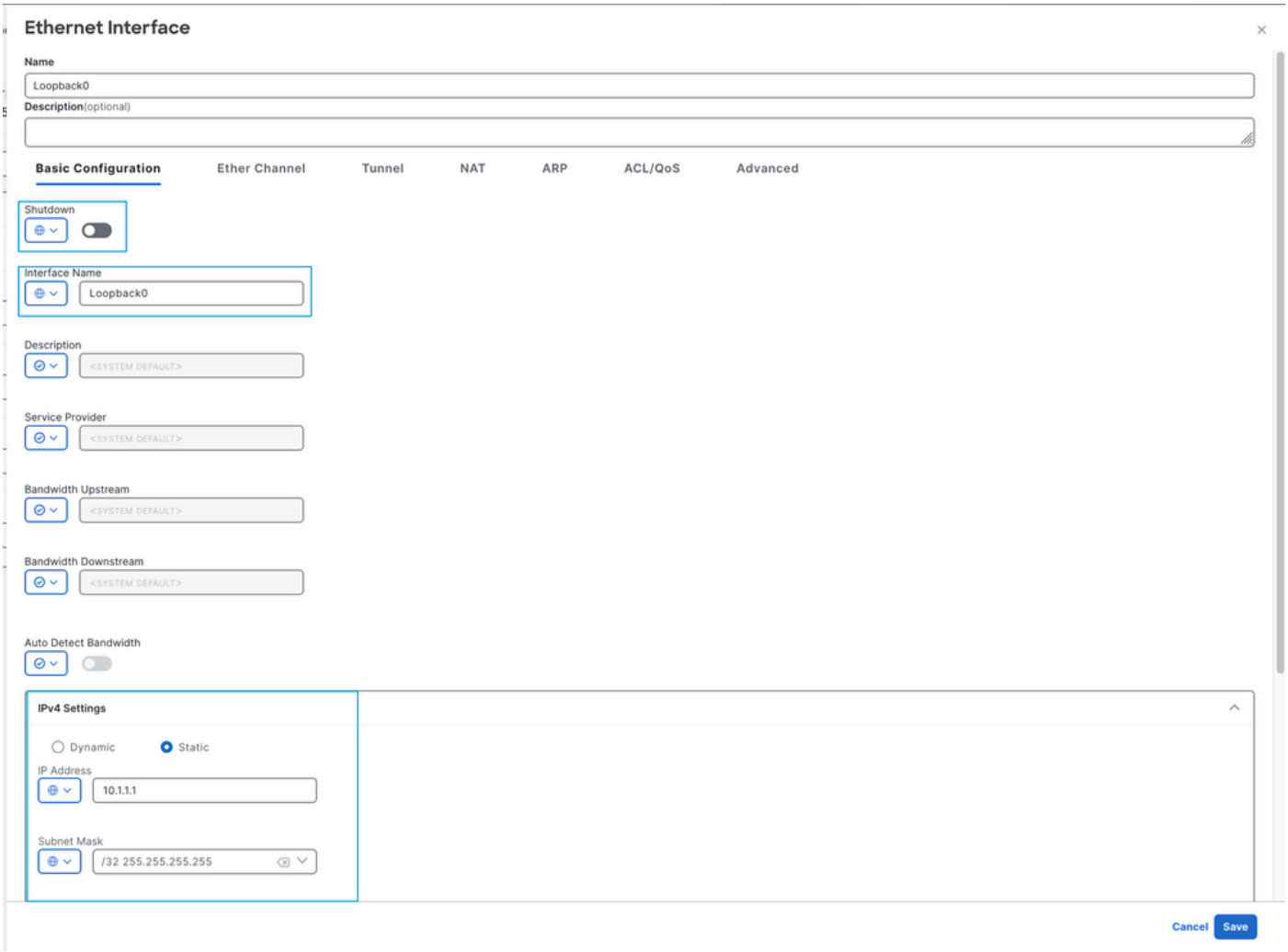
1. Configuration > Configuration Groups > Configuration Group Name> Transport & Management Profileの順に移動し、Editをクリックします。.

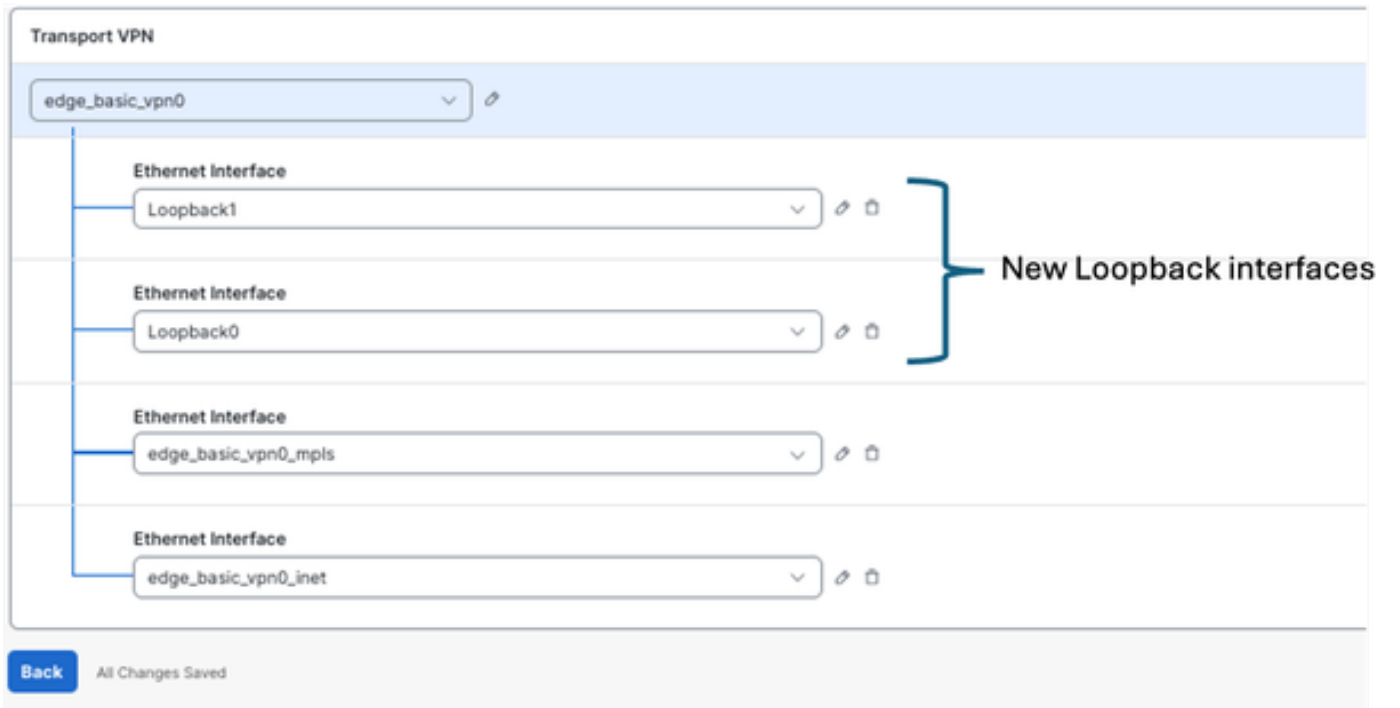
2. transport VPN Profile (メインプロファイル) の右側にあるプラス記号(+)をクリックします。すると、右端にある機能の追加メニューが開きます。

