Private App Interconnect tussen Security Service Edge en SD-WAN configureren met behulp van handmatige methode

Inhoud

Inleiding

Dit document beschrijft een uitgebreide handleiding voor het aansluiten van Cisco Secure Access op SD-WAN routers, met focus op beveiligde persoonlijke app-toegang.

Over deze gids

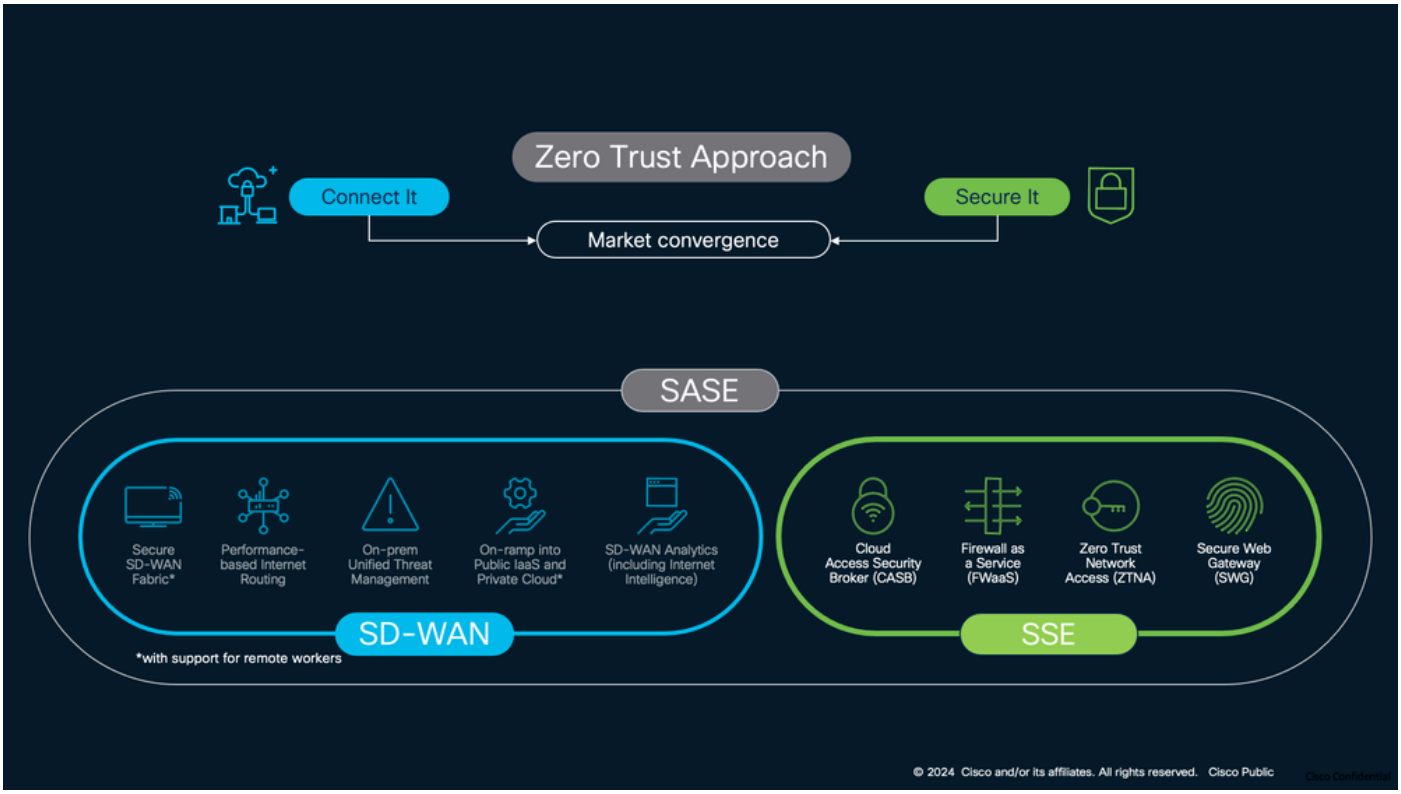
Opmerking: de hier genoemde configuraties zijn ontwikkeld voor UX1.0 en 17.9/20.9 versies van SD-WAN.

Deze gids presenteert een gestructureerde analyse van deze belangrijkste stappen:

- Netwerktunnelgroepen (NTSG's) definiëren
- Configuratie van IPSec-tunnels: Gedetailleerde instructies voor het instellen van beveiligde IPSec-tunnels tussen Cisco SD-WAN routers en Cisco Secure Access NTSG's.
- BGP-groep: Stap-voor-stap procedures voor het uitvoeren van BGP-buurten via de IPSec-tunnels om dynamische routing en verbeterde netwerkveerkracht te garanderen.
- Particuliere toegang tot toepassingen: Advies over het configureren en beveiligen van

toegang tot particuliere toepassingen via de bestaande tunnels.

Afbeelding 1: Cisco SD-WAN en SSE Zero Trust-benadering



SSE met SD-WAN

Deze gids concentreert zich op ontwerpoverweging en implementatie beste praktijken voor NTG interconnect. In deze handleiding worden SD-WAN controllers geïmplementeerd in de cloud en WAN Edge-routers worden ingezet in het datacenter en zijn verbonden met ten minste één internetcircuit.

Belangrijkste veronderstellingen

- Cisco Secure Access Secure Service Edge (SSE): Er wordt vanuit gegaan dat Cisco Secure Access SE al voor uw organisatie is geleverd.
- Cisco SD-WAN WAN Edge-router: De WAN Edge-router wordt verondersteld te worden geïntegreerd in het overlay-netwerk, waardoor op efficiënte wijze gebruikersverkeer via de SD-WAN-infrastructuur wordt vergemakkelijkt.
- Hoewel deze handleiding zich voornamelijk richt op de SD-WAN-aspecten van ontwerp en configuratie, biedt hij een holistische benadering van het integreren van Cisco Secure Access-oplossingen binnen uw bestaande netwerkarchitectuur.

Over deze oplossing

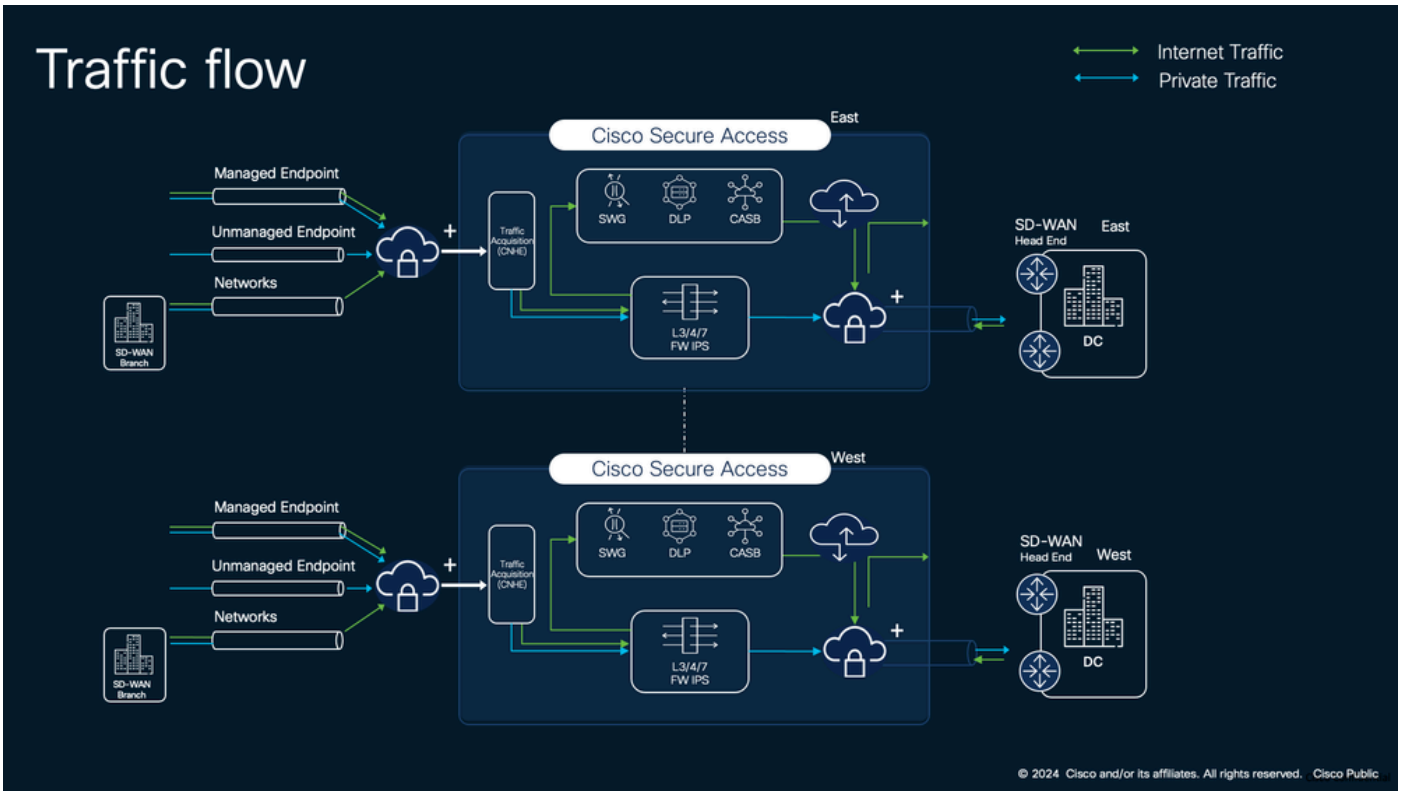
Private app-tunnels, aangeboden door Cisco Secure Access, bieden beveiligde connectiviteit met privé-toepassingen voor gebruikers die verbinding maken via Zero Trust Network Access (ZTNA) en VPN as a Service (VPNaaS). Deze tunnels stellen organisaties in staat om externe gebruikers veilig te koppelen aan privébronnen die worden gehost in datacenters of privéclouds.

