Миграция от устаревшего EzVPN до расширенного примера конфигурации EzVPN

Содержание

Введение

Этот документ описывает, как настроить Легкую VPN (EzVPN) настройка, где Луч, 1 использование улучшило EzVPN для соединения с концентратором, в то время как Луч 2 устаревших EzVPN использования для соединения с тем же концентратором. Концентратор настроен для расширенного EzVPN. Различием между расширенным EzVPN и устаревшим EzVPN является использование динамических интерфейсов виртуальных туннелей (dVTIs) в прежнем и криптокартах в последнем. Cisco dVTI является методом, который может использоваться клиентами с EzVPN Cisco и для Сервера и для Удаленной конфигурации. Туннели предоставляют по требованию отдельный интерфейс виртуального доступа для каждого соединения EzVPN. Конфигурация интерфейсов виртуального доступа клонирована от настройки виртуального шаблона, которая включает Конфигурацию IPSec и любую функцию программного обеспечения Cisco IOS, настроенную на интерфейсе виртуального шаблона, таком как QoS, NetFlow или списки контроля доступа (ACL).

С IPsec dVTIs и EzVPN Cisco, пользователи могут предоставить очень безопасное подключение для VPN удаленного доступа, которые могут быть объединены с CISCO AVVID (Architecture for Voice, Video and Integrated Data) для отправки объединенного голоса, видео и данных по IP - сетям.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с EzVPN.

Используемые компоненты

Сведения в этом документе основываются на версии Cisco IOS 15.4 (2) T.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

EzVPN Cisco с dVTI конфигурацией предоставляет маршрутизируемый интерфейс, чтобы выборочно передать трафик другим назначениям, таким как концентратор EzVPN, другой узел от узла к узлу или Интернет. Конфигурация IPsec dVTI не требует статического отображения Сеансов IPSec к физическому интерфейсу. Это обеспечивает гибкость, чтобы передать и получить зашифрованный поток данных на любом физическом интерфейсе, такой как в случае разнообразных путей. Трафик зашифрован, когда он передан от или до туннельного интерфейса.

Трафик передан к или от туннельного интерфейса на основании таблицы IP-

маршрутизации. Маршруты динамично изучены во время Конфигурации режима Протокола IKE и вставлены в таблицу маршрутизации, которая указывает к dVTI. Dynamic IP Routing может использоваться для распространения маршрутов через VPN. Использование IP-маршрутизации для передачи трафика к шифрованию упрощает конфигурацию IPSec VPN при сравнении с использованием ACL с криптокартой в собственной Конфигурации IPSec.

В версиях ранее, чем Cisco IOS Release 12.4 (2) T, при tunnel-up/tunnel-down переходе, атрибуты, которые были выдвинуты во время конфигурации режима, должны были быть проанализированы и применены. Когда такие атрибуты привели к приложению конфигураций на интерфейсе, существующая конфигурация должна была быть отвергнута. С dVTI Функцией поддержки туннельная конфигурация может быть применена к отдельным интерфейсам, который упрощает поддерживать отдельные характеристики в туннельное время. Функции, которые применены к трафику (перед шифрованием), который входит в туннель, могут быть отдельными от функций, которые применены для трафика, который не проходит туннель (например, трафик разделения туннеля и трафик, который оставляет устройство, когда туннель не подключен).

Когда согласование EzVPN успешно, состояние протокола линии связи интерфейса виртуального доступа изменено на. Когда туннель EzVPN выключается, потому что сопоставление безопасности истекает или удалено, состояние протокола линии связи интерфейса виртуального доступа изменяется на вниз.

Действие таблиц маршрутизации как селекторы трафика в конфигурации виртуального интерфейса EzVPN - т.е. маршруты заменяют список доступа на криптокарте. Если сервер EzVPN был настроен с IPsec dVTI, в конфигурации виртуального интерфейса EzVPN выполняет согласование об одиночном Сопоставлении безопасности IPSec. Это одиночное сопоставление безопасности создано независимо от режима EzVPN, который настроен.

После того, как сопоставление безопасности установлено, маршруты, которые указывают к интерфейсу виртуального доступа, добавлены для направления трафик к корпоративной сети. EzVPN также добавляет маршрут к концентратору VPN так, чтобы инкапсулированные пакеты Ipsec маршрутизировались к корпоративной сети. В случае работы в неразделенном режиме добавляется маршрут по умолчанию, указывающий на интерфейс виртуального доступа. Когда сервер EzVPN "выдвигает" разделение туннеля, подсеть разделения туннеля становится назначением, к который маршруты, которые указывают к виртуальному доступу, добавлены. В любом случае, если узел (концентратор VPN) непосредственно не связан, EzVPN добавляет маршрут к узлу.

> **Примечание:** Большинству маршрутизаторов, которые выполняют программное обеспечение Cisco EzVPN Client, настроили маршрут по умолчанию. Маршрут по умолчанию, который настроен, должен иметь значение метрики, больше, чем 1, так как EzVPN добавляет маршрут по умолчанию, который имеет значение метрики 1. Точки маршрута к интерфейсу виртуального доступа так, чтобы весь трафик был направлен к корпоративной сети, когда концентратор не "выдвигает" атрибут раздельного туннелирования.

QoS может использоваться для улучшения производительности других приложений по сети. В этой конфигурации формирование трафика используется между двумя узлами для ограничения общего объема трафика, который должен быть передан между узлами. Кроме того, конфигурация QoS может поддержать любую комбинацию Характеристик QoS, предлагаемых в программном обеспечении Cisco IOS, для поддержки любого голоса, видео или приложений для данных.

Примечание: Конфигурация QoS в этом руководстве для демонстрации только. Ожидается, что результаты масштабируемости VTI будут подобны точка-точка (P2P) Универсальная инкапсуляция маршрутизации (GRE) по IPsec. Для масштабирования и соображений производительности, свяжитесь со своим представителем Cisco. Для дополнительных сведений посмотрите Настройку Виртуальный туннельный интерфейс с IP-безопасностью.

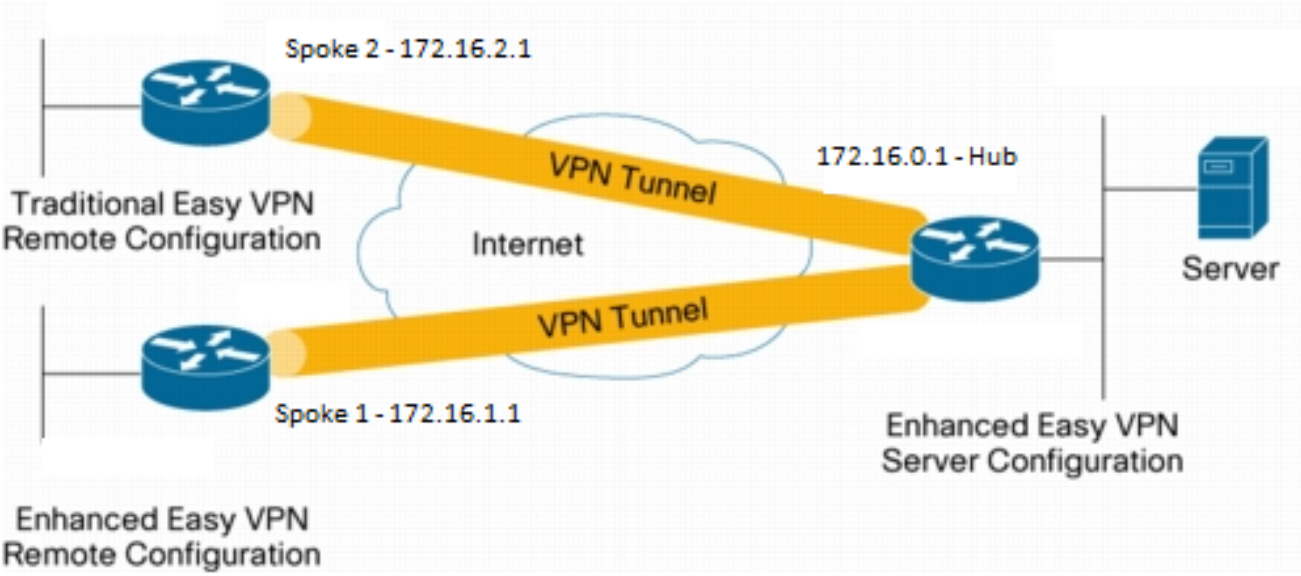
Преимущества

- **Упрощает менеджмент**
  Клиенты могут использовать виртуальный шаблон Cisco IOS для клонирования, по требованию, новых интерфейсов виртуального доступа для IPsec, который упрощает сложность конфигурации VPN и преобразовывает в уменьшенные затраты. Кроме того, существующие приложения управления сетью теперь могут контролировать отдельные интерфейсы для других узлов для мониторинга целей.
- **Предоставляет маршрутизируемый интерфейс**
  Cisco IPSec VTIs может поддержать все типы протоколов IP-маршрутизации. Клиенты могут использовать эти возможности для соединения больших офисных сред, таких как филиалы компании.
- **Улучшает масштабирование**
  VTIs IPsec используют одиночные сопоставления безопасности на узел, которые покрывают различные типы трафика, включая улучшенное масштабирование.
- **Гибкость предложений в определении функций**
  IPsec VTI является инкапсуляцией в своем собственном интерфейсе. Это предлагает гибкость определения функций трафика открытого текста на IPsec VTIs и определяет функции зашифрованного потока данных на физических интерфейсах.

Настройка

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети



Сведения о конфигурации

Конфигурация концентратора

```
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
```

Говорил 1 (расширенный EzVPN) конфигурация

```
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
```

Внимание. : Виртуальный шаблон должен быть определен, прежде чем конфигурация клиента введена. Без существующего виртуального шаблона того же номера маршрутизатор не примет **команду virtual-interface 1**.

Говорил 2 (устаревший EzVPN) конфигурация

```
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
```

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Средство интерпретации выходных данных (только зарегистрированные клиенты)

поддерживает некоторые команды show. Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.

Концентратор к лучу 1 туннель

Этап 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
```

Этап 2

Прокси здесь для любого/любого, который подразумевает, что любой трафик, который выходит из Виртуального доступа 1, будет зашифрован и передал к 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
```

Примечание: Луч 2 не формирует запись, поскольку не возможно сформировать узел Протокола EIGRP без маршрутизируемого интерфейса. Это - одно из преимуществ использования dVTIs на луче.

Луч 1

Этап 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
```

Этап 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
```

Маршрутизация - EIGRP

В Луче 2 прокси таковы, что будет зашифрован любой трафик, который выходит из интерфейса виртуального доступа. Пока существует маршрут, который указывает, что интерфейс для сети, будет зашифрован трафик:

```
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#
```

Концентратор к лучу 2 туннеля

Этап 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
```

Этап 2

ACL разделения туннеля под конфигурацией клиента на концентраторе не используется в данном примере. Поэтому прокси, которые сформированы о луче, для любого EzVPN "в" сети на луче к любой сети. В основном, на концентраторе, любой трафик, предназначенный к одной из "внутренних" сетей на луче, будет зашифрован и передал к 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:
```

Луч 2

Этап 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
```

Этап 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
```

Маршрутизация - статичный

В отличие от Луча 1, Луч 2 должен иметь статические маршруты или использовать Включение ввода обратной маршрутизации (RRI) для введения маршрутов для сообщения его, какой трафик должен быть зашифрован и что не должно. В данном примере только трафик, полученный от Loopback 0, зашифрован согласно прокси и маршрутизации.

```
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
```

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

> **Совет:** Очень часто в EzVPN туннели не подходят после изменений конфигурации. Очистка фазы 1 и фазы 2 не переведет туннели в рабочее состояние в этом случае. В большинстве случаев введите команду **<group-name> clear crypto ipsec client ezvpn** в луч для внедрения туннеля.

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Команды концентратора

- **debug crypto ipsec – отображает согласования IPSec на Этапе 2.**
- **debug crypto isakmp – отображает согласования ISAKMP на 1-м этапе.**

Лучевые команды

- **debug crypto ipsec – отображает согласования IPSec на Этапе 2.**
- **debug crypto isakmp – отображает согласования ISAKMP на 1-м этапе.**
- **debug crypto ipsec client ezvpn -** Отображает отладки EzVPN.

Дополнительные сведения

- Страница поддержки IPSec
- Функция Cisco Easy VPN Remote
- Сервер Easy VPN
- Интерфейс виртуальных туннелей IPsec
- Настройка параметров сетевой безопасности IPSec Network Security
- Настройка протокола защищенного обмена ключами IKE
- Cisco Systems – техническая поддержка и документация