Guia de solução de problemas de depurações da fase 1 do DMVPN

Contents

Introduction

Este documento descreve as mensagens de depuração que você encontraria no hub e spoke de uma implantação da fase 1 da DMVPN (Dynamic Multipoint Virtual Private Network).

Prerequisites

Para os comandos de configuração e depuração neste documento, você precisará de dois roteadores Cisco que executam o Cisco IOS® versão 12.4(9)T ou posterior. Em geral, uma fase 1 de DMVPN básica exige o Cisco IOS versão 12.2(13)T ou posterior ou a versão 12.2(33)XNC para o ASR (Aggregation Services Router), embora os recursos e depurações vistos neste documento talvez não sejam suportados.

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

As informações neste documento são baseadas nos Cisco 2911 Integrated Services Routers (ISRs) que executam o Cisco IOS versão 15.1(4)M4.

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

Melhorias significativas

Essas versões do Cisco IOS introduziram recursos ou correções significativos para a fase 1 do DMVPN:

- Versão 12.2(18)SXF5 - melhor suporte para ISAKMP ao usar a Public Key Infrastructure (PKI)
- Versão 12.2(33)XNE - ASR, Perfis IPSec, Proteção de túnel, Conversão de endereço de rede (NAT - Network Address Translation) IPSec
- Versão 12.3(7)T - suporte interno a roteamento e encaminhamento virtual (iVRF)
- Versão 12.3(11)T - suporte a encaminhamento e roteamento virtual (fVRF) de porta frontal
- Versão 12.4(9)T - suporte para várias depurações e comandos relacionados ao DMVPN
- Versão 12.4(15)T - Proteção de Túnel Compartilhado
- Versão 12.4(20)T - IPv6 sobre DMVPN
- Versão 15.0(1)M - Monitoramento da integridade do túnel NHRP

Conventions

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

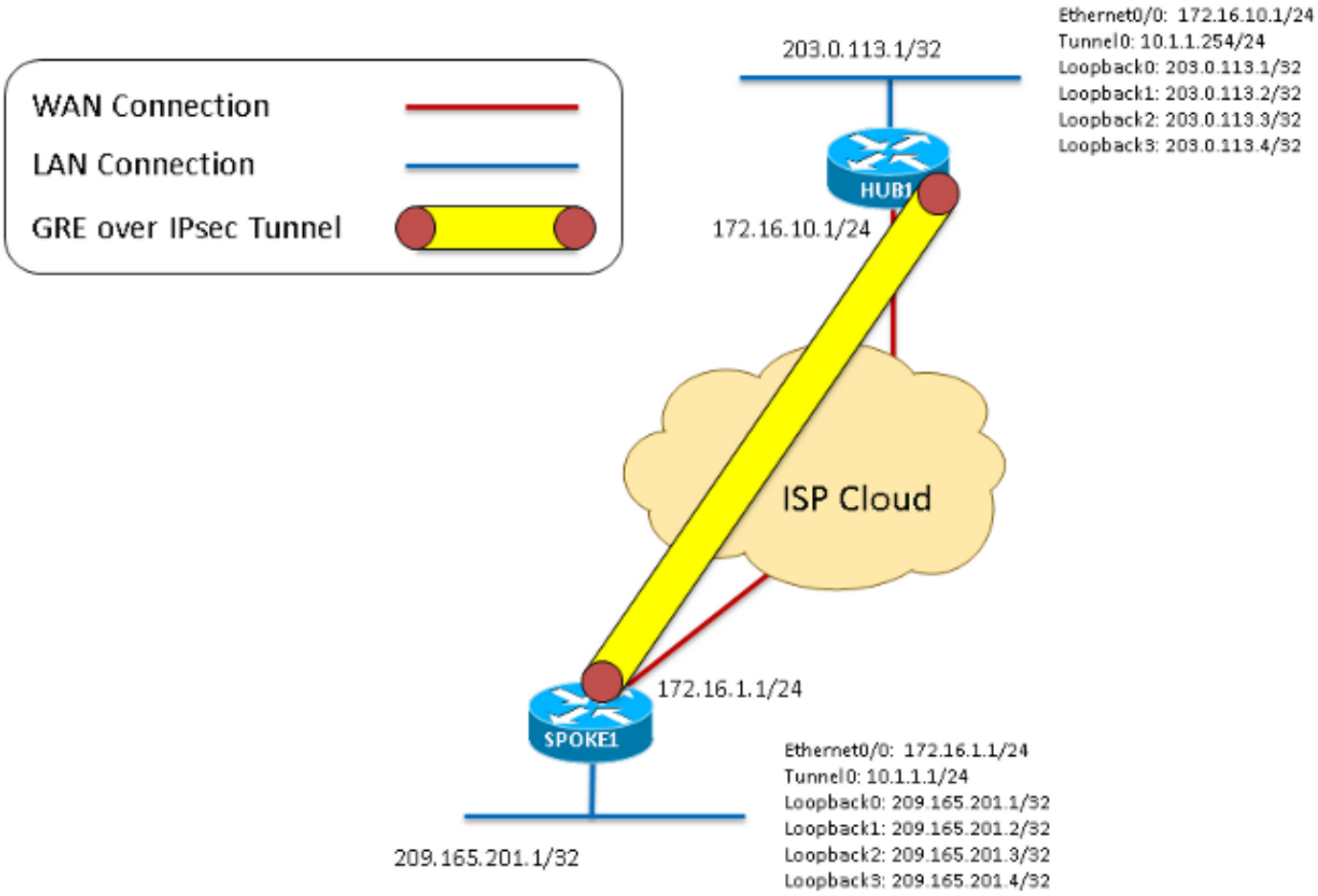
Configuração relevante

Visão geral da topologia

Para essa topologia, dois ISRs 2911 que executam a versão 15.1(4)M4 foram configurados para a fase 1 do DMVPN: um como hub e um como um spoke. A Ethernet0/0 foi usada como a interface "Internet" em cada roteador. As quatro interfaces de loopback são configuradas para

simular redes locais que vivem no hub ou no local de raio. Como esta é uma topologia DMVPN Fase 1 com apenas um spoke, o spoke é configurado com um túnel GRE ponto a ponto em vez de um túnel GRE multiponto. A mesma configuração de criptografia (ISAKMP e IPSec) foi usada em cada roteador para garantir que correspondesse exatamente.

Diagrama 1



Crypto

Isso 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
```

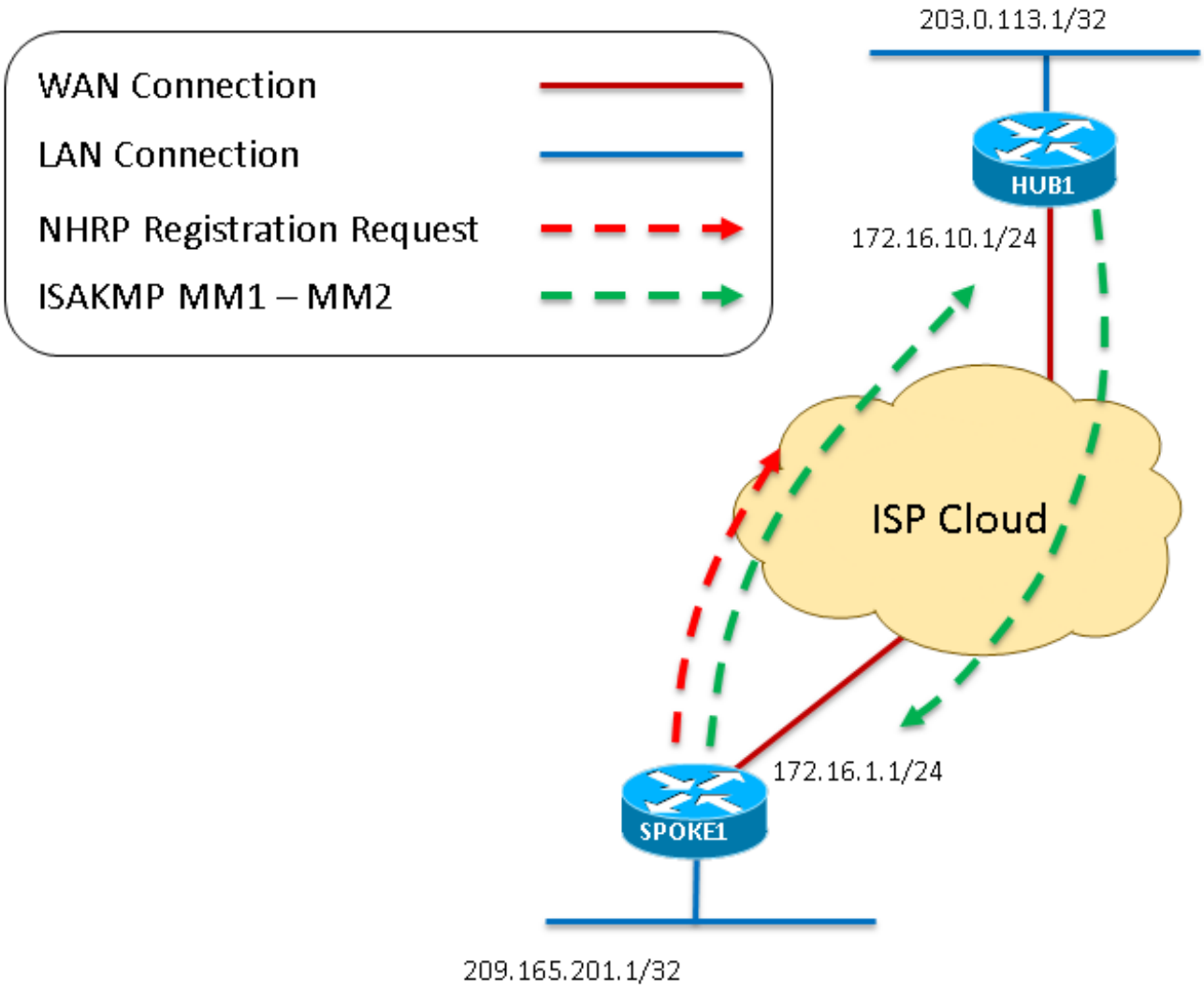
```
network 209.165.201.4 0.0.0.0
network 10.1.1.0 0.0.0.255
```

Debugs

Visualização do fluxo de pacote

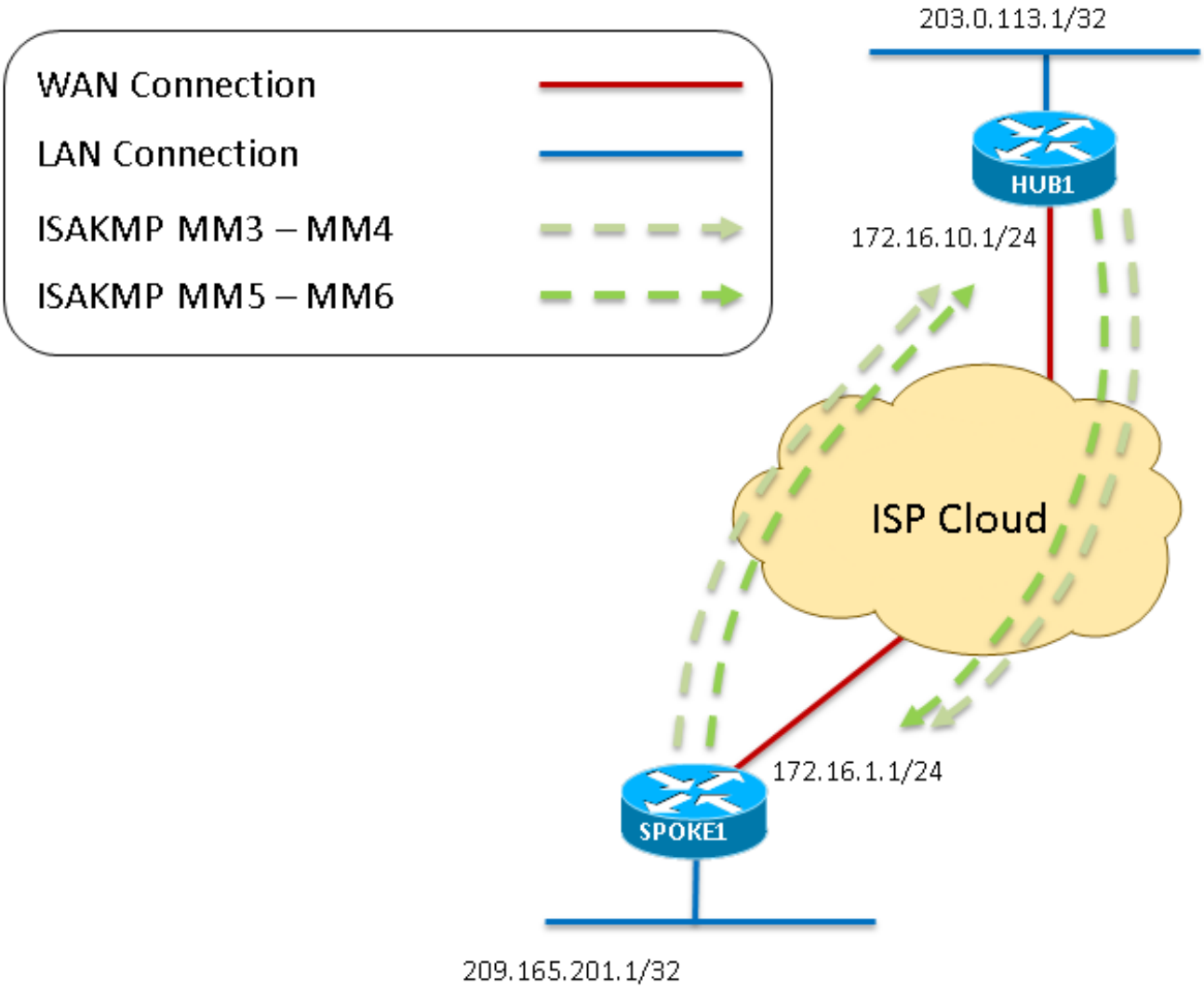
Esta é uma visualização de todo o fluxo do pacote DMVPN conforme visto neste documento. Também estão incluídas depurações mais detalhadas que explicam cada uma das etapas.

1. Quando o túnel no spoke é "no shutdown", ele gera uma solicitação de registro NHRP, que inicia o processo DMVPN. Como a configuração do Hub é completamente dinâmica, o Spoke deve ser o endpoint que inicia a conexão.
2. A solicitação de registro NHRP é encapsulada em GRE, que ativa o processo de criptografia para iniciar.
3. Neste ponto, a primeira mensagem ISAKMP Main Mode - ISAKMP MM1 - é enviada do Spoke para o Hub na porta UDP500.
4. O Hub recebe e processa MM1 e responde com ISAKMP MM2, pois tem uma política ISAKMP correspondente.
   Diagrama 2 - refere-se às etapas 1 a 4

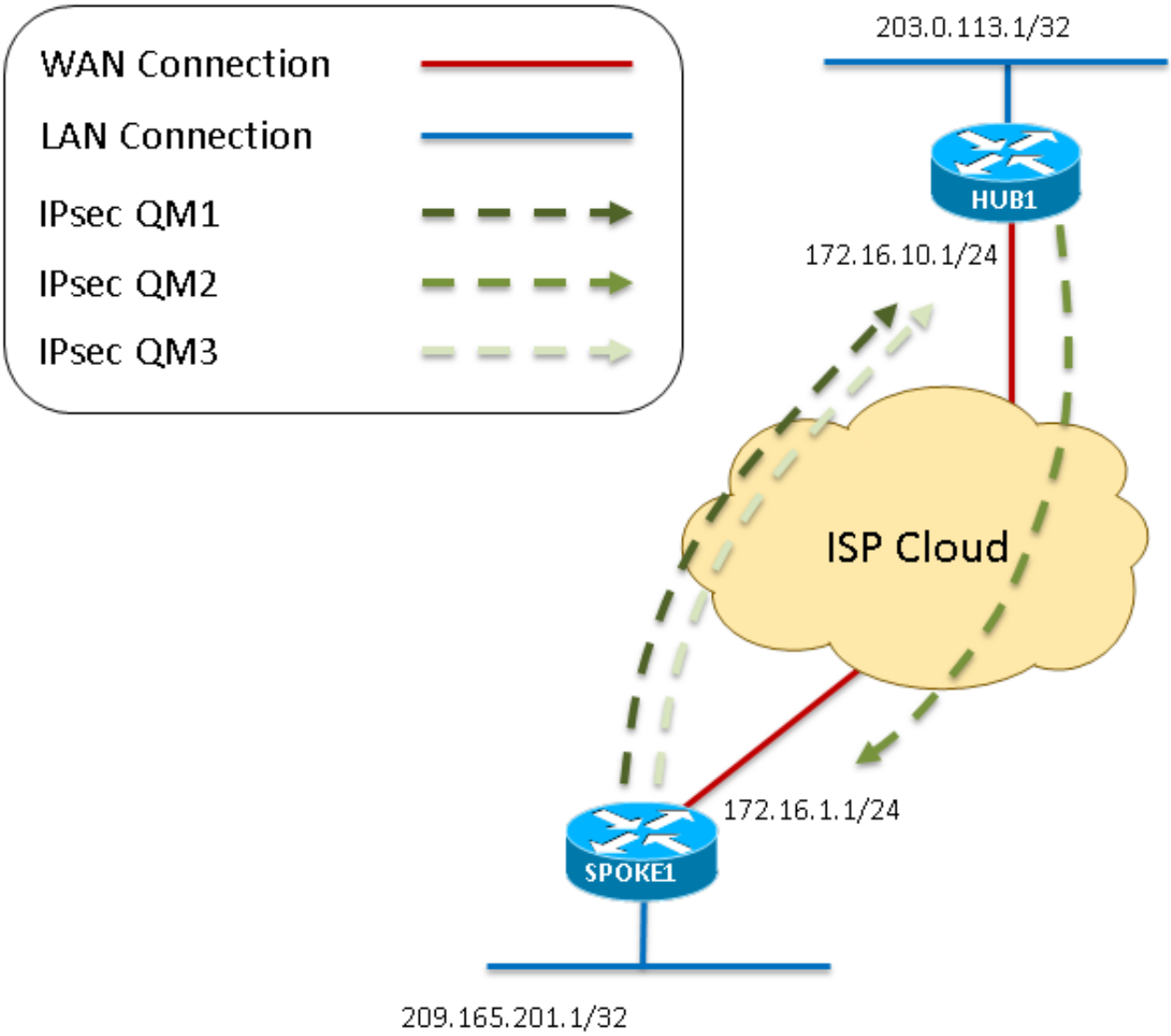


5. Quando o Spoke recebe o MM2, ele responde com MM3. Como com MM1, o Spoke confirma que a política ISAKMP recebida é válida.

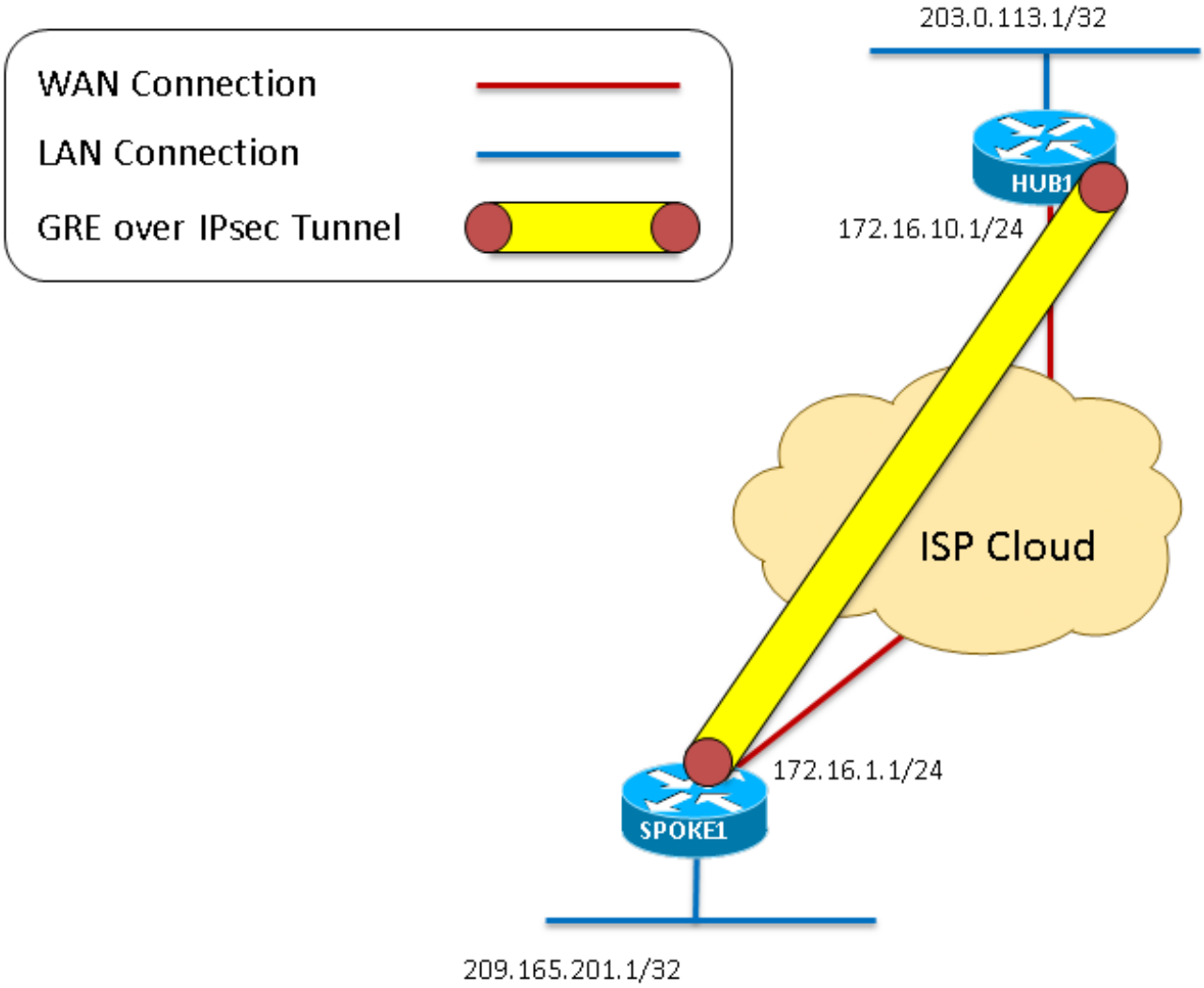
6. O Hub recebe MM3 e responde com MM4.
7. Nesse ponto da negociação ISAKMP, o Spoke pode responder na porta UDP4500 se o NAT for detectado no caminho de trânsito. No entanto, se nenhum NAT for detectado, o Spoke continuará e enviará MM5 em UDP500. Por fim, o hub responde com MM6 para concluir a troca do modo principal.
   Figura 3 - refere-se às etapas 5 a 7



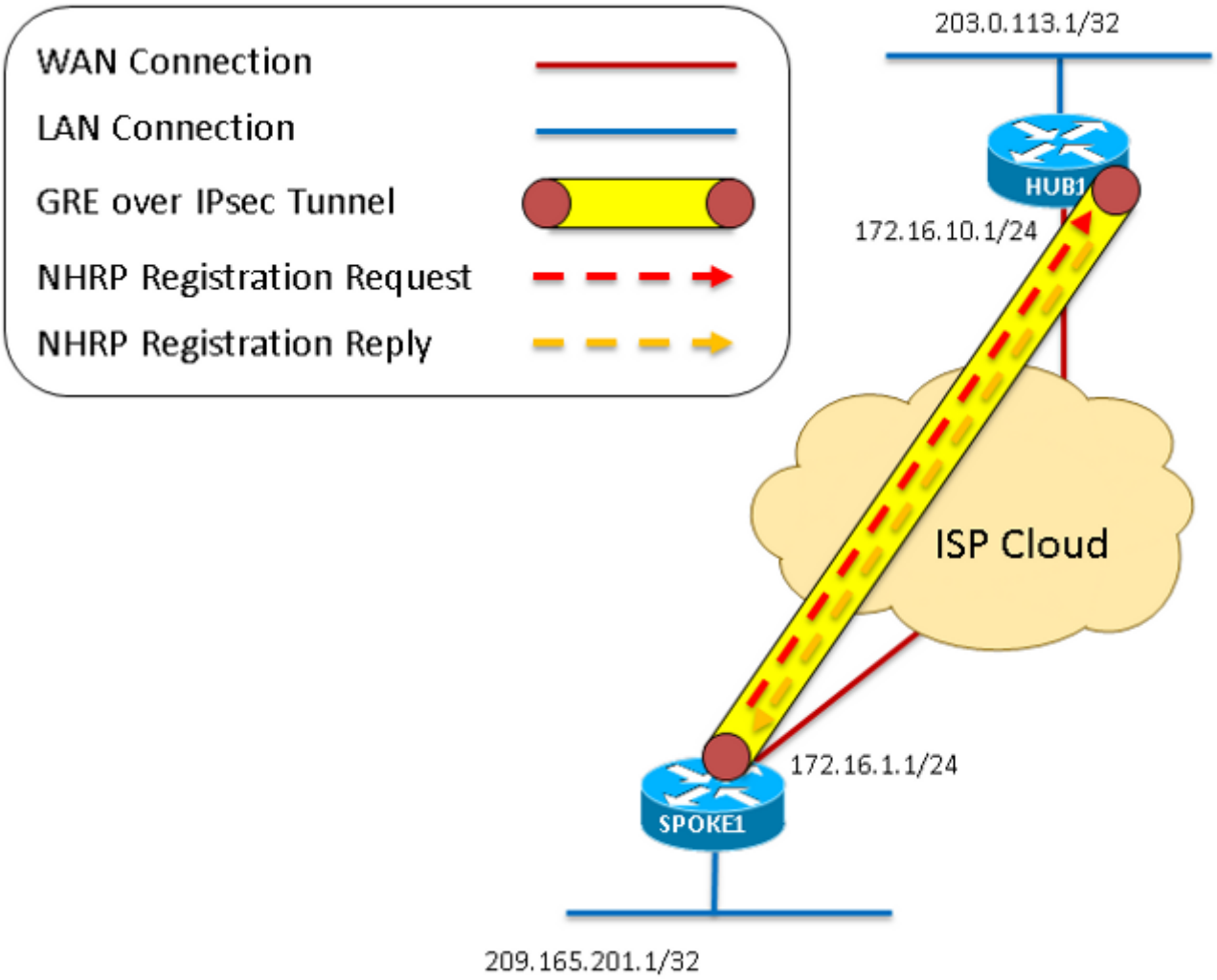
8. Quando o Spoke recebe MM6 do Hub, ele envia QM1 para o Hub no UDP500 para iniciar o Modo rápido.
9. O Hub recebe QM1 e responde com QM2, pois todos os atributos recebidos são aceitos. Neste ponto, o Hub cria as SAs da Fase 2 para esta sessão.
10. Como última etapa da negociação do Modo rápido, o QM2 é recebido pelo Spoke. Em seguida, o Spoke cria seus SAs da Fase 2 e envia o QM3 em resposta. Isso conclui a negociação de ISAKMP e IPSec. Agora há uma sessão IPSec que criptografa o tráfego GRE entre esses dois pares.
    Figura 4 - refere-se às etapas 8 a 10



11. Agora que a sessão de criptografia está ativa e é capaz de transmitir tráfego, esses pacotes são encapsulados dentro do túnel GRE sobre IPSec.
    Figura 5 - refere-se à etapa
    11



12. Como visto nas primeiras etapas, o Spoke gera uma Solicitação de Registro de NHRP que é enviada através do GRE sobre o túnel de IPSec.
13. O Hub recebe as Solicitações de Registro do NHRP e envia uma Resposta de Registro do NHRP depois de confirmar que o Spoke tem um endereço de túnel válido e de multiacesso de não broadcast (NBMA). O Spoke recebe esta Resposta de registro NHRP que conclui o processo de registro.
    Figura 6 - refere-se às etapas 12 a 13



Essas depurações são o resultado quando o **comando debug dmvpn all** é inserido nos roteadores hub e spoke. Este comando específico ativa este conjunto de depurações:

```
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
```

Depurações com explicação

Como essa é uma configuração em que o IPSec é implementado, as depurações mostram todas as depurações de ISAKMP e IPSec. Se nenhuma criptografia estiver configurada, ignore todas as depurações que começam com "IPsec" ou "ISAKMP".

EXPLICAÇÃO DE DEPURAÇÃO DE HUB	DEPURAÇÕES EM SEQUÊNCIA	EXPLICAÇÃO D DEPURAÇÃO DE F
Essas primeiras mensagens de depuração são geradas por um comando **no shutdown** inserido na interface do túnel. As mensagens são geradas por serviços de criptografia, GRE e NHRP sendo iniciados. Um erro de registro de NHRP é visto no hub porque ele não tem um Next Hop Server (NHS) configurado (o hub é o NHS para nossa nuvem DMVPN). Isso é esperado.	IPSEC-IFC MGRE/Tu0: Verificando o status do túnel. **NHRP: if_up: Tunnel0 proto 0** IPSEC-IFC MGRE/Tu0: túnel chegando IPSEC-IFC MGRE/Tu0: crypto_ss_hear_start já está ouvindo **%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP está ATIVADO** **NHRP: Não é possível enviar registro - nenhum NHS configurado** %LINK-3-UPDOWN: Interface Tunnel0, estado alterado para ativado NHRP: if_up: Tunnel0 proto 0 NHRP: Não é possível enviar registro - nenhum NHS configurado IPSEC-IFC MGRE/Tu0: túnel chegando IPSEC-IFC MGRE/Tu0: crypto_ss_hear_start já está ouvindo **%LINEPROTO-5-UPDOWN: Protocolo de linha no túnel de interface0, estado alterado para ativado** IPSEC-IFC GRE/Tu0: Verificando o status do túnel. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): consulta de conexão retornada 0 **IPSEC-IFC GRE/Tu0: crypto_ss_hear_start já está ouvindo** **IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Abrindo um soquete com o perfil DMVPN-IPSEC** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): consulta de conexão retornada 0 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Túnel disparando imediatamente. IPSEC-IFC GRE/Tu0: Adicionando a interface túnel Tunnel0 à lista compartilhada **NHRP: if_up: Tunnel0 proto 0** **NHRP: Túnel0: Adição de cache para o destino 10.1.1.254/32 próximo salto 10.1.1.254** **172.16.10.1**	Essas primeiras mensagens de depur são geradas por um comando **no shutdow** inserido na interface túnel. As mensagens geradas por serviços criptografia, GRE e N iniciados. Além disso, o spoke adiciona uma entrada seu próprio cache NH para seu próprio NBM endereço de túnel.

IPSEC-IFC GRE/Tu0: túnel chegando
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):
consulta de conexão retornada 961D220
IPSEC-IFC GRE/Tu0: crypto_ss_hear_start já está ouvindo
IPSEC-IFC GRE/Tu0: crypto_ss_hear_start já está ouvindo
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):
Abrindo um soquete com o perfil DMVPN-IPSEC
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):
consulta de conexão retornada 961D220
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): O soquete já está sendo aberto. Ignorando.
CRYPTO_SS(TUNNEL SEC): O aplicativo começou a escutar
falha na inserção do mapa no mapdb AVL, o par map + ace já existe no mapdb
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP está ATIVADO
CRYPTO_SS(TUNNEL SEC): Abrir ativo, informações do soquete: local 172.16.1.1
172.16.1.1/255.255.255.255/0, remoto 172.16.10.1
172.16.10.1/255.255.255.255/0, porta 47, ifc Tu0
INÍCIO DA NEGOCIAÇÃO DE ISAKMP (FASE I)
IPSEC(recalcular_mtu): reset sadb_root 94EFDC0 mtu to 1500
IPSEC(sa_request): ,
(chave eng. msg.) Local de saída= 172.16.1.1:500, remoto= 172.16.10.1:500,
local_proxy= 172.16.1.1/255.255.255.255/47/0 (tipo=1),
remote_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac (Transporte),
vida útil= 3600s e 4608000kb,
spi= 0x0(0), conn_id= 0, tamanho da chave= 0, flags= 0x0
ISAKMP:(0): O perfil de solicitação SA é (NULL)
ISAKMP: Criada uma estrutura de peer para 172.16.10.1, porta de peer 500
ISAKMP: Novo peer criado = 0x95F6858 peer_handle = 0x80000004
ISAKMP: Locking peer struct 0x95F6858, recontagem 1 para isakmp_initiator
ISAKMP: porta local 500, porta remota 500
ISAKMP: set new node 0 to QM_IDLE
ISAKMP:(0):insert sa successfully sa = 8A26FB0
ISAKMP:(0):Não é possível iniciar o modo Agressivo, tentando o modo Principal.
ISAKMP:(0):chave pré-compartilhada de peer encontrada correspondente a 172.16.10.1
ISAKMP:(0): ID construída do fornecedor NAT-T-

A primeira etapa qua
túnel estiver "no shut
é iniciar a negociação
criptografia. Aqui o sp
cria uma solicitação S
tenta iniciar o Modo
agressivo e falha de
ao Modo principal. Co
Modo agressivo não
configurado em nenh
dos roteadores, isso
esperado.
O spoke inicia o mod
principal e envia a pri
mensagem ISAKMP,
MM_NO_STATE. O e
ISAKMP muda de
IKE_READY para
IKE_I_MM1.
As mensagens de ID
fornecedor NAT-T sã
usadas na detecção
passagem do NAT. E
mensagens são espe
durante a negociação
ISAKMP
independentemente
NAT ser ou não
implementado. Como

	rfc3947 ISAKMP:(0): ID construída do fornecedor-07 NAT-T ISAKMP:(0): ID construída do fornecedor-03 NAT-T ISAKMP:(0): ID de fornecedor-02 NAT-T construída **ISAKMP:(0):Entrada = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM** **ISAKMP:(0):Estado Antigo = Estado Novo IKE_READY = IKE_I_MM1** **ISAKMP:(0): início de troca do Modo Principal** **ISAKMP:(0): enviando pacote para 172.16.10.1 my_port 500 peer_port 500 (I) MM_NO_STATE** ISAKMP:(0):Envio de um pacote IPv4 IKE. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): consulta de conexão retornada 961D220 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): mensagem de bom soquete pronto	mensagens do modo agressivo, elas são esperadas.
Depois que o túnel do spoke estiver "no shutdown", o hub receberá a mensagem IKE NEW SA (Main Mode 1) na porta 500. Como respondedor, o hub cria uma ISAKMP Security Association (SA). O estado ISAKMP muda de IKE_READY para IKE_R_MM1.	**ISAKMP (0): pacote recebido de 172.16.1.1 dport 500 sport 500 Global (N) NEW SA** **ISAKMP: Criada uma estrutura de peer para 172.16.1.1, porta de peer 500** ISAKMP: Novo peer criado = 0x8CACD00 peer_handle = 0x80000003 ISAKMP: Travando peer struct 0x8CACD00, recontagem 1 para crypto_isakmp_process_block ISAKMP: porta local 500, porta remota 500 **ISAKMP:(0):insert sa successfully sa = 6A5BDE8** ISAKMP:(0):Entrada = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(0):Estado Antigo = Estado Novo IKE_READY = IKE_R_MM1**	
A mensagem IKE Main Mode 1 recebida é processada. O hub determina que o peer tem atributos ISAKMP correspondentes e eles são preenchidos no SA ISAKMP que acabou de ser criado. As mensagens mostram que o peer usa 3DES-CBC para criptografia, hashing de SHA, Diffie Hellman (DH) group 1, chave pré-compartilhada para autenticação e o tempo de vida de SA padrão de 86400 segundos (0x0 0x1 0x51 0x80 = 0x15180 = 8640 segundos) . O estado ISAKMP ainda é IKE_R_MM1, pois uma	ISAKMP:(0): processando o payload SA. ID da mensagem = 0 ISAKMP:(0): payload de ID do fornecedor de processamento **ISAKMP:(0): ID do fornecedor parece Unity/DPD, mas há uma diferença de 69** **ISAKMP (0): ID do fornecedor é NAT-T RFC 3947** ISAKMP:(0): payload de ID do fornecedor de processamento ISAKMP:(0): ID do fornecedor parece Unity/DPD, mas há uma incompatibilidade de 245 principais ISAKMP (0): ID do fornecedor é NAT-T v7 ISAKMP:(0): payload de ID do fornecedor de processamento ISAKMP:(0): ID do fornecedor parece Unity/DPD, mas a diferença principal é de 157 ISAKMP:(0): ID do fornecedor é NAT-T v3 ISAKMP:(0): payload de ID do fornecedor de processamento ISAKMP:(0): ID do fornecedor parece Unity/DPD, mas a diferença principal é 123 ISAKMP:(0): ID do fornecedor é NAT-T v2	

resposta não foi enviada ao spoke. As mensagens de ID do fornecedor NAT-T são usadas na detecção e passagem do NAT. Essas mensagens são esperadas durante a negociação de ISAKMP independentemente de o NAT ser ou não implementado. Mensagens semelhantes são vistas para Dead Peer Detection (DPD).	**ISAKMP:(0):chave pré-compartilhada de peer encontrada correspondente a 172.16.1.1** **ISAKMP:(0): chave pré-compartilhada local encontrada** ISAKMP: A analisar perfis para xauth... **ISAKMP:(0):Verificando a transformação de ISAKMP 1 em relação à política de prioridade 1** **ISAKMP: criptografia 3DES-CBC** **ISAKMP: hash SHA** **ISAKMP: grupo padrão 1** **ISAKMP: auth pre-share** **ISAKMP: tipo de vida em segundos** **ISAKMP: duração da vida útil (VPI) de 0x0 0x1 0x51 0x80** **ISAKMP:(0):as atts são aceitáveis. O próximo payload é 0** **ISAKMP:(0):Atos aceitáveis:vida real: 0** **ISAKMP:(0):Atos aceitáveis:vida: 0** **ISAKMP:(0):Preencha os atts em sa vpi_length:4** **ISAKMP:(0):Preencher atts em sa life_in_seconds:86400** **ISAKMP:(0):Retornando o tempo de vida real: 86400** **ISAKMP:(0)::Temporizador de vida iniciado: 86400.** ISAKMP:(0): payload de ID do fornecedor de processamento ISAKMP:(0): ID do fornecedor parece Unity/DPD, mas há uma diferença de 69 ISAKMP (0): ID do fornecedor é NAT-T RFC 3947 ISAKMP:(0): payload de ID do fornecedor de processamento ISAKMP:(0): ID do fornecedor parece Unity/DPD, mas há uma incompatibilidade de 245 principais ISAKMP (0): ID do fornecedor é NAT-T v7 ISAKMP:(0): payload de ID do fornecedor de processamento ISAKMP:(0): ID do fornecedor parece Unity/DPD, mas a diferença principal é de 157 ISAKMP:(0): ID do fornecedor é NAT-T v3 ISAKMP:(0): payload de ID do fornecedor de processamento ISAKMP:(0): ID do fornecedor parece Unity/DPD, mas a diferença principal é 123 ISAKMP:(0): ID do fornecedor é NAT-T v2 ISAKMP:(0):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(0):Estado Antigo = IKE_R_MM1 Novo Estado = IKE_R_MM1
MM_SA_SETUP (Main Mode 2) é enviado ao spoke, o que confirma que MM1 foi recebido e aceito como um pacote ISAKMP	ISAKMP:(0): ID construída do fornecedor NAT-T-rfc3947 **ISAKMP:(0): enviando pacote para 172.16.1.1 my_port 500 peer_port 500 (R) MM_SA_SETUP** ISAKMP:(0):Envio de um pacote IPv4 IKE.

válido. O estado ISAKMP muda de IKE_R_MM1 para IKE_R_MM2.	ISAKMP:(0):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(0):Estado Antigo = IKE_R_MM1 Novo Estado = IKE_R_MM2**	
	ISAKMP (0): pacote recebido de 172.16.10.1 dport 500 sport 500 Global (I) MM_NO_STATE **ISAKMP:(0):Entrada = IKE_MESG_FROM_PEER, IKE_MM_EXCH** **ISAKMP:(0):Estado Antigo = IKE_I_MM1 Novo Estado = IKE_I_MM2** ISAKMP:(0): processando o payload SA. ID da mensagem = 0 ISAKMP:(0): payload de ID do fornecedor de processamento **ISAKMP:(0): ID do fornecedor parece Unity/DPD, mas há uma diferença de 69** ISAKMP (0): ID do fornecedor é NAT-T RFC 3947 ISAKMP:(0):chave pré-compartilhada de peer encontrada correspondente a 172.16.10.1 ISAKMP:(0): chave pré-compartilhada local encontrada ISAKMP: A analisar perfis para xauth... **ISAKMP:(0):Verificando a transformação de ISAKMP 1 em relação à política de prioridade 1** **ISAKMP: criptografia 3DES-CBC** **ISAKMP: hash SHA** **ISAKMP: grupo padrão 1** **ISAKMP: auth pre-share** **ISAKMP: tipo de vida em segundos** **ISAKMP: duração da vida útil (VPI) de 0x0 0x1 0x51 0x80** **ISAKMP:(0):as atts são aceitáveis. O próximo payload é 0** **ISAKMP:(0):Atos aceitáveis:vida real: 0** **ISAKMP:(0):Atos aceitáveis:vida: 0** **ISAKMP:(0):Preencha os atts em sa vpi_length:4** **ISAKMP:(0):Preencher atts em sa life_in_seconds:86400** **ISAKMP:(0):Retornando o tempo de vida real: 86400** **ISAKMP:(0)::Temporizador de vida iniciado: 86400.**	Em resposta à mens MM1 enviada ao hub MM2 chega confirma que o MM1 foi recebi mensagem IKE Main 2 recebida é process spoke percebe que o peer tem atributos IS correspondentes e e atributos são preench no SA ISAKMP que f criado. Este pacote n que o peer usa 3DES para criptografia, has de SHA, Diffie Hellm (DH) group 1, chave compartilhada para autenticação e o tem vida de SA padrão de 86400 segundos (0x 0x51 0x80 = 0x1518 8640 segundos) . Além das mensagen T, há uma troca para determinar se a sess usará DPD. O estado ISAKMP m IKE_I_MM1 para IKE_I_MM2.
	ISAKMP:(0): payload de ID do fornecedor de processamento ISAKMP:(0): ID do fornecedor parece Unity/DPD, mas há uma diferença de 69 ISAKMP (0): ID do fornecedor é NAT-T RFC 3947 ISAKMP:(0):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(0):Estado Antigo = IKE_I_MM2 Novo Estado = IKE_I_MM2	
	ISAKMP:(0): enviando pacote para 172.16.10.1 my_port 500 peer_port 500 (I) MM_SA_SETUP	MM_SA_SETUP (Ma Mode 3) é enviado a

	ISAKMP:(0):Envio de um pacote IPv4 IKE. ISAKMP:(0):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(0):Estado Antigo = IKE_I_MM2 Novo Estado = IKE_I_MM3**	o que confirma que o spoke recebeu MM2 deseja continuar. O estado ISAKMP m IKE_I_MM2 para IKE_I_MM3.
MM_SA_SETUP (Main Mode 3) é recebido pelo hub. O hub conclui que o peer é outro dispositivo Cisco IOS e nenhum NAT é detectado para nós ou para nosso peer. O estado ISAKMP muda de IKE_R_MM2 para IKE_R_MM3.	**ISAKMP (0): pacote recebido de 172.16.1.1 dport 500 sport 500 Global (R) MM_SA_SETUP** ISAKMP:(0):Entrada = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(0):Estado Antigo = IKE_R_MM2 Novo Estado = IKE_R_MM3**	
	ISAKMP:(0): processando payload KE. ID da mensagem = 0 ISAKMP:(0): processando payload NONCE. ID da mensagem = 0 **ISAKMP:(0):chave pré-compartilhada de peer encontrada correspondente a 172.16.1.1** ISAKMP (1002): payload de ID do fornecedor de processamento ISAKMP (1002): ID do fornecedor é DPD ISAKMP (1002): payload de ID do fornecedor de processamento **ISAKMP (1002): falando com outra caixa do IOS!** ISAKMP (1002): payload de ID do fornecedor de processamento ISAKMP (1002): ID do fornecedor parece Unity/DPD, mas há uma incompatibilidade de 225 principais ISAKMP (1002): ID do fornecedor é XAUTH ISAKMP:tipo de payload recebido 20 **ISAKMP (1002): Seu hash no match - esse nó fora do NAT** ISAKMP:tipo de payload recebido 20 **ISAKMP (1002): Nenhum NAT encontrado para si mesmo ou par** ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(1002):Estado Antigo = IKE_R_MM3 Novo Estado = IKE_R_MM3	
MM_KEY_EXCH (Modo principal 4) é enviado pelo hub. O estado ISAKMP muda de IKE_R_MM3 para IKE_R_MM4.	**ISAKMP (1002): enviando pacote para 172.16.1.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH** ISAKMP:(1002):Envio de um pacote IPv4 IKE. ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(1002):Estado Antigo = IKE_R_MM3 Novo Estado = IKE_R_MM4**	
	ISAKMP (0): pacote recebido de 172.16.10.1 porta 500 esportivo 500 Global (I) MM_SA_SETUP ISAKMP:(0):Entrada = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(0):Estado Antigo = IKE_I_MM3 Novo Estado = IKE_I_MM4**	MM_SA_SETUP (Mo principal 4) é recebid spoke. O spoke conc o peer é outro dispos Cisco IOS e nenhum é detectado para nós

		nosso peer.
	ISAKMP:(0): processando payload KE. ID da mensagem = 0	O estado ISAKMP mu
	ISAKMP:(0): processando payload NONCE. ID da mensagem = 0	IKE_I_MM3 para IKE_I_MM4.
	ISAKMP:(0):chave pré-compartilhada de peer encontrada correspondente a 172.16.10.1	
	ISAKMP (1002): payload de ID do fornecedor de processamento	
	ISAKMP (1002): ID do fornecedor é Unity	
	ISAKMP (1002): payload de ID do fornecedor de processamento	
	ISAKMP (1002): ID do fornecedor é DPD	
	ISAKMP (1002): payload de ID do fornecedor de processamento	
	ISAKMP (1002): falando com outra caixa do IOS!	
	ISAKMP:tipo de payload recebido 20	
	ISAKMP (1002): Seu hash no match - esse nó fora do NAT	
	ISAKMP:tipo de payload recebido 20	
	ISAKMP (1002): Nenhum NAT encontrado para si mesmo ou par	
	ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE	
	ISAKMP:(1002):Estado Antigo = IKE_I_MM4 Novo Estado = IKE_I_MM4	
	ISAKMP:(1002):Enviar contato inicial	MM_KEY_EXCH (Mo principal 5) é enviado spoke.
	ISAKMP:(1002):SA está fazendo autenticação de chave pré-compartilhada usando o tipo de ID ID_IPV4_ADDR.	O estado ISAKMP mu IKE_I_MM4 para IKE_I_MM5.
	ISAKMP (1002): payload de ID próximo payload: 8 digite: 1 endereço: 172.16.1.1 protocolo: 17 porta: 500 comprimento: 12	
	ISAKMP:(1002):Comprimento total do payload: 12	
	ISAKMP (1002): enviando pacote para 172.16.10.1 my_port 500 peer_port 500 (I) MM_KEY_EXCH	
	ISAKMP:(1002):Envio de um pacote IPv4 IKE.	
	ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE	
	ISAKMP:(1002):Estado Antigo = IKE_I_MM4 Novo Estado = IKE_I_MM5	
MM_KEY_EXCH (Modo principal 5) é recebido pelo hub. O estado ISAKMP muda de IKE_R_MM4 para IKE_R_MM5. Além disso, a "correspondência de peer	**ISAKMP (1002): pacote recebido de 172.16.1.1 dport 500 sport 500 Global (R) MM_KEY_EXCH**	
	ISAKMP:(1002):Entrada = IKE_MESG_FROM_PEER, IKE_MM_EXCH	
	ISAKMP:(1002):Estado Antigo = IKE_R_MM4 Novo Estado = IKE_R_MM5	
	ISAKMP (1002): payload de ID de processamento. ID	

nenhum dos perfis" é vista devido à falta de um perfil ISAKMP. Como esse é o caso, ISAKMP não usa um perfil.	da mensagem = 0 ISAKMP (1002): payload de ID próximo payload: 8 digite: 1 endereço: 172.16.1.1 protocolo: 17 porta: 500 comprimento: 12 **ISAKMP:(0): correspondências de peer *none* dos perfis** ISAKMP (1002): processando carga útil HASH. ID da mensagem = 0 ISAKMP (1002): processando o NOTIFY INITIAL_CONTACT protocol 1 spi 0, ID da mensagem = 0, sa = 0x6A5BDE8 ISAKMP:(1002):Status da autenticação SA: autenticado ISAKMP:(1002):SA foi autenticado com 172.16.1.1 ISAKMP:(1002):Status da autenticação SA: autenticado ISAKMP (1002): Processar contato inicial, desativar SAs de fase 1 e 2 atuais com porta remota 172.16.10.1 remota 172.16.1.1 500 local **ISAKMP: Tentando inserir um peer 172.16.10.1/172.16.1.1/500/, e inserir com êxito 8CACD00.** ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(1002):Estado Antigo = IKE_R_MM5 Estado Novo = IKE_R_MM5 IPSEC(key_engine): recebeu um evento de fila com 1 mensagem KMI ISAKMP:(1002):SA está fazendo autenticação de chave pré-compartilhada usando o tipo de ID ID_IPV4_ADDR. ISAKMP (1002): payload de ID próximo payload: 8 digite: 1 endereço: 172.16.10.1 protocolo: 17 porta: 500 comprimento: 12 ISAKMP:(1002):Comprimento total do payload: 12
O pacote MM_KEY_EXCH final (Main Mode 6) é enviado pelo hub. Isso conclui a negociação da Fase 1, o que significa que esse dispositivo está pronto para a Fase 2 (Modo Rápido IPSec).	**ISAKMP (1002): enviando pacote para 172.16.1.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH** ISAKMP:(1002):Envio de um pacote IPv4 IKE. ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(1002):Estado Antigo = IKE_R_MM5 Novo Estado = IKE_P1_COMPLETE**
O estado ISAKMP muda de	ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL,

IKE_R_MM5 para IKE_P1_COMPLETE.	IKE_PHASE1_COMPLETE ISAKMP:(1002):Estado Antigo = IKE_P1_COMPLETE Novo Estado = IKE_P1_COMPLETE	
	ISAKMP (1002): pacote recebido de 172.16.10.1 porta 500 esportivo 500 Global (I) MM_KEY_EXCH	O pacote MM_KEY_E final (modo principal recebido pelo spoke. conclui a negociação Fase 1, o que signific esse dispositivo está pronto para a Fase 2 (Modo Rápido IPSec) O estado ISAKMP mu IKE_I_MM5 para IKE_I_MM6 e imediatamente para IKE_P1_COMPLETE Além disso, a "correspondência de *nenhum* dos perfis" vista devido à falta de perfil ISAKMP. Como é o caso, ISAKMP nã um perfil.
	ISAKMP (1002): payload de ID de processamento. ID da mensagem = 0 ISAKMP (1002): payload de ID próximo payload: 8 digite: 1 endereço: 172.16.10.1 protocolo: 17 porta: 500 comprimento: 12	
	ISAKMP:(0): correspondências de peer *none* dos perfis	
	ISAKMP (1002): processando carga útil HASH. ID da mensagem = 0 ISAKMP:(1002):Status da autenticação SA: autenticado ISAKMP:(1002):SA foi autenticado com 172.16.10.1	
	ISAKMP: Tentando inserir um peer 172.16.1.1/172.16.10.1/500/, e inserir com êxito 95F6858.	
	ISAKMP:(1002):Entrada = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(1002):Estado Antigo = IKE_I_MM5 Novo Estado = IKE_I_MM6**	
	ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(1002):Estado Antigo = IKE_I_MM6 Novo Estado = IKE_I_MM6	
	ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(1002):Estado Antigo = IKE_I_MM6 Novo Estado = IKE_P1_COMPLETE**	
FIM DA NEGOTAÇÃO ISAKMP (FASE I), INÍCIO DA NEGOTAÇÃO IPSEC (FASE II)		
	ISAKMP:(1002):início da troca do modo rápido, M-ID de 3464373979	A troca do modo rápi (Fase II, IPSec) é inic o spoke envia a prim mensagem de QM ac
	ISAKMP:(1002):O iniciador QM obtém spi **ISAKMP (1002): enviando pacote para 172.16.10.1 my_port 500 peer_port 500 (I) QM_IDLE** ISAKMP:(1002):Envio de um pacote IPv4 IKE. ISAKMP:(1002):Nó 3464373979, Entrada = IKE_MESG_INTERNAL, IKE_INIT_QM **ISAKMP:(1002):Estado Antigo = IKE_QM_READY Novo Estado = IKE_QM_I_QM1** ISAKMP:(1002):Entrada = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE ISAKMP:(1002):Estado Antigo = IKE_P1_COMPLETE Novo Estado = IKE_P1_COMPLETE	

O hub recebe o primeiro pacote de Modo rápido (QM) que tem a proposta de IPSec. Os atributos recebidos especificam que: encaps flag definido como 2 (modo de transporte, flag de 1 seria modo de túnel), tempo de vida padrão de SA de 3600 segundos e 4608000 kilobytes (0x465000 em hex), HMAC-SHA para autenticação e 3DES para criptografia. Como esses são os mesmos atributos definidos na configuração local, a proposta é aceita e o shell de um SA IPSec é criado. Como nenhum valor de Índice de Parâmetro de Segurança (SPI) está associado a esses valores ainda, esse é apenas um shell de um SA que ainda não pode ser usado para transmitir tráfego.	**ISAKMP (1002): pacote recebido de 172.16.1.1 porta 500 esportivo 500 Global (R) QM_IDLE** **ISAKMP: set new node -830593317 to QM_IDLE** ISAKMP (1002): processando carga útil HASH. ID da mensagem = 3464373979 ISAKMP (1002): processando o payload SA. ID da mensagem = 3464373979 **ISAKMP:(1002):Verificando a proposta de IPSec 1** **ISAKMP: transformação 1, ESP_3DES** **ISAKMP: atributos em transformação:** **ISAKMP: encaps is 2 (Transporte)** **ISAKMP: Tipo de vida SA em segundos** **ISAKMP: duração da SA (básica) de 3600** **ISAKMP: Tipo de vida SA em kilobytes** **ISAKMP: duração da vida útil SA (VPI) de 0x0 0x46 0x50 0x0** **ISAKMP: o autenticador é HMAC-SHA** **ISAKMP:(1002):as atts são aceitáveis.** IPSEC(validation_Proposal_request): parte da proposta nº 1 IPSEC(validation_Proposal_request): parte da proposta nº 1, **(chave eng. msg.) INBOUND local= 172.16.10.1:0, remoto= 172.16.1.1:0,** **local_proxy= 172.16.10.1/255.255.255.255/47/0 (tipo=1),** **remote_proxy= 172.16.1.1/255.255.255.255/47/0 (type=1),** **protocol= ESP, transform= NONE (Transport),** **Liedur= 0s e 0kb,** **spi= 0x0(0), conn_id= 0, tamanho da chave= 128, flags= 0x0**
São apenas mensagens gerais de serviço IPSec que dizem que funciona corretamente.	IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): consulta de conexão retornada 0 IPSEC-IFC MGRE/Tu0: crypto_ss_hear_start já está ouvindo **IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Abrindo um soquete com o perfil DMVPN-IPSEC** IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): consulta de conexão retornada 0 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Túnel disparando imediatamente. IPSEC-IFC MGRE/Tu0: Adicionando a interface túnel 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): Boa solicitação de escuta
A entrada do mapa de pseudo-criptografia é criada para o protocolo IP 47 (GRE) de 172.16.10.1 (endereço público do hub)	falha na inserção do mapa no mapdb AVL, o par map + ace já existe no mapdb CRYPTO_SS(TUNNEL SEC): Informações passivas e abertas do soquete: local 172.16.10.1 172.16.10.1/255.255.255.255/0, remoto 172.16.1.1

para 172.16.1.1 (endereço público do spoke). Um SA/SPI de IPSec é criado para o tráfego de entrada e saída com valores da proposta aceita.	172.16.1.1/255.255.255.255/0, porta 47, ifc Tu0 Mapdb de criptografia: proxy_match **endereço src: 172.16.10.1** **dst addr : 172.16.1.1** **protocolo: 47** porta src: 0 porta dst: 0 ISAKMP (1002): processando payload NONCE. ID da mensagem = 3464373979 ISAKMP (1002): payload de ID de processamento. ID da mensagem = 3464373979 ISAKMP (1002): payload de ID de processamento. ID da mensagem = 3464373979 ISAKMP:(1002):O respondedor QM recebe spi ISAKMP:(1002):Nó 3464373979, Entrada = IKE_MESG_FROM_PEER, IKE_QM_EXCH **ISAKMP:(1002):Estado Antigo = IKE_QM_READY Novo Estado = IKE_QM_SPI_STARVE** **ISAKMP (1002): Criando SAs 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 spi 0xDD2AC2B3 e conn_id 0** **duração de 3600 segundos** **duração de 4608000 kilobytes** **SA de saída 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 spi 0x82C3E0C4 e conn_id 0** **duração de 3600 segundos** **duração de 4608000 kilobytes**
A segunda mensagem do QM enviada pelo hub. Mensagem gerada pelo serviço IPSec que confirma que a proteção do túnel está ativa no Tunnel0. Outra mensagem de criação de SA é vista, que tem IPs de destino, SPIs, atributos de conjunto de transformação e duração em kilobytes e segundos restantes.	**ISAKMP (1002): enviando pacote para 172.16.1.1 my_port 500 peer_port 500 (R) QM_IDLE** ISAKMP:(1002):Envio de um pacote IPv4 IKE. ISAKMP:(1002):Nó 3464373979, Entrada = IKE_MESG_INTERNAL, IKE_GOT_SPI **ISAKMP:(1002):Estado Antigo = IKE_QM_SPI_STARVE Novo Estado = IKE_QM_R_QM2** CRYPTO_SS(TUNNEL SEC): Enlace concluído do aplicativo ao soquete IPSEC(key_engine): recebeu um evento de fila com 1 mensagem KMI Mapdb de criptografia: proxy_match endereço src: 172.16.10.1 dst addr : 172.16.1.1 protocolo: 47 porta src: 0 porta dst: 0 IPSEC(crypto_ipsec_sa_find_ident_head): reconexão com os mesmos proxies 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 criado,
(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/seg)= (4536779/3600)
IPSEC(create_sa): sa criado,
(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/seg)= (4536779/3600)
IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce): atualizando o túnel0 ident 8B6A0E8 com tun_decap_oce 6A648F0
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): consulta de conexão retornada 8C93888
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): mensagem de bom soquete pronto
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): consulta de conexão retornada 8C93888
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): tunnel_protection_socket_up
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Sinalização de NHRP
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Mensagem MTU mtu 1458
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): consulta de conexão retornada 8C93888
ISAKMP (1002): pacote recebido de 172.16.10.1 porta 500 esportivo 500 Global (I) QM_IDLE
ISAKMP (1002): processando carga útil HASH. ID da mensagem = 3464373979
ISAKMP (1002): processando o payload SA. ID da mensagem = 3464373979
ISAKMP:(1002):Verificando a proposta de IPSec 1
ISAKMP: transformação 1, ESP_3DES
ISAKMP: atributos em transformação:
ISAKMP: encaps is 2 (Transporte)
ISAKMP: Tipo de vida SA em segundos
ISAKMP: duração da SA (básica) de 3600
ISAKMP: Tipo de vida SA em kilobytes
ISAKMP: duração da vida útil SA (VPI) de 0x0 0x46 0x50 0x0
ISAKMP: o autenticador é HMAC-SHA
ISAKMP:(1002):as atts são aceitáveis.
IPSEC(validation_Proposal_request): parte da proposta nº 1
IPSEC(validation_Proposal_request): parte da proposta nº 1,
(chave eng. msg.) INBOUND local= 172.16.1.1:0, remoto= 172.16.10.1:0,
local_proxy= 172.16.1.1/255.255.255.255/47/0 (tipo=1),
remote_proxy= 172.16.10.1/255.255.255.255/47/0

O spoke recebe o se
pacote de QM que te
proposta de IPSec. Is
confirma que o QM1
recebido pelo hub. O
atributos recebidos
especificam que: enc
flag definido como 2
de transporte, flag de
seria modo de túnel),
tempo de vida padrã
SA de 3600 segundo
4608000 kilobytes
(0x465000 em hex),
HMAC-SHA para
autenticação e DES p
criptografia. Como es
são os mesmos atrib
definidos na configur
local, a proposta é ac
o shell de um SA IPS
criado. Como nenhur
de Índice de Parâmet
Segurança (SPI) está
associado a esses va
ainda, esse é apenas

(type=1),
protocol= ESP, transform= NONE (Transport),
Liedur= 0s e 0kb,
spi= 0x0(0), conn_id= 0, tamanho da chave= 128, flags= 0x0
Mapdb de criptografia: proxy_match
endereço src: 172.16.1.1
dst addr : 172.16.10.1
protocolo: 47
porta src: 0
porta dst: 0
ISAKMP (1002): processando payload NONCE. ID da mensagem = 3464373979
ISAKMP (1002): payload de ID de processamento. ID da mensagem = 3464373979
ISAKMP (1002): payload de ID de processamento. ID da mensagem = 3464373979
ISAKMP (1002): Criando SAs 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)
tem spi 0x82C3E0C4 e conn_id 0
duração de 3600 segundos
duração de 4608000 kilobytes
SA de saída 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 spi 0xDD2AC2B3 e conn_id 0
duração de 3600 segundos
duração de 4608000 kilobytes
ISAKMP (1002): enviando pacote para 172.16.10.1 my_port 500 peer_port 500 (I) QM_IDLE
ISAKMP:(1002):Envio de um pacote IPv4 IKE.
ISAKMP:(1002):exclusão do nó -830593317 erro FALSE motivo "Sem erro"
ISAKMP:(1002):Nó 3464373979, Entrada = IKE_MESG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1002):Estado Antigo = IKE_QM_I_QM1 Novo Estado = IKE_QM_PHASE2_COMPLETE
IPSEC(key_engine): recebeu um evento de fila com 1 mensagem KMI
Mapdb de criptografia: proxy_match
endereço src: 172.16.1.1
dst addr : 172.16.10.1
protocolo: 47
porta src: 0
porta dst: 0
IPSEC(crypto_ipsec_sa_find_ident_head): reconexão com os mesmos proxies 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 criado,
(sa) sa_dest= 172.16.1.1, sa_proto= 50,

shell de um SA que a
não pode ser usado p
transmitir tráfego.
A entrada do mapa d
pseudo-criptografia é
criada para o protoco
47 (GRE) de 172.16.
(endereço público do
a 172.16.1.1 (endere
público do spoke).

Um SA/SPI de IPSec
criado para o tráfego
entrada e saída com
valores da proposta a

O spoke envia a terc
última mensagem de
ao hub, que conclui a
de QM. Ao contrário
ISAKMP, onde cada
passa por cada estad
(MM1 a
MM6/P1_COMPLETE
IPSec é um pouco
diferente, pois há ape
três mensagens em v
seis. O iniciador (nos
spoke nesse caso,
conforme indicado po
na mensagem
IKE_QM_I_QM1) vai
QM_READY e depois
QM_I_QM1 diretame
para
QM_PHASE2_COMP
O Respondente (hub
para QM_READY,
QM_SPI_STARVE,
QM_R_QM2,

	sa_spi= 0x82C3E0C4(2193875140), sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 3 sa_lifetime(k/seg)= (4499172/3600) **IPSEC(create_sa): sa criado,** (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/seg)= (4499172/3600) **IPSEC(update_current_outbound_sa): get enable SA peer 172.16.10.1 current outbound sa to SPI DD2AC2B3** **IPSEC(update_current_outbound_sa): atualização da saída atual do peer 172.16.10.1 para SPI DD2AC2B3** IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce): atualizando o Tunnel0 ident 94F2740 com tun_decap_oce 794ED30 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): consulta de conexão retornada 961D220 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): tunnel_protection_socket_up IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Sinalização de NHRP NHRP: NHS 10.1.1.254 Tunnel0 vrf 0 Cluster Prioridade 0 Transição para 'E' de ' ' IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): consulta de conexão retornada 961D220 NHRP: Tentando enviar pacote via DEST 10.1.1.254	QM_PHASE2_COMP Outra mensagem de criação de SA é vista tem IPs de destino, S atributos de conjunto transformação e dura em kilobytes e segun restantes.
Essas mensagens de QM finais confirmam que o Modo rápido está concluído e que o IPSec está ativado em ambos os lados do túnel. Ao contrário do ISAKMP, onde cada peer passa por cada estado (MM1 a MM6/P1_COMPLETE), o IPSec é um pouco diferente, pois há apenas três mensagens em vez de seis. O Respondedor (nosso hub neste caso, conforme indicado por "R" na mensagem IKE_QM_**R**_QM1) vai para QM_READY, QM_SPI_STARVE, QM_R_QM2, QM_PHASE2_COMPLETE. O iniciador (spoke) vai de QM_READY e, em seguida, para QM_I_QM1	**ISAKMP (1002): pacote recebido de 172.16.1.1 porta 500 esportivo 500 Global (R) QM_IDLE** ISAKMP:(1002):exclusão do nó -830593317 erro FALSO motivo "QM concluído (aguardar)" ISAKMP:(1002):Nó 3464373979, Entrada = IKE_MESG_FROM_PEER, IKE_QM_EXCH **ISAKMP:(1002):Estado Antigo = IKE_QM_R_QM2 Novo Estado = IKE_QM_PHASE2_COMPLETE** IPSEC(key_engine): recebeu um evento de fila com 1 mensagem KMI IPSEC(key_engine_enable_outbound): rec'd ativar notificação de ISAKMP **IPSEC(key_engine_enable_outbound): enable SA com spi 2193875140/50** **IPSEC(update_current_outbound_sa): get enable SA peer 172.16.1.1 current outbound sa to SPI 82C3E0C4** **IPSEC(update_current_outbound_sa): ponto de saída atual 172.16.1.1 atualizado do sa para SPI 82C3E0C4**	

diretamente para
QM_PHASE2_COMPLETE.

NHRP: Enviar solicitação de registro via Tunnel0 vrf 0, tamanho do pacote: 108
src: 10.1.1.1, dst: 10.1.1.254
F) Fn: IPv4(1), tipo: IP(800), salto: 255, ver: 1
shtl: 4(NSAP), sstl: 0(NSAP)
pktsz: 108 saídas: 52
M) Sinais: "nat exclusivo ", reqid: 65540
NBMA src: 172.16.1.1
protocolo src: 10.1.1.1, protocolo dst: 10.1.1.254
Código (C-1): sem erro(0)
prefixo: 32, mtu: 17912, hd_time: 7200
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
Extensão do endereço do respondedor(3):
Extensão de registro NHS de trânsito adiante(4):
Extensão do registro NHS de trânsito reverso(5):
Extensão de autenticação(7):
tipo:Cleartext(1), data:NHRPAUTH
Extensão do endereço NAT(9):
Código (C-1): sem erro(0)
prefixo: 32, mtu: 17912, hd_time: 0
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref.: 0
NBMA do cliente: 172.16.10.1
protocolo cliente: 10.1.1.254

Essas são as solicita
de registro NHRP en
ao hub na tentativa d
registrar no NHS (o h
normal ver vários des
números, já que o sp
continua tentando se
registrar no NHS até
receber uma "respos
registro".
src,dst: Endereços IP
origem do túnel (spok
destino (hub). Esses
origem e o destino do
pacote GRE enviado
roteador
src NBMA: o endereç
NBMA (Internet) do s
que enviou esse pac
tenta se registrar no
protocolo src: endere
túnel do spoke que te
registrar
protocolo dst: endere
túnel do NHS/hub
Extensão de Autentic
dados: string d
autenticação NHRP
NBMA do cliente: En
NBMA do NHS/hub
protocolo cliente: end
do túnel do NHS/hub

TAXA DE NHRP: Enviando solicitação de registro inicial para 10.1.1.254, solicitação 65540
%LINK-3-UPDOWN: Interface Tunnel0, estado alterado para ativado
NHRP: if_up: Tunnel0 proto 0
NHRP: Túnel0: Atualização do cache para o destino 10.1.1.254/32 próximo salto 10.1.1.254
172.16.10.1
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):
consulta de conexão retornada 961D220
NHRP: Tentando enviar pacote via DEST 10.1.1.254

Mais mensagens de
serviço NHRP que di
que a solicitação de
registro inicial foi env
ao NHS em 10.1.1.25
Também há uma
confirmação de que u
entrada de cache foi
adicionada para o túr
10.1.1.254/24 que viv
NBMA 172.16.10.1. A
mensagem atrasada
que o túnel foi "no sh
(sem fechamento) é v
aqui.

IPSEC-IFC GRE/Tu0: túnel chegando
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):
consulta de conexão retornada 961D220
IPSEC-IFC GRE/Tu0: crypto_ss_hear_start já está

Essas são mensagen
gerais de serviço IPS
que dizem que funcio
corretamente. Aqui é

	ouvindo IPSEC-IFC GRE/Tu0: crypto_ss_hear_start já está ouvindo **IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Abrindo um soquete com o perfil DMVPN-IPSEC** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): consulta de conexão retornada 961D220 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): O soquete já está aberto. Ignorando. %LINEPROTO-5-UPDOWN: Protocolo de linha no túnel de interface0, estado alterado para ativado
Estas são as solicitações de registro NHRP recebidas do spoke na tentativa de se registrar no NHS (o hub). É normal ver vários desses números, já que o spoke continua tentando se registrar no NHS até receber uma "resposta de registro". **src NBMA**: o endereço NBMA (Internet) do spoke que enviou esse pacote e tenta se registrar no NHS **protocolo src**: endereço de túnel do spoke que tenta registrar **protocolo dst**: endereço do túnel do NHS/hub **Extensão de Autenticação**, dados: string de autenticação NHRP **NBMA do cliente**: Endereço NBMA do NHS/hub **protocolo cliente**: endereço do túnel do NHS/hub	**NHRP: Receber solicitação de registro via Tunnel0 vrf 0, tamanho do pacote: 108** F) Fn: IPv4(1), tipo: IP(800), salto: 255, ver: 1 shtl: 4(NSAP), sstl: 0(NSAP) pktsz: 108 saídas: 52 M) Sinais: "nat exclusivo ", reqid: 65540 **NBMA src: 172.16.1.1** **protocolo src: 10.1.1.1, protocolo dst: 10.1.1.254** Código (C-1): sem erro(0) prefixo: 32, mtu: 17912, hd_time: 7200 addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0 Extensão do endereço do respondedor(3): Extensão de registro NHS de trânsito adiante(4): Extensão do registro NHS de trânsito reverso(5): **Extensão de autenticação(7): tipo:Cleartext(1), data:NHRPAUTH** Extensão do endereço NAT(9): Código (C-1): sem erro(0) prefixo: 32, mtu: 17912, hd_time: 0 addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref.: 0 **NBMA do cliente: 172.16.10.1** **protocolo cliente: 10.1.1.254**
Pacotes de depuração NHRP adicionando a rede de destino 10.1.1.1/32 disponíveis através do salto seguinte de 10.1.1.1 no NHRP de 172.16.1.1. 172.16.1.1 também é adicionado à lista de endereços para os quais o hub encaminha o tráfego multicast. Essas mensagens confirmam que o registro foi bem-sucedido, assim como uma resolução para o endereço do túnel de	NHRP: netid_in = 1, to_us = 1 **NHRP: Túnel0: Adição de cache para o destino 10.1.1.1/32 próximo salto 10.1.1.1 172.16.1.1** **NHRP: Adicionando pontos finais de túnel (VPN: 10.1.1.1, NBMA: 172.16.1.1)** **NHRP: Subbloco NHRP conectado com êxito para Endpoints de túnel (VPN: 10.1.1.1, NBMA: 172.16.1.1)** NHRP: Nó de subbloco inserido para cache: Nó de subbloco de destino inserido para cache: Destino 10.1.1.1/32nhop 10.1.1.1 NHRP: Entrada de cache dinâmica interna convertida para 10.1.1.1/32 interface Tunnel0 para externa **NHRP: Tu0: Criando NBMA de mapeamento multicast dinâmico: 172.16.1.1** **NHRP: Adicionado mapeamento multicast dinâmico**

finalmente se vê que protocolo de túnel es ativo.

spokes.

Esta é a Resposta de Registro de NHRP enviada pelo hub para o spoke em resposta à "Solicitação de Registro de NHRP" recebida anteriormente. Como os outros pacotes de registro, o hub envia vários desses em resposta às várias solicitações.
src,dst: Endereços IP origem do túnel (hub) e destino (spoke). Esses são a origem e o destino do pacote GRE enviado pelo roteador
src NBMA: Endereço NBMA (Internet) do spoke
protocolo src: endereço de túnel do spoke que tenta registrar
protocolo dst: endereço do túnel do NHS/hub
NBMA do cliente: Endereço NBMA do NHS/hub
protocolo cliente: endereço do túnel do NHS/hub
Extensão de Autenticação, dados: string de autenticação NHRP

para NBMA: 172.16.1.1
NHRP: Atualizando nosso cache com NBMA: 172.16.10.1, NBMA_ALT: 172.16.10.1
NHRP: Novo comprimento obrigatório: 32
NHRP: Tentando enviar o pacote via DEST 10.1.1.1
NHRP: NHRP resolvido com êxito 10.1.1.1 para NBMA 172.16.1.1
NHRP: Encapsulamento bem-sucedido. Endereço IP do túnel 172.16.1.1
NHRP: Enviar resposta de registro via Tunnel0 vrf 0, tamanho do pacote: 128
src: 10.1.1.254, dst: 10.1.1.1
F) Fn: IPv4(1), tipo: IP(800), salto: 255, ver: 1
shtl: 4(NSAP), sstl: 0(NSAP)
pktsz: 128 saídas: 52
M) Sinais: "nat exclusivo ", reqid: 65540
NBMA src: 172.16.1.1
protocolo src: 10.1.1.1, protocolo dst: 10.1.1.254
Código (C-1): sem erro(0)
prefixo: 32, mtu: 17912, hd_time: 7200
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
Extensão do endereço do respondedor(3):
C) Código: sem erro(0)
prefixo: 32, mtu: 17912, hd_time: 7200
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref.: 0
NBMA do cliente: 172.16.10.1
protocolo cliente: 10.1.1.254
Extensão de registro NHS de trânsito adiante(4):
Extensão do registro NHS de trânsito reverso(5):
Extensão de autenticação(7):
tipo:Cleartext(1), data:NHRPAUTH
Extensão do endereço NAT(9):
Código (C-1): sem erro(0)
prefixo: 32, mtu: 17912, hd_time: 0
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref.: 0
NBMA do cliente: 172.16.10.1
protocolo cliente: 10.1.1.254
NHRP: Receber resposta de registro via Tunnel0 vrf 0, tamanho do pacote: 128
F) Fn: IPv4(1), tipo: IP(800), salto: 255, ver: 1
shtl: 4(NSAP), sstl: 0(NSAP)
pktsz: 128 saídas: 52
M) Sinais: "nat exclusivo ", reqid: 65541
NBMA src: 172.16.1.1
protocolo src: 10.1.1.1, protocolo dst: 10.1.1.254
Código (C-1): sem erro(0)
prefixo: 32, mtu: 17912, hd_time: 7200
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
Extensão do endereço do respondedor(3):

Esta é a Resposta de
Registro de NHRP en
pelo hub para o spok
resposta à "Solicitaçã
Registro de NHRP"
recebida anteriormen
Como os outros pacc
registro, o hub envia
desses em resposta
várias solicitações.
src NBMA: Endereço
NBMA (Internet) do s
protocolo src: endere

	C) Código: sem erro(0) prefixo: 32, mtu: 17912, hd_time: 7200 addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref.: 0 **NBMA do cliente: 172.16.10.1** **protocolo cliente: 10.1.1.254** Extensão de registro NHS de trânsito adiante(4): Extensão do registro NHS de trânsito reverso(5): **Extensão de autenticação(7):** **tipo:Cleartext(1), data:NHRPAUTH** Extensão do endereço NAT(9): Código (C-1): sem erro(0) prefixo: 32, mtu: 17912, hd_time: 0 addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref.: 0 **NBMA do cliente: 172.16.10.1** **protocolo cliente: 10.1.1.254**	túnel do spoke que te registrar **protocolo dst**: endere túnel do NHS/hub **NBMA do cliente**: En NBMA do NHS/hub **protocolo cliente**: enc do túnel do NHS/hub **Extensão de Autentic** dados: string d autenticação NHRP
Mensagens de serviço IPSec mais gerais que dizem que funciona corretamente.	NHRP: netid_in = 0, to_us = 1 IPSEC-IFC MGRE/Tu0: crypto_ss_hear_start já está ouvindo IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Abrindo um soquete com o perfil DMVPN-IPSEC IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): consulta de conexão retornada 8C93888 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): O soquete já está aberto. Ignorando. IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): tunnel_protection_stop_pending_timer 8C93888	
	NHRP: NHS-UP: 10.1.1.254	Mensagens de serviç NHRP que dizem que NHS localizado em 10.1.1.254 está ativa
A mensagem do sistema que indica que a adjacência do EIGRP está ativa com o spoke vizinho em 10.1.1.1.	%DUAL-5-NBRCHANGE: EIGRP-IPv4 1: O vizinho 10.1.1.1 (Tunnel0) está ativado: nova adjacência	
	%DUAL-5-NBRCHANGE: EIGRP-IPv4 1: O vizinho 10.1.1.254 (Tunnel0) está ativado: nova adjacência	A mensagem do siste que indica que a adjacência do EIGRP ativa com o hub vizin 10.1.1.254.
Mensagem de sistema que confirma uma resolução NHRP bem-sucedida.	NHRP: NHRP resolvido com êxito 10.1.1.1 para NBMA 172.16.1.1	

Confirmar funcionalidade e solucionar problemas

Esta seção tem alguns dos comandos **show** mais úteis usados para solucionar problemas de hub e spoke. Para habilitar depurações mais específicas, use estas condições de depuração:

- debug dmvpn condition peer nbma *NBMA_ADDRESS*

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

show crypto sockets

```
Spoke1#show crypto sockets

Number of Crypto Socket connections 1

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

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

Hub#show crypto sockets

Number of Crypto Socket connections 1

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

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

show crypto session detail

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

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

Interface: Tunnel0
Uptime: 00:01:01
Session status: UP-ACTIVE
Peer: 172.16.10.1 port 500 fvrf: (none) ivrf: (none)
Phase1_id: 172.16.10.1
Desc: (none)
IKEv1 SA: local 172.16.1.1/500 remote 172.16.10.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:58
IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.10.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 25 drop 0 life (KB/Sec) 4596087/3538
Outbound: #pkts enc'ed 25 drop 3 life (KB/Sec) 4596087/3538

Hub#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
```

```
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

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

show crypto isakmp sa detail

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

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

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

IPv6 Crypto ISAKMP SA

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

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

IPv6 Crypto ISAKMP SA
```

show crypto ipsec sa detail

```
Spoke1#show crypto ipsec sa detail
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 172.16.1.1
protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.10.1/255.255.255.255/47/0)
current_peer 172.16.10.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 24, #pkts encrypt: 24, #pkts digest: 24
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#pkts no sa (send) 3, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

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

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

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

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

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

local crypto endpt.: 172.16.10.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
```

```
current outbound spi: 0x8D538D11(2371063057)
PFS (Y/N): N, DH group: none

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

inbound ah sas:

inbound pcp sas:

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

outbound ah sas:
outbound pcp sas:
```

show ip nhrp

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

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

show ip nhs

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

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

show dmvpn [detail]

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

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

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

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

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

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

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

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


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

Pending DMVPN Sessions:

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

Interface: Tunnel0, IPv4 NHRP Details Type:Hub, NHRP Peers:1,
```

```
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.1.1.1 UP 00:01:30 D

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

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

Pending DMVPN Sessions:
```

Informações Relacionadas

- Solução de problemas de IPsec: Entendendo e usando comandos debug
- Criptografia de próxima geração
- RFC3706: Detecção de peer inoperante de IKE
- RFC3947: IKE NAT Traversal
- Suporte Técnico e Documentação - Cisco Systems