Transfert de FlexVPN : Mouvement dur de DMVPN à FlexVPN sur les mêmes périphériques

Contenu

Introduction

Ce document fournit des informations au sujet de la façon migrer du réseau existant DMVPN à FlexVPN sur les mêmes périphériques.

Les configurations de les deux cadres coexisteront sur les périphériques.

Dans ce document seulement le scénario le plus commun est affiché : DMVPN utilisant la clé pré-partagée pour l'authentification et EIGRP comme protocole de routage.

Ce document explique le transfert à BGP (protocole de routage recommandé) et à EIGRP moins desirable.

Conditions préalables

Conditions requises

Ce document suppose que le lecteur connaît des concepts de base de DMVPN et de FlexVPN.

Composants utilisés

Notez que non tous les logiciel et supports matériels IKEv2. Référez-vous au navigateur de caractéristique de Cisco pour information. Dans le meilleur des cas, les versions de logiciel à utiliser sont :

- ISR - 15.2(4)M1 ou plus nouveau
- ASR1k - 3.6.2 libèrent 15.2(2)S2 ou plus nouveaux

Parmi les avantages d'une plus nouveaux plate-forme et logiciel est la possibilité d'utiliser le chiffrement de nouvelle génération, par exemple, AES GCM pour le cryptage dans IPsec. Ceci est discuté dans RFC 4106.

AES GCM laisse atteindre une vitesse beaucoup plus rapide de cryptage sur du matériel.

Afin de voir des recommandations de Cisco concernant utiliser et migrer vers le chiffrement de nouvelle génération, référez-vous :

http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Procédure de transfert

Actuellement, la manière recommandée de migrer de DMVPN vers FlexVPN est pour les deux cadres à ne pas fonctionner en même temps.

Cette limite devra retiré de nouvelles caractéristiques de transfert être introduite dans la release ASR 3.10, dépistée sous de plusieurs demandes d'amélioration sous le côté de Cisco, y compris CSCuc08066. Ces caractéristiques devraient être disponibles fin juin, 2013.

Un transfert où les deux cadres coexistent et fonctionnent en même temps sur les mêmes périphériques désigné sous le nom doucement du transfert, qui indique l'incidence minimum et le Basculement sans heurt d'un cadre à l'autre.

Un transfert où la configuration de les deux cadres coexistent, mais ne fonctionnent pas en même temps désigné sous le nom du transfert dur. Ceci indique qu'un basculement d'un cadre à l'autre signifie un manque de transmission au-dessus de VPN, même si minimal.

Transfert dur sur les mêmes périphériques

Dans ce document le transfert d'un réseau existant DMVPN à un nouveau réseau de FlexVPN sur les mêmes périphériques est discuté.

Ce transfert exige que les deux cadres ne fonctionnent pas en même temps sur les périphériques, exigeant essentiellement que la fonctionnalité DMVPN est désactivée d'un bout de l'affaire à l'autre avant d'activer FlexVPN.

Jusqu'à ce que la nouvelle caractéristique de transfert soit disponible, la manière d'exécuter des transferts utilisant les mêmes périphériques est à :

1. Vérifiez la Connectivité au-dessus de DMVPN.
2. Ajoutez la configuration de FlexVPN en place et arrêtez le tunnel et les interfaces de modèle virtuel appartenant à la nouvelle configuration.
3. (Pendant une fenêtre de maintenance) arrêtez toutes les interfaces de tunnel DMVPN sur tous les rais et Concentrateurs avant le déplacement à l'étape 4.
4. Interfaces de tunnel d'Unshut FlexVPN.
5. Vérifiez a parlé à la Connectivité de hub.
6. Vérifiez a parlé à la Connectivité de rai.
7. *Si la vérification au point 5 ou 6 n'allait pas correctement revenez à DMVPN en arrêtant l'interface de FlexVPN et ONU-en fermant des interfaces DMVPN.*
8. *Vérifiez a parlé à la transmission de hub.*
9. *Vérifiez a parlé à la transmission de rai.*

