Configurer la superposition sécurisée avec les annonces de routage BGP

Table des matières

Introduction

Ce document décrit comment configurer la superposition sécurisée et les annonces eBGP sur NFVIS pour la gestion exclusive du trafic vBranch.

Composants utilisés

Les informations contenues dans ce document sont basées sur les composants matériels et logiciels suivants :

- ENCS5412 exécutant NFVIS 4.7.1
- Catalyst 8000v exécutant Cisco IOS® XE 17.09.03a

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.

Annonce de route BGP

La fonctionnalité NFVIS BGP fonctionne avec la fonctionnalité de superposition sécurisée pour apprendre les routes à partir du voisin BGP sur un tunnel de superposition sécurisé. Ces routes ou sous-réseaux acquis sont ajoutés à la table de routage NFVIS pour le tunnel sécurisé, ce qui rend les routes accessibles via le tunnel. Puisque la superposition sécurisée autorise seulement 1 route privée unique à apprendre du tunnel, la configuration du protocole BGP permet de surmonter cette limitation en établissant une contiguïté par le biais du tunnel chiffré et en injectant les routes exportées dans la table de routage NFVIS vpnv4 et vice versa.

Exemple de configuration

Schéma de topologie

L'objectif de cette configuration est d'atteindre l'adresse IP de gestion de NFVIS à partir du c8000v. Une fois le tunnel établi, il est possible d'annoncer plus de routes à partir des sous-réseaux private-vrf en utilisant les annonces de route eBGP.

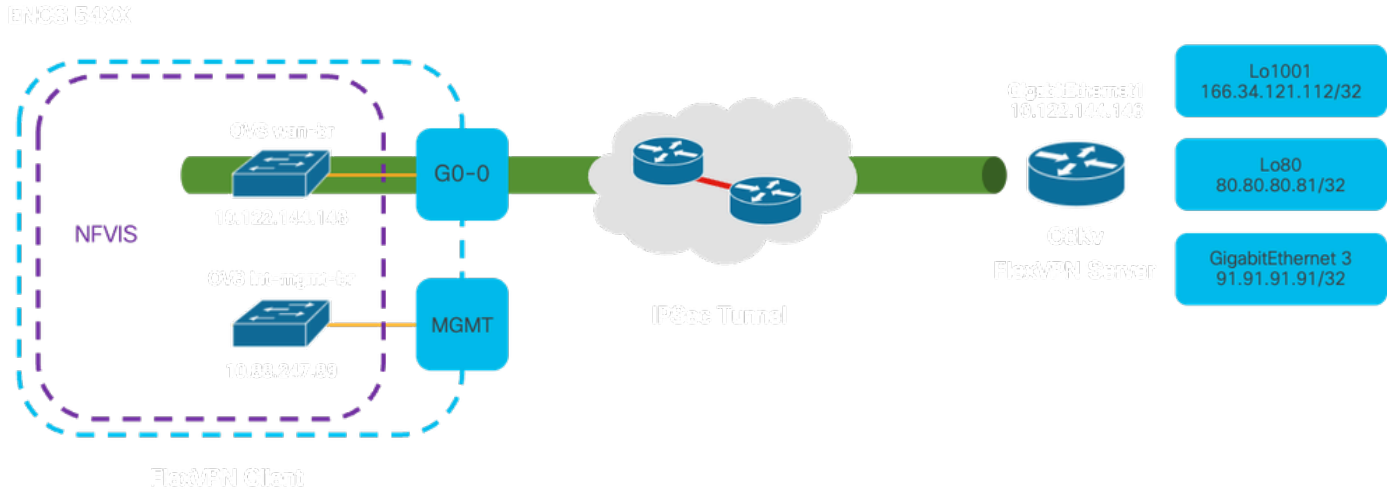


Figure 1. Schéma de topologie pour l'exemple préparé sur cet article

Configuration initiale

Configurez l'adressage IP approprié sur le serveur FlexVPN (en mode de configuration globale)

```
vrf definition private-vrf
 rd 65000:7
 address-family ipv4
 exit-address-family

vrf definition public-vrf
 address-family ipv4
 exit-address-family

interface GigabitEthernet1
 description Public-Facing Interface
 vrf forwarding public-vrf
 ip address 10.88.247.84 255.255.255.224

interface Loopback1001
 description Tunnel Loopback
 vrf forwarding private-vrf
 ip address 166.34.121.112 255.255.255.255

interface Loopback80
 description Route Announced Loopback
 vrf forwarding private-vrf
 ip address 81.81.81.1 255.255.255.255

interface GigabitEthernet3
 description Route Announced Physical Interface
 vrf forwarding private-vrf
 ip address 91.91.91.1 255.255.255.0
```

Pour NFVIS, configurez l'interface WAN et MGMT en conséquence

```
system settings mgmt ip address 192.168.1.1 255.255.255.0
system settings wan ip address 10.88.247.89 255.255.255.224
system settings default-gw 10.88.247.65
system settings ip-receive-acl 0.0.0.0/0
 service  [ ssh https netconf scpd ]
 action   accept
 priority 10
!
```

