DMVPN에서 FlexVPN으로의 소프트 마이그레이션 컨피그레이션 예

목차

소개

이 문서에서는 DMVPN(Dynamic Multipoint VPN) 및 FlexVPN이 장치에서 해결 방법 없이 동시에 작동하는 *소프트* 마이그레이션을 수행하는 방법과 컨피그레이션 예를 제공합니다.

> **참고:**이 문서는 FlexVPN [마이그레이션](#)에 설명된 개념을 [확장합니다.동일한 디바이스](#) 및 FlexVPN [마이그레이션에서 DMVPN에서 FlexVPN으로](#) 하드 [이동:Hard Move from DMVPN to FlexVPN on a Different Hub](#) Cisco 기사.이 두 문서는 모두 *하드* 마이그레이션에 대해 설명하며, 이로 인해 마이그레이션 중에 트래픽이 다소 중단됩니다.이러한 문서의 제한 사항은 현재 개선되고 있는 Cisco IOS® 소프트웨어의 결함으로 인한 것입니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- DMVPN
- FlexVPN

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISR(Integrated Service Router) 버전 15.3(3)M 이상
- Cisco 1000 Series ASR1K(Aggregated Service Router) 릴리스 3.10 이상

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

배경 정보

최신 Cisco IOS 플랫폼 및 소프트웨어의 장점 중 하나는 차세대 암호화를 사용하는 기능입니다.예를 들어 RFC 4106에 설명된 대로 IPsec에서 암호화를 위해 GCM(Galois/Counter Mode)에서 AES(Advanced Encryption Standard)를 사용하는 것이 예입니다.AES GCM은 일부 하드웨어에서 훨씬 빠른 암호화 속도를 지원합니다.

> **참고:**차세대 암호화 사용 및 마이그레이션에 대한 자세한 내용은 Next Generation Encryption Cisco 기사를 참조하십시오.

구성

이 컨피그레이션 예제는 DMVPN 3단계 컨피그레이션에서 FlexVPN으로의 마이그레이션에 중점을 둡니다. 두 설계 모두 비슷하게 작동하기 때문입니다.

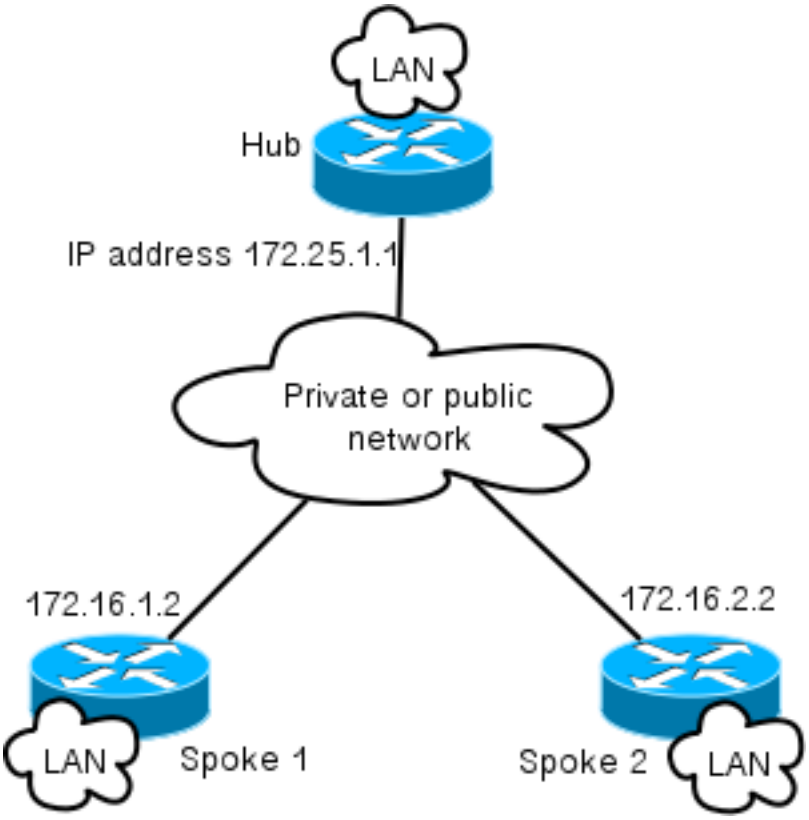
	DMVPN 2단계	DMVPN 3단계	FlexVPN
전송	GRE over IPsec	GRE over IPsec	GRE over IPsec, VTI
NHRP 사용	등록 및 해결	등록 및 해결	해결
스포크의 다음 홉입니다.	기타 스포크 또는 허브	허브의 요약	허브의 요약
NHRP 바로 가기 스위칭	아니요	예	예(선택 사항)
NHRP 리디렉션	아니요	예	예
IKE 및 IPsec	IPsec 옵션, IKEv1 일반	IPsec 옵션, IKEv1 일반	IPsec, IKEv2