3. Ethernet Interfaceをクリックします。Transport VPNに新しいインターネットインターフェイスを追加する

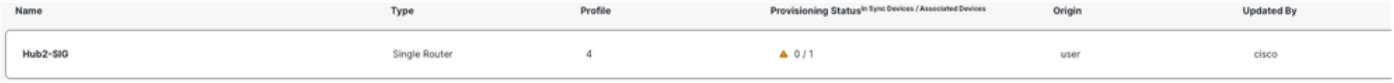


4.RFC1918 IPv4アドレスを使用して、図のLoopback0の例のように2つのループバックインターフェイスを作成します。



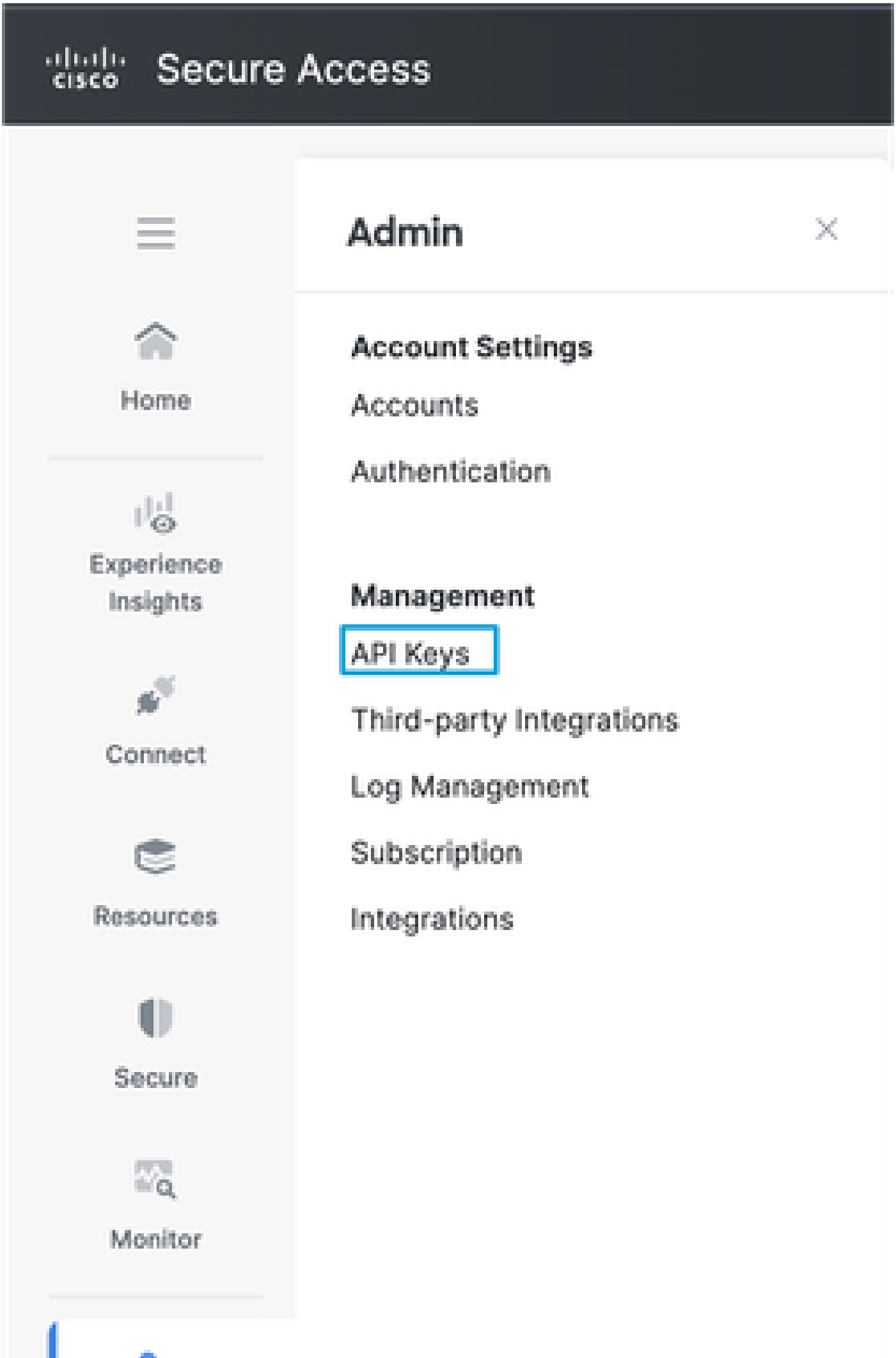


5. ループバック設定を適用した後、設定の変更をデバイスに導入します。プロビジョニングステータスが1/1から0/1に変更されていることに注意してください。



SSEポータルでの新しいAPIキーの設定

1. SSEポータルhttps://login.sse.cisco.com/へのアクセス
2. Admin > API Keysの順に移動します。


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

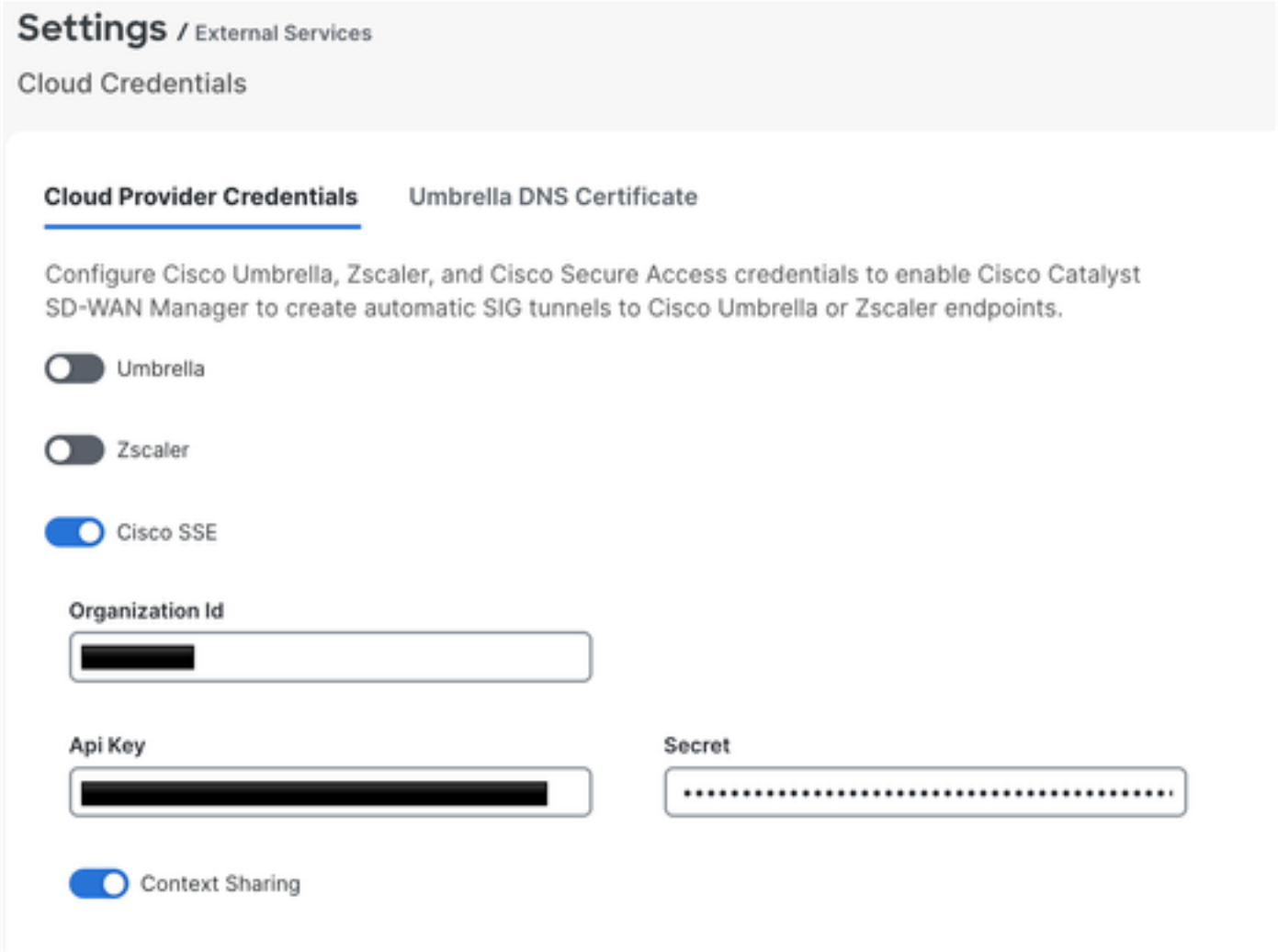
6. APIキーとキーシークレットをメモ帳にコピーし、ACCEPTとCLOSEを選択します。

7. URL https://dashboard.sse.cisco.com/#some-numbers#/admin/apikeys the#some-numbers#の下に組織IDを入力します。その情報もメモ帳にコピーします。

Catalyst ManagerでのSSEの設定

クラウド資格情報の設定

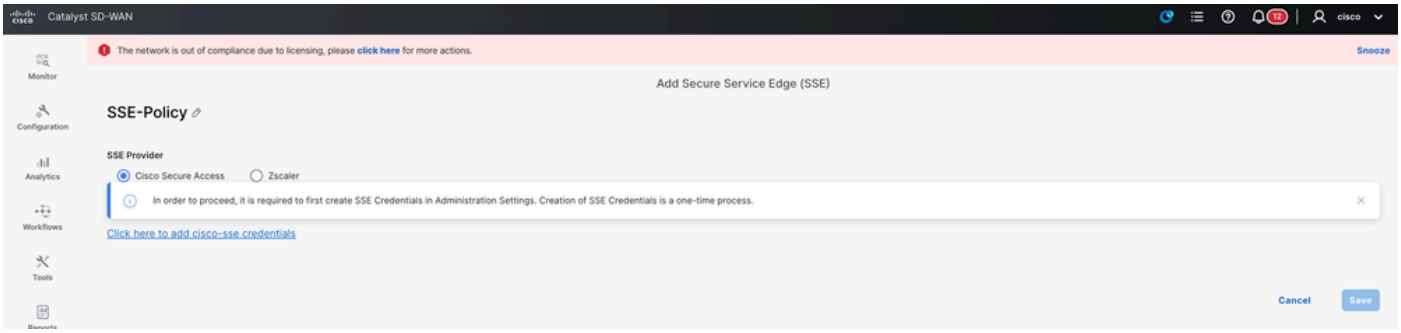
1. Administration > Settings > Cloud Credentials > Cloud Provider Credentialsの順に移動し、Cisco Secure Accessを有効にします
をクリックして詳細を入力します。



