EzVPN met NEM op IOS-router met VPN 3000 Concentrator Configuratievoorbeeld

Inhoud

Inleiding

Dit document legt de procedure uit die u gebruikt om een Cisco IOS® router te configureren als een EzVPN in Network Extension Mode (NEM) om verbinding te maken met een Cisco VPN 3000 Concentrator. Een nieuwe fase-II-functie van EzVPN is ondersteuning voor een basisconfiguratie voor netwerkadresomzetting (NAT). De EzVPN fase II is afgeleid van het Unity Protocol (VPN-clientsoftware). Het externe apparaat is altijd de initiator van de IPsec-tunnel. Internet Key Exchange (IKE) en IPsec-voorstellen zijn echter niet Configureerbaar op de EzVPN-client. De VPN-client onderhandelt over voorstellen met de server.

Om IPsec te configureren tussen een PIX/ASA 7.x en een Cisco 871-router die Easy VPN gebruikt, raadpleegt u PIX/ASA 7.x Easy VPN met een ASA 5500 als de Server en Cisco 871 als het Easy VPN Configuration-voorbeeld.

Om IPsec te configureren tussen de Cisco IOS® Easy VPN Remote Hardware Client en de PIX Easy VPN Server, raadpleegt u IOS Easy VPN Remote Hardware Client naar een PIX Easy VPN Server Configuratievoorbeeld.

Om Cisco 7200 router als een EzVPN en Cisco 871 router als de Easy VPN-afstandsbediening te

configureren raadpleegt u 7200 Easy VPN-server aan 871 Easy VPN-afstandsconfiguratievoorbeeld.

Voorwaarden

Vereisten

Voordat u deze configuratie probeert te controleren dat de Cisco IOS-router de optie EzVPN Fase II ondersteunt en de IP-connectiviteit heeft met end-to-end verbindingen om de IPsec-tunnel op te zetten.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS-softwarerelease 12.2(8)YJ (EzVPN fase II)
- VPN 3000 Concentrator 3.6.x
- Cisco 1700 router

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Opmerking: Deze configuratie is onlangs getest met een Cisco 3640 router met Cisco IOS-softwarerelease 12.4(8) en de VPN 3000 Concentrator 4.7.x versie.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

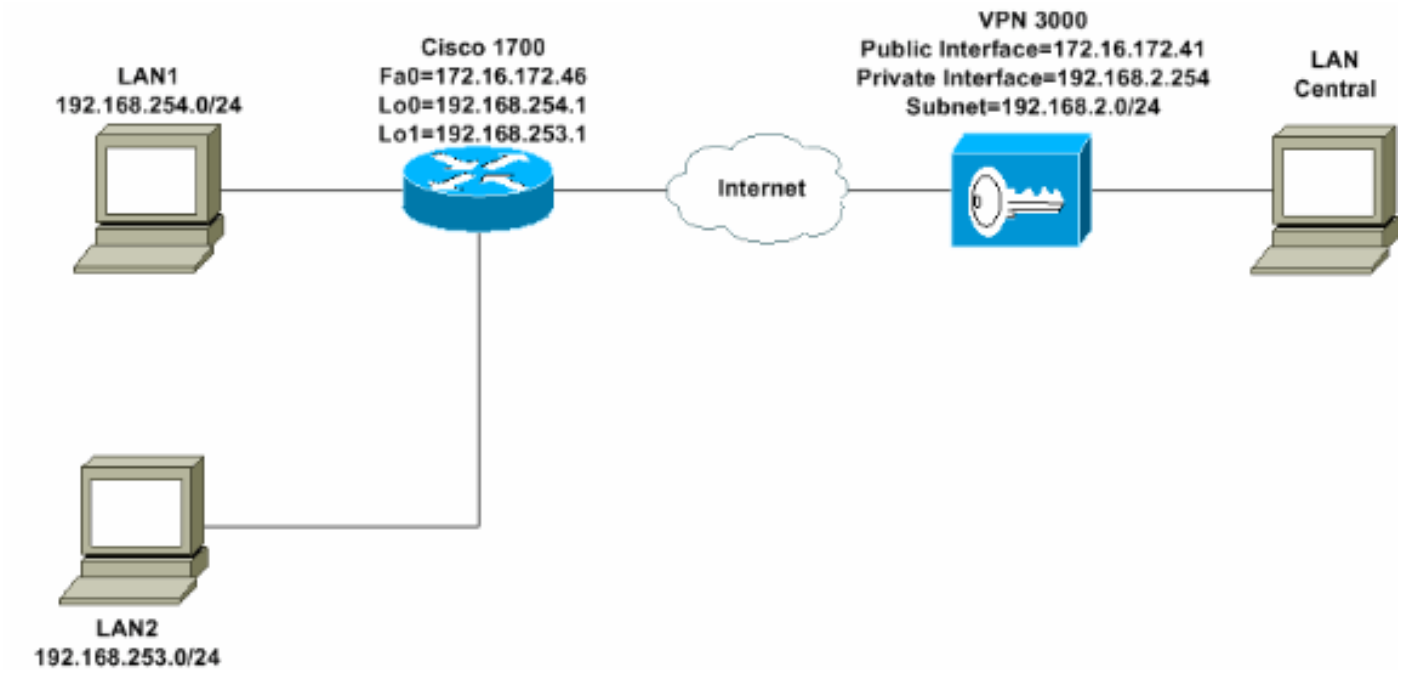
De VPN 3000-concentratie configureren

Taak

In deze sectie, wordt u voorgesteld met de informatie om de VPN 3000 Concentrator te configureren.

Netwerkdiagram

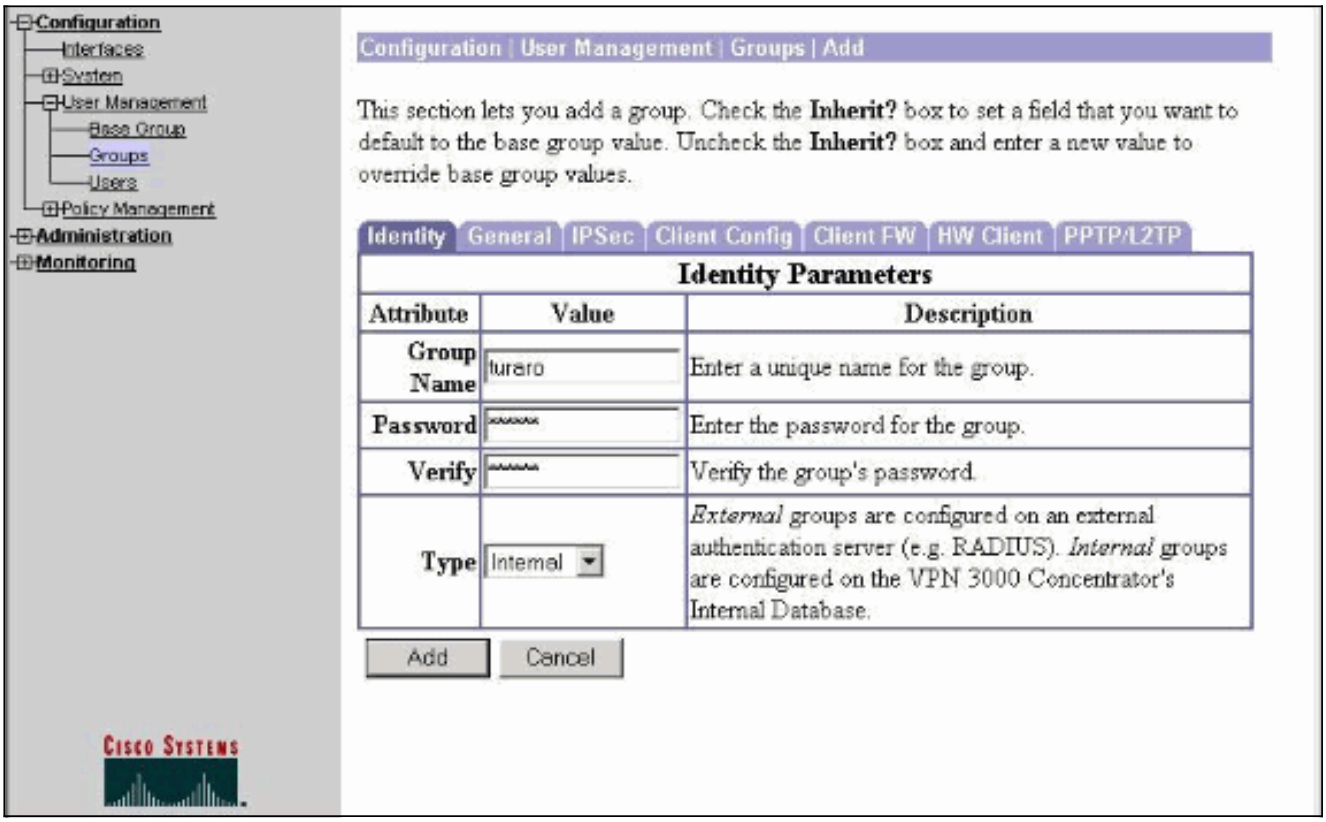
Dit document gebruikt de netwerkinstellingen die in dit diagram worden weergegeven. De interfaces van de Loopback worden gebruikt als interne subnetten, en FastEthernet 0 is de standaard aan Internet.



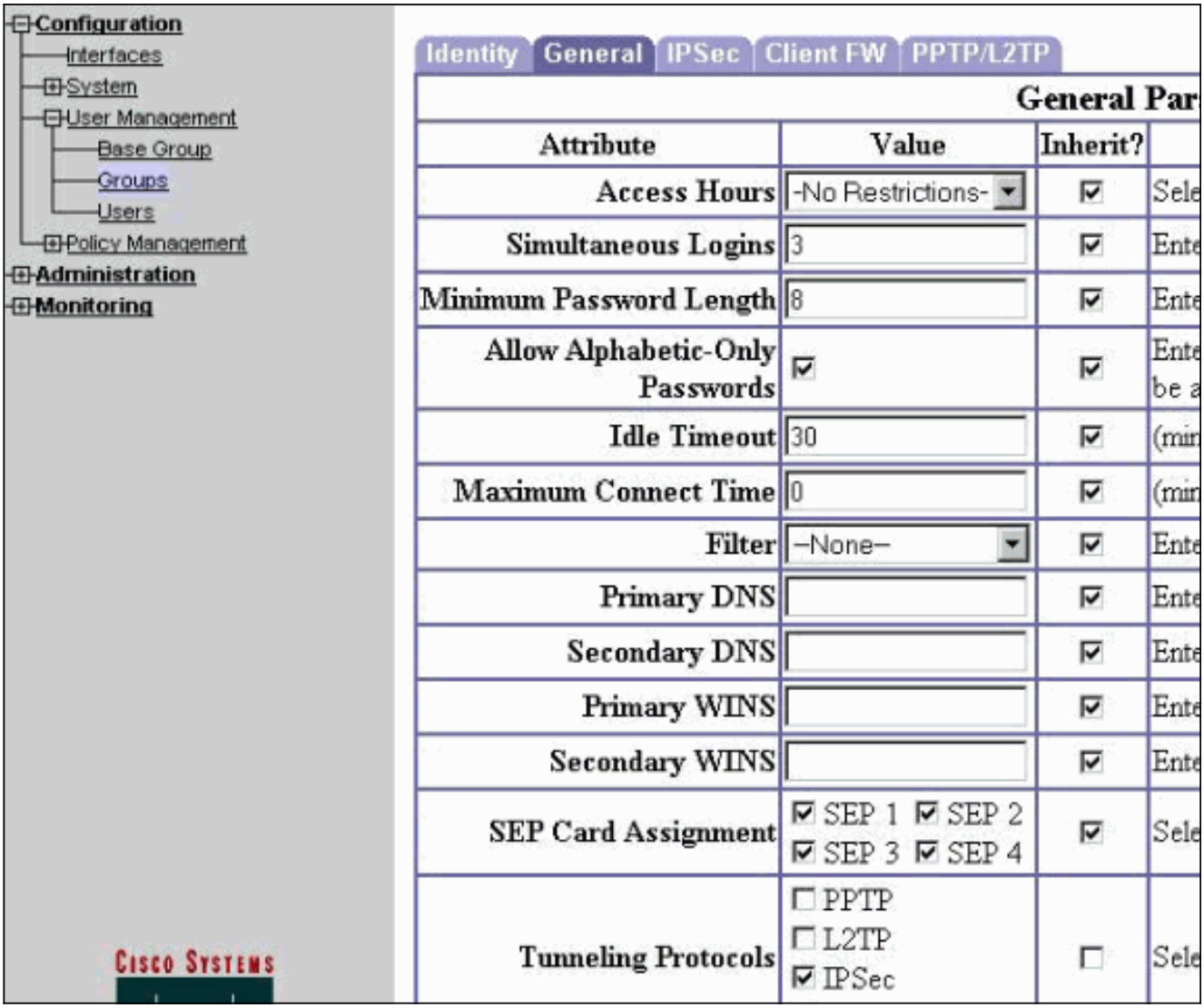
Stap voor stap-instructies

Voer de volgende stappen uit:

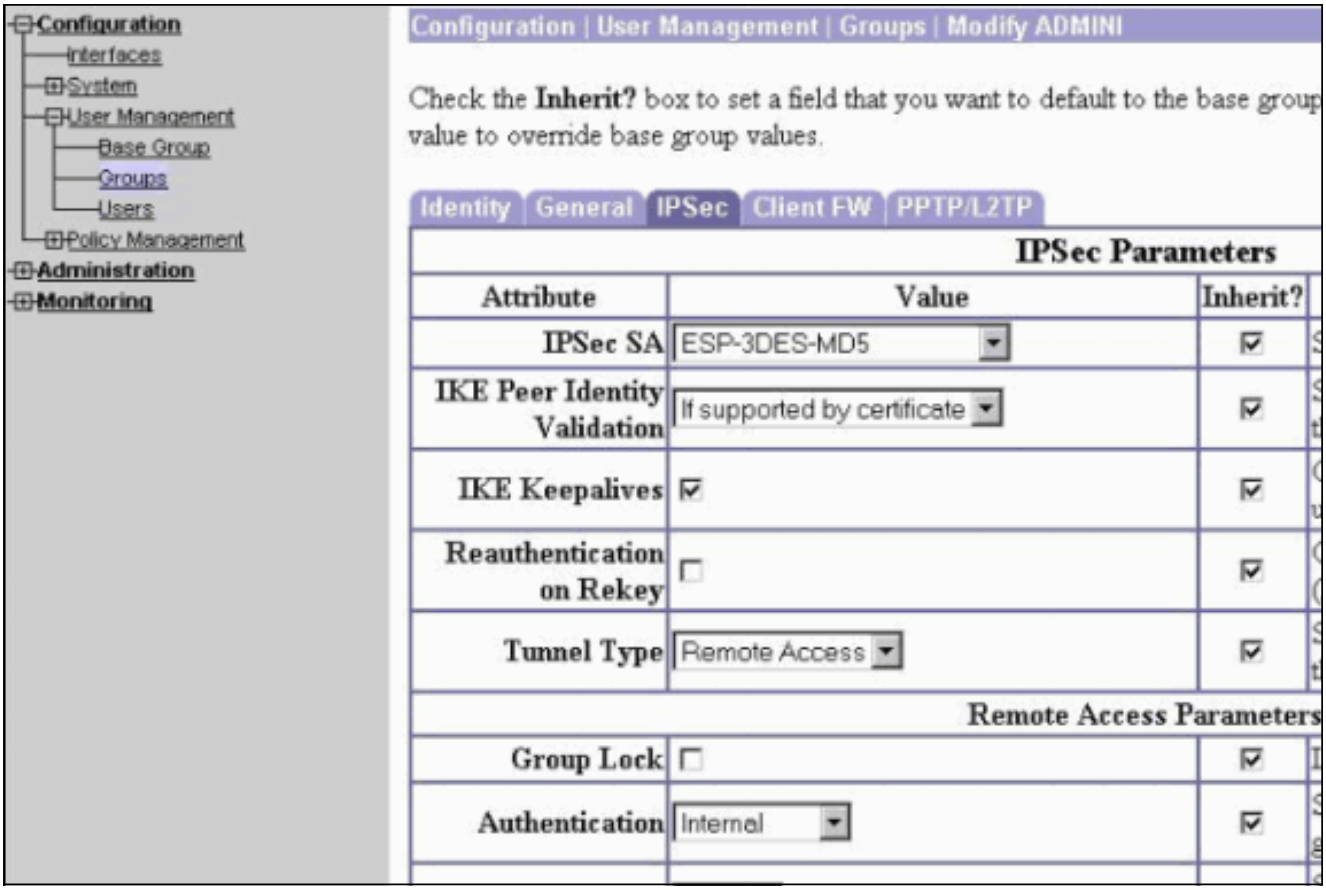
1. Kies **Configuration > User Management > Groepen > Add** en definieer een groepsnaam en een wachtwoord om een IPsec-groep voor de gebruikers te configureren.Dit voorbeeld gebruikt de groepsnaam **turaro** met wachtwoord/verify **tulo**.



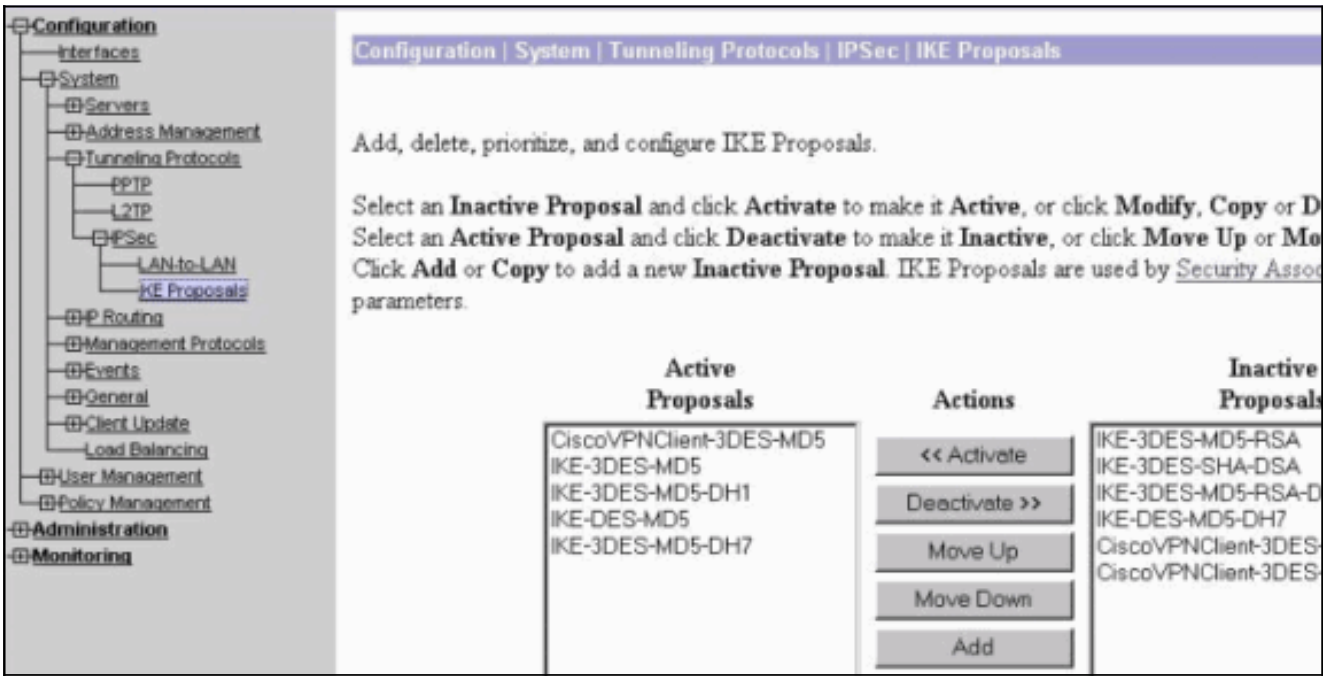
2. Kies **Configuration > User Management > Groepen > Turbo > General om IPSec in te schakelen en Point-to-Point Tunneling Protocol (PPTP) en Layer 2 Tunnel Protocol (L2TP) uit te schakelen.**Maak uw selectie en klik op **Toepassen**.



3. Stel verificatie in op **interne** verificatie (Xauth) en zorg ervoor dat het tunneltype **afstandsbediening** is en dat IPSec SA **ESP-3DES-MD5** is.

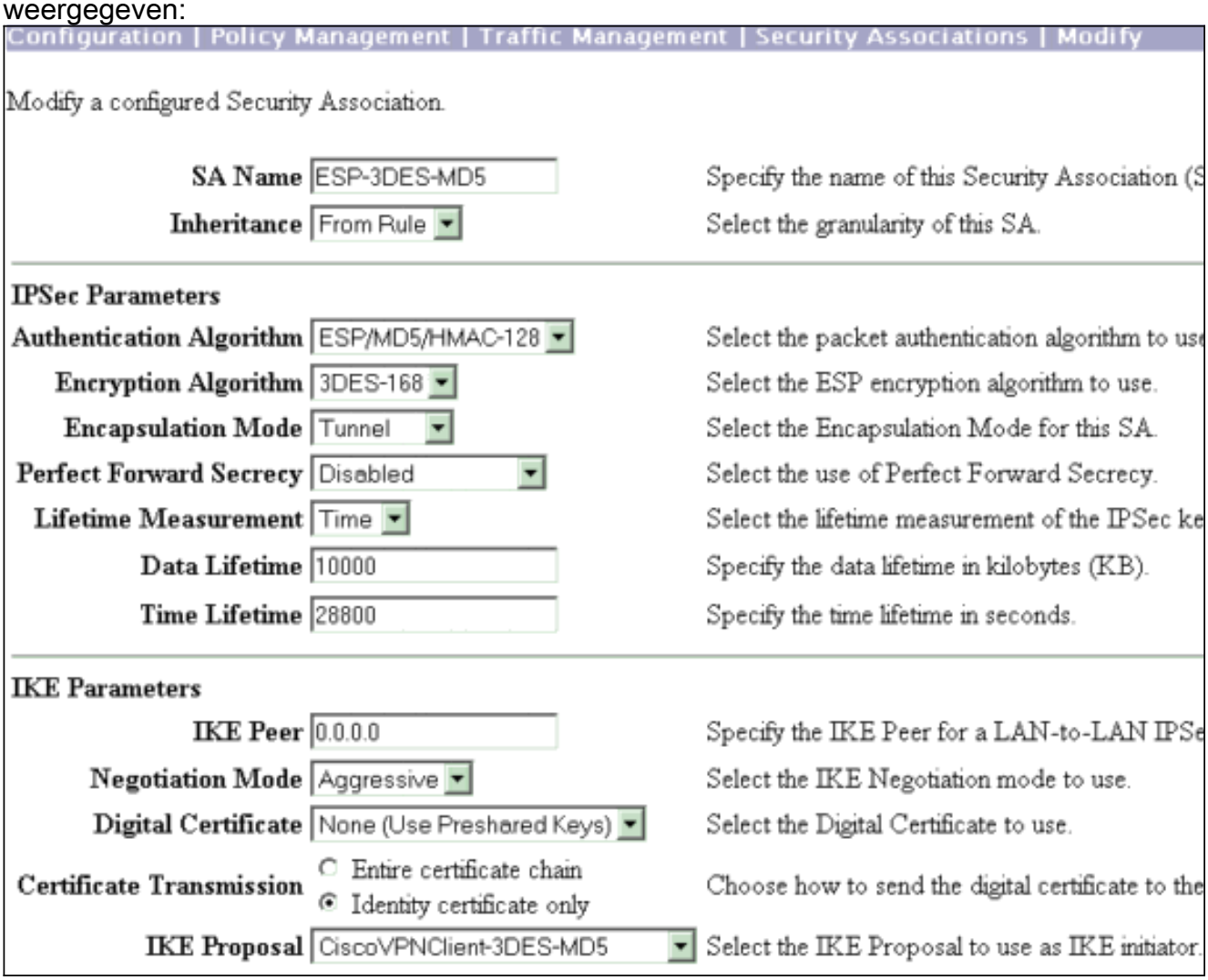


4. Kies **Configuration > System > Tunneling Protocols > IPSec > IKE-voorstellen** om te verzekeren dat de Cisco VPN-client (Cisco VPN-client-3DES-MD5) zich in actieve voorstellen voor IKE bevindt (fase 1).**Opmerking:** Van VPN Concentrator 4.1.x is de procedure anders om ervoor te zorgen dat de Cisco VPN-client in de lijst met actieve voorstellen voor IKE (fase 1) staat. Kies **Configuration > Tunneling en Security > IPSec > IKE-voorstellen.**



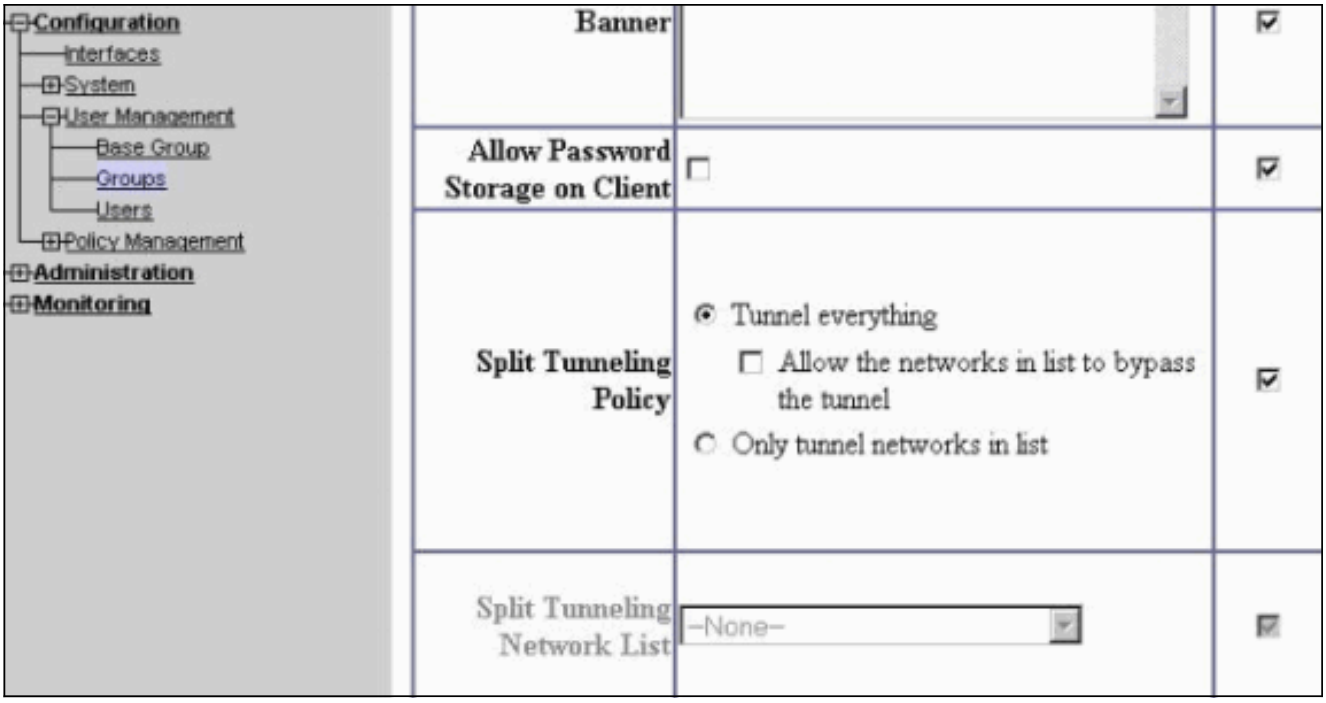
5. Controleer de IPsec Security Association (SA).Op stap 3 is uw IPsec SA ESP-3DES-MD5. U kunt een nieuwe creëren als u wilt maar zorg ervoor dat u de juiste IPsec SA in uw groep gebruikt. U dient Perfect Forward Security (PFS) uit te schakelen voor de IPsec SA dat u gebruikt. Selecteer de Cisco VPN-client als het IKE-voorstel door **Configuration > Policy**

Management > Traffic Management > SA's te kiezen. Typ de SA-naam in het tekstvak en selecteer de gewenste opties zoals hieronder wordt weergegeven:

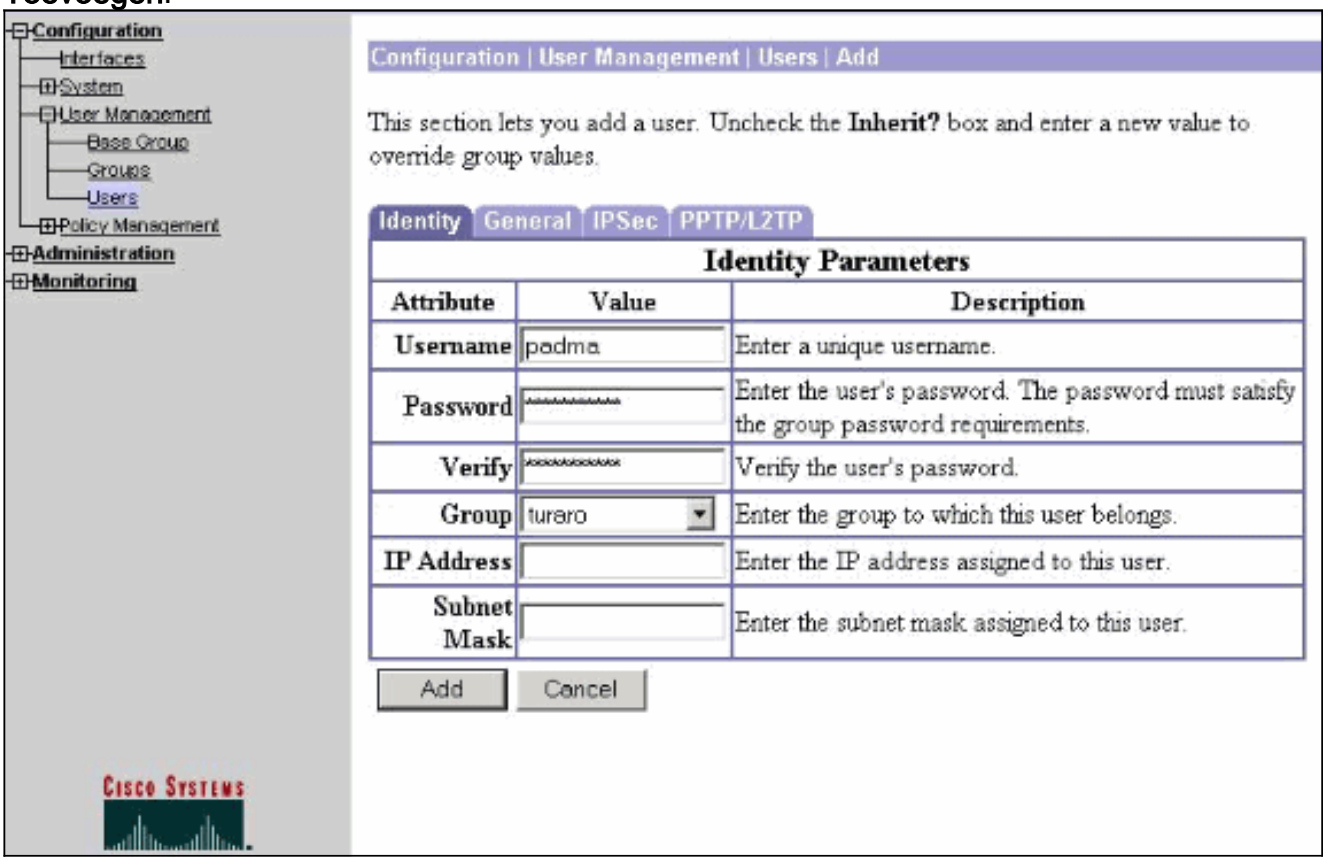


Opmerking: Deze stap en de volgende stap zijn optioneel als u liever een vooraf gedefinieerde SA kiest. Als uw client een dynamisch toegewezen IP-adres heeft, gebruikt u 0.0.0.0 in het tekstvak IKE peer. Zorg ervoor dat het IKE Proposal is ingesteld op **CiscoVPN-client-3DES-MD5** zoals in dit voorbeeld wordt aangegeven.

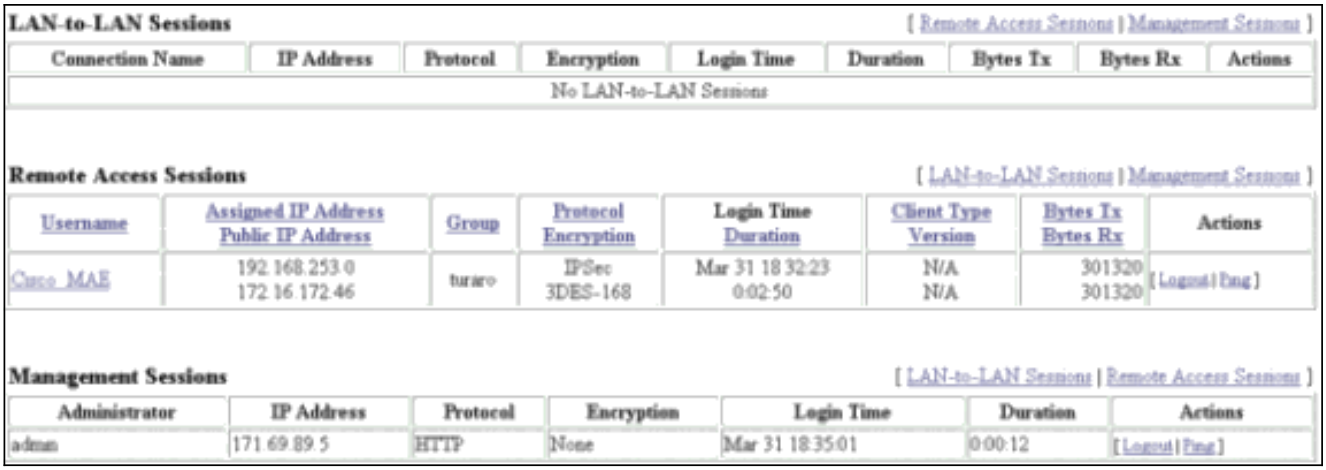
6. U moet **niet** op *Toestaan de netwerken in de lijst klikken om de tunnel te omzeilen*. De reden is dat gesplitste tunneling wordt ondersteund, maar de omzeilingsfunctie wordt niet ondersteund met de optie EzVPN-client.



7. Kies **Configuration > User Management > Gebruikers** om een gebruiker toe te voegen. Defineer een gebruikersnaam en een wachtwoord, wijs deze aan een groep toe en klik op **Toevoegen**.



8. Kies **Administratie > Admin Sessies** en controleer of de gebruiker is aangesloten. In NEM wijst de VPN Concentrator geen IP-adres uit de pool toe.**Opmerking:** Deze stap is optioneel als u liever een vooraf gedefinieerde SA
kiest.



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. Klik op het **pictogram Opslaan nodig** of op het pictogram **Opslaan** om de configuratie op te slaan.

Routerconfiguratie

Versie-uitgang tonen

```
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
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Zodra u beide apparaten vormt, probeert de Cisco 3640-router de VPN-tunnel in te stellen door automatisch contact op te nemen met de VPN-centrator met het IP-adres van de peer. Nadat de

eerste ISAKMP-parameters zijn uitgewisseld, geeft de router dit bericht weer:

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

U moet de opdracht **crypto ipsec client ezvpn xauth** invoeren die u om een gebruikersnaam en wachtwoord vraagt. Dit moet overeenkomen met de gebruikersnaam en het wachtwoord die in de VPN-Concentrator zijn ingesteld (stap 7). Zodra de gebruikersnaam en het wachtwoord door beide peers zijn overeengekomen, wordt de rest van de parameters overeengekomen en komt de IPsec VPN-tunnel naar boven.

```
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
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten voor troubleshooting

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten afgeeft.

- **debug van crypto ipsec client ezvpn**-displays die de configuratie en implementatie van de EzVPN-clientfunctie toont.
- **debug van crypto ipsec**-displays debug informatie over IPsec-verbindingen.
- **debug crypto isakmp**-displays debug informatie over IPsec verbindingen en toont de eerste reeks eigenschappen die worden ontkend als gevolg van onverenigbaarheden op beide eindpunten.
- **tonen debug**-displays de staat van elke optie voor het foutoptreden.

Uitvoer van debug-opdrachten

Zodra u de opdracht **crypto ipsec client ezvpn SJVPN** ingeeft, probeert de EzVPN-client verbinding te maken met de server. Als u de opdracht **connect handleiding** wijzigt onder de groepsconfiguratie, voert u de **crypto ipsec client ezvpn in om SJVPN-**opdracht te **verbinden** om

de uitwisseling van voorstellen met de server te starten.

```
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
```

Verwante Cisco IOS-show Opdrachten voor probleemoplossing

```
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:
```

Een actieve tuner wissen

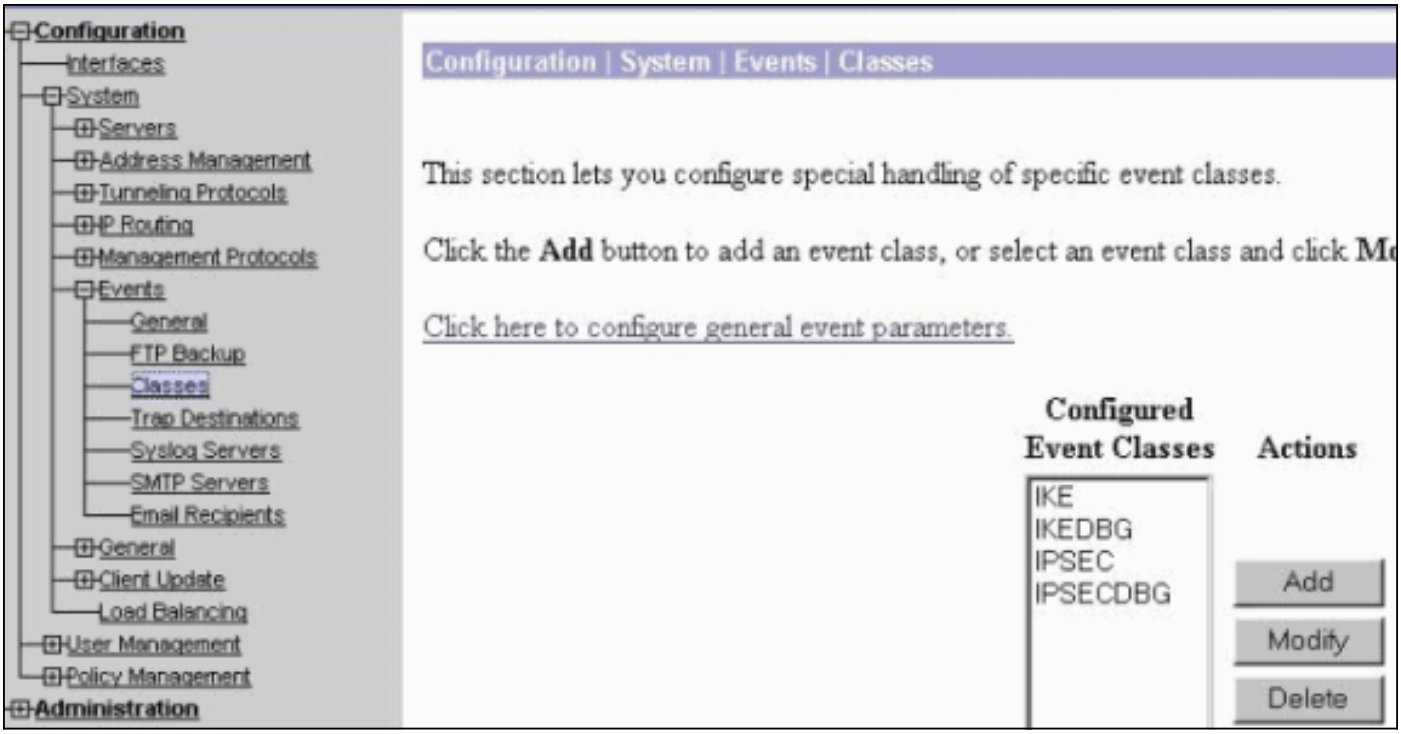
U kunt de tunnels met deze opdrachten verwijderen:

- **duidelijke cryptografie isakmp**
- **crypto sa**
- **duidelijke crypto ipsec-client ezvpn**

N.B.: U kunt de VPN-centrator gebruiken om de sessie te beëindigen wanneer u **Administratie > Admin-sessies** kiest, de gebruiker in **Remote Access Session** selecteert en **logout** klikt.

VPN 3000 Concentrator-debug

Kies **Configuratie > Systeem > Gebeurtenissen > Klassen** om dit **te** debug in te schakelen als er problemen zijn met de verbinding. U kunt altijd meer klassen toevoegen als de weergegeven klassen u niet helpen het probleem te identificeren.



Om het huidige logbestand van de gebeurtenis in het geheugen te bekijken, filtreerbaar door gebeurtenis klasse, ernst, IP adres, enzovoort, kies **Controle > Filterable Event log**.

Om de statistieken van het IPsec protocol te bekijken, kiest u **Controle > Statistieken > IPSec.** Dit venster toont statistieken voor IPsec-activiteit, inclusief de huidige IPsec-tunnels, op de VPN-centrator sinds deze voor het laatst is opgestart of hersteld. Deze statistieken voldoen aan het IETF ontwerp voor de IPsec Flow Monitoring MIB. Het venster **Monitoring > Sessions > Detail** geeft ook IPsec-gegevens weer.

Monitoring | Statistics | IPSec   Friday, 28 July 2006 10:00:1

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

Wat er kan misgaan

- De Cisco IOS router zit vast in de AG_INIT_EXCH staat. Wanneer u een oplossing hebt gevonden, schakelt u IPsec en ISAKMP versies in met deze opdrachten:**crypto ipsec debugdebug van crypto isakmpdebug van crypto ezvpn**Op de Cisco IOS router ziet u dit:

```
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
```

  Op de VPN 3000 Concentrator is Xauth vereist. Het geselecteerde voorstel steunt Xauth echter niet. Controleer dat de interne authenticatie voor Xauth gespecificeerd is. interne verificatie inschakelen en ervoor zorgen dat de IKE-voorstellen de verificatiemodus hebben ingesteld op **PreShared Keys (Xauth)**, zoals in het vorige screenshot. Klik op **Wijzigen** om het voorstel te bewerken.
- Het wachtwoord is onjuist.U ziet het **Ongeldige** Wachtwoord niet op de Cisco IOS-router. Op de VPN Concentrator **ziet** u **onverwachte gebeurtenis EV_ACTIVATE_NEW_SA in de deelstaat AM_TM_INIT_XAUTH.**Zorg ervoor dat uw wachtwoord juist is.
- De gebruikersnaam is onjuist.Op de Cisco IOS router ziet u een debug gelijkend op dit als u het verkeerde wachtwoord hebt. In VPN Concentrator wordt **verificatie verworpen: Reden = gebruiker is niet gevonden.**

Gerelateerde informatie

- Ondersteuning van Cisco VPN 3000 Series Concentrator-pagina
- Cisco Makkelijk VPN Remote Fase II
- Cisco VPN 3000 Series clientondersteuningspagina
- Ondersteuning van IPsec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie – Cisco Systems