다른 허브의 DMVPN에서 FlexVPN으로 하드 이동 마이그레이션

목차

소개
사전 요구 사항
요구 사항
사용되는 구성 요소
마이그레이션 절차
서로 다른 두 허브 간의 하드 마이그레이션
맞춤형 접근 방식
네트워크 토폴로지
전송 네트워크 토폴로지
오버레이 네트워크 토폴로지
구성
DMVPN 컨피그레이션
스포크 DMVPN 컨피그레이션
허브 DMVPN 컨피그레이션
FlexVPN 컨피그레이션
Spoke FlexVPN 구성
FlexVPN 허브 구성
트래픽 마이그레이션
오버레이 라우팅 프로토콜로 BGP로 마이그레이션 [권장]
Spoke BGP 컨피그레이션
허브 BGP 컨피그레이션
BGP/FlexVPN으로 트래픽 마이그레이션
EIGRP를 사용하여 새 터널로 마이그레이션
스포크 구성 업데이트
업데이트된 FlexVPN 허브 구성
DMVPN 허브 - 업데이트된 BGP 컨피그레이션
FlexVPN 허브 - 업데이트된 BGP 컨피그레이션
FlexVPN으로 트래픽 마이그레이션
확인 단계
추가 고려 사항
이미 존재하는 스포크 투 스포크 터널
NHRP 항목 지우기
알려진 주의 사항
관련 정보

소개

이 문서에서는 현재 존재하는 DMVPN(Dynamic Multipoint VPN) 네트워크에서 다른 허브 디바이스의 FlexVPN으로 마이그레이션하는 방법에 대한 정보를 제공합니다. 두 프레임워크의 컨피그레이션은 디바이스에서 공존합니다. 이 문서에서는 가장 일반적인 시나리오만 표시됩니다. 즉, 인증에 사전 공유 키를 사용하는 DMVPN과 라우팅 프로토콜로 EIGRP(Enhanced Interior Gateway Routing Protocol)를 사용하는 DMVPN입니다. 이 문서에서는 권장 라우팅 프로토콜인 BGP(Border Gateway Protocol)로의 마이그레이션이 설명되고, 덜 바람직한 EIGRP가 입증됩니다.

사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대한 기본적인 지식을 얻을 것을 권장합니다.

- DMVPN
- FlexVPN

사용되는 구성 요소

> **참고:** 모든 소프트웨어 및 하드웨어가 IKEv2(Internet Key Exchange version 2)를 지원하지는 않습니다. 자세한 내용은 Cisco Feature Navigator를 참조하십시오.

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISR(Integrated Service Router) 버전 15.2(4)M1 이상
- Cisco Aggregation Services Router 1000 Series(ASR1K) 3.6.2 릴리스 15.2(2)S2 이상

최신 플랫폼 및 소프트웨어의 장점 중 하나는 RFC(Request for Comments) 4106에 설명된 대로 IPsec(Internet Protocol Security)에서 암호화를 위해 AES(Advanced Encryption Standard) GCM(Galois/Counter Mode)과 같은 차세대 암호화를 사용하는 기능입니다. AES GCM을 사용하면 일부 하드웨어에서 훨씬 빠른 암호화 속도를 실현할 수 있습니다. Next Generation Cryptography의 사용 및 마이그레이션에 대한 Cisco 권장 사항을 보려면 Next Generation Encryption 문서를 참조하십시오.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

마이그레이션 절차

현재 DMVPN에서 FlexVPN으로 마이그레이션하는 권장 방법은 두 프레임워크가 동시에 작동하지 않는 것입니다. 이 제한은 ASR 3.10 릴리스에 도입되는 새로운 마이그레이션 기능, Cisco 측에서 Cisco 버그 ID CSCuc08066을 포함한 여러 개선 요청을 통해 추적되어 제거될 예정입니다. 이러한 기능은 2013년 6월 말에 사용할 수 있어야 합니다.

동일한 디바이스에서 두 프레임워크가 공존하고 동시에 작동하는 마이그레이션을 **소프트 마이그레이션**이라고 합니다. 즉, 한 프레임워크에서 다른 프레임워크로 미치는 영향이 최소화되고 원활한 장애 조치가 가능함을 나타냅니다. 두 프레임워크에 대한 구성이 공존하지만 동시에 작동하지 않는 마이그레이션을 **하드 마이그레이션이라고 합니다**. 이는 한 프레임워크에서 다른 프레임워크로 전환하면 최소한의 경우에도 VPN을 통한 통신이 부족하다는 것을 의미합니다.

서로 다른 두 허브 간의 하드 마이그레이션

이 문서에서는 현재 새 FlexVPN 허브로 사용되는 DMVPN 허브에서 마이그레이션에 대해 설명합니다. 이 마이그레이션을 통해 이미 FlexVPN으로 마이그레이션된 스포크와 DMVPN에서 계속 실행되며 각 스포크에서 여러 단계로 수행할 수 있는 스포크 간 통신이 가능합니다.

라우팅 정보가 올바르게 입력되어 있는 경우 마이그레이션된 스포크와 마이그레이션되지 않은 스포크 간의 통신은 계속 가능해야 합니다. 그러나 마이그레이션된 스포크와 마이그레이션되지 않은 스포크는 서로 스포크 투 스포크 터널을 구축하지 않으므로 추가 레이턴시를 관찰할 수 있습니다. 그와 동시에 마이그레이션된 스포크는 자체 간에 직접 스포크-스포크 터널을 설정할 수 있어야 합니다. 마이그레이션되지 않은 스포크에도 마찬가지입니다.

이 새로운 마이그레이션 기능을 사용할 수 있을 때까지 DMVPN 및 FlexVPN에서 다른 허브로 마이그레이션을 수행하려면 다음 단계를 완료하십시오.

1. DMVPN을 통한 연결을 확인합니다.
2. FlexVPN 컨피그레이션을 추가하고 새 컨피그레이션에 속하는 터널을 종료합니다.
3. (유지 보수 기간 중) 각 스포크에서 하나씩 DMVPN 터널을 종료합니다.
4. 3단계와 동일한 스포크에서 FlexVPN 터널 인터페이스의 종료를 해제합니다.
5. spoke-to-hub 연결을 확인합니다.
6. FlexVPN 내에서 스포크 대 스포크 연결을 확인합니다.
7. FlexVPN에서 DMVPN을 사용하여 스포크 투 스포크 연결을 확인합니다.
8. 각 스포크에 대해 3단계부터 7단계까지 각각 반복합니다.
9. 5단계, 6 또는 7단계에서 설명한 확인 관련 문제가 발생한 경우 FlexVPN 인터페이스를 종료하고 DMVPN으로 돌아가려면 DMVPN 인터페이스를 종료하십시오.
10. 백업된 DMVPN을 통해 스포크-허브 통신을 확인합니다.
11. 백업된 DMVPN을 통한 스포크 투 스포크 통신을 확인합니다.

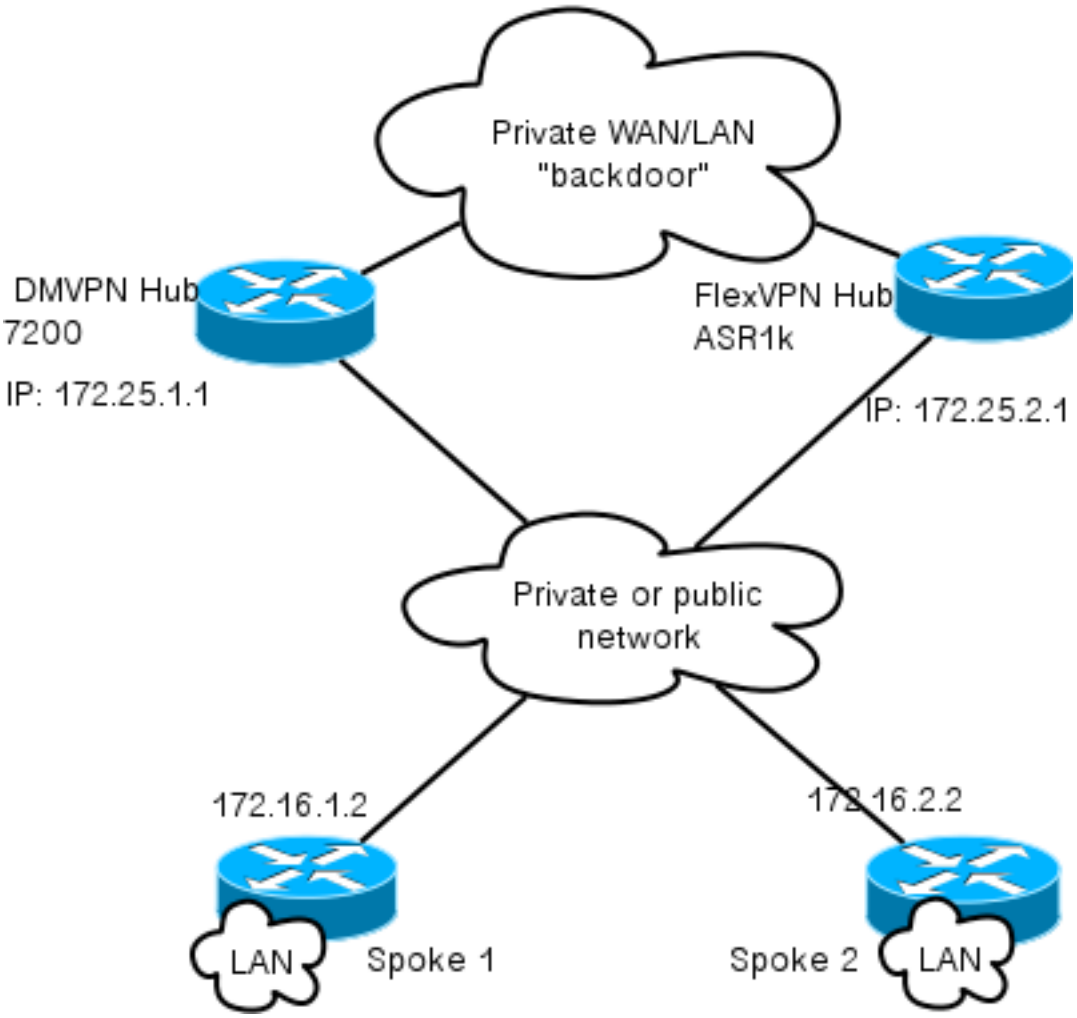
맞춤형 접근 방식

네트워크 또는 라우팅의 복잡성으로 인해 이전 방식이 최상의 솔루션이 아닐 수 있는 경우 마이그레이션하기 전에 Cisco 담당자와 논의를 시작하십시오. 사용자 지정 마이그레이션 프로세스를 논의할 가장 적합한 담당자는 시스템 엔지니어 또는 고급 서비스 엔지니어입니다.

네트워크 토폴로지

전송 네트워크 토폴로지

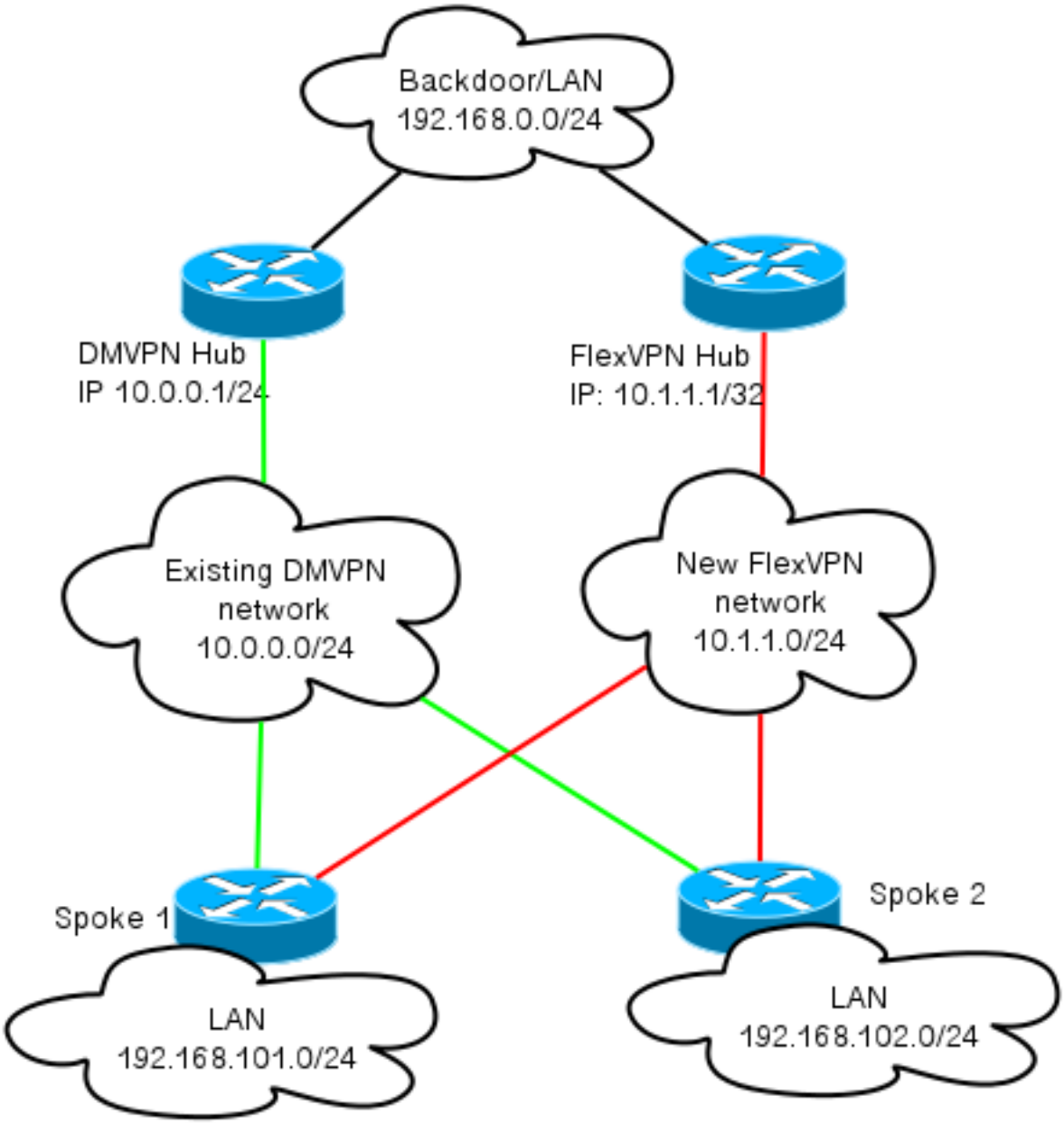
이 다이어그램은 인터넷에 있는 호스트의 일반적인 연결 토폴로지를 보여줍니다. DMVPN IPsec 세션을 종료하기 위해 허브의 **루프백0(172.25.1.1)** IP 주소가 사용됩니다. 새 허브의 IP 주소(**172.25.2.1**)는 FlexVPN에 사용됩니다.



두 허브 간의 링크를 확인합니다. 이 링크는 마이그레이션 중에 FlexVPN과 DMVPN 클라우드 간의 연결을 허용하려면 매우 중요합니다. 또한 이미 FlexVPN으로 마이그레이션된 스포크가 DMVPN 네트워크와 통신하거나 그 반대로 통신할 수 있습니다.

오버레이 네트워크 토폴로지

이 토폴로지 다이어그램은 오버레이에 사용되는 두 개의 개별 클라우드를 보여줍니다. DMVPN(녹색 연결) 및 FlexVPN(빨간색 연결) 해당 사이트에 대한 LAN 접두사가 표시됩니다. **10.1.1.0/24** 서브넷은 인터페이스 주소 지정 측면에서 실제 서브넷을 나타내지 않지만 FlexVPN 클라우드 전용 IP 공간 청크를 나타냅니다. 이에 대한 근거에 대해서는 FlexVPN 컨피그레이션 섹션의 뒷부분**에서** 설명합니다.



구성

이 섹션에서는 DMVPN 및 FlexVPN 컨피그레이션에 대해 설명합니다.

DMVPN 컨피그레이션

이 섹션에서는 DMVPN 허브 및 스포크의 기본 컨피그레이션에 대해 설명합니다.

PSK(Pre-Shared Key)는 IKEv1 인증에 사용됩니다. IPsec이 설정되면 허브가 스포크의 NBMA(Nonbroadcast Multiaccess) 주소를 동적으로 학습할 수 있도록 spoke-to-hub에서 NHRP(Next Hop Resolution Protocol) 등록이 수행됩니다.

NHRP가 스포크와 허브에 대해 등록을 수행하면 라우팅 인접성이 설정되고 경로가 교환될 수 있습니다. 이 예에서 EIGRP는 오버레이 네트워크의 기본 라우팅 프로토콜로 사용됩니다.

스포크 DMVPN 컨피그레이션

여기서는 PSK 인증을 사용하는 DMVPN 및 라우팅 프로토콜로 EIGRP의 기본 컨피그레이션의 예를 확인할 수 있습니다.

```
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 **172.25.1.1**의 IP 주소를 가진 **loopback0**에서 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 IKEv2는 IPsec SA(Security Associations)를 협상하기 위해 IKEv1 대신 사용됩니다. IKEv2는 보호된 데이터 채널을 설정하기 위해 필요한 메시지 수 및 복원력 등 IKEv1보다 향상된 기능을 제공합니다.

- **GRE :** DMVPN과 달리 정적 및 동적 포인트-투-포인트 인터페이스가 사용되며 고정 다중 지점 GRE 인터페이스가 하나만 사용됩니다. 이 컨피그레이션을 사용하면 특히 스포크당/허브당 동작에 유연성을 추가할 수 있습니다.

- **NHRP**: FlexVPN에서 NHRP는 주로 스포크 간 통신을 설정하기 위해 사용됩니다. 스포크는 허브에 등록되지 않습니다.

- **라우팅**: 스포크는 허브에 대한 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 라우팅 정보를 소개하기 위해 IPsec을 사용할 수 있습니다. 기본값은 터널의 다른 쪽에 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(Virtual Routing and Forwarding) - VRF 분리를 통해 유연성을 높일 수 있지만 여기서는 다루지 않습니다(선택 사항).

Spoke FlexVPN 구성

FlexVPN의 스포크 컨피그레이션과 DMVPN의 차이점 중 하나는 두 개의 인터페이스가 있을 가능성이 있다는 것입니다. 스포크 투 허브 통신에는 필수 터널이 있으며 스포크 투 스포크 터널에는 선택적 터널이 있습니다. 동적 스포크 투 스포크 터널링을 사용하지 않도록 선택하고 모든 것이 허브 디바이스를 통과하도록 하려면 가상 템플릿 인터페이스를 제거하고 터널 인터페이스에서 NHRP 바로 가기 스위칭을 제거할 수 있습니다.

고정 터널 인터페이스는 협상을 기반으로 IP 주소를 수신합니다. 이를 통해 허브는 FlexVPN 클라우드에서 정적 주소 지정을 생성하지 않고도 스포크에 터널 인터페이스 IP 주소를 동적으로 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
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
```

> **참고:** 기본적으로 로컬 ID는 IP 주소를 사용하도록 설정됩니다. 따라서 피어의 해당 match 문은 주소도 기준으로 일치해야 합니다. 인증서의 DN(Distinguished Name)을 기반으로 일치 하는 요구 사항이 있는 경우 인증서 맵을 사용하여 일치 작업을 수행해야 합니다.

AES GCM을 지원하는 하드웨어와 함께 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 172.25.2.1
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
```

PKI(Public Key Infrastructure)는 IKEv2에서 대규모 인증을 수행하는 권장 방법입니다. 그러나 PSK의 제한을 알고 있는 한 계속 사용할 수 있습니다.

다음은 **cisco**를 PSK로 사용하는 컨피그레이션의 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
virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

FlexVPN 허브 구성

일반적으로 허브는 동적 스포크 투 허브 터널만 종료합니다. 따라서 허브 컨피그레이션에서 FlexVPN에 대한 고정 터널 인터페이스를 찾을 수 없습니다. 대신 가상 템플릿 인터페이스가 사용됩니다.

참고: 허브 측에서 스포크에 할당할 풀 주소를 지정해야 합니다.

이 풀의 주소는 라우팅 테이블에서 각 스포크에 대한 **/32** 경로로서 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
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
```

AES GCM을 지원하는 하드웨어와 함께 사용하는 것이 좋습니다.

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

참고: 이 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 172.25.2.1 255.255.255.255
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
```

IKEv2에서 인증을 사용하는 경우 스포크의 경우와 동일한 원칙이 허브에 적용됩니다. 확장성과 유연성을 위해 인증서를 사용하십시오. 그러나 PSK에 대해 스포크와 동일한 컨피그레이션을 다시 사용할 수 있습니다.

> **참고:** IKEv2는 인증 측면에서 유연성을 제공합니다. 한 쪽은 PSK를 인증할 수 있고 다른 쪽은 RSA-SIG(Rivest-Shamir-Adleman Signature)를 사용합니다.

인증에 사전 공유 키를 사용해야 하는 경우 컨피그레이션 변경 사항은 여기에서 스포크 라우터에 대해 설명한 것과 유사합니다.

Inter-Hub BGP 연결

허브가 특정 접두사의 위치를 알고 있는지 확인합니다. 일부 스포크가 FlexVPN으로 마이그레이션된 반면 다른 스포크는 DMVPN에 남아 있기 때문에 이 점이 점점 중요해지고 있습니다.

다음은 DMVPN 허브 컨피그레이션을 기반으로 하는 인터허브 BGP 연결입니다.

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

트래픽 마이그레이션

오버레이 라우팅 프로토콜로 BGP로 마이그레이션 [권장]

BGP는 유니캐스트 교환을 기반으로 하는 라우팅 프로토콜입니다. 이러한 특성 때문에 DMVPN 네트워크에서 최상의 확장 프로토콜입니다.

이 예에서는 iBGP(Internal BGP)가 사용됩니다.

Spoke BGP 컨피그레이션

Spoke 마이그레이션은 두 부분으로 구성됩니다. 먼저 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(다음 섹션 참조) BGP를 통한 새 접두사를 학습한 후 현재 DMVPN 클라우드에서 새 FlexVPN 클라우드로 트래픽을 스윙할 수 있습니다.

허브 BGP 컨피그레이션

FlexVPN 허브 - 전체 BGP 컨피그레이션

허브에서 각 스포크의 인접 컨피그레이션을 별도로 유지하지 않도록 동적 리스너를 구성합니다. 이 설정에서 BGP는 새 연결을 시작하지 않지만 제공된 IP 주소 풀의 연결을 허용합니다. 이 경우 해당 풀은 **10.1.1.0/24**이며, 이는 새 FlexVPN 클라우드의 모든 주소입니다.

두 가지 요점:

- FlexVPN 허브는 특정 접두사를 DMVPN 허브에 알립니다. unsupress 맵이 사용되고 있습니다.
- **10.1.1.0/24**의 FlexVPN 서브넷을 라우팅 테이블에 알리거나 DMVPN 허브가 FlexVPN 허브를 다음 홉으로 인식하는지 확인합니다.

이 문서에서는 후자의 접근 방식을 보여줍니다.

```
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
```

DMVPN 허브 - 전체 BGP 및 EIGRP 컨피그레이션

DMVPN 허브의 컨피그레이션은 기본입니다. FlexVPN 허브에서 특정 접두사만 수신하고 EIGRP에서 학습한 접두사를 광고하기 때문입니다.

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

BGP/FlexVPN으로 트래픽 마이그레이션

앞서 설명한 대로 마이그레이션을 수행하려면 DMVPN 기능을 종료하고 FlexVPN을 가동해야 합니다.

이 절차는 다음과 같은 최소 영향을 보장합니다.

1. 각 스포크에서 별도로 다음을 입력합니다.

```
interface tunnel 0
 shut
```

   이 시점에서 이 스포크에 설정된 IKEv1 세션이 없는지 확인합니다. 이는 **show crypto isakmp sa** 명령의 출력을 확인하고 crypto logging session 명령에 의해 생성된 syslog 메시지를 모니터링하는 경우에 확인할 수 있습니다. 확인되면 FlexVPN을 계속 사용할 수 있습니다.

2. 동일한 스포크에서 다음을 입력합니다.

```
interface tunnel 1
  no shut
```

확인 단계

IPsec 안정성

IPsec 안정성을 평가하는 가장 좋은 방법은 crypto logging session configuration 명령을 활성화하여 **syslog**를 모니터링하는 것입니다. 세션이 작동 및 중단되는 경우, 마이그레이션을 시작하기 전에 수정해야 하는 IKEv2/FlexVPN 레벨의 문제를 나타낼 수 있습니다.

BGP 정보 입력

IPsec이 안정적인 경우 BGP 테이블이 스포크의 항목(허브의 항목)과 허브의 요약(스포크의 요약)으로 채워졌는지 확인합니다. BGP의 경우 다음 명령으로 볼 수 있습니다.

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

다음은 FlexVPN 허브의 올바른 정보의 예입니다.

```
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
```

이 출력은 허브가 각 스포크에서 하나의 접두사를 학습했으며, 두 스포크는 모두 동적이며 별표(*) 기호로 표시되어 있음을 보여줍니다. 또한 인터허브 연결에서 총 4개의 접두사가 수신되었음을 보여줍니다.

다음은 스포크의 유사 정보의 예입니다.

```
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
```

스포크가 허브에서 두 개의 접두사를 받았습니다. 이 설정의 경우 FlexVPN 허브에서 광고되는 요약에는 접두사 하나가 포함되어야 합니다. 또 다른 하나는 DMVPN 스포크에서 BGP로 재배포된 DMVPN 10.0.0.0/24 네트워크입니다.

EIGRP를 사용하여 새 터널로 마이그레이션

EIGRP는 비교적 간단한 구축 및 빠른 컨버전스로 인해 DMVPN 네트워크에서 널리 사용되는 옵션입니다. 그러나 BGP보다 더 크게 확장되며, BGP에서 즉시 사용할 수 있는 많은 고급 메커니즘을 제공하지 않습니다. 다음 섹션에서는 새로운 EIGRP 프로세스를 사용하여 FlexVPN으로 이동하는 방법 중 하나를 설명합니다.

스포크 구성 업데이트

별도의 EIGRP 프로세스로 새로운 AS(Autonomous System)가 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 투 스포크 터널을 통해 라우팅 프로토콜 인접성을 설정하지 않는 것이 가장 좋습니다. 따라서 tunnel1의 인터페이스만 패시브가 되도록 합니다(spoke-to-hub).

업데이트된 FlexVPN 허브 구성

마찬가지로 FlexVPN 허브의 경우, 스포크에 구성된 라우팅 프로토콜을 일치시켜 해당 AS에서 라우팅 프로토콜을 준비합니다.

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

스포크에 대한 요약을 다시 제공하기 위해 두 가지 방법이 사용됩니다.

- null0을 가리키는 고정 경로를 재배포합니다(기본 설정 옵션).

```
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
```

이 옵션을 사용하면 허브의 VT(Virtualization Technology) 컨피그레이션을 수정하지 않고도 요약 및 재배포를 제어할 수 있습니다. 연결된 활성 가상 액세스가 있는 경우 허브의 VT 컨피그레이션을 수정할 수 없기 때문에 이는 중요합니다.

- 가상 템플릿에 DMVPN 스타일 요약 주소를 설정합니다.

  각 가상 액세스에 대한 내부 처리 및 해당 요약의 복제 때문에 이 컨피그레이션은 *권장되지 않습니다*. 참고로 여기 나와 있습니다

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

고려해야 할 또 다른 측면은 인터허브 라우팅 교환입니다. EIGRP 인스턴스를 iBGP에 재배포하는 경우 이 작업을 수행할 수 있습니다.

DMVPN 허브 - 업데이트된 BGP 컨피그레이션

컨피그레이션은 기본 상태로 유지됩니다. EIGRP에서 BGP로 특정 접두사를 재배포해야 합니다.

```
router bgp 65001

redistribute eigrp 100

neighbor 192.168.0.2 remote-as 65001
```

FlexVPN 허브 - 업데이트된 BGP 컨피그레이션

FlexVPN에서 DMVPN 허브와 비슷하게 새 EIGRP 프로세스의 접두사를 BGP에 재배포해야 합니다
.

```
router bgp 65001

 redistribute eigrp 200 redistribute static

 neighbor 192.168.0.1 remote-as 65001
```

FlexVPN으로 트래픽 마이그레이션

마이그레이션을 수행하려면 DMVPN 기능을 종료하고 각 스포크에서 FlexVPN을 한 번에 하나씩 가동해야 합니다. 이 절차는 최소 영향을 보장합니다.

1. 각 스포크에서 별도로 다음을 입력합니다.

```
interface tunnel 0
 shut
```

   이 시점에서 이 스포크에 설정된 IKEv1 세션이 없는지 확인합니다. 이는 **show crypto isakmp sa** 명령의 출력을 확인하고 crypto logging session 명령에 의해 생성된 syslog 메시지를 모니터링하는 경우에 확인할 수 있습니다. 확인되면 FlexVPN을 계속 사용할 수 있습니다.
2. 동일한 스포크에서 다음을 입력합니다.

```
interface tunnel 1
  no shut
```

확인 단계

IPsec 안정성

BGP의 경우와 마찬가지로 IPsec이 안정적인지 평가해야 합니다. 가장 좋은 방법은 crypto logging session configuration 명령을 활성화하여 syslog를 모니터링하는 것입니다. 세션이 작동 및 중단되는 경우 마이그레이션을 시작하기 전에 수정해야 하는 IKEv2/FlexVPN 레벨의 문제를 나타낼 수 있습니다.

토폴로지 테이블의 EIGRP 정보

EIGRP 토폴로지 테이블이 허브의 스포크 LAN 항목과 스포크의 요약에 채워져 있는지 확인합니다. 허브 및 스포크에 이 명령을 입력한 경우 이를 확인할 수 있습니다.

show ip eigrp [AS_NUMBER] topology
다음은 스포크의 출력의 예입니다.

```
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
```

출력은 스포크가 해당 LAN 서브넷(*기/울임체*)과 요약에 대해 알고 있음을 **보여줍니다**.

다음은 허브의 출력의 예입니다.

```
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)
```

그러면 허브가 스포크의 LAN 서브넷(*기울임꼴*), 알리는 요약 접두사(**굵게** 표시) 및 협상을 통해 각 스포크의 할당된 IP 주소에 대해 알고 있는 것으로 표시됩니다.

추가 고려 사항

이미 존재하는 스포크 투 스포크 터널

DMVPN 터널 인터페이스를 종료하면 NHRP 항목이 제거되므로, 이미 존재하는 스포크 투 스포크 터널이 해제됩니다.

NHRP 항목 지우기

FlexVPN 허브는 트래픽을 다시 라우팅하는 방법을 알기 위해 스포크의 NHRP 등록 프로세스에 의존하지 않습니다. 그러나 동적 스포크 투 스포크 터널은 NHRP 항목을 사용합니다.

DMVPN에서 허브의 NHRP가 지워지면 단기간 연결 문제가 발생할 수 있습니다. FlexVPN에서 스포크의 NHRP를 지우면 스포크 투 스포크 터널과 관련된 FlexVPN IPsec 세션이 해제됩니다. 허브에서 NHRP를 지우는 것은 FlexVPN 세션에 영향을 주지 않습니다.

이는 기본적으로 FlexVPN에서 다음을 수행하기 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 투 스포크 트래픽은 Cisco 버그 ID CSCub07382의 영향을 받을 수 있습니다.

관련 정보

- DMVPN에서 FlexVPN으로의 소프트 마이그레이션 컨피그레이션 예
- 기술 지원 및 문서 – Cisco Systems