Esempio di configurazione di PIX/ASA e VPN Client per VPN Internet pubblica su Memory Stick

Sommario

Introduzione

In questo documento viene descritto come configurare un'appliance ASA Security 7.2 e versioni successive per eseguire IPSec su una chiave. Questa configurazione è applicabile quando l'ASA non permette lo split tunneling e gli utenti si connettono direttamente all'ASA prima di potersi collegare a Internet.

Nota: nella versione 7.2 e successive di PIX/ASA, la parola chiave *intra-interface* permette a tutto il traffico di entrare e uscire dalla stessa interfaccia, e non solo al traffico IPsec.

Per completare una configurazione simile su un router del sito centrale, fare riferimento agli esempi di configurazione di router e client VPN per Internet pubblico su una Memory Stick.

Per ulteriori informazioni sullo scenario in cui il PIX hub reindirizza il traffico dal client VPN al PIX spoke, fare riferimento all'esempio di configurazione dell'autenticazione TACACS+ 7.x Enhanced Spoke-to-Client VPN.

Nota: per evitare una sovrapposizione di indirizzi IP nella rete, assegnare un pool di indirizzi IP

completamente diverso al client VPN (ad esempio, 10.x.x.x, 172.16.x.x e 192.168.x.x). Questo schema di indirizzamento IP è utile per risolvere i problemi relativi alla rete.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Hub PIX/ASA Security Appliance deve eseguire la versione 7.2 o successive
- Cisco VPN Client versione 5.x

Componenti usati

Le informazioni di questo documento si basano sulle versioni 8.0.2 e 5.0 di Cisco VPN Client per appliance di sicurezza PIX o ASA.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco PIX Security Appliance versione 7.2 e successive.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

Hairpinning o inversione a U

Questa funzionalità è utile per il traffico VPN che entra in un'interfaccia ma che viene quindi instradato all'esterno della stessa interfaccia. Ad esempio, se si dispone di una rete VPN hub e spoke, in cui l'appliance di sicurezza è l'hub, e le reti VPN remote sono spoke, affinché uno spoke comunichi con un altro spoke, il traffico deve passare all'appliance di sicurezza e quindi essere di nuovo indirizzato all'altro spoke.

Usare il comando **same-security-traffic** per consentire al traffico di entrare e uscire dalla stessa interfaccia.

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

Nota: il hairpinning o l'inversione a U è applicabile anche per la comunicazione tra client VPN e client VPN.

