# L2TP over IPsec tussen Windows 2000/XP PC en PIX/ASA 7.2 met behulp van voorgedeeld toetconfiguratie voorbeeld

## Inhoud



## Inleiding

Dit document beschrijft hoe u Layer 2 Tunneling Protocol (L2TP) kunt configureren via IP Security (IPsec) van externe Microsoft Windows 2000/2003 en XP-clients naar een PIX security applicatie voor bedrijven met behulp van vooraf gedeelde sleutels bij Microsoft Windows 2003 Internet Verificatie Service (IAS) RADIUS-server voor gebruikersverificatie. Raadpleeg Microsoft - checklist: Het configureren van IAS voor inbeltoegang en VPN-toegang voor meer informatie over IAS.

Het primaire voordeel van het configureren van L2TP met IPsec in een scenario voor externe toegang is dat externe gebruikers toegang kunnen krijgen tot een VPN via een openbaar IP-

netwerk zonder gateway of een speciale lijn. Hierdoor kan u op afstand toegang krijgen vanaf vrijwel elke plek met POTS. Een extra voordeel is dat het enige clientvereiste voor VPN-toegang het gebruik van Windows 2000 met Microsoft Dial-Up Network (DUN) is. Er is geen extra clientsoftware nodig, zoals Cisco VPN-clientsoftware.

Dit document beschrijft ook hoe u het Cisco Adaptieve Security Devices Manager (ASDM) kunt gebruiken om de PIX 500 Series security applicatie voor L2TP via IPsec te configureren.

**Opmerking:** Layer 2 Tunneling Protocol (L2TP) via IPsec wordt ondersteund op Cisco Secure PIX-firewall softwarerelease 6.x en hoger.

Om L2TP over IPsec te configureren tussen PIX 6.x en Windows 2000, raadpleegt u L2TP-over IPsec configureren tussen PIX-firewall en Windows 2000 PC met behulp van certificaten.

Om L2TP via IPsec te configureren van externe Microsoft Windows 2000- en XP-clients naar een bedrijfslocatie met een versleutelde methode, raadpleegt u L2TP-configuratie via IPsec van een Windows 2000- of XP-client naar een Cisco VPN 3000 Series Concentrator met pre-Shared Keys.

# Voorwaarden

## Vereisten

Voordat er een beveiligde tunnelverbinding tot stand komt, moet er IP-verbinding tussen de peers bestaan.

Zorg ervoor dat UDP-poort 1701 niet ergens langs het pad van de verbinding wordt geblokkeerd.

Gebruik alleen het standaard tunnelgroepsbeleid en de standaard groepsbeleid op Cisco PIX/ASA. Door gebruikers gedefinieerd beleid en groepen werken niet.

**Opmerking:** het security apparaat maakt geen L2TP/IPsec-tunnel met Windows 2000 als Cisco VPN-client 3.x of Cisco VPN 3000 Client 2.5 is geïnstalleerd. Schakel de Cisco VPN-service voor Cisco VPN-client 3.x of de ANetIKE-service voor Cisco VPN 3000 client 2.5 uit het servicespaneel in Windows 2000. Om dit te doen kiest u **Start > Programma's > Administratieve Gereedschappen > Services**, start u de IPsec Policy Agent Service opnieuw uit het Servicespaneel en start de machine opnieuw op.

## Gebruikte componenten

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

- PIX security applicatie 5150E met softwareversie 7.2(1) of hoger
- Adaptieve Security Adapter Manager 5.2(1) of hoger
- Microsoft Windows 2000-server
- Microsoft Windows XP Professional met SP2
- Windows 2003-server met IAS

**Opmerking:** Als u de PIX 6.3-bewerking naar versie 7.x verbetert, zorg er dan voor dat u SP2 in Windows XP (L2TP-client) hebt geïnstalleerd.

**Opmerking:** de informatie in het document is ook geldig voor ASA-beveiligingsapparaat.

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.

### Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco ASA 5500 Series security applicatie 7.2(1) of hoger.

### Conventies

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

## Achtergrondinformatie

Voltooi deze stappen om L2TP via IPsec te configureren.

1. Configuratie van IPsec transportmodus om IPsec met L2TP uit te schakelen.Windows 2000 L2TP/IPsec-client gebruikt IPsec-transportmodus — Alleen de IP-lading is versleuteld en de oorspronkelijke IP-headers blijven intact. De voordelen van deze modus zijn dat er slechts een paar bytes aan elk pakket worden toegevoegd en dat apparaten op het openbare netwerk de eindbron en de bestemming van het pakket kunnen zien. Om Windows 2000 L2TP/IPsec-clients aan te sluiten op het security apparaat, moet u daarom IPsec-transportmodus configureren voor een transformatie (zie stap 2 in de ASDM-configuratie). Met deze mogelijkheid (transport) kunt u speciale verwerking (bijvoorbeeld QoS) op het intermediaire netwerk inschakelen op basis van de informatie in de IP-header. Layer 4 header is echter versleuteld waardoor het pakketonderzoek wordt beperkt. Helaas, de overdracht van de IP-header in duidelijke tekst, laat de transportmodus een aanvaller toe om wat verkeersanalyse uit te voeren.
2. Configuratie L2TP met een virtuele privé inbelnetwerk (VPDN) groep.

De configuratie van L2TP met IPsec ondersteunt certificaten die de vooraf gedeelde toetsen of RSA-handtekeningen gebruiken, en het gebruik van dynamische (in tegenstelling tot statische) crypto kaarten. Vooraf gedeelde sleutel wordt gebruikt als een authenticatie om de L2TP via IPsec-tunnel te creëren.

## Configureren

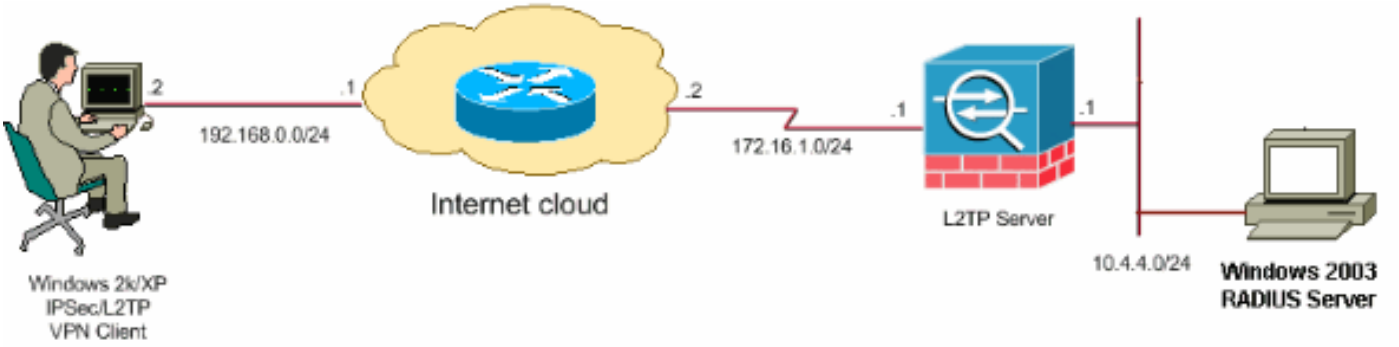
Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

**N.B.:** Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

**Opmerking:** de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Het zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

## Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:




## Configuraties

Dit document gebruikt deze configuraties:

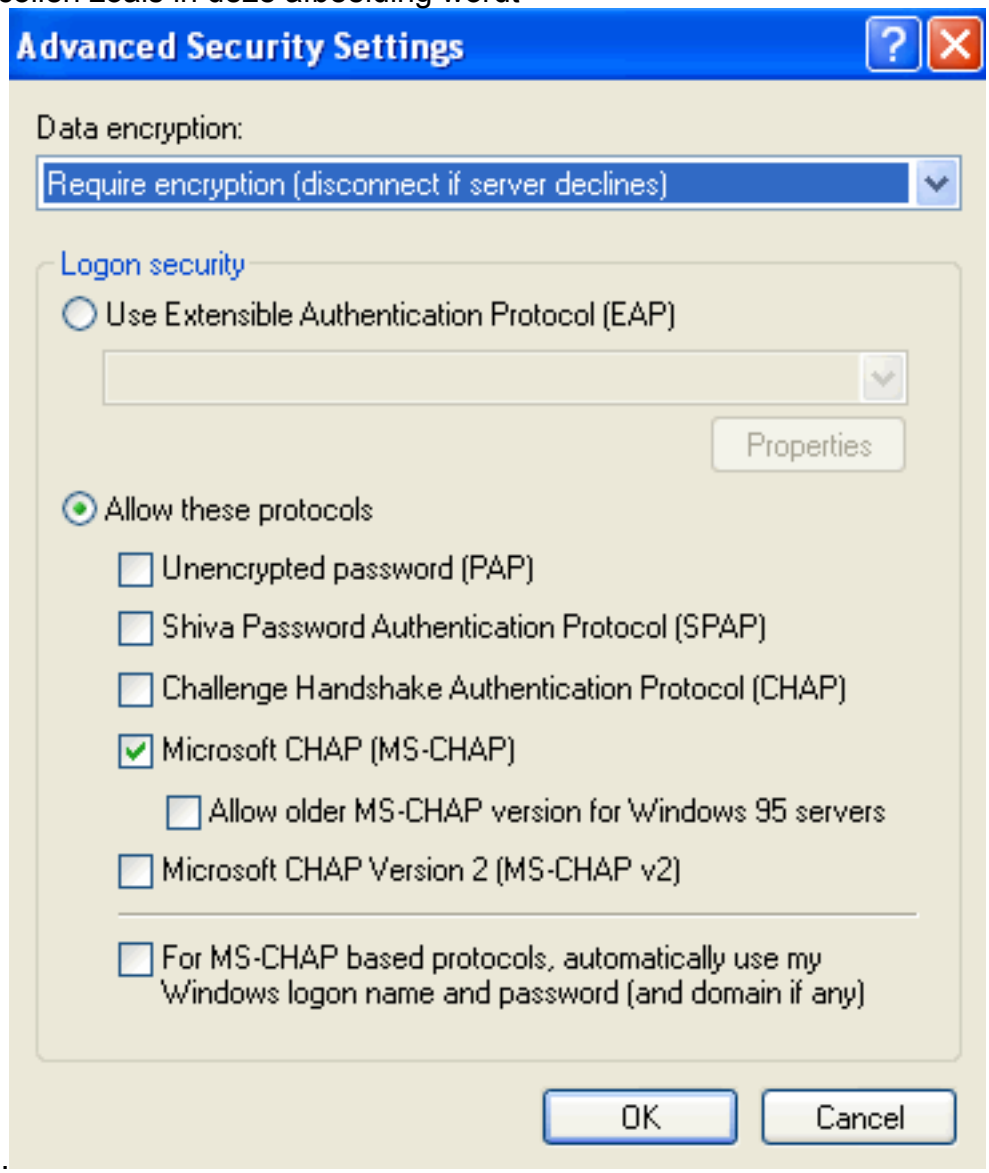
- Configuratie van Windows L2TP/IPsec-client
- L2TP-server in PIX-configuratie
- L2TP-gebruik van ASDM-configuratie
- Microsoft Windows 2003-server met IAS-configuratie

## Configuratie van Windows L2TP/IPsec-client

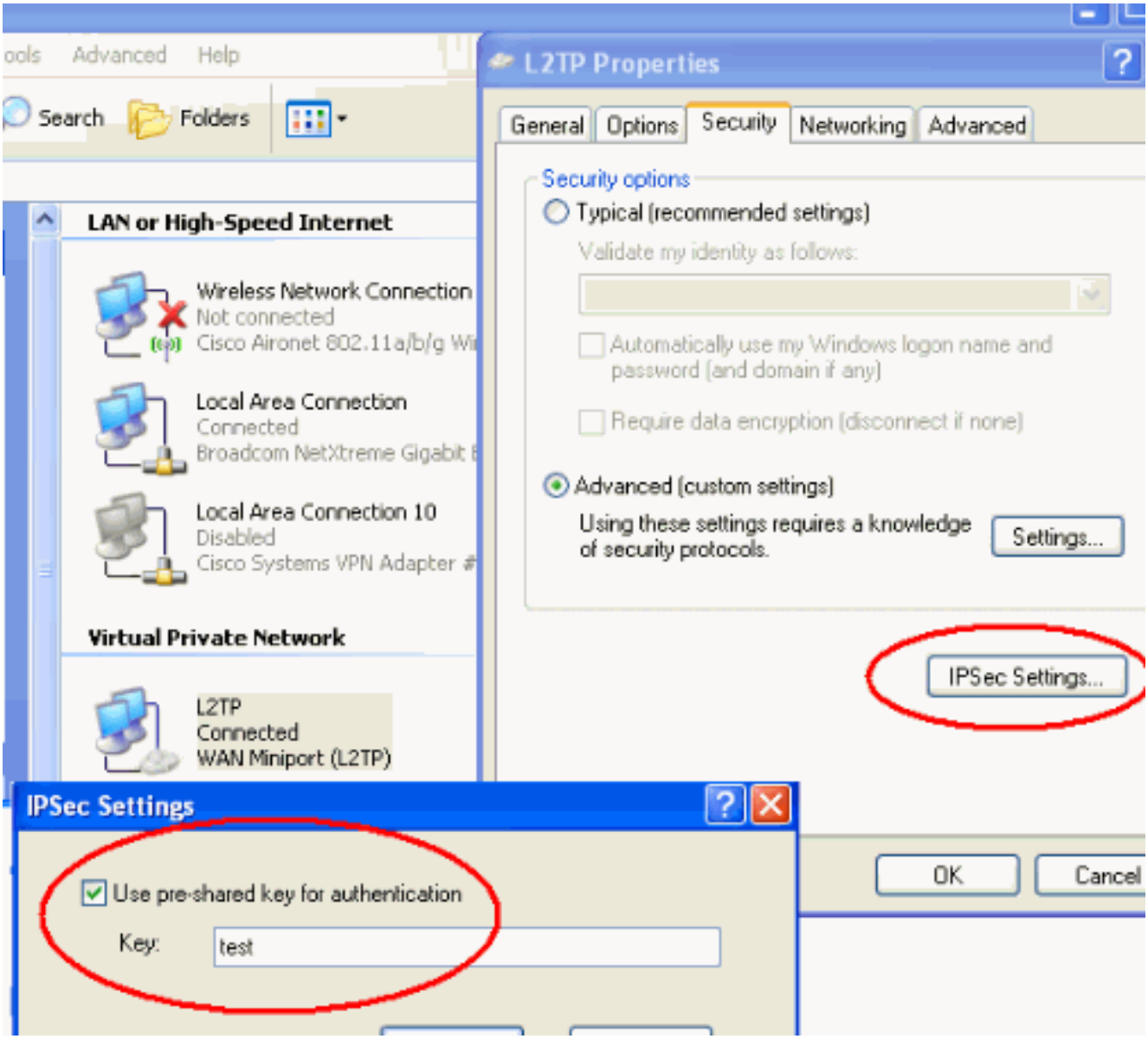
Voltooi deze stappen om L2TP via IPsec te configureren op Windows 2000. Voor Windows XP skip stappen 1 en 2 en start vanaf stap 3:

1. Voeg deze registratiewaarde toe aan uw Windows 2000-machine:
   `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters`
2. Voeg deze registratiewaarde toe aan deze toets:
   ```
   Value Name: ProhibitIpSec
   Data Type: REG_DWORD
   Value: 1
   ```
   **Opmerking:** In sommige gevallen (Windows XP SP2) is de toevoeging van deze toets **(waarde: 1)** lijkt de verbinding te verbreken aangezien het XP-vak alleen L2TP in plaats van een L2TP met IPsec-verbinding onderhandelt. Het is verplicht om een IPsec-beleid toe te voegen in combinatie met die registratiesleutel. Als u een `fout 800` ontvangt wanneer u probeert een verbinding tot stand te brengen, verwijdert u de toets (Waarde: 1 ) om de aansluiting te laten werken .**Opmerking:** U moet Windows 2000/2003 of XP-machine opnieuw opstarten voordat de wijzigingen van kracht worden. Standaard probeert de Windows-client IPsec te gebruiken met een certificeringsinstantie (CA). De configuratie van deze registratiesleutel voorkomt dat dit gebeurt. U kunt nu een IPsec-beleid op het Windows-station configureren om de parameters die u op de PIX/ASA wilt op elkaar af te stemmen. Raadpleeg hoe u een L2TP/IPSec-verbinding kunt configureren met behulp van pre-gedeeld toetsing-verificatie (Q240262) voor een stapsgewijze configuratie van het Windows IPsec-beleid.Raadpleeg een vooraf gedeelde sleutel voor gebruik met Layer 2 Tunneling Protocol-verbindingen in Windows XP (Q28155)\ voor meer informatie.

3. Maak je verbinding.
4. Klik onder Connecties met netwerk- en inbelverbindingen met de rechtermuisknop op de aansluiting en kies **Eigenschappen**.Ga naar het tabblad Beveiliging en klik op **Geavanceerd**. Kies de protocollen zoals in deze afbeelding wordt weergegeven.




5. **Opmerking:** Deze stap is alleen van toepassing voor Windows XP.Klik op **IPSec Settings**, controleer **de vooraf gedeelde sleutel van het gebruik voor authenticatie** en type in de vooraf gedeelde sleutel om de voorgedeelde sleutel in te stellen.In dit voorbeeld wordt de test gebruikt als de vooraf gedeelde
toets.




## L2TP-server in PIX-configuratie

| PIX 7.2 |
| --- |

```
pixfirewall#show run

PIX Version 7.2(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
!--- Configures the outside and inside interfaces.
interface Ethernet0 nameif outside security-level 0 ip
address 172.16.1.1 255.255.255.0 ! interface Ethernet1
nameif inside security-level 100 ip address 10.4.4.1
255.255.255.0 ! passwd 2KFQnbNIdI.2KYOU encrypted ftp
mode passive dns server-group DefaultDNS domain-name
default.domain.invalid access-list nonat extended permit
ip 10.4.4.0 255.255.255.0 10.4.5.0 255.255.255.0
nat (inside) 0 access-list nonat

pager lines 24
```

```
logging console debugging
mtu outside 1500
mtu inside 1500

!--- Creates a pool of addresses from which IP addresses
are assigned !--- dynamically to the remote VPN Clients.
ip local pool clientVPNpool 10.4.5.10-10.4.5.20 mask
255.255.255.0

no failover
asdm image flash:/asdm-521.bin
no asdm history enable
arp timeout 14400

!--- The global and nat command enable !--- the Port
Address Translation (PAT) using an outside interface IP
!--- address for all outgoing traffic.

global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0


route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute

!--- Create the AAA server group "vpn" and specify its
protocol as RADIUS. !--- Specify the IAS server as a
member of the "vpn" group and provide its !--- location
and key. aaa-server vpn protocol radius
aaa-server vpn host 10.4.4.2
 key radiuskey

!--- Identifies the group policy as internal. group-
policy DefaultRAGroup internal
!--- Instructs the security appliance to send DNS and !-
-- WINS server IP addresses to the client. group-policy
DefaultRAGroup attributes
 wins-server value 10.4.4.99
 dns-server value 10.4.4.99
!--- Configures L2TP over IPsec as a valid VPN tunneling
protocol for a group. vpn-tunnel-protocol IPSec l2tp-
ipsec
 default-domain value cisco.com
!--- Configure usernames and passwords on the device !--
- in addition to using AAA. !--- If the user is an L2TP
client that uses Microsoft CHAP version 1 or !---
version 2, and the security appliance is configured !---
to authenticate against the local !--- database, you
must include the mschap keyword. !--- For example,
username



          .


username test password DLaUiAX3178qgoB5c7iVNw== nt-
```

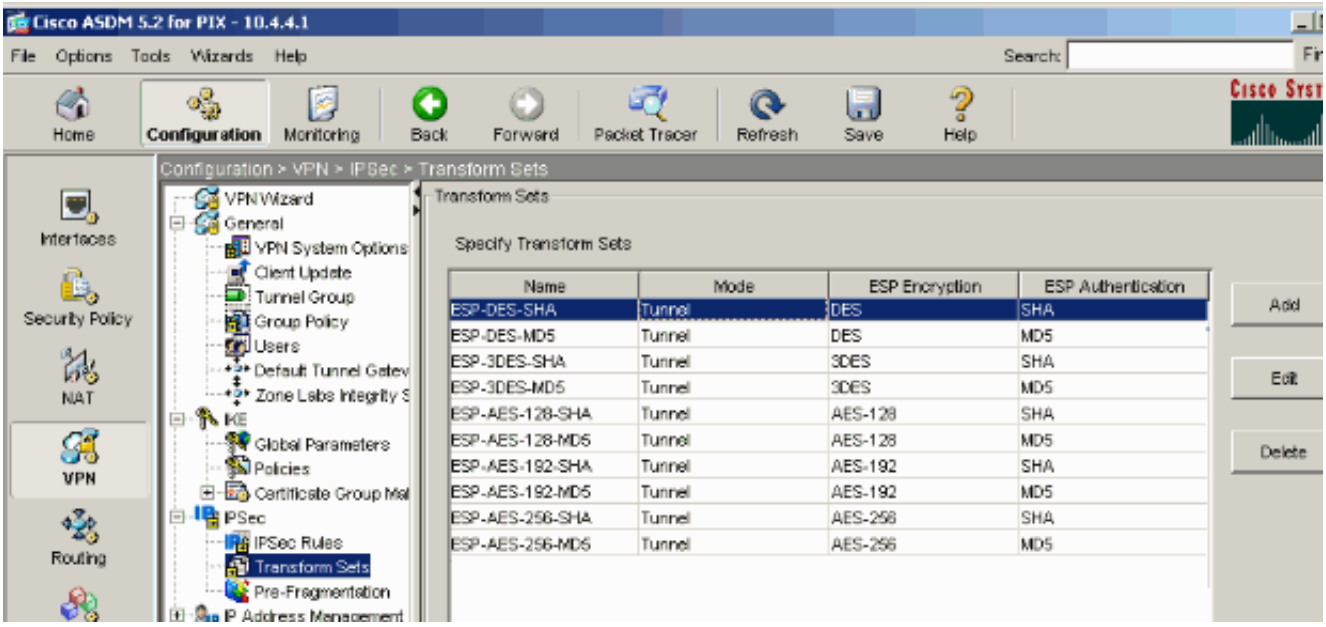
```
encrypted


 vpn-tunnel-protocol l2tp-ipsec

http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart

!--- Identifies the IPsec encryption and hash algorithms
!--- to be used by the transform set. crypto ipsec
transform-set TRANS_ESP_3DES_MD5 esp-3des esp-md5-hmac

!--- Since the Windows 2000 L2TP/IPsec client uses IPsec
transport mode, !--- set the mode to transport. !--- The
default is tunnel mode. crypto ipsec transform-set
TRANS_ESP_3DES_MD5 mode transport




!--- Specifies the transform sets to use in a dynamic
crypto map entry. crypto dynamic-map outside_dyn_map 20
set transform-set TRANS_ESP_3DES_MD5

!--- Requires a given crypto map entry to refer to a
pre-existing !--- dynamic crypto map. crypto map
outside_map 20 ipsec-isakmp dynamic outside_dyn_map

!--- Applies a previously defined crypto map set to an
outside interface. crypto map outside_map interface
outside

crypto isakmp enable outside
crypto isakmp nat-traversal 20

!--- Specifies the IKE Phase I policy parameters. crypto
isakmp policy 10
 authentication pre-share
 encryption 3des
 hash md5
 group 2
 lifetime 86400

!--- Creates a tunnel group with the tunnel-group
command, and specifies the local !--- address pool name
used to allocate the IP address to the client. !---
Associate the AAA server group (VPN) with the tunnel
group.


tunnel-group DefaultRAGroup general-attributes
 address-pool clientVPNpool
 authentication-server-group vpn

!--- Link the name of the group policy to the default
tunnel !--- group from tunnel group general-attributes
mode. default-group-policy DefaultRAGroup

!--- Use the tunnel-group ipsec-attributes command !---
in order to enter the ipsec-attribute configuration
```

```
mode. !--- Set the pre-shared key. !--- This key should
be the same as the key configured on the Windows
machine.


tunnel-group DefaultRAGroup ipsec-attributes
 pre-shared-key *

!--- Configures the PPP authentication protocol with the
authentication type !--- command from tunnel group ppp-
attributes mode.


tunnel-group DefaultRAGroup ppp-attributes
 no authentication chap
 authentication ms-chap-v2

telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:e1e0730fa260244caa2e2784f632accd
: end
```

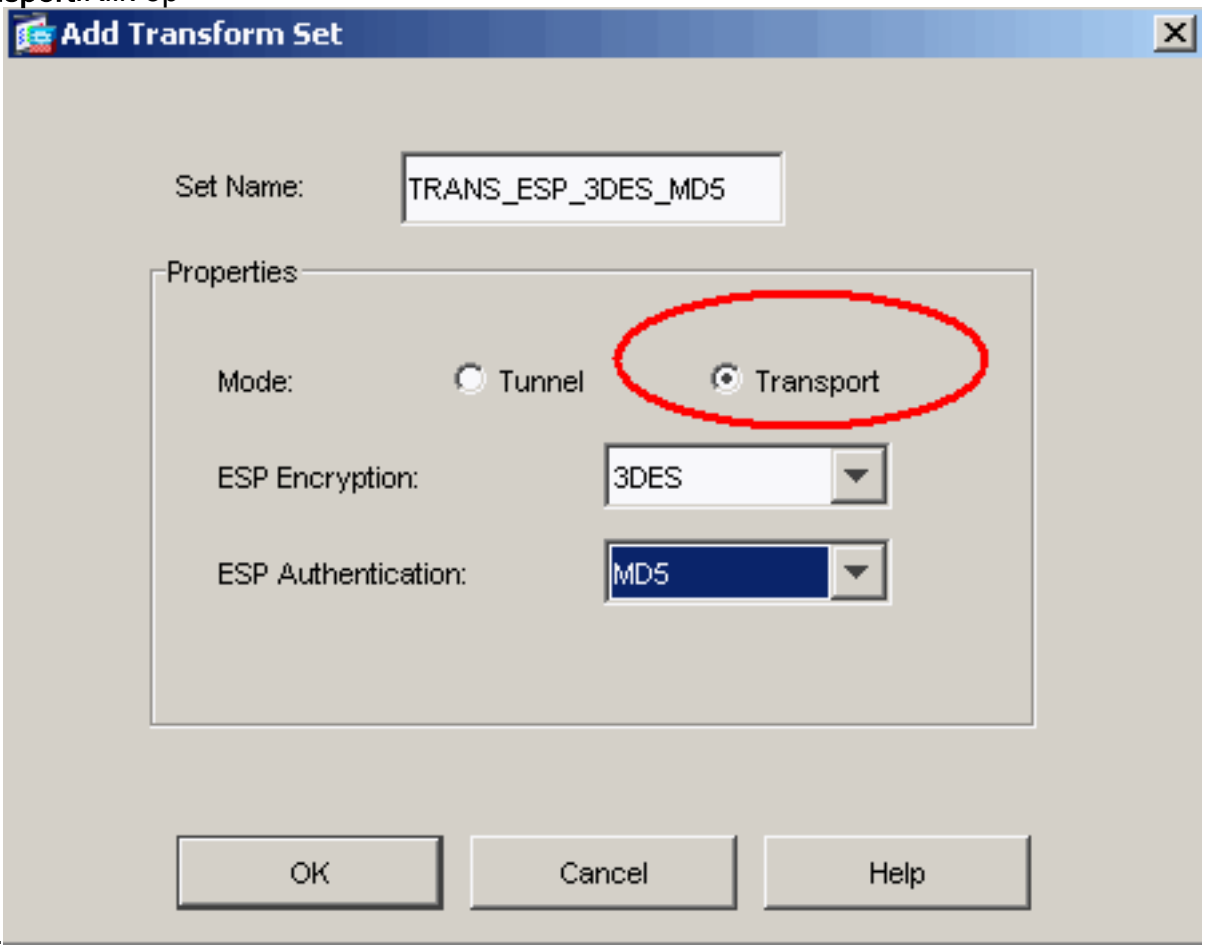
## L2TP-gebruik van ASDM-configuratie

Voltooi deze stappen om het security apparaat te configureren en L2TP via IPsec-verbindingen te aanvaarden:

1. Voeg een reeks IPsec-transformatie toe en specificeer IPsec om transportmodus te gebruiken in plaats van tunnelmodus. Kies hiervoor **Configuration > VPN > IPSec > Transformer-switches** en klik op **Add**. Het venster Omzetten stelt u in.

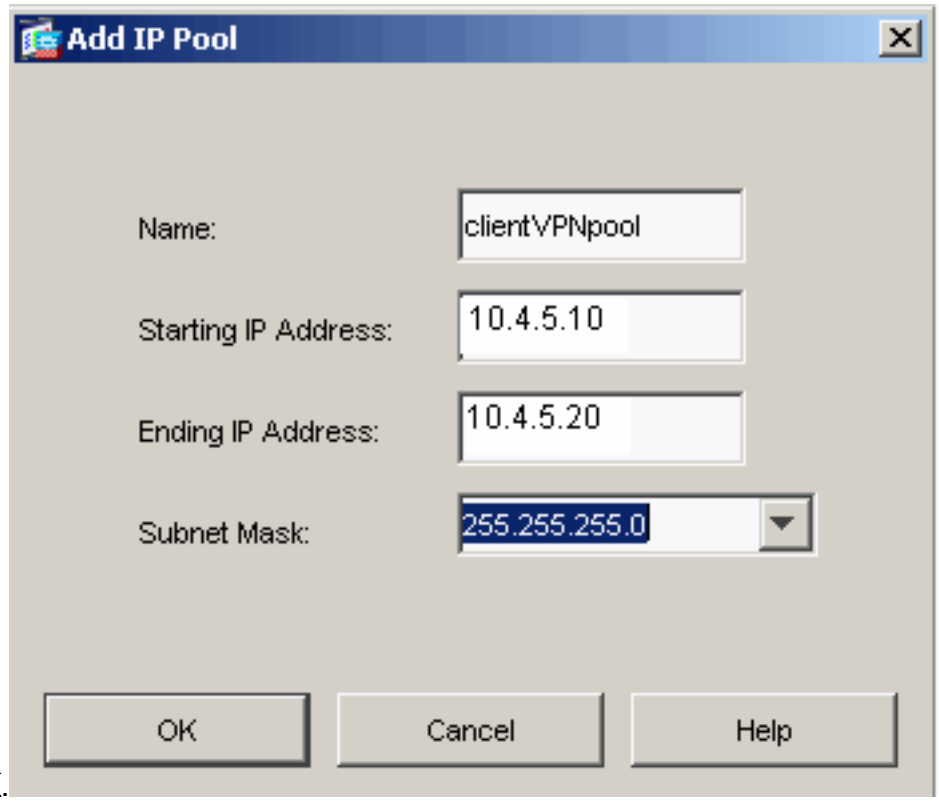



2. Volg deze stappen om een transformatieset toe te voegen:Voer een naam in voor de transformatieset.Kies de ESP-encryptie en de ESP-verificatiemethoden.Kies de modus als **transport**.Klik op



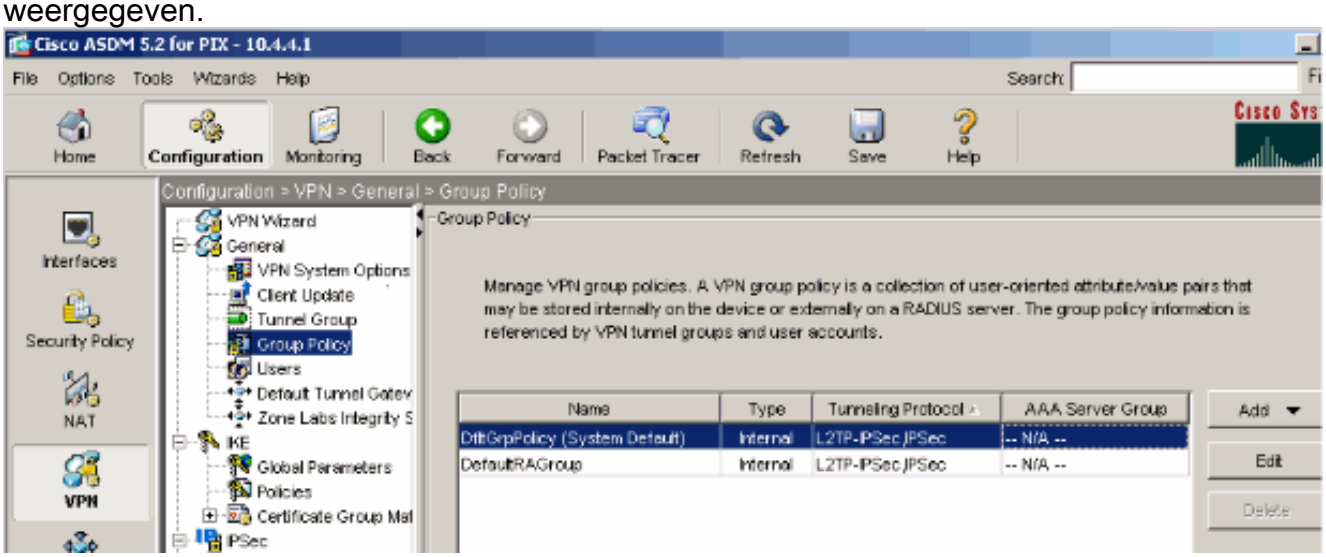

**OK**.

3. Voltooi deze stappen om een methode van adrestoewijzing te configureren. Dit voorbeeld gebruikt IP adrespools.Kies **Configuration > VPN > IP-adresbeheer > IP-pools**.Klik op **Add** (Toevoegen). Het dialoogvenster Wol toevoegen verschijnt.Voer de naam van de nieuwe IP-adrespool in.Voer de begin- en eindadressen in.Voer het subnetmasker in en klik op

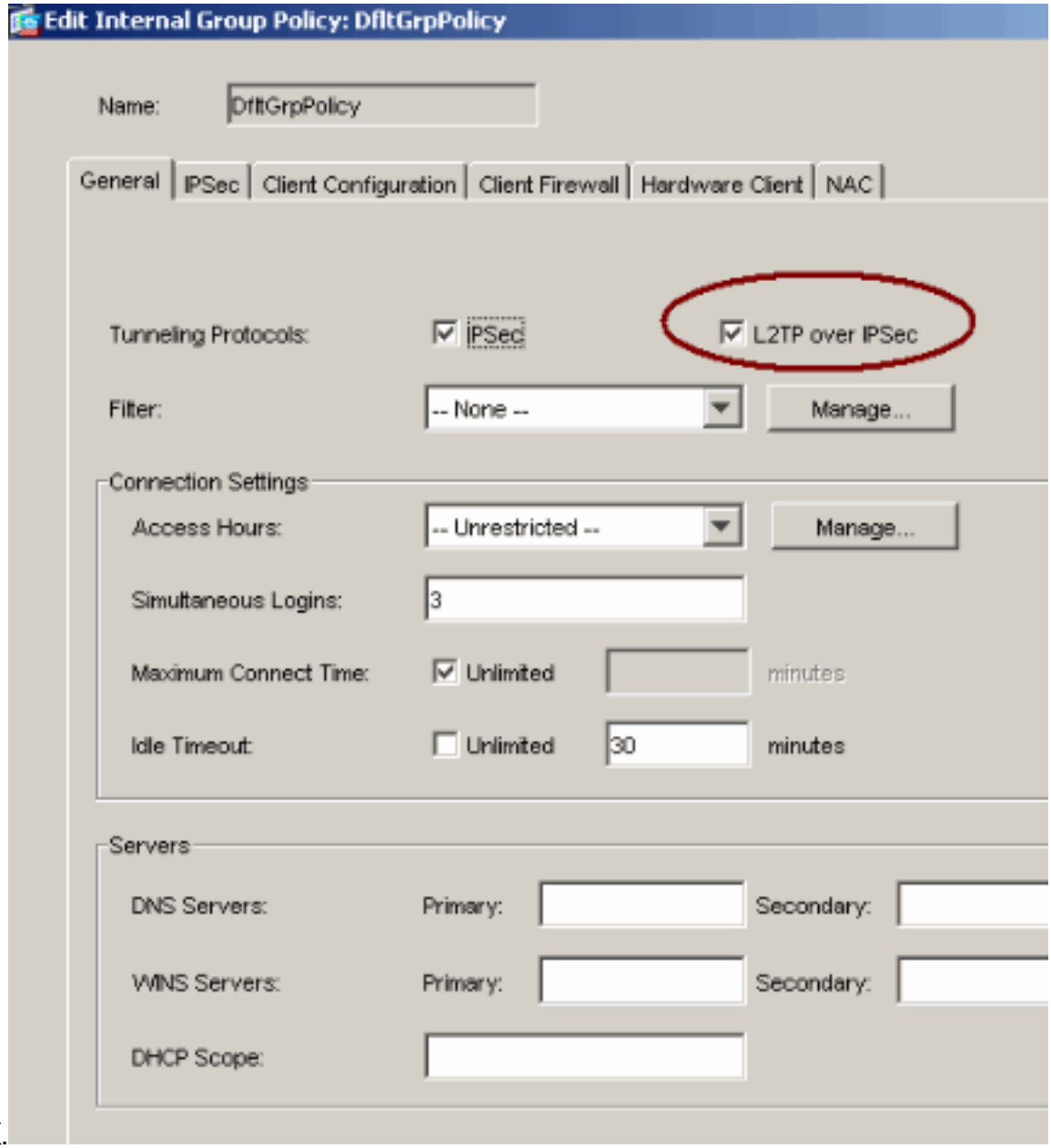



**OK**.

4. Kies **Configuration > VPN > General > Group Policy** om L2TP via IPsec te configureren als een geldig VPN-tunneling-protocol voor het groepsbeleid. Het deelvenster groepsbeleid wordt
weergegeven.

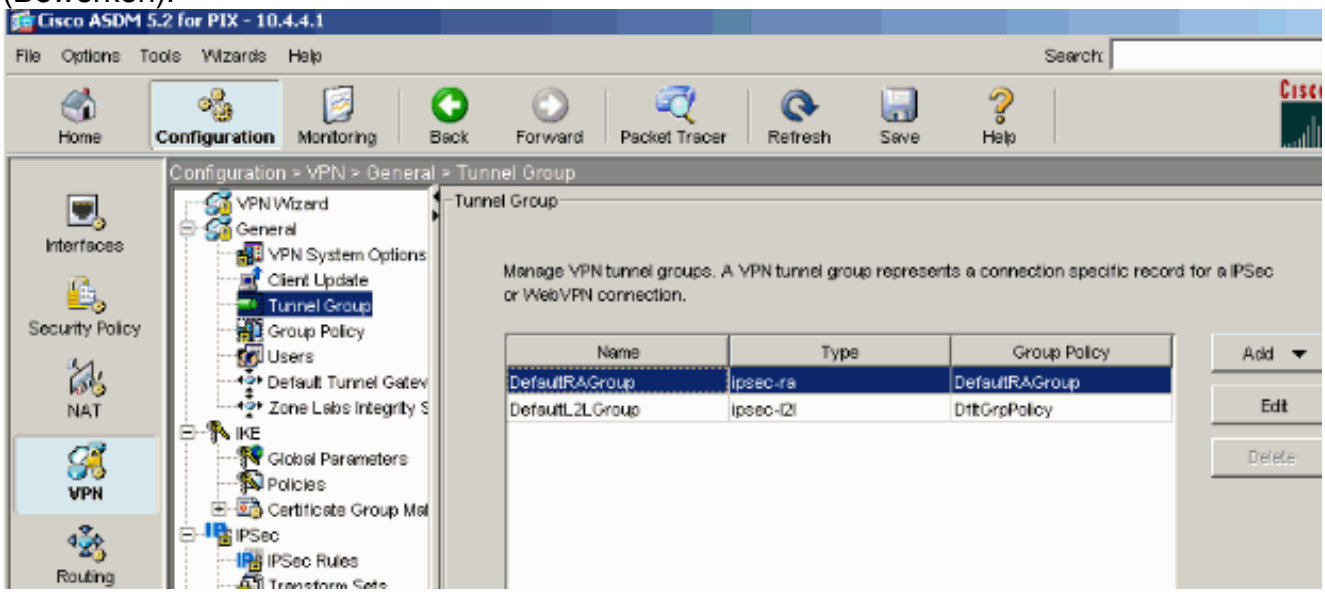



5. Selecteer een groepsbeleid (DiffGrpPolicy) en klik op **Bewerken**.Het dialoogvenster Gebiedsbeleid bewerken wordt weergegeven. Controleer **L2TP via IPSec** om het protocol voor het groepsbeleid in te schakelen en klik vervolgens op



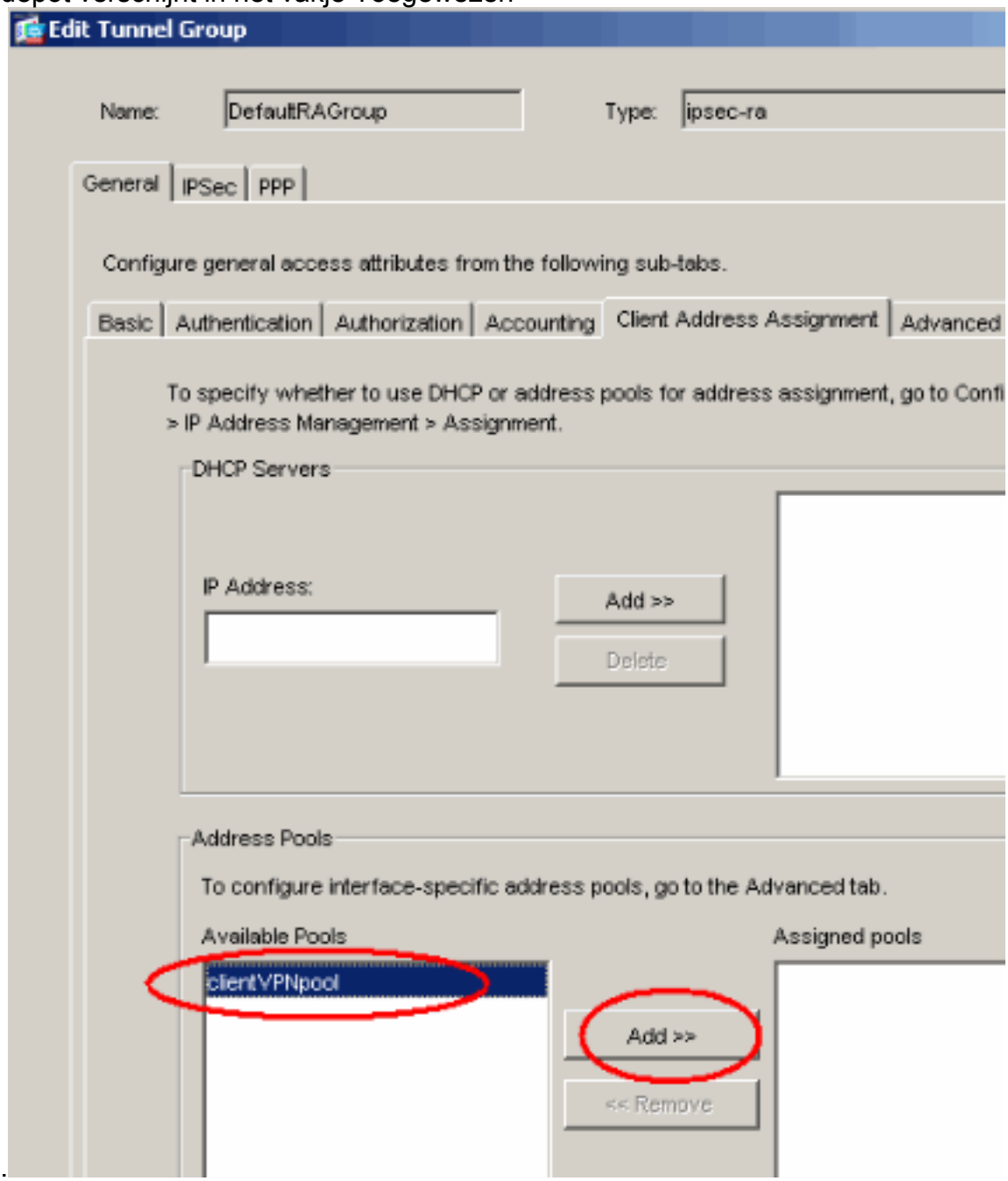

**OK**.

6. Voltooi deze stappen om de IP-adrespool aan een tunnelgroep toe te wijzen:Kies **Configuration > VPN > General > Tunnel Group**.Nadat het deelvenster Tunnel-groep wordt weergegeven, selecteert u een tunnelgroep (DefaultRAGGroup) in de tabel.Klik op **Edit** (Bewerken).

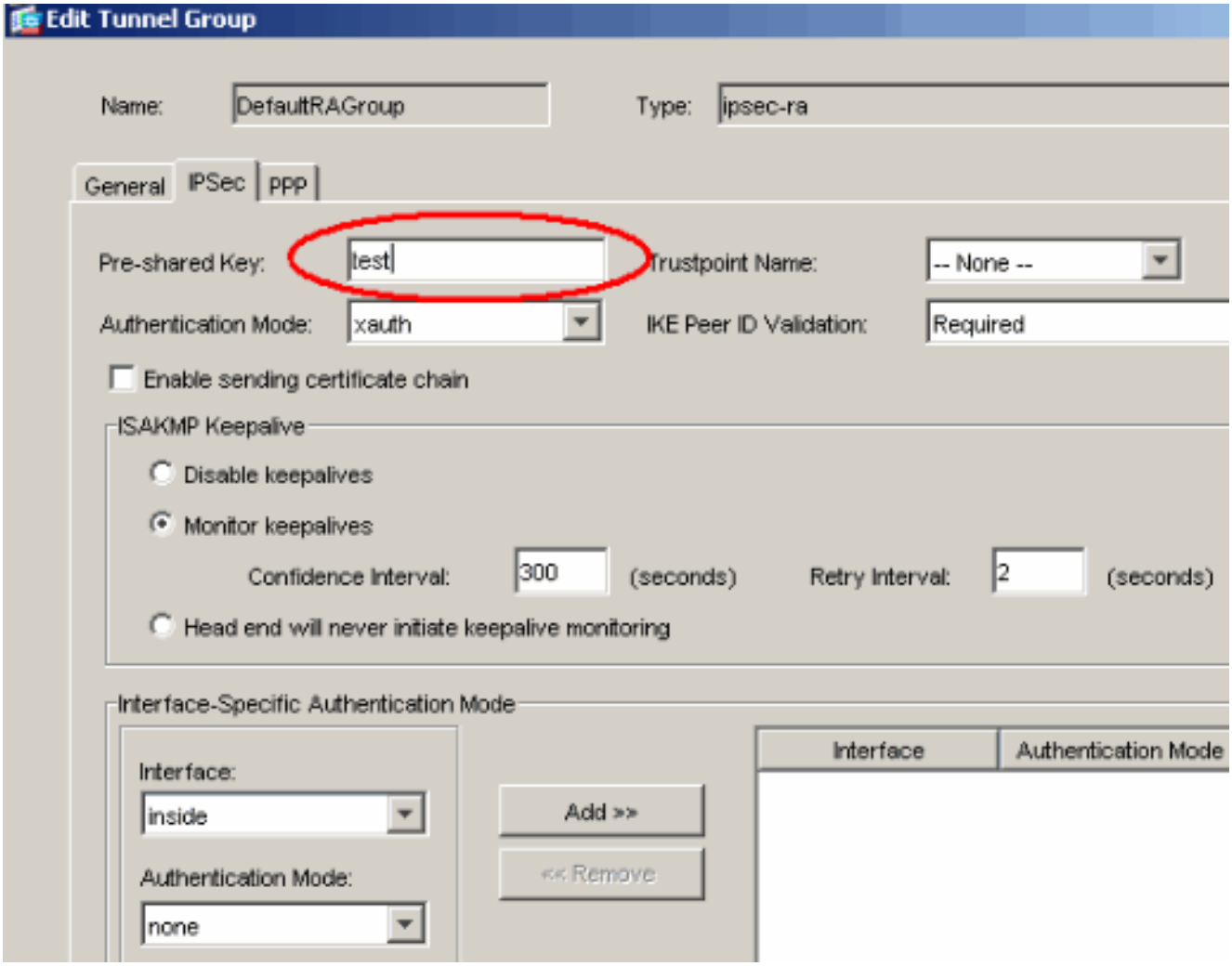



7. Voltooi deze stappen wanneer het venster Tunnel groep bewerken wordt weergegeven:Ga

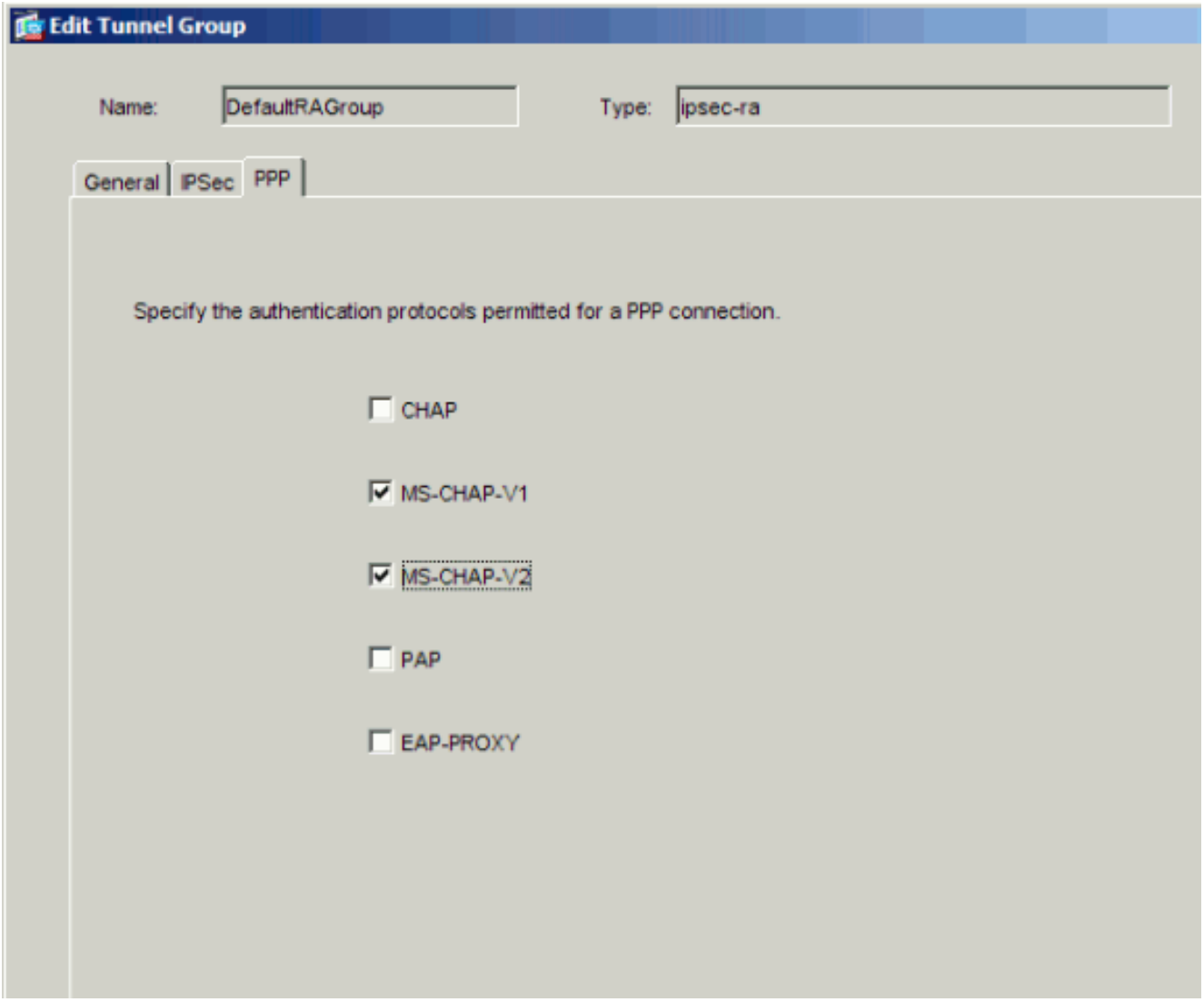
vanuit het tabblad Algemeen naar het tabblad Toewijzing van clientadres.In het gebied Adres Pools, kies een adrepool om aan de tunnelgroep toe te wijzen.Klik op **Add** (Toevoegen). Het adresdepot verschijnt in het vakje Toegewezen Pools.



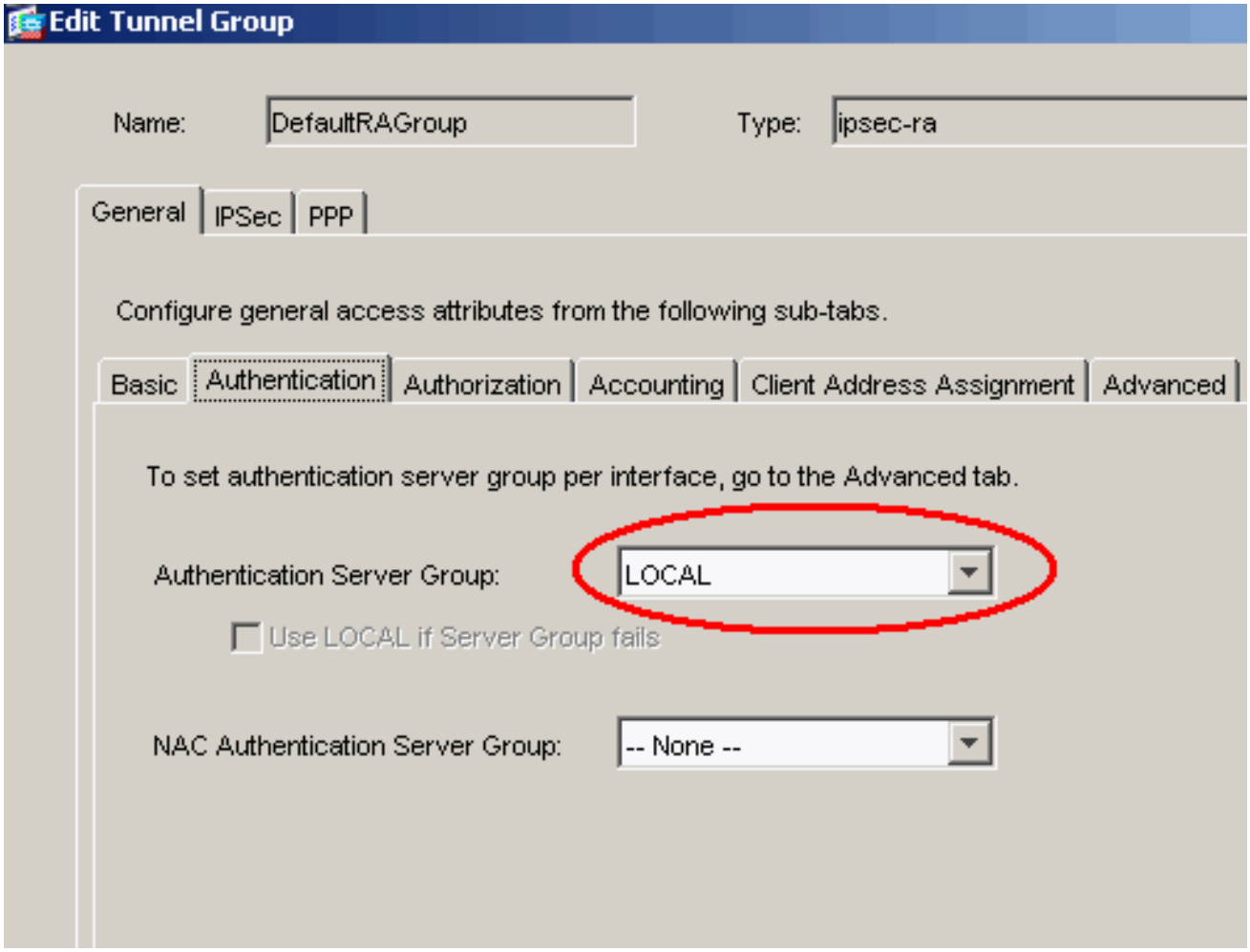

8. Ga naar het tabblad IPSec om de voorgedeelde toets in te stellen, voer uw **voorgedeelde sleutel in** en klik op **OK**.




9. L2TP via IPsec gebruikt PPP-verificatieprotocollen. Specificeer de protocollen die voor PPP-verbindingen zijn toegestaan op het tabblad PPP van de tunnelgroep. Selecteer het **MS-CHAP-V1** protocol voor
authenticatie.



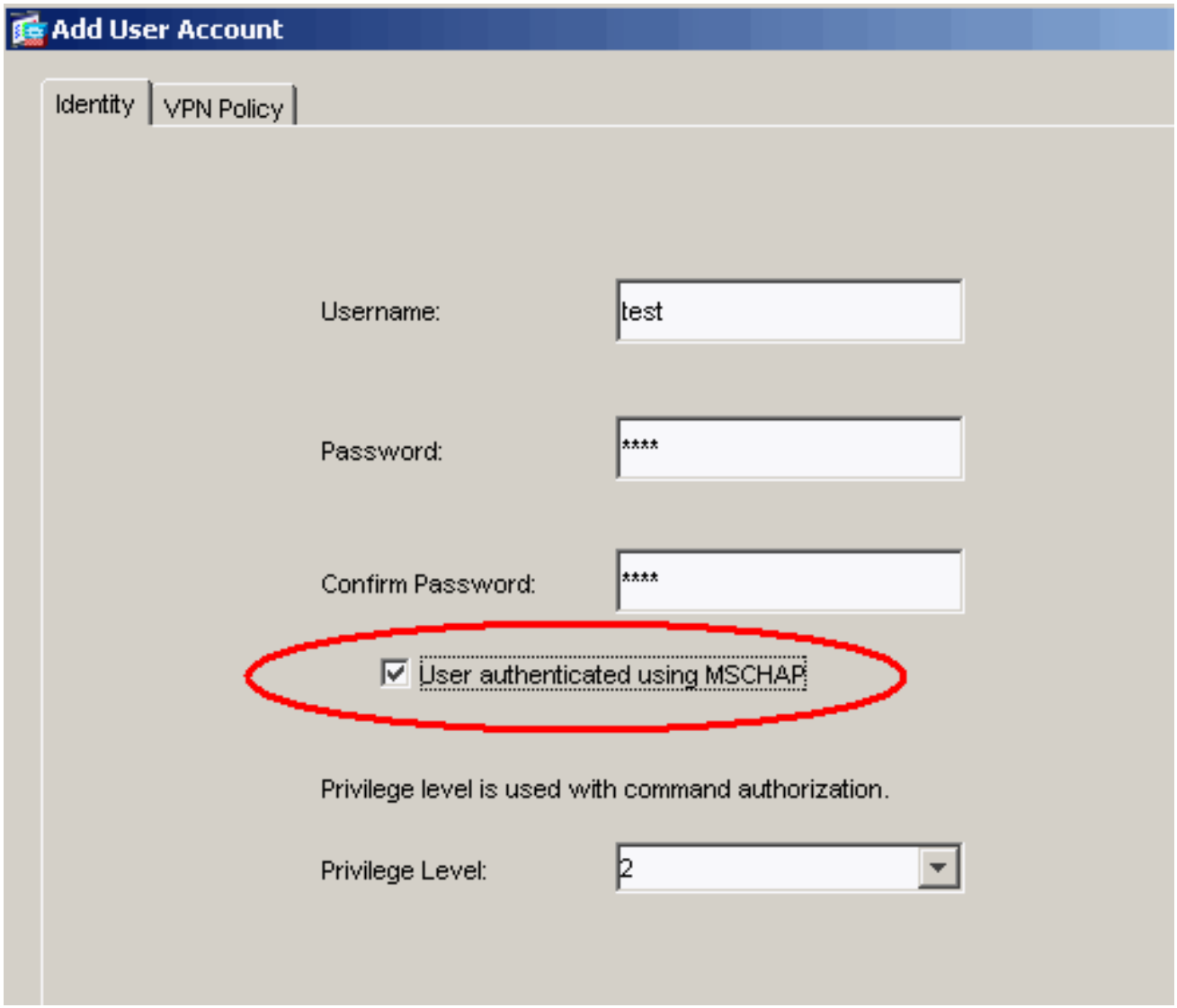

10. Specificeer een methode om gebruikers die L2TP via IPsec-verbindingen proberen te authenticeren.U kunt het beveiligingsapparaat configureren om een verificatieserver of een eigen lokale database te gebruiken. Ga om dit te doen naar het tabblad Verificatie van de tunnelgroep. Standaard gebruikt het beveiligingsapparaat de lokale database. De vervolgkeuzelijst Verificatieservergroep toont de LOKALE taal. Selecteer een van de lijst om een verificatieserver te gebruiken.**Opmerking:** het security apparaat ondersteunt alleen de PPP-authenticaties (PAP) en Microsoft CHAP-versies 1 en 2 in de lokale database. EAP en CHAP worden uitgevoerd door proxyverificatieservers. Als een externe gebruiker daarom behoort tot een tunnelgroep die is ingesteld met EAP of CHAP en het beveiligingsapparaat is ingesteld om de lokale database te gebruiken, kan die gebruiker geen verbinding maken.



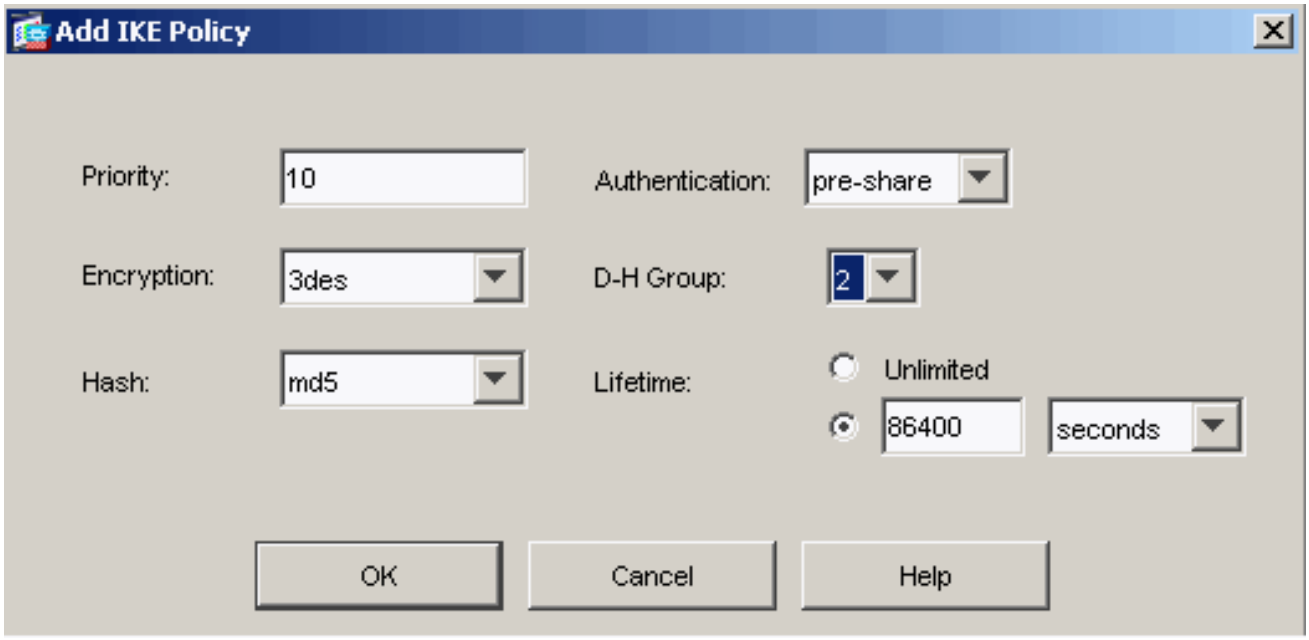

**Opmerking:** Kies **Configuration > VPN > General > Tunnel Group** om terug te gaan naar de configuratie van de tunnelgroep, zodat u het groepsbeleid kunt koppelen aan de tunnelgroep en Tunnel Group Switching (optioneel) mogelijk maakt. Wanneer het deelvenster Tunnel groep wordt weergegeven, kiest u de tunnelgroep en klikt u op **Bewerken**.**Opmerking:** Tunnel Group Switching stelt het security apparaat in staat om verschillende gebruikers die L2TP via IPsec-verbindingen instellen, te koppelen aan verschillende tunnelgroepen. Aangezien elke tunnelgroep zijn eigen AAA server group en IP adrespools heeft, kunnen de gebruikers door methodes worden authentiek verklaard die specifiek zijn voor hun tunnelgroep. Met deze functie verstuurt de gebruiker niet alleen een gebruikersnaam, maar stuurt hij een gebruikersnaam en een groepsnaam in de notatie username@group_name, waarbij "@" een scheidingsteken vertegenwoordigt die u kunt configureren en de groepsnaam de naam is van een tunnelgroep die op het beveiligingsapparaat is ingesteld.**Opmerking:** Tunnel Group Switching is ingeschakeld door Strip Group Processing, zodat het security apparaat de tunnelgroep voor gebruikersverbindingen kan selecteren door de groepsnaam te verkrijgen van de gebruikersnaam die door de VPN-client wordt aangeboden. Het veiligheidsapparaat stuurt dan alleen het gebruikersgedeelte van de gebruikersnaam naar toestemming en verificatie. Anders (indien uitgeschakeld) stuurt het beveiligingsapparaat de volledige gebruikersnaam, inclusief het domein. Om het switching van de Tunnel Group in te schakelen, controleert u **de naam van de gebruiker voordat u deze doorgeeft aan de AAA-server** en controleert u **de naam van de groep voordat u deze doorgeeft aan de AAA-server**. Klik vervolgens op **OK**.

11. Voltooi deze stappen om een gebruiker in de lokale database te maken:Kies **Configuratie >Eigenschappen > Apparaatbeheer > Gebruikersrekeningen**.Klik op **Add** (Toevoegen).Als de gebruiker een L2TP-client is die gebruik maakt van Microsoft CHAP, versie 1 of 2, en het

security apparaat is ingesteld om authenticatie aan te vragen tegen de lokale database, moet u **Gebruiker** Verificeerd **met MSCHAP controleren** om de MSCHAP in te schakelen.Klik op
**OK**.




12. Kies **Configuration > VPN > IKE > Policy** en klik op **Add** om een IKE-beleid voor fase I te maken. Klik op **OK** om door te
gaan.



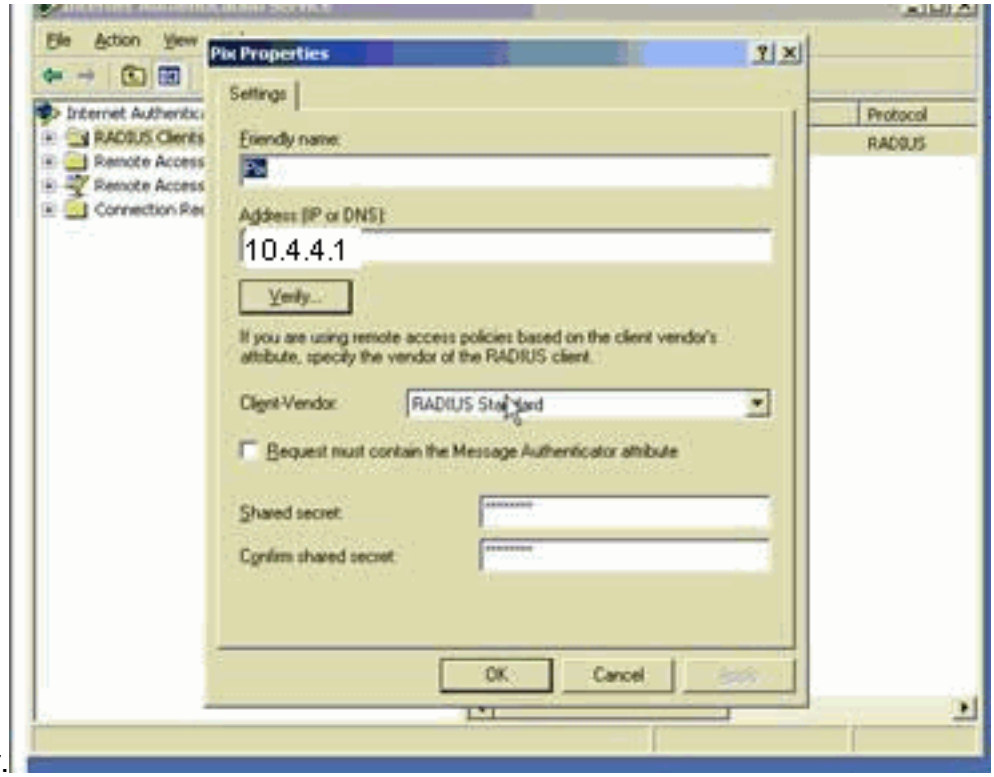

13. (Optioneel) Als u verwacht dat meerdere L2TP-clients achter een NAT-apparaat L2TP-via-IPsec-verbindingen naar het security apparaat zullen proberen, moet u NAT-verplaatsingen inschakelen zodat ESP-pakketten door een of meer NAT-apparaten kunnen worden verzonden. Volg deze stappen om dit te doen:Kies **Configuratie > VPN > IKE > Mondiale parameters**.Zorg ervoor dat **ISAKMP** op een interface is ingeschakeld.Controleer **IPSec inschakelen via NAT-T**.Klik op **OK**.

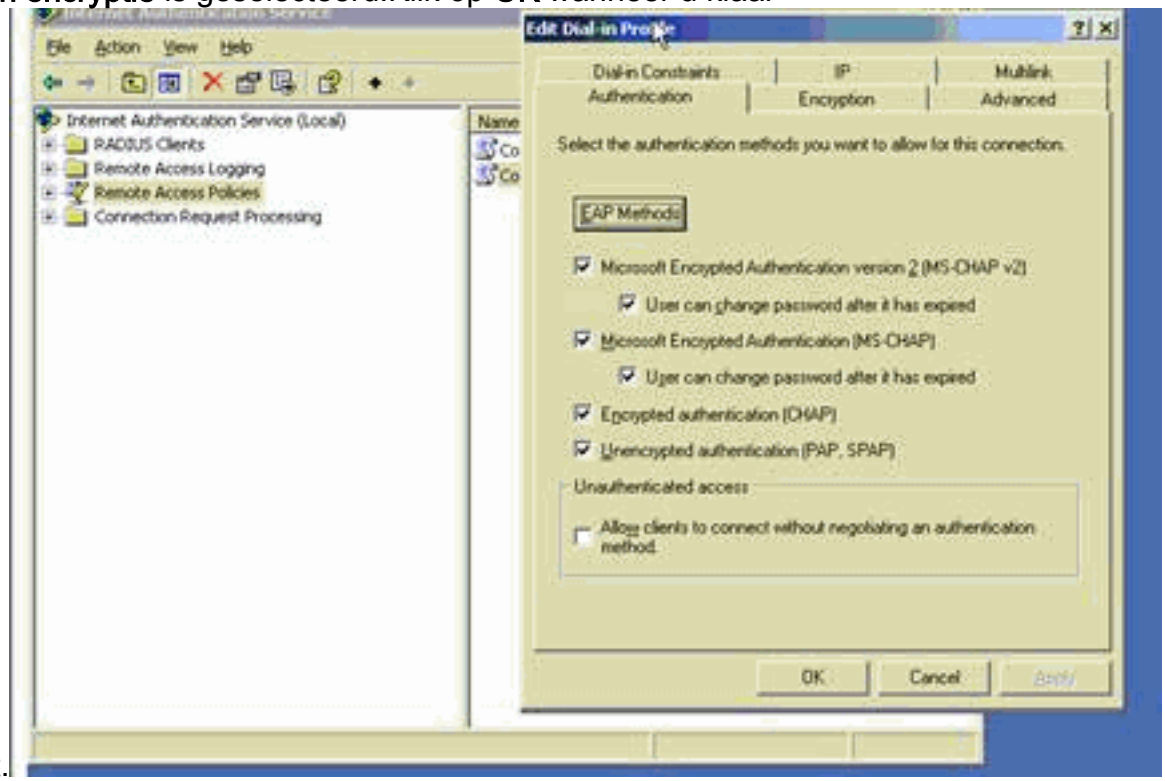
## Microsoft Windows 2003-server met IAS-configuratie

Voltooi deze stappen om de Microsoft Windows 2003-server te configureren met IAS.

**Toelichting:** In deze stappen wordt ervan uitgegaan dat de IAS reeds op de lokale machine is geïnstalleerd. Als dit niet het geval is, kunt u dit toevoegen via **Configuratiescherm > Software**.

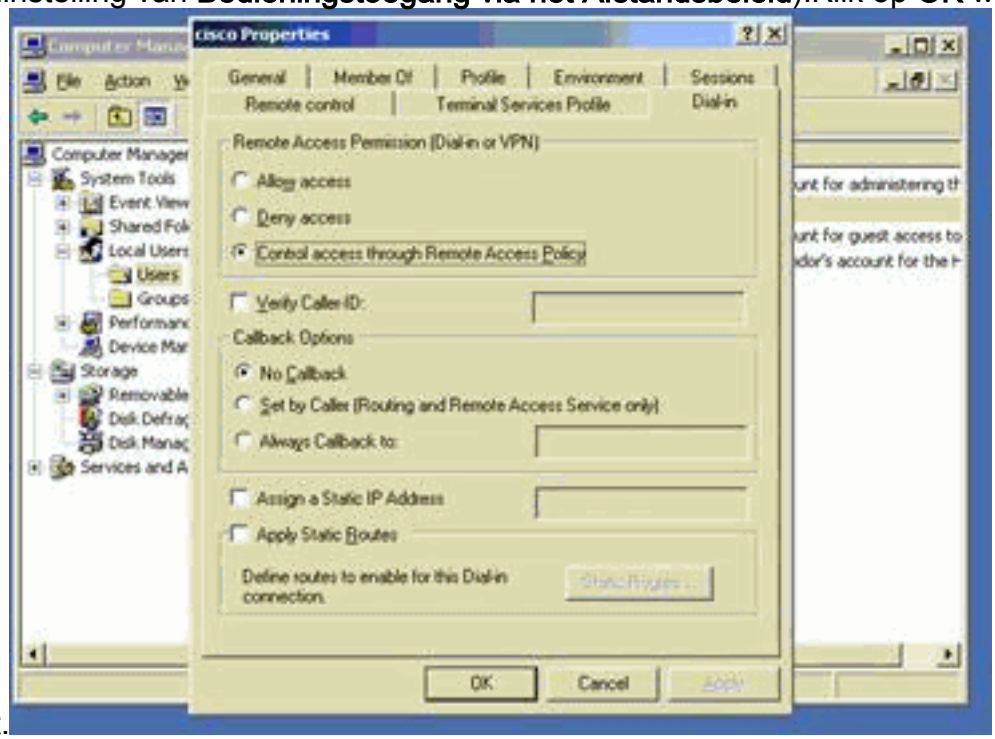
1. Kies **Administratieve Gereedschappen > Internet-verificatieservice** en klik met de rechtermuisknop op **RADIUS-client** om een nieuwe RADIUS-client toe te voegen. Klik nadat u de clientinformatie hebt getypt op **OK**.Dit voorbeeld toont een client met de naam "Pix" met een IP-adres van 10.4.4.1. De client-verkoper is ingesteld op **RADIUS-standaard** en het gedeelde geheim is

radiuskey. 


2. Kies **het beleid voor toegang op afstand**, klik met de rechtermuisknop op **Aansluitingen met andere toegangsservers** en selecteer **Eigenschappen**.
3. Zorg ervoor dat de optie voor **Grant Remote Access Permissions** is geselecteerd.
4. Klik op **Profiel bewerken** en controleer deze instellingen:Controleer op het tabblad Verificatie **Niet-versleutelde verificatie (PAP, SPAP)**.Zorg er in het tabblad Encryptie voor dat de optie **Geen encryptie** is geselecteerd.Klik op **OK** wanneer u klaar bent. 


5. Kies **Administratieve tools > Computerbeheer > Systeemtools > Lokale gebruikers en groepen**, klik met de rechtermuisknop op **gebruikers** en selecteer **Nieuwe gebruikers** om een gebruiker aan de lokale computeraccount toe te voegen.
6. Voeg een gebruiker toe met het Cisco-wachtwoord **wachtwoord 1** en controleer deze profielinformatie:Zorg er in het tabblad Algemeen voor dat de optie voor **Wachtwoord dat**

**nooit is verlopen** is geselecteerd in plaats van de optie voor Gebruiker moet Wachtwoord wijzigen.Selecteer in het tabblad Inbellen de optie voor **Toegang toestaan** (of laat de standaardinstelling van **Bedieningstoegang via het Afstandsbeleid**).Klik op **OK** wanneer u klaar bent.




## Uitgebreide verificatie voor L2TP via IPSec met actieve map

Gebruik deze configuratie op de ASA om de authenticatie voor de L2tp verbinding mogelijk te maken van de Actieve Map:

```
ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup
ppp-attributes
ciscoasa(config-ppp)# authentication pap
```

Ga ook, op de L2TP-client, naar **Geavanceerde security instellingen (Aangepast)** en kies alleen de optie voor **Unencryptie wachtwoord (PAP)**.

# Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

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.

- **toon crypto ipsec sa**-Toont alle huidige IKE security associaties (SAs) bij een peer.

```
pixfirewall#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_dyn_map, seq num: 20, local addr: 172.16.1.1

      access-list 105 permit ip host 172.16.1.1 host 192.168.0.2
      local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/17/0)
```

```
      remote ident (addr/mask/prot/port): (192.168.0.2/255.255.255.255/17/1701)
      current_peer: 192.168.0.2, username: test
      dynamic allocated peer ip: 10.4.5.15

#pkts encaps: 23, #pkts encrypt: 23, #pkts digest: 23
       #pkts decaps: 93, #pkts decrypt: 93, #pkts verify: 93
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 23, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.16.1.1, remote crypto endpt.: 192.168.0.2

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: C16F05B8

    inbound esp sas:
      spi: 0xEC06344D (3959829581)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Transport, }
         slot: 0, conn_id: 3, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (sec): 3335
         IV size: 8 bytes
         replay detection support: Y

outbound esp sas:
      spi: 0xC16F05B8 (3245278648)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Transport, }
         slot: 0, conn_id: 3, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (sec): 3335
         IV size: 8 bytes
         replay detection support: Y
```

- toon crypto isakmp sa-toont alle huidige IKE SAs bij een peer.

```
pixfirewall#show crypto isakmp sa

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.0.2
    Type    : user            Role    : responder
    Rekey   : no              State   : MM_ACTIVE
```

- tonen vpn-sessiondb-Omvat protocolfilters die u kunt gebruiken om gedetailleerde informatie over L2TP via IPsec verbindingen weer te geven. De volledige opdracht van de mondiale configuratiemodus is om vpn-sessoindb gedetailleerd afstandsfilterprotocol l2tpOverIPsec te tonen.Dit voorbeeld toont de details van één enkele L2TP over IPsec verbinding:

```
pixfirewall#show vpn-sessiondb detail remote filter protocol L2TPOverIPSec

Session Type: Remote Detailed

Username     : test
Index        : 1
Assigned IP  : 10.4.5.15             Public IP    : 192.168.0.2
Protocol     : L2TPOverIPSec         Encryption   : 3DES
Hashing      : MD5
Bytes Tx     : 1336                  Bytes Rx     : 14605
Client Type  :                       Client Ver   :
Group Policy : DefaultRAGroup
Tunnel Group : DefaultRAGroup
Login Time   : 18:06:08 UTC Fri Jan 1 1993
```

```
Duration     : 0h:04m:25s
Filter Name  :
NAC Result   : N/A
Posture Token:

IKE Sessions: 1
IPSec Sessions: 1
L2TPOverIPSec Sessions: 1


IKE:
  Session ID   : 1
  UDP Src Port : 500                    UDP Dst Port : 500
  IKE Neg Mode : Main                   Auth Mode    : preSharedKeys
  Encryption   : 3DES                   Hashing      : MD5
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 28536 Seconds
  D/H Group    : 2

IPSec:
  Session ID   : 2
  Local Addr   : 172.16.1.1/255.255.255.255/17/1701
  Remote Addr  : 192.168.0.2/255.255.255.255/17/1701
  Encryption   : 3DES                   Hashing      : MD5
  Encapsulation: Transport
  Rekey Int (T): 3600 Seconds           Rekey Left(T): 3333 Seconds
  Idle Time Out: 30 Minutes             Idle TO Left : 30 Minutes
  Bytes Tx     : 1336                   Bytes Rx     : 14922
  Pkts Tx      : 25                     Pkts Rx      : 156


L2TPOverIPSec:
  Session ID   : 3
  Username     : test
  Assigned IP  : 10.4.5.15
  Encryption   : none                   Auth Mode    : msCHAPV1
  Idle Time Out: 30 Minutes             Idle TO Left : 30 Minutes
  Bytes Tx     : 378                    Bytes Rx     : 13431
  Pkts Tx      : 16                     Pkts Rx      : 146
```

# Problemen oplossen

Deze sectie verschaft informatie om uw configuratie problemen op te lossen. Ook wordt een voorbeelduitvoer van debug-uitvoer weergegeven.

## Opdrachten voor troubleshooting

Bepaalde opdrachten worden ondersteund door het Uitvoergereedschap Interpreter (alleen geregistreerde klanten), waardoor u een analyse kunt bekijken van de opdrachtoutput.

**Opmerking:** Raadpleeg Belangrijke informatie over debug Commands en IP security probleemoplossing - Bezig met begrijpen en gebruiken debug Commands voordat u **debug-**opdrachten gebruikt.

- **debug crypto ipsec 7**-displays de IPsec onderhandelingen van fase 2.
- **debug crypto isakmp 7** — Hiermee geeft u de ISAKMP-onderhandelingen van fase 1 weer.

## Monster debug-uitvoer

## PIX-firewall

```
PIX#debug crypto isakmp 7
pixfirewall# Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Mess
age (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + NONE (0) total length : 256
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Oakley proposal is acceptable
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received Fragmentation VID
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received NAT-Traversal ver 02 V
ID
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing IKE SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, IKE SA Proposal # 1, Transform
# 2 acceptable  Matches global IKE entry # 2
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ISAKMP SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Fragmentation VID
+ extended capabilities payload
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 104
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0)
 with payloads : HDR + KE (4) + NONCE (10) + NONE (0) total length : 184
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ke payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ISA_KE payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ke payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Cisco Unity VID pa
yload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing xauth V6 VID paylo
ad
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send IOS VID
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Constructing ASA spoofing IOS V
endor ID payload (version: 1.0.0, capabilities: 20000001)
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send Altiga/Cisco VPN3000/Cisco
 ASA GW VID
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group Def
aultRAGroup
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat
ing keys for Responder...
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (
13) + VENDOR (13) + NONE (0) total length : 256
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0)
 with payloads : HDR + ID (5) + HASH (8) + NONE (0) total length : 60
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing ID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computi
ng hash for ISAKMP
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group Def
aultRAGroup
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Freeing previ
ously allocated memory for authorization-dn-attributes
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting ID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting hash payload
```

```
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computi
ng hash for ISAKMP
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting dpd vid payload
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length :
80

!--- Phase 1 completed succesfully. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP =
192.168.0.2, PHASE 1 COMPL
ETED
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alive type for this connection:
None
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alives configured on but peer do
es not support keep-alives (type = None)
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Startin
g P1 rekey timer: 21600 seconds.
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1
b84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +
NONE (0) total length : 164
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing ID payload
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received remo
te Proxy Host data in ID Payload:  Address 192.168.0.2, Protocol 17, Port 1701
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing ID payload
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received loca
l Proxy Host data in ID Payload:  Address 172.16.1.1, Protocol 17, Port 1701

!--- PIX identifies the L2TP/IPsec session. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP
= 192.168.0.2, L2TP/IPSec se
ssion detected.
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, QM IsRekeyed
old sa not found by addr
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE Remote Pe
er configured for crypto map: outside_dyn_map
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing IPSec SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IPSec S
A Proposal # 1, Transform # 1 acceptable  Matches global IPSec SA entry # 20
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE: requesti
ng SPI!
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got
 SPI from key engine: SPI = 0xce9f6e19

!--- Constructs Quick mode in Phase 2. Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP
= 192.168.0.2, oakley
constucting quick mode
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting blank hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting IPSec SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting IPSec nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting proxy ID
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Transmi
tting Proxy Id:
```

```
  Remote host: 192.168.0.2  Protocol 17  Port 1701
  Local host:  172.16.1.1  Protocol 17  Port 1701
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting qm hash payload
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=e1b
84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + N
ONE (0) total length : 144
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1
b84b0) with payloads : HDR + HASH (8) + NONE (0) total length : 48
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, loading
 all IPSEC SAs
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat
ing Quick Mode Key!
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat
ing Quick Mode Key!
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Security nego
tiation complete for User ()  Responder, Inbound SPI = 0xce9f6e19, Outbound SPI
= 0xd08f711b
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got
 a KEY_ADD msg for SA: SPI = 0xd08f711b
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Pitcher
: received KEY_UPDATE, spi 0xce9f6e19
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Startin
g P2 rekey timer: 3059 seconds.
```

*!--- Phase 2 completes succesfully.* Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, PHASE 2 COMPL ETED (msgid=0e1b84b0) Jan 02 18:26:44 [IKEv1]: IKEQM_Active() Add L2TP classification rules: ip <192.1 68.0.2> mask <0xFFFFFFFF> port <1701> PIX#**debug crypto ipsec 7**

```
pixfirewall# IPSEC: Deleted inbound decrypt rule, SPI 0x71933D09
    Rule ID: 0x028D78D8
IPSEC: Deleted inbound permit rule, SPI 0x71933D09
    Rule ID: 0x02831838
IPSEC: Deleted inbound tunnel flow rule, SPI 0x71933D09
    Rule ID: 0x029134D8
IPSEC: Deleted inbound VPN context, SPI 0x71933D09
    VPN handle: 0x0048B284
IPSEC: Deleted outbound encrypt rule, SPI 0xAF4DA5FA
    Rule ID: 0x028DAC90
IPSEC: Deleted outbound permit rule, SPI 0xAF4DA5FA
    Rule ID: 0x02912AF8
IPSEC: Deleted outbound VPN context, SPI 0xAF4DA5FA
    VPN handle: 0x0048468C
IPSEC: New embryonic SA created @ 0x01BFCF80,
    SCB: 0x01C262D0,
    Direction: inbound
    SPI      : 0x45C3306F
    Session ID: 0x0000000C
    VPIF num  : 0x00000001
    Tunnel type: ra
    Protocol   : esp
    Lifetime   : 240 seconds
IPSEC: New embryonic SA created @ 0x0283A3A8,
    SCB: 0x028D1B38,
    Direction: outbound
    SPI      : 0x370E8DD1
    Session ID: 0x0000000C
    VPIF num  : 0x00000001
    Tunnel type: ra
    Protocol   : esp
    Lifetime   : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x370E8DD1
```

```
IPSEC: Creating outbound VPN context, SPI 0x370E8DD1
    Flags: 0x00000205
    SA   : 0x0283A3A8
    SPI  : 0x370E8DD1
    MTU  : 1500 bytes
    VCID : 0x00000000
    Peer : 0x00000000
    SCB  : 0x028D1B38
    Channel: 0x01693F08
IPSEC: Completed outbound VPN context, SPI 0x370E8DD1
    VPN handle: 0x0048C164
IPSEC: New outbound encrypt rule, SPI 0x370E8DD1
    Src addr: 172.16.1.1
    Src mask: 255.255.255.255
    Dst addr: 192.168.0.2
    Dst mask: 255.255.255.255
    Src ports
      Upper: 1701
      Lower: 1701
      Op   : equal
    Dst ports
      Upper: 1701
      Lower: 1701
      Op   : equal
    Protocol: 17
    Use protocol: true
    SPI: 0x00000000
    Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x370E8DD1
    Rule ID: 0x02826540
IPSEC: New outbound permit rule, SPI 0x370E8DD1
    Src addr: 172.16.1.1
    Src mask: 255.255.255.255
    Dst addr: 192.168.0.2
    Dst mask: 255.255.255.255
    Src ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Dst ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 50
    Use protocol: true
    SPI: 0x370E8DD1
    Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x370E8DD1
    Rule ID: 0x028D78D8
IPSEC: Completed host IBSA update, SPI 0x45C3306F
IPSEC: Creating inbound VPN context, SPI 0x45C3306F
    Flags: 0x00000206
    SA   : 0x01BFCF80
    SPI  : 0x45C3306F
    MTU  : 0 bytes
    VCID : 0x00000000
    Peer : 0x0048C164
    SCB  : 0x01C262D0
    Channel: 0x01693F08
IPSEC: Completed inbound VPN context, SPI 0x45C3306F
    VPN handle: 0x0049107C
IPSEC: Updating outbound VPN context 0x0048C164, SPI 0x370E8DD1
    Flags: 0x00000205
    SA   : 0x0283A3A8
```

```
    SPI  : 0x370E8DD1
    MTU  : 1500 bytes
    VCID : 0x00000000
    Peer : 0x0049107C
    SCB  : 0x028D1B38
    Channel: 0x01693F08
IPSEC: Completed outbound VPN context, SPI 0x370E8DD1
    VPN handle: 0x0048C164
IPSEC: Completed outbound inner rule, SPI 0x370E8DD1
    Rule ID: 0x02826540
IPSEC: Completed outbound outer SPD rule, SPI 0x370E8DD1
    Rule ID: 0x028D78D8
IPSEC: New inbound tunnel flow rule, SPI 0x45C3306F
    Src addr: 192.168.0.2
    Src mask: 255.255.255.255
    Dst addr: 172.16.1.1
    Dst mask: 255.255.255.255
    Src ports
      Upper: 1701
      Lower: 1701
      Op   : equal
    Dst ports
      Upper: 1701
      Lower: 1701
      Op   : equal
    Protocol: 17
    Use protocol: true
    SPI: 0x00000000
    Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x45C3306F
    Rule ID: 0x02831838
IPSEC: New inbound decrypt rule, SPI 0x45C3306F
    Src addr: 192.168.0.2
    Src mask: 255.255.255.255
    Dst addr: 172.16.1.1
    Dst mask: 255.255.255.255
    Src ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Dst ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 50
    Use protocol: true
    SPI: 0x45C3306F
    Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x45C3306F
    Rule ID: 0x028DAC90
IPSEC: New inbound permit rule, SPI 0x45C3306F
    Src addr: 192.168.0.2
    Src mask: 255.255.255.255
    Dst addr: 172.16.1.1
    Dst mask: 255.255.255.255
    Src ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Dst ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 50
```

```
    Use protocol: true
    SPI: 0x45C3306F
    Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x45C3306F
    Rule ID: 0x02912E50
```

## Probleemoplossing met ASDM

U kunt ASDM gebruiken om houtkap mogelijk te maken en om de logbestanden te bekijken.

1. Kies **Configuration > Properties > Logging > Logging Setup**, selecteer **Vastlegging inschakelen** en klik **op Toepassen** om vastlegging mogelijk te maken.
2. Kies **Monitoring > Vastlegging > Logboek Buffer > Op vastlegging niveau**, selecteer **Logging Buffer** en klik op **Weergeven** om de logbestanden te bekijken.

## Probleem: Frequente afsluiten

### Time-out bij sessie

Als de inactiviteitstimer is ingesteld op 30 minuten (standaard), betekent dit dat de tunnel valt nadat er 30 minuten geen verkeer door is gepasseerd. De VPN-client wordt na 30 minuten losgekoppeld, ongeacht de instelling van de tijdelijke uitvoer, en ontmoet de `PEER_DELETE-IKE_DELETE_UNSPECIFIED` foutmelding.

Configureer de tijdelijke time-out en sessietimeout als geen om de tunnel altijd omhoog te laten gaan zodat deze nooit valt.

Voer de opdracht **vpn-idle-timeout in** de configuratie-modus voor groepsbeleid of in de configuratie-modus voor gebruikersnaam in om de time-out periode van de gebruiker te configureren:

```
hostname(config)#group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#vpn-idle-timeout none
```

Configureer een maximale hoeveelheid tijd voor VPN-verbindingen met de opdracht **vpn-sessie-timeout** in de configuratie-modus van het groepsbeleid of in de configuratie-modus van de gebruikersnaam:

```
hostname(config)#group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#vpn-session-timeout none
```

## Probleemoplossing voor Windows Vista

### Gelijktijdige gebruiker

Windows Vista L2TP/IPsec heeft een aantal architectuurwijzigingen geïntroduceerd die meer dan één gelijktijdige gebruiker ervan weerhouden te worden aangesloten op een head-end PIX/ASA. Dit gedrag komt niet voor in Windows 2K/XP. Cisco heeft een tijdelijke oplossing voor deze wijziging geïmplementeerd vanaf release 7.2(3) en hoger.

### Vista PC kan niet worden aangesloten

Als de Windows Vista-computer niet in staat is om de L2TP-server aan te sluiten, controleer dan of u alleen mschap-v2 hebt ingesteld onder de ppp-eigenschappen van de DefaultRAGGroup.

## Gerelateerde informatie

- Meest gebruikelijke L2L- en IPSec VPN-oplossingen voor probleemoplossing
- Cisco PIX 500 Series security applicaties
- Adaptieve security applicaties van Cisco ASA 5500 Series
- Productondersteuning voor Cisco PIX-firewall
- Opdrachtreferenties van Cisco Secure PIX-firewall
- RADIUS-ondersteuningspagina
- Ondersteuning van IPSec-onderhandeling/IKE-protocollen
- Verzoeken om opmerkingen (RFC's)
- Layer 2 Tunnel Protocol (L2TP)
- Technische ondersteuning en documentatie – Cisco Systems