FlexVPN a parlé dans la conception redondante de hub avec un double exemple de configuration d'approche de nuage

Contenu

Introduction

Ce document décrit comment configurer un rai dans un réseau de FlexVPN avec l'utilisation du bloc de configuration de client de FlexVPN dans un scénario où les plusieurs concentrateurs sont disponibles.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- FlexVPN
- Protocoles de routage de Cisco

Composants utilisés

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

- Routeur de service intégré de gamme Cisco G2 (ISR)
- Version 15.2M de Cisco IOS®

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Pour des raisons de redondance, un rai pourrait devoir se connecter aux plusieurs concentrateurs. La Redondance du côté de l'étoile permet le fonctionnement continu sans point de défaillance unique du côté concentrateur.

Les deux conceptions redondantes de hub de FlexVPN les plus communes qui utilisent la configuration en étoile sont :

- **Double approche de nuage**, où un rai a deux tunnels distincts actifs aux deux Concentrateurs à tout moment.
- **Approche de Basculement**, où un rai a un tunnel actif avec un hub à n'importe quel moment donné.

Les deux approches ont un seul ensemble d'avantages - et - des inconvénients.

Approche	Avantages	Inconvénients
Conjuguent le nuage	• Une reprise plus rapide pendant la panne, basée sur des temporisateurs de protocole de routage • Plus de possibilties pour distribuer le trafic parmi des Concentrateurs, puisque la connexion aux deux Concentrateurs sont en activité	• Le rai met à jour la session aux deux Concentrateurs en même temps, qui consomme des ressources sur les deux Concentrateurs
Basculement	• Configuration simple - établie dans FlexVPN • Ne compte pas sur le protocole de routage dans une panne	• Un temps de rétablissement plus lent - base sur Dead Peer Detection (DPD) ou (sur option) le Suivi d'objets • Tout le trafic est forcé pour voyager à un hu à la fois.

Ce document décrit la première approche. L'approche à cette configuration est semblable à la double configuration de nuage de VPN multipoint dynamique (DMVPN). La configuration de base du hub and spoke est basée sur des documents de transfert de DMVPN à FlexVPN. Référez-vous au transfert de FlexVPN : Mouvement dur de DMVPN à FlexVPN sur le même article de périphériques pour une description de cette configuration.

Diagramme du réseau

Réseau de transport

Ce diagramme montre le réseau de transport de base typiquement utilisé dans des réseaux de FlexVPN.

Réseau de substitution

Le diagramme montre le réseau de substitution avec la Connectivité logique qui affiche comment le Basculement devrait fonctionner. Pendant le fonctionnement normal, le rai 1 et le rai 2 mettent à jour des relations avec les deux Concentrateurs. Sur une panne, le protocole de routage commute d'un hub à l'autre.

> Remarque: Dans le diagramme, les lignes vertes affichent la connexion et la direction de la version 2 d'échange de clés Internet (IKE) (les sessions IKEv2)/Flex au hub 1, et les lignes bleues indiquent la connexion au hub 2.

Les deux Concentrateurs retiennent l'adressage IP distinct en nuages de recouvrement. L'adressage de **/24** représente le groupe d'adresses allouées pour ce nuage, pas l'adressage réel d'interface. C'est parce que le hub de FlexVPN alloue typiquement une adresse IP dynamique pour l'interface de rai, et se fonde sur des artères insérées dynamiquement par l'intermédiaire des commandes d'artère dans le bloc d'autorisation de FlexVPN.

Configurations en étoile

Configuration d'interface de tunnel de rai

La configuration typique utilisée dans cet exemple est simplement deux interfaces de tunnel avec deux adresses de destination distinctes.

```
interface Tunnel1
ip address negotiated
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel destination 172.25.1.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default

interface Tunnel2
ip address negotiated
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel destination 172.25.2.1
```

```
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

Afin de permettre à des tunnels de spoke-to-spoke pour former correctement, un modèle virtuel (VT) est nécessaire.

```
interface Virtual-Template1 type tunnel
ip unnumbered ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

Le rai utilise une interface non numérotée qui indique l'interface de RÉSEAU LOCAL dans le Virtual Routing and Forwarding (VRF), qui est global dans ce cas. Cependant, il pourrait être meilleur de mettre en référence une interface de bouclage. C'est parce que les interfaces de bouclage demeurent en ligne dans presque toutes les conditions.

Configuration de Protocole BGP (Border Gateway Protocol) de rai

Puisque Cisco recommande l'iBGP comme protocole de routage à utiliser dans le réseau de substitution, des mentions de ce document seulement cette configuration.

> Remarque: Les rais doivent retenir l'accessibilité BGP aux deux Concentrateurs.

```
router bgp 65001
bgp log-neighbor-changes
network 192.168.101.0
neighbor 10.1.1.1 remote-as 65001
neighbor 10.1.1.1 fall-over
neighbor 10.2.2.1 remote-as 65001
neighbor 10.2.2.1 fall-over
```

FlexVPN dans cette configuration n'a pas un concept primaire ou secondaire de hub. L'administrateur décide si le protocole de routage préfère un hub au-dessus des autres ou, dans quelques scénarios, exécute l'Équilibrage de charge.

Considérations de Basculement et de convergence de rai

Afin de réduire le temps où il prend pour a parlé pour détecter la panne, utilisent ces deux méthodes typiques.

