Exemplo de configuração de migração do EzVPN legado para o EzVPN avançado

Contents

Introduction

Este documento descreve como configurar uma configuração Easy VPN (EzVPN) em que o Spoke 1 usa EzVPN aprimorada para se conectar ao hub, enquanto o Spoke 2 usa EzVPN legado para se conectar ao mesmo hub. O hub está configurado para EzVPN avançado. A diferença entre o EzVPN aprimorado e o EzVPN legado é o uso de dVTIs (Virtual Tunnel Interfaces) dinâmicas no primeiro e mapas de criptografia no segundo. O Cisco dVTI é um método que pode ser usado por clientes com Cisco EzVPN para configuração de servidor e remoto. Os túneis fornecem uma interface de acesso virtual separada sob demanda para cada conexão EzVPN. A configuração das interfaces de acesso virtual é clonada a partir de uma configuração de modelo virtual, que inclui a configuração IPsec e qualquer recurso de software Cisco IOS® configurado na interface de modelo virtual, como QoS, NetFlow ou listas de controle de acesso (ACLs).

Com o IPsec dVTIs e o Cisco EzVPN, os usuários podem fornecer conectividade altamente segura para VPNs de acesso remoto que podem ser combinadas com o Cisco AVVID (Architecture for Voice, Video and Integrated Data) para fornecer voz, vídeo e dados convergentes sobre redes IP.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do EzVPN.

Componentes Utilizados

As informações neste documento são baseadas no Cisco IOS versão 15.4(2)T.

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.

Informações de Apoio

O Cisco EzVPN com a configuração dVTI fornece uma interface roteável para enviar seletivamente tráfego para diferentes destinos, como um concentrador EzVPN, um ponto a ponto diferente ou a Internet. A configuração do IPsec dVTI não exige um mapeamento estático de sessões IPsec para uma interface física. Isso permite a flexibilidade de enviar e receber tráfego criptografado em qualquer interface física, como no caso de vários caminhos. O tráfego é criptografado quando é encaminhado da interface do túnel ou para ela.

O tráfego é encaminhado para ou da interface do túnel em virtude da tabela de roteamento IP. As rotas são aprendidas dinamicamente durante a configuração do modo Internet Key Exchange (IKE) e inseridas na tabela de roteamento que aponta para o dVTI. O roteamento IP dinâmico pode ser usado para propagar rotas através da VPN. O uso do roteamento IP para encaminhar o

tráfego à criptografia simplifica a configuração da VPN IPsec quando comparado ao uso de ACLs com o mapa de criptografia na configuração IPsec nativa.

Em versões anteriores à versão 12.4(2)T do Cisco IOS, na transição de túnel para cima/túnel para baixo, os atributos que foram enviados durante a configuração do modo tiveram que ser analisados e aplicados. Quando tais atributos resultaram na aplicação de configurações na interface, a configuração existente tinha que ser substituída. Com o recurso de suporte do dVTI, a configuração do túnel pode ser aplicada a interfaces separadas, o que facilita o suporte a recursos separados no momento do túnel. Os recursos aplicados ao tráfego (antes da criptografia) que entra no túnel podem ser separados dos recursos aplicados ao tráfego que não passa pelo túnel (por exemplo, tráfego de túnel dividido e tráfego que sai do dispositivo quando o túnel não está ativo).

Quando a negociação de EzVPN é bem-sucedida, o estado do protocolo de linha da interface de acesso virtual é alterado para ativado. Quando o túnel EzVPN é desativado porque a associação de segurança expira ou é excluída, o estado do protocolo de linha da interface de acesso virtual é alterado para inativo.

As tabelas de roteamento atuam como seletores de tráfego em uma configuração de interface virtual EzVPN, ou seja, as rotas substituem a lista de acesso no mapa de criptografia. Em uma configuração de interface virtual, o EzVPN negocia uma única associação de segurança IPsec se o EzVPN Server tiver sido configurado com um IPsec dVTI. Essa associação de segurança única é criada independentemente do modo EzVPN configurado.

Depois que a associação de segurança é estabelecida, as rotas que apontam para a interface de acesso virtual são adicionadas ao tráfego direto para a rede corporativa. O EzVPN também adiciona uma rota ao concentrador VPN para que os pacotes encapsulados de IPsec sejam roteados para a rede corporativa. Uma rota padrão que aponta para a interface de acesso virtual é adicionada no caso de um modo não dividido. Quando o servidor EzVPN "empurra" o túnel dividido, a sub-rede do túnel dividido torna-se o destino ao qual as rotas que apontam para o acesso virtual são adicionadas. Em ambos os casos, se o peer (VPN concentrator) não estiver diretamente conectado, o EzVPN adiciona uma rota ao peer.

> **Note**: A maioria dos roteadores que executam o software Cisco EzVPN Client tem uma rota padrão configurada. A rota padrão configurada deve ter um valor de métrica maior que 1, pois EzVPN adiciona uma rota padrão que tem um valor de métrica 1. A rota aponta para a interface de acesso virtual de modo que todo o tráfego seja direcionado para a rede corporativa quando o concentrador não "empurra" o atributo de túnel dividido.

A QoS pode ser usada para melhorar o desempenho de diferentes aplicativos na rede. Nesta configuração, a modelagem de tráfego é usada entre os dois sites para limitar a quantidade total de tráfego que deve ser transmitida entre os sites. Além disso, a configuração de QoS pode suportar qualquer combinação de recursos de QoS oferecidos no Cisco IOS Software, para suportar qualquer dos aplicativos de voz, vídeo ou dados.

> **Note**: A configuração de QoS neste guia é somente para demonstração. Espera-se que os resultados da escalabilidade do VTI sejam semelhantes ao GRE (Generic Routing Encapsulation, Encapsulamento de roteamento genérico) P2P (Point-to-Point) sobre IPsec. Para considerações sobre dimensionamento e desempenho, entre em contato com o representante da Cisco. Para obter informações adicionais, consulte Configurando uma Interface de Túnel Virtual com Segurança IP.

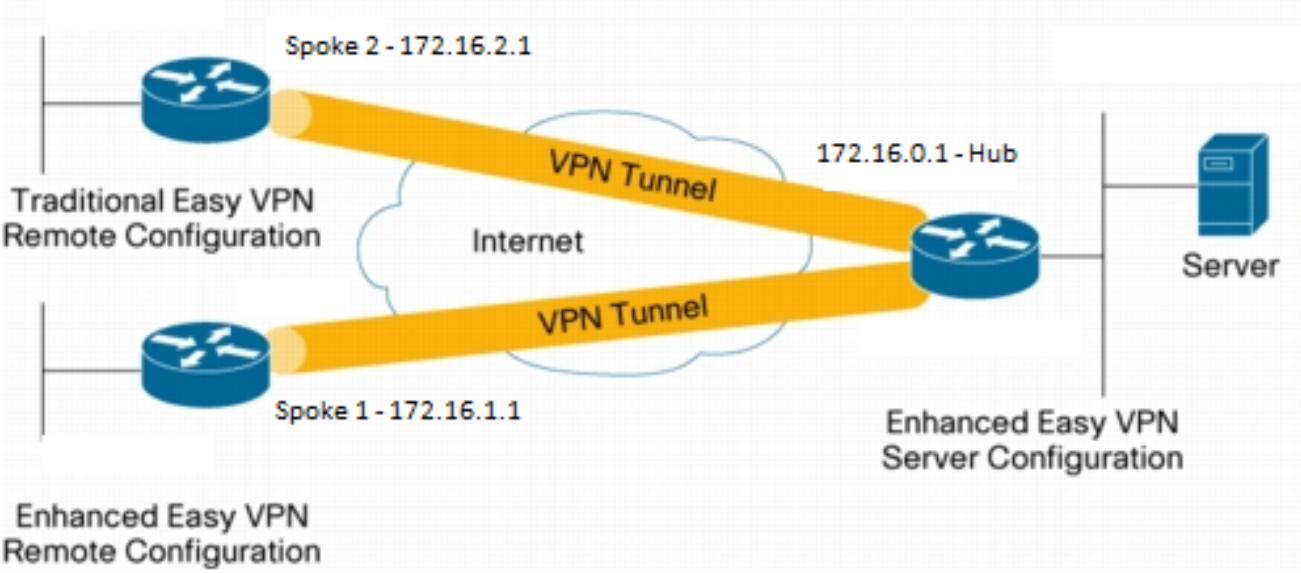
Benefícios

- **Simplifica o gerenciamento**
  Os clientes podem usar o modelo virtual do Cisco IOS para clonar, sob demanda, novas interfaces de acesso virtual para IPsec, o que simplifica a complexidade da configuração da VPN e se traduz em custos reduzidos. Além disso, os aplicativos de gerenciamento existentes agora podem monitorar interfaces separadas para locais diferentes para fins de monitoramento.
- **Fornece uma interface roteável**
  Os VTIs IPsec da Cisco podem suportar todos os tipos de protocolos de roteamento IP. Os clientes podem usar esses recursos para conectar ambientes de escritório maiores, como filiais.
- **Melhora o dimensionamento**
  Os VTIs IPsec usam associações de segurança únicas por local, que cobrem diferentes tipos de tráfego, permitindo melhor dimensionamento.
- **Oferece flexibilidade na definição de recursos**
  Um VTI IPsec é um encapsulamento em sua própria interface. Isso oferece flexibilidade de definição de recursos para tráfego de texto claro em VTIs IPsec e define recursos para tráfego criptografado em interfaces físicas.

Configurar

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede



Resumo da configuração

Configuração do 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
```

Configuração do Spoke 1 (Enhanced 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
```

> **Caution**: O modelo virtual precisa ser definido antes que a configuração do cliente seja inserida. Sem um modelo virtual existente com o mesmo número, o roteador não aceitará o comando **virtual-interface 1**.

Configuração do Spoke 2 (EzVPN legado)

```
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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Túnel de Hub para Spoke 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

Os proxies aqui são para qualquer/qualquer que implique que qualquer tráfego que saia do Virtual Access 1 será criptografado e enviado para 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
```

Note: O Spoke 2 não forma uma entrada, pois não é possível formar um peer EIGRP (Enhanced Interior Gateway Routing Protocol) sem uma interface roteável. Essa é uma das vantagens do uso de dVTIs no 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
```

Roteamento - EIGRP

No Spoke 2, os proxies são tais que qualquer tráfego que sai da interface de acesso virtual será criptografado. Enquanto houver uma rota que aponte essa interface para uma rede, o tráfego será criptografado:

```
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 Hub para Spoke 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

Uma ACL de túnel dividido na configuração do cliente no hub não é usada neste exemplo. Portanto, os proxies formados no spoke são para qualquer rede "interna" de EzVPN no spoke para qualquer rede. Basicamente, no hub, qualquer tráfego destinado a uma das redes "internas" no spoke será criptografado e enviado para 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
```

Roteamento - estático

Ao contrário do Spoke 1, o Spoke 2 tem que ter rotas estáticas ou usar a Reverse Route Inject (RRRI) para injetar rotas para informar qual tráfego deve ser criptografado e o que não deve ser.

Neste exemplo, somente o tráfego originado do loopback 0 é criptografado de acordo com os proxies e o roteamento.

```
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

Esta seção disponibiliza informações para a solução de problemas de configuração.

> **Tip**: Muito frequentemente, no EzVPN, os túneis não aparecem após alterações de configuração. A limpeza das fases 1 e 2 não levará os túneis para cima neste caso. Na maioria dos casos, insira o comando **clear crypto ipsec client ezvpn <group-name>** no spoke para ativar o túnel.

> **Note**: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug.**

Comandos do hub

- **debug crypto isakmp – Exibe as negociações IPSec da Fase 2.**

- **debug crypto isakmp – Exibe as negociações ISAKMP da Fase 1.**

Comandos Spoke

- **debug crypto isakmp – Exibe as negociações IPSec da Fase 2.**
- **debug crypto isakmp – Exibe as negociações ISAKMP da Fase 1.**
- **debug crypto ipsec client ezvpn -** Exibe as depurações de EzVPN.

Informações Relacionadas

- Página de suporte do IPSec
- Cisco Easy VPN Remote
- Easy VPN Server
- Interface de túnel virtual IPsec
- Configuração da segurança de rede IPSec
- Configurando o protocolo de segurança do intercâmbio chave de Internet
- Suporte Técnico e Documentação - Cisco Systems