

VPN 3000 コンセントレータを備えた IOS ルータ上の MEM の EzVPN の設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[VPN 3000 コンセントレータの設定](#)

[タスク](#)

[ネットワーク図](#)

[手順](#)

[ルータの設定](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[debugコマンドの出力](#)

[トラブルシューティングのための関連Cisco IOS showコマンド](#)

[VPN 3000 コンセントレータのデバッグ](#)

[不具合の原因](#)

[関連情報](#)

概要

このドキュメントでは、Cisco VPN 3000 コンセントレータに接続するために Network Extension Mode (NEM) で EzVPN として Cisco IOS® ルータを設定するときに使用する手順について説明します。新しい EzVPN Phase II 機能は、基本的なネットワーク アドレス変換 (NAT) 設定のサポートです。EzVPN Phase II は Unity プロトコル (VPN Client ソフトウェア) から派生したものです。リモート デバイスが常に IPsec トンネルの発信側となります。ただし、インターネット キー交換 (IKE) および IPsec プロポーザルは EzVPN クライアントで設定可能ではありません。VPN Client は、サーバとプロポーザルをネゴシエートします。

Easy VPN を使用して PIX/ASA 7.x と Cisco 871 間に IPsec を設定するには、『[ASA 5500 をサーバ、Cisco 871 を Easy VPN Remote として使用する PIX/ASA 7.x Easy VPN の設定例](#)』を参照してください。

Cisco IOS(R) Easy VPN リモート ハードウェア クライアントと PIX Easy VPN サーバ間に IPsec を設定するには、『[IOS Easy VPN リモート ハードウェア クライアントと PIX Easy VPN サーバの設定例](#)』を参照してください。

Cisco 7200ルータをEzVPNとして設定し、Cisco 871ルータをEasy VPNリモートとして設定する

には、『[7200 Easy VPNサーバから871 Easy VPNリモートへの設定例](#)』を参照してください。

前提条件

要件

この設定を試す前に、Cisco IOSルータが[EzVPNフェーズII機能](#)をサポートし、エンドツーエンド接続でIP接続を確立してIPsecトンネルを確立していることを確認してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOSソフトウェアリリース12.2(8)YJ (EzVPNフェーズII)
- VPN 3000コンセントレータ3.6.x
- Cisco 1700 ルータ

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。

注：この設定は、Cisco IOSソフトウェアリリース12.4(8)およびVPN 3000コンセントレータ4.7.xバージョンを搭載したCisco 3640ルータで最近テストされました。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

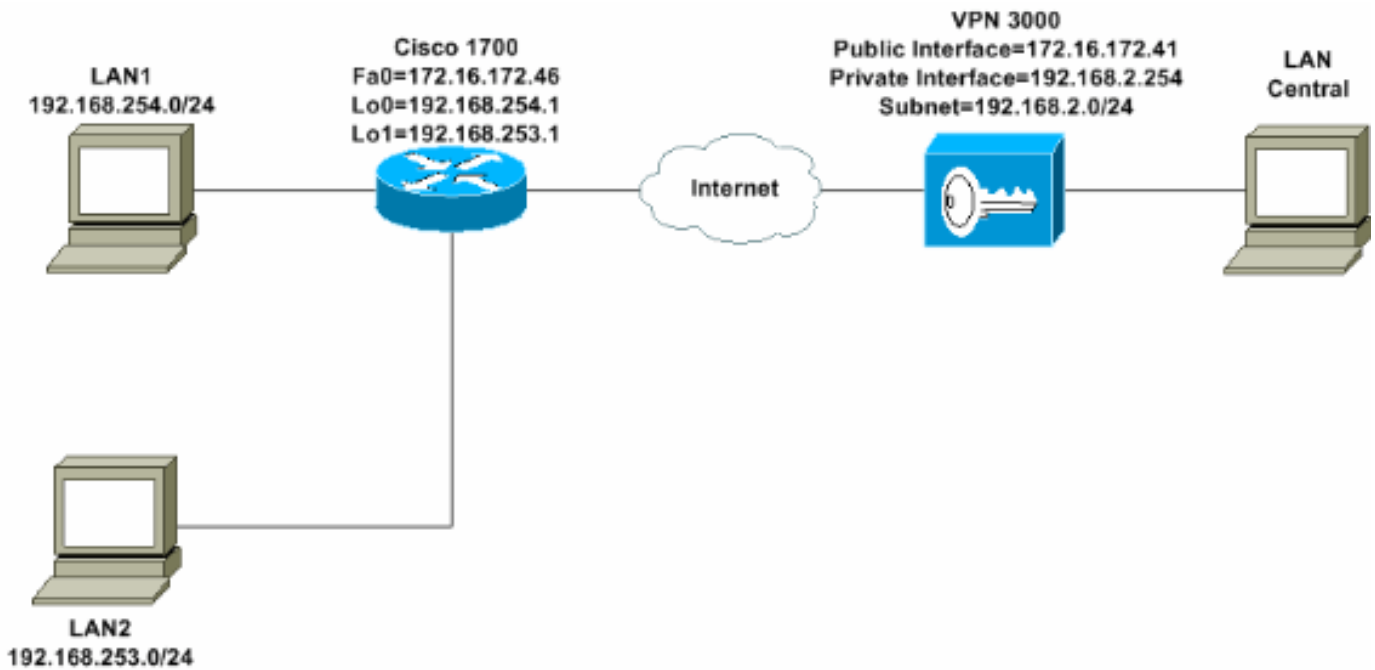
VPN 3000 コンセントレータの設定

タスク

このセクションでは、VPN 3000コンセントレータを設定するための情報を提供します。

ネットワーク図

このドキュメントでは、次の図で示されるネットワーク設定を使用しています。ループバックインターフェイスは内部サブネットとして使用され、ファストイーサネット0はインターネットのデフォルトです。



手順

次のステップを実行します。

1. [Configuration] > [User Management] > [Groups] > [Add] を選択し、グループ名とパスワードを定義して、ユーザのIPsecグループを設定します。次の例では、グループ名turaroとpassword/verify tulloを使用します。

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Attribute	Value	Description
Group Name	turaro	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	Internal	<i>External groups</i> are configured on an external authentication server (e.g. RADIUS). <i>Internal groups</i> are configured on the VPN 3000 Concentrator's Internal Database.

Add Cancel

2. [Configuration] > [User Management] > [Groups] > turaro > [General]の順に選択してIPsecを有効にし、ポイントツーポイントトンネリングプロトコル(PPTP)とレイヤ2トンネルプロトコル(L2TP)を無効にします。選択を行い、[適用]をクリックします。

- [-] Configuration
 - Interfaces
 - [-] System
 - [-] User Management
 - Base Group
 - Groups
 - Users
 - [-] Policy Management
- [-] Administration
- [-] Monitoring

Identity
General
IPSec
Client FW
PPTP/L2TP

General Par

Attribute	Value	Inherit?	
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Sele
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Ente
Minimum Password Length	8	<input checked="" type="checkbox"/>	Ente
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Ente be a
Idle Timeout	30	<input checked="" type="checkbox"/>	(mir
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(mir
Filter	-None-	<input checked="" type="checkbox"/>	Ente
Primary DNS		<input checked="" type="checkbox"/>	Ente
Secondary DNS		<input checked="" type="checkbox"/>	Ente
Primary WINS		<input checked="" type="checkbox"/>	Ente
Secondary WINS		<input checked="" type="checkbox"/>	Ente
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Sele
Tunneling Protocols	<input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPSec	<input type="checkbox"/>	Sele

CISCO SYSTEMS

3. [Authentication]を[Internal for Extended Authentication (Xauth)]に設定し、[Tunnel Type]が [Remote Access]で、[IPSec SA]が[ESP-3DES-MD5]であることを確認します。

Configuration | User Management | Groups | Modify ADMINI

Check the **Inherit?** box to set a field that you want to default to the base group value to override base group values.

Identity General **IPSec** Client FW PPTP/L2TP

IPSec Parameters

Attribute	Value	Inherit?
IPSec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Reauthentication on Rekey	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>

Remote Access Parameters

Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Authentication	Internal	<input checked="" type="checkbox"/>

4. Configuration > System > Tunneling Protocols > IPSec > IKE Proposalsの順に選択し、Cisco VPN Client(CiscoVPNClient-3DES-MD5)がActive Proposals for IKE (フェーズ1) にあることを確認します。注：VPN Concentrator 4.1.xでは、Cisco VPN ClientがIKE (フェーズ1) のアクティブなプロポーザルのリストに含まれるかどうかは、手順が異なります。
Configuration > Tunneling and Security > IPSec > IKE Proposalsの順に選択します。

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete**.
 Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down**.
 Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by Security Association parameters.

Active Proposals	Actions	Inactive Proposals
CiscoVPNClient-3DES-MD5 IKE-3DES-MD5 IKE-3DES-MD5-DH1 IKE-DES-MD5 IKE-3DES-MD5-DH7	<< Activate Deactivate >> Move Up Move Down Add	IKE-3DES-MD5-RSA IKE-3DES-SHA-DSA IKE-3DES-MD5-RSA-D IKE-DES-MD5-DH7 CiscoVPNClient-3DES CiscoVPNClient-3DES

5. IPSecセキュリティアソシエーション(SA)を確認します。ステップ3では、IPsec SAはESP-3DES-MD5です。必要に応じて新しいIPsec SAを作成できますが、グループで正しいIPsec SAを使用していることを確認してください。使用するIPsec SAのPerfect Forward Secrecy(PFS)を無効にする必要があります。[Configuration] > [Policy Management] > [Traffic Management] > [SAs] の順に選択して、IKEプロポーザルとしてCisco VPN Clientを選択します。テキストボックスにSA名を入力し、次のように適切な選択を行います。

Configuration | Policy Management | Traffic Management | Security Associations | Modify

Modify a configured Security Association.

SA Name Specify the name of this Security Association (S

Inheritance Select the granularity of this SA.

IPSec Parameters

Authentication Algorithm Select the packet authentication algorithm to use

Encryption Algorithm Select the ESP encryption algorithm to use.

Encapsulation Mode Select the Encapsulation Mode for this SA.

Perfect Forward Secrecy Select the use of Perfect Forward Secrecy.

Lifetime Measurement Select the lifetime measurement of the IPSec ke

Data Lifetime Specify the data lifetime in kilobytes (KB).

Time Lifetime Specify the time lifetime in seconds.

IKE Parameters

IKE Peer Specify the IKE Peer for a LAN-to-LAN IPSe

Negotiation Mode Select the IKE Negotiation mode to use.

Digital Certificate Select the Digital Certificate to use.

Certificate Transmission Entire certificate chain
 Identity certificate only Choose how to send the digital certificate to the

IKE Proposal Select the IKE Proposal to use as IKE initiator.

注：事前に定義されたSAを選択する場合、この手順と次の手順はオプションです。クライアントにダイナミックに割り当てられたIPアドレスがある場合は、[IKE peer]テキストボックスで0.0.0.0を使用します。次の例に示すように、IKE ProposalがCiscoVPNClient-3DES-MD5に設定されていることを確認します。

6. [リスト内のネットワークがトンネルをバイパスできるようにする]をクリックしないでください。この理由は、スプリットトンネリングがサポートされていますが、EzVPN Client機能ではバイパス機能がサポートされていないためです。

<ul style="list-style-type: none"> [-] Configuration <ul style="list-style-type: none"> [-] Interfaces [-] System [-] User Management <ul style="list-style-type: none"> [-] Base Group [-] Groups [-] Users [-] Policy Management [-] Administration [-] Monitoring 	Banner	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Allow Password Storage on Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Split Tunneling Policy	<input checked="" type="radio"/> Tunnel everything <input type="checkbox"/> Allow the networks in list to bypass the tunnel <input type="radio"/> Only tunnel networks in list	<input checked="" type="checkbox"/>
	Split Tunneling Network List	<input type="text" value="-None-"/>	<input checked="" type="checkbox"/>

7. [Configuration] > [User Management] > [Users] を選択して、ユーザを追加します。ユーザー名とパスワードを定義し、グループに割り当て、「追加」をクリックします。

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity General IPsec PPTP/L2TP

Identity Parameters		
Attribute	Value	Description
Username	podma	Enter a unique username.
Password	*****	Enter the user's password. The password must satisfy the group password requirements.
Verify	*****	Verify the user's password.
Group	turaro	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

Add Cancel

CISCO SYSTEMS

8. [Administration] > [Admin Sessions]を選択し、ユーザが接続されていることを確認します。NEMでは、VPNコンセントレータはプールからIPアドレスを割り当てません。注：事前定義SAを選択する場合、この手順はオプションです。

LAN-to-LAN Sessions									[Remote Access Sessions Management Sessions]
Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx	Actions	
No LAN-to-LAN Sessions									
Remote Access Sessions									[LAN-to-LAN Sessions Management Sessions]
Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	Actions		
Cisco_MAE	192.168.253.0 172.16.172.46	turaro	IPsec 3DES-168	Mar 31 18:32:23 0:02:50	N/A N/A	301320 301320	[Logout] [Ping]		
Management Sessions									[LAN-to-LAN Sessions Remote Access Sessions]
Administrator	IP Address	Protocol	Encryption	Login Time	Duration	Actions			
admin	171.69.89.5	HTTP	None	Mar 31 18:35:01	0:00:12	[Logout] [Ping]			

9. [Save Needed]または[Save]アイコンをクリックして、設定を保存します。

ルータの設定

show versionの出力

show version

```
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-BK9N03R2S7-M), Version 12.2(8)YJ,
EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
```

1721-1(ADSL) uptime is 4 days, 5 hours, 33 minutes
System returned to ROM by reload
System image file is "flash:c1700-bk9no3r2sy7-mz.122-8.YJ.bin"
cisco 1721 (MPC860P) processor (revision 0x100) with 88474K/9830K bytes
16384K bytes of processor board System flash (Read/Write)

1721-1

```
1721-1(ADSL)#show run
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1721-1(ADSL)
!
!--- Specify the configuration name !--- to be assigned
to the interface. crypto ipsec client ezvpn SJVPN
!--- Tunnel control; automatic is the default. connect
auto
!--- The group name and password should be the same as
given in the VPN Concentrator. group turaro key tululo
!--- The mode that is chosen as the network extension.
mode network-extension
!--- The tunnel peer end (VPN Concentrator public
interface IP address). peer 172.16.172.41
!
interface Loopback0
 ip address 192.168.254.1 255.255.255.0
!--- Configure the Loopback interface !--- as the inside
interface. ip nat inside
!--- Specifies the Cisco EzVPN Remote configuration name
!--- to be assigned to the inside interface.

crypto ipsec client ezvpn SJVPN inside
!
interface Loopback1
 ip address 192.168.253.1 255.255.255.0
ip nat inside
crypto ipsec client ezvpn SJVPN inside
!
interface FastEthernet0
 ip address 172.16.172.46 255.255.255.240
!--- Configure the FastEthernet interface !--- as the
outside interface. ip nat outside
!--- Specifies the Cisco EzVPN Remote configuration name
!--- to be assigned to the first outside interface,
because !--- outside is not specified for the interface.
!--- The default is outside.

crypto ipsec client ezvpn SJVPN
!
!--- Specify the overload option with the ip nat command
!--- in global configuration mode in order to enable !--
- Network Address Translation (NAT) of the inside source
address !--- so that multiple PCs can use the single IP
address.

ip nat inside source route-map EZVPN interface
FastEthernet0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.172.41
!
access-list 177 deny ip 192.168.254.0 0.0.0.255
```



```
192.168.2.0 0.0.0.255
access-list 177 deny ip 192.168.253.0 0.0.0.255
192.168.2.0 0.0.0.255
access-list 177 permit ip 192.168.253.0 0.0.0.255 any
access-list 177 permit ip 192.168.254.0 0.0.0.255 any
!
route-map EZVPN permit 10
 match ip address 177
!
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
no scheduler allocate
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 \(登録ユーザ専用\) \(OIT\)](#) は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

両方のデバイスを設定すると、Cisco 3640ルータは、ピアのIPアドレスを使用してVPNコンセントレータに自動的に接続することによって、VPNトンネルの設定を試みます。最初の ISAKMP パラメータが交換されると、ルータは次のメッセージを表示します。

```
Pending XAuth Request, Please enter the
following command: crypto ipsec client ezvpn xauth
```

crypto ipsec client ezvpn xauth コマンドを入力する必要があり、入力するとユーザ名とパスワードが求められます。これは、VPNコンセントレータで設定されているユーザ名とパスワードと一致する必要があります (ステップ7)。ユーザ名とパスワードが両方のピアで合意されると、残りのパラメータが一致し、IPsec VPNトンネルが起動します。

```
EZVPN(SJVPN): Pending XAuth Request, Please enter the following command:
```

```
EZVPN: crypto ipsec client ezvpn xauth
```

```
!--- Enter the crypto ipsec client ezvpn xauth command.
```

```
crypto ipsec client ezvpn xauth
```

```
Enter Username and Password.: padma
```

```
Password: : password
```

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使用できる情報を示します。

トラブルシューティングのためのコマンド

一部の show コマンドは アウトプット インタープリタ ツールによってサポートされています (登録ユーザ専用)。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

注 : debugコマンドを発行する前に、『debugコマンドの重要な情報』を参照してください。

- **debug crypto ipsec client ezvpn:** EzVPN Client機能の設定と実装を示す情報を表示します。
- **debug crypto ipsec :** IPsec 接続に関するデバッグ情報を表示します。
- **debug crypto isakmp:** IPsec接続に関するデバッグ情報を表示し、両端で互換性がないために拒否された最初の属性セットを表示します。
- **show debug :** 各デバッグオプションの状態を表示します。

debugコマンドの出力

crypto ipsec client ezvpn SJVPNコマンドを入力するとすぐに、EzVPN Clientはサーバへの接続を試みます。グループ設定でconnect manualコマンドを変更する場合は、crypto ipsec client ezvpn connect SJVPNコマンドを入力して、サーバへのプロポーザルの交換を開始します。

```
4d05h: ISAKMP (0:3): beginning Aggressive Mode exchange
4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) AG_INIT_EXCH
4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) AG_INIT_EXCH
4d05h: ISAKMP (0:3): processing SA payload. message ID = 0
4d05h: ISAKMP (0:3): processing ID payload. message ID = 0
4d05h: ISAKMP (0:3): processing vendor id payload
4d05h: ISAKMP (0:3): vendor ID is Unity
4d05h: ISAKMP (0:3): processing vendor id payload
4d05h: ISAKMP (0:3): vendor ID seems Unity/DPD but bad major
4d05h: ISAKMP (0:3): vendor ID is XAUTH
4d05h: ISAKMP (0:3): processing vendor id payload
4d05h: ISAKMP (0:3): vendor ID is DPD
4d05h: ISAKMP (0:3) local preshared key found
4d05h: ISAKMP (0:3) Authentication by xauth preshared
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65527 policy
4d05h: ISAKMP:      encryption 3DES-CBC
4d05h: ISAKMP:      hash MD5
4d05h: ISAKMP:      default group 2
4d05h: ISAKMP:      auth XAUTHInitPreShared
4d05h: ISAKMP:      life type in seconds
4d05h: ISAKMP:      life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65528 policy
4d05h: ISAKMP:      encryption 3DES-CBC
4d05h: ISAKMP:      hash MD5
4d05h: ISAKMP:      default group 2
4d05h: ISAKMP:      auth XAUTHInitPreShared
4d05h: ISAKMP:      life type in seconds
4d05h: ISAKMP:      life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65529 policy
4d05h: ISAKMP:      encryption 3DES-CBC
4d05h: ISAKMP:      hash MD5
4d05h: ISAKMP:      default group 2
4d05h: ISAKMP:      auth XAUTHInitPreShared
```

4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65530 policy
4d05h: ISAKMP: encryption 3DES-CBC
4d05h: ISAKMP: hash MD5
4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared
4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65531 policy
4d05h: ISAKMP: encryption 3DES-CBC
4d05h: ISAKMP: hash MD5
4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared
4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Hash algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65532 policy
4d05h: ISAKMP: encryption 3DES-CBC
4d05h: ISAKMP: hash MD5
4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared
4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): **atts are acceptable.** Next payload is 0
4d05h: ISAKMP (0:3): processing KE payload. message ID = 0
4d05h: ISAKMP (0:3): processing NONCE payload. message ID = 0
4d05h: ISAKMP (0:3): SKEYID state generated
4d05h: ISAKMP (0:3): processing HASH payload. message ID = 0
4d05h: ISAKMP (0:3): **SA has been authenticated with 172.16.172.41**
4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) AG_INIT_EXCH
4d05h: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_I_AM1 New State = IKE_P1_COMPLETE

4d05h: IPSEC(key_engine): got a queue event...

4d05h: IPsec: Key engine got KEYENG_IKMP_MORE_SAS message

4d05h: ISAKMP (0:3): Need XAUTH

4d05h: ISAKMP (0:3): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE

Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

!--- Phase 1 (ISAKMP) is complete. 4d05h: ISAKMP: received ke message (6/1) 4d05h: ISAKMP: received KEYENG_IKMP_MORE_SAS message 4d05h: ISAKMP: set new node -857862190 to CONF_XAUTH *!--- Initiate extended authentication.* 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP (0:3): purging node -857862190 4d05h: ISAKMP (0:3): Sending initial contact. 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP: set new node -1898481791 to CONF_XAUTH 4d05h: ISAKMP (0:3): processing transaction payload from 172.16.172.41. message ID = -1898481791 4d05h: ISAKMP: Config payload REQUEST 4d05h: ISAKMP (0:3): checking request: 4d05h: ISAKMP: XAUTH_TYPE_V2 4d05h: ISAKMP: XAUTH_USER_NAME_V2 4d05h: ISAKMP: XAUTH_USER_PASSWORD_V2 4d05h: ISAKMP: XAUTH_MESSAGE_V2 4d05h: ISAKMP (0:3): Xauth process request 4d05h: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_REPLY_AWAIT 4d05h: EZVPN(SJVPN): Current State: READY 4d05h: EZVPN(SJVPN): Event: XAUTH_REQUEST 4d05h: EZVPN(SJVPN): ezvpn_xauth_request 4d05h: EZVPN(SJVPN): ezvpn_parse_xauth_msg 4d05h: EZVPN: Attributes sent in xauth request message: 4d05h: XAUTH_TYPE_V2(SJVPN): 0 4d05h: XAUTH_USER_NAME_V2(SJVPN): 4d05h: XAUTH_USER_PASSWORD_V2(SJVPN): 4d05h: XAUTH_MESSAGE_V2(SJVPN) <Enter Username and Password.>

4d05h: EZVPN(SJVPN): New State: XAUTH_REQ 4d05h: ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE Old State = IKE_XAUTH_REPLY_AWAIT New State = IKE_XAUTH_REPLY_AWAIT 4d05h: EZVPN(SJVPN): Pending XAuth Request, Please enter the following command: 4d05h: EZVPN: **crypto ipsec client ezvpn xauth**

!--- Enter the crypto ipsec client ezvpn xauth command.

crypto ipsec client ezvpn xauth

Enter Username and Password.: **padma**

Password: : **password**

!--- The router requests your username and password that is !--- configured on the server.

4d05h: EZVPN(SJVPN): Current State: XAUTH_REQ 4d05h: EZVPN(SJVPN): Event: XAUTH_PROMPTING 4d05h: EZVPN(SJVPN): New State: XAUTH_PROMPT 1721-1(ADSL)# 4d05h: EZVPN(SJVPN): Current State: XAUTH_PROMPT 4d05h: EZVPN(SJVPN): Event: XAUTH_REQ_INFO_READY 4d05h: EZVPN(SJVPN): ezvpn_xauth_reply 4d05h: XAUTH_TYPE_V2(SJVPN): 0 4d05h: XAUTH_USER_NAME_V2(SJVPN): Cisco_MAE 4d05h: XAUTH_USER_PASSWORD_V2(SJVPN): <omitted> 4d05h: EZVPN(SJVPN): New State: XAUTH_REPLIED 4d05h: xauth-type: 0 4d05h: username: Cisco_MAE 4d05h: password: <omitted> 4d05h: message <Enter Username and Password.> 4d05h: ISAKMP (0:3): responding to peer config from 172.16.172.41. ID = -1898481791 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP (0:3): deleting node -1898481791 error FALSE reason "done with xauth request/reply exchange" 4d05h: ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_XAUTH_REPLY_ATTR Old State = IKE_XAUTH_REPLY_AWAIT New State = IKE_XAUTH_REPLY_SENT 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP: set new node -1602220489 to CONF_XAUTH 4d05h: ISAKMP (0:3): processing transaction payload from 172.16.172.41. message ID = -1602220489 4d05h: ISAKMP: Config payload SET 4d05h: ISAKMP (0:3): Xauth process set, status = 1 4d05h: ISAKMP (0:3): checking SET: 4d05h: ISAKMP: XAUTH_STATUS_V2 XAUTH-OK 4d05h: ISAKMP (0:3): attributes sent in message: 4d05h: Status: 1 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP (0:3): deleting node -1602220489 error FALSE reason "" 4d05h: ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_CFG_SET Old State = IKE_XAUTH_REPLY_SENT New State = IKE_P1_COMPLETE 4d05h: EZVPN(SJVPN): Current State: XAUTH_REPLIED 4d05h: EZVPN(SJVPN): Event: XAUTH_STATUS 4d05h: EZVPN(SJVPN): New State: READY 4d05h: ISAKMP (0:3): Need config/address 4d05h: ISAKMP (0:3): Need config/address 4d05h: ISAKMP: set new node 486952690 to CONF_ADDR 4d05h: ISAKMP (0:3): initiating peer config to 172.16.172.41. ID = 486952690 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) CONF_ADDR 4d05h: ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_MODE_REQ_SENT 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) CONF_ADDR 4d05h: ISAKMP (0:3): processing transaction payload from 172.16.172.41. message ID = 486952690 4d05h: ISAKMP: Config payload REPLY 4d05h: ISAKMP(0:3) process config reply 4d05h: ISAKMP (0:3): deleting node 486952690 error FALSE reason "done with transaction" 4d05h: ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_CFG_REPLY Old State = IKE_CONFIG_MODE_REQ_SENT New State = IKE_P1_COMPLETE 4d05h: EZVPN(SJVPN): Current State: READY 4d05h: EZVPN(SJVPN): Event: MODE_CONFIG_REPLY 4d05h: EZVPN(SJVPN): ezvpn_mode_config 4d05h: EZVPN(SJVPN): ezvpn_parse_mode_config_msg 4d05h: EZVPN: Attributes sent in message 4d05h: ip_ifnat_modified: old_if 0, new_if 2 4d05h: ip_ifnat_modified: old_if 0, new_if 2 4d05h: ip_ifnat_modified: old_if 1, new_if 2 4d05h: EZVPN(SJVPN): New State: SS_OPEN 4d05h: ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-sha-hmac , lifedur= 2147483s and 4608000kb, spi= 0xE6DB9372(3873149810), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 2147483s and 4608000kb, spi= 0x3C77C53D(1014482237), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 2147483s and 4608000kb, spi= 0x79BB8DF4(2042334708), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 2147483s and 4608000kb, spi=

0x19C3A5B2(432252338), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: ISAKMP: received ke message (1/4) 4d05h: ISAKMP: set new node 0 to QM_IDLE 4d05h: EZVPN(SJVPN): Current State: SS_OPEN 4d05h: EZVPN(SJVPN): Event: SOCKET_READY 4d05h: EZVPN(SJVPN): No state change 4d05h: ISAKMP (0:3): sitting IDLE. Starting QM immediately (QM_IDLE) 4d05h: ISAKMP (0:3): beginning Quick Mode exchange, M-ID of -1494477527 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-sha-hmac , lifedur= 2147483s and 4608000kb, spi= 0xB18CF11E(2978803998), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 2147483s and 4608000kb, spi= 0xA8C469EC(2831444460), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 2147483s and 4608000kb, spi= 0xBC5AD5EE(3160069614), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 2147483s and 4608000kb, spi= 0x8C34C692(2352268946), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): Node -1494477527, Input = IKE_MSG_INTERNAL, IKE_INIT_QM Old State = IKE_QM_READY New State = IKE_QM_I_QM1 4d05h: ISAKMP: received ke message (1/4) 4d05h: ISAKMP: set new node 0 to QM_IDLE 4d05h: ISAKMP (0:3): sitting IDLE. Starting QM immediately (QM_IDLE) 4d05h: ISAKMP (0:3): beginning Quick Mode exchange, M-ID of -1102788797 4d05h: EZVPN(SJVPN): Current State: SS_OPEN 4d05h: EZVPN(SJVPN): Event: SOCKET_READY 4d05h: EZVPN(SJVPN): No state change 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): Node -1102788797, Input = IKE_MSG_INTERNAL, IKE_INIT_QM Old State = IKE_QM_READY New State = IKE_QM_I_QM1 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP: set new node 733055375 to QM_IDLE 4d05h: ISAKMP (0:3): processing HASH payload. message ID = 733055375 4d05h: ISAKMP (0:3): processing NOTIFY RESPONDER_LIFETIME protocol 1 spi 0, message ID = 733055375, sa = 820ABFA0 4d05h: ISAKMP (0:3): processing responder lifetime 4d05h: ISAKMP (0:3): start processing isakmp responder lifetime 4d05h: ISAKMP (0:3): restart ike sa timer to 86400 secs 4d05h: ISAKMP (0:3): deleting node 733055375 error FALSE reason "informational (in) state 1" 4d05h: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_INFO_NOTIFY Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): processing HASH payload. message ID = -1494477527 4d05h: ISAKMP (0:3): processing SA payload. message ID = -1494477527 4d05h: ISAKMP (0:3): Checking IPsec proposal 1 4d05h: ISAKMP: transform 1, ESP_3DES 4d05h: ISAKMP: attributes in transform: 4d05h: ISAKMP: SA life type in seconds 4d05h: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 4d05h: ISAKMP: SA life type in kilobytes 4d05h: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 4d05h: ISAKMP: encaps is 1 4d05h: ISAKMP: authenticator is HMAC-MD5 4d05h: ISAKMP (0:3): atts are acceptable. 4d05h: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 4d05h: ISAKMP (0:3): processing NONCE payload. message ID = -1494477527 4d05h: ISAKMP (0:3): processing ID payload. message ID = -1494477527 4d05h: ISAKMP (0:3): processing ID payload. message ID = -1494477527 4d05h: ISAKMP (0:3): processing NOTIFY RESPONDER_LIFETIME protocol 3 spi 1344958901, message ID = -1494477527, sa = 820ABFA0 4d05h: ISAKMP (0:3): processing responder lifetime 4d05h: ISAKMP (3): responder lifetime of 28800s 4d05h: ISAKMP (3): responder lifetime of 0kb 4d05h: ISAKMP (0:3): Creating IPsec SAs 4d05h: inbound SA from 172.16.172.41 to 172.16.172.46 (proxy 0.0.0.0 to 192.168.254.0) 4d05h: has spi 0x3C77C53D and conn_id 2000 and flags 4 4d05h: lifetime of 28800 seconds 4d05h: outbound SA from 172.16.172.46 to 172.16.172.41 (proxy 192.168.254.0 to 0.0.0.0) 4d05h: has spi 1344958901 and conn_id 2001 and flags C 4d05h: lifetime of 28800 seconds 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): deleting node -1494477527 error FALSE reason "" 4d05h: ISAKMP (0:3): Node -1494477527, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): processing HASH payload. message ID = -1102788797 4d05h: ISAKMP (0:3): processing SA payload. message ID = -1102788797 4d05h: ISAKMP (0:3): Checking IPsec proposal 1 4d05h: ISAKMP: transform 1, ESP_3DES 4d05h: ISAKMP: attributes in transform: 4d05h: ISAKMP: SA life type in seconds 4d05h: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 4d05h: ISAKMP: SA life type in kilobytes 4d05h: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 4d05h: ISAKMP: encaps is 1

4d05h: ISAKMP: authenticator is HMAC-MD5 4d05h: ISAKMP (0:3): atts are acceptable. 4d05h: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 4d05h: ISAKMP (0:3): processing NONCE payload. message ID = -1102788797 4d05h: ISAKMP (0:3): processing ID payload. message ID = -1102788797 4d05h: ISAKMP (0:3): processing ID payload. message ID = -1102788797 4d05h: ISAKMP (0:3): processing NOTIFY RESPONDER_LIFETIME protocol 3 spi 653862918, message ID = -1102788797, sa = 820ABFA0 4d05h: ISAKMP (0:3): processing responder lifetime 4d05h: ISAKMP (3): responder lifetime of 28800s 4d05h: ISAKMP (3): responder lifetime of 0kb 4d05h: IPSEC(key_engine): got a queue event... 4d05h: IPSEC(initialize_sas): , (key eng. msg.) INBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 28800s and 0kb, spi= 0x3C77C53D(1014482237), conn_id= 2000, keysize= 0, flags= 0x4 4d05h: IPSEC(initialize_sas): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= **192.168.254.0**/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 28800s and 0kb, spi= 0x502A71B5(1344958901), conn_id= 2001, keysize= 0, flags= 0xC 4d05h: IPSEC(create_sa): sa created, (sa) sa_dest= 172.16.172.46, sa_prot= 50, sa_spi= **0x3C77C53D(1014482237)**, *!--- SPI that is used on inbound SA.* sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2000 4d05h: IPSEC(create_sa): sa created, (sa) sa_dest= 172.16.172.41, sa_prot= 50, sa_spi= **0x502A71B5(1344958901)**, *!--- SPI that is used on outbound SA.* sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001 4d05h: ISAKMP (0:3): Creating IPsec SAs 4d05h: inbound SA from 172.16.172.41 to 172.16.172.46 (proxy 0.0.0.0 to 192.168.253.0) 4d05h: has spi 0xA8C469EC and conn_id 2002 and flags 4 4d05h: lifetime of 28800 seconds 4d05h: outbound SA from 172.16.172.46 to 172.16.172.41 (proxy 192.168.253.0 to 0.0.0.0) 4d05h: has spi 653862918 and conn_id 2003 and flags C 4d05h: lifetime of 28800 seconds 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): deleting node -1102788797 error FALSE reason "" 4d05h: ISAKMP (0:3): Node -1102788797, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE 4d05h: ISAKMP: received ke message (4/1) 4d05h: ISAKMP: Locking CONFIG struct 0x81F433A4 for crypto_ikmp_config_handle_kei_mess, count 3 4d05h: EZVPN(SJVPN): Current State: SS_OPEN 4d05h: EZVPN(SJVPN): Event: MTU_CHANGED 4d05h: EZVPN(SJVPN): No state change 4d05h: IPSEC(key_engine): got a queue event... 4d05h: IPSEC(initialize_sas): , (key eng. msg.) INBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 28800s and 0kb, spi= 0xA8C469EC(2831444460), conn_id= 2002, keysize= 0, flags= 0x4 4d05h: IPSEC(initialize_sas): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= **192.168.253.0**/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 28800s and 0kb, spi= 0x26F92806(653862918), conn_id= 2003, keysize= 0, flags= 0xC 4d05h: IPSEC(create_sa): sa created, (sa) sa_dest= 172.16.172.46, sa_prot= 50, sa_spi= **0xA8C469EC(2831444460)**, sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002 4d05h: IPSEC(create_sa): sa created, (sa) sa_dest= 172.16.172.41, sa_prot= 50, sa_spi= **0x26F92806(653862918)**, sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2003 4d05h: ISAKMP: received ke message (4/1) 4d05h: ISAKMP: Locking CONFIG struct 0x81F433A4 for crypto_ikmp_config_handle_kei_mess, count 4 4d05h: EZVPN(SJVPN): Current State: SS_OPEN 4d05h: EZVPN(SJVPN): Event: SOCKET_UP 4d05h: ezvpn_socket_up 4d05h: EZVPN(SJVPN): New State: IPSEC_ACTIVE 4d05h: EZVPN(SJVPN): Current State: IPSEC_ACTIVE 4d05h: EZVPN(SJVPN): Event: MTU_CHANGED

```
4d05h: EZVPN(SJVPN): No state change
4d05h: EZVPN(SJVPN): Current State: IPSEC_ACTIVE
4d05h: EZVPN(SJVPN): Event: SOCKET_UP
4d05h: ezvpn_socket_up
4d05h: EZVPN(SJVPN): No state change
```

[トラブルシューティングのための関連Cisco IOS showコマンド](#)

```
1721-1(ADSL)#show crypto ipsec client ezvpn
```

```
Tunnel name : SJVPN
Inside interface list: Loopback0, Loopback1,
Outside interface: FastEthernet0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
1721-1(ADSL)#show crypto isakmp sa
```

dst	src	state	conn-id	slot
172.16.172.41	172.16.172.46	QM_IDLE	3	0

```
1721-1(ADSL)#show crypto ipsec sa
```

```
interface: FastEthernet0
  Crypto map tag: FastEthernet0-head-0, local addr. 172.16.172.46
  local ident (addr/mask/prot/port): (192.168.253.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

  current_peer: 172.16.172.41
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 100, #pkts encrypt: 100, #pkts digest 100
    #pkts decaps: 100, #pkts decrypt: 100, #pkts verify 100
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

  local crypto endpt.: 172.16.172.46, remote crypto endpt.: 172.16.172.41
  path mtu 1500, media mtu 1500
  current outbound spi: 26F92806
```

```
inbound esp sas:
```

```
  spi: 0xA8C469EC(2831444460)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2002, flow_id: 3, crypto map: FastEthernet0-head-0
    sa timing: remaining key lifetime (k/sec): (4607848/28656)
    IV size: 8 bytes
    replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
```

```
  spi: 0x26F92806(653862918)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2003, flow_id: 4, crypto map: FastEthernet0-head-0
    sa timing: remaining key lifetime (k/sec): (4607848/28647)
    IV size: 8 bytes
    replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:

local ident (addr/mask/prot/port): (192.168.254.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 172.16.172.41
PERMIT, flags={origin_is_acl,}
#pkts encaps: 105, #pkts encrypt: 105, #pkts digest 105
#pkts decaps: 105, #pkts decrypt: 105, #pkts verify 105
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
local crypto endpt.: 172.16.172.46, remote crypto endpt.: 172.16.172.41
path mtu 1500, media mtu 1500
current outbound spi: 502A71B5
```

```
inbound esp sas:
spi: 0x3C77C53D(1014482237)
transform: esp-3des esp-md5-hmac ,
in use settings = {Tunnel, }
slot: 0, conn id: 2000, flow_id: 1, crypto map: FastEthernet0-head-0
sa timing: remaining key lifetime (k/sec): (4607847/28644)
IV size: 8 bytes
replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
spi: 0x502A71B5(1344958901)
transform: esp-3des esp-md5-hmac ,
in use settings = {Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: FastEthernet0-head-0
sa timing: remaining key lifetime (k/sec): (4607847/28644)
IV size: 8 bytes
replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

[アクティブなトンネルのクリア](#)

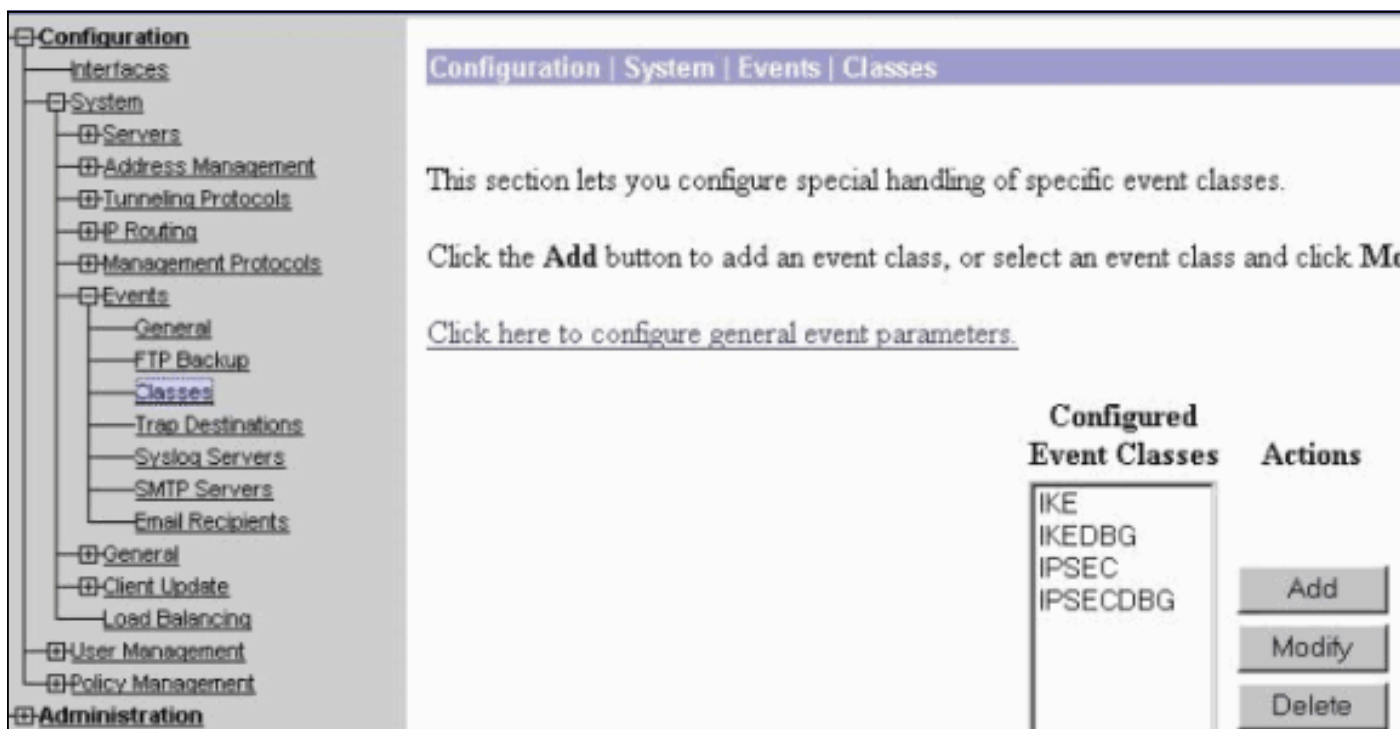
次のコマンドを使用して、トンネルをクリアできます。

- **clear crypto isakmp**
- **clear crypto sa**
- **clear crypto ipsec client ezvpn**

注：VPNコンセントレータを使用してセッションをログアウトするには、[Administration] > [Admin Sessions]の順に選択し、[Remote Access Session]でユーザを選択して[logout]をクリックします。

[VPN 3000 コンセントレータのデバッグ](#)

イベント接続の障害が発生した場合には、[Configuration] > [System] > [Events] > [Classes]の順に選択して、このデバッグを有効にします。表示されているクラスが問題の特定に役立たない場合は、常にクラスを追加できます。



メモリ内の現在のイベントログを表示するには、[Monitoring] > [Filterable Event log]を選択し、イベントクラス、重大度、IPアドレスなどでフィルタ可能にします。



IPsecプロトコルの統計情報を表示するには、[Monitoring] > [Statistics] > [IPSec]を選択します。このウィンドウには、VPNコンセントレータが最後に起動またはリセットされてから、現在のIPsecトンネルを含むIPsecアクティビティの統計情報が表示されます。これらの統計情報は、IPsecフローモニタリングMIBのIETFドラフトに準拠しています。[Monitoring] > [Sessions] > [Detail]ウィンドウにもIPsecデータが表示されます。

IKE (Phase 1) Statistics		IPSec (Phase 2) Statistics	
Active Tunnels	1	Active Tunnels	2
Total Tunnels	122	Total Tunnels	362
Received Bytes	2057442	Received Bytes	0
Sent Bytes	332256	Sent Bytes	1400
Received Packets	3041	Received Packets	0
Sent Packets	2128	Sent Packets	5
Received Packets Dropped	1334	Received Packets Dropped	0
Sent Packets Dropped	0	Received Packets Dropped (Anti-Replay)	0
Received Notifies	15	Sent Packets Dropped	0
Sent Notifies	254	Inbound Authentications	0
Received Phase-2 Exchanges	362		

不具合の原因

- Cisco IOSルータがAG_INIT_EXCH状態のままになる。トラブルシューティングを行う際は、次のコマンドを使用してIPSecおよびISAKMPデバッグをオンにします。debug crypto ipsecdebug crypto isakmpdebug crypto ezvpnCisco IOSルータでは、次のように表示されま

```

5d16h: ISAKMP (0:9): beginning Aggressive Mode exchange
5d16h: ISAKMP (0:9): sending packet to 10.48.66.115 (I) AG_INIT_EXCH
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH...
5d16h: ISAKMP (0:9): incrementing error counter on sa: retransmit phase 1
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH
5d16h: ISAKMP (0:9): sending packet to 10.48.66.115 (I) AG_INIT_EXCH
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH...
5d16h: ISAKMP (0:9): incrementing error counter on sa: retransmit phase 1
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH
5d16h: ISAKMP (0:9): sending packet to 10.48.66.115 (I) AG_INIT_EXCH
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH...
5d16h: ISAKMP (0:9): incrementing error counter on sa: retransmit phase 1
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH
5d16h: ISAKMP (0:9): sending packet to 10.48.66.115 (I) AG_INIT_EXCH

```

VPN 3000コンセントレータでは、Xauthが必要です。ただし、選択されたプロポーザルはXauthをサポートしていません。Xauthの内部認証が指定されていることを確認します。内部認証を有効にし、前のスクリーンショットのように、IKEプロポーザルの認証モードがPreshared Keys (Xauth)に設定されていることを確認します。[Modify]をクリックして、提案を編集します。

- パスワードが正しくありません。Cisco IOSルータに「Invalid Password」メッセージが表示されません。VPNコンセントレータで、Received unexpected event EV_ACTIVATE_NEW_SA in state AM_TM_INIT_XAUTHと表示される場合があります。パスワードが正しいことを確認します。
- ユーザ名が正しくない。Cisco IOSルータで、パスワードが間違っている場合は、次のようなデバッグが表示されます。VPNコンセントレータでAuthentication rejected:理由=ユーザーが見つかりませんでした。

関連情報

- [Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ](#)
- [Cisco Easy VPNリモートフェーズII](#)
- [Cisco VPN 3000 シリーズ クライアントに関するサポート ページ](#)
- [IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)