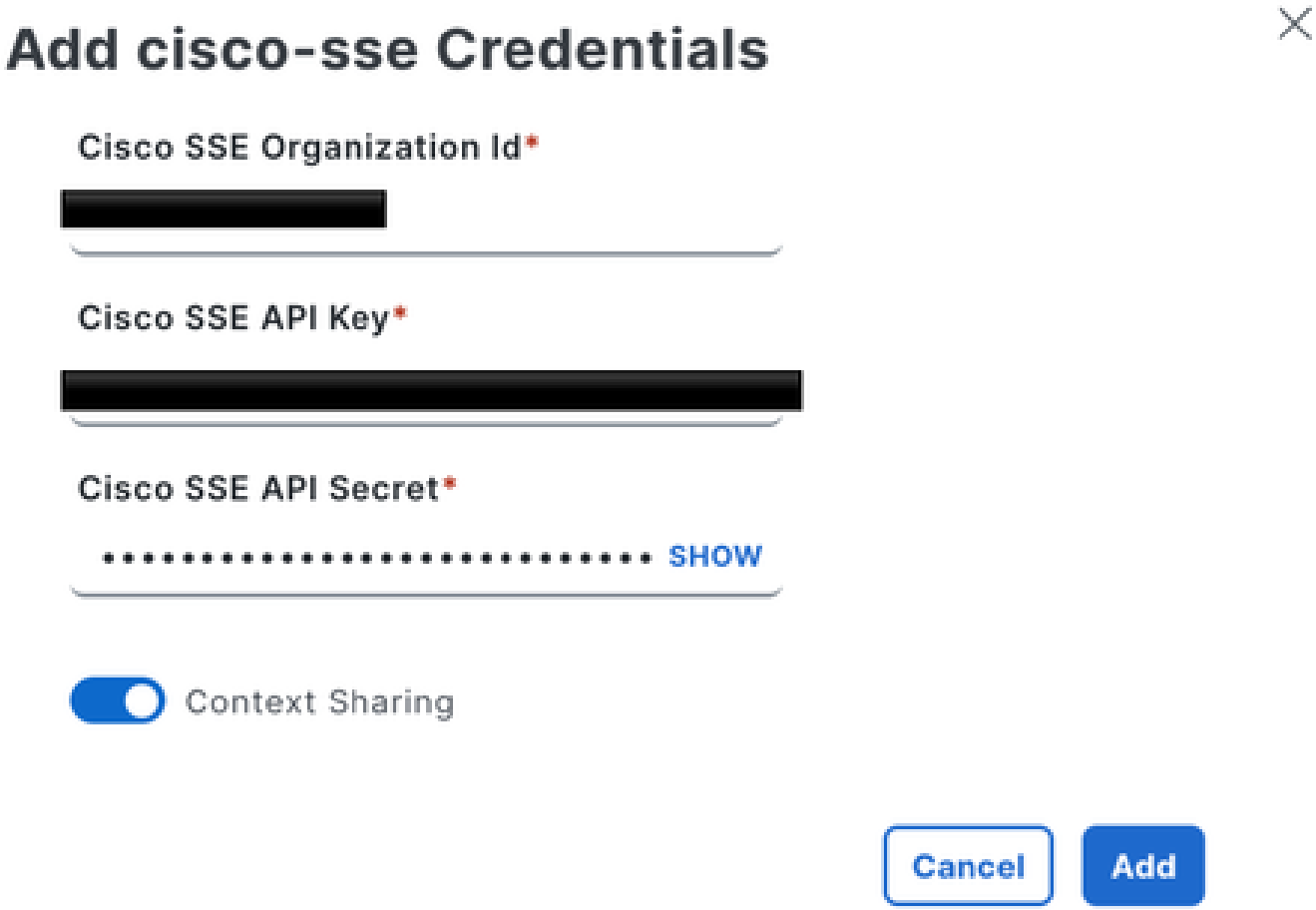
2. オプション：拡張された機能のコンテキスト共有を有効にできます。詳細については、『コンテキスト共有に関するCisco SSEユーザガイド』を参照してください。.

ポリシーグループによるSSEトンネルの設定

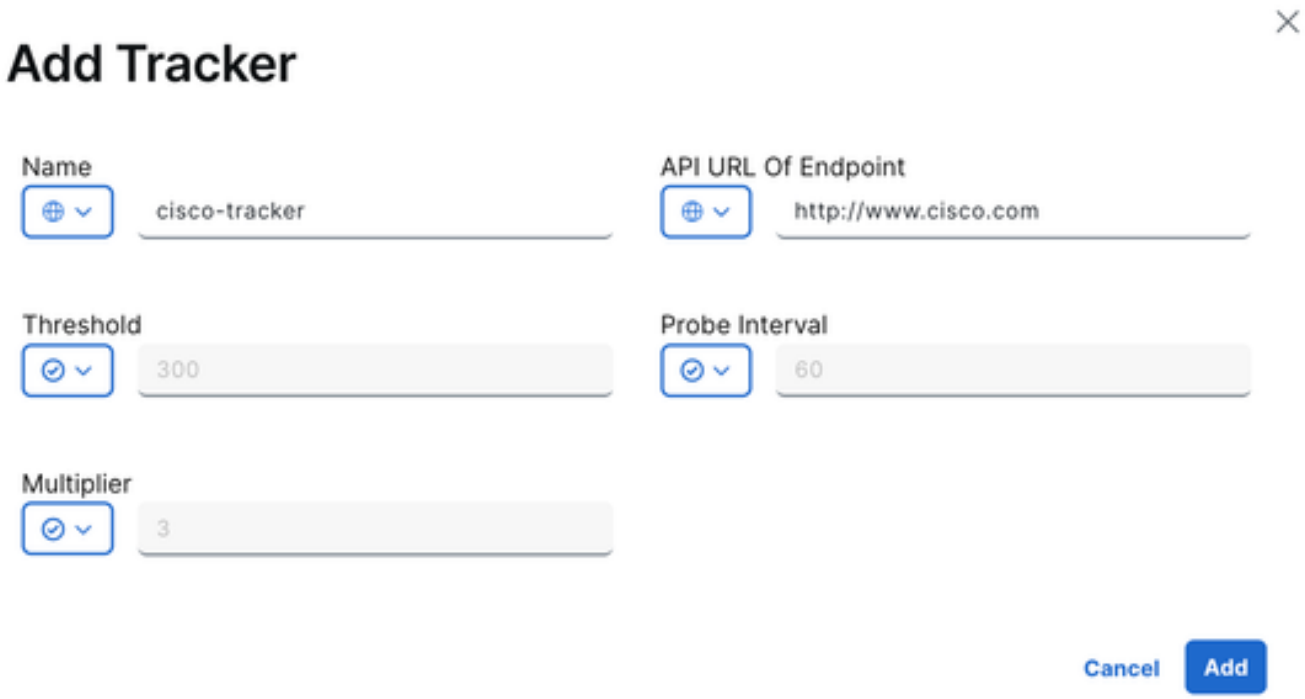
SD-WAN Managerで、Configuration > Policy Groups > Secure Internet Gateway/Secure Service Edge の順に選択し、Add Secure Service Edge (SSE)をクリックします。