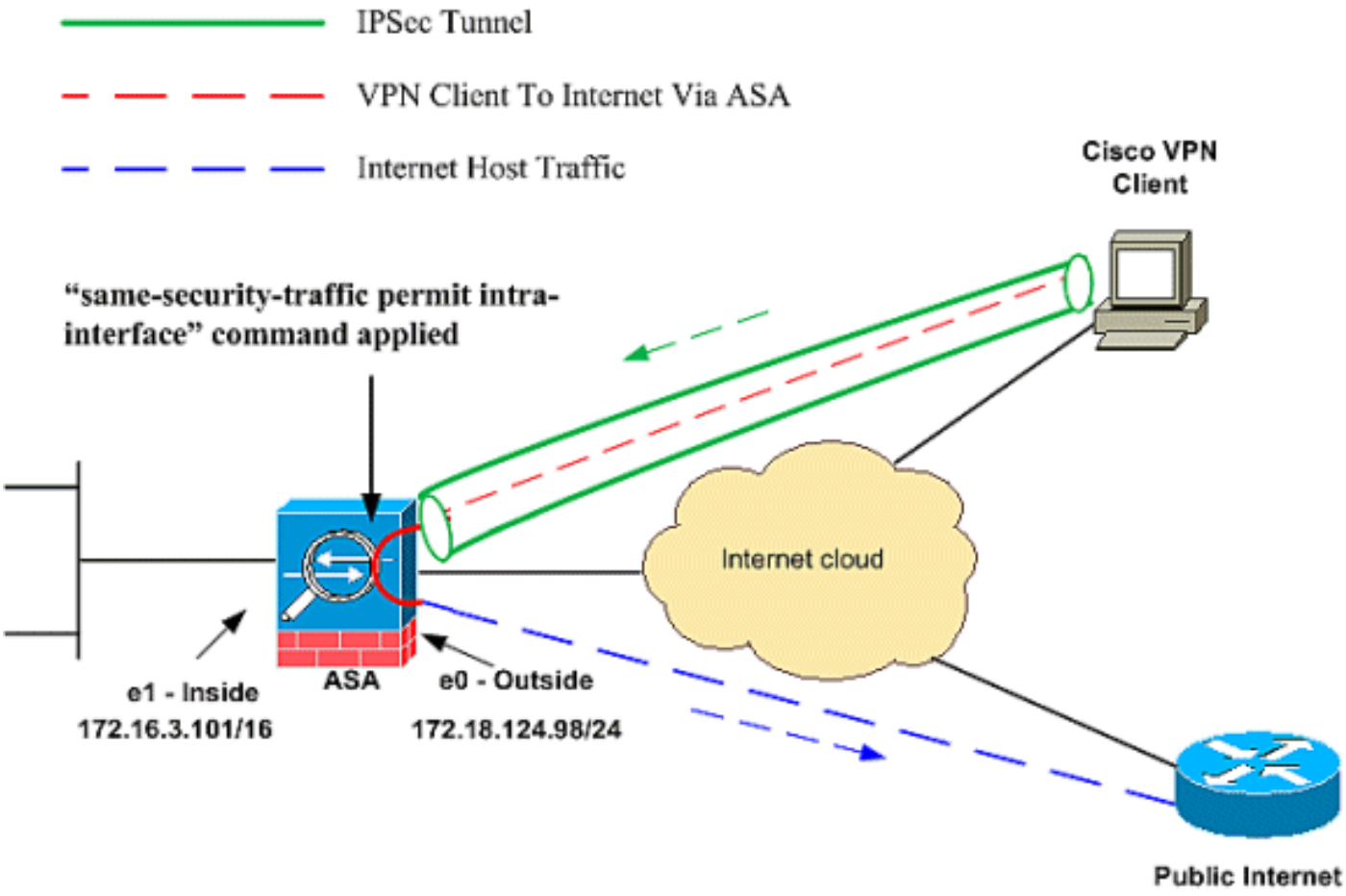
Configurazioni

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazione CLI di PIX/ASA

- PIX/ASA

Esegui configurazione su 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
```

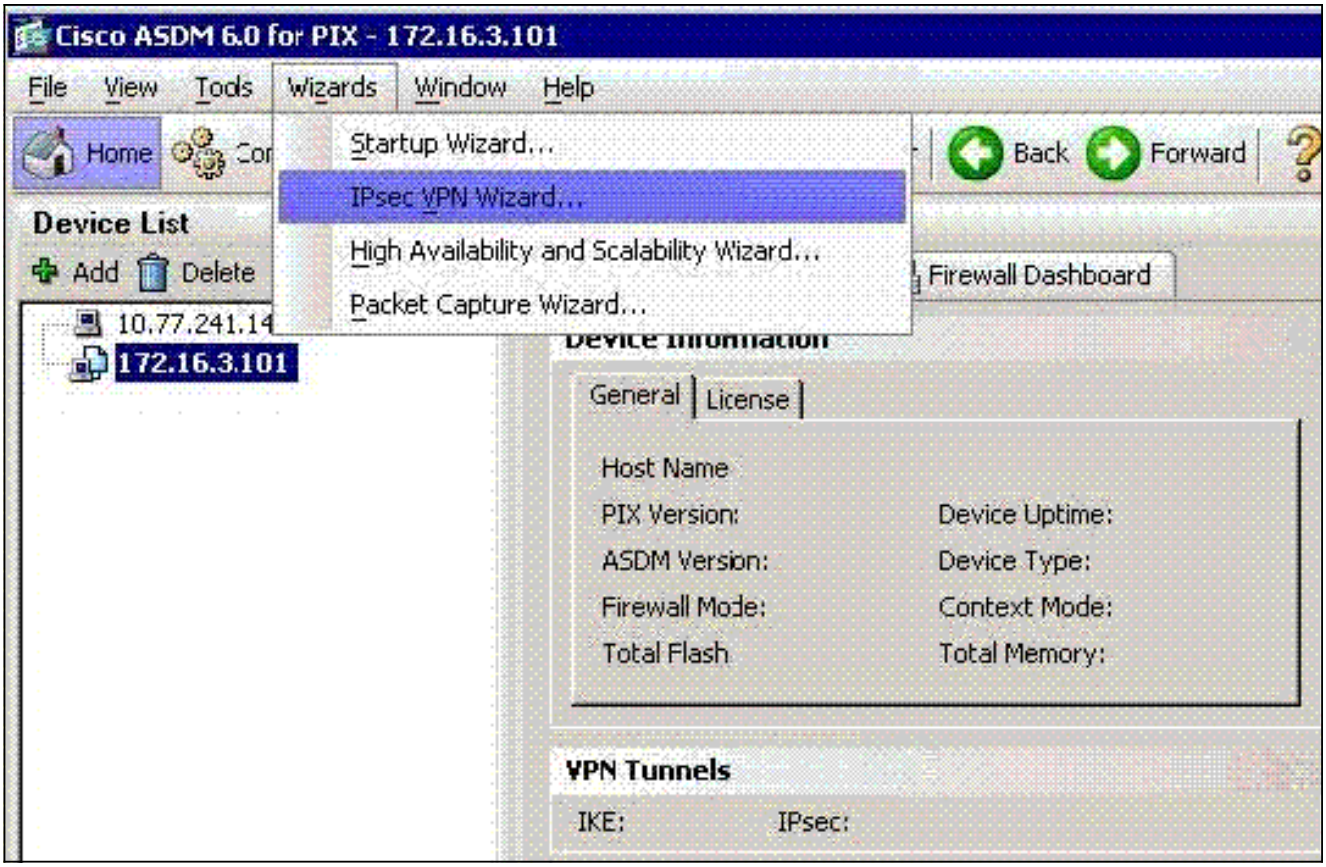
```
addresses from the vpn-pool). nat (outside) 1
192.168.10.0 255.255.255.0

