Exemple de configuration de la migration d'EzVPN hérité vers Enhanced EzVPN

Contenu

Introduction

Ce document décrit comment configurer une configuration Easy VPN (EzVPN) où Spoke 1 utilise EzVPN amélioré afin de se connecter au concentrateur, tandis que Spoke 2 utilise EzVPN hérité afin de se connecter au même concentrateur. Le concentrateur est configuré pour EzVPN amélioré. La différence entre EzVPN amélioré et EzVPN hérité réside dans l'utilisation d'interfaces de tunnel virtuel dynamiques (dVTI) dans la première et de crypto-cartes dans la seconde. Cisco dVTI est une méthode qui peut être utilisée par les clients disposant de Cisco EzVPN pour la configuration du serveur et de la configuration à distance. Les tunnels fournissent une interface d'accès virtuel séparée à la demande pour chaque connexion EzVPN. La configuration des interfaces d'accès virtuel est clonée à partir d'une configuration de modèle virtuel, qui inclut la configuration IPsec et toute fonctionnalité du logiciel Cisco IOS® configurée sur l'interface de modèle virtuel, telle que QoS, NetFlow ou listes de contrôle d'accès.

Grâce aux dVTI IPsec et à Cisco EzVPN, les utilisateurs peuvent fournir une connectivité hautement sécurisée pour les VPN d'accès à distance qui peuvent être combinés à Cisco AVVID (Architecture for Voice, Video and Integrated Data) pour fournir la voix, la vidéo et les données convergées sur des réseaux IP.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître EzVPN.

Components Used

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

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.

Informations générales

La configuration de Cisco EzVPN avec dVTI fournit une interface routable pour envoyer sélectivement le trafic vers différentes destinations, comme un concentrateur EzVPN, un homologue site à site différent ou Internet. La configuration IPsec dVTI ne nécessite pas de mappage statique des sessions IPsec vers une interface physique. Cela permet la flexibilité d'envoyer et de recevoir du trafic chiffré sur n'importe quelle interface physique, par exemple dans le cas de chemins multiples. Le trafic est chiffré lorsqu'il est transféré depuis ou vers l'interface du tunnel.

Le trafic est transmis à ou depuis l’interface de tunnel en vertu de la table de routage IP. Les routes sont apprises dynamiquement lors de la configuration du mode IKE (Internet Key Exchange) et insérées dans la table de routage qui pointe vers dVTI. Le routage IP dynamique

peut être utilisé pour propager des routes à travers le VPN. L'utilisation du routage IP pour transférer le trafic vers le chiffrement simplifie la configuration VPN IPsec par rapport à l'utilisation de listes de contrôle d'accès avec la carte de chiffrement dans la configuration IPsec native.

Dans les versions antérieures à la version 12.4(2)T de Cisco IOS, lors de la transition tunnel-up/tunnel-down, les attributs qui ont été poussés pendant la configuration du mode ont dû être analysés et appliqués. Lorsque de tels attributs ont abouti à l'application de configurations sur l'interface, la configuration existante a dû être remplacée. Grâce à la fonctionnalité de prise en charge dVTI, la configuration de tunnel up peut être appliquée à des interfaces distinctes, ce qui facilite la prise en charge de fonctions distinctes au moment de la mise en tunnel. Les fonctionnalités appliquées au trafic (avant cryptage) qui entre dans le tunnel peuvent être distinctes des fonctionnalités appliquées au trafic qui ne traverse pas le tunnel (par exemple, le trafic à tunnel partagé et le trafic qui quitte le périphérique lorsque le tunnel n'est pas actif).

Lorsque la négociation EzVPN est réussie, l'état du protocole de ligne de l'interface d'accès virtuelle devient actif. Lorsque le tunnel EzVPN tombe en panne en raison de l'expiration ou de la suppression de l'association de sécurité, l'état du protocole de ligne de l'interface d'accès virtuelle devient désactivé.

Les tables de routage agissent comme des sélecteurs de trafic dans une configuration d'interface virtuelle EzVPN, c'est-à-dire que les routes remplacent la liste d'accès sur la carte de chiffrement. Dans une configuration d'interface virtuelle, EzVPN négocie une association de sécurité IPsec unique si le serveur EzVPN a été configuré avec un dVTI IPsec. Cette association de sécurité unique est créée indépendamment du mode EzVPN configuré.

Une fois l'association de sécurité établie, les routes qui pointent vers l'interface d'accès virtuel sont ajoutées pour diriger le trafic vers le réseau d'entreprise. EzVPN ajoute également une route au concentrateur VPN afin que les paquets encapsulés IPsec soient routés vers le réseau d'entreprise. Une route par défaut qui pointe vers l'interface d'accès virtuelle est ajoutée dans le cas d'un mode non partagé. Lorsque le serveur EzVPN « pousse » le tunnel partagé, le sous-réseau du tunnel partagé devient la destination vers laquelle les routes qui pointent vers l'accès virtuel sont ajoutées. Dans les deux cas, si l'homologue (concentrateur VPN) n'est pas directement connecté, EzVPN ajoute une route à l'homologue.

> **Note**: La plupart des routeurs qui exécutent le logiciel Cisco EzVPN Client ont une route par défaut configurée. La route par défaut configurée doit avoir une valeur de métrique supérieure à 1, car EzVPN ajoute une route par défaut ayant une valeur de métrique de 1. La route pointe vers l'interface d'accès virtuel de sorte que tout le trafic soit dirigé vers le réseau d'entreprise lorsque le concentrateur ne pousse pas l'attribut de tunnel partagé.

La QoS peut être utilisée pour améliorer les performances de différentes applications sur le réseau. Dans cette configuration, le formatage du trafic est utilisé entre les deux sites afin de limiter la quantité totale de trafic qui doit être transmise entre les sites. En outre, la configuration QoS peut prendre en charge n'importe quelle combinaison de fonctions QoS offertes dans le logiciel Cisco IOS, pour prendre en charge n'importe quelle application voix, vidéo ou données.

> **Note**: La configuration QoS de ce guide est réservée à la démonstration. Les résultats d'évolutivité VTI devraient être similaires à ceux de l'encapsulation de routage générique (GRE) point à point (P2P) sur IPsec. Pour des considérations d'évolutivité et de performances, contactez votre représentant Cisco. Pour plus d'informations, consultez Configuration d'une interface de tunnel virtuel avec la sécurité IP.

