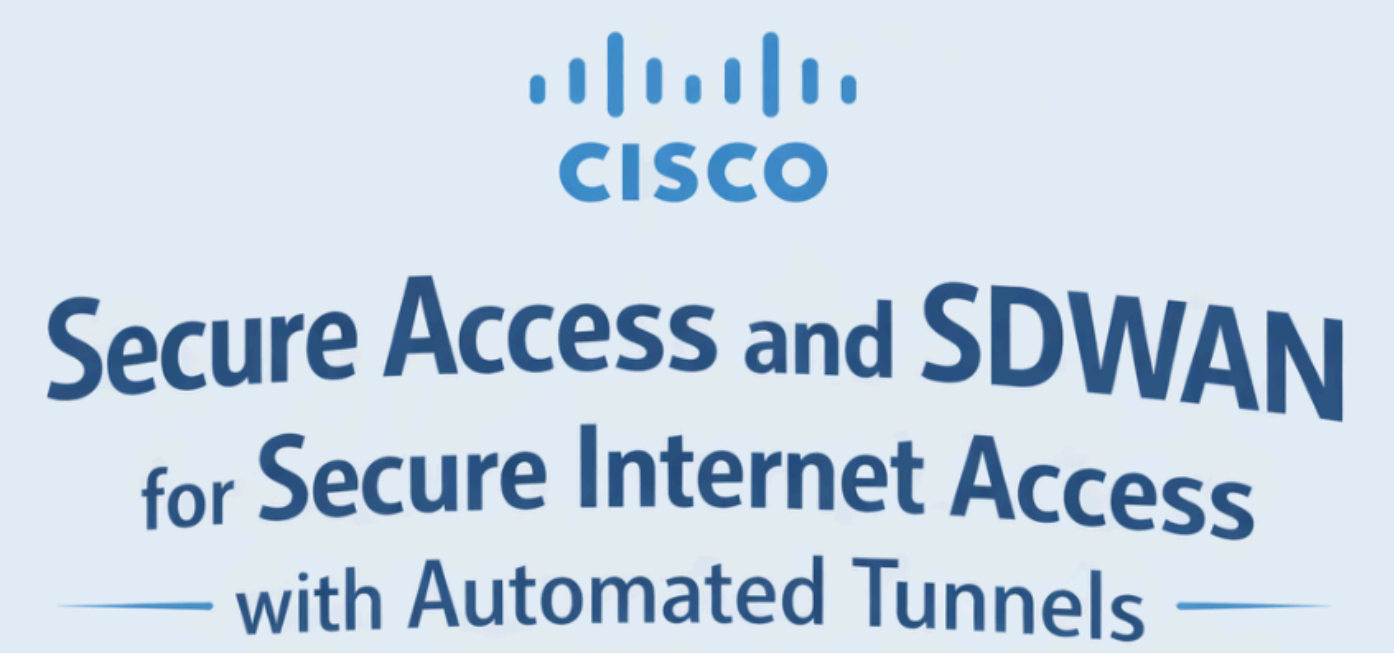
Beveiligde toegang configureren met automatische SD-WAN-tunnels voor beveiligde internettoegang

Inhoud

Inleiding

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



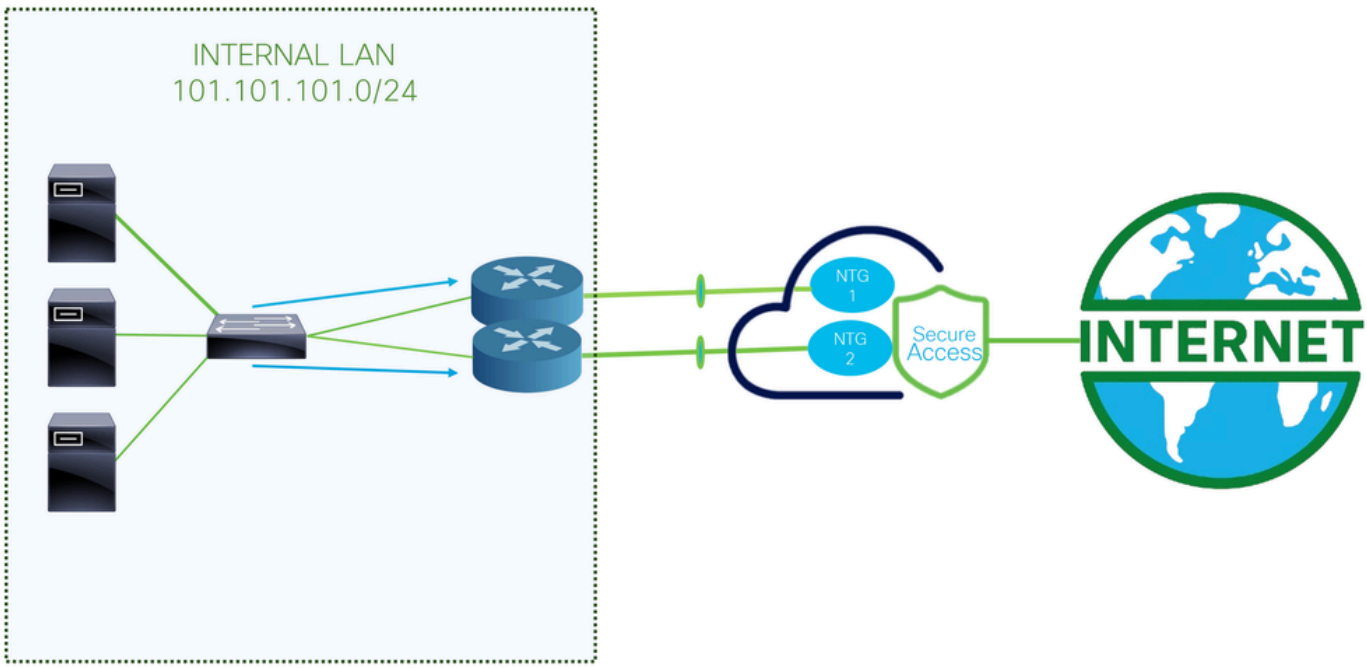
Achtergrondinformatie

Naarmate organisaties steeds meer cloud-gebaseerde applicaties gebruiken en gedistribueerde werknemers ondersteunen, moeten netwerkarchitecturen evolueren om veilige, betrouwbare en schaalbare toegang tot bronnen te bieden. Secure Access Service Edge (SASE) is een framework dat netwerken en beveiliging converteert naar één cloud-geleverde service, waarbij SD-WAN-mogelijkheden worden gecombineerd met geavanceerde beveiligingsfuncties zoals Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), DNS-layer beveiliging, Zero Trust Network Access (ZTNA) of geïntegreerde VPN voor beveiligde externe toegang.

De integratie van Cisco Secure Access met SD-WAN via geautomatiseerde tunnels stelt organisaties in staat om internetverkeer veilig en efficiënt te routeren. SD-WAN biedt intelligente padselectie en geoptimaliseerde connectiviteit op gedistribueerde locaties, terwijl Cisco Secure Access ervoor zorgt dat al het verkeer wordt geïnspecteerd en beschermd volgens het beveiligingsbeleid van het bedrijf voordat het internet wordt bereikt.

Door tunnelconfiguratie tussen SD-WAN-apparaten en Secure Access te automatiseren, kunnen organisaties de implementatie vereenvoudigen, de schaalbaarheid verbeteren en zorgen voor consistente handhaving van de beveiliging voor gebruikers, ongeacht waar ze zich bevinden. Deze integratie is een belangrijk onderdeel van een moderne SASE-architectuur, die veilige internettoegang mogelijk maakt voor filialen, externe sites en mobiele gebruikers.

Netwerkdiagram



Dit is de architectuur die voor dit configuratievoorbeeld wordt gebruikt. Zoals je kunt zien zijn er twee edge routers:

Als u ervoor kiest om het beleid op twee verschillende apparaten te implementeren, wordt voor elke router een NTG geconfigureerd en wordt NAT ingeschakeld aan de kant van Secure Access. Hierdoor kunnen beide routers verkeer van dezelfde bron door de tunnels sturen. Normaal gesproken is dit niet toegestaan, maar door de NAT-optie voor deze tunnels in te schakelen, kunnen twee edge-routers verkeer verzenden dat afkomstig is van hetzelfde bronadres.

Voorwaarden

Vereisten

- Veilige toegang tot kennis
- Cisco Catalyst SD-WAN Manager Release 20.15.1 en Cisco IOS XE Catalyst SD-WAN Release 17.15.1 of hoger
- Tussentijdse kennis van routing en switching
- ECMP-kennis
- VPN-kennis

Gebruikte componenten

- Secure Access-huurder
- Catalyst SD-WAN Manager Release 20.18.1 en Cisco IOS XE Catalyst SD-WAN Release 17.18.1
- 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

