Esempio di configurazione di EzVPN con NEM su router IOS con concentratore VPN 3000

Sommario

Introduzione

Questo documento spiega la procedura da usare per configurare un router Cisco IOS® come EzVPN in modalità di estensione della rete (NEM) per collegarsi a un concentratore Cisco VPN 3000. Una nuova funzionalità EzVPN Fase II è il supporto di una configurazione NAT (Network Address Translation) di base. EzVPN Fase II è derivata dal protocollo Unity (software client VPN). La periferica remota è sempre l'iniziatore del tunnel IPsec. Tuttavia, le proposte IKE (Internet Key Exchange) e IPSec non sono configurabili sul client EzVPN. Il client VPN negozia le proposte con il server.

Per configurare IPsec tra un PIX/ASA 7.x e un router Cisco 871 con Easy VPN, fare riferimento a PIX/ASA 7.x Easy VPN con ASA 5500 come server e Cisco 871 come esempio di configurazione remota per Easy VPN.

Per configurare IPsec tra il client hardware remoto Cisco IOS® Easy VPN e il server PIX Easy VPN, fare riferimento all'esempio di configurazione di un server PIX Easy VPN da un client hardware remoto IOS Easy VPN.

Per configurare un router Cisco 7200 come EzVPN e il router Cisco 871 come Easy VPN Remote, fare riferimento all'esempio di configurazione remota di Easy VPN 7200 e 871.

Prerequisiti

Requisiti

Prima di provare la configurazione, verificare che il router Cisco IOS supporti la funzionalità EzVPN fase II e disponga della connettività IP con connessioni end-to-end per stabilire il tunnel IPsec.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Nota: questa configurazione è stata testata di recente con un router Cisco 3640 con software Cisco IOS versione 12.4(8) e la versione VPN 3000 Concentrator 4.7.x.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

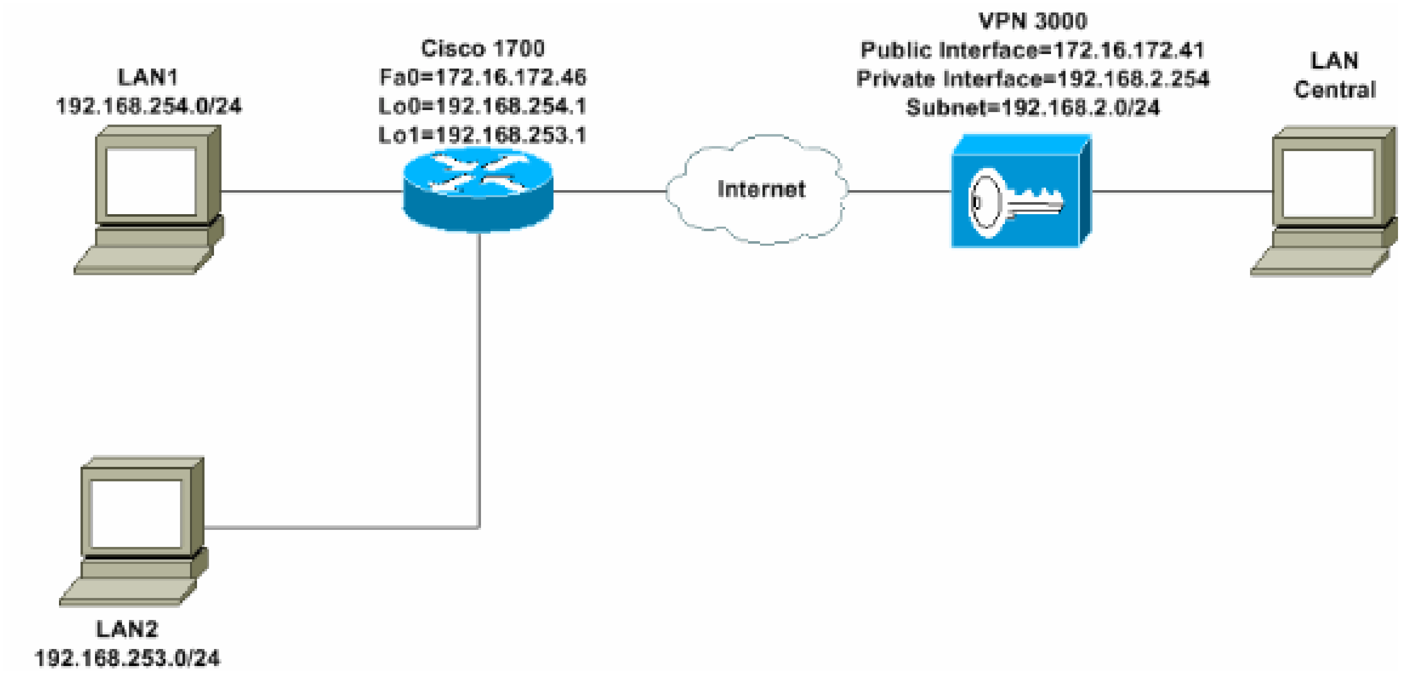
Configurazione di VPN 3000 Concentrator

Attività

In questa sezione vengono presentate le informazioni necessarie per configurare VPN 3000 Concentrator.

Esempio di rete

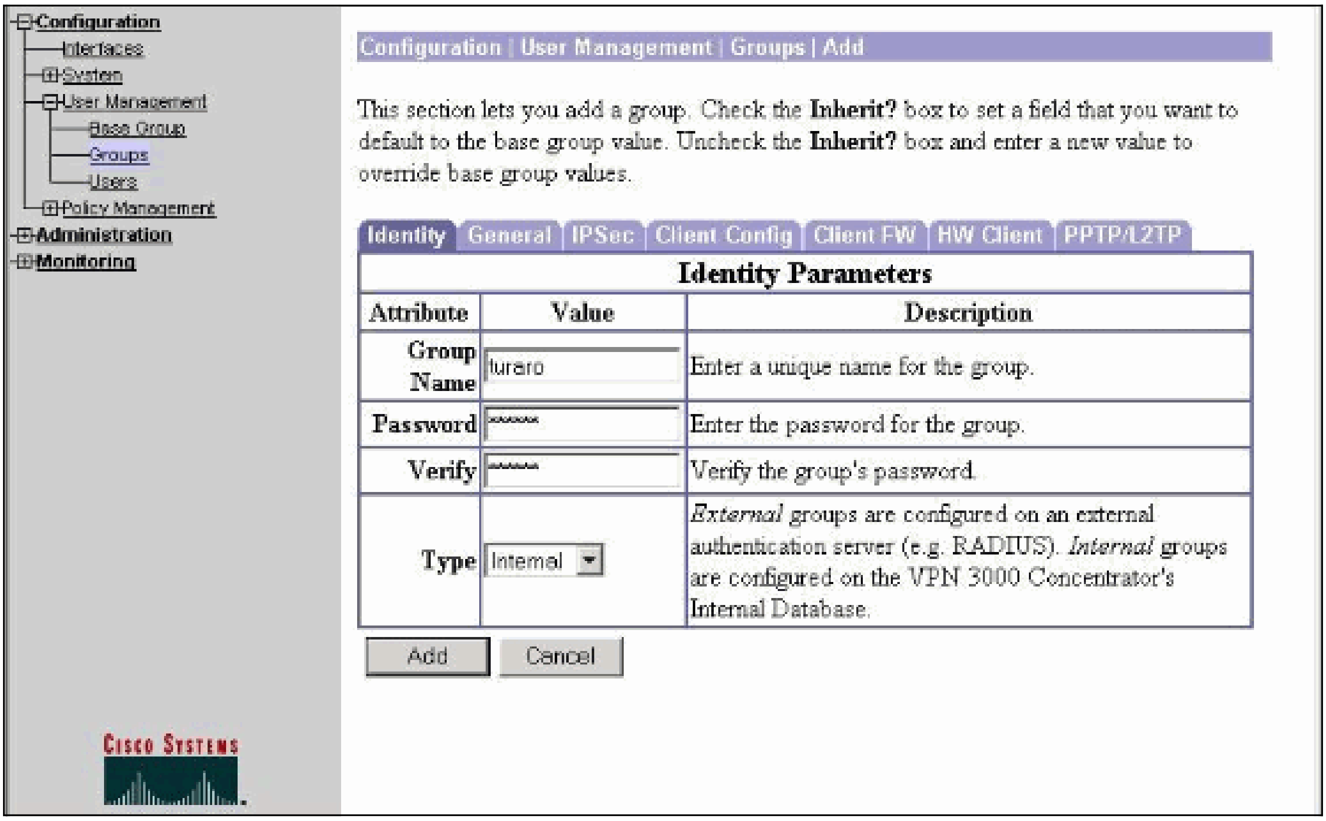
Nel documento viene usata l'impostazione di rete mostrata nel diagramma. Le interfacce di loopback vengono utilizzate come subnet interne e Fast Ethernet 0 è l'impostazione predefinita per Internet.



Istruzioni dettagliate

Attenersi alla seguente procedura:

1. Per configurare un gruppo IPSec per gli utenti, scegliere **Configurazione** > **Gestione utente** > **Gruppi** > **Aggiungi** e definire un nome e una password per il gruppo.In questo esempio viene utilizzato il nome del gruppo **turaro** con password/verify **tululo**.



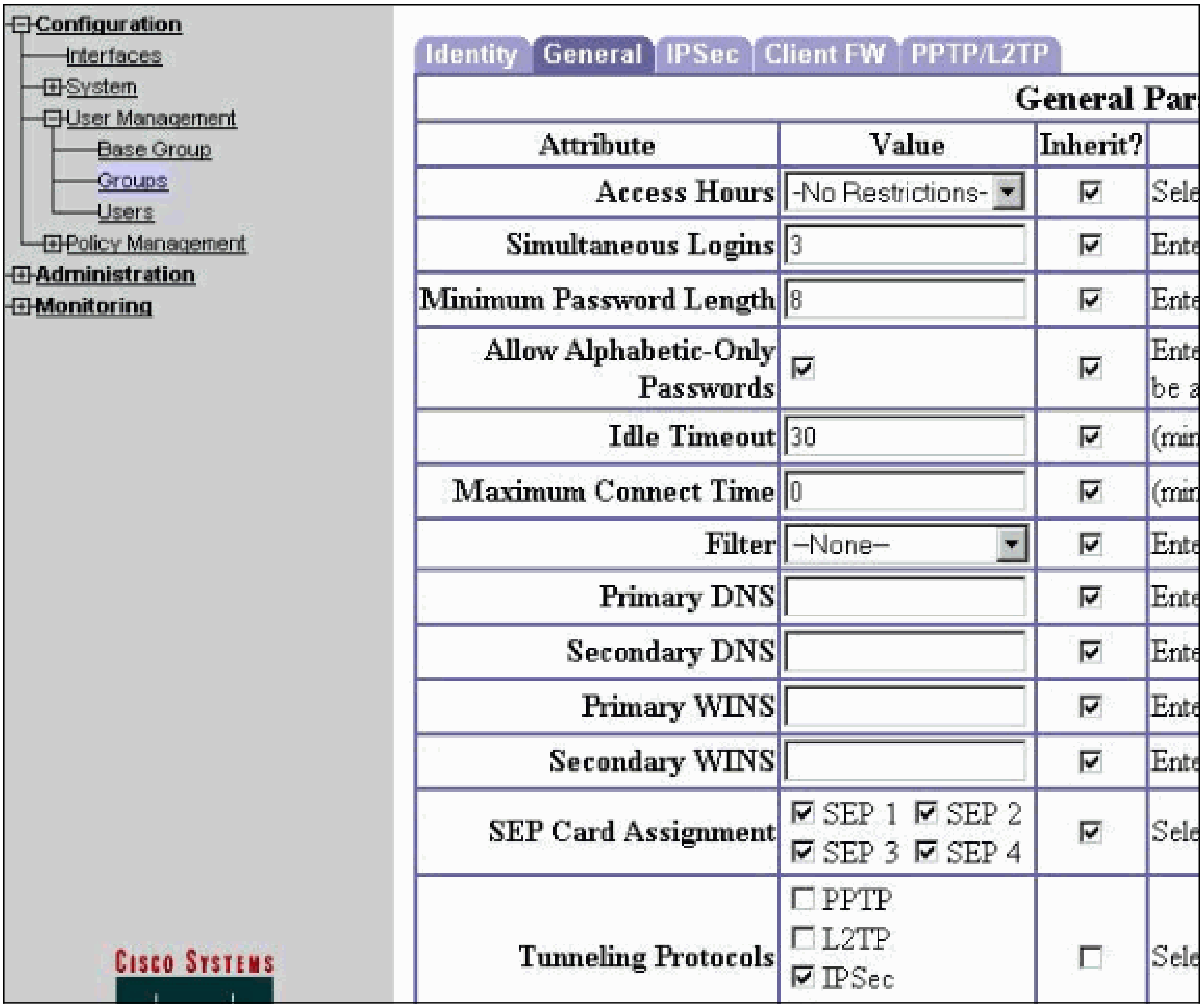
Configuration | User Management | Groups | Add

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 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.

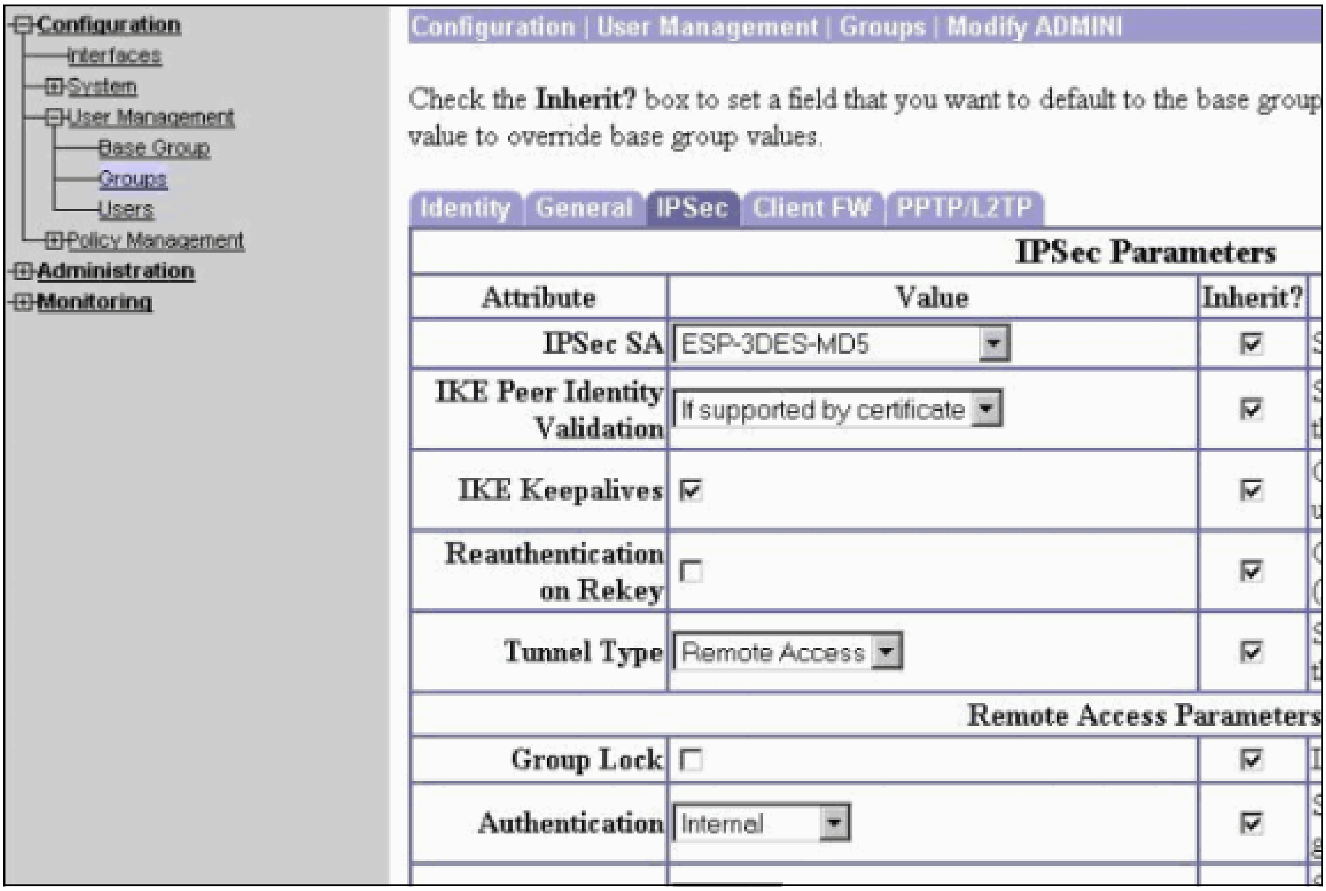
2. Scegliere Configurazione > Gestione utente > Gruppi > **Turaro** > **Generale** per abilitare **IPSec** e disabilitare il protocollo PPTP (Point-to-Point Tunneling Protocol) e L2TP (Layer 2 Tunnel Protocol).Effettuare le selezioni desiderate e fare clic su **Applica**.



General Par

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

3. Impostare Authentication (Autenticazione **interna** per autenticazione estesa) (Xauth) e verificare che il tipo di tunnel sia **Accesso remoto** e che la SA IPSec sia **ESP-3DES-MD5**.



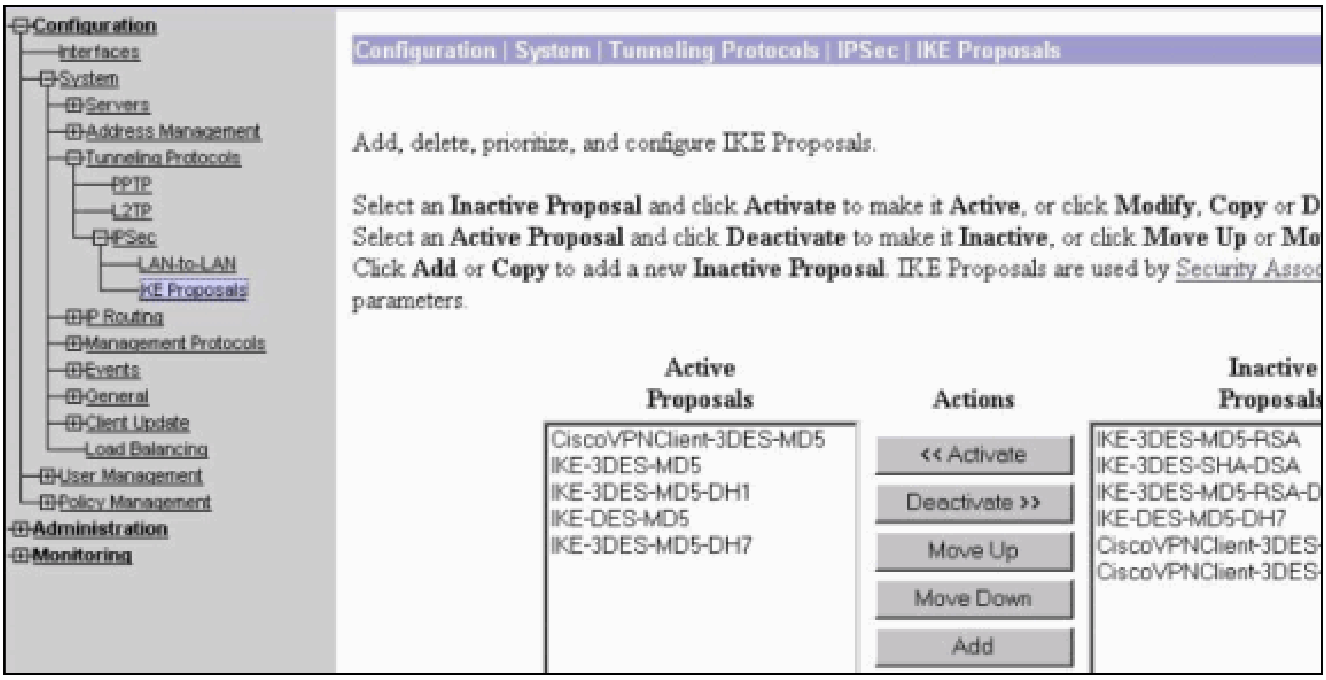
Configuration | User Management | Groups | Modify ADMINI

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

IPSec Parameters

Attribute	Value	Inherit?
IPSec SA	ESP-3DES-MD5	☑
IKE Peer Identity Validation	If supported by certificate	☑
IKE Keepalives	☑	☑
Reauthentication on Rekey	□	☑
Tunnel Type	Remote Access	☑
Remote Access Parameters		
Group Lock	□	☑
Authentication	Internal	☑

4. Scegliere **Configurazione > Sistema > Protocolli di tunneling > IPSec > Proposte IKE** per essere certi che il client VPN Cisco (CiscoVPNClient-3DES-MD5) sia incluso nelle proposte attive per IKE (fase 1).**Nota:** da VPN Concentrator 4.1.x, la procedura è diversa per verificare che il client VPN Cisco sia nell'elenco di proposte attive per IKE (fase 1). Scegliere **Configurazione > Tunneling e sicurezza > IPSec > Proposte 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 **D**
Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Mo**
Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by Security Assoc
parameters.

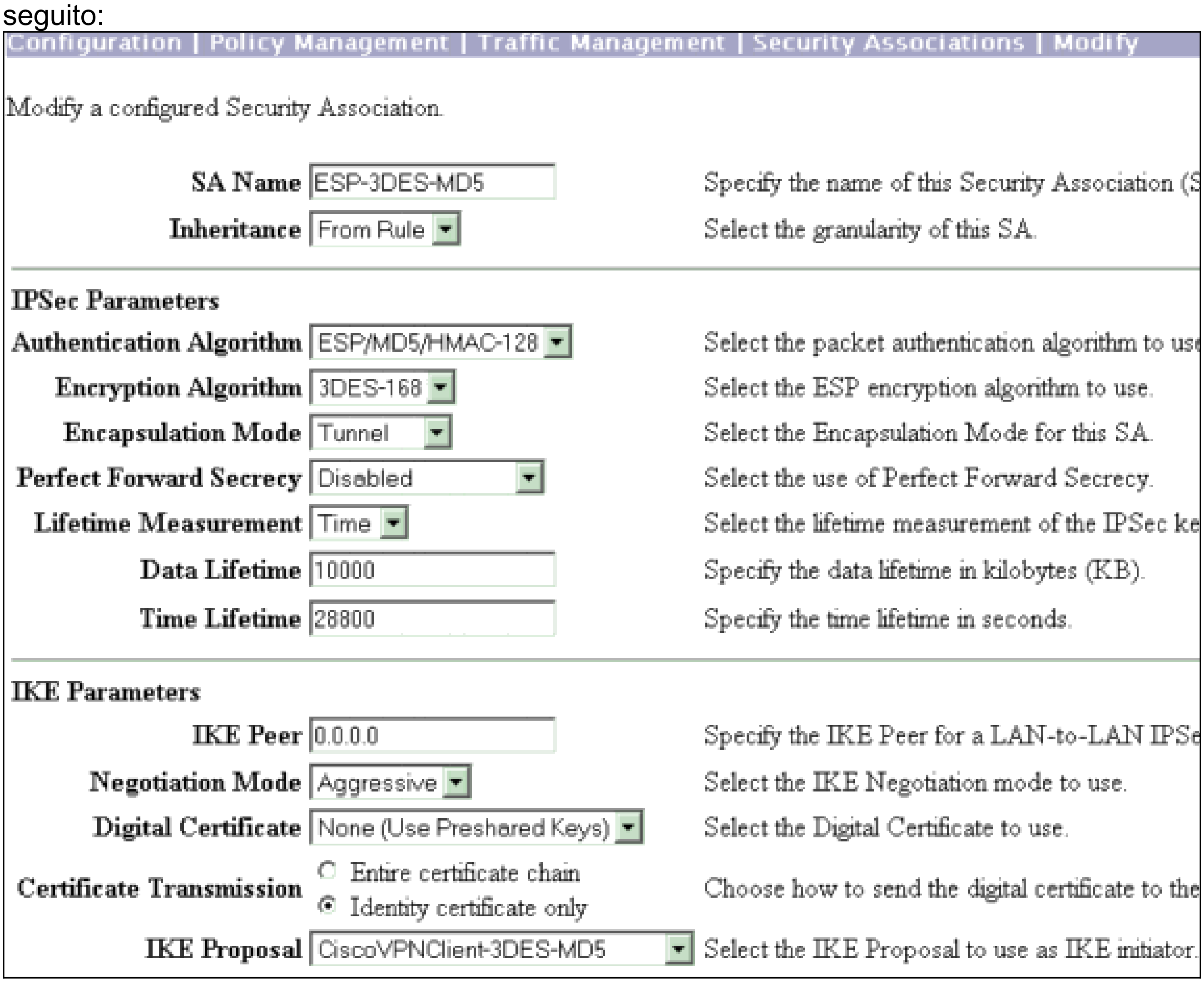
Active Proposals
CiscoVPNClient-3DES-MD5
IKE-3DES-MD5
IKE-3DES-MD5-DH1
IKE-DES-MD5
IKE-3DES-MD5-DH7

Actions

Inactive Proposals
IKE-3DES-MD5-RSA
IKE-3DES-SHA-DSA
IKE-3DES-MD5-RSA-D
IKE-DES-MD5-DH7
CiscoVPNClient-3DES-
CiscoVPNClient-3DES-

5. Verificare l'associazione di sicurezza (SA) IPsec.Nel passaggio 3 la SA IPsec è ESP-3DES-MD5. Se lo si desidera, è possibile crearne una nuova, ma accertarsi di utilizzare la SA IPsec corretta nel gruppo. È consigliabile disabilitare PFS (Perfect Forward Secrecy) per l'associazione di protezione IPsec utilizzata. Selezionare il client VPN Cisco come proposta IKE scegliendo **Configurazione** > **Gestione policy** > **Gestione traffico** > **SA**. Digitare il nome

dell'associazione di protezione nella casella di testo ed effettuare le selezioni appropriate come illustrato di seguito:



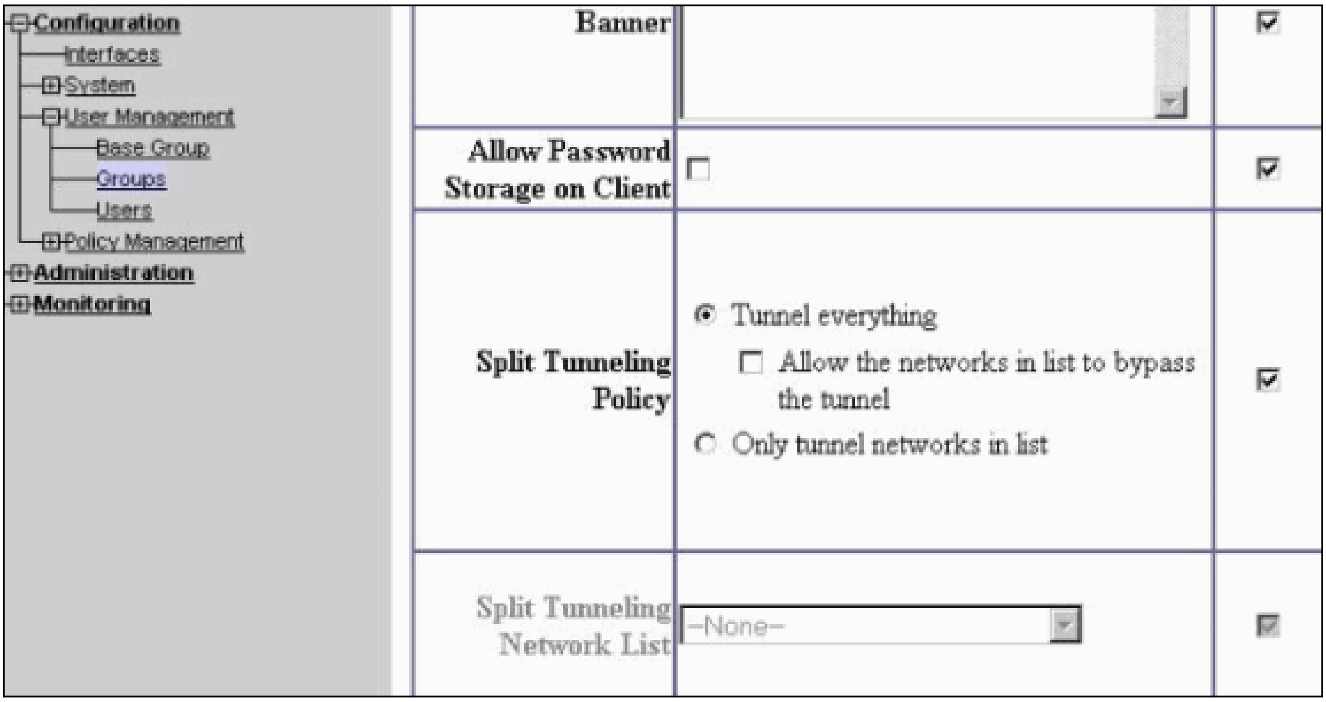
Configuration | Policy Management | Traffic Management | Security Associations | Modify

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 ke
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	○ Entire certificate chain ● 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.

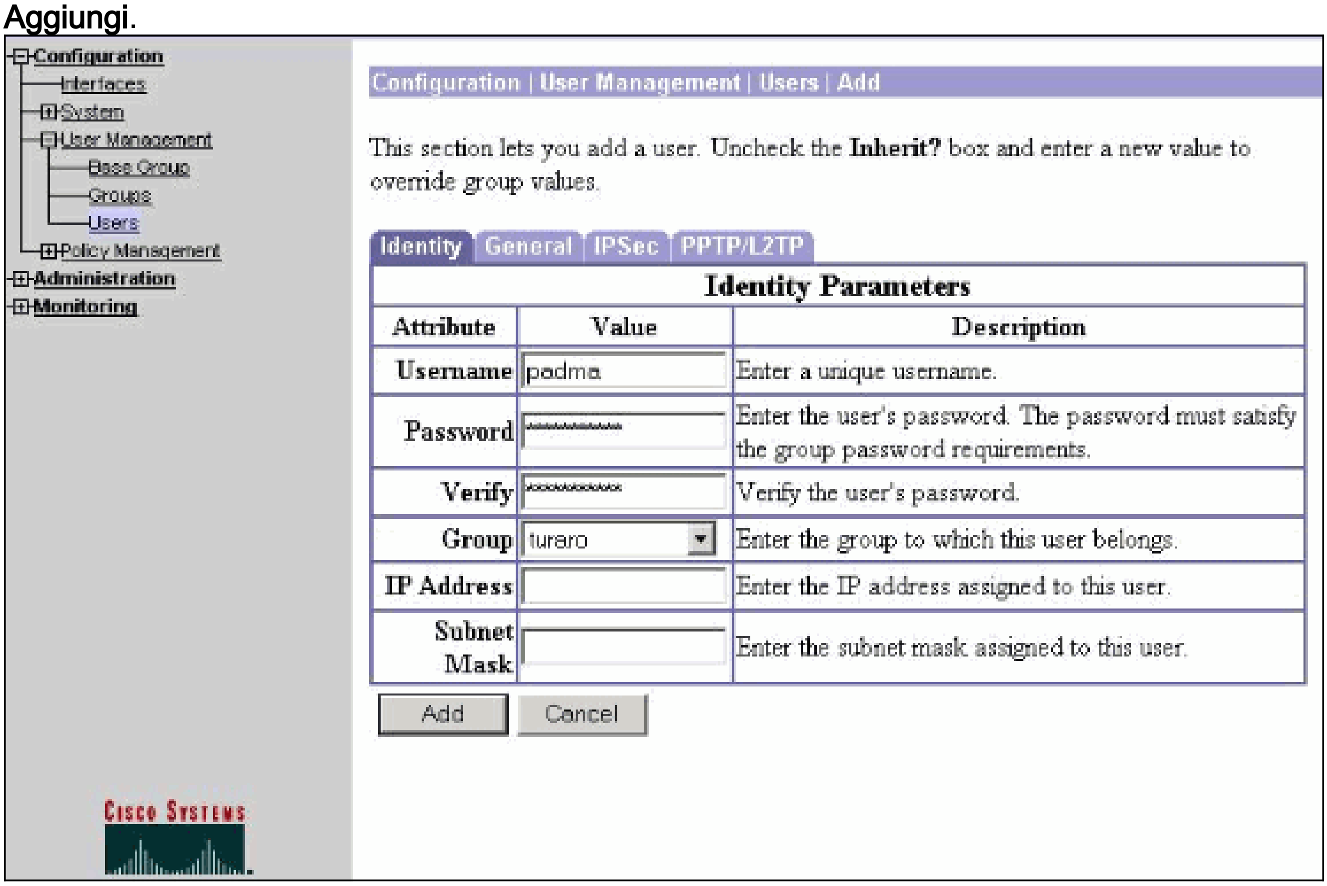
Nota: questo passo e quello successivo sono facoltativi se si preferisce scegliere un'associazione di protezione predefinita. Se al client è assegnato un indirizzo IP in modo dinamico, utilizzare 0.0.0.0 nella casella di testo peer IKE. Verificare che la proposta IKE sia impostata su **CiscoVPNClient-3DES-MD5**, come mostrato nell'esempio.

6. **Non** fare clic su *Consenti alle reti nell'elenco di ignorare il tunnel*. Il motivo è che il tunneling diviso è supportato, ma la funzione di bypass non è supportata con la funzione client EzVPN.



Banner		☑
Allow Password Storage on Client	□	☑
Split Tunneling Policy	● Tunnel everything □ Allow the networks in list to bypass the tunnel ○ Only tunnel networks in list	☑
Split Tunneling Network List	--None--	☑

7. Per aggiungere un utente, scegliere **Configurazione** > **Gestione utente** > **Utenti**. Definire un nome utente e una password, assegnarli a un gruppo e fare clic su **Aggiungi**.

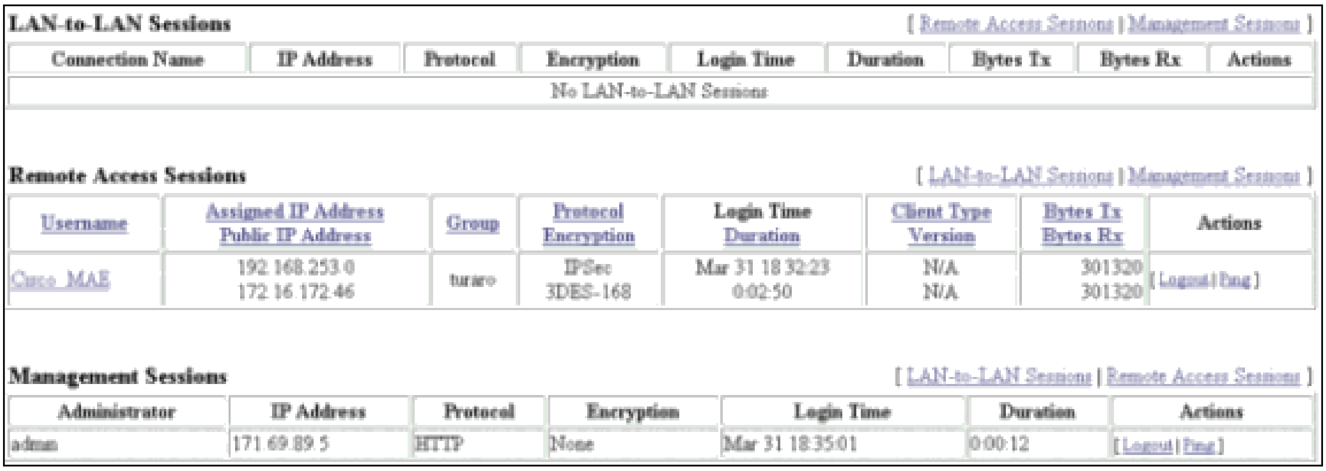


Configuration | User Management | Users | Add

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

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

8. Scegliere **Amministrazione > Sessioni di amministrazione** e verificare che l'utente sia connesso. In NEM, il concentratore VPN non assegna un indirizzo IP dal pool.**Nota:** questo passo è facoltativo se si preferisce scegliere un'associazione di protezione predefinita.



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. Per salvare la configurazione, fare clic sull'icona **Save Needed** (Salva necessario)o **Save** (Salva).

Configurazione router

Mostra output versione

```
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
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Dopo aver configurato entrambi i dispositivi, il router Cisco 3640 tenta di configurare il tunnel VPN contattando automaticamente il concentratore VPN con l'indirizzo IP del peer. Dopo aver scambiato i parametri ISAKMP iniziali, il router visualizza questo messaggio:

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

Ènecessario immettere il comando **crypto ipsec client ezvpn xauth** che richiede un nome utente e una password. Deve corrispondere al nome utente e alla password configurati sul concentratore VPN (passaggio 7). Dopo che il nome utente e la password sono stati concordati da entrambi i peer, il resto dei parametri viene concordato e viene visualizzato il tunnel VPN IPsec.

```
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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug crypto ipsec client ezvpn**: visualizza le informazioni che mostrano la configurazione e l'implementazione della funzione client EzVPN.
- **debug crypto ipsec**: visualizza le informazioni di debug sulle connessioni IPsec.
- **debug crypto isakmp**: visualizza le informazioni di debug sulle connessioni IPsec e mostra il primo set di attributi negati a causa di incompatibilità su entrambi i lati.
- **show debug**: visualizza lo stato di ciascuna opzione di debug.

Output dei comandi di debug

Non appena si immette il comando **crypto ipsec client ezvpn SJVPN**, il client EzVPN tenta di connettersi al server. Se si modifica il comando **connect manual** nella configurazione di gruppo, immettere il comando **crypto ipsec client ezvpn connect SJVPN** per avviare lo scambio di proposte al server.

```
4d05h: ISAKMP (0:3): beginning Aggressive Mode exchange
4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) AG_INIT_EXCH
4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) AG_INIT_EXCH
4d05h: ISAKMP (0:3): processing SA payload. message ID = 0
4d05h: ISAKMP (0:3): processing ID payload. message ID = 0
4d05h: ISAKMP (0:3): processing vendor id payload
4d05h: ISAKMP (0:3): vendor ID is Unity
4d05h: ISAKMP (0:3): processing vendor id payload
4d05h: ISAKMP (0:3): vendor ID seems Unity/DPD but bad major
4d05h: ISAKMP (0:3): vendor ID is XAUTH
4d05h: ISAKMP (0:3): processing vendor id payload
4d05h: ISAKMP (0:3): vendor ID is DPD
4d05h: ISAKMP (0:3) local preshared key found
4d05h: ISAKMP (0:3) Authentication by xauth preshared
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65527 policy
4d05h: ISAKMP:      encryption 3DES-CBC
4d05h: ISAKMP:      hash MD5
4d05h: ISAKMP:      default group 2
4d05h: ISAKMP:      auth XAUTHInitPreShared
4d05h: ISAKMP:      life type in seconds
4d05h: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65528 policy
4d05h: ISAKMP:      encryption 3DES-CBC
4d05h: ISAKMP:      hash MD5
4d05h: ISAKMP:      default group 2
4d05h: ISAKMP:      auth XAUTHInitPreShared
4d05h: ISAKMP:      life type in seconds
4d05h: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65529 policy
4d05h: ISAKMP:      encryption 3DES-CBC
4d05h: ISAKMP:      hash MD5
4d05h: ISAKMP:      default group 2
4d05h: ISAKMP:      auth XAUTHInitPreShared
4d05h: ISAKMP:      life type in seconds
4d05h: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65530 policy
4d05h: ISAKMP:      encryption 3DES-CBC
4d05h: ISAKMP:      hash MD5
4d05h: ISAKMP:      default group 2
4d05h: ISAKMP:      auth XAUTHInitPreShared
4d05h: ISAKMP:      life type in seconds
4d05h: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65531 policy
4d05h: ISAKMP:      encryption 3DES-CBC
4d05h: ISAKMP:      hash MD5
4d05h: ISAKMP:      default group 2
4d05h: ISAKMP:      auth XAUTHInitPreShared
4d05h: ISAKMP:      life type in seconds
4d05h: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Hash algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65532 policy
4d05h: ISAKMP:      encryption 3DES-CBC
4d05h: ISAKMP:      hash MD5
```

```
4d05h: ISAKMP:      default group 2
4d05h: ISAKMP:      auth XAUTHInitPreShared
4d05h: ISAKMP:      life type in seconds
4d05h: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): atts are acceptable. Next payload is 0
4d05h: ISAKMP (0:3): processing KE payload. message ID = 0
4d05h: ISAKMP (0:3): processing NONCE payload. message ID = 0
4d05h: ISAKMP (0:3): SKEYID state generated
4d05h: ISAKMP (0:3): processing HASH payload. message ID = 0
4d05h: ISAKMP (0:3): SA has been authenticated with 172.16.172.41
4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) AG_INIT_EXCH
4d05h: ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_I_AM1  New State = IKE_P1_COMPLETE

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

4d05h: IPSec: Key engine got KEYENG_IKMP_MORE_SAS message

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

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

Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

 !--- Phase 1 (ISAKMP) is complete. 4d05h: ISAKMP: received ke message (6/1) 4d05h: ISAKMP:
received KEYENG_IKMP_MORE_SAS message 4d05h: ISAKMP: set new node -857862190 to CONF_XAUTH !---
Initiate extended authentication. 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I)
CONF_XAUTH 4d05h: ISAKMP (0:3): purging node -857862190 4d05h: ISAKMP (0:3): Sending initial
contact. 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP:
set new node -1898481791 to CONF_XAUTH 4d05h: ISAKMP (0:3): processing transaction payload from
172.16.172.41. message ID = -1898481791 4d05h: ISAKMP: Config payload REQUEST 4d05h: ISAKMP
(0:3): checking request: 4d05h: ISAKMP: XAUTH_TYPE_V2 4d05h: ISAKMP: XAUTH_USER_NAME_V2 4d05h:
ISAKMP: XAUTH_USER_PASSWORD_V2 4d05h: ISAKMP: XAUTH_MESSAGE_V2 4d05h: ISAKMP (0:3): Xauth
process request 4d05h: ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST Old State =
IKE_P1_COMPLETE New State = IKE_XAUTH_REPLY_AWAIT 4d05h: EZVPN(SJVPN): Current State: READY
4d05h: EZVPN(SJVPN): Event: XAUTH_REQUEST 4d05h: EZVPN(SJVPN): ezvpn_xauth_request 4d05h:
EZVPN(SJVPN): ezvpn_parse_xauth_msg 4d05h: EZVPN: Attributes sent in xauth request message:
4d05h: XAUTH_TYPE_V2(SJVPN): 0 4d05h: XAUTH_USER_NAME_V2(SJVPN): 4d05h:
XAUTH_USER_PASSWORD_V2(SJVPN): 4d05h: XAUTH_MESSAGE_V2(SJVPN) <Enter Username and Password.>
4d05h: EZVPN(SJVPN): New State: XAUTH_REQ 4d05h: ISAKMP (0:3): Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE Old State = IKE_XAUTH_REPLY_AWAIT New State = IKE_XAUTH_REPLY_AWAIT 4d05h:
EZVPN(SJVPN): Pending XAuth Request, Please enter the following command: 4d05h: EZVPN: crypto
ipsec client ezvpn xauth

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

crypto ipsec client ezvpn xauth

Enter Username and Password.: padma

Password: : password

!--- The router requests your username and password that is !--- configured on the server.
4d05h: EZVPN(SJVPN): Current State: XAUTH_REQ 4d05h: EZVPN(SJVPN): Event: XAUTH_PROMPTING 4d05h:
EZVPN(SJVPN): New State: XAUTH_PROMPT 1721-1(ADSL)# 4d05h: EZVPN(SJVPN): Current State:
XAUTH_PROMPT 4d05h: EZVPN(SJVPN): Event: XAUTH_REQ_INFO_READY 4d05h: EZVPN(SJVPN):
ezvpn_xauth_reply 4d05h: XAUTH_TYPE_V2(SJVPN): 0 4d05h: XAUTH_USER_NAME_V2(SJVPN): Cisco_MAE
4d05h: XAUTH_USER_PASSWORD_V2(SJVPN): <omitted> 4d05h: EZVPN(SJVPN): New State: XAUTH_REPLIED
4d05h: xauth-type: 0 4d05h: username: Cisco_MAE 4d05h: password: <omitted> 4d05h: message <Enter
Username and Password.> 4d05h: ISAKMP (0:3): responding to peer config from 172.16.172.41. ID =
-1898481791 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP
(0:3): deleting node -1898481791 error FALSE reason "done with xauth request/reply exchange"
4d05h: ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_XAUTH_REPLY_ATTR Old State =
IKE_XAUTH_REPLY_AWAIT New State = IKE_XAUTH_REPLY_SENT 4d05h: ISAKMP (0:3): received packet from
```

```
172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP: set new node -1602220489 to CONF_XAUTH 4d05h: ISAKMP
(0:3): processing transaction payload from 172.16.172.41. message ID = -1602220489 4d05h:
ISAKMP: Config payload SET 4d05h: ISAKMP (0:3): Xauth process set, status = 1 4d05h: ISAKMP
(0:3): checking SET: 4d05h: ISAKMP: XAUTH_STATUS_V2 XAUTH-OK 4d05h: ISAKMP (0:3): attributes
sent in message: 4d05h: Status: 1 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I)
CONF_XAUTH 4d05h: ISAKMP (0:3): deleting node -1602220489 error FALSE reason "" 4d05h: ISAKMP
(0:3): Input = IKE_MESG_FROM_PEER, IKE_CFG_SET Old State = IKE_XAUTH_REPLY_SENT New State =
IKE_P1_COMPLETE 4d05h: EZVPN(SJVPN): Current State: XAUTH_REPLIED 4d05h: EZVPN(SJVPN): Event:
XAUTH_STATUS 4d05h: EZVPN(SJVPN): New State: READY 4d05h: ISAKMP (0:3): Need config/address
4d05h: ISAKMP (0:3): Need config/address 4d05h: ISAKMP: set new node 486952690 to CONF_ADDR
4d05h: ISAKMP (0:3): initiating peer config to 172.16.172.41. ID = 486952690 4d05h: ISAKMP
(0:3): sending packet to 172.16.172.41 (I) CONF_ADDR 4d05h: ISAKMP (0:3): Input =
IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE Old State = IKE_P1_COMPLETE New State =
IKE_CONFIG_MODE_REQ_SENT 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) CONF_ADDR
4d05h: ISAKMP (0:3): processing transaction payload from 172.16.172.41. message ID = 486952690
4d05h: ISAKMP: Config payload REPLY 4d05h: ISAKMP(0:3) process config reply 4d05h: ISAKMP (0:3):
deleting node 486952690 error FALSE reason "done with transaction" 4d05h: ISAKMP (0:3): Input =
IKE_MESG_FROM_PEER, IKE_CFG_REPLY Old State = IKE_CONFIG_MODE_REQ_SENT New State =
IKE_P1_COMPLETE 4d05h: EZVPN(SJVPN): Current State: READY 4d05h: EZVPN(SJVPN): Event:
MODE_CONFIG_REPLY 4d05h: EZVPN(SJVPN): ezvpn_mode_config 4d05h: EZVPN(SJVPN):
ezvpn_parse_mode_config_msg 4d05h: EZVPN: Attributes sent in message 4d05h: ip_ifnat_modified:
old_if 0, new_if 2 4d05h: ip_ifnat_modified: old_if 0, new_if 2 4d05h: ip_ifnat_modified: old_if
1, new_if 2 4d05h: EZVPN(SJVPN): New State: SS_OPEN 4d05h: ISAKMP (0:3): Input =
IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE
4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote=
172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy=
0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-sha-hmac , lifedur=
2147483s and 4608000kb, spi= 0xE6DB9372(3873149810), conn_id= 0, keysize= 0, flags= 0x400C
4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote=
172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy=
0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur=
2147483s and 4608000kb, spi= 0x3C77C53D(1014482237), conn_id= 0, keysize= 0, flags= 0x400C
4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote=
172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy=
0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 2147483s
and 4608000kb, spi= 0x79BB8DF4(2042334708), conn_id= 0, keysize= 0, flags= 0x400C 4d05h:
IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41,
local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0
(type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 2147483s and 4608000kb, spi=
0x19C3A5B2(432252338), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: ISAKMP: received ke message
(1/4) 4d05h: ISAKMP: set new node 0 to QM_IDLE 4d05h: EZVPN(SJVPN): Current State: SS_OPEN
4d05h: EZVPN(SJVPN): Event: SOCKET_READY 4d05h: EZVPN(SJVPN): No state change 4d05h: ISAKMP
(0:3): sitting IDLE. Starting QM immediately (QM_IDLE ) 4d05h: ISAKMP (0:3): beginning Quick
Mode exchange, M-ID of -1494477527 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local=
172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4),
remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-sha-hmac ,
lifedur= 2147483s and 4608000kb, spi= 0xB18CF11E(2978803998), conn_id= 0, keysize= 0, flags=
0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote=
172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy=
0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur=
2147483s and 4608000kb, spi= 0xA8C469EC(2831444460), conn_id= 0, keysize= 0, flags= 0x400C
4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote=
172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy=
0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 2147483s
and 4608000kb, spi= 0xBC5AD5EE(3160069614), conn_id= 0, keysize= 0, flags= 0x400C 4d05h:
IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41,
local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0
(type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 2147483s and 4608000kb, spi=
0x8C34C692(2352268946), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: ISAKMP (0:3): sending
packet to 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): Node -1494477527, Input =
IKE_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
```

Comandi show Cisco IOS correlati per la risoluzione dei problemi

```
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:
```

Cancellare un tunnel attivo

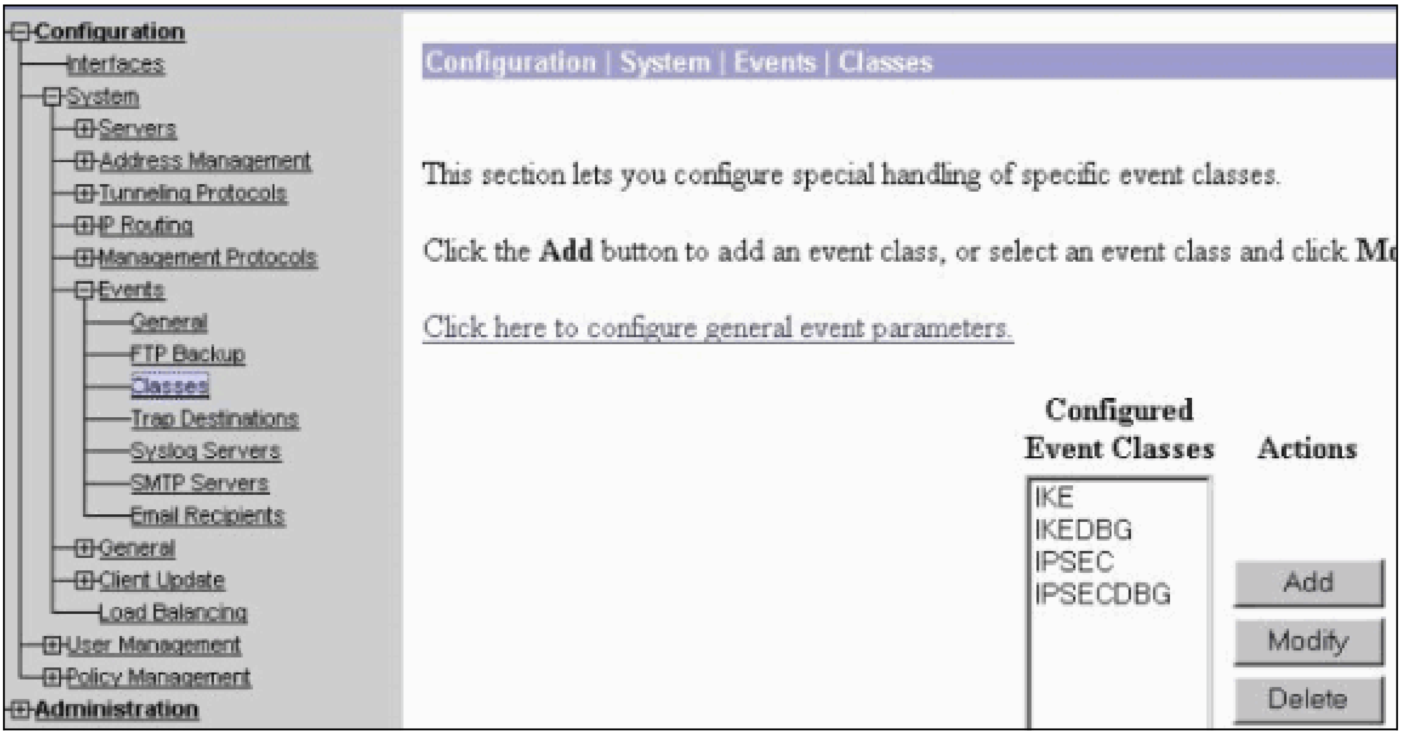
Per cancellare i tunnel, usare i seguenti comandi:

- **cancellare crypto isakmp**
- **clear crypto sa**
- **cancella crittografia client ipsec ezvpn**

Nota: è possibile utilizzare il concentratore VPN per uscire dalla sessione quando si sceglie **Amministrazione > Sessioni di amministrazione**, si seleziona l'utente in **Sessione di accesso remoto** e si fa clic su **disconnetti**.

Debug VPN 3000 Concentrator

Scegliere **Configurazione > Sistema > Eventi > Classi** per abilitare il debug in caso di errori di connessione degli eventi. È sempre possibile aggiungere altre classi se quelle visualizzate non consentono di identificare il problema.



Configuration | System | Events | Classes

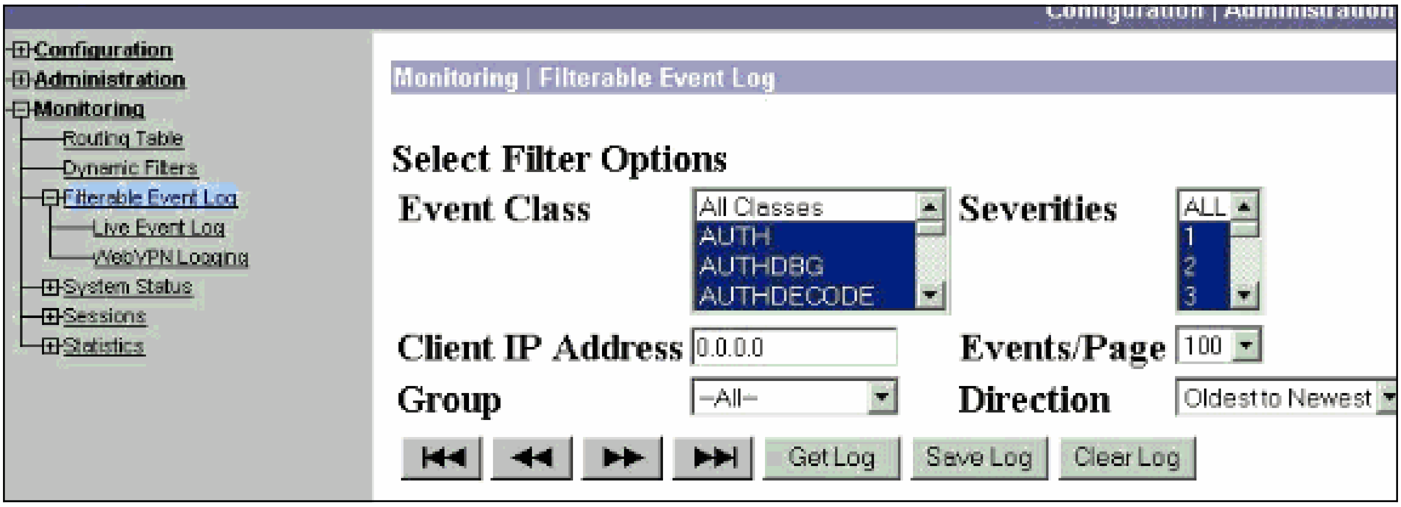
This section lets you configure special handling of specific event classes.

Click the **Add** button to add an event class, or select an event class and click **Mo**

Click here to configure general event parameters.

Configured Event Classes	Actions
IKE IKEDBG IPSEC IPSECDBG	

Per visualizzare il registro eventi corrente in memoria, filtrabile per classe di evento, gravità, indirizzo IP e così via, scegliere **Monitoraggio > Registro eventi filtrabile**.

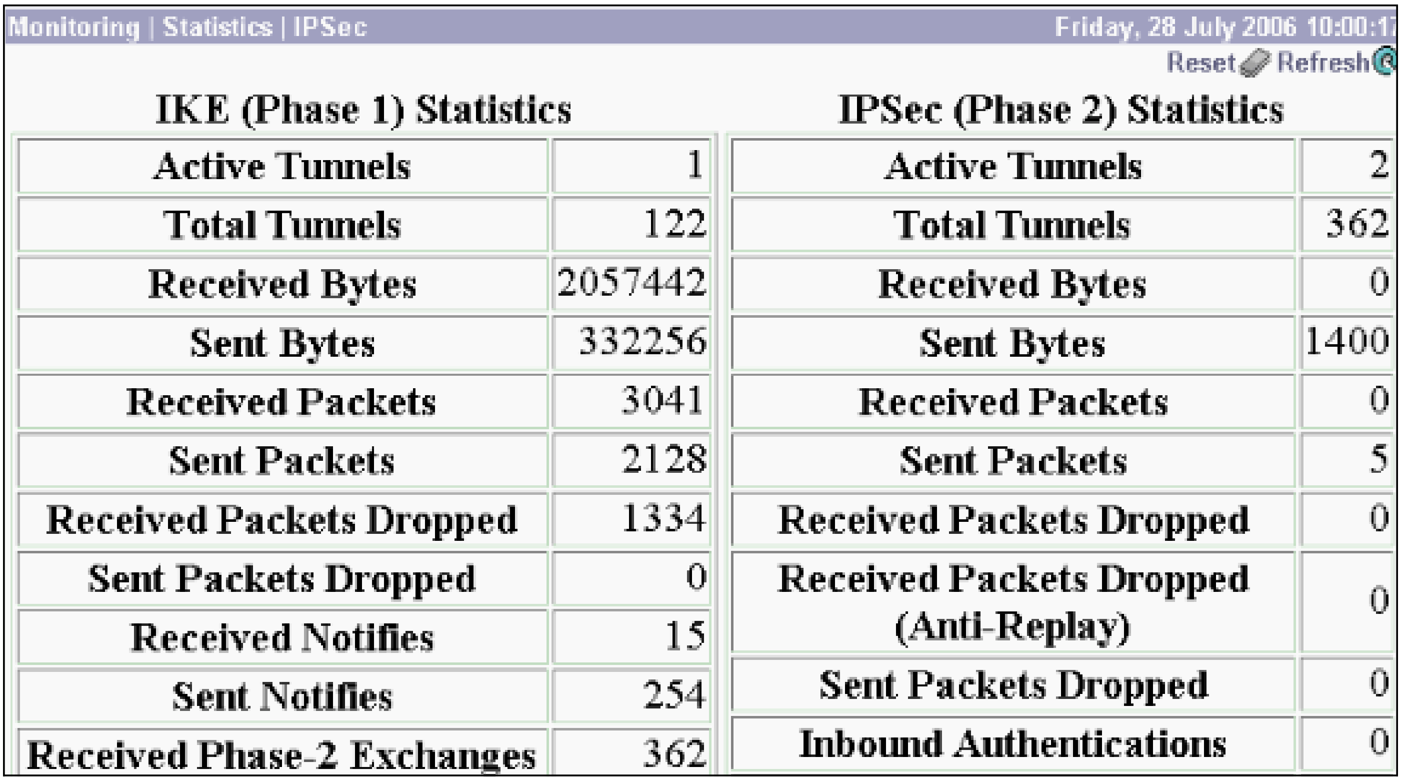


Monitoring | Filterable Event Log

Select Filter Options

Event Class	All Classes AUTH AUTHDBG AUTHDECODE	Severities	ALL 1 2 3
Client IP Address	0.0.0.0	Events/Page	100
Group	-All-	Direction	Oldest to Newest

Per visualizzare le statistiche del protocollo IPSec, scegliere **Monitoraggio > Statistiche > IPSec.** In questa finestra vengono visualizzate le statistiche relative all'attività di IPSec, inclusi i tunnel IPSec correnti, nel concentratore VPN dall'ultimo avvio o reimpostazione. Queste statistiche sono conformi alla bozza IETF per il MIB di monitoraggio del flusso IPsec. Anche la finestra **Monitoraggio > Sessioni >** Dettagli mostra i dati IPSec.


Monitoring | Statistics | IPSec
Friday, 28 July 2006 10:00:17
Reset
Refresh

IKE (Phase 1) Statistics

Active Tunnels	1
Total Tunnels	122
Received Bytes	2057442
Sent Bytes	332256
Received Packets	3041
Sent Packets	2128
Received Packets Dropped	1334
Sent Packets Dropped	0
Received Notifies	15
Sent Notifies	254
Received Phase-2 Exchanges	362

IPSec (Phase 2) Statistics

Active Tunnels	2
Total Tunnels	362
Received Bytes	0
Sent Bytes	1400
Received Packets	0
Sent Packets	5
Received Packets Dropped	0
Received Packets Dropped (Anti-Replay)	0
Sent Packets Dropped	0
Inbound Authentications	0

Problemi che possono verificarsi

- Il router Cisco IOS rimane bloccato nello stato AG_INIT_EXCH. Durante la risoluzione dei problemi, attivare i debug IPsec e ISAKMP con questi comandi:**debug crypto ipsecdebug crypto isakmpdebug crypto ezvpn**Sul router Cisco IOS, viene visualizzato quanto segue:

```
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
```

  Sul concentratore VPN 3000, è richiesto Xauth. Tuttavia, la proposta selezionata non supporta Xauth. Verificare che l'autenticazione interna per Xauth sia specificata. Abilitare l'autenticazione interna e verificare che la modalità di autenticazione delle proposte IKE sia impostata su **Chiavi già condivise (Xauth)**, come nella schermata precedente. Per modificare la proposta, fare clic su **Modifica**.
- Password non corretta.Il messaggio **Password non valida** non viene visualizzato sul router Cisco IOS. Sul concentratore VPN, è possibile che venga visualizzato l'**evento imprevisto Received EV_ACTIVATE_NEW_SA nello stato AM_TM_INIT_XAUTH.**Assicurarsi che la password sia corretta.
- Nome utente non corretto.Sul router Cisco IOS, se la password è errata, il debug è simile a questo. Su VPN Concentrator viene visualizzato il messaggio **Autenticazione rifiutata: Motivo = Impossibile trovare l'utente.**

Informazioni correlate

- Cisco VPN serie 3000 Concentrator Support Page
- Cisco Easy VPN Remote fase II
- Cisco VPN serie 3000 Client Support Page
- Pagina di supporto per la negoziazione IPsec/i protocolli IKE
- Documentazione e supporto tecnico – Cisco Systems