DMVPN ao exemplo de configuração macio da migração de FlexVPN

Índice

Introdução

Este documento descreve como executar uma migração *macia* onde o Dynamic Multipoint VPN (DMVPN) e FlexVPN trabalhem em um dispositivo simultaneamente sem a necessidade para uma ação alternativa e fornece um exemplo de configuração.

> **Note**: Este documento expande nos conceitos descritos na migração de FlexVPN: Movimento duro do DMVPN a FlexVPN nos mesmos dispositivos e migração de FlexVPN: Movimento duro do DMVPN a FlexVPN em artigos diferentes de Cisco de um hub. Both of these documentos descrevem as migrações *duras*, que fazem com que algum rompimento trafique durante a migração. As limitações nestes artigos são devido a uma deficiência no

software do ® do Cisco IOS que é retificado agora.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- DMVPN
- FlexVPN

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versões 15.3(3)M ou mais recente do roteador do serviço integrado de Cisco (ISR)
- O roteador agregado Cisco 1000 Series do serviço (ASR1K) libera 3.10 ou mais atrasado

> **Note**: Não toda a versão 2 do intercâmbio de chave de Internet do suporte de software e hardware (IKEv2). Refira o Cisco Feature Navigator para a informação.

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.

Informações de Apoio

Uma das vantagens da plataforma do IOS da Cisco e do software mais novos é a capacidade para usar a criptografia da próxima geração. Um exemplo é o uso do Advanced Encryption Standard (AES) em Galois/modo contrário (GCM) para a criptografia no IPsec, como discutido no RFC 4106. O AES GCM reserva umas velocidades muito mais rápidas da criptografia em algum hardware.

> **Note**: Para obter informações adicionais sobre do uso de e da migração à criptografia da próxima geração, refira o artigo de Cisco da criptografia da próxima geração.

Configurar

Este exemplo de configuração centra-se sobre uma migração de uma configuração da fase 3 DMVPN a um FlexVPN, porque ambos os projetos trabalham similarmente.

	Fase 2 DMVPN	Fase 3 DMVPN	FlexVPN
Transporte	GRE sobre o IPsec	GRE sobre o IPsec	GRE sobre o IPsec,

Uso NHRP	Registro e definição	Registro e definição	Resolução
Salto seguinte do spoke	O outro spokes ou hub	Sumário do hub	Sumário do hub
Interruptor do atalho NHRP	No	Yes	Sim (opcional)
Reorientação NHRP	No	Yes	Yes
IKE e IPsec	IPsec opcional, IKEv1 típico	IPsec opcional, IKEv1 típico	IPsec, IKEv2

Diagramas da rede

Esta seção fornece diagramas da rede do transporte e da folha de prova.

Diagrama de rede de transporte

A rede de transporte usada neste exemplo inclui um concentrador único com os dois spokes conectados. Todos os dispositivos são conectados através de uma rede que simule o Internet.

Diagrama da rede da folha de prova

A rede de folha de prova usada neste exemplo inclui um concentrador único com os dois spokes conectados. Recorde que o DMVPN e FlexVPN são ativos simultaneamente, mas eles usam os espaços de endereços IP diferentes.

Configurações

Esta configuração migra o desenvolvimento o mais popular da fase 3 DMVPN através do Enhanced Interior Gateway Routing Protocol (EIGRP) a FlexVPN com Border Gateway Protocol (BGP). Cisco recomenda o uso do BGP com FlexVPN, porque permite que as disposições escalem melhor.

> **Note**: O hub termina (FlexVPN) as sessões IKEv1 (DMVPN) e IKEv2 no mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT. Isto é possível somente com liberações recentes do Cisco IOS.

Configuração de raio

Esta é muito uma configuração básica, com duas exceções notável que permitem a interactuação de IKEv1 e de IKEv2, assim como duas estruturas que usam o Generic Routing Encapsulation (GRE) sobre o IPsec para o transporte a fim coexistir.

> **Note**: As mudanças relevantes ao Internet Security Association and Key Management Protocol (ISAKMP) e a configuração IKEv2 são destacadas em corajoso.

```
crypto keyring DMVPN_IKEv1
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco
```

```
crypto logging session

crypto ikev2 keyring Flex_key
peer Spokes
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco
pre-shared-key remote cisco

crypto ikev2 profile Flex_IKEv2
match identity remote address 0.0.0.0
authentication remote pre-share
authentication local pre-share
keyring local Flex_key
aaa authorization group psk list default default
virtual-template 1

crypto ikev2 dpd 30 5 on-demand

crypto isakmp policy 10
encr aes
authentication pre-share

crypto isakmp keepalive 30 5

crypto isakmp profile DMVPN_IKEv1
keyring DMVPN_IKEv1
match identity address 0.0.0.0

crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
mode transport

crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1
set isakmp-profile DMVPN_IKEv1

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

interface Tunnel0
 desciption DMVPN tunnel
ip address 10.0.0.101 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map 10.0.0.1 172.25.1.1
ip nhrp map multicast 172.25.1.1
ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp nhs 10.0.0.1
ip nhrp shortcut
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel mode gre multipoint
 tunnel key 0
tunnel protection ipsec profile DMVPN_IKEv1 isakmp-profile DMVPN_IKEv1

interface Tunnel1
description FlexVPN spoke-to-hub tunnel
ip address negotiated
ip mtu 1400
 ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
```

```
tunnel source Ethernet0/0
tunnel destination 172.25.1.1
 tunnel protection ipsec profile default ikev2-profile Flex_IKEv2


interface Virtual-Template1 type tunnel
description FlexVPN spoke-to-spoke
ip unnumbered Ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel protection ipsec profile default ikev2-profile Flex_IKEv2
```

O Cisco IOS Release 15.3 permite que você amarre IKEv2 e perfis ISAKMP junto em uma *configuração de proteção do túnel*. Junto com algumas mudanças internas ao código, isto permite que IKEv1 e IKEv2 operem sobre o mesmo dispositivo simultaneamente.

Devido à maneira o Cisco IOS seleciona os perfis (IKEv1 ou IKEv2) nas liberações mais cedo de 15.3, ele conduziram a algumas advertências, tais como as situações onde IKEv1 é iniciado a IKEv2 através do par. A separação de IKE é baseada agora no perfil-nível, não o relação-nível, que é conseguido através do CLI novo.

Uma outra elevação na liberação do Novo Cisco IOS é a adição da *chave do túnel*. Isto é precisado porque o DMVPN e FlexVPN usam a mesma interface de origem e o mesmo endereço IP de destino. Com isto no lugar, não há nenhuma maneira para que o túnel GRE saiba que interface de túnel é tráfego usado do decapsulate. A chave do túnel permite que você diferencie o **tunnel0** e o **tunnel1** com a adição (de umas despesas gerais pequenas do byte 4). Uma chave diferente pode ser configurada em ambas as relações, mas você precisa tipicamente somente de diferenciar um túnel.

> **Note**: A opção de proteção compartilhada do túnel não é exigida quando o DMVPN e FlexVPN compartilham da mesma relação.

Assim, a configuração de protocolo de roteamento do spoke é básica. O EIGRP e o BGP trabalham separadamente. O EIGRP anuncia somente sobre a interface de túnel a fim evitar espreitar sobre túneis spoke-to-spoke, que limita a escalabilidade. O BGP mantém um relacionamento somente com o roteador de hub (**10.1.1.1**) a fim anunciar a rede local (**192.168.101.0/24**).

```
interface Virtual-Template1 type tunnel
description FlexVPN spoke-to-spoke
ip unnumbered Ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel protection ipsec profile default ikev2-profile Flex_IKEv2
```

Configuração do hub

Você deve fazer mudanças similares na configuração do lado de hub como aquelas descritas na seção de **configuração de raio**.

Note: As mudanças relevantes à configuração ISAKMP e IKEV2 são destacadas em corajoso.

```
interface Virtual-Template1 type tunnel
description FlexVPN spoke-to-spoke
ip unnumbered Ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel protection ipsec profile default ikev2-profile Flex_IKEv2


crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

interface Tunnel0
ip address 10.0.0.1 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map multicast dynamic
 ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp server-only
ip nhrp redirect
 ip summary-address eigrp 100 192.168.0.0 255.255.0.0
ip tcp adjust-mss 1360
tunnel source Loopback0
tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile DMVPN_IKEv1

interface Virtual-Template1 type tunnel
ip unnumbered Loopback100
ip mtu 1400
 ip nhrp network-id 2
ip tcp adjust-mss 1360
 tunnel protection ipsec profile default
```

No lado de hub, o emperramento entre o perfil IKE e o perfil IPSec ocorre no perfil-nível, ao contrário da configuração de raio, onde este é terminado através do comando tunnel protection. Ambas as aproximações são métodos viáveis para terminar este emperramento.

Éimportante notar que os ID de rede do Next Hop Resolution Protocol (NHRP) são diferentes para o DMVPN e o FlexVPN na nuvem. Na maioria dos casos, é indesejável quando o NHRP cria um único domínio sobre ambas as estruturas.

A chave do túnel diferencia o DMVPN e os túneis de FlexVPN no GRE-nível a fim conseguir o mesmo objetivo que é mencionado na seção de configuração de raio.

A configuração de roteamento no hub é razoavelmente básica. O dispositivo do hub mantém dois relacionamentos com o qualquer spoke, que usa o EIGRP e dados que usar o BGP. A configuração de BGP usa a escutar-escala a fim evitar um longo, configuração do por-spoke.

Os endereços sumário são introduzidos duas vezes. A configuração de EIGRP envia um sumário com uso da configuração do **tunnel0** (sumário-endereço EIGRP 100 IP), e o BGP introduz um sumário com uso do agregado-endereço. Os sumários são exigidos a fim assegurar-se de que a reorientação NHRP ocorra, e a fim simplificar as atualizações de roteamento. Você pode enviar um NHRP reorienta (bem como um Internet Control Message Protocol (ICMP) reoriente) que indique se um salto melhor existe para um destino fornecido, que permita que um túnel spoke-to-spoke seja estabelecido. Estes sumários são usados igualmente a fim minimizar a quantidade de atualizações de roteamento que são enviadas entre o hub e cada spoke, que permite que as instalações escalem melhor.

```
router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.0.0 0.0.255.255
passive-interface default
no passive-interface Tunnel0

router bgp 65001
bgp log-neighbor-changes
 bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
 aggregate-address 192.168.0.0 255.255.0.0 summary-only
neighbor Spokes peer-group
neighbor Spokes remote-as 65001
```

Verificar

A verificação para este exemplo de configuração é dividida em diversas seções.

Verificações da PRE-migração

Desde que DMVPN/EIGRP e FlexVPN/BGP se operam simultaneamente, você deve verificar que o spoke mantém um relacionamento sobre o IPsec com o IKEv1 e o IKEv2, e que os prefixos apropriados são instruídos sobre o EIGRP e o BGP.

Neste exemplo, **Spoke1** mostra que duas sessões estão mantidas com o roteador de hub; um usa IKEv1/Tunnel0 e um usa IKEv2/Tunnel1.

> **Note**: Duas associações de segurança IPSec (SA) (um de entrada e um de partida) são mantidas para cada um dos túneis.

```
Spoke1#show cry sess
Crypto session current status

Interface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto map
```

```
Interface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
 IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

Quando você verifica os protocolos de roteamento, você deve verificar que um neighborship está formado, e que os prefixos corretos são instruídos. Isto é verificado primeiramente com o EIGRP. Verifique que o hub é visível como um vizinho, e que o endereço 192.168.0.0/16 (o sumário) é instruído do hub:

```
Spoke1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.0.0.1 Tu0 10 00:04:02 7 1398 0 13

Spoke1#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

P 192.168.101.0/24, 1 successors, FD is 281600
via Connected, Ethernet1/0
P 192.168.0.0/16, 1 successors, FD is 26880000
via 10.0.0.1 (26880000/256), Tunnel0
P 10.0.0.0/24, 1 successors, FD is 26880000
via Connected, Tunnel0
```

Em seguida, verifique o BGP:

