Migração de FlexVPN: Movimento duro do DMVPN a FlexVPN em um hub diferente

Índice

Introdução

Este documento fornece a informação sobre como migrar de uma rede do Dynamic Multipoint VPN (DMVPN) que exista atualmente a FlexVPN em dispositivos diferentes do hub. Os configuations para ambas as estruturas coexistem nos dispositivos. Neste documento, somente a maioria de cenário comum é mostrado - DMVPN com o uso da chave preshared para a autenticação e do Enhanced Interior Gateway Routing Protocol (EIGRP) como o protocolo de roteamento. Neste documento, a migração ao Border Gateway Protocol (BGP), que é o protocolo de roteamento recomendado, e o EIGRP menos-desejável são demonstrados.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento básico destes assuntos:

- DMVPN
- FlexVPN

Componentes Utilizados

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

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

- Versão 15.2(4)M1 mais recente do roteador do serviço integrado de Cisco (ISR)
- Liberação 3.6.2 15.2(2)S2 do 1000 Series do roteador dos serviços da agregação de Cisco (ASR1K) ou mais novo

Um as vantagens de uma plataforma e de um software mais novos é a capacidade para usar a criptografia da próxima geração, tal como o Advanced Encryption Standard (AES) Galois/modo contrário (GCM) para a criptografia na segurança de protocolo do Internet (IPsec), como discutido na solicitação para comentários (RFC) 4106. O AES GCM permite que você alcance uma velocidade muito mais rápida da criptografia em algum hardware. A fim ver recomendações da Cisco no uso de e na migração à criptografia da próxima geração, refira o artigo da criptografia da próxima geração.

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.

Procedimento de Migração

Atualmente, o método recomendada a migrar do DMVPN a FlexVPN é para que as duas

estruturas não se operem ao mesmo tempo. Esta limitação é programada para ser removido devido às características novas da migração ser introduzido na liberação ASR 3.10, seguida sob as requisições de aprimoramento do multilple no lado de Cisco, que incluem a identificação de bug Cisco CSCuc08066. Aquelas características devem ser ao fim de junho 2013 disponíveis.

Uma migração onde ambas as estruturas coexistam e se operem ao mesmo tempo nos mesmos dispositivos é referida como uma **migração do delicado**, que indique o impacto mínimo e o Failover liso de uma estrutura a outra. Uma migração onde as configurações para ambas as estruturas coexistam, mas não se opera ao mesmo tempo é referida como uma **migração dura**. Isto indica que um switchover de uma estrutura a outra significa uma falta de uma comunicação sobre o VPN, mesmo se mínimo.

Migração dura entre dois Hubs diferentes

Neste documento, a migração do hub DMVPN que é usado atualmente a um hub novo de FlexVPN é discutida. Esta migração permite a intercomunicação entre o spokes migrada já a FlexVPN, e aquelas que ainda são executado no DMVPN e podem ser executadas em fases múltiplas, no cada falaram separadamente.

Contanto que a informação de roteamento é povoada corretamente, uma comunicação entre o spokes migrado e nonmigrated deve permanecer possível. Contudo, a latência adicional pode ser observada porque migrado e o spokes nonmigrated não constrói túneis spoke-to-spoke entre se. Ao mesmo tempo, o spokes migrado deve poder estabelecer túneis spoke-to-spoke diretos entre se. O mesmo aplica-se ao spokes nonmigrated.

Até que esta característica nova da migração esteja disponível, termine estas etapas a fim executar migrações com um hub diferente do DMVPN e do FlexVPN:

1. Verifique a Conectividade sobre o DMVPN.
2. Adicionar a configuração de FlexVPN, e feche o túnel que pertence à configuração nova.
3. (Durante uma janela de manutenção) em cada spoke, um por um, feche o túnel DMVPN.
4. No mesmo spoke que em etapa 3, unshut as interfaces de túnel de FlexVPN.
5. Verifique a Conectividade spoke-to-hub.
6. Verifique a Conectividade spoke-to-spoke dentro de FlexVPN.
7. Verifique a Conectividade spoke-to-spoke com o DMVPN de FlexVPN.
8. Repita etapas 3 com 7 para o cada falou separadamente.
9. Se você encontra quaisquer problemas com as verificações descritas nas etapas 5, 6, ou 7, feche a relação de FlexVPN, e o unshut as relações DMVPN a fim reverter ao DMVPN.
10. Verifique uma comunicação spoke-to-hub sobre o DMVPN suportado.
11. Verifique uma comunicação spoke-to-spoke sobre o DMVPN suportado.

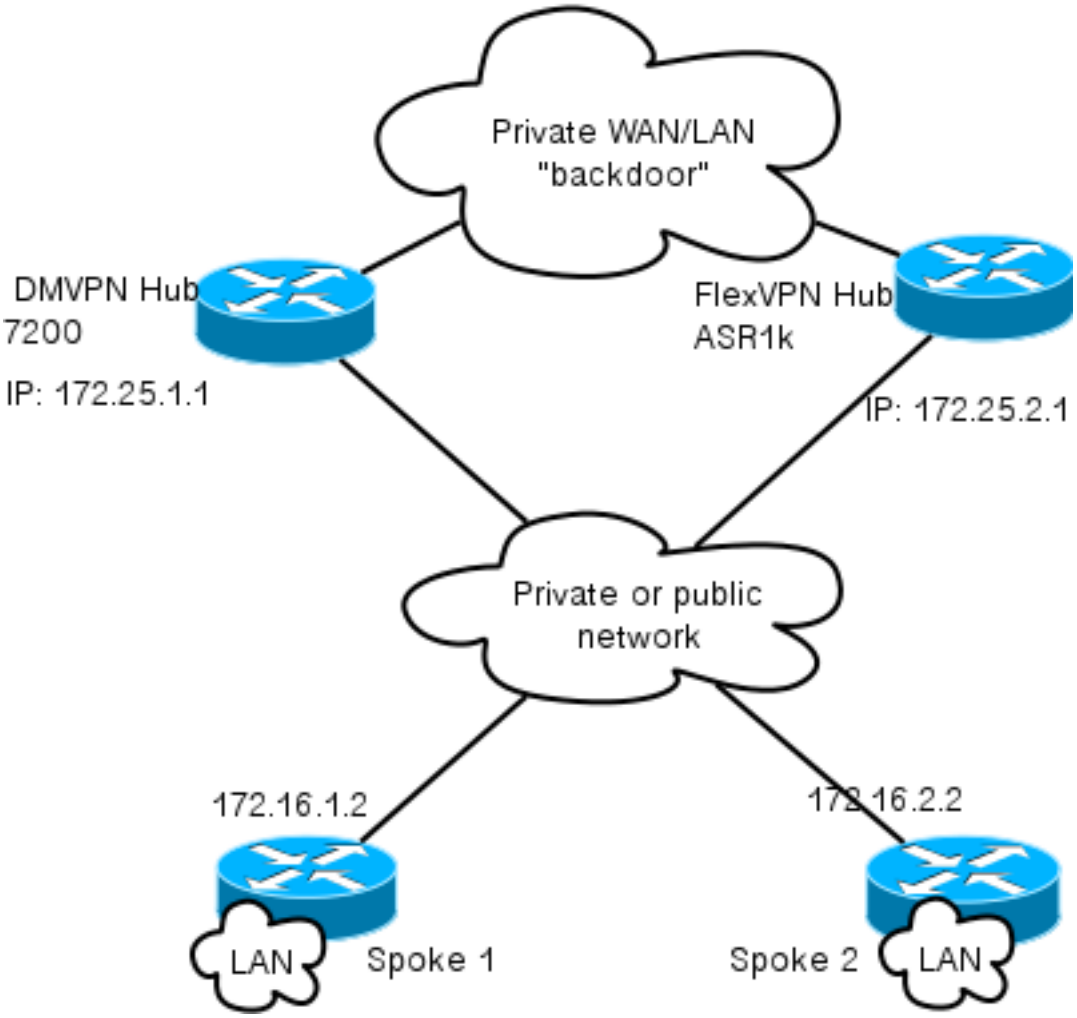
Aproximação feita sob encomenda

Se a aproximação precedente não pôde ser a melhor solução para você devido a suas complexidades da rede ou do roteamento, comece uma discussão com seu representante do Cisco antes que você migre. A melhor pessoa com que discutir um processo de migração feito sob encomenda é seu engenheiro de sistema ou coordenador dos Serviços avançados.

Topologia de rede

Topologia de rede de transporte

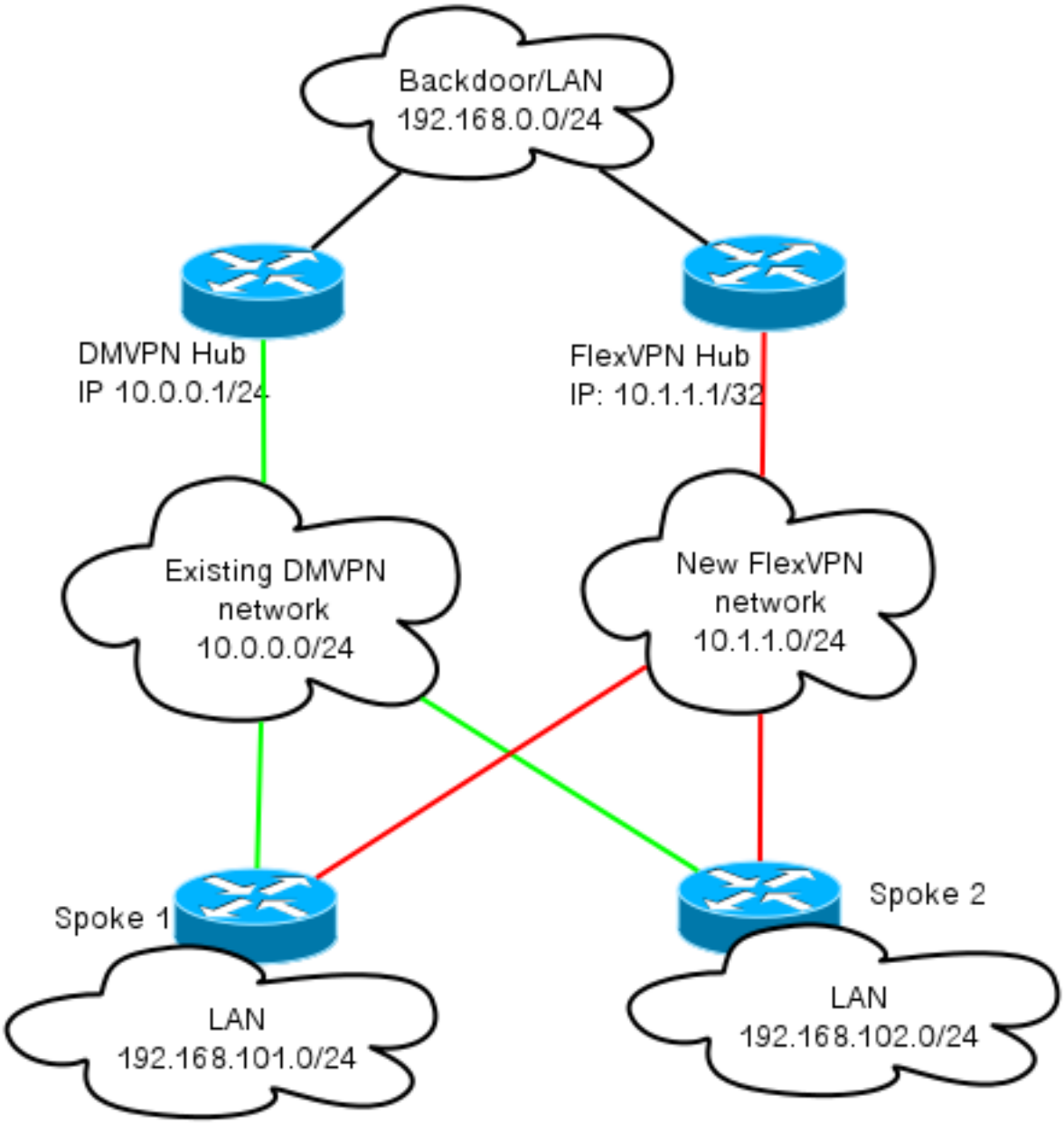
Este diagrama mostra a Topologia da conexão típica dos anfitriões no Internet. O endereço IP de Um ou Mais Servidores Cisco ICM NT do hub de **loopback0** (**172.25.1.1**) é usado a fim terminar a sessão IPSec DMVPN. O endereço IP de Um ou Mais Servidores Cisco ICM NT no hub novo (**172.25.2.1**) é usado para FlexVPN.



Observe o link entre os dois Hubs. Este link é crucial a fim permitir a Conectividade entre o FlexVPN e nuvens DMVPN durante a migração. Permite o spokes já migrado a FlexVPN para comunicar-se e vice-versa com as redes de DMVPN.

Topologia de rede da folha de prova

Este diagrama de topologia mostra duas nuvens separadas usadas para a folha de prova: DMVPN (conexões verdes) e FlexVPN (conexões vermelhas). Os prefixos LAN são mostrados para locais correspondentes. A sub-rede **10.1.1.0/24** não representa sub-rede real em termos do endereçamento da relação, mas representa um pedaço do espaço IP dedicado à nuvem de FlexVPN. A base racional atrás desta é discutida mais tarde na **seção de configuração de FlexVPN**.



Configuração

Esta seção descreve o DMVPN e as configurações de FlexVPN.

Configuração DMVPN

Esta seção descreve a configuração básica para o hub and spoke DMVPN.

A chave pré-compartilhada (PSK) é usada para a autenticação IKEv1. Uma vez que o IPsec é estabelecido, o registro do Next Hop Resolution Protocol (NHRP) de spoke-to-hub está executado de modo que o hub possa aprender o multiacesso sem broadcast dos raios (NBMA) que endereça dinamicamente.

Quando o NHRP executa o registro no spoke e no hub, distribuir o adjacancy pode estabelecer, e as rotas podem ser trocadas. Neste exemplo, o EIGRP é usado como um protocolo de roteamento básico para a rede de folha de prova.

Configuração do spoke DMVPN

Aqui você pode encontrar uma configuração do exemplo básico do DMVPN com autenticação PSK e do EIGRP como o protocolo de roteamento.

```
crypto isakmp policy 10
 encr aes
 authentication pre-share

crypto isakmp key cisco address 0.0.0.0

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

interface Tunnel0

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 protection ipsec profile DMVPN_IKEv1

router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.102.0
passive-interface default
no passive-interface Tunnel0
```

Configuração do hub DMVPN

Na configuração do hub, o túnel é originado de **loopback0** com um endereço IP de Um ou Mais Servidores Cisco ICM NT de **172.25.1.1**. O resto é um desenvolvimento padrão de um hub DMVPN com o EIGRP como o protocolo de roteamento.

```
crypto isakmp policy 10
encr aes
authentication pre-share

crypto isakmp key cisco 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

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 protection ipsec profile DMVPN_IKEv1

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
```

Configuração de FlexVPN

FlexVPN é baseado nestas mesmas Tecnologias fundamentais:

- **IPsec**: Ao contrário do padrão no DMVPN, IKEv2 é usado em vez de IKEv1 a fim negociar as associações de segurança IPSec (SA). IKEv2 oferece melhorias sobre IKEv1, tal como a elasticidade e o número de mensagens que são precisadas a fim estabelecer um canal de dados protegidos.

- **GRE**: Ao contrário do DMVPN, as interfaces Point-to-Point estáticas e dinâmicas são usadas, e não somente uma relação estática do multpoint GRE. Esta configuração permite a flexibilidade adicionada, especialmente para o por-spoke/comportamento do por-hub.

- **NHRP**: Em FlexVPN, o NHRP é usado primeiramente a fim estabelecer uma comunicação spoke-to-spoke. O spokes não se registra ao hub.

- **Distribuição**: Porque o spokes não executa o registro NHRP ao hub, você deve confiar em outros mecanismos a fim certificar-se que o hub e o spokes podem se comunicar bidirecional. Simliar ao DMVPN, protocolos de roteamento dinâmico pode ser usado. Contudo, FlexVPN permite que você use o IPsec a fim introduzir a informação de roteamento. O padrão é introduzir como a rota de **/32** para o endereço IP de Um ou Mais Servidores Cisco ICM NT no outro lado do túnel, que permite uma comunicação direta spoke-to-hub.

Em uma migração dura do DMVPN a FlexVPN, os dois framemworks não trabalham ao mesmo tempo nos mesmos dispositivos. Contudo, recomenda-se mantê-los separados.

Separe-os em diversos níveis:

- NHRP - Use uma rede NHRP diferente ID (recomendada).
- Distribuir - Use os processos de roteamento separados (recomendados).
- Roteamento virtual e transmissão (VRF) - A separação VRF permite a flexibilidade adicionada

mas não é discutida aqui (opcional).

Configuração de FlexVPN do spoke

Uma das diferenças na configuração de raio em FlexVPN em relação ao DMVPN é que você tem potencialmente duas relações. Há um túnel exigido para uma comunicação spoke-to-hub e um túnel opcional para túneis spoke-to-spoke. Se você escolhe não ter o Tunelamento spoke-to-spoke dinâmico e preferiria que tudo atravessa o dispositivo do hub, você pode remover a relação virtual do molde, e remove o interruptor do atalho NHRP da interface de túnel.

Observe que a interface de túnel estática recebe um endereço IP de Um ou Mais Servidores Cisco ICM NT baseado na negociação. Isto permite que o hub forneça o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de túnel ao spoke dinamicamente sem a necessidade de criar o endereçamento estático na nuvem de FlexVPN.

```
aaa new-model
aaa authorization network default local
aaa session-id common

crypto ikev2 profile Flex_IKEv2
match identity remote fqdn domain cisco.com
local identity fqdn spoke.cisco.com
authentication remote rsa-sig
authentication local rsa-sig
aaa authorization group cert list default default
virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

> Nota: À revelia, a identidade local é ajustada a fim usar o endereço IP de Um ou Mais Servidores Cisco ICM NT. Assim a instrução compatível correspondente no par deve combinar baseado no endereço também. Se a exigência é combinar baseado no nome destacado (DN) no certifcate, a seguir o fósforo deve ser feito com o uso de um mapa do certificado.

Cisco recomenda que você usa AES GCM com hardware que o apoia.

```
crypto ipsec transform-set IKEv2 esp-gcm
mode transport

crypto ipsec profile default
set ikev2-profile Flex_IKEv2
! set transform-set IKEv2

interface Tunnel1
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
shutdown
tunnel source Ethernet0/0
tunnel destination 172.25.2.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default

interface Virtual-Template1 type tunnel
ip unnumbered Tunnel1
```

```
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

O Public Key Infrastructure (PKI) é o método recomendada para executar a autenticação da larga escala em IKEv2. Contudo, você pode ainda usar o PSK enquanto você está ciente de suas limitações.

Está aqui um exemplo de configuração que use **Cisco** como o PSK.

```
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
```

Configuração do hub de FlexVPN

Tipicamente, um hub termina somente túneis spoke-to-hub dinâmicos. Eis porque você não encontra uma interface de túnel estática para FlexVPN na configuração do hub. Em lugar de, uma relação virtual do molde é usada.

> Nota: No lado de hub, você deve indicar os endereços do conjunto a ser atribuídos ao spokes.

Os endereços deste pool são adicionados mais tarde na tabela de roteamento como rotas de **/32** para cada spoke.

```
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
```

Cisco recomenda que você usa AES GCM com hardware que o apoia.

```
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
```

Nota: Nesta configuração, a operação AES GCM foi comentada para fora.

```
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
```

Com autenticação em IKEv2, o mesmo princípio aplica-se no hub como no spoke. Para a escalabilidade e a flexibilidade, use Certificados. Contudo, você pode reutilizar a mesma configuração para o PSK como no spoke.

Nota: IKEv2 oferece a flexibilidade em termos da autenticação. Um lado pode autenticar com PSK quando o outro lado usar a assinatura de Rivest-Shamir-Adleman (RSA-SIG).

Se a exigência é usar chaves preshared para a autenticação, a seguir as alterações de configuração são similares àquelas descritas para o roteador do spoke aqui.

Conexão BGP do Inter-hub

Certifique-se de que o Hubs sabe onde os prefixos particulares são encontrados. Isto torna-se cada vez mais importante porque algum spokes esteve migrado a FlexVPN quando algum outro spokes permanecer no DMVPN.

Está aqui a conexão BGP do inter-hub baseada na configuração do hub DMVPN:

```
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
```

Migração do tráfego

Migre ao BGP como o [Recommended] do protocolo de roteamento da folha de prova

O BGP é um protocolo de roteamento que seja baseado na troca do unicast. Devido a suas características, é o melhor protocolo da escamação nas redes de DMVPN.

Neste exemplo, o Internal BGP (iBGP) é usado.

Configuração de BGP do spoke

A migração do spoke consiste em duas porções. Primeiramente, permita o BGP como o roteamento dinâmico:

```
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
```

Depois que o vizinho de BGP vem acima (vê a próxima seção) e os prefixos novos sobre o BGP são instruídos, você pode balançar o tráfego da nuvem atual DMVPN a uma nuvem nova de FlexVPN.

Configuração de BGP do hub

Hub de FlexVPN - Configuração de BGP completa

No hub, a fim evitar manter a configuração do neighborship para o cada falou separadamente, configura ouvintes dinâmicos. Nesta instalação, o BGP não inicia novas conexões, mas aceita conexões do pool fornecido dos endereços IP de Um ou Mais Servidores Cisco ICM NT. Neste caso, o pool dito é 10.1.1.0/24, que é todos os endereços na nuvem nova de FlexVPN.

Dois pontos a notar:

- O hub de FlexVPN anuncia prefixos específicos ao hub DMVPN; assim o mapa dos unsupress está sendo usado.

- Anuncie a sub-rede de FlexVPN de 10.1.1.0/24 à tabela de roteamento, ou certifique-se de que o hub DMVPN vê o hub de FlexVPN como o salto seguinte.

Este documento mostra a última abordagem.

```
access-list 1 permit any
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

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

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

Hub DMVPN - BGP completo e configuração de EIGRP

A configuração no hub DMVPN é básica, porque recebe somente prefixos específicos do hub de FlexVPN e anuncia prefixos que aprende do EIGRP.

```
access-list 1 permit any
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

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

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

Migre o tráfego a BGP/FlexVPN

Como discutido antes, você deve fechar a funcionalidade DMVPN e trazer FlexVPN acima a fim executar a migração.

Este procedimento garante o impacto mínimo:

1. Em cada spoke, separadamente, entre nisto:
   `access-list 1 permit any`

```
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

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

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

Neste momento, certifique-se que não há nenhuma sessão IKEv1 estabelecida a este spoke. Isto pode ser verificado se você verifica a saída dos mensagens do syslog do comando show crypto isakmp sa e do monitor gerados pelo comando session de registro cripto. Uma vez que isto é confirmado, você pode continuar trazer acima FlexVPN.

2. No mesmo spoke, entre nisto:

```
access-list 1 permit any
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

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

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

Etapas de verificação

Estabilidade do IPsec

A melhor maneira de avaliar a estabilidade do IPsec é monitorar sylogs com o comando enabled de registro cripto da configuração de sessão. Se você vê as sessões que vá para cima e para baixo, isto pode indicar um problema no nível IKEv2/FlexVPN que deve ser corrigido antes que a migração possa começar.

Informação de BGP povoada

Se o IPsec é estável, certifique-se de que a tabela de BGP está povoada com entradas do spokes (no hub) e sumário do hub (no spokes). No caso do BGP, isto pode ser visto com estes comandos:

```
access-list 1 permit any
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

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

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

Está aqui um exemplo da informação correta do hub de FlexVPN:

```
BGP router identifier 172.25.2.1, local AS number 65001
(...omitted...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
*10.1.1.100 4 65001 112 123 16 0 0 01:35:58 1
192.168.0.1 4 65001 97 99 16 0 0 01:24:12 4
```

A saída mostra que o hub aprendeu um prefixo de cada um do spokes, e ambo o spokes é dinâmico e marcado com um sinal do asterisco (*). Igualmente mostra que um total de quatro prefixos da conexão do inter-hub está recebido.

Está aqui um exemplo da informação similar do spoke:

```
show ip bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
(...omitted...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 120 109 57 0 0 01:33:23 2
```

O spoke recebeu dois prefixos do hub. No caso desta instalação, um prefixo deve ser o sumário anunciado no hub de FlexVPN. A outro é rede DMVPN **10.0.0.0/24** redistribuída no spoke DMVPN no BGP.

Migre aos túneis novos com EIGRP

O EIGRP é uma escolha popular nas redes de DMVPN devido a seus desenvolvimento e convergência rápida relativamente simples. Contudo, escala mais ruim do que o BGP, e não oferece muitos mecanismos avançados que podem ser usados pelo BGP em linha reta fora da caixa. A próxima seção descreve uma das maneiras de mover-se para FlexVPN com um processo de EIGRP novo.

Configuração de raio actualizado

Um sistema autônomo novo é adicionado com um processo de EIGRP separado:

```
show ip bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
(...omitted...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 120 109 57 0 0 01:33:23 2
```

Nota: É o melhor não estabelecer a adjacência do protocolo de roteamento sobre túneis spoke-to-spoke. Consequentemente, faça somente a relação de **tunnel1** não passiva (spoke-to-hub).

Configuração actualizado do hub de FlexVPN

Similarmente, para o hub de FlexVPN, prepare o protocolo de roteamento no appopriate COMO, combinando um configurado no spokes.

```
show ip bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
(...omitted...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 120 109 57 0 0 01:33:23 2
```

Há dois métodos que são usados a fim fornecer a parte traseira do sumário para o spoke.

- Redistribua uma rota estática que aponte ao **null0** (opção preferida).

  ```
  show ip bgp summary
  BGP router identifier 192.168.101.1, local AS number 65001
  (...omitted...)

  Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
  10.1.1.1 4 65001 120 109 57 0 0 01:33:23 2
  ```

  Esta opção permite o controle sobre o sumário e a redistribução sem alterações à configuração da tecnologia da virtualização do hub (VT). Isto é importante, porque a configuração VT do hub não pode ser alterada se há um acesso virtual ativo associado com ele.

- Estabelecer um endereço sumário do DMVPN-estilo em um molde virtual.

  Esta configuração *não é recomendada*, devido ao processamento interno e à replicação de sumário dito a cada acesso virtual. Mostra-se aqui para a referência.

  ```
  interface Virtual-Template1 type tunnel
   ip summary-address eigrp 200 192.168.0.0 255.255.0.0
  ```

  Um outro aspecto a esclarecer é o intercâmbio de roteamento do inter-hub. Isto pode ser feito se você redistribui exemplos EIGRP ao iBGP.

Hub DMVPN - Configuração de BGP actualizado

A configuração permanece básica. Você deve redistribuir prefixos específicos do EIGRP ao BGP:

```
interface Virtual-Template1 type tunnel
```

```
 ip summary-address eigrp 200 192.168.0.0 255.255.0.0
```

Hub de FlexVPN - Configuração de BGP actualizado

Similar ao hub DMVPN, em FlexVPN, você deve redistribuir os prefixos dos processos de EIGRP novos ao BGP:

