Beveiligde toegang configureren met automatische Catalyst SD-WAN-tunnels voor beveiligde privétoegang

Inhoud

Inleiding

In dit document wordt beschreven hoe u Secure Access configureert met automatische Catalyst SD-WAN-tunnels voor beveiligde privétoegang.

Achtergrondinformatie

Naarmate organisaties verder gaan dan traditionele perimeter-gebaseerde netwerken, wordt veilige toegang tot privébronnen net zo belangrijk als het beveiligen van internetverkeer. Toepassingen zijn niet langer beperkt tot één enkel datacenter, ze leven nu in on-premises omgevingen, openbare clouds en hybride architecturen. Deze verschuiving vereist een flexibelere en modernere benadering van particuliere toegang.

Dit is waar een op SASE gebaseerde architectuur en Cisco Secure Access een rol spelen. In plaats van te vertrouwen op legacy VPN-concentrators en platte netwerktoegang, biedt Cisco Secure Access privéconnectiviteit als een cloud-geleverde service, waarbij VPN-as-a-Service (VPNaaS) en Zero Trust Network Access (ZTNA) worden gecombineerd.

Voor private toegang op netwerkniveau integreert Cisco Secure Access met SD-WAN met behulp van geautomatiseerde site-to-site IPsec-tunnels. Deze tunnels zorgen ervoor dat privéverkeer veilig kan stromen tussen Secure Access en on-premises of cloudnetwerken, terwijl de beveiligingsinspectie en beleidshandhaving gecentraliseerd blijven in de cloud. Vanuit operationeel oogpunt neemt dit de noodzaak weg om traditionele VPN-headends te implementeren en te onderhouden en vereenvoudigt het schalen naarmate omgevingen groeien.

In een VPNaaS-model fungeert Secure Access als het VPN-terminatiepunt in de cloud. SD-WAN behandelt intelligente routering en veerkracht met Secure Access en zorgt ervoor dat het verkeer wordt beschermd en beheerd door een consistent beveiligingsbeleid voordat het particuliere bronnen bereikt.

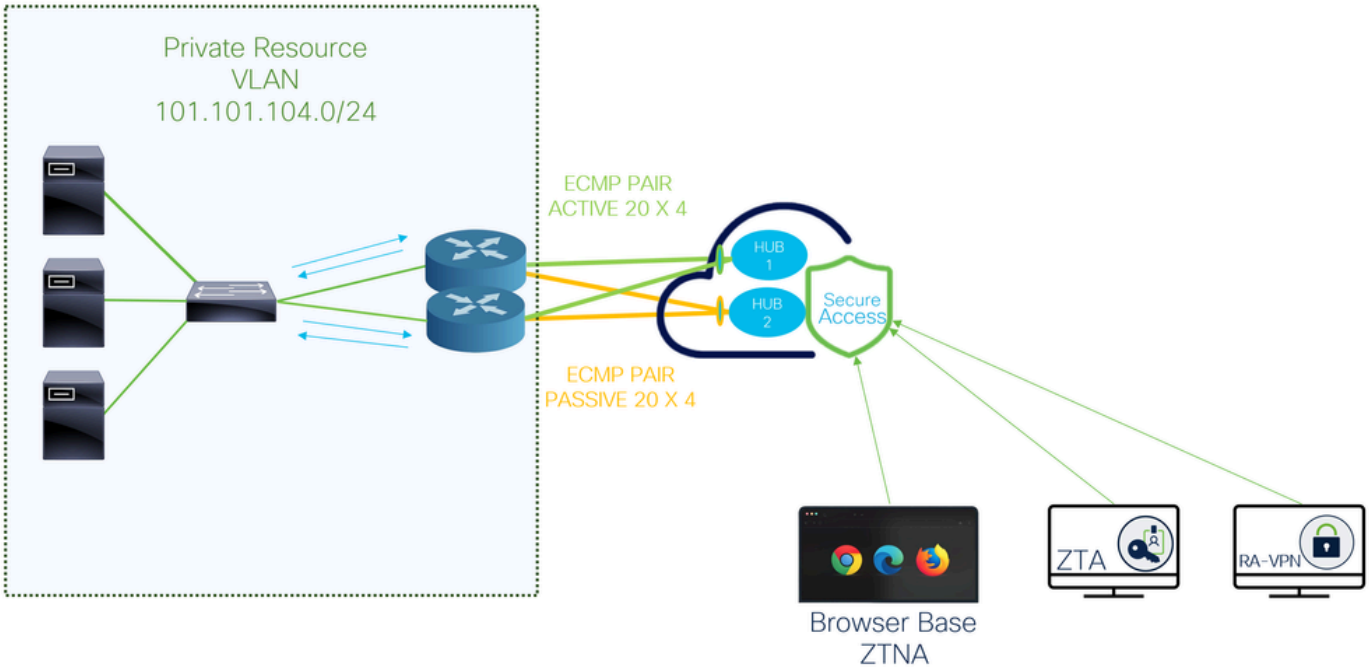
Cisco Secure Access ondersteunt ook geavanceerde site-to-site tunnelarchitecturen, waaronder multiregionale backhaul. Deze mogelijkheid stelt organisaties in staat om tunnels te bouwen naar meerdere Secure Access-regio's tegelijk, wat zorgt voor geografische redundantie en een hogere beschikbaarheid. Door verbinding te maken met verschillende regio's, kan het verkeer automatisch uitvallen in geval van regionale uitval, latentievermindering of onderhoudsgebeurtenissen.

Een organisatie kan bijvoorbeeld site-to-site tunnels opzetten vanuit haar SD-WAN-omgeving naar Secure Access-regio's in Londen en Duitsland. Beide tunnels blijven actief, waardoor veerkrachtige particuliere toegang over regio's mogelijk wordt en continuïteit wordt gewaarborgd, zelfs als één regio niet beschikbaar is. Dit multiregionale ontwerp versterkt de hoge beschikbaarheid, verbetert de fouttolerantie en sluit aan bij de vereisten voor veerkracht op bedrijfsniveau.

Cisco Secure Access dwingt het Zero Trust Network Access (ZTNA)-model af voor meer granulaire toegang. In plaats van gebruikers brede netwerkconnectiviteit te bieden, biedt ZTNA alleen toegang tot specifieke toepassingen, op basis van identiteit, apparaathouding en context. Deze aanpak vermindert het aanvalsoppervlak aanzienlijk en sluit aan bij de Zero Trust-principes.

ZTNA-toegang wordt mogelijk gemaakt door een combinatie van site-to-site tunnels en Resource Connectors. Resource Connectors zijn lichtgewicht virtuele apparaten die alleen uitgaande verbindingen tot stand brengen met Secure Access, wat betekent dat privébronnen nooit rechtstreeks aan internet hoeven te worden blootgesteld.

Netwerkdiagram



Voorwaarden

Vereisten

- Veilige toegang tot kennis
- Cisco Catalyst SD-WAN Manager release 20.18.2 en Cisco IOS XE Catalyst SD-WAN release 17.18.2 of hoger
- Tussentijdse kennis van routing en switching
- ECMP-kennis
- VPN-kennis

- Aangezien deze integratie is gebaseerd op gecontroleerde beschikbaarheid, moet u een TAC-geval indienen om te vragen of u de functie in Cisco Secure Access wilt inschakelen

Gebruikte componenten

- Secure Access-huurder
- Catalyst SD-WAN Manager Release 20.18.2 en Cisco IOS XE Catalyst SD-WAN Release 17.18.2
- Catalyst SD-WAN Manager

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.