```
Spoke1#show bgp summary
(...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 13 11 3 0 0 00:06:56 1
Spoke1#show bgp
BGP table version is 3, local router ID is 192.168.101.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
r>i 192.168.0.0/16 10.1.1.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
```

A saída mostra que o endereço IP de Um ou Mais Servidores Cisco ICM NT de FlexVPN do hub (10.1.1.1) é um vizinho através de que o spoke recebe um prefixo (192.168.0.0/16). Adicionalmente, o BGP informa o administrador que uma falha do Routing Information Base (RIB) ocorreu para o prefixo 192.168.0.0/16. Esta falha ocorre porque há uma rota melhor para esse prefixo que já existe na tabela de roteamento. Esta rota está originada pelo EIGRP, e pode ser confirmada se você verifica a tabela de roteamento.

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
 Known via "eigrp 100", distance 90, metric 26880000, type internal
Redistributing via eigrp 100
Last update from 10.0.0.1 on Tunnel0, 00:10:07 ago
Routing Descriptor Blocks:
* 10.0.0.1, from 10.0.0.1, 00:10:07 ago, via Tunnel0
Route metric is 26880000, traffic share count is 1
Total delay is 50000 microseconds, minimum bandwidth is 100 Kbit
Reliability 255/255, minimum MTU 1400 bytes
Loading 1/255, Hops 1
```

Migração

A seção anterior verificou que o IPsec e os protocolos de roteamento estão configurados e trabalho como esperado. Uma das maneiras as mais fáceis de migrar do DMVPN a FlexVPN no mesmo dispositivo é mudar a distância administrativa (AD). Neste exemplo, o Internal BGP (iBGP) tem um AD de 200, e o EIGRP tem um AD de 90.

Para que o tráfego corra através do FlexVPN corretamente, o BGP deve ter um AD melhor. Neste exemplo, o EIGRP AD é mudado a 230 e a 240 para rotas internas e externas, respectivamente. Isto faz o BGP AD (de 200) mais preferível para o prefixo 192.168.0.0/16.

Um outro método que seja usado a fim conseguir este é diminuir o BGP AD. Contudo, o protocolo que é executado depois que a migração tem os valores fora de padrão, que podem impactar outras partes do desenvolvimento.

Neste exemplo, o comando debug ip routing é usado a fim verificar a operação no spoke.

> **Note**: Se a informação nesta seção é usada em uma rede de produção, evite o uso dos comandos debug, e confie nos comandos show alistados na próxima seção. Também, o processo de EIGRP do spoke deve restabelecer a adjacência com o hub.

```
Spoke1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Spoke1(config)#router eigrp 100
Spoke1(config-router)# distance eigrp 230 240
Spoke1(config-router)#^Z
Spoke1#
*Oct 9 12:12:34.207: %SYS-5-CONFIG_I: Configured from console by console
*Oct 9 12:12:43.648: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is down: route configuration changed

*Oct 9 12:12:43.648: RT: delete route to 192.168.0.0 via 10.0.0.1,
 eigrp metric [90/26880000]
*Oct 9 12:12:43.648: RT: no routes to 192.168.0.0, delayed flush
*Oct 9 12:12:43.648: RT: delete network route to 192.168.0.0/16
*Oct 9 12:12:43.650: RT: updating bgp 192.168.0.0/16 (0x0) :
via 10.1.1.1

Spoke1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Spoke1(config)#router eigrp 100
Spoke1(config-router)# distance eigrp 230 240
Spoke1(config-router)#^Z
Spoke1#
```

```
*Oct 9 12:12:34.207: %SYS-5-CONFIG_I: Configured from console by console
*Oct 9 12:12:43.648: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is down: route configuration changed

*Oct 9 12:12:43.648: RT: delete route to 192.168.0.0 via 10.0.0.1,
 eigrp metric [90/26880000]
*Oct 9 12:12:43.648: RT: no routes to 192.168.0.0, delayed flush
*Oct 9 12:12:43.648: RT: delete network route to 192.168.0.0/16
*Oct 9 12:12:43.650: RT: updating bgp 192.168.0.0/16 (0x0) :
via 10.1.1.1
```

Há três ações importantes a observar nesta saída:

- O spoke observa que o AD mudado, e desabilita a adjacência.
- Na tabela de roteamento, o prefixo EIGRP retied, e o BGP é introduzido.
- A adjacência ao hub sobre o EIGRP volta em linha.

Quando você muda o AD em um dispositivo, afeta somente o trajeto do dispositivo às outras redes; não afeta como o outro Roteadores executa o roteamento. Por exemplo, depois que a distância EIGRP está aumentada em **Spoke1** (e nele usa FlexVPN na nuvem a fim distribuir o tráfego), o hub mantém (padrão) os AD configurados. Isto significa que usa o DMVPN a fim distribuir o tráfego de volta a **Spoke1**.

Em determinadas encenações, isto pode causar problemas, como quando os Firewall esperam o tráfego de retorno na mesma relação. Consequentemente, você deve mudar o AD em todo o spokes antes que você o mude no hub. O tráfego está migrado inteiramente por FlexVPN somente uma vez que este está completo.

Migração EIGRP-à-EIGRP

Uma migração do DMVPN a FlexVPN que executa somente o EIGRP não é detalhada discutido neste documento; contudo, menciona-se aqui para a integralidade.

Épossível adicionar o DMVPN e o EIGRP ao mesmo sistema autônomo de EIGRP (QUE) que distribui o exemplo. Com isto no lugar, a adjacência do roteamento é estabelecida sobre ambos os tipos de nuvens. Isto pode fazer com que a função de balanceamento de carga ocorra, que não é recomendada tipicamente.

A fim assegurar-se de que FlexVPN ou o DMVPN estejam escolhidos, um administrador pode atribuir **valores de atraso** diferentes em uma base da interface per. Contudo, é importante recordar que nenhuma mudança é possível nas interfaces de molde virtual quando as interfaces de acesso virtual correspondentes estarem presente.

Verificações da Cargo-migração

Similar ao processo usado na PRE-**migração verifica a** seção, o IPsec e o protocolo de roteamento deve ser verificado.

Primeiramente, verifique o IPsec:

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

```
Interface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto map

Interface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

Como antes, duas sessões são consideradas, ambo têm dois o IPSec ativo SA.

No spoke, a rota agregada (192.168.0.0/16) aponta do hub e é instruída sobre o BGP.

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
Known via "bgp 65001", distance 200, metric 0, type internal
Last update from 10.1.1.1 00:14:07 ago
Routing Descriptor Blocks:
* 10.1.1.1, from 10.1.1.1, 00:14:07 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none
```

Similarmente, o spoke LAN que é prefixado no hub deve ser sabido através do EIGRP. Neste exemplo, a sub-rede de LAN de Spoke2 é verificada:

```
Hub#show ip route 192.168.102.0 255.255.255.0
Routing entry for 192.168.102.0/24
 Known via "bgp 65001", distance 200, metric 0, type internal
Last update from 10.1.1.106 00:04:35 ago
Routing Descriptor Blocks:
* 10.1.1.106, from 10.1.1.106, 00:04:35 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none

Hub#show ip cef 192.168.102.100
192.168.102.0/24
nexthop 10.1.1.106 Virtual-Access2
```

Na saída, o trajeto de encaminhamento é atualizado corretamente e indica de uma interface de acesso virtual.

Considerações adicionais

Esta seção descreve algumas áreas adicionais da importância que são relevantes a este exemplo de configuração.

Túneis spoke-to-spoke existentes

Com uma migração do EIGRP ao BGP, os túneis spoke-to-spoke não são impactados, porque o atalho-interruptor está ainda na operação. o Atalho-interruptor no spoke introduz uma rota mais específica NHRP com um AD de 250.

Está aqui um exemplo de tal rota:

```
Spoke1#show ip route 192.168.102.100
Routing entry for 192.168.102.0/24
Known via "nhrp", distance 250, metric 1
Last update from 10.1.1.106 on Virtual-Access1, 00:00:42 ago
Routing Descriptor Blocks:
* 10.1.1.106, from 10.1.1.106, 00:00:42 ago, via Virtual-Access1
Route metric is 1, traffic share count is 1
```

Uma comunicação entre o spokes migrado e NON-migrado

Se um spoke que está já em um FlexVPN/BGP quer se comunicar com um dispositivo para que o processo de migração não começou, o tráfego flui sempre sobre o hub.

Este é o processo que ocorre:

1. O spoke executa uma consulta da rota para o destino, que aponta através de uma rota sumária que seja anunciada pelo hub.
2. O pacote é enviado para o hub.
3. O hub recebe o pacote e executa uma consulta da rota para o destino, que indica de uma outra relação que seja parte de um domínio diferente NHRP.

