ASA/PIX: Servidor VPN remoto con el NAT entrante para el tráfico del cliente VPN con el CLI y el ejemplo de la Configuración de ASDM

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Productos Relacionados
Convenciones
Antecedentes
Configuraciones
Configure ASA/PIX como servidor VPN remoto con el ASDM
Configure ASA/PIX al tráfico entrada de NAT del cliente VPN con el ASDM
Configure ASA/PIX como servidor VPN remoto y para el NAT entrante con el CLI
Verificación
ASA/PIX dispositivo de seguridad - comandos show
Troubleshooting
Información Relacionada

Introducción

Este documento describe cómo configurar Cisco 5500 Series Adaptive Security Appliance (ASA) para que actúe como servidor VPN remoto mediante el Adaptive Security Device Manager (ASDM) o la CLI y NAT el tráfico entrante del cliente VPN. El ASDM ofrece administración de seguridad de talla mundial y monitoreo a través de una Interfaz de administración basada en la Web intuitiva, fácil de utilizar. Una vez que la configuración de ASA de Cisco es completa, puede ser verificada a través del Cliente Cisco VPN.

prerrequisitos

Requisitos

Este documento asume que el ASA está completamente operativo y está configurado para permitir que el ASDM de Cisco o el CLI realice los cambios de configuración. El ASA también se asume para ser configurado para el NAT saliente. Refiérase no prohiben a host interiores el acceso a las redes externas con el uso de la PALMADITA para más información sobre cómo configurar el NAT saliente.

Nota: Consulte Cómo Permitir el Acceso HTTPS para el ASDM o el PIX/ASA 7.x: SSH en el Ejemplo de Configuración de las Interfaces Interiores y Exteriores para permitir que el dispositivo sea configurado remotamente por el ASDM o el Secure Shell (SSH).

Componentes Utilizados

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

- Versión de software adaptante 7.x del dispositivo de seguridad de Cisco y posterior
- Versión 5.x y posterior adaptante del Administrador de dispositivos de seguridad
- Cliente VPN de Cisco versión 4.x y posterior

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.x y posterior del dispositivo de seguridad del Cisco PIX.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Las configuraciones del acceso remoto proporcionan el acceso remoto seguro para los clientes de Cisco VPN, tales como usuarios móviles. Una VPN de acceso remoto permite que los usuarios remotos accedan de forma segura a los recursos de red centralizada. El Cisco VPN Client cumple con el Protocolo IPSec y se está diseñado específicamente para funcionar con el dispositivo de seguridad. Sin embargo, el dispositivo de seguridad puede establecer las conexiones de IPSec con muchos clientes compatibles con el protocolo. Refiera a las guías de configuración ASA para más información sobre el IPSec.

Los grupos y los usuarios son conceptos fundamentales en la administración de seguridad de los VPN y en la configuración del dispositivo de seguridad. Especifican los atributos que determinan el acceso de los usuarios y el uso de VPN. Un grupo es un conjunto de usuarios considerado una sola entidad. Los usuarios consiguen sus atributos de las políticas del grupo. Los grupos de túnel identifican la directiva del grupo para las conexiones específicas. Si usted no asigna una directiva del grupo determinado a los usuarios, la directiva del grupo predeterminado para la conexión se aplica.

Un grupo de túnel consiste en un conjunto de registros que determina las políticas de conexión del túnel. Estos expedientes identifican los servidores a los cuales autentican a los usuarios del túnel, así como a los servidores de contabilidad, eventualmente, a quienes se envía la información de conexión. Ellos también identifican una política de grupo predeterminada para las conexiones, y contienen los parámetros de la conexión específicos del protocolo. Los grupos de

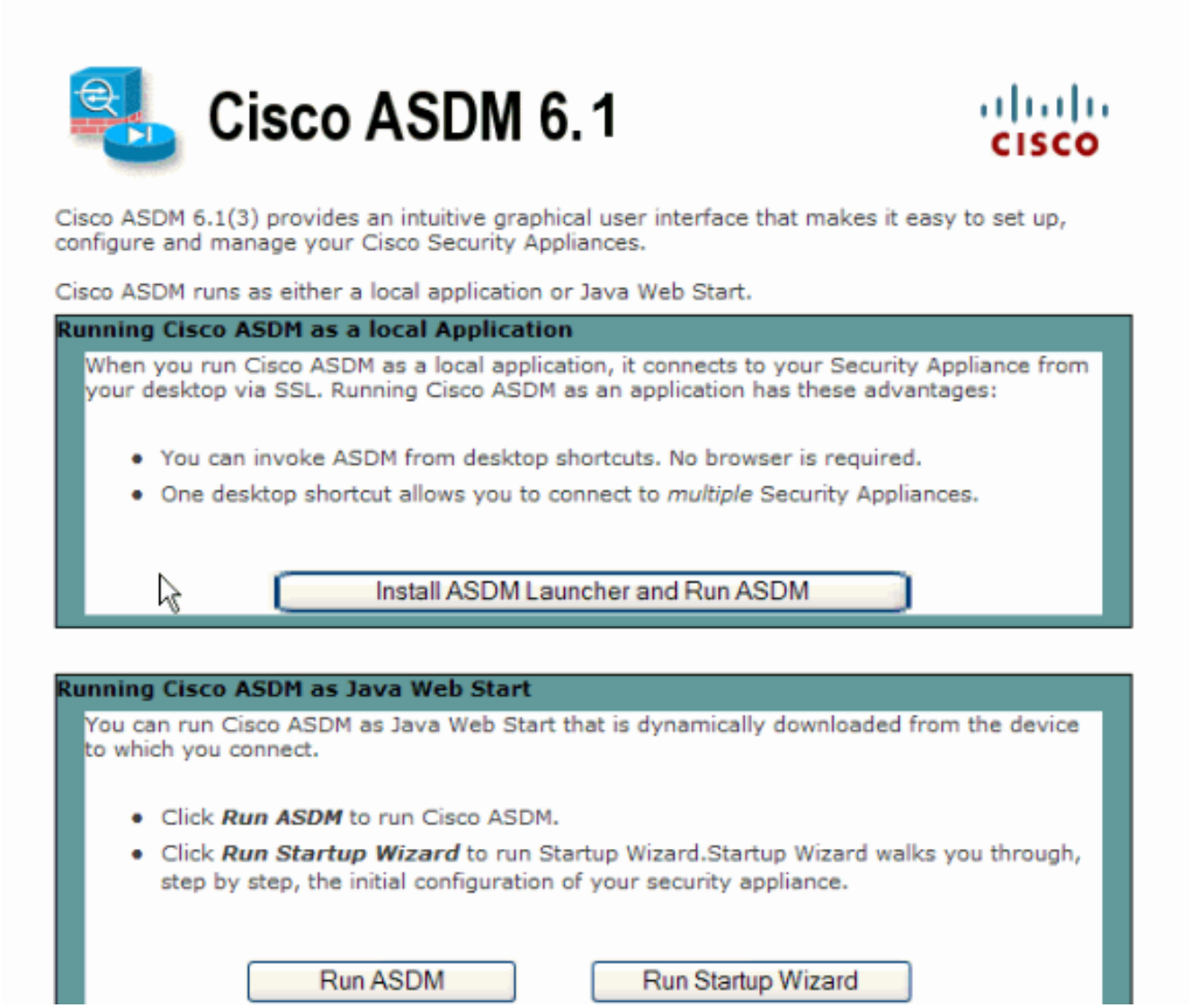
túnel incluyen una pequeña cantidad de atributos que pertenezcan a la creación del túnel sí mismo. Los grupos de túnel incluyen un indicador a una política del grupo que define los atributos orientados hacia el usuario.

Configuraciones

Configure ASA/PIX como servidor VPN remoto con el ASDM

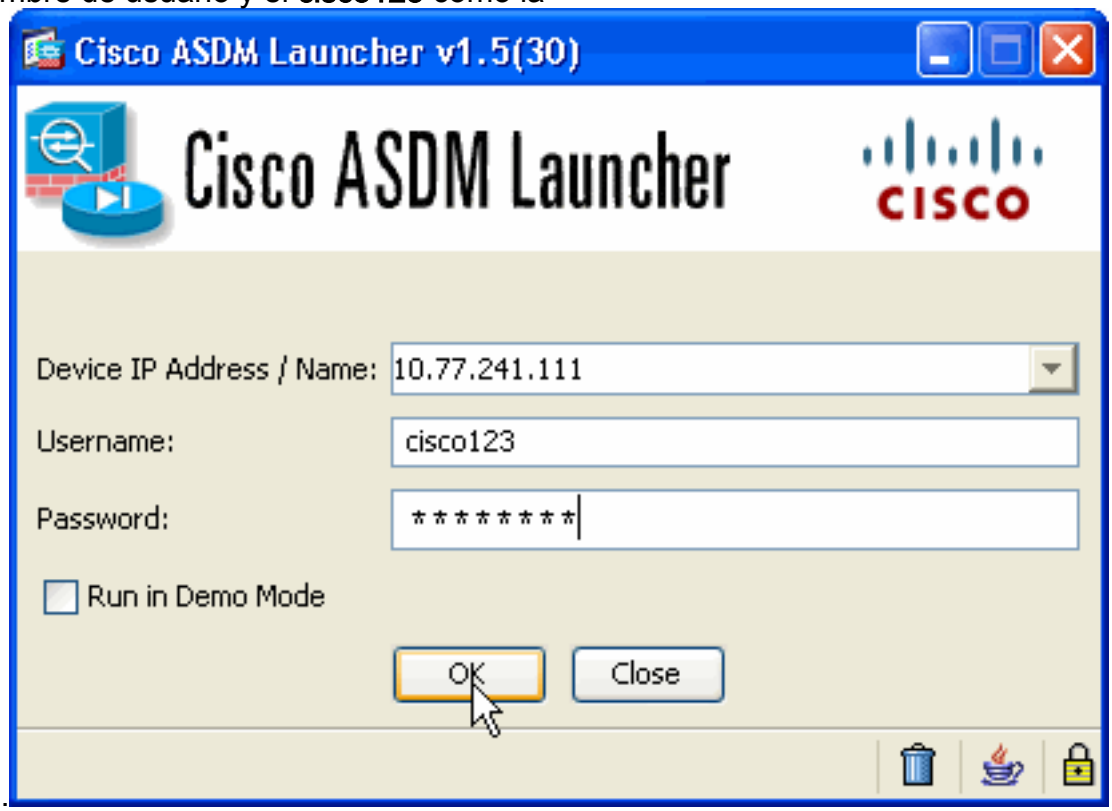
Complete estos pasos para configurar Cisco ASA como servidor VPN remoto con el ASDM:

1. Abra su hojeador y ingrese los **<IP_Address de https:// de la interfaz del ASA que se ha configurado para el ASDM Access>** para acceder el ASDM en el ASA.Aseegurese autorizar cualquier advertencia que su navegador le dé relacionado con la autenticidad de certificados SSL. Nombre de usuario predeterminado y la contraseña son ambos espacio en blanco.El ASA presenta esta ventana para permitir la descarga de la aplicación ASDM. Este ejemplo carga la aplicación sobre la computadora local y no se ejecuta en los subprogramas java.

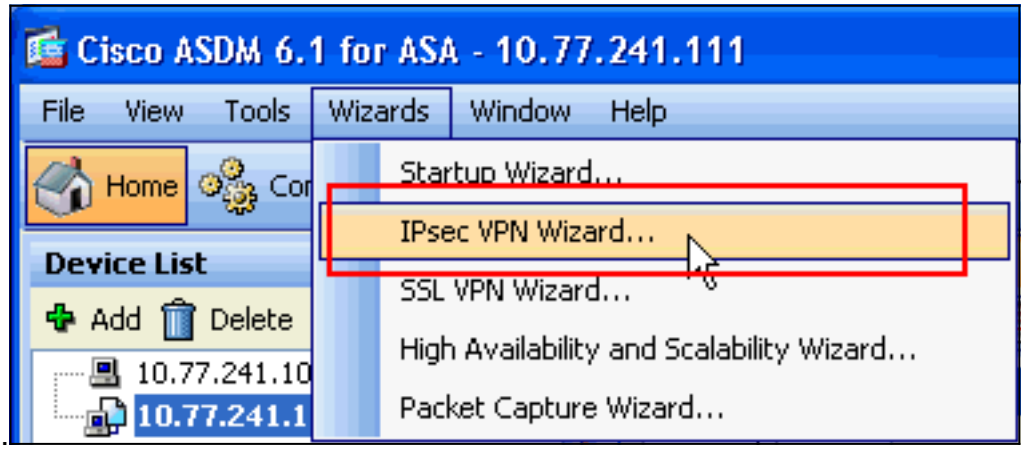


2. Haga clic el **activador de ASDM de la descarga y comience el ASDM** para descargar el instalador para la aplicación ASDM.
3. Una vez que el activador de ASDM descarga, complete los pasos ordenados por los prompts para instalar el software y funcionar con el Cisco ASDM launcher.

