동일한 장치에서 DMVPN에서 FlexVPN으로 하드 이동 마이그레이션

목차

소개

이 문서에서는 동일한 디바이스의 기존 DMVPN 네트워크에서 FlexVPN으로 마이그레이션하는 방법에 대한 정보를 제공합니다.

두 프레임워크 컨피그레이션이 모두 디바이스에 공존합니다.

이 문서에서는 가장 일반적인 시나리오만 표시됩니다. 인증에 사전 공유 키를 사용하는 DMVPN 및 라우팅 프로토콜로 EIGRP 사용

이 문서에서는 BGP(권장 라우팅 프로토콜) 및 덜 바람직한 EIGRP로의 마이그레이션을 보여 줍니다.

사전 요구 사항

요구 사항

이 문서에서는 독자가 DMVPN 및 FlexVPN의 기본 개념을 알고 있다고 가정합니다.

사용되는 구성 요소

모든 소프트웨어 및 하드웨어가 IKEv2를 지원하지는 않습니다. 자세한 내용은 Cisco Feature Navigator를 참조하십시오. 가장 이상적인 소프트웨어 버전은 다음과 같습니다.

- ISR - 15.2(4)M1 이상
- ASR1k - 3.6.2 릴리스 15.2(2)S2 이상

최신 플랫폼 및 소프트웨어의 장점 중 하나는 IPsec에서 암호화하는 AES GCM과 같은 차세대 암호화를 사용할 수 있다는 것입니다. 이 내용은 RFC 4106에 설명되어 있습니다.

AES GCM은 일부 하드웨어에서 훨씬 빠른 암호화 속도를 제공합니다.

Next Generation Cryptography 사용 및 마이그레이션에 대한 Cisco 권장 사항을 보려면 다음을 참조하십시오.

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

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

마이그레이션 절차

현재 DMVPN에서 FlexVPN으로 마이그레이션하는 권장 방법은 두 프레임워크가 동시에 작동하지 않는 것입니다.

이 제한은 ASR 3.10 릴리스에 도입되는 새로운 마이그레이션 기능, CSCuc08066을 포함하여 Cisco 측에서 여러 개선 요청을 추적한 결과 제거될 예정입니다. 이러한 기능은 2013년 6월 말에 사용할 수 있어야 합니다.

두 프레임워크가 공존하고 동일한 디바이스에서 동시에 작동하는 마이그레이션을 소프트 마이그레이션이라고 합니다. 즉, 한 프레임워크에서 다른 프레임워크로의 원활한 페일오버를 나타내며,

두 프레임워크 구성이 공존하지만 동시에 작동하지 않는 마이그레이션을 하드 마이그레이션이라고 합니다. 이는 한 프레임워크에서 다른 프레임워크로 전환하면 최소한의 경우에도 VPN을 통한 통신이 부족하다는 것을 의미합니다.

동일한 장치에서 하드 마이그레이션

이 문서에서는 기존 DMVPN 네트워크에서 동일한 디바이스의 새 FlexVPN 네트워크로 마이그레이션하는 방법에 대해 설명합니다.

이 마이그레이션을 수행하려면 두 프레임워크가 디바이스에서 동시에 작동하지 않아야 하며, 기본적으로 FlexVPN을 활성화하기 전에 보드 전체에서 DMVPN 기능을 비활성화해야 합니다.

새로운 마이그레이션 기능을 사용할 수 있을 때까지 동일한 디바이스를 사용하여 마이그레이션을 수행하는 방법은 다음과 같습니다.

1. DMVPN을 통한 연결을 확인합니다.
2. FlexVPN 컨피그레이션을 추가하고 새 컨피그레이션에 속하는 터널 및 가상 템플릿 인터페이스를 종료합니다.
3. (유지 보수 기간 중) 4단계로 이동하기 전에 모든 스포크와 허브의 모든 DMVPN 터널 인터페이스를 종료합니다.
4. FlexVPN 터널 인터페이스를 종료합니다.
5. 스포크와 허브 연결 상태를 확인합니다.
6. 스포크 대 스포크 연결을 확인합니다.
7. *포인트 5 또는 6에서 검증이 제대로 작동하지 않으면 FlexVPN 인터페이스를 종료하고 DMVPN 인터페이스를 종료하여 DMVPN으로 다시 돌아갑니다.*
8. *허브 통신에 대한 스포크를 확인합니다.*
9. *스포크 대 스포크 통신을 확인합니다.*

