

# Exemple de configuration de EzVPN avec NEM sur routeur IOS avec concentrateur VPN 3000

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez le concentrateur VPN 3000](#)

[Tâche](#)

[Diagramme du réseau](#)

[Instructions pas à pas](#)

[Configuration du routeur](#)

[Vérifiez](#)

[Dépannez](#)

[Dépannage des commandes](#)

[Sortie des commandes de debug](#)

[Commandes show de Cisco IOS relatives pour le dépannage](#)

[Debug de concentrateur VPN 3000](#)

[Causes de problèmes potentiels](#)

[Informations connexes](#)

## Introduction

Ce document explique la procédure que vous utilisez afin de configurer un routeur de Cisco IOS® comme EzVPN dans le [mode d'extension réseau \(PAS MENTIONNÉ AILLEURS\)](#) pour se connecter à un concentrateur de Cisco VPN 3000. Une nouvelle caractéristique de la phase II d'EzVPN est le support d'une configuration de base de Traduction d'adresses de réseau (NAT). La phase II d'EzVPN est dérivée de l'Unity Protocol (logiciel de client VPN). Le périphérique distant est toujours le demandeur du tunnel d'IPsec. Cependant, les propositions d'Échange de clés Internet (IKE) et d'IPsec ne sont pas configurables sur le client d'EzVPN. Le client vpn est en pourparlers des propositions avec le serveur.

Afin de configurer IPsec entre un PIX/ASA 7.x et un routeur de Cisco 871 utilisant l'Easy VPN, référez-vous à l'[Easy VPN PIX/ASA 7.x avec une ASA 5500 en tant que le serveur et Cisco 871 comme exemple de configuration d'Easy VPN distant](#).

Afin de configurer IPsec entre le client matériel d'Easy VPN Remote de Cisco IOS® et le serveur PIX Easy VPN, référez-vous au [client matériel d'IOS Easy VPN Remote à un exemple de configuration de serveur PIX Easy VPN](#).

Afin de configurer un routeur Cisco 7200 comme EzVPN et le routeur Cisco 871 comme Easy VPN distant, consultez [Exemple de configuration distante du serveur Easy VPN 7200 sur Easy VPN 871](#).

## Conditions préalables

### Conditions requises

Avant que vous tentiez ce contrôle de configuration que le routeur Cisco IOS prend en charge la [caractéristique de la phase II d'EzVPN](#) et a la connectivité IP avec des connexions de bout en bout pour établir le tunnel d'IPsec.

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco IOS version 12.2(8)YJ (phase d'EzVPN II)
- Concentrateur VPN 3000 3.6.x
- Routeur de Cisco 1700

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

**Note:** Cette configuration a été récemment testée avec un routeur de Cisco 3640 avec la version du logiciel Cisco IOS 12.4(8) et la version du concentrateur VPN 3000 4.7.x.

### Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

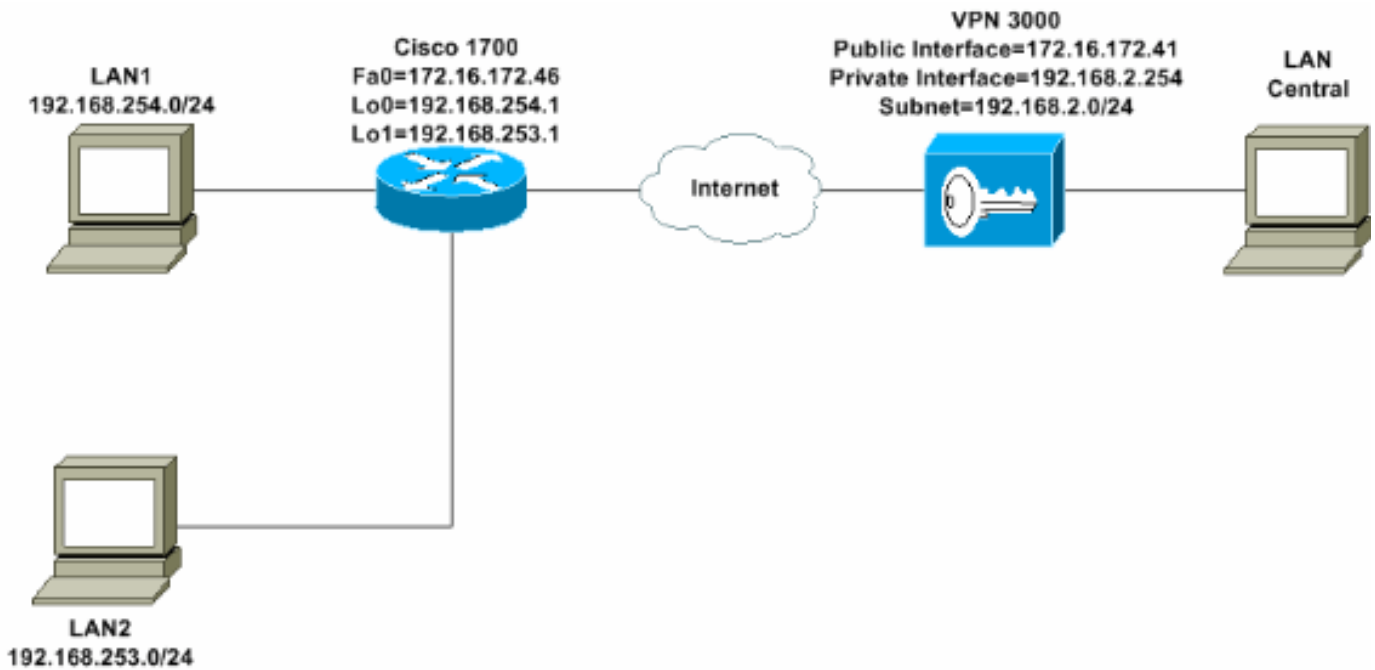
## Configurez le concentrateur VPN 3000

### Tâche

Dans cette section, vous êtes présenté avec les informations pour configurer le concentrateur VPN 3000.

### Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant. Des interfaces de bouclage sont utilisées en tant que sous-réseaux internes, et FastEthernet 0 est le par défaut à l'Internet.



## Instructions pas à pas

Procédez comme suit :

1. Choisissez le **Configuration > User Management > Groups > ajoutent** et définissent un nom et un mot de passe de groupe afin de configurer un groupe d'IPsec pour les utilisateurs. Cet exemple utilise le **turaro** de nom de groupe avec le mot de passe/vérifie le **tululo**.

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.

Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

Identity Parameters		
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.

2. Choisissez le **Configuration > User Management > Groups > le turaro > le général** pour activer IPsec et pour désactiver le Protocole PPTP (Point-to-Point Tunneling Protocol) et pour poser 2 protocol (L2TP) de tunnel. Faites vos sélections et cliquez sur Apply.

- [-] 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"/>	(min
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(min
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. Placez l'authentification à **interne** pour l'authentification étendue (Xauth) et assurez-vous que le type de tunnel est **Accès à distance** et IPSec SA est **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.

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. Choisissez la configuration > les protocoles de système > de Tunnellisation > l'IPSec > les propositions d'IKE afin de s'assurer que le Client VPN Cisco (CiscoVPNClient-3DES-MD5) est dans des propositions actives pour l'IKE (phase 1). **Note:** Du concentrateur 4.1.x VPN, la procédure est différente pour s'assurer que le Client VPN Cisco est dans la liste de propositions actives pour l'IKE (phase 1). Choisissez la configuration > le Tunnellisation et la Sécurité > l'IPSec > les propositions d'IKE.

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. Vérifiez votre association de sécurité IPSec (SA). Sur l'étape 3 votre IPsec SA est ESP-3DES-MD5. Vous pouvez créer un neuf si vous souhaitez mais vous assurez que vous utilisez IPsec correct SA sur votre groupe. Vous devriez désactiver le perfect forward secrecy (PFS) pour IPsec SA que vous utilisez. Sélectionnez le Client VPN Cisco comme proposition

d'IKE en choisissant la **configuration** > la **Gestion des stratégies** > la **gestion de trafic** > la **SAS**. Introduisez le nom SA dans la zone de texte et faites les sélections appropriées comme affiché ici

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

Modify a configured Security Association.

<b>SA Name</b>	<input type="text" value="ESP-3DES-MD5"/>	Specify the name of this Security Association (S
<b>Inheritance</b>	<input type="text" value="From Rule"/>	Select the granularity of this SA.

---

**IPSec Parameters**

<b>Authentication Algorithm</b>	<input type="text" value="ESP/MD5/HMAC-128"/>	Select the packet authentication algorithm to use
<b>Encryption Algorithm</b>	<input type="text" value="3DES-168"/>	Select the ESP encryption algorithm to use.
<b>Encapsulation Mode</b>	<input type="text" value="Tunnel"/>	Select the Encapsulation Mode for this SA.
<b>Perfect Forward Secrecy</b>	<input type="text" value="Disabled"/>	Select the use of Perfect Forward Secrecy.
<b>Lifetime Measurement</b>	<input type="text" value="Time"/>	Select the lifetime measurement of the IPSec ke
<b>Data Lifetime</b>	<input type="text" value="10000"/>	Specify the data lifetime in kilobytes (KB).
<b>Time Lifetime</b>	<input type="text" value="28800"/>	Specify the time lifetime in seconds.

---

**IKE Parameters**


<b>IKE Peer</b>	<input type="text" value="0.0.0.0"/>	Specify the IKE Peer for a LAN-to-LAN IPSe
<b>Negotiation Mode</b>	<input type="text" value="Aggressive"/>	Select the IKE Negotiation mode to use.
<b>Digital Certificate</b>	<input type="text" value="None (Use Preshared Keys)"/>	Select the Digital Certificate to use.
<b>Certificate Transmission</b>	<input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the
<b>IKE Proposal</b>	<input type="text" value="CiscoVPNClient-3DES-MD5"/>	Select the IKE Proposal to use as IKE initiator.

**Note:** Cette étape et l'étape suivante sont facultatives si vous préférez choisir SA prédéfinie. Si votre client a une adresse IP dynamiquement assignée, utilisez 0.0.0.0 dans la zone de texte de pair d'IKE. Make s'assurent que la proposition d'IKE est placée au comme indiqué dans cet exemple **CiscoVPNClient-3DES-MD5**.

- Vous ne devez pas cliquer sur *permettez aux réseaux dans la liste pour sauter le tunnel*. La raison est que la Segmentation de tunnel est prise en charge, mais la caractéristique de contournement n'est pas prise en charge avec la fonctionnalité client d'EzVPN.

<ul style="list-style-type: none"> <li>[-] Configuration <ul style="list-style-type: none"> <li>[-] Interfaces</li> <li>[-] System</li> <li>[-] User Management <ul style="list-style-type: none"> <li>[-] Base Group</li> <li>[-] Groups</li> <li>[-] Users</li> </ul> </li> <li>[-] Policy Management</li> </ul> </li> <li>[-] Administration</li> <li>[-] Monitoring</li> </ul>	Banner		<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	-None-	<input checked="" type="checkbox"/>

7. Choisissez le **Configuration > User Management > les utilisateurs** afin d'ajouter un utilisateur. Définissez un nom d'utilisateur et un mot de passe, assignez-le à un groupe, et cliquez sur Add.

<ul style="list-style-type: none"> <li>[-] Configuration <ul style="list-style-type: none"> <li>[-] Interfaces</li> <li>[-] System</li> <li>[-] User Management <ul style="list-style-type: none"> <li>[-] Base Group</li> <li>[-] Groups</li> <li>[-] Users</li> </ul> </li> <li>[-] Policy Management</li> </ul> </li> <li>[-] Administration</li> <li>[-] Monitoring</li> </ul>	Configuration   User Management   Users   Add		
	<p>This section lets you add a user. Uncheck the <b>Inherit?</b> box and enter a new value to override group values.</p>		
	<p>Identity    General    IPsec    PPTP/L2TP</p>		
	<b>Identity Parameters</b>		
	<b>Attribute</b>	<b>Value</b>	<b>Description</b>
	Username	podma	Enter a unique username.
Password	XXXXXXXXXX	Enter the user's password. The password must satisfy the group password requirements.	
Verify	XXXXXXXXXX	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.	
<input type="button" value="Add"/> <input type="button" value="Cancel"/>			
			

8. Choisissez les **sessions de gestion > d'admin** et vérifiez que l'utilisateur est connecté. Dans PAS MENTIONNÉ AILLEURS, le concentrateur VPN n'assigne pas une adresse IP du groupe. **Note:** Cette étape est facultative si vous préférez choisir prédéfinis 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. Cliquez sur la **sauvegarde** icône **requis** ou de **sauvegarde** afin de sauvegarder la configuration.

## Configuration du routeur

### sortie de show version

#### **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

```

## Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'[Outil Interpréteur de sortie](#) (clients [enregistrés](#) uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

Une fois que vous configurez les deux périphériques, le routeur de Cisco 3640 tente d'installer le tunnel VPN en contactant le concentrateur VPN automatiquement utilisant l'adresse IP de pair.

Une fois les paramètres ISAKMP initiaux permutés, le routeur affiche ce message :

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

Vous devez entrer la commande de **crypto ipsec client ezvpn xauth** qui demande un nom d'utilisateur et mot de passe. Ceci devrait apparier le nom d'utilisateur et mot de passe configuré sur le concentrateur VPN (étape 7). Une fois que le nom d'utilisateur et mot de passe sont convenus par les deux pairs, le reste des paramètres sont convenus et le tunnel VPN d'IPsec est soulevé.

```
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
```

## [Dépannez](#)

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

### [Dépannage des commandes](#)

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool](#) ([clients enregistrés](#) uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

**Note:** Reportez-vous à [Informations importantes sur les commandes de débogage](#) avant d'émettre des commandes **debug**.

- **EzVPN de client de debug crypto ipsec** — Affiche des informations qui affiche la configuration et l'implémentation de la fonctionnalité client d'EzVPN.
- **debug crypto ipsec** — Affiche des informations de débogage sur les connexions IPsec.
- **debug crypto isakmp** - Affiche les informations de débogage sur les connexions IPsec et le premier ensemble d'attributs refusés en raison d'incompatibilités sur les deux extrémités.
- **show debug** — Affiche l'état de chaque option d'élimination des imperfections.

### [Sortie des commandes de debug](#)

Dès que vous sélectionnez la **crypto** commande de l'**EzVPN SJVPN de client d'ipsec**, les tentatives de client d'EzVPN de se connecter au serveur. Si vous changez la commande **manuelle de connecter** sous la configuration de groupe, sélectionnez la commande du **crypto ipsec client ezvpn connect SJVPN** d'initier l'échange des propositions au serveur.

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_MSG_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_MSG_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\_MSG\_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\_MSG\_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\_MSG\_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\_MSG\_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\_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_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
```

## [Commandes show de Cisco IOS relatives pour le dépannage](#)

```
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:

### [Effacez un tunnel actif](#)

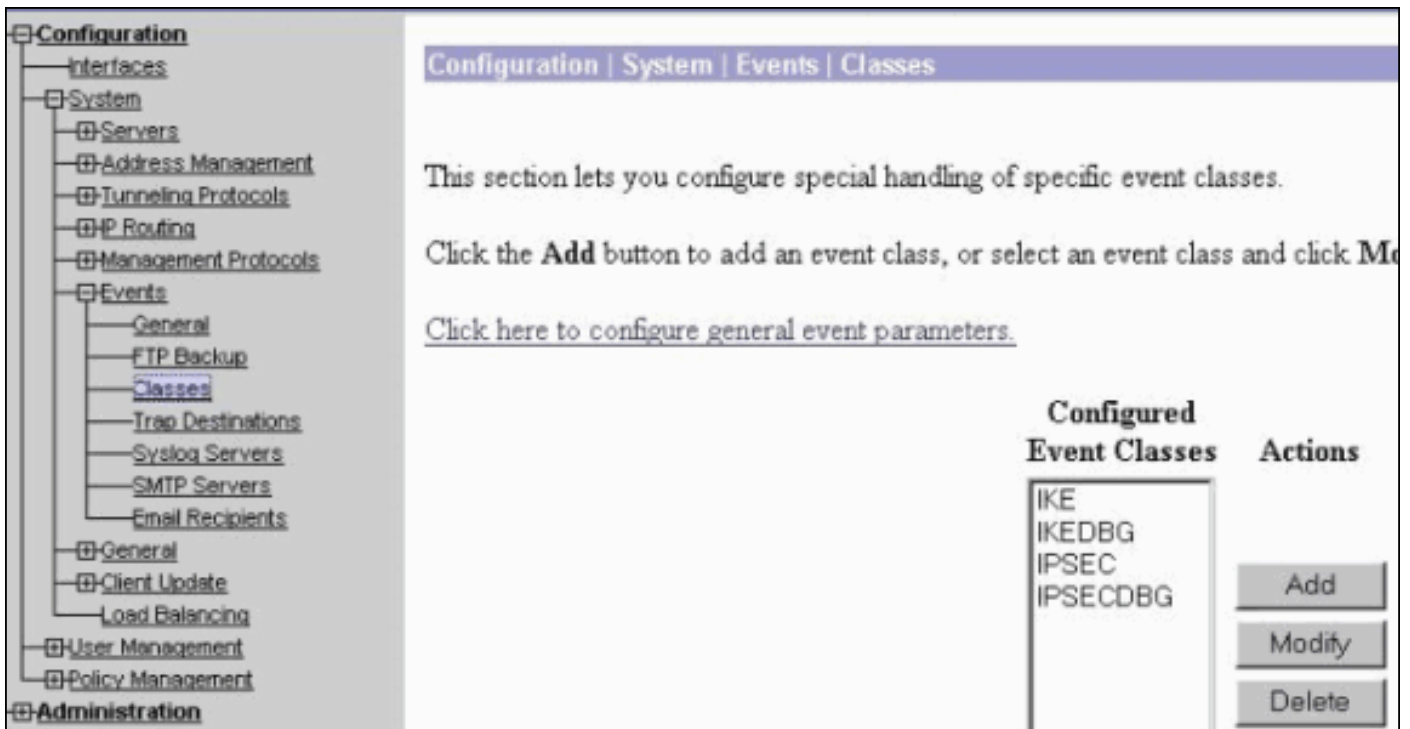
Vous pouvez effacer les tunnels avec ces commandes :

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

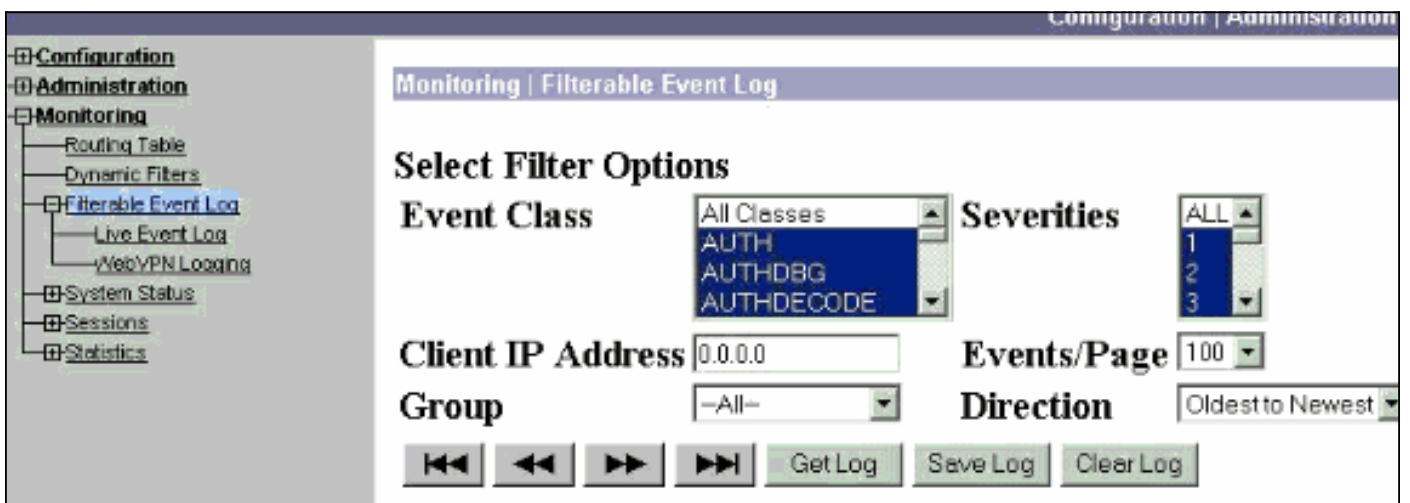
**Note:** Vous pouvez employer le concentrateur VPN afin de se déconnecter de la session quand vous choisissez des **sessions de gestion > d'admin**, sélectionnez l'utilisateur en **session d'Accès à distance** et cliquez sur la **déconnexion**.

### [Debug de concentrateur VPN 3000](#)

Choisissez la **configuration > le système > les événements > les classes** afin d'activer ceci mettent au point s'il y a des défaillances de connexion d'événement. Vous pouvez toujours ajouter plus de classes si celles affichées ne vous aident pas à identifier le problème.



Afin de visualiser la mémoire de procédure de connexion d'événement actuel, filtrable par la classe d'événement, la sévérité, adresse IP, et ainsi de suite, choisissez la **surveillance > le journal d'événements filtrables**.



Afin de visualiser les statistiques du protocole IPsec, choisissez la **surveillance > les statistiques > l'IPSec**. Cette fenêtre affiche des statistiques pour l'activité d'IPsec, y compris les tunnels en cours d'IPsec, sur le concentrateur VPN puisqu'elle a été pour la dernière fois amorcée ou remise. Ces les statistiques se conforment au projet soumis à l'IETF pour l'écoulement d'IPsec surveillant le MIB. La fenêtre de **Monitoring > Sessions > de détail** affiche également des données d'IPsec.

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		

## Causes de problèmes potentiels

- Le routeur Cisco IOS est bloqué dans l'état AG\_INIT\_EXCH. Tandis que vous dépannez, activez IPsec et l'ISAKMP met au point avec ces commandes : [debug crypto ipsecdebug crypto isakmp](#) EzVPN de [debug crypto](#) Sur le routeur Cisco IOS, vous voyez ceci :

```
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:

Sur le concentrateur VPN 3000, le Xauth est exigé. Cependant, la proposition sélectionnée ne prend en charge pas le Xauth. Vérifiez que l'[authentification interne pour le Xauth](#) est spécifiée. Activez l'authentification interne et assurez-vous que les propositions d'IKE ont l'authentification mode réglée aux **clés pré-partagées (Xauth)**, comme dans le [tir d'écran](#) précédent. Le clic **modifie** afin d'éditer la proposition.

- Le mot de passe est incorrect. Vous ne voyez pas le message de **mot de passe incorrect** sur le routeur Cisco IOS. Sur le concentrateur VPN, vous pourriez voir l'**événement inattendu reçu EV\_ACTIVATE\_NEW\_SA dans l'état AM\_TM\_INIT\_XAUTH**. Assurez que votre mot de passe est correct.
- Le nom d'utilisateur est incorrect. Sur le routeur Cisco IOS vous voyez un débogage semblable à ceci si vous avez le mot de passe incorrect. Sur le concentrateur VPN vous voyez l'**authentification rejetée : La raison = l'utilisateur n'ont pas été trouvés**.

## [Informations connexes](#)

- [Page d'assistance des concentrateurs VPN Cisco 3000](#)
- [Phase distante II de Solution Cisco Easy VPN](#)
- [Page d'assistance du Client VPN 3000 Series Cisco](#)
- [Page de support de la négociation IPSec/des protocoles IKE](#)
- [Support et documentation techniques - Cisco Systems](#)