Configurar a interconexão de aplicativos privada entre a borda do serviço de segurança e a SD-WAN USANDO o método manual

Contents

Introdução

Este documento descreve um guia abrangente para conectar o Cisco Secure Access com roteadores SD-WAN, com foco no acesso de aplicativo privado seguro.

Sobre este guia

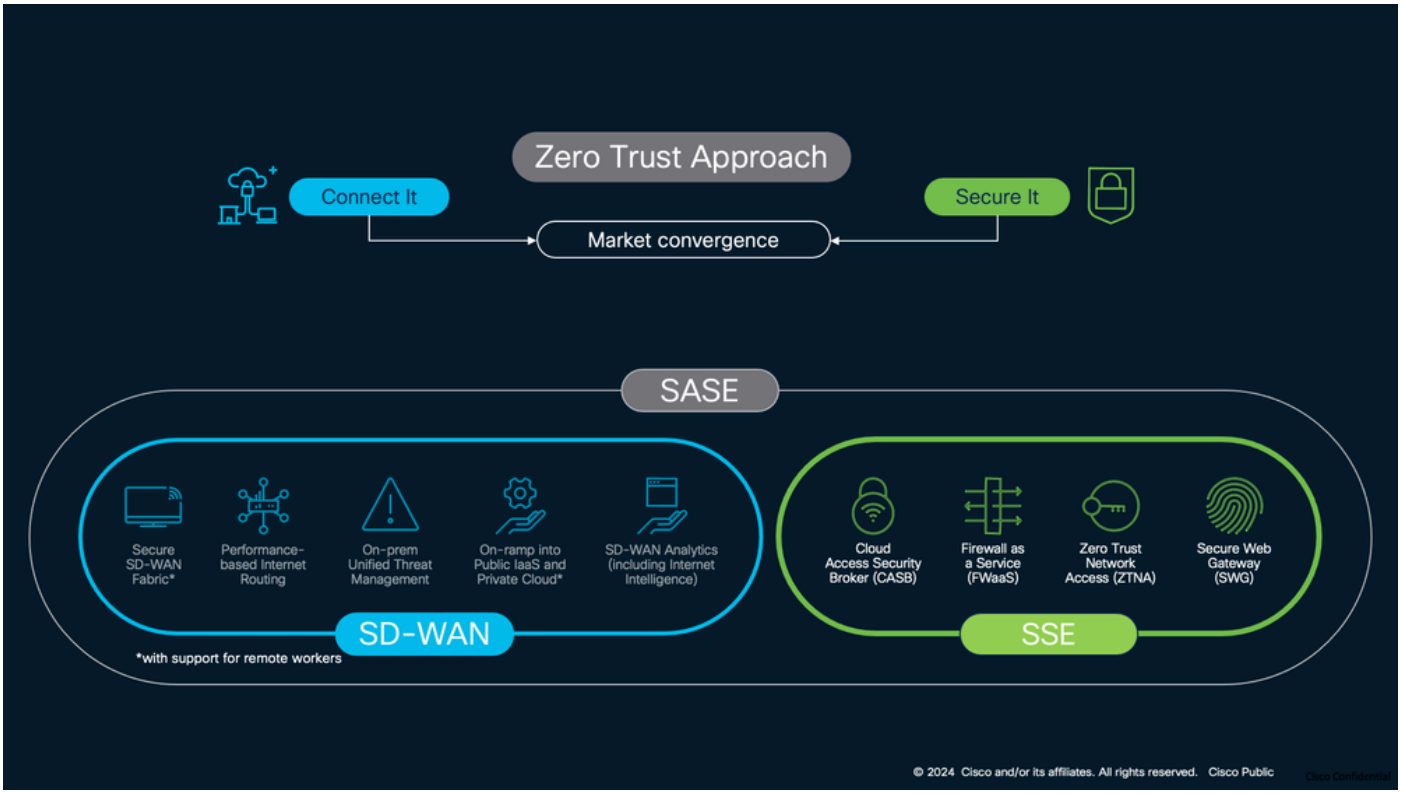
Observação: as configurações listadas aqui foram desenvolvidas para as versões UX1.0 e 17.9/20.9 do SD-WAN.

Este guia apresenta um passo a passo estruturado destas etapas principais:

- Definindo grupos de túneis de rede (NTGs)
- Configuração de túnel IPSec: Instruções detalhadas sobre a configuração de túneis IPSec seguros entre roteadores SD-WAN da Cisco e NTGs de acesso seguro da Cisco.
- Vizinhança de BGP: Procedimentos passo a passo para executar BGP Neighships nos túneis IPSec para garantir o roteamento dinâmico e a resiliência de rede melhorada.
- Acesso a aplicativos privados: Orientação sobre como configurar e proteger o acesso a

aplicativos privados através dos túneis estabelecidos.

Figura 1: Abordagem Cisco SD-WAN e SSE sem confiança



SSE com SD-WAN

Este guia se concentra na consideração do projeto e nas melhores práticas de implantação para interconexão NTG. Neste guia, os controladores SD-WAN são implantados na nuvem e os roteadores de borda da WAN são implantados no data center e conectados a pelo menos um circuito de Internet.

Principais premissas

- Cisco Secure Access Secure Service Edge (SSE): Supõe-se que o Cisco Secure Access SSE já esteja provisionado para a sua organização.
- Roteador de borda WAN Cisco SD-WAN: Supõe-se que o roteador de borda da WAN esteja integrado à rede de sobreposição, facilitando com eficiência o tráfego do usuário na infraestrutura de SD-WAN.
- Embora este guia se concentre principalmente nos aspectos de SD-WAN do design e da configuração, ele fornece uma abordagem holística para integrar as soluções Cisco Secure Access dentro da arquitetura de rede existente.

Sobre esta solução

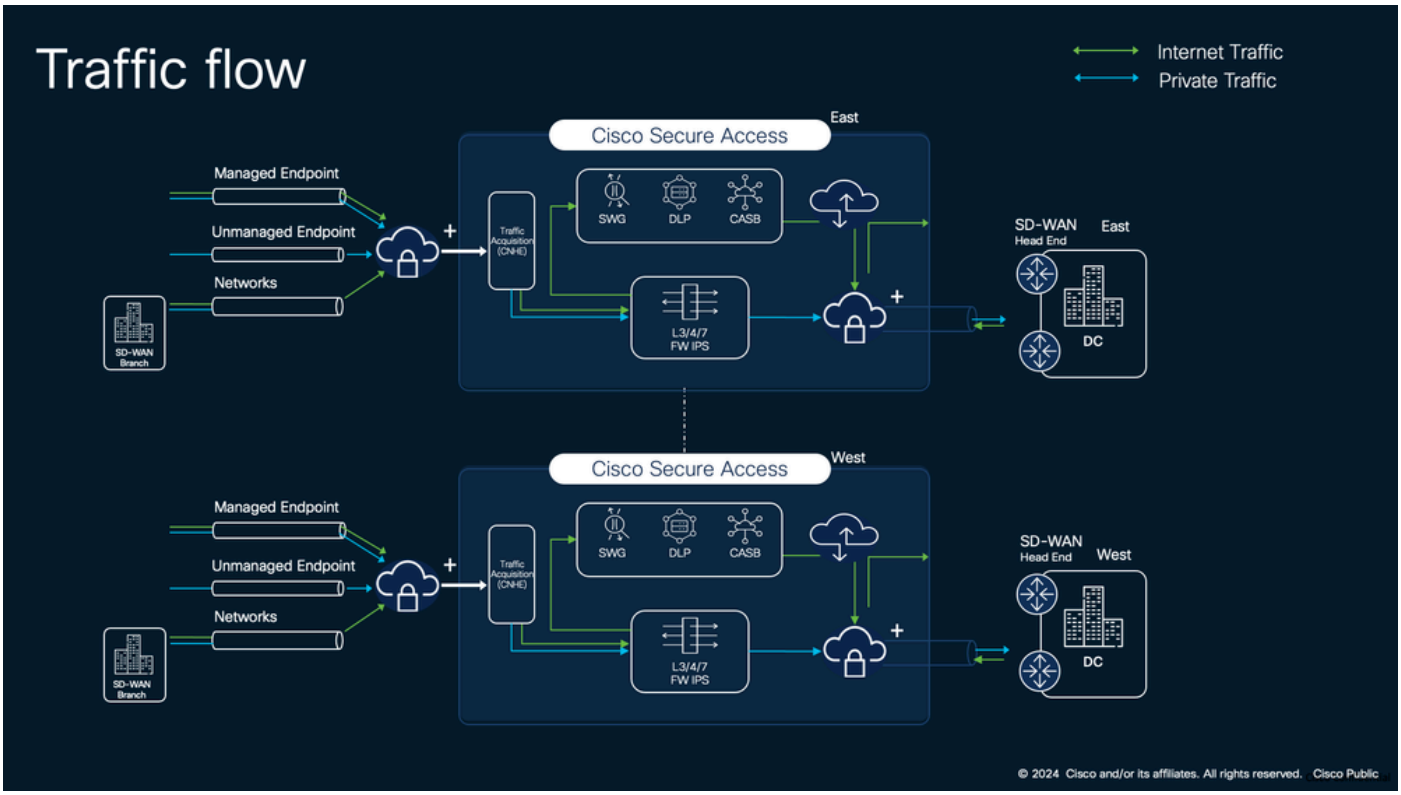
Túneis de aplicativos privados, oferecidos pelo Cisco Secure Access, fornecem conectividade segura a aplicativos privados para usuários que se conectam através do Zero Trust Network Access (ZTNA) e VPN as a Service (VPNaaS). Esses túneis permitem que as organizações vinculem com segurança usuários remotos a recursos privados hospedados em data centers ou

nuvens privadas.
Usando IKEv2 (Internet Key Exchange versão 2), esses grupos de túneis estabelecem conexões bidirecionais seguras entre os roteadores Cisco Secure Access e SD-WAN. Eles suportam alta disponibilidade através de vários túneis dentro do mesmo grupo e oferecem gerenciamento de tráfego flexível através de roteamento estático e dinâmico (BGP).
Os túneis IPsec podem transportar tráfego de várias fontes, incluindo:

- Usuários de VPN de acesso remoto
- Conexões ZTNA baseadas em navegador ou em cliente
- Outros locais de rede conectados ao Cisco Secure Access

Essa abordagem permite que as empresas roteiem com segurança todos os tipos de tráfego de aplicativos privados por meio de um canal unificado e criptografado, aumentando a segurança e a eficiência operacional.
O Cisco Secure Access, como parte da solução Cisco Security Service Edge (SSE), simplifica as operações de TI através de um único console gerenciado em nuvem, cliente unificado, criação centralizada de políticas e relatórios agregados. Ele incorpora vários módulos de segurança em uma solução oferecida em nuvem, incluindo ZTNA, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS), segurança DNS, Remote Browser Isolation (RBI) e muito mais. Essa abordagem abrangente reduz os riscos de segurança aplicando princípios de confiança zero e aplicando políticas de segurança granulares

Figura 2: Fluxo de tráfego entre o Cisco Secure Access e o aplicativo privado



Fluxo de Tráfego de Aplicativo Privado SSE

A solução descrita neste guia aborda considerações de redundância abrangentes, abrangendo o roteador SD-WAN no data center e o Network Tunnel Group (NTG) no lado do Security Service

Edge (SSE). Este guia se concentra em um modelo de implantação de hub SD-WAN ativo/ativo, que ajuda a manter o fluxo de tráfego ininterrupto e garante alta disponibilidade.

Pré-requisitos

Requisitos

Recomenda-se que você tenha conhecimento destes tópicos:

- Configuração e gerenciamento do Cisco SD-WAN
- Conhecimento básico dos protocolos IKEv2 e IPSec
- Configuração do Network Tunnel Group no portal Cisco Secure Access
- Conhecimento de BGP e ECMP

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Controladores Cisco SD-WAN em 20.9.5a
- Roteadores de borda WAN SD-WAN da Cisco na versão 17.9.5a
- Portal Cisco Secure Access

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Projeto

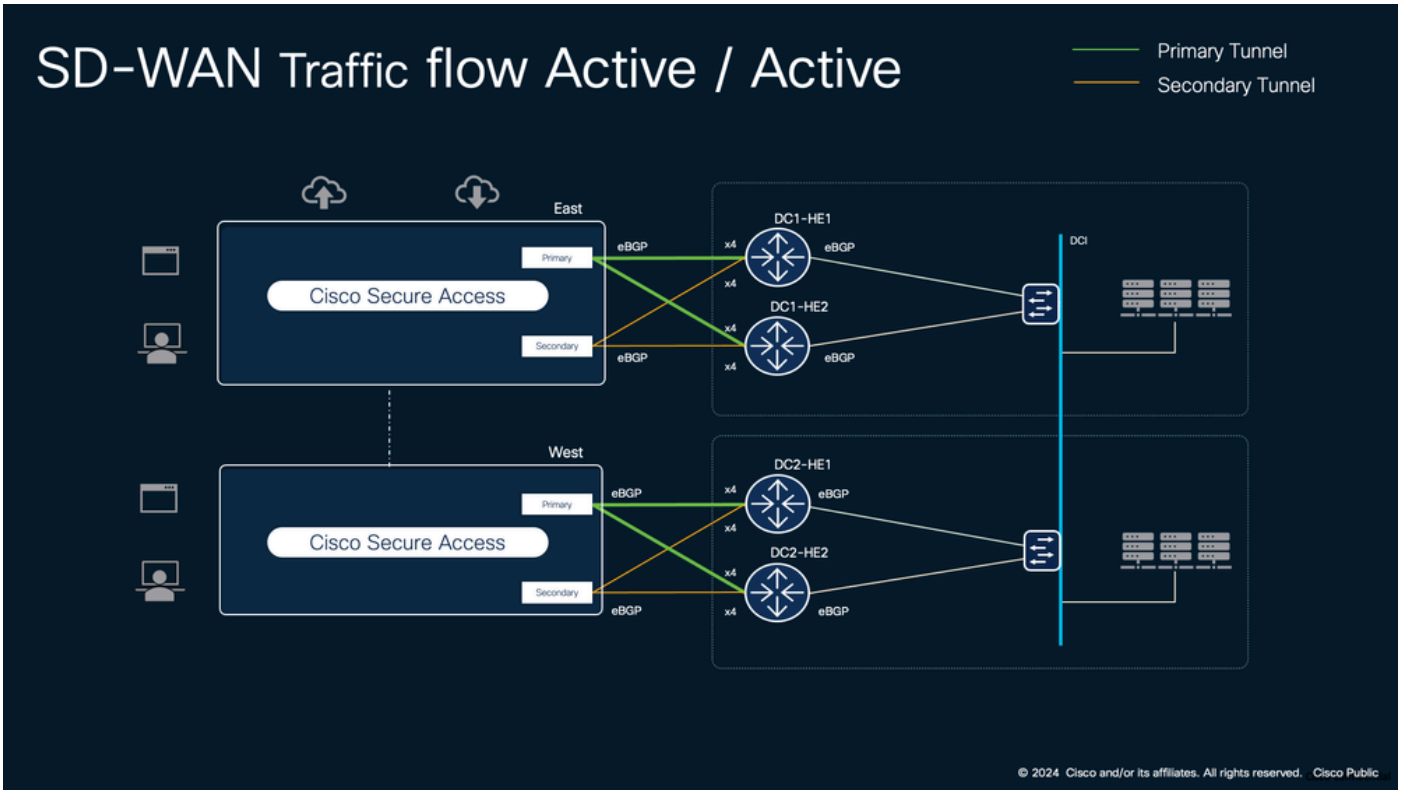
Este guia descreve a solução usando um modelo de design Ativo/Ativo para roteadores headend SD-WAN. Um modelo de design Ativo/Ativo no contexto de roteadores head-end de SD-WAN pressupõe dois roteadores em um data center, ambos conectados ao Grupo de Túnel de Rede (NTG) da Borda de Serviço de Segurança (SSE), como ilustrado na Figura 3. Neste cenário, ambos os roteadores SD-WAN no data center (DC1-HE1 e DC1-HE2) lidam ativamente com o fluxo de tráfego. Eles conseguem isso enviando o mesmo AS Path Length (ASPL) ao vizinho de DC interno. Como resultado, o tráfego de dentro do DC equilibra a carga entre os dois headends.

Cada roteador headend pode estabelecer vários túneis para Pontos de Presença (POPs) SSE. O número de túneis varia de acordo com seus requisitos e o modelo de dispositivo SD-WAN. Neste design:

- Cada roteador tem 4 túneis para o hub SSE primário e 4 túneis para o hub SSE secundário.
- O número máximo de túneis suportados por cada hub SSE pode variar. Para obter as informações mais atualizadas, consulte a documentação oficial: https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

Esses roteadores headend formam vizinhanças BGP sobre os túneis em direção ao SSE. Por meio dessas vizinhanças, os headends anunciam prefixos de aplicativos privados para seus vizinhos SSE, permitindo o roteamento seguro e eficiente do tráfego para recursos privados.

Figura 3: Modelo de implantação SD-WAN para SSE ativo/ativo



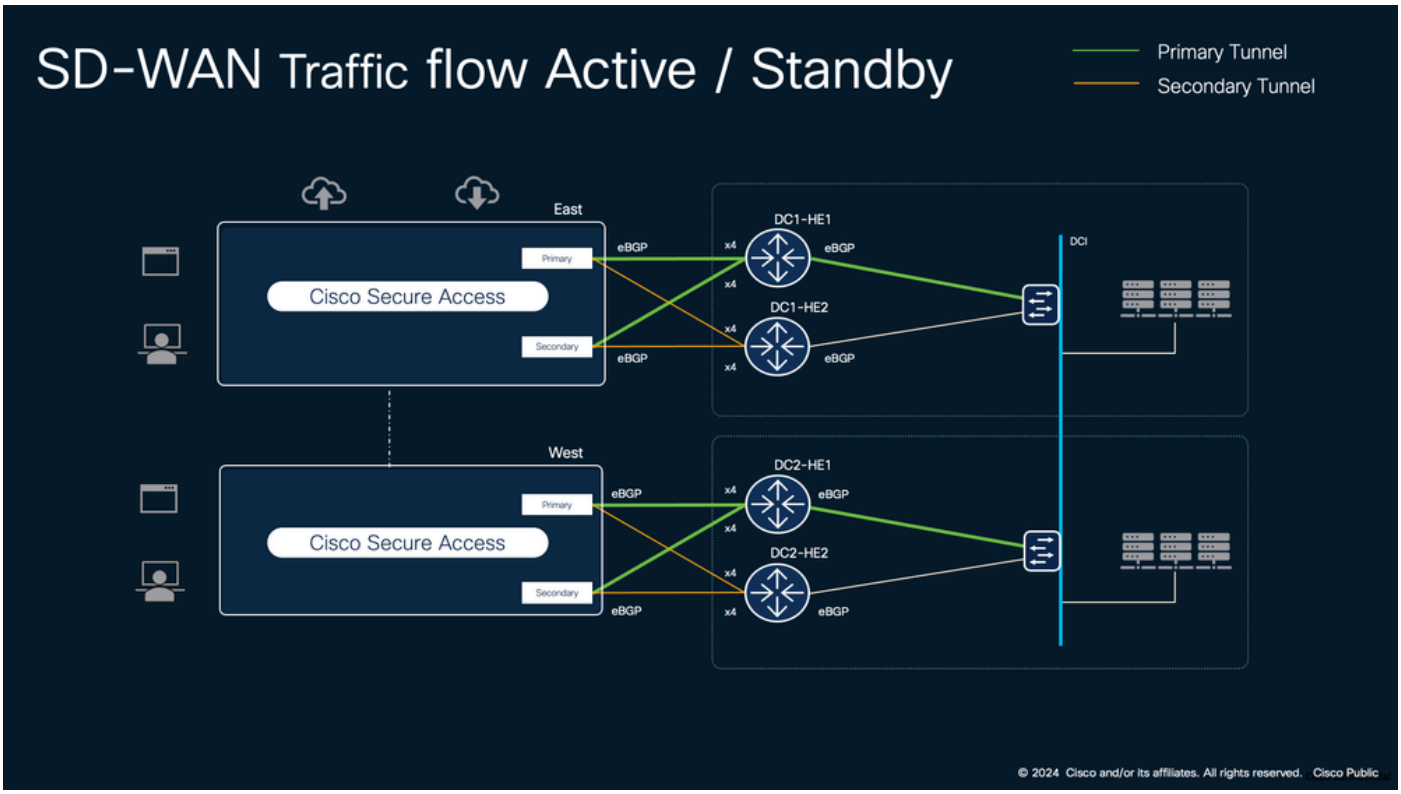
Modelo de implantação SD-WAN para SSE ativo/ativo

Um design Ativo/Em espera designa um roteador (DC1-HE1) como sempre ativo, enquanto o roteador secundário (DC1-HE2) permanece em espera. O tráfego flui consistentemente pelo headend ativo (DC1-HE1) a menos que ele falhe completamente. Esse modelo de implantação tem uma desvantagem: se o túnel principal para o SSE cair, o tráfego muda para os túneis SSE secundários que são somente via DC1-HE2, fazendo com que qualquer tráfego stateful seja redefinido.

No modelo Ativo/Standby, o BGP AS-Path Length é usado para direcionar o tráfego dentro do DC e em direção ao SSE. DC1-HE1 envia atualizações de prefixo ao vizinho BGP SSE com uma ASPL de 2, enquanto DC1-HE2 envia atualizações com uma ASPL de 3. O vizinho DC interno de DC1-HE1 anuncia prefixos com um comprimento de caminho AS mais curto que DC1-HE2, garantindo a preferência de tráfego para DC1-HE1. (Os clientes podem escolher outros atributos ou protocolos para influenciar a preferência de tráfego.)

Os clientes podem selecionar um modelo de implantação Ativo/Ativo ou Ativo/Em espera com base em seus requisitos específicos.

Figura 4: Modelo de implantação ativo/em espera de SD-WAN para SSE



Modelo de implantação ativo/em espera de SD-WAN para SSE

Configurar

Esta seção descreve o procedimento:

1. Verifique os pré-requisitos para provisionar um Network Tunnel Group no portal Cisco Secure Access.
2. Configure a interconexão SD-WAN com o Cisco Secure Access Network Tunnel Group (NTG) usando o método manual de IPsec.
3. Configurar vizinhança de BGP

Note: Essa configuração é baseada em um modelo de implantação Ativo/Ativo

---

Procedimento 1. Verificar a configuração do grupo de túneis de rede no Cisco Secure Access Portal

O guia não aborda como configurar o grupo de túneis de rede. Revise esta referência.

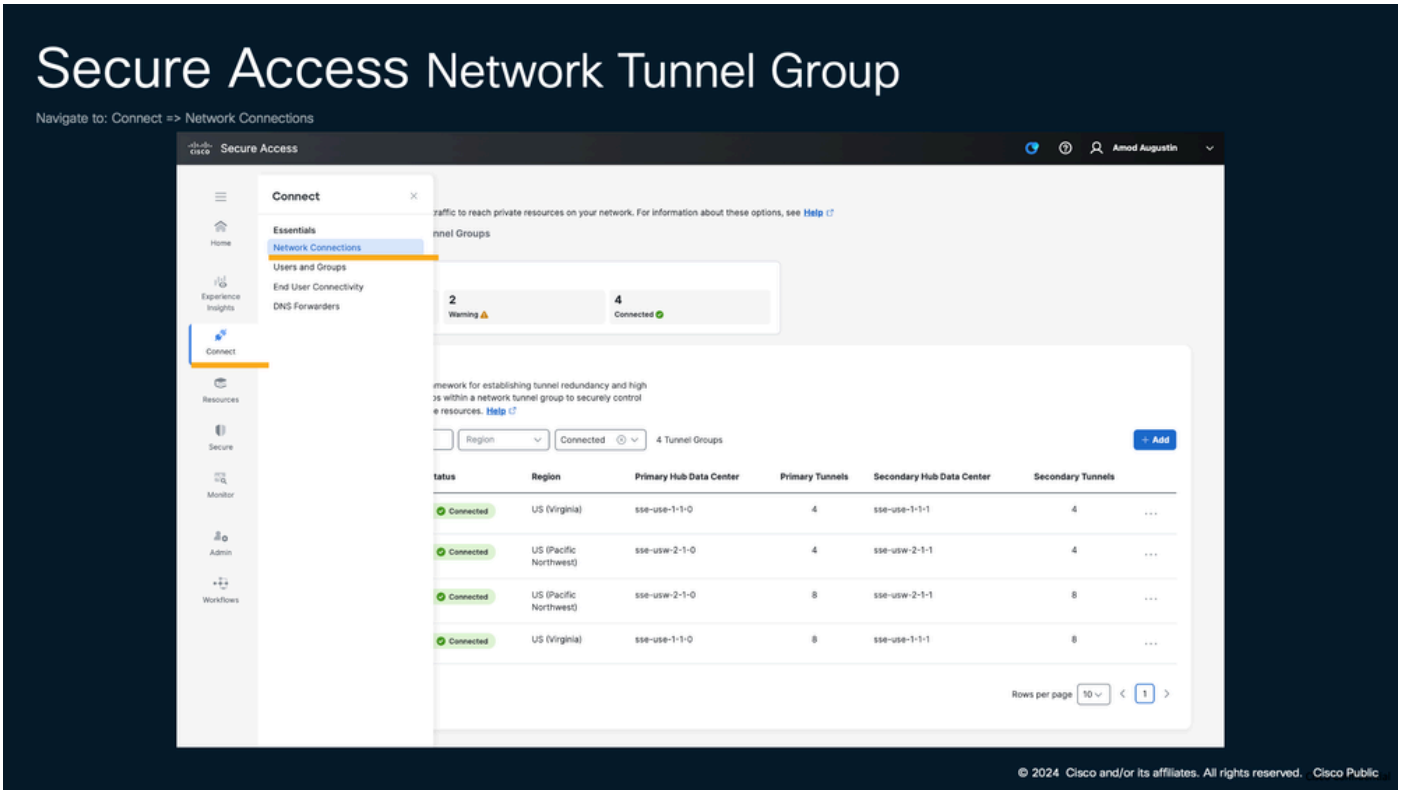
- Adicionar um grupo de túnel de rede: Documentação do SSE
- Configurar o túnel de rede entre o Cisco Secure Access e o roteador Cisco IOS XE usando ECMP com BGP

Navegue até Cisco Secure Access e verifique se os Network Tunnel Groups (NTGs) estão provisionados. Para o projeto atual, precisamos provisionar NTGs em dois Pontos de Presença (POPs) diferentes. Neste guia, usamos NTGs no US (Virginia) POP e US (Pacific Northwest)

POP.

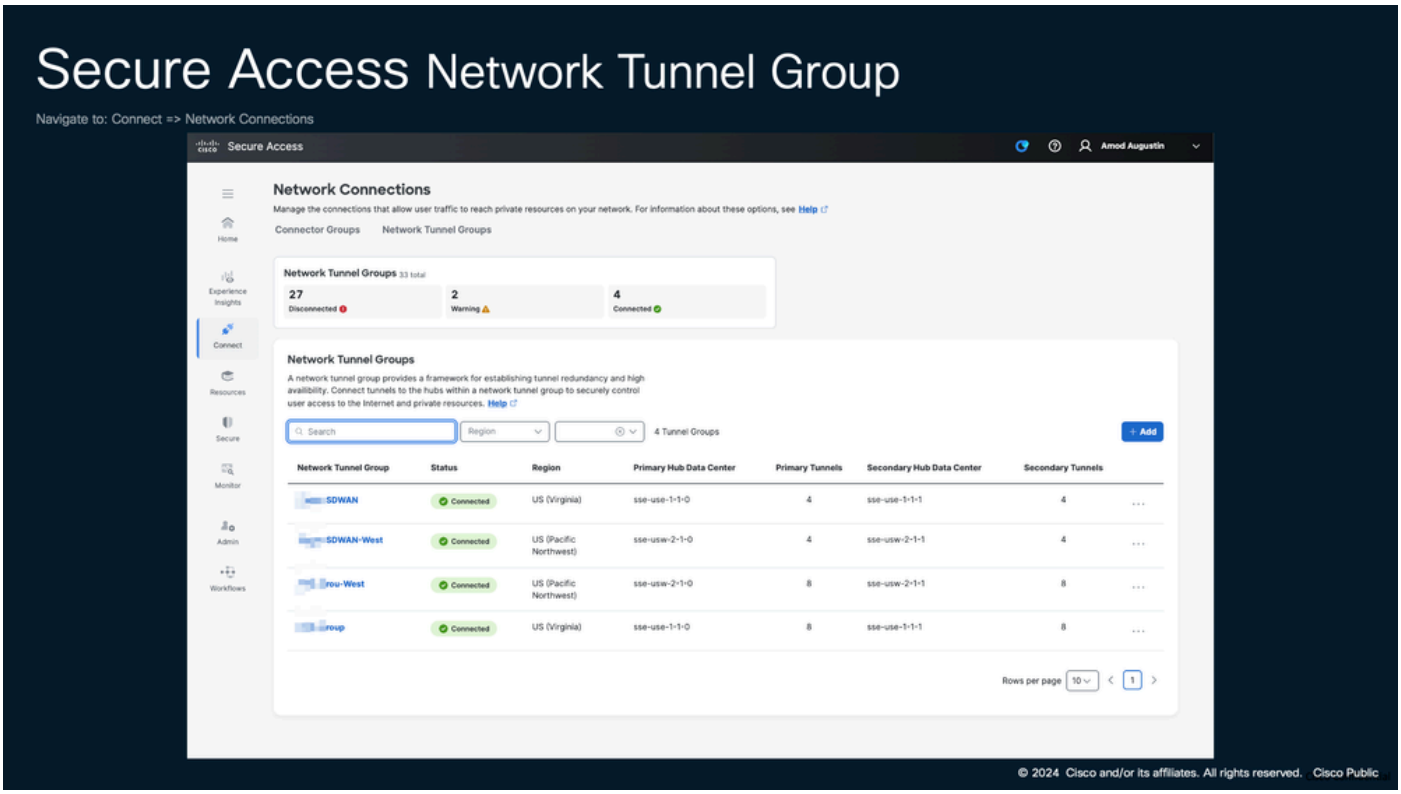
Nota:Os nomes e os locais dos POPs podem variar, mas o conceito-chave é ter vários NTGs provisionados em locais geograficamente próximos ao seu data center. Essa abordagem ajuda a otimizar o desempenho da rede e fornece redundância.

