Easy VPN の設定例

このマニュアルでは、Cisco 1800 シリーズ、Cisco 2800 シリーズ、および Cisco 3800 シリーズのルータを使用した Easy VPN（EzVPN）の設定例を示します。

目次

概要

このマニュアルでは、次の特徴を持つ Easy VPN（EzVPN）の設定例を示します。

- 2 つのクライアント ブランチ サイトと本社の間のすべてのトラフィックは、IP Security（IPSec）暗号化トンネルの Virtual Private Network（VPN; 仮想私設網）を介して送受信されます。
- 使用されている技術には Internet Key Exchange（IKE; インターネット キー エクスチェンジ）Dead Peer Detection（DPD）、スプリット トンネリング、グループ ポリシーなどがあり、これらをサーバ上で Domain Name Server（DNS; ドメイン名サーバ）情報、Windows Information Name Service（WINS）情報、ドメイン名、およびクライアントの IP アドレス プールを使用して採用しています。
- 本社では、EzVPN コンセントレータ、および ATM インターフェイスを搭載した Cisco 3800 シリーズ ルータを使用しています。
- 片方のブランチでは、Cisco 2800 シリーズ ルータを使用し、シリアル インターフェイスを搭載したネットワーク モードの EzVPN クライアントを採用しています。もう一方のブランチでは、Cisco 1800 シリーズ ルータと、SHDSL インターフェイスを搭載したクライアント モードの EzVPN を使用しています。

- さまざまな **show** コマンドを使用して、EzVPN コンセントレータでの Internet Security Association Key Management Protocol（ISAKMP）や IPSec セキュリティ アソシエーション（SA）の設定を表示したり、クライアント上の IPSec クライアント EzVPN のステータスを表示できます。

用語集

ATM：Asynchronous Transfer Mode（非同期転送モード）の略。データを 53 バイトのセル単位に整理し、それらをデジタル信号で送信する接続スイッチング プロトコルです。単一のメッセージ内で、各セルは、他のセルの送信または着信に対して非同期的に処理されます（これが名前の由来です）。また、セルは多重化方式で送信される前にキューに格納されます。ATM は、音声、ビデオ、データなど、さまざまなサービスで使用できます。

DNS：Domain Name Server（ドメイン名サーバ）の略。名前とインターネット プロトコル（IP）アドレス、およびアドレスと名前の対応付けを行います。DNS は、ドメイン名と IP アドレスのマッピング リストを格納します。

DPD：Dead Peer Detection の略。クライアント キープアライブ機能を実装したもので、IPSec トンネルの反対側の VPN デバイスの可用性をチェックします。

IKE：Internet Key Exchange（インターネット キー エクスチェンジ）の略。IKE は、共有セキュリティ ポリシーを確立し、キーを必要とするサービス（IPSec など）のキーを認証します。IPSec トラフィックが通過する前に、各ルータ、ファイアウォール、およびホストはそのピアの ID を検証する必要があります。これは、事前共有キーを両側のホストに手動で入力するか、認証局（CA）のサービスによって行われます。

IPSec：IP Security（IP セキュリティ）の略。参加ピア間でのデータの機密性、整合性、および認証を提供するオープン スタンダードの枠組みです。IPSec は、このようなセキュリティ サービスを IP レイヤで提供します。IPSec は IKE を使用して、プロトコルやアルゴリズムのネゴシエーションをローカル ポリシーに基づいて処理し、IPSec で使用される暗号化キーや認証キーを生成します。IPSec では、一対のホスト間、一対のセキュリティ ゲートウェイ間、または一対のセキュリティ ゲートウェイとホストの間で 1 つ以上のデータ フローを保護できます。

ISAKMP：Internet Security Association Key Management Protocol の略。鍵交換による暗号化と認証のためのプロトコルです。ISAKMP では、VPN 接続された 2 つのピア間に少なくとも一組のメッセージが交換されないと、安全なリンクを確立できません。

NETBEUI：NetBIOS Extended User Interface の略。Microsoft ベースのネットワークに関連する転送プロトコル。TCP/IP と違い、NETBEUI は、ルーティング可能なネットワーク プロトコルではありません。

NetBIOS：Network Basic Input/Output System の略。1980 年代に登場したピアツーピアの低レベル ネットワーキング プロトコルです。NetBIOS は、ネットワーク オペレーティング システムをネットワーク ハードウェアとリンクします。NetBIOS はルーティング可能ではないので、ルータを通過させるには TCP/IP でカプセル化する必要があります。

SA：Security Association（セキュリティ アソシエーション）の略。IPSec によってネゴシエーションされる一方向チャネルです。双方向通信には一組の SA が必要です。SA は、セッション キーと初期ベクトルのインデックス付けに使用されます。

SHDSL：Symmetrical High-Speed Digital Subscriber Line の略。どちらの送信方向でも同じ速度（192 kbps ～ 2.3 Mbps）で動作する DSL の実装です。

WINS：Windows Internet Naming Service の略。ホスト名を IP アドレスに変換する Microsoft ベースのネットワークのサービスです。NETBEUI プロトコルを使用しており、NetBIOS とも互換性があります。

はじめに

次に、この設定例を使用する際の要件を示します。

表記法

表記法の詳細については、『*Cisco Technical Tips Conventions*』を参照してください。

使用されるコンポーネント

このマニュアルの情報は、次のソフトウェアおよびハードウェアのバージョンに基づいています。

- 本社の Cisco 3845 ルータ：Cisco CallManager クラスタ、インターネットへの ATM アクセスあり
- ブランチ 1 の Cisco 1841 ルータ：WIC-1SHDSL インターフェイス カード搭載、インターネットへの DSL アクセスあり
- ブランチ 2 の Cisco 2811 ルータ：インターネットへのシリアル インターフェイス接続あり
- Cisco 1800 シリーズ ルータおよび Cisco 2800 シリーズ ルータ：Cisco IOS Release 12.3(8)T4
- Cisco 3800 シリーズ ルータ：Cisco IOS Release 12.3(11)T
- Advanced Enterprise Services フィーチャ セット

このマニュアルの情報には、特定のラボのセットアップと環境で使用されたデバイスの結果が反映されています。このマニュアルで使用されるデバイスはすべて、初期設定（デフォルト）の状態から作業が開始されています。ライブ ネットワークライブ ネットワークで操作している場合は、使用前に、コマンドが及ぼす潜在的な影響を事前に十分に理解しておく必要があります。

（注） Cisco 2811 ルータの IPSec にステートフル フェールオーバーを設定する場合、AIM-VPN モジュールが設置されていないと、次のメッセージが表示されることがあります。

```
%crypto_ha_ipsec-4-crypto_ha_not_supported_by_hw 2811
```

AIM-VPN モジュールが Cisco 2811 ルータに設置されると、このエラー メッセージは表示されなくなります。

関連製品

この設定は、次のハードウェアにも使用できます。

- Cisco 1800 シリーズ ルータ
- Cisco 2800 シリーズ ルータ
- Cisco 3800 シリーズ ルータ

設定

ここでは、このマニュアルで説明する機能を設定するための情報を示します。

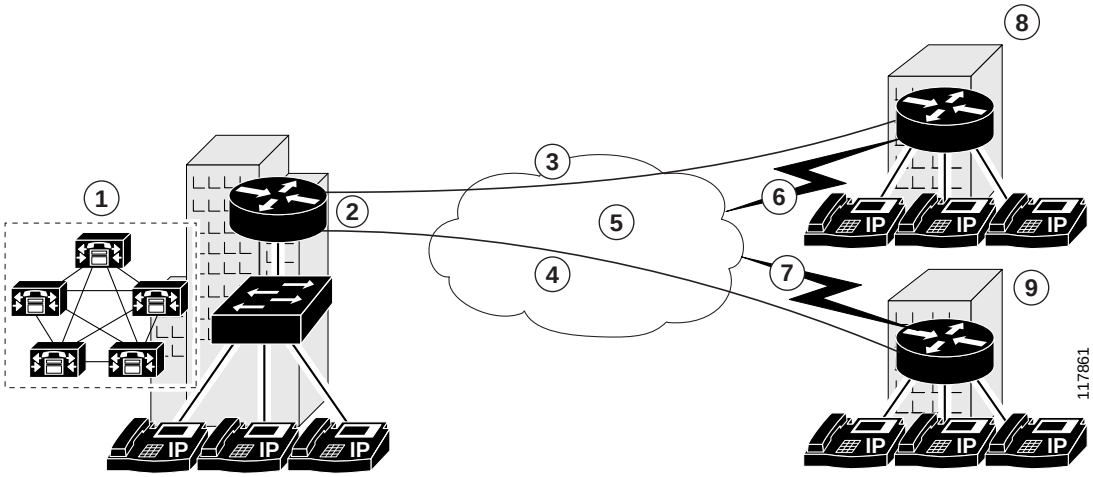
（注） このマニュアルで使用されるコマンドに関する追加情報については、Cisco IOS Command Lookup Tool を使用してください。アクセスするには、Cisco.com のアカウントが必要です。アカウントをお持ちでない場合や、ユーザ名やパスワードを忘れた場合は、ログイン ダイアログボックスで [Cancel] をクリックし、表示される説明に従ってください。

設定のヒント

- クリプト マップを適用する前に、トンネルが機能していることを確認します。
- トンネル インターフェイスと物理インターフェイスの両方に IPSec クリプト マップを適用します。

ネットワーク図

このマニュアルでは、次の図に示すネットワーク セットアップを使用します。



次に、図内に番号で示す要素と意味を説明します。

1. 本社の場所	6. ブランチ 1 のルータからインターネットへの DSL リンク
2. 本社のルータからインターネットへの ATM リンク	7. ブランチ 2 のルータからインターネットへのシリアル リンク
3. インターネット経由によるブランチ 1 への VPN トンネル	8. ブランチ 1 の場所
4. インターネット経由によるブランチ 2 への VPN トンネル	9. ブランチ 2 の場所
5. インターネット（クラウドで表現）	

本社の場所（番号 1）は、次の特徴を持つ Cisco 3845 ルータを使用しています。

- EzVPN サーバ
- インターネットへの ATM アクセス
- Cisco CallManager クラスタで稼動
- パブリック IP アドレス：10.32.152.26
- プライベート IP アドレス プール：192.168.1.0/24

ブランチ 1 の場所（番号 8）は、次の特徴を持つ Cisco 1841 ルータを使用しています。

- クライアント モードを使用する EzVPN クライアント

- インターネットへの DSL アクセス
- WIC-1SHDSL インターフェイス カードを搭載
- パブリック IP アドレス：10.32.152.46
- プライベート IP アドレス プール：192.168.3.0/24

ブランチ 2 の場所（番号 9）は、次の特徴を持つ Cisco 2811 ルータを使用しています。

- ネットワーク モードを使用する EzVPN クライアント
- インターネットへのシリアル アクセス
- パブリック IP アドレス：10.32.150.46
- プライベート IP アドレス プール：192.168.3.1/24

設定

この例では次の設定を使用しています。

- 「本社の設定（Cisco 3845 ルータ）」（P.5）
- 「ブランチ 1 のルータ設定（Cisco 1841 ルータ）」（P.8）
- 「ブランチ 2 のルータ設定（Cisco 2811 ルータ）」（P.10）

本社の設定（Cisco 3845 ルータ）

```
EzVPN-Hub# show running-config

Building configuration...
Current configuration : 6824 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname EzVPN-Hub
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$t8oN$hXnGodPh8ZM/ka6k/9aO51
!
username admin secret 5 $1$cfjP$kKpB7e3pfKXfpK0RIqX/E.
username ezvpn-spoke2 secret 5 $1$vrSS$AhSPxEUnPOsSpJkGdzjXg/
username ezvpn-spoke1 secret 5 $1$VK0p$4D0YXNOtC6K7MR4/vinUL.

mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
aaa new-model
!
!
aaa authentication login USER_AAA local
aaa authentication login USERLIST local
aaa authorization network GROUP_AAA local
aaa session-id common
```

```
ip subnet-zero
!
ip cef
no ip domain lookup
ip domain name cisco.com
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
voice-card 0
 no dspfarm
!
!--- IKE configuration
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp keepalive 90 12
!
crypto isakmp client configuration group VPN1
 acl SPLIT_T
 ip access-list extended SPLIT_T
 permit ip 192.168.0.0 0.0.255.255 any
 key cisco123
 dns 192.168.168.183 192.168.226.120
 wins 192.168.179.89 192.168.2.87
 domain cisco.com
 pool VPN-POOL
 save-password
!
!--- IPSec configuration
!
crypto ipsec transform-set TRANSFORM-1 esp-3des esp-md5-hmac
!
crypto dynamic-map INT_MAP 1
 set security-association lifetime kilobytes 530000000
 set security-association lifetime seconds 14400
 set transform-set TRANSFORM-1
!
!
crypto map INT_MAP client authentication list USER_AAA
crypto map INT_MAP isakmp authorization list GROUP_AAA
crypto map INT_MAP client configuration address respond
crypto map INT_MAP 30000 ipsec-isakmp dynamic INT_MAP
!
!
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
```

```
interface ATM0/0/0
 description === public interface ===
 ip address 10.32.152.26 255.255.255.252
 ip pim sparse-dense-mode
 ip ospf network point-to-point
 no atm ilmi-keepalive
 pvc 10/100
  protocol ip 10.32.152.25 broadcast
 !
 crypto map INT_MAP
!
interface FastEthernet4/0
 no ip address
 shutdown
!
interface FastEthernet4/1
 switchport access vlan 10
 no ip address
!
interface FastEthernet4/2
 switchport access vlan 10
 no ip address
!
interface FastEthernet4/3
 switchport access vlan 10
 no ip address
!
interface FastEthernet4/4
 switchport access vlan 10
 no ip address
!
interface FastEthernet4/5
 switchport access vlan 10
 no ip address
!
interface FastEthernet4/6
 switchport access vlan 10
 no ip address
!
interface FastEthernet4/7
 switchport access vlan 10
 no ip address
!
interface FastEthernet4/8
 switchport access vlan 10
 no ip address
!
interface FastEthernet4/9
 switchport access vlan 10
 no ip address
!
interface FastEthernet4/10
 switchport access vlan 10
 no ip address
!
interface FastEthernet4/11
 switchport access vlan 10
 no ip address
!
interface FastEthernet4/12
 switchport access vlan 10
 no ip address
!
interface FastEthernet4/13
```

```
 switchport access vlan 10
 no ip address
!
interface FastEthernet4/14
 switchport access vlan 10
 no ip address
!
interface FastEthernet4/15
 switchport access vlan 10
 no ip address
!
!-- Entries for FastEthernet 4/16 through 4/35 omitted for redundancy
!
interface GigabitEthernet4/0
 no ip address
 shutdown
!
interface GigabitEthernet4/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
!
interface Vlan10
 ip address 192.168.1.1 255.255.255.0
!
!
ip local pool VPN-POOL 10.1.1.1 10.1.1.10
ip classless
ip route 0.0.0.0 0.0.0.0 10.32.152.25
!
ip http server
no ip http secure-server
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 login authentication USERLIST
!
!
end
!
```

ブランチ 1 のルータ設定（Cisco 1841 ルータ）

```
EzVPN-Spoke-1# show running-config

Building configuration...
.
.
Current configuration : 4252 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
```

```
!
hostname EzVPN-Spoke-1
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 informational
enable secret 5 $1$b7.Q$Y2x1UXyRifSStbkH/YyrP.
!
username admin password 7 0519030B234D5C0617
memory-size iomem 20
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
aaa new-model
!
!
aaa authentication login USERLIST local
aaa session-id common
ip subnet-zero
ip cef
!
!
ip dhcp excluded-address 192.168.2.1
!
ip dhcp pool PRIVATE_DHCP
   import all
   network 192.168.2.0 255.255.255.0
   default-router 192.168.2.1
!
!
no ip domain lookup
ip domain name cisco.com
ip sap cache-timeout 30
ip ssh time-out 30
ip ids po max-events 100
no ftp-server write-enable
!
!--- IPSec configuration
!
crypto ipsec client ezvpn VPN1
 connect auto
 group VPN1 key cisco123
 mode client
 peer 10.32.152.26
 username ezvpn-spoke1 password  cisco1
!
interface FastEthernet0/0
 description === private interface ===
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
 crypto ipsec client ezvpn VPN1 inside
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface ATM0/1/0
 no ip address
 no atm ilmi-keepalive
```

```
 dsl equipment-type CPE
 dsl operating-mode GSHDSL symmetric annex A
 dsl linerate AUTO
 pvc 0/35
  encapsulation aal5snap
 !
 pvc 8/35
  encapsulation aal5mux ppp dialer
  dialer pool-member 1
 !
!
interface Dialer0
 description === public interface ===
 ip address 10.32.152.46 255.255.255.252
 ip pim sparse-dense-mode
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 crypto ipsec client ezvpn VPN1
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.32.152.45
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login authentication USERLIST
!
!
end
```

ブランチ 2 のルータ設定（Cisco 2811 ルータ）

```
EzVPN-Spoke-2# show running-config

Building configuration...
.
Current configuration : 4068 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname EzVPN-Spoke-2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$9BB/$KP4mHUWzUxzpuEPg5s7ow/
!
username admin password 7 10481A110C07
memory-size iomem 25
aaa new-model
!
!
```

```
aaa authentication login USERLIST local
aaa session-id common
ip subnet-zero
!
!
ip cef
ip dhcp excluded-address 192.168.3.1
!
ip dhcp pool PRIVATE_DHCP
   import all
   network 192.168.3.0 255.255.255.0
   default-router 192.168.3.1
!
!
no ip domain lookup
ip multicast-routing
ip ids po max-events 100
!
no ftp-server write-enable
voice-card 0
 no dspfarm
!
!--- IPSec configuration
!
crypto ipsec client ezvpn VPN1
 connect auto
 group VPN1 key cisco123
 mode network-extension
 peer 10.32.152.26
 username ezvpn-spoke2 password  cisco2
!
interface FastEthernet0/0
 description === private interface ===
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
 crypto ipsec client ezvpn VPN1 inside
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 description === public interface ===
 ip address 10.32.150.46 255.255.255.252
 crypto ipsec client ezvpn VPN1
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.32.150.45
!
ip http server
no ip http secure-server
!
control-plane
!
dial-peer cor custom
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login authentication USERLIST
```

```
!
end
```

確認

ここでは、設定が正しく機能していることを確認する手順を説明します。

一部の **show** コマンドは Output Interpreter Tool でサポートされています（登録ユーザのみ）。このツールを使用すると、**show** コマンド出力の分析結果を表示できます。次に要約を示します。

- **show crypto engine connections active**：暗号化パケットおよび復号化パケットを表示します。
- **show crypto ipsec sa**：ハブのフェーズ 2 IPSec セキュリティ アソシエーションを表示します。
- **show crypto ipsec client ezvpn**：EzVPN クライアントのフェーズ 2 IPSec セキュリティ アソシエーションを表示します。
- **show crypto isakmp sa**：フェーズ 1 ISAKMP セキュリティ アソシエーションを表示します。

IPSec のネゴシエーションが成功したことを示す最初の兆候の 1 つは、Virtual Private Network（VPN; 仮想私設網）のコンセントレータ コンソールに表示されるメッセージです。EzVPN クライアントによる IPSec ネゴシエーションが成功すると、次の内容に似たメッセージが VPN コンセントレータ コンソールに表示され、リモート EzVPN クライアントへの暗号化接続が確立されたことを示します。

```
EzVPN-Hub#

*Feb 23 10:33:10.663: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP  .  Peer
10.32.150.46:500       Id: VPN1
*Feb 23 10:33:37.439: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP  .  Peer
10.32.152.46:500       Id: VPN1
```

次に、**show crypto ipsec sa** コマンドおよび **show crypto ipsec client ezvpn** コマンドの出力例を示します。

次は、EzVPN ハブの場所での設定を使用して実行された **show crypto ipsec sa** コマンドの出力例です。

```
EzVPN-Hub# show crypto ipsec sa

interface: ATM0/0/0
    Crypto map tag: INT_MAP, local addr. 10.32.152.26

   protected vrf:
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.3/255.255.255.255/0/0)
   current_peer: 10.32.152.46:500
     PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.32.152.26, remote crypto endpt.: 10.32.152.46
     path mtu 4470, media mtu 4470
     current outbound spi: EBA2AC93

     inbound esp sas:
      spi: 0xDBEB20(14412576)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5131, flow_id: 11, crypto map: INT_MAP
        crypto engine type: Hardware, engine_id: 2
```

```
      sa timing: remaining key lifetime (k/sec): (4570368/14331)
      ike_cookies: 787F69F1 41C7488D 92A37C71 AE8FEC38
      IV size: 8 bytes
      replay detection support: Y

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0xEBA2AC93(3953306771)
      transform: esp-3des esp-md5-hmac ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 5132, flow_id: 12, crypto map: INT_MAP
      crypto engine type: Hardware, engine_id: 2
      sa timing: remaining key lifetime (k/sec): (4570368/14331)
      ike_cookies: 787F69F1 41C7488D 92A37C71 AE8FEC38
      IV size: 8 bytes
      replay detection support: Y

    outbound ah sas:

    outbound pcp sas:

protected vrf:
local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer: 10.32.150.46:500
  PERMIT, flags={}
 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0

  local crypto endpt.: 10.32.152.26, remote crypto endpt.: 10.32.150.46
  path mtu 4470, media mtu 4470
  current outbound spi: 59C46762

  inbound esp sas:
   spi: 0xA9344358(2838774616)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 5129, flow_id: 9, crypto map: INT_MAP
     crypto engine type: Hardware, engine_id: 2
     sa timing: remaining key lifetime (k/sec): (4574224/14292)
     ike_cookies: A479BC19 B6199FB9 E043AE83 9DECB0E8
     IV size: 8 bytes
     replay detection support: Y

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0x59C46762(1506043746)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 5130, flow_id: 10, crypto map: INT_MAP
     crypto engine type: Hardware, engine_id: 2
     sa timing: remaining key lifetime (k/sec): (4574224/14292)
     ike_cookies: A479BC19 B6199FB9 E043AE83 9DECB0E8
     IV size: 8 bytes
```

```
        replay detection support: Y

    outbound ah sas:

    outbound pcp sas:
```

次は、EzVPN スポーク 1 の場所での設定を使用して実行された **show crypto ipsec client ezvpn** コマンドの出力例です。

```
EzVPN-Spoke-1#show crypto ipsec client ezvpn

Easy VPN Remote Phase: 2

Tunnel name : VPN1
Inside interface list: FastEthernet0/0,
Outside interface: Dialer0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 10.1.1.3
Mask: 255.255.255.255
DNS Primary: 192.168.168.183
DNS Secondary: 192.168.226.120
NBMS/WINS Primary: 192.168.179.89
NBMS/WINS Secondary: 192.168.2.87
Default Domain: cisco.com
```