```
interface Virtual-Template1 type tunnel
 ip summary-address eigrp 200 192.168.0.0 255.255.0.0
```

Migre o tráfego a FlexVPN

Você deve fechar a funcionalidade DMVPN e trazer FlexVPN acima em cada spoke, um de cada vez, a fim executar a migração. Este procedimento garante o impacto mínimo:

1. Em cada spoke, separadamente, entre nisto:
   ```
   interface Virtual-Template1 type tunnel
    ip summary-address eigrp 200 192.168.0.0 255.255.0.0
   ```
   Neste momento, certifique-se que não há nenhuma sessão IKEv1 estabelecida neste spoke. Isto pode ser verificado se você verifica a saída dos mensagens do syslog do **comando show crypto isakmp sa** e do monitor gerados pelo **comando session de registro cripto**. Uma vez que isto é confirmado, você pode continuar trazer acima FlexVPN.
2. No mesmo spoke, entre nisto:
   ```
   interface Virtual-Template1 type tunnel
    ip summary-address eigrp 200 192.168.0.0 255.255.0.0
   ```

Etapas de verificação

Estabilidade do IPsec

Como no caso do BGP, você deve avaliar se o IPsec é estável. A melhor maneira de fazer assim é monitorar sylogs com o comando enabled de **registro cripto da configuração de sessão**. Se você vê sessões ir para cima e para baixo, este pode indicar um problema no nível IKEv2/FlexVPN que deve ser corrigido antes que a migração possa começar.

Informação de EIGRP na tabela de topologia

Certifique-se de que sua tabela de topologia de EIGRP está povoada com entradas do spoke LAN no hub e no sumário no spokes. Isto pode ser verificado se você incorpora este comando nos hub e nos spoke:

```
show ip eigrp [AS_NUMBER] topology
```

Está aqui um exemplo de saída do spoke:

```
Spoke1#show ip eigrp 200 topology
EIGRP-IPv4 Topology Table for AS(200)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 26112000
via Rstatic (26112000/0)
```

```
via 10.1.1.1 (26240000/128256), Tunnel1

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 26114560
via 10.1.1.1 (26114560/2562560), Tunnel1

P 10.1.1.100/32, 1 successors, FD is 26112000
via Connected, Tunnel1

P 10.1.1.0/24, 1 successors, FD is 26114560
via 10.1.1.1 (26114560/2562560), Tunnel1
```

A saída mostra que o spoke sabe sobre sua sub-rede de LAN (no *itálico*) e os sumários para aqueles (em **corajoso**).

Está aqui um exemplo de saída do hub:

```
hub2# show ip eigrp 200 topology
EIGRP-IPv4 Topology Table for AS(200)/ID(172.25.2.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 128256
via Connected, Loopback200

P 192.168.101.0/24, 1 successors, FD is 26905600
via 10.1.1.100 (26905600/281600), Virtual-Access1

P 192.168.0.0/16, 1 successors, FD is 2562560
via Rstatic (2562560/0)

P 10.1.1.0/24, 1 successors, FD is 2562560
via Rstatic (2562560/0)
```

A saída mostra que o hub sabe sobre as sub-redes de LAN dos raios (no *itálico*), o prefixo que sumário anuncia (em **corajoso**), e o endereço IP atribuído de cada raio através da negociação.

Considerações adicionais

Túneis spoke-to-spoke que já existem

Porque uma parada programada da interface de túnel DMVPN faz com que as entradas NHRP sejam removidas, os túneis spoke-to-spoke que já existem serão rasgados para baixo.

Cancele entradas NHRP

Um hub de FlexVPN não confia no processo de registro NHRP do spoke a fim saber distribuir a parte traseira do tráfego. Contudo, os túneis spoke-to-spoke dinâmicos confiam em entradas NHRP.

No DMVPN, se o NHRP no hub é cancelado, pode conduzir aos breves problemas de conectividade. Em FlexVPN, o NHRP de cancelamento no spokes causará a sessão IPSec de FlexVPN, relativa aos túneis spoke-to-spoke, para ser rasgado para baixo. Cancelar o NHRP no

hub não tem nenhum efeito na sessão de FlexVPN.

Isto é porque, em FlexVPN à revelia:

- O spokes não se registra ao Hubs.
- O Hubs funciona somente como redirecionadores NHRP, e não instala entradas NHRP.
- As entradas do atalho NHRP são instaladas no spokes para túneis spoke-to-spoke e são dinâmicas.

Caveats conhecidos

O tráfego spoke-to-spoke pôde ser afetado pela identificação de bug Cisco CSCub07382.

Informações Relacionadas

- DMVPN ao exemplo de configuração macio da migração de FlexVPN
- Suporte Técnico e Documentação - Cisco Systems