Guía del Troubleshooting de los debugs de la fase 1 DMVPN

Contenido

Introducción

Este documento describe los mensajes del debug que usted encontraría en el hub and spoke de un despliegue de múltiples puntos dinámico de la fase 1 de Virtual Private Network (DMVPN).

Prerequisites

Para la configuración y los comandos debug en este documento, usted necesitará a dos routeres Cisco que funcionen con la versión 12.4(9)T del ® del Cisco IOS o más adelante. Una fase básica 1 DMVPN requiere generalmente el Cisco IOS Release 12.2(13)T o Posterior o la versión 12.2(33)XNC para el router de los servicios de la agregación (ASR), aunque las características y los debugs vistos en este documento no pudieron ser soportados.

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Generic Routing Encapsulation (GRE)
- Protocolo de resolución de salto siguiente (NHRP)
- Internet Security Association and Key Management Protocol (ISAKMP)
- Internet Key Exchange (IKE)
- Seguridad de protocolos en Internet (IPSec)
- Por lo menos uno de estos Routing Protocol: Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), y Border Gateway Protocol (BGP)

Componentes Utilizados

La información en este documento se basa en Cisco 2911 Routers de los Servicios integrados (ISR) que funcionen con el Cisco IOS Release 15.1(4)M4.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Mejoras significativas

Estas versiones deL Cisco IOS introdujeron las características o los arreglos significativos para la fase 1 DMVPN:

- Versión 12.2(18)SXF5 - un mejor soporte para el ISAKMP al usar el Public Key Infrastructure (PKI)
- Versión 12.2(33)XNE - ASR, perfiles de ipsec, protección del túnel, Traversal de la traducción de la dirección (NAT) de la red IPsec
- Versión 12.3(7)T - soporte del ruteo virtual y de la expedición del interior (iVRF)
- Versión 12.3(11)T - soporte del ruteo virtual y de la expedición de la puerta frontal (fVRF)
- Versión 12.4(9)T - soporte para los diversos debugs y comandos relacionados DMVPN
- Versión 12.4(15)T - Protección compartida del túnel
- Versión 12.4(20)T - IPv6 sobre el DMVPN
- Versión el 15.0(1)M - Control de salud del túnel NHRP

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener información sobre las convenciones sobre documentos.

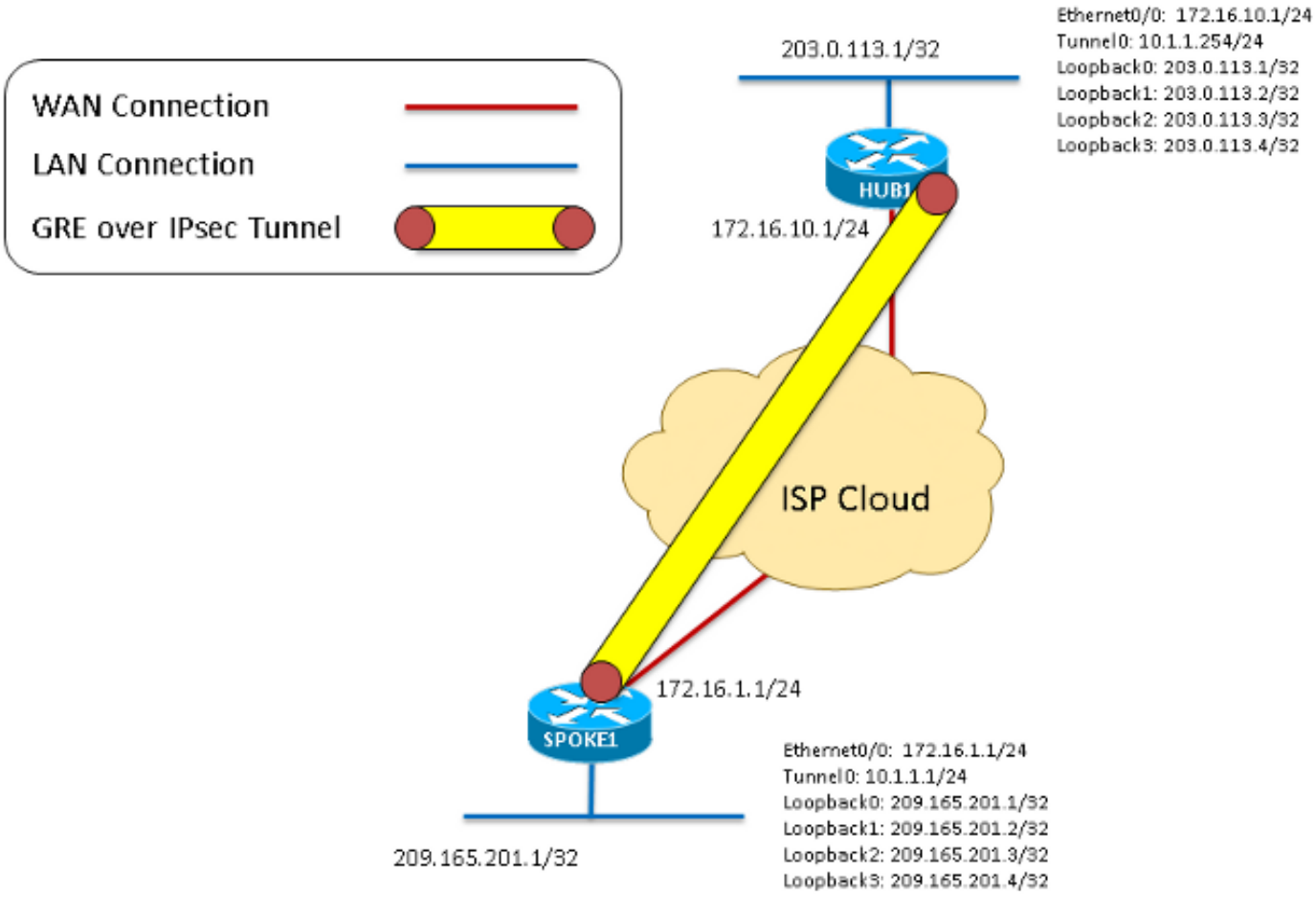
Configuración pertinente

Descripción de la topología

Para esta topología, dos 2911 ISR que se ejecutan la versión 15.1(4)M4 fueron configurados para la fase 1 DMVPN: uno como concentrador y uno como spoke. El Ethernet0/0 fue utilizado como la

interfaz de “Internet” en cada router. Las cuatro interfaces del loopback se configuran para simular las redes de área local que viven en el concentrador o el sitio radial. Pues esto es una topología de la fase 1 DMVPN con solamente una habló, el spoke se configura con un túnel GRE de punto a punto bastante que un túnel GRE de múltiples puntos. El mismo configuraton crypto (ISAKMP y IPSec) fue utilizado en cada router para asegurarlos correspondió con exactamente.

Diagrama 1



Crypto

Éste es lo mismo en el concentrador y el spoke.

```
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
```

