Configuración de la interconexión de aplicaciones privadas entre el perímetro del servicio de seguridad y la SD-WAN UTILIZANDO el método manual

Contenido

Introducción

Este documento describe una guía completa para conectar Cisco Secure Access con routers SD-WAN, centrándose en el acceso seguro a aplicaciones privadas.

Sobre Esta Guía

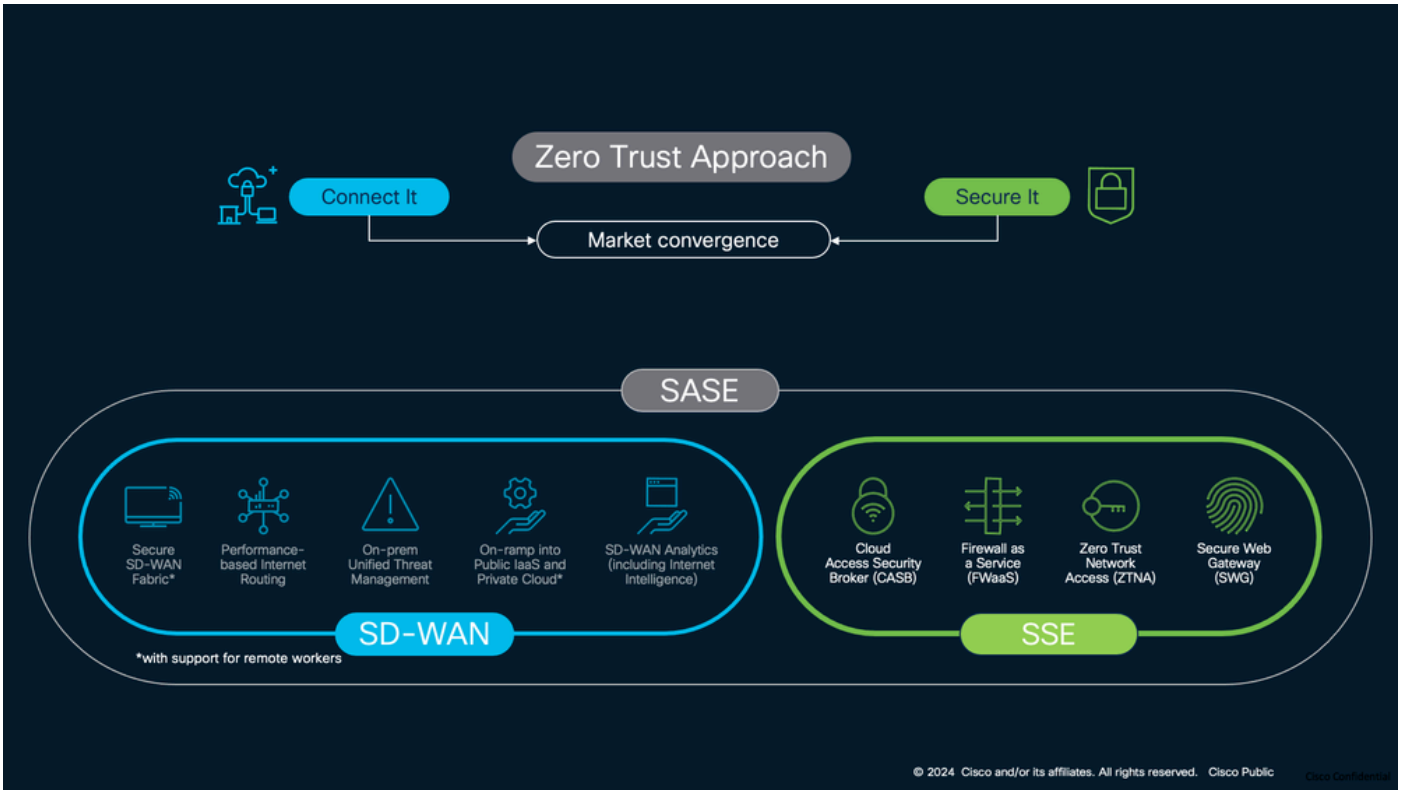
Nota: Las configuraciones enumeradas aquí se han desarrollado para las versiones UX1.0 y 17.9/20.9 de SD-WAN.

En esta guía se presenta un tutorial estructurado de estos pasos clave:

- Definición de Grupos de Túnel de Red (NTG)
- Configuración del túnel IPSec: Instrucciones detalladas sobre la configuración de túneles IPSec seguros entre routers SD-WAN de Cisco y NTG de Cisco Secure Access.
- Vecindad BGP: Procedimientos paso a paso para ejecutar vecindades BGP a través de los

túneles IPSec para garantizar el ruteo dinámico y la resistencia de red mejorada.
- Acceso a aplicaciones privadas: Guía para configurar y proteger el acceso a aplicaciones privadas a través de los túneles establecidos.

Figura 1: Enfoque de confianza cero para SD-WAN y SSE de Cisco



SSE con SD-WAN

Esta guía se centra en las prácticas recomendadas de implementación y consideración del diseño para la interconexión NTG. En esta guía, los controladores SD-WAN se implementan en la nube y los routers periféricos WAN se implementan en el Data Center y están conectados al menos a un circuito de Internet.

Suposiciones clave

- Cisco Secure Access Secure Service Edge (SSE): Se supone que Cisco Secure Access SSE ya está aprovisionado para su organización.
- Router periférico WAN SD-WAN de Cisco: Se supone que el router de extremo de la WAN está integrado en la red superpuesta, lo que facilita de forma eficaz el tráfico de los usuarios a través de la infraestructura SD-WAN.
- Aunque esta guía se centra principalmente en los aspectos de diseño y configuración de la SD-WAN, proporciona un enfoque integral para integrar las soluciones Cisco Secure Access en su arquitectura de red existente.

Acerca de esta solución

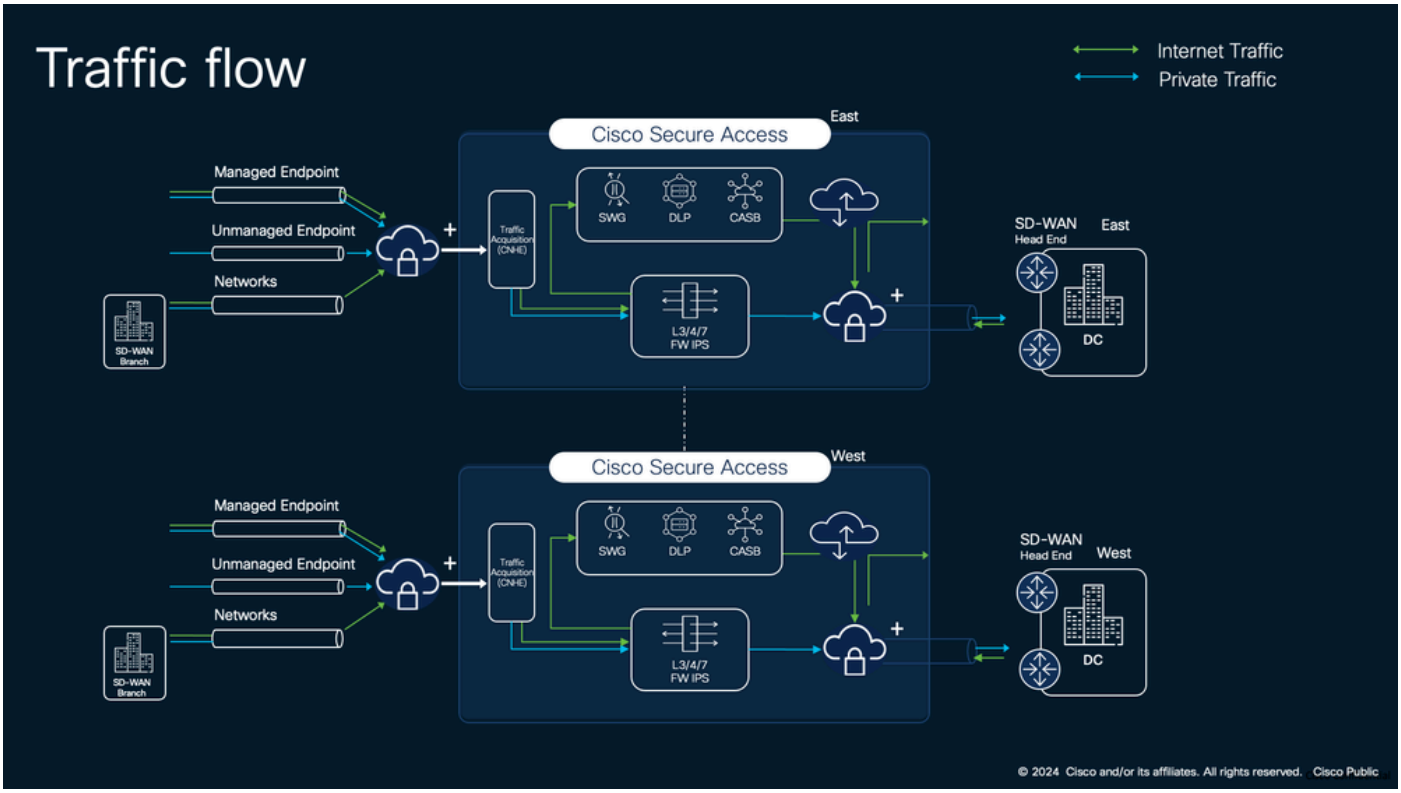
Los túneles de aplicaciones privadas, ofrecidos por Cisco Secure Access, proporcionan conectividad segura a aplicaciones privadas para los usuarios que se conectan a través de Zero

Trust Network Access (ZTNA) y VPN as a Service (VPNaaS). Estos túneles permiten a las organizaciones vincular de forma segura a los usuarios remotos con recursos privados alojados en Data Centers o nubes privadas.
Mediante IKEv2 (Intercambio de claves de Internet versión 2), estos grupos de túnel establecen conexiones bidireccionales seguras entre Cisco Secure Access y los routers SD-WAN. Admiten una alta disponibilidad a través de varios túneles dentro del mismo grupo y ofrecen una gestión del tráfico flexible a través de un routing estático y dinámico (BGP).
Los túneles IPsec pueden transportar tráfico de varias fuentes, incluidas:

