Guide de dépannage des débogages de phase 1 DMVPN

Contenu

Introduction

Ce document décrit les messages de débogage que vous rencontreriez sur le concentrateur et parle d'un déploiement DMVPN (Dynamic Multipoint Virtual Private Network) de phase 1.

Conditions préalables

Pour les commandes de configuration et de débogage de ce document, vous aurez besoin de deux routeurs Cisco qui exécutent Cisco IOS® version 12.4(9)T ou ultérieure. En règle générale, une DMVPN de base Phase 1 nécessite Cisco IOS version 12.2(13)T ou ultérieure ou version 12.2(33)XNC pour le routeur ASR (Aggregation Services Router), bien que les fonctionnalités et les débogages présentés dans ce document ne soient pas pris en charge.

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Encapsulation de routage générique (GRE)
- Protocole NHRP (Next Hop Resolution Protocol)
- ISAKMP (Internet Security Association and Key Management Protocol)
- IKE (Internet Key Exchange)
- Sécurité du protocole Internet (IPSec)
- Au moins un de ces protocoles de routage : EIGRP (Enhanced Interior Gateway Routing Protocol), OSPF (Open Shortest Path First), RIP (Routing Information Protocol) et BGP (Border Gateway Protocol)

Components Used

Les informations de ce document sont basées sur les routeurs à services intégrés (ISR) Cisco 2911 qui exécutent Cisco IOS version 15.1(4)M4.

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. If your network is live, make sure that you understand the potential impact of any command.

Améliorations importantes

Ces versions de Cisco IOS ont introduit des fonctionnalités ou des correctifs importants pour DMVPN Phase 1 :

- Version 12.2(18)SXF5 : meilleure prise en charge d'ISAKMP lors de l'utilisation de l'infrastructure à clé publique (PKI)
- Version 12.2(33)XNE - ASR, profils IPSec, protection du tunnel, NAT (Network Address Translation) IPSec
- Version 12.3(7)T : prise en charge du routage et transfert virtuels (iVRF)
- Version 12.3(11)T : prise en charge du routage et transfert virtuels (fVRF) de porte d'entrée
- Version 12.4(9)T : prise en charge de divers débogages et commandes DMVPN
- Version 12.4(15)T - Protection par tunnel partagé
- Version 12.4(20)T - IPv6 sur DMVPN
- Version 15.0(1)M - Surveillance de l'intégrité du tunnel NHRP

Conventions

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

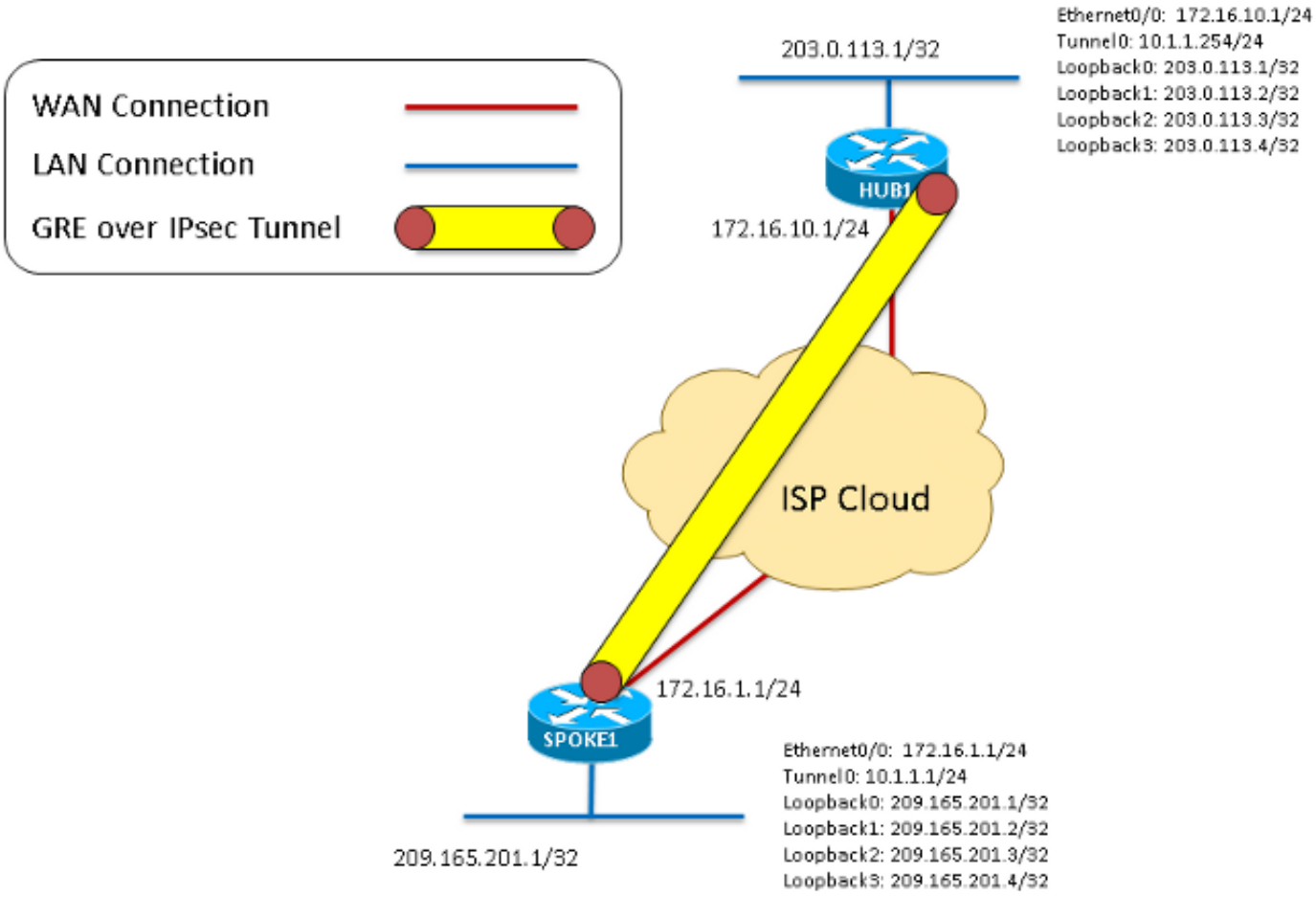
Configuration pertinente

Présentation de la topologie

Pour cette topologie, deux routeurs ISR 2911 qui exécutent la version 15.1(4)M4 ont été configurés pour DMVPN Phase 1 : un en tant que concentrateur et un en tant que rayon. Ethernet0/0 a été utilisé comme interface Internet sur chaque routeur. Les quatre interfaces de

bouclage sont configurées pour simuler les réseaux locaux qui vivent au niveau du concentrateur ou du site en étoile. Comme il s'agit d'une topologie DMVPN de phase 1 avec un seul rayon, le rayon est configuré avec un tunnel GRE point à point plutôt qu'un tunnel GRE multipoint. La même configuration de chiffrement (ISAKMP et IPSec) a été utilisée sur chaque routeur pour s'assurer qu'ils correspondent exactement.

Diagramme 1



Crypto

C'est la même chose sur le concentrateur et le rayon.

```
crypto isakmp policy 1
encr 3des
hash sha
authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set DMVPN-TSET esp-3des esp-sha-hmac
mode transport
crypto ipsec profile DMVPN-IPSEC
set transform-set DMVPN-TSET
```

Concentrateur

```
interface Tunnel0
ip address 10.1.1.254 255.255.255.0
no ip redirects
```

```
ip mtu 1400
ip nhrp authentication NHRPAUTH
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip tcp adjust-mss 1360
no ip split-horizon eigrp 1
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel key 1
tunnel protection ipsec profile DMVPN-IPSEC
end

interface Ethernet0/0
ip address 172.16.10.1 255.255.255.0
end

interface Loopback0
ip address 203.0.113.1 255.255.255.255
interface Loopback1
ip address 203.0.113.2 255.255.255.255
interface Loopback2
ip address 203.0.113.3 255.255.255.255
interface Loopback3
ip address 203.0.113.4 255.255.255.255

router eigrp 1
network 10.1.1.0 0.0.0.255
network 203.0.113.1 0.0.0.0
network 203.0.113.2 0.0.0.0
network 203.0.113.3 0.0.0.0
network 203.0.113.4 0.0.0.0
```

Spoke

```
interface Tunnel0
ip address 10.1.1.1 255.255.255.0
ip mtu 1400
ip nhrp authentication NHRPAUTH
ip nhrp map 10.1.1.254 172.16.10.1
ip nhrp network-id 1
ip nhrp nhs 10.1.1.254
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel destination 172.16.10.1
tunnel key 1
tunnel protection ipsec profile DMVPN-IPSEC
end

interface Ethernet0/0
ip address 172.16.1.1 255.255.255.0
end

interface Loopback0
ip address 209.165.201.1 255.255.255.255
interface Loopback1
ip address 209.165.201.2 255.255.255.255
interface Loopback2
ip address 209.165.201.3 255.255.255.255
interface Loopback3
ip address 209.165.201.4 255.255.255.255

router eigrp 1
network 209.165.201.1 0.0.0.0
```

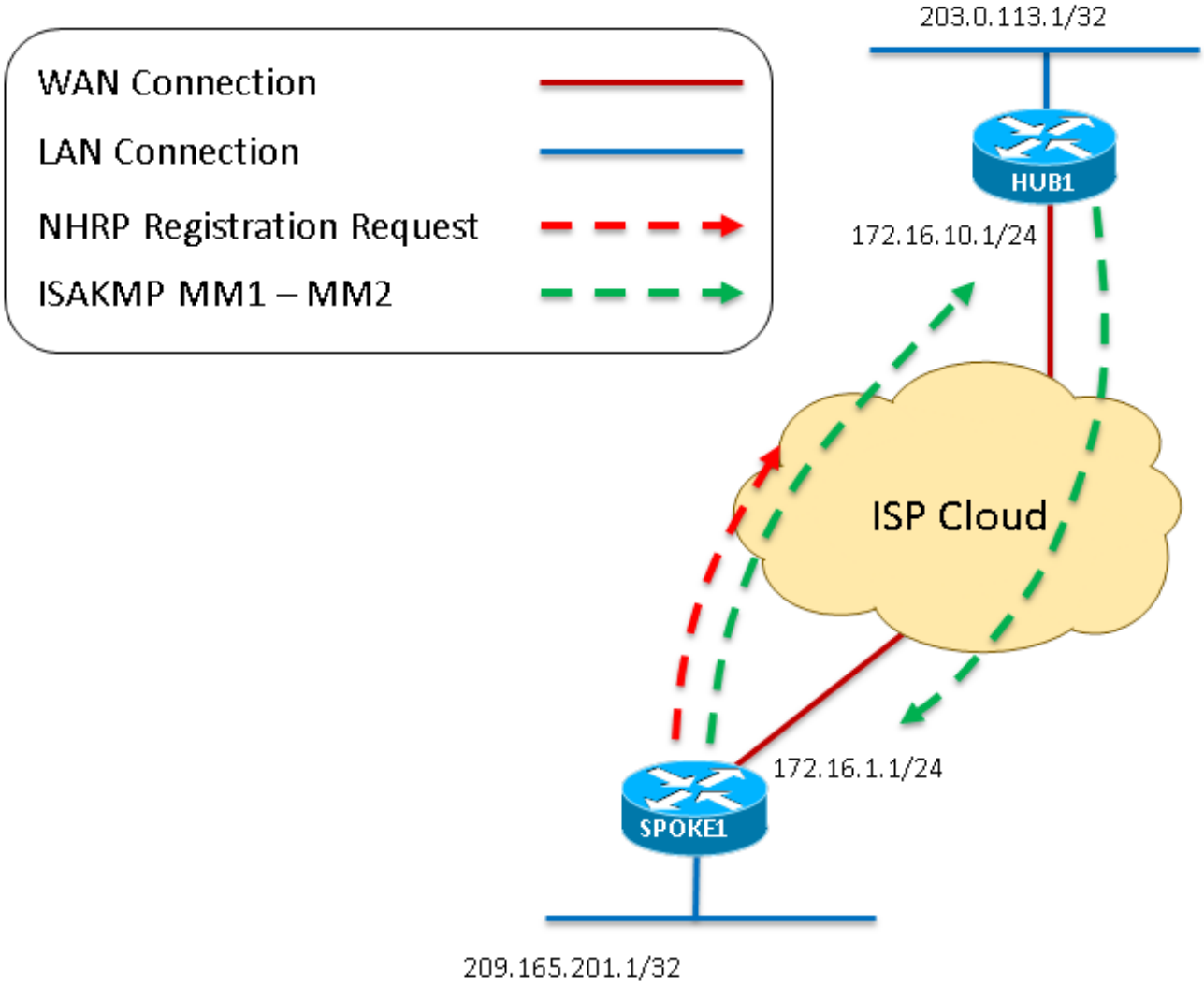
```
network 209.165.201.2 0.0.0.0
network 209.165.201.3 0.0.0.0
network 209.165.201.4 0.0.0.0
network 10.1.1.0 0.0.0.255
```

