Guía de Troubleshooting de Debugs de la Fase 1 de DMVPN

Contenido

Introducción

Este documento describe los mensajes de depuración que encontraría en el hub y habla de una implementación de fase 1 de red privada virtual multipunto dinámica (DMVPN).

Prerequisites

Para los comandos de configuración y depuración en este documento, necesitará dos routers Cisco que ejecuten Cisco IOS® Release 12.4(9)T o posterior. En general, una Fase 1 básica de DMVPN requiere Cisco IOS Release 12.2(13)T o posterior o Release 12.2(33)XNC para el Aggregation Services Router (ASR), aunque es posible que las características y las depuraciones que se ven en este documento no sean compatibles.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Encapsulación de routing genérico (GRE)
- Protocolo de resolución de salto siguiente (NHRP)
- Asociación de seguridad de Internet y protocolo de gestión de claves (ISAKMP)
- Intercambio de claves de Internet (IKE)
- Seguridad de protocolo de Internet (IPSec)
- Al menos uno de estos protocolos de ruteo: protocolo de routing de gateway interior mejorado (EIGRP), ruta de acceso más corta primero (OSPF), protocolo de información de routing (RIP) y protocolo de gateway fronterizo (BGP)

Componentes Utilizados

La información de este documento se basa en los routers de servicios integrados (ISR) Cisco 2911 que ejecutan Cisco IOS Release 15.1(4)M4.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Mejoras significativas

Estas versiones de Cisco IOS introdujeron características o correcciones significativas para la Fase 1 de DMVPN:

- Versión 12.2(18)SXF5: mejor compatibilidad con ISAKMP cuando se utiliza Public Key Infrastructure (PKI)
- Versión 12.2(33)XNE - ASR, perfiles IPSec, protección de túnel, traducción de direcciones de red (NAT) IPSec transversal
- Versión 12.3(7)T: compatibilidad con routing y reenvío virtuales (iVRF)
- Versión 12.3(11)T: compatibilidad con routing y reenvío virtuales (fVRF) de la puerta frontal
- Versión 12.4(9)T: compatibilidad con varios comandos y depuraciones relacionados con DMVPN
- Versión 12.4(15)T: protección de túnel compartido
- Versión 12.4(20)T - IPv6 sobre DMVPN
- Versión 15.0(1)M - Supervisión del estado del túnel NHRP

Convenciones

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

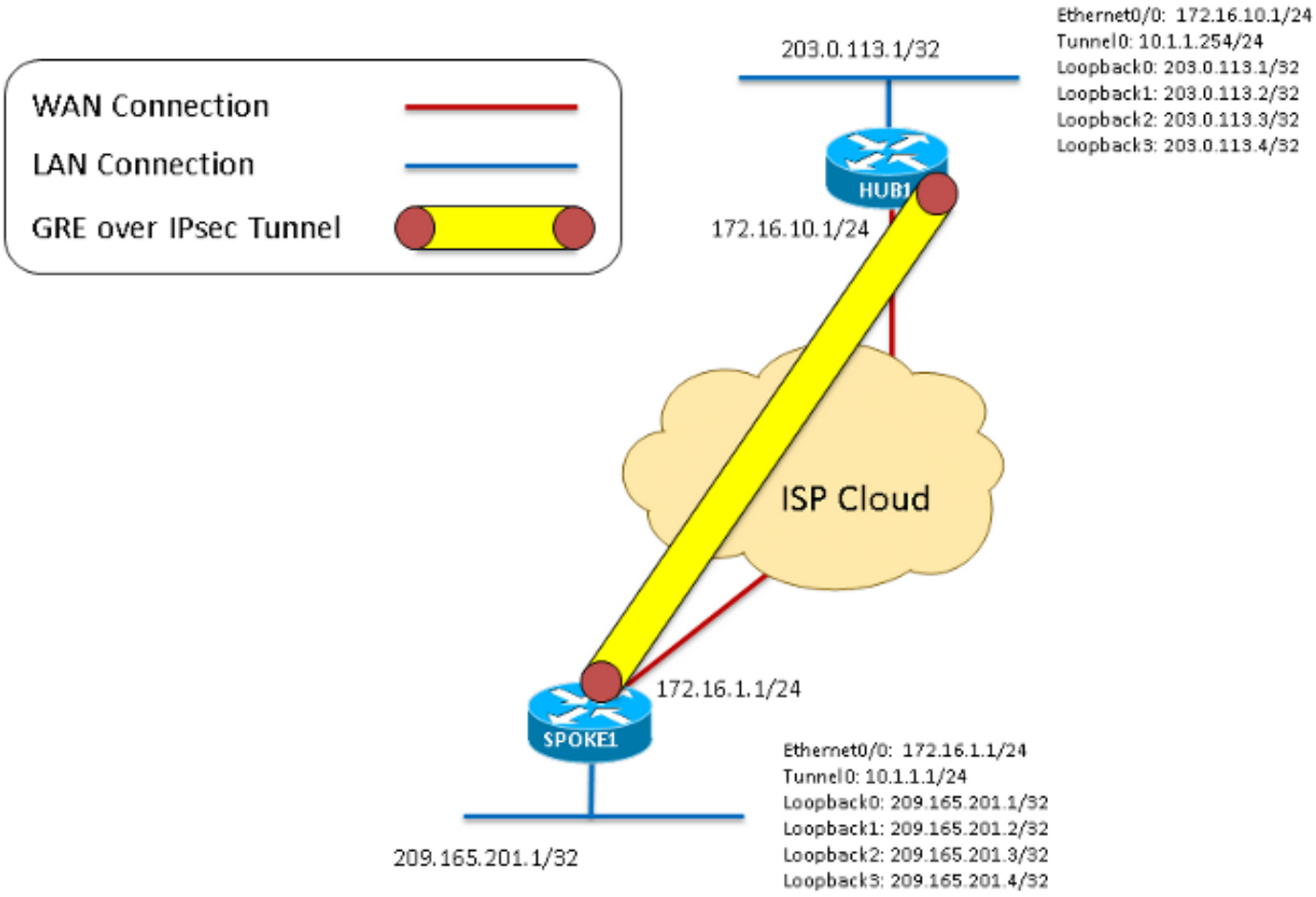
Configuración relevante

Descripción general de la topología

Para esta topología, se configuraron dos ISR 2911 que ejecutan la versión 15.1(4)M4 para la fase 1 de DMVPN: uno como concentrador y otro como radio. Ethernet0/0 se utilizó como la interfaz de

"Internet" en cada router. Las cuatro interfaces loopback se configuran para simular las redes de área local que viven en el hub o el sitio spoke. Como se trata de una topología de fase 1 de DMVPN con sólo un radio, el spoke se configura con un túnel GRE punto a punto en lugar de un túnel GRE multipunto. Se utilizó la misma configuración de criptografía (ISAKMP e IPSec) en cada router para asegurarse de que coincidían exactamente.

Diagrama 1



Criptografía

Esto es lo mismo en el hub 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
```

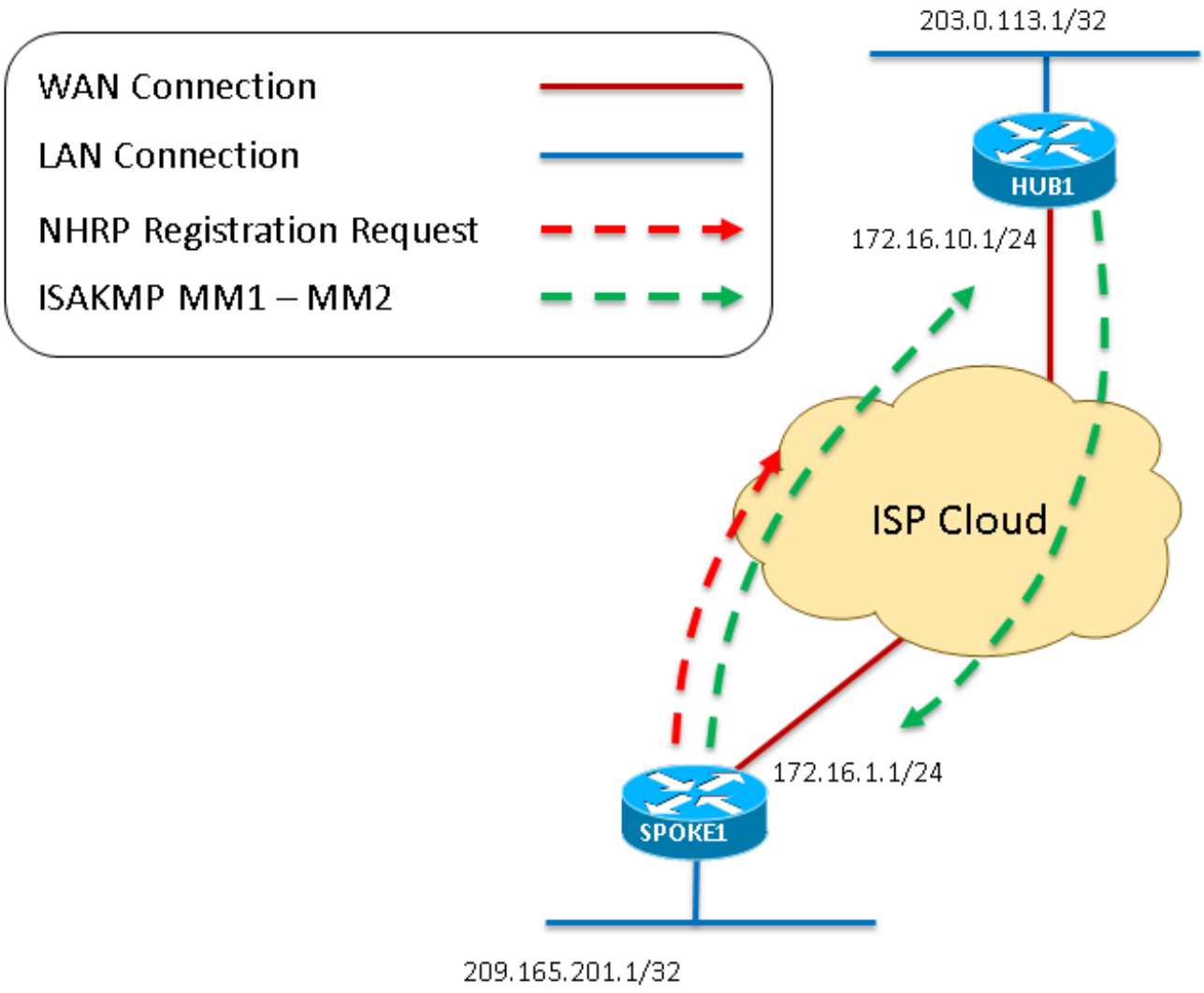
```
network 209.165.201.2 0.0.0.0
network 209.165.201.3 0.0.0.0
network 209.165.201.4 0.0.0.0
network 10.1.1.0 0.0.0.255
```

Depuraciones

Visualización del flujo de paquetes

Esta es una visualización de todo el flujo de paquetes DMVPN tal como se ve en este documento. También se incluyen depuraciones más detalladas que explican cada uno de los pasos.

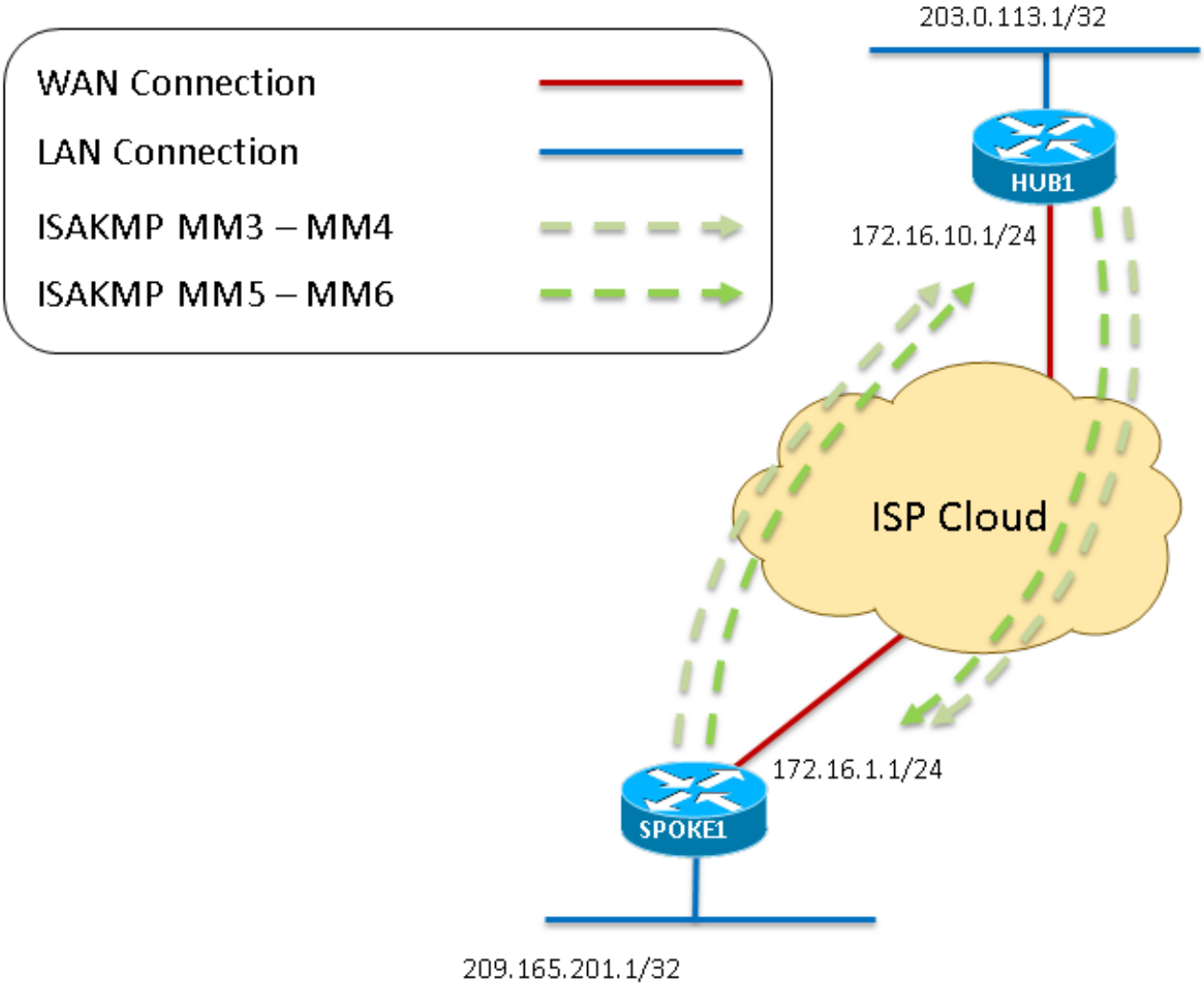
1. Cuando el Túnel en el Spoke "no shutdown" genera una Solicitud de Registro NHRP, que inicia el proceso DMVPN. Como la configuración del hub es completamente dinámica, Spoke debe ser el punto final que inicie la conexión.
2. La solicitud de registro NHRP se encapsula en GRE, lo que activa el proceso crypto para que se inicie.
3. En este punto, el primer mensaje del Modo principal ISAKMP - ISAKMP MM1 - se envía desde el Spoke al Hub en el puerto UDP500.
4. El Hub recibe y procesa MM1 y responde con ISAKMP MM2, ya que tiene una política ISAKMP coincidente.
   Diagrama 2: se refiere a los pasos 1 a 4



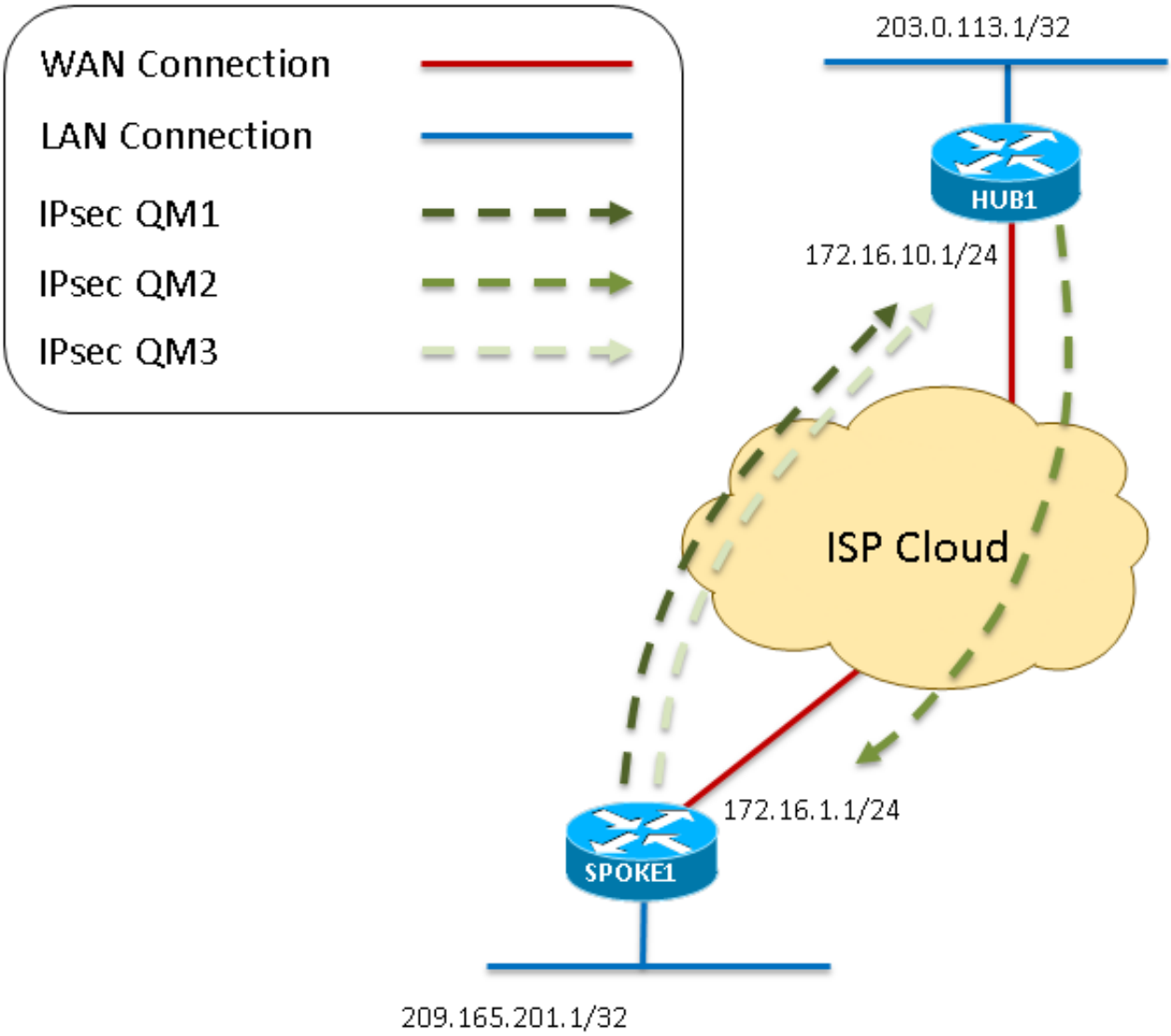
5. Una vez que Spoke recibe el MM2, responde con MM3. Al igual que con MM1, Spoke

confirma que la política ISAKMP recibida es válida.

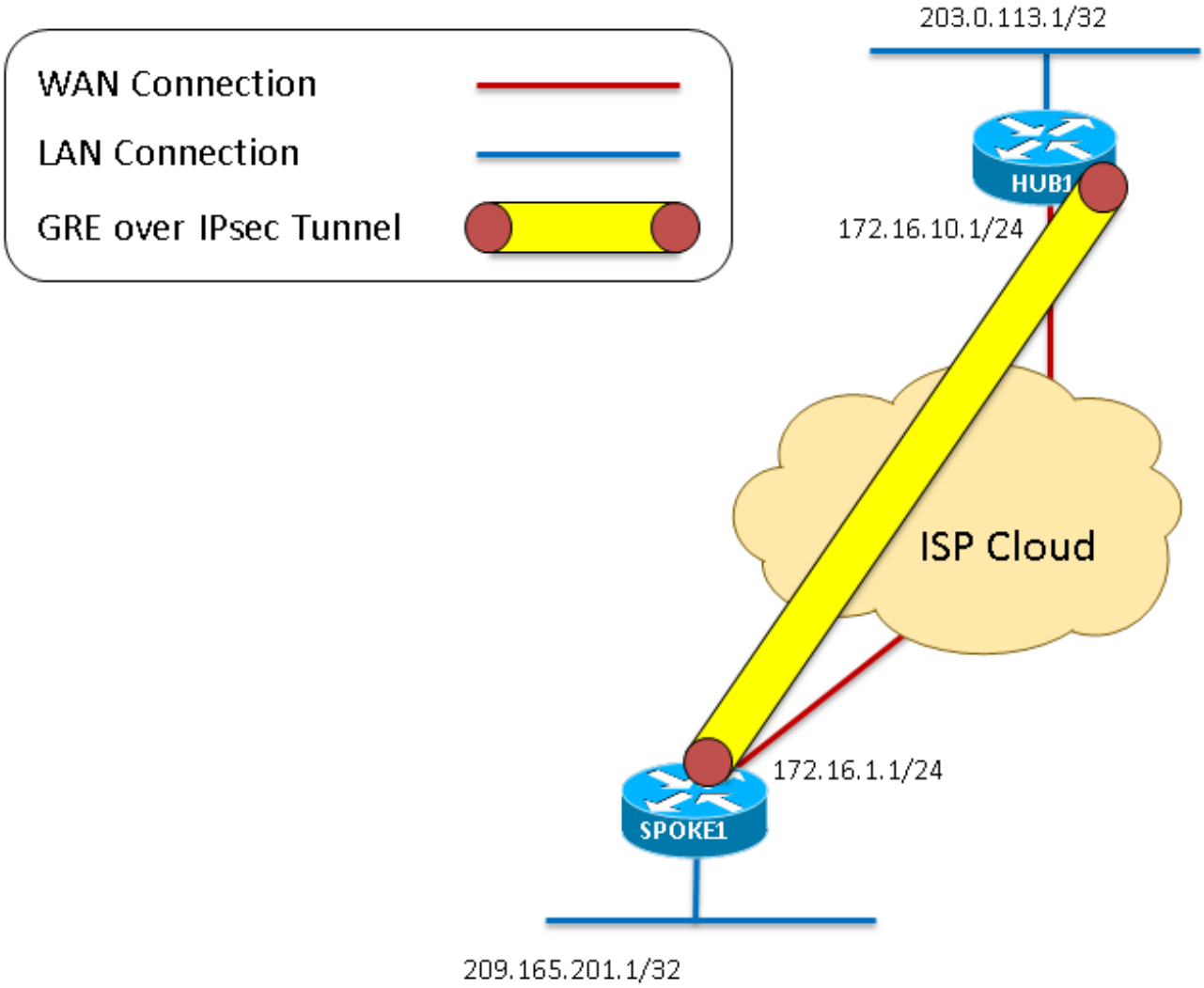
6. El Hub recibe MM3 y responde con MM4.
7. En este punto de la negociación ISAKMP, el Spoke podría responder en el puerto UDP4500 si se detecta NAT en la trayectoria de tránsito. Sin embargo, si no se detecta ninguna NAT, Spoke continúa y envía el MM5 en UDP500. Por último, el concentrador responde con MM6 para completar el intercambio de modo principal.
   Diagrama 3: se refiere a los pasos 5 a 7



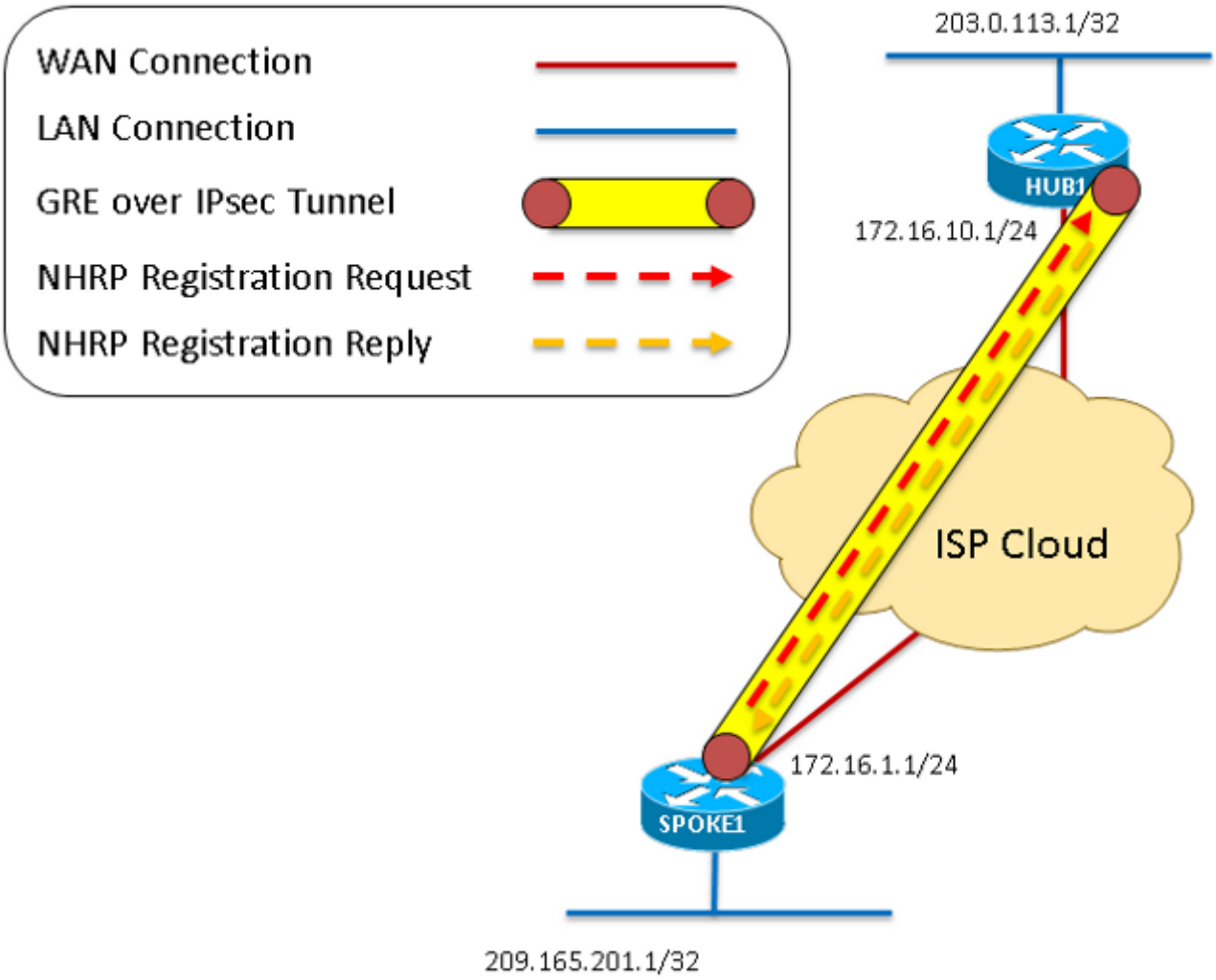
8. Una vez que Spoke recibe MM6 del Hub, envía QM1 al Hub en UDP500 para comenzar el Modo rápido.
9. El Hub recibe QM1 y responde con QM2, ya que se aceptan todos los atributos recibidos. En este momento, el Hub crea las SA de Fase 2 para esta sesión.
10. Como último paso de la negociación de modo rápido, el Spoke recibe QM2. El Spoke luego crea sus SA de Fase 2 y envía QM3 en respuesta. Esto completa la negociación ISAKMP e IPSec. Ahora hay una sesión IPSec que cifra el tráfico GRE entre estos dos peers.
    Diagrama 4: se refiere a los pasos 8 a 10



11. Ahora que la sesión de criptografía está activa y puede pasar tráfico, estos paquetes se encapsulan dentro del GRE sobre el túnel IPSec.
    Diagrama 5: se refiere al paso
    11



12. Como se observó en los primeros pasos, el Spoke genera una Solicitud de Registro NHRP que se envía a través del GRE sobre el túnel IPSec.
13. El concentrador recibe las solicitudes de registro NHRP y envía una respuesta de registro NHRP una vez que confirma que el radio tiene una dirección válida de túnel y acceso múltiple sin difusión (NBMA). El Spoke recibe esta respuesta de registro NHRP que completa el proceso de registro.
    Diagrama 6: se refiere a los pasos 12 a
    13



Estas depuraciones son el resultado cuando se ingresa el comando **debug dmvpn all** en los routers hub y spoke. Este comando en particular habilita este conjunto de depuraciones:

```
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
```

Depuraciones con explicación

Dado que se trata de una configuración en la que se implementa IPSec, las depuraciones muestran todas las depuraciones ISAKMP e IPSec. Si no se configura ninguna criptografía, ignore cualquier depuración que comience con "IPsec" o "ISAKMP".

EXPLICACIÓN DE DEPURACIÓN DEL HUB	DEPURACIÓN EN SECUENCIA	EXPLICACIÓN D DEPURACIÓN DE S
Estos primeros mensajes de depuración son generados por un comando **no shutdown** ingresado en la interfaz de túnel. Los mensajes son generados por los servicios crypto, GRE y NHRP que se inician. Se ve un error de registro NHRP en el hub porque no tiene configurado un servidor de próximo salto (NHS) (el hub es el NHS para nuestra nube DMVPN). Esto se espera.	IPSEC-IFC MGRE/Tu0: Comprobando el estado del túnel. **NHRP: if_up: Tunnel0 proto 0** IPSEC-IFC MGRE/Tu0: túnel que se aproxima IPSEC-IFC MGRE/Tu0: crypto_ss_hear_start ya está escuchando **%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP está ACTIVADO** **NHRP: No se puede enviar el registro: no hay NHS configurados** %LINK-3-UPDOWN: Interface Tunnel0, estado cambiado a up NHRP: if_up: Tunnel0 proto 0 NHRP: No se puede enviar el registro: no hay NHS configurados IPSEC-IFC MGRE/Tu0: túnel que se aproxima IPSEC-IFC MGRE/Tu0: crypto_ss_hear_start ya está escuchando **%LINEPROTO-5-UPDOWN: Protocolo de línea en la interfaz Tunnel0, estado cambiado a activo** IPSEC-IFC GRE/Tu0: Comprobando el estado del túnel. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): búsqueda de conexión devuelta 0 **IPSEC-IFC GRE/Tu0: crypto_ss_hear_start ya está escuchando** **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): búsqueda de conexión devuelta 0 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Activación del túnel inmediatamente. IPSEC-IFC GRE/Tu0: Adición de la interfaz de túnel Tunnel0 a la lista compartida **NHRP: if_up: Tunnel0 proto 0** **NHRP: Túnel0: Agregación de caché para el destino**	Estos primeros mens de depuración son generados por un co **no shutdown** ingresa la interfaz de túnel. L mensajes son genera por servicios crypto, NHRP que se inician Además, el spoke ag una entrada a su pro memoria caché NHR su propia dirección d y NBMA.

10.1.1.254/32 salto siguiente 10.1.1.254
172.16.10.1
IPSEC-IFC GRE/Tu0: túnel que se aproxima
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):
búsqueda de conexión 961D220
IPSEC-IFC GRE/Tu0: crypto_ss_hear_start ya está escuchando
IPSEC-IFC GRE/Tu0: crypto_ss_hear_start ya está escuchando
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):
búsqueda de conexión 961D220
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): El socket ya está siendo abierto. Ignorando.
CRYPTO_SS(TUNNEL SEC): La aplicación comenzó a escuchar
la inserción de mapa en mapdb AVL falló, el par map + ace ya existe en el mapdb
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP está ACTIVADO
CRYPTO_SS(TUNNEL SEC): Abrir activo, información de socket: local 172.16.1.1
172.16.1.1/255.255.255.255/0, remote 172.16.10.1
172.16.10.1/255.255.255.255/0, prot 47, ifc Tu0
INICIO DE LA NEGOCIACIÓN ISAKMP (FASE I)
IPSEC(recalculate_mtu): reset sadb_root 94EFDC0 mtu a 1500
IPSEC(sa_request): ,
(eng clave. msg.) OUTBOUND local= 172.16.1.1:500, remoto= 172.16.10.1:500,
local_proxy= 172.16.1.1/255.255.255.255/47/0 (tipo=1),
remote_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac (Transport),
lifedur= 3600 y 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 0, indicadores= 0x0
ISAKMP:(0): El perfil de solicitud SA es (NULL)
ISAKMP: Creó una estructura de peer para 172.16.10.1, puerto de peer 500
ISAKMP: Nuevo peer creado = 0x95F6858 peer_handle = 0x80000004
ISAKMP: Bloqueo de la estructura del par 0x95F6858, recuento 1 para isakmp_initiator
ISAKMP: puerto local 500, puerto remoto 500
ISAKMP: set new node 0 to QM_IDLE
ISAKMP:(0):insertar sa correctamente = 8A26FB0
ISAKMP:(0): No se puede iniciar el modo Agresivo, intentando el modo principal.
ISAKMP:(0):clave precompartida de par encontrada

El primer paso una v
el túnel es "no shutd
es iniciar la negociac
crypto. Aquí el spoke
una solicitud SA, inte
iniciar el Modo Agres
falla en el Modo Princ
Dado que el modo ag
no está configurado e
ninguno de los router
espera esto.
El spoke comienza el
principal y envía el pr
mensaje ISAKMP,
MM_NO_STATE. El e
ISAKMP cambia de
IKE_READY a IKE_I_
Los mensajes de ID d
proveedor NAT-T se
utilizan en la detecció
inversión de NAT. Es
mensajes se esperan
durante la negociació
ISAKMP
independientemente
NAT se implementa c
Al igual que los mens

	que coincide con 172.16.10.1 ISAKMP:(0): ID de proveedor de NAT-T construido-rfc3947 ISAKMP:(0): ID del proveedor de NAT-T construido-07 ISAKMP:(0): ID del proveedor de NAT-T construido-03 ISAKMP:(0): ID del proveedor de NAT-T construido-02 **ISAKMP:(0):Entrada = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM** **ISAKMP:(0):Estado antiguo = IKE_READY Nuevo estado = IKE_I_MM1** **ISAKMP:(0): Inicio del intercambio de modo principal** **ISAKMP:(0): envío de paquetes a 172.16.10.1 my_port 500 peer_port 500 (I) MM_NO_STATE** ISAKMP:(0):Envío de un paquete IPv4 IKE. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): búsqueda de conexión 961D220 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): mensaje listo para socket	del modo agresivo, s esperan.
Después de que el túnel del spoke "no shutdown", el hub recibe el mensaje IKE NEW SA (Main Mode 1) en el puerto 500. Como Respondedor, el hub crea una Asociación de seguridad ISAKMP (SA). El estado ISAKMP cambia de IKE_READY a IKE_R_MM1.	**ISAKMP (0): paquete recibido desde 172.16.1.1 puerto 500 sport 500 Global (N) NEW SA** **ISAKMP: Creó una estructura de peer para 172.16.1.1, puerto de peer 500** ISAKMP: Nuevo peer creado = 0x8CACD00 peer_handle = 0x80000003 ISAKMP: Bloqueo de la estructura de peer 0x8CACD00, descuento 1 para crypto_isakmp_process_block ISAKMP: puerto local 500, puerto remoto 500 **ISAKMP:(0):insertar sa correctamente = 6A5BDE8** ISAKMP:(0):Entrada = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(0):Estado antiguo = IKE_READY Nuevo estado = IKE_R_MM1**	
Se procesa el mensaje IKE Main Mode 1 recibido. El hub determina que el par tiene atributos ISAKMP coincidentes y que se rellenan en la SA ISAKMP que se acaba de crear. Los mensajes muestran que el par utiliza 3DES-CBC para el cifrado, el hash de SHA, Diffie Hellman (DH) group 1, la clave precompartida para la autenticación y la duración de SA predeterminada de 86400 segundos (0x0 0x1 0x51 0x80 = 0x15180 = 86400 segundos) ... El estado ISAKMP sigue	ISAKMP:(0): procesamiento de carga útil SA. ID de mensaje = 0 ISAKMP:(0): carga útil de ID del proveedor de procesamiento **ISAKMP:(0): ID del proveedor parece Unity/DPD pero hay una discordancia importante de 69** **ISAKMP (0): la ID del proveedor es NAT-T RFC 3947** ISAKMP:(0): carga útil de ID del proveedor de procesamiento ISAKMP:(0): ID del proveedor parece Unity/DPD pero la mayor discordancia 245 ISAKMP (0): ID del proveedor es NAT-T v7 ISAKMP:(0): carga útil de ID del proveedor de procesamiento ISAKMP:(0): ID del proveedor parece Unity/DPD pero la mayor discordancia 157 ISAKMP:(0): ID del proveedor es NAT-T v3 ISAKMP:(0): carga útil de ID del proveedor de procesamiento	

siendo IKE_R_MM1 ya que no se ha enviado una respuesta al spoke. Los mensajes de ID de proveedor NAT-T se utilizan en la detección y la inversión de NAT. Estos mensajes se esperan durante la negociación de ISAKMP independientemente de si NAT se implementa o no. Se ven mensajes similares para la detección de puntos inactivos (DPD).	ISAKMP:(0): ID del proveedor parece Unity/DPD, pero la mayor discordancia 123 ISAKMP:(0): ID del proveedor es NAT-T v2 **ISAKMP:(0):clave precompartida de par encontrada que coincide con 172.16.1.1** **ISAKMP:(0): clave precompartida local encontrada** ISAKMP: Perfiles de exploración para xauth ... **ISAKMP:(0):Verificación de la transformación 1 de ISAKMP con respecto a la política de prioridad 1** **ISAKMP: cifrado 3DES-CBC** **ISAKMP: hash SHA** **ISAKMP: grupo predeterminado 1** **ISAKMP: auth pre-share** **ISAKMP: tipo de vida en segundos** **ISAKMP: duración de vida (VPI) de 0x0 0x1 0x51 0x80** **ISAKMP:(0):los actos son aceptables. La siguiente carga útil es 0** **ISAKMP:(0):Actos aceptables:vida real: 0** **ISAKMP:(0):Actos aceptables:vida: 0** **ISAKMP:(0):Rellene los datos en sa vpi_length:4** **ISAKMP:(0):Rellene los datos en sa life_in_seconds:86400** **ISAKMP:(0):Devolver vida real: 86400** **ISAKMP:(0)::Temporizador de vida útil de inicio: 86400.** ISAKMP:(0): carga útil de ID del proveedor de procesamiento ISAKMP:(0): ID del proveedor parece Unity/DPD pero hay una discordancia importante de 69 ISAKMP (0): la ID del proveedor es NAT-T RFC 3947 ISAKMP:(0): carga útil de ID del proveedor de procesamiento ISAKMP:(0): ID del proveedor parece Unity/DPD pero la mayor discordancia 245 ISAKMP (0): ID del proveedor es NAT-T v7 ISAKMP:(0): carga útil de ID del proveedor de procesamiento ISAKMP:(0): ID del proveedor parece Unity/DPD pero la mayor discordancia 157 ISAKMP:(0): ID del proveedor es NAT-T v3 ISAKMP:(0): carga útil de ID del proveedor de procesamiento ISAKMP:(0): ID del proveedor parece Unity/DPD, pero la mayor discordancia 123 ISAKMP:(0): ID del proveedor es NAT-T v2 ISAKMP:(0):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(0):Estado antiguo = IKE_R_MM1 Nuevo estado = IKE_R_MM1
MM_SA_SETUP (Modo principal 2) se envía al spoke, lo que confirma que	ISAKMP:(0): ID de proveedor de NAT-T construido-rfc3947 **ISAKMP:(0): envío de paquetes a 172.16.1.1 my_port**

se recibió y se aceptó el MM1 como un paquete ISAKMP válido. El estado ISAKMP cambia de IKE_R_MM1 a IKE_R_MM2.	**500 peer_port 500 (R) MM_SA_SETUP** ISAKMP:(0):Envío de un paquete IPv4 IKE. ISAKMP:(0):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(0):Estado antiguo = IKE_R_MM1 Nuevo estado = IKE_R_MM2**	
	ISAKMP (0): paquete recibido desde 172.16.10.1 puerto 500 sport 500 Global (I) MM_NO_STATE **ISAKMP:(0):Entrada = IKE_MESG_FROM_PEER, IKE_MM_EXCH** **ISAKMP:(0):Estado antiguo = IKE_I_MM1 Nuevo estado = IKE_I_MM2**	En respuesta al mens MM1 enviado al hub, MM2 que confirma qu recibió MM1. Se proc mensaje IKE Main M recibido. El spoke se cuenta de que el hub peer tiene atributos ISAKMP coincidentes estos atributos se rel en la SA ISAKMP qu creó. Este paquete m que el par utiliza 3DE CBC para el cifrado, hash de SHA, Diffie Hellman (DH) group clave precompartida la autenticación y la duración de SA predeterminada de 8 segundos (0x0 0x1 0 0x80 = 0x15180 = 86 segundos) ... Además de los mens NAT-T, hay un interc para determinar si la utilizará DPD. El estado ISAKMP ca de IKE_I_MM1 a IKE_I_MM2.
	ISAKMP:(0): procesamiento de carga útil SA. ID de mensaje = 0 ISAKMP:(0): carga útil de ID del proveedor de procesamiento **ISAKMP:(0): ID del proveedor parece Unity/DPD pero hay una discordancia importante de 69** ISAKMP (0): la ID del proveedor es NAT-T RFC 3947 ISAKMP:(0):clave precompartida de par encontrada que coincide con 172.16.10.1 ISAKMP:(0): clave precompartida local encontrada ISAKMP: Perfiles de exploración para xauth ... **ISAKMP:(0):Verificación de la transformación 1 de ISAKMP con respecto a la política de prioridad 1** **ISAKMP: cifrado 3DES-CBC** **ISAKMP: hash SHA** **ISAKMP: grupo predeterminado 1** **ISAKMP: auth pre-share** **ISAKMP: tipo de vida en segundos** **ISAKMP: duración de vida (VPI) de 0x0 0x1 0x51 0x80** **ISAKMP:(0):los actos son aceptables. La siguiente carga útil es 0** **ISAKMP:(0):Actos aceptables:vida real: 0** **ISAKMP:(0):Actos aceptables:vida: 0** **ISAKMP:(0):Rellene los datos en sa vpi_length:4** **ISAKMP:(0):Rellene los datos en sa life_in_seconds:86400** **ISAKMP:(0):Devolver vida real: 86400** **ISAKMP:(0)::Temporizador de vida útil de inicio: 86400.**	
	ISAKMP:(0): carga útil de ID del proveedor de procesamiento ISAKMP:(0): ID del proveedor parece Unity/DPD pero hay una discordancia importante de 69 ISAKMP (0): la ID del proveedor es NAT-T RFC 3947 ISAKMP:(0):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(0):Estado antiguo = IKE_I_MM2 Nuevo estado = IKE_I_MM2 **ISAKMP:(0): envío de paquetes a 172.16.10.1 my_port**	MM_SA_SETUP (Mo

	500 peer_port 500 (I) MM_SA_SETUP ISAKMP:(0):Envío de un paquete IPv4 IKE. ISAKMP:(0):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(0):Estado antiguo = IKE_I_MM2 Nuevo estado = IKE_I_MM3**	principal 3) se envía a lo que confirma que e spoke recibió MM2 y continuar. El estado ISAKMP ca de IKE_I_MM2 a IKE_I_MM3.
MM_SA_SETUP (Modo principal 3) es recibido por el hub. El hub concluye que el par es otro dispositivo Cisco IOS y que no se detecta NAT para nosotros ni para nuestro par. El estado ISAKMP cambia de IKE_R_MM2 a IKE_R_MM3.	**ISAKMP (0): paquete recibido desde 172.16.1.1 puerto 500 sport 500 Global (R) MM_SA_SETUP** ISAKMP:(0):Entrada = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(0):Estado antiguo = IKE_R_MM2 Nuevo estado = IKE_R_MM3**	
	ISAKMP:(0): procesamiento de carga útil KE. ID de mensaje = 0 ISAKMP:(0): procesamiento de la carga útil NONCE. ID de mensaje = 0 **ISAKMP:(0):clave precompartida de par encontrada que coincide con 172.16.1.1** ISAKMP:(1002): carga útil de ID del proveedor de procesamiento ISAKMP:(1002): ID del proveedor es DPD ISAKMP:(1002): carga útil de ID del proveedor de procesamiento **ISAKMP:(1002): hablando a otro cuadro del IOS** ISAKMP:(1002): carga útil de ID del proveedor de procesamiento ISAKMP:(1002): ID del proveedor parece Unity/DPD pero la mayor discordancia 225 ISAKMP:(1002): la ID del proveedor es XAUTH ISAKMP:carga útil recibida tipo 20 **ISAKMP (1002): Su hash no coincide - este nodo fuera de NAT** ISAKMP:carga útil recibida tipo 20 **ISAKMP (1002): No se ha encontrado NAT para sí mismo o par** ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(1002):Estado antiguo = IKE_R_MM3 Nuevo estado = IKE_R_MM3	
El hub envía MM_KEY_EXCH (modo principal 4). El estado ISAKMP cambia de IKE_R_MM3 a IKE_R_MM4.	**ISAKMP:(1002): envío de paquetes a 172.16.1.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH** ISAKMP:(1002):Envío de un paquete IPv4 IKE. ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(1002):Estado antiguo = IKE_R_MM3 Nuevo estado = IKE_R_MM4**	
	ISAKMP (0): paquete recibido desde 172.16.10.1 puerto 500 sport 500 Global (I) MM_SA_SETUP ISAKMP:(0):Entrada = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(0):Estado antiguo = IKE_I_MM3 Nuevo**	MM_SA_SETUP (Mo principal 4) es recibid spoke. El spoke conc que el par es otro dispositivo Cisco IOS

	estado = IKE_I_MM4	no se detecta NAT pa nosotros ni para nues par.
	ISAKMP:(0): procesamiento de carga útil KE. ID de mensaje = 0 ISAKMP:(0): procesamiento de la carga útil NONCE. ID de mensaje = 0 **ISAKMP:(0):clave precompartida de par encontrada que coincide con 172.16.10.1** ISAKMP:(1002): carga útil de ID del proveedor de procesamiento ISAKMP:(1002): ID del proveedor es Unity ISAKMP:(1002): carga útil de ID del proveedor de procesamiento ISAKMP:(1002): ID del proveedor es DPD ISAKMP:(1002): carga útil de ID del proveedor de procesamiento **ISAKMP:(1002): hablando a otro cuadro del IOS** ISAKMP:carga útil recibida tipo 20 **ISAKMP (1002): Su hash no coincide - este nodo fuera de NAT** ISAKMP:carga útil recibida tipo 20 **ISAKMP (1002): No se ha encontrado NAT para sí mismo o par** ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(1002):Estado antiguo = IKE_I_MM4 Nuevo estado = IKE_I_MM4	El estado ISAKMP ca de IKE_I_MM3 a IKE_I_MM4.
	ISAKMP:(1002):Enviar contacto inicial **ISAKMP:(1002):SA está realizando una autenticación de clave previamente compartida mediante el tipo de ID_IPV4_ADDR.** ISAKMP (1002): carga útil de ID siguiente carga útil: 8 type: 1 dirección: 172.16.1.1 protocolo: 17 puerto: 500 longitud: 12 ISAKMP:(1002):Longitud total de la carga útil: 12 **ISAKMP:(1002): envío de paquetes a 172.16.10.1 my_port 500 peer_port 500 (I) MM_KEY_EXCH** ISAKMP:(1002):Envío de un paquete IPv4 IKE. ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(1002):Estado antiguo = IKE_I_MM4 Nuevo estado = IKE_I_MM5**	MM_KEY_EXCH (Mo principal 5) es enviad el spoke. El estado ISAKMP ca de IKE_I_MM4 a IKE_I_MM5.
El hub recibe MM_KEY_EXCH (modo principal 5). El estado ISAKMP cambia de IKE_R_MM4 a IKE_R_MM5. Además, "el par coincide	**ISAKMP (1002): paquete recibido desde 172.16.1.1 puerto 500 sport 500 Global (R) MM_KEY_EXCH** ISAKMP:(1002):Entrada = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(1002):Estado antiguo = IKE_R_MM4 Nuevo estado = IKE_R_MM5**	

con *ninguno* de los perfiles" se ve debido a la falta de un perfil ISAKMP. Dado que este es el caso, ISAKMP no utiliza un perfil.	ISAKMP:(1002): carga útil de ID de procesamiento. ID de mensaje = 0 ISAKMP (1002): carga útil de ID siguiente carga útil: 8 type: 1 dirección: 172.16.1.1 protocolo: 17 puerto: 500 longitud: 12 **ISAKMP:(0): peer coincide con *ninguno* de los perfiles** ISAKMP:(1002): procesamiento de carga útil HASH. ID de mensaje = 0 ISAKMP:(1002): procesando NOTIFICACIÓN INITIAL_CONTACT protocol 1 spi 0, ID de mensaje = 0, sa = 0x6A5BDE8 ISAKMP:(1002):Estado de autenticación SA: autenticado ISAKMP:(1002):SA se ha autenticado con 172.16.1.1 ISAKMP:(1002):Estado de autenticación SA: autenticado ISAKMP:(1002): Procesar contacto inicial, desactive las SA de fase 1 y 2 existentes con el puerto remoto local 172.16.10.1 172.16.1.1 500 **ISAKMP: Intentando insertar un par 172.16.10.1/172.16.1.1/500/, e insertado con éxito 8CACD00.** ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(1002):Estado antiguo = IKE_R_MM5 Nuevo estado = IKE_R_MM5 IPSEC(key_engine): se obtuvo un evento en cola con 1 mensaje KMI ISAKMP:(1002):SA está realizando una autenticación de clave previamente compartida mediante el tipo de ID_IPV4_ADDR. ISAKMP (1002): carga útil de ID siguiente carga útil: 8 type: 1 dirección: 172.16.10.1 protocolo: 17 puerto: 500 longitud: 12 ISAKMP:(1002):Longitud total de la carga útil: 12
El paquete final MM_KEY_EXCH (Modo principal 6) es enviado por el hub. Esto completa la negociación de la fase 1, que significa que este dispositivo está listo para la fase 2 (modo rápido	**ISAKMP:(1002): envío de paquetes a 172.16.1.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH** ISAKMP:(1002):Envío de un paquete IPv4 IKE. ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(1002):Estado antiguo = IKE_R_MM5 Nuevo estado = IKE_P1_COMPLETE**

IPSec). El estado ISAKMP cambia de IKE_R_MM5 a IKE_P1_COMPLETE.	ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE ISAKMP:(1002):Estado antiguo = IKE_P1_COMPLETE Nuevo estado = IKE_P1_COMPLETE	
	ISAKMP (1002): paquete recibido desde 172.16.10.1 puerto 500 sport 500 Global (I) MM_KEY_EXCH ISAKMP:(1002): carga útil de ID de procesamiento. ID de mensaje = 0 ISAKMP (1002): carga útil de ID siguiente carga útil: 8 type: 1 dirección: 172.16.10.1 protocolo: 17 puerto: 500 longitud: 12 **ISAKMP:(0): peer coincide con *ninguno* de los perfiles** ISAKMP:(1002): procesamiento de carga útil HASH. ID de mensaje = 0 ISAKMP:(1002):Estado de autenticación SA: autenticado ISAKMP:(1002):SA se ha autenticado con 172.16.10.1 **ISAKMP: Intentando insertar un peer 172.16.1.1/172.16.10.1/500/, e insertado con éxito 95F6858.** ISAKMP:(1002):Entrada = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(1002):Estado antiguo = IKE_I_MM5 Nuevo estado = IKE_I_MM6** ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(1002):Estado antiguo = IKE_I_MM6 Nuevo estado = IKE_I_MM6 ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(1002):Estado antiguo = IKE_I_MM6 Nuevo estado = IKE_P1_COMPLETE**	El spoke recibe el pa final MM_KEY_EXCH (Modo principal 6). Es completa la negociac la fase 1, que signific este dispositivo está para la fase 2 (modo IPSec). El estado ISAKMP ca de IKE_I_MM5 a IKE_I_MM6, y luego inmediatamente a IKE_P1_COMPLETE Además, "el par coinc con *ninguno* de los perfiles" se ve debido falta de un perfil ISAK Dado que este es el c ISAKMP no utiliza un
FIN DE LA NEGOCIACIÓN ISAKMP (FASE I), INICIO DE LA NEGOCIACIÓN IPSEC (FASE II)		
	ISAKMP:(1002):inicio del intercambio en modo rápido, M-ID de 3464373979 ISAKMP:(1002):El iniciador de QM obtiene spi **ISAKMP:(1002): envío de paquetes a 172.16.10.1 my_port 500 peer_port 500 (I) QM_IDLE** ISAKMP:(1002):Envío de un paquete IPv4 IKE. ISAKMP:(1002):Nodo 3464373979, Entrada = IKE_MESG_INTERNAL, IKE_INIT_QM **ISAKMP:(1002):Estado antiguo = IKE_QM_READY Nuevo estado = IKE_QM_I_QM1** ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE	Se inicia el intercamb modo rápido (fase II, IPSec) y el spoke env primer mensaje QM a

	ISAKMP:(1002):Estado antiguo = IKE_P1_COMPLETE Nuevo estado = IKE_P1_COMPLETE
El hub recibe el primer paquete de modo rápido (QM) que tiene la propuesta IPSec. Los atributos recibidos especifican que: el indicador encaps se establece en 2 (modo de transporte, el indicador 1 sería modo túnel), la duración de SA predeterminada de 3600 segundos y 4608000 kilobytes (0x465000 en hexadecimal), HMAC-SHA para autenticación y 3DES para cifrado. Como estos son los mismos atributos configurados en la configuración local, se acepta la propuesta y se crea el shell de una SA IPSec. Puesto que todavía no se han asociado valores de Índice de parámetros de seguridad (SPI), se trata simplemente de un shell de una SA que todavía no se puede utilizar para pasar tráfico.	**ISAKMP (1002): paquete recibido desde 172.16.1.1 puerto 500 sport 500 Global (R) QM_IDLE** **ISAKMP: set new node -830593317 to QM_IDLE** ISAKMP:(1002): procesamiento de carga útil HASH. ID del mensaje = 3464373979 ISAKMP:(1002): procesamiento de carga útil SA. ID del mensaje = 3464373979 **ISAKMP:(1002):Comprobación de la propuesta IPSec 1** **ISAKMP: Transformar 1, ESP_3DES** **ISAKMP: atributos en transformación:** **ISAKMP: los límites son 2 (Transporte)** **ISAKMP: tipo de vida SA en segundos** **ISAKMP: duración de vida de SA (básica) de 3600** **ISAKMP: tipo de vida SA en kilobytes** **ISAKMP: duración de vida SA (VPI) de 0x0 0x46 0x50 0x0** **ISAKMP: el autenticador es HMAC-SHA** **ISAKMP:(1002):los actos son aceptables.** IPSEC(Validar_propuesta_solicitud): parte 1 de la propuesta IPSEC(Validar_propuesta_solicitud): parte 1 de la propuesta, **(eng clave. msg.) INBOUND local= 172.16.10.1:0, remoto= 172.16.1.1:0,** **local_proxy= 172.16.10.1/255.255.255.255/47/0 (tipo=1),** **remote_proxy= 172.16.1.1/255.255.255.255/47/0 (type=1),** **protocol= ESP, transform= NONE (Transport),** **lifedur= 0s y 0kb,** **spi= 0x0(0), conn_id= 0, keysize= 128, indicadores= 0x0**
Estos son solo mensajes generales del servicio IPSec que dicen que funciona correctamente.	IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): búsqueda de conexión devuelta 0 IPSEC-IFC MGRE/Tu0: crypto_ss_hear_start ya está escuchando **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): búsqueda de conexión devuelta 0 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Activación del túnel inmediatamente. IPSEC-IFC MGRE/Tu0: Adición de la interfaz de túnel 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): Solicitud de escucha correcta
Se crea una entrada de	la inserción de mapa en mapdb AVL falló, el par map

mapa pseudocriptográfico para el protocolo IP 47 (GRE) desde 172.16.10.1 (dirección pública del hub) a 172.16.1.1 (dirección pública de spoke). Se crea una SA/SPI IPSec para el tráfico entrante y saliente con valores de la propuesta aceptada.

```
+ ace ya existe en el mapdb
CRYPTO_SS(TUNNEL SEC): Abrir pasivo,
información de socket: local 172.16.10.1
172.16.10.1/255.255.255.255/0, remote 172.16.1.1
172.16.1.1/255.255.255.255/0, prot 47, ifc Tu0
Crypto mapdb: proxy_match
      src addr : 172.16.10.1
      dst addr : 172.16.1.1
      protocolo: 47
      puerto src: 0
      puerto DST: 0
ISAKMP:(1002): procesamiento de la carga útil
NONCE. ID del mensaje = 3464373979
ISAKMP:(1002): carga útil de ID de procesamiento. ID
del mensaje = 3464373979
ISAKMP:(1002): carga útil de ID de procesamiento. ID
del mensaje = 3464373979
ISAKMP:(1002):QM Responder obtiene spi
ISAKMP:(1002):Nodo 3464373979, Entrada =
IKE_MESG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1002):Estado antiguo = IKE_QM_READY
Nuevo estado = IKE_QM_SPI_STARVE
ISAKMP:(1002): Creación de SAs 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 spi 0xDD2AC2B3 y conn_id 0
      duración de 3600 segundos
      vida útil 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 spi 0x82C3E0C4 y conn_id 0
      duración de 3600 segundos
      vida útil de 4608000 kilobytes
```

El segundo mensaje QM enviado por el hub.

```
ISAKMP:(1002): envío de paquetes a 172.16.1.1
my_port 500 peer_port 500 (R) QM_IDLE
```

Mensaje generado por el servicio IPSec que confirma que la protección del túnel está activa en Tunnel0.

```
ISAKMP:(1002):Envío de un paquete IPv4 IKE.
ISAKMP:(1002):Nodo 3464373979, entrada =
IKE_MESG_INTERNAL, IKE_GOT_SPI
ISAKMP:(1002):Estado antiguo =
IKE_QM_SPI_STARVE Nuevo estado =
IKE_QM_R_QM2
CRYPTO_SS(TUNNEL SEC): Enlace completado de
la aplicación al socket
IPSEC(key_engine): se obtuvo un evento en cola con
1 mensaje KMI
Crypto mapdb: proxy_match
      src addr : 172.16.10.1
      dst addr : 172.16.1.1
      protocolo: 47
      puerto src: 0
      puerto DST: 0
IPSEC(crypto_ipsec_sa_find_ident_head): reconexión
con los mismos proxies y par 172.16.1.1
```

Se ve otro mensaje de creación de SA que tiene las IP de destino, los SPI, los atributos de conjuntos de transformación y la vida útil en kilobytes y segundos restantes.

IPSEC(policy_db_add_ident): src 172.16.10.1, dest 172.16.1.1, dest_port 0

IPSEC(create_sa): sa creado,
(sa) sa_dest= 172.16.10.1, sa_proto= 50,
sa_spi= 0xDD2AC2B3(3710567091),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 3
sa_lifetime(k/sec)= (4536779/3600)
IPSEC(create_sa): sa creado,
(sa) sa_dest= 172.16.1.1, sa_proto= 50,
sa_spi= 0x82C3E0C4(2193875140),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 4
sa_lifetime(k/sec)= (4536779/3600)
IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce): actualización del identificador de túnel0 8B6A0E8 con tun_decap_oce 6A648F0
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): búsqueda de conexión devuelta 8C93888
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): mensaje listo para socket
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): búsqueda de conexión devuelta 8C93888
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): tunnel_protection_socket_up
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Señalización NHRP
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Mensaje MTU obtenido 1458
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): búsqueda de conexión devuelta 8C93888
ISAKMP (1002): paquete recibido de 172.16.10.1 puerto 500 sport 500 Global (I) QM_IDLE
ISAKMP:(1002): procesamiento de carga útil HASH. ID del mensaje = 3464373979
ISAKMP:(1002): procesamiento de carga útil SA. ID del mensaje = 3464373979
ISAKMP:(1002):Comprobación de la propuesta IPSec 1
ISAKMP: Transformar 1, ESP_3DES
ISAKMP: atributos en transformación:
ISAKMP: los límites son 2 (Transporte)
ISAKMP: tipo de vida SA en segundos
ISAKMP: duración de vida de SA (básica) de 3600
ISAKMP: tipo de vida SA en kilobytes
ISAKMP: duración de vida SA (VPI) de 0x0 0x46 0x50 0x0
ISAKMP: el autenticador es HMAC-SHA
ISAKMP:(1002):los actos son aceptables.
IPSEC(Validar_propuesta_solicitud): parte 1 de la propuesta
IPSEC(Validar_propuesta_solicitud): parte 1 de la propuesta,
(eng clave. msg.) INBOUND local= 172.16.1.1:0,

El spoke recibe el se
paquete QM que tien
propuesta IPSec. Est
confirma que el hub r
QM1. Los atributos
recibidos especifican
el indicador encaps s
establece en 2 (modo
transporte, el indicad
sería modo túnel), la
duración de SA
predeterminada de 3
segundos y 4608000
kilobytes (0x465000 e
hexadecimal), HMAC
para autenticación y
para cifrado. Como e
son los mismos atribu
configurados en la
configuración local, s
acepta la propuesta y
crea el shell de una S
IPSec. Puesto que to

remoto= 172.16.10.1:0, **local_proxy= 172.16.1.1/255.255.255.255/47/0 (tipo=1),** **remote_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1),** **protocol= ESP, transform= NONE (Transport),** **lifedur= 0s y 0kb,** **spi= 0x0(0), conn_id= 0, keysize= 128, indicadores= 0x0**	no se han asociado v de Índice de paráme seguridad (SPI), se t simplemente de un s una SA que todavía puede utilizar para pa tráfico.
Crypto mapdb: proxy_match **src addr : 172.16.1.1** **dst addr : 172.16.10.1** **protocolo: 47** **puerto src: 0** **puerto DST: 0**	La entrada de mapa pseudocriptográfico s para el protocolo IP 4 (GRE) desde 172.16. (dirección pública del a 172.16.1.1 (direcci pública del spoke).
ISAKMP:(1002): procesamiento de la carga útil NONCE. ID del mensaje = 3464373979 ISAKMP:(1002): carga útil de ID de procesamiento. ID del mensaje = 3464373979 ISAKMP:(1002): carga útil de ID de procesamiento. ID del mensaje = 3464373979	Se crea una SA/SPI para el tráfico entrant saliente con valores propuesta aceptada.
ISAKMP:(1002): Creación de SAs 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 spi 0x82C3E0C4 y conn_id 0** **duración de 3600 segundos** **vida útil 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 spi 0xDD2AC2B3 y conn_id 0** **duración de 3600 segundos** **vida útil de 4608000 kilobytes**	
ISAKMP:(1002): envío de paquetes a 172.16.10.1 my_port 500 peer_port 500 (I) QM_IDLE ISAKMP:(1002):Envío de un paquete IPv4 IKE. ISAKMP:(1002):eliminación del nodo -830593317 error FRASE razón "Sin error" ISAKMP:(1002):Nodo 3464373979, Entrada = IKE_MESG_FROM_PEER, IKE_QM_EXCH **ISAKMP:(1002):Estado antiguo = IKE_QM_I_QM1 Nuevo estado = IKE_QM_PHASE2_COMPLETE** IPSEC(key_engine): se obtuvo un evento en cola con 1 mensaje KMI	El spoke envía el terc último mensaje QM a que completa el intercambio QM. A diferencia de ISAKM donde cada par pasa cada estado (MM1 a MM6/P1_COMPLETE IPSec es un poco dif ya que hay sólo tres mensajes en lugar de
Crypto mapdb: proxy_match src addr : 172.16.1.1 dst addr : 172.16.10.1 protocolo: 47 puerto src: 0 puerto DST: 0 IPSEC(crypto_ipsec_sa_find_ident_head): reconexión con los mismos proxies y peer 172.16.10.1 IPSEC(policy_db_add_ident): src 172.16.1.1, dest 172.16.10.1, dest_port 0	El iniciador (nuestro s en este caso, como l indica la "I" en el me IKE_QM_I_QM1) va QM_READY, luego a QM_I_QM1 directam QM_PHASE2_COMP El respondedor (hub) a QM_READY, QM_SPI_STARVE,

	IPSEC(create_sa): sa creado, (sa) sa_dest= 172.16.1.1, sa_proto= 50, sa_spi= 0x82C3E0C4(2193875140), sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 3 sa_lifetime(k/sec)= (4499172/3600) **IPSEC(create_sa): sa creado,** (sa) sa_dest= 172.16.10.1, sa_proto= 50, sa_spi= 0xDD2AC2B3(3710567091), sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 4 sa_lifetime(k/sec)= (4499172/3600) **IPSEC(update_current_outbound_sa): get enable SA peer 172.16.10.1 current outbound sa to SPI DD2AC2B3** **IPSEC(update_current_outbound_sa): actualizado peer 172.16.10.1 actual saliente a SPI DD2AC2B3** IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce): actualización del identificador Tunnel0 94F2740 con tun_decap_oce 794ED30 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): búsqueda de conexión 961D220 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): tunnel_protection_socket_up IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Señalización NHRP NHRP: Túnel NHS 10.1.1.254 vrf 0 Clúster 0 Prioridad 0 Trasladado a 'E' desde ' IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): búsqueda de conexión 961D220 NHRP: Intentando enviar el paquete a través del DEST 10.1.1.254	QM_R_QM2, QM_PHASE2_COMP Se ve otro mensaje d creación de SA que t las IP de destino, los los atributos de conju de transformación y l útil en kilobytes y seg restantes.
Estos mensajes QM finales confirman que el modo rápido está completo y que IPSec está activo en ambos lados del túnel. A diferencia de ISAKMP, donde cada par pasa por cada estado (MM1 a MM6/P1_COMPLETE), IPSec es un poco diferente ya que hay sólo tres mensajes en lugar de seis. El Respondedor (nuestro hub en este caso, como lo indica la "R" en el mensaje IKE_QM_**R**_QM1) va a QM_READY, QM_SPI_STARVE, QM_R_QM2, QM_PHASE2_COMPLETE. El iniciador (spoke) pasa	**ISAKMP (1002): paquete recibido desde 172.16.1.1 puerto 500 sport 500 Global (R) QM_IDLE** ISAKMP:(1002):eliminación del nodo -830593317 error FRASE razón "QM done (await)" ISAKMP:(1002):Nodo 3464373979, Entrada = IKE_MESG_FROM_PEER, IKE_QM_EXCH **ISAKMP:(1002):Estado antiguo = IKE_QM_R_QM2 Nuevo estado = IKE_QM_PHASE2_COMPLETE** IPSEC(key_engine): se obtuvo un evento en cola con 1 mensaje KMI IPSEC(key_engine_enable_outbound): recd habilitar notificación de ISAKMP **IPSEC(key_engine_enable_outbound): enable SA con spi 2193875140/50** **IPSEC(update_current_outbound_sa): get enable SA peer 172.16.1.1 current outbound sa to SPI 82C3E0C4** **IPSEC(update_current_outbound_sa): actualización del peer 172.16.1.1 actual saliente a SPI 82C3E0C4**	

de QM_READY y luego a QM_I_QM1 directamente a QM_PHASE2_COMPLETE.

NHRP: Enviar solicitud de registro a través del túnel0 vrf 0, tamaño del paquete: 108
src: 10.1.1.1, dst: 10.1.1.254
(F) Fn: IPv4(1), tipo: IP(800), salto: 255, ver: 1
shtl: 4(NSAP), stl: 0(NSAP)
pktsz: 108 Extoff: 52
(M) indicadores: "nat único", se requiere: 65540
src NBMA: 172.16.1.1
protocolo src: 10.1.1.1, protocolo dst: 10.1.1.254
(C-1) código: no error(0)
prefijo: 32, mtu: 17912, hd_time: 7200
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
Extensión de dirección del respondedor(3):
Extensión de registro NHS de tránsito directo(4):
Extensión del registro NHS de tránsito inverso(5):
Extensión de autenticación(7):
tipo:Cleartext(1), data:NHRPAUTH
Extensión de dirección NAT(9):
(C-1) código: no error(0)
prefijo: 32, mtu: 17912, hd_time: 0
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0
NBMA del cliente: 172.16.10.1
protocolo de cliente: 10.1.1.254

Estas son las solicitu registro NHRP enviad hub en un intento de registrarse en el NHS hub). Es normal ver múltiplos de estos, pu spoke continúa intent registrarse en el NHS que recibe una "respu de registro".
src,dst: Direcciones I origen de túnel (spok de destino (hub). Ést el origen y el destino paquete GRE enviad el router
SRC NBMA: la direcc NBMA (internet) del s que envió este paque intenta registrarse en NHS
protocolo src: direcci túnel del spoke que i registrarse
protocolo dst: direcci túnel del NHS/hub
Extensión de autentic datos y punto; caden autenticación NHRP
NBMA del cliente: Dirección NBMA del NHS/hub
protocolo de cliente: dirección de túnel del NHS/hub

NHRP-RATE: Envío de la solicitud de registro inicial para 10.1.1.254, requerida 65540
%LINK-3-UPDOWN: Interface Tunnel0, estado cambiado a up
NHRP: if_up: Tunnel0 proto 0
NHRP: Túnel0: Actualización de caché para el destino 10.1.1.254/32 salto siguiente 10.1.1.254
172.16.10.1
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): búsqueda de conexión 961D220
NHRP: Intentando enviar el paquete a través del DEST 10.1.1.254

IPSEC-IFC GRE/Tu0: túnel que se aproxima
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):

Más mensajes de ser NHRP que dicen que solicitud de registro i se envió al NHS en 10.1.1.254. También una confirmación de agregó una entrada c caché para la IP 10.1.1.254/24 del tún vive en NBMA 172.16
El mensaje retrasado que el túnel ha sido " shut" se ve aquí.
Estos son mensajes generales del servicio

búsqueda de conexión 961D220
IPSEC-IFC GRE/Tu0: crypto_ss_hear_start ya está escuchando
IPSEC-IFC GRE/Tu0: crypto_ss_hear_start ya está escuchando
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): búsqueda de conexión 961D220
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): El socket ya está abierto. Ignorando.
%LINEPROTO-5-UPDOWN: Protocolo de línea en la interfaz Tunnel0, estado cambiado a activo

IPSec que dicen que funciona correctamer Aquí es donde finalm se ve que el protocol túnel está activo.

Estas son las solicitudes de registro NHRP recibidas del spoke en un intento de registrarse en el NHS (el hub). Es normal ver múltiplos de estos, pues el spoke continúa intentando registrarse en el NHS hasta que recibe una "respuesta de registro".

NHRP: Recibir solicitud de registro a través del túnel0 vrf 0, tamaño del paquete: 108
(F) Fn: IPv4(1), tipo: IP(800), salto: 255, ver: 1
shtl: 4(NSAP), stl: 0(NSAP)
pktsz: 108 Extoff: 52
(M) indicadores: "nat único", se requiere: 65540
src NBMA: 172.16.1.1
protocolo src: 10.1.1.1, protocolo dst: 10.1.1.254
(C-1) código: no error(0)
prefijo: 32, mtu: 17912, hd_time: 7200
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
Extensión de dirección del respondedor(3):
Extensión de registro NHS de tránsito directo(4):
Extensión del registro NHS de tránsito inverso(5):
Extensión de autenticación(7): tipo:Cleartext(1), data:NHRPAUTH
Extensión de dirección NAT(9):
(C-1) código: no error(0)
prefijo: 32, mtu: 17912, hd_time: 0
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0
NBMA del cliente: 172.16.10.1
protocolo de cliente: 10.1.1.254

SRC NBMA: la dirección NBMA (internet) del spoke que envió este paquete e intenta registrarse en el NHS
protocolo src: dirección de túnel del spoke que intenta registrarse
protocolo dst: dirección de túnel del NHS/hub
Extensión de autenticación, datos y punto; cadena de autenticación NHRP
NBMA del cliente: Dirección NBMA del NHS/hub
protocolo de cliente: dirección de túnel del NHS/hub

Los paquetes de depuración NHRP agregan la red de destino 10.1.1.1/32 disponible a través del salto siguiente de 10.1.1.1 en NHRP de 172.16.1.1. 172.16.1.1 también se agrega a la lista de direcciones a las que el hub reenvía el tráfico multicast.

NHRP: netid_in = 1, to_us = 1
NHRP: Túnel0: Agregación de caché para el destino 10.1.1.1/32 salto siguiente 10.1.1.1 172.16.1.1
NHRP: Adición de Terminales de Túnel (VPN: 10.1.1.1, NBMA: 172.16.1.1)
NHRP: Subbloque NHRP conectado correctamente para terminales de túnel (VPN: 10.1.1.1, NBMA: 172.16.1.1)
NHRP: Nodo de subbloque insertado para la memoria caché: Nodo de subbloque insertado de destino para

Estos mensajes confirman que el registro fue exitoso, al igual que una resolución para la dirección del túnel radial.

la memoria caché: Objetivo 10.1.1.1/32nhop 10.1.1.1
NHRP: Entrada de caché dinámica interna convertida para la interfaz 10.1.1.1/32 Tunnel0 a externa
NHRP: Tu0: Creación de NBMA de asignación de multidifusión dinámica: 172.16.1.1
NHRP: Asignación de multidifusión dinámica añadida para NBMA: 172.16.1.1
NHRP: Actualización de nuestra memoria caché con NBMA: 172.16.10.1, NBMA_ALT: 172.16.10.1
NHRP: Nueva longitud obligatoria: 32
NHRP: Intentando enviar el paquete a través de DEST 10.1.1.1
NHRP: NHRP resolvió correctamente 10.1.1.1 a NBMA 172.16.1.1
NHRP: Encapsulación correcta. Tunnel IP addr 172.16.1.1

Esta es la respuesta de registro NHRP enviada por el hub al spoke en respuesta a la "Solicitud de registro NHRP" recibida anteriormente. Al igual que los demás paquetes de registro, el hub envía múltiplos de estos en respuesta a las múltiples solicitudes.
src,dst: Direcciones IP de origen de túnel (hub) y de destino (spoke). Éstos son el origen y el destino del paquete GRE enviado por el router
SRC NBMA: Dirección NBMA (Internet) del spoke
protocolo src: dirección de túnel del spoke que intenta registrarse
protocolo dst: dirección de túnel del NHS/hub
NBMA del cliente: Dirección NBMA del NHS/hub
protocolo de cliente: dirección de túnel del NHS/hub
Extensión de autenticación, datos y punto; cadena de autenticación NHRP

NHRP: Enviar respuesta de registro a través del túnel0 vrf 0, tamaño del paquete: 128
src: 10.1.1.254, dst: 10.1.1.1
(F) Fn: IPv4(1), tipo: IP(800), salto: 255, ver: 1
shtl: 4(NSAP), stl: 0(NSAP)
pktsz: 128 extinto: 52
(M) indicadores: "nat único", se requiere: 65540
src NBMA: 172.16.1.1
protocolo src: 10.1.1.1, protocolo dst: 10.1.1.254
(C-1) código: no error(0)
prefijo: 32, mtu: 17912, hd_time: 7200
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
Extensión de dirección del respondedor(3):
(C) código: no error(0)
prefijo: 32, mtu: 17912, hd_time: 7200
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0
NBMA del cliente: 172.16.10.1
protocolo de cliente: 10.1.1.254
Extensión de registro NHS de tránsito directo(4):
Extensión del registro NHS de tránsito inverso(5):
Extensión de autenticación(7):
tipo:Cleartext(1), data:NHRPAUTH
Extensión de dirección NAT(9):
(C-1) código: no error(0)
prefijo: 32, mtu: 17912, hd_time: 0
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0
NBMA del cliente: 172.16.10.1
protocolo de cliente: 10.1.1.254

NHRP: Recibir respuesta de registro a través del túnel0 vrf 0, tamaño del paquete: 128
(F) Fn: IPv4(1), tipo: IP(800), salto: 255, ver: 1
shtl: 4(NSAP), stl: 0(NSAP)

Esta es la respuesta
registro NHRP enviad
el hub al spoke en
respuesta a la "Solici

	pktsz: 128 extinto: 52 (M) indicadores: "nat único", se requiere: 65541 **src NBMA: 172.16.1.1** **protocolo src: 10.1.1.1, protocolo dst: 10.1.1.254** (C-1) código: no error(0) prefijo: 32, mtu: 17912, hd_time: 7200 addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0 Extensión de dirección del respondedor(3): (C) código: no error(0) prefijo: 32, mtu: 17912, hd_time: 7200 addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0 **NBMA del cliente: 172.16.10.1** **protocolo de cliente: 10.1.1.254** Extensión de registro NHS de tránsito directo(4): Extensión del registro NHS de tránsito inverso(5): **Extensión de autenticación(7):** **tipo:Cleartext(1), data:NHRPAUTH** Extensión de dirección NAT(9): (C-1) código: no error(0) prefijo: 32, mtu: 17912, hd_time: 0 addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0 **NBMA del cliente: 172.16.10.1** **protocolo de cliente: 10.1.1.254**	registro NHRP" recib anteriormente. Al igu los demás paquetes registro, el hub envía múltiplos de estos en respuesta a las múlti solicitudes. **SRC NBMA**: Direcció NBMA (Internet) del s **protocolo src**: direcci túnel del spoke que i registrarse **protocolo dst**: direcci túnel del NHS/hub **NBMA del cliente**: Dirección NBMA del NHS/hub **protocolo de cliente**: dirección de túnel de NHS/hub **Extensión de autentic** datos y punto; caden autenticación NHRP
Mensajes de servicio IPSec más generales que dicen que funciona correctamente.	NHRP: netid_in = 0, to_us = 1 IPSEC-IFC MGRE/Tu0: crypto_ss_hear_start ya está escuchando 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): búsqueda de conexión devuelta 8C93888 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): El socket ya está abierto. Ignorando. 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	Mensajes de servicio NHRP que dicen que NHS ubicado en 10.1 está activo.
Mensaje del sistema que indica que la adyacencia EIGRP está activa con el spoke vecino en 10.1.1.1.	%DUAL-5-NBRCHANGE: EIGRP-IPv4 1: El Vecino 10.1.1.1 (Túnel0) está activo: nueva adyacencia	
	%DUAL-5-NBRCHANGE: EIGRP-IPv4 1: El vecino 10.1.1.254 (túnel0) está activo: nueva adyacencia	Mensaje del sistema indica que la adyacen EIGRP está activa co hub vecino en 10.1.1
Mensaje del sistema que confirma una resolución NHRP exitosa.	NHRP: NHRP resolvió correctamente 10.1.1.1 a NBMA 172.16.1.1	

Confirmar funcionalidad y solucionar problemas

Esta sección tiene algunos de los comandos **show** más útiles utilizados para resolver problemas tanto del hub como del spoke. Para habilitar depuraciones más específicas, utilice estas condiciones de depuración:

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

show crypto sockets

```
Spoke1#show crypto sockets

Number of Crypto Socket connections 1

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

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

Hub#show crypto sockets

Number of Crypto Socket connections 1

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

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

show crypto session detail

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

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

Interface: Tunnel0
Uptime: 00:01:01
Session status: UP-ACTIVE
Peer: 172.16.10.1 port 500 fvrf: (none) ivrf: (none)
Phase1_id: 172.16.10.1
Desc: (none)
IKEv1 SA: local 172.16.1.1/500 remote 172.16.10.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:58
```

```
IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.10.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 25 drop 0 life (KB/Sec) 4596087/3538
Outbound: #pkts enc'ed 25 drop 3 life (KB/Sec) 4596087/3538

Hub#show crypto session detail
Crypto session current status

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

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

show crypto isakmp sa detail

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

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

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

IPv6 Crypto ISAKMP SA

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

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

IPv6 Crypto ISAKMP SA
```

show crypto ipsec sa detail

```
Spoke1#show crypto ipsec sa detail
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 172.16.1.1
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.10.1/255.255.255.255/47/0)
current_peer 172.16.10.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 24, #pkts encrypt: 24, #pkts digest: 24
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#pkts no sa (send) 3, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

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

inbound esp sas:
spi: 0x8D538D11(2371063057)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport,}
conn id: 1, flow_id: SW:1, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4596087/3543)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

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

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

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

```
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

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

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

inbound ah sas:

inbound pcp sas:

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

outbound ah sas:
outbound pcp sas:
```

show ip nhrp

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

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

show ip nhs

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

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

show dmvpn [detail]

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

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

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

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

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

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

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

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


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

Pending DMVPN Sessions:
```

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

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

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

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

Pending DMVPN Sessions:
```

Información Relacionada

- Resolución de problemas de IPsec: Introducción y uso de los comandos debug
- Cifrado de última generación
- RFC3706: Detección de par muerto IKE
- RFC3947: IKE NAT transversal
- Soporte Técnico y Documentación - Cisco Systems