- Usuarios de VPN de acceso remoto
- Conexiones ZTNA basadas en navegador o en cliente
- Otras ubicaciones de red conectadas a Cisco Secure Access

Este enfoque permite a las organizaciones enrutar de forma segura todos los tipos de tráfico de aplicaciones privadas a través de un canal unificado y cifrado, lo que mejora tanto la seguridad como la eficacia operativa.
Cisco Secure Access, como parte de la solución Cisco Security Service Edge (SSE), simplifica las operaciones de TI a través de una única consola gestionada en la nube, un cliente unificado, la creación centralizada de políticas y la generación de informes agregados. Incorpora varios módulos de seguridad en una solución en la nube, entre los que se incluyen ZTNA, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall como servicio (FWaaS), seguridad DNS, Remote Browser Isolation (RBI) y mucho más. Este completo enfoque mitiga los riesgos de seguridad aplicando principios de confianza cero y aplicando políticas de seguridad granulares

Figura 2: Flujo de tráfico entre Cisco Secure Access y la aplicación privada



Flujo de tráfico de aplicaciones privadas de SSE

La solución descrita en esta guía aborda consideraciones de redundancia completas, que abarcan tanto el router SD-WAN del Data Center como el grupo de túnel de red (NTG) del lado del extremo de servicio de seguridad (SSE). Esta guía se centra en un modelo de implementación de hub SD-WAN activo/activo, que ayuda a mantener un flujo de tráfico ininterrumpido y garantiza una alta disponibilidad.

Prerequisites

Requirements

Se recomienda que tenga conocimiento de estos temas:

- Configuración y gestión de Cisco SD-WAN
- Conocimientos básicos de los protocolos IKEv2 e IPSec
- Configuración del grupo de túnel de red en el portal de Cisco Secure Access
- Conocimiento de BGP y ECMP

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controladores Cisco SD-WAN en 20.9.5a
- Routers periféricos WAN SD-WAN de Cisco en 17.9.5a
- Portal de acceso seguro de Cisco

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Diseño

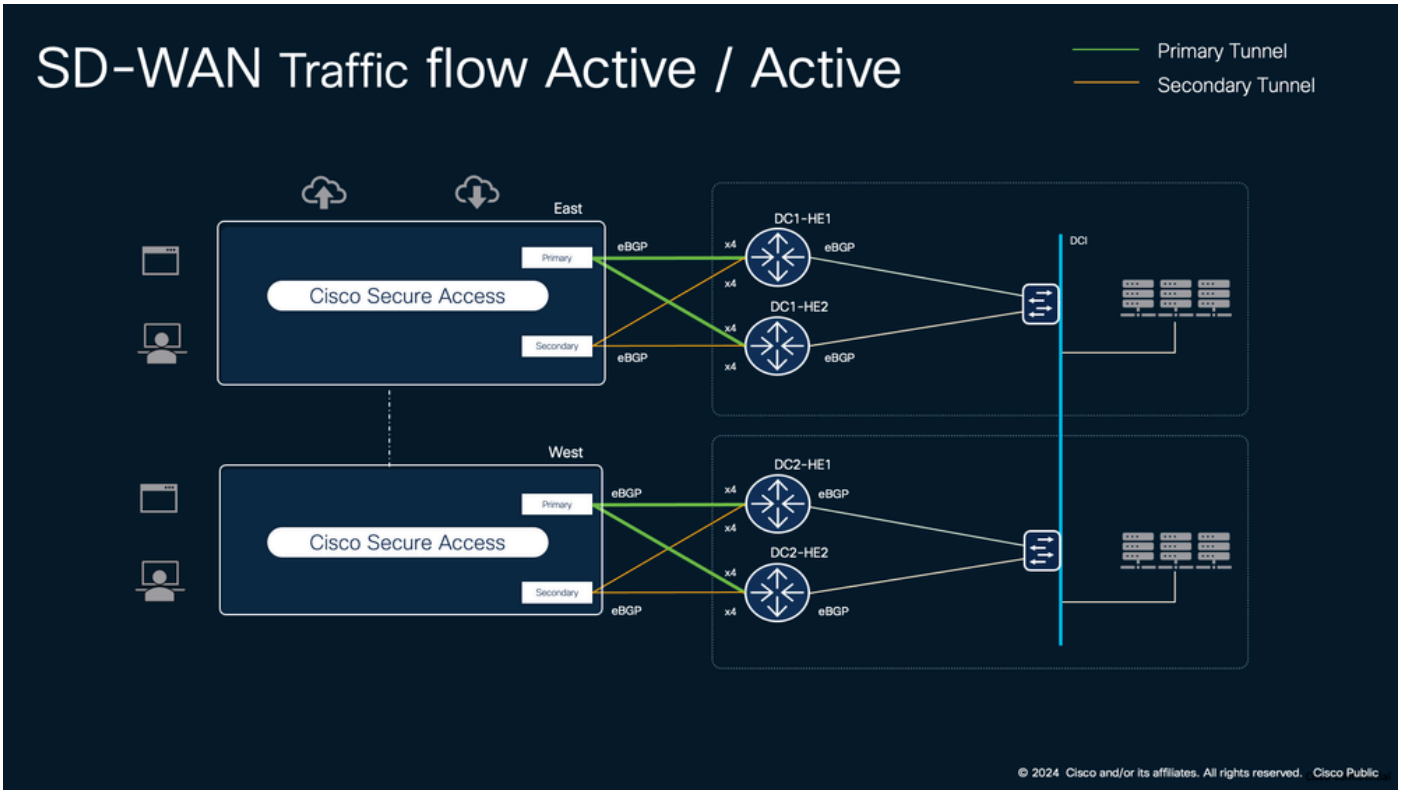
Esta guía describe la solución mediante un modelo de diseño Activo/Activo para routers de cabecera SD-WAN. Un modelo de diseño Activo/Activo en el contexto de los routers de cabecera SD-WAN supone que hay dos routers en un Data Center, ambos conectados al grupo de túnel de red (NTG) del extremo del servicio de seguridad (SSE), como se muestra en la figura 3. En esta situación, ambos routers SD-WAN del Data Center (DC1-HE1 y DC1-HE2) gestionan de forma activa el flujo de tráfico. Para ello, envían la misma longitud de ruta AS (ASPL) al vecino interno del DC. Como resultado, el tráfico desde dentro de la carga del DC se equilibra entre las dos cabeceras.

Cada router de cabecera puede establecer varios túneles a puntos de presencia (POP) SSE. El número de túneles varía en función de sus requisitos y del modelo de dispositivo SD-WAN. En este diseño:

- Cada router tiene 4 túneles hacia el SSE Hub principal y 4 túneles hacia el SSE Hub secundario.
- El número máximo de túneles admitidos por cada concentrador SSE puede variar. Para obtener la información más actualizada, consulte la documentación oficial: https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

Estos routers de cabecera forman vecindades BGP a través de los túneles hacia el SSE. A través de estos vecindarios, las cabeceras anuncian prefijos de aplicaciones privadas a sus vecinos SSE, lo que permite un routing seguro y eficiente del tráfico a los recursos privados.

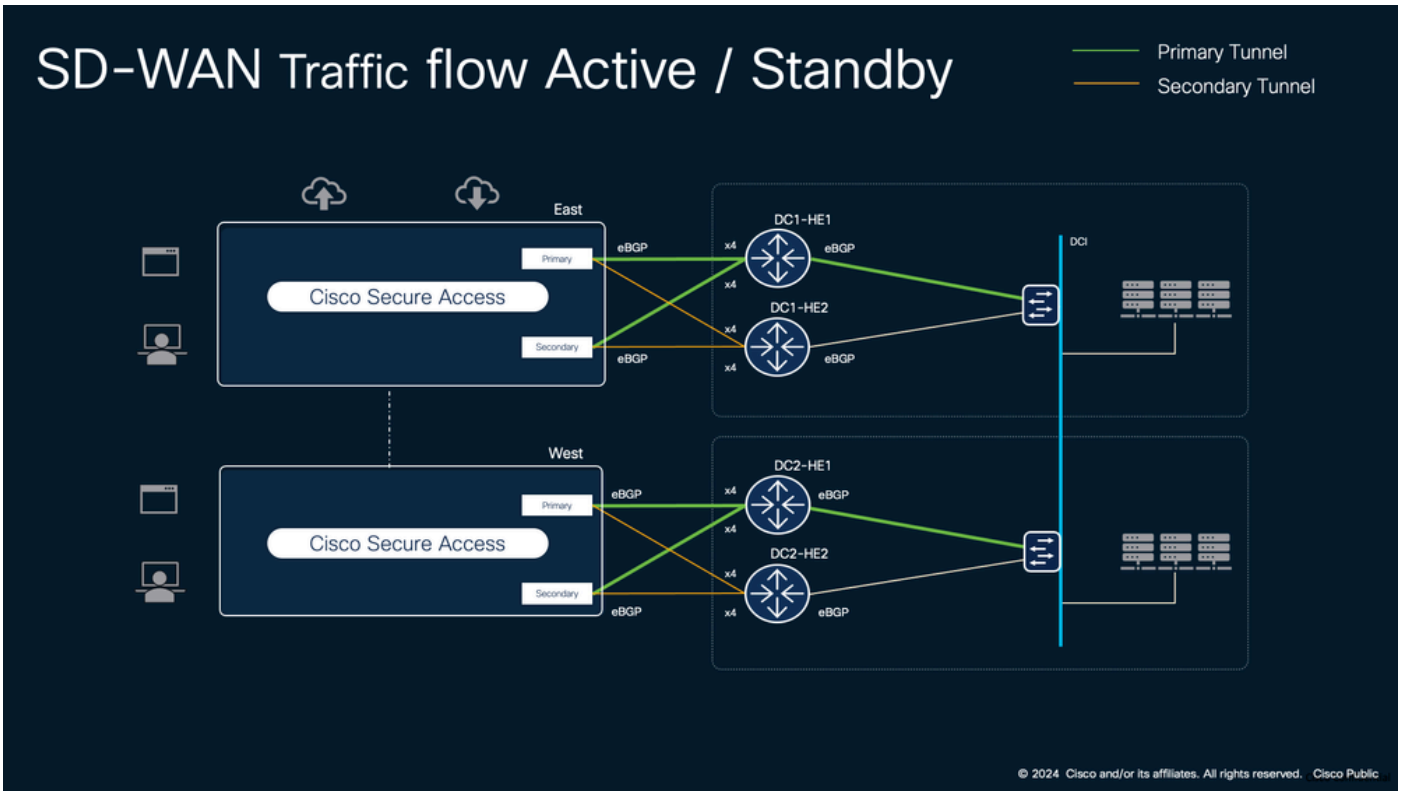
Figura 3: Modelo de implementación activo/activo de SD-WAN a SSE



Modelo de implementación activo/activo de SD-WAN a SSE

Un diseño Activo/En espera designa un router (DC1-HE1) como siempre activo, mientras que el router secundario (DC1-HE2) permanece en espera. El tráfico fluye constantemente a través de la cabecera activa (DC1-HE1) a menos que falle por completo. Este modelo de implementación tiene un inconveniente: si el túnel principal a SSE deja de funcionar, el tráfico pasa a los túneles SSE secundarios que es solamente vía DC1-HE2, causando que cualquier tráfico stateful se reinicie.
En el modelo activo/en espera, BGP AS-Path Length se utiliza para dirigir el tráfico tanto dentro del DC como hacia el SSE. DC1-HE1 envía actualizaciones de prefijo al vecino BGP SSE con una ASPL de 2, mientras que DC1-HE2 envía actualizaciones con una ASPL de 3. El vecino DC interno de DC1-HE1 anuncia prefijos con una longitud de trayecto AS más corta que DC1-HE2, lo que garantiza la preferencia de tráfico para DC1-HE1. (Los clientes pueden elegir otros atributos o protocolos para influir en la preferencia de tráfico).
Los clientes pueden seleccionar un modelo de implementación Activo/Activo o Activo/En espera en función de sus requisitos específicos.

Figura 4: Modelo de implementación activo/en espera de SD-WAN a SSE



Modelo de implementación activo/en espera de SD-WAN a SSE

Configurar

En esta sección se describe el procedimiento:

1. Verifique los requisitos previos para el aprovisionamiento de un grupo de túnel de red en el portal de Cisco Secure Access.
2. Configure la interconexión SD-WAN con Cisco Secure Access Network Tunnel Group (NTG) mediante el método manual IPsec.
3. Configurar vecindad BGP

Nota: Esta configuración se basa en un modelo de implementación Activo/Activo

---

Procedimiento 1. Verificar la Configuración del Grupo de Túnel de Red en Cisco Secure Access Portal

La guía no trata sobre cómo configurar el grupo de túnel de red. Revise esta referencia.

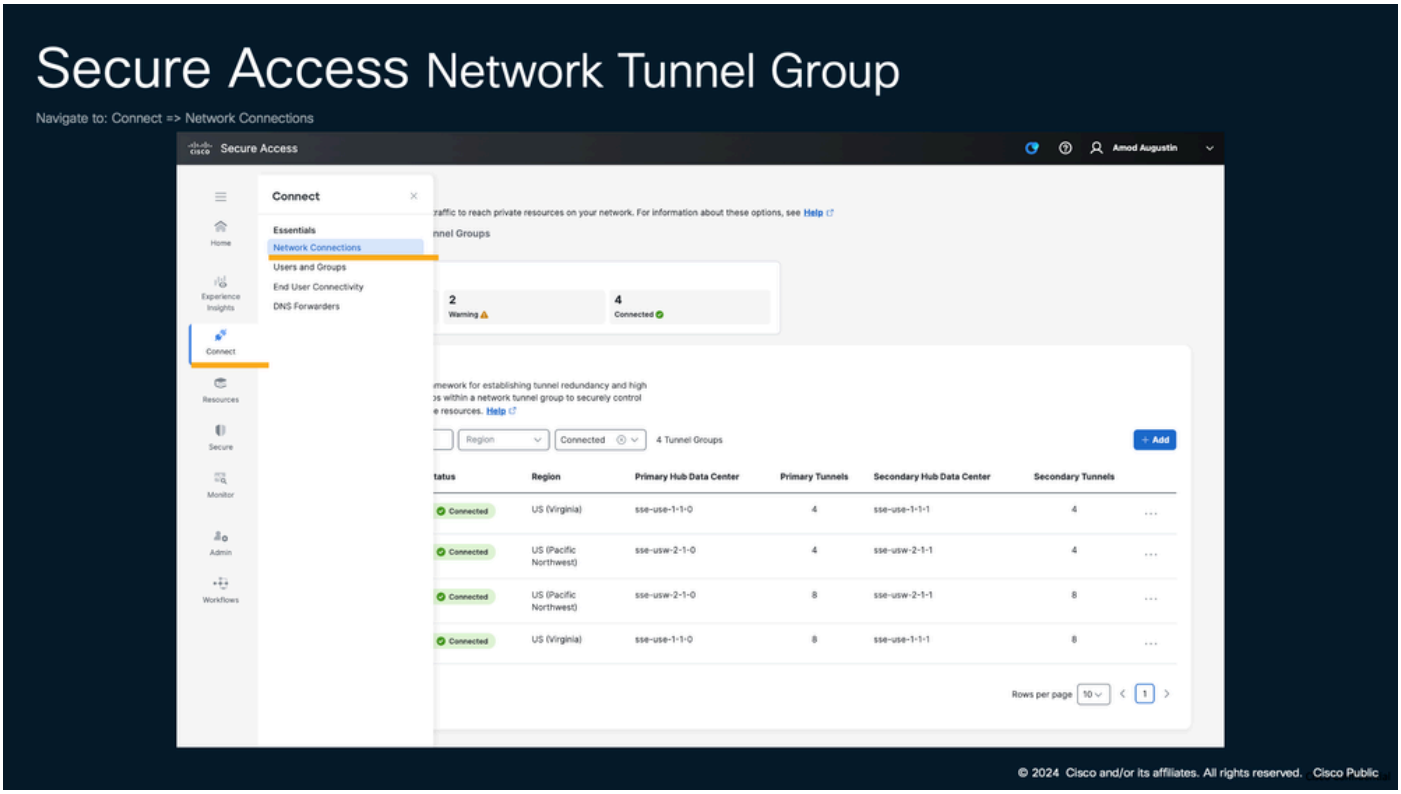
- Agregar un grupo de túnel de red: Documentación de SSE
- Configuración del túnel de red entre Cisco Secure Access y el router Cisco IOS XE mediante ECMP con BGP

Desplácese hasta Cisco Secure Access y asegúrese de que se han aprovisionado los grupos de

túnel de red (NTG). Para el diseño actual, debemos aprovisionar las NTG en dos puntos de presencia (POP) diferentes. En esta guía, utilizamos NTG en los POP de Estados Unidos (Virginia) y de Estados Unidos (Noroeste del Pacífico).

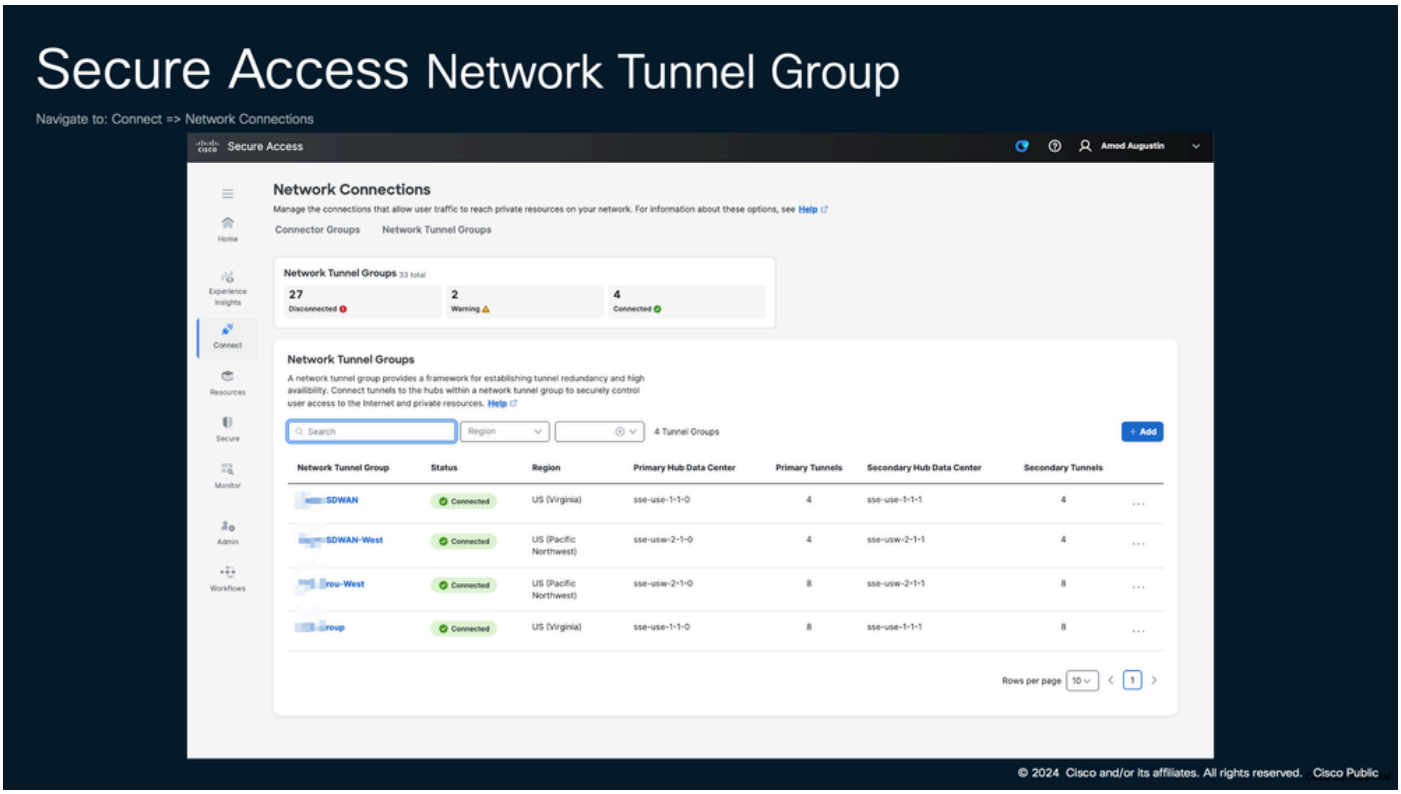
Nota:Los nombres y ubicaciones de los POP pueden variar, pero el concepto clave es tener varias NTG aprovisionadas en ubicaciones geográficamente cercanas a su Data Center. Este enfoque ayuda a optimizar el rendimiento de la red y proporciona redundancia.

