듀얼 클라우드 접근 방식을 사용한 이중화 허브 설계의 FlexVPN 스포크 컨피그레이션 예

목차

소개

이 문서에서는 여러 허브가 사용 가능한 시나리오에서 FlexVPN 클라이언트 컨피그레이션 블록을 사용하여 FlexVPN 네트워크에서 스포크를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FlexVPN
- Cisco 라우팅 프로토콜

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco G2 Series ISR(Integrated Service Router)
- Cisco IOS® 버전 15.2M

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.

구성

이중화를 위해 스포크는 여러 허브에 연결해야 할 수 있습니다.스포크 측의 이중화를 통해 허브 측에서 단일 장애 지점 없이 지속적인 작업을 수행할 수 있습니다.

스포크 컨피그레이션을 사용하는 가장 일반적인 두 가지 FlexVPN 이중화 허브 설계는 다음과 같습니다.

- **듀얼 클라우드 방식**으로, 스포크에 두 개의 개별 터널이 항상 두 허브에 활성화되어 있습니다.
- **장애 조치 방식**: 스포크에 지정된 시점에 하나의 허브가 있는 활성 터널이 있습니다.

두 접근 방식 모두 고유한 장단점을 가지고 있다.

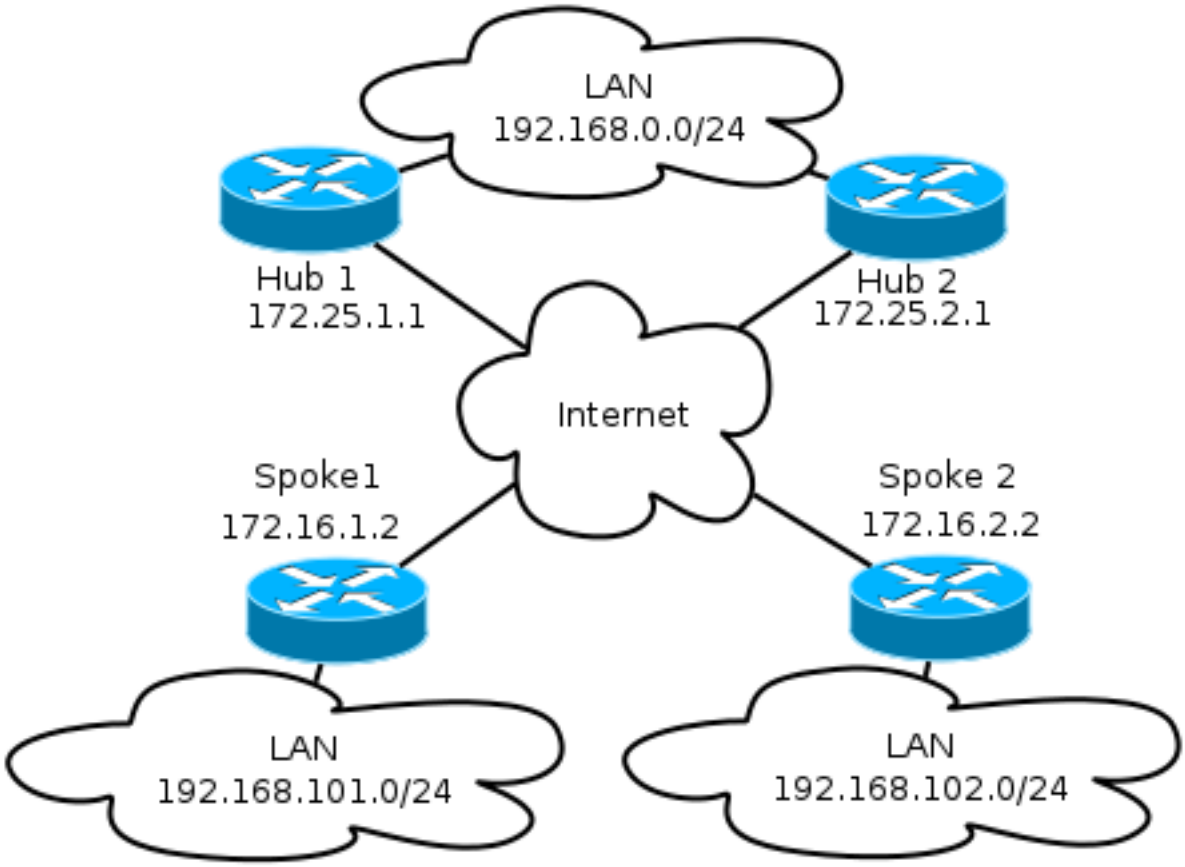
접근 방식	장점	단점
듀얼 클라우드	• 라우팅 프로토콜 타이머를 기반으로 장애 발생 시 더 빠른 복구 • 두 허브에 대한 연결이 활성 상태이므로 허브 간에 트래픽을 분산할 수 있는 가능성 증가	• Spoke는 두 허브에 대한 세션을 동시에 유지 관리하므로 두 허브의 리소스를 모두 사용합니다.
장애 조치	• 손쉬운 구성 - FlexVPN에 내장 • 장애 시 라우팅 프로토콜에 의존하지 않음	• 느린 복구 시간 - DPD(Dead Peer Detection) 또는 (선택 사항) 객체 추적을 기반으로 함 • 모든 트래픽은 한 번에 하나의 허브로 이동해야 합니다.

이 문서에서는 첫 번째 접근 방식에 대해 설명합니다.이 컨피그레이션에 대한 접근 방식은 DMVPN(Dynamic Multipoint VPN) 듀얼 클라우드 컨피그레이션과 유사합니다.허브 및 스포크의 기본 컨피그레이션은 DMVPN에서 FlexVPN으로의 마이그레이션 문서를 기반으로 합니다.FlexVPN 마이그레이션을 참조하십시오.이 컨피그레이션에 대한 설명을 보려면 동일한 디바이스의 DMVPN에서 FlexVPN으로 하드 이동 문서를 참조하십시오.

네트워크 다이어그램

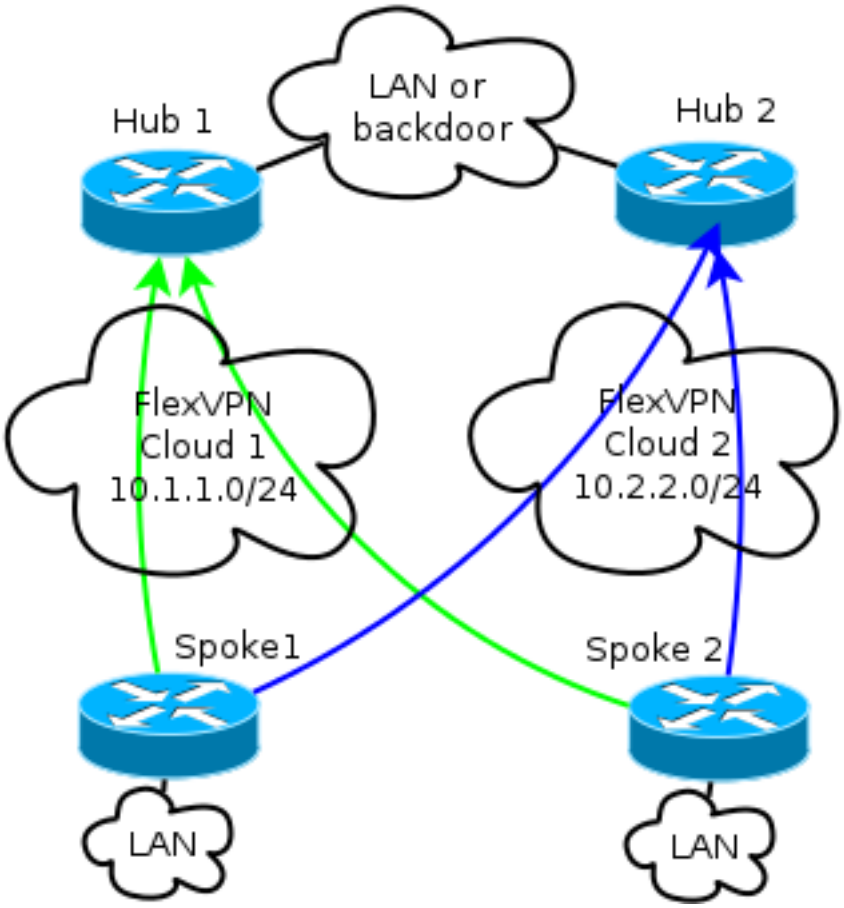
전송 네트워크

이 다이어그램은 FlexVPN 네트워크에서 일반적으로 사용되는 기본 전송 네트워크를 보여줍니다.