- Raccourcissez les temporisateurs BGP. Le temps de maintien par défaut entraîne le Basculement.
- Configurez le BGP chute-au-dessus de, qui discused en cet article, support de BGP pour la mise hors fonction scrutante de session Fast.
- N'utilisez pas la détection bidirectionnelle d'expédition (BFD), parce qu'elle n'est pas recommandée dans la plupart des déploiements de FlexVPN.

Tunnels et Basculement de spoke-to-spoke

Commutation raccourcie par Protocole NHRP (Next Hop Resolution Protocol) d'utilisation de tunnels de spoke-to-spoke. Le Cisco IOS indique que ces raccourcis sont des artères de NHRP, par exemple :

```
Spoke1#show ip route nhrp
(...) 192.168.102.0/24 is variably subnetted, 2 subnets, 2 masks
H 192.168.102.0/24 [250/1] via 10.2.2.105, 00:00:21, Virtual-Access1
```

Ces artères n'expirent pas quand la connexion BGP expire ; au lieu de cela, ils sont tenus pour le holdtime de NHRP, qui est de deux heures par défaut. Ceci signifie que les tunnels actifs de spoke-to-spoke restent en fonction même dans une panne.

Configurations de hub

Groupes locaux

Comme évoqué dans la section de **schéma de réseau**, les deux Concentrateurs retiennent l'adressage IP distinct.

Hub1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

Hub2

```
ip local pool FlexSpokes 10.2.2.100 10.2.2.254
```

Configuration BGP de hub

La configuration BGP de hub demeure semblable aux exemples précédents.

Cette sortie provient le hub 1 avec une adresse IP de RÉSEAU LOCAL de **192.168.0.1**.

```
router bgp 65001
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
aggregate-address 192.168.0.0 255.255.0.0 summary-only
neighbor Spokes peer-group
neighbor Spokes remote-as 65001
neighbor Spokes fall-over
neighbor 192.168.0.2 remote-as 65001
neighbor 192.168.0.2 route-reflector-client
neighbor 192.168.0.2 next-hop-self all
neighbor 192.168.0.2 unsuppress-map ALL route-map ALL permit 10
match ip address 1

ip access-list standard 1
permit any
```

Essentiellement, c'est ce qui est fait :

- Le pool d'adresses de FlexVPN de gens du pays est dans la chaîne de bgp listen.
- Le réseau local est 192.168.0.0/24.
- Un résumé est annoncé seulement aux rais. La configuration d'aggregate-address crée une artère statique pour ce préfixe par l'intermédiaire de l'interface null0, qui est une route de suppression qui est utilisée afin d'empêcher des boucles de routage.
- Tous les préfixes spécifiques sont annoncés à l'autre hub. Puisque c'est également une connexion d'iBGP, il exige une configuration de route-reflector.

Ce diagramme représente l'échange des préfixes BGP entre les rais et les Concentrateurs en un nuage de FlexVPN.

> Remarque: Dans le diagramme, la ligne verte représente les informations fournies par des rais au hub, la ligne rouge représente les informations fournies par chaque hub aux rais (un résumé seulement), et la ligne bleue représente des préfixes permutés entre les Concentrateurs.

Vérifiez

Puisque chaque rai retient l'association avec les deux Concentrateurs, deux sessions IKEv2 sont vues avec la **crypto** commande d'**ikev2 SA d'exposition**.

```
IPv4 Crypto IKEv2 SATunnel-id Local Remote fvrf/ivrf Status
3 172.16.1.2/500 172.16.2.2/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3147 sec Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.1.2/500 172.25.2.1/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3256 sec
```

Afin de visualiser les informations de protocole de routage, sélectionnez ces commandes :

show bgp ipv4 unicast

show bgp summary

Sur les rais, vous devriez voir que le préfixe récapitulatif est reçu des Concentrateurs, et que les connexions aux deux Concentrateurs sont en activité.

```
Spoke1#show bgp ipv4 unicast
BGP table version is 4, local router ID is 192.168.101.1
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,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found Network Next Hop Metric LocPrf Weight Path
*>i 192.168.0.0/16 10.1.1.1 0 100 0 i
* i 10.2.2.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
Spoke1#show bgp summa
Spoke1#show bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
BGP table version is 4, main routing table version 4
2 network entries using 296 bytes of memory
3 path entries using 192 bytes of memory
3/2 BGP path/bestpath attribute entries using 408 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 896 total bytes of memory
BGP activity 2/0 prefixes, 3/0 paths, scan interval 60 secs Neighbor V AS MsgRcvd MsgSent TblVer
InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 7 7 4 0 0 00:00:17 1
10.2.2.1 4 65001 75 72 4 0 0 01:02:24 1
```

Dépannez

Il y a deux blocs importants à dépanner :

- Échange de clés Internet (IKE)
- IPSec (IPsec)

Voici les commandes show appropriées :

```
show crypto ipsec sa
```

```
show crypto ikev2 sa
```

Voici les commandes de débogage appropriées :

```
debug crypto ikev2 [internal|packet]
```

```
debug crypto ipsec
```

```
debug vtemplate event
```

Voici le protocole de routage approprié :

```
show bgp ipv4 unicast (or show ip bgp)
```

```
show bgp summary
```