

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

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Cisco Secure Access](#)

[Voorlopige configuraties](#)

[Loopback-interfaces maken](#)

[Nieuwe API-sleutels configureren op SSE Portal](#)

[SSE configureren in Catalyst Manager](#)

[Cloudreferenties instellen](#)

[SSE-tunnels configureren met behulp van Beleidsgroep](#)

[Beleidsgroep configureren](#)

[Beleidsgroep configureren om verkeer naar SSE om te leiden](#)

[Verifiëren](#)

[bedrijfsleider](#)

[Dashboard voor beveiligde toegang](#)

[CLI-opdrachten \(Command Line Interface\)](#)

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

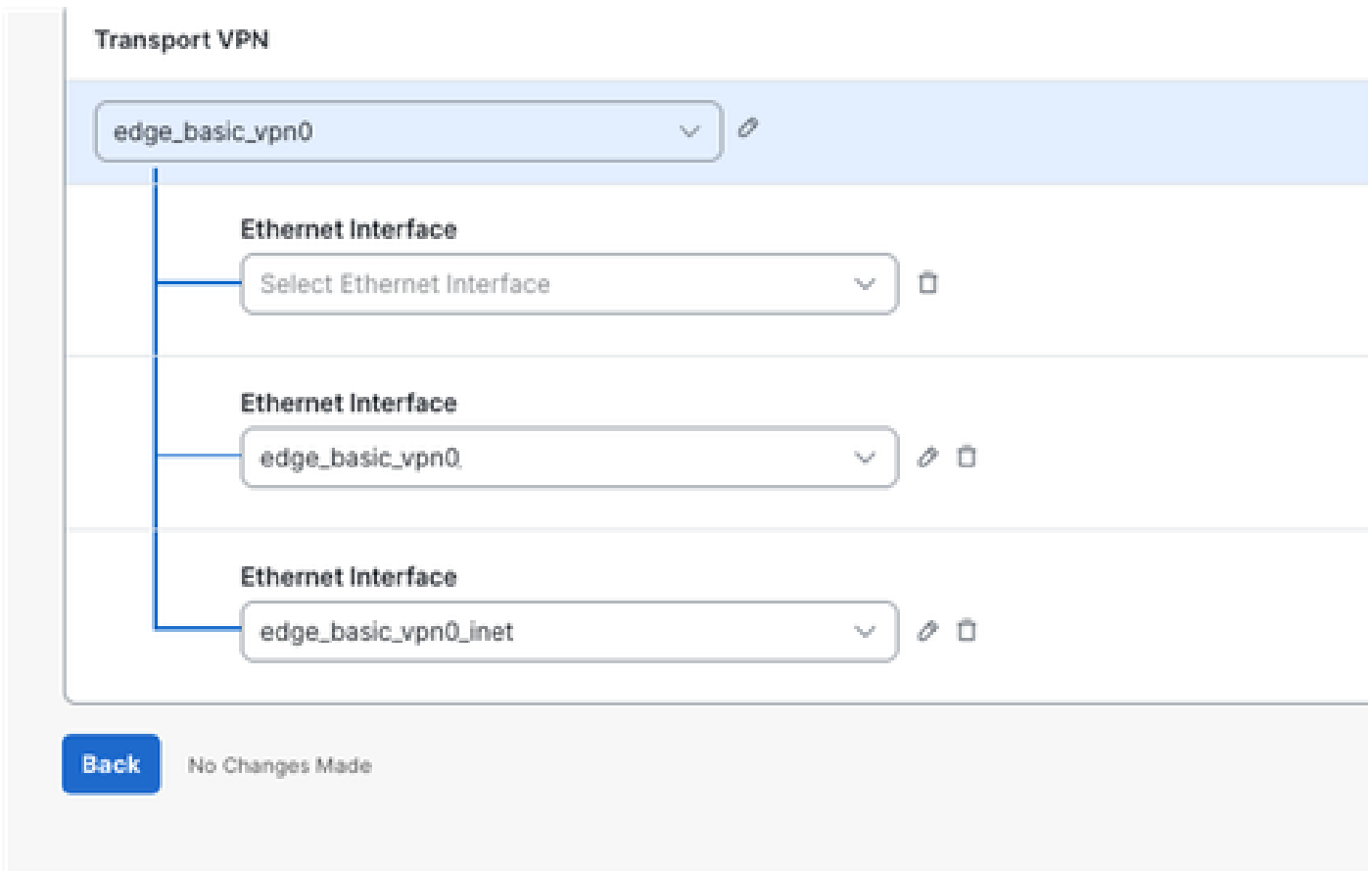
Als beide tunnels in een Active/Active-configuratie verbinding maken met hetzelfde bestemmingsdatacenter en dezelfde WAN-interface gebruiken als de bron, moeten twee loopback-IP-adressen worden gemaakt.



