Migratie van verouderde EZVPN naar uitgebreid EzVPN-configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u een Easy VPN (EzVPN)-instelling kunt configureren waarbij Spoke 1 gebruik maakt van uitgebreide EzVPN om verbinding te maken met het hub, terwijl Spoke 2 gebruik maakt van bestaande EzVPN om verbinding te maken met hetzelfde hub. De hub is ingesteld voor EzVPN. Het verschil tussen uitgebreide EzVPN en bestaande EzVPN is het gebruik van dynamische Virtual Tunnel Interfaces (dVTI's) in de eerstgenoemde en crypto kaarten in de laatstgenoemde. Cisco dVTI is een methode die door klanten met Cisco EzVPN voor zowel de server als de afstandsconfiguratie kan worden gebruikt. De tunnels bieden een on-demand afzonderlijke virtuele access interface voor elke EzVPN-verbinding. De configuratie van de virtuele toegangsinterfaces is gebaseerd op een virtuele sjabloonconfiguratie, die de IPsec-configuratie en elke Cisco IOS®-softwarefunctie omvat die is ingesteld op de virtuele sjablooninterface, zoals QoS, NetFlow of toegangscontrolelijsten (ACL's).

Dankzij IPsec-dVTI's en Cisco EzVPN kunnen gebruikers zeer beveiligde connectiviteit bieden voor VPN's met toegang op afstand die kunnen worden gecombineerd met Cisco AVVID (Architecture for Voice, Video en Integrated Data) om geconvergeerde spraak, video en gegevens via IP-netwerken te leveren.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van EzVPN.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco IOS versie 15.4(2)T.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

De configuratie van Cisco EzVPN met dVTI biedt een routekaarten om selectief verkeer naar verschillende bestemmingen, zoals een EzVPN-concentrator, een ander site-to-site peer of het internet, te verzenden. De configuratie van IPsec dVTI vereist geen statische mapping van IPsec-sessies naar een fysieke interface. Dit staat voor de flexibiliteit toe om gecodeerd verkeer op om het even welke fysieke interface te verzenden en te ontvangen, zoals in het geval van meervoudige paden. Het verkeer wordt versleuteld wanneer het van of naar de tunnelinterface wordt doorgestuurd.

Het verkeer wordt naar of van de tunnelinterface verstuurd uit hoofde van de IP-routingtabel. Routes worden dynamisch geleerd tijdens de Configuratie van de Modus van Internet Key

Exchange (IKE) en in de routingtabel ingevoegd die naar het dVTI wijst. De dynamische IP routing kan worden gebruikt om routes door VPN te propageren. Gebruik van IP-routing om het verkeer naar encryptie te doorsturen maakt de IPsec VPN-configuratie eenvoudiger in vergelijking met het gebruik van ACL's met de crypto-kaart in de native IPsec-configuratie.

In releases eerder dan Cisco IOS release 12.4(2)T, bij de tunnelup/tunnelomlaag-overgang, moesten eigenschappen die tijdens de modemconfiguratie werden geduwd, worden geparseerd en toegepast. Wanneer dergelijke eigenschappen resulteerden in de toepassing van configuraties op de interface, moest de bestaande configuratie worden gecorrigeerd. Dankzij de dVTI Support optie kan de tunnelconfiguratie worden toegepast op afzonderlijke interfaces, waardoor het gemakkelijker wordt om afzonderlijke functies te ondersteunen tijdens de tunneluptijd. Kenmerken die van toepassing zijn op het verkeer (vóór encryptie) dat in de tunnel gaat, kunnen los worden gezien van de functies die van toepassing zijn op verkeer dat niet door de tunnel gaat (bijvoorbeeld het gesplitste tunnelverkeer en verkeer dat het apparaat verlaat wanneer de tunnel niet omhoog is).

Wanneer de onderhandeling van EzVPN succesvol is, wordt de status van het lijnprotocol van de virtuele toegangsinterface veranderd in omhoog. Wanneer de EzVPN-tunnel omlaag gaat omdat de beveiligingsassociatie verlopen of wordt verwijderd, verandert de status van de virtuele access interface in het lijnprotocol.

De routingtabellen fungeren als verkeerselectie in een EzVPN virtuele interfaceconconfiguratie-dat wil zeggen, de routes vervangen de toegangslijst op de crypto-kaart. In een virtuele interfaceconfiguratie onderhandelt EzVPN over één IPsec-beveiligingsassociatie als de EzVPN-server is geconfigureerd met een IPsec dVTI. Deze enige veiligheidsassociatie wordt gecreëerd ongeacht de EzVPN-modus die is ingesteld.

Nadat de veiligheidsvereniging wordt opgericht, worden de routes die op de virtuele toegangsinterface wijzen toegevoegd aan direct verkeer aan het bedrijfsnetwerk. EzVPN voegt ook een route aan de VPN-concentrator toe zodat de in IPsec ingekapselde pakketten naar het bedrijfsnetwerk worden verzonden. Een standaardroute die naar de virtuele access interface wijst wordt bij een niet-gesplitste modus toegevoegd. Wanneer de EzVPN server "de gesplitste tunnel"duwt, wordt gesplitste tunnelnet de bestemming waaraan de routes die naar de virtuele toegang wijzen worden toegevoegd. In beide gevallen, als de peer (VPN concentrator) niet direct verbonden is, voegt EzVPN een route aan de peer toe.

> **Opmerking:** De meeste routers die de clientsoftware van Cisco EzVPN uitvoeren, hebben een standaardroute ingesteld. De standaardroute die wordt geconfigureerd moet een metrische waarde van meer dan 1 hebben sinds EzVPN een standaardroute met een metrische waarde van 1 toevoegt. De route wijst naar de virtuele toegangsinterface zodat al het verkeer naar het bedrijfsnetwerk wordt gericht wanneer de concentrator de gesplitste tunneleigenschap niet "indrukt".

QoS kan worden gebruikt om de prestaties van verschillende toepassingen in het netwerk te verbeteren. In deze configuratie wordt traffic shaping tussen de twee locaties gebruikt om de totale hoeveelheid verkeer te beperken die tussen de locaties moet worden doorgegeven. Daarnaast kan de QoS-configuratie elke combinatie van QoS-functies ondersteunen die in Cisco IOS-software wordt aangeboden, om een of meer spraak-, video- of gegevenstoepassingen te ondersteunen.

> **Opmerking:** De QoS-configuratie in deze handleiding is alleen bedoeld voor demonstratie.

Verwacht wordt dat de resultaten van de schaalbaarheid van VTI vergelijkbaar zullen zijn met de Point-to-Point (P2P) Generic Routing Encapsulation (GRE) via IPsec. Voor schaalings- en prestatieoverwegingen kunt u contact opnemen met uw Cisco-vertegenwoordiger. Zie Een virtuele tunnelinterface met IP-beveiliging configureren voor meer informatie.

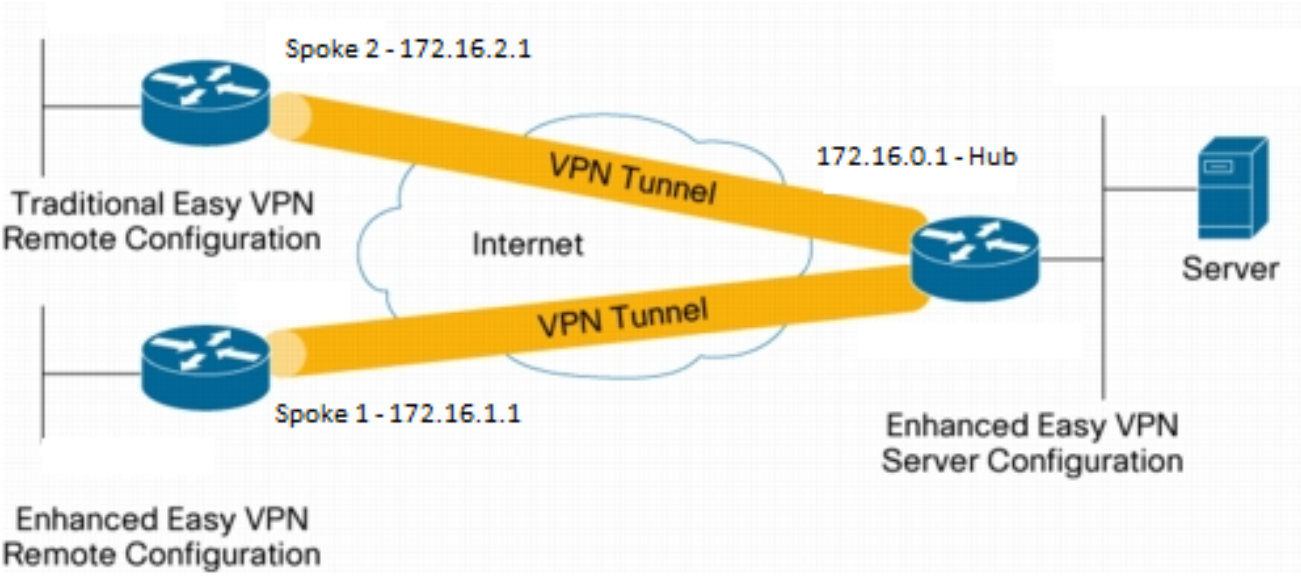
Voordelen

- **Vereenvoudig beheer**
  Klanten kunnen de virtuele sjabloon van Cisco IOS gebruiken om, op verzoek, nieuwe virtuele toegangsinterfaces voor IPsec te klonen die de configuratiecomplexiteit van VPN vereenvoudigt en in lagere kosten vertaalt. Daarnaast kunnen bestaande beheertoepassingen nu afzonderlijke interfaces voor verschillende locaties bewaken voor monitoringdoeleinden.
- **Biedt een routebare interface**
  Cisco IPsec VTI's kunnen alle typen IP-routingprotocollen ondersteunen. Klanten kunnen deze mogelijkheden gebruiken om grotere kantooromgevingen, zoals bijkantoren, aan te sluiten.
- **Verbetert het schalen**
  IPsec VTIs gebruiken één veiligheidsverenigingen per plaats, die verschillende types van verkeer bestrijken, wat verbetert de schaal toelaat.
- **Biedt flexibiliteit in het definiëren van functies**
  Een IPsec VTI is een insluiting binnen zijn eigen interface. Dit biedt flexibiliteit van het definiëren van functies voor duidelijk-tekstverkeer op IPsec VTIs en definieert functies voor versleuteld verkeer op fysieke interfaces.

Configureren

Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram



Configuratieoverzicht

Hub-configuratie

```
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
```

Configuratie van Spoel 1 (uitgebreide EzVPN)

```
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
```

> **Voorzichtig:** De virtuele sjabloon moet worden gedefinieerd voordat de clientconfiguratie is ingevoerd. Zonder een bestaand virtueel sjabloon van hetzelfde nummer accepteert de router de opdracht **virtuele interface 1** niet.

Configuratie van Spoke 2 (Verouderde EzVPN)

```
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
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met **show.** Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

hub om 1 te spuiten

Fase 1

```
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
```

Fase 2

Deze proxy's zijn voor any/any die impliceert dat elk verkeer dat Virtual Access 1 verlaat, versleuteld wordt en naar 172.16.1.1 wordt verzonden.

```
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:
```

EINDTIJD

```
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
```

Opmerking: Spoke 2 vormt geen ingang aangezien het niet mogelijk is om een Enhanced Interior Gateway Protocol (DHCP) te vormen zonder een routeerbare interface. Dit is een van de voordelen van het gebruik van dVTI's op het woord.

Gesproken 1

Fase 1

```
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
```

Fase 2

```
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
```

Routing - EHMINIER

In Spoke 2 zijn de proxy's zo dat elk verkeer dat de virtuele toegangsinterface verlaat, versleuteld wordt. Zolang er een route is die wijst op die interface voor een netwerk, wordt het verkeer versleuteld:

```
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 Tunnel

Fase 1

```
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
```

Fase 2

Een split-tunnel ACL onder de clientconfiguratie op de hub wordt in dit voorbeeld niet gebruikt. Daarom zijn de proxy's die op het platform worden gevormd voor elk EzVPN "binnennetwerk" op het aangesloten netwerk op elk netwerk. In de hub zal elk verkeer dat bestemd is voor een van de "binnennetwerken" op de spits versleuteld worden en naar 172.16.2.1 worden verzonden.

```
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:
```

Gesproken 2

Fase 1

```
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
```

Fase 2

```
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
```

Routing - statisch

Anders dan Spoke 1 moet Spoke 2 statische routes hebben of RRI (Reverse Route Injection) gebruiken om routes te injecteren om hem te vertellen welk verkeer versleuteld moet worden en wat niet. In dit voorbeeld wordt alleen verkeer dat afkomstig is van Loopback 0 versleuteld volgens de proxy's en de routing.

```
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
```

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

> **Tip**: Zeer vaak komen in EzVPN de tunnels niet in nadat de configuratie is veranderd. De tunnels zullen in dit geval niet worden opgeruimd door fase 1 en fase 2. Voer in de meeste gevallen de **heldere crypto ipsec client ezvpn <group-name>** opdracht in om de tunnel op te halen.

> **Opmerking:** Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**

Hub-opdrachten

- **debug crypto ipsec** - displays de IPsec-onderhandelingen van fase 2.
- **debug crypto isakmp -** Hiermee geeft u de ISAKMP-onderhandelingen van fase 1 weer.

Spoekopdrachten

- **debug crypto ipsec -** Hiermee geeft u de IPsec-onderhandelingen van fase 2 weer.
- **debug crypto isakmp -** Hiermee geeft u de ISAKMP-onderhandelingen van fase 1 weer.
- **debug van crypto ipsec client ezvpn -** Hiermee geeft u de EzVPN-apparaten weer.

Gerelateerde informatie

- Ondersteuning van IPsec
- Cisco Easy VPN-afstandsbediening
- Makkelijke VPN-server
- IPsec virtuele tunnelinterface
- IPsec-netwerkbeveiliging configureren
- Het configureren van Internet Key Exchange-beveiligingsprotocol
- Technische ondersteuning en documentatie – Cisco Systems