Ejemplo de Configuración de Migración de EzVPN Heredada a EzVPN Mejorada

Contenido

Introducción

Este documento describe cómo configurar una configuración Easy VPN (EzVPN) donde Spoke 1 utiliza EzVPN mejorado para conectarse al hub, mientras que Spoke 2 utiliza EzVPN heredada para conectarse al mismo hub. El hub está configurado para EzVPN mejorado. La diferencia entre EzVPN mejorada y EzVPN heredada es el uso de interfaces de túnel virtual dinámicas (dVTIs) en los mapas de criptografía y en los mapas criptográficos de estos últimos. Cisco dVTI es un método que pueden utilizar los clientes con Cisco EzVPN para la configuración del servidor y remota. Los túneles proporcionan una interfaz de acceso virtual independiente a demanda para cada conexión EzVPN. La configuración de las interfaces de acceso virtual se clona a partir de una configuración de plantilla virtual, que incluye la configuración de IPsec y cualquier función de Cisco IOS® Software configurada en la interfaz de plantilla virtual, como QoS, NetFlow o listas de control de acceso (ACL).

Con los dVTIs de IPsec y Cisco EzVPN, los usuarios pueden proporcionar una conectividad muy segura para las VPNs de acceso remoto que se pueden combinar con Cisco AVVID (Architecture for Voice, Video and Integrated Data) para ofrecer voz, vídeo y datos convergentes a través de redes IP.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de EzVPN.

Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Cisco EzVPN con configuración dVTI proporciona una interfaz enrutable para enviar el tráfico selectivamente a diferentes destinos, como un concentrador EzVPN, un par de sitio a sitio diferente o Internet. La configuración dVTI de IPSec no requiere un mapping estático de las sesiones IPsec a una interfaz física. Esto permite la flexibilidad para enviar y recibir tráfico cifrado en cualquier interfaz física, como en el caso de varias trayectorias. El tráfico se cifra cuando se reenvía desde o hacia la interfaz de túnel.

El tráfico se reenvía hacia o desde la interfaz de túnel en virtud de la tabla de IP Routing. Las rutas se aprenden dinámicamente durante la configuración del modo de intercambio de claves de Internet (IKE) e se insertan en la tabla de routing que apunta a dVTI. El ruteo IP dinámico se puede utilizar para propagar rutas a través de la VPN. El uso del ruteo IP para reenviar el tráfico

al encripción simplifica la configuración de VPN IPSec cuando se compara con el uso de ACL con el mapa crypto en la configuración IPsec nativa.

En las versiones anteriores a Cisco IOS Release 12.4(2)T, en la transición de túnel ascendente/túnel descendente, los atributos que se presionaron durante la configuración de modo tuvieron que analizarse y aplicarse. Cuando dichos atributos dieron como resultado la aplicación de configuraciones en la interfaz, la configuración existente tuvo que ser reemplazada. Con la función dVTI Support, la configuración de túnel se puede aplicar a interfaces separadas, lo que facilita el soporte de funciones separadas en el tiempo de túnel. Las funciones que se aplican al tráfico (antes del cifrado) que entra en el túnel pueden estar separadas de las funciones que se aplican al tráfico que no pasa por el túnel (por ejemplo, el tráfico de túnel dividido y el tráfico que sale del dispositivo cuando el túnel no está activo).

Cuando la negociación EzVPN es exitosa, el estado del protocolo de línea de la interfaz de acceso virtual cambia a up. Cuando el túnel EzVPN se desactiva porque la asociación de seguridad caduca o se elimina, el estado del protocolo de línea de la interfaz de acceso virtual cambia a desactivado.

Las tablas de ruteo actúan como selectores de tráfico en una configuración de interfaz virtual EzVPN, es decir, las rutas reemplazan la lista de acceso en el mapa criptográfico. En una configuración de interfaz virtual, EzVPN negocia una única asociación de seguridad IPsec si el servidor EzVPN se ha configurado con un dVTI IPSec. Esta única asociación de seguridad se crea independientemente del modo EzVPN configurado.

Después de establecer la asociación de seguridad, las rutas que apuntan a la interfaz de acceso virtual se agregan para dirigir el tráfico a la red corporativa. EzVPN también agrega una ruta al concentrador VPN para que los paquetes encapsulados por IPSec se enruten a la red corporativa. En el caso de un modo no dividido, se agrega una ruta predeterminada que apunta a la interfaz de acceso virtual. Cuando el servidor EzVPN "empuja" el túnel dividido, la subred del túnel dividido se convierte en el destino al que se agregan las rutas que apuntan al acceso virtual. En cualquier caso, si el par (concentrador VPN) no está conectado directamente, EzVPN agrega una ruta al par.

> **Nota:** La mayoría de los routers que ejecutan el software Cisco EzVPN Client tienen una ruta predeterminada configurada. La ruta predeterminada configurada debe tener un valor de métrica mayor que 1, ya que EzVPN agrega una ruta predeterminada que tiene un valor de métrica de 1. La ruta apunta a la interfaz de acceso virtual para que todo el tráfico se dirija a la red corporativa cuando el concentrador no "empuja" el atributo de túnel dividido.

QoS se puede utilizar para mejorar el rendimiento de las diferentes aplicaciones en 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 admitir cualquier combinación de funciones de QoS ofrecidas en Cisco IOS Software, para soportar cualquiera de las aplicaciones de voz, vídeo o datos.

> **Nota:** La configuración de QoS de esta guía es sólo para demostración. Se espera que los resultados de la escalabilidad de VTI sean similares a la encapsulación de routing genérico (GRE) punto a punto (P2P) a través de IPsec. Para conocer las consideraciones de escalabilidad y rendimiento, póngase en contacto con su representante de Cisco. Para obtener información adicional, vea Configuración de una Interfaz de Túnel Virtual con Seguridad IP.

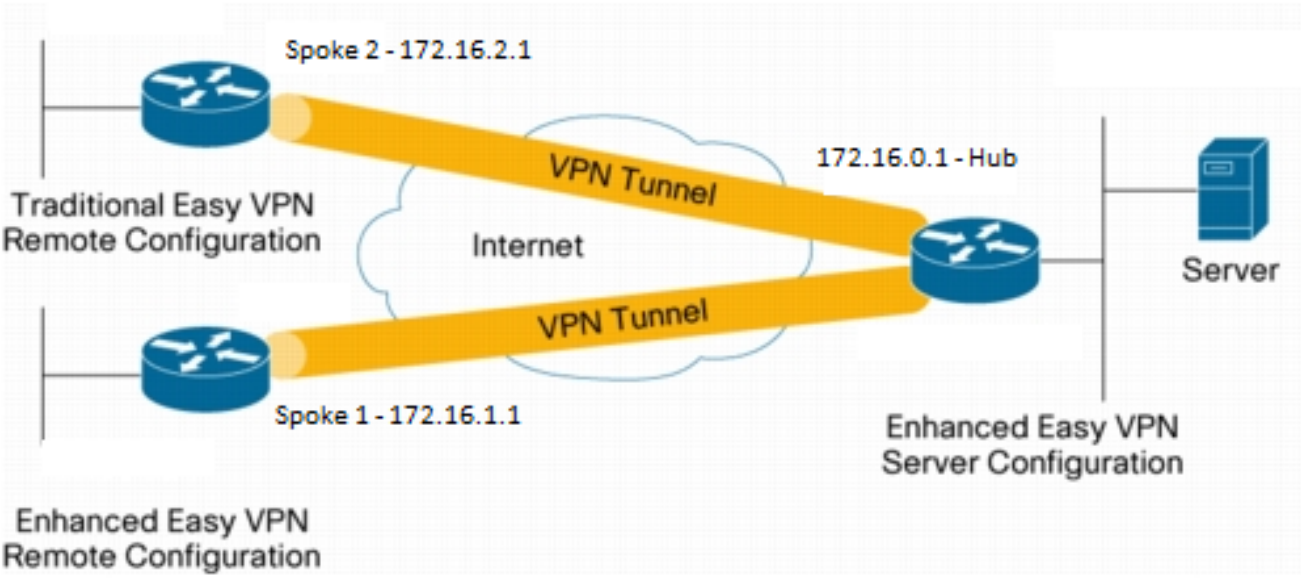
Beneficios

- **Simplifica la gestión**
  Los clientes pueden utilizar la plantilla virtual de Cisco IOS para clonar, a demanda, nuevas interfaces de acceso virtual para IPsec, lo que simplifica la complejidad de la configuración de VPN y se traduce en costes reducidos. Además, las aplicaciones de gestión existentes ahora pueden supervisar interfaces separadas para diferentes sitios con fines de supervisión.
- **Proporciona una interfaz enrutable**
  Cisco IPsec VTI puede admitir todos los tipos de protocolos de routing IP. Los clientes pueden utilizar estas capacidades para conectar entornos de oficinas más grandes, como las sucursales.
- **Mejora la escalabilidad**
  Las VTIs IPsec utilizan asociaciones de seguridad únicas por sitio, que cubren diferentes tipos de tráfico, lo que permite mejorar la escalabilidad.
- **Ofrece flexibilidad a la hora de definir funciones**
  Un VTI IPSec es una encapsulación dentro de su propia interfaz. Esto ofrece flexibilidad para definir funciones para el tráfico de texto sin cifrar en VTIs IPsec y define funciones para el tráfico cifrado en 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 de Spoke 1 (EzVPN mejorado)

```
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 debe definirse antes de ingresar la configuración del cliente. Sin una plantilla virtual existente del mismo número, el router no aceptará el comando **virtual-interface 1**.

Configuración de Spoke 2 (EzVPN heredada)

```
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 de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

Túnel de eje a radio 1

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 proxies aquí son para cualquiera/cualquiera, lo que implica que cualquier tráfico que salga de Virtual Access 1 se cifrará y se enviará 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 radio 2 no forma una entrada, ya que no es posible formar un par EIGRP (del inglés Enhanced Interior Gateway Routing Protocol, protocolo de routing de gateway interior mejorado) sin una interfaz enrutable. Esta es una de las ventajas del uso de dVTI en el spoke.

Spoke 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 - EIGRP

En Spoke 2, los proxies son tales que cualquier tráfico que salga de la interfaz de acceso virtual se cifrará. Mientras haya una ruta que señale esa interfaz para una red, el tráfico se cifrará:

```
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#
```

Túnel de eje a radio 2

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

En este ejemplo no se utiliza una ACL de túnel dividido bajo la configuración del cliente en el hub. Por lo tanto, los proxies que se forman en el spoke son para cualquier red "interna" EzVPN en el spoke a cualquier red. Básicamente, en el hub, cualquier tráfico destinado a una de las redes "internas" en el spoke será 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
```

Routing - Estático

A diferencia del Spoke 1, el Spoke 2 debe tener rutas estáticas o utilizar Inyección de ruta inversa (RRI) para inyectar rutas que le digan qué tráfico debe cifrarse y qué no. En este ejemplo, sólo el tráfico originado en Loopback 0 se cifra según los proxies y el ruteo.

```
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
```

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

> **Consejo:** Muy a menudo en EzVPN los túneles no aparecen después de los cambios de configuración. En este caso, la fase de limpieza 1 y la fase 2 no activarán los túneles. En la mayoría de los casos, ingrese el comando **clear crypto ipsec client ezvpn <group-name>** en el spoke para activar el túnel.

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

Comandos Hub

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

Comandos Spoke

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

Información Relacionada

- Página de soporte de IPSec
- Cisco Easy VPN Remote
- Servidor Easy VPN
- Interfaz del Túnel Virtual IPSec
- Configuración de seguridad de red IPSec
- Configuración del protocolo de seguridad de intercambio de claves de Internet
- Soporte Técnico y Documentación - Cisco Systems