네트워크 다이어그램

이 섹션에서는 전송 및 오버레이 네트워크 다이어그램을 모두 제공합니다.

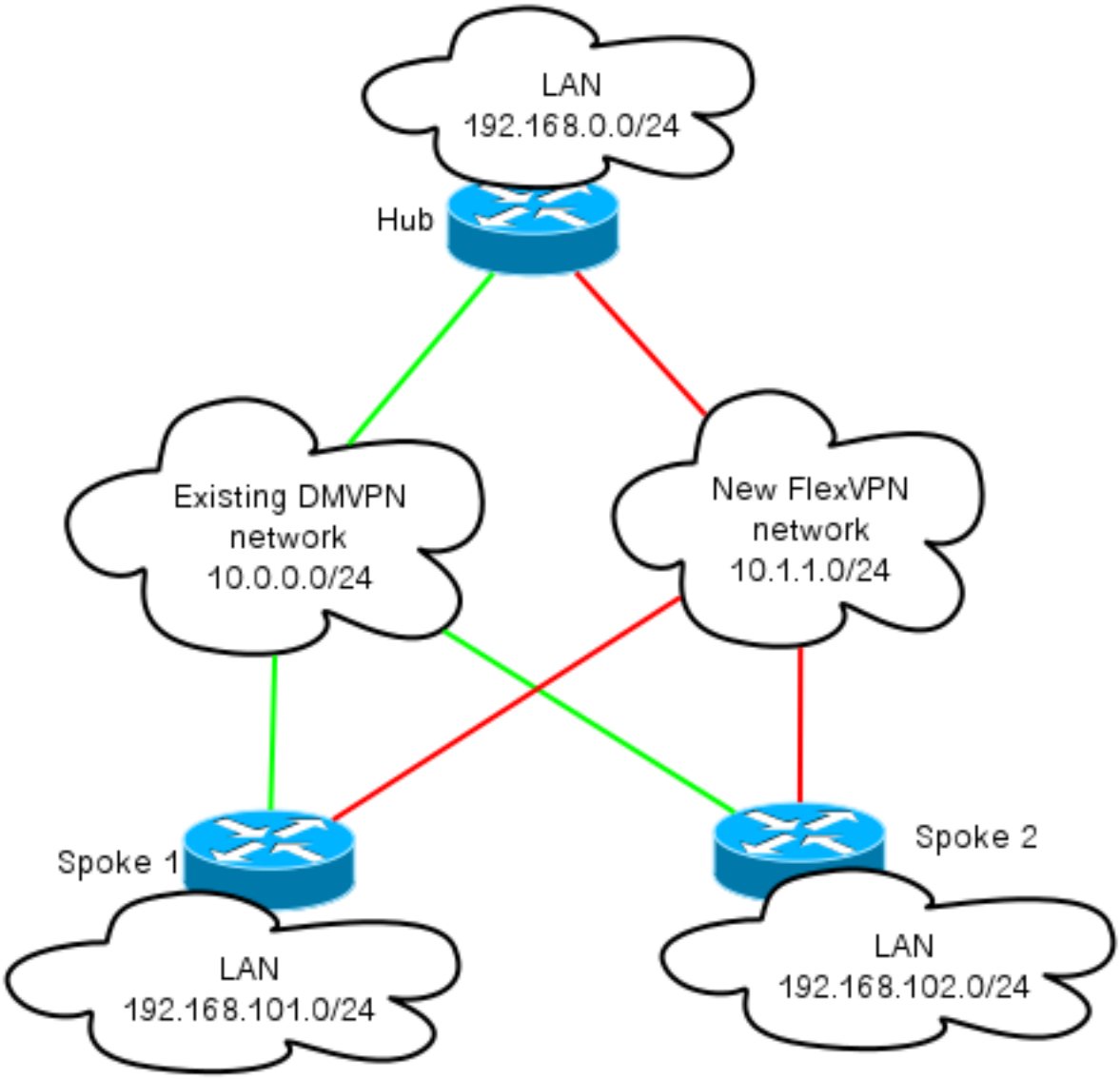
전송 네트워크 다이어그램

이 예에서 사용되는 전송 네트워크에는 두 스포크가 연결된 단일 허브가 포함됩니다.모든 디바이스는 인터넷을 시뮬레이션하는 네트워크를 통해 연결됩니다.



오버레이 네트워크 다이어그램

이 예에서 사용되는 오버레이 네트워크에는 두 스포크가 연결된 단일 허브가 포함됩니다.
DMVPN과 FlexVPN이 동시에 활성화되지만 서로 다른 IP 주소 공간을 사용합니다.



구성

이 구성은 EIGRP(Enhanced Interior Gateway Routing Protocol)를 통해 DMVPN 단계 3의 가장 인기 있는 배포를 BGP(Border Gateway Protocol)가 있는 FlexVPN으로 마이그레이션합니다. Cisco에서는 구축을 더 효과적으로 확장할 수 있도록 하기 때문에 FlexVPN에 BGP를 사용하는 것이 좋습니다.

> **참고:**허브는 동일한 IP 주소에서 IKEv1(DMVPN) 및 IKEv2(FlexVPN) 세션을 종료합니다.이는 최신 Cisco IOS 릴리스에서만 가능합니다.

스포크 구성

이는 IKEv1과 IKEv2의 상호 연동을 허용하는 두 가지 특별한 예외와 함께 전송을 위해 IPsec을 통한 GRE(Generic Routing Encapsulation)를 사용하는 두 프레임워크를 함께 사용하는 매우 기본적인 구성입니다.

> **참고:**ISAKMP(Internet Security Association and Key Management Protocol) 및 IKEv2 컨피그레이션의 관련 변경 사항은 굵게 강조 표시됩니다.

```
crypto keyring DMVPN_IKEv1
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco

crypto logging session

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

crypto isakmp policy 10
encr aes
authentication pre-share

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

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

interface Tunnel0
 desciption DMVPN tunnel
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 key 0
tunnel protection ipsec profile DMVPN_IKEv1 isakmp-profile DMVPN_IKEv1

interface Tunnel1
description FlexVPN spoke-to-hub tunnel
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
tunnel source Ethernet0/0
tunnel destination 172.25.1.1
 tunnel protection ipsec profile default ikev2-profile Flex_IKEv2
```

```
interface Virtual-Template1 type tunnel
description FlexVPN spoke-to-spoke
ip unnumbered Ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel protection ipsec profile default ikev2-profile Flex_IKEv2
```

Cisco IOS Release 15.3을 사용하면 IKEv2 및 ISAKMP 프로필을 *터널 보호* 구성에 결합할 수 있습니다. 코드에 대한 일부 내부 변경과 함께 IKEv1 및 IKEv2가 동일한 장치에서 동시에 작동할 수 있습니다.

Cisco IOS가 15.3 이전 릴리스에서 프로파일(IKEv1 또는 IKEv2)을 선택하는 방식 때문에 IKEv1이 피어를 통해 IKEv2로 시작되는 상황과 같은 몇 가지 경고가 발생했습니다.이제 IKE의 분리는 새로운 CLI를 통해 구현되는 인터페이스 레벨이 아니라 프로필 레벨을 기반으로 합니다.

새로운 Cisco IOS 릴리스의 또 다른 업그레이드는 *터널 키* 추가입니다.DMVPN과 FlexVPN은 동일한 소스 인터페이스와 동일한 대상 IP 주소를 사용하기 때문에 이 기능이 필요합니다.이 경우 GRE 터널에서 트래픽을 역캡슐화하기 위해 어떤 터널 인터페이스를 사용하는지 알 수 있는 방법은 없습니다.터널 키를 사용하면 작은(4바이트) 오버헤드를 추가하여 **tunnel0** 및 **tunnel1**을 구별할 수 있습니다. 두 인터페이스에서 다른 키를 구성할 수 있지만 일반적으로 하나의 터널을 구별하기만 하면 됩니다.

> **참고:**DMVPN 및 FlexVPN이 동일한 인터페이스를 공유하는 경우 공유 터널 보호 옵션이 필요하지 않습니다.

따라서 스포크 라우팅 프로토콜 컨피그레이션은 기본입니다.EIGRP와 BGP는 별도로 작동합니다. EIGRP는 확장성을 제한하는 스포크 투 스포크 터널을 통한 피어링을 방지하기 위해 터널 인터페이스만 광고합니다. BGP는 로컬 네트워크(**192.168.101.0/24**)를 알리기 위해 허브 라우터(**10.1.1.1**)와의 관계만 유지합니다.

```
router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.101.0
passive-interface default
no passive-interface Tunnel0

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

허브 구성

Spoke Configuration(스포크 컨피그레이션) 섹션에 설명된 것과 마찬가지로 허브 측 컨피그레이션

에서 유사한 변경을 수행해야 합니다.

참고:ISAKMP 및 IKEV2 구성에 대한 관련 변경 사항은 굵게 강조 표시됩니다.

```
crypto ikev2 authorization policy default
pool FlexSpokes
route set interface

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

crypto isakmp policy 10
encr aes
authentication pre-share

crypto isakmp key cisco address 0.0.0.0


crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

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 key 0
 tunnel protection ipsec profile DMVPN_IKEv1

interface Virtual-Template1 type tunnel
ip unnumbered Loopback100
ip mtu 1400
 ip nhrp network-id 2
ip tcp adjust-mss 1360
 tunnel protection ipsec profile default
```

허브 측에서 IKE 프로파일과 IPsec 프로파일 간의 바인딩은 스포크 컨피그레이션과 달리 프로파일

레벨에서 발생합니다. 여기서 **tunnel protection** 명령을 통해 이가 완료됩니다. 두 방법 모두 이 바인딩을 완료하는 실행 가능한 방법입니다.

NHRP(Next Hop Resolution Protocol) 네트워크 ID는 클라우드의 DMVPN 및 FlexVPN에 대해 다릅니다.대부분의 경우 NHRP가 두 프레임워크를 통해 단일 도메인을 생성하는 경우에는 바람직하지 않습니다.

터널 키는 Spoke Configuration(스포크 컨피그레이션) 섹션에서 언급한 동일한 목표를 달성하기 위해 GRE 레벨에서 DMVPN 및 FlexVPN 터널을 **구별합니다**.

허브의 라우팅 컨피그레이션은 상당히 기본적입니다.허브 디바이스는 EIGRP를 사용하는 스포크와 BGP를 사용하는 스포크와 두 개의 관계를 유지 관리합니다. BGP 컨피그레이션은 대기 중인 스포크당 컨피그레이션을 방지하기 위해 수신 범위를 사용합니다.

요약 주소가 두 번 도입되었습니다.EIGRP 구성은 **tunnel0 구성**(IP summary-address EIGRP 100)을 사용하여 요약을 전송하고 BGP는 집계 주소를 사용하여 요약을 생성합니다. NHRP 리디렉션이 발생하는지 확인하고 라우팅 업데이트를 간소화하기 위해 요약이 필요합니다. NHRP 리디렉션이 더 나은 ICMP(Internet Control Message Protocol) 홉이 있는지 여부를 나타내는 NHRP 리디렉션을 보낼 수 있습니다. 지정된 대상 - 스포크 대 스포크 터널을 설정할 수 있습니다. 이러한 요약은 허브와 각 스포크 간에 전송되는 라우팅 업데이트의 양을 최소화하기 위해 사용되므로 설정을 더 효과적으로 확장할 수 있습니다.

```
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

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

다음을 확인합니다.

이 컨피그레이션 예제의 확인은 여러 섹션으로 구분되어 있습니다.

마이그레이션 전 확인

DMVPN/EIGRP 및 FlexVPN/BGP가 동시에 작동하므로 스포크가 IKEv1 및 IKEv2와 IPsec을 통해 관계를 유지하고 적절한 접두사가 EIGRP 및 BGP를 통해 학습되는지 확인해야 합니다.

이 예에서 **Spoke1**은 두 세션이 허브 라우터와 유지 관리됨을 보여줍니다.하나는 IKEv1/**Tunnel0**을 사용하고 다른 하나는 IKEv2/**Tunnel1을 사용합니다**.

> **참고:**각 터널에 대해 2개의 IPsec SA(Security Associations)(인바운드 1개와 아웃바운드 1개)가 유지됩니다.

```
Spoke1#show cry sess
Crypto session current status

Interface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto map

Interface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
 IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

라우팅 프로토콜을 확인할 때 인접 라우터가 구성되었는지, 올바른 접두사가 학습되었는지 확인해야 합니다. 이는 EIGRP에서 먼저 확인합니다.허브가 네이버로 표시되고 192.168.0.0/16 주소(요약)가 허브에서 학습되는지 확인합니다.

```
Spoke1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.0.0.1 Tu0 10 00:04:02 7 1398 0 13

Spoke1#show 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

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 26880000
via 10.0.0.1 (26880000/256), Tunnel0
P 10.0.0.0/24, 1 successors, FD is 26880000
via Connected, Tunnel0
```

다음으로 BGP를 확인합니다.

```
Spoke1#show bgp summary
(...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 13 11 3 0 0 00:06:56 1
Spoke1#show bgp
BGP table version is 3, local router ID is 192.168.101.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
```

```
Network Next Hop Metric LocPrf Weight Path
r>i 192.168.0.0/16 10.1.1.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
```

출력에서는 허브 FlexVPN IP 주소(10.1.1.1)가 스포크가 하나의 접두사(192.168.0.0/16)를 수신하는 인접 디바이스임을 보여줍니다. 또한 BGP는 192.168.0.0/16 접두사에 대해 RIB(Routing Information Base) 오류가 발생했음을 관리자에게 알립니다.이 오류는 라우팅 테이블에 이미 존재하는 접두사에 대해 더 나은 경로가 있기 때문에 발생합니다.이 경로는 EIGRP에서 시작되며 라우팅 테이블을 확인하면 확인할 수 있습니다.

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
 Known via "eigrp 100", distance 90, metric 26880000, type internal
Redistributing via eigrp 100
Last update from 10.0.0.1 on Tunnel0, 00:10:07 ago
Routing Descriptor Blocks:
* 10.0.0.1, from 10.0.0.1, 00:10:07 ago, via Tunnel0
Route metric is 26880000, traffic share count is 1
Total delay is 50000 microseconds, minimum bandwidth is 100 Kbit
Reliability 255/255, minimum MTU 1400 bytes
Loading 1/255, Hops 1
```

마이그레이션

이전 섹션에서는 IPsec 및 라우팅 프로토콜이 모두 구성되었으며 예상대로 작동하는지 확인했습니다.동일한 디바이스에서 DMVPN에서 FlexVPN으로 마이그레이션할 수 있는 가장 쉬운 방법 중 하나는 AD(관리 거리)를 변경하는 것입니다. 이 예에서 iBGP(내부 BGP)는 AD가 200이고, EIGRP는 AD가 90입니다.

FlexVPN을 통해 트래픽이 제대로 전달되려면 BGP에 더 나은 AD가 있어야 합니다. 이 예에서 EIGRP AD는 내부 및 외부 경로의 경우 각각 230 및 240으로 변경됩니다. 이렇게 하면 192.168.0.0/16 접두사에 BGP AD(2000)가 더 적합합니다.

이를 위해 사용되는 또 다른 방법은 BGP AD를 줄이는 것입니다.그러나 마이그레이션 후에 실행되는 프로토콜에 기본값이 아닌 값이 있으므로 구축의 다른 부분에 영향을 줄 수 있습니다.

이 예에서는 debug ip routing 명령을 사용하여 스포크의 작업을 확인합니다.

> **참고:**이 섹션의 정보가 프로덕션 네트워크에서 사용되는 경우 debug 명령을 사용하지 말고 다음 섹션에 나열된 show 명령을 사용합니다. 또한 스포크 EIGRP 프로세스는 허브와 인접성을 재설정해야 합니다.

```
Spoke1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Spoke1(config)#router eigrp 100
Spoke1(config-router)# distance eigrp 230 240
Spoke1(config-router)#^Z
Spoke1#
*Oct 9 12:12:34.207: %SYS-5-CONFIG_I: Configured from console by console
*Oct 9 12:12:43.648: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is down: route configuration changed

*Oct 9 12:12:43.648: RT: delete route to 192.168.0.0 via 10.0.0.1,
 eigrp metric [90/26880000]
*Oct 9 12:12:43.648: RT: no routes to 192.168.0.0, delayed flush
```

```
*Oct 9 12:12:43.648: RT: delete network route to 192.168.0.0/16
*Oct 9 12:12:43.650: RT: updating bgp 192.168.0.0/16 (0x0) :
via 10.1.1.1

*Oct 9 12:12:43.650: RT: add 192.168.0.0/16 via 10.1.1.1, bgp metric [200/0]
Spoke1#
*Oct 9 12:12:45.750: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is up: new adjacency
```

이 출력에는 다음 세 가지 중요한 작업이 있습니다.

- 스포크는 AD가 변경되었음을 알리고 인접성을 비활성화합니다.
- 라우팅 테이블에서 EIGRP 접두사가 검색되고 BGP가 도입됩니다.
- EIGRP를 통한 허브에 대한 인접성이 다시 온라인 상태가 됩니다.

디바이스에서 AD를 변경하면 디바이스에서 다른 네트워크로 가는 경로만 영향을 받습니다.다른 라우터가 라우팅을 수행하는 방식에는 영향을 주지 않습니다.예를 들어 EIGRP 거리가 **Spoke1**에서 증가하면(트래픽을 라우팅하기 위해 클라우드에서 FlexVPN을 사용) 허브는 구성된(기본) AD를 유지합니다.즉, 트래픽을 다시 **Spoke1**으로 라우팅하기 위해 DMVPN을 **사용합니다**.

특정 시나리오에서는 방화벽이 동일한 인터페이스에서 반환 트래픽을 예상하는 경우와 같은 문제가 발생할 수 있습니다. 따라서 허브에서 AD를 변경하기 전에 모든 스포크의 AD를 변경해야 합니다.트래픽은 FlexVPN에 의해 완전히 마이그레이션됩니다. 이 작업이 완료되면 됩니다.

EIGRP-EIGRP 마이그레이션

EIGRP만 실행하는 DMVPN에서 FlexVPN으로의 마이그레이션은 이 문서에서 자세히 다루지 않습니다.그러나 완전성을 위해 여기에도 언급되어 있습니다.

동일한 EIGRP 자동 시스템(AS) 라우팅 인스턴스에 DMVPN과 EIGRP를 모두 추가할 수 있습니다. 이 경우 라우팅 인접성이 두 가지 유형의 클라우드에 모두 설정됩니다. 이로 인해 로드 밸런싱이 발생할 수 있으며 일반적으로 권장되지 않습니다.

FlexVPN 또는 DMVPN을 선택하려면 관리자가 인터페이스별로 서로 다른 **지연** 값을 할당할 수 있습니다. 그러나 가상 템플릿 인터페이스에는 해당 가상 액세스 인터페이스가 있는 동안 변경이 불가능하다는 점에 유의해야 합니다.

마이그레이션 후 검사

Pre-Migration Checks 섹션에 사용된 프로세스와 마찬가지로 IPsec 및 라우팅 프로토콜을 확인해야 합니다.

먼저 IPsec을 확인합니다.

```
Spoke1#show crypto session
Crypto session current status

Interface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
```

```
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto map

Interface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

전과 같이 두 개의 세션이 표시되며, 두 세션 모두 두 개의 활성 IPsec SA를 갖습니다.

스포크에서 종합 경로(192.168.0.0/16)는 허브에서 시작되며 BGP를 통해 학습됩니다.

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
Known via "bgp 65001", distance 200, metric 0, type internal
Last update from 10.1.1.1 00:14:07 ago
Routing Descriptor Blocks:
* 10.1.1.1, from 10.1.1.1, 00:14:07 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none
```

마찬가지로, 허브에 접두사가 붙은 스포크 LAN은 EIGRP를 통해 알려져야 합니다. 이 예에서는 Spoke2 LAN 서브넷을 확인합니다.

```
Hub#show ip route 192.168.102.0 255.255.255.0
Routing entry for 192.168.102.0/24
 Known via "bgp 65001", distance 200, metric 0, type internal
Last update from 10.1.1.106 00:04:35 ago
Routing Descriptor Blocks:
* 10.1.1.106, from 10.1.1.106, 00:04:35 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none

Hub#show ip cef 192.168.102.100
192.168.102.0/24
nexthop 10.1.1.106 Virtual-Access2
```

출력에서 포워딩 경로가 올바르게 업데이트되고 가상 액세스 인터페이스를 벗어납니다.

추가 고려 사항

이 섹션에서는 이 컨피그레이션 예와 관련된 몇 가지 중요한 추가 영역에 대해 설명합니다.

기존 스포크-스포크 터널

EIGRP에서 BGP로 마이그레이션하면 바로 가기 스위칭이 여전히 작동하므로 스포크 투 스포크 터널에 영향을 주지 않습니다. 스포크의 바로 가기 스위칭은 AD가 250인 보다 구체적인 NHRP 경로를 삽입합니다.

다음은 이러한 경로의 예입니다.

```
Spoke1#show ip route 192.168.102.100
Routing entry for 192.168.102.0/24
Known via "nhrp", distance 250, metric 1
Last update from 10.1.1.106 on Virtual-Access1, 00:00:42 ago
Routing Descriptor Blocks:
* 10.1.1.106, from 10.1.1.106, 00:00:42 ago, via Virtual-Access1
Route metric is 1, traffic share count is 1
```

마이그레이션된 스포크와 마이그레이션되지 않은 스포크 간 통신

FlexVPN/BGP에 이미 있는 스포크가 마이그레이션 프로세스가 시작되지 않은 디바이스와 통신하려는 경우 트래픽은 항상 허브를 통해 이동합니다.

이 프로세스는 다음과 같이 이루어집니다.

1. 스포크는 대상에 대해 경로 조회를 수행하며, 이 경로는 허브에서 광고하는 요약 경로를 가리킵니다.
2. 패킷이 허브로 전송됩니다.
3. 허브는 패킷을 수신하고 대상에 대한 경로 조회를 수행하며, 이는 다른 NHRP 도메인에 속한 다른 인터페이스를 가리킵니다.

참고:이전 허브 컨피그레이션의 NHRP 네트워크 ID는 FlexVPN과 DMVPN에 모두 다릅니다. NHRP 네트워크 ID가 통합된 경우에도 마이그레이션된 스포크가 FlexVPN 네트워크를 통해 객체를 라우팅하는 경우에 문제가 발생할 수 있습니다.여기에는 바로 가기 스위칭을 구성하는 데 사용되는 지시어가 포함됩니다.마이그레이션되지 않은 스포크는 바로 가기 스위칭을 수행하는 특정 목표에 따라 DMVPN 네트워크를 통해 개체를 실행하려고 시도합니다.

문제 해결

이 섹션에서는 마이그레이션을 해결하기 위해 일반적으로 사용되는 두 가지 카테고리에 대해 설명합니다.

터널 설정 시도 문제

IKE 협상이 실패할 경우 다음 단계를 완료합니다.

1. 다음 명령을 사용하여 현재 상태를 확인합니다.

show crypto isakmp sa - 이 명령은 IKEv1 세션의 양, 소스 및 대상을 표시합니다.**show crypto ipsec sa** - 이 명령은 IPsec SA의 활동을 표시합니다.**참고:**IKEv1과 달리 이 출력에서는 PFS(Perfect Forward Secrecy) DH(Diffie-Hellman) 그룹 값이 PFS**(Y/N)로** 나타납니다.**N, DH 그룹:**첫 번째 터널 협상 중 **없음**그러나 rekey가 발생하면 올바른 값이 나타납니다 .CSCug67056에서 동작에 대해 설명하지만 이는 버그가 아닙니다. IKEv1과 IKEv2의 차이점은 후자의 하위 SA가 **AUTH** 교환의 일부로 생성된다는 것입니다.암호화 맵에서 구성된 DH 그룹은 키 재설정 중에만 사용됩니다.따라서 PFS**(Y/N)가 표시됩니다.N, DH 그룹:**첫 번째 키 다시 **키**가 올 때까지 없음IKEv1에서는 Child SA가 빠른 모드 중에 생성되고 CREATE_**CHILD_SA** 메시지는 새 공유 암호를 파생시키기 위해 DH 매개변수를 지정하는 Key Exchange 페이로드의 변환에 대한 프로비저닝을 가지고 있기 때문에 다른 동작이 표시됩니다.**show crypto ikev2 sa** - 이 명령은 ISAKMP와 유사하지만 IKEv2와 관련된 출력을 제공합니다.**show crypto session** - 이 명령은

이 디바이스에서 암호화 세션의 요약 출력을 제공합니다.**show crypto socket** - 이 명령은 crypto-sockets 상태를 표시합니다.**show crypto map** - 이 명령은 인터페이스에 대한 IKE 및 IPsec 프로파일의 매핑을 보여줍니다.**show ip nhrp** - 이 명령은 디바이스에서 NHRP 정보를 제공합니다.이는 FlexVPN 설정에서 스포크 투 스포크(spoke-to-spoke) 설정과 DMVPN 설정에서 스포크 투 스포크(spoke-to-spoke) 및 스포크 투 허브(spoke-to-hub) 바인딩 모두에 유용합니다.

2. 터널 설정을 디버깅하려면 다음 명령을 사용합니다.

   디버그 암호화 ikev2디버그 암호화 isakmp디버그 암호화 ipsec디버그 암호화 kmi

경로 전파 문제

다음은 EIGRP 및 토폴로지를 트러블슈팅하기 위해 사용할 수 있는 몇 가지 유용한 명령입니다.

- **show bgp summary** - 연결된 인접 디바이스 및 해당 상태를 확인하려면 이 명령을 사용합니다.
- **show ip eigrp neighbor** - EIGRP를 통해 연결된 네이버를 표시하려면 이 명령을 사용합니다.
- **show bgp** - BGP를 통해 학습된 접두사를 확인하려면 이 명령을 사용합니다.
- **show ip eigrp topology** - EIGRP를 통해 학습된 접두사를 표시하려면 이 명령을 사용합니다.

학습된 접두사가 라우팅 테이블에 설치된 접두사와 다르다는 것을 알고 있어야 합니다. 이에 대한 자세한 내용은 Cisco 라우터 Cisco 문서 또는 라우팅 TCP/IP Cisco Press 설명서의 경로 선택 문서를 참조하십시오.

알려진 주의 사항

ASR1K에 GRE 터널 처리와 유사한 제한이 있습니다.이는 Cisco 버그 ID CSCue00443에서 추적됩니다. 이 경우 Cisco IOS XE Software Release 3.12에서 제한 사항에 대한 수정 일정이 있습니다.

수정 사항을 사용할 수 있게 되면 알림을 원하는 경우 이 버그를 모니터링합니다.