

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configurer le concentrateur VPN 3000](#)

[Tâche](#)

[Diagramme du réseau](#)

[Instructions pas à pas](#)

[Configuration du routeur](#)

[Vérification](#)

[Dépannage](#)

[Dépannage des commandes](#)

[Sortie des commandes de débogage](#)

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

[Débogage du concentrateur VPN 3000](#)

[Causes de problèmes potentiels](#)

[Informations connexes](#)

[Introduction](#)

Ce document explique la procédure que vous utilisez pour configurer un routeur Cisco IOS® en tant qu'EzVPN en [mode d'extension de réseau \(NEM\)](#) pour la connexion à un concentrateur Cisco VPN 3000. Une nouvelle fonctionnalité EzVPN Phase II est la prise en charge d'une configuration NAT (Network Address Translation) de base. La phase II EzVPN est dérivée du protocole Unity (logiciel client VPN). Le périphérique distant est toujours l'initiateur du tunnel IPsec. Cependant, les propositions IKE (Internet Key Exchange) et IPsec ne sont pas configurables sur le client EzVPN. Le client VPN négocie les propositions avec le serveur.

Afin de configurer IPsec entre un routeur PIX/ASA 7.x et un routeur Cisco 871 utilisant Easy VPN, référez-vous à [Exemple de configuration Easy VPN PIX/ASA 7.x avec un ASA 5500 comme serveur et Cisco 871 comme Easy VPN Remote](#).

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

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 de tenter cette configuration, vérifiez que le routeur Cisco IOS prend en charge la [fonctionnalité EzVPN Phase II](#) et dispose de la connectivité IP avec des connexions de bout en bout pour établir le tunnel IPsec.

Components Used

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 (EzVPN Phase II)
- Concentrateur VPN 3000 3.6.x
- Routeur Cisco 1700

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.

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

Conventions

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

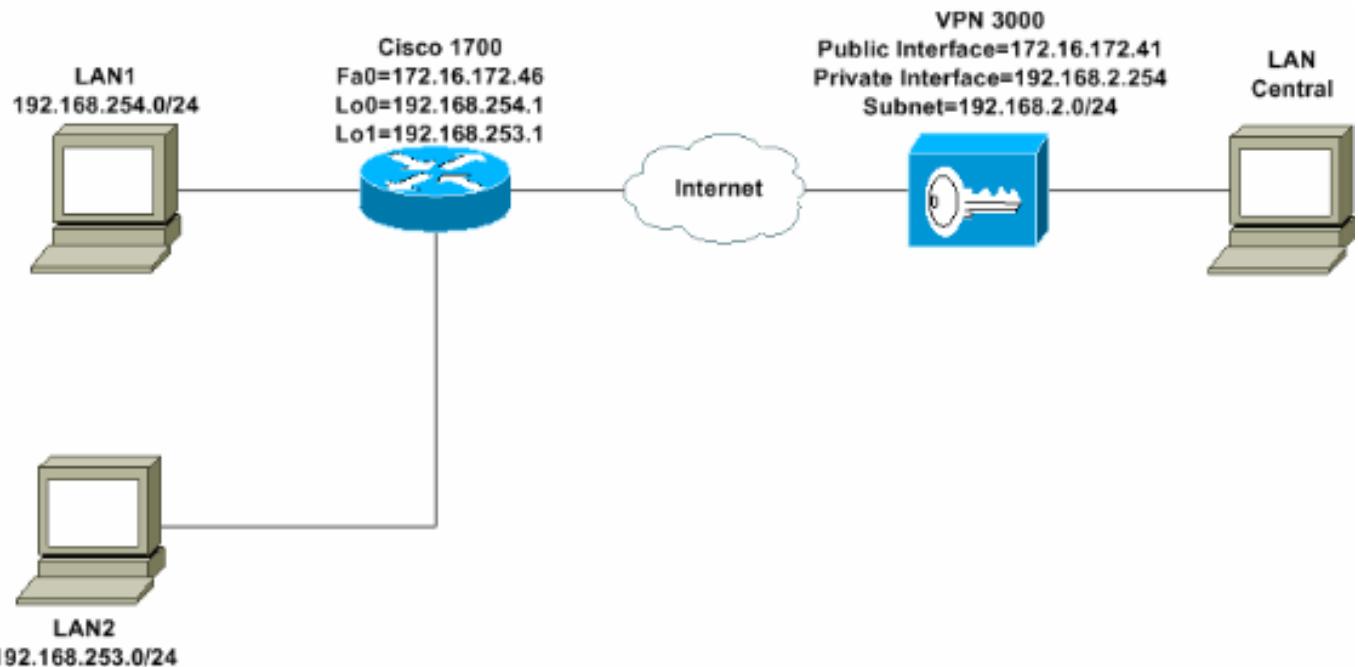
Configurer le concentrateur VPN 3000

Tâche

Cette section présente les informations nécessaires à la configuration du concentrateur VPN 3000.

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant. Les interfaces de bouclage sont utilisées comme sous-réseaux internes et FastEthernet 0 est la valeur par défaut d'Internet.



Instructions pas à pas

Procédez comme suit :

1. Choisissez Configuration > User Management > Groups > Add et définissez un nom de groupe et un mot de passe afin de configurer un groupe IPsec pour les utilisateurs.Cet exemple utilise le nom de groupe **turaro** avec mot de passe/verify **tululo**.

- Configuration
 - > Interfaces
 - > System
 - > User Management
 - > Base Group
 - > Groups
 - > Users
 - > Policy Management

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	External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.							
		Add	Cancel						

2. Choisissez Configuration > User Management > Groups > **turaro** > General pour activer **IPSec** et désactiver PPTP (Point-to-Point Tunneling Protocol) et L2TP (Layer 2 Tunnel Protocol).Faites vos sélections et cliquez sur **Apply**.

General Par			
Attribute	Value	Inherit?	
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter
Minimum Password Length	8	<input checked="" type="checkbox"/>	Enter
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enter 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"/>	Enter
Primary DNS		<input checked="" type="checkbox"/>	Enter
Secondary DNS		<input checked="" type="checkbox"/>	Enter
Primary WINS		<input checked="" type="checkbox"/>	Enter
Secondary WINS		<input checked="" type="checkbox"/>	Enter
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"/>	Select
Tunneling Protocols	<input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPSec	<input type="checkbox"/>	Select

3. Définissez Authentication sur Internal for Extended Authentication (Xauth) et assurez-vous que le type de tunnel est Remote Access et que la SA IPSec est ESP-3DES-MD5.

The screenshot shows the 'IPSec Parameters' section with the following settings:

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"/>

The 'Remote Access Parameters' section contains the following settings:

Attribute	Value	Inherit?
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Authentication	Internal	<input checked="" type="checkbox"/>

4. Choisissez Configuration > System > Tunneling Protocols > IPSec > IKE Propositions afin de vous assurer que le client VPN Cisco (CiscoVPNClient-3DES-MD5) figure dans les propositions actives pour IKE (Phase 1). Remarque : à partir du concentrateur VPN 4.1.x, la procédure est différente pour s'assurer que le client VPN Cisco figure dans la liste des propositions actives pour IKE (phase 1). Choisissez Configuration > Tunneling and Security > IPSec > IKE

Propositions.

The screenshot shows the 'IKE Proposals' section with the following details:

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	<input type="button" value="Activate"/> <input type="button" value="Deactivate"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Add"/>	IKE-3DES-MD5-RSA IKE-3DES-SHA-DSA IKE-3DES-MD5-RSA-DH IKE-DES-MD5-DH7 CiscoVPNClient-3DES-MD5 CiscoVPNClient-3DES-SHA-DSA

5. Vérifiez votre association de sécurité IPsec (SA). À l'étape 3, votre SA IPsec est ESP-3DES-MD5. Vous pouvez en créer un si vous le souhaitez, mais assurez-vous d'utiliser la SA IPsec correcte sur votre groupe. Vous devez désactiver Perfect Forward Secrecy (PFS) pour l'association de sécurité IPsec que vous utilisez. Sélectionnez Cisco VPN Client comme

proposition IKE en choisissant Configuration > Policy Management > Traffic Management > SA. Tapez le nom du SA dans la zone de texte et effectuez les sélections appropriées comme indiqué ici

Configuration Policy Management Traffic Management Security Associations Modify		
Modify a configured Security Association.		
SA Name	ESP-3DES-MD5	Specify the name of this Security Association (S)
Inheritance	From Rule	Select the granularity of this SA.
IPSec Parameters		
Authentication Algorithm	ESP/MD5/HMAC-128	Select the packet authentication algorithm to use.
Encryption Algorithm	3DES-168	Select the ESP encryption algorithm to use.
Encapsulation Mode	Tunnel	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy	Disabled	Select the use of Perfect Forward Secrecy.
Lifetime Measurement	Time	Select the lifetime measurement of the IPSec key.
Data Lifetime	10000	Specify the data lifetime in kilobytes (KB).
Time Lifetime	28800	Specify the time lifetime in seconds.
IKE Parameters		
IKE Peer	0.0.0.0	Specify the IKE Peer for a LAN-to-LAN IPSe
Negotiation Mode	Aggressive	Select the IKE Negotiation mode to use.
Digital Certificate	None (Use Preshared Keys)	Select the Digital Certificate to use.
Certificate Transmission	<input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the
IKE Proposal	CiscoVPNClient-3DES-MD5	Select the IKE Proposal to use as IKE initiator.

Remarque : Cette étape et l'étape suivante sont facultatives si vous préférez choisir une SA prédéfinie. Si votre client a une adresse IP attribuée dynamiquement, utilisez 0.0.0.0 dans la zone de texte homologue IKE. Assurez-vous que la proposition IKE est définie sur CiscoVPNClient-3DES-MD5 comme le montre cet exemple.

6. Vous ne devez pas cliquer sur *Autoriser les réseaux de la liste à contourner le tunnel*. La raison en est que la transmission tunnel partagée est prise en charge, mais que la fonction de contournement n'est pas prise en charge avec la fonctionnalité EzVPN Client.

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

7. Choisissez Configuration > User Management > Users afin d'ajouter un utilisateur. Définissez un nom d'utilisateur et un mot de passe, affectez-le à un groupe, puis cliquez sur Ajouter.

<ul style="list-style-type: none"> - Configuration <ul style="list-style-type: none"> Interfaces System User Management <ul style="list-style-type: none"> Base Group Groups Users Policy Management - Administration - Monitoring 	Configuration User Management Users Add		
	<p>This section lets you add a user. Uncheck the Inherit? box and enter a new value to override group values.</p>		
	Identity General IPSec PPTP/L2TP		
	Identity Parameters		
	Attribute	Value	Description
	Username	<input type="text" value="padma"/>	Enter a unique username.
	Password	<input type="password" value="*****"/>	Enter the user's password. The password must satisfy the group password requirements.
	Verify	<input type="password" value="*****"/>	Verify the user's password.
	Group	<input type="text" value="turaro"/>	Enter the group to which this user belongs.
	IP Address	<input type="text"/>	Enter the IP address assigned to this user.
	Subnet Mask	<input type="text"/>	Enter the subnet mask assigned to this user.
	<input type="button" value="Add"/> <input type="button" value="Cancel"/>		

8. Choisissez Administration > Admin Sessions et vérifiez que l'utilisateur est connecté. Dans NEM, le concentrateur VPN n'attribue pas d'adresse IP du pool. Remarque : Cette étape est facultative si vous préférez choisir une SA prédefinie.

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						
Chico_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 l'icône **Save Needed** ou **Save** afin d'enregistrer la configuration.

[Configuration du routeur](#)

[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 inside
!
interface Loopback1
 ip address 192.168.253.1 255.255.255.0
ip nat inside
crypto ipsec client eZVPN 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
!
!--- 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

```

Vérification

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 avez configuré les deux périphériques, le routeur Cisco 3640 tente de configurer le tunnel VPN en contactant le concentrateur VPN automatiquement à l'aide de l'adresse IP de l'homologue. Une fois les paramètres ISAKMP initiaux permuts, 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. Cette opération doit correspondre au nom d'utilisateur et au mot de passe configurés sur le concentrateur VPN (étape 7). Une fois que le nom d'utilisateur et le mot de passe ont été convenus par les deux homologues, les autres paramètres sont convenus et le tunnel VPN IPsec s'active.

```
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
```

Dépannage

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 de débogage.

- **debug crypto ipsec client ezvpn** - Affiche les informations qui indiquent la configuration et l'implémentation de la fonctionnalité EzVPN Client.
- **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 de débogage.

Sortie des commandes de débogage

Dès que vous entrez la commande **crypto ipsec client ezvpn SJVPN**, le client EzVPN tente de se connecter au serveur. Si vous modifiez la commande **connect Manual** sous la configuration de groupe, entrez la commande **crypto ipsec client ezvpn connect SJVPN** pour initier l'échange de 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_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 = -1602220489 4d05h: ISAKMP: Config payload SET 4d05h: ISAKMP (0:3): Xauth process set, status = 1 4d05h: ISAKMP (0:3): checking SET: 4d05h: ISAKMP: XAUTH_STATUS_V2 XAUTH-OK 4d05h: ISAKMP (0:3): attributes

```

sent in message: 4d05h: Status: 1 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP (0:3): deleting node -1602220489 error FALSE reason "" 4d05h: ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_CFG_SET Old State = IKE_XAUTH_REPLY_SENT New State = IKE_P1_COMPLETE 4d05h: EZVPN(SJVPN): Current State: XAUTH_REPLYED 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

```

Commandes show de Cisco IOS associées 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:

[Effacer un tunnel actif](#)

Vous pouvez effacer les tunnels à l'aide des commandes suivantes :

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

Remarque : Vous pouvez utiliser le concentrateur VPN afin de vous déconnecter de la session lorsque vous choisissez **Administration > Admin Sessions**, sélectionnez l'utilisateur dans **Session d'accès à distance** et cliquez sur **déconnexion**.

[Débogage du concentrateur VPN 3000](#)

Choisissez **Configuration > System > Events > Classes** afin d'activer ce débogage en cas d'échec de connexion d'événement. Vous pouvez toujours ajouter d'autres classes si celles illustrées ne vous aident pas à identifier le problème.

The screenshot shows the Juniper Firewall configuration interface. On the left, there is a navigation tree under 'Configuration': Interfaces, System (Servers, Address Management, Tunneling Protocols, IP Routing, Management Protocols), Events (General, FTP Backup, Classes, Trap Destinations, Syslog Servers, SMTP Servers, Email Recipients), General, Client Update, Load Balancing, User Management, Policy Management, Administration. The 'Classes' link under 'Events' is highlighted. The main pane title is 'Configuration | System | Events | Classes'. Below the title, there is a descriptive text: 'This section lets you configure special handling of specific event classes. Click the Add button to add an event class, or select an event class and click Modify or Delete.' A link 'Click here to configure general event parameters.' is also present. On the right, there is a table titled 'Configured Event Classes' with columns 'Event Classes' and 'Actions'. The table contains four entries: IKE, IKEDBG, IPSEC, and IPSECDDBG. To the right of the table are three buttons: 'Add', 'Modify', and 'Delete'.

Event Classes	Actions
IKE	
IKEDBG	
IPSEC	
IPSECDDBG	

Afin d'afficher le journal des événements actuel en mémoire, filtrable par classe d'événements, gravité, adresse IP, etc., choisissez **Monitoring > Filterable Event log**.

Afin d'afficher les statistiques du protocole IPsec, choisissez **Monitoring > Statistics > IPsec**. Cette fenêtre affiche les statistiques de l'activité IPsec, y compris les tunnels IPsec actuels, sur le concentrateur VPN depuis son dernier démarrage ou réinitialisation. Ces statistiques sont conformes au brouillon IETF pour la MIB de surveillance de flux IPsec. La fenêtre **Surveillance > Sessions > Detail** affiche également les données IPsec.

Monitoring Statistics IPsec		Friday, 28 July 2006 10:00:11	
		Reset Refresh	
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. Pendant le dépannage, activez les débogages IPsec et ISAKMP avec les commandes suivantes :

```
debug crypto ipsec
debug crypto isakmp
debug crypto ezvpn
```

Sur le routeur Cisco IOS, vous voyez ceci :

```
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
```

Sur le concentrateur VPN 3000, Xauth est requis. Cependant, la proposition sélectionnée ne prend pas en charge Xauth. Vérifiez que l'[authentification interne pour Xauth](#) est spécifiée. Activez l'authentification interne et assurez-vous que le mode d'authentification des propositions IKE est défini sur **Clés pré-partagées (Xauth)**, comme dans la [capture d'écran](#) précédente. Cliquez sur **Modifier** afin de modifier la proposition.

- Le mot de passe est incorrect. Vous ne voyez pas le message **Mot de passe non valide** sur le routeur Cisco IOS. Sur le concentrateur VPN, vous pouvez voir l'**événement EV_ACTIVATE_NEW_SA** reçu dans l'état **AM_TM_INIT_XAUTH**. Assurez-vous que votre mot de passe est correct.
- Le nom d'utilisateur est incorrect. Sur le routeur Cisco IOS, un débogage similaire s'affiche si vous avez un mot de passe incorrect. Sur le concentrateur VPN, l'**authentification est rejetée** : Raison = Utilisateur introuvable.

Informations connexes

- [Page d'assistance des concentrateurs VPN Cisco 3000](#)
- [Cisco Easy VPN Remote Phase II](#)
- [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](#)