Les debugs de Phase 1 DMVPN dépannent le guide

Contenu

Introduction

Ce document décrit les messages de débogage que vous rencontreriez sur le hub and spoke d'un déploiement multipoint dynamique de Phase 1 du réseau privé virtuel (DMVPN).

Conditions préalables

Pour la configuration et les commandes de débogage dans ce document, vous aurez besoin de deux Routeurs de Cisco qui exécutent la release 12.4(9)T de Cisco IOS® ou plus tard. Généralement un Phase 1 de base DMVPN exige la Cisco IOS version 12.2(13)T ou ultérieures

ou la version 12.2(33)XNC pour le routeur de services d'agrégation (ASR), bien que les caractéristiques et met au point vu dans ce document ne pourrait pas être prise en charge.

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Améliorations significatif

Ces versions de Cisco IOS ont introduit les caractéristiques ou les difficultés significatives pour le Phase 1 DMVPN :

- Release 12.2(18)SXF5 - un meilleur soutien d'ISAKMP en utilisant l'Infrastructure à clés publiques (PKI)
- Release 12.2(33)XNE - ASR, profils IPSecs, tunnel protection, traversée de Traduction d'adresses de réseau (NAT) d'IPSec
- Release 12.3(7)T - support de Virtual Routing and Forwarding d'intérieur (iVRF)
- Release 12.3(11)T - support de Virtual Routing and Forwarding d'entrée principale (fVRF)
- La release 12.4(9)T - soutien de divers DMVPN associé met au point et commande
- Release 12.4(15)T - Tunnel protection partagé
- Release 12.4(20)T - IPv6 au-dessus de DMVPN
- Version 15.0(1)M - Surveillance de la santé de tunnel de NHRP

Conventions

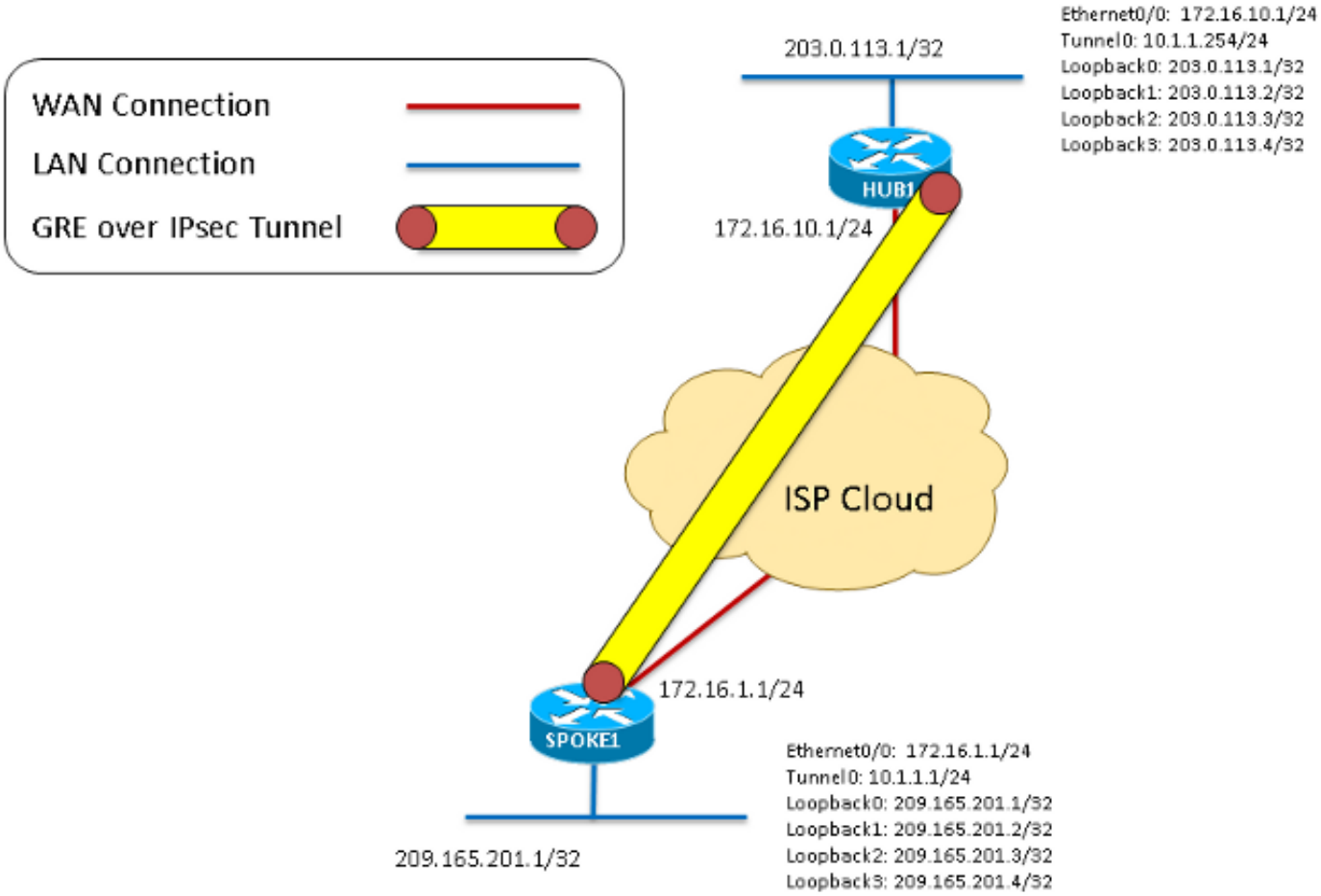
Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration appropriée

Aperçu de topologie

Pour cette topologie, deux 2911 ISR que la release 15.1(4)M4 de passage ont été configurés pour le Phase 1 DMVPN : un comme hub et un comme rai. Ethernet0/0 a été utilisé comme l'interface de « Internet » sur chaque routeur. Les quatre interfaces de bouclage sont configurées pour simuler les réseaux locaux qui vivent au hub ou au site en étoile. Car c'est une topologie de Phase 1 DMVPN avec seulement une a parlé, le rai est configurée avec un tunnel du Point à point GRE plutôt qu'un tunnel multipoint GRE. Le même crypto configuraton (ISAKMP et IPSec) a été utilisé sur chaque routeur pour les assurer a apparié exactement.

Diagramme 1



Crypto

C'est identique sur le hub et le rai.

```
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
```

Hub

```
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
```

Rai

```
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
```

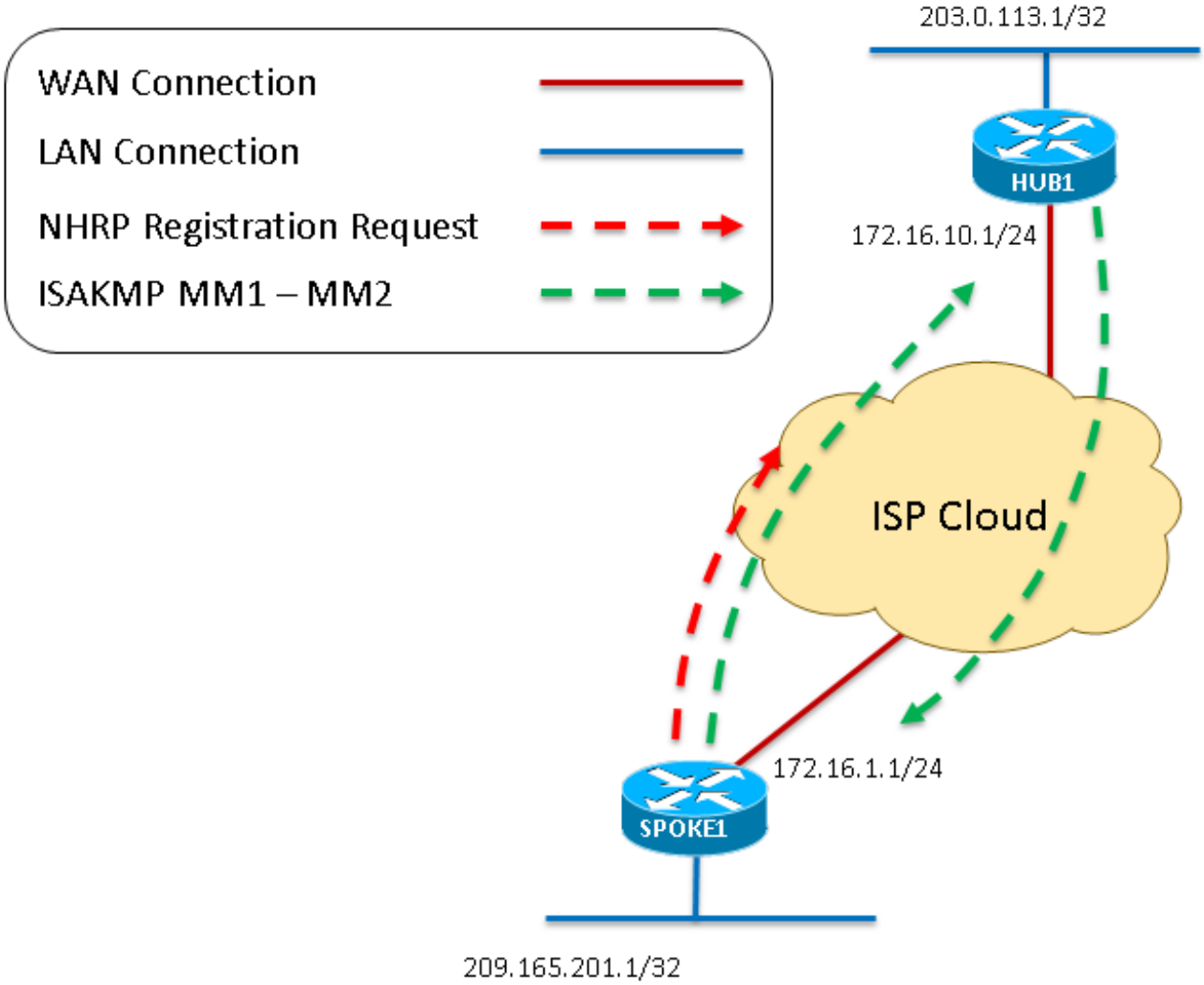
```
ip address 209.165.201.1 255.255.255.255
interface Loopback1
ip address 209.165.201.2 255.255.255.255
interface Loopback2
ip address 209.165.201.3 255.255.255.255
interface Loopback3
ip address 209.165.201.4 255.255.255.255

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
```