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.



Transport VPN

edge_basic_vpn0

Ethernet Interface

Select Ethernet Interface

Ethernet Interface

edge_basic_vpn0

Ethernet Interface

edge_basic_vpn0_inet

Back No Changes Made

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

Ethernet Interface

Name: Loopback0

Description(optional):

Basic Configuration | Ether Channel | Tunnel | NAT | ARP | ACL/QoS | Advanced

Shutdown: ☐ ☒

Interface Name: Loopback0

Description: <SYSTEM DEFAULT>

Service Provider: <SYSTEM DEFAULT>

Bandwidth Upstream: <SYSTEM DEFAULT>

Bandwidth Downstream: <SYSTEM DEFAULT>

Auto Detect Bandwidth: ☐ ☒

IPv4 Settings

☐ Dynamic ☒ Static

IP Address: 10.1.1.1

Subnet Mask: /32 255.255.255.255

Cancel Save

Transport VPN

edge_basic_vpn0

Ethernet Interface: Loopback1

Ethernet Interface: Loopback0

Ethernet Interface: edge_basic_vpn0_mpls

Ethernet Interface: edge_basic_vpn0_inet

New Loopback interfaces

Back All Changes Saved

- 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 ¹ 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



Home



Experience
Insights



Connect



Resources



Secure



Monitor

Admin



Account Settings

Accounts

Authentication

Management

API Keys

Third-party Integrations

Log Management

Subscription

Integrations

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

Click Refresh to generate a new key and secret.

API Key	Key Secret

Copy the Key Secret. For security reasons, it is only displayed once. If lost, it cannot be retrieved.

ACCEPT AND CLOSE

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.



Discover your SSE organization ID

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.

Settings / External Services

Cloud Credentials

Cloud Provider Credentials

Umbrella DNS Certificate

Configure Cisco Umbrella, Zscaler, and Cisco Secure Access credentials to enable Cisco Catalyst SD-WAN Manager to create automatic SIG tunnels to Cisco Umbrella or Zscaler endpoints.

☐ Umbrella

☐ Zscaler

☒ Cisco SSE

Organization Id

Api Key

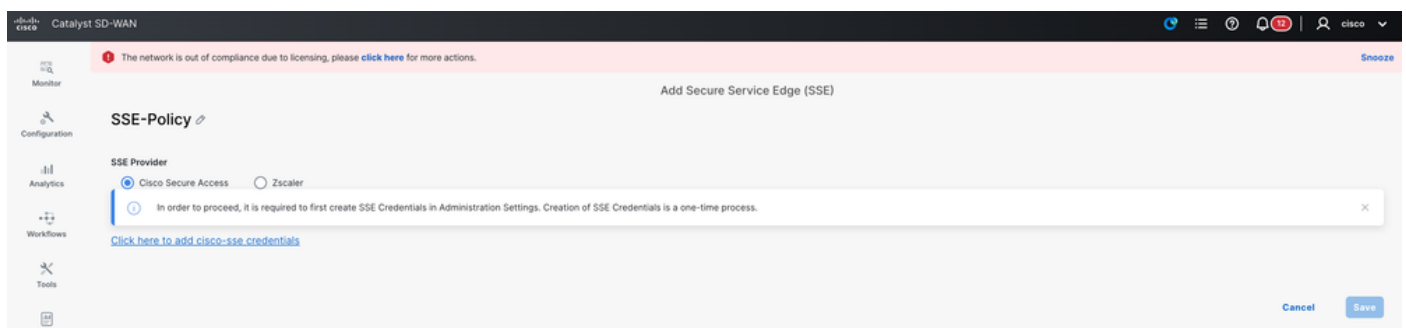
Secret

☒ Context Sharing

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

Add cisco-sse Credentials



Cisco SSE Organization Id*

Cisco SSE API Key*

Cisco SSE API Secret*

 [SHOW](#)

Context Sharing

Cancel

Add

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.