Figura 5: Grupo de túnel de red de acceso seguro de Cisco



Grupo de túnel de red de acceso seguro de Cisco

Figura 6: Lista de grupos de túneles de red de Cisco Secure Access



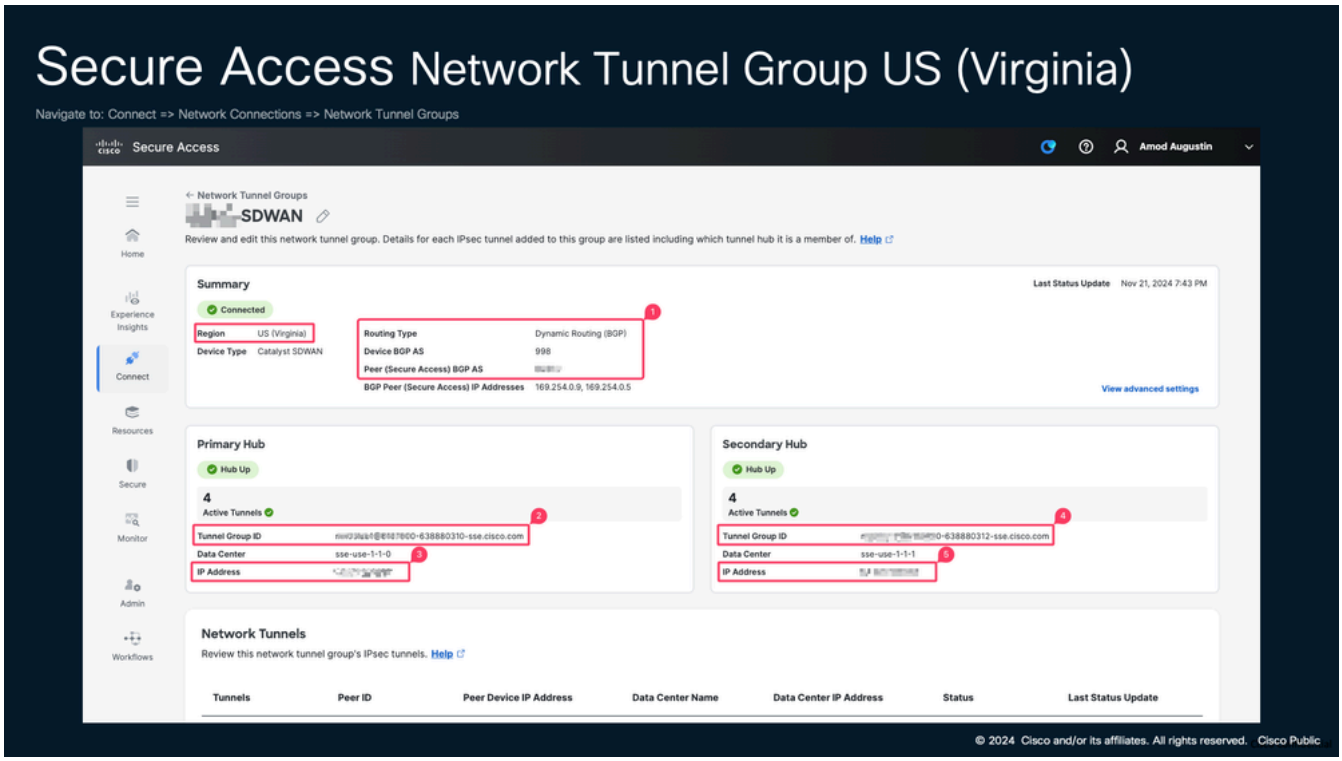
Lista de grupos de túneles de red de acceso seguro

Asegúrese de haber anotado la frase de contraseña del túnel (que sólo se muestra una vez durante la creación del túnel).

Nota: Paso 6 de Agregar un Grupo de Túnel de Red

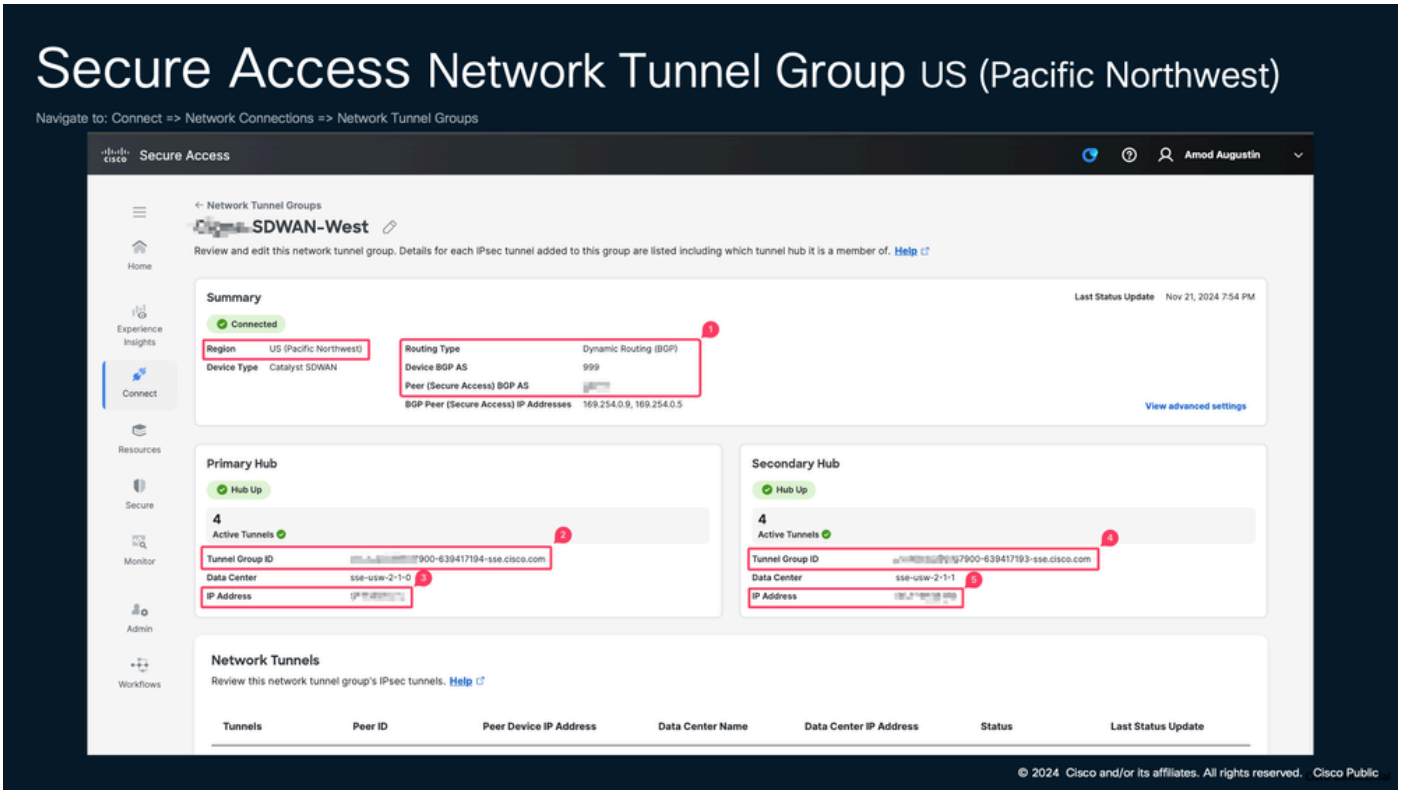
Tome nota también de los atributos del grupo de túnel que utilizamos durante nuestra configuración IPSec. La captura de pantalla (Figura 6) se toma de un entorno de laboratorio para crear grupos NTG en un escenario de producción según las recomendaciones de diseño o uso.

Figura 7: Secure Access Network Tunnel Group (Estados Unidos) (Virginia)



Secure Access Network Tunnel Group (Estados Unidos)

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



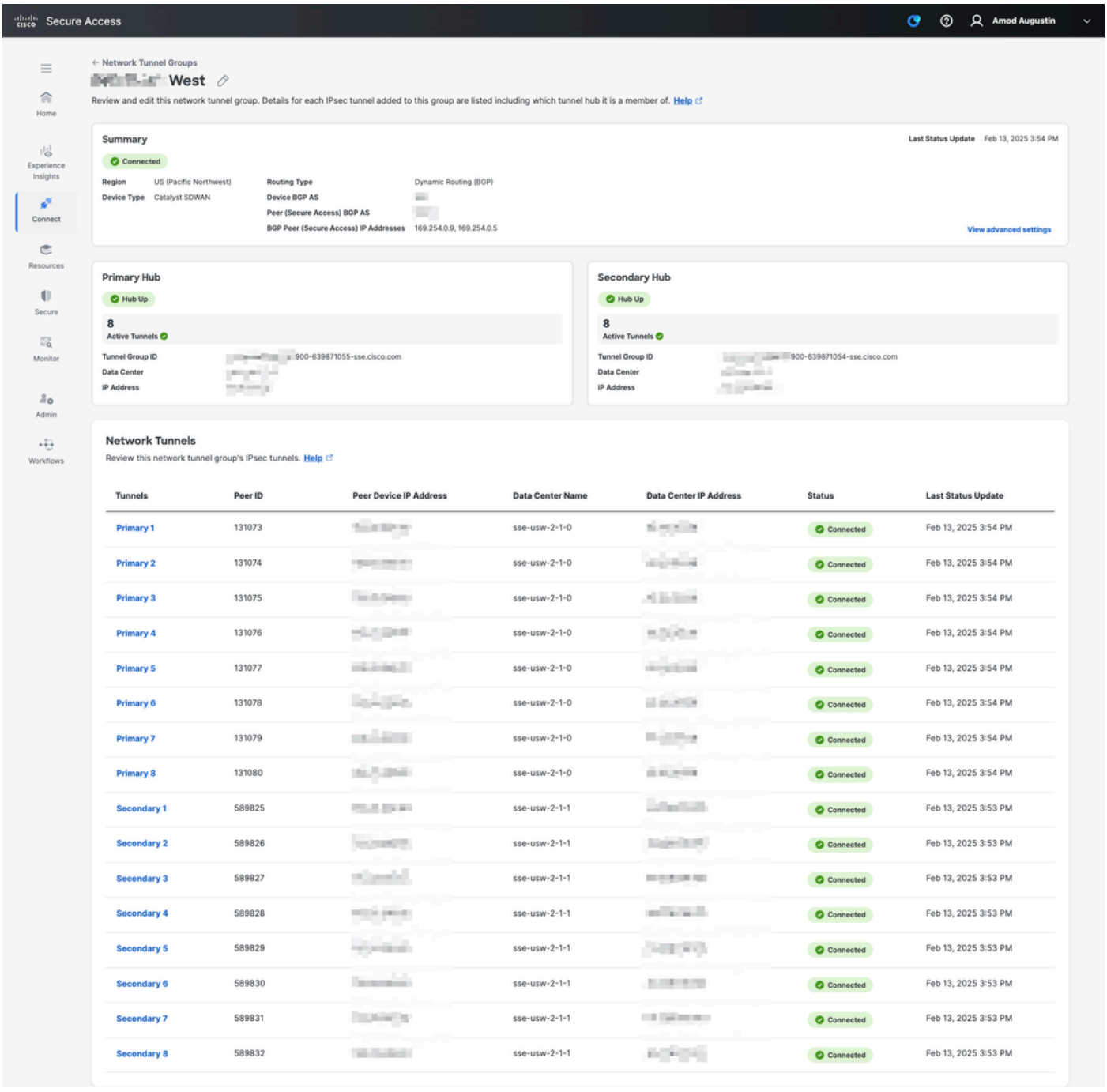
Secure Access Network Tunnel Group EE. UU. (Noroeste del Pacífico)

La figura 8 muestra solo 4 túneles en los hubs primario y secundario. Sin embargo, se ha probado con éxito un máximo de 8 túneles en un entorno de controlador. La compatibilidad máxima con el túnel puede variar en función del dispositivo de hardware que utilice y de la compatibilidad actual con el túnel SSE. Para obtener la información más actualizada, consulte la documentación oficial:

https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels y la nota de la versión del dispositivo de hardware correspondiente.

Aquí se proporciona un ejemplo de una configuración de 8 túneles.

Figura 8a: Túneles NTG de hasta 8 túneles



SSE NTG hasta 8 túneles

Procedimiento 2. Configure la interconexión SD-WAN con el Cisco Secure Access Network Tunnel Group (NTG) mediante el método manual IPsec.

Este procedimiento muestra cómo conectar un Network Tunnel Group (NTG) mediante plantillas de funciones en Cisco Catalyst SD-WAN Manager 20.9 y Cisco Catalyst Edge Router que ejecuta

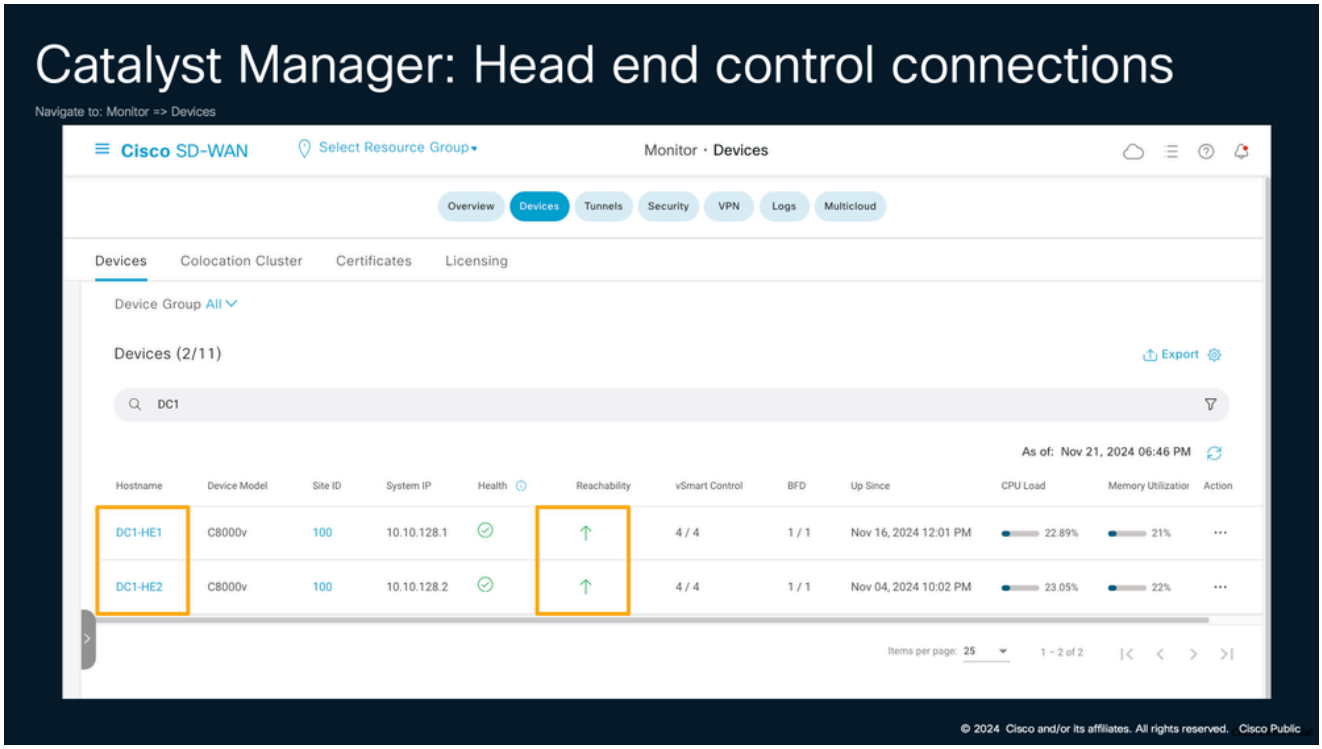
la versión 17.9.

Nota:En esta guía se presupone una implementación de superposición de SD-WAN existente con una topología de hub y radio o de malla completa, donde los hubs sirven como puntos de acceso para aplicaciones privadas alojadas en el Data Center. Este procedimiento también se puede aplicar a implementaciones de sucursales o en la nube.

Antes de continuar, asegúrese de que se cumplen los requisitos previos:

1. Las conexiones de control están activas en el dispositivo para permitir las actualizaciones necesarias desde Cisco Catalyst SD-WAN Manager.

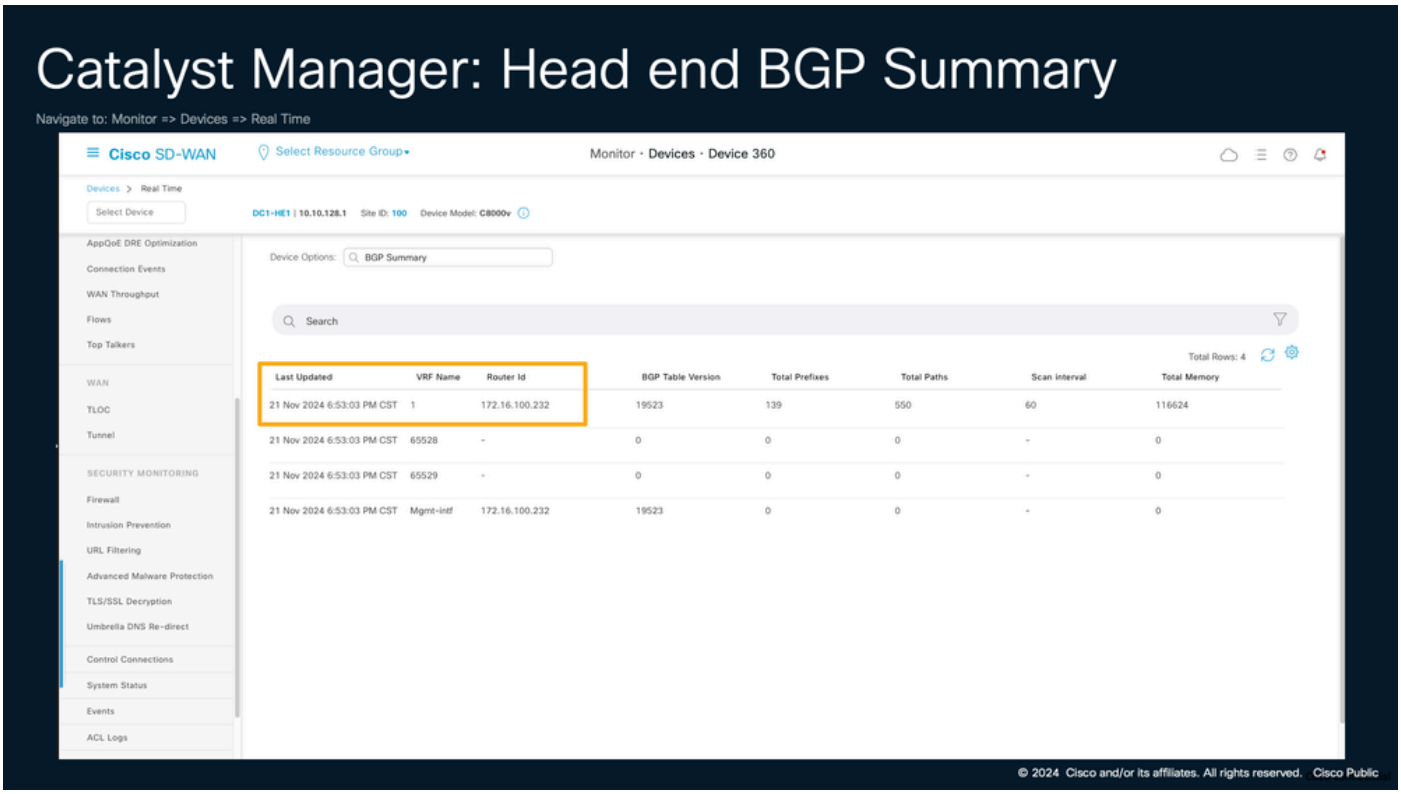
   Figura 9: Administrador de SD-WAN de Cisco Catalyst: Conexiones de control de cabecera



Administrador de Catalyst: Conexiones de control de cabecera

2. Las VPN del lado del servicio se configuran y utilizan un protocolo de ruteo para anunciar los prefijos. Esta guía utiliza BGP como protocolo de ruteo en el lado del servicio.

Figura 10: Administrador de SD-WAN de Cisco Catalyst: Resumen de BGP de cabecera



Para configurar la interconexión SD-WAN con el grupo de túnel de red (NTG) mediante el método IPSec manual, siga estos pasos:

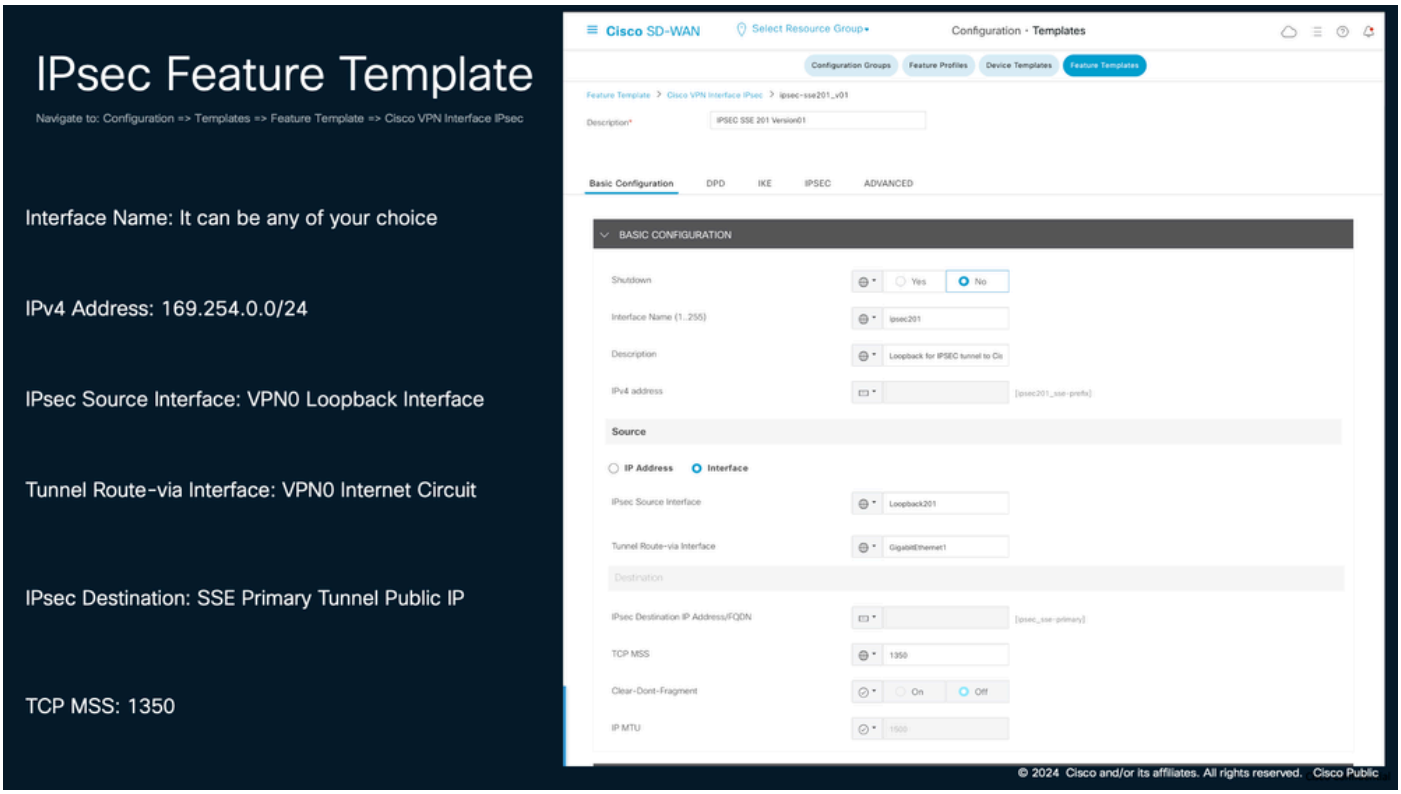
Nota: Repita este paso para el número necesario de túneles para la implementación.

Consulte la documentación oficial para la limitación de túneles: https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

Estos pasos detallan el proceso de conexión de DC1-HE1 (centro de datos 1, centro distribuidor 1) al centro principal de SSE Virginia. Esta configuración establece un túnel seguro entre el router SD-WAN del Data Center y el Cisco Secure Access Network Tunnel Group (NTG) ubicado en el punto de presencia (POP) de Virginia

Paso 1: Crear plantilla de función IPSec
Cree una plantilla de función IPSec para definir los parámetros del túnel IPSec que conecta el router de cabecera SD-WAN al NTG.

Figura 11: Plantilla de la función IPSec: Configuración Básica



Plantilla de función IPsec: Configuración Básica

Nombre de interfaz: Puede ser cualquiera de su elección
Dirección IPv4: SSE escucha 169.254.0.0/24 basándose en el requisito de que puede dividir la subred a su elección, como práctica recomendada, utilice con /30. En esta guía, excluimos el primer bloque para su uso futuro.

Interfaz de origen IPsec: Defina una interfaz de loopback VPN0 que sea única para la interfaz IPsec actual. Por motivos de coherencia y resolución de problemas, se recomienda mantener la misma numeración.
Ruta del túnel a través de la interfaz: Señale la interfaz que se puede utilizar como base para alcanzar SSE (debe tener acceso a Internet).

Destino IPsec: Dirección IP del hub principal

Consulte la Figura 7: Secure Access Network Tunnel Group US (Virginia) (Grupo de túneles de la red de acceso seguro de EE. UU.). Este es el 35.171.214.188.

TCP MSS: Debe ser 1350 (Referencia: [https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters)](https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters)