Debugs

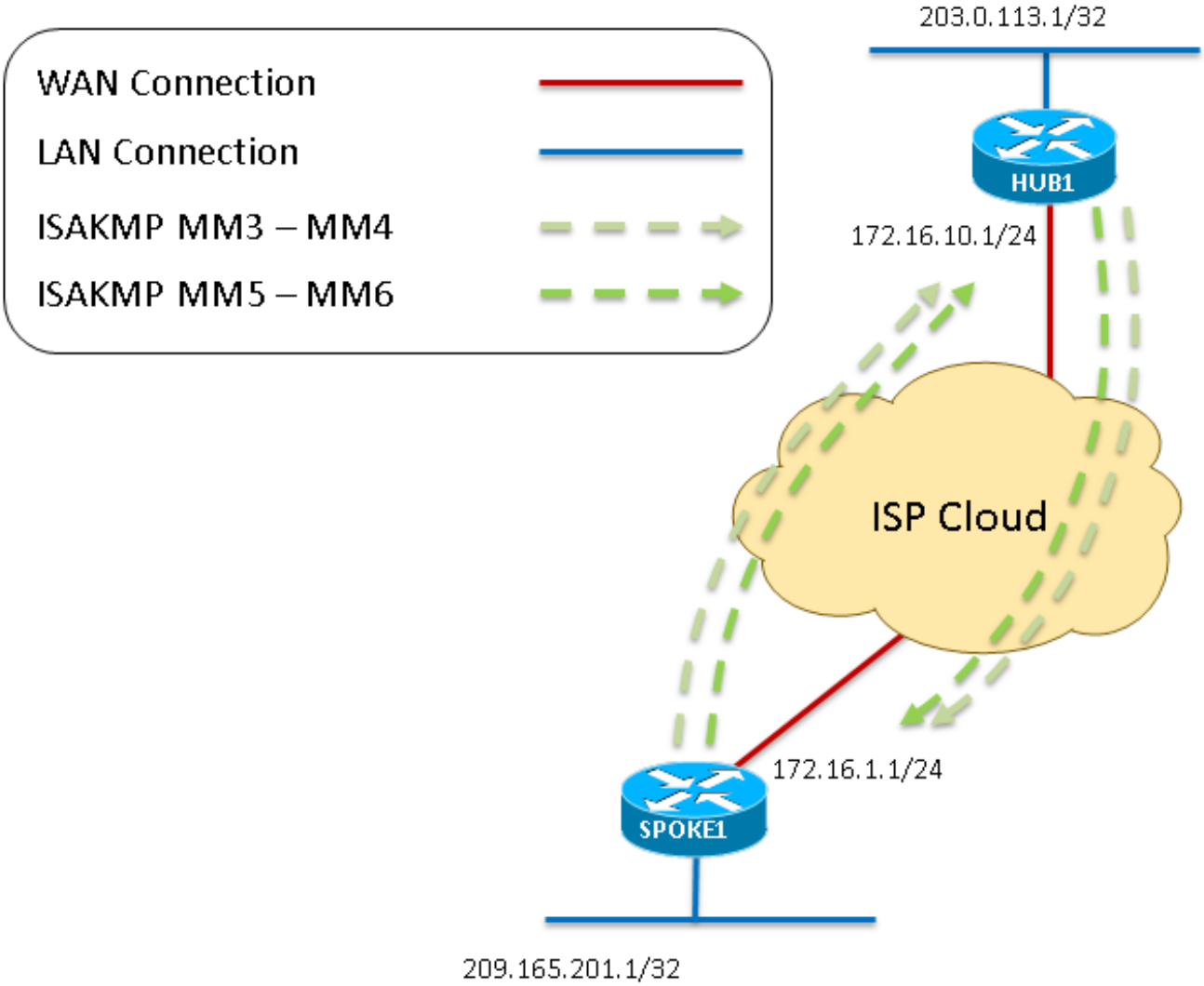
Visualisation de l'écoulement de paquet

C'est une visualisation de l'écoulement entier de paquet DMVPN comme vu dans ce document. Plus détaillé met au point qui expliquent chacune des étapes sont également inclus.

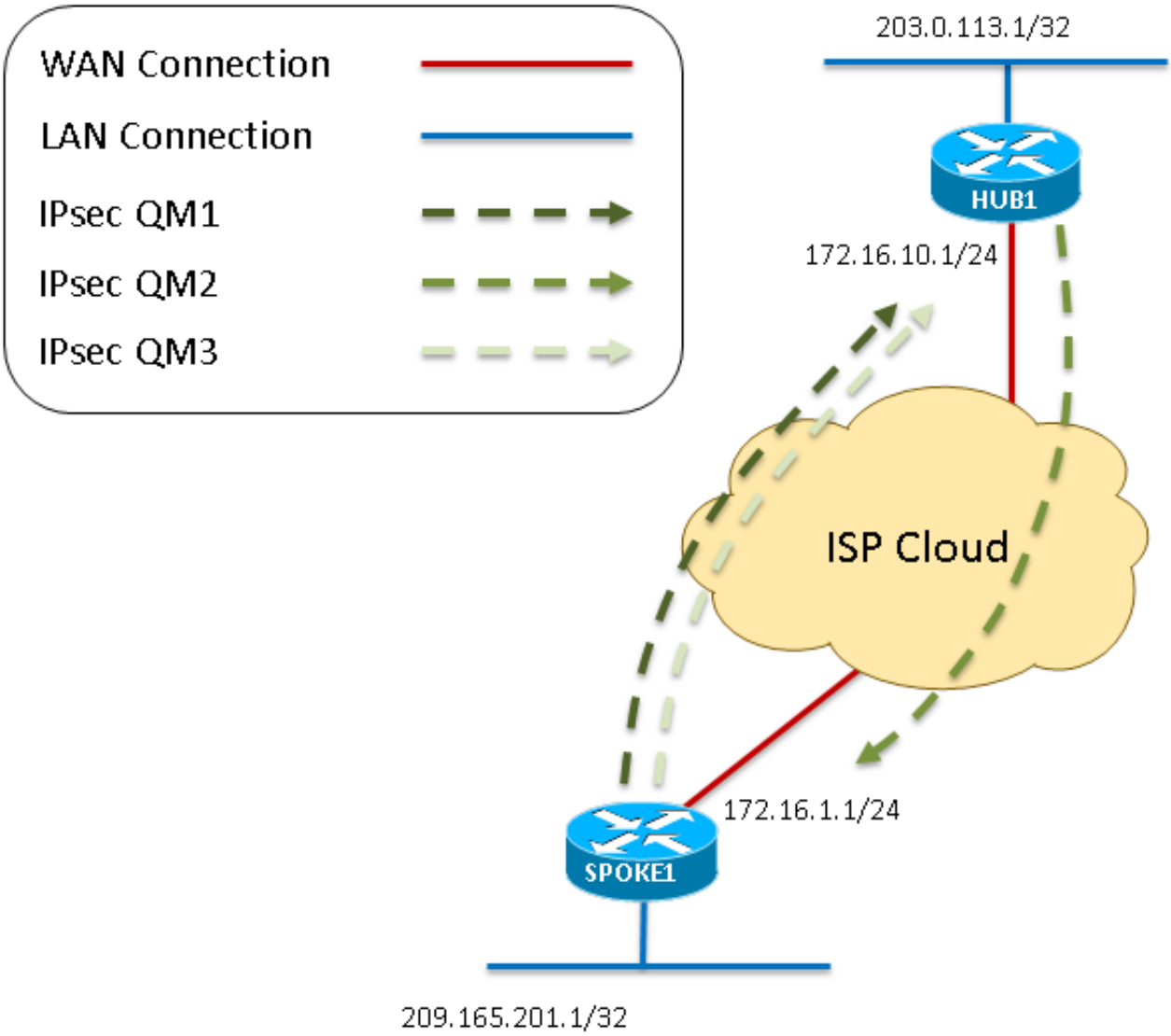
1. Quand le tunnel sur le rai n'est « aucun arrêt » il génère une demande d'enregistrement de NHRP, qui commence le processus DMVPN. Car la configuration du hub est complètement dynamique, le rai doit être le point final qui initie la connexion.
2. La demande d'enregistrement de NHRP est alors encapsulée dans GRE qui déclenche le crypto processus pour commencer.
3. En ce moment, le premier ISAKMP le message que principal de mode - l'ISAKMP MM1 - est envoyé du a parlé au hub sur le port UDP500.
4. Le hub reçoit et traite MM1 et répond avec l'ISAKMP MM2, car il a une stratégie ISAKMP assortie.
   Le diagramme 2 - se rapporte aux étapes 1
   4



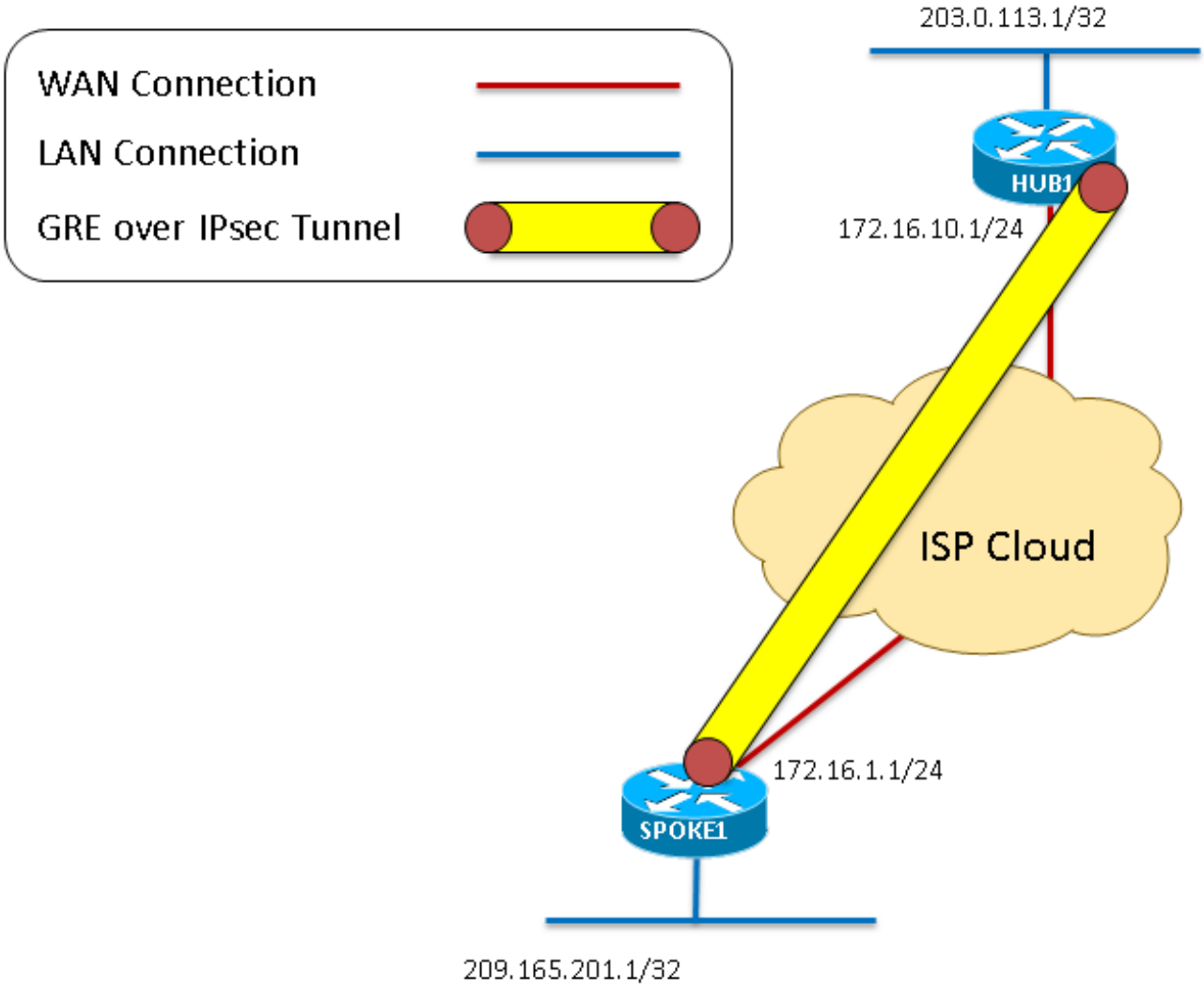
5. Une fois le rai reçoit le MM2, il répond avec MM3. Comme avec MM1, le rai confirme la stratégie ISAKMP reçue est valide.
6. Le hub reçoit MM3 et répond avec MM4.
7. En ce moment dans la négociation ISAKMP, le rai pourrait répondre sur le port UDP4500 si NAT est détecté dans le chemin de transit. Cependant, si pas NAT est détecté le rai continue et envoie MM5 sur UDP500. Pour finir, le hub répond avec MM6 afin de se terminer l'échange principal de mode.
   Le diagramme 3 - se rapporte aux étapes 5
   7



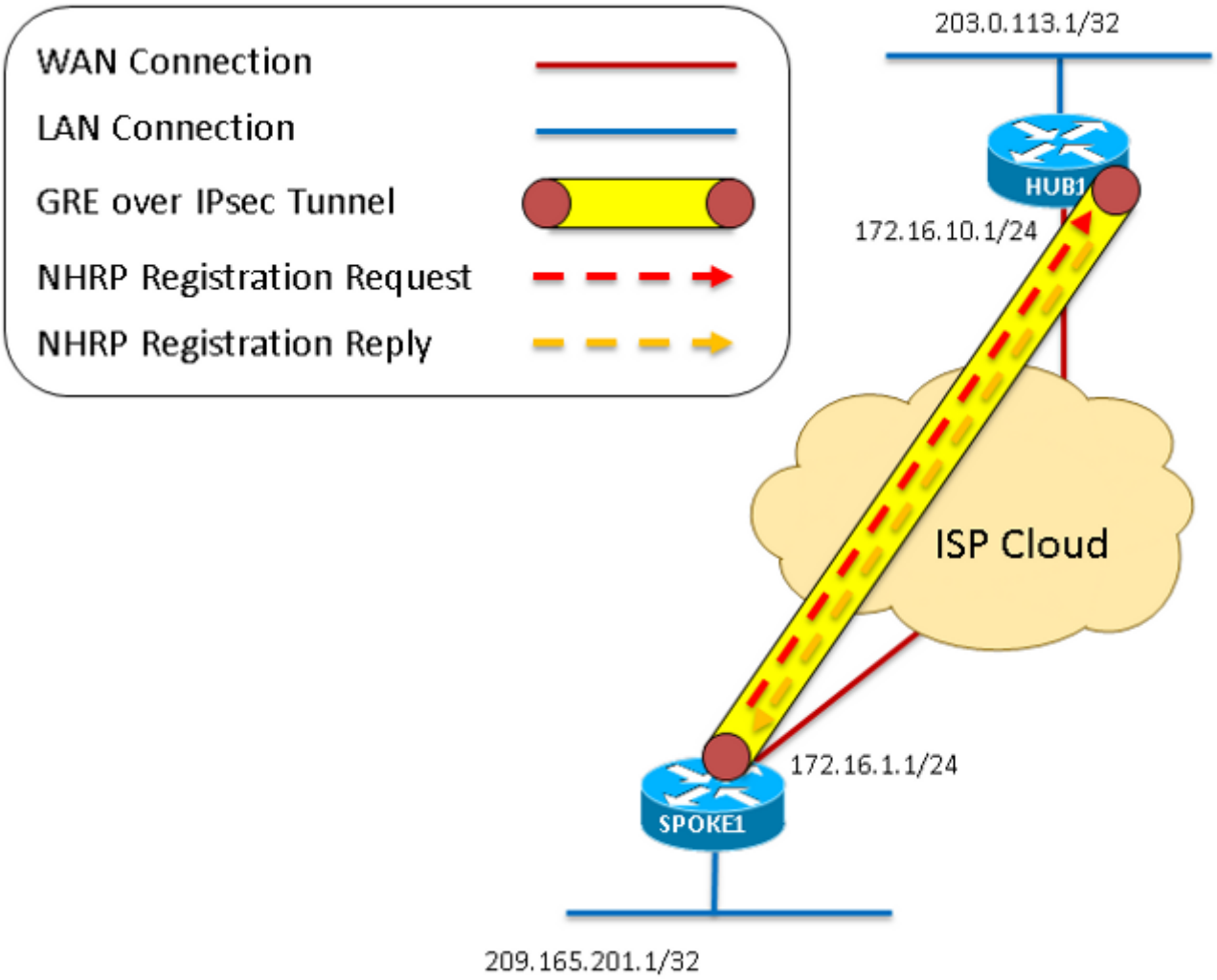
8. Une fois le rai reçoit MM6 du hub, il envoie QM1 au hub sur UDP500 afin de commencer le mode rapide.
9. Le hub reçoit QM1 et répond avec QM2, comme tous des attributs reçus sont reçus. En ce moment le hub crée le Phase 2 SAS pour cette session.
10. Comme dernière étape de la négociation rapide de mode, QM2 est reçu par le rai. Le rai alors crée son Phase 2 SAS et envoie QM3 dans la réponse. Ceci se termine l'ISAKMP et la négociation IPSec. Il y a maintenant une session d'IPSec qui chiffre le trafic GRE entre ces deux pairs.
    Le diagramme 4 - se rapporte aux étapes 8
    10



11. Maintenant que la crypto session est en hausse et capable passer le trafic, ces paquets sont encapsulés dans le GRE au-dessus du tunnel d'IPSec.
    Le diagramme 5 - se rapporte à l'étape
    11



12. Comme a été vu dans les premières étapes, le rai génère une demande d'enregistrement de NHRP qui est envoyée à travers le GRE au-dessus du tunnel d'IPSec.
13. Le hub reçoit les demandes d'enregistrement de NHRP et envoie une réponse d'enregistrement de NHRP une fois qu'il confirme le rai a une adresse à plusieurs accès valide de tunnel et de Nonbroadcast (NBMA). Le rai reçoit cette réponse d'enregistrement de NHRP qui complète la procédure d'enregistrement.
    Le diagramme 6 - se rapporte aux étapes 12
    13



Ceux-ci met au point sont le résultat quand le **debug dmvpn toute toute la** commande est entré sur les Routeurs de hub and spoke. Ce commandes enables particulières que cet ensemble de met au point :

```
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
```

Debugs avec l'explication

Car c'est un configuraton où IPSec est mis en application, met au point l'exposition tout les ISAKMP et IPSec met au point. Si pas crypto en est configuré, ignore met au point ce début avec « IPsec » ou « ISAKMP. »

EXPLICATION DE DEBUG DE HUB	DEBUGS DANS L'ORDRE	EXPLICATION DE D DE RAI
Ces messages de débogage premiers sont générés par une **aucune commande shutdown** sélectionnée sur l'interface de tunnel. Des messages sont générés par services de cryptos, GRE, et de NHRP étant initiés. Une erreur d'enregistrement de NHRP est vue sur le hub parce qu'il ne fait pas configurer un prochain serveur de saut (NHS) (le hub est NHS pour notre nuage DMVPN). Ceci est prévu.	IPSEC-IFC MGRE/Tu0 : Vérifier l'état de tunnel. **NHRP : if_up : Tunnel0 0 proto** IPSEC-IFC MGRE/Tu0 : monter de tunnel IPSEC-IFC MGRE/Tu0 : crypto_ss_listen_start écoutant déjà **%CRYPTO-6-ISAKMP_ON_OFF : L'ISAKMP est allumé** **NHRP : Incapable d'envoyer l'enregistrement - aucun NHSes n'a configuré** %LINK-3-UPDOWN : Interface Tunnel0, état modifié à NHRP : if_up : Tunnel0 0 proto NHRP : Incapable d'envoyer l'enregistrement - aucun NHSes n'a configuré IPSEC-IFC MGRE/Tu0 : monter de tunnel IPSEC-IFC MGRE/Tu0 : crypto_ss_listen_start écoutant déjà **%LINEPROTO-5-UPDOWN : Line protocol on Interface Tunnel0, état modifié à**	
	IPSEC-IFC GRE/Tu0 : Vérifier l'état de tunnel. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : la consultation de connexion a renvoyé 0 **IPSEC-IFC GRE/Tu0 : crypto_ss_listen_start écoutant déjà** **IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : Ouvrir un socket avec le profil DMVPN-IPSEC** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : la consultation de connexion a renvoyé 0 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : Déclenchant le tunnel immédiatement. IPSEC-IFC GRE/Tu0 : Ajouter l'interface de tunnel Tunnel0 à la liste partagée **NHRP : if_up : Tunnel0 0 proto** **NHRP : Tunnel0 : Le cache ajoutent pour le prochain-saut 10.1.1.254 de la cible 10.1.1.254/32**	Ces messages de débogage premiers s générés par une **aucu** **commande shutdown** sélectionnée sur l'inte de tunnel. Des messa sont générés par serv de cryptos, GRE, et d NHRP qui sont initiés Supplémentaire, le ra ajoute une entrée à s propre cache de NHR pour sa propre adres NBMA et de tunnel.

