Configurare l'interconnessione dell'app privata tra Security Service Edge e SD-WAN con il metodo manuale

Sommario

Introduzione

Questo documento descrive una guida completa per la connessione di Cisco Secure Access con router SD-WAN, focalizzata sull'accesso sicuro alle app private.

Informazioni sulla Guida

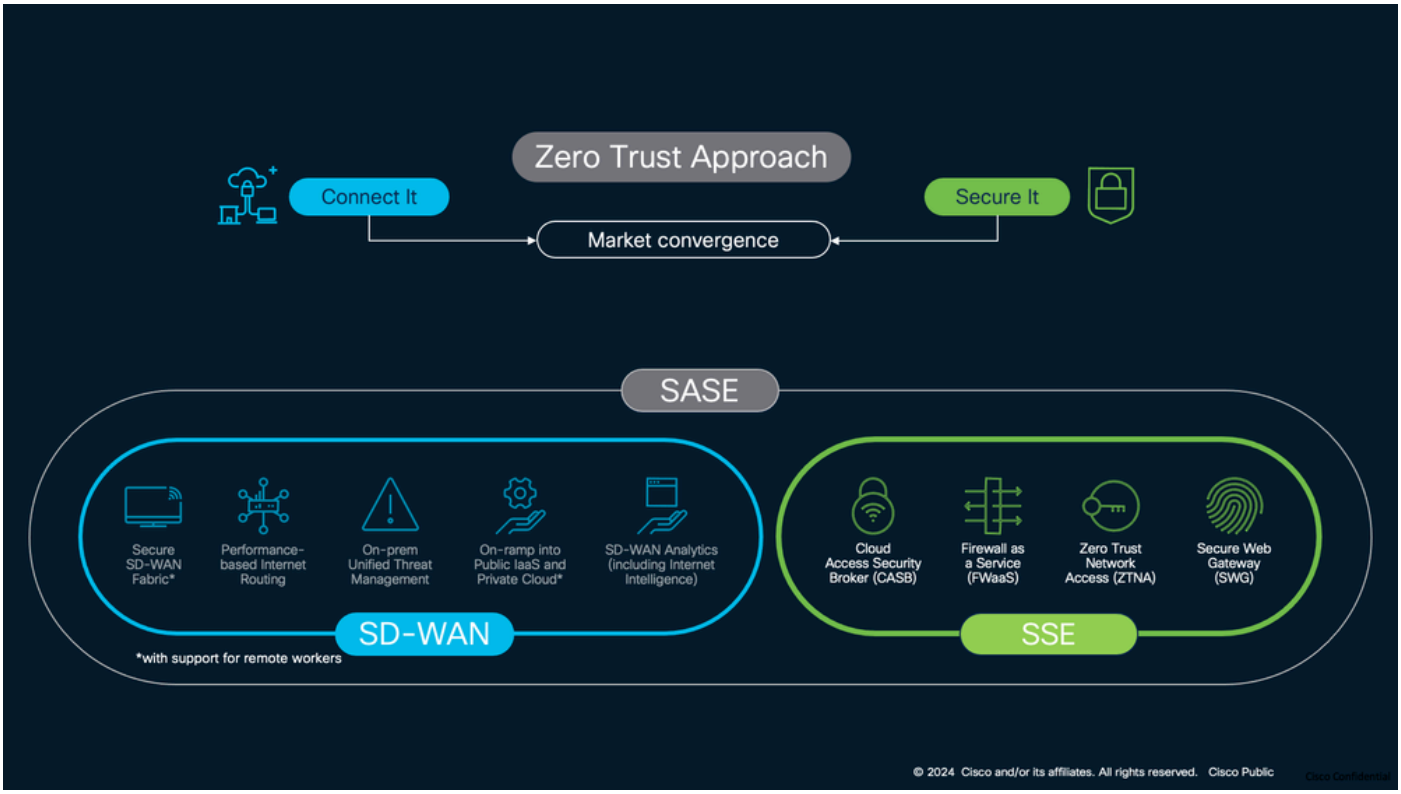
Nota: le configurazioni elencate di seguito sono sviluppate per le versioni UX1.0 e 17.9/20.9 di SD-WAN.

In questa guida viene fornita una procedura dettagliata strutturata dei seguenti passaggi chiave:

- Definizione dei gruppi di tunnel di rete (NTG)
- Configurazione tunnel IPSec: Istruzioni dettagliate sulla configurazione di tunnel IPSec sicuri tra i router Cisco SD-WAN e i Cisco Secure Access NTG.
- Villaggio BGP: Procedure dettagliate per l'esecuzione di BGP neighbors sui tunnel IPSec per garantire il routing dinamico e una migliore resilienza della rete.
- Accesso applicazione privata: Linee guida per la configurazione e la protezione dell'accesso

alle applicazioni private tramite i tunnel stabiliti.

Figura 1: Cisco SD-WAN e approccio SSE Zero Trust



SSE con SD-WAN

Questa guida è incentrata sulla valutazione della progettazione e sulle best practice di installazione per l'interconnessione NTG. In questa guida, i controller SD-WAN sono installati nel cloud e i router WAN Edge sono installati nel centro dati e sono connessi ad almeno un circuito Internet.

Presupposti principali

- SSE (Secure Access Secure Service Edge) Cisco: Si presume che Cisco Secure Access SSE sia già stato predisposto per l'organizzazione.
- Cisco SD-WAN WAN Edge Router: Si presume che il router perimetrale WAN sia integrato nella rete di sovrapposizione, facilitando in modo efficiente il traffico degli utenti attraverso l'infrastruttura SD-WAN.
- Anche se questa guida si concentra principalmente sugli aspetti SD-WAN della progettazione e della configurazione, fornisce un approccio olistico per l'integrazione delle soluzioni Cisco Secure Access nell'architettura di rete esistente.

Informazioni su questa soluzione

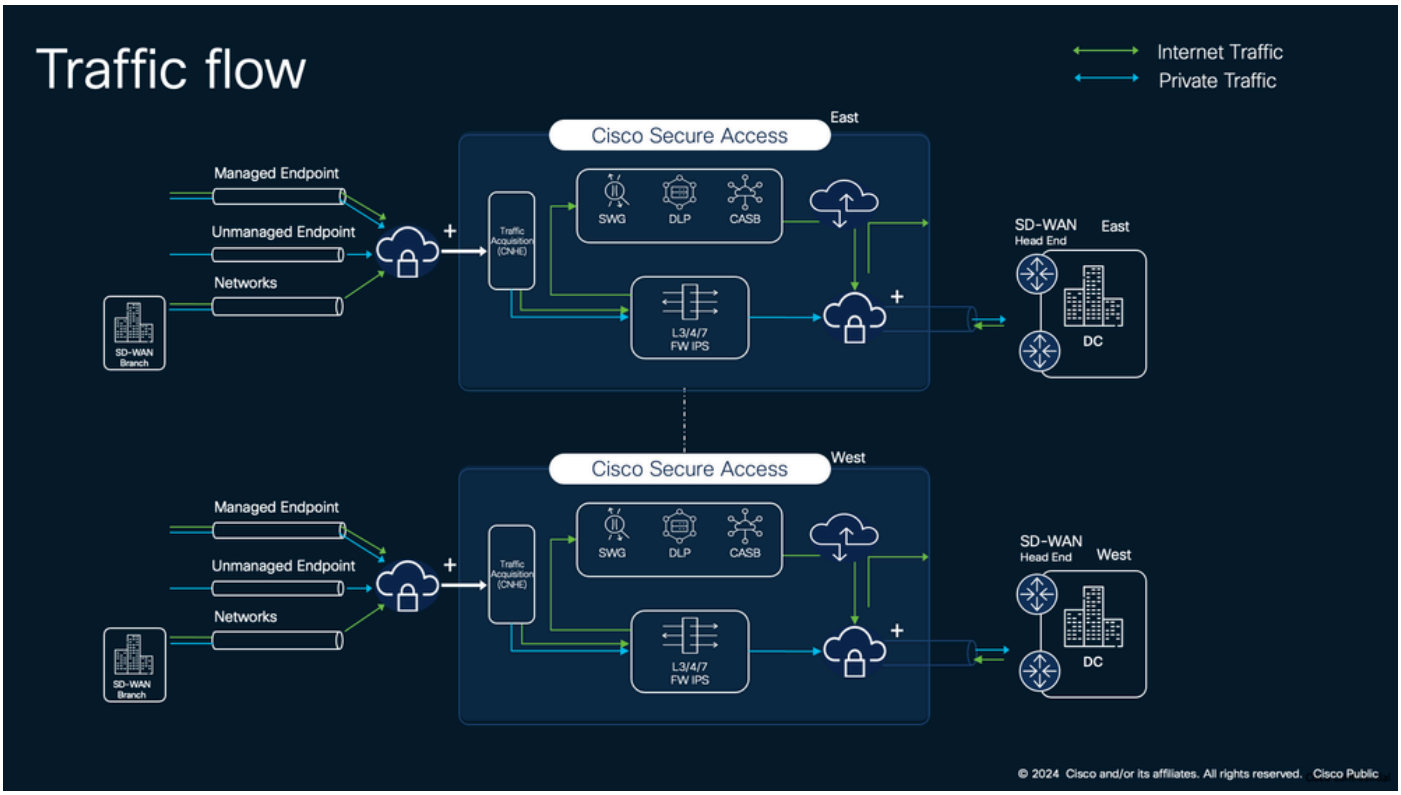
I tunnel delle app private, offerti da Cisco Secure Access, forniscono connettività protetta alle applicazioni private per gli utenti che si connettono tramite Zero Trust Network Access (ZTNA) e VPN as a Service (VPNaaS). Questi tunnel consentono alle organizzazioni di collegare in modo sicuro gli utenti remoti alle risorse private ospitate nei centri dati o nei cloud privati.

Utilizzando IKEv2 (Internet Key Exchange versione 2), questi gruppi di tunnel stabiliscono connessioni bidirezionali sicure tra Cisco Secure Access e i router SD-WAN. Supportano l'elevata disponibilità attraverso più tunnel all'interno dello stesso gruppo e offrono una gestione flessibile del traffico tramite routing statico e dinamico (BGP).
I tunnel IPsec possono trasportare traffico da diverse origini, tra cui:

- Utenti VPN ad accesso remoto
- Connessioni ZTNA basate su browser o client
- Altri percorsi di rete connessi a Cisco Secure Access

Questo approccio consente alle organizzazioni di indirizzare in modo sicuro tutti i tipi di traffico delle applicazioni private attraverso un canale unificato e crittografato, migliorando sia la sicurezza che l'efficienza operativa.
Cisco Secure Access, come parte della soluzione SSE (Security Service Edge) di Cisco, semplifica le operazioni IT tramite un'unica console gestita dal cloud, un client unificato, la creazione centralizzata di policy e il reporting aggregato. Incorpora più moduli di sicurezza in un'unica soluzione fornita tramite cloud, tra cui ZTNA, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS), sicurezza DNS, Remote Browser Isolation (RBI) e molto altro ancora. Questo approccio completo riduce i rischi per la sicurezza applicando principi di attendibilità zero e applicando policy di sicurezza granulari

Figura 2: Flusso di traffico tra Cisco Secure Access e l'app privata



Flusso traffico app privato SSE

La soluzione descritta in questa guida fa riferimento a considerazioni complete sulla ridondanza, incluse sia il router SD-WAN nel centro dati che il Network Tunnel Group (NTG) sul lato SSE (Security Service Edge). Questa guida si concentra su un modello di installazione hub SD-WAN

attivo/attivo, che contribuisce a mantenere un flusso di traffico ininterrotto e garantisce un'elevata disponibilità.

Prerequisiti

Requisiti

È consigliabile conoscere i seguenti argomenti:

- Configurazione e gestione di Cisco SD-WAN
- Conoscenze base dei protocolli IKEv2 e IPSec
- Configurazione di Network Tunnel Group nel portale Cisco Secure Access
- Conoscenza di BGP ed ECMP

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Controller Cisco SD-WAN su 20.9.5a
- Router Cisco SD-WAN Wan Edge su 17.9.5a
- Cisco Secure Access Portal

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Progettazione

Questa guida descrive la soluzione usando un modello di progettazione attiva/attiva per router headend SD-WAN. Un modello di progettazione attiva/attiva nel contesto di router headend SD-WAN presuppone due router in un centro dati, entrambi collegati al Security Service Edge (SSE) Network Tunnel Group (NTG), come illustrato nella Figura 3. In questo scenario, entrambi i router SD-WAN nel centro dati (DC1-HE1 e DC1-HE2) gestiscono attivamente il flusso del traffico. A tale scopo, viene inviato lo stesso valore ASPL (AS Path Length) al controller di dominio adiacente interno. Di conseguenza, il traffico proveniente dall'interno del bilanciamento del carico CC tra i due headend.

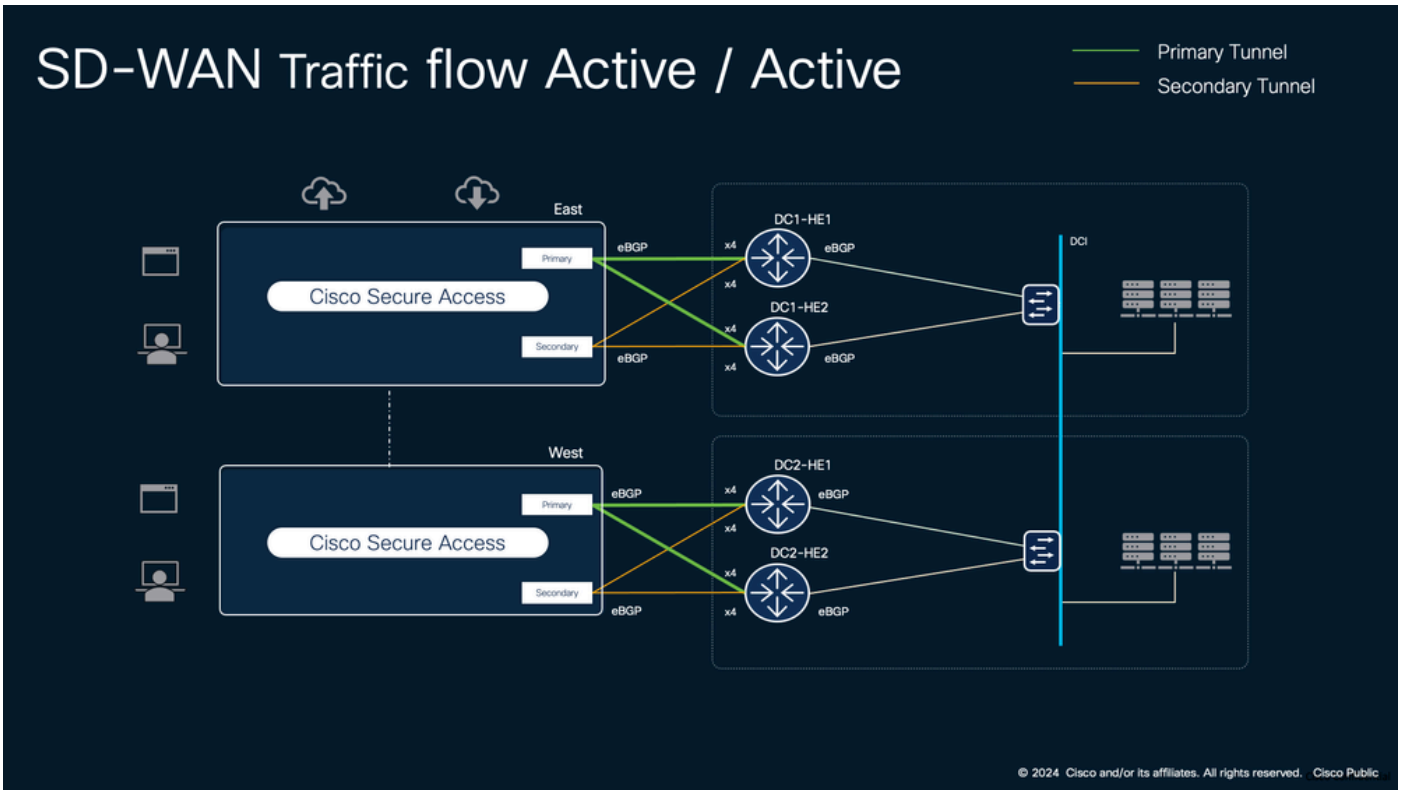
Ogni router headend può stabilire più tunnel per i punti di presenza (POP) SSE. Il numero di tunnel varia in base ai requisiti e al modello di dispositivo SD-WAN. In questo progetto:

- Ogni router dispone di 4 tunnel per raggiungere l'hub SSE primario e di 4 tunnel per raggiungere l'hub SSE secondario.
- Il numero massimo di tunnel supportati da ogni hub SSE può variare. Per le informazioni più

aggiornate, consultare la documentazione ufficiale: https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

Questi router headend formano i quartieri BGP sui tunnel verso l'SSE. Tramite questi quartieri, gli headend pubblicizzano i prefissi delle applicazioni private ai loro vicini SSE, consentendo un routing sicuro ed efficiente del traffico alle risorse private.

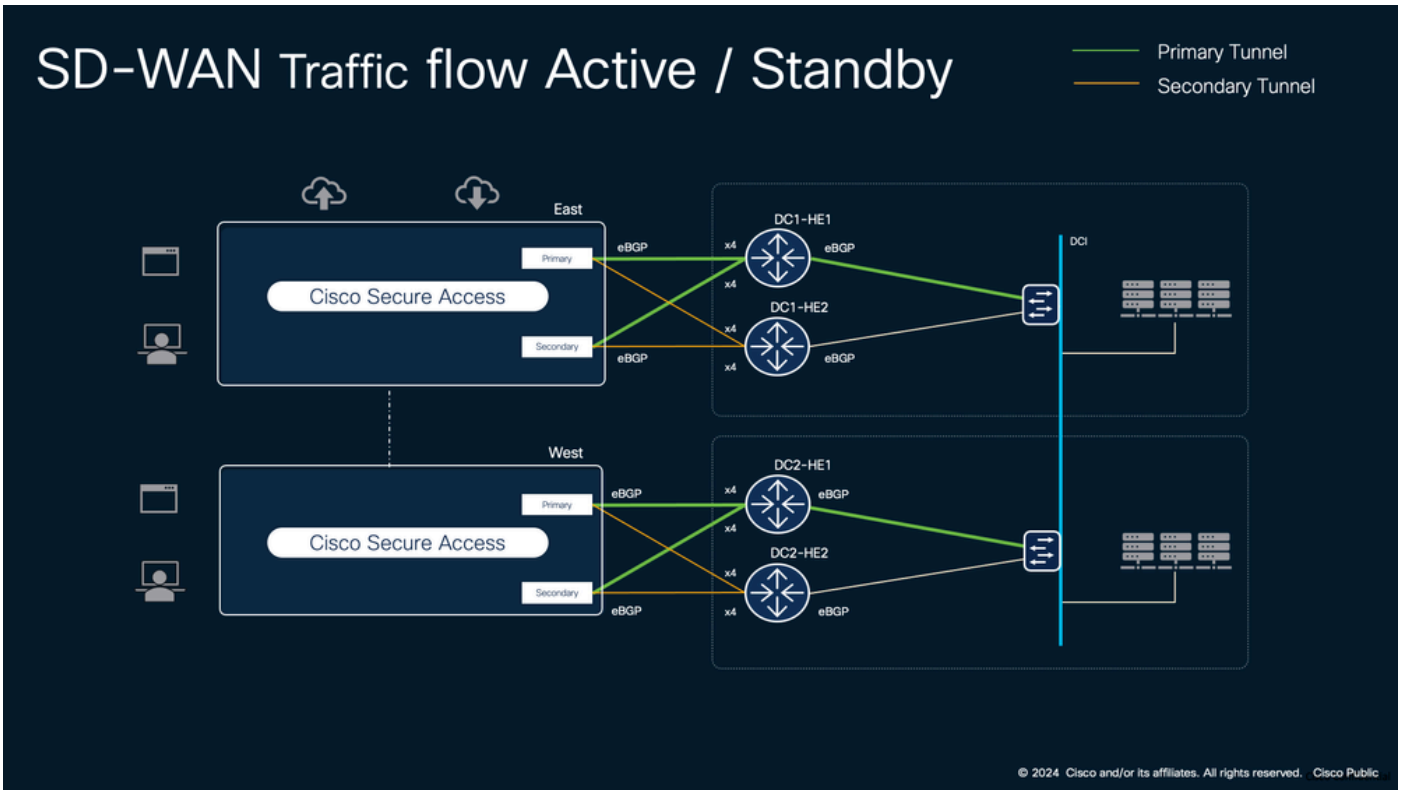
Figura 3: Modello di implementazione da SD-WAN a SSE attivo/attivo



Modello di implementazione da SD-WAN a SSE attivo/attivo

Un design attivo/standby designa un router (DC1-HE1) come sempre attivo, mentre il router secondario (DC1-HE2) rimane in standby. Il traffico attraversa in modo costante l'headend attivo (DC1-HE1) a meno che non si guasti completamente. Questo modello di distribuzione presenta uno svantaggio: se il tunnel primario per SSE si interrompe, il traffico passa ai tunnel SSE secondari che si trovano solo tramite DC1-HE2, causando la reimpostazione di qualsiasi traffico con stato.
Nel modello Active/Standby, la lunghezza del percorso BGP AS viene utilizzata per indirizzare il traffico sia all'interno del controller di dominio sia verso l'SSE. DC1-HE1 invia aggiornamenti dei prefissi al router adiacente SSE BGP con un ASPL di 2, mentre DC1-HE2 invia aggiornamenti con un ASPL di 3. Il router adiacente interno DC1-HE1 annuncia prefissi con una lunghezza del percorso AS inferiore a DC1-HE2, garantendo la preferenza per il traffico per DC1-HE1. (I clienti possono scegliere altri attributi o protocolli per influenzare la preferenza per il traffico.)
I clienti possono selezionare un modello di installazione Attivo/Attivo o Attivo/Standby in base ai propri requisiti specifici.

Figura 4: Modello di installazione da SD-WAN a SSE attivo/standby



Modello di installazione da SD-WAN a SSE attivo/standby

Configurazione

In questa sezione viene descritta la procedura:

1. Verificare i prerequisiti per il provisioning di un gruppo di tunnel di rete nel portale Cisco Secure Access.
2. Configurare l'interconnessione SD-WAN con Cisco Secure Access Network Tunnel Group (NTG) utilizzando il metodo manuale IPsec.
3. Configurare il vicinato BGP

Nota: Questa configurazione è basata su un modello di distribuzione attivo/attivo

---

Procedura 1. Verifica della configurazione del gruppo di tunnel di rete sul portale Cisco Secure Access

La modalità di configurazione di Network Tunnel Group non è trattata nella Guida. Rivedere questa referenza.

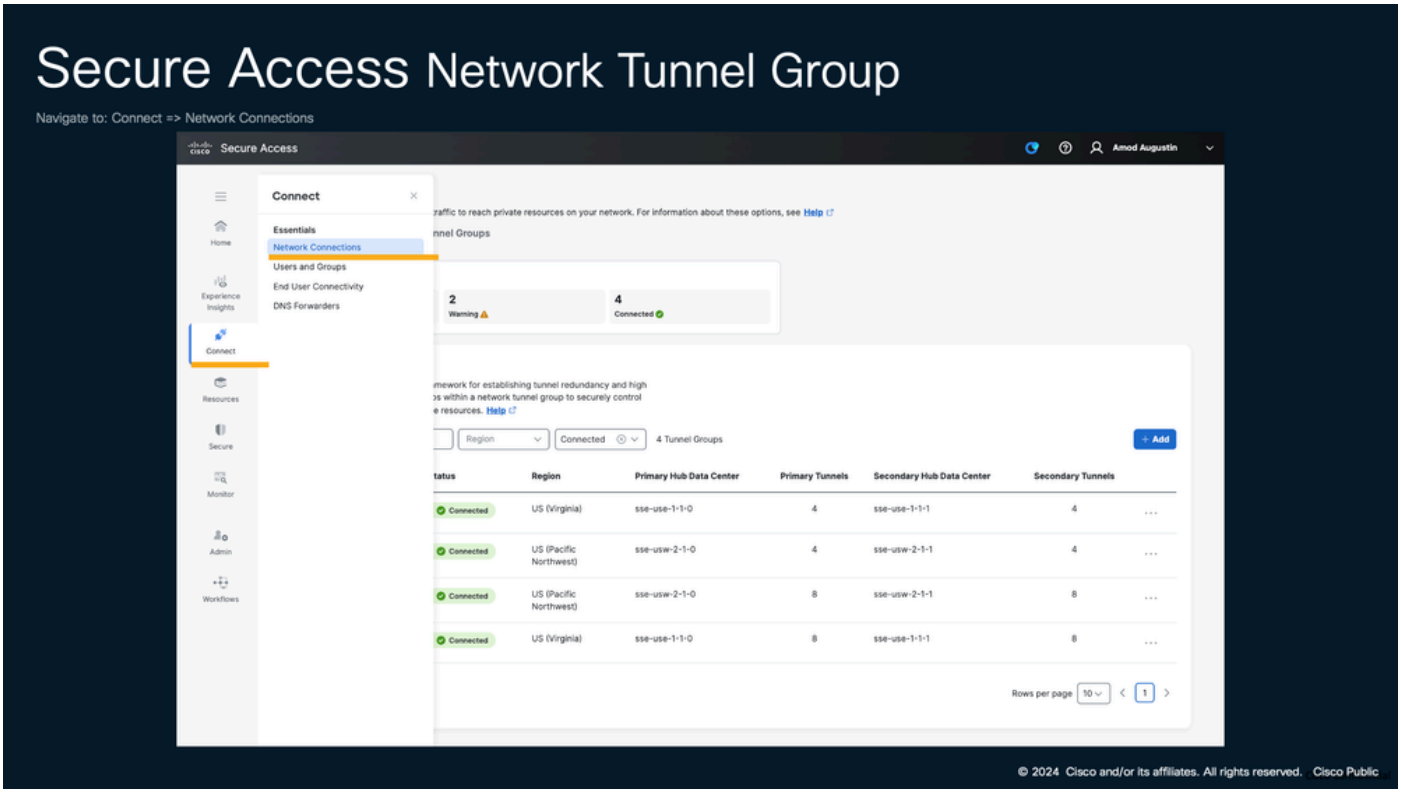
- Aggiungere un gruppo di tunnel di rete: Documentazione SSE
- Configurazione del tunnel di rete tra Cisco Secure Access e il router Cisco IOS XE con ECMP con BGP

Passare a Cisco Secure Access e verificare che sia stato eseguito il provisioning dei gruppi di tunnel di rete (NTG). Per il progetto corrente, è necessario effettuare il provisioning degli NTG in

due diversi punti di presenza (POP). In questa guida, utilizziamo i NTG negli USA POP (Virginia) e POP (Pacifico nordoccidentale).

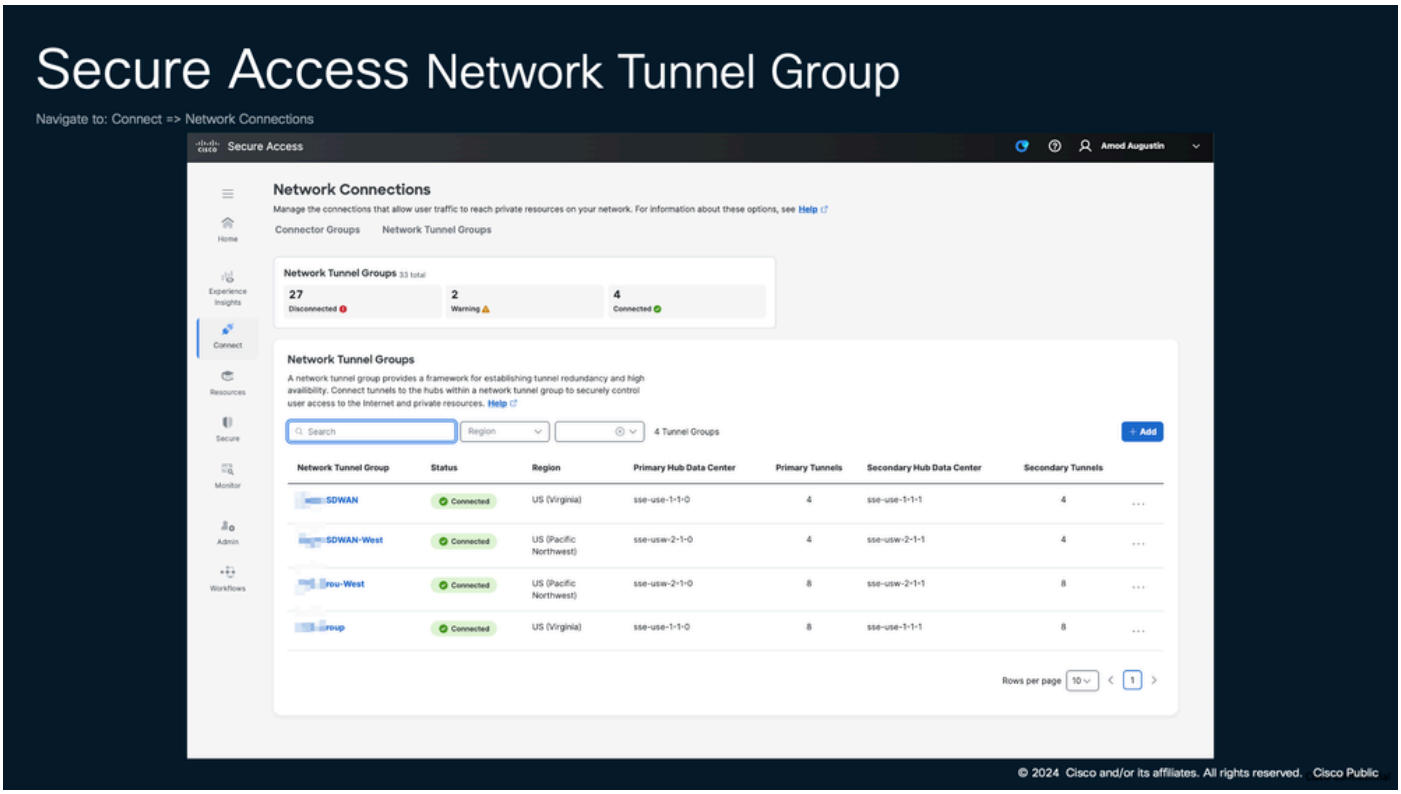
Nota: i nomi e le posizioni dei POP possono variare, ma il concetto chiave è quello di avere più NTG attivati in posizioni geograficamente vicine al centro dati. Questo approccio consente di ottimizzare le prestazioni della rete e fornisce ridondanza.

Figura 5: Cisco Secure Access Network Tunnel Group



Cisco Secure Access Network Tunnel Group

Figura 6: Elenco gruppi tunnel di rete Cisco Secure Access



Elenco dei gruppi di tunnel di rete ad accesso sicuro

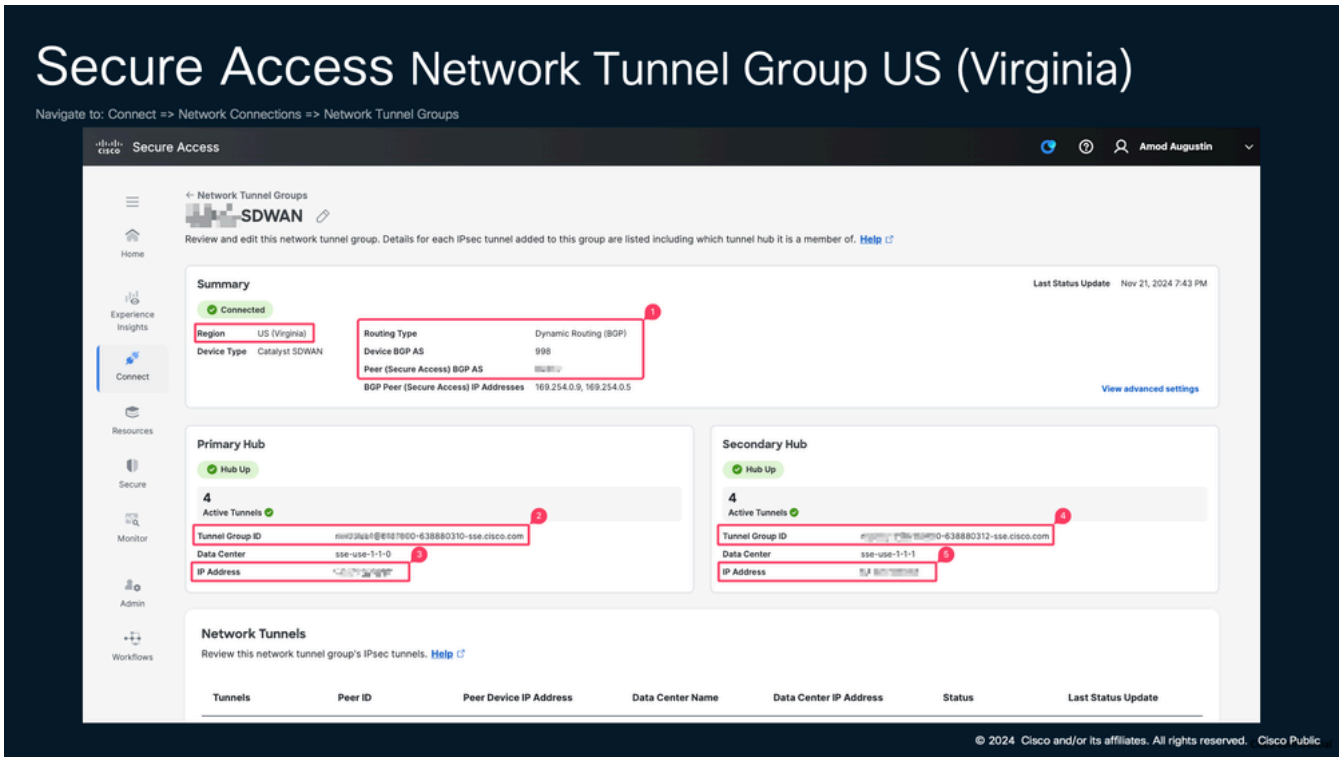
Accertarsi di aver annotato la passphrase del tunnel (visualizzata una sola volta durante la creazione del tunnel).

✎ Nota: Passaggio 6 in Aggiunta di un gruppo di tunnel di rete

---

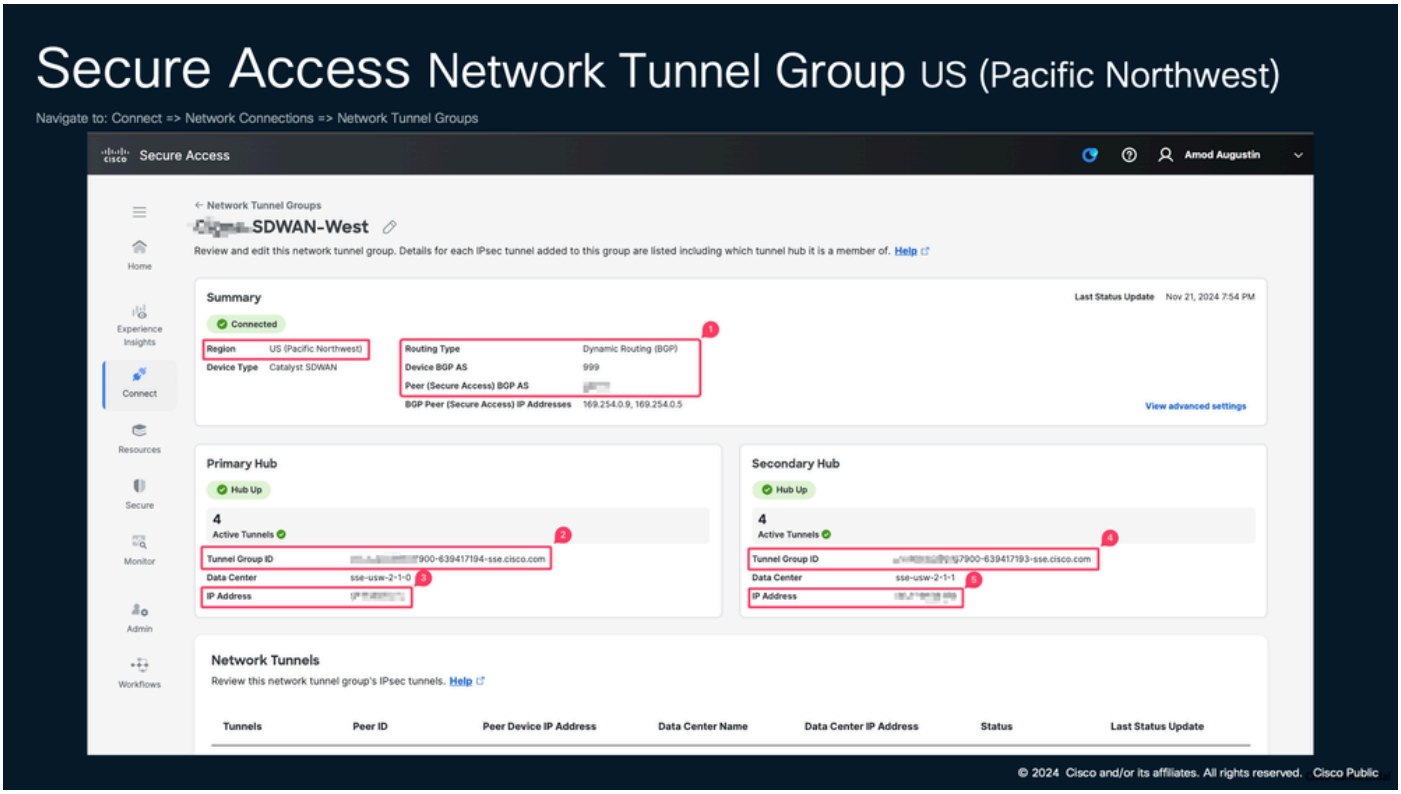
Prendere inoltre nota degli attributi di Tunnel Group utilizzati durante la configurazione IPSec. Lo screenshot (Figura 6) viene preso da un ambiente lab per uno scenario di produzione che crea gruppi NTG in base alle raccomandazioni di progettazione o utilizzo.

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



Secure Access Network Tunnel Group US (Virginia)

Figura 8: Secure Access Network Tunnel Group US (Pacifico nordoccidentale)



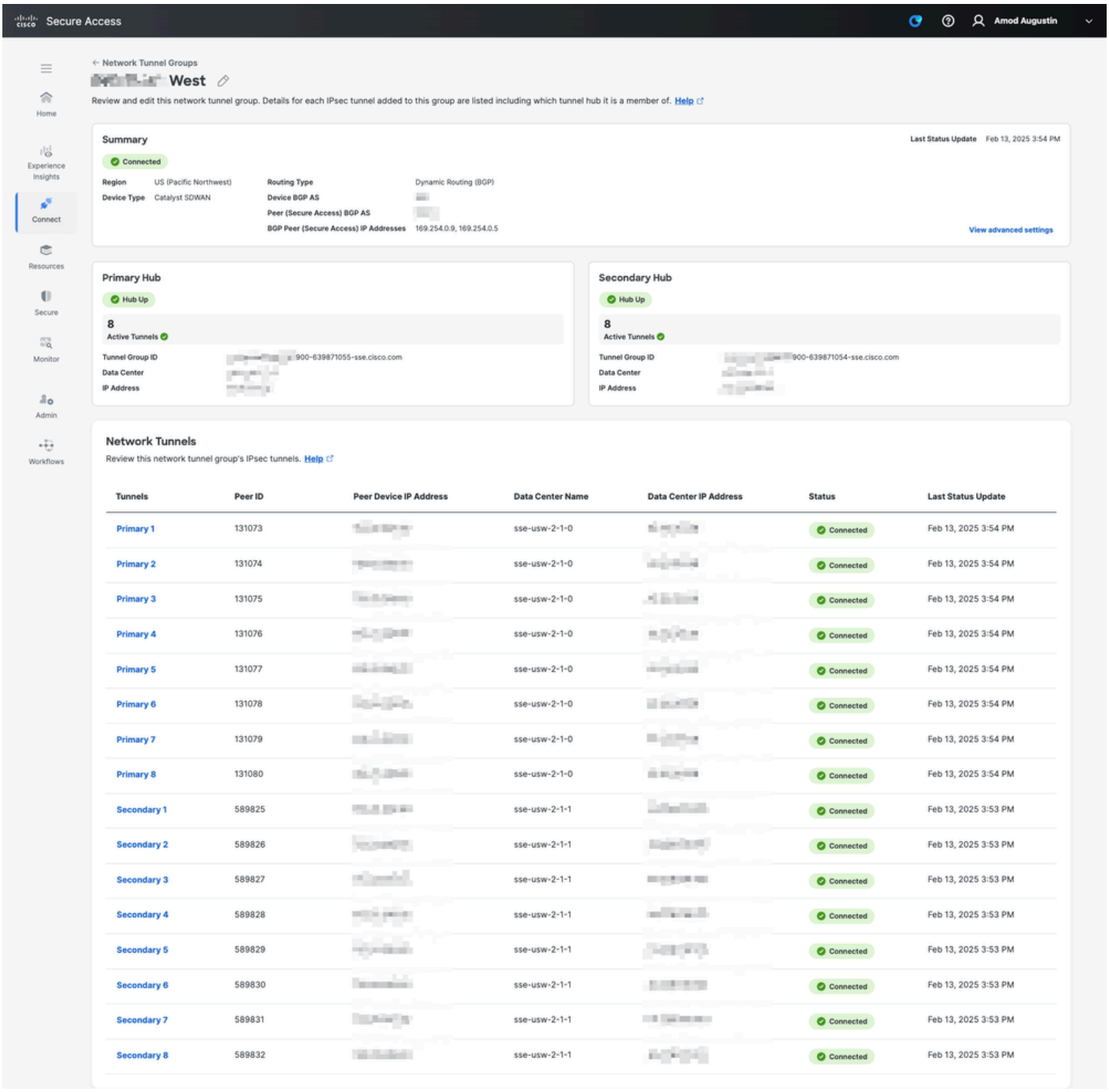
Secure Access Network Tunnel Group US (Pacifico nordoccidentale)

Nella figura 8 sono illustrati solo 4 tunnel su hub primari e secondari. Tuttavia, è stato verificato un massimo di 8 tunnel in un ambiente controller. Il supporto massimo per il tunnel può variare a seconda del dispositivo hardware in uso e del supporto corrente per il tunnel SSE. Per le informazioni più aggiornate, consultare la documentazione ufficiale:

https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels e la nota sulla versione del rispettivo dispositivo hardware.

Di seguito è riportato un esempio di configurazione a 8 tunnel.

Figura 8a: Tunnel NTG fino a 8 tunnel



SSE NTG fino a 8 tunnel

Procedura 2. Configurare l'interconnessione SD-WAN con Cisco Secure Access Network Tunnel Group (NTG) utilizzando il metodo manuale IPsec.

In questa procedura viene mostrato come connettere un Network Tunnel Group (NTG) utilizzando i modelli di funzionalità di Cisco Catalyst SD-WAN Manager 20.9 e Cisco Catalyst Edge Router

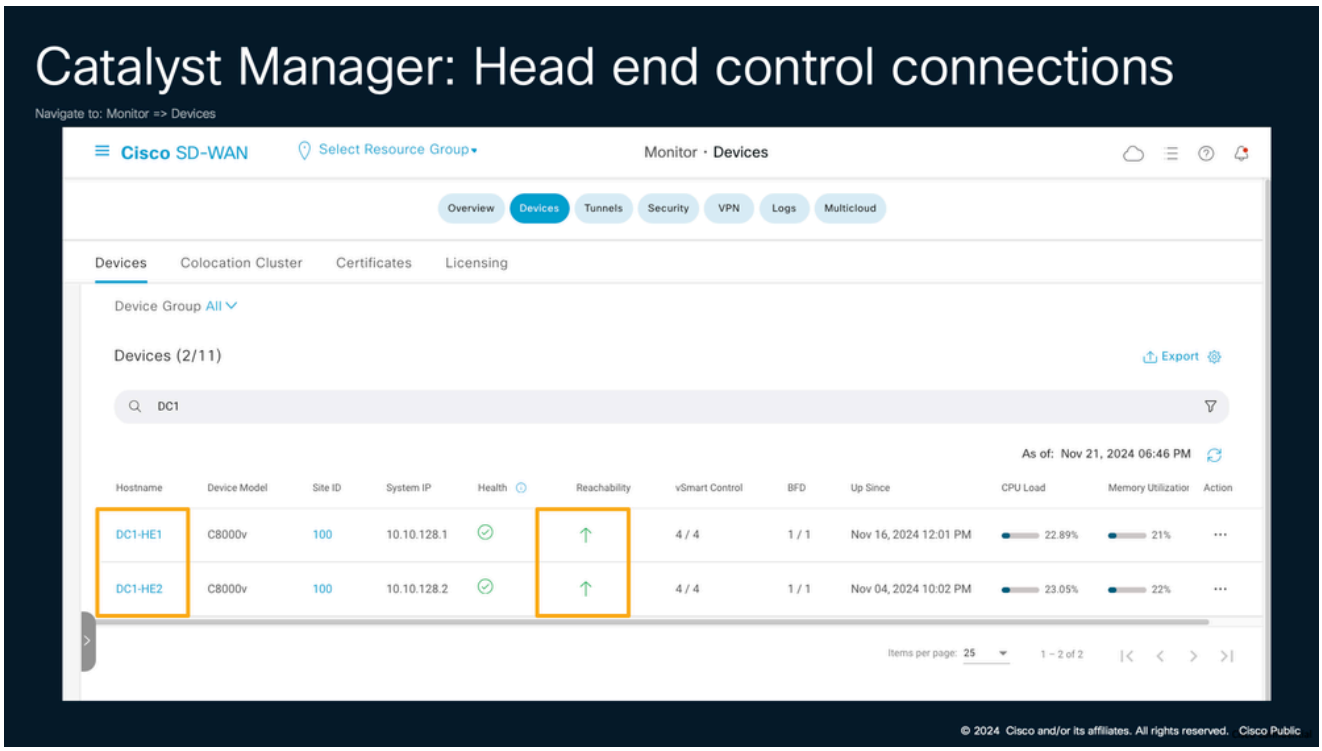
con versione 17.9.

Nota:in questa guida si presume un'implementazione di overlay SD-WAN esistente con una topologia hub e spoke o completamente mesh, in cui gli hub fungono da punti di accesso per le applicazioni private ospitate nel centro dati. Questa procedura può essere applicata anche alle distribuzioni di filiali o cloud.

Prima di procedere, verificare che i prerequisiti siano soddisfatti:

1. Le connessioni di controllo sono attive sul dispositivo per consentire gli aggiornamenti necessari da Cisco Catalyst SD-WAN Manager.

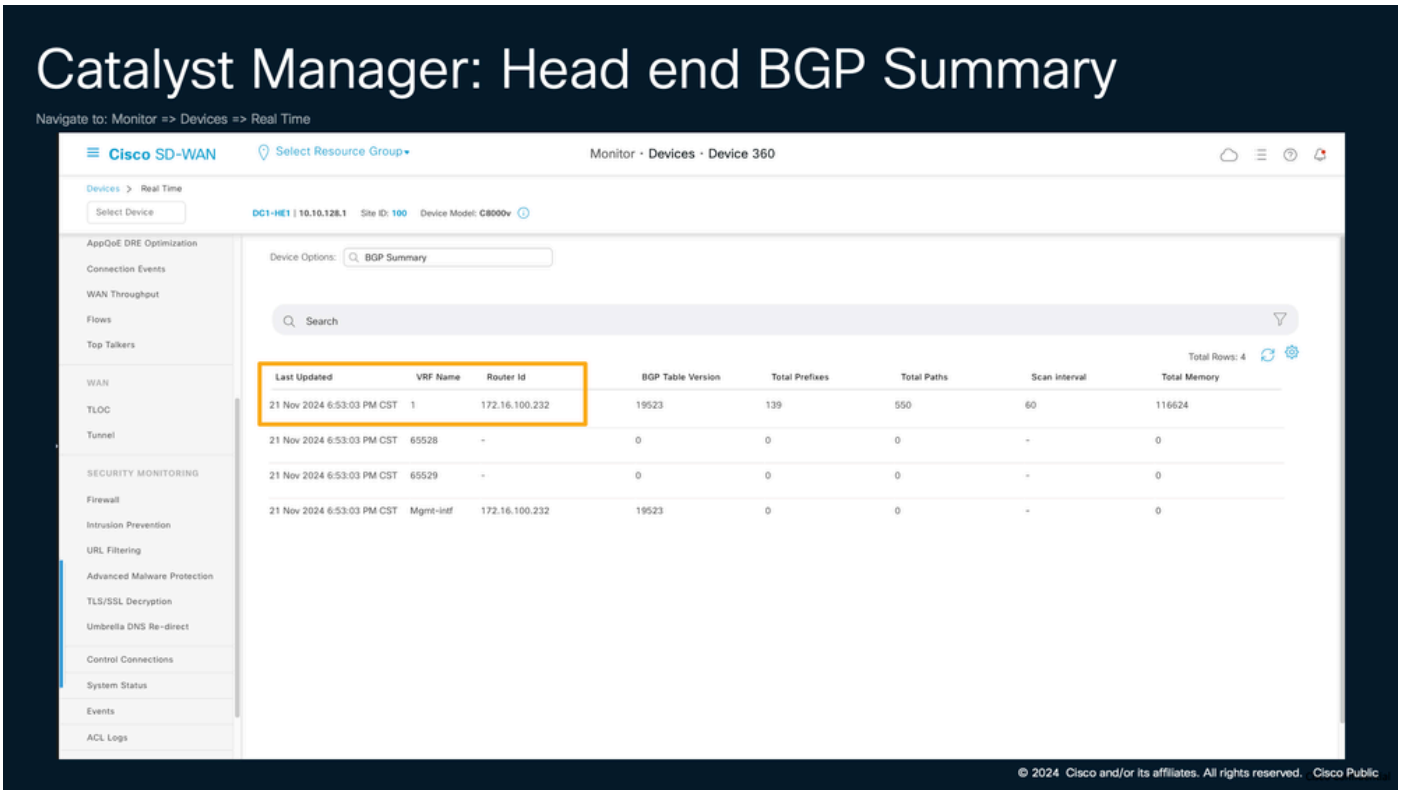
   Figura 9: Cisco Catalyst SD-WAN Manager: Connessioni di controllo dell'headend



   Catalyst Manager Connessioni di controllo dell'headend

2. Le VPN sul lato servizio sono configurate e utilizzano un protocollo di routing per annunciare i prefissi. Questa guida utilizza BGP come protocollo di routing sul lato servizio.

Figura 10: Cisco Catalyst SD-WAN Manager: Riepilogo BGP headend



Per configurare l'interconnessione SD-WAN con Network Tunnel Group (NTG) utilizzando il metodo IPSec manuale, attenersi alla seguente procedura:

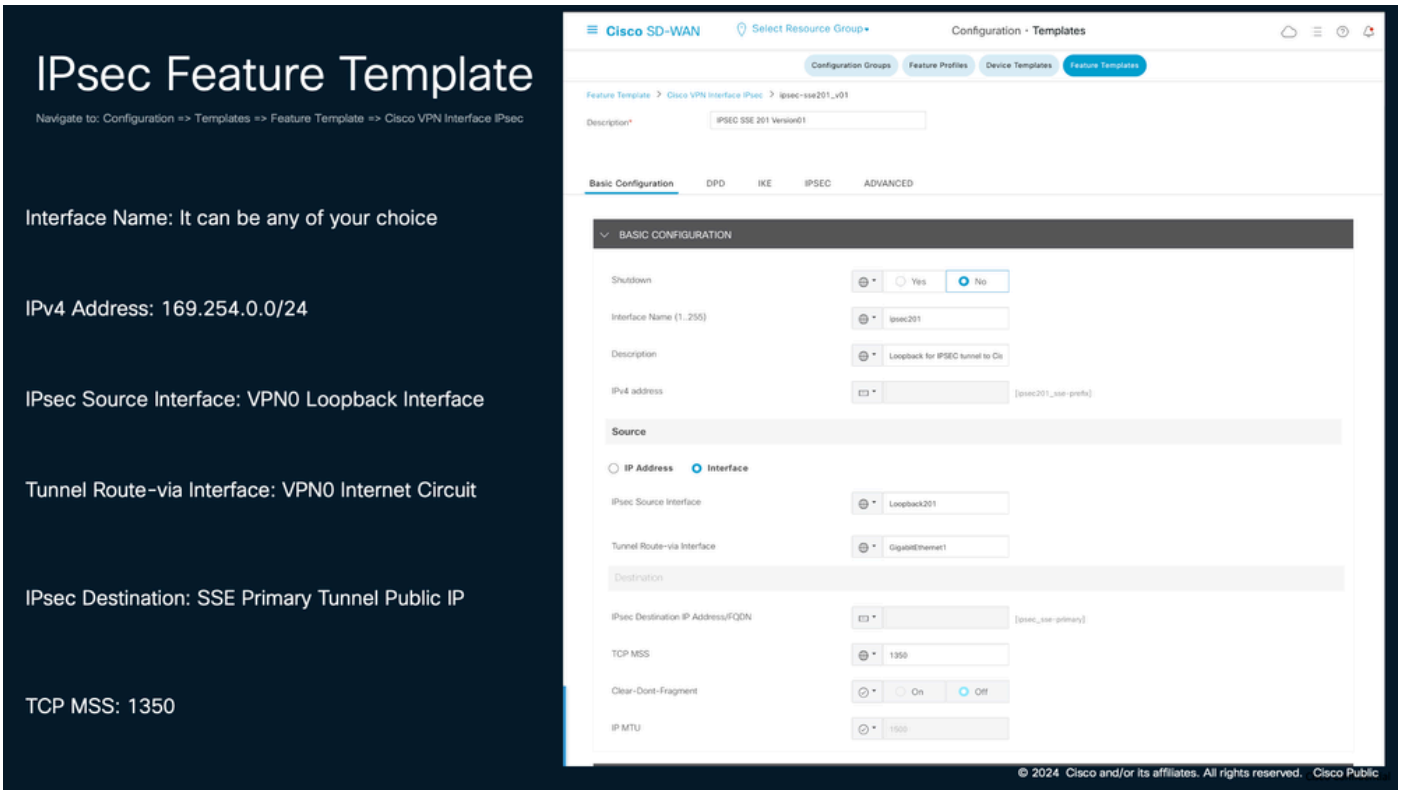
Nota: Ripetere questo passaggio per il numero richiesto di tunnel per la distribuzione.

Fare riferimento alla documentazione ufficiale per la limitazione del tunnel: https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

Questi passaggi descrivono in dettaglio il processo di connessione di DC1-HE1 (headend 1 del centro dati 1) all'hub primario SSE Virginia. Questa configurazione stabilisce un tunnel sicuro tra il router SD-WAN nel centro dati e il Cisco Secure Access Network Tunnel Group (NTG) situato nel punto di presenza (POP) della Virginia

Passaggio 1: Crea modello di funzionalità IPSec
Creare un modello di funzionalità IPSec per definire i parametri del tunnel IPSec che connette il router headend SD-WAN al protocollo NTG.

Figura 11: modello della funzionalità IPSec: Configurazione di base



Modello funzionalità IPSec: Configurazione di base

Nome interfaccia: Può essere di vostra scelta
Indirizzo IPv4: SSE esegue l'ascolto di 169.254.0.0/24 in base al requisito che consente di dividere la subnet in base alla scelta, come procedura ottimale da utilizzare con /30. In questa guida non viene incluso il primo blocco per un utilizzo futuro.

Interfaccia origine IPsec: Definire un'interfaccia di loopback VPN0 univoca per l'interfaccia IPsec corrente. Per coerenza e risoluzione dei problemi è consigliabile mantenere la stessa numerazione.
Tunnel Route-via interfaccia: Puntare l'interfaccia che può essere utilizzata come base per raggiungere SSE (deve avere accesso a Internet)

Destinazione IPsec: Indirizzo IP hub primario

Fare riferimento alla Figura 7: Secure Access Network Tunnel Group US (Virginia) - versione 35.171.214.188

TCP MSS: Deve essere 1350 (Riferimento: [https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters)](https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters)

Esempio: DC1-HE1 verso l'hub primario SSE Virginia

Nome interfaccia: ipsec201

Descrizione: loopback per tunnel IPSEC su Cisco

Indirizzo IPv4: 169.254.0.x/30

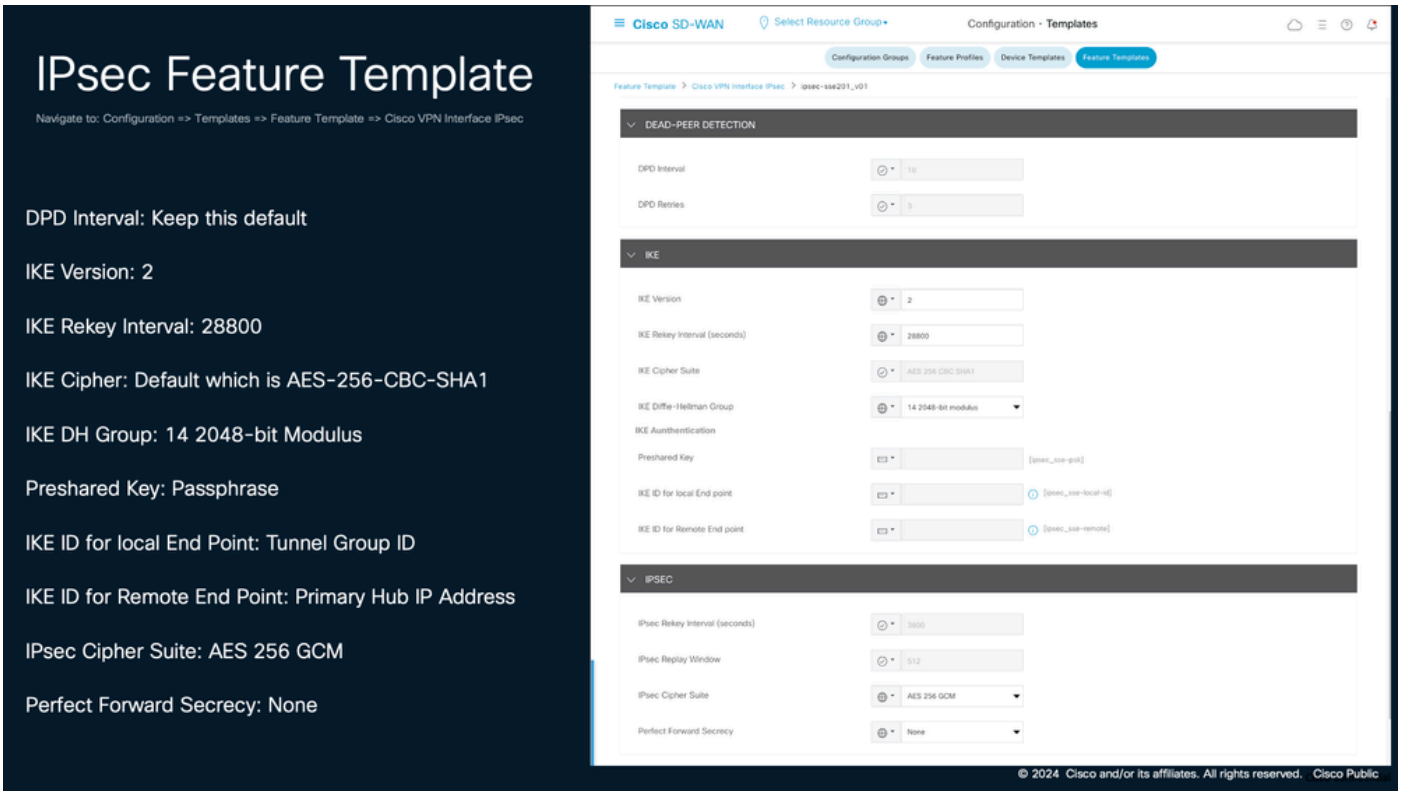
Interfaccia origine IPsec: loopback201

Tunnel Route-via interfaccia: Gigabit Ethernet1

Indirizzo IP/FQDN destinazione IPsec: 35.xxx.xxx.xxx

TCP MSS: 1350

Figura 12: modello della funzionalità IPSec: IPSEC IKE



Modello funzionalità IPSec: IPSEC IKE

Intervallo DPD: Mantieni questa impostazione predefinita
Versione IKE: 2
Intervallo di rigenerazione IKE: 28800
Cifratura IKE: Predefinito: AES-256-CBC-SHA1
Gruppo DH IKE: 14 Modulo a 2048 bit
Chiave già condivisa: Passphrase
ID IKE per endpoint locale: ID gruppo tunnel

Fare riferimento alla Figura 7: Secure Access Network Tunnel Group US (Virginia), in inglese mn03lab1+201@8167900-638880310-sse.cisco.com

---

Nota: A ciascun tunnel deve essere associato un endpoint univoco; utilizzare "+loopbackID" Esempio: mn03lab1+202@8167900-638880310-sse.cisco.com, mn03lab1+203@8167900-638880310-sse.cisco.com e così via.

ID IKE per endpoint remoto: Indirizzo IP hub primario
Suite di crittografia IPsec: AES 256 GCM

Perfect Forward Secrecy Nessuna

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

Esempio:

Versione IKE: 2
Intervallo di rigenerazione IKE: 28800
Cifratura IKE: AES-256-CBC-SHA1
Gruppo DH IKE: 14 Modulo a 2048 bit
Chiave già condivisa: ****

Nota: Passaggio 6 in Aggiunta di un gruppo di tunnel di rete

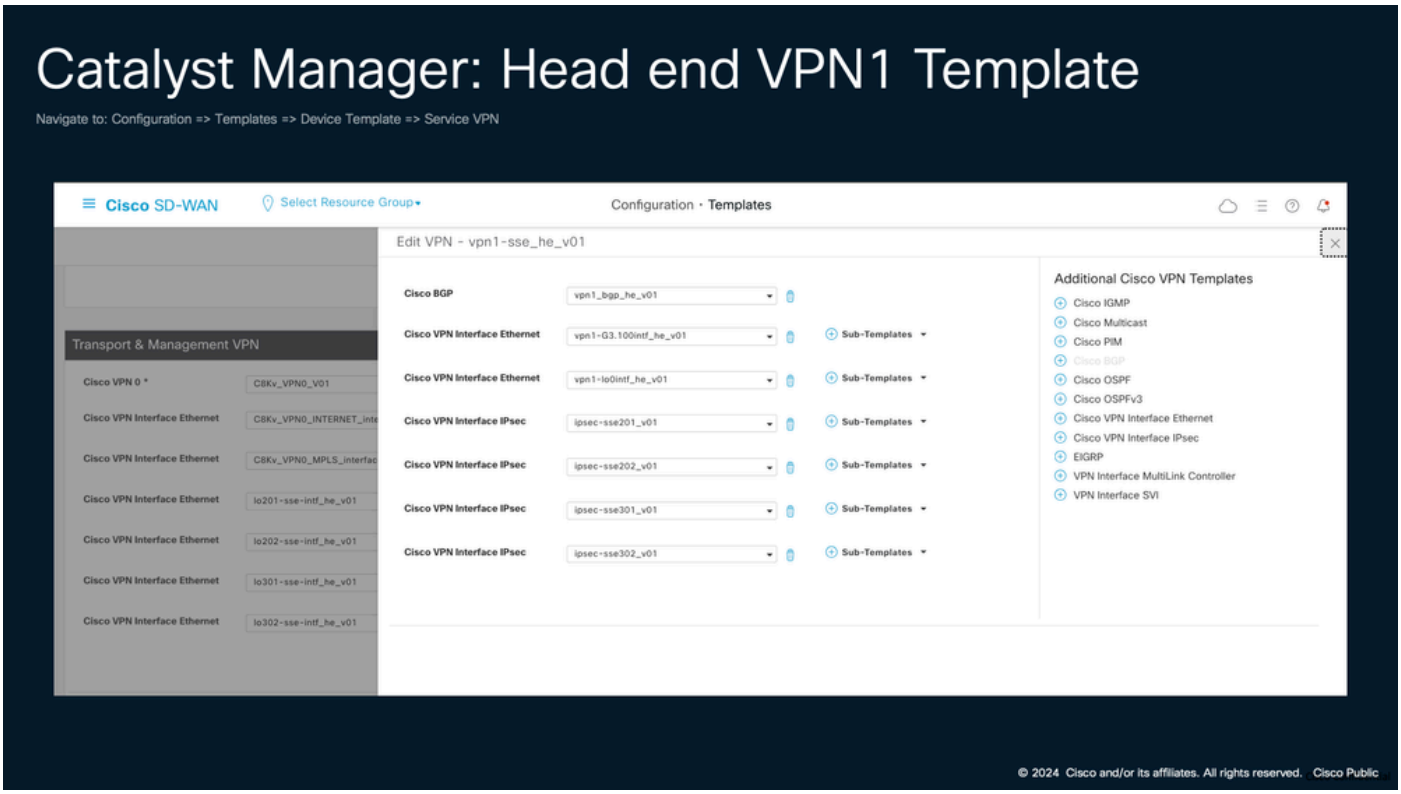
ID IKE per endpoint locale: mn03lab1@8167900-638880310-sse.cisco.com
ID IKE per endpoint remoto: 35.171.xxx.xxx
Suite di crittografia IPsec: AES 256 GCM
Perfect Forward Secrecy Nessuna

Ripetere i passaggi per configurare i tunnel richiesti per gli hub di accesso sicuro primario e secondario.Per una configurazione 2x2, si creano quattro tunnel in totale:

- Due tunnel da DC1-HE1 all'hub di accesso sicuro primario
- Due tunnel da DC1-HE1 all'hub di accesso sicuro secondario

Ora che i modelli sono stati creati, li utilizzeremmo sul lato assistenza vrf mostrata nella figura 13 e il loopback definito allegato al vrf globale mostrato nella figura 14.

Figura 13: Catalyst SD-WAN Manager: Headend VPN1 modello 2x2



Catalyst Manager Modello VPN1 headend

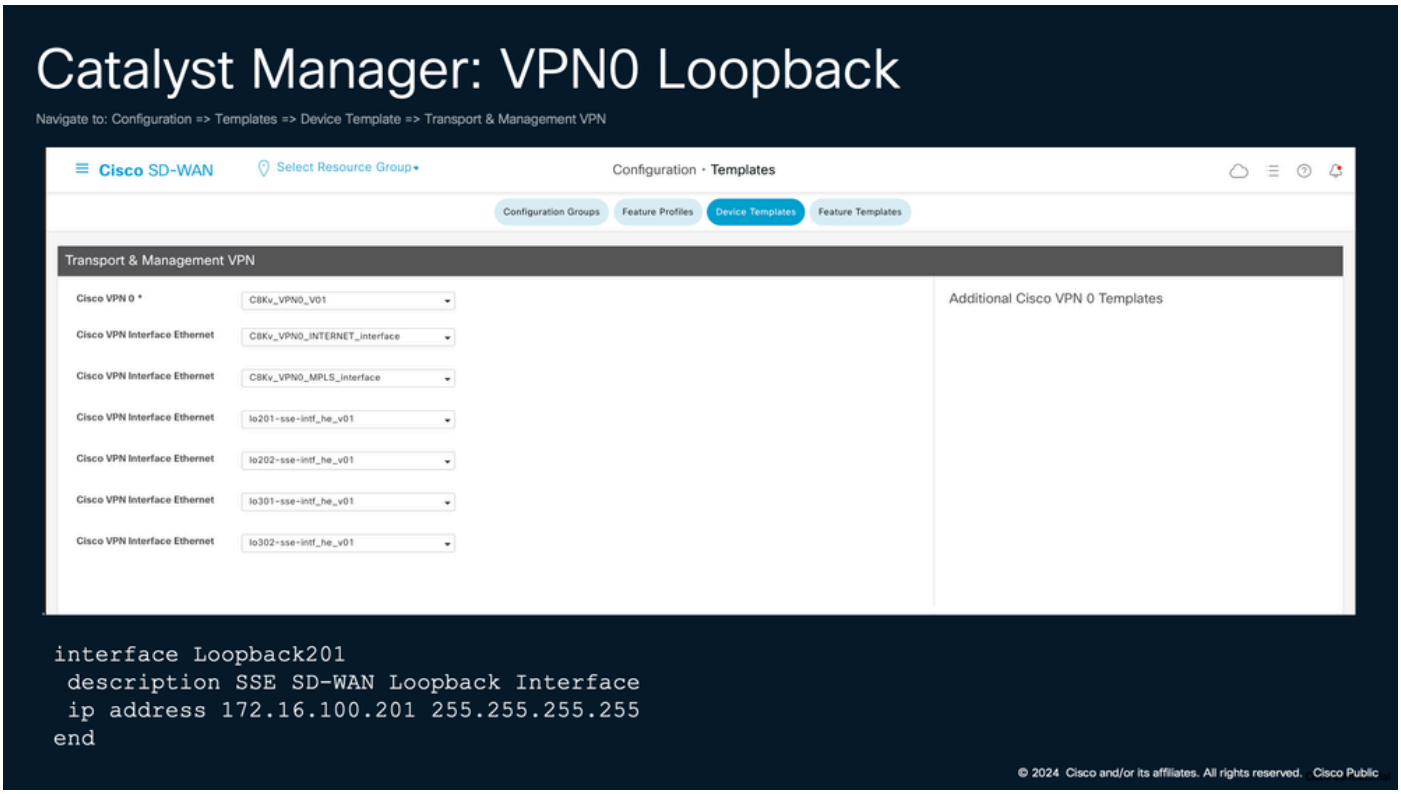
Passaggio 2: Definizione del loopback in VRF globale

Configurare un'interfaccia di loopback nella tabella globale VRF (Virtual Routing and Forwarding). Questo loopback funge da interfaccia di origine per il tunnel IPSec creato nel passaggio 1.

Tutti i loopback a cui si fa riferimento nel passo 1 devono essere definiti nel VRF globale.

L'indirizzo IP può essere definito in qualsiasi intervallo RFC1918.

Figura 14: Catalyst SD-WAN Manager: Loopback VPN0

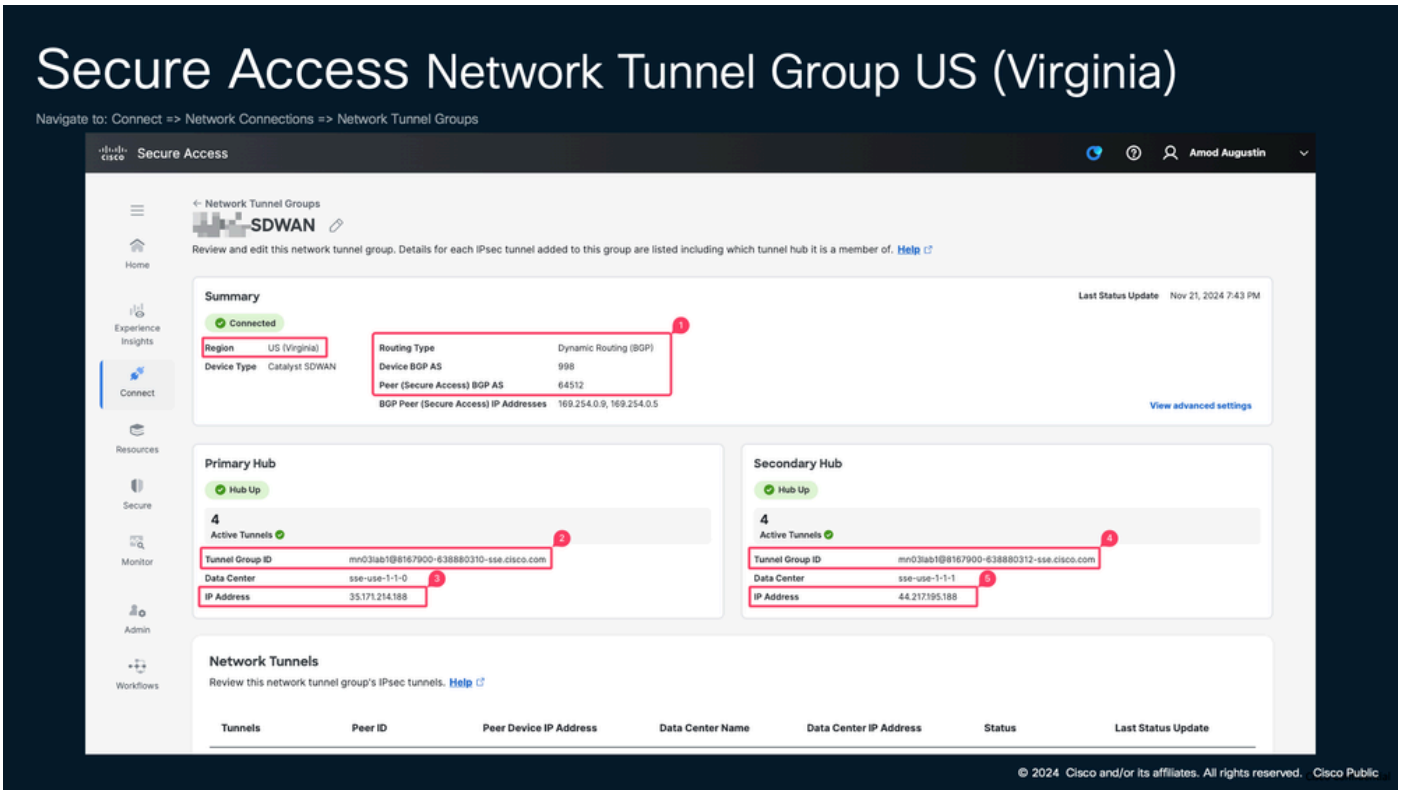


Catalyst Manager Loopback VPN0

Procedura 3. Configurare il vicinato BGP

Usare il modello di funzionalità BGP per definire il vicinato BGP per tutte le interfacce del tunnel. Per configurare i valori BGP, fare riferimento alla configurazione dei rispettivi gruppi di tunnel di rete BGP nel portale Cisco Secure Access.

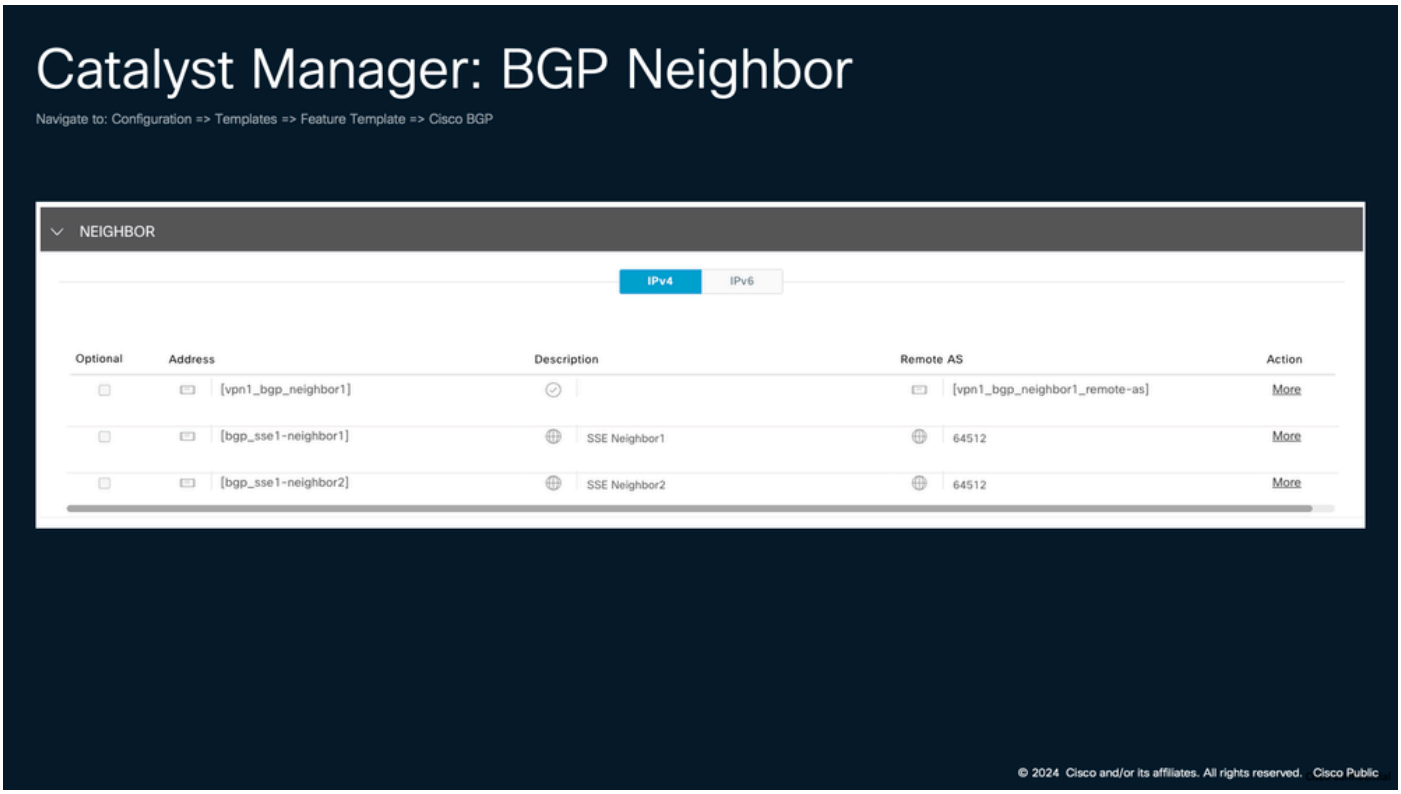
Figura 15: Secure Access Network Tunnel Group US (Virginia)



Secure Access Network Tunnel Group US (Virginia)

In questo esempio, vengono utilizzate le informazioni della Figura 15 (casella 1) per definire BGP utilizzando un modello di feature.

Figura 16: Router adiacente Catalyst SD-WAN Manager BGP



Router adiacente Catalyst SD-WAN Manager BGP

Configurazione generata utilizzando il modello di feature:

```
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#
```

Verifica

```
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
```

Riferimento

Un'implementazione attiva/attiva avrebbe un percorso multiplo dallo switch principale collegato a entrambi gli headend SD-WAN.

Figura 17: Scenario attivo/attivo per router adiacente BGP

```
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>
```

Adiacente BGP attivo/attivo

Un'implementazione Active/Standby avrebbe un percorso attivo dal core switch agli headend SD-WAN a causa della prelazione dell'ASPL (che viene eseguita utilizzando una mappa del percorso al router adiacente).

Figura 18: Scenario attivo/standby per router adiacente BGP

```
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>
```

Adiacente BGP attivo/standby

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).