Add Tracker



Name



cisco-tracker

API URL Of Endpoint



http://www.cisco.com

Threshold



300

Probe Interval



60

Multiplier



3

Cancel

Add

SSE-Policy

SSE Provider
☒ Cisco Secure Access ☐ Zscaler

Context Sharing
☒ VPN ☐ SGT

Tracker
Source IP address: 10.0.0.10

+ Add Tracker

Name	Threshold	Interval	Multiplier	API URL Of Endpoint	Action
cisco-tracker	300	60	3	http://www.cisco.com	

1 Record

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

Configuration
+ Add Tunnel

Interface Name	Description	Shutdown	TCP MSS	IP MTU	Action
There is no data.					

0 Record

Region: Auto

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

Add Tunnel



Tunnel Type

☒ ipsec

Interface Name(1..255)

Tunnel Source Interface*

Tracker

Tunnel Route-via Interface

Data Center

☒ Primary ☐ Secondary

> Advanced Options

Cancel

Add

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.



Add Tunnel

Tunnel Type

☒ ipsec

Interface Name(1..255)



ipsec2

Tunnel Source Interface*



Loopback1

Tracker



cisco-tracker



Tunnel Route-via Interface



GigabitEthernet1

Data Center

☒ Primary

☐ Secondary

> Advanced Options

Cancel

Add

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.



Add Interface Pair

Active Interface



ipsec1



Active Interface Weight



1

Backup Interface



None



Backup Interface Weight



1

Cancel

Add

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

Configuration

+ Add Tunnel

Interface Name	Description	Shutdown	TCP MSS	IP MTU	Action
ipsec1		false		1400	
ipsec2		false		1400	

2 Records

Items per page: 5

1 - 2 of 2

Region

Auto

High Availability

+ Add Interface Pair

Active Interface	Active Interface Weight	Backup Interface	Backup Interface Weight	Action
ipsec1	1	None	1	
ipsec2	1	None	1	

2 Records

Items per page: 5

1 - 2 of 2

8. Sla de configuratie op.

Beleidsgroep configureren

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

Policy Groups

Policy Group 1

Application Priority & SLA 0

NGFW 0

Secure Internet Gateway / Secure Service Edge 2

DNS Security 0

+ Add Policy Group

Export

Import

Group of Interest

As of: 29 de julio de 2025, 1:09 p.m.

Search

Name	Description	Number of Policies	Number of Devices	Devices Up to Date	Updated By	Last Updated On	Actions
PG-SSE-C8V Policy Group Name PG-SSE-C8V Description(optional) Application Priority Please Select one NGFW Please Select one Secure Internet Gateway / Secure Service Edge SSE-Policy DNS Security Please Select one Device Solution Type sdwan Deployment Associated + Add Save Deploy							

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

PG-SSE-C8V

Policy Group Name

PG-SSE-C8V

Description(optional)

Application Priority

Please Select one

NGFW

Please Select one

Secure Internet Gateway / Secure Service Edge

SSE-Policy

DNS Security

Please Select one

Device Solution

Type sdwan

Deployment

Associated 1 device

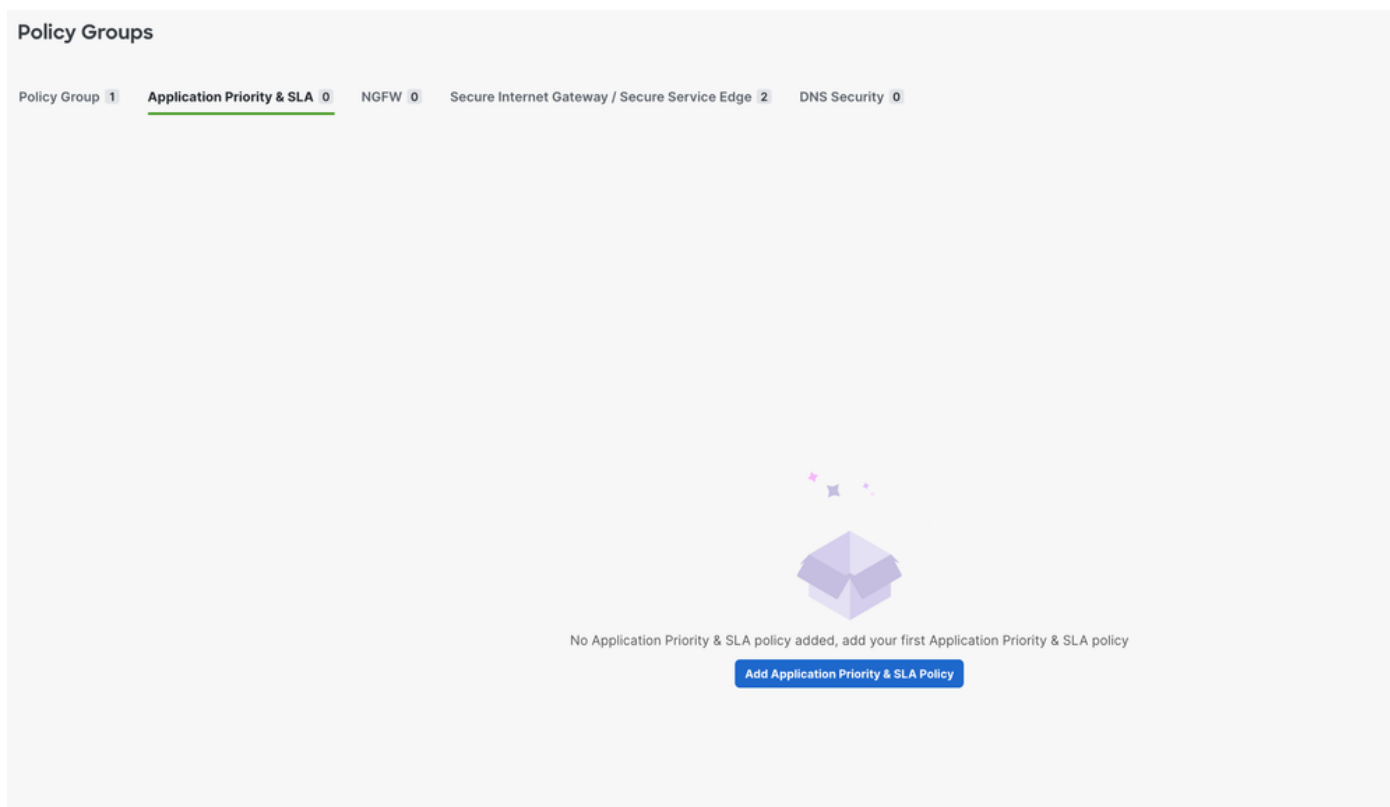
Save

Deploy

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.

Edit Traffic Policy List

Policy Name

SSE-Redirect

VPN(s)

edge_basic_vpn1

Direction

Service

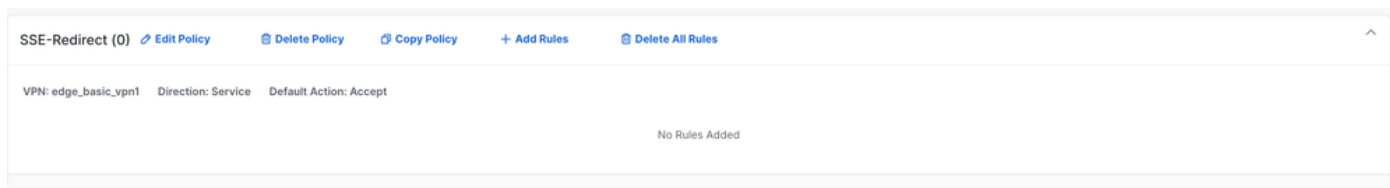
Default Action

☒ Accept ☐ Drop

Cancel

Save

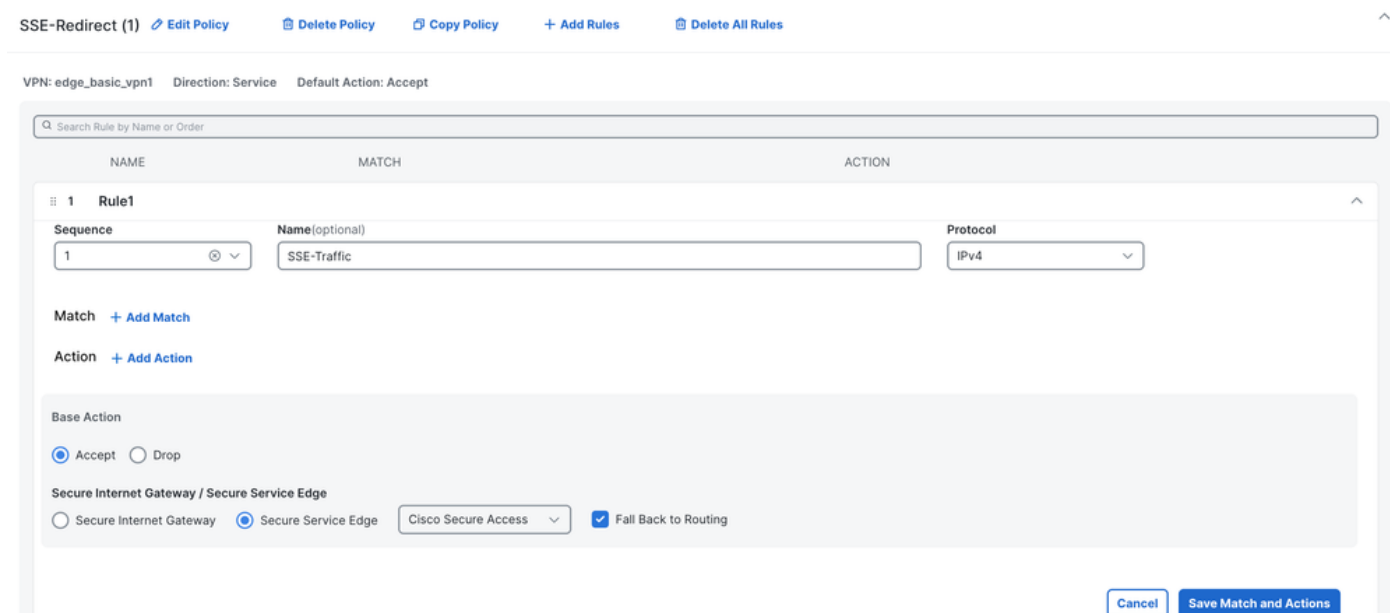
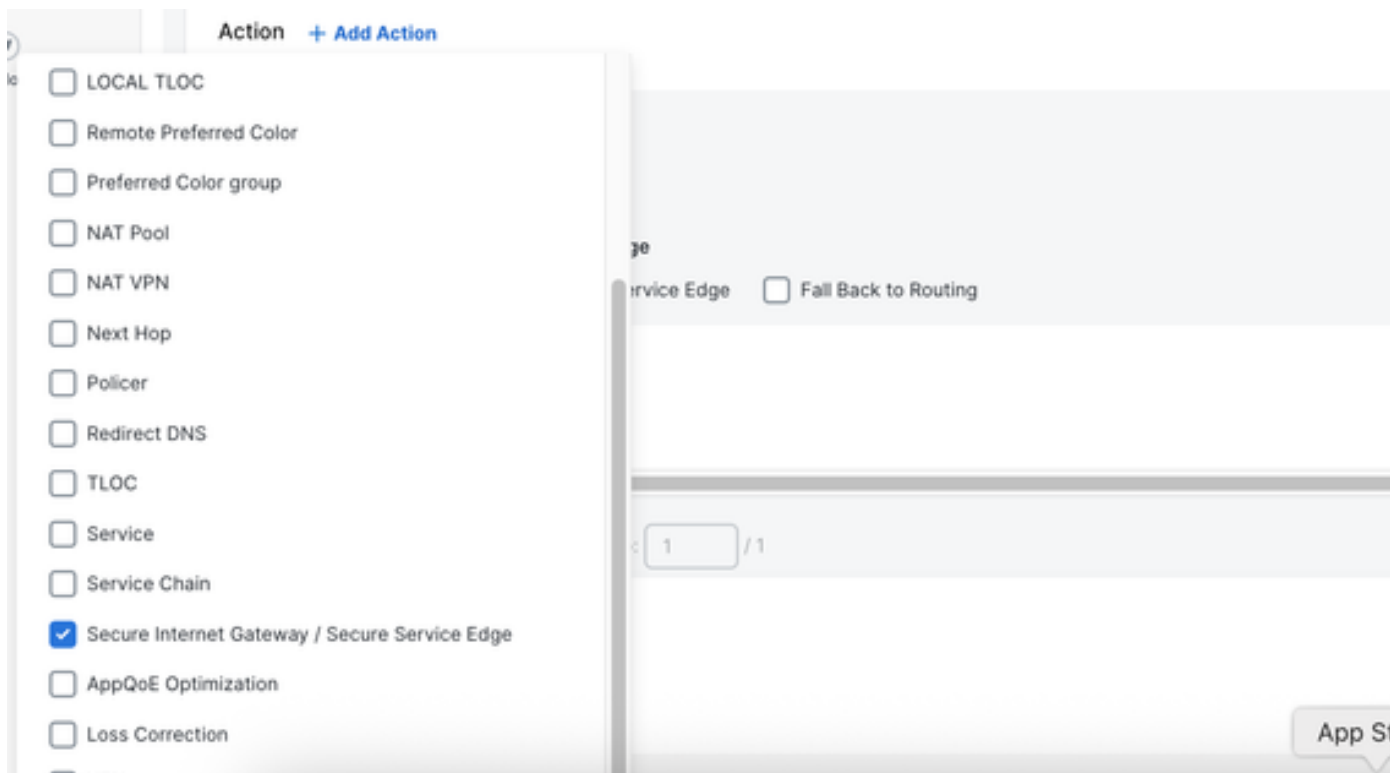
4. Selecteer + Regel toevoegen.



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

Policies > Application Priority & SLA
SSE-Redirect (Total Traffic Policy: 2)

Change made in advanced view won't save to simple view.

Search Traffic Policy + Add Traffic Policy

SSE-Redirect (1) Edit Policy Delete Policy Copy Policy + Add Rules Delete All Rules

VPN: edge_basic_vpn1 Direction: Service Default Action: Accept

Search Rule by Name or Order

NAME	MATCH	ACTION
1 SSE-Traffic	Source Data Prefix List - rfc1918_default_dataprefixes	Base Action - accept Secure Service Edge - sse Secure Service Edge Instance - Cisco-Secure-Access

Rules per page 10 < 1 > Go to: 1 / 1

Traffic Policies per page 5 < 1 > Go to: 1 / 1 Cancel Save

9. Klik op Opslaan.

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

PG-SSE-CBV

Policy Group Name: PG-SSE-CBV

Description(optional):

Application Priority: SSE-Redirect

NGFW: Please Select one

Secure Internet Gateway / Secure Service Edge: SSE-Policy

DNS Security: Please Select one

Device Solution

Type: sdwan

Deployment

Associated: 1 device

Save Deploy

Verifiëren

bedrijfsleider

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

Cisco Catalyst SD-WAN

The network is out of compliance due to licensing, please [click here](#) for more actions.

Monitor All Sites

Overview Devices Applications Security Multicloud Tunnels Logs

Alarms Events Audit Logs ACL Logs

Filter 24 Hours

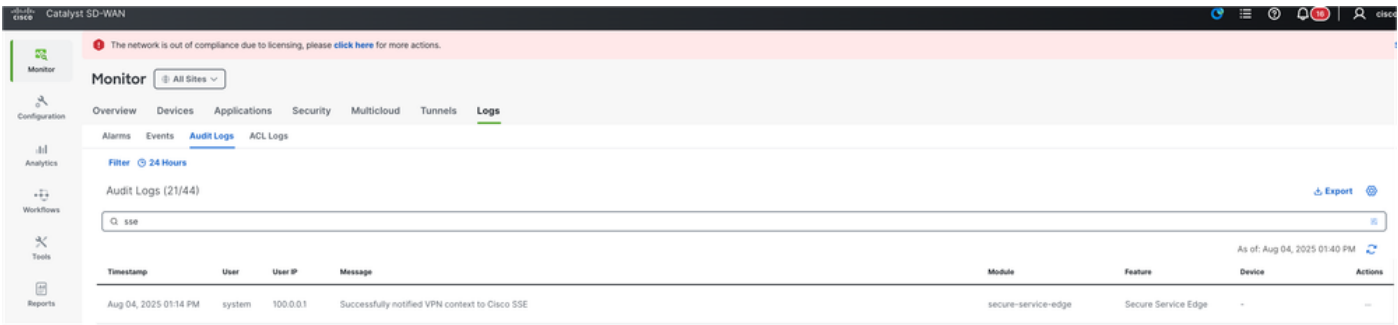
Audit Logs (21/44)

Export

As of: Aug 04, 2025 01:40 PM

Time	System	IP	Event	Device	Instance	Action	Result
Aug 04, 2025 01:08 PM	system	100.0.0.1	Fetched SSE regions successfully	secure-service-edge	Secure Service Edge	-	...
Aug 04, 2025 01:08 PM	system	100.0.0.1	Fetched SSE regions successfully	secure-service-edge	Secure Service Edge	-	...

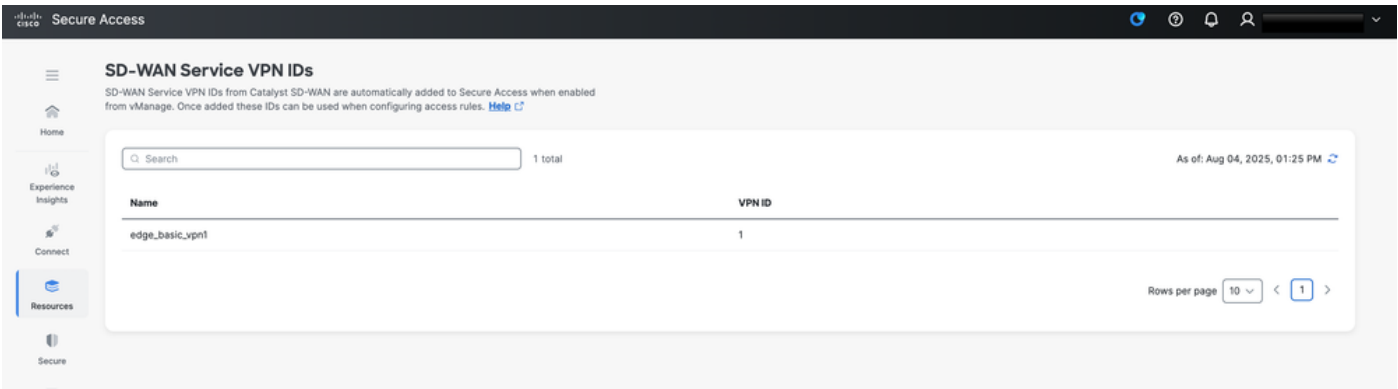
2. U kunt controleren of de VPN voor het delen van context is ingeschakeld door Manager te controleren.



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

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Destination Country	Int.
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80	23.33.181.29-80	United States	10.1
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80	23.33.181.29-80	United States	10.1
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80	23.33.181.29-80	United States	10.1
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80	23.33.181.29-80	United States	10.1
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80	23.33.181.29-80	United States	10.1
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80	23.33.181.29-80	United States	10.1
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80	23.33.181.29-80	United States	10.1
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80	23.33.181.29-80	United States	10.1
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80	23.33.181.29-80	United States	10.1
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80	23.33.181.29-80	United States	10.1

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-routing](#)
- [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.