	172.16.10.1 IPSEC-IFC GRE/Tu0 : monter de tunnel IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : connexion 961D220 retourné par consultation IPSEC-IFC GRE/Tu0 : crypto_ss_listen_start écoutant déjà IPSEC-IFC GRE/Tu0 : crypto_ss_listen_start écoutant déjà IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : Ouvrir un socket avec le profil DMVPN-IPSEC IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : connexion 961D220 retourné par consultation IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : Le socket déjà est ouvert. Ignorer. CRYPTO_SS (SEC DE TUNNEL) : Écoute commencée par application l'insertion de la carte dans le mapdb AVL a manqué, des paires de carte + d'as existe déjà sur le mapdb **%CRYPTO-6-ISAKMP_ON_OFF : L'ISAKMP est allumé** CRYPTO_SS (SEC DE TUNNEL) : Active ouvert, les informations de socket : gens du pays 172.16.1.1 172.16.1.1/255.255.255.255/0, 172.16.10.1 distant 172.16.10.1/255.255.255.255/0, protocole 47, ifc Tu0	
DÉBUT D'ISAKMP (NÉGOCIATION DE PHASE I)		
	IPSEC(recalculate_mtu) : remettez à l'état initial le mtu du sadb_root 94EFDC0 à 1500 **IPSEC(sa_request) : ,** **(msg principaux de l'Eng.) local= SORTANT 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),** **l'ESP de protocol=, ESP-SHA-hmac du transform= esp-3des (transport),** **lifedur= 3600s et 4608000kb,** **spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0** ISAKMP:(0) : Le profil de demande SA est (le NULL) ISAKMP : A créé un struct de pair pour 172.16.10.1, le peer port 500 ISAKMP : Le nouveau pair a créé le pair = le peer_handle 0x95F6858 = le 0x80000004 ISAKMP : Verrouillage du struct 0x95F6858 de pair, isakmp_initiator de 1par de refcount ISAKMP : port local 500, port distant 500 ISAKMP : placez le nouveau noeud 0 à QM_IDLE ISAKMP:(0):insert SA avec succès SA = 8A26FB0 **Mode agressif de début ISAKMP:(0):Can pas, essayant le mode principal.** Clé pré-partagée de pair ISAKMP:(0):found appariant 172.16.10.1 ISAKMP:(0) : ID NAT-T construit vendor-rfc3947	La première étape ur que le tunnel n'est « a arrêt » est de comme la crypto négociation. rai crée une demande des tentatives de commencer le mode agressif et échoue de nouveau au mode pri Puisque le mode agre n'est pas configuré su ou l'autre de routeur, est prévu. Le rai commence le r principal et envoie le premier message d'ISAKMP, MM_NO_STATE. Modifications d'état d'ISAKMP d'IKE_REA IKE_I_MM1. Les messages d'ID d constructeur NAT-T s utilisés dans la détec la traversée de NAT. messages sont prévu pendant la négociatio l'ISAKMP indépendar

	ISAKMP:(0) : ID NAT-T construit vendor-07 ISAKMP:(0) : ID NAT-T construit vendor-03 ISAKMP:(0) : ID NAT-T construit vendor-02 **ISAKMP:(0):Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM** **État ISAKMP:(0):Old = état IKE_READY nouvel = IKE_I_MM1** **ISAKMP:(0) : commencer l'échange principal de mode** **ISAKMP:(0) : envoyant le paquet au peer_port 500 (i) MM_NO_STATE du my_port 500 de 172.16.10.1** ISAKMP:(0):sending un paquet d'ipv4 d'IKE. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : connexion 961D220 retourné par consultation IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : message prêt de bon socket	de si NAT est mis en application. Comme l messages agressifs mode, ceux-ci sont p
Après que le tunnel du rai ne soit « aucun arrêt, » le hub reçoit NOUVELLE SA d'IKE (message principal de mode 1) sur port 500. En tant que responder, le hub crée une association de sécurité d'ISAKMP (SA). Les modifications d'état d'ISAKMP d'IKE_READY à IKE_R_MM1.	**ISAKMP (0) : paquet reçu SA globale du sport 500 du dport 500 de 172.16.1.1 (n) de NOUVELLE** **ISAKMP : A créé un struct de pair pour 172.16.1.1, le peer port 500** ISAKMP : Le nouveau pair a créé le pair = le peer_handle 0x8CACD00 = le 0x80000003 ISAKMP : Verrouillage du struct 0x8CACD00 de pair, crypto_isakmp_process_block de 1par de refcount ISAKMP : port local 500, port distant 500 **ISAKMP:(0):insert SA avec succès SA = 6A5BDE8** ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **État ISAKMP:(0):Old = état IKE_READY nouvel = IKE_R_MM1**	
Le message principal reçu du mode 1 d'IKE est traité. Le hub détermine que le pair a des attributs assortis d'ISAKMP et ils sont versés dans le SA ISAKMP qui a été juste créé. Les messages prouvent que le pair utilise 3DES-CBC pour le cryptage, le hachage du SHA, le groupe 1 de Diffie Hellman (CAD), la clé pré-partagée pour l'authentification, et la vie de par défaut SA de 86400 secondes (0x0 0x1 0x51 0x80 = 0x15180 = 86400 secondes). L'état d'ISAKMP est toujours IKE_R_MM1 puisqu'une réponse a pour ne pas être envoyée au rai.	ISAKMP:(0) : traitement de la charge utile SA. ID de message = 0 ISAKMP:(0) : traitement de la charge utile d'id de constructeur **ISAKMP:(0) : l'ID de constructeur semble non-concordance Unity/DPD mais de commandant 69** **ISAKMP (0) : l'ID de constructeur est RFC 3947 NAT-T** ISAKMP:(0) : traitement de la charge utile d'id de constructeur ISAKMP:(0) : l'ID de constructeur semble non-concordance Unity/DPD mais de commandant 245 ISAKMP (0) : l'ID de constructeur est NAT-T v7 ISAKMP:(0) : traitement de la charge utile d'id de constructeur ISAKMP:(0) : l'ID de constructeur semble non-concordance Unity/DPD mais de commandant 157 ISAKMP:(0) : l'ID de constructeur est NAT-T v3 ISAKMP:(0) : traitement de la charge utile d'id de constructeur ISAKMP:(0) : l'ID de constructeur semble non-concordance Unity/DPD mais de commandant 123	

Les messages d'ID de constructeur NAT-T sont utilisés dans la détection et la traversée de NAT. Ces messages sont prévus pendant la négociation de l'ISAKMP indépendamment de si NAT est mis en application. Des messages semblables sont vus pour Dead Peer Detection (DPD).	ISAKMP:(0) : l'ID de constructeur est NAT-T v2 **Clé pré-partagée de pair ISAKMP:(0):found appariant 172.16.1.1** **ISAKMP:(0) : clé pré-partagée locale trouvée** ISAKMP : Profils de balayage pour le Xauth… **L'ISAKMP ISAKMP:(0):Checking transforment 1 contre la stratégie prioritaire 1** **ISAKMP : cryptage 3DES-CBC** **ISAKMP : SHA d'informations parasites** **ISAKMP : groupe par défaut 1** **ISAKMP : pré-partage authentique** **ISAKMP : type de vie en quelques secondes** **ISAKMP : durée de vie (VPI) de 0x0 0x1 0x51 0x80** **ISAKMP:(0):atts sont acceptables. La prochaine charge utile est 0** **Atts ISAKMP:(0):Acceptable : vie réelle : 0** **Atts ISAKMP:(0):Acceptable : vie : 0** **Atts ISAKMP:(0):Fill à SA vpi_length:4** **Atts ISAKMP:(0):Fill à SA life_in_seconds:86400** **Vie réelle ISAKMP:(0):Returning : 86400** **Temporisateur de vie ISAKMP:(0)::started : 86400.** ISAKMP:(0) : traitement de la charge utile d'id de constructeur ISAKMP:(0) : l'ID de constructeur semble non-concordance Unity/DPD mais de commandant 69 ISAKMP (0) : l'ID de constructeur est RFC 3947 NAT-T ISAKMP:(0) : traitement de la charge utile d'id de constructeur ISAKMP:(0) : l'ID de constructeur semble non-concordance Unity/DPD mais de commandant 245 ISAKMP (0) : l'ID de constructeur est NAT-T v7 ISAKMP:(0) : traitement de la charge utile d'id de constructeur ISAKMP:(0) : l'ID de constructeur semble non-concordance Unity/DPD mais de commandant 157 ISAKMP:(0) : l'ID de constructeur est NAT-T v3 ISAKMP:(0) : traitement de la charge utile d'id de constructeur ISAKMP:(0) : l'ID de constructeur semble non-concordance Unity/DPD mais de commandant 123 ISAKMP:(0) : l'ID de constructeur est NAT-T v2 ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE État ISAKMP:(0):Old = nouvel état IKE_R_MM1 = IKE_R_MM1	
MM_SA_SETUP (le mode principal 2) est envoyé au rai, qui confirme ce MM1 a été reçu et a reçu comme paquet valide d'ISAKMP.	ISAKMP:(0) : ID NAT-T construit vendor-rfc3947 **ISAKMP:(0) : envoyant le paquet au peer_port 500 (r) MM_SA_SETUP du my_port 500 de 172.16.1.1** ISAKMP:(0):sending un paquet d'ipv4 d'IKE. ISAKMP:(0):Input = IKE_MESG_INTERNAL,	