Met behulp van IKEv2 (Internet Key Exchange versie 2) maken deze tunnelgroepen beveiligde, bidirectionele verbindingen tussen Cisco Secure Access en SD-WAN routers. Ze ondersteunen hoge beschikbaarheid via meerdere tunnels binnen dezelfde groep en bieden flexibel verkeersbeheer via zowel statische als dynamische routing (BGP).
De IPsec-tunnels kunnen verkeer vanuit verschillende bronnen transporteren, zoals:

- Externe toegang voor VPN-gebruikers
- Op browser gebaseerde of op client gebaseerde ZTNA-verbindingen
- Andere netwerklocaties die zijn aangesloten op Cisco Secure Access

Deze benadering staat organisaties toe om veilig alle soorten privé toepassingsverkeer door een verenigd, gecodeerd kanaal te leiden, dat zowel veiligheid als operationele efficiency verbetert. Cisco Secure Access, als onderdeel van Cisco Security Service Edge (SSE)-oplossing, vereenvoudigt IT-bewerkingen via één cloudbeheerde console, één client, gecentraliseerde beleidsvorming en geaggregeerde rapportage. Het bevat meerdere beveiligingsmodules in één cloudoplossing, waaronder ZTNA, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS), DNS-beveiliging, Remote Browser Isolation (RBI) en nog veel meer. Deze allesomvattende aanpak beperkt de veiligheidsrisico's door vertrouwensnulbeginselen toe te passen en granulair beveiligingsbeleid af te dwingen

Afbeelding 2: Traffic Flow tussen Cisco Secure Access en Private App



SSE Private App Traffic Flow

De oplossing die in deze handleiding wordt beschreven, is gericht op uitgebreide redundantieoverwegingen, die zowel de SD-WAN router in het datacenter als de Network Tunnel Group (NTG) aan de kant van Security Service Edge (SSE) omvatten. Deze gids concentreert zich op een Actief/Actief SD-WAN hub implementatiemodel, dat helpt bij het onderhouden van

ononderbroken verkeersstroom en zorgt voor hoge beschikbaarheid.

Voorwaarden

Vereisten

Aanbevolen wordt dat u kennis van deze onderwerpen hebt:

- Cisco SD-WAN configuratie en -beheer
- Basiskennis van IKEv2- en IPSec-protocollen
- Configuratie van Network Tunnel Group in Cisco Secure Access-portal
- Kennis van BGP en ECMP

Gebruikte componenten

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

- Cisco SD-WAN controllers op 20.9.5a
- Cisco SD-WAN Edge-routers op 17.9.5a
- Cisco Secure Access-portal

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.

Ontwerpen

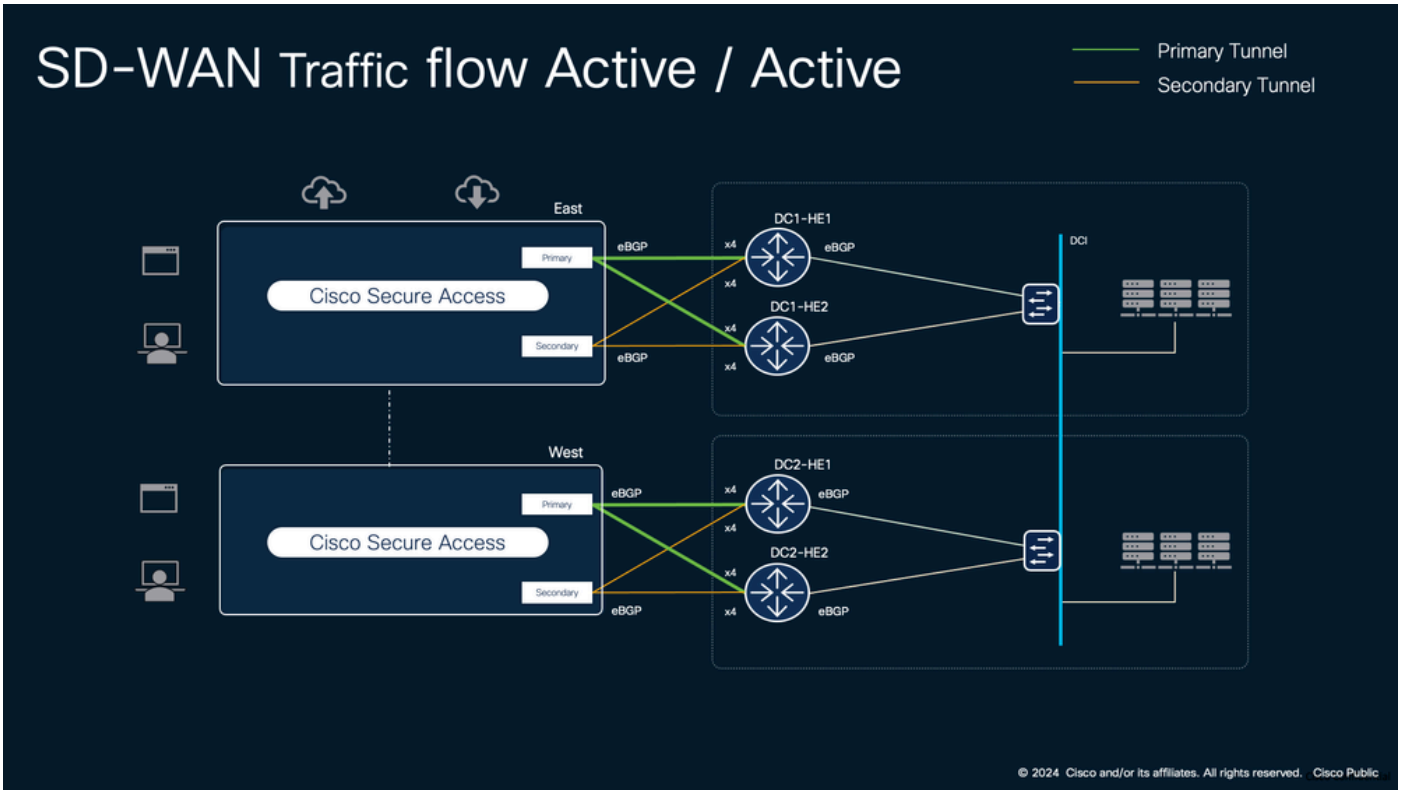
Deze handleiding beschrijft de oplossing met behulp van een Active/Active-ontwerpmodel voor SD-WAN head-end routers. Een actief/actief ontwerpmodel in de context van SD-WAN head-end routers veronderstelt twee routers in een datacenter, beide verbonden met de Security Service Edge (SSE) Network Tunnel Group (NTG), zoals geïllustreerd in afbeelding 3. In dit scenario behandelen beide SD-WAN routers in het datacenter (DC1-HE1 en DC1-HE2) actief verkeersstromen. Dit bereiken ze door dezelfde AS Path Lengte (ASPL) te verzenden naar de interne DC buurman. Dientengevolge, verkeer van binnen de de ladingssaldi van gelijkstroom tussen de twee hoofden.

Elke head-end router kan meerdere tunnels instellen op SSE Points of Presence (POP's). Het aantal tunnels varieert op basis van uw vereisten en SD-WAN apparatenmodel. In dit ontwerp:

- Elke router heeft 4 tunnels naar de primaire SSE Hub en 4 tunnels naar de secundaire SSE Hub.
- Het maximale aantal tunnels dat door elke SSE-hub wordt ondersteund, kan variëren. Raadpleeg voor de meest recente informatie de officiële documentatie: https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

Deze head-end routers vormen BGP-buurten via de tunnels naar de SSE. Door deze buurten, adverteren de hoofden privé toepassingsprefixes aan hun buren SSE, toelatend veilige en efficiënte routing van verkeer aan privé middelen.

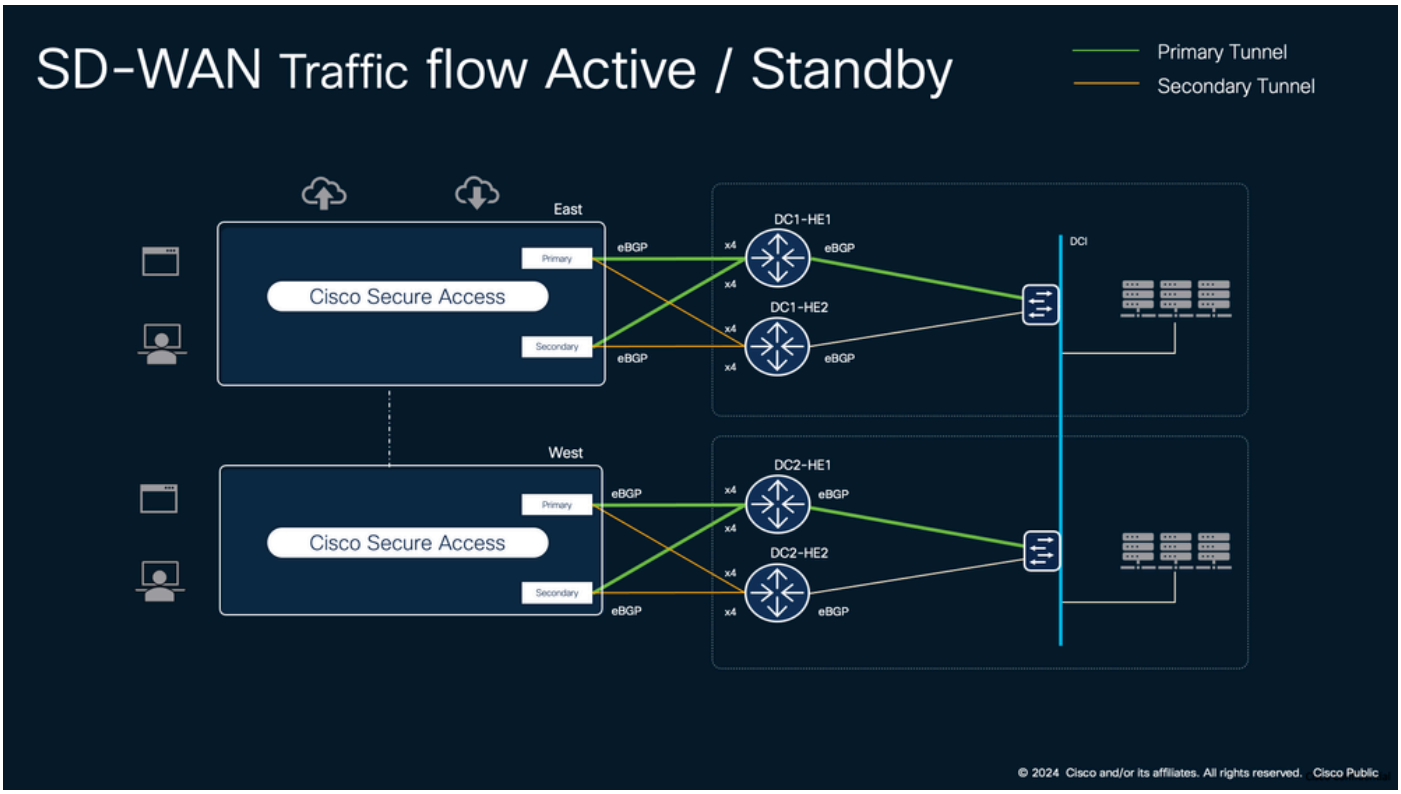
Afbeelding 3: SD-WAN naar SSE actief/actief implementatiemodel



SD-WAN naar SSE actief/actief implementatiemodel

Een Active/Standby-ontwerp wijst één router (DC1-HE1) aan als altijd actief, terwijl de secundaire router (DC1-HE2) stand-by blijft. Het verkeer stroomt consequent door het actieve head-end (DC1-HE1) tenzij het volledig faalt. Dit implementatiemodel heeft een nadeel: als de hoofdtunnel naar SSE daalt, switches verkeer naar de secundaire SSE tunnels die alleen via DC1-HE2 is, waardoor elk stateful verkeer te resetten.
In het Active/Standby-model wordt BGP AS-Path Lengte gebruikt om verkeer zowel binnen de DC als naar de SSE te sturen. DC1-HE1 verstuurt prefixupdates naar de SSE BGP-buurman met een ASPL van 2, terwijl DC1-HE2 updates verstuurt met een ASPL van 3. De interne DC-buur van DC1-HE1 adverteert prefixes met een kortere AS-weglengte dan DC1-HE2, waardoor de verkeersvoorkeur voor DC1-HE1 wordt gewaarborgd. (Klanten kunnen andere kenmerken of protocollen kiezen om de verkeersvoorkeur te beïnvloeden.)
Klanten kunnen op basis van hun specifieke vereisten een Active/Active of Active/Standby-implementatiemodel selecteren.

Afbeelding 4: SD-WAN naar SSE active/stand-by implementatiemodel



SD-WAN naar SSE active/stand-by implementatiemodel

Configureren

In dit deel wordt de procedure beschreven:

1. Controleer de vereisten voor de provisioning van een Network Tunnel Group in het Cisco Secure Access-portal.
2. Configureer SD-WAN interconnect met Cisco Secure Access Network Tunnel Group (NTG) met behulp van de handmatige methode van IPsec.
3. BGP-nabuurschap configureren

Opmerking: Deze configuratie is gebaseerd op een actief/actief implementatiemodel

Procedure 1. Controleer de configuratie van de netwerktunnelgroep op Cisco Secure Access Portal

Hoe te om de Groep van de Tunnel van het Netwerk te vormen wordt niet behandeld in de gids. Controleer deze referentie.

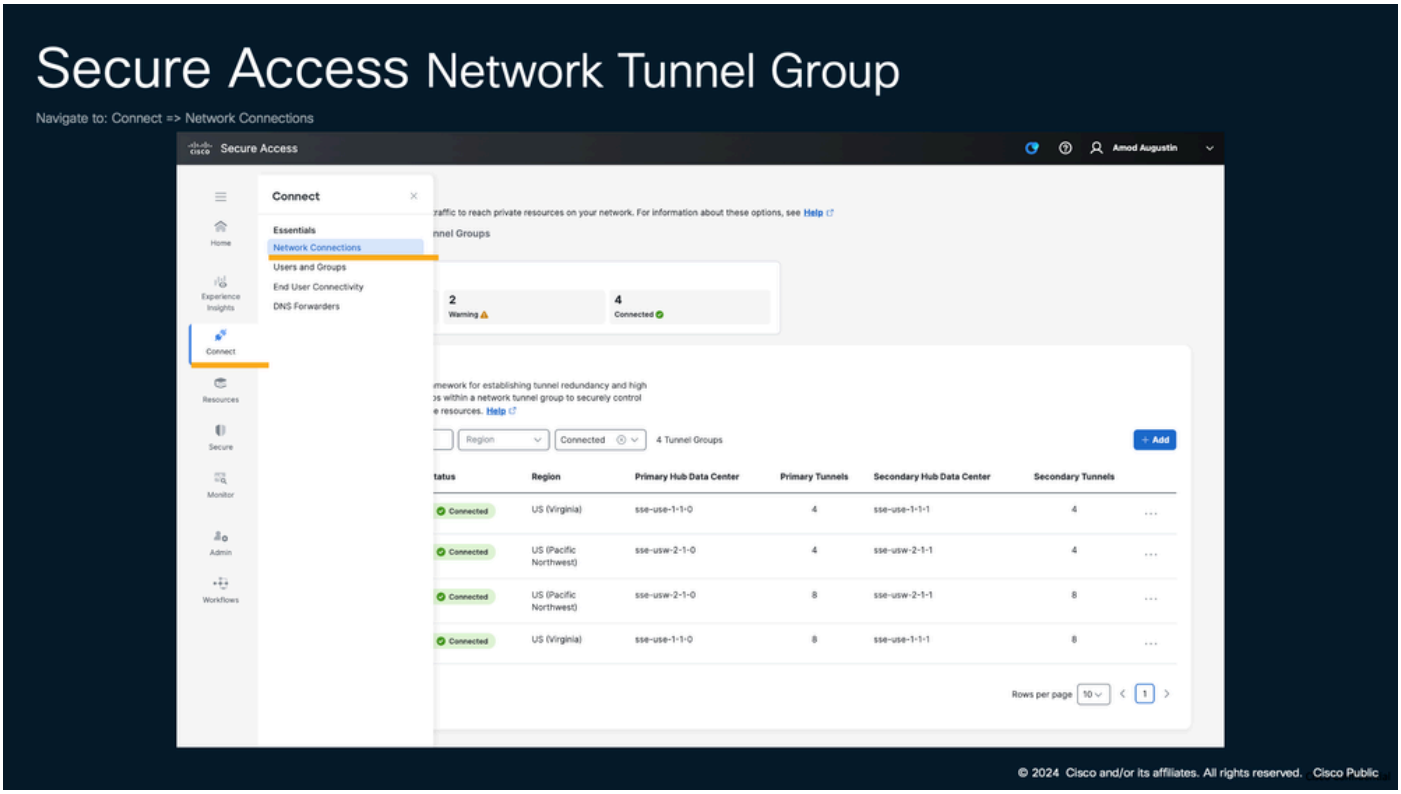
- Een netwerktunnelgroep toevoegen: SSE-documentatie
- Netwerktunnel tussen Cisco Secure Access en Cisco IOS XE router configureren met behulp van ECMP en BGP

Navigeer naar Cisco Secure Access en controleer of de Network Tunnel Groups (NTSG's) zijn geleverd. Voor het huidige ontwerp moeten wij NTSG's in twee verschillende Punten van

Aanwezigheid (POP's) voorzien. In deze handleiding gebruiken we NTG's in de VS (Virginia) POP en US (Pacific Northwest) POP.

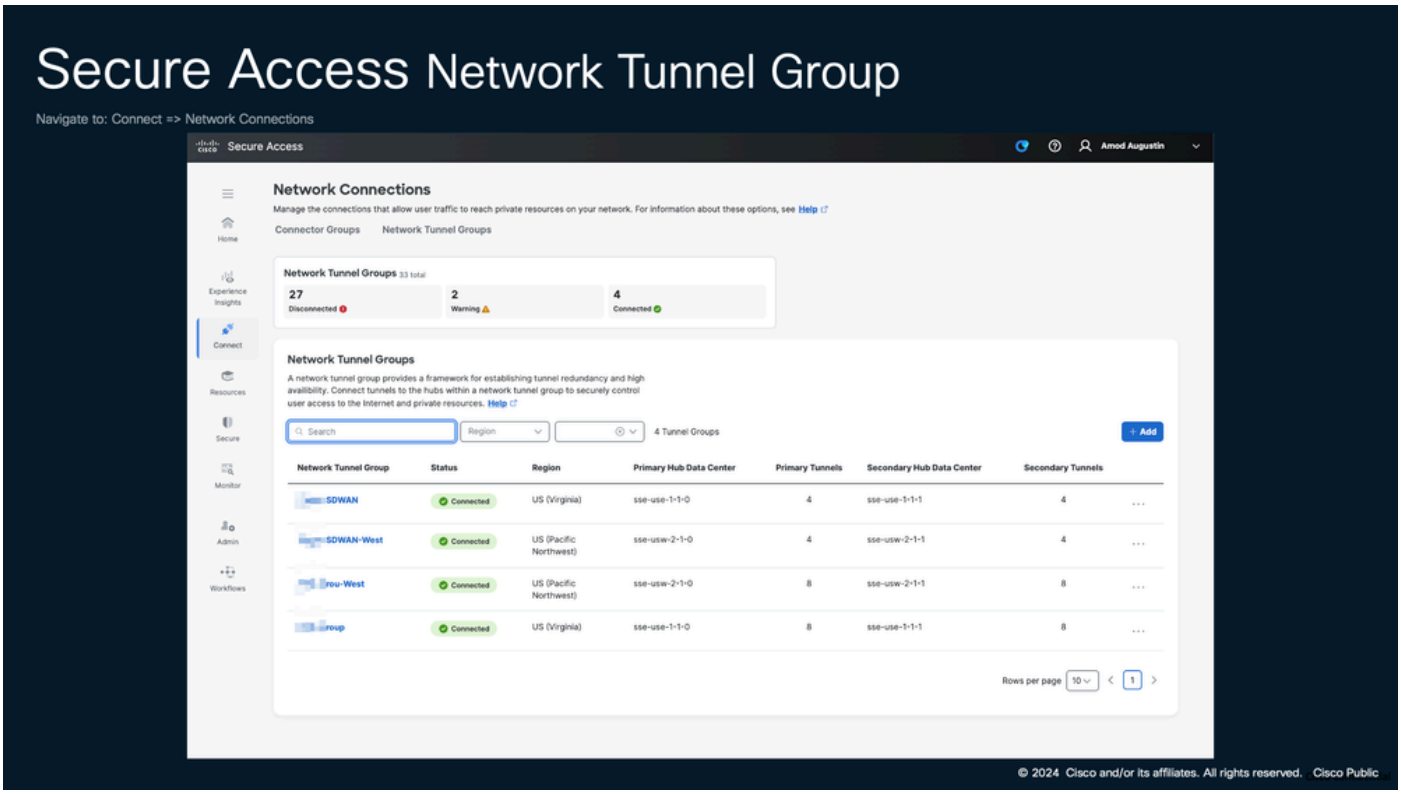
Opmerking:De namen en locaties van POP's kunnen variëren, maar het belangrijkste concept is om meerdere NTSG's te hebben voorzien op locaties die geografisch dicht bij uw datacenter liggen. Deze benadering helpt netwerkprestaties te optimaliseren en biedt redundantie.

