Beveiligde toegang (SSE) configureren en oplossen op Catalyst SD-WAN

Inhoud

Inleiding

In dit document wordt beschreven hoe u de actief-actieve SSE-integratie op Catalyst SD-WAN configureert en hoe u het probleem kunt oplossen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Software-defined Wide Area Network (SD-WAN)
- Configuratiegroepen
- Beleidsgroepen

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- C8000V versie 17.15.02
- vManage versie 20.15.02

- Cisco Secure Access-account

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Cisco Secure Access

Cisco Secure Access is een cloudgebaseerde Security Service Edge (SSE)-oplossing die meerdere netwerkbeveiligingsservices convergeert en vanuit de cloud levert om een hybride personeelsbestand te ondersteunen. Cisco SD-WAN Manager maakt gebruik van REST API's om beleidsinformatie van Cisco Secure Access op te halen en verspreidt deze informatie naar Cisco IOS XE SD-WAN-apparaten. Deze integratie maakt naadloze, transparante en veilige Direct Internet Access (DIA) voor gebruikers mogelijk, zodat ze vanaf elk apparaat, overal en veilig verbinding kunnen maken.

Met Cisco SSE kunnen SD-WAN-apparaten verbindingen tot stand brengen met SSE-providers met behulp van IPSec-tunnels. Dit document is bedoeld voor gebruikers van Cisco Secure Access.

Voorlopige configuraties

- Domain Lookup voor het apparaat inschakelen: Navigeer naar Configuratiegroepen > Systeemprofiel > Globaal en schakel Domain Lookup in.

Opmerking: het opzoeken van domeinen is standaard uitgeschakeld.

- Configureer DNS: De router kan DNS oplossen en toegang krijgen tot internet via VPN 0.
- NAT DIA configureren: De DIA-configuratie moet aanwezig zijn op de router waar de SSE-tunnel is gemaakt.

Loopback-interfaces maken

Als beide tunnels in een Active/Active-configuratie verbinding maken met hetzelfde bestemmingsdatacenter en dezelfde WAN-interface gebruiken als de bron, moeten twee loopback-IP-adressen worden gemaakt.

Opmerking: Wanneer twee tunnels zijn geconfigureerd met dezelfde bron en bestemming, vormt IKEv2 een identiteitspaar dat bestaat uit een lokale ID en een externe ID. Standaard is de lokale ID het IP-adres van de broninterface van de tunnel. Dit identiteitspaar moet uniek

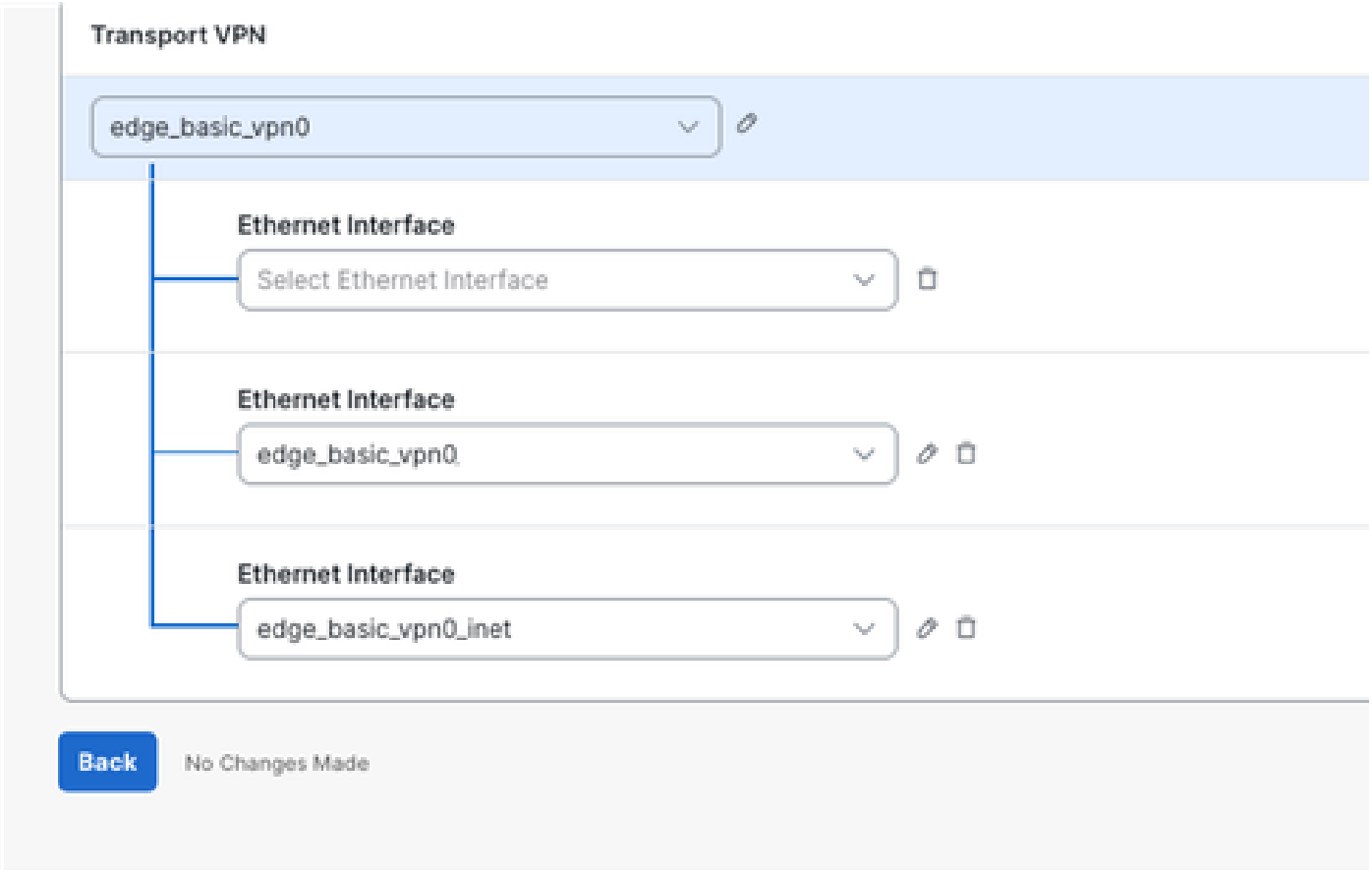
---

zijn en mag niet tussen twee tunnels worden gedeeld. Om verwarring binnen de IKEv2-status te voorkomen, gebruikt elke tunnel een andere loopback-interface als bron. Hoewel IKE-pakketten worden vertaald (NATed) op de DIA-interface, blijft de lokale ID ongewijzigd en behoudt het oorspronkelijke loopback-IP-adres.

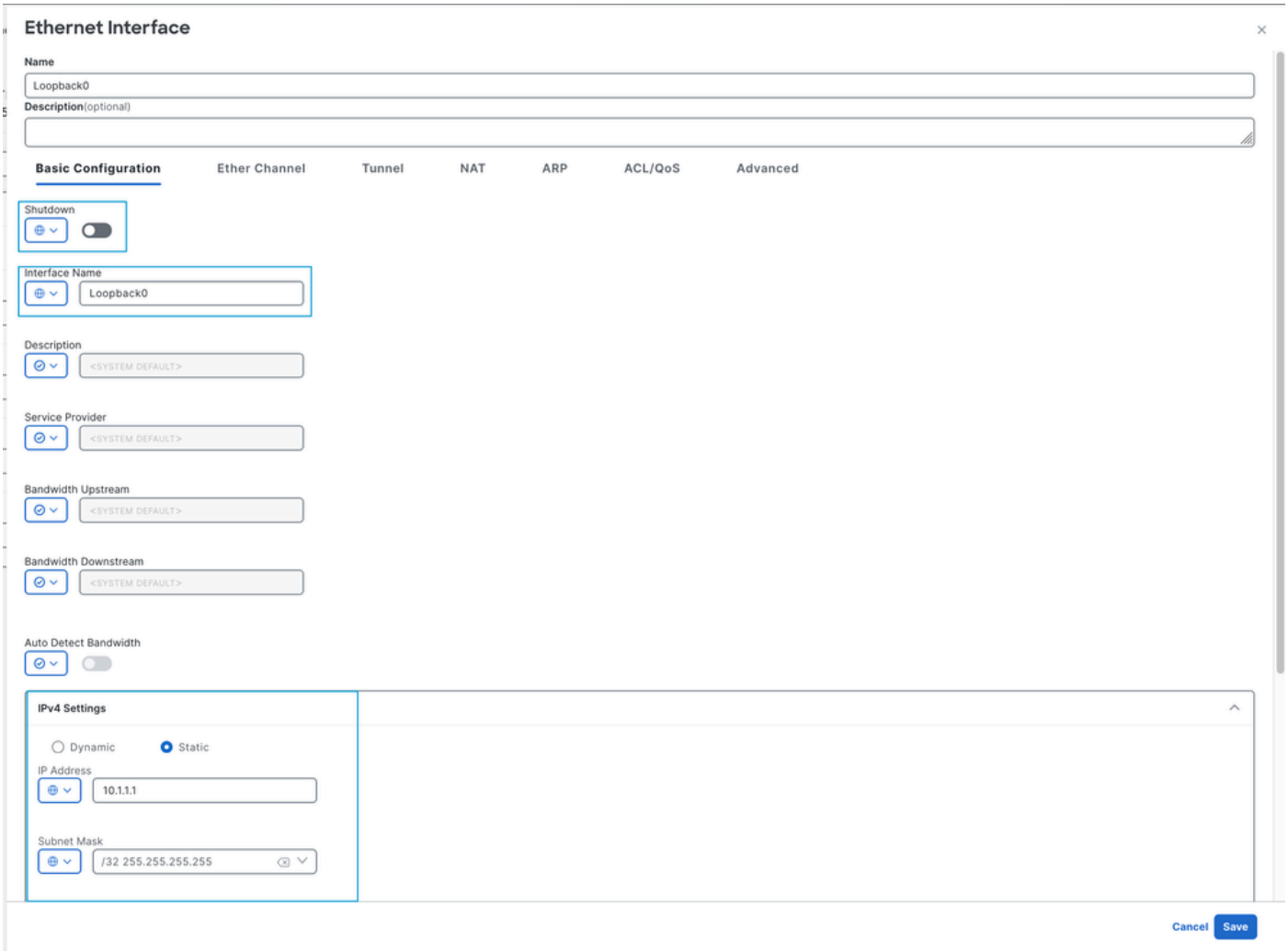
1. Navigeer naar Configuratie > Configuratiegroepen > Configuratiegroepnaam> Transport- en beheerprofiel > klik op Bewerken.

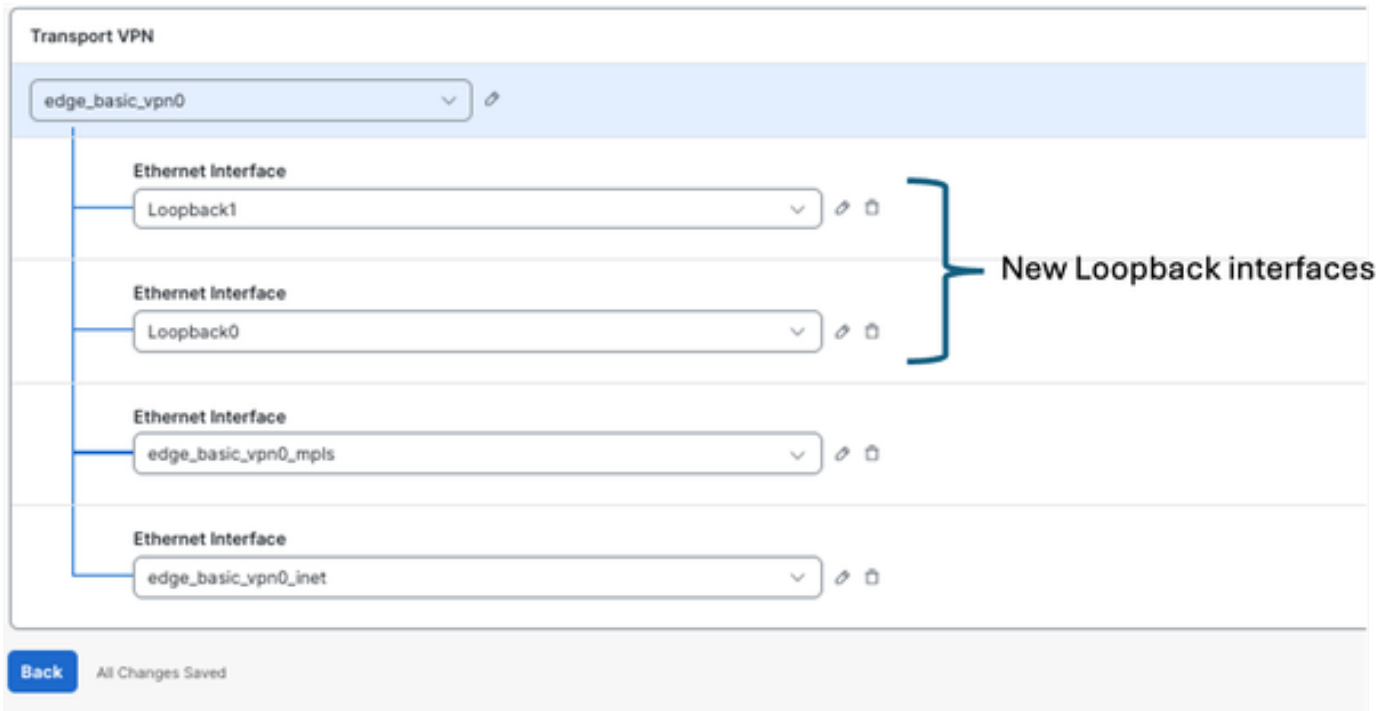
2. Klik op het plusteken (+) aan de rechterkant van het transport VPN-profiel (hoofdprofiel). Dit opent een menu Add Feature (Extra functies) helemaal rechts.

3. Klik op Ethernet-interface. Het voegt een nieuwe internetinterface toe onder Transport VPN.



4. Maak de twee Loopback-interfaces met behulp van RFC1918 IPv4-adressen, zoals het Loopback0-voorbeeld in de afbeelding.



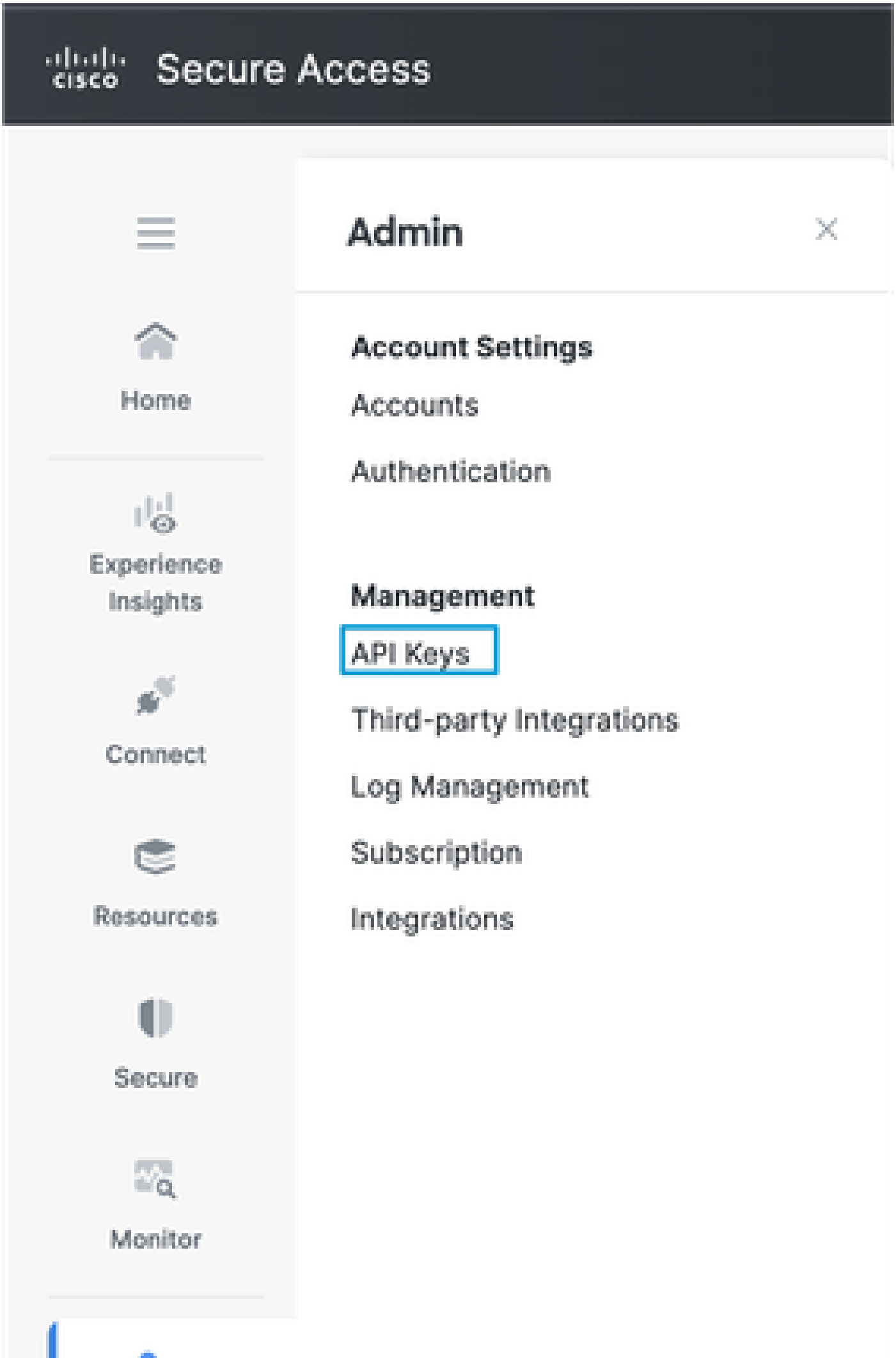


5. Nadat u de loopbackconfiguratie hebt toegepast, gaat u verder met het implementeren van de configuratiewijziging op het apparaat. De status van de voorziening verandert van 1/1 naar 0/1.

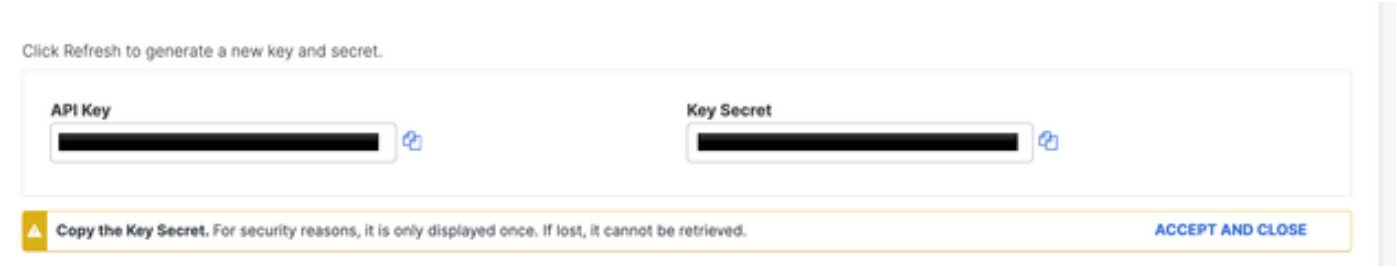
Name	Type	Profile	Provisioning Status In Sync Devices / Associated Devices	Origin	Updated By
Hub2-SIG	Single Router	4	▲ 0 / 1	user	cisco

Nieuwe API-sleutels configureren op SSE Portal

1. Toegang tot het SSE Portal https://login.sse.cisco.com/
2. Navigeer naar Beheer > API-sleutels


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. Kopieer de API-sleutel en Key Secret in een notitieblok en selecteer ACCEPTEREN EN SLUITEN

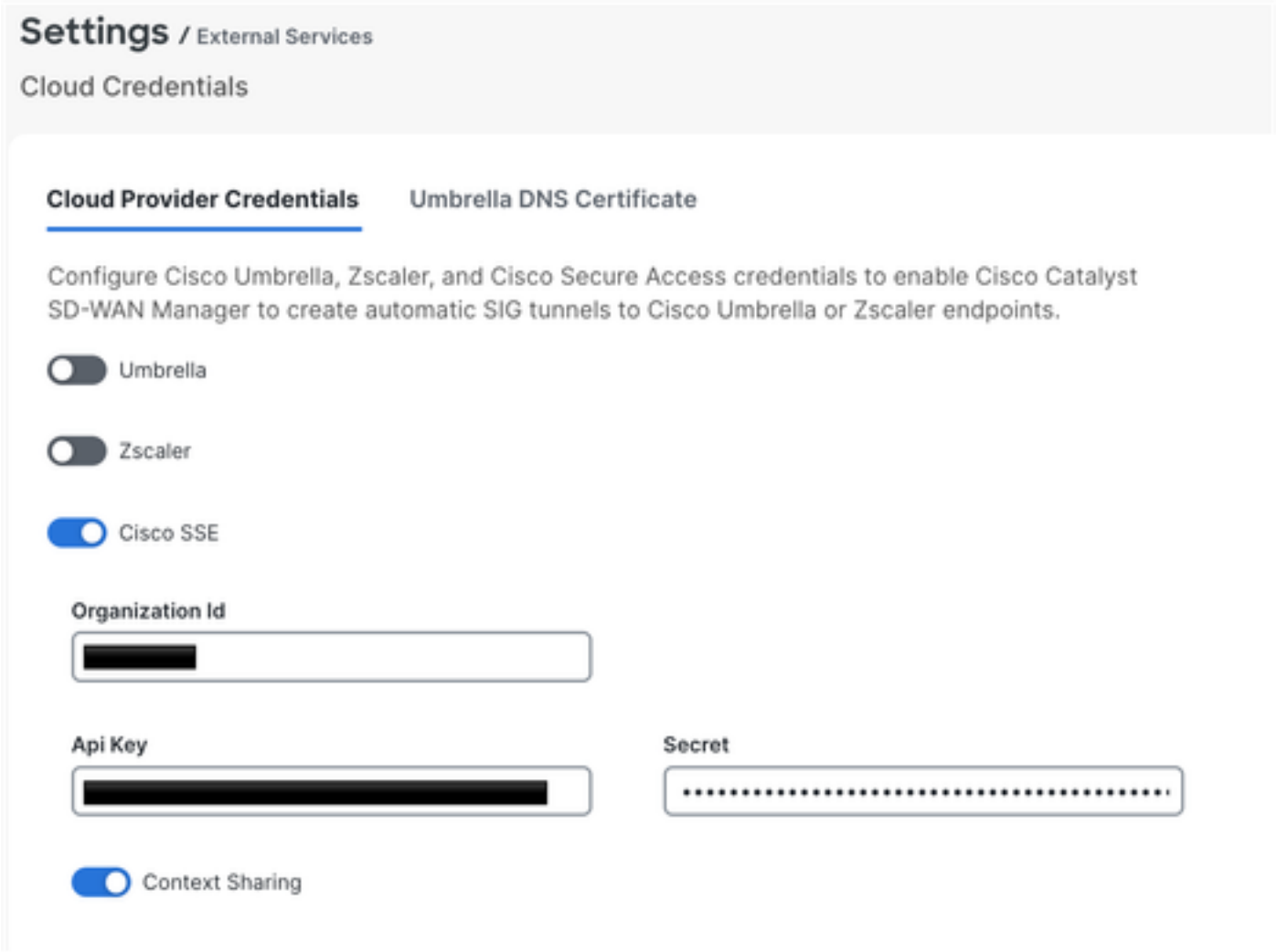


7. Onder de URL https://dashboard.sse.cisco.com/#some-numbers#/admin/apikeys is de #some-numbers# uw organisatie-ID. Kopieer die informatie ook naar uw notitieblok.

SSE configureren in Catalyst Manager

Cloudreferenties instellen

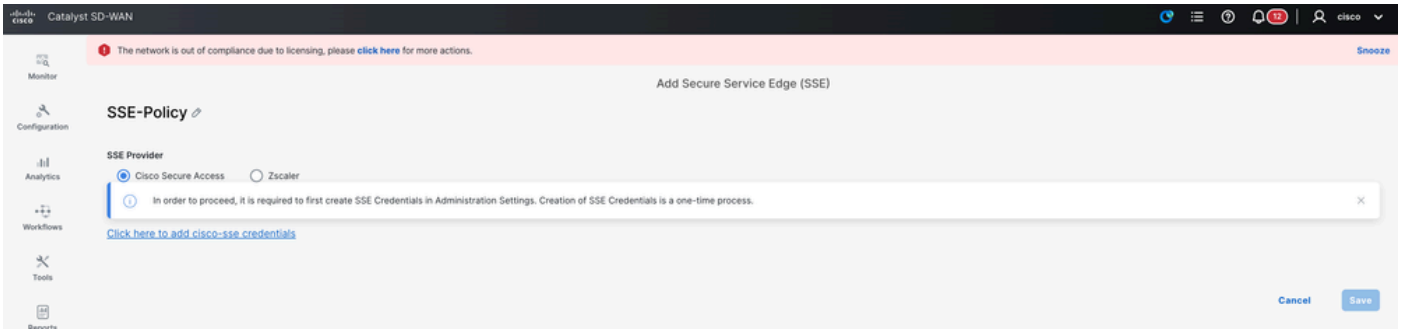
1. Navigeer naar Beheer > Instellingen > Cloudreferenties > Cloudproviderreferenties en schakel Cisco Secure Access in
en voer de details in.



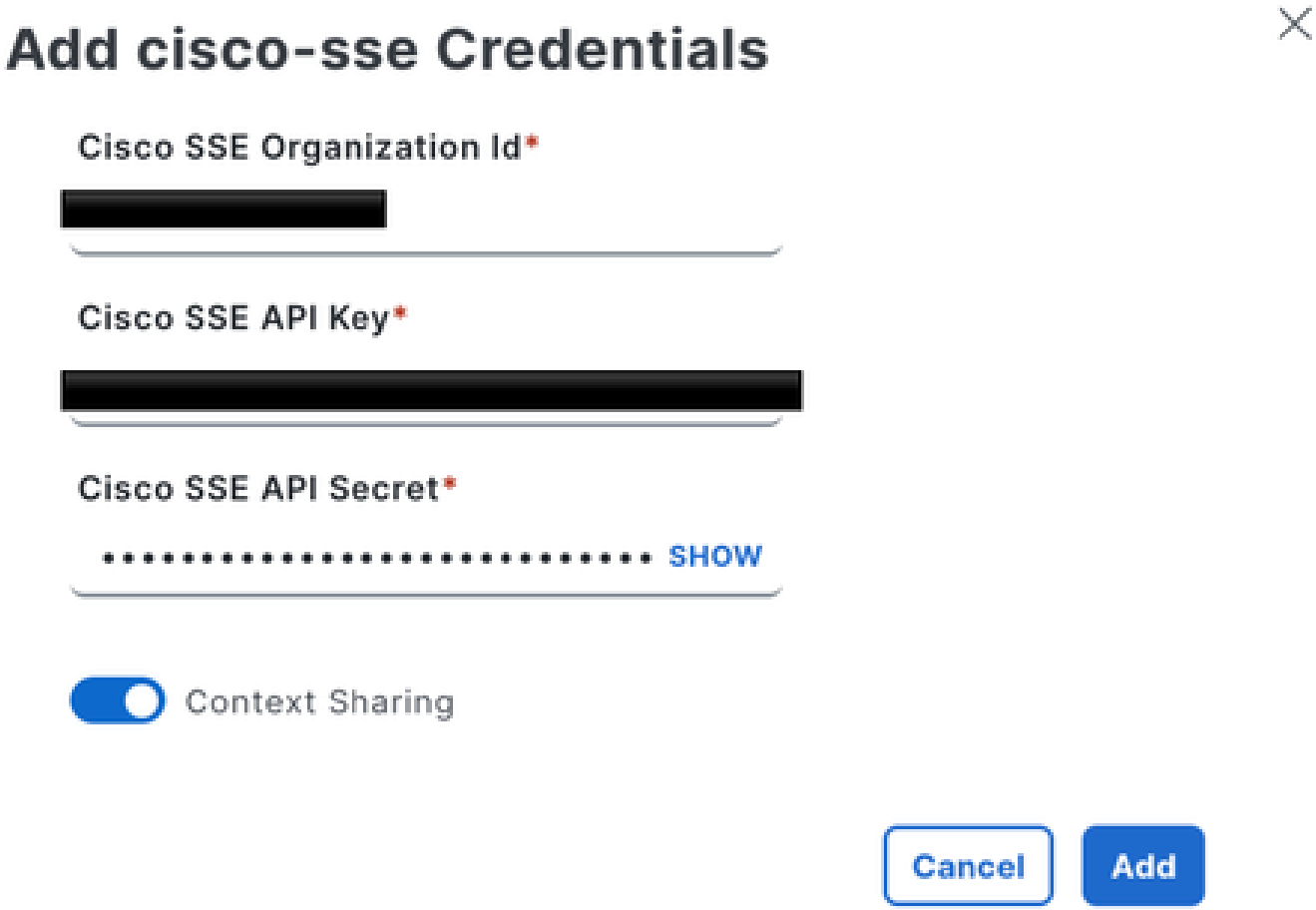
2. Optioneel: u kunt het delen van context inschakelen voor verbeterde functionaliteit. Raadpleeg de Cisco SSE-gebruikershandleiding voor meer informatie over het delen van context.

SSE-tunnels configureren met behulp van Beleidsgroep

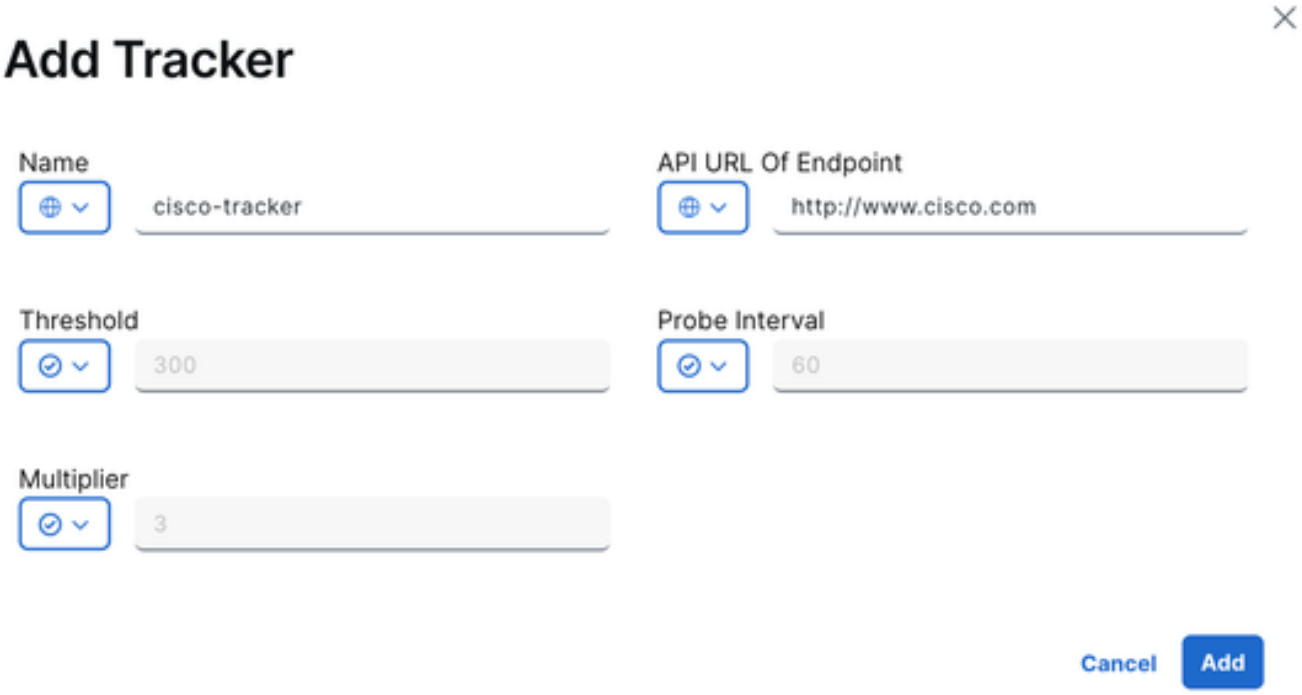
Navigeer in SD-WAN Manager naar Configuratie > Beleidsgroepen > Secure Internet Gateway/Secure Service Edge en klik op Secure Service Edge (SSE).

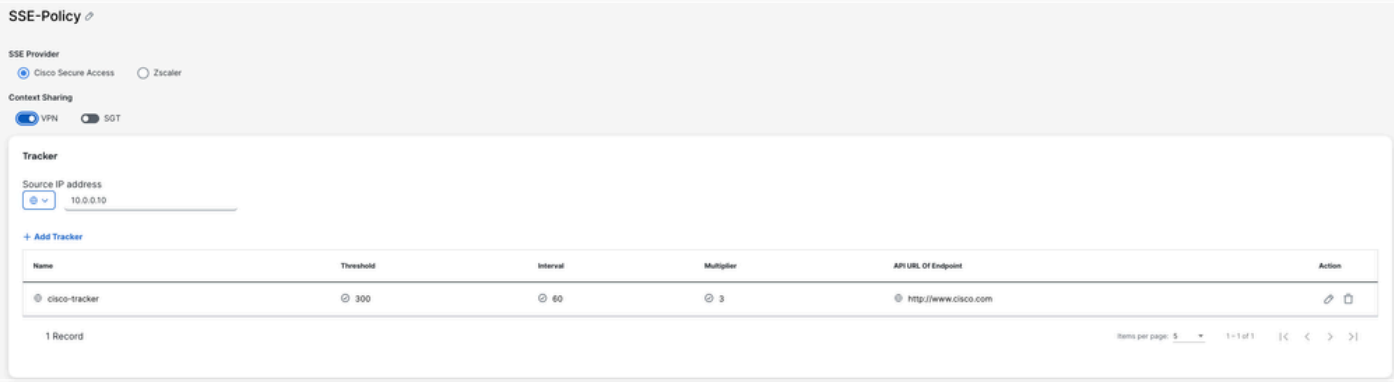


Opmerking: Als cloudreferenties nog niet zijn geconfigureerd, kunt u deze in deze stap toevoegen. Als de referenties al zijn geconfigureerd, worden ze automatisch geladen.



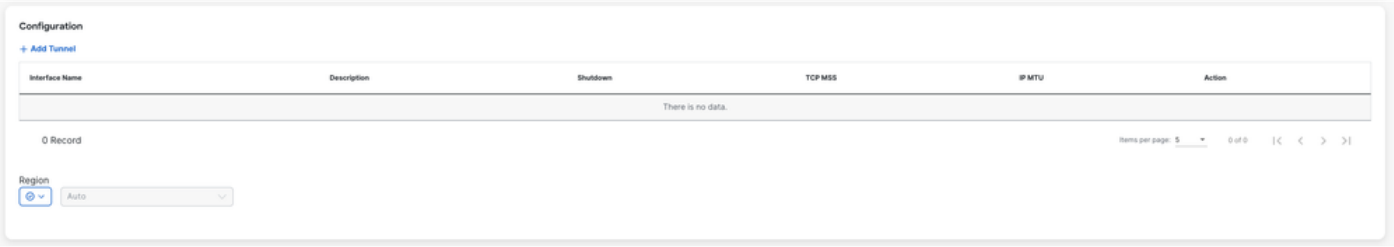
1. Configureer de SSE Tracker. In dit voorbeeld wordt de tracker-URL ingesteld op http://www.cisco.com en wordt het IP-adres van de bron toegewezen via een van de loopback-interfaces.



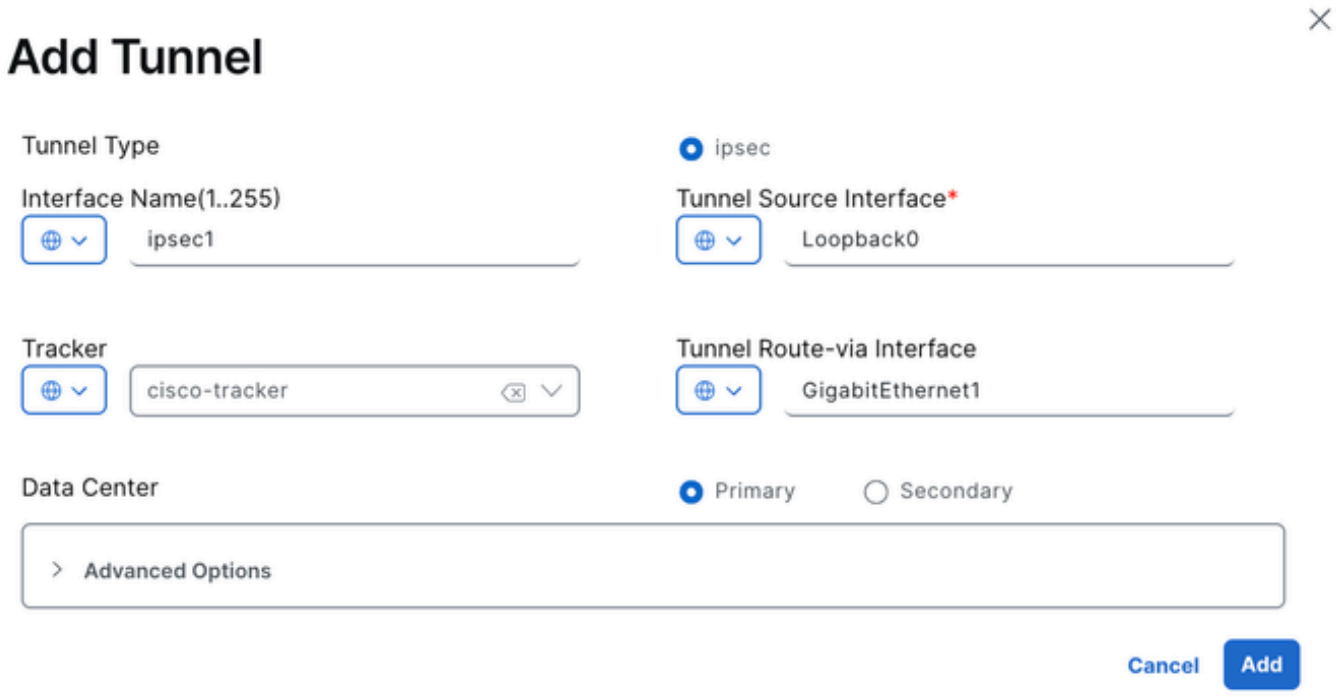


Aangezien het delen van context is ingeschakeld toen de cloudreferenties werden geconfigureerd, wordt VPN in dit voorbeeld optioneel als optie geselecteerd.

2. Klik op Tunnel toevoegen

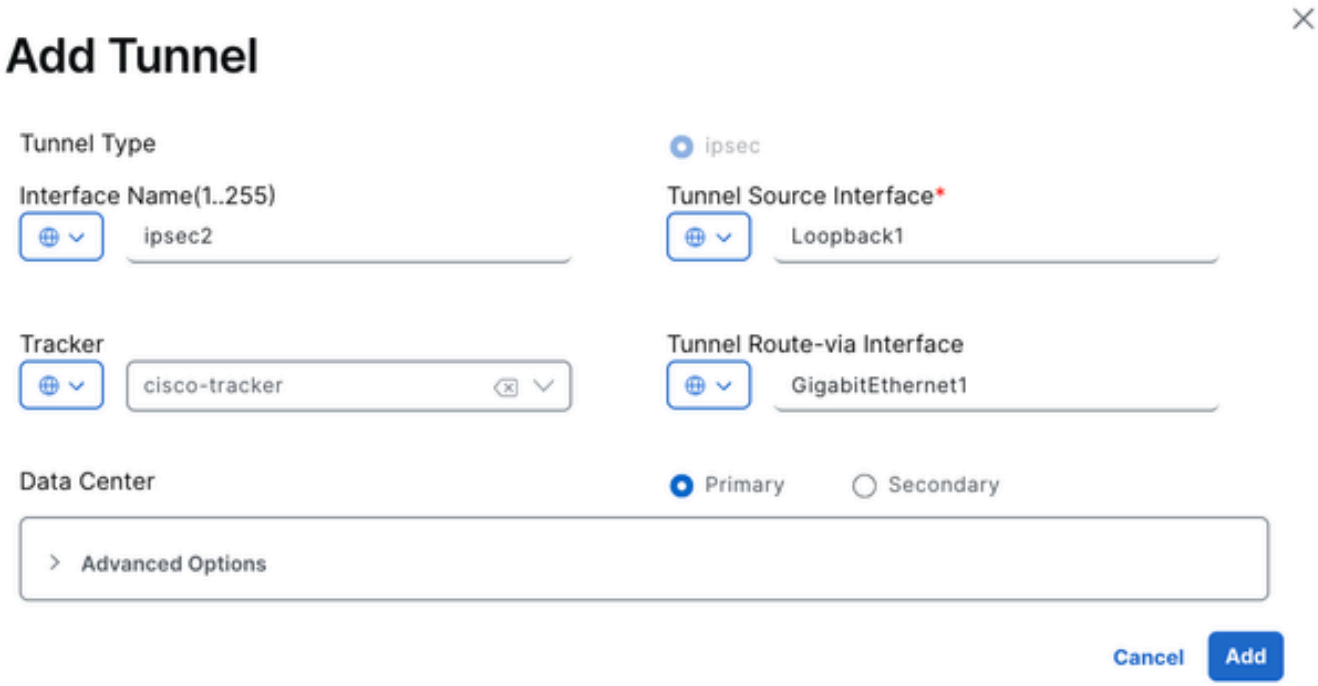


3. In dit voorbeeld wordt de Loopback0-interface gebruikt als tunnelbron, terwijl de GigabitEthernet1-interface dient als de WAN-interface om verkeer te routeren.



Aangezien de tracker in dit voorbeeld is geconfigureerd, wordt de instelling gewijzigd in Globaal en wordt de vooraf geconfigureerde cisco-tracker geselecteerd.

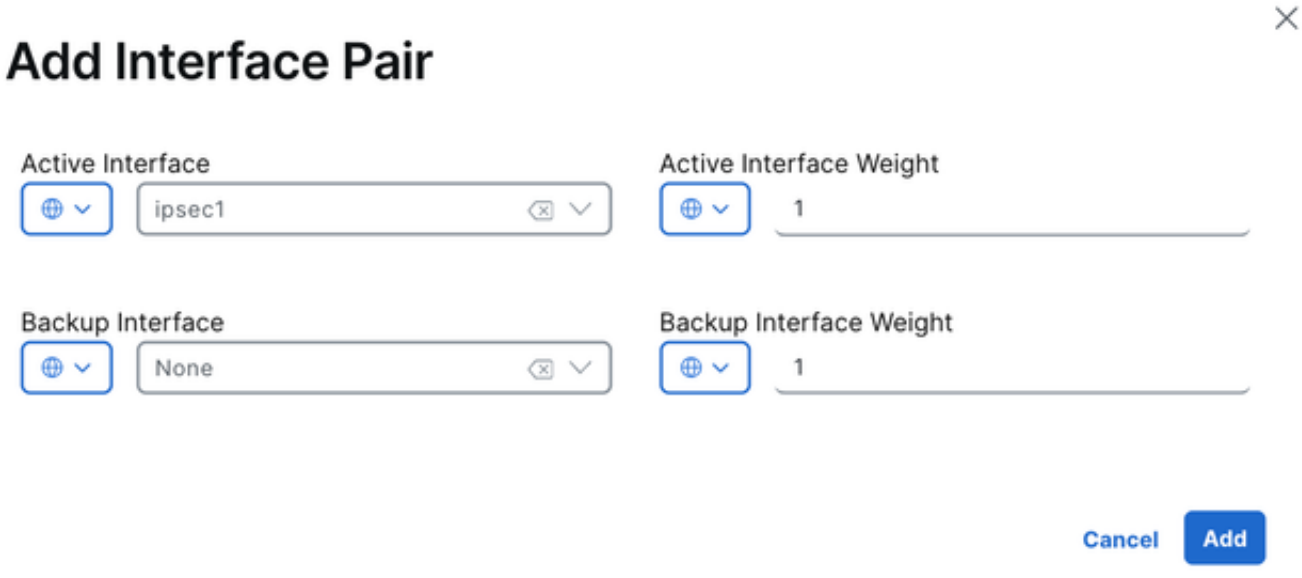
4. Herhaal voor de tweede tunnel dezelfde stappen met dezelfde parameters, maar wijzig de naam van de interface van ipsec1 in ipsec2 en de naam van de broninterface in loopback1.



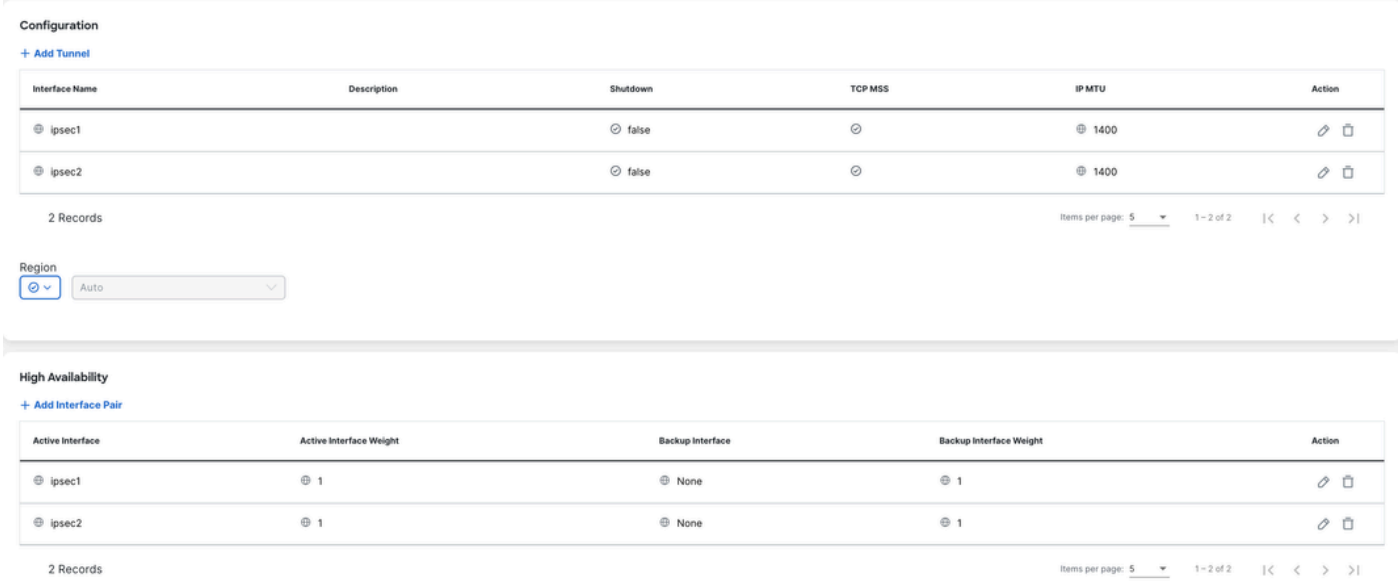
Beide tunnels zijn geconfigureerd om tegelijkertijd actief te zijn, zonder een back-up.

5. Klik op Interfacepaar toevoegen.

6. Klik op Toevoegen. De actieve interface is ingesteld op ipsec1 en er is geen back-upinterface opgegeven.



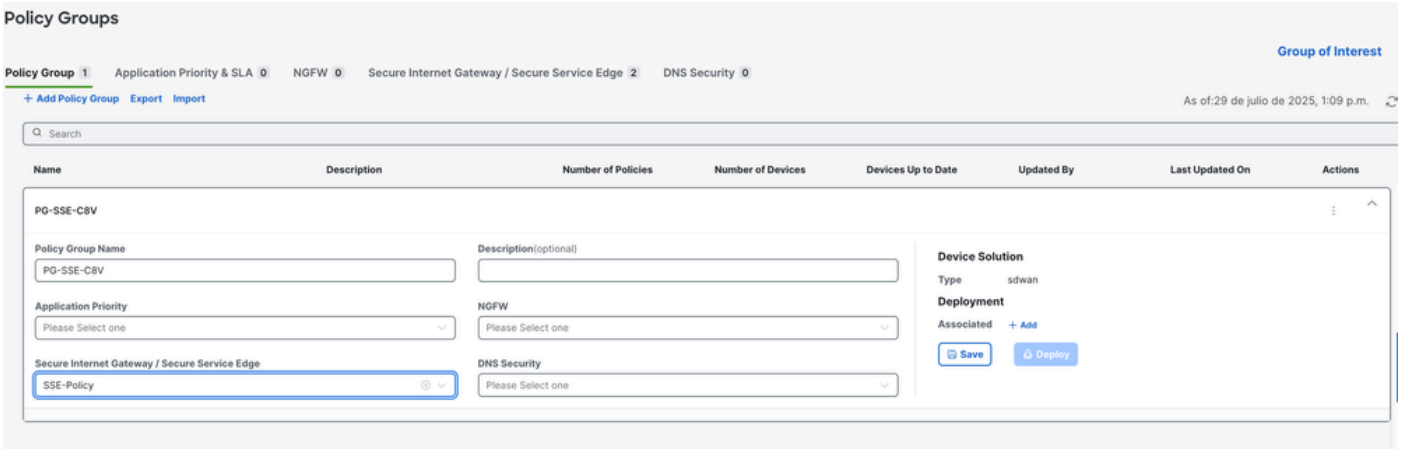
7. Dezelfde handeling wordt herhaald voor de tweede tunnel, ipsec2.



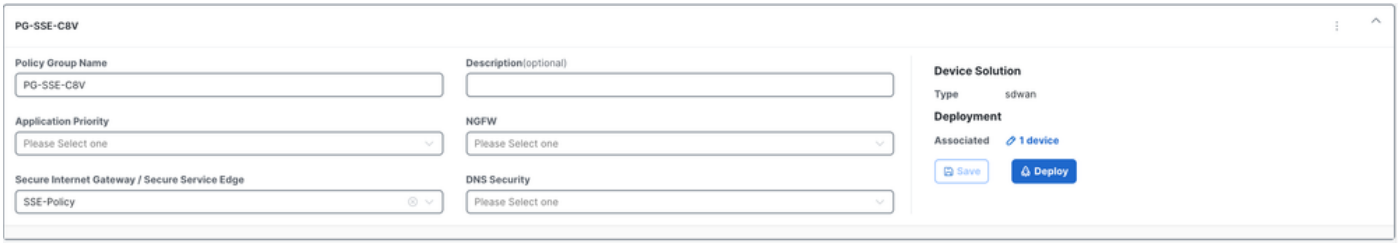
8. Sla de configuratie op.

Beleidsgroep configureren

1. U kunt het beleid selecteren dat eerder in de beleidsgroep is gemaakt en het opslaan.



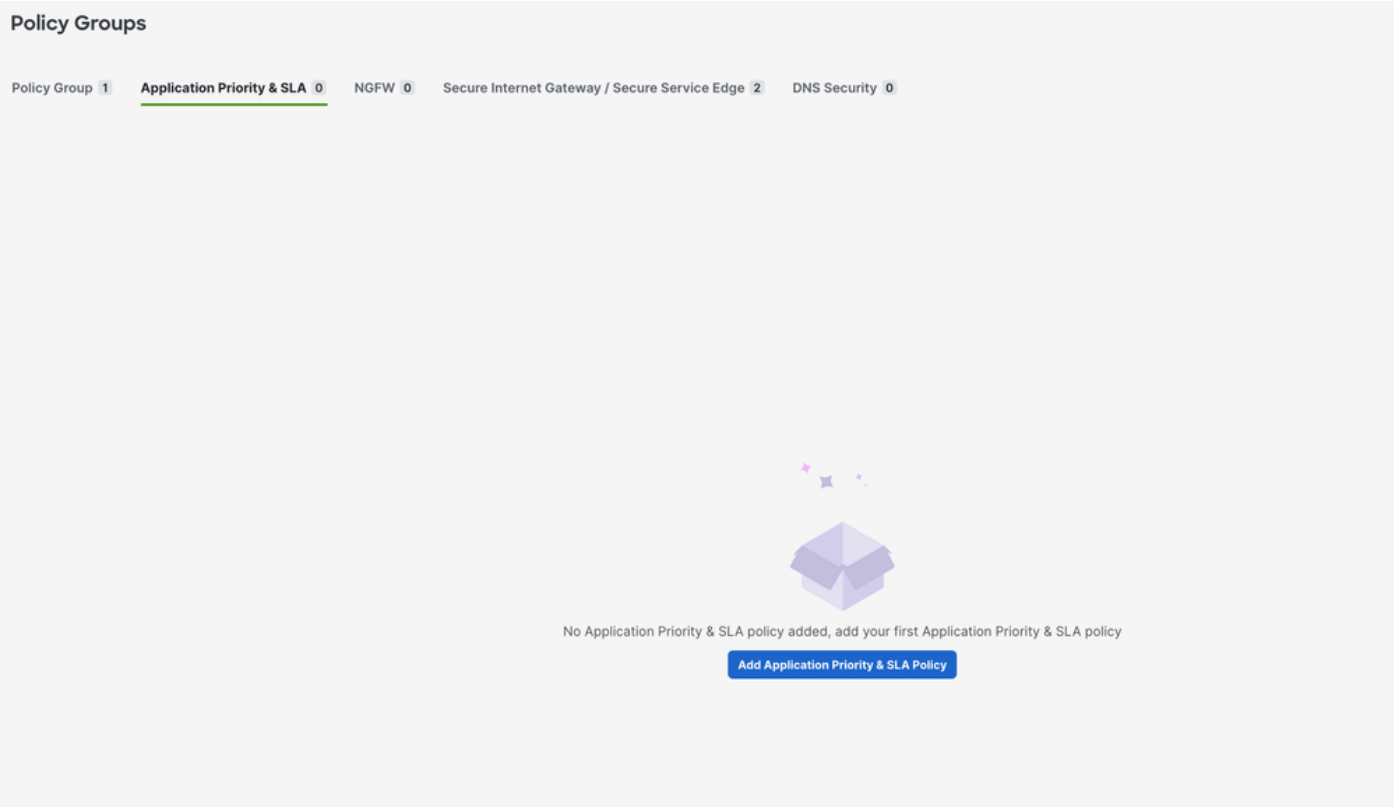
2. Zodra het apparaat of de apparaten aan de beleidsgroep zijn gekoppeld, gaat u verder met het implementeren van de beleidsgroep.



Beleidsgroep configureren om verkeer naar SSE om te leiden

1. Navigeer in SD-WAN Manager naar Configuratie > Beleidsgroepen > Toepassingsprioriteit en SLA.

- Selecteer Toepassingsprioriteit en SLA-beleid toevoegen
- Geef een naam op voor het beleid.

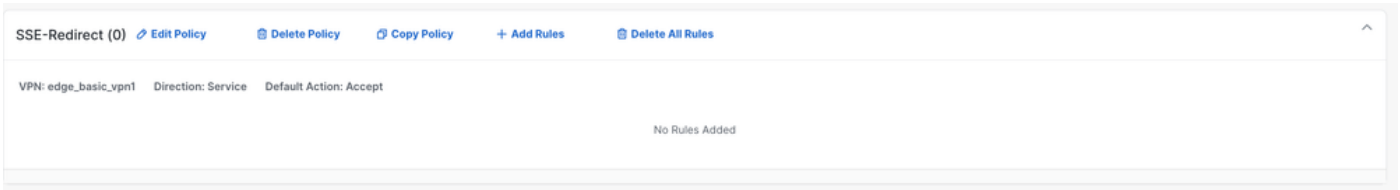


2. Wanneer het nieuwe beleid is weergegeven, selecteert u de schakelaar Geavanceerde lay-out.

3. Selecteer Verkeersbeleidlijst toevoegen.

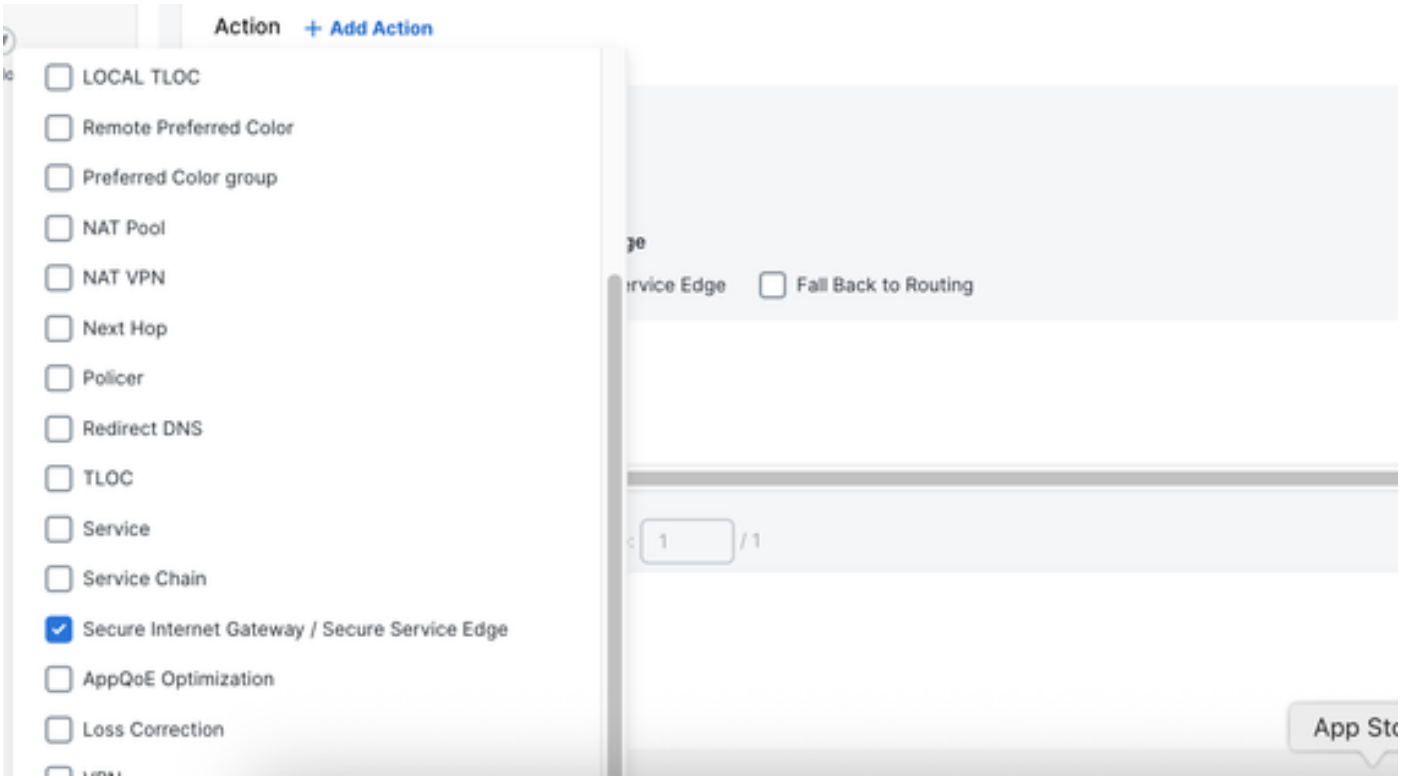
- Configureer de VPN's om het verkeer om te leiden naar de SSE-tunnel.
- Stel de richting en de standaardactie in als dat nodig is en sla op.

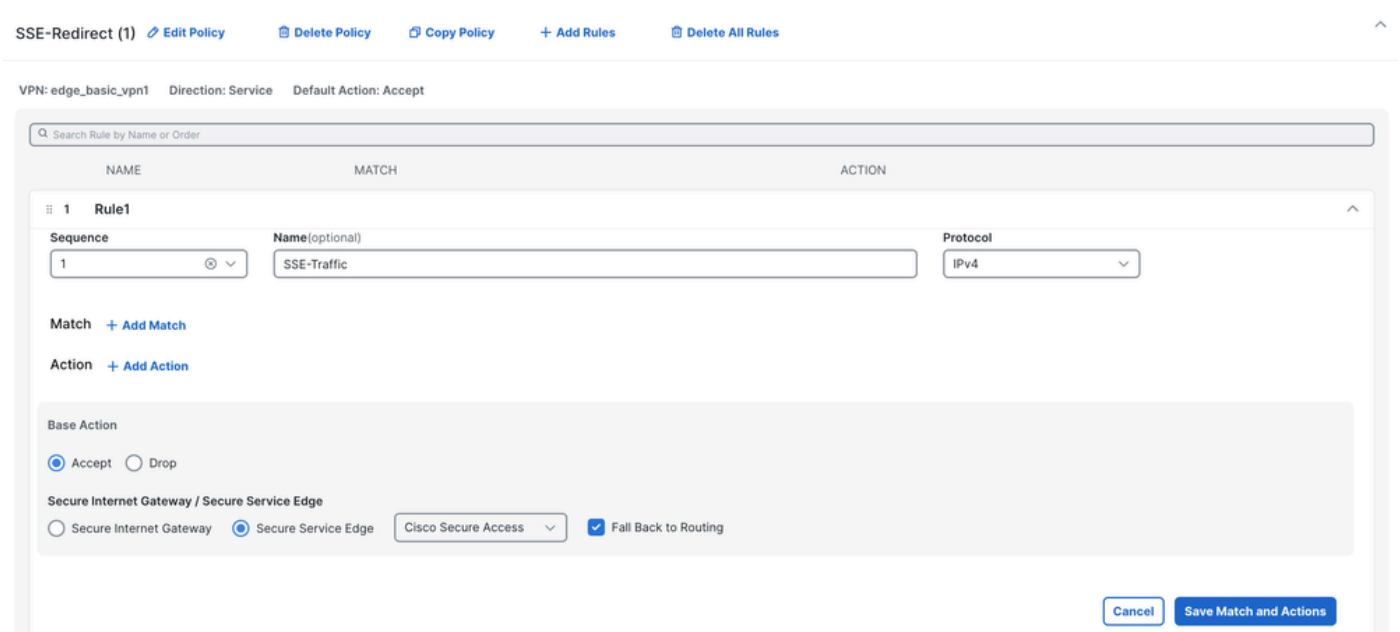
4. Selecteer + Regel toevoegen.



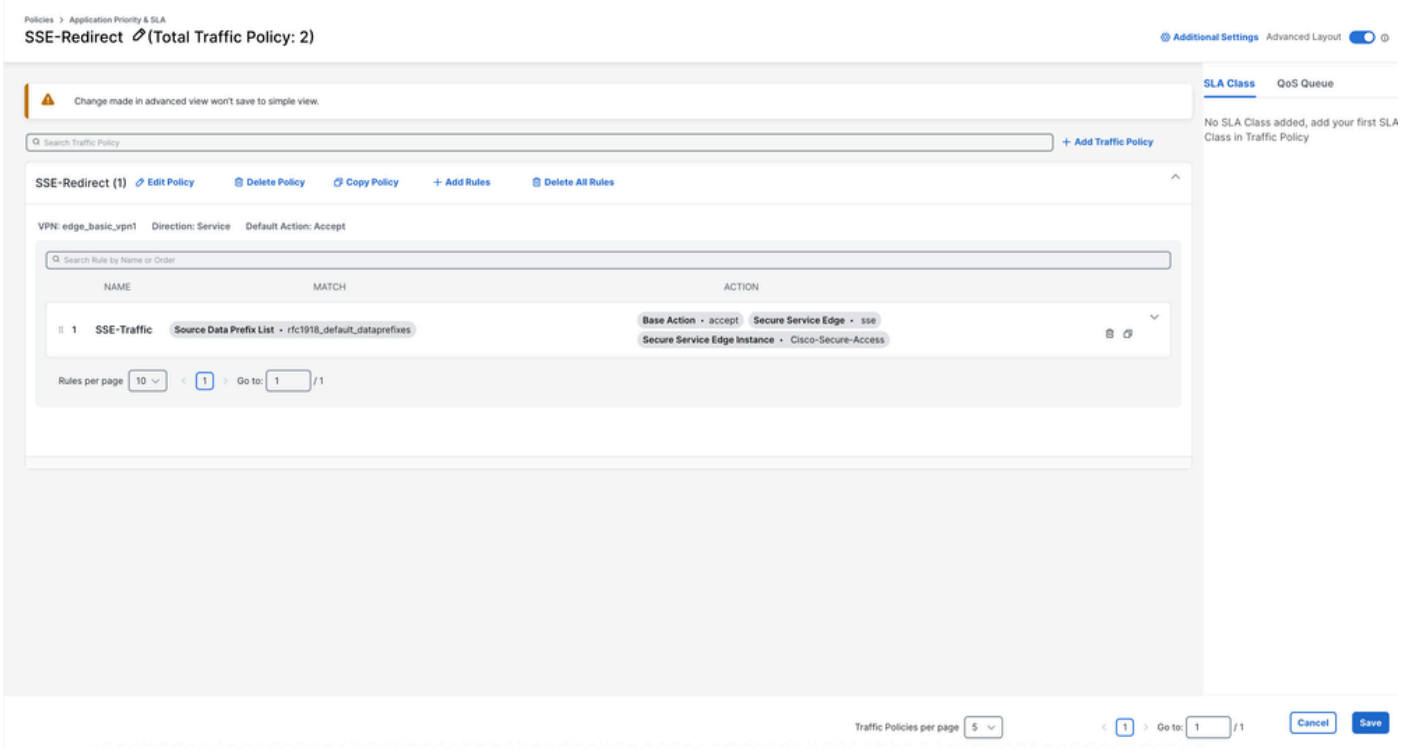
5. Configureer uw overeenkomende verkeerscriteria om het verkeer naar de SSE te leiden.
6. Selecteer Accepteren als basisactie en klik op + Actie.

7. Zoek naar de Secure Internet Gateway / Secure Service Edge-actie en stel deze in op Secure Service Edge.



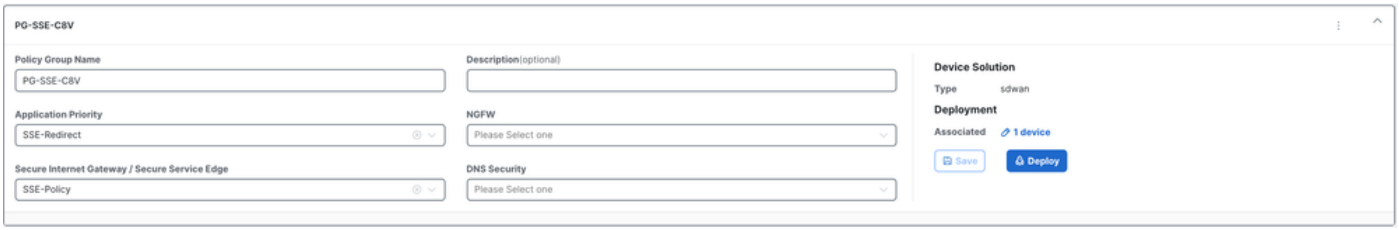


8. Klik op Match en acties opslaan



9. Klik op Opslaan.

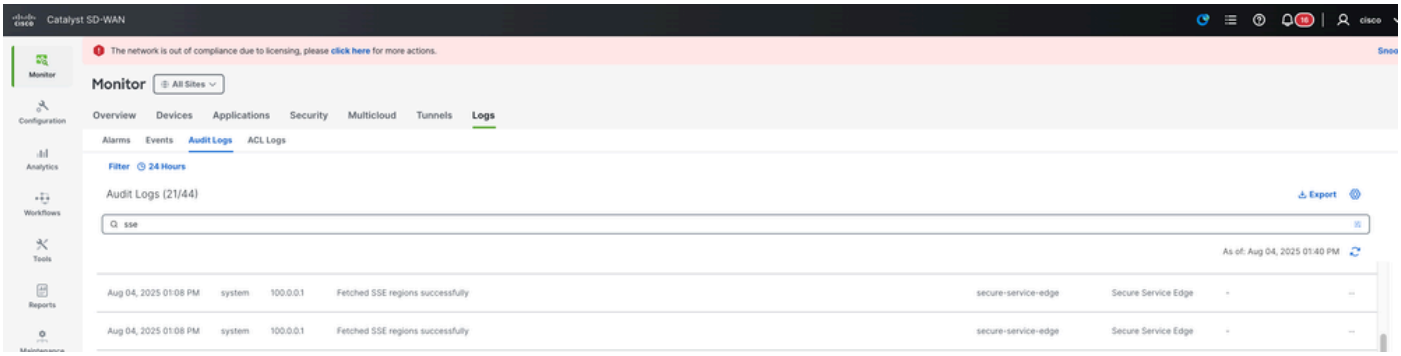
10. Navigeer naar Configuratie > Beleidsgroepen en selecteer het beleid Toepassingsprioriteit dat u zojuist hebt gemaakt. Opslaan en vervolgens implementeren.



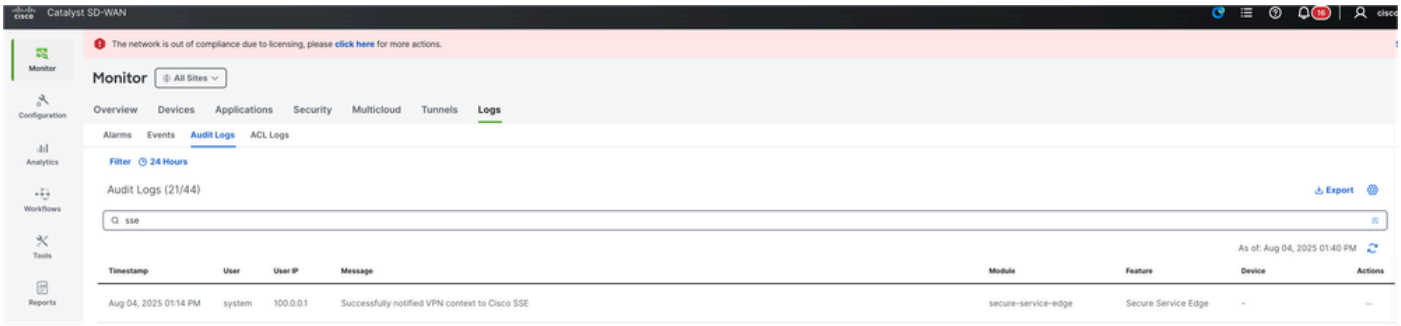
Verifiëren

bedrijfsleider

1. Monitor > Logboeken > Controlelogboeken en zoek naar "sse".

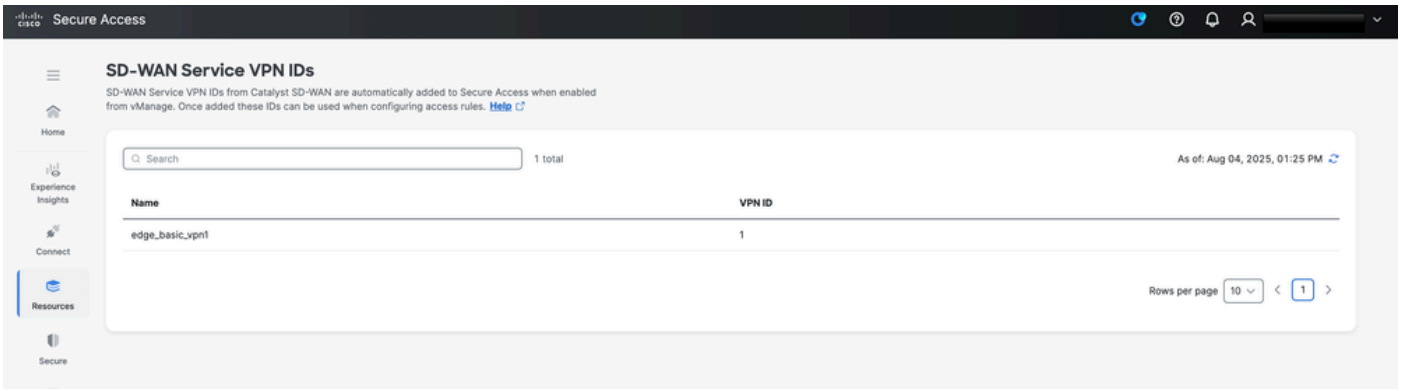


2. U kunt controleren of de VPN voor het delen van context is ingeschakeld door Manager te controleren.



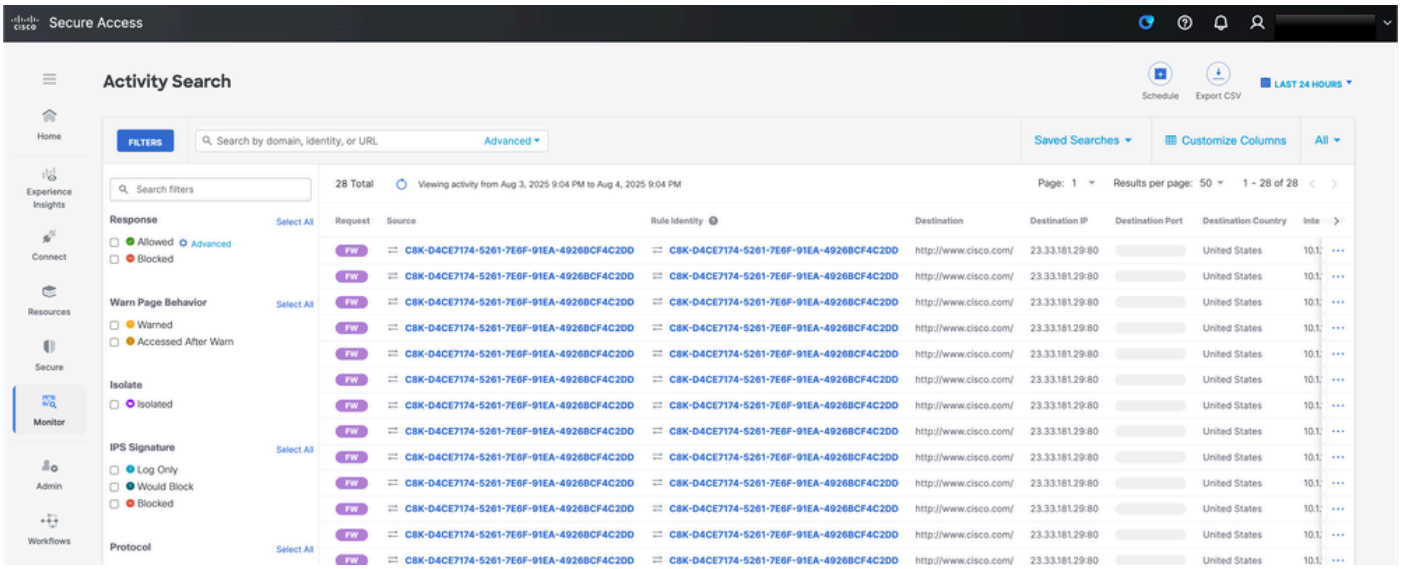
Dashboard voor beveiligde toegang

contextdeling
U kunt controleren of de VPN voor het delen van context is ingeschakeld door het SSE-dashboard te controleren,Bronnen > SD-WAN VPN Service ID's



Tunnel omhoog

Wanneer de tunnel is geopend en de tracker operationeel is met verkeer dat door de tunnel stroomt, kunt u dit valideren door te navigeren naar Monitor > Activity Search. Op dit scherm zie je het verkeer door de tunnel gaan, zoals verzoeken aan www.cisco.com gegenereerd door de tracker. Deze zichtbaarheid bevestigt dat de tracker actief is en het verkeer door de tunnel controleert



CLI-opdrachten (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
```

Gerelateerde informatie

- Contextdeling SD-WAN configureren
- Cisco Secure Access-integratie met SD-routering
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.