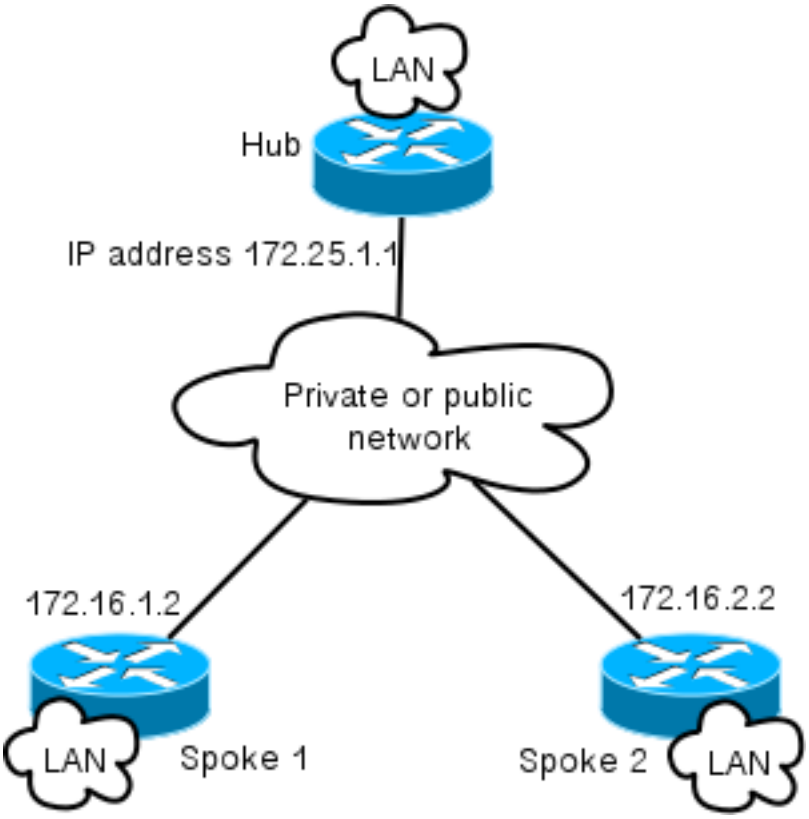
맞춤형 접근 방식

네트워크 또는 라우팅의 복잡성으로 인해 이러한 접근 방식이 최상의 방법이 아닐 수 있는 경우 마이그레이션하기 전에 Cisco 담당자와 논의를 시작하십시오. 사용자 지정 마이그레이션 프로세스에 대해 논의할 수 있는 가장 적합한 사람은 시스템 엔지니어 또는 고급 서비스 엔지니어입니다.

네트워크 토폴로지

전송 네트워크 토폴로지

이 다이어그램은 인터넷에 있는 호스트의 일반적인 연결 토폴로지를 보여줍니다. 이 문서에서는 허브의 루프백0(172.25.1.1)의 IP 주소를 사용하여 IPsec 세션을 종료합니다.

