Dépannage des problèmes courants de DMVPN

Table des matières

Introduction

Ce document décrit les solutions les plus courantes aux problèmes de VPN multipoint dynamique (DMVPN).

Conditions préalables

Exigences

Cisco recommande que vous ayez des connaissances sur la configuration de DMVPN sur les routeurs Cisco IOS® .

Composants utilisés

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

- Cisco IOS

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.

Conventions

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

Informations générales

Ce document décrit les solutions les plus courantes aux problèmes de VPN multipoint dynamique (DMVPN). La plupart de ces solutions peuvent être mises en oeuvre avant tout dépannage approfondi 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.

Pour plus d'informations, référez-vous au Guide de configuration VPN multipoint dynamique, Cisco IOS version 15M&T .

Référez-vous à Comprendre et utiliser les commandes de débogage pour dépanner IPsec pour fournir une explication des commandes de débogage courantes qui sont utilisées pour dépanner les problèmes IPsec.

La configuration DMVPN ne fonctionne pas

Problème

Une solution DMVPN récemment configurée ou modifiée ne fonctionne pas.

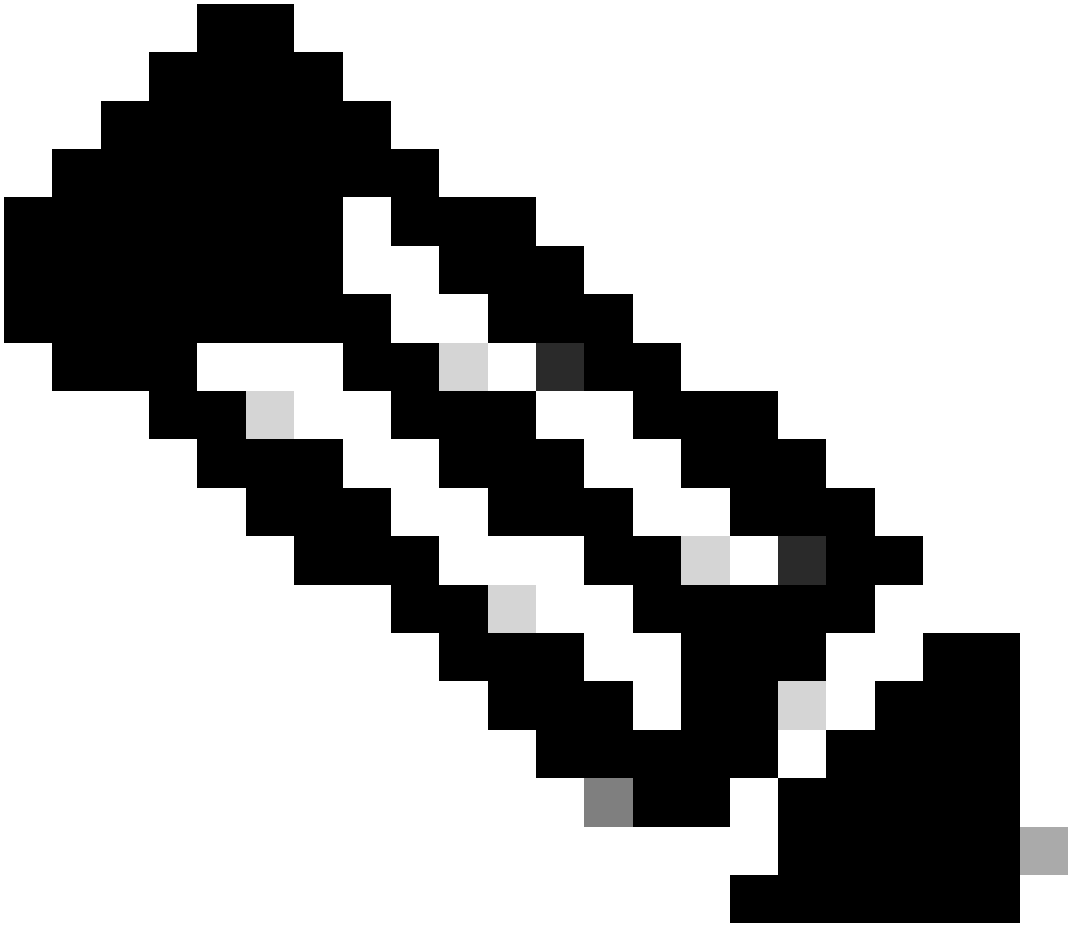
Une configuration actuelle de DMVPN ne fonctionne plus.

Solutions

Cette section contient des solutions aux problèmes de DMVPN les plus courants.

Ces solutions (sans ordre particulier) peuvent être utilisées comme liste de contrôle des éléments à vérifier ou à essayer avant de procéder à un dépannage approfondi :

- Problèmes courants
- Vérifiez si les paquets ISAKMP (Internet Security Association and Key Management Protocol) sont bloqués chez le fournisseur d'accès Internet (FAI)
- Vérifiez si l'encapsulation de routage générique (GRE) fonctionne lorsque la protection du tunnel est supprimée
- Échec de l'enregistrement du protocole NHRP (Next-Hop Resolution Protocol)
- Vérifiez si les durées de vie sont correctement configurées
- Vérifiez si le trafic est acheminé dans une seule direction
- Vérifiez que le voisin du protocole de routage est établi



Remarque : avant de commencer, vérifiez les étapes suivantes :

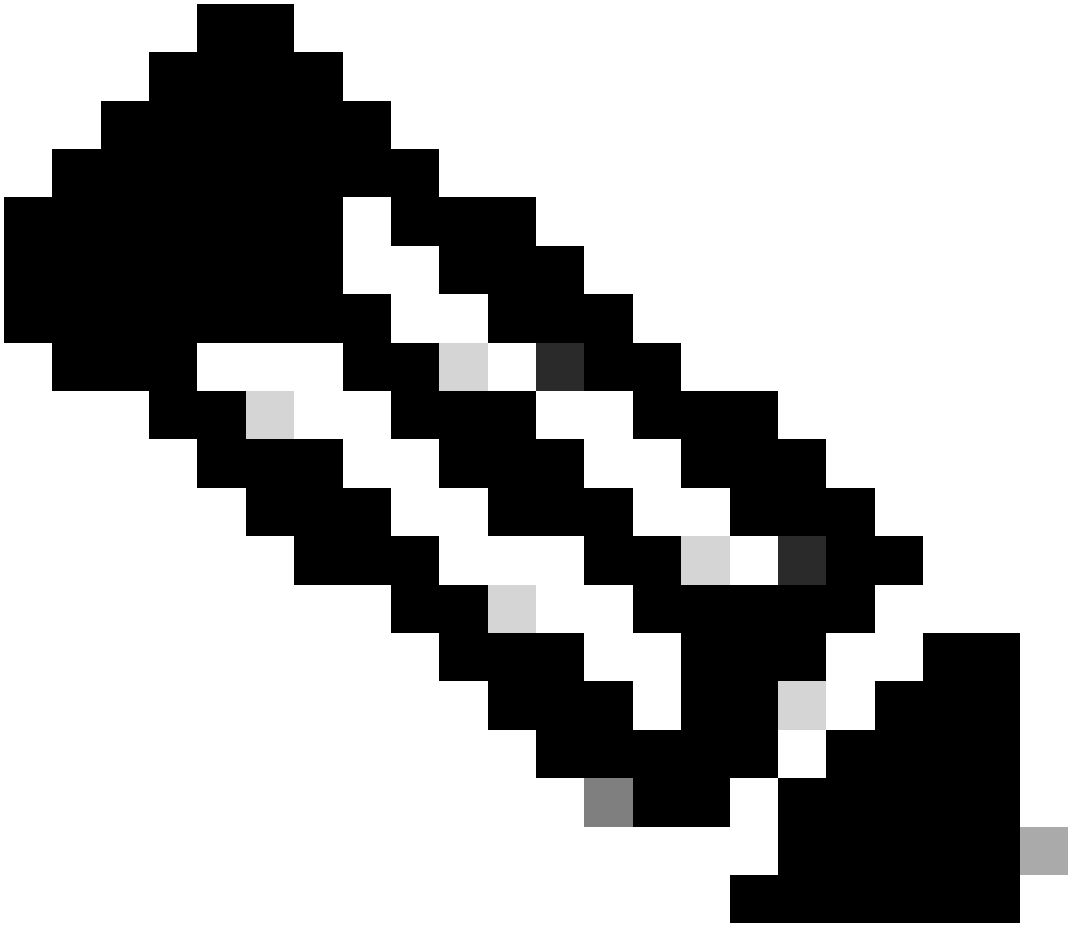
1. Synchronisez l’horodatage entre les éléments du réseau en étoile
2. Activez msec debug and log timestamps :

```
Router(config)#service timestamps debug datetime msec

Router(config)#service timestamps log datetime msec
```