Figura 5: Grupo de Túnel de Rede de Acesso Seguro da Cisco



Grupo de Túnel de Rede de Acesso Seguro da Cisco

Figura 6: Lista de grupos de túneis de rede de acesso seguro da Cisco



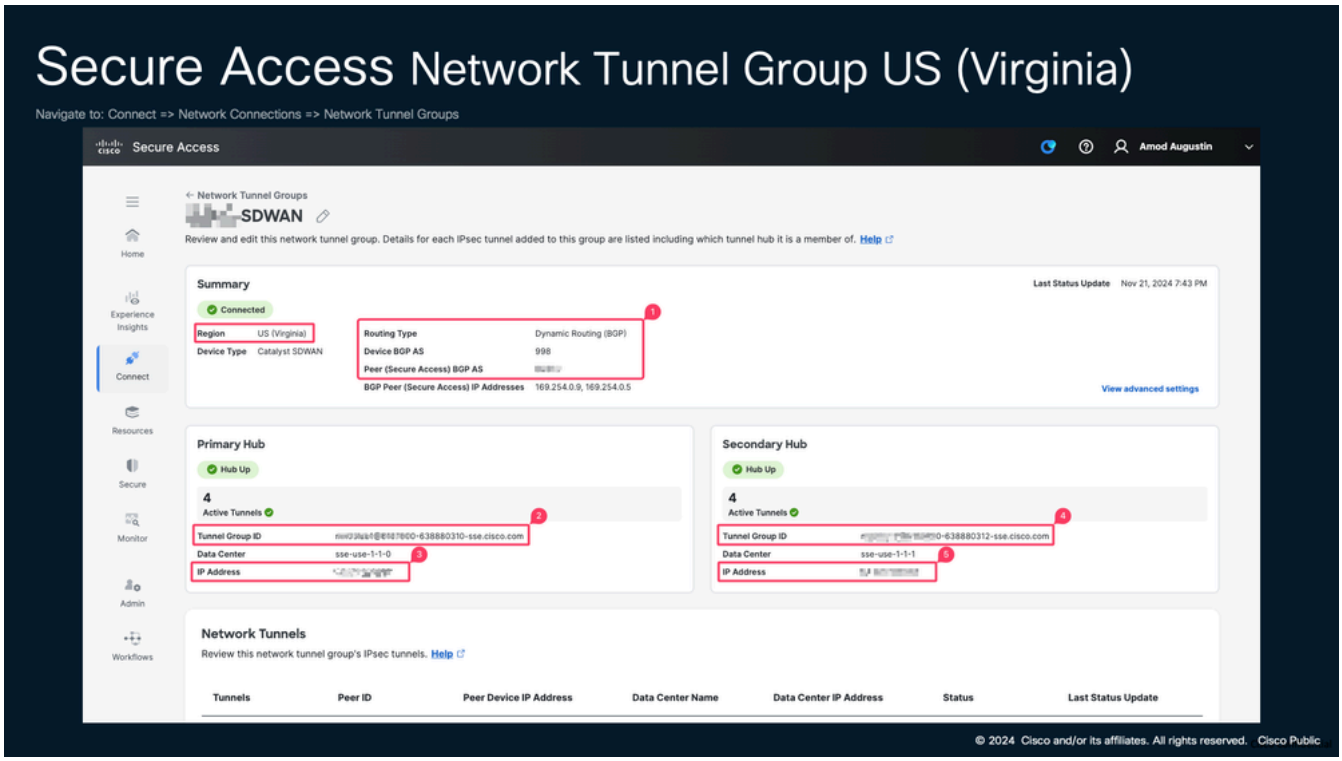
Lista de grupos de túneis de rede de acesso seguro

Certifique-se de anotar a frase secreta do túnel (que é mostrada apenas uma vez durante a criação do túnel).

Note: Etapa 6 em Adicionar um grupo de túneis de rede

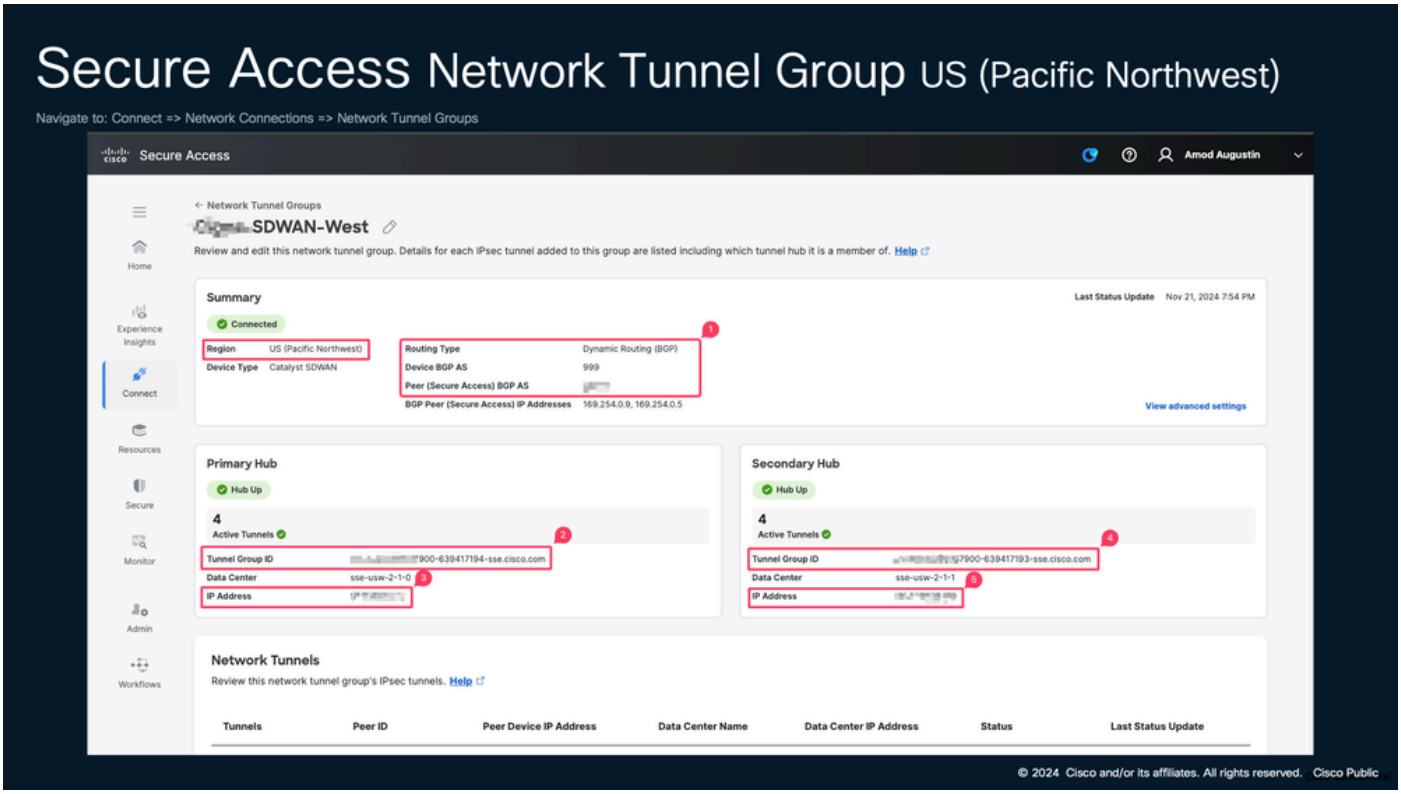
Anote também os atributos do grupo de túneis que usamos durante a configuração de IPSec. A captura de tela (Figura 6) é tirada de um ambiente de laboratório para um cenário de produção para criar grupos NTG de acordo com a recomendação de design ou uso.

