Migración del EzVPN de la herencia al ejemplo de configuración aumentado del EzVPN

Contenido

Introducción

Este documento describe cómo configurar un VPN fácil (EzVPN) puesto donde el Spoke1 utiliza el EzVPN aumentado para conectar con el concentrador, mientras que el Spoke2 utiliza el EzVPN de la herencia para conectar con el mismo concentrador. El concentrador se configura para el EzVPN aumentado. La diferencia entre el EzVPN aumentado y el EzVPN de la herencia es el uso de las interfaces del túnel virtuales dinámicas (dVTIs) en el anterior y de las correspondencias de criptografía en estos últimos. El dVTI de Cisco es un método que se puede utilizar por los clientes con el EzVPN de Cisco para el servidor y la configuración remota. Los túneles proporcionan una interfaz de acceso virtual separada a pedido para cada conexión del EzVPN. La configuración de las interfaces de acceso virtual se reproduce de una configuración de plantilla virtual, que incluye la configuración IPSec y cualquier característica del Cisco IOS ® Software configuradas en la interfaz de plantilla virtual, tal como QoS, Netflow, o Listas de control de acceso (ACL).

Con los dVTIs del IPSec y el EzVPN de Cisco, los usuarios pueden proporcionar altamente la conectividad segura para los VPN de accesos remotos que se pueden combinar con el Cisco AVVID (Architecture for Voice, Video and integrated Data) para entregar la voz con convergencia, el vídeo, y los datos sobre las redes del IP.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento del EzVPN.

Componentes Utilizados

La información en este documento se basa en la versión deL Cisco IOS 15.4(2)T.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

El EzVPN de Cisco con la configuración del dVTI proporciona una interfaz enrutable para enviar selectivamente el tráfico a diversos destinos, tales como un concentrador del EzVPN, un diverso par del sitio a localizar, o Internet. La configuración del dVTI del IPSec no requiere una correlación estática de las sesiones del IPSec a una interfaz física. Esto permite para que la flexibilidad envíe y reciba el tráfico encriptado en cualquier interfaz física, por ejemplo en el caso de los trayectos múltiples. Se cifra el tráfico cuando se remite o a la interfaz del túnel.

El tráfico se remite a o desde la interfaz del túnel en virtud de la tabla de IP Routing. Las rutas son dinámicamente doctas durante la configuración de modo del Internet Key Exchange (IKE) y se

insertan en la tabla de ruteo esas puntas al dVTI. El Dynamic IP Routing se puede utilizar para propagar las rutas a través del VPN. Usando el Routing IP remitir el tráfico al cifrado simplifica la configuración del IPSec VPN en comparación con el uso de los ACL con la correspondencia de criptografía en la configuración IPSec nativa.

En las versiones anterior que el Cisco IOS Release 12.4(2)T, en el túnel-para arriba/la transición del túnel-abajo, los atributos que fueron avanzados durante la configuración de modo tuvieron que ser analizados y ser aplicados. Cuando tales atributos dieron lugar a la aplicación de las configuraciones en la interfaz, la configuración existente tuvo que ser reemplazada. Con la característica del soporte del dVTI, la configuración del túnel-para arriba se puede aplicar a las interfaces diferentes, que hace más fácil soportar las características diferentes en el tiempo del túnel-para arriba. Las características que se aplican al tráfico (antes de que cifrado) que entra el túnel pueden estar a parte de las características que se aplican para traficar eso no pasan a través del túnel (por ejemplo, tráfico del túnel dividido y el tráfico que sale del dispositivo cuando el túnel no está para arriba).

Cuando la negociación del EzVPN es acertada, el estado del Line Protocol de la interfaz de acceso virtual consigue cambiado a para arriba. Cuando va el túnel del EzVPN abajo porque la asociación de seguridad expira o se borra, el estado del Line Protocol de la interfaz de acceso virtual cambia a abajo.

Las tablas de ruteo actúan como selectores del tráfico en una interfaz virtual del EzVPN configuración-que es, las rutas substituyen la lista de acceso en la correspondencia de criptografía. En una configuración de la interfaz virtual, el EzVPN negocia una sola asociación de seguridad IPSec si han configurado al servidor EzVPN con un dVTI del IPSec. Crean a esta sola asociación de seguridad sin importar el modo del EzVPN se configura que.

Después de que establezcan a la asociación de seguridad, las rutas que la punta a la interfaz de acceso virtual está agregada al tráfico directo a la red corporativa. El EzVPN también agrega una ruta al concentrador VPN de modo que los paquetes encapsulados por IPsec consigan ruteados a la red corporativa. Una ruta predeterminado que señala a la interfaz de acceso virtual se agrega en el caso de un modo del nonsplit. Cuando el servidor EzVPN “avanza” el túnel dividido, la subred del túnel dividido se convierte en el destino al cual se agregan las rutas que señalan al acceso virtual. En ambos casos, si el par (concentrador VPN) no está conectado directamente, el EzVPN agrega una ruta al par.

> Nota: La mayoría del Routers que funciona con el software del cliente EzVPN de Cisco hace una ruta predeterminado configurar. La ruta predeterminado se configura que debe tener un valor métrico mayor de 1 puesto que el EzVPN agrega una ruta predeterminado que tenga un valor métrico de 1. Los puntos de ruta a la interfaz de acceso virtual para dirigir todo el tráfico a la red corporativa cuando el concentrador “no avanza” el atributo del túnel dividido.

QoS se puede utilizar para mejorar el funcionamiento de diversas aplicaciones a través de la red. En esta configuración, el modelado de tráfico se utiliza entre los dos sitios para limitar la cantidad total de tráfico que se debe transmitir entre los sitios. Además, la configuración de QoS puede soportar cualquier combinación de características de QoS ofrecidas en Cisco IOS Software, para soportar la Voz, el vídeo, o las aplicaciones de datos un de los.

> Nota: La configuración de QoS en esta guía está para la demostración solamente. Se espera que los resultados del scalability VTI sean similares al Generic Routing Encapsulation (GRE) de punto a punto (P2P) sobre el IPSec. Por escalar y Consideraciones

de rendimiento, entre en contacto su representante de Cisco. Para la información adicional, vea configurar una interfaz del túnel virtual con la seguridad IP.

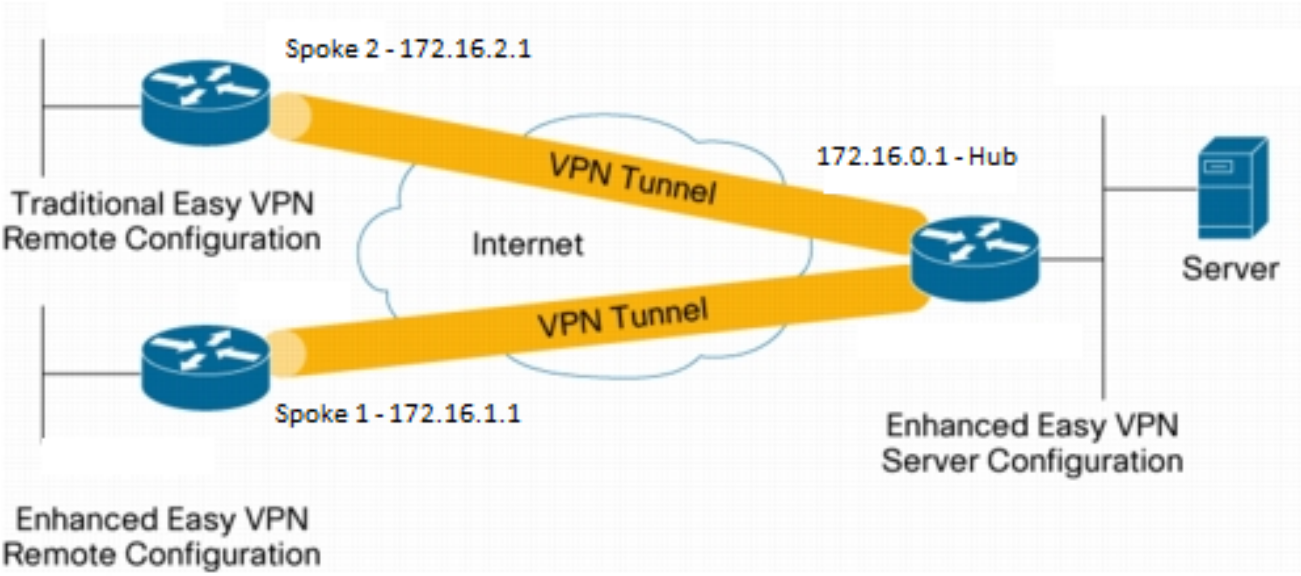
Beneficios

- **Simplifica la Administración**
  Los clientes pueden utilizar la plantilla virtual del Cisco IOS para reproducirse, las interfaces de acceso virtual a pedido, nuevas para el IPSec que simplifica la complejidad de la configuración VPN y la traduce a los costes reducidos. Además, las aplicaciones de administración existentes ahora pueden monitorear las interfaces diferentes para diversos sitios para monitorear los propósitos.
- **Proporciona una interfaz enrutable**
  El IPSec de Cisco VTIs puede apoyar todos los tipos de IP Routing Protocol. Los clientes pueden utilizar estas capacidades para conectar entornos de oficina más grandes, tales como sucursales.
- **Mejora el escalamiento**
  Asociaciones de seguridad del uso de VTIs del IPSec solas por el sitio, que cubren diversos tipos de tráfico, habilitando el escalamiento mejorado.
- **Flexibilidad de las ofertas en la definición de las características**
  Un IPSec VTI es una encapsulación dentro de su propia interfaz. Esto ofrece la flexibilidad de definir las características para el tráfico del texto claro en el IPSec VTIs y define las características para el tráfico encriptado en las interfaces físicas.

Configurar

Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red



Resumen de la configuración

Configuración del hub

```
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
```

Configuración del Spoke1 (EzVPN aumentado)

```
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
```

> Precaución: La plantilla virtual necesita ser definida antes de que se ingrese la configuración del cliente. Sin una plantilla virtual existente del mismo número, el router no validará el **comando 1 de la interfaz virtual**.

Configuración del Spoke2 (EzVPN de la herencia)

```
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
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del

comando show.

Concentrador al túnel del Spoke1

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

Los proxys aquí están para ningunos/ningunos que implique que cualquier tráfico que salga el acceso virtual 1 conseguirá cifrado y enviado a 172.16.1.1.

```
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
```

Nota: El Spoke2 no forma una entrada pues no es posible formar a un par del Enhanced Interior Gateway Routing Protocol (EIGRP) sin una interfaz enrutable. Éste es una de las ventajas del uso de los dVTIs en el spoke.

Spoke1

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
```

El rutear - EIGRP

En el Spoke2 los proxys son tales que cualquier tráfico que salga la interfaz de acceso virtual conseguirá cifrado. Mientras haya una ruta que señala que la interfaz para una red, el tráfico conseguirá cifrada:

```
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#
```

Concentrador al túnel del Spoke2

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

Un túnel dividido ACL bajo configuración del cliente en el concentrador no se utiliza en este ejemplo. Por lo tanto los proxys que se forman en el spoke están para cualquier red del “interior” del EzVPN en hablaron a cualquier red. Básicamente, en el concentrador, cualquier tráfico destinado a una de las redes del “interior” en el spoke conseguirá cifrado y enviado a 172.16.2.1.

```
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:
```

Spoke 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
```

El rutear - Estático

A diferencia del Spoke1, el Spoke2 tiene que tener las Static rutas o Reverse Route Injection (RRI) del uso para inyectar las rutas para decirle qué tráfico debe conseguir cifrado y qué no debe. En este ejemplo, trafique solamente originado del loopback0 consigue cifrado según los proxys y la encaminamiento.

```
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
```

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

> Consejo: En el EzVPN los túneles no suben muy a menudo después de los cambios de configuración. Borrar la fase 1 y la fase 2 no traerá los túneles para arriba en este caso. En la mayoría de los casos, ingrese **crypto ipsec client el** comando **claro del EzVPN <group-name>** en el spoke para traer para arriba el túnel.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Comandos hub

- **IPSec del debug crypto** - Visualiza los IPSec Negotiations de la fase 2.
- debug crypto isakmp - Muestra las negociaciones ISAKMP para la fase 1.

Comandos del spoke

- **IPSec del debug crypto -** Visualiza los IPSec Negotiations de la fase 2.
- debug crypto isakmp - Muestra las negociaciones ISAKMP para la fase 1.
- **debug crypto ipsec client ezvpn -** Visualiza los debugs del EzVPN.

Información Relacionada

- Página de soporte de IPSec
- Cisco Easy VPN Remote
- Easy VPN Server
- Interfaz del túnel virtual del IPSec
- Configurar el IPSec Network Security
- Configuración del protocolo de seguridad de intercambio de claves de Internet
- Soporte Técnico y Documentación - Cisco Systems