Configurer l'interconnexion d'applications privées entre la périphérie du service de sécurité et le SD-WAN à l'AIDE de la méthode manuelle

Table des matières

Introduction

Ce document décrit un guide complet pour la connexion de Cisco Secure Access avec des routeurs SD-WAN, en se concentrant sur l'accès sécurisé aux applications privées.

À propos de ce guide

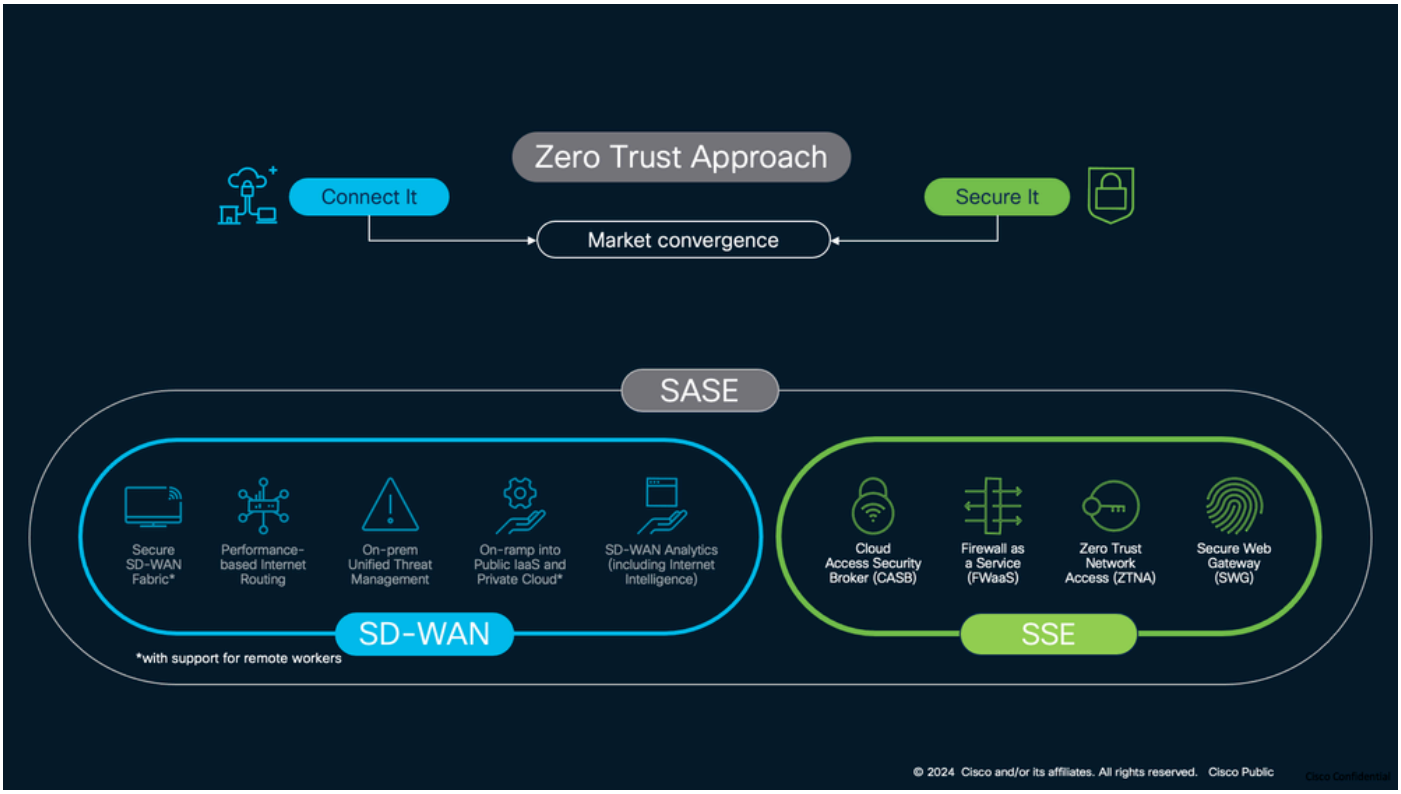
Remarque : les configurations répertoriées ici sont développées pour les versions UX1.0 et 17.9/20.9 de SD-WAN.

Ce guide présente une présentation structurée des étapes clés suivantes :

- Définition des groupes de tunnels réseau (NTG)
- Configuration du tunnel IPSec : Instructions détaillées sur la configuration de tunnels IPSec sécurisés entre les routeurs Cisco SD-WAN et les NTG Cisco Secure Access.
- Voisinage BGP : Procédures pas à pas pour l'exécution de voisins BGP sur les tunnels IPSec afin de garantir un routage dynamique et une meilleure résilience du réseau.
- Accès aux applications privées : Conseils sur la configuration et la sécurisation de l'accès

aux applications privées via les tunnels établis.

Figure 1 : Approche Cisco SD-WAN et SSE Zero Trust



SSE avec SD-WAN

Ce guide porte sur les considérations de conception et les meilleures pratiques de déploiement pour l'interconnexion NTG. Dans ce guide, les contrôleurs SD-WAN sont déployés dans le cloud et les routeurs de périphérie WAN sont déployés dans le data center et sont connectés à au moins un circuit Internet.

Hypothèses clés

- Cisco Secure Access Secure Service Edge (SSE) : Nous supposons que Cisco Secure Access SSE est déjà provisionné pour votre entreprise.
- Routeur de périphérie WAN SD-WAN Cisco : Le routeur de périphérie WAN est supposé être intégré au réseau de superposition, facilitant ainsi efficacement le trafic utilisateur sur l'infrastructure SD-WAN.
- Bien que ce guide se concentre principalement sur les aspects SD-WAN de la conception et de la configuration, il propose une approche holistique de l'intégration des solutions Cisco Secure Access dans votre architecture réseau existante.

À propos de cette solution

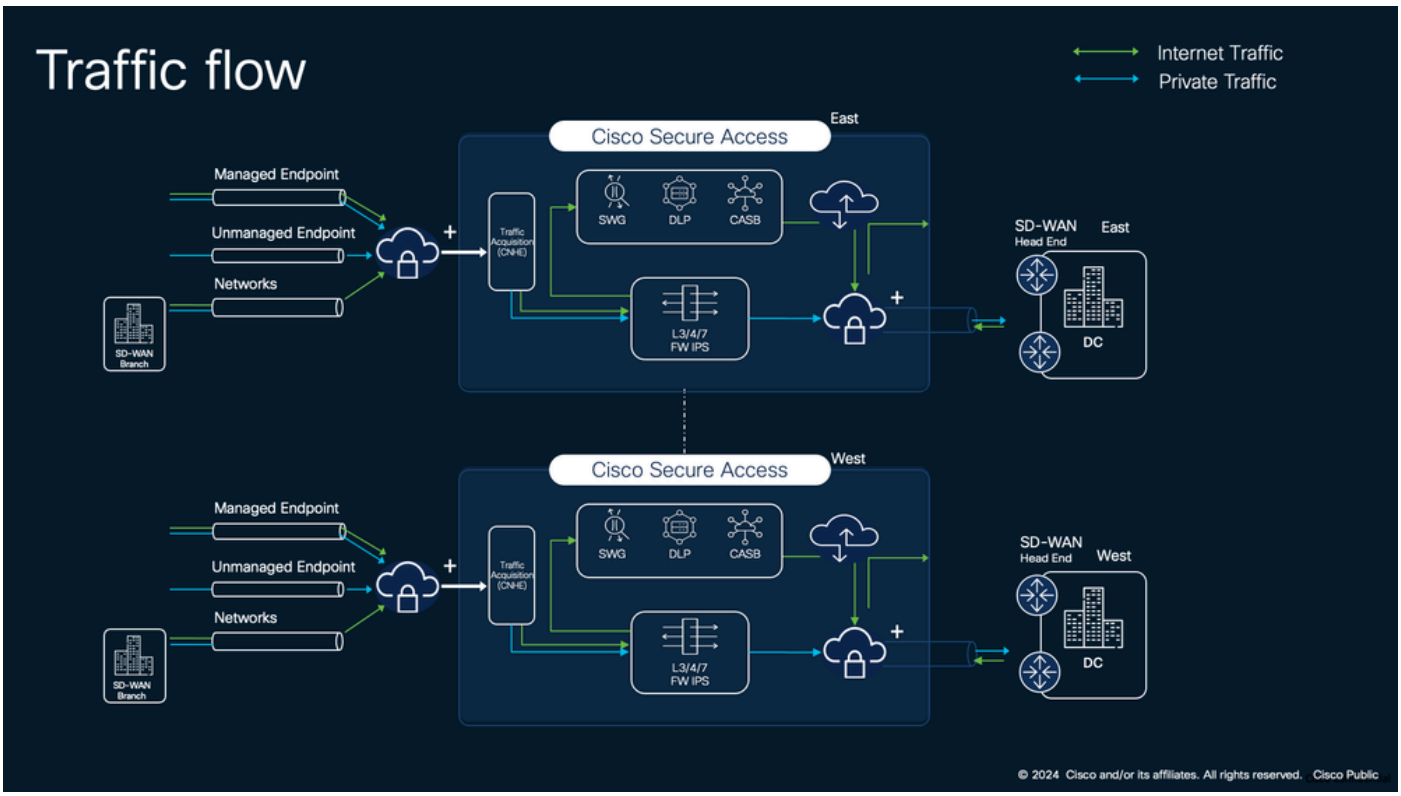
Les tunnels d'applications privées, proposés par Cisco Secure Access, fournissent une connectivité sécurisée aux applications privées pour les utilisateurs qui se connectent via ZTNA (Zero Trust Network Access) et VPN as a Service (VPNaaS). Ces tunnels permettent aux entreprises de relier en toute sécurité des utilisateurs distants à des ressources privées hébergées

dans des data centers ou des clouds privés.
Grâce à IKEv2 (Internet Key Exchange version 2), ces groupes de tunnels établissent des connexions bidirectionnelles sécurisées entre les routeurs Cisco Secure Access et SD-WAN. Ils prennent en charge la haute disponibilité via plusieurs tunnels au sein du même groupe et offrent une gestion flexible du trafic via le routage statique et dynamique (BGP).
Les tunnels IPsec peuvent acheminer le trafic provenant de diverses sources, notamment :