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
```

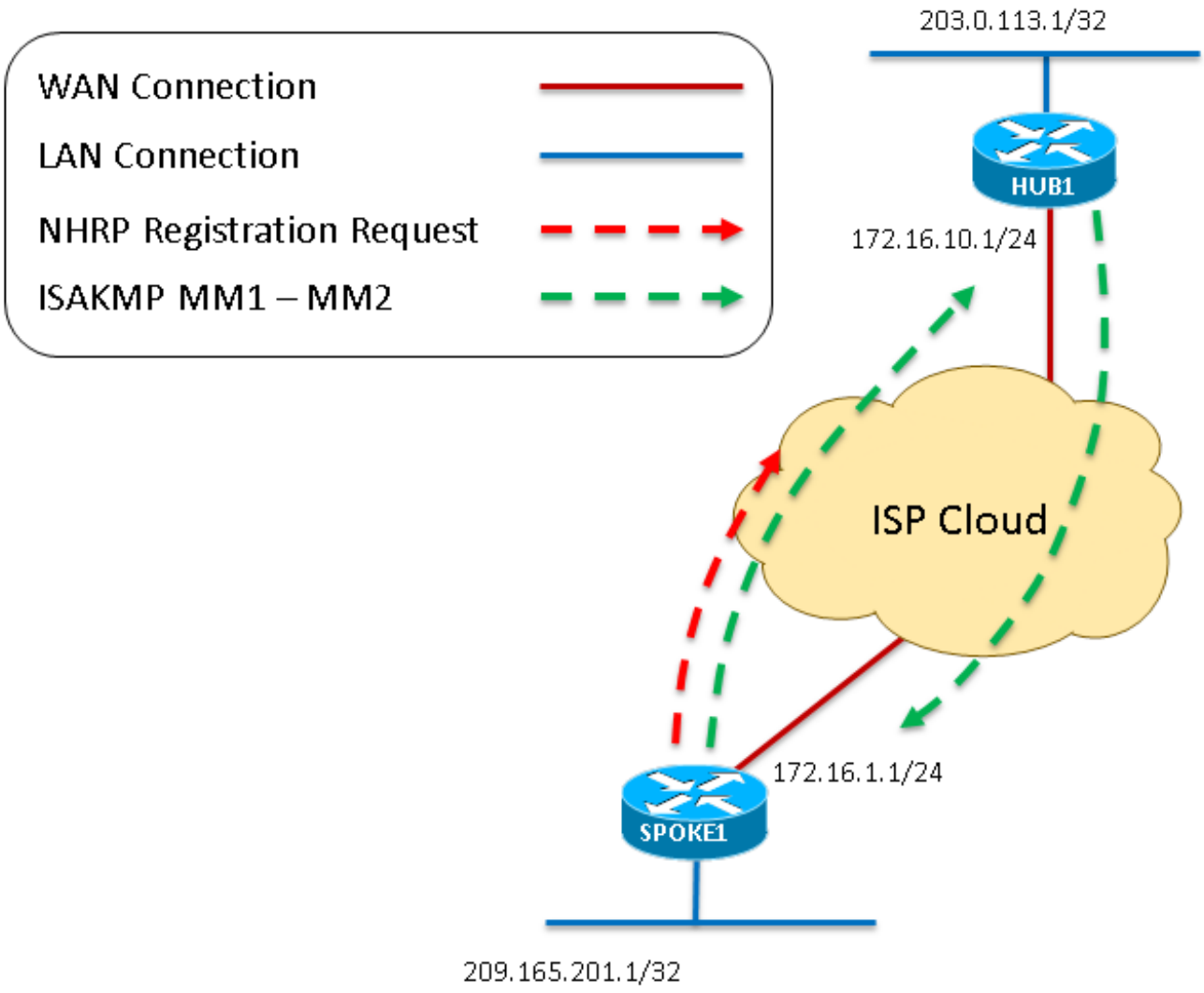
```
network 209.165.201.2 0.0.0.0
network 209.165.201.3 0.0.0.0
network 209.165.201.4 0.0.0.0
network 10.1.1.0 0.0.0.255
```

Depuraciones

Visualización de flujo de paquetes

Ésta es una visualización del flujo de paquetes entero DMVPN como se ve en este documento. Debugs más detallados que explican cada uno de los pasos también se incluyen.

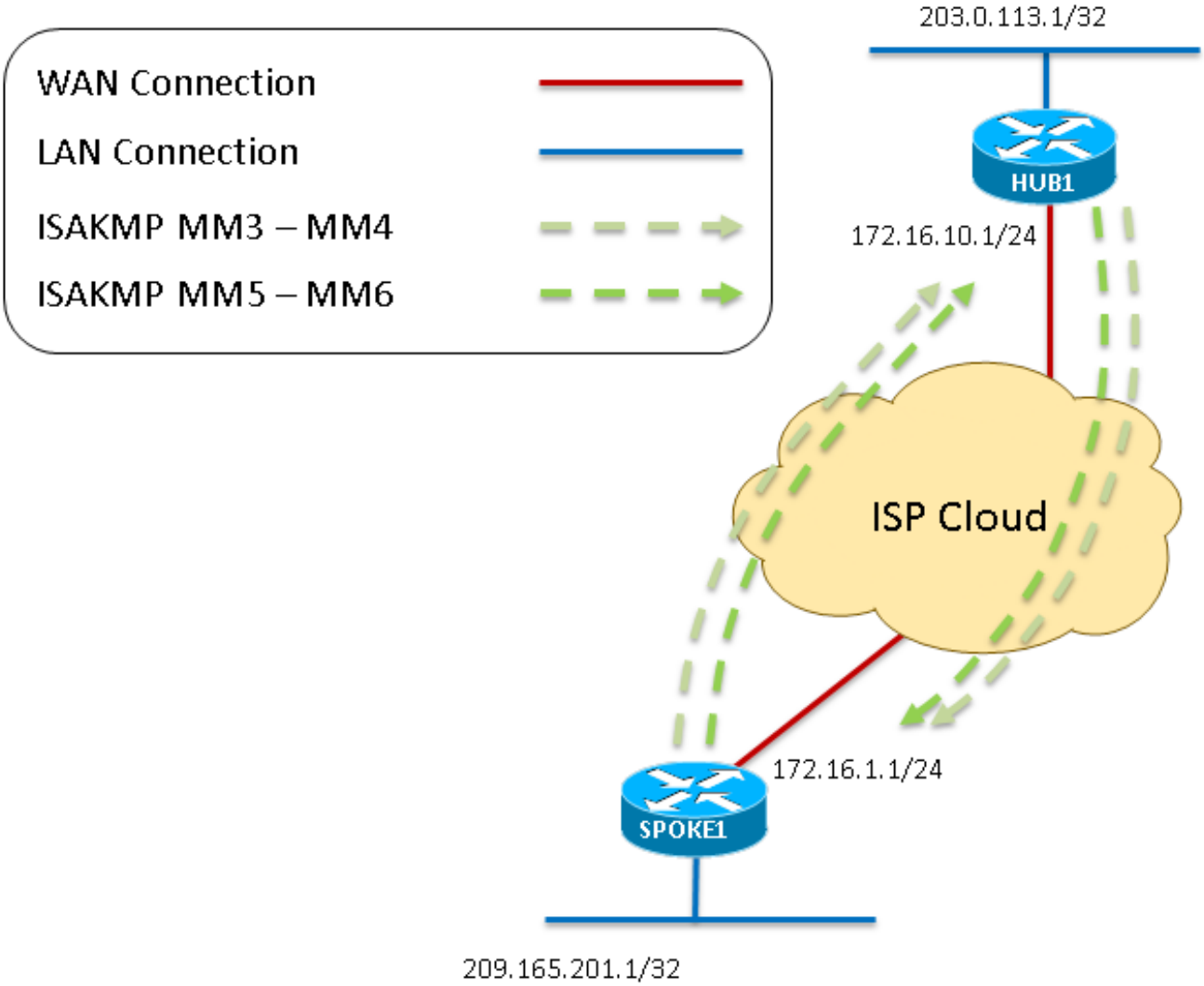
1. Cuando el túnel en el spoke es “ningún apaguelo” genera un pedido de inscripción NHRP, que comienza el proceso DMVPN. Pues la configuración del concentrador es totalmente dinámica, el spoke debe ser el punto final que inicia la conexión.
2. El pedido de inscripción NHRP entonces se encapsula en el GRE que acciona el proceso criptográfico para comenzar.
3. En este momento, el primer modo principal ISAKMP que el mensaje – ISAKMP MM1 – se envía del habló al concentrador en el puerto UDP500.
4. El concentrador recibe y procesa MM1 y responde con ISAKMP MM2, pues tiene una política isakmp que corresponde con.
   El diagrama 2 - refiere a los pasos 1 a
   4



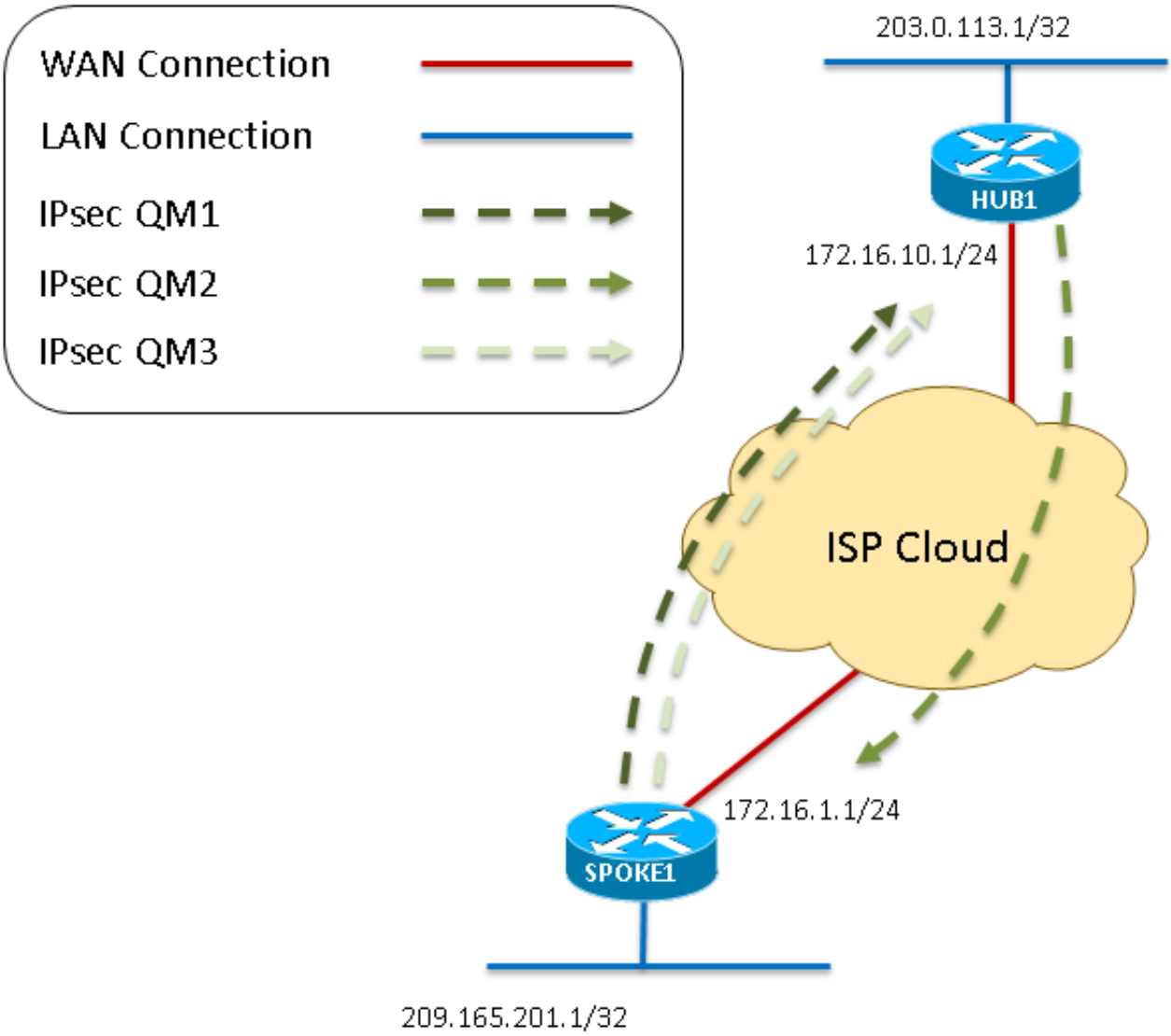
5. Una vez que el spoke recibe el MM2, responde con MM3. Como con MM1, el spoke

confirma la política isakmp recibida es válido.

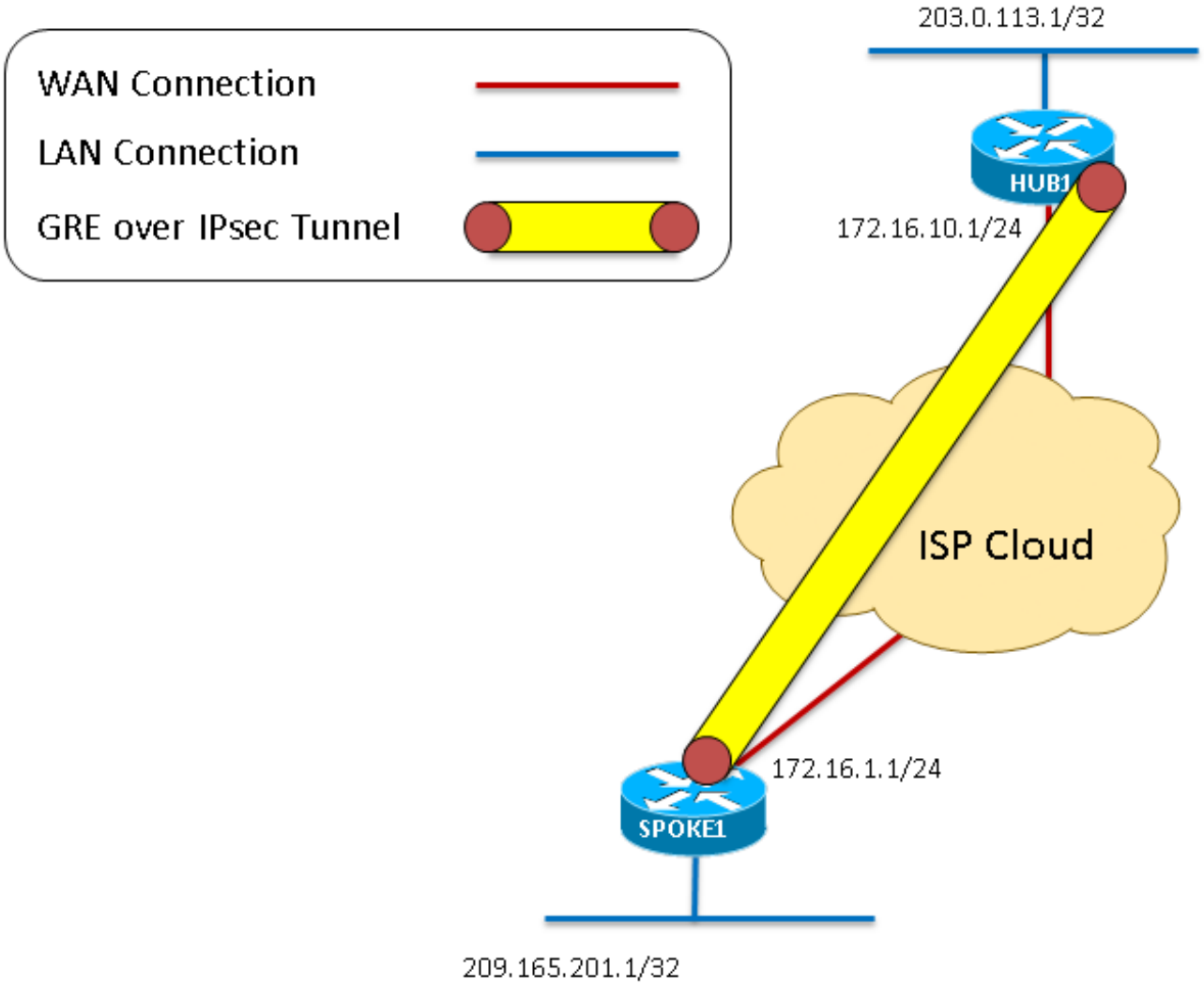
6. El concentrador recibe MM3 y responde con MM4.
7. En este momento en la negociación ISAKMP, el spoke pudo responder en el puerto UDP4500 si el NAT se detecta en el trayecto de tránsito. Sin embargo, si no se detecta ningún NAT el spoke continúa y envía MM5 en UDP500. Pasado, el concentrador responde con MM6 para completar el intercambio del modo principal.
   El diagrama 3 - refiere a los pasos 5 a 7



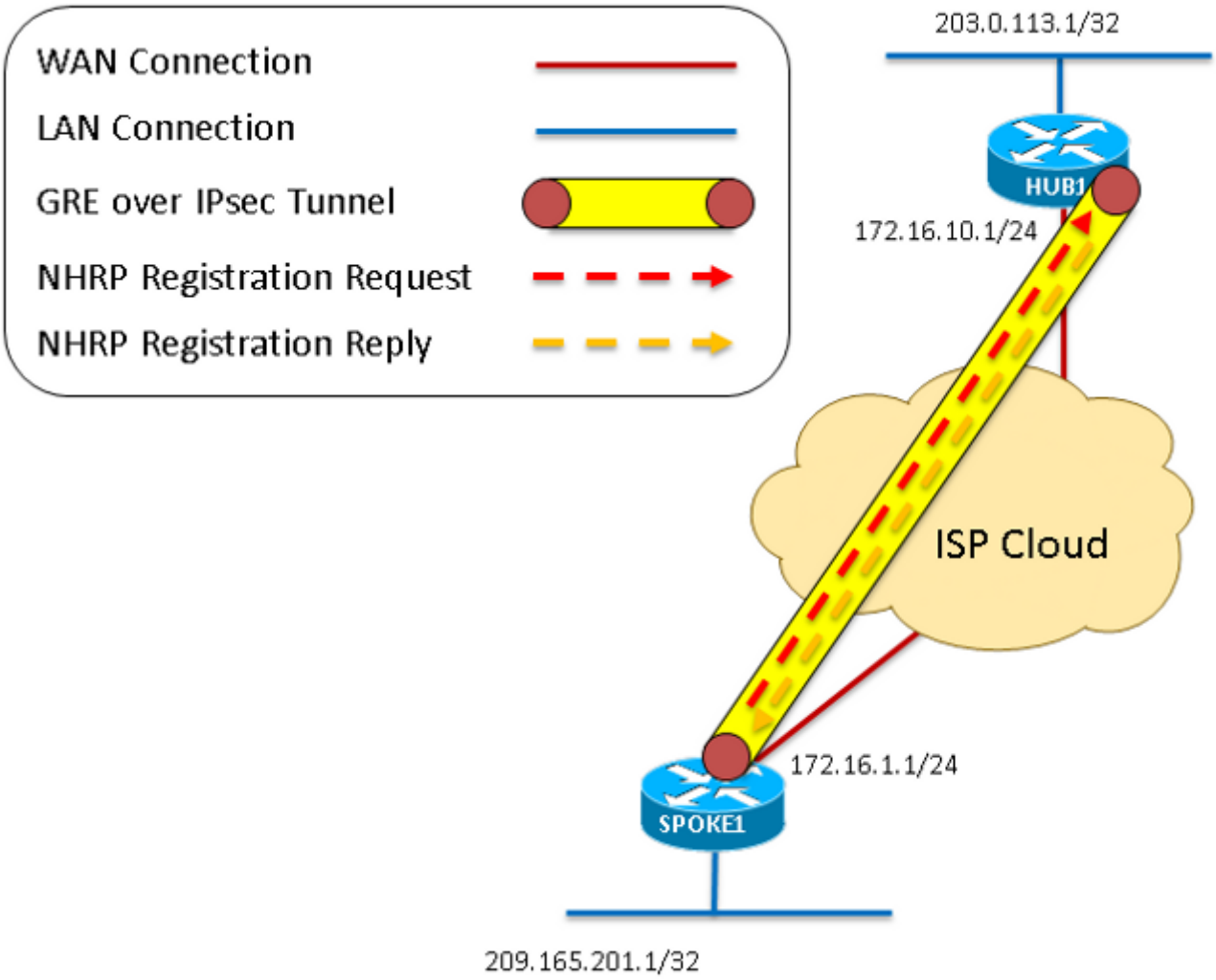
8. Una vez que el spoke recibe MM6 del concentrador, envía QM1 al concentrador en UDP500 para comenzar el Quick Mode.
9. El concentrador recibe QM1 y responde con QM2, como se validan todos los atributos recibidos. En este momento el concentrador crea la fase 2 SA para esta sesión.
10. Como el paso más reciente de la negociación del Quick Mode, QM2 es recibido por el spoke. El spoke después crea su fase 2 SA y envía QM3 en la respuesta. Esto completa el ISAKMP y el IPSec Negotiation. Ahora hay sesión IPSec que cifra el tráfico GRE entre estos dos pares.
    El diagrama 4 - refiere a los pasos 8 a 10



11. Ahora que la sesión de criptografía puede ascendente y pasar el tráfico, estos paquetes se encapsulan dentro del túnel del GRE sobre IPSec.
    El diagrama 5 - refiere al paso
    11



12. Como fue visto en los primeros pasos, el spoke genera un pedido de inscripción NHRP que se envíe a través del túnel del GRE sobre IPSec.
13. El concentrador recibe los pedidos de inscripción NHRP y envía una contestación del registro NHRP una vez que confirma el spoke tiene un direccionamiento válido del túnel y del acceso múltiple sin broadcast (NBMA). El spoke recibe esta contestación del registro NHRP que complete el proceso de inscripción.
    El diagrama 6 - refiere a los pasos 12 a
    13



Estos debugs son el resultado cuando el **dmvpn del debug todo el comando all** se ingresa en el Routers del hub and spoke. Este comando determinado habilita este conjunto de los debugs:

```
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 con la explicación

Pues esto es un configuraton donde se implementa el IPSec, la demostración de los debugs todo el ISAKMP y debugs del IPSec. Si no es crypto se configura, ignoran cualquier debug que comience con el “IPSec” o el “ISAKMP.”

EXPLICACIÓN DEL DEBUG DEL CONCENTRADOR	DEBUGS EN ORDEN	EXPLICACIÓN D DEBUG DEL SPO
Estos primeros mensajes del debug son generados por un **comando no shutdown** ingresado en la interfaz del túnel. Los mensajes son generados por los servicios crypto, GRE, y NHRP que son iniciados. Un error de inscripción NHRP se considera en el concentrador porque no hace un Next Hop Server (NHS) configurar (el concentrador es el NHS para nuestra nube DMVPN). Se espera esto.	IPSEC-IFC MGRE/Tu0: Marcar el estado del túnel. **NHRP: if_up: Tunnel0 0 proto** IPSEC-IFC MGRE/Tu0: túnel que sube IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start que escucha ya **%CRYPTO-6-ISAKMP_ON_OFF: El ISAKMP está PRENDIDO** **NHRP: Incapaz de enviar el registro - ningún NHSes configuró** %LINK-3-UPDOWN: Tunnel0 de la interfaz, estado cambiado a para arriba NHRP: if_up: Tunnel0 0 proto NHRP: Incapaz de enviar el registro - ningún NHSes configuró IPSEC-IFC MGRE/Tu0: túnel que sube IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start que escucha ya **%LINEPROTO-5-UPDOWN: Line Protocol en el tunnel0 de la interfaz, estado cambiado a para arriba** IPSEC-IFC GRE/Tu0: Marcar el estado del túnel. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): las operaciones de búsqueda de la conexión volvieron 0 **IPSEC-IFC GRE/Tu0: crypto_ss_listen_start que escucha ya** **IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Apertura de un socket con el perfil DMVPN-IPSEC** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): las operaciones de búsqueda de la conexión volvieron 0 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Accionando el túnel inmediatamente. IPSEC-IFC GRE/Tu0: Agregar la interfaz del túnel del tunnel0 a la lista compartida **NHRP: if_up: Tunnel0 0 proto** **NHRP: Tunnel0: El caché agrega para el Next-Hop 10.1.1.254 de la blanco 10.1.1.254/32**	Estos primeros mens del debug son genera por un **comando no shutdown** ingresado interfaz del túnel. Los mensajes son genera por los servicios cryp GRE, y NHRP se inic que. Además, el spoke ag una entrada a su pro caché NHRP para su propio direccionamie NBMA y del túnel.

172.16.10.1
IPSEC-IFC GRE/Tu0: túnel que sube
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): conexión 961D220 vuelto operaciones de búsqueda
IPSEC-IFC GRE/Tu0: crypto_ss_listen_start que escucha ya
IPSEC-IFC GRE/Tu0: crypto_ss_listen_start que escucha ya
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Apertura de un socket con el perfil DMVPN-IPSEC
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): conexión 961D220 vuelto operaciones de búsqueda
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): El socket se está abriendo ya. Negligencia.
CRYPTO_SS (TÚNEL SEC): La aplicación comenzó a escuchar
el separador de millares de la correspondencia en el mapdb AVL fallado, los pares de la correspondencia + del as existe ya en el mapdb
%CRYPTO-6-ISAKMP_ON_OFF: El ISAKMP está PRENDIDO
CRYPTO_SS (TÚNEL SEC): Active abierto, información del socket: 172.16.1.1 local 172.16.1.1/255.255.255.255/0, 172.16.10.1 remoto 172.16.10.1/255.255.255.255/0, prot 47, ifc Tu0
COMIENZO DE LA NEGOCIACIÓN ISAKMP (FASE I)
IPSEC(recalculate_mtu): reajuste el MTU del sadb_root 94EFDC0 a 1500
IPSEC(sa_request): ,
(inglés dominante. local= SALIENTE 172.16.1.1:500 de los msg.), 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, esp-sha-hmac del esp-3des del transform= (transporte),
lifedur= 3600s y 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
ISAKMP:(0): El perfil de la petición SA es (la FALTA DE INFORMACIÓN)
ISAKMP: Creó un struct del par para 172.16.10.1, el puerto de peer 500
ISAKMP: El nuevo par creó el par = el peer_handle 0x95F6858 = 0x80000004
ISAKMP: Bloquear el struct 0x95F6858 del par, refcount 1 para el isakmp_initiator
ISAKMP: puerto local 500, puerto remoto 500
ISAKMP: fije el nuevo nodo 0 al QM_IDLE
ISAKMP:(0):insert sa con éxito sa = 8A26FB0
Modo agresivo del comienzo ISAKMP:(0):Can no, modo principal que intenta.
Clave previamente compartida del par

El primer paso una ve
el túnel es “ningún ap
es comenzar la
negociación crypto. A
spoke crea una petici
SA, intenta comenzar
modo agresivo y falla
nuevo al modo princi
Puesto que no config
al modo agresivo en
cualquier router, se e
esto.
El spoke comienza al
principal y envía el pr
mensaje ISAKMP,
MM_NO_STATE. Ca
de estado ISAKMP d
IKE_READY a IKE_I_
Los mensajes del Ve
ID NAT-T se utilizan
detección y el travers
NAT. Estos mensajes
esperan durante la
negociación del ISAK
sin importar
independientemente
el NAT esté impleme

	ISAKMP:(0):found que corresponde con 172.16.10.1 ISAKMP:(0): NAT-T construido vendor-rfc3947 ID ISAKMP:(0): NAT-T construido vendor-07 ID ISAKMP:(0): NAT-T construido vendor-03 ID ISAKMP:(0): NAT-T construido vendor-02 ID **ISAKMP:(0):Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM** **Estado ISAKMP:(0):Old = estado IKE_READY nuevo = IKE_I_MM1** **ISAKMP:(0): intercambio del modo principal que comienza** **ISAKMP:(0): enviando el paquete al peer_port del my_port 500 de 172.16.10.1 500 (i) MM_NO_STATE** ISAKMP:(0):Sending un IKE paquete IPV4. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): conexión 961D220 vuelto operaciones de búsqueda IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): mensaje listo del buen socket
Después de que el túnel del rayo sea “ningún apague,” el concentrador recibe el IKE NUEVO SA (mensaje del modo principal 1) en el puerto 500. Como el respondedor, el concentrador crea una asociación de seguridad ISAKMP (SA). Los cambios de estado ISAKMP de IKE_READY a IKE_R_MM1.	**ISAKMP (0): paquete recibido del deporte 500 (n) NUEVO SA global del dport 500 de 172.16.1.1** **ISAKMP: Creó un struct del par para 172.16.1.1, el puerto de peer 500** ISAKMP: El nuevo par creó el par = el peer_handle 0x8CACD00 = 0x80000003 ISAKMP: Bloquear el struct 0x8CACD00 del par, refcount 1 para el crypto_isakmp_process_block ISAKMP: puerto local 500, puerto remoto 500 **ISAKMP:(0):insert sa con éxito sa = 6A5BDE8** ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **Estado ISAKMP:(0):Old = estado IKE_READY nuevo = IKE_R_MM1**
Se procesa el mensaje recibido del modo principal 1 IKE. El concentrador determina que el par tiene atributos ISAKMP que corresponden con y están llenados en ISAKMP SA que acaba de ser creado. Los mensajes muestran que el par utiliza 3DES-CBC para el cifrado, desmenuzar del SHA, el group1 del Diffie Hellman (DH), la clave del preshared para la autenticación, y el curso de la vida valor por defecto SA de 86400 segundos (0x0 0x1 0x51 0x80 = 0x15180 = 86400 segundos).	ISAKMP:(0): proceso del payload SA. ID del mensaje = 0 ISAKMP:(0): proceso del payload del Vendor ID **ISAKMP:(0): el Vendor ID parece discordancía Unity/DPD pero del comandante 69** **ISAKMP (0): el Vendor ID es RFC 3947 NAT-T** ISAKMP:(0): proceso del payload del Vendor ID ISAKMP:(0): el Vendor ID parece discordancía Unity/DPD pero del comandante 245 ISAKMP (0): el Vendor ID es NAT-T v7 ISAKMP:(0): proceso del payload del Vendor ID ISAKMP:(0): el Vendor ID parece discordancía Unity/DPD pero del comandante 157 ISAKMP:(0): el Vendor ID es v3 NAT-T ISAKMP:(0): proceso del payload del Vendor ID ISAKMP:(0): el Vendor ID parece discordancía Unity/DPD pero del comandante 123 ISAKMP:(0): el Vendor ID es v2 NAT-T **Clave previamente compartida del par** **ISAKMP:(0):found que corresponde con 172.16.1.1**

Como los mensajes d
modo agresivo, se es
éstos.

El estado ISAKMP sigue siendo IKE_R_MM1 puesto que una contestación tiene no ser enviada al spoke. Los mensajes del Vendor ID NAT-T se utilizan en la detección y el traversal del NAT. Estos mensajes se esperan durante la negociación del ISAKMP sin importar independientemente de si el NAT esté implementado. Los mensajes similares se consideran para el Dead Peer Detection (DPD).

ISAKMP:(0): clave local del preshared encontrada
ISAKMP: Analizando los perfiles para el Xauth…
ISAKMP:(0):Checking ISAKMP transforman 1 contra la directiva de la prioridad 1
ISAKMP: cifrado 3DES-CBC
ISAKMP: hash SHA
ISAKMP: grupo predeterminado 1
ISAKMP: PRE-parte del auth
ISAKMP: la vida teclea adentro los segundos
ISAKMP: duración de la vida (VPI) de 0x0 0x1 0x51 0x80
ISAKMP:(0):atts son aceptables. El payload siguiente es 0
Atts ISAKMP:(0):Acceptable: vida real: 0
Atts ISAKMP:(0):Acceptable: vida: 0
Atts ISAKMP:(0):Fill en sa vpi_length:4
Atts ISAKMP:(0):Fill en sa life_in_seconds:86400
Curso de la vida real ISAKMP:(0):Returning: 86400
Temporizador del curso de la vida
ISAKMP:(0)::Started: 86400.

ISAKMP:(0): proceso del payload del Vendor ID
ISAKMP:(0): el Vendor ID parece discordancía Unity/DPD pero del comandante 69
ISAKMP (0): el Vendor ID es RFC 3947 NAT-T
ISAKMP:(0): proceso del payload del Vendor ID
ISAKMP:(0): el Vendor ID parece discordancía Unity/DPD pero del comandante 245
ISAKMP (0): el Vendor ID es NAT-T v7
ISAKMP:(0): proceso del payload del Vendor ID
ISAKMP:(0): el Vendor ID parece discordancía Unity/DPD pero del comandante 157
ISAKMP:(0): el Vendor ID es v3 NAT-T
ISAKMP:(0): proceso del payload del Vendor ID
ISAKMP:(0): el Vendor ID parece discordancía Unity/DPD pero del comandante 123
ISAKMP:(0): el Vendor ID es v2 NAT-T
ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Estado ISAKMP:(0):Old = nuevo estado IKE_R_MM1 = IKE_R_MM1

MM_SA_SETUP (envían el modo principal 2) al spoke, que confirma que MM1 fue recibido y validó como paquete ISAKMP válido. Cambios de estado ISAKMP de IKE_R_MM1 a IKE_R_MM2.