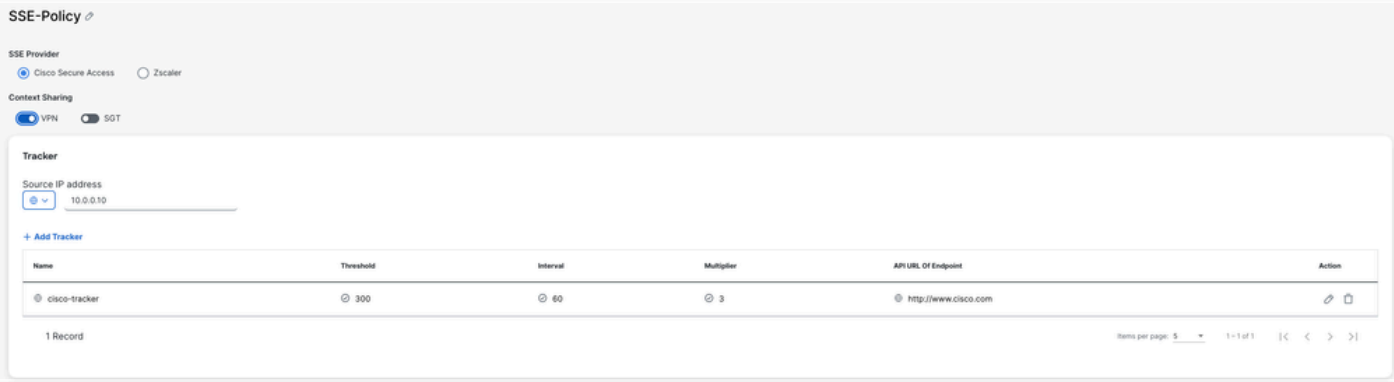


注:クラウドのクレデンシャルがまだ設定されていない場合は、この手順で追加できます。クレデンシャルがすでに設定されている場合は、自動的にロードされます。



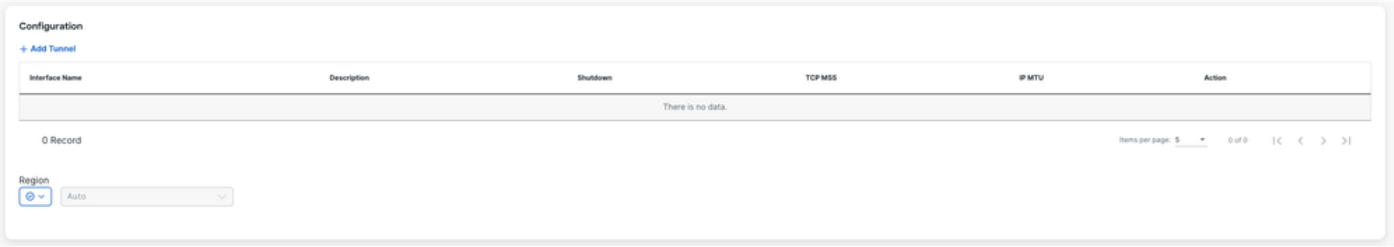
1. SSE Trackerを設定します。 この例では、トラッカーのURLはhttp://www.cisco.comに設定され、送信元IPアドレスはいずれかのループバックインターフェイスから割り当てられます。



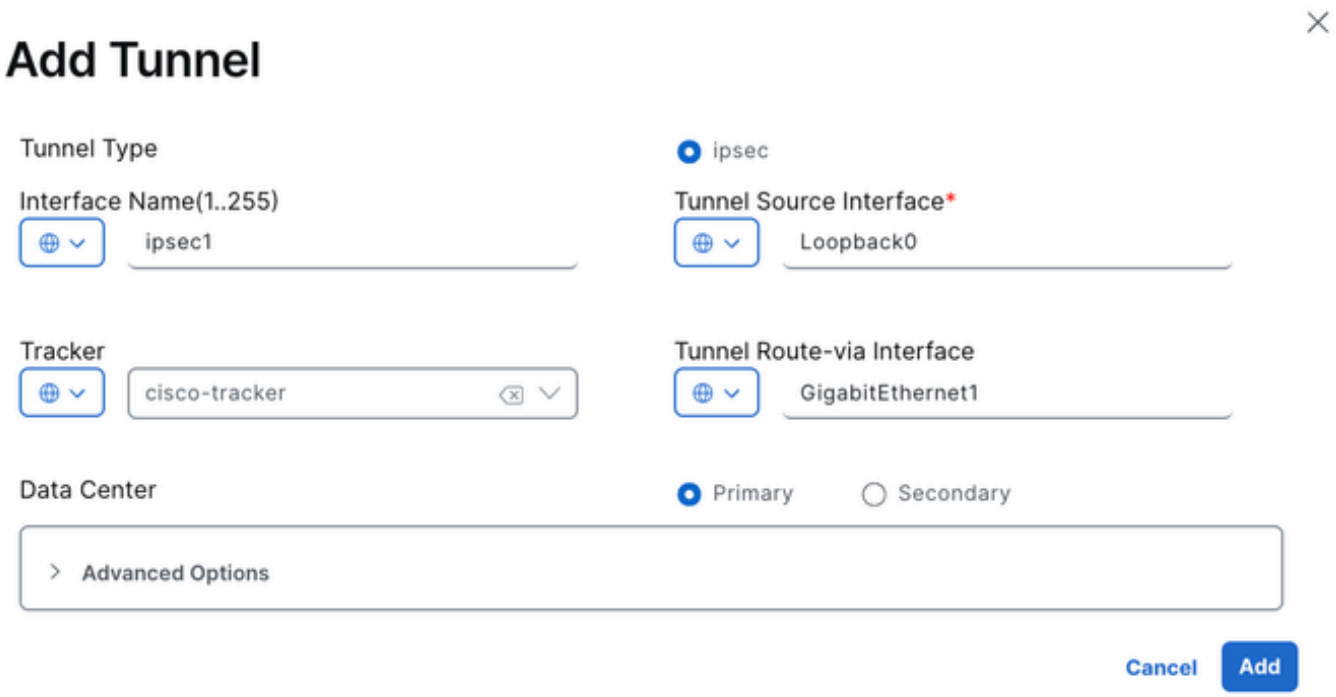


オプションとして、クラウドのクレデンシャルを設定する際にコンテキスト共有が有効になっているので、この例ではオプションとしてVPNが選択されています。

2. Add Tunnelをクリックします。



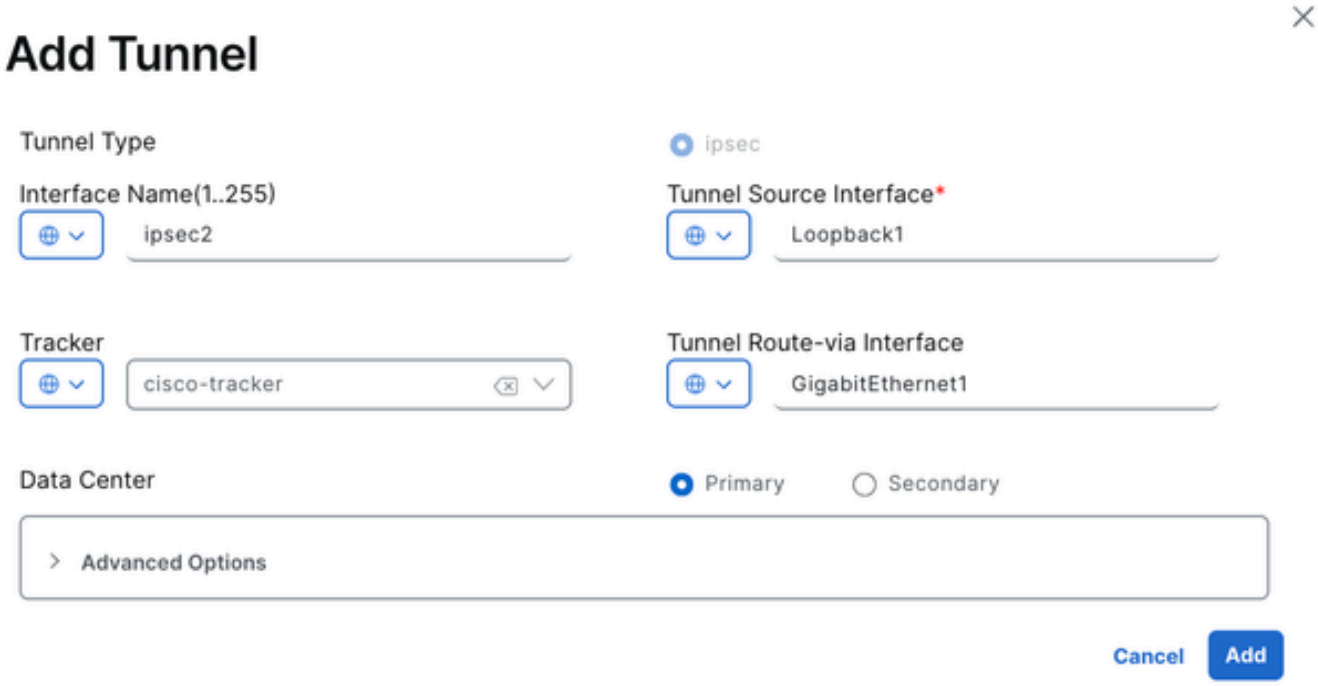
3. この例では、Loopback0インターフェイスがトンネル送信元として使用され、GigabitEthernet1インターフェイスがトラフィックをルーティングするためのWANインターフェイスとして機能します。



