Migration de DurMove de DMVPN vers FlexVPN sur les mêmes périphériques

Contenu

Introduction

Ce document fournit des informations sur la migration du réseau DMVPN existant vers FlexVPN sur les mêmes périphériques.

Les configurations des deux cadres coexisteront sur les périphériques.

Dans ce document, seul le scénario le plus courant est présenté : DMVPN utilisant une clé pré-partagée pour l'authentification et EIGRP comme protocole de routage.

Ce document montre la migration vers BGP (protocole de routage recommandé) et EIGRP moins souhaitable.

Conditions préalables

Conditions requises

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

Components Used

Notez que tous les logiciels et le matériel ne prennent pas en charge IKEv2. Référez-vous à Navigateur de fonctionnalités Cisco pour plus d'informations. Idéalement, les versions logicielles à utiliser sont les suivantes :

- ISR - 15.2(4)M1 ou ultérieur
- ASR1k - 3.6.2 version 15.2(2)S2 ou ultérieure

Parmi les avantages d'une plate-forme et d'un logiciel plus récents figure la possibilité d'utiliser la cryptographie nouvelle génération, par exemple AES GCM pour le cryptage dans IPsec. Cette question est traitée dans le document RFC 4106.

AES GCM permet d'atteindre une vitesse de cryptage beaucoup plus rapide sur certains matériels.

Afin de consulter les recommandations de Cisco sur l'utilisation et la migration vers la cryptographie de nouvelle génération, référez-vous à :

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 migration

Actuellement, la méthode recommandée pour migrer de DMVPN vers FlexVPN est que les deux cadres ne fonctionnent pas en même temps.

Cette limitation sera supprimée en raison des nouvelles fonctionnalités de migration qui seront introduites dans la version ASR 3.10, suivies sous plusieurs demandes d'amélioration sous Cisco,

y compris CSCuc08066. Ces fonctionnalités devraient être disponibles fin juin 2013.

Une migration dans laquelle les deux cadres coexistent et fonctionnent simultanément sur les mêmes périphériques sera appelée migration logicielle, ce qui indique un impact minimal et un basculement fluide d'un cadre à un autre.

Une migration dans laquelle la configuration des deux cadres coexiste, mais ne fonctionne pas en même temps est appelée migration dure. Cela indique qu'un basculement d'un cadre à un autre signifie un manque de communication sur VPN, même si cela est minime.

Migration dure sur les mêmes périphériques

Dans ce document, la migration d'un réseau DMVPN existant vers un nouveau réseau FlexVPN sur les mêmes périphériques est abordée.

Cette migration nécessite que les deux cadres ne fonctionnent pas en même temps sur les périphériques, ce qui nécessite essentiellement que la fonctionnalité DMVPN soit désactivée dans l'ensemble avant d'activer FlexVPN.

Tant que la nouvelle fonction de migration n'est pas disponible, la manière d'effectuer des migrations à l'aide des mêmes périphériques consiste à :

1. Vérifiez la connectivité sur DMVPN.
2. Ajoutez la configuration FlexVPN en place et arrêtez les interfaces de modèle de tunnel et virtuel appartenant à la nouvelle configuration.
3. (Pendant une fenêtre de maintenance) Arrêtez toutes les interfaces de tunnel DMVPN sur tous les rayons et concentrateurs avant de passer à l'étape 4.
4. Désactivez les interfaces de tunnel FlexVPN.
5. Vérifiez la connectivité du réseau en étoile avec le concentrateur.
6. Vérifiez la connectivité en étoile.
7. *Si la vérification du point 5 ou 6 n'a pas été correctement effectuée, revenez au DMVPN en arrêtant l'interface FlexVPN et en désarrêtant les interfaces DMVPN.*
8. *Vérifier la communication entre le satellite et le concentrateur*
9. *Vérifiez la communication en étoile.*

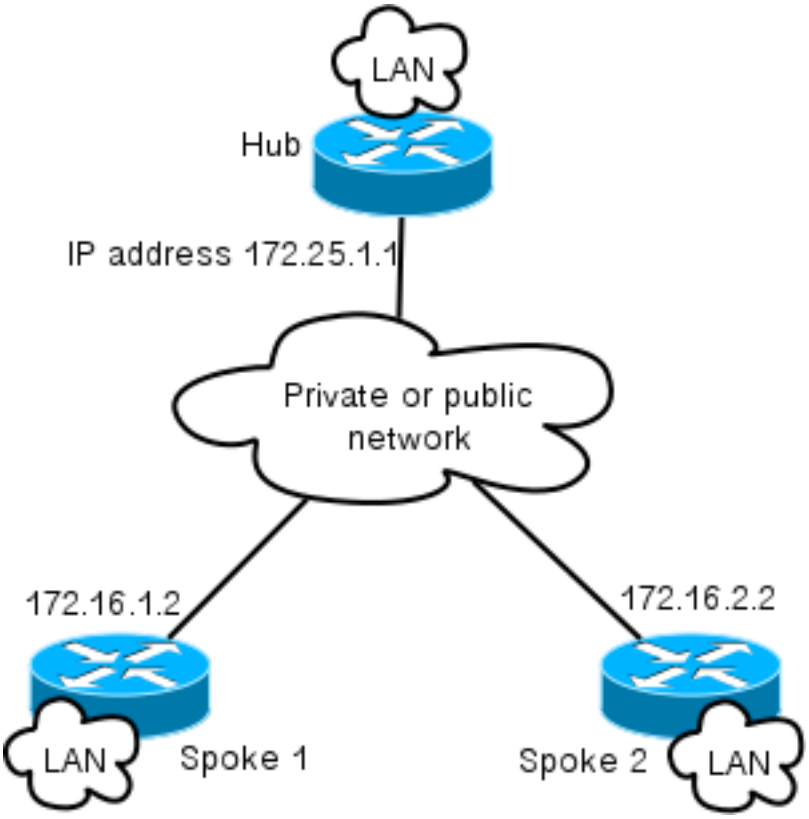
Approche personnalisée

Si, en raison de la complexité de votre réseau ou de votre routage, l'approche n'est peut-être pas la meilleure solution pour vous, commencez une discussion avec votre représentant Cisco avant de procéder à la migration. La meilleure personne pour discuter d'un processus de migration personnalisé est votre ingénieur système ou votre ingénieur des services avancés.

Topologie du réseau

Topologie du réseau de transport

Ce schéma présente une topologie type de connexions d’hôtes sur Internet. Dans ce document, l'adresse IP du concentrateur de loopback0 (172.25.1.1) est utilisée pour mettre fin à la session IPsec.

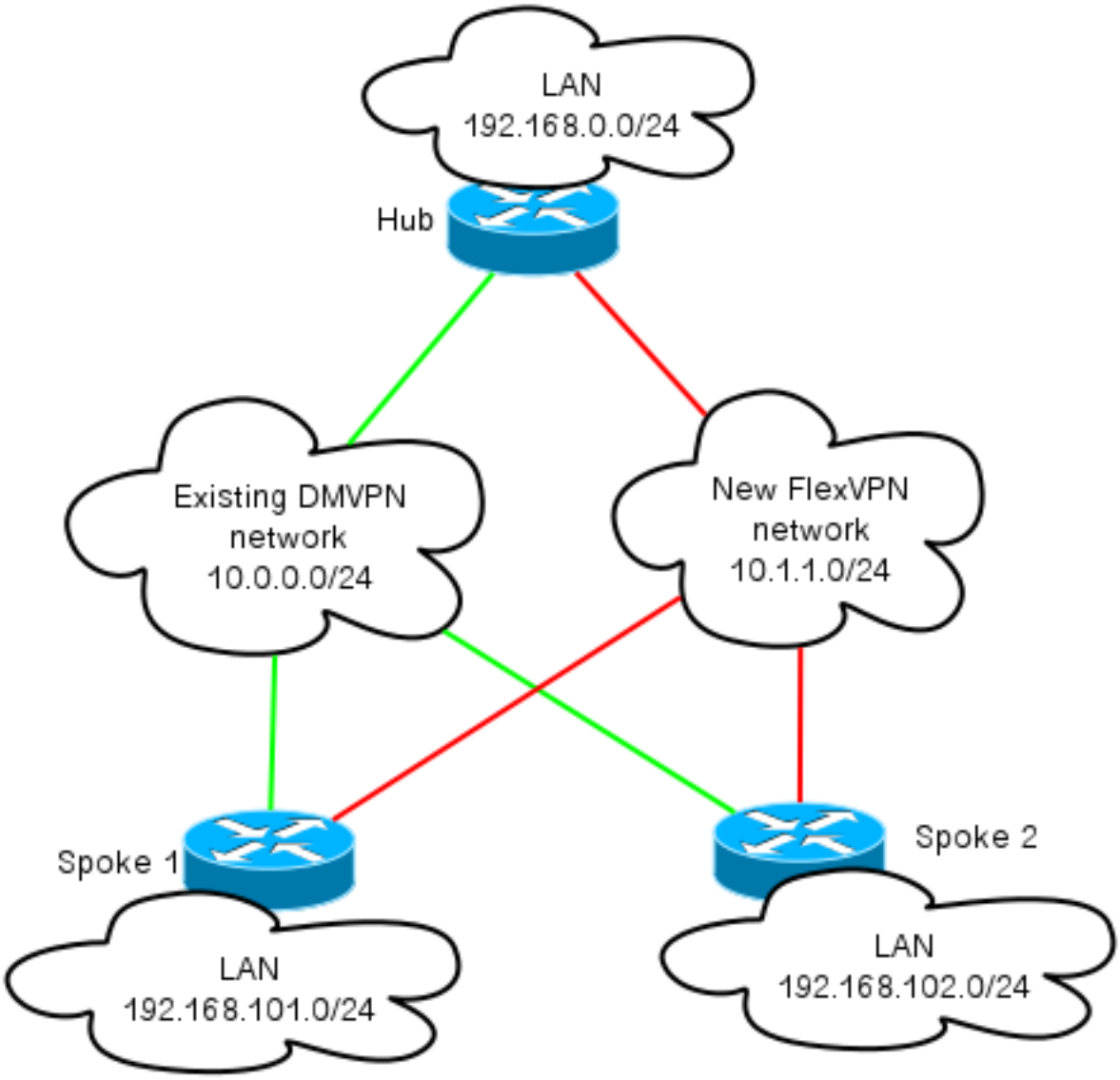


Topologie de réseau de superposition

Ce schéma de topologie présente deux nuages distincts utilisés pour la superposition : Connexions DMVPN (connexions vertes) et FlexVPN.

Les 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'adressage d'interface, mais plutôt une partie de l'espace IP dédiée au cloud FlexVPN. La raison d'être est traitée plus loin dans la section Configuration FlexVPN.



Configuration

Configuration DMVPN

Cette section contient la configuration de base du concentrateur et du rayon DMVPN.

La clé prépartagée (PSK) est utilisée pour l'authentification IKEv1.

Une fois IPsec établi, l'enregistrement NHRP est effectué du rayon au concentrateur, afin que le concentrateur puisse apprendre l'adressage NBMA des rayons dynamiques.

Lorsque le protocole NHRP effectue l'enregistrement sur un rayon et un concentrateur, la contiguïté de routage peut établir et échanger des routes. Dans cet exemple, le protocole EIGRP est utilisé comme protocole de routage de base pour le réseau de superposition.

Configuration DMVPN satellite

Il s'agit d'un exemple de configuration de base de DMVPN avec authentification de clé pré-partagée et 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 DMVPN du concentrateur

Dans la configuration du concentrateur, le tunnel provient de loopback0 avec l'adresse IP 172.25.1.1.

Le reste est le déploiement standard du concentrateur DMVPN avec 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 FlexVPN

FlexVPN repose sur les mêmes technologies fondamentales :

- IPSEC : Contrairement à la valeur par défaut dans DMVPN, IKEv2 est utilisé à la place d'IKEv1 pour négocier les SA IPsec. IKEv2 offre des améliorations par rapport à IKEv1, en commençant par la résilience et en se terminant par le nombre de messages nécessaires pour établir un canal de données protégé.
- GRE: Contrairement au DMVPN, les interfaces point à point statiques et dynamiques sont utilisées, et pas seulement sur les interfaces GRE multipoints statiques. Cette configuration permet une plus grande flexibilité, en particulier pour le comportement par rayon/par concentrateur.
- NHRP : Dans FlexVPN, le protocole NHRP est principalement utilisé pour établir une communication en étoile. Les rayons ne s'inscrivent pas au concentrateur.
- Routage : Comme les rayons n'enregistrent pas NHRP vers le concentrateur, vous devez vous fier à d'autres mécanismes pour vous assurer que le concentrateur et les rayons peuvent communiquer bidirectionnellement. Des protocoles de routage dynamique similaires à DMVPN peuvent être utilisés. Cependant, FlexVPN vous permet d'utiliser IPsec pour introduire des informations de routage. La valeur par défaut est d'introduire en tant que route /32 pour l'adresse IP de l'autre côté du tunnel, ce qui permettra une communication directe de rayon à concentrateur.

Lors de la migration dure de DMVPN vers FlexVPN, les deux trames ne fonctionnent pas simultanément sur les mêmes périphériques. Il est toutefois recommandé de les séparer.

Séparez-les sur plusieurs niveaux :

- NHRP : utilisez un ID réseau NHRP différent (recommandé).
- Routage : utilisez des processus de routage distincts (recommandé).
- VRF : la séparation VRF peut permettre une plus grande flexibilité mais ne sera pas abordée ici (facultatif).

Configuration de Spoke FlexVPN

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

Il existe un tunnel nécessaire pour la communication entre les rayons et les concentrateurs et un tunnel facultatif pour les tunnels entre les rayons. Si vous choisissez de ne pas avoir de transmission tunnel en étoile dynamique et que vous préférez que tout passe par le périphérique concentrateur, vous pouvez supprimer l'interface de modèle virtuel et supprimer la commutation de raccourcis NHRP de l'interface de tunnel.

Vous remarquerez également que l'interface de tunnel statique a une adresse IP reçue en fonction

de la négociation. Cela permet au concentrateur de fournir une interface de tunnel IP pour le rayon dynamiquement sans avoir besoin de créer un adressage statique dans le cloud 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 d'utiliser 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
```

PKI est la méthode recommandée pour effectuer une authentification à grande échelle dans IKEv2.

Cependant, vous pouvez toujours utiliser une clé pré-partagée tant que vous connaissez ses 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 du concentrateur FlexVPN

En règle générale, un concentrateur ne terminera que les tunnels de rayon à concentrateur dynamiques. C'est pourquoi, dans la configuration du concentrateur, vous ne trouverez pas d'interface de tunnel statique pour FlexVPN, mais une interface de modèle virtuel est utilisée. Cela génère une interface d'accès virtuel pour chaque connexion.

Notez que, côté concentrateur, vous devez indiquer les adresses de pool à attribuer aux rayons.

Les adresses de ce pool seront ajoutées ultérieurement dans la table de routage en tant que routes /32 pour chaque rayon.

```
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 d'utiliser AES GCM dans le matériel qui le prend en charge.

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

Notez que dans la configuration ci-dessous, l'opération AES GCM a été commentée.

```
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 au concentrateur que sur le rayon.

Pour des raisons d'évolutivité et de flexibilité, utilisez des certificats. Cependant, vous pouvez réutiliser la même configuration pour PSK que sur Spoke.

Remarque : IKEv2 offre une certaine flexibilité en termes d'authentification. Un côté peut s'authentifier à l'aide de PSK tandis que l'autre RSA-SIG.

Migration du trafic

Migration vers BGP en tant que protocole de routage de superposition [recommandé]

BGP est un protocole de routage basé sur l'échange de monodiffusion. En raison de ses caractéristiques, il a été le meilleur protocole d'évolutivité dans les réseaux DMVPN.

Dans cet exemple, iBGP est utilisé.

Configuration de Spoke BGP

La migration des rayons se compose de deux parties. Activation du protocole BGP en tant que routage dynamique.

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

Une fois que le voisin BGP est activé (voir la configuration BGP du concentrateur dans cette section de la migration) et que de nouveaux préfixes sur BGP sont appris, vous pouvez basculer le trafic du cloud DMVPN existant vers le nouveau cloud FlexVPN.

Configuration du concentrateur BGP

Sur le concentrateur pour éviter de conserver la configuration de voisinage pour chaque rayon séparément, les écouteurs dynamiques sont configurés.

Dans cette configuration, BGP n'initiera pas de nouvelles connexions, mais acceptera la connexion à partir du pool d'adresses IP fourni. Dans ce cas, ce pool est 10.1.1.0/24, qui est toutes les adresses du nouveau cloud 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
```

Migration du trafic vers FlexVPN

Comme indiqué précédemment, la migration doit être effectuée en arrêtant la fonctionnalité DMVPN et en activant FlexVPN.

Cette procédure garantit un impact minimum.

1. Sur tous les rayons :
```
interface tunnel 0
   shut
```
2. Sur le concentrateur :
```
interface tunnel 0
  shut
```
Àce stade, assurez-vous qu'aucune session IKEv1 n'est établie sur ce concentrateur à partir de rayons.Ceci peut être vérifié en vérifiant la sortie de la commande **show crypto isakmp sa** et en surveillant les messages syslog générés par la session de journalisation de chiffrement.Une fois que cela a été confirmé, vous pouvez passer à l'activation de FlexVPN.
3. Poursuite du concentrateur :
```
interface Virtual-template 1
 no shut
```
4. Sur les rayons :
```
interface tunnel 1
   no shut
```

Étapes de vérification

Stabilité IPsec

La meilleure façon d'évaluer la stabilité IPsec est de surveiller les sylogs avec cette commande de configuration activée :

```
crypto logging session
```
Si vous voyez des sessions s'ouvrir et s'arrêter, cela peut indiquer un problème au niveau IKEv2/FlexVPN qui doit être corrigé avant que la migration puisse commencer.

Informations BGP renseignées

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

Dans le cas de BGP, ceci peut être affiché en effectuant :

```
show bgp
! or
show bgp ipv4 unicast
! or
show ip bgp summary
```
Exemple d'informations correctes à partir du concentrateur :

```
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 concentrateur a appris que 1 préfixe de chacun des rayons et les deux

rayons sont dynamiques (marqués d'un astérisque (*)).

Exemple d'informations similaires provenant du satellite :

```
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
```

Spoke a reçu un préfixe du concentrateur. Dans le cas de cette configuration, ce préfixe doit être le résumé annoncé sur le concentrateur.

Migration vers de nouveaux tunnels à l'aide du protocole EIGRP

Le protocole EIGRP est un choix populaire dans les réseaux DMVPN en raison de son déploiement relativement simple et de sa convergence rapide.

Il va cependant évoluer plus mal que BGP et ne propose pas beaucoup de mécanismes avancés qui peuvent être utilisés par BGP directement.

Cette section décrit l'une des façons de passer à FlexVPN à l'aide d'un nouveau processus EIGRP.

Configuration en étoile mise à jour

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

```
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 : évitez d'établir la contiguïté du protocole de routage sur les tunnels en étoile, et donc ne faites que rendre l'interface du tunnel1 (rayon vers concentrateur) non passive.

Configuration du concentrateur mise à jour

De même, sur le concentrateur, DMVPN doit rester la méthode préférée pour échanger le trafic. Cependant, FlexVPN doit déjà annoncer et apprendre les mêmes préfixes.

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

Il y a deux façons de fournir un résumé en retour vers l'orateur.

- Redistribution d'une route statique pointant vers 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 permet de contrôler le résumé et la redistribution sans toucher à la configuration VT du concentrateur.

- Vous pouvez également configurer une adresse récapitulative de type DMVPN sur Virtual-template. Cette configuration n'est pas recommandée en raison du traitement interne et de la réplication de ce résumé à chaque accès virtuel. Il est présenté ici à titre de 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
```

Migration du trafic vers FlexVPN

La migration doit être effectuée en arrêtant la fonctionnalité DMVPN et en activant FlexVPN.

La procédure suivante garantit un impact minimum.

1. Sur tous les rayons :
```
interface tunnel 0
   shut
```
2. Sur le concentrateur :
```
interface tunnel 0
  shut
```
Àce stade, assurez-vous qu'aucune session IKEv1 n'est établie sur ce concentrateur à partir de rayons.Ceci peut être vérifié en vérifiant la sortie de la commande **show crypto isakmp sa** et en surveillant les messages syslog générés par la session de journalisation de chiffrement.Une fois que cela a été confirmé, vous pouvez passer à l'activation de FlexVPN.
3. Poursuite du concentrateur :
```
interface Virtual-template 1
 no shut
```
4. Sur tous les rayons :
```
interface tunnel 1
   no shut
```

Étapes de vérification

Stabilité IPsec

Comme dans le cas de BGP, vous devez évaluer si IPsec est stable. La meilleure façon de procéder est de surveiller sylogs avec cette commande de configuration activée :

```
crypto logging session
```

Si vous voyez des sessions s'ouvrir et s'arrêter, cela peut indiquer un problème au niveau IKEv2/FlexVPN qui doit être corrigé avant que la migration puisse commencer.

Informations EIGRP dans la table topologique

Assurez-vous que votre table topologique EIGRP est remplie d'entrées LAN en étoile sur le concentrateur et d'un résumé sur les rayons. Vous pouvez le vérifier en exécutant cette

commande sur les concentrateurs et les rayons.

```
show ip eigrp topology
```

Exemple de sortie correcte du rayon :

```
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 remarquerez que Spoke connaît son sous-réseau LAN (en italique) et les résumés pour ceux-ci (en gras).

Exemple de sortie correcte du concentrateur.

```
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 remarquerez que le concentrateur connaît les sous-réseaux LAN des rayons (en italique), le préfixe de résumé qu'il annonce (en **gras**) et l'adresse IP attribuée à chaque rayon par négociation.

Considérations supplémentaires

Tunnels en étoile existants

Comme l'arrêt de l'interface de tunnel DMVPN entraîne la suppression des entrées NHRP, les tunnels existants en étoile seront désactivés.

Suppression des entrées NHRP

Comme mentionné précédemment, un concentrateur FlexVPN ne se basera pas sur le processus d'enregistrement NHRP à partir du rayon pour savoir comment router le trafic. Cependant, les tunnels en étoile dynamique dépendent des entrées NHRP.

Dans DMVPN où l'effacement de NHRP sur le concentrateur aurait pu entraîner des problèmes de connectivité de courte durée.

Dans FlexVPN, la suppression de NHRP sur les rayons entraîne la désactivation de la session IPsec FlexVPN, liée aux tunnels en étoile, En désactivant NHRP, aucun concentrateur n'aura d'effet sur la session FlexVPN.

Ceci est dû au fait que dans FlexVPN, par défaut :

- Les rayons ne s'inscrivent pas aux concentrateurs.
- Les concentrateurs fonctionnent uniquement en tant que redirecteur NHRP et n'installent pas d'entrées NHRP.
- Les entrées de raccourci NHRP sont installées sur les rayons des tunnels de rayon à rayon et sont dynamiques.

Caveats connus

Le trafic Spoke-to-Spoke peut être affecté par CSCub07382.

Informations connexes

- Support et documentation techniques - Cisco Systems