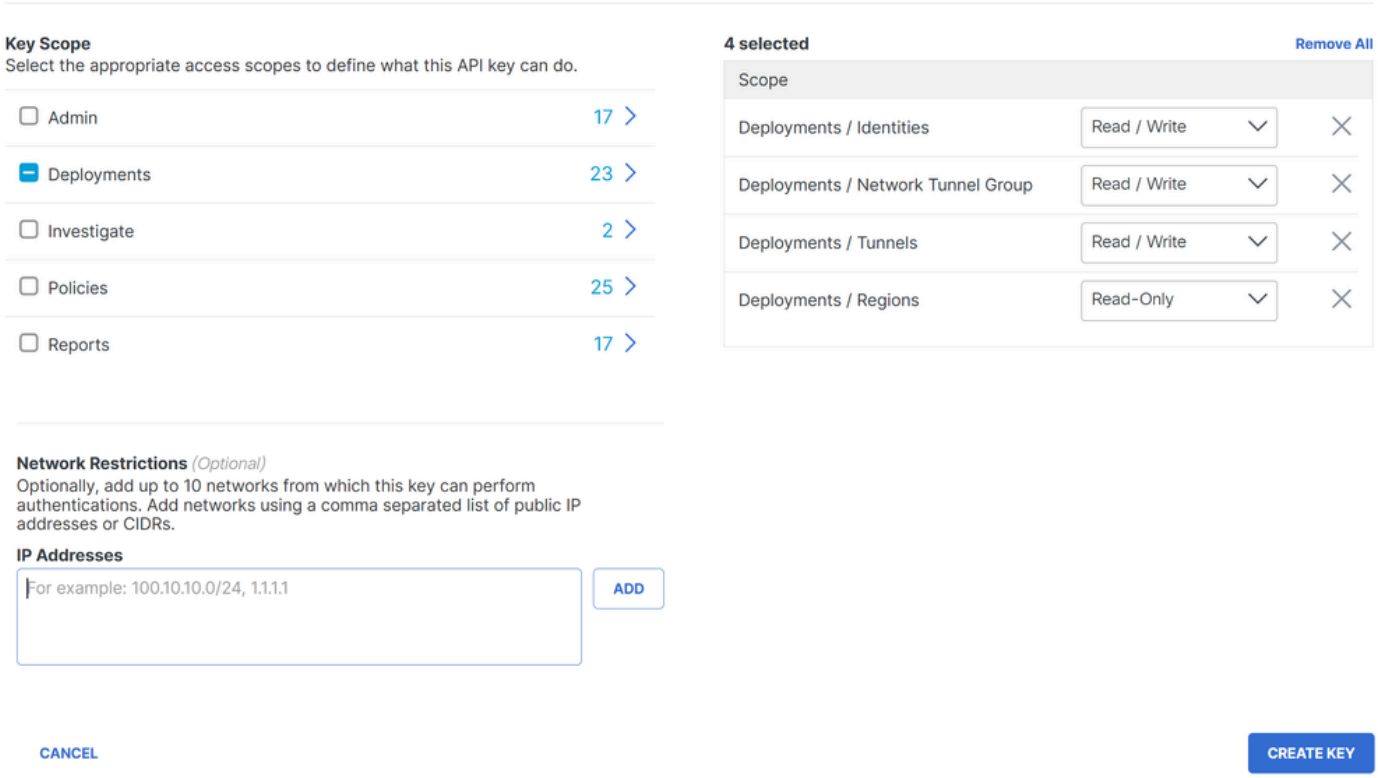
Beveiligde toegangsconfiguratie

API maken

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

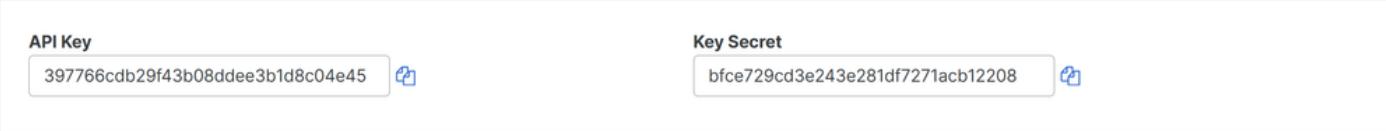
Navigeer naar het Secure Access Dashboard.

- 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.

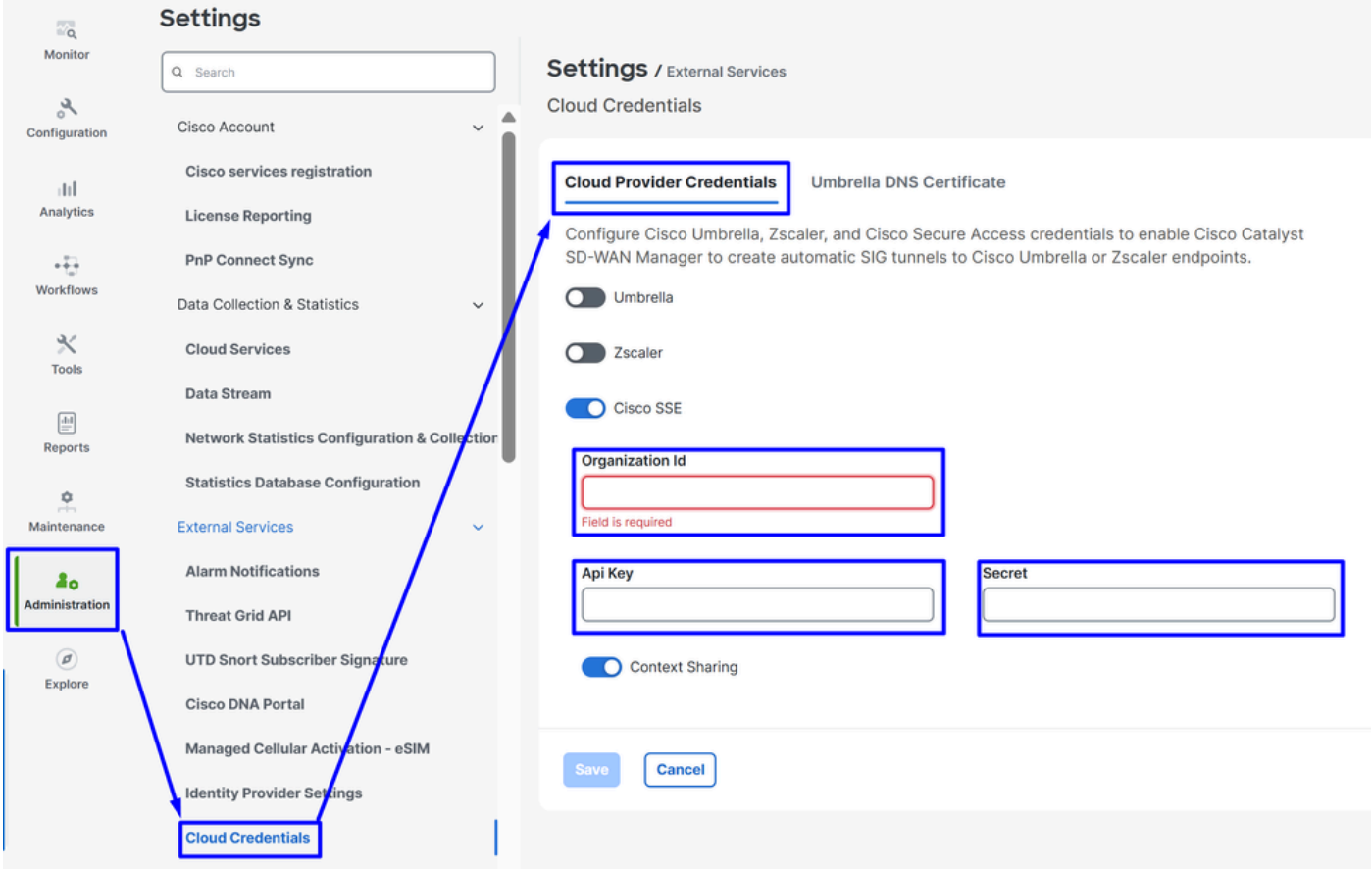
Om vervolgens te finaliseren klik ACCEPT AND CLOSE.

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



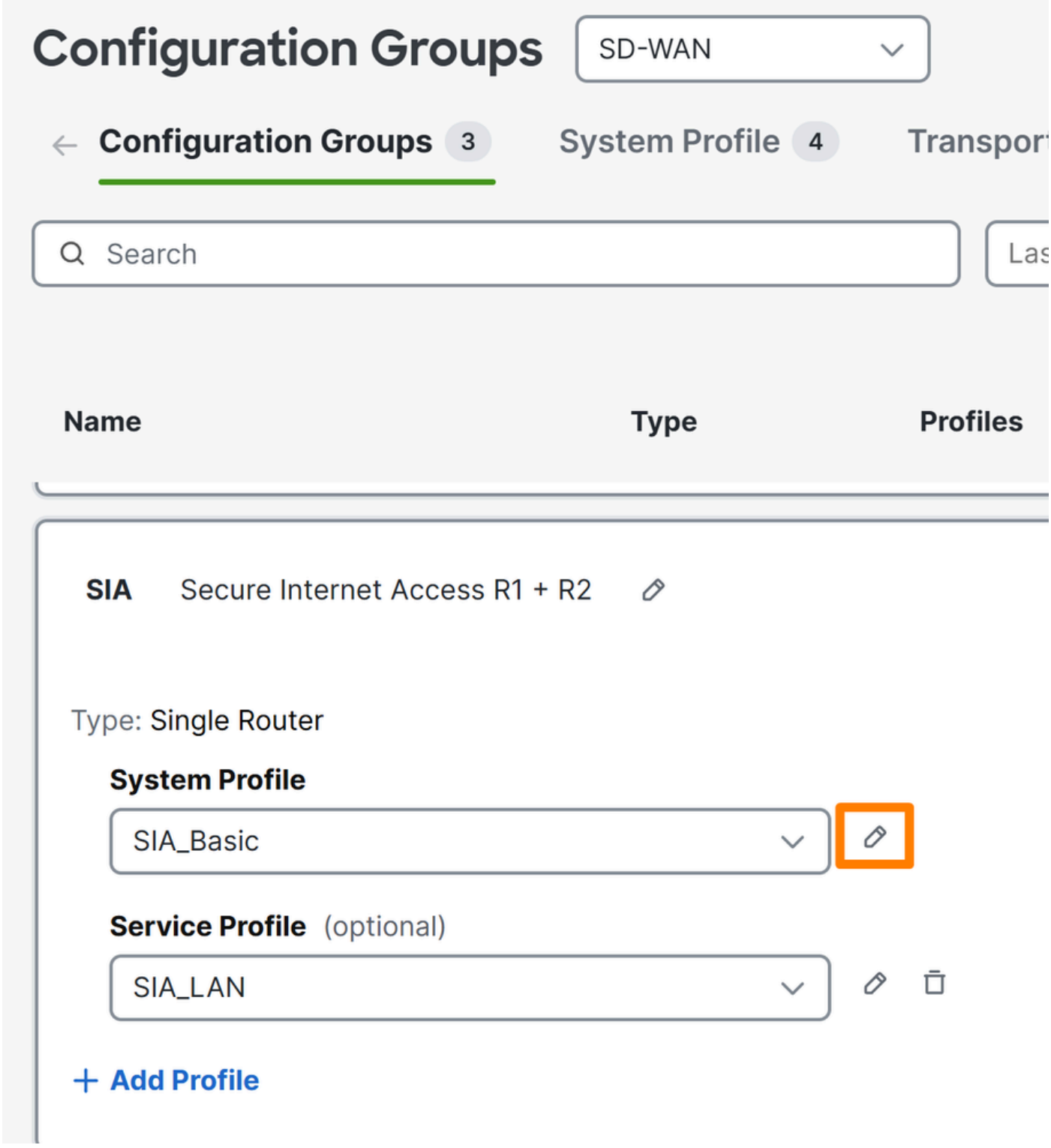
- Organization ID: U kunt dat uit de URL van uw SSE Dashboard https://dashboard.sse.cisco.com/org/xxxxx
- Api Key: Kopieer het vanuit de stap Beveiligde toegangsconfiguratie
- Secret: Kopieer het vanuit de stap Beveiligde toegangsconfiguratie

Daarna klik je op de Save knop.

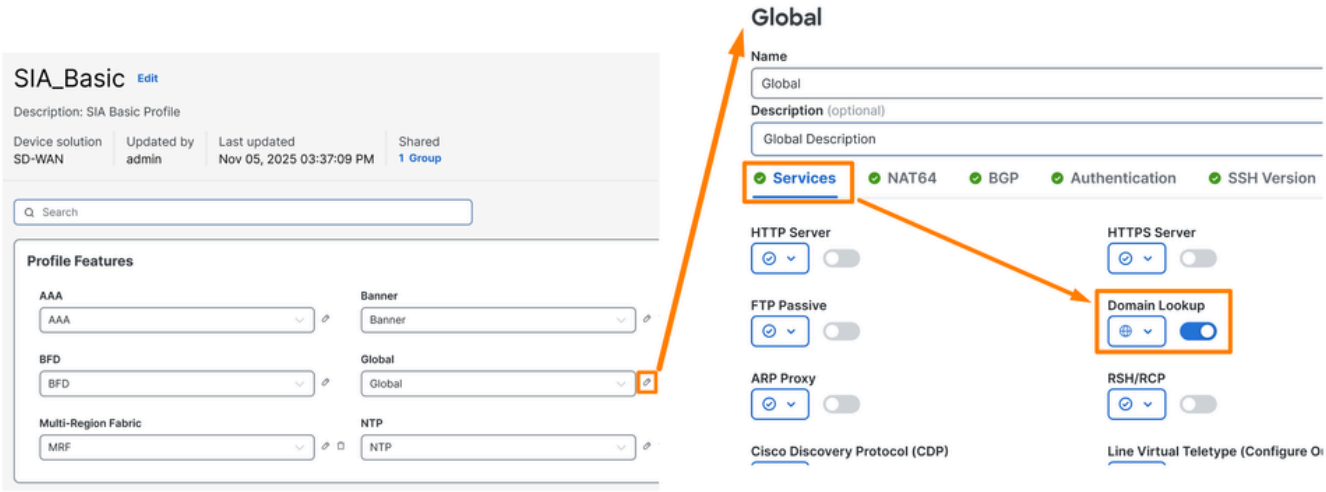
Opmerking: Voordat u verder gaat met de volgende stappen, moet u ervoor zorgen dat de SD-WAN-manager en de Catalyst SD-WAN-randen DNS-resolutie en internettoegang hebben.

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



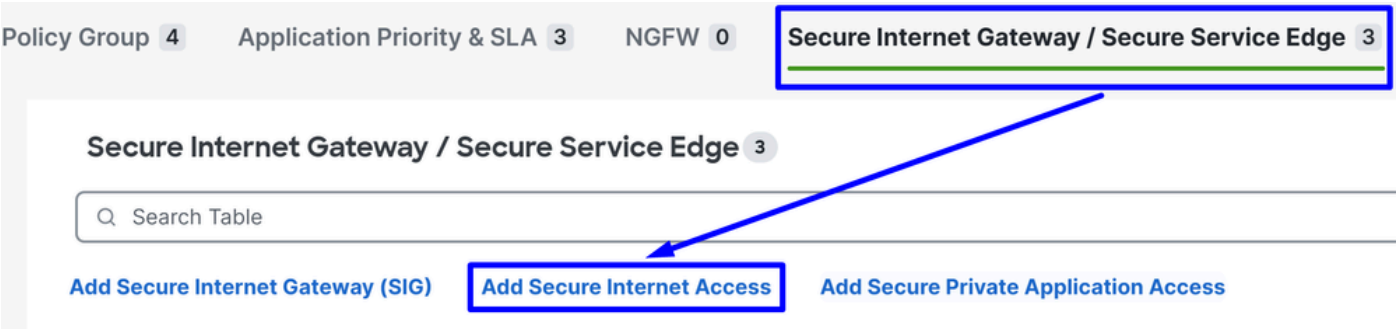
- Bewerk vervolgens de optie Globaal en zorg ervoor dat de optie Domeinresolutie is ingeschakeld



Beleidsgroep configureren

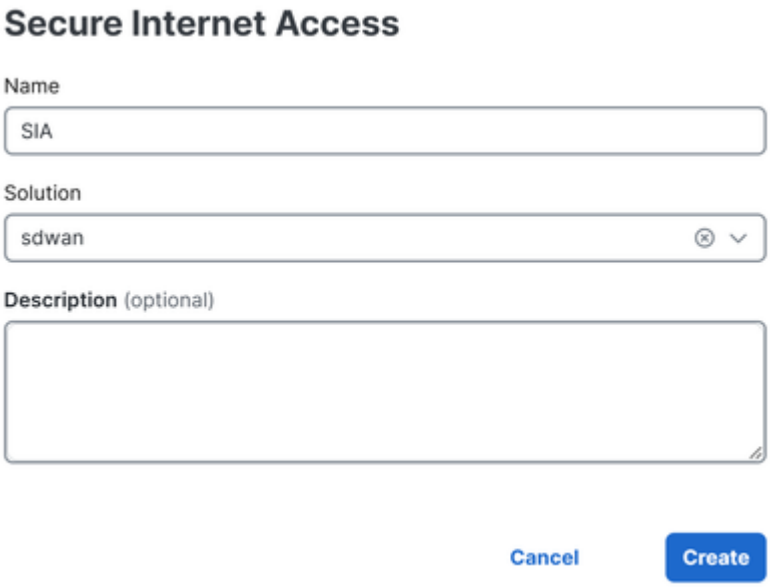
Navigeer naar Configuratie > Beleidsgroepen:

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

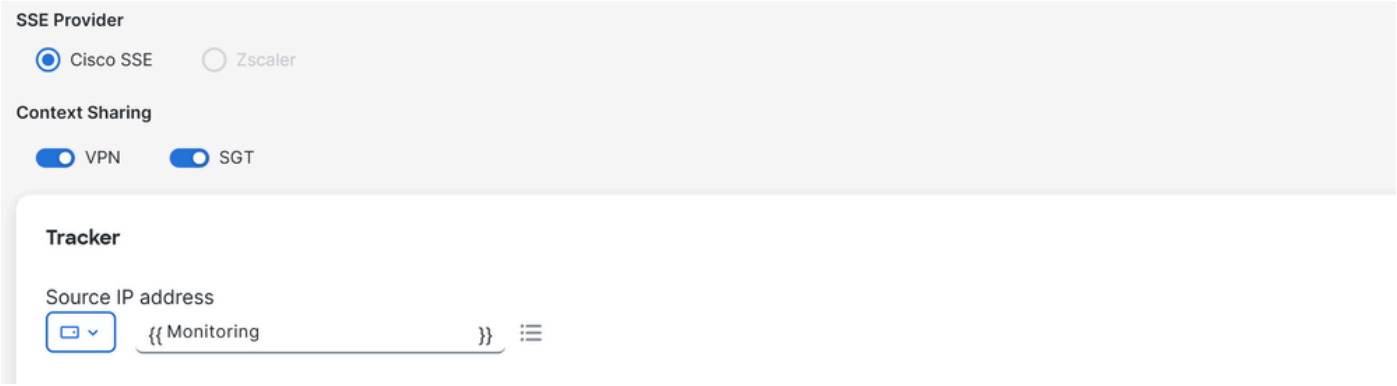


Opmerking: in releases lager dan 20,18 wordt deze optie Secure Service Edge (SSE) toevoegen genoemd

- Configureer een naam, oplossing en klik op Create

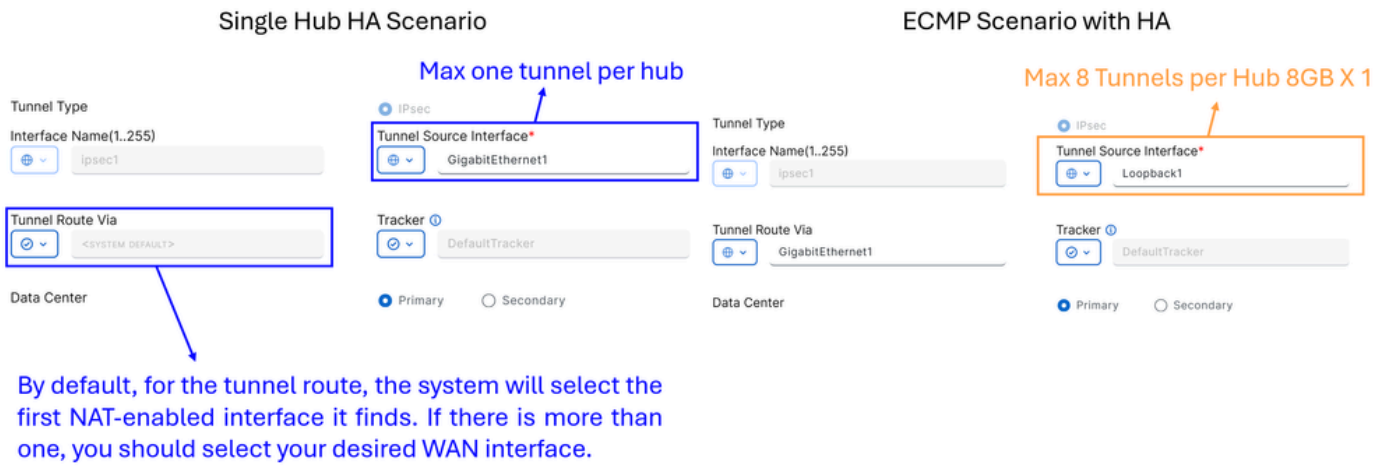


Met de volgende configuraties kunt u de tunnels maken nadat u de configuratie in uw Catalyst SD-WAN-randen hebt geïmplementeerd:



- SSE Provider: SSE
- Context SharingKies: VPN of/en SGT is afhankelijk van uw behoeften
- Tracker
  - **Source IP Address**: Kies Apparaatspecifiek (hiermee kunt u het per apparaat wijzigen en de gebruikssituatie voor het apparaat in de implementatiefase identificeren)

Onder de Configuration trede zet je de tunnels:



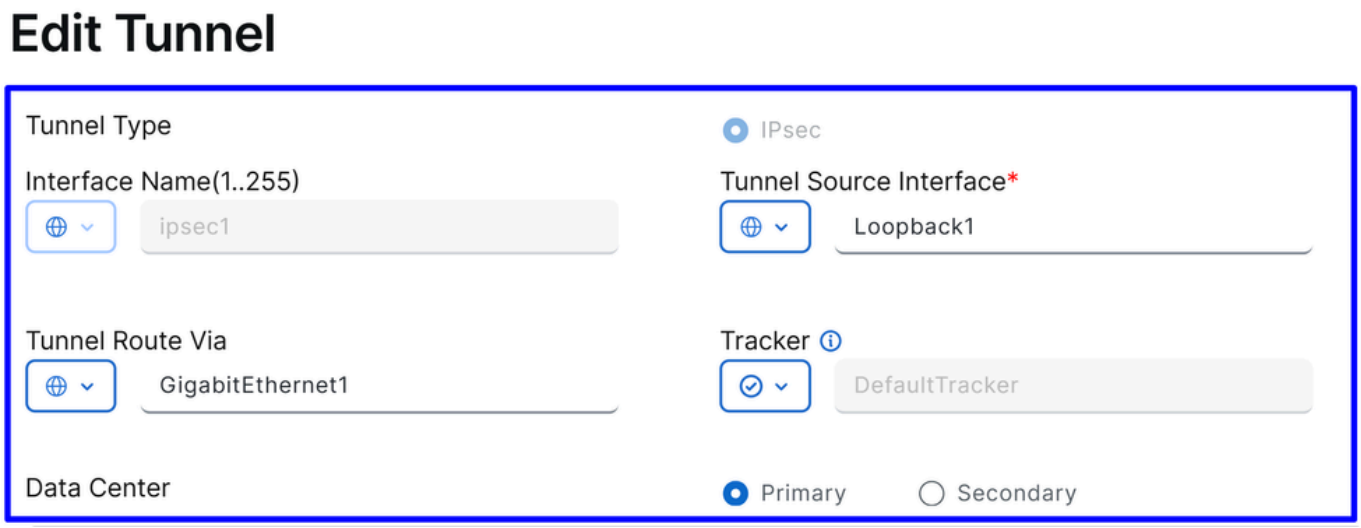
- **Single Hub HA Scenario**: In dit scenario kunt u hoge beschikbaarheid configureren met de ene NTG als actief en de andere als passief, met een maximale doorvoer van 1 Gbps per NTG
- ECMP Scenario with HA: In dit scenario kunt u maximaal 8 tunnels per hub configureren, met ondersteuning van in totaal maximaal 16 tunnels per NTG. Deze opstelling zorgt voor een hogere doorvoer over de tunnels

---

Opmerking: als uw netwerkinterfaces een doorvoer hebben van meer dan 1 Gbps en u schaalbaarheid nodig hebt, moet u loopback-interfaces gebruiken. Anders kunt u standaardinterfaces op uw apparaat gebruiken. Dit is om ECMP in te schakelen vanaf de kant met beveiligde toegang.

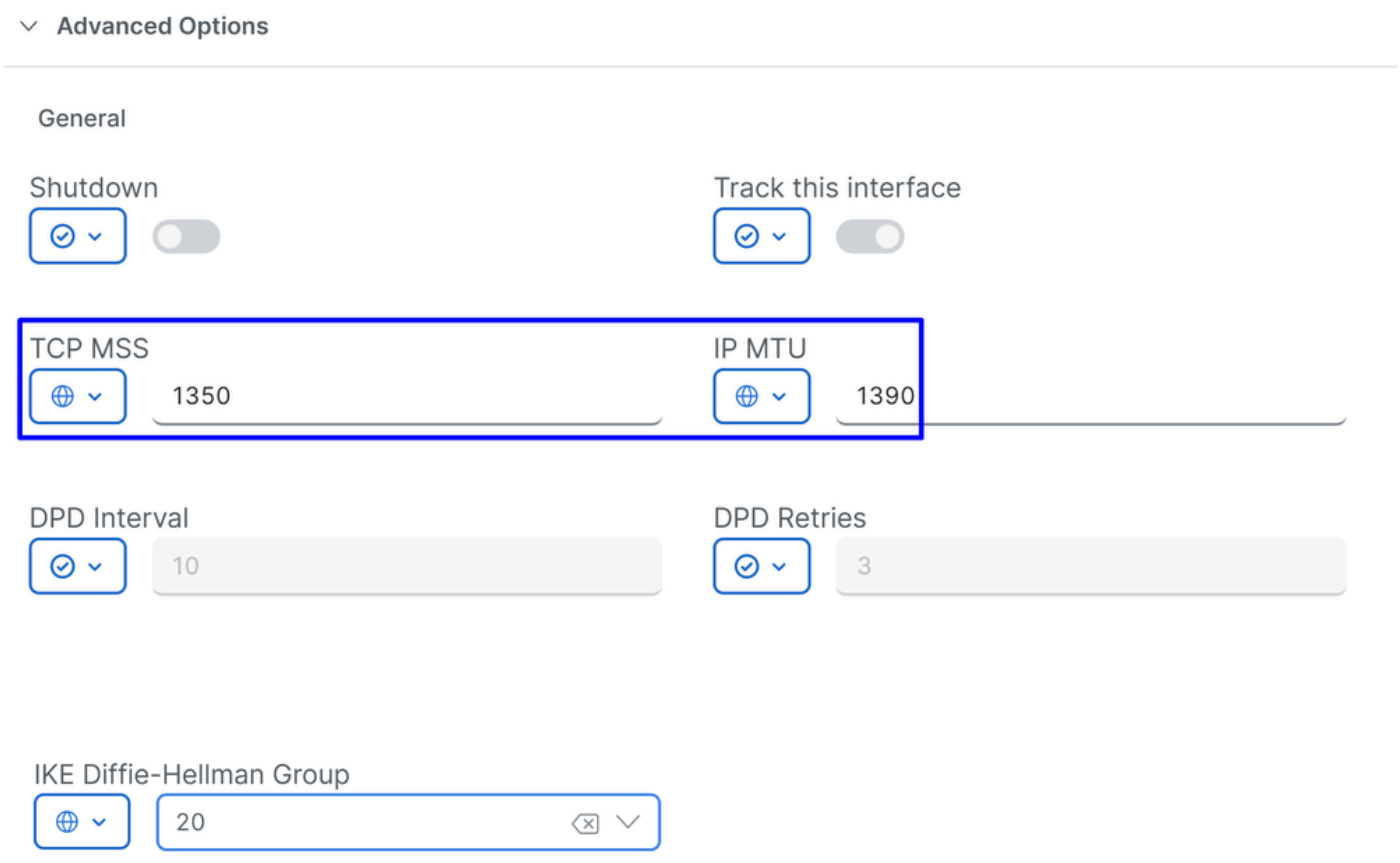
Waarschuwing: Als u loopback-interfaces wilt configureren voor een ECMP-scenario, moet u eerst de loopback-interfaces instellen in Configuration Groups > Transport & Management Profile, onder het beleid dat u in uw router gebruikt.

- Klik opAdd Tunnel



- Interface Name: IPSec1, IPSec2, IPSec3 enzovoort
- Tunnel Source InterfaceKies Loopback Interfaces of een specifieke interface van waaruit u de tunnel instelt
- **Tunnel Route Via**: Als u Loopback kiest, moet u de fysieke interface selecteren van waaruit u het verkeer wilt routeren. Als u Loopback niet selecteert, wordt deze optie grijs weergegeven en wordt de eerste interface met NAT gebruikt die door het systeem wordt gevonden. Als er meerdere zijn, moet u de gewenste WAN-interface selecteren
- **Data Center**: Dit betekent met welke Hub in Secure Access u de verbinding tot stand brengt

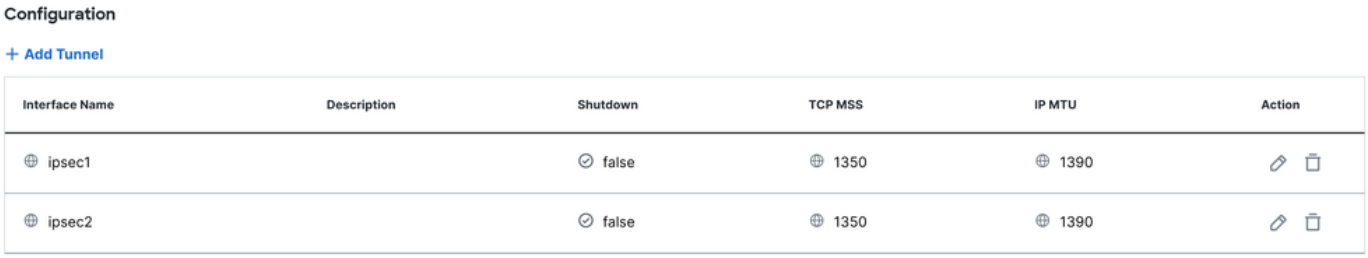
In het volgende deel van de tunnelconfiguratie configureert u de tunnels volgens de best practices van Cisco.



- TCP MSS:1350
- IP MTU:1390
- IKE Diffie-Hellman Group:20

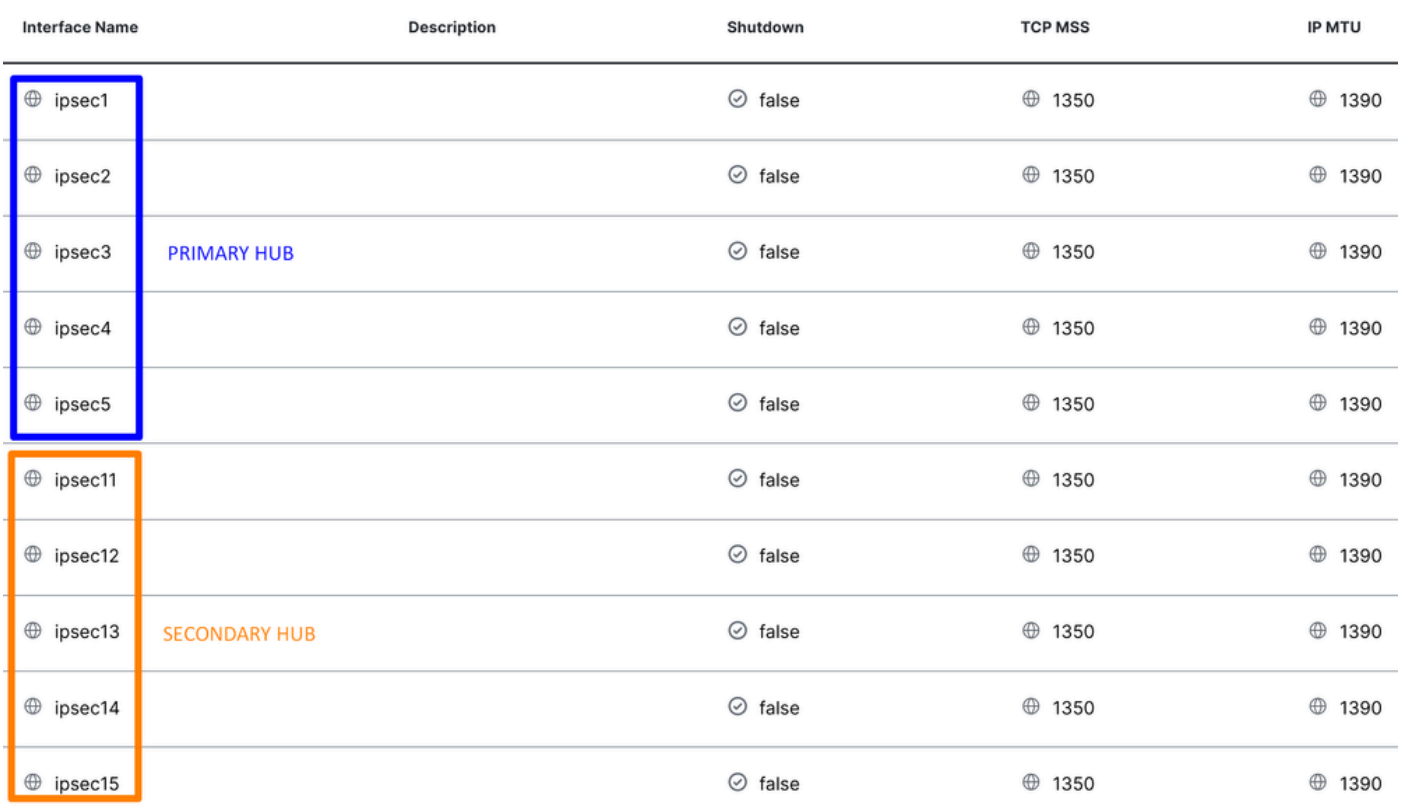
Daarna moet u de secundaire tunnel configureren die naar het secundaire datacenter wijst.

SINGLE HUB HA-SCENARIO

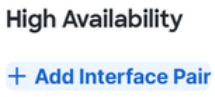


Dit is het uiteindelijke resultaat wanneer u de normale scenario-implementatie gebruikt.

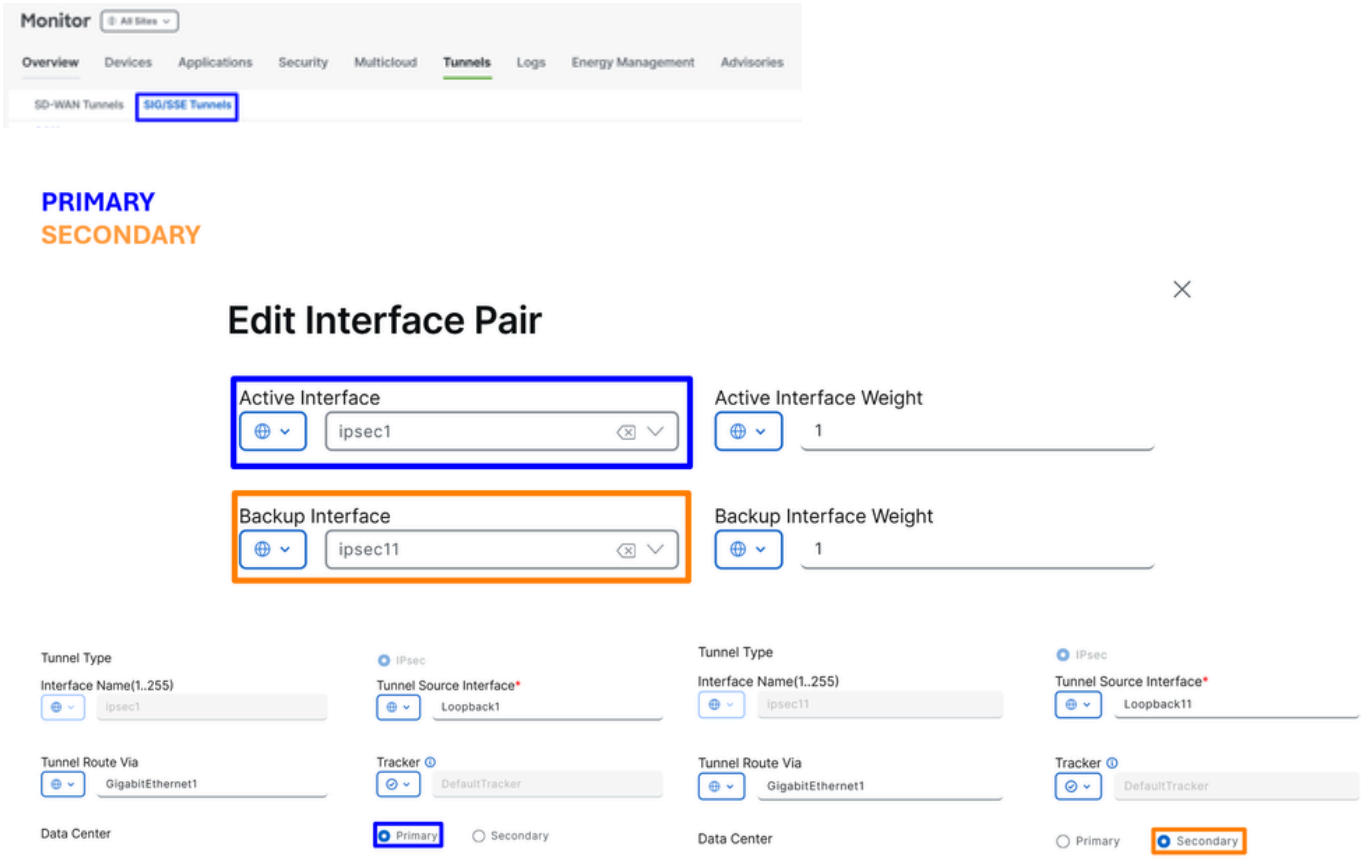
ECMP SCENARIO WITH HA



Vervolgens moet u High Availability configureren in het beleid voor veilig internet.



Klik op Interfacepaar toevoegen:

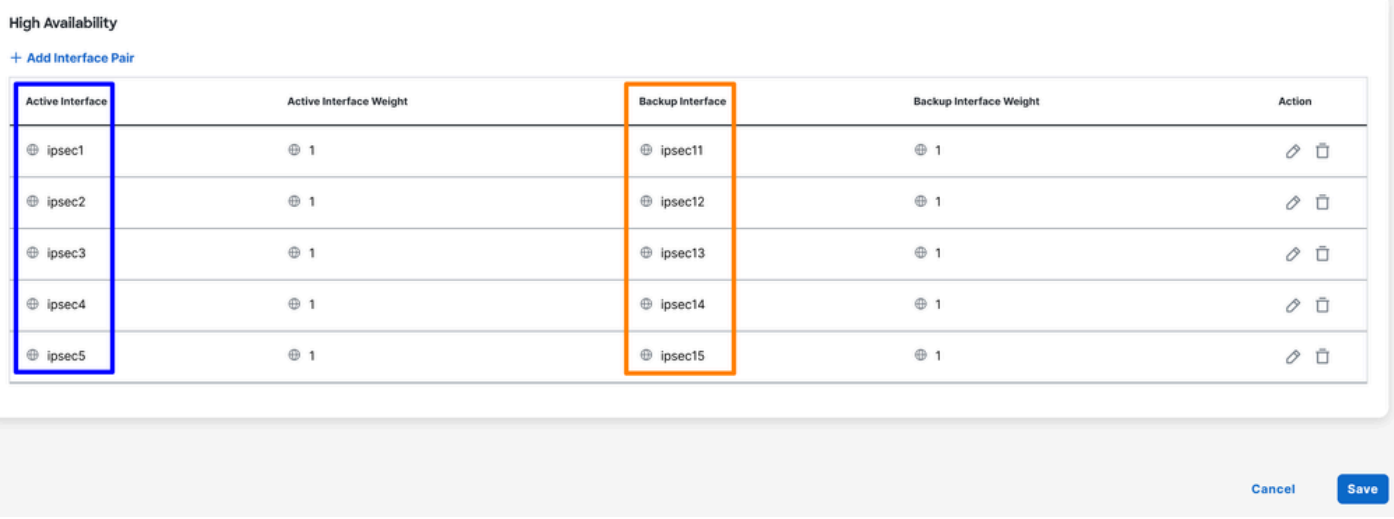


In deze stap moet u de primaire en secundaire tunnel configureren voor elk tunnelpaar dat u instelt. Dit betekent dat elke tunnel zijn eigen back-up heeft. Vergeet niet dat deze tunnels werden gemaakt als Primair en Secundair voor dit exacte doel.
"Active interface" verwijst naar de primaire tunnel, terwijl "Backup interface" verwijst naar de secundaire tunnel:

- Active Interface:Primair
- Backup InterfaceBetreft: Secundair

Waarschuwing: Als deze stap wordt overgeslagen, komen de tunnels niet naar boven en wordt er geen verbinding tot stand gebracht van de routers naar Secure Access.

Nadat High Availability is geconfigureerd voor de tunnels, wordt de installatie weergegeven zoals weergegeven in de onderstaande afbeelding. In het labvoorbeeld dat voor deze gids wordt gebruikt, worden vijf tunnels getoond in HA. Het aantal tunnels kan naar behoefte worden aangepast.



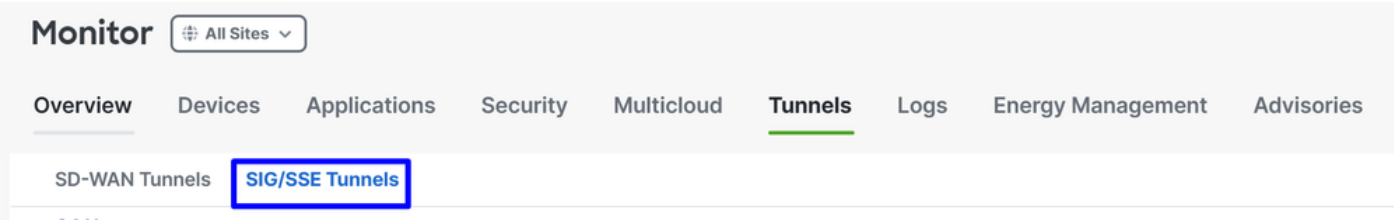
Opmerking: Er kunnen maximaal 8 tunnelparen (16 tunnels: 8 primaire en 8 secundaire) worden geconfigureerd in SD-WAN Catalyst vManage. Cisco Secure Access ondersteunt maximaal 10 tunnelparen.

- Klik op de knop Save

Na dit punt, als alles correct is geconfigureerd, worden de tunnels weergegeven als UP in de SD-WAN Manager en Secure Access.

Controleer de volgende stappen voor verificatie in SD-WAN:

- Klik op Monitor > Tunnels
- Klik vervolgens opSIG/SSE Tunnels

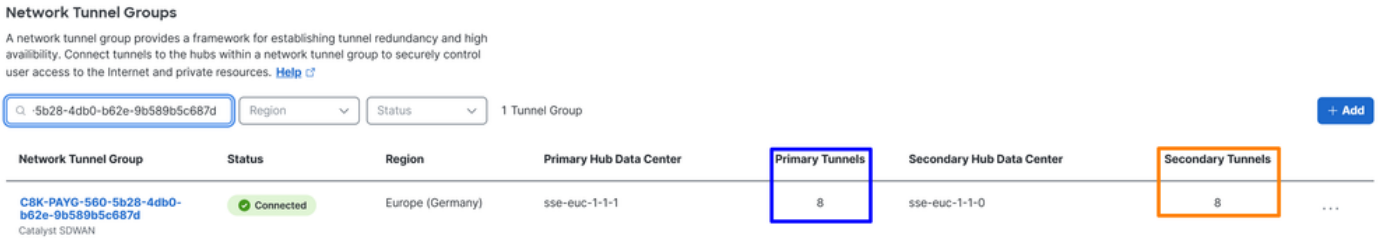


En u kunt de tunnels zien die zijn ingesteld om Cisco Secure Access UP te gebruiken of niet.

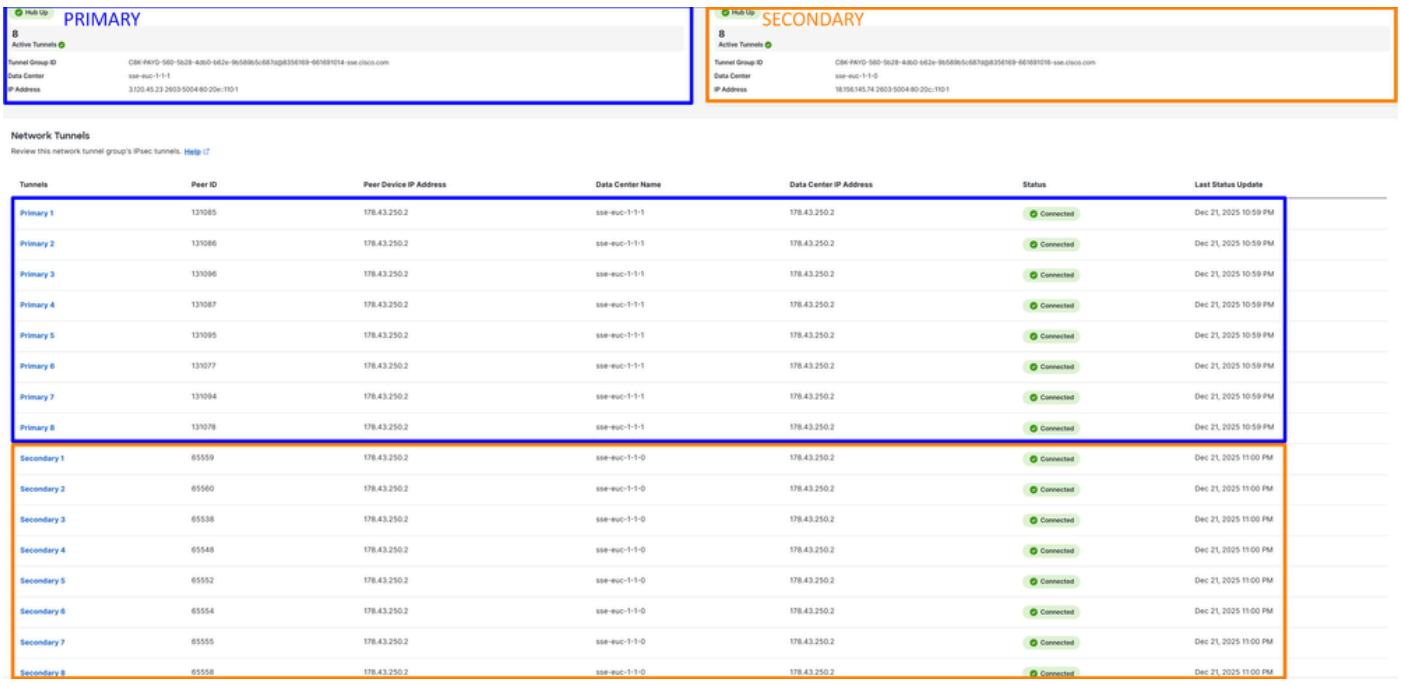
Network Tunnel Group	Tunnel Name	Host Name	Site Name	Tunnel Group ID	Transport Type	Tunnel Type	HA Pair	Provider	Destination Data Center	Tunnel Status(Local)	Tunnel Status(Remote)
		R101-1	SITE_101								
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000001	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000002	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000003	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000004	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000005	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000006	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000007	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000008	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000011	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000012	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000013	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000014	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000015	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000016	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000017	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000018	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up

Controleer de volgende stappen om in Secure Accessteste controleren:

- Klik op Connect > Network Connections



Klik in een gedetailleerde weergave op de naam van de tunnel:



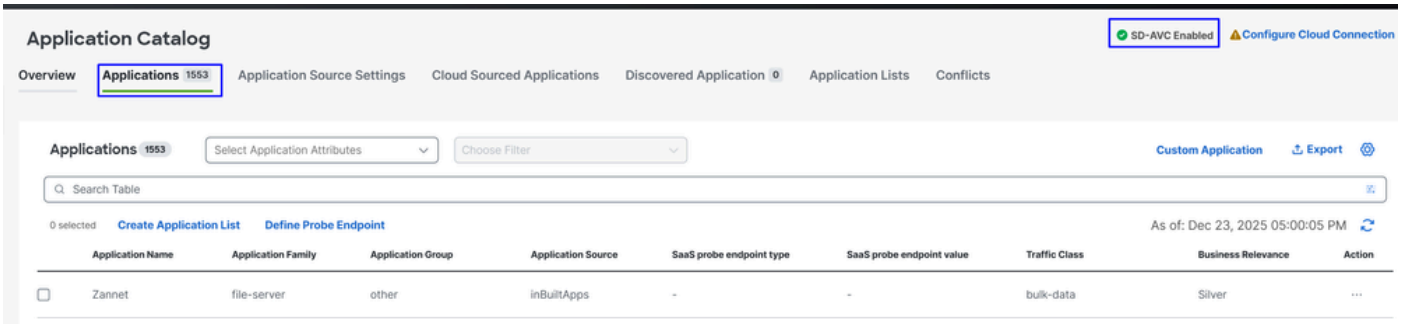
Daarna kun je de stap zetten, Create your Custom Bypass FQDN or APP in SD-WAN

Maak uw aangepaste Bypass FQDN of APP in SD-WAN (OPTIONEEL)

Er zijn speciale gebruikssituaties waarin u Application Bypass en FQDN of IP moet maken die u kunt toepassen op uw routeringsbeleid:

Navigeer naar de SD-WAN Manager portal:

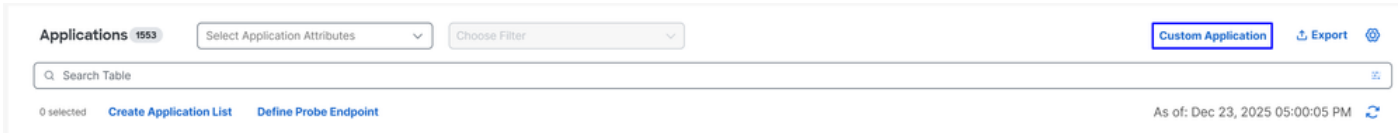
- Klik op Configuration > Application Catalog > Applications



Tip: Als u een versie gebruikt die lager is dan 20.15, kunnen aangepaste toepassingen worden gemaakt onder Beleidslijsten

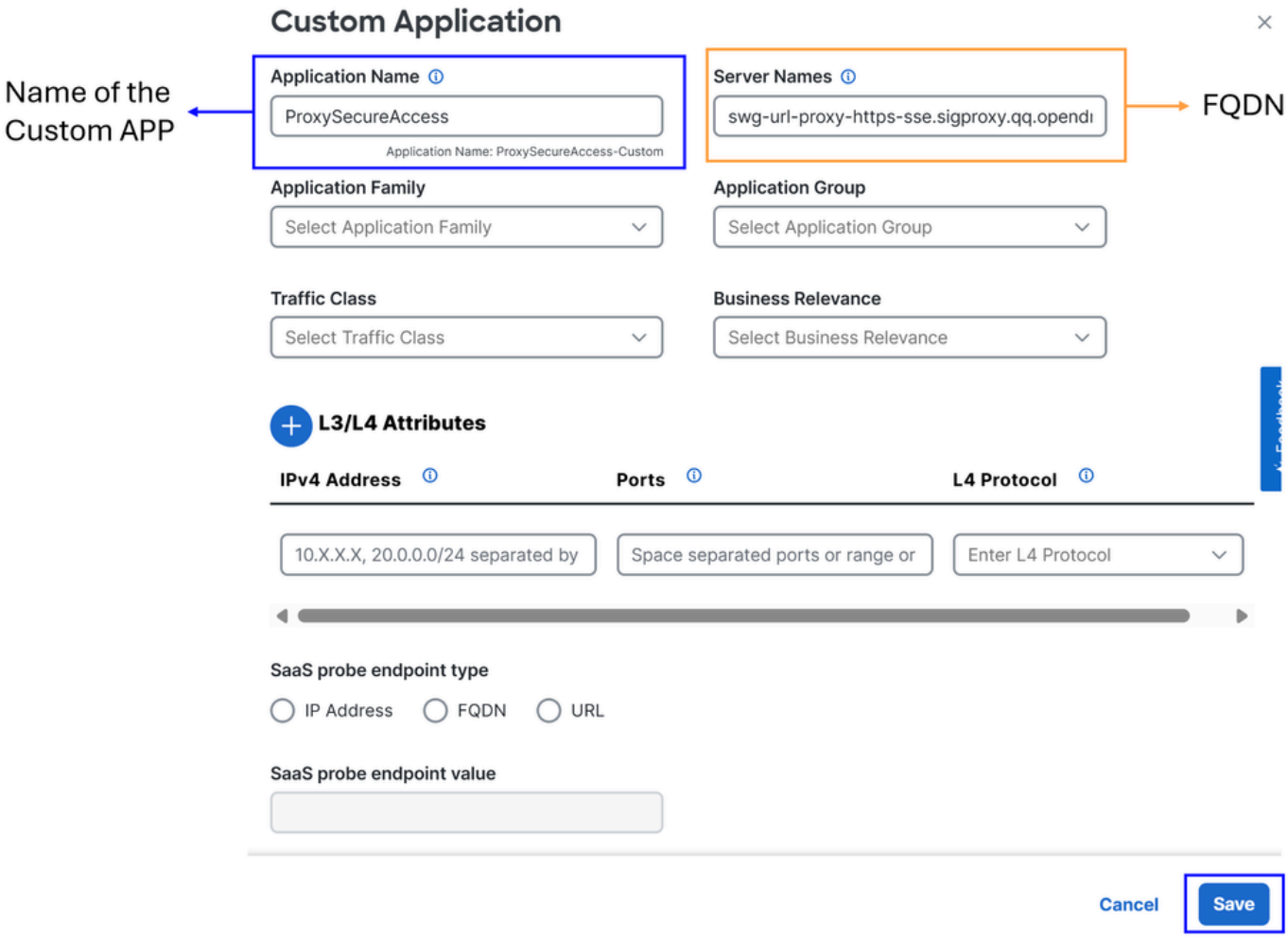
Opmerking: om toegang te krijgen tot de toepassingscatalogus moet u SD-AVC inschakelen.

- Klik op Custom Application



In dit stadium wordt een basisuitsluiting geconfigureerd met behulp van de SWG FQDN-module Secure Client – Umbrella Module:

ProxySecureAccess

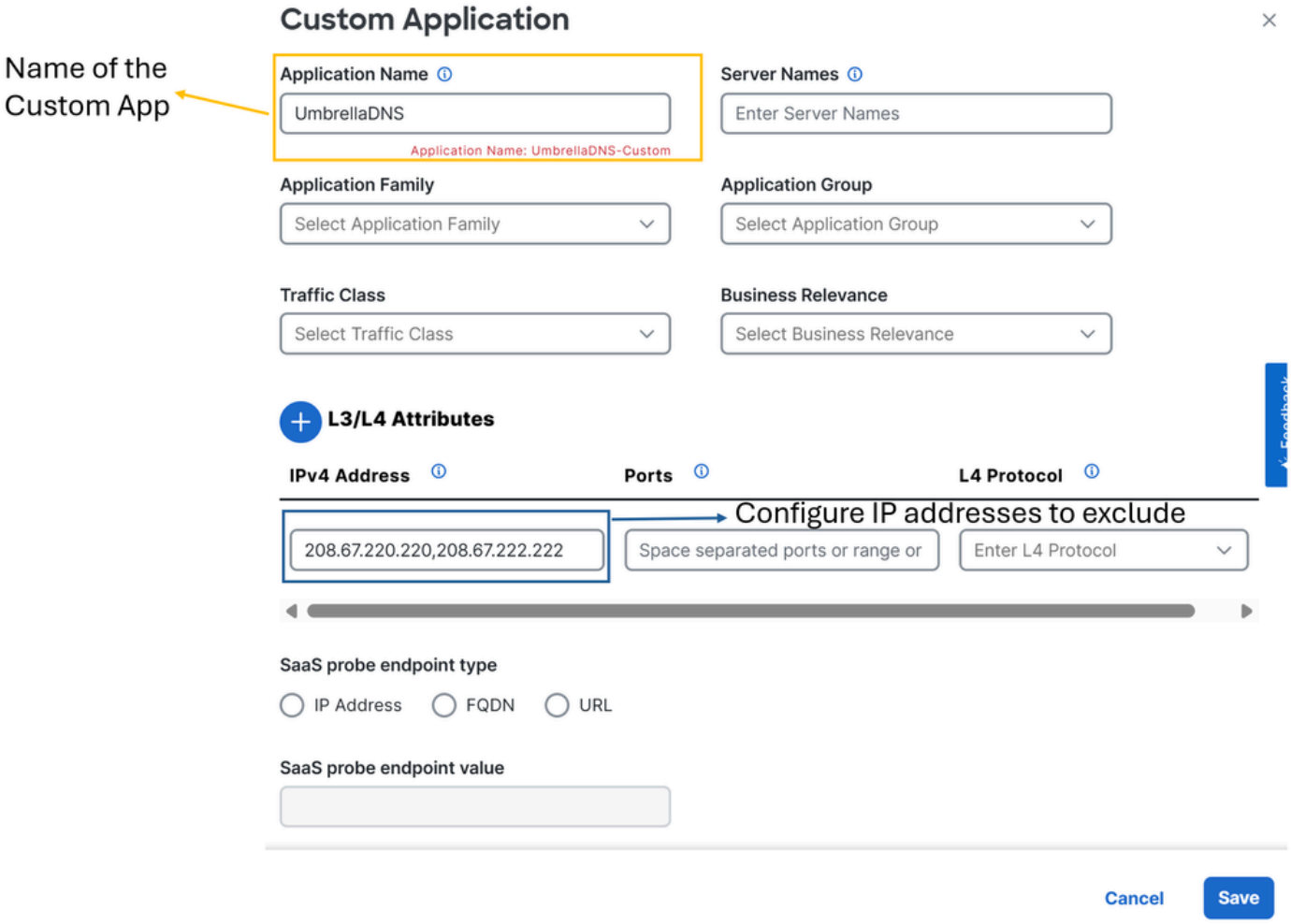


- Server Name: Gebruik de FQDN die u wilt omzeilen (In dit voorbeeld zijn FQDN van SWG geconfigureerd)
  - swg-url-proxy-https-sse.sigproxy.qq.opendns.com
  - swg-url-proxy-https-ORGID.sseproxy.qq.opendns.com
- Klik op Save

Opmerking: wijzig ORGID met uw SSE-organisatienummer.

Vervolgens wordt een basisuitsluiting gemaakt; in dit geval de Umbrella DNS-servers:

UmbrellaDNS



Nu kunt u doorgaan met de configuraties van het routeringsbeleid.

Uw verkeer routeren

In deze stap moet u internetverkeer door de tunnels leiden om het te beschermen via Cisco Secure Access. In dit geval gebruikt u een flexibel routeringsbeleid waarmee we bepaalde verkeersstromen kunnen omzeilen om te voorkomen dat ongewenst verkeer via Secure Access wordt verzonden of om mogelijke slechte praktijken te voorkomen.
Laat het eerst de twee routeringsmethoden definiëren die kunnen worden gebruikt:

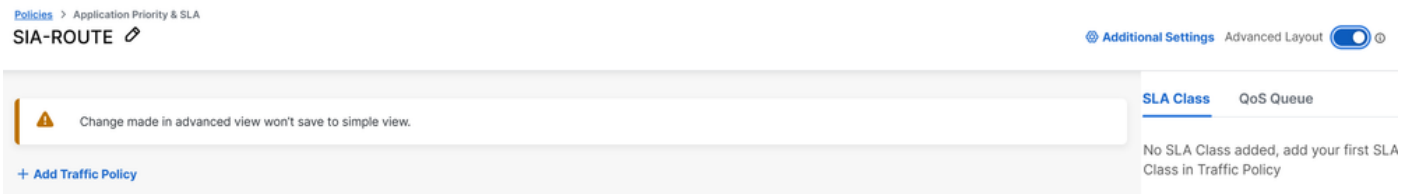
- Configuration > Configuration Groups > Service Profile > Service Route: Deze methode biedt routering naar Secure Access, maar mist flexibiliteit.
- **Configuration** > Policy Groups > Application Priority & SLA: Deze methode biedt verschillende routeringsopties binnen SD-WAN en, belangrijker nog, stelt u in staat om specifiek verkeer te omzeilen, zodat het niet via Secure Access wordt verzonden.

Voor flexibiliteit en afstemming op best practices wordt deze configuratie gebruikt, Application Priority & SLA:

- Klik op **Configuration** > Policy Groups > Application Priority & SLA
- Klik vervolgens op Application Priority & SLA Policy

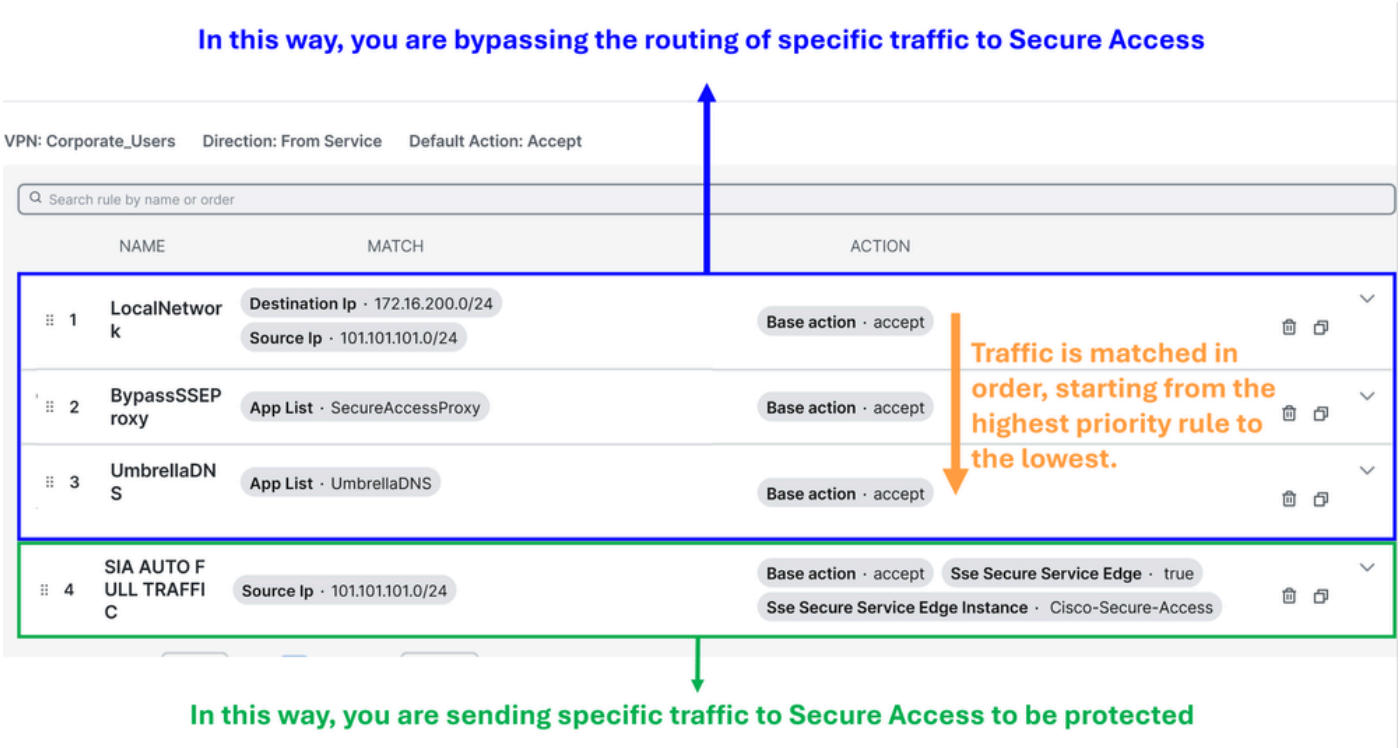
- Configureer een beleidsnaam en klik op Create

- Inschakelen Advanced Layout
- Klik op + Add Traffic Policy



- Policy Name: Naam die dit aanpast aan het doel van deze lijst met verkeersbeleid
- VPN(s): Kies de VPN-service van de gebruiker van waar u het verkeer routeert
- **Direction**: Uit dienst
- Default action: accepteren

Daarna kunt u beginnen met het opstellen van het verkeersbeleid:



1. Local Network Policy (Optional)Bron: 101.101.101.0/24, bestemming 172.16.200.0/24. Deze route voorkomt dat verkeer binnen het netwerk wordt verzonden naar Cisco Secure Access. Doorgaans doen klanten dit niet, omdat interne routering meestal wordt afgehandeld door de distributierouter in SD-WAN-implementaties. Deze configuratie zorgt ervoor dat intern

verkeer tussen deze subnetten niet wordt gerouteerd naar Secure Access, afhankelijk van of uw scenario dit vereist (optioneel, afhankelijk van uw netwerkomgeving)

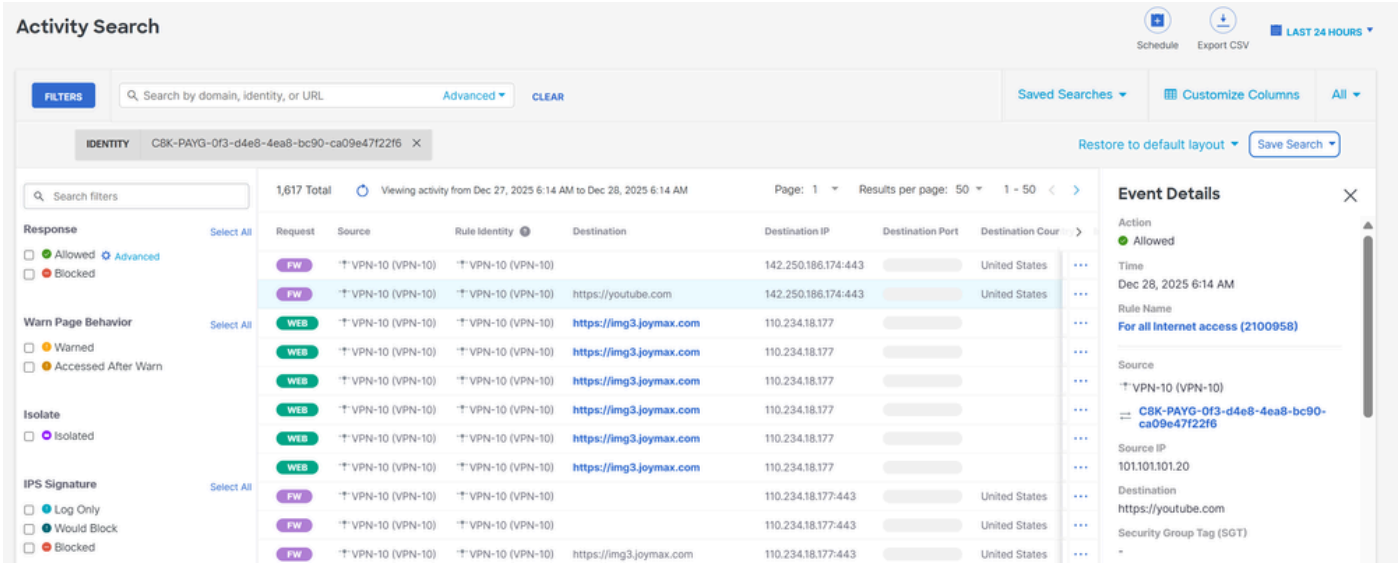
2. **BypassSSEProxy (Optional)**: Dit beleid voorkomt dat interne computers met de Cisco Umbrella-module in Secure Client en SWG ingeschakeld, proxyverkeer terugsturen naar de cloud. Het opnieuw routeren van proxy-verkeer naar de cloud wordt niet als beste praktijk beschouwd.
3. UmbrellaDNS (Best Practice): Dit beleid voorkomt dat DNS-query's die bestemd zijn voor het internet door de tunnel worden verzonden. Het verzenden van DNS-query's naar Umbrella resolvers (208.67.222.222,208.67.220.220) via de tunnel wordt niet aanbevolen.
4. SIA AUTO FULL TRAFFIC: Dit beleid routeert al het verkeer van de bron 101.101.101.0/24 naar het internet via de SSE-tunnels die u eerder hebt gemaakt, zodat dit verkeer in de cloud wordt beschermd.

Verifiëren

Om te controleren of het verkeer al overstroomt via Cisco Secure Access, navigeert u naar Events of Activity Search of Network-Wide Path Insights filtert u op uw tunnelidentiteit:

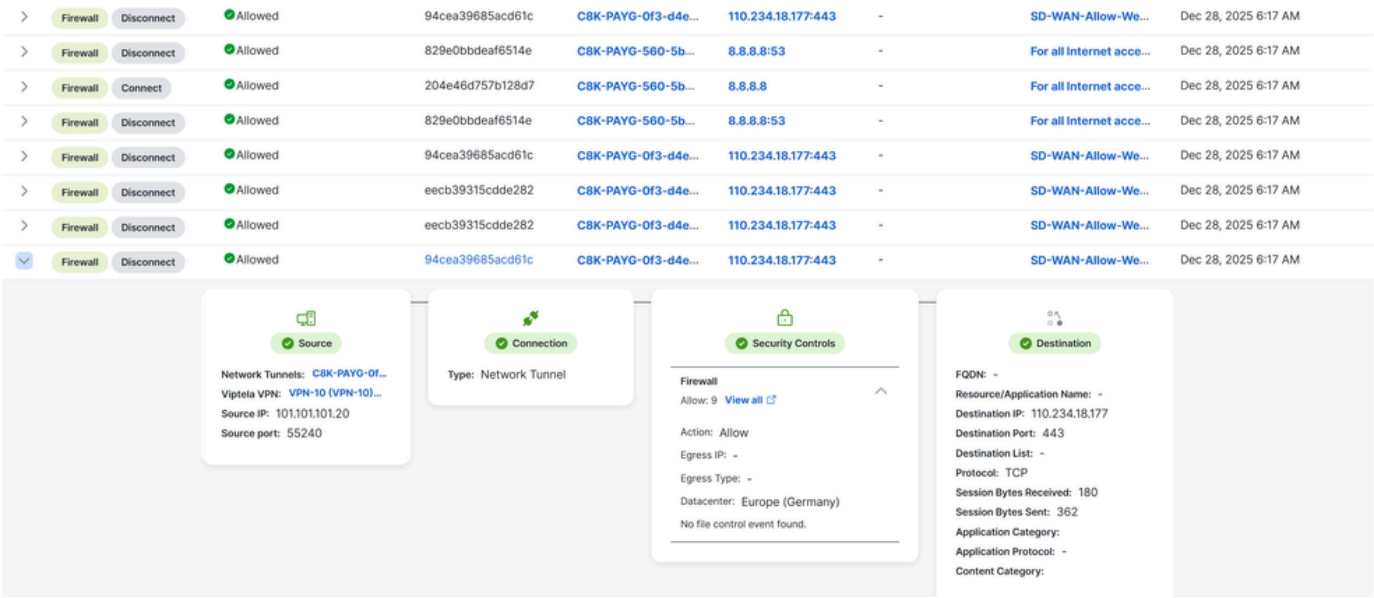
Veilige toegang - zoeken naar activiteiten

Navigeer naar Monitor > Activity Search:



Veilige toegang - Evenementen

Navigeer naar Monitor > Events:

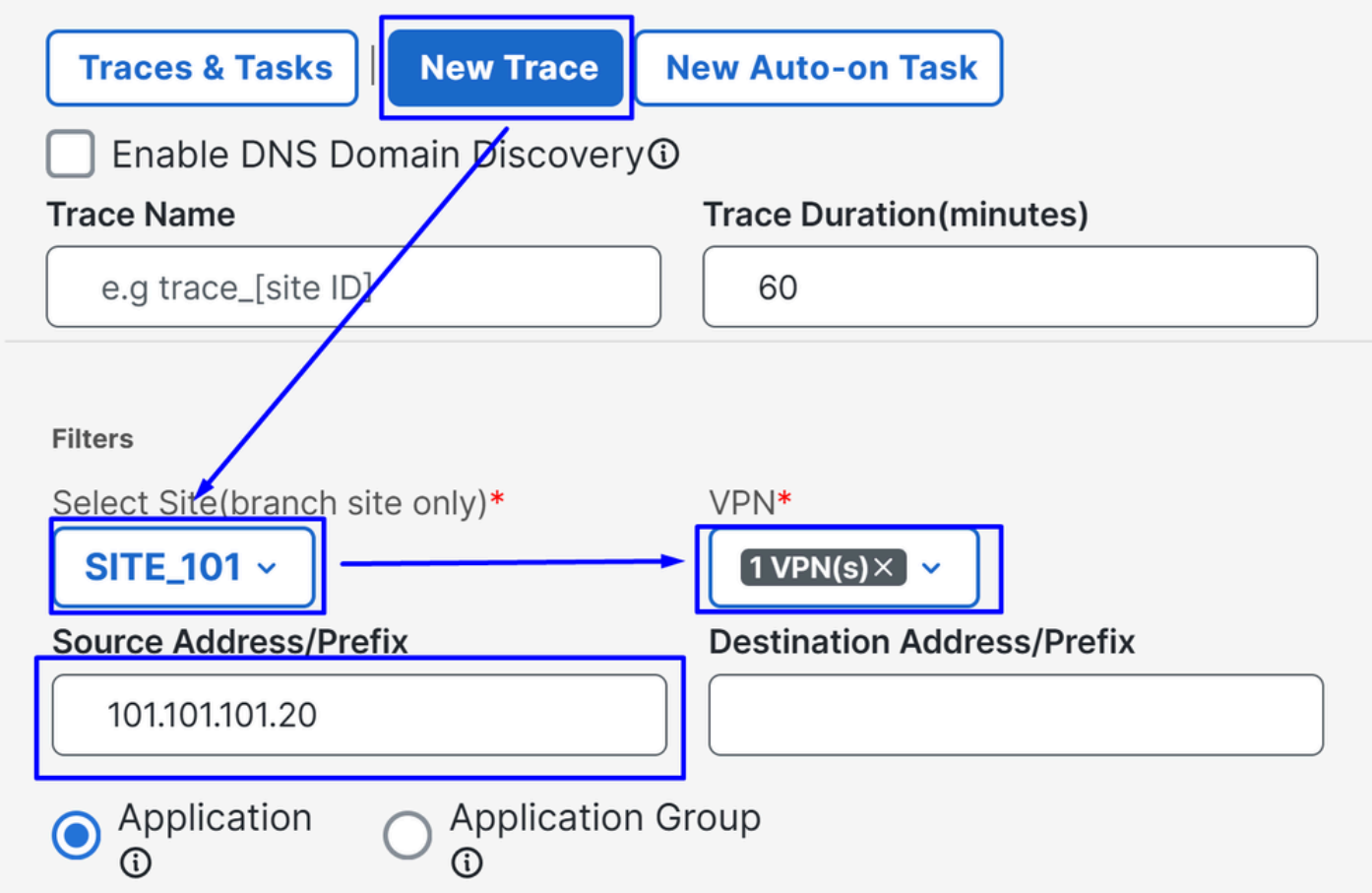


Opmerking: zorg ervoor dat uw standaardbeleid met logboekregistratie is ingeschakeld, standaard is uitgeschakeld.

Catalyst SD-WAN Manager - inzicht in netwerkbrede paden

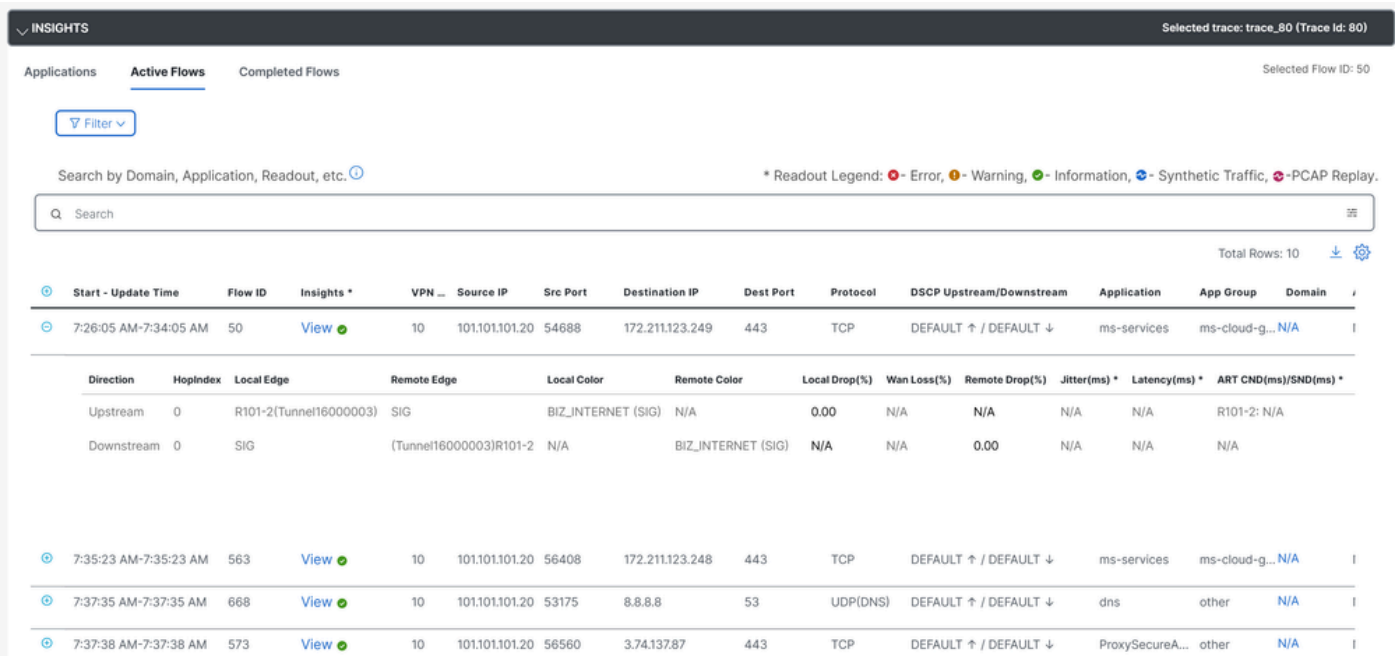
Navigeer naar Catalyst SD-WAN Manager:

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



- Site: Kies de site van waar uw verkeer zich voortzet
- VPN: Kies de VPN-ID van uw subnet waar uw verkeer zich bevindt
- Source: Zet het IP-adres of laat het leeg om al het verkeer te filteren dat door de **Site** en VPN gekozen

Vervolgens kun je in Insights het verkeer zien dat door de tunnels stroomt en het type verkeer dat naar Secure Access gaat:



Gerelateerde informatie

- Cisco Technical Support en downloads
- Cisco Secure Access Help Center
- Cisco SASE-ontwerphandleiding
- 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.