Konfiguration und Fehlerbehebung bei der SSE-Integration (Secure Access) im Catalyst SD-WAN

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Aktiv/Aktiv-SSE-Integration auf dem Catalyst SD-WAN konfigurieren, und es wird erläutert, wie Sie diese Fehler beheben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Software-Defined Wide Area Network (SD-WAN)
- Konfigurationsgruppen
- Richtliniengruppen

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- C8000V Version17.15.02
- vManage, Version 20.15.02

- Cisco Secure Access-Konto

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Sicherer Zugriff von Cisco

Cisco Secure Access ist eine Cloud-basierte Security Service Edge (SSE)-Lösung, die mehrere Netzwerksicherheitsservices zusammenführt und diese über die Cloud bereitstellt, um eine hybride Belegschaft zu unterstützen. Der Cisco SD-WAN Manager nutzt REST-APIs, um Richtlinieninformationen von Cisco Secure Access abzurufen, und verteilt diese Informationen an Cisco IOS XE SD-WAN-Geräte. Diese Integration ermöglicht einen nahtlosen, transparenten und sicheren direkten Internetzugang (Direct Internet Access, DIA) für Benutzer, sodass diese von jedem Gerät aus und von jedem Ort aus sicher auf das Netzwerk zugreifen können.

Mit Cisco SSE können SD-WAN-Geräte über IPSec-Tunnel Verbindungen zu SSE-Anbietern herstellen. Dieses Dokument ist für Benutzer von Cisco Secure Access bestimmt.

Vorkonfigurationen

- Domänensuche für das Gerät aktivieren: Navigieren Sie zu Configuration Groups > System Profile > Global, und aktivieren Sie Domain Lookup.

Anmerkung: Standardmäßig ist die Domänensuche deaktiviert.

- DNS konfigurieren: Der Router kann DNS auflösen und über VPN 0 auf das Internet zugreifen.
- NAT-DIA konfigurieren: Die DIA-Konfiguration muss auf dem Router vorhanden sein, auf dem der SSE-Tunnel erstellt wird.

Loopback-Schnittstellen erstellen

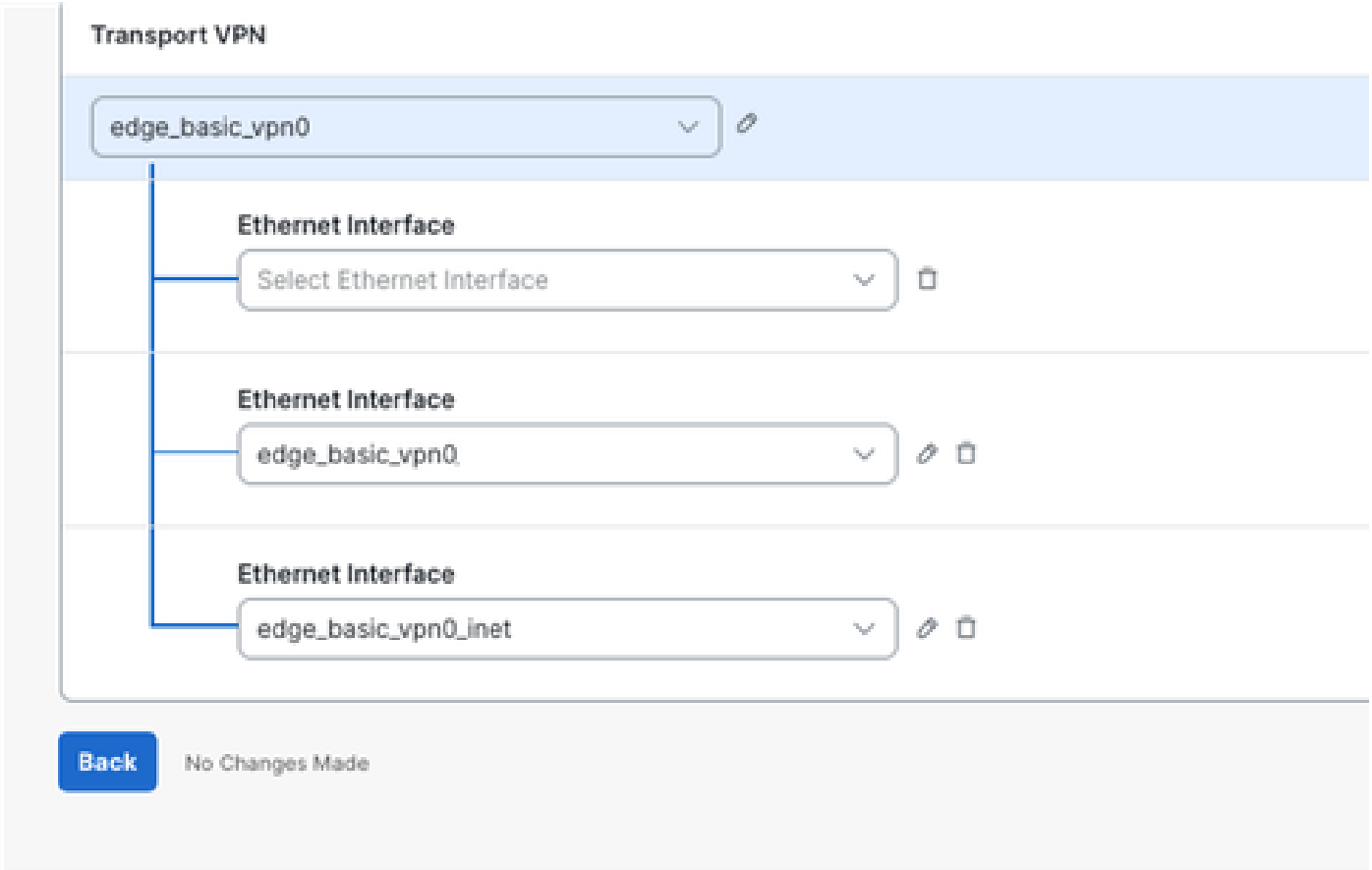
Wenn beide Tunnel in einer Aktiv/Aktiv-Konfiguration eine Verbindung mit demselben Zielrechenzentrum herstellen und dieselbe WAN-Schnittstelle wie die Quelle verwenden, müssen zwei Loopback-IP-Adressen erstellt werden.

Anmerkung: Wenn zwei Tunnel mit derselben Quelle und demselben Ziel konfiguriert werden, bildet IKEv2 ein Identitätspaar, das aus einer lokalen ID und einer Remote-ID besteht. Standardmäßig ist die lokale ID die IP-Adresse der Quellschnittstelle des Tunnels. Dieses Identitätspaar muss eindeutig sein und kann nicht von zwei Tunneln gemeinsam genutzt werden. Um Verwechslungen mit dem IKEv2-Status zu vermeiden, verwendet jeder Tunnel eine andere Loopback-Schnittstelle als Quelle. Obwohl IKE-Pakete auf der DIA-Schnittstelle übersetzt (NATed) werden, bleibt die lokale ID unverändert und behält die ursprüngliche Loopback-IP-Adresse bei.

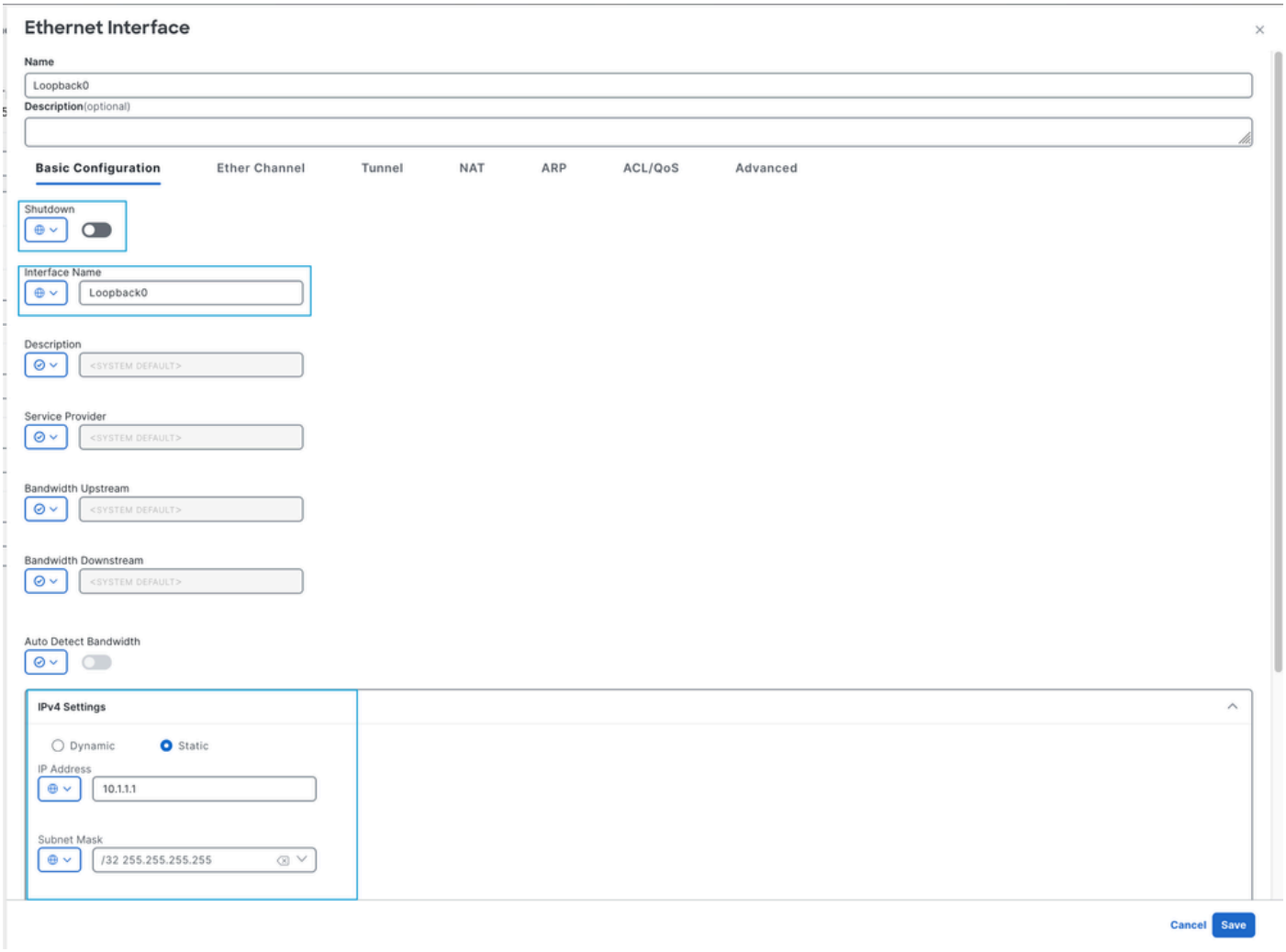
1. Navigieren Sie zu Konfiguration > Konfigurationsgruppen > Konfigurationsgruppenname> Transport- und Managementprofil > klicken Sie auf "Bearbeiten"..

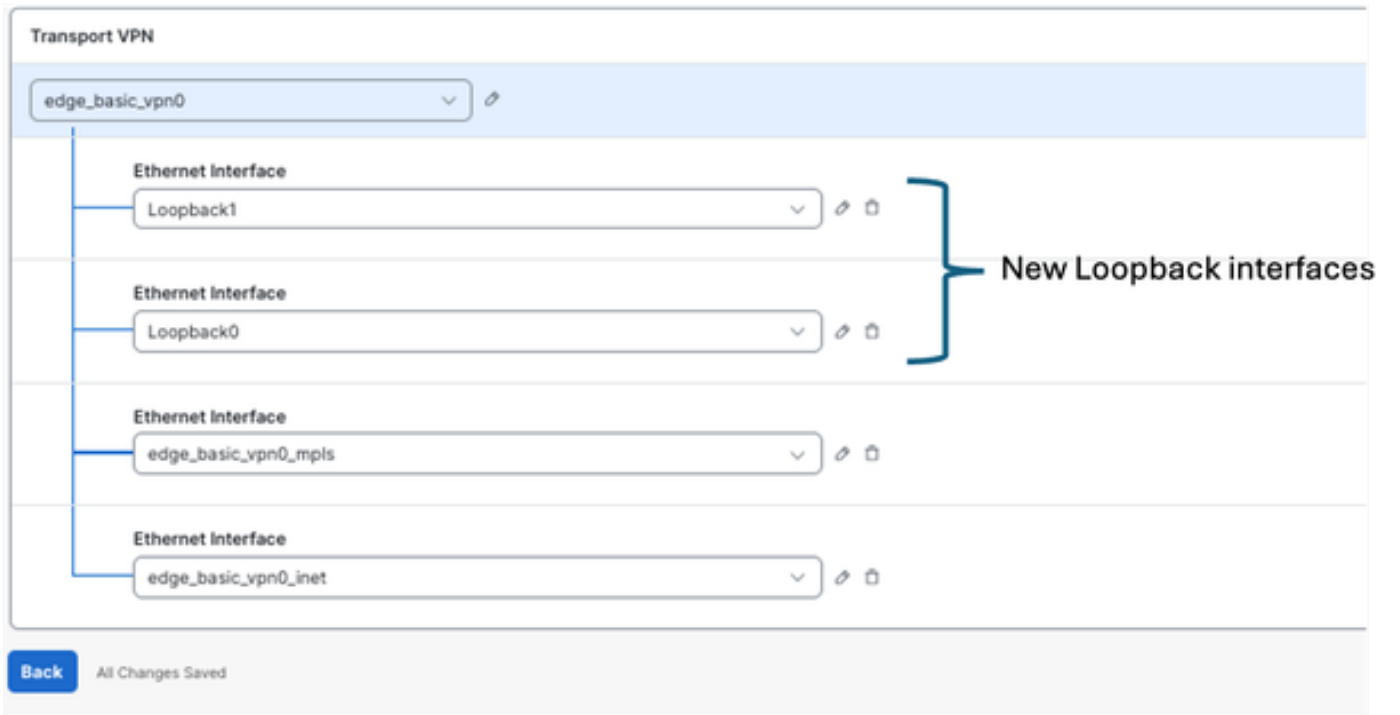
2. Klicken Sie auf das Pluszeichen (+) auf der rechten Seite des Transport-VPN-Profils (Hauptprofil). Daraufhin wird ganz rechts ein Menü zum Hinzufügen von Funktionen geöffnet.

3. Klicken Sie auf Ethernet Interface. Es fügt eine neue Internet-Schnittstelle unter Transport VPN.

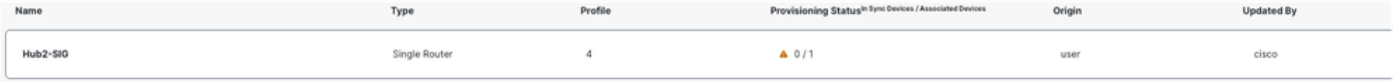


4. Erstellen Sie die beiden Loopback-Schnittstellen mit RFC1918 IPv4-Adressen, wie im Beispiel Loopback0 in der Abbildung dargestellt.



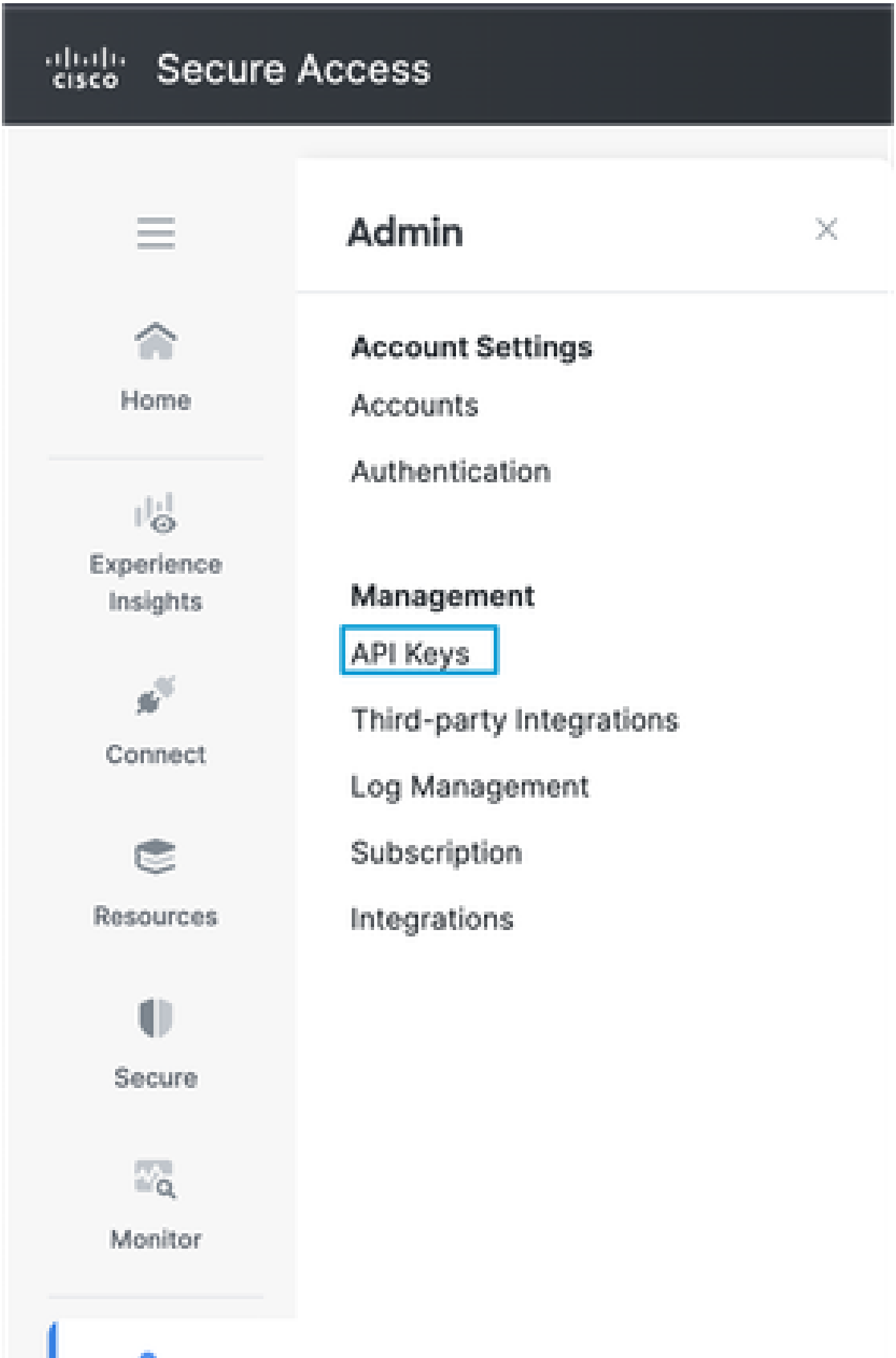


5. Fahren Sie nach dem Anwenden der Loopback-Konfiguration mit der Bereitstellung der Konfigurationsänderung auf dem Gerät fort. Beachten Sie, dass sich der Bereitstellungsstatus von1/1 zu 0/1 ändert.

