Migration from Legacy EzVPN to Enhanced EzVPN Configuration Example

Document ID: 118240

Contributed by Atri Basu, Cisco TAC Engineer.
Nov 20, 2014

Contents

Introduction
Prerequisites
- Requirements
- Components Used

Background Information
- Benefits

Configure
- Network Diagram
- Configuration Summary
  - Hub Configuration
  - Spoke 1 (Enhanced EzVPN) Configuration
  - Spoke 2 (Legacy EzVPN) Configuration

Verify
- Hub to Spoke 1 Tunnel
  - Phase 1
  - Phase 2
  - EIGRP
- Spoke 1
  - Phase 1
  - Phase 2
  - EZVPN
  - Routing − EIGRP
- Hub to Spoke 2 Tunnel
  - Phase 1
  - Phase 2
- Spoke 2
  - Phase 1
  - Phase 2
  - EZVPN
  - Routing − Static

Troubleshoot
- Hub Commands
- Spoke Commands

Related Information

Introduction

This document describes how to configure an Easy VPN (EzVPN) setup where Spoke 1 uses enhanced EzVPN in order to connect to the hub, while Spoke 2 uses legacy EzVPN in order to connect to the same hub. The hub is configured for enhanced EzVPN. The difference between enhanced EzVPN and legacy EzVPN is the use of dynamic Virtual Tunnel Interfaces (dVTIs) in the former and crypto maps in the latter. Cisco dVTI

is a method that can be used by customers with Cisco EzVPN for both the Server and Remote configuration. The tunnels provide an on−demand separate virtual access interface for each EzVPN connection. The configuration of the virtual access interfaces is cloned from a virtual template configuration, which includes the IPsec configuration and any Cisco IOS® Software feature configured on the virtual template interface, such as QoS, NetFlow, or access control lists (ACLs).

With IPsec dVTIs and Cisco EzVPN, users can provide highly secure connectivity for remote−access VPNs that can be combined with Cisco AVVID (Architecture for Voice, Video and Integrated Data) to deliver converged voice, video, and data over IP networks.

Prerequisites

Requirements

Cisco recommends that you have knowledge of EzVPN.

Components Used

The information in this document is based on Cisco IOS Version 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.

Background Information

The Cisco EzVPN with dVTI configuration provides a routable interface to selectively send traffic to different destinations, such as an EzVPN concentrator, a different site−to−site peer, or the Internet. IPsec dVTI configuration does not require a static mapping of IPsec sessions to a physical interface. This allows for the flexibility to send and receive encrypted traffic on any physical interface, such as in the case of multiple paths. Traffic is encrypted when it is forwarded from or to the tunnel interface.

The traffic is forwarded to or from the tunnel interface by virtue of the IP routing table. Routes are dynamically learned during Internet Key Exchange (IKE) Mode Configuration and inserted into the routing table that points to the dVTI. Dynamic IP routing can be used to propagate routes across the VPN. Using IP routing to forward the traffic to encryption simplifies the IPsec VPN configuration when compared with the use of ACLs with the crypto map in native IPsec configuration.

In releases earlier than Cisco IOS Release 12.4(2)T, at the tunnel−up/tunnel−down transition, attributes that were pushed during the mode configuration had to be parsed and applied. When such attributes resulted in the application of configurations on the interface, the existing configuration had to be overridden. With the dVTI Support feature, the tunnel−up configuration can be applied to separate interfaces, which makes it easier to support separate features at tunnel−up time. Features that are applied to the traffic (before encryption) that goes into the tunnel can be separate from the features that are applied to traffic that does not go through the tunnel (for example, split−tunnel traffic and traffic that leaves the device when the tunnel is not up).

When the EzVPN negotiation is successful, the line protocol state of the virtual access interface gets changed to up. When the EzVPN tunnel goes down because the security association expires or is deleted, the line protocol state of the virtual access interface changes to down.

The routing tables act as traffic selectors in an EzVPN virtual interface configuration−that is, the routes replace the access list on the crypto map. In a virtual interface configuration, EzVPN negotiates a single IPsec

security association if the EzVPN Server has been configured with an IPsec dVTI. This single security association is created regardless of the EzVPN mode that is configured.

After the security association is established, routes that point to the virtual access interface are added to direct traffic to the corporate network. EzVPN also adds a route to the VPN concentrator so that IPsec−encapsulated packets get routed to the corporate network. A default route that points to the virtual access interface is added in the case of a nonsplit mode. When the EzVPN server "pushes" the split tunnel, the split tunnel subnet becomes the destination to which the routes that point to the virtual access are added. In either case, if the peer (VPN concentrator) is not directly connected, EzVPN adds a route to the peer.

Note: Most routers that run the Cisco EzVPN Client software have a default route configured. The default route that is configured must have a metric value greater than 1 since EzVPN adds a default route that has a metric value of 1. The route points to the virtual access interface so that all traffic is directed to the corporate network when the concentrator does not "push" the split tunnel attribute.

QoS can be used to improve the performance of different applications across the network. In this configuration, traffic shaping is used between the two sites in order to limit the total amount of traffic that should be transmitted between the sites. Additionally, the QoS configuration can support any combination of QoS features offered in Cisco IOS Software, to support any of the voice, video, or data applications.

Note: The QoS configuration in this guide is for demonstration only. It is expected that the VTI scalability results will be similar to the Point−to−Point (P2P) Generic Routing Encapsulation (GRE) over IPsec. For scaling and performance considerations, contact your Cisco representative. For additional information, see Configuring a Virtual Tunnel Interface with IP Security.

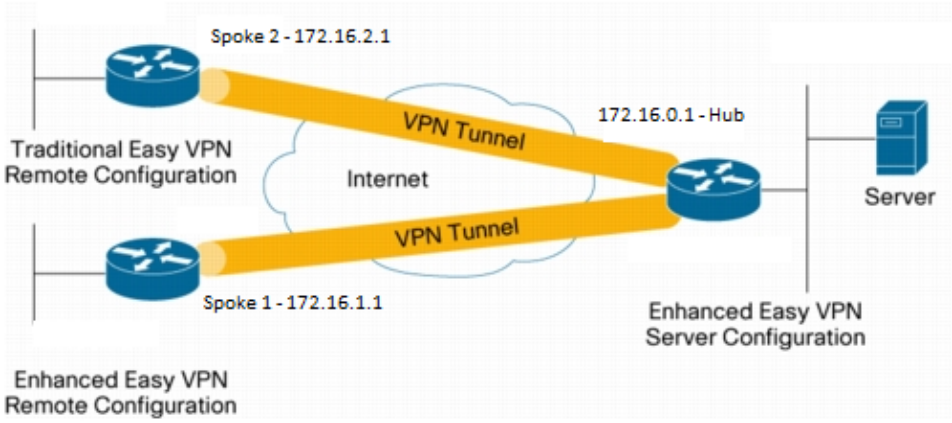
Benefits

- ***Simplifies Management***
  Customers can use the Cisco IOS virtual template to clone, on demand, new virtual access interfaces for IPsec which simplifies VPN configuration complexity and translates into reduced costs. In addition, existing management applications now can monitor separate interfaces for different sites for monitoring purposes.
- ***Provides a Routable Interface***
  Cisco IPsec VTIs can support all types of IP routing protocols. Customers can use these capabilities in order to connect larger office environments, such as branch offices.
- ***Improves Scaling***
  IPsec VTIs use single security associations per site, which cover different types of traffic, enabling improved scaling.
- ***Offers Flexibility in Defining Features***
  An IPsec VTI is an encapsulation within its own interface. This offers flexibility of defining features for clear−text traffic on IPsec VTIs and defines features for encrypted traffic on physical interfaces.

Configure

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram



Configuration Summary

Hub Configuration

```
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
```

Spoke 1 (Enhanced EzVPN) Configuration

```
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: The virtual template needs to be defined before the client configuration is entered. Without an existing virtual template of the same number, the router will not accept the the ***virtual−interface 1*** command.

Spoke 2 (Legacy EzVPN) Configuration

```
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
```

Verify

Use this section in order to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) supports certain ***show*** commands. Use the Output Interpreter Tool in order to view an analysis of ***show*** command output.

Hub to Spoke 1 Tunnel

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

The proxies here are for any/any which implies that any traffic which exits Virtual Access 1 will get encrypted and sent to 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 does not form an entry as it is not possible to form an Enhanced Interior Gateway Routing Protocol (EIGRP) peer without a routable interface. This is one of the advantages of the use of dVTIs on the spoke.

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
```

Routing – EIGRP

In Spoke 2 the proxies are such that any traffic that exits the virtual access interface will get encrypted. As long as there is a route that points out that interface for a network, the traffic will get encrypted:

```
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 to Spoke 2 Tunnel

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

A split-tunnel ACL under the client configuration on the hub is not used in this example. Therefore the proxies that are formed on the spoke are for any EzVPN "inside" network on the spoke to any network. Basically, on the hub, any traffic destined to one of the "inside" networks on the spoke will get encrypted and sent to 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
```

Routing − Static

Unlike Spoke 1, Spoke 2 has to have static routes or use Reverse Route Injection (RRI) in order to inject routes to tell it what traffic should get encrypted and what should not. In this example, only traffic sourced from Loopback 0 gets encrypted as per the proxies and the routing.

```
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

This section provides information you can use in order to troubleshoot your configuration.

Tip: Very often in EzVPN the tunnels do not come up after configuration changes. Clearing phase 1 and phase 2 will not bring the tunnels up in this case. In most cases, enter the ***clear crypto ipsec client ezvpn*** **<*group-name*>** command in the spoke in order to bring up the tunnel.

Note: Refer to Important Information on Debug Commands before you use ***debug*** commands.

Hub Commands

- ***debug crypto ipsec*** − Displays the IPsec negotiations of Phase 2.
- ***debug crypto isakmp*** − Displays the ISAKMP negotiations of Phase 1.

Spoke Commands

- ***debug crypto ipsec*** − Displays the IPsec negotiations of Phase 2.
- ***debug crypto isakmp*** − Displays the ISAKMP negotiations of Phase 1.
- ***debug crypto ipsec client ezvpn*** − Displays the EzVPN debugs.

Related Information

- ***IPsec Support Page***
- ***Cisco Easy VPN Remote***
- ***Easy VPN Server***
- ***IPsec Virtual Tunnel Interface***
- ***Configuring IPsec Network Security***
- ***Configuring Internet Key Exchange Security Protocol***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Nov 20, 2014 Document ID: 118240