Afbeelding 5: Cisco Secure Access Network-tunnelgroep



Cisco Secure Access Network-tunnelgroep

Afbeelding 6: Lijst van Cisco Secure Access Network-tunnelgroepen



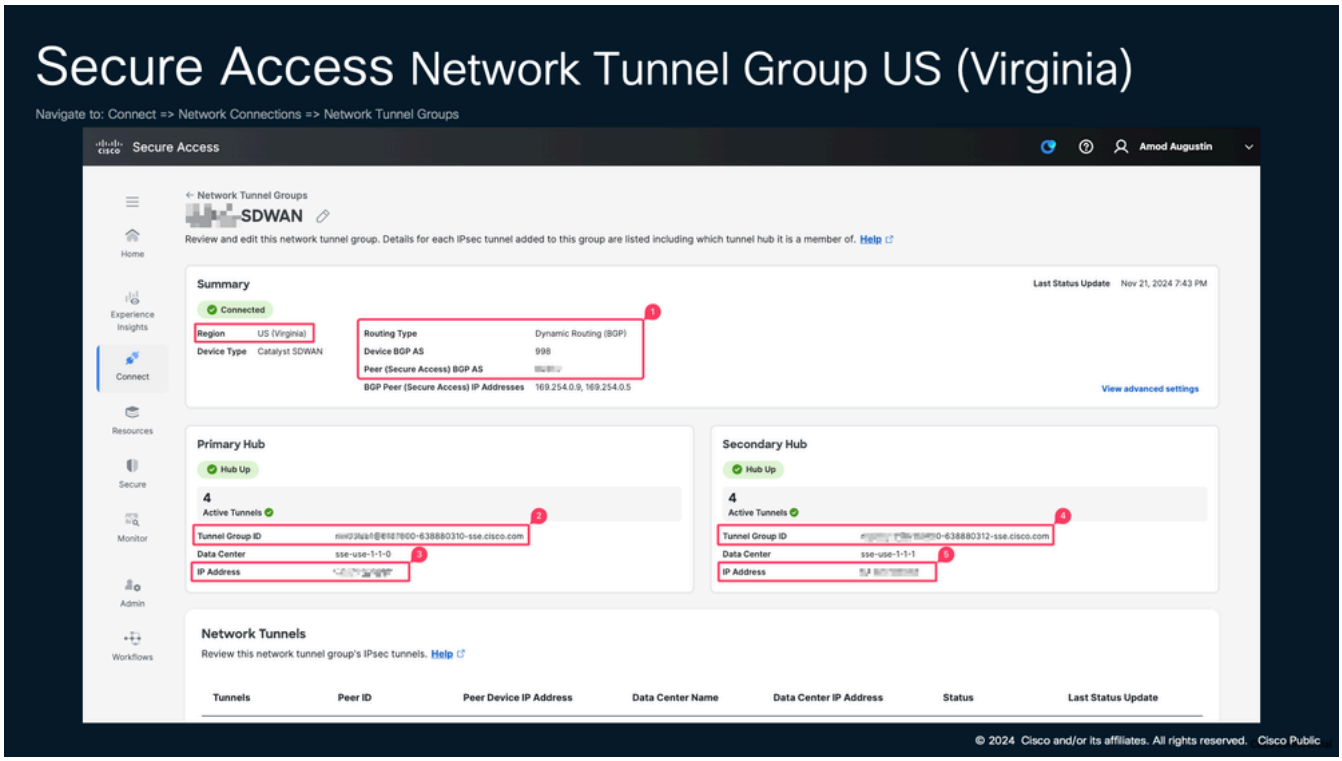
Lijst met tunnelgroepen voor Secure Access Network

Zorg ervoor dat u tunnelpassphrase hebt genoteerd (die slechts één keer tijdens tunnelcreatie wordt getoond).

Opmerking: Stap 6 in Een netwerktunnelgroep toevoegen

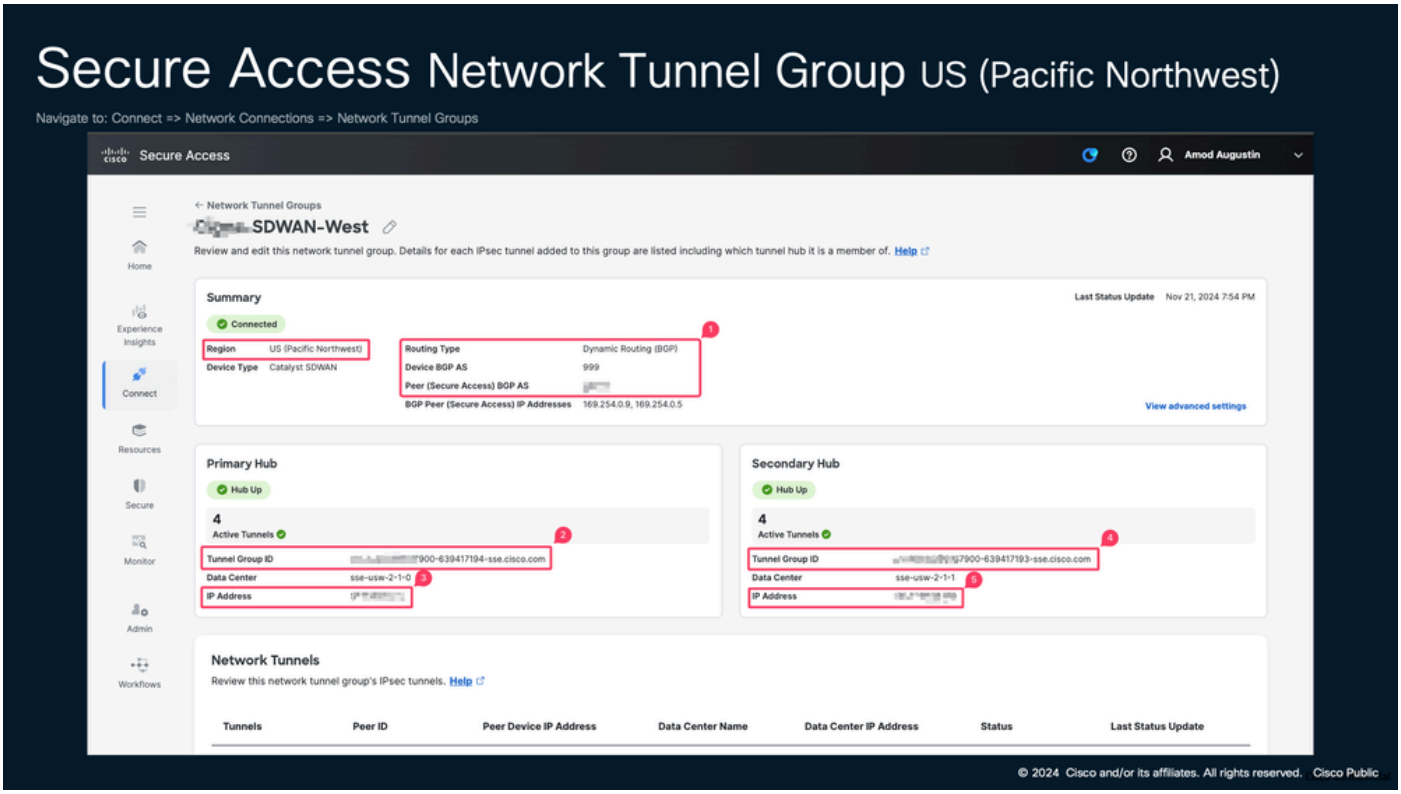
Maak ook een notitie van Tunnel Group attributen die we gebruiken tijdens onze IPSec configuratie. De screenshot (afbeelding 6) wordt genomen uit een laboratoriumomgeving voor een productiescenario om NTG-groepen te maken volgens de ontwerp- of gebruiksaanbeveling.

Afbeelding 7: Secure Access Network Tunnel Group US (Virginia)



Secure Access Network Tunnel Group (Virginia)

Afbeelding 8: Secure Access Network Tunnel Group US (Pacific Northwest)



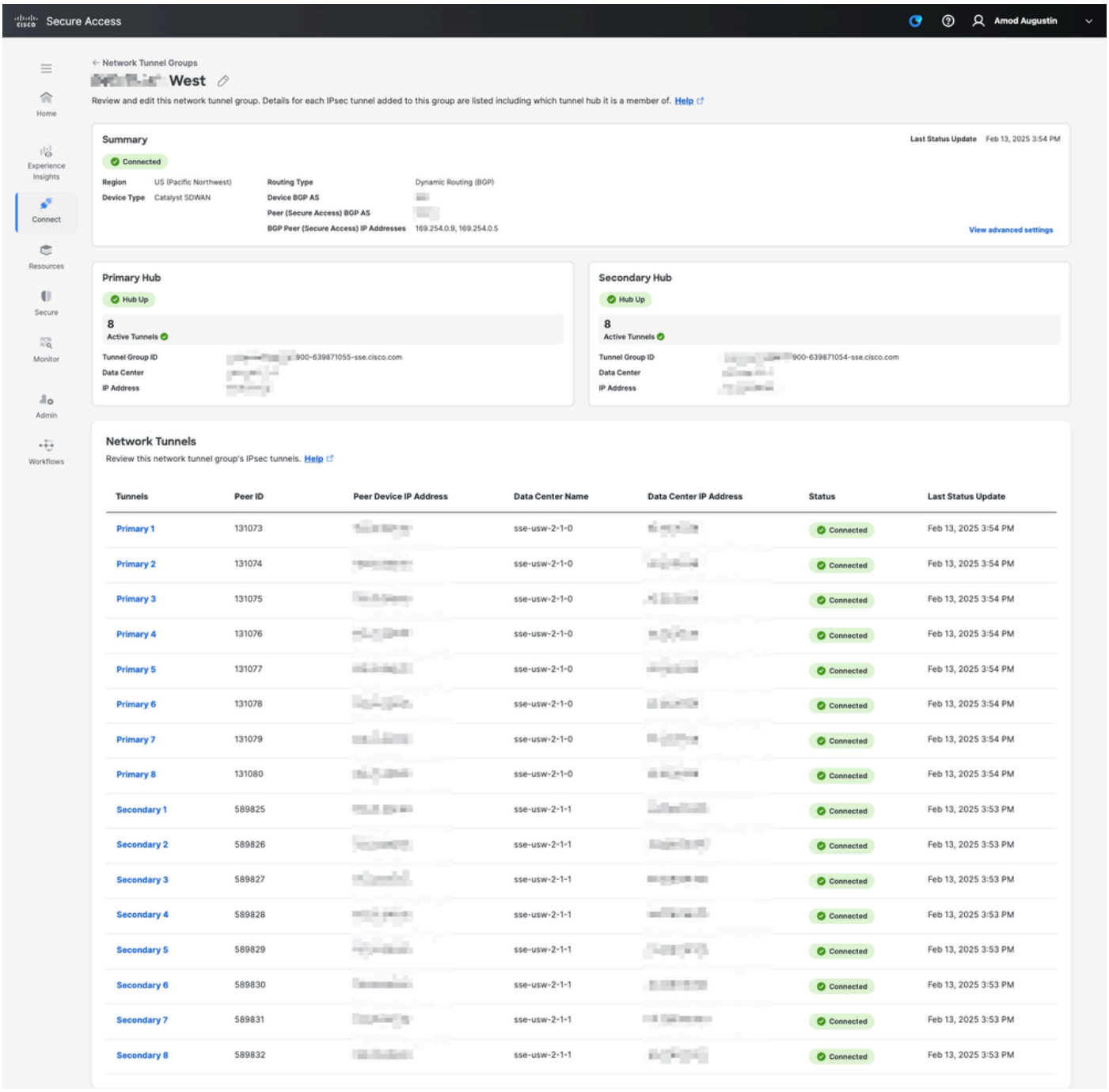
Secure Access Network Tunnel Group (Pacific Northwest)

Figuur 8 toont slechts 4 tunnels op zowel primaire als secundaire hubs. Echter, een maximum van 8 tunnels is met succes getest in een controlleromgeving. De maximale tunnelondersteuning kan variëren afhankelijk van het hardwareapparaat dat u gebruikt en de huidige SSE tunnelondersteuning. Raadpleeg voor de meest recente informatie de officiële documentatie:

https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels en de release note van het betreffende hardwareapparaat.

Een voorbeeld voor een 8-tunnelopstelling wordt hier verstrekt.

Afbeelding 8a: NTG-tunnels tot 8 tunnels



SSE NTG tot 8 tunnels

Procedure 2. Configureer SD-WAN interconnect met Cisco Secure Access Network Tunnel Group (NTG) met behulp van de handmatige IPsec-methode.

Deze procedure toont aan hoe u een Network Tunnel Group (NTSG) kunt verbinden met behulp van functiesjablonen op Cisco Catalyst SD-WAN Manager 20.9 en Cisco Catalyst Edge-router met

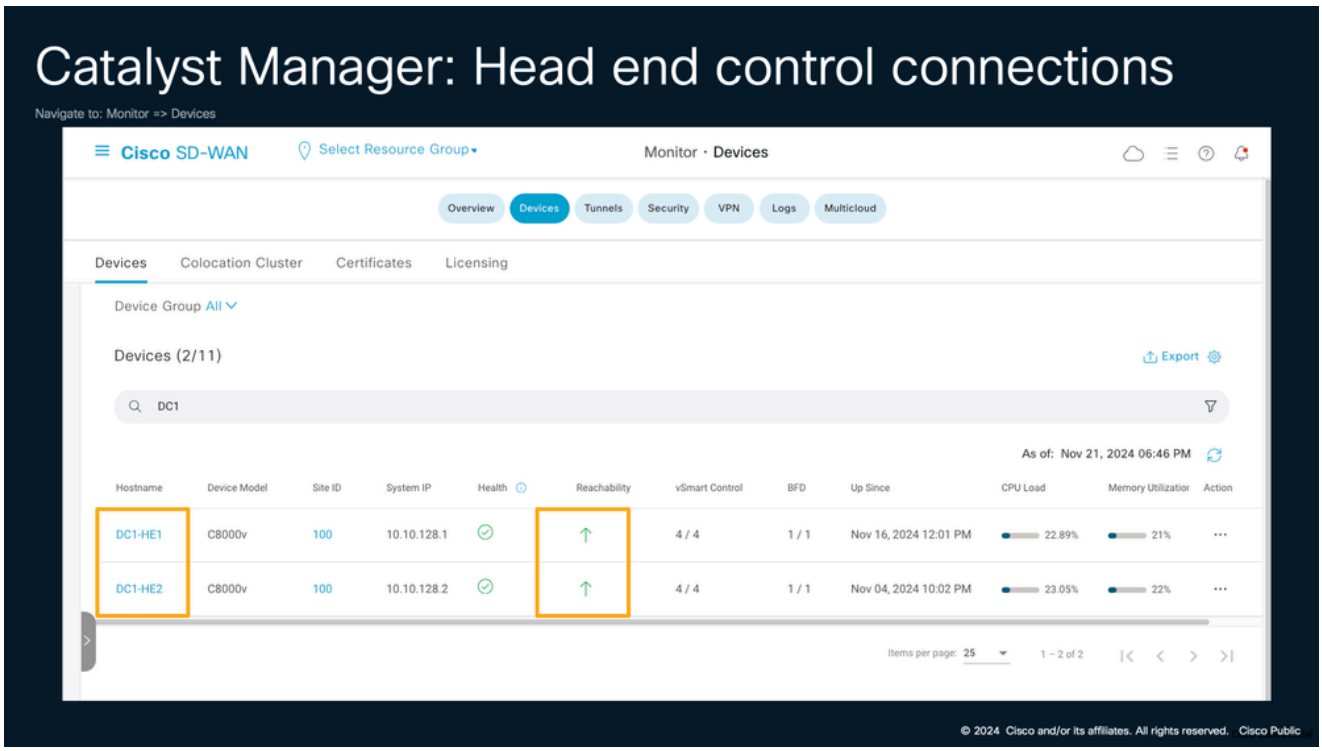
17.9 release.

Opmerking:Deze handleiding gaat uit van een bestaande SD-WAN overlay-implementatie met een hub-and-spoke of volledig ingekapselde topologie, waarbij hubs dienen als toegangspunten voor private toepassingen die worden gehost in het datacenter. Deze procedure kan ook worden toegepast op implementaties in een tak of cloud.

Controleer voordat u verdergaat of aan de volgende voorwaarden is voldaan:

1. De verbindingen van de controle zijn omhoog op het apparaat om noodzakelijke updates van Cisco Catalyst SD-WAN Manager toe te staan.

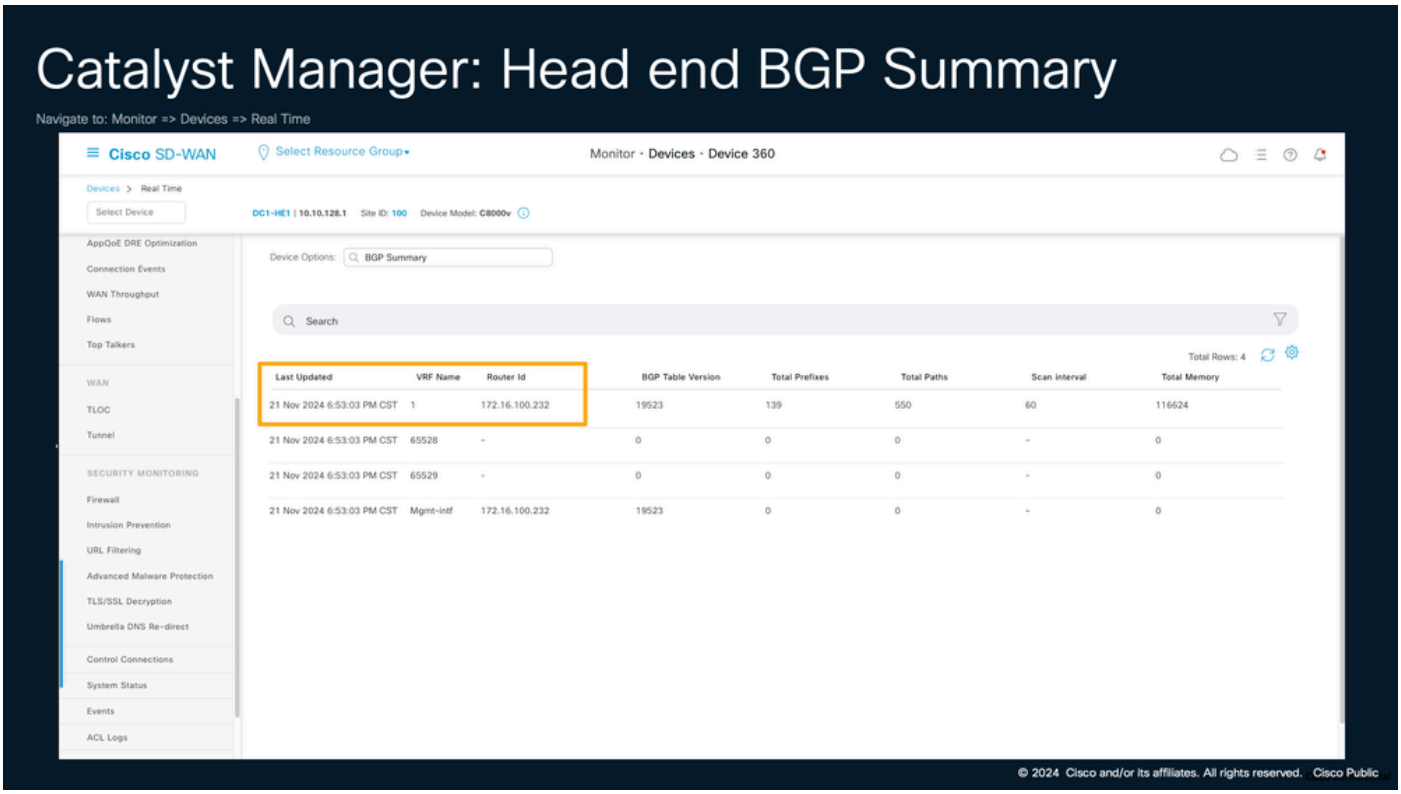
   Afbeelding 9: Cisco Catalyst SD-WAN Manager: Koppelingen voor head-end bediening



   Catalyst Manager: Koppelingen voor head-end bediening

2. Service-side VPN's worden geconfigureerd en gebruiken een routingprotocol om prefixes te adverteren. Deze gids gebruikt BGP als routeringsprotocol aan de servicekant.

Afbeelding 10: Cisco Catalyst SD-WAN Manager: Head-end BGP-samenvatting



Voltooi de volgende stappen om SD-WAN interconnect met Network Tunnel Group (NTG) te configureren met behulp van handmatige IPSec-methode:

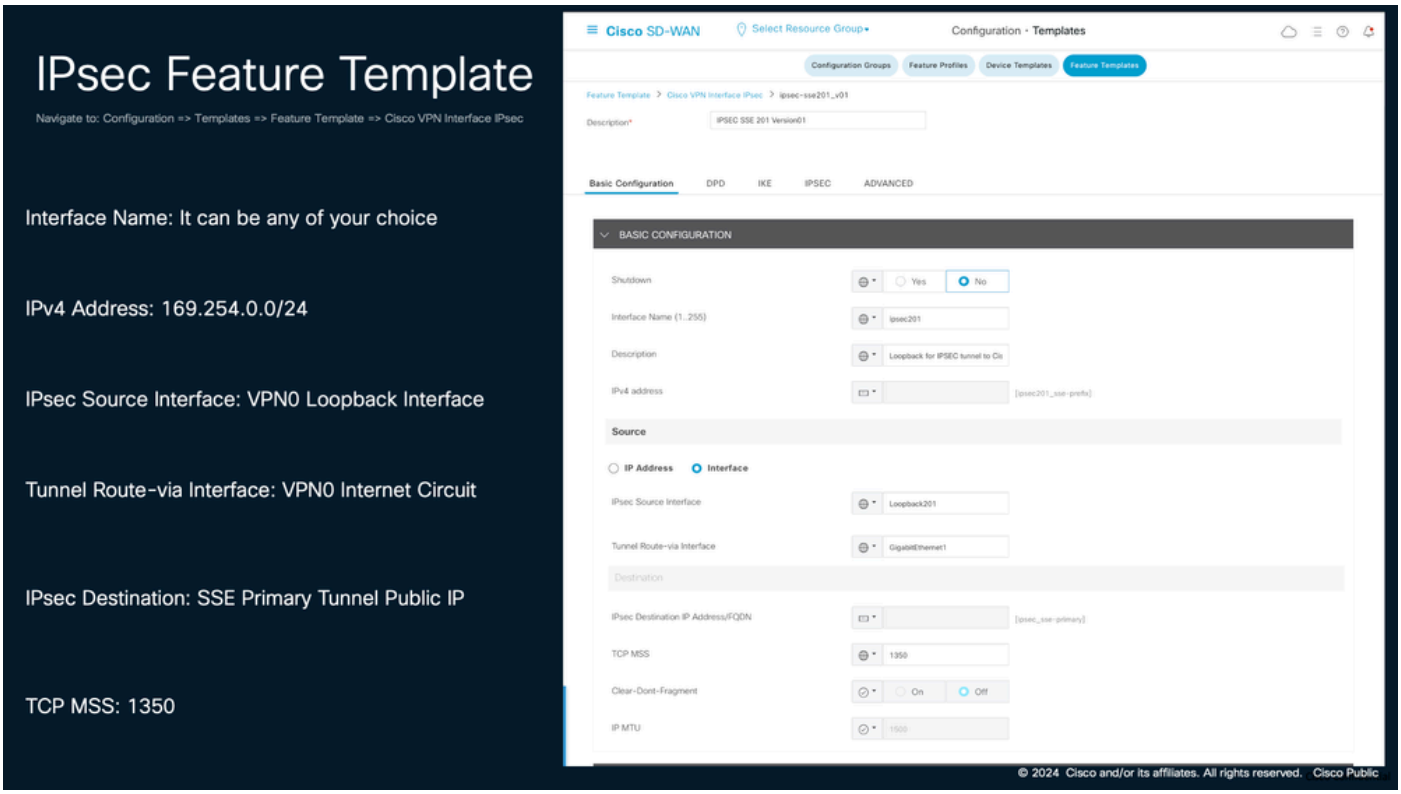
Opmerking: Herhaal deze stap voor het vereiste aantal tunnels voor de inzet.

Raadpleeg de officiële documentatie voor tunnelbeperking: https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

In deze stappen wordt het proces voor het aansluiten van DC1-HE1 (Data Center 1 Head-End 1) op de primaire hub SSE Virginia gedetailleerd. Met deze configuratie wordt een beveiligde tunnel tot stand gebracht tussen de SD-WAN router in het datacenter en de Cisco Secure Access Network Tunnel Group (NTG) in het Virginia Point of Presence (POP)

Stap 1: Functiesjabloon voor IPSec maken
Maak een IPSec-functiesjabloon om de parameters te definiëren voor de IPSec-tunnel die SD-WAN head-end router verbindt met de NTG.

Afbeelding 11: Sjabloon voor IPsec-functies: Basisconfiguratie



IPsec-functiesjabloon: Basisconfiguratie

Interfacenaam: Het kan elk van uw keuzen zijn
IPv4-adres: SSE luistert naar 169.254.0.0/24 op basis van het vereiste kunt u het subnetnummer naar keuze verdelen, als beste praktijk te gebruiken met /30. In deze handleiding laten we het eerste blok voor toekomstig gebruik weg.

IPsec-broninterface: Definieer een VPN0-loopbackinterface die uniek is voor de huidige IPsec-interface. Voor consistentie en probleemoplossing is het raadzaam dezelfde nummering te houden.
Tunnel router-via-interface: Richt de interface die als ondergrond kan worden gebruikt om SSE (moet internettoegang hebben) te bereiken

IPsec-bestemming: IP-adres primaire hub

Zie figuur 7: Secure Access Network Tunnel Group US (Virginia), versie 35.171.214.188

TCP-MSS: Dit moet 1350 zijn (Referentie: [https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters)](https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters)

Voorbeeld: DC1-HE1 naar SSE Virginia Primary Hub

Interfacenaam: ipsec201

Beschrijving: Loopback voor IPSEC-tunnel naar Cisco

IPv4-adres: 169.254.0.x/30

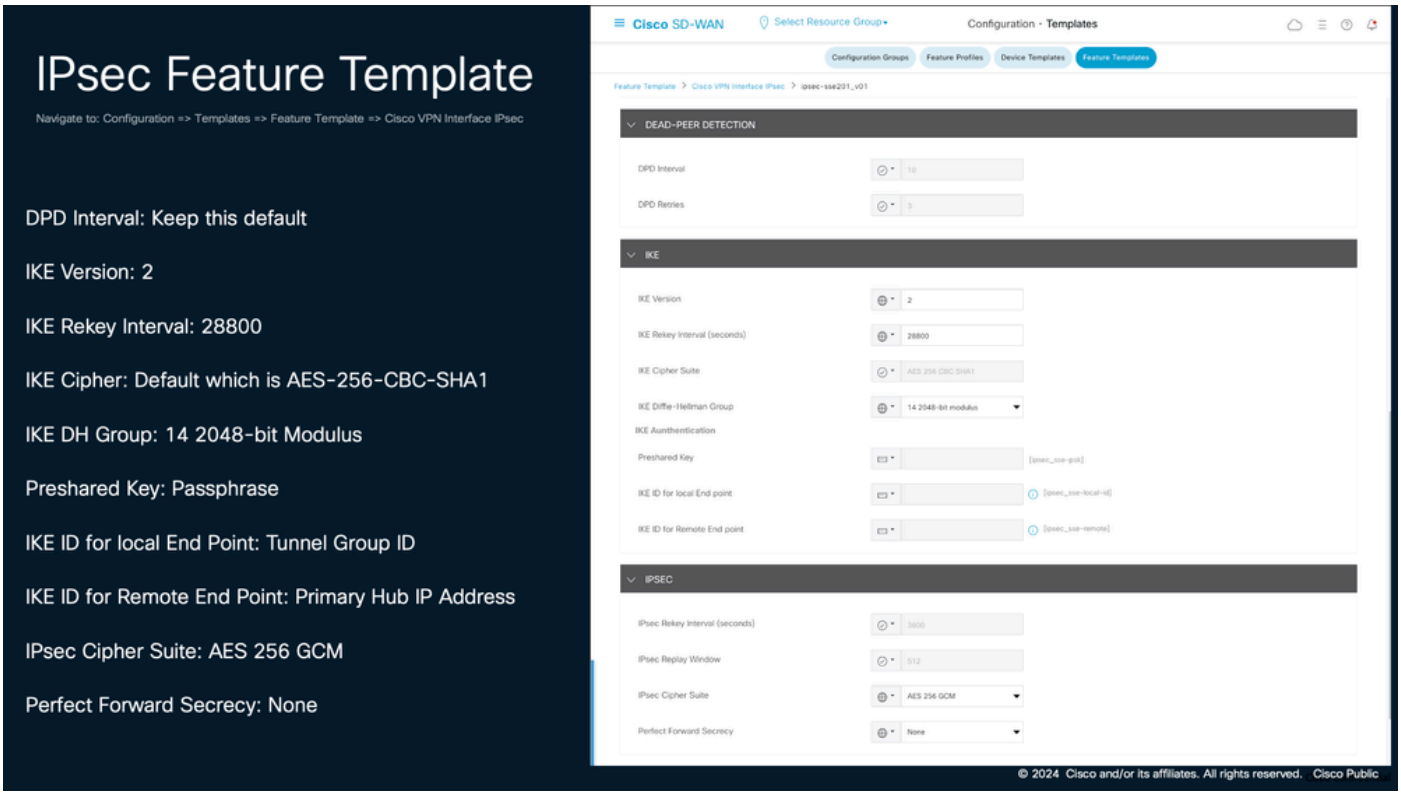
IPsec-broninterface: Loopback201

Tunnel router-via-interface: Gigabit Ethernet1

IPsec-doeladres/FQDN: 35.xxx.xxx.xxx

TCP-MSS: 1350

Afbeelding 12: Sjabloon voor IPsec-functies: IKE IPSEC



IPsec-functiesjabloon: IKE IPSEC

DPD-interval: Deze standaard behouden
IKE versie: 2
Interval IKE-sleutel: 28800
IKE-codering: Standaard: AES-256-CBC-SHA1
IKE DH-groep: 14/2048-bits modulus
Preshared sleutel: Wachtwoord
IKE-id voor lokaal eindpunt: Tunnelgroep-ID

Zie afbeelding 7: Secure Access Network Tunnel Group US (Virginia). Dit is mn03lab1+201@8167900-638880310-sse.cisco.com

---

Opmerking: Elke tunnel moet hiervoor een uniek eindpunt hebben; gebruik "+loopbackID" Voorbeeld: mn03lab1+202@8167900-638880310-sse.cisco.com, mn03lab1+203@8167900-638880310-sse.cisco.com enzovoort.