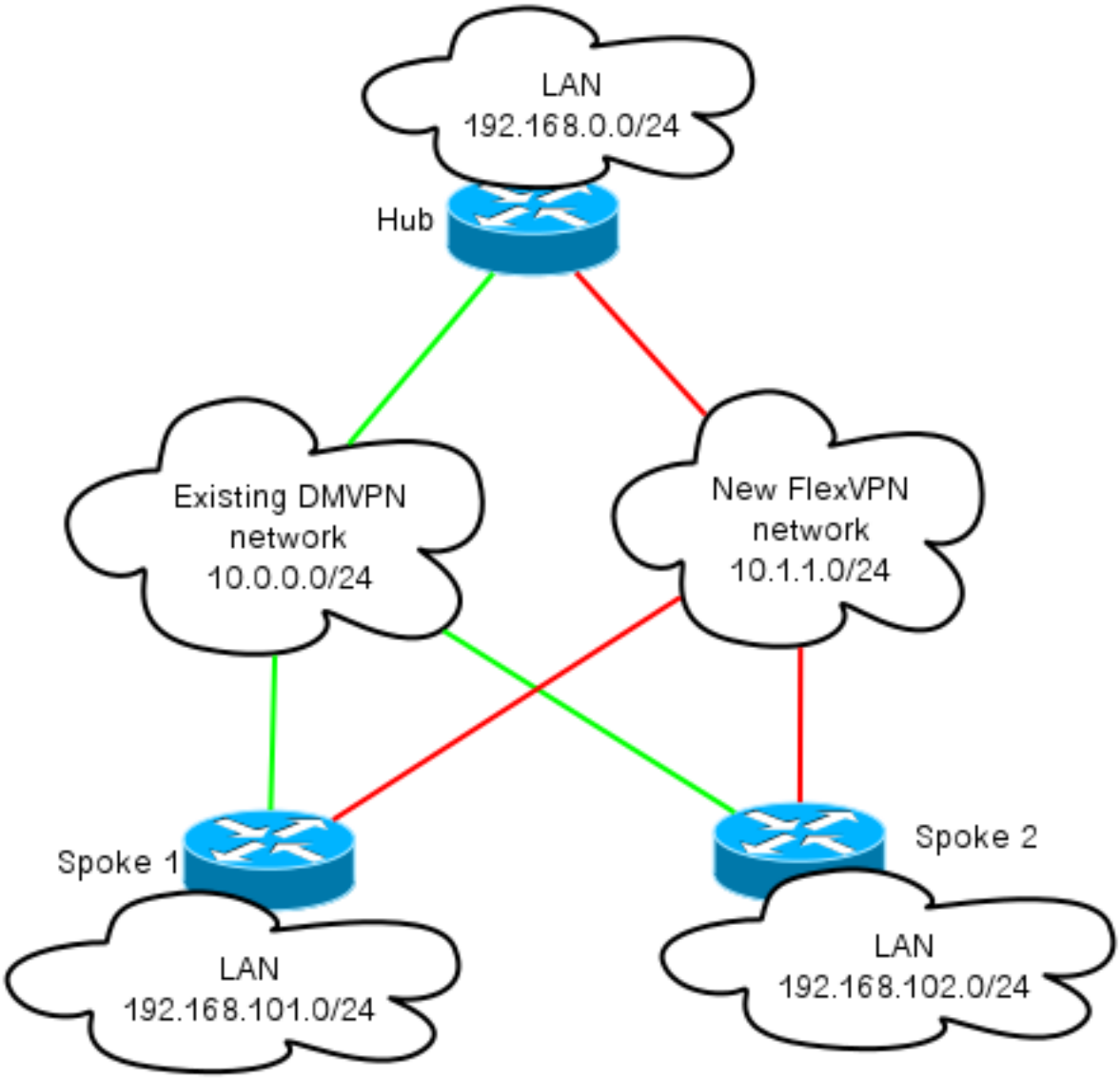


오버레이 네트워크 토폴로지

이 토폴로지 다이어그램은 오버레이에 사용되는 두 개의 개별 클라우드를 보여줍니다. DMVPN(녹색 연결) 및 FlexVPN 연결

Local Area Network 접두사는 해당 측면에 표시됩니다.

10.1.1.0/24 서브넷은 인터페이스 주소 지정 측면에서 실제 서브넷을 나타내지 않고 FlexVPN 클라우드 전용 IP 공간의 청크를 나타냅니다. 그 이유에 대해서는 나중에 FlexVPN Configuration 섹션에서 설명합니다.



구성

DMVPN 컨피그레이션

이 섹션에는 DMVPN 허브 및 스포크의 기본 컨피그레이션이 포함되어 있습니다.

PSK(사전 공유 키)는 IKEv1 인증에 사용됩니다.

IPsec이 설정되면 허브가 동적으로 스포크의 NBMA 주소를 학습할 수 있도록 스포크에서 허브로 NHRP 등록이 수행됩니다.

NHRP가 스포크 및 허브에 대한 등록을 수행하면 라우팅 인접성이 교환된 경로를 설정하고 라우팅할 수 있습니다. 이 예에서 EIGRP는 오버레이 네트워크의 기본 라우팅 프로토콜로 사용됩니다.

스포크 DMVPN 컨피그레이션

이것은 사전 공유 키 인증 및 EIGRP를 라우팅 프로토콜로 사용하는 DMVPN의 기본 컨피그레이션의 예입니다.

```
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
```

허브 DMVPN 컨피그레이션

허브 컨피그레이션에서 터널은 IP 주소가 172.25.1.1인 loopback0에서 소싱됩니다.

나머지는 라우팅 프로토콜로 EIGRP를 사용하는 DMVPN 허브의 표준 구축입니다.

```
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
```

FlexVPN 컨피그레이션

FlexVPN은 다음과 같은 기본적인 기술을 기반으로 합니다.

