동일한 서버의 레거시 EzVPN-NEM+에서 FlexVPN으로 마이그레이션

목차

소개

이 문서에서는 EzVPN에서 FlexVPN으로의 마이그레이션 프로세스에 대해 설명합니다. FlexVPN은 Cisco에서 제공하는 새로운 통합 VPN 솔루션입니다. FlexVPN은 IKEv2 프로토콜을 활용하고 원격 액세스, 사이트 간, 허브 및 스포크, 부분 메시 VPN 구축을 결합합니다. EzVPN과 같은 레거시 기술을 통해 Cisco는 풍부한 기능을 활용하기 위해 FlexVPN으로 마이그레이션할 것을 적극 권장합니다.

이 문서에서는 레거시 암호화 맵 기반 EzVPN 헤드엔드 디바이스에서 터널을 종료하는 레거시 EzVPN 하드웨어 클라이언트로 구성된 기존 EzVPN 구축을 살펴봅니다. 목표는 이 구성에서 FlexVPN을 지원하도록 마이그레이션하여 다음과 같은 요건을 충족하는 것입니다.

- 기존 레거시 클라이언트는 컨피그레이션을 변경하지 않고도 계속 원활하게 작동합니다. 이를 통해 이러한 클라이언트를 FlexVPN으로 단계적으로 마이그레이션할 수 있습니다.
- 헤드엔드 디바이스는 새로운 FlexVPN 클라이언트의 종료를 동시에 지원해야 합니다.

이러한 마이그레이션 목표를 달성하기 위해 두 가지 주요 IPsec 구성 요소가 사용됩니다. 즉, IKEv2 및 VTI(Virtual Tunnel Interfaces)입니다. 이 문서에서는 이러한 목표에 대해 간략하게 설명합니다.

이 시리즈의 기타 문서

- FlexVPN 구축 설명서: IKEv2 및 인증서를 사용하는 IOS Headend Over IPsec에 AnyConnect

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

IKEv1 vs IKEv2

FlexVPN은 RFC 4306을 기반으로 하는 차세대 키 관리 프로토콜인 IKEv2 프로토콜과 IKEv1 프로토콜의 개선을 기반으로 합니다. FlexVPN은 IKEv1(예: EzVPN)만 지원하는 기술과 역호환되지 않습니다. 이는 EzVPN에서 FlexVPN으로 마이그레이션할 때 고려해야 할 주요 사항 중 하나입니다. IKEv2에 대한 프로토콜 소개 및 IKEv1과의 비교에 대해서는 IKE 버전 2 살펴보기를 참조하십시오.

암호화 맵 대 가상 터널 인터페이스

VTI(Virtual Tunnel Interface)는 VPN 서버 및 클라이언트 컨피그레이션에 모두 사용되는 새로운 컨피그레이션 방법입니다. VTI:

- 이제 레거시 컨피그레이션으로 간주되는 동적 암호화 맵의 교체.
- 네이티브 IPsec 터널링을 지원합니다.
- 물리적 인터페이스에 IPsec 세션을 정적 매핑하지 않아도 됩니다. 따라서 모든 물리적 인터페이스(예: 다중 경로)에서 암호화된 트래픽을 보내고 받을 수 있는 유연성을 제공합니다.
- 가상 템플릿 인터페이스에서 온디맨드 가상 액세스가 복제될 때 최소한의 컨피그레이션
- 트래픽은 터널 인터페이스로 전달/전달 시 암호화/해독되며 IP 라우팅 테이블에 의해 관리됩니다(따라서 암호화 프로세스에서 중요한 역할을 함).
- VTI 인터페이스의 일반 텍스트 패킷에 기능을 적용하거나 물리적 인터페이스의 암호화된 패킷에 기능을 적용할 수 있습니다.

사용 가능한 VTI의 두 가지 유형은 다음과 같습니다.

- 고정(sVTI) - 고정 가상 터널 인터페이스에는 고정 터널 소스와 대상이 있으며 일반적으로 사이트 간 구축 시나리오에서 사용됩니다. 다음은 sVTI 컨피그레이션의 예입니다.

```
interface Tunnel2
```

```
 ip address negotiated
 tunnel source Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile testflex
```

- 동적(dVTI) - 동적 가상 터널 인터페이스를 사용하여 고정 터널 대상이 없는 동적 IPsec 터널을 종료할 수 있습니다. 터널 협상이 성공하면 Virtual-Access 인터페이스는 Virtual-Template에서 복제되고 해당 Virtual-Template의 모든 L3 기능을 상속합니다. dVTI 컨피그레이션의 예는 다음과 같습니다.

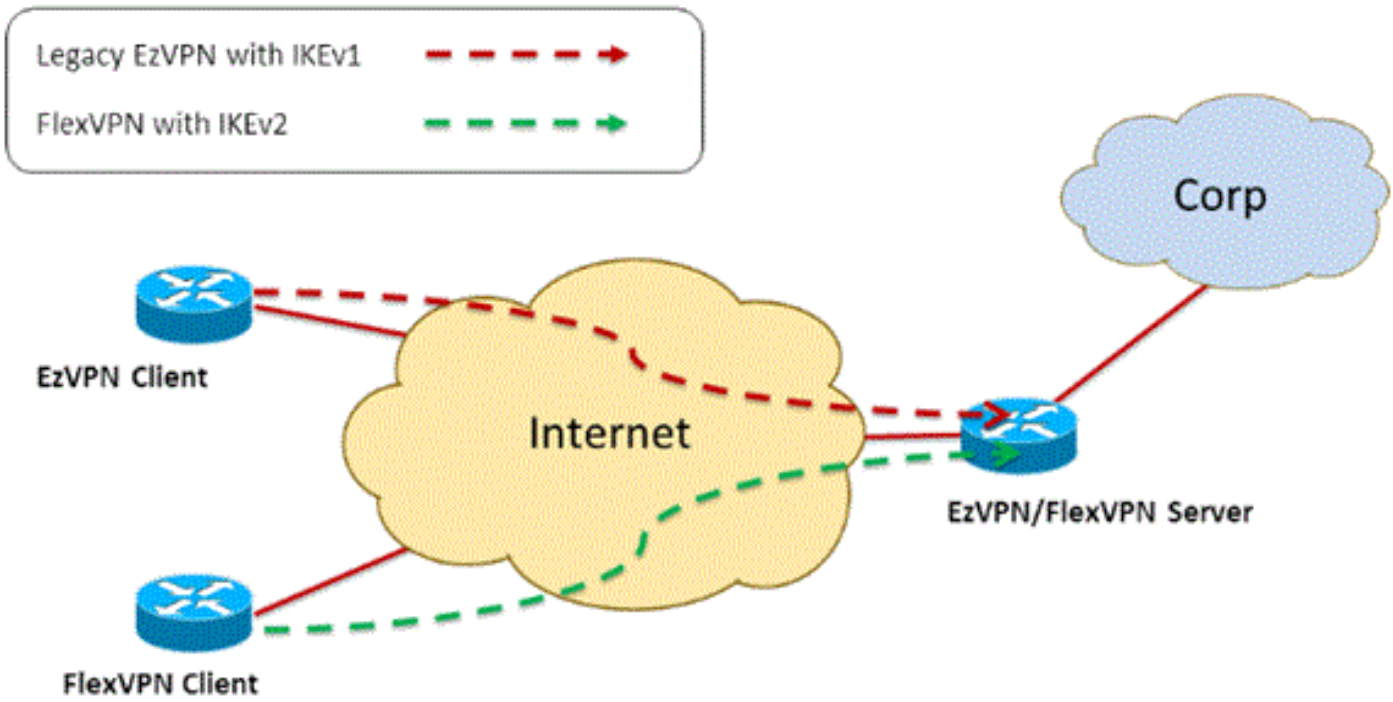
```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile testflex
```

dVTI에 대한 자세한 내용은 다음 문서를 참조하십시오.

- IPSec DVTI(Dynamic Virtual Tunnel Interface)를 사용하여 Cisco Easy VPN 구성
- IPsec 가상 터널 인터페이스에 대한 제한 사항
- IKEv1을 사용하여 동적 가상 터널 인터페이스에 대한 다중 SA 지원 구성

EzVPN 및 FlexVPN 클라이언트가 공존하려면 먼저 레거시 암호화 맵 컨피그레이션에서 dVTI 컨피그레이션으로 EzVPN 서버를 마이그레이션해야 합니다. 다음 섹션에서는 필요한 단계를 자세히 설명합니다.

네트워크 토폴로지



레거시 NEM+ 모드 EzVPN 클라이언트를 사용하는 현재 컨피그레이션

클라이언트 구성

다음은 일반적인 EzVPN 클라이언트 라우터 컨피그레이션입니다. 이 컨피그레이션에서는

NEM+(Network Extension Plus) 모드가 사용됩니다. 이 모드는 LAN 내부 인터페이스와 클라이언트에 할당된 모드 컨피그레이션 모두에 대해 여러 SA 쌍을 생성합니다.

```
crypto ipsec client ezvpn legacy-client
 connect manual
 group Group-One key cisco123
 mode network-plus
 peer 192.168.1.10
 username client1 password client1
 xauth userid mode local
!
interface Ethernet0/0
 description EzVPN WAN interface
 ip address 192.168.2.101 255.255.255.0
 crypto ipsec client ezvpn legacy-client
!
interface Ethernet1/0
 description EzVPN LAN inside interface
 ip address 172.16.1.1 255.255.255.0
 crypto ipsec client ezvpn legacy-client inside
```

서버 구성

EzVPN 서버에서 레거시 암호화 맵 컨피그레이션은 마이그레이션 전에 기본 컨피그레이션으로 사용됩니다.

```
aaa new-model
!
aaa authentication login client-xauth local
aaa authorization network ezvpn-author local
!
username client1 password 0 client1
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp client configuration group Group-One
 key cisco123
 pool Group-One-Pool
 acl split-tunnel-acl
crypto isakmp profile Group-One-Profile
   match identity group Group-One
   client authentication list client-xauth
   isakmp authorization list ezvpn-author
   client configuration address respond
!
crypto ipsec transform-set aes-sha esp-aes esp-sha-hmac
!
crypto dynamic-map client-dynamic-map 1
 set transform-set aes-sha
 reverse-route
!
crypto map client-map 1 ipsec-isakmp dynamic client-dynamic-map
!
interface Ethernet0/0
 description EzVPN server WAN interface
 ip address 192.168.1.10 255.255.255.0
```

```
 crypto map client-map
!
ip local pool Group-One-Pool 10.1.1.100 10.1.1.200
!
ip access-list extended split-tunnel-acl
  remark EzVPN split tunnel ACL
 permit ip 172.16.0.0 0.0.0.255 any
```

FlexVPN으로 서버 마이그레이션

이전 섹션에서 설명한 대로 FlexVPN은 IKEv2를 컨트롤 플레인 프로토콜로 사용하며 IKEv1 기반 EzVPN 솔루션과 역호환되지 않습니다. 따라서 이 마이그레이션의 일반적인 개념은 기존 EzVPN(IKEv1) 및 FlexVPN(IKEv2)을 공존할 수 있도록 기존 EzVPN 서버를 구성하는 것입니다. 이 목표를 달성하기 위해 다음 2단계 마이그레이션 방식을 사용할 수 있습니다.

1. 헤드엔드의 레거시 EzVPN 컨피그레이션을 암호화 맵 기반 컨피그레이션에서 dVTI로 이동합니다.
2. dVTI를 기반으로 하는 FlexVPN 컨피그레이션을 추가합니다.

레거시 암호화 맵을 dVTI로 이동

서버 구성 변경

물리적 인터페이스에서 암호화 맵으로 구성된 EzVPN 서버에는 기능 지원 및 유연성에 대한 몇 가지 제한 사항이 포함됩니다. EzVPN이 있는 경우 Cisco는 dVTI를 대신 사용하도록 적극 권장합니다. 기존 EzVPN 및 FlexVPN 컨피그레이션으로 마이그레이션하려면 먼저 dVTI 컨피그레이션으로 변경해야 합니다. 이렇게 하면 두 클라이언트 유형을 모두 수용할 수 있도록 서로 다른 가상 템플릿 인터페이스 간에 IKEv1 및 IKEv2 분리가 제공됩니다.

참고: EzVPN 클라이언트에서 EzVPN 작업의 Network Extension Plus Mode를 지원하려면 헤드엔드 라우터가 dVTI에서 다중 SA 기능을 지원해야 합니다. 이를 통해 여러 IP 흐름을 터널에 의해 보호할 수 있습니다. 이는 헤드엔드에서 EzVPN 클라이언트의 내부 네트워크에 대한 트래픽을 암호화하고 IKEv1 모드 컨피그레이션을 통해 클라이언트에 할당된 IP 주소를 암호화하는 데 필요합니다. IKEv1을 사용하는 dVTI에서 다중 SA 지원에 대한 자세한 내용은 IKEv1용 동적 가상 터널 인터페이스에 대한 Multi-SA Support를 참조하십시오.

서버에서 컨피그레이션 변경을 구현하려면 다음 단계를 완료하십시오.

1단계 - EzVPN 클라이언트 터널을 종료하는 물리적 이그레스 인터페이스에서 암호화 맵을 제거합니다.

```
interface Ethernet0/0
 ip address 192.168.1.10 255.255.255.0
 no crypto map client-map
```

2단계 - 터널이 설정되면 가상 액세스 인터페이스를 복제할 가상 템플릿 인터페이스를 생성합니다.

```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet1/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile legacy-profile
```

3단계 - 새로 생성된 이 가상 템플릿 인터페이스를 구성된 EzVPN 그룹의 isakmp 프로필에 연결합니다.

```
crypto isakmp profile Group-One-Profile
   match identity group Group-One
   client authentication list client-xauth
   isakmp authorization list ezvpn-author
   client configuration address initiate
   client configuration address respond
   virtual-template 1
```

위의 컨피그레이션이 변경되면 기존 EzVPN 클라이언트가 계속 작동하는지 확인합니다. 그러나 이제 동적으로 생성된 가상 액세스 인터페이스에서 터널이 종료됩니다. 이 예와 같이 **show crypto session** 명령을 사용하여 확인할 수 있습니다.

```
PE-EzVPN-Server#show crypto session
Crypto session current status
Interface: Virtual-Access1
Username: client1
Profile: Group-One-Profile
Group: Group-One
Assigned address: 10.1.1.101
Session status: UP-ACTIVE
Peer: 192.168.2.101 port 500
  IKEv1 SA: local 192.168.1.10/500 remote 192.168.2.101/500 Active
  IPSEC FLOW: permit ip 172.16.0.0/255.255.255.0 host 10.1.1.101
        Active SAs: 2, origin: crypto map
  IPSEC FLOW: permit ip 172.16.0.0/255.255.255.0 172.16.1.0/255.255.255.0
        Active SAs: 2, origin: crypto map
```

서버에 FlexVPN 컨피그레이션 추가

이 예에서는 FlexVPN 클라이언트와 서버 모두에서 RSA-SIG(즉, Certificate Authority)를 사용합니다. 이 섹션의 컨피그레이션에서는 서버가 이미 성공적으로 인증되고 CA 서버에 등록되었다고 가정합니다.

1단계 - IKEv2 스마트 기본 컨피그레이션을 확인합니다.

이제 IKEv2를 사용하면 15.2(1)T에 도입된 스마트 기본 기능을 활용할 수 있습니다. FlexVPN 컨피그레이션을 간소화하는 데 사용됩니다. 다음은 몇 가지 기본 컨피그레이션입니다.

기본 IKEv2 권한 부여 정책:

```
VPN-Server#show crypto ikev2 authorization policy default
 IKEv2 Authorization Policy : default
 route set interface
 route accept any tag : 1 distance : 1
```

기본 IKEv2 제안:

```
VPN-Server#show crypto ikev2 proposal default
 IKEv2 proposal: default
 Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
 Integrity : SHA512 SHA384 SHA256 SHA96 MD596
 PRF : SHA512 SHA384 SHA256 SHA1 MD5
```

```
 DH Group : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

기본 IKEv2 정책:

```
VPN-Server#show crypto ikev2 policy default
 IKEv2 policy : default
 Match fvrf : any
 Match address local : any
 Proposal : default
```

기본 IPsec 프로필:

```
VPN-Server#show crypto ipsec profile default
IPSEC profile default
 Security association lifetime: 4608000 kilobytes/3600 seconds
 Responder-Only (Y/N): N
 PFS (Y/N): N
 Transform sets={
 default: { esp-aes esp-sha-hmac } ,
 }
```

기본 IPsec 변형 집합:

```
VPN-Server#show crypto ipsec transform default
{ esp-aes esp-sha-hmac }
 will negotiate = { Transport, },
```

IKEv2 스마트 기본 기능에 대한 자세한 내용은 IKEv2 스마트 기본값(등록된 고객만 해당)을 참조하십시오.

2단계 - 기본 IKEv2 권한 부여 정책을 수정하고 FlexVPN 클라이언트에 대한 기본 IKEv2 프로필을 추가합니다.

여기에서 생성된 IKEv2 프로파일은 도메인 이름 cisco.com을 기반으로 하는 피어 ID에서 일치하며, 클라이언트에 대해 생성된 가상 액세스 인터페이스는 가상 템플릿 2에서 생성됩니다. 또한 권한 부여 정책은 피어 IP 주소를 할당하는 데 사용되는 IP 주소 풀과 IKEv2 컨피그레이션 모드를 통해 교환되는 경로를 정의합니다.

```
crypto ikev2 authorization policy default
 pool flexvpn-pool
 def-domain cisco.com
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn VPN-Server.cisco.com
 authentication remote pre-share
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
 virtual-template 2
```

3단계 - FlexVPN 클라이언트에 사용되는 가상 템플릿 인터페이스를 생성합니다.

```
interface Virtual-Template2 type tunnel
```

```
 ip unnumbered Ethernet1/0
 tunnel protection ipsec profile default
```

FlexVPN 클라이언트 컨피그레이션

```
crypto ikev2 authorization policy default
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Client2.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.10
 tunnel protection ipsec profile default
```

구성 완료

하이브리드 서버 구성 완료

```
hostname VPN-Server
!
!
aaa new-model
!
aaa authentication login client-xauth local
aaa authorization network default local
aaa authorization network ezvpn-author local
!
!
no ip domain lookup
ip domain name cisco.com
ip host ca-server 192.168.2.1
!
crypto pki trustpoint flex-trustpoint
 enrollment url http://ca-server:80
 serial-number
 ip-address none
 fingerprint 08CBB1E948A6D9571965B5EE58FBB726
 subject-name cn=vpn-server.cisco.com, OU=Flex, O=cisco
 revocation-check crl
 rsakeypair flex-key-pair 1024
!
!
crypto pki certificate chain flex-trustpoint
 certificate 07
 certificate ca 01
username client1 password 0 client1
```

```
username cisco password 0 cisco
!
crypto ikev2 authorization policy default
 pool flexvpn-pool
 def-domain cisco.com
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn VPN-Server.cisco.com
 authentication remote pre-share
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
 virtual-template 2
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp client configuration group Group-One
 key cisco123
 pool Group-One-Pool
 acl split-tunnel-acl
 save-password
crypto isakmp profile Group-One-Profile
 match identity group Group-One
 client authentication list client-xauth
 isakmp authorization list ezvpn-author
 client configuration address initiate
 client configuration address respond
 virtual-template 1
!
crypto ipsec transform-set aes-sha esp-aes esp-sha-hmac
!
crypto ipsec profile default
 set ikev2-profile default
!
crypto ipsec profile legacy-profile
 set transform-set aes-sha
!
crypto dynamic-map client-dynamic-map 1
 set transform-set aes-sha
 reverse-route
!
crypto map client-map 1 ipsec-isakmp dynamic client-dynamic-map
!
interface Ethernet0/0
 description WAN
 ip address 192.168.1.10 255.255.255.0
!
interface Ethernet1/0
 description LAN
 ip address 172.16.0.1 255.255.255.0
!
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet1/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile legacy-profile
!
```

```
interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet1/0
 tunnel protection ipsec profile default
!
ip local pool Group-One-Pool 10.1.1.100 10.1.1.200
ip local pool flexvpn-pool 10.1.1.201 10.1.1.250
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
ip access-list extended split-tunnel-acl
 remark EzVPN split tunnel ACL
 permit ip 172.16.0.0 0.0.0.255 any
!
access-list 1 permit 172.16.0.0 0.0.0.255
```

IKEv1 EzVPN 클라이언트 구성 완료

```
hostname Client1
!
crypto ipsec client ezvpn legacy-client
 connect manual
 group Group-One key cisco123
 mode network-extension
 peer 192.168.1.10
 username client1 password client1
 xauth userid mode local
!
interface Ethernet0/0
 description WAN
 ip address 192.168.2.101 255.255.255.0
 crypto ipsec client ezvpn legacy-client
!
interface Ethernet1/0
 description LAN
 ip address 172.16.1.1 255.255.255.0
 crypto ipsec client ezvpn legacy-client inside
!
ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

전체 IKEv2 FlexVPN 클라이언트 구성

```
hostname Client2
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization network default local
!
!
no ip domain lookup
ip domain name cisco.com
ip host ca-server 192.168.2.1
!
crypto pki trustpoint flex-trustpoint
 redundancy
 enrollment url http://ca-server:80
 serial-number
 ip-address none
```

```
 fingerprint 08CBB1E948A6D9571965B5EE58FBB726
 subject-name cn=Client2.cisco.com, OU=Flex, O=cisco
 revocation-check crl
 rsakeypair flex-key-pair 1024
!
!
crypto pki certificate chain flex-trustpoint
 certificate 06
 certificate ca 01
!
!
crypto ikev2 authorization policy default
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Client2.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.10
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 description WAN
 ip address 192.168.2.102 255.255.255.0
!
interface Ethernet1/0
 description LAN
 ip address 172.16.2.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.2.1
!
access-list 1 permit 172.16.2.0 0.0.0.255
```

구성 확인

다음은 라우터에서 EzVPN/FlexVPN 작업을 확인하는 데 사용되는 몇 가지 명령입니다.

```
show crypto session

show crypto session detail

show crypto isakmp sa

show crypto ikev2 sa

show crypto ipsec sa detail

show crypto ipsec client ez (for legacy clients)
```

```
show crypto socket

show crypto map
```

관련 정보

- 기술 지원 및 문서 – Cisco Systems