- Utilisateurs VPN d'accès à distance
- Connexions ZTNA basées sur un navigateur ou sur un client
- Autres emplacements réseau connectés à Cisco Secure Access

Cette approche permet aux entreprises d'acheminer en toute sécurité tous les types de trafic d'applications privées via un canal unifié et crypté, améliorant ainsi la sécurité et l'efficacité opérationnelle.
Cisco Secure Access, intégré à la solution Cisco Security Service Edge (SSE), simplifie les opérations informatiques grâce à une console unique gérée dans le cloud, un client unifié, la création de politiques centralisées et la création de rapports agrégés. Elle intègre plusieurs modules de sécurité dans une solution cloud unique, notamment ZTNA, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS), la sécurité DNS, Remote Browser Isolation (RBI) et bien plus encore. Cette approche complète limite les risques de sécurité en appliquant des principes de confiance zéro et en appliquant des politiques de sécurité granulaires

Figure 2 : Flux de trafic entre Cisco Secure Access et l'application privée



Flux de trafic des applications privées SSE

La solution décrite dans ce guide répond à des considérations complètes en matière de

redondance, englobant à la fois le routeur SD-WAN du centre de données et le groupe de tunnels de réseau (NTG) côté SSE (Security Service Edge). Ce guide se concentre sur un modèle de déploiement de concentrateur SD-WAN actif/actif, qui permet de maintenir un flux de trafic ininterrompu et garantit une haute disponibilité.

Conditions préalables

Exigences

Il est recommandé que vous ayez des connaissances sur les sujets suivants :

- Configuration et gestion de Cisco SD-WAN
- Connaissances de base des protocoles IKEv2 et IPSec
- Configuration du groupe de tunnels réseau dans le portail d'accès sécurisé Cisco
- Connaissance des protocoles BGP et ECMP

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleurs Cisco SD-WAN sur 20.9.5a
- Routeurs de périphérie WAN SD-WAN Cisco sur 17.9.5a
- Portail d'accès sécurisé Cisco

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Conception

Ce guide décrit la solution utilisant un modèle de conception actif/actif pour les routeurs de tête de réseau SD-WAN. Un modèle de conception actif/actif dans le contexte de routeurs de tête de réseau SD-WAN suppose deux routeurs dans un data center, tous deux connectés au groupe de tunnels réseau (NTG) SSE (Security Service Edge), comme illustré à la Figure 3. Dans ce scénario, les deux routeurs SD-WAN du data center (DC1-HE1 et DC1-HE2) gèrent activement le flux de trafic. Pour ce faire, ils envoient la même longueur de chemin AS (ASPL) au voisin DC interne. Par conséquent, le trafic provenant de l'intérieur du DC équilibre la charge entre les deux têtes de réseau.

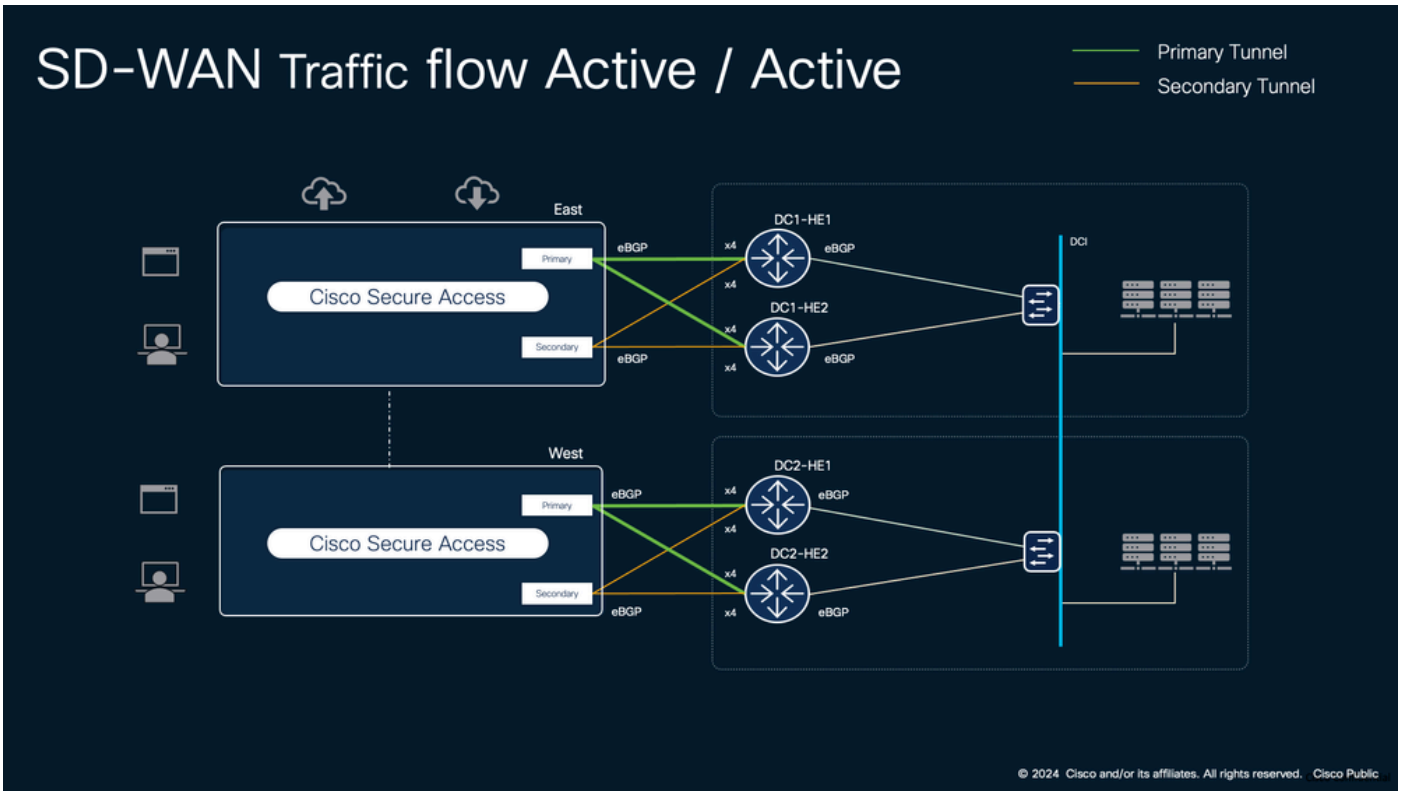
Chaque routeur de tête de réseau peut établir plusieurs tunnels vers les points de présence SSE (POP). Le nombre de tunnels varie en fonction de vos besoins et du modèle de périphérique SD-WAN. Dans cette conception :

- Chaque routeur comporte 4 tunnels vers le concentrateur SSE principal et 4 tunnels vers le

concentrateur SSE secondaire.
- Le nombre maximal de tunnels pris en charge par chaque concentrateur SSE peut varier. Pour obtenir les informations les plus récentes, reportez-vous à la documentation officielle : https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

Ces routeurs de tête de réseau forment des voisinages BGP sur les tunnels vers le SSE. Grâce à ces voisins, les têtes de réseau annoncent des préfixes d'application privés à leurs voisins SSE, permettant ainsi un routage sécurisé et efficace du trafic vers des ressources privées.

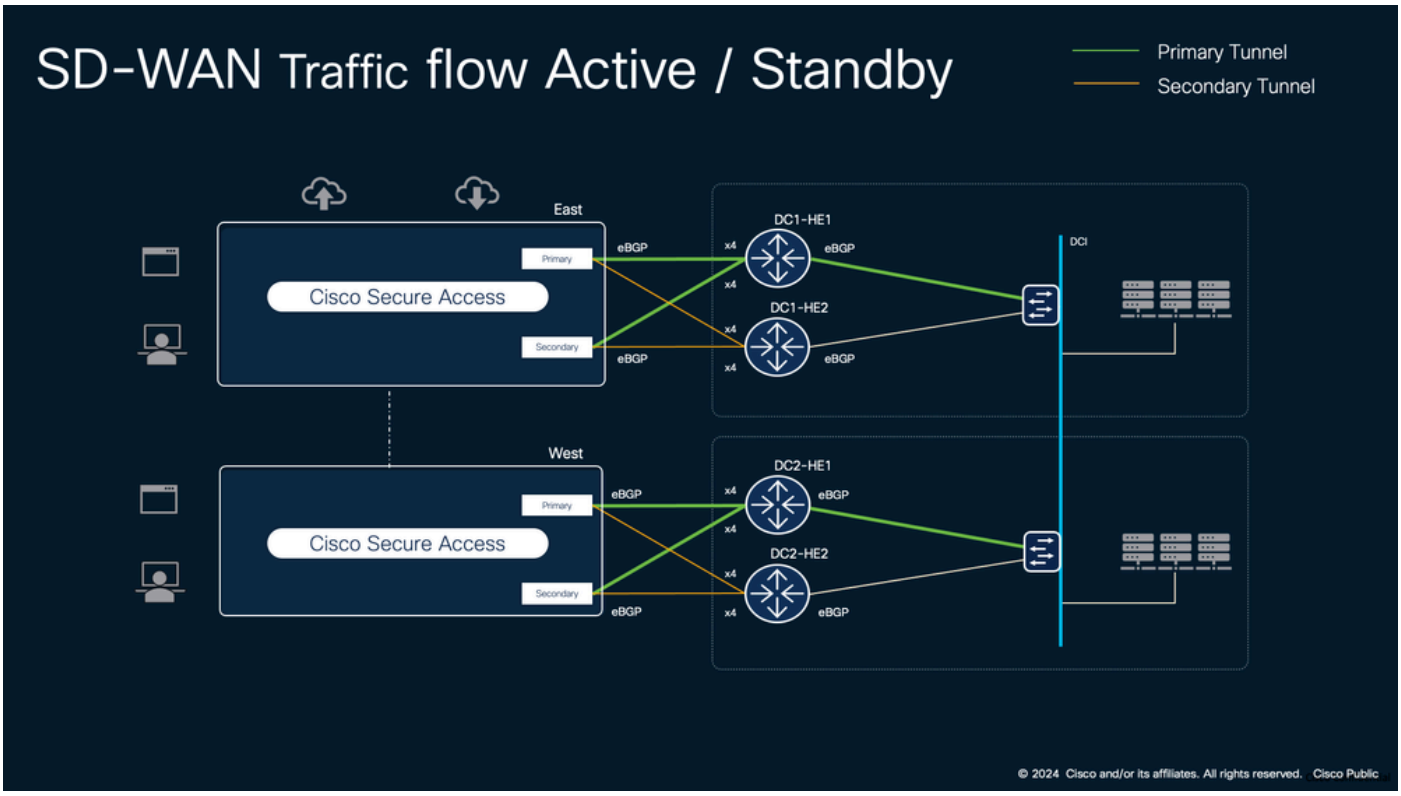
Figure 3 : Modèle de déploiement actif/actif SD-WAN vers SSE