오버레이 네트워크

이 다이어그램은 장애 조치가 작동하는 방법을 보여 주는 논리적 연결이 있는 오버레이 네트워크를 보여줍니다.정상 작동 중에 스포크 1과 스포크 2는 두 허브와 관계를 유지합니다.장애가 발생하면 라우팅 프로토콜은 한 허브에서 다른 허브로 전환됩니다.



참고:다이어그램에서 녹색 선은 허브 1에 대한 IKEv2(Internet Key Exchange Version 2)/Flex 세션의 연결 및 방향을 보여주고 파란색 선은 허브 2에 대한 연결을 나타냅니다.

두 허브 모두 오버레이 클라우드에서 별도의 IP 주소를 유지합니다.**/24 주소**는 실제 인터페이스 주소 지정이 아닌 이 클라우드에 할당된 주소 풀을 나타냅니다.이는 FlexVPN 허브가 일반적으로 스포크 인터페이스에 동적 IP 주소를 할당하고 FlexVPN 권한 부여 블록의 경로 명령을 통해 동적으로 삽입되는 경로를 사용하기 때문입니다.

스포크 구성

스포크 터널 인터페이스 구성

이 예에서 사용되는 일반적인 컨피그레이션은 2개의 개별 대상 주소를 가진 2개의 터널 인터페이스입니다.

```
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
tunnel source Ethernet0/0
tunnel destination 172.25.1.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

```
interface Tunnel2
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 172.25.2.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

스포크 투 스포크 터널이 제대로 형성되도록 하려면 가상 템플릿(VT)이 필요합니다.

```
interface Virtual-Template1 type tunnel
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 path-mtu-discovery
tunnel protection ipsec profile default
```

Spoke는 VRF(Virtual Routing and Forwarding)의 LAN 인터페이스를 나타내는 번호가 지정되지 않은 인터페이스를 사용하며, 이 경우 전역입니다.그러나 루프백 인터페이스를 참조하는 것이 나을 수 있습니다.이는 루프백 인터페이스가 거의 모든 조건에서 온라인 상태를 유지하기 때문입니다.

BGP(Spoke Border Gateway Protocol) 구성

Cisco에서는 오버레이 네트워크에서 사용할 라우팅 프로토콜로 iBGP를 권장하기 때문에 이 문서에서는 이 컨피그레이션만 다룹니다.

> **참고:**스포크는 두 허브에 대한 BGP 연결성을 유지해야 합니다.

```
router bgp 65001
bgp log-neighbor-changes
network 192.168.101.0
neighbor 10.1.1.1 remote-as 65001
neighbor 10.1.1.1 fall-over
neighbor 10.2.2.1 remote-as 65001
neighbor 10.2.2.1 fall-over
```

이 컨피그레이션의 FlexVPN에는 기본 또는 보조 허브 개념이 없습니다.관리자는 라우팅 프로토콜이 다른 허브보다 다른 허브를 선호하는지 아니면 일부 시나리오에서 로드 밸런싱을 수행할지를 결정합니다.

스포크 장애 조치 및 통합 고려 사항

스포크가 실패를 감지하는 데 걸리는 시간을 최소화하려면 이 두 가지 일반적인 방법을 사용합니다.

- BGP 타이머를 줄입니다.기본 보류 시간으로 인해 장애 조치가 발생합니다.
- 이 문서에서 설명하는 BGP Fall-over를 구성합니다. BGP Support for Fast Peering Session Deactivation.

- 대부분의 FlexVPN 구축에서는 권장되지 않으므로 BFD(Bidirectional Forwarding Detection)를 사용하지 마십시오.

스포크 투 스포크 터널 및 장애 조치

스포크 투 스포크 터널은 NHRP(Next Hop Resolution Protocol) 바로 가기 스위칭을 사용합니다 .Cisco IOS는 이러한 바로가기가 NHRP 경로임을 나타냅니다(예:

```
Spoke1#show ip route nhrp
(...)

192.168.102.0/24 is variably subnetted, 2 subnets, 2 masks
H 192.168.102.0/24 [250/1] via 10.2.2.105, 00:00:21, Virtual-Access1
```

이러한 경로는 BGP 연결이 만료될 때 만료되지 않습니다.대신 기본적으로 2시간인 NHRP holdtime에 대해 보유됩니다.즉, 활성 스포크 투 스포크 터널이 장애 상태에서도 작동 중입니다.

허브 구성

로컬 풀

Network Diagram 섹션에서 설명한 대로 두 허브는 서로 다른 IP 주소 지정을 유지합니다.

허브1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

허브2

```
ip local pool FlexSpokes 10.2.2.100 10.2.2.254
```

허브 BGP 컨피그레이션

허브 BGP 컨피그레이션은 이전 예와 유사한 상태로 유지됩니다.

이 출력은 LAN IP 주소가 **192.168.0.1인** 허브 1**에서 가져옵니다**.

```
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
neighbor Spokes fall-over
neighbor 192.168.0.2 remote-as 65001
neighbor 192.168.0.2 route-reflector-client
neighbor 192.168.0.2 next-hop-self all
neighbor 192.168.0.2 unsuppress-map ALL

route-map ALL permit 10
```

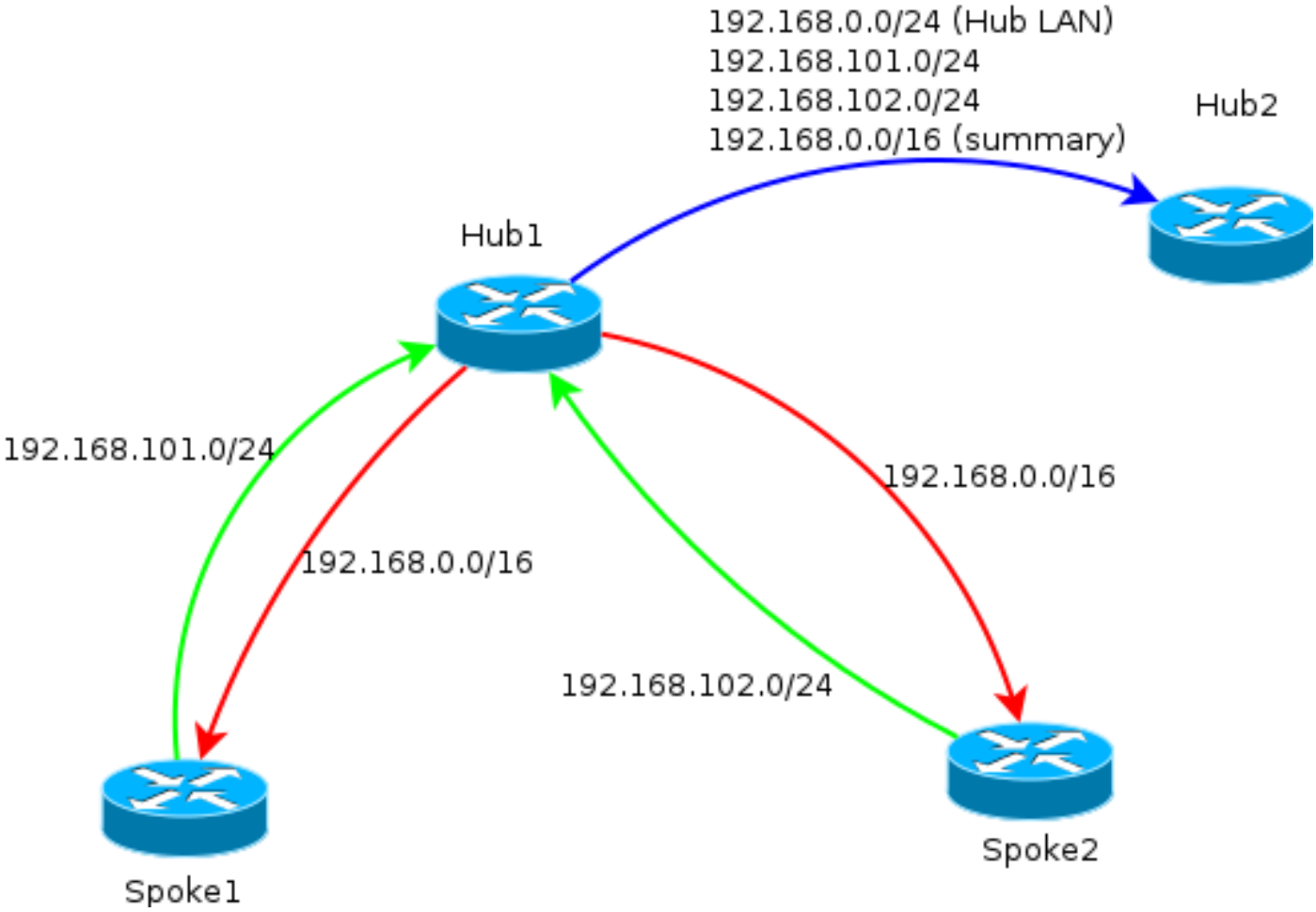
```
match ip address 1

ip access-list standard 1
permit any
```

기본적으로 이것은 다음과 같습니다.

- 로컬 FlexVPN 주소 풀이 BGP 수신 대기 범위에 있습니다.
- 로컬 네트워크는 192.168.0.0/24입니다.
- 요약은 스포크에만 광고됩니다.Aggregate-address 컨피그레이션은 null0 인터페이스를 통해 해당 접두사에 대한 고정 경로를 생성합니다. 이는 라우팅 루프를 방지하기 위해 사용되는 폐기 경로입니다.
- 모든 특정 접두사는 다른 허브에 광고됩니다.iBGP 연결이므로 경로 리플렉터 컨피그레이션이 필요합니다.

이 다이어그램은 하나의 FlexVPN 클라우드에서 스포크와 허브 간의 BGP 접두사 교환을 나타냅니다.



참고:다이어그램에서 녹색 선은 스포크가 허브에 제공한 정보를 나타내고, 빨간색 선은 각 허브가 스포크에 제공한 정보를 나타내며(요약만 해당), 파란색 선은 허브 간에 교환되는 접두사를 나타냅니다.

다음을 확인합니다.

각 스포크는 두 허브와의 연결을 유지하므로 show crypto ikev**2 sa** 명령과 함께 두 IKEv2 세션**이** 표시됩니다.

```
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
3 172.16.1.2/500 172.16.2.2/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3147 sec

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.1.2/500 172.25.2.1/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3256 sec
```

라우팅 프로토콜 정보를 보려면 다음 명령을 입력합니다.

```
show bgp ipv4 unicast

show bgp summary
```

스포크에서 요약 접두사가 허브에서 수신되고 두 허브에 대한 연결이 활성화되어 있음을 확인해야 합니다.

```
Spoke1#show bgp ipv4 unicast
BGP table version is 4, 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
*>i 192.168.0.0/16 10.1.1.1 0 100 0 i
* i 10.2.2.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
Spoke1#show bgp summa
Spoke1#show bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
BGP table version is 4, main routing table version 4
2 network entries using 296 bytes of memory
3 path entries using 192 bytes of memory
3/2 BGP path/bestpath attribute entries using 408 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 896 total bytes of memory
BGP activity 2/0 prefixes, 3/0 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 7 7 4 0 0 00:00:17 1
10.2.2.1 4 65001 75 72 4 0 0 01:02:24 1
```

문제 해결

트러블슈팅에는 두 가지 주요 블록이 있습니다.

- IKE(Internet Key Exchange)
- IPsec(인터넷 프로토콜 보안)

다음과 같은 관련 show 명령이 있습니다.

show crypto ipsec sa

show crypto ikev2 sa

관련 debug 명령은 다음과 같습니다.

debug crypto ikev2 [internal|packet]

debug crypto ipsec

debug vtemplate event

관련 라우팅 프로토콜은 다음과 같습니다.

show bgp ipv4 unicast (or show ip bgp)

show bgp summary