레거시 EzVPN에서 고급 EzVPN 컨피그레이션으로 마이그레이션 예

목차

소개

이 문서에서는 Spoke 1이 허브에 연결하기 위해 향상된 EzVPN을 사용하는 Easy VPN(EzVPN) 설정을 구성하는 방법과 Spoke 2는 기존 EzVPN을 사용하여 동일한 허브에 연결하는 방법에 대해 설명합니다.허브는 향상된 EzVPN에 대해 구성됩니다. 향상된 EzVPN과 레거시 EzVPN의 차이점은 이전 맵에서 동적 Virtual Tunnel Interface(dVTI)를 사용하고 후자의 암호화 맵을 사용하는 것입니다.Cisco dVTI는 Cisco EzVPN을 사용하는 고객이 서버 및 원격 구성 모두에 사용할 수 있는 방법입니다.터널은 각 EzVPN 연결에 대해 온디맨드 개별 가상 액세스 인터페이스를 제공합니다.가상 액세스 인터페이스의 컨피그레이션은 가상 템플릿 컨피그레이션에서 복제되며, 여기에는 IPsec 컨피그레이션 및 가상 템플릿 인터페이스(예: QoS, NetFlow 또는 ACL(Access Control List)에 구성된 모든 Cisco IOS® 소프트웨어 기능이 포함됩니다.

사용자는 IPsec dVTI 및 Cisco EzVPN을 사용하여 Cisco AVVID(Architecture for Voice, Video and Integrated Data)와 결합하여 IP 네트워크를 통해 통합된 음성, 비디오 및 데이터를 제공할 수 있는 원격 액세스 VPN에 매우 안전한 연결을 제공할 수 있습니다.

사전 요구 사항

요구 사항

EzVPN에 대한 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco IOS 버전 15.4(2)T를 기반으로 합니다.

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

dVTI 컨피그레이션이 포함된 Cisco EzVPN은 EzVPN Concentrator, 다른 사이트 간 피어 또는 인터넷과 같은 다른 대상에 트래픽을 선택적으로 전송할 수 있는 라우팅 가능한 인터페이스를 제공합니다.IPsec dVTI 컨피그레이션에는 물리적 인터페이스에 IPsec 세션을 정적 매핑하지 않아도 됩니다.이를 통해 여러 경로의 경우와 같이 모든 물리적 인터페이스에서 암호화된 트래픽을 유연하게 보내고 받을 수 있습니다.트래픽은 터널 인터페이스에서 또는 터널 인터페이스로 전달될 때 암호화됩니다.

트래픽은 IP 라우팅 테이블을 통해 터널 인터페이스로 또는 터널 인터페이스로 전달됩니다.경로는 IKE(Internet Key Exchange) 모드 컨피그레이션 중에 동적으로 학습되고 dVTI를 가리키는 라우팅 테이블에 삽입됩니다.동적 IP 라우팅을 사용하여 VPN을 통해 경로를 전파할 수 있습니다.IP 라우팅을 사용하여 트래픽을 암호화에 전달하면 네이티브 IPsec 컨피그레이션에서 암호화 맵으로 ACL을 사용하는 경우와 비교할 때 IPsec VPN 컨피그레이션이 간소화됩니다.

Cisco IOS Release 12.4(2)T 이전 릴리스에서는 터널 업/터널 다운 전환에서 모드 컨피그레이션 중

에 푸시된 특성을 구문 분석하고 적용해야 했습니다.이러한 특성으로 인해 인터페이스에서 컨피그레이션이 적용되었을 때 기존 컨피그레이션을 재정의해야 했습니다.dVTI 지원 기능을 사용하면 별도의 인터페이스에 터널업 컨피그레이션을 적용할 수 있으므로 터널업 시 별도의 기능을 더 쉽게 지원할 수 있습니다.터널로 들어가는 트래픽(암호화 전)에 적용되는 기능은 터널을 통과하지 않는 트래픽에 적용되는 기능(예: 스플릿 터널 트래픽 및 터널이 가동되지 않은 경우 디바이스를 떠나는 트래픽)과 분리할 수 있습니다.

EzVPN 협상이 성공하면 가상 액세스 인터페이스의 라인 프로토콜 상태가 up으로 변경됩니다.보안 연결이 만료되거나 삭제되어 EzVPN 터널이 다운되면 가상 액세스 인터페이스의 회선 프로토콜 상태가 다운으로 변경됩니다.

라우팅 테이블은 EzVPN 가상 인터페이스 컨피그레이션에서 트래픽 선택기 역할을 합니다. 즉, 경로가 암호화 맵의 액세스 목록을 대체합니다.가상 인터페이스 컨피그레이션에서 EzVPN 서버가 IPsec dVTI로 구성된 경우 EzVPN이 단일 IPsec 보안 연결을 협상합니다.이 단일 보안 연결은 구성된 EzVPN 모드에 관계없이 생성됩니다.

보안 연결이 설정되면 가상 액세스 인터페이스를 가리키는 경로가 기업 네트워크에 트래픽을 전달하도록 추가됩니다.또한 EzVPN은 IPsec 캡슐화된 패킷이 기업 네트워크로 라우팅되도록 VPN Concentrator에 경로를 추가합니다.가상 액세스 인터페이스를 가리키는 기본 경로는 분할되지 않은 모드의 경우 추가됩니다.EzVPN 서버가 스플릿 터널을 "푸시함"하면 스플릿 터널 서브넷이 가상 액세스를 가리키는 경로가 추가되는 대상이 됩니다.어느 경우든 피어(VPN 집선 장치)가 직접 연결되지 않은 경우 EzVPN은 피어에 경로를 추가합니다.

> **참고:**Cisco EzVPN Client 소프트웨어를 실행하는 대부분의 라우터에는 기본 경로가 구성되어 있습니다.EzVPN은 메트릭 값이 1인 기본 경로를 추가하므로 구성된 기본 경로의 메트릭 값이 1보다 커야 합니다. 이 경로는 가상 액세스 인터페이스를 가리키므로 Concentrator가 스플릿 터널 특성을 "push"하지 않을 때 모든 트래픽이 기업 네트워크로 전송되도록 합니다.

QoS를 사용하여 네트워크 전반의 다양한 애플리케이션의 성능을 개선할 수 있습니다.이 컨피그레이션에서는 사이트 간에 전송해야 하는 총 트래픽 양을 제한하기 위해 두 사이트 간에 트래픽 셰이핑이 사용됩니다.또한 QoS 구성은 음성, 비디오 또는 데이터 애플리케이션을 지원하기 위해 Cisco IOS Software에 제공되는 모든 QoS 기능 조합을 지원할 수 있습니다.

> **참고:**이 가이드의 QoS 컨피그레이션은 데모용입니다.VTI 확장성 결과는 IPsec을 통한 P2P(Point-to-Point) GRE(Generic Routing Encapsulation)와 비슷할 것으로 예상됩니다.확장 및 성능 고려 사항은 Cisco 담당자에게 문의하십시오.자세한 내용은 IP 보안으로 가상 터널 인터페이스 구성을 참조하십시오.

혜택

- **관리 간소화**
  고객은 Cisco IOS 가상 템플릿을 사용하여 온디맨드 방식으로 IPsec용 새로운 가상 액세스 인터페이스를 복제할 수 있습니다. 이를 통해 VPN 컨피그레이션의 복잡성을 간소화하고 비용을 절감할 수 있습니다.또한 기존 관리 애플리케이션은 모니터링 목적으로 여러 사이트의 개별 인터페이스를 모니터링할 수 있습니다.
- **라우팅 가능한 인터페이스 제공**
  Cisco IPsec VTI는 모든 유형의 IP 라우팅 프로토콜을 지원할 수 있습니다.고객은 이러한 기능을 사용하여 지사와 같은 대규모 사무실 환경을 연결할 수 있습니다.
- **확장 개선**

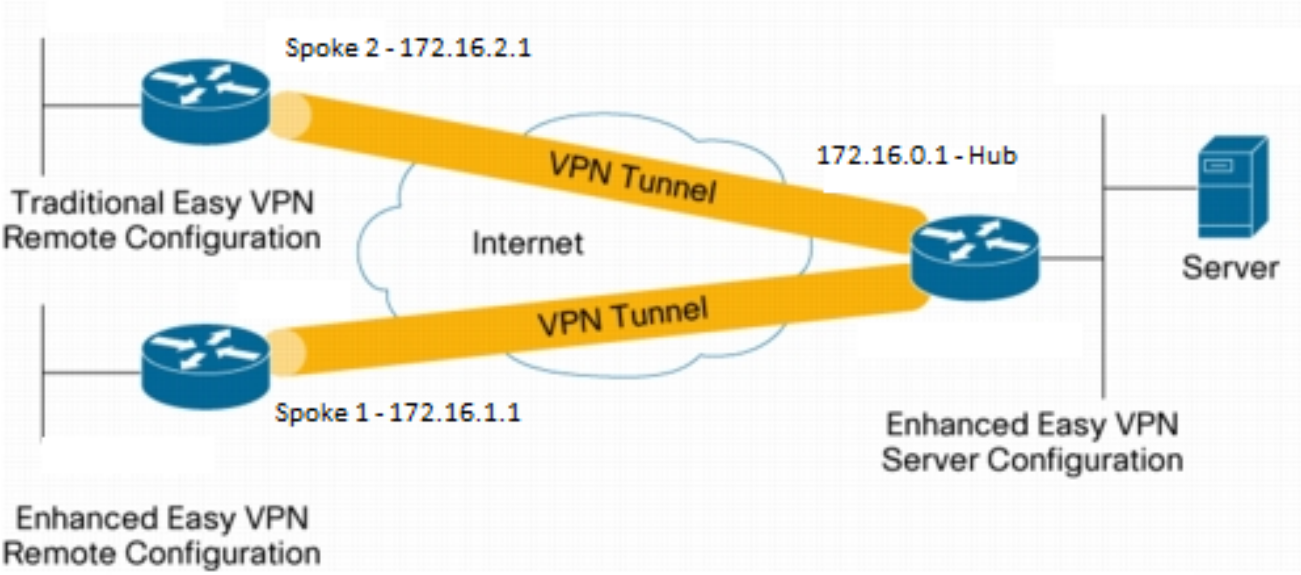
IPsec VTI는 사이트당 단일 보안 연결을 사용하므로 여러 유형의 트래픽을 처리하므로 확장성이 향상됩니다.

- **기능 정의 유연성 제공**
  IPsec VTI는 자체 인터페이스 내의 캡슐화입니다.이는 IPsec VTI에서 일반 텍스트 트래픽에 대한 기능을 유연하게 정의하고 물리적 인터페이스에서 암호화된 트래픽에 대한 기능을 정의합니다.

구성

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

네트워크 다이어그램



구성 요약

허브 구성

```
hostname Hub
!
no aaa new-model
!
no ip domain lookup
!
username test-user privilege 15 password 0 cisco123
!
```

```
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp client configuration group En-Ezvpn
 key test-En-Ezvpn
crypto isakmp profile En-EzVpn-Isakmp-Profile
  match identity group En-Ezvpn
  isakmp authorization list default
  client configuration address respond
  virtual-template 1
!
!
crypto ipsec transform-set VPN-TS esp-aes esp-sha-hmac
 mode tunnel
!
crypto ipsec profile En-EzVpn-Ipsec-Profile
 set transform-set VPN-TS
 set isakmp-profile En-EzVpn-Isakmp-Profile
!
!
interface Loopback0
 description Router-ID
 ip address 10.0.0.1 255.255.255.255
!
interface Loopback1
 description inside-network
 ip address 192.168.0.1 255.255.255.255
!
interface Ethernet0/0
 description WAN-Link
 ip address 172.16.0.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile En-EzVpn-Ipsec-Profile
!
router eigrp 1
 network 10.0.0.1 0.0.0.0
 network 192.168.0.1 0.0.0.0
 network 192.168.1.1 0.0.0.0
!
ip route 0.0.0.0 0.0.0.0 172.16.0.100
!
end
```

스포크 1(Enhanced EzVPN) 컨피그레이션

```
hostname Spoke1
!
no aaa new-model
!
interface Loopback0
 description Router-ID
 ip address 10.0.1.1 255.255.255.255
 crypto ipsec client ezvpn En-EzVpn inside
```

```
!
interface Loopback1
 description Inside-network
 ip address 192.168.1.1 255.255.255.255
!
interface Ethernet0/0
 description WAN-Link
 ip address 172.16.1.1 255.255.255.0
 crypto ipsec client ezvpn En-EzVpn
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel mode ipsec ipv4
!
router eigrp 1
 network 10.0.1.1 0.0.0.0
 network 192.168.1.1 0.0.0.0
!
ip route 0.0.0.0 0.0.0.0 172.16.1.100
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto ipsec client ezvpn En-EzVpn
 connect auto
 group En-Ezvpn key test-En-Ezvpn
 mode network-extension
 peer 172.16.0.1
 virtual-interface 1
!
end
```

주의:클라이언트 구성을 입력하기 전에 가상 템플릿을 정의해야 합니다.동일한 수의 기존 가상 템플릿이 없으면 라우터는 **virtual-interface 1** 명령을 수락하지 않습니다.

스포크 2(레거시 EzVPN) 컨피그레이션

```
hostname Spoke2
!
no aaa new-model
!
no ip domain lookup
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto ipsec client ezvpn Leg-Ezvpn
 connect auto
 group En-Ezvpn key test-En-Ezvpn
 mode network-extension
 peer 172.16.0.1
 xauth userid mode interactive
!
```

```
!
interface Loopback0
 ip address 10.0.2.1 255.255.255.255
 crypto ipsec client ezvpn Leg-Ezvpn inside
!
interface Loopback1
 ip address 192.168.2.1 255.255.255.255
!
interface Ethernet0/0
 ip address 172.16.2.1 255.255.255.0
 crypto ipsec client ezvpn Leg-Ezvpn
!
ip route 0.0.0.0 0.0.0.0 172.16.2.100
!
end
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

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

Hub to Spoke 1 터널

1단계

```
Hub#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF  Status Encr Hash   Auth DH Lifetime Cap.

1006  172.16.0.1      172.16.2.1             ACTIVE aes  sha    psk  2  23:54:53 C
      Engine-id:Conn-id =  SW:6

1005  172.16.0.1      172.16.1.1             ACTIVE aes  sha    psk  2  23:02:14 C
      Engine-id:Conn-id =  SW:5

IPv6 Crypto ISAKMP SA
```

2단계

이 프록시는 Virtual Access 1을 종료하는 모든 트래픽이 암호화되어 172.16.1.1으로 전송됨을 의미합니다.

```
Hub#show crypto ipsec sa peer 172.16.1.1 detail

interface: Virtual-Access1
```

```
   Crypto map tag: Virtual-Access1-head-0, local addr 172.16.0.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 172.16.1.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 776, #pkts encrypt: 776, #pkts digest: 776
   #pkts decaps: 771, #pkts decrypt: 771, #pkts verify: 771
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
   #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
   #pkts invalid prot (recv) 0, #pkts verify failed: 0
   #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
   #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
   ##pkts replay failed (rcv): 0
   #pkts tagged (send): 0, #pkts untagged (rcv): 0
   #pkts not tagged (send): 0, #pkts not untagged (rcv): 0
   #pkts internal err (send): 0, #pkts internal err (recv) 0

    local crypto endpt.: 172.16.0.1, remote crypto endpt.: 172.16.1.1
    plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
    current outbound spi: 0x9159A91E(2438572318)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0xB82853D4(3089650644)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 13, flow_id: SW:13, sibling_flags 80000040, crypto map:
Virtual-Access1-head-0
       sa timing: remaining key lifetime (k/sec): (4342983/3529)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x9159A91E(2438572318)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 14, flow_id: SW:14, sibling_flags 80000040, crypto map:
Virtual-Access1-head-0
       sa timing: remaining key lifetime (k/sec): (4342983/3529)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
```

EIGRP

```
Hub#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
```

```
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                  (sec)         (ms)       Cnt Num
0   172.16.1.1              Vi1                      13 00:59:28   31  1398  0  3
```

참고: Spoke 2는 라우팅 가능한 인터페이스 없이 EIGRP(Enhanced Interior Gateway Routing Protocol) 피어를 구성할 수 없으므로 항목을 형성하지 않습니다.이는 스포크에서 dVTI를 사용할 때의 장점 중 하나입니다.

스포크 1

1단계

```
Spoke1#show cry is sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF  Status Encr Hash   Auth DH Lifetime Cap.

1005  172.16.1.1      172.16.0.1             ACTIVE aes  sha    psk  2  22:57:07 C
      Engine-id:Conn-id =  SW:5

IPv6 Crypto ISAKMP SA
```

2단계

```
Spoke1#show crypto ipsec sa detail

interface: Virtual-Access1
   Crypto map tag: Virtual-Access1-head-0, local addr 172.16.1.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 172.16.0.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 821, #pkts encrypt: 821, #pkts digest: 821
   #pkts decaps: 826, #pkts decrypt: 826, #pkts verify: 826
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
   #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
   #pkts invalid prot (recv) 0, #pkts verify failed: 0
   #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
   #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
   ##pkts replay failed (rcv): 0
   #pkts tagged (send): 0, #pkts untagged (rcv): 0
   #pkts not tagged (send): 0, #pkts not untagged (rcv): 0
   #pkts internal err (send): 0, #pkts internal err (recv) 0

    local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.0.1
```

```
    plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
    current outbound spi: 0xB82853D4(3089650644)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0x9159A91E(2438572318)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 11, flow_id: SW:11, sibling_flags 80004040, crypto map:
Virtual-Access1-head-0
       sa timing: remaining key lifetime (k/sec): (4354968/3290)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0xB82853D4(3089650644)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 12, flow_id: SW:12, sibling_flags 80004040, crypto map:
Virtual-Access1-head-0
       sa timing: remaining key lifetime (k/sec): (4354968/3290)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
```

EZVPN

```
Spoke1#show crypto ipsec client ezvpn
Easy VPN Remote Phase: 8

Tunnel name : En-EzVpn
Inside interface list: Loopback0
Outside interface: Virtual-Access1 (bound to Ethernet0/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Save Password: Disallowed
Current EzVPN Peer: 172.16.0.1
```

라우팅 - EIGRP

Spoke 2에서 프록시는 가상 액세스 인터페이스를 종료하는 모든 트래픽이 암호화되는 것입니다.네트워크에 대한 인터페이스를 가리키는 경로가 있는 한 트래픽은 암호화됩니다.

```
Spoke1#ping 192.168.0.1 source loopback 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/6 ms
```

```
Spoke1#ping 192.168.0.1 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
Packet sent with a source address of 10.0.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms

Spoke1# sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.1.100 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.1.100
                [1/0] via 0.0.0.0, Virtual-Access1
      10.0.0.0/32 is subnetted, 2 subnets
D        10.0.0.1 [90/27008000] via 10.0.0.1, 01:16:15, Virtual-Access1
C        10.0.1.1 is directly connected, Loopback0
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
S        172.16.0.1/32 [1/0] via 172.16.1.100
C        172.16.1.0/24 is directly connected, Ethernet0/0
L        172.16.1.1/32 is directly connected, Ethernet0/0
      192.168.0.0/32 is subnetted, 1 subnets
D        192.168.0.1 [90/27008000] via 10.0.0.1, 01:16:15, Virtual-Access1
       192.168.1.0/32 is subnetted, 1 subnets
C        192.168.1.1 is directly connected, Loopback1
Spoke1#
```

Hub to Spoke 2 터널

1단계

```
Hub#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF  Status Encr Hash   Auth DH Lifetime Cap.

1006  172.16.0.1      172.16.2.1             ACTIVE aes  sha    psk  2  23:54:53 C
      Engine-id:Conn-id =  SW:6

1005  172.16.0.1      172.16.1.1             ACTIVE aes  sha    psk  2  23:02:14 C
      Engine-id:Conn-id =  SW:5

IPv6 Crypto ISAKMP SA
```

2단계

이 예에서는 허브의 클라이언트 컨피그레이션 아래에 있는 스플릿 터널 ACL이 사용되지 않습니다 .따라서 스포크에 형성되는 프록시는 모든 네트워크에 대한 스포크의 모든 EzVPN "내부" 네트워크에 사용됩니다.기본적으로 허브에서 스포크의 "내부" 네트워크 중 하나로 향하는 모든 트래픽은 암호화되어 172.16.2.1으로 전송됩니다.

```
Hub#show crypto ipsec sa  peer 172.16.2.1 detail

interface: Virtual-Access2
   Crypto map tag: Virtual-Access2-head-0, local addr 172.16.0.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (10.0.2.1/255.255.255.255/0/0)
   current_peer 172.16.2.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 15, #pkts encrypt: 15, #pkts digest: 15
   #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
   #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
   #pkts invalid prot (recv) 0, #pkts verify failed: 0
   #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
   #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
   ##pkts replay failed (rcv): 0
   #pkts tagged (send): 0, #pkts untagged (rcv): 0
   #pkts not tagged (send): 0, #pkts not untagged (rcv): 0
   #pkts internal err (send): 0, #pkts internal err (recv) 0

    local crypto endpt.: 172.16.0.1, remote crypto endpt.: 172.16.2.1
    plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
    current outbound spi: 0x166CAC10(376220688)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0x8525868A(2233829002)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 11, flow_id: SW:11, sibling_flags 80000040, crypto map:
Virtual-Access2-head-0
       sa timing: remaining key lifetime (k/sec): (4217845/1850)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x166CAC10(376220688)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 12, flow_id: SW:12, sibling_flags 80000040, crypto map:
Virtual-Access2-head-0
       sa timing: remaining key lifetime (k/sec): (4217845/1850)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)
```

```
    outbound ah sas:

    outbound pcp sas:
```

스포크 2

1단계

```
Spoke2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.16.0.1      172.16.2.1      QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

2단계

```
Spoke2#show crypto ipsec sa detail

interface: Ethernet0/0
   Crypto map tag: Ethernet0/0-head-0, local addr 172.16.2.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (10.0.2.1/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 172.16.0.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
   #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
   #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
   #pkts invalid prot (recv) 0, #pkts verify failed: 0
   #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
   #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
   ##pkts replay failed (rcv): 0
   #pkts tagged (send): 0, #pkts untagged (rcv): 0
   #pkts not tagged (send): 0, #pkts not untagged (rcv): 0
   #pkts internal err (send): 0, #pkts internal err (recv) 0

    local crypto endpt.: 172.16.2.1, remote crypto endpt.: 172.16.0.1
    plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
    current outbound spi: 0x8525868A(2233829002)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0x166CAC10(376220688)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 1, flow_id: SW:1, sibling_flags 80004040, crypto map:
Ethernet0/0-head-0
       sa timing: remaining key lifetime (k/sec): (4336232/2830)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)
```

```
    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x8525868A(2233829002)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2, flow_id: SW:2, sibling_flags 80004040, crypto map:
Ethernet0/0-head-0
       sa timing: remaining key lifetime (k/sec): (4336232/2830)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
```

EZVPN

```
Spoke2#show crypto ipsec client ezvpn
Easy VPN Remote Phase: 8

Tunnel name : Leg-Ezvpn
Inside interface list: Loopback0
Outside interface: Ethernet0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Save Password: Disallowed
Current EzVPN Peer: 172.16.0.1
```

라우팅 - 정적

스포크 1과 달리 스포크 2는 고정 경로를 가지거나 RRI(Reverse Route Injection)를 사용하여 어떤 트래픽이 암호화되어야 하는지, 어떤 트래픽이 암호화되지 않아야 하는지를 알려주는 경로를 삽입해야 합니다.이 예에서는 루프백 0에서 제공된 트래픽만 프록시 및 라우팅에 따라 암호화됩니다.

```
Spoke2#ping 192.168.0.1 source loopback 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
.....
Success rate is 0 percent (0/5)

Spoke2#ping 192.168.0.1 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
Packet sent with a source address of 10.0.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/7 ms

Spoke2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.2.100 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.2.100
      10.0.0.0/32 is subnetted, 1 subnets
C        10.0.2.1 is directly connected, Loopback0
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.2.0/24 is directly connected, Ethernet0/0
L        172.16.2.1/32 is directly connected, Ethernet0/0
      192.168.2.0/32 is subnetted, 1 subnets
C        192.168.2.1 is directly connected, Loopback1
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

> **팁:**EzVPN에서는 컨피그레이션 변경 후 터널이 나타나지 않는 경우가 많습니다.1단계와 2단계를 지우면 이 경우에는 터널이 가동되지 않습니다.대부분의 경우 터널을 **표시하려면 스포크에 clear crypto ipsec client ezvpn <group-name>** 명령을 입력합니다.

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

허브 명령

- **debug crypto ipsec** - 2단계의 IPsec 협상을 표시합니다.
- **debug crypto isakmp** - 1단계의 ISAKMP 협상을 표시합니다.

스포크 명령

- **debug crypto ipsec** - 2단계의 IPsec 협상을 표시합니다.
- **debug crypto isakmp** - 1단계의 ISAKMP 협상을 표시합니다.
- **debug crypto ipsec client ezvpn** - EzVPN 디버그를 표시합니다.

관련 정보

- IPsec 지원 페이지
- Cisco Easy VPN Remote
- Easy VPN 서버
- IPsec 가상 터널 인터페이스
- IPsec 네트워크 보안 구성
- 인터넷 키 교환 보안 프로토콜 구성
- 기술 지원 및 문서 – Cisco Systems