- IPsec: DMVPN의 기본값과 달리 IKEv1 대신 IKEv2를 사용하여 IPsec SA를 협상합니다. IKEv2는 IKEv1보다 향상된 기능을 제공합니다. 복원력을 시작으로 보호된 데이터 채널을 설정하는 데 필요한 메시지 수로 끝납니다.
- GRE : DMVPN과 달리 고정 및 동적 포인트 투 포인트 인터페이스가 사용되며 고정 멀티포인트 GRE 인터페이스에서만 사용됩니다. 이 컨피그레이션을 사용하면 특히 스포크당/허브당 동작에 유연성을 추가할 수 있습니다.
- NHRP: FlexVPN NHRP에서는 주로 스포크 대 스포크 통신을 설정하는 데 사용됩니다. 스포크는 허브에 등록되지 않습니다.
- 라우팅: 스포크는 허브에 NHRP 등록을 수행하지 않으므로 허브와 스포크가 양방향으로 통신할 수 있도록 다른 메커니즘에 의존해야 합니다. DMVPN과 마찬가지로 동적 라우팅 프로토콜을 사용할 수 있습니다. 그러나 FlexVPN을 사용하면 IPsec을 사용하여 라우팅 정보를 도입할 수 있습니다. 기본값은 터널의 반대쪽에 있는 IP 주소에 대해 /32 경로를 도입하여 스포크 투 허브 직접 통신을 허용합니다.

DMVPN에서 FlexVPN으로 하드 마이그레이션하는 경우 두 프레임워크가 동일한 디바이스에서 동시에 작동하지 않습니다. 그러나, 이를 별도로 유지하는 것이 좋습니다.

여러 레벨로 구분합니다.

- NHRP - 다른 NHRP 네트워크 ID를 사용합니다(권장).
- 라우팅 - 별도의 라우팅 프로세스를 사용합니다(권장).
- VRF - VRF 분리는 유연성을 높일 수 있지만 여기서는 논의되지 않습니다(선택 사항).

Spoke FlexVPN 구성

FlexVPN의 스포크 컨피그레이션과 DMVPN의 차이점 중 하나는 잠재적으로 두 개의 인터페이스가 있다는 것입니다.

스포크 대 허브 통신에는 필요한 터널이 있으며 스포크 대 스포크 터널에는 선택적 터널이 있습니다. 스포크 터널링에 동적 스포크가 없도록 선택하고 모든 작업이 허브 디바이스를 통과하도록 하려면 가상 템플릿 인터페이스를 제거하고 터널 인터페이스에서 NHRP 바로 가기 스위칭을 제거할 수 있습니다.

또한 고정 터널 인터페이스의 IP 주소가 협상을 기반으로 수신되었음을 확인할 수 있습니다. 이를 통해 허브는 FlexVPN 클라우드에서 정적 주소 지정을 생성할 필요 없이 동적으로 스포크에 터널 인터페이스 IP를 제공할 수 있습니다.

```
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
```

Cisco에서는 AES GCM을 지원하는 하드웨어에서 사용하는 것이 좋습니다.

```
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
```

PKI는 IKEv2에서 대규모 인증을 수행하는 권장 방법입니다.

그러나 사전 공유 키는 제한 사항을 알고 있는 한 계속 사용할 수 있습니다.

다음은 "cisco"를 PSK로 사용하는 구성의 예입니다.

```
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
```

FlexVPN 허브 구성

일반적으로 허브는 동적 스포크 투 허브 터널만 종료합니다. 따라서 허브의 컨피그레이션에서 가상 템플릿 인터페이스가 사용되는 대신 FlexVPN에 대한 고정 터널 인터페이스를 찾을 수 없습니다. 그러면 각 연결에 대한 가상 액세스 인터페이스가 생성됩니다.

허브 측에서 스포크에 할당할 풀 주소를 가리켜야 합니다.

이 풀의 주소는 라우팅 테이블에서 각 스포크에 대한 /32 경로로 나중에 추가됩니다.

```
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
```

Cisco에서는 이를 지원하는 하드웨어에서 AES GCM을 사용하는 것이 좋습니다.

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

아래 구성에서 AES GCM 작업이 주석 처리되었습니다.

```
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
```

IKEv2에서 인증을 사용하는 경우 스포크에서와 동일한 원칙이 허브에 적용됩니다.

확장성과 유연성을 위해 인증서를 사용하십시오. 그러나 PSK에 대해 스포크에서와 동일한 컨피그레이션을 다시 사용할 수 있습니다.

참고: IKEv2는 인증 측면에서 유연성을 제공합니다. 한 쪽은 PSK를 사용하여 인증할 수 있고 다른 한 쪽은 RSA-SIG를 사용하여 인증할 수 있습니다.

트래픽 마이그레이션

오버레이 라우팅 프로토콜로 BGP로 마이그레이션 [권장]

BGP는 유니캐스트 교환을 기반으로 하는 라우팅 프로토콜입니다. 이러한 특성으로 인해 DMVPN 네트워크에서 최고의 확장 프로토콜이 되었습니다.

이 예에서는 iBGP가 사용됩니다.

Spoke BGP 컨피그레이션

Spoke 마이그레이션은 두 부분으로 구성됩니다. BGP를 동적 라우팅으로 활성화합니다.

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

BGP 네이버가 나타나고(마이그레이션의 이 섹션에 있는 허브 BGP 컨피그레이션 참조) BGP를 통한 새 접두사가 학습되면 기존 DMVPN 클라우드에서 새 FlexVPN 클라우드로 트래픽을 스윙할 수 있습니다.

허브 BGP 컨피그레이션

허브에서 각 스포크의 인접 구성을 별도로 유지하지 않도록 동적 리스너가 구성됩니다.

이 설정에서 BGP는 새 연결을 시작하지 않지만 제공된 IP 주소 풀의 연결을 수락합니다. 이 경우 해당 풀은 새 FlexVPN 클라우드의 모든 주소인 10.1.1.0/24입니다.

```
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
```

FlexVPN으로 트래픽 마이그레이션

앞서 언급했듯이 DMVPN 기능을 종료하고 FlexVPN을 가동하여 마이그레이션을 수행해야 합니다.

이 절차는 최소 영향을 보장합니다.

1. 모든 스포크에서:
   ```
   interface tunnel 0
      shut
   ```
2. 허브:
   ```
   interface tunnel 0
     shut
   ```
   이 시점에서 스포크에서 이 허브에 설정된 IKEv1 세션이 없는지 확인합니다.이는 show crypto isakmp sa 명령의 출력을 확인하고 암호화 로깅 세션에서 생성된 syslog 메시지를 모니터링하여 확인할 수 있습니다.이 사실이 확인되면 FlexVPN을 계속 사용할 수 있습니다.
3. 허브에서 계속:
   ```
   interface Virtual-template 1
    no shut
   ```
4. 스포크:
   ```
   interface tunnel 1
      no shut
   ```

확인 단계

IPsec 안정성

IPsec 안정성을 평가하는 가장 좋은 방법은 다음 컨피그레이션 명령을 활성화하여 syslog를 모니터링하는 것입니다.

```
crypto logging session
```

세션이 작동 및 중단되는 경우 마이그레이션을 시작하기 전에 수정해야 하는 IKEv2/FlexVPN 레벨의 문제를 나타낼 수 있습니다.

BGP 정보가 입력됨

IPsec이 안정적인 경우 BGP 테이블이 스포크의 항목(허브)과 허브의 요약(스포크)으로 채워져 있는지 확인합니다.

BGP의 경우 다음을 수행하여 볼 수 있습니다.

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

허브의 올바른 정보 예:

```
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
```

허브가 각 스포크와 두 스포크의 1개 접두사가 동적(별표(*) 기호로 표시됨)이라는 것을 알 수 있습니다.

스포크의 유사 정보 예:

```
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
```

스포크가 허브에서 하나의 접두사를 받았습니다. 이 설정의 경우 이 접두사는 허브에 광고된 요약이어야 합니다.

EIGRP를 사용하여 새 터널로 마이그레이션

EIGRP는 비교적 간단한 구축 및 빠른 컨버전스로 인해 DMVPN 네트워크에서 널리 사용되는 옵션입니다.

그러나 BGP보다 확장성이 떨어지며 BGP에서 즉시 사용할 수 있는 많은 고급 메커니즘을 제공하지 않습니다.

다음 섹션에서는 새 EIGRP 프로세스를 사용하여 FlexVPN으로 이동하는 방법 중 하나를 설명합니다.

스포크 구성 업데이트

이 예에서는 별도의 EIGRP 프로세스로 새 AS가 추가됩니다.

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

참고: 스포크 터널에 대한 라우팅 프로토콜 인접성을 설정하지 않도록 해야 합니다. 따라서 패시브가 아닌 tunnel1(hub에 스포크)의 인터페이스만 만들 수 있습니다.

허브 구성 업데이트

마찬가지로, 허브에서 DMVPN은 트래픽을 교환하는 기본 방법으로 유지해야 합니다. 그러나 FlexVPN은 이미 동일한 접두사를 광고하고 학습해야 합니다.

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

두 가지 방법으로 스포크에 대한 요약을 다시 제공할 수 있습니다.

- null0을 가리키는 고정 경로를 재배포합니다(기본 설정 옵션).
  ```
  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
  ```
  이 옵션을 사용하면 허브의 VT 컨피그레이션에 연결하지 않고도 요약 및 재배포를 제어할 수 있습니다.
- 또는 가상 템플릿에 DMVPN 스타일 요약 주소를 설정할 수 있습니다. 이 구성은 각 가상 액세스에 대해 해당 요약의 내부 처리 및 복제 때문에 권장되지 않습니다. 참조:
  ```
  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
  ```

FlexVPN으로 트래픽 마이그레이션

DMVPN 기능을 종료하고 FlexVPN을 가동하여 마이그레이션을 수행해야 합니다.

다음 절차는 최소 영향을 보장합니다.

1. 모든 스포크에서:
   ```
   interface tunnel 0
      shut
   ```
2. 허브:
   ```
   interface tunnel 0
   ```

```
shut
```

이 시점에서 스포크에서 이 허브에 설정된 IKEv1 세션이 없는지 확인합니다.이는 **show crypto isakmp sa** 명령의 출력을 확인하고 암호화 로깅 세션에서 생성된 syslog 메시지를 모니터링하여 확인할 수 있습니다.이 사실이 확인되면 FlexVPN을 계속 사용할 수 있습니다.

3. 허브에서 계속:

```
interface Virtual-template 1
 no shut
```

4. 모든 스포크에서:

```
interface tunnel 1
   no shut
```

확인 단계

IPsec 안정성

BGP의 경우 IPsec이 안정적인지 평가해야 합니다. 가장 좋은 방법은 다음 컨피그레이션 명령을 활성화하여 syslog를 모니터링하는 것입니다.

```
crypto logging session
```

세션이 작동 및 중단되는 경우 마이그레이션을 시작하기 전에 수정해야 하는 IKEv2/FlexVPN 레벨의 문제를 나타낼 수 있습니다.

토폴로지 테이블의 EIGRP 정보

허브의 스포크 LAN 항목과 스포크의 요약이 채워진 EIGRP 토폴로지 테이블이 있는지 확인합니다. 허브 및 스포크에서 이 명령을 실행하여 이를 확인할 수 있습니다.

```
show ip eigrp topology
```

스포크의 적절한 출력 예:

```
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
```

스포크가 해당 LAN 서브넷(기울임체) 및 요약에 대해 알고 있음을 알 수 있습니다(굵게).

허브의 적절한 출력의 예.

```
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
```

허브는 스포크의 LAN 서브넷(기울임꼴), 광고 중인 요약 접두사(**굵게** 표시) 및 협상을 통해 각 스포크의 할당된 IP 주소에 대해 알고 있습니다.

추가 고려 사항

스포크 터널에 대한 기존 스포크

DMVPN 터널 인터페이스를 종료하면 NHRP 항목이 제거되므로 스포크 터널에 대한 기존 스포크가 해제됩니다.

NHRP 항목 지우기

앞에서 언급했듯이 FlexVPN 허브는 트래픽을 다시 라우팅하는 방법을 알기 위해 스포크의 NHRP 등록 프로세스에 의존하지 않습니다. 그러나 스포크 터널에 대한 동적 스포크는 NHRP 항목을 사용합니다.

허브에서 NHRP를 지운 DMVPN에서는 연결 문제가 짧을 수 있습니다.

FlexVPN에서 스포크의 NHRP를 지우면 스포크 터널과 관련된 FlexVPN IPsec 세션이 해제됩니다. NHRP를 지우면 허브는 FlexVPN 세션에 영향을 주지 않습니다.

이는 FlexVPN에서 기본적으로 다음과 같은 사실이 있기 때문입니다.

- 스포크는 허브에 등록되지 않습니다.

- 허브는 NHRP 리디렉터로만 작동하며 NHRP 엔트리를 설치하지 않습니다.
- NHRP 바로 가기 항목은 스포크 투 스포크 터널의 스포크에 설치되며 동적 항목입니다.

알려진 주의 사항

스포크 대 스포크 트래픽은 CSCub07382의 영향을 받을 수 있습니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems