Transfert d'EzVPN existant à l'exemple amélioré de configuration d'EzVPN

Contenu

Introduction

Ce document décrit comment configurer un Easy VPN (EzVPN) installé où les utilisations du rai 1 ont amélioré l'EzVPN afin de se connecter au hub, alors que le rai 2 emploie l'EzVPN existant afin de se connecter au même hub. Le hub est configuré pour l'EzVPN amélioré. La différence entre l'EzVPN amélioré et l'EzVPN de legs est l'utilisation des interfaces de tunnel virtuelles dynamiques (dVTIs) dans l'ancien et des crypto map dans ce dernier. Le dVTI de Cisco est une méthode qui peut être utilisée par des clients avec l'EzVPN de Cisco pour le serveur et la configuration distante. Les tunnels fournissent une interface d'accès virtuelle distincte de à la demande pour chaque connexion d'EzVPN. La configuration des interfaces d'accès virtuelles est copiée d'une configuration de modèle virtuel, qui inclut la configuration d'IPsec et n'importe quelle caractéristique de logiciel de Cisco IOS® configurées sur l'interface de modèle virtuel, telle que QoS, NetFlow, ou Listes de contrôle d'accès (ACL).

Avec des dVTIs d'IPsec et l'EzVPN de Cisco, les utilisateurs peuvent fournir fortement la connectivité sécurisée pour la remote-access VPN qui peut être combinée avec le Cisco AVVID (architecture pour la Voix, le vidéo et les données intégrées) pour fournir la Voix, le vidéo, et les données convergés au-dessus des réseaux IP.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de l'EzVPN.

Composants utilisés

Les informations dans ce document sont basées sur la version 15.4(2)T de Cisco IOS.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

L'EzVPN de Cisco avec la configuration de dVTI fournit une interface routable pour envoyer sélectivement le trafic à différentes destinations, telles qu'un concentrateur d'EzVPN, un pair différent de site à site, ou l'Internet. La configuration de dVTI d'IPsec n'exige pas un mappage statique des sessions d'IPsec à une interface physique. Ceci tient compte pour que la flexibilité envoie et de reçoit le trafic chiffré sur n'importe quelle interface physique, comme dans le cas des plusieurs chemins. Le trafic est chiffré quand il est expédié ou derrière l'interface de tunnel.

Le trafic est expédié à ou de l'interface de tunnel en vertu de la table de Routage IP. Des artères sont dynamiquement apprises pendant la configuration de mode d'Échange de clés Internet (IKE) et insérées dans la table de routage ces points au dVTI. Le Routage IP dynamique peut être

utilisé pour propager des artères à travers le VPN. Utilisant le Routage IP expédier le trafic au cryptage simplifie la configuration du VPN d'IPsec en comparaison avec l'utilisation d'ACLs avec le crypto map dans la configuration indigène d'IPsec.

Dans les versions plus tôt que la Cisco IOS version 12.4(2)T, au tunnel-/à transition de tunnel-vers le bas, des attributs qui ont été poussés pendant la configuration de mode ont dû être analysés et appliqués. Quand de tels attributs ont eu comme conséquence l'application des configurations sur l'interface, la configuration existante a dû être ignorée. Avec la configuration de support de dVTI, la configuration de tunnel- peut être appliquée pour séparer des interfaces, qui le facilite pour prendre en charge les caractéristiques distinctes au temps de tunnel-. Les caractéristiques qui sont appliquées au trafic (avant cryptage) qui entre dans le tunnel peuvent être séparé des caractéristiques qui sont appliquées pour trafiquer cela ne passe pas par le tunnel (par exemple, le trafic de tunnel partagé et le trafic qui laisse le périphérique quand le tunnel n'est pas).

Quand la négociation d'EzVPN est réussie, la ligne état de protocole de l'interface d'accès virtuelle obtient changé à. Quand le tunnel d'EzVPN descend parce que l'association de sécurité expire ou est supprimée, la ligne état de protocole de l'interface d'accès virtuelle change à vers le bas.

Les tables de routage agissent en tant que sélecteurs du trafic dans une interface virtuelle d'EzVPN configuration-qu'est, les artères remplacent la liste d'accès sur le crypto map. Dans une configuration d'interface virtuelle, l'EzVPN négocie une association de sécurité simple d'IPsec si le serveur d'EzVPN a été configuré avec un dVTI d'IPsec. Cette association de sécurité simple est créée indépendamment du mode d'EzVPN qui est configuré.

Après que l'association de sécurité soit établie, des artères que le point à l'interface d'accès virtuelle sont ajoutés pour se diriger le trafic au réseau d'entreprise. L'EzVPN ajoute également une artère au concentrateur VPN de sorte que les paquets IPsec-encapsulés obtiennent conduit au réseau d'entreprise. Un default route qui indique l'interface d'accès virtuelle est ajouté dans le cas d'un mode de nonsplit. Quand le serveur d'EzVPN « pousse » le tunnel partagé, le sous-réseau de tunnel partagé devient la destination à laquelle les artères qui indiquent l'accès virtuel sont ajoutées. Dans l'un ou l'autre de cas, si le pair (concentrateur VPN) n'est pas directement connecté, l'EzVPN ajoute une artère au pair.

> Remarque: La plupart des Routeurs qui exécutent le logiciel client d'EzVPN de Cisco font configurer un default route. Le default route qui est configuré doit avoir une valeur métrique plus grande que 1 puisque l'EzVPN ajoute un default route qui a une valeur métrique de 1. Les points d'acheminement à l'interface d'accès virtuelle de sorte que tout le trafic soit dirigé vers le réseau d'entreprise quand le concentrateur « ne pousse pas » l'attribut de tunnel partagé.

QoS peut être utilisé pour améliorer la représentation des applications différentes à travers le réseau. Dans cette configuration, la formation du trafic est utilisée entre les deux sites afin de limiter le trafic total qui devrait être transmis entre les sites. Supplémentaire, la configuration QoS peut prendre en charge n'importe quelle combinaison des caractéristiques de QoS offertes en logiciel de Cisco IOS, pour prendre en charge la Voix, le vidéo, ou les applications de données l'un des.

> Remarque: La configuration QoS de ce guide est pour la démonstration seulement. On s'attend à ce que les résultats d'évolutivité VTI soient semblables à l'Encapsulation de routage générique (GRE) point par point (de P2P) au-dessus d'IPsec. Pour des considérations de mesurage et de représentation, entrez en contact avec votre représentant

Cisco. Pour information les informations complémentaires, voyez configurer une interface de tunnel virtuelle avec la sécurité IP.

Avantages

- **Simplifie la Gestion**
  Les clients peuvent utiliser le modèle virtuel de Cisco IOS pour copier, à la demande, de nouvelles interfaces d'accès virtuelles pour IPsec qui simplifie la complexité de configuration du VPN et se traduit en coûts réduits. En outre, les applications d'administration existantes maintenant peuvent surveiller les interfaces distinctes pour différents sites pour surveiller des buts.
- **Fournit une interface de Routable**
  Cisco IPsec VTIs peut prendre en charge tous les types de protocoles de Routage IP. Les clients peuvent employer ces capacités afin de connecter de plus grands environnements de bureau, tels que des succursales.
- **Améliore l'évolution**
  Associations de sécurité simples d'utilisation d'IPsec VTIs par site, qui couvrent différents types de trafic, activant l'évolution améliorée.
- **Flexibilité d'offres en définissant des caractéristiques**
  Un IPsec VTI est une encapsulation dans sa propre interface. Ceci offre la flexibilité de définir des caractéristiques pour le trafic de libellé sur IPsec VTIs et définit des caractéristiques pour le trafic chiffré sur des interfaces physiques.

Configurez

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Résumé de configuration

Configuration du concentrateur

```
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
```

Configuration du rai 1 (EzVPN amélioré)

```
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
```

Attention : Le modèle virtuel doit être défini avant que la configuration de client soit écrite. Sans modèle virtuel existant du même nombre, le routeur ne recevra pas la la commande de l'**interface virtuelle 1**.

Configuration du rai 2 (EzVPN existant)

```
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
```

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Hub au tunnel du rai 1

Phase 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
```

Phase 2

Les proxys ici en sont pour/qui impliquent que n'importe quel trafic qui quitte Access virtuel 1 obtiendra chiffré et envoyé à 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
```

Remarque: Le rai 2 ne forme pas une entrée car il n'est pas possible de former un pair de Protocole EIGPR (Enhanced Interior Gateway Routing Protocol) sans interface routable.

C'est l'un des avantages de l'utilisation des dVTIs sur le rai.

Rai 1

Phase 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
```

Phase 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
```

Acheminement - EIGRP

Dans le 2le de rai les proxys sont tels que n'importe quel trafic qui quitte l'interface d'accès virtuelle obtiendra chiffré. Tant que il y a une artère qui précise cette interface pour un réseau, le trafic obtiendra chiffré :

```
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 au tunnel du rai 2

Phase 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
```

Phase 2

Un ACL de tunnel partagé sous la configuration de client sur le hub n'est pas utilisé dans cet exemple. Par conséquent les proxys qui sont formés sur le rai sont pour n'importe quel réseau de « intérieur » d'EzVPN sur ont parlé à n'importe quel réseau. Fondamentalement, sur le hub, en trafiquent destiné à un des réseaux de « intérieur » sur le rai obtiendront chiffré et envoyé à 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:
```

Rai 2

Phase 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
```

Phase 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
```

Acheminement - Statique

Àla différence du rai 1, le rai 2 doit avoir les artères statiques ou l'Injection inversée de routes (RRI) d'utilisation afin d'injecter des artères pour lui indiquer quel trafic devrait obtenir chiffré et ce qui ne devrait pas. Dans cet exemple, trafiquez seulement originaire du bouclage 0 obtient chiffré selon les proxys et le routage.

```
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
```

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

> **Conseil** : Très souvent dans l'EzVPN les tunnels ne montent pas après des modifications de configuration. Effacer la phase 1 et la phase 2 n'apportera pas les tunnels dans ce cas. Dans la plupart des cas, sélectionnez la commande de **<group-name> de clear crypto ipsec client ezvpn** dans le rai afin d'apporter le tunnel.

> Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Commandes de hub

- **debug crypto ipsec** - Affiche les négociations IPSecs du Phase 2.
- **debug crypto isakmp -** Affiche les négociations ISAKMP du Phase 1.

Commandes de rai

- **debug crypto ipsec -** Affiche les négociations IPSecs du Phase 2.
- **debug crypto isakmp -** Affiche les négociations ISAKMP du Phase 1.
- **EzVPN de client de debug crypto ipsec -** Affiche l'EzVPN met au point.

Informations connexes

- Page d'assistance IPsec
- Distant de Solution Cisco Easy VPN
- Serveur Easy VPN
- Interface de tunnel virtuelle d'IPsec
- Sécurité des réseaux de configuration d'IPSec
- Configurer le protocole de sécurité IKE
- Support et documentation techniques - Cisco Systems