Modifications d'état d'ISAKMP d'IKE_R_MM1 à IKE_R_MM2.	IKE_PROCESS_COMPLETE **État ISAKMP:(0):Old = nouvel état IKE_R_MM1 = IKE_R_MM2**	
	ISAKMP (0) : paquet reçu du sport 500 (i) MM_NO_STATE global du dport 500 de 172.16.10.1 **ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH** **État ISAKMP:(0):Old = nouvel état IKE_I_MM1 = IKE_I_MM2** ISAKMP:(0) : traitement de la charge utile SA. ID de message = 0 ISAKMP:(0) : traitement de la charge utile d'id de constructeur **ISAKMP:(0) : l'ID de constructeur semble non-concordance Unity/DPD mais de commandant 69** ISAKMP (0) : l'ID de constructeur est RFC 3947 NAT-T Clé pré-partagée de pair ISAKMP:(0):found appariant 172.16.10.1 ISAKMP:(0) : clé pré-partagée locale trouvée ISAKMP : Profils de balayage pour le Xauth… **L'ISAKMP ISAKMP:(0):Checking transforment 1 contre la stratégie prioritaire 1** **ISAKMP : cryptage 3DES-CBC** **ISAKMP : SHA d'informations parasites** **ISAKMP : groupe par défaut 1** **ISAKMP : pré-partage authentique** **ISAKMP : type de vie en quelques secondes** **ISAKMP : durée de vie (VPI) de 0x0 0x1 0x51 0x80** **ISAKMP:(0):atts sont acceptables. La prochaine charge utile est 0** **Atts ISAKMP:(0):Acceptable : vie réelle : 0** **Atts ISAKMP:(0):Acceptable : vie : 0** **Atts ISAKMP:(0):Fill à SA vpi_length:4** **Atts ISAKMP:(0):Fill à SA life_in_seconds:86400** **Vie réelle ISAKMP:(0):Returning : 86400** **Temporisateur de vie ISAKMP:(0)::started : 86400.** ISAKMP:(0) : traitement de la charge utile d'id de constructeur ISAKMP:(0) : l'ID de constructeur semble non-concordance Unity/DPD mais de commandant 69 ISAKMP (0) : l'ID de constructeur est RFC 3947 NAT-T ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE État ISAKMP:(0):Old = nouvel état IKE_I_MM2 = IKE_I_MM2	En réponse au messa MM1 envoyé au hub, arrive qui des confim MM1 a été reçu. Le message principal re mode 2 d'IKE est trai rai se rend compte qu hub de pair a des attr assortis d'ISAKMP et attributs sont versés le SA ISAKMP qui a é créé. Ce paquet prou que le pair utilise 3DE CBC pour le cryptage hachage du SHA, le g 1 de Diffie Hellman (la clé pré-partagée p l'authentification, et la de par défaut SA de 8 secondes (0x0 0x1 0x 0x80 = 0x15180 = 86 secondes). En plus des message NAT-T, il y a un écha pour déterminer si la session utilisera DPD Les modifications d'é d'ISAKMP d'IKE_I_M IKE_I_MM2.
	ISAKMP:(0) : envoyant le paquet au peer_port 500 (i) MM_SA_SETUP du my_port 500 de 172.16.10.1 ISAKMP:(0):sending un paquet d'ipv4 d'IKE.	MM_SA_SETUP (le r principal 3) est envoy hub, qui confirme que

	ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **État ISAKMP:(0):Old = nouvel état IKE_I_MM2 = IKE_I_MM3**	a reçu MM2 et le vou poursuivre. Les modifications d'é d'ISAKMP d'IKE_I_M IKE_I_MM3.
MM_SA_SETUP (le mode principal 3) est reçu par le hub. Le hub conclut que le pair est un autre Cisco IOS périphérique et pas NAT est détecté pour nous ou notre pair. Les modifications d'état d'ISAKMP d'IKE_R_MM2 à IKE_R_MM3.	**ISAKMP (0) : paquet reçu du sport 500 (r) MM_SA_SETUP global du dport 500 de 172.16.1.1** ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **État ISAKMP:(0):Old = nouvel état IKE_R_MM2 = IKE_R_MM3** ISAKMP:(0) : traitement de la charge utile du KE. ID de message = 0 ISAKMP:(0) : charge utile de processing NONCE. ID de message = 0 **Clé pré-partagée de pair ISAKMP:(0):found appariant 172.16.1.1** ISAKMP:(1002) : traitement de la charge utile d'id de constructeur ISAKMP:(1002) : l'ID de constructeur est DPD ISAKMP:(1002) : traitement de la charge utile d'id de constructeur **ISAKMP:(1002) : parler dans une autre case IOS !** ISAKMP:(1002) : traitement de la charge utile d'id de constructeur ISAKMP:(1002) : l'ID de constructeur semble non-concordance Unity/DPD mais de commandant 225 ISAKMP:(1002) : l'ID de constructeur est XAUTH ISAKMP : type reçu 20 de charge utile **ISAKMP (1002) : Le sien ne hachent aucune correspondance - ce noeud en dehors de NAT** ISAKMP : type reçu 20 de charge utile **ISAKMP (1002) : Pas NAT trouvé pour l'individu ou le pair** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE État ISAKMP:(1002):Old = nouvel état IKE_R_MM3 = IKE_R_MM3	
MM_KEY_EXCH (le mode principal 4) est envoyé par le hub. Modifications d'état d'ISAKMP d'IKE_R_MM3 à IKE_R_MM4.	**ISAKMP:(1002) : envoyant le paquet au peer_port 500 (r) MM_KEY_EXCH du my_port 500 de 172.16.1.1** ISAKMP:(1002):sending un paquet d'ipv4 d'IKE. ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **État ISAKMP:(1002):Old = nouvel état IKE_R_MM3 = IKE_R_MM4**	
	ISAKMP (0) : paquet reçu du sport 500 (i) MM_SA_SETUP global du dport 500 de 172.16.10.1 ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **État ISAKMP:(0):Old = nouvel état IKE_I_MM3 = IKE_I_MM4**	MM_SA_SETUP (le r principal 4) est reçu p rai. Le rai conclut que pair est un autre Cisc périphérique et pas N est détecté pour nous

	ISAKMP:(0) : traitement de la charge utile du KE. ID de message = 0 ISAKMP:(0) : charge utile de processing NONCE. ID de message = 0 **Clé pré-partagée de pair ISAKMP:(0):found appariant 172.16.10.1** ISAKMP:(1002) : traitement de la charge utile d'id de constructeur ISAKMP:(1002) : l'ID de constructeur est Unity ISAKMP:(1002) : traitement de la charge utile d'id de constructeur ISAKMP:(1002) : l'ID de constructeur est DPD ISAKMP:(1002) : traitement de la charge utile d'id de constructeur **ISAKMP:(1002) : parler dans une autre case IOS !** ISAKMP : type reçu 20 de charge utile **ISAKMP (1002) : Le sien ne hachent aucune correspondance - ce noeud en dehors de NAT** ISAKMP : type reçu 20 de charge utile **ISAKMP (1002) : Pas NAT trouvé pour l'individu ou le pair** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE État ISAKMP:(1002):Old = nouvel état IKE_I_MM4 = IKE_I_MM4	notre pair. Les modifications d'é d'ISAKMP d'IKE_I_M IKE_I_MM4.
	Contact d'initiale ISAKMP:(1002):send **ISAKMP:(1002):sA fait l'authentification principale pré-partagée utilisant le type ID_IPV4_ADDR d'id** ISAKMP (1002) : Charge utile d'ID prochain-charge utile : 8 type : 1 adresse : 172.16.1.1 protocole : 17 port : 500 longueur : 12 Longueur de charge utile ISAKMP:(1002):Total : 12 **ISAKMP:(1002) : envoyant le paquet au peer_port 500 (i) MM_KEY_EXCH du my_port 500 de 172.16.10.1** ISAKMP:(1002):sending un paquet d'ipv4 d'IKE. ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **État ISAKMP:(1002):Old = nouvel état IKE_I_MM4 = IKE_I_MM5**	MM_KEY_EXCH (le r principal 5) est envoy le rai. Les modifications d'é d'ISAKMP d'IKE_I_M IKE_I_MM5.
MM_KEY_EXCH (le mode principal 5) est reçu par le hub. Les modifications d'état d'ISAKMP d'IKE_R_MM4 à IKE_R_MM5. Supplémentaire, « le *none* de	**ISAKMP (1002) : paquet reçu du sport 500 (r) MM_KEY_EXCH global du dport 500 de 172.16.1.1** ISAKMP:(1002):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **État ISAKMP:(1002):Old = nouvel état IKE_R_MM4 = IKE_R_MM5** ISAKMP:(1002) : charge utile d'IDENTIFICATEUR DE	

correspondances de pair des profils » est dû vu au manque d'un profil d'ISAKMP. Puisque c'est le cas, l'ISAKMP n'utilise pas un profil.	PROCESSUS. ID de message = 0 ISAKMP (1002) : Charge utile d'ID prochain-charge utile : 8 type : 1 adresse : 172.16.1.1 protocole : 17 port : 500 longueur : 12 **ISAKMP:(0) : : le pair apparie le *none* des profils** ISAKMP:(1002) : charge utile de processing HASH. ID de message = 0 ISAKMP:(1002) : le traitement INFORMENT le protocole 1 INITIAL_CONTACT spi 0, ID de message = 0, SA = 0x6A5BDE8 État d'authentification ISAKMP:(1002):sA : authentifié ISAKMP:(1002):sA a été authentifié avec 172.16.1.1 État d'authentification ISAKMP:(1002):sA : authentifié ISAKMP:(1002) : Contact initial de processus, apportez SA vers le bas existantes de la phase 1 et 2 avec le port distant distant 500 de 172.16.10.1 172.16.1.1 de gens du pays **ISAKMP : Essayant d'insérer un pair 172.16.10.1/172.16.1.1/500/, et avec succès inséré 8CACD00.** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE État ISAKMP:(1002):Old = nouvel état IKE_R_MM5 = IKE_R_MM5 IPSEC(key_engine) : a obtenu un événement de file d'attente avec 1 message KMI ISAKMP:(1002):sA fait l'authentification principale pré-partagée utilisant le type ID_IPV4_ADDR d'id ISAKMP (1002) : Charge utile d'ID prochain-charge utile : 8 type : 1 adresse : 172.16.10.1 protocole : 17 port : 500 longueur : 12 Longueur de charge utile ISAKMP:(1002):Total : 12	
Le paquet de la finale MM_KEY_EXCH (le mode principal 6) est envoyé par le hub. Ceci se termine la négociation de Phase 1 qui signifie ce périphérique est prête pour le Phase 2 (mode rapide d'IPSec). Les modifications d'état d'ISAKMP d'IKE_R_MM5 à	**ISAKMP:(1002) : envoyant le paquet au peer_port 500 (r) MM_KEY_EXCH du my_port 500 de 172.16.1.1** ISAKMP:(1002):sending un paquet d'ipv4 d'IKE. ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **État ISAKMP:(1002):Old = nouvel état IKE_R_MM5 = IKE_P1_COMPLETE** ISAKMP:(1002):Input = IKE_MESG_INTERNAL,	