Modèle de déploiement actif/actif SD-WAN vers SSE

Une conception active/veille désigne un routeur (DC1-HE1) comme toujours actif, tandis que le routeur secondaire (DC1-HE2) reste en veille. Le trafic circule régulièrement dans la tête de réseau active (DC1-HE1), sauf en cas de défaillance complète. Ce modèle de déploiement présente un inconvénient : si le tunnel principal vers SSE tombe en panne, le trafic bascule vers les tunnels SSE secondaires qui se trouvent uniquement via DC1-HE2, provoquant la réinitialisation de tout trafic avec état.
Dans le modèle Active/Standby, la longueur de chemin AS BGP est utilisée pour diriger le trafic à la fois au sein du DC et vers le SSE. DC1-HE1 envoie des mises à jour de préfixe au voisin BGP SSE avec une liste ASPL de 2, tandis que DC1-HE2 envoie des mises à jour avec une liste ASPL de 3. Le voisin DC interne de DC1-HE1 annonce des préfixes avec une longueur de chemin AS plus courte que DC1-HE2, ce qui garantit la préférence de trafic pour DC1-HE1. (Les clients peuvent choisir d'autres attributs ou protocoles pour influencer la préférence de trafic.)
Les clients peuvent sélectionner un modèle de déploiement actif/actif ou actif/veille en fonction de leurs besoins spécifiques.

Figure 4 : Modèle de déploiement actif/veille SD-WAN vers SSE



Modèle de déploiement actif/veille SD-WAN vers SSE

Configurer

Cette section décrit la procédure à suivre :

1. Vérifiez les conditions requises pour le provisionnement d'un groupe de tunnels réseau dans le portail Cisco Secure Access.
2. Configurez l'interconnexion SD-WAN avec le groupe de tunnels réseau d'accès sécurisé Cisco (NTG) à l'aide de la méthode manuelle IPsec.
3. Configurer le voisinage BGP

Remarque : Cette configuration est basée sur un modèle de déploiement actif/actif

---

Procédure 1. Vérification de la configuration du groupe de tunnels réseau sur le portail d’accès sécurisé Cisco

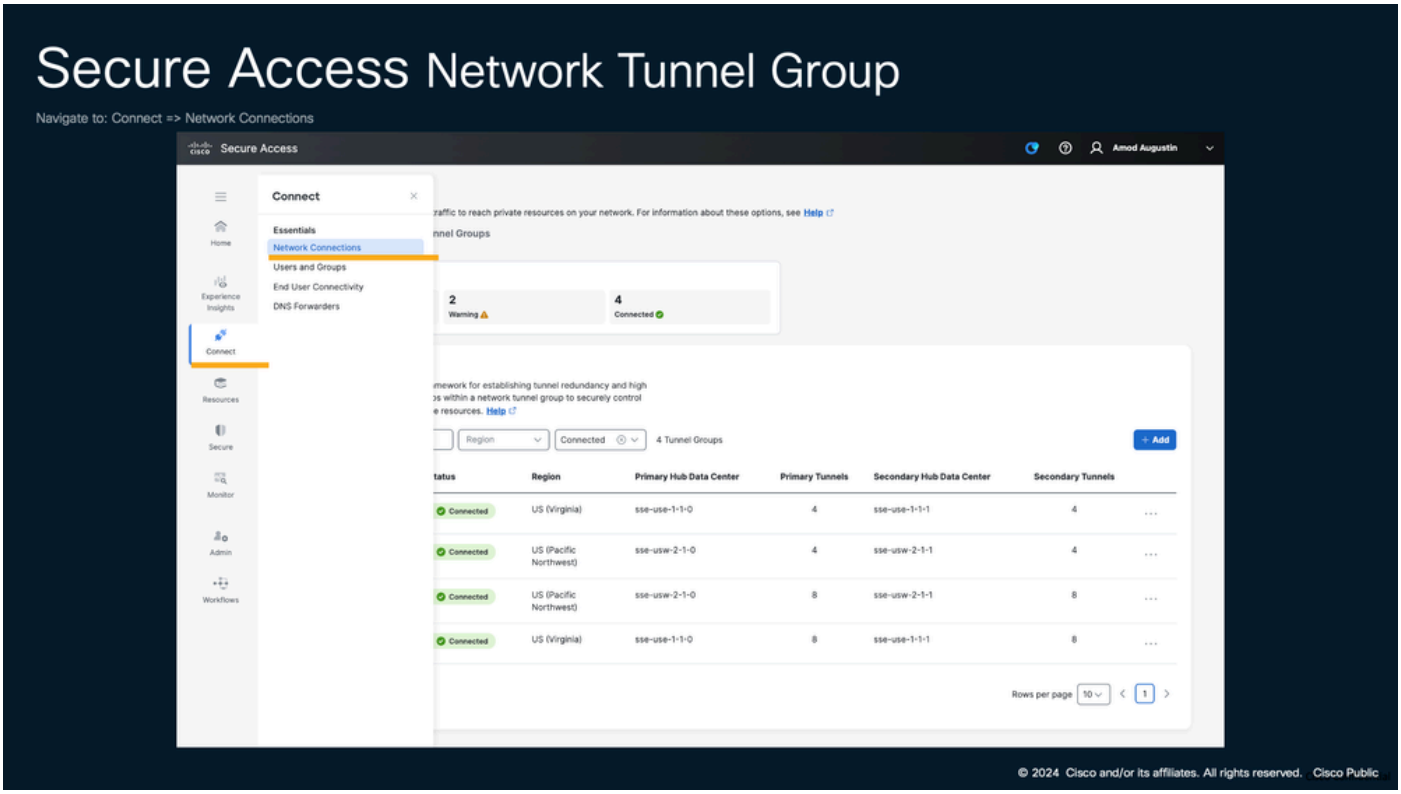
Le guide ne traite pas de la configuration du groupe de tunnels réseau. Veuillez réviser cette référence.

- Ajouter un groupe de tunnels réseau : Documentation SSE
- Configuration d'un tunnel réseau entre Cisco Secure Access et le routeur Cisco IOS XE à l'aide d'ECMP avec BGP

Accédez à Cisco Secure Access et vérifiez que les groupes de tunnels réseau (NTG) sont configurés. Pour la conception actuelle, nous devons mettre en service des NTG dans deux points de présence (POP) différents. Dans ce guide, nous utilisons des GNT dans le POP des États-Unis (Virginie) et dans le POP des États-Unis (Pacifique Nord-Ouest).

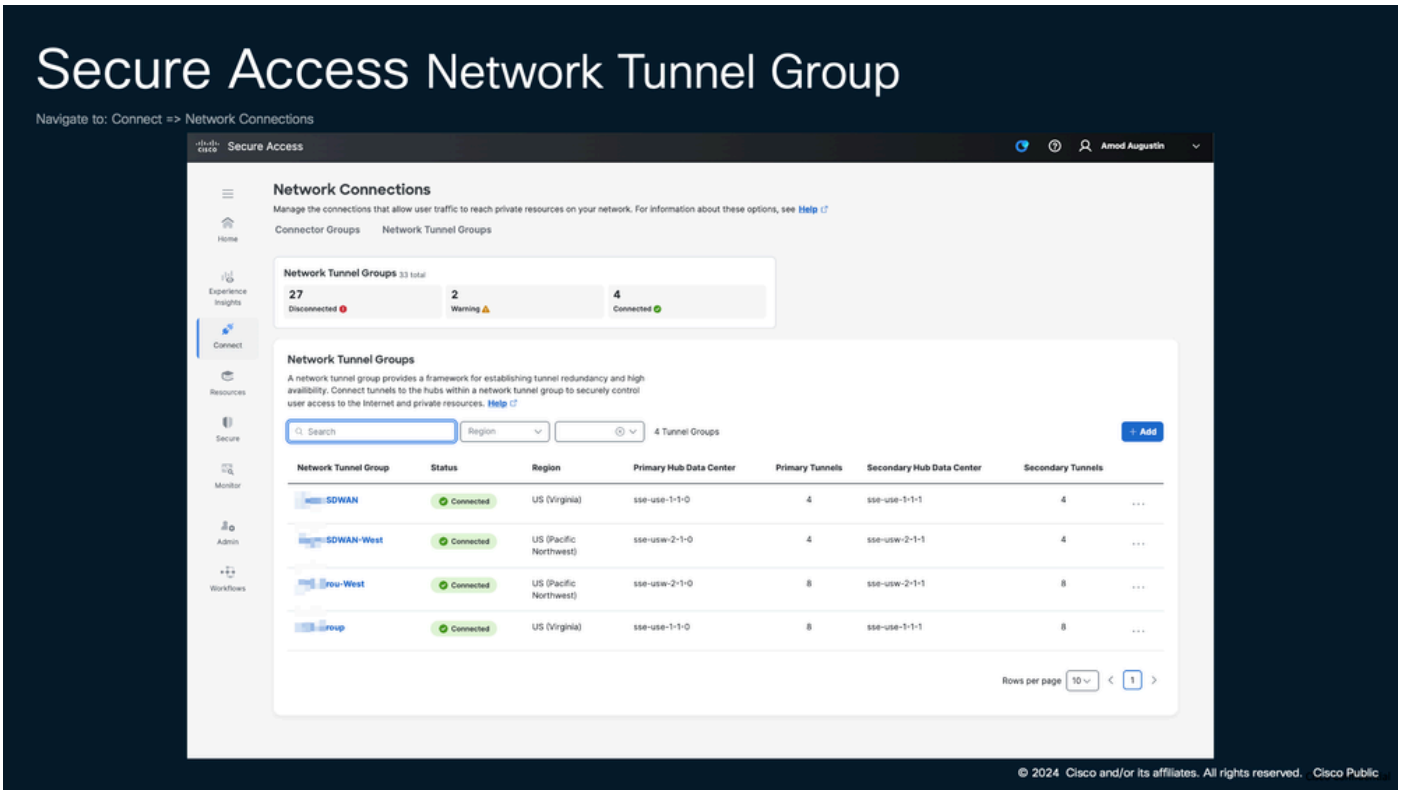
Remarque : les noms et les emplacements des POP peuvent varier, mais le concept clé est d'avoir plusieurs NTG provisionnés dans des emplacements géographiquement proches de votre data center. Cette approche permet d'optimiser les performances du réseau et assure la redondance.

Figure 5 : Groupe de tunnels réseau Cisco Secure Access



Groupe de tunnels réseau Cisco Secure Access

Figure 6 : Liste des groupes de tunnels réseau d'accès sécurisé Cisco



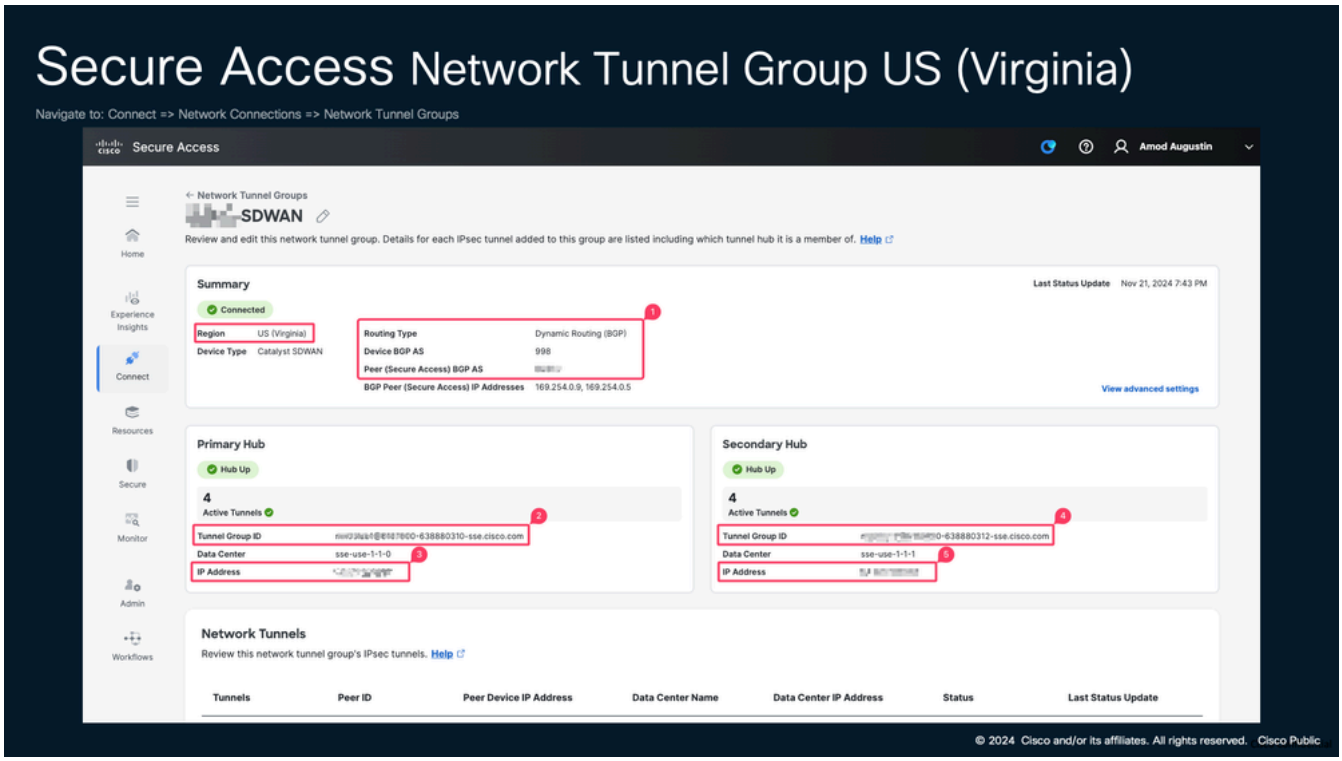
Liste des groupes de tunnels réseau d'accès sécurisé

Assurez-vous d'avoir noté la phrase de passe du tunnel (qui n'est affichée qu'une fois pendant la création du tunnel).

Remarque : Étape 6 - Ajouter un groupe de tunnels réseau

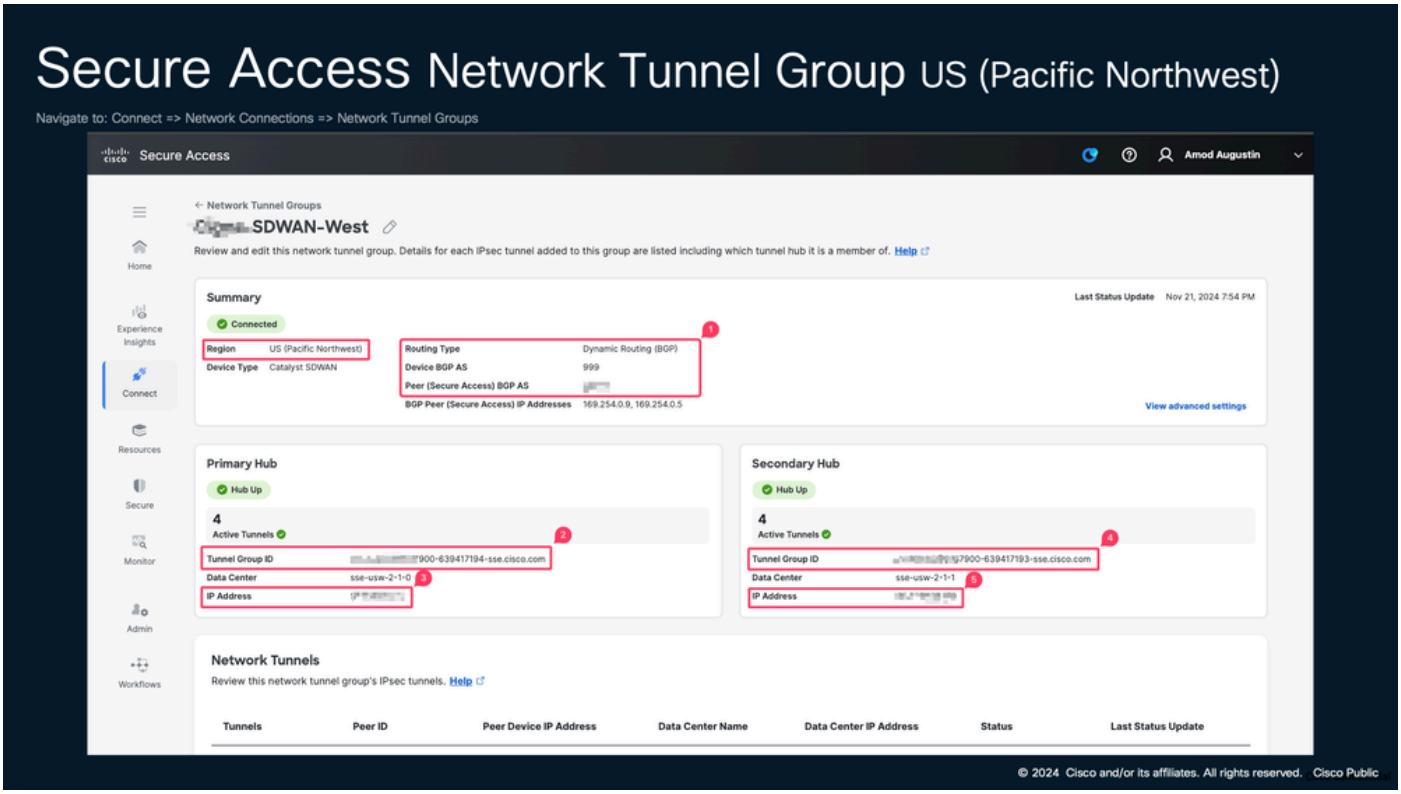
Notez également les attributs du groupe de tunnels que nous utilisons lors de la configuration IPSec. La capture d'écran (Figure 6) provient d'un environnement de laboratoire pour un scénario de production et permet de créer des groupes NTG conformément aux recommandations de conception ou d'utilisation.

Figure 7 : Secure Access Network Tunnel Group US (Virginie)



Secure Access Network Tunnel Group US (Virginie)

Figure 8 : Groupe de tunnels de réseau d'accès sécurisé US (Pacifique Nord-Ouest)



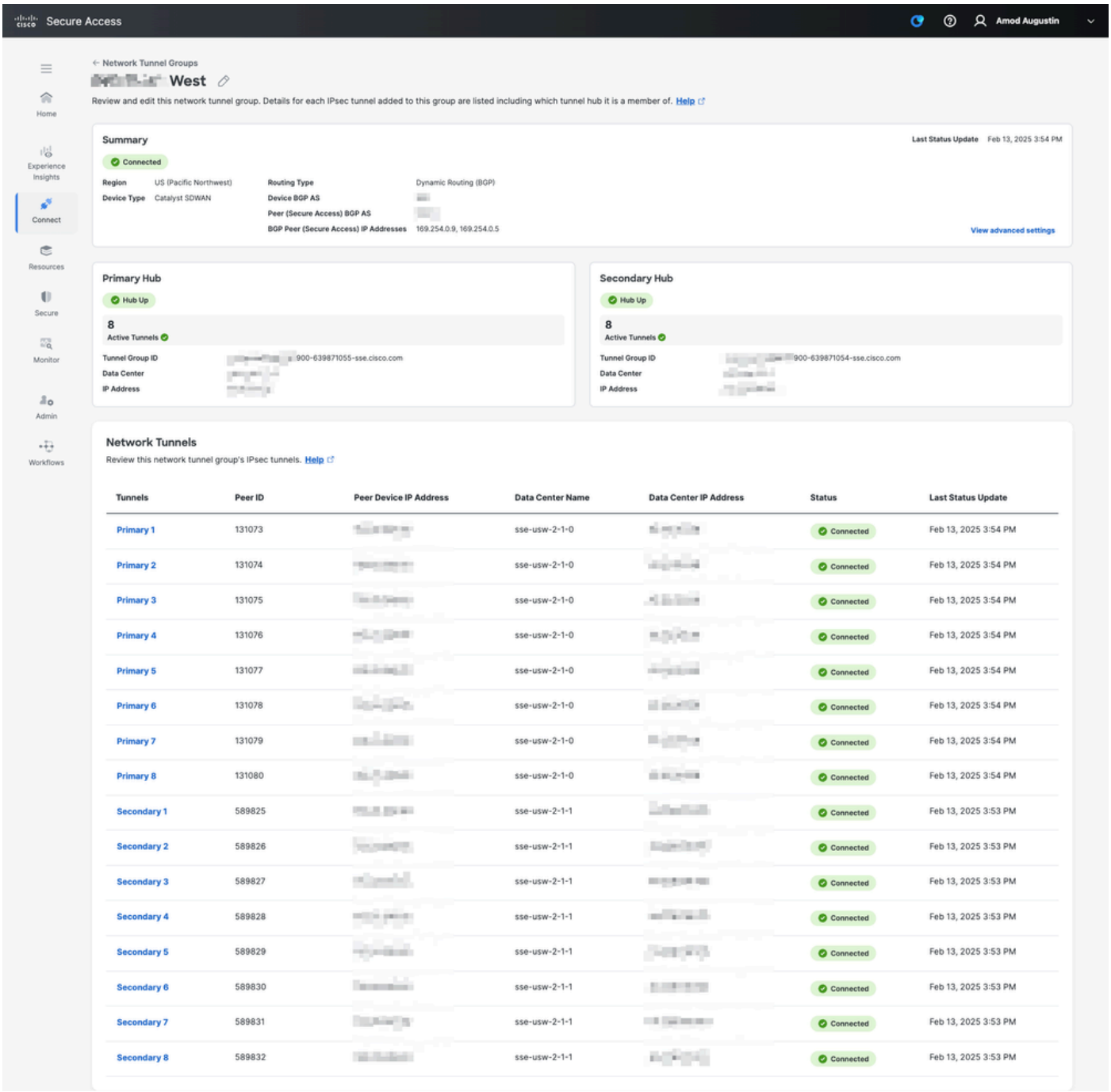
Secure Access Network Tunnel Group US (Pacifique Nord-Ouest)

La figure 8 montre seulement 4 tunnels sur les concentrateurs principal et secondaire. Cependant, un maximum de 8 tunnels a été testé avec succès dans un environnement de contrôleur. La prise en charge maximale du tunnel peut varier en fonction du périphérique matériel que vous utilisez et de la prise en charge actuelle du tunnel SSE. Pour obtenir les informations les plus récentes,

reportez-vous à la documentation officielle : https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels et la note de version du périphérique matériel correspondant.

Un exemple de configuration à 8 tunnels est fourni ici.

Figure 8a : Tunnels NTG jusqu'à 8 tunnels



SSE NTG jusqu'à 8 tunnels

Procédure 2. Configurer l’interconnexion SD-WAN avec le groupe de tunnels réseau d’accès sécurisé Cisco (NTG) à l’aide de la méthode manuelle IPsec.

Cette procédure explique comment connecter un groupe de tunnels de réseau (NTG) à l'aide de

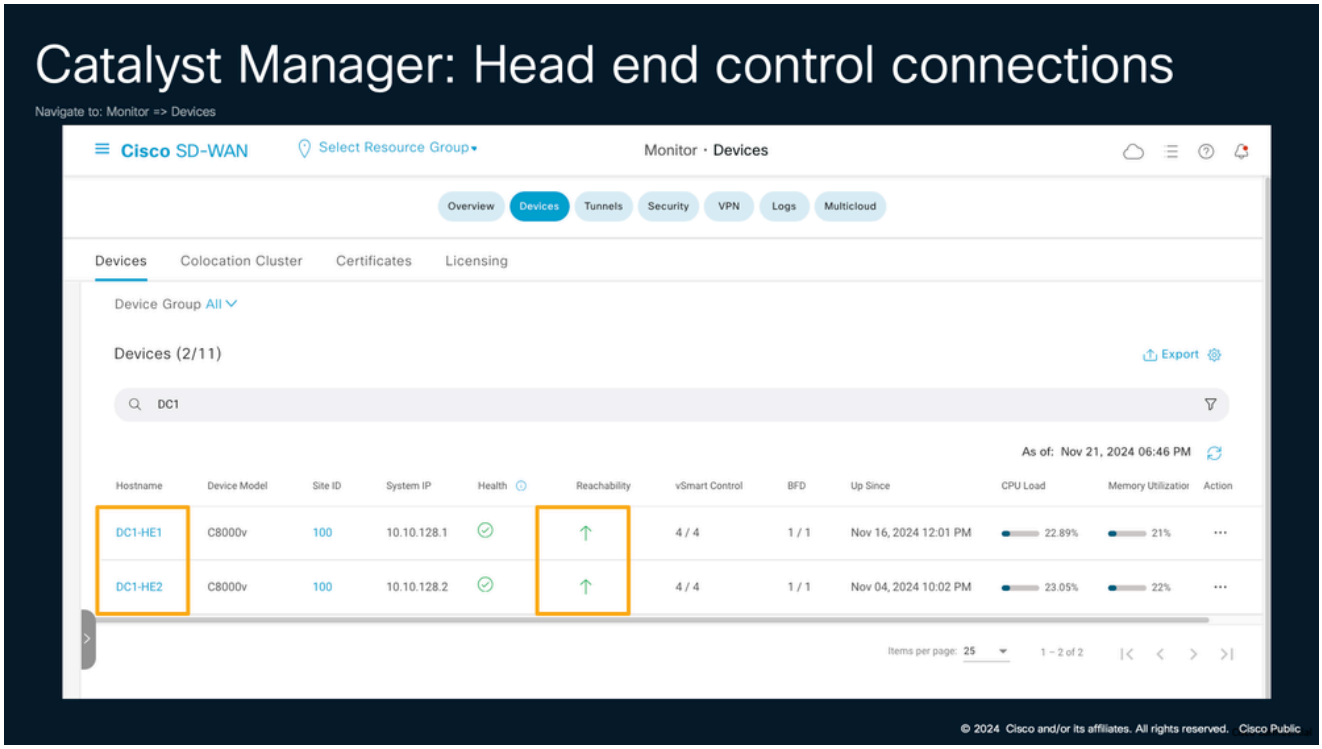
modèles de fonctionnalités sur Cisco Catalyst SD-WAN Manager 20.9 et Cisco Catalyst Edge Router exécutant la version 17.9.

Remarque : ce guide suppose un déploiement de superposition SD-WAN existant avec une topologie Hub and Spoke ou entièrement maillée, où les concentrateurs servent de points d'accès pour les applications privées hébergées dans le data center. Cette procédure peut également s'appliquer aux déploiements de filiales ou de cloud.

Avant de continuer, assurez-vous que les conditions requises sont remplies :

1. Les connexions de contrôle sont activées sur le périphérique pour permettre les mises à jour nécessaires depuis Cisco Catalyst SD-WAN Manager.

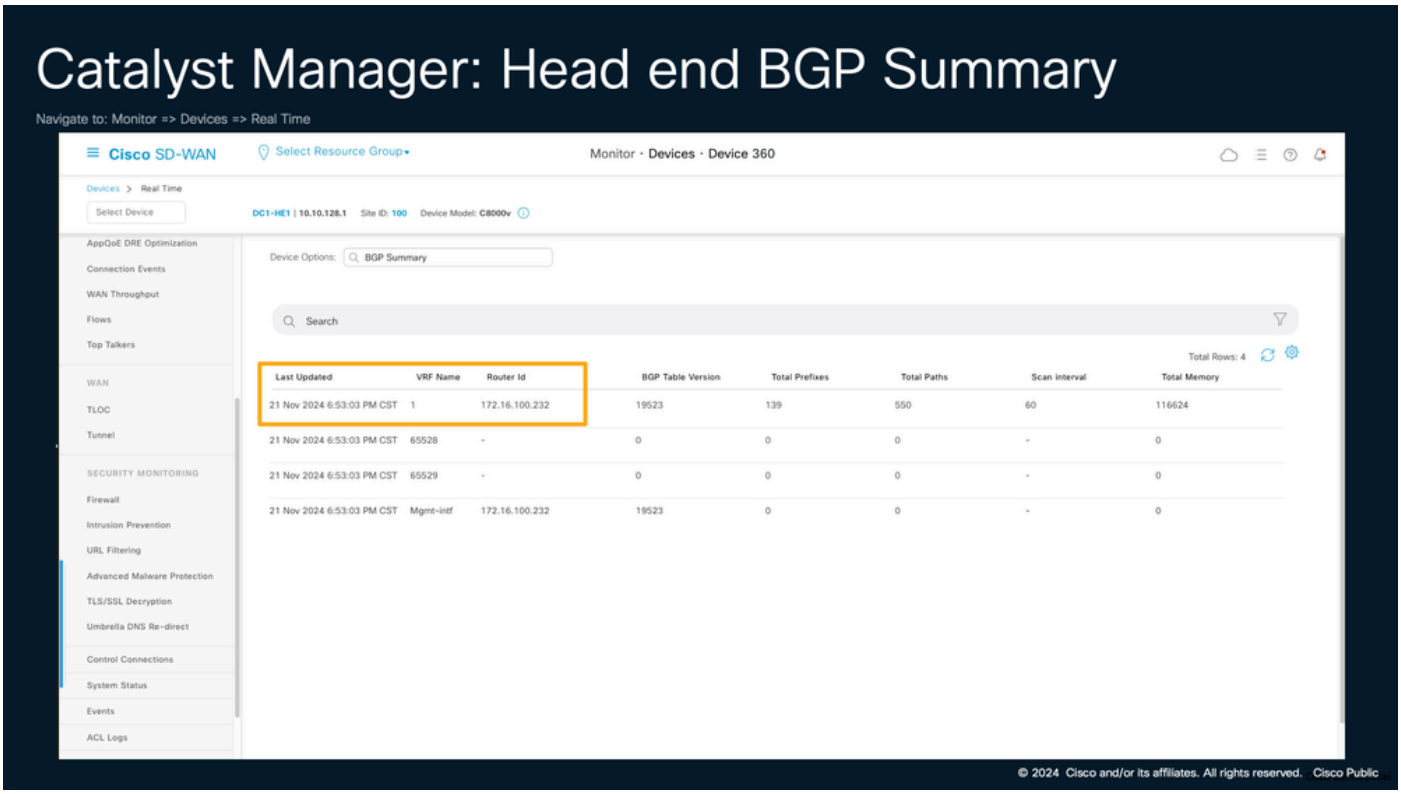
   Figure 9 : Cisco Catalyst SD-WAN Manager : Connexions de contrôle de tête de réseau



Catalyst Manager : Connexions de contrôle de tête de réseau

2. Les VPN côté service sont configurés et utilisent un protocole de routage pour annoncer les préfixes. Ce guide utilise le protocole BGP comme protocole de routage côté service.

Figure 10 : Cisco Catalyst SD-WAN Manager : Résumé BGP de tête de réseau



Pour configurer l'interconnexion SD-WAN avec le groupe de tunnels de réseau (NTG) à l'aide de la méthode IPSec manuelle, procédez comme suit :

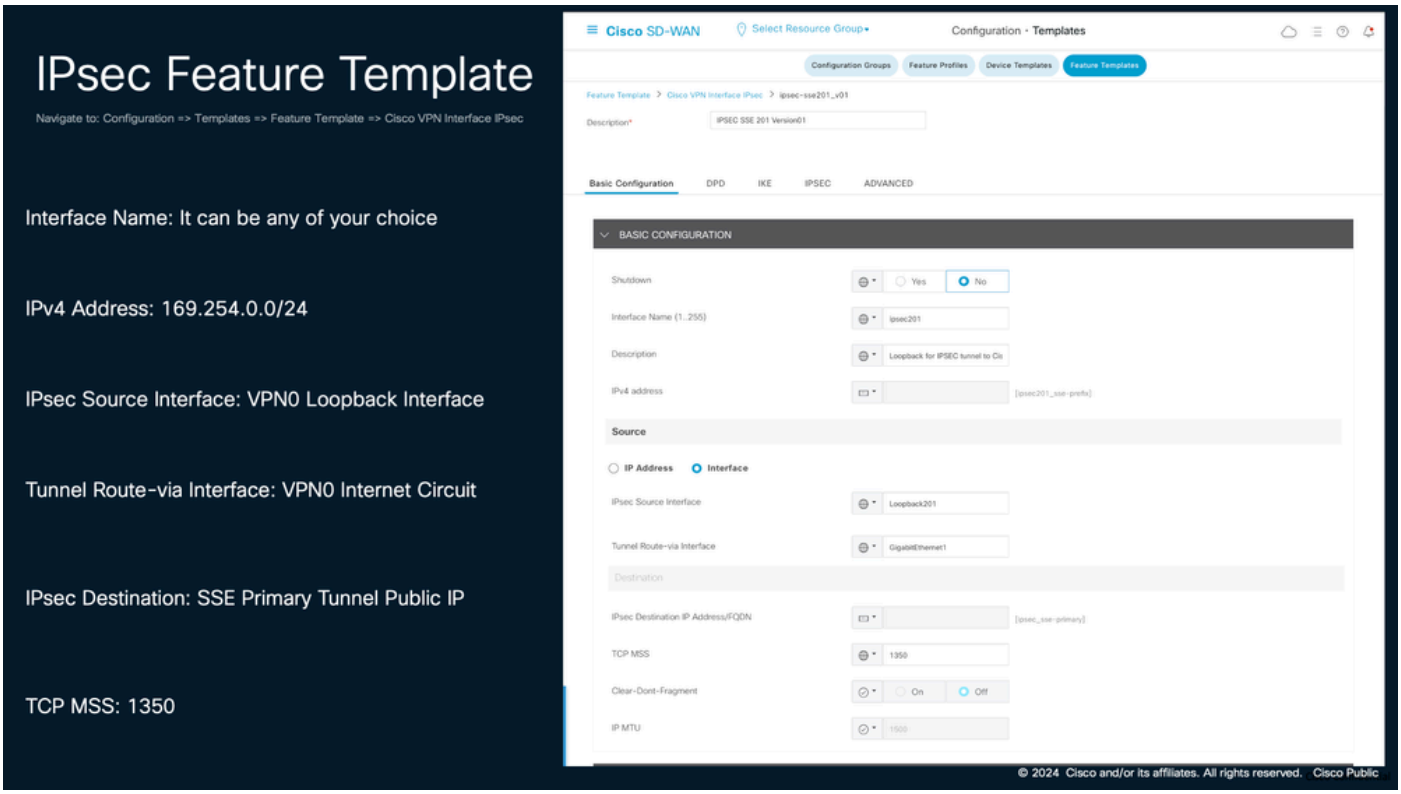
Remarque : Répétez cette étape pour le nombre de tunnels requis pour le déploiement.

Reportez-vous à la documentation officielle relative à la limitation du tunnel : https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

Ces étapes détaillent le processus de connexion de DC1-HE1 (tête de réseau 1 du centre de données 1) au concentrateur principal SSE Virginia. Cette configuration établit un tunnel sécurisé entre le routeur SD-WAN du centre de données et le groupe de tunnels réseau d'accès sécurisé Cisco (NTG) situé dans le point de présence de Virginie (POP)

Étape 1 : Créer un modèle de fonctionnalité IPSec
Créez un modèle de fonctionnalité IPSec pour définir les paramètres du tunnel IPSec qui connecte le routeur de tête de réseau SD-WAN au NTG.

Figure 11 : Modèle de fonctionnalité IPsec : Configuration de base



Modèle de fonctionnalité IPsec : Configuration de base

Nom de l'interface : Il peut être n'importe lequel de votre choix
Adresse IPv4 : SSE écoute 169.254.0.0/24 en fonction de l'exigence selon laquelle vous pouvez diviser le sous-réseau en fonction de votre choix, comme pratique recommandée, utilisez avec /30. Dans ce guide, nous omettons le premier bloc pour une utilisation ultérieure.

Interface source IPsec : Définissez une interface de bouclage VPN0 unique pour l'interface IPsec actuelle. Pour des raisons de cohérence et de dépannage, il est recommandé de conserver la même numérotation.
Interface de routage via le tunnel : Pointez vers l'interface qui peut être utilisée comme sous-réseau pour atteindre SSE (doit disposer d'un accès Internet)

Destination IPsec : Adresse IP du concentrateur principal

Reportez-vous à la figure 7 : Secure Access Network Tunnel Group US (Virginia) (35.171.214.188)

MSS TCP : Il doit s'agir de 1350 (référence : [https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters)](https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters)

Exemple : DC1-HE1 vers le concentrateur principal SSE Virginia

Nom de l'interface : ipsec201

Description : bouclage pour le tunnel IPSEC vers Cisco

Adresse IPv4 : 169.254.0.x/30

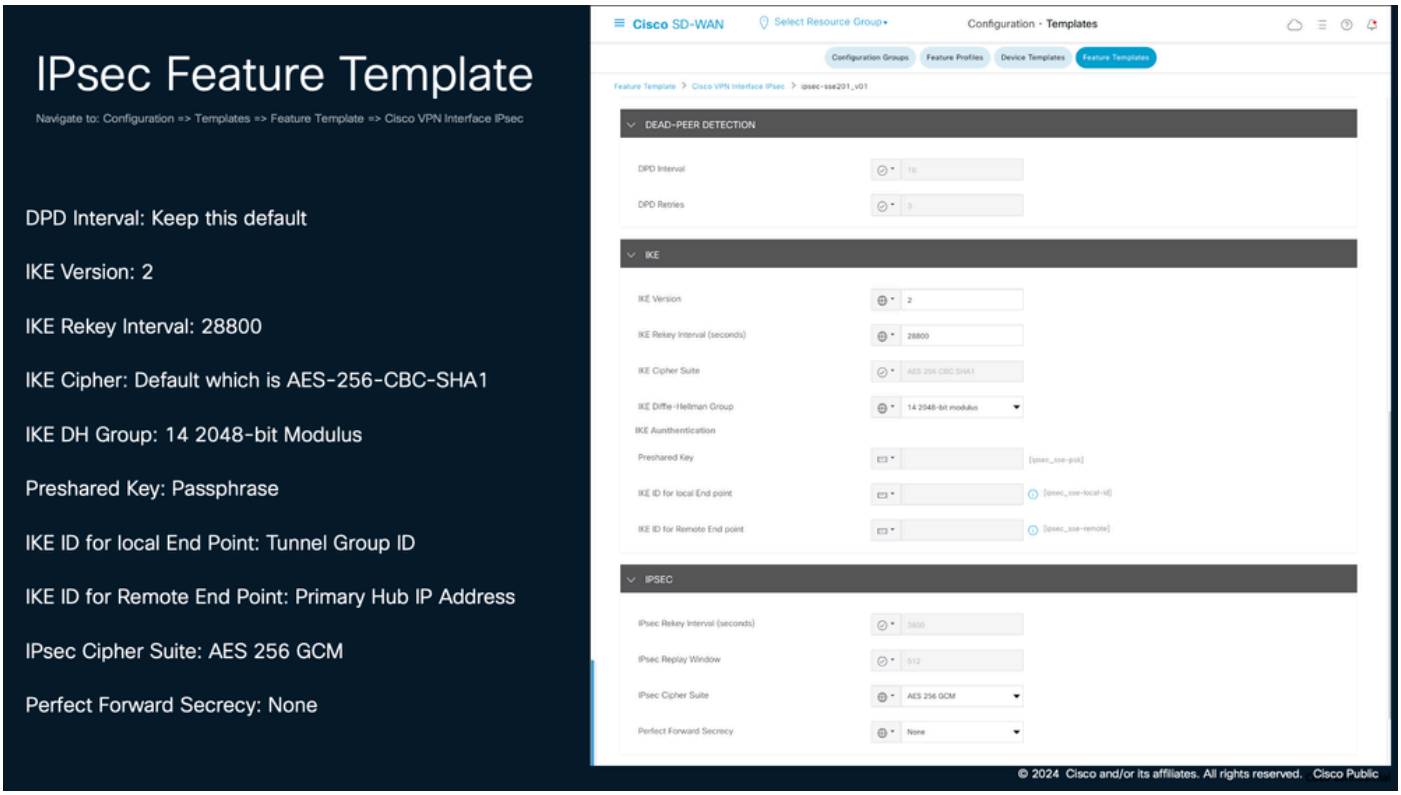
Interface source IPsec : Bouclage201

Interface de routage via tunnel : GigabitEthernet1

Adresse IP de destination IPsec/nom de domaine complet : 35.xxx.xxx.xxx

MSS TCP : 1350

Figure 12 : Modèle de fonctionnalité IPsec : IKE IPSEC



Modèle de fonctionnalité IPsec : IKE IPSEC

Intervalle DPD : Conserver cette valeur par défaut
Version IKE : 2
Intervalle de renouvellement des clés IKE : 28800
Chiffre IKE : Valeur par défaut : AES-256-CBC-SHA1
Groupe IKE DH : Module 14 2048 bits
Clé pré-partagée : Phrase De Passe
ID IKE du point d'extrémité local : ID du groupe de tunnels

Reportez-vous à la figure 7 : Secure Access Network Tunnel Group US (Virginie) : mn03lab1+201@8167900-638880310-sse.cisco.com

---

Remarque : Chaque tunnel doit avoir un point de terminaison unique pour cela ; utiliser "+loopbackID" Exemple : mn03lab1+202@8167900-638880310-sse.cisco.com, mn03lab1+203@8167900-638880310-sse.cisco.com, etc.

ID IKE du point d'extrémité distant : Adresse IP du concentrateur principal
Suite de chiffrement IPsec : AES 256 GCM

Secret de transmission parfait : Aucune

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

Exemple :

Version IKE : 2
Intervalle de renouvellement des clés IKE : 28800
Chiffre IKE : AES-256-CBC-SHA1
Groupe IKE DH : Module 14 2048 bits
Clé pré-partagée : *****

Remarque : Étape 6 - Ajouter un groupe de tunnels réseau

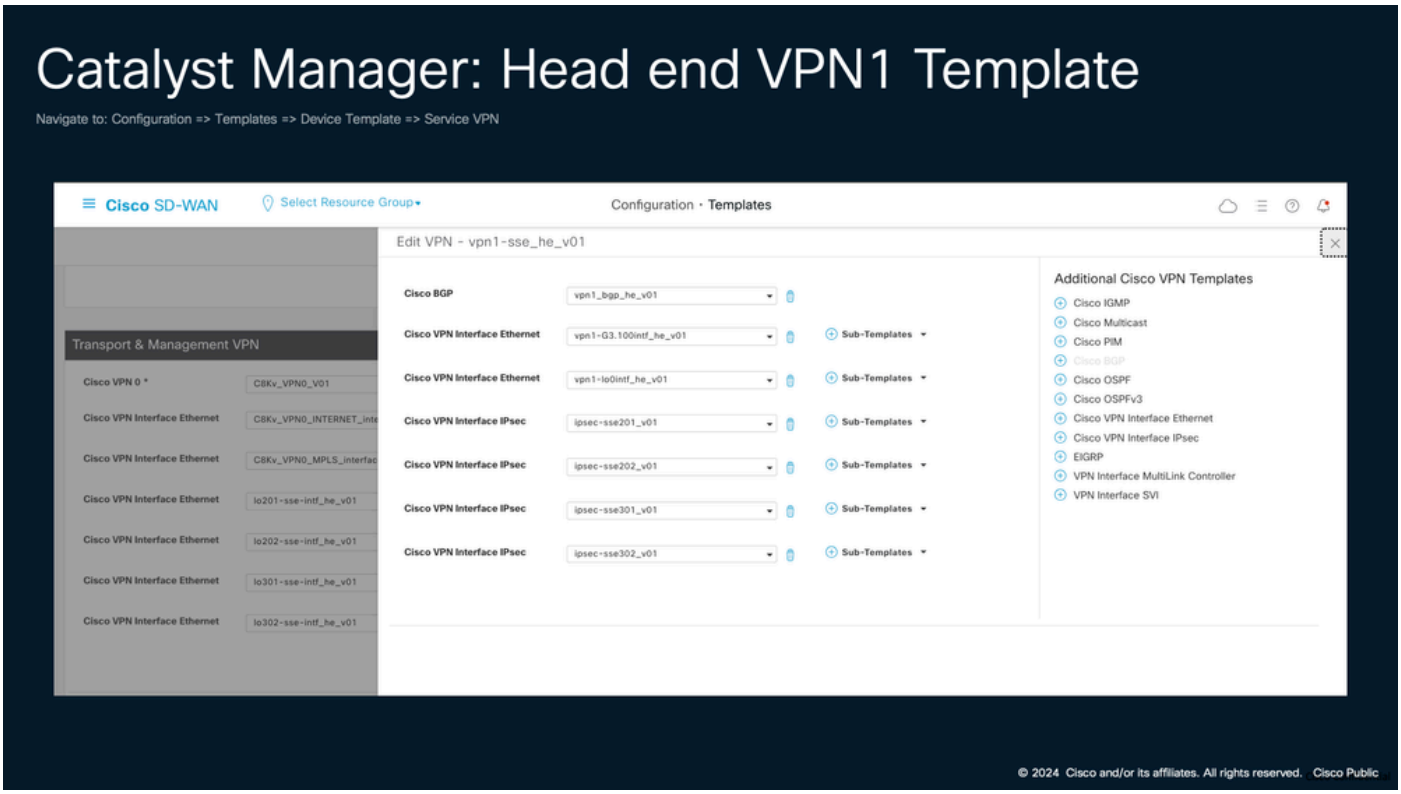
ID IKE du point d'extrémité local : mn03lab1@8167900-638880310-sse.cisco.com
ID IKE du point d'extrémité distant : 35.171.xxx.xxx
Suite de chiffrement IPsec : AES 256 GCM
Secret de transmission parfait : Aucune

Répétez les étapes pour configurer les tunnels requis pour les concentrateurs d'accès sécurisé principal et secondaire.Pour une configuration 2x2, vous créeriez quatre tunnels au total :

- Deux tunnels reliant DC1-HE1 au concentrateur d'accès sécurisé principal
- Deux tunnels reliant DC1-HE1 au concentrateur d'accès sécurisé secondaire

Maintenant que les modèles sont créés, nous les utilisons du côté du service vrf show dans la figure 13 et le bouclage défini joint sur le vrf global montré dans la figure 14.

Figure 13 : Catalyst SD-WAN Manager : Modèle VPN1 de tête de réseau 2x2



Catalyst Manager : Modèle VPN1 de tête de réseau

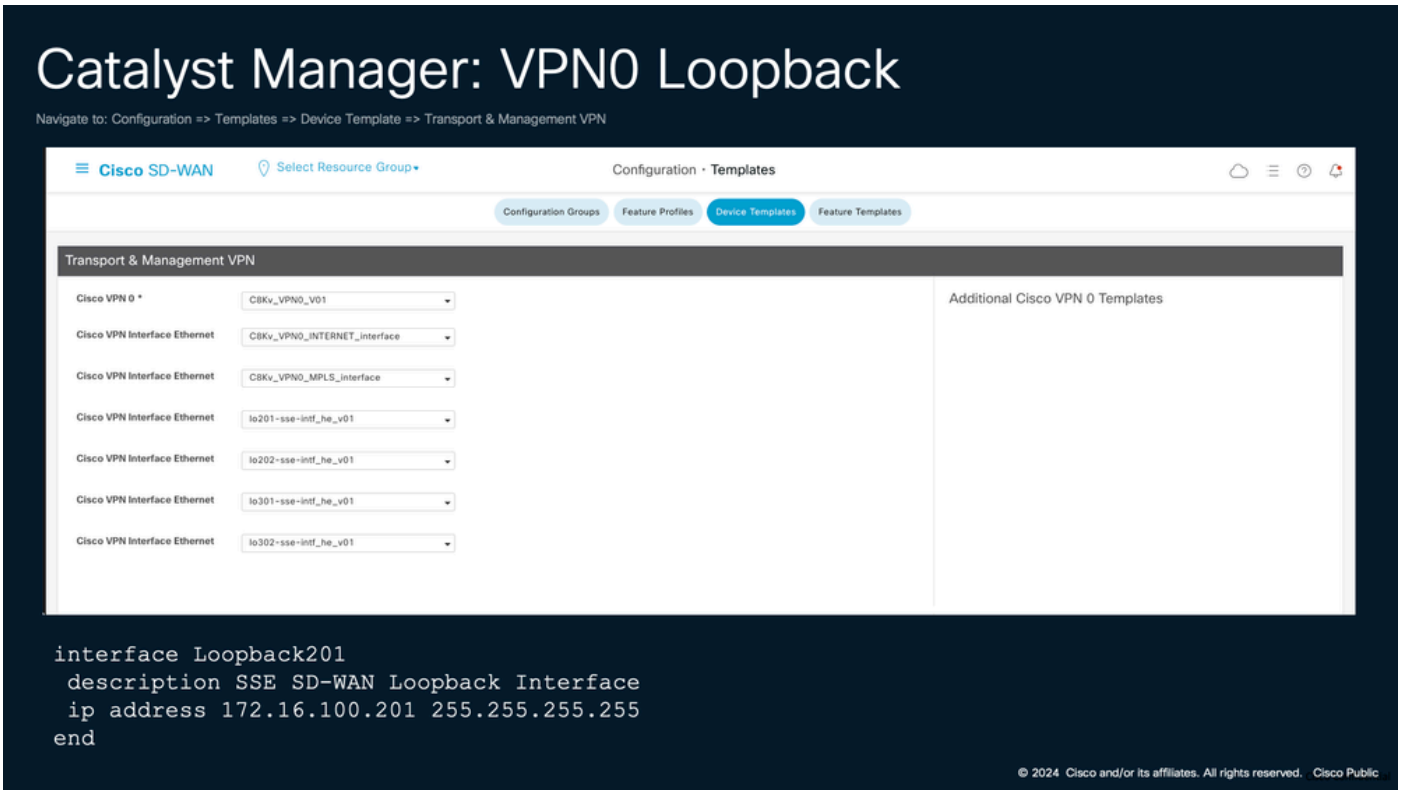
Étape 2 : Définition du bouclage dans le VRF global

Configurez une interface de bouclage dans la table VRF (Virtual Routing and Forwarding) globale. Ce bouclage sert d'interface source pour le tunnel IPSec créé à l'étape 1.

Tous les bouclages référencés à l'étape 1 doivent être définis dans le VRF global.

L'adresse IP peut être définie dans n'importe quelle plage RFC1918.

Figure 14 : Catalyst SD-WAN Manager : Bouclage VPN0

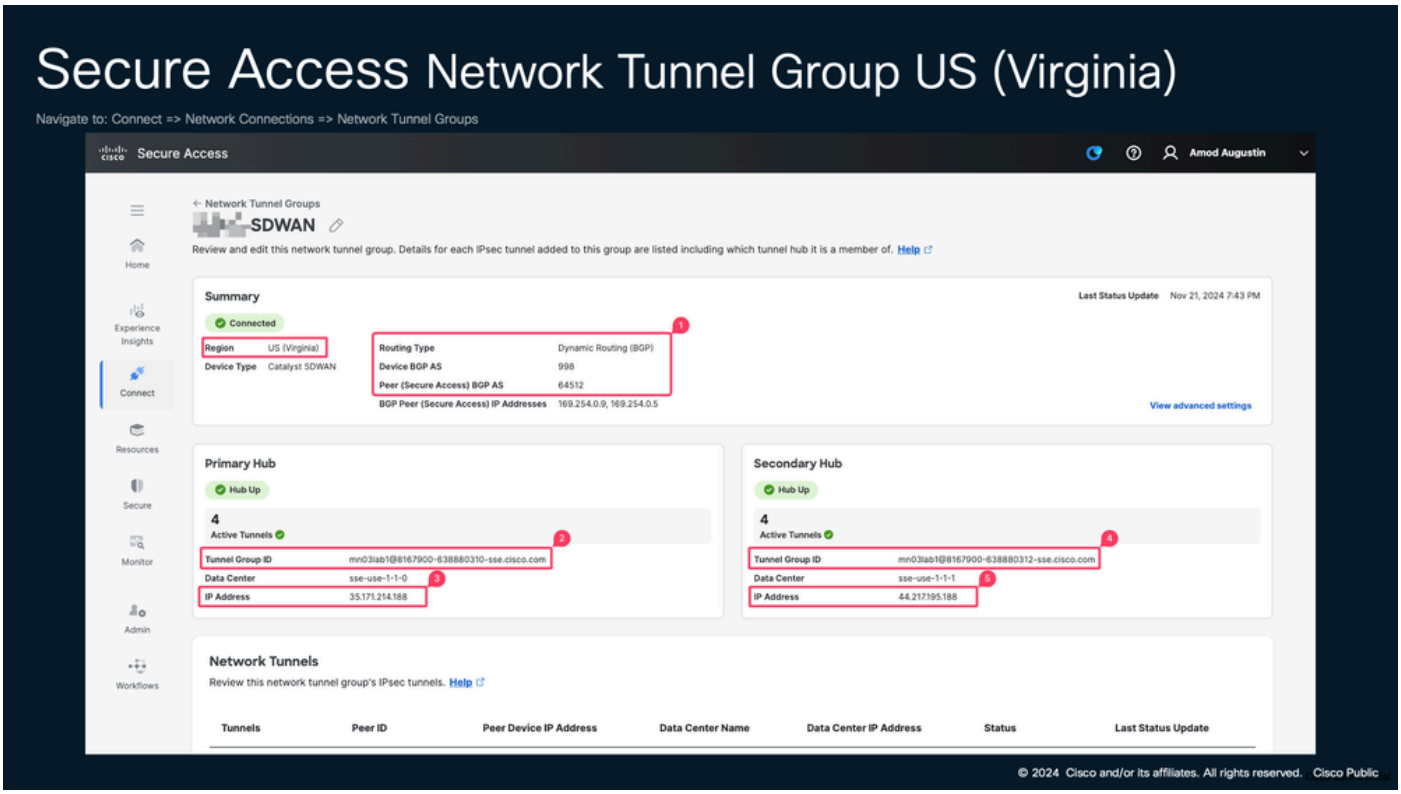


Catalyst Manager : Bouclage VPN0

Procédure 3. Configurer le voisinage BGP

Utilisez le modèle de fonctionnalité BGP pour définir le voisinage BGP pour toutes les interfaces de tunnel. Référez-vous à la configuration BGP des groupes de tunnels réseau respectifs dans le portail d'accès sécurisé Cisco pour configurer les valeurs BGP.

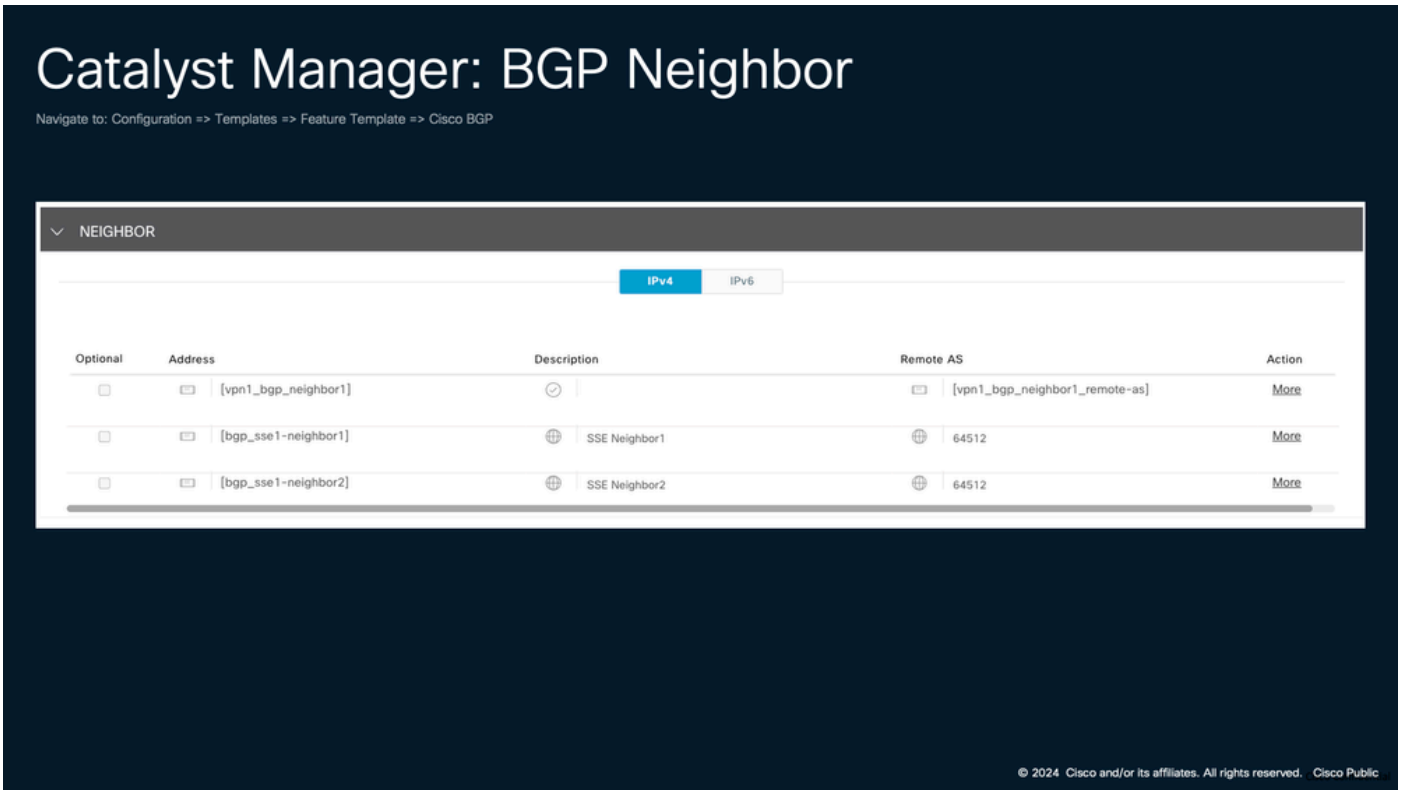
Figure 15 : Secure Access Network Tunnel Group US (Virginie)



Secure Access Network Tunnel Group US (Virginie)

Dans cet exemple, nous utilisons les informations de la Figure 15 (case 1) pour définir le protocole BGP à l'aide d'un modèle de fonctionnalité.

Figure 16 : Voisin BGP du gestionnaire SD-WAN Catalyst



Voisin BGP du gestionnaire SD-WAN Catalyst

Configuration générée à l'aide du modèle de fonction :

```
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#
```

Vérification

```
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
```

Référence

Une implémentation active/active aurait un chemin multiple à partir du commutateur principal qui est connecté aux deux têtes de réseau SD-WAN.

Figure 17 : Scénario actif/actif pour voisin 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>
```

Voisin BGP actif/actif

Une implémentation active/en veille aurait un chemin actif unique entre le commutateur principal et les têtes de réseau SD-WAN en raison de la mise en attente ASPL (qui est effectuée à l'aide d'une carte de route vers le voisin).

Figure 18 : Scénario actif/veille pour voisin 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>
```

Voisin BGP actif/veille

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.