Migração de FlexVPN: Movimento duro do DMVPN a FlexVPN nos mesmos dispositivos

Índice

Introdução

Este documento fornece a informação sobre como migrar de rede de DMVPN existente a FlexVPN nos mesmos dispositivos.

As configurações de ambas as estruturas coexistirão nos dispositivos.

Neste documento somente a maioria de cenário comum é mostrado: DMVPN usando a chave pré-compartilhada para a autenticação e o EIGRP como o protocolo de roteamento.

Este documento demonstra a migração a BGP (protocolo de roteamento recomendado) e ao EIGRP menos desejável.

Pré-requisitos

Requisitos

Este documento supõe que o leitor conhece conceitos básicos do DMVPN e do FlexVPN.

Componentes Utilizados

Note que não todo o suporte de software e hardware IKEv2. Refira o Cisco Feature Navigator para a informação. Idealmente, as versões de software a ser usadas são:

- ISR - 15.2(4)M1 ou mais novo
- ASR1k - 3.6.2 liberam 15.2(2)S2 ou mais novos

Entre as vantagens de uma plataforma e de um software mais novos é a possibilidade de usar a criptografia da próxima geração, por exemplo, AES GCM para a criptografia no IPsec. Isto é discutido no RFC 4106.

O AES GCM reserva alcançar uma velocidade muito mais rápida da criptografia em algum hardware.

A fim ver recomendações da Cisco na utilização e na migração à criptografia da próxima geração, refira:

http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

Convenções

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

Procedimento de migração

Atualmente, a maneira recomendada de migrar do DMVPN a FlexVPN é para as duas estruturas a não se operar ao mesmo tempo.

Esta limitação será removido devido às características novas da migração ser introduzido na liberação ASR 3.10, seguida sob requisições de aprimoramento múltiplas sob o lado de Cisco, incluindo CSCuc08066. Aquelas características devem estar disponíveis ao fim de junho, 2013.

Uma migração onde ambas as estruturas coexistam e se operem ao mesmo tempo nos mesmos dispositivos será referida que brandamente a migração, que indica o impacto mínimo e o Failover liso de uma estrutura a outra.

Uma migração onde a configuração de ambas as estruturas coexista, mas não se opera ao mesmo tempo é referida como a 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 nos mesmos dispositivos

Neste documento a migração de uma rede de DMVPN existente a uma rede nova de FlexVPN nos mesmos dispositivos é discutida.

Esta migração exige que ambas as estruturas não se operam ao mesmo tempo nos dispositivos, exigindo essencialmente que a funcionalidade DMVPN está desabilitada em toda a linha antes de permitir FlexVPN.

Até que a característica nova da migração esteja disponível, a maneira de executar as migrações que usam os mesmos dispositivos está a:

1. Verifique a Conectividade sobre o DMVPN.
2. Adicionar a configuração de FlexVPN no lugar e feche o túnel e as relações virtuais do molde que pertencem à configuração nova.
3. (Durante uma janela de manutenção) feche todas as interfaces de túnel DMVPN em todo o spokes e Hubs antes de mover-se para etapa 4.
4. Interfaces de túnel de Unshut FlexVPN.
5. Verifique falou à Conectividade do hub.
6. Verifique falou à Conectividade do spoke.
7. *Se a verificação no ponto 5 ou 6 não foi corretamente reverta de volta ao DMVPN fechando a relação de FlexVPN e un-fechando relações DMVPN.*
8. *Verifique falou a uma comunicação do hub.*
9. *Verifique falou a uma comunicação do spoke.*

Aproximação feita sob encomenda

Se, devido a suas complexidades da rede ou do roteamento, a aproximação não pôde ser a melhor ideia para você, comece uma discussão com seu representante do Cisco antes de migrar. A melhor pessoa para 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 uma topologia típica das conexões dos anfitriões no Internet. Neste documento, o endereço IP de Um ou Mais Servidores Cisco ICM NT do hub de loopback0 (172.25.1.1) é usado para terminar a sessão IPSec.

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 conexões de FlexVPN.

Os prefixos da rede de área local são mostrados para lados correspondentes.

A sub-rede 10.1.1.0/24 não representa o sub-rede real em termos do endereçamento da relação, mas um pouco pedaço do espaço IP dedicado à nuvem de FlexVPN. A base racional atrás é discutida mais tarde na seção de configuração de FlexVPN.

Configuração

Configuração DMVPN

Esta seção contém a configuração básica do hub and spoke DMVPN.

A chave pré-compartilhada (PSK) é usada para a autenticação IKEv1.

Uma vez que o IPsec foi estabelecido, o registro NHRP está executado de falou ao hub, de modo que o hub possa aprender o endereçamento NBMA dinamicamente dos raios.

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

Configuração do spoke DMVPN

Esta é uma configuração do exemplo básico do DMVPN com autenticação da chave pré-compartilhada 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 desenvolvimento padrão do 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 para negociar o sas de IPSec. IKEv2 oferece melhorias sobre IKEv1, começando com elasticidade e terminando com quantas mensagens são precisadas de estabelecer um canal de dados protegidos.
- GRE: Ao contrário do DMVPN, as relações pontos a ponto estáticas e dinâmicas são usadas, e não somente no GRE multiponto estático conecta. Esta configuração permite a flexibilidade adicionada, especialmente para o por-spoke/comportamento do por-hub.
- NHRP: Em FlexVPN o NHRP é usado primeiramente para estabelecer falou a uma comunicação do spoke. O spokes não se registra ao hub.
- Distribuição: Porque o spokes não executa o registro NHRP ao hub, você precisa de confiar em outros mecanismos para 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 para 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 permitirá uma comunicação direta spoke-to-hub.

Na 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 a rede NHRP diferente ID (recomendada).
- Distribuir - Use os processos de roteamento separados (recomendados).
- VRF - A separação VRF pode permitir a flexibilidade adicionada mas não será 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 necessário para falou a uma comunicação do hub e o túnel opcional para falou aos túneis do spoke. Se você escolhe não ter dinâmico falou ao spoke que escava um túnel e um pouco que tudo atravessa o dispositivo do hub, você pode remover a interface de molde virtual e remover o interruptor do atalho NHRP da interface de túnel.

Você igualmente observará que a interface de túnel estática tem um endereço IP de Um ou Mais Servidores Cisco ICM NT recebido baseado na negociação. Isto permite que o hub forneça o IP da interface de túnel falou 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
 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
```

Cisco recomenda usar AES GCM no 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 172.25.1.1
 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 PKI é a maneira recomendada de executar a autenticação da larga escala em IKEv2.

Contudo, você pode ainda usar a chave pré-compartilhada enquanto você está ciente dela é limitações.

Está aqui um exemplo de configuração usando “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
```

Configuração do hub de FlexVPN

Tipicamente um hub terminará somente túneis spoke-to-hub dinâmicos. Eis porque na configuração do hub você não encontrará uma interface de túnel estática para FlexVPN, em lugar de uma interface de molde virtual é usada. Isto desovará uma interface de acesso virtual para cada conexão.

Note que no lado de hub você precisa de indicar os endereços do conjunto a ser atribuídos ao spokes.

Os endereços deste pool serão adicionados mais tarde na tabela de roteamento como rotas de /32 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
 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
```

Cisco recomenda usar AES GCM no hardware que o apoia.

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

Note isso na configuração abaixo da operação AES GCM foi comentado para fora.

```
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2
! set transform-set IKEv2
interface Loopback0
 description DMVPN termination
 ip address 172.25.1.1 255.255.255.255
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
 shutdown
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

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 puder autenticar usando o PSK quando o outro RSA-SIG.

Migração do tráfego

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

O BGP é um protocolo de roteamento baseado na troca do unicast. Devido a ele são as características que foi o melhor protocolo da escamação nas redes de DMVPN.

Neste exemplo, o iBGP é usado.

Configuração de BGP do spoke

A migração do spoke consiste em duas porções. Permitindo o BGP como o 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 de BGP vem acima (vê a configuração de BGP do hub nesta seção da migração) e os prefixos novos sobre o BGP são instruídos, você pode balançar o tráfego da nuvem existente DMVPN à nuvem nova de FlexVPN.

Configuração de BGP do hub

No hub evitar manter a configuração do neighborship para o cada falou separadamente, ouvintes dinâmicos é configurada.

Nesta instalação o BGP não iniciará novas conexões, mas aceitará a conexão 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.

```
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
```

Tráfego da migração a FlexVPN

Como mencionado antes a migração precisa de ser feita fechar DMVPN e trazer FlexVPN pela funcionalidade acima.

Este procedimento garante o impacto mínimo.

1. Em todo o spokes:`interface tunnel 0`
   `shut`
2. No hub:`interface tunnel 0`
   `shut`Certifique-se neste momento de que não há nenhuma sessão IKEv1 estabelecida a este hub do spokes.Isto pode ser verificado verificando a saída do **comando show crypto isakmp sa** e monitorando os mensagens do syslog gerados pela sessão de registro cripto.Uma vez que isto foi confirmado você pode continuar a trazer acima FlexVPN.
3. Continuação no hub:`interface Virtual-template 1`
   `no shut`
4. No spokes:`interface tunnel 1`
   `no shut`

Etapas de verificação

Estabilidade do IPsec

A melhor maneira de avaliar a estabilidade do IPsec está monitorando por sylogs com este comando configuration permitido:

```
crypto logging session
```

Se você vê sessões ir para cima e para baixo, este pode indicar um problema no nível IKEv2/FlexVPN que precisa de 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).

Em caso do BGP, isto pode ser visto executando:

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

Exemplo da informação correta do hub:

```
Hub#show bgp
BGP router identifier 172.25.1.1, local AS number 65001
(...omitted...)
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
*10.1.1.101 4 65001 83 82 13 0 0 01:10:46 1 *10.1.1.102 4 65001 7 7 13 0 0 00:00:44 1
```

Você pode ver que o hub aprendeu que 1 prefixo de cada um do spokes e ambo o spokes são dinâmicos (identificado por meio de sinal do asterisco (*)).

Exemplo da informação similar do spoke:

```
Spoke1#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 11 11 6 0 0 00:03:43 1
```

O spoke recebeu um prefixo do hub. Em caso desta instalação, este prefixo deve ser o sumário anunciado no hub.

Migração aos túneis novos usando o EIGRP

O EIGRP é uma escolha popular nas redes de DMVPN devido a ele é desenvolvimento e convergência rápida relativamente simples.

, Contudo, escalará mais ruim do que o BGP e não oferece muitos dos mecanismos avançados que podem ser usados pelo BGP em linha reta fora da caixa.

Esta próxima seção descreve uma das maneiras de mover-se para FlexVPN usando um processo de EIGRP novo.

Configuração de raio actualizado

Neste exemplo, um novo COMO é adicionado com um processo de 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
```

Nota: Você deve evitar estabelecer a adjacência do protocolo de roteamento sobre falou aos túneis do spoke, assim faz somente a relação de tunnel1 (falou ao hub) não passiva.

Configuração actualizado do hub

Similarmente no hub, o DMVPN deve permanecer a maneira preferida trocar sobre o tráfego. Contudo, FlexVPN deve anunciar e aprender os mesmos prefixos já.

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

Há duas maneiras de fornecer a parte traseira do sumário para o spoke.

- Redistribuindo uma rota estática que aponta ao null0 (opção preferida).`ip route 192.168.0.0 255.255.0.0 null 0`
  ```
  ip access-list standard EIGRP_SUMMARY
   permit 192.168.0.0 0.0.255.255
  ```

```
router eigrp 200
 distribute-list EIGRP_SUMMARY out Virtual-Template1
 redistribute static metric 1500 10 10 1 1500
```
Esta opção reserva ter o controle sobre o sumário e a redistribuição sem configuração VT do hub tocante.

- Ou, você pode estabelecer um endereço sumário do DMVPN-estilo no Virtual-molde. 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 200 172.16.1.0 255.255.255.0
 ip summary-address eigrp 200 192.168.0.0 255.255.0.0 delay 2000
```

Tráfego da migração a FlexVPN

A migração precisa de ser feita fechar DMVPN e trazer FlexVPN pela funcionalidade acima.

O seguinte procedimento garante o impacto mínimo.

1. Em todo o spokes:
```
interface tunnel 0
 shut
```
2. No hub:
```
interface tunnel 0
 shut
```
Certifique-se neste momento de que não há nenhuma sessão IKEv1 estabelecida a este hub do spokes.Isto pode ser verificado verificando a saída do **comando show crypto isakmp sa** e monitorando os mensagens do syslog gerados pela sessão de registro cripto.Uma vez que isto foi confirmado você pode continuar a trazer acima FlexVPN.
3. Continuação no hub:
```
interface Virtual-template 1
 no shut
```
4. Em todo o spokes:
```
interface tunnel 1
 no shut
```

Passos de verificação

Estabilidade do IPsec

Como em caso do BGP, você precisa de avaliar se o IPsec é estável. A melhor maneira de fazer assim está monitorando por sylogs com este comando configuration permitido:

```
crypto logging session
```
Se você vê sessões ir para cima e para baixo, este pode indicar um problema no nível IKEv2/FlexVPN que precisa de ser corrigido antes que a migração possa começar.

Informação de EIGRP na tabela de topologia

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

```
show ip eigrp topology
```
Exemplo da saída apropriada do spoke:

```
Spoke1#sh 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
(...omitted as output related to DMVPN cloud ...)
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)


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 (26114560/1709056), Tunnel1 P 10.1.1.107/32, 1
successors, FD is 26112000 via Connected, Tunnel1
```

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

Exemplo da saída apropriada do hub.

```
Hub#sh ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(172.25.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status
(...omitted, related to DMVPN...)
EIGRP-IPv4 Topology Table for AS(200)/ID(172.25.1.1)
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, Loopback100


P 192.168.101.0/24, 1 successors, FD is 1561600 via 10.1.1.107 (1561600/281600), Virtual-Access1
P 192.168.0.0/16, 1 successors, FD is 1709056 via Rstatic (1709056/0) P 10.1.1.107/32, 1
successors, FD is 1709056 via Rstatic (1709056/0) P 10.1.1.106/32, 1 successors, FD is 1709056
via Rstatic (1709056/0) P 0.0.0.0/0, 1 successors, FD is 1709056 via Rstatic (1709056/0) P
192.168.102.0/24, 1 successors, FD is 1561600 via 10.1.1.106 (1561600/281600), Virtual-Access2
```

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

Considerações adicionais

Existir falou aos túneis do spoke

Porque fechar a interface de túnel DMVPN faz com que as entradas NHRP sejam removidas, existir falou aos túneis do spoke será rasgada para baixo.

Cancelando entradas NHRP

Como mencionado antes, um hub de FlexVPN não confiará no processo de registro NHRP do falou para saber distribuir a parte traseira do tráfego. Contudo, dinâmico falou aos túneis do spoke confiam em entradas NHRP.

No DMVPN onde o NHRP de cancelamento no hub poderia ter conduzido aos breves problemas de conectividade.

Em FlexVPN cancelar o NHRP no spokes causará a sessão IPSec de FlexVPN, relativa ao falou aos túneis do spoke, para ser rasgado para baixo. Em cancelar o NHRP nenhum hub terá um efeito na sessão de FlexVPN.

Isto é devido ao fato que em FlexVPN, à revelia:

- O spokes não se registra ao Hubs.
- O Hubs funciona somente como o redirecionador 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

Falou ao tráfego do spoke pôde ser afetado por CSCub07382.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems