Solutions de dépannage DMVPN les plus fréquentes

Contenu

Introduction

Ce document contient les solutions les plus communes aux problèmes de VPN multipoint dynamique (DMVPN). Plusieurs de ces solutions peuvent être mises en application avant le dépannage en profondeur de la connexion DMVPN. Ce document est présenté comme une liste de contrôle des procédures communes pour essayer avant que vous commenciez à effectuer le dépannage d'une connexion et appeller le support technique de Cisco.

Si vous avez besoin des documents d'exemple de configuration pour le DMVPN, référez-vous aux exemples et au TechNotes de configuration DMVPN.

Note: Référez-vous au dépannage d'IPsec - Comprenant et utilisant des commandes de débogage de fournir une explication des commandes de **débogage** communes qui sont utilisées pour dépanner des questions d'IPsec.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de la configuration DMVPN sur des Routeurs de Cisco IOS®.

Composants utilisés

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

- 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.

Conventions

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

La configuration DMVPN ne fonctionne pas

Problème

Une solution récemment configurée ou modifiée DMVPN ne fonctionne pas.

Du courant DMVPN d'une configuration travaux plus.

Solutions

Cette section contient des solutions aux problèmes DMVPN les plus communs.

Ces solutions (dans aucune commande particulière) peuvent être utilisées comme liste de contrôle des éléments pour vérifier ou de l'essai avant que vous vous engagiez dans le dépannage en profondeur :

- Problèmes courants
- Vérifiez si des paquets d'ISAKMP sont bloqués à l'ISP

- Vérifiez si GRE fonctionne bien à côté d'enlever le tunnel protection
- L'enregistrement de NHRP manque
- Vérifiez si les vies sont configurées correctement
- Vérifiez si la circulation dans seulement une direction
- Vérifiez que le voisin de protocole de routage est établi

Note: Avant que vous commenciez, vérifiez ces derniers :

1. Synchronisation- les horodateurs entre le hub and spoke
2. L'enable **milliseconde mettent au point et se connectent des horodateurs** :`Les horodateurs de Router(config)#service mettent au point la milliseconde date-heureLes horodateurs de Router(config)#service se connectent la milliseconde date-heure`
3. **Horodateur de demande de terminal exec d'**enable pour les sessions d'élimination des imperfections :`Horodateur de demande d'exécutif de Router#terminal`

Note: De cette façon, vous pouvez facilement corréler la **sortie de débogage** avec la **sortie de commande show**.

Problèmes courants

Vérifiez la Connectivité de base

1. Ping du hub au rai utilisant des adresses et l'inverse NBMA.Ces pings devraient passer directement l'interface physique, pas par le tunnel DMVPN. Si tout va bien, il n'y a pas un Pare-feu qui bloque des paquets de ping. Si ceci ne fonctionne pas, vérifiez le routage et tous les Pare-feu entre les Routeurs de hub and spoke.
2. En outre, **traceroute d'**utilisation pour vérifier le chemin que les paquets de tunnel chiffré prennent.
3. Utilisez le **débogage** et les **commandes show** de ne vérifier aucune Connectivité :**debug ip icmp**debug ip packet**Note**: La commande de **debug ip packet** génère une quantité substantielle de sortie et utilise un montant substantiel de ressources système. Cette commande devrait être utilisée avec prudence dans les réseaux de production. Toujours utilisation avec la **commande access-list**.**Note**: Pour plus d'informations sur la façon utiliser la **liste d'accès** avec le **debug ip packet**, référez-vous dépannent avec des Listes d'accès IP.

Vérifiez pour assurer la stratégie ISAKMP incompatible

Si les stratégies ISAKMP configurées ne correspondent pas à la stratégie proposée par l'homologue distant, le routeur essaye la stratégie par défaut 65535. Si cela ne s'assortit pas non plus, il échoue la négociation ISAKMP.

La commande de show crypto isakmp sa affiche que le SA ISAKMP était dans **MM_NO_STATE**, signifiant le principal-mode a manqué.

Vérifiez pour assurer le secret principal pré-partagé incorrect

Si les secrets pré-partagés ne sont pas identiques des deux côtés, la négociation échouera.

Le routeur renvoie le **« contrôle de validité a manqué »** message.

Vérifiez pour assurer le jeu de transformations incompatible d'IPsec

Si le transform-set d'IPsec n'est pas compatible ou mal adapté sur les deux périphériques d'IPsec, la négociation IPSec échouera.

Le routeur renvoie le message **non acceptable de « atts »** pour la proposition d'IPsec.

Vérifiez si des paquets d'ISAKMP sont bloqués à l'ISP

```
Router#show crypto isakmp sa


IPv4 Crypto ISAKMP SA
Dst             src               state    conn-id  slot   status
172.17.0.1  172.16.1.1    MM_NO_STATE     0           0   ACTIVE
172.17.0.1  172.16.1.1    MM_NO_STATE     0           0   ACTIVE (deleted)
172.17.0.5        172.16.1.1        MM_NO_STATE      0             0   ACTIVE
172.17.0.5        172.16.1.1        MM_NO_STATE      0             0   ACTIVE (deleted)
```

Ce qui précède affiche le lien instable de tunnel VPN.

De plus, **debug crypto isakmp de** contrôle à vérifier que le routeur en étoile envoie le paquet de l'UDP 500 :

```
Router#debug crypto isakmp


04:14:44.450: ISAKMP:(0):Old State = IKE_READY
                      New State = IKE_I_MM1
04:14:44.450: ISAKMP:(0): beginning Main Mode exchange
04:14:44.450: ISAKMP:(0): sending packet to 172.17.0.1
              my_port 500 peer_port 500 (I) MM_NO_STATE
04:14:44.450: ISAKMP:(0):Sending an IKE IPv4 Packet.
04:14:54.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
04:14:54.450: ISAKMP (0:0): incrementing error counter on sa,
              attempt 1 of 5: retransmit phase 1
04:14:54.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
04:14:54.450: ISAKMP:(0): sending packet to 172.17.0.1
              my_port 500 peer_port 500 (I) MM_NO_STATE
04:14:54.450: ISAKMP:(0):Sending an IKE IPv4 Packet.
04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
04:15:04.450: ISAKMP (0:0): incrementing error counter on sa,
              attempt 2 of 5: retransmit phase 1
04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
```

Le routeur en étoile ci-dessus d'expositions de **sortie de débogage** envoie le paquet de l'UDP 500 en toutes les 10 secondes.

Vérifiez avec l'ISP pour voir si le routeur en étoile est directement connecté au routeur de l'ISP pour s'assurer qu'ils permettent le trafic de l'UDP 500.

Après que l'ISP ait permis l'UDP 500, ajoutez l'ACL d'arrivée dans l'interface de sortie, qui est source du tunnel pour permettre à l'UDP 500 pour s'assurer le trafic de l'UDP 500 entre dans le routeur. Utilisez la commande access-list d'exposition de vérifier si les nombres de hits incrémentent :

```
Router#show access-lists 101
```

```
Router#show access-lists 101
```

Attention : Veillez-vous pour avoir le **tout d'IP** permis dans votre liste d'accès. Autrement, tout autre trafic sera bloqué en tant que d'arrivée appliqué par **liste d'accès** sur l'interface de sortie.

Vérifiez si GRE fonctionne en enlevant le tunnel protection

Quand DMVPN ne fonctionne pas, avant le dépannage avec IPsec, vérifiez que les tunnels GRE fonctionnent bien sans cryptage d'IPsec.

Le pour en savoir plus, se rapportent configurent le tunnel GRE.

L'enregistrement de NHRP manque

Le tunnel VPN entre le hub and spoke est en hausse, mais incapable de passer le trafic de données :

```
Router#show crypto isakmp sa
        dst             src             state          conn-id  slot   status
        172.17.0.1      172.16.1.1      QM_IDLE           1082    0    ACTIVE

Router#show crypto IPSEC sa
local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
#pkts encaps: 154, #pkts encrypt: 154, #pkts digest: 154
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
inbound esp sas:
spi: 0xF830FC95(4163959957)
outbound esp sas:
spi: 0xD65A7865(3596253285)
!--- !--- Output is truncated !---
```

Il prouve que le trafic de retour ne revient pas de l'autre extrémité du tunnel.

Entrée de NHS de contrôle dans le routeur en étoile :

```
Router#show  ip nhrp nhs detail
Legend: E=Expecting replies, R=Responding
Tunnel0: 172.17.0.1  E  req-sent 0  req-failed 30 repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 4371, Ret 64  NHS 172.17.0.1
```

Il prouve que la demande de NHS manque. Pour résoudre ce problème, assurez-vous que la configuration sur l'interface de tunnel de routeur en étoile est correcte.

Exemple de configuration :

```
interface Tunnel0
 ip address 10.0.0.9 255.255.255.0
```

```
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1
 ip nhrp nhs 172.17.0.1
!--- !--- Output is truncated !---
```

Exemple de configuration avec l'entrée correcte pour le serveur de NHS :

```
interface Tunnel0
 ip address 10.0.0.9 255.255.255.0
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1
 ip nhrp nhs 10.0.0.1
!--- !--- Output is truncated !---
```

Maintenant, vérifiez les compteurs d'entrée de NHS et d'encrypt/decrypt d'IPsec :

```
Router#show ip nhrp nhs detail
Legend: E=Expecting replies, R=Responding
Tunnel0:        10.0.0.1 RE  req-sent 4  req-failed 0  repl-recv 3 (00:01:04 ago)

Router#show crypto IPSec sa
local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
#pkts encaps: 121, #pkts encrypt: 121, #pkts digest: 121
#pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118
inbound esp sas:
spi: 0x1B7670FC(460747004)
outbound esp sas:
spi: 0x3B31AA86(993110662)
!--- !--- Output is truncated !---
```

Vérifiez si les vies sont configurées correctement

Utilisez ces commandes de vérifier la vie de courant SA et le moment pour la prochaine renégociation :

- **show crypto isakmp sa detail**
- *<NBMA-address-peer>* de ***pair de show crypto ipsec sa***

Valeurs de vie d'avis SA. S'ils sont proches des vies configurées (le par défaut est de 24 heures pour l'ISAKMP et 1 heure pour IPsec), alors ce signifie que ces SAS ont été récemment négociées. Si vous regardez un peu de temps plus tard et ils ont été renégociés de nouveau, alors l'ISAKMP et/ou l'IPsec peuvent rebondir en haut et en bas.

```
Router#show crypto ipsec security-assoc lifetime
Security association lifetime: 4608000 kilobytes/3600 seconds

Router#show crypto isakmp policy
Global IKE policy
Protection suite of priority 1
Encryption algorithm: DES-Data Encryption Standard (65 bit keys)
Hash algorithm: Message Digest 5
Authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)
Lifetime: 86400 seconds, no volume limit
Default protection suite
 Encryption algorithm: DES- Data Encryption Standard (56 bit keys)
 Hash algorithm: Secure Hash Standard
 Authentication method: Rivest-Shamir-Adleman Signature
```

```
 Diffie-Hellman group: #1 (768 bit)
 Lifetime: 86400 seconds, no volume limit

Router# show crypto ipsec sa
interface: Ethernet0/3
    Crypto map tag: vpn, local addr. 172.17.0.1
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
   current_peer: 172.17.0.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19
    #pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0
     local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.17.0.1
     path mtu 1500, media mtu 1500
     current outbound spi: 8E1CB77A

 inbound esp sas:
      spi: 0x4579753B(1165587771)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4456885/3531)
        IV size: 8 bytes
        replay detection support: Y
outbound esp sas:
      spi: 0x8E1CB77A(2384246650)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4456885/3531)
        IV size: 8 bytes
        replay detection support: Y
```

Vérifiez si la circulation dans seulement une direction

Le tunnel VPN entre le routeur de spoke-to-spoke est en hausse, mais incapable de passer le trafic de données :

```
Spoke1# show crypto ipsec sa peer 172.16.2.11
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
    #pkts encaps: 110, #pkts encrypt: 110
    #pkts decaps: 0, #pkts decrypt: 0,
local crypto endpt.: 172.16.1.1,
remote crypto endpt.: 172.16.2.11
      inbound esp sas:
      spi: 0x4C36F4AF(1278669999)
      outbound esp sas:
      spi: 0x6AC801F4(1791492596)
!--- !--- Output is truncated !--- Spoke2#sh crypto ipsec sa peer 172.16.1.1
   local  ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   #pkts encaps: 116, #pkts encrypt: 116,
   #pkts decaps: 110, #pkts decrypt: 110,
local crypto endpt.: 172.16.2.11,
remote crypto endpt.: 172.16.1.1
     inbound esp sas:
     spi: 0x6AC801F4(1791492596)
     outbound esp sas:
```

```
     spi: 0x4C36F4AF(1278669999
!--- !--- Output is truncated !---
```

Il n'y a aucun paquet de decap dans spoke1, qui signifie que des paquets de l'ESP sont relâchés quelque part dans le retour de chemin de spoke2 vers spoke1.

L'encap et le decap des routeurs show spoke2, ainsi lui signifie que le trafic de l'ESP est filtré avant spoke2 de atteinte. Il peut se produire à l'extrémité ISP à spoke2 ou à n'importe quel Pare-feu dans le chemin entre le routeur spoke2 et le routeur spoke1. Après avoir permis l'ESP (IP Protocol 50), spoke1 et spoke2 affichent que les encaps et les compteurs de decaps incrémentent.

```
spoke1# show crypto ipsec sa peer 172.16.2.11
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
    #pkts encaps: 300, #pkts encrypt: 300
    #pkts decaps: 200, #pkts decrypt: 200
!--- !--- Output is truncated !--- spoke2#sh crypto ipsec sa peer 172.16.1.1
   local  ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   #pkts encaps: 316, #pkts encrypt: 316,
   #pkts decaps: 300, #pkts decrypt: 310
!--- !--- Output is truncated !---
```

Vérifiez que le voisin de protocole de routage est établi

Les rais ne peuvent pas établir des relations voisines de protocole de routage :

```
Hub# show ip eigrp neighbors
H   Address     Interface   Hold Uptime     SRTT    RTO   Q  Seq
                                (sec)             (ms)  Cnt Num
2   10.0.0.9     Tu0         13  00:00:37     1    5000   1  0
0   10.0.0.5     Tu0         11 00:00:47   1587   5000   0 1483
1   10.0.0.11    Tu0         13 00:00:56     1    5000   1  0
Syslog message:
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10:
Neighbor 10.0.0.9 (Tunnel0) is down: retry limit exceeded

Hub# show ip route eigrp
172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, FastEthernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 172.17.0.100
```

Vérifiez si le mappage de Multidiffusion de NHRP est configuré correctement dans le hub.

Dans le hub, on l'exige pour avoir le mappage dynamique de Multidiffusion de NHRP configuré dans l'interface de tunnel de hub.

Exemple de configuration :

```
Hub# show ip eigrp neighbors
H   Address     Interface   Hold Uptime     SRTT    RTO   Q  Seq
                                (sec)             (ms)  Cnt Num
2   10.0.0.9     Tu0         13  00:00:37     1    5000   1  0
0   10.0.0.5     Tu0         11 00:00:47   1587   5000   0 1483
```

```
1   10.0.0.11     Tu0          13 00:00:56     1    5000   1  0
Syslog message:
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10:
Neighbor 10.0.0.9 (Tunnel0) is down: retry limit exceeded

Hub# show ip route eigrp
172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, FastEthernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 172.17.0.100
```

Exemple de configuration avec l'entrée correcte pour le mappage dynamique de Multidiffusion de NHRP :

```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 no ip next-hop-self eigrp 10
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 10
 no ip split-horizon eigrp 10
 tunnel mode gre multipoint
!--- !--- Output is truncated !---
```

Ceci permet au NHRP pour ajouter automatiquement des routeurs en étoile aux mappages de NHRP de Multidiffusion.

Le pour en savoir plus, se rapportent à la section d'**ip nhrp map multicast dynamic de** commandes de NHRP.

```
Hub#show ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address      Interface   Hold   Uptime    SRTT     RTO      Q      Seq
                                              (sec)    (ms)    Cnt    Num
2   10.0.0.9     Tu0          12   00:16:48   13      200      0      334
1   10.0.0.11    Tu0          13   00:17:10   11      200      0      258
0   10.0.0.5     Tu0          12   00:48:44  1017     5000     0      1495

Hub#show ip route

     172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, FastEthernet0/0
D    192.168.11.0/24 [90/2944000] via 10.0.0.11, 00:16:12, Tunnel0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, FastEthernet0/1
D    192.168.2.0/24 [90/2818560] via 10.0.0.9, 00:15:45, Tunnel0
S*   0.0.0.0/0 [1/0] via 172.17.0.100
```

Des artères aux rais sont apprises par le protocole d'eigrp.

Problème avec intégrer la remote-access VPN avec DMVPN

Problème

DMVPN fonctionne bien, mais incapable d'établir le RAVPN.

Solution

Employez les profils et les profils IPSecs d'ISAKMP pour réaliser ceci.

Créez les profils distincts pour le DMVPN et le RAVPN.

Le pour en savoir plus, se rapportent à DMVPN et à serveur Easy VPN avec l'exemple de configuration de profils d'ISAKMP.

Problème avec double-hub-double-dmvpn.

Problème

Problème avec double-hub-double-dmvpn. Spécifiquement, les tunnels vont vers le bas et incapable de renégocier.

Solution

Utilisez le mot clé partagé dans la protection d'IPsec de tunnel pour les les deux les interfaces de tunnel sur le hub, et sur le rai également.

Exemple de configuration :

```
Hub#show ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address      Interface   Hold   Uptime   SRTT     RTO      Q      Seq
                                             (sec)    (ms)    Cnt    Num
2   10.0.0.9      Tu0         12   00:16:48   13      200      0      334
1   10.0.0.11     Tu0         13   00:17:10   11      200      0      258
0   10.0.0.5      Tu0         12   00:48:44  1017    5000      0      1495

Hub#show ip route

     172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, FastEthernet0/0
D    192.168.11.0/24 [90/2944000] via 10.0.0.11, 00:16:12, Tunnel0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, FastEthernet0/1
D    192.168.2.0/24 [90/2818560] via 10.0.0.9, 00:15:45, Tunnel0
S*   0.0.0.0/0 [1/0] via 172.17.0.100
```

Le pour en savoir plus, se rapportent à la section de **tunnel protection** dans la référence de commandes de Cisco IOS Security.

Préoccupez se connecter dans un serveur par DMVPN

Problème

Sortez avec accéder à un serveur par le réseau DMVPN.

Solution

Le problème pourrait être lié à la taille de MTU et MSS du paquet qui utilise GRE et IPsec.

Maintenant, la longueur de paquet a pu être une question avec la fragmentation. Pour éliminer ce problème, utilisez ces commandes :

```
ip mtu 1400
ip tcp adjust-mss 1360
crypto IPSec fragmentation after-encryption (global)
```

Vous pourriez également configurer la commande de **tunnel path-mtu-discovery** de découvrir dynamiquement la taille de MTU.

Pour une explication plus détaillée, référez-vous à la fragmentation IP de résolution, aux questions de MTU, MSS, et PMTUD avec GRE et IPSEC.

Incapable d'accéder aux serveurs sur DMVPN par certains ports

Problème

Incapable aux serveurs d'accès sur DMVPN par les ports spécifiques.

Solution

Vérifiez en désactivant l'ensemble de caractéristiques du pare-feu d'IOS et voyez si cela fonctionne.

S'il fonctionne bien, alors le problème est rapporté au config du pare-feu d'IOS, pas avec le DMVPN.

Informations connexes

- VPN multipoint dynamique (DMVPN)
- Négociation IPSec/Protocoles IKE
- Support et documentation techniques - Cisco Systems