   Note: A rede NHRP ID na configuração precedente do hub é diferente para FlexVPN e DMVPN.

Mesmo se a rede NHRP ID é unificada, um problema pôde ocorrer onde o spoke migrado distribui objetos sobre a rede de FlexVPN. Isto inclui a diretriz orientadora usada a fim configurar o interruptor do atalho. O spoke NON-migrado tenta executar objetos sobre a rede de DMVPN, com um objetivo específico para executar o interruptor do atalho.

Troubleshooting

Esta seção descreve o toubleshoot tipicamente usado de duas categorias a migração.

Problemas com tentativas de estabelecer túneis

Termine estas etapas se a negociação de IKE falha:

1. Verifique o estado atual com estes comandos:

   mostre isakmp cripto sa - Este comando revela a quantidade, a fonte, e o destino de uma sessão IKEv1.**a mostra cripto** comando **sa do IPsec** este revela a atividade do sas de

IPSec.**Note**: Ao contrário em IKEv1, no este output o valor de grupo do Diffie-Hellman (DH) do discrição perfeita adiante (PFS) aparece como o **PFS (Y/N): N, grupo DH: nenhuns** durante a primeira negociação do túnel; contudo, depois que um rekey ocorre, os valores corretos aparecem. Este não é um erro, mesmo que o comportamento seja descrito em CSCug67056. A diferença entre IKEv1 e IKEv2 é aquela nos últimos, a criança que os SA são criados como parte da troca do **AUTH**. O grupo DH que é configurado sob o crypto map é usado somente durante um rekey. Por este motivo, você vê o **PFS (Y/N): N, grupo DH: nenhuns** até os primeiros rekey. Com IKEv1, você vê um comportamento diferente porque a criação criança SA ocorre durante o Quick Mode, e a mensagem **CREATE_CHILD_SA** tem disposições para a transferência do payload das trocas de chave que especifica os parâmetros DH a fim derivar um segredo compartilhado novo.**mostre ikev2 criptos sa** - Este comando fornece a saída similar ao ISAKMP mas é específico a IKEv2.**sessão de criptografia da mostra** - Este comando fornece as saídas de sumário das sessões criptograficamente neste dispositivo.**mostre o soquete cripto** - Este comando mostra o estado dos cripto-soquetes.**crypto map da mostra** - Este comando mostra o mapeamento do IKE e dos perfis IPSec às relações.**mostre o nhrp IP** - Este comando fornece a informação NHRP do dispositivo. Isto é útil para spoke-to-spoke em instalações de FlexVPN, e para emperramentos spoke-to-spoke e spoke-to-hub em instalações DMVPN.
2. Use estes comandos a fim debugar o estabelecimento de túnel:

   debug crypto ikev2[debug crypto isakmp]**debug crypto ipsec**[kmi do debug crypto]

Problemas com propagação da rota

Estão aqui alguns comandos úteis que você pode usar a fim pesquisar defeitos o EIGRP e a topologia:

- **mostre o sumário BGP** - Use este comando a fim verificar os vizinhos conectados e seus estados.
- **mostre o vizinho EIGRP IP** - Use este comando a fim mostrar os vizinhos que são conectados através do EIGRP.
- **BGP da mostra** - Use este comando a fim verificar os prefixos aprendidos sobre o BGP.
- **mostre a topologia do eigrp IP** - Use este comando a fim mostrar os prefixos aprendidos através do EIGRP.

Éimportante saber que um prefixo instruído é diferente do que um prefixo que seja instalado na tabela de roteamento. Para obter mais informações sobre disto, proveja a seleção de rota no artigo de Cisco dos roteadores Cisco, ou o livro da Cisco Press de distribuição TCP/IP.

Caveats conhecidos

Uma limitação que paralelize a manipulação do túnel GRE existe no ASR1K. Isto é seguido sob a identificação de bug Cisco CSCue00443. Neste tempo, a limitação tem um reparo programado na liberação 3.12 do Software Cisco IOS XE.

Monitore este erro se você deseja uma notificação uma vez que o reparo se torna disponível.