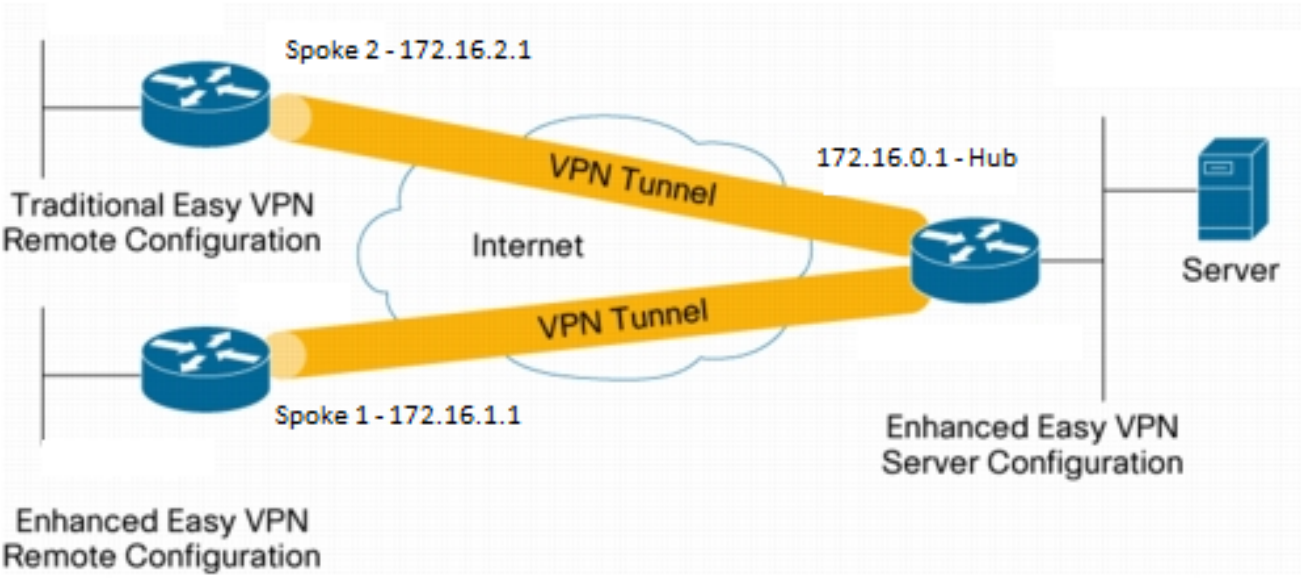
Avantages

- **Simplifie la gestion**
  Les clients peuvent utiliser le modèle virtuel Cisco IOS pour cloner, à la demande, de nouvelles interfaces d'accès virtuel pour IPsec, ce qui simplifie la configuration VPN et se traduit par une réduction des coûts. En outre, les applications de gestion existantes peuvent désormais surveiller des interfaces distinctes pour différents sites à des fins de surveillance.
- **Fournit une interface de routage**
  Les VTI Cisco IPsec peuvent prendre en charge tous les types de protocoles de routage IP. Les clients peuvent utiliser ces fonctionnalités pour connecter des environnements de bureau plus importants, tels que les filiales.
- **Améliore l'évolutivité**
  Les VTI IPsec utilisent des associations de sécurité uniques par site, qui couvrent différents types de trafic, permettant une évolutivité améliorée.
- **Flexibilité dans la définition des fonctionnalités**
  Une VTI IPsec est une encapsulation au sein de sa propre interface. Cela offre la souplesse nécessaire pour définir des fonctionnalités pour le trafic en texte clair sur les VTI IPsec et définit des fonctionnalités pour le trafic chiffré sur les interfaces physiques.

Configuration

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

Diagramme du réseau



Résumé de la 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 de 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
```

> **Attention** : Le modèle virtuel doit être défini avant d'entrer la configuration du client. Sans modèle virtuel existant du même numéro, le routeur n'accepte pas la commande **virtual-interface 1**.

Configuration de Spoke 2 (EzVPN hérité)

```
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
```

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Tunnel Hub to Spoke 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 proxies ici sont pour any/any, ce qui implique que tout trafic qui quitte Virtual Access 1 sera 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
```

Note: Spoke 2 ne forme pas d'entrée car il n'est pas possible de former un homologue EIGRP (Enhanced Interior Gateway Routing Protocol) sans interface routable. C'est l'un des avantages de l'utilisation dVTI sur le rayon.

Spoke 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
```

Routage - EIGRP

Dans Spoke 2, les proxys sont tels que tout trafic qui sort de l'interface d'accès virtuel sera chiffré. Tant qu'il existe une route qui indique cette interface pour un réseau, le trafic sera 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#
```

Tunnel Hub to Spoke 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

Une liste de contrôle d'accès à tunnel partagé sous la configuration du client sur le concentrateur n'est pas utilisée dans cet exemple. Par conséquent, les proxies qui sont formés sur le rayon sont pour n'importe quel réseau EzVPN « interne » sur le rayon à n'importe quel réseau. En gros, sur le concentrateur, tout trafic destiné à l'un des réseaux « internes » du rayon sera 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:
```

Spoke 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
```

Routage - Statique

Contrairement à Spoke 1, Spoke 2 doit avoir des routes statiques ou utiliser RI (Reverse Route Injection) afin d'injecter des routes pour lui dire quel trafic doit être chiffré et ce qui ne doit pas l'être. Dans cet exemple, seul le trafic provenant de Loopback 0 est chiffré selon les proxies 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
```

Dépannage

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

> **Astuce** : Très souvent, dans EzVPN, les tunnels ne s'allument pas après les modifications de configuration. Les phases 1 et 2 de défrichement ne feront pas monter les tunnels dans ce cas. Dans la plupart des cas, entrez la commande **clear crypto ipsec client ezvpn <nom-groupe>** dans le rayon afin d'activer le tunnel.

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

Commandes Hub

- **debug crypto ipsec** - Affiche les négociations IPsec de la phase 2.
- **debug crypto isakmp -** Affiche les négociations ISAKMP de la phase 1.

Commandes Spoke

- **debug crypto ipsec -** Affiche les négociations IPsec de la phase 2.
- **debug crypto isakmp -** Affiche les négociations ISAKMP de la phase 1.
- **debug crypto ipsec client ezvpn -** Affiche les débogages EzVPN.

Informations connexes

- Page d'assistance IPsec
- Cisco Easy VPN Remote
- Serveur Easy VPN
- Interface de tunnel virtuel IPsec
- Configuration de la sécurité des réseaux IPSec
- Configuration du protocole IKE (Internet Key Exchange)
- Support et documentation techniques - Cisco Systems