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



Secure Access Network Tunnel Group EUA (Virgínia)

Figura 8: Secure Access Network Tunnel Group US (Pacífico Noroeste)



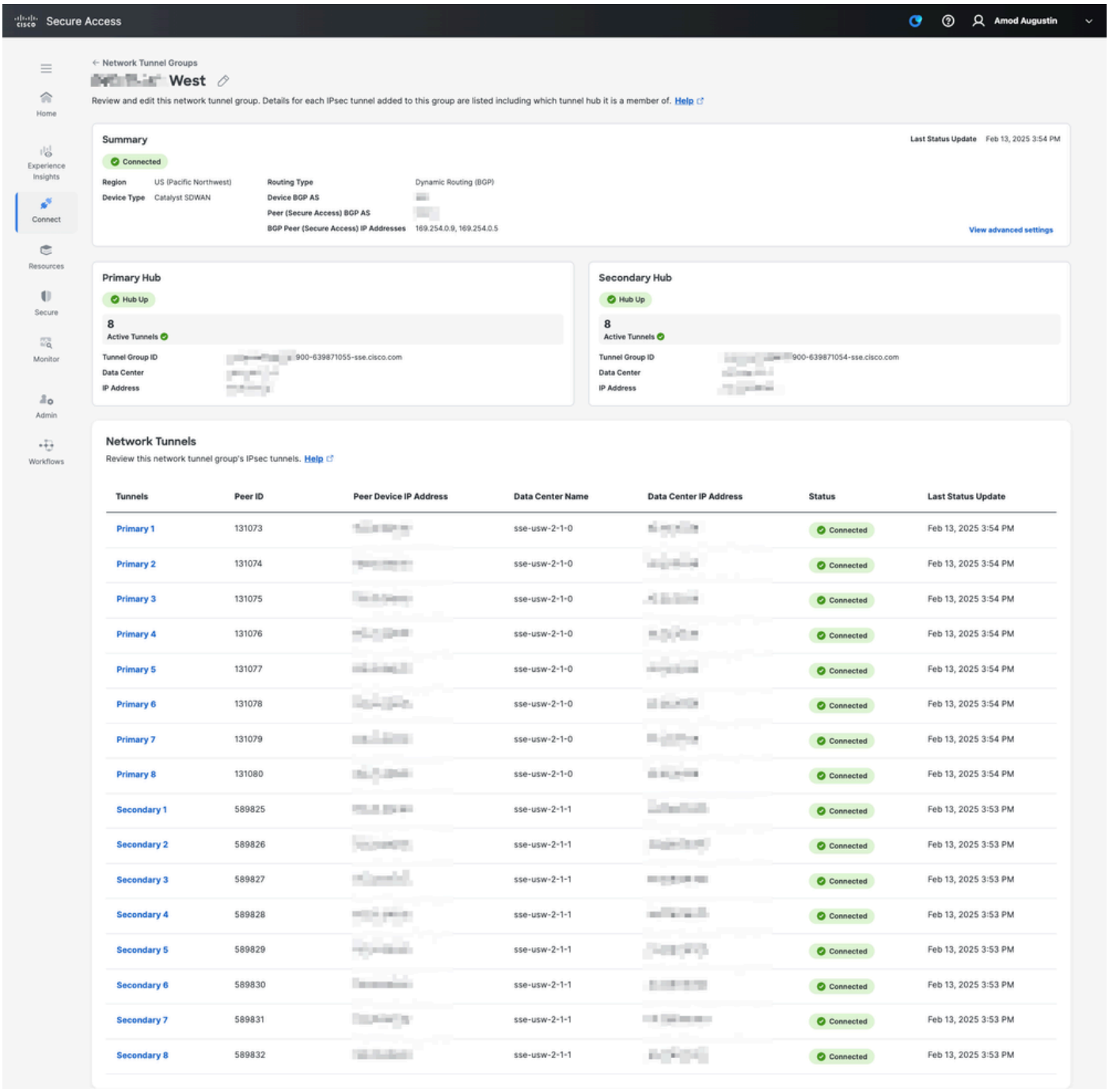
Secure Access Network Tunnel Group EUA (Pacífico Noroeste)

A figura 8 mostra apenas 4 túneis nos hubs principal e secundário. No entanto, um máximo de 8 túneis foi testado com êxito em um ambiente de controlador. O suporte de túnel máximo pode variar dependendo do dispositivo de hardware que você usa e do suporte de túnel SSE atual. Para obter as informações mais atualizadas, consulte a documentação oficial:

https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels e a nota de versão do respectivo dispositivo de hardware.

Um exemplo para uma configuração de 8 túneis é fornecido aqui.

Figura 8a: Túneis NTG com até 8 túneis



SSE NTG até 8 túneis

Procedimento 2. Configure a interconexão SD-WAN com o Cisco Secure Access Network Tunnel Group (NTG) usando o Método Manual de IPsec.

Este procedimento demonstra como conectar um Network Tunnel Group (NTG) usando modelos de recursos no Cisco Catalyst SD-WAN Manager 20.9 e no Cisco Catalyst Edge Router

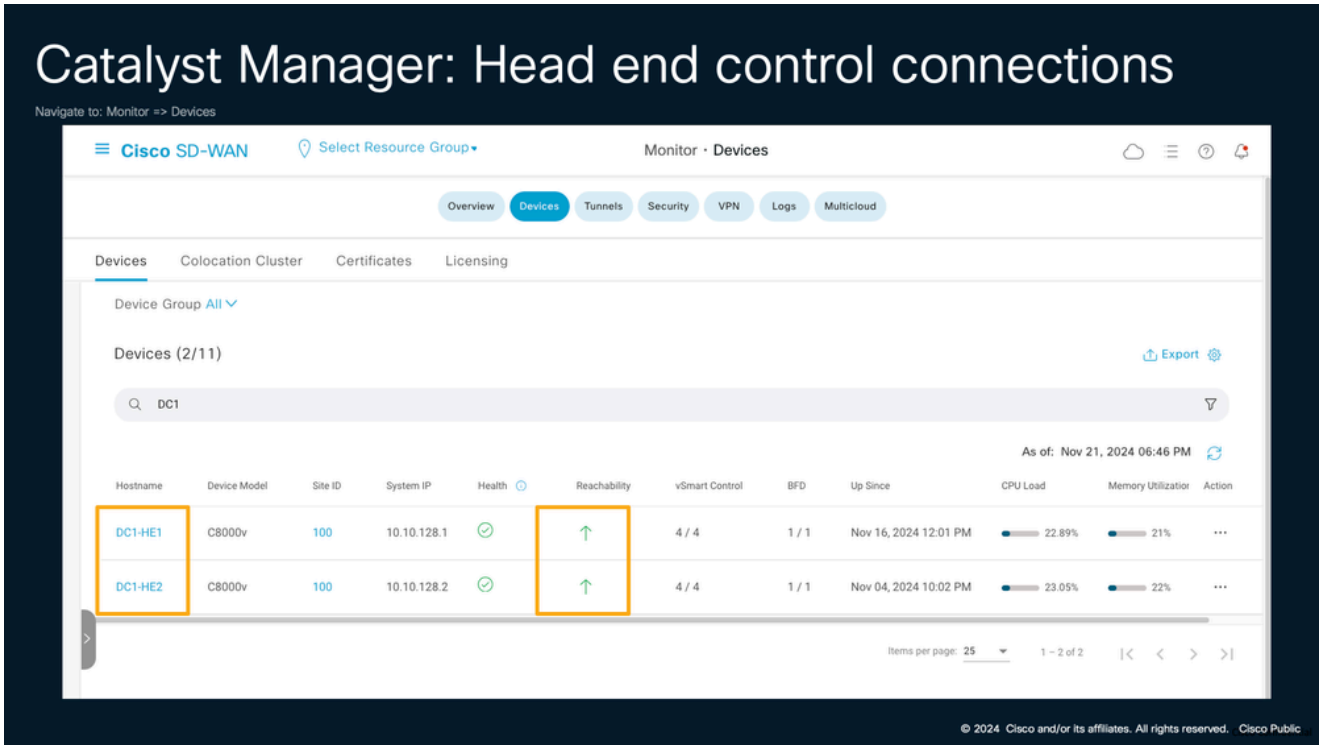
executando a versão 17.9.

Nota:Este guia pressupõe uma implantação de sobreposição de SD-WAN existente com uma topologia hub-and-spoke ou totalmente em malha, em que os hubs servem como pontos de entrada de acesso para aplicativos privados hospedados no data center. Esse procedimento também pode ser aplicado a implantações em filiais ou em nuvem.

Antes de continuar, verifique se os pré-requisitos foram atendidos:

1. As conexões de controle estão ativas no dispositivo para permitir as atualizações necessárias do Cisco Catalyst SD-WAN Manager.

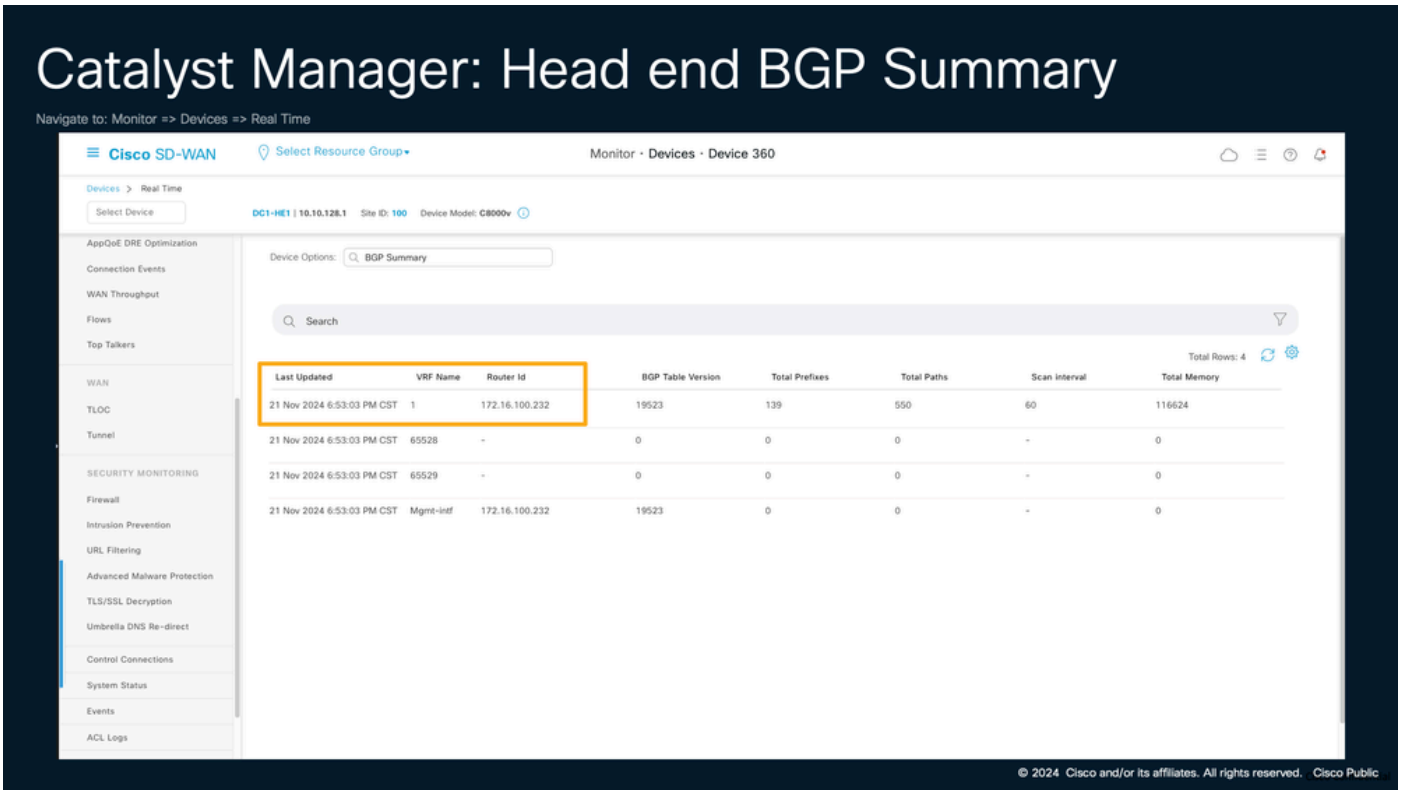
   Figura 9: Cisco Catalyst SD-WAN Manager: Conexões de controle da extremidade principal



