PIX/ASA y cliente VPN para el Internet pública VPN en un ejemplo de configuración del palillo

Contenido

Introducción

Este documento describe cómo configurar un dispositivo de seguridad 7.2 ASA y posterior para realizar el IPSec en un palillo. Esta configuración se aplica a un caso específico, cuando ASA no permite la tunelización dividida y los usuarios se conectan directamente al ASA antes de que se les permita entrar a Internet.

Nota: En la versión 7.2 y posterior del PIX/ASA, la palabra clave de la intra-*interfaz* permite que todo el tráfico ingrese y salga la misma interfaz, y no apenas el tráfico IPSec.

Refiera al router y al cliente VPN para el Internet pública en un ejemplo de configuración del palillo para completar una configuración similar en un router del sitio central.

Refiera al Spoke-a-cliente aumentado 7.x VPN del PIX/ASA con autenticación de TACACS+ el ejemplo de configuración para aprender más sobre el escenario donde el eje de conexión PIX reorienta el tráfico del cliente VPN al spoke PIX.

Nota: Para evitar una coincidencia de los IP Addresses en la red, asigne un pool totalmente diverso de los IP Addresses al cliente VPN (por ejemplo, 10.x.x.x, 172.16.x.x, y 192.168.x.x). Este esquema de IP Addressing es útil para resolver problemas su red.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- El dispositivo de seguridad del PIX/ASA del concentrador necesita funcionar con la versión 7.2 o posterior
- Cliente VPN de Cisco versión 5.x

Componentes Utilizados

La información en este documento se basa en versión 8.0.2 y Cliente VPN de Cisco versión 5.0 del dispositivo de seguridad PIX o ASA.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Esta configuración se puede también utilizar con la versión 7.2 y posterior del dispositivo de seguridad del Cisco PIX.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Hairpinning o giro de 180 grados

Esta característica es útil para el tráfico VPN que ingrese una interfaz pero después se rutea fuera de esa misma interfaz. Por ejemplo, si usted tiene una red VPN del hub-and-spoke, donde está el concentrador el dispositivo de seguridad, y las redes VPN remotas es spokes, para que uno habló para comunicar con otro spoke, trafica debe salir en el dispositivo de seguridad y entonces otra vez al otro spoke.

Utilice el **comando same-security-traffic** de permitir que el tráfico ingrese y que salga la misma interfaz.

```
securityappliance(config)#same-security-traffic permit intra-interface
```

Nota: El hairpinning o el giro de 180 grados es aplicable para el cliente VPN a la comunicación del cliente VPN, también.

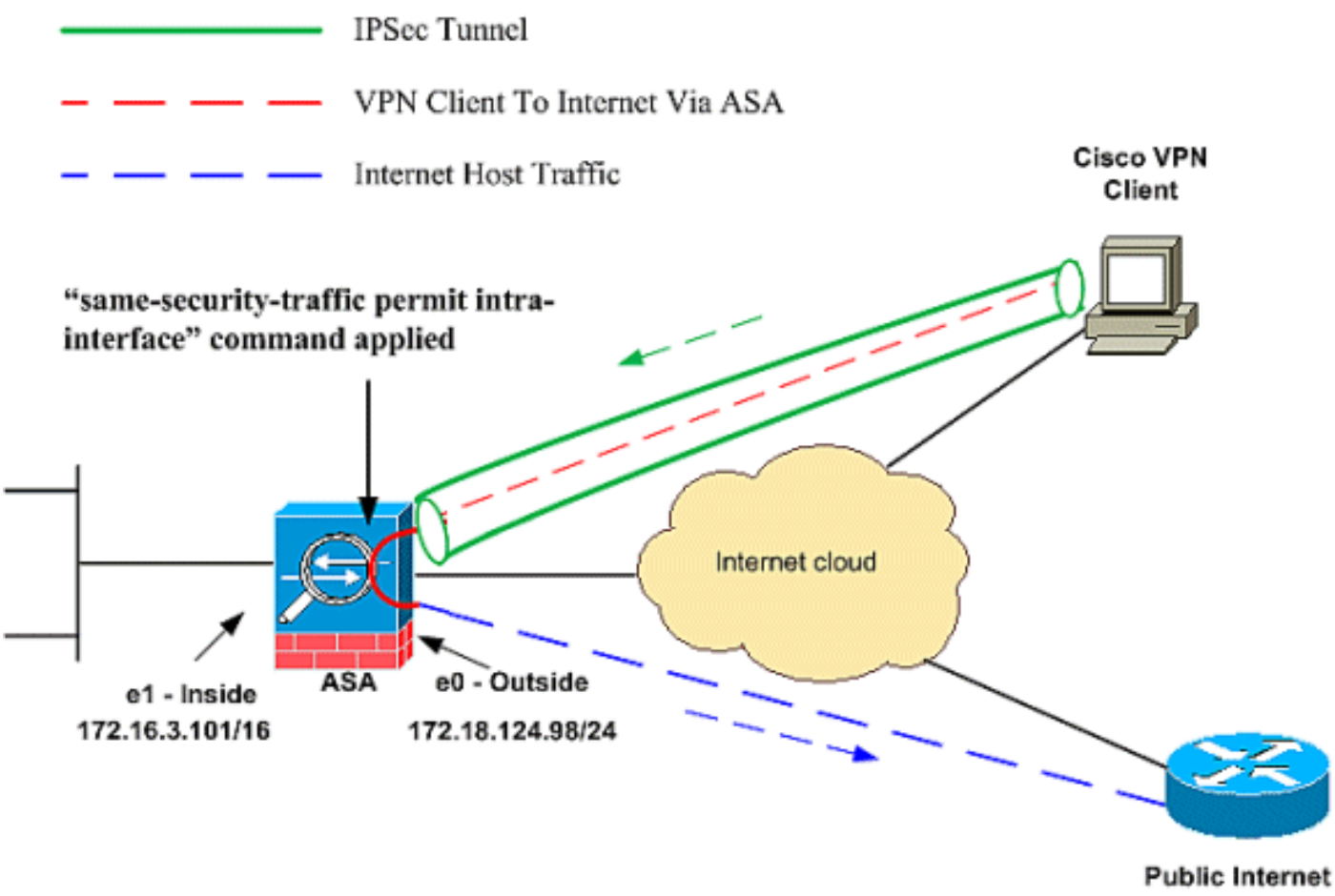
Configuraciones

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

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuración CLI del PIX/ASA

- PIX/ASA

Configuración de ejecución en el PIX/ASA
PIX Version 8.0(2) names ! interface Ethernet0 nameif outside security-level 0 ip address 172.18.124.98 255.255.255.0 ! interface Ethernet1

```
nameif inside
security-level 100
ip address 172.16.3.101 255.255.255.0
!
interface Ethernet2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet3
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet5
shutdown
no nameif
no security-level
no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
ftp mode passive
!--- Command that permits IPsec traffic to enter and
exit the same interface. same-security-traffic permit
intra-interface
access-list 100 extended permit icmp any any echo-reply
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500

ip local pool vpnpool
   192.168.10.1-192.168.10.254 mask 255.255.255.0

no failover
monitor-interface outside
monitor-interface inside
icmp permit any outside
no asdm history enable
arp timeout 14400
nat-control!--- The address pool for the VPN Clients. !-
-- The global address for Internet access used by VPN
Clients. !--- Note: Uses an RFC 1918 range for lab
setup. !--- Apply an address from your public range
provided by your ISP.

global (outside) 1 172.18.124.166

!--- The NAT statement to define what to encrypt (the
addresses from the vpn-pool). nat (outside) 1
192.168.10.0 255.255.255.0

nat (inside) 1 0.0.0.0 0.0.0.0
```

```
static (inside,outside) 172.16.3.102 172.16.3.102
   netmask 255.255.255.255
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.18.124.98 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
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute

!--- The configuration of group-policy for VPN Clients.
group-policy clientgroup internal
group-policy clientgroup attributes
vpn-idle-timeout 20

!--- Forces VPN Clients over the tunnel for Internet
access. split-tunnel-policy tunnelall


no snmp-server location
no snmp-server contact
snmp-server enable traps snmp

!--- Configuration of IPsec Phase 2. crypto ipsec
transform-set myset esp-3des esp-sha-hmac

!--- Crypto map configuration for VPN Clients that
connect to this PIX. crypto dynamic-map rtpdynmap 20 set
transform-set myset

!--- Binds the dynamic map to the crypto map process.
crypto map mymap 20 ipsec-isakmp dynamic rtpdynmap

!--- Crypto map applied to the outside interface. crypto
map mymap interface outside

!--- Enable ISAKMP on the outside interface. isakmp
identity address
isakmp enable outside

!--- Configuration of ISAKMP policy. isakmp policy 10
authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0

!--- Configuration of tunnel-group with group
information for VPN Clients. tunnel-group rtptacvpn type
ipsec-ra

!--- Configuration of group parameters for the VPN
Clients. tunnel-group rtptacvpn general-attributes
address-pool vpnpool
```

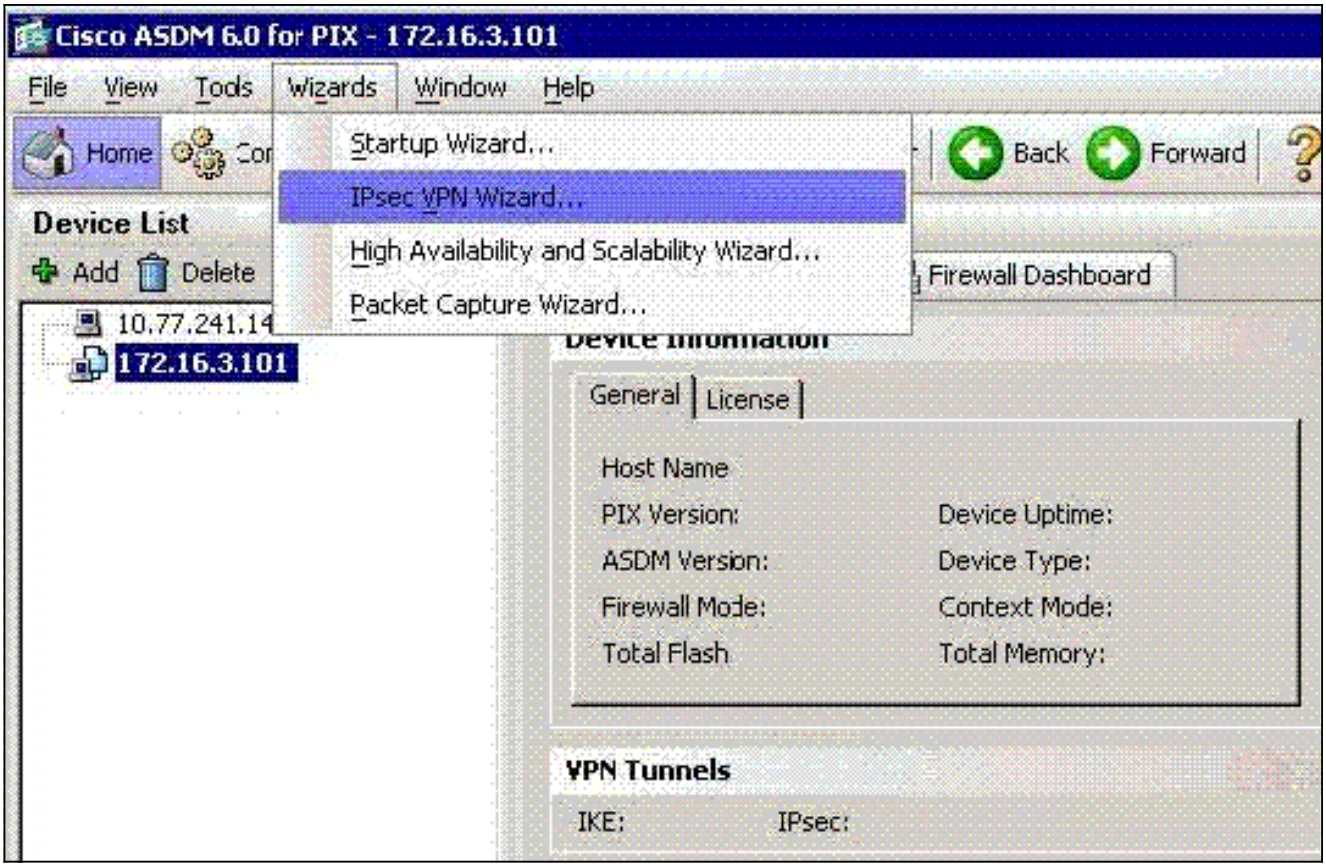
```
!--- Disable user authentication. authentication-server-
group none


!--- Bind group-policy parameters to the tunnel-group
for VPN Clients. default-group-policy clientgroup
tunnel-group rtptacvpn ipsec-attributes
pre-shared-key *
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
 inspect dns maximum-length 512
 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
Cryptochecksum:1a1ad58226e700404e1053159f0c5fb0
: end
```

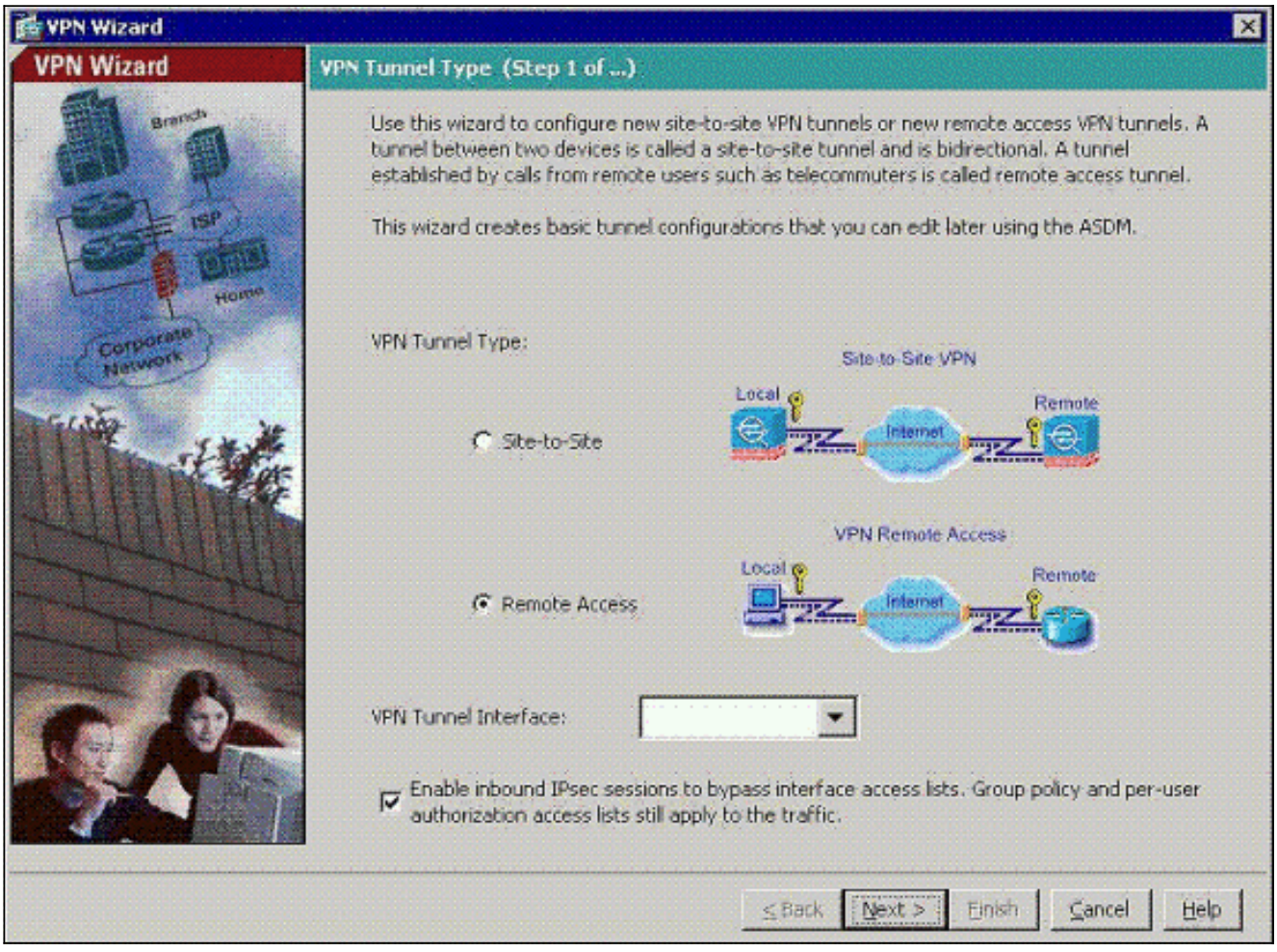
Configure ASA/PIX con el ASDM

Complete estos pasos para configurar Cisco ASA como servidor VPN remoto con el ASDM:

1. Elija los **Asisitente > al Asisitente del IPSec VPN de la** ventana casera.

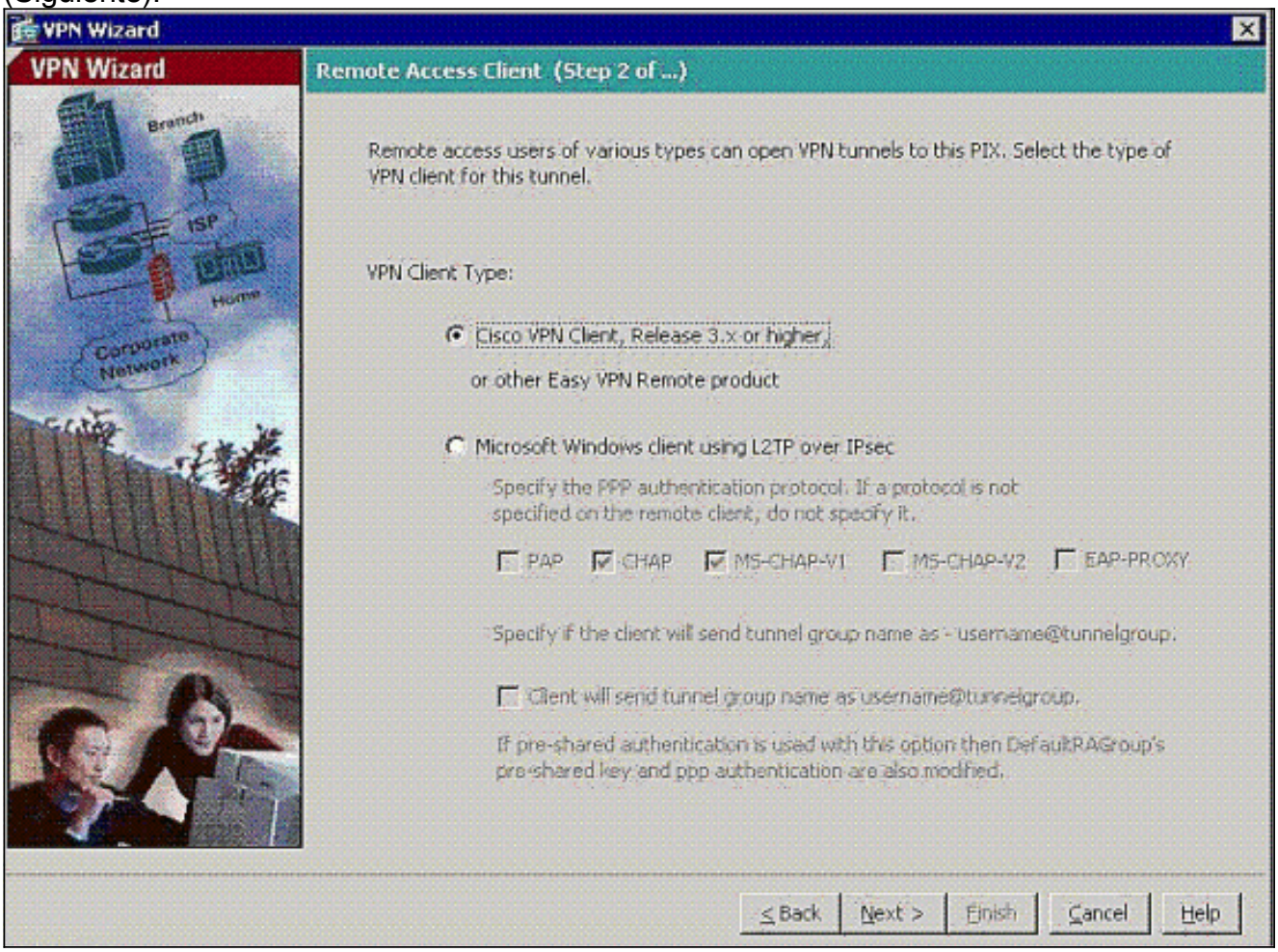


2. Elija el tipo de túnel del **VPN de acceso remoto**, y asegúrese de que la interfaz del túnel VPN está fijada según lo
deseado.

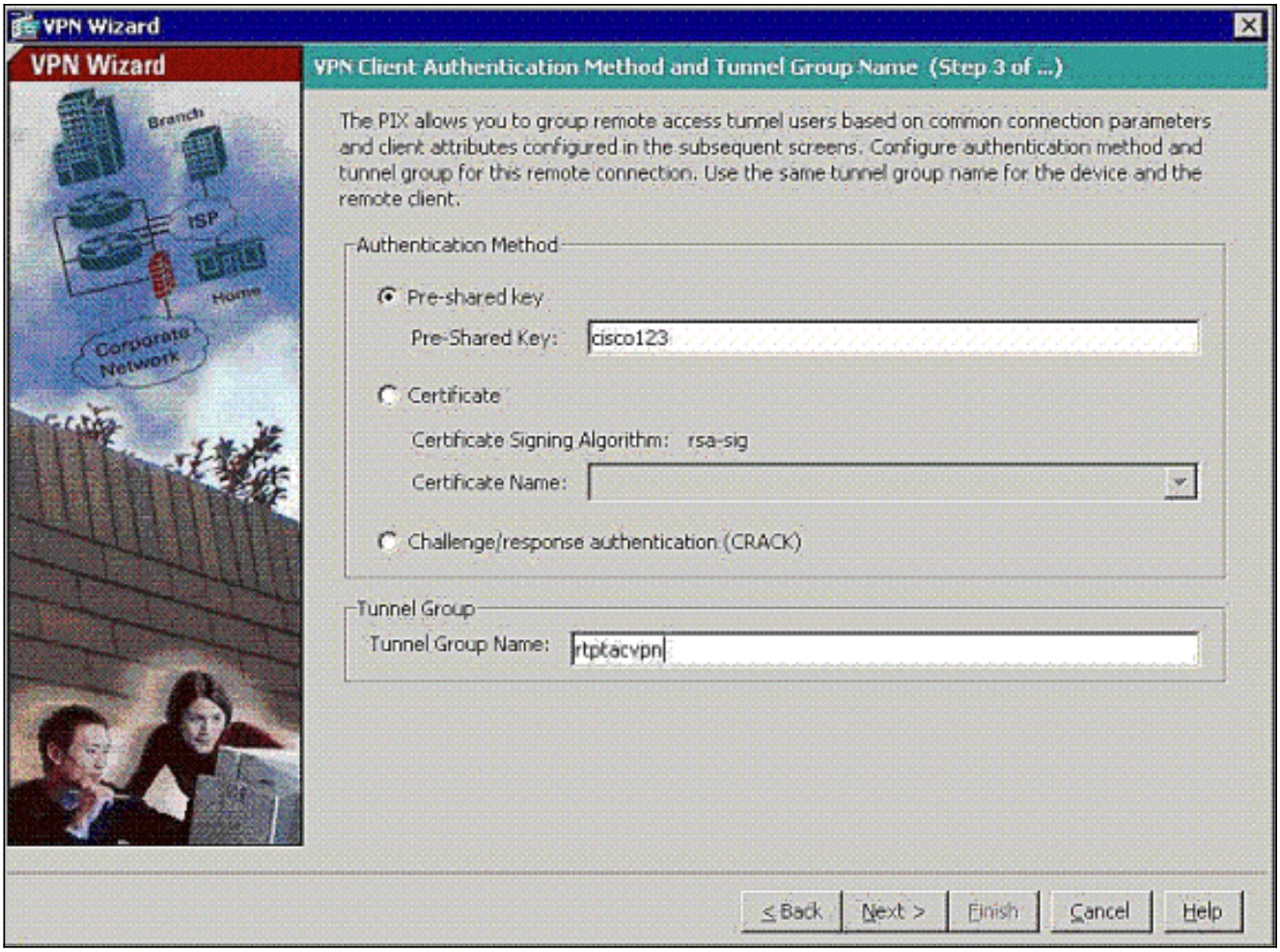


3. Eligen al único tipo del cliente VPN disponible ya. Haga clic en Next

(Siguiente).

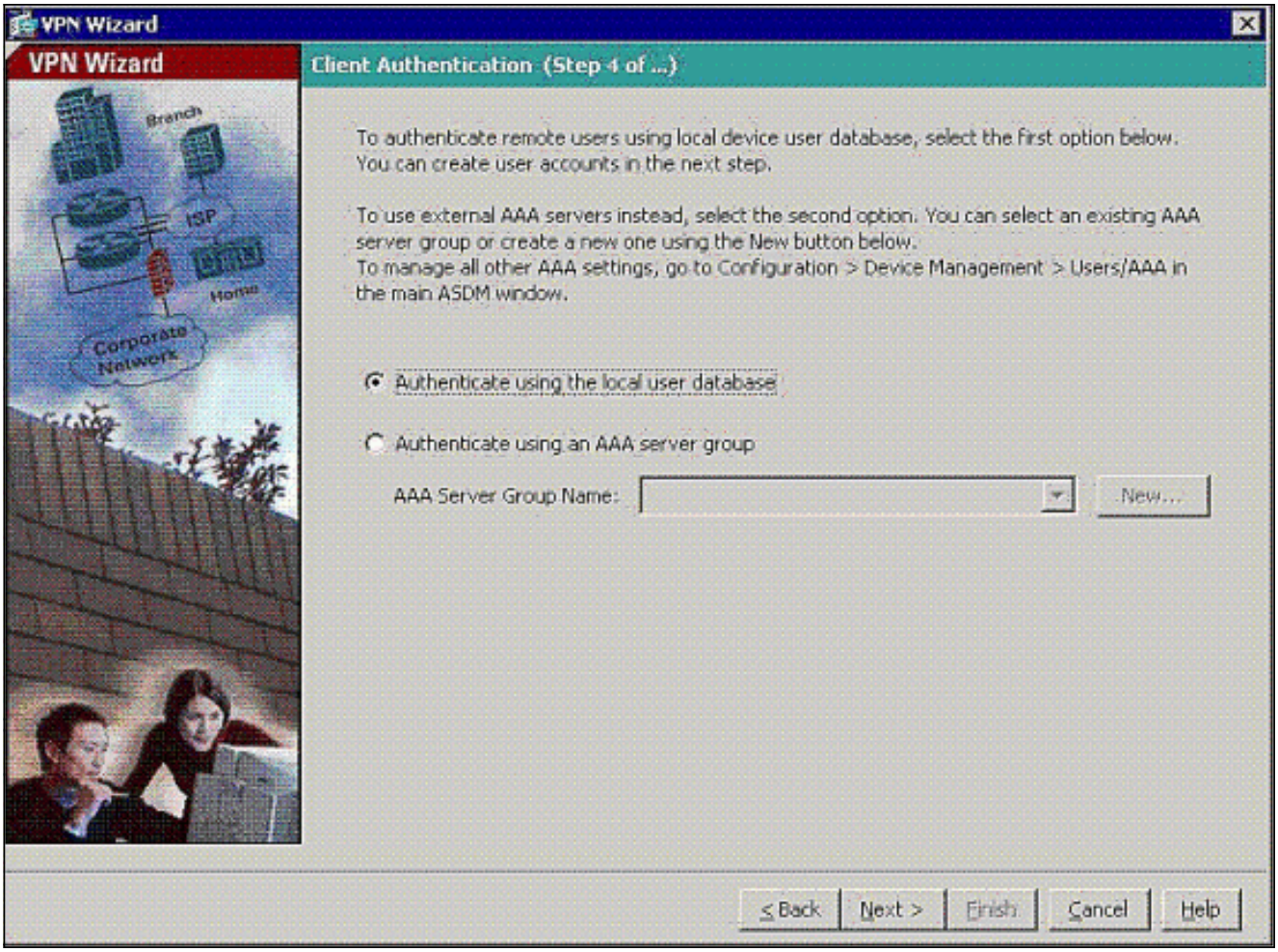


4. Ingrese un nombre para el Nombre de Grupo de Túnel. Suministre la información de autenticación que utilizará.**La clave previamente compartida** se elige en este ejemplo.

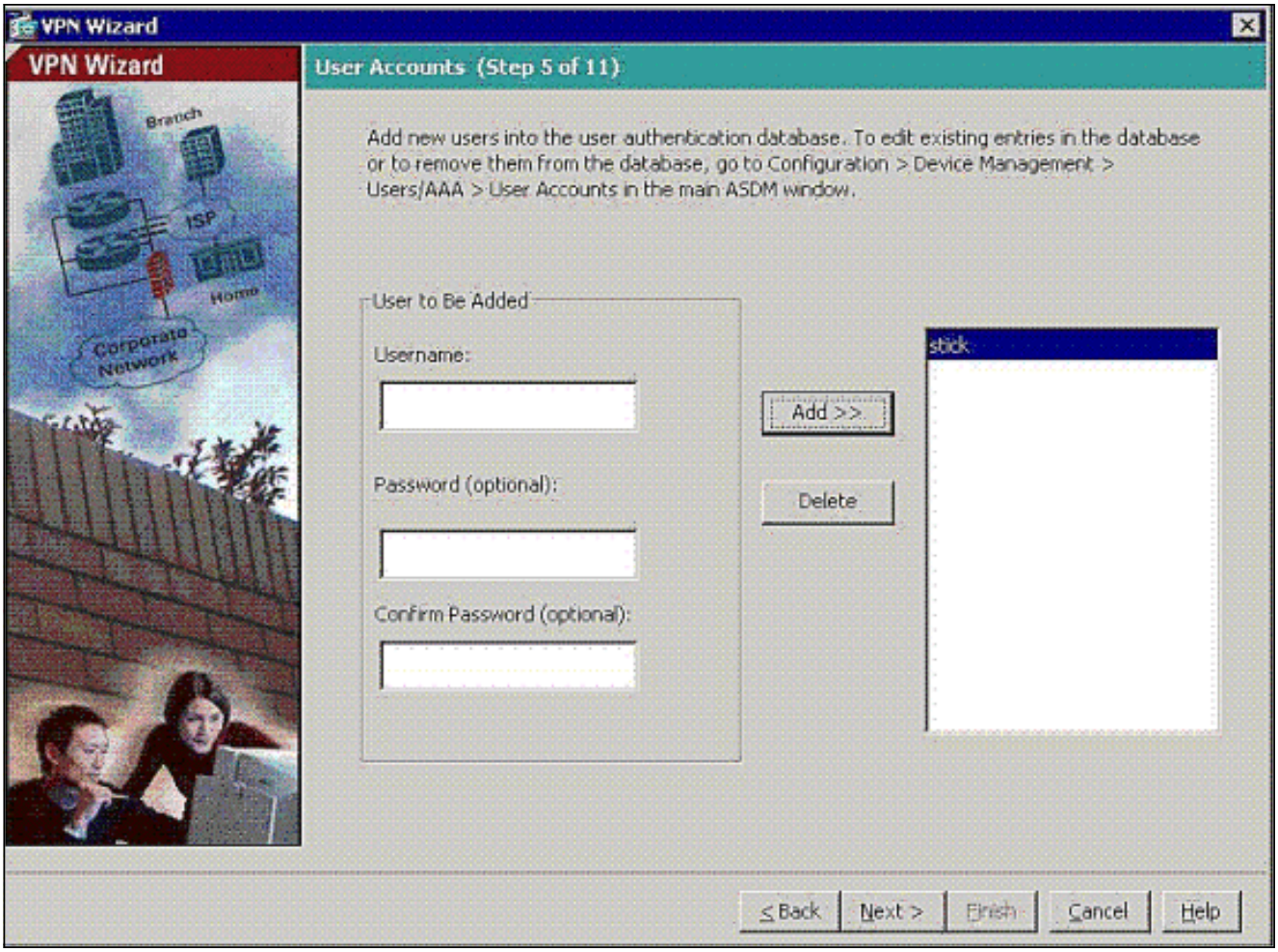


Nota: No hay una manera de ocultar/cifrar la clave previamente compartida en el ASDM. La razón es que el ASDM se debe utilizar solamente por la gente que configura el ASA o por la gente que ayuda al cliente con esta configuración.

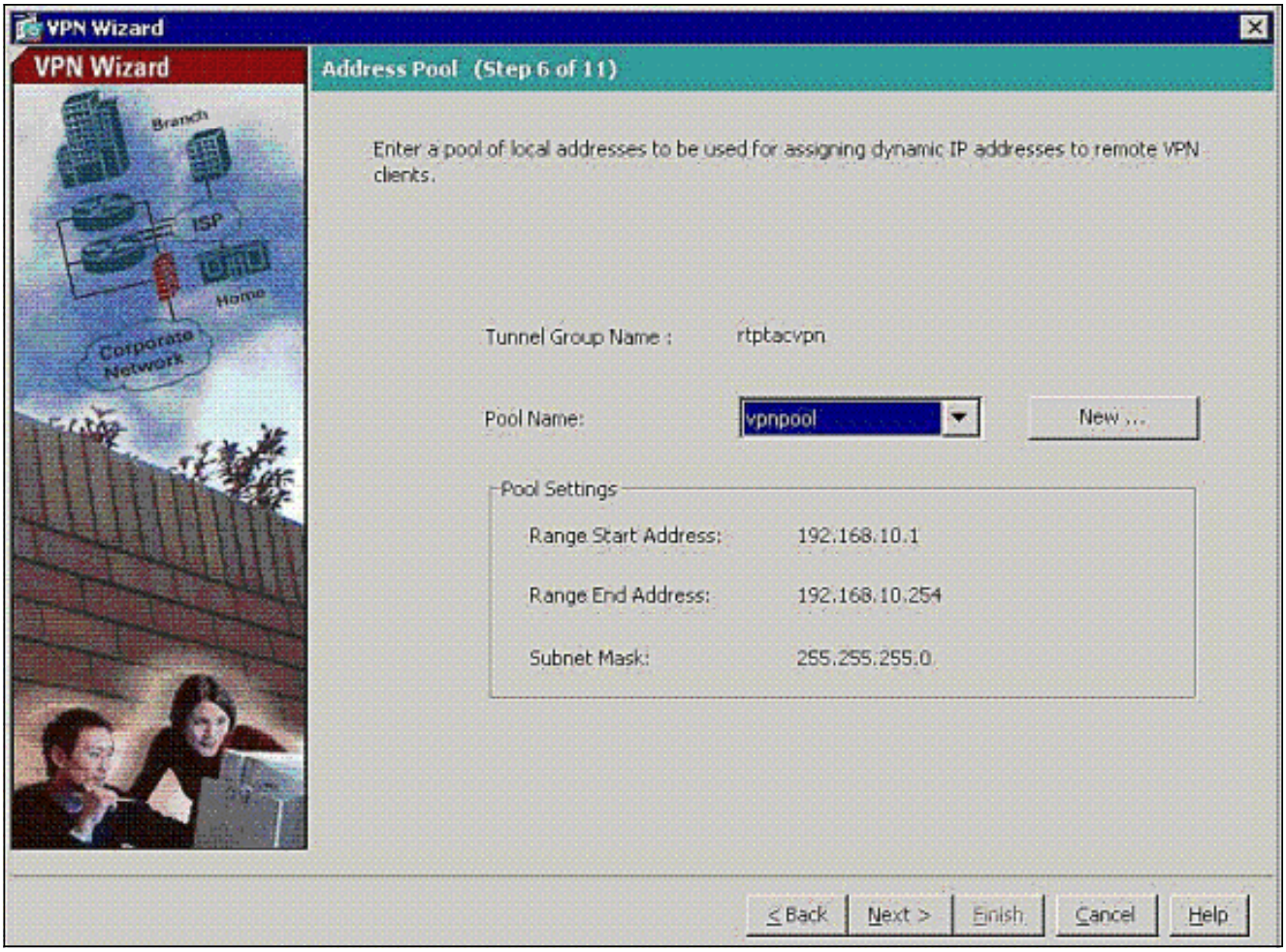
5. Elija si desea que los usuarios remotos sean autenticados en las bases de datos de usuarios locales o en un grupo de servidores AAA externo.**Nota:** Agrega a los usuarios a las bases de datos de usuarios locales en el paso 6.**Nota:** Refiera a los grupos de servidores de la autenticación y autorización del PIX/ASA 7.x para los usuarios de VPN vía el ejemplo de la Configuración de ASDM para la información sobre cómo configurar a un Grupo de servidores AAA externo con el
ASDM.



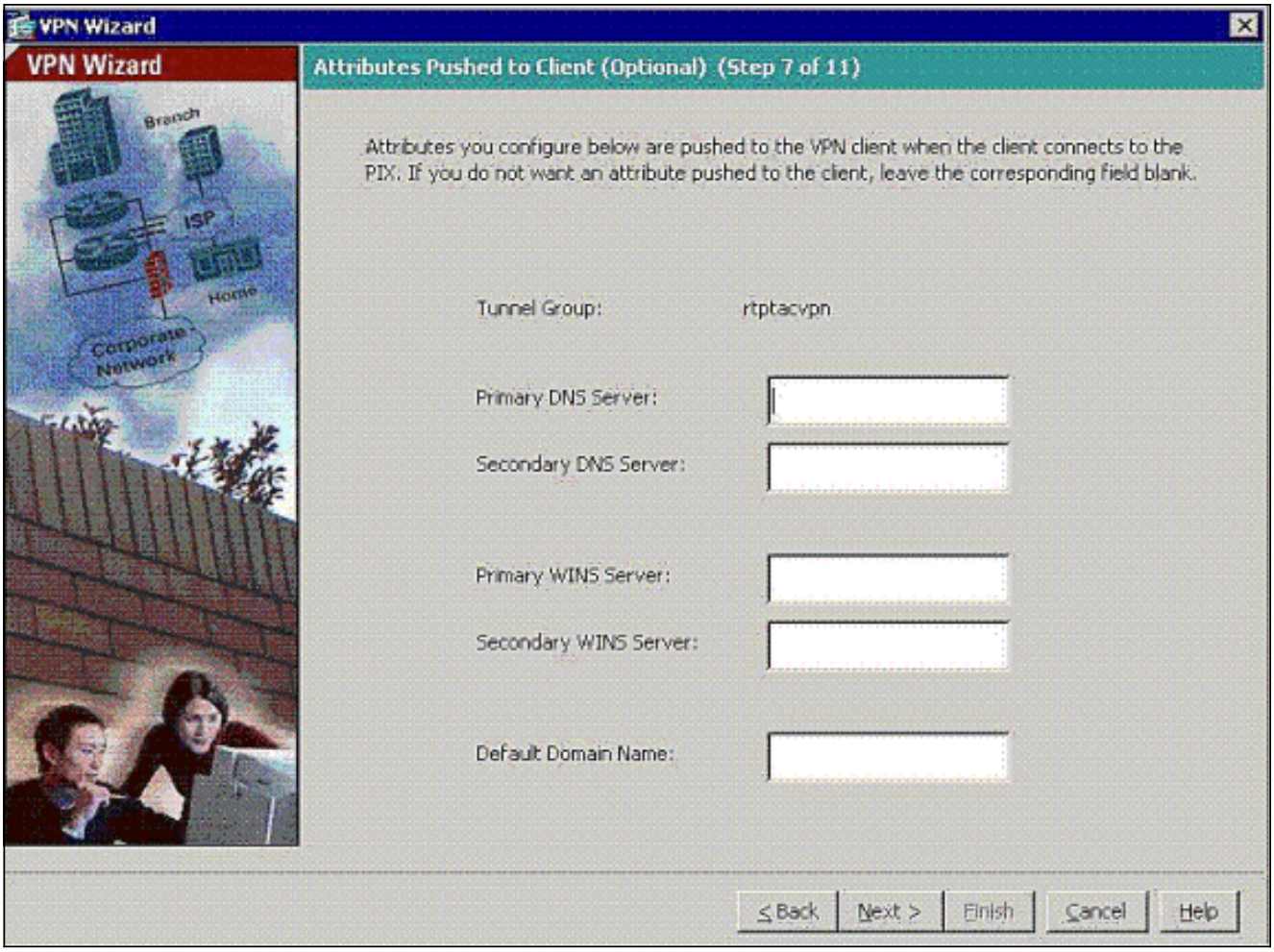
6. Agregue a los usuarios a la base de datos local, en caso necesario.**Nota:** No quite a los Usuarios usuarios actuales de esta ventana. Elija la **configuración > Device Administration (Administración del dispositivo) > la administración > las cuentas de usuario en la ventana ASDM principal** para editar las entradas existentes en la base de datos o para quitarlas de la base de
datos.



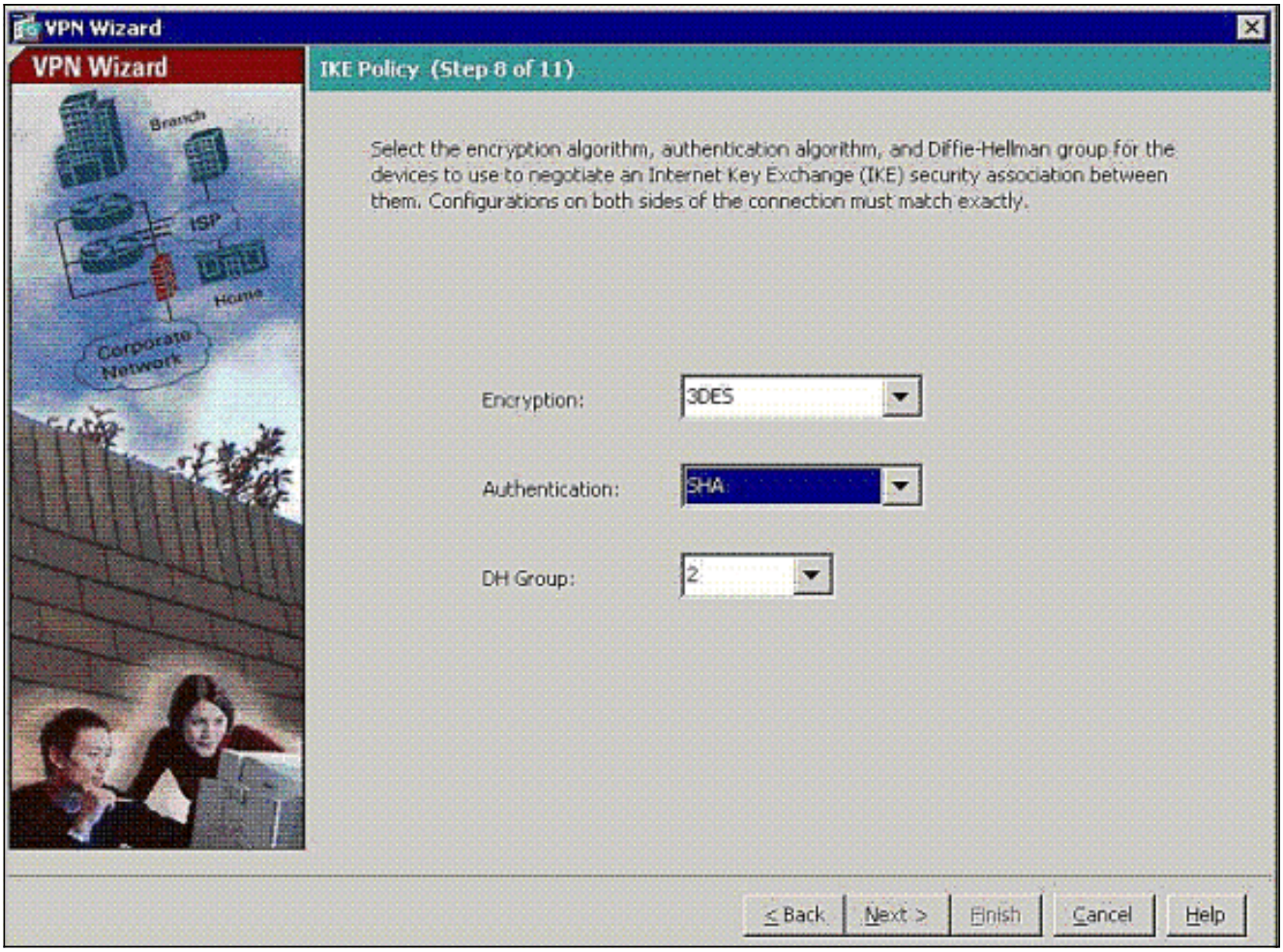
7. Defina un pool de las direcciones locales que se asignarán dinámicamente a los clientes de VPN remotos cuando se
conectan.



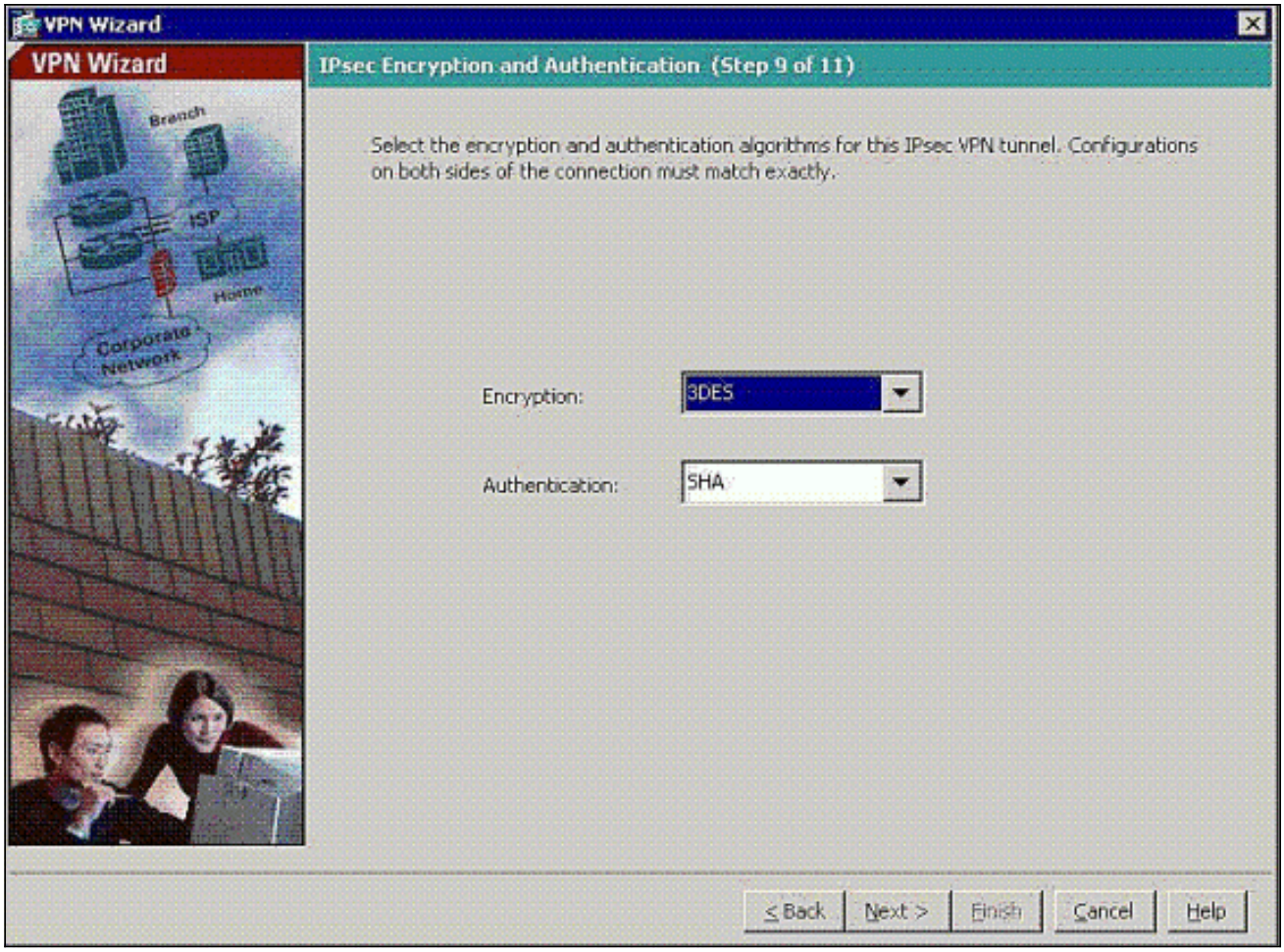
8. *Opcional:* Especifique la información de servidor DNS y WINS y un Nombre de Dominio Predeterminado que se avanzará a los clientes de VPN remotos.



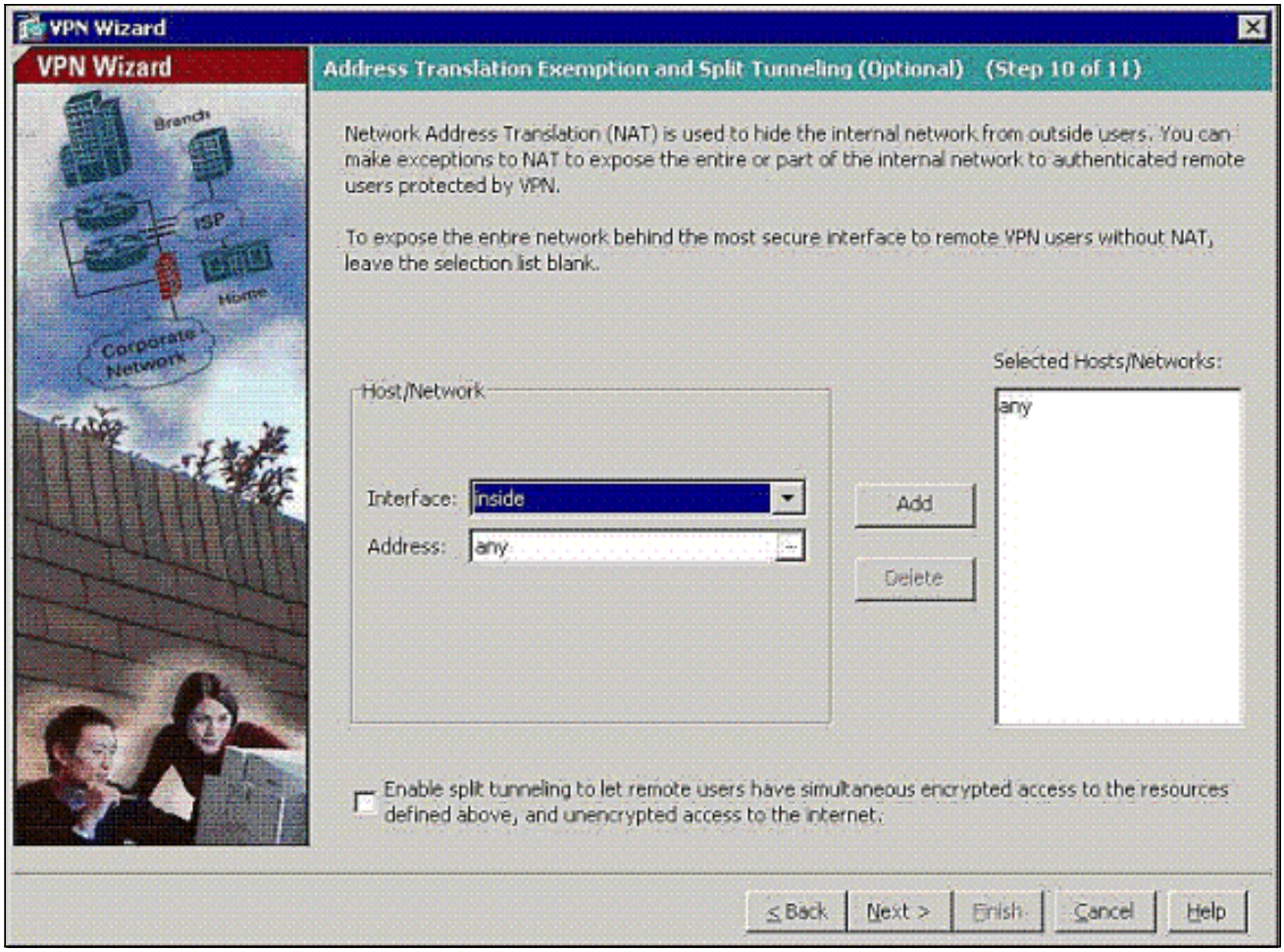
9. Especifique los parámetros para el IKE, también conocidos como fase 1. IKE.Las configuraciones a ambos lados del túnel deben hacer juego exactamente, pero el Cliente Cisco VPN elige automáticamente la configuración adecuada para sí mismo. No hay configuración IKE necesaria en PC del
cliente.



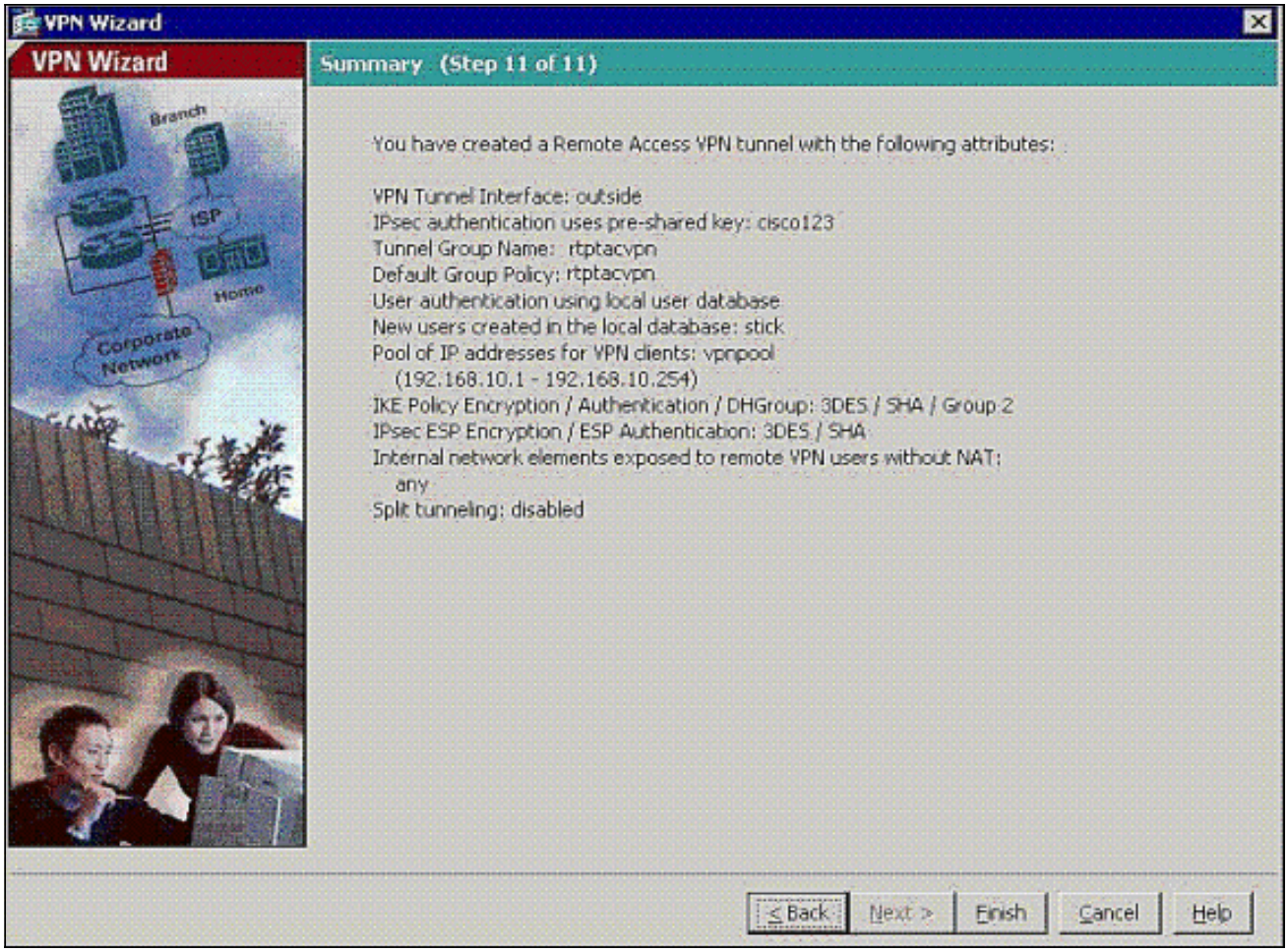
10. Especifique los parámetros para el IPSec, también conocidos como fase 2 IKE.Las configuraciones a ambos lados del túnel deben hacer juego exactamente, pero el Cliente Cisco VPN elige automáticamente la configuración adecuada para sí mismo. No hay configuración IKE necesaria en PC del
    cliente.



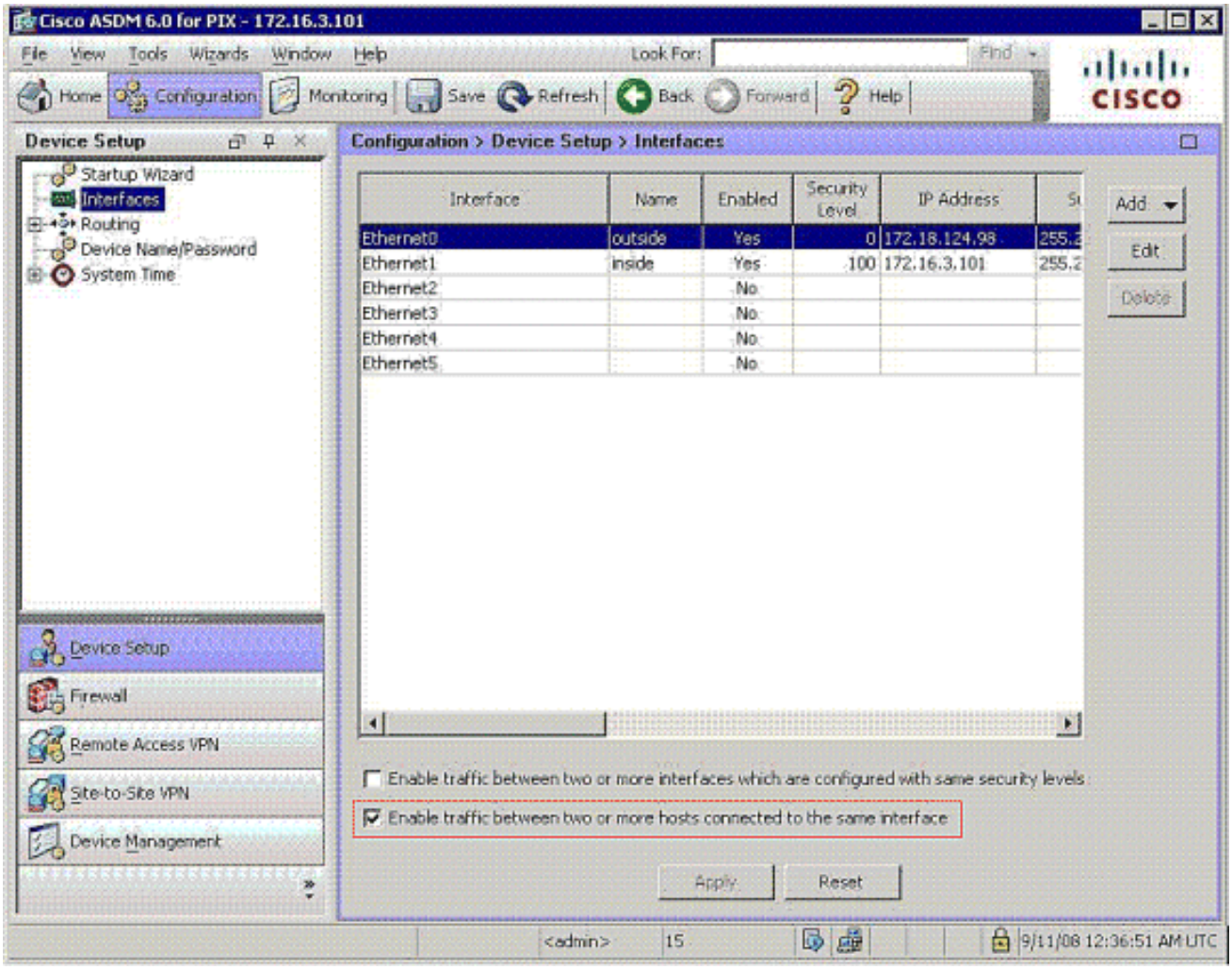
11. Especifique cuál, eventualmente, se pueden exponer los host internos o las redes a los usuarios de VPN remotos.Si deja esta lista vacía, permita que los usuarios de VPN remotos acceden a la red interna completa del ASA.Puede también habilitar la tunelización dividida en esta ventana. La tunelización dividida encripta el tráfico a los recursos definidos anteriormente en este procedimiento y proporciona el acceso no cifrado a Internet en general al no tunelizar ese tráfico. Si la tunelización dividida no se habilita, todo el tráfico de los usuarios de VPN remotos se tuneliza al ASA. Éste puede convertirse en un gran ancho de banda y hacer un uso intensivo del procesador, sobre la base de su configuración.



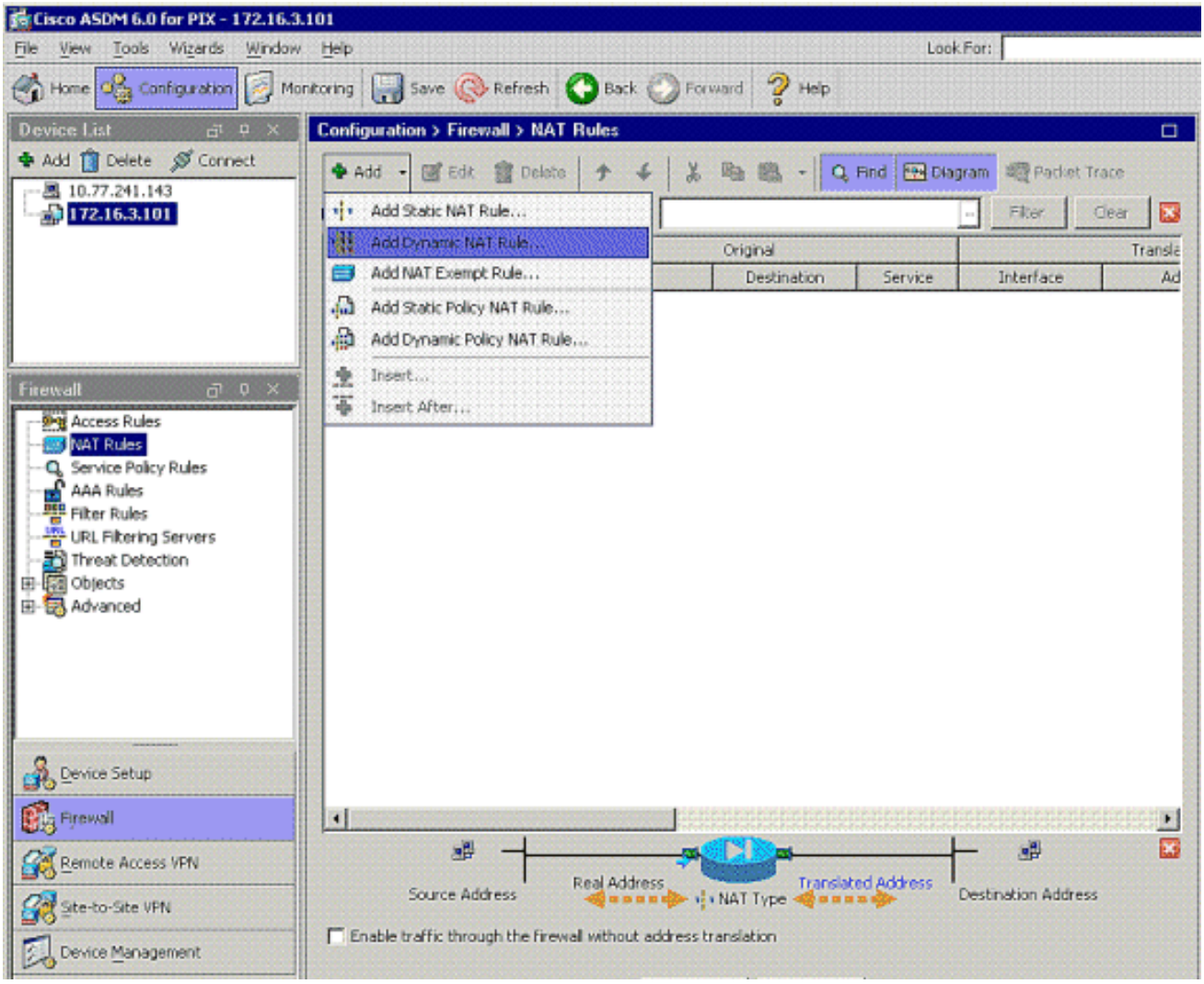
12. Esta ventana muestra un resumen de las acciones que ha realizado. Haga clic en **Finalizar** si está satisfecho con la configuración.



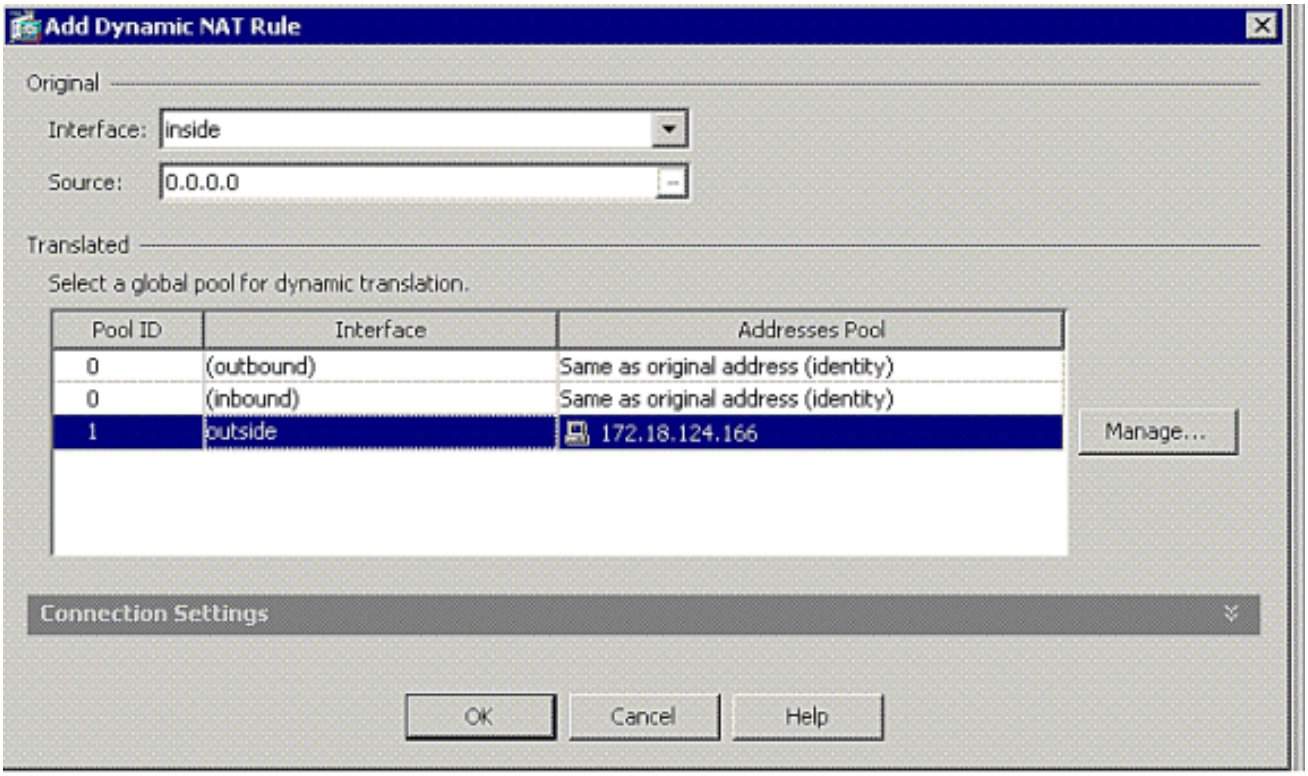
13. Configure el comando same-security-traffic de habilitar el tráfico entre dos o más host conectados con la misma interfaz cuando usted hace clic el checkbox como se muestra:



14. Elija las **reglas de la configuración > del Firewall >NAT**, y el tecleo **agrega la regla dinámica NAT** para crear esta traducción dinámica con el uso del ASDM.

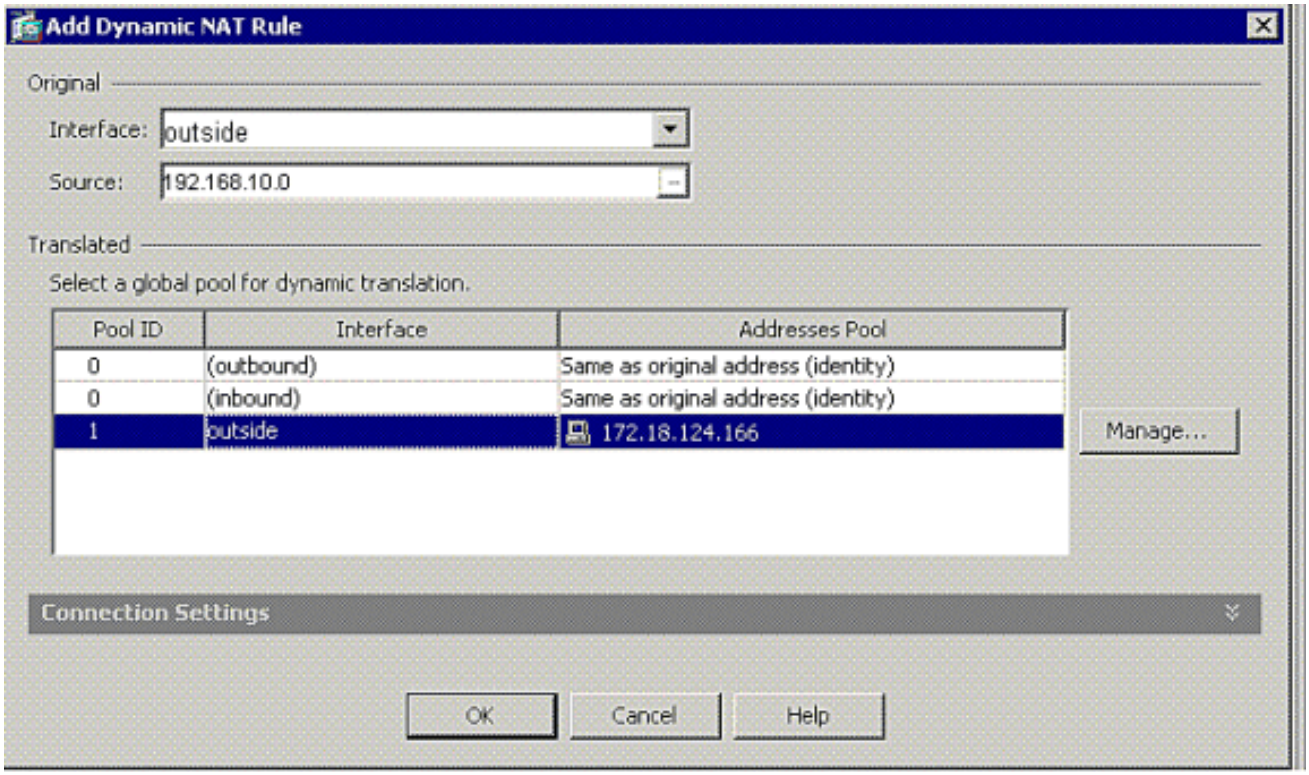


15. Elija el **interior** como la interfaz de origen, y ingrese los direccionamientos que usted quiere al NAT. Para el direccionamiento Translate en la interfaz, elija **afuera** y haga clic la **AUTORIZACIÓN**.

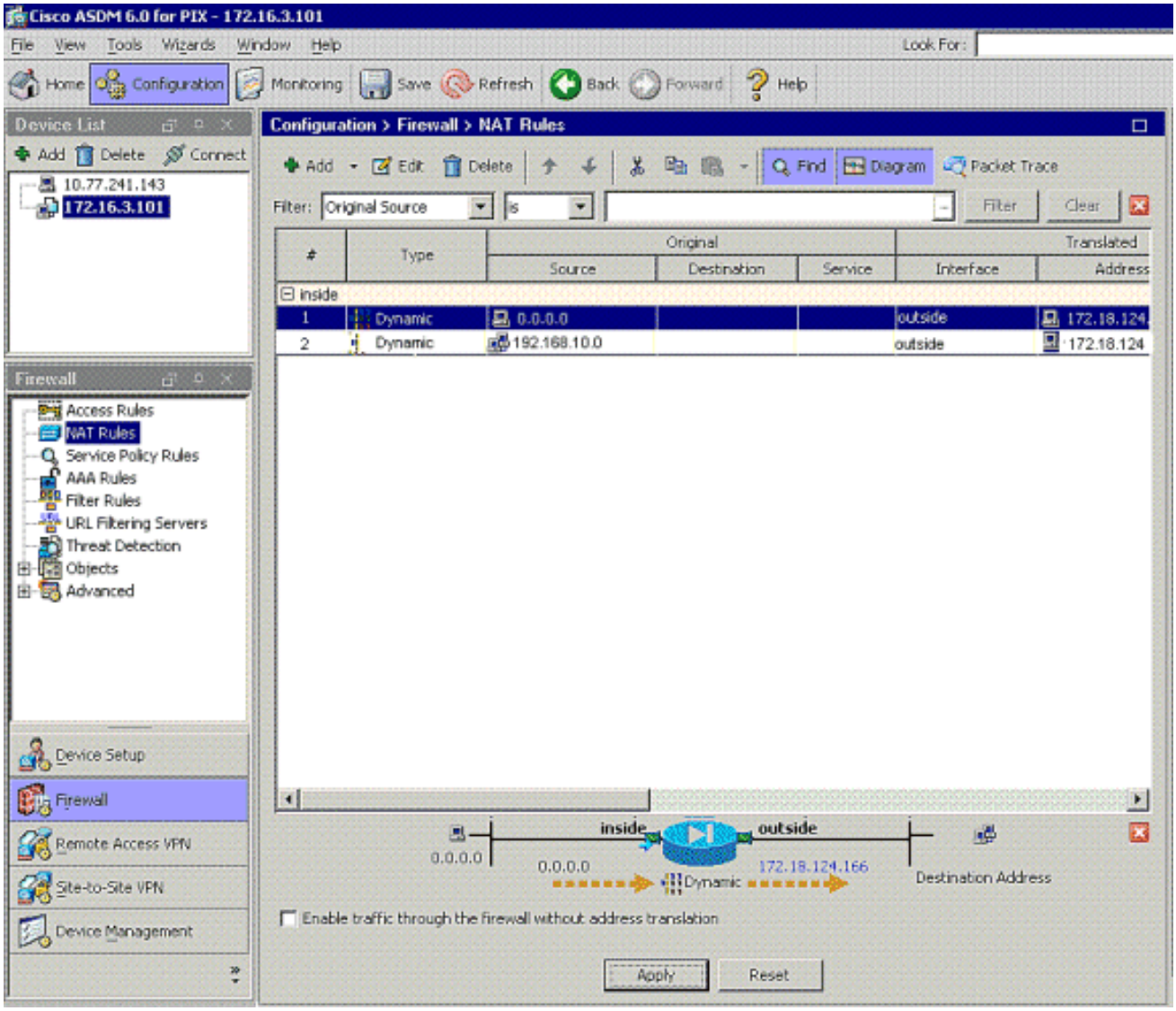


16. Elija el **exterior** como la interfaz de origen, y ingrese los direccionamientos que usted quiere al NAT. Para el direccionamiento Translate en la interfaz, elija **afuera** y haga clic la

AUTORIZACIÓN.



17. La traducción aparece en las Reglas de traducción en las **reglas de la configuración > del Firewall >NAT**.



Nota 1: El comando de permiso-VPN de la conexión del sysopt necesita ser configurado. El comando show running-config sysopt verifica si se configura.

Nota 2: Agregue esta salida para el transporte opcional UDP:

```
group-policy clientgroup attributes vpn-idle-timeout 20
ipsec-udp enable ipsec-udp-port 10000
split-tunnel-policy tunnelspecified split-tunnel-network-list value splittunnel
```

Nota 3: Configure este comando en la configuración global del Dispositivo de PIX para que los clientes VPN conecten vía el IPSec sobre el TCP:

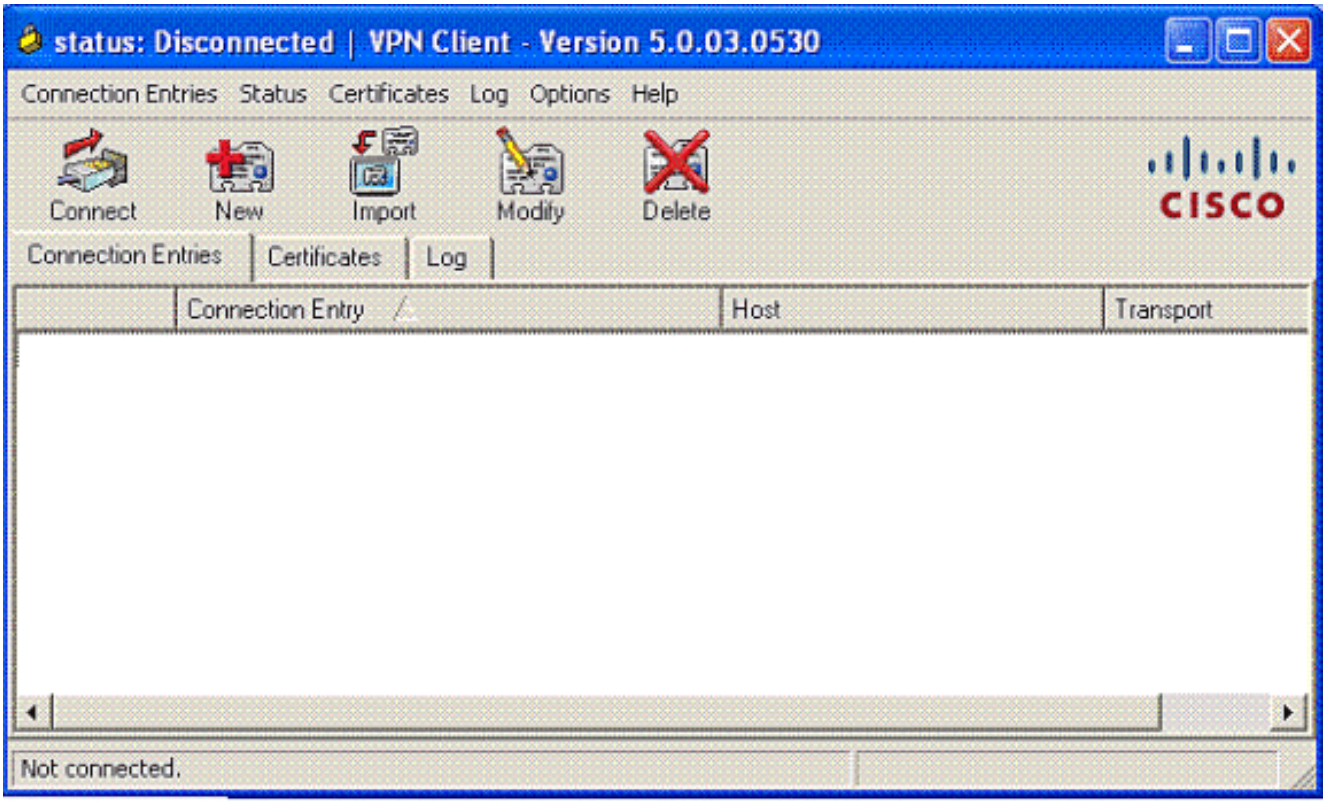
```
isakmp ipsec-over-tcp port 10000
```

Nota: Refiera a la Conexión mediante pines en el vídeo de Cisco ASA para más información sobre diversos escenarios donde la conexión mediante pines puede ser utilizada.

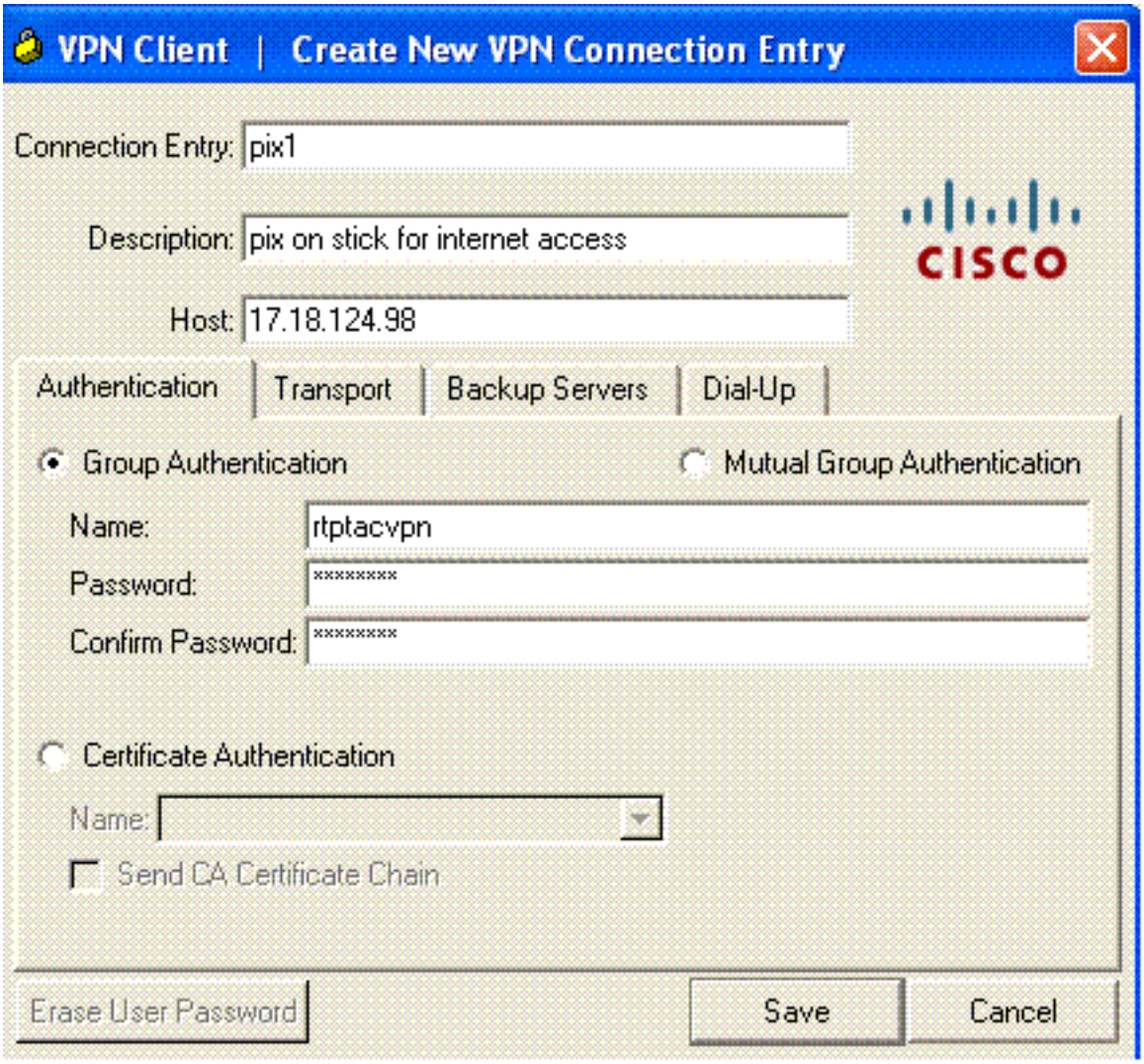
Configuración de cliente VPN

Complete estos pasos para configurar al cliente VPN:

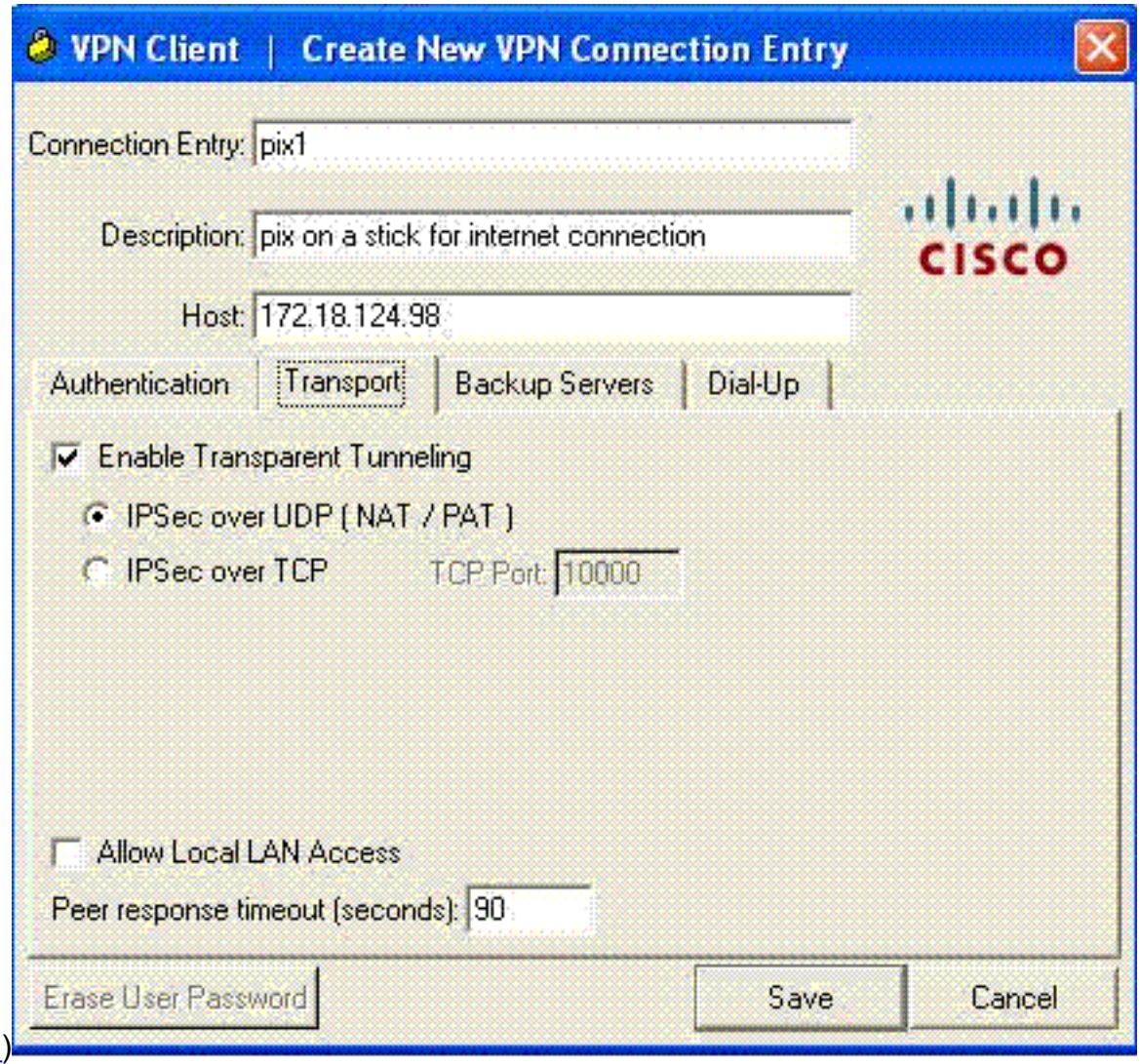
1. Elija
   nuevo.



2. Ingrese el nombre del IP Address y de grupo de túnel de la interfaz exterior PIX junto con la contraseña para
   autenticación.



3. (*Opcional*) haga clic el **Tunelización transparente del permiso** bajo transporte cuadro (esto es opcional y requiere la configuración adicional del PIX/ASA mencionada en la [nota]



2.)

4. Salve el perfil.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- show crypto isakmp sa: muestra las asociaciones de seguridad IKE (SAs) actuales en una par.
- muestre IPSec crypto sa — Visualiza todos los SA actuales. Look for cifra y desencripta los paquetes en el SA que definen el tráfico del cliente VPN.

Intente hacer ping u hojear a un IP Address público del cliente (por ejemplo, www.cisco.com).

Nota: La interfaz interior del PIX no se puede hacer ping para la formación de un túnel a menos que el comando del Acceso de administración se configure en el modo de configuración global.

```
PIX1(config)#management-access inside
PIX1(config)#show management-access

management-access inside
```

Verificación del cliente VPN

Complete estos pasos para verificar al cliente VPN.

1. Haga clic con el botón derecho del ratón en el icono del bloqueo del cliente VPN presente en la bandeja del sistema después de una conexión satisfactoria y elija la opción para estadísticas de ver cifra y desencripta.
2. Haga clic en la lengueta de los detalles de la ruta para no verificar la ninguna lista de túnel dividido pasajera abajo de la aplicación.

Troubleshooting

Nota: Para más información sobre cómo resolver problemas los problemas VPN, refiera a las soluciones del troubleshooting VPN.

Información Relacionada

- Ejemplo aumentado de la configuración VPN del Spoke-a-cliente para la versión 7.0 del dispositivo de seguridad PIX
- Cliente de Cisco VPN
- Negociación IPSec/Protocolos IKE
- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Conexión mediante pines en Cisco ASA
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems