Konfigurieren einer privaten App-Verbindung zwischen Sicherheitsservice-Edge und SD-WAN mithilfe der manuellen Methode

Inhalt

Einleitung

Dieses Dokument beschreibt einen umfassenden Leitfaden für die Verbindung von Cisco Secure Access mit SD-WAN-Routern mit Schwerpunkt auf dem sicheren Zugriff über private Anwendungen.

Informationen zu diesem Leitfaden

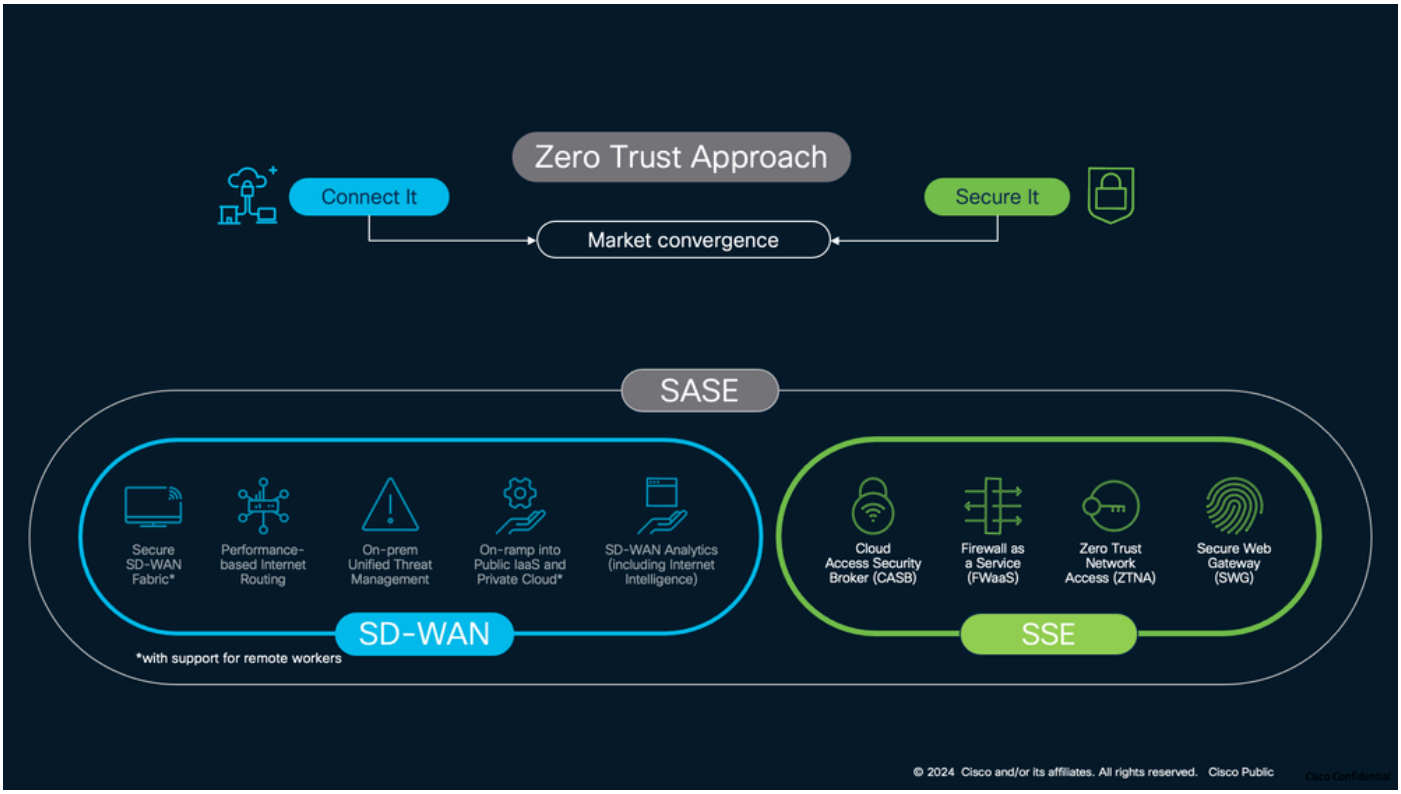
Hinweis: Die hier aufgeführten Konfigurationen wurden für die SD-WAN-Versionen UX1.0 und 17.9/20.9 entwickelt.

In diesem Leitfaden wird eine strukturierte exemplarische Vorgehensweise mit den folgenden wichtigen Schritten vorgestellt:

- Definieren von Netzwerk-Tunnelgruppen (NTGs)
- IPSec-Tunnelkonfiguration: Detaillierte Anleitung zum Einrichten sicherer IPSec-Tunnel zwischen Cisco SD-WAN-Routern und Cisco Secure Access NTGs.
- BGP-Nachbarschaft: Schrittweise Verfahren zum Ausführen von BGP-Nachbarschaften über

die IPSec-Tunnel, um dynamisches Routing und verbesserte Ausfallsicherheit des Netzwerks zu gewährleisten.
- Privater Anwendungszugriff: Anleitung zur Konfiguration und Sicherung des Zugriffs auf private Anwendungen über die eingerichteten Tunnel.

Abbildung 1: Der Cisco SD-WAN- und SSE Zero Trust-Ansatz



SSE mit SD-WAN

Der Schwerpunkt dieses Leitfadens liegt auf Überlegungen zum Design und Best Practices für die Bereitstellung von NTG Interconnects. In diesem Leitfaden werden SD-WAN-Controller in der Cloud und WAN-Edge-Router im Rechenzentrum bereitgestellt und mit mindestens einem Internetanschluss verbunden.

Wichtigste Annahmen

- Cisco Secure Access Secure Service Edge (SSE): Es wird davon ausgegangen, dass die Cisco Secure Access SSE bereits für Ihr Unternehmen bereitgestellt wurde.
- Cisco SD-WAN-WAN-Edge-Router: Es wird davon ausgegangen, dass der WAN-Edge-Router in das Overlay-Netzwerk integriert ist, um den Benutzerdatenverkehr in der gesamten SD-WAN-Infrastruktur effizient zu vereinfachen.
- Der Schwerpunkt dieses Leitfadens liegt zwar primär auf den SD-WAN-Aspekten von Design und Konfiguration, er bietet jedoch einen ganzheitlichen Ansatz zur Integration von Cisco Secure Access-Lösungen in Ihre bestehende Netzwerkarchitektur.

Über diese Lösung

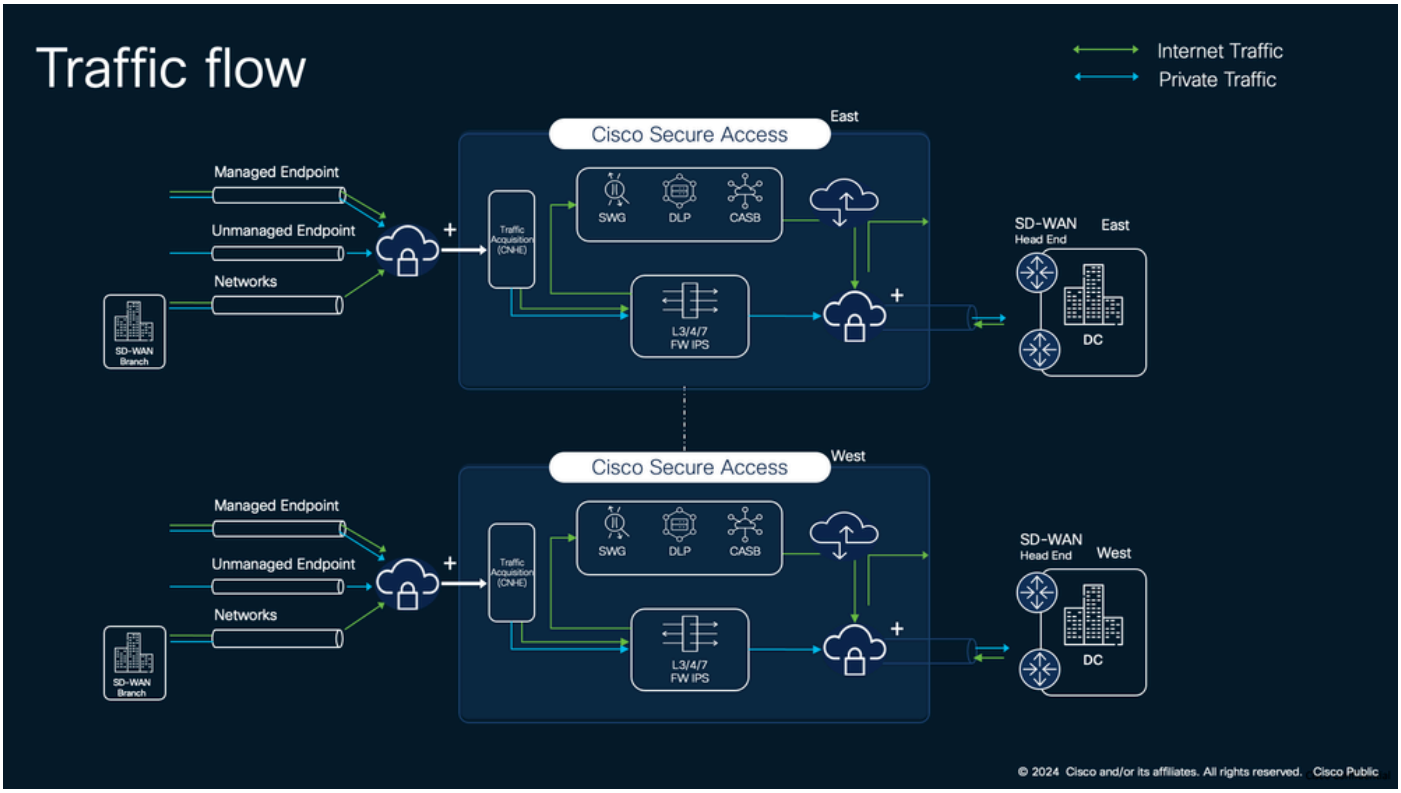
Private App-Tunnel, die von Cisco Secure Access angeboten werden, bieten Benutzern sichere

Verbindungen zu privaten Anwendungen, die über ZTNA (Zero Trust Network Access) und VPN-as-a-Service (VPNaaS) verbunden sind. Mithilfe dieser Tunnel können Unternehmen Remote-Benutzer sicher mit privaten Ressourcen verbinden, die in Rechenzentren oder Private Clouds gehostet werden.
Mithilfe von IKEv2 (Internet Key Exchange Version 2) stellen diese Tunnelgruppen sichere bidirektionale Verbindungen zwischen Cisco Secure Access und SD-WAN-Routern her. Sie unterstützen hohe Verfügbarkeit über mehrere Tunnel innerhalb einer Gruppe und bieten ein flexibles Datenverkehrsmanagement über statisches und dynamisches Routing (BGP).
Die IPsec-Tunnel können Datenverkehr von verschiedenen Quellen transportieren, darunter:

- Remote Access-VPN-Benutzer
- Browserbasierte oder clientbasierte ZTNA-Verbindungen
- Andere Netzwerkstandorte, die mit Cisco Secure Access verbunden sind

Dieser Ansatz ermöglicht die sichere Weiterleitung aller Arten von privatem Anwendungsdatenverkehr über einen einheitlichen, verschlüsselten Kanal, wodurch sowohl die Sicherheit als auch die Betriebseffizienz verbessert werden.
Cisco Secure Access ist Teil der Cisco Security Service Edge (SSE)-Lösung und vereinfacht IT-Abläufe durch eine einzige, über die Cloud verwaltete Konsole, einen einheitlichen Client, die zentrale Richtlinienerstellung und aggregierte Berichte. Sie umfasst mehrere Sicherheitsmodule in einer Cloud-basierten Lösung, darunter ZTNA, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS), DNS-Sicherheit, Remote Browser Isolation (RBI) und vieles mehr. Dieser umfassende Ansatz minimiert Sicherheitsrisiken durch die Anwendung von "Zero Trust"-Prinzipien und die Durchsetzung präziser Sicherheitsrichtlinien

Abbildung 2: Datenverkehrsfluss zwischen Cisco Secure Access und privaten Anwendungen



Datenverkehrsfluss der privaten SSE-Anwendung

Die in diesem Leitfaden beschriebene Lösung berücksichtigt umfassende Redundanzüberlegungen, die sowohl den SD-WAN-Router im Rechenzentrum als auch die Network Tunnel Group (NTG) am Security Service Edge (SSE) umfassen. Der Schwerpunkt dieses Leitfadens liegt auf einem Aktiv/Aktiv-SD-WAN-Hub-Bereitstellungsmodell, das einen unterbrechungsfreien Datenverkehrsfluss gewährleistet und eine hohe Verfügbarkeit gewährleistet.

Voraussetzungen

Anforderungen

Es wird empfohlen, dass Sie über Kenntnisse in den folgenden Themen verfügen:

- Konfiguration und Verwaltung des Cisco SD-WAN
- Grundkenntnisse der IKEv2- und IPSec-Protokolle
- Konfiguration der Netzwerk-Tunnelgruppe im Cisco Secure Access-Portal
- Kenntnisse von BGP und ECMP

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco SD-WAN Controller auf 20.9.5a
- Cisco SD-WAN WAN-Edge-Router mit 17.9.5a
- Cisco Secure Access-Portal

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Design

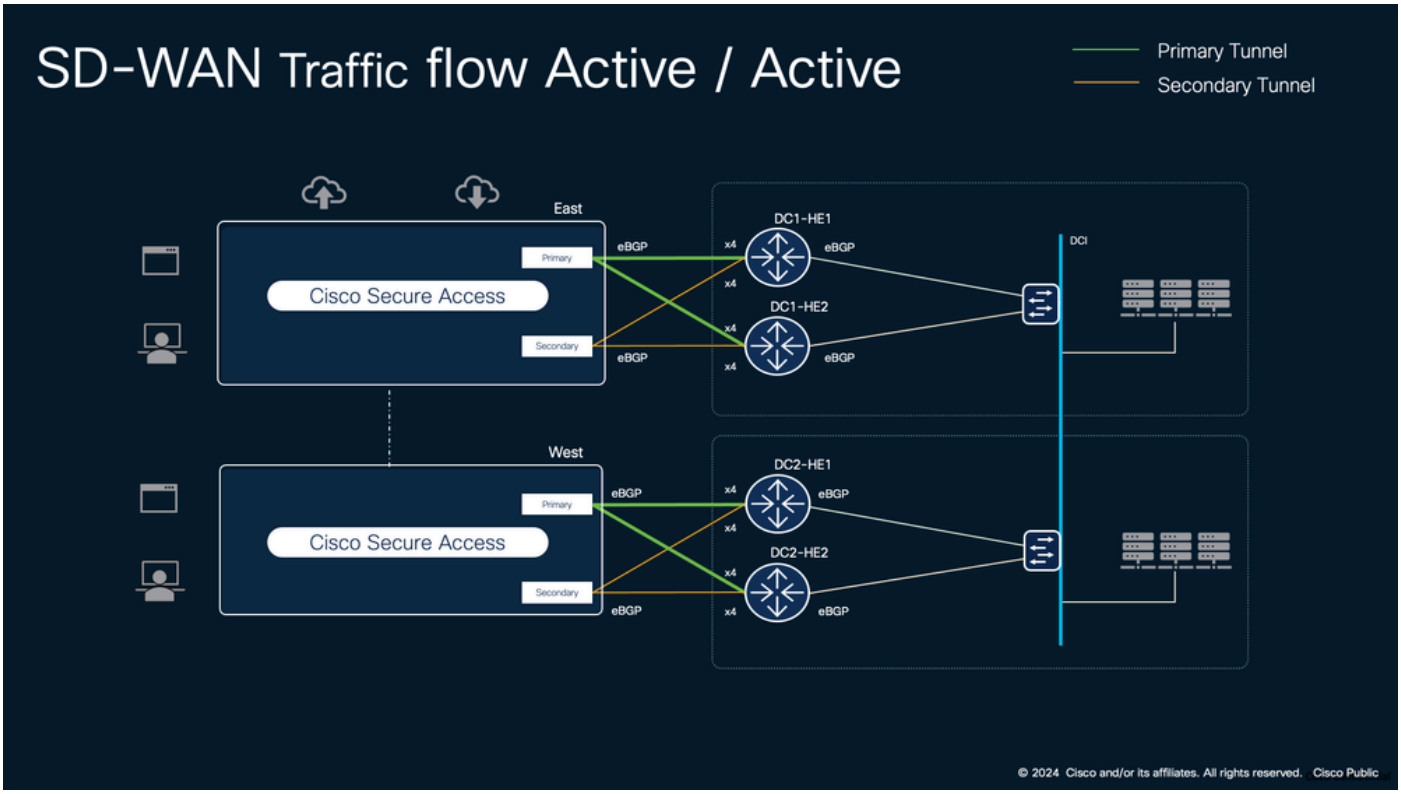
In diesem Leitfaden wird die Lösung anhand eines Aktiv/Aktiv-Designmodells für SD-WAN-Headend-Router beschrieben. Ein Aktiv/Aktiv-Designmodell im Kontext von SD-WAN-Headend-Routern setzt zwei Router in einem Rechenzentrum voraus, die beide mit der Security Service Edge (SSE) Network Tunnel Group (NTG) verbunden sind, wie in Abbildung 3 dargestellt. In diesem Szenario verarbeiten beide SD-WAN-Router im Rechenzentrum (DC1-HE1 und DC1-HE2) aktiv den Datenverkehrsfluss. Dazu senden sie dieselbe AS-Pfadlänge (ASPL) an den internen Nachbarn des Rechenzentrums. Dadurch wird der Datenverkehr innerhalb des Rechenzentrums zwischen den beiden Headends ausgeglichen.

Jeder Headend-Router kann mehrere Tunnel zu SSE Points of Presence (POPs) einrichten. Die Anzahl der Tunnel variiert je nach Anforderungen und SD-WAN-Gerätemodell. Bei diesem Design:

- Jeder Router verfügt über 4 Tunnel zum primären SSE-Hub und 4 Tunnel zum sekundären SSE-Hub.
- Die maximale Anzahl der von jedem SSE-Hub unterstützten Tunnel kann variieren. Die aktuellsten Informationen finden Sie in der offiziellen Dokumentation: https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

Diese Headend-Router bilden über die Tunnel zum SSE BGP-Nachbarschaften. Über diese Nachbarschaften kündigen die Headends ihren SSE-Nachbarn private Anwendungspräfixe an, was ein sicheres und effizientes Routing des Datenverkehrs zu privaten Ressourcen ermöglicht.

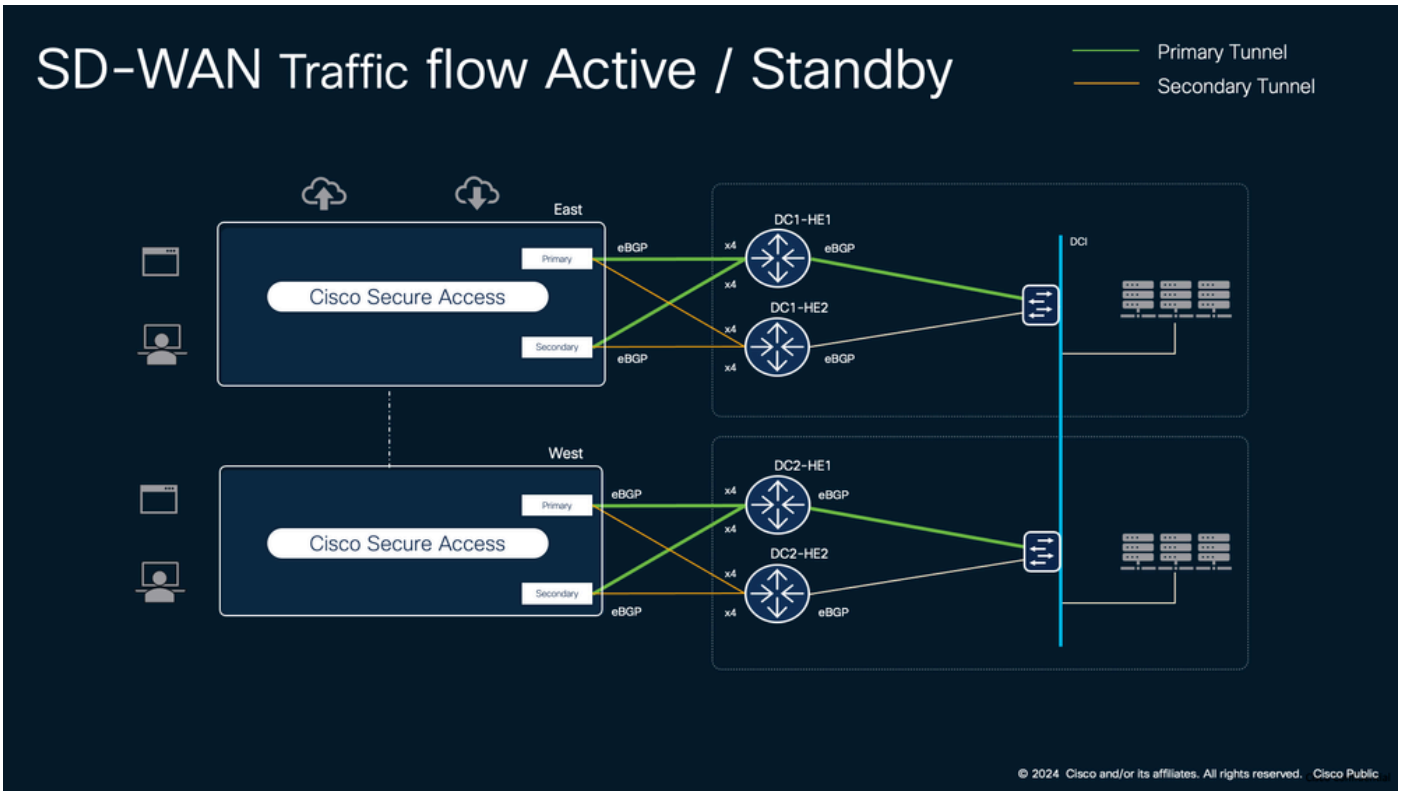
Abbildung 3: SD-WAN zu SSE Aktiv/Aktiv-Bereitstellungsmodell



SD-WAN zu SSE Aktiv/Aktiv-Bereitstellungsmodell

Bei einem Aktiv/Standby-Design ist ein Router (DC1-HE1) immer aktiv, während der sekundäre Router (DC1-HE2) im Standby-Modus verbleibt. Der Datenverkehr fließt konsistent über das aktive Headend (DC1-HE1), es sei denn, er fällt vollständig aus. Dieses Bereitstellungsmodell hat den Nachteil: Wenn der primäre Tunnel zu SSE ausfällt, wechselt der Datenverkehr zu den sekundären SSE-Tunneln, die nur über DC1-HE2 erreicht werden, wodurch der zustandsbehaftete Datenverkehr zurückgesetzt wird.
Im Aktiv/Standby-Modell dient die BGP AS-Path-Länge dazu, den Datenverkehr innerhalb des Rechenzentrums und in Richtung SSE zu lenken. DC1-HE1 sendet Präfix-Updates an den SSE BGP-Nachbarn mit einer ASPL von 2, während DC1-HE2 Updates mit einer ASPL von 3 sendet. Der interne DC-Nachbarn von DC1-HE1 kündigt Präfixe mit einer kürzeren AS-Pfadlänge als DC1-HE2 an und stellt so sicher, dass der Datenverkehr für DC1-HE1 bevorzugt wird. (Kunden können andere Attribute oder Protokolle auswählen, um die Datenverkehrspräferenz zu beeinflussen.) Kunden können je nach ihren spezifischen Anforderungen entweder ein aktives/aktives oder ein aktives/Standby-Bereitstellungsmodell auswählen.

Abbildung 4: Bereitstellungsmodell SD-WAN zu SSE Aktiv/Standby



Bereitstellungsmodell SD-WAN zu SSE Aktiv/Standby

Konfigurieren

In diesem Abschnitt wird das Verfahren beschrieben:

1. Überprüfen der Voraussetzungen für die Bereitstellung einer Netzwerk-Tunnelgruppe im Cisco Secure Access-Portal
2. Konfigurieren Sie die SD-WAN-Verbindung mit der Cisco Secure Access Network Tunnel Group (NTG) mithilfe der manuellen IPsec-Methode.
3. Konfigurieren der BGP-Nachbarschaft

Anmerkung: Diese Konfiguration basiert auf einem Active/Active-Bereitstellungsmodell.

Verfahren 1: Überprüfen der Konfiguration der Netzwerk-Tunnelgruppe im Cisco Secure Access-Portal

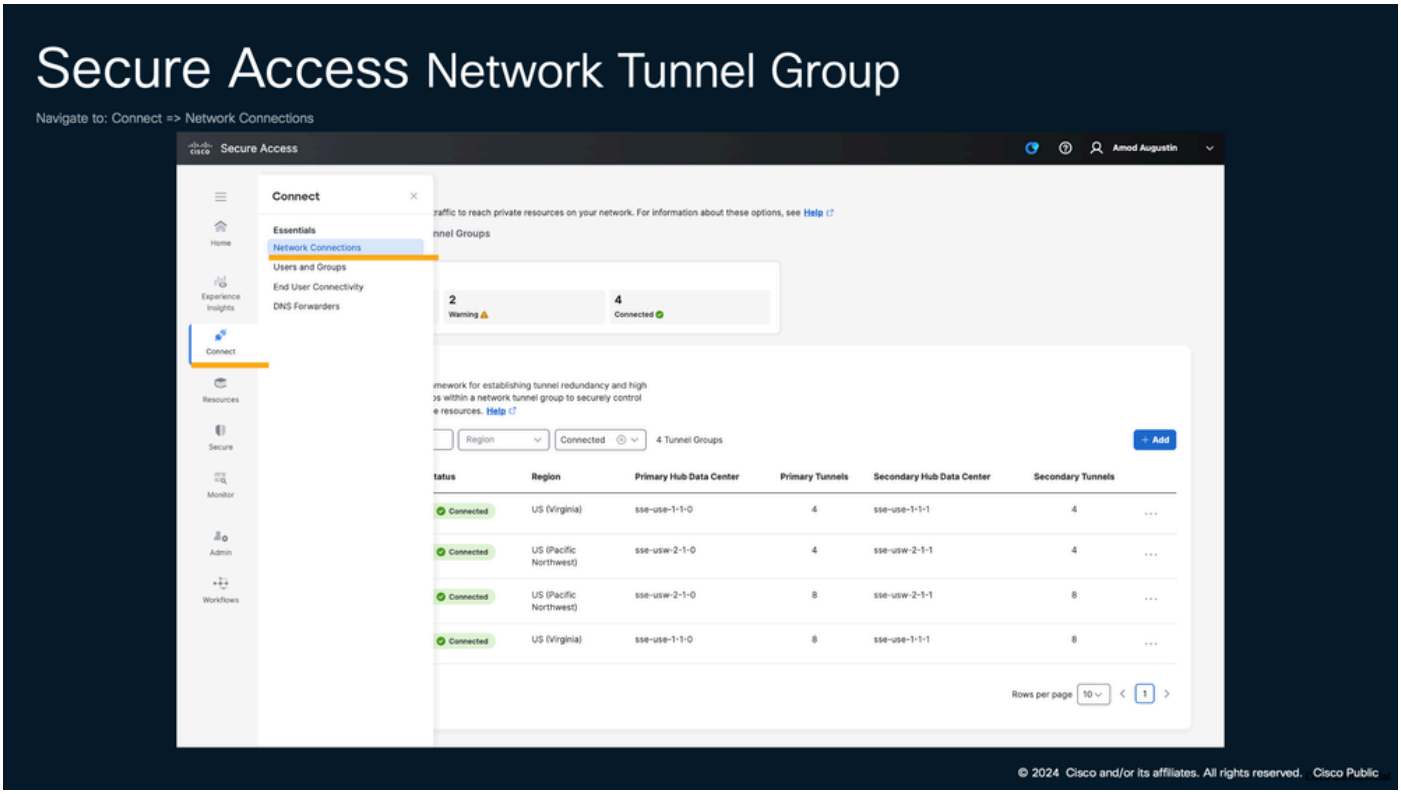
Die Konfiguration der Netzwerk-Tunnelgruppe wird im Leitfaden nicht behandelt. Bitte lesen Sie diese Referenz.

- Netzwerk-Tunnelgruppe hinzufügen: SSE-Dokumentation
- Konfigurieren von Netzwerktunneln zwischen Cisco Secure Access und dem Cisco IOS XE-Router mit ECMP und BGP

Navigieren Sie zu Cisco Secure Access, und stellen Sie sicher, dass die Network Tunnel Groups (NTGs) bereitgestellt werden. Für das vorliegende Design müssen NTGs in zwei verschiedenen Points of Presence (POPs) bereitgestellt werden. In diesem Leitfaden werden NTG in den POP-Standorten USA (Virginia) und USA (Pacific Northwest) verwendet.

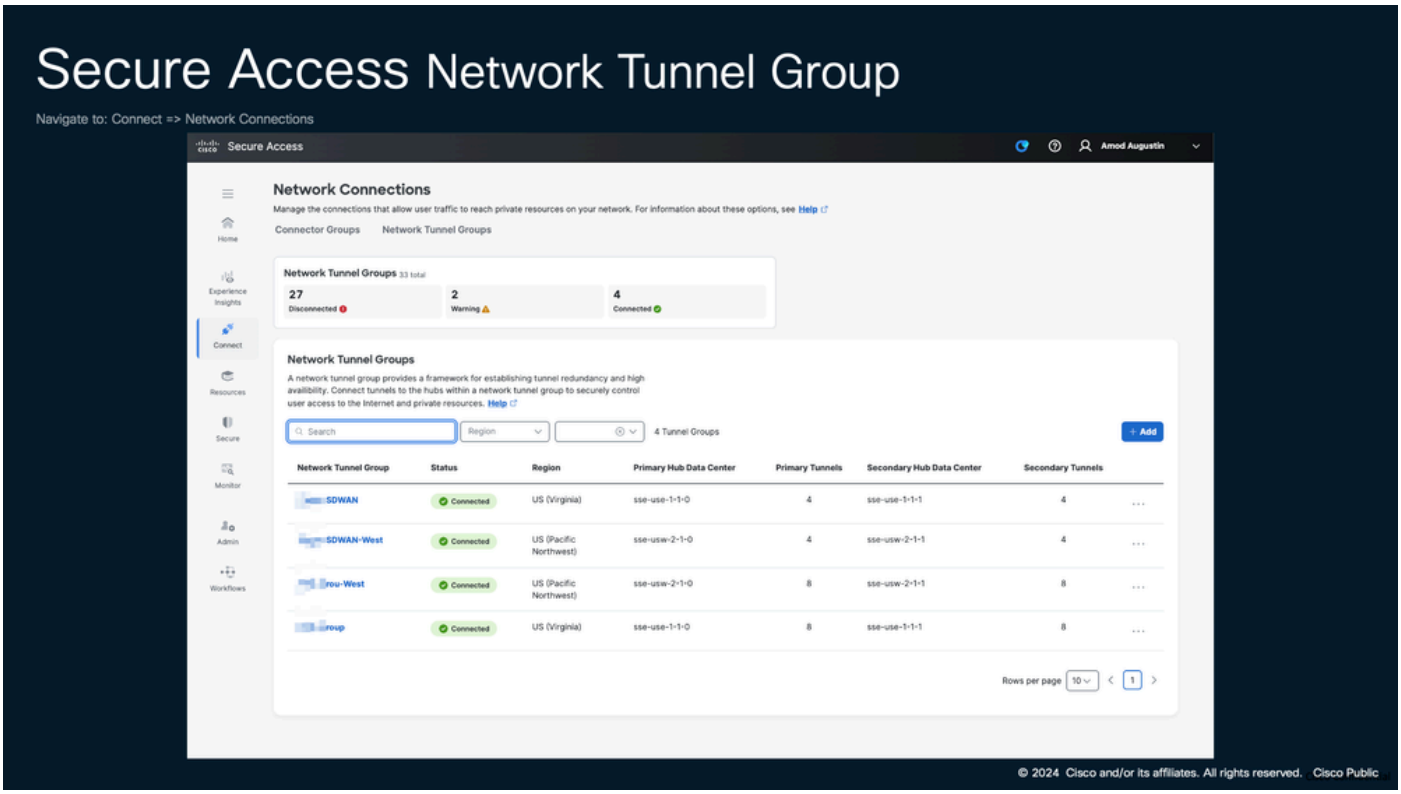
Hinweis:Die Namen und Standorte von POPs können variieren, das Hauptkonzept besteht jedoch darin, mehrere NTGs an Standorten bereitzustellen, die sich geografisch in der Nähe Ihres Rechenzentrums befinden. Dieser Ansatz trägt zur Optimierung der Netzwerkleistung bei und bietet Redundanz.

Abbildung 5: Cisco Secure Access Network Tunnel Group



Cisco Secure Access Network Tunnel Group

Abbildung 6: Liste der Cisco Secure Access Network Tunnel-Gruppen



Liste der Tunnelgruppen für sicheres Zugriffsnetzwerk

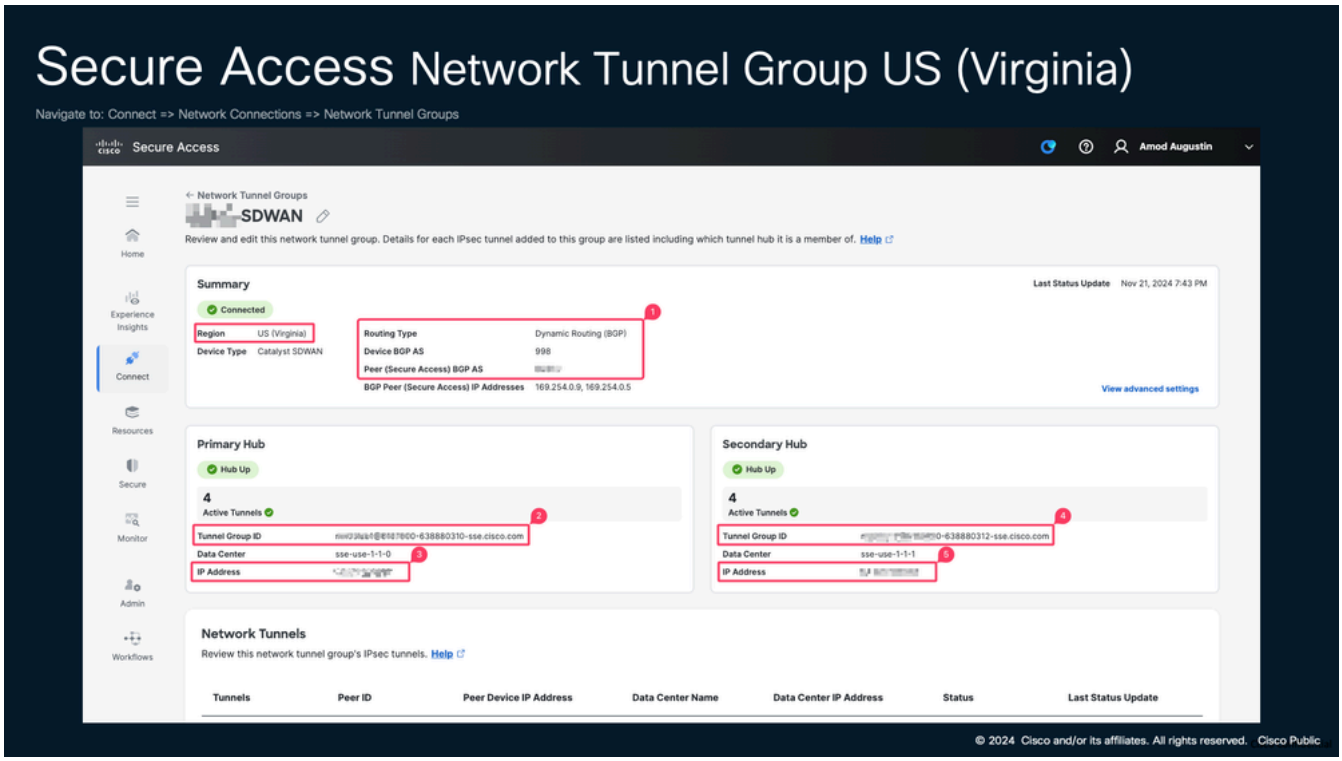
Stellen Sie sicher, dass Sie die Tunnel-Passphrase notiert haben (diese wird nur einmal während der Tunnelerstellung angezeigt).

Anmerkung: Schritt 6 unter Hinzufügen einer Netzwerk-Tunnelgruppe

---

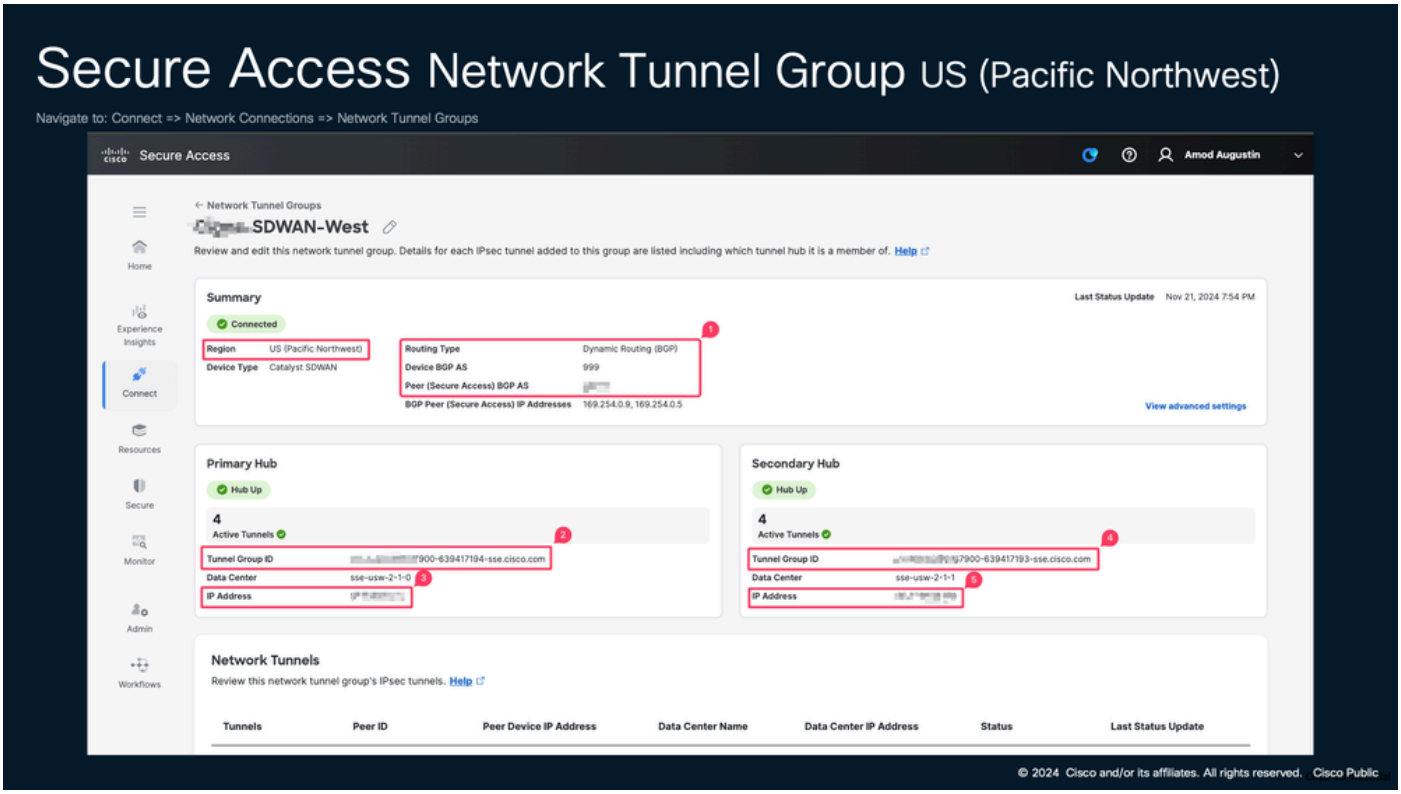
Notieren Sie sich auch die Attribute der Tunnelgruppe, die wir während der IPSec-Konfiguration verwenden. Der Screenshot (Abbildung 6) stammt aus einer Laborumgebung für ein Produktionsszenario, in dem NTG-Gruppen entsprechend der Design- oder Verwendungsempfehlung erstellt werden.

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



Secure Access Network Tunnel Group USA (Virginia)

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



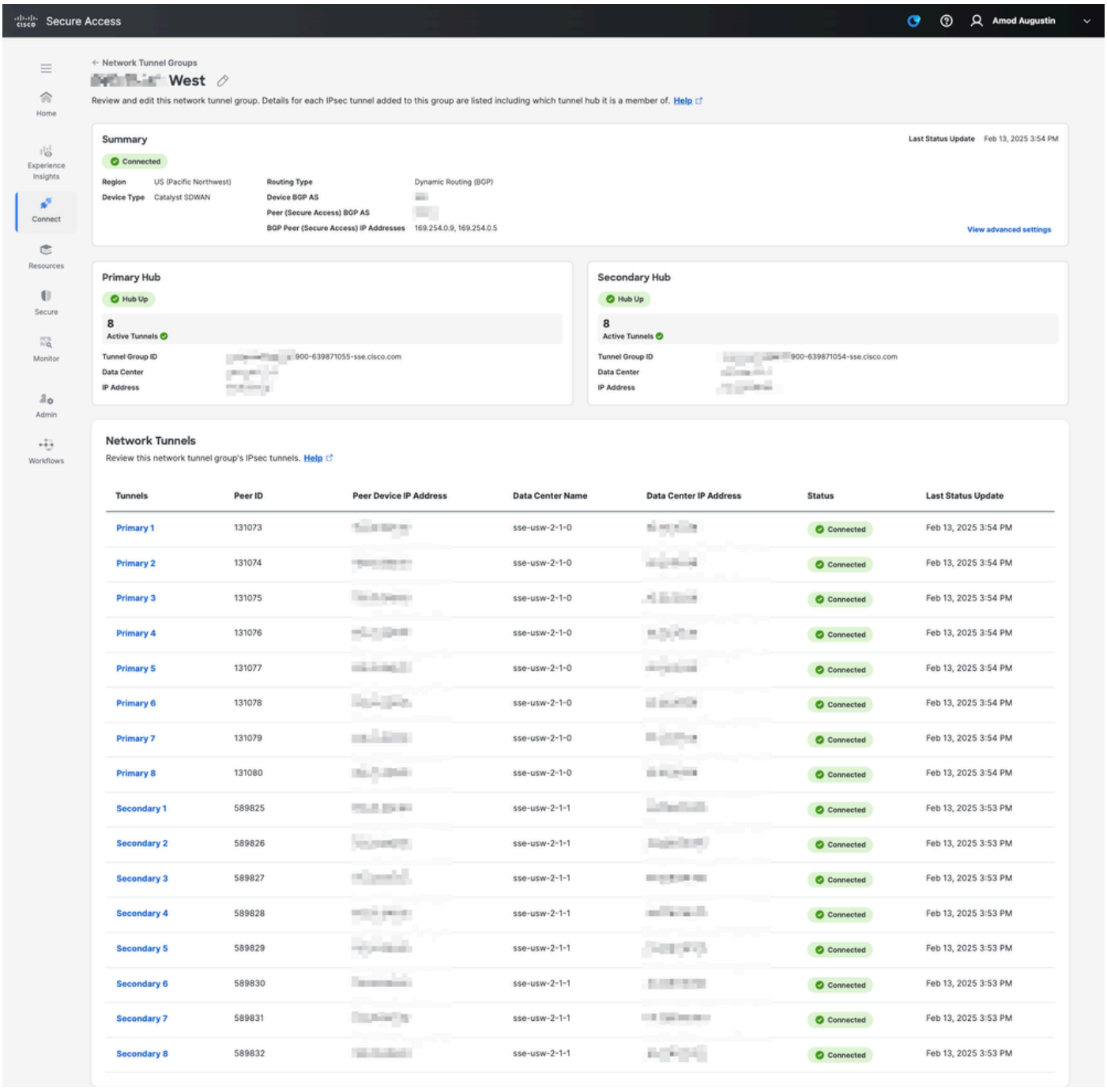
Secure Access Network Tunnel Group US (Pazifik-Nordwesten)

In Abbildung 8 sind nur vier Tunnel an den primären und sekundären Hubs dargestellt. Es wurden jedoch maximal 8 Tunnel erfolgreich in einer Controller-Umgebung getestet. Die maximale Tunnelunterstützung kann je nach verwendetem Hardwaregerät und aktueller SSE-Tunnelunterstützung variieren. Die aktuellsten Informationen finden Sie in der offiziellen

Dokumentation: https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels und den Release-Hinweis des jeweiligen Hardware-Geräts.

Ein Beispiel für einen 8-Tunnel-Aufbau ist hier dargestellt.

Abbildung 8a: NTG-Tunnel mit bis zu 8 Tunneln



SSE NTG bis zu 8 Tunnel

Verfahren 2: Konfigurieren der SD-WAN-Verbindung mit der Cisco Secure Access Network Tunnel Group (NTG) mithilfe der manuellen IPsec-Methode

Dieses Verfahren zeigt, wie eine Network Tunnel Group (NTG) mithilfe von Funktionsvorlagen auf dem Cisco Catalyst SD-WAN Manager 20.9 und dem Cisco Catalyst Edge Router der Version

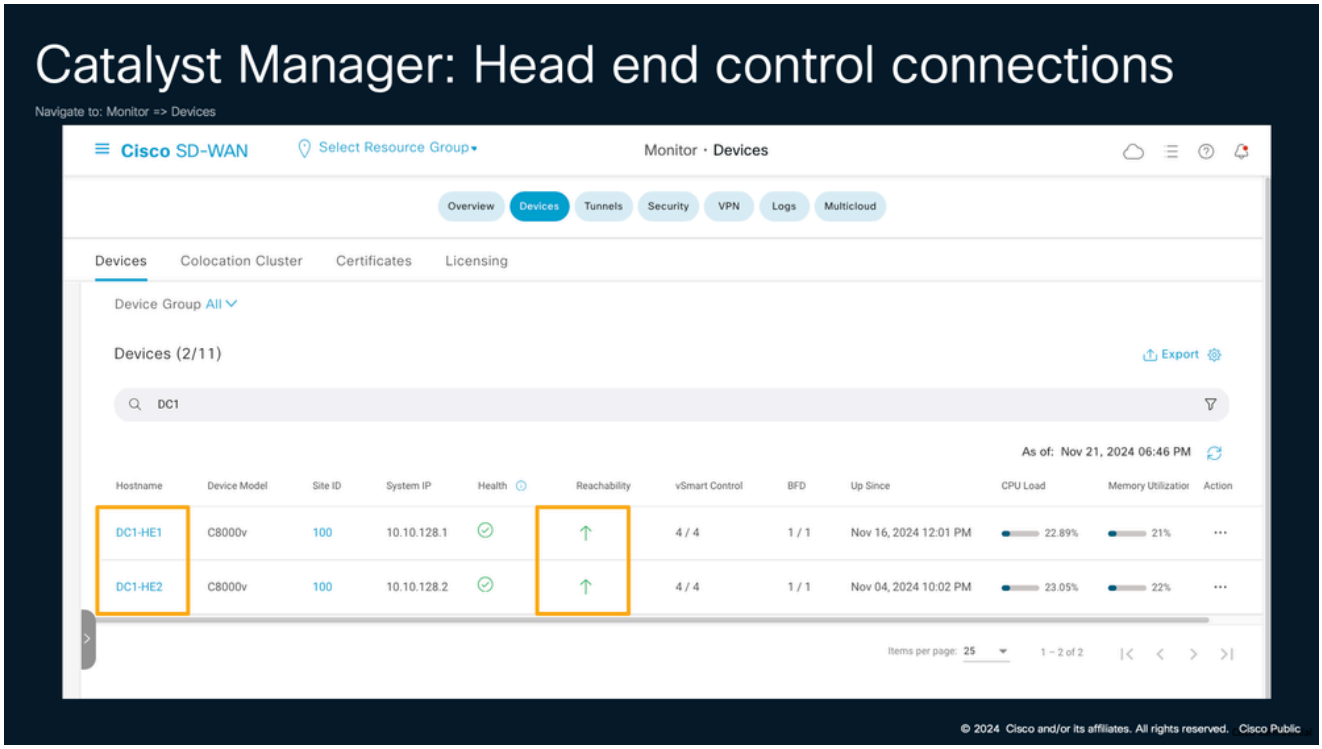
17.9 verbunden wird.

Hinweis: In diesem Leitfaden wird von einer vorhandenen SD-WAN-Overlay-Bereitstellung mit Hub-and-Spoke- oder vollständig vernetzter Topologie ausgegangen, bei der Hubs als Zugangspunkte für im Rechenzentrum gehostete private Anwendungen dienen. Dieses Verfahren kann auch auf Bereitstellungen in Zweigstellen oder in der Cloud angewendet werden.

Bevor Sie fortfahren, stellen Sie sicher, dass die Voraussetzungen erfüllt sind:

1. Steuerungsverbindungen sind am Gerät aktiviert, um erforderliche Updates vom Cisco Catalyst SD-WAN Manager zu ermöglichen.

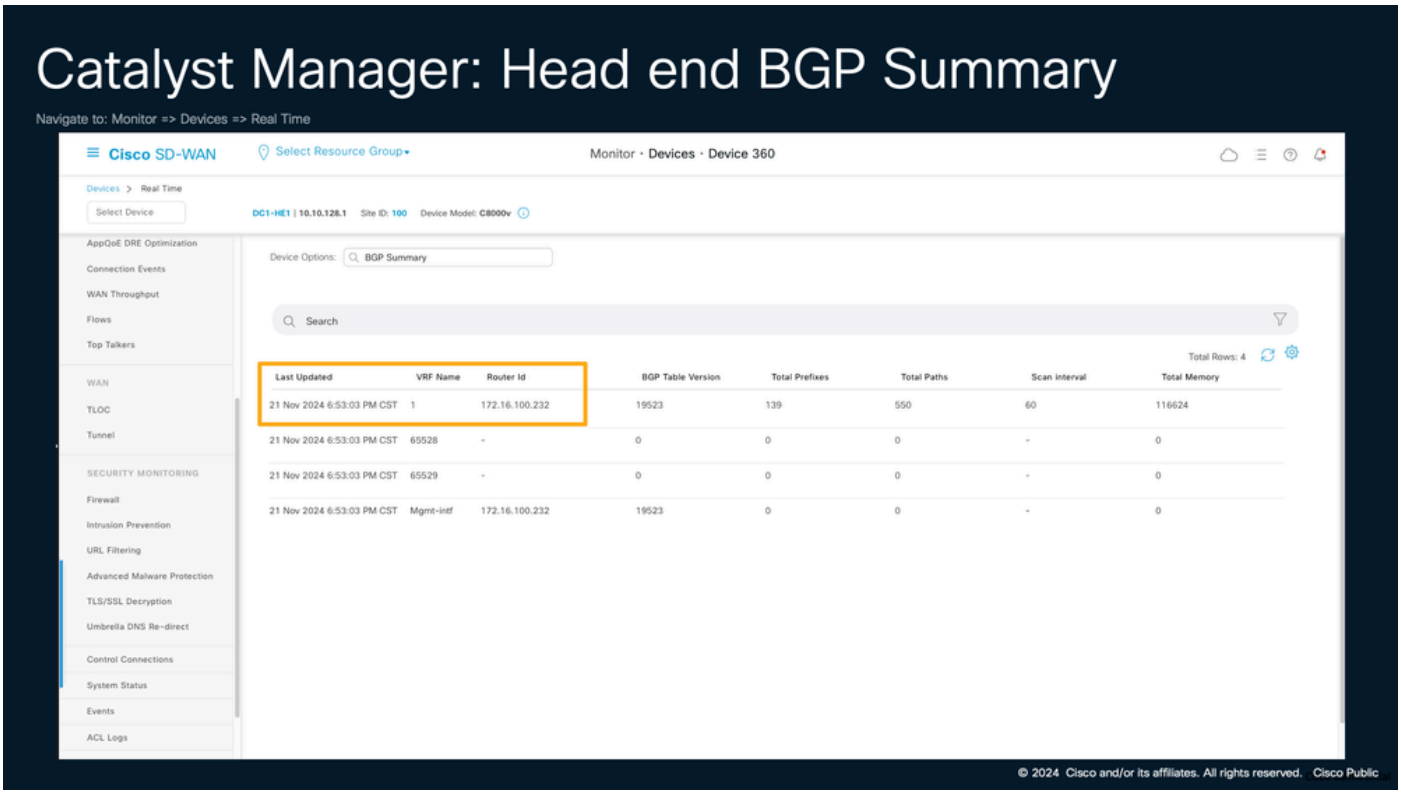
   Abbildung 9: Cisco Catalyst SD-WAN-Manager: Steueranschlüsse am Kopfende

   Catalyst Manager: Steueranschlüsse am Kopfende

2. Dienstseitige VPNs werden konfiguriert und verwenden ein Routing-Protokoll, um Präfixe anzukündigen. In diesem Leitfaden wird BGP als Routing-Protokoll auf der Serviceseite verwendet.

Abbildung 10: Cisco Catalyst SD-WAN-Manager: BGP-Headend - Zusammenfassung



Führen Sie die folgenden Schritte aus, um die SD-WAN-Verbindung mithilfe der manuellen IPSec-Methode mit der Network Tunnel Group (NTG) zu konfigurieren:

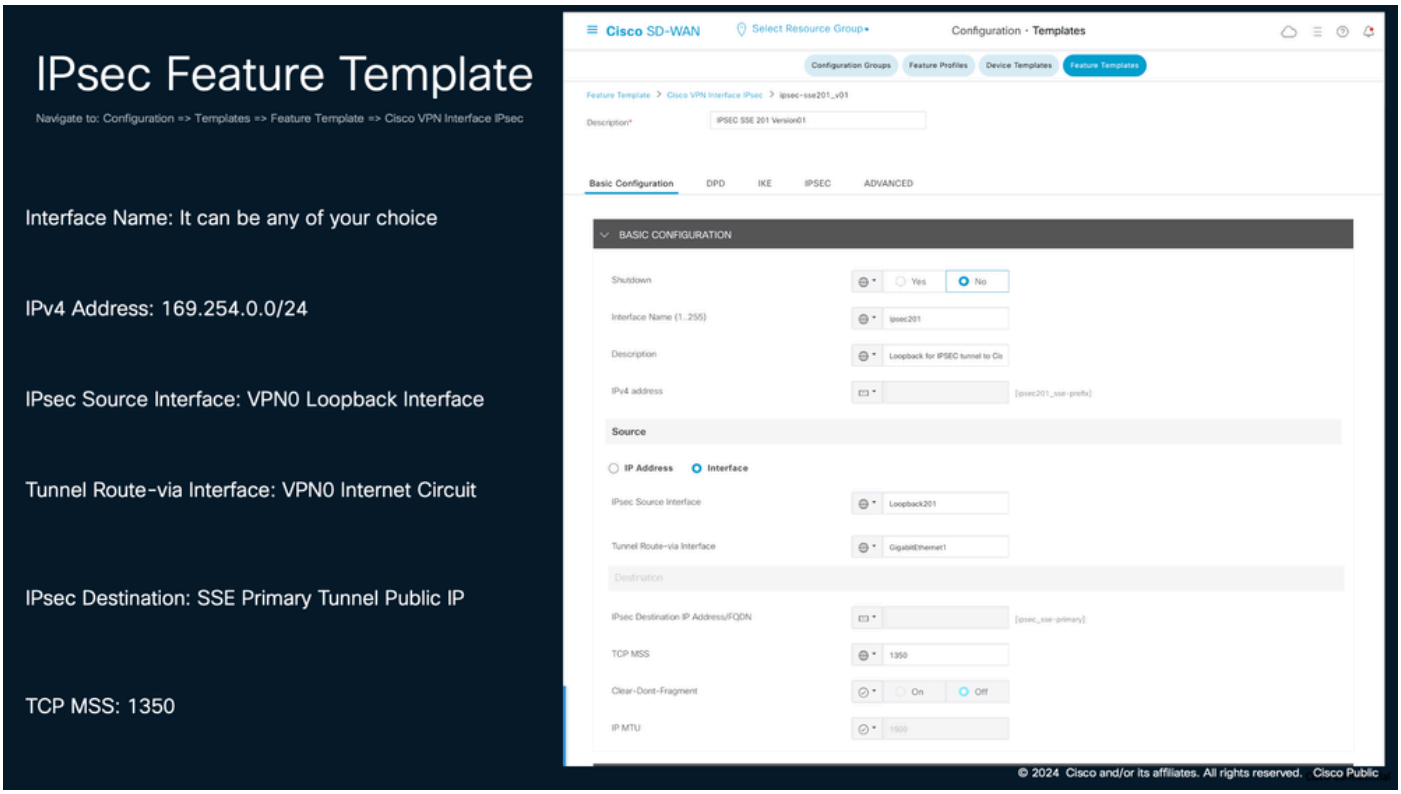
Anmerkung: Wiederholen Sie diesen Schritt für die erforderliche Anzahl an Tunneln für die Bereitstellung.

Bitte beachten Sie die offizielle Dokumentation zur Tunnelbegrenzung: https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

Diese Schritte beschreiben detailliert den Prozess für die Verbindung von DC1-HE1 (Rechenzentrum 1, Headend 1) mit dem primären SSE Virginia Hub. Mit dieser Konfiguration wird ein sicherer Tunnel zwischen dem SD-WAN-Router im Rechenzentrum und der Cisco Secure Access Network Tunnel Group (NTG) am Virginia Point of Presence (POP) eingerichtet.

Schritt 1: IPSec-Funktionsvorlage erstellen
Erstellen Sie eine IPSec-Funktionsvorlage, um die Parameter für den IPSec-Tunnel festzulegen, der den SD-WAN-Headend-Router mit dem NTG verbindet.

Abbildung 11: IPsec-Funktionsvorlage: Basiskonfiguration



IPsec-Funktionsvorlage: Basiskonfiguration

Schnittstellenname: Es kann eine beliebige Option sein
IPv4-Adresse: SSE hört auf 169.254.0.0/24 basierend auf der Anforderung, dass Sie das Subnetz nach Ihrer Wahl unterteilen können. Verwenden Sie als Best Practice /30. In diesem Leitfaden wird der erste Block für die zukünftige Verwendung nicht erwähnt.

IPsec-Quellschnittstelle: Definieren Sie eine VPN0-Loopback-Schnittstelle, die für die aktuelle IPsec-Schnittstelle eindeutig ist. Aus Gründen der Konsistenz und zur Fehlerbehebung wird empfohlen, die gleiche Nummerierung beizubehalten.
Tunnel-Route-via-Schnittstelle: Zeigen Sie auf die Schnittstelle, die als Underlay verwendet werden kann, um SSE zu erreichen (muss über einen Internetzugang verfügen).

IPsec-Ziel: Primäre Hub-IP-Adresse

Siehe Abbildung 7: Secure Access Network Tunnel Group US (Virginia), hier spricht man von 35.171.214.188

TCP-MSS: Hier spricht 1350 (Referenz: [https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters)](https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters)

Beispiel: DC1-HE1 zum primären Hub SSE Virginia

Schnittstellenname: IPSec201

Beschreibung: Loopback für IPSEC-Tunnel zu Cisco

IPv4-Adresse: 169.254.0.x/30

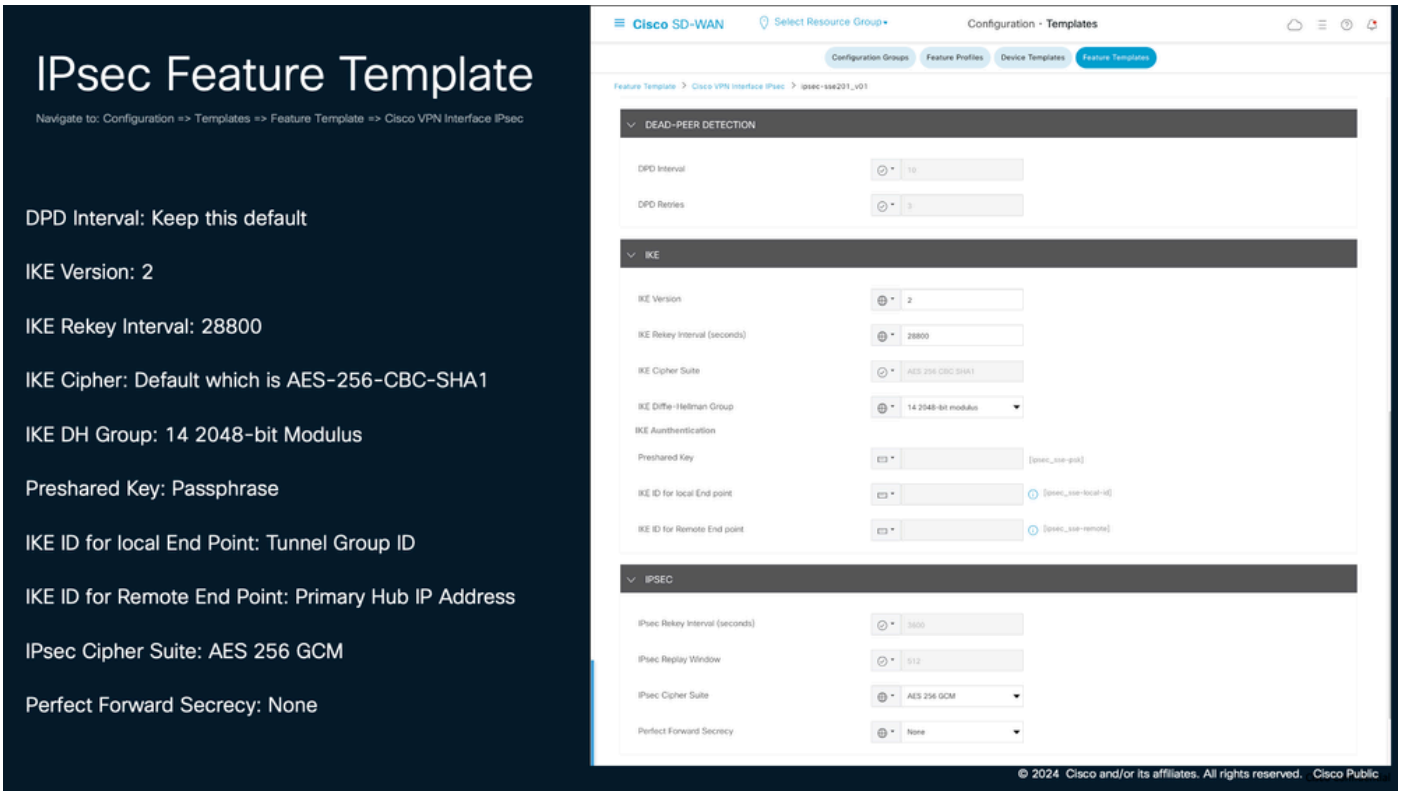
IPsec-Quellschnittstelle: Loopback201

Tunnel-Route-via-Schnittstelle: GigabitEthernet1

IPsec-Ziel-IP-Adresse/FQDN: 35.xxx.xxx.xxx

TCP-MSS: 1350

Abbildung 12: IPsec-Funktionsvorlage: IKE-IPSEC



IPsec-Funktionsvorlage: IKE-IPSEC

DPD-Intervall: Standard beibehalten
IKE-Version: 2
IKE-Neuschlüsselintervall: 28800
IKE-Verschlüsselung: Standardwert: AES-256-CBC-SHA1
IKE DH-Gruppe: 14-2048-Bit-Modul
Vorinstallierter Schlüssel: Passphrase
IKE-ID für lokalen Endpunkt: Tunnelgruppen-ID

Siehe Abbildung 7: Secure Access Network Tunnel Group US (Virginia). Dies ist mn03lab1+201@8167900-638880310-sse.cisco.com

---

Anmerkung: Jeder Tunnel muss einen eindeutigen Endpunkt für diesen Vorgang aufweisen. "+loopbackID" verwenden Beispiel: mn03lab1+202@8167900-638880310-sse.cisco.com, mn03lab1+203@8167900-638880310-sse.cisco.com usw.

IKE-ID für Remote-Endpunkt: Primäre Hub-IP-Adresse
IPsec-Cipher-Suite: AES 256 GCM

Perfekte Weiterleitung Geheimhaltung: None

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

Beispiel:

IKE-Version: 2
IKE-Neuschlüsselintervall: 28800
IKE-Verschlüsselung: AES-256-CBC-SHA1
IKE DH-Gruppe: 14-2048-Bit-Modul
Vorinstallierter Schlüssel: *****

Anmerkung: Schritt 6 unter Hinzufügen einer Netzwerk-Tunnelgruppe

---

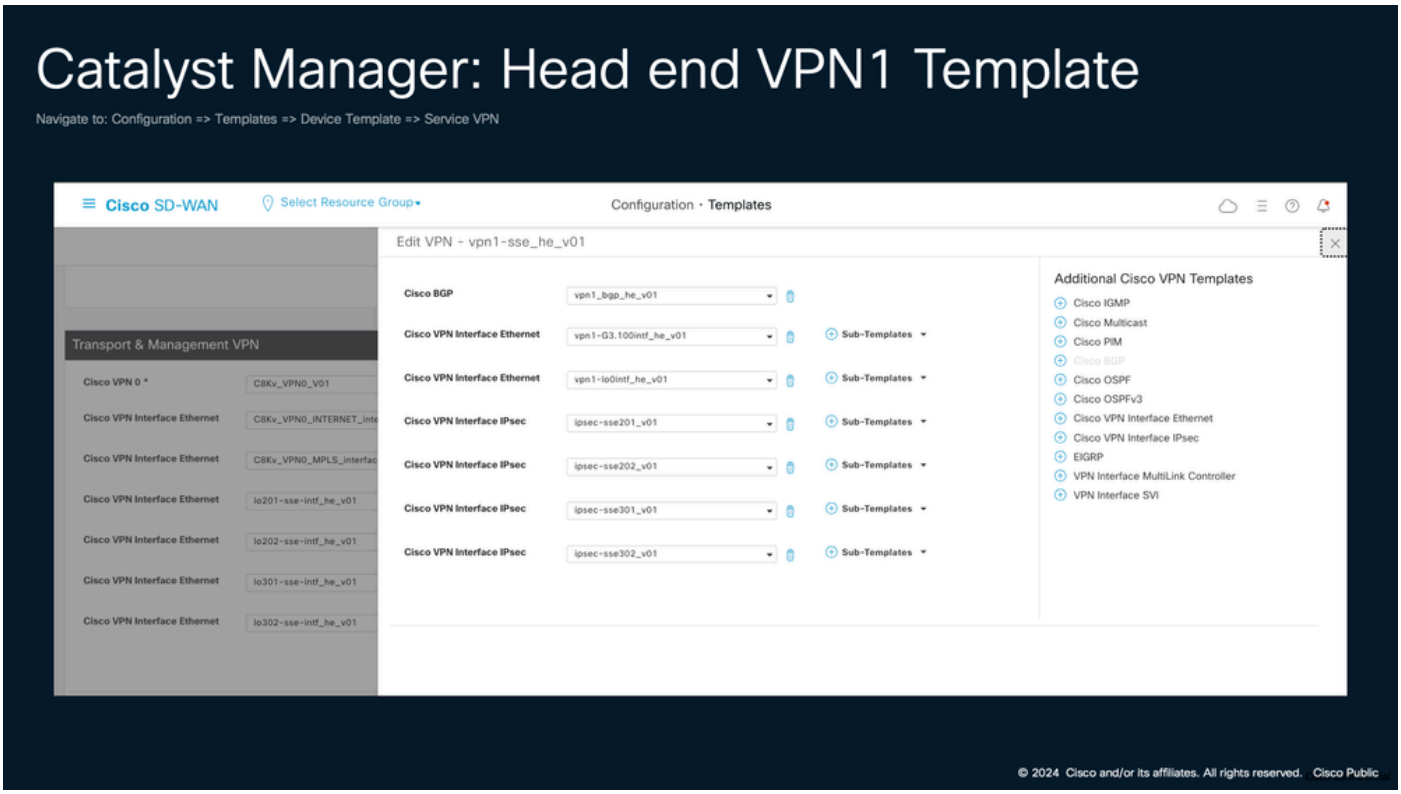
IKE-ID für lokalen Endpunkt: mn03lab1@8167900-638880310-sse.cisco.com
IKE-ID für Remote-Endpunkt: 35.171.xxx.xxx
IPsec-Cipher-Suite: AES 256 GCM
Perfekte Weiterleitung Geheimhaltung: None

Wiederholen Sie die Schritte zum Konfigurieren der erforderlichen Tunnel für den primären und sekundären sicheren Zugriffs-Hub.Für eine 2x2-Konfiguration würden Sie insgesamt vier Tunnel erstellen:

- Zwei Tunnel von DC1-HE1 zum primären sicheren Zugriffs-Hub
- Zwei Tunnel von DC1-HE1 zum sekundären Secure Access Hub

Nachdem die Vorlagen erstellt wurden, würden wir sie für das in Abbildung 13 gezeigte serviceseitige VRF und das in Abbildung 14 gezeigte, an das globale VRF angehängte Loopback verwenden.

Abbildung 13: Catalyst SD-WAN-Manager: Head-End-VPN1-Vorlage 2x2



Catalyst Manager: Head-End-VPN1-Vorlage

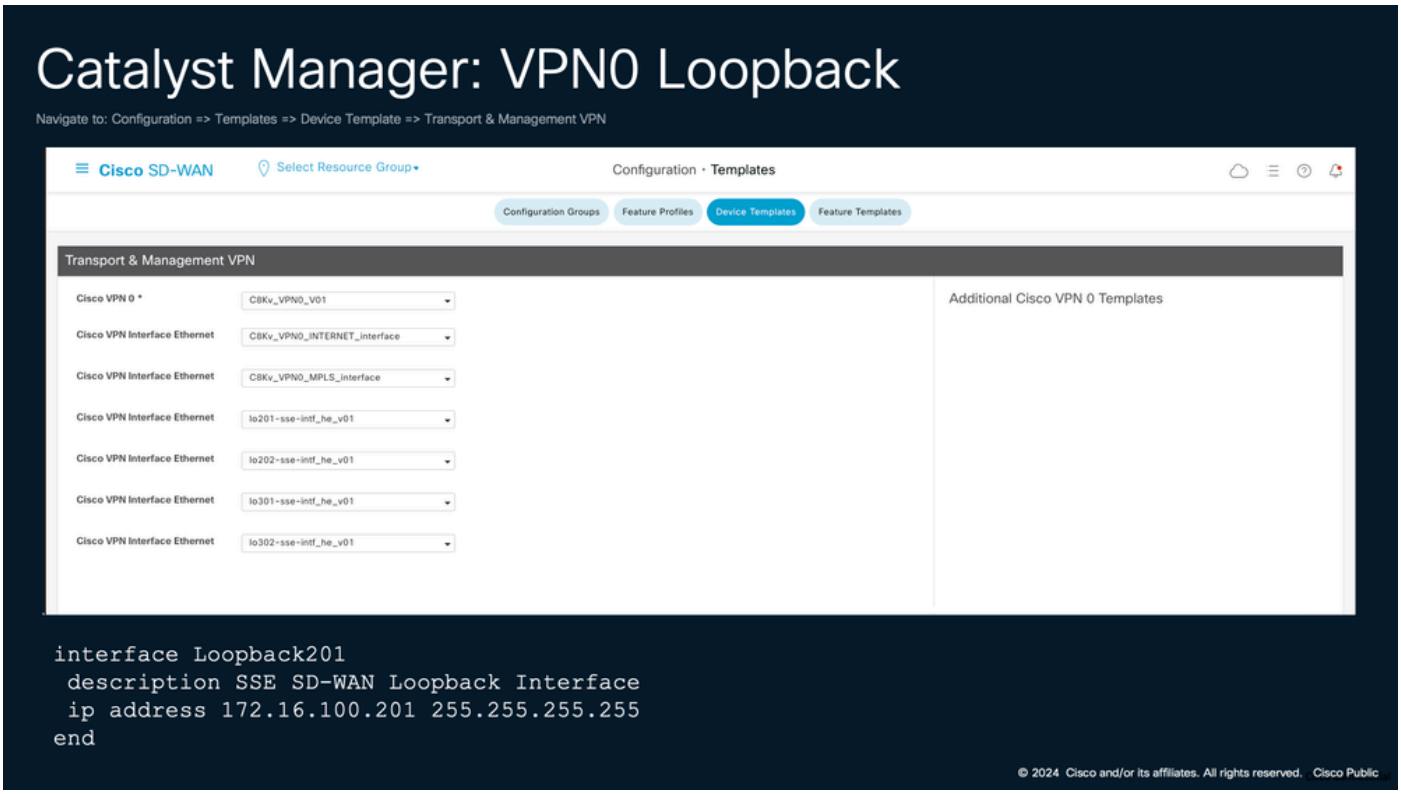
Phase 2: Definition von Loopback in Global VRF

Konfigurieren Sie eine Loopback-Schnittstelle in der globalen VRF-Tabelle (Virtual Routing and Forwarding). Dieser Loopback dient als Quellschnittstelle für den in Schritt 1 erstellten IPSec-Tunnel.

Alle Loopbacks, auf die in Schritt 1 Bezug genommen wird, müssen in Global VRF definiert werden.

Die IP-Adresse kann in einem beliebigen RFC1918-Bereich definiert werden.

Abbildung 14: Catalyst SD-WAN-Manager: VPN0-Loopback

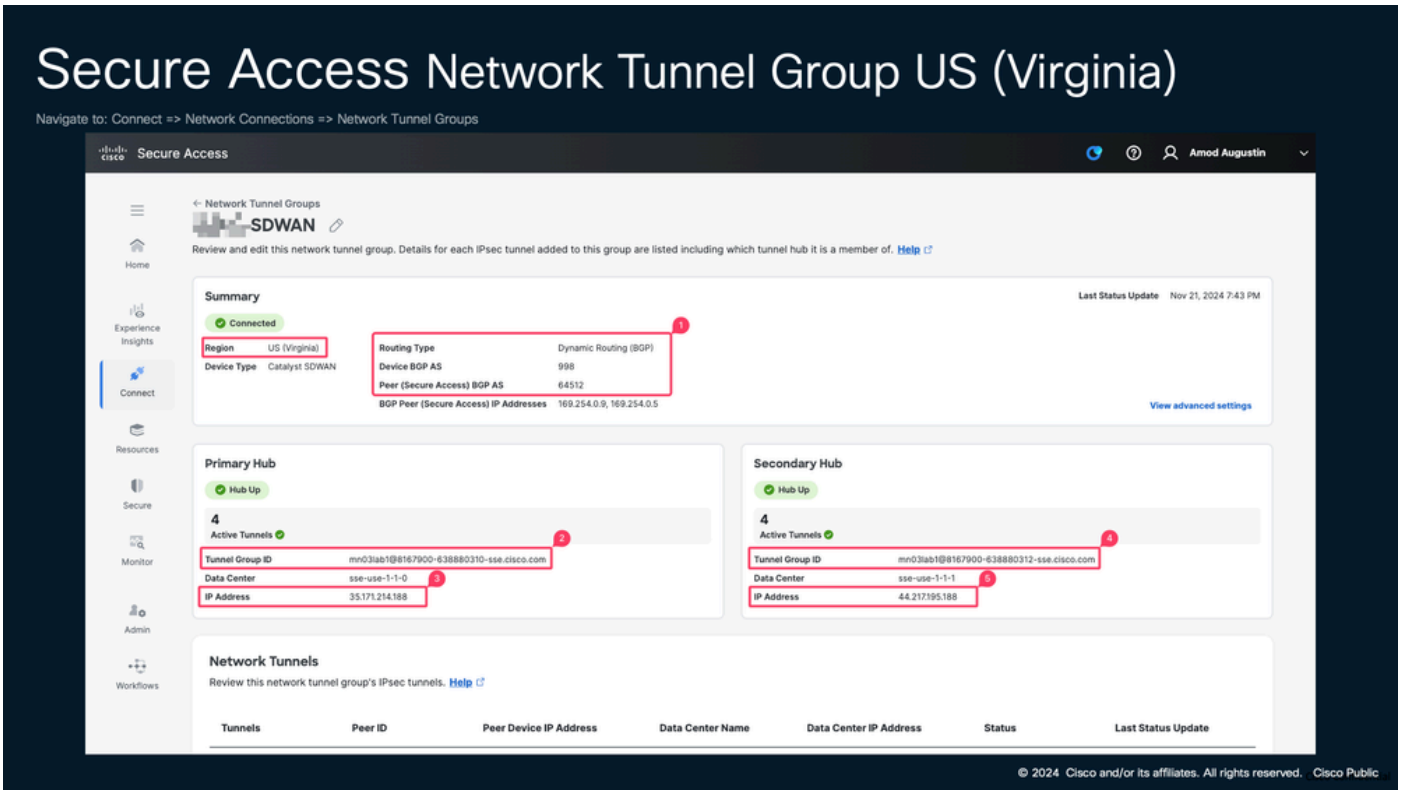


Catalyst Manager: VPN0-Loopback

Verfahren 3. Konfigurieren der BGP-Nachbarschaft

Die BGP-Funktionsvorlage definiert die BGP-Nachbarschaft für alle Tunnelschnittstellen. Informationen zur Konfiguration der BGP-Werte finden Sie in der BGP-Konfiguration der Netzwerk-Tunnelgruppen im Cisco Secure Access-Portal.

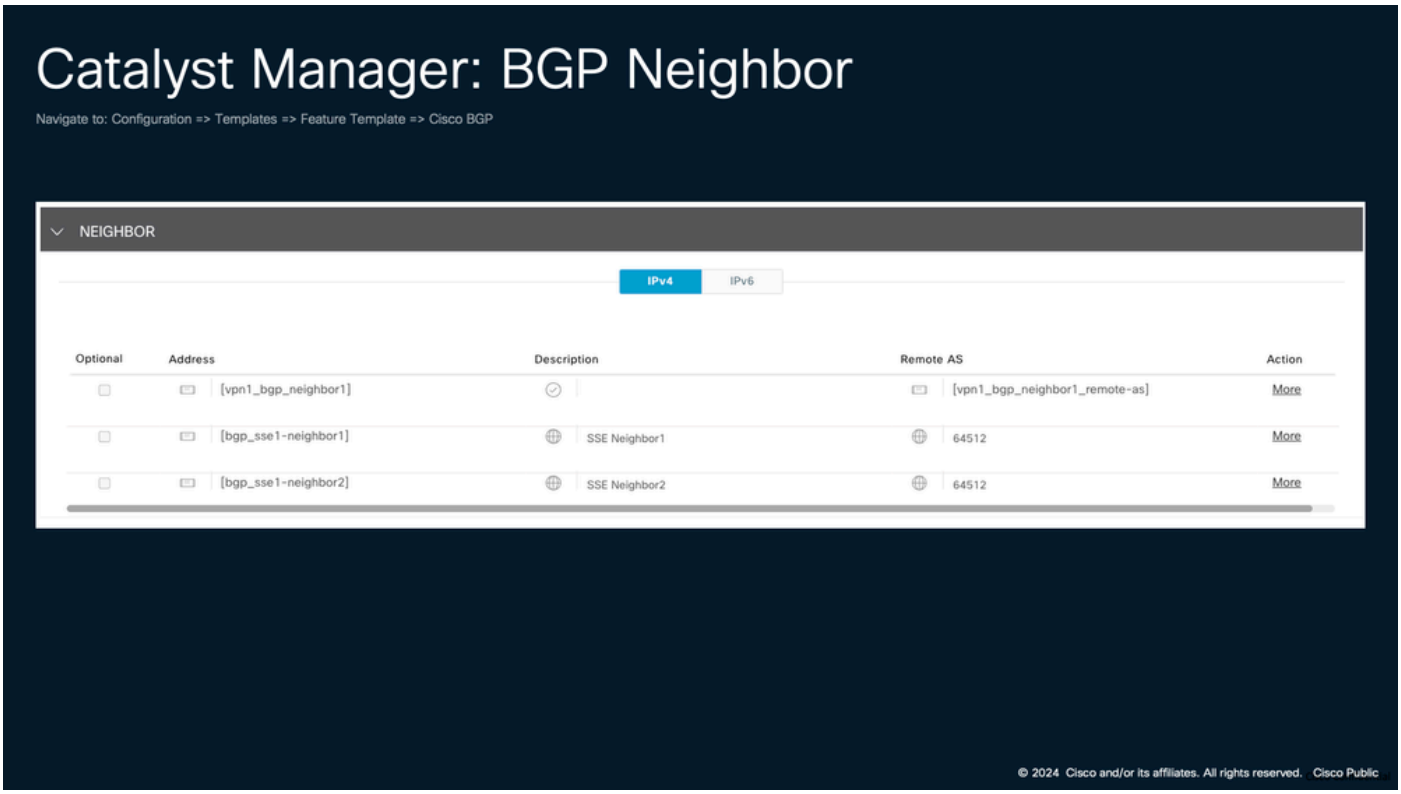
Abbildung 15: Secure Access Network Tunnel Group USA (Virginia)



Secure Access Network Tunnel Group USA (Virginia)

In diesem Beispiel verwenden wir die Informationen aus Abbildung 15 (Feld 1), um BGP mithilfe einer Funktionsvorlage zu definieren.

Abbildung 16: Catalyst SD-WAN Manager BGP Neighbor



Catalyst SD-WAN Manager BGP Neighbor

Mithilfe der Funktionsvorlage generierte Konfiguration:

```
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#
```

Verifizierung

```
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
```

Referenz

Eine Active/Active-Implementierung hätte einen Multipath vom Core-Switch, der mit beiden SD-WAN-Headends verbunden ist.

Abbildung 17: Aktiv/Aktiv-Szenario für BGP-Nachbarn

```
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>
```

Aktiver/aktiver BGP-Nachbar

Eine Active/Stanby-Implementierung hätte einen aktiven Pfad vom Core-Switch zu SD-WAN-Headends, da eine ASPL-Präferenz vorliegt (bei der eine Route Map zum Nachbarn verwendet wird).

Abbildung 18: Aktiv/Standby-Szenario für BGP-Nachbar

```
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>
```

Aktiver/Standby-BGP-Nachbar

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.