IKE_P1_COMPLETE.	IKE_PHASE1_COMPLETE État ISAKMP:(1002):Old = état IKE_P1_COMPLETE nouvel = IKE_P1_COMPLETE	
	ISAKMP (1002) : paquet reçu du sport 500 (i) MM_KEY_EXCH global du dport 500 de 172.16.10.1 ISAKMP:(1002) : charge utile d'IDENTIFICATEUR DE PROCESSUS. ID de message = 0 ISAKMP (1002) : Charge utile d'ID prochain-charge utile : 8 type : 1 adresse : 172.16.10.1 protocole : 17 port : 500 longueur : 12 **ISAKMP:(0) : : le pair apparie le *none* des profils** ISAKMP:(1002) : charge utile de processing HASH. ID de message = 0 État d'authentification ISAKMP:(1002):sA : authentifié ISAKMP:(1002):sA a été authentifié avec 172.16.10.1 **ISAKMP : Essayant d'insérer un pair 172.16.1.1/172.16.10.1/500/, et avec succès inséré 95F6858.** ISAKMP:(1002):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **État ISAKMP:(1002):Old = nouvel état IKE_I_MM5 = IKE_I_MM6** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE État ISAKMP:(1002):Old = nouvel état IKE_I_MM6 = IKE_I_MM6 ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **État ISAKMP:(1002):Old = nouvel état IKE_I_MM6 = IKE_P1_COMPLETE**	Le paquet de la finale MM_KEY_EXCH (le r principal 6) est reçu p rai. Ceci se termine la négociation de Phase signifie ce périphériqu prête pour le Phase 2 (mode rapide d'IPSec Les modifications d'é d'ISAKMP d'IKE_I_M IKE_I_MM6, et puis immédiatement à IKE_P1_COMPLETE Supplémentaire, « le *none* de correspondances de des profils » est dû vu manque d'un profil d'ISAKMP. Puisque c cas, l'ISAKMP n'utilis un profil.
FIN D'ISAKMP (NÉGOCIATION DE PHASE I), DÉBUT D'IPSEC (NÉGOCIATION DE PHASE II)		
	Échange rapide de mode ISAKMP:(1002):beginning, MI de 3464373979 Le demandeur ISAKMP:(1002):QM obtient le spi **ISAKMP:(1002) : envoyant le paquet au peer_port 500 (i) QM_IDLE du my_port 500 de 172.16.10.1** ISAKMP:(1002):sending un paquet d'ipv4 d'IKE. ISAKMP:(1002):Node 3464373979, entrée = IKE_MESG_INTERNAL, IKE_INIT_QM **État ISAKMP:(1002):Old = état IKE_QM_READY nouvel = IKE_QM_I_QM1** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE État ISAKMP:(1002):Old = état IKE_P1_COMPLETE nouvel = IKE_P1_COMPLETE	Les débuts rapides d'échange de mode (II, IPSec) et le rai env le premier message C hub.
Le hub reçoit le premier	**ISAKMP (1002) : paquet reçu du sport 500 (r)**	

paquet rapide du mode (QM) qui a la proposition d'IPSec. Les attributs reçus spécifient cela : les encaps signalent le positionnement à 2 (le mode de transport, indicateur de 1 serait tunnel mode), la vie par défaut SA de 3600 secondes et de 4608000 kilo-octets (0x465000 dans l'hexa), le HMAC-SHA pour l'authentification, et le 3DES pour le cryptage. Car ce sont les mêmes attributs réglés en configuration locale, la proposition est reçue et le shell d'IPSec SA est créé. Puisqu'aucune valeur de l'index de paramètre de Sécurité (SPI) n'est associée avec ces derniers encore, c'est juste un shell de SA qui ne peut pas être utilisée pour passer le trafic encore.	**QM_IDLE global du dport 500 de 172.16.1.1** **ISAKMP : placez le nouveau noeud -830593317 à QM_IDLE** ISAKMP:(1002) : charge utile de processing HASH. ID de message = 3464373979 ISAKMP:(1002) : traitement de la charge utile SA. ID de message = 3464373979 **Proposition 1 ISAKMP:(1002):Checking IPSec** **ISAKMP : transformez 1, ESP_3DES** **ISAKMP : les attributs transforment dedans :** **ISAKMP : les encaps est 2 (le transport)** **ISAKMP : Type de vie SA en quelques secondes** **ISAKMP : Durée de vie SA (de base) de 3600** **ISAKMP : Type de vie SA dans les kilo-octets** **ISAKMP : Durée de vie SA (VPI) de 0x0 0x46 0x50 0x0** **ISAKMP : l'authentificateur est HMAC-SHA** **ISAKMP:(1002):atts sont acceptables.** IPSEC(validate_proposal_request) : pièce proposée #1 IPSEC(validate_proposal_request) : pièce proposée #1, **(msg principaux de l'Eng.) local= D'ARRIVÉE 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),** **l'ESP de protocol=, transform= AUCUN (transport),** **lifedur= 0s et 0kb,** **spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0**	
Ce sont juste des messages de service du Général IPSec qui indiquent que cela fonctionne correctement.	IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : la consultation de connexion a renvoyé 0 IPSEC-IFC MGRE/Tu0 : crypto_ss_listen_start écoutant déjà **IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : Ouvrir un socket avec le profil DMVPN-IPSEC** IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : la consultation de connexion a renvoyé 0 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : Déclenchant le tunnel immédiatement. IPSEC-IFC MGRE/Tu0 : Ajouter l'interface de tunnel Tunnel0 à la liste partagée IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : tunnel_protection_start_pending_timer 8C93888 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : Bon écoutent la demande	
la Pseudo-crypto entrée de mappage est créée pour le protocole 47 (GRE) IP de 172.16.10.1 (annonce publique de hub) à 172.16.1.1 (annonce	l'insertion de la carte dans le mapdb AVL a manqué, des paires de carte + d'as existe déjà sur le mapdb CRYPTO_SS (SEC DE TUNNEL) : Passif ouvert, les informations de socket : gens du pays 172.16.10.1 172.16.10.1/255.255.255.255/0, 172.16.1.1 distant 172.16.1.1/255.255.255.255/0, protocole 47, ifc Tu0	

publique de rai). Un IPSec SA/SPI est créé pour chacun des deux le trafic en entrée et en sortie avec des valeurs de la proposition reçue.	Crypto mapdb : proxy_match **adr de src : 172.16.10.1** **adr de dst : 172.16.1.1** **protocole : 47** port de src : 0 port de dst : 0 ISAKMP:(1002) : charge utile de processing NONCE. ID de message = 3464373979 ISAKMP:(1002) : charge utile d'IDENTIFICATEUR DE PROCESSUS. ID de message = 3464373979 ISAKMP:(1002) : charge utile d'IDENTIFICATEUR DE PROCESSUS. ID de message = 3464373979 Le responder ISAKMP:(1002):QM obtient le spi ISAKMP:(1002):Node 3464373979, entrée = IKE_MESG_FROM_PEER, IKE_QM_EXCH **État ISAKMP:(1002):Old = état IKE_QM_READY nouvel = IKE_QM_SPI_STARVE** **ISAKMP:(1002) : Création d'IPSec SAS** **SA d'arrivée 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 le spi 0xDD2AC2B3 et le conn_id 0** **vie de 3600 secondes** **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 le spi 0x82C3E0C4 et le conn_id 0** **vie de 3600 secondes** **vie de 4608000 kilo-octets**	
Le deuxième message QM envoyé par le hub. Le message généré par le service d'IPSec qui confirme ce tunnel protection est en hausse sur Tunnel0. On voit un autre message de création SA qui a la destination IPS, SPI, attributs de jeu de transformations, et vie dans rester de kilo-octets et de secondes.	**ISAKMP:(1002) : envoyant le paquet au peer_port 500 (r) QM_IDLE du my_port 500 de 172.16.1.1** ISAKMP:(1002):sending un paquet d'ipv4 d'IKE. ISAKMP:(1002):Node 3464373979, entrée = IKE_MESG_INTERNAL, IKE_GOT_SPI **État ISAKMP:(1002):Old = état IKE_QM_SPI_STARVE nouvel = IKE_QM_R_QM2** CRYPTO_SS (SEC DE TUNNEL) : Attache Completed d'application au socket IPSEC(key_engine) : a obtenu un événement de file d'attente avec 1 message KMI Crypto mapdb : proxy_match adr de src : 172.16.10.1 adr de dst : 172.16.1.1 protocole : 47 port de src : 0 port de dst : 0 IPSEC(crypto_ipsec_sa_find_ident_head) : rebranchement avec les mêmes proxys et pair 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 créée,**	

	sa_dest= (SA) 172.16.10.1, sa_proto= 50, sa_spi= 0xDD2AC2B3(3710567091), ESP-SHA-hmac du sa_trans= esp-3des, sa_conn_id= 3 sa_lifetime (k/sec) = (4536779/3600) **IPSEC(create_sa) : SA créée,** sa_dest= (SA) 172.16.1.1, sa_proto= 50, sa_spi= 0x82C3E0C4(2193875140), ESP-SHA-hmac du sa_trans= esp-3des, sa_conn_id= 4 sa_lifetime (k/sec) = (4536779/3600) IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce) : mise à jour Tunnel0 de l'ident 8B6A0E8 avec le tun_decap_oce 6A648F0 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : connexion 8C93888 retourné par consultation IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : message prêt de bon socket IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : connexion 8C93888 retourné par consultation **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 du NHRP IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : Mtu obtenu 1458 de message de MTU IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : connexion 8C93888 retourné par consultation	
	ISAKMP (1002) : paquet reçu du sport 500 (i) QM_IDLE global du dport 500 de 172.16.10.1 ISAKMP:(1002) : charge utile de processing HASH. ID de message = 3464373979 ISAKMP:(1002) : traitement de la charge utile SA. ID de message = 3464373979 **Proposition 1 ISAKMP:(1002):Checking IPSec ISAKMP : transformez 1, ESP_3DES** **ISAKMP : les attributs transforment dedans :** **ISAKMP : les encaps est 2 (le transport)** **ISAKMP : Type de vie SA en quelques secondes** **ISAKMP : Durée de vie SA (de base) de 3600** **ISAKMP : Type de vie SA dans les kilo-octets** **ISAKMP : Durée de vie SA (VPI) de 0x0 0x46 0x50 0x0** **ISAKMP : l'authentificateur est HMAC-SHA** **ISAKMP:(1002):atts sont acceptables.** IPSEC(validate_proposal_request) : pièce proposée #1 IPSEC(validate_proposal_request) : pièce proposée #1, **(msg principaux de l'Eng.) local= D'ARRIVÉE 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),**	Le rai reçoit le deuxiè paquet QM qui a la proposition d'IPSec. C confirme que QM1 a reçu par le hub. Les attributs reçus spécifi cela : les encaps sign le positionnement à 2 mode de transport, indicateur de 1 serait mode), la vie par défa de 3600 secondes et 4608000 kilo-octets (0x465000 dans l'hex HMAC-SHA pour l'authentification, et le pour le cryptage. Car sont les mêmes attrib réglés en configuratio locale, la proposition reçue et le shell d'IPS est créé. Puisqu'aucu valeur de l'index de paramètre de Sécurit (SPI) n'est associée a

	remote_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1), **l'ESP de protocol=, transform= AUCUN (transport),** **lifedur= 0s et 0kb,** **spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0** **Crypto mapdb : proxy_match** **adr de src : 172.16.1.1** **adr de dst : 172.16.10.1** **protocole : 47** **port de src : 0** **port de dst : 0**	ces derniers encore, juste un shell de SA peut pas être utilisée passer le trafic encor La pseudo-crypto ent mappage est créée p protocole 47 (GRE) I 172.16.10.1 (annonce publique de hub) à 172.16.1.1 (annonce publique de rai).
	ISAKMP:(1002) : charge utile de processing NONCE. ID de message = 3464373979 ISAKMP:(1002) : charge utile d'IDENTIFICATEUR DE PROCESSUS. ID de message = 3464373979 ISAKMP:(1002) : charge utile d'IDENTIFICATEUR DE PROCESSUS. ID de message = 3464373979 **ISAKMP:(1002) : Création d'IPSec SAS** **SA d'arrivée 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 le spi 0x82C3E0C4 et le conn_id 0** **vie de 3600 secondes** **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 le spi 0xDD2AC2B3 et le conn_id 0** **vie de 3600 secondes** **vie de 4608000 kilo-octets**	Un IPSec SA/SPI est pour chacun des deu trafic en entrée et en avec des valeurs de l proposition reçue.
	ISAKMP:(1002) : envoyant le paquet au peer_port 500 (i) QM_IDLE du my_port 500 de 172.16.10.1 ISAKMP:(1002):sending un paquet d'ipv4 d'IKE. Raison FAUSSE d'erreur du noeud -830593317 ISAKMP:(1002):deleting « aucune erreur » ISAKMP:(1002):Node 3464373979, entrée = IKE_MESG_FROM_PEER, IKE_QM_EXCH **État ISAKMP:(1002):Old = nouvel état IKE_QM_I_QM1 = IKE_QM_PHASE2_COMPLETE** IPSEC(key_engine) : a obtenu un événement de file d'attente avec 1 message KMI Crypto mapdb : proxy_match adr de src : 172.16.1.1 adr de dst : 172.16.10.1 protocole : 47 port de src : 0 port de dst : 0 IPSEC(crypto_ipsec_sa_find_ident_head) : rebranchement avec les mêmes proxys et pair 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 créée,** sa_dest= (SA) 172.16.1.1, sa_proto= 50,	Le rai envoie le troisi final message QM au qui se termine l'échan QM. À la différence d l'ISAKMP où chaque passe par chaque éta (MM1 par MM6/P1_COMPLETE IPSec est un peu tou différent qu'il y a seul trois messages plutôt six. Le demandeur (n parlé dans ce cas, co signifié par « me » da message IKE_QM_I_ va de QM_READY, p QM_I_QM1 directeme QM_PHASE2_COMP Le responder (hub) v QM_READY, QM_SPI_STARVE, QM_R_QM2, QM_PHASE2_COMP On voit un autre mes de création SA qui a

	sa_spi= 0x82C3E0C4(2193875140), ESP-SHA-hmac du sa_trans= esp-3des, sa_conn_id= 3 sa_lifetime (k/sec) = (4499172/3600) **IPSEC(create_sa) : SA créée,** sa_dest= (SA) 172.16.10.1, sa_proto= 50, sa_spi= 0xDD2AC2B3(3710567091), ESP-SHA-hmac du sa_trans= esp-3des, sa_conn_id= 4 sa_lifetime (k/sec) = (4499172/3600) **IPSEC(update_current_outbound_sa) : obtenez SA sortante en cours de 172.16.10.1 de pair d'enable SA à SPI DD2AC2B3** **IPSEC(update_current_outbound_sa) : SA sortante en cours de 172.16.10.1 de pair mis à jour à SPI DD2AC2B3** IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce) : mise à jour Tunnel0 de l'ident 94F2740 avec le tun_decap_oce 794ED30 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : connexion 961D220 retourné par consultation 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 du NHRP NHRP : Le vrf de NHS 10.1.1.254 Tunnel0 0 priorités 0 de la batterie 0 Transitioned à « E » de '' IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : connexion 961D220 retourné par consultation NHRP : Tenter pour envoyer le paquet par l'intermédiaire de DEST 10.1.1.254	destination IPS, SPI, attributs de jeu de transformations, et vi rester de kilo-octets e secondes.
Ces messages de la finale QM confirment que le mode rapide est complet et IPSec est des deux côtés du tunnel. Àla différence de l'ISAKMP où chaque pair passe par chaque état (MM1 par MM6/P1_COMPLETE), IPSec est un peu tout différent qu'il y a seulement trois messages plutôt que six. Le responder (notre hub dans ce cas, comme signifié par le « R » dans le message IKE_QM_R_QM1) va QM_READY, QM_SPI_STARVE, QM_R_QM2, QM_PHASE2_COMPLETE. Le demandeur (rai) va de	**ISAKMP (1002) : paquet reçu du sport 500 (r) QM_IDLE global du dport 500 de 172.16.1.1** Raison FAUSSE « QM d'erreur du noeud -830593317 ISAKMP:(1002):deleting faite (attendez) » ISAKMP:(1002):Node 3464373979, entrée = IKE_MESG_FROM_PEER, IKE_QM_EXCH **État ISAKMP:(1002):Old = nouvel état IKE_QM_R_QM2 = IKE_QM_PHASE2_COMPLETE** IPSEC(key_engine) : a obtenu un événement de file d'attente avec 1 message KMI IPSEC(key_engine_enable_outbound) : l'enable de rec'd annoncent de l'ISAKMP **IPSEC(key_engine_enable_outbound) : enable SA avec le spi 2193875140/50** **IPSEC(update_current_outbound_sa) : obtenez SA sortante en cours de 172.16.1.1 de pair d'enable SA à SPI 82C3E0C4** **IPSEC(update_current_outbound_sa) : SA sortante en cours de 172.16.1.1 de pair mis à jour à SPI 82C3E0C4**	

QM_READY, puis à QM_I_QM1 directement à QM_PHASE2_COMPLETE.		
	NHRP : Envoyez la demande d'enregistrement par l'intermédiaire Tunnel0 du vrf 0, longueur de paquet : 108 **src : 10.1.1.1, dst : 10.1.1.254** (f) afn : IPv4(1), type : IP(800), saut : 255, ver : 1 shtl : 4(NSAP), sstl : 0(NSAP) pktsz : extoff 108 : 52 (m) indicateurs : « seul nat », reqid : 65540 **src NBMA : 172.16.1.1** **protocole de src : 10.1.1.1, protocole de dst : 10.1.1.254** Code (C-1) : aucun error(0) préfixe : 32, mtu : 17912, hd_time : 7200 addr_len : 0(NSAP), subaddr_len : 0(NSAP), proto_len : 0, de préférence : 0 Adresse de responder Extension(3) : Enregistrement en avant de NHS de transit Extension(4) : Renversez l'enregistrement de NHS de transit Extension(5) : **Authentification Extension(7) :** **type:Cleartext(1), données : NHRPAUTH** Adresse NAT Extension(9) : Code (C-1) : aucun error(0) préfixe : 32, mtu : 17912, hd_time : 0 addr_len : 4(NSAP), subaddr_len : 0(NSAP), proto_len : 4, de préférence : 0 **client NBMA : 172.16.10.1** **protocole de client : 10.1.1.254**	C'est les demandes d'enregistrement de N envoyées au hub dar tentative de s'enregis NHS (le hub). Il est n de voir des multiples ces derniers, car le ra continue à tenter de s'inscrire à NHS jusq qu'il reçoive une « ré d'enregistrement. » **src, dst** : Adresses IP source du tunnel (rai) destination (hub). Ce la source et la destina du paquet GRE envo le routeur **src NBMA** : l'adresse NBMA (Internet) du ra a envoyé ces paquet essais pour s'inscrire NHS **protocole de src** : per un tunnel l'adresse du qui essaye de s'enreg **protocole de dst** : adr de tunnel du NHS/hu **Extension d'authentification**, dor : Chaîne d'authentific de NHRP **client NBMA** : Adress NBMA du NHS/hub **protocole de client** : adresse de tunnel du NHS/hub
	NHRP-RATE : Envoi de la demande d'enregistrement initiale pour 10.1.1.254, reqid 65540 **%LINK-3-UPDOWN : Interface Tunnel0, état modifié à** NHRP : if_up : Tunnel0 0 proto **NHRP : Tunnel0 : Mise à jour de cache pour le prochain-saut 10.1.1.254 de la cible 10.1.1.254/32** **172.16.10.1** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : connexion 961D220 retourné par consultation NHRP : Tenter pour envoyer le paquet par l'intermédiaire de DEST 10.1.1.254	Plus de messages de service de NHRP qui indiquent la demande d'enregistrement initi été envoyés à NHS c 10.1.1.254. Il y a également une confirmation qu'une e de cache a été ajouté pour IP 10.1.1.254/24 tunnel ce des vies à N 172.16.10.1. Le mess retardé indique que le tunnel a été « aucun