Configuration du serveur FlexVPN sur le routeur Catalyst 8000v

1. Créer une proposition IKEv2

Il spécifie les protocoles et algorithmes de sécurité que deux points d’extrémité VPN doivent utiliser pendant la phase initiale (phase 1) d’établissement d’un canal de communication sécurisé. L'objectif de la proposition IKEv2 est de définir les paramètres d'authentification, de cryptage, d'intégrité et d'échange de clés, afin de garantir que les deux terminaux s'accordent sur un

ensemble commun de mesures de sécurité avant d'échanger des données sensibles.

```
crypto ikev2 proposal uCPE-proposal
 encryption aes-cbc-256
 integrity sha512
 group 16 14
```

Where:

cryptage <algorithm>	La proposition inclut les algorithmes de cryptage (comme AES ou 3DES) que le VPN doit utiliser pour protéger les données. Le chiffrement empêche les écouteurs de lire le trafic qui passe par le tunnel VPN.
intégrité <hash>	Il spécifie les algorithmes (tels que SHA-512) utilisés pour garantir l'intégrité et l'authenticité des messages échangés pendant la négociation IKEv2. Cela empêche les tentatives d'altération et de relecture.

2. Créez une stratégie IKEv2 et associez-la à la proposition.

Il s’agit d’un jeu de configuration qui détermine les paramètres de la phase initiale (phase 1) de l’établissement d’une connexion VPN IPsec. Il se concentre principalement sur la façon dont les points d'extrémité VPN s'authentifient mutuellement et établissent un canal de communication sécurisé pour la configuration VPN.

```
crypto ikev2 policy uCPE-policy
 match fvrf public-vrf
 proposal uCPE-proposal
```

3. Configurez la stratégie d'autorisation IKEv2

IKEv2 est un protocole utilisé pour établir une session sécurisée entre deux points d'extrémité sur un réseau, et la stratégie d'autorisation est un ensemble de règles qui détermine les ressources et les services auxquels un client VPN est autorisé à accéder une fois le tunnel VPN établi.

```
crypto ikev2 authorization policy uCPE-author-pol
 pfs
 route set interface Loopback1001
```

Where:

pfs	Perfect Forward Secrecy (PFS) est une fonctionnalité qui améliore la sécurité d'une connexion VPN en s'assurant que chaque nouvelle clé de cryptage est

	sécurisée indépendamment, même si les clés précédentes sont compromises.
route set interface <nom-interface>	Lorsqu'une session VPN est établie avec succès, les routes définies dans la stratégie d'autorisation IKEv2 sont automatiquement ajoutées à la table de routage des périphériques. Cela garantit que le trafic destiné aux réseaux spécifiés dans l'ensemble de routes est correctement routé via le tunnel VPN.

4. Créer un profil IKEv2

Une stratégie IKEv2 (Internet Key Exchange version 2) est un ensemble de règles ou de paramètres utilisés pendant la phase IKEv2 d'établissement d'un tunnel VPN IPsec (Internet Protocol Security). IKEv2 est un protocole qui facilite l'échange sécurisé de clés et la négociation d'associations de sécurité (SA) entre deux parties souhaitant communiquer de manière sécurisée sur un réseau non fiable, tel qu'Internet. La stratégie IKEv2 définit la manière dont cette négociation doit avoir lieu, en spécifiant divers paramètres de sécurité sur lesquels les deux parties doivent se mettre d'accord pour établir un canal de communication sécurisé et chiffré.

Le profil IKEv2 DOIT avoir :

- Une méthode d'authentification locale et à distance.
- Une identité de correspondance ou un certificat de correspondance ou une instruction de correspondance.

```
crypto ikev2 profile uCPE-profile
 description uCPE profile
 match fvrf public-vrf
 match identity remote any
 authentication remote pre-share key ciscociscocisco123
 authentication local pre-share key ciscociscocisco123
 dpd 60 2 on-demand
 aaa authorization group psk list default uCPE-author-pol local
 virtual-template 1 mode auto
```

Where:

match fvrf public-vrf	Rendre un profil compatible avec le vrf.
match identity remote any	Mesure permettant de reconnaître une session entrante comme valide ; dans ce cas, n'importe qui.
authentification clé de pré-partage distante ciscociscocisco123	Spécifie que l'homologue distant doit être authentifié à l'aide de clés pré-partagées.
authentification clé de pré-partage locale ciscociscocisco123	Spécifie que ce périphérique (local) doit s'authentifier à l'aide de clés pré-partagées.
dpd 60 2 à la demande	Dead Peer Detection ; si aucun paquet n'a été reçu pendant une minute (60 secondes), envoyez 2 paquets dpd dans cet intervalle de 60 secondes.

aaa authorization group psk list default uCPE-author-pol local	Attribution de route.
virtual-template 1 mode auto	Lier à un virtual-template.

