



## Easy VPN の設定例

---

この資料では、Cisco Integrated Service Router (ISR) 1800 シリーズ、Cisco ISR 2800 シリーズ、および Cisco ISR 3800 シリーズを使用した Easy VPN (EzVPN) の設定例を紹介します。

### 目次

- [概要 \(p.1\)](#)
- [はじめに \(p.3\)](#)
- [設定 \(p.4\)](#)
- [設定の確認 \(p.13\)](#)
- [トラブルシューティング \(p.16\)](#)
- [関連資料 \(p.18\)](#)

### 概要

この資料では、EzVPN の設定例を紹介します。この設定例の特徴は次のとおりです。

- 2 つのクライアント ブランチ サイトと本社間のトラフィックはすべて、IP Security (IPSec) 暗号化トンネルの Virtual Private Network (VPN; 仮想私設網) を通じて送受信されます。
- Domain Name Server (DNS; ドメイン ネーム サーバ) 情報、Windows Information Name Service (WINS) 情報、ドメイン ネーム、クライアントの IP アドレス プールを使用したサーバ上での Internet Key Exchange (IKE) Dead Peer Detection (DPD)、スプリット トンネリング、グループ ポリシーなどの技術が使用されています。
- 本社では、EzVPN コンセントレータ、ATM インターフェイスが搭載された Cisco ISR 3800 シリーズが使用されています。
- 一方のブランチには Cisco ISR 2800 シリーズが配備され、シリアル インターフェイスによるネットワーク モードの EzVPN クライアントが使用されています。もう一方のブランチには Cisco ISR 1800 シリーズが配備され、SHDSL インターフェイスによるクライアント モードの EzVPN が使用されています。
- さまざまな **show** コマンドを使用して、EzVPN コンセントレータ上の Internet Security Association Key Management Protocol (ISAKMP) や IPSec Security Association (SA)、さらにクライアント上の 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)。データを 53 バイトのセル単位に区切り、デジタル信号によって送信する接続スイッチング プロトコル。1 つのストリング メッセージ内の各セルは、他のセルの送信または着信と非同期に処理されます (これが名前の由来になっています)。セルは多重方式で送信される前にキューに割り振られます。ATM は音声、ビデオ、データなど、多様なサービスに使用できます。

**DNS** Domain Name Server (ドメイン ネーム サーバ)。名前から IP アドレスおよび IP アドレスから名前の対応付けを実行します。DNS にはドメイン ネームと IP アドレスのマッピング リストが保存されています。

**DPD** Dead Peer Detection。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 デバイスが利用可能な状態であるかどうかをチェックします。

**IKE** Internet Key Exchange。IKE は、共有セキュリティ ポリシーの確立や、キーを必要とするサービス (IPSec など) 用のキー認証を行います。IPSec トラフィックを通過させるためには、事前に各ルータ / ファイアウォール / ホストが通信相手の ID を検証しなければなりません。これは、両側のホストに事前共有キーを手動で入力する方法でも、CA (認証局) サービスを実行する方法でも可能です。

**IPSec** IP Security。参加ピア間でのデータの機密性、完全性、認証を提供するオープン スタンドアードの枠組み。IPSec はこれらのセキュリティ サービスを IP レイヤで提供します。IPSec は、ローカル ポリシーに基づいてプロトコルとアルゴリズムのネゴシエーションを処理し、IPSec で使用される暗号キーおよび認証キーを生成するために IKE を使用します。IPSec は、ホスト間、セキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホストの間の 1 つまたは複数のデータフローを保護できます。

**ISAKMP** Internet Security Association Key Management Protocol。キー交換の暗号化および認証用のプロトコル。ISAKMP では、2 つの VPN 接続ピア間で少なくとも一組のメッセージが交換されないと、セキュアなリンクを確立できません。

**NETBEUI** NetBIOS Extended User Interface。マイクロソフトベースのネットワークと関連付けられたトランスポート プロトコル。NETBEUI は TCP/IP とは異なり、ルーティングに対応したネットワーク プロトコルではありません。

**NetBIOS** Network Basic Input/Output System。1980 年代に開発されたピアツーピアのローレベル 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 ハードウェアと結び付けます。NetBIOS は、ルーティングに対応していないので、ルータを通過させるためには、TCP/IP でカプセル化する必要があります。

**SA** Security Association。IPSec がネゴシエーションを実行する単一方向チャネル。双方向通信には一組の SA が必要です。SA はセッション キーと初期化ベクトルの索引付けに使用されます。

**SHDSL** Symmetrical High-Speed Digital Subscriber Line。両方の送信方向が同じ速度 (192 kbps ~ 2.3 Mbps) で動作する DSL の実装。

**WINS** Windows Internet Naming Service。ホスト名を IP アドレスに変換するマイクロソフトベースのネットワーク サービス。NETBEUI プロトコルを使用しており、NetBIOS と互換性があります。

## はじめに

ここでは、この資料で紹介する設定例を使用する場合の必要事項を説明します。

## 表記法

資料の表記法については、『[Cisco Technical Tips Conventions](#)』を参照してください。

## 使用されたコンポーネント

この資料の内容は、以下のバージョンのソフトウェアおよびハードウェアに基づいています。

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

この資料の内容は、特定のラボ環境におかれたデバイスを使用して作成されたものです。この資料に使用されたデバイスはすべて、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。実働環境で利用する場合は、事前にコマンドが及ぼす潜在的な影響について十分に理解する必要があります。

## 関連製品

この設定は、以下のハードウェアにも使用できます。

- Cisco ISR 1800 シリーズ
- Cisco ISR 2800 シリーズ
- Cisco ISR 3800 シリーズ

# 設定

ここでは、この資料に記載されている機能の設定について説明します。



(注)

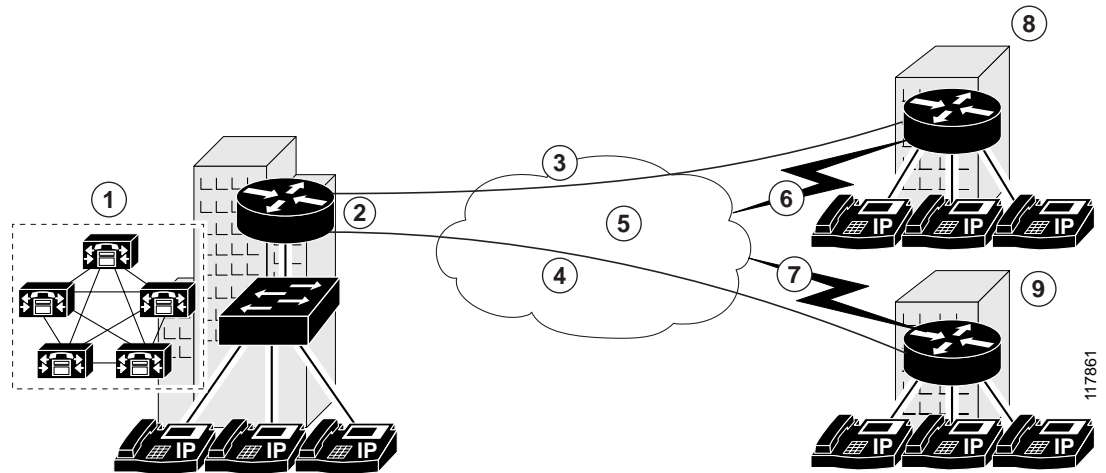
この資料で使用されるコマンドの詳細を調べるには、[Cisco IOS Command Lookup](#) ツールをご利用ください。このツールの利用には、Cisco.com のアカウントが必要です。アカウントを持っていないか、またはユーザ名やパスワードを忘れた場合は、ログイン ダイアログ ボックスで Cancel をクリックし、表示される説明に従ってください。

## 設定のヒント

- クリプト マップを適用する前に、トンネルが有効に機能していることを確認してください。
- IPSec クリプト マップは、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適用する必要があります。

## ネットワーク ダイアグラム

この資料では、以下の図に示すネットワーク構成を使用します。



図内の数字は次の語句を表しています。

1. 本社	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. インターネットを介したブランチ 1 への VPN トンネル	8. ブランチ 1
4. インターネットを介したブランチ 2 への VPN トンネル	9. ブランチ 2
5. インターネット (クラウドとして表示)	

本社（図内の 1）で使用されている Cisco ISR 3845 の特徴は次のとおりです。

- EzVPN サーバ
- インターネットへの ATM アクセス
- Cisco CallManager クラスタの稼働
- 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（図内の 8）で使用されている Cisco ISR 1841 の特徴は次のとおりです。

- EzVPN クライアント（クライアント モードを使用）
- 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（図内の 9）で使用されている Cisco ISR 2811 の特徴は次のとおりです。

- EzVPN クライアント（ネットワーク モードを使用）
- 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

この例では以下の設定が使用されています。

- [本社の設定（Cisco ISR 3845）](#)（p.5）
- [ブランチ 1 のルータの設定（Cisco ISR 1841）](#)（p.9）
- [ブランチ 2 のルータの設定（Cisco ISR 2811）](#)（p.11）

### 本社の設定（Cisco ISR 3845）

```
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/9a051
!
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 53000000
  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 のルータの設定 (Cisco ISR 1841)

```
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 のルータの設定 (Cisco ISR 2811)

```
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
```

## 設定の確認

ここでは、設定が正しく機能しているかどうかの確認手順を説明します。

一部の **show** コマンドは Output Interpreter ツール（登録済みのお客様のみ利用可能）に対応しています。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。コマンドの概要：

- **show crypto engine connections active** 暗号化パケットおよび復号化パケットを示します。
- **show crypto ipsec sa** ハブのフェーズ 2 IPsec SA を示します。
- **show crypto ipsec client ezvpn** EzVPN クライアントのフェーズ 2 IPsec SA を示します。
- **show crypto isakmp sa** フェーズ 1 ISAKMP SA を示します。

VPN コンセントレータのコンソール上にメッセージが表示されれば、IPsec ネゴシエーションが成功したといえます。EzVPN クライアントが IPsec ネゴシエーションに成功すると、リモートの EzVPN クライアントへの暗号化接続の確立を示す以下のようなメッセージが表示されます。

```
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
```

以下に、**show crypto ipsec sa** コマンドと **show crypto ipsec client ezvpn** コマンドの出力例を示します。

次に示すのは、EzVPN ハブ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:

```

次に示すのは、EzVPN Spoke 1 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
```

次に示すのは、EzVPN Spoke 2 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について説明します。

次に示すテクニカル 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。

以下に示す **debug** コマンドは、両方の IPsec ルータ (ピア) で実行しなければなりません。いずれのピアでも SA を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や復号化の動作を実行しているときなど、暗号化エンジンに関連した情報を表示します。
- **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 クライアントと VPN コンセントレータ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 SA をクリアします。
- **clear crypto sa** フェーズ 2 の SA をクリアします。

次に示すのは、**debug crypto ipsec client ezvpn** コマンドの出力例です。

```
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-spokel 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-spokel
*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

```

## 関連資料

- 『[Cisco IOS Wide-Area Networking Configuration Guide](#)』
- 『[Cisco IOS Dial Technologies Configuration Guide](#)』
- 『[Cisco IOS Security Configuration Guide](#)』
- 『[CiscoIOS Interface and Hardware Component Configuration Guide](#)』
- [TAC](#)

---

CCSP、Cisco Square Bridge のロゴ、Follow Me Browsing、StackWise は、Cisco Systems, Inc. の商標です。Changing the Way We Work, Live, Play, and Learn、iQuick Study は、Cisco Systems, Inc. のサービスマークです。Access Registrar、Aironet、ASIST、BPX、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、Cisco、Cisco Certified Internetwork Expert のロゴ、Cisco IOS、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems のロゴ、Cisco Unity、Empowering the Internet Generation、Enterprise/Solver、EtherChannel、EtherFast、EtherSwitch、Fast Step、FormShare、GigaDrive、GigaStack、HomeLink、Internet Quotient、IOS、IP/TV、iQ Expertise、iQ のロゴ、iQ Net Readiness Scorecard、LightStream、Linksys、MeetingPlace、MGX、Networkers のロゴ、Networking Academy、Network Registrar、Packet、PIX、Post-Routing、Pre-Routing、ProConnect、RateMUX、ScriptShare、SlideCast、SMARTnet、StrataView Plus、SwitchProbe、TeleRouter、The Fastest Way to Increase Your Internet Quotient、TransPath、VCO は、米国および一部の国における Cisco Systems, Inc. または関連会社の登録商標です。

このマニュアルまたは Web サイトで言及している他の商標はいずれも、それぞれの所有者のもので、「パートナー」という用語を使用しているも、シスコシステムズと他社とのパートナー関係を意味するものではありません。(0411R)

Copyright © 2004, Cisco Systems, Inc.  
All rights reserved.

お問い合わせは、購入された各代理店へご連絡ください。

シスコシステムズでは以下のURLで最新の日本語マニュアルを公開しております。  
本書とあわせてご利用ください。

Cisco.com 日本語サイト

[http://www.cisco.com/japanese/warp/public/3/jp/service/manual\\_j/](http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/)

日本語マニュアルの購入を希望される方は、以下のURLからお申し込みいただけます。

シスコシステムズマニュアルセンター

<http://www2.hipri.com/cisco/>

上記の両サイトで、日本語マニュアルの記述内容に関するご意見もお受けいたしますので、  
どうぞご利用ください。

なお、技術内容に関するご質問は、製品を購入された各代理店へお問い合わせください。



シスコシステムズ株式会社

URL:<http://www.cisco.com/jp/>

問合せ URL:<http://www.cisco.com/jp/service/contactcenter/>

〒107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館

TEL.03-5549-6500 FAX.03-5549-6501