		fermé » est vu ici.
	IPSEC-IFC GRE/Tu0 : monter de tunnel IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : connexion 961D220 retourné par consultation IPSEC-IFC GRE/Tu0 : crypto_ss_listen_start écoutant déjà IPSEC-IFC GRE/Tu0 : crypto_ss_listen_start écoutant déjà **IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : Ouvrir un socket avec le profil DMVPN-IPSEC** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : connexion 961D220 retourné par consultation IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1) : Le socket est déjà ouvert. Ignorer. %LINEPROTO-5-UPDOWN : Line protocol on Interface Tunnel0, état modifié à	Ce sont des message service du Général IP qui indiquent que cela fonctionne correctem Voici où on le voit finalement que le pro de tunnel est en haus
C'est les demandes d'enregistrement de NHRP reçues du rai dans la tentative de s'enregistrer à NHS (le hub). Il est normal de voir des multiples de ces derniers, car le rai continue à tenter de s'inscrire à NHS jusqu'à ce qu'il reçoive une « réponse d'enregistrement. » **src NBMA** : l'adresse NBMA (Internet) du rai qui a envoyé ces paquet et essais pour s'inscrire à NHS **protocole de src** : percez un tunnel l'adresse du rai qui essaye de s'enregistrer **protocole de dst** : adresse de tunnel du NHS/hub **Extension d'authentification**, données : Chaîne d'authentification de NHRP **client NBMA** : Adresse NBMA du NHS/hub **protocole de client** : adresse de tunnel du NHS/hub	**NHRP : Recevez la demande d'enregistrement par l'intermédiaire Tunnel0 du vrf 0, longueur de paquet : 108** (f) afn : IPv4(1), type : IP(800), saut : 255, ver : 1 shtl : 4(NSAP), sstl : 0(NSAP) pktsz : extoff 108 : 52 (m) indicateurs : « seul nat », reqid : 65540 **src NBMA : 172.16.1.1** **protocole de src : 10.1.1.1, protocole de dst : 10.1.1.254** Code (C-1) : aucun error(0) préfixe : 32, mtu : 17912, hd_time : 7200 addr_len : 0(NSAP), subaddr_len : 0(NSAP), proto_len : 0, de préférence : 0 Adresse de responder Extension(3) : Enregistrement en avant de NHS de transit Extension(4) : Renversez l'enregistrement de NHS de transit Extension(5) : **Authentification Extension(7) :** **type:Cleartext(1), données : NHRPAUTH** Adresse NAT Extension(9) : Code (C-1) : aucun error(0) préfixe : 32, mtu : 17912, hd_time : 0 addr_len : 4(NSAP), subaddr_len : 0(NSAP), proto_len : 4, de préférence : 0 **client NBMA : 172.16.10.1** **protocole de client : 10.1.1.254**	
Debugs packets de NHRP ajoutant le réseau de destination 10.1.1.1/32 disponible par l'intermédiaire du prochain saut de 10.1.1.1 au NHRP de 172.16.1.1. 172.16.1.1	NHRP : netid_in = 1, to_us = 1 **NHRP : Tunnel0 : Le cache ajoutent pour le prochain-saut 10.1.1.1 de la cible 10.1.1.1/32** **172.16.1.1** **NHRP : Ajouter les périphériques du tunnel (VPN : 10.1.1.1, NBMA : 172.16.1.1)** **NHRP : Subblock avec succès relié de NHRP pour**	

est également ajouté à la liste d'adresses aux lesquelles de hub le trafic de multidiffusion en avant. Ces messages confirment que l'enregistrement était réussi, de même qu'une résolution pour les rais percez un tunnel l'adresse.	**les périphériques du tunnel (VPN : 10.1.1.1, NBMA : 172.16.1.1)** NHRP : Noeud inséré de subblock pour le cache : Noeud de subblock inséré par cible pour le cache : Cible 10.1.1.1/32nhop 10.1.1.1 NHRP : Entrée dynamique interne convertie de cache pour 10.1.1.1/32 l'interface Tunnel0 à externe **NHRP : Tu0 : Création de la Multidiffusion dynamique traçant NBMA : 172.16.1.1** **NHRP : Mappage dynamique ajouté de Multidiffusion 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 : Tenter pour envoyer le paquet par l'intermédiaire de DEST 10.1.1.1 **NHRP : NHRP 10.1.1.1 avec succès résolu à NBMA 172.16.1.1** **NHRP : Encapsulation réussie. Adr 172.16.1.1 IP de tunnel**	
C'est la réponse d'enregistrement de NHRP envoyée par le hub au rai en réponse à la « demande d'enregistrement de NHRP » reçue plus tôt. Comme les autres paquets d'enregistrement, le hub envoie des multiples de ces derniers en réponse aux plusieurs demandes. **src, dst** : Adresses IP de source du tunnel (hub) et de destination (rai). Ce sont la source et la destination du paquet GRE envoyé par le routeur **src NBMA** : Adresse NBMA (Internet) du rai **protocole de src** : percez un tunnel l'adresse du rai qui essaye de s'enregistrer **protocole de dst** : adresse de tunnel du NHS/hub **client NBMA** : Adresse NBMA du NHS/hub **protocole de client** : adresse de tunnel du NHS/hub **Extension d'authentification**, données : Chaîne d'authentification de NHRP	**NHRP : Envoyez la réponse d'enregistrement par l'intermédiaire Tunnel0 du vrf 0, longueur de paquet : 128** **src : 10.1.1.254, dst : 10.1.1.1** (f) afn : IPv4(1), type : IP(800), saut : 255, ver : 1 shtl : 4(NSAP), sstl : 0(NSAP) pktsz : extoff 128 : 52 (m) indicateurs : « seul nat », reqid : 65540 **src NBMA : 172.16.1.1** **protocole de src : 10.1.1.1, protocole de dst : 10.1.1.254** Code (C-1) : aucun error(0) préfixe : 32, mtu : 17912, hd_time : 7200 addr_len : 0(NSAP), subaddr_len : 0(NSAP), proto_len : 0, de préférence : 0 Adresse de responder Extension(3) : (c) code : aucun error(0) préfixe : 32, mtu : 17912, hd_time : 7200 addr_len : 4(NSAP), subaddr_len : 0(NSAP), proto_len : 4, de préférence : 0 **client NBMA : 172.16.10.1** **protocole de client : 10.1.1.254** Enregistrement en avant de NHS de transit Extension(4) : Renversez l'enregistrement de NHS de transit Extension(5) : **Authentification Extension(7) :** **type:Cleartext(1), données : NHRPAUTH** Adresse NAT Extension(9) : Code (C-1) : aucun error(0) préfixe : 32, mtu : 17912, hd_time : 0 addr_len : 4(NSAP), subaddr_len : 0(NSAP), proto_len : 4, de préférence : 0	

	client NBMA : 172.16.10.1 **protocole de client : 10.1.1.254**	
	NHRP : Recevez la réponse d'enregistrement par l'intermédiaire Tunnel0 du vrf 0, longueur de paquet : 128 (f) afn : IPv4(1), type : IP(800), saut : 255, ver : 1 shtl : 4(NSAP), sstl : 0(NSAP) pktsz : extoff 128 : 52 (m) indicateurs : « seul nat », reqid : 65541 **src NBMA : 172.16.1.1** **protocole de src : 10.1.1.1, protocole de dst : 10.1.1.254** Code (C-1) : aucun error(0) préfixe : 32, mtu : 17912, hd_time : 7200 addr_len : 0(NSAP), subaddr_len : 0(NSAP), proto_len : 0, de préférence : 0 Adresse de responder Extension(3) : (c) code : aucun error(0) préfixe : 32, mtu : 17912, hd_time : 7200 addr_len : 4(NSAP), subaddr_len : 0(NSAP), proto_len : 4, de préférence : 0 **client NBMA : 172.16.10.1** **protocole de client : 10.1.1.254** Enregistrement en avant de NHS de transit Extension(4) : Renversez l'enregistrement de NHS de transit Extension(5) : **Authentification Extension(7) :** **type:Cleartext(1), données : NHRPAUTH** Adresse NAT Extension(9) : Code (C-1) : aucun error(0) préfixe : 32, mtu : 17912, hd_time : 0 addr_len : 4(NSAP), subaddr_len : 0(NSAP), proto_len : 4, de préférence : 0 **client NBMA : 172.16.10.1** **protocole de client : 10.1.1.254** NHRP : netid_in = 0, to_us = 1	C'est la réponse d'enregistrement de N envoyée par le hub a en réponse à la « der d'enregistrement de NHRP » reçue plus tô Comme les autres pa d'enregistrement, le h envoie des multiples derniers en réponse a plusieurs demandes. **src NBMA** : Adresse (Internet) du rai **protocole de src** : per un tunnel l'adresse du qui essaye de s'enreg **protocole de dst** : adr de tunnel du NHS/hu **client NBMA** : Adress NBMA du NHS/hub **protocole de client** : adresse de tunnel du NHS/hub **Extension d'authentification**, dor : Chaîne d'authentific de NHRP
Plus de messages de service du Général IPSec qui indiquent cela fonctionne correctement.	IPSEC-IFC MGRE/Tu0 : crypto_ss_listen_start écoutant déjà IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : Ouvrir un socket avec le profil DMVPN-IPSEC IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : connexion 8C93888 retourné par consultation IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : Le socket est déjà ouvert. Ignorer. IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1) : tunnel_protection_stop_pending_timer 8C93888	
	NHRP : NHS-UP : 10.1.1.254	Les messages de ser de NHRP qui indique NHS situé à 10.1.1.2 en hausse.
Le message système qui énonce que la contiguïté	%DUAL-5-NBRCHANGE : EIGRP-IPv4 1 : Le voisin 10.1.1.1 (Tunnel0) est : nouvelle contiguïté	

EIGRP est en hausse avec le voisin a parlé chez 10.1.1.1.		
	%DUAL-5-NBRCHANGE : EIGRP-IPv4 1 : Le voisin 10.1.1.254 (Tunnel0) est : nouvelle contiguïté	Le message système énonce la contiguïté EIGRP est en hausse le hub voisin chez 10.1.1.254.
Message système qui confirme une résolution réussie de NHRP.	NHRP : NHRP 10.1.1.1 avec succès résolu à NBMA 172.16.1.1	

Confirmez la fonctionnalité et la dépannez

Cette section a certaines des **commandes show** les plus utiles utilisées pour dépanner chacun des deux le hub and spoke. Afin d'activer plus de particularité met au point, utilise ces derniers mettent au point des conditionals :

- nbma *NBMA_ADDRESS de* pair de debug dmvpn condition
- tunnel *TUNNEL_ADDRESS de* pair de debug dmvpn condition
- ipv4 *NBMA_ADDRESS de* pair de debug crypto condition

shows cryptos 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"
```

petit groupe de show crypto session

```
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 encryptionIPv4 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

détail de show crypto ipsec sa

```
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
```

nhs de show ip

```
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 [détail]

```
"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 de nouvelle génération
- RFC3706 : IKE Dead Peer Detection
- RFC3947 : NAT Traversal d'IKE
- Support et documentation techniques - Cisco Systems