Transferência forçada de migração de DMVPN para FlexVPN em um hub diferente

Contents

Introduction
Prerequisites
Requirements
Componentes Utilizados
Procedimento de Migração
Migração Forçada Entre Dois Hubs Diferentes
Abordagem personalizada
Topologia de rede
Topologia da rede de transporte
Topologia de sobreposição de rede
Configuração
Configuração de DMVPN
Configuração de Spoke DMVPN
Configuração de DMVPN de hub
Configuração FlexVPN
Configuração de Spoke FlexVPN
Configuração do Hub FlexVPN
Migração de tráfego
Migre para BGP como o protocolo de roteamento de sobreposição [recomendado]
Configuração de Spoke BGP
Configuração do BGP do hub
Migrar tráfego para BGP/FlexVPN
Migre para novos túneis com EIGRP
Configuração de spoke atualizada
Configuração atualizada do hub FlexVPN
Hub DMVPN - Configuração BGP atualizada
Hub FlexVPN - Configuração BGP atualizada
Migre o tráfego para FlexVPN
Etapas de verificação
Considerações adicionais
Túneis spoke-to-spoke que já existem
Limpar entradas NHRP
Caveats conhecidos
Informações Relacionadas

Introduction

Este documento fornece informações sobre como migrar de uma rede VPN multiponto dinâmica (DMVPN) que existe atualmente para FlexVPN em diferentes dispositivos de hub. As configurações para ambas as estruturas coexistem nos dispositivos. Neste documento, somente o cenário mais comum é mostrado - DMVPN com o uso da chave pré-compartilhada para autenticação e Enhanced Interior Gateway Routing Protocol (EIGRP) como o protocolo de roteamento. Neste documento, é demonstrada a migração para o Border Gateway Protocol (BGP), que é o protocolo de roteamento recomendado, e o EIGRP menos desejável.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico sobre estes tópicos:

- DMVPN
- FlexVPN

Componentes Utilizados

> **Note**: Nem todos os softwares e hardwares oferecem suporte ao Internet Key Exchange versão 2 (IKEv2). Consulte o Cisco Feature Navigator para obter mais informações.

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

- Cisco Integrated Service Router (ISR) versão 15.2(4)M1 ou mais recente
- Cisco Aggregation Services Router 1000 Series (ASR1K) 3.6.2 Versão 15.2(2)S2 ou mais recente

Uma das vantagens de uma plataforma e software mais novos é a capacidade de usar a Criptografia de última geração, como o Modo Galois/Contador de AES (Advanced Encryption Standard) para criptografia no IPsec (Internet Protocol Security), conforme discutido na RFC 4106. O AES GCM permite alcançar uma velocidade de criptografia muito mais rápida em algum hardware. Para ver as recomendações da Cisco sobre o uso e a migração para a criptografia de próxima geração, consulte o artigo Criptografia de próxima geração.

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.

Procedimento de Migração

Atualmente, o método recomendado para migrar de DMVPN para FlexVPN é que as duas estruturas não operem ao mesmo tempo. Essa limitação está programada para ser removida devido aos novos recursos de migração a serem introduzidos no ASR 3.10 Release, rastreados

sob várias solicitações de aprimoramento no lado da Cisco, que incluem o bug da Cisco ID CSCuc08066. Esses recursos devem estar disponíveis no final de junho de 2013.

Uma migração em que ambas as estruturas coexistem e operam ao mesmo tempo nos mesmos dispositivos é chamada de **migração suave**, que indica o impacto mínimo e o failover tranquilo de uma estrutura para outra. Uma migração em que as configurações para ambas as estruturas coexistem, mas não operam ao mesmo tempo, é chamada de **migração difícil**. Isso indica que um switchover de uma estrutura para outra significa uma falta de comunicação sobre a VPN, mesmo que mínima.

