Guida alla risoluzione dei problemi relativi ai debug di DMVPN fase 1

Sommario

Introduzione

In questo documento vengono descritti i messaggi di debug che verrebbero visualizzati sull'hub e in una distribuzione DMVPN (Dynamic Multipoint Virtual Private Network) di fase 1.

Prerequisiti

Per i comandi di configurazione e debug illustrati in questo documento, sono necessari due router Cisco con Cisco IOS® versione 12.4(9)T o successive. In generale, una DMVPN di base della fase 1 richiede Cisco IOS versione 12.2(13)T o successive o la versione 12.2(33)XNC per Aggregation Services Router (ASR), anche se le funzionalità e i debug menzionati in questo documento potrebbero non essere supportati.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- GRE (Generic Routing Encapsulation)
- Protocollo NHRP (Next Hop Resolution Protocol)
- Protocollo ISAKMP (Internet Security Association and Key Management Protocol)
- IKE (Internet Key Exchange)
- IPSec (Internet Protocol Security)
- Almeno uno dei seguenti protocolli di routing: Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Routing Information Protocol (RIP) e Border Gateway Protocol (BGP)

Componenti usati

Per questo documento, sono stati usati Cisco 2911 Integrated Services Router (ISR) con Cisco IOS versione 15.1(4)M4.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Miglioramenti significativi

Queste versioni di Cisco IOS hanno introdotto funzionalità significative o correzioni per DMVPN Fase 1:

- Release 12.2(18)SXF5 - migliore supporto per ISAKMP quando si utilizza l'infrastruttura a chiave pubblica (PKI)
- Release 12.2(33)XNE - ASR, profili IPSec, protezione tunnel, attraversamento NAT (Network Address Translation) IPSec
- Release 12.3(7)T - Supporto iVRF (Virtual Routing and Forwarding) interno
- Release 12.3(11)T - Supporto fVRF (Front-Door Virtual Routing and Forwarding)
- Release 12.4(9)T - supporto per vari debug e comandi relativi a DMVPN
- Release 12.4(15)T - Protezione tunnel condiviso
- Release 12.4(20)T - IPv6 over DMVPN
- Release 15.0(1)M - Monitoraggio dello stato del tunnel NHRP

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

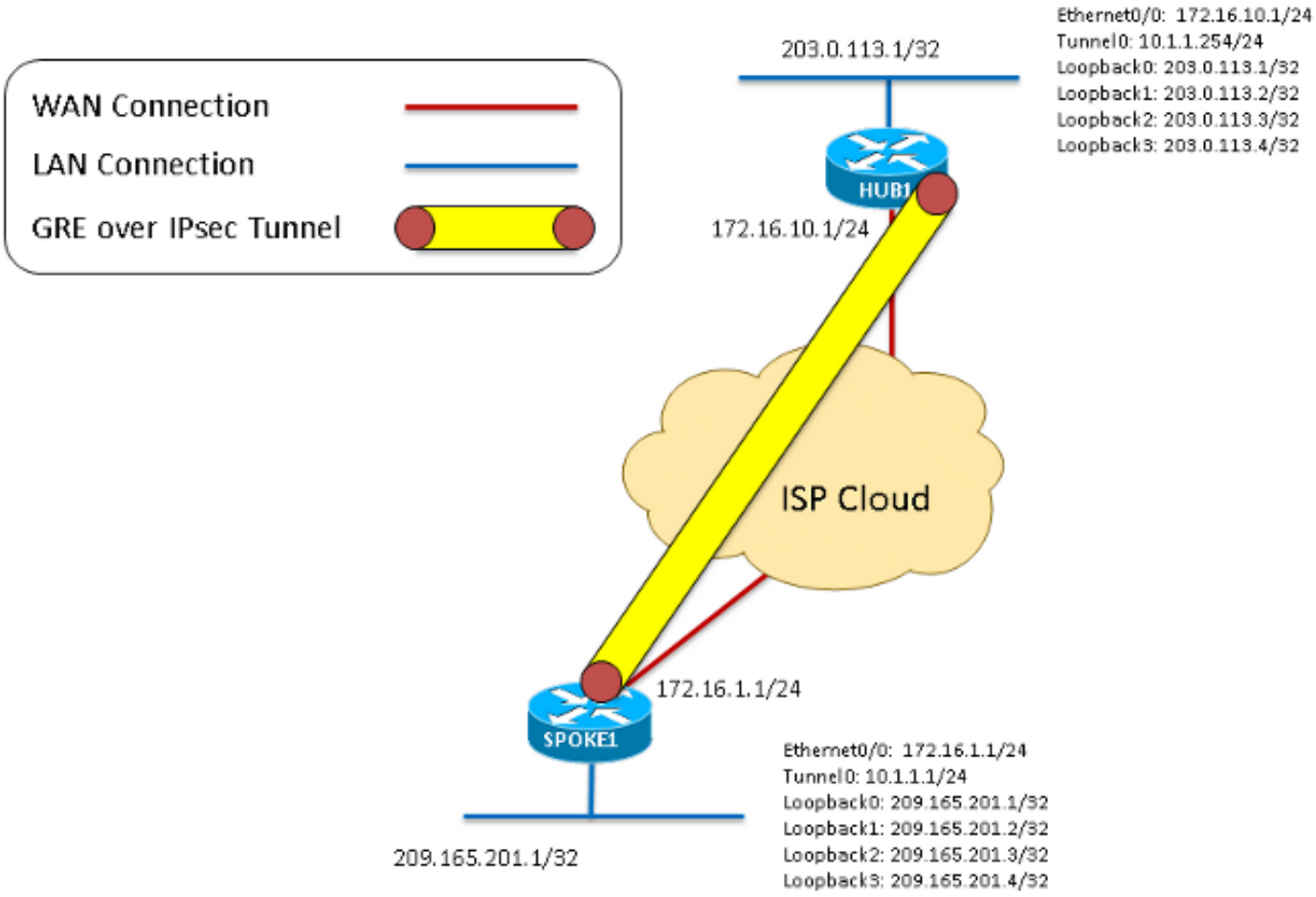
Configurazione rilevante

Panoramica della topologia

Per questa topologia, due ISR 2911 con versione 15.1(4)M4 sono stati configurati per DMVPN fase 1: uno come hub e uno come spoke. Ethernet0/0 è stata utilizzata come interfaccia "Internet"

su ciascun router. Le quattro interfacce di loopback sono configurate per simulare le reti locali che risiedono nel sito hub o spoke. Poiché si tratta di una topologia DMVPN fase 1 con un solo spoke, il spoke è configurato con un tunnel GRE point-to-point anziché multipoint. la stessa configurazione crittografica (ISAKMP e IPSec) è stata utilizzata su ciascun router per garantire una corrispondenza esatta.

Diagramma 1



Crittografia

Questo è lo stesso sul hub e sul 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
```

Raggi

```
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
```

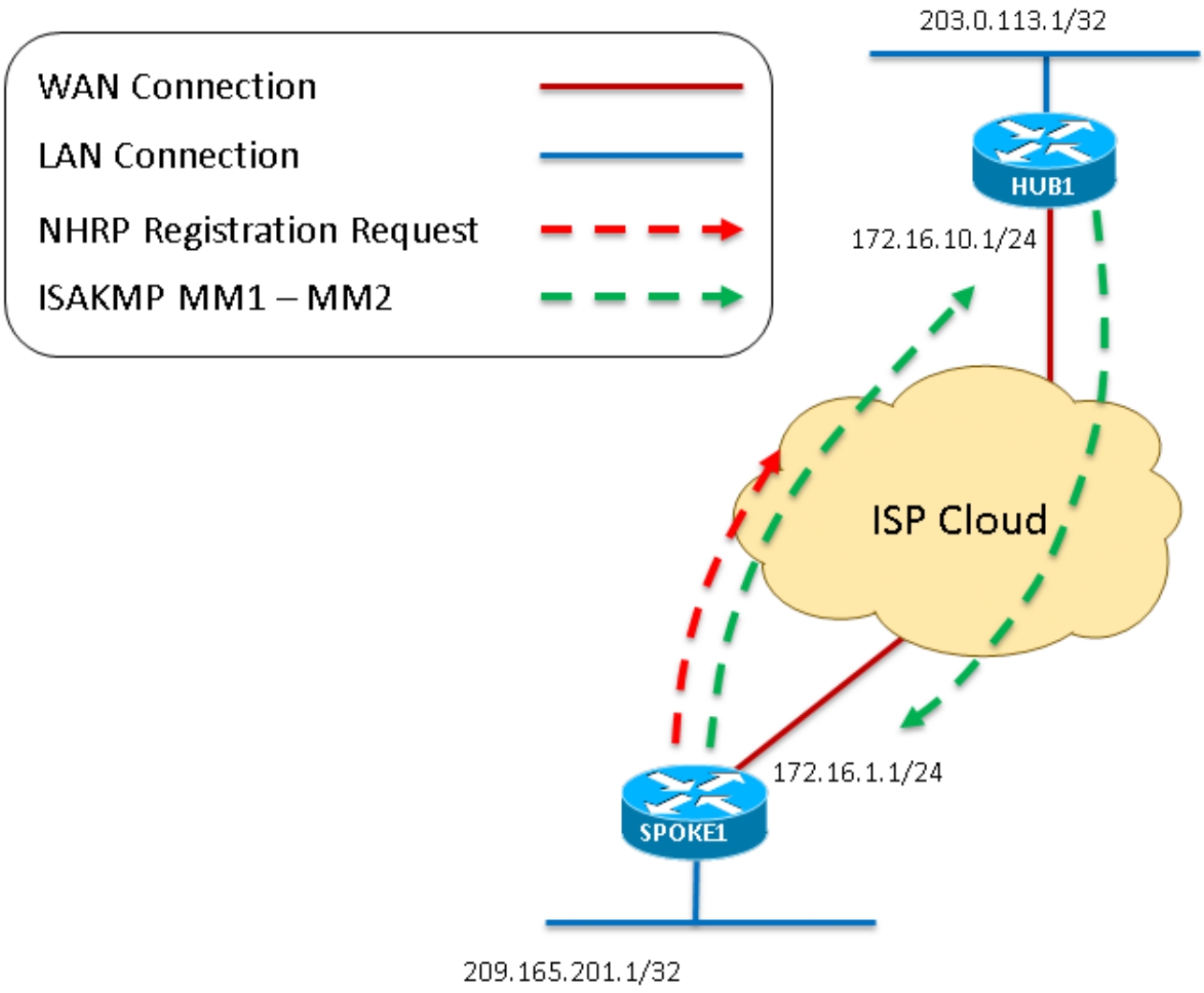
```
network 209.165.201.2 0.0.0.0
network 209.165.201.3 0.0.0.0
network 209.165.201.4 0.0.0.0
network 10.1.1.0 0.0.0.255
```

Debug

Visualizzazione flusso di pacchetti

Questa è una visualizzazione dell'intero flusso di pacchetti DMVPN, come mostrato in questo documento. Sono inoltre inclusi debug più dettagliati che illustrano i singoli passaggi.

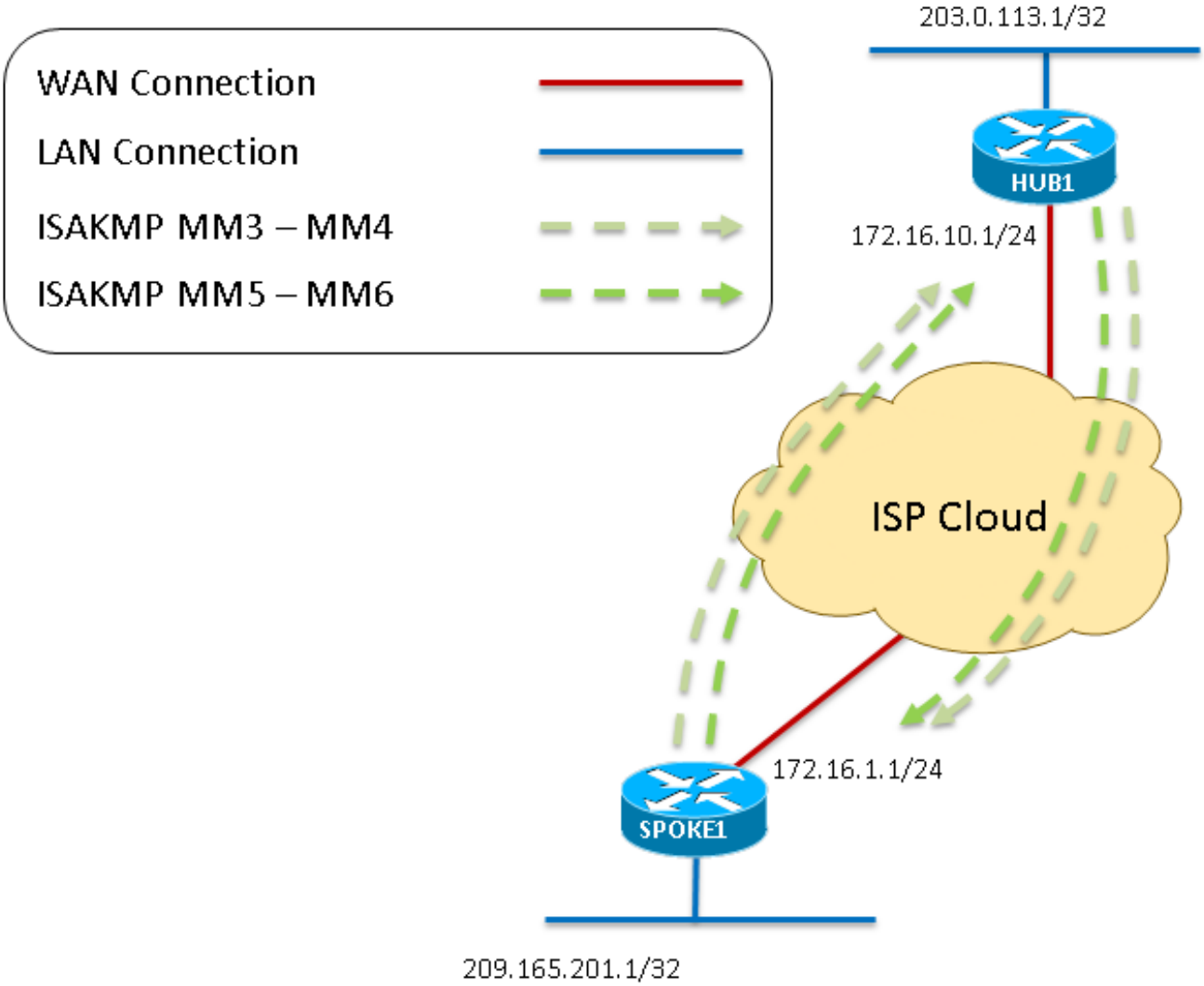
1. Quando il tunnel sul spoke è "no shutdown", genera una richiesta di registrazione NHRP, che avvia il processo DMVPN. Poiché la configurazione dell'hub è completamente dinamica, lo spoke deve essere l'endpoint che avvia la connessione.
2. La richiesta di registrazione NHRP viene quindi incapsulata nel GRE e ciò attiva l'avvio del processo di crittografia.
3. A questo punto, il primo messaggio ISAKMP in modalità principale - ISAKMP MM1 - viene inviato dal spoke all'hub sulla porta UDP500.
4. L'hub riceve ed elabora MM1 e risponde con ISAKMP MM2, poiché dispone di criteri ISAKMP corrispondenti.
   Diagramma 2 - si riferisce ai punti da 1 a 4



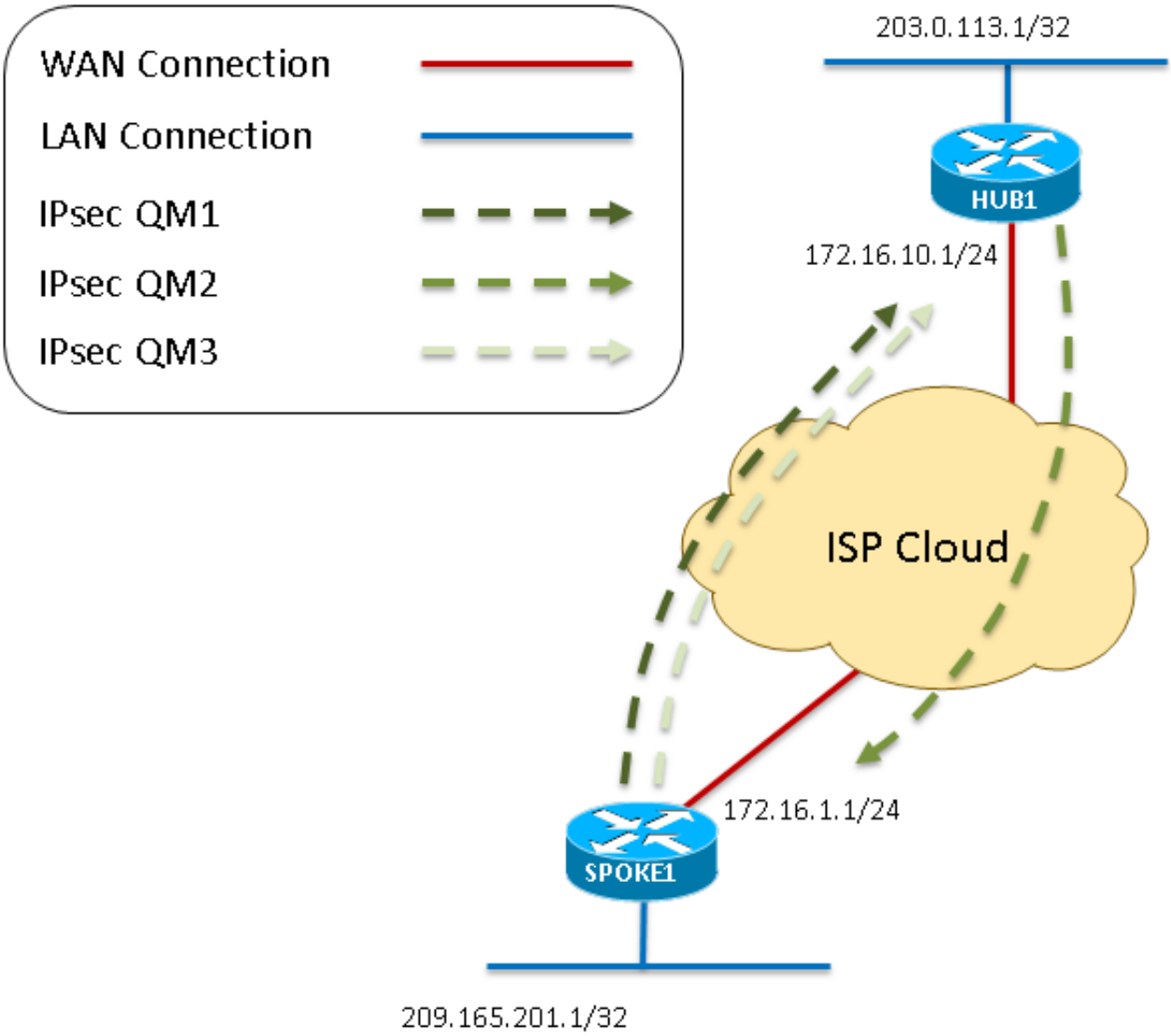
5. Una volta che il spoke riceve il MM2, risponde con MM3. Come con MM1, il spoke conferma

che i criteri ISAKMP ricevuti sono validi.

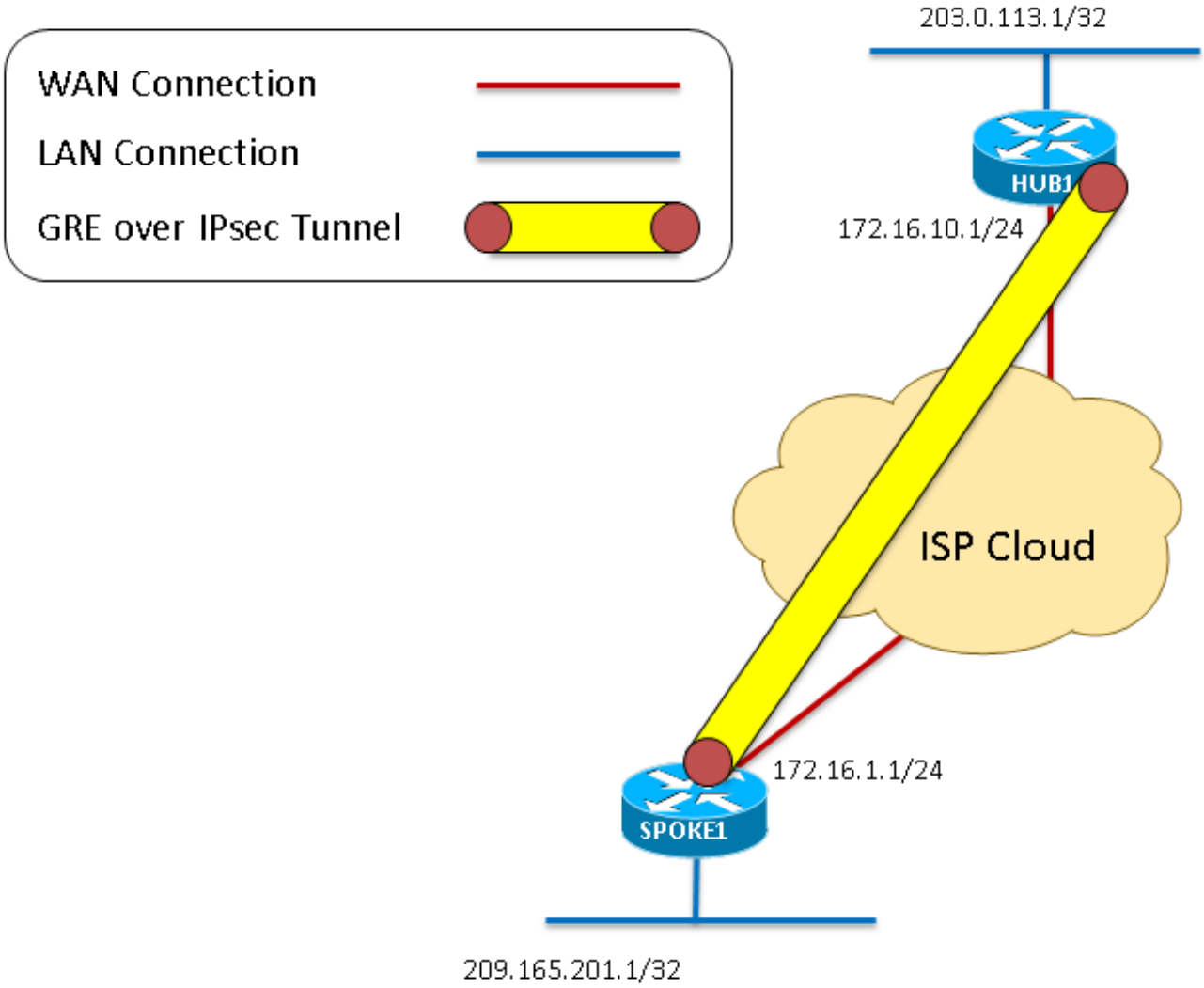
6. L'hub riceve MM3 e risponde con MM4.
7. A questo punto della negoziazione ISAKMP, il spoke potrebbe rispondere sulla porta UDP4500 se viene rilevato NAT nel percorso di transito. Tuttavia, se non viene rilevato alcun NAT, il spoke continua e invia MM5 su UDP500. Infine, l'hub risponde con MM6 per completare lo scambio in modalità principale.
   Diagramma 3 - si riferisce ai punti da 5 a 7



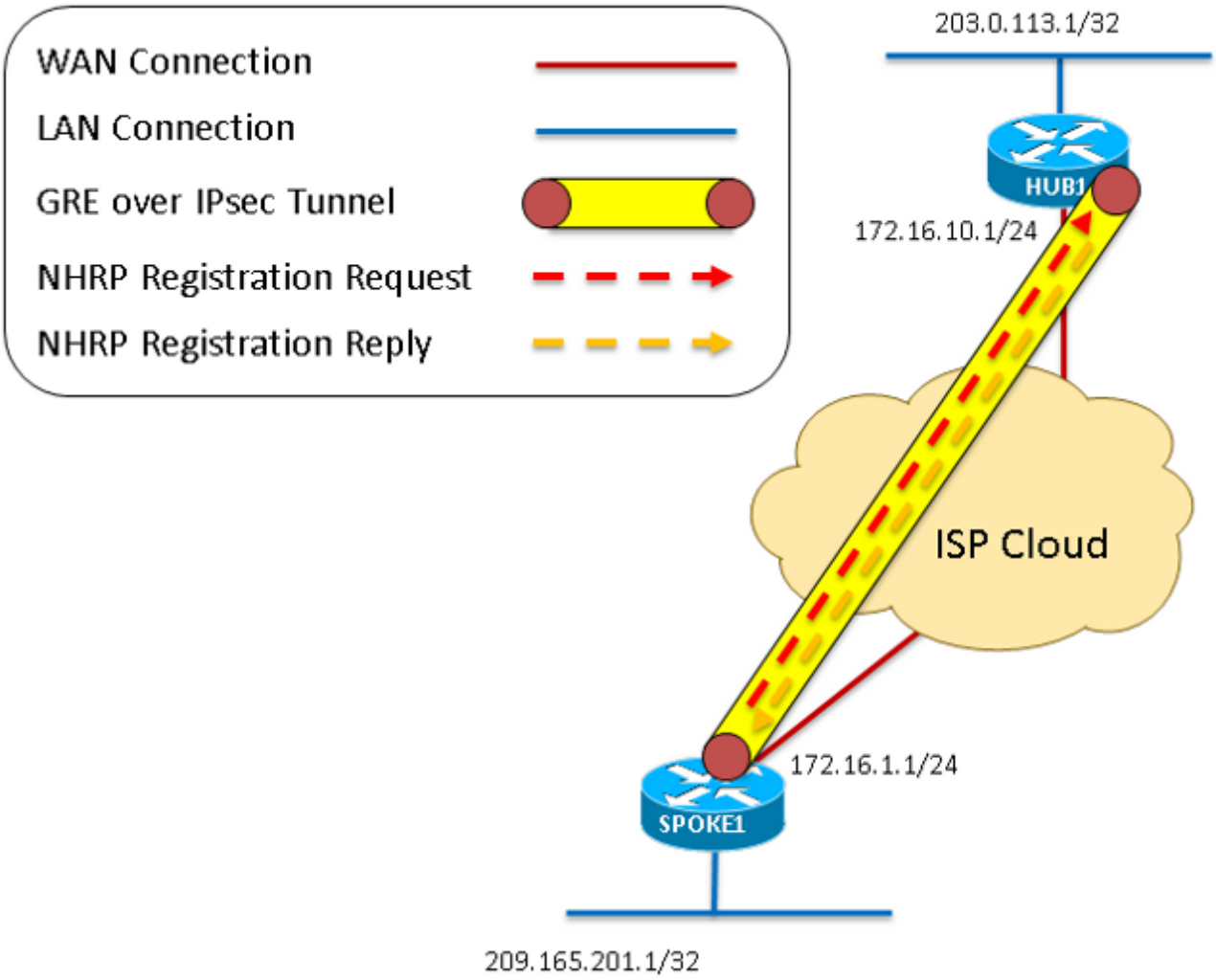
8. Una volta che il spoke riceve MM6 dall'hub, invia QM1 all'hub su UDP500 per avviare la modalità rapida.
9. L'hub riceve QM1 e risponde con QM2, poiché tutti gli attributi ricevuti vengono accettati. A questo punto, l'hub crea le associazioni di sicurezza per la fase 2 per la sessione.
10. Come ultimo passaggio della negoziazione in modalità rapida, QM2 viene ricevuto dal spoke. Spoke crea quindi le SA di fase 2 e invia QM3 in risposta. La negoziazione ISAKMP e IPSec è stata completata. A questo punto, è presente una sessione IPSec che crittografa il traffico GRE tra i due peer.
    Diagramma 4 - si riferisce ai punti da 8 a 10



11. Ora che la sessione crittografica è attiva e può trasmettere il traffico, questi pacchetti vengono incapsulati nel tunnel GRE su IPSec.
    Diagramma 5 - si riferisce al passaggio
    11



12. Come mostrato nei primi passaggi, Spoke genera una richiesta di registrazione NHRP che viene inviata attraverso il tunnel GRE su IPSec.
13. L'hub riceve le richieste di registrazione NHRP e invia una risposta di registrazione NHRP dopo aver confermato che lo spoke ha un indirizzo tunnel e NBMA (Nonbroadcast Multiaccess) valido. Lo spoke riceve questa risposta di registrazione NHRP che completa il processo di registrazione.
    Diagramma 6 - si riferisce ai punti da 12 a
    13



Di seguito vengono riportati i risultati del comando **debug dmvpn all** immesso sui router hub e spoke. Questo particolare comando abilita questo gruppo di debug:

```
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
```

Debug con spiegazione

Trattandosi di una configurazione in cui viene implementato IPSec, i debug mostrano tutti i debug ISAKMP e IPSec. Se non è configurata alcuna crittografia, ignorare i debug che iniziano con "IPsec" o "ISAKMP".

SPIEGAZIONE DEBUG HUB	DEBUG IN SEQUENZA	SPIEGAZIONE DE SPOKE
I primi messaggi di debug sono generati dal comando **no shutdown** immesso sull'interfaccia del tunnel. I messaggi vengono generati dai servizi crypto, GRE e NHRP avviati. Un errore di registrazione NHRP viene visualizzato sull'hub perché non dispone di un server NHS (Next Hop Server) configurato (l'hub è il server NHS per il cloud DMVPN). Questo è previsto.	IPSEC-IFC MGRE/Tu0: Verifica dello stato del tunnel. **NHRP: if_up: Proto tunnel0 0** IPSEC-IFC MGRE/Tu0: tunnel in arrivo IPSEC-IFC MGRE/Tu0: crypto_ss_Listen_start già in ascolto **%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP attivato** **NHRP: Impossibile inviare la registrazione. Nessun servizio NHS configurato** %LINK-3-UPDOWN: Interfaccia Tunnel0, stato modificato in attivo NHRP: if_up: Proto tunnel0 0 NHRP: Impossibile inviare la registrazione. Nessun servizio NHS configurato IPSEC-IFC MGRE/Tu0: tunnel in arrivo IPSEC-IFC MGRE/Tu0: crypto_ss_Listen_start già in ascolto **%LINEPROTO-5-UPDOWN: Protocollo di linea su tunnel di interfaccia0, stato modificato in attivo** IPSEC-IFC GRE/Tu0: Verifica dello stato del tunnel. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): la ricerca della connessione ha restituito 0 **IPSEC-IFC GRE/Tu0: crypto_ss_Listen_start già in ascolto** **IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Apertura di un socket con il profilo DMVPN-IPSEC** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): la ricerca della connessione ha restituito 0 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Avvio immediato del tunnel. IPSEC-IFC GRE/Tu0: Aggiunta dell'interfaccia tunnel Tunnel0 all'elenco condiviso **NHRP: if_up: Proto tunnel0 0** **NHRP: Tunnel0: Aggiunta cache per la destinazione 10.1.1.254/32 next-hop 10.1.1.254** **172.16.10.1** IPSEC-IFC GRE/Tu0: tunnel in arrivo	I primi messaggi di d sono generati dal co **no shutdown** immess sull'interfaccia del tu messaggi vengono g dai servizi crypto, GR NHRP avviati. Inoltre, il spoke aggiu una voce alla propria NHRP per il proprio N e indirizzo del tunnel.

IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): la ricerca della connessione ha restituito 961D220
IPSEC-IFC GRE/Tu0: crypto_ss_Listen_start già in ascolto
IPSEC-IFC GRE/Tu0: crypto_ss_Listen_start già in ascolto
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Apertura di un socket con il profilo DMVPN-IPSEC
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): la ricerca della connessione ha restituito 961D220
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Apertura del socket già in corso. Ignorare.
CRYPTO_SS(SEC TUNNEL): L'applicazione ha avviato l'ascolto
inserimento della mappa nell'AVL di mapdb non riuscito. La coppia mappa + ace esiste già nel mapdb
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP attivato
CRYPTO_SS(SEC TUNNEL): Informazioni sul socket attive e aperte: 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, port 47, ifc Tu0
AVVIO DELLA NEGOZIAZIONE ISAKMP (FASE I)
IPSEC(recalculate_mtu): reimpostare l'mtu sadb_root 94EFDC0 su 1500
IPSEC(sa_request): ,
(chiave eng. msg.) OUTBOUND local= 172.16.1.1:500, remote= 172.16.10.1:500,
local_proxy= 172.16.1.1/255.255.255.255/47/0 (tipo=1),
remote_proxy= 172.16.10.1/255.255.255.255/47/0 (tipo=1),
protocol= ESP, transform= esp-3des esp-sha-hmac (trasporto),
lifedur= 3600 e 4608000 kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flag= 0x0
ISAKMP:(0): Il profilo di richiesta SA è (NULL)
ISAKMP È stato creato uno struct peer per 172.16.10.1, porta peer 500
ISAKMP Nuovo peer creato = 0x95F6858 peer_handle = 0x80000004
ISAKMP Blocco struttura peer 0x95F6858, conteggio aggiornato 1 per isakmp_initiator
ISAKMP local port 500, remote port 500
ISAKMP impostare il nuovo nodo 0 su QM_IDLE
ISAKMP:(0):inserimento sa riuscito = 8A26FB0
ISAKMP:(0): impossibile avviare la modalità aggressiva. Verrà utilizzata la modalità principale.
ISAKMP:(0):trovata chiave già condivisa peer corrispondente a 172.16.10.1
ISAKMP:(0): ID costruito NAT-T vendor-rfc3947
ISAKMP:(0): ID fornitore NAT-T-07 costruito
ISAKMP:(0): ID NAT-T vendor-03 costruito
ISAKMP:(0): ID fornitore NAT-T-02 costruito

Il primo passaggio, q
il tunnel è impostato
shutdown", è avviare
negoziazione crittogr
In questo caso, il spo
crea una richiesta SA
di avviare la modalità
aggressiva e fallisce
modalità principale. L
modalità aggressiva
configurata su nessu
due router, pertanto è
prevista.
Il raggio inizia in mod
principale e invia il pr
messaggio ISAKMP,
MM_NO_STATE. Lo
di ISAKMP passa da
IKE_READY a IKE_I_
I messaggi ID fornito
NAT-T vengono utiliz
nel rilevamento e
nell'attraversamento
NAT. Questi messag
sono attesi durante la
negoziazione di ISAK
indipendentemente d
fatto che NAT sia
implementato o meno
Come i messaggi del
modalità aggressiva,

	ISAKMP:(0):Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM **ISAKMP:(0):Stato precedente = IKE_READY Nuovo stato = IKE_I_MM1**
	ISAKMP:(0): avvio dello scambio in modalità principale **ISAKMP:(0): invio del pacchetto alla porta 172.16.10.1 my_port 500 peer_port 500 (I) MM_NO_STATE** ISAKMP:(0):invio di un pacchetto IPv4 IKE. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): la ricerca della connessione ha restituito 961D220 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): messaggio socket ready valido
Quando il tunnel dello spoke è impostato su "no shutdown", l'hub riceve il messaggio IKE NEW SA (modalità principale 1) sulla porta 500. In qualità di risponditore, l'hub crea un'associazione di sicurezza ISAKMP (SA). Lo stato di ISAKMP passa da IKE_READY a IKE_R_MM1.	**ISAKMP (0): ricevuto pacchetto da 172.16.1.1 dport 500 sport 500 Global (N) NEW SA** **ISAKMP È stato creato uno struct peer per 172.16.1.1, porta peer 500** ISAKMP Nuovo peer creato = 0x8CACD00 peer_handle = 0x80000003 ISAKMP Blocco struttura peer 0x8CACD00, refcount 1 per crypto_isakmp_process_block ISAKMP local port 500, remote port 500 **ISAKMP:(0):inserimento sa riuscito sa = 6A5BDE8** ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(0):Stato precedente = IKE_READY Nuovo stato = IKE_R_MM1**
Viene elaborato il messaggio IKE modalità principale 1 ricevuto. L'hub determina che il peer dispone di attributi ISAKMP corrispondenti e questi vengono inseriti nell'associazione di protezione ISAKMP appena creata. I messaggi mostrano che il peer utilizza 3DES-CBC per la crittografia, l'hashing di SHA, il gruppo Diffie Hellman (DH) 1, la chiave già condivisa per l'autenticazione e la durata predefinita dell'associazione di protezione di 86400 secondi (0x0 0x1 0x51 0x80 = 0x15180 = 86400 secondi). Lo stato ISAKMP è ancora IKE_R_MM1 poiché non è stata inviata una risposta al	ISAKMP:(0): elaborazione del payload SA. ID messaggio = 0 ISAKMP:(0): elaborazione payload id fornitore **ISAKMP:(0): l'ID fornitore sembra Unity/DPD, ma le principali 69 non corrispondono** **ISAKMP (0): l'ID fornitore è NAT-T RFC 3947** ISAKMP:(0): elaborazione payload id fornitore ISAKMP:(0): l'ID fornitore sembra Unity/DPD ma non corrisponde all'ID principale 245 ISAKMP (0): l'ID fornitore è NAT-T v7 ISAKMP:(0): elaborazione payload id fornitore ISAKMP:(0): l'ID fornitore sembra Unity/DPD ma il numero 157 non corrisponde ISAKMP:(0): l'ID fornitore è NAT-T v3 ISAKMP:(0): elaborazione payload id fornitore ISAKMP:(0): l'ID fornitore sembra Unity/DPD ma non corrisponde al numero 123 principale ISAKMP:(0): l'ID fornitore è NAT-T v2 **ISAKMP:(0):trovata chiave già condivisa peer corrispondente a 172.16.1.1** **ISAKMP:(0): chiave locale già condivisa trovata** ISAKMP : Analisi dei profili per xauth in corso... **ISAKMP:(0):Verifica della trasformazione 1 ISAKMP rispetto al criterio di priorità 1** **ISAKMP crittografia 3DES-CBC** **ISAKMP Hash SHA**

questi sono attesi.

spoke.
I messaggi ID fornitore NAT-T vengono utilizzati nel rilevamento e nell'attraversamento di NAT. Questi messaggi sono attesi durante la negoziazione di ISAKMP indipendentemente dal fatto che NAT sia implementato o meno.
Messaggi simili vengono visualizzati per Dead Peer Detection (DPD).

ISAKMP gruppo predefinito 1
ISAKMP auth pre-share
ISAKMP tipo di durata in secondi
ISAKMP durata (VPI) di 0x0 0x1 0x51 0x80
ISAKMP:(0):atts sono accettabili. Il payload successivo è 0
ISAKMP:(0):Acceptable atts:actual life: 0
ISAKMP:(0):Accettabile atts:life: 0
ISAKMP:(0):Riempire atts in sa vpi_length:4
ISAKMP:(0):Riempire atts in sa life_in_seconds:86400
ISAKMP:(0):Restituzione durata effettiva: 86400
ISAKMP:(0)::Avviato timer durata: 86400.

ISAKMP:(0): elaborazione payload id fornitore
ISAKMP:(0): l'ID fornitore sembra Unity/DPD, ma le principali 69 non corrispondono
ISAKMP (0): l'ID fornitore è NAT-T RFC 3947
ISAKMP:(0): elaborazione payload id fornitore
ISAKMP:(0): l'ID fornitore sembra Unity/DPD ma non corrisponde all'ID principale 245
ISAKMP (0): l'ID fornitore è NAT-T v7
ISAKMP:(0): elaborazione payload id fornitore
ISAKMP:(0): l'ID fornitore sembra Unity/DPD ma il numero 157 non corrisponde
ISAKMP:(0): l'ID fornitore è NAT-T v3
ISAKMP:(0): elaborazione payload id fornitore
ISAKMP:(0): l'ID fornitore sembra Unity/DPD ma non corrisponde al numero 123 principale
ISAKMP:(0): l'ID fornitore è NAT-T v2
ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(0):Stato precedente = IKE_R_MM1 Nuovo stato = IKE_R_MM1

MM_SA_SETUP (modalità principale 2) viene inviato al raggio per confermare che MM1 è stato ricevuto e accettato come pacchetto ISAKMP valido.
Lo stato di ISAKMP passa da IKE_R_MM1 a IKE_R_MM2.

ISAKMP:(0): ID costruito NAT-T vendor-rfc3947
ISAKMP:(0): invio del pacchetto alla porta 172.16.1.1 my_port 500 peer_port 500 (R) MM_SA_SETUP
ISAKMP:(0):invio di un pacchetto IPv4 IKE.
ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(0):Stato precedente = IKE_R_MM1 Nuovo stato = IKE_R_MM2

ISAKMP (0): ha ricevuto un pacchetto da 172.16.10.1 dport 500 sport 500 Global (I) MM_NO_STATE
ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):Stato precedente = IKE_I_MM1 Nuovo stato = IKE_I_MM2

ISAKMP:(0): elaborazione del payload SA. ID messaggio = 0
ISAKMP:(0): elaborazione payload id fornitore
ISAKMP:(0): l'ID fornitore sembra Unity/DPD, ma le

In risposta al messag
MM1 inviato all'hub, a
MM2 che conferma la
ricezione di MM1. Vie
elaborato il messaggi
modalità principale 2
ricevuto. Lo spoke si
conto che l'hub peer
attributi ISAKMP
corrispondenti e ques
attributi vengono inse

	principali 69 non corrispondono ISAKMP (0): l'ID fornitore è NAT-T RFC 3947 ISAKMP:(0):trovata chiave già condivisa peer corrispondente a 172.16.10.1 ISAKMP:(0): chiave locale già condivisa trovata ISAKMP : Analisi dei profili per xauth in corso... **ISAKMP:(0):Verifica della trasformazione 1 ISAKMP rispetto al criterio di priorità 1** **ISAKMP crittografia 3DES-CBC** **ISAKMP Hash SHA** **ISAKMP gruppo predefinito 1** **ISAKMP auth pre-share** **ISAKMP tipo di durata in secondi** **ISAKMP durata (VPI) di 0x0 0x1 0x51 0x80** **ISAKMP:(0):atts sono accettabili. Il payload successivo è 0** **ISAKMP:(0):Acceptable atts:actual life: 0** **ISAKMP:(0):Accettabile atts:life: 0** **ISAKMP:(0):Riempire atts in sa vpi_length:4** **ISAKMP:(0):Riempire atts in sa life_in_seconds:86400** **ISAKMP:(0):Restituzione durata effettiva: 86400** **ISAKMP:(0)::Avviato timer durata: 86400.**	nell'associazione di protezione ISAKMP c Questo pacchetto mo che il peer utilizza 3D CBC per la crittografi l'hashing di SHA, il gr Diffie Hellman (DH) 1 chiave già condivisa l'autenticazione e la c predefinita dell'associazione di sicurezza di 86400 se (0x0 0x1 0x51 0x80 = 0x15180 = 86400 sec Oltre ai messaggi NA disponibile uno scam per determinare se la sessione utilizzerà DI Lo stato ISAKMP pas IKE_I_MM1 a IKE_I_M
	ISAKMP:(0): elaborazione payload id fornitore ISAKMP:(0): l'ID fornitore sembra Unity/DPD, ma le principali 69 non corrispondono ISAKMP (0): l'ID fornitore è NAT-T RFC 3947 ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(0):Stato precedente = IKE_I_MM2 Nuovo stato = IKE_I_MM2 **ISAKMP:(0): invio del pacchetto alla porta 172.16.10.1 my_port 500 peer_port 500 (I) MM_SA_SETUP** ISAKMP:(0):invio di un pacchetto IPv4 IKE. ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(0):Stato precedente = IKE_I_MM2 Nuovo stato = IKE_I_MM3**	MM_SA_SETUP (mo principale 3) viene inv all'hub, che conferma raggio ha ricevuto MM desidera procedere. Lo stato ISAKMP pas IKE_I_MM2 a IKE_I_M
MM_SA_SETUP (Modalità principale 3) viene ricevuto dall'hub. L'hub conclude che il peer è un altro dispositivo Cisco IOS e non viene rilevato alcun NAT per noi o per il nostro peer. Lo stato di ISAKMP passa da IKE_R_MM2 a IKE_R_MM3.	**ISAKMP (0): ricevuto pacchetto da 172.16.1.1 dport 500 sport 500 Global (R) MM_SA_SETUP** ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(0):Stato precedente = IKE_R_MM2 Nuovo stato = IKE_R_MM3** ISAKMP:(0): elaborazione payload KE. ID messaggio = 0 ISAKMP:(0): elaborazione del payload NONCE. ID messaggio = 0 **ISAKMP:(0):trovata chiave già condivisa peer corrispondente a 172.16.1.1** ISAKMP (1002): elaborazione payload id fornitore ISAKMP (1002): ID fornitore DPD	

	ISAKMP (1002): elaborazione payload id fornitore **ISAKMP (1002): parlare con un'altra scatola IOS!** ISAKMP (1002): elaborazione payload id fornitore ISAKMP (1002): l'ID fornitore sembra Unity/DPD ma non corrisponde all'ID principale 225 ISAKMP (1002): ID fornitore è XAUTH ISAKMP: tipo payload ricevuto 20 **ISAKMP (1002): Il suo hash non corrisponde - questo nodo al di fuori di NAT** ISAKMP: tipo payload ricevuto 20 **ISAKMP (1002): NAT non trovato per se stesso o peer** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(1002):Vecchio stato = IKE_R_MM3 Nuovo stato = IKE_R_MM3	
MM_KEY_EXCH (Modalità principale 4) viene inviato dall'hub. Lo stato di ISAKMP passa da IKE_R_MM3 a IKE_R_MM4.	**ISAKMP (1002): invio del pacchetto alla porta 172.16.1.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH** ISAKMP:(1002):invio di un pacchetto IPv4 IKE. ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(1002):Vecchio stato = IKE_R_MM3 Nuovo stato = IKE_R_MM4**	
	ISAKMP (0): ha ricevuto un pacchetto da 172.16.10.1 dport 500 sport 500 Global (I) MM_SA_SETUP ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(0):Stato precedente = IKE_I_MM3 Nuovo stato = IKE_I_MM4** ISAKMP:(0): elaborazione payload KE. ID messaggio = 0 ISAKMP:(0): elaborazione del payload NONCE. ID messaggio = 0 **ISAKMP:(0):trovata chiave già condivisa peer corrispondente a 172.16.10.1** ISAKMP (1002): elaborazione payload id fornitore ISAKMP (1002): ID fornitore è Unity ISAKMP (1002): elaborazione payload id fornitore ISAKMP (1002): ID fornitore DPD ISAKMP (1002): elaborazione payload id fornitore **ISAKMP (1002): parlare con un'altra scatola IOS!** ISAKMP: tipo payload ricevuto 20 **ISAKMP (1002): Il suo hash non corrisponde - questo nodo al di fuori di NAT** ISAKMP: tipo payload ricevuto 20 **ISAKMP (1002): NAT non trovato per se stesso o peer** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(1002):Vecchio stato = IKE_I_MM4 Nuovo stato = IKE_I_MM4	MM_SA_SETUP (mo principale 4) viene ric da spoke. Il comment conclude che il peer altro dispositivo Cisc e non viene rilevato a NAT per noi o per i n peer. Lo stato ISAKMP pas IKE_I_MM3 a IKE_I_
	ISAKMP:(1002):Invio del contatto iniziale **ISAKMP:(1002):SA sta eseguendo l'autenticazione**	MM_KEY_EXCH (Mo principale 5) viene in

	con chiave già condivisa utilizzando il tipo di ID ID ID_IPV4_ADDR. ISAKMP (1002): Payload ID payload successivo: 8 tipo: 1 Indirizzo: 172.16.1.1 protocollo: 17 port: 500 lunghezza: 12 ISAKMP:(1002):Lunghezza totale payload: 12 **ISAKMP (1002): invio del pacchetto alla porta 172.16.10.1 my_port 500 peer_port 500 (I) MM_KEY_EXCH** ISAKMP:(1002):invio di un pacchetto IPv4 IKE. ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(1002):Vecchio stato = IKE_I_MM4 Nuovo stato = IKE_I_MM5**	dal raggio. Lo stato ISAKMP pas IKE_I_MM4 a IKE_I_I
MM_KEY_EXCH (Modalità principale 5) viene ricevuto dall'hub. Lo stato di ISAKMP passa da IKE_R_MM4 a IKE_R_MM5. Inoltre, viene visualizzato il messaggio "peer match *none* of the profiles" (nessun profilo) per la mancanza di un profilo ISAKMP. In questo caso, ISAKMP non utilizza un profilo.	**ISAKMP (1002): ricevuto pacchetto da 172.16.1.1 dport 500 sport 500 Global (R) MM_KEY_EXCH** ISAKMP:(1002):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(1002):Vecchio stato = IKE_R_MM4 Nuovo stato = IKE_R_MM5** ISAKMP (1002): elaborazione payload ID. ID messaggio = 0 ISAKMP (1002): Payload ID payload successivo: 8 tipo: 1 Indirizzo: 172.16.1.1 protocollo: 17 port: 500 lunghezza: 12 **ISAKMP:(0): peer corrisponde *nessuno* dei profili** ISAKMP (1002): elaborazione payload HASH. ID messaggio = 0 ISAKMP (1002): elaborazione del protocollo NOTIFY INITIAL_CONTACT 1 spi 0, ID messaggio = 0, sa = 0x6A5BDE8 ISAKMP:(1002):stato autenticazione SA: autenticato ISAKMP:(1002):SA è stato autenticato con 172.16.1.1 ISAKMP:(1002):stato autenticazione SA: autenticato ISAKMP (1002): Elabora contatto iniziale, eliminare le associazioni di protezione esistenti di fase 1 e 2 con la porta remota 172.16.10.1 locale 172.16.1.1 500 **ISAKMP Tentativo di inserimento di un peer 172.16.10.1/172.16.1.1/500/, completato con 8CACD00.** ISAKMP:(1002):Input = IKE_MESG_INTERNAL,	

IKE_PROCESS_MAIN_MODE
ISAKMP:(1002):Vecchio stato = IKE_R_MM5 Nuovo stato = IKE_R_MM5

IPSEC(key_engine): è stato ricevuto un evento di coda con 1 messaggio/i KMI
ISAKMP:(1002):SA sta eseguendo l'autenticazione con chiave già condivisa utilizzando il tipo di ID ID ID_IPV4_ADDR.
ISAKMP (1002): Payload ID
payload successivo: 8
tipo: 1
Indirizzo: 172.16.10.1
protocollo: 17
port: 500
lunghezza: 12
ISAKMP:(1002):Lunghezza totale payload: 12

Il pacchetto MM_KEY_EXCH finale (modalità principale 6) viene inviato dall'hub. La negoziazione per la fase 1 è stata completata, a indicare che il dispositivo è pronto per la fase 2 (modalità rapida IPSec). Lo stato di ISAKMP passa da IKE_R_MM5 a IKE_P1_COMPLETE.

ISAKMP (1002): invio del pacchetto alla porta 172.16.1.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH
ISAKMP:(1002):invio di un pacchetto IPv4 IKE.
ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1002):Vecchio stato = IKE_R_MM5 Nuovo stato = IKE_P1_COMPLETE

ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP:(1002):Stato precedente = IKE_P1_COMPLETE Nuovo stato = IKE_P1_COMPLETE

Il pacchetto MM_KEY_EXCH fina
(modalità principale 6
viene ricevuto dallo s
La negoziazione per
1 è stata completata,
indicare che il dispos
pronto per la fase 2
(modalità rapida IPSe
Lo stato di ISAKMP p
da IKE_I_MM5 a
IKE_I_MM6 e quindi
immediatamente a
IKE_P1_COMPLETE
Inoltre, viene visualiz
messaggio "peer mat
none of the profiles
(nessun profilo) per la
mancanza di un profi
ISAKMP. In questo ca
ISAKMP non utilizza
profilo.

ISAKMP (1002): ha ricevuto un pacchetto da 172.16.10.1 port 500 sport 500 Global (I) MM_KEY_EXCH
ISAKMP (1002): elaborazione payload ID. ID messaggio = 0
ISAKMP (1002): Payload ID
payload successivo: 8
tipo: 1
Indirizzo: 172.16.10.1
protocollo: 17
port: 500
lunghezza: 12
ISAKMP:(0): peer corrisponde *nessuno* dei profili
ISAKMP (1002): elaborazione payload HASH. ID messaggio = 0
ISAKMP:(1002):stato autenticazione SA:
autenticato
ISAKMP:(1002):SA è stato autenticato con 172.16.10.1
ISAKMP Tentativo di inserimento di un peer 172.16.1.1/172.16.10.1/500/, completato con 95F6858.

	ISAKMP:(1002):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(1002):Vecchio stato = IKE_I_MM5 Nuovo stato = IKE_I_MM6** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(1002):Vecchio stato = IKE_I_MM6 Nuovo stato = IKE_I_MM6 ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(1002):Vecchio stato = IKE_I_MM6 Nuovo stato = IKE_P1_COMPLETE**
FINE DELLA NEGOZIAZIONE ISAKMP (FASE I), INIZIO DELLA NEGOZIAZIONE IPSEC (FASE II	
	ISAKMP:(1002):inizio scambio modalità rapida, M-ID di 3464373979 ISAKMP:(1002):QM Initiator ottiene spi **ISAKMP (1002): invio del pacchetto alla porta 172.16.10.1 my_port 500 peer_port 500 (I) QM_IDLE** ISAKMP:(1002):invio di un pacchetto IPv4 IKE. ISAKMP:(1002):Nodo 3464373979, Input = IKE_MESG_INTERNAL, IKE_INIT_QM **ISAKMP:(1002):Stato precedente = IKE_QM_READY Nuovo stato = IKE_QM_I_QM1** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE ISAKMP:(1002):Stato precedente = IKE_P1_COMPLETE Nuovo stato = IKE_P1_COMPLETE
L'hub riceve il primo pacchetto QM (Quick Mode) con la proposta IPSec. Gli attributi ricevuti specificano che: incapsula il flag impostato su 2 (modalità di trasporto, il flag 1 indica la modalità tunnel), la durata dell'associazione di sicurezza predefinita di 3600 secondi e 4608000 kilobyte (0x465000 in formato esadecimale), HMAC-SHA per l'autenticazione e 3DES per la crittografia. Poiché si tratta degli stessi attributi impostati nella configurazione locale, la proposta viene accettata e viene creata la shell di un'associazione di	**ISAKMP (1002): pacchetto ricevuto da 172.16.1.1 dport 500 sport 500 Global (R) QM_IDLE** **ISAKMP impostare il nuovo nodo -830593317 su QM_IDLE** ISAKMP (1002): elaborazione payload HASH. ID messaggio = 3464373979 ISAKMP (1002): elaborazione del payload SA. ID messaggio = 3464373979 **ISAKMP:(1002):verifica della proposta IPSec 1** **ISAKMP trasformazione 1, ESP_3DES** **ISAKMP attributi nella trasformazione:** **ISAKMP encaps è 2 (trasporto)** **ISAKMP Tipo di durata SA in secondi** **ISAKMP Durata SA (base) di 3600** **ISAKMP Tipo di durata SA in kilobyte** **ISAKMP Durata SA (VPI) di 0x0 0x46 0x50 0x0** **ISAKMP l'autenticatore è HMAC-SHA** **ISAKMP:(1002):atts sono accettabili.** IPSEC(validate_request_proposta): parte proposta n. 1 IPSEC(validate_request_proposta): parte proposta n. 1, **(chiave eng. msg.) INBOUND local= 172.16.10.1:0,**

Lo scambio in modali
rapida (Fase II, IPSe
viene avviato e spok
il primo messaggio Q
all'hub.

protezione IPSec. Poiché a questi valori non sono ancora associati valori SPI (Security Parameter Index), si tratta solo di una shell di un'associazione di sicurezza che non può ancora essere utilizzata per passare il traffico.	**remote= 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 (tipo=1),** **protocol= ESP, transform= NONE (trasporto),** **lifedur= 0s e 0kb,** **spi= 0x0(0), conn_id= 0, keysize= 128, flag= 0x0**
Si tratta solo di messaggi generici del servizio IPSec che indicano che funziona correttamente.	IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): la ricerca della connessione ha restituito 0 IPSEC-IFC MGRE/Tu0: crypto_ss_Listen_start già in ascolto **IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Apertura di un socket con il profilo DMVPN-IPSEC** IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): la ricerca della connessione ha restituito 0 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Avvio immediato del tunnel. IPSEC-IFC MGRE/Tu0: Aggiunta dell'interfaccia tunnel Tunnel0 all'elenco condiviso IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): tunnel_protection_start_pending_timer 8C9388 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Buona richiesta di ascolto
La voce della mappa pseudo-crittografica viene creata per il protocollo IP 47 (GRE) da 172.16.10.1 (indirizzo pubblico hub) a 172.16.1.1 (indirizzo pubblico spoke). Per il traffico in entrata e in uscita viene creata un'associazione di protezione IPSec/SPI con i valori della proposta accettata.	inserimento della mappa nell'AVL di mapdb non riuscito. La coppia mappa + ace esiste già nel mapdb CRYPTO_SS(SEC TUNNEL): Informazioni passive sull'apertura e sul 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, port 47, ifc Tu0 Mapdb crittografia: corrispondenza_proxy **src addr: 172.16.10.1** **dst addr: 172.16.1.1** **protocollo: 47** porta src: 0 porta dst: 0 ISAKMP (1002): elaborazione del payload NONCE. ID messaggio = 3464373979 ISAKMP (1002): elaborazione payload ID. ID messaggio = 3464373979 ISAKMP (1002): elaborazione payload ID. ID messaggio = 3464373979 ISAKMP:(1002):QM Responder gets spi ISAKMP:(1002):Nodo 3464373979, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH **ISAKMP:(1002):Stato precedente = IKE_QM_READY Nuovo stato = IKE_QM_SPI_STARVE** **ISAKMP (1002): Creazione di associazioni di protezione IPSec** **SA in entrata da 172.16.1.1 a 172.16.10.1 (f/i) 0/ 0** **(proxy da 172.16.1.1 a 172.16.10.1)**

ha spi 0xDD2AC2B3 e conn_id 0
durata di 3600 secondi
durata di 4608000 kilobyte
SA in uscita da 172.16.10.1 a 172.16.1.1 (f/i) 0/0
(proxy da 172.16.10.1 a 172.16.1.1)
ha spi 0x82C3E0C4 e conn_id 0
durata di 3600 secondi
durata di 4608000 kilobyte

Secondo messaggio QM inviato dall'hub. Messaggio generato dal servizio IPSec che conferma che la protezione del tunnel è attiva su Tunnel0.

ISAKMP (1002): invio del pacchetto alla porta 172.16.1.1 my_port 500 peer_port 500 (R) QM_IDLE
ISAKMP:(1002):invio di un pacchetto IPv4 IKE.
ISAKMP:(1002):Nodo 3464373979, Input = IKE_MESG_INTERNAL, IKE_GOT_SPI
ISAKMP:(1002):Vecchio stato = IKE_QM_SPI_STARVE Nuovo stato = IKE_QM_R_QM2

Viene visualizzato un altro messaggio di creazione dell'associazione di protezione (SA) con gli IP di destinazione, gli SPI, gli attributi del set di trasformazioni e la durata in kilobyte e secondi rimanenti.

CRYPTO_SS(SEC TUNNEL): Associazione dell'applicazione al socket completata
IPSEC(key_engine): è stato ricevuto un evento di coda con 1 messaggio/i KMI
Mapdb crittografia: corrispondenza_proxy
src addr: 172.16.10.1
dst addr: 172.16.1.1
protocollo: 47
porta src: 0
porta dst: 0
IPSEC(crypto_ipsec_sa_find_ident_head): riconnessione con gli stessi proxy e peer 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 creato,
(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 creato,
(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): aggiornamento di Tunnel0 ident 8B6A0E8 con tun_decap_oce 6A648F0
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): la ricerca della connessione ha restituito 8C93888
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): messaggio socket ready valido
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): la ricerca della connessione ha restituito 8C93888
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): socket_protezione_tunnel

IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Segnalazione NHRP
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Ricevuto messaggio MTU mtu 1458
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): la ricerca della connessione ha restituito 8C93888
ISAKMP (1002): pacchetto ricevuto da 172.16.10.1 dport 500 sport 500 Global (I) QM_IDLE
ISAKMP (1002): elaborazione payload HASH. ID messaggio = 3464373979
ISAKMP (1002): elaborazione del payload SA. ID messaggio = 3464373979
ISAKMP:(1002):verifica della proposta IPSec 1
ISAKMP trasformazione 1, ESP_3DES
ISAKMP attributi nella trasformazione:
ISAKMP encaps è 2 (trasporto)
ISAKMP Tipo di durata SA in secondi
ISAKMP Durata SA (base) di 3600
ISAKMP Tipo di durata SA in kilobyte
ISAKMP Durata SA (VPI) di 0x0 0x46 0x50 0x0
ISAKMP l'autenticatore è HMAC-SHA
ISAKMP:(1002):atts sono accettabili.
IPSEC(validate_request_proposta): parte proposta n. 1
IPSEC(validate_request_proposta): parte proposta n. 1,
(chiave eng. msg.) INBOUND local= 172.16.1.1:0, remote= 172.16.10.1:0,
local_proxy= 172.16.1.1/255.255.255.255/47/0 (tipo=1),
remote_proxy= 172.16.10.1/255.255.255.255/47/0 (tipo=1),
protocol= ESP, transform= NONE (trasporto),
lifedur= 0s e 0kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flag= 0x0
Mapdb crittografia: corrispondenza_proxy
src addr: 172.16.1.1
dst addr: 172.16.10.1
protocollo: 47
porta src: 0
porta dst: 0
ISAKMP (1002): elaborazione del payload NONCE. ID messaggio = 3464373979
ISAKMP (1002): elaborazione payload ID. ID messaggio = 3464373979
ISAKMP (1002): elaborazione payload ID. ID messaggio = 3464373979
ISAKMP (1002): Creazione di associazioni di

Il spoke riceve il secc pacchetto QM conter la proposta IPSec. Ci conferma che QM1 è ricevuto dall'hub. Gli attributi ricevuti speci che: incapsula il flag impostato su 2 (moda trasporto, il flag 1 ind modalità tunnel), la d dell'associazione di sicurezza predefinita 3600 secondi e 4608 kilobyte (0x465000 in formato esadecimale HMAC-SHA per l'autenticazione e DE la crittografia. Poiché tratta degli stessi attri impostati nella configurazione locale proposta viene accet viene creata la shell d un'associazione di protezione IPSec. Po questi valori non sono ancora associati valo (Security Parameter I si tratta solo di una sh un'associazione di sicurezza che non pu ancora essere utilizza passare il traffico.
La voce della mappa pseudo-crittografica v creata per il protocoll 47 (GRE) da 172.16. (indirizzo pubblico hu 172.16.1.1 (indirizzo pubblico spoke).
Per il traffico in entrat uscita viene creata un'associazione di protezione IPSec/SP valori della proposta accettata.

protezione IPSec
SA in entrata da 172.16.10.1 a 172.16.1.1 (f/i) 0/0
(proxy da 172.16.10.1 a 172.16.1.1)
ha spi 0x82C3E0C4 e conn_id 0
durata di 3600 secondi
durata di 4608000 kilobyte
SA in uscita da 172.16.1.1 a 172.16.10.1 (f/i) 0/0
(proxy da 172.16.1.1 a 172.16.10.1)
ha spi 0xDD2AC2B3 e conn_id 0
durata di 3600 secondi
durata di 4608000 kilobyte

ISAKMP (1002): invio del pacchetto alla porta 172.16.10.1 my_port 500 peer_port 500 (I) QM_IDLE

ISAKMP:(1002):invio di un pacchetto IPv4 IKE.

ISAKMP:(1002):eliminazione nodo -830593317 errore FALSO motivo "Nessun errore"

ISAKMP:(1002):Nodo 3464373979, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH

ISAKMP:(1002):Stato precedente = IKE_QM_I_QM1 Nuovo stato = IKE_QM_PHASE2_COMPLETE

IPSEC(key_engine): è stato ricevuto un evento di coda con 1 messaggio/i KMI

Mapdb crittografia: corrispondenza_proxy
src addr: 172.16.1.1
dst addr: 172.16.10.1
protocollo: 47
porta src: 0
porta dst: 0

IPSEC(crypto_ipsec_sa_find_ident_head): riconnessione con gli stessi proxy e peer 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 creato,
(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)= (449172/3600)

IPSEC(create_sa): sa creato,
(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)= (449172/3600)

IPSEC(update_current_outbound_sa): get enable SA peer 172.16.10.1 current outbound sa su SPI DD2AC2B3

IPSEC(update_current_outbound_sa): peer aggiornato 172.16.10.1 corrente in uscita sa su SPI DD2AC2B3

IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce): aggiornamento di Tunnel0 ident 94F2740 con tun_decap_oce 794ED30

Il spoke invia il terzo ultimo messaggio QM all'hub, che completa scambio QM. A differ di ISAKMP, in cui ogn passa attraverso ogn (da MM1 a MM6/P1_COMPLETE IPSec è leggermente diverso in quanto son presenti solo tre mes anziché sei. L'iniziato nostro raggio in ques caso, come indicato "I" nel messaggio IKE_QM_I_QM1) va QM_READY, quindi a QM_I_QM1 direttame QM_PHASE2_COMP Il risponditore (hub) p a QM_READY, QM_SPI_STARVE, QM_R_QM2, QM_PHASE2_COMP Viene visualizzato un messaggio di creazio dell'associazione di protezione (SA) con g di destinazione, gli SI attributi del set di trasformazioni e la du in kilobyte e secondi rimanenti.

IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): la ricerca della connessione ha restituito 961D220
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): socket_protezione_tunnel
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Segnalazione NHRP
NHRP: NHS 10.1.1.254 Tunnel0 vrf 0 Cluster 0 Priorità 0 Transizione da 'E' a ' '

IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): la ricerca della connessione ha restituito 961D220
NHRP: Tentativo di invio del pacchetto tramite DEST 10.1.1.254

I messaggi QM finali confermano che la modalità rapida è stata completata e che IPSec è attivo su entrambi i lati del tunnel. A differenza di ISAKMP, in cui ogni peer passa attraverso ogni stato (da MM1 a MM6/P1_COMPLETE), IPSec è leggermente diverso in quanto sono presenti solo tre messaggi anziché sei. Il Responder (il nostro hub in questo caso, come indicato dalla "R" nel messaggio IKE_QM_**R**_QM1) va QM_READY, QM_SPI_STARVE, QM_R_QM2, QM_PHASE2_COMPLETE. L'iniziatore (spoke) va da QM_READY, quindi a QM_I_QM1 direttamente a QM_PHASE2_COMPLETE.

ISAKMP (1002): pacchetto ricevuto da 172.16.1.1 dport 500 sport 500 Global (R) QM_IDLE
ISAKMP:(1002):eliminazione nodo -830593317 errore FALSO motivo "QM completato (await)"
ISAKMP:(1002):Nodo 3464373979, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1002):Stato precedente = IKE_QM_R_QM2 Nuovo stato = IKE_QM_PHASE2_COMPLETE
IPSEC(key_engine): è stato ricevuto un evento di coda con 1 messaggio/i KMI
IPSEC(key_engine_enable_outbound): reg. abilitazione notifica da ISAKMP
IPSEC(key_engine_enable_outbound): abilita SA con spi 2193875140/50
IPSEC(update_current_outbound_sa): get enable SA peer 172.16.1.1 current outbound sa su SPI 82C3E0C4
IPSEC(update_current_outbound_sa): aggiornato peer 172.16.1.1 corrente in uscita sa su SPI 82C3E0C4

NHRP: Invia richiesta di registrazione tramite Tunnel0 vrf 0, dimensioni pacchetto: 108
src 10.1.1.1, dst: 10.1.1.254
F) afn: IPv4(1), tipo: IP(800), hop: 255, ver.: 1
shtl 4(NSAP), sstl: 0(NSAP)
pktsz: 108 estraibile: 52
M) bandiere: "unique nat ", richiesto: 65540
NBMA src: 172.16.1.1
protocollo src: 10.1.1.1, protocollo dst: 10.1.1.254
(C-1) codice: nessun errore(0)
prefisso: 32, mtu: 17912, ora_hd: 7200
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
Estensione indirizzo risponditore(3):

Si tratta delle richiest registrazione NHRP i all'hub nel tentativo d eseguire la registrazi all'NHS (hub). E 'norr vederne moltissimi, d che l'oratore continua tentare la registrazion servizio sanitario naz fino a quando non ric una "risposta di registrazione".
src,dst: Indirizzi IP di origine (spoke) e di

Estensione record NHS Forward Transit(4):
Estensione record NHS Reverse Transit(5):
Estensione autenticazione(7):
tipo:Testo normale(1), colon&dati;NHRPAUTH
Estensione indirizzo NAT(9):
(C-1) codice: nessun errore(0)
prefisso: 32, mtu: 17912, ora_hd: 0
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0
NBMA client: 172.16.10.1
protocollo client: 10.1.1.254

destinazione (hub) de
tunnel. Queste sono
l'origine e la destinaz
del pacchetto GRE in
dal router
NBMA src: l'indirizzo
(Internet) del spoke c
inviato questo pacche
cerca di registrarsi al
protocollo src: indiriz
tunnel dell'spoke che
di eseguire la registra
protocollo dst: indiriz
tunnel NHS/hub
Estensione di autenticazione, data&
Stringa di autenticazi
NHRP
NBMA client: Indirizzo
NBMA dell'NHS/hub
protocollo client: indir
tunnel NHS/hub

TASSO NHRP: Invio della richiesta di registrazione iniziale per 10.1.1.254, richiesta 65540
%LINK-3-UPDOWN: Interfaccia Tunnel0, stato modificato in attivo
NHRP: if_up: Proto tunnel0 0
NHRP: Tunnel0: Aggiornamento cache per target 10.1.1.254/32 next-hop 10.1.1.254 172.16.10.1
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): la ricerca della connessione ha restituito 961D220
NHRP: Tentativo di invio del pacchetto tramite DEST 10.1.1.254

Altri messaggi del se
NHRP che dicono ch
richiesta di registrazio
iniziale è stata inviata
servizio NHS alla
10.1.1.254. Vi è anch
conferma che è stata
aggiunta una voce de
cache per il tunnel IP
10.1.1.254/24 che viv
NBMA 172.16.10.1. I
messaggio di ritardo
afferma che il tunnel
"non chiuso".

IPSEC-IFC GRE/Tu0: tunnel in arrivo
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): la ricerca della connessione ha restituito 961D220
IPSEC-IFC GRE/Tu0: crypto_ss_Listen_start già in ascolto
IPSEC-IFC GRE/Tu0: crypto_ss_Listen_start già in ascolto
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Apertura di un socket con il profilo DMVPN-IPSEC
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): la ricerca della connessione ha restituito 961D220
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Socket già aperto. Ignorare.
%LINEPROTO-5-UPDOWN: Protocollo di linea su tunnel di interfaccia0, stato modificato in attivo

Si tratta di messaggi
generici del servizio I
che indicano che funz
correttamente. Qui è
finalmente possibile v
che il protocollo del tu
è attivo.

Si tratta delle richieste di registrazione NHRP

NHRP: Receive Registration Request via Tunnel0 vrf 0, dimensioni del pacchetto: 108

ricevute dall'utente spoke nel tentativo di registrarsi al servizio sanitario nazionale (hub). E 'normale vederne moltissimi, dato che l'oratore continua a tentare la registrazione al servizio sanitario nazionale fino a quando non riceve una "risposta di registrazione".

NBMA src: l'indirizzo NBMA (Internet) del spoke che ha inviato questo pacchetto e cerca di registrarsi al NHS

protocollo src: indirizzo tunnel dell'spoke che tenta di eseguire la registrazione

protocollo dst: indirizzo tunnel NHS/hub

Estensione di autenticazione, data: Stringa di autenticazione NHRP

NBMA client: Indirizzo NBMA dell'NHS/hub

protocollo client: indirizzo tunnel NHS/hub

Pacchetti di debug NHRP che aggiungono la rete di destinazione 10.1.1.1/32 disponibili tramite l'hop successivo della versione 10.1.1.1 a NHRP della versione 172.16.1.1. 172.16.1.1 vengono aggiunti anche all'elenco di indirizzi a cui l'hub inoltra il traffico multicast. Questi messaggi confermano che la registrazione è riuscita, così come la risoluzione dell'indirizzo del tunnel spoke.

F) afn: IPv4(1), tipo: IP(800), hop: 255, ver.: 1
shtl 4(NSAP), sstl: 0(NSAP)
pktsz: 108 estraibile: 52
M) bandiere: "unique nat ", richiesto: 65540
NBMA src: 172.16.1.1
protocollo src: 10.1.1.1, protocollo dst: 10.1.1.254
(C-1) codice: nessun errore(0)
prefisso: 32, mtu: 17912, ora_hd: 7200
addr_len: 0(NSAP), subaddr_len: 0(NSAP),
proto_len: 0, pref: 0
Estensione indirizzo risponditore(3):
Estensione record NHS Forward Transit(4):
Estensione record NHS Reverse Transit(5):
Estensione autenticazione(7):
tipo:Testo normale(1), colon&dati;NHRPAUTH
Estensione indirizzo NAT(9):
(C-1) codice: nessun errore(0)
prefisso: 32, mtu: 17912, ora_hd: 0
addr_len: 4(NSAP), subaddr_len: 0(NSAP),
proto_len: 4, pref: 0
NBMA client: 172.16.10.1
protocollo client: 10.1.1.254

NHRP: netid_in = 1, to_us = 1
NHRP: Tunnel0: Aggiunta cache per la destinazione 10.1.1.1/32 next-hop 10.1.1.1
172.16.1.1
NHRP: Aggiunta di endpoint del tunnel (VPN: 10.1.1.1, NBMA: 172.16.1.1)
NHRP: Collegamento del sottoblocco NHRP per gli endpoint del tunnel (VPN: 10.1.1.1, NBMA: 172.16.1.1)
NHRP: Inserito nodo di sottoblocco per la cache: Nodo sottoblocco inserito destinazione per la cache: Target 10.1.1.1/32nhop 10.1.1.1
NHRP: Voce della cache dinamica interna convertita per l'interfaccia 10.1.1.1/32 Tunnel0 in esterna
NHRP: Tu0 Creazione mapping multicast dinamico NBMA: 172.16.1.1
NHRP: Mapping multicast dinamico aggiunto per NBMA: 172.16.1.1
NHRP: Aggiornamento della cache con NBMA: 172.16.10.1, NBMA_ALT: 172.16.10.1
NHRP: Nuova lunghezza obbligatoria: 32
NHRP: Tentativo di invio del pacchetto tramite DEST 10.1.1.1
NHRP: NHRP ha risolto correttamente 10.1.1.1 in NBMA 172.16.1.1
NHRP: Incapsulamento completato. Tunnel IP addr

172.16.1.1
NHRP: Invia risposta di registrazione tramite Tunnel0 vrf 0, dimensioni pacchetto: 128
src 10.1.1.254, dst: 10.1.1.1
F) afn: IPv4(1), tipo: IP(800), hop: 255, ver.: 1
shtl 4(NSAP), sstl: 0(NSAP)
pktsz: 128 estraibile: 52
M) bandiere: "unique nat ", richiesto: 65540
NBMA src: 172.16.1.1
protocollo src: 10.1.1.1, protocollo dst: 10.1.1.254
(C-1) codice: nessun errore(0)
prefisso: 32, mtu: 17912, ora_hd: 7200
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
Estensione indirizzo risponditore(3):
C) codice: nessun errore(0)
prefisso: 32, mtu: 17912, ora_hd: 7200
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0
NBMA client: 172.16.10.1
protocollo client: 10.1.1.254
Estensione record NHS Forward Transit(4):
Estensione record NHS Reverse Transit(5):
Estensione autenticazione(7):
tipo:Testo normale(1), colon&dati;NHRPAUTH
Estensione indirizzo NAT(9):
(C-1) codice: nessun errore(0)
prefisso: 32, mtu: 17912, ora_hd: 0
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0
NBMA client: 172.16.10.1
protocollo client: 10.1.1.254

Si tratta della risposta di registrazione NHRP inviata dall'hub al spoke in risposta alla "richiesta di registrazione NHRP" ricevuta in precedenza. Come gli altri pacchetti di registrazione, l'hub invia multipli di questi in risposta alle richieste multiple.
src,dst: Indirizzi IP di origine (hub) e di destinazione (spoke) del tunnel. Queste sono l'origine e la destinazione del pacchetto GRE inviato dal router
NBMA src: Indirizzo NBMA (Internet) dell'oratore
protocollo src: indirizzo tunnel dell'spoke che tenta di eseguire la registrazione
protocollo dst: indirizzo tunnel NHS/hub
NBMA client: Indirizzo NBMA dell'NHS/hub
protocollo client: indirizzo tunnel NHS/hub
Estensione di autenticazione, data: Stringa di autenticazione NHRP

NHRP: Receive Registration Reply via Tunnel0 vrf 0, dimensioni del pacchetto: 128
F) afn: IPv4(1), tipo: IP(800), hop: 255, ver.: 1
shtl 4(NSAP), sstl: 0(NSAP)
pktsz: 128 estraibile: 52
M) bandiere: "unique nat ", richiesto: 65541
NBMA src: 172.16.1.1
protocollo src: 10.1.1.1, protocollo dst: 10.1.1.254
(C-1) codice: nessun errore(0)
prefisso: 32, mtu: 17912, ora_hd: 7200
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
Estensione indirizzo risponditore(3):
C) codice: nessun errore(0)
prefisso: 32, mtu: 17912, ora_hd: 7200
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0
NBMA client: 172.16.10.1
protocollo client: 10.1.1.254
Estensione record NHS Forward Transit(4):

Si tratta della risposta
registrazione NHRP i
dall'hub al spoke in ri
alla "richiesta di
registrazione NHRP"
ricevuta in precedenz
Come gli altri pacche
registrazione, l'hub in
multipli di questi in ris
alle richieste multiple
NBMA src: Indirizzo N
(Internet) dell'oratore
protocollo src: indiriz
tunnel dell'spoke che
di eseguire la registra
protocollo dst: indiriz
tunnel NHS/hub
NBMA client: Indirizz
NBMA dell'NHS/hub
protocollo client: indir

	Estensione record NHS Reverse Transit(5): **Estensione autenticazione(7):** **tipo:Testo normale(1), colon&dati;NHRPAUTH** Estensione indirizzo NAT(9): (C-1) codice: nessun errore(0) prefisso: 32, mtu: 17912, ora_hd: 0 addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0 **NBMA client: 172.16.10.1** **protocollo client: 10.1.1.254** NHRP: netid_in = 0, to_us = 1	tunnel NHS/hub **Estensione di autenticazione**, data& Stringa di autenticazi NHRP
Messaggi di servizio IPSec più generici che indicano che funziona correttamente.	IPSEC-IFC MGRE/Tu0: crypto_ss_Listen_start già in ascolto IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Apertura di un socket con il profilo DMVPN-IPSEC IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): la ricerca della connessione ha restituito 8C93888 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Socket già aperto. Ignorare. IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): tunnel_protection_stop_pending_timer 8C9388	
	NHRP: NHS-UP: 10.1.1.254	Messaggi del servizio NHRP indicanti che il servizio NHS che si t 10.1.1.254 è attivo.
Messaggio di sistema che indica che l'adiacenza EIGRP è attiva con il vicino che ha parlato alla 10.1.1.1.	%DUAL-5-NBRCHANGE: EIGRP-IPv4.1: Adiacente 10.1.1.1 (Tunnel0) attivo: nuova adiacenza	
	%DUAL-5-NBRCHANGE: EIGRP-IPv4.1: Router adiacente 10.1.1.254 (Tunnel0) attivo: nuova adiacenza	Messaggio di sistema indica che l'adiacenza EIGRP è attiva con l'I adiacente alla posizio 10.1.1.254.
Messaggio di sistema che conferma la riuscita della risoluzione NHRP.	NHRP: NHRP ha risolto correttamente 10.1.1.1 in NBMA 172.16.1.1	

Conferma funzionalità e risoluzione problemi

Questa sezione contiene alcuni dei comandi **show** più utili utilizzati per risolvere i problemi sia dell'hub che dello spoke. Per abilitare debug più specifici, usare le seguenti condizioni di debug:

- debug dmvpn condition peer nbma *NBMA_ADDRESS*
- debug dmvpn condizione peer tunnel *INDIRIZZO_TUNNEL*
- 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"
```

mostra dettagli sessione crittografica

```
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
```

visualizzare i dettagli di 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
```

mostra dettagli sa crypto ipsec

```
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 [dettaglio]

```
"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:
```

Informazioni correlate

- Risoluzione dei problemi IPSec: descrizione e uso dei comandi di debug
- Crittografia di nuova generazione
- RFC 3706 IKE Dead Peer Detection
- RFC 3947: IKE NAT Traversal
- Documentazione e supporto tecnico – Cisco Systems