Configuration et dépannage de l'intégration de l'accès sécurisé (SSE) sur le SD-WAN Catalyst

Table des matières

Introduction

Ce document décrit comment configurer l'intégration SSE active-active sur le SD-WAN Catalyst et guide son dépannage.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réseau étendu défini par logiciel (SD-WAN) Cisco
- Groupes de configuration
- Groupes de stratégies

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- C8000V version17.15.02
- vManage version 20.15.02

- Compte Cisco Secure Access

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Accès sécurisé Cisco

Cisco Secure Access est une solution SSE (Security Service Edge) basée sur le cloud qui fait converger plusieurs services de sécurité réseau, en les fournissant à partir du cloud pour prendre en charge une main-d'oeuvre hybride. Cisco SD-WAN Manager exploite les API REST pour récupérer des informations de stratégie à partir de Cisco Secure Access et les distribue aux périphériques SD-WAN Cisco IOS XE. Cette intégration permet aux utilisateurs de bénéficier d'un accès direct à Internet (DIA) transparent, transparent et sécurisé, leur permettant de se connecter à partir de n'importe quel périphérique, n'importe où et en toute sécurité.

Cisco SSE permet aux périphériques SD-WAN d'établir des connexions avec les fournisseurs SSE à l'aide de tunnels IPSec. Ce document est destiné aux utilisateurs de Cisco Secure Access.

Configurations préliminaires

- Activer la recherche de domaine pour le périphérique : Accédez à Groupes de configuration > Profil système > Global et activez la recherche de domaine.

Remarque : Par défaut, la recherche de domaine est désactivée.

- Configurer DNS : Le routeur peut résoudre le DNS et accéder à Internet sur le VPN 0.
- Configurez NAT DIA : La configuration DIA doit être présente sur le routeur où le tunnel SSE est créé.

Créer des interfaces de bouclage

Si les deux tunnels d'une configuration active/active se connectent au même data center de destination et utilisent la même interface WAN que la source, deux adresses IP de bouclage doivent être créées.

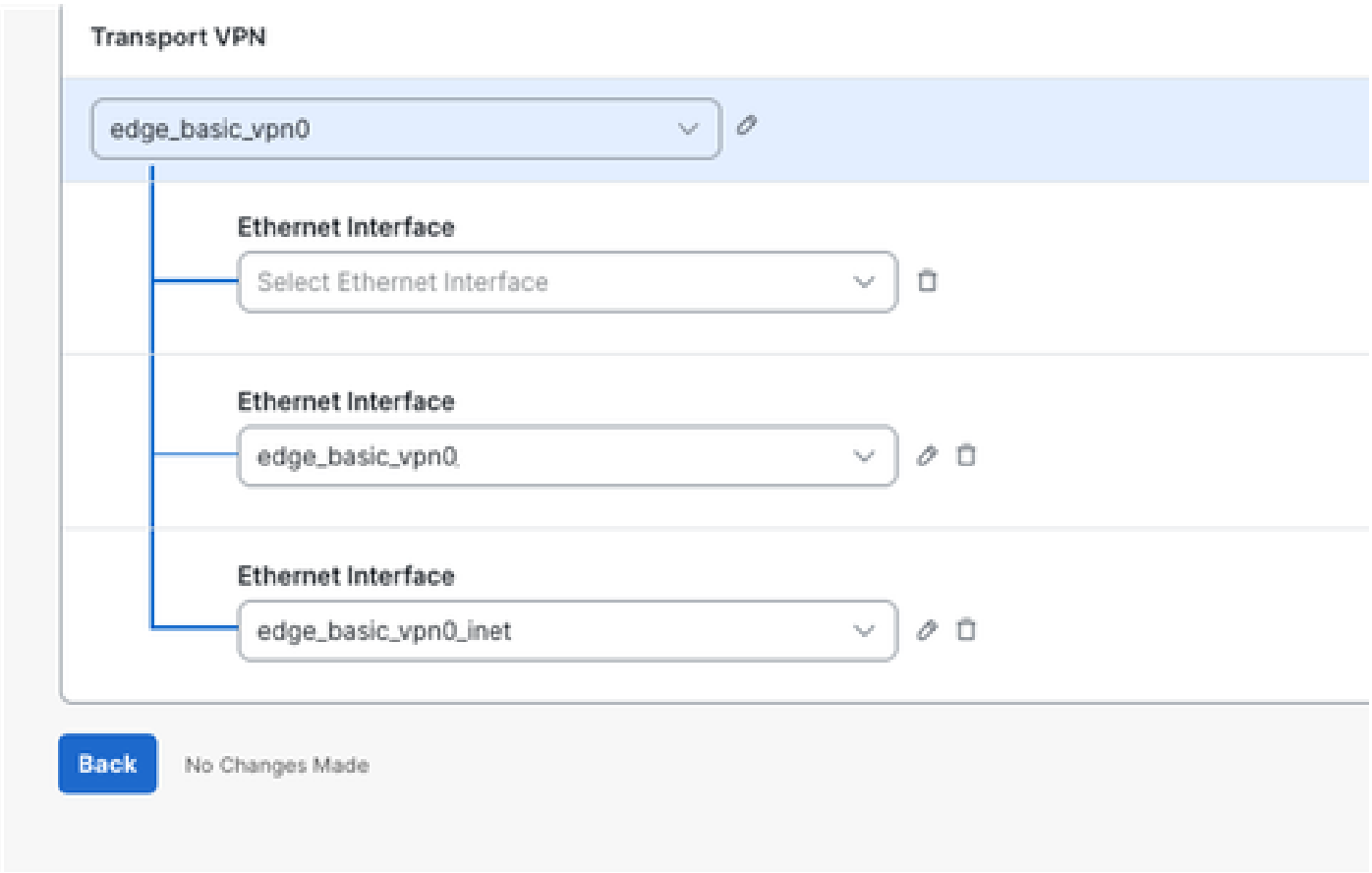
Remarque : Lorsque deux tunnels sont configurés avec la même source et la même destination, IKEv2 forme une paire d'identités composée d'un ID local et d'un ID distant. Par défaut, l'ID local est l'adresse IP de l'interface source du tunnel. Cette paire d'identités doit être unique et ne peut pas être partagée entre deux tunnels. Pour éviter toute confusion dans l'état IKEv2, chaque tunnel utilise une interface de bouclage différente comme source.

Bien que les paquets IKE soient traduits (NATed) sur l'interface DIA, l'ID local reste inchangé et conserve l'adresse IP de bouclage d'origine.

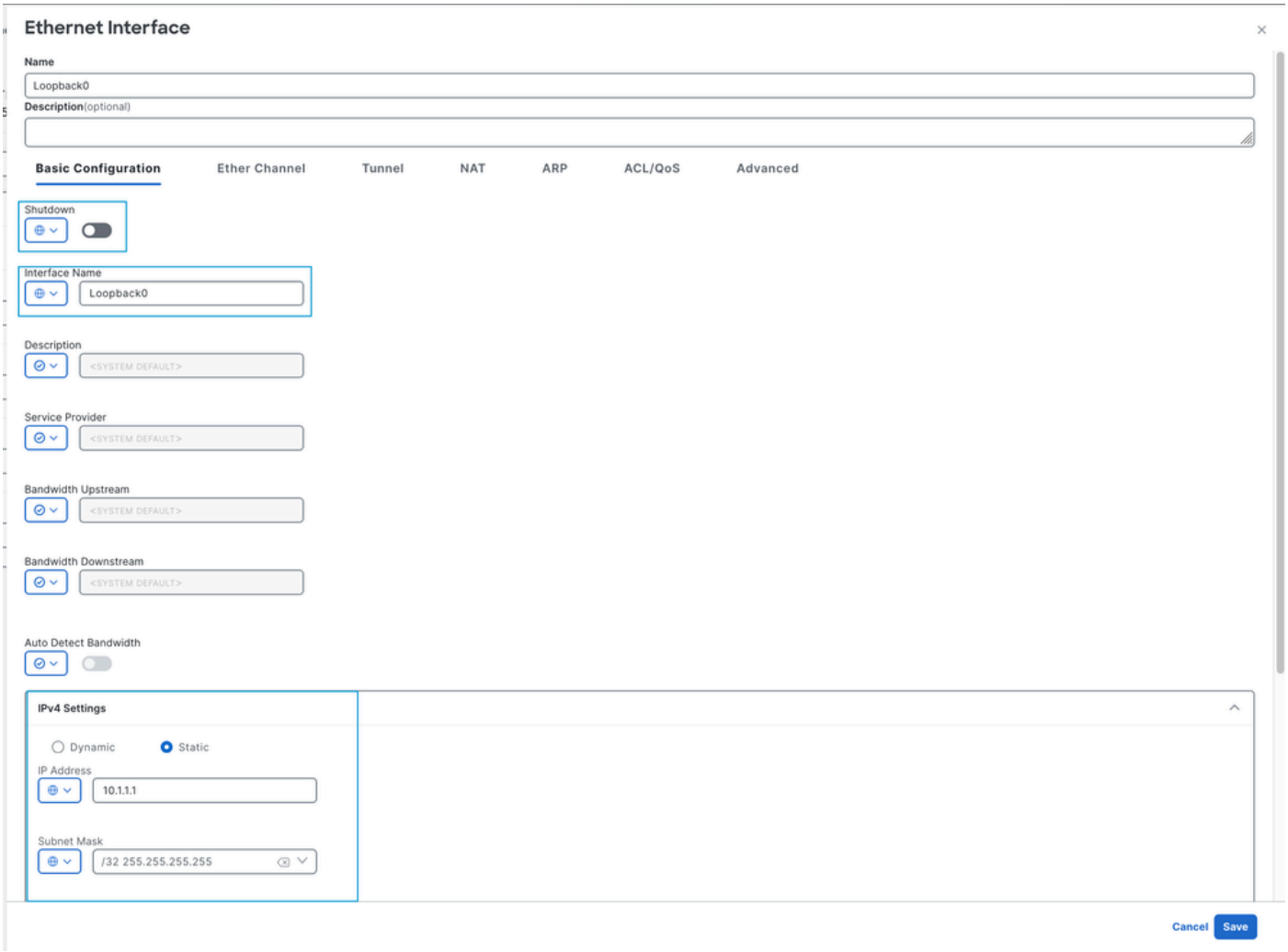
1. Accédez à Configuration > Configuration Groups > Configuration Group Name> Transport & Management Profile > cliquez sur Edit.

