FlexVPN 솔루션 구성 및 확인

목차

소개

이 문서에서는 Flex Virtual Private Network 환경에 대해 설명하고, 기능을 소개하고, 각 FlexVPN 토폴로지를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco IOS 및 Cisco IOS XE
- IKE(Internet Key Exchange) 버전 2
- 인터넷 프로토콜 보안(IPsec)
- FlexVPN

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS XE Amsterdam-17.3.6

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

배경 정보

FlexVPN은 다양한 유형의 VPN 연결을 위한 통합 프레임워크를 제공하도록 설계된, Cisco에서 제공하는 다기능 종합 VPN 솔루션입니다. IKEv2(Internet Key Exchange 버전 2) 프로토콜을 기반으로 구축된 FlexVPN은 VPN의 구성, 관리 및 구축을 간소화할 수 있도록 설계되었으며 일관된 도구 집합을 활용합니다. 동일한 명령과 구성 단계는 여러 VPN 유형(사이트 간, 원격 액세스 등)에 적용됩니다. 이러한 일관성은 오류를 줄이는 데 도움이 되며 구축 프로세스를 더욱 직관적으로 만들어 줍니다.

IKEv2 대 IKEv1

FlexVPN은 AES(Advanced Encryption Standard) 및 SHA-256(Secure Hash Algorithm)과 같은 최신 암호화 알고리즘을 지원하는 IKEv2를 활용합니다. 이러한 알고리즘은 강력한 암호화 및 데이터 무결성을 제공하여 VPN을 통해 전송된 데이터가 가로채거나 변조되지 않도록 보호합니다.

IKEv2는 IKEv1에 비해 더 많은 인증 방법을 제공합니다. PSK(Pre-Shared Key), 인증서 기반 및 하이브리드 인증 유형 외에 IKEv2를 사용하면 응답자가 클라이언트 인증에 EAP(Extensible Authentication Protocol)를 활용할 수 있습니다.

FlexVPN에서 EAP는 클라이언트 인증에 사용되며 라우터는 릴레이 역할을 하여 클라이언트와 백엔드 EAP 서버(일반적으로 RADIUS 서버) 간에 EAP 메시지를 전달합니다. FlexVPN은 인증 프로세스 보안을 위해 EAP-TLS, EAP-PEAP, EAP-PSK 등 다양한 EAP 방법을 지원합니다.

이 표에서는 IKEv1 함수와 IKEv2 함수의 차이를 보여 줍니다.

	IKEv2	IKEv1
프로토콜 설정 메시지	4개의 메시지	6개의 메시지
EAP 지원	예(2개의 추가 메시지)	아니요
보안 연결에 대한 협상	추가 메시지 2개	3개의 추가 메시지
UDP 500/4500에서 실행	예	예

NAT Traversal(NAT-T)	예	예
재전송 및 승인 기능	예	예
ID 보호, DoS 보호 메커니즘 및 PFS(Perfect Forward Secrecy) 제공	예	예
차세대 암호 지원	예	아니요

확장성

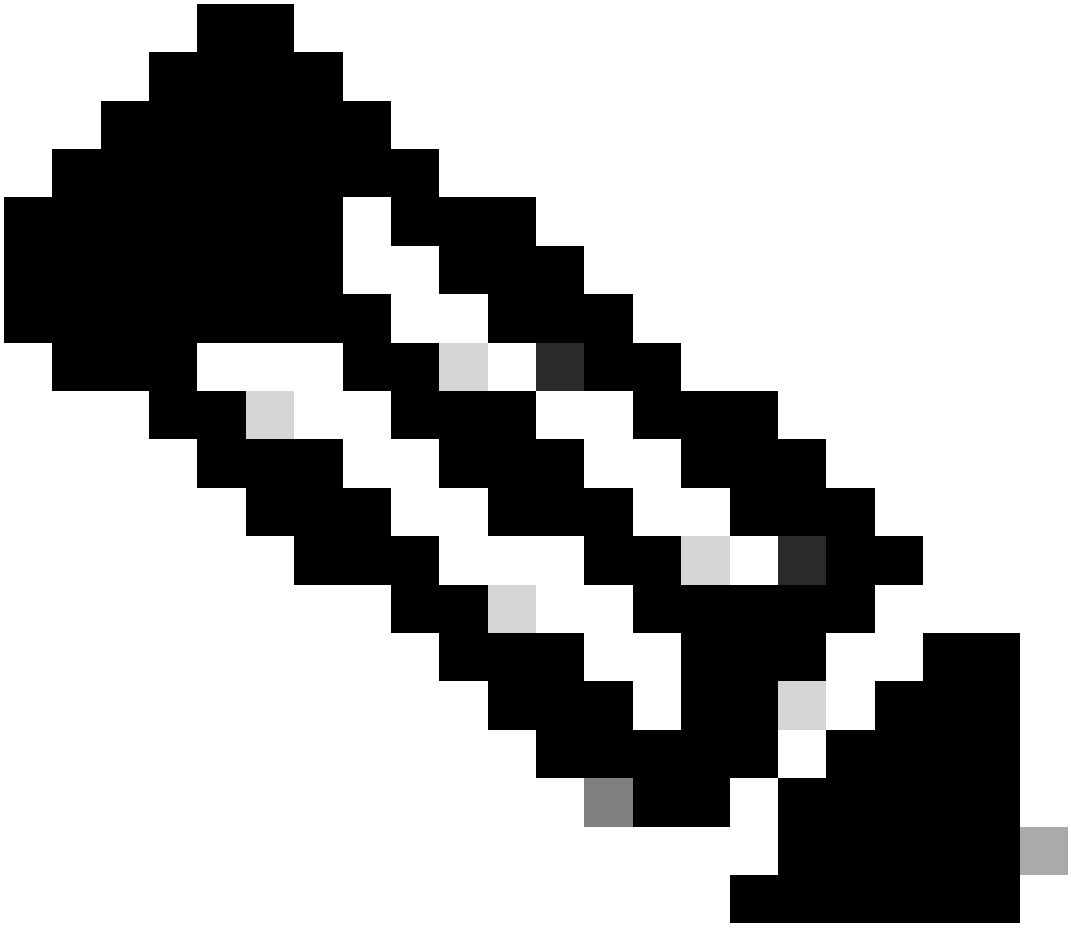
FlexVPN은 소규모 사무실에서 대규모 비즈니스 네트워크로 쉽게 확장할 수 있습니다. 따라서 안전하고 신뢰할 수 있는 네트워크 액세스가 필요한 원격 사용자가 많은 조직에 이상적인 선택입니다.

주요 기능

- 동적 구성 및 온디맨드 터널:
  - FlexVPN 연결이 시작되면 시스템은 사전 구성된 템플릿을 기반으로 가상 액세스 인터페이스를 생성합니다. 이 인터페이스는 연결 기간 동안 터널 엔드포인트 역할을 합니다. 터널이 더 이상 필요하지 않으면 가상 액세스 인터페이스가 해제되어 시스템 리소스가 확보됩니다.

- 구축의 유연성:
  - 허브 앤 스포크 모델: 중앙 허브는 여러 지사에 연결됩니다. FlexVPN은 단일 프레임워크를 통해 이러한 연결 설정을 간소화하여 대규모 네트워크에 이상적입니다.
  - 풀 메시 및 부분 메시 토폴로지: 모든 사이트가 중앙 허브를 거치지 않고 직접 통신할 수 있어 지연 시간이 줄어들고 성능이 향상됩니다.

- 고가용성 및 이중화:
  - 이중화 허브: 백업을 위해 여러 허브를 지원합니다. 한 허브에 장애가 발생하면 브랜치가 다른 허브에 연결하여 지속적인 연결을 보장할 수 있습니다.
  - 로드 밸런싱: 이렇게 하면 여러 디바이스에 VPN 연결이 분산되므로 단일 디바이스에 과부하가 발생하지 않습니다. 이는 대규모 구축에서 성능을 유지하는 데 매우 중요합니다.



참고: 다음 가이드에서는 허브 연결을 위한 로드 밸런싱 컨피그레이션에 대한 자세한 정보를 제공합니다.

