EzVPN mit NEM auf IOS-Router mit VPN 300 Concentrator - Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird das Verfahren erläutert, mit dem Sie einen Cisco IOS®-Router als EzVPN im Network Extension Mode (NEM) konfigurieren, um eine Verbindung mit einem Cisco VPN 3000-Konzentrator herzustellen. Eine neue EzVPN Phase II-Funktion ist die Unterstützung einer grundlegenden Network Address Translation (NAT)-Konfiguration. Die EzVPN Phase II wird aus dem Unity Protocol (VPN Client Software) abgeleitet. Das Remote-Gerät ist immer der Initiator des IPsec-Tunnels. Angebote für Internet Key Exchange (IKE) und IPsec können jedoch nicht auf dem EzVPN-Client konfiguriert werden. Der VPN Client verhandelt Vorschläge mit dem Server.

Um IPsec zwischen einem PIX/ASA 7.x und einem Cisco 871-Router mit Easy VPN zu konfigurieren, lesen Sie PIX/ASA 7.x Easy VPN mit ASA 5500 als Server und Cisco 871 als Easy VPN Remote Configuration Example.

Informationen zum Konfigurieren von IPsec zwischen dem Cisco IOS® Easy VPN Remote Hardware Client und dem PIX Easy VPN Server finden Sie unter IOS Easy VPN Remote Hardware Client in einem Konfigurationsbeispiel für einen PIX Easy VPN Server.

Informationen zur Konfiguration eines Cisco 7200-Routers als EzVPN und des Cisco 871-Routers

als Easy VPN-Remote finden Sie im Konfigurationsbeispiel für den Easy VPN-Server 7200 zu 871 Easy VPN Remote.

Voraussetzungen

Anforderungen

Bevor Sie diese Konfiguration versuchen, überprüfen Sie, ob der Cisco IOS-Router die EzVPN Phase II-Funktion unterstützt und über die IP-Verbindung mit End-to-End-Verbindungen verfügt, um den IPsec-Tunnel einzurichten.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hinweis: Diese Konfiguration wurde kürzlich mit einem Cisco 3640 Router mit Cisco IOS Software Release 12.4(8) und der VPN 3000 Concentrator 4.7.x getestet.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

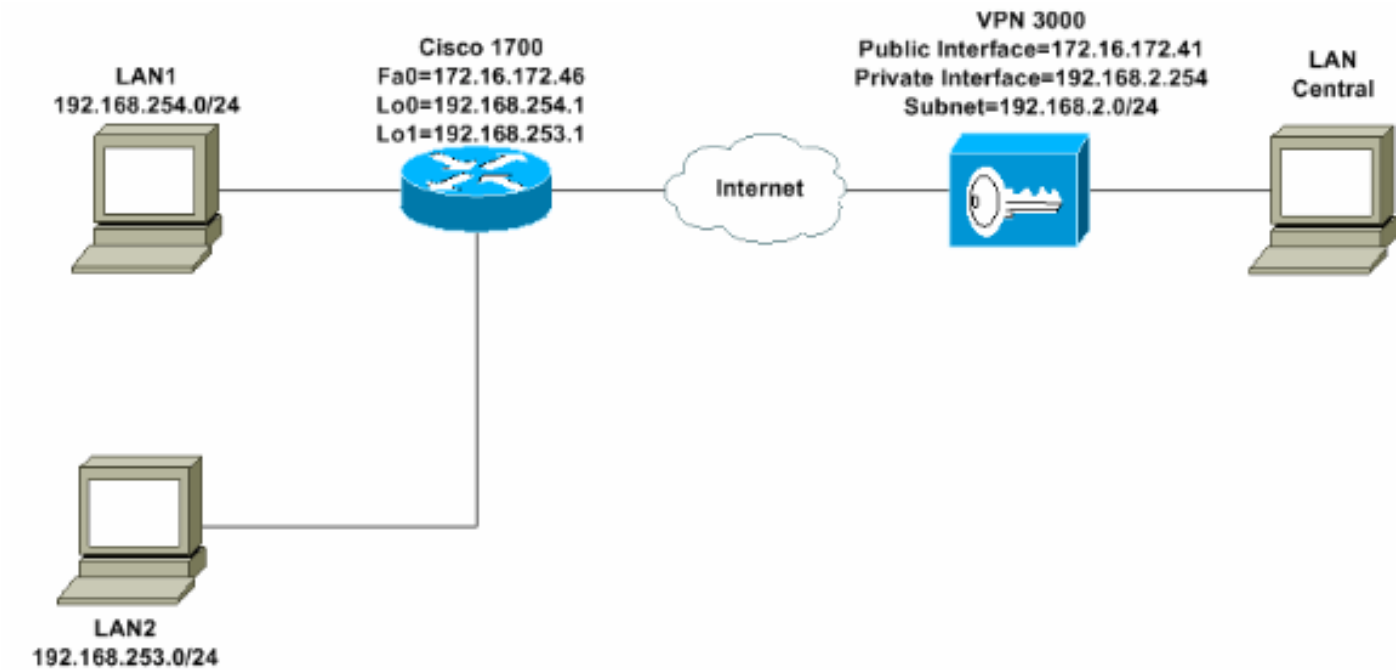
Konfigurieren des VPN 3000-Konzentrators

Aufgabe

In diesem Abschnitt werden die Informationen zum Konfigurieren des VPN 3000-Konzentrators angezeigt.

Netzwerkdiagramm

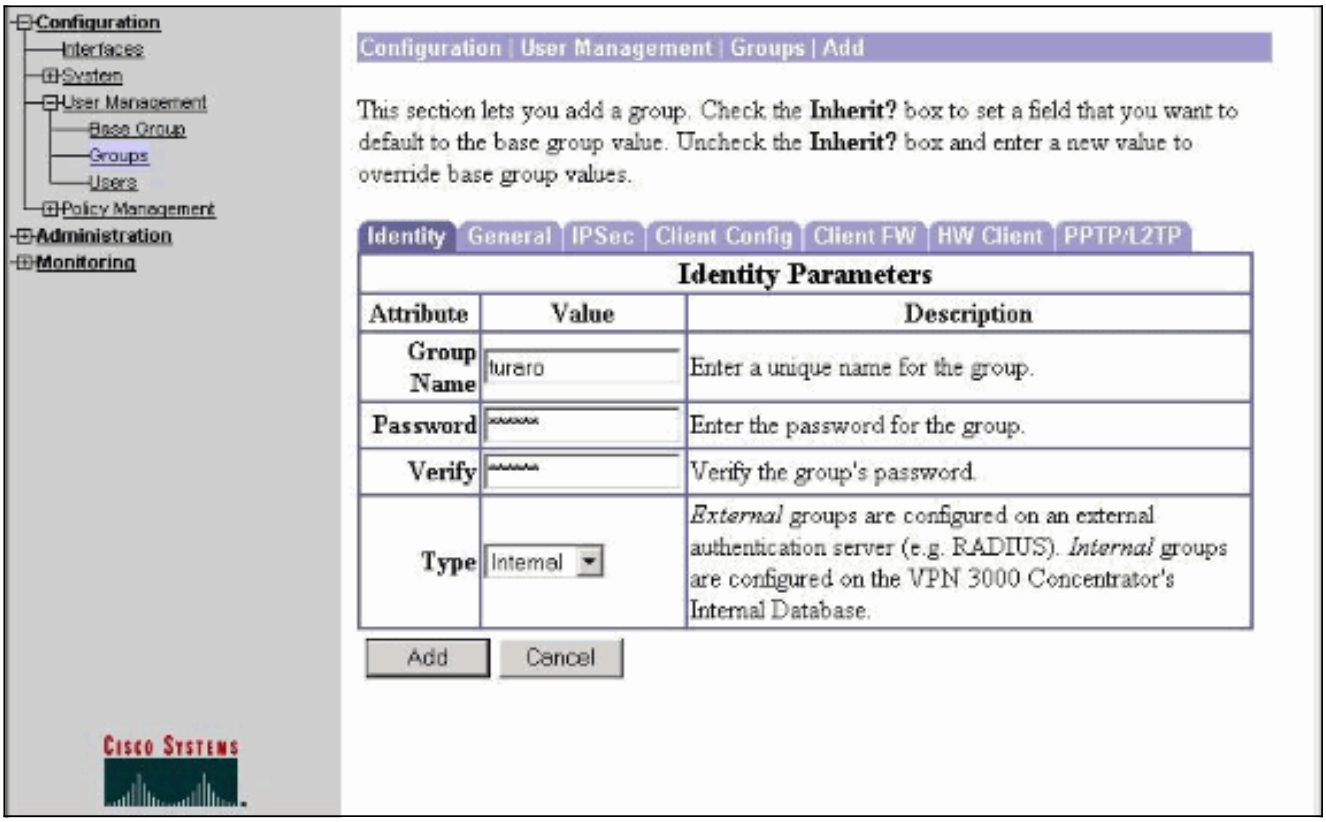
In diesem Dokument wird die in diesem Diagramm dargestellte Netzwerkeinrichtung verwendet. Loopback-Schnittstellen werden als interne Subnetze verwendet, und FastEthernet 0 ist die Standardeinstellung für das Internet.



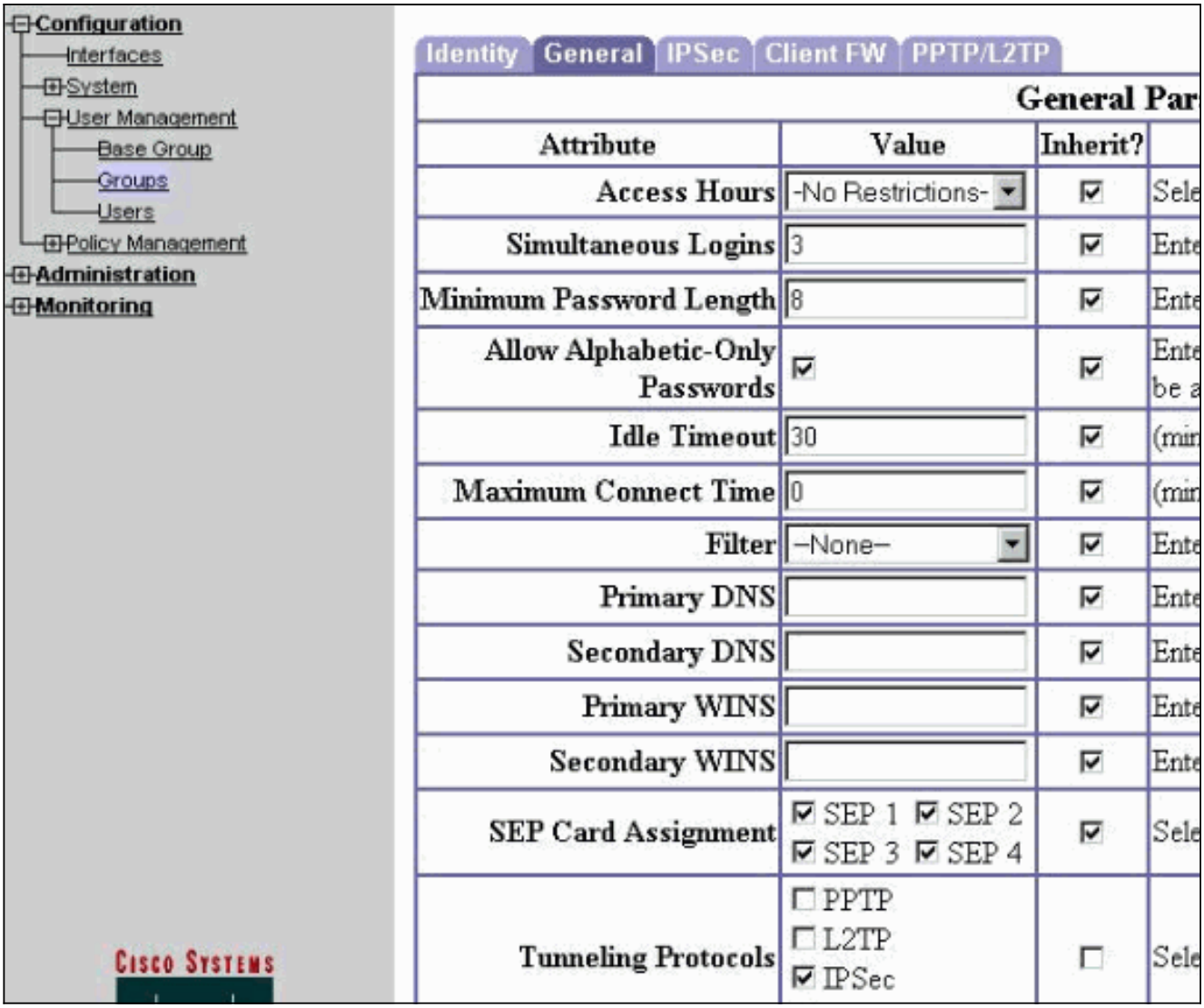
Schrittweise Anleitung

Gehen Sie wie folgt vor:

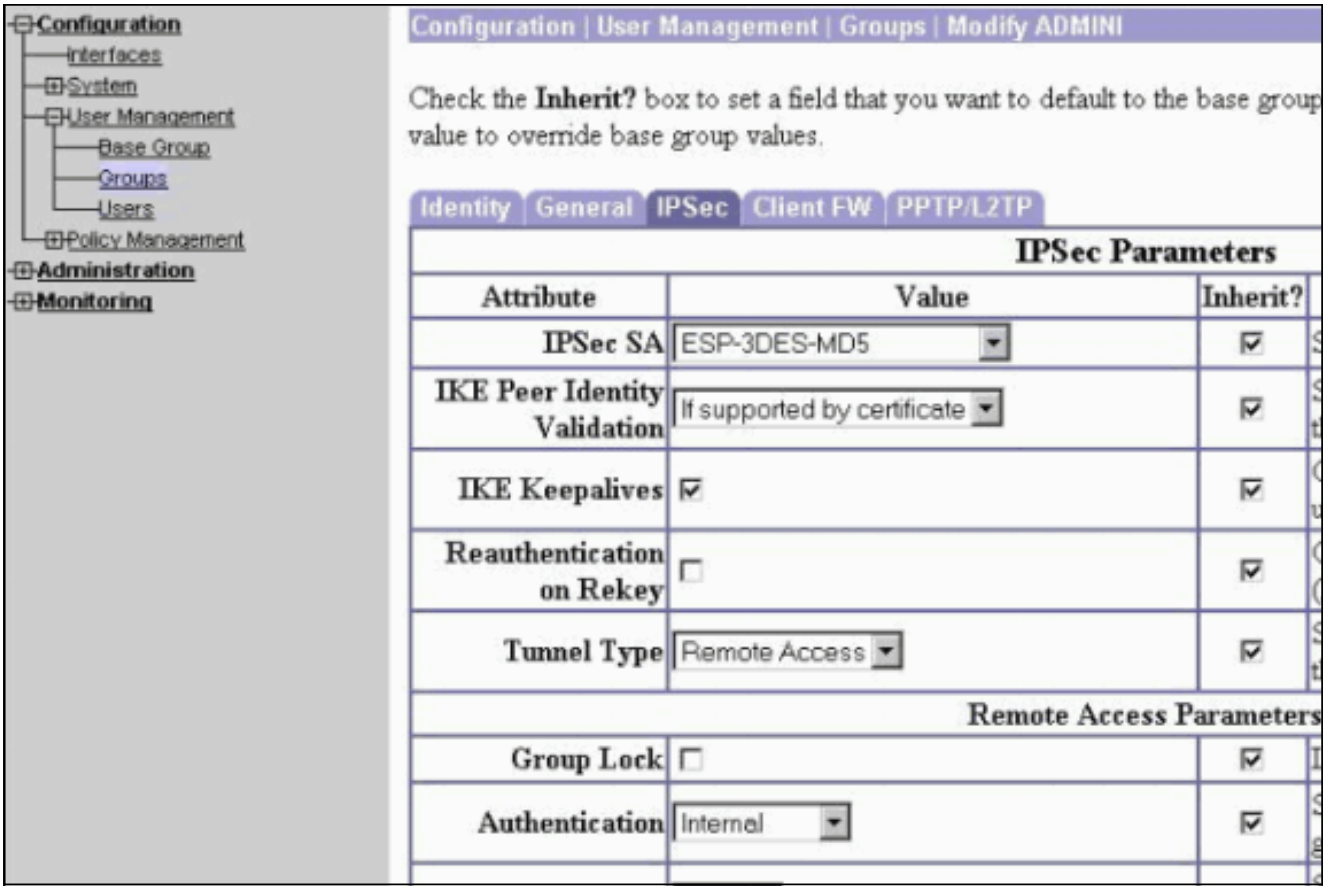
1. Wählen Sie **Configuration > User Management > Groups > Add** aus, und definieren Sie einen Gruppennamen und ein Kennwort, um eine IPsec-Gruppe für die Benutzer zu konfigurieren.In diesem Beispiel wird der Gruppenname **turaro** mit Kennwort/Verifizieren **tulo** verwendet.



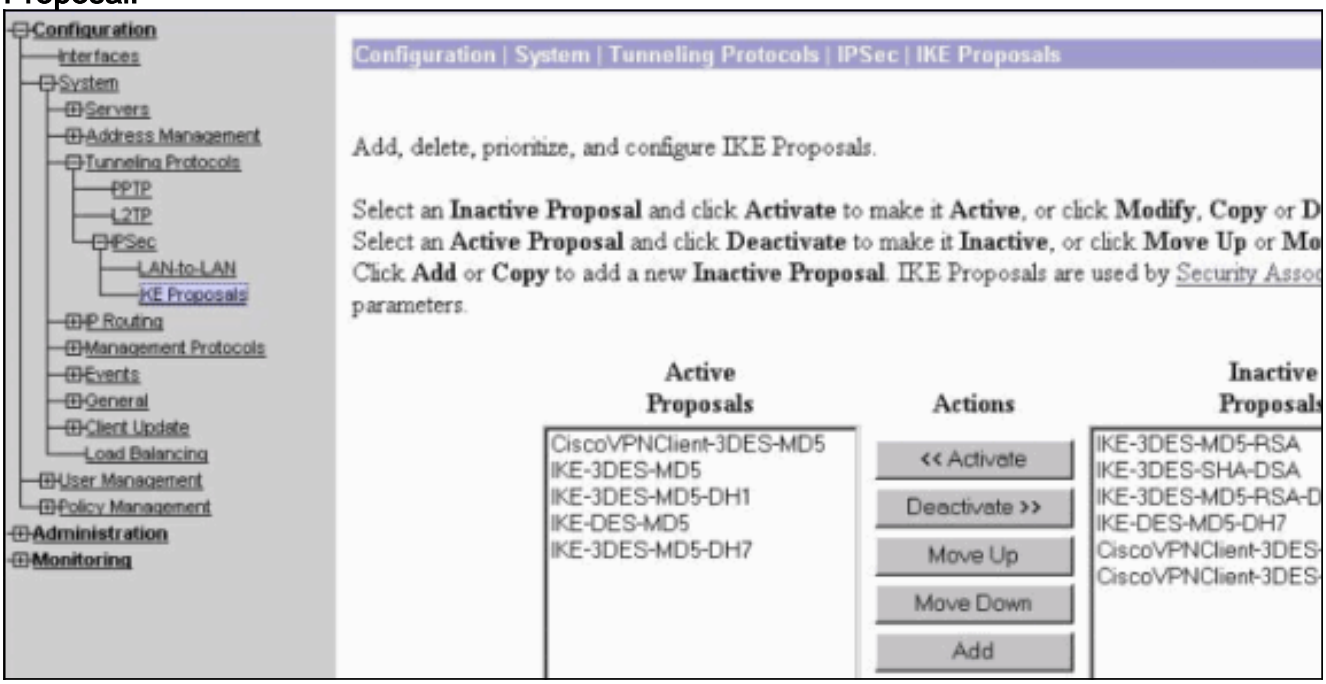
2. Wählen Sie **Configuration > User Management > Groups > turaro > General aus, um IPSec zu aktivieren und Point-to-Point Tunneling Protocol (PPTP) und Layer 2 Tunnel Protocol (L2TP) zu deaktivieren.**Treffen Sie eine Auswahl, und klicken Sie auf **Übernehmen**.



3. Legen Sie für die Authentifizierung **Internal** for Extended Authentication (Xauth) fest, und stellen Sie sicher, dass der Tunneltyp **Remote Access** und IPSec SA **ESP-3DES-MD5** ist.

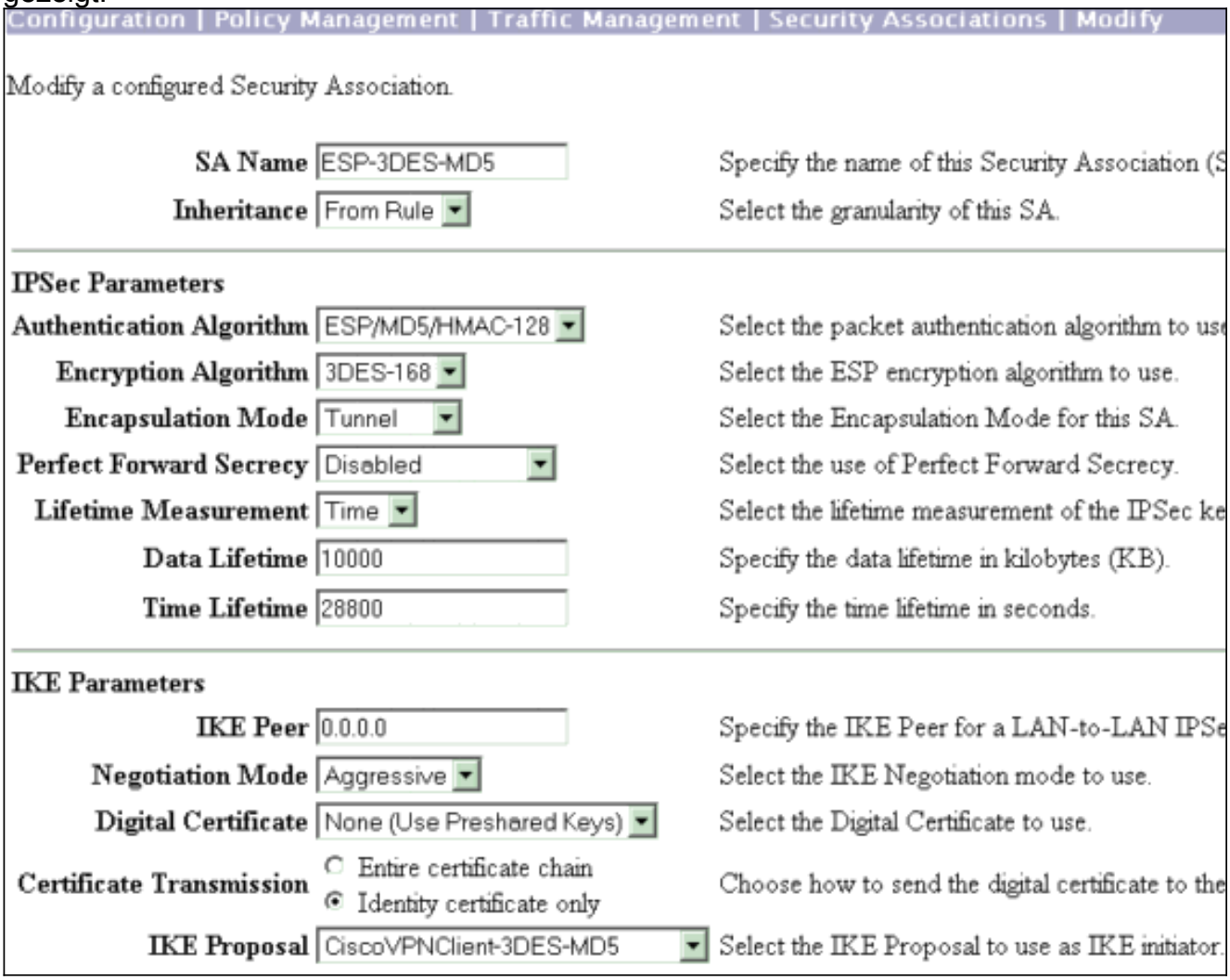


4. Wählen Sie **Configuration > System > Tunneling Protocols > IPSec > IKE Proposal**, um sicherzustellen, dass sich der Cisco VPN Client (CiscoVPNClient-3DES-MD5) in aktiven Vorschlägen für IKE (Phase 1) befindet.**Hinweis:** Ab VPN Concentrator 4.1.x wird anders verfahren, um sicherzustellen, dass der Cisco VPN Client in der Liste der aktiven Vorschläge für IKE enthalten ist (Phase 1). Wählen Sie **Configuration > Tunneling and Security > IPSec > IKE Proposal.**



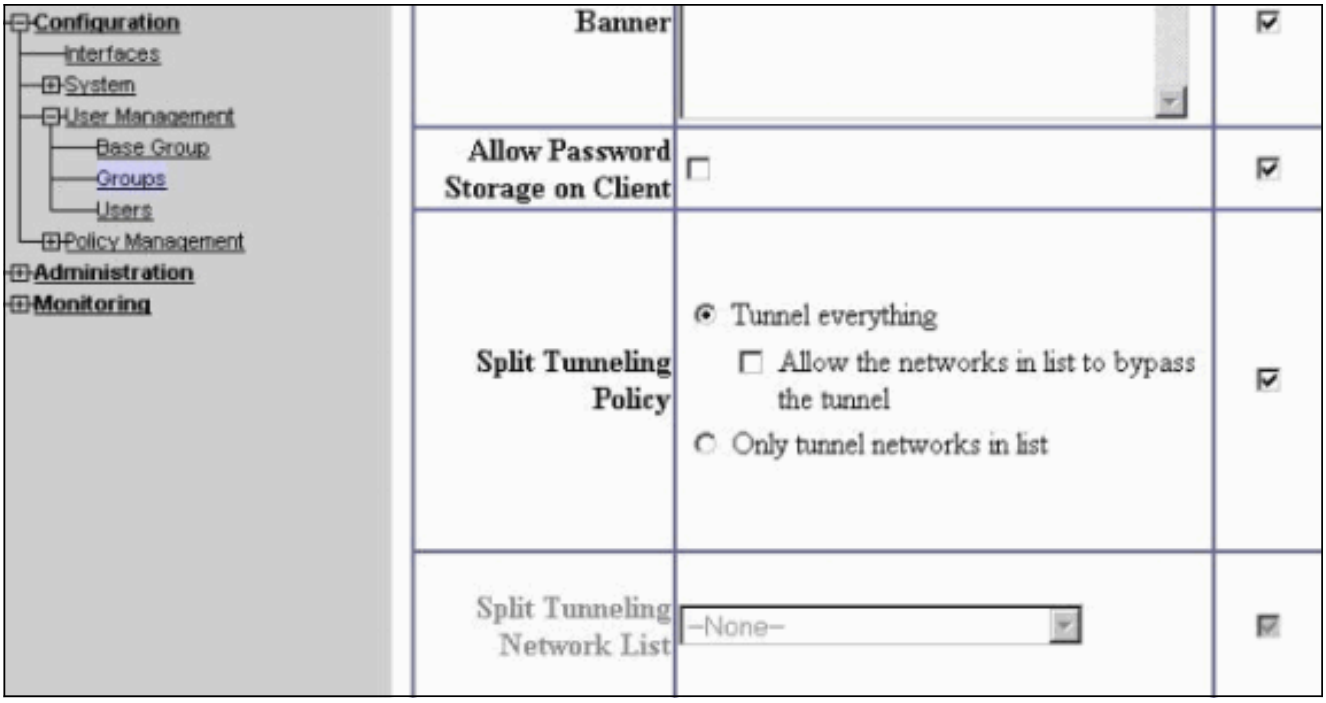
5. Überprüfen Sie Ihre IPsec Security Association (SA).In Schritt 3 ist Ihr IPsec SA ESP-3DES-MD5. Sie können eine neue erstellen, wenn Sie möchten, aber stellen Sie sicher, dass Sie die richtige IPsec SA für Ihre Gruppe verwenden. Sie sollten Perfect Forward Secrecy (PFS) für die von Ihnen verwendete IPsec SA deaktivieren. Wählen Sie den Cisco VPN Client als

IKE-Angebot aus, indem Sie **Configuration > Policy Management > Traffic Management > SAs** auswählen. Geben Sie den SA-Namen in das Textfeld ein, und treffen Sie die entsprechende Auswahl, wie hier gezeigt:

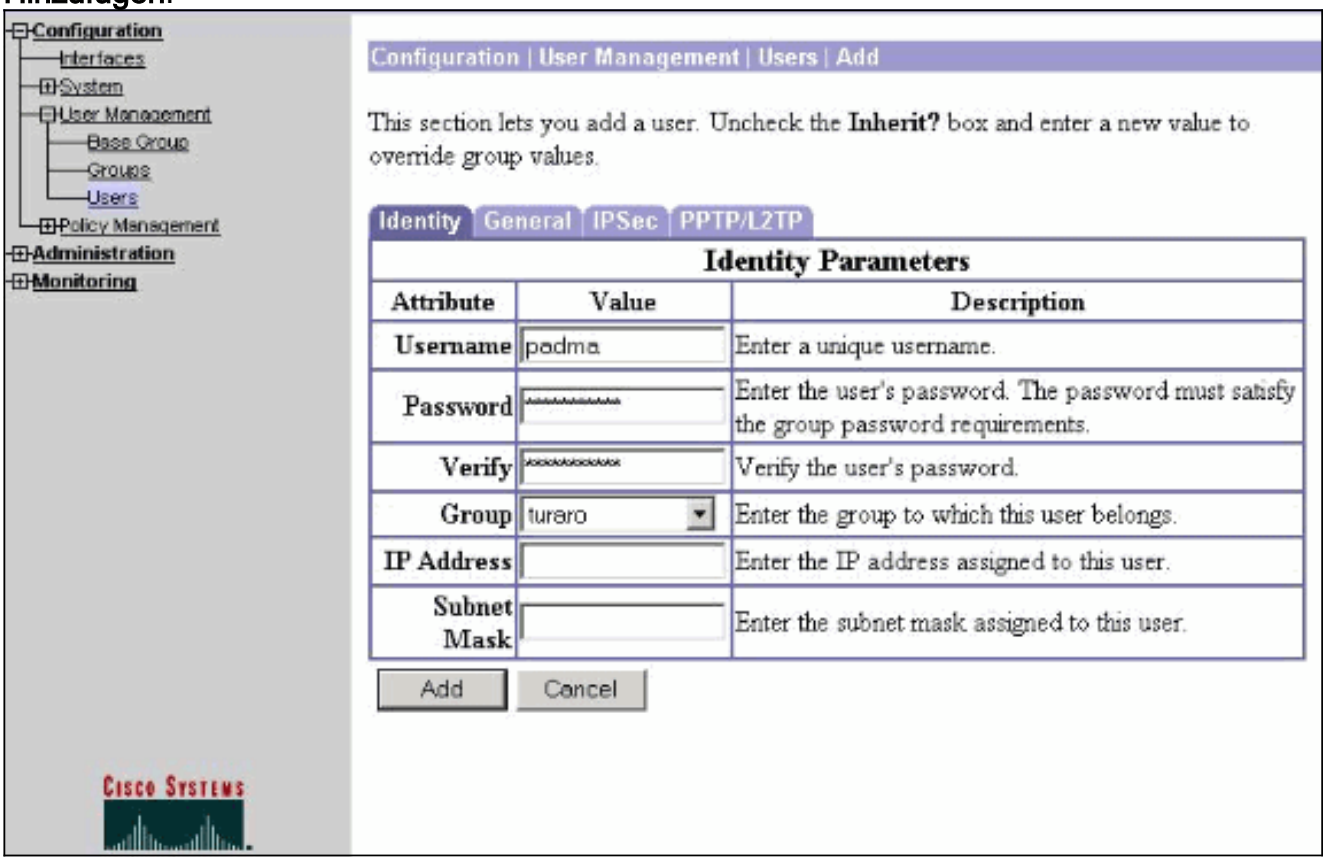


Hinweis: Dieser Schritt und der nächste Schritt sind optional, wenn Sie eine vordefinierte SA auswählen möchten. Wenn Ihr Client über eine dynamisch zugewiesene IP-Adresse verfügt, verwenden Sie im Textfeld für den IKE-Peer 0.0.0.0. Stellen Sie sicher, dass das IKE-Angebot auf **CiscoVPNClient-3DES-MD5** festgelegt ist, wie in diesem Beispiel gezeigt.

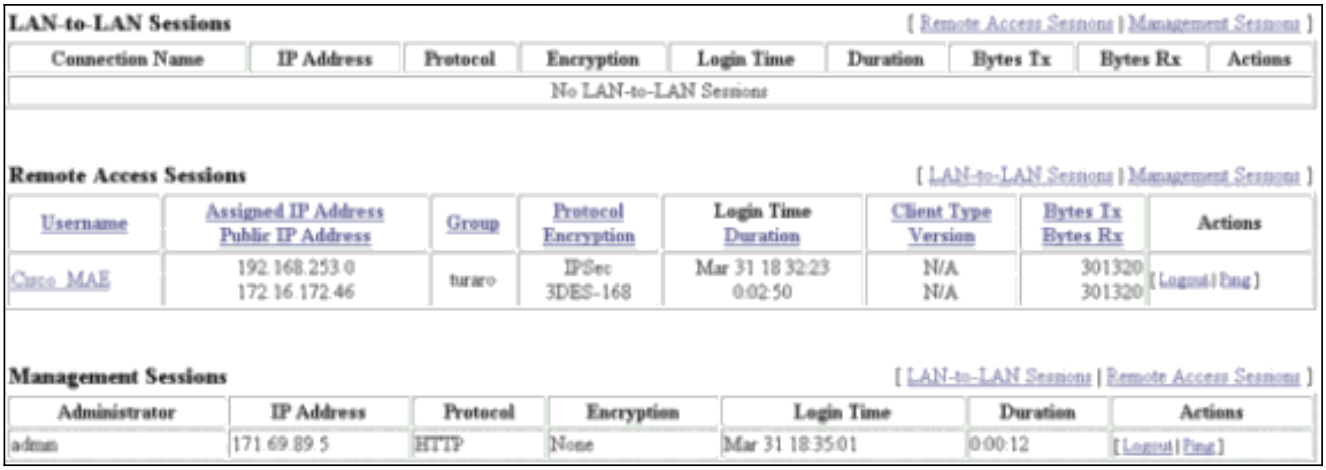
6. Sie dürfen **nicht** *auf Zulassen*, *dass die Netzwerke in der Liste den Tunnel umgehen*. Der Grund hierfür ist, dass Split-Tunneling unterstützt wird, die Umgehungsfunktion jedoch nicht von der EzVPN-Client-Funktion unterstützt wird.



7. Wählen Sie **Configuration > User Management > Users** aus, um einen Benutzer hinzuzufügen. Definieren Sie einen Benutzernamen und ein Kennwort, weisen Sie diesen einer Gruppe zu, und klicken Sie auf **Hinzufügen**.



8. Wählen Sie **Administration > Admin Sessions** und überprüfen Sie, ob der Benutzer verbunden ist. Im NEM weist der VPN Concentrator keine IP-Adresse aus dem Pool zu.**Hinweis:** Dieser Schritt ist optional, wenn Sie einen vordefinierten SA auswählen möchten.



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. Klicken Sie entweder auf das Symbol **Save Needed** (Erforderlich **speichern**) oder auf das **Symbol Save** (Speichern), um die Konfiguration zu speichern.

Routerkonfiguration

Ausgabe anzeigen

```
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
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Sobald Sie beide Geräte konfigurieren, versucht der Cisco 3640 Router, den VPN-Tunnel einzurichten, indem er den VPN-Konzentrator automatisch über die Peer-IP-Adresse kontaktiert.

Nachdem die ursprünglichen ISAKMP-Parameter ausgetauscht wurden, zeigt der Router die folgende Meldung an:

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

Sie müssen den Befehl **crypto ipsec client ezvpn xauth** eingeben, der Sie zur Eingabe von Benutzername und Kennwort auffordert. Dies muss mit dem im VPN Concentrator konfigurierten Benutzernamen und Kennwort übereinstimmen (Schritt 7). Sobald Benutzername und Kennwort von beiden Peers vereinbart wurden, werden die übrigen Parameter vereinbart und der IPsec-VPN-Tunnel aktiviert.

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

Hinweis: Lesen Sie vor dem Ausgabe von **Debug-**Befehlen unter Wichtige Informationen zu Debug-Befehlen nach.

- **debug crypto ipsec client ezvpn**: Zeigt Informationen an, die die Konfiguration und Implementierung der EzVPN-Clientfunktion anzeigen.
- **debug crypto ipsec**: Zeigt Debuginformationen über IPsec-Verbindungen an.
- **debug crypto isakmp**: Zeigt Debuginformationen über IPsec-Verbindungen an und zeigt den ersten Satz von Attributen an, die aufgrund von Inkompatibilitäten an beiden Enden abgelehnt werden.
- **show debug**: Zeigt den Status jeder Debugoption an.

Ausgabe aus Debugbefehlen

Sobald Sie den Befehl **crypto ipsec client ezvpn SJVPN** eingeben, versucht der EzVPN Client, eine Verbindung zum Server herzustellen. Wenn Sie den Befehl **connect Manual** unter der Gruppenkonfiguration ändern, geben Sie den Befehl **crypto ipsec client ezvpn connect SJVPN** ein,

um den Austausch von Vorschlägen an den Server zu initiieren.

```
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
```

Ähnliches Cisco IOS zeigt Befehle zur Fehlerbehebung an

```
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:
```

Löschen eines aktiven Tunnels

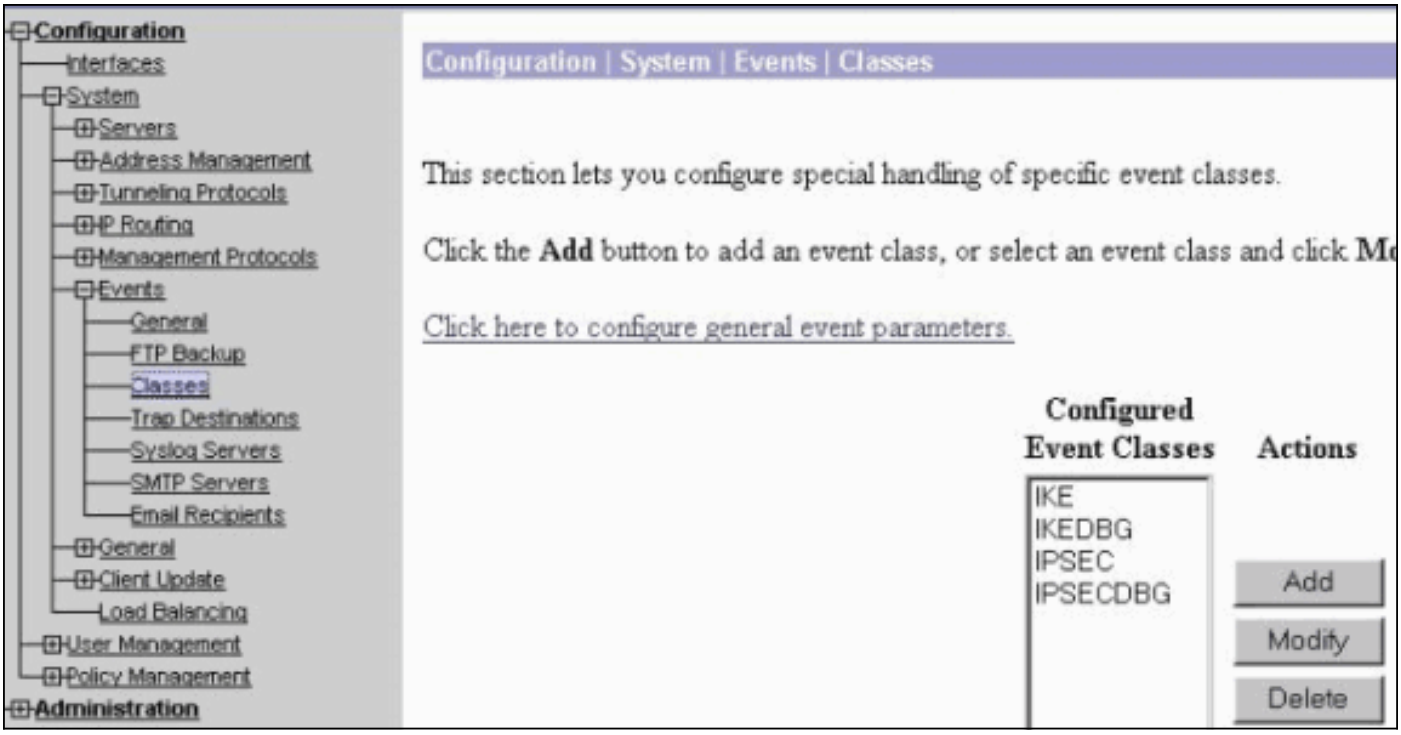
Sie können die Tunnel mit den folgenden Befehlen löschen:

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

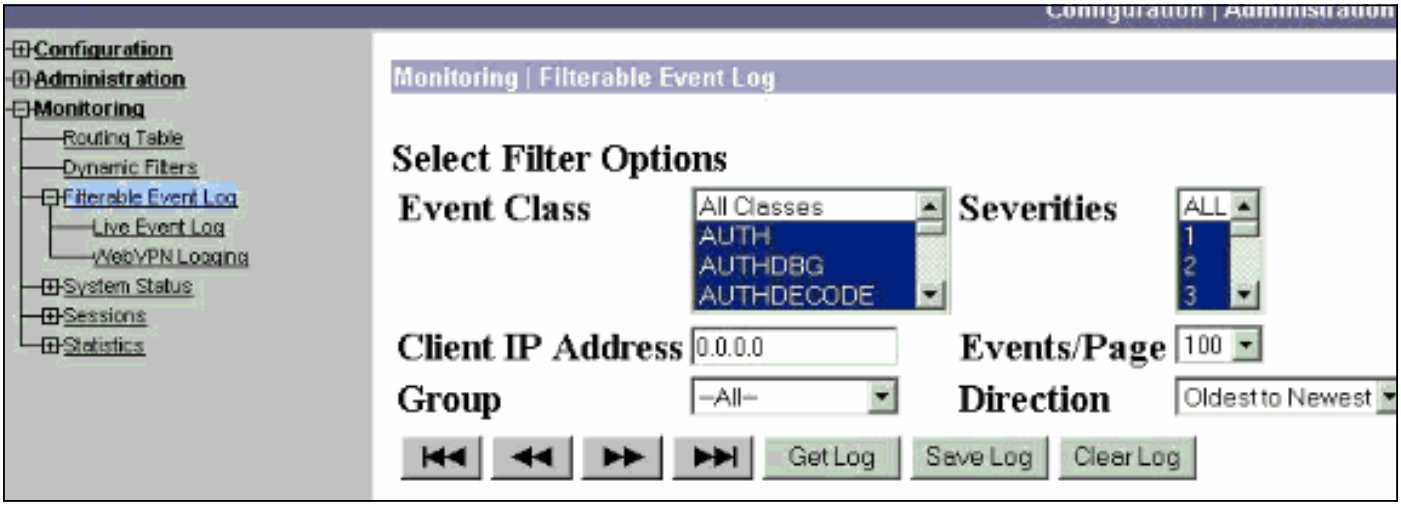
Hinweis: Sie können den VPN-Konzentrator verwenden, um sich bei der Sitzung abzumelden, wenn Sie **Administration > Admin Sessions** auswählen, den Benutzer in der **Remotezugriffssitzung** auswählen und auf **Abmelden** klicken.

VPN 3000 Concentrator-Debugging

Wählen Sie **Configuration > System > Events > Classes (Konfiguration > System > Ereignisse > Klassen)**, um dieses Debuggen zu aktivieren, wenn eine Ereignisverbindung fehlschlägt. Sie können immer weitere Klassen hinzufügen, wenn die angegebenen nicht helfen, das Problem zu identifizieren.



Um das aktuelle Ereignisprotokoll im Arbeitsspeicher anzuzeigen, das nach Ereignisklasse, Schweregrad, IP-Adresse usw. gefiltert werden kann, wählen Sie **Monitoring > Filterable Event log (Überwachung > Filterbares Ereignisprotokoll)** aus.



Um die Statistiken des IPsec-Protokolls anzuzeigen, wählen Sie **Monitoring > Statistics > IPSec.** Dieses Fenster zeigt Statistiken für IPsec-Aktivitäten, einschließlich aktueller IPsec-Tunnel, auf dem VPN Concentrator seit dem letzten Booten oder Zurücksetzen an. Diese Statistiken entsprechen dem IETF-Entwurf für die IPsec-Flow Monitoring-MIB. Im Fenster **Überwachung > Sitzungen > Detail** werden auch IPsec-Daten angezeigt.

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

Was kann schief gehen?

- Der Cisco IOS-Router ist im Bundesstaat AG_INIT_EXCH fixiert. Schalten Sie während der Fehlerbehebung die IPsec- und ISAKMP-Debugger mit den folgenden Befehlen ein:**debuggen crypto ipsecdebuggen crypto isakmpdebuggen crypto ezvpn**Auf dem Cisco IOS-Router wird Folgendes angezeigt:

```
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
```

  Im VPN 3000-Konzentrator ist Xauth erforderlich. Das ausgewählte Angebot unterstützt Xauth jedoch nicht. Überprüfen Sie, ob die interne Authentifizierung für Xauth angegeben ist. Aktivieren Sie die interne Authentifizierung, und stellen Sie sicher, dass für die IKE-Vorschläge der Authentifizierungsmodus auf **Preshared Keys (Xauth)** festgelegt ist, wie im vorherigen Screenshot. Klicken Sie auf **Ändern**, um das Angebot zu bearbeiten.
- Das Kennwort ist falsch.Die Meldung **Ungültiges Kennwort** wird auf dem Cisco IOS-Router nicht angezeigt. Auf dem VPN Concentrator wird möglicherweise das **unerwartete Ereignis "EV_ACTIVATE_NEW_SA" im Status "AM_TM_INIT_XAUTH"** angezeigt.Stellen Sie sicher, dass Ihr Kennwort korrekt ist.
- Der Benutzername ist falsch.Auf dem Cisco IOS-Router wird ein ähnliches Debugging angezeigt, wenn Sie das falsche Kennwort eingegeben haben. Auf dem VPN Concentrator wird die **Authentifizierung abgelehnt angezeigt: Grund = Benutzer wurde nicht gefunden**.

Zugehörige Informationen

- Support-Seite für Cisco VPN Concentrator der Serie 3000
- Cisco Easy VPN Remote Phase II
- Cisco VPN Client Support-Seite der Serie 3000
- Support-Seite für IPsec-Aushandlung/IKE-Protokolle
- Technischer Support und Dokumentation - Cisco Systems