5. Créer un ensemble de transformations IPsec

Il définit un ensemble de protocoles et d'algorithmes de sécurité qui doivent être appliqués au trafic de données passant par le tunnel IPsec. Essentiellement, l'ensemble de transformation spécifie la manière dont les données doivent être chiffrées et authentifiées, assurant ainsi une transmission sécurisée entre les points d'extrémité VPN. Le mode tunnel configure le tunnel IPsec pour encapsuler l'intégralité du paquet IP afin de sécuriser le transport sur le réseau.

```
crypto ipsec transform-set tset_aes_256_sha512 esp-aes 256 esp-sha512-hmac
 mode tunnel
```

Where:

set transform-set <nom-jeu-transformation>	Spécifie les algorithmes de chiffrement et d'intégrité (par exemple, AES pour le chiffrement et SHA pour l'intégrité) qui doivent être utilisés pour protéger les données circulant dans le tunnel VPN.
set ikev2-profile <nom_profil_ikev2>	Définit les paramètres de négociation des associations de sécurité (SA) dans la phase 1 de la configuration VPN, y compris les algorithmes de chiffrement, les algorithmes de hachage, les méthodes d'authentification et le groupe Diffie-Hellman.
set pfs <group>	Paramètre facultatif qui, s'il est activé, garantit que chaque nouvelle clé de cryptage n'est liée à aucune clé précédente, améliorant ainsi la sécurité.

6. Supprimer le profil IPsec par défaut

La suppression du profil IPsec par défaut est une pratique adoptée pour plusieurs raisons liées à la sécurité, à la personnalisation et à la clarté du système. Le profil IPsec par défaut ne peut pas répondre aux stratégies ou exigences de sécurité spécifiques de votre réseau. Sa suppression garantit qu'aucun tunnel VPN n'utilise par inadvertance des paramètres non optimaux ou non sécurisés, réduisant ainsi le risque de vulnérabilités.

Chaque réseau a des exigences de sécurité uniques, notamment des algorithmes de chiffrement et de hachage, des longueurs de clé et des méthodes d’authentification spécifiques. La suppression du profil par défaut encourage la création de profils personnalisés adaptés à ces besoins spécifiques, garantissant ainsi une protection et des performances optimales.

```
no crypto ipsec profile default
```

7. Créez un profil IPsec et associez-le à un jeu de transformation et au profil IKEv2.

Un profil IPsec (Internet Protocol Security) est une entité de configuration qui encapsule les paramètres et les stratégies utilisés pour établir et gérer les tunnels VPN IPsec. Il sert de modèle pouvant être appliqué à plusieurs connexions VPN, en normalisant les paramètres de sécurité et en simplifiant la gestion des communications sécurisées sur un réseau.

```
crypto ipsec profile uCPE-ips-prof
 set security-association lifetime seconds 28800
 set security-association idle-time 1800
 set transform-set tset_aes_256_sha512
 set pfs group14
 set ikev2-profile uCPE-profile
```

8. Créer un modèle virtuel

L'interface Virtual-Template agit comme un modèle dynamique pour les interfaces d'accès virtuelles, offrant un moyen évolutif et efficace de gérer les connexions VPN. Il permet l'instanciation dynamique des interfaces d'accès virtuel. Lorsqu'une nouvelle session VPN est lancée, le périphérique crée une interface d'accès virtuel basée sur la configuration spécifiée dans le modèle virtuel. Ce processus prend en charge un grand nombre de clients et de sites distants en allouant dynamiquement des ressources en fonction des besoins, sans qu'il soit nécessaire de préconfigurer des interfaces physiques pour chaque connexion.

Grâce aux modèles virtuels, les déploiements FlexVPN peuvent évoluer efficacement à mesure que de nouvelles connexions sont établies, sans qu'il soit nécessaire de configurer manuellement chaque session individuelle.

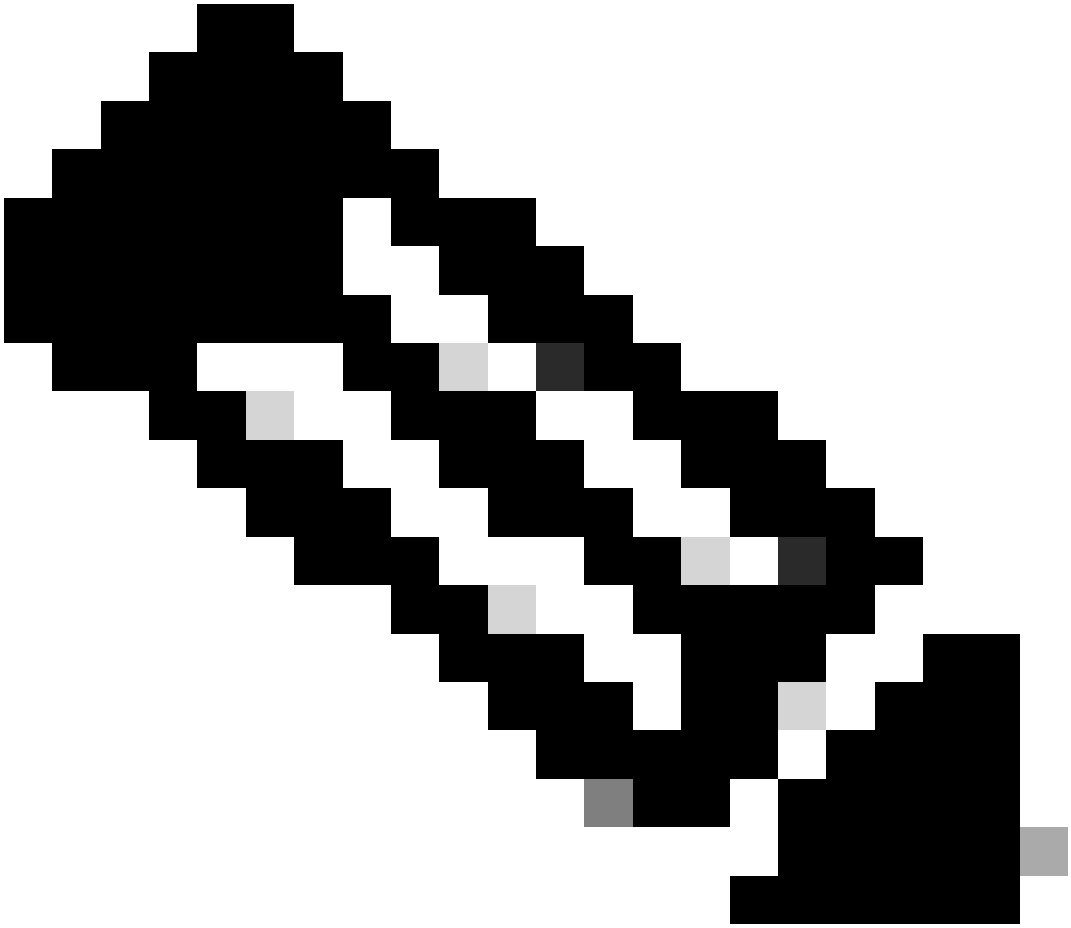
```
interface Virtual-Template1 type tunnel
 vrf forwarding private-vrf
 ip unnumbered Loopback1001
 ip mtu 1400
 ip tcp adjust-mss 1380
 tunnel mode ipsec ipv4
 tunnel vrf public-vrf
 tunnel protection ipsec profile uCPE-ips-prof
```

Configuration minimale de NFVIS Secure Overlay

Configurez l'instance secure-overlay

```
secure-overlay myconn local-bridge wan-br local-system-ip-addr 10.122.144.146 local-system-ip-subnet 10
```

```
ike-cipher aes256-sha512-modp4096 esp-cipher aes256-sha512-modp4096
psk local-psk ciscociscocisco123 remote-psk ciscociscocisco123
commit
```



> Remarque : lors de la configuration de l'annonce de route BGP sur un tunnel IPSec, assurez-vous que vous configurez la superposition sécurisée pour utiliser une adresse IP virtuelle (non originaire d'une interface physique ou d'un pont OVS) pour l'adresse IP du tunnel local. Pour l'exemple ci-dessus, voici les commandes d'adressage virtuel modifiées : local-system-ip-addr 10.122.144.146 local-system-ip-subnet 10.122.144.128/27

Vérifier l'état de superposition

```
show secure-overlay
secure-overlay myconn
 state                          up
 active-local-bridge            wan-br
```

```
 selected-local-bridge           wan-br
 active-local-system-ip-addr     10.122.144.146
 active-remote-interface-ip-addr 10.88.247.84
 active-remote-system-ip-addr    166.34.121.112
 active-remote-system-ip-subnet  166.34.121.112/32
 active-remote-id                10.88.247.84
```

Configuration de l'annonce de route BGP pour le serveur FlexVPN

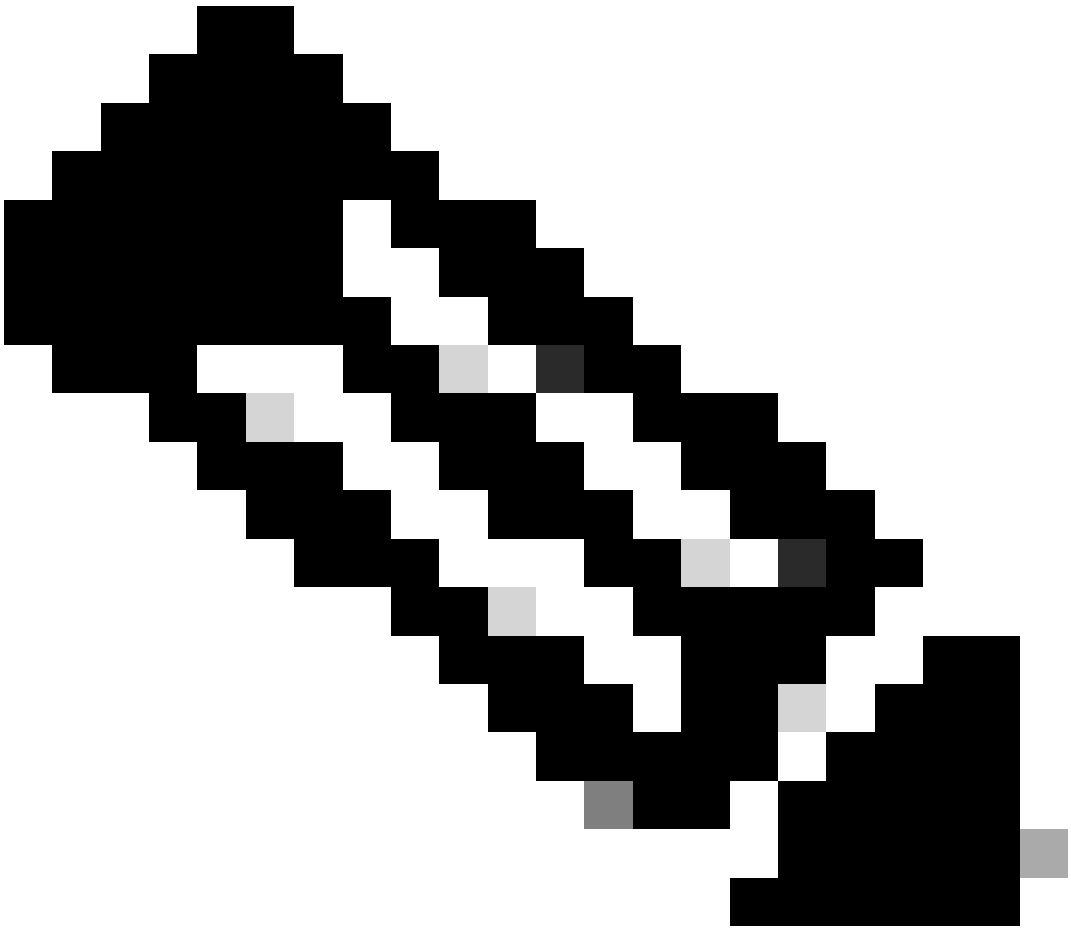
Cette configuration doit utiliser eBGP pour les homologues, où l'adresse source (adresse IP virtuelle pour l'adresse IP du tunnel local) du côté NFVIS doit être ajoutée à la plage d'écoute.

```
router bgp 65000
 bgp router-id 166.34.121.112
 bgp always-compare-med
 bgp log-neighbor-changes
 bgp deterministic-med
 bgp listen range 10.122.144.0/24 peer-group uCPEs
 bgp listen limit 255
 no bgp default ipv4-unicast
 address-family ipv4 vrf private-vrf
  redistribute connected
  redistribute static
  neighbor uCPEs peer-group
  neighbor uCPEs remote-as 200
  neighbor uCPEs ebgp-multihop 10
  neighbor uCPEs timers 610 1835
 exit-address-family
```

Where:

bgp always-compare-med	Configure le routeur pour qu'il compare toujours l'attribut MED (Multi-Exit Discriminator) pour toutes les routes, quel que soit leur AS d'origine.
bgp log-neighbor-changes	Active la journalisation des événements liés aux modifications dans les relations de voisinage BGP.
bgp deterministic-med	Assure la comparaison du MED pour les chemins des voisins dans différents systèmes autonomes.
plage d’écoute bgp <network>/<mask> peer-group <nom-groupe-homologue>	Active la détection dynamique des voisins dans la plage IP spécifiée (réseau/masque) et attribue les voisins détectés au nom du groupe d'homologues. Cela simplifie la configuration en appliquant des paramètres communs à tous les homologues du groupe.
bgp listen limit 255	Définit à 255 le nombre maximal de voisins BGP dynamiques pouvant être acceptés dans la plage d'écoute.
no bgp default ipv4-unicast	Désactive l'envoi automatique d'informations de routage de monodiffusion IPv4 aux voisins BGP, ce qui nécessite une configuration explicite pour l'activer.

redistribuer connecté	Redistribue les routes des réseaux connectés directement dans BGP (sous-réseaux privés du serveur FlexVPN qui appartiennent à private-vrf)
redistribute static	Redistribue les routes statiques dans BGP.
uCPE voisins ebgp-multihop 10	Permet aux connexions EBGP (External BGP) avec des homologues dans le groupe d'homologues de couvrir jusqu'à 10 sauts, utile pour connecter des périphériques non directement adjacents.
compteurs des uCPE voisins <keep-alive> <hold-down>	Définit les minuteurs de maintien de la connexion et de mise hors service BGP pour les voisins dans le groupe homologue respectivement (610 secondes et 1835 secondes pour l'exemple).



Remarque : une liste de préfixes sortants peut être configurée pour contrôler les annonces de routage de voisinage dans le groupe d'homologues : neighbor prefix-list out

Configuration BGP sur NFVIS

Démarrer le processus BGP avec les paramètres de voisinage eBGP

```
router bgp 200
 router-id 10.122.144.146
 neighbor 166.34.121.112 remote-as 65000
 commit
```

Révision BGP

Ce résultat révèle l'état d'une session BGP tel que rapporté par le démon de routage Internet BIRD. Ce logiciel de routage est responsable de la gestion des routes IP et de la prise de décisions concernant leur direction. D'après les informations fournies, il est clair que la session BGP est dans un état « établi », indiquant l'achèvement réussi du processus d'appairage BGP, et la session est actuellement active. Il a importé avec succès quatre routes et a noté qu'il existe une limite supérieure de 15 routes pouvant être importées.

```
nfvis# support show bgp
BIRD 1.6.8 ready.
name     proto    table    state  since       info
bgp_166_34_121_112 BGP      bgp_table_166_34_121_112 up     09:54:14    Established
  Preference:     100
  Input filter:   ACCEPT
  Output filter:  ACCEPT
  Import limit:   15
    Action:       disable
  Routes:         4 imported, 0 exported, 8 preferred
  Route change stats:     received   rejected   filtered    ignored   accepted
    Import updates:              4          0          0          0          4
    Import withdraws:            0          0        ---          0          0
    Export updates:              4          4          0        ---          0
    Export withdraws:            0        ---        ---        ---          0
  BGP state:          Established
    Neighbor address: 166.34.121.112
    Neighbor AS:      65000
    Neighbor ID:      166.34.121.112
    Neighbor caps:    refresh enhanced-refresh AS4
    Session:          external multihop AS4
    Source address:   10.122.144.146
    Route limit:      4/15
    Hold timer:       191/240
    Keepalive timer:  38/80
```

Assurez-vous que les sous-réseaux privés du serveur FlexVPN ont été annoncés via BGP

Lors de la configuration de l'annonce de route BGP, la seule combinaison configurable de famille d'adresses ou de transmission est ipv4 unicast pour IPSec. Pour afficher l'état BGP, la famille d'adresses configurable ou la transmission pour IPSec est vpnv4 unicast.

```
nfvis# show bgp vpnv4 unicast
Family Transmission Router ID       Local AS Number
vpnv4  unicast      10.122.144.146  200
```

Avec la commande show bgp vpnv4 unicast route, vous pouvez récupérer des informations sur les routes de monodiffusion VPNv4 connues du processus BGP.

```
nfvis# show bgp vpnv4 unicast route
Network            Next-Hop        Metric LocPrf Path
81.81.81.1/32      166.34.121.112  0      100    65000 ?
91.91.91.0/24      166.34.121.112  0      100    65000 ?
10.122.144.128/27  166.34.121.112  0      100    65000 ?
166.34.121.112/32  166.34.121.112  0      100    65000 ?
```

Pour le serveur VPN de tête de réseau, une vue d'ensemble de la configuration BGP et de l'état opérationnel peut être générée pour évaluer rapidement l'état et la configuration des sessions BGP.

```
c8000v# show ip bgp summary
Number of dynamically created neighbors in vrf private-vrf: 1/(100 max)
Total dynamically created neighbors: 1/(255 max), Subnet ranges: 1
```

En outre, des informations détaillées sur les entrées de la table de routage VPNv4 (VPN sur IPv4) gérées par BGP peuvent être affichées, elles doivent inclure des attributs spécifiques de chaque route VPNv4, tels que le préfixe de route, l'adresse IP de tronçon suivant, le numéro de système autonome d'origine et divers attributs BGP tels que la préférence locale, MED (Multi-Exit Discriminator) et les valeurs de communauté.

```
c8000v# show ip bgp vpnv4 all
BGP table version is 5, local router ID is 166.34.121.112
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, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 65000:7 (default for vrf private-vrf)
 *>   10.122.144.128/27
                      0.0.0.0                  0         32768 ?
 *>   81.81.81.1/32    0.0.0.0                  0         32768 ?
 *>   91.91.91.0/24    0.0.0.0                  0         32768 ?
 *>   166.34.121.112/32
                      0.0.0.0                  0         32768 ?
```

Dépannage

NFVIS (client FlexVPN)

Fichiers journaux NFVIS

Vous pouvez afficher tous les journaux d'initialisation et d'erreur pour les phases IPsec à partir du fichier journal NFVIS charon.log :

```
nfvis# show log charon.log
Feb  5 07:55:36.771 00[JOB] spawning 16 worker threads
Feb  5 07:55:36.786 05[CFG] received stroke: add connection 'myconn'
Feb  5 07:55:36.786 05[CFG] added configuration 'myconn'
Feb  5 07:55:36.787 06[CFG] received stroke: initiate 'myconn'
Feb  5 07:55:36.787 06[IKE] <myconn|1> initiating IKE_SA myconn[1] to 10.88.247.84
Feb  5 07:55:36.899 06[ENC] <myconn|1> generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_
Feb  5 07:55:36.899 06[NET] <myconn|1> sending packet: from 10.88.247.89[500] to 10.88.247.84[500] (741
Feb  5 07:55:37.122 09[NET] <myconn|1> received packet: from 10.88.247.84[500] to 10.88.247.89[500] (80
Feb  5 07:55:37.122 09[ENC] <myconn|1> parsed IKE_SA_INIT response 0 [ SA KE No V V V V N(NATD_S_IP) N(
Feb  5 07:55:37.122 09[IKE] <myconn|1> received Cisco Delete Reason vendor ID
Feb  5 07:55:37.122 09[ENC] <myconn|1> received unknown vendor ID: 43:49:53:43:4f:56:50:4e:2d:52:45:56:
Feb  5 07:55:37.122 09[ENC] <myconn|1> received unknown vendor ID: 43:49:53:43:4f:2d:44:59:4e:41:4d:49:
Feb  5 07:55:37.122 09[IKE] <myconn|1> received Cisco FlexVPN Supported vendor ID
Feb  5 07:55:37.122 09[CFG] <myconn|1> selected proposal: IKE:AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SH
Feb  5 07:55:37.235 09[IKE] <myconn|1> cert payload ANY not supported - ignored
Feb  5 07:55:37.235 09[IKE] <myconn|1> authentication of '10.88.247.89' (myself) with pre-shared key
Feb  5 07:55:37.235 09[IKE] <myconn|1> establishing CHILD_SA myconn{1}
Feb  5 07:55:37.236 09[ENC] <myconn|1> generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) IDr AUTH SA
Feb  5 07:55:37.236 09[NET] <myconn|1> sending packet: from 10.88.247.89[4500] to 10.88.247.84[4500] (4
Feb  5 07:55:37.322 10[NET] <myconn|1> received packet: from 10.88.247.84[4500] to 10.88.247.89[4500] (
Feb  5 07:55:37.322 10[ENC] <myconn|1> parsed IKE_AUTH response 1 [ V IDr AUTH SA TSi TSr N(SET_WINSIZE
Feb  5 07:55:37.323 10[IKE] <myconn|1> authentication of '10.88.247.84' with pre-shared key successful
Feb  5 07:55:37.323 10[IKE] <myconn|1> IKE_SA myconn[1] established between 10.88.247.89[10.88.247.89].
Feb  5 07:55:37.323 10[IKE] <myconn|1> scheduling rekeying in 86190s
Feb  5 07:55:37.323 10[IKE] <myconn|1> maximum IKE_SA lifetime 86370s
Feb  5 07:55:37.323 10[IKE] <myconn|1> received ESP_TFC_PADDING_NOT_SUPPORTED, not using ESPv3 TFC padd
Feb  5 07:55:37.323 10[CFG] <myconn|1> selected proposal: ESP:AES_CBC_256/HMAC_SHA2_512_256/NO_EXT_SEQ
Feb  5 07:55:37.323 10[IKE] <myconn|1> CHILD_SA myconn{1} established with SPIs cfc15900_i 49f5e23c_o a
Feb  5 07:55:37.342 11[NET] <myconn|1> received packet: from 10.88.247.84[4500] to 10.88.247.89[4500] (
Feb  5 07:55:37.342 11[ENC] <myconn|1> parsed INFORMATIONAL request 0 [ CPS(SUBNET VER U_PFS) ]
Feb  5 07:55:37.342 11[IKE] <myconn|1> Processing informational configuration payload CONFIGURATION
Feb  5 07:55:37.342 11[IKE] <myconn|1> Processing information configuration payload of type CFG_SET
Feb  5 07:55:37.342 11[IKE] <myconn|1> Processing attribute INTERNAL_IP4_SUBNET
Feb  5 07:55:37.342 11[ENC] <myconn|1> generating INFORMATIONAL response 0 [ ]
Feb  5 07:55:37.342 11[NET] <myconn|1> sending packet: from 10.88.247.89[4500] to 10.88.247.84[4500] (9
```

Routes injectées par strongSwan du noyau interne

Sous Linux, strongswan (implémentation IPsec multiplate-forme utilisée par NFVIS) installe les routes (y compris les routes de monodiffusion BGP VPNv4) dans la table de routage 220 par défaut et nécessite donc que le noyau prenne en charge le routage basé sur des stratégies.

```
nfvis# support show route 220
10.122.144.128/27 dev ipsec0 proto bird scope link
81.81.81.1 dev ipsec0 proto bird scope link
91.91.91.0/24 dev ipsec0 proto bird scope link
166.34.121.112 dev ipsec0 scope link
```

Vérifier l'état de l'interface IPsec0

Vous pouvez obtenir plus de détails sur l'interface virtuelle ipsec0 en utilisant ifconfig

```
nfvis# support show ifconfig ipsec0
ipsec0: flags=209<UP,POINTOPOINT,RUNNING,NOARP>  mtu 9196
        inet 10.122.144.146  netmask 255.255.255.255  destination 10.122.144.146
        tunnel   txqueuelen 1000  (IPIP Tunnel)
        RX packets 5105  bytes 388266 (379.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5105  bytes 389269 (380.1 KiB)
        TX errors 1  dropped 0 overruns 0  carrier 1  collisions 0
```

Tête de réseau (serveur FlexVPN)

Examiner les SA IPsec construites entre homologues

À partir du résultat ci-dessous, le tunnel chiffré est construit entre 10.88.247.84 via l'interface Virtual-Access1 et 10.88.247.89 pour le trafic qui va entre les réseaux 0.0.0.0/0 et 10.122.144.128/27 ; deux SA ESP (Encapsulating Security Payload) construites en entrée et en sortie.

```
c8000v# show crypto ipsec sa

interface: Virtual-Access1
    Crypto map tag: Virtual-Access1-head-0, local addr 10.88.247.84

   protected vrf: private-vrf
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (10.122.144.128/255.255.255.224/0/0)
   current_peer 10.88.247.89 port 4500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 218, #pkts encrypt: 218, #pkts digest: 218
    #pkts decaps: 218, #pkts decrypt: 218, #pkts verify: 218
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.88.247.84, remote crypto endpt.: 10.88.247.89
     plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
     current outbound spi: 0xC91BCDE0(3374042592)
```

```
     PFS (Y/N): Y, DH group: group16

     inbound esp sas:
      spi: 0xB80E6942(3087952194)
        transform: esp-256-aes esp-sha512-hmac ,
        in use settings ={Tunnel, }
        conn id: 2123, flow_id: CSR:123, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-he
         sa timing: remaining key lifetime (k/sec): (4607969/27078)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xC91BCDE0(3374042592)
        transform: esp-256-aes esp-sha512-hmac ,
        in use settings ={Tunnel, }
        conn id: 2124, flow_id: CSR:124, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-he
         sa timing: remaining key lifetime (k/sec): (4607983/27078)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

Afficher les sessions de cryptage actives

Le résultat de la commande show crypto session detail doit fournir des détails complets sur chaque session de chiffrement active, y compris le type de VPN (tel que site à site ou accès distant), les algorithmes de chiffrement et de hachage utilisés, et les associations de sécurité (SA) pour le trafic entrant et sortant. Comme il affiche également des statistiques sur le trafic chiffré et déchiffré, telles que le nombre de paquets et d'octets ; cela peut être utile pour surveiller la quantité de données sécurisées par le VPN et pour résoudre les problèmes de débit.

```
c8000v# show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN

Interface: Virtual-Access1
Profile: uCPE-profile
Uptime: 11:39:46
Session status: UP-ACTIVE
Peer: 10.88.247.89 port 4500 fvrf: public-vrf ivrf: private-vrf
      Desc: uCPE profile
      Phase1_id: 10.88.247.89
```

```
  Session ID: 1235
  IKEv2 SA: local 10.88.247.84/4500 remote 10.88.247.89/4500 Active
          Capabilities:D connid:2 lifetime:12:20:14
  IPSEC FLOW: permit ip   0.0.0.0/0.0.0.0 10.122.144.128/255.255.255.224
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 296 drop 0 life (KB/Sec) 4607958/7 hours, 20 mins
        Outbound: #pkts enc'ed 296 drop 0 life (KB/Sec) 4607977/7 hours, 20 mins
```

Réinitialiser les connexions VPN

Les commandes clear crypto sont utilisées pour réinitialiser manuellement les connexions VPN, ou effacer les associations de sécurité (SA) sans avoir besoin de redémarrer le périphérique entier.

- clear crypto ikev2 aurait effacé les associations de sécurité IKEv2 (IKEv2 SA).
- clear crypto session effacerait les SA IKEv1 (isakmp)/IKEv2 et IPSec.
- clear crypto sa effacerait uniquement les SA IPSec.
- clear crypto ipsec sa supprimerait les associations de sécurité IPSec actives.

Effectuer des débogages pour un dépannage supplémentaire

Les débogages IKEv2 peuvent aider à identifier et à dépanner les erreurs sur le périphérique de tête de réseau (c8000v) qui peuvent se produire pendant le processus de négociation IKEv2 et les connexions client FlexVPN, telles que les problèmes d'établissement de la session VPN, l'application de stratégie ou toute erreur spécifique au client.

```
c8000v# terminal no monitor
c8000v(config)# logging buffer 1000000
c8000v(config)# logging buffered debugging
c8000v# debug crypto ikev2 error
c8000v# debug crypto ikev2 internal
c8000v# debug crypto ikev2 client flexvpn
```

Articles et documentation associés

Superposition sécurisée et configuration IP unique

Prise en charge BGP sur NFVIS

Commandes Secure Overlay et BGP

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.