Ejemplo: DC1-HE1 hacia el hub principal de SSE Virginia

Nombre de interfaz: IPSec201

Descripción: Bucle invertido para túnel IPSEC a Cisco

Dirección IPv4: 169.254.0.x/30

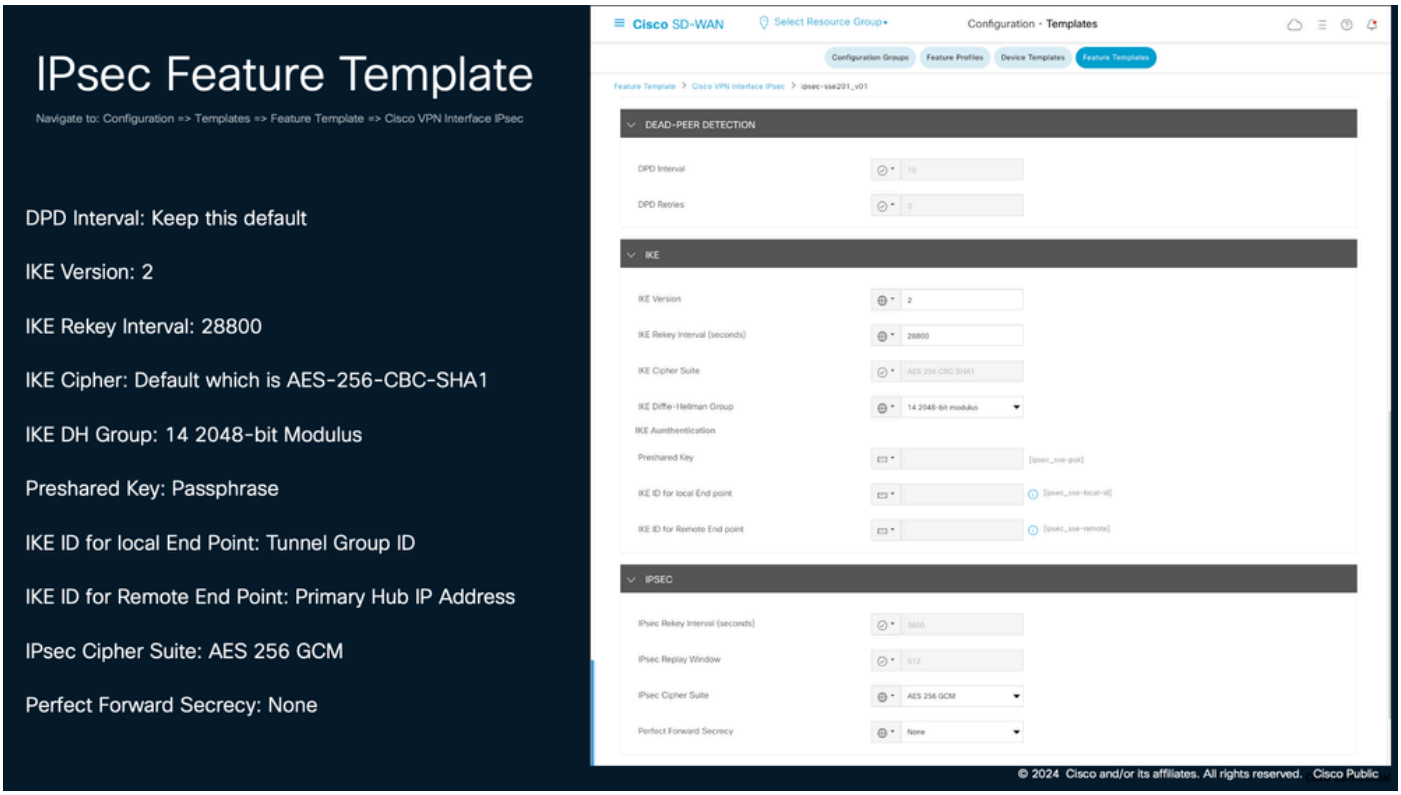
Interfaz de origen IPsec: Loopback201

Ruta del túnel a través de la interfaz: GigabitEthernet1

Dirección IP/FQDN de destino de IPsec: 35.xxx.xxx.xxx

TCP MSS: 1350

Figura 12: Plantilla de la función IPSec: IKE IPSEC



Plantilla de función IPsec: IKE IPSEC

Intervalo DPD: Mantener este valor predeterminado
Versión IKE: 2
Intervalo de regeneración de claves IKE: 28800
Cifrado IKE: Valor predeterminado: AES-256-CBC-SHA1
Grupo IKE DH: Módulo de 14 2048 bits
Clave previamente compartida: Frase de contraseña
ID de IKE para punto final local: ID del grupo de túnel

Consulte la figura 7: Secure Access Network Tunnel Group (EE. UU.) (Virginia). Esta es mn03lab1+201@8167900-638880310-sse.cisco.com

---

Nota: Cada túnel debe tener un punto final único para esto; use "+loopbackID" Ejemplo: mn03lab1+202@8167900-638880310-sse.cisco.com, mn03lab1+203@8167900-638880310-sse.cisco.com, etc.

ID de IKE para punto final remoto: Dirección IP del hub principal
Conjunto de cifrado IPsec: AES 256 GCM

Confidencialidad directa perfecta: Ninguno

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

Ejemplo:

Versión IKE: 2
Intervalo de regeneración de claves IKE: 28800
Cifrado IKE: AES-256-CBC-SHA1
Grupo IKE DH: Módulo de 14 2048 bits
Clave previamente compartida: *****

Nota: Paso 6 de Agregar un Grupo de Túnel de Red

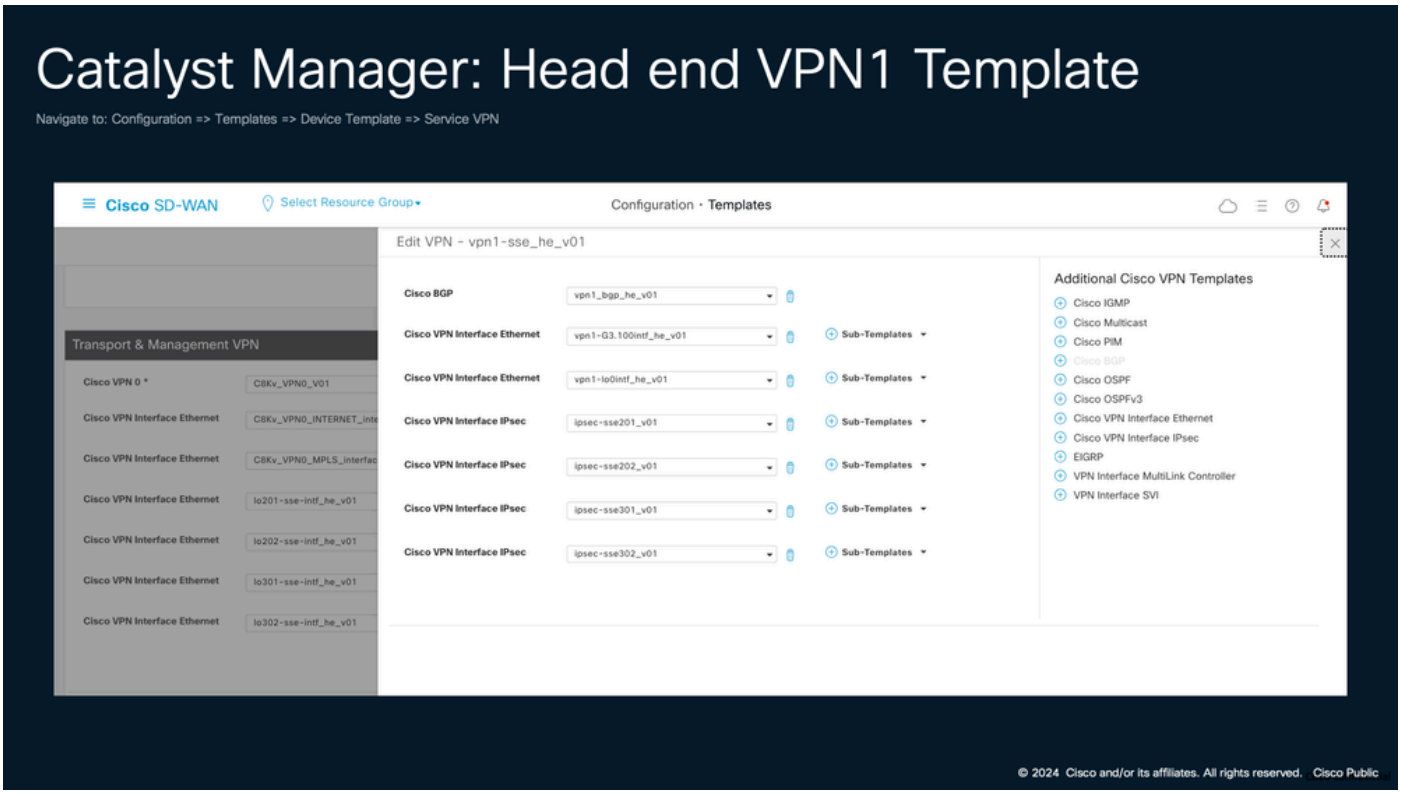
ID de IKE para el terminal local: mn03lab1@8167900-638880310-sse.cisco.com
ID de IKE para el punto final remoto: 35.171.xxx.xxx
Conjunto de cifrado IPsec: AES 256 GCM
Confidencialidad directa perfecta: Ninguno

Repita los pasos para configurar los túneles requeridos para los hubs de Secure Access primario y secundario.Para una configuración 2x2, debe crear cuatro túneles en total:

- Dos túneles desde DC1-HE1 hasta el hub de acceso seguro principal
- Dos túneles desde DC1-HE1 hasta el hub de acceso seguro secundario

Ahora que se han creado las plantillas, las utilizaríamos en el lado del servicio vrf mostrado en la figura 13 y el loopback definido adjunto en el vrf global mostrado en la figura 14.

Figura 13: Catalyst SD-WAN Manager: Plantilla VPN1 de cabecera 2x2



Administrador de Catalyst: Plantilla VPN1 de cabecera

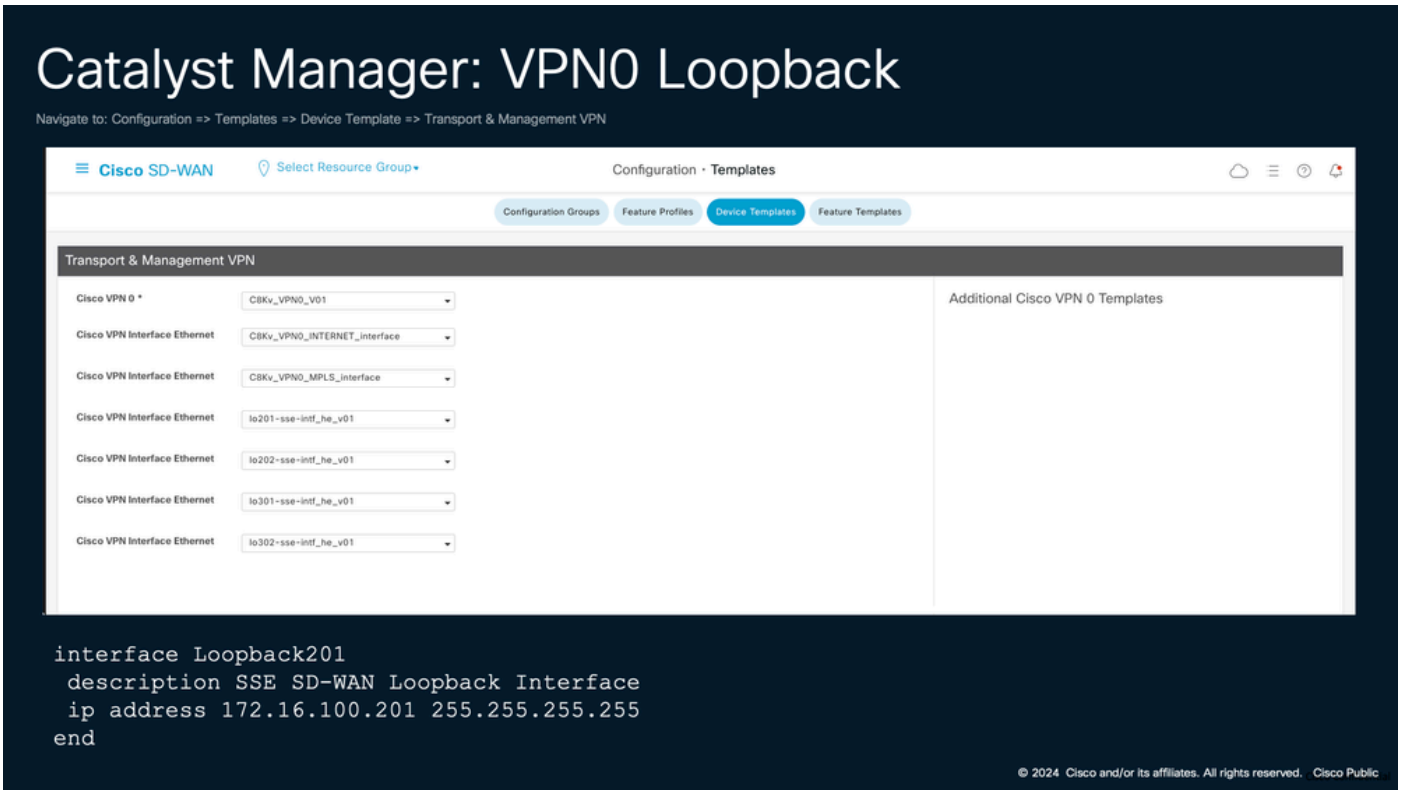
Paso 2: Definición del Loopback en Global VRF

Configure una interfaz de loopback en la tabla global VRF (Virtual Routing and Forwarding). Este loopback sirve como interfaz de origen para el túnel IPSec creado en el paso 1.

