Exemplo de configuração de migração de software DMVPN para FlexVPN

Contents

Introduction

Este documento descreve como executar uma migração de *software* na qual tanto a VPN multiponto dinâmica (DMVPN) como a FlexVPN funcionam em um dispositivo simultaneamente sem a necessidade de uma solução alternativa e fornece um exemplo de configuração.

> **Note**: Este documento expande os conceitos descritos na Migração do FlexVPN: Transferência forçada de DMVPN para FlexVPN nos mesmos dispositivos e migração de FlexVPN: Transferência forçada de DMVPN para FlexVPN em artigos diferentes de hub da Cisco. Esses dois documentos descrevem migrações *difíceis*, que causam alguma interrupção no tráfego durante a migração. As limitações nesses artigos se devem a uma

deficiência no software Cisco IOS® que agora é corrigida.

Prerequisites

Requirements

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:

- Cisco Integrated Service Router (ISR) versões 15.3(3)M ou posterior
- Cisco 1000 Series Aggregated Service Router (ASR1K) versões 3.10 ou posterior

Note: Nem todos os softwares e hardwares suportam o Internet Key Exchange Versão 2 (IKEv2). Consulte o Cisco Feature Navigator para obter informações.

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.

Informações de Apoio

Uma das vantagens da plataforma e do software Cisco IOS mais novos é a capacidade de usar a criptografia de última geração. Um exemplo é o uso do AES (Advanced Encryption Standard, Padrão de Criptografia Avançada) no GCM (Galois/Counter Mode) para criptografia no IPsec, conforme discutido no RFC 4106. O AES GCM permite velocidades de criptografia muito mais rápidas em algum hardware.

Note: Para obter informações adicionais sobre o uso e a migração para a criptografia de próxima geração, consulte o artigo da Cisco Next Generation Encryption.

Configurar

Este exemplo de configuração concentra-se em uma migração de uma configuração da fase 3 do DMVPN para um FlexVPN, porque ambos os designs funcionam da mesma forma.

	Fase 2 do DMVPN	Fase 3 do DMVPN	FlexVPN
Transporte	GRE sobre IPsec	GRE sobre IPsec	GRE sobre IPsec,
Uso de NHRP	Registro e resolução	Registro e resolução	Resolução

Próximo salto do Spoke	Outros Spokes ou Hub	Resumo do hub	Resumo do hub
Switching de atalho NHRP	No	Yes	Sim (opcional)
Redirecionamento de NHRP	No	Yes	Yes
IKE e IPsec	IPsec opcional, IKEv1 típico	IPsec opcional, IKEv1 típico	IPsec, IKEv2

Diagramas de rede

Esta seção fornece diagramas de rede de transporte e sobreposição.

Diagrama da rede de transporte

A rede de transporte usada neste exemplo inclui um único hub com dois spokes conectados. Todos os dispositivos são conectados através de uma rede que simula a Internet.

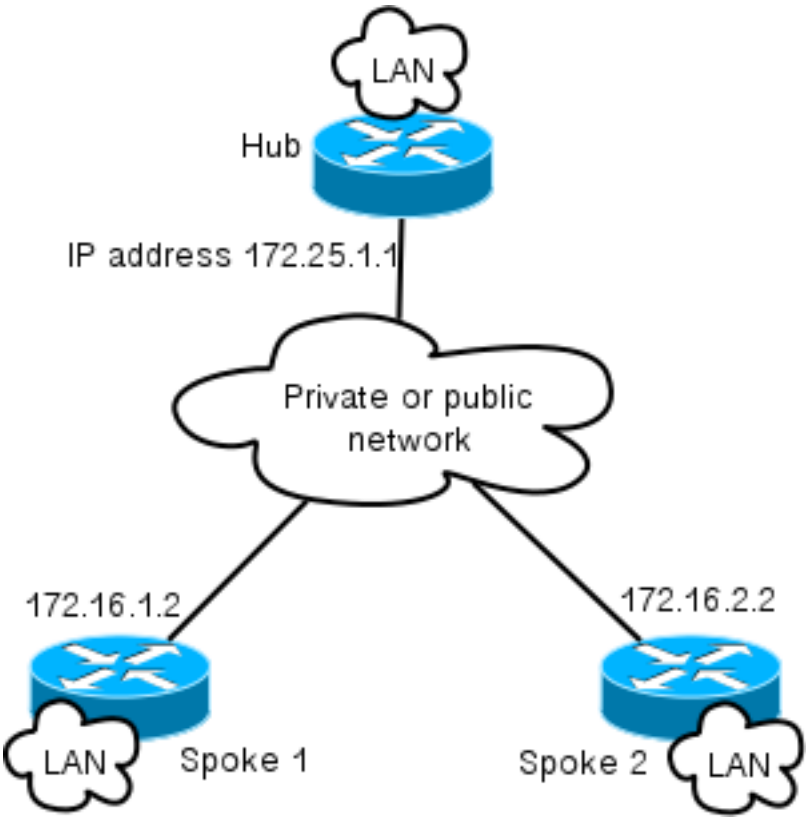
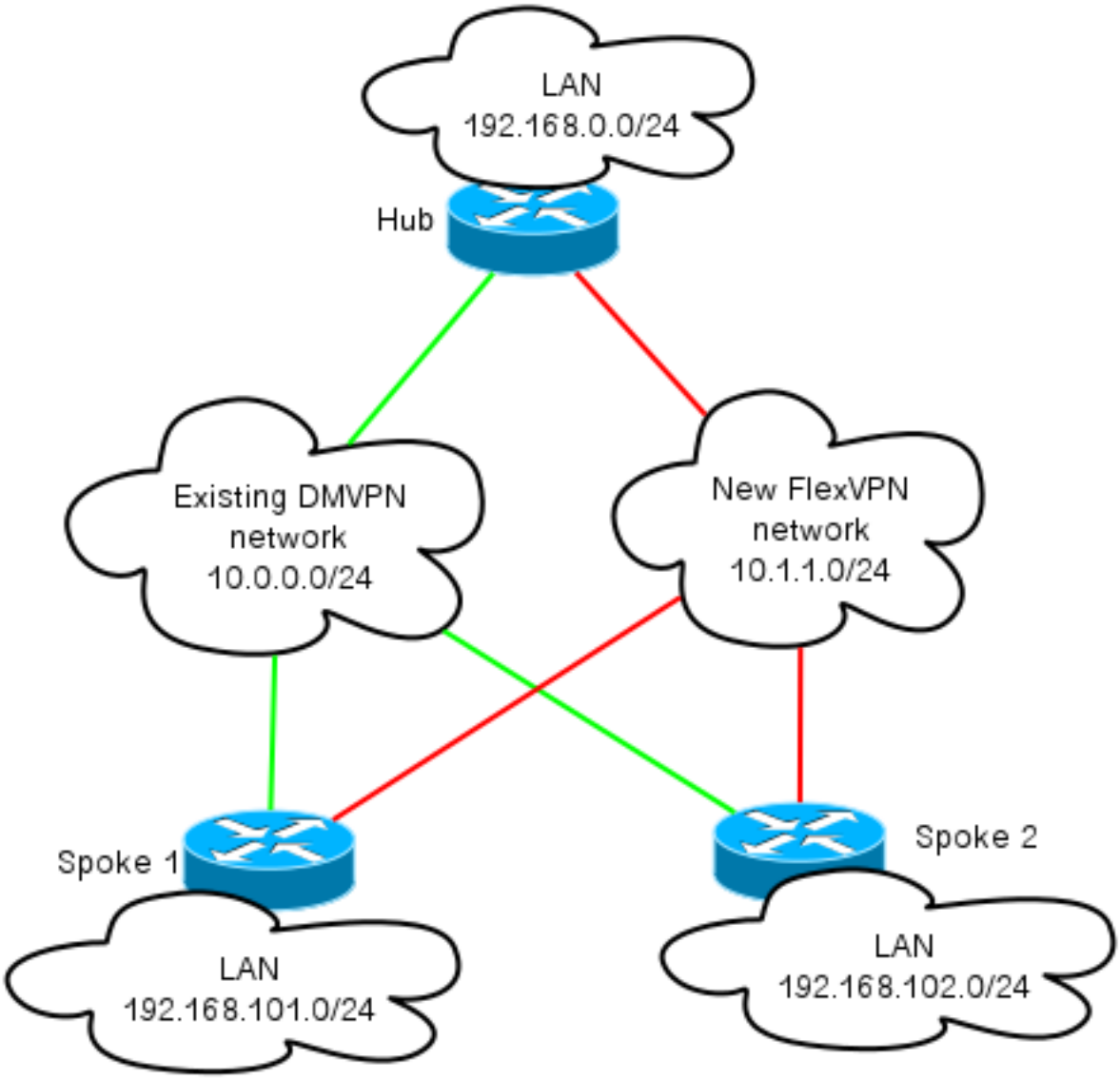


Diagrama de sobreposição de rede

A rede de sobreposição usada neste exemplo inclui um único hub com dois spokes conectados. Lembre-se de que o DMVPN e o FlexVPN estão ativos simultaneamente, mas usam espaços de endereços IP diferentes.



