FlexVPN 클라이언트 블록 컨피그레이션을 사용한 이중화 허브 설계의 FlexVPN 스포크 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.

배경 정보

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 타이머에 따라 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. • 느린 복구 시간 - DPD(Dead Peer Detection) 또는 (선택 사항) 객체 추적을 기반으로 함
장애 조치	• 손쉬운 구성 - FlexVPN에 내장 • 장애 시 라우팅 프로토콜에 의존하지 않음	• 모든 트래픽은 한 번에 하나의 허브로 이동해야 합니다.

이 문서에서는 두 번째 접근 방식에 대해 설명합니다.

구성

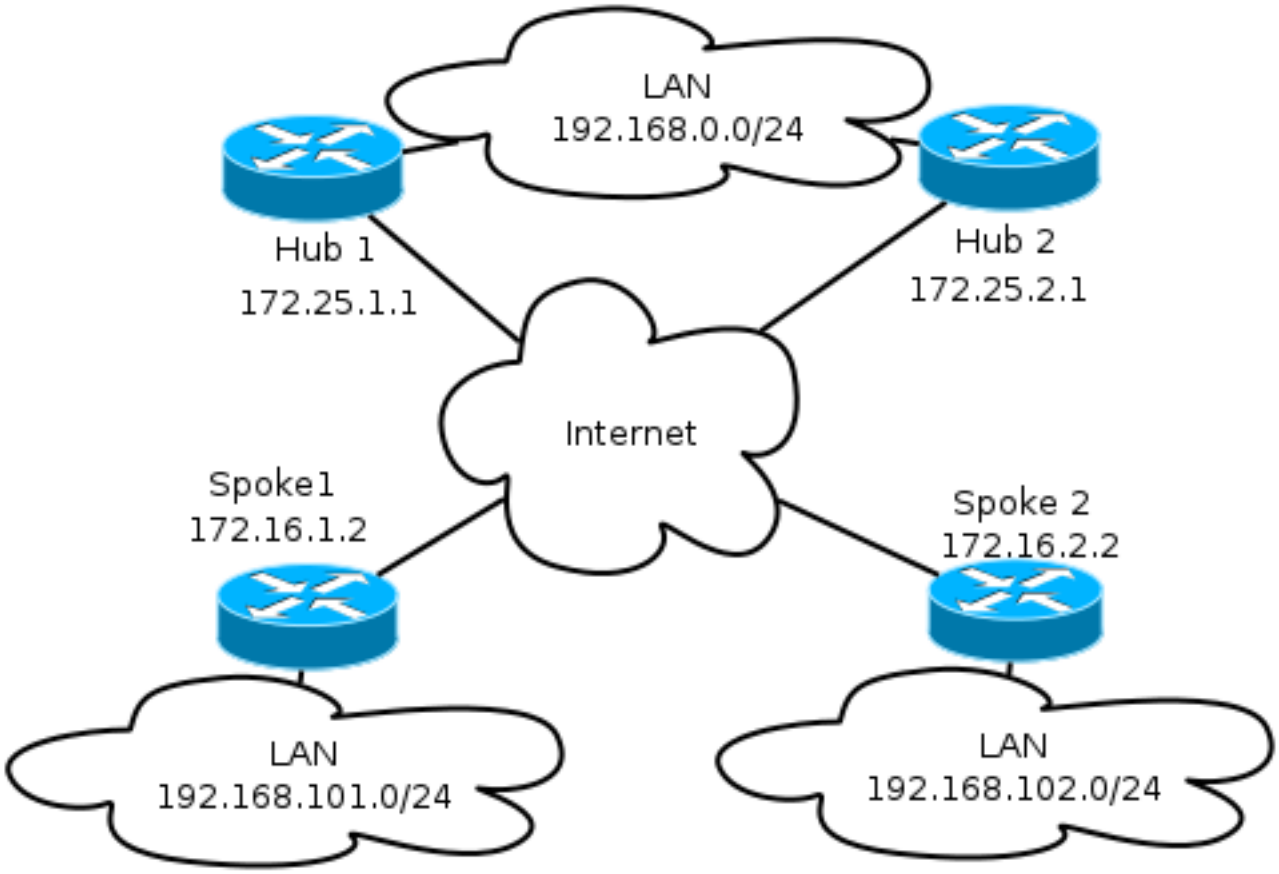
> **참고:** 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

네트워크 다이어그램

이러한 다이어그램에는 전송 및 오버레이 토폴로지 다이어그램이 모두 표시됩니다.

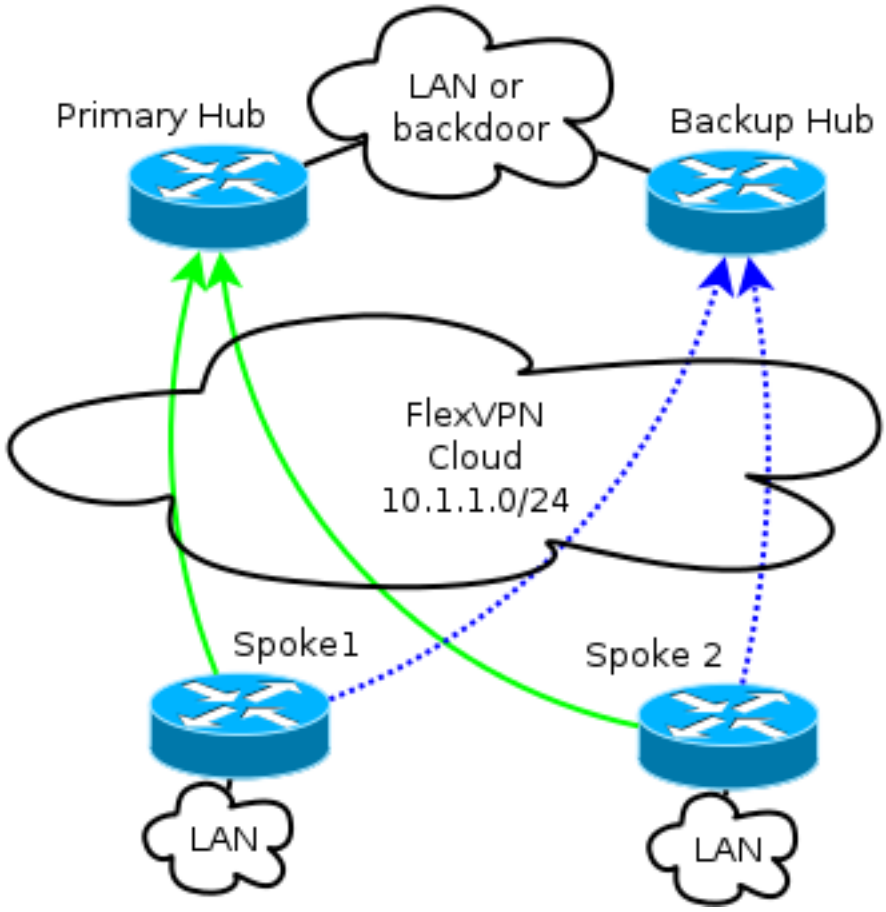
전송 네트워크

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 중에는 Spoke 1 및 Spoke 2는 하나의 허브만 관계를 유지합니다.



참고: 다이어그램에서 녹색 선은 기본 IKEv2(Internet Key Exchange Version 2)/Flex 세션의 연결 및 방향을 보여주고, 점선 파란색 선은 기본 허브에 대한 IKE(Internet Key Exchange) 세션이 실패할 경우 백업 연결을 나타냅니다.

/24 주소는 이 클라우드에 할당된 주소 풀을 나타내며 실제 인터페이스 주소 지정을 나타냅니다. 이는 FlexVPN 허브가 일반적으로 스포크 인터페이스에 동적 IP 주소를 할당하고 FlexVPN 권한 부여 블록의 경로 명령을 통해 동적으로 삽입되는 경로를 사용하기 때문입니다.

스포크 및 허브의 기본 구성

허브 및 스포크의 기본 컨피그레이션은 DMVPN(Dynamic Multipoint VPN)에서 FlexVPN으로의 마이그레이션 문서를 기반으로 합니다. 이 컨피그레이션은 FlexVPN 마이그레이션에서 설명합니다. Hard Move from DMVPN to FlexVPN on Same Devices 기사

스포크 구성 조정

Spoke 구성 - 클라이언트 구성 블록

Spoke 구성은 클라이언트 구성 블록에 의해 확장되어야 합니다.

기본 컨피그레이션에서는 여러 피어가 지정됩니다. 우선순위가 가장 높은(가장 낮은) 피어는 다른 피어보다 먼저 고려됩니다.

```
crypto ikev2 client flexvpn Flex_Client
peer 1 172.25.1.1
peer 2 172.25.2.1
client connect Tunnel1
```

FlexVPN 클라이언트 컨피그레이션 블록을 기반으로 터널 대상을 동적으로 선택할 수 있도록 하려면 터널 컨피그레이션을 변경해야 합니다.

```
interface Tunnel1
 tunnel destination dynamic
```

FlexVPN 클라이언트 컨피그레이션 블록이 IKEv2 또는 IPsec(Internet Protocol Security) 프로파일이 아닌 인터페이스에 연결되어 있다는 점을 기억해야 합니다.

클라이언트 컨피그레이션 블록은 추적 객체 사용, 다이얼 백업, 백업 그룹 기능 등 장애 조치 시간 및 작업을 조정하기 위해 여러 옵션을 제공합니다.

기본 컨피그레이션에서는 스포크가 응답하지 않는지 여부를 탐지하기 위해 스포크가 DPD에 의존하며 피어가 데드로 선언되면 변경 사항이 트리거됩니다. DPD의 작동 방식 때문에 DPD를 사용하는 옵션은 빠른 옵션이 아닙니다. 관리자는 객체 추적 또는 이와 유사한 개선 사항을 통해 구성을 개선하고자 할 수 있습니다.

자세한 내용은 이 문서 끝의 **관련 정보** 섹션에 링크되어 있는 Cisco IOS 컨피그레이션 가이드의 **FlexVPN 클라이언트 컨피그레이션** 장을 참조하십시오.

전체 스포크 구성 - 참조

```
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 ikev2 client flexvpn Flex_Client
 peer 1 172.25.1.1
 peer 2 172.25.2.1
 client connect Tunnel1

crypto ipsec transform-set IKEv2 esp-gcm
 mode transport

crypto ipsec profile default
 set ikev2-profile Flex_IKEv2
```

```
interface Tunnel1
 description FlexVPN 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
 delay 2000
 tunnel source Ethernet0/0
 tunnel destination dynamic
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
```

허브 구성

허브 컨피그레이션의 대부분은 동일하게 유지되지만 몇 가지 사항을 해결해야 합니다. 대부분의 스포크는 한 개 이상의 스포크가 한 허브에 연결되어 있는 반면 다른 스포크는 다른 허브와 계속 관련되어 있는 상황과 관련이 있습니다.

스포크 주소

스포크는 허브에서 IP 주소를 얻으므로 일반적으로 허브가 다른 서브넷 또는 서브넷의 다른 부분에서 주소를 할당하는 것이 좋습니다.

예를 들면 다음과 같습니다.

허브1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.175
```

허브2

```
ip local pool FlexSpokes 10.1.1.176 10.1.1.254
```

이렇게 하면 주소가 FlexVPN 클라우드 외부로 라우팅되지 않은 경우에도 중복 생성이 방지되므로 문제 해결에 지장을 줄 수 있습니다.

허브 오버레이 주소

두 허브 모두 가상 템플릿 인터페이스에서 동일한 IP 주소를 유지할 수 있습니다. 그러나 경우에 따라 문제 해결에 영향을 미칠 수 있습니다. 이러한 설계 선택을 통해 스포크는 BGP(Border Gateway Protocol)에 대해 피어 주소가 하나만 있어야 하므로 구축 및 계획을 보다 쉽게 수행할 수 있습니다.

경우에 따라, 이것은 원하지 않거나 필요하지 않을 수도 있습니다.

라우팅

허브가 연결된 스포크에 대한 정보를 교환해야 합니다.

허브는 연결된 디바이스의 특정 경로를 교환할 수 있어야 하며 스포크에 요약 정보를 제공해야 합

니다.

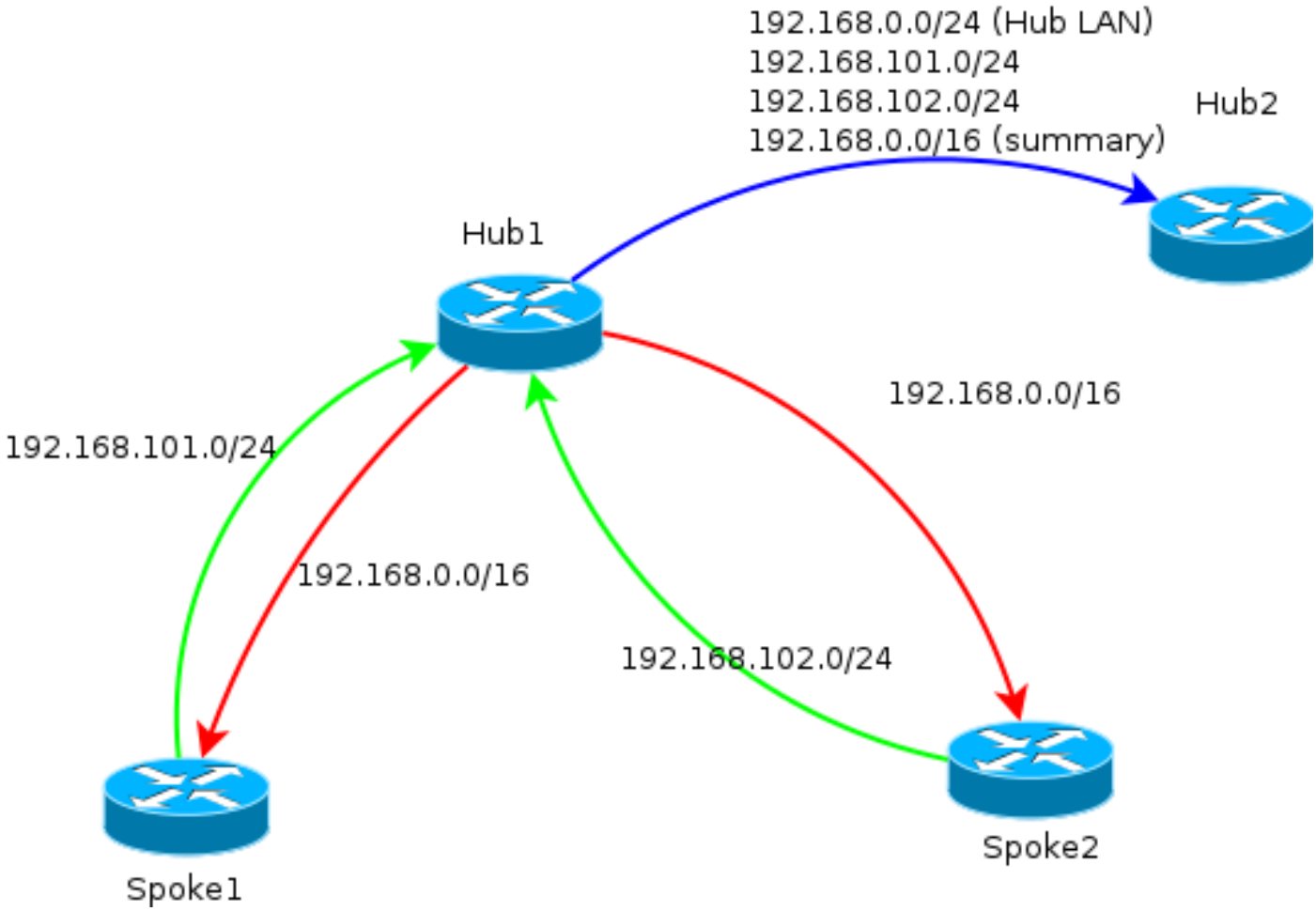
Cisco에서는 FlexVPN 및 DMVPN에서 iBGP를 사용하는 것이 권장되므로 해당 라우팅 프로토콜만 표시됩니다.

```
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
neighbor Spokes peer-group
neighbor Spokes remote-as 65001
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

access-list 1 permit any

route-map ALL permit 10
match ip address 1
```

이 컨피그레이션에서는 다음을 수행할 수 있습니다.

- 스포크에 할당된 주소의 동적 리스너
- 192.168.0.0/24의 광고 네트워크
- 모든 스포크에 192.168.0.0/16의 광고 요약 경로 aggregate-address 컨피그레이션은 null0 인터페이스를 통해 해당 접두사에 대한 고정 경로를 생성합니다. 이는 라우팅 루프를 방지하기 위해 사용되는 폐기 경로입니다.
- 특정 접두사를 다른 허브에 전달
- Route-reflector 클라이언트는 허브가 서로 스포크에서 학습된 정보를 교환하도록 합니다.

이 다이어그램은 허브 중 하나의 관점에서 이 설정의 BGP에서 접두사 교환을 나타냅니다.



참고: 이 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.

네트워크 요약 사용

일부 시나리오에서는 요약이 적용되지 않거나 필요하지 않을 수 있습니다. iBGP는 기본적으로 다음 홉을 재정의하지 않으므로 접두사에서 대상 IP를 지정할 때는 주의해야 합니다.

상태를 자주 변경하는 네트워크에서는 요약을 권장합니다. 예를 들어, 불안정한 인터넷 연결을 위해 다음과 같은 목적으로 요약이 필요할 수 있습니다. 접두사가 제거되거나 추가되지 않도록 하고, 업데이트 수를 제한하며, 대부분의 설정이 제대로 확장되도록 합니다.

스포크 투 스포크 터널

이전 섹션에서 설명한 시나리오 및 컨피그레이션에서는 다른 허브의 스포크가 직접 스포크 투 스포크 터널을 설정할 수 없습니다. 서로 다른 허브에 연결된 스포크 간 트래픽은 중앙 디바이스를 통해 이동합니다.

이를 위한 쉬운 해결 방법이 있습니다. 그러나 허브 간에 동일한 네트워크 ID를 가진 NHRP(Next Hop Resolution Protocol)가 활성화되어 있어야 합니다. 예를 들어, 허브 간에 포인트 투 포인트 GRE(Generic Routing Encapsulation) 터널을 생성하는 경우 이 작업을 수행할 수 있습니다. 그러면 IPsec이 필요하지 않습니다.

다음을 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

show crypto ikev**2 sa** 명령은 스포크가 현재 연결된 위치를 알려줍니다.

show crypto ikev**2 client flexvpn** 명령을 사용하면 관리자가 FlexVPN 클라이언트 작업의 현재 상태를 이해할 수 있습니다.

```
Spoke2# show crypto ikev2 client flexvpn

Profile : Flex_Client
Current state:ACTIVE
Peer : 172.25.1.1
Source : Ethernet0/0
ivrf : IP DEFAULT
fvrf : IP DEFAULT
Backup group: Default
Tunnel interface : Tunnel1
Assigned IP address: 10.1.1.111
```

show logging 컨피그레이션으로 장애 조치를 성공적으로 수행하면 스포크 디바이스에서 이 출력이 기록됩니다.

```
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is DOWN.  Peer 172.25.1.1:500
Id: 172.25.1.1
%FLEXVPN-6-FLEXVPN_CONNECTION_DOWN: FlexVPN(Flex_Client) Client_public_addr =
172.16.2.2 Server_public_addr = 172.25.1.1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP.  Peer 172.25.2.1:500
Id: 172.25.2.1
%FLEXVPN-6-FLEXVPN_CONNECTION_UP: FlexVPN(Flex_Client) Client_public_addr =
172.16.2.2 Server_public_addr = 172.25.2.1 Assigned_Tunnel_v4_addr = 10.1.1.177
```

이 출력에서 스포크는 **허브 172.25.1.1에서** 연결을 해제하며 Flex_Client 구성 블록은 오류를 감지하고 터널이 발생하는 **172.25.2.1**에 강제로 연결하며 스포크는 **10.1.1.177**의 IP를 할당합니다.

문제 해결

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

> **참고: debug** 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

관련 debug 명령은 다음과 같습니다.

- **디버그 암호화 ikev2**
- **디버그 반경**

관련 정보

- FlexVPN 및 Internet Key Exchange 버전 2 컨피그레이션 가이드, Cisco IOS 릴리스 15 M&T
- 기술 지원 및 문서 – Cisco Systems