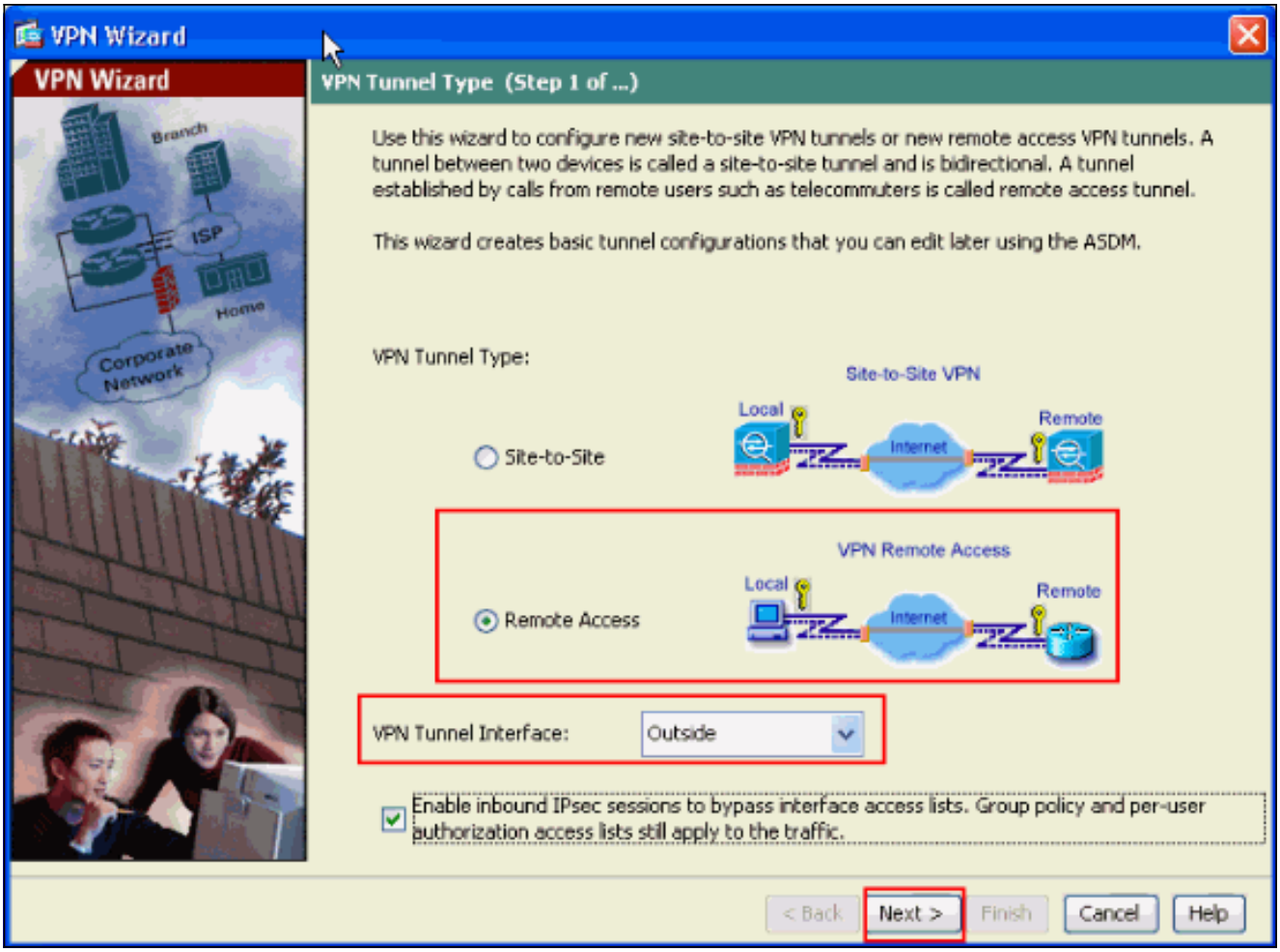
4. Ingrese el IP Address para la interfaz que usted configuró con el **HTTP -** ordene, y un nombre de usuario y contraseña si usted especificó uno.Este ejemplo utiliza el **cisco123** como el nombre de usuario y el **cisco123** como la contraseña.



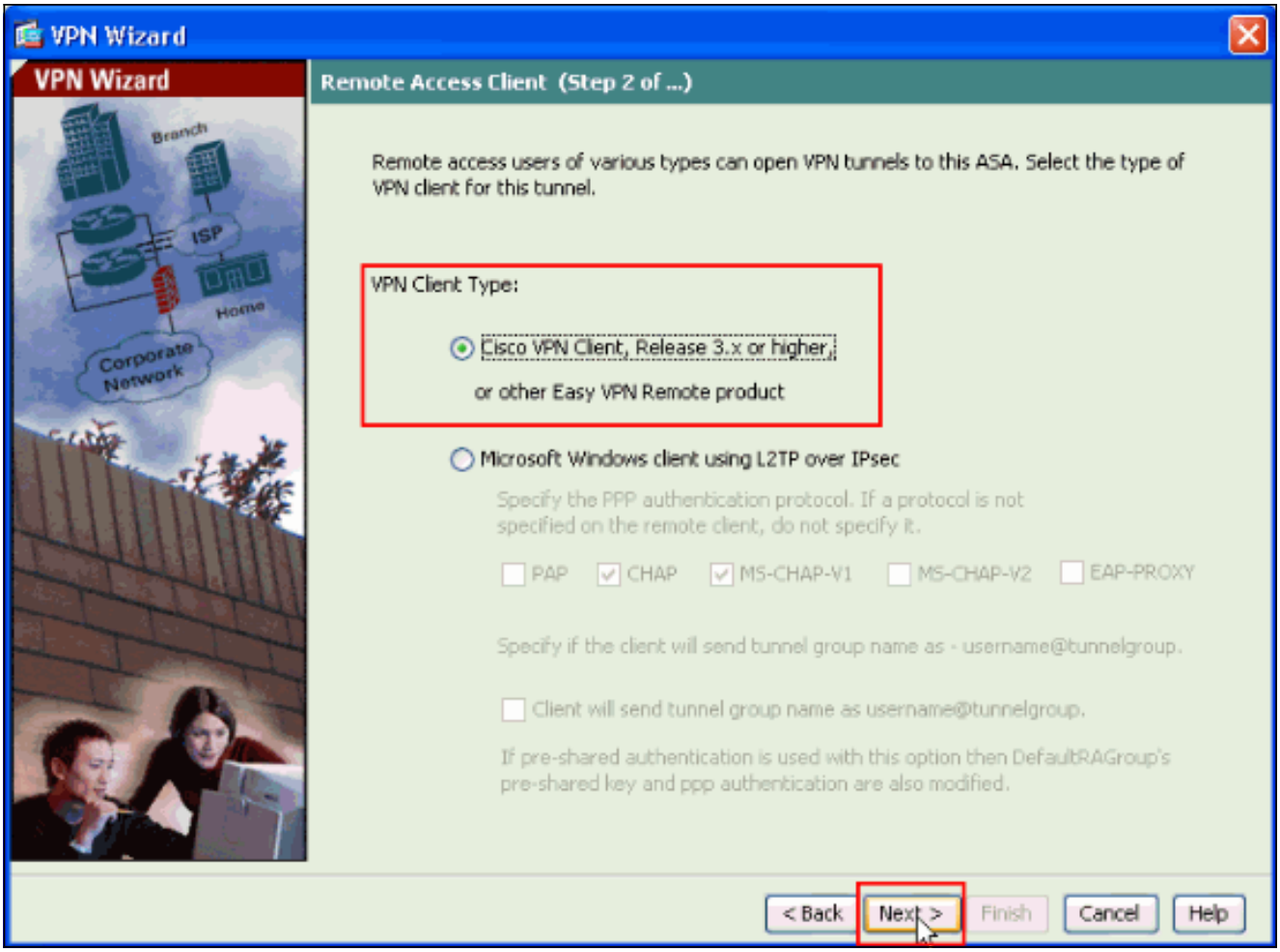
5. Seleccione los **Asisitente > al Asisitente del IPSec VPN de la** ventana casera.



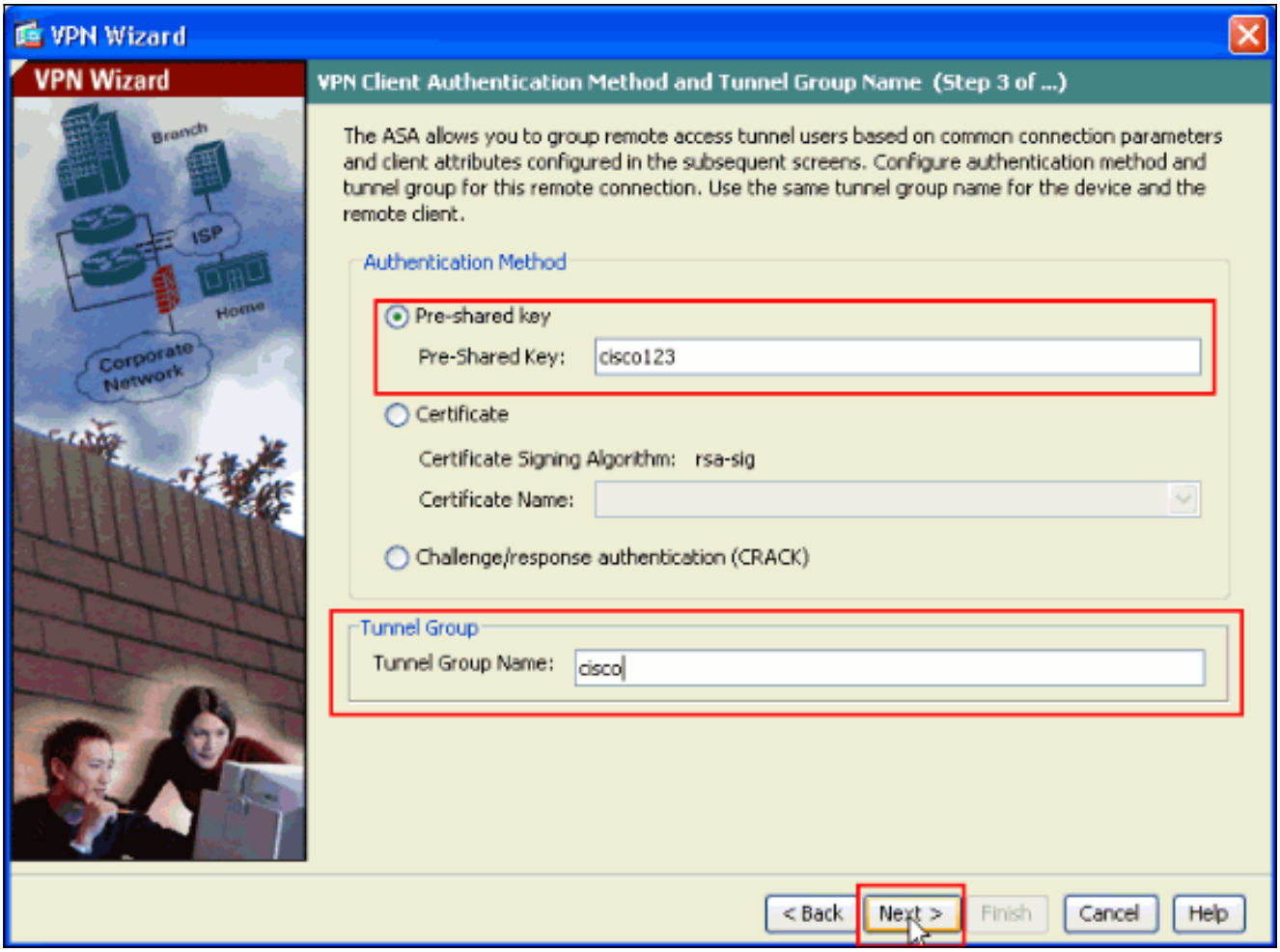
6. Seleccione el tipo de túnel del **VPN de acceso remoto** y asegúrese de que la interfaz del túnel VPN está fijada según lo deseado, y haga clic **después** como se muestra aquí.



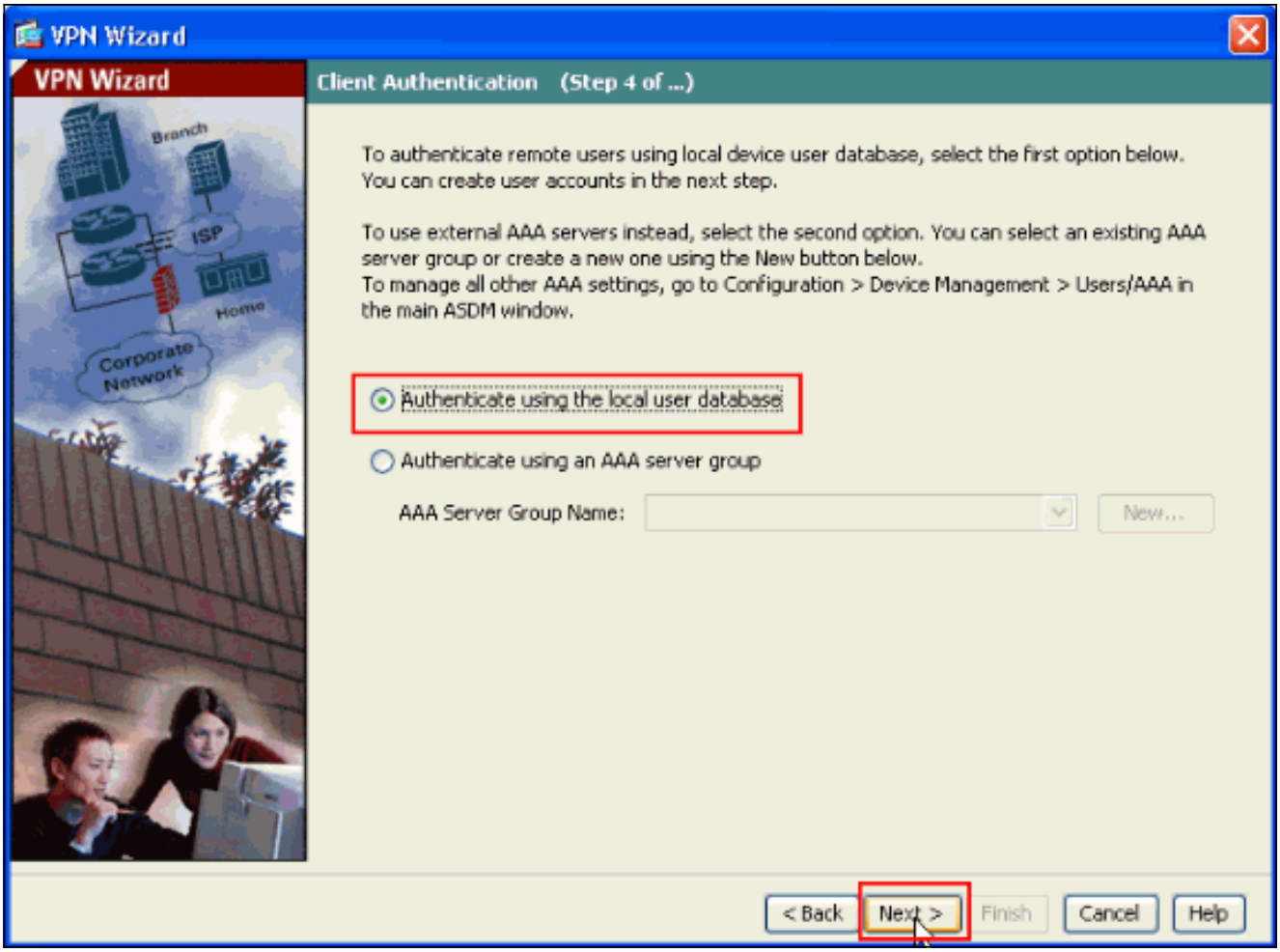
7. Eligen al tipo del cliente VPN, como se muestra. Eligen al **Cliente Cisco VPN** aquí. Haga clic en Next
(Siguiente).



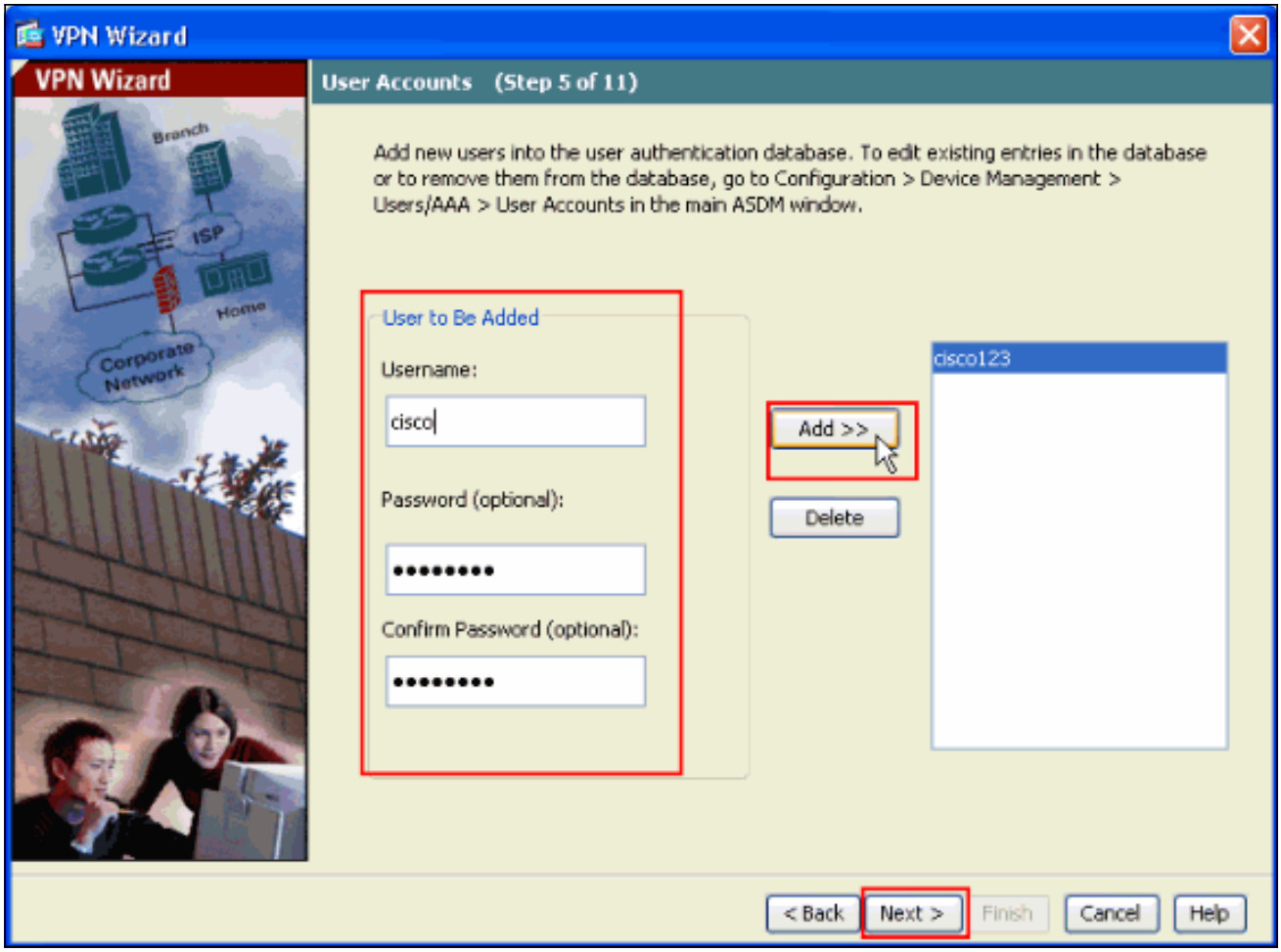
8. Ingrese un nombre para el Nombre de Grupo de Túnel. Ingrese la información de autenticación para utilizar, que es la **clave previamente compartida** en este ejemplo. La clave previamente compartida usada en este ejemplo es **cisco123**. El nombre de grupo de túnel usado en este ejemplo es **Cisco**. Haga clic en Next (Siguiente).



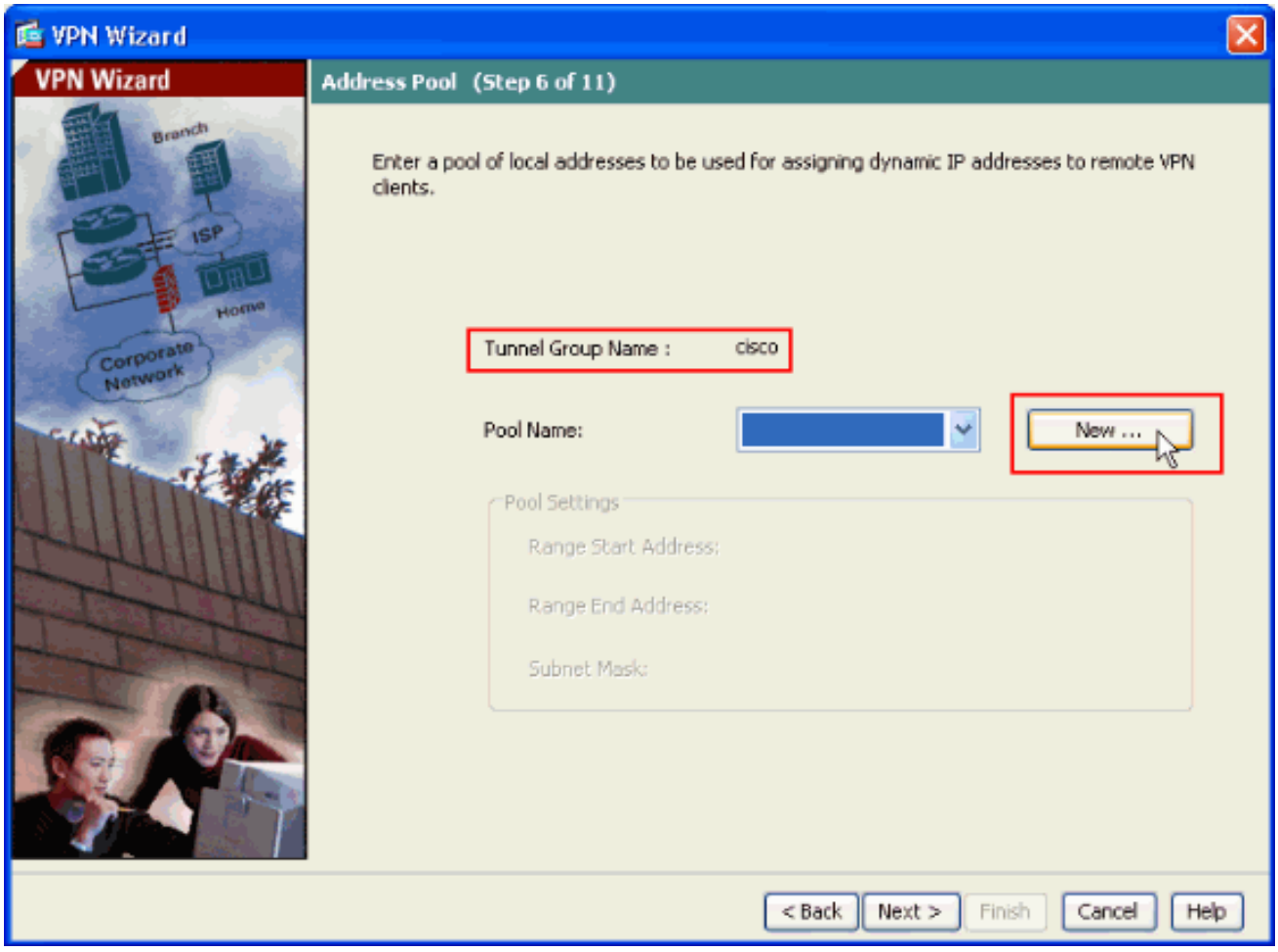
9. Elija si desea que los usuarios remotos sean autenticados en las bases de datos de usuarios locales o en un grupo de servidores AAA externo.**Nota:** Usted agrega a los usuarios a la base de datos de usuarios locales en el paso 10.**Nota:** Refiera a los grupos de servidores de la autenticación y 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.



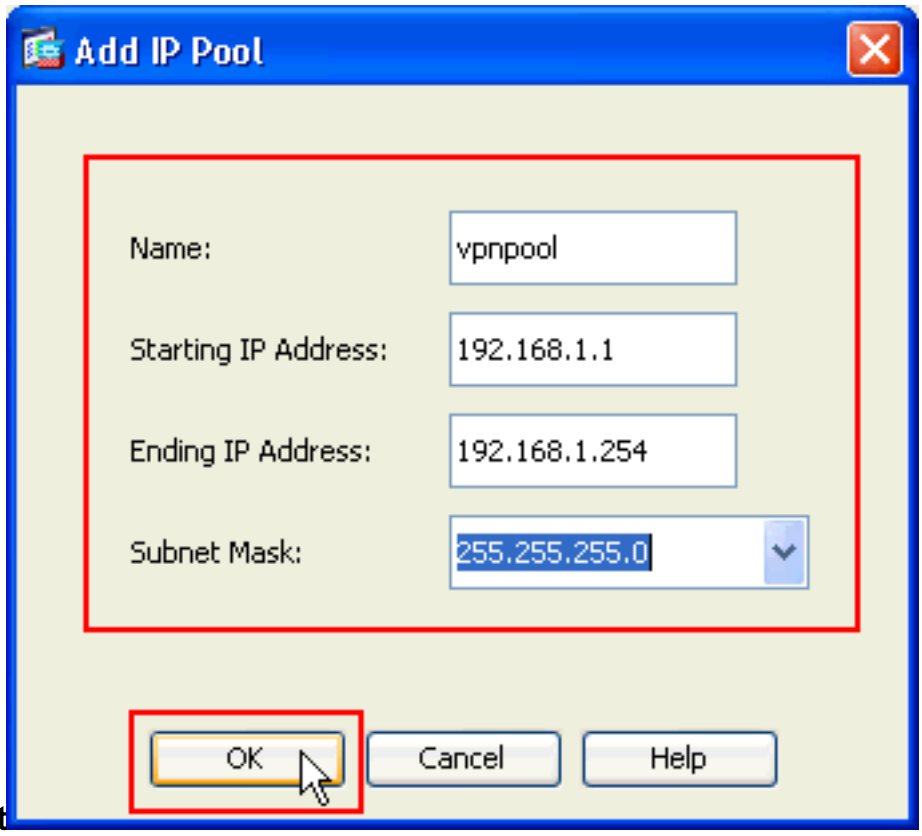
10. Proporcione un **nombre de usuario** y la **contraseña** y el tecleo opcionales **agregan** para agregar a los usuarios nuevos a la base de datos de autenticación de usuario. Haga clic en Next (Siguiente).**Nota:** No quite a los usuarios existentes de esta ventana. Seleccione la **configuración > la Administración de dispositivos > Users/AAA > 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.



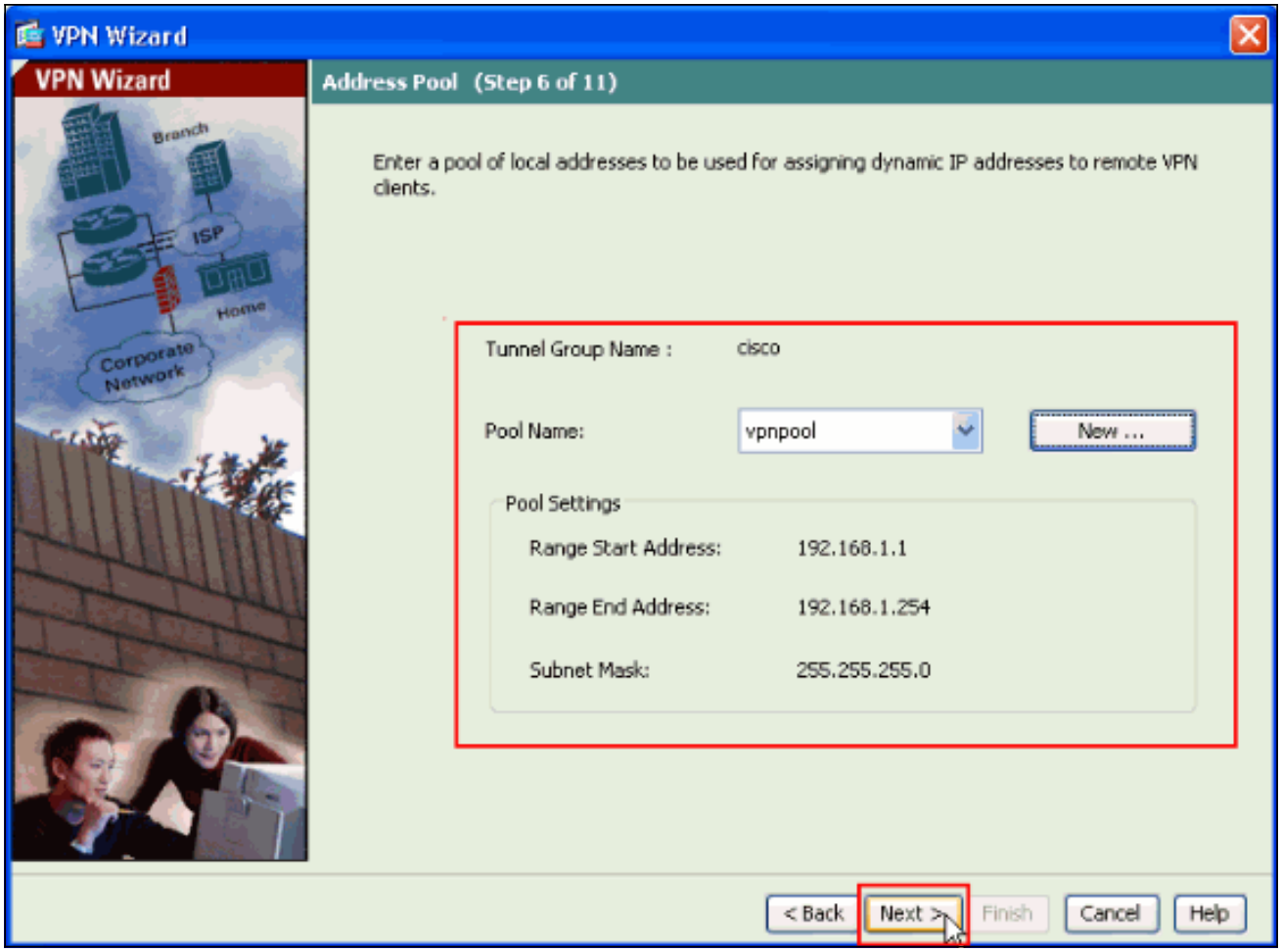
11. Para definir un pool de las direcciones locales que se asignarán dinámicamente a los clientes VPN remotos, haga clic **nuevo** para crear a una nueva **agrupación IP**.



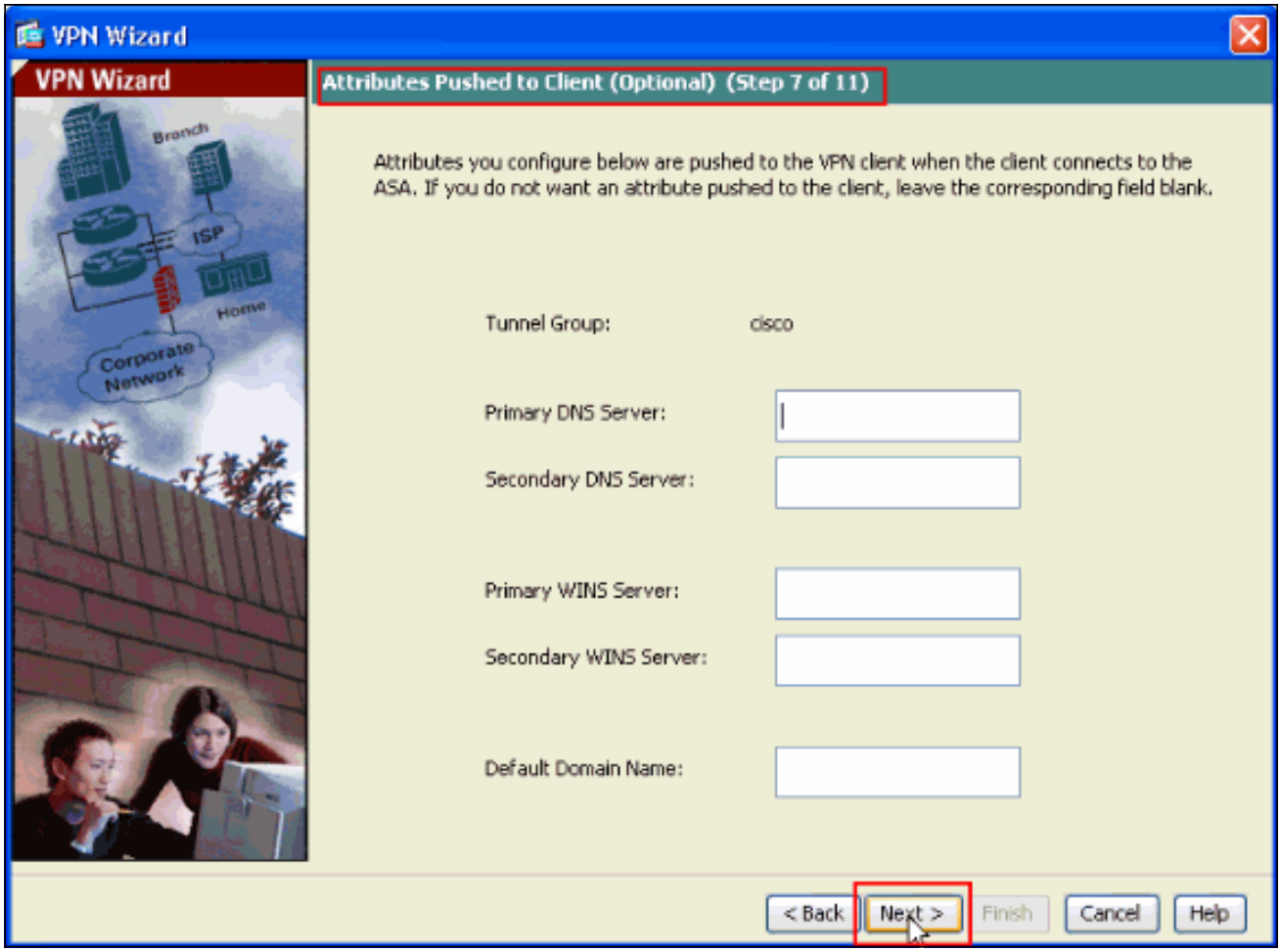
12. En la nueva ventana titulada **agregue a la agrupación IP** proporcionan esta información, y hacen clic la **AUTORIZACIÓN.Nombre de la agrupación IPComenzar la dirección IPTerminación de la dirección IPMáscara de subnet**



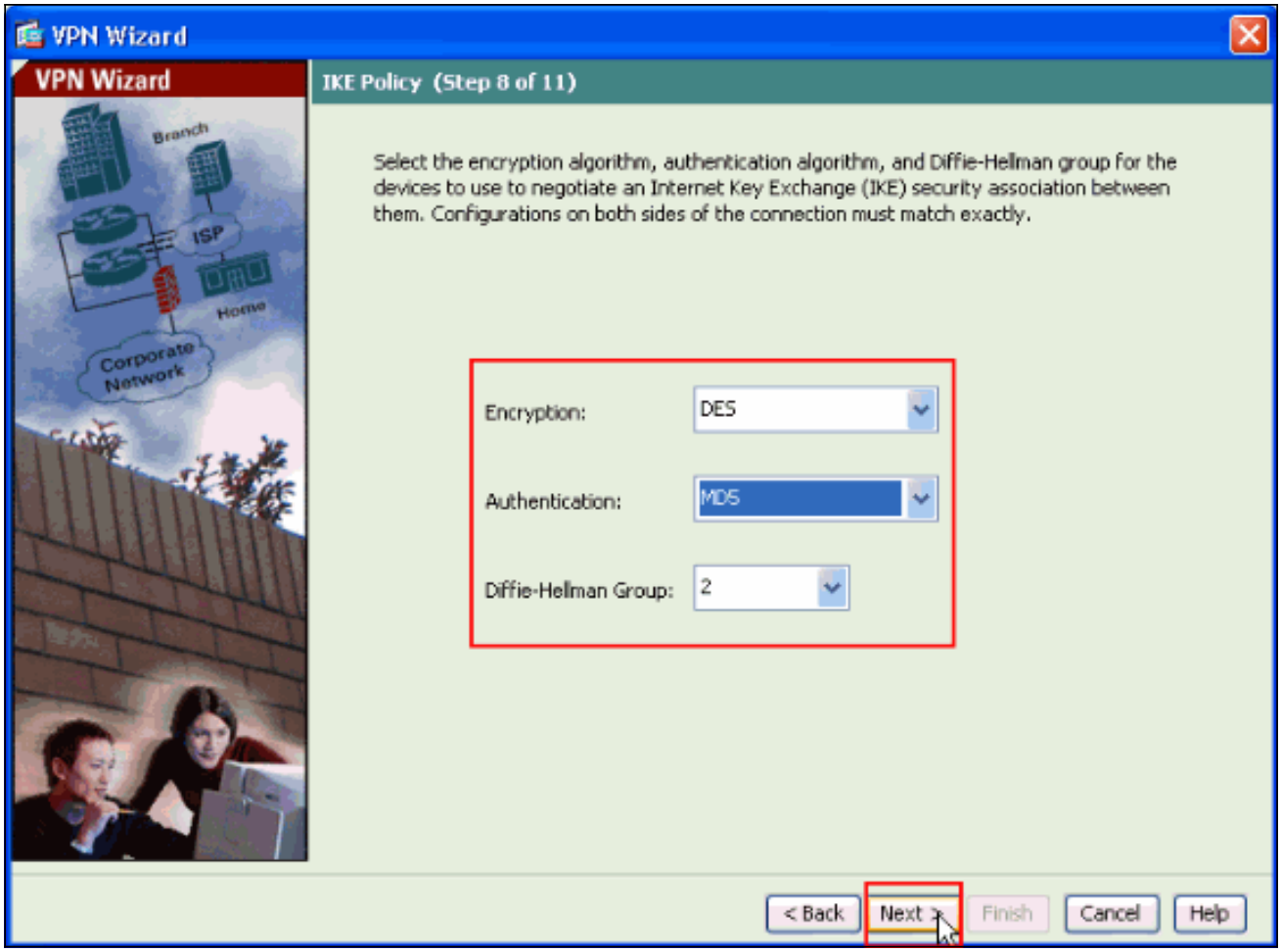
13. Después de que usted defina el pool de las direcciones locales que se asignarán dinámicamente a los clientes VPN remotos cuando conectan, haga clic **después.**



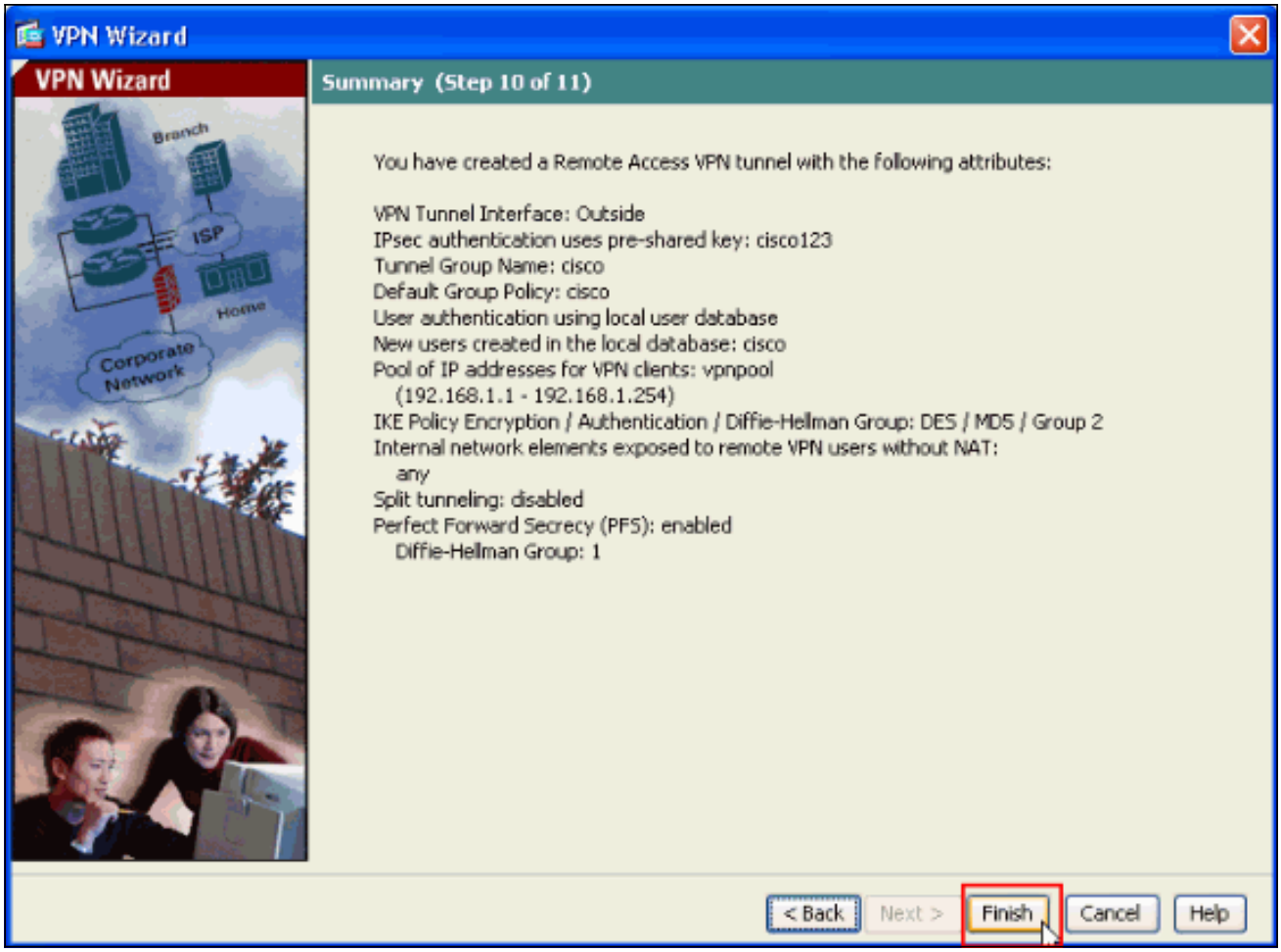
14. *Opcional:* Especifique la información de servidor DNS y WINS y un Nombre de Dominio Predeterminado que se avanzará a los clientes de VPN remotos.



15. Especifique los parámetros para el IKE, también conocidos como fase 1. IKE.Las configuraciones a ambos lados del túnel deben coincidir de manera exacta. Sin embargo, el Cisco VPN Client selecciona automáticamente la configuración adecuada para sí mismo. Por lo tanto, no hay configuración IKE necesaria en PC del cliente.



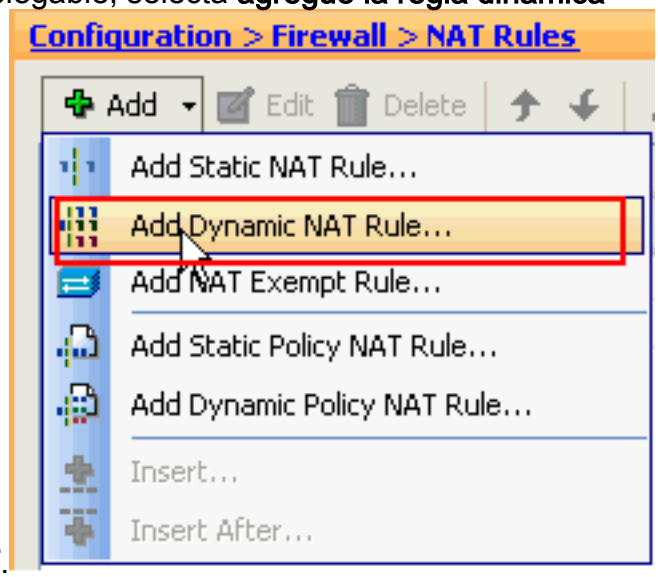
16. Esta ventana muestra un resumen de las acciones que ha realizado. Haga clic en **Finalizar** si está satisfecho con la configuración.



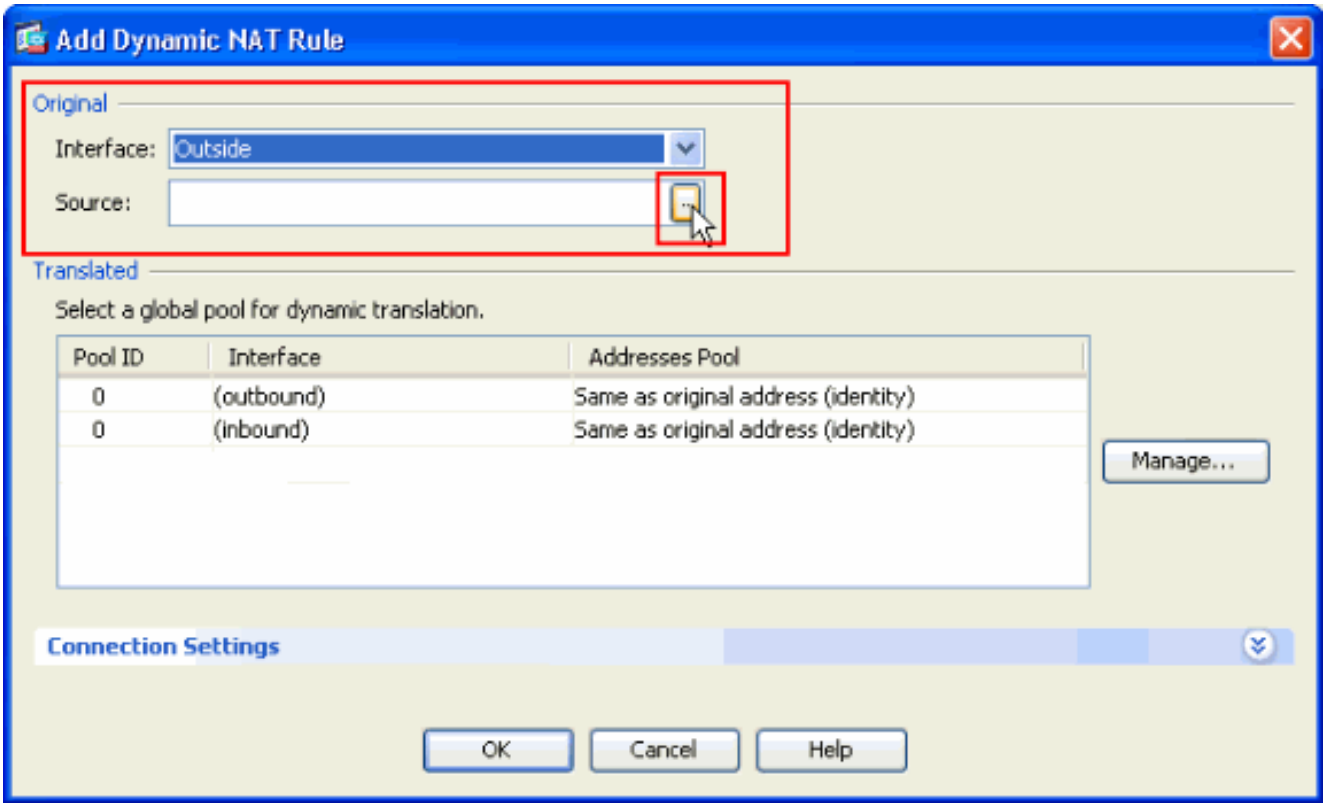
Configure ASA/PIX al tráfico entrada de NAT del cliente VPN con el ASDM

Complete estos pasos para configurar Cisco ASA al tráfico entrada de NAT del cliente VPN con el ASDM:

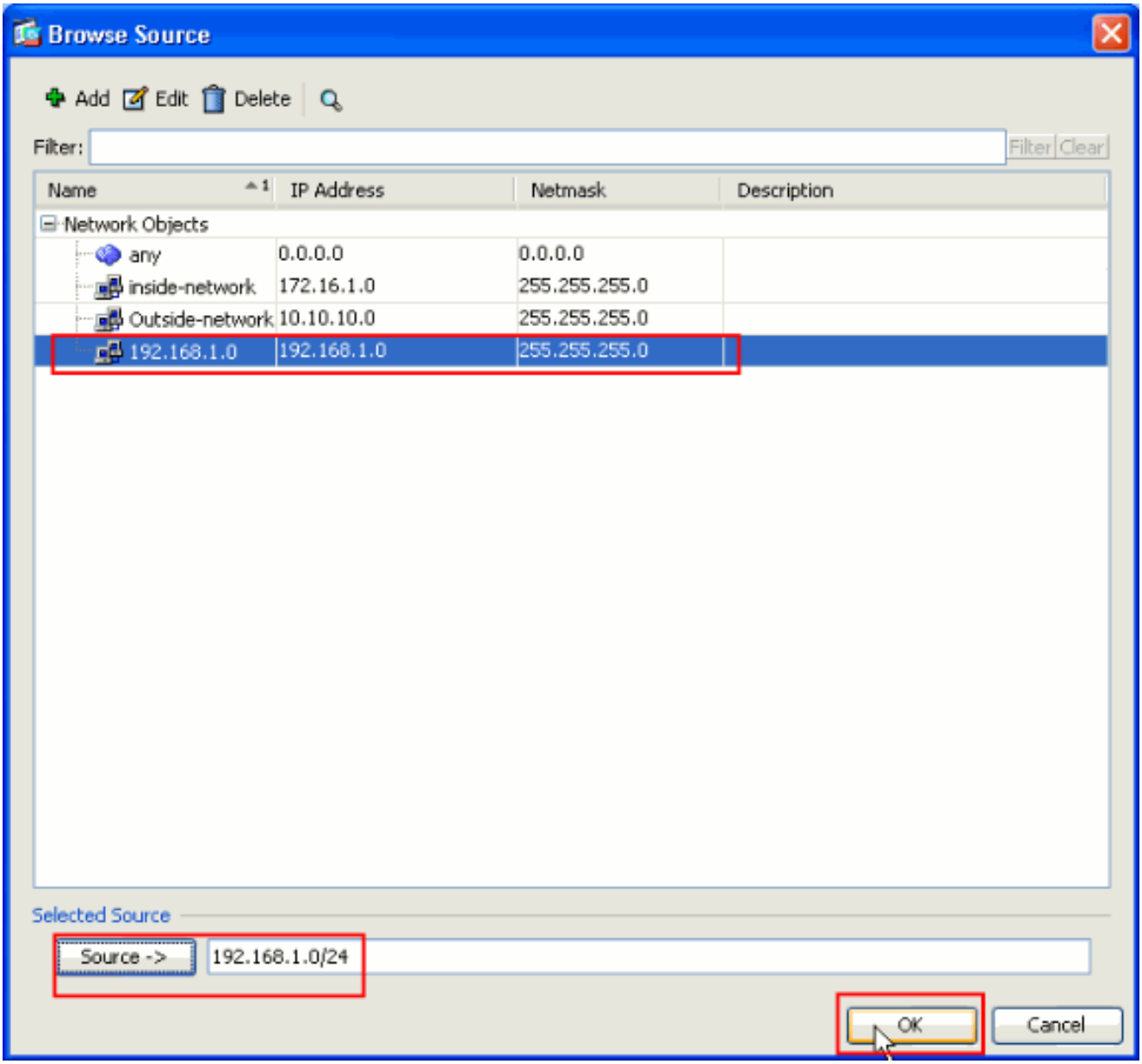
1. Elija la **configuración > el Firewall > las reglas nacionales**, y el haga click en Add En la lista desplegable, selecta **agregue la regla dinámica NAT**.



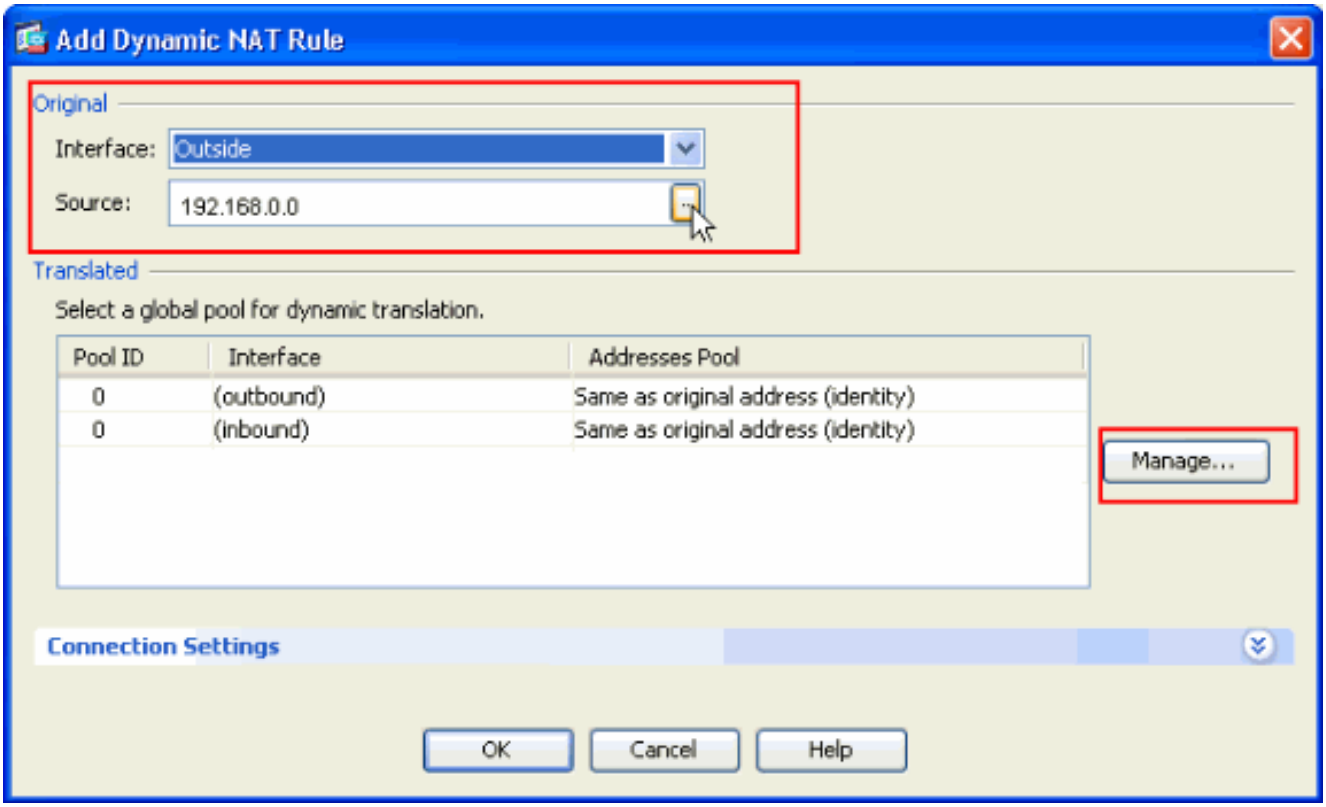
2. En la ventana **dinámica de la regla del agregar NAT**, elija el **exterior** como la interfaz, y haga clic el botón Browse al lado del cuadro de la **fuente**.



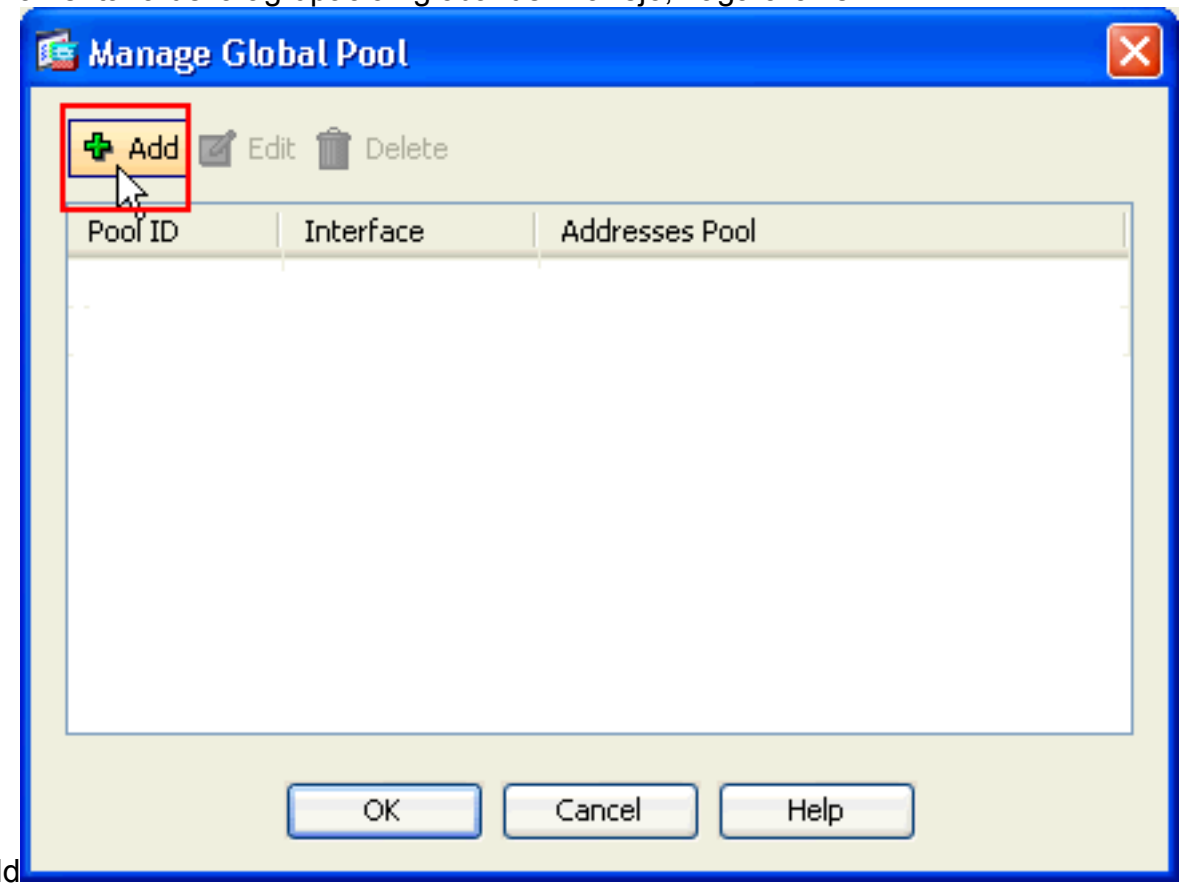
3. En la ventana de la fuente de la ojeada, seleccione los objetos de red adecuada y también elija la **fuente** bajo sección seleccionada de la fuente, y haga clic la **AUTORIZACIÓN**. Aquí el objeto de red de 192.168.1.0 se
elige.



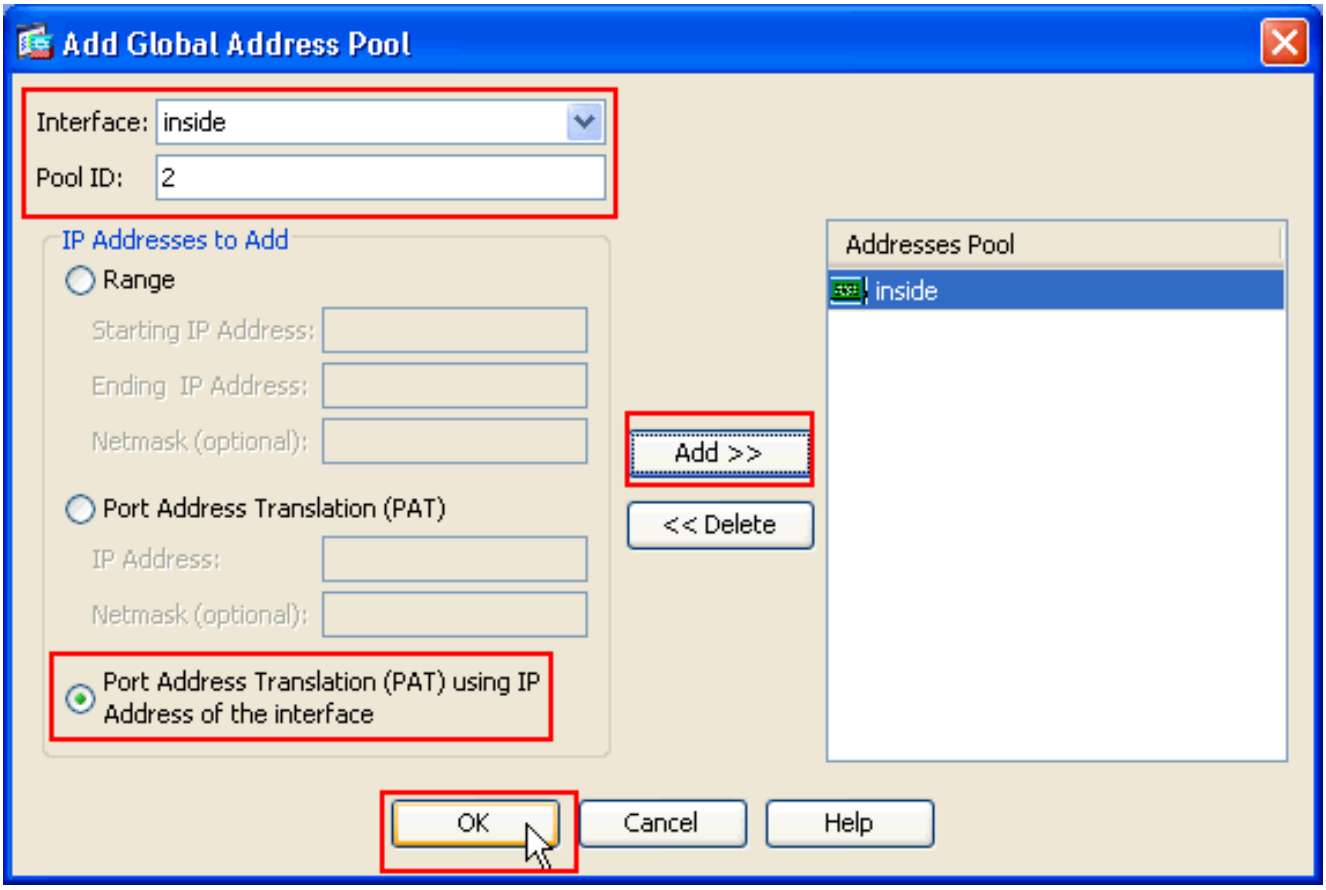
4. El tecleo **maneja**.



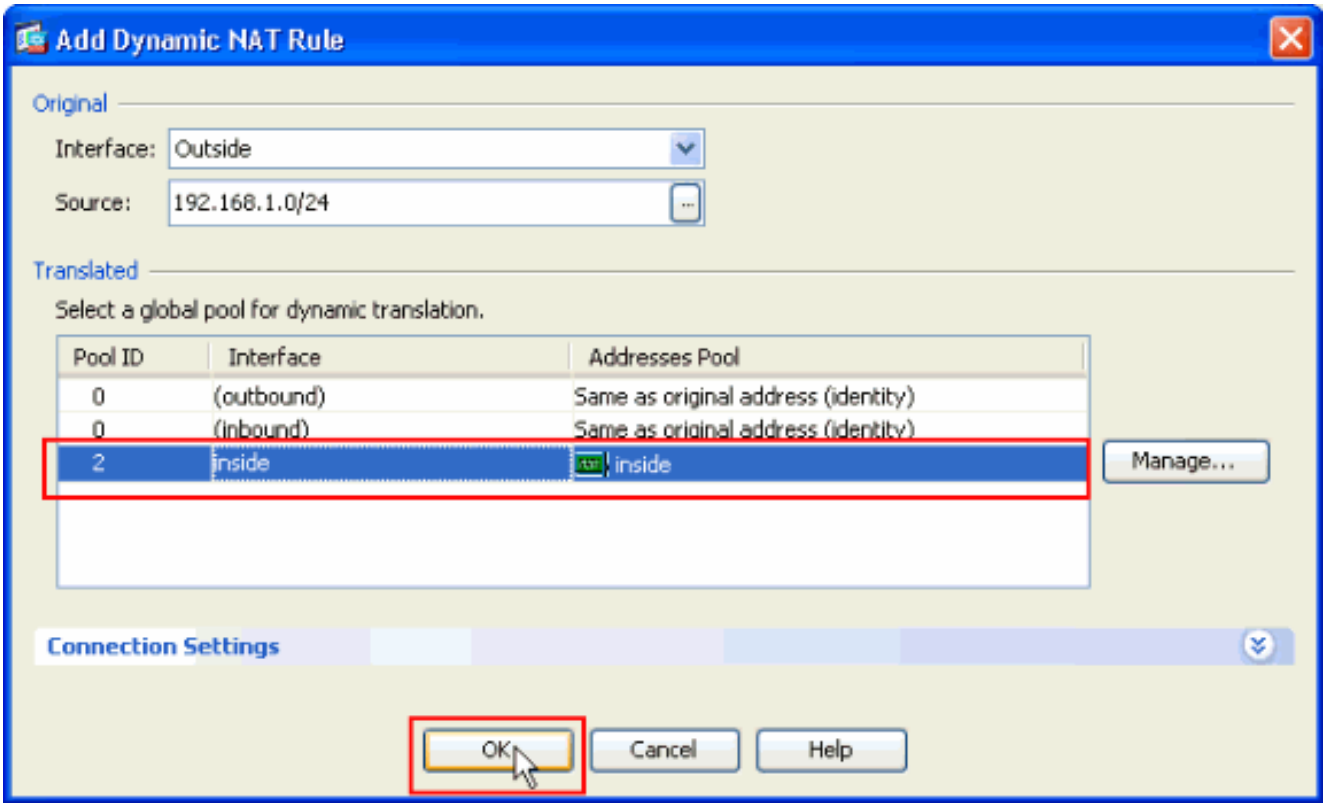
5. En la ventana de la agrupación global del manejo, haga click en Add



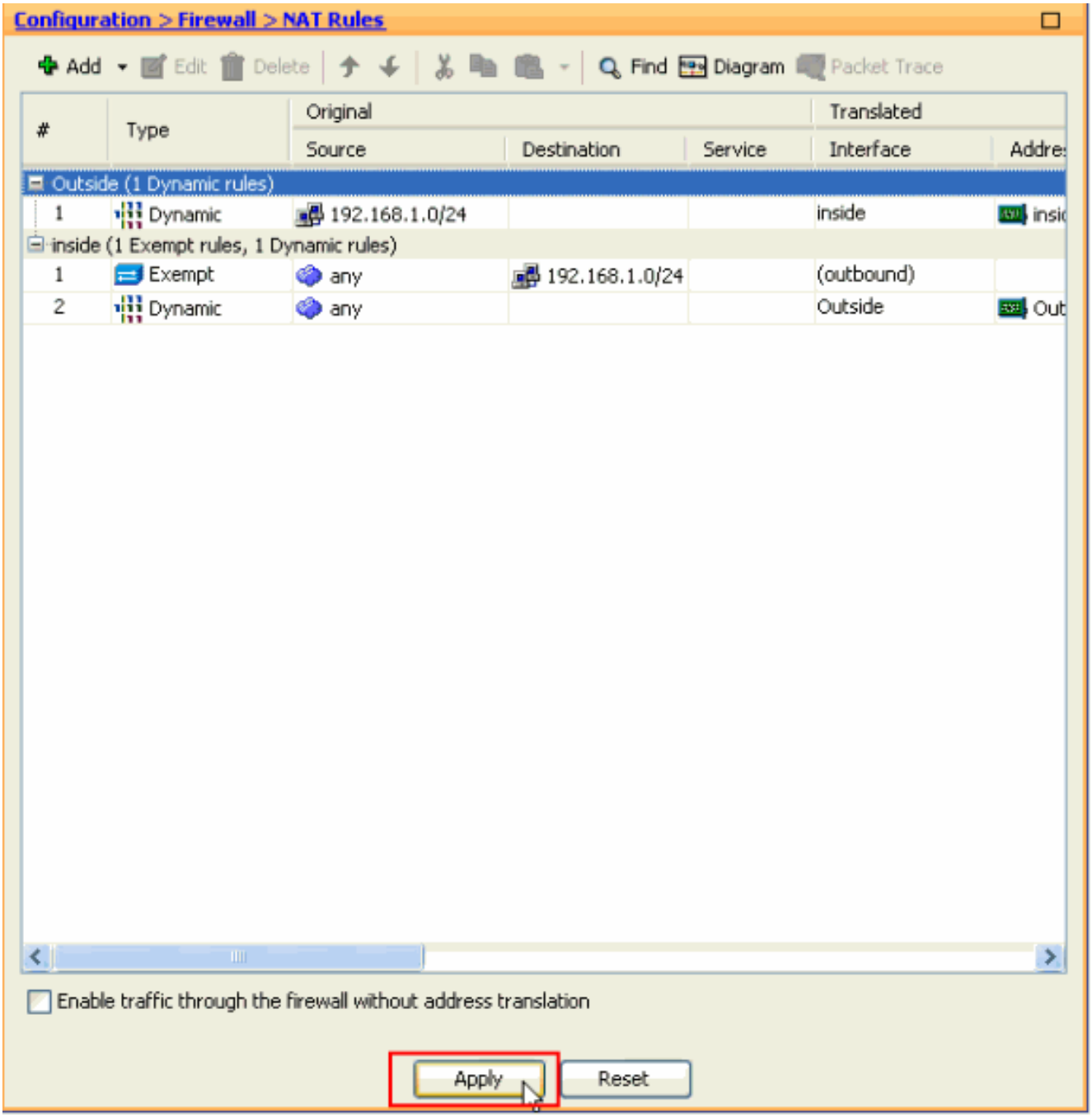
6. En la ventana de la agrupación global de direcciones del agregar, elija el **interior** como la interfaz y **2** como el **pool ID**. También aseegurese que el botón de radio al lado de la **PALMADITA usando la dirección IP de la interfaz** está seleccionado. Haga clic **Add>>**, y después haga clic la **AUTORIZACIÓN**.



7. Haga Click en OK después de que usted seleccione a la agrupación global con el **pool ID 2** configurado en el paso
anterior.



8. Ahora el tecleo **se aplica** para aplicar la configuración al ASA.This complete la configuración.



Configure ASA/PIX como servidor VPN remoto y para el NAT entrante con el CLI

Configuración que se está ejecutando en el Dispositivo ASA
ciscoasa#**show running-config** : Saved ASA Version 8.0(3) ! hostname ciscoasa enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0 nameif Outside security-level 0 ip address 10.10.10.2 255.255.255.0 ! interface Ethernet0/1 nameif inside security-level 100 ip address 172.16.1.2 255.255.255.0 ! ! passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa803-k8.bin ftp mode passive access-list inside_nat0_outbound extended permit ip any 192.168.1.0 255.255.255 0 pager lines 24 logging enable mtu Outside 1500 mtu inside 1500 **ip local pool vpnpool 192.168.1.1-192.168.1.254 mask 255.255.255.0** no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-615.bin asdm history enable arp timeout 14400 nat-control **global (Outside) 1 interface global (inside) 2 interface nat (Outside) 2**

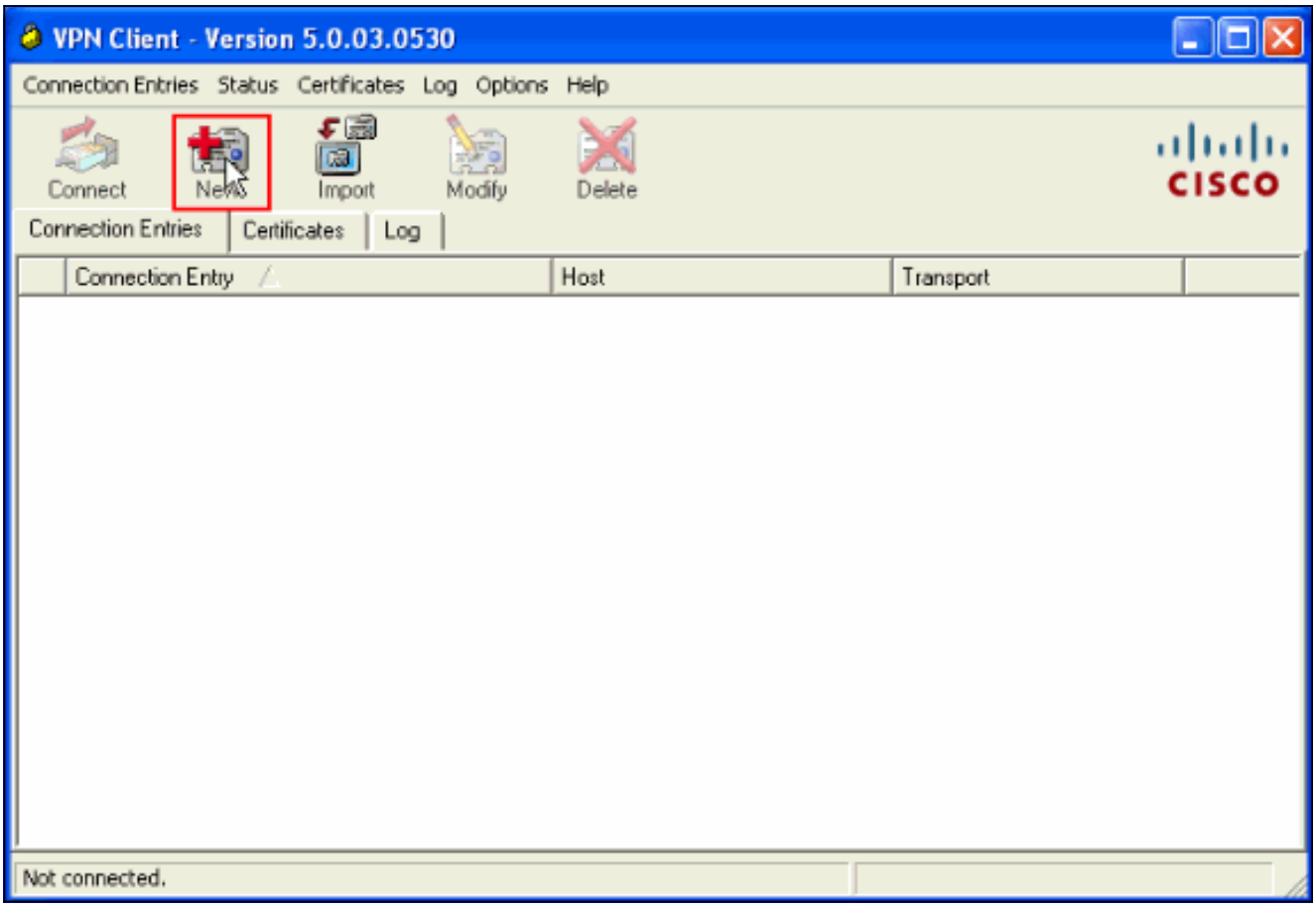
```
192.168.1.0 255.255.255.0 outside nat (inside) 0 access-
list inside_nat0_outbound nat (inside) 1 0.0.0.0 0.0.0.0
route Outside 0.0.0.0 0.0.0.0 10.10.10.3 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 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
dynamic-access-policy-record DfltAccessPolicy http
server enable no snmp-server location no snmp-server
contact !--- Configuration for IPsec policies. !---
Enables the crypto transform configuration mode, !---
where you can specify the transform sets that are used
!--- during an IPsec negotiation. crypto ipsec
transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto
ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set
pfs group1 crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP
65535 set transform-set ESP-DES-SH ESP-DES-MD5 crypto
map Outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP crypto map Outside_map
interface Outside crypto isakmp enable Outside !---
Configuration for IKE policies. !--- Enables the IKE
policy configuration (config-isakmp) !--- command mode,
where you can specify the parameters that !--- are used
during an IKE negotiation. Encryption and !--- Policy
details are hidden as the default values are chosen.
crypto isakmp policy 10 authentication pre-share
encryption des hash sha group 2 lifetime 86400 crypto
isakmp policy 30 authentication pre-share encryption des
hash md5 group 2 lifetime 86400 telnet timeout 5 ssh
timeout 60 console timeout 0 management-access inside
threat-detection basic-threat threat-detection
statistics access-list group-policy cisco internal
group-policy cisco attributes vpn-tunnel-protocol IPSec
!--- Specifies the username and password with their !---
respective privilege levels username cisco123 password
ffIRPGpDSOJh9YLq encrypted privilege 15 username cisco
password ffIRPGpDSOJh9YLq encrypted privilege 0 username
cisco attributes vpn-group-policy cisco tunnel-group
cisco type remote-access tunnel-group cisco general-
attributes address-pool vpnpool default-group-policy
cisco !--- Specifies the pre-shared key "cisco123" which
must !--- be identical at both peers. This is a global
!--- configuration mode command. tunnel-group cisco
ipsec-attributes pre-shared-key * ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns migrated_dns_map_1
parameters message-length maximum 512 policy-map
global_policy class inspection_default inspect dns
migrated_dns_map_1 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:f2ad6f9d5bf23810a26f5cb464e1fdf3 : end
ciscoasa#
```

Verificación

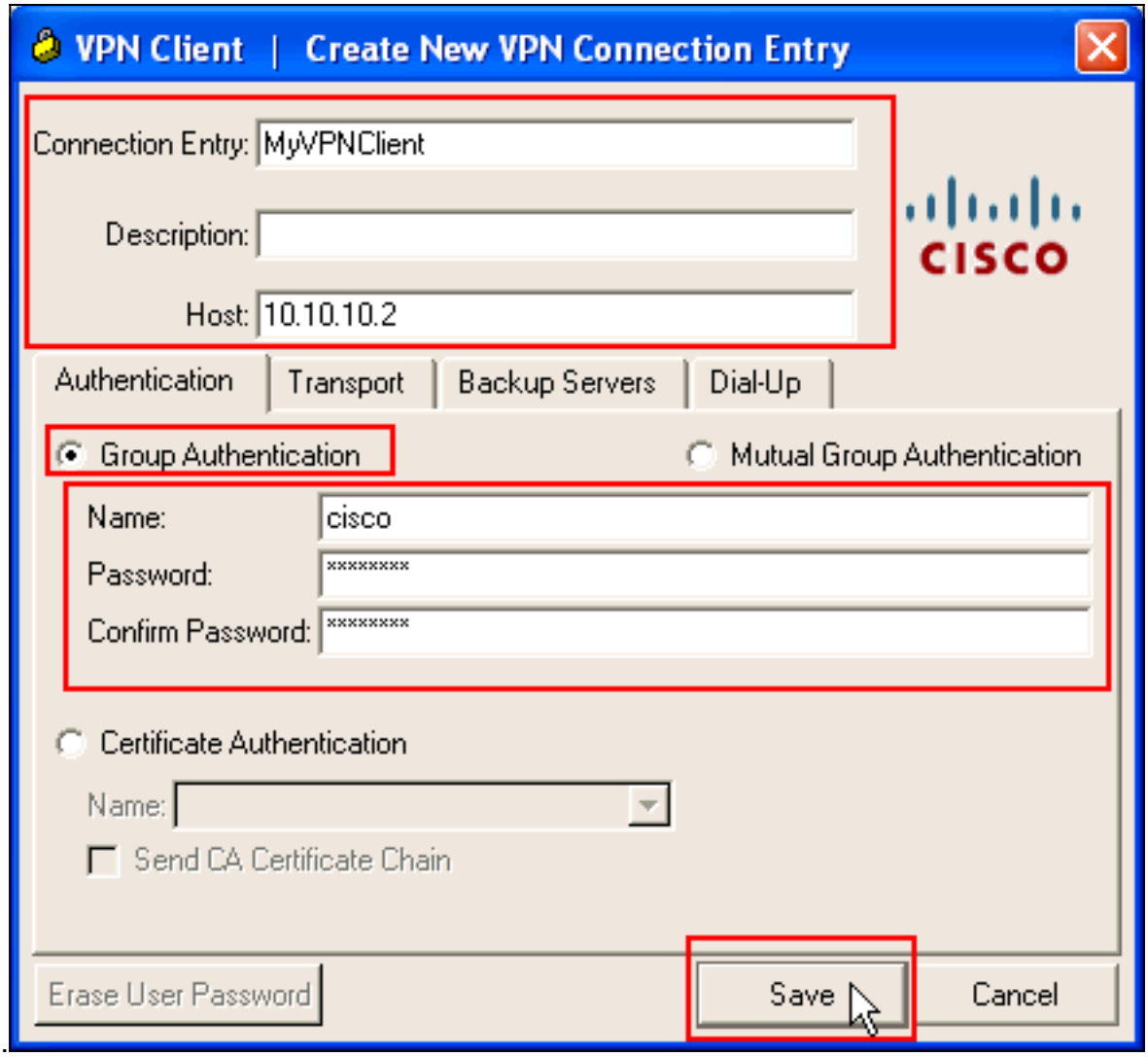
Intente conectar con Cisco ASA a través del Cliente Cisco VPN para verificar que el ASA está

configurado con éxito.

1. Haga clic en
   New.

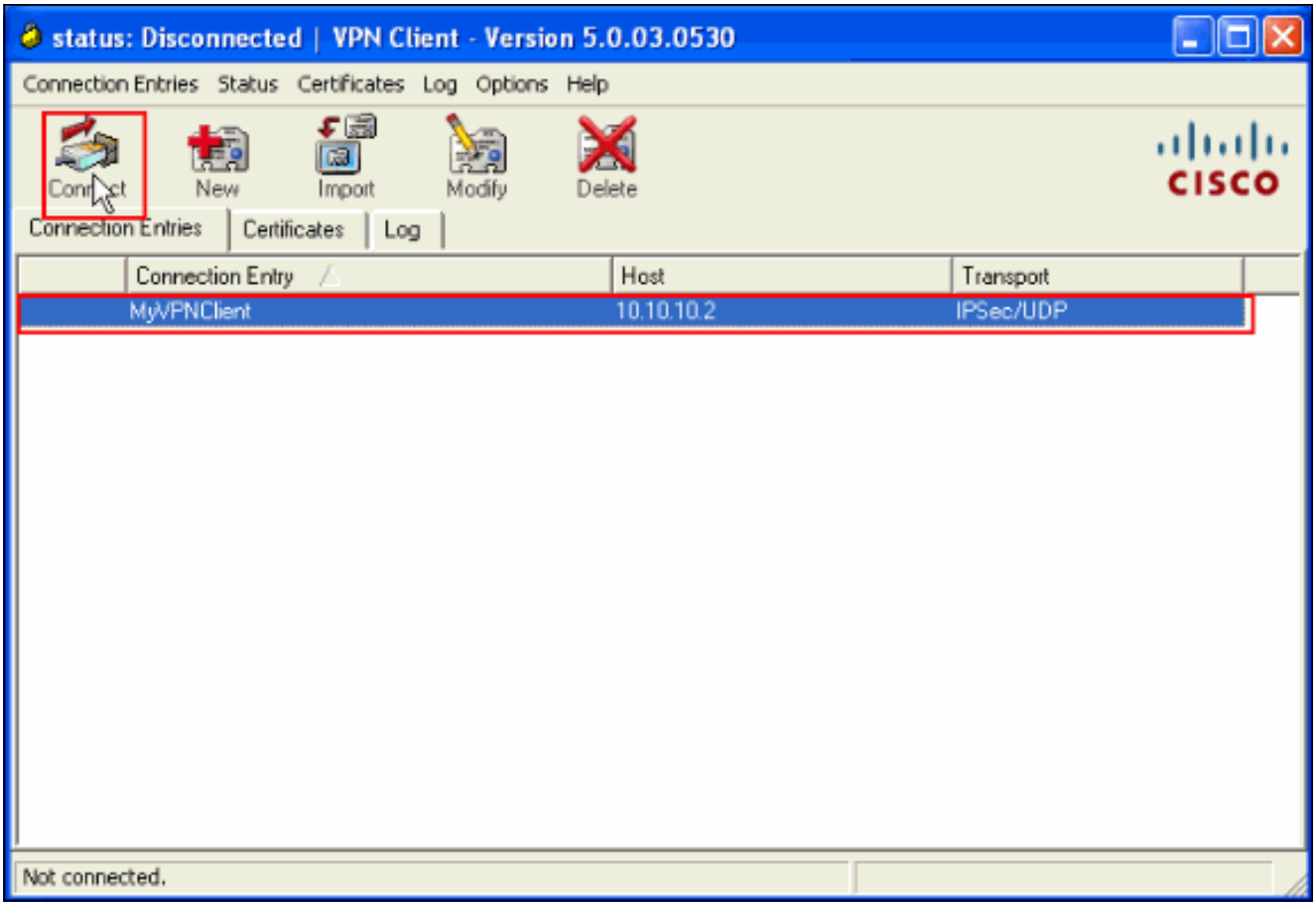


2. Complete la información de su nueva conexión.El campo del host debe contener la dirección IP o el nombre de host de Cisco previamente configurado ASA. La información de autenticación del grupo debe corresponder a eso usado en la **salvaguardia del** tecleo del **paso 4.** cuando le

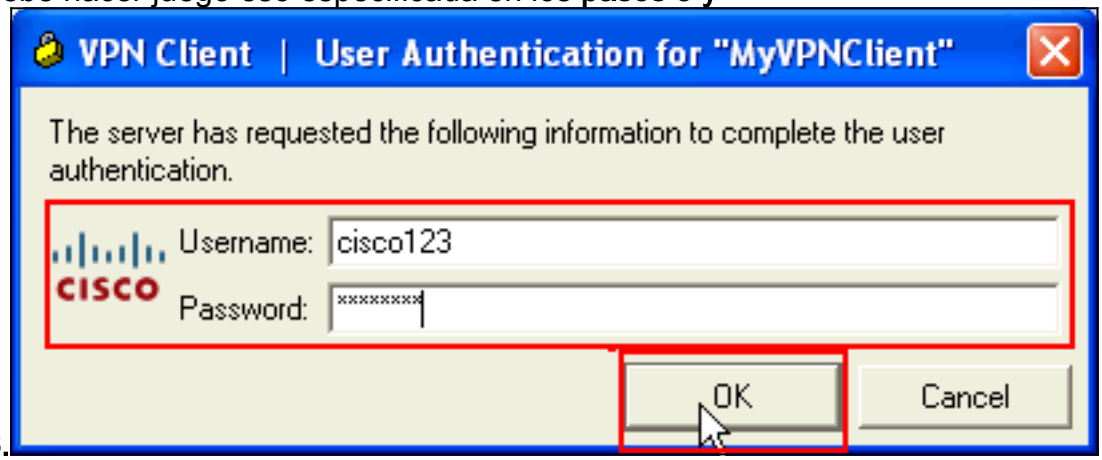


acaban.

3. Seleccione la conexión creada recientemente, y el haga clic en **Conectar**.

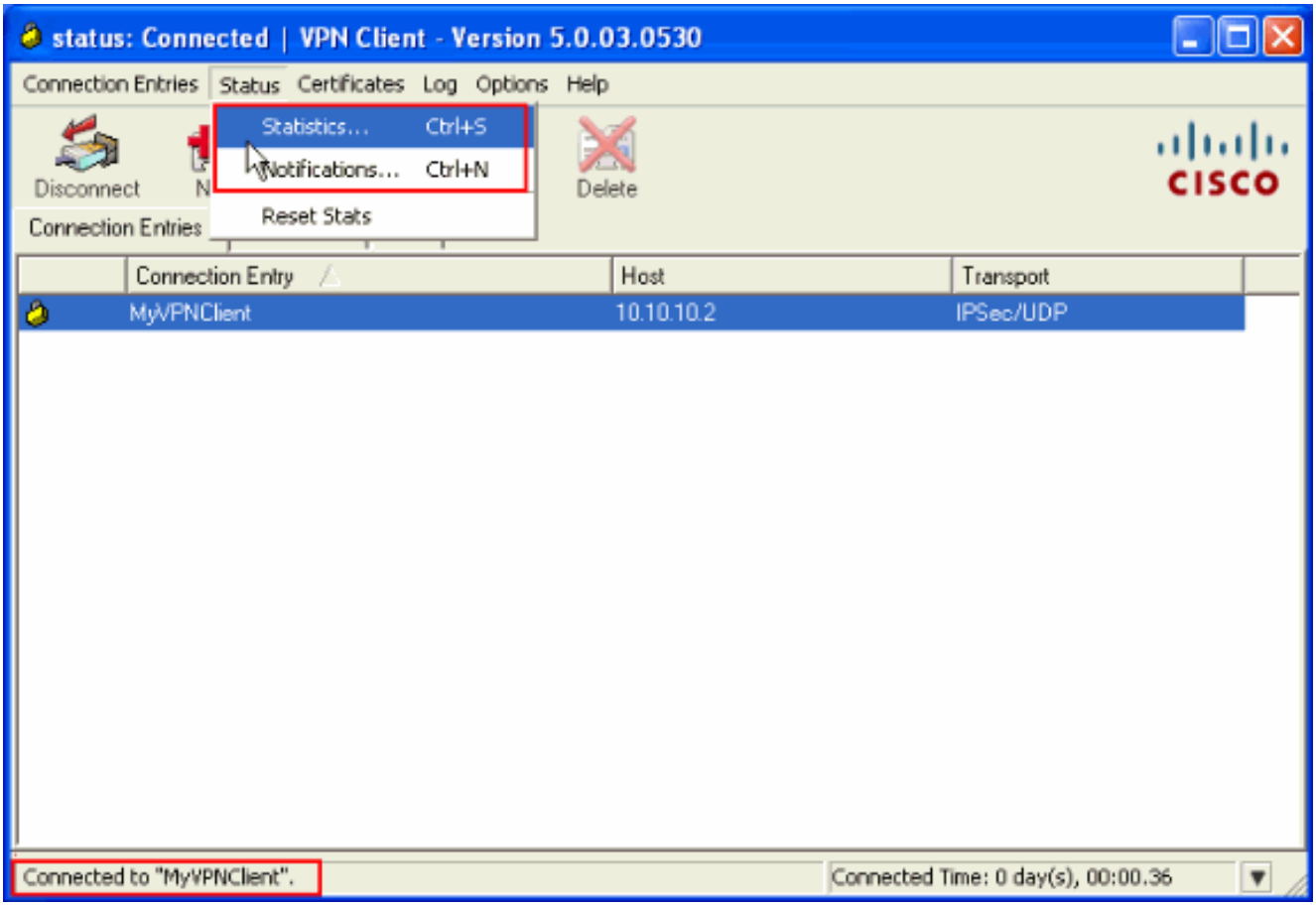


4. Ingrese un nombre de usuario y contraseña para la autenticación ampliada. Esta información debe hacer juego eso especificada en los **pasos 5 y**

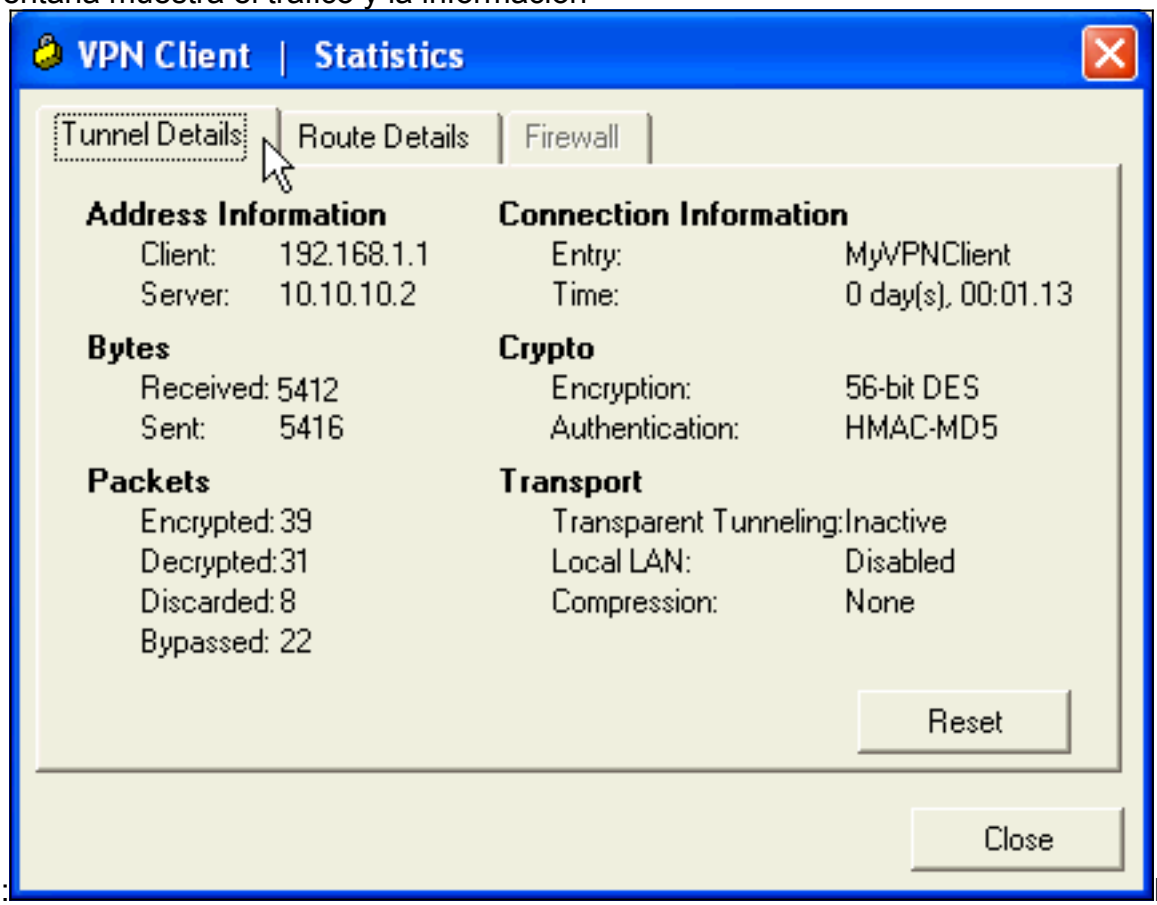


6.

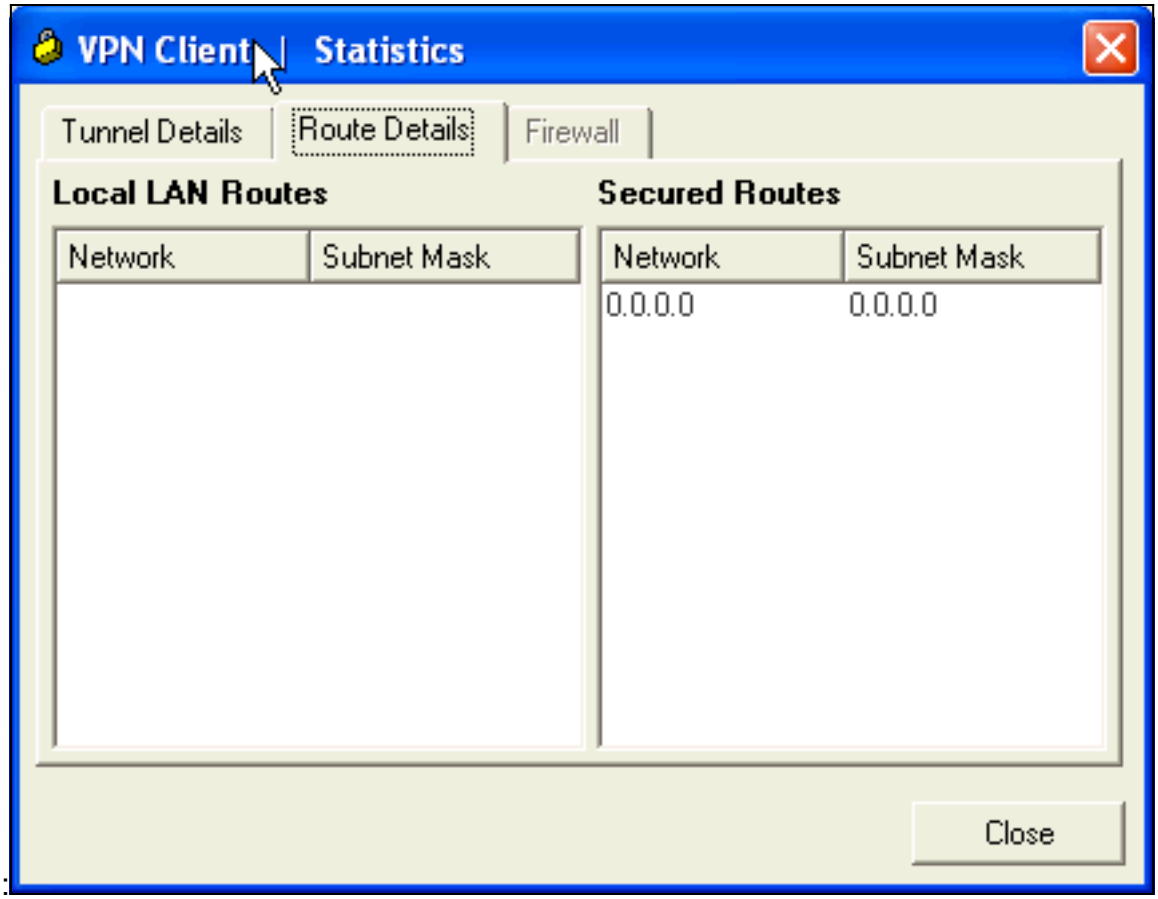
5. Una vez que la conexión se establece con éxito, elija las **estadísticas del** menú Status (Estado) para verificar los detalles del
túnel.



Esta ventana muestra el tráfico y la información



crypto: Esta ventana muestra la información de la tunelización

dividida: 

ASA/PIX dispositivo de seguridad - comandos show

- **show crypto isakmp sa** — Muestra todas las IKE SAs actuales en un par.ASA#**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: 10.10.10.1 Type : user Role : responder Rekey : no State : AM_ACTIVE
- **muestre IPSec crypto sa** — Muestra todo el SA de IPSec actual en un par.ASA#**show crypto ipsec sa** interface: Outside **Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: 10.10 .10.2 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0) current_peer: 10.10.10.1, username: cisco123 dynamic allocated peer ip: 192.168.1.1 #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20 #pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 20, #pkts comp failed: 0, #pkts decomp failed: 0** #pre-frag successes: 0, #pre-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.: 10.10.10.2, remote crypto endpt.: 10.10.10.1** path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: F49F954C inbound esp sas: spi: 0x3C10F9DD (1007745501) transform: esp-des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (sec): 27255 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xF49F954C (4104099148) transform: esp-des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (sec): 27255 IV size: 8 bytes replay detection support: Y
- ciscoasa(config)#**debug icmp trace** *!--- Inbound Nat Translation is shown below for Outside to Inside* **ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1** ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=7936 len=3 2 *!--- Inbound Nat Translation is shown below for Inside to Outside* **ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768** ICMP echo request from Outside:192.168.1.1 to inside:172.16.1.3 ID=768 seq=8192 len=32 ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1 ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=8192 len=3 2 ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768 ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8448 len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8448 len=32 ICMP echo

```
request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8704 len=32 ICMP echo reply from
172.16.1.2 to 192.168.1.1 ID=768 seq=8704 len=32 ICMP echo request from 192.168.1.1 to
172.16.1.2 ID=768 seq=8960 len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768
seq=8960 len=32
```

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

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.

Refiera a la mayoría del IPSec VPN común L2L y del Acceso Remoto que resuelve problemas las soluciones para más información sobre cómo resolver problemas el Sitio-sitio VPN.

Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco Adaptive Security Device Manager
- Alertas y Troubleshooting de Cisco ASA 5500 Series Adaptive Security Appliances
- Soporte Técnico y Documentación - Cisco Systems