Déboguages

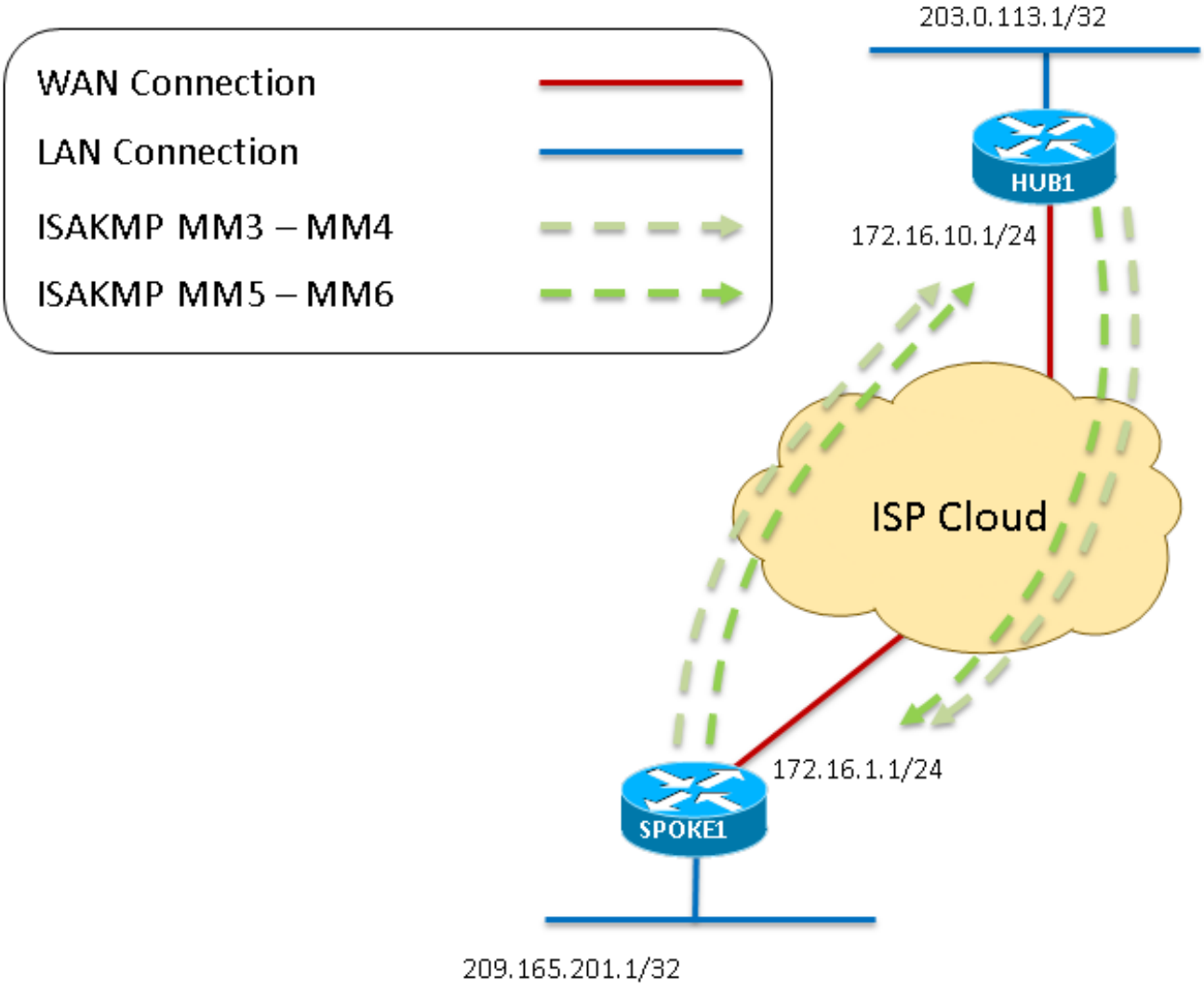
Visualisation du flux de paquets

Il s'agit d'une visualisation de l'intégralité du flux de paquets DMVPN, comme le montre ce document. Des débogages plus détaillés qui expliquent chacune des étapes sont également inclus.

1. Lorsque le tunnel sur le satellite est “ no shutdown ” il génère une requête d'enregistrement NHRP, qui démarre le processus DMVPN. Comme la configuration du concentrateur est complètement dynamique, le point de terminaison Spoke doit être le point d’extrémité qui initie la connexion.
2. La requête d'enregistrement NHRP est ensuite encapsulée dans GRE, ce qui déclenche le démarrage du processus de chiffrement.
3. Àce stade, le premier message ISAKMP Main Mode - ISAKMP MM1 - est envoyé du satellite au concentrateur sur le port UDP500.
4. Le concentrateur reçoit et traite MM1 et répond avec ISAKMP MM2, car il possède une stratégie ISAKMP correspondante.
   Diagramme 2 - fait référence aux étapes 1 à
   4

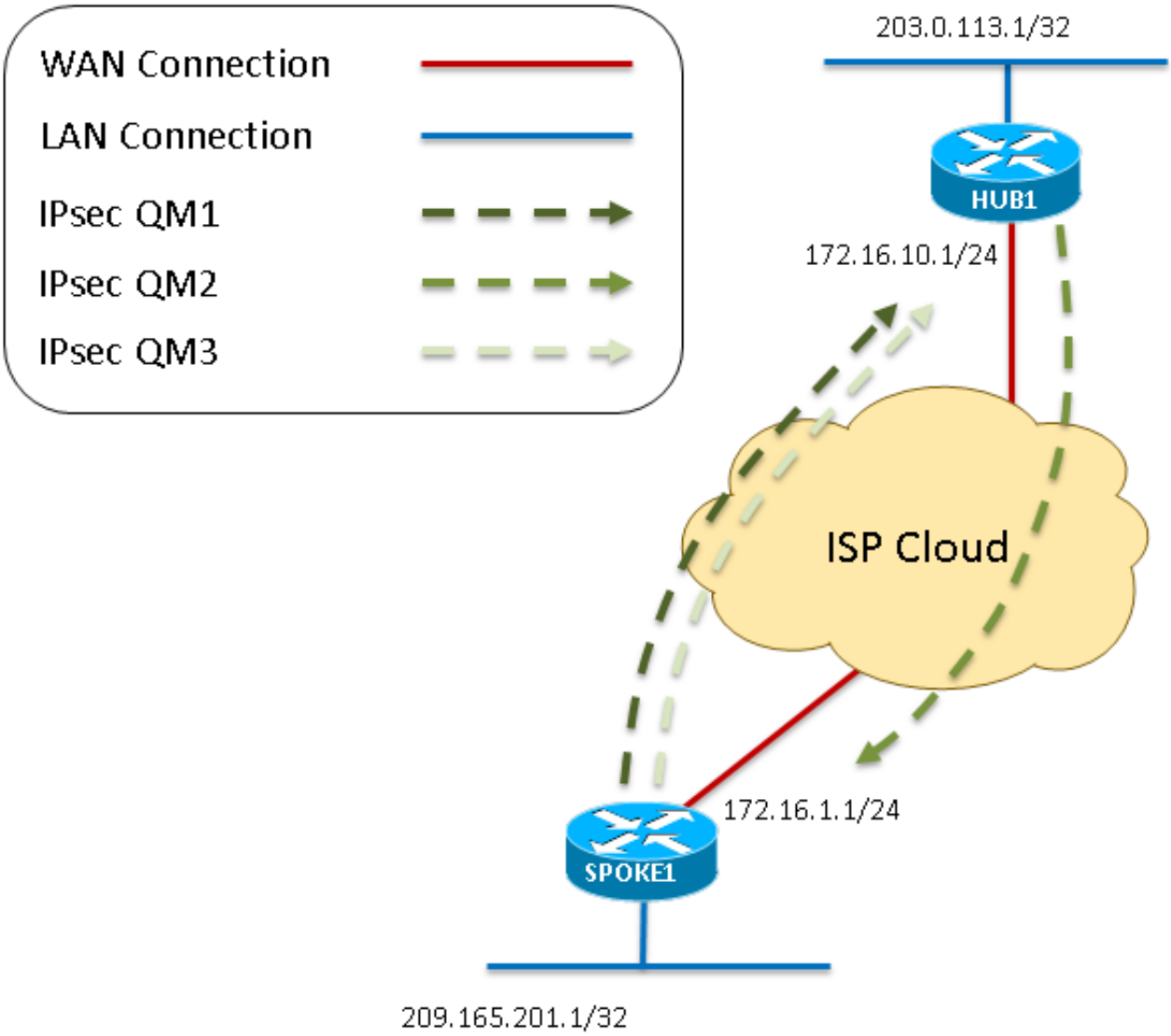


5. Une fois que le Spoke reçoit le MM2, il répond avec le MM3. Comme pour MM1, le Spoke confirme que la politique ISAKMP reçue est valide.
6. Le concentrateur reçoit MM3 et répond avec MM4.
7. Àce stade de la négociation ISAKMP, le Spoke peut répondre sur le port UDP4500 si NAT est détecté dans le chemin de transit. Cependant, si aucune NAT n'est détectée, Spoke continue et envoie MM5 sur UDP500. Enfin, le concentrateur répond avec MM6 afin de terminer l'échange en mode principal.
   Diagramme 3 - fait référence aux étapes 5 à
   7

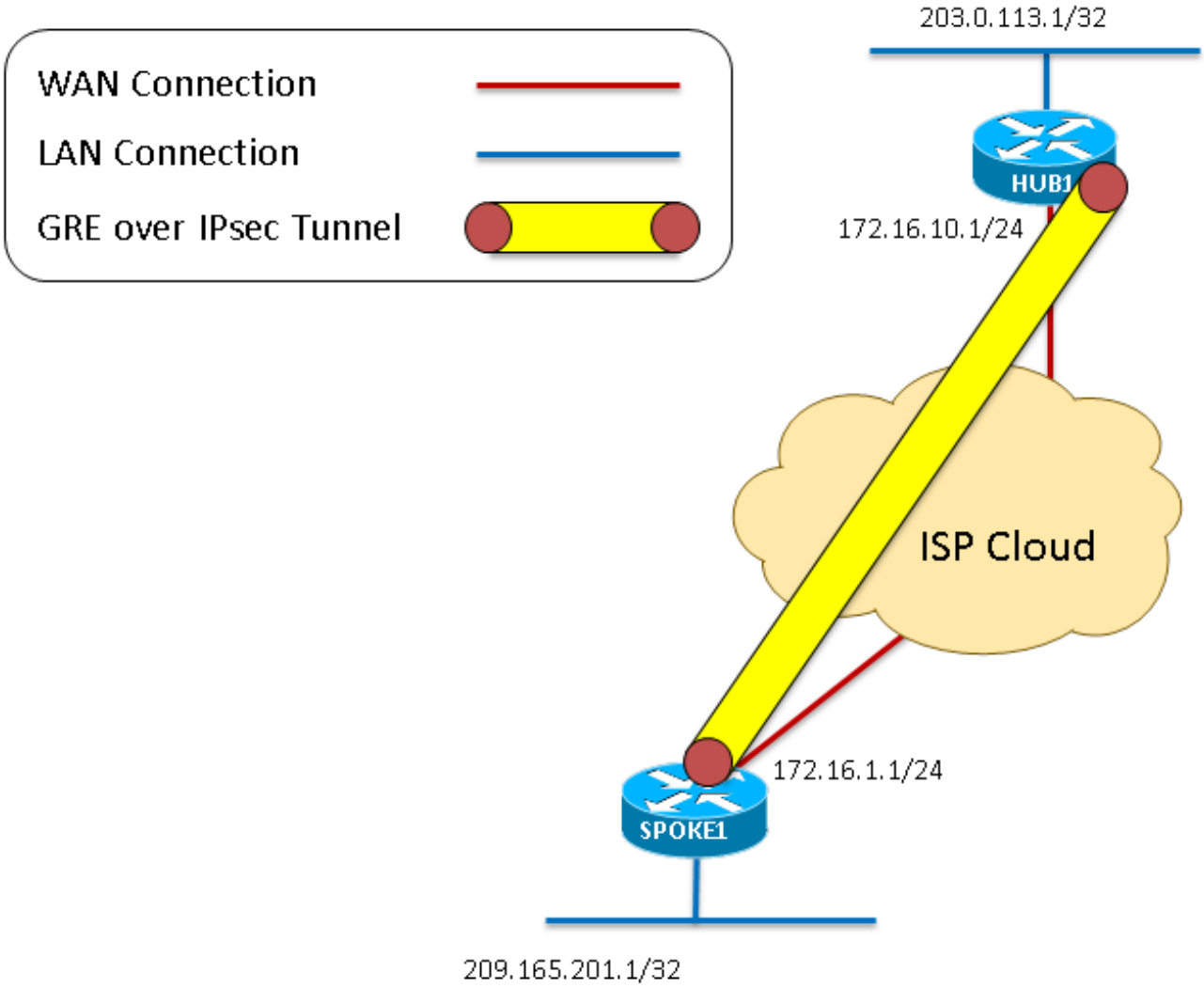


8. Une fois que le Spoke reçoit MM6 du concentrateur, il envoie QM1 au concentrateur sur UDP500 afin de commencer le mode rapide.
9. Le concentrateur reçoit QM1 et répond avec QM2, car tous les attributs reçus sont acceptés. À ce stade, le concentrateur crée les SA de phase 2 pour cette session.
10. Comme dernière étape de la négociation en mode rapide, QM2 est reçu par la Spoke. Le Spoke crée ensuite ses SA de phase 2 et envoie QM3 en réponse. Ceci termine la négociation ISAKMP et IPSec. Il existe maintenant une session IPSec qui chiffre le trafic GRE entre ces deux homologues.

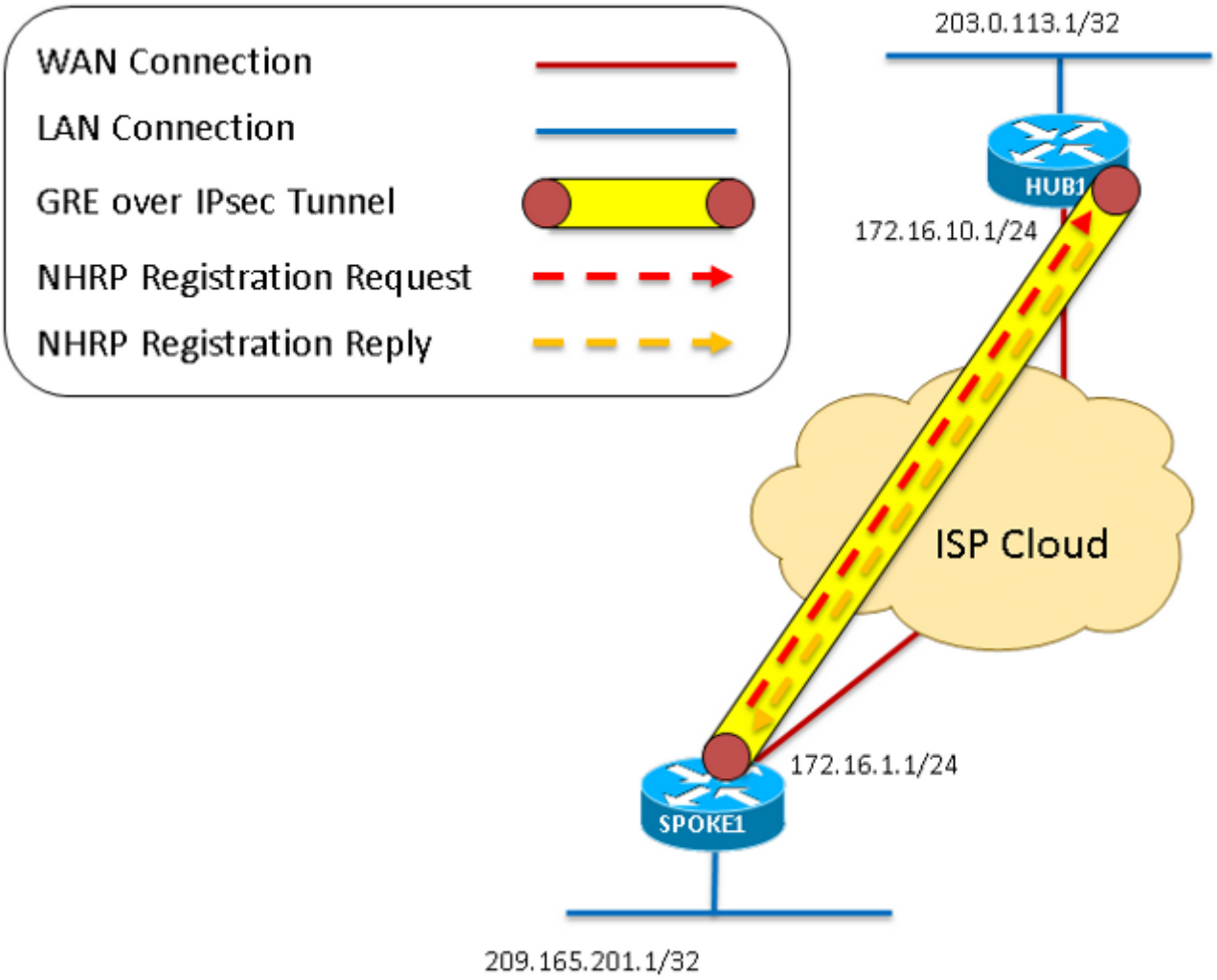
    Diagramme 4 - fait référence aux étapes 8 à 10



11. Maintenant que la session de chiffrement est active et capable de transmettre le trafic, ces paquets sont encapsulés dans le tunnel GRE sur IPSec.
    Diagramme 5 - fait référence à l'étape
    11



12. Comme nous l'avons vu dans les premières étapes, le satellite génère une requête d'enregistrement NHRP qui est envoyée via le tunnel GRE sur IPSec.
13. Le concentrateur reçoit les requêtes d'enregistrement NHRP et envoie une réponse d'enregistrement NHRP une fois qu'il confirme que le satellite a une adresse de tunnel et de NBMA valide. Le Spoke reçoit cette réponse d'enregistrement NHRP qui termine le processus d'enregistrement.
    Diagramme 6 - fait référence aux étapes 12 à 13



Ces débogages sont le résultat lorsque la commande **debug dmvpn all** est entrée sur les routeurs en étoile et en étoile. Cette commande particulière active cet ensemble de débogages :

```
Spoke1#debug dmvpn all all
DMVPN all level debugging is on
Spoke1#show debug


NHRP:
NHRP protocol debugging is on
NHRP activity debugging is on
NHRP extension processing debugging is on
NHRP cache operations debugging is on
NHRP routing debugging is on
NHRP rate limiting debugging is on
NHRP errors debugging is on
IKEV2:
IKEV2 error debugging is on
IKEV2 terse debugging is on
IKEV2 event debugging is on
IKEV2 packet debugging is on
IKEV2 detail debugging is on



Cryptographic Subsystem:
Crypto ISAKMP debugging is on
Crypto ISAKMP Error debugging is on
Crypto IPSEC debugging is on
```

```
Crypto IPSEC Error debugging is on
Crypto secure socket events debugging is on
Tunnel Protection Debugs:
Generic Tunnel Protection debugging is on
DMVPN:
DMVPN error debugging is on
DMVPN UP/DOWN event debugging is on
DMVPN detail debugging is on
DMVPN packet debugging is on
DMVPN all level debugging is on
```

Débogues avec explication

Comme il s'agit d'une configuration où IPSec est implémenté, les débogages affichent tous les débogages ISAKMP et IPSec. Si aucun chiffrement n'est configuré, ignorez les débogages qui commencent par « IPsec » ou « ISAKMP. »

EXPLICATION DU DÉBOGAGE DU CONCENTRATEUR	DÉBOGUES DANS LA SÉQUENCE	EXPLICATION D DÉBOGAGE PAR
Ces premiers messages de débogage sont générés par une commande **no shutdown** entrée sur l'interface de tunnel. Les messages sont générés par les services de chiffrement, GRE et NHRP en cours d'exécution. Une erreur d'enregistrement NHRP est détectée sur le concentrateur, car aucun serveur de tronçon suivant (NHS) n'est configuré (le concentrateur est le NHS pour notre cloud DMVPN). On s'y attend.	IPSEC-IFC MGRE/Tu0 : Vérification de l'état du tunnel. **NHRP : if_up : Tunnel0 proto 0** IPSEC-IFC MGRE/Tu0 : tunnel montant IPSEC-IFC MGRE/Tu0 : crypto_ss_hear_start déjà en cours d'écoute **%CRYPTO-6-ISAKMP_ON_OFF : ISAKMP est activé** **NHRP : Impossible d'envoyer l'enregistrement - aucun NHS configuré** %LINK-3-UPDOWN : Interface Tunnel0, état modifié en up NHRP : if_up : Tunnel0 proto 0 NHRP : Impossible d'envoyer l'enregistrement - aucun NHS configuré IPSEC-IFC MGRE/Tu0 : tunnel montant IPSEC-IFC MGRE/Tu0 : crypto_ss_hear_start déjà en cours d'écoute **%LINEPROTO-5-UPDOWN : Protocole de ligne sur l'interface Tunnel0, état modifié en up**	
	IPSEC-IFC GRE/Tu0 : Vérification de l'état du tunnel. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : recherche de connexion renvoyée 0 **IPSEC-IFC GRE/Tu0 : crypto_ss_hear_start déjà en cours d'écoute** **IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : Ouverture d'un socket avec le profil DMVPN-IPSEC** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : recherche de connexion renvoyée 0 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : Déclenchement immédiat du tunnel. IPSEC-IFC GRE/Tu0 : Ajout de l'interface de tunnel Tunnel0 à la liste partagée **NHRP : if_up : Tunnel0 proto 0** **NHRP : Tunnel0 : Cache add pour la cible 10.1.1.254/32 tronçon suivant 10.1.1.254**	Ces premiers messag débogage sont génér une commande **no shutdown** entrée sur l'interface de tunnel. L messages sont génér par les services de chiffrement, GRE et N qui sont initiés. En outre, le rayon ajo une entrée à son prop cache NHRP pour sa propre NBMA et son adresse de tunnel.