ISAKMP:(0): NAT-T construido vendor-rfc3947 ID
ISAKMP:(0): enviando el paquete al peer_port 500 (r) MM_SA_SETUP del my_port 500 de 172.16.1.1
ISAKMP:(0):Sending un IKE paquete IPV4.
ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Estado ISAKMP:(0):Old = nuevo estado IKE_R_MM1 = IKE_R_MM2
ISAKMP (0): paquete recibido del deporte del dport 500 de 172.16.10.1 500 (i) global MM_NO_STATE
ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH

En respuesta al mens
MM1 enviado al
concentrador, MM2 ll
que los confims que l

	Estado ISAKMP:(0):Old = nuevo estado IKE_I_MM1 = IKE_I_MM2 ISAKMP:(0): proceso del payload SA. ID del mensaje = 0 ISAKMP:(0): proceso del payload del Vendor ID **ISAKMP:(0): el Vendor ID parece discordancía Unity/DPD pero del comandante 69** ISAKMP (0): el Vendor ID es RFC 3947 NAT-T Clave previamente compartida del par ISAKMP:(0):found que corresponde con 172.16.10.1 ISAKMP:(0): clave local del preshared encontrada ISAKMP: Analizando los perfiles para el Xauth… **ISAKMP:(0):Checking ISAKMP transforman 1 contra la directiva de la prioridad 1** **ISAKMP: cifrado 3DES-CBC** **ISAKMP: hash SHA** **ISAKMP: grupo predeterminado 1** **ISAKMP: PRE-parte del auth** **ISAKMP: la vida teclea adentro los segundos** **ISAKMP: duración de la vida (VPI) de 0x0 0x1 0x51 0x80** **ISAKMP:(0):atts son aceptables. El payload siguiente es 0** **Atts ISAKMP:(0):Acceptable: vida real: 0** **Atts ISAKMP:(0):Acceptable: vida: 0** **Atts ISAKMP:(0):Fill en sa vpi_length:4** **Atts ISAKMP:(0):Fill en sa life_in_seconds:86400** **Curso de la vida real ISAKMP:(0):Returning: 86400** **Temporizador del curso de la vida ISAKMP:(0)::Started: 86400.** ISAKMP:(0): proceso del payload del Vendor ID ISAKMP:(0): el Vendor ID parece discordancía Unity/DPD pero del comandante 69 ISAKMP (0): el Vendor ID es RFC 3947 NAT-T ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE Estado ISAKMP:(0):Old = nuevo estado IKE_I_MM2 = IKE_I_MM2	fue recibido. Se proce mensaje recibido del principal 2 IKE. El sp realiza que el concen del par tiene atributos ISAKMP que corresp con y estos atributos llenados en ISAKMP que fue creado. Este paquete muestra que utiliza 3DES-CBC pa cifrado, desmenuzar SHA, el group1 del D Hellman (DH), la clav preshared para la autenticación, y el cu la vida valor por defe de 86400 segundos (0x1 0x51 0x80 = 0x1 = 86400 segundos). Además de los mens NAT-T, hay un interc a determinar si la ses utiliza el DPD. Los cambios de estad ISAKMP de IKE_I_MI IKE_I_MM2.
	ISAKMP:(0): enviando el paquete al peer_port 500 (i) MM_SA_SETUP del my_port 500 de 172.16.10.1 ISAKMP:(0):Sending un IKE paquete IPV4. ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **Estado ISAKMP:(0):Old = nuevo estado IKE_I_MM2 = IKE_I_MM3**	MM_SA_SETUP (env modo principal 3) al concentrador, que co que el spoke recibió lo quisiera proceder. Los cambios de estad ISAKMP de IKE_I_MI IKE_I_MM3.
MM_SA_SETUP (el concentrador recibe al modo principal 3). El concentrador concluye que el par es otro dispositivo	**ISAKMP (0): paquete recibido del deporte 500 (r) MM_SA_SETUP global del dport 500 de 172.16.1.1** ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **Estado ISAKMP:(0):Old = nuevo estado IKE_R_MM2**	

Cisco IOS y no se detecta ningún NAT para nosotros o nuestro par. Los cambios de estado ISAKMP de IKE_R_MM2 a IKE_R_MM3.	**= IKE_R_MM3** ISAKMP:(0): proceso del payload KE. ID del mensaje = 0 ISAKMP:(0): proceso del payload del NONCE. ID del mensaje = 0 **Clave previamente compartida del par ISAKMP:(0):found que corresponde con 172.16.1.1** ISAKMP:(1002): proceso del payload del Vendor ID ISAKMP:(1002): el Vendor ID es DPD ISAKMP:(1002): proceso del payload del Vendor ID **ISAKMP:(1002): ¡discurso a otro cuadro IOS!** ISAKMP:(1002): proceso del payload del Vendor ID ISAKMP:(1002): el Vendor ID parece discordancía Unity/DPD pero del comandante 225 ISAKMP:(1002): el Vendor ID es XAUTH ISAKMP: tipo de carga útil recibido 20 **ISAKMP (1002): El suyo no desmenuza ninguna coincidencia - este nodo fuera del NAT** ISAKMP: tipo de carga útil recibido 20 **ISAKMP (1002): Ningún NAT encontrado para el uno mismo o el par** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE Estado ISAKMP:(1002):Old = nuevo estado IKE_R_MM3 = IKE_R_MM3	
MM_KEY_EXCH (el concentrador envía el modo principal 4). Cambios de estado ISAKMP de IKE_R_MM3 a IKE_R_MM4.	**ISAKMP:(1002): enviando el paquete al peer_port del my_port 500 de 172.16.1.1 500 (r) MM_KEY_EXCH** ISAKMP:(1002):Sending un IKE paquete IPV4. ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **Estado ISAKMP:(1002):Old = nuevo estado IKE_R_MM3 = IKE_R_MM4**	
	ISAKMP (0): paquete recibido del deporte 500 (i) MM_SA_SETUP global del dport 500 de 172.16.10.1 ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **Estado ISAKMP:(0):Old = nuevo estado IKE_I_MM3 = IKE_I_MM4** ISAKMP:(0): proceso del payload KE. ID del mensaje = 0 ISAKMP:(0): proceso del payload del NONCE. ID del mensaje = 0 **Clave previamente compartida del par ISAKMP:(0):found que corresponde con 172.16.10.1** ISAKMP:(1002): proceso del payload del Vendor ID ISAKMP:(1002): el Vendor ID es Unity ISAKMP:(1002): proceso del payload del Vendor ID ISAKMP:(1002): el Vendor ID es DPD ISAKMP:(1002): proceso del payload del Vendor ID **ISAKMP:(1002): ¡discurso a otro cuadro IOS!** ISAKMP: tipo de carga útil recibido 20	MM_SA_SETUP (el s recibe al modo princi El spoke concluye qu par es otro dispositiv Cisco IOS y no se de ningún NAT para nos o nuestro par. Los cambios de esta ISAKMP de IKE_I_M IKE_I_MM4.

ISAKMP (1002): El suyo no desmenuza ninguna coincidencia - este nodo fuera del NAT
ISAKMP: tipo de carga útil recibido 20
ISAKMP (1002): Ningún NAT encontrado para el uno mismo o el par
ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Estado ISAKMP:(1002):Old = nuevo estado IKE_I_MM4 = IKE_I_MM4
Contacto inicial ISAKMP:(1002):Send
ISAKMP:(1002):SA está haciendo la autenticación de la clave previamente compartida usando el tipo ID_IPV4_ADDR identificación
ISAKMP (1002): Payload ID
siguiente-payload: 8
tipo: 1
direccionamiento: 172.16.1.1
protocolo: 17
puerto: 500
longitud: 12
Magnitud de carga útil ISAKMP:(1002):Total: 12
ISAKMP:(1002): enviando el paquete al peer_port del my_port 500 de 172.16.10.1 500 (i) MM_KEY_EXCH
ISAKMP:(1002):Sending un IKE paquete IPV4.
ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Estado ISAKMP:(1002):Old = nuevo estado IKE_I_MM4 = IKE_I_MM5

MM_KEY_EXCH (el concentrador recibe al modo principal 5).
Los cambios de estado ISAKMP de IKE_R_MM4 a IKE_R_MM5.
Además, “el *none* de las coincidencias del par de los perfiles” es considerado debido a la falta de un perfil ISAKMP. Porque éste es el caso, el ISAKMP no utiliza un perfil.

ISAKMP (1002): paquete recibido del deporte del dport 500 de 172.16.1.1 500 (r) global MM_KEY_EXCH
ISAKMP:(1002):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Estado ISAKMP:(1002):Old = nuevo estado IKE_R_MM4 = IKE_R_MM5

ISAKMP:(1002): payload identificador de proceso. ID del mensaje = 0
ISAKMP (1002): Payload ID
siguiente-payload: 8
tipo: 1
direccionamiento: 172.16.1.1
protocolo: 17
puerto: 500
longitud: 12
ISAKMP:(0):: el par hace juego el *none* de los perfiles
ISAKMP:(1002): proceso del payload del HASH. ID del mensaje = 0
ISAKMP:(1002): el proceso NOTIFICA el protocolo 1 INITIAL_CONTACT
spi 0, ID del mensaje = 0, sa = 0x6A5BDE8
Estado de autenticación ISAKMP:(1002):SA:

MM_KEY_EXCH (el s
envía el modo princip
Los cambios de esta
ISAKMP de IKE_I_M
IKE_I_MM5.

autenticado
ISAKMP:(1002):SA se ha autenticado con 172.16.1.1
Estado de autenticación ISAKMP:(1002):SA:
autenticado
ISAKMP:(1002): Contacto inicial de proceso,
traiga los SA abajo existentes de la fase 1 y 2 con el
puerto remoto remoto local 500 de 172.16.10.1
172.16.1.1
ISAKMP: Intentando insertar un par
172.16.10.1/172.16.1.1/500/, y con éxito insertado
8CACD00.
ISAKMP:(1002):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
Estado ISAKMP:(1002):Old = nuevo estado
IKE_R_MM5 = IKE_R_MM5

IPSEC(key_engine): consiguió un evento de la cola
con 1 mensaje KMI
ISAKMP:(1002):SA está haciendo la autenticación de
la clave previamente compartida usando el tipo
ID_IPV4_ADDR identificación
ISAKMP (1002): Payload ID
siguiente-payload: 8
tipo: 1
direccionamiento: 172.16.10.1
protocolo: 17
puerto: 500
longitud: 12
Magnitud de carga útil ISAKMP:(1002):Total: 12
ISAKMP:(1002): enviando el paquete al peer_port del
my_port 500 de 172.16.1.1 500 (r) MM_KEY_EXCH
ISAKMP:(1002):Sending un IKE paquete IPV4.
ISAKMP:(1002):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
Estado ISAKMP:(1002):Old = nuevo estado
IKE_R_MM5 = IKE_P1_COMPLETE

ISAKMP:(1002):Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE
Estado ISAKMP:(1002):Old =
estado IKE_P1_COMPLETE nuevo =
IKE_P1_COMPLETE
ISAKMP (1002): paquete recibido del deporte del
dport 500 de 172.16.10.1 500 (i) global
MM_KEY_EXCH
ISAKMP:(1002): payload identificador de proceso. ID
del mensaje = 0
ISAKMP (1002): Payload ID
siguiente-payload: 8
tipo: 1
direccionamiento: 172.16.10.1
protocolo: 17
puerto: 500

Del final el paquete MM_KEY_EXCH (el concentrador envía el modo principal 6). Esto completa la negociación de la fase 1 que significa este dispositivo está lista para la fase 2 (Quick Mode del IPSec).
Los cambios de estado ISAKMP de IKE_R_MM5 a IKE_P1_COMPLETE.