この例ではトラッカーが設定されているため、設定はGlobalに変更され、事前設定されたcisco-trackerが選択されます。

4. 2番目のトンネルに対して、同じパラメータを使用して同じ手順を繰り返しますが、インター

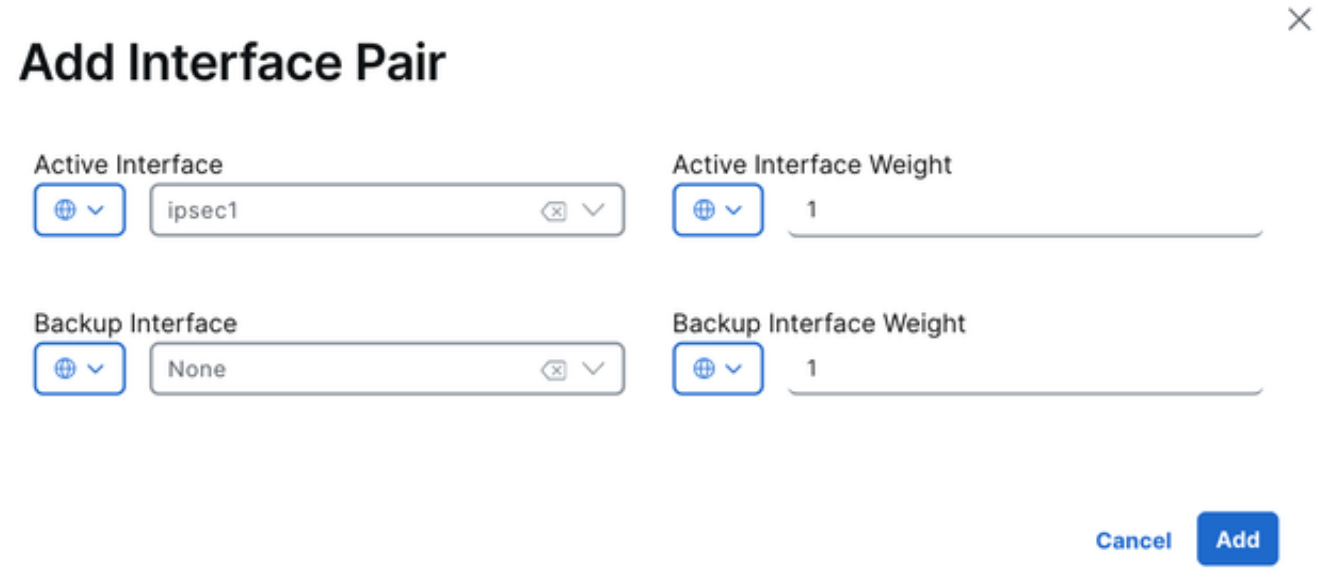
フェイス名をipsec1からipsec2に、送信元インターフェイス名をLoopback1に変更します。



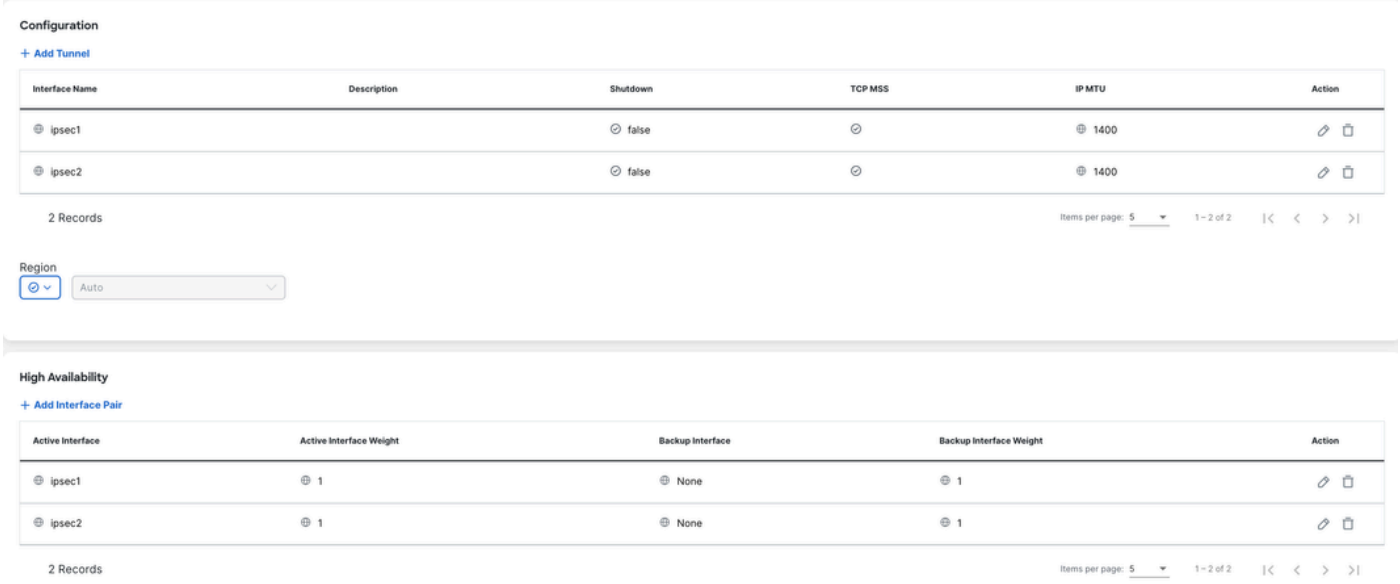
両方のトンネルは、バックアップなしで同時にアクティブになるように設定されます。

5. Add Interface Pairをクリックします。

6. Addをクリックします。アクティブなインターフェイスはipsec1に設定され、バックアップインターフェイスは指定されていません。



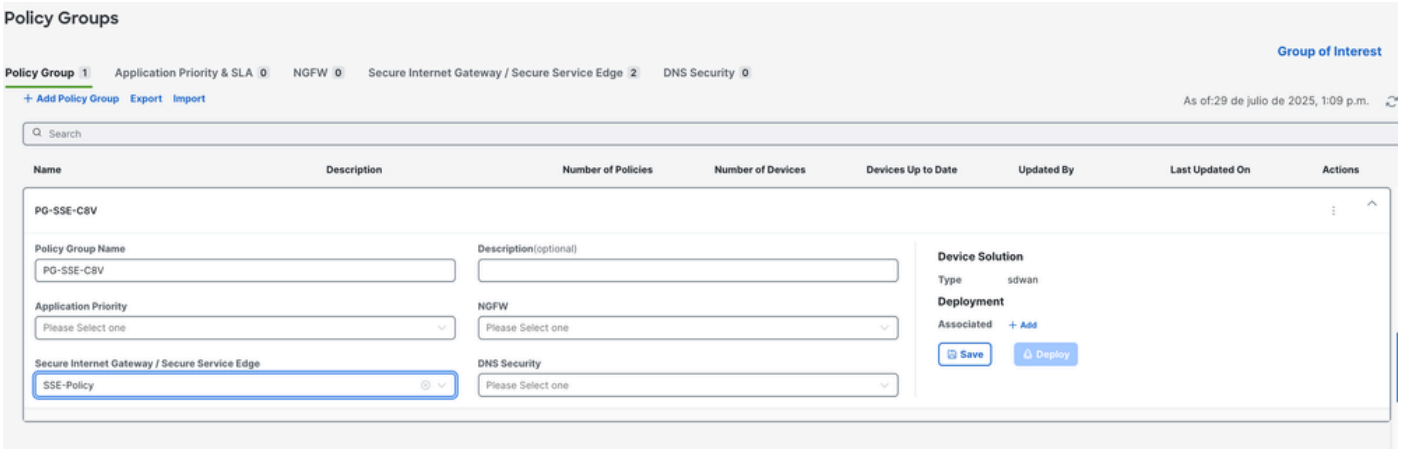
7. 同じ操作が2番目のトンネルipsec2に対して繰り返されます。



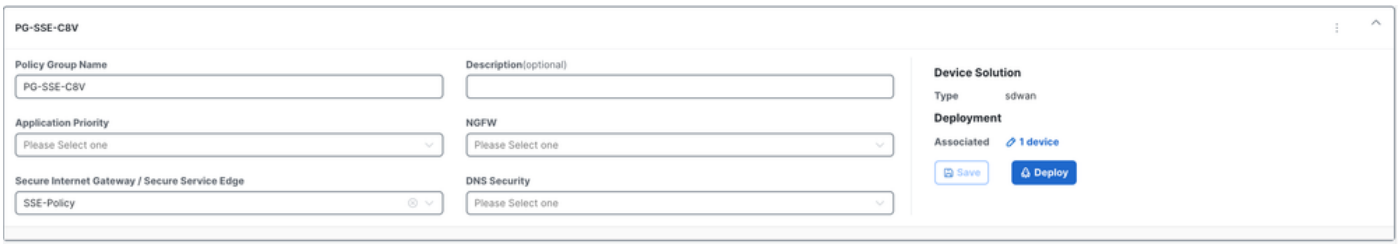
8. 設定を保存します。

ポリシーグループの設定

1. 以前にポリシーグループ内で作成したポリシーを選択して保存するだけです。



2. デバイスがポリシーグループに関連付けられたら、ポリシーグループの導入に進みます。

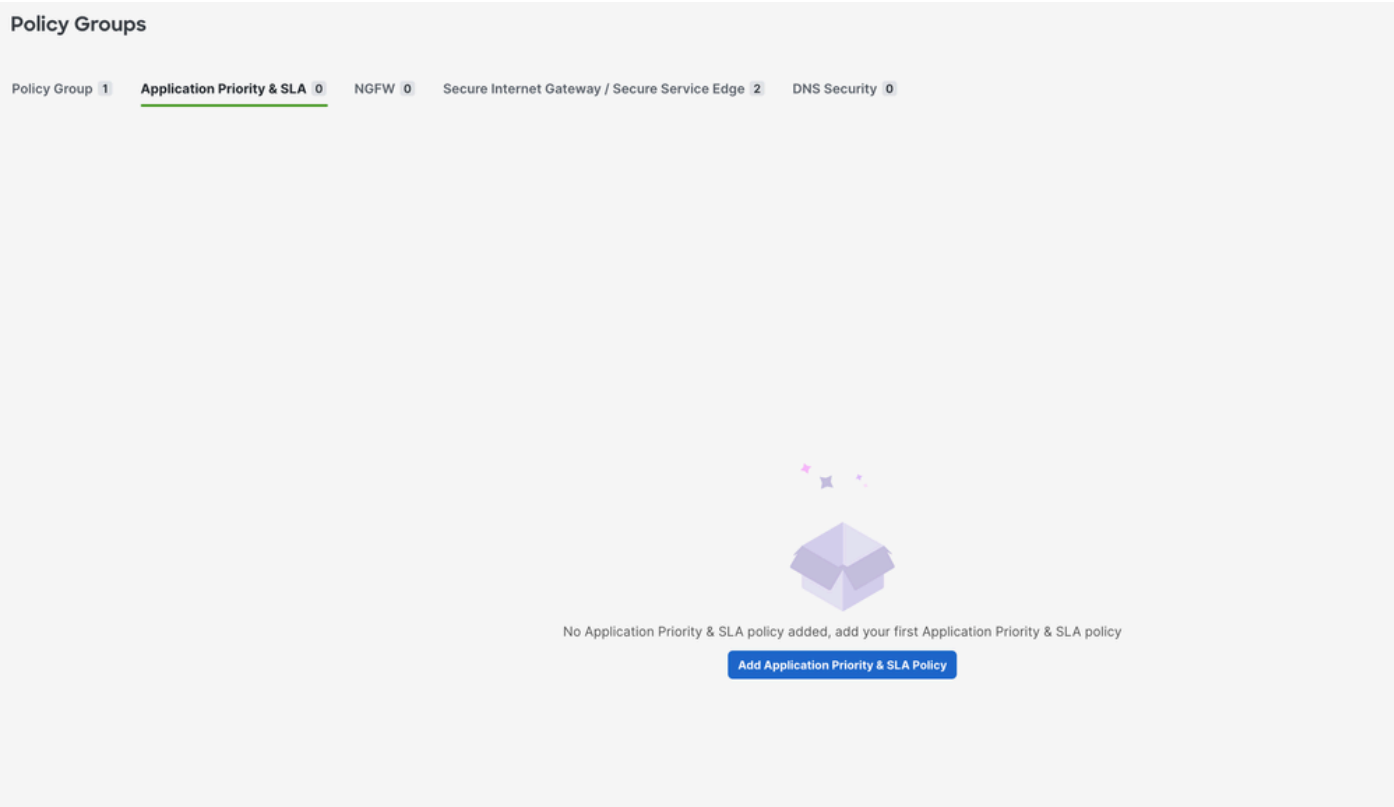


SSEにトラフィックをリダイレクトするためのポリシーグループの設定

1. SD-WAN Managerで、Configuration > Policy Groups > Application Priority & SLAの順に移動し

ます。

- Add Application Priority & SLA Policyを選択します。
- ポリシーの名前を指定します。

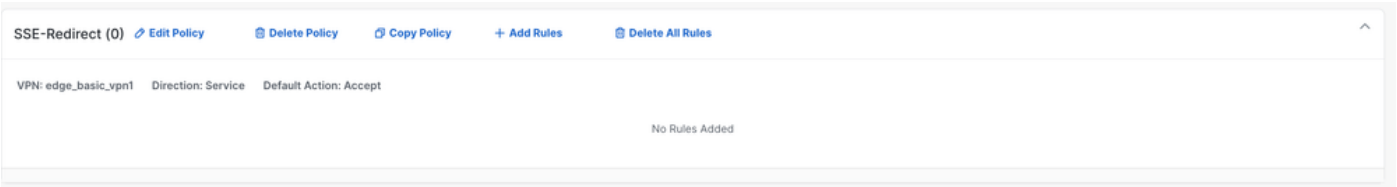


2. 新しいポリシーが表示されたら、「拡張レイアウト」トグルを選択します。

3. Add Traffic Policy Listを選択します。

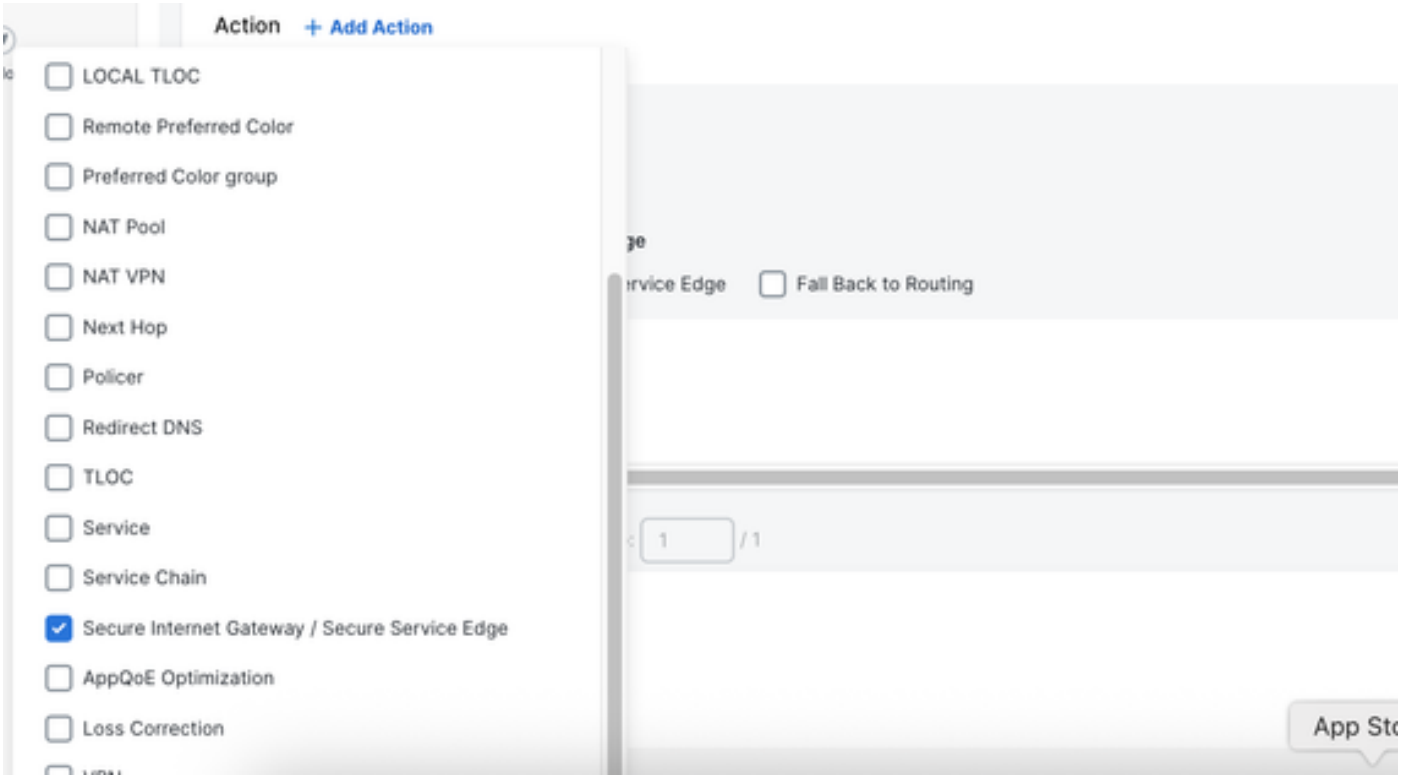
- トラフィックをSSEトンネルにリダイレクトするようにVPNを設定します。
- 必要に応じてDirectionとDefault Actionを設定して保存します。

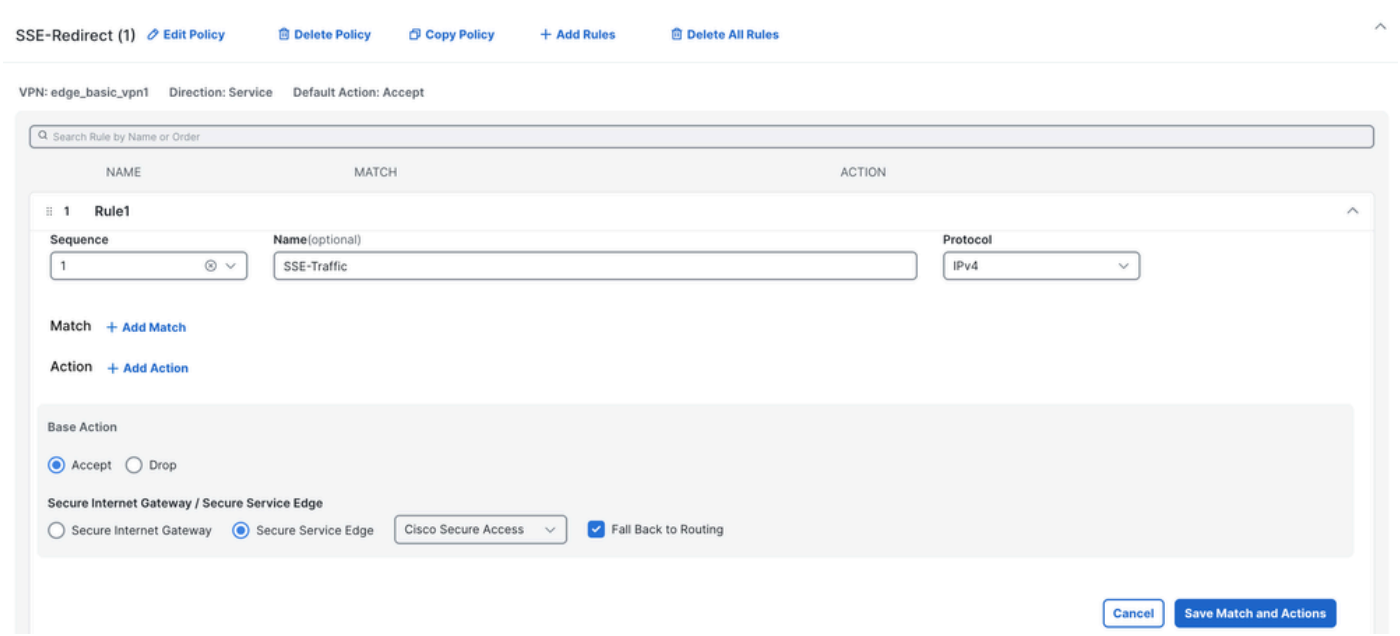
4. + Add Ruleを選択します。



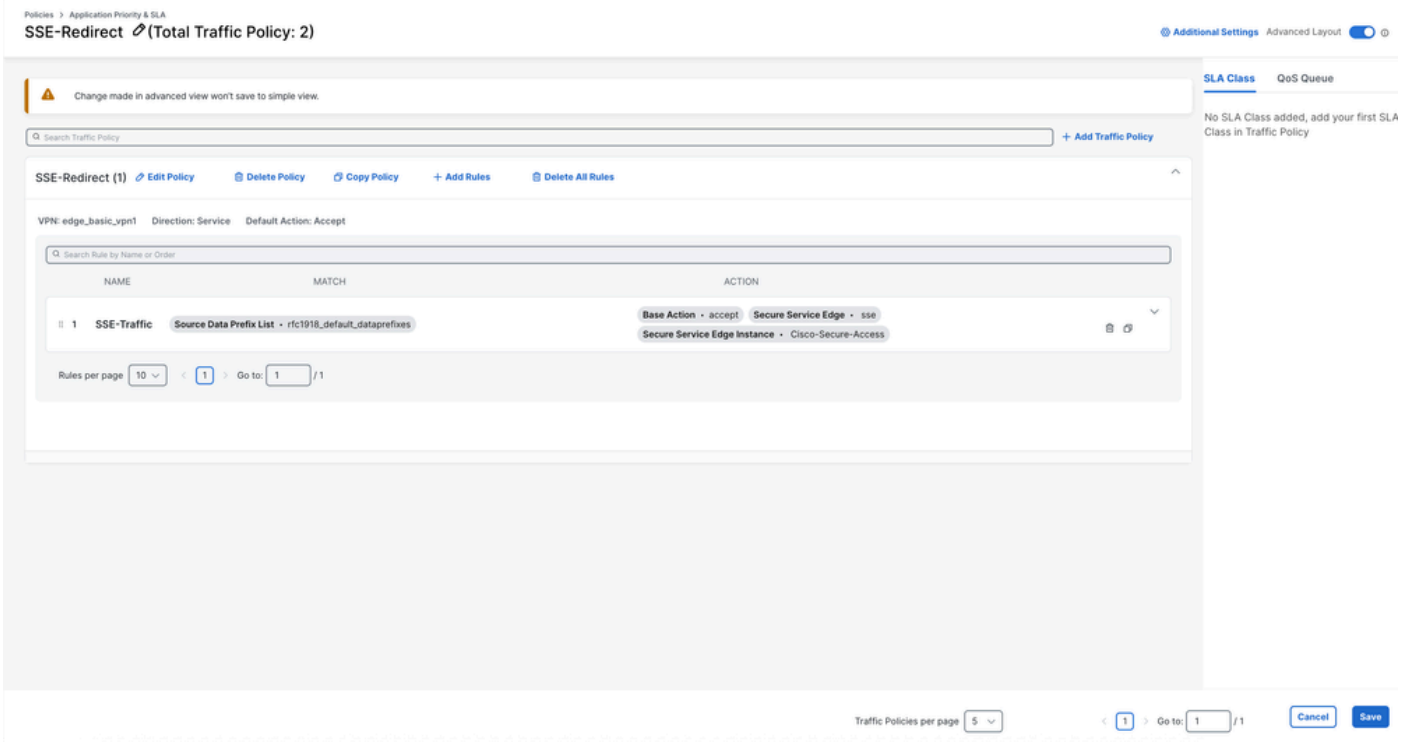
5. トラフィックをSSEにリダイレクトするためのトラフィック一致基準を設定します。
6. 基本アクションとしてAcceptを選択し、+アクションをクリックします。

7. Secure Internet Gateway / Secure Service Edgeアクションを探し、Secure Service Edgeに設定します。



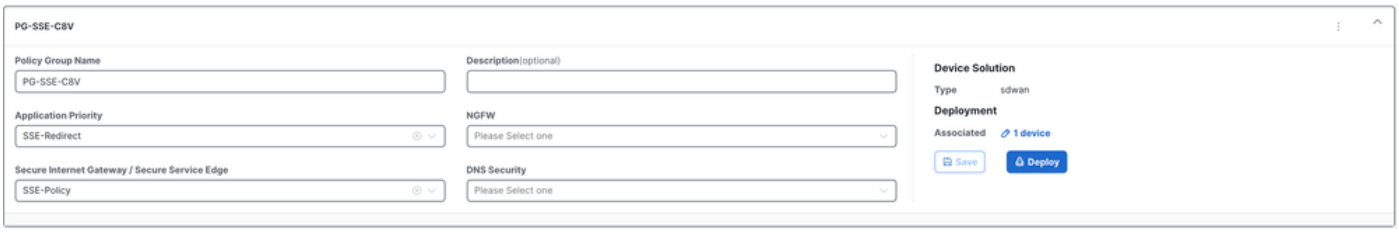


8. 「一致とアクションの保存」をクリックします。



9. Saveをクリックします。

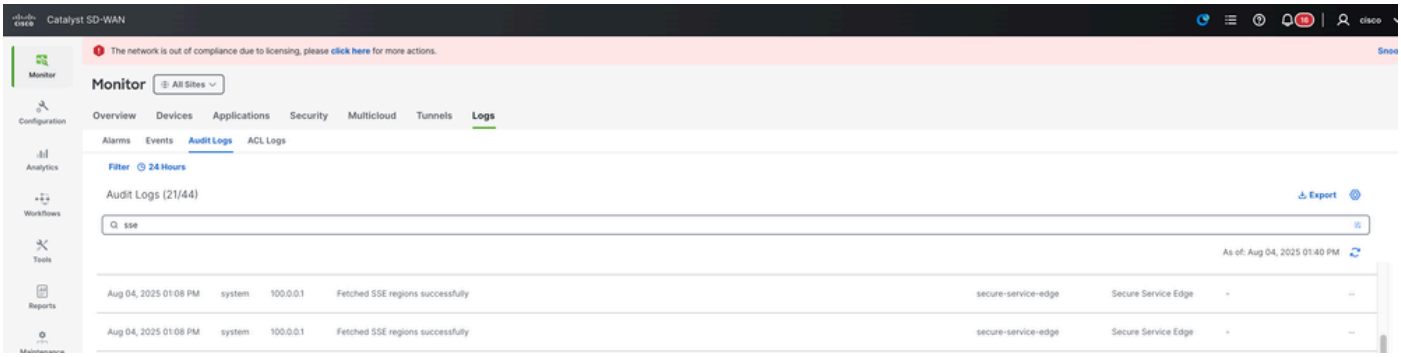
10. Configuration > Policy Groupsの順に移動し、作成したApplication Priorityポリシーを選択します。保存して展開します。



確認

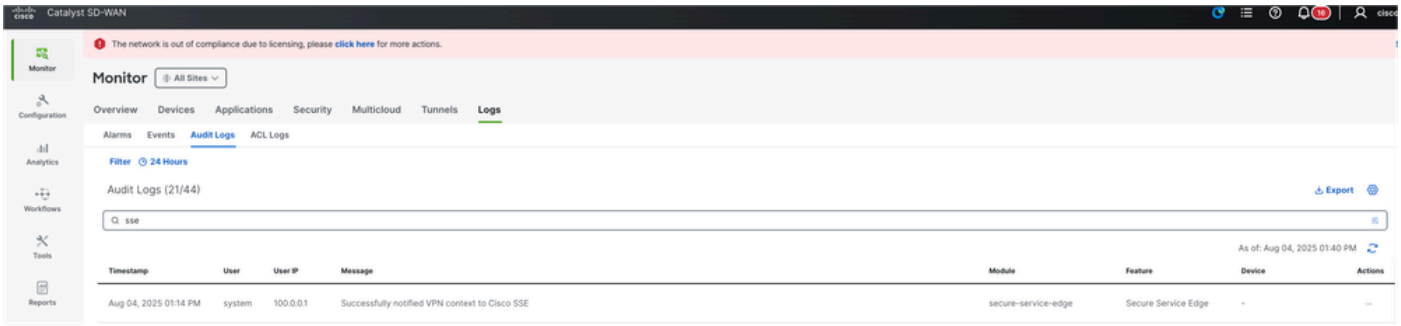
マネージャ

1. Monitor > Logs > Audit Logsの順に選択し、「sse」を検索します。



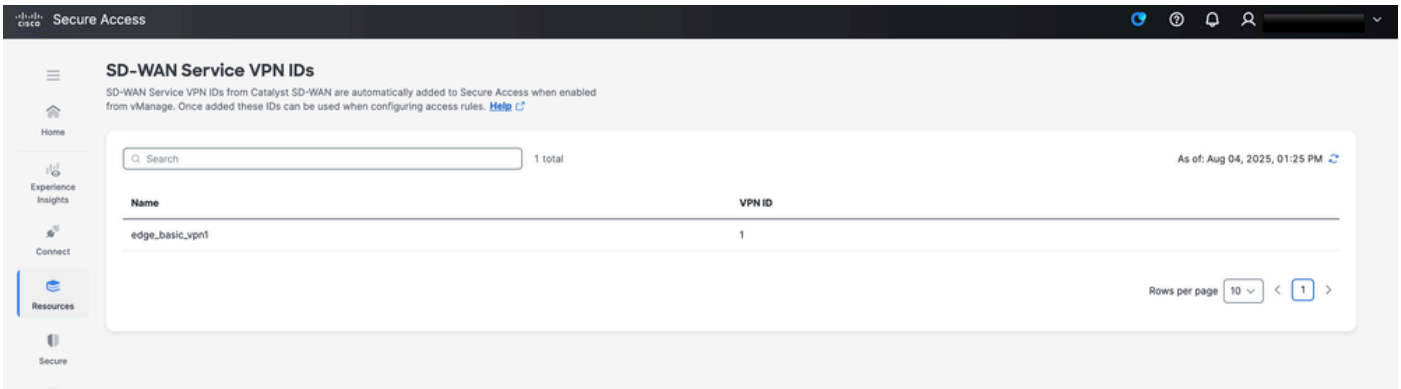
2. マネージャを確認することで、コンテキスト共有VPNが正常に有効になっているかどうかを確

認できます。



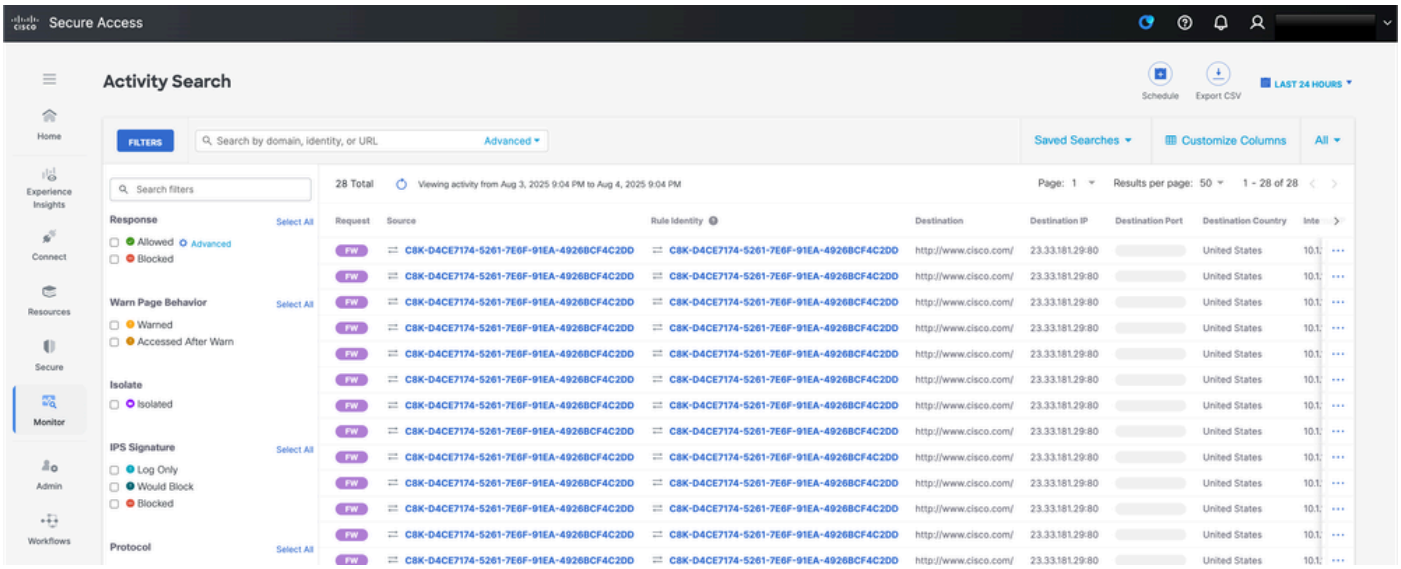
セキュアアクセスダッシュボード

コンテキスト共有
コンテキスト共有VPNが正常に有効かどうかは、SSEダッシュボードを確認することで確認できます。リソース> SD-WANサービスVPN ID



トンネルアップ

トンネルがアップ状態で、トラッカがトンネルを流れるトラフィックに対して動作可能である場合は、Monitor > Activity Searchに移動して、これを検証できます。この画面には、www.cisco.comへの要求がトラッカーによって生成されるなど、トンネルを通過するトラフィックが表示されます。この可視性により、トラッカーがアップ状態で、トンネルを通過するトラフィックをアクティブに監視していることが確認できます



コマンドラインインターフェイス(CLI)コマンド

<#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
```

関連情報

- コンテキスト共有SD-WANの設定
- Cisco Secure AccessとSDルーティングの統合
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。