172.16.10.1
IPSEC-IFC GRE/Tu0 : tunnel montant
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : recherche de connexion renvoyée 961D220
IPSEC-IFC GRE/Tu0 : crypto_ss_hear_start déjà en cours d'écoute
IPSEC-IFC GRE/Tu0 : crypto_ss_hear_start déjà en cours d'écoute
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : Ouverture d'un socket avec le profil DMVPN-IPSEC
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : recherche de connexion renvoyée 961D220
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : Socket est déjà ouvert. Ignorer.
CRYPTO_SS(TUNNEL SEC) : L'application a commencé à écouter
échec de l'insertion de la carte dans l'AVL mapdb, la paire map + ace existe déjà sur la mapdb
%CRYPTO-6-ISAKMP_ON_OFF : ISAKMP est activé
CRYPTO_SS(TUNNEL SEC) : Informations de socket ouvertes actives : local 172.16.1.1 172.16.1.1/255.255.255.255/0, distant 172.16.10.1 172.16.10.1/255.255.255.255/0, port 47, ifc Tu0
DÉBUT DE LA NÉGOCIATION ISAKMP (PHASE I)
IPSEC(recalculate_mtu) : réinitialiser sadb_root 94EFDC0 mtu sur 1500
IPSEC(sa_request) : ,
(key eng. msg.) OUTBOUND local= 172.16.1.1:500, remote= 172.16.10.1:500,
local_proxy= 172.16.1.1/255.255.255.255/47/0 (type=1),
remote_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1),
protocol= ESP, Transformation= esp-3des esp-sha-hmac (transport),
lifedur= 3600 et 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
ISAKMP : (0) : Le profil de demande de SA est (NULL)
ISAKMP : Création d'une structure homologue pour 172.16.10.1, port homologue 500
ISAKMP : Nouvel homologue créé = 0x95F6858 peer_handle = 0x80000004
ISAKMP : struct homologue de verrouillage 0x95F6858, refcount 1 pour isakmp_initiator
ISAKMP : port local 500, port distant 500
ISAKMP : définir le nouveau noeud 0 sur QM_IDLE
ISAKMP:(0):insérer sa = 8A26FB0 avec succès
ISAKMP:(0) : Impossible de démarrer le mode agressif, en essayant le mode principal.
ISAKMP:(0):clé pré-partagée d'homologue trouvée correspondant à 172.16.10.1

La première étape un
que le tunnel est “ no
shutdown ” est de
commencer la négoci
de chiffrement. Ici, le
crée une demande de
tente de démarrer le
agressif et revient au
principal. Comme le
agressif n’est configu
aucun des routeurs, c
est attendu.
Le rayon commence
mode principal et env
premier message ISA
MM_NO_STATE. L'ét
ISAKMP passe de
IKE_READY à IKE_I_
Les messages d'ID de
fournisseur NAT-T so
utilisés pour la détecti
la traversée de NAT.
messages sont attend
lors de la négociation
d'ISAKMP, que NAT s
non implémenté. Com
les messages du mod
agressif, ils sont atten

	ISAKMP : (0) : ID fournisseur NAT-T construit-rfc3947 ISAKMP : (0) : ID fournisseur NAT-T construit-07 ISAKMP : (0) : ID fournisseur NAT-T construit-03 ISAKMP : (0) : ID fournisseur NAT-T construit-02 **ISAKMP : (0) : Entrée = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM** **ISAKMP:(0):Ancien état = IKE_READY Nouvel état = IKE_I_MM1** **ISAKMP : (0) : début de l'échange en mode principal** **ISAKMP : (0) : envoi du paquet à 172.16.10.1 my_port 500 peer_port 500 (I) MM_NO_STATE** ISAKMP:(0):envoi d'un paquet IPv4 IKE. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : recherche de connexion renvoyée 961D220 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : bon message prêt à l'emploi
Une fois que le tunnel du rayon est “ no shutdown, ” concentrateur reçoit le message IKE NEW SA (Main Mode 1) sur le port 500. En tant que répondeur, le concentrateur crée une association de sécurité ISAKMP (SA). L'état ISAKMP passe de IKE_READY à IKE_R_MM1.	**ISAKMP (0) : paquet reçu de 172.16.1.1 dport 500 sport 500 Global (N) NEW SA** **ISAKMP : Création d'une structure homologue pour 172.16.1.1, port homologue 500** ISAKMP : Nouvel homologue créé = 0x8CACD00 peer_handle = 0x80000003 ISAKMP : struct homologue de verrouillage 0x8CACD00, refcount 1 pour crypto_isakmp_process_block ISAKMP : port local 500, port distant 500 **ISAKMP : (0) : insérer sa = 6A5BDE8** ISAKMP : (0) : Entrée = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(0):Ancien état = IKE_READY Nouvel état = IKE_R_MM1**
Le message IKE Main Mode 1 reçu est traité. Le concentrateur détermine que l'homologue a des attributs ISAKMP correspondants et qu'ils sont remplis dans la SA ISAKMP qui vient d'être créée. Les messages montrent que l'homologue utilise 3DES-CBC pour le chiffrement, le hachage de SHA, Diffie Hellman (DH) groupe 1, la clé pré-partagée pour l'authentification et la durée de vie par défaut de SA de 86 400 secondes (0x0 0x1 0x51 0x80 = 0x15180 = 8640 secondes). L'état ISAKMP est toujours	ISAKMP : (0) : traitement de la charge utile SA. ID du message = 0 ISAKMP : (0) : traitement de la charge utile de l'id fournisseur **ISAKMP : (0) : L'ID du fournisseur semble Unity/DPD mais la différence majeure entre les 69** **ISAKMP (0) : L'ID de fournisseur est NAT-T RFC 3947** ISAKMP : (0) : traitement de la charge utile de l'id fournisseur ISAKMP : (0) : L'ID du fournisseur semble Unity/DPD mais incompatibilité majeure 245 ISAKMP (0) : L'ID de fournisseur est NAT-T v7 ISAKMP : (0) : traitement de la charge utile de l'id fournisseur ISAKMP : (0) : L'ID du fournisseur semble Unity/DPD mais incompatibilité majeure 157 ISAKMP : (0) : L'ID du fournisseur est NAT-T v3 ISAKMP : (0) : traitement de la charge utile de l'id fournisseur ISAKMP : (0) : L'ID du fournisseur semble Unity/DPD

IKE_R_MM1, car aucune réponse n'a été envoyée au rayon. Les messages d'ID de fournisseur NAT-T sont utilisés pour la détection et la traversée de NAT. Ces messages sont attendus lors de la négociation d'ISAKMP, que NAT soit ou non implémenté. Des messages similaires sont affichés pour la détection des homologues morts (DPD).	mais incompatibilité majeure 123 ISAKMP : (0) : L'ID de fournisseur est NAT-T v2 **ISAKMP:(0):clé pré-partagée d'homologue trouvée correspondant à 172.16.1.1** **ISAKMP : (0) : clé prépartagée locale trouvée** ISAKMP : Analyse des profils pour xauth... **ISAKMP:(0):vérification de la stratégie de priorité 1 de la transformation ISAKMP par rapport à la stratégie de priorité 1** **ISAKMP : cryptage 3DES-CBC** **ISAKMP : hachage SHA** **ISAKMP : groupe par défaut 1** **ISAKMP : auth pre-share** **ISAKMP : type de vie en secondes** **ISAKMP : durée de vie (VPI) de 0x0 0x1 0x51 0x80** **ISAKMP:(0) : les ATT sont acceptables. La charge utile suivante est 0** **ISAKMP:(0):actions acceptables:vie réelle : 0** **ISAKMP:(0):actions acceptables:vie : 0** **ISAKMP:(0):Remplissez les champs en sa vpi_length:4** **ISAKMP:(0):Remplissez les champs en sa life_in_seconds:86400** **ISAKMP:(0) : Renvoi de la durée de vie réelle : 86400** **ISAKMP:(0)::Début du minuteur de durée de vie : 86400.**
	ISAKMP : (0) : traitement de la charge utile de l'id fournisseur ISAKMP : (0) : L'ID du fournisseur semble Unity/DPD mais la différence majeure entre les 69 ISAKMP (0) : L'ID de fournisseur est NAT-T RFC 3947 ISAKMP : (0) : traitement de la charge utile de l'id fournisseur ISAKMP : (0) : L'ID du fournisseur semble Unity/DPD mais incompatibilité majeure 245 ISAKMP (0) : L'ID de fournisseur est NAT-T v7 ISAKMP : (0) : traitement de la charge utile de l'id fournisseur ISAKMP : (0) : L'ID du fournisseur semble Unity/DPD mais incompatibilité majeure 157 ISAKMP : (0) : L'ID du fournisseur est NAT-T v3 ISAKMP : (0) : traitement de la charge utile de l'id fournisseur ISAKMP : (0) : L'ID du fournisseur semble Unity/DPD mais incompatibilité majeure 123 ISAKMP : (0) : L'ID de fournisseur est NAT-T v2 ISAKMP : (0) : Entrée = IKE_MESG_INTERNE, IKE_PROCESS_MAIN_MODE ISAKMP:(0):Ancien état = IKE_R_MM1 Nouveau état = IKE_R_MM1
MM_SA_SETUP (Main	ISAKMP : (0) : ID fournisseur NAT-T construit-rfc3947

Mode 2) est envoyé au rayon, ce qui confirme que MM1 a été reçu et accepté en tant que paquet ISAKMP valide.
L'état ISAKMP passe de IKE_R_MM1 à IKE_R_MM2.

ISAKMP : (0) : envoi du paquet à 172.16.1.1 my_port 500 peer_port 500 (R) MM_SA_SETUP
ISAKMP:(0):envoi d'un paquet IPv4 IKE.
ISAKMP : (0) : Entrée = IKE_MESG_INTERNE, IKE_PROCESS_COMPLETE
ISAKMP:(0):Ancien état = IKE_R_MM1 Nouveau état = IKE_R_MM2

ISAKMP (0) : paquet reçu de 172.16.10.1 dport 500 sport 500 Global (I) MM_NO_STATE
ISAKMP : (0) : Entrée = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP : (0) : Ancien état = IKE_I_MM1 Nouvel état = IKE_I_MM2

ISAKMP : (0) : traitement de la charge utile SA. ID du message = 0
ISAKMP : (0) : traitement de la charge utile de l'id fournisseur
ISAKMP : (0) : L'ID du fournisseur semble Unity/DPD mais la différence majeure entre les 69
ISAKMP (0) : L'ID de fournisseur est NAT-T RFC 3947
ISAKMP:(0):clé pré-partagée d'homologue trouvée correspondant à 172.16.10.1
ISAKMP : (0) : clé prépartagée locale trouvée
ISAKMP : Analyse des profils pour xauth...
ISAKMP:(0):vérification de la stratégie de priorité 1 de la transformation ISAKMP par rapport à la stratégie de priorité 1
ISAKMP : cryptage 3DES-CBC
ISAKMP : hachage SHA
ISAKMP : groupe par défaut 1
ISAKMP : auth pre-share
ISAKMP : type de vie en secondes
ISAKMP : durée de vie (VPI) de 0x0 0x1 0x51 0x80
ISAKMP:(0) : les ATT sont acceptables. La charge utile suivante est 0
ISAKMP:(0):actions acceptables:vie réelle : 0
ISAKMP:(0):actions acceptables:vie : 0
ISAKMP:(0):Remplissez les champs en sa vpi_length:4
ISAKMP:(0):Remplissez les champs en sa life_in_seconds:86400
ISAKMP:(0) : Renvoi de la durée de vie réelle : 86400
ISAKMP:(0)::Début du minuteur de durée de vie : 86400.

ISAKMP : (0) : traitement de la charge utile de l'id fournisseur
ISAKMP : (0) : L'ID du fournisseur semble Unity/DPD mais la différence majeure entre les 69
ISAKMP (0) : L'ID de fournisseur est NAT-T RFC

En réponse au messa
MM1 envoyé au concentrateur, MM2 a et confirme que MM1 reçu. Le message IKE Mode 2 reçu est traité rayon se rend compte le concentrateur homologue a des attri ISAKMP correspond que ces attributs sont remplis dans la SA ISAKMP qui a été cré Ce paquet montre que l'homologue utilise 3D CBC pour le chiffreme hachage de SHA, Diff Hellman (DH) groupe clé pré-partagée pour l'authentification et la de vie par défaut de S 86 400 secondes (0x0 0x51 0x80 = 0x15180 8640 secondes).
En plus des message NAT-T, il y a un échan pour déterminer si la session va utiliser DP
L'état ISAKMP passe IKE_I_MM1 à IKE_I_M

	3947 ISAKMP : (0) : Entrée = IKE_MESG_INTERNE, IKE_PROCESS_MAIN_MODE ISAKMP : (0) : Ancien état = IKE_I_MM2 Nouvel état = IKE_I_MM2 **ISAKMP : (0) : envoi du paquet à 172.16.10.1 my_port 500 peer_port 500 (I) MM_SA_SETUP** ISAKMP:(0):envoi d'un paquet IPv4 IKE. ISAKMP : (0) : Entrée = IKE_MESG_INTERNE, IKE_PROCESS_COMPLETE **ISAKMP : (0) : Ancien état = IKE_I_MM2 Nouvel état = IKE_I_MM3**	MM_SA_SETUP (Mai Mode 3) est envoyé a concentrateur, ce qui confirme que le rayon reçu MM2 et souhaite continuer. L'état ISAKMP passe IKE_I_MM2 à IKE_I_M
MM_SA_SETUP (Main Mode 3) est reçu par le concentrateur. Le concentrateur conclut que l'homologue est un autre périphérique Cisco IOS et qu'aucune NAT n'est détectée pour nous ou notre homologue. L'état ISAKMP passe de IKE_R_MM2 à IKE_R_MM3.	**ISAKMP (0) : paquet reçu de 172.16.1.1 dport 500 sport 500 Global (R) MM_SA_SETUP** ISAKMP : (0) : Entrée = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(0):Ancien état = IKE_R_MM2 Nouvel état = IKE_R_MM3** ISAKMP : (0) : traitement de la charge utile KE. ID du message = 0 ISAKMP : (0) : traitement de la charge utile NONCE. ID du message = 0 **ISAKMP:(0):clé pré-partagée d'homologue trouvée correspondant à 172.16.1.1** ISAKMP : (1002) : traitement de la charge utile de l'id fournisseur ISAKMP : (1002) : ID fournisseur DPD ISAKMP : (1002) : traitement de la charge utile de l'id fournisseur **ISAKMP : (1002) : s'adressant à une autre boîte IOS.** ISAKMP : (1002) : traitement de la charge utile de l'id fournisseur ISAKMP : (1002) : L'ID du fournisseur semble Unity/DPD mais incompatibilité majeure 225 ISAKMP : (1002) : L'ID du fournisseur est XAUTH ISAKMP:type de données utiles reçues 20 **ISAKMP (1002) : Son hachage ne correspond pas - ce noeud en dehors de NAT** ISAKMP:type de données utiles reçues 20 **ISAKMP (1002) : Aucune NAT trouvée pour soi-même ou pour homologue** ISAKMP : (1002) : Entrée = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP : (1002) : Ancien état = IKE_R_MM3 Nouvel état = IKE_R_MM3	
MM_KEY_EXCH (Main Mode 4) est envoyé par le concentrateur. L'état ISAKMP passe de IKE_R_MM3 à IKE_R_MM4.	**ISAKMP : (1002) : envoi du paquet à 172.16.1.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH** ISAKMP:(1002):envoi d'un paquet IPv4 IKE. ISAKMP : (1002) : Entrée = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP : (1002) : Ancien état = IKE_R_MM3 Nouvel**	

	état = IKE_R_MM4	
	ISAKMP (0) : paquet reçu de 172.16.10.1 dport 500 sport 500 Global (I) MM_SA_SETUP	MM_SA_SETUP (Mai
	ISAKMP : (0) : Entrée = IKE_MESG_FROM_PEER, IKE_MM_EXCH	Mode 4) est reçu en é L'intervenant conclut q
	ISAKMP : (0) : Ancien état = IKE_I_MM3 Nouvel état = IKE_I_MM4	l'homologue est un au périphérique Cisco IO qu'aucune NAT n'est
	ISAKMP : (0) : traitement de la charge utile KE. ID du message = 0	détectée pour nous ou notre homologue. L'état ISAKMP passe
	ISAKMP : (0) : traitement de la charge utile NONCE. ID du message = 0	IKE_I_MM3 à IKE_I_M
	ISAKMP:(0):clé pré-partagée d'homologue trouvée correspondant à 172.16.10.1	
	ISAKMP : (1002) : traitement de la charge utile de l'id fournisseur	
	ISAKMP : (1002) : L'ID fournisseur est Unity	
	ISAKMP : (1002) : traitement de la charge utile de l'id fournisseur	
	ISAKMP : (1002) : ID fournisseur DPD	
	ISAKMP : (1002) : traitement de la charge utile de l'id fournisseur	
	ISAKMP : (1002) : s'adressant à une autre boîte IOS.	
	ISAKMP:type de données utiles reçues 20	
	ISAKMP (1002) : Son hachage ne correspond pas - ce noeud en dehors de NAT	
	ISAKMP:type de données utiles reçues 20	
	ISAKMP (1002) : Aucune NAT trouvée pour soi-même ou pour homologue	
	ISAKMP : (1002) : Entrée = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE	
	ISAKMP : (1002) : Ancien état = IKE_I_MM4 Nouvel état = IKE_I_MM4	
	ISAKMP : (1002) : Envoyer le contact initial	MM_KEY_EXCH (Mai
	ISAKMP:(1002):SA effectue une authentification de clé pré-partagée à l'aide du type ID_IPV4_ADDR.	Mode 5) est envoyé p rayon.
	ISAKMP (1002) : Charge utile ID charge utile suivante : 8 type : 1 adresse : 172.16.1.1 protocole : 17 port : 500 longueur: 12	L'état ISAKMP passe IKE_I_MM4 à IKE_I_M
	ISAKMP : (1002) : longueur totale de la charge utile : 12	
	ISAKMP : (1002) : envoi du paquet à 172.16.10.1 my_port 500 peer_port 500 (I) MM_KEY_EXCH	
	ISAKMP:(1002):envoi d'un paquet IPv4 IKE.	
	ISAKMP : (1002) : Entrée = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE	
	ISAKMP : (1002) : Ancien état = IKE_I_MM4 Nouvel état = IKE_I_MM5	
MM_KEY_EXCH (Main	**ISAKMP (1002) : paquet reçu de 172.16.1.1 dport 500**	

Mode 5) est reçu par le concentrateur.
L'état ISAKMP passe de IKE_R_MM4 à IKE_R_MM5.
En outre, l'homologue “ correspond *aucun* des profils ” est vu en raison de l'absence d'un profil ISAKMP. Comme c'est le cas, ISAKMP n'utilise pas de profil.

sport 500 Global (R) MM_KEY_EXCH
ISAKMP : (1002) : Entrée = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP : (1002) : Ancien état = IKE_R_MM4 Nouvel état = IKE_R_MM5

ISAKMP : (1002) : charge utile de l'ID de traitement.
ID du message = 0
ISAKMP (1002) : Charge utile ID
charge utile suivante : 8
type : 1
adresse : 172.16.1.1
protocole : 17
port : 500
longueur: 12
ISAKMP : (0) : homologue correspond à *aucun* des profils
ISAKMP : (1002) : traitement de la charge utile HASH.
ID du message = 0
ISAKMP : (1002) : traitement NOTIFY INITIAL_CONTACT, protocole 1
spi 0, ID du message = 0, sa = 0x6A5BDE8
ISAKMP:(1002):état de l'authentification SA :
authentifié
ISAKMP:(1002):SA a été authentifiée avec 172.16.1.1
ISAKMP:(1002):état de l'authentification SA :
authentifié
ISAKMP : (1002) : Traiter le contact initial, supprimer les SA de phase 1 et 2 existantes avec le port distant local 172.16.10.1 172.16.1.1 172.16.1.1 500
ISAKMP : Tentative d'insertion d'un homologue 172.16.10.1/172.16.1.1/500/, et insertion réussie de 8CACD00.
ISAKMP : (1002) : Entrée = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP : (1002) : Ancien état = IKE_R_MM5 Nouvel état = IKE_R_MM5

IPSEC(key_engine) : a reçu un événement de file d'attente avec 1 message(s) KMI
ISAKMP:(1002):SA effectue une authentification de clé pré-partagée à l'aide du type ID_IPV4_ADDR.
ISAKMP (1002) : Charge utile ID
charge utile suivante : 8
type : 1
adresse : 172.16.10.1
protocole : 17
port : 500
longueur: 12
ISAKMP : (1002) : longueur totale de la charge utile : 12
Le paquet MM_KEY_EXCH **ISAKMP : (1002) : envoi du paquet à 172.16.1.1**

final (Main Mode 6) est envoyé par le concentrateur. Ceci termine la négociation de phase 1, ce qui signifie que ce périphérique est prêt pour la phase 2 (mode rapide IPSec). L'état ISAKMP passe de IKE_R_MM5 à IKE_P1_COMPLETE.	**my_port 500 peer_port 500 (R) MM_KEY_EXCH** ISAKMP:(1002):envoi d'un paquet IPv4 IKE. ISAKMP : (1002) : Entrée = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP : (1002) : Ancien état = IKE_R_MM5 Nouvel état = IKE_P1_COMPLETE** ISAKMP : (1002) : Entrée = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE ISAKMP : (1002) : Ancien état = IKE_P1_COMPLETE Nouvel état = IKE_P1_COMPLETE	
	ISAKMP (1002) : paquet reçu de 172.16.10.1 dport 500 sport 500 Global (I) MM_KEY_EXCH ISAKMP : (1002) : charge utile de l'ID de traitement. ID du message = 0 ISAKMP (1002) : Charge utile ID charge utile suivante : 8 type : 1 adresse : 172.16.10.1 protocole : 17 port : 500 longueur: 12 **ISAKMP : (0) : homologue correspond à *aucun* des profils** ISAKMP : (1002) : traitement de la charge utile HASH. ID du message = 0 ISAKMP:(1002):état de l'authentification SA : authentifié ISAKMP:(1002):SA a été authentifiée avec 172.16.10.1 **ISAKMP : Tentative d'insertion d'un homologue 172.16.1.1/172.16.10.1/500/, et insertion réussie de 95F6858.** ISAKMP : (1002) : Entrée = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP : (1002) : Ancien état = IKE_I_MM5 Nouvel état = IKE_I_MM6** ISAKMP : (1002) : Entrée = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP : (1002) : Ancien état = IKE_I_MM6 Nouvel état = IKE_I_MM6 ISAKMP : (1002) : Entrée = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP : (1002) : Ancien état = IKE_I_MM6 Nouvel état = IKE_P1_COMPLETE**	Le paquet MM_KEY_E final (Main Mode 6) es reçu par le rayon. Ceci termine la négociation phase 1, ce qui signifi ce périphérique est pr pour la phase 2 (mode rapide IPSec). L'état ISAKMP passe IKE_I_MM5 à IKE_I_M puis immédiatement à IKE_P1_COMPLETE. En outre, l'homologue correspond *aucun* d profils " est vu en rais l'absence d'un profil ISAKMP. Comme c'es cas, ISAKMP n'utilise de profil.
FIN DES NÉGOCIATIONS ISAKMP (PHASE I), DÉBUT DES NÉGOCIATIONS IPSEC (PHASE II)		
	ISAKMP:(1002):début de l'échange en mode rapide, M-ID de 3464373979 ISAKMP:(1002):L'initiateur QM obtient spi **ISAKMP : (1002) : envoi du paquet à 172.16.10.1 my_port 500 peer_port 500 (I) QM_IDLE**	L'échange Quick Mod (Phase II, IPSec) dém et le rayon envoie le premier message QM concentrateur.

	ISAKMP:(1002):envoi d'un paquet IPv4 IKE. ISAKMP : (1002) : Noeud 3464373979, Entrée = IKE_MESG_INTERNAL, IKE_INIT_QM **ISAKMP : (1002) : Ancien état = IKE_QM_READY Nouvel état = IKE_QM_I_QM1** ISAKMP : (1002) : Entrée = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE ISAKMP : (1002) : Ancien état = IKE_P1_COMPLETE Nouvel état = IKE_P1_COMPLETE
Le concentrateur reçoit le premier paquet Quick Mode (QM) qui a la proposition IPSec. Les attributs reçus indiquent que : indicateur d'encapsulation défini sur 2 (mode transport, indicateur de 1 serait le mode tunnel), durée de vie par défaut de SA de 3 600 secondes et 4 60 8 000 kilo-octets (0x46 5 000 hexadécimal), HMAC-SHA pour l'authentification et 3DES pour le chiffrement. Comme il s'agit des mêmes attributs définis dans la configuration locale, la proposition est acceptée et le shell d'une SA IPSec est créé. Étant donné qu'aucune valeur SPI (Security Parameter Index) n'est encore associée à ces valeurs, il s'agit simplement d'un shell d'une SA qui ne peut pas encore être utilisée pour transmettre le trafic.	**ISAKMP (1002) : paquet reçu de 172.16.1.1 dport 500 sport 500 Global (R) QM_IDLE** **ISAKMP : définir le nouveau noeud -830593317 sur QM_IDLE** ISAKMP : (1002) : traitement de la charge utile HASH. ID de message = 3464373979 ISAKMP : (1002) : traitement de la charge utile SA. ID de message = 3464373979 **ISAKMP : (1002):vérification de la proposition 1 IPSec** **ISAKMP : transformation 1, ESP_3DES** **ISAKMP : attributs dans la transformation :** **ISAKMP : les majuscules sont 2 (transport)** **ISAKMP : type de vie SA en secondes** **ISAKMP : durée de vie de SA (de base) de 3600** **ISAKMP : type de vie SA en kilo-octets** **ISAKMP : durée de vie de SA (VPI) de 0x0 0x46 0x50 0x0** **ISAKMP : l'authentificateur est HMAC-SHA** **ISAKMP:(1002) : les tâches sont acceptables.** IPSEC(validation_proposition_request) : partie 1 de la proposition IPSEC(validation_proposition_request) : partie 1 de la proposition, **(key eng. msg.) INBOUND local= 172.16.10.1:0, remote= 172.16.1.1:0,** **local_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1),** **remote_proxy= 172.16.1.1/255.255.255.255/47/0 (type=1),** **protocol= ESP, transformée= AUCUN (transport),** **lifedur= 0 et 0kb,** **spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0**
Il s'agit uniquement de messages de service IPSec généraux qui indiquent qu'il fonctionne correctement.	IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : recherche de connexion renvoyée 0 IPSEC-IFC MGRE/Tu0 : crypto_ss_hear_start déjà en cours d'écoute **IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : Ouverture d'un socket avec le profil DMVPN-IPSEC** IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : recherche de connexion renvoyée 0 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : Déclenchement immédiat du tunnel. IPSEC-IFC MGRE/Tu0 : Ajout de l'interface de tunnel Tunnel0 à la liste partagée

	IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : tunnel_protection_start_wait_timer 8C93888 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : Bonne demande d'écoute
L'entrée Pseudo-crypto map est créée pour le protocole IP 47 (GRE) de 172.16.10.1 (adresse publique du concentrateur) à 172.16.1.1 (adresse publique du rayon). Une SA/SPI IPSec est créée pour le trafic entrant et sortant avec des valeurs de la proposition acceptée.	échec de l'insertion de la carte dans l'AVL mapdb, la paire map + ace existe déjà sur la mapdb CRYPTO_SS(TUNNEL SEC) : Informations de socket ouvertes passives : local 172.16.10.1 172.16.10.1/255.255.255.255/0, distant 172.16.1.1 172.16.1.1/255.255.255.255/0, port 47, ifc Tu0 Crypto mapdb : correspondance_proxy **adresse src : 172.16.10.1** **dst addr : 172.16.1.1** **protocole : 47** port src : 0 port dst : 0 ISAKMP : (1002) : traitement de la charge utile NONCE. ID de message = 3464373979 ISAKMP : (1002) : charge utile de l'ID de traitement. ID de message = 3464373979 ISAKMP : (1002) : charge utile de l'ID de traitement. ID de message = 3464373979 ISAKMP:(1002):QM Responder reçoit un spi ISAKMP : (1002) : Noeud 3464373979, Entrée = IKE_MESG_FROM_PEER, IKE_QM_EXCH **ISAKMP : (1002) : Ancien état = IKE_QM_READY Nouvel état = IKE_QM_SPI_STARVE** **ISAKMP : (1002) : Création de SA IPSec** **SA entrante de 172.16.1.1 à 172.16.10.1 (f/i) 0/ 0 (proxy 172.16.1.1 à 172.16.10.1)** **a spi 0xDD2AC2B3 et conn_id 0** **durée de vie de 3 600 secondes** **durée de vie de 4608000 kilo-octets** **SA sortante de 172.16.10.1 à 172.16.1.1 (f/i) 0/0 (proxy 172.16.10.1 à 172.16.1.1)** **a spi 0x82C3E0C4 et conn_id 0** **durée de vie de 3 600 secondes** **durée de vie de 4608000 kilo-octets**
Deuxième message QM envoyé par le concentrateur. Message généré par le service IPSec qui confirme que la protection du tunnel est activée sur Tunnel0.	**ISAKMP : (1002) : envoi du paquet à 172.16.1.1 my_port 500 peer_port 500 (R) QM_IDLE** ISAKMP:(1002):envoi d'un paquet IPv4 IKE. ISAKMP : (1002) : Noeud 3464373979, Entrée = IKE_MESG_INTERNAL, IKE_GOT_SPI **ISAKMP : (1002) : Ancien état = IKE_QM_SPI_STARVE Nouvel état = IKE_QM_R_QM2** CRYPTO_SS(TUNNEL SEC) : Liaison de l'application au socket terminée IPSEC(key_engine) : a reçu un événement de file d'attente avec 1 message(s) KMI Crypto mapdb : correspondance_proxy adresse src : 172.16.10.1 dst addr : 172.16.1.1
Un autre message de création de SA s'affiche. Il reste les adresses IP de destination, les SPI, les attributs de jeu de transformation et la durée de vie en kilo-octets et secondes.	

protocole : 47
port src : 0
port dst : 0
IPSEC(crypto_ipsec_sa_find_ident_head) :
reconnexion avec les mêmes proxies et homologue
172.16.1.1
IPSEC(policy_db_add_ident) : src 172.16.10.1, dest
172.16.1.1, dest_port 0

IPSEC(create_sa) : sa création,
sa_dest= 172.16.10.1, sa_proto= 50,
sa_spi= 0xDD2AC2B3(3710567091),
sa_trans= esp-3des esp-sha-hmac, sa_conn_id= 3
sa_lifetime(k/s)= (4536779/3600)
IPSEC(create_sa) : sa création,
sa_dest= 172.16.1.1, sa_proto= 50,
sa_spi= 0x82C3E0C4(2193875140),
sa_trans= esp-3des esp-sha-hmac, sa_conn_id= 4
sa_lifetime(k/s)= (4536779/3600)
IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce)
: mise à jour de Tunnel0 ident 8B6A0E8 avec
tun_decap_oce 6A648F0
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) :
recherche de connexion renvoyée par 8C93888
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : bon
message prêt à l'emploi
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) :
recherche de connexion renvoyée par 8C93888
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) :
tunnel_protection_socket_up
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) :
Signalisation NHRP
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) :
Message MTU obtenu mtu 1458
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) :
recherche de connexion renvoyée par 8C93888

ISAKMP (1002) : paquet reçu de 172.16.10.1 dport 500 sport 500 Global (I) QM_IDLE	Le rayon reçoit le deu paquet QM qui a la
ISAKMP : (1002) : traitement de la charge utile HASH. ID de message = 3464373979	proposition IPSec. Ce confirme que QM1 a é
ISAKMP : (1002) : traitement de la charge utile SA. ID de message = 3464373979	reçu par le concentrat Les attributs reçus
ISAKMP : (1002):vérification de la proposition 1 IPSec	indiquent que : indicat
ISAKMP : transformation 1, ESP_3DES	d'encapsulation défini
ISAKMP : attributs dans la transformation :	(mode transport, indic
ISAKMP : les majuscules sont 2 (transport)	de 1 serait le mode tu
ISAKMP : type de vie SA en secondes	durée de vie par défa
ISAKMP : durée de vie de SA (de base) de 3600	SA de 3 600 seconde
ISAKMP : type de vie SA en kilo-octets	60 8 000 kilo-octets (0
ISAKMP : durée de vie de SA (VPI) de 0x0 0x46 0x50 0x0	000 hexadécimal), HM SHA pour l'authentific
ISAKMP : l'authentificateur est HMAC-SHA	et DES pour le chiffre
ISAKMP:(1002) : les tâches sont acceptables.	Comme il s'agit des m

IPSEC(validation_proposition_request) : partie 1 de la proposition IPSEC(validation_proposition_request) : partie 1 de la proposition, **(key eng. msg.) INBOUND local= 172.16.1.1:0, remote= 172.16.10.1:0,** **local_proxy= 172.16.1.1/255.255.255.255/47/0 (type=1),** **remote_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1),** **protocol= ESP, transformée= AUCUN (transport),** **lifedur= 0 et 0kb,** **spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0**	attributs définis dans l configuration locale, la proposition est accept le shell d'une SA IPSe créé. Étant donné qu'aucune valeur SPI (Security Parameter In n'est encore associée valeurs, il s'agit simple d'un shell d'une SA qu peut pas encore être utilisée pour transmet trafic.
Crypto mapdb : correspondance_proxy **adresse src : 172.16.1.1** **dst addr : 172.16.10.1** **protocole : 47** **port src : 0** **port dst : 0**	L'entrée de carte pseu crypto est créée pour protocole IP 47 (GRE) 172.16.10.1 (adresse publique du concentra à 172.16.1.1 (adresse publique du rayon).
ISAKMP : (1002) : traitement de la charge utile NONCE. ID de message = 3464373979 ISAKMP : (1002) : charge utile de l'ID de traitement. ID de message = 3464373979 ISAKMP : (1002) : charge utile de l'ID de traitement. ID de message = 3464373979 **ISAKMP : (1002) : Création de SA IPSec** **SA entrante de 172.16.10.1 à 172.16.1.1 (f/i) 0/ 0** **(proxy 172.16.10.1 à 172.16.1.1)** **a spi 0x82C3E0C4 et conn_id 0** **durée de vie de 3 600 secondes** **durée de vie de 4608000 kilo-octets** **SA sortante de 172.16.1.1 à 172.16.10.1 (f/i) 0/0** **(proxy 172.16.1.1 à 172.16.10.1)** **a spi 0xDD2AC2B3 et conn_id 0** **durée de vie de 3 600 secondes** **durée de vie de 4608000 kilo-octets**	Une SA/SPI IPSec es créée pour le trafic en et sortant avec des va de la proposition acce
ISAKMP : (1002) : envoi du paquet à 172.16.10.1 my_port 500 peer_port 500 (I) QM_IDLE ISAKMP:(1002):envoi d'un paquet IPv4 IKE. ISAKMP:(1002):suppression du noeud -830593317 erreur FALSE Raison « Aucune erreur » ISAKMP : (1002) : Noeud 3464373979, Entrée = IKE_MESG_FROM_PEER, IKE_QM_EXCH **ISAKMP : (1002) : Ancien état = IKE_QM_I_QM1 Nouvel état = IKE_QM_PHASE2_COMPLETE** IPSEC(key_engine) : a reçu un événement de file d'attente avec 1 message(s) KMI Crypto mapdb : correspondance_proxy adresse src : 172.16.1.1 dst addr : 172.16.10.1 protocole : 47 port src : 0	Le rayon envoie le troisième et dernier message QM au concentrateur, qui ter l'échange QM. Contrairement à ISAK où chaque homologue passe par chaque éta (MM1 à MM6/P1_COMPLETE IPSec est un peu diffé car il n'y a que trois messages au lieu de s L'initiateur (notre intervention dans ce c comme indiqué par le

	port dst : 0 IPSEC(crypto_ipsec_sa_find_ident_head) : reconnexion avec les mêmes proxies et homologue 172.16.10.1 IPSEC(policy_db_add_ident) : src 172.16.1.1, dest 172.16.10.1, dest_port 0 **IPSEC(create_sa) : sa création,** sa_dest= 172.16.1.1, sa_proto= 50, sa_spi= 0x82C3E0C4(2193875140), sa_trans= esp-3des esp-sha-hmac, sa_conn_id= 3 sa_lifetime(k/s)= (4499172/3600) **IPSEC(create_sa) : sa création,** sa_dest= 172.16.10.1, sa_proto= 50, sa_spi= 0xDD2AC2B3(3710567091), sa_trans= esp-3des esp-sha-hmac, sa_conn_id= 4 sa_lifetime(k/s)= (4499172/3600) **IPSEC(update_current_outbound_sa) : get enable SA peer 172.16.10.1 current outbound sa to SPI DD2AC2B3** **IPSEC(update_current_outbound_sa) : homologue mis à jour 172.16.10.1 sortant actuel en tant que SPI DD2AC2B3** IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce) : mise à jour de Tunnel0 ident 94F2740 avec tun_decap_oce 794ED30 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : recherche de connexion renvoyée 961D220 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : tunnel_protection_socket_up IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : Signalisation NHRP NHRP : NHS 10.1.1.254 Tunnel0 vrf 0 Cluster 0 Priorité 0 Transmise à 'E' à partir de ' ' IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : recherche de connexion renvoyée 961D220 NHRP : Tentative d'envoi de paquet via DEST 10.1.1.254	dans le message IKE_QM_I_QM1) va d QM_READY, puis à QM_I_QM1 directeme QM_PHASE2_COMP Le répondeur (concentrateur) passe QM_READY, QM_SPI_STARVE, QM_R_QM2, QM_PHASE2_COMP Un autre message de création de SA s'affich reste les adresses IP destination, les SPI, le attributs de jeu de transformation et la du de vie en kilo-octets e secondes.
Ces derniers messages QM confirment que le mode rapide est terminé et qu'IPSec est activé des deux côtés du tunnel. Contrairement à ISAKMP où chaque homologue passe par chaque état (MM1 à MM6/P1_COMPLETE), IPSec est un peu différent car il n'y a que trois messages au lieu de six. Le répondeur (notre	**ISAKMP (1002) : paquet reçu de 172.16.1.1 dport 500 sport 500 Global (R) QM_IDLE** ISAKMP:(1002):suppression du noeud -830593317 erreur FALSE Raison « QM terminé (attente)" ISAKMP : (1002) : Noeud 3464373979, Entrée = IKE_MESG_FROM_PEER, IKE_QM_EXCH **ISAKMP : (1002) : Ancien état = IKE_QM_R_QM2 Nouvel état = IKE_QM_PHASE2_COMPLETE** IPSEC(key_engine) : a reçu un événement de file d'attente avec 1 message(s) KMI IPSEC(key_engine_enable_outbound) : recenable notification d'ISAKMP **IPSEC(key_engine_enable_outbound) : activer SA avec spi 2193875140/50**	

concentrateur dans ce cas, comme indiqué par le “ R ” dans le message IKE_QM_R_QM1) va à QM_READY, QM_SPI_STARVE, QM_R_QM2, QM_PHASE2_COMPLETE. L'initiateur (en étoile) passe de QM_READY, puis à QM_I_QM1 directement à QM_PHASE2_COMPLETE.	**IPSEC(update_current_outbound_sa) : get enable SA peer 172.16.1.1 current outbound sa to SPI 82C3E0C4** **IPSEC(update_current_outbound_sa) : homologue mis à jour 172.16.1.1 actuel sortant vers SPI 82C3E0C4**	
	NHRP : Envoyer une demande d'enregistrement via Tunnel0 vrf 0, taille de paquet : 108 **src : 10.1.1.1, dst : 10.1.1.254** F) afn : IPv4(1), type : IP(800), saut : 255, version : 1 shtl : 4(NSAP), sstl : 0 (NSAP) pktsz : 108 Extoff : 52 (M) drapeaux : « nat unique », requis : 65540 **src NBMA : 172.16.1.1** **protocole src : 10.1.1.1, protocole dst : 10.1.1.254** (C-1) code : aucune erreur(0) préfixe : 32, mtu : 17912, hd_time : 7200 addr_len : 0(NSAP), sous-addr_len : 0(NSAP), proto_len : 0, préf : 0 Extension d'adresse du répondeur(3) : Extension du dossier NHS du transport en transit(4) : Extension de l'enregistrement NHS du transport inversé(5) : **Extension d'authentification(7) :** **type : texte clair(1), données&deux-points ; NHRPAUTH** Extension d'adresse NAT(9) : (C-1) code : aucune erreur(0) préfixe : 32, mtu : 17912, hd_time : 0 addr_len : 4(NSAP), subaddr_len : 0(NSAP), proto_len : 4, préf : 0 **NBMA client : 172.16.10.1** **protocole client : 10.1.1.254**	Il s'agit des demandes d'enregistrement NHR envoyées au concentr pour tenter de s'enreg au NHS (le concentra Il est normal de voir d multiples de ceux-ci, c porte-parole continue tenter de s'enregistrer auprès du NHS jusqu' qu'il reçoive une répo d'enregistrement “. ” **src, dst** : Adresses IP source (en étoile) et d destination (concentra du tunnel. Il s’agit de l source et de la destina du paquet GRE envoy le routeur **Src NBMA** : adresse N (Internet) du rayon qu envoyé ce paquet et c tente de s'enregistrer auprès du NHS **protocole src** : adress tunnel du satellite qui de s'enregistrer **protocole dst** : adress tunnel du NHS/concentrateur **Extension d'authentification**, données&deux-points chaîne d'authentificati NHRP **NBMA client** : Adresse NBMA du NHS/concentrateur **protocole client** : adre du tunnel du NHS/concentrateur

	NHRP-RATE : Envoi de la demande d'enregistrement initiale pour 10.1.1.254, requise 65540 **%LINK-3-UPDOWN : Interface Tunnel0, état modifié en up** NHRP : if_up : Tunnel0 proto 0 **NHRP : Tunnel0 : Mise à jour du cache de la cible 10.1.1.254/32 tronçon suivant 10.1.1.254 172.16.10.1** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : recherche de connexion renvoyée 961D220 NHRP : Tentative d'envoi de paquet via DEST 10.1.1.254	Plus de messages de service NHRP indiqua que la demande d'enregistrement initia été envoyée au NHS à l'adresse 10.1.1.254. également une confirmation qu'une e de cache a été ajouté pour le tunnel IP 10.1.1.254/24 qui vit à NBMA 172.16.10.1. L message retardé dit q tunnel a été “ pas ferm est vu ici.
	IPSEC-IFC GRE/Tu0 : tunnel montant IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : recherche de connexion renvoyée 961D220 IPSEC-IFC GRE/Tu0 : crypto_ss_hear_start déjà en cours d'écoute IPSEC-IFC GRE/Tu0 : crypto_ss_hear_start déjà en cours d'écoute **IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : Ouverture d'un socket avec le profil DMVPN-IPSEC** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : recherche de connexion renvoyée 961D220 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : Socket est déjà ouvert. Ignorer. %LINEPROTO-5-UPDOWN : Protocole de ligne sur l’interface Tunnel0, état modifié en up	Il s'agit de messages service IPSec généra indiquent qu'il fonctio correctement. C'est ic l'on voit enfin que le protocole de tunnel es actif.
Il s'agit des demandes d'enregistrement NHRP reçues du satellite pour tenter de s'enregistrer auprès du NHS (le concentrateur). Il est normal de voir des multiples de ceux-ci, car le porte-parole continue de tenter de s'enregistrer auprès du NHS jusqu'à ce qu'il reçoive une réponse d'enregistrement “. ” **Src NBMA** : adresse NBMA (Internet) du rayon qui a envoyé ce paquet et qui tente de s'enregistrer auprès du NHS **protocole src** : adresse du tunnel du satellite qui tente de s'enregistrer **protocole dst** : adresse du tunnel du	**NHRP : Réception de la demande d'enregistrement via Tunnel0 vrf 0, taille de paquet : 108** F) afn : IPv4(1), type : IP(800), saut : 255, version : 1 shtl : 4(NSAP), sstl : 0 (NSAP) pktsz : 108 Extoff : 52 (M) drapeaux : « nat unique », requis : 65540 **src NBMA : 172.16.1.1** **protocole src : 10.1.1.1, protocole dst : 10.1.1.254** (C-1) code : aucune erreur(0) préfixe : 32, mtu : 17912, hd_time : 7200 addr_len : 0(NSAP), sous-addr_len : 0(NSAP), proto_len : 0, préf : 0 Extension d'adresse du répondeur(3) : Extension du dossier NHS du transport en transit(4) : Extension de l'enregistrement NHS du transport inversé(5) : **Extension d'authentification(7) :** **type : texte clair(1), données&deux-points ; NHRPAUTH** Extension d'adresse NAT(9) : (C-1) code : aucune erreur(0) préfixe : 32, mtu : 17912, hd_time : 0 addr_len : 4(NSAP), subaddr_len : 0(NSAP),	

NHS/concentrateur **Extension d'authentification**, données&deux-points ; chaîne d'authentification NHRP **NBMA client** : Adresse NBMA du NHS/concentrateur **protocole client** : adresse du tunnel du NHS/concentrateur	proto_len : 4, préf : 0 **NBMA client : 172.16.10.1** **protocole client : 10.1.1.254**
Paquets de débogage NHRP ajoutant le réseau cible 10.1.1.1/32 disponible via le tronçon suivant 10.1.1.1 au niveau du protocole NHRP 172.16.1.1. 172.16.1.1 est également ajouté à la liste des adresses auxquelles le concentrateur transfère le trafic de multidiffusion. Ces messages confirment que l'enregistrement a réussi, ainsi qu'une résolution pour l'adresse du tunnel des rayons.	NHRP : netid_in = 1, to_us = 1 **NHRP : Tunnel0 : Ajout de cache pour la cible 10.1.1.1/32 tronçon suivant 10.1.1.1 172.16.1.1** **NHRP : Ajout de terminaux de tunnel (VPN : 10.1.1.1, NBMA : 172.16.1.1)** **NHRP : Sous-bloc NHRP correctement connecté pour les terminaux de tunnel (VPN : 10.1.1.1, NBMA : 172.16.1.1)** NHRP : Noeud de sous-bloc inséré pour le cache : Noeud de sous-bloc inséré cible pour le cache : Cible 10.1.1.1/32nhop 10.1.1.1 NHRP : Entrée de cache dynamique interne convertie pour l'interface 10.1.1.1/32 Tunnel0 vers externe **NHRP : Tu0 : Création de NBMA de mappage de multidiffusion dynamique : 172.16.1.1** **NHRP : Mappage de multidiffusion dynamique ajouté pour NBMA : 172.16.1.1** NHRP : Mise à jour de notre cache avec NBMA : 172.16.10.1, NBMA_ALT : 172.16.10.1 NHRP : Nouvelle longueur obligatoire : 32 NHRP : Tentative d'envoi de paquet via DEST 10.1.1.1 **NHRP : NHRP a correctement résolu 10.1.1.1 en NBMA 172.16.1.1** **NHRP : L'encapsulation a réussi. Adresse IP du tunnel 172.16.1.1**
Il s'agit de la réponse d'enregistrement NHRP envoyée par le concentrateur au rayon en réponse à la ” de demande d'enregistrement NHRP “ reçue plus tôt. Comme les autres paquets d'enregistrement, le concentrateur envoie des multiples de ceux-ci en réponse aux demandes multiples. **src, dst** : Adresses IP	**NHRP : Envoyer une réponse d'enregistrement via Tunnel0 vrf 0, taille de paquet : 128** **src : 10.1.1.254, dst : 10.1.1.1** F) afn : IPv4(1), type : IP(800), saut : 255, version : 1 shtl : 4(NSAP), sstl : 0 (NSAP) pktsz : 128 Extoff : 52 (M) drapeaux : « nat unique », requis : 65540 **src NBMA : 172.16.1.1** **protocole src : 10.1.1.1, protocole dst : 10.1.1.254** (C-1) code : aucune erreur(0) préfixe : 32, mtu : 17912, hd_time : 7200 addr_len : 0(NSAP), sous-addr_len : 0(NSAP), proto_len : 0, préf : 0 Extension d'adresse du répondeur(3) :

source (concentrateur) et de destination (rayon) du tunnel. Il s'agit de la source et de la destination du paquet GRE envoyé par le routeur

Src NBMA : Adresse NBMA (Internet) du rayon

protocole src : adresse du tunnel du satellite qui tente de s'enregistrer

protocole dst : adresse du tunnel du NHS/concentrateur

NBMA client : Adresse NBMA du NHS/concentrateur

protocole client : adresse du tunnel du NHS/concentrateur

Extension d'authentification, données&deux-points ; chaîne d'authentification NHRP

(C) code : aucune erreur(0)
préfixe : 32, mtu : 17912, hd_time : 7200
addr_len : 4(NSAP), subaddr_len : 0(NSAP), proto_len : 4, préf : 0
NBMA client : 172.16.10.1
protocole client : 10.1.1.254
Extension du dossier NHS du transport en transit(4) :
Extension de l'enregistrement NHS du transport inversé(5) :
Extension d'authentification(7) :
type : texte clair(1), données&deux-points ; NHRPAUTH
Extension d'adresse NAT(9) :
(C-1) code : aucune erreur(0)
préfixe : 32, mtu : 17912, hd_time : 0
addr_len : 4(NSAP), subaddr_len : 0(NSAP), proto_len : 4, préf : 0
NBMA client : 172.16.10.1
protocole client : 10.1.1.254

NHRP : Recevoir une réponse d'enregistrement via Tunnel0 vrf 0, taille de paquet : 128
F) afn : IPv4(1), type : IP(800), saut : 255, version : 1
shtl : 4(NSAP), sstl : 0 (NSAP)
pktsz : 128 Extoff : 52
(M) drapeaux : « nat unique », requis : 65541
src NBMA : 172.16.1.1
protocole src : 10.1.1.1, protocole dst : 10.1.1.254
(C-1) code : aucune erreur(0)
préfixe : 32, mtu : 17912, hd_time : 7200
addr_len : 0(NSAP), sous-addr_len : 0(NSAP), proto_len : 0, préf : 0
Extension d'adresse du répondeur(3) :
(C) code : aucune erreur(0)
préfixe : 32, mtu : 17912, hd_time : 7200
addr_len : 4(NSAP), subaddr_len : 0(NSAP), proto_len : 4, préf : 0
NBMA client : 172.16.10.1
protocole client : 10.1.1.254
Extension du dossier NHS du transport en transit(4) :
Extension de l'enregistrement NHS du transport inversé(5) :
Extension d'authentification(7) :
type : texte clair(1), données&deux-points ; NHRPAUTH
Extension d'adresse NAT(9) :
(C-1) code : aucune erreur(0)
préfixe : 32, mtu : 17912, hd_time : 0

Il s'agit de la réponse d'enregistrement NHR envoyée par le concentrateur au rayo réponse à la " de dem d'enregistrement NHR reçue plus tôt. Comm autres paquets d'enregistrement, le concentrateur envoie multiples de ceux-ci e réponse aux demande multiples.

Src NBMA : Adresse I (Internet) du rayon

protocole src : adress tunnel du satellite qui de s'enregistrer

protocole dst : adress tunnel du NHS/concentrateur

NBMA client : Adresse NBMA du NHS/concentrateur

protocole client : adre du tunnel du NHS/concentrateur

Extension

	addr_len : 4(NSAP), subaddr_len : 0(NSAP), proto_len : 4, préf : 0 **NBMA client : 172.16.10.1** **protocole client : 10.1.1.254** NHRP : netid_in = 0, to_us = 1	**d'authentification**, données&deux-points chaîne d'authentificati NHRP
Messages de service IPSec plus généraux indiquant qu'il fonctionne correctement.	IPSEC-IFC MGRE/Tu0 : crypto_ss_hear_start déjà en cours d'écoute IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : Ouverture d'un socket avec le profil DMVPN-IPSEC IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : recherche de connexion renvoyée par 8C93888 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : Socket est déjà ouvert. Ignorer. IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : tunnel_protection_stop_wait_timer 8C93888	
	NHRP : NHS-UP : 10.1.1.254	Messages de service NHRP indiquant que l NHS situé à l'adresse 10.1.1.254 est actif.
Message système qui indique que la contiguïté EIGRP est active avec le voisin en étoile à 10.1.1.1.	%DUAL-5-NBRCHANGE : EIGRP-IPv4 1 : Le voisin 10.1.1.1 (Tunnel0) est actif : nouvelle contiguïté	
	%DUAL-5-NBRCHANGE : EIGRP-IPv4 1 : Le voisin 10.1.1.254 (Tunnel0) est actif : nouvelle contiguïté	Message système indiquant que la conti EIGRP est active ave concentrateur voisin à 10.1.1.254.
Message système qui confirme une résolution NHRP réussie.	NHRP : NHRP a correctement résolu 10.1.1.1 en NBMA 172.16.1.1	

Confirmer la fonctionnalité et résoudre les problèmes

Cette section contient certaines des commandes **show** les plus utiles utilisées pour dépanner le concentrateur et le rayon. Afin d'activer des débogages plus spécifiques, utilisez ces conditions de débogage :

- debug dmvpn condition peer nbma *NBMA_ADDRESS*
- debug dmvpn condition peer tunnel *TUNNEL_ADDRESS*
- debug crypto condition peer ipv4 *NBMA_ADDRESS*

show crypto sockets

```
Spoke1#show crypto sockets

Number of Crypto Socket connections 1

Tu0 Peers (local/remote): 172.16.1.1/172.16.10.1
Local Ident (addr/mask/port/prot): (172.16.1.1/255.255.255.255/0/47)
Remote Ident (addr/mask/port/prot): (172.16.10.1/255.255.255.255/0/47)
IPSec Profile: "DMVPN-IPSEC"
```

```
Socket State: Open
Client: "TUNNEL SEC" (Client State: Active)

Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "DMVPN-IPSEC" Map-name: "Tunnel0-head-0"

Hub#show crypto sockets

Number of Crypto Socket connections 1

Tu0 Peers (local/remote): 172.16.10.1/172.16.1.1
Local Ident (addr/mask/port/prot): (172.16.10.1/255.255.255.255/0/47)
Remote Ident (addr/mask/port/prot): (172.16.1.1/255.255.255.255/0/47)
IPSec Profile: "DMVPN-IPSEC"
Socket State: Open
Client: "TUNNEL SEC" (Client State: Active)

Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "DMVPN-IPSEC" Map-name: "Tunnel0-head-0"
```

show crypto session detail

```
Spoke1#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel0
Uptime: 00:01:01
Session status: UP-ACTIVE
Peer: 172.16.10.1 port 500 fvrf: (none) ivrf: (none)
Phase1_id: 172.16.10.1
Desc: (none)
IKEv1 SA: local 172.16.1.1/500 remote 172.16.10.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:58
IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.10.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 25 drop 0 life (KB/Sec) 4596087/3538
Outbound: #pkts enc'ed 25 drop 3 life (KB/Sec) 4596087/3538

Hub#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel0
Uptime: 00:01:47
Session status: UP-ACTIVE
Peer: 172.16.1.1 port 500 fvrf: (none)
ivrf: (none)
Phase1_id: 172.16.1.1
Desc: (none)
IKEv1 SA: local 172.16.10.1/500 remote 172.16.1.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:12
IPSEC FLOW: permit 47 host 172.16.10.1 host 172.16.1.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 35 drop 0 life (KB/Sec) 4576682/3492
Outbound: #pkts enc'ed 35 drop 0 life (KB/Sec) 4576682/3492
```

show crypto isakmp sa detail

```
Spoke1#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
T - cTCP encapsulation, X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap.

1001 172.16.1.1 172.16.10.1 ACTIVE 3des sha psk 1 23:59:10
Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA

Hub#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
T - cTCP encapsulation, X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature
renc - RSA encryption IPv4 Crypto ISAKMP SA
C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap.

1001 172.16.10.1 172.16.1.1 ACTIVE 3des sha psk 1 23:58:20
Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA
```

show crypto ipsec sa detail

```
Spoke1#show crypto ipsec sa detail
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 172.16.1.1
protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.10.1/255.255.255.255/47/0)
current_peer 172.16.10.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 24, #pkts encrypt: 24, #pkts digest: 24
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#pkts no sa (send) 3, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.10.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0xA259D71(170237297)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8D538D11(2371063057)
transform: esp-3des esp-sha-hmac ,
```

```
in use settings ={Transport,}
conn id: 1, flow_id: SW:1, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4596087/3543)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0xA259D71(170237297)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2, flow_id: SW:2, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4596087/3543)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE
outbound ah sas:
outbound pcp sas:

Hub#show crypto ipsec sa detail
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 172.16.10.1

protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.10.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
current_peer 172.16.1.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 34, #pkts encrypt: 34, #pkts digest: 34
#pkts decaps: 34, #pkts decrypt: 34, #pkts verify: 34
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#pkts no sa (send) 0, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

local crypto endpt.: 172.16.10.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x8D538D11(2371063057)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xA259D71(170237297)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 1, flow_id: SW:1, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4576682/3497)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:
```

```
inbound pcp sas:

outbound esp sas: spi: 0x8D538D11(2371063057)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2, flow_id: SW:2, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4576682/3497)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:
outbound pcp sas:
```

show ip nhrp

```
Spoke1#show ip nhrp
10.1.1.254/32 via 10.1.1.254
Tunnel0 created 00:00:55, never expire
Type: static, Flags:
NBMA address: 172.16.10.1

Hub#show ip nhrp
10.1.1.1/32 via 10.1.1.1
Tunnel0 created 00:01:26, expire 01:58:33
Type: dynamic, Flags: unique registered
NBMA address: 172.16.1.1
```

show ip nhs

```
Spoke1#show ip nhrp nhs
Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel0:
10.1.1.254 RE priority = 0 cluster = 0

Hub#show ip nhrp nhs (As the hub is the only NHS for this DMVPN cloud,
it does not have any servers configured)
```

show dmvpn [detail]

```
"show dmvpn detail" returns the output of show ip nhrp nhs, show dmvpn,
and show crypto session detail

Spoke1#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.10.1 10.1.1.254 UP 00:00:39 S

Spoke1#show dmvpn detail
```

```
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface Tunnel0 is up/up, Addr. is 10.1.1.1, VRF ""
Tunnel Src./Dest. addr: 172.16.1.1/172.16.10.1, Tunnel VRF ""
Protocol/Transport: "GRE/IP", Protect "DMVPN-IPSEC"
Interface State Control: Disabled

IPv4 NHS:
10.1.1.254 RE priority = 0 cluster = 0
Type:Spoke, Total NBMA Peers (v4/v6): 1

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network
----- --------------- --------------- ----- -------- ----- -----------------
1 172.16.10.1 10.1.1.254 UP 00:00:41 S 10.1.1.254/32


Crypto Session Details:
--------------------------------------------------------------------------------
Interface: Tunnel0
Session: [0x08D513D0]
IKEv1 SA: local 172.16.1.1/500 remote 172.16.10.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:59:18
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 172.16.10.1
IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.10.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 21 drop 0 life (KB/Sec) 4596088/3558
Outbound: #pkts enc'ed 21 drop 3 life (KB/Sec) 4596088/3558
Outbound SPI : 0x A259D71, transform : esp-3des esp-sha-hmac
Socket State: Open

Pending DMVPN Sessions:

Hub#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details Type:Hub, NHRP Peers:1,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.1.1.1 UP 00:01:30 D

Hub#show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket # Ent --> Number of NHRP entries with same NBMA peer NHS
Status: E --> Expecting Replies, R --> Responding, W --> Waiting UpDn Time --> Up or Down Time
for a Tunnel ==========================================================================
Interface Tunnel0 is up/up, Addr. is 10.1.1.254, VRF "" Tunnel Src./Dest. addr:
172.16.10.1/MGRE, Tunnel VRF "" Protocol/Transport: "multi-GRE/IP", Protect "DMVPN-IPSEC"
Interface State Control: Disabled Type:Hub, Total NBMA Peers (v4/v6): 1
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network ----- --------------- --
------------- ----- -------- ----- ----------------- 1 172.16.1.1 10.1.1.1 UP 00:01:32 D
10.1.1.1/32
```

```
Crypto Session Details:
-------------------------------------------------------------------------------- Interface:
Tunnel0
Session: [0x08A27858]
IKEv1 SA: local 172.16.10.1/500 remote 172.16.1.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:26
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 172.16.1.1
IPSEC FLOW: permit 47 host 172.16.10.1 host 172.16.1.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 32 drop 0 life (KB/Sec) 4576682/3507
Outbound: #pkts enc'ed 32 drop 0 life (KB/Sec) 4576682/3507
Outbound SPI : 0x8D538D11, transform : esp-3des esp-sha-hmac
Socket State: Open

Pending DMVPN Sessions:
```

Informations connexes

- Dépannage IPsec : Présentation et utilisation des commandes de débogage
- Cryptage nouvelle génération
- RFC3706 : Détection des homologues morts IKE
- RFC3947 : Traversée NAT IKE
- Support et documentation techniques - Cisco Systems