Del final el paquete MM_KEY_EXCH (el s
recibe al modo princi
Esto completa la
negociación de la fas
que significa este
dispositivo está lista p
fase 2 (Quick Mode d
IPSec).
Los cambios de estad
ISAKMP de IKE_I_MI

	longitud: 12 **ISAKMP:(0):: el par hace juego el *none* de los perfiles** ISAKMP:(1002): proceso del payload del HASH. ID del mensaje = 0 Estado de autenticación ISAKMP:(1002):SA: autenticado ISAKMP:(1002):SA se ha autenticado con 172.16.10.1 **ISAKMP: Intentando insertar un par 172.16.1.1/172.16.10.1/500/, y con éxito insertado 95F6858.** ISAKMP:(1002):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **Estado ISAKMP:(1002):Old = nuevo estado IKE_I_MM5 = IKE_I_MM6** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE Estado ISAKMP:(1002):Old = nuevo estado IKE_I_MM6 = IKE_I_MM6 ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **Estado ISAKMP:(1002):Old = nuevo estado IKE_I_MM6 = IKE_P1_COMPLETE**	IKE_I_MM6, y entonc inmediatamente a IKE_P1_COMPLETE Además, “el *none* d coincidencias del par perfiles” es considera debido a la falta de u ISAKMP. Porque éste caso, el ISAKMP no un perfil.
FINAL DE LA NEGOCIACIÓN ISAKMP (FASE I), COMIENZO DEL IPSEC (NEGOCIACIÓN DE LA FAS		
	Intercambio del Quick Mode **ISAKMP:(1002):beginning, MEDIADOS DE de 3464373979** El iniciador ISAKMP:(1002):QM consigue el spi **ISAKMP:(1002): envío del paquete al QM_IDLE del peer_port 500 del my_port 500 de 172.16.10.1 (i)** ISAKMP:(1002):Sending un IKE paquete IPV4. ISAKMP:(1002):Node 3464373979, entrada = IKE_MESG_INTERNAL, IKE_INIT_QM **Estado ISAKMP:(1002):Old = estado IKE_QM_READY nuevo = IKE_QM_I_QM1** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE Estado ISAKMP:(1002):Old = estado IKE_P1_COMPLETE nuevo = IKE_P1_COMPLETE	El intercambio del Qu Mode (fase II, IPSec) comienza y el spoke enviar el primer mens QM al concentrador.
El concentrador recibe el primer paquete del quick mode (QM) que tiene la propuesta IPSec. Los atributos recibidos especifican eso: indicador del encaps fijado a 2 (el modo de transporte, indicador de 1 sería modo túnel), al curso de la vida predeterminado SA de	**ISAKMP (1002): paquete recibido del QM_IDLE global del deporte 500 del dport 500 de 172.16.1.1 (r)** **ISAKMP: fije el nuevo nodo -830593317 al QM_IDLE** ISAKMP:(1002): proceso del payload del HASH. ID del mensaje = 3464373979 ISAKMP:(1002): proceso del payload SA. ID del mensaje = 3464373979 **Propuesta IPSec 1 ISAKMP:(1002):Checking ISAKMP: transforme 1, ESP_3DES** **ISAKMP: los atributos adentro transforman:**	

3600 segundos y de 4608000 kilobytes (0x465000 en el maleficio), al HMAC-SHA para la autenticación, y al 3DES para el cifrado. Pues éstos son los mismos atributos fijados en la configuración local, se valida la oferta y el shell IPSec SA se crea. Puesto que no se asocia ningunos valores del Security Parameter Index (SPI) a éstos todavía, éste es apenas un shell de un SA que no se pueda utilizar para pasar el tráfico todavía.	**ISAKMP: el encaps es 2 (el transporte)** **ISAKMP: La vida SA teclea adentro los segundos** **ISAKMP: Duración de la vida SA (básica) de 3600** **ISAKMP: La vida SA teclea adentro los kilobytes** **ISAKMP: Duración de la vida SA (VPI) de 0x0 0x46 0x50 0x0** **ISAKMP: el authenticator es HMAC-SHA** **ISAKMP:(1002):atts son aceptables.** IPSEC(validate_proposal_request): pieza #1 de la oferta IPSEC(validate_proposal_request): pieza #1 de la oferta, **(inglés dominante. local= ENTRANTE 172.16.10.1:0 de los msg.), 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, transform= NINGUNOS (transporte),** **lifedur= 0s y 0kb,** **spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0**
Éstos son apenas los mensajes de servicio IPSec generales que lo dicen trabajan correctamente.	IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): las operaciones de búsqueda de la conexión volvieron 0 IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start que escucha ya **IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Apertura de un socket con el perfil DMVPN-IPSEC** IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): las operaciones de búsqueda de la conexión volvieron 0 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Accionando el túnel inmediatamente. IPSEC-IFC MGRE/Tu0: Agregar la interfaz del túnel del tunnel0 a la lista compartida 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): Bueno escucha la petición
la entrada de mapeo Pseudo-crypto se crea para protocolo IP 47 (GRE) de 172.16.10.1 (dirección pública del concentrador) a 172.16.1.1 (dirección pública del spoke). Un IPSec SA/SPI se crea para ambos el tráfico entrante y saliente con los valores de la oferta validada.	el separador de millares de la correspondencia en el mapdb AVL fallado, los pares de la correspondencia + del as existe ya en el mapdb CRYPTO_SS (TÚNEL SEC): Voz pasiva abierta, información del socket: 172.16.10.1 local 172.16.10.1/255.255.255.255/0, 172.16.1.1 remoto 172.16.1.1/255.255.255.255/0, prot 47, ifc Tu0 Mapdb Crypto: proxy_match **addr del src: 172.16.10.1** **addr del dst: 172.16.1.1** **protocolo: 47** puerto del src: 0 puerto del dst: 0 ISAKMP:(1002): proceso del payload del NONCE. ID del mensaje = 3464373979 ISAKMP:(1002): payload identificador de proceso. ID

```
del mensaje = 3464373979
ISAKMP:(1002): payload identificador de proceso. ID
del mensaje = 3464373979
El respondedor ISAKMP:(1002):QM consigue el spi
ISAKMP:(1002):Node 3464373979, entrada =
IKE_MESG_FROM_PEER, IKE_QM_EXCH
Estado ISAKMP:(1002):Old = estado IKE_QM_READY
nuevo = IKE_QM_SPI_STARVE
ISAKMP:(1002): Crear el SA de IPSec
        SA entrante de 172.16.1.1 a 172.16.10.1 (f/i) 0 0
        (proxy 172.16.1.1 a 172.16.10.1)
        tiene el spi 0xDD2AC2B3 y conn_id 0
        curso de la vida de 3600 segundos
        curso de la vida de 4608000 kilobytes
        SA saliente de 172.16.10.1 a 172.16.1.1 (f/i) 0/0
        (proxy 172.16.10.1 a 172.16.1.1)
        tiene el spi 0x82C3E0C4 y conn_id 0
        curso de la vida de 3600 segundos
        curso de la vida de 4608000 kilobytes
ISAKMP:(1002): envío del paquete al QM_IDLE del
peer_port 500 del my_port 500 de 172.16.1.1 (r)
ISAKMP:(1002):Sending un IKE paquete IPV4.
ISAKMP:(1002):Node 3464373979, entrada =
IKE_MESG_INTERNAL, IKE_GOT_SPI
Estado ISAKMP:(1002):Old =
estado IKE_QM_SPI_STARVE nuevo =
IKE_QM_R_QM2
CRYPTO_SS (TÚNEL SEC): Atascamiento Completed
de la aplicación al socket
IPSEC(key_engine): consiguió un evento de la cola
con 1 mensaje KMI
Mapdb Crypto: proxy_match
        addr del src: 172.16.10.1
        addr del dst: 172.16.1.1
        protocolo: 47
        puerto del src: 0
        puerto del dst: 0
IPSEC(crypto_ipsec_sa_find_ident_head): el volver a
conectar con los mismos proxys y par 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 creado,
  sa_dest= (sa) 172.16.10.1, sa_proto= 50,
    sa_spi= 0xDD2AC2B3(3710567091),
    esp-sha-hmac del esp-3des del sa_trans=,
sa_conn_id= 3
    sa_lifetime (k/sec) = (4536779/3600)
IPSEC(create_sa): sa creado,
  sa_dest= (sa) 172.16.1.1, sa_proto= 50,
    sa_spi= 0x82C3E0C4(2193875140),
    esp-sha-hmac del esp-3des del sa_trans=,
sa_conn_id= 4
```

El segundo mensaje QM enviado por el concentrador. Mensaje generado por el servicio IPSec que confirma que la protección del túnel está para arriba en el tunnel0. Sigue habiendo otro mensaje de la creación SA se considera que tiene el IP de destino, los SPI, transforma los atributos fijados, y el curso de la vida en de los kilobytes y de los segundos.

```
   sa_lifetime (k/sec) = (4536779/3600)
IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce):
puesta al día de la identificación 8B6A0E8 del tunnel0
con el tun_decap_oce 6A648F0
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):
conexión 8C93888 vuelto operaciones de búsqueda
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):
mensaje listo del buen socket
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):
conexión 8C93888 vuelto operaciones de búsqueda
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):
Señalización del NHRP
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): MTU
conseguido 1458 del mensaje MTU
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):
conexión 8C93888 vuelto operaciones de búsqueda
ISAKMP (1002): paquete recibido del QM_IDLE global
del deporte 500 del dport 500 de 172.16.10.1 (i)
ISAKMP:(1002): proceso del payload del HASH. ID del
mensaje = 3464373979
ISAKMP:(1002): proceso del payload SA. ID del
mensaje = 3464373979
Propuesta IPSec 1 ISAKMP:(1002):Checking
ISAKMP: transforme 1, ESP_3DES
ISAKMP:   los atributos adentro transforman:
ISAKMP:      el encaps es 2 (el transporte)
ISAKMP:      La vida SA teclea adentro los segundos
ISAKMP:      Duración de la vida SA (básica) de 3600
ISAKMP:      La vida SA teclea adentro los kilobytes
ISAKMP:      Duración de la vida SA (VPI) de 0x0 0x46
0x50 0x0
ISAKMP:      el authenticator es HMAC-SHA
ISAKMP:(1002):atts son aceptables.
IPSEC(validate_proposal_request): pieza #1 de la
oferta
IPSEC(validate_proposal_request): pieza #1 de la
oferta,
  (inglés dominante. local= ENTRANTE 172.16.1.1:0
de los msg.), 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, transform= NINGUNOS (transporte),
   lifedur= 0s y 0kb,
   spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
Mapdb Crypto: proxy_match
      addr del src: 172.16.1.1
      addr del dst: 172.16.10.1
      protocolo: 47
      puerto del src: 0
```

El spoke recibe el se
paquete QM que tien
propuesta IPSec. Est
confirma que QM1 fu
recibido por el
concentrador. Los atr
recibidos especifican
indicador del encaps
a 2 (el modo de trans
indicador de 1 sería
túnel), al curso de la
predeterminado SA d
3600 segundos y de
4608000 kilobytes
(0x465000 en el male
al HMAC-SHA para la
autenticación, y al DE
para el cifrado. Pues
son los mismos atribu
fijados en la configura
local, se valida la ofe
shell IPSec SA se cre
Puesto que no se asc
ningunos valores del
Security Parameter In
(SPI) a éstos todavía
es apenas un shell de
SA que no se pueda
para pasar el tráfico
todavía.
La entrada de mapeo
pseudo-crypto se cre
protocolo IP 47 (GRE
172.16.10.1 (direcció
pública del concentra

puerto del dst: 0

ISAKMP:(1002): proceso del payload del NONCE. ID del mensaje = 3464373979
ISAKMP:(1002): payload identificador de proceso. ID del mensaje = 3464373979
ISAKMP:(1002): payload identificador de proceso. ID del mensaje = 3464373979
ISAKMP:(1002): Crear el SA de IPSec
SA entrante de 172.16.10.1 a 172.16.1.1 (f/i) 0 0
(proxy 172.16.10.1 a 172.16.1.1)
tiene el spi 0x82C3E0C4 y conn_id 0
curso de la vida de 3600 segundos
curso de la vida de 4608000 kilobytes
SA saliente de 172.16.1.1 a 172.16.10.1 (f/i) 0/0
(proxy 172.16.1.1 a 172.16.10.1)
tiene el spi 0xDD2AC2B3 y conn_id 0
curso de la vida de 3600 segundos
curso de la vida de 4608000 kilobytes
ISAKMP:(1002): envío del paquete al QM_IDLE del peer_port 500 del my_port 500 de 172.16.10.1 (i)
ISAKMP:(1002):Sending un IKE paquete IPV4.
Razón FALSA del error del nodo -830593317
ISAKMP:(1002):deleting “ningún error”
ISAKMP:(1002):Node 3464373979, entrada = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Estado ISAKMP:(1002):Old = nuevo estado IKE_QM_I_QM1 = IKE_QM_PHASE2_COMPLETE
IPSEC(key_engine): consiguió un evento de la cola con 1 mensaje KMI
Mapdb Crypto: proxy_match
addr del src: 172.16.1.1
addr del dst: 172.16.10.1
protocolo: 47
puerto del src: 0
puerto del dst: 0
IPSEC(crypto_ipsec_sa_find_ident_head): el volver a conectar con los mismos proxys y par 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 creado,
sa_dest= (sa) 172.16.1.1, sa_proto= 50,
sa_spi= 0x82C3E0C4(2193875140),
esp-sha-hmac del esp-3des del sa_trans=, sa_conn_id= 3
sa_lifetime (k/sec) = (4499172/3600)
IPSEC(create_sa): sa creado,
sa_dest= (sa) 172.16.10.1, sa_proto= 50,
sa_spi= 0xDD2AC2B3(3710567091),
esp-sha-hmac del esp-3des del sa_trans=, sa_conn_id= 4
sa_lifetime (k/sec) = (4499172/3600)

172.16.1.1 (dirección pública del spoke). Un IPSec SA/SPI se para ambos el tráfico entrante y saliente co valores de la oferta validada.

El spoke envía el terc final mensaje QM al concentrador, que completa el intercam QM. A diferencia del ISAKMP adonde cad pasa a través de cad estado (MM1 con MM6/P1_COMPLETE IPSec es un poco tan diferente que hay solamente tres mens bastante que seis. El iniciador (nuestro hab este caso, según lo significado por “me” e mensaje IKE_QM_I_ va de QM_READY, entonces a QM_I_QM directamente a QM_PHASE2_COMP El respondedor (concentrador) va QM_READY, QM_SPI_STARVE, QM_R_QM2, QM_PHASE2_COMP Sigue habiendo otro mensaje de la creaci se considera que tien IP de destino, los SP transforma los atribut fijados, y el curso de en de los kilobytes y

	IPSEC(update_current_outbound_sa): consiga a par 172.16.10.1 permiso SA el sa saliente actual a SPI DD2AC2B3 **IPSEC(update_current_outbound_sa): sa saliente actual de 172.16.10.1 del par actualizado a SPI DD2AC2B3** IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce): puesta al día de la identificación 94F2740 del tunnel0 con el tun_decap_oce 794ED30 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): conexión 961D220 vuelto operaciones de búsqueda 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): Señalización del NHRP NHRP: Prioridad 0 del cluster 0 del vrf 0 del tunnel0 NHS 10.1.1.254 transitioned a “E” de '' IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): conexión 961D220 vuelto operaciones de búsqueda NHRP: El intentar enviar el paquete vía DEST 10.1.1.254	segundos.
Estos mensajes finales QM confirman que el Quick Mode es completo y el IPSec está para arriba a ambos lados del túnel. A diferencia del ISAKMP adonde cada par pasa a través de cada estado (MM1 con MM6/P1_COMPLETE), el IPSec es un poco tan diferente que hay solamente tres mensajes bastante que seis. El respondedor (nuestro concentrador en este caso, según lo significado por el “R” en el mensaje IKE_QM_R_QM1) va QM_READY, QM_SPI_STARVE, QM_R_QM2, QM_PHASE2_COMPLETE. El iniciador (spoke) va de QM_READY, entonces a QM_I_QM1 directamente a QM_PHASE2_COMPLETE.	**ISAKMP (1002): paquete recibido del QM_IDLE global del deporte 500 del dport 500 de 172.16.1.1 (r)** Razón FALSA “QM del error del nodo -830593317 ISAKMP:(1002):deleting hecha (aguarde)” ISAKMP:(1002):Node 3464373979, entrada = IKE_MESG_FROM_PEER, IKE_QM_EXCH **Estado ISAKMP:(1002):Old = nuevo estado IKE_QM_R_QM2 = IKE_QM_PHASE2_COMPLETE** IPSEC(key_engine): consiguió un evento de la cola con 1 mensaje KMI IPSEC(key_engine_enable_outbound): el permiso del rec'd notifica del ISAKMP **IPSEC(key_engine_enable_outbound): permiso SA con el spi 2193875140/50** **IPSEC(update_current_outbound_sa): consiga a par 172.16.1.1 permiso SA el sa saliente actual a SPI 82C3E0C4** **IPSEC(update_current_outbound_sa): sa saliente actual de 172.16.1.1 del par actualizado a SPI 82C3E0C4**	
	NHRP: Envíe el pedido de inscripción vía el vrf 0 del tunnel0, tamaño de paquetes: 108 **src: 10.1.1.1, dst: 10.1.1.254** (f) afn: IPv4(1), tipo: IP(800), salto: 255, ver: 1	Éste es los pedidos d inscripción NHRP en al concentrador en la tentativa de registrars

shtl: 4(NSAP), sstl: 0(NSAP)
pktsz: extoff 108: 52
(m) indicadores: “nacional único”, reqid: 65540
src NBMA: 172.16.1.1
protocolo del src: 10.1.1.1, protocolo del dst: 10.1.1.254
Código (C-1): ningún error(0)
prefijo: 32, MTU: 17912, hd_time: 7200
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
Direccionamiento del respondedor Extension(3):
Delantero transite el expediente NHS Extension(4):
El revés transita el expediente NHS Extension(5):
Autenticación Extension(7):
type:Cleartext(1), data: NHRPAUTH
Direccionamiento NAT Extension(9):
Código (C-1): ningún error(0)
prefijo: 32, MTU: 17912, hd_time: 0
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0
cliente NBMA: 172.16.10.1
protocolo cliente: 10.1.1.254

NHS (el concentrado
normal ver los múltip
éstos, a medida que
spoke continúa intent
registrarse con el NH
hasta que reciba una
“contestación del reg
src, dst: IP Addresse
origen de túnel (spok
del destino (concentr
Éstos son la fuente y
destino del Paquete
enviado por el router
src NBMA: el
direccionamiento NB
(Internet) del spoke q
enviaron este paquet
intentos para registra
con el NHS
protocolo del src:
direccionamiento del
del spoke que intenta
registrarse
protocolo del dst:
direccionamiento del
del NHS/hub
Extensión de la autenticación, data&c
Autenticación nhrp ca
cliente NBMA:
Direccionamiento NB
del NHS/hub
protocolo cliente:
direccionamiento del
del NHS/hub

NHRP-RATE: Envío del pedido de inscripción inicial para 10.1.1.254, reqid 65540
%LINK-3-UPDOWN: Tunnel0 de la interfaz, estado cambiado a para arriba
NHRP: if_up: Tunnel0 0 proto
NHRP: Tunnel0: Actualización del caché para el Next-Hop 10.1.1.254 de la blanco 10.1.1.254/32 172.16.10.1
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): conexión 961D220 vuelto operaciones de búsqueda
NHRP: El intentar enviar el paquete vía DEST 10.1.1.254

IPSEC-IFC GRE/Tu0: túnel que sube
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): conexión 961D220 vuelto operaciones de búsqueda
IPSEC-IFC GRE/Tu0: crypto_ss_listen_start que

Más mensajes de ser
NHRP que dicen el p
de inscripción inicial
enviados al NHS en
10.1.1.254. Hay tamb
una confirmación que
entrada de caché fue
agregada para IP
10.1.1.254/24 del tún
las vidas en NBMA
172.16.10.1. El mens
retrasado dice el túne
sido “ningún cerrado”
considera aquí.
Éstos son los mensaj
servicio IPSec genera
que lo dicen trabajan
correctamente. Aquí

	escucha ya IPSEC-IFC GRE/Tu0: crypto_ss_listen_start que escucha ya **IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Apertura de un socket con el perfil DMVPN-IPSEC** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): conexión 961D220 vuelto operaciones de búsqueda IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): El socket está ya abierto. Negligencia. %LINEPROTO-5-UPDOWN: Line Protocol en el tunnel0 de la interfaz, estado cambiado a para arriba
Éste es los pedidos de inscripción NHRP recibidos del spoke en la tentativa de registrarse al NHS (el concentrador). Es normal ver los múltiplos de éstos, a medida que el spoke continúa intentando registrarse con el NHS hasta que reciba una "contestación del registro." **src NBMA**: el direccionamiento NBMA (Internet) del spoke que enviaron este paquete e intentos para registrarse con el NHS **protocolo del src**: haga un túnel el direccionamiento del spoke que intenta registrarse **protocolo del dst**: direccionamiento del túnel del NHS/hub **Extensión de la autenticación**, data: Autenticación nhrp cadena **cliente NBMA**: Direccionamiento NBMA del NHS/hub **protocolo cliente**: direccionamiento del túnel del NHS/hub	**NHRP: Reciba el pedido de inscripción vía el vrf 0 del tunnel0, tamaño de paquetes: 108** (f) afn: IPv4(1), tipo: IP(800), salto: 255, ver: 1 shtl: 4(NSAP), sstl: 0(NSAP) pktsz: extoff 108: 52 (m) indicadores: "nacional único", reqid: 65540 **src NBMA: 172.16.1.1** **protocolo del src: 10.1.1.1, protocolo del dst: 10.1.1.254** Código (C-1): ningún error(0) prefijo: 32, MTU: 17912, hd_time: 7200 addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0 Direccionamiento del respondedor Extension(3): Delantero transite el expediente NHS Extension(4): El revés transita el expediente NHS Extension(5): **Autenticación Extension(7):** **type:Cleartext(1), data: NHRPAUTH** Direccionamiento NAT Extension(9): Código (C-1): ningún error(0) prefijo: 32, MTU: 17912, hd_time: 0 addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0 **cliente NBMA: 172.16.10.1** **protocolo cliente: 10.1.1.254**
Paquetes del debug NHRP que agregan la red objetivo 10.1.1.1/32 disponible vía el salto siguiente de 10.1.1.1 en el NHRP de 172.16.1.1. 172.16.1.1 también se agrega a la lista de direccionamientos a los cuales del concentrador el	NHRP: netid_in = 1, to_us = 1 **NHRP: Tunnel0: El caché agrega para el Next-Hop 10.1.1.1 de la blanco 10.1.1.1/32** **172.16.1.1** **NHRP: Agregar los puntos finales del túnel (VPN: 10.1.1.1, NBMA: 172.16.1.1)** **NHRP: Subblock con éxito asociado NHRP para los puntos finales del túnel (VPN: 10.1.1.1, NBMA: 172.16.1.1)**

donde finalmente se
el Tunnel Protocol es
para arriba.

tráfico Multicast adelante. Estos mensajes confirman que el registro era acertado, al igual que una resolución para el direccionamiento del túnel del spokes.

NHRP: Nodo insertado del subblock para el caché: Nodo insertado blanco del subblock para el caché: Blanco 10.1.1.1/32nhop 10.1.1.1
NHRP: Entrada de caché dinámica interna convertida para 10.1.1.1/32 tunnel0 de la interfaz al externo
NHRP: Tu0: Crear el mapeo multidifusión dinámico NBMA: 172.16.1.1
NHRP: Mapeo multidifusión dinámico agregado para el NBMA: 172.16.1.1
NHRP: Puesta al día de nuestro caché con el NBMA: 172.16.10.1, NBMA_ALT: 172.16.10.1
NHRP: Nueva longitud obligatoria: 32
NHRP: El intentar enviar el paquete vía DEST 10.1.1.1
NHRP: NHRP con éxito 10.1.1.1 resuelto a NBMA 172.16.1.1
NHRP: Encapsulación tenida éxito. Addr 172.16.1.1 IP del túnel

Ésta es la contestación del registro NHRP enviada por el concentrador al spoke en respuesta al “pedido de inscripción NHRP” recibido anterior. Como los otros paquetes de inscripción, el concentrador envía los múltiplos de éstos en respuesta a las peticiones múltiples.

src, dst: IP Addresses del origen de túnel (concentrador) y del destino (spoke). Éstos son la fuente y el destino del Paquete GRE enviado por el router

src NBMA: Direccionamiento NBMA (Internet) del spoke

protocolo del src: direccionamiento del túnel del spoke que intenta registrarse

protocolo del dst: direccionamiento del túnel del NHS/hub

cliente NBMA: Direccionamiento NBMA del NHS/hub

protocolo cliente: direccionamiento del túnel del NHS/hub

Extensión de la autenticación, data:

NHRP: Envíe la contestación del registro vía el vrf 0 del tunnel0, tamaño de paquetes: 128
src: 10.1.1.254, dst: 10.1.1.1
(f) afn: IPv4(1), tipo: IP(800), salto: 255, ver: 1
shtl: 4(NSAP), sstl: 0(NSAP)
pktsz: extoff 128: 52
(m) indicadores: “nacional único”, reqid: 65540
src NBMA: 172.16.1.1
protocolo del src: 10.1.1.1, protocolo del dst: 10.1.1.254
Código (C-1): ningún error(0)
prefijo: 32, MTU: 17912, hd_time: 7200
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
Direccionamiento del respondedor Extension(3):
(c) código: ningún error(0)
prefijo: 32, MTU: 17912, hd_time: 7200
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0
cliente NBMA: 172.16.10.1
protocolo cliente: 10.1.1.254
Delantero transite el expediente NHS Extension(4):
El revés transita el expediente NHS Extension(5):
Autenticación Extension(7):
type:Cleartext(1), data: NHRPAUTH
Direccionamiento NAT Extension(9):
Código (C-1): ningún error(0)
prefijo: 32, MTU: 17912, hd_time: 0
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0
cliente NBMA: 172.16.10.1
protocolo cliente: 10.1.1.254

Autenticación nhrp cadena		
	NHRP: Reciba la contestación del registro vía el vrf 0 del tunnel0, tamaño de paquetes: 128 (f) afn: IPv4(1), tipo: IP(800), salto: 255, ver: 1 shtl: 4(NSAP), sstl: 0(NSAP) pktsz: extoff 128: 52 (m) indicadores: “nacional único”, reqid: 65541 **src NBMA: 172.16.1.1** **protocolo del src: 10.1.1.1, protocolo del dst: 10.1.1.254** Código (C-1): ningún error(0) prefijo: 32, MTU: 17912, hd_time: 7200 addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0 Direccionamiento del respondedor Extension(3): (c) código: ningún error(0) prefijo: 32, MTU: 17912, hd_time: 7200 addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0 **cliente NBMA: 172.16.10.1** **protocolo cliente: 10.1.1.254** Delantero transite el expediente NHS Extension(4): El revés transita el expediente NHS Extension(5): **Autenticación Extension(7):** **type:Cleartext(1), data: NHRPAUTH** Direccionamiento NAT Extension(9): Código (C-1): ningún error(0) prefijo: 32, MTU: 17912, hd_time: 0 addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0 **cliente NBMA: 172.16.10.1** **protocolo cliente: 10.1.1.254**	Ésta es la contestaci registro NHRP enviad el concentrador al sp respuesta al “pedido inscripción NHRP” re anterior. Como los ot paquetes de inscripci concentrador envía lo múltiplos de éstos en respuesta a las petici múltiples. **src NBMA**: Direccionamiento NB (Internet) del spoke **protocolo del src**: direccionamiento del del spoke que intenta registrarse **protocolo del dst**: direccionamiento del del NHS/hub **cliente NBMA**: Direccionamiento NB del NHS/hub **protocolo cliente**: direccionamiento del del NHS/hub **Extensión de la autenticación**, data&c Autenticación nhrp ca
	NHRP: netid_in = 0, to_us = 1	
Mensajes de servicio IPSec más generales que digan trabaja correctamente.	IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start que escucha ya IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Apertura de un socket con el perfil DMVPN-IPSEC IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): conexión 8C93888 vuelto operaciones de búsqueda IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): El socket está ya abierto. Negligencia. 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	Los mensajes de ser NHRP que dicen el N situado en 10.1.1.254 están para arriba.
El mensaje del sistema que estado la adyacencia del EIGRP está para arriba con el vecino habló en 10.1.1.1.	%DUAL-5-NBRCHANGE: EIGRP-IPv4 1: El vecino 10.1.1.1 (tunnel0) está para arriba: nueva adyacencia	
	%DUAL-5-NBRCHANGE: EIGRP-IPv4 1: El vecino 10.1.1.254 (tunnel0) está para arriba: nueva	El mensaje del sisten estado la adyacencia

	adyacencia	EIGRP está para arri el concentrador vecin 10.1.1.254.
Mensaje del sistema que confirma una resolución NHRP acertada.	NHRP: NHRP con éxito 10.1.1.1 resuelto a NBMA 172.16.1.1	

Confirme las funciones y resuelvalas problemas

Esta sección tiene algunos de la mayoría de los comandos show útiles usados para resolver problemas ambos el hub and spoke. Para habilitar debugs más específicos, utilice estos conditionals del debug:

- haga el debug del nbma *NBMA_ADDRESS del* par de la condición del dmvpn
- haga el debug del túnel *TUNNEL_ADDRESS del* par de la condición del dmvpn
- par ipv4 *NBMA_ADDRESS de la* condición del debug crypto

muestre los socketes crypto

```
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"
```

muestre al detalle de la sesión de criptografía

```
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
```

muestre el detalle crypto isakmp sa

```
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

muestre el detalle 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:
```

muestre el nhrp del IP

```
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
```

muestre los nhs del 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)*

muestre el 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:
```

Información Relacionada

- Troubleshooting de IPSec: Entendiendo y con los comandos debug
- Cifrado de la última generación
- RFC3706: Dead Peer Detection IKE
- RFC3947: Traversal IKE NAT
- Soporte Técnico y Documentación - Cisco Systems