3. Activez terminal exec prompt timestamp pour les sessions de débogage :

```
Router#terminal exec prompt timestamp
```



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

Problèmes courants

Vérifiez la connectivité de base

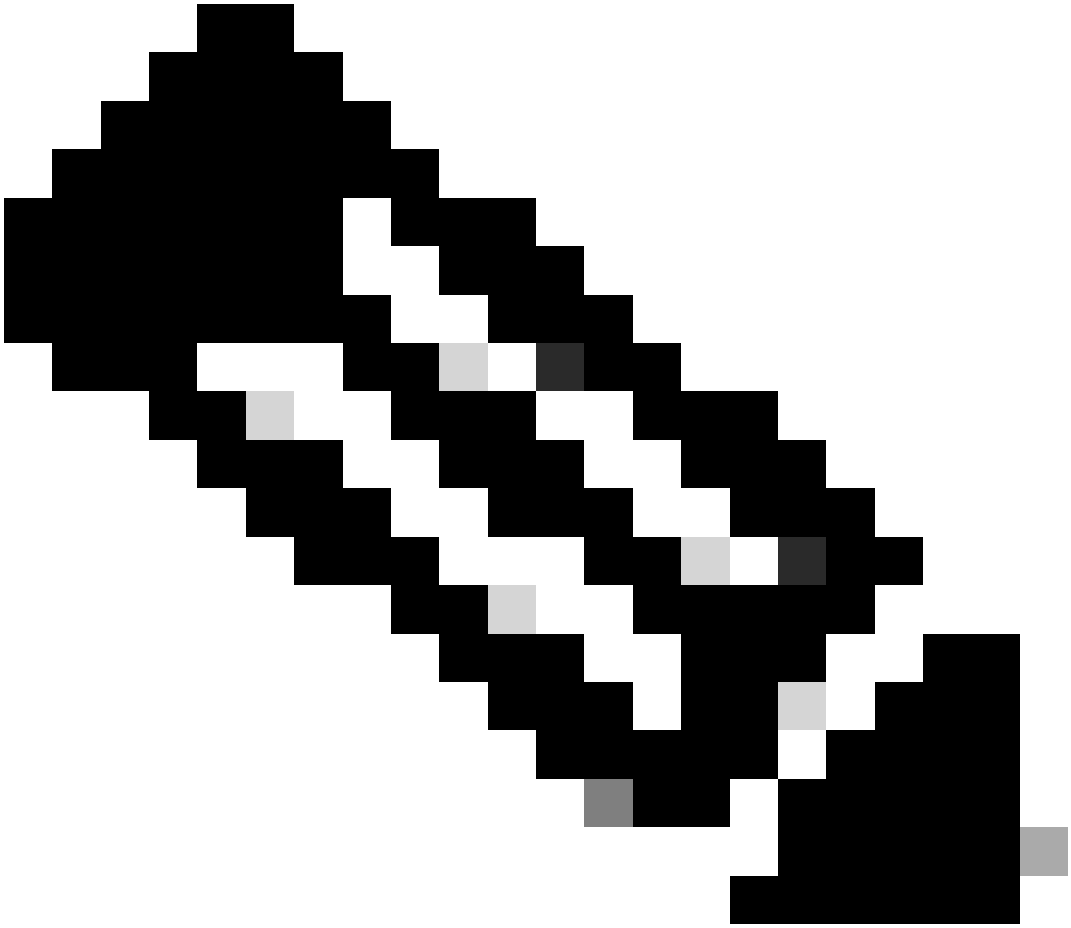
1. Envoyez une requête ping du concentrateur vers le rayon avec des adresses NBMA et inversement.

   Ces requêtes ping doivent sortir directement de l'interface physique, et non via le tunnel DMVPN. Avec un peu de chance, il n’y a pas de pare-feu qui bloque les paquets ping. Si cette option ne fonctionne pas, vérifiez le routage et les pare-feu qui se trouvent entre les routeurs du réseau en étoile.