IKEv2 로드 밸런서 구성

- 확장 가능한 인증 및 권한 부여:
  - AAA 통합: 대규모 사용에 필수적인 사용자 자격 증명 및 정책의 중앙 집중식 관리를 위해 Cisco ISE 또는 RADIUS와 같은 AAA 서버와 연동됩니다.
  - PKI 및 인증서: 보안 인증을 위해 PKI(Public Key Infrastructure) 및 디지털 인증서를 지원하며, 이는 특히 대규모 환경에서 사전 공유 키를 사용하는 것보다 확장성이 높습니다.

라우팅

FlexVPN의 라우팅 기능은 확장성을 개선하고 여러 VPN 연결을 효율적으로 관리하며 각 연결로 트래픽을 동적으로 라우팅할 수 있도록 설계되었습니다. FlexVPN 라우팅을 효율적으로 만드는 다음 주요 구성 요소 및 메커니즘:

- 가상 템플릿 인터페이스: IP 주소 할당, 터널 소스, IPsec 설정 등 VPN 연결에 필요한 모든 설정을 포함하는 구성 템플릿입니다. 이 인터페이스에서는 특정 IP 주소를ip unnumbered터널의 소스로 구성하는 대신 일반적으로 루프백에서 IP 주소를 차용하도록 명령을 구성합니다. 이렇게 하면 각 스포크에서 동일한 템플릿을 사용할 수 있으므로 각 스포크가 자체 소스 IP 주소를 사용할 수 있습니다.

- 가상 액세스 인터페이스: 가상 템플릿 인터페이스에서 설정을 상속하도록 동적으로 생성된 인터페이스입니다. 새 VPN 연결이 설정될 때마다 가상 템플릿을 기반으로 새 가상 액세스 인터페이스가 생성됩니다. 즉, 각 VPN 세션에는 고유한 인터페이스가 있으며, 이를 통해 관리 및 확장이 간소화됩니다.

- 동적 라우팅 프로토콜: OSPF, EIGRP, BGP over VPN 터널과 같은 라우팅 프로토콜에서 작동합니다. 이렇게 하면 라우팅 정보가 자동으로 업데이트됩니다. 이는 대규모 및 동적 네트워크에서 중요합니다.

- IKEv2는 FlexVPN 서버가 클라이언트에 네트워크 특성을 푸시하도록 허용하여 경로를 광고하며, 클라이언트는 터널 인터페이스에 이러한 경로를 설치합니다. 또한 클라이언트는 컨피그레이션 모드 교환 중에 자체 네트워크를 서버에 통신하여 양쪽 끝에서 라우트 업데이트를 활성화합니다.

- NHRP(Next Hop Resolution Protocol)는 공용 IP 주소를 사설 VPN 엔드포인트에 매핑하기 위해 허브 및 스포크 토폴로지에서 사용되는 동적 주소 확인 프로토콜입니다. 스포크가 직접 통신을 위해 다른 스포크 IP를 검색할 수 있도록 합니다.

권한 부여 정책

FlexVPN에 대한 IKEv2 권한 부여 정책을 구성하여 VPN 연결의 다양한 측면을 제어할 수 있습니다. IKEv2 권한 부여 정책은 로컬 권한 부여 정책을 정의하며 로컬 및/또는 원격 특성을 포함합니다.

- VRF(VPN routing and forwarding) 및 QOS 정책과 같은 로컬 특성은 로컬로 적용됩니다.
- 경로와 같은 원격 특성은 컨피그레이션 모드를 통해 피어에 푸시됩니다.
- crypto ikev2 authorization policy 명령을 사용하여 로컬 정책을 정의합니다.
- IKEv2 권한 부여 정책은 IKEv2 프로파일에서 AAA authorization 명령을 통해 참조합니다.

이 표에서는 IKEv2 권한 부여 정책에서 구성할 수 있는 주요 매개변수의 개요를 제공합니다.

매개변수	설명
AAA	AAA 서버와의 통합을 통해 사용자 자격 증명을 검증하고 액세스 권한을 부여하며 사용을 위한 계정 관리 정책은 검증이 라우터에서 로컬로 수행되는지 아니면 원격으로 수행되는지(예: RADIUS 서버를 통해 수행되는지)를 지정할 수 있습니다.
클라이언트 컨피그레이션	유휴 시간 제한 값, keepalive, DNS 및 WINS 서버 할당 등의 컨피그레이션 설정을 클라이언트에 푸시합니다.
클라이언트별 컨피그레이션	ID 또는 그룹 멤버십에 따라 서로 다른 클라이언트에 대해 서로 다른 컨피그레이션을 허용합니다.

경로 집합	이 컨피그레이션은 특정 트래픽이 VPN 터널을 통과하도록 허용합니다. 이렇게 하면 연결에 성공할 때 VPN 클라이언트에 푸시되는 경로 주입이 수행됩니다.

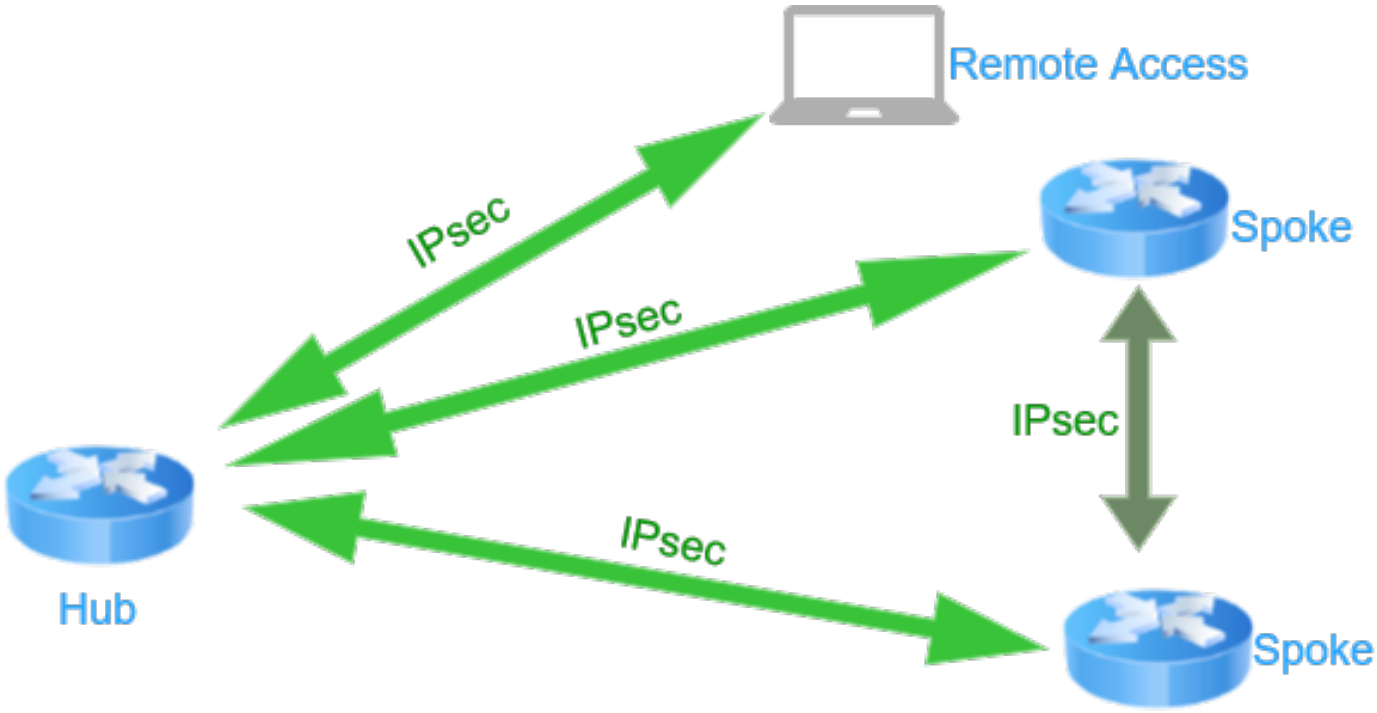
FlexVPN과 기타 기술 비교

FlexVPN은 최신 네트워크 환경에 매력적인 선택인 다양한 이점을 제공합니다. FlexVPN은 통합 프레임워크를 제공함으로써 구성 및 관리를 간소화하고 보안을 강화하며 확장성을 지원하고 상호운용성을 보장하며 복잡성을 줄입니다.

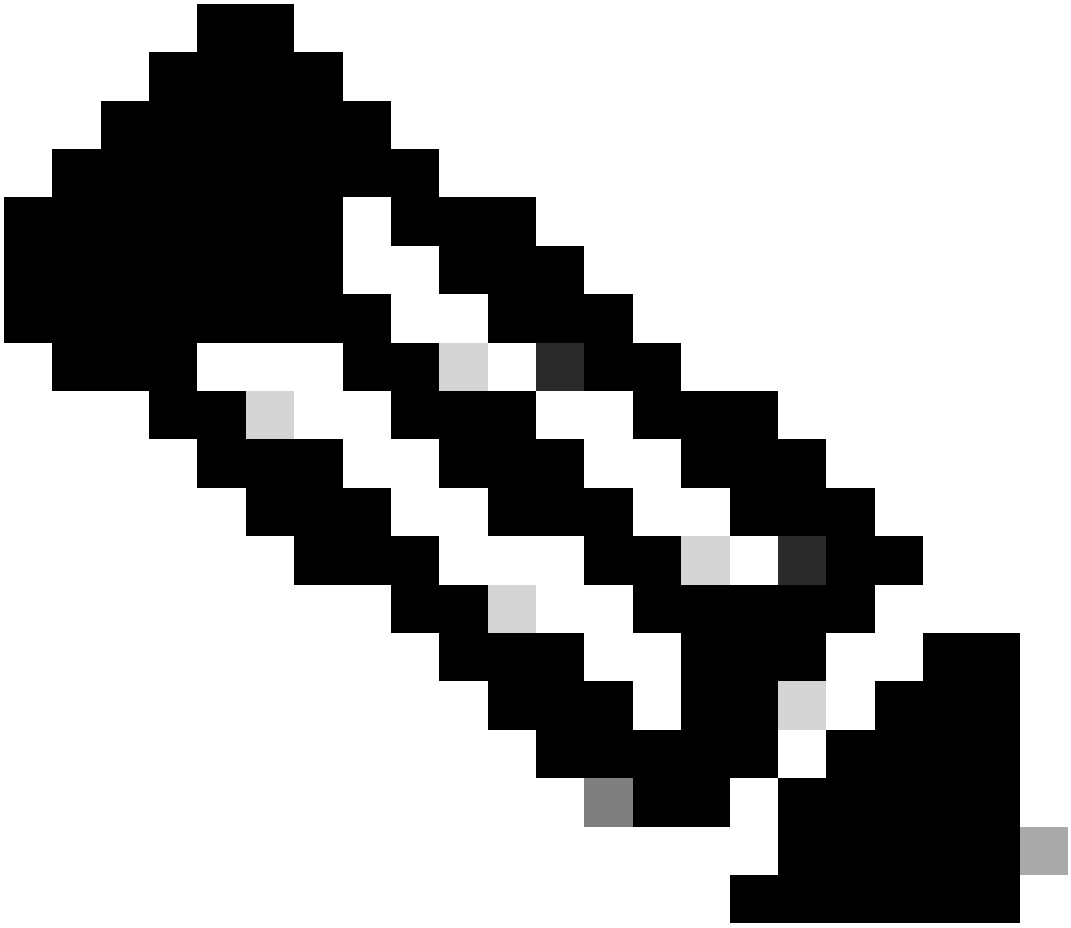
	암호화 맵	DMVPN	FlexVPN
동적 라우팅	아니요	예	예
동적 스포크 대 스포크 직접	아니요	예	예
원격 액세스 VPN	예	아니요	예
컨피그레이션 푸시	아니요	아니요	예
피어-피어 컨피그레이션	아니요	아니요	예
피어-피어 Qos	아니요	예	예
AAA 서버 통합	아니요	아니요	예

네트워크 다이어그램

FlexVPN을 사용하면 디바이스 간에 터널을 생성하여 허브와 스포크 간의 통신을 설정할 수 있습니다. 또한 다이어그램에 나와 있는 것처럼 원격 액세스 VPN 사용자를 위한 연결 및 스포크 간 직접 통신을 위한 터널 생성도 가능합니다.



FlexVPN 다이어그램



참고: 원격 액세스 VPN에 대한 구성은 이 가이드에서 다루지 않습니다. 컨피그레이션에 대한 자세한 내용은 설명서를 참조하십시오.

로컬 사용자 데이터베이스를 사용하여 보안 클라이언트(AnyConnect) IKEv2 원격 액세스를 위한 FlexVPN 헤드엔드 구성

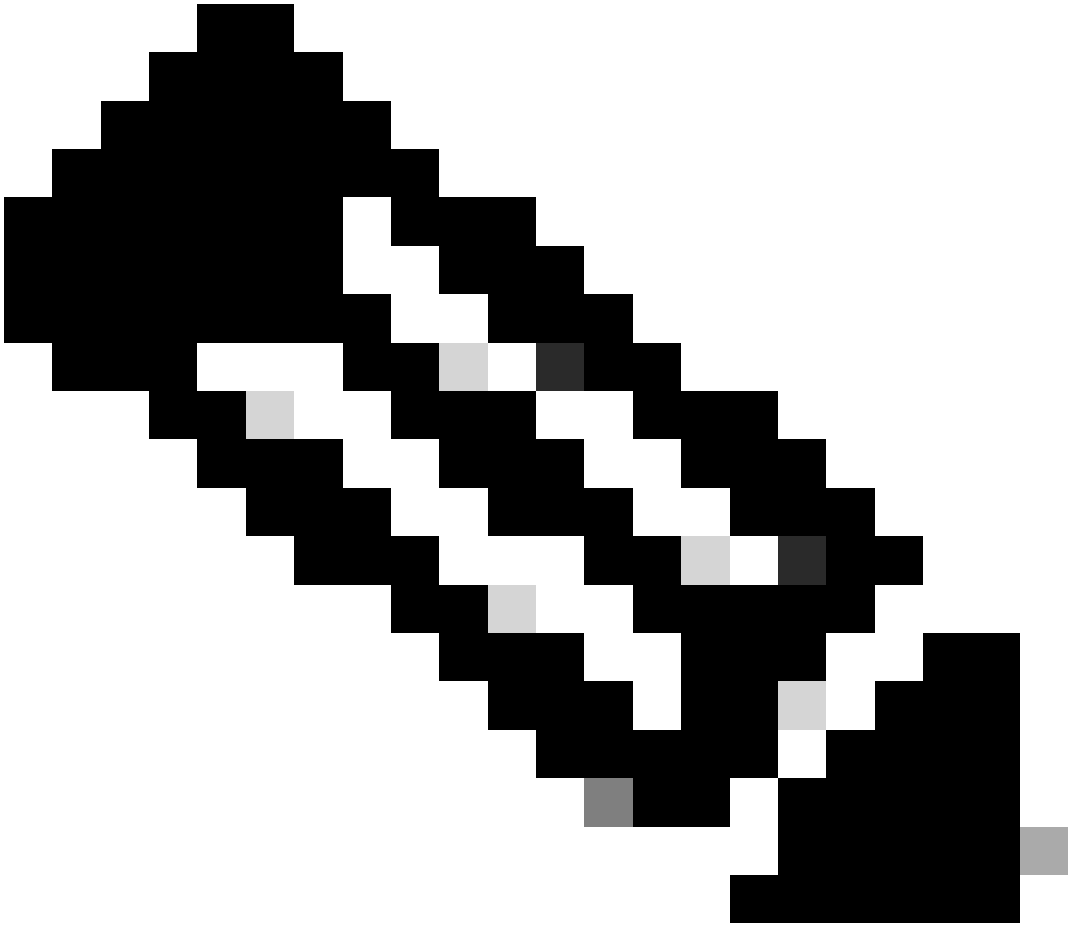
구성

FlexVPN은 구성이 간소화된 것이 특징입니다. 이러한 단순성은 다양한 유형의 VPN에 사용되는 일관된 컨피그레이션 블록에서 분명합니다. FlexVPN은 일반적으로 적용되는 간단한 구성 블록을 제공하며, 토폴로지의 특정 기능 또는 요구 사항에 따라 사용 가능한 선택적 구성 또는 추가 단계가 있습니다.

- IKEv2 제안: IKEv2 SA(Security Association)의 협상에 사용되는 알고리즘을 정의합니다. 일단 생성되면 이 제안을 IKEv2 정책에 추가하여 협상 중에 선택할 수 있습니다.
- IKEv2 정책: 제안을 VRF(Virtual Routing and Forwarding) 인스턴스 또는 로컬 IP 주소에 연결

합니다. IKEv2 제안서에 대한 정책 링크

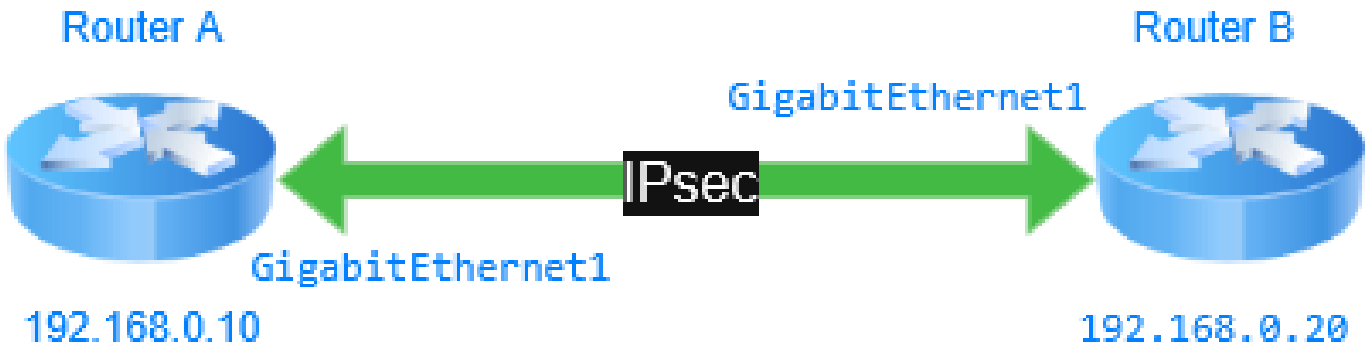
- IKEv2 키 링: 피어 인증에 사용할 경우 비대칭적일 수 있는 PSK(Pre-Shared Key)를 지정합니다.
- 신뢰 지점(선택 사항): PKI(Public Key Infrastructure)를 인증 방법으로 사용할 때 피어 인증을 위한 ID 및 CA(Certificate Authority) 특성을 구성합니다.
- AAA 통합(선택 사항): FlexVPN은 Cisco ISE(Identity Services Engine) 또는 RADIUS 서버와 같은 AAA 서버를 인증 방법으로 통합합니다.
- IKEv2 프로파일: VPN 피어 주소 및 인증 방법과 같은 IKE SA의 협상할 수 없는 매개변수를 저장합니다. 기본 IKEv2 프로파일은 없으므로 하나를 구성하고 개시자의 IPsec 프로파일에 연결해야 합니다. PSK 인증이 사용되는 경우 IKEv2 프로필은 IKEv2 키링을 참조합니다. PKI 인증 또는 AAA 인증 방법을 사용하는 경우 여기서 참조합니다.
- IPsec 변형 집합: IPsec SA에 허용되는 알고리즘의 조합을 지정합니다.
- IPsec 프로필: FlexVPN 설정을 인터페이스에 적용할 수 있는 단일 프로필로 통합합니다. 이 프로파일은 IPsec 변형 집합 및 IKEv2 프로파일을 참조합니다.



참고: 컨피그레이션 예에서는 사전 공유 키를 사용하여 FlexVPN 컨피그레이션 및 단순성에 대한 간단한 데모를 제공합니다. 사전 공유 키를 사용하여 손쉽게 구축하고 작은 토폴로지를 만들 수 있지만, AAA 또는 PKI 방법은 대규모 토폴로지에 더 적합합니다.

사이트 대 사이트 FlexVPN 구성

FlexVPN Site-to-Site 토폴로지는 두 사이트 간의 직접 VPN 연결을 위해 설계되었습니다. 각 사이트에는 트래픽이 이동할 수 있는 보안 채널을 설정하는 터널 인터페이스가 있습니다. 이 컨피그레이션에서는 다이어그램에 표시된 대로 두 사이트 간에 직접 VPN 연결을 설정하는 방법에 대해 설명합니다.



Site_to_Site_Diagram

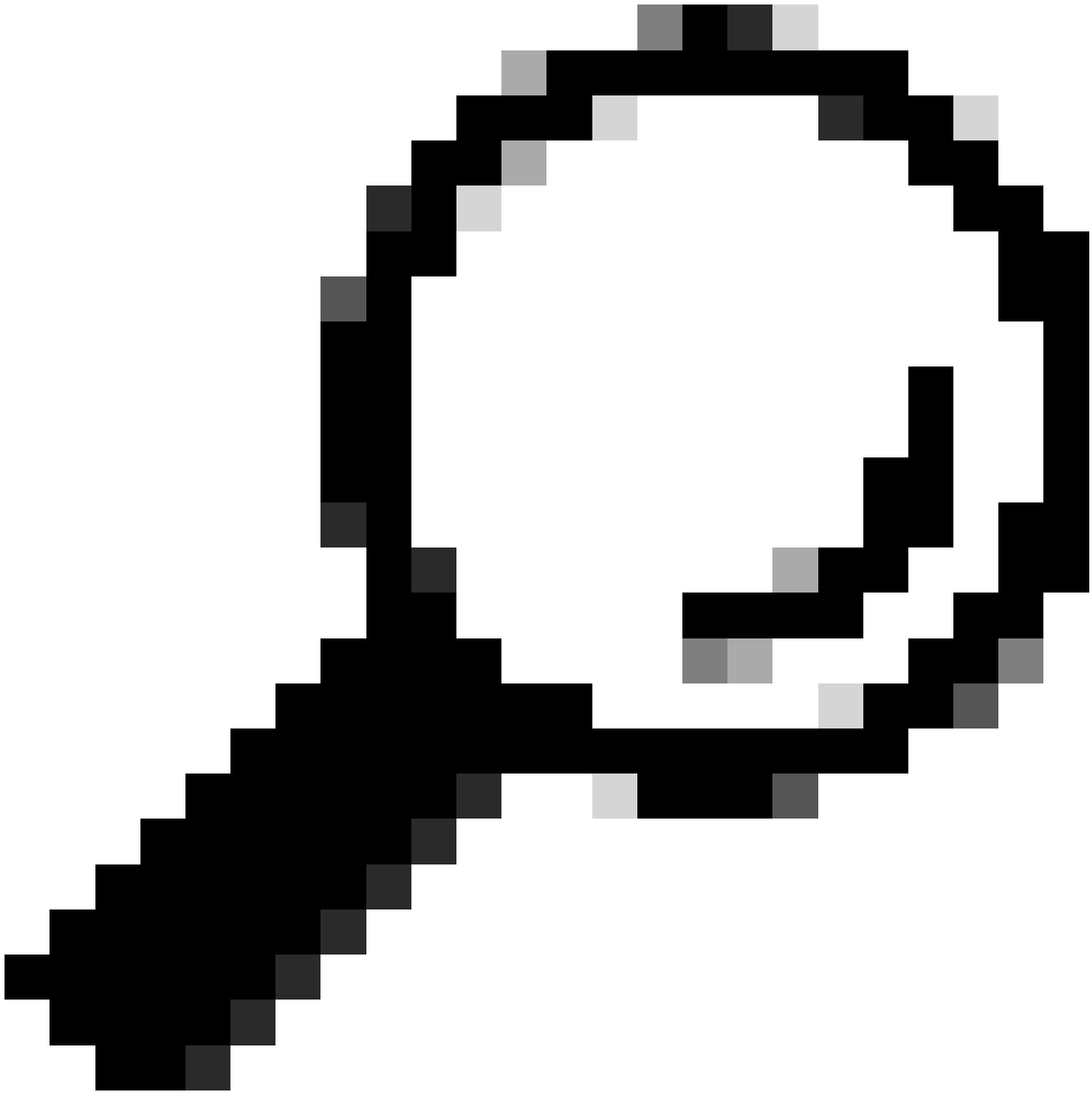
1단계: 라우터 A 컨피그레이션

a. IKEv2 제안 및 정책을 정의합니다.

b. 키링을 구성하고 피어를 인증하Pre-Shared Key는 데 사용되는 를 입력합니다.

c. 를 IKEv2 profile 생성하고 를 keyring할당합니다.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 192.168.0.20
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
crypto ikev2 profile FLEXVPN_PROFILE
match identity remote address 192.168.0.20
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
lifetime 86400
dpd 10 2 on-demand
!
```



팁: 이 **IKEv2 Smart Defaults** 기능은FlexVPN대부분의 활용 사례를 다루어 구성을 최소화합니다. 특정 활용 사례에 **IKEv2 Smart Defaults** 맞게 사용자 지정할 수 있지만 Cisco에서는 이 방법을 권장하지 않습니다.

d. 를 Transport Set 생성하고 데이터를 보호하는 데 사용되는 암호화 및 해시 알고리즘을 정의합니다.

e. 를 **IPsec profile**생성합니다.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
```

```
 set ikev2-profile FLEXVPN_PROFILE
!
```

f. 터널 인터페이스를 구성합니다.

```
!
interface Tunnel0
 ip address 10.1.120.10 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.20
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
 ip address 192.168.0.10 255.255.255.0
!
```

g. 터널 인터페이스를 알리기 위해 동적 라우팅을 구성합니다. 그런 다음 터널을 통과해야 하는 다른 네트워크를 광고할 수 있습니다.

```
router eigrp 100
 no auto-summary
 network 10.1.120.0 0.0.0.255
```

2단계: 라우터 B 컨피그레이션

a. IKEv2 제안 및 정책을 정의합니다.

b. 를 keyring 구성하고 피어를 인증하Pre-Shared Key는 데 사용되는 를 입력합니다.

c. 를 IKEv2 profile 생성하고 를 keyring할당합니다.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 192.168.0.10
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
crypto ikev2 profile FLEXVPN_PROFILE
```

```
match identity remote address 192.168.0.10
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
lifetime 86400
dpd 10 2 on-demand
!
```

d. 를 Transport Set 생성하고 데이터를 보호하는 데 사용되는 암호화 및 해시 알고리즘을 정의합니다.

e. 를 IPsec profile 생성하고 이전에 생성한 IKEv2 프로파일과 변형 집합을 할당합니다.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

f. 를 Tunnel interface구성합니다.

```
!
interface Tunnel0
 ip address 10.1.120.20 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
 ip address 192.168.0.20 255.255.255.0
!
```

g. 터널 인터페이스를 광고하도록 동적 라우팅을 구성합니다. 그런 다음 터널을 통과해야 하는 다른 네트워크를 광고할 수 있습니다.

```
router eigrp 100
 no auto-summary
 network 10.1.120.0 0.0.0.255
```

다음을 확인합니다.

- show ip interface brief 명령을 사용하여 터널 인터페이스 상태를 검토하고 터널이 up/up 상태

인지 확인합니다.

<#root>

```
RouterB#
```

show ip interface brief

```
Interface              IP-Address      OK?   Method    Status   Protocol
GigabitEthernet1       192.168.0.20    YES   NVRAM     up       up
Tunnel0                10.1.120.11     YES   manual
```

up

```
 up
```

1. show crypto ikev2 sa 명령을 사용하여 라우터 간 보안 연결이 설정되었는지 확인합니다.

<#root>

```
RouterB#
```

show crypto ikev2 sa

```
IPv4 Crypto IKEv2 SA

Tunnel-id  Local                Remote               fvrf/ivrf   Status
2          192.168.0.20/500     192.168.0.10/500     none/none
```

READY

```
    Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
```

Life/Active Time: 86400/3139 sec

```
IPv6 Crypto IKEv2 SA
```

- show crypto ipsec sa 명령을 사용하여 암호화 및 디캡스 카운터가 증가하는지 확인하여 트래픽이 암호화되어 터널을 통과하는지 확인할 수 있습니다.

<#root>

```
RouterB#
```

show crypto ipsec sa

```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.168.0.20
```

```
   protected vrf: (none)
   local ident (addr/mask/prot/port): (192.168.0.20/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.0.10/255.255.255.255/47/0)
   current_peer 192.168.0.10 port 500
     PERMIT, flags={origin_is_acl,}


#pkts encaps: 669, #pkts encrypt: 669, #pkts digest: 669




#pkts decaps: 668, #pkts decrypt: 668, #pkts verify: 668


    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

      local crypto endpt.: 192.168.0.20, remote crypto endpt.: 192.168.0.10
      plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
      current outbound spi: 0x93DCB8AE(2480715950)
      PFS (Y/N): N, DH group: none

      inbound esp sas:


spi: 0x89C141EB(2311143915)


         transform: esp-256-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 5578, flow_id: CSR:3578, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0


sa timing: remaining key lifetime (k/sec): (4607913/520)


         IV size: 16 bytes
         replay detection support: Y


Status: ACTIVE(ACTIVE)



      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:


spi: 0x93DCB8AE(2480715950)


         transform: esp-256-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 5577, flow_id: CSR:3577, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0


sa timing: remaining key lifetime (k/sec): (4607991/3137)
```

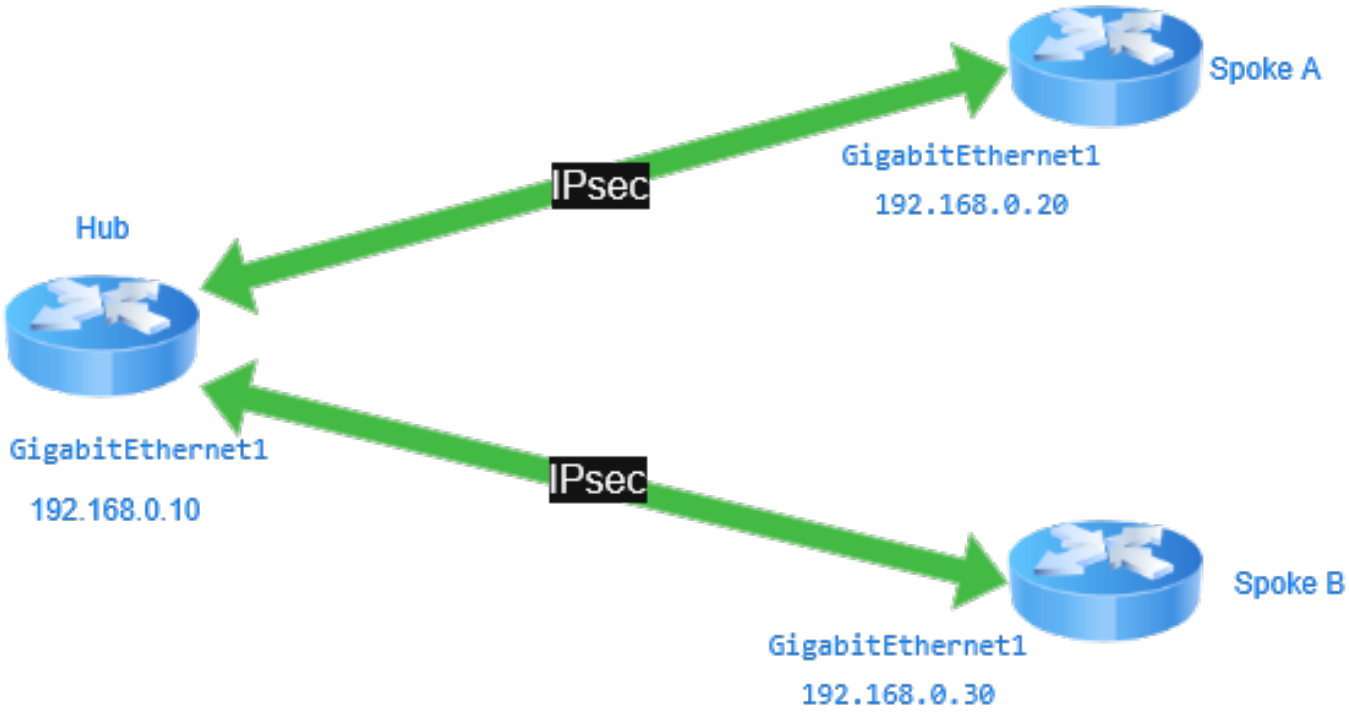
```
         IV size: 16 bytes
         replay detection support: Y

Status: ACTIVE(ACTIVE)


      outbound ah sas:

      outbound pcp sas:
```

- show ip eigrp neighbors 명령을 사용하여 EIGRP 인접성이 다른 사이트와 설정되었는지 확인합니다.

```
RouterB#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface              Hold  Uptime     SRTT    RTO    Q   Seq
                                                   (sec)            (ms)          Cnt  Num
0   10.1.120.10             Tu0                     13   00:51:26    3      1470   0   2
```

허브 앤 스포크 FlexVPN

허브-앤-스포크 토폴로지에서는 여러 스포크 라우터가 중앙 허브 라우터에 연결됩니다. 이 컨피그레이션은 스포크가 주로 허브와 통신하는 시나리오에 적합합니다. FlexVPN에서는 통신 효율성을 높이기 위해 동적 터널을 구성할 수 있습니다. 허브는 IKEv2 라우팅을 사용하여 경로를 스포크 라우터로 배포하여 원활한 연결을 보장합니다. 다이어그램에서 참조되는 것처럼, 컨피그레이션에서는 허브와 스포크 간의 VPN 연결 및 허브가 여러 스포크와 동적 연결을 설정하도록 구성된 방법과 스포크를 더 추가할 수 있는 방법에 대해 설명합니다.



Hub_and_Spoke_Diagram

1단계: 허브 컨피그레이션

a. IKEv2 제안 및 정책을 정의합니다.

b. 를 keyring 구성하고 스포크를 인증하Pre-Shared Key는 데 사용되는 를 입력합니다.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. 허브 라우터에서 AAA 서비스를 활성화한 다음 로컬 디바이스 컨피그레이션의 정책을 지정하는 네트워크FlexAuth권한 부여 목록을 정의합니다.

```
!
aaa new-model
```

```
 aaa authorization network FlexAuth local
!
```

d. 주소 10.1.1.2~10.1.1.254를 포함하는IP address pool명명된FlexPool이름을 정의합니다. 이 풀은 스포크의 터널 인터페이스에 IP 주소를 자동으로 할당하는 데 사용됩니다.

```
!
ip local pool FlexPool 10.1.1.2 10.1.1.254
!
```

e. 이름이FlexTraffic지정되고 네트워크 10.10.1.0/24를 허용하는 표준 IP 액세스 목록을 정의합니다. 이 ACL은 터널을 통해 도달할 수 있도록 FlexVPN 스포크에 푸시되는 네트워크를 정의합니다.

```
!
ip access-list standard FlexTraffic
 permit 10.10.1.0 0.0.0.255
!
```

액세스 목록 및 IP 주소 풀은에서 **IKEv2 Authorization Policy**참조됩니다.

```
!
crypto ikev2 authorization policy HUBPolicy
 pool FlexPool
 route set interface
 route set access-list FlexTraffic
!
```

f. 를 생성하고 IKEv2 profile및 AAA 권한 keyring 부여 그룹을 할당합니다.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth HUBPolicy
 virtual-template 1
!
```

g. 데이터 보호에 사용되는 암호화 및 해시 알고리즘을 만들고 Transport Set정의합니다.

h. 를 생성하고 IPsec profile를 할당하며 IKEv2 profile 이전에 Transport Set 생성한 를 할당합니다.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

i. 를 **virtual-template 1** as **type tunnel**구성합니다. 인터페이스를 로IP unnumbered address참조하고 **IPsec profile**

```
!
interface virtual-template 1 type tunnel
 ip unnumbered loopback1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
```

2단계: 스포크 컨피그레이션

a. IKEv2 제안 및 정책을 정의합니다.

b. 키링을 구성하고 허브에 인증하는 데 사용되는 사전 공유 키를 입력합니다.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. 허브 라우터에서 AAA 서비스를 활성화한 다음 로컬 디바이스 컨피그레이션에서 정책을 지정하 **FlexAuth**는 이름이 지정된 네트워크 권한 부여 목록을 정의합니다. 다음으로, IP 주소 및 경로를

FlexVPN 스포크에 푸시하도록 모드 컨피그레이션 정책을 구성합니다.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. 이름이 지정되고 네트워크 10.20.2.0/24. **FlexTraffic**를 허용하는 표준 IP 액세스 목록을 정의합니다. 이 ACL은 이 스포크가 터널을 통과하기 위해 공유하는 네트워크를 정의합니다.

```
!
ip access-list standard FlexTraffic
 permit 10.20.2.0 0.0.0.255
!
```

액세스 목록은에 **IKEv2 Authorization Policy**할당됩니다.

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e. 를 생성하고 IKEv2 profile및 AAA 권한 keyring 부여 그룹을 할당합니다.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
!
```

f. 전송 집합을 만들고 데이터 보호에 사용되는 암호화 및 해시 알고리즘을 정의합니다.

g. IPsec 프로필을 생성하고 IKEv2 프로필 및 이전에 생성한 전송 세트를 할당합니다.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
```

```
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h. 허브(Hub)에 구성한 풀에서 얻은 협상된 IP 주소의 속성으로 터널 인터페이스를 구성합니다.

```
!
interface tunnel 0
 ip address negotiated
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.20 255.255.255.0
!
```

다음을 확인합니다.

show ip interface brief 명령을 사용하여 Tunnel, Virtual-Template 및 Virtual-Access 상태를 검토합니다.

- Hub에서 Virtual-Template의 up/down 상태는 정상입니다. 가상 액세스는 허브와의 연결을 설정하고 작동/작동 상태를 표시하는 각 스포크에 대해 생성됩니다.
- Spoke에서 터널 인터페이스가 IP 주소를 수신하고 up/up 상태를 표시합니다.

<#root>

```
FlexVPN_HUB#
```

show ip interface brief

```
Interface              IP-Address      OK? Method Status           Protocol
GigabitEthernet1       192.168.0.10    YES NVRAM  up               up
GigabitEthernet2       10.10.1.10      YES manual up               up
Loopback1              10.1.1.1        YES manual up               up
```

Virtual-Access1 10.1.1.1 YES unset up up

```
 <<<<<<< This Virtual-Access has been created and is up/up
Virtual-Template1      10.1.1.1        YES unset  up


FlexVPN_Spoke#
```

show ip interface brief

```
Interface               IP-Address      OK? Method  Status            Protocol
GigabitEthernet1        192.168.0.20    YES NVRAM   up                up
GigabitEthernet2        10.20.2.20      YES manual  up                up
```

Tunnel0 10.1.1.8 YES manual up up <<<<<<

The tunnel interface received an IP address from pool defined

- show crypto ikev2 sa 명령을 사용하여 허브와 스포크 간의 보안 연결이 설정되었는지 확인합니다.

<#root>

FlexVPN_HUB#

show crypto ikev2 sa

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 192.168.0.10/500 192.168.0.20/500 none/none

READY

Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/587 sec

IPv6 Crypto IKEv2 SA

- show crypto ipsec sa 명령을 사용하여 암호화 및 디캡스 카운터가 증가하는지 확인하여 트래픽이 암호화되어 터널을 통과하는지 확인할 수 있습니다.

<#root>

FlexVPN_HUB#

show crypto ipsec sa

interface: Virtual-Access1

Crypto map tag: Virtual-Access1-head-0, local addr 192.168.0.10

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.0.10/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (192.168.0.20/255.255.255.255/47/0)
current_peer 192.168.0.20 port 500
PERMIT, flags={origin_is_acl,}

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10

#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 192.168.0.10, remote crypto endpt.: 192.168.0.20
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
current outbound spi: 0xAFC2F841(2948790337)
PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x7E780336(2121794358)

transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 5581, flow_id: CSR:3581, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-h

sa timing: remaining key lifetime (k/sec): (4607998/3010)

IV size: 16 bytes
replay detection support: Y

Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xAFC2F841(2948790337)

transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 5582, flow_id: CSR:3582, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-

sa timing: remaining key lifetime (k/sec): (4607998/3010)

IV size: 16 bytes
replay detection support: Y

Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

- show ip route 명령을 사용하여 경로가 스포크에 푸시되었는지 확인합니다.
  - HUB 컨피그레이션의 route set interface 문 때문에 10.1.1.1/32에 대한 경로가 IKEv2 컨피그레이션 페이로드를 통해 푸시되었습니다.
  - HUB 컨피그레이션의 route set access-list FlexTraffic 문으로 인해 10.10.1.0/24에 대한 경로가 IKEv2 컨피그레이션 페이로드를 통해 푸시되었습니다.

<#root>

```
FlexVPN_Spoke#show ip route
<<< Omitted >>>

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.0.1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S        10.1.1.1/32 is directly connected, Tunnel0   <<<<<<<


C        10.1.1.8/32 is directly connected, Tunnel0
S        10.10.1.0/24 is directly connected, Tunnel0  <<<<<<<


C        10.20.2.20/32 is directly connected, GigabitEthernet2
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet1
L        192.168.0.20/32 is directly connected, GigabitEthernet1
```

- 보급된 네트워크에 대한 연결을 확인하려면 ping 명령을 사용합니다.

<#root>

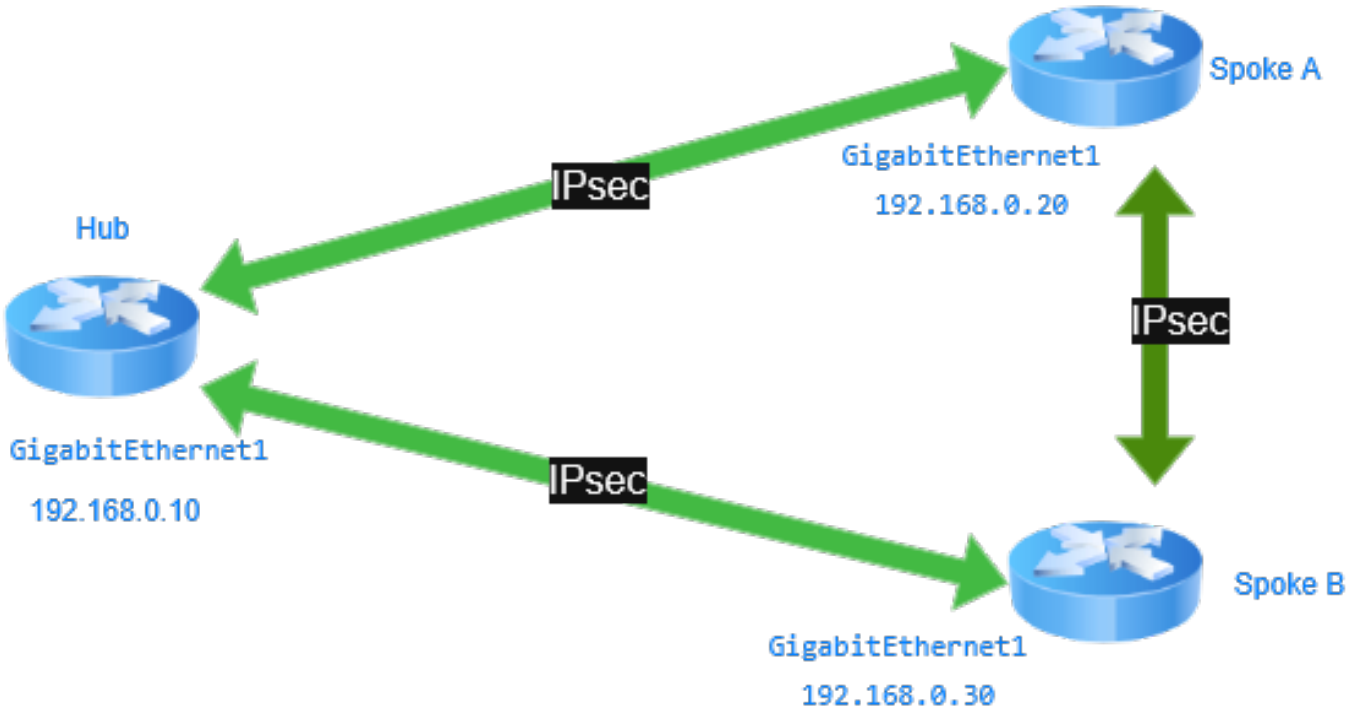
```
FlexVPN_HUB#

ping 10.20.2.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.2.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms



FlexVPN_Spoke#

ping 10.10.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.10, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

스포크 투 스포크 FlexVPN

스포크 투 스포크(Spoke to Spoke) 연결을 사용하는 허브 및 스포크 토폴로지의 FlexVPN은 동적이고 확장 가능하며 안전한 VPN 통신을 지원합니다. 허브는 NHRP가 스포크가 허브에 다른 스포크 IP 주소를 쿼리할 수 있도록 하는 중앙 제어 지점 역할을 하므로 효율적인 통신 및 지연 시간 감소를 위해 스포크 IPsec 터널에 직접 스포크를 사용할 수 있습니다.

허브에서 이 명령을 **ip nhrp redirect** 사용하여 스포크 통신에 직접 스포크가 가능함을 스포크에 알리고, 데이터 플레인 트래픽에 대해 허브를 우회하여 트래픽 흐름을 최적화합니다. 스포크에서 이 명령을 **ip nhrp shortcut** 사용하면 허브에서 리디렉션을 수신한 후 다른 스포크와 직접 터널을 동적으로 설정할 수 있습니다. 다이어그램은 Hub와 Spoke 간 및 Spoke와 Spoke 간 통신을 참조합니다.



스포크_투_스포크_다이어그램

1단계: 허브 컨피그레이션

a. IKEv2 정책 및 프로파일을 정의합니다.

b. 를 keyring 구성하고 스포크를 인증하Pre-Shared Key는 데 사용되는 를 입력합니다.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
```

```
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. 허브 라우터에서 AAA 서비스를 활성화한 다음 로컬 디바이스 컨피그레이션에서 정책을 지정하 **FlexAuth**는 이름이 지정된 네트워크 권한 부여 목록을 정의한 다음 IP 주소 및 경로를 FlexVPN 스포크에 푸시하도록 모드 컨피그레이션 정책을 구성합니다.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. 주소 10.1.1.2~10.1.1.254를 포함하는IP address pool **FlexPool**, 명명된 이름을 정의합니다. 이 풀은 스포크의 터널 인터페이스에 IP 주소를 자동으로 할당하는 데 사용됩니다.

```
!
ip local pool FlexPool 10.1.1.2 10.1.1.254
!
```

e. 이름이FlexTraffic지정되고 네트워크 10.0.0.0/8을 허용하는 표준 IP 액세스 목록을 정의합니다. 이 ACL은 허브에 연결된 다른 스포크의 네트워크를 포함하여 FlexVPN 스포크에 푸시되는 네트워크를 정의하므로, 스포크는 해당 네트워크가 허브를 통해 먼저 도달했음을 알 수 있습니다.

```
!
ip access-list standard FlexTraffic
 permit 10.0.0.0 0.255.255.255
!
```

액세스 목록 및 IP address pool 이(가) 에 할당됩니다**IKEv2 Authorization Policy**.

```
!
crypto ikev2 authorization policy HUBPolicy
```

```
 pool FlexPool
 route set interface
 route set access-list FlexTraffic
!
```

f. 를 생성하고 IKEv2 profile및 AAA 권한 keyring 부여 그룹을 할당합니다.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth HUBPolicy
 virtual-template 1
!
```

g. 를 Transport Set 생성하고 데이터를 보호하는 데 사용되는 암호화 및 해시 알고리즘을 정의합니다.

h. 를 생성하고, IPsec profile를 할당하며IKEv2 profile, 이전에 Transport Set 생성한 를 할당합니다.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

i. 를 **virtual-template 1** as **type tunnel**구성합니다. 인터페이스를 로 **IP unnumbered address** 참조하고 를 **IPsec profile**적용합니다.

이 **ip nhrp redirect** 명령은 Virtual-Template에서 구성하여 스포크가 네트워크에 연결하기 위해 다른 스포크와 직접 연결할 수 있도록 알립니다.

```
!
interface virtual-template 1 type tunnel
 ip unnumbered loopback1
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
```

2단계: Spoke A 구성

a. IKEv2 정책 및 프로파일을 정의합니다.

b. 를 keyring 구성하고 스포크를 인증하Pre-Shared Key는 데 사용되는 를 입력합니다.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. 허브 라우터에서 AAA 서비스를 활성화한 다음 로컬 디바이스 컨피그레이션에서 정책을 지정하 **FlexAuth**는 이름이 지정된 네트워크 권한 부여 목록을 정의합니다. 다음으로, IP 주소 및 경로를 FlexVPN 스포크에 푸시하도록 모드 컨피그레이션 정책을 구성합니다.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. 이름이 지정되고 네트워크 10.20.2.0/24**FlexTraffic**를 허용하는 표준 IP 액세스 목록을 정의합니다. 이 ACL은 이 스포크가 터널을 통과하기 위해 공유하는 네트워크를 정의합니다.

```
!
ip access-list standard FlexTraffic
 permit 10.20.2.0 0.0.0.255
!
```

액세스 목록은 **IKEv2 Authorization Policy.**

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
```

```
 route set access-list FlexTraffic
!
```

e. 를 생성하고 IKEv2 profile 및 AAA 권한 keyring 부여 그룹을 할당합니다.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
 virtual-template 1
!
```

f. 를 Transport Set 생성하고 데이터를 보호하는 데 사용되는 암호화 및 해시 알고리즘을 정의합니다.

g. IPsec 프로필을 생성하고 IKEv2 프로필 및 이전에 생성한 전송 세트를 할당합니다.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h. tunnelinterface 및 virtualtemplate을 구성합니다. **Virtual-Template1** 지원하도록 생성된 dVTI에 대해 **NHRP shortcuts**지정합니다. 또한tunnel0에서 번호가 지정되지 않은 주소로virtual-template설정합니다.

명령**ip nhrp shortcut**은 허브의 NHRP 리디렉션 메시지를 기반으로 다른 스포크에 대한 직접 터널을 동적으로 설정할 수 있도록 스포크에서 구성됩니다.

```
!
interface tunnel 0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface virtual-template 1 type tunnel
 ip unnumbered tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
```

```
 tunnel source GigabitEthernet1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.20 255.255.255.0
!
```

3단계: 스포크 B 컨피그레이션

a. IKEv2 정책 및 프로파일을 정의합니다.

b. 를 keyring 구성하고 스포크를 인증하Pre-Shared Key는 데 사용되는 를 입력합니다.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. 허브 라우터에서 AAA 서비스를 활성화한 다음 로컬 디바이스 컨피그레이션에서 정책을 지정하 **FlexAuth**는 이름이 지정된 네트워크 권한 부여 목록을 정의한 다음 IP 주소 및 경로를 FlexVPN 스포크에 푸시하도록 모드 컨피그레이션 정책을 구성합니다.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. 이름이 지정되고 네트워크 10.30.3.0/24. **FlexTraffic**를 허용하는 표준 IP 액세스 목록을 정의합니다. 이 ACL은 이 스포크가 터널을 통과하기 위해 공유하는 네트워크를 정의합니다.

```
!
ip access-list standard FlexTraffic
 permit 10.30.3.0 0.0.0.255
!
```

액세스 목록은 IKEv2 Authorization Policy.

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e. 를 생성하고 IKEv2 profile및 AAA 권한 keyring 부여 그룹을 할당합니다.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
 virtual-template 1
!
```

f. 를 Transport Set 생성하고 데이터를 보호하는 데 사용되는 암호화 및 해시 알고리즘을 정의합니다.

g. 를 생성하고 IPsec profile를 할당하며 IKEv2 profile 이전에 Transport Set 생성했습니다.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h. 및 을 tunnel interface 구성합니다virtual template. 지원**Virtual-Template1**을 위해 생성된 dVTI에 대해 지정합니다NHRP shortcuts. 또한tunnel0에서 번호가 지정되지 않은 주소로virtual-template설정합니다.

명령**ip nhrp shortcut**은 허브의 NHRP 리디렉션 메시지를 기반으로 다른 스포크에 대한 직접 터널을 동적으로 설정할 수 있도록 스포크에서 구성됩니다.

```
!
interface tunnel 0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
```

```
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface virtual-template 1 type tunnel
 ip unnumbered tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.30 255.255.255.0
!
```

다음을 확인합니다.

show ip interface brief 명령을 사용하여 Tunnel, Virtual-Template 및 Virtual-Access 상태를 검토합니다. 이제 스포크-투-스포크 직접 연결입니다.

- Spokes에서 Virtual-Template의 up/down 상태는 정상입니다. Virtual-Access는 Up/Up 상태의 연결을 위해 생성됩니다.

<#root>

FlexVPN_Spoke#

show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet1	192.168.0.30	YES	NVRAM	up	up
GigabitEthernet2	10.20.2.20	YES	manual	up	up
Tunnel0	**10.1.1.12**	**YES**	**manual**	**up**	**up**
Virtual-Access1	**10.1.1.12**	**YES**	**unset**	**up**	**up**
Virtual-Template1	10.1.1.12	YES	unset	up	down

- 각 디바이스 간 보안 연결이 설정되었는지 확인하려면 show crypto ikev2 sa 명령을 사용합니다.
- show crypto ipsec sa 명령을 사용하여 암호화 및 디캡스 카운터가 증가하는지 확인하여 트래픽이 암호화되어 터널을 통과하는지 확인할 수 있습니다.
- show ip nhrp 명령을 사용하여 스포크 간 트래픽 리디렉션을 확인합니다.
  <#root>

  FlexVPN_Spoke#

  show ip nhrp

  10.1.1.10/32 via 10.1.1.10

```
   Virtual-Access1 created 00:00:13, expire 00:09:46
   Type:
```

dynamic

```
, Flags: router nhop rib nho
   NBMA address: 192.168.0.30
```

10.30.3.0/24 via 10.1.1.10

```
   Virtual-Access1 created 00:00:13, expire 00:09:46
   Type:
```

dynamic

```
, Flags: router rib nho
   NBMA address: 192.168.0.30
```

show ip route 명령을 사용하여 경로가 스포크에 푸시되었는지 확인합니다.

- 두 경로는 Virtual-Access1 인터페이스에 연결되며 새로운 경로이며 NHRP 바로 가기와 연결됩니다.
- % 문자는 next-hop 재정의를 나타냅니다.

<#root>

```
FlexVPN_Spoke#sh ip route
<<<< Omitted >>>>

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.0.1
      10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
S        10.0.0.0/8 is directly connected, Tunnel0
S        10.1.1.1/32 is directly connected, Tunnel0
```

S %   10.1.1.10/32 is directly connected, Virtual-Access1

```
C        10.1.1.12/32 is directly connected, Tunnel0
C        10.20.2.20/32 is directly connected, GigabitEthernet2
```

S %   10.30.3.0/24 is directly connected, Virtual-Access1

```
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet1
L        192.168.0.30/32 is directly connected, GigabitEthernet1
```

- 보급된 네트워크에 대한 연결을 확인하려면 ping 명령을 사용합니다.

<#root>

```
FlexVPN_Spoke#
```

```
ping 10.30.3.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.30.3.30, timeout is 2 seconds:

.!!!!


Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다. 다음 명령을 사용하여 터널 협상 프로세스를 디버깅할 수 있습니다.

```
debug crypto interface

debug crypto ikev2
debug crypto ikev2 client flexvpn
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ikev2 packet

debug crypto ipsec
debug crypto ipsec error
debug crypto ipsec message
debug crypto ipsec states
```

NHRP 디버그는 스포크 대 스포크 연결의 트러블슈팅에 도움이 될 수 있습니다.

```
debug nhrp
debug nhrp detail
debug nhrp event
debug nhrp error
debug nhrp packet
debug nhrp routing
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.