Configurações

Essa configuração migra a implantação mais popular da fase 3 do DMVPN via Enhanced Interior Gateway Routing Protocol (EIGRP) para o FlexVPN com Border Gateway Protocol (BGP). A Cisco recomenda o uso do BGP com FlexVPN, pois permite que as implantações escalem melhor.

> **Note**: O hub termina as sessões de IKEv1 (DMVPN) e IKEv2 (FlexVPN) no mesmo endereço IP. Isso só é possível com versões recentes do Cisco IOS.

Configuração de Spoke

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

> **Note**: As alterações relevantes na configuração da Internet Security Association and Key Management Protocol (ISAKMP) e IKEv2 estão destacadas em negrito.

```
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 versão 15.3 permite que você vincule os perfis IKEv2 e ISAKMP em uma configuração de *proteção de túnel*. Juntamente com algumas alterações internas ao código, isso permite que IKEv1 e IKEv2 operem no mesmo dispositivo simultaneamente.

Por causa da maneira como o Cisco IOS seleciona os perfis (IKEv1 ou IKEv2) em versões anteriores à 15.3, ele levou a algumas advertências, como situações em que IKEv1 é iniciado para IKEv2 através do peer. A separação da IKE agora se baseia no nível do perfil, não no nível da interface, o que é obtido através da nova CLI.

Outra atualização na nova versão do Cisco IOS é a adição da *chave* do *túnel*. Isso é necessário porque o DMVPN e o FlexVPN usam a mesma interface de origem e o mesmo endereço IP de destino. Com isso em vigor, não há como o túnel GRE saber qual interface de túnel é usada para desencapsular o tráfego. A chave de túnel permite diferenciar **tunnel0** e **tunnel1** com a adição de uma pequena sobrecarga (4 bytes). Uma chave diferente pode ser configurada em ambas as interfaces, mas você normalmente só precisa diferenciar um túnel.

> **Note**: A opção de proteção de túnel compartilhado não é necessária quando DMVPN e FlexVPN compartilham a mesma interface.

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

```
router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.101.0
passive-interface default
no passive-interface Tunnel0

router bgp 65001
bgp log-neighbor-changes
network 192.168.101.0
neighbor 10.1.1.1 remote-as 65001
```

Configuração do hub

Você deve fazer alterações semelhantes na configuração do lado do hub às descritas na seção **Configuração de Spoke**.

> **Note**: As alterações relevantes na configuração de ISAKMP e IKEV2 estão destacadas em negrito.

```
crypto ikev2 authorization policy default
pool FlexSpokes
route set interface

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 key cisco address 0.0.0.0


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 do hub, a associação entre o perfil IKE e o perfil IPsec ocorre no nível do perfil, ao contrário da configuração do spoke, onde isso é concluído através do comando **tunnel protection**. Ambas as abordagens são métodos viáveis para concluir esta ligação.

Éimportante observar que as IDs de rede do Next Hop Resolution Protocol (NHRP) são diferentes para DMVPN e 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 os túneis DMVPN e FlexVPN no nível de GRE para alcançar o mesmo objetivo mencionado na seção **Configuração de Spoke**.

A configuração de roteamento no hub é bastante básica. O dispositivo de hub mantém duas relações com qualquer spoke dado, uma que usa EIGRP e outra que usa BGP. A configuração do BGP usa o intervalo de escuta para evitar uma configuração longa por raio.

Os endereços de resumo são apresentados duas vezes. A configuração do EIGRP envia um resumo com o uso da configuração **tunnel0** (IP summary-address EIGRP 100), e o BGP introduz um resumo com o uso do aggregate-address. Os resumos são necessários para garantir que o redirecionamento de NHRP ocorra e para simplificar as atualizações de roteamento. Você pode enviar um redirecionamento de NHRP (como um redirecionamento de Internet Control Message Protocol (ICMP)) que indica se existe um salto melhor para um determinado destino, o que permite que um túnel spoke-to-spoke seja estabelecido. Esses resumos também são usados para minimizar a quantidade de atualizações de roteamento enviadas entre o hub e cada spoke, o que permite que as configurações sejam dimensionadas 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 deste exemplo de configuração é dividida em várias seções.

Verificações de pré-migração

Como tanto DMVPN/EIGRP quanto FlexVPN/BGP operam simultaneamente, você deve verificar se o spoke mantém uma relação sobre IPsec com IKEv1 e IKEv2, e se os prefixos apropriados são aprendidos sobre EIGRP e BGP.

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

Note: Duas SAs (Associações de Segurança IPsec) (uma entrada e uma saída) 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
```

Ao verificar os protocolos de roteamento, você deve verificar se uma vizinhança é formada e se os prefixos corretos são aprendidos. Isso é primeiro verificado com o EIGRP. Verifique se o hub está visível como um vizinho e se o endereço **192.168.0.0/16** (o resumo) é aprendido 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 FlexVPN do hub (10.1.1.1) é um vizinho através do qual o spoke recebe um prefixo (192.168.0.0/16). Além disso, o BGP informa ao administrador que ocorreu uma falha de Routing Information Base (RIB) para o prefixo 192.168.0.0/16. Essa falha ocorre porque há uma rota melhor para esse prefixo que já existe na tabela de roteamento. Essa rota é originada pelo EIGRP e pode ser confirmada se você verificar 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 se o IPsec e os protocolos de roteamento estão configurados e funcionam conforme esperado. Uma das maneiras mais fáceis de migrar de DMVPN para FlexVPN no mesmo dispositivo é alterar a distância administrativa (AD). Neste exemplo, o BGP interno (iBGP) tem um AD de 200, e o EIGRP tem um AD de 90.

Para que o tráfego flua pelo FlexVPN corretamente, o BGP deve ter um AD melhor. Neste exemplo, o AD do EIGRP é alterado para 230 e 240 para rotas internas e externas, respectivamente. Isso torna o BGP AD (de 200) mais preferível para o prefixo 192.168.0.0/16.

Outro método usado para alcançar isso é diminuir o AD BGP. No entanto, o protocolo executado após a migração tem valores não padrão, o que pode afetar outras partes da implantação.

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

> **Note**: Se as informações nesta seção forem usadas em uma rede de produção, evite o uso de comandos debug e confie nos comandos show listados na próxima seção. Além disso, o processo EIGRP de 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

*Oct 9 12:12:43.650: RT: add 192.168.0.0/16 via 10.1.1.1, bgp metric [200/0]
Spoke1#
*Oct 9 12:12:45.750: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is up: new adjacency
```

Há três ações importantes a serem observadas nesta saída:

- O spoke percebe que o AD mudou e desabilita a adjacência.
- Na tabela de roteamento, o prefixo do EIGRP é desativado e o BGP é apresentado.
- A adjacência ao hub através do EIGRP volta a estar online.

Quando você altera o AD em um dispositivo, ele afeta apenas o caminho do dispositivo para as outras redes; não afeta a forma como outros roteadores executam o roteamento. Por exemplo, depois que a distância EIGRP é aumentada em **Spoke1** (e usa FlexVPN na nuvem para rotear o tráfego), o hub mantém os ADs configurados (padrão). Isso significa que ele usa DMVPN para rotear o tráfego de volta para **Spoke1**.

Em determinados cenários, isso pode causar problemas, como quando os firewalls esperam tráfego de retorno na mesma interface. Portanto, você deve alterar o AD em todos os spokes antes de alterá-lo no hub. O tráfego é totalmente migrado pelo FlexVPN somente quando isso estiver concluído.

Migração do EIGRP para EIGRP

Uma migração de DMVPN para FlexVPN que executa somente o EIGRP não é discutida em profundidade neste documento; no entanto, é aqui mencionada para ser completa.

Épossível adicionar DMVPN e EIGRP à mesma instância de roteamento EIGRP Autonomous System (AS). Com isso em vigor, a adjacência de roteamento é estabelecida em ambos os tipos de nuvens. Isso pode fazer com que ocorra o balanceamento de carga, o que geralmente não é recomendado.

Para garantir que FlexVPN ou DMVPN seja escolhido, um administrador pode atribuir diferentes valores **de atraso** por interface. No entanto, é importante lembrar que nenhuma alteração é possível nas interfaces de modelo virtual enquanto as interfaces de acesso virtual correspondentes estão presentes.

Verificações pós-migração

Semelhante ao processo usado na seção **Verificações de Pré-Migração**, o IPsec e o protocolo de roteamento devem ser verificados.

Primeiro, 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 vistas, ambas com duas SAs IPsec ativas.

No spoke, a rota agregada (192.168.0.0/16) aponta do hub e é aprendida 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
```

Da mesma forma, a LAN de raio prefixada no hub deve ser conhecida através do EIGRP. Neste exemplo, a sub-rede de LAN 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 caminho de encaminhamento é atualizado corretamente e aponta para fora de uma interface de acesso virtual.

Considerações adicionais

Esta seção descreve algumas áreas adicionais importantes que são relevantes para este exemplo de configuração.

Túneis spoke-to-spoke existentes

Com uma migração do EIGRP para o BGP, os túneis spoke-to-spoke não são afetados, porque a comutação de atalhos ainda está em operação. A comutação de atalho no spoke insere uma rota NHRP mais específica com um AD de 250.

Aqui está um exemplo dessa 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
```

Comunicação entre spokes migrados e não migrados

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

Esse é o processo que ocorre:

1. O spoke executa uma pesquisa de rota para o destino, que aponta através de uma rota sumarizada anunciada pelo hub.
2. O pacote é enviado para o hub.
3. O hub recebe o pacote e executa uma pesquisa de rota para o destino, que aponta para outra interface que faz parte de um domínio NHRP diferente.

   Note: O ID da rede NHRP na configuração de hub anterior é diferente para FlexVPN e DMVPN.

Mesmo que as IDs de rede NHRP sejam unificadas, pode ocorrer um problema em que os objetos de rotas de spoke migradas pela rede FlexVPN. Isso inclui a diretiva usada para configurar a comutação de atalhos. O spoke não migrado tenta executar objetos na rede DMVPN, com um objetivo específico de executar a comutação de atalhos.

Troubleshoot

Esta seção descreve as duas categorias tipicamente usadas para solucionar problemas da migração.

Problemas com tentativas de estabelecer túneis

Conclua estes passos se a negociação IKE falhar:

1. Verifique o estado atual com estes comandos:

   show crypto isakmp sa - Este comando revela a quantidade, a origem e o destino de uma

sessão IKEv1.**show crypto ipsec sa** - Este comando revela a atividade de SAs IPsec.**Note**: Ao contrário do IKEv1, nesta saída o valor do grupo Diffie-Hellman (DH) do Perfect Forward Secsecret (PFS) aparece como **PFS (Y/N): N, grupo DH: nenhuma** durante a primeira negociação de túnel; no entanto, depois que uma chave de rechaveamento ocorre, os valores corretos são exibidos. Isso não é um bug, mesmo que o comportamento seja descrito em CSCug67056. A diferença entre IKEv1 e IKEv2 é que neste último caso, as SAs filho são criadas como parte da troca **AUTH**. O Grupo DH configurado no mapa de criptografia é usado somente durante uma chave de rechaveamento. Por esta razão, você vê **PFS (S/N): N, grupo DH: nenhuma até a primeira chave.** Com o IKEv1, você vê um comportamento diferente porque a criação do SA filho ocorre durante o Modo Rápido, e a mensagem **CREATE_CHILD_SA** tem provisões para a transferência do payload do Key Exchange que especifica os parâmetros DH para derivar um novo segredo compartilhado.**show crypto ikev2 sa** - Este comando fornece uma saída semelhante a ISAKMP, mas é específico para IKEv2.**show crypto session** - Este comando fornece a saída de resumo das sessões criptográficas neste dispositivo.**show crypto socket** - Este comando mostra o status de crypto-sockets.**show crypto map** - Este comando mostra o mapeamento dos perfis IKE e IPsec para as interfaces.**show ip nhrp** - Este comando fornece as informações de NHRP do dispositivo. Isso é útil para conexões spoke-to-spoke em configurações de FlexVPN e para conexões spoke-to-spoke e spoke-to-hub em configurações de DMVPN.

2. Use estes comandos para depurar o estabelecimento do túnel:

   debug crypto ikev2debug crypto isakmpdebug crypto ipsecdebug crypto kmi

Problemas com Propagação de Rota

Aqui estão alguns comandos úteis que você pode usar para solucionar problemas do EIGRP e da topologia:

- **show bgp summary** - Use este comando para verificar os vizinhos conectados e seus estados.
- **show ip eigrp neighbor** - Use este comando para mostrar os vizinhos conectados via EIGRP.
- **show bgp** - Use este comando para verificar os prefixos aprendidos sobre o BGP.
- **show ip eigrp topology** - Use este comando para mostrar os prefixos aprendidos via EIGRP.

Éimportante saber que um prefixo aprendido é diferente de um prefixo instalado na tabela de roteamento. Para obter mais informações sobre isso, consulte o artigo Seleção de rota nos Cisco Routers Cisco ou o manual Routing TCP/IP Cisco Press.

Caveats conhecidos

Uma limitação de que o tratamento de túnel GRE paralela existe no ASR1K. Isso é controlado na ID de bug da Cisco CSCue00443. No momento, a limitação tem uma correção programada no Cisco IOS XE Software Release 3.12.

Monitore esse bug se desejar uma notificação assim que a correção estiver disponível.