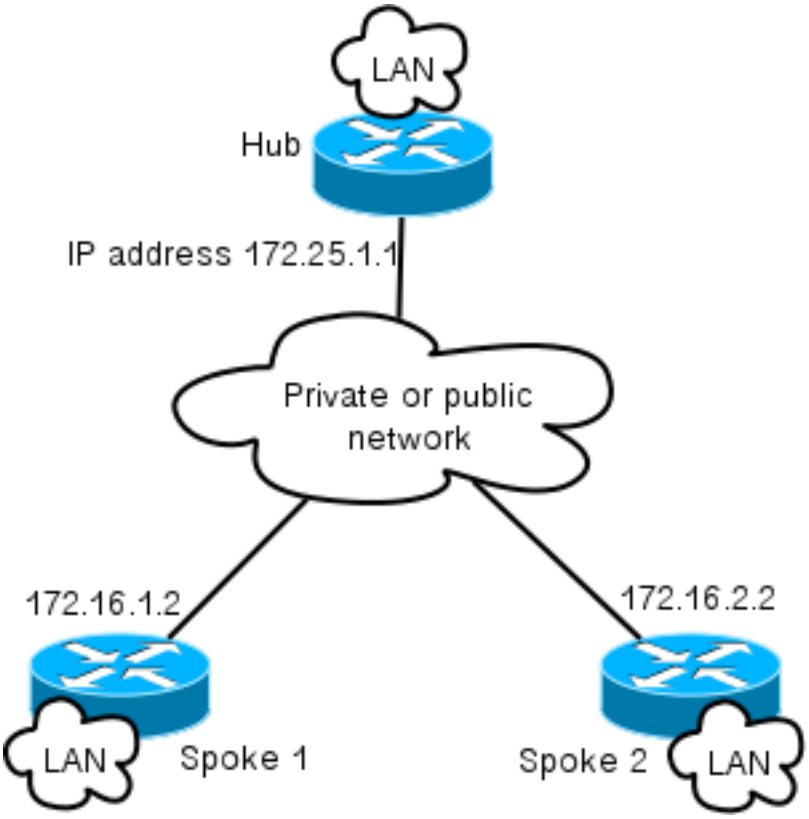
Approche faite sur commande

Si, en raison de vos complexités de réseau ou de routage, l'approche ne pourrait pas être la meilleure idée pour vous, commencez une discussion avec votre représentant Cisco avant de migrer. La meilleure personne pour discuter un procédé fait sur commande de transfert est votre ingénieur système ou ingénieur de Services avancés.

Topologie du réseau

Topologie du réseau de transport

Ce diagramme affiche une topologie typique de connexions des hôtes sur l'Internet. Dans ce document, l'adresse IP du hub de loopback0 (172.25.1.1) est utilisée pour terminer la session d'IPsec.

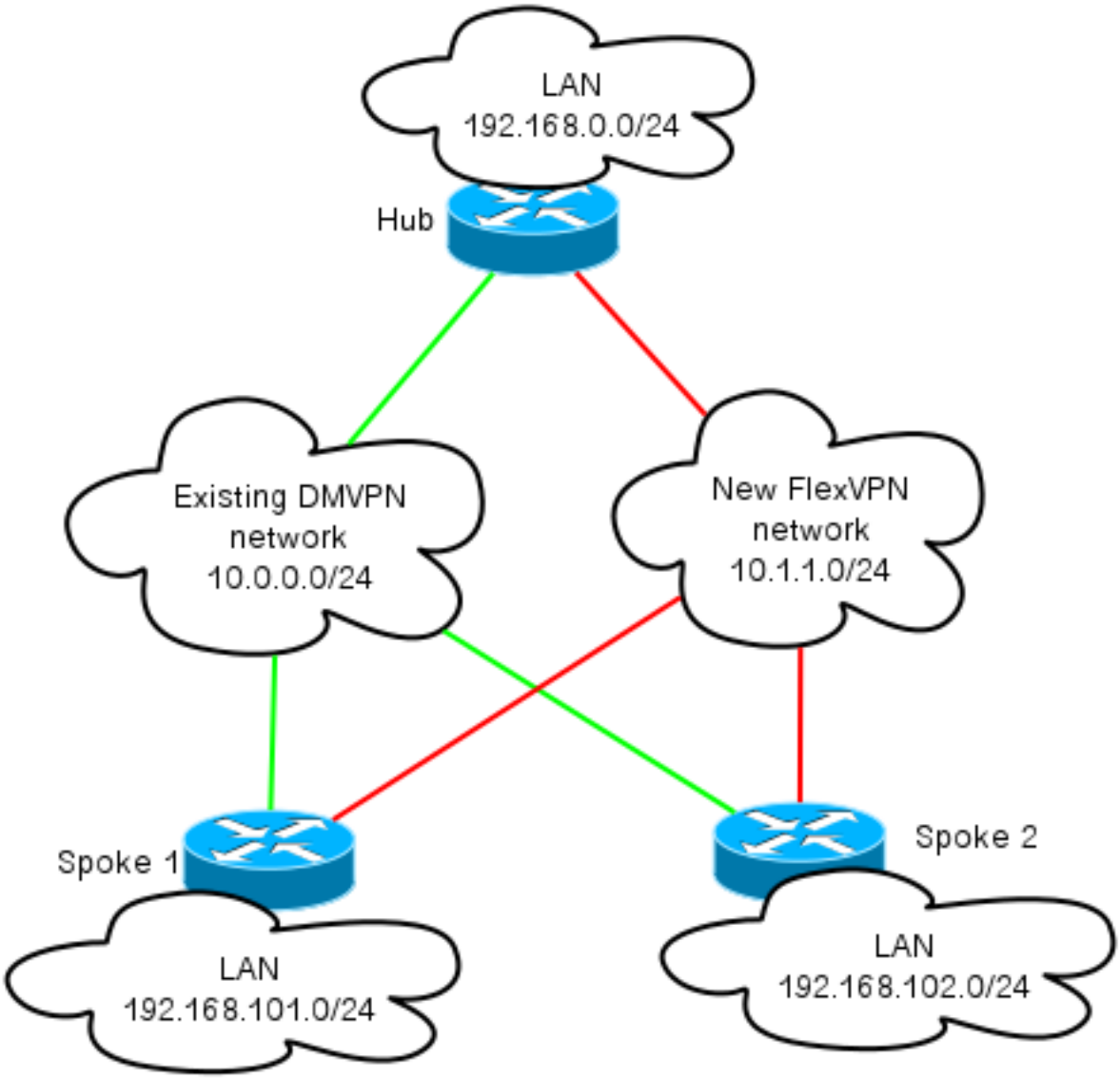


Topologie du réseau de recouvrement

Ce diagramme de topologie affiche deux nuages distincts utilisés pour le recouvrement : DMVPN (connexions vertes) et connexions de FlexVPN.

Des préfixes de réseau local sont affichés pour les côtés correspondants.

Le sous-réseau 10.1.1.0/24 ne représente pas un sous-réseau réel en termes d'interface adressant, mais plutôt un bloc de l'espace IP dédié au nuage de FlexVPN. Le raisonnement derrière est discuté plus tard dans la section de configuration de FlexVPN.



Configuration

Configuration DMVPN

Cette section contient la configuration de base du hub and spoke DMVPN.

La clé pré-partagée (PSK) est utilisée pour l'authentification IKEv1.

Une fois qu'IPsec a été établi, l'enregistrement de NHRP est exécuté de a parlé au hub, de sorte que le hub puisse apprendre dynamiquement l'adressage NBMA des rais.

Quand le NHRP exécute l'enregistrement sur le rai et le hub, l'acheminement de l'adjacancy peut établir et des artères permutées. Dans cet exemple, l'EIGRP est utilisé en tant que protocole de routage de base pour le réseau de substitution.

Configuration du rai DMVPN

C'est un exemple de configuration de base de DMVPN avec l'authentification principale pré-partagée et d'EIGRP comme protocole de routage.

```
crypto isakmp policy 10
```

```
  encr aes
  authentication pre-share
crypto isakmp key cisco address 0.0.0.0
crypto isakmp keepalive 30 5
crypto isakmp profile DMVPN_IKEv1
  keyring DMVPN_IKEv1
  match identity address 0.0.0.0
crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
  mode transport
crypto ipsec profile DMVPN_IKEv1
  set transform-set IKEv1
  set isakmp-profile DMVPN_IKEv1
interface Tunnel0
ip address 10.0.0.101 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp map 10.0.0.1 172.25.1.1
 ip nhrp map multicast 172.25.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 900
 ip nhrp nhs 10.0.0.1
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN_IKEv1
router eigrp 100
 network 10.0.0.0 0.0.0.255
 network 192.168.102.0
 passive-interface default
 no passive-interface Tunnel0
```

Configuration du hub DMVPN

Dans la configuration de hub le tunnel est originaire de loopback0 avec une adresse IP de 172.25.1.1.

Le repos est déploiement standard de hub DMVPN avec l'EIGRP comme protocole de routage.

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0
crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
 mode transport
crypto ipsec profile DMVPN_IKEv1
 set transform-set IKEv1
 interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp holdtime 900
 ip nhrp server-only
 ip nhrp redirect
 ip summary-address eigrp 100 192.168.0.0 255.255.0.0
 ip tcp adjust-mss 1360
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN_IKEv1
router eigrp 100
 network 10.0.0.0 0.0.0.255
```

```
network 192.168.0.0 0.0.255.255
passive-interface default
no passive-interface Tunnel0
```

Configuration de FlexVPN

FlexVPN est basé sur ces mêmes Technologies fondamentales :

- IPsec : À la différence du par défaut dans DMVPN, IKEv2 est utilisé au lieu d'IKEv1 pour négocier IPsec SAS. IKEv2 offre des améliorations au-dessus d'IKEv1, commençant par la résilience et la fin avec combien de messages sont nécessaires pour établir une voie de transmission de données protégés.
- GRE : À la différence de DMVPN, des interfaces point par point statiques et dynamiques sont utilisées, et non seulement sur GRE multipoint statique relie. Cette configuration permet la flexibilité accrue, particulièrement pour le comportement de par-rai/par-hub.
- NHRP : Dans FlexVPN le NHRP est principalement utilisé pour établir a parlé à la transmission de rai. Les rais ne s'enregistrent pas au hub.
- Acheminement : Puisque les rais n'exécutent pas l'enregistrement de NHRP au hub, vous devez compter sur d'autres mécanismes pour s'assurer que le hub and spoke peut communiquer bidirectionnel. Simliar à DMVPN, des protocoles de routage dynamique peut être utilisé. Cependant, FlexVPN te permet pour employer IPsec pour introduire les informations de routage. Le par défaut est d'introduire comme artère de /32 pour l'adresse IP de l'autre côté du tunnel, qui permettra à rai-à-hub la transmission directe.

Dans le transfert dur de DMVPN à FlexVPN les deux framemworks ne fonctionnent pas en même temps sur les mêmes périphériques. Cependant, il est recommandé pour les maintenir distincts.

Séparez-les à plusieurs niveaux :

- NHRP - (recommandé) différent d'ID de réseau de NHRP d'utilisation.
- Acheminement - (recommandé) distinct de processus de routage d'utilisation.
- VRF - La séparation de VRF peut laisser a ajouté la flexibilité mais ne sera pas discutée ici (facultatif).

Configuration de FlexVPN de rai

Une des différences en configuration en étoile dans FlexVPN par rapport à DMVPN, est que vous avez potentiellement deux interfaces.

Il y a un tunnel nécessaire pour a parlé à la transmission de hub et le tunnel facultatif pour a parlé aux tunnels de rai. Si vous choisissez de ne pas avoir dynamique parliez au Tunnellisation de rai et plutôt que tout passe par le périphérique de hub, vous pouvez retirer l'interface de modèle virtuel et enlever la commutation raccourcie par NHRP de l'interface de tunnel.

Vous noterez également que l'interface de tunnel statique a une adresse IP reçue basée sur la négociation. Ceci permet au hub pour fournir l'IP d'interface de tunnel a parlé dynamiquement sans nécessité de créer l'adressage statique dans le nuage de FlexVPN.

```
aaa new-model
aaa authorization network default local
aaa session-id common
```

```
crypto ikev2 profile Flex_IKEv2
 match identity remote fqdn domain cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 aaa authorization group cert list default default
 virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

Cisco recommande utilisant AES GCM dans le matériel qui le prend en charge.

```
crypto ipsec transform-set IKEv2 esp-gcm
    mode transport
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2
! set transform-set IKEv2
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
 shutdown
 tunnel source Ethernet0/0
 tunnel destination 172.25.1.1
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel1
 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 PKI est la manière recommandée d'exécuter l'authentification de large échelle dans IKEv2.

Cependant, vous pouvez encore utiliser la clé pré-partagée tant que vous vous rendez compte de elle est des limites.

Voici un exemple de configuration utilisant « Cisco » comme PSK :

```
crypto ikev2 keyring Flex_key
 peer Spokes
 address 0.0.0.0 0.0.0.0
 pre-shared-key local cisco
 pre-shared-key remote cisco
crypto ikev2 profile Flex_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local Flex_key
 aaa authorization group psk list default default
```

Configuration de hub de FlexVPN

Typiquement un hub terminera seulement les tunnels dynamiques de rai-à-hub. C'est pourquoi dans la configuration du hub vous ne trouverez pas une interface de tunnel statique pour FlexVPN, au lieu de cela une interface de modèle virtuel est utilisée. Ceci engendrera une interface d'accès virtuel pour chaque connexion.

Notez que du côté concentrateur vous devez préciser des adresses de groupe à assigner aux rais.

Des adresses de ce groupe seront ajoutées plus tard dans la table de routage comme artères de /32 pour chaque rai.

```
aaa new-model
aaa authorization network default local
aaa session-id common
crypto ikev2 authorization policy default
 pool FlexSpokes
crypto ikev2 profile Flex_IKEv2
 match identity remote fqdn domain cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 aaa authorization group cert list default default
 virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

Cisco recommande utilisant AES GCM dans le matériel qui le prend en charge.

```
crypto ipsec transform-set IKEv2 esp-gcm
 mode transport
```

Notez cela dans la configuration au-dessous de l'exécution AES GCM a été commenté.

```
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2
! set transform-set IKEv2
interface Loopback0
 description DMVPN termination
 ip address 172.25.1.1 255.255.255.255
interface Loopback100
 ip address 10.1.1.1 255.255.255.255
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback100
 ip nhrp network-id 2
 ip nhrp redirect
 shutdown
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

Avec l'authentification dans IKEv2, le même principe s'applique sur le hub comme sur le rai.

Pour l'évolutivité et la flexibilité, Certificats d'utilisation. Cependant, vous pouvez réutiliser la même configuration pour PSK que sur le rai.

Remarque: IKEv2 offre la flexibilité en termes d'authentification. Un côté peut authentifier utilisant PSK tandis que l'autre RSA-SIG.

Transfert du trafic

Migrer vers le BGP comme protocole de routage de recouvrement [recommandé]

Le BGP est un protocole de routage basé sur l'échange d'unicast. Dues à lui est les caractéristiques que c'a étées le meilleur protocole d'évolution dans des réseaux DMVPN.

Dans cet exemple, l'iBGP est utilisé.

Configuration BGP de rai

Le transfert de rai se compose de deux parts. Activation du BGP comme routage dynamique.

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

Après que le voisin BGP monte (voient la configuration BGP de hub dans cette section de transfert) et de nouveaux préfixes au-dessus de BGP sont appris, vous pouvez balancer le trafic du nuage existant DMVPN au nouveau nuage de FlexVPN.

Configuration BGP de hub

Sur le hub éviter de garder la configuration de proximité pour le chaque a parlé séparément, les auditeurs dynamiques sont configurées.

Dans cette installation le BGP n'initiera pas de nouvelles connexions, mais recevra la connexion du groupe fourni d'adresses IP. Dans ce cas ledit groupe a 10.1.1.0/24 ans, qui est toutes les adresses dans le nouveau nuage de FlexVPN.

```
router bgp 65001
 network 192.168.0.0
 bgp log-neighbor-changes
 bgp listen range 10.1.1.0/24 peer-group Spokes aggregate-address 192.168.0.0 255.255.0.0
summary-only neighbor Spokes peer-group neighbor Spokes remote-as 65001
```

Migrer le trafic vers FlexVPN

Comme indiqué précédemment le transfert doit être fait par de l'arrêt DMVPN et apport de FlexVPN la fonctionnalité.

Cette procédure garantit l'incidence minimum.

1. Sur tous les rais :`interface tunnel 0`
   `shut`
2. Sur le hub :`interface tunnel 0`
   `shut`Assurez-vous en ce moment qu'il n'y a aucune session IKEv1 établie à ce hub des rais.Ceci peut être vérifié en vérifiant la sortie de la commande de **show crypto isakmp sa** et en surveillant des messages de Syslog générés par la session de crypto logging.Une fois que ceci a été confirmé vous pouvez poursuivre à apporter FlexVPN.
3. Continuation sur le hub :`interface Virtual-template 1`
   `no shut`
4. Sur des rais :`interface tunnel 1`
   `no shut`

Étapes de vérification

Stabilité d'IPsec

La meilleure manière d'évaluer la stabilité d'IPsec est en surveillant des sylogs avec cette commande enabled de configuration :

```
crypto logging session
```

Si vous voyez des sessions allant en haut et en bas, ceci peut indiquer un problème au niveau IKEv2/FlexVPN qui doit être corrigé avant que le transfert puisse commencer.

Les informations BGP remplies

Si IPsec est stable, assurez-vous que la table BGP est remplie avec des entrées des rais (sur le hub) et du résumé du hub (sur des rais).

En cas de BGP, ceci peut être visualisé en exécutant :

```
show bgp
! or
show bgp ipv4 unicast
! or
show ip bgp summary
```

Exemple des informations correctes du hub :

```
Hub#show bgp
BGP router identifier 172.25.1.1, local AS number 65001
(...omitted...)
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
*10.1.1.101 4 65001 83 82 13 0 0 01:10:46 1 *10.1.1.102 4 65001 7 7 13 0 0 00:00:44 1
```

Vous pouvez voir que le hub a appris que 1 préfixe de chacun des rais et les deux rais sont dynamiques (identifié par le signe d'astérisque (*)).

Exemple des informations semblables du rai :

```
Spoke1#show ip bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
(...omitted...)
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 11 11 6 0 0 00:03:43 1
```

Le rai a reçu un préfixe du hub. En cas de cette installation, ce préfixe devrait être le résumé annoncé sur le hub.

Migrer vers de nouveaux tunnels utilisant l'EIGRP

L'EIGRP est un choix populaire dans des réseaux DMVPN dus à lui est déploiement et convergence rapide relativement simples.

Il, cependant, mesurera plus mauvais que le BGP et n'offre pas plusieurs de mécanismes avancés qui peuvent être utilisés par BGP directement hors de la case.

Cette section suivante décrit une des manières de se déplacer à FlexVPN utilisant un nouveau processus EIGRP.

Configuration en étoile mise à jour

Dans cet exemple, un nouveau COMME est ajouté avec un processus distinct EIGRP.

```
router eigrp 200
 network 10.1.1.0 0.0.0.255
 network 192.168.101.0
```

```
 passive-interface default
 no passive-interface Tunnel1
```
Remarque: Vous devriez éviter d'établir la contiguïté de protocole de routage plus d'avez parlé aux tunnels de rai, ainsi rendez seulement l'interface de tunnel1 (a parlé au hub) non passive.

Configuration mise à jour de hub

De même sur le hub, DMVPN devrait rester le moyen privilégié de permuter le trafic plus de. Cependant, FlexVPN devrait annoncer et apprendre les mêmes préfixes déjà.

```
router eigrp 200
 network 10.1.1.0 0.0.0.255
```
Il y a deux manières de fournir le dos de résumé vers le rai.

- Redistribuer une route statique pointant à null0 (option préférée).`ip route 192.168.0.0 255.255.0.0 null 0`
```
ip access-list standard EIGRP_SUMMARY
 permit 192.168.0.0 0.0.255.255
router eigrp 200
 distribute-list EIGRP_SUMMARY out Virtual-Template1
```
`redistribute static metric 1500 10 10 1 1500`Cette option laisse avoir le contrôle du résumé et la redistribution sans configuration VT du hub émouvant.
- Ou, vous pouvez installer une adresse récapitulative de style DMVPN sur le virtual-template. Cette configuration n'est pas recommandée en raison du traitement interne et de la réplication de ledit résumé à chaque accès virtuel. On lui affiche ici pour la référence :`interface Virtual-Template1 type tunnel`
```
 ip summary-address eigrp 200 172.16.1.0 255.255.255.0
 ip summary-address eigrp 200 192.168.0.0 255.255.0.0 delay 2000
```

Migrer le trafic vers FlexVPN

Le transfert doit être fait par de l'arrêt DMVPN et apport de FlexVPN la fonctionnalité.

L'incidence minimum de garanties de procédure suivante.

1. Sur tous les rais :`interface tunnel 0`
```
    shut
```
2. Sur le hub :`interface tunnel 0`
```
  shut
```
Assurez-vous en ce moment qu'il n'y a aucune session IKEv1 établie à ce hub des rais.Ceci peut être vérifié en vérifiant la sortie de la commande de **show crypto isakmp sa** et en surveillant des messages de Syslog générés par session de crypto logging.Une fois que ceci a été confirmé vous pouvez poursuivre à apporter FlexVPN.
3. Continuation sur le hub :`interface Virtual-template 1`
```
 no shut
```
4. Sur tous les rais :`interface tunnel 1`
```
    no shut
```

Étapes de vérification

Stabilité d'IPsec

Comme en cas de BGP, vous devez évaluer si IPsec est stable. La meilleure manière de faire

ainsi est en surveillant des sylogs avec cette commande enabled de configuration :

```
crypto logging session
```

Si vous voyez des sessions allant en haut et en bas, ceci peut indiquer un problème au niveau IKEv2/FlexVPN qui doit être corrigé avant que le transfert puisse commencer.

Les informations EIGRP dans la table de topologie

Assurez-vous que vous faites remplir votre table de topologie EIGRP avec des entrées de RÉSEAU LOCAL de rai sur le hub et le résumé sur des rais. Ceci peut être vérifié en émettant cette commande sur le hub and spoke.

```
show ip eigrp topology
```

Exemple de sortie appropriée de rai :

```
Spoke1#sh ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status
(...omitted as output related to DMVPN cloud ...)
EIGRP-IPv4 Topology Table for AS(200)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 26112000
 via Rstatic (26112000/0)


P 192.168.101.0/24, 1 successors, FD is 281600 via Connected, Ethernet1/0 P 192.168.0.0/16, 1
successors, FD is 26114560 via 10.1.1.1 (26114560/1709056), Tunnel1 P 10.1.1.107/32, 1
successors, FD is 26112000 via Connected, Tunnel1
```

Vous noterez que le rai sait son sous-réseau LAN (en italique) et les résumés pour ceux (en **gras**).

Exemple de sortie appropriée de hub.

```
Hub#sh ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(172.25.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status
(...omitted, related to DMVPN...)
EIGRP-IPv4 Topology Table for AS(200)/ID(172.25.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 128256
 via Connected, Loopback100


P 192.168.101.0/24, 1 successors, FD is 1561600 via 10.1.1.107 (1561600/281600), Virtual-Access1
P 192.168.0.0/16, 1 successors, FD is 1709056 via Rstatic (1709056/0) P 10.1.1.107/32, 1
successors, FD is 1709056 via Rstatic (1709056/0) P 10.1.1.106/32, 1 successors, FD is 1709056
via Rstatic (1709056/0) P 0.0.0.0/0, 1 successors, FD is 1709056 via Rstatic (1709056/0) P
192.168.102.0/24, 1 successors, FD is 1561600 via 10.1.1.106 (1561600/281600), Virtual-Access2
```

Vous noterez que le hub sait les sous-réseaux LAN des rais (en italique), le préfixe récapitulatif qu'il annonce (en **gras**) et l'adresse IP assigné de chaque rai par l'intermédiaire de la négociation.

Considérations supplémentaires

Exister a parlé aux tunnels de rai

Puisque l'arrêt de l'interface de tunnel DMVPN cause des entrées de NHRP d'être retirées, exister a parlé aux tunnels de rai sera démoli.

Effacer des entrées de NHRP

Comme indiqué précédemment, un hub de FlexVPN ne se fondera pas sur la procédure d'enregistrement de NHRP du du parler pour savoir conduire le trafic de retour. Cependant, dynamique a parlé aux tunnels de rai comptent sur des entrées de NHRP.

Dans DMVPN où le NHRP effaçant sur le hub pourrait avoir eu comme conséquence des problèmes de courte durée de Connectivité.

Dans l'effacement de FlexVPN le NHRP sur des rais entraînera la session de FlexVPN IPsec, liée au au parler aux tunnels de rai, pour être démoli. Dans le NHRP d'effacement aucun hub n'exercera un effet sur la session de FlexVPN.

C'est dû au fait qui dans FlexVPN, par défaut :

- Les rais ne s'enregistrent pas aux Concentrateurs.
- Les Concentrateurs fonctionnent seulement comme redirection de NHRP et n'installent pas des entrées de NHRP.
- Des entrées raccourcies de NHRP sont installées sur des rais pour des tunnels de spoke-to-spoke et sont dynamiques.

Mises en garde connues

A parlé au trafic de rai pourrait être affecté par CSCub07382.

Informations connexes

- Support et documentation techniques - Cisco Systems