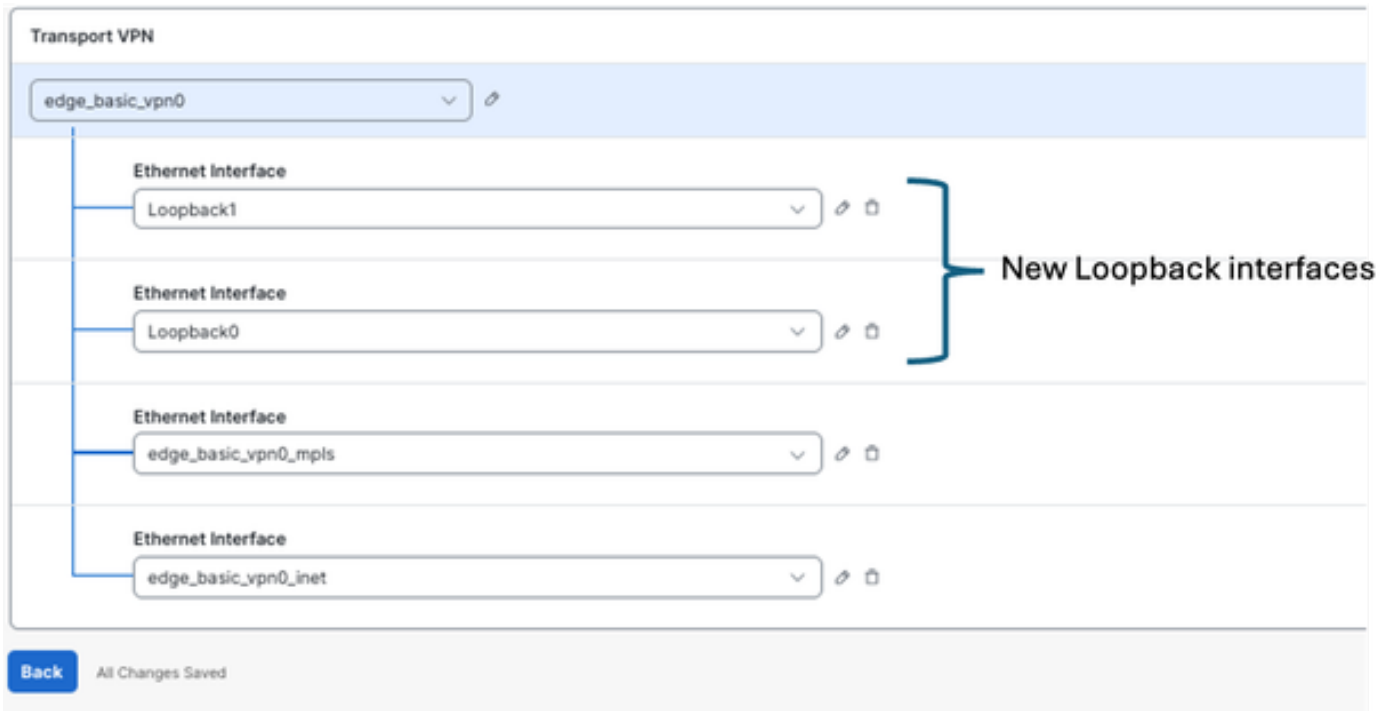
2. Cliquez sur le signe plus (+) à droite du profil VPN de transport (profil principal). Le menu Ajouter une fonction (Add Feature) situé à l'extrême droite s'ouvre.

3. Cliquez sur Ethernet Interface. Il ajoute une nouvelle interface Internet sous Transport VPN.

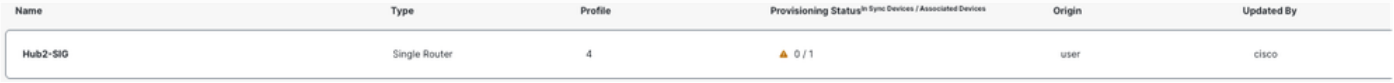


4. Créez les deux interfaces de bouclage à l'aide des adresses IPv4 RFC1918, comme l'exemple Loopback0 dans l'image.



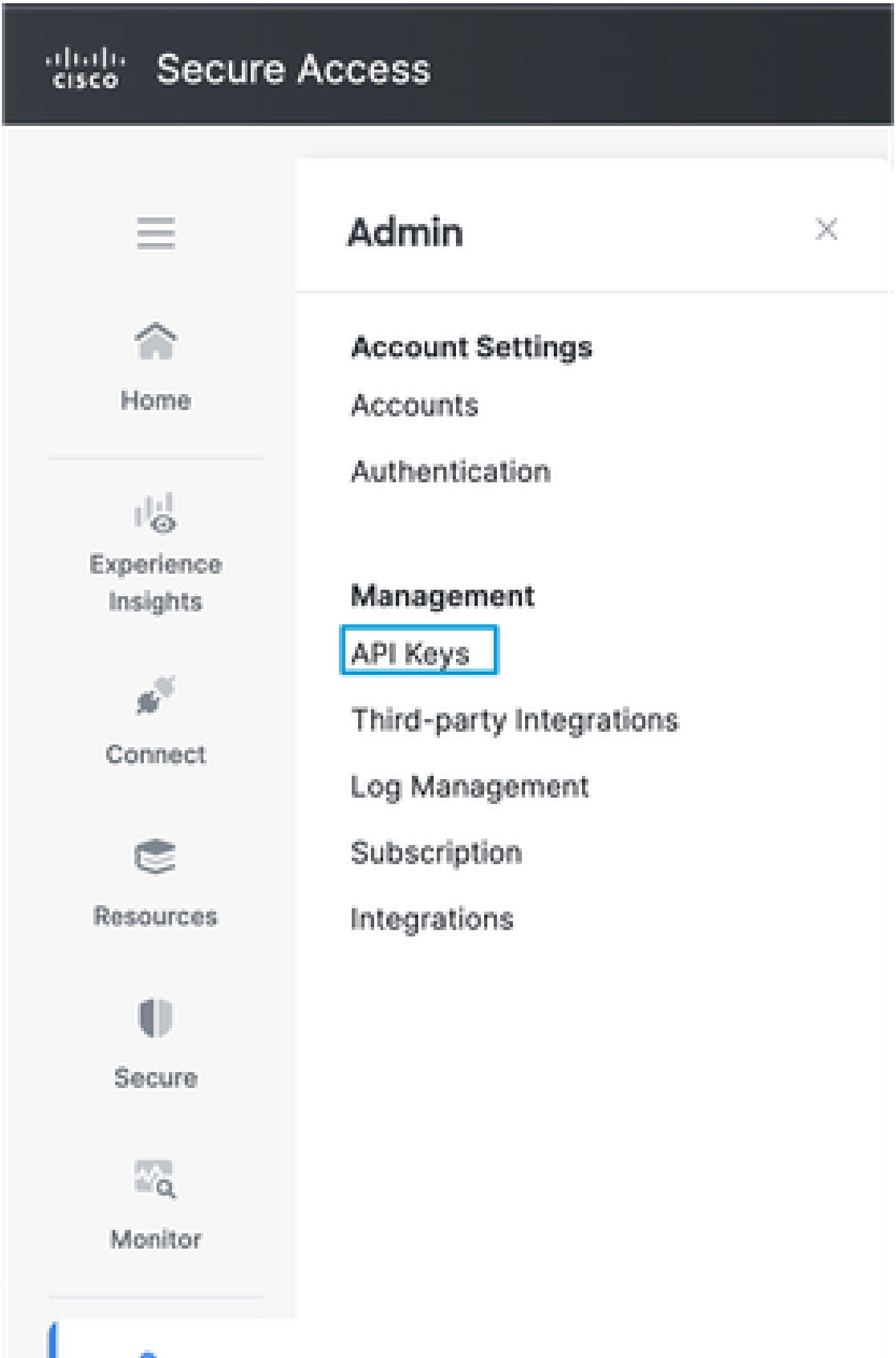


5. Après avoir appliqué la configuration de bouclage, poursuivez le déploiement de la modification de configuration sur le périphérique. Notez que l'état d'approvisionnement passe de 1/1 à 0/1.

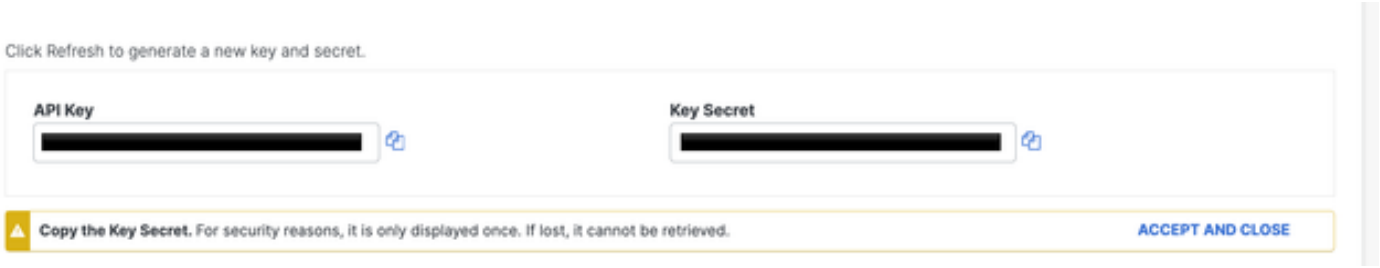


Configurer de nouvelles clés API sur le portail SSE

1. Accès au portail SSE https://login.sse.cisco.com/
2. Accédez à Admin > Clés API


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. Copiez la clé API et la clé secrète dans un bloc-notes et sélectionnez ACCEPT AND CLOSE (ACCEPTER ET FERMER)

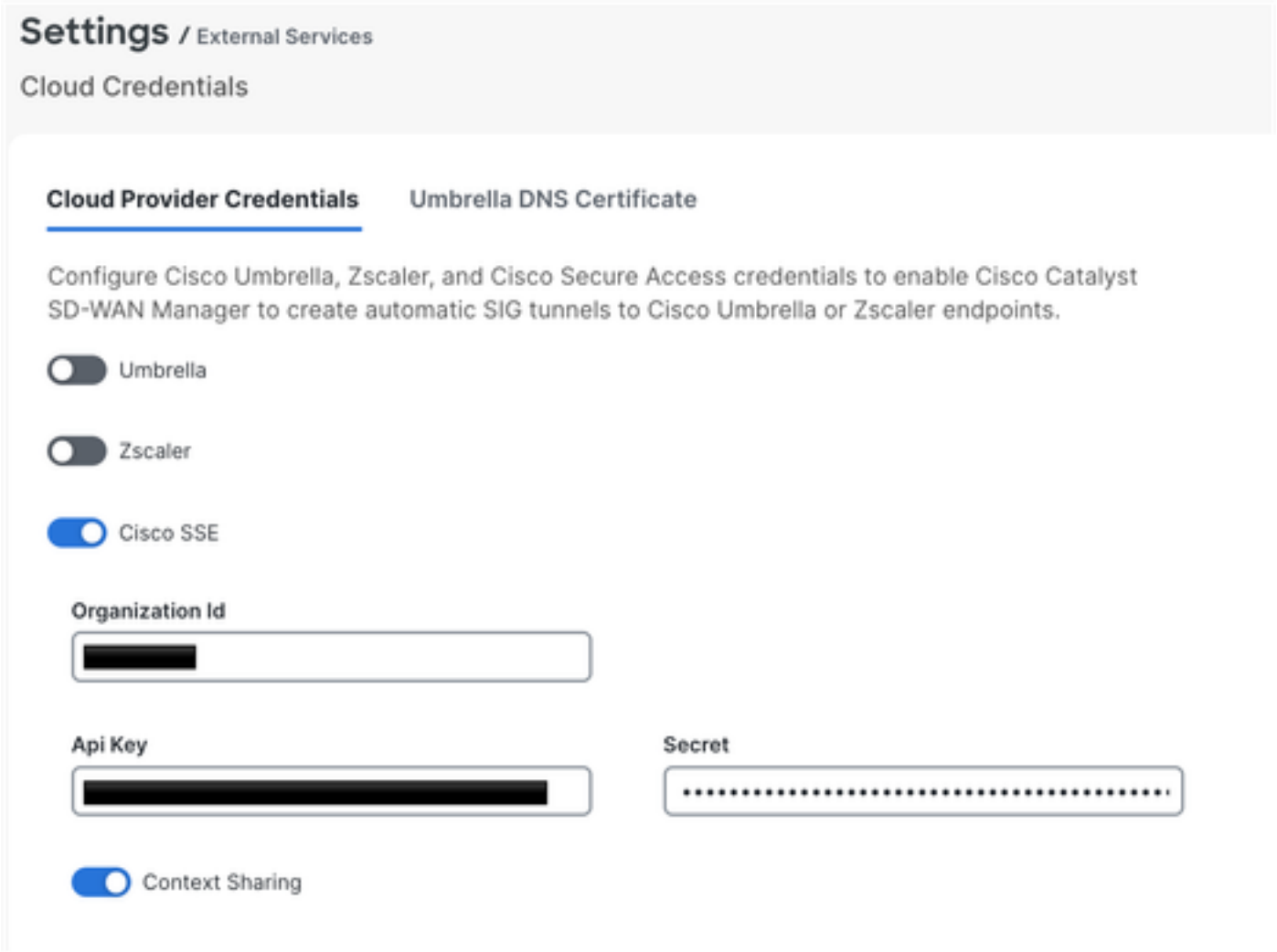


7. Sous l'URL https://dashboard.sse.cisco.com/#some-numbers#/admin/apikeys#some-numbers# est votre ID d'organisation. Copiez également ces informations dans votre bloc-notes.

Configurer SSE sur Catalyst Manager

Configurer les informations d'identification cloud

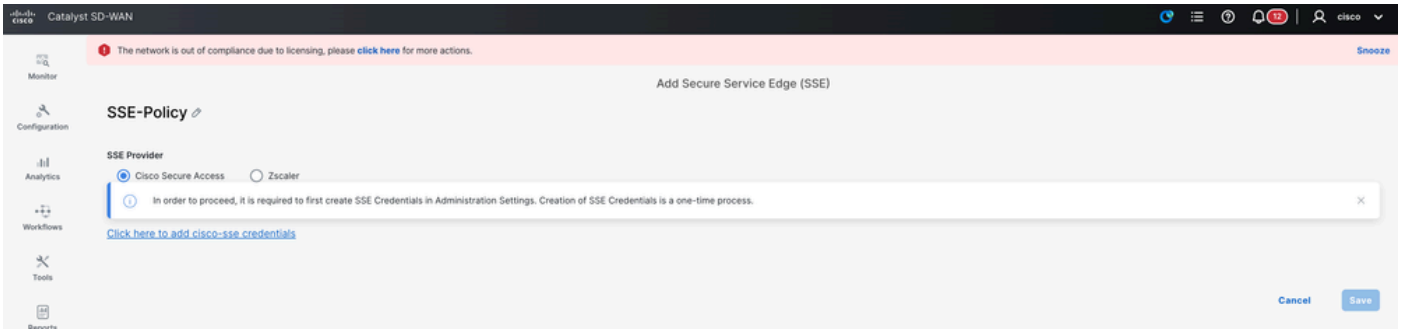
1. Accédez à Administration > Settings > Cloud Credentials > Cloud Provider Credentials, et activez l'accès sécurisé Cisco
et entrez les détails.



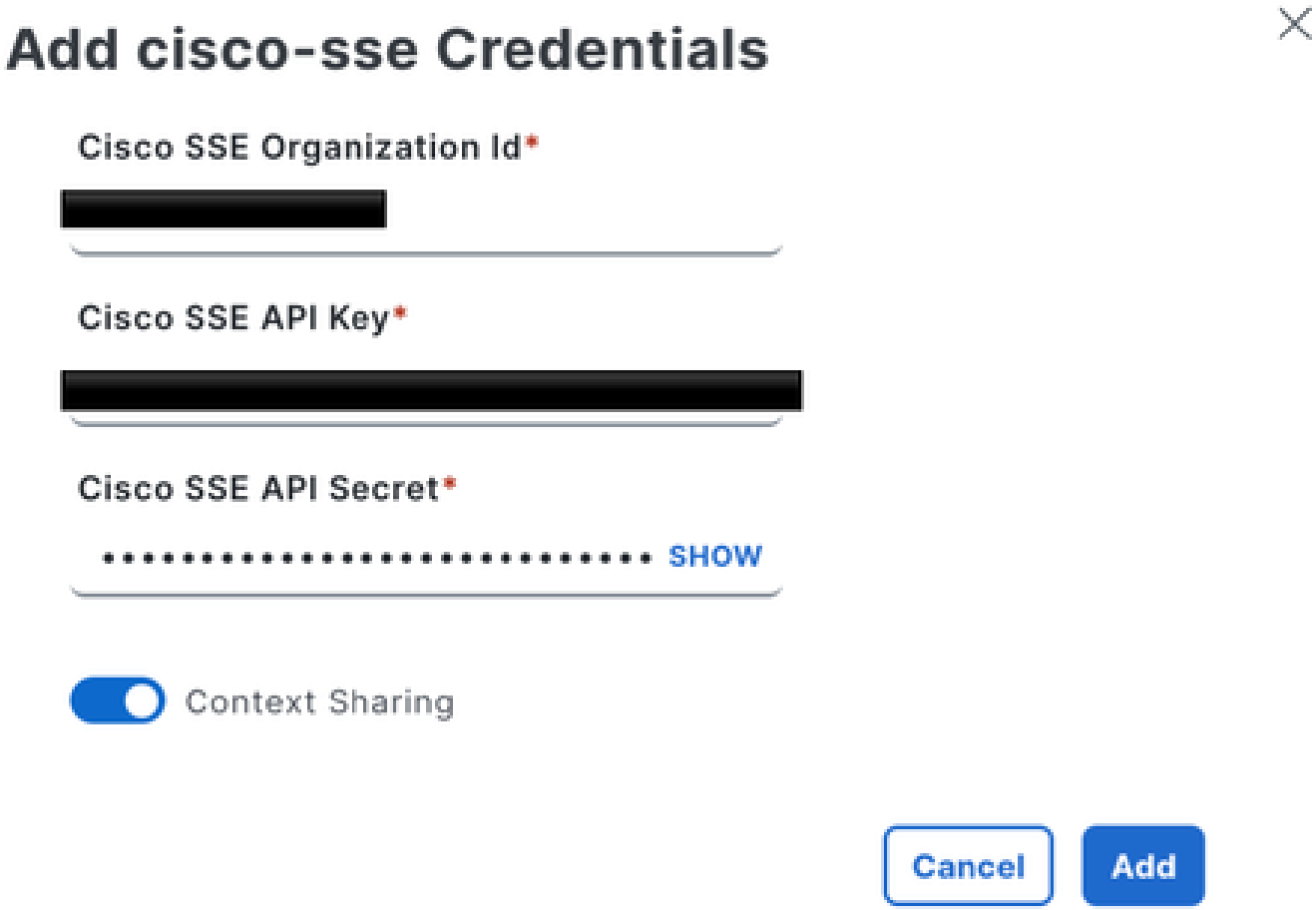
2. Facultatif : Vous pouvez activer le partage de contexte pour une fonctionnalité améliorée. Pour plus d'informations, reportez-vous au Guide de l'utilisateur Cisco SSE sur le partage de contexte.

Configuration des tunnels SSE à l'aide du groupe de stratégies

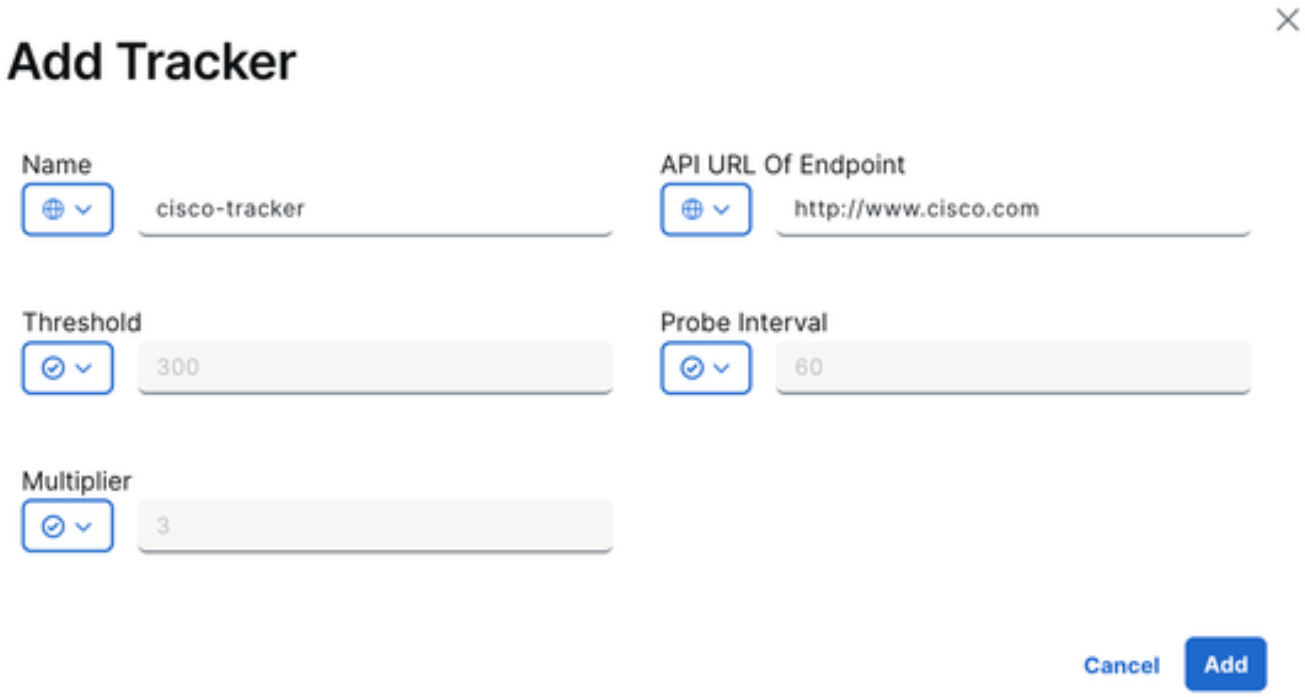
Dans le gestionnaire SD-WAN, accédez à Configuration > Policy Groups > Secure Internet Gateway/Secure Service Edge et cliquez sur Add Secure Service Edge (SSE) .

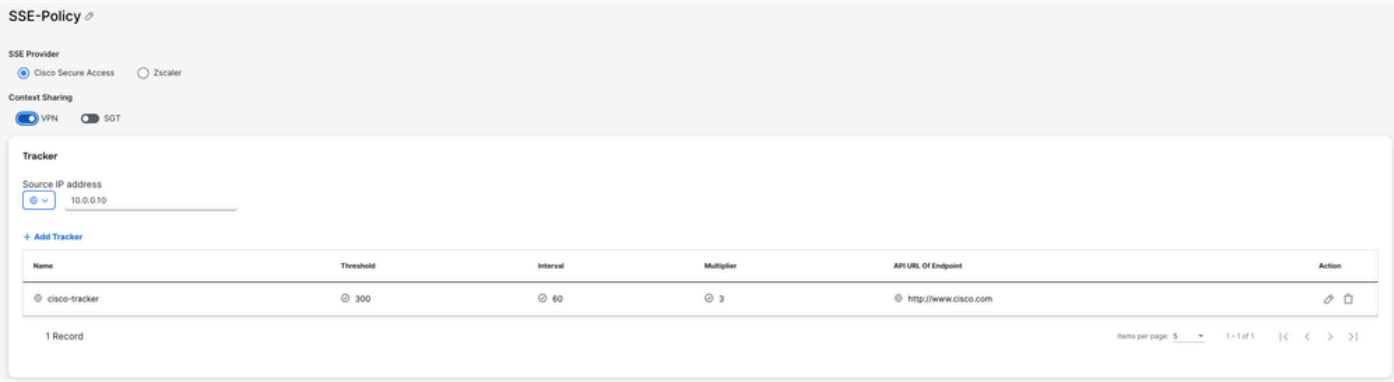


Remarque : si les informations d'identification du cloud n'ont pas encore été configurées, vous pouvez les ajouter à cette étape. Si les informations d'identification ont déjà été configurées, elles sont chargées automatiquement.



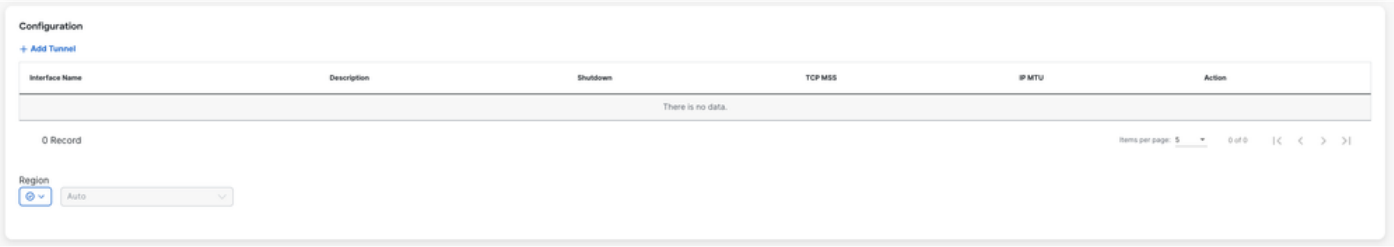
1. Configurez le dispositif de suivi SSE. Dans cet exemple, l'URL du dispositif de suivi est définie sur http://www.cisco.com, et l'adresse IP source est attribuée à partir de l'une des interfaces de bouclage.



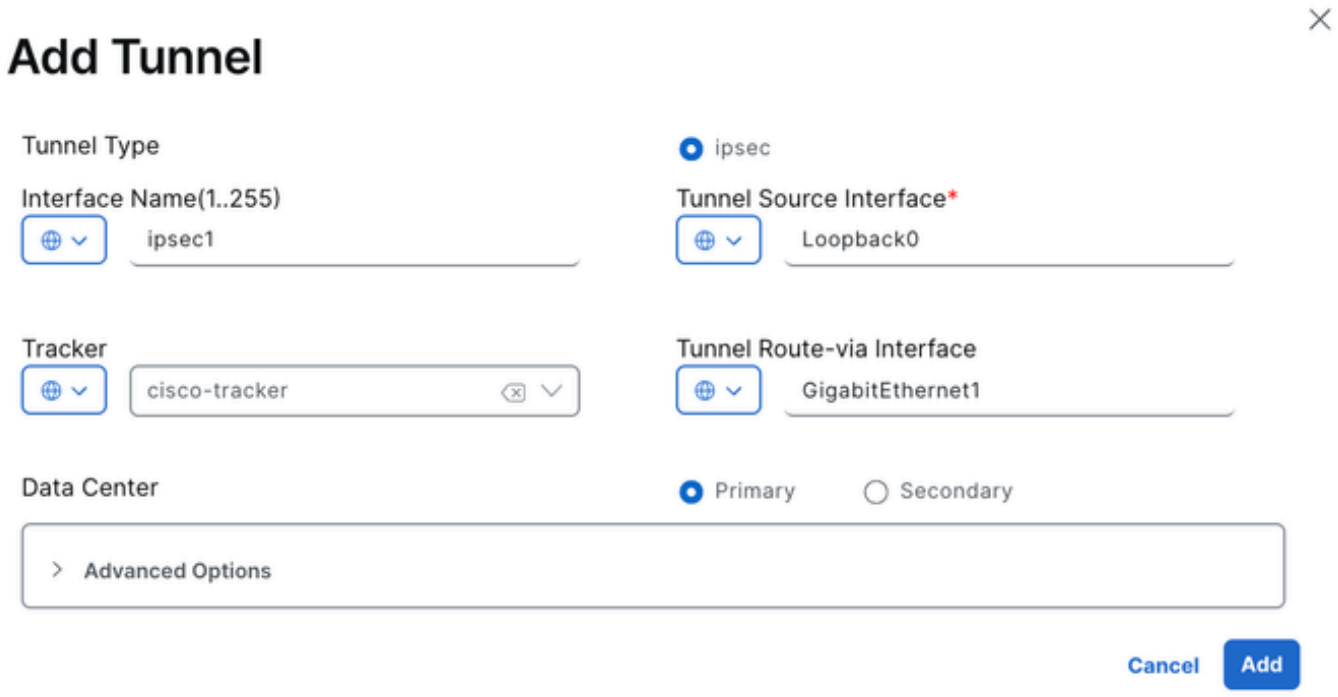


Comme le partage de contexte a été activé lorsque les informations d'identification du cloud ont été configurées, le VPN est sélectionné comme option facultative dans cet exemple.

2. Cliquez sur Add Tunnel

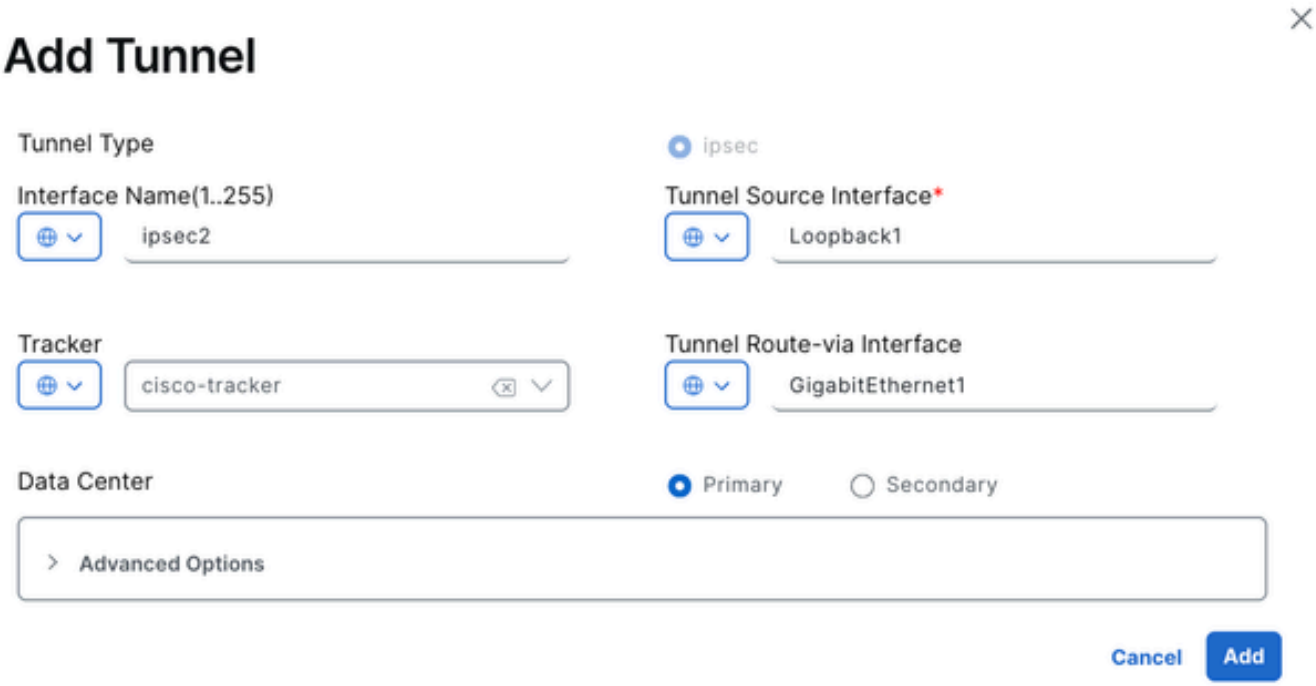


3. Dans cet exemple, l’interface Loopback0 est utilisée comme source du tunnel, tandis que l’interface GigabitEthernet1 sert d’interface WAN pour acheminer le trafic.



Comme le tracker a été configuré dans cet exemple, le paramètre est changé en Global, et le tracker cisco préconfiguré est sélectionné.

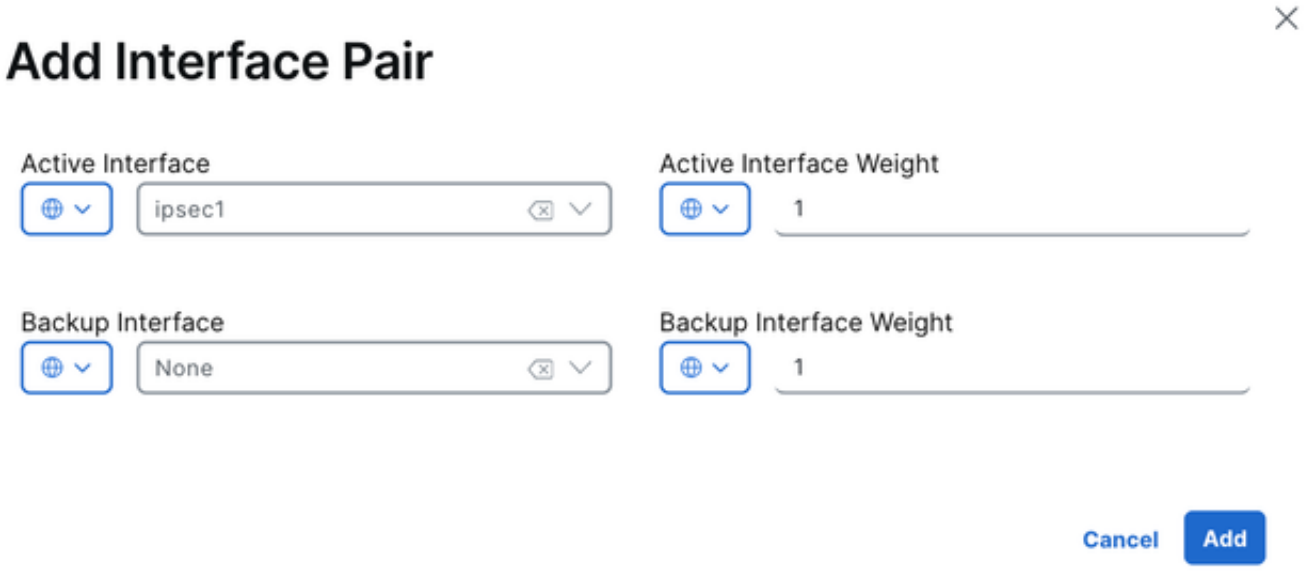
4. Pour le deuxième tunnel, répétez les mêmes étapes en utilisant les mêmes paramètres, mais changez le nom d'interface de ipsec1 à ipsec2, et le nom d'interface source à Loopback1.



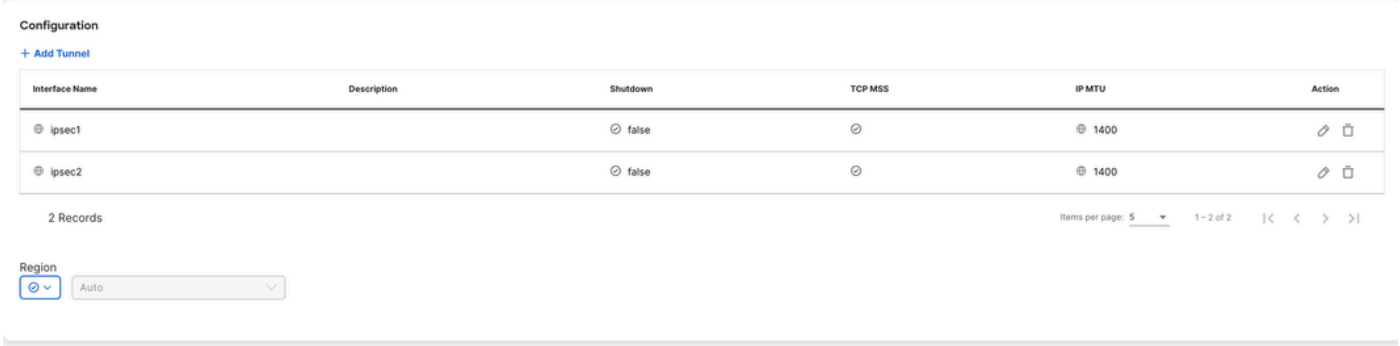
Les deux tunnels sont configurés pour être actifs simultanément, sans sauvegarde.

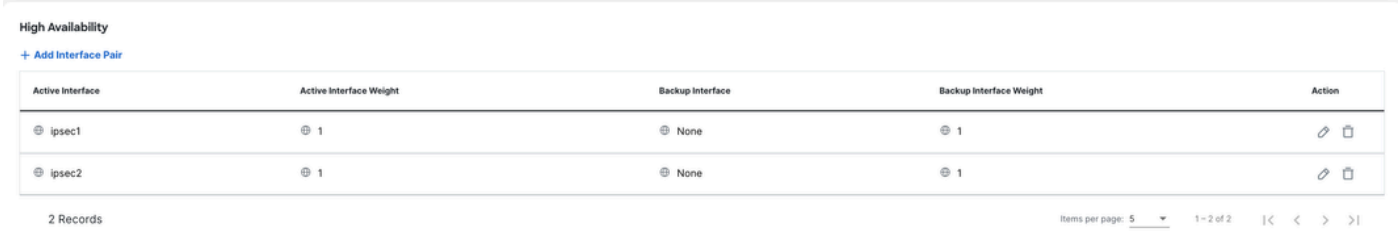
5. Cliquez sur Add Interface Pair.

6. Cliquez sur Ajouter. L'interface active est définie sur ipsec1 et aucune interface de sauvegarde n'est spécifiée.



7. La même opération est répétée pour le deuxième tunnel, ipsec2.

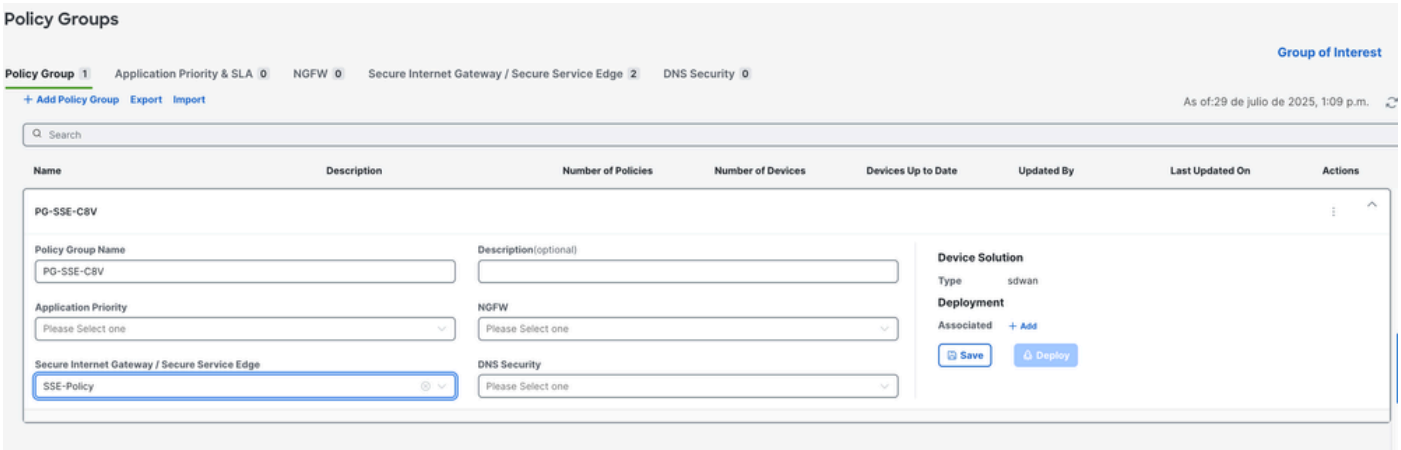




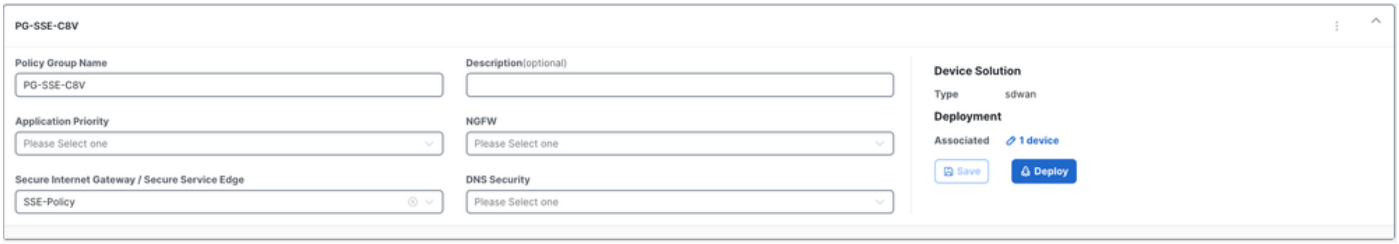
8. Enregistrez la configuration.

Configurer le groupe de stratégies

1. Il vous suffit de sélectionner la règle précédemment créée dans le groupe de règles et de l'enregistrer.



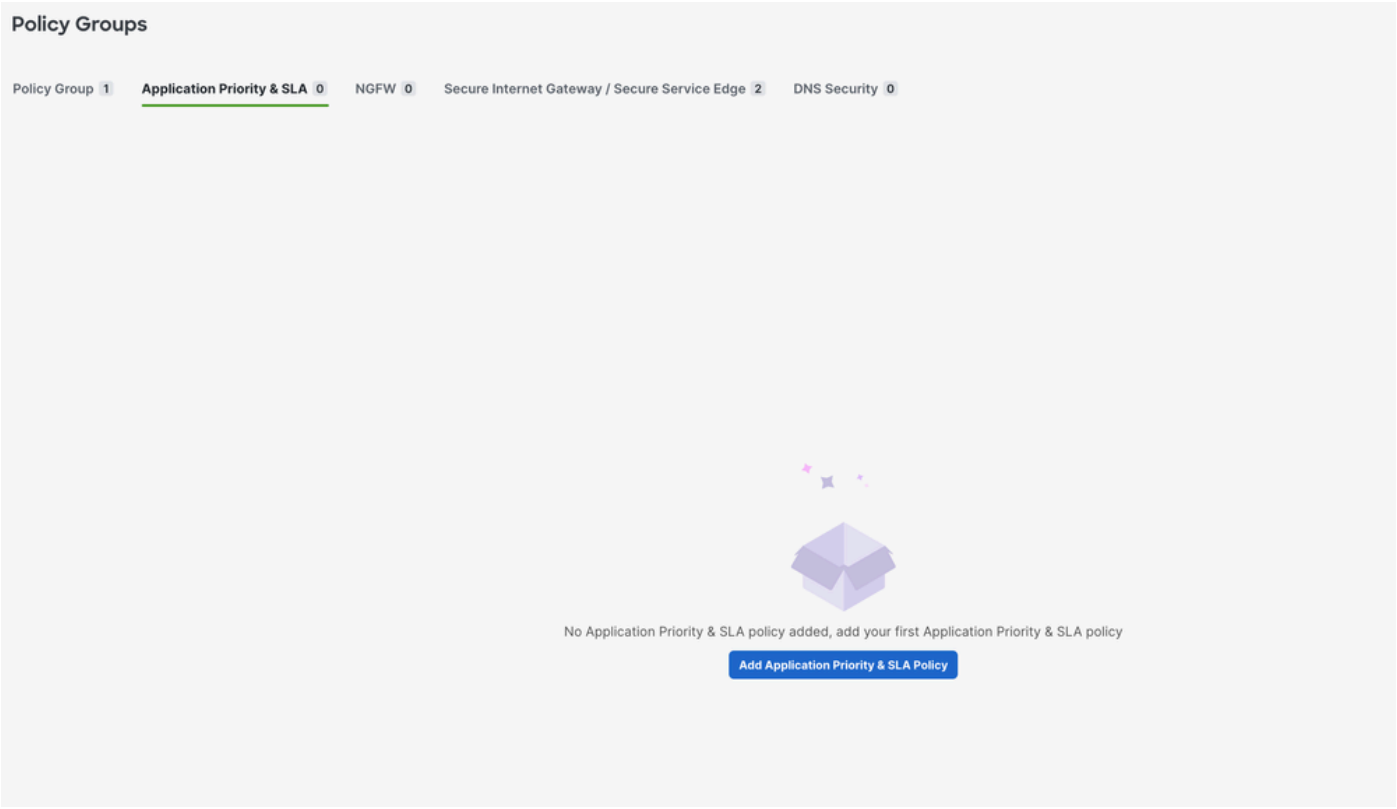
2. Une fois que le ou les périphériques ont été associés au groupe de stratégies, poursuivez le déploiement du groupe de stratégies.



Configurer le groupe de stratégies pour rediriger le trafic vers SSE

1. Sur le gestionnaire SD-WAN, accédez à Configuration > Policy Groups > Application Priority & SLA.

- Sélectionnez Ajouter une priorité d'application et une politique SLA
- Spécifiez un nom pour la stratégie.

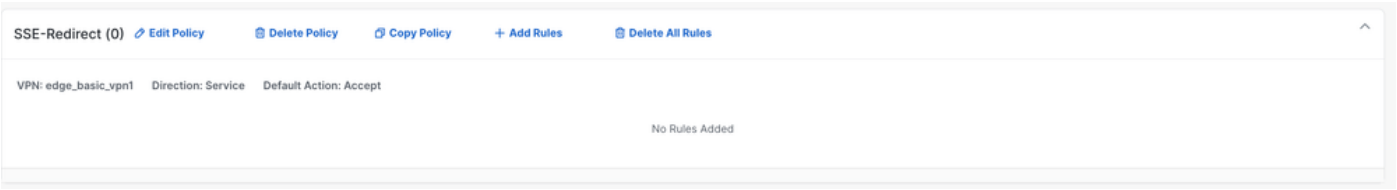


2. Une fois la nouvelle stratégie affichée, sélectionnez la bascule Mise en page avancée.

3. Sélectionnez Add Traffic Policy List.

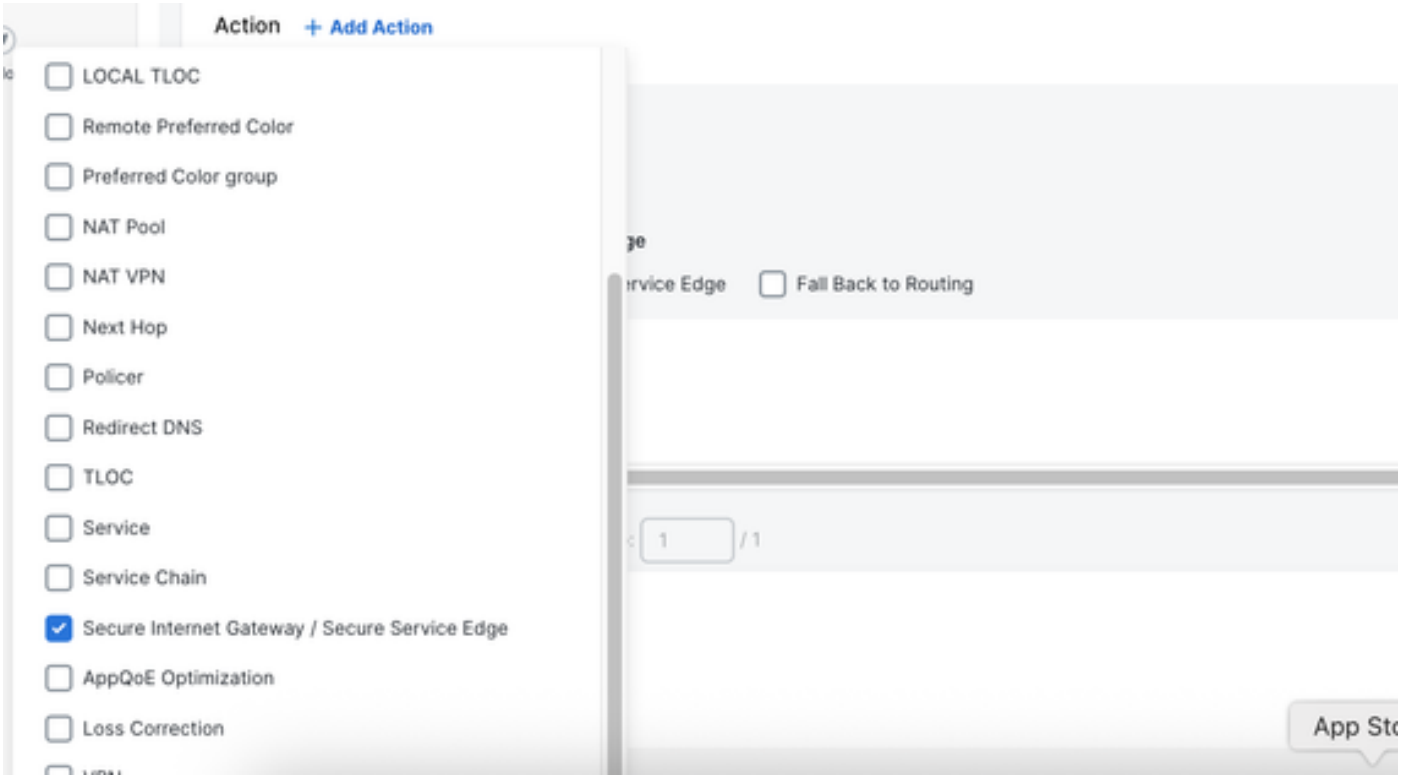
- Configurez les VPN pour rediriger le trafic vers le tunnel SSE.
- Définissez la direction et l'action par défaut selon vos besoins, puis enregistrez.

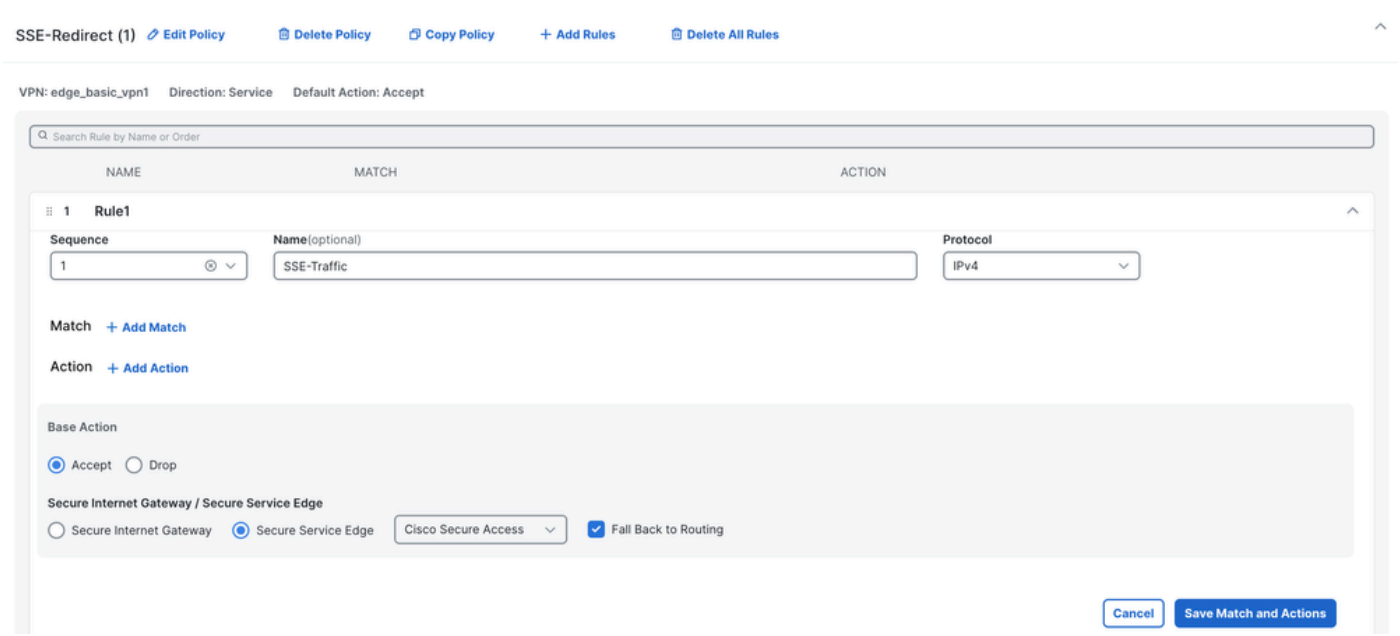
4. Sélectionnez + Ajouter une règle.



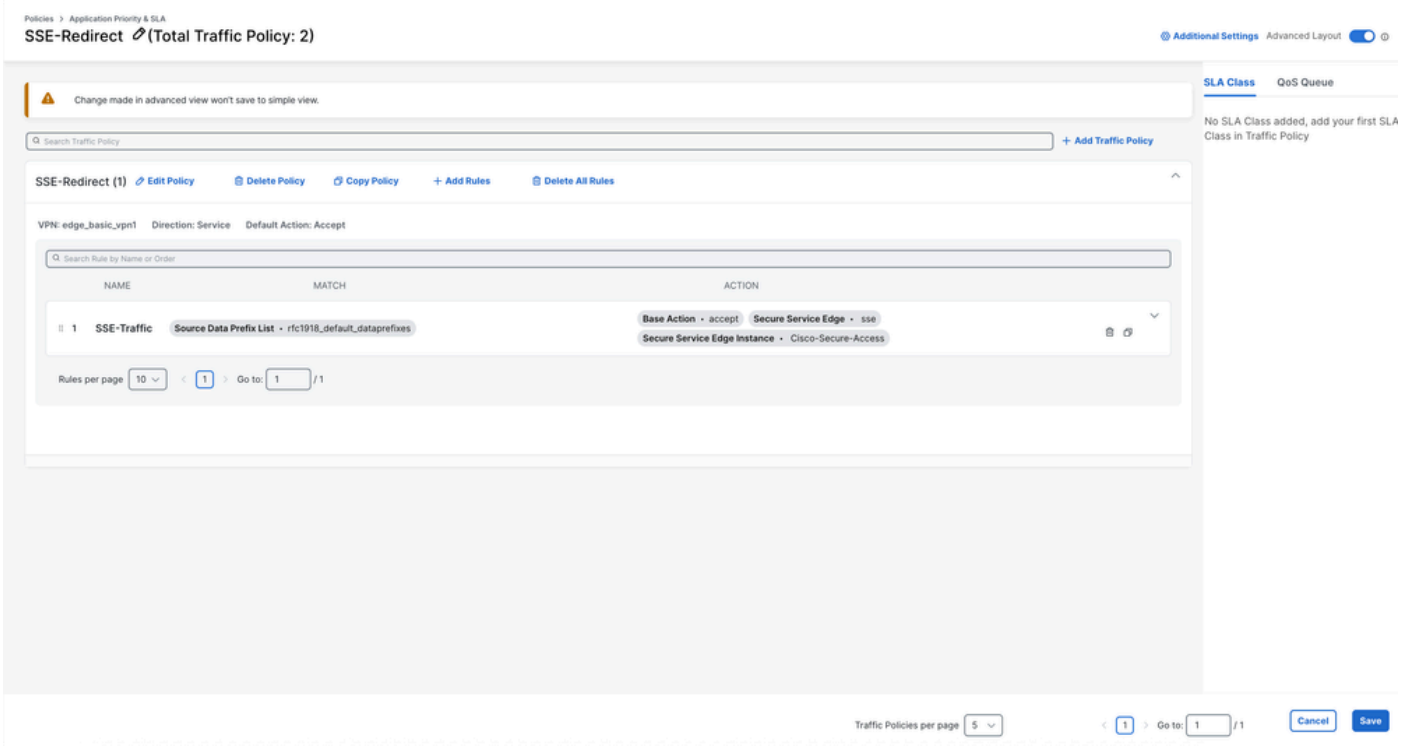
5. Configurez vos critères de trafic de correspondance pour rediriger le trafic vers le SSE.
6. Sélectionnez Accepter comme action de base, puis cliquez sur + Action.

7. Recherchez l'action Secure Internet Gateway / Secure Service Edge et définissez-la sur Secure Service Edge.



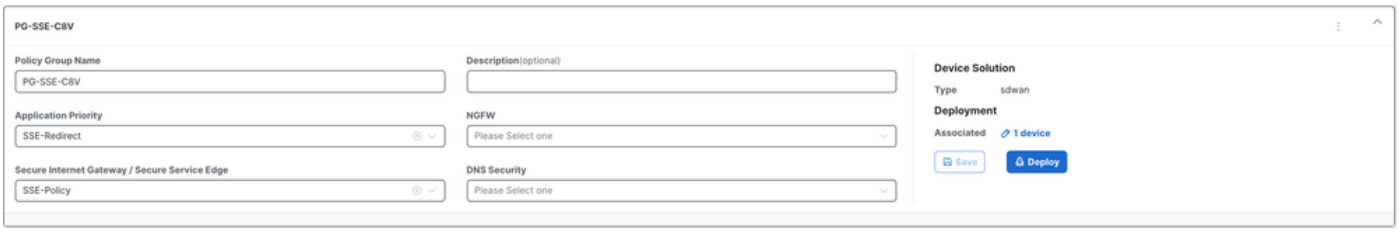


8. Cliquez sur Enregistrer la correspondance et les actions



9. Cliquez sur Enregistrer.

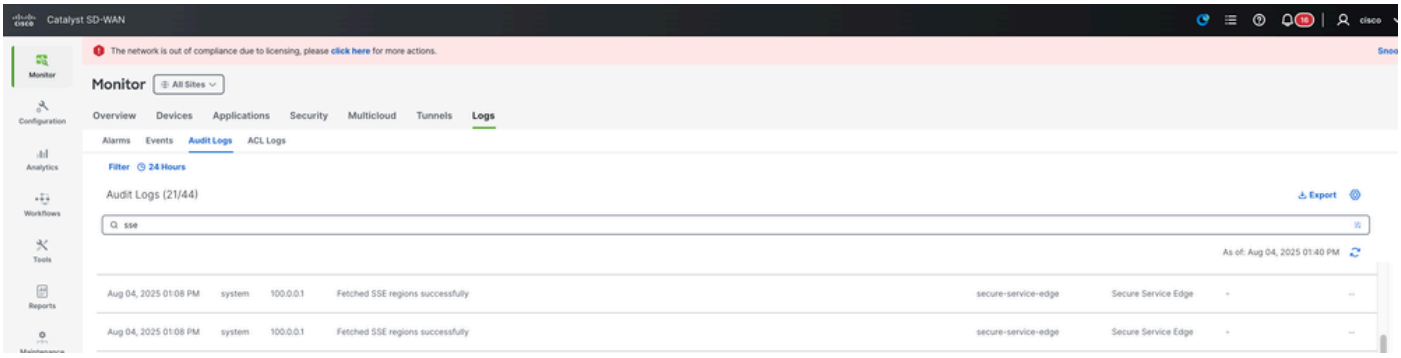
10. Accédez à Configuration > Policy Groups et sélectionnez la stratégie Application Priority que vous venez de créer. Enregistrez, puis déployez.



Vérifier

Responsable

1. Surveiller > Journaux > Journaux d'audit et recherchez « sse ».



2. Vous pouvez vérifier si le VPN de partage de contexte est activé correctement en cochant la

case Manager.

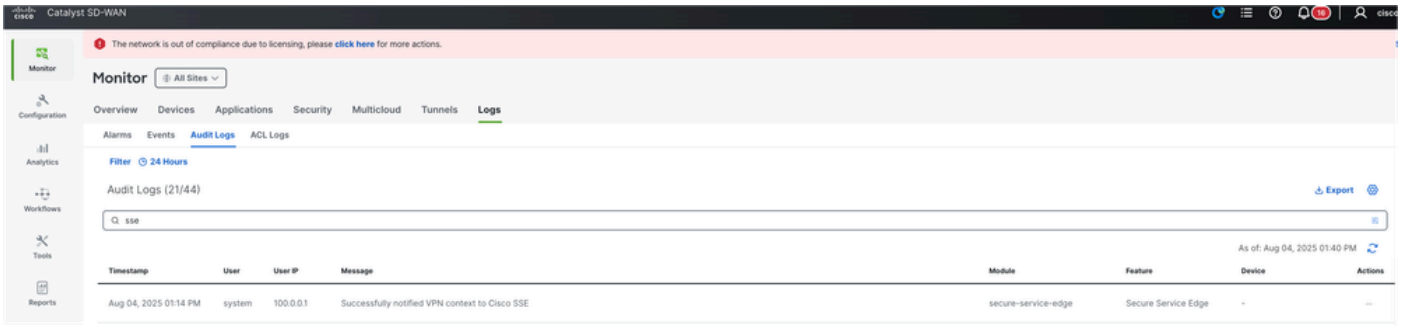
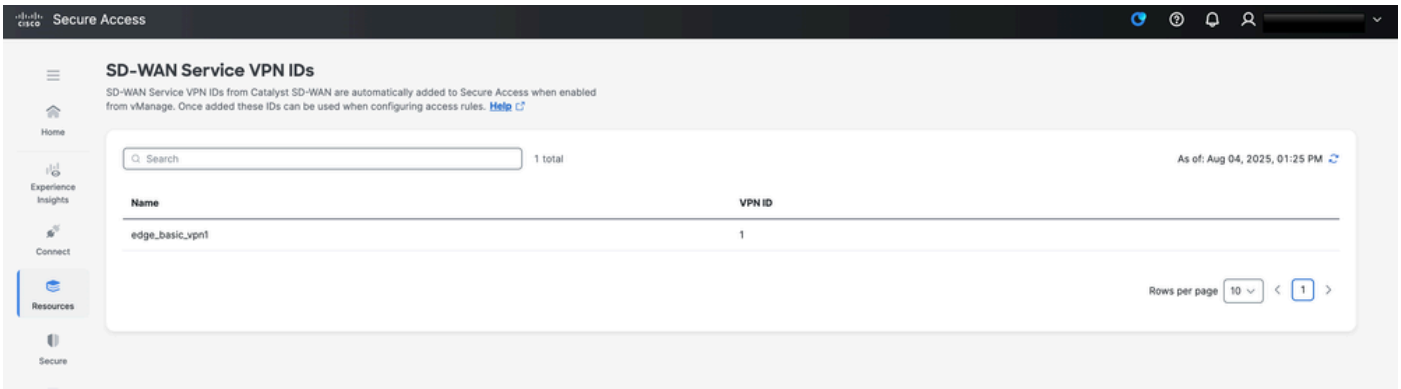


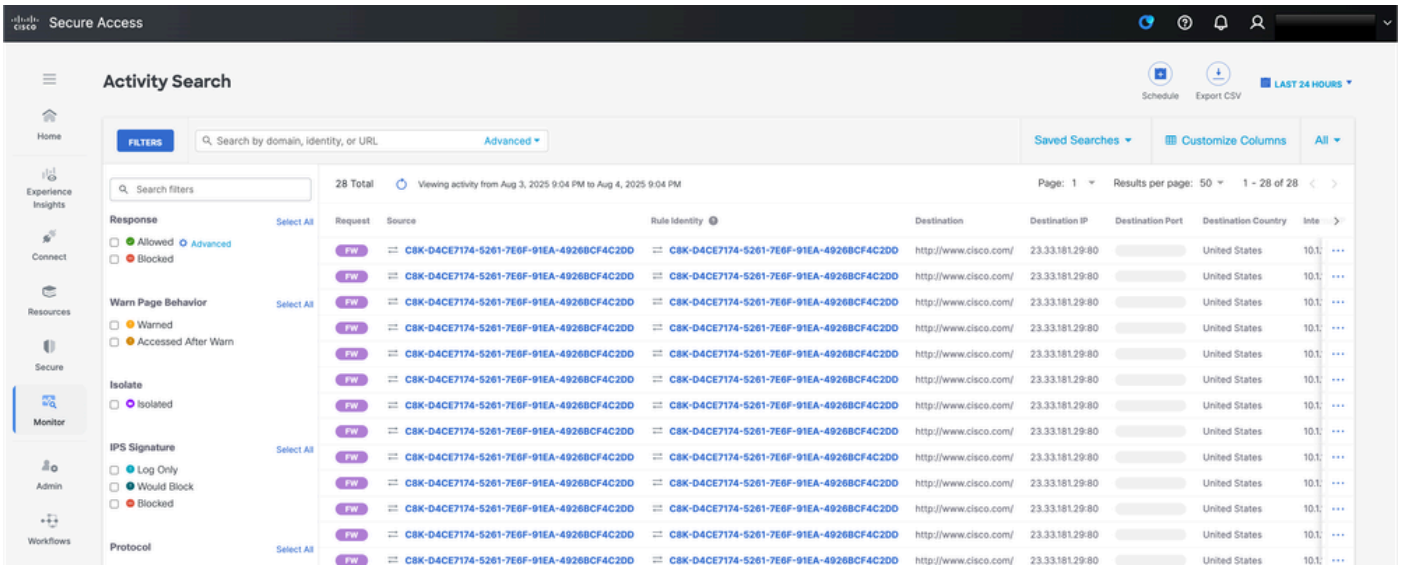
Tableau de bord Secure Access

Partage de contexte
Vous pouvez vérifier si le VPN de partage de contexte est activé correctement en vérifiant le tableau de bord SSE,Ressources > ID VPN du service SD-WAN



Tunnel vers le haut

Lorsque le tunnel est actif et que le traqueur est opérationnel avec le trafic circulant à travers le tunnel, vous pouvez le valider en naviguant vers Monitor > Activity Search. Dans cet écran, vous voyez le trafic qui traverse le tunnel, comme les requêtes vers www.cisco.com générées par le traqueur. Cette visibilité confirme que le traqueur est actif et surveille activement le trafic à travers le tunnel



Commandes CLI (Command Line Interface)

<#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
```

Informations connexes

- Configuration du partage de contexte SD-WAN
- Intégration de Cisco Secure Access avec le routage SD
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.