Configuration de BGP sur DMVPN Phase 3

Table des matières

Introduction

Ce document décrit la configuration et le fonctionnement de DMVPN Phase 3 à l'aide de BGP, y compris le dépannage en couches pour IPsec sur des tunnels DMVPN.

Conditions préalables

Pour les commandes de configuration et de débogage de ce document, vous avez besoin de deux routeurs Cisco qui exécutent Cisco IOS® version 15.3(3)M ou ultérieure. En général, un VPN multipoint dynamique (DMVPN) de base phase 3 nécessite Cisco IOS version 12.4(6)T, bien que les fonctionnalités et débogages présentés dans ce document ne soient pas entièrement pris en charge.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- IKEV1/IKEV2 et IPsec
- Composants DMVPN :

- Protocole NHRP (Next Hop Resolution Protocol) : Crée une base de données de mappage

distribuée (NHRP) de tous les tunnels du rayon vers des adresses réelles (interface publique)
- Interface de tunnel mGRE (Multipoint Generic Routing Encapsulation) : Interface GRE (Generic Routing Encapsulation) unique pour la prise en charge de plusieurs tunnels GRE/IPsec, simplifie la taille et la complexité de la configuration et prend en charge la création de tunnels dynamiques
- Protection du tunnel IPsec : Crée et applique dynamiquement des politiques de cryptage
- Routage : Réseaux dynamiques ; presque tous les protocoles de routage (Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol (RIP), Open Shortest Path First (OSPF), BGP, ODR) sont pris en charge

Composants utilisés

Les informations contenues dans ce document sont basées sur les routeurs à services d'agrégation de la gamme Cisco ASR1000, version 17.6.5(MD).

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.

Informations générales

Qu'est-ce que DMVPN ?

DMVPN est une solution logicielle Cisco IOS permettant de créer des VPN IPsec+GRE facilement, dynamiquement et de manière évolutive. Il s'agit d'une solution permettant de créer un réseau VPN avec plusieurs sites sans avoir à configurer tous les périphériques de manière statique. Il s'agit d'un réseau en étoile où les rayons peuvent communiquer directement entre eux sans passer par le concentrateur. Le cryptage est pris en charge par IPsec, ce qui fait du DMVPN un choix populaire pour connecter différents sites à l'aide de connexions Internet normales.

Comment fonctionne DMVPN ?

- Les rayons créent un tunnel GRE/IPsec permanent dynamique vers le concentrateur, mais pas vers les autres rayons. Ils s'enregistrent en tant que clients du serveur NHRP (concentrateur).
- Lorsqu'un rayon doit envoyer un paquet à un sous-réseau de destination (privé) derrière un autre rayon, il demande via NHRP l'adresse réelle (externe) du rayon de destination.
- Maintenant, le rayon d'origine peut initier un tunnel GRE/IPsec dynamique vers le rayon cible (parce qu'il connaît l'adresse de l'homologue).
- Le tunnel dynamique de rayon à rayon est construit sur l'interface mGRE.
- Lorsque le trafic cesse, le tunnel de rayon à rayon est supprimé.

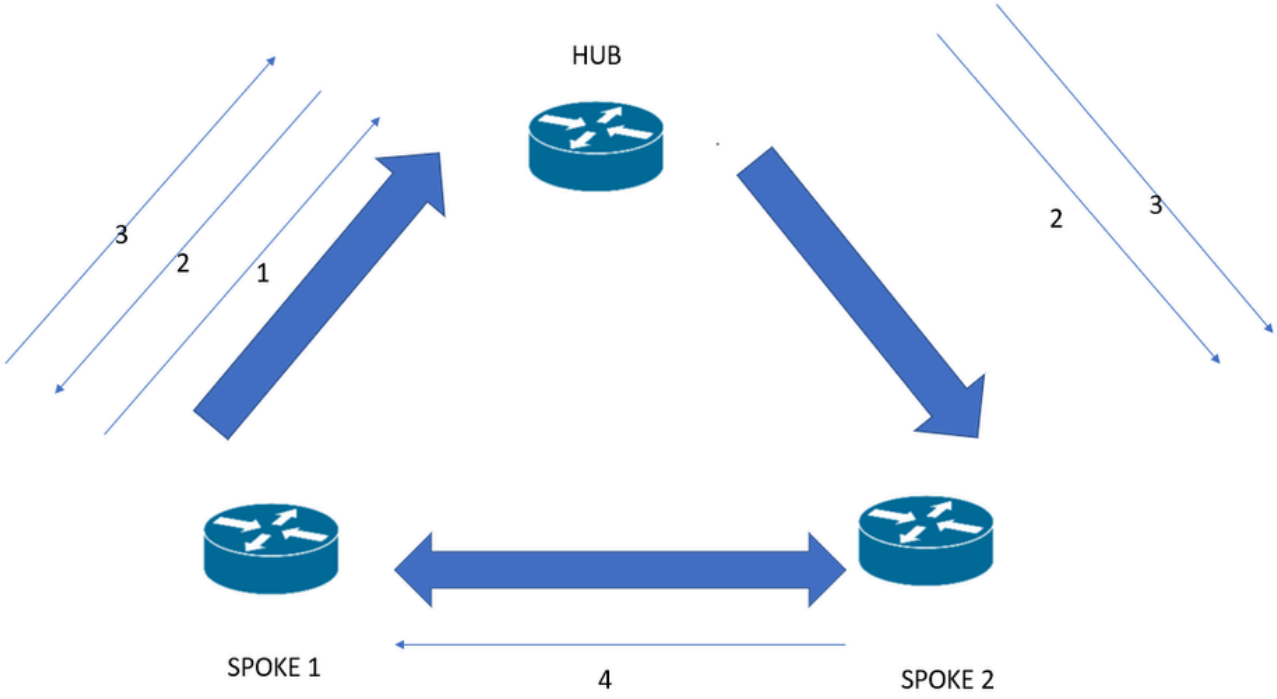
Quels sont les différents types de DMVPN ?

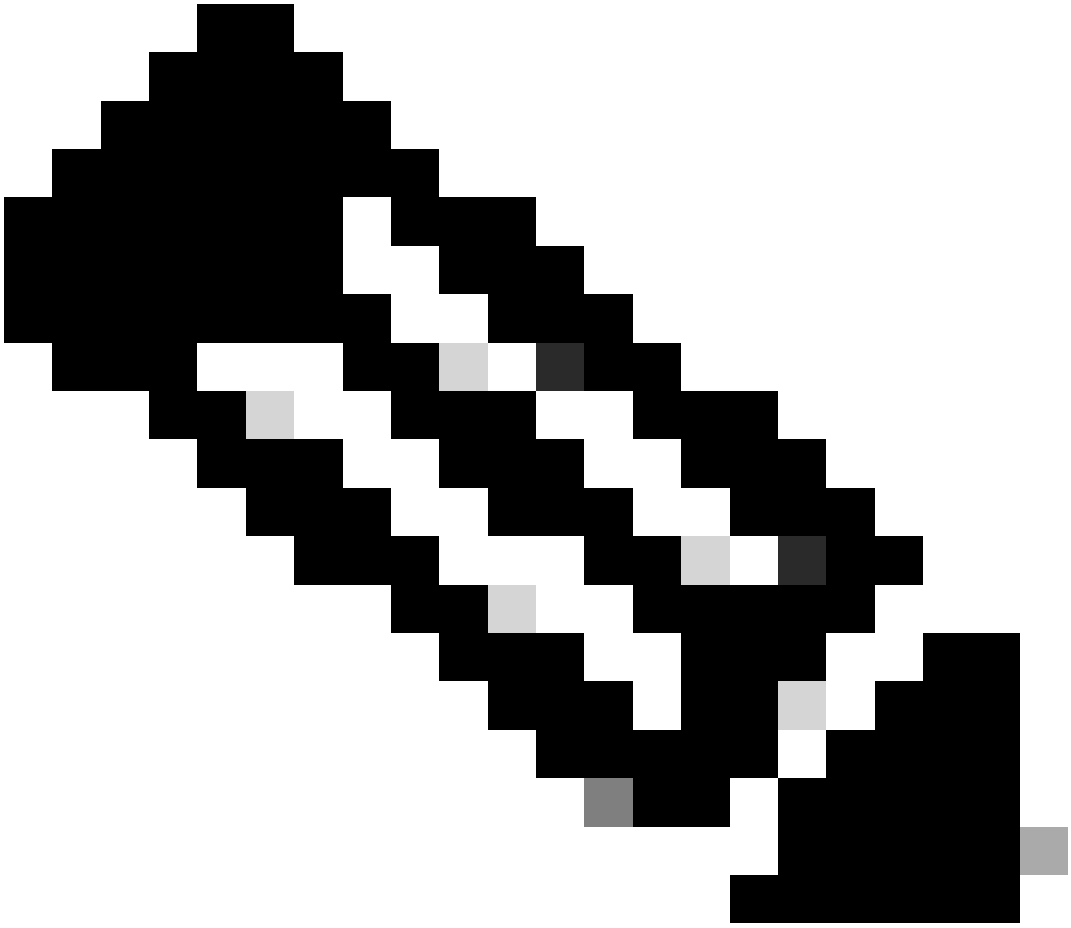
1. DMVPN phase I : Cette phase implique une interface mGRE unique sur le concentrateur, et

tous les rayons sont toujours des tunnels statiques, de sorte que vous n'obtenez aucune connectivité dynamique de rayon à rayon.
2. DMVPN phase II : Cette phase implique que chaque site soit configuré avec une interface mGRE afin que vous obteniez votre connectivité dynamique de rayon à rayon.
3. DMVPN Phase III : cette phase étend l'évolutivité du réseau DMVPN. Cela implique la récapitulation dans le cloud DMVPN. Avec la configuration des redirections NHRP et la commutation de raccourcis NHRP. Les redirections NHRP indiquent à la source de trouver un meilleur chemin vers la destination qu'elle tente d'atteindre. Les raccourcis NHRP permettent à DMVPN de découvrir d'autres réseaux derrière d'autres routeurs DMVPN.

Flux de trafic pour DMVPN Phase 3

1. Le paquet est envoyé du réseau 1 de Spoke aux 2 réseaux de Spoke via le concentrateur (selon la table de routage).
2. Le concentrateur achemine le paquet vers Spoke2 mais renvoie parallèlement le message de redirection NHRP vers Spoke1 contenant des informations sur le chemin sous-optimal vers Spoke2 et l'adresse IP du tunnel de Spoke2.
3. Spoke1 émet ensuite la requête de résolution NHRP de l'adresse IP NBMA (Nonbroadcast Multiaccess) 2 de Spoke vers le serveur de tronçon suivant (NHS) avec l'adresse IP de destination du tunnel Spoke 2. Cette demande de résolution NHRP est envoyée à Spoke2 via NHS (selon la table de routage). Il s'agit d'un processus normal de transfert NHRP saut par saut.
4. Spoke2, après réception de la demande de résolution incluant l'adresse IP NBMA de Spoke1, envoie la réponse de résolution NHRP directement à Spoke1 - Reply does not cross the Hub !
5. Spoke1 après avoir reçu l'adresse IP NBMA correcte de Spoke2 réécrit l'entrée CEF pour le préfixe de destination - cette procédure est appelée Raccourci NHRP.
6. Les rayons ne déclenchent pas NHRP en glanant des contiguïtés, mais les réponses NHRP mettent à jour le CEF.


HUB
3
2
1
2
3
SPOKE 1
4
SPOKE 2

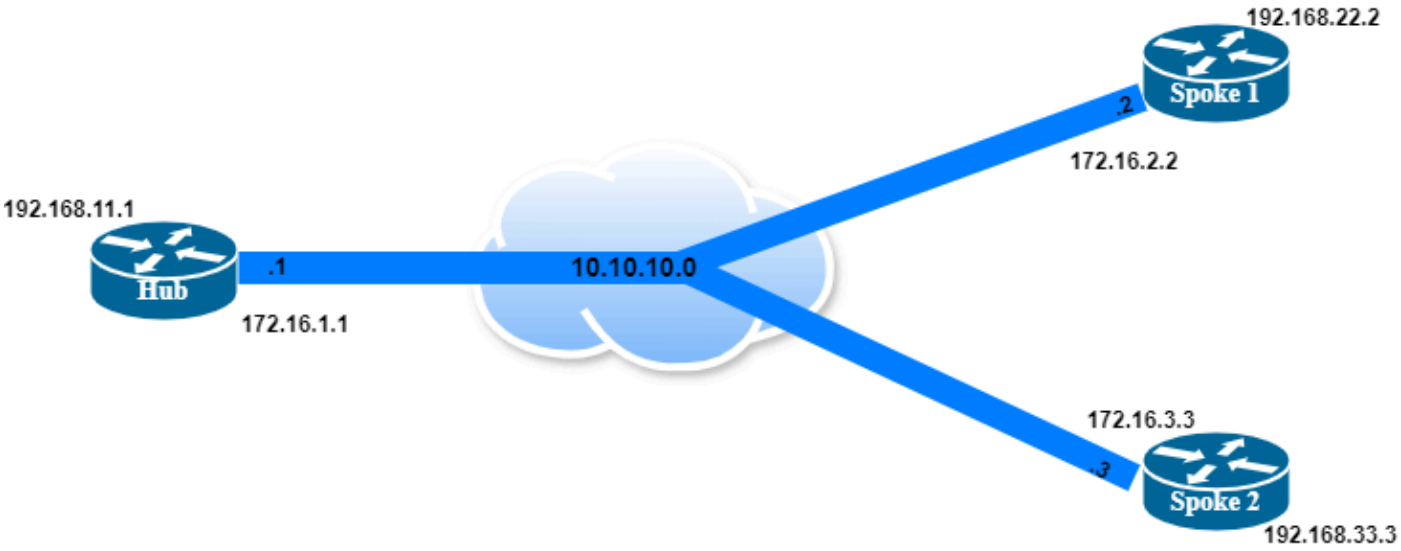


Remarque :

DMVPN Phase 2 : Dans cette phase, le paquet initial de rayon à rayon est en effet commuté par processus, car la contiguïté CEF est dans l'état « glean ». Cela signifie que le routeur ne dispose pas de suffisamment d'informations pour transférer le paquet à l'aide de CEF et doit utiliser une commutation de processus plus gourmande en ressources pour résoudre le saut suivant à l'aide du protocole NHRP (Next Hop Resolution Protocol).

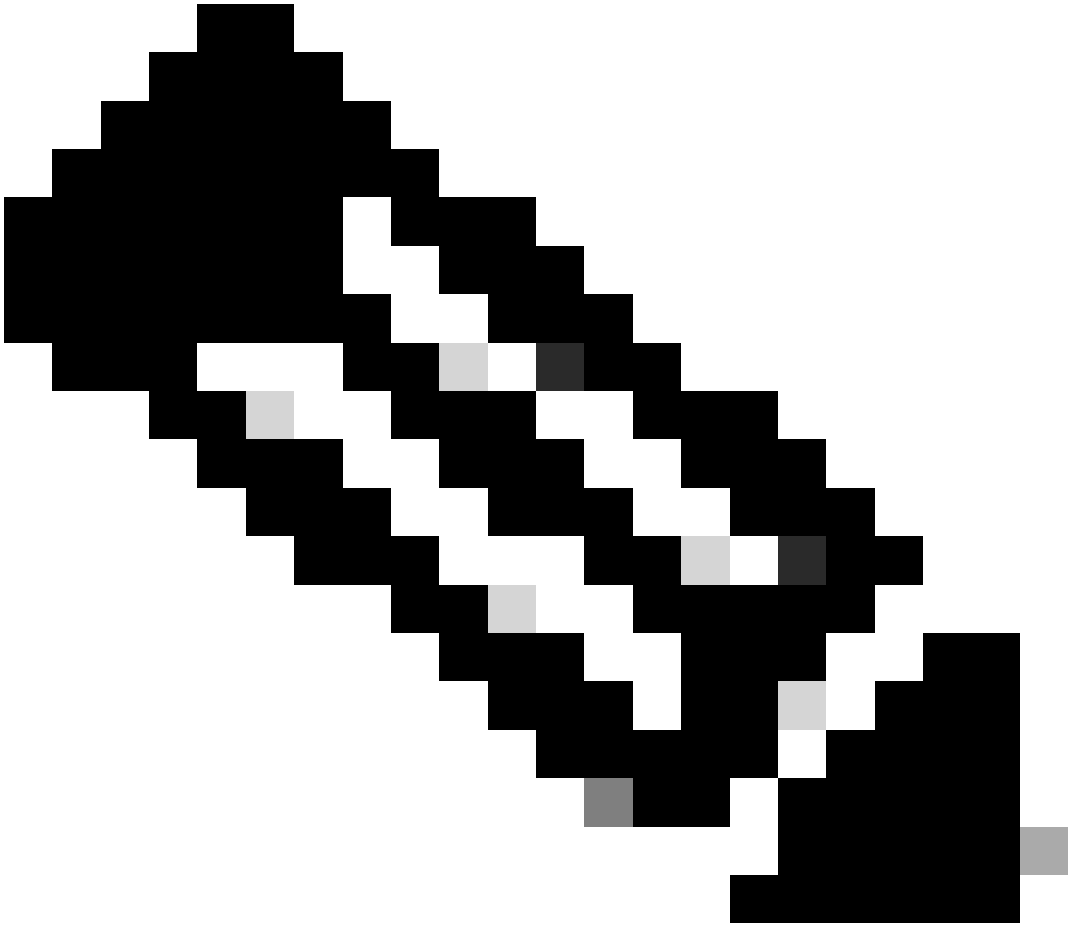
DMVPN Phase 3 : Cette phase améliore la phase 2 en permettant la commutation du paquet satellite à satellite initial à l’aide de CEF dès le début. Pour ce faire, les fonctions NHRP Redirect et NHRP Shortcut permettent d'établir rapidement des tunnels satellite à satellite directs. Par conséquent, le protocole CEF est utilisé de manière plus cohérente, ce qui réduit la dépendance vis-à-vis de la commutation de processus.

Diagramme du réseau



Configurations

Configurations de cryptage



Remarque : C'est la même chose sur le concentrateur et tous les rayons.

1. Configurez une proposition Ikev2 et un porte-clés.

```
crypto ikev2 proposition DMVPN
cryptage aes-cbc-256
intégrité sha256
groupe 14
crypto ikev2 porte-clés IKEV2-KEYRING
peer any
adresse 0.0.0.0 0.0.0.0
clé pré-partagée CISCO123
!
```

2. Configurez le profil Ikev2 qui contient toutes les informations relatives à la connexion.

```
crypto ikev2 profile IKEV2-PROF
```

match address interface locale GigabitEthernet0/0/0
match identity remote address 0.0.0.0
authentication local pre-share
authentication remote pre-share
porte-clés local IKEV2-KEYRING

Voici le détail des commandes utilisées dans le profil ikev2 :

- match address interface locale GigabitEthernet0/0/0 : Interface externe locale où le VPN se termine, dans ce cas, GigabitEthernet0/0/0
- match identity remote address 0.0.0.0 : Puisque l'homologue distant peut être multiple, utilisez 0.0.0.0 qui indique n'importe quel homologue
- prépartage local d'authentification : Le mode d'authentification sur le site local est pré-partagé
- prépartage à distance d'authentification : Le mode d'authentification sur le site local est pré-partagé
- keyring local IKEV2-KEYRING : Utilisez le même porte-clés que celui que vous avez créé précédemment.

3. Configurer le profil IPsec.

crypto ipsec transform-set T-SET esp-aes 256 esp-sha256-hmac
tunnel de mode

crypto ipsec profile IPSEC-IKEV2

set transform-set T-SET
set ikev2-profile IKEV2-PROF

Créez un jeu de transformation pour la négociation de tunnel IPsec et appelez le jeu de transformation et le profil Ikev2 sous le profil IPsec.

Configuration DMVPN

1. Configurez l'interface externe.

interface GigabitEthernet0/0/0

ip address 172.16.1.1 255.255.255.0
auto négociation
cdp enable

2. Configurer le routeur concentrateur pour l'intégration mGRE et IPsec (c'est-à-dire associer le tunnel au profil IPsec configuré dans la procédure précédente)

interface Tunnel0
ip address 10.10.10.1 255.255.255.0
no ip redirects

```
ip nhrp authentication DMVPN
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp redirect <-------- Obligatoire pour activer DMVPN Phase 3 sur le routeur concentrateur
source du tunnel GigabitEthernet0/0/0
tunnel mode gre multipoint
tunnel protection ipsec profile IPSEC-IKEV2
!
```

Ces commandes sont utilisées dans la configuration d'interface de tunnel :

- ip nhrp authentication DMVPN : Dans ce cas, la chaîne d'authentification « DMVPN » doit avoir la même valeur sur tous les concentrateurs et les rayons qui font partie du même réseau DMVPN.
- ip nhrp map multicast dynamic : Permet au protocole NHRP d'ajouter dynamiquement des rayons au mappage de multidiffusion NHRP.
- ip nhrp network-id 1 : Identificateur réseau 32 bits qui active le protocole NHRP sur une interface.
- ip nhrp redirect : Active l'indication de redirection du trafic si le trafic est transféré avec le réseau NHRP.
- source du tunnel GigabitEthernet0/0/0 : Définit l'adresse source d'une interface de tunnel, où vous utilisez l'adresse IP GigaEthernet 0/0/0.
- mode tunnel gre multipoint : Définit le mode d'encapsulation sur mGRE pour cette interface de tunnel.
- tunnel protection ipsec profile IPSEC-IKEV2 : Associe une interface de tunnel à un profil IPsec qui a déjà été créé dans des configurations de chiffrement.

3. Configurez les routeurs Spoke pour l'intégration de mGRE et IPsec avec une interface externe et un bouclage pour tester la connectivité BGP (Border Gateway Protocol).

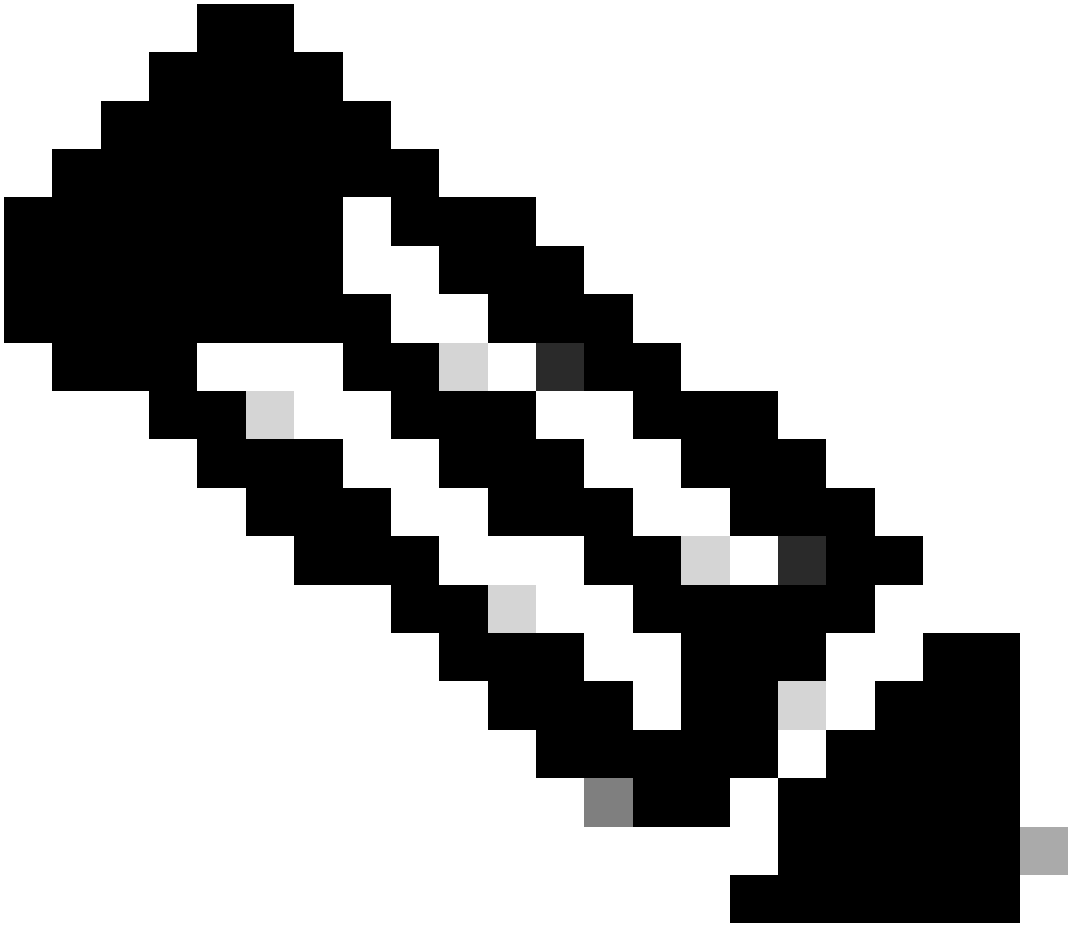
RAYON X : (Une configuration similaire peut être utilisée dans tous les rayons)

```
interface GigabitEthernet0/0/0
ip address 172.16.3.3 255.255.255.0
vitesse 1000
no negotiation auto

!

interface Loopback10
ip address 192.168.33.3 255.255.255.0
!
interface Tunnel0
ip address 10.10.10.3 255.255.255.0
no ip redirects
ip nhrp authentication DMVPN
ip nhrp map 10.10.10.1 172.16.1.1
ip nhrp map multicast 172.16.1.1
```

ip nhrp network-id 1
ip nhrp nhs 10.10.10.1
ip nhrp shortcut <-------- Obligatoire pour activer DMVPN Phase 3 sur le routeur satellite
source du tunnel GigabitEthernet0/0/0
tunnel mode gre multipoint
tunnel protection ipsec profile IPSEC-IKEV2

Ces commandes sont utilisées dans la configuration d'interface de tunnel :

- ip nhrp authentication DMVPN : Dans ce cas, la chaîne d'authentification « DMVPN » doit avoir la même valeur sur tous les concentrateurs et les rayons qui font partie du même réseau DMVPN.
- ip nhrp map 10.10.10.1 172.16.1.1 : Mappe manuellement l'adresse IP NBMA du concentrateur avec l'adresse IP de l'interface du tunnel.
- ip nhrp map multicast 172.16.1.1 : Redirige tout le trafic de multidiffusion vers le concentrateur.
- ip nhrp network-id 1 : Identificateur réseau 32 bits qui active le protocole NHRP sur une interface.
- ip nhrp nhs 10.10.10.1 : Le serveur de tronçon suivant qui est notre concentrateur est configuré à l'aide de cette commande.
- raccourci ip nhrp : Active la commutation de raccourcis NHRP sur une interface.
- source du tunnel GigabitEthernet0/0/0 : Définit l'adresse source d'une interface de tunnel, où vous utilisez l'adresse IP GigaEthernet 0/0/0.
- mode tunnel gre multipoint : Définit le mode d'encapsulation sur mGRE pour cette interface de tunnel.
- tunnel protection ipsec profile IPSEC-IKEV2 : Associe une interface de tunnel à un profil IPsec qui a déjà été créé dans des configurations de chiffrement.



Remarque : La commande ip nhrp redirect envoie le message aux satellites qui dit « Il y a une meilleure route vers le satellite de destination que via le concentrateur » et le raccourci ip nhrp impose l'installation de cette route dans la base d'informations de transfert (FIB) sur les satellites.

Configuration BGP

Vous avez le choix entre plusieurs variantes :

- eBGP avec un numéro de système autonome différent sur chaque rayon
- eBGP avec le même numéro AS sur chaque rayon
- iBGP

L'explication de ces trois scénarios sort du cadre de ce document.

Un eBGP avec un numéro de système autonome différent sur tous les rayons est configuré, de sorte que les voisins dynamiques ne peuvent pas être utilisés. Par conséquent, vous devez

configurer les voisins manuellement.

eBGP avec différents AS sur les satellites

1. Configuration BGP sur le concentrateur :

Concentrateur(config)#router bgp 65010

Hub(config-router)#bgp log-neighbor-changes

Concentrateur(config-router)#network 192.168.11.1 masque 255.255.255.255

Concentrateur(config-router)#neighbor 10.10.10.2 remote-as 65011

Concentrateur(config-router)#neighbor 10.10.10.3 remote-as 65012

!

Ces commandes sont utilisées dans la configuration BGP sur le concentrateur :

- routeur bgp 65010 : Configure un processus de routage BGP. Utilisez l'argument « numéro-système-autonome » qui identifie le périphérique aux autres haut-parleurs BGP.
- réseau 192.168.11.1 masque 255.255.255.255 : Spécifie un réseau en tant que réseau local pour ce système autonome et l'ajoute à la table de routage BGP.
- neighbor 10.10.10.2 remote-as 65011 : Ajoute l'adresse IP du satellite 1 voisin dans le système autonome spécifié à la table de voisinage BGP multiprotocole IPv4 du périphérique local.
- neighbor 10.10.10.3 remote-as 65012 : Ajoute l'adresse IP du satellite 2 voisin dans le système autonome spécifié à la table de voisinage BGP multiprotocole IPv4 du périphérique local.

2. Configuration BGP sur Spoke X :

Spoke2(config)#router bgp 65012

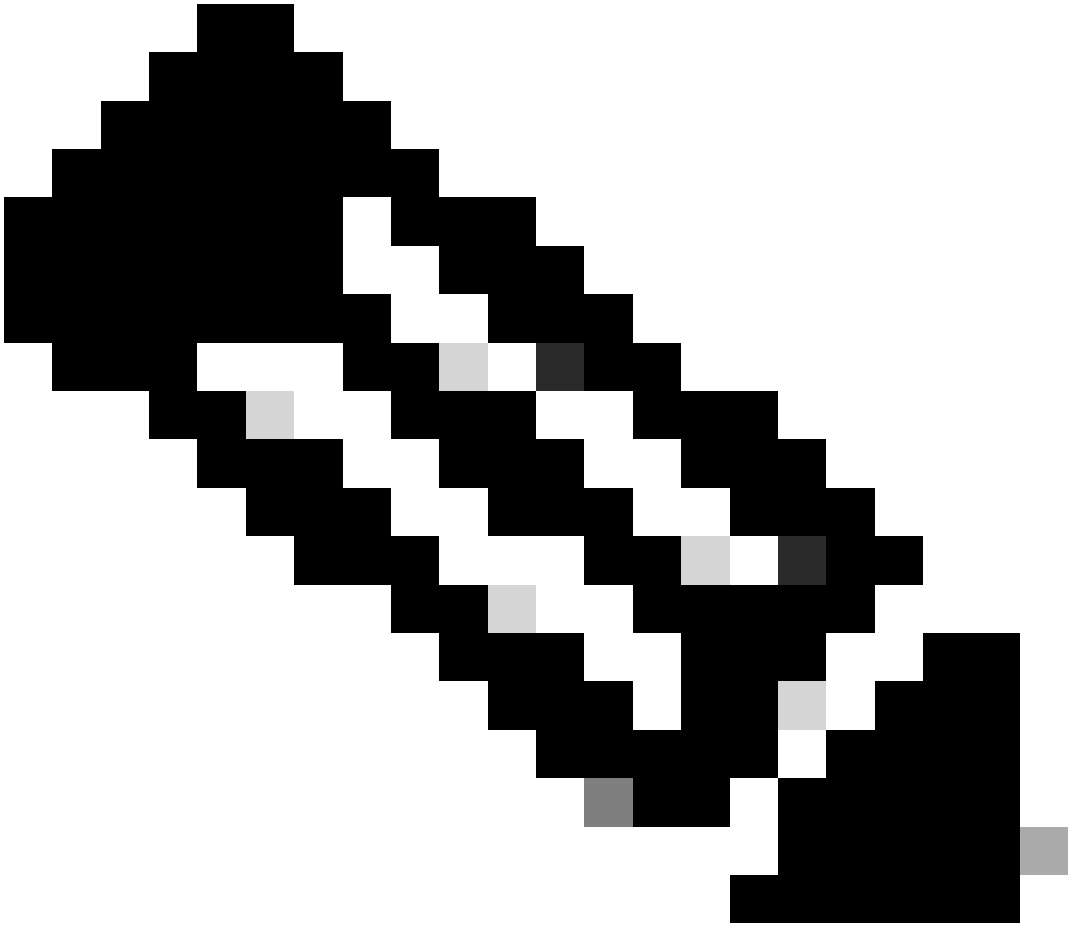
Spoke2(config-router) #bgp log-neighbor-changes

Spoke2(config-router)# network 192.168.33.3 mask 255.255.255.255

Spoke2(config-router)# neighbor 10.10.10.1 remote-as 65010

Ces commandes sont utilisées dans la configuration BGP sur Spoke X :

- routeur bgp 65012 : Configure un processus de routage BGP. Utilisez l'argument « numéro-système-autonome » qui identifie le périphérique aux autres haut-parleurs BGP.
- réseau 192.168.33.3 masque 255.255.255.255 : Spécifie un réseau en tant que réseau local pour ce système autonome et l'ajoute à la table de routage BGP.
- neighbor 10.10.10.1 remote-as 65010 : Ajoute l'adresse IP du concentrateur du système autonome spécifié à la table de voisinage BGP multiprotocole IPv4 du périphérique local.



Remarque : Une configuration similaire doit être effectuée sur tous les rayons du réseau DMVPN.

Vérifier

1. Commandes de vérification sur le périphérique Hub :

HUB#sh dmvpn

Affiche les informations de session spécifiques à DMVPN.

Légende : Attrb —> S - Statique, D - Dynamique, I - Incomplet
N - NATed, L - Local, X - Pas de socket
T1 - Route installée, T2 - Nexthop-override
C - Compatible CTS
Ent —> Nombre d'entrées NHRP avec le même homologue NBMA
État NHS : E —> Réponses attendues, R —> Réponse, W —> En attente

UpDn Time —> Up ou Down Time pour un tunnel
===

Interface: Tunnel0, IPv4 NHRP Details
Type : Hub, NHRP Peers : 2, <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< Informe que le périphérique agit en tant que concentrateur et que 2 homologues NHRP sont connectés à ce concentrateur.

Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- -------------- ----- -------- -----
1 172.16.2.2 10.10.10.2 UP 01:47:08 D <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< Les deux homologues ont été inscrits de manière dynamique auprès du concentrateur et sont à l'état UP.
1 172.16.3.3 10.10.10.3 UP 01:08:58 D

HUB#sh ip nhrp

Affiche le mappage d'adresse NBMA sur l'adresse IP de l'interface de tunnel de tous les homologues NHRP connectés au concentrateur. Le concentrateur gère la base de données de tous les rayons.

10.10.10.2/32 via 10.10.10.2
Tunnel0 créé 01:47:22, expire 01:32:27
type : dynamique, Indicateurs : nhop usagé enregistré unique
Adresse NBMA : 172.16.2.2
10.10.10.3/32 via 10.10.10.3
Tunnel0 créé 01:09:11, expire 01:29:58
type : dynamique, Indicateurs : nhop usagé enregistré unique
Adresse NBMA : 172.16.3.3

HUB#sh ip nhrp multicast

Affiche les informations de mappage multidiffusion NHRP.

Adresse NBMA I/F
Indicateurs du tunnel0 172.16.2.2 : dynamic (activé)
Tunnel0 172.16.3.3 Indicateurs : dynamic (activé)

HUB#sh crypto sockets

Nombre de connexions Crypto Socket 2

Homologues Tu0 (locaux/distants) : 172.16.1.1/172.16.2.2
Ident local (addr/mask/port/port) : (172.16.1.1/255.255.255.255/0/47)
Remote Ident (addr/mask/port/port) : (172.16.2.2/255.255.255.255/0/47)
Profil IPSec : "IPSEC-IKEV2"
État du socket : Open (ouvert)
Client : "TUNNEL SEC" (État du client : Actif)

Homologues Tu0 (locaux/distants) : 172.16.1.1/172.16.3.3
Ident local (addr/mask/port/port) : (172.16.1.1/255.255.255.255/0/47)
Remote Ident (addr/mask/port/port) : (172.16.3.3/255.255.255.255/0/47)
Profil IPSec : "IPSEC-IKEV2"
État du socket : Open (ouvert)
Client : "TUNNEL SEC" (État du client : Actif)
Sockets de chiffrement à l'état Listen :
Client : Profil « TUNNEL SEC » : Nom de mappage "IPSEC-IKEV2" : "Tunnel0-head-0"

HUB#sh cry ikev2 sa

SA IKEv2 de cryptage IPv4

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.1.1/500 172.16.2.2/500 aucun/aucun PRÊT
Encr : AES-CBC, taille de clé : 256, PRF : SHA512, Hachage : SHA512, DH Grp : 5, Signal d'authentification : PSK, Auth vérifier : PSK
Durée de vie/Durée active : 86400/6524 s

Tunnel-id Local Remote fvrf/ivrf Status
2 172.16.1.1/500 172.16.3.3/500 aucun/aucun PRÊT
Encr : AES-CBC, taille de clé : 256, PRF : SHA512, Hachage : SHA512, DH Grp : 5, Signal d'authentification : PSK, Auth vérifier : PSK
Durée de vie/Durée active : 86400/4234 s

SA IKEv2 de cryptage IPv6

HUB#sh ip bgp summary

Affiche l'état actuel de la session BGP/le nombre de préfixes que le routeur a reçus d'un voisin ou d'un groupe d'homologues.

Identificateur de routeur BGP 192.168.11.1 numéro de système autonome local 65010
La version de la table BGP est 4, la version de la table de routage principale est 4.
3 entrées réseau utilisant 432 octets de mémoire
3 entrées de chemin utilisant 252 octets de mémoire
3/3 entrées d'attribut path/bestpath BGP utilisant 480 octets de mémoire
2 entrées BGP AS-PATH utilisant 48 octets de mémoire
0 entrées de cache de route-map BGP utilisant 0 octet de mémoire
0 entrée de cache de liste de filtres BGP utilisant 0 octet de mémoire
BGP utilisant un total de 1212 octets de mémoire
Exercice BGP : préfixes 3/0, chemins 3/0, intervalle d'analyse de 60 secondes

Voisin V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.10.2 4 65011 33 33 4 0 0 0 00:25:35 1
10.10.10.3 4 65012 21 25 4 0 0 0 00:14:58 1

Hub#sh ip route bgp

Codes : L - local, C - connecté, S - statique, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP externe, O - OSPF, IA - OSPF inter-zone
N1 - OSPF NSSA de type externe 1, N2 - OSPF NSSA de type externe 2
E1 - type externe OSPF 1, E2 - type externe OSPF 2
i - IS-IS, su - Résumé IS-IS, L1 - IS-IS niveau 1, L2 - IS-IS niveau 2
ia - IS-IS inter-zone, * - candidat default, U - route statique par utilisateur
o - ODR, P - route statique téléchargée périodiquement, H - NHRP, l - LISP
a - route d'application
+ - route répliquée, % - saut suivant, p - remplacements depuis PfR

La passerelle de dernier recours est 172.16.1.2 vers le réseau 0.0.0.0

192.168.0.0/16 est divisé en sous-réseaux variables, 4 sous-réseaux, 2 masques
B 192.168.22.0/24 [20/0] via 10.10.10.2, 00:29:15 <<<<<<<<<<<<<<<Entrée pour les routes annoncées du satellite 1
B 192.168.33.0/24 [20/0] via 10.10.10.3, 00:18:37 <<<<<<<<<<<<<<<Entrée pour les routes annoncées du satellite 2

2. Commandes de vérification sur le satellite 1 :

Spoke1#sh dmvpn

Légende : Attrb —> S - Statique, D - Dynamique, I - Incomplet
N - NATed, L - Local, X - Pas de socket
T1 - Route installée, T2 - Nexthop-override
C - CTS Capable, I2 - Temporaire
Ent —> Nombre d'entrées NHRP avec le même homologue NBMA
État NHS : E —> Réponses attendues, R —> Réponse, W —> En attente
UpDn Time —> Up ou Down Time pour un tunnel
==========

Interface: Tunnel0, IPv4 NHRP Details
Type : Spoke, homologues NHRP : 2,

Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.10.10.1 UP 01:32:09 S <<<<<<<<<<<<<Le concentrateur s'affiche comme S-statique, car nous l'avons configuré comme entrée statique sous l'interface de tunnel
1 172.16.3.3 10.10.10.3 UP 00:19:34 D <<<<<<<<<<< Tunnel dynamique Spoke to Spoke à la demande créé après l'envoi du trafic vers Spoke 2

Spoke1#sh ip bgp summary

Identificateur de routeur BGP 192.168.22.2, numéro de système autonome local 65011
La version de la table BGP est 4, la version de la table de routage principale est 4.
3 entrées réseau utilisant 744 octets de mémoire
3 entrées de chemin utilisant 432 octets de mémoire

3/3 entrées d'attribut path/bestpath BGP utilisant 864 octets de mémoire
2 entrées BGP AS-PATH utilisant 64 octets de mémoire
0 entrées de cache de route-map BGP utilisant 0 octet de mémoire
0 entrée de cache de liste de filtres BGP utilisant 0 octet de mémoire
BGP utilisant un total de 2104 octets de mémoire
Exercice BGP : préfixes 3/0, chemins 3/0, intervalle d'analyse de 60 secondes
3 networks peaked at 08:16:54 Jun 2 2022 UTC (il y a 01:11:51.732)

Voisin V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.10.1 4 65010 85 85 4 0 0 0 1:12:21 2 **<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<**
Nous avons reçu 2 préfixes du concentrateur, chacun pour le bouclage du concentrateur et le bouclage Spoke2

Spoke1#sh ip route bgp

Codes : L - local, C - connecté, S - statique, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP externe, O - OSPF, IA - OSPF inter-zone
N1 - OSPF NSSA de type externe 1, N2 - OSPF NSSA de type externe 2
E1 - OSPF de type externe 1, E2 - OSPF de type externe 2, m - OMP
n - NAT, Ni - NAT interne, Non - NAT externe, Nd - NAT DIA
i - IS-IS, su - Résumé IS-IS, L1 - IS-IS niveau 1, L2 - IS-IS niveau 2
ia - IS-IS inter-zone, * - candidat default, U - route statique par utilisateur
H - NHRP, G - NHRP homologué, g - Résumé de l'homologation NHRP
o - ODR, P - route statique téléchargée périodiquement, l - LISP
a - route d'application
+ - route répliquée, % - saut suivant, p - remplacements depuis PfR

La passerelle de dernier recours est 172.16.2.10 vers le réseau 0.0.0.0

B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:13:16 **>>>>>>>>>>>>>>>>>>** Réseau de concentrateur accessible directement via le concentrateur

B 192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:46 **>>>>>>>>>>>>>>>>>>** Réseau satellite directement accessible via IP du tunnel satellite.

Spoke1#sh ip route

Codes : L - local, C - connecté, S - statique, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP externe, O - OSPF, IA - OSPF inter-zone
N1 - OSPF NSSA de type externe 1, N2 - OSPF NSSA de type externe 2
E1 - OSPF de type externe 1, E2 - OSPF de type externe 2, m - OMP
n - NAT, Ni - NAT interne, Non - NAT externe, Nd - NAT DIA
i - IS-IS, su - Résumé IS-IS, L1 - IS-IS niveau 1, L2 - IS-IS niveau 2
ia - IS-IS inter-zone, * - candidat default, U - route statique par utilisateur
H - NHRP, G - NHRP homologué, g - Résumé de l'homologation NHRP
o - ODR, P - route statique téléchargée périodiquement, l - LISP
a - route d'application

+ - route répliquée, % - saut suivant, p - remplacements depuis PfR

La passerelle de dernier recours est 172.16.2.10 vers le réseau 0.0.0.0

S* 0.0.0.0/0 [1/0] via 172.16.2.10
172.16.2.0/24 est divisé en sous-réseaux variables, 2 sous-réseaux, 2 masques
C 172.16.2.0/24 est directement connecté, GigabitEthernet2
L 172.16.2.2/32 est directement connecté, GigabitEthernet2
10.0.0.0/8 est divisé en sous-réseaux variables, 2 sous-réseaux, 2 masques
C 10.10.10.0/24 est directement connecté, Tunnel0
L 10.10.10.2/32 est directement connecté, Tunnel0
B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:13:21
192.168.22.0/24 est divisé en sous-réseaux variables, 2 sous-réseaux, 2 masques
C 192.168.22.0/24 est directement connecté, Bouclage10
L 192.168.22.2/32 est directement connecté, Bouclage10
B 192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:51

Spoke1#sh ip nhrp nhs

Légende : E=Réponses attendues, R=Répondre, W=En attente, D=Dynamique
Tunnel0 :
10.10.10.1 RE priority = 0 cluster = 0 **>>>>>>>>>>>>>>** Un seul serveur de tronçon suivant est configuré

Spoke1#sh ip nhrp traffic

Tunnel0 : Limite d'envoi max. :10000Paquets/10 sec, utilisation : 0 %
Envoyé : Total 52
1 Demande de résolution 0 Réponse de résolution 51 Demande d’enregistrement **<<<<<<<<<**
Nombre de fois où les demandes d’enregistrement ont été envoyées au concentrateur
0 Réponse d'inscription 0 Demande de purge 0 Réponse de purge
0 Indication d'erreur 0 Indication de trafic 0 Redirection Supprimer
Rcvd : Total 25
0 Demande de résolution 1 Réponse de résolution 0 Demande d’enregistrement
<<<<<<<<<<<<< Nombre de fois où nous avons reçu des réponses à ces demandes d’enregistrement
24 Réponse d'inscription 0 Demande de purge 0 Réponse de purge
0 Indication d'erreur 0 Indication de trafic 0 Redirection Supprimer

Spoke1#sh ip nhrp multicast

Adresse NBMA I/F
Tunnel0 172.16.1.1 Indicateurs : static (Enabled) **<<<<<<<<<<<** Le trafic multidiffusion est configuré pour être transféré vers le concentrateur NBMA

Spoke1#sh crypto sockets

Nombre de connexions Crypto Socket 2

Homologues Tu0 (locaux/distants) : 172.16.2.2/172.16.1.1
Ident local (addr/mask/port/port) : (172.16.2.2/255.255.255.255/0/47)
Remote Ident (addr/mask/port/port) : (172.16.1.1/255.255.255.255/0/47)
Profil IPSec : "IPSEC-IKEV2"
État du socket : Ouvrir <<<<<<<<<<<<<<<<<<<<<<<< État du socket pour cet homologue particulier
Client : "TUNNEL SEC" (État du client : Actif)
Homologues Tu0 (locaux/distants) : 172.16.2.2/172.16.3.3
Ident local (addr/mask/port/port) : (172.16.2.2/255.255.255.255/0/47)
Remote Ident (addr/mask/port/port) : (172.16.3.3/255.255.255.255/0/47)
Profil IPSec : "IPSEC-IKEV2"
État du socket : Open (ouvert)
Client : "TUNNEL SEC" (État du client : Actif)
Sockets de chiffrement à l'état Listen :
Client : Profil « TUNNEL SEC » : Nom de mappage "IPSEC-IKEV2" : "Tunnel0-head-0"

Spoke1#sh cry ikev2 sa

SA IKEv2 de cryptage IPv4

Tunnel-id Local Remote fvrf/ivrf Status
2 172.16.2.2/500 172.16.3.3/500 aucun/aucun PRÊT
Encr : AES-CBC, taille de clé : 256, PRF : SHA512, Hachage : SHA512, DH Grp : 19, Signal d'authentification : PSK, Auth vérifier : PSK
Durée de vie/Durée active : 86400/287 s

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.2.2/500 172.16.1.1/500 aucun/aucun PRÊT
Encr : AES-CBC, taille de clé : 256, PRF : SHA512, Hachage : SHA512, DH Grp : 19, Signal d'authentification : PSK, Auth vérifier : PSK
Durée de vie/Durée active : 86400/4643 s

SA IKEv2 de cryptage IPv6

Spoke1#traceroute 192.168.33.3 source lo10

Tapez la séquence d'échappement à abandonner.
Traçage de la route vers 192.168.33.3
Informations VRF : (vrf in name/id, vrf out name/id)
1 10.10.10.3 3 ms 4 ms * <<<<<<<<<<<<<<<<<<< Le trafic est acheminé directement vers le routeur Spoke 2 sans passer par le concentrateur.

Spoke2#sh dmvpn

Légende : Attrb —> S - Statique, D - Dynamique, I - Incomplet
N - NATed, L - Local, X - Pas de socket
T1 - Route installée, T2 - Nexthop-override
C - CTS Capable, I2 - Temporaire
Ent —> Nombre d'entrées NHRP avec le même homologue NBMA
État NHS : E —> Réponses attendues, R —> Réponse, W —> En attente
UpDn Time —> Up ou Down Time pour un tunnel
==========

Interface: Tunnel0, IPv4 NHRP Details
Type : Spoke, homologues NHRP : 2,

Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.10.10.1 À 01:20:26 S
1 172.16.2.2 10.10.10.2 UP 00:07:51 D

3. Commandes de vérification sur le satellite 2 :

Spoke2#sh ip nhrp

10.10.10.1/32 via 10.10.10.1
Tunnel0 créé 01:36:06, ne jamais expirer
type : statique, Indicateurs :
Adresse NBMA : 172.16.1.1
10.10.10.2/32 via 10.10.10.2
Tunnel0 créé 00:08:09, expire 00:01:50
type : dynamique, Indicateurs : routeur implicite
Adresse NBMA : 172.16.2.2
10.10.10.3/32 via 10.10.10.3
Tunnel0 créé 00:08:09, expire 00:01:50
type : dynamique, Indicateurs : routeur local unique
Adresse NBMA : 172.16.3.3
(sans socket)
Spoke2#sh ip nhrp mul
Spoke2#sh ip nhrp multicast
Adresse NBMA I/F
Indicateurs du tunnel0 172.16.1.1 : static (Activé)
Spoke2#

Spoke2#sh crypto sockets

Nombre de connexions Crypto Socket 2

Homologues Tu0 (locaux/distants) : 172.16.3.3/172.16.1.1
Ident local (addr/mask/port/port) : (172.16.3.3/255.255.255.255/0/47)
Remote Ident (addr/mask/port/port) : (172.16.1.1/255.255.255.255/0/47)

Profil IPSec : "IPSEC-IKEV2"
État du socket : Ouvrir <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< État du socket pour cet homologue particulier
Client : "TUNNEL SEC" (État du client : Actif)
Homologues Tu0 (locaux/distants) : 172.16.3.3/172.16.2.2
Ident local (addr/mask/port/port) : (172.16.3.3/255.255.255.255/0/47)
Remote Ident (addr/mask/port/port) : (172.16.2.2/255.255.255.255/0/47)
Profil IPSec : "IPSEC-IKEV2"
État du socket : Open (ouvert)
Client : "TUNNEL SEC" (État du client : Actif)
Sockets de chiffrement à l'état Listen :
Client : Profil « TUNNEL SEC » : Nom de mappage "IPSEC-IKEV2" : "Tunnel0-head-0"

Spoke2#sh cry ikev2 sa

SA IKEv2 de cryptage IPv4

Tunnel-id Local Remote fvrf/ivrf Status
2 172.16.3.3/500 172.16.2.2/500 aucun/aucun PRÊT
Encr : AES-CBC, taille de clé : 256, PRF : SHA512, Hachage : SHA512, DH Grp : 19, Signal d'authentification : PSK, Auth vérifier : PSK
Durée de vie/Durée active : 86400/509 s

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.3.3/500 172.16.1.1/500 aucun/aucun PRÊT
Encr : AES-CBC, taille de clé : 256, PRF : SHA512, Hachage : SHA512, DH Grp : 19, Signal d'authentification : PSK, Auth vérifier : PSK
Durée de vie/Durée active : 86400/4866 s

SA IKEv2 de cryptage IPv6

Spoke2#sh ip bgp summary

Identificateur de routeur BGP 192.168.33.3, numéro de système autonome local 65012
La version de la table BGP est 4, la version de la table de routage principale est 4.
3 entrées réseau utilisant 744 octets de mémoire
3 entrées de chemin utilisant 432 octets de mémoire
3/3 entrées d'attribut path/bestpath BGP utilisant 864 octets de mémoire
2 entrées BGP AS-PATH utilisant 64 octets de mémoire
0 entrées de cache de route-map BGP utilisant 0 octet de mémoire
0 entrée de cache de liste de filtres BGP utilisant 0 octet de mémoire
BGP utilisant un total de 2104 octets de mémoire
Exercice BGP : préfixes 3/0, chemins 3/0, intervalle d'analyse de 60 secondes
3 networks peaked at 08:16:54 Jun 2 2022 UTC (il y a 01:20:43.775)

Voisin V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.10.1 465010 97 94 4 0 0 01:21:07 2 >>>>>>>>>>>>>>>>>>>>>. Nous avons reçu 2 préfixes du concentrateur, chacun pour le bouclage du concentrateur et le bouclage Spoke2

Spoke2#sh ip route

Codes : L - local, C - connecté, S - statique, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP externe, O - OSPF, IA - OSPF inter-zone
N1 - OSPF NSSA de type externe 1, N2 - OSPF NSSA de type externe 2
E1 - OSPF de type externe 1, E2 - OSPF de type externe 2, m - OMP
n - NAT, Ni - NAT interne, Non - NAT externe, Nd - NAT DIA
i - IS-IS, su - Résumé IS-IS, L1 - IS-IS niveau 1, L2 - IS-IS niveau 2
ia - IS-IS inter-zone, * - candidat default, U - route statique par utilisateur
H - NHRP, G - NHRP homologué, g - Résumé de l'homologation NHRP
o - ODR, P - route statique téléchargée périodiquement, l - LISP
a - route d'application
+ - route répliquée, % - saut suivant, p - remplacements depuis PfR

La passerelle de dernier recours est 172.16.3.10 vers le réseau 0.0.0.0

S* 0.0.0.0/0 [1/0] via 172.16.3.10
172.16.3.0/24/8 est divisé en sous-réseaux variables, 2 sous-réseaux, 2 masques
C 172.16.3.0/24 est directement connecté, GigabitEthernet3
L 172.16.3.3/32 est directement connecté, GigabitEthernet3
10.0.0.0/8 est divisé en sous-réseaux variables, 2 sous-réseaux, 2 masques
C 10.10.10.0/24 est directement connecté, Tunnel0
L 10.10.10.3/32 est directement connecté, Tunnel0
B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:47:08
B 192.168.22.0/24 [20/0] via 10.10.10.2, 01:46:45
192.168.33.0/24 est divisé en sous-réseaux variables, 2 sous-réseaux, 2 masques
C 192.168.33.0/24 est directement connecté, Bouclage10
L 192.168.33.3/32 est directement connecté, Bouclage10

Spoke2#sh ip route bgp

Codes : L - local, C - connecté, S - statique, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP externe, O - OSPF, IA - OSPF inter-zone
N1 - OSPF NSSA de type externe 1, N2 - OSPF NSSA de type externe 2
E1 - OSPF de type externe 1, E2 - OSPF de type externe 2, m - OMP
n - NAT, Ni - NAT interne, Non - NAT externe, Nd - NAT DIA
i - IS-IS, su - Résumé IS-IS, L1 - IS-IS niveau 1, L2 - IS-IS niveau 2
ia - IS-IS inter-zone, * - candidat default, U - route statique par utilisateur
H - NHRP, G - NHRP homologué, g - Résumé de l'homologation NHRP
o - ODR, P - route statique téléchargée périodiquement, l - LISP
a - route d'application
+ - route répliquée, % - saut suivant, p - remplacements depuis PfR

La passerelle de dernier recours est 172.16.3.10 vers le réseau 0.0.0.0

B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:21:11 **>>>>>>>>>>>>>>>>**Réseau concentrateur accessible directement via le concentrateur

B 192.168.22.0/24 [20/0] via 10.10.10.2, 01:20:48 >>>>>>>>>>>>>>>>> Réseau satellite directement accessible via IP du tunnel satellite.

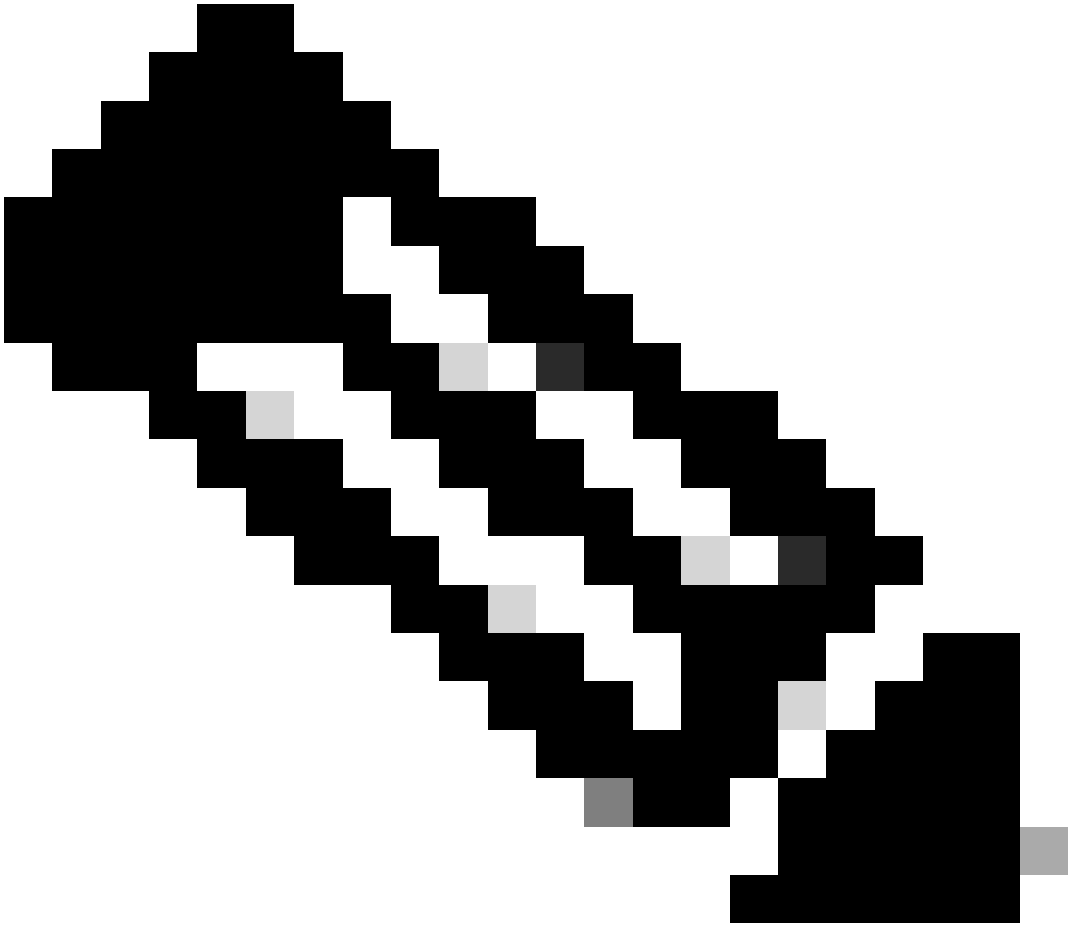
Spoke2#sh ip nhrp nhs

Légende : E=Réponses attendues, R=Répondre, W=En attente, D=Dynamique
Tunnel0 :
10.10.10.1 RE priority = 0 cluster = 0 >>>>>>>>>>>>>>>>>> Un seul serveur de tronçon suivant est configuré

Spoke2#traceroute 192.168.22.2 bouclage source 10

Tapez la séquence d'échappement à abandonner.
Traçage de la route vers 192.168.22.2
Informations VRF : (vrf in name/id, vrf out name/id)
1 10.10.10.2 4 ms 4 ms * <<<<<<<<<<<<<<<<<< Le trafic est acheminé directement vers le routeur Spoke 1 sans passer par le concentrateur.

Dépannage



Remarque : Il est toujours conseillé d'utiliser des débogages conditionnels, car l'exécution de débogages non conditionnels peut avoir un impact sur le processeur et donc sur l'environnement de production. L'adresse NBMA correspond à l'« adresse IP externe » (adresse IP utilisée pour créer l'interface du tunnel) et l'adresse IP du tunnel correspond à l'« adresse IP logique, c'est-à-dire l'adresse IP de l'interface du tunnel ».

debug dmvpn condition peer <nmbma/tunnel> <IP NMBA ou adresse IP de tunnel de l'homologue>
debug crypto condition peer ipv4 <IP WAN de l'homologue>
debug nhrp condition peer <nbma/tunnel> <NBMA ou adresse IP de tunnel de l'homologue>

Afin de dépanner DMVPN, vous devez adopter une approche en couches :

debug dmvpn detail all

1. Couche de cryptage : Après avoir confirmé la connectivité physique entre deux homologues, le chiffrement doit être vérifié. Cette couche chiffre/déchiffre les paquets GRE.

Commandes de débogage courantes utilisées pour vérifier la partie cryptage :

debug crypto condition peer ipv4 <adresse IP WAN de l'homologue>

debug crypto ikev2

debug crypto ikev2 error

debug crypto ikev2 internal

debug crypto ikev2 packet

debug crypto ipsec

debug crypto ipsec error

OU

debug dmvpn condition peer <nmbma/tunnel> <IP NMBA ou adresse IP de tunnel de l'homologue>

debug crypto condition peer ipv4 <IP WAN de l'homologue>

debug dmvpn detail crypto

Pour une compréhension approfondie du dépannage de la couche de cryptage, reportez-vous au lien externe :

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html.

2. GRE/NHRP : Certains problèmes courants incluent les échecs d'enregistrement NHRP et les changements d'adresse NBMA dynamiques dans le satellite, ce qui entraîne un mappage NHRP incohérent dans le concentrateur.

Commandes de débogage courantes utilisées pour vérifier le mappage NHRP :

debug nhrp condition peer <nbma/tunnel> <NBMA ou adresse IP de tunnel de l'homologue>

debug nhrp cache

debug nhrp packet

debug nhrp detail

debug nhrp error

Pour connaître les solutions de dépannage DMVPN les plus courantes, reportez-vous au lien externe :

https://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troubleshoot-00.html.

3. Routage : Le protocole de routage ne surveille pas l'état des tunnels en étoile à la demande.

Les mises à jour de routage IP et les paquets de données de multidiffusion IP traversent uniquement les tunnels hub-and-spoke.

Les paquets de données IP de monodiffusion traversent à la fois les tunnels en étoile et les tunnels en étoile à la demande.

Déboguer : Différentes commandes debug en fonction du protocole de routage.

Pour le lecteur profond de routage BGP, référez-vous au lien externe :

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html.

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.