2. En outre, utilisez traceroute pour vérifier le chemin que les paquets de tunnel chiffrés prennent.

3. Utilisez les commandes debug (déboguer) et show (afficher) pour vérifier s’il n’y a aucune connectivité :

    - debug ip icmp
    - debug ip packet



Remarque : la commande debug IP packet génère une quantité importante de résultats et utilise une quantité importante de ressources système. Cette commande doit être utilisée avec précaution dans les réseaux de production. Toujours utiliser avec la commande access-list (liste d’accès). Pour plus d'informations sur la façon d'utiliser la liste de contrôle d'accès avec le paquet IP de débogage, référez-vous à Dépannage avec les listes de contrôle d'accès IP.

Vérifiez si la politique ISAKMP est 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. S'il n'y a pas de correspondance, la négociation ISAKMP échoue.

La commande show crypto isakmp sa montre que la SA ISAKMP est dans MM_NO_STATE, ce qui signifie que le mode principal a échoué.

Vérifiez s'il y a des secrets de clés partagées qui sont inexacts

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

Le routeur renvoie le message d'échec du contrôle d'intégrité.

Vérifiez l'ensemble de transformation IPsec pour une incompatibilité

Si le transform-set IPsec n'est pas compatible ou ne correspond pas sur les deux périphériques IPsec, la négociation IPsec échoue.

Le routeur renvoie le message atts not acceptable pour la proposition IPsec.

Vérifiez si les paquets ISAKMP sont bloqués à ISP

<#root>

```
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)
```

L'exemple précédent montre l'oscillation du tunnel VPN.

En outre, vérifiez`debug crypto isakmp` que le routeur en étoile envoie le paquet udp 500 :

<#root>

```
Router#
```

debug crypto isakmp

<#root>

```
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`debug` résultat précédent montre que le routeur en étoile envoie un paquet UDP 500 toutes les 10 secondes.

Vérifiez auprès du FAI si le routeur en étoile est directement connecté au routeur FAI pour vous assurer qu'il autorise le trafic UDP 500.

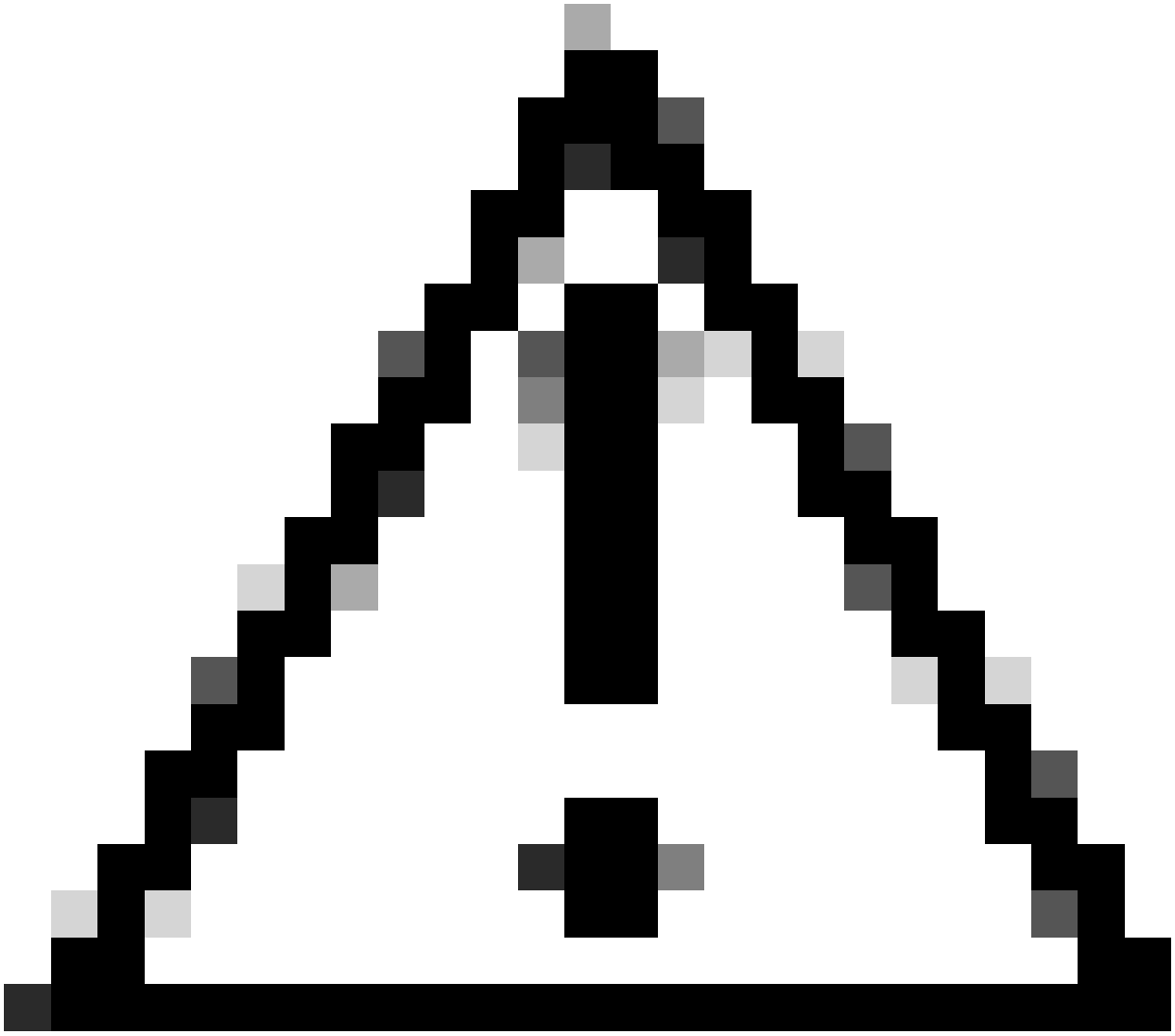
Une fois que ISP a autorisé UDP 500, ajoutez une liste de contrôle d'accès entrante dans l'interface de sortie, qui est la source du tunnel pour autoriser UDP 500 afin de s'assurer que le trafic UDP 500 arrive dans le routeur. Utilisez la`show access-list`commande pour vérifier si le nombre de succès augmente.

<#root>

```
Router#

show access-lists 101
```

```
Extended IP access list 101
    10 permit udp host 172.17.0.1 host 172.16.1.1 eq isakmp log (4 matches)
    20 permit udp host 172.17.0.5 host 172.16.1.1 eq isakmp log (4 matches)
    30 permit ip any any (295 matches)
```



Attention : assurez-vous que votre liste de contrôle d'accès contient IP any any. Sinon, tout autre trafic peut être bloqué en tant que liste d'accès appliquée en entrée sur l'interface de sortie.

Vérifier si GRE fonctionne lorsque la protection de tunnel est supprimée

Lorsque DMVPN ne fonctionne pas, avant de procéder au dépannage avec IPsec, vérifiez que les tunnels GRE fonctionnent correctement sans cryptage IPsec.

Pour plus d'informations, référez-vous à Comment configurer un tunnel GRE.

Échec de l'enregistrement NHRP

Le tunnel VPN entre les éléments du réseau en étoile est en fonction, mais il est impossible de faire passer le trafic de données :

<#root>

```
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
```

<#root>

```
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 indique que le trafic de retour ne revient pas de l'autre extrémité du tunnel.

Vérifiez l’entrée NHS dans le routeur Spoke :

<#root>

```
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
```

Elle indique que la requête NHS a échoué. Pour résoudre ce problème, assurez-vous que la configuration de l’interface de tunnel de routeur Spoke est exacte.

Exemple de configuration :

<#root>

```
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 NHS :

<#root>

```
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 l'entrée de NHS et les compteurs de chiffrement/déchiffrement IPsec :

<#root>

```
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 durées de vie sont correctement configurées

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

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

Observez les valeurs de durée de vie de la SA. S'il s'agit de valeurs semblables aux durées de vie configurées (les valeurs par défaut sont 24 heures pour ISAKMP et 1 heure pour IPsec), cela signifie que ces SA ont été négociées récemment. Si vous regardez un peu plus tard et qu'ils ont été négociés à nouveau, l'ISAKMP et/ou IPsec peuvent rebondir de haut en bas.

<#root>

```
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 le trafic est acheminé dans une seule direction

Le tunnel VPN entre les éléments de la configuration de routage Spoke-à-Spoke est en fonction, mais il est impossible de faire passer le trafic de données .

<#root>

```
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 au niveau du routeur Spoke1. Cela signifie que les paquets esp sont perdus sur le trajet du retour du routeur Spoke2 au routeur Spoke1.

Le routeur spoke2 affiche les protocoles encap et decap, ce qui signifie que le trafic ESP est filtré avant d'atteindre spoke2. Cela peut se produire à l'extrémité FAI à spoke2 ou à tout pare-feu dans le chemin entre le routeur spoke2 et le routeur spoke1. Après avoir autorisé ESP (IP Protocol 50), spoke1 et spoke2 affichent tous deux l'incrémentation des compteurs d'encapsulation et de décapsulation.

<#root>

```
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 du protocole de routage est établi

Les routeurs Spoke ne prviennent pas à établir la relation voisin de protocole de routage :

<#root>

```
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 la multidiffusion de NHRP est correctement configurée dans le concentrateur.

Dans le concentrateur, il faut que la mise en correspondance de la multidiffusion de nhrp dynamique soit configurée dans l'interface de tunnel du concentrateur.

Exemple de configuration :

```
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 network-id 10
 no ip split-horizon eigrp 10
 tunnel mode gre multipoint

!--- !--- Output is truncated !---
```

Exemple de configuration avec l'entrée correcte pour la mise en correspondance de la multidiffusion nhrp dynamique :

<#root>

```
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 !---
```

Cela permet au NHRP d'ajouter automatiquement les routeurs Spoke pour la mise en correspondance de NHRP de multidiffusion.

Pour plus d'informations, référez-vous à la`ip nhrp map multicast dynamic` commande dans le Guide de référence des commandes des services d'adressage IP Cisco IOS.

<#root>

```
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 routage vers les routeurs Spokes est décrit dans le protocole eigrp.

Problème avec VPN d'accès à distance avec intégration DMVPN

Problème

DMVPN fonctionne correctement, mais ne parvient pas à établir le RAVPN.

Solution

Utilisez des profils ISAKMP et des profils IPsec pour y parvenir. Créez des profils distincts pour DMVPN et pour RAVPN.

Pour en savoir plus, consultez l’exemple de configuration de DMVPN et Easy VPN avec des profils ISAKMP.

Problème lié à dual-hub-dual-dmvpn

Problème

Problème lié à dual-hub-dual-dmvpn. Plus précisément, les tunnels tombent en panne et ne peuvent pas renégocier.

Solution

Utilisez le mot clé shared dans la protection IPsec du tunnel pour les interfaces du tunnel sur le concentrateur, ainsi que sur le rayon.

Exemple de configuration :

```
interface Tunnel43
 description <<tunnel to primary cloud>>
 tunnel source interface vlan10
 tunnel protection IPSec profile myprofile shared

!--- !--- Output is truncated !---

interface Tunnel44
 description <<tunnel to secondary cloud>>
 tunnel source interface vlan10
 tunnel protection IPSec profile myprofile shared

!--- !--- Output is truncated !---
```

Pour plus d'informations, référez-vous à la**tunnel protection** commande dans le Guide de référence des commandes de sécurité de Cisco IOS (A-C).

Problème de connexion à un serveur via DMVPN

Problème

Impossible d'accéder au trafic du problème via le serveur réseau DMVPN.

Solution

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

Maintenant, la taille de paquet pourrait créer un problème, dans le contexte de la fragmentation. Pour éliminer ce problème, utilisez ces commandes :

<#root>

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

Vous pouvez également configurer la **tunnel path-mtu-discovery** commande pour détecter dynamiquement la taille de MTU.

Pour une explication plus détaillée, référez-vous àRésoudre les problèmes de fragmentation IP, MTU, MSS et PMTUD avec GRE et IPSEC.

Impossible d’accéder aux serveurs sur DMVPN par l’entremise de certains ports

Problème

Impossible d’accéder aux serveurs sur DMVPN par l’entremise de ports en particulier.

Solution

Pour vérifier si le jeu de fonctions du pare-feu Cisco IOS est désactivé et s'il fonctionne.

Si cela fonctionne correctement, le problème est lié à la configuration du pare-feu Cisco IOS et non au DMVPN.

Informations connexes

- VPN multipoint dynamique (DMVPN)
- Négociation IPSec/Protocoles IKE
- Assistance technique de Cisco et téléchargements

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.