Configureren

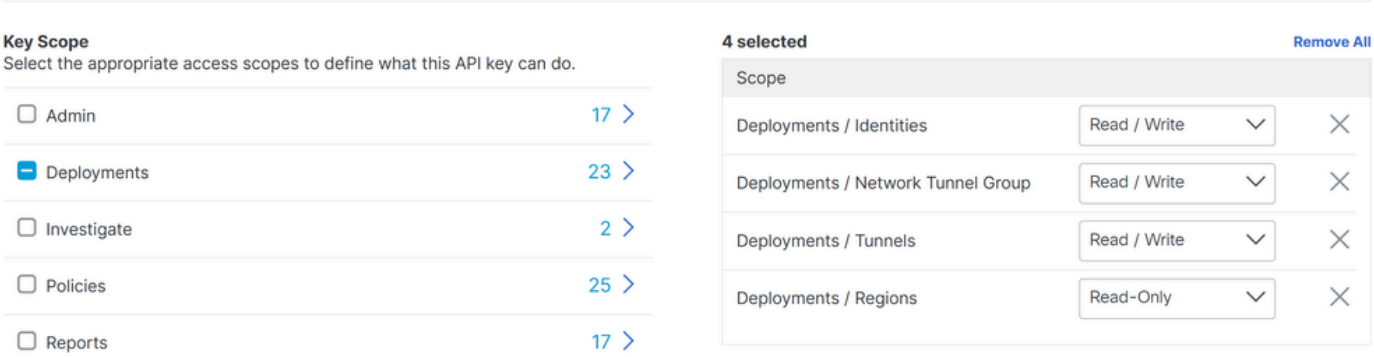
Beveiligde toegangsconfiguratie

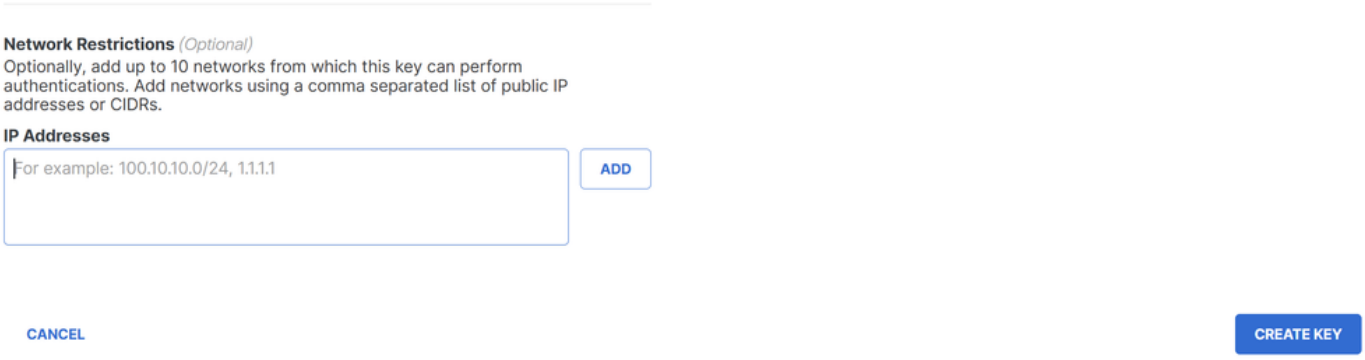
API maken

Om de geautomatiseerde tunnels met Secure Access te maken, controleert u de volgende stappen:

Navigeer naar het Secure Access Dashboard.

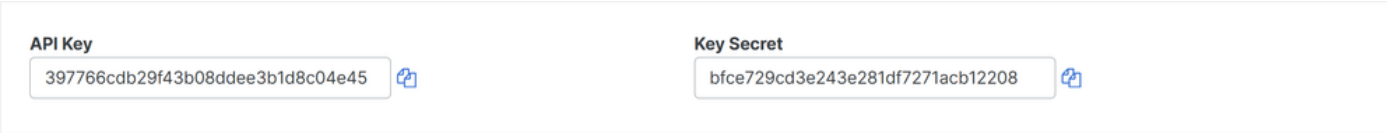
- Klik op Admin > API Keys
- Klik op Add
- Kies de volgende opties:
  - Deployments / Network Tunnel Group: lezen/schrijven
  - Deployments / Tunnels: lezen/schrijven
  - Deployments / Regions:Alleen-lezen
  - Deployments / IdentitiesBetreft: Lezen-schrijven
  - Expiry Date: Nooit verlopen





Opmerking: Voeg optioneel maximaal 10 netwerken toe van waaruit deze sleutel verificaties kan uitvoeren. Voeg netwerken toe met behulp van een door komma's gescheiden lijst met openbare IP-adressen of CIDR's.

- Klik CREATE KEY om de creatie van de API Key en Key Secrette voltooien.



Let op: Kopieer ze voordat u klikt ACCEPT AND CLOSE; anders moet u ze opnieuw maken en degenen verwijderen die niet zijn gekopieerd.

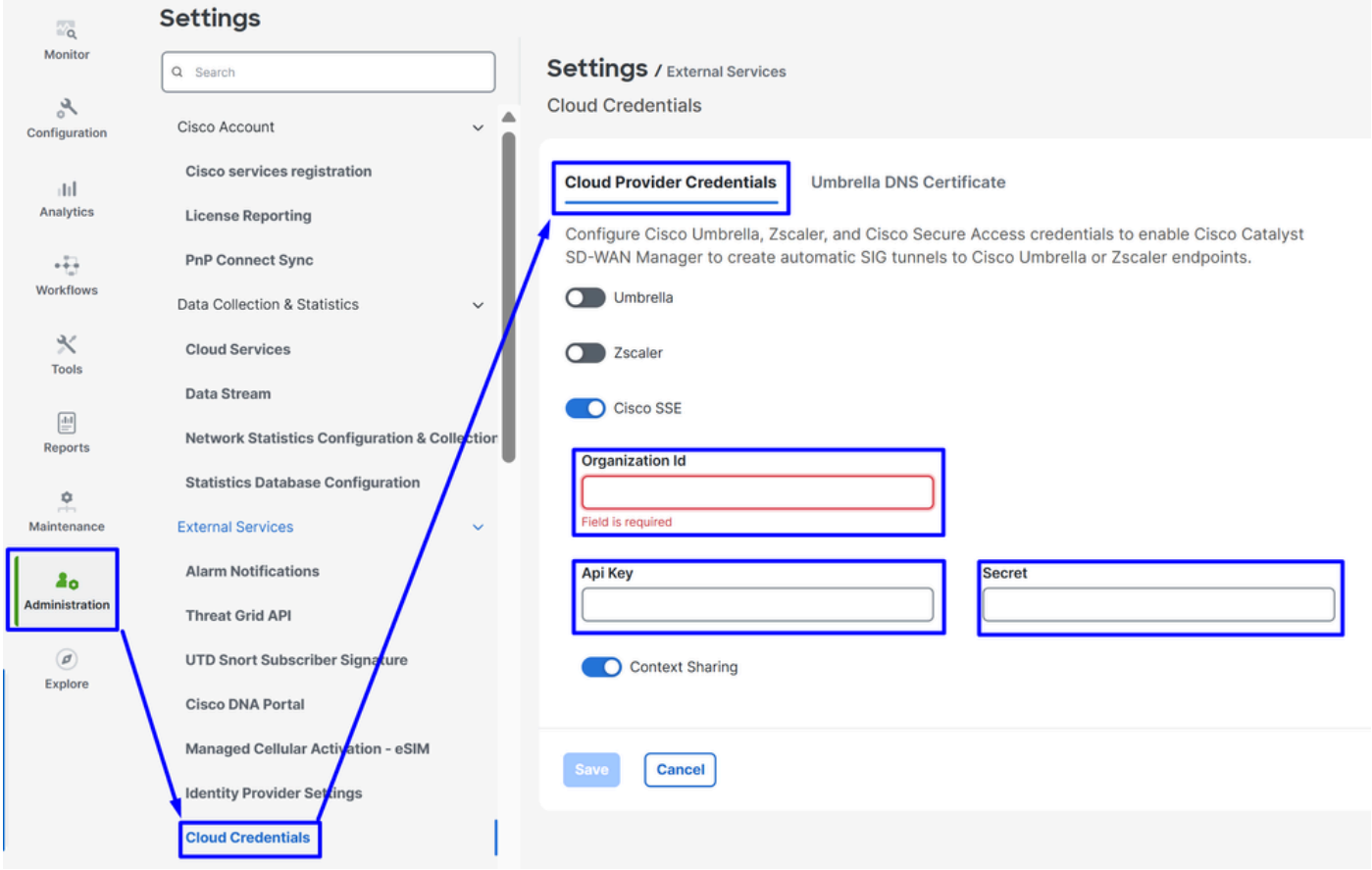
Om vervolgens te finaliseren klik ACCEPT AND CLOSE.

SD-WAN-configuratie

API-integratie

Navigeer naar Catalyst SD-WAN Manager:

- Klik op **Administration** >Settings> Cloud Credentials
- Klik vervolgens op Cloud Provider Credentials en schakel de API- en Cisco SSEorganisatieinstellingen in en vul deze in



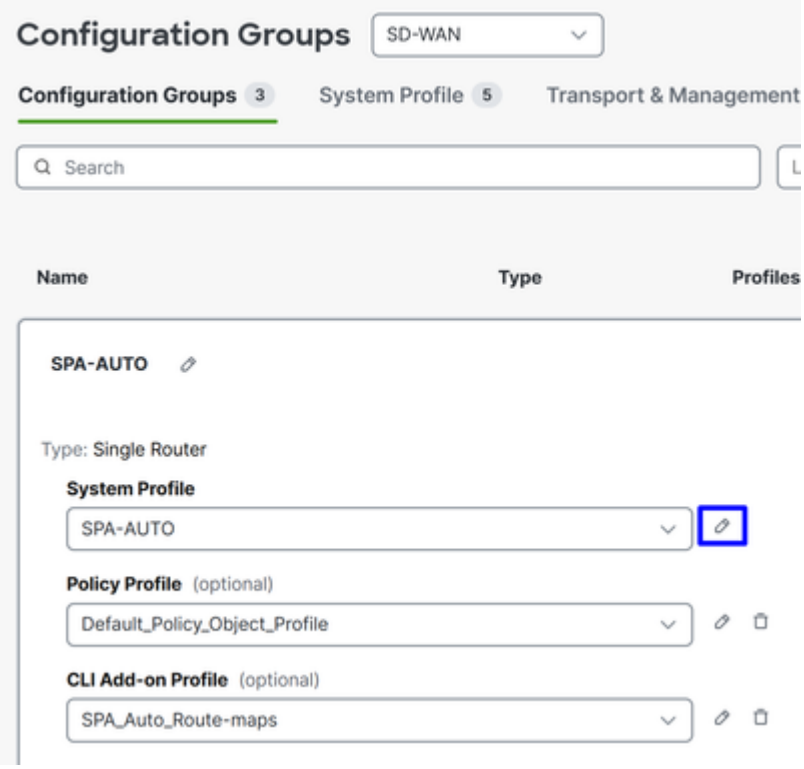
- **Organization ID**: U kunt dat uit de URL van uw SSE Dashboard https://dashboard.sse.cisco.com/org/xxxxx
- Api Key: Kopieer het vanuit de stap Beveiligde toegangsconfiguratie
- Secret: Kopieer het vanuit de stap Beveiligde toegangsconfiguratie

Daarna klik je op de Save knop.

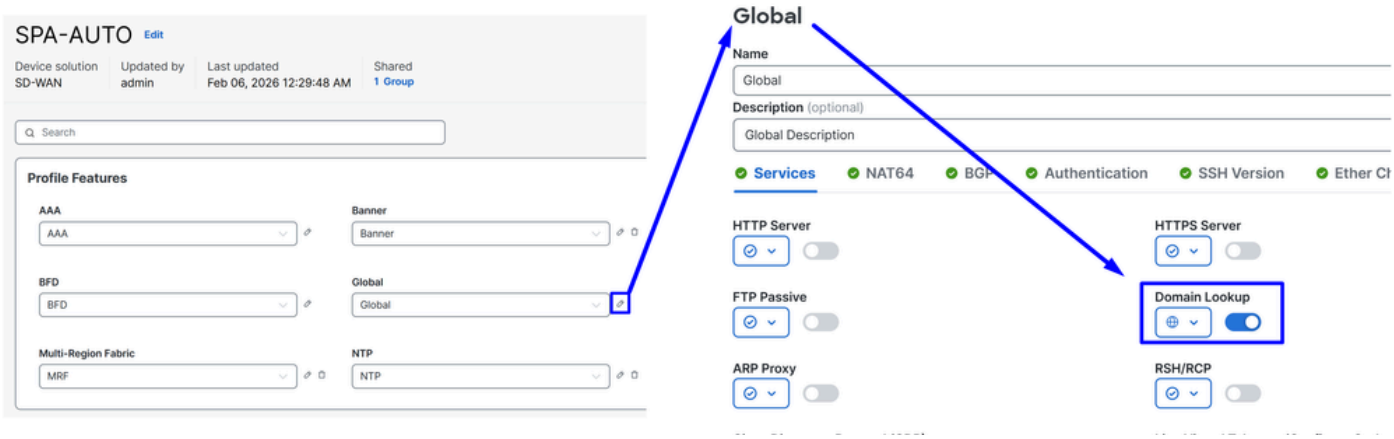
Opmerking: Voordat u verder gaat met de volgende stappen, moet u ervoor zorgen dat de SD-WAN-manager en de Catalyst SD-WAN-randen DNS-resolutie en internettoegang hebben.

Als u wilt controleren of DNS-Lookup is ingeschakeld, gaat u naar:

- Klik op Configuratie > Configuratiegroepen
- Klik op het profiel van uw Edge-apparaten en bewerk het systeemprofiel



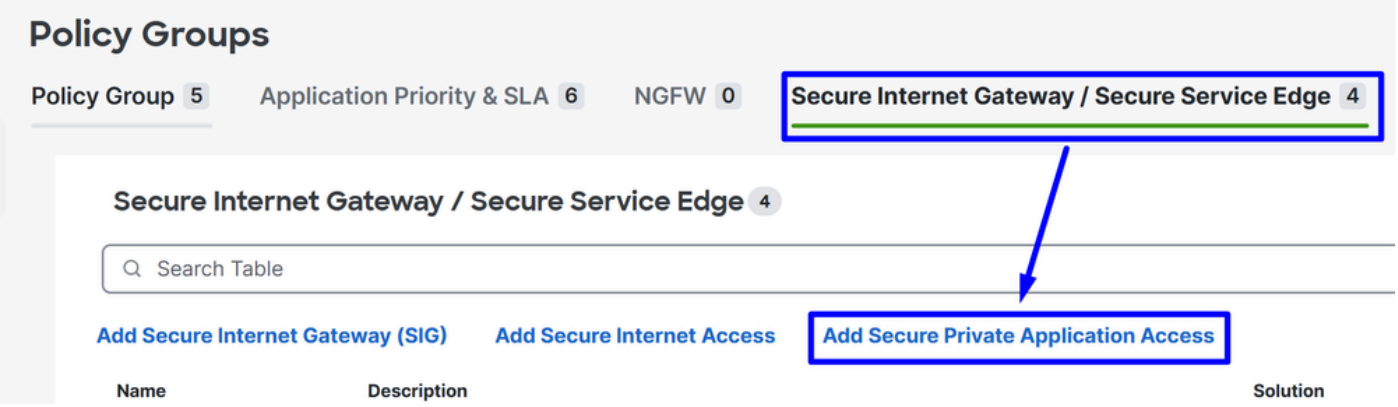
- Bewerk vervolgens de optie Globaal en zorg ervoor dat de optie Domeinresolutie is ingeschakeld