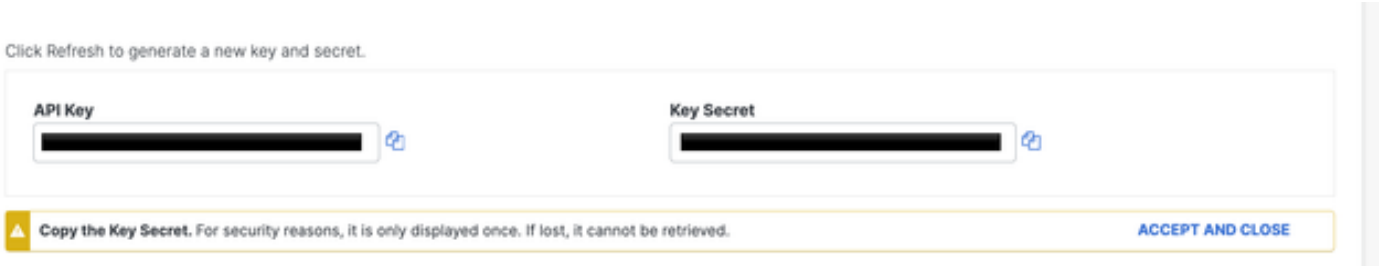


Konfigurieren neuer API-Schlüssel im SSE-Portal

1. Zugang zum SSE-Portal https://login.sse.cisco.com/
2. Navigieren Sie zu 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. Kopieren Sie den API-Schlüssel und Key Secret in einen Notizblock und wählen Sie AKZEPTIEREN UND SCHLIESSEN

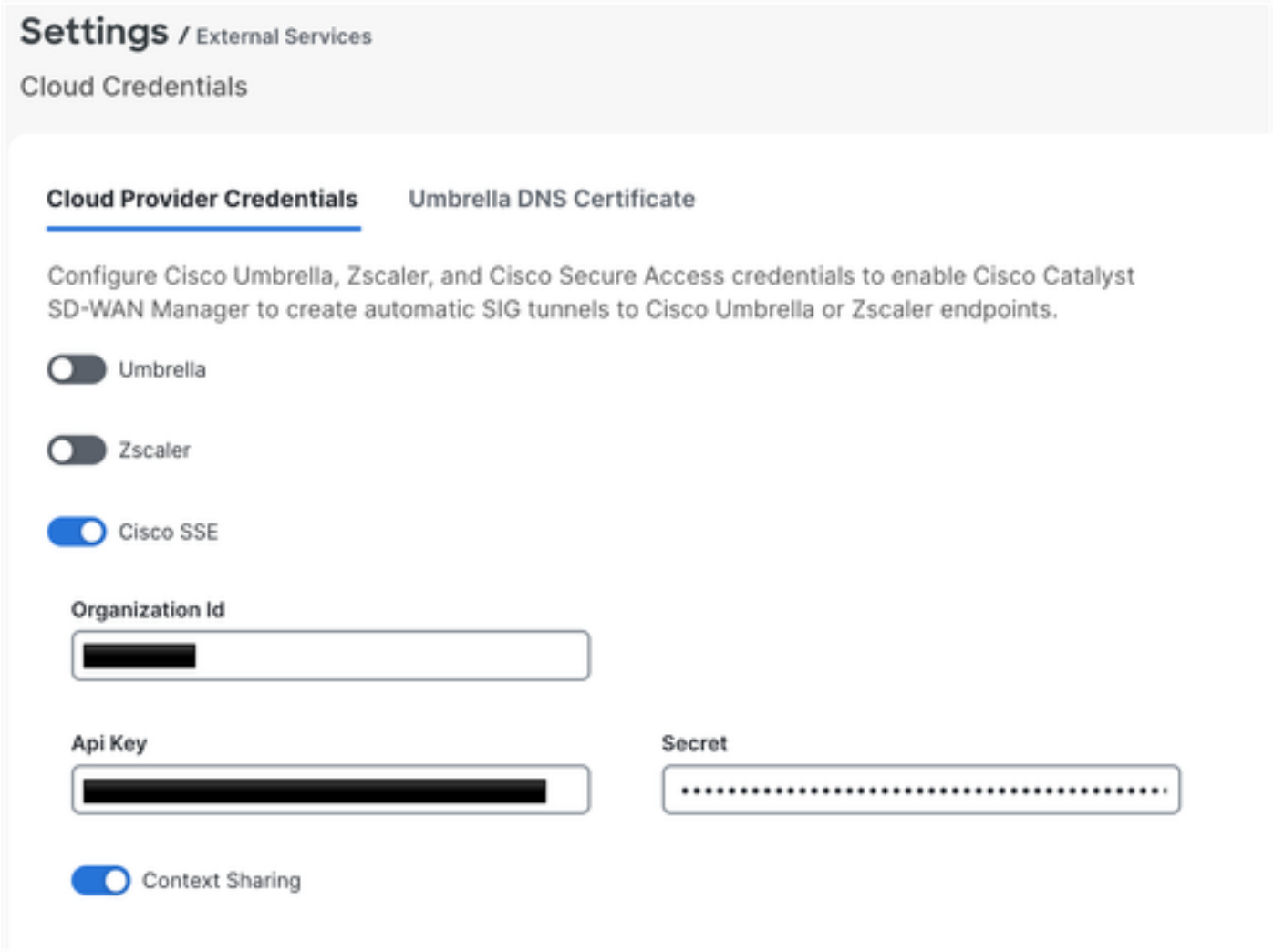


7. Unter der URL https://dashboard.sse.cisco.com/#some-numbers#/admin/apikeys ist die#some-numbers# Ihre Organisations-ID. Kopieren Sie diese Informationen ebenfalls in Ihr Notizbuch.

Konfigurieren von SSE auf Catalyst Manager

Einrichten von Cloud-Anmeldeinformationen

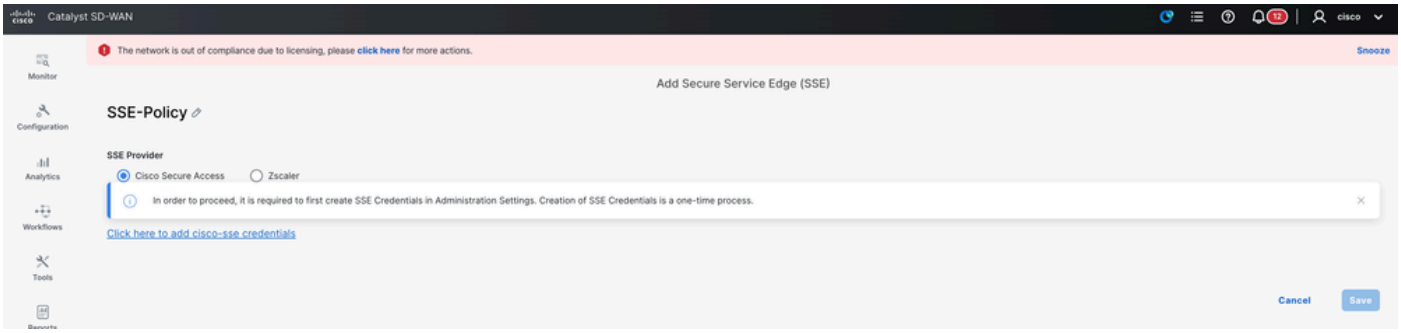
1. Navigieren Sie zu Administration > Settings > Cloud Credentials > Cloud Provider Credentials, und aktivieren Sie die Option "Cisco Secure Access".
und geben Sie die Details ein.



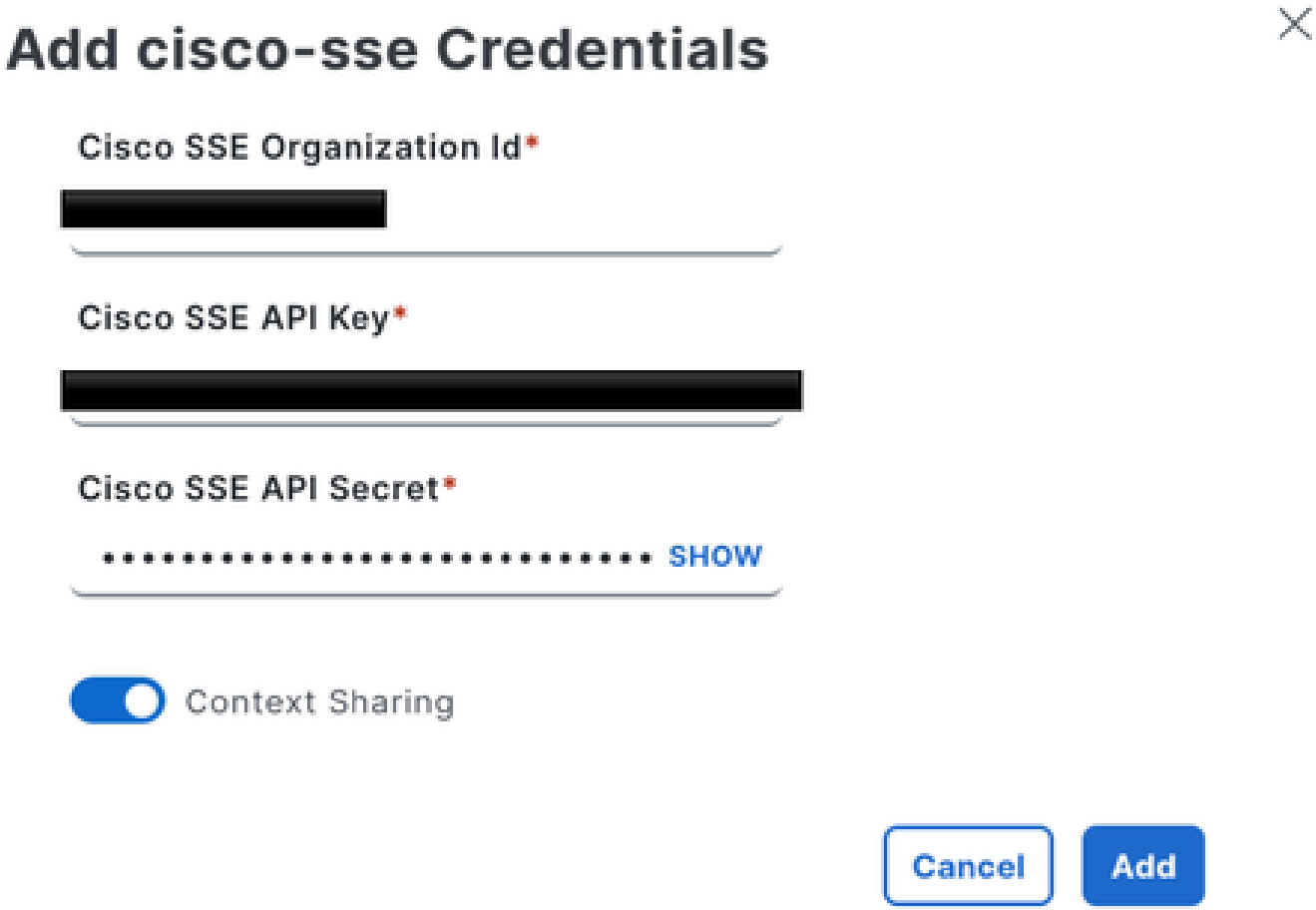
2. Optional: Sie können die gemeinsame Nutzung von Kontext für erweiterte Funktionen aktivieren. Weitere Informationen finden Sie im Cisco SSE-Benutzerhandbuch zur gemeinsamen Nutzung von Kontexten..

