A fase 1 DMVPN debuga pesquisa defeitos o guia

Índice

Introdução

Este documento descreve as mensagens que debugar você encontraria no hub and spoke de um desenvolvimento multiponto dinâmico da fase 1 de Virtual Private Network (DMVPN).

Pré-requisitos

Para a configuração e os comandos debug neste documento, você precisará dois roteadores Cisco que executam a liberação 12.4(9)T do ® do Cisco IOS ou mais tarde. Geralmente, uma fase básica 1 DMVPN exige o Cisco IOS Release 12.2(13)T ou Mais Recente ou a liberação

12.2(33)XNC para o roteador dos serviços da agregação (ASR), embora as características e debuga considerado neste documento não pôde ser apoiada.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Generic Routing Encapsulation (GRE)
- Protocolo de Resolução do Próximo Salto (NHRP)
- Internet Security Association and Key Management Protocol (ISAKMP)
- Internet Key Exchange (IKE)
- Segurança de protocolo do Internet (IPsec)
- Pelo menos um destes protocolos de roteamento: Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), e Border Gateway Protocol (BGP)

Componentes Utilizados

A informação neste documento é baseada em Cisco 2911 Roteadores dos Serviços integrados (ISR) que executam o Cisco IOS Release 15.1(4)M4.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Realces significativos

Estas versões do Cisco IOS introduziram características ou reparos significativos para a fase 1 DMVPN:

- Liberação 12.2(18)SXF5 - melhor apoio para o ISAKMP ao usar o Public Key Infrastructure (PKI)
- Liberação 12.2(33)XNE - ASR, perfis IPSec, proteção do túnel, tradução de endereços da rede IPsec (NAT) Traversal
- Liberação 12.3(7)T - apoio do roteamento virtual e da transmissão do interior (iVRF)
- Liberação 12.3(11)T - apoio do roteamento virtual e da transmissão da porta frontal (fVRF)
- A liberação 12.4(9)T - apoio para o vário DMVPN relativo debuga e comanda
- Liberação 12.4(15)T - Proteção compartilhada do túnel
- Liberação 12.4(20)T - IPv6 sobre o DMVPN
- Liberação 15.0(1)M - Monitoramento de funcionamento do túnel NHRP

Convenções

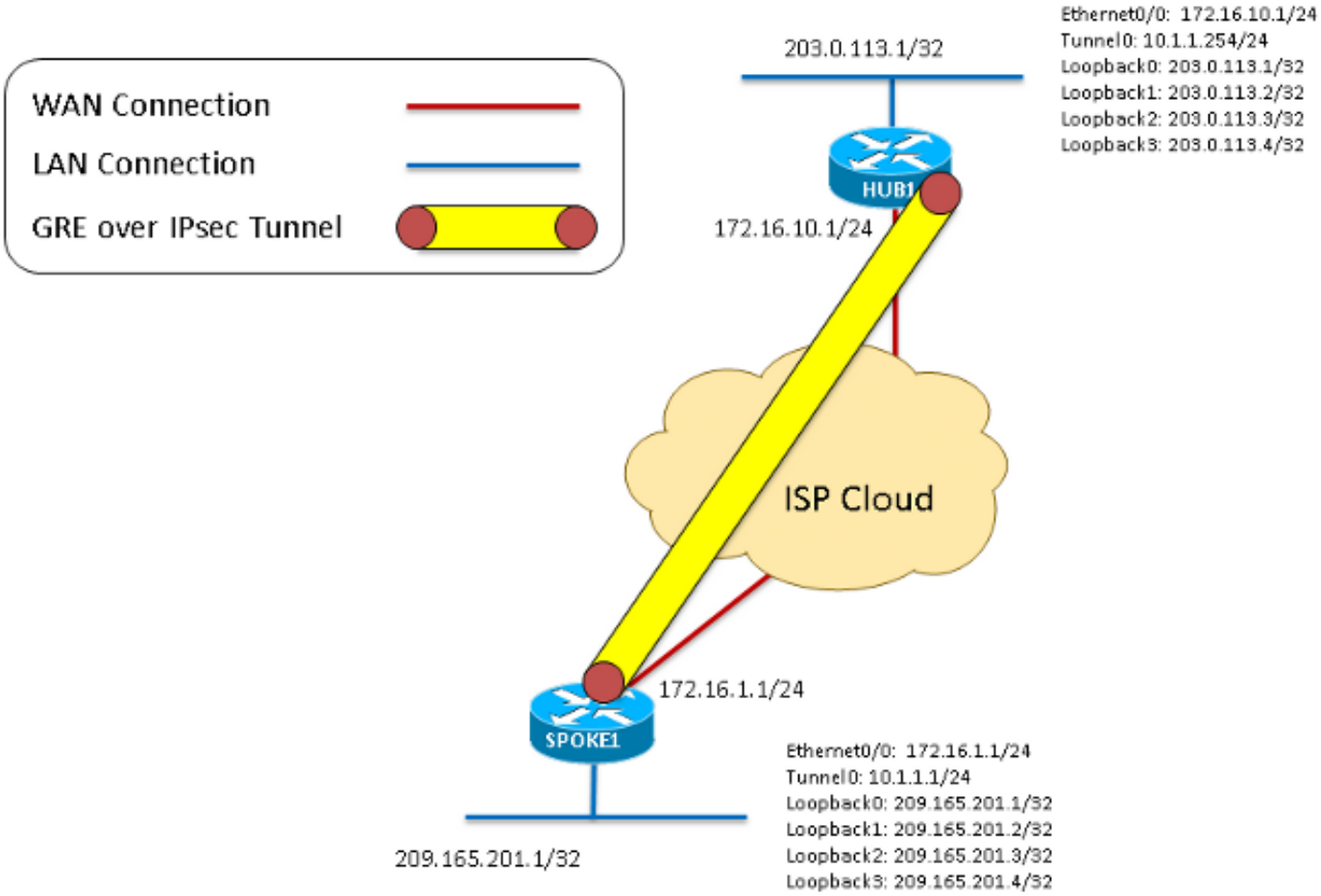
Consulte as Convenções de Dicas Técnicas da Cisco para obter informações sobre convenções de documentos.

Configuração relevante

Vista geral da topologia

Para esta topologia, dois 2911 ISR que são executado a liberação 15.1(4)M4 foram configurados para a fase 1 DMVPN: um como um hub e um como um spoke. O Ethernet0/0 foi usado como a relação do “Internet” em cada roteador. As quatro interfaces de loopback são configuradas para simular as redes de área local que vivem no hub ou na instalação de raio. Porque esta é uma topologia da fase 1 DMVPN com somente uma falou, o spoke é configurado com um túnel GRE ponto a ponto um pouco do que um túnel GRE multiponto. O mesmo configuraton cripto (ISAKMP e IPsec) foi usado em cada roteador para assegurá-los combinou exatamente.

Diagrama 1



Cripto

Este é o mesmo no hub e no 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
```

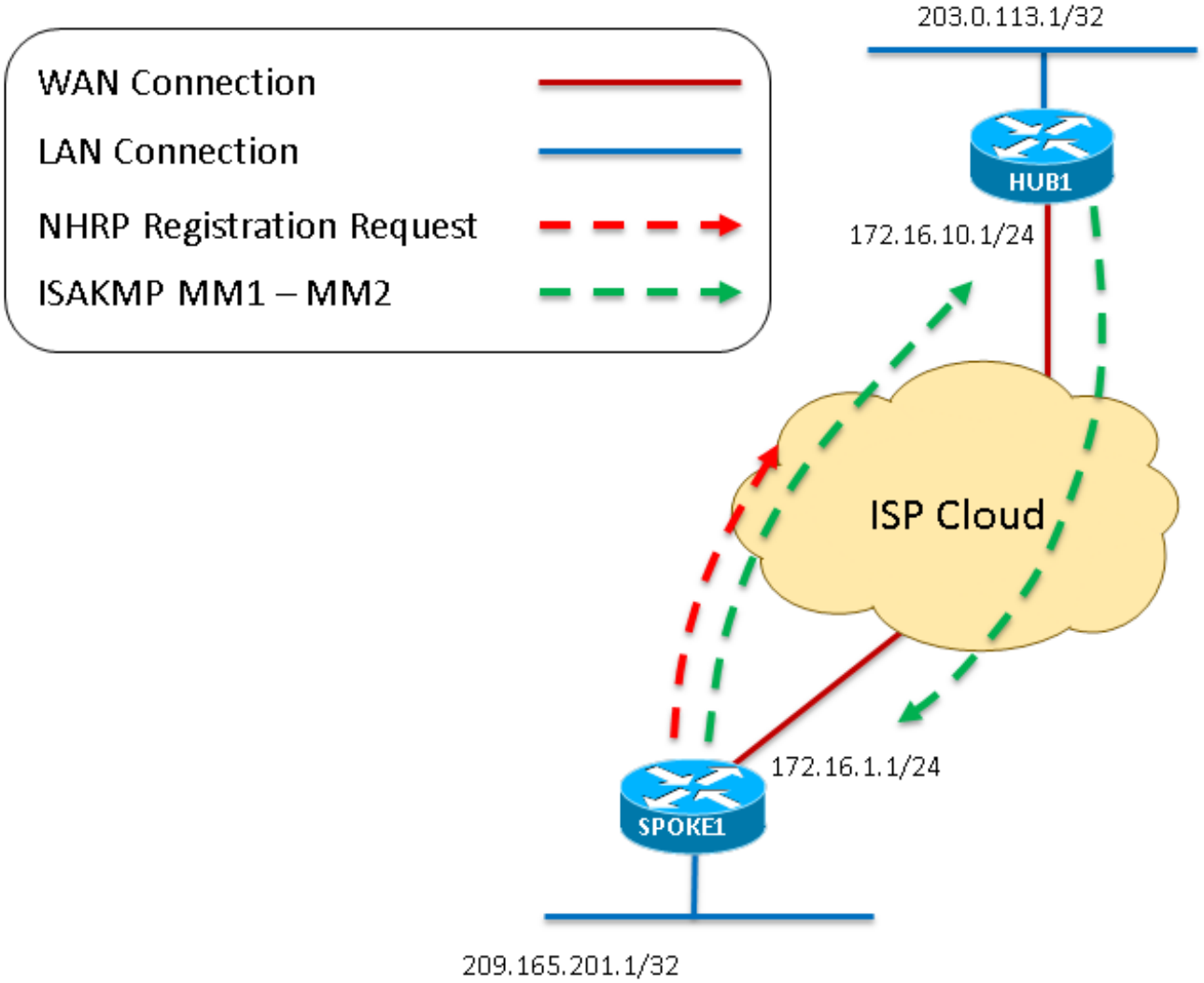
```
ip address 209.165.201.1 255.255.255.255
interface Loopback1
ip address 209.165.201.2 255.255.255.255
interface Loopback2
ip address 209.165.201.3 255.255.255.255
interface Loopback3
ip address 209.165.201.4 255.255.255.255

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
```

Debugs

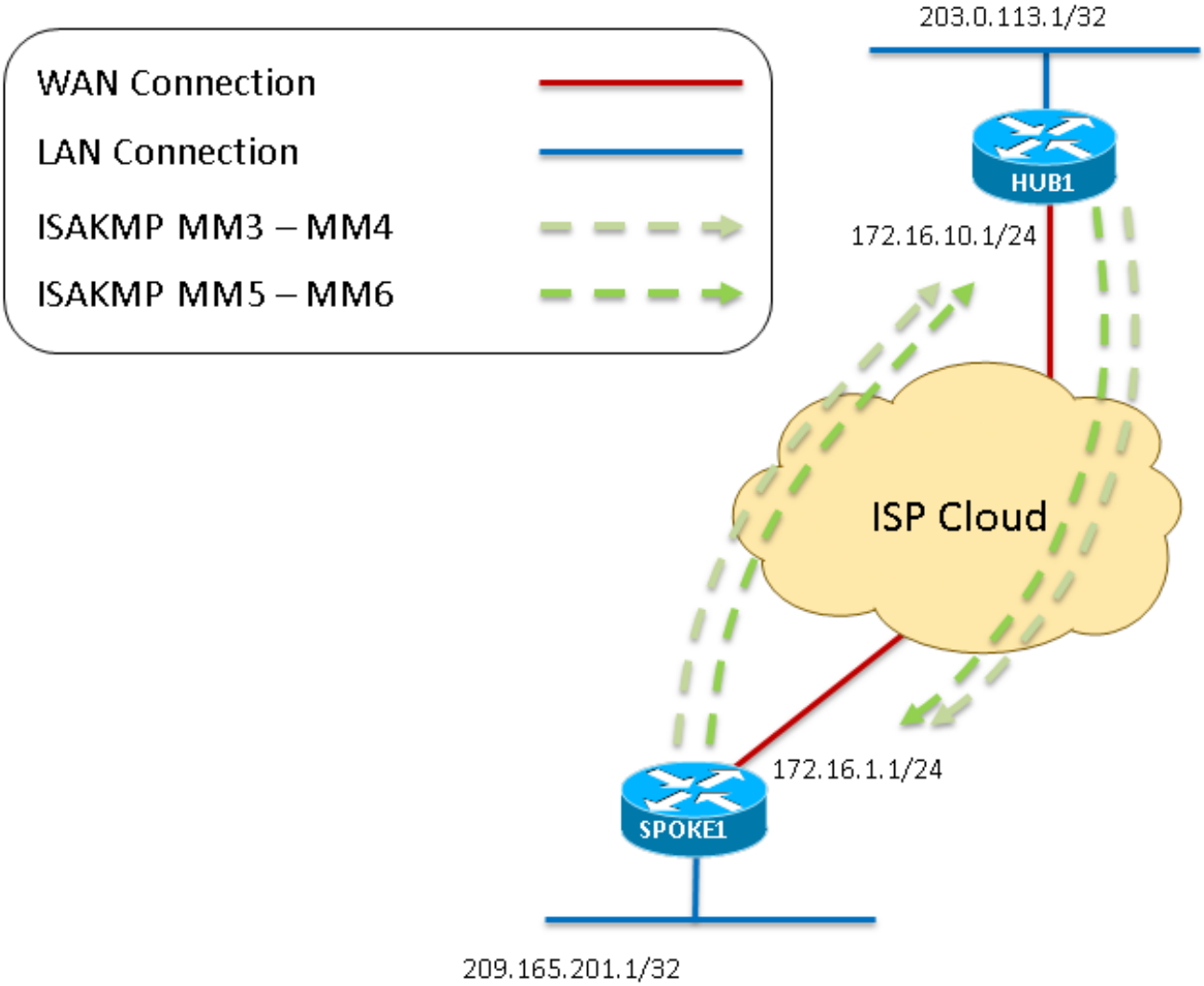
Visualização de fluxo de pacote de informação

Este é um visualização do fluxo de pacote de informação inteiro DMVPN como visto neste documento. Mais detalhado debuga que explica cada um das etapas é incluído igualmente.

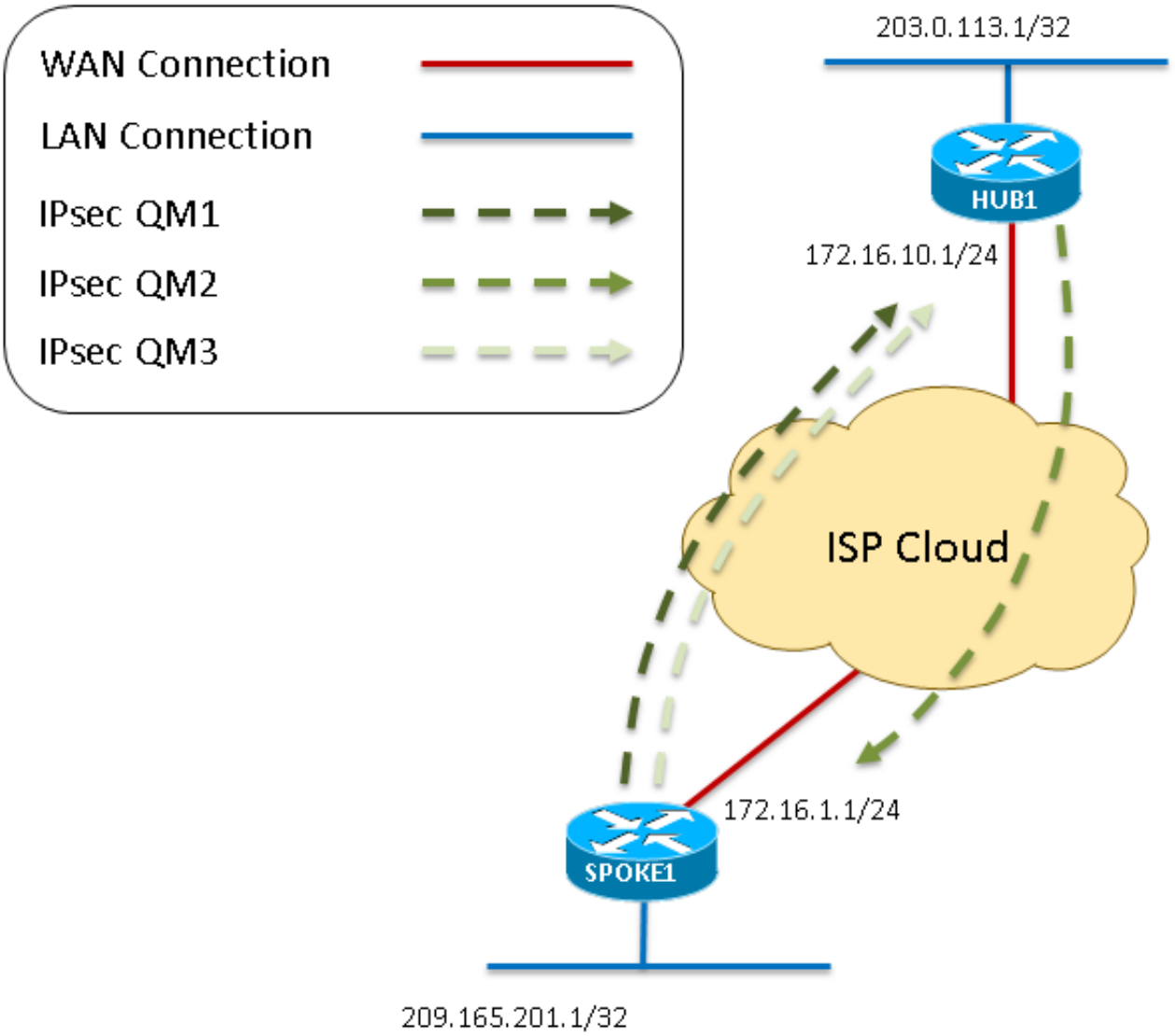
1. Quando o túnel no spoke não é “nenhuma parada programada” gerencie uma requisição de registro NHRP, que comece o processo DMVPN. Porque a configuração do hub é completamente dinâmica, o spoke deve ser o valor-limite que inicia a conexão.
2. A requisição de registro NHRP é encapsulada então no GRE que provoca o processo de criptografia para começar.
3. Neste momento, a primeira mensagem do modo principal ISAKMP - ISAKMP MM1 - é enviada do falou ao hub na porta UDP500.
4. O hub recebe e processa MM1 e responde com ISAKMP MM2, porque tem uma política de ISAKMP de harmonização.
   O diagrama 2 - refere etapas 1
   4



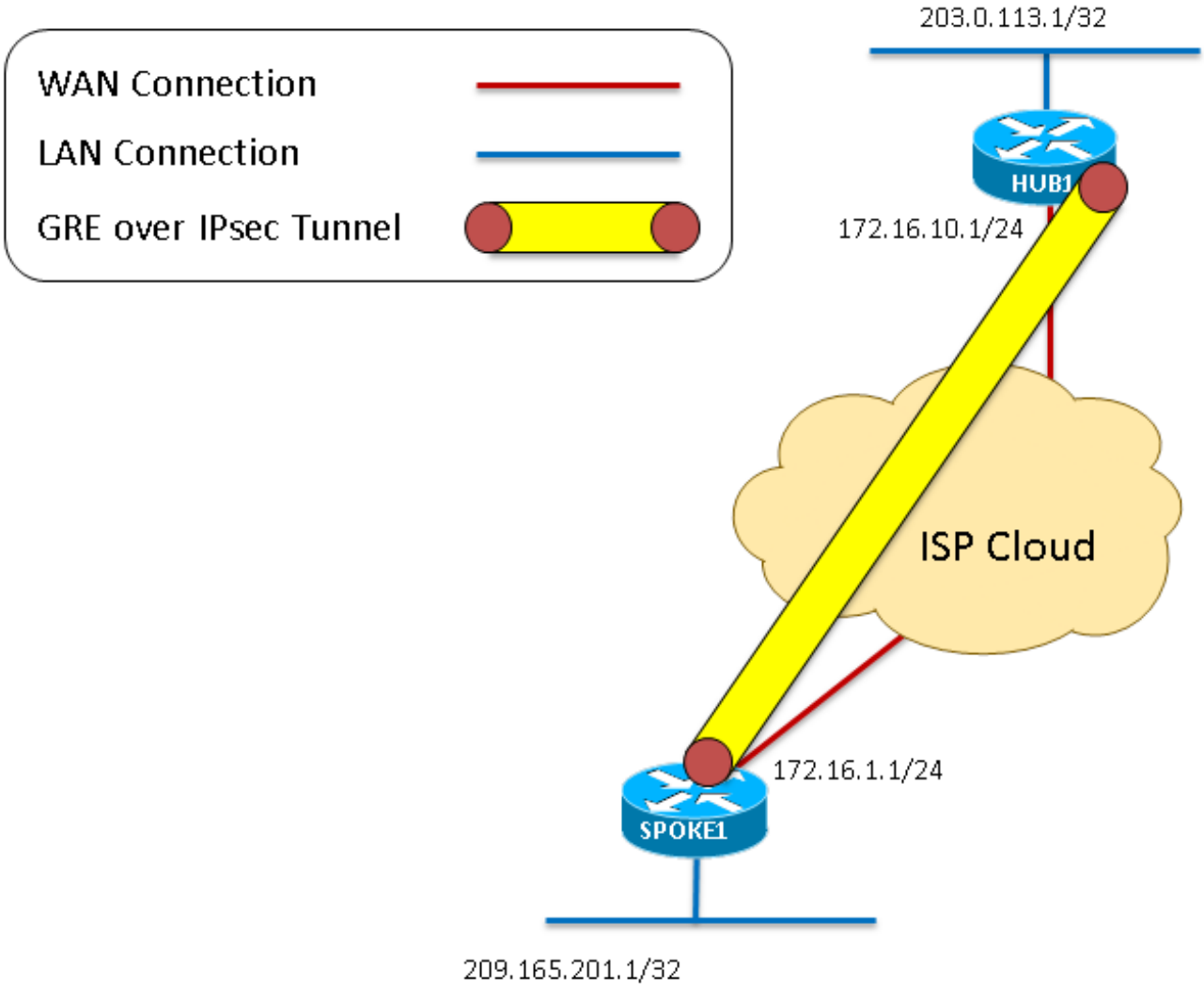
5. Uma vez que o spoke recebe o MM2, responde com MM3. Como com MM1, o spoke confirma a política de ISAKMP recebida é válido.
6. O hub recebe MM3 e responde com MM4.
7. Neste momento na negociação de ISAKMP, o spoke pôde responder na porta UDP4500 se o NAT é detectado no caminho de trânsito. Contudo, se nenhum NAT é detectado o spoke continua e envia MM5 em UDP500. Ultimamente, o hub responde com MM6 a fim terminar a troca do modo principal.
   O diagrama 3 - refere as etapas 5 a
   7



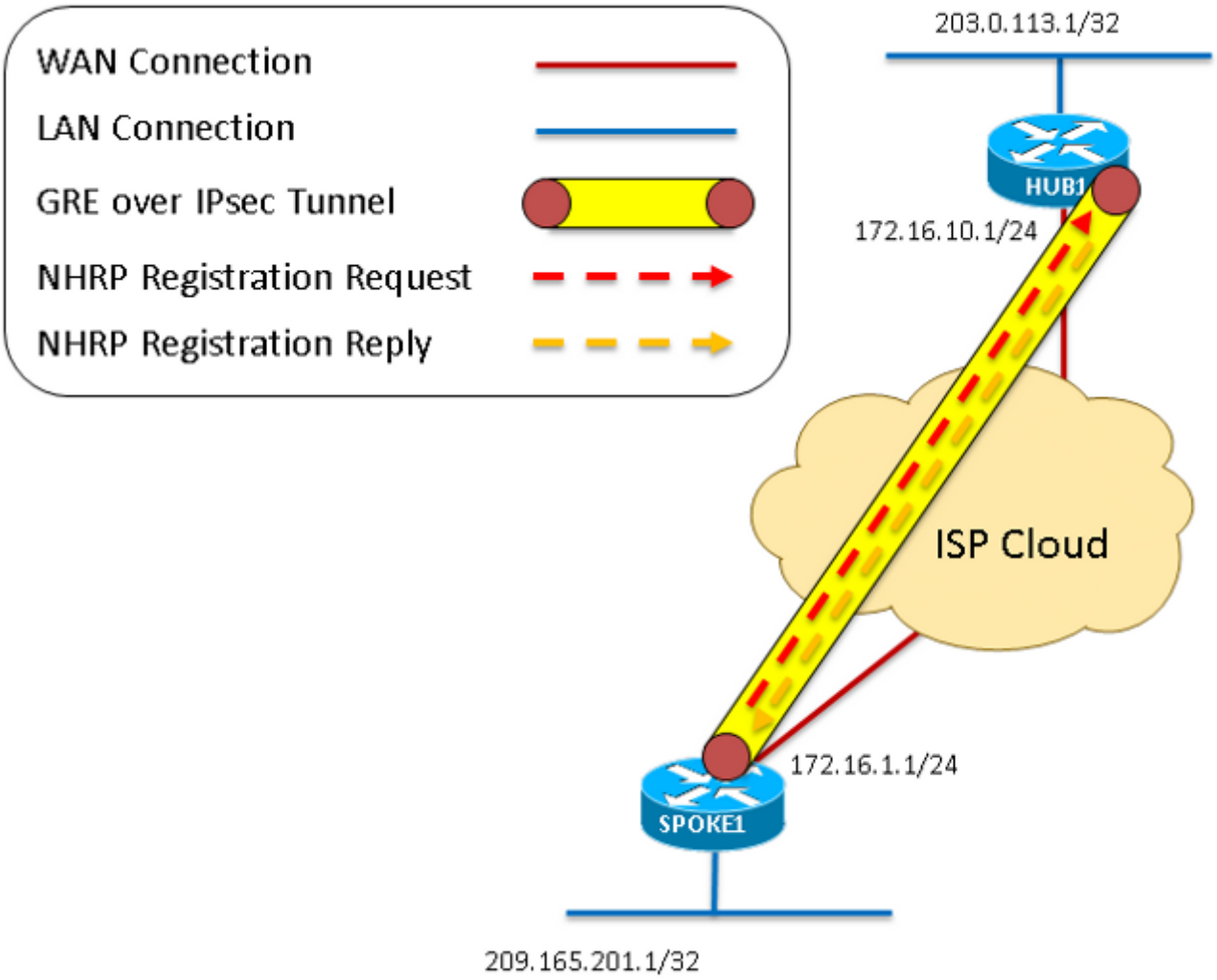
8. Uma vez que o spoke recebe MM6 do hub, envia QM1 ao hub em UDP500 a fim começar o Quick Mode.
9. O hub recebe QM1 e responde com QM2, como todos atributos recebidos são aceitados. Neste momento o hub cria a fase 2 SA para esta sessão.
10. Como a última etapa da negociação do Quick Mode, QM2 é recebido pelo spoke. O spoke então cria sua fase 2 SA e envia QM3 na resposta. Isto termina o ISAKMP e a negociação de IPSec. Há agora uma sessão IPSec que cifre o tráfego GRE entre estes dois pares.
    O diagrama 4 - refere etapas 8 ao
    10



11. Agora que a sessão de criptografia pode ascendente e passar o tráfego, estes pacotes estão encapsulados dentro do GRE sobre o túnel de IPsec.
    O diagrama 5 - refere etapa
    11



12. Como foi visto nas primeiras etapas, o spoke gerencie uma requisição de registro NHRP que seja enviada através do GRE sobre o túnel de IPsec.
13. O hub recebe as requisições de registro NHRP e envia uma resposta do registro NHRP uma vez que confirma o spoke tem um endereço válido do túnel e do multiacesso sem broadcast (NBMA). O spoke recebe esta resposta do registro NHRP que termina o processo de registro.
    O diagrama 6 - refere etapas 12
    13



Estes debugam são o resultado quando o **dmvpn debugar todo o comando all** é incorporado no Roteadores do hub and spoke. Este comando específico permite este grupo de debuga:

```
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
```

Debuga com explicação

Porque este é um configuraton onde o IPsec seja executado, debuga a mostra todo o ISAKMP e IPsec debuga. Se não cripto é configurado, ignoram alguns debuga esse começo com o “IPsec” ou o “ISAKMP.”

O HUB DEBUGA A EXPLICAÇÃO	DEBUGA EM ORDEM	O SPOKE DEBUG EXPLICAÇÃO
Estes primeiros debugam mensagens são gerados por um **comando no shutdown** inscrito na interface de túnel. As mensagens são geradas pelos serviços criptos, GRE, e NHRP que estão sendo iniciados. Um erro de registro NHRP é considerado no hub porque não tem um servidor de próximo salto (NHS) configurado (o hub é NHS para nossa nuvem DMVPN). Isto é esperado.	IPSEC-IFC MGRE/Tu0: Verificando o status de túnel. **NHRP: if_up: Tunnel0 0 proto** IPSEC-IFC MGRE/Tu0: túnel que vem acima IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start já que escuta **%CRYPTO-6-ISAKMP_ON_OFF: O ISAKMP está LIGADA** **NHRP: Incapaz de enviar o registro - nenhum NHSes configurou** %LINK-3-UPDOWN: Tunnel0 da relação, estado mudado a acima NHRP: if_up: Tunnel0 0 proto NHRP: Incapaz de enviar o registro - nenhum NHSes configurou IPSEC-IFC MGRE/Tu0: túnel que vem acima IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start já que escuta **%LINEPROTO-5-UPDOWN: Protocolo de linha no tunnel0 da relação, estado mudado a acima**	
	IPSEC-IFC GRE/Tu0: Verificando o status de túnel. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): a consulta da conexão retornou 0 **IPSEC-IFC GRE/Tu0: crypto_ss_listen_start já que escuta** **IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Abrindo um soquete com perfil DMVPN-IPSEC** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): a consulta da conexão retornou 0 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Provocando o túnel imediatamente. IPSEC-IFC GRE/Tu0: Adicionando a interface de túnel do tunnel0 à lista compartilhada **NHRP: if_up: Tunnel0 0 proto** **NHRP: Tunnel0: O esconderijo adiciona para o salto seguinte 10.1.1.254 do alvo 10.1.1.254/32** **172.16.10.1**	Estes primeiros debu mensagens são gera por um **comando no shutdown** inscrito na interface de túnel. As mensagens são gera pelos serviços cripto GRE, e NHRP que s iniciados. Adicionalmente, o sp adiciona uma entrad seu próprio esconde NHRP para seu próp endereço NBMA e d

	IPSEC-IFC GRE/Tu0: túnel que vem acima IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): conexão 961D220 retornado consulta IPSEC-IFC GRE/Tu0: crypto_ss_listen_start já que escuta IPSEC-IFC GRE/Tu0: crypto_ss_listen_start já que escuta IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Abrindo um soquete com perfil DMVPN-IPSEC IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): conexão 961D220 retornado consulta IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): O soquete está sendo aberto já. Ignorância. CRYPTO_SS (TÚNEL SEC): O aplicativo começou escutar a inserção do mapa no mapdb AVL falhado, pares do mapa + do ás já existe no mapdb **%CRYPTO-6-ISAKMP_ON_OFF: O ISAKMP está LIGADA** CRYPTO_SS (TÚNEL SEC): Active aberto, informação de soquete: 172.16.1.1 local 172.16.1.1/255.255.255.255/0, 172.16.10.1 remoto 172.16.10.1/255.255.255.255/0, prot 47, ifc Tu0	
COMEÇO DE ISAKMP (NEGOCIAÇÃO DA FASE I)		
	IPSEC(recalculate_mtu): restaure o MTU do sadb_root 94EFDC0 a 1500 **IPSEC(sa_request): ,** **(inglês chave. local= DE PARTIDA 172.16.1.1:500 dos msg.), remote= 172.16.10.1:500,** **local_proxy= 172.16.1.1/255.255.255.255/47/0 (type=1),** **remote_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1),** **protocol= ESP, esp-sha-hmac do esp-3des do transform= (transporte),** **lifedur= 3600s e 4608000kb,** **spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0** ISAKMP:(0): O perfil do pedido SA é (o ZERO) ISAKMP: Criou um struct do par para 172.16.10.1, a porta de peer 500 ISAKMP: O par novo criou o par = o peer_handle 0x95F6858 = o 0x80000004 ISAKMP: Travando o struct 0x95F6858 do par, refcount 1 para o isakmp_initiator ISAKMP: porta local 500, porta remota 500 ISAKMP: ajuste o novo nó 0 ao QM_IDLE ISAKMP:(0):insert sa com sucesso sa = 8A26FB0 **Modo assertivo do começo ISAKMP:(0):Can não, modo principal de tentativa.** Chave pré-compartilhada do par ISAKMP:(0):found que combina 172.16.10.1 ISAKMP:(0): NAT-T construído vendor-rfc3947 ID ISAKMP:(0): NAT-T construído vendor-07 ID	A primeira etapa um que o túnel não é “nenhuma parada programada” é come negociação cripto. A spoke cria um pedid tenta começar o mod assertivo e falha de ao modo principal. D que o modo assertiv é configurado em um outro roteador, este esperado. O spoke começa o m principal e envia o pr mensagem ISAKMP MM_NO_STATE. Mudanças de estado ISAKMP de IKE_RE IKE_I_MM1. As mensagens do V ID NAT-T são usada detecção e no traver NAT. Estas mensage são esperadas duran negociação do ISAK apesar de mesmo se NAT está executado as mensagens do m

	ISAKMP:(0): NAT-T construído vendor-03 ID ISAKMP:(0): NAT-T construído vendor-02 ID **ISAKMP:(0):Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM** **Estado ISAKMP:(0):Old = estado novo IKE_READY = IKE_I_MM1** **ISAKMP:(0): troca de começo do modo principal** **ISAKMP:(0): enviando o pacote ao peer_port 500 (i) MM_NO_STATE do my_port 500 de 172.16.10.1** ISAKMP:(0):sending um pacote IPv4 IKE. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): conexão 961D220 retornado consulta IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): mensagem pronta do bom soquete	assertivo, estes são esperados.
Depois que o túnel do raio não é “nenhuma parada programada,” o hub recebe a mensagem NOVA IKE SA (modo principal 1) na porta 500. Como o que responde, o hub cria uma associação de segurança ISAKMP (SA). As mudanças de estado ISAKMP de IKE_READY a IKE_R_MM1.	**ISAKMP (0): pacote recebido do esporte 500 do dport 500 de 172.16.1.1 global (N) SA NOVO** **ISAKMP: Criou um struct do par para 172.16.1.1, a porta de peer 500** ISAKMP: O par novo criou o par = o peer_handle 0x8CACD00 = o 0x80000003 ISAKMP: Travando o struct 0x8CACD00 do par, refcount 1 para o crypto_isakmp_process_block ISAKMP: porta local 500, porta remota 500 **ISAKMP:(0):insert sa com sucesso sa = 6A5BDE8** ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **Estado ISAKMP:(0):Old = estado novo IKE_READY = IKE_R_MM1**	
A mensagem recebida do modo principal 1 IKE é processada. O hub determina que o par tem atributos de harmonização ISAKMP e estão enchidos ISAKMP SA que foi criado apenas. As mensagens mostram que o par usa 3DES-CBC para a criptografia, picar do SHA, o grupo1 do Diffie Hellman (DH), a chave preshared para a autenticação, e a vida padrão SA de 86400 segundos (0x0 0x1 0x51 0x80 = 0x15180 = 86400 segundos). O estado ISAKMP é ainda IKE_R_MM1 desde que uma resposta tem não ser enviada ao spoke. As mensagens do Vendor ID NAT-T são usadas na	ISAKMP:(0): processando o payload SA. ID de mensagem = 0 ISAKMP:(0): processando o payload do Vendor ID **ISAKMP:(0): o Vendor ID parece má combinação Unity/DPD mas de major 69** **ISAKMP (0): o Vendor ID é RFC 3947 NAT-T** ISAKMP:(0): processando o payload do Vendor ID ISAKMP:(0): o Vendor ID parece má combinação Unity/DPD mas de major 245 ISAKMP (0): o Vendor ID é NAT-T v7 ISAKMP:(0): processando o payload do Vendor ID ISAKMP:(0): o Vendor ID parece má combinação Unity/DPD mas de major 157 ISAKMP:(0): o Vendor ID é NAT-T v3 ISAKMP:(0): processando o payload do Vendor ID ISAKMP:(0): o Vendor ID parece má combinação Unity/DPD mas de major 123 ISAKMP:(0): o Vendor ID é NAT-T v2 **Chave pré-compartilhada do par ISAKMP:(0):found que combina 172.16.1.1** **ISAKMP:(0): chave preshared local encontrada** ISAKMP: Perfis de varredura para o Xauth… **ISAKMP:(0):Checking ISAKMP transformam 1 contra a política da prioridade 1**	

detecção e no traversal do NAT. Estas mensagens são esperadas durante a negociação do ISAKMP apesar de mesmo se o NAT está executado. As mensagens similares são consideradas para o Dead Peer Detection (DPD).	**ISAKMP: criptografia 3DES-CBC** **ISAKMP: mistura SHA** **ISAKMP: grupo padrão 1** **ISAKMP: PRE-parte do AUTH** **ISAKMP: a vida datilografa dentro segundos** **ISAKMP: duração da vida (VPI) de 0x0 0x1 0x51 0x80** **ISAKMP:(0):atts são aceitáveis. O payload seguinte é 0** **Atts ISAKMP:(0):Acceptable: vida real: 0** **Atts ISAKMP:(0):Acceptable: vida: 0** **Atts ISAKMP:(0):Fill em sa vpi_length:4** **Atts ISAKMP:(0):Fill em sa life_in_seconds:86400** **Vida real ISAKMP:(0):Returning: 86400** **Temporizador da vida ISAKMP:(0)::started: 86400.** ISAKMP:(0): processando o payload do Vendor ID ISAKMP:(0): o Vendor ID parece má combinação Unity/DPD mas de major 69 ISAKMP (0): o Vendor ID é RFC 3947 NAT-T ISAKMP:(0): processando o payload do Vendor ID ISAKMP:(0): o Vendor ID parece má combinação Unity/DPD mas de major 245 ISAKMP (0): o Vendor ID é NAT-T v7 ISAKMP:(0): processando o payload do Vendor ID ISAKMP:(0): o Vendor ID parece má combinação Unity/DPD mas de major 157 ISAKMP:(0): o Vendor ID é NAT-T v3 ISAKMP:(0): processando o payload do Vendor ID ISAKMP:(0): o Vendor ID parece má combinação Unity/DPD mas de major 123 ISAKMP:(0): o Vendor ID é NAT-T v2 ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE Estado ISAKMP:(0):Old = estado IKE_R_MM1 novo = IKE_R_MM1	
MM_SA_SETUP (modo principal 2) é enviado ao spoke, que confirma que MM1 esteve recebido e aceitou como um pacote ISAKMP válido. Mudanças de estado ISAKMP de IKE_R_MM1 a IKE_R_MM2.	ISAKMP:(0): NAT-T construído vendor-rfc3947 ID **ISAKMP:(0): enviando o pacote ao peer_port 500 do my_port 500 de 172.16.1.1 (R) MM_SA_SETUP** ISAKMP:(0):sending um pacote IPv4 IKE. ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **Estado ISAKMP:(0):Old = estado IKE_R_MM1 novo = IKE_R_MM2**	
	ISAKMP (0): pacote recebido do esporte 500 (i) MM_NO_STATE global do dport 500 de 172.16.10.1 **ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH** **Estado ISAKMP:(0):Old = estado IKE_I_MM1 novo = IKE_I_MM2** ISAKMP:(0): processando o payload SA. ID de	Em resposta à mens MM1 enviada ao hub chega que confims c MM1 esteve recebid mensagem recebida modo principal 2 IKE processada. O spok realiza que o hub do

	mensagem = 0 ISAKMP:(0): processando o payload do Vendor ID **ISAKMP:(0): o Vendor ID parece má combinação Unity/DPD mas de major 69** ISAKMP (0): o Vendor ID é RFC 3947 NAT-T Chave pré-compartilhada do par ISAKMP:(0):found que combina 172.16.10.1 ISAKMP:(0): chave preshared local encontrada ISAKMP: Perfis de varredura para o Xauth… **ISAKMP:(0):Checking ISAKMP transformam 1 contra a política da prioridade 1** **ISAKMP: criptografia 3DES-CBC** **ISAKMP: mistura SHA** **ISAKMP: grupo padrão 1** **ISAKMP: PRE-parte do AUTH** **ISAKMP: a vida datilografa dentro segundos** **ISAKMP: duração da vida (VPI) de 0x0 0x1 0x51 0x80** **ISAKMP:(0):atts são aceitáveis. O payload seguinte é 0** **Atts ISAKMP:(0):Acceptable: vida real: 0** **Atts ISAKMP:(0):Acceptable: vida: 0** **Atts ISAKMP:(0):Fill em sa vpi_length:4** **Atts ISAKMP:(0):Fill em sa life_in_seconds:86400** **Vida real ISAKMP:(0):Returning: 86400** **Temporizador da vida ISAKMP:(0)::started: 86400.** ISAKMP:(0): processando o payload do Vendor ID ISAKMP:(0): o Vendor ID parece má combinação Unity/DPD mas de major 69 ISAKMP (0): o Vendor ID é RFC 3947 NAT-T ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE Estado ISAKMP:(0):Old = estado IKE_I_MM2 novo = IKE_I_MM2	tem atributos de harmonização ISAK estes atributos estão enchidos ISAKMP S foi criado. Este paco mostra que o par usa 3DES-CBC para a criptografia, picar do o grupo1 do Diffie He (DH), a chave presha para a autenticação, vida padrão SA de 8 segundos (0x0 0x1 0 0x80 = 0x15180 = 86 segundos). Além do que as mensagens NAT-T, troca para determina sessão usará o DPD As mudanças de est ISAKMP de IKE_I_M IKE_I_MM2.
	ISAKMP:(0): enviando o pacote ao peer_port 500 (i) MM_SA_SETUP do my_port 500 de 172.16.10.1 ISAKMP:(0):sending um pacote IPv4 IKE. ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **Estado ISAKMP:(0):Old = estado IKE_I_MM2 novo = IKE_I_MM3**	MM_SA_SETUP (mo principal 3) é enviad hub, que confirma qu spoke recebeu MM2 gostou de continuar. As mudanças de est ISAKMP de IKE_I_M IKE_I_MM3.
MM_SA_SETUP (modo principal 3) é recebido pelo hub. O hub conclui que o par é um outro dispositivo IOS Cisco e nenhum NAT está detectado para nós ou nosso par. As mudanças de estado ISAKMP de IKE_R_MM2 a IKE_R_MM3.	**ISAKMP (0): pacote recebido do esporte 500 do dport 500 de 172.16.1.1 global (R) MM_SA_SETUP** ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **Estado ISAKMP:(0):Old = estado IKE_R_MM2 novo = IKE_R_MM3** ISAKMP:(0): processando o payload KE. ID de mensagem = 0 ISAKMP:(0): processando o payload do NONCE. ID	

	de mensagem = 0 **Chave pré-compartilhada do par ISAKMP:(0):found que combina 172.16.1.1** ISAKMP:(1002): processando o payload do Vendor ID ISAKMP:(1002): o Vendor ID é DPD ISAKMP:(1002): processando o payload do Vendor ID **ISAKMP:(1002): discurso a uma outra caixa IO!** ISAKMP:(1002): processando o payload do Vendor ID ISAKMP:(1002): o Vendor ID parece má combinação Unity/DPD mas de major 225 ISAKMP:(1002): o Vendor ID é XAUTH ISAKMP: tipo de payload recebido 20 **ISAKMP (1002): O seu não pica nenhum fósforo - este nó fora do NAT** ISAKMP: tipo de payload recebido 20 **ISAKMP (1002): Nenhum NAT encontrado para o auto ou o par** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE Estado ISAKMP:(1002):Old = estado IKE_R_MM3 novo = IKE_R_MM3	
MM_KEY_EXCH (modo principal 4) é enviado pelo hub. Mudanças de estado ISAKMP de IKE_R_MM3 a IKE_R_MM4.	**ISAKMP:(1002): enviando o pacote ao peer_port 500 do my_port 500 de 172.16.1.1 (R) MM_KEY_EXCH** ISAKMP:(1002):sending um pacote IPv4 IKE. ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **Estado ISAKMP:(1002):Old = estado IKE_R_MM3 novo = IKE_R_MM4**	
	ISAKMP (0): pacote recebido do esporte 500 (i) MM_SA_SETUP global do dport 500 de 172.16.10.1 ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **Estado ISAKMP:(0):Old = estado IKE_I_MM3 novo = IKE_I_MM4** ISAKMP:(0): processando o payload KE. ID de mensagem = 0 ISAKMP:(0): processando o payload do NONCE. ID de mensagem = 0 **Chave pré-compartilhada do par ISAKMP:(0):found que combina 172.16.10.1** ISAKMP:(1002): processando o payload do Vendor ID ISAKMP:(1002): o Vendor ID é Unity ISAKMP:(1002): processando o payload do Vendor ID ISAKMP:(1002): o Vendor ID é DPD ISAKMP:(1002): processando o payload do Vendor ID **ISAKMP:(1002): discurso a uma outra caixa IO!** ISAKMP: tipo de payload recebido 20 **ISAKMP (1002): O seu não pica nenhum fósforo - este nó fora do NAT** ISAKMP: tipo de payload recebido 20 **ISAKMP (1002): Nenhum NAT encontrado para o auto ou o par**	MM_SA_SETUP (mo principal 4) é recebid spoke. O spoke conc o par é um outro disp IOS Cisco e nenhum está detectado para nosso par. As mudanças de est ISAKMP de IKE_I_M IKE_I_MM4.

	ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE Estado ISAKMP:(1002):Old = estado IKE_I_MM4 novo = IKE_I_MM4	
	Contato inicial ISAKMP:(1002):send **ISAKMP:(1002):sA está fazendo a autenticação da chave pré-compartilhada usando o tipo ID_IPV4_ADDR identificação** ISAKMP (1002): Payload ID seguinte-payload: 8 tipo: 1 endereço: 172.16.1.1 protocolo: 17 porta: 500 comprimento: 12 Comprimento de carga útil ISAKMP:(1002):Total: 12 **ISAKMP:(1002): enviando o pacote ao peer_port 500 (i) MM_KEY_EXCH do my_port 500 de 172.16.10.1** ISAKMP:(1002):sending um pacote IPv4 IKE. ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **Estado ISAKMP:(1002):Old = estado IKE_I_MM4 novo = IKE_I_MM5**	MM_KEY_EXCH (mo principal 5) é enviad spoke. As mudanças de est ISAKMP de IKE_I_M IKE_I_MM5.
MM_KEY_EXCH (modo principal 5) é recebido pelo hub. As mudanças de estado ISAKMP de IKE_R_MM4 a IKE_R_MM5. Adicionalmente, do “o *none* dos fósforos par dos perfis” é considerado devido à falta de um perfil ISAKMP. Porque este é o caso, o ISAKMP não usa um perfil.	**ISAKMP (1002): pacote recebido do esporte 500 do dport 500 de 172.16.1.1 global (R) MM_KEY_EXCH** ISAKMP:(1002):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **Estado ISAKMP:(1002):Old = estado IKE_R_MM4 novo = IKE_R_MM5** ISAKMP:(1002): payload do processamento ID. ID de mensagem = 0 ISAKMP (1002): Payload ID seguinte-payload: 8 tipo: 1 endereço: 172.16.1.1 protocolo: 17 porta: 500 comprimento: 12 **ISAKMP:(0):: o par combina o *none* dos perfis** ISAKMP:(1002): processando o payload da MISTURA. ID de mensagem = 0 ISAKMP:(1002): processar NOTIFICA o protocolo 1 INITIAL_CONTACT spi 0, ID de mensagem = 0, sa = 0x6A5BDE8 Status de autenticação ISAKMP:(1002):sA: autenticado ISAKMP:(1002):sA foi autenticado com 172.16.1.1 Status de autenticação ISAKMP:(1002):sA: autenticado ISAKMP:(1002): Contato inicial do processo, traga SA para baixo existentes da fase 1 e 2 com porta remota remota local 500 de 172.16.10.1	

	172.16.1.1 **ISAKMP: Tentando introduzir um par 172.16.10.1/172.16.1.1/500/, e 8CACD00 com sucesso introduzido.** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE Estado ISAKMP:(1002):Old = estado IKE_R_MM5 novo = IKE_R_MM5 IPSEC(key_engine): obteve um evento da fila com 1 mensagem KMI ISAKMP:(1002):sA está fazendo a autenticação da chave pré-compartilhada usando o tipo ID_IPV4_ADDR identificação ISAKMP (1002): Payload ID seguinte-payload: 8 tipo: 1 endereço: 172.16.10.1 protocolo: 17 porta: 500 comprimento: 12 Comprimento de carga útil ISAKMP:(1002):Total: 12	
O pacote final MM_KEY_EXCH (modo principal 6) é enviado pelo hub. Isto termina a negociação da fase 1 que significa este dispositivo está pronta para a fase 2 (Quick Mode do IPsec). As mudanças de estado ISAKMP de IKE_R_MM5 a IKE_P1_COMPLETE.	**ISAKMP:(1002): enviando o pacote ao peer_port 500 do my_port 500 de 172.16.1.1 (R) MM_KEY_EXCH** ISAKMP:(1002):sending um pacote IPv4 IKE. ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **Estado ISAKMP:(1002):Old = estado IKE_R_MM5 novo = IKE_P1_COMPLETE** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE Estado ISAKMP:(1002):Old = estado novo IKE_P1_COMPLETE = IKE_P1_COMPLETE	
	ISAKMP (1002): pacote recebido do esporte 500 (i) MM_KEY_EXCH global do dport 500 de 172.16.10.1 ISAKMP:(1002): payload do processamento ID. ID de mensagem = 0 ISAKMP (1002): Payload ID seguinte-payload: 8 tipo: 1 endereço: 172.16.10.1 protocolo: 17 porta: 500 comprimento: 12 **ISAKMP:(0):: o par combina o *none* dos perfis** ISAKMP:(1002): processando o payload da MISTURA. ID de mensagem = 0 Status de autenticação ISAKMP:(1002):sA: autenticado ISAKMP:(1002):sA foi autenticado com 172.16.10.1 **ISAKMP: Tentando introduzir um par 172.16.1.1/172.16.10.1/500/, e 95F6858 com sucesso**	O pacote final MM_KEY_EXCH (mo principal 6) é recebic spoke. Isto termina a negociação da fase significa este disposi está pronta para a fa (Quick Mode do IPse As mudanças de est ISAKMP de IKE_I_M IKE_I_MM6, e então imediatamente a IKE_P1_COMPLETE Adicionalmente, do “ *none* dos fósforos dos perfis” é conside devido à falta de um ISAKMP. Porque est caso, o ISAKMP não

	introduzido. ISAKMP:(1002):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH **Estado ISAKMP:(1002):Old = estado IKE_I_MM5 novo = IKE_I_MM6** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE Estado ISAKMP:(1002):Old = estado IKE_I_MM6 novo = IKE_I_MM6 ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **Estado ISAKMP:(1002):Old = estado IKE_I_MM6 novo = IKE_P1_COMPLETE**	um perfil.
FIM DE ISAKMP (NEGOCIAÇÃO DA FASE I), COMEÇO DA NEGOCIAÇÃO DO IPSEC (FASE II)		
	Troca do Quick Mode ISAKMP:(1002):beginning, MEADOS DE de 3464373979 O iniciador ISAKMP:(1002):QM obtém o spi **ISAKMP:(1002): enviando o pacote ao peer_port 500 (i) QM_IDLE do my_port 500 de 172.16.10.1** ISAKMP:(1002):sending um pacote IPv4 IKE. ISAKMP:(1002):Node 3464373979, entrada = IKE_MESG_INTERNAL, IKE_INIT_QM **Estado ISAKMP:(1002):Old = estado novo IKE_QM_READY = IKE_QM_I_QM1** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE Estado ISAKMP:(1002):Old = estado novo IKE_P1_COMPLETE = IKE_P1_COMPLETE	A troca do Quick Mo (fase II, IPsec) come spoke enviar a prime mensagem QM ao h
O hub recebe o primeiro pacote do quick mode (QM) que tem o propósito de IPSec. Os atributos recebidos especificam aquele: os encaps embandeiram o grupo a 2 (o modo de transporte, uma bandeira de 1 seria modo de túnel), a vida padrão SA de 3600 segundos e de 4608000 quilobytes (0x465000 encantam dentro), o HMAC-SHA para a autenticação, e o 3DES para a criptografia. Porque estes são os mesmos atributos ajustados na configuração local, a proposta é aceitada e o shell IPsec SA é criado. Desde que nenhum valor	**ISAKMP (1002): pacote recebido do esporte 500 do dport 500 de 172.16.1.1 global (R) QM_IDLE** **ISAKMP: ajuste o novo nó -830593317 ao QM_IDLE** ISAKMP:(1002): processando o payload da MISTURA. ID de mensagem = 3464373979 ISAKMP:(1002): processando o payload SA. ID de mensagem = 3464373979 **Propósito de IPSec 1 ISAKMP:(1002):Checking** **ISAKMP: transforme 1, ESP_3DES** **ISAKMP: os atributos transformam dentro:** **ISAKMP: os encaps são 2 (o transporte)** **ISAKMP: A vida SA datilografa dentro segundos** **ISAKMP: Duração da vida SA (básica) de 3600** **ISAKMP: A vida SA datilografa dentro quilobytes** **ISAKMP: Duração da vida SA (VPI) de 0x0 0x46 0x50 0x0** **ISAKMP: o autenticador é HMAC-SHA** **ISAKMP:(1002):atts são aceitáveis.** IPSEC(validate_proposal_request): peça #1 da proposta IPSEC(validate_proposal_request): peça #1 da proposta,	

do Security Parameter Index (SPI) é associado com o estes ainda, este é apenas um shell de um SA que não possa ser usado para passar ainda o tráfego.	**(inglês chave. local= DE ENTRADA 172.16.10.1:0 dos msg.), remote= 172.16.1.1:0, local_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1), remote_proxy= 172.16.1.1/255.255.255.255/47/0 (type=1), protocol= ESP, transform= NENHUNS (transporte), lifedur= 0s e 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0**	
Estas são apenas as mensagens de serviço IPSec gerais que dizem que trabalham corretamente.	IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): a consulta da conexão retornou 0 IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start já que escuta **IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Abrindo um soquete com perfil DMVPN-IPSEC** IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): a consulta da conexão retornou 0 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Provocando o túnel imediatamente. IPSEC-IFC MGRE/Tu0: Adicionando a interface de túnel do tunnel0 à lista compartilhada 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): Bom escuta o pedido	
a entrada de mapa Pseudo--cripto é criada para o protocolo IP 47 (GRE) de 172.16.10.1 (endereço público do hub) a 172.16.1.1 (endereço público do spoke). Um IPsec SA/SPI é criado para ambos o tráfego de entrada e de saída com os valores da proposta aceitada.	a inserção do mapa no mapdb AVL falhado, pares do mapa + do ás já existe no mapdb CRYPTO_SS (TÚNEL SEC): Voz passiva aberta, informação de soquete: 172.16.10.1 local 172.16.10.1/255.255.255.255/0, 172.16.1.1 remoto 172.16.1.1/255.255.255.255/0, prot 47, ifc Tu0 Mapdb cripto: proxy_match **ADDR do src: 172.16.10.1** **ADDR do dst: 172.16.1.1** **protocolo: 47** porta do src: 0 porta do dst: 0 ISAKMP:(1002): processando o payload do NONCE. ID de mensagem = 3464373979 ISAKMP:(1002): payload do processamento ID. ID de mensagem = 3464373979 ISAKMP:(1002): payload do processamento ID. ID de mensagem = 3464373979 O que responde ISAKMP:(1002):QM obtém o spi ISAKMP:(1002):Node 3464373979, entrada = IKE_MESG_FROM_PEER, IKE_QM_EXCH **Estado ISAKMP:(1002):Old = estado novo IKE_QM_READY = IKE_QM_SPI_STARVE** **ISAKMP:(1002): Criando o sas de IPSec** **SA de entrada de 172.16.1.1 a 172.16.10.1 (f/i) 0 0** **(proxy 172.16.1.1 a 172.16.10.1)** **tem o spi 0xDD2AC2B3 e o conn_id 0**	

	vida de 3600 segundos **vida de 4608000 quilobytes** **SA de partida de 172.16.10.1 a 172.16.1.1 (f/i) 0/0** **(proxy 172.16.10.1 a 172.16.1.1)** **tem o spi 0x82C3E0C4 e o conn_id 0** **vida de 3600 segundos** **vida de 4608000 quilobytes**	
A segunda mensagem QM enviada pelo hub. Mensagem gerada pelo serviço IPSec que confirma que a proteção do túnel está acima no tunnel0. Uma outra mensagem da criação SA é considerada que tenha o ips de destino, SPI, transforma atributos ajustados, e vida em permanecer dos quilobytes e dos segundos.	**ISAKMP:(1002): enviando o pacote ao peer_port 500 do my_port 500 de 172.16.1.1 (R) QM_IDLE** ISAKMP:(1002):sending um pacote IPv4 IKE. ISAKMP:(1002):Node 3464373979, entrada = IKE_MESG_INTERNAL, IKE_GOT_SPI **Estado ISAKMP:(1002):Old = estado novo IKE_QM_SPI_STARVE = IKE_QM_R_QM2** CRYPTO_SS (TÚNEL SEC): Emperramento terminado do aplicativo ao soquete IPSEC(key_engine): obteve um evento da fila com 1 mensagem KMI Mapdb cripto: proxy_match ADDR do src: 172.16.10.1 ADDR do dst: 172.16.1.1 protocolo: 47 porta do src: 0 porta do dst: 0 IPSEC(crypto_ipsec_sa_find_ident_head): reconexão com os mesmos proxys e par 172.16.1.1 IPSEC(policy_db_add_ident): src 172.16.10.1, dest 172.16.1.1, dest_port 0 **IPSEC(create_sa): sa criado,** sa_dest= (sa) 172.16.10.1, 50 pés do sa_proto=, sa_spi= 0xDD2AC2B3(3710567091), esp-sha-hmac do esp-3des do sa_trans=, sa_conn_id= 3 sa_lifetime (k/sec) = (4536779/3600) **IPSEC(create_sa): sa criado,** sa_dest= (sa) 172.16.1.1, 50 pés do sa_proto=, sa_spi= 0x82C3E0C4(2193875140), esp-sha-hmac do esp-3des do sa_trans=, sa_conn_id= 4 sa_lifetime (k/sec) = (4536779/3600) IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce): atualizando a identificação 8B6A0E8 do tunnel0 com tun_decap_oce 6A648F0 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): conexão 8C93888 retornado consulta IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): mensagem pronta do bom soquete IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): conexão 8C93888 retornado consulta **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): Sinalizando o NHRP IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): MTU obtido 1458 da mensagem MTU IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): conexão 8C93888 retornado consulta	
	ISAKMP (1002): pacote recebido do esporte 500 (i) QM_IDLE global do dport 500 de 172.16.10.1 ISAKMP:(1002): processando o payload da MISTURA. ID de mensagem = 3464373979 ISAKMP:(1002): processando o payload SA. ID de mensagem = 3464373979 **Propósito de IPSec 1 ISAKMP:(1002):Checking ISAKMP: transforme 1, ESP_3DES** **ISAKMP: os atributos transformam dentro:** **ISAKMP: os encaps são 2 (o transporte)** **ISAKMP: A vida SA datilografa dentro segundos** **ISAKMP: Duração da vida SA (básica) de 3600** **ISAKMP: A vida SA datilografa dentro quilobytes** **ISAKMP: Duração da vida SA (VPI) de 0x0 0x46 0x50 0x0** **ISAKMP: o autenticador é HMAC-SHA** **ISAKMP:(1002):atts são aceitáveis.** IPSEC(validate_proposal_request): peça #1 da proposta IPSEC(validate_proposal_request): peça #1 da proposta, **(inglês chave. local= DE ENTRADA 172.16.1.1:0 dos msg.), remote= 172.16.10.1:0,** **local_proxy= 172.16.1.1/255.255.255.255/47/0 (type=1),** **remote_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1),** **protocol= ESP, transform= NENHUNS (transporte),** **lifedur= 0s e 0kb,** **spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0** **Mapdb cripto: proxy_match** **ADDR do src: 172.16.1.1** **ADDR do dst: 172.16.10.1** **protocolo: 47** **porta do src: 0** **porta do dst: 0**	O spoke recebe o se pacote QM que tem propósito de IPSec. confirma que QM1 e recebido pelo hub. C atributos recebidos especificam aquele: encaps embandeiran grupo a 2 (o modo d transporte, uma ban de 1 seria modo de t a vida padrão SA de segundos e de 4608 quilobytes (0x46500 encantam dentro), o HMAC-SHA para a autenticação, e o DE a criptografia. Porqu são os mesmos atrib ajustados na configu local, a proposta é a e o shell IPsec SA é Desde que nenhum do Security Paramet Index (SPI) é associa com o estes ainda, e apenas um shell de que não possa ser u para passar ainda o tráfego. A entrada de mapa pseudo--cripto é cria para o protocolo IP 4 (GRE) de 172.16.10. (endereço público do a 172.16.1.1 (endere público do spoke).
	ISAKMP:(1002): processando o payload do NONCE. ID de mensagem = 3464373979 ISAKMP:(1002): payload do processamento ID. ID de mensagem = 3464373979 ISAKMP:(1002): payload do processamento ID. ID de mensagem = 3464373979 **ISAKMP:(1002): Criando o sas de IPSec** **SA de entrada de 172.16.10.1 a 172.16.1.1 (f/i) 0 0** **(proxy 172.16.10.1 a 172.16.1.1)**	Um IPsec SA/SPI é para ambos o tráfeg entrada e de saída c valores da proposta aceitada.

	tem o spi 0x82C3E0C4 e o conn_id 0 **vida de 3600 segundos** **vida de 4608000 quilobytes** **SA de partida de 172.16.1.1 a 172.16.10.1 (f/i) 0/0** **(proxy 172.16.1.1 a 172.16.10.1)** **tem o spi 0xDD2AC2B3 e o conn_id 0** **vida de 3600 segundos** **vida de 4608000 quilobytes**	
	ISAKMP:(1002): enviando o pacote ao peer_port 500 (i) QM_IDLE do my_port 500 de 172.16.10.1 ISAKMP:(1002):sending um pacote IPv4 IKE. Razão FALSA do erro do nó -830593317 ISAKMP:(1002):deleting “nenhum erro” ISAKMP:(1002):Node 3464373979, entrada = IKE_MESG_FROM_PEER, IKE_QM_EXCH **Estado ISAKMP:(1002):Old = estado IKE_QM_I_QM1 novo = IKE_QM_PHASE2_COMPLETE** IPSEC(key_engine): obteve um evento da fila com 1 mensagem KMI Mapdb cripto: proxy_match ADDR do src: 172.16.1.1 ADDR do dst: 172.16.10.1 protocolo: 47 porta do src: 0 porta do dst: 0 IPSEC(crypto_ipsec_sa_find_ident_head): reconexão com os mesmos proxys e par 172.16.10.1 IPSEC(policy_db_add_ident): src 172.16.1.1, dest 172.16.10.1, dest_port 0 **IPSEC(create_sa): sa criado,** sa_dest= (sa) 172.16.1.1, 50 pés do sa_proto=, sa_spi= 0x82C3E0C4(2193875140), esp-sha-hmac do esp-3des do sa_trans=, sa_conn_id= 3 sa_lifetime (k/sec) = (4499172/3600) **IPSEC(create_sa): sa criado,** sa_dest= (sa) 172.16.10.1, 50 pés do sa_proto=, sa_spi= 0xDD2AC2B3(3710567091), esp-sha-hmac do esp-3des do sa_trans=, sa_conn_id= 4 sa_lifetime (k/sec) = (4499172/3600) **IPSEC(update_current_outbound_sa): obtenha permitem o par 172.16.10.1 SA sa de partida atual a SPI DD2AC2B3** **IPSEC(update_current_outbound_sa): sa de partida atual de 172.16.10.1 do par actualizado a SPI DD2AC2B3** IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce): atualizando a identificação 94F2740 do tunnel0 com tun_decap_oce 794ED30 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):	O spoke envia a terc mensagem final QM hub, que termina a tr QM. Ao contrário do ISAKMP aonde cada atravessa cada esta (MM1 com MM6/P1_COMPLET IPsec é um pouco de mais diferente que h somente três mensa um pouco do que se iniciador (nosso falou caso, como significa “me” na mensagem IKE_QM_I_QM1) vai QM_READY, então a QM_I_QM1 diretame QM_PHASE2_COMI O que responde (hub QM_READY, QM_SPI_STARVE, QM_R_QM2, QM_PHASE2_COMI Uma outra mensage criação SA é conside que tenha o ips de d SPI, transforma atrib ajustados, e vida em permanecer dos quil e dos segundos.

	conexão 961D220 retornado consulta 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): Sinalizando o NHRP NHRP: Concluiu a transição da prioridade 0 do conjunto 0 do vrf 0 do tunnel0 de NHS 10.1.1.254 a “E” de '' IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): conexão 961D220 retornado consulta NHRP: Tentativa enviar o pacote através de DEST 10.1.1.254	
Estas mensagens finais QM confirmam que o Quick Mode está completo e o IPsec está acima em ambos os lados do túnel. Ao contrário do ISAKMP aonde cada par atravessa cada estado (MM1 com MM6/P1_COMPLETE), o IPsec é um pouco de por mais diferente que haja somente três mensagens um pouco do que seis. O que responde (nosso hub neste caso, como significado pelo “R” na mensagem IKE_QM_R_QM1) vai QM_READY, QM_SPI_STARVE, QM_R_QM2, QM_PHASE2_COMPLETE. O iniciador (spoke) vai de QM_READY, então a QM_I_QM1 diretamente a QM_PHASE2_COMPLETE.	**ISAKMP (1002): pacote recebido do esporte 500 do dport 500 de 172.16.1.1 global (R) QM_IDLE** Razão FALSA “QM do erro do nó -830593317 ISAKMP:(1002):deleting feita (espere)” ISAKMP:(1002):Node 3464373979, entrada = IKE_MESG_FROM_PEER, IKE_QM_EXCH **Estado ISAKMP:(1002):Old = estado IKE_QM_R_QM2 novo = IKE_QM_PHASE2_COMPLETE** IPSEC(key_engine): obteve um evento da fila com 1 mensagem KMI IPSEC(key_engine_enable_outbound): o rec'd permite notifica do ISAKMP **IPSEC(key_engine_enable_outbound): permita o SA com spi 2193875140/50** **IPSEC(update_current_outbound_sa): obtenha permitem o par 172.16.1.1 SA sa de partida atual a SPI 82C3E0C4** **IPSEC(update_current_outbound_sa): sa de partida atual de 172.16.1.1 do par actualizado a SPI 82C3E0C4**	
	NHRP: Envie a requisição de registro através do vrf 0 do tunnel0, tamanho do pacote: 108 **src: 10.1.1.1, dst: 10.1.1.254** (f) afn: IPv4(1), tipo: IP(800), salto: 255, ver: 1 shtl: 4(NSAP), sstl: 0(NSAP) pktsz: extoff 108: 52 (M) bandeiras: “nat original”, reqid: 65540 **src NBMA: 172.16.1.1** **protocolo do src: 10.1.1.1, protocolo do dst: 10.1.1.254** Código (C-1): nenhum error(0) prefixo: 32, MTU: 17912, hd_time: 7200 addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0	Esta é as requisiçõe registro NHRP envia hub na tentativa de registrar-se a NHS (É normal ver múltiplo destes, porque o spo continua a tentar se registrar com NHS a receba do “uma resp registro.” **src, dst**: Endereços I Um ou Mais Servido Cisco ICM NT do ori de túnel (spoke) e do

	Endereço do que responde Extension(3): Registro dianteiro de NHS do trânsito Extension(4): Inverta o registro de NHS do trânsito Extension(5): **Autenticação Extension(7):** **type:Cleartext(1), dados: NHRPAUTH** Endereço NAT Extension(9): Código (C-1): nenhum error(0) prefixo: 32, MTU: 17912, hd_time: 0 addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0 **cliente NBMA: 172.16.10.1** **protocolo de cliente: 10.1.1.254**	destino (hub). Estes fonte e o destino do GRE enviado pelo ro **src NBMA**: o endere NBMA (Internet) do s que enviaram estes e tentativas para se registrar com NHS **protocolo do src**: end do túnel do spoke qu tenta se registrar **protocolo do dst**: end do túnel do NHS/hub **Extensão da autentic** dados: Corda da autenticação de NHF **cliente NBMA**: Ender NBMA do NHS/hub **protocolo de cliente**: endereço do túnel do NHS/hub
	NHRP-RATE: Enviando a requisição de registro inicial para 10.1.1.254, reqid 65540 **%LINK-3-UPDOWN: Tunnel0 da relação, estado mudado a acima** NHRP: if_up: Tunnel0 0 proto **NHRP: Tunnel0: Atualização do esconderijo para o salto seguinte 10.1.1.254 do alvo 10.1.1.254/32 172.16.10.1** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): conexão 961D220 retornado consulta NHRP: Tentativa enviar o pacote através de DEST 10.1.1.254	Mais mensagens de serviço NHRP que d requisição de registr inicial foram enviado NHS em 10.1.1.254. igualmente uma confirmação que um entrada de cache es adicionada para IP 10.1.1.254/24 do tún esse vidas em NBM 172.16.10.1. A mens atrasada diz que o tú “nenhum fechado” es considerado aqui.
	IPSEC-IFC GRE/Tu0: túnel que vem acima IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): conexão 961D220 retornado consulta IPSEC-IFC GRE/Tu0: crypto_ss_listen_start já que escuta IPSEC-IFC GRE/Tu0: crypto_ss_listen_start já que escuta **IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Abrindo um soquete com perfil DMVPN-IPSEC** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): conexão 961D220 retornado consulta IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): O soquete está já aberto. Ignorância. %LINEPROTO-5-UPDOWN: Protocolo de linha no tunnel0 da relação, estado mudado a acima	Estas são as mensa de serviço IPSec ge que dizem que traba corretamente. É aqu se vê finalmente que protocolo de túnel es acima.
Esta é as requisições de registro NHRP recebidas	**NHRP: Receba a requisição de registro através do vrf 0 do tunnel0, tamanho do pacote: 108**	

do spoke na tentativa de registrar-se a NHS (o hub). É normal ver múltiplos destes, porque o spoke continua a tentar se registrar com NHS até que receba do “uma resposta registro.” **src NBMA**: o endereço NBMA (Internet) do spoke que enviaram estes pacote e tentativas para se registrar com NHS **protocolo do src**: escave um túnel o endereço do spoke que tenta se registrar **protocolo do dst**: endereço do túnel do NHS/hub **Extensão da autenticação**, dados: Corda da autenticação de NHRP **cliente NBMA**: Endereço NBMA do NHS/hub **protocolo de cliente**: endereço do túnel do NHS/hub	(f) afn: IPv4(1), tipo: IP(800), salto: 255, ver: 1 shtl: 4(NSAP), sstl: 0(NSAP) pktsz: extoff 108: 52 (M) bandeiras: “nat original”, reqid: 65540 **src NBMA: 172.16.1.1** **protocolo do src: 10.1.1.1, protocolo do dst: 10.1.1.254** Código (C-1): nenhum error(0) prefixo: 32, MTU: 17912, hd_time: 7200 addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0 Endereço do que responde Extension(3): Registro dianteiro de NHS do trânsito Extension(4): Inverta o registro de NHS do trânsito Extension(5): **Autenticação Extension(7):** **type:Cleartext(1), dados: NHRPAUTH** Endereço NAT Extension(9): Código (C-1): nenhum error(0) prefixo: 32, MTU: 17912, hd_time: 0 addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0 **cliente NBMA: 172.16.10.1** **protocolo de cliente: 10.1.1.254**	
O NHRP debuga os pacotes que adicionam a rede do alvo 10.1.1.1/32 disponível através do salto seguinte de 10.1.1.1 no NHRP de 172.16.1.1. 172.16.1.1 é adicionado igualmente à lista de endereços a que do hub o tráfego multicast para a frente. Estas mensagens confirmam que o registro era bem sucedido, como eram uma definição para o endereço do túnel do spokes.	NHRP: netid_in = 1, to_us = 1 **NHRP: Tunnel0: O esconderijo adiciona para o salto seguinte 10.1.1.1 do alvo 10.1.1.1/32 172.16.1.1** **NHRP: Adicionando os pontos finais de túnel (VPN: 10.1.1.1, NBMA: 172.16.1.1)** **NHRP: Subblock com sucesso anexado NHRP para os pontos finais de túnel (VPN: 10.1.1.1, NBMA: 172.16.1.1)** NHRP: Nó introduzido do subblock para o esconderijo: Nó introduzido alvo do subblock para o esconderijo: Alvo 10.1.1.1/32nhop 10.1.1.1 NHRP: Entrada de cache dinâmica interna convertida para 10.1.1.1/32 tunnel0s da relação a externo **NHRP: Tu0: Criando o mapeamento de multicast dinâmico NBMA: 172.16.1.1** **NHRP: Mapeamento de multicast dinâmico adicionado para o NBMA: 172.16.1.1** NHRP: Atualizando nosso esconderijo com NBMA: 172.16.10.1, NBMA_ALT: 172.16.10.1 NHRP: Comprimento imperativo novo: 32 NHRP: Tentativa enviar o pacote através de DEST 10.1.1.1 **NHRP: NHRP com sucesso 10.1.1.1 resolved a NBMA 172.16.1.1** **NHRP: Encapsulamento sucedido. ADDR 172.16.1.1**	

	IP do túnel	
Esta é a resposta do registro NHRP enviada pelo hub ao spoke em resposta “à requisição de registro NHRP” recebida mais cedo. Como os outros pacotes de registro, o hub envia múltiplos destes em resposta aos pedidos múltiplos. **src, dst**: Endereços IP de Um ou Mais Servidores Cisco ICM NT do origem de túnel (hub) e do destino (spoke). Estes são a fonte e o destino do pacote GRE enviado pelo roteador **src NBMA**: Endereço NBMA (Internet) do spoke **protocolo do src**: endereço do túnel do spoke que tenta se registrar **protocolo do dst**: endereço do túnel do NHS/hub **cliente NBMA**: Endereço NBMA do NHS/hub **protocolo de cliente**: endereço do túnel do NHS/hub **Extensão da autenticação**, dados: Corda da autenticação de NHRP	**NHRP: Envie a resposta do registro através do vrf 0 do tunnel0, tamanho do pacote: 128** **src: 10.1.1.254, dst: 10.1.1.1** (f) afn: IPv4(1), tipo: IP(800), salto: 255, ver: 1 shtl: 4(NSAP), sstl: 0(NSAP) pktsz: extoff 128: 52 (M) bandeiras: “nat original”, reqid: 65540 **src NBMA: 172.16.1.1** **protocolo do src: 10.1.1.1, protocolo do dst: 10.1.1.254** Código (C-1): nenhum error(0) prefixo: 32, MTU: 17912, hd_time: 7200 addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0 Endereço do que responde Extension(3): (c) código: nenhum error(0) prefixo: 32, MTU: 17912, hd_time: 7200 addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0 **cliente NBMA: 172.16.10.1** **protocolo de cliente: 10.1.1.254** Registro dianteiro de NHS do trânsito Extension(4): Inverta o registro de NHS do trânsito Extension(5): **Autenticação Extension(7):** **type:Cleartext(1), dados: NHRPAUTH** Endereço NAT Extension(9): Código (C-1): nenhum error(0) prefixo: 32, MTU: 17912, hd_time: 0 addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0 **cliente NBMA: 172.16.10.1** **protocolo de cliente: 10.1.1.254**	
	NHRP: Receba a resposta do registro através do vrf 0 do tunnel0, tamanho do pacote: 128 (f) afn: IPv4(1), tipo: IP(800), salto: 255, ver: 1 shtl: 4(NSAP), sstl: 0(NSAP) pktsz: extoff 128: 52 (M) bandeiras: “nat original”, reqid: 65541 **src NBMA: 172.16.1.1** **protocolo do src: 10.1.1.1, protocolo do dst: 10.1.1.254** Código (C-1): nenhum error(0) prefixo: 32, MTU: 17912, hd_time: 7200 addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0 Endereço do que responde Extension(3): (c) código: nenhum error(0) prefixo: 32, MTU: 17912, hd_time: 7200 addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0 **cliente NBMA: 172.16.10.1** **protocolo de cliente: 10.1.1.254**	Esta é a resposta do registro NHRP envia pelo hub ao spoke e resposta “à requisiçã registro NHRP” rece mais cedo. Como os pacotes de registro, envia múltiplos deste resposta aos pedido múltiplos. **src NBMA**: Endereço NBMA (Internet) do s **protocolo do src**: end do túnel do spoke qu tenta se registrar **protocolo do dst**: end do túnel do NHS/hub **cliente NBMA**: Ende NBMA do NHS/hub **protocolo de cliente**:

	Registro dianteiro de NHS do trânsito Extension(4): Inverta o registro de NHS do trânsito Extension(5): **Autenticação Extension(7):** **type:Cleartext(1), dados: NHRPAUTH** Endereço NAT Extension(9): Código (C-1): nenhum error(0) prefixo: 32, MTU: 17912, hd_time: 0 addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0 **cliente NBMA: 172.16.10.1** **protocolo de cliente: 10.1.1.254** NHRP: netid_in = 0, to_us = 1	endereço do túnel do NHS/hub **Extensão da autentic** dados: Corda da autenticação de NHR
Umas mensagens de serviço IPSec mais gerais que digam trabalha corretamente.	IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start já que escuta IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Abrindo um soquete com perfil DMVPN-IPSEC IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): conexão 8C93888 retornado consulta IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): O soquete está já aberto. Ignorância. 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	Os mensagens de se NHRP que dizem NH situado em 10.1.1.25 estão acima.
O mensagem de sistema que indica que a adjacência EIGRP está acima com o vizinho falou em 10.1.1.1.	%DUAL-5-NBRCHANGE: EIGRP-IPv4 1: O vizinho 10.1.1.1 (tunnel0) está acima: adjacência nova	
	%DUAL-5-NBRCHANGE: EIGRP-IPv4 1: O vizinho 10.1.1.254 (tunnel0) está acima: adjacência nova	O mensagem de sist que indica a adjacên EIGRP está acima c hub vizinho em 10.1.
Mensagem de sistema que confirma uma resolução de NHRP bem sucedida.	NHRP: NHRP com sucesso 10.1.1.1 resolved a NBMA 172.16.1.1	

Confirme a funcionalidade e pesquise-a defeitos

Esta seção tem alguns da maioria de comandos de exibição úteis usados para pesquisar defeitos ambos o hub and spoke. A fim permitir mais específico debuga, usam estes debugam conditionals:

- debugar o nbma *NBMA_ADDRESS do* par da condição do dmvpn
- debugar o túnel *TUNNEL_ADDRESS do* par da condição do dmvpn
- IPv4 *NBMA_ADDRESS do* par da condição do debug crypto

mostre os soquetes criptos

```
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"
```

mostre o detalhe da sessão de criptografia

```
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
```

mostre o detalhe cripto 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 encryptionIPv4 Crypto ISAKMP SA
C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap.

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

IPv6 Crypto ISAKMP SA
```

mostre o detalhe cripto IPsec sa

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

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

inbound esp sas:
```

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

inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0xA259D71(170237297)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2, flow_id: SW:2, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4596087/3543)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE
outbound ah sas:
outbound pcp sas: Hub#show crypto ipsec sa detail
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 172.16.10.1

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

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

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

inbound ah sas:
```

```
inbound pcp sas:

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

outbound ah sas:
outbound pcp sas:
```

mostre o nhrp IP

```
Spoke1#show ip nhrp
10.1.1.254/32 via 10.1.1.254
Tunnel0 created 00:00:55, never expire
Type: static, Flags:
NBMA address: 172.16.10.1 Hub#show ip nhrp
10.1.1.1/32 via 10.1.1.1
Tunnel0 created 00:01:26, expire 01:58:33
Type: dynamic, Flags: unique registered
NBMA address: 172.16.1.1
```

mostre nhs IP

```
Spoke1#show ip nhrp nhs
Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel0:
10.1.1.254 RE priority = 0 cluster = 0 Hub#show ip nhrp nhs (As the hub is the only NHS for this
DMVPN cloud,
it does not have any servers configured)
```

mostre o [detail] do dmvpn

```
"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:
```

Informações Relacionadas

- Troubleshooting de IPSec: Compreendendo e usando comandos debug
- Criptografia da próxima geração
- RFC3706: Dead Peer Detection IKE
- RFC3947: IKE NAT Traversal
- Suporte Técnico e Documentação - Cisco Systems