Migração do EzVPN do legado ao exemplo de configuração aumentado do EzVPN

Índice

Introdução

Este documento descreve como configurar um VPN fácil (EzVPN) setup onde Spoke1 usa o EzVPN aumentado a fim conectar ao hub, quando Spoke2 usar o EzVPN do legado a fim conectar ao mesmo hub. O hub é configurado para o EzVPN aumentado. A diferença entre o EzVPN aumentado e o EzVPN do legado é o uso de interfaces de túnel virtuais dinâmicas (dVTIs) no anterior e de crypto map nos últimos. O dVTI de Cisco é um método que possa ser usado por clientes com o EzVPN de Cisco para o server e a configuração remota. Os túneis fornecem uma interface de acesso virtual separada por encomenda para cada conexão do EzVPN. A configuração das interfaces de acesso virtual é clonada de uma configuração de molde virtual, que inclua a configuração IPSec e toda a característica do Cisco IOS ® Software configuradas na relação virtual do molde, tal como QoS, Netflow, ou Access Control Lists (ACLs).

Com dVTIs do IPsec e EzVPN de Cisco, os usuários podem fornecer altamente a conectividade segura para os acessos remoto VPN que podem ser combinados com o Cisco AVVID (Architecture for Voice, Video and integrated Data) para entregar a voz convergida, o vídeo, e os dados sobre redes IP.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do EzVPN.

Componentes Utilizados

A informação neste documento é baseada na versão do Cisco IOS 15.4(2)T.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O EzVPN de Cisco com configuração do dVTI fornece uma interface roteável para enviar seletivamente o tráfego aos destinos diferentes, tais como um concentrador do EzVPN, um par de site para site diferente, ou o Internet. A configuração do dVTI do IPsec não exige um mapeamento estático das sessões IPSec a uma interface física. Isto permite a flexibilidade enviar e receber o tráfego criptografado em toda a interface física, como no caso de caminhos múltiplos. O tráfego é cifrado quando é enviado ou à interface de túnel.

O tráfego é enviado a ou da interface de túnel em virtude da tabela de IP Routing. As rotas são dinamicamente instruídas durante a configuração de modo do Internet Key Exchange (IKE) e são introduzidas na tabela de roteamento esses pontos ao dVTI. O Dynamic IP Routing pode ser usado para propagar rotas através do VPN. Usar Roteamento IP para enviar o tráfego à

criptografia simplifica a configuração do IPSec VPN quando comparada com o uso dos ACL com o crypto map na configuração IPSec nativa.

Nas liberações mais cedo do que o Cisco IOS Release 12.4(2)T, na transição do túnel-acima/túnel-para baixo, os atributos que foram empurrados durante a configuração de modo tiveram que ser analisados gramaticalmente e aplicado. Quando tais atributos conduziram ao aplicativo das configurações na relação, a configuração existente teve que ser cancelada. Com a característica do apoio do dVTI, a configuração do túnel-acima pode ser aplicada às interfaces separadas, que facilita apoiar se separar recursos no tempo do túnel-acima. As características que são aplicadas ao tráfego (antes que criptografia) que entra no túnel podem ser separam das características que são aplicadas para traficar aquela não atravessam o túnel (por exemplo, tráfego do túnel em divisão e tráfego que sae do dispositivo quando o túnel não está acima).

Quando a negociação do EzVPN é bem sucedida, o estado do protocolo de linha da interface de acesso virtual obtém mudado a acima. Quando o túnel do EzVPN vai para baixo porque a associação de segurança expira ou está suprimida, o estado do protocolo de linha da interface de acesso virtual muda a para baixo.

As tabelas de roteamento atuam como os seletores do tráfego em uma interface virtual do EzVPN configuração-que é, as rotas substituem a lista de acessos no crypto map. Em uma configuração da interface virtual, o EzVPN negocia uma única associação de segurança IPSec se o servidor de EzVPN foi configurado com um dVTI do IPsec. Esta única associação de segurança é criada apesar do modo do EzVPN que é configurado.

Depois que a associação de segurança é estabelecida, rotas que o ponto à interface de acesso virtual está adicionado ao tráfego direto à rede corporativa. O EzVPN igualmente adiciona uma rota ao concentrador VPN de modo que os pacotes IPsec-encapsulados obtenham roteados à rede corporativa. Uma rota padrão que aponte à interface de acesso virtual é adicionada no caso de um modo do nonsplit. Quando o servidor de EzVPN “empurra” o túnel em divisão, a sub-rede do túnel em divisão transforma-se o destino a que as rotas que apontam ao acesso virtual são adicionadas. Em qualquer dos casos, se o par (concentrador VPN) não é conectado diretamente, o EzVPN adiciona uma rota ao par.

> Nota: A maioria de Roteadores que executa o software do cliente ezvpn de Cisco tem uma rota padrão configurada. A rota padrão que é configurada deve ter um valor de métrica maior de 1 desde que o EzVPN adiciona uma rota padrão que tenha um valor de métrica de 1. Os pontos de rota à interface de acesso virtual de modo que todo o tráfego esteja dirigido à rede corporativa quando o concentrador “não empurrar” o atributo do túnel em divisão.

QoS pode ser usado para melhorar o desempenho de aplicativos diferentes através da rede. Nesta configuração, o modelagem de tráfego é usado entre os dois locais a fim limitar a quantidade total de tráfego que deve ser transmitida entre os locais. Adicionalmente, a configuração de QoS pode apoiar toda a combinação de características de QoS oferecidas no Cisco IOS Software, apoiar alguma da Voz, o vídeo, ou os aplicativos de dados.

> Nota: A configuração de QoS neste guia é para a demonstração somente. Espera-se que os resultados da escalabilidade VTI serão similares ao Generic Routing Encapsulation (GRE) (P2P) ponto a ponto sobre o IPsec. Para a escamação e as considerações de desempenho, contacte seu representante do Cisco. Para a informação adicional, veja configurar uma interface de túnel virtual com a Segurança IP.

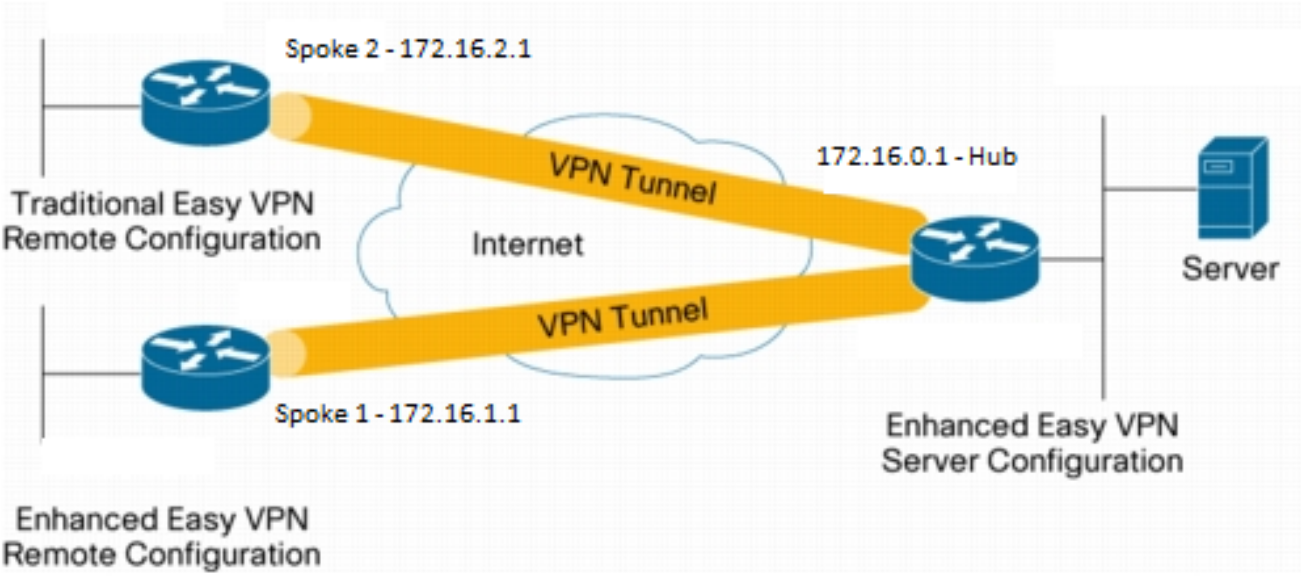
Benefícios

- **Simplifica o Gerenciamento**
  Os clientes podem usar o molde virtual do Cisco IOS para clonar, interfaces de acesso virtual por encomenda, novas para o IPsec que simplifica a complexidade da configuração de VPN e a traduz em custos reduzidos. Além, os aplicativos de gerenciamento existentes agora podem monitorar interfaces separadas para locais diferentes para monitorar finalidades.
- **Fornece uma interface roteável**
  O Cisco IPSEC VTIs pode apoiar todos os tipos de protocolos de IP Routing. Os clientes podem usar estas capacidades a fim conectar ambientes de escritório maiores, tais como escritórios filiais.
- **Melhora a escamação**
  Associações de segurança do uso de VTIs do IPsec únicas pelo local, que cobrem tipos de tráfego diferentes, permitindo a escamação melhorada.
- **Flexibilidade das ofertas em definir características**
  Um IPsec VTI é um encapsulamento dentro de sua própria relação. Isto oferece a flexibilidade de definir características para o tráfego da minuta no IPsec VTIs e define características para o tráfego criptografado em interfaces física.

Configurar

> Nota: 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 de 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
```

> Cuidado: O molde virtual precisa de ser definido antes que a configuração de cliente esteja incorporada. Sem um molde virtual existente do mesmo número, o roteador não aceitará o o comando 1 da interface virtual.

Configuração de Spoke2 (EzVPN do 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 (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Hub ao túnel de 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

Os proxys aqui são para alguns/alguns que implicarem que todo o tráfego que retirar o acesso virtual 1 obterá cifrado e 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: Spoke2 não forma uma entrada porque não é possível formar um par do Enhanced Interior Gateway Routing Protocol (EIGRP) sem uma interface roteável. Esta é uma das vantagens do uso dos dVTIs no 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
```

Distribuir - EIGRP

Em Spoke2 os proxys são tais que todo o tráfego que retirar a interface de acesso virtual obterá cifrado. Enquanto há uma rota que indique essa relação para uma rede, o tráfego obterá cifrado:

```
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 ao túnel de 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

Um túnel em divisão ACL sob a configuração de cliente no hub não é usado neste exemplo. Consequentemente os proxys que são formados no spoke são para toda a rede do “interior” do EzVPN no falaram a qualquer rede. Basicamente, no hub, todo o tráfego destinado a uma das redes do “interior” no spoke obterá cifrado e 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:
```

Spoke2

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
```

Distribuir - Estático

Ao contrário de Spoke1, Spoke2 tem que ter rotas estáticas ou Reverse Route Injection (RRI) do uso a fim injetar rotas para dizer lhe que tráfego deve obter cifrado e o que não deve. Neste exemplo, trafique somente originado de Loopback0 obtém cifrado conforme os proxys 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
```

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

> Dica: Muito frequentemente no EzVPN os túneis não vêm acima após alterações de configuração. Cancelar a fase 1 e a fase 2 não trará os túneis acima neste caso. Na maioria dos casos, incorpore o comando **claro do <group-name> do EzVPN do cliente de IPSec de criptografia ao** spoke a fim trazer acima o túnel.

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

Comandos hub

- **IPsec do debug crypto** - Indica as negociações de IPSEC de fase 2.
- debug crypto isakmp – Exibe as negociações ISAKMP da Fase 1.

Comandos do spoke

- **IPsec do debug crypto -** Indica as negociações de IPSEC de fase 2.
- debug crypto isakmp – Exibe as negociações ISAKMP da Fase 1.
- **debug crypto ipsec client ezvpn -** Indica o EzVPN debuga.

Informações Relacionadas

- Página de suporte IPSec
- Telecontrole do Cisco Easy VPN
- Easy VPN Server
- Interface de túnel virtual do IPsec

- Configurando a Segurança de rede IPSec
- Configurando o protocolo de segurança do intercâmbio chave de Internet
- Suporte Técnico e Documentação - Cisco Systems