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
```

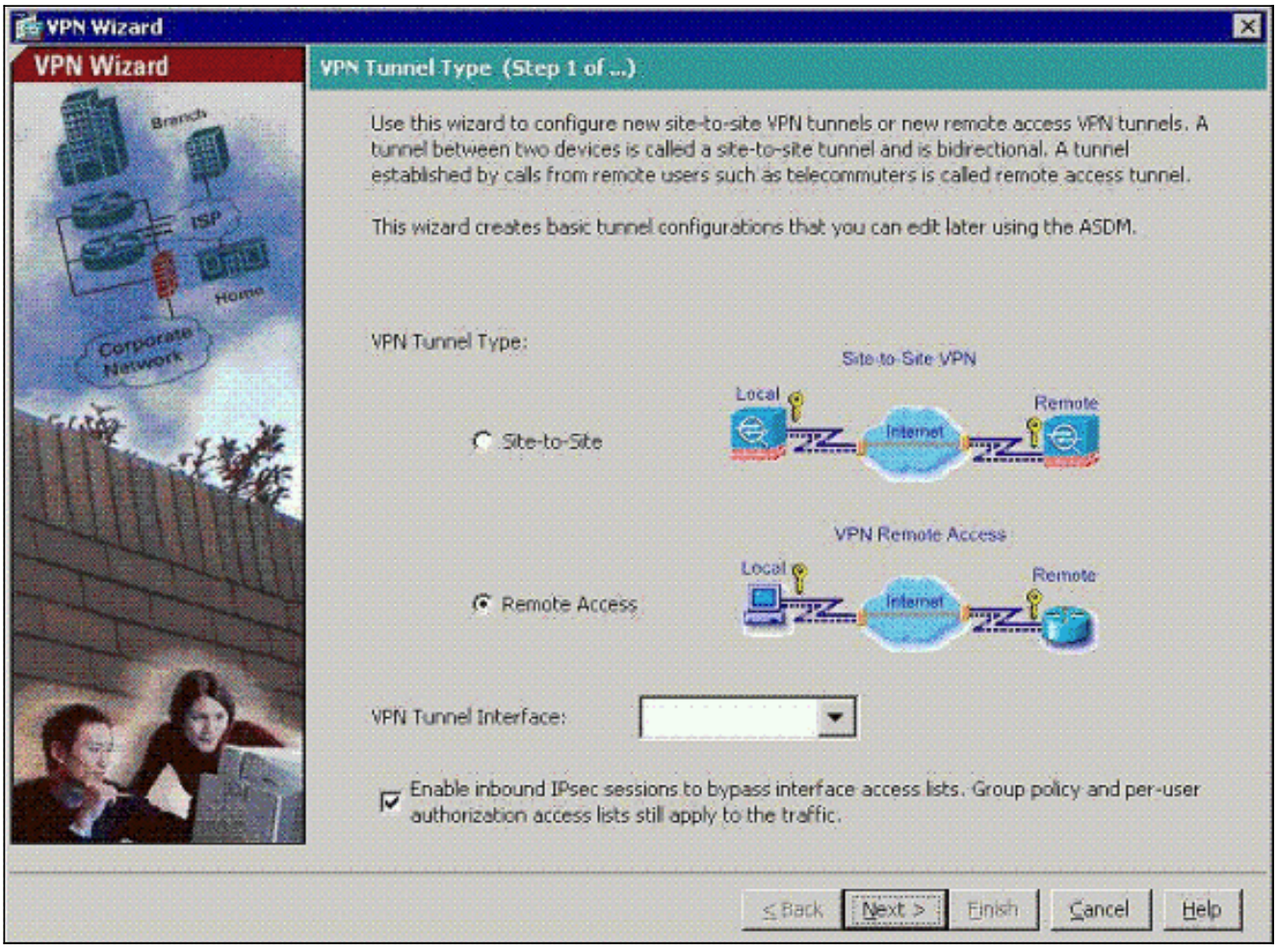
Configurazione di ASA/PIX con ASDM

Per configurare Cisco ASA come server VPN remoto con ASDM, completare la procedura seguente:

1. Scegliere **Procedure guidate > Creazione guidata VPN IPSec** dalla finestra Home.

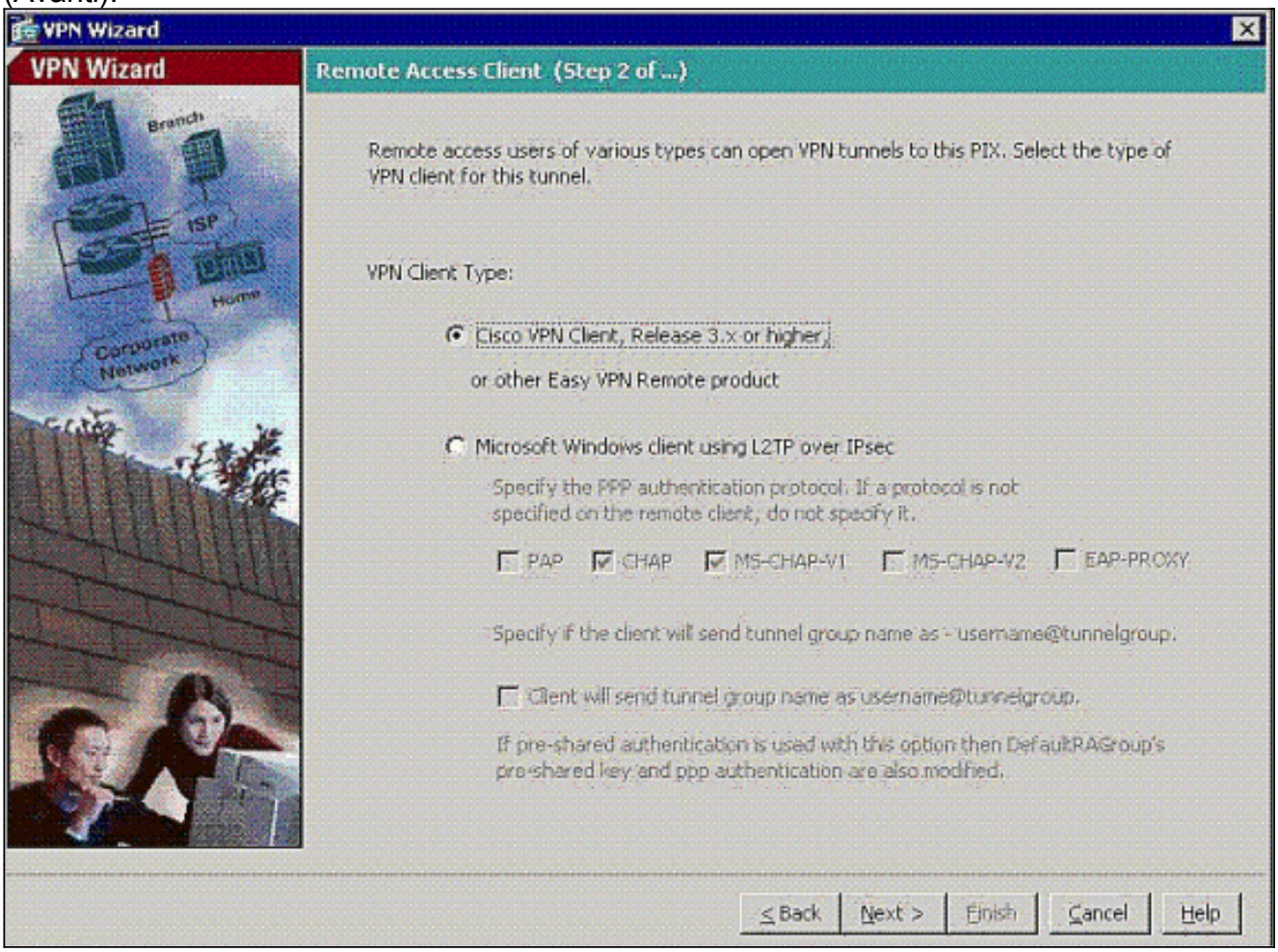


2. Scegliere il tipo di tunnel VPN di **accesso remoto** e verificare che l'interfaccia tunnel VPN sia impostata come
desiderato.

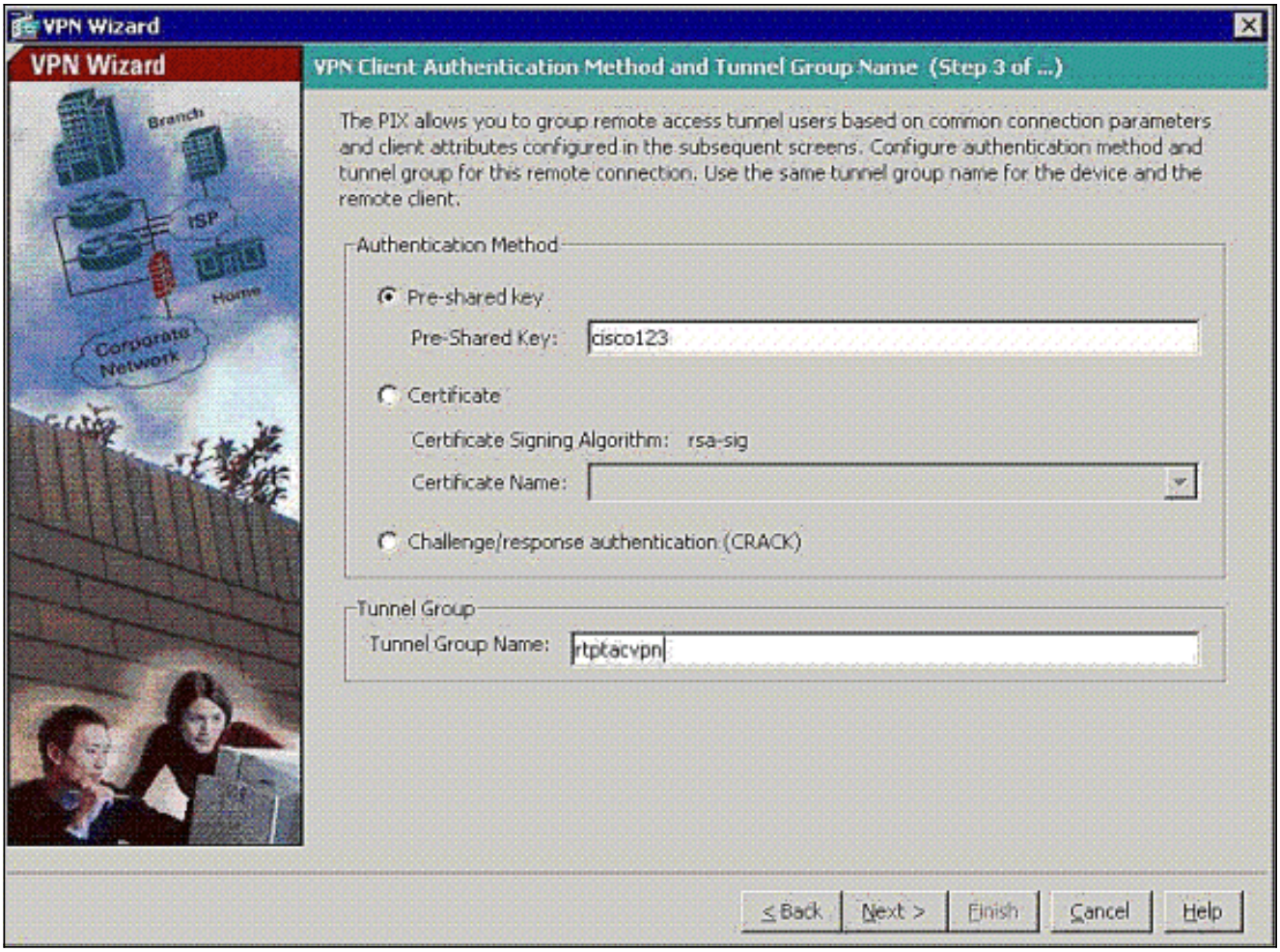


3. L'unico tipo di client VPN disponibile è già selezionato. Fare clic su **Next**

(Avanti).

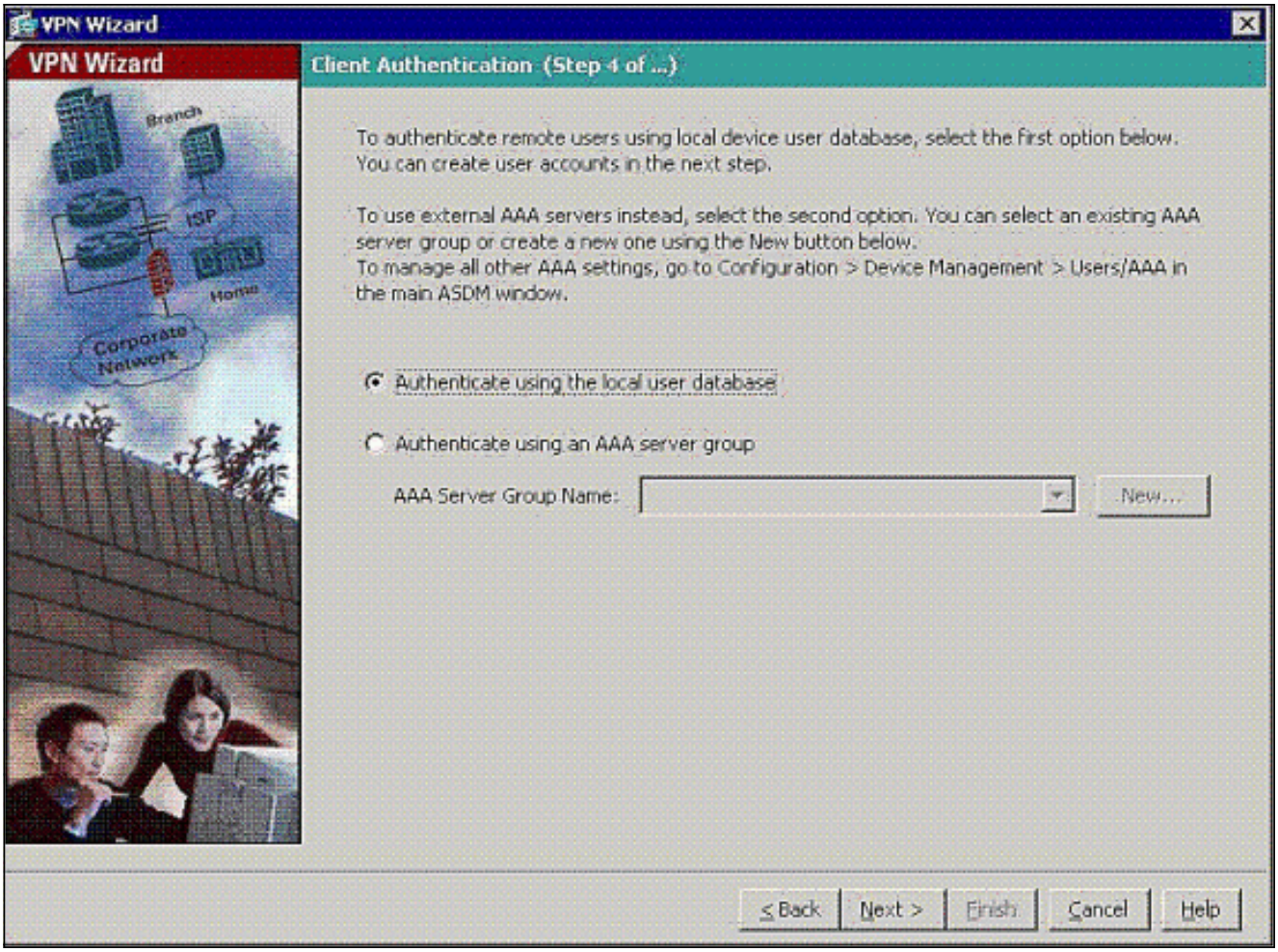


4. Immettere un nome per il nome del gruppo di tunnel. Specificare le informazioni di autenticazione da utilizzare.In questo esempio viene scelta la **chiave già condivisa**.

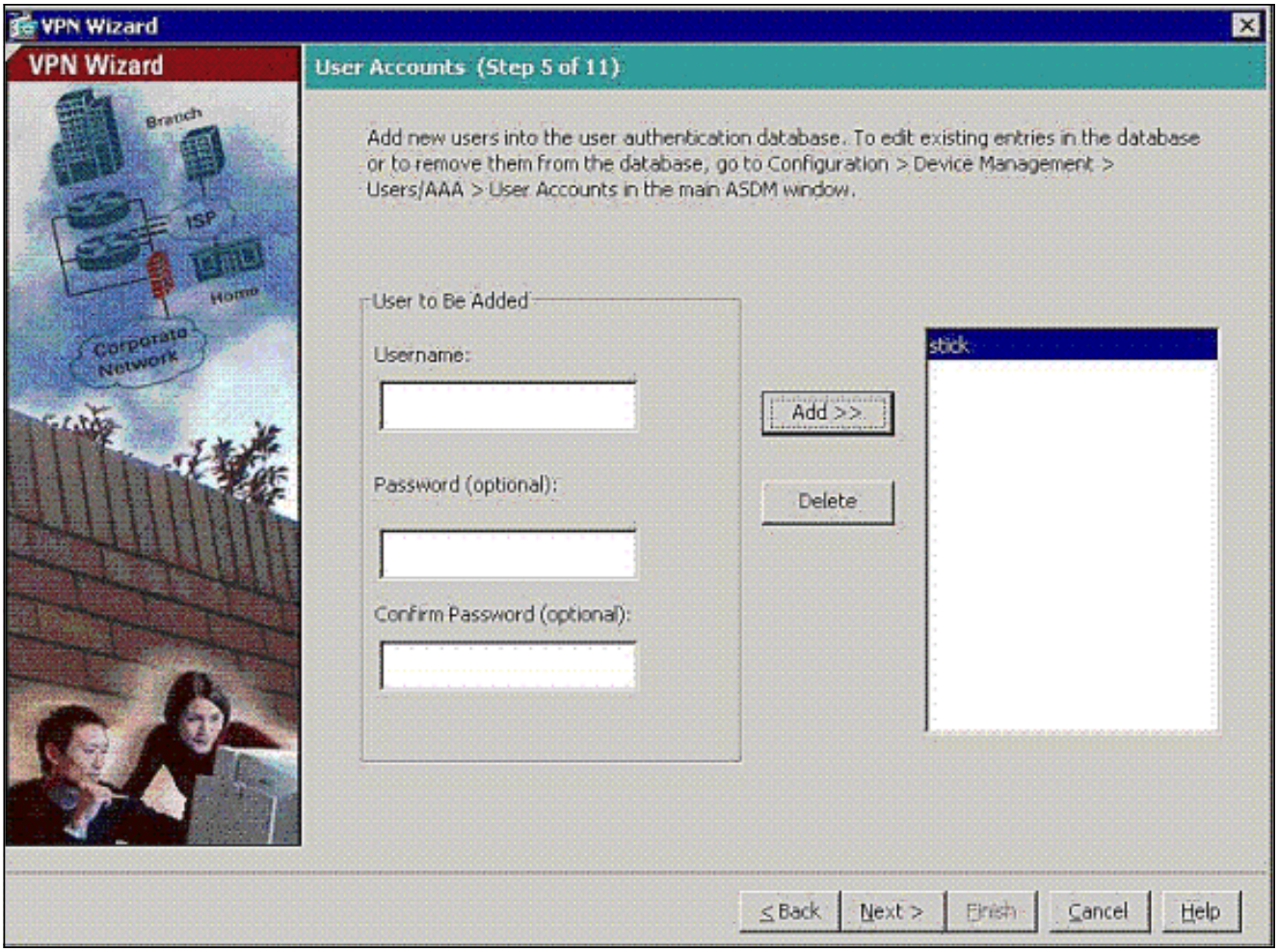


Nota: non è possibile nascondere/crittografare la chiave già condivisa sull'ASDM. Infatti, l'ASDM deve essere utilizzata solo da utenti che hanno configurato l'ASA o da utenti che hanno assistito il cliente nella configurazione.

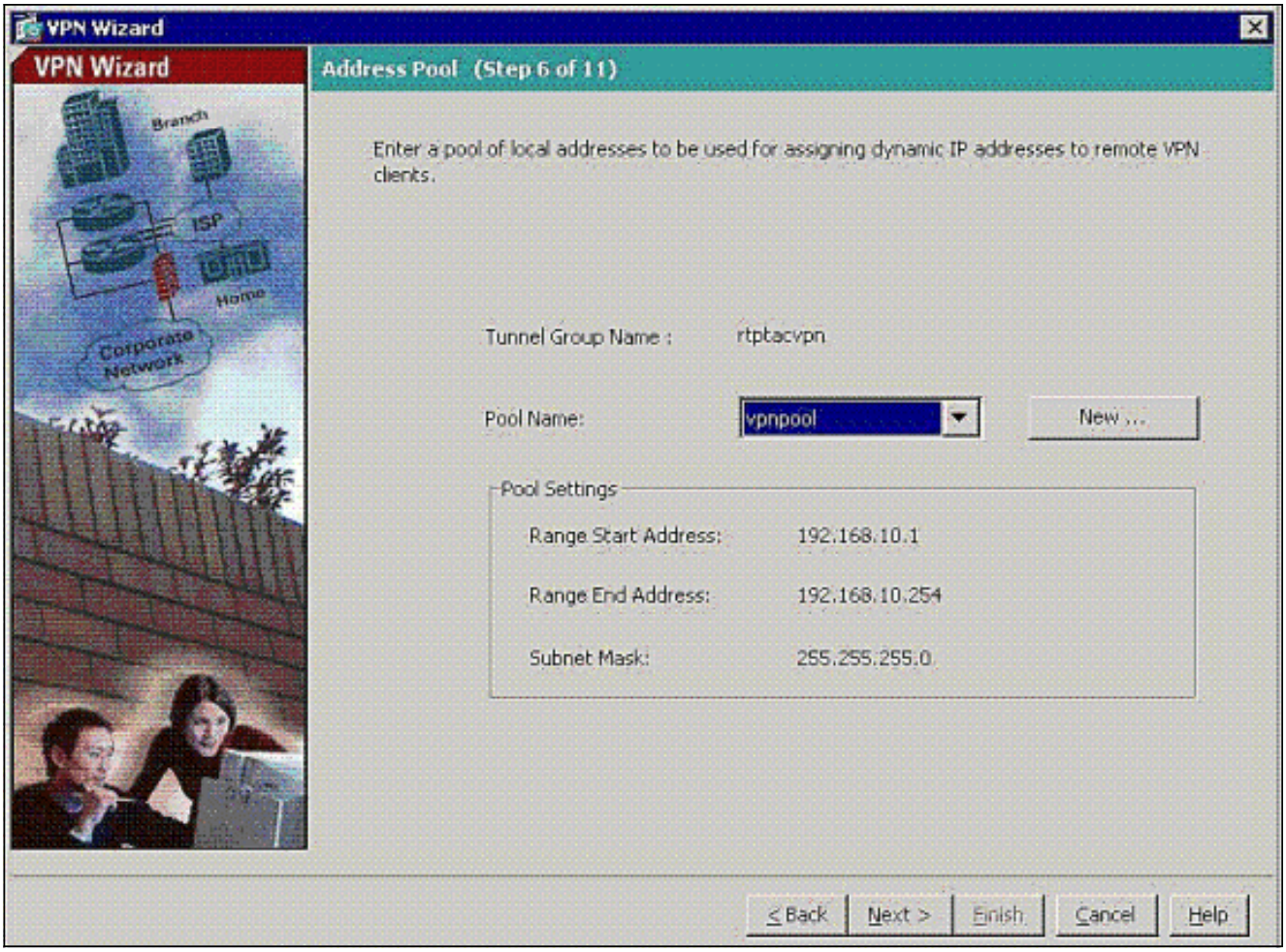
5. Specificare se si desidera che gli utenti remoti vengano autenticati nel database degli utenti locale o in un gruppo di server AAA esterno.**Nota:** aggiungere gli utenti al database locale nel passo 6.**Nota: per** informazioni su come configurare un gruppo di server AAA esterno tramite ASDM, fare riferimento all'esempio di configurazione dell'autenticazione e dell'autorizzazione PIX/ASA 7.x per utenti VPN tramite
ASDM.



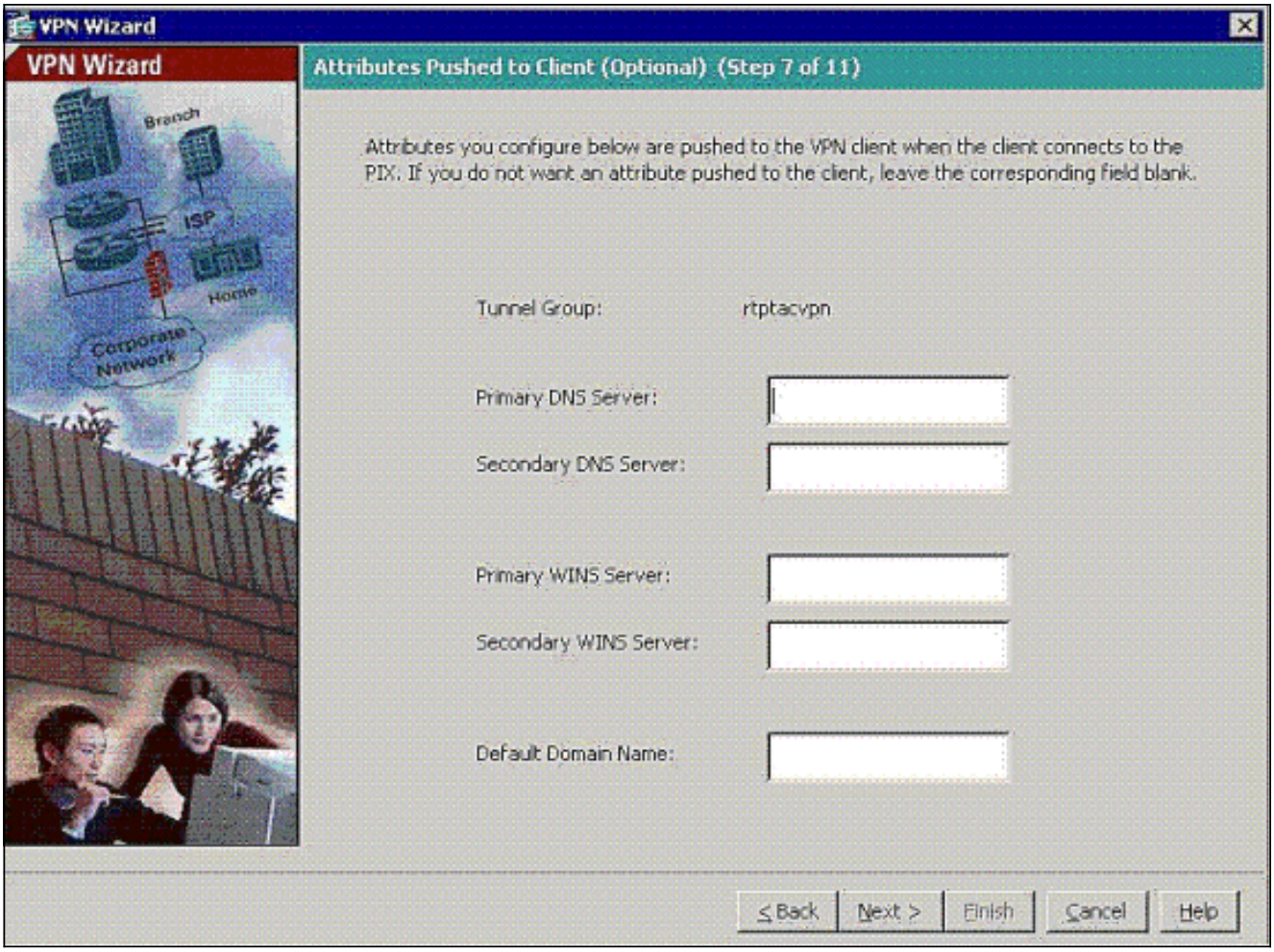
6. Se necessario, aggiungere utenti al database locale.**Nota:** non rimuovere gli utenti correnti da questa finestra. Scegliere **Configurazione > Amministrazione dispositivi > Amministrazione > Account utente nella finestra principale di ASDM** per modificare le voci esistenti nel database o rimuoverle dal
database.



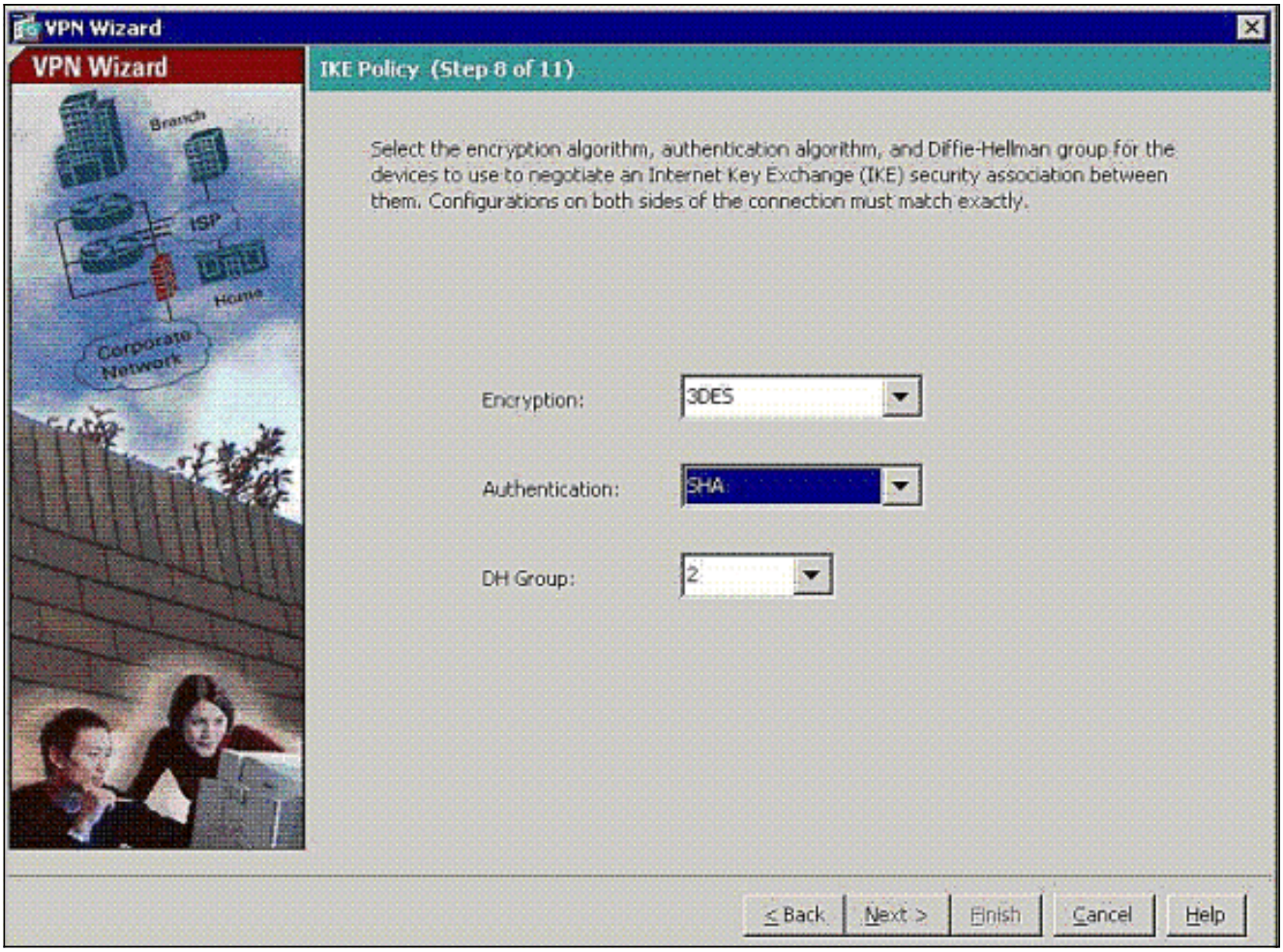
7. Definire un pool di indirizzi locali da assegnare dinamicamente ai client VPN remoti quando si
connettono.



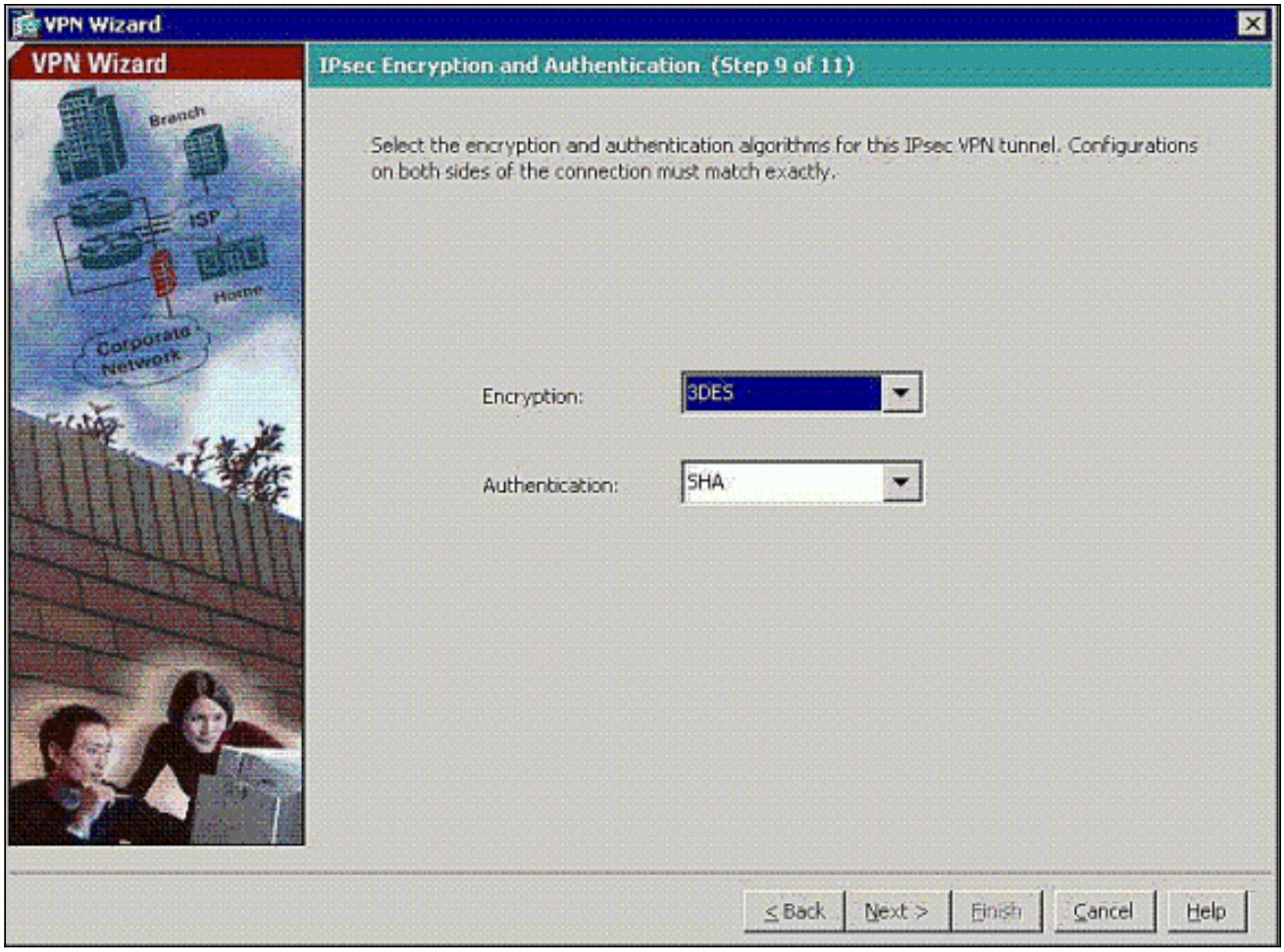
8. *Facoltativo:* Specificare le informazioni sui server DNS e WINS e un nome di dominio predefinito da inserire nei client VPN
remoti.



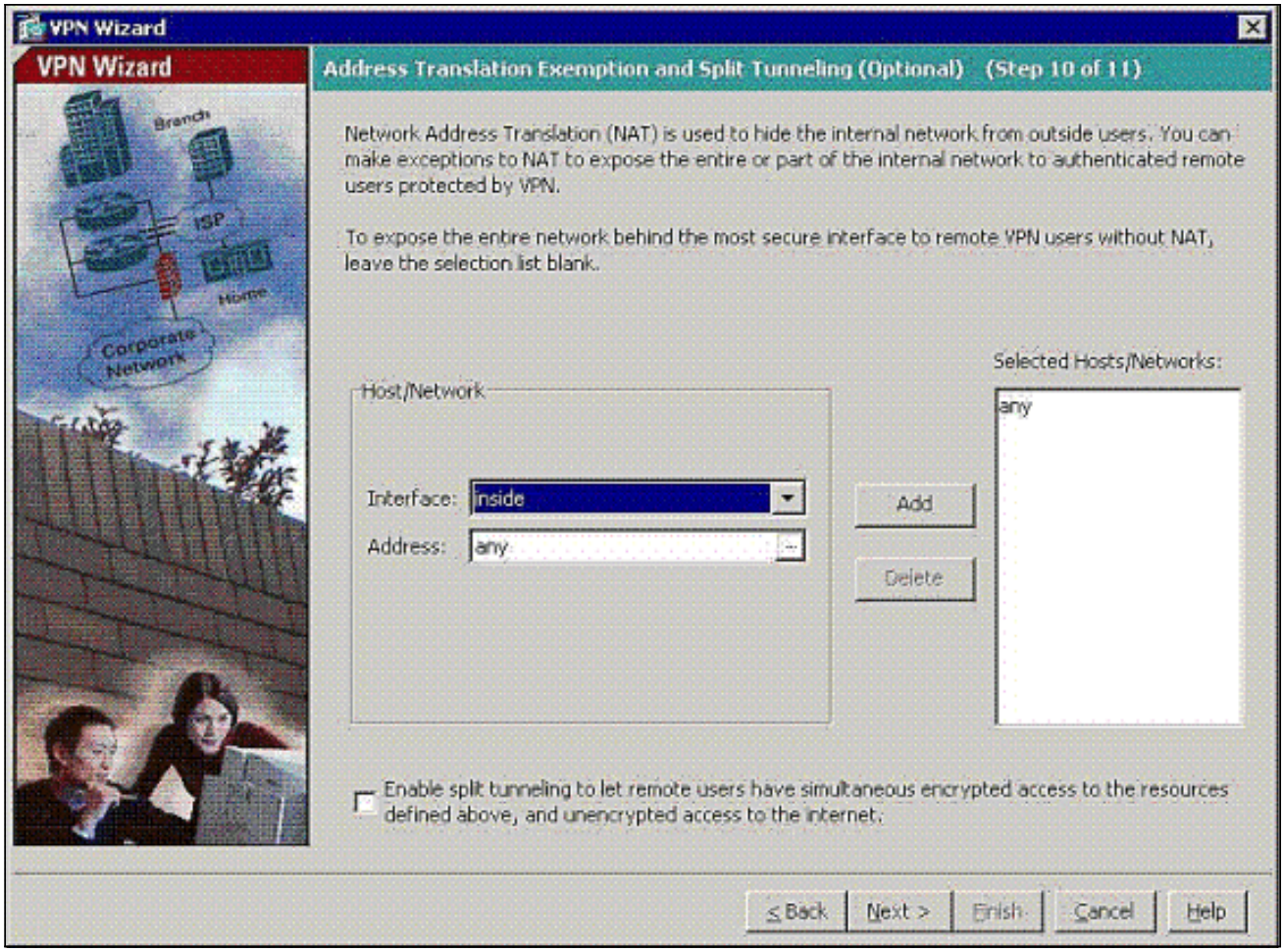
9. Specificare i parametri per IKE, noto anche come IKE fase 1.Le configurazioni su entrambi i lati del tunnel devono corrispondere esattamente, ma il client VPN Cisco sceglie automaticamente la configurazione appropriata per se stesso. Sul PC client non è necessaria alcuna configurazione
   IKE.



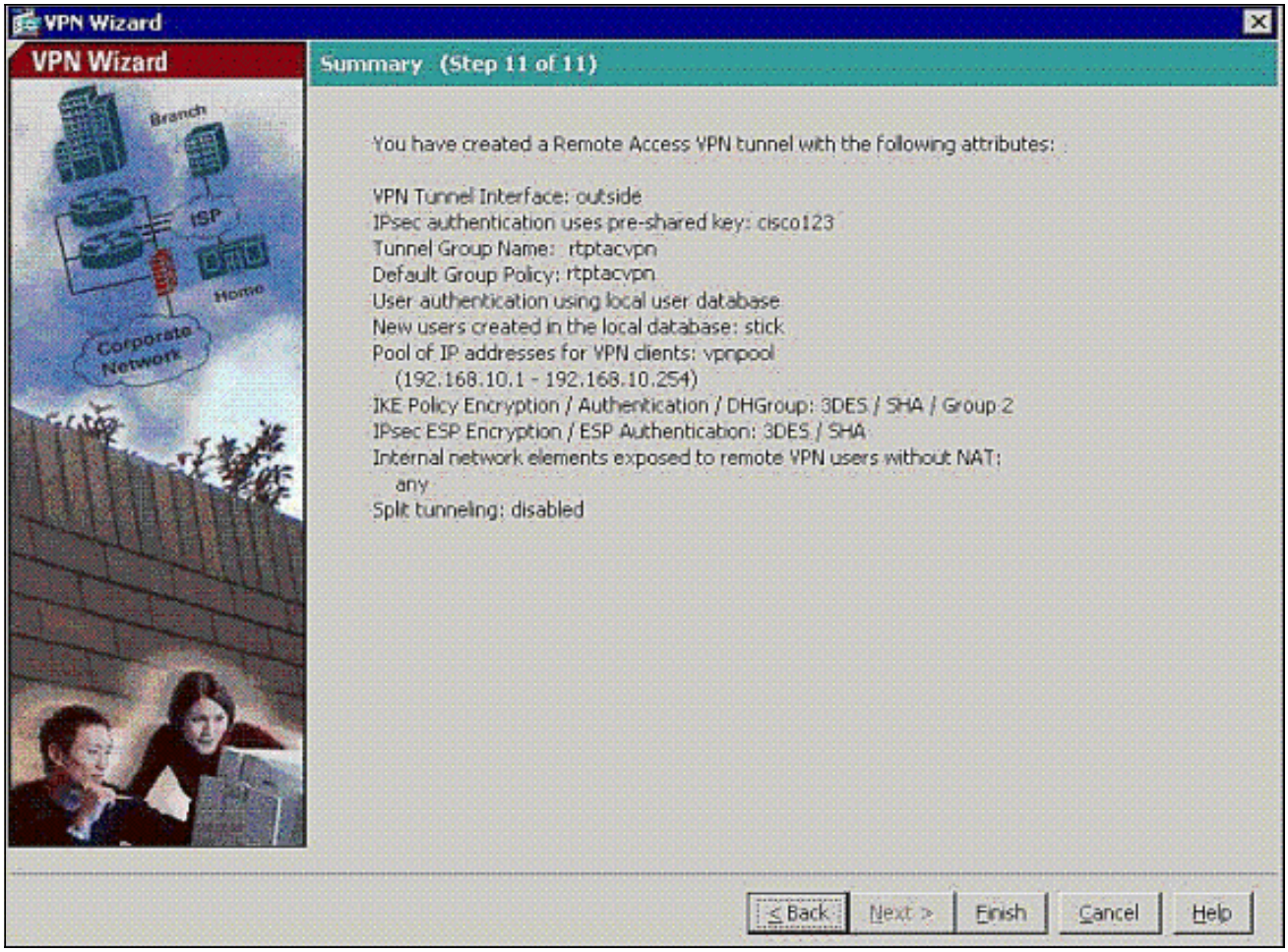
10. Specificare i parametri per IPSec, noto anche come IKE fase 2.Le configurazioni su entrambi i lati del tunnel devono corrispondere esattamente, ma il client VPN Cisco sceglie automaticamente la configurazione appropriata per se stesso. Sul PC client non è necessaria alcuna configurazione
    IKE.