Konfigurieren von SSE-Tunneln mithilfe der Richtliniengruppe

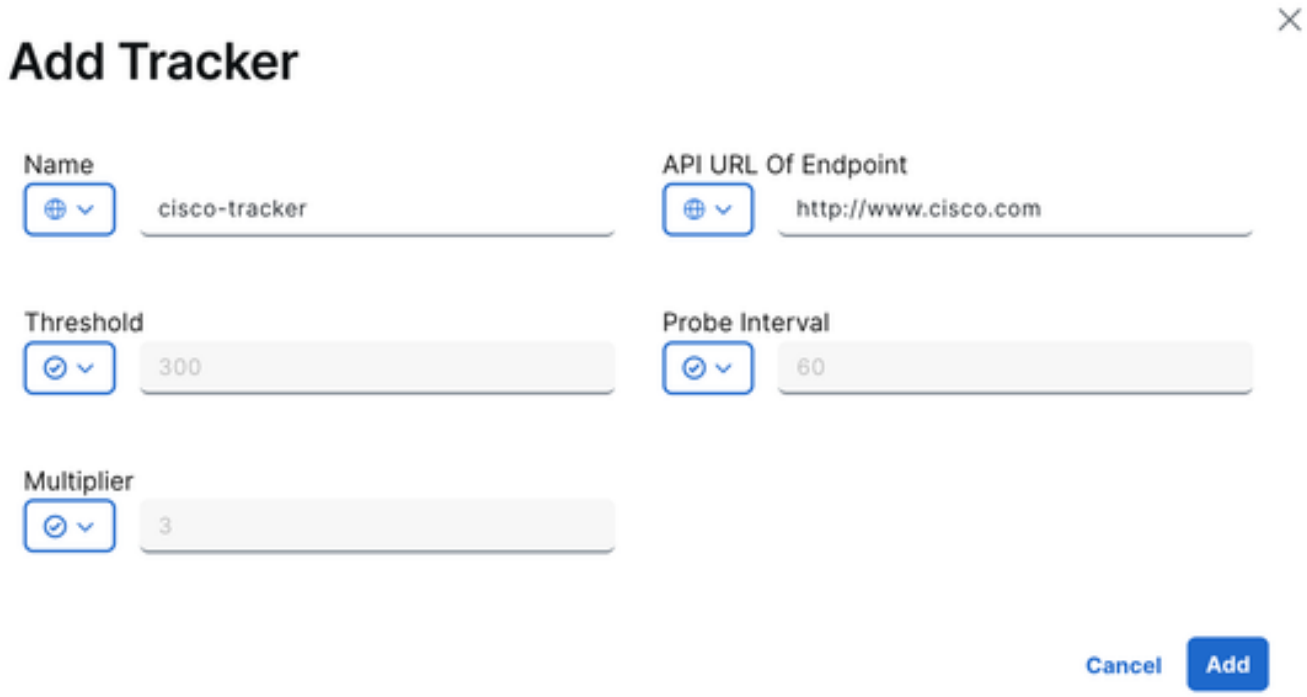
Navigieren Sie im SD-WAN-Manager zu Configuration > Policy Groups > Secure Internet Gateway/Secure Service Edge, und klicken Sie auf Add Secure Service Edge (SSE).

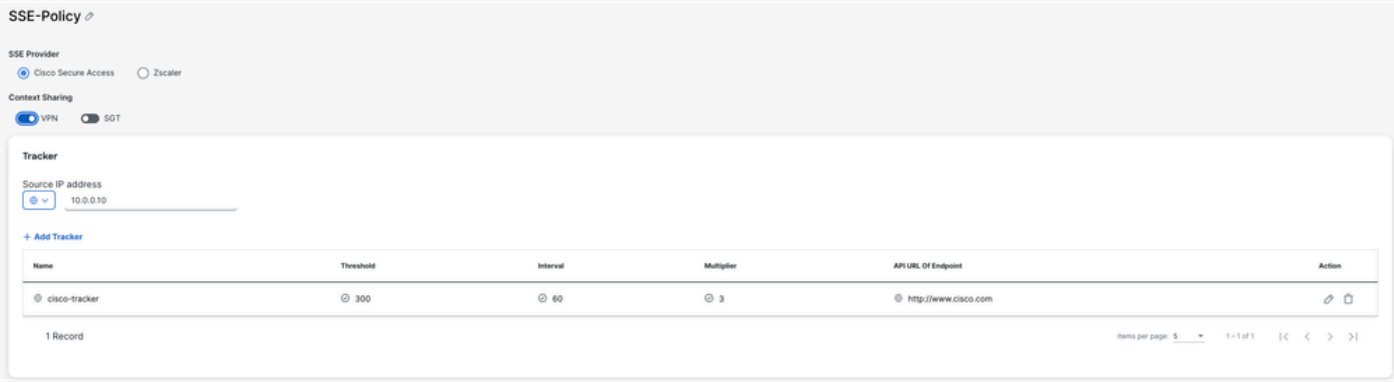


Hinweis: Wenn die Cloud-Anmeldeinformationen noch nicht konfiguriert wurden, können Sie sie in diesem Schritt hinzufügen. Wenn die Anmeldeinformationen bereits konfiguriert wurden, werden sie automatisch geladen.



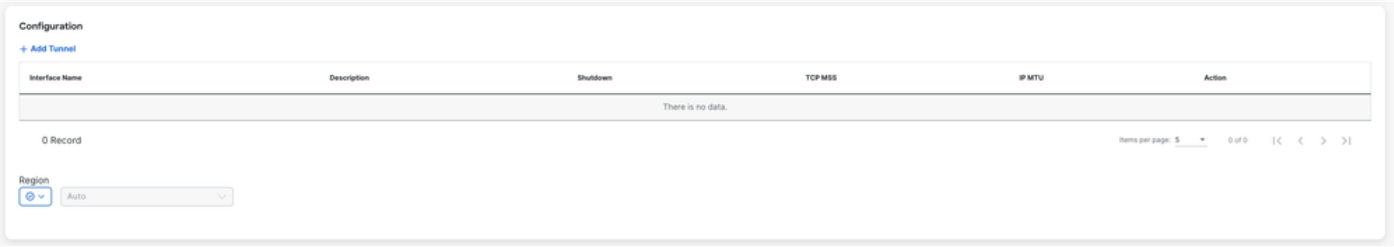
1. Konfigurieren Sie den SSE-Tracker. In diesem Beispiel ist die Tracker-URL auf http://www.cisco.com festgelegt, und die Quell-IP-Adresse wird von einer der Loopback-Schnittstellen zugewiesen.



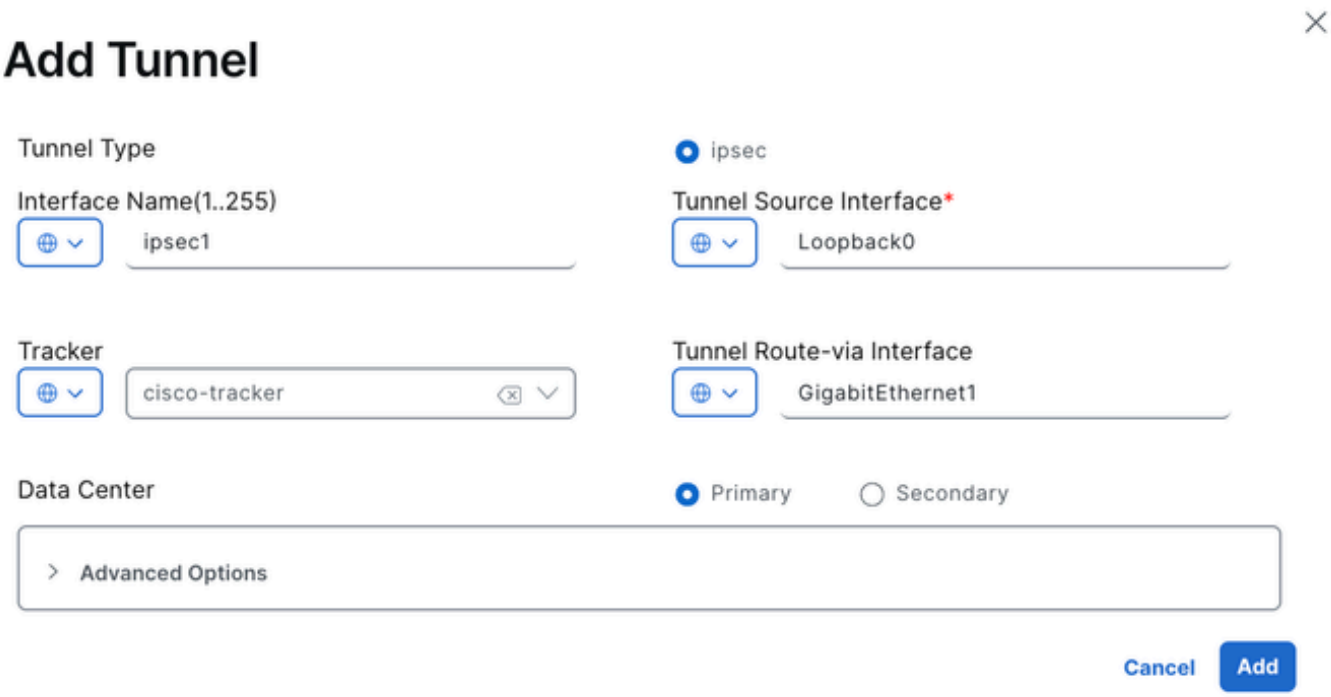


Da die gemeinsame Nutzung von Kontext bei der Konfiguration der Cloud-Anmeldeinformationen aktiviert wurde, ist in diesem Beispiel optional die Option VPN ausgewählt.

2. Klicken Sie auf Tunnel hinzufügen



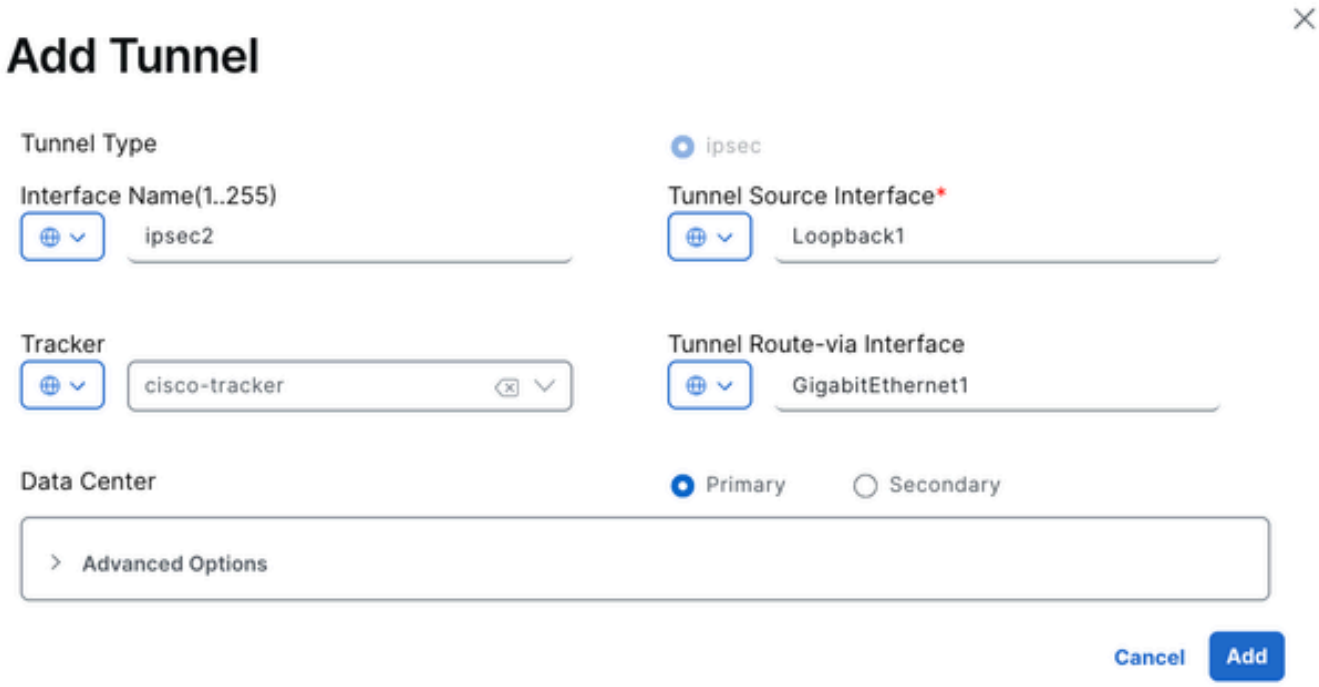
3. In diesem Beispiel wird die Loopback0-Schnittstelle als Tunnelquelle verwendet, während die GigabitEthernet1-Schnittstelle als WAN-Schnittstelle für die Weiterleitung des Datenverkehrs dient.



Da der Tracker in diesem Beispiel konfiguriert wurde, wird die Einstellung in Global geändert und der vorkonfigurierte cisco-tracker ausgewählt.

4. Wiederholen Sie für den zweiten Tunnel dieselben Schritte mit denselben Parametern, ändern

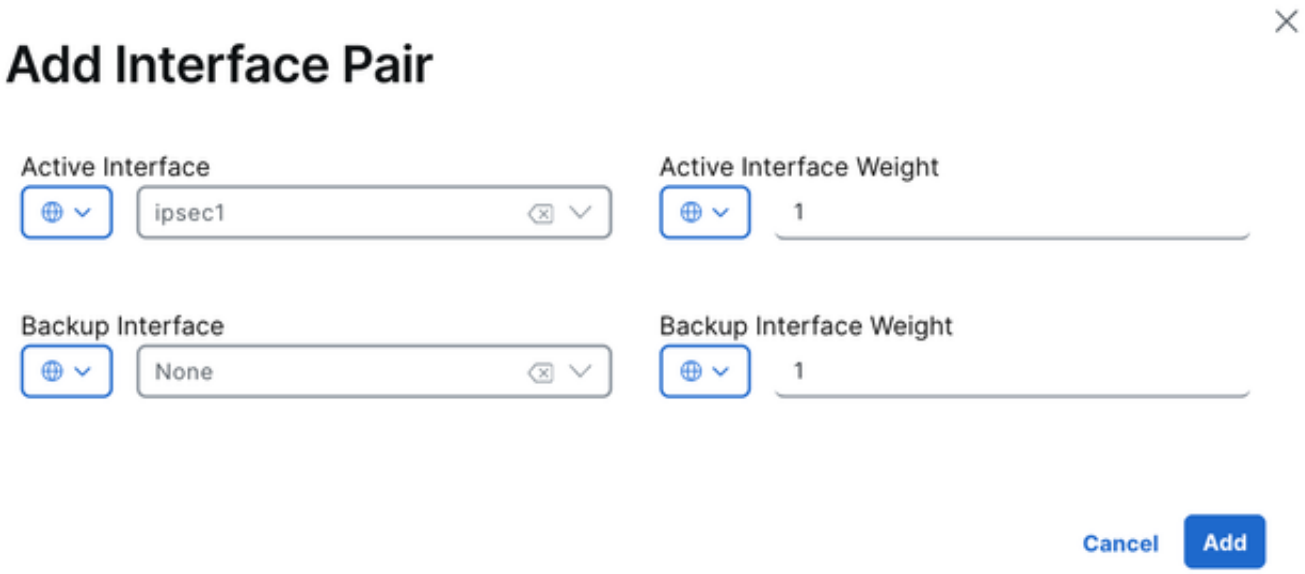
Sie jedoch den Schnittstellennamen von ipsec1 in ipsec2 und den Quellschnittstellennamen in Loopback1.



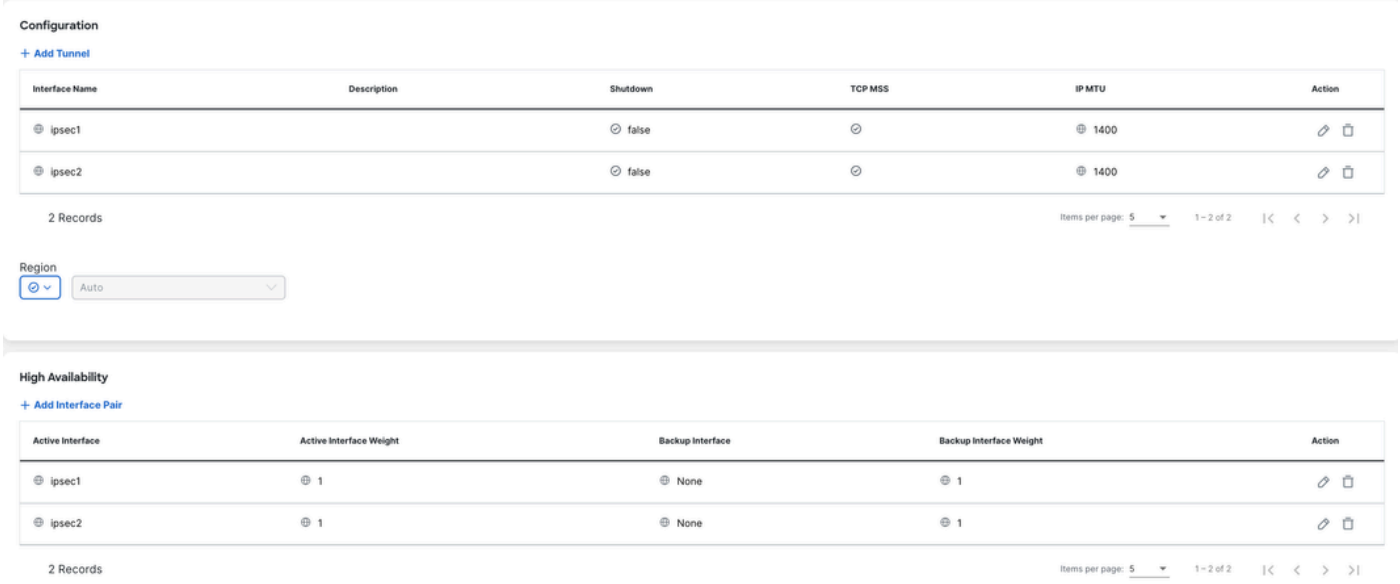
Beide Tunnel sind so konfiguriert, dass sie ohne Sicherung gleichzeitig aktiv sind.

5. Klicken Sie auf Schnittstellenpaar hinzufügen.

6. Klicken Sie auf Hinzufügen. Die aktive Schnittstelle ist auf ipsec1 festgelegt, und es wird keine Backup-Schnittstelle angegeben.



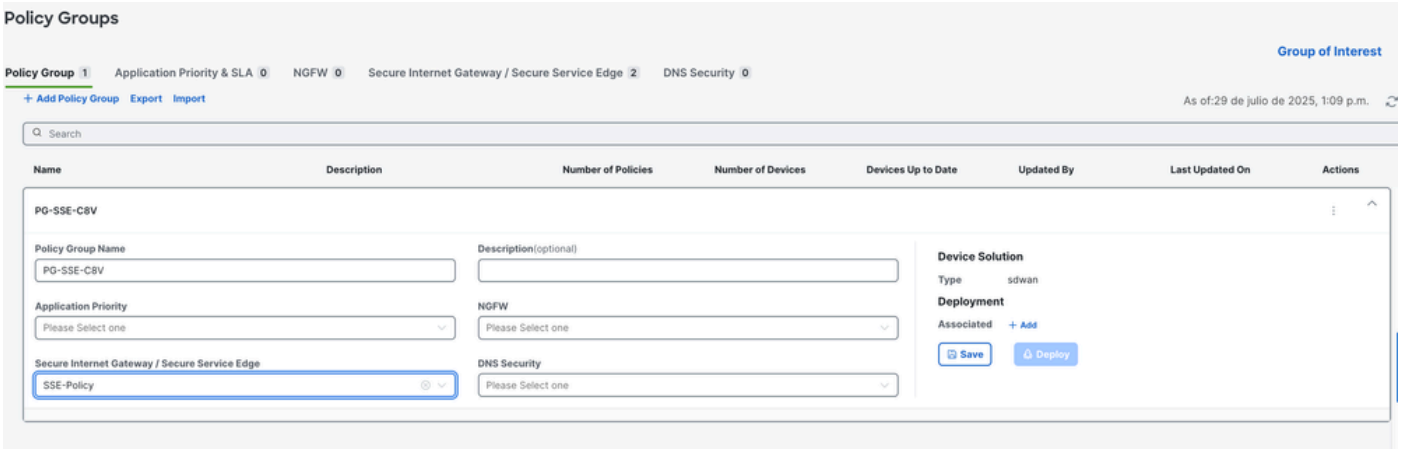
7. Der gleiche Vorgang wird für den zweiten Tunnel ipsec2 wiederholt.



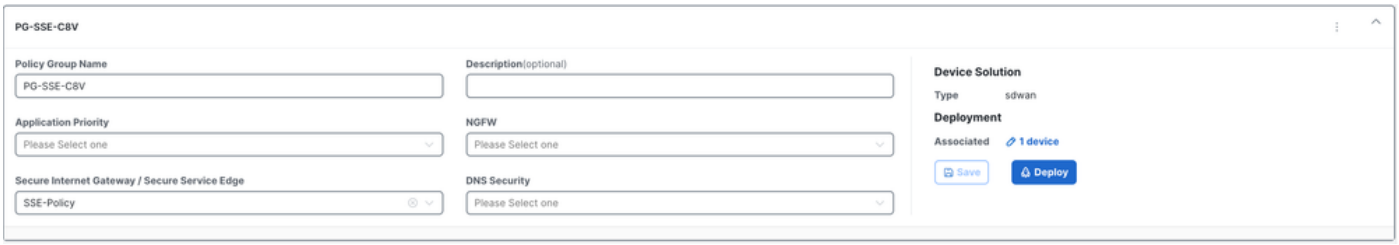
8. Speichern Sie die Konfiguration.

Konfigurieren der Richtliniengruppe

1. Sie können die zuvor in der Richtliniengruppe erstellte Richtlinie auswählen und speichern.



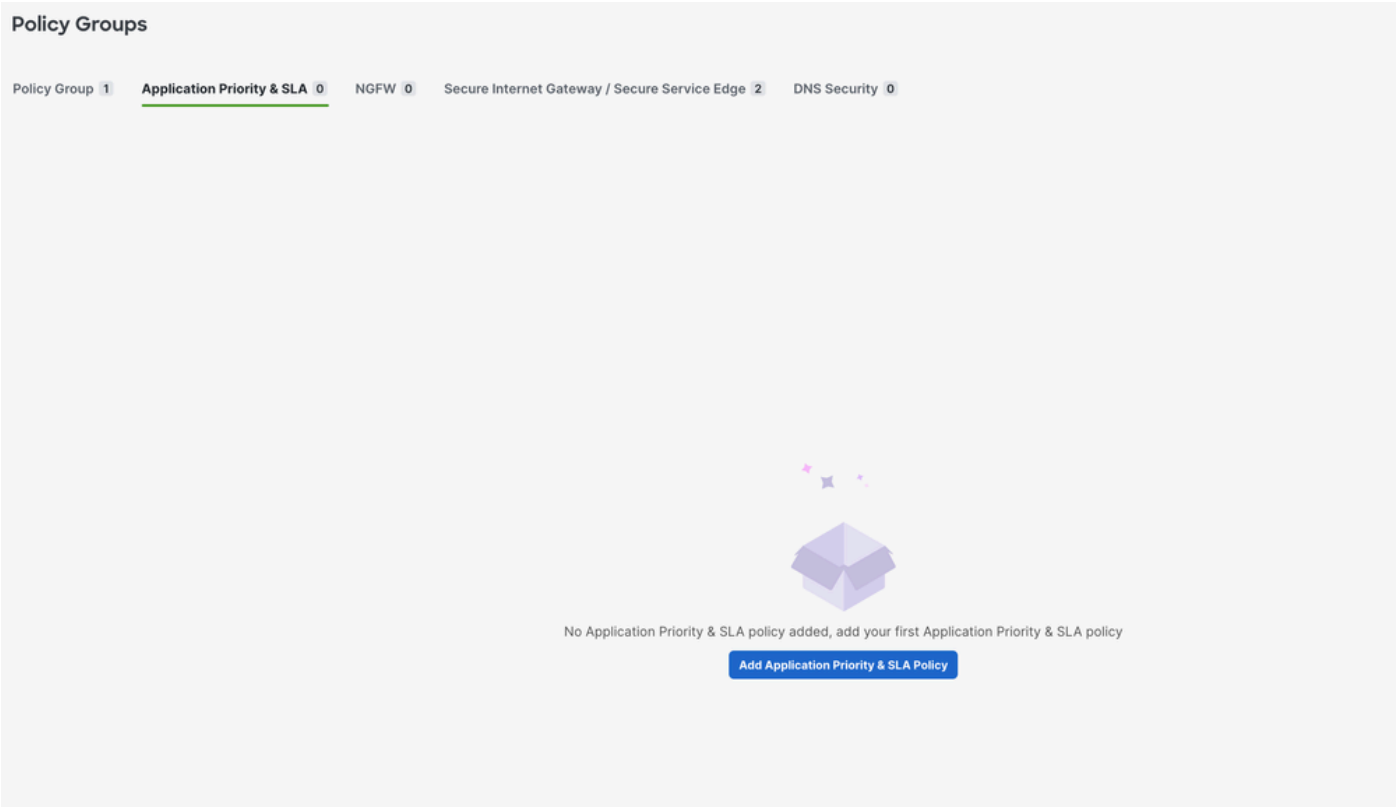
2. Sobald das Gerät bzw. die Geräte der Richtliniengruppe zugeordnet wurden, fahren Sie mit der Bereitstellung der Richtliniengruppe fort.



Konfigurieren einer Richtliniengruppe zum Umleiten von Datenverkehr an SSE

1. Navigieren Sie im SD-WAN-Manager zu Configuration > Policy Groups > Application Priority & SLA.

- Wählen Sie Anwendungspriorität und SLA-Richtlinie hinzufügen aus.
- Geben Sie einen Namen für die Richtlinie an.

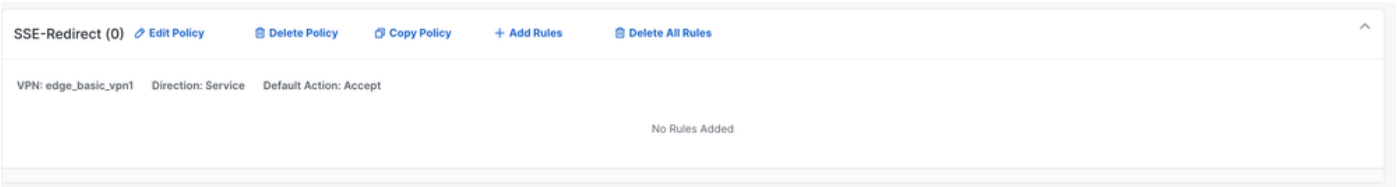


2. Wenn die neue Richtlinie angezeigt wird, wählen Sie den Umschalter Erweitertes Layout.

3. Wählen Sie Datenverkehrsrichtlinienliste hinzufügen aus.

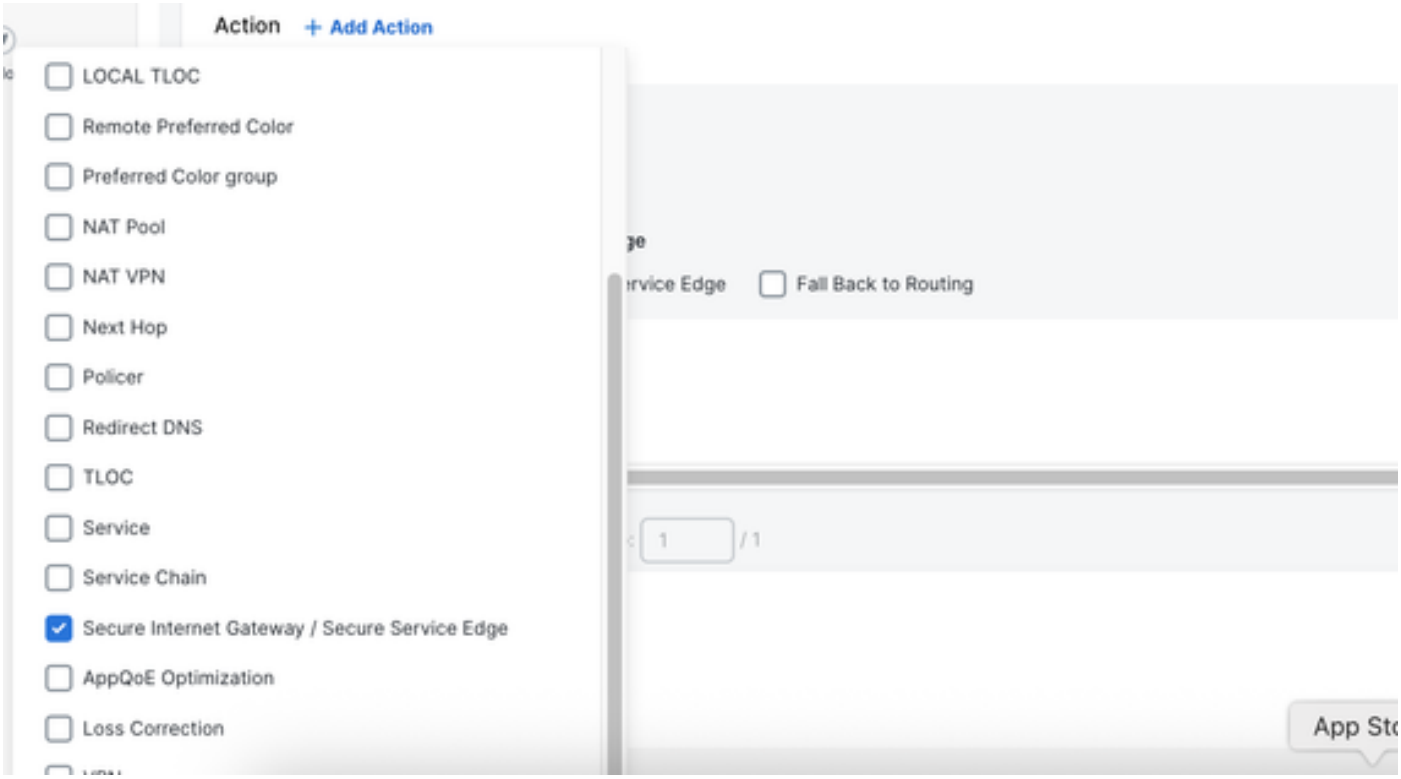
- Konfigurieren der VPNs zum Umleiten des Datenverkehrs an den SSE-Tunnel
- Legen Sie die Richtung und die Standardaktion nach Bedarf fest, und speichern Sie.

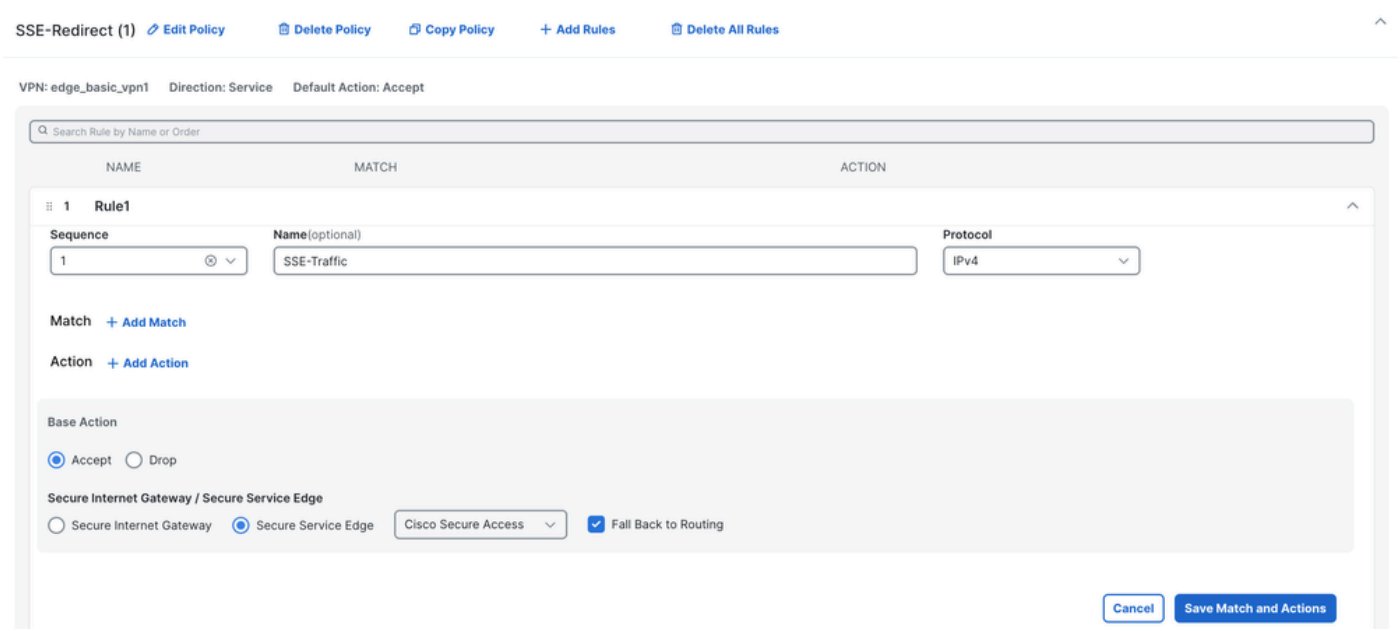
4. Wählen Sie + Regel hinzufügen.



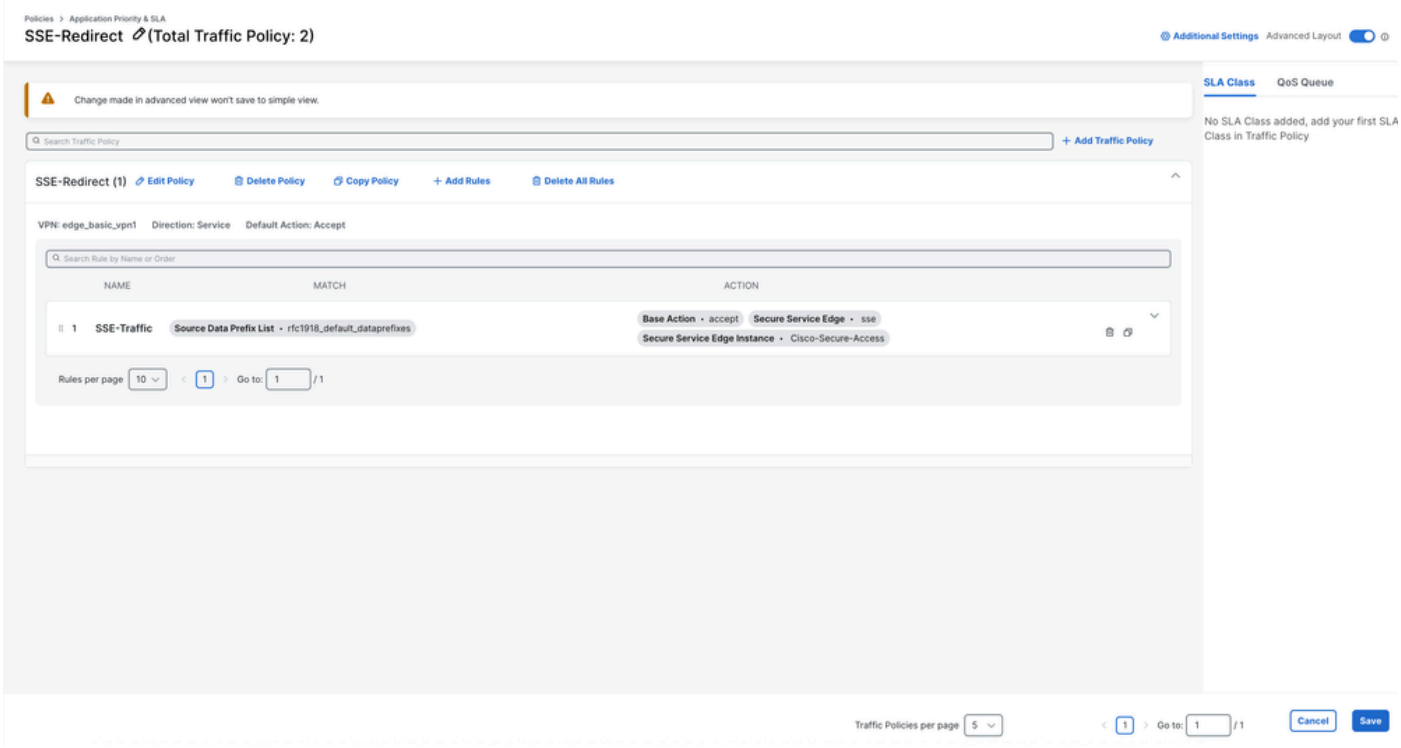
5. Konfigurieren Sie die Kriterien für den abgeglichenen Datenverkehr, um den Datenverkehr an den SSE umzuleiten.
6. Wählen Sie Akzeptieren als Basisaktion und klicken Sie dann auf + Aktion.

7. Suchen Sie nach der Aktion Sicheres Internet-Gateway/Sicherer Service-Edge, und setzen Sie sie auf Sicherer Service-Edge.



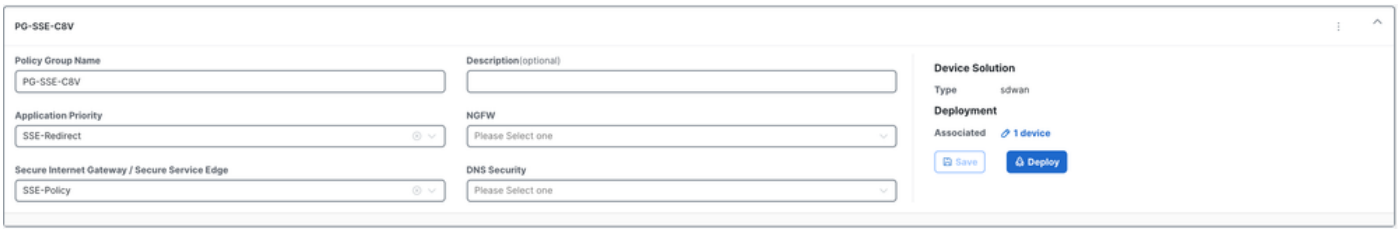


8. Klicken Sie auf Spiel und Aktionen speichern



9. Klicken Sie auf Speichern.

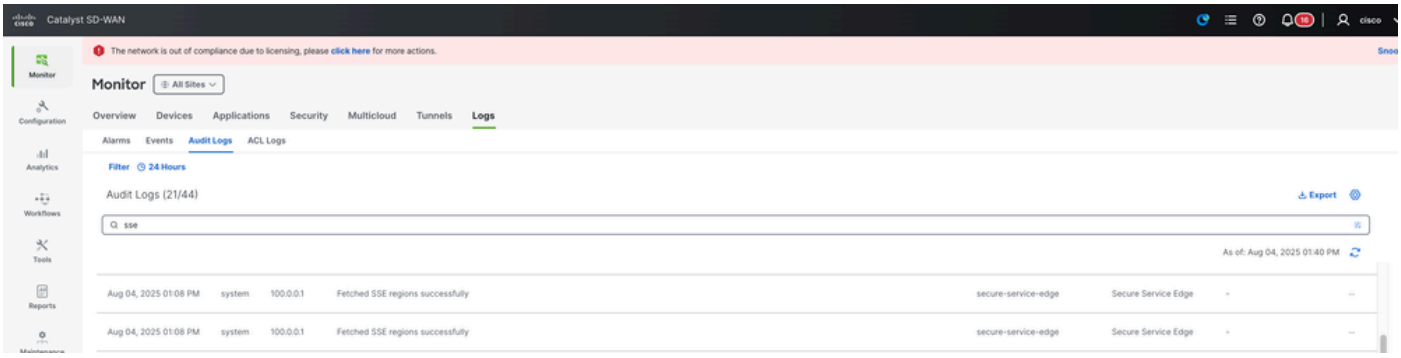
10. Navigieren Sie zu Konfiguration > Richtliniengruppen, und wählen Sie die soeben erstellte Richtlinie Anwendungspriorität aus. Speichern und dann bereitstellen.



Überprüfung

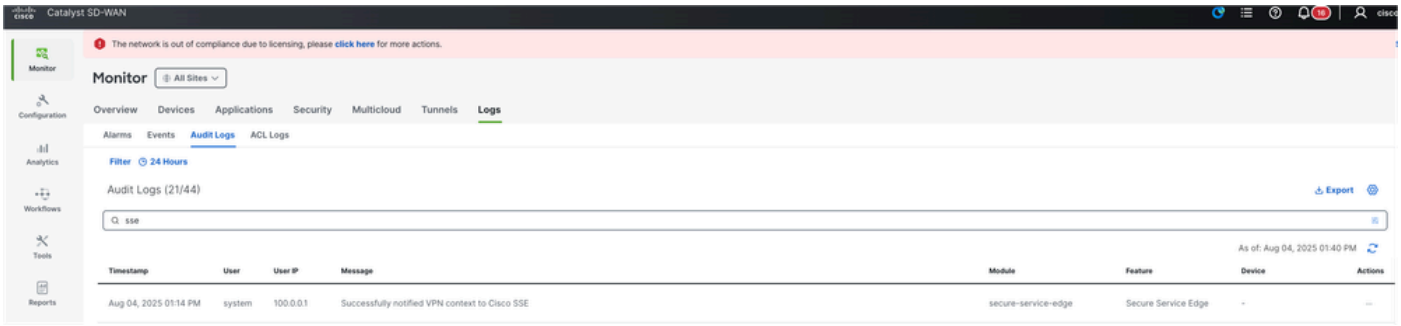
Manager

1. Überwachen > Protokolle > Überwachungsprotokolle und Suchen nach "sse".



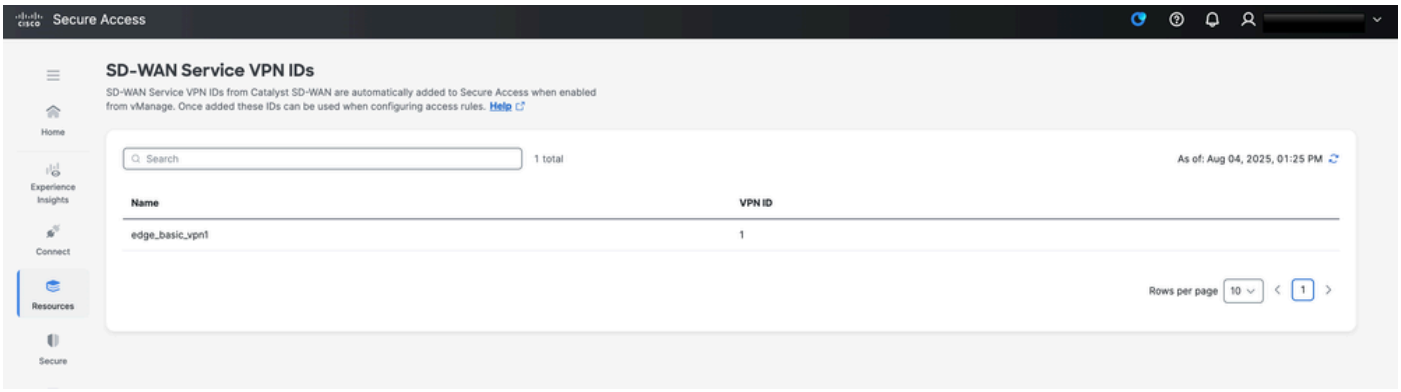
2. Sie können überprüfen, ob das VPN für die gemeinsame Nutzung von Kontext erfolgreich

aktiviert wurde, indem Sie den Manager überprüfen.



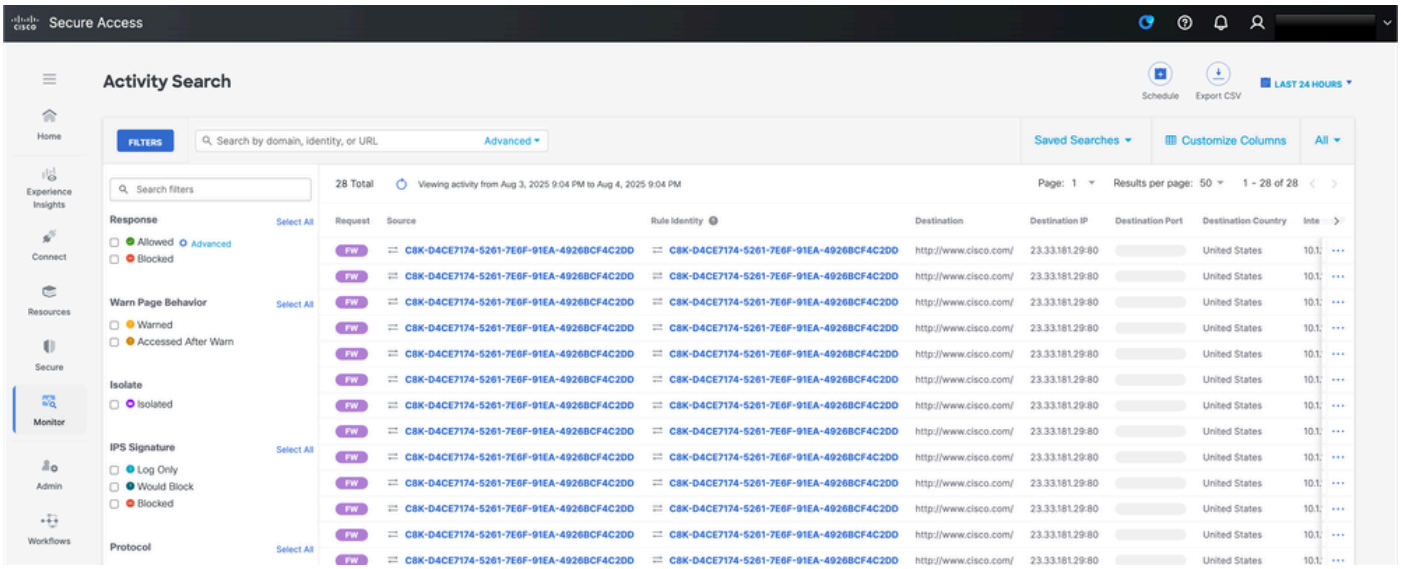
Dashboard für sicheren Zugriff

Kontextfreigabe
Sie können überprüfen, ob das Context-Sharing-VPN erfolgreich aktiviert wurde, indem Sie das SSE-Dashboard überprüfen.Ressourcen > SD-WAN Service-VPN-IDs



Tunnel nach oben

Wenn der Tunnel geöffnet ist und der Tracker betriebsbereit ist und Datenverkehr durch den Tunnel fließt, können Sie dies überprüfen, indem Sie zu Monitor > Activity Search (Überwachung > Aktivitätssuche) navigieren. Auf diesem Bildschirm sehen Sie den Datenverkehr, der durch den Tunnel fließt, z. B. Anfragen an www.cisco.com, die vom Tracker generiert werden. Diese Transparenz bestätigt, dass der Tracker aktiv ist, und überwacht aktiv den Datenverkehr durch den Tunnel.



Kommandozeilenschnittstellenbefehle (CLI)

<#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
```

Zugehörige Informationen

- Konfigurieren der Kontextfreigabe SD-WAN
- Cisco Secure Access-Integration mit SD-Routing
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.