Gerenciador Catalyst: Conexões de controle da extremidade principal

2. As VPNs do lado do serviço são configuradas e usam um protocolo de roteamento para anunciar prefixos. Este guia usa o BGP como o protocolo de roteamento no lado do serviço.

Figura 10: Cisco Catalyst SD-WAN Manager: Resumo do BGP da extremidade principal



Para configurar a interconexão SD-WAN com o Network Tunnel Group (NTG) usando o método IPSec manual, siga estas etapas:

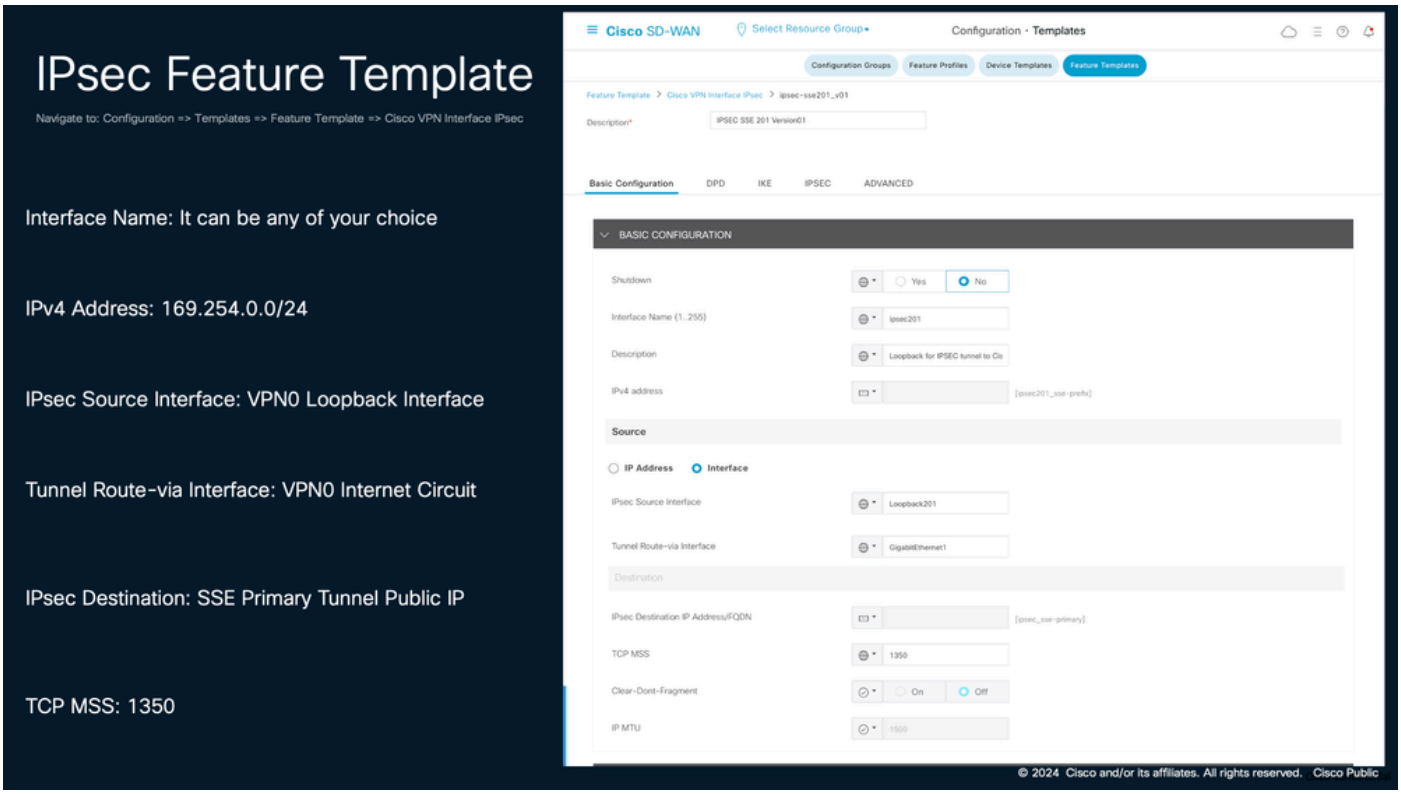
Note: Repita essa etapa para o número necessário de túneis para a implantação.

Consulte a documentação oficial para obter informações sobre a limitação de túnel: https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

Estas etapas detalham o processo para conectar DC1-HE1 (Data Center 1 Head-End 1) ao hub principal do SSE Virginia. Essa configuração estabelece um túnel seguro entre o roteador SD-WAN no data center e o Cisco Secure Access Network Tunnel Group (NTG) localizado no Ponto de Presença da Virgínia (POP)

Passo 1: Criar modelo de recurso IPSec
Crie um IPSec Feature Template para definir os parâmetros do túnel IPSec que conecta o roteador headend da SD-WAN ao NTG.

Figura 11: Modelo de recurso IPsec: Configuração básica



Modelo de recurso IPsec: Configuração básica

Nome da interface: Pode ser qualquer uma de sua escolha
Endereço IPv4: O SSE escuta 169.254.0.0/24 com base no requisito de que você pode dividir a sub-rede à sua escolha, como prática recomendada, use com /30. Neste guia, deixamos de fora o primeiro bloco para uso futuro.

Interface de origem IPsec: Defina uma Interface de Loopback VPN0 exclusiva para a interface IPsec atual. Para fins de consistência e solução de problemas, é recomendável manter a mesma numeração.
Rota de túnel via interface: Aponte a interface que pode ser usada como base para acessar o SSE (deve ter acesso à Internet)

Destino IPsec: Endereço IP do Hub Principal

Consulte a Figura 7: Secure Access Network Tunnel Group US (Virginia) - este é 35.171.214.188

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

Exemplo: DC1-HE1 em direção ao hub principal SSE Virginia

Nome da interface: IPSec201

Descrição: Loopback para túnel IPSEC para Cisco

Endereço IPv4: 169.254.0.x/30

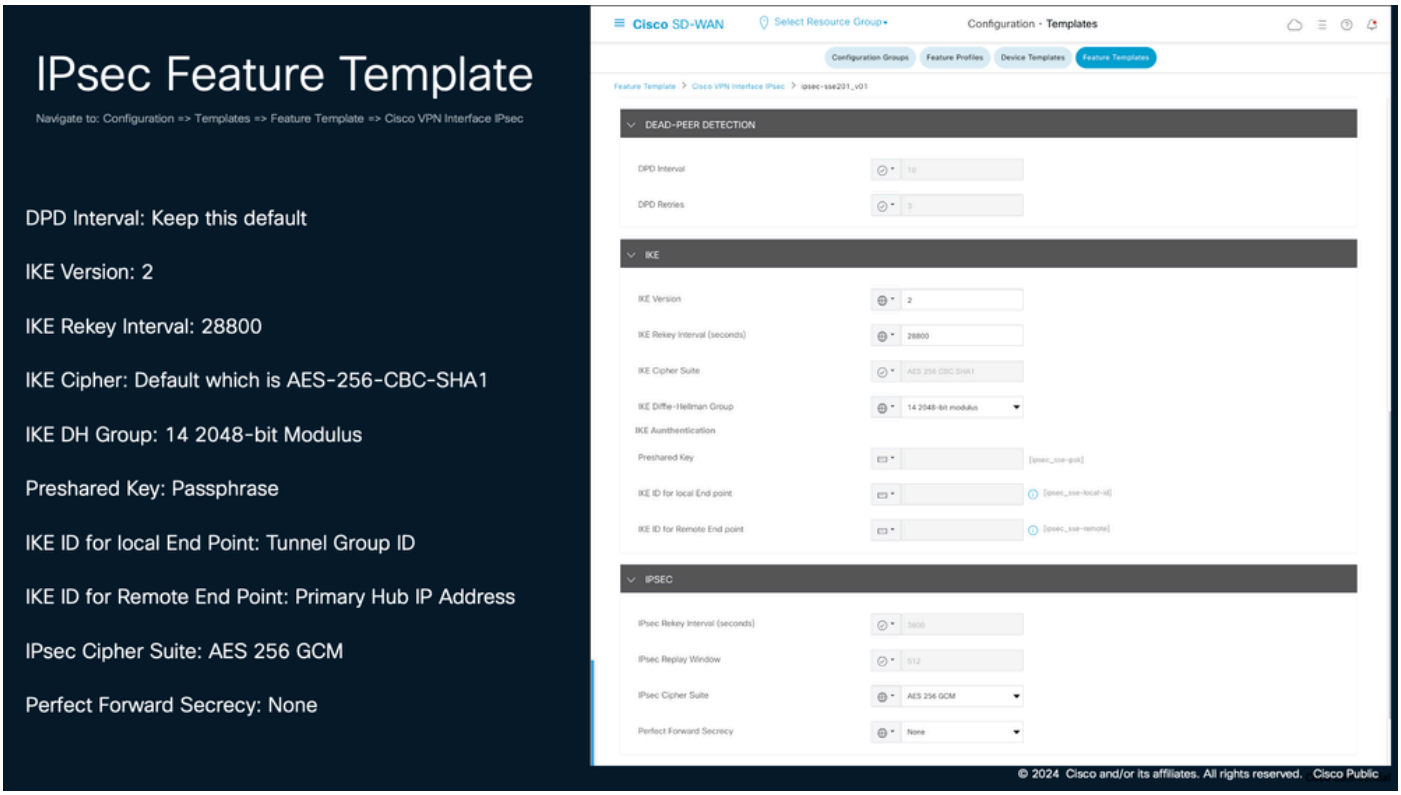
Interface de origem IPsec: Loopback201

Rota de túnel via interface: GigabitEthernet1

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

MSS TCP: 1350

Figura 12: Modelo de recurso IPsec: IKE IPSEC



Modelo de recurso IPsec: IKE IPSEC

Intervalo DPD: Manter este padrão
Versão do IKE: 2
Intervalo de rechaveamento IKE: 28800
Cifra IKE: O padrão é AES-256-CBC-SHA1
Grupo DH do IKE: Módulo de 14 2048 bits
Chave pré-compartilhada: Senha
ID do IKE para o ponto de extremidade local: ID do grupo de túneis

Consulte a Figura 7: Secure Access Network Tunnel Group US (Virginia) Este é mn03lab1+201@8167900-638880310-sse.cisco.com

---

Note: Cada túnel deve ter um Endpoint exclusivo para isso; use "+loopbackID" Exemplo: mn03lab1+202@8167900-638880310-sse.cisco.com, mn03lab1+203@8167900-638880310-sse.cisco.com, etc.

ID de IKE para ponto de extremidade remoto: Endereço IP do Hub Principal
Pacote de criptografia IPsec: AES 256 GCM

Segredo perfeito para o futuro: Nenhum

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

Exemplo:

Versão do IKE: 2
Intervalo de rechaveamento IKE: 28800
Cifra IKE: AES-256-CBC-SHA1
Grupo DH do IKE: Módulo de 14 2048 bits
Chave pré-compartilhada: *****

Note: Etapa 6 em Adicionar um grupo de túneis de rede

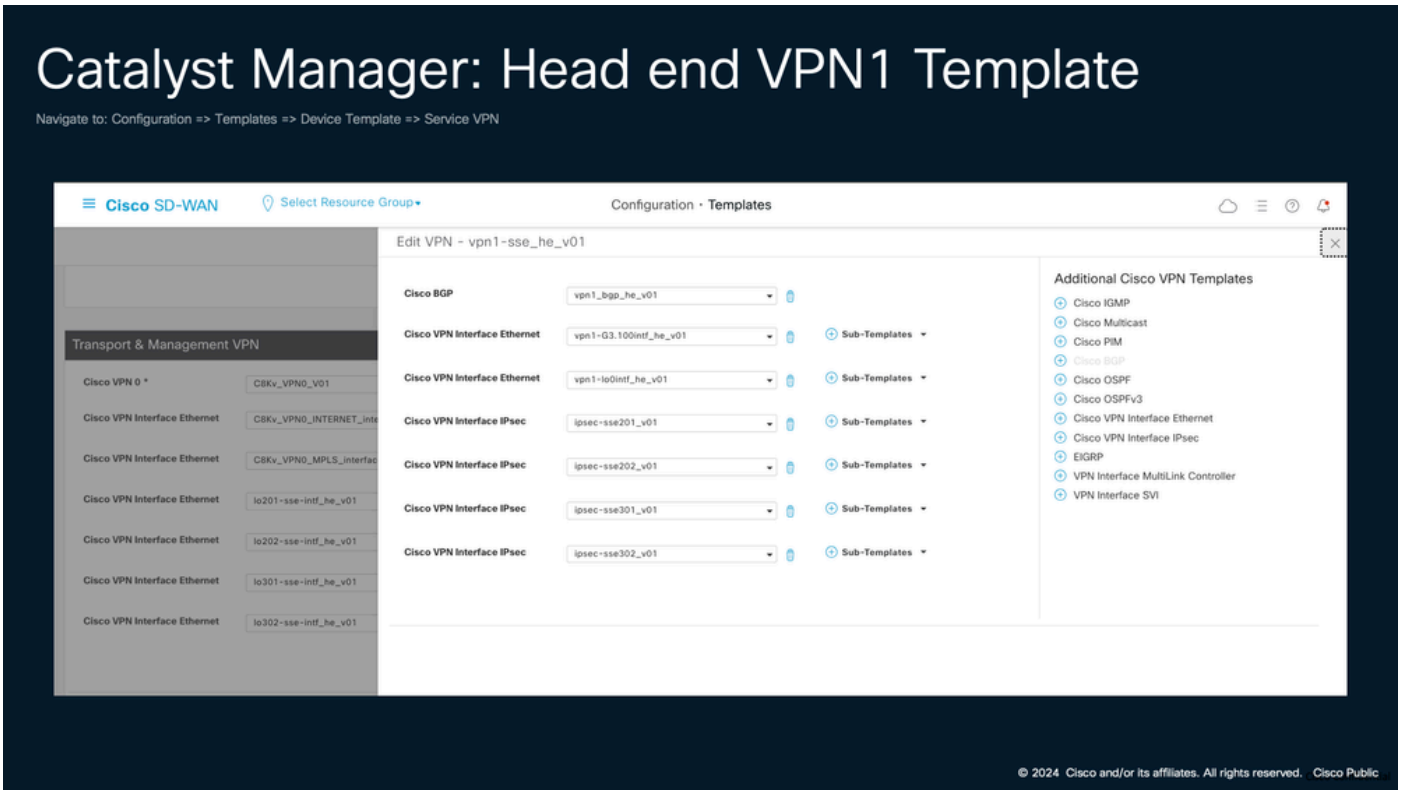
ID do IKE para o ponto de extremidade local: mn03lab1@8167900-638880310-sse.cisco.com
ID do IKE para ponto de extremidade remoto: 35.171.xxx.xxx
Pacote de criptografia IPsec: AES 256 GCM
Segredo perfeito para o futuro: Nenhum

Repita as etapas para configurar os túneis necessários para os hubs de acesso seguro primário e secundário.Para uma configuração 2x2, você criaria quatro túneis no total:

- Dois túneis de DC1-HE1 para o hub de acesso seguro primário
- Dois túneis de DC1-HE1 para o hub de acesso seguro secundário

Agora que os modelos são criados, nós os usaríamos no lado do serviço vrf show na figura 13 e o loopback definido anexado no vrf global mostrado na figura 14.

Figura 13: Catalyst SD-WAN Manager: Modelo 2x2 de VPN1 de headend



Gerenciador Catalyst: Modelo de VPN1 de headend

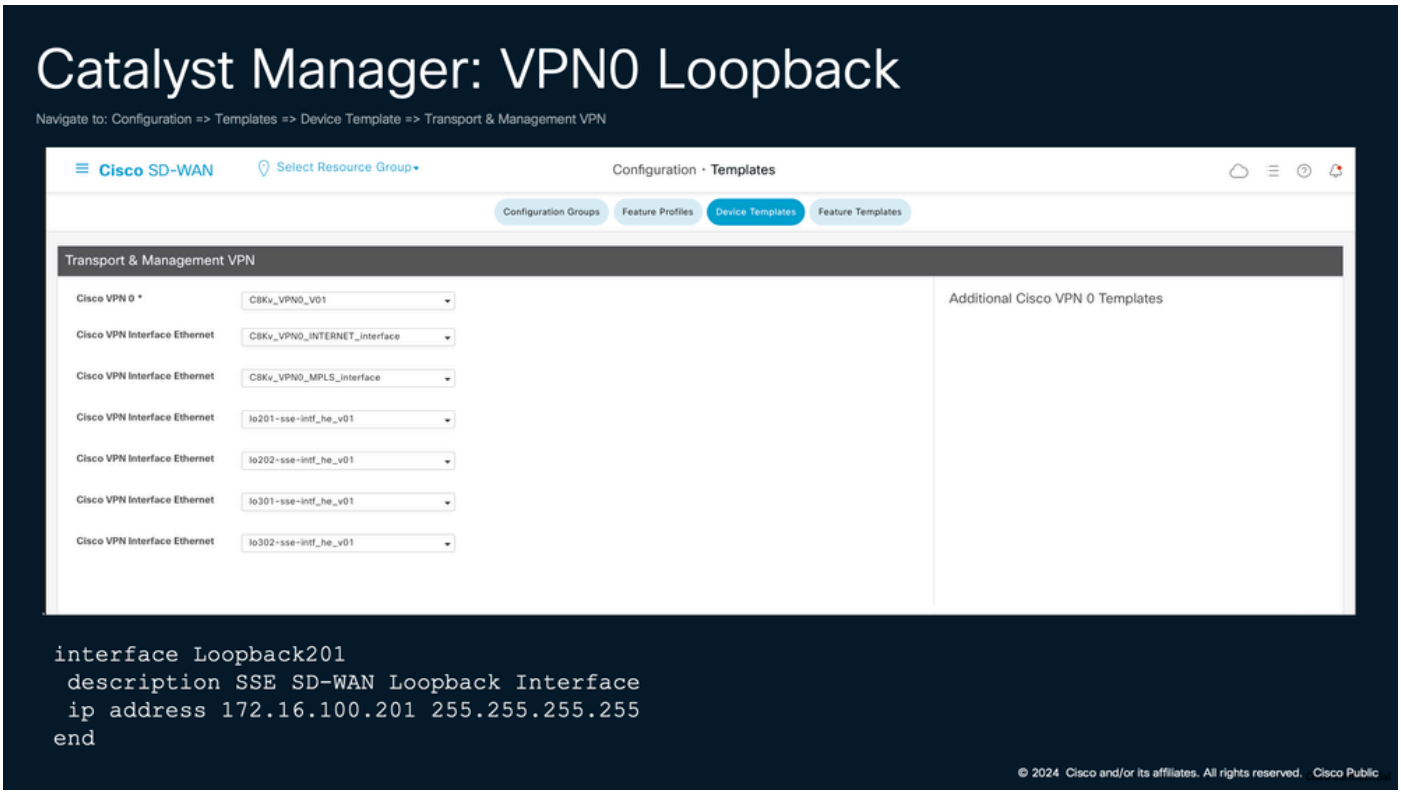
Passo 2: Defina o loopback no VRF global

Configure uma interface de loopback na tabela VRF (Virtual Routing and Forwarding) global. Esse loopback serve como a interface de origem para o túnel IPSec criado na Etapa 1.

Todo o loopback mencionado na Etapa 1 deve ser definido no Global VRF.

O endereço IP pode ser definido em qualquer intervalo RFC1918.

Figura 14: Catalyst SD-WAN Manager: Loopback de VPN0

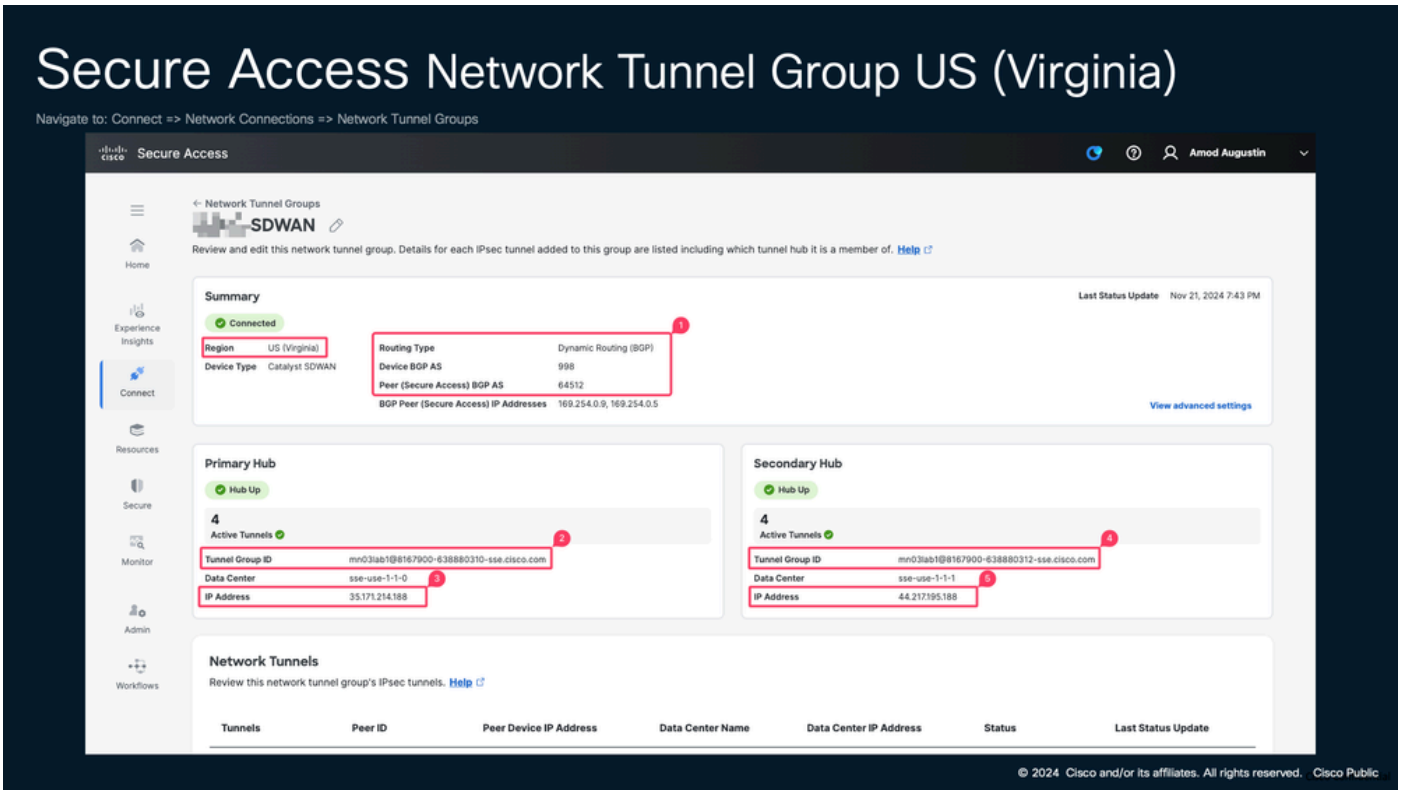


Gerenciador Catalyst: Loopback de VPN0

Procedimento 3. Configurar a vizinhança do BGP

Use o modelo de recurso BGP para definir a vizinhança BGP para todas as interfaces de túnel. Consulte a respectiva configuração de BGP dos grupos de túnel de rede no portal de acesso seguro da Cisco para configurar os valores de BGP.

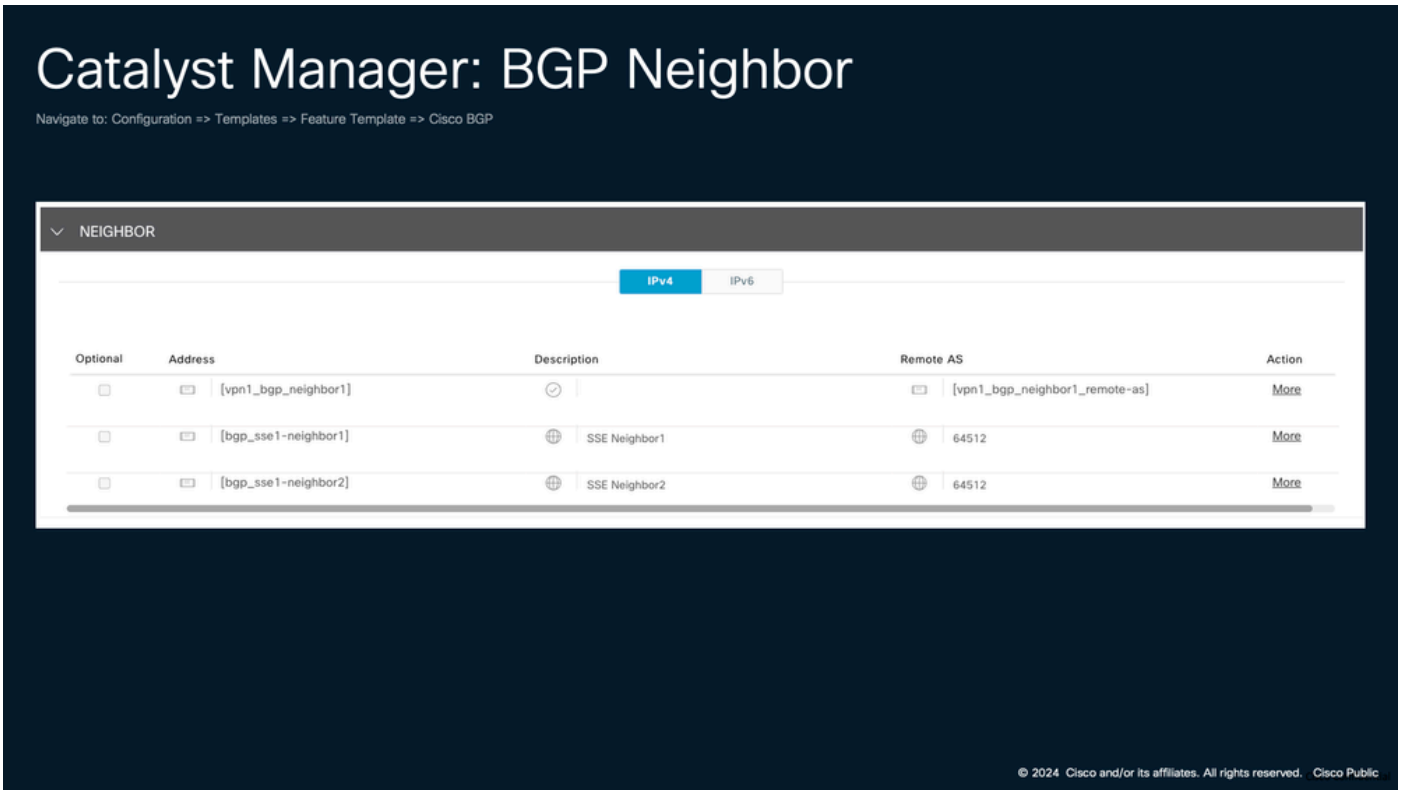
Figura 15: Secure Access Network Tunnel Group EUA (Virgínia)



Secure Access Network Tunnel Group EUA (Virgínia)

Neste exemplo, usamos as informações da Figura 15 (caixa 1) para definir o BGP usando um modelo de recurso.

Figura 16: Vizinho BGP do gerenciador de SD-WAN do Catalyst



Vizinho BGP do gerenciador de SD-WAN do Catalyst

Configuração gerada usando o modelo de recurso:

```
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#
```

Verificação

```
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
```

Referência

Uma implementação Ativa/Ativa teria um multipath do switch central que é conectado a ambos os headends da SD-WAN.

Figura 17: Cenário Ativo/Ativo para Vizinho 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>
```

Vizinho BGP ativo/ativo

Uma implementação Ativa/Em espera teria um caminho ativo do switch central para os headends da SD-WAN devido à pré-conexão ASPL (que é feita usando um mapa de rota para o vizinho).

Figura 18: Cenário ativo/em espera para vizinho 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>
```

Vizinho de BGP ativo/em standby

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.