Migração Forçada Entre Dois Hubs Diferentes

Neste documento, a migração do hub DMVPN usado atualmente para um novo hub FlexVPN é discutida. Essa migração permite a intercomunicação entre spokes migrados já para FlexVPN e aqueles que ainda são executados em DMVPN e podem ser executados em várias fases, em cada spoke separadamente.

Desde que as informações de roteamento sejam preenchidas corretamente, a comunicação entre spokes migrados e não migrados deve permanecer possível. No entanto, pode-se observar latência adicional porque os spokes migrados e não migrados não criam túneis spoke-to-spoke entre si. Ao mesmo tempo, os spokes migrados devem ser capazes de estabelecer túneis spoke-to-spoke diretos entre si. O mesmo se aplica a spokes não migrados.

Até que esse novo recurso de migração esteja disponível, faça o seguinte para executar migrações com um hub diferente de DMVPN e FlexVPN:

1. Verifique a conectividade via DMVPN.
2. Adicione a configuração FlexVPN e desligue o túnel que pertence à nova configuração.
3. (Durante uma janela de manutenção) Em cada spoke, um por um, desligue o túnel DMVPN.
4. No mesmo spoke da Etapa 3, desligue as interfaces de túnel FlexVPN.
5. Verifique a conectividade spoke-to-hub.
6. Verifique a conectividade spoke-to-spoke em FlexVPN.
7. Verifique a conectividade spoke-to-spoke com DMVPN do FlexVPN.
8. Repita as Etapas 3 a 7 para cada spoke separadamente.
9. Se você encontrar algum problema com as verificações descritas nas Etapas 5, 6 ou 7, desligue a interface FlexVPN e desligue as interfaces DMVPN para reverter para DMVPN.
10. Verifique a comunicação spoke-to-hub através do DMVPN com backup.
11. Verifique a comunicação spoke-to-spoke sobre o DMVPN de backup.

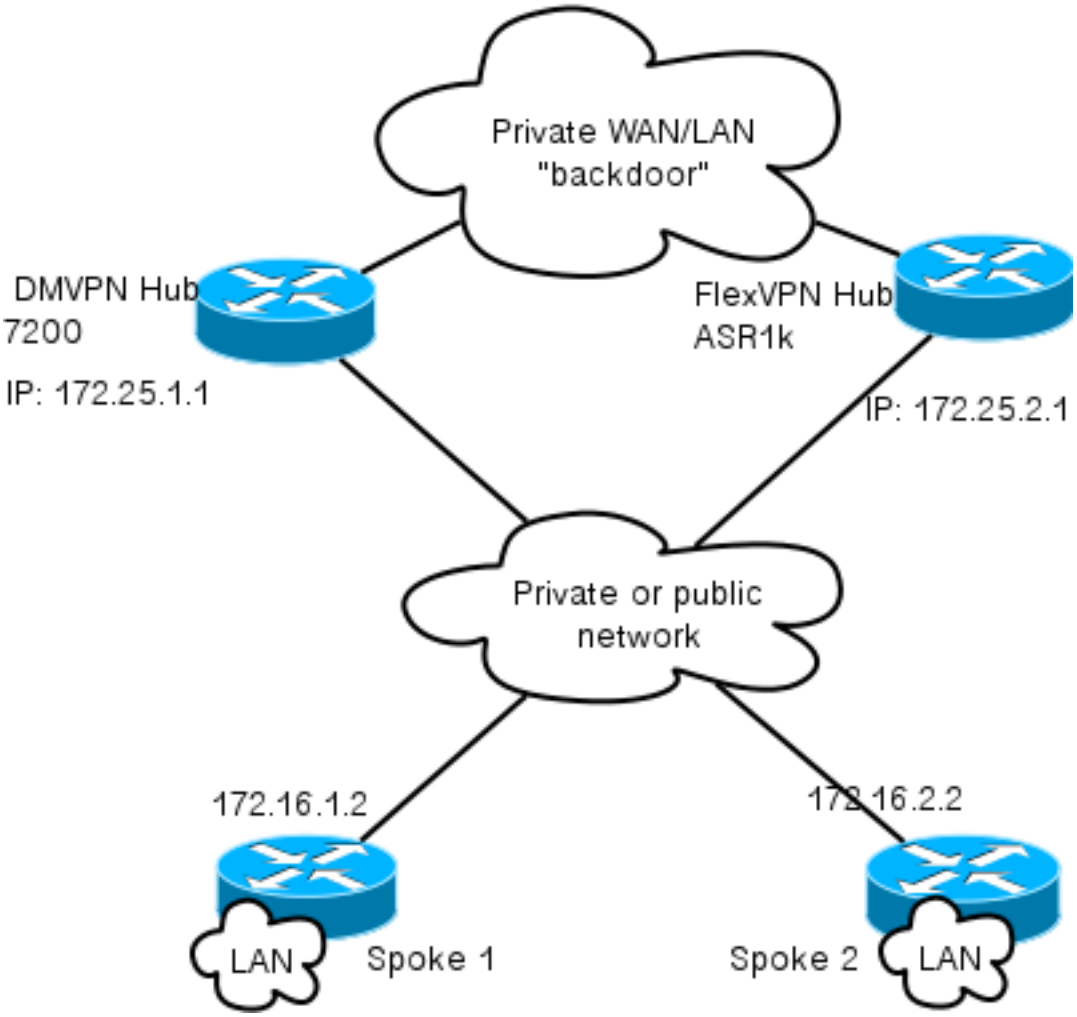
Abordagem personalizada

Se a abordagem anterior pode não ser a melhor solução para você devido às complexidades da rede ou do roteamento, inicie uma discussão com o representante da Cisco antes de migrar. A melhor pessoa com quem discutir um processo de migração personalizada é o engenheiro de sistemas ou engenheiro de serviços avançados.

Topologia de rede

Topologia da rede de transporte

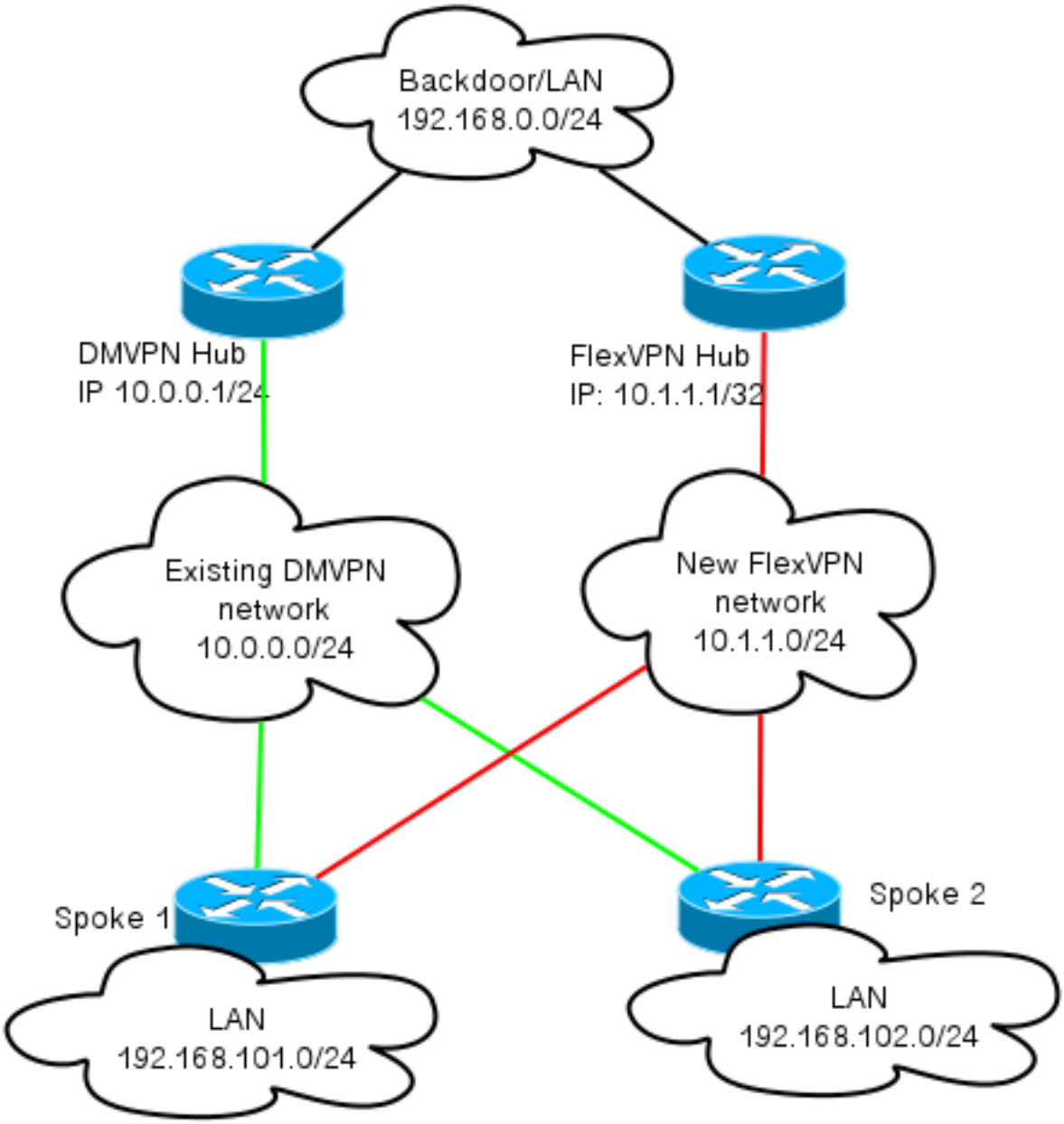
Este diagrama mostra a topologia de conexão típica dos hosts na Internet. O endereço IP do hub de **loopback0** (**172.25.1.1**) é usado para encerrar a sessão DMVPN IPsec. O endereço IP no novo hub (**172.25.2.1**) é usado para FlexVPN.



Observe o link entre os dois hubs. Esse link é crucial para permitir a conectividade entre as nuvens FlexVPN e DMVPN durante a migração. Permite que spokes já migrados para FlexVPN se comuniquem com redes DMVPN e vice-versa.

Topologia de sobreposição de rede

Este diagrama de topologia mostra duas nuvens separadas usadas para sobreposição: DMVPN (conexões verdes) e FlexVPN (conexões vermelhas). Os prefixos de LAN são mostrados para os sites correspondentes. A sub-rede **10.1.1.0/24** não representa uma sub-rede real em termos de endereçamento de interface, mas representa um pedaço de espaço IP dedicado à nuvem FlexVPN. A razão por trás disso é discutida posteriormente na seção **Configuração de FlexVPN**.



Configuração

Esta seção descreve as configurações de DMVPN e FlexVPN.

Configuração de DMVPN

Esta seção descreve a configuração básica do hub e spoke DMVPN.

A chave pré-compartilhada (PSK) é usada para autenticação IKEv1. Depois que o IPsec é estabelecido, o registro do Next Hop Resolution Protocol (NHRP) do spoke-to-hub é executado para que o hub possa aprender dinamicamente o endereçamento NBMA (Nonbroadcast Multiaccess) dos spokes.

Quando o NHRP executa o registro no spoke e no hub, a adjacência de roteamento pode ser estabelecida e as rotas podem ser trocadas. Neste exemplo, o EIGRP é usado como um protocolo de roteamento básico para a rede de sobreposição.

Configuração de Spoke DMVPN

Aqui você pode encontrar um exemplo básico de configuração de DMVPN com autenticação PSK e 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 de DMVPN de hub

Na configuração do hub, o túnel é originado do **loopback0** com um endereço IP de **172.25.1.1**. O restante é uma implantação padrão de um hub DMVPN com EIGRP como 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 FlexVPN

O FlexVPN é baseado nas mesmas tecnologias fundamentais:

- **IPSEC:** Ao contrário do padrão em DMVPN, IKEv2 é usado em vez de IKEv1 para negociar Associações de Segurança (SAs) IPsec. O IKEv2 oferece melhorias em relação ao IKEv1, como resiliência e o número de mensagens necessárias para estabelecer um canal de dados protegido.

- **GRE :** Diferentemente do DMVPN, são usadas interfaces ponto-a-ponto estáticas e dinâmicas, e não apenas uma interface GRE multiponto estática. Essa configuração permite maior flexibilidade, especialmente para comportamento por spoke/por hub.

- **NHRP**: No FlexVPN, o NHRP é usado principalmente para estabelecer comunicação spoke-to-spoke. Os spokes não se registram no hub.

- **Roteamento:** Como os spokes não executam o registro de NHRP no hub, você deve confiar em outros mecanismos para garantir que o hub e os spokes possam se comunicar bidirecionalmente. Da mesma forma que DMVPN, os protocolos de roteamento dinâmico podem ser usados. No entanto, o FlexVPN permite usar o IPsec para apresentar informações de roteamento. O padrão é introduzir a rota as **/32** para o endereço IP no outro lado do túnel, que permite a comunicação direta de spoke para hub.

Em uma migração forçada de DMVPN para FlexVPN, as duas estruturas não funcionam ao mesmo tempo nos mesmos dispositivos. No entanto, recomenda-se mantê-los separados.

Separe-os em vários níveis:

- NHRP - Use uma ID de rede NHRP diferente (recomendado).

- Roteamento - Use processos de roteamento separados (recomendado).
- Virtual Routing and Forwarding (VRF) - A separação de VRF permite maior flexibilidade, mas não é discutida aqui (opcional).

Configuração de Spoke FlexVPN

Uma das diferenças na configuração de spoke em FlexVPN em comparação com DMVPN é que você tem duas interfaces possíveis. Há um túnel necessário para comunicação spoke-to-hub e um túnel opcional para túneis spoke-to-spoke. Se você optar por não ter tunelamento spoke-to-spoke dinâmico e preferir que tudo passe pelo dispositivo de hub, você poderá remover a interface de modelo virtual e a comutação de atalho NHRP da interface de túnel.

Observe que a interface de túnel estático recebe um endereço IP com base na negociação. Isso permite que o hub forneça o endereço IP da interface do túnel ao spoke dinamicamente sem a necessidade de criar endereçamento estático na nuvem 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
```

> **Note**: Por padrão, a identidade local é definida para usar o endereço IP. Portanto, a instrução de correspondência correspondente no peer também deve corresponder com base no endereço. Se o requisito for corresponder com base no Nome distinto (DN) no certificado, então a correspondência deve ser feita com o uso de um mapa de certificado.

A Cisco recomenda que você use o AES GCM com hardware compatível.

```
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
```

Public Key Infrastructure (PKI) é o método recomendado para executar autenticação em larga escala em IKEv2. No entanto, você ainda pode usar a PSK desde que esteja ciente de suas limitações.

Aqui está um exemplo de configuração que usa **cisco** como 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 FlexVPN

Geralmente, um hub encerra apenas túneis spoke-to-hub dinâmicos. É por isso que você não encontra uma interface de túnel estático para FlexVPN na configuração do hub. Em vez disso, uma interface de modelo virtual é usada.

> **Note**: No lado do hub, você deve indicar os endereços do pool a serem atribuídos aos spokes.

Os endereços desse pool são adicionados posteriormente na tabela de roteamento como **/32** rotas para cada spoke.

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

crypto ikev2 authorization policy default
pool FlexSpokes
crypto ikev2 profile Flex_IKEv2
match identity remote fqdn domain cisco.com
local identity fqdn hub.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
```

A Cisco recomenda que você use o AES GCM com hardware compatível.

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

> **Note**: Nesta configuração, a operação AES GCM foi comentada.

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

interface Loopback0
description DMVPN termination
ip address 172.25.2.1 255.255.255.255
interface Loopback100
ip address 10.1.1.1 255.255.255.255
interface Virtual-Template1 type tunnel
ip unnumbered Loopback100
ip nhrp network-id 2
ip nhrp redirect
tunnel path-mtu-discovery
tunnel protection ipsec profile default
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

Com a autenticação em IKEv2, o mesmo princípio se aplica no hub do spoke. Para escalabilidade e flexibilidade, use certificados. No entanto, você pode reutilizar a mesma configuração para PSK do spoke.

> **Note**: O IKEv2 oferece flexibilidade em termos de autenticação. Um lado pode autenticar com PSK, enquanto o outro lado usa a assinatura Rivest-Shamir-Adleman (RSA-SIG).

Se o requisito for usar chaves pré-compartilhadas para autenticação, as alterações de configuração serão semelhantes às descritas para o roteador spoke aqui.

Conexão BGP entre hubs

Certifique-se de que os hubs saibam onde os prefixos específicos estão localizados. Isso se torna cada vez mais importante porque alguns spokes foram migrados para o FlexVPN enquanto outros spokes permanecem no DMVPN.

Esta é a conexão BGP entre hubs com base na configuração do hub DMVPN:

```
router bgp 65001
network 192.168.0.0
neighbor 192.168.0.2 remote-as 65001
```

Migração de tráfego

Migre para BGP como o protocolo de roteamento de sobreposição [recomendado]

O BGP é um protocolo de roteamento baseado na troca unicast. Devido às suas características, é o melhor protocolo de dimensionamento em redes DMVPN.

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

Configuração de Spoke BGP

A migração de spoke consiste em duas partes. Primeiro, ative o BGP como roteamento dinâmico:

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

Depois que o vizinho BGP aparecer (consulte a próxima seção) e novos prefixos sobre BGP forem aprendidos, você poderá alternar o tráfego da nuvem DMVPN atual para uma nova nuvem FlexVPN.

Configuração do BGP do hub

Hub FlexVPN - Configuração BGP completa

No hub, para evitar manter a configuração de vizinhança de cada spoke separadamente, configure ouvintes dinâmicos. Nesta configuração, o BGP não inicia novas conexões, mas aceita conexões do pool de endereços IP fornecido. Nesse caso, o pool em questão é **10.1.1.0/24**, que são todos os endereços na nova nuvem FlexVPN.

Dois pontos para observar:

- O hub FlexVPN anuncia prefixos específicos ao hub DMVPN; assim, o mapa de descompactação está sendo usado.
- Anuncie a sub-rede FlexVPN de **10.1.1.0/24** à tabela de roteamento ou certifique-se de que o hub DMVPN veja o hub FlexVPN como o próximo salto.

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 - Configuração completa de BGP e EIGRP

A configuração no hub DMVPN é básica, porque recebe apenas prefixos específicos do hub FlexVPN e anuncia os prefixos que aprende com o EIGRP.

```
router bgp 65001
bgp log-neighbor-changes
redistribute eigrp 100
neighbor 192.168.0.2 remote-as 65001
```

Migrar tráfego para BGP/FlexVPN

Conforme discutido anteriormente, você deve desligar a funcionalidade DMVPN e ativar o FlexVPN para executar a migração.

Este procedimento garante um impacto mínimo:

1. Em cada spoke, separadamente, insira:

   ```
   interface tunnel 0
    shut
   ```

   Neste ponto, certifique-se de que não há sessões IKEv1 estabelecidas para este spoke. Isso pode ser verificado se você verificar a saída do comando **show crypto isakmp sa** e monitorar mensagens de syslog geradas pelo comando **crypto logging session**. Depois que isso for confirmado, você poderá continuar a ativar o FlexVPN.

2. No mesmo spoke, digite:

   ```
   interface tunnel 1
     no shut
   ```

Etapas de verificação

Estabilidade de IPsec

A melhor maneira de avaliar a estabilidade do IPsec é monitorar sylogs com o comando de configuração **crypto logging session** habilitado. Se você vir sessões que vão para cima e para baixo, isso pode indicar um problema no nível IKEv2/FlexVPN que deve ser corrigido antes que a migração possa começar.

Informações de BGP preenchidas

Se o IPsec for estável, certifique-se de que a tabela BGP seja preenchida com entradas dos spokes (no hub) e resumo do hub (nos spokes). No caso do BGP, isso pode ser visto com estes

comandos:

```
show bgp
! or
show bgp ipv4 unicast
! or
show ip bgp summary
```

Aqui está um exemplo de informações corretas do hub 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 dos spokes, e ambos os spokes são dinâmicos e marcados com um sinal de asterisco (*). Ele também mostra que um total de quatro prefixos da conexão entre hubs é recebido.

Aqui está um exemplo de informações semelhantes 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 dessa configuração, um prefixo deve ser o resumo anunciado no hub FlexVPN. A outra é a rede DMVPN **10.0.0.0/24** redistribuída no spoke DMVPN no BGP.

Migre para novos túneis com EIGRP

O EIGRP é uma escolha popular em redes DMVPN devido à sua implantação relativamente simples e rápida convergência. No entanto, ele pode escalar pior que o BGP e não oferece muitos mecanismos avançados que podem ser usados pelo BGP diretamente da caixa. A próxima seção descreve uma das maneiras de mudar para FlexVPN com um novo processo EIGRP.

Configuração de spoke atualizada

Um novo sistema autônomo (AS) é adicionado com um processo EIGRP separado:

```
router eigrp 200
network 10.1.1.0 0.0.0.255
network 192.168.101.0
passive-interface default
no passive-interface Tunnel1
```

> **Note**: É melhor não estabelecer adjacência de protocolo de roteamento em túneis spoke-to-spoke. Portanto, faça apenas com que a interface de **tunnel1** (spoke-to-hub) não seja

passiva.

Configuração atualizada do hub FlexVPN

Da mesma forma, para o hub FlexVPN, prepare o protocolo de roteamento no AS apropriado, correspondendo a um configurado nos spokes.

```
router eigrp 200
network 10.1.1.0 0.0.0.255
```

Há dois métodos que são usados para fornecer resumo para o spoke.

- Redistribua uma rota estática que aponta para **null0** (opção preferencial).

```
ip route 192.168.0.0 255.255.0.0 null 0
ip route 10.1.1.0 255.255.255.0 null 0

ip prefix-list EIGRP_SUMMARY_ONLY seq 5 permit 192.168.0.0/16
ip prefix-list EIGRP_SUMMARY_ONLY seq 10 permit 10.1.1.0/24

route-map EIGRP_SUMMARY permit 20
match ip address prefix-list EIGRP_SUMMARY_ONLY

router eigrp 200
distribute-list route-map EIGRP_SUMMARY out Virtual-Template1
redistribute static metric 1500 10 10 1 1500 route-map EIGRP_SUMMARY
```

  Essa opção permite o controle sobre resumo e redistribuição sem modificações na configuração da Tecnologia de virtualização (VT) do hub. Isso é importante porque a configuração de VT do hub não pode ser modificada se houver acesso virtual ativo associado a ela.

- Configure um endereço de resumo no estilo DMVPN em um modelo virtual.

  Esta configuração *não* é *recomendada*, devido ao processamento interno e à replicação desse resumo para cada acesso virtual. Ele é mostrado aqui para referência.

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

  Outro aspecto a ser considerado é a troca de roteamento entre hubs. Isso pode ser feito se você redistribuir instâncias do EIGRP para o iBGP.

Hub DMVPN - Configuração BGP atualizada

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

```
router bgp 65001

redistribute eigrp 100

neighbor 192.168.0.2 remote-as 65001
```

Hub FlexVPN - Configuração BGP atualizada

Semelhante ao hub DMVPN, no FlexVPN, você deve redistribuir os prefixos do novo processo EIGRP para o BGP:

```
router bgp 65001

 redistribute eigrp 200 redistribute static

 neighbor 192.168.0.1 remote-as 65001
```

Migre o tráfego para FlexVPN

Você deve desligar a funcionalidade DMVPN e ativar o FlexVPN em cada spoke, um de cada vez, para executar a migração. Este procedimento garante um impacto mínimo:

1. Em cada spoke, separadamente, insira:

   ```
   interface tunnel 0
    shut
   ```

   Neste ponto, certifique-se de que não há sessões IKEv1 estabelecidas neste spoke. Isso pode ser verificado se você verificar a saída do comando **show crypto isakmp sa** e monitorar mensagens de syslog geradas pelo comando **crypto logging session**. Depois que isso for confirmado, você poderá continuar a ativar o FlexVPN.
2. No mesmo spoke, digite:

   ```
   interface tunnel 1
     no shut
   ```

Etapas de verificação

Estabilidade de IPsec

Como no caso do BGP, você deve avaliar se o IPsec é estável. A melhor maneira de fazer isso é monitorar sylogs com o comando de configuração **crypto logging session** ativado. Se você vir sessões subindo e descendo, isso pode indicar um problema no nível IKEv2/FlexVPN que deve ser corrigido antes que a migração possa começar.

Informações do EIGRP na Tabela de Topologia

Certifique-se de que sua tabela de topologia EIGRP seja preenchida com entradas de LAN de

raio no hub e resumo nos spokes. Isso pode ser verificado se você inserir esse comando no(s) hub(s) e nos spoke(s):

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

Aqui está 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 conhece sua sub-rede de LAN (em *itálico*) e os resumos para esses (em **negrito**).

Aqui está 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 spokes (em *itálico*), o prefixo de sumarização anunciado (em **negrito**) e o endereço IP atribuído a cada spoke via negociação.

Considerações adicionais

Túneis spoke-to-spoke que já existem

Como um desligamento da interface de túnel DMVPN faz com que as entradas NHRP sejam removidas, os túneis spoke-to-spoke já existentes serão desmontados.

Limpar entradas NHRP

Um hub FlexVPN não depende do processo de registro NHRP do spoke para saber como rotear o tráfego de volta. No entanto, os túneis spoke-to-spoke dinâmicos dependem de entradas NHRP.

No DMVPN, se o NHRP no hub for limpo, pode resultar em problemas de conectividade de vida curta. No FlexVPN, limpar o NHRP nos spokes fará com que a sessão FlexVPN IPsec, relacionada aos túneis spoke-to-spoke, seja destruída. Limpar o NHRP no hub não tem efeito na sessão FlexVPN.

Isso ocorre porque, no FlexVPN por padrão:

- Os spokes não se registram em hubs.
- Os hubs funcionam somente como redirecionadores NHRP e não instalam entradas NHRP.
- As entradas de atalho NHRP são instaladas em spokes para túneis spoke-to-spoke e são dinâmicas.

Caveats conhecidos

O tráfego spoke-to-spoke pode ser afetado pela ID de bug da Cisco CSCub07382 .

Informações Relacionadas

- Exemplo de configuração de migração de software DMVPN para FlexVPN
- Suporte Técnico e Documentação - Cisco Systems