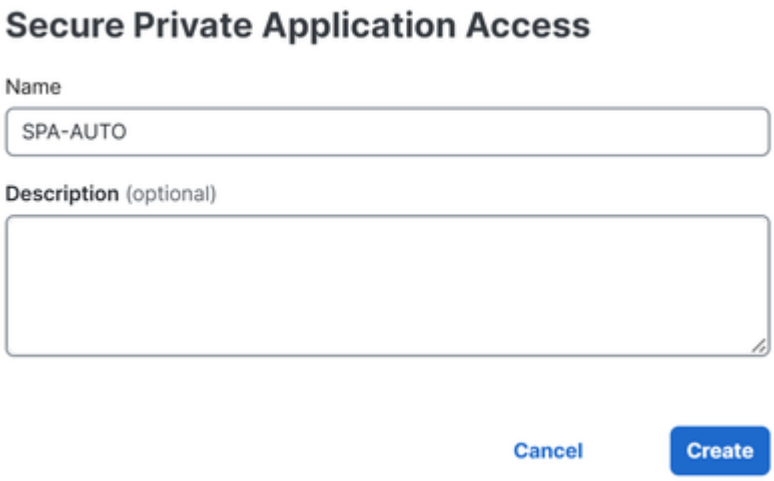
Beleidsgroep configureren

Navigeer naar Configuratie > Beleidsgroepen:

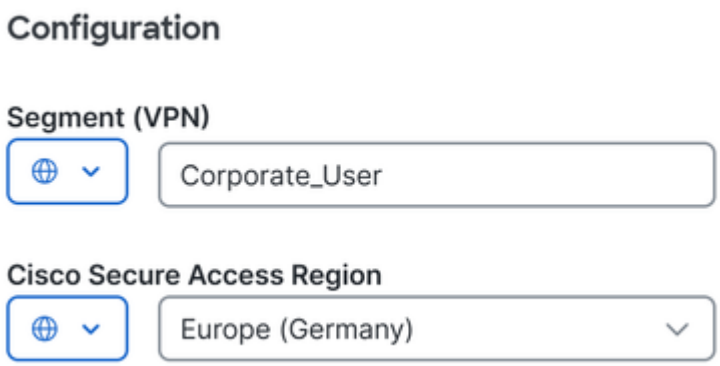
- Klik op Secure Internet Gateway / Secure Service Edge>*Add Secure Private Access*



- Configureer een naam en klik op Create



Met de volgende configuraties kunt u de tunnels maken nadat u de configuratie in uw Catalyst SD-WAN-randen hebt geïmplementeerd:

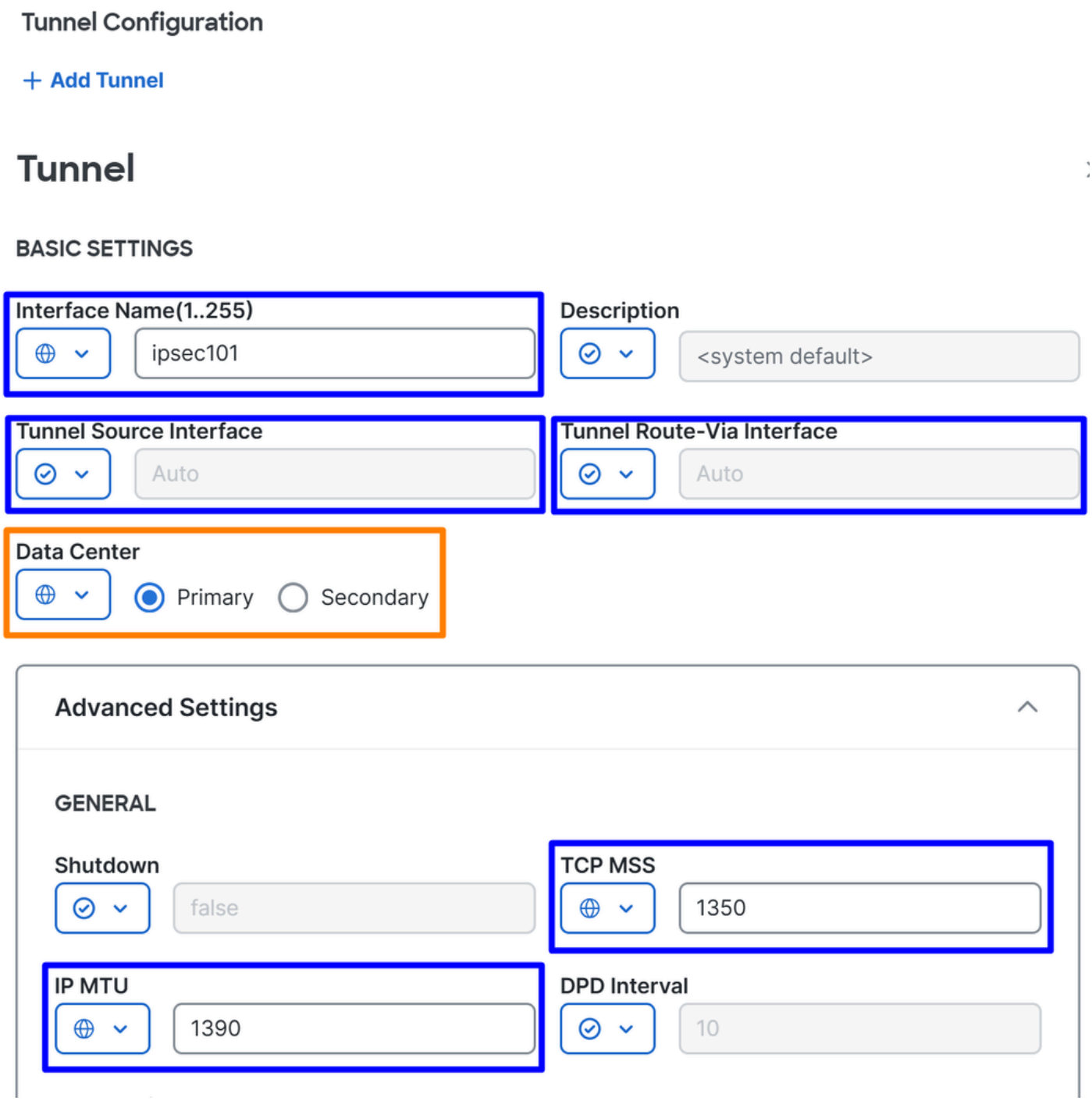


- Configuration
  - Segment (VPN): Kies de VRF die de toepassing(en) host die toegankelijk is via Secure Access
  - Cisco Secure Access Region: Kies de regio die het dichtst bij de SD-WAN-hub of -tak ligt waar de toepassingen worden gehost

Definieer vervolgens de tunnelconfiguratie. Tunnels die zijn gemaakt voor het primaire beveiligde toegangscentrum zijn actief, terwijl tunnels die zijn gemaakt voor het secundaire beveiligde

toegangscentrum fungeren als back-up.

Klik onder Tunnel Configuration klik + Add Tunnelop:



- Tunnel
  - Interface Name: Geef de tunnelnaam op, deze wordt automatisch bijgewerkt telkens wanneer een nieuwe tunnel wordt toegevoegd
  - Tunnel Source Interface: U hoeft deze instelling niet te wijzigen. Als Autohet systeem wordt verlaten, maakt het automatisch een loopback-interface met een /31-masker.
  - Tunnel Route-Via Interface: U hoeft deze instelling niet te wijzigen. Standaard gebruikt het de eerste NATed fysieke WAN-interface op de edge-router, maar deze kan worden gewijzigd als een specifieke WAN-interface vereist is
  - Data Center: Selecteer Primair of Secundair. Als de primaire tunnel al is geconfigureerd,

selecteert u Secundair. In normale scenario's kan de ene tunnel worden geconfigureerd als Primair en een andere als Secundair

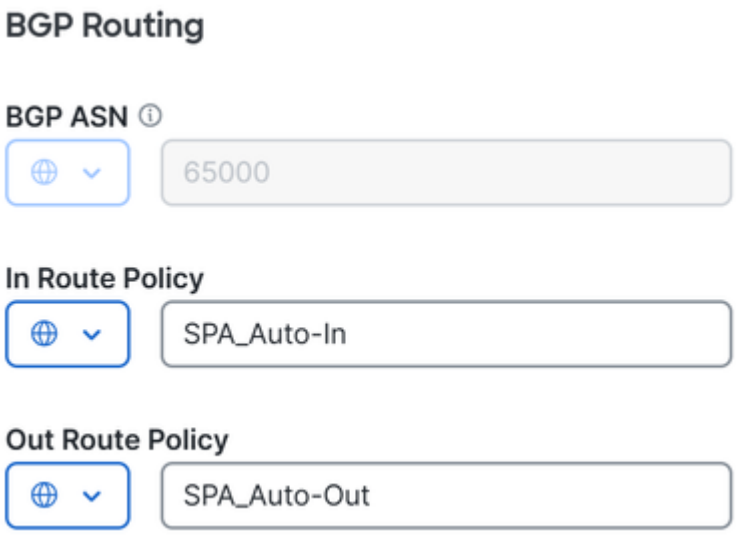
- Advanced Settings
  - IP MTUGebruik 1390
  - TCP MSSGebruik 1350

Opmerking: als u meerdere tunnels wilt maken om ECMP in te schakelen en de tunnelcapaciteit te verhogen, kunt u maximaal 10 actieve/10 back-uptunnels per router configureren. Dit levert tot 10 × 4 Gbps per NTG.

Interface Name	Description	Tunnel Source Interface	Tunnel Route-Via Interface	Data Center	Action	
ipsec101		Auto	Auto	Primary		
ipsec102		Auto	Auto	Secondary		
ipsec103		Auto	Auto	Primary		
ipsec104		Auto	Auto	Secondary		
ipsec105		Auto	Auto	Primary		
ipsec106		Auto	Auto	Secondary		
ipsec107		Auto	Auto	Primary		
ipsec108		Auto	Auto	Secondary		
ipsec109		Auto	Auto	Primary		MAXIMUM OF 10 TUNNELS PER HUB
ipsec110		Auto	Auto	Secondary		10 x 1 Primary
ipsec111		Auto	Auto	Primary		10 x 1 Secondary
ipsec112		Auto	Auto	Secondary		
ipsec113		Auto	Auto	Primary		
ipsec114		Auto	Auto	Secondary		
ipsec115		Auto	Auto	Primary		
ipsec116		Auto	Auto	Secondary		
ipsec117		Auto	Auto	Primary		
ipsec118		Auto	Auto	Secondary		
ipsec119		Auto	Auto	Primary		
ipsec120		Auto	Auto	Secondary		

Opmerking: Als u meerdere tunnels per router implementeert, moet u ervoor zorgen dat de transportinterface de totale bandbreedte van alle actieve tunnels samen kan behouden. Als twee tunnels naar verwachting elk maximaal 1 Gbps vervoeren, moet de transportverbinding ten minste 2 Gbps doorvoer ondersteunen.

Nadat de tunnels zijn geconfigureerd, gaat u verder met de BGP-configuratie.



- **BGP Routing**
  - BGP ASN: AS-nummer opgeven voor de SD-WAN-hub. De AS 64512 is gereserveerd voor beveiligde toegang en kan niet worden gebruikt. Voor meer informatie over BGP, zie
  - In Route Policy: Het systeem maakt automatisch dit inkomende routebeleid met een deny all instructie om routeringsproblemen te voorkomen. Het moet handmatig worden gewijzigd door middel van een CLI Add-On Template protocol om de juiste routes toe te staan/te weigeren.
  - Out Route Policy: Het systeem maakt dit uitgaande routebeleid met een deny all verklaring om routeringsproblemen te voorkomen. Het moet handmatig worden bewerkt via een CLI Add-On Template link om de juiste routes toe te staan/te weigeren.

Waarschuwing: vanaf november 2025 gebruiken alle nieuw opgerichte organisaties voor beveiligde toegang standaard de openbare ASN 32644 voor BGP-peering in netwerktunnelgroepen. Bestaande organisaties die vóór november 2025 zijn opgericht, blijven gebruikmaken van de private ASN 64512 die voorheen was gereserveerd voor Secure Access BGP-peers. Als het privé-AS-nummer 64512 is toegewezen aan een apparaat in uw netwerk, kan het niet peer met een netwerktunnelgroep die is geconfigureerd voor Peer (Secure Access) BGP AS 64512.

De volgende BGP en route-map configuratie wordt automatisch gemaakt voor elke BGP-buur nadat u het nieuwe beleid hebt Deploy ingevoerd in uw Policy Groupwebsite.

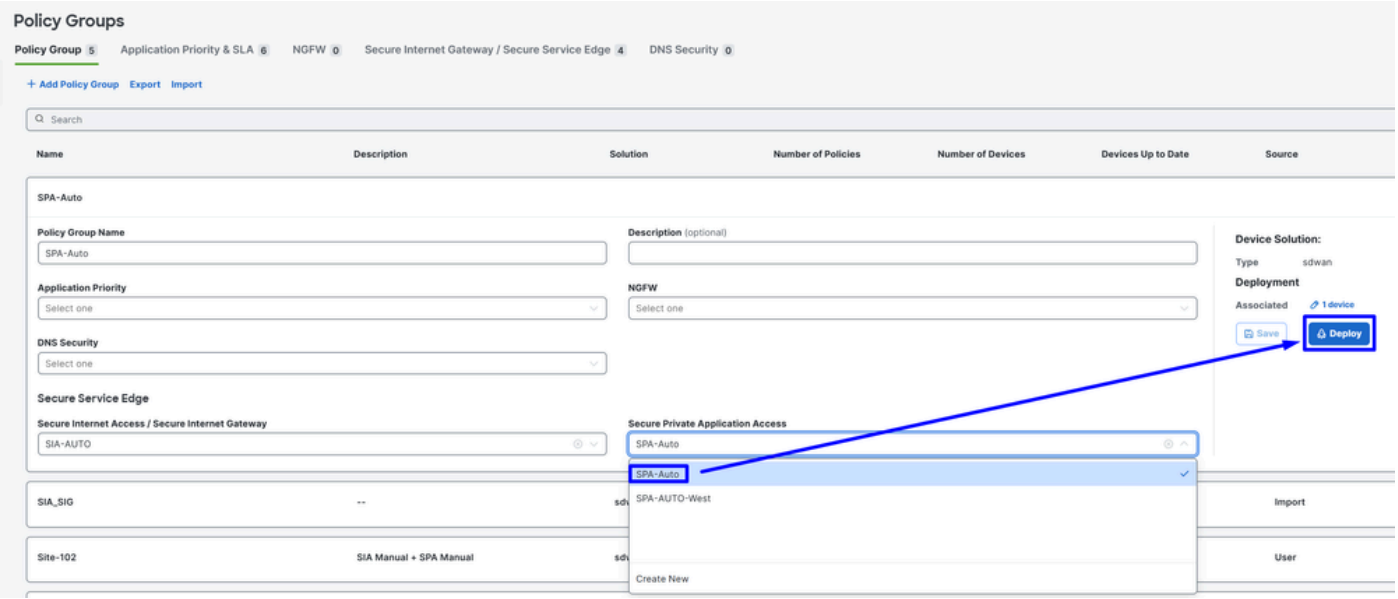
```
route-map SPA_Auto-In deny 65534
 description Default Deny Configured from Secure Private Application Access feature
route-map SPA_Auto-Out deny 65534
 description Default Deny Configured from Secure Private Application Access feature

R104#sh run | s r b
router bgp 65000
```

```
bgp log-neighbor-changes
!
address-family ipv4 vrf 10
 neighbor 169.254.0.3 remote-as 64512
 neighbor 169.254.0.3 activate
 neighbor 169.254.0.3 send-community both
 neighbor 169.254.0.3 route-map SPA_Auto-In in
 neighbor 169.254.0.3 route-map SPA_Auto-Out out
 ...
 maximum-paths 32
exit-address-family
```

Hierna klikt u op Save en gaat u verder met de beleidsimplementatie om de tunnels naar boven te brengen.

- Klik op Configuration > Policy Groups
- Kies onder uw Policy > Secure Service Edge > Secure Private Application Access en klik op het recente profiel dat is gemaakt voor SPA.
- KlikDeployom te voltooien



Voer de volgende stappen uit om inSecure Accessste controleren:

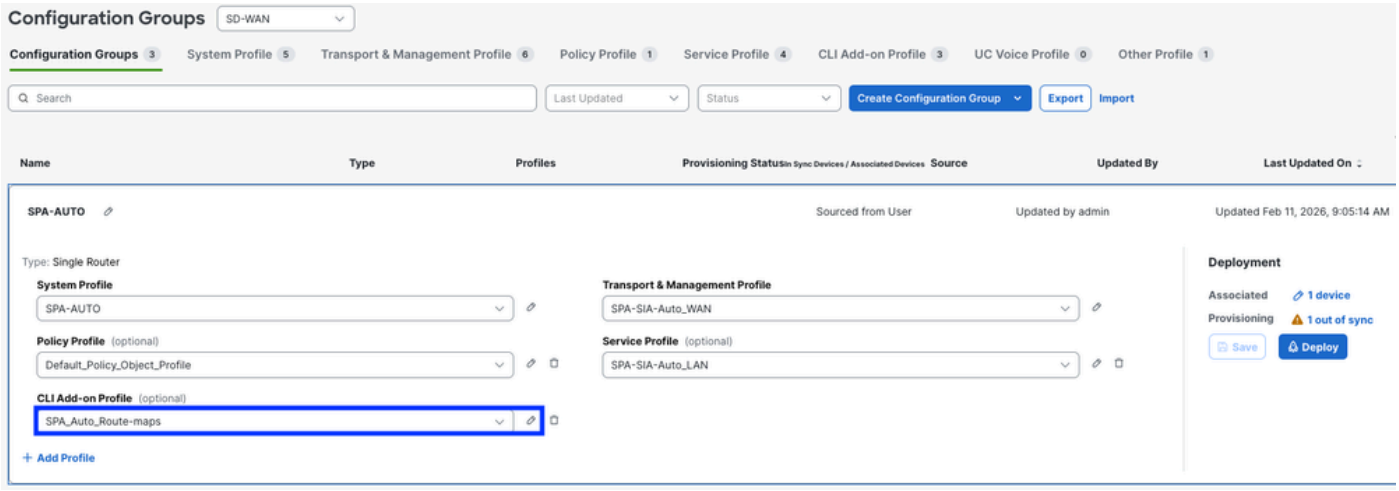
- Klik op Connect> Network Connections

TUNNELINRICHTING

Routering configureren

Navigeer naar Configure > Configuration Groups

- Klik op je Configuration Group website en maak/bewerk je CLI Add-on Profile



Als u BGP-routes wilt laten uitwisselen, gebruikt u de eerder geconfigureerde In Route Policy en **Out Route Policy**geconfigureerde. U kunt een basisvoorbeeld vinden voor de configuratie van de CLI Add-On route. Deze sjabloon biedt een startpunt en moet naar behoefte worden aangepast:

```
ip bgp-community new-format
ip prefix-list ALL-ROUTES seq 5 permit 0.0.0.0/0 le 32

route-map SPA_Auto-In permit 10
match ip address prefix-list ALL-ROUTES
route-map SPA_Auto-In deny 65534
description Default Deny Configured from Secure Private Application Access feature

route-map SPA_Auto-Out permit 10
match ip address prefix-list ALL-ROUTES
description Default Deny Configured from Secure Private Application Access feature
route-map SPA_Auto-Out deny 65534
description Default Deny Configured from Secure Private Application Access feature

router bgp 65000
bgp log-neighbor-changes
!
```

```
address-family ipv4 vrf 10
network 172.16.104.0 mask 255.255.255.0
```

Waarschuwing: Een zorgvuldige planning is vereist bij het definiëren van de netwerken die zijn toegestaan in en uit via BGP routekaarten. Het toestaan van alle routes, zoals getoond in het bovenstaande voorbeeld, kan onbedoeld routegedrag introduceren. Geef voor een optimale implementatie expliciet alleen de benodigde netwerken op in uw routekaarten om gecontroleerde en voorspelbare routeringsuitkomsten te garanderen

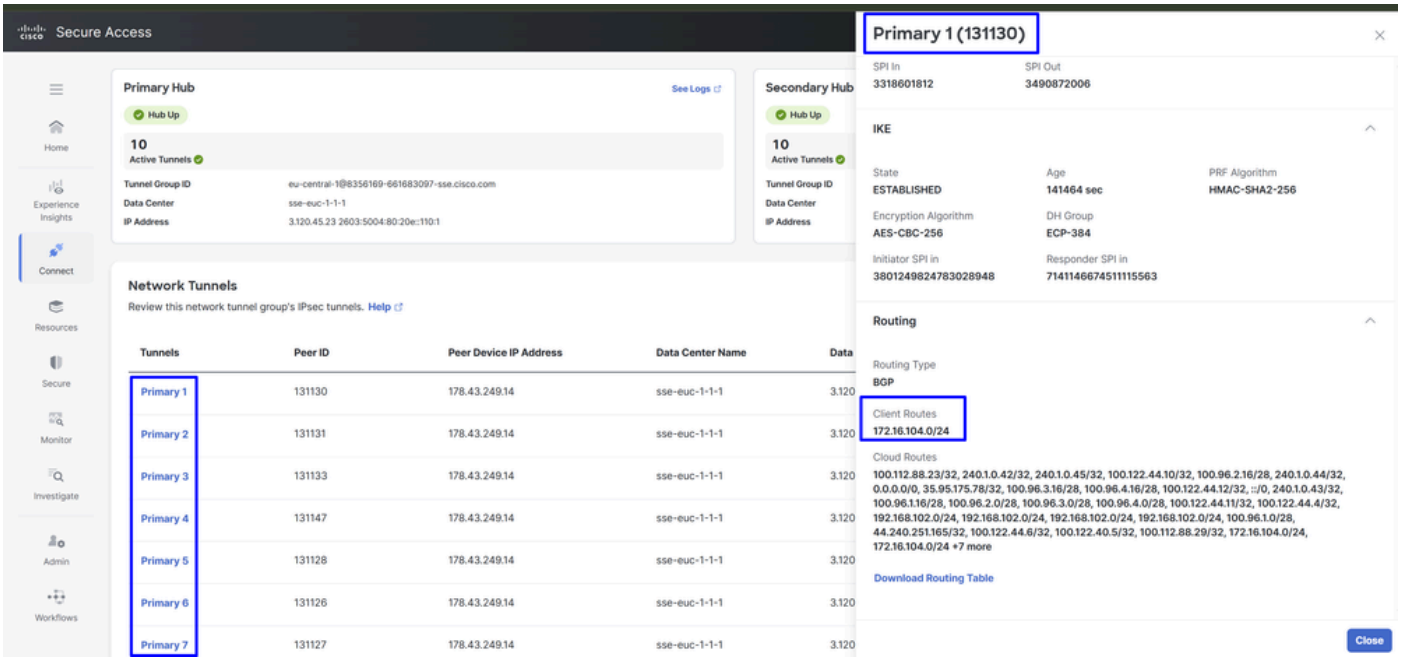
---

Nu kunt u doorgaan naar Deploy the changes

Om te controleren of BGP-routes zijn ontvangenSecure Access, controleert u de volgende stappen:

- Klik op Connect> Network Connections > en Network Tunnel Groups select de NTG-naam

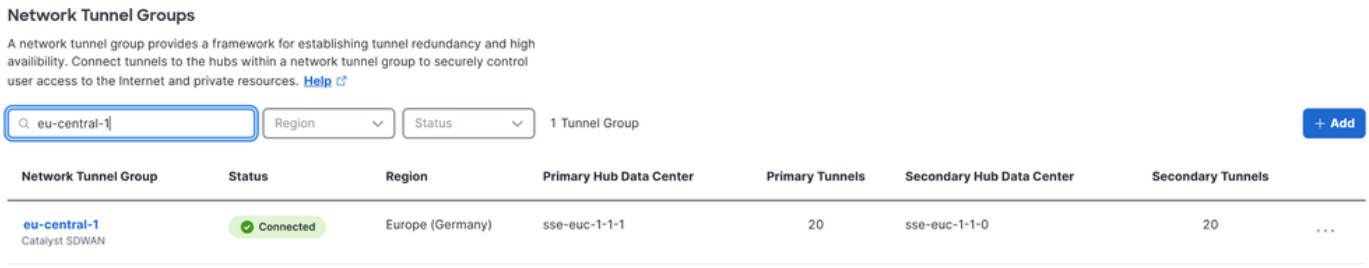
ROUTERENDE INRICHTING



Opmerking: In dit voorbeeld wordt het subnet voor zakelijke gebruikers 172.16.104.0/24 geadverteerd voor Secure Access via BGP. Dit maakt een goede routering tussen Catalyst SD-WAN en de SSE-omgeving mogelijk.

Hetzelfde beleid kan worden toegepast op beide WAN-randen in de Catalyst SD-WAN-hubs, wat resulteert in 20 actieve tunnels en 20 standby-tunnels. Het totale aantal tunnels hangt af van het aantal dat op elke rand is geconfigureerd. Elke router die is aangesloten op beide Secure Access-hubs (Hub 1 en Hub 2) vormt een ECMP-paar in alle gevestigde tunnels.

Als bijvoorbeeld Catalyst SD-WAN Edge 1 10 tunnels heeft en Catalyst SD-WAN Edge 2 10 tunnels, vormt Secure Access ECMP in de 20 actieve tunnels. Hetzelfde geldt voor de secundaire SSE-hub.

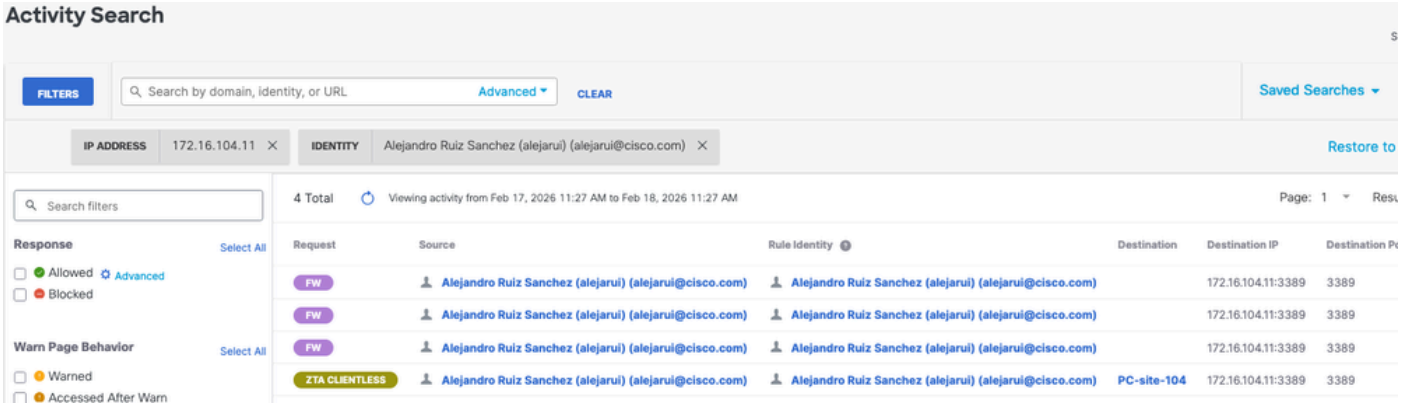


Verifiëren

Om te controleren of het verkeer via Cisco Secure Access verloopt, navigeert u naar Eventsof Activity Search of Network-Wide Path Insightsen filtert u op uw tunnelidentiteit:

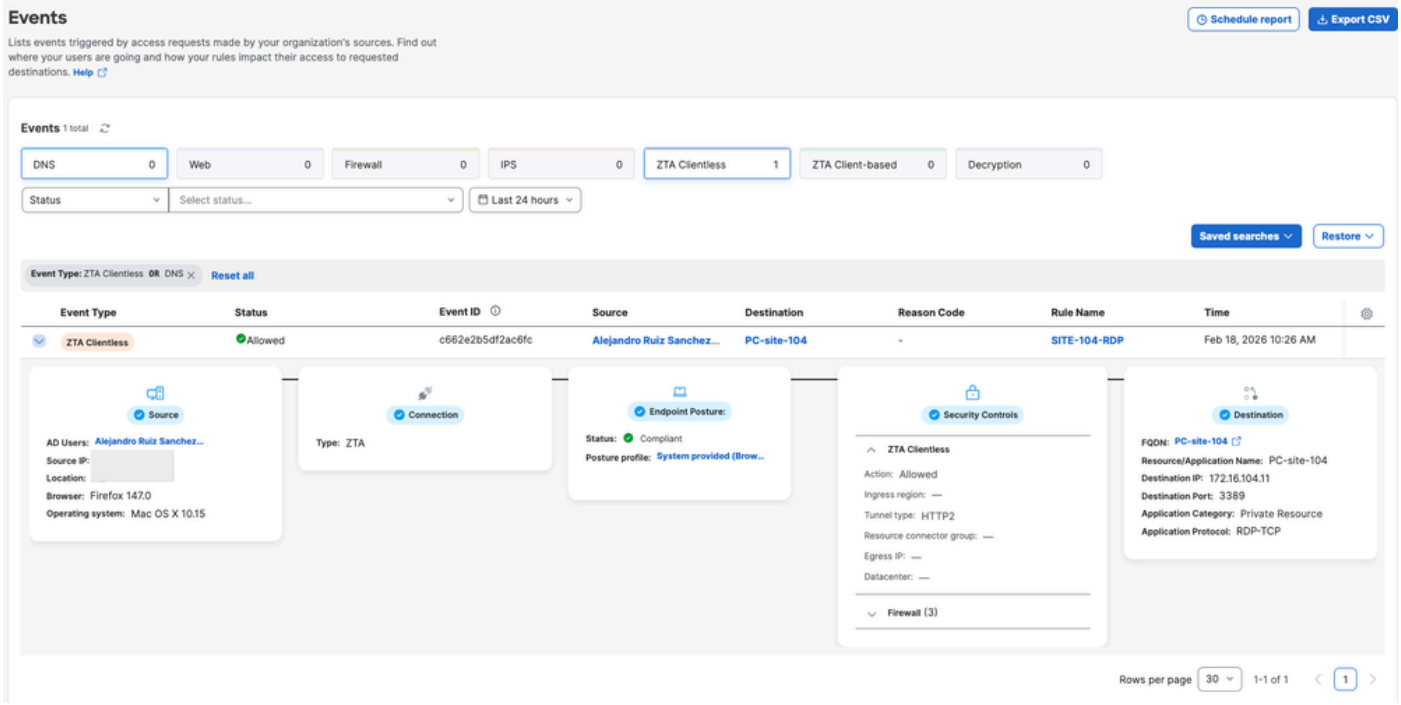
Veilige toegang - zoeken naar activiteiten

Navigeer naar Monitor>Activity Search :



Veilige toegang - Evenementen

Navigeer naar Monitor>Events:

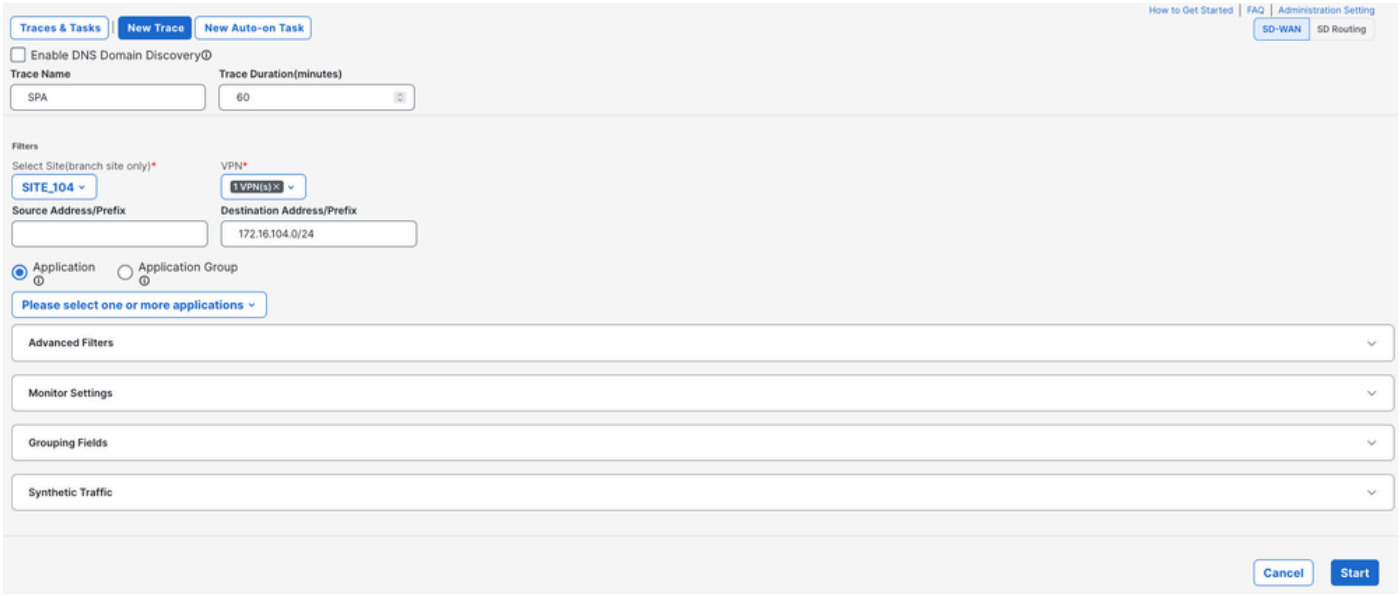


Opmerking: zorg ervoor dat uw standaardbeleid met logboekregistratie is ingeschakeld, standaard is uitgeschakeld.

Catalyst SD-WAN Manager - inzicht in netwerkbrede paden

Navigeer naar Catalyst SD-WAN Manager:

- Klik op Tools> Network-Wide Path Insights
- Klik op New Trace

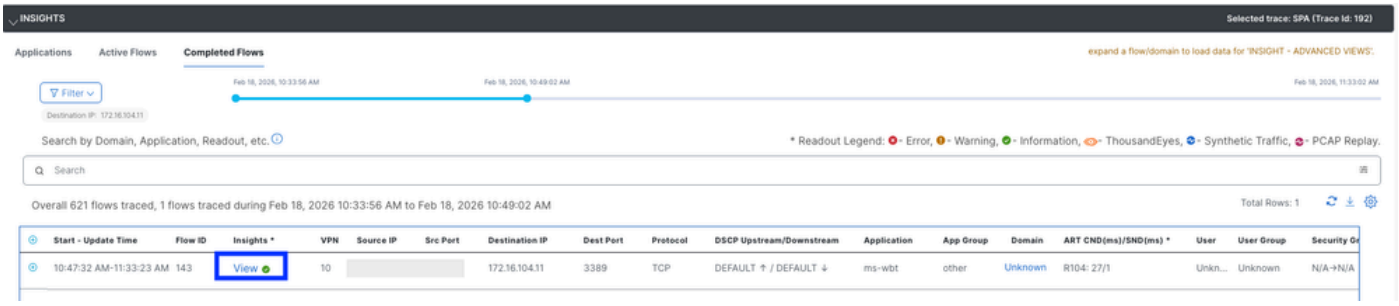


- Trace Name: (optioneel) Trace-naam opgeven

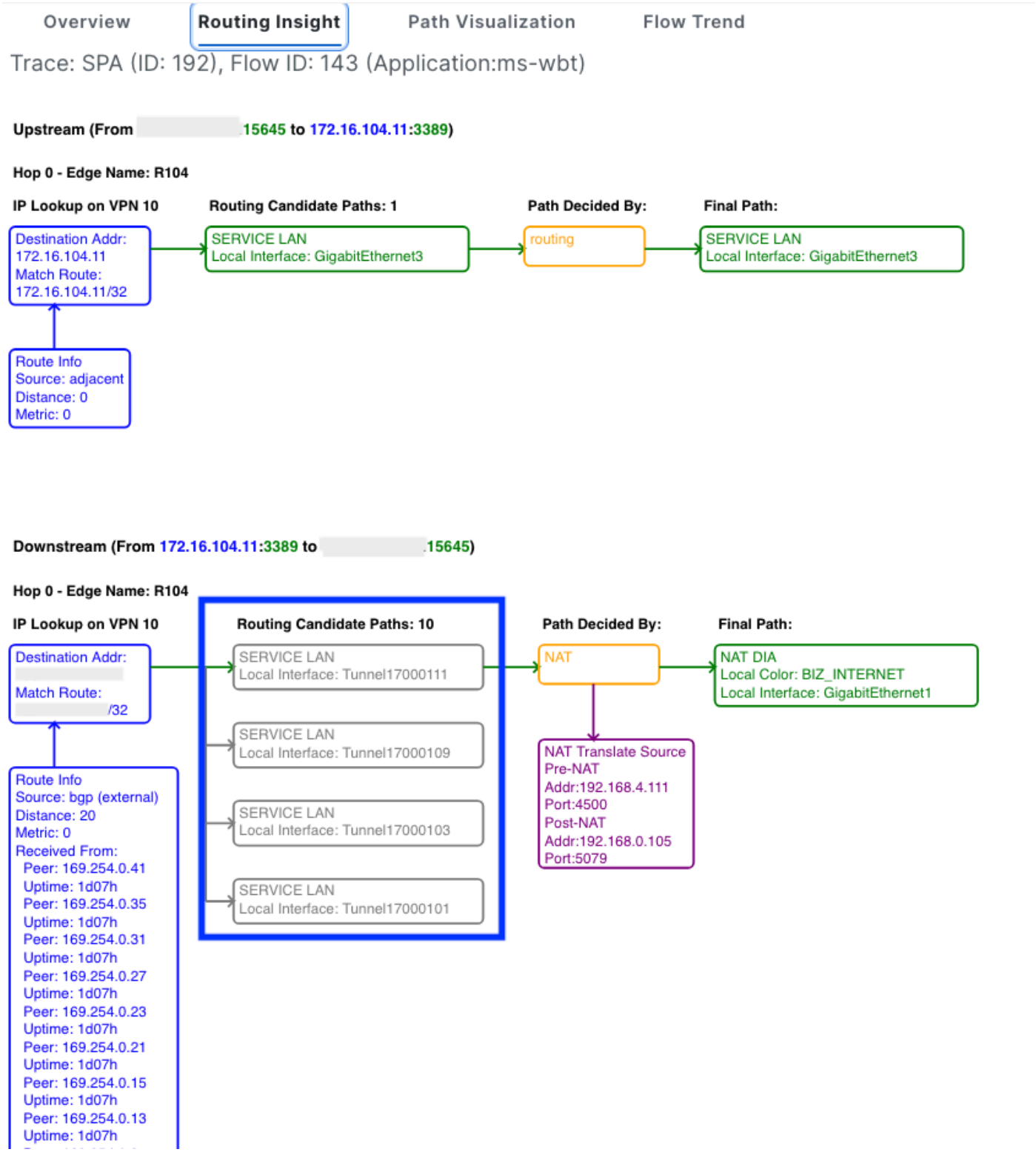
- Site: Kies de site waar de privébron zich bevindt
- VPN: Kies de VPN-ID waar de privébron zich bevindt
- Source/Destination Address: (Optioneel) Voer het IP-adres in of laat het leeg om al het verkeer vast te leggen dat is gefilterd op basis van **Site**en VPNgekozen

Start het spoor

Zoek de verkeersstroom en klik op Weergave in de kolom Inzichten



De kolom Inzichten routering geeft de kandidaatpaden weer en geeft de IPSec-tunnels voor beveiligde toegang weer



Gerelateerde informatie

- Cisco Technical Support en downloads
- Cisco Secure Access Help Center
- Cisco SASE-ontwerphandleiding
- Beveiligde toegang configureren met automatische SD-WAN-tunnels voor beveiligde internettoegang

- Cisco Catalyst SD-WAN Security Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x
- Cisco SASE-oplossing: Cisco Catalyst SD-WAN geïntegreerd met Cisco Secure Access in één oogopslag

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.