IKE-id voor extern eindpunt: IP-adres primaire hub
IPsec-coderingssuite: AES 256 GCM

Perfect voorwaartse geheimhouding: None

Referentie: https://docs.sse.cisco.com/sse-user-guide/docs/configure-tunnels-with-catalyst-sdwan#define-the-feature-template

Voorbeeld:

IKE versie: 2
Interval IKE-sleutel: 28800
IKE-codering: AES-256-CBC-SHA1-software
IKE DH-groep: 14/2048-bits modulus
Preshared sleutel: *****

Opmerking: Stap 6 in Een netwerktunnelgroep toevoegen

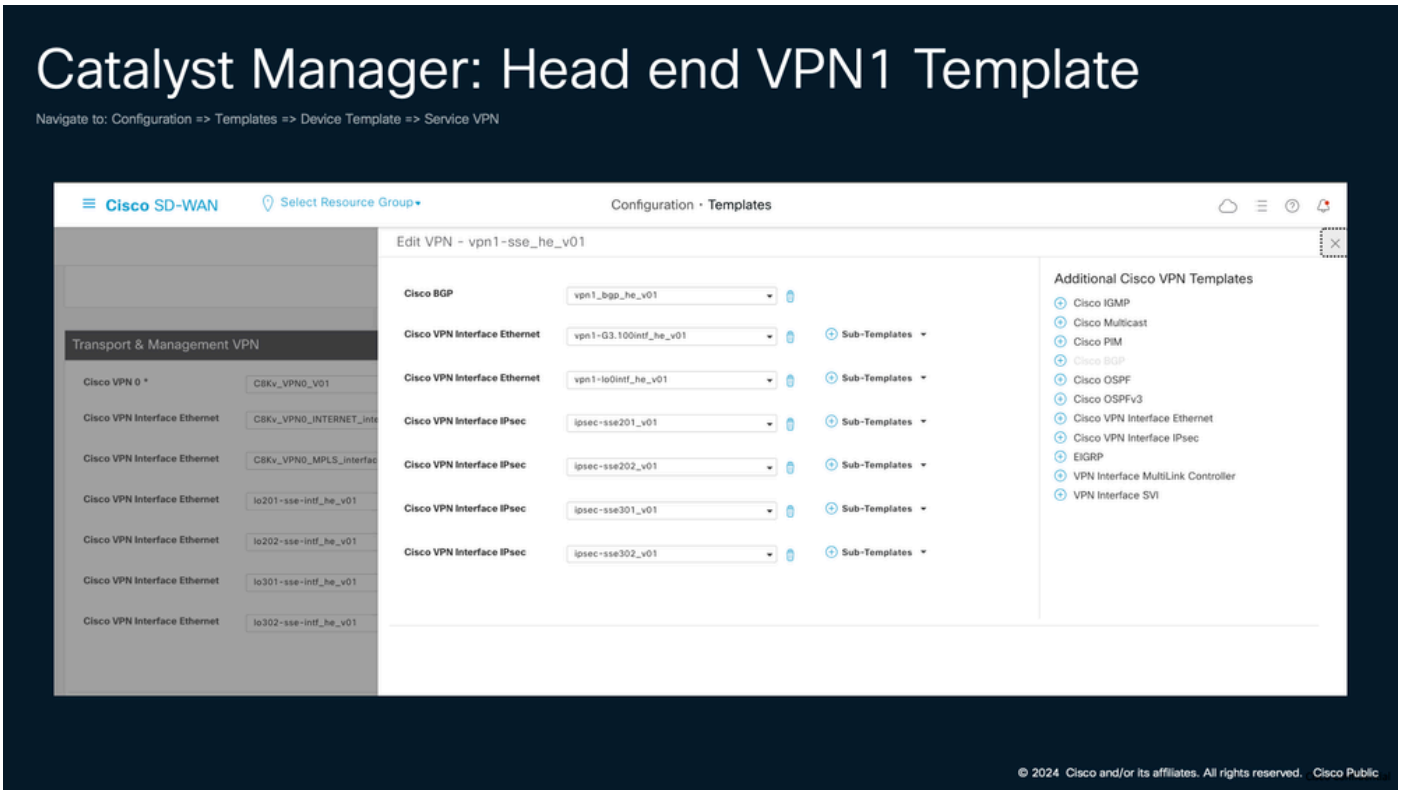
IKE-id voor lokaal eindpunt: mn03lab1@8167900-638880310-sse.cisco.com
IKE-id voor extern eindpunt: 35.171.xxx.xxx
IPsec-coderingssuite: AES 256 GCM
Perfect voorwaartse geheimhouding: None

Herhaal de stappen om de vereiste tunnels te configureren voor zowel de primaire als de secundaire beveiligde access hubs.Voor een 2x2 opstelling, zou u vier tunnels in totaal creëren:

- Twee tunnels van DC1-HE1 naar de primaire Secure Access-hub
- Twee tunnels van DC1-HE1 naar de secundaire beveiligde access hub

Nu de sjablonen zijn gemaakt, gebruiken we ze op de servicekant vrf in afbeelding 13 en de loopback gedefinieerd in bijlage op de globale vrf weergegeven in afbeelding 14.

Afbeelding 13: Catalyst SD-WAN Manager: Head-end VPN1 sjabloon 2x2



Catalyst Manager: Head-end VPN1-sjabloon

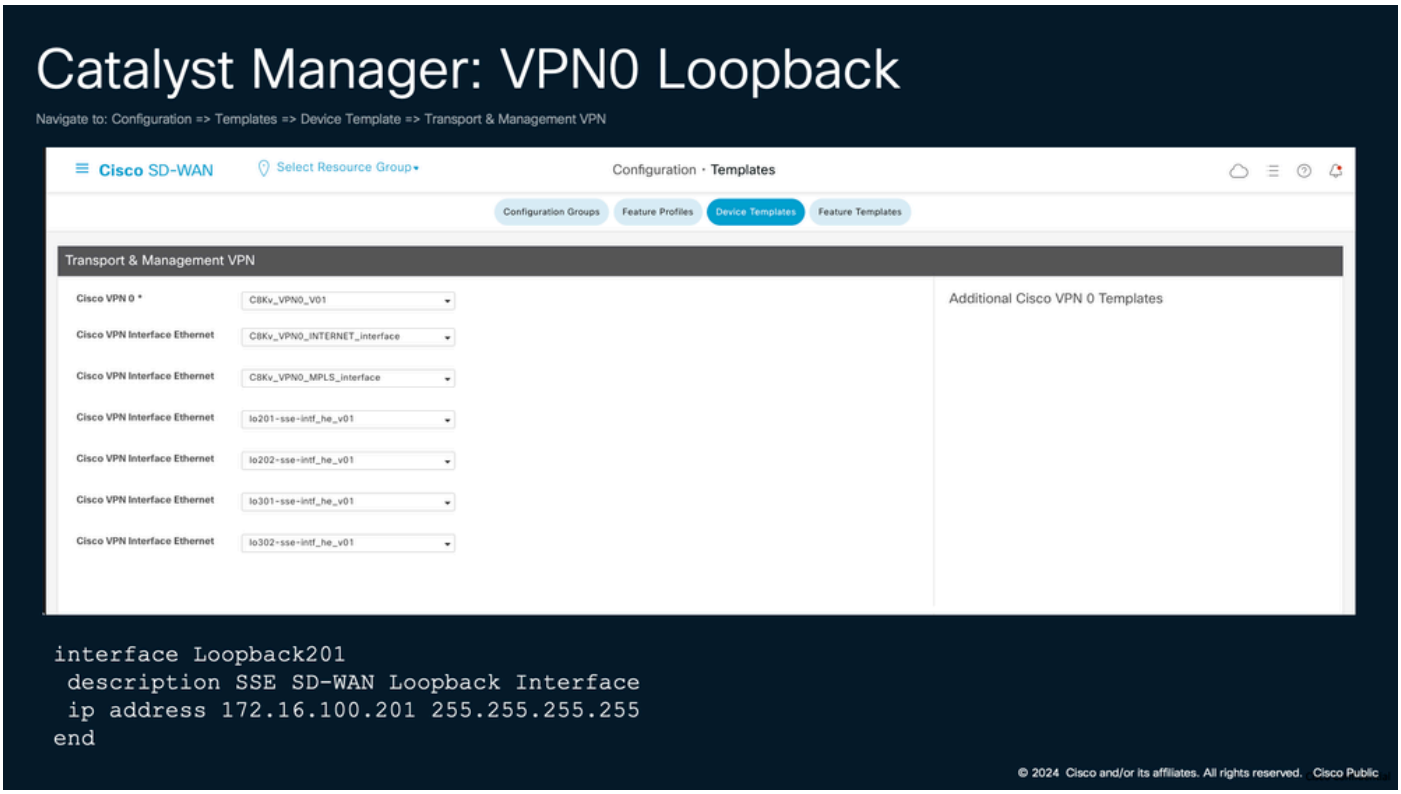
Stap 2: Bepaal de feedback in wereldwijde VRF

Configureer een loopback-interface in de algemene VRF-tabel (Virtual Routing and Forwarding). Deze loopback dient als de broninterface voor de IPSec-tunnel die in Stap 1 is gemaakt.

Alle loopback die in Stap 1 van verwijzingen wordt voorzien moet in Globale VRF worden bepaald.

IP-adres kan in elk RFC1918-bereik worden gedefinieerd.

Afbeelding 14: Catalyst SD-WAN Manager: VPN0-loopback

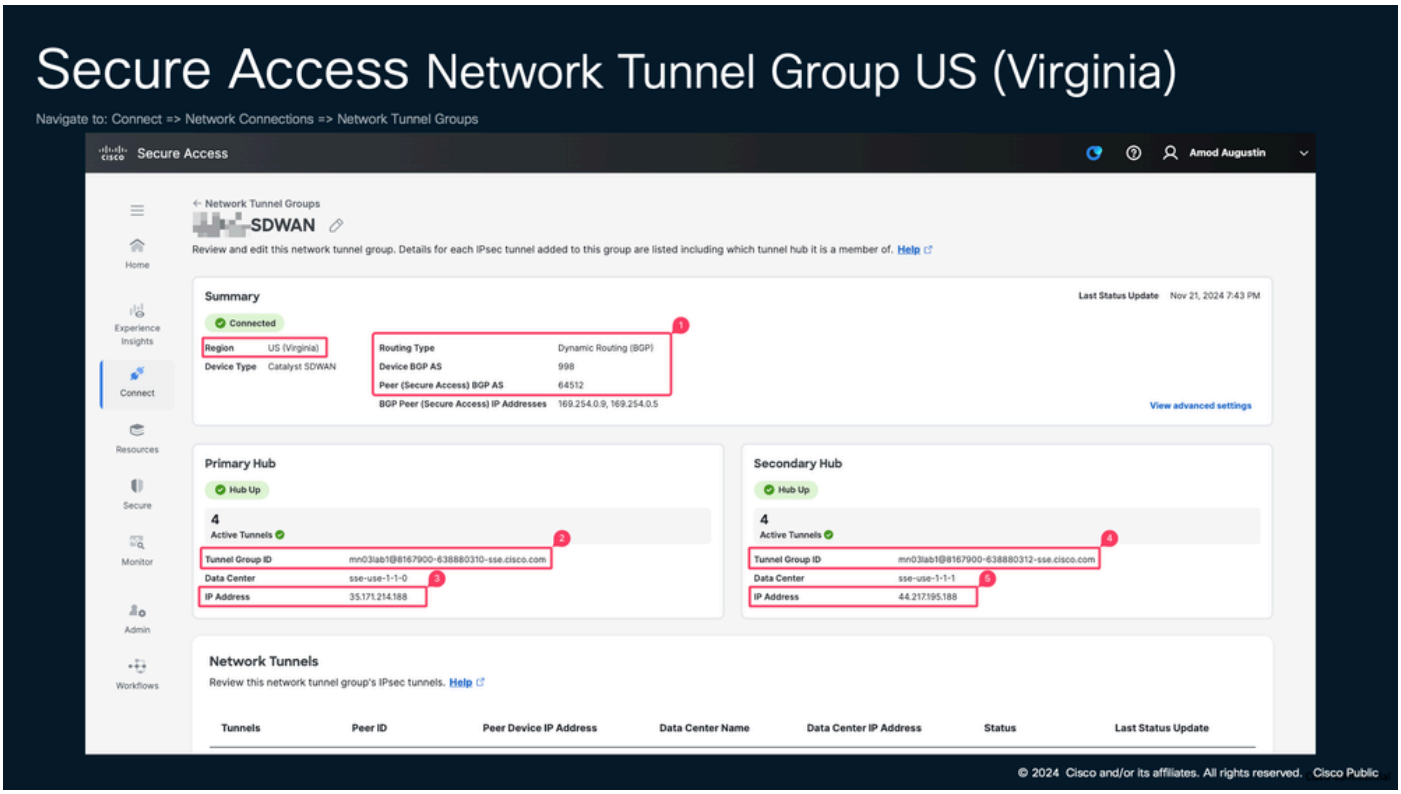


Catalyst Manager: VPN0-loopback

Procedure 3. BGP-nabuurschap configureren

Gebruik de BGP-functiesjabloon om de BGP-buurt voor alle tunnelinterfaces te definiëren. Raadpleeg de configuratie van de respectieve netwerktunnelgroepen en de BGP-configuratie in het Cisco Secure Access Portal om BGP-waarden te configureren.

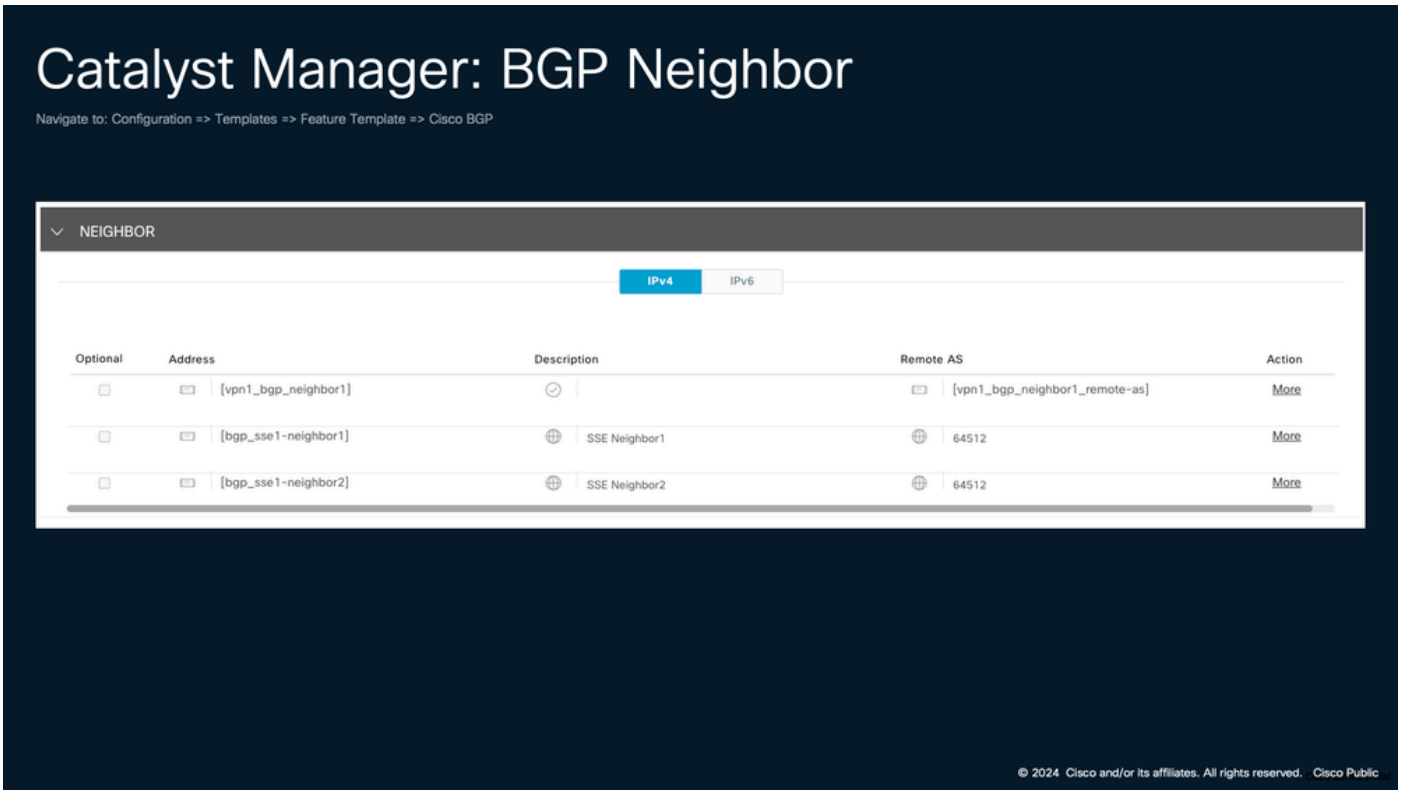
Afbeelding 15: Secure Access Network Tunnel Group (Virginia)



Secure Access Network Tunnel Group (Virginia)

In dit voorbeeld gebruiken we de informatie uit afbeelding 15 (vak 1) om BGP te definiëren met behulp van een functiesjabloon.

Afbeelding 16: Catalyst SD-WAN Manager BGP-buur



Catalyst SD-WAN Manager BGP-buur

Configuratie gegenereerd met behulp van de functiesjabloon:

```
router bgp 998
 bgp log-neighbor-changes
 !
 address-family ipv4 vrf 1
  network 10.10.128.1 mask 255.255.255.255
  neighbor 169.254.0.5 remote-as 64512
  neighbor 169.254.0.5 description SSE Neighbor1
  neighbor 169.254.0.5 ebgp-multihop 5
  neighbor 169.254.0.5 activate
  neighbor 169.254.0.5 send-community both
  neighbor 169.254.0.5 next-hop-self
  neighbor 169.254.0.9 remote-as 64512
  neighbor 169.254.0.9 description SSE Neighbor2
  neighbor 169.254.0.9 ebgp-multihop 5
  neighbor 169.254.0.9 activate
  neighbor 169.254.0.9 send-community both
  neighbor 169.254.0.9 next-hop-self
  neighbor 169.254.0.105 remote-as 64512
  neighbor 169.254.0.105 description SSE Neighbor3
  neighbor 169.254.0.105 ebgp-multihop 5
  neighbor 169.254.0.105 activate
  neighbor 169.254.0.105 send-community both
  neighbor 169.254.0.105 next-hop-self
  neighbor 169.254.0.109 remote-as 64512
  neighbor 169.254.0.109 description SSE Neighbor4
  neighbor 169.254.0.109 ebgp-multihop 5
  neighbor 169.254.0.109 activate
  neighbor 169.254.0.109 send-community both
  neighbor 169.254.0.109 next-hop-self
  neighbor 172.16.128.2 remote-as 65510
  neighbor 172.16.128.2 activate
  neighbor 172.16.128.2 send-community both
  neighbor 172.16.128.2 route-map sse-routes-in in
  neighbor 172.16.128.2 route-map sse-routes-out out
  maximum-paths eibgp 4
  distance bgp 20 200 20
 exit-address-family
DC1-HE1#
```

Verificatie

```
DC1-HE1#show ip route vrf 1 bgp | begin Gateway
Gateway of last resort is not set

35.0.0.0/32 is subnetted, 1 subnets
B 35.95.175.78 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
44.0.0.0/32 is subnetted, 1 subnets
B 44.240.251.165 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
100.0.0.0/8 is variably subnetted, 17 subnets, 2 masks
B 100.81.0.58/32 [20/0] via 169.254.0.9, 3d01h
```

```
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.59/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.60/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.61/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.62/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.63/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.64/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.65/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h

DC1-HE1#show ip bgp vpnv4 all summary
BGP router identifier 172.16.100.232, local AS number 998

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
169.254.0.5 4 64512 12787 13939 3891 0 0 4d10h 18
169.254.0.9 4 64512 66124 64564 3891 0 0 3d01h 18
169.254.0.13 4 64512 12786 13933 3891 0 0 4d10h 18
169.254.0.17 4 64512 12786 13927 3891 0 0 4d10h 18
172.16.128.2 4 65510 83956 84247 3891 0 0 7w3d 1

DC1-HE1#show ip interface brief | include Tunnnel
Tunnel1 192.168.128.202 YES TFTP up up
Tunnel4 198.18.128.11 YES TFTP up up
Tunnel100022 172.16.100.22 YES TFTP up up
Tunnel100023 172.16.100.23 YES TFTP up up
Tunnel100201 169.254.0.6 YES other up up
Tunnel100202 169.254.0.10 YES other up up
Tunnel100301 169.254.0.14 YES other up up
Tunnel100302 169.254.0.18 YES other up up
```

Referentie

Een actieve/actieve implementatie zou een multipath van de kern switch hebben die is verbonden met beide SD-WAN head-ends.

Afbeelding 17: Active/actief scenario voor BGP-buur

```
DC1-Core-Switch#show ip bgp
BGP table version is 62893, local router ID is 172.16.128.6
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,

     Network          Next Hop            Metric LocPrf Weight Path
 *m   1.1.1.1/32       172.16.128.5           65535             0 998 ?
 *>                    172.16.128.1           65535             0 998 ?
 *m   3.[redacted]/32  172.16.128.5           65535             0 998 ?
 *>                    172.16.128.1           65535             0 998 ?
 *m   3.[redacted]/32  172.16.128.5           65535             0 998 ?
 *>                    172.16.128.1           65535             0 998 ?
<snip>
```

Actieve/actieve BGP-buur

Een Active/Stanby-implementatie zou een één actief pad hebben van de kern switch naar SD-WAN head-ends vanwege ASPL preending (wat gebeurt met een routekaart naar de buur).

Afbeelding 18: Active/stand-by scenario voor BGP-buur

```
DC1-Core-Switch#show ip bgp
BGP table version is 62893, local router ID is 172.16.128.6
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,

     Network          Next Hop            Metric LocPrf Weight Path
 *    1.1.1.1/32       172.16.128.5           65535             0 998 998?
 *>                    172.16.128.1           65535             0 998 ?
 *    [redacted]32     172.16.128.5           65535             0 998 998?
 *>                    172.16.128.1           65535             0 998 ?
 *    [redacted]/32    172.16.128.5           65535             0 998 998?
 *>                    172.16.128.1           65535             0 998 ?
 <snip>
```

Active/stand-by BGP-buur

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.