Todos los loopback a los que se hace referencia en el Paso 1 deben definirse en Global VRF.

La dirección IP se puede definir en cualquier intervalo RFC1918.

Figura 14: Catalyst SD-WAN Manager: VPN0 Loopback

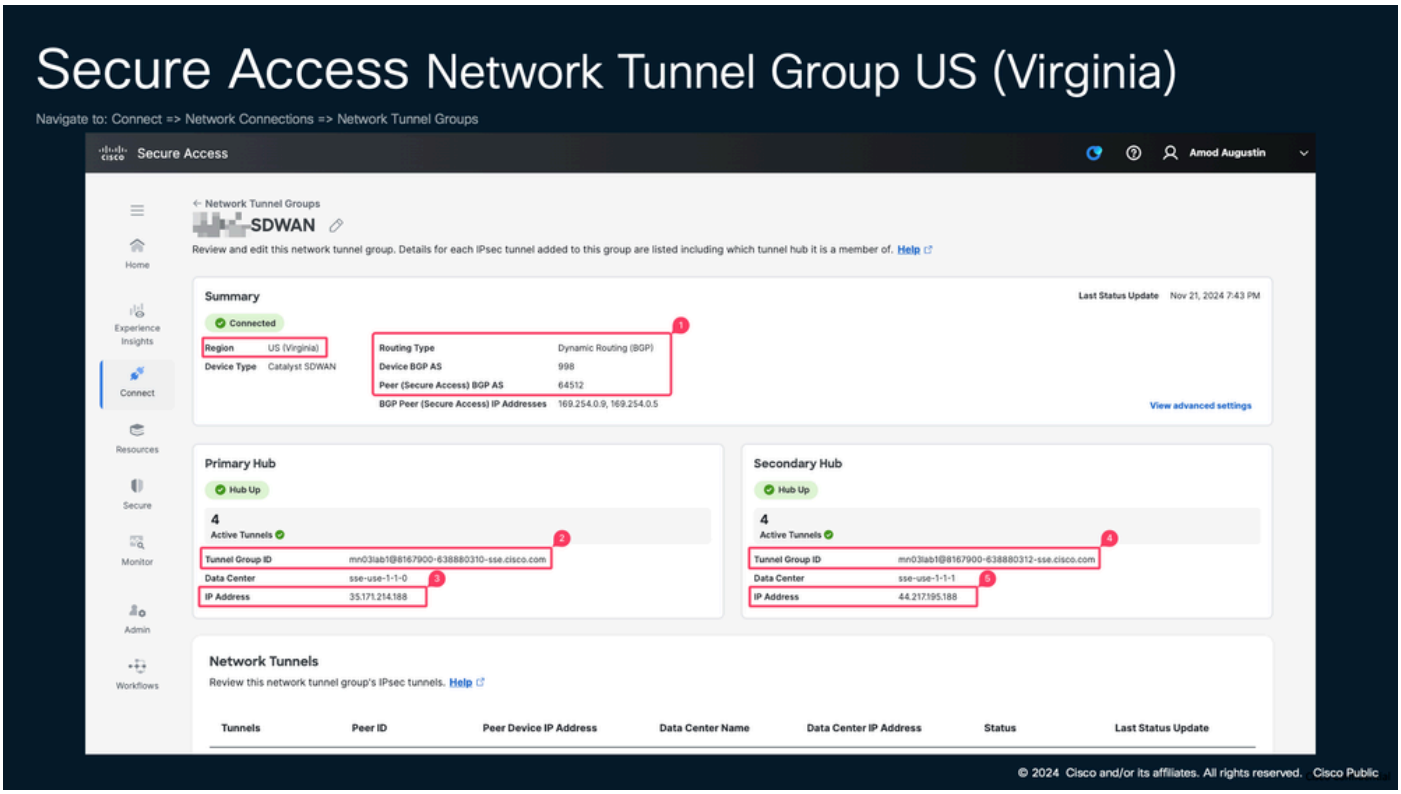


Administrador de Catalyst: VPN0 Loopback

Procedimiento 3. Configuración de la vecindad BGP

Utilice la plantilla de función BGP para definir la vecindad BGP para todas las interfaces de túnel. Consulte la configuración de BGP de los grupos de túnel de red correspondientes en el portal de acceso seguro de Cisco para configurar los valores de BGP.

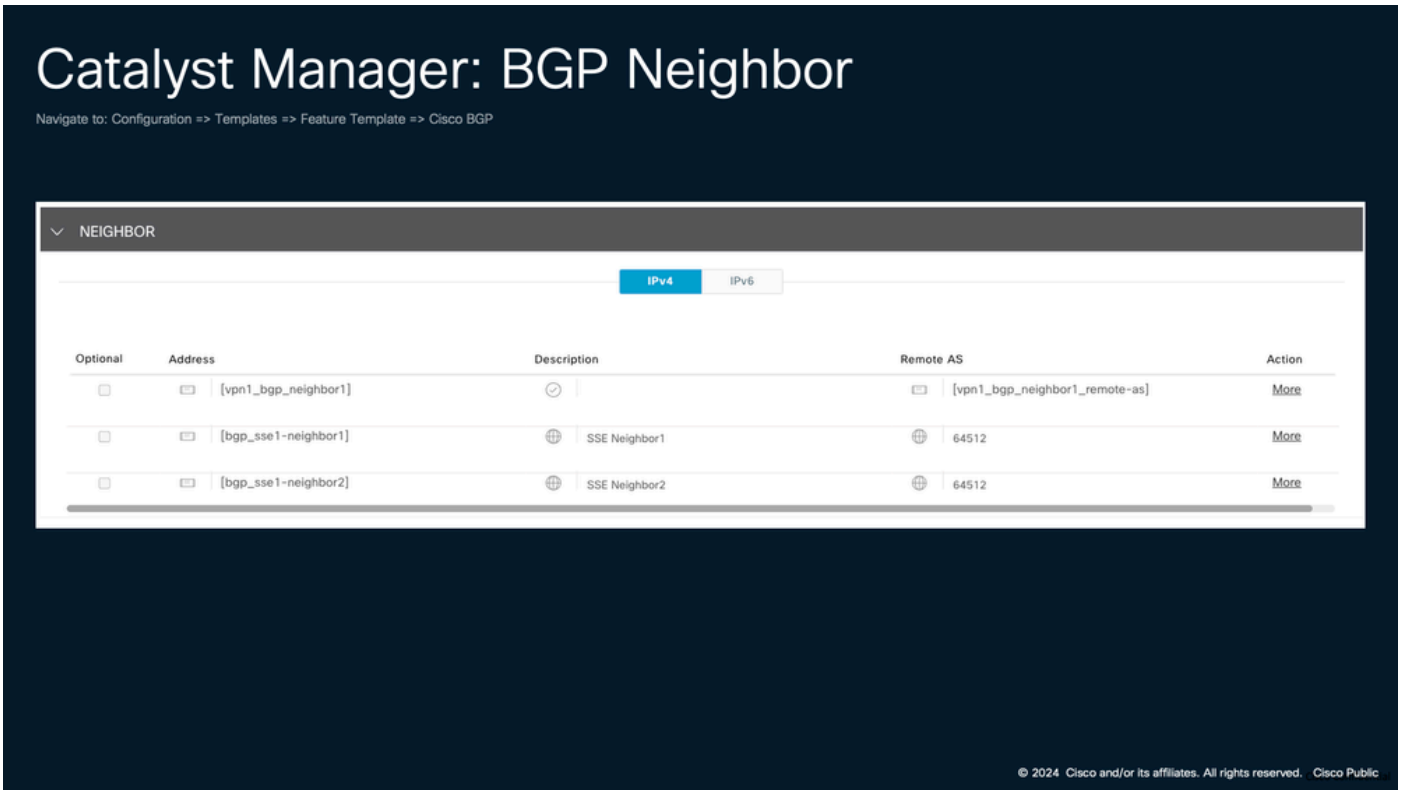
Figura 15: Secure Access Network Tunnel Group (Estados Unidos)



Secure Access Network Tunnel Group (Estados Unidos)

En este ejemplo, utilizamos la información de la Figura 15 (casilla 1) para definir BGP mediante una plantilla de función.

Figura 16: Catalyst SD-WAN Manager BGP Neighbor



Catalyst SD-WAN Manager BGP Neighbor

Configuración generada mediante la plantilla de función:

```
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#
```

Verificación

```
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
```

Referencia

Una implementación Activo/Activo tendría un trayecto múltiple desde el switch principal que está conectado a ambos centros distribuidores SD-WAN.

Figura 17: Escenario Activo/Activo para Vecino 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>
```

Vecino BGP Activo/Activo

Una implementación activa/en espera tendría una ruta activa desde el switch principal a los centros distribuidores de SD-WAN debido a la precedencia de ASPL (que se realiza mediante un mapa de ruta al vecino).

Figura 18: Escenario Activo/En Espera para el Vecino 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>
```

Vecino BGP activo/en espera

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).