次は、EzVPN スポーク 2 の場所での設定を使用して実行された **show crypto ipsec client ezvpn** コマンドの出力例です。

```
EzVPN-Spoke-2#show crypto ipsec client ezvpn

Easy VPN Remote Phase: 2

Tunnel name : VPN1
Inside interface list: FastEthernet0/0,
Outside interface: Serial0/0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Primary: 192.168.168.183
DNS Secondary: 192.168.226.120
NBMS/WINS Primary: 192.168.179.89
NBMS/WINS Secondary: 192.168.2.87
Default Domain: cisco.com
```

トラブルシューティング

ここでは、設定のトラブルシューティングのための情報を示します。

次のテクニカル ノートを参照してください。

- 『*IP Security Troubleshooting - Understanding and Using debug Commands*』

トラブルシューティング コマンド

（注） **debug** コマンドを実行する前に、『*Important Information on Debug Commands*』を参照してください。

次の **debug** コマンドは、両方の IPSec ルータ（ピア）で実行する必要があります。セキュリティ アソシエーションは、両方のピアでクリアする必要があります。

- **debug crypto engine**：Cisco IOS ソフトウェアが暗号化または復号化を実行するタイミングなど、暗号化エンジンに関連する情報を表示します。
- **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 ipsec client ezvpn**：EzVPN クライアントから VPN コンセントレータへの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。
- **clear crypto ipsec client ezvpn**：既存の EzVPN 接続をクリアします。
- **clear crypto isakmp**：フェーズ 1 のセキュリティ アソシエーションをクリアします。
- **clear crypto sa**：フェーズ 2 のセキュリティ アソシエーションをクリアします。

次に、**debug crypto ipsec client ezvpn** コマンドの出力例を示します。

```
EzVPN-Spoke-1# debug crypto ipsec client ezvpn

*May 24 03:04:51.923: EZVPN(VPN1): New State: CONNECT_REQUIRED
!
!--- The following line shows the connection going down, not part of the debug output.
!
*May 24 03:04:51.923: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.  Peer
10.32.152.26:500       Id: 10.32.152.26
!
!---Debug output resumes
!
*May 24 03:04:51.927: EZVPN(VPN1): Current State: CONNECT_REQUIRED
*May 24 03:04:51.927: EZVPN(VPN1): Event: CONNECT
*May 24 03:04:51.927: EZVPN(VPN1): ezvpn_connect_request
*May 24 03:04:51.927: EZVPN(VPN1): New State: READY
*May 24 03:04:51.999: EZVPN(VPN1): Current State: READY
*May 24 03:04:51.999: EZVPN(VPN1): Event: CONN_UP
*May 24 03:04:51.999: EZVPN(VPN1): ezvpn_conn_up 7F890E16 DB923EE3 67C9C0D2 7EE723AC
*May 24 03:04:51.999: EZVPN(VPN1): No state change
*May 24 03:04:52.007: EZVPN(VPN1): Current State: READY
*May 24 03:04:52.007: EZVPN(VPN1): Event: XAUTH_REQUEST
*May 24 03:04:52.007: EZVPN(VPN1): ezvpn_xauth_request
*May 24 03:04:52.007: EZVPN(VPN1): ezvpn_parse_xauth_msg
*May 24 03:04:52.007: EZVPN: Attributes sent in xauth request message:
*May 24 03:04:52.007:         XAUTH_USER_NAME_V2(VPN1):
*May 24 03:04:52.007:         XAUTH_USER_PASSWORD_V2(VPN1):
*May 24 03:04:52.007: EZVPN(VPN1): send saved username ezvpn-spoke1 and password <omitted>
*May 24 03:04:52.007: EZVPN(VPN1): New State: XAUTH_REQ
*May 24 03:04:52.007: EZVPN(VPN1): Current State: XAUTH_REQ
*May 24 03:04:52.007: EZVPN(VPN1): Event: XAUTH_REQ_INFO_READY
*May 24 03:04:52.007: EZVPN(VPN1): ezvpn_xauth_reply
*May 24 03:04:52.007:         XAUTH_USER_NAME_V2(VPN1): ezvpn-spoke1
*May 24 03:04:52.011:         XAUTH_USER_PASSWORD_V2(VPN1): <omitted>
*May 24 03:04:52.011: EZVPN(VPN1): New State: XAUTH_REPLIED
*May 24 03:04:52.023: EZVPN(VPN1): Current State: XAUTH_REPLIED
*May 24 03:04:52.023: EZVPN(VPN1): Event: XAUTH_STATUS
*May 24 03:04:52.023: EZVPN(VPN1): New State: READY
*May 24 03:04:52.039: EZVPN(VPN1): Current State: READY
*May 24 03:04:52.039: EZVPN(VPN1): Event: MODE_CONFIG_REPLY
*May 24 03:04:52.039: EZVPN(VPN1): ezvpn_mode_config
*May 24 03:04:52.039: EZVPN(VPN1): ezvpn_parse_mode_config_msg
*May 24 03:04:52.039: EZVPN: Attributes sent in message:
*May 24 03:04:52.039:         Address: 10.1.1.4
*May 24 03:04:52.039:         DNS Primary: 192.168.168.183
*May 24 03:04:52.039:         DNS Secondary: 192.168.226.120
```

```
*May 24 03:04:52.039:         NBMS/WINS Primary: 192.168.179.89
*May 24 03:04:52.039:         NBMS/WINS Secondary: 192.168.2.87
*May 24 03:04:52.039:         Split Tunnel List: 1
*May 24 03:04:52.039:               Address    : 192.168.0.0
*May 24 03:04:52.039:               Mask       : 255.255.0.0
*May 24 03:04:52.039:               Protocol   : 0x0
*May 24 03:04:52.039:               Source Port: 0
*May 24 03:04:52.039:               Dest Port  : 0
*May 24 03:04:52.039: EZVPN: Unknown/Unsupported Attr: SPLIT_DNS (0x7003)
*May 24 03:04:52.039:         Default Domain: cisco.com
*May 24 03:04:52.039:         Savepwd on
*May 24 03:04:52.039: EZVPN: Unknown/Unsupported Attr: BACKUP_SERVER (0x7009)
*May 24 03:04:52.039: EZVPN: Unknown/Unsupported Attr: APPLICATION_VERSION (0x7)
*May 24 03:04:52.039: EZVPN(VPN1): ezvpn_nat_config
*May 24 03:04:52.043: EZVPN(VPN1): New State: SS_OPEN
*May 24 03:04:52.047: EZVPN(VPN1): Current State: SS_OPEN
*May 24 03:04:52.047: EZVPN(VPN1): Event: SOCKET_READY
*May 24 03:04:52.047: EZVPN(VPN1): No state change
!
!--- The following line shows the connection coming up, not part of the debug output.
!
*May 24 03:04:52.075: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP  .  Peer
10.32.152.26:500       Id: 10.32.152.26
!
!---Debug output resumes
!
*May 24 03:04:52.079: EZVPN(VPN1): Current State: SS_OPEN
*May 24 03:04:52.079: EZVPN(VPN1): Event: MTU_CHANGED
*May 24 03:04:52.079: EZVPN(VPN1): No state change
*May 24 03:04:52.079: EZVPN(VPN1): Current State: SS_OPEN
*May 24 03:04:52.079: EZVPN(VPN1): Event: SOCKET_UP
*May 24 03:04:52.079: ezvpn_socket_up
*May 24 03:04:52.079: EZVPN(VPN1): New State: IPSEC_ACTIVE
```

関連情報

- 『*Cisco IOS Wide-Area Networking Configuration Guide*』
- 『*Cisco IOS Dial Technologies Configuration Guide*』
- 『*Cisco IOS Security Configuration Guide*』
- 『*Cisco IOS Interface and Hardware Component Configuration Guide*』
- Cisco Technical Assistance Center