

Ejemplo de Configuración de L2TP sobre IPsec entre Windows 2000/XP PC y PIX/ASA 7.2 Usando Clave Previamente Compartida

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Productos Relacionados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración de Windows L2TP/IPsec Client](#)

[Servidor L2TP en la Configuración PIX](#)

[L2TP con Configuración de ASDM](#)

[Servidor de Microsoft Windows 2003 con Configuración IAS](#)

[Autenticación ampliada para L2TP sobre IPsec mediante Active Directory](#)

[Verificación](#)

[Troubleshoot](#)

[Comandos para resolución de problemas](#)

[Ejemplo de resultado del comando debug](#)

[Troubleshooting con ASDM](#)

[Problema: Desconexiones frecuentes](#)

[Troubleshooting Windows Vista](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar el Layer 2 Tunneling Protocol (L2TP) sobre la seguridad IP (IPsec) desde Microsoft Windows 2000/2003 remoto clientes XP a una oficina corporativa de PIX Security Appliance con claves previamente compartidas con el servidor RADIUS de Internet Authentication Service de Microsoft Windows 2003 (IAS) para la autenticación de usuario. Consulte [Microsoft - Lista de verificación: Configuración de IAS para marcación manual y acceso VPN para más información sobre el IAS.](#)

La ventaja principal de configurar el L2TP con el IPsec en un escenario de acceso remoto es que los usuarios remotos pueden acceder a un VPN en una red IP pública sin un gateway o una línea

dedicada. Esto habilita el acceso remoto desde prácticamente cualquier lugar con POTS. Una ventaja adicional es que el único requisito del cliente para el acceso VPN es el uso del Windows 2000 con Microsoft Dial-Up Networking de Microsoft (DUN). No se requiere ningún software de cliente adicional, tal como Cisco VPN Client.

Este documento también describe cómo utilizar el Cisco Adaptive Security Device Manager (ASDM) para configurar el PIX 500 Series PIX 500 Security Appliance para L2TP sobre el IPsec.

Nota: [El protocolo de túnel de capa 2 \(L2TP\) sobre IPsec](#) es compatible con Cisco Secure PIX Firewall Software Release 6.x y posteriores.

Para configurar el L2TP a través de IPsec entre el PIX 6.x y Windows 2000, consulte [Configuración de L2TP a través de IPsec entre el firewall PIX y el Windows 2000 PC usando los certificados](#).

Para configurar el L2TP a través de IPsec desde Microsoft Windows 2000 remoto y los clientes XP a un sitio corporativo usando un método cifrado, consulte [Configuración de L2TP a través de IPsec desde Windows 2000 o XP Client a un Cisco VPN 3000 Series usando las Caves Previamente Compartidas](#)

Prerequisites

Requirements

Ante del establecimiento del túnel seguro, debe haber conectividad IP entre los pares.

Asegúrese de que el puerto 1701 UDP no esté bloqueado en la trayectoria de la conexión.

Use la política predeterminada solamente del grupo de túnel y del grupo predeterminado en el PIX/ASA de Cisco. Las políticas y los grupos definidos por el usuario no funcionan.

Nota: El dispositivo de seguridad no establece un túnel L2TP/IPsec con Windows 2000 si Cisco VPN Client 3.x o Cisco VPN 3000 Client 2.5 están instalados. Inhabilite el servicio de Cisco VPN para Cisco VPN Client 3.x, o el servicio de ANetIKE para Cisco VPN 3000 Client 2.5 del panel de Servicios en Windows 2000. Para hacerlo, elija **Start > Programs > Administrative Tools > Services**, reinicie el Agente de Servicios Política IPsec del panel de Servicios y reinicie el equipo.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- PIX Security Appliance 515E con versión de software 7.2(1) o posterior
- Adaptive Security Device Manager 5.2(1) o posterior
- Microsoft Windows 2000 Server
- Microsoft Windows XP Professional con SP2
- Servidor de Windows 2003 con IAS

Nota: Si actualiza el PIX 6.3 a la versión 7.x, asegúrese de haber instalado SP2 en Windows XP (cliente L2TP).

Nota: La información del documento también es válida para el dispositivo de seguridad ASA.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Productos Relacionados

Esta configuración puede también se utilizar con Cisco ASA 5500 Series Security Appliance 7.2(1) o posterior.

Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco para obtener más información sobre las convenciones del documento.](#)

Antecedentes

Complete estos pasos para configurar el L2TP a través de IPsec.

1. Configure al modo de transporte de IPsec para habilitar el IPsec con el L2TP. El cliente de Windows 2000 L2TP/IPsec utiliza al modo de transporte de IPsec - Solamente se encripta el contenido IP, y los encabezados IP originales quedan intactos. Las ventajas de este modo son que agrega solamente algunos bytes a cada paquete y permite que los dispositivos en la red pública vean el origen final y el destino del paquete. Por lo tanto, para que los clientes de Windows 2000 L2TP/IPsec se conecten con el dispositivo de seguridad, debe configurar al modo de transporte de IPsec para una transformación (consulte el paso 2 en la [Configuración de ASDM](#)). Con esta capacidad (transporte), puede habilitar el proceso especial (por ejemplo, QoS) en la red intermedia basada en la información en el encabezado IP. Sin embargo, se encripta el encabezado de la Capa 4, que limita e examen del paquete. Lamentablemente, la transmisión del encabezado IP en el texto no cifrado, el modo de transporte permite que un atacante realice cierto análisis del tráfico.
2. Configure el L2TP con un grupo de red virtual de marcación privada (VPDN).

La configuración de L2TP con los certificados de los soportes para IPsec que utilizan las claves previamente compartidas o los métodos de firma RSA, como el uso de mapas crypto dinámicos (en lugar de estáticos). La clave previamente compartida se utiliza como autenticación para establecer el L2TP a través de túnel IPsec.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

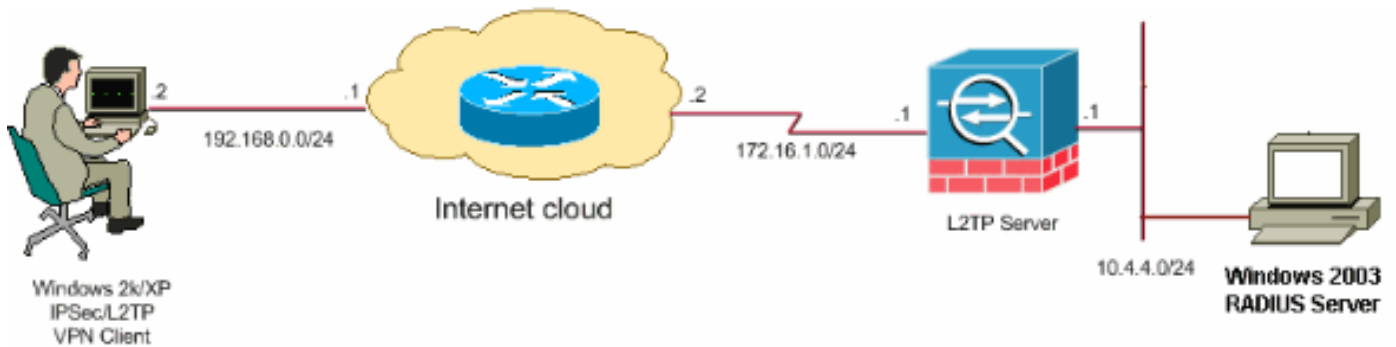
Nota: Use la [Command Lookup Tool](#) (sólo [clientes registrados](#)) para obtener más información sobre los comandos utilizados en este documento.

Nota: Los esquemas de direccionamiento IP utilizados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de

laboratorio.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- [Configuración de Windows L2TP/IPsec Client](#)
- [Servidor L2TP en la Configuración PIX](#)
- [L2TP con Configuración de ASDM](#)
- [Servidor de Microsoft Windows 2003 con Configuración IAS](#)

Configuración de Windows L2TP/IPsec Client

Complete estos pasos para configurar el L2TP a través de IPsec en Windows 2000. Para Windows XP omite los pasos 1 y 2 y diríjase al paso 3:

1. Agregue este valor de registro al equipo con Windows 2000:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
```

2. Agregue este valor de registro a esta clave:

Value Name: ProhibitIpSec

Data Type: REG_DWORD

Value: 1

Nota: En algunos casos (Windows XP Sp2), la adición de esta clave (**Valor: 1**) aparece para interrumpir la conexión haciendo que el cuadro XP negocie el L2TP solamente en lugar de un L2TP con conexión IPsec. Es obligatorio agregar una Política de IPsec junto con la clave de registro. Si recibe el error 800 cuando intenta establecer una conexión, quite la clave (Valor: 1) para que la conexión funcione. **Nota:** Debe reiniciar el equipo Windows 2000/2003 o XP para que los cambios surtan efecto. De forma predeterminada, el cliente de Windows intenta utilizar el IPsec con Certificate Authority (CA). La configuración de esta clave de registro evita que esto suceda. Ahora puede configurar una Política de IPsec en la estación de Windows para coincidir con los parámetros que desea en PIX/ASA. Consulte [Cómo Configurar una Conexión L2TP/IPsec usando la Autenticación de la Clave Previamente Compartida \(Q240262\)](#) para una configuración paso a paso de la Política de IPsec de Windows. Consulte [Configuración de una Clave Previamente Compartida para Uso con](#)

[Conexiones de Protocolo de Tunelización de Capa 2 en Windows XP \(Q281555\)](#) para obtener más información.

3. Cree su conexión.
4. Bajo Red y Conexiones por Línea Telefónica, haga clic con el botón derecho del mouse en la conexión y elija **Propiedades**. Diríjase a la pestaña Security y haga clic en **Advanced**. Elija los protocolos como muestra la

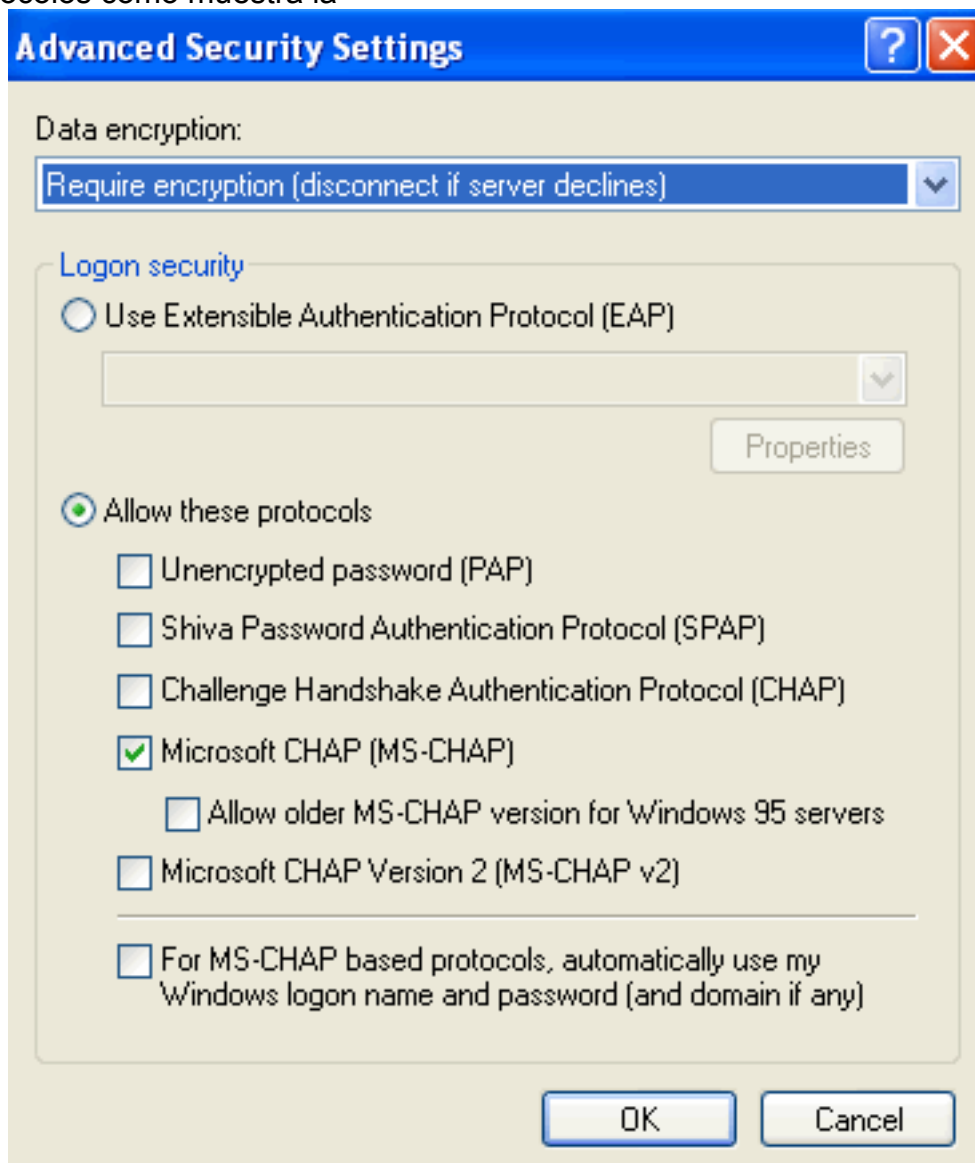
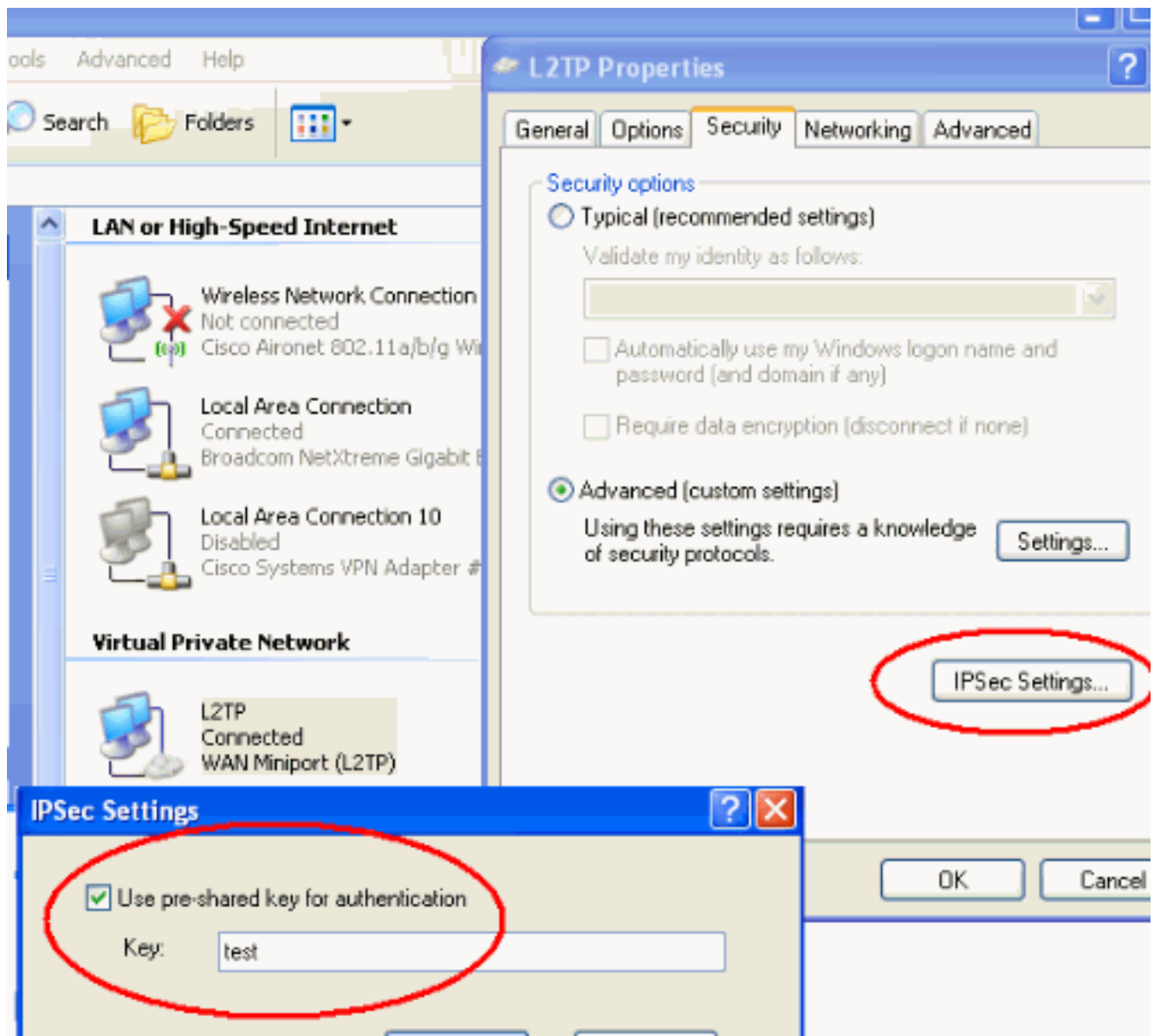


imagen.

5. **Nota:** Este paso es aplicable solamente para Windows XP. Haga clic en **Configuraciones del IPSec**, marque **Usar clave previamente compartida y escriba la clave previamente compartida para establecer la clave previamente compartida**. En este ejemplo, la prueba se utiliza como la clave previamente compartida.



Servidor L2TP en la Configuración PIX

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.
```

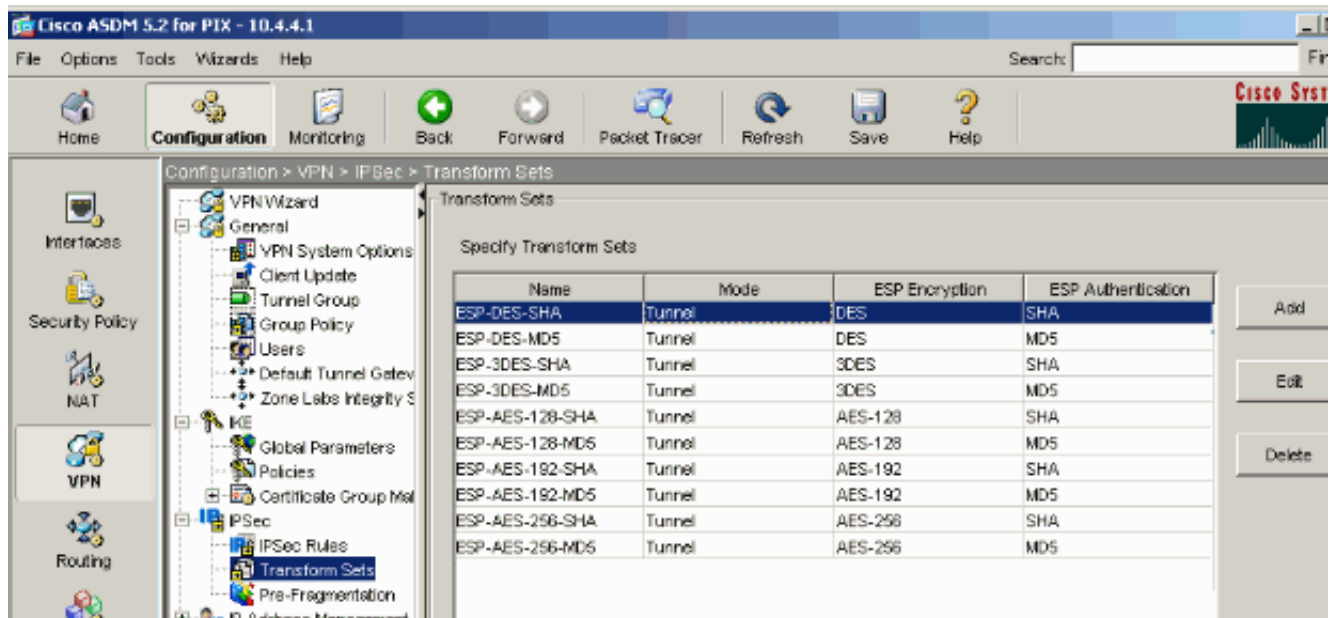
```
tunnel-group DefaultRAGroup ppp-attributes
no authentication chap
authentication ms-chap-v2
```

```
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
```

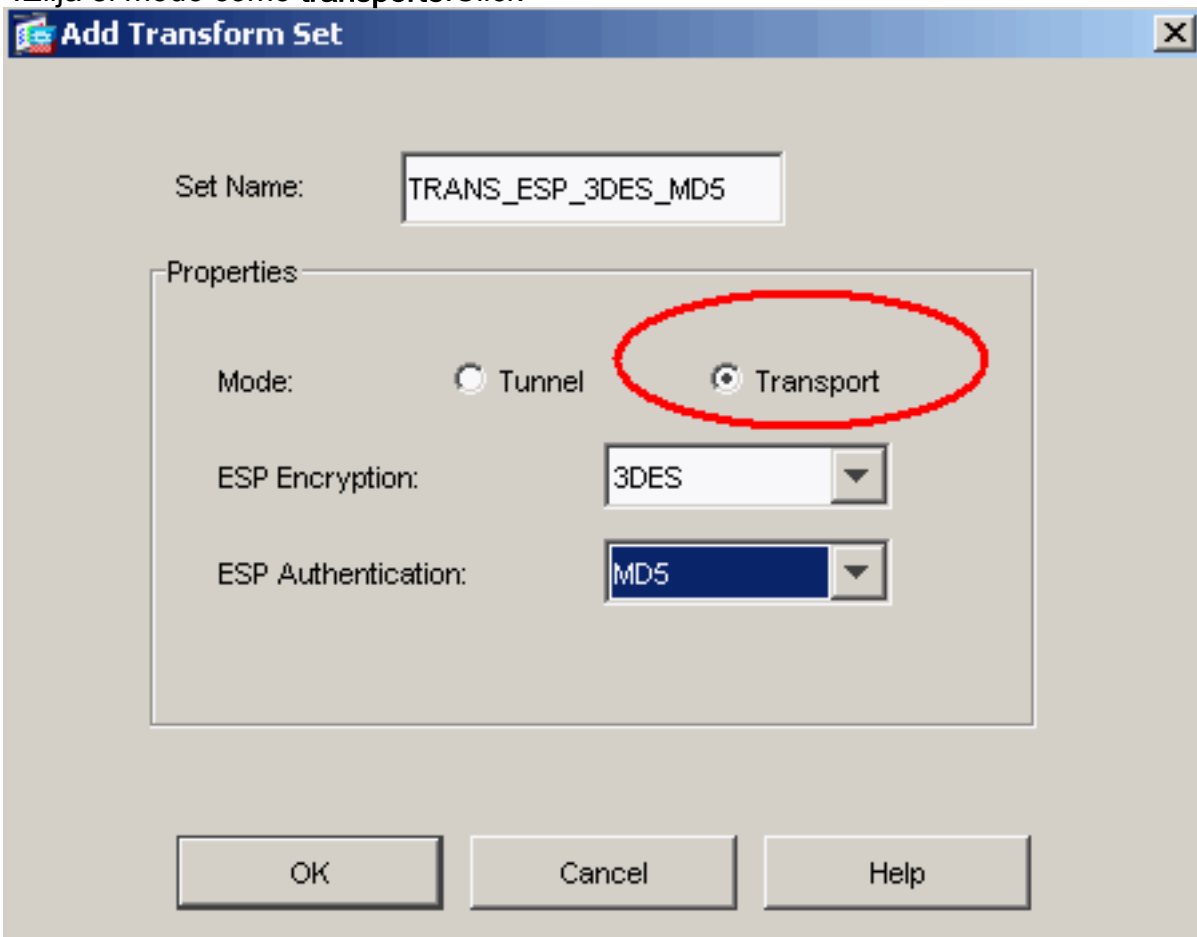
[L2TP con Configuración de ASDM](#)

Complete estos pasos para configurar el dispositivo de seguridad para validar el L2TP a través de las conexiones del IPsec:

1. Agregue un conjunto de transformaciones IPsec y especifique IPsec para usar el modo de transformaciones en lugar del modo túnel. para hacerlo, elija **Configuration > VPN > IPsec > Transform Sets** y haga clic en **Agregar**. Se muestra el panel Conjuntos de Transformaciones.

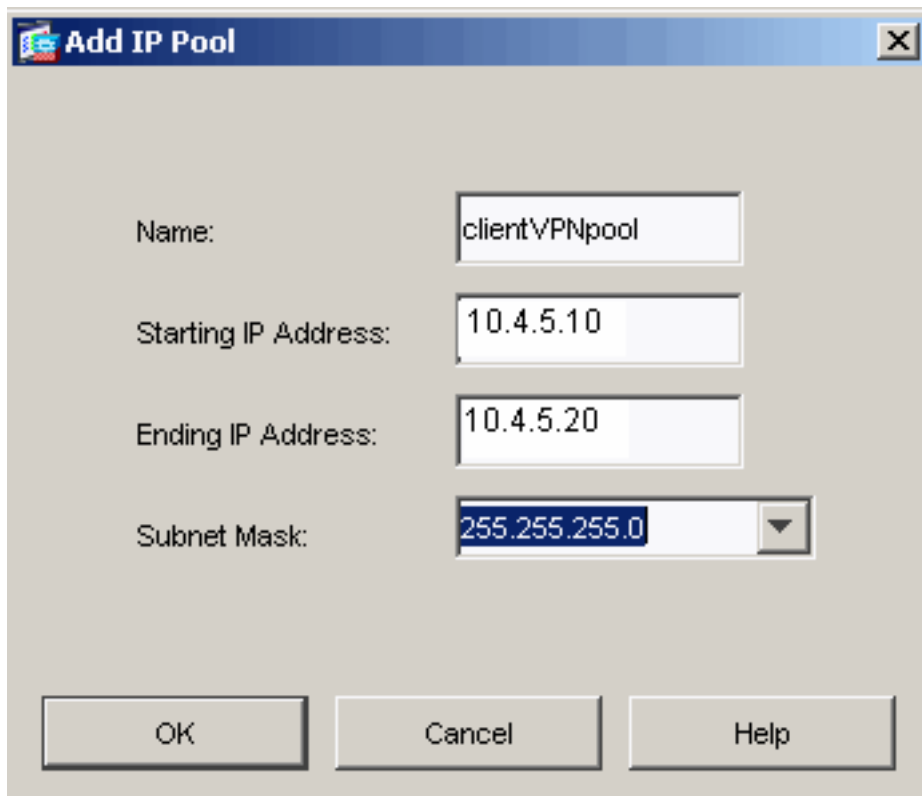


- Complete estos pasos para agregar una transformación establecida: Ingrese un nombre para el conjunto de transformaciones. Elija los métodos de Cifrado ESP y de Autenticación ESP. Elija el modo como **transporte**. Click



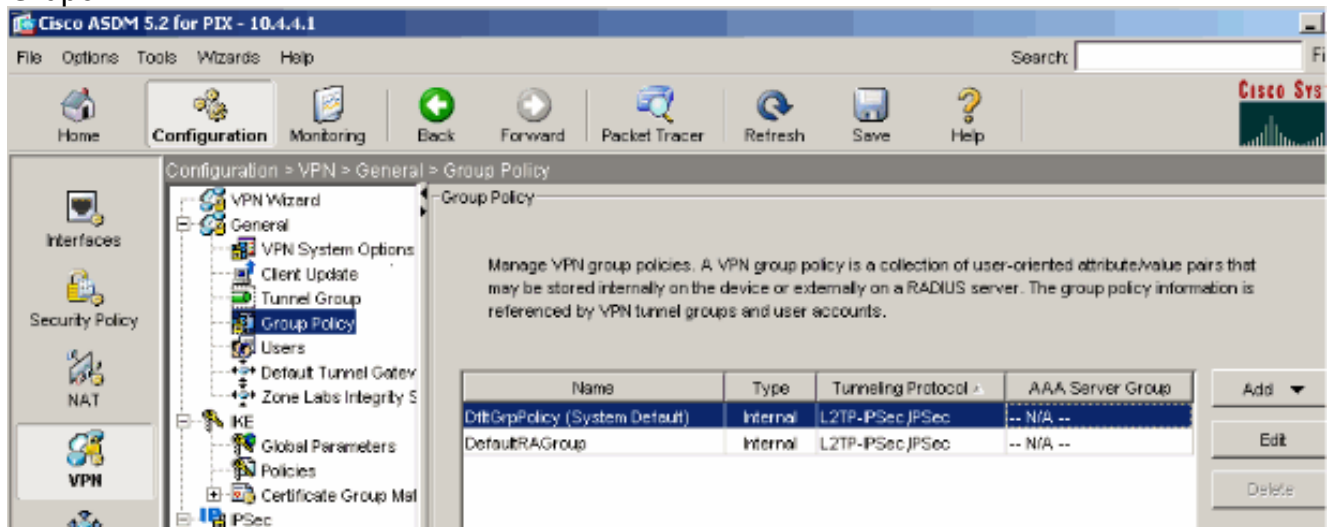
OK.

- Termina estos pasos para configurar un método de asignación de dirección. Este ejemplo utiliza los pools de la dirección IP. Elija **Configuration > VPN > IP Address Management > IP Pools**. Haga clic en Add (Agregar). Aparece el cuadro de diálogo Agregar Pool IP. Ingrese el nombre del nuevo pool de dirección IP. Ingrese las direcciones IP de inicio y de finalización. Ingrese la máscara de subred y haga clic en

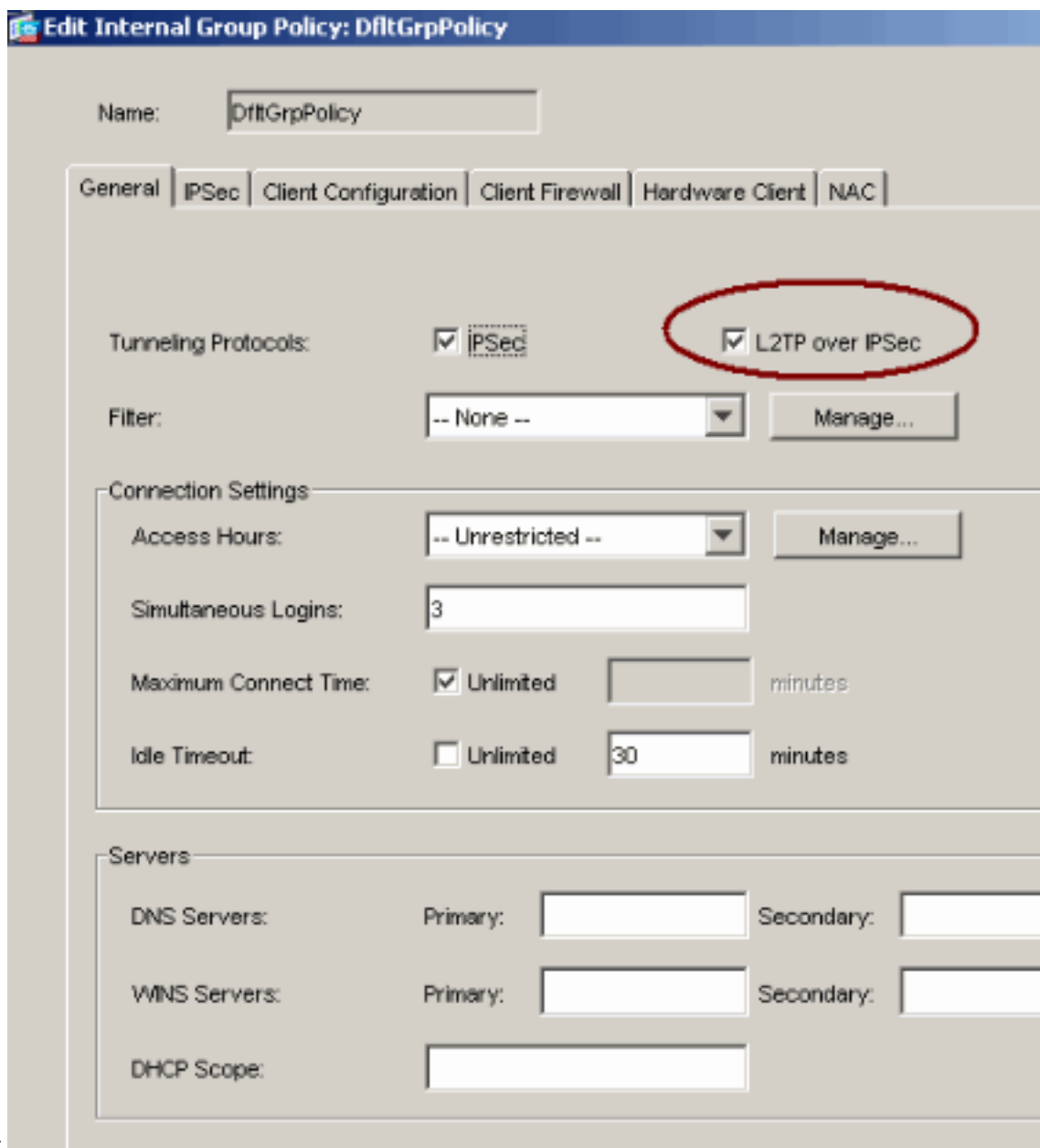


Aceptar.

4. Elija Configuration > VPN > General > Group Policy para configurar L2TP a través de IPsec como VPN tunneling protocol válido para la política de grupo. Se muestra el panel de Política de Grupo.

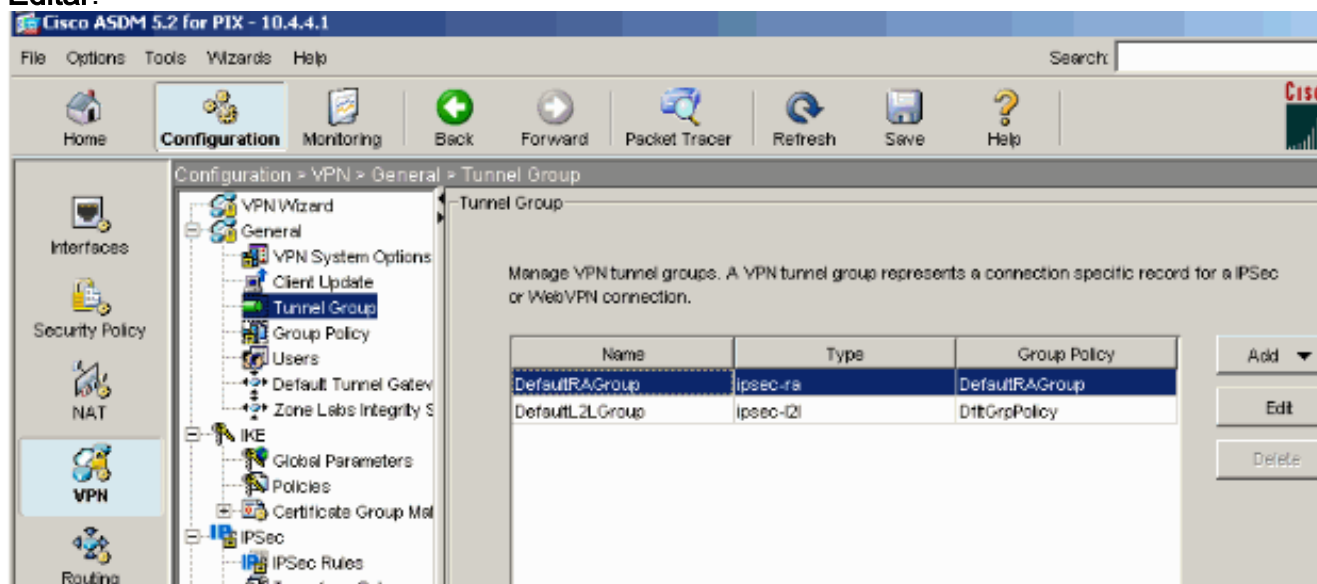


5. Seleccione una política de grupo (DiffGrpPolicy) y haga clic en **Editar**. Se muestra el cuadro de diálogo Editar Política de Grupo. Verifique L2TP a través de IPsec para habilitar el protocolo para la política de grupo y luego haga clic en



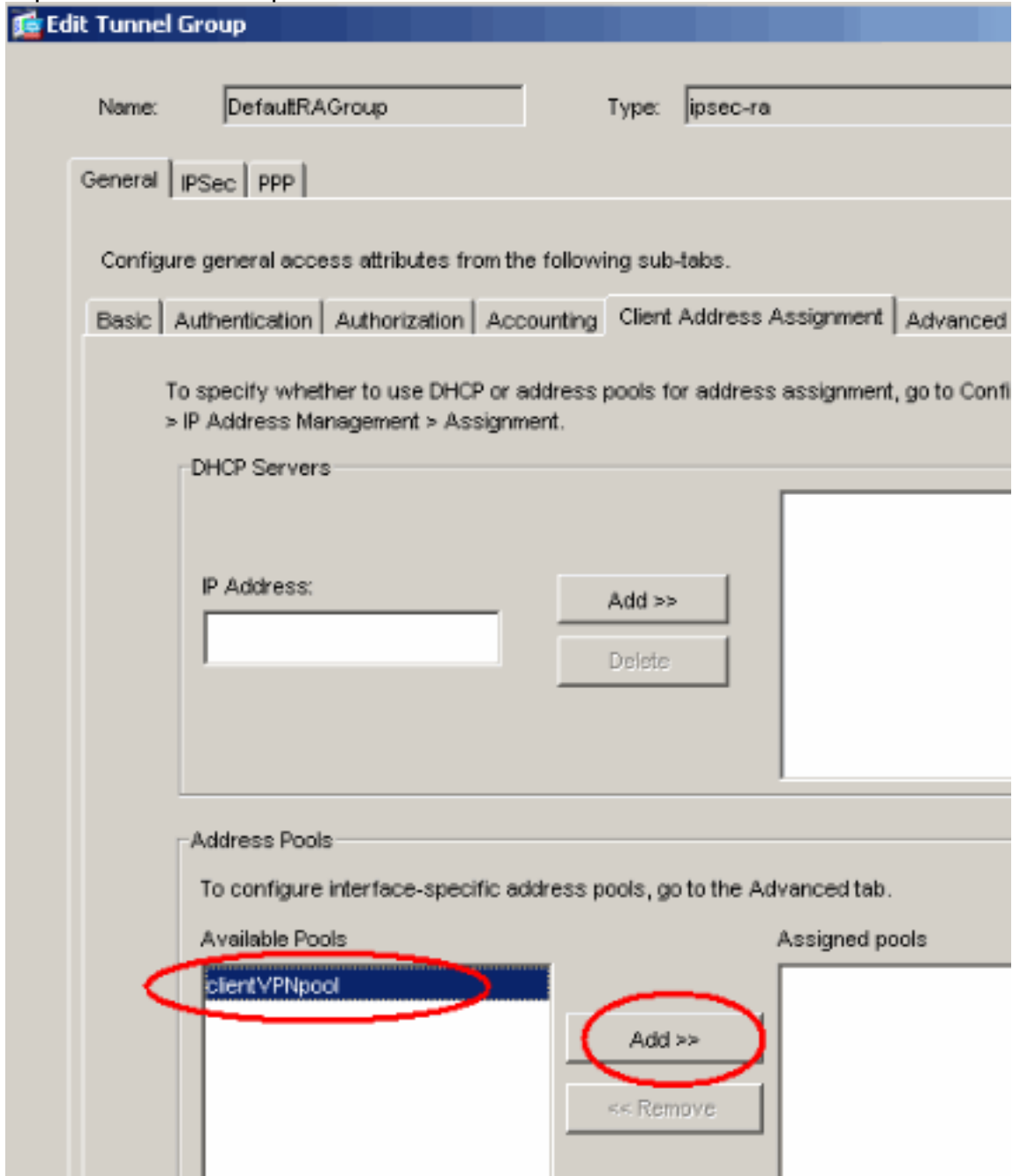
Aceptar.

- Complete estos pasos para asignar el pool de dirección IP a un grupo de túnel: Elija **Configuration > VPN > General > Tunnel Group**. Una vez que aparece el Grupo de Túnel, seleccione el grupo de túnel (DefaultRAGroup) en la tabla. Haga clic en **Editar**.



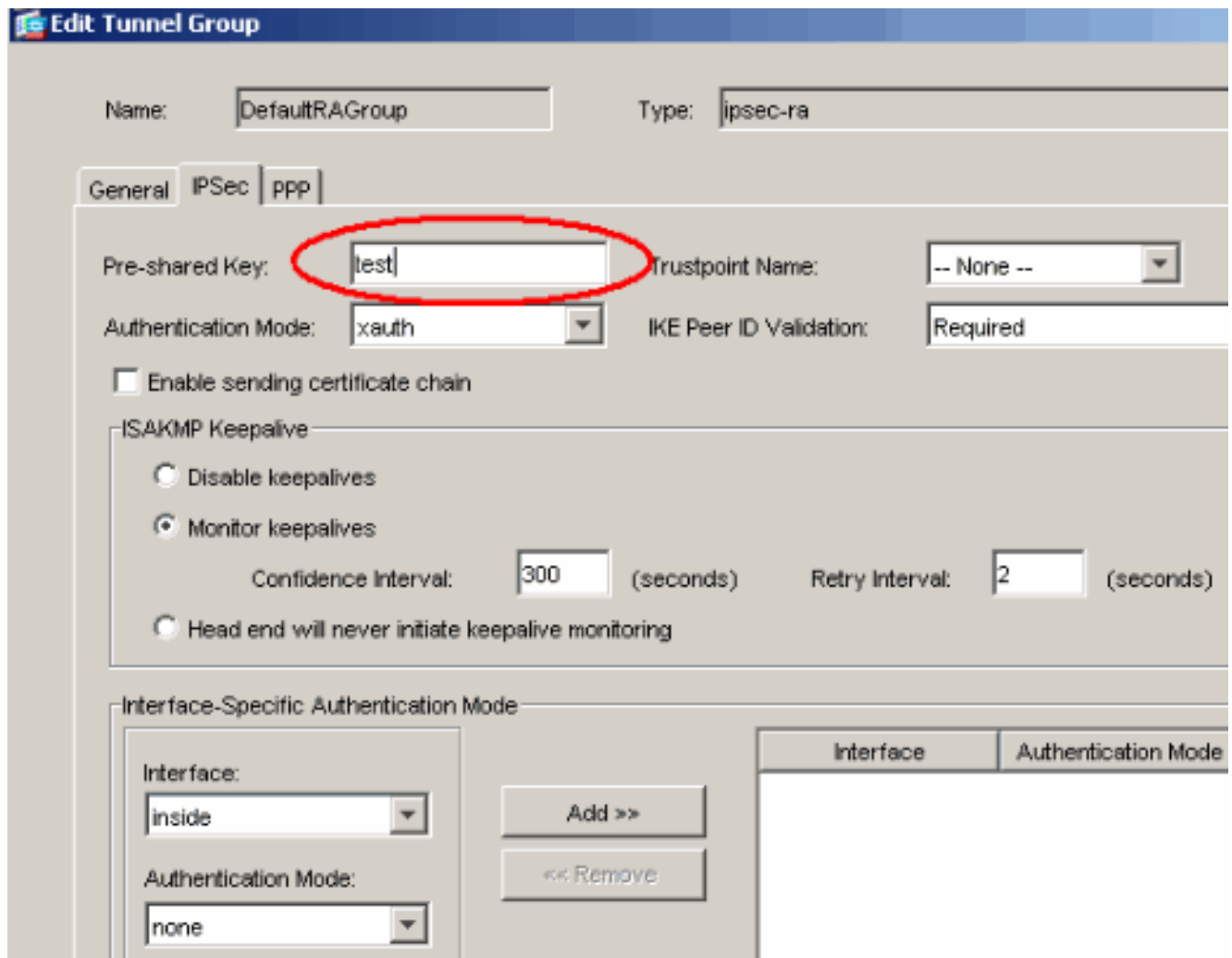
- Complete estos pasos cuando aparezca la ventana Edita Grupo de Túnel: Desde la pestaña

General, diríjase a la pestaña Client Address Assignment. En el área de Pools de Direcciones, elija un pool de direcciones para asignar al grupo de túnel. Haga clic en Add (Agregar). El pool de dirección aparece en el cuadro Pools

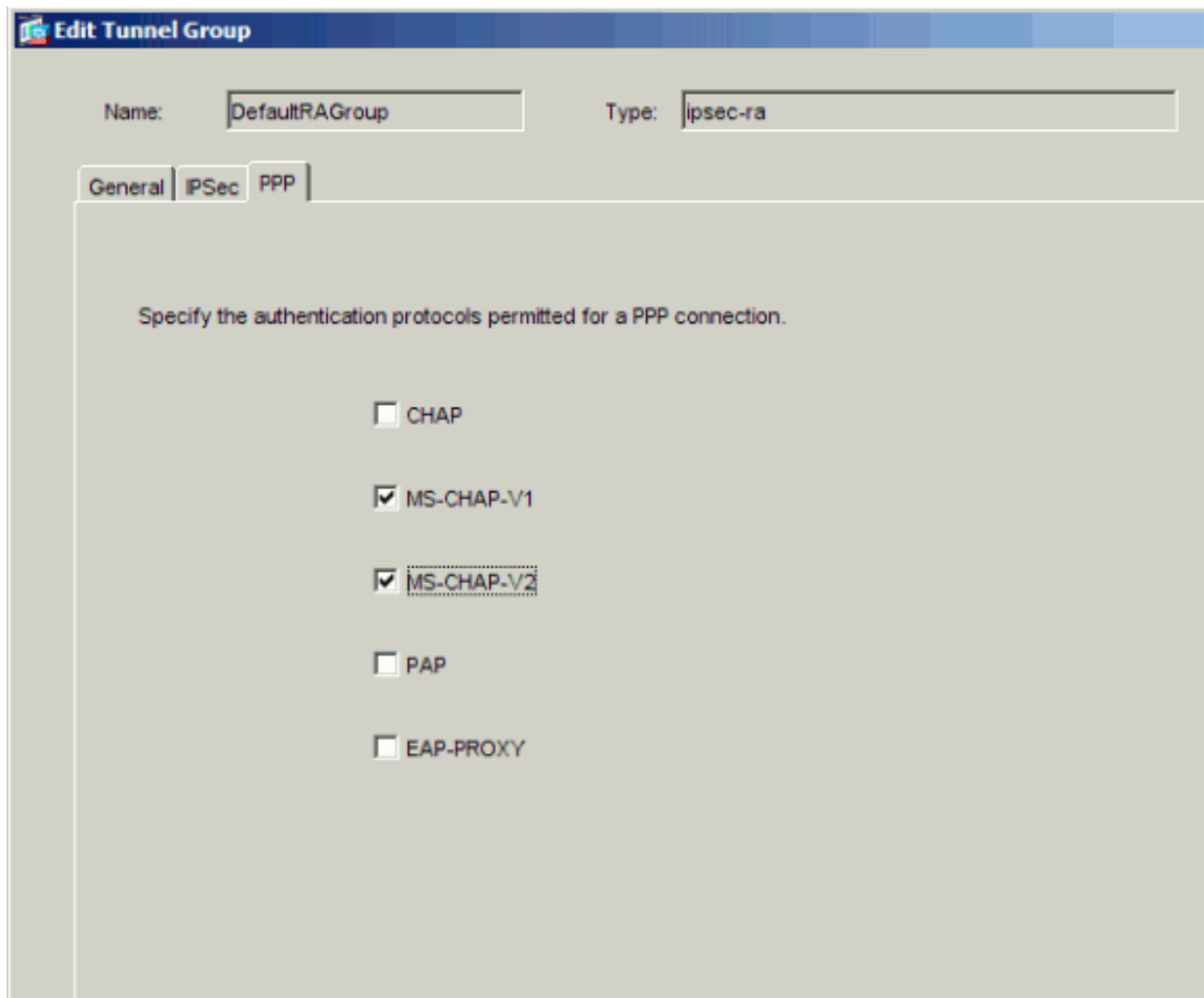


Asignados.

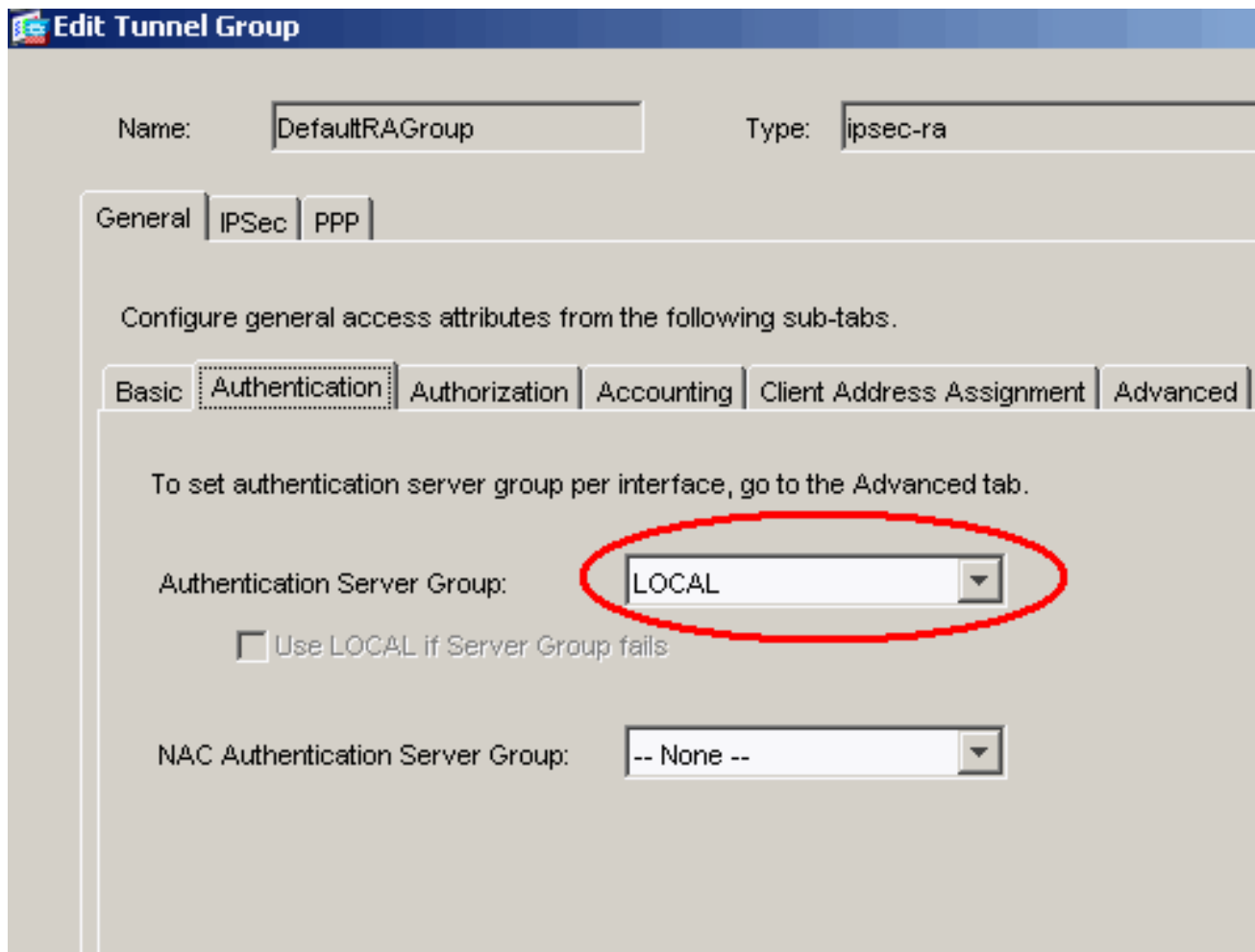
8. Para configurar la clave previamente compartida, diríjase a la pestaña IPSec, ingrese su clave previamente compartida (Pre-shared Key), y haga clic en OK.



9. L2TP a través de IPsec usa los protocolos de autenticación PPP. Especifique los protocolos que se permiten para las conexiones PPP en la pestaña PPP del grupo de túnel. Seleccione el protocolo **MS-CHAP-V1** para la autenticación.



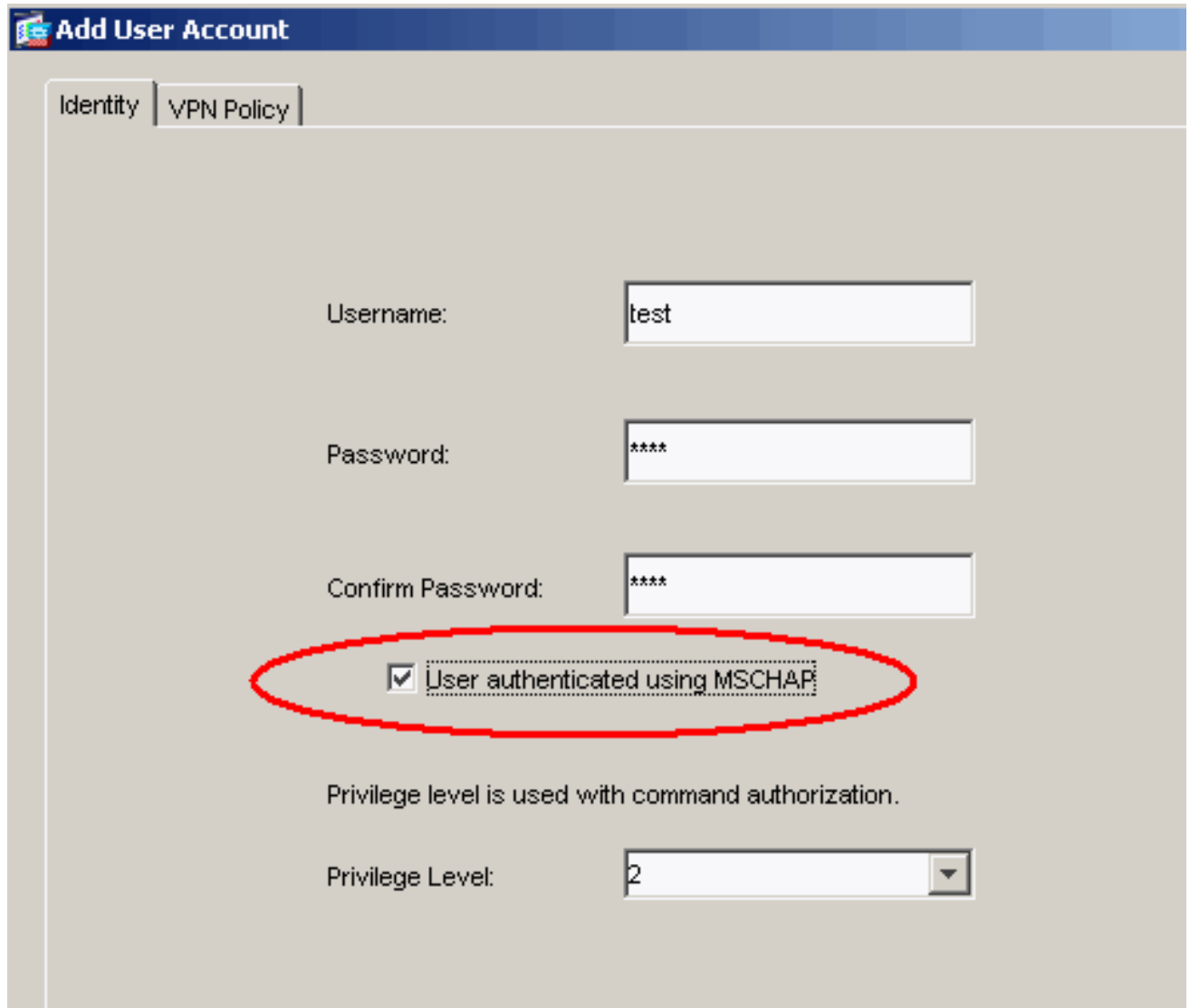
10. Especifique un método para autenticar los usuarios que intenten el L2TP a través de conexiones del IPSec. Puede configurar el dispositivo de seguridad para utilizar un servidor de autenticación o sus propias bases de datos locales. Para hacerlo, diríjase a la pestaña Authentication del grupo de túnel. De forma predeterminada, el dispositivo de seguridad usa sus bases de datos locales. La lista desplegable del Grupo de Servidor de Autenticación muestra LOCAL. Para utilizar un servidor de autenticación, seleccione uno de la lista. **Nota:** El dispositivo de seguridad sólo admite las autenticaciones PPP PAP y Microsoft CHAP versiones 1 y 2 en la base de datos local. El EAP y el CHAP son realizados por servidores de autenticación proxy. Por lo tanto, si un usuario remoto pertenece a un grupo de túnel configurado con EAP o CHAP, y el dispositivo de seguridad se configura para utilizar las bases de datos locales, que el usuario no puede conectar.



Nota: Elija **Configuration > VPN > General > Tunnel Group** para volver a la configuración del grupo de túnel de modo que pueda vincular la política de grupo al grupo de túnel y habilitar Tunnel Group Switching (opcional). Cuando aparece el panel del Grupo de Túnel, elija al grupo de túnel y haga clic en **Editar**. **Nota:** El Switching de Grupo de Túnel permite al dispositivo de seguridad asociar diferentes usuarios que establecen L2TP a través de conexiones IPsec con diferentes grupos de túnel. Como cada grupo de túnel tiene sus propios pools del grupo de servidores AAA y pools de dirección IP, los usuarios pueden ser autenticados con los métodos específicos a su grupo de túnel. Con esta función, en vez de enviar solo un nombre de usuario, el usuario envía un nombre de usuario y un nombre del grupo en el formato `username@group_name`, donde "@" representa un delimitador que puede configurar, y el nombre del grupo es el nombre de un grupo de túnel que se configura en el dispositivo de seguridad. **Nota:** El Switching de Grupo de Túnel se habilita mediante el procesamiento de Grupo de Tiras, que permite que el dispositivo de seguridad seleccione el grupo de túnel para las conexiones de usuario al obtener el nombre de grupo del nombre de usuario presentado por el Cliente VPN. El dispositivo de seguridad entonces envía solamente la parte usuario del nombre de usuario para la autorización y la autenticación. De lo contrario (si está inhabilitado), el dispositivo de seguridad envía el nombre de usuario entero, incluido el dominio. Para habilitar el Switching de Grupo de Túnel, verifique **Quitar dominio del nombre de usuario antes de transferirlo al servidor de AAA**, y verifique **Quitar el grupo del nombre de usuario antes de transferirlo al servidor de AAA**. Luego haga clic en OK (Aceptar).

11. Termina estos pasos para crear a un usuario en las bases de datos locales: Elija **Configuration > Properties > Device Administration > User Accounts**. Haga clic en Add (Agregar). Si el usuario es un cliente L2TP que utiliza la Microsoft CHAP versión 1 o 2, y el

dispositivo de seguridad se configura para autenticar contra las bases de datos locales, debe marcar al **usuario autenticado usando el MSCHAP** para habilitar el MSCHAP. Click OK.



Add User Account

Identity | VPN Policy

Username: test

Password: ****

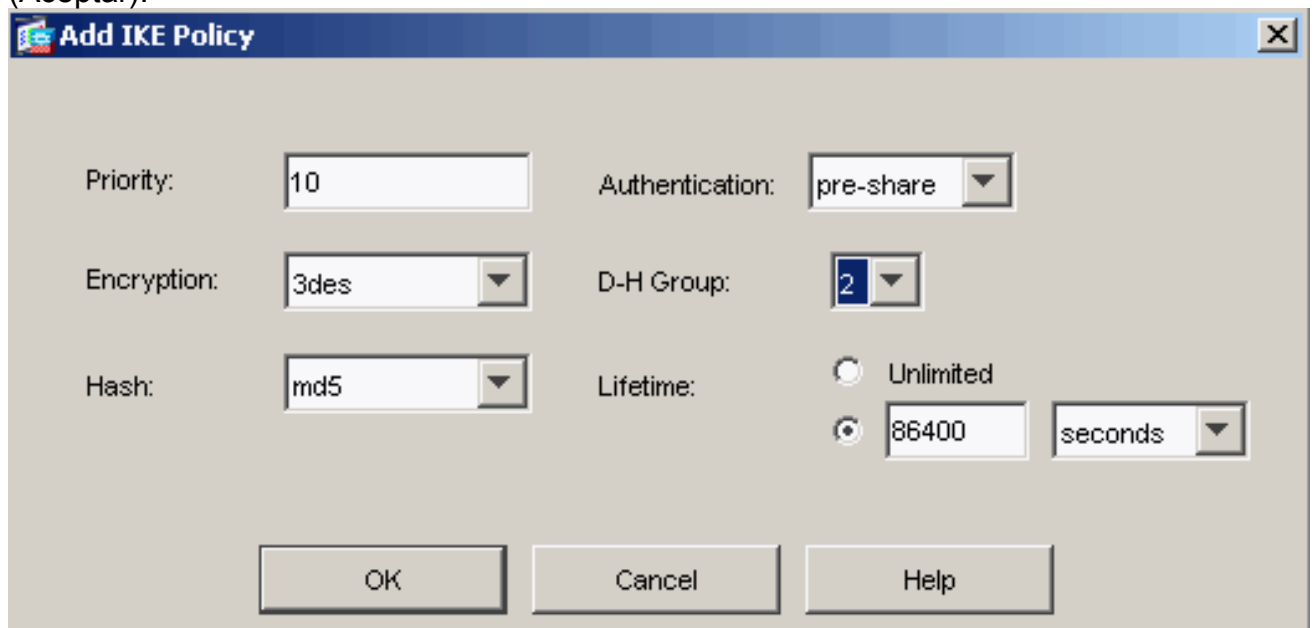
Confirm Password: ****

User authenticated using MSCHAP

Privilege level is used with command authorization.

Privilege Level: 2

12. Elija **Configuration > VPN > IKE > Políticas** y haga clic en **Add** para crear una política IKE para la Fase I. Para continuar, haga clic en OK (Aceptar).



Add IKE Policy

Priority: 10

Authentication: pre-share

Encryption: 3des

D-H Group: 2

Hash: md5

Lifetime: Unlimited 86400 seconds

OK Cancel Help

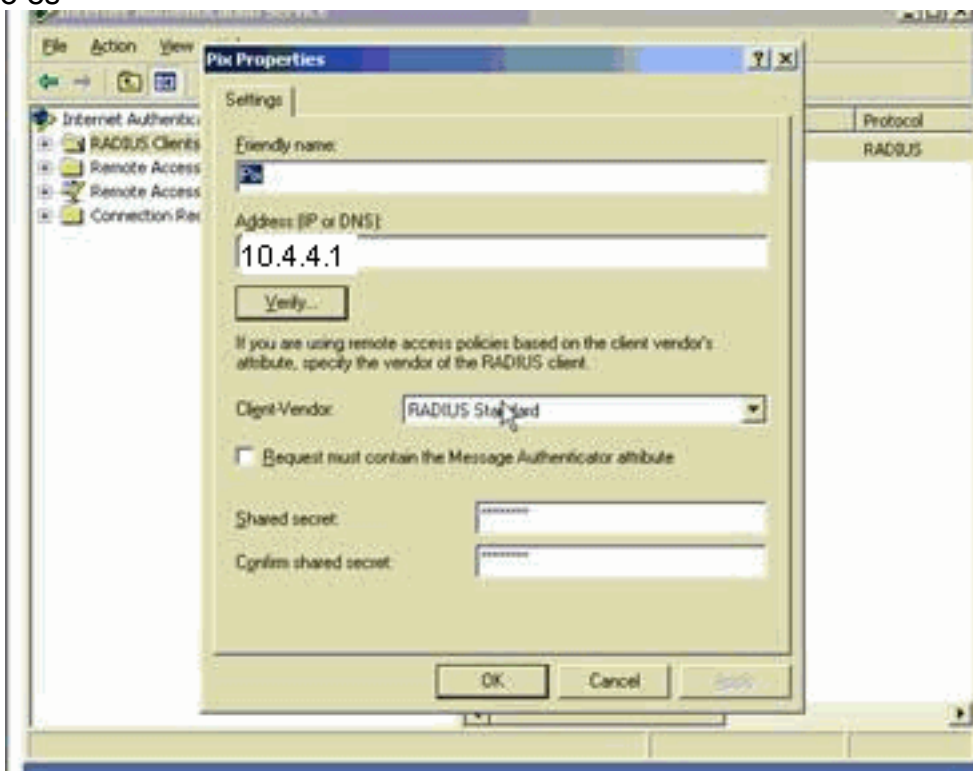
13. (Opcional) Si desea que los clientes múltiples L2TP detrás de un dispositivo NAT intenten el L2TP a través de conexiones del IPsec al dispositivo de seguridad, debe habilitar el NAT pasajero de modo que los paquetes ESP puedan pasar a través de uno o más dispositivos NAT. Para hacerlo, complete estos pasos: Elija **Configuration > VPN > IKE > Global Parameters**. Asegúrese de que el **ISAKMP** esté habilitado en una interfaz. Verifique **Habilitar IPsec a través NAT-T**. Click OK.

[Servidor de Microsoft Windows 2003 con Configuración IAS](#)

Complete estos pasos para configurar el servidor de Microsoft Windows 2003 con IAS.

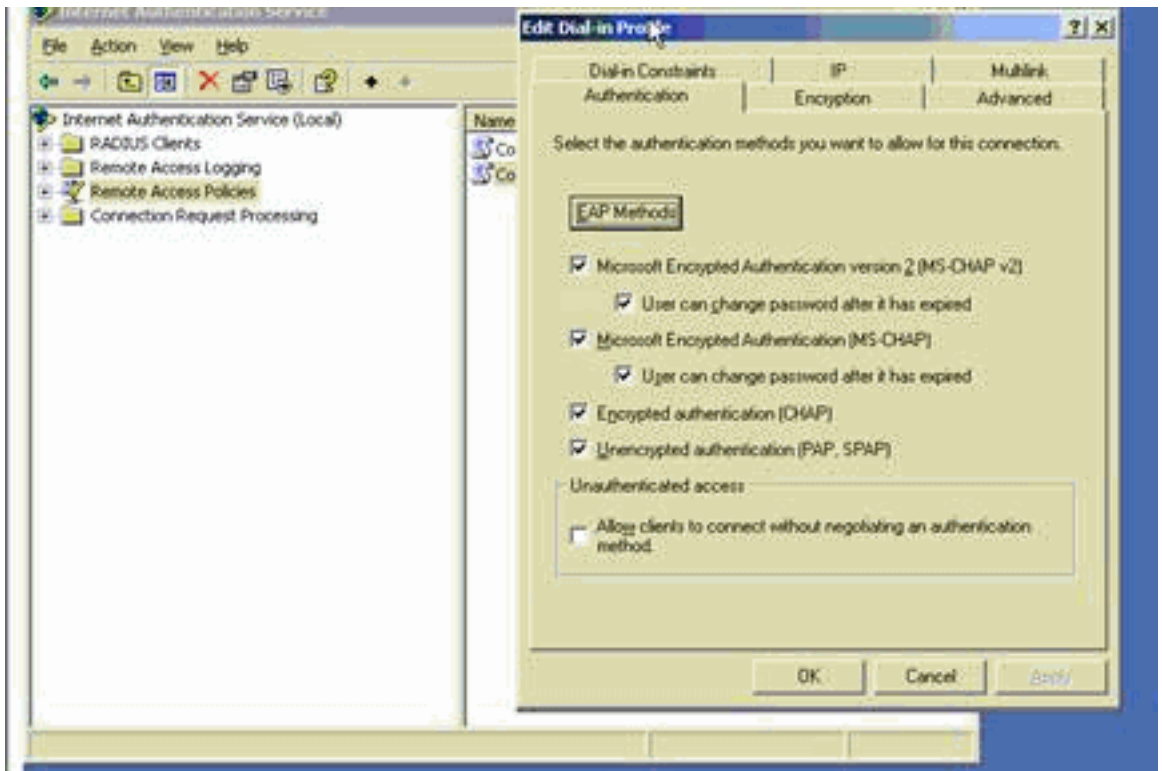
Nota: Estos pasos suponen que IAS ya está instalada en la máquina local. De lo contrario, agregue el IAS a través del **Control Panel > Add/Remove Programs**.

1. Elija **Administrative Tools > Internet Authentication Service** y haga clic con el botón derecho en **RADIUS Client** para agregar un nuevo cliente **RADIUS**. Luego de escribir la información del cliente, haga clic en **OK**. Este ejemplo muestra un cliente denominado "Pix" con una dirección IP de 10.4.4.1. Client-Vendor se ha configurado en **RADIUS Standar**, y el secreto compartido es



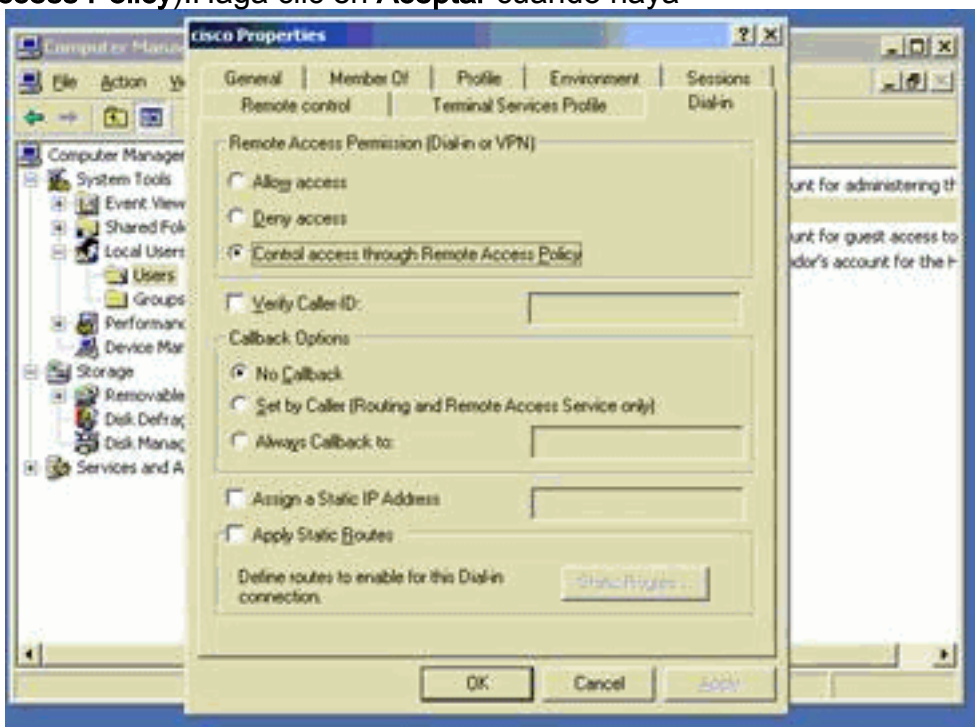
radiuskey.

2. Elija **Remote Access Policies**, haga clic con el botón derecho del mouse en **Connections to Other Access Servers**, y seleccione **Properties**.
3. Asegúrese de que la opción **Grant Remote Access Permissions** esté seleccionada.
4. Haga clic en **Edit Profile** y marque estas configuraciones: En la pestaña **Authentication**, marque **Unencrypted authentication (PAP, SPAP)**. En la pestaña **Encryption**, asegúrese de que esté seleccionada la opción **No Encryption**. Haga clic en **Aceptar** cuando haya



terminado.

5. Elija **Administrative Tools > Computer Management > System Tools > Local Users and Groups**, haga clic con el botón derecho en **Usuarios** y seleccione **Nuevos Usuarios para agregar un usuario en la cuenta computadora local**.
6. Agregue un usuario con la contraseña de Cisco **password1** y marque esta información del perfil: En la pestaña **General**, asegúrese de que esté seleccionada la opción **Password Never Expired** en vez de la opción **User Must Change Password**. En la pestaña **Dial-in**, seleccione la opción **Allow access** (o deje la configuración predeterminada **Control access through Remote Access Policy**). Haga clic en **Aceptar** cuando haya



terminado.

[Autenticación ampliada para L2TP sobre IPsec mediante Active Directory](#)

Utilice esta configuración en el ASA para permitir que la autenticación para la conexión L2tp tenga lugar desde el Active Directory:

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

Además, en el cliente L2tp, vaya a **Advanced Security Settings (Custom)** y elija solamente la opción para **Unencryption password (PAP)**.

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta [Output Interpreter](#) (sólo para clientes [registrados](#)) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **show crypto ipsec sa** — Muestra todas las asociaciones de seguridad IKE (SAs) actuales en un par.

```
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
```

- **show crypto isakmp sa** — Muestra todas las IKE SAs actuales en un par.

```
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
```

- **show vpn-sessiondb** — Incluye filtros de protocolo que puede usar para ver información detallada acerca L2TP a través de las conexiones IPsec. El comando completo del modo de configuración global es el protocolo de filtro remoto detallado **show vpn-sessiondb l2tpoveripsec**. Este ejemplo muestra los detalles de un solo L2TP a través de una conexión IPsec:

```
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

Troubleshoot

Esta sección proporciona la información para resolver problemas en su configuración. También se muestra un ejemplo de salida del debug .

Comandos para resolución de problemas

Ciertos comandos son soportados por la [herramienta Output Interpreter Tool \(clientes registrados solamente\)](#), que le permite ver un análisis de la salida del comando `show`.

Nota: Refiérase a [Información Importante sobre Comandos Debug y Resolución de Problemas de Seguridad IP - Comprensión y Uso de Comandos debug](#) antes de utilizar los comandos `debug`.

- `debug crypto ipsec 7` — Muestra negociaciones IPsec de la Fase 2.
- `debug crypto isakmp 7` — Muestra negociaciones ISAKMP de la Fase 1.

Ejemplo de resultado del comando debug

Firewall PIX

```
PIX#debug crypto isakmp 7
pixfirewall# Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (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 VID
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 payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing xauth V6 VID payload
```

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 Vendor 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 DefaultRAGroup
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generating 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, processing ID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computing hash for ISAKMP
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group DefaultRAGroup
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Freeing previously allocated memory for authorization-dn-attributes
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing ID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computing hash for ISAKMP
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing 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 successfully. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, **PHASE 1 COMPLETED**
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 does not support keep-alives (type = None)
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Starting P1 rekey timer: 21600 seconds.
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1b84b0) 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, processing hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing ID payload
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received remote 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, processing ID payload
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received local 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 session 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 Peer configured for crypto map: outside_dyn_map

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing IPsec SA payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IPsec SA 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: requesting 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**

constructing quick mode

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing blank hash payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing IPsec SA payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing IPsec nonce payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing proxy ID

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Transmitting 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, constructing qm hash payload

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=e1b84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 144

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1b84b0) with payloads : HDR + HASH (8) + NONE (0) total length : 48

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing 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, Generating Quick Mode Key!

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generating Quick Mode Key!

Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Security negotiation 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, Starting P2 rekey timer: 3059 seconds.

!--- Phase 2 completes successfully. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, PHASE 2 COMPLETED (msgid=0e1b84b0) Jan 02 18:26:44 [IKEv1]: IKEQM_Active() Add L2TP classification rules: ip <192.168.0.2> 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
```

[Troubleshooting con ASDM](#)

Usted puede utilizar el ASDM para habilitar la registraci3n y ver los registros.

1. Elija **Configuration > Properties > Logging > Logging Setup**, select **Enable Logging** y haga clic en **Aplicar** para habilitar el registro.
2. Elija **Monitoring > Logging > Log Buffer > On Logging Level**, seleccione **B3fer de Registro**, y haga clic en **Ver** para ver los registros.

[Problema: Desconexiones frecuentes](#)

Tiempo de espera de sesi3n/inactividad

Si el tiempo de espera inactivo se establece en 30 minutos (predeterminado), significa que descarta el t3nel despu3s de que no pase tr3fico por 3l durante 30 minutos. El cliente VPN se desconecta despu3s de 30 minutos independientemente de la configuraci3n del tiempo de espera inactivo y encuentra el mensaje de error `PEER_DELETE-IKE_DELETE_UNSPECIFIED`.

Configure idle timeout y session timeout como none para que el t3nel est3 siempre activop y nunca se caiga.

Ingrese el comando `vpn-idle-timeout` en el modo de configuraci3n de pol3tica de grupo o en el

modo de configuración de nombre de usuario para configurar el período de tiempo de espera del usuario:

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

Configure una cantidad máxima de tiempo para las conexiones VPN con el comando **vpn-session-timeout** en el modo de configuración de política de grupo o en el modo de configuración de nombre de usuario:

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

[Troubleshooting Windows Vista](#)

Usuario simultáneo

Windows Vista L2TP/IPsec introdujo algunos cambios de la arquitectura que prohibieron a más de un usuario simultáneo de la conexión con un PIX/ASA del centro distribuidor. Este comportamiento no ocurre en Windows 2K/XP. Cisco ha implementado una solución alternativa para este cambio a partir de la versión 7.2(3) y superior.

No se Puede Conectar el Equipo Vista

Si el ordenador de Windows Vista no se puede conectar con el servidor L2TP, verifique que haya configurado SOLAMENTE mschap-v2 bajo PPP-atributo en el DefaultRAGroup.

[Información Relacionada](#)

- [Soluciones a los Problemas más frecuentes de IPsec VPN L2L y de Acceso Remoto](#)
- [Dispositivos de seguridad Cisco PIX de la serie 500](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Soporte de Productos del Software Cisco PIX Firewall](#)
- [Referencias de Comandos de Cisco Secure PIX Firewall](#)
- [Página de soporte de RADIUS](#)
- [Página de Soporte de IPsec Negotiation/IKE Protocols](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Layer Two Tunnel Protocol \(L2TP\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)