# レガシー EzVPN から強化された EzVPN への移行の設定例

## 内容

# 概要

このドキュメントでは、スポーク 1 が拡張 EzVPN を使用してハブに接続し、スポーク 2 がレガシー EzVPN を使用して同じハブに接続する Easy VPN（EzVPN）セットアップを設定する方法について説明します。ハブは、拡張 EzVPN 用として設定します。 拡張 EzVPN とレガシー EZVPN の違いは、前者がダイナミック仮想トンネル インターフェイス（dVTI）を使用するのに対して、後者がクリプト マップを使用することです。Cisco dVTI は、Cisco EzVPN のユーザがサーバとリモートの両方の設定のために使用できる方法です。トンネルにより、各 EzVPN 接続に対して個別の仮想アクセス インターフェイスがオンデマンドで提供されます。仮想アクセス インターフェイス設定は、仮想テンプレート設定からコピーされます。このコピーには、IPsec 設定と、QoS、NetFlow、アクセス コントロール リスト（ACL）といった、仮想テンプレート インターフェイス上で設定されたすべての Cisco IOS® ソフトウェア機能が含まれています。

IPsec dVTI を使用すれば、リモート アクセス VPN 用のセキュリティ保護が強化された接続を作成できます。また、Cisco AVVID（Architecture for Voice, Video, and Integrated Data）と組み合わせて、IP ネットワーク経由で集約された音声、ビデオ、およびデータを転送できます。

# 前提条件

## 要件

EzVPN に関する知識があることが推奨されます。

## 使用するコンポーネント

このドキュメントの情報は、Cisco IOS バージョン 15.4(2)T に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

# 背景説明

dVTI 設定を使用する Cisco EzVPN により、ルーティング可能なインターフェイスから、EzVPN コンセントレータ、別のサイト間ピア、インターネットなどのさまざまな接続先にトラフィックを選択的に送信できます。IPsec dVTI 設定では、IPsec セッションの物理インターフェイスへのスタティック マッピングは必要ありません。そのため、複数パスの場合のように、物理インターフェイス上における暗号化トラフィックの送受信の柔軟性が高まります。トラフィックは、トンネル インターフェイスに、またはトンネル インターフェイスから転送されるときに暗号化されます。

トラフィックは、IP ルーティング テーブルによってトンネル インターフェイスに、またはトンネル インターフェイスから転送されます。ルートは、インターネット キー交換（IKE）モード設定中に動的に学習され、dVTI を指し示すルーティング テーブルに挿入されます。ダイナミック IP ルーティングを使用すると、VPN 全体にルートを伝播できます。IP ルーティングを使用して

トラフィックを暗号化すると、ネイティブの IPsec 設定でクリプト マップと ACL を使用する必要がなくなるため、IPsec VPN の設定が簡単になります。

Cisco IOS Release 12.4(2)T より前のリリースでは、トンネルの状態がアップ状態からダウン状態またはその逆に遷移した時点で、モード設定中にプッシュされた属性を解析し、それを適用する必要がありました。また、これらの属性により設定内容がインターフェイスに適用されると、既存の設定内容は上書きされていました。dVTI インターフェイスのサポート機能を使用すると、トンネルがアップ状態での設定を個々のインターフェイスに適用できるため、トンネルのアップ時に個々の機能を別々に適用することが容易になります。トンネルへ送出されるトラフィックに（暗号化前に）適用される機能と、トンネルを経由しないトラフィック（スプリット トンネルのトラフィックや、トンネルがダウン状態のときにデバイスから送出されたトラフィックなど）に適用される機能は区別できます。

EzVPN のネゴシエーションが完了すると、仮想アクセス インターフェイスの回線プロトコルは、アップ状態に変更されます。セキュリティ アソシエーションの失効または削除により EzVPN トンネルがダウンすると、仮想アクセス インターフェイスの回線プロトコルは、ダウン状態に変更されます。

ルーティング テーブルは、EzVPN の仮想インターフェイス設定においてトラフィック セレクタとして機能します。つまり、クリプト マップ上のアクセス リストが持つ役割をルートが代行します。仮想インターフェイスの設定では、EzVPN サーバにダイナミック仮想 IPsec dVTI が設定されている場合、EzVPN は 1 つの IPsec セキュリティ アソシエーションとネゴシエーションします。この唯一のセキュリティ アソシエーションは、設定されている EzVPN モードにかかわらず作成されます。

このセキュリティ アソシエーションが作成されると、仮想アクセス インターフェイスへのルートが追加され、トラフィックが社内ネットワークに送信されます。また、EzVPN では、VPN コンセントレータへのルートも追加されます。それによって、IPsec カプセル化されたパケットが、社内ネットワークへルーティングされます。スプリット モード以外のモードでは、仮想アクセス インターフェイスへのデフォルト ルートが追加されます。EzVPN サーバによりスプリット トンネルが「プッシュ」された場合は、そのスプリット トンネルのサブネットに、仮想アクセス インターフェイスへのルートが追加されます。どちらの場合も、ピア（VPN コンセントレータ）が直接接続されていない場合、EzVPN はそのピアにルートを追加します。

> **注**：Cisco EzVPN Client ソフトウェアを搭載した大半のルータには、デフォルトのルートが設定されています。EzVPNはメトリック値が1のデフォルトルートを追加するため、設定するデフォルトルートは1より大きいメトリック値を持つ必要があります。このルートは仮想アクセスインターフェイスを指し、コンセントレータがスプリットトンネル属性を「プッシュ」しない場合に企業ネットワークに宛です。

QoS を使用して、ネットワーク上の各種アプリケーションのパフォーマンスを向上させることが可能です。この設定では、トラフィック シェーピングが 2 つのサイト間で使用され、これらのサイト間で送信される合計トラフィック量を制限します。さらに QoS 設定は、Cisco IOS ソフトウェアで提供される QoS 機能のあらゆる組み合わせをサポートしており、音声、ビデオ、またはデータ アプリケーションをサポートできます。

> **注**：このガイドの QoS 設定はデモ用です。VTI のスケーラビリティの結果は、ポイントツーポイント（P2P）の Generic Routing Encapsulation（GRE）over IPsec とほぼ同じであることが予想されます。スケーリングとパフォーマンスの考慮事項については、シスコの代理店にお問い合わせください。詳細については、IP セキュリティを使用した仮想トンネル インターフェイスの設定を参照してください。

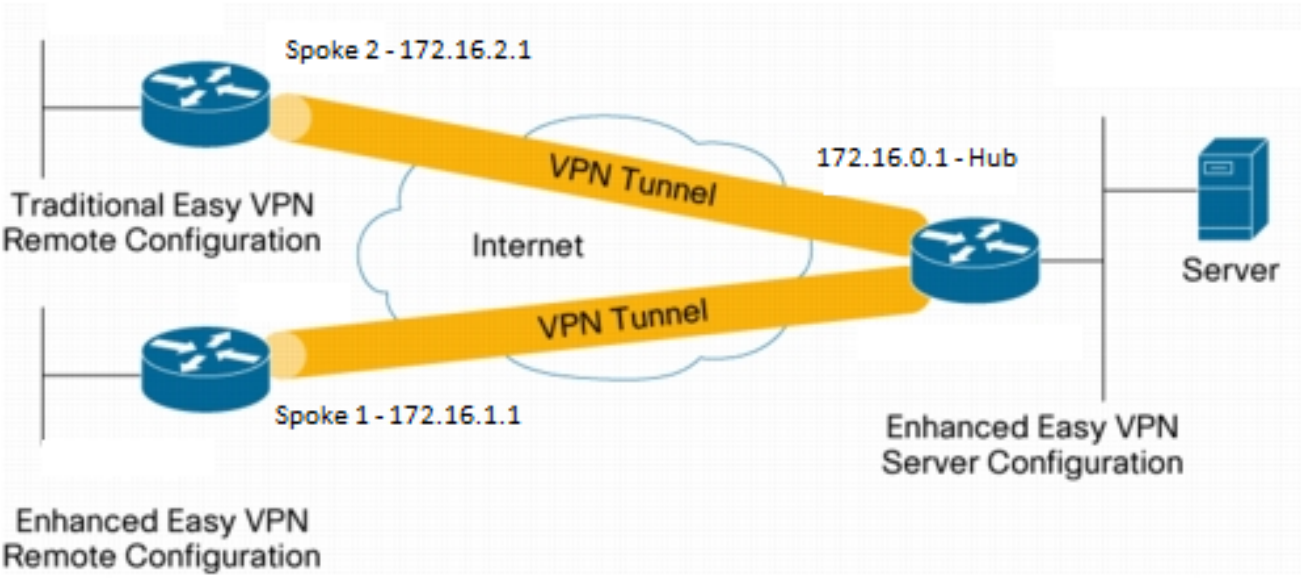
### 利点

- **管理の簡素化**
  Cisco IOS 仮想テンプレートを使用すると、IPSec 用の新しい仮想アクセス インターフェイスをオンデマンドで複製できるため、VPN 設定の複雑さを簡素化してコストを削減できます。また、既存の管理アプリケーションで異なるサイトの個別のインターフェイスをモニタできるようになります。
- **ルーティング可能なインターフェイスの提供**
  Cisco IPsec VTI は、あらゆる種類の IP ルーティング プロトコルをサポートできます。これらの機能を使用することで、ブランチ オフィスなどの大規模なオフィス環境を接続できます。
- **スケーリングの向上**
  IPsec VTI は、さまざまな種類のトラフィックを対象とする単一のセキュリティ アソシエーションをサイトごとに使用します。このため、スケーリングの向上を実現できます。
- **機能の柔軟な定義を実現**
  IPsec VTI は、その独自のインターフェイスにカプセル化されています。これにより、IPsec VTI のクリア テキスト トラフィック用の機能を定義する一方、物理インターフェイスの暗号化トラフィック用の機能を定義するという柔軟性が実現されます。

## 設定

> **注**：このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

### ネットワーク図



## 設定の概要

### ハブ設定

```
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
```

### スポーク 1 ( 拡張 EzVPN ) の設定

```
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
```

> **注意**：クライアント設定を入力する前に仮想テンプレートを定義する必要があります。同じ番号の既存の仮想テンプレートが存在しない場合、ルータは **virtual-interface 1 コマンドを受け付けません。**

### スポーク 2 ( レガシー EzVPN ) の設定

```
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
```

# 確認

ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール ( 登録ユーザ専用 ) は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

## ハブからスポーク 1 へのトンネル

### フェーズ 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
```

## フェーズ 2

これらのプロキシにより、仮想アクセス 1 を出るすべてのトラフィックが暗号化されて 172.16.1.1 に送信されます。

```
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
```

**注：**ルーティング可能なインターフェイスなしで Enhanced Interior Gateway Routing Protocol（EIGRP）ピアを形成できないため、スポーク 2 はエントリを形成しません。これは、スポークで dVTI を使用するメリットの 1 つです。

## スポーク 1

### フェーズ 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
```

### フェーズ 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
```

### ルーティング：EIGRP

スポーク 2 では、これのプロキシにより、仮想アクセス インターフェイスを出るすべてのトラフィックが暗号化されます。ネットワーク用のそのインターフェイスへのルートが存在する限り、トラフィックは暗号化されます。

```
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#
```

## ハブからスポーク 2 へのトンネル

### フェーズ 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
```

## フェーズ 2

ハブのクライアント設定にあるスプリット トンネル ACL は、この例では使用しません。そのため、スポークで構築されるプロキシは、そのスポークの任意の EzVPN「内部」ネットワークから任意のネットワーク用です。基本的に、ハブでは、スポークの「内部」ネットワークの 1 つを宛先とするすべてのトラフィックが暗号化されて 172.16.2.1 に送信されます。

```
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:
```

## スポーク 2

### フェーズ 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
```

### フェーズ 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
```

## ルーティング：スタティック

スポーク 1 とは異なり、スポーク 2 はスタティック ルートを持つか、逆ルート注入（RRI）を使用してルートを注入して、暗号化するトラフィックを指定する必要があります。この例では、ループバック 0 からのトラフィックのみがプロキシとルーティングに基づいて暗号化されます。

```
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
```

# トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

> **ヒント**：多くの場合、EzVPN ではトンネルは設定の変更後にアップ状態になりません。この場合、フェーズ 1 とフェーズ 2 をクリアしても、トンネルはアップ状態になりません。ほとんどの場合、トンネルをアップ状態にするには、スポークで **clear crypto ipsec client ezvpn <group-name> コマンドを入力します。**

> **注：debug コマンドを使用する前に、「**デバッグ コマンドの重要な情報」を参照してください。

## ハブ コマンド

- **debug crypto ipsec：フェーズ 2 の IPsec ネゴシエーションを表示します。**
- **debug crypto isakmp：フェーズ 1 の ISAKMP ネゴシエーションを表示します。**

## スポーク コマンド

- debug crypto ipsec：フェーズ 2 の IPsec ネゴシエーションを表示します。
- debug crypto isakmp：フェーズ 1 の ISAKMP ネゴシエーションを表示します。
- debug crypto ipsec client ezvpn：EzVPN デバッグを表示します。

## 関連情報

- IPSec サポート ページ
- Cisco Easy VPN Remote
- Easy VPN Server
- IPsec 仮想トンネル インターフェイス
- IPsec ネットワーク セキュリティの設定
- Internet Key Exchange セキュリティ プロトコルの設定
- テクニカル サポートとドキュメント – Cisco Systems