EzVPN with NEM on IOS Router with VPN 3000 Concentrator Configuration Example

Document ID: 19291

Contents

Introduction

This document explains the procedure you use in order to configure a Cisco IOS® router as an EzVPN in Network Extension Mode (NEM) to connect to a Cisco VPN 3000 Concentrator. A new EzVPN Phase II feature is the support of a basic Network Address Translation (NAT) configuration. The EzVPN Phase II is derived from the Unity Protocol (VPN Client software). The remote device is always the initiator of the IPsec tunnel. However, Internet Key Exchange (IKE) and IPsec proposals are not configurable on the EzVPN Client. The VPN Client negotiates proposals with the server.

In order to configure IPsec between a PIX/ASA 7.x and a Cisco 871 router using Easy VPN, refer to PIX/ASA 7.x Easy VPN with an ASA 5500 as the Server and Cisco 871 as the Easy VPN Remote Configuration Example.

In order to configure IPsec between the Cisco IOS® Easy VPN Remote Hardware Client and the PIX Easy VPN Server, refer to IOS Easy VPN Remote Hardware Client to a PIX Easy VPN Server Configuration Example.

In order to configure a Cisco 7200 Router as an EzVPN and the Cisco 871 Router as the Easy VPN Remote, refer to 7200 Easy VPN Server to 871 Easy VPN Remote Configuration Example.

Prerequisites

Requirements

Before you attempt this configuration check that the Cisco IOS router supports the EzVPN Phase II feature and has the IP connectivity with end−to−end connections to establish the IPsec tunnel.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS Software Release 12.2(8)YJ (EzVPN Phase II)
- VPN 3000 Concentrator 3.6.x
- Cisco 1700 Router

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Note: This configuration was recently tested with a Cisco 3640 Router with Cisco IOS Software Release 12.4(8) and the VPN 3000 Concentrator 4.7.x version.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.
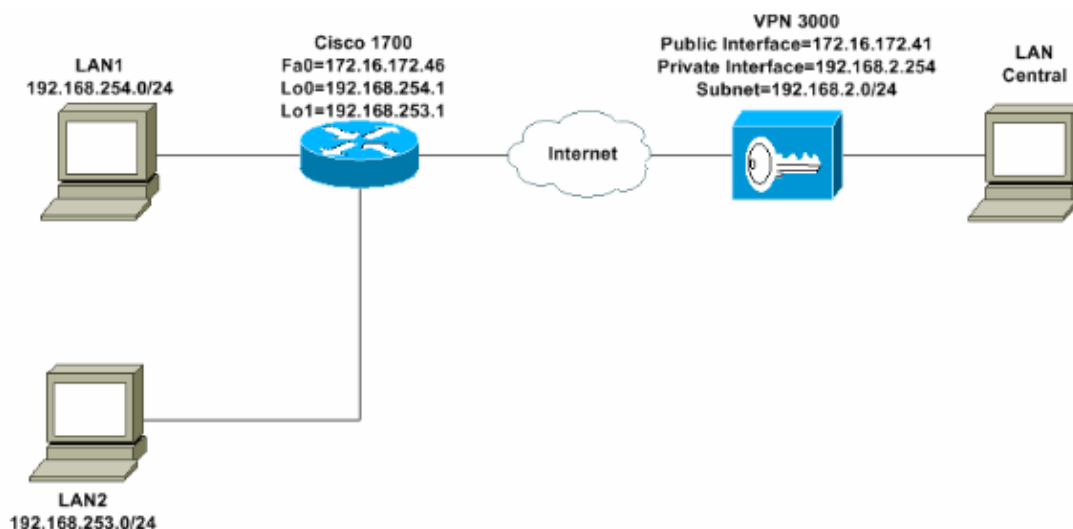
Configure the VPN 3000 Concentrator

Task

In this section, you are presented with the information to configure the VPN 3000 Concentrator.

Network Diagram

This document uses the network setup shown in this diagram. Loopback interfaces are used as internal subnets, and FastEthernet 0 is the default to the Internet.
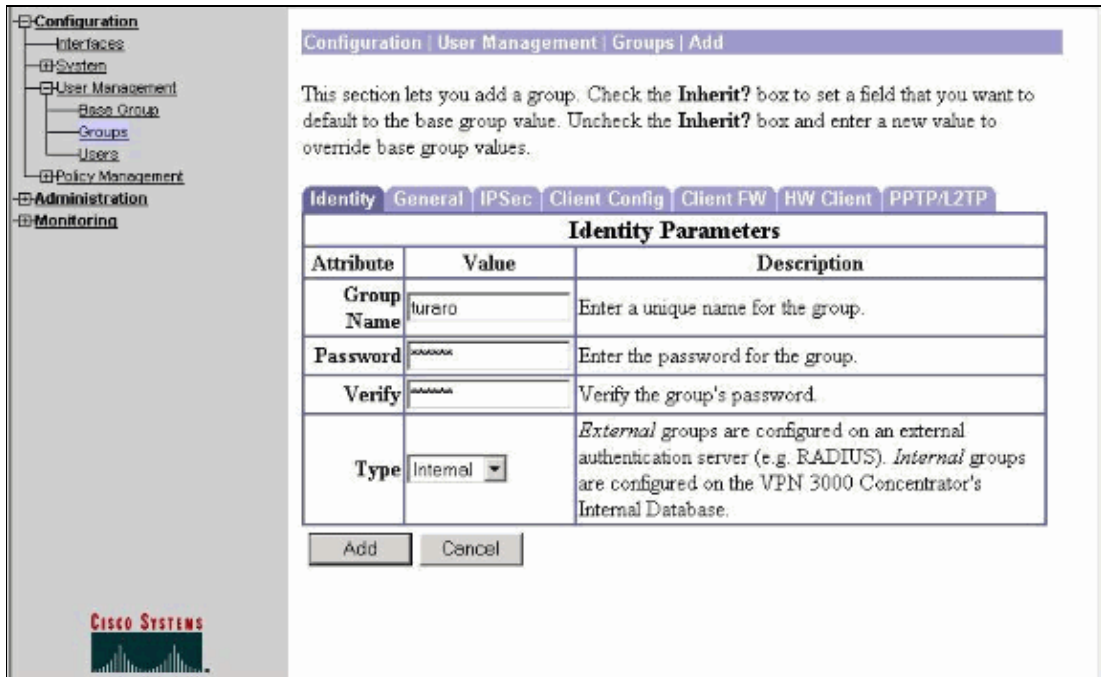
Step by Step Instructions

Complete these steps:

1. Choose **Configuration** > **User Management** > **Groups** > **Add** and define a group name and password in order to configure an IPsec group for the users.

   This example uses the group name **turaro** with password/verify **tululo**.

2. Choose **Configuration** > **User Management** > **Groups** > **turaro** > **General** to enable **IPSec** and disable Point–to–Point Tunneling Protocol (PPTP) and Layer 2 Tunnel Protocol (L2TP).

   Make your selections and click **Apply**.

Attribute	Value	Inherit?	
Access Hours	-No Restrictions-	☑	Sele
Simultaneous Logins	3	☑	Ente
Minimum Password Length	8	☑	Ente
Allow Alphabetic-Only Passwords	☑	☑	Ente / be a
Idle Timeout	30	☑	(min
Maximum Connect Time	0	☑	(min
Filter	–None–	☑	Ente
Primary DNS		☑	Ente
Secondary DNS		☑	Ente
Primary WINS		☑	Ente
Secondary WINS		☑	Ente
SEP Card Assignment	☑ SEP 1 ☑ SEP 2 ☑ SEP 3 ☑ SEP 4	☑	Sele
Tunneling Protocols	☐ PPTP ☐ L2TP ☑ IPSec	☐	Sele

3. Set Authentication to **Internal** for Extended Authentication (Xauth) and ensure that the Tunnel Type is **Remote Access** and the IPSec SA is **ESP−3DES−MD5**.

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.

IPSec Parameters

Attribute	Value	Inherit?	
IPSec SA	ESP-3DES-MD5	☑	S
IKE Peer Identity Validation	If supported by certificate	☑	S / t
IKE Keepalives	☑	☑	C / u
Reauthentication on Rekey	☐	☑	C / C
Tunnel Type	Remote Access	☑	S / t

Remote Access Parameters

Group Lock	☐	☑	I
Authentication	Internal	☑	S / g

4. Choose **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals** in order to make sure that the Cisco VPN Client (CiscoVPNClient−3DES−MD5) is in Active Proposals for IKE (Phase 1).

Note: From VPN Concentrator 4.1.x, the procedure is different for ensuring that the Cisco VPN Client is in the list of Active Proposals for IKE (phase 1). Choose **Configuration > Tunneling and Security > IPSec > IKE Proposals.**
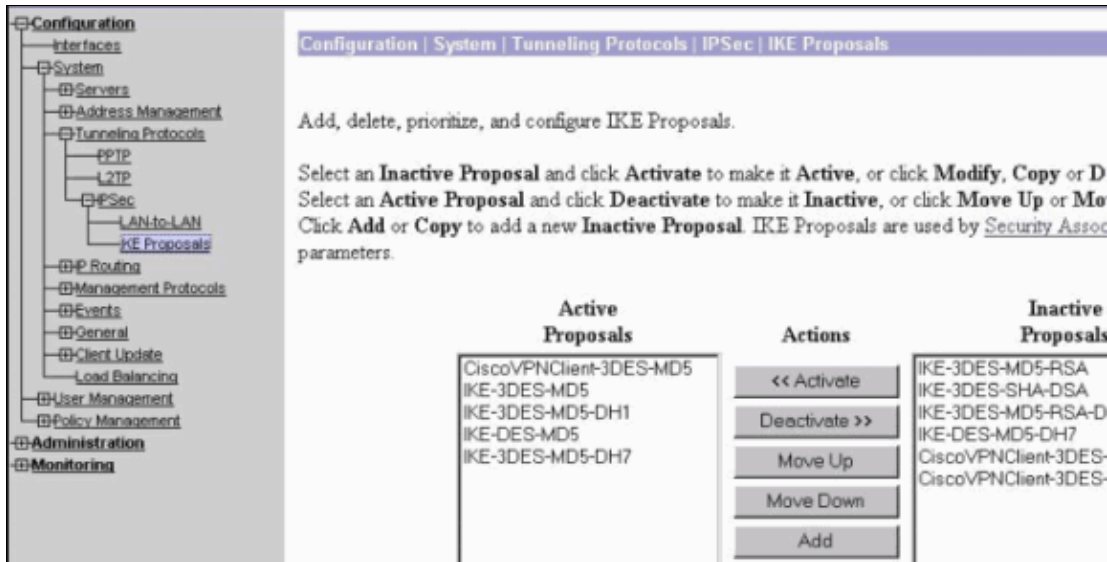
5. Verify your IPsec Security Association (SA).

On step 3 your IPsec SA is ESP–3DES–MD5. You can create a new one if you wish but make sure you use the correct IPsec SA on your group. You should disable Perfect Forward Secrecy (PFS) for the IPsec SA that you use. Select the Cisco VPN Client as the IKE proposal by choosing **Configuration** > **Policy Management** > **Traffic Management** > **SAs**. Type the SA name in the text box and make the appropriate selections as shown here:
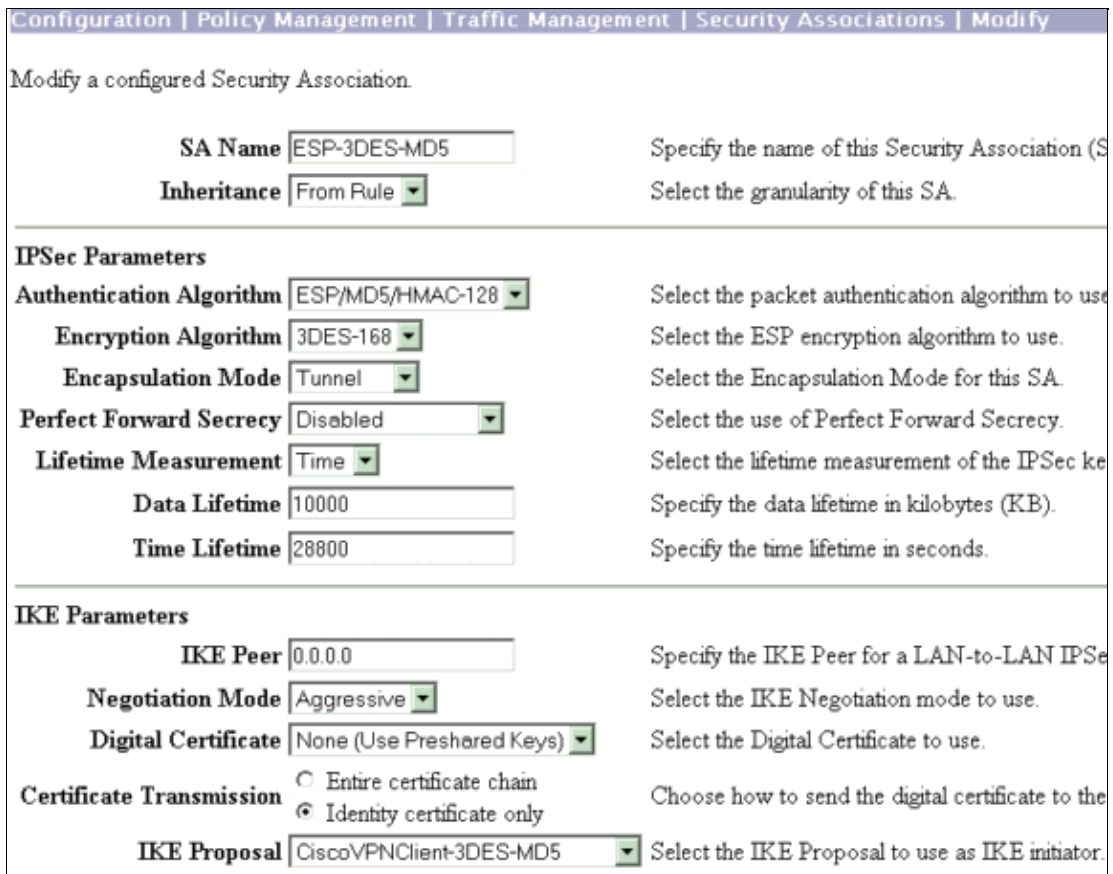
Note: This step and the next step are optional if you prefer to choose a pre–defined SA. If your client has a dynamically assigned IP address, use 0.0.0.0 in the IKE peer text box. Make ensure that IKE Proposal is set to **CiscoVPNClient–3DES–MD5** as this example shows.

6. You must **not** click *Allow the networks in the list to bypass the tunnel*. The reason is that split tunneling is supported, but the bypass feature is not supported with the EzVPN Client feature.

7. Choose **Configuration** > **User Management** > **Users** in order to add a user. Define a user name and password, assign it to a group, and click **Add**.

8. Choose **Administration > Admin Sessions** and check that the user is connected. In NEM, the VPN Concentrator does not assign an IP address from the pool.

   Note: This step is optional if you prefer to choose a predefined SA.

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. Click either the **Save Needed** or **Save** icon in order to save the configuration.

Router Configuration

show version Output

```
show version
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-BK9NO3R2SY7-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
```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Once you configure both devices, the Cisco 3640 router attempts to set up the VPN tunnel by contacting the VPN Concentrator automatically using the peer IP address. After the initial ISAKMP parameters are exchanged, the router displays this message:

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

You have to enter the **crypto ipsec client ezvpn xauth** command which prompts you for a username and password. This should match the username and password configured on the VPN Concentrator (step 7). Once the username and password are agreed by both peers, the rest of the parameters are agreed and the IPsec VPN tunnel comes up.

```
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
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you issue **debug** commands.

- **debug crypto ipsec client ezvpn** Displays information that shows the configuration and implementation of the EzVPN Client feature.
- **debug crypto ipsec** Displays debug information about IPsec connections.
- **debug crypto isakmp** Displays debug information about IPsec connections, and shows the first set of attributes that are denied due to incompatibilities on both ends.
- **show debug** Displays the state of each debugging option.

Output from Debug Commands

As soon as you enter the **crypto ipsec client ezvpn SJVPN** command, the EzVPN Client attempts to connect to the server. If you change the **connect manual** command under the group configuration, enter the **crypto ipsec client ezvpn connect SJVPN** command to initiate the exchange of proposals to the server.

```
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_MESG_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_MESG_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_MESG_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 = -1602
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_MESG_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_MESG_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_MESG_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_MESG_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_MESG_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
```

Related Cisco IOS show Commands for Troubleshooting

```
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:
```

Clear an Active Tunnel

You can clear the tunnels with these commands:

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

Note: You can use the VPN Concentrator in order to logout of the session when you choose **Administration > Admin Sessions**, select the user in **Remote Access Session** and click **logout**.

VPN 3000 Concentrator Debug

Choose **Configuration > System > Events > Classes** in order to enable this debug if there are event connection failures. You can always add more classes if the ones shown do not help you identify the problem.
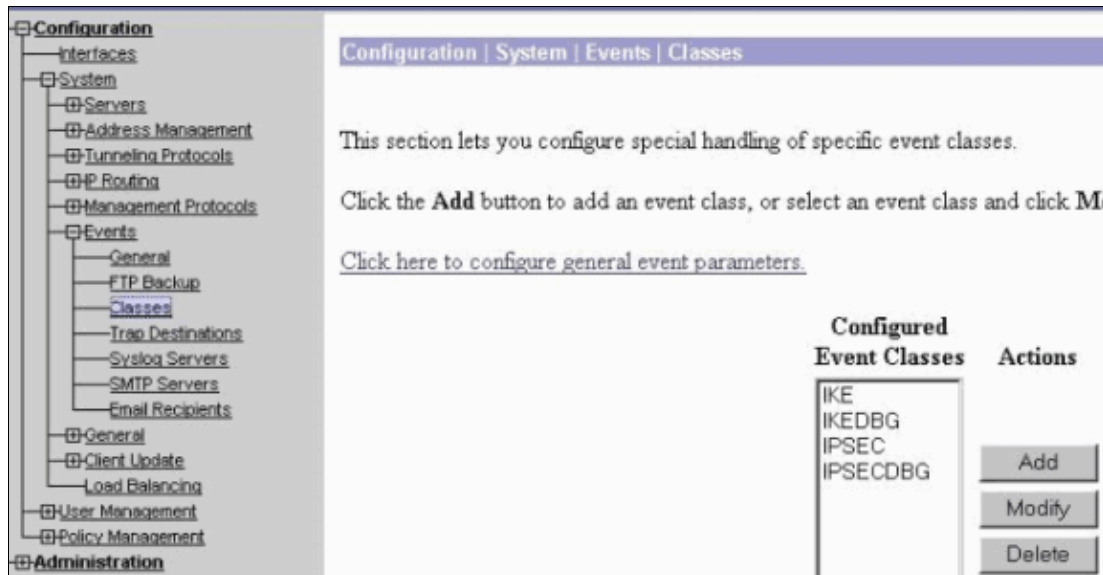
In order to view the current event log in memory, filterable by event class, severity, IP address, and so forth, choose **Monitoring > Filterable Event log**.
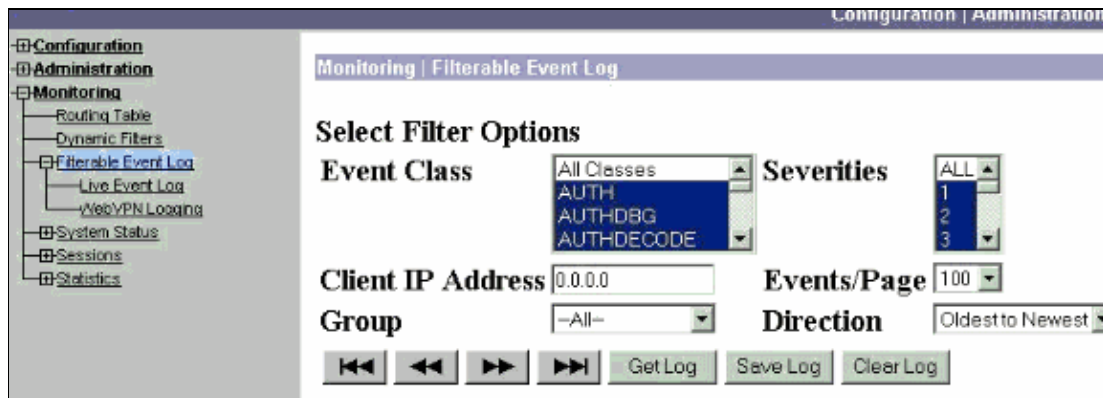
In order to view the statistics of the IPsec protocol, choose **Monitoring > Statistics > IPSec.** This window shows statistics for IPsec activity, including current IPsec tunnels, on the VPN Concentrator since it was last booted or reset. These statistics conform to the IETF draft for the IPsec Flow Monitoring MIB. The **Monitoring > Sessions > Detail** window also shows IPsec data.

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 Notifies	254	Sent Packets Dropped	0
Received Phase-2 Exchanges	362	Inbound Authentications	0

What Can Go Wrong

- The Cisco IOS router gets stuck in the AG_INIT_EXCH state. While you troubleshoot, turn on IPsec and ISAKMP debugs with these commands:

    - **debug crypto ipsec**
    - **debug crypto isakmp**
    - **debug crypto ezvpn**
  On the Cisco IOS router, you see this:

    ```
    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
    ```

  On the VPN 3000 Concentrator, Xauth is required. However, the selected proposal does not support Xauth. Verify that the internal authentication for Xauth is specified. Enable internal authentication and ensure that the IKE proposals have the authentication mode set to **Preshared Keys (Xauth)**, as in the previous screenshot. Click **Modify** in order to edit the proposal.
- The password is incorrect.

  You do not see the **Invalid Password** message on the Cisco IOS router. On the VPN Concentrator, you might see **Received unexpected event EV_ACTIVATE_NEW_SA in state AM_TM_INIT_XAUTH**.

  Ensure your password is correct.
- The username is incorrect.

On the Cisco IOS router you see a debug similar to this if you have the wrong password. On the VPN Concentrator you see **Authentication rejected: Reason = User was not found**.

Related Information

- **Cisco VPN 3000 Series Concentrator Support Page**
- **Cisco Easy VPN Remote Phase II**
- **Cisco VPN 3000 Series Client Support Page**
- **IPsec Negotiation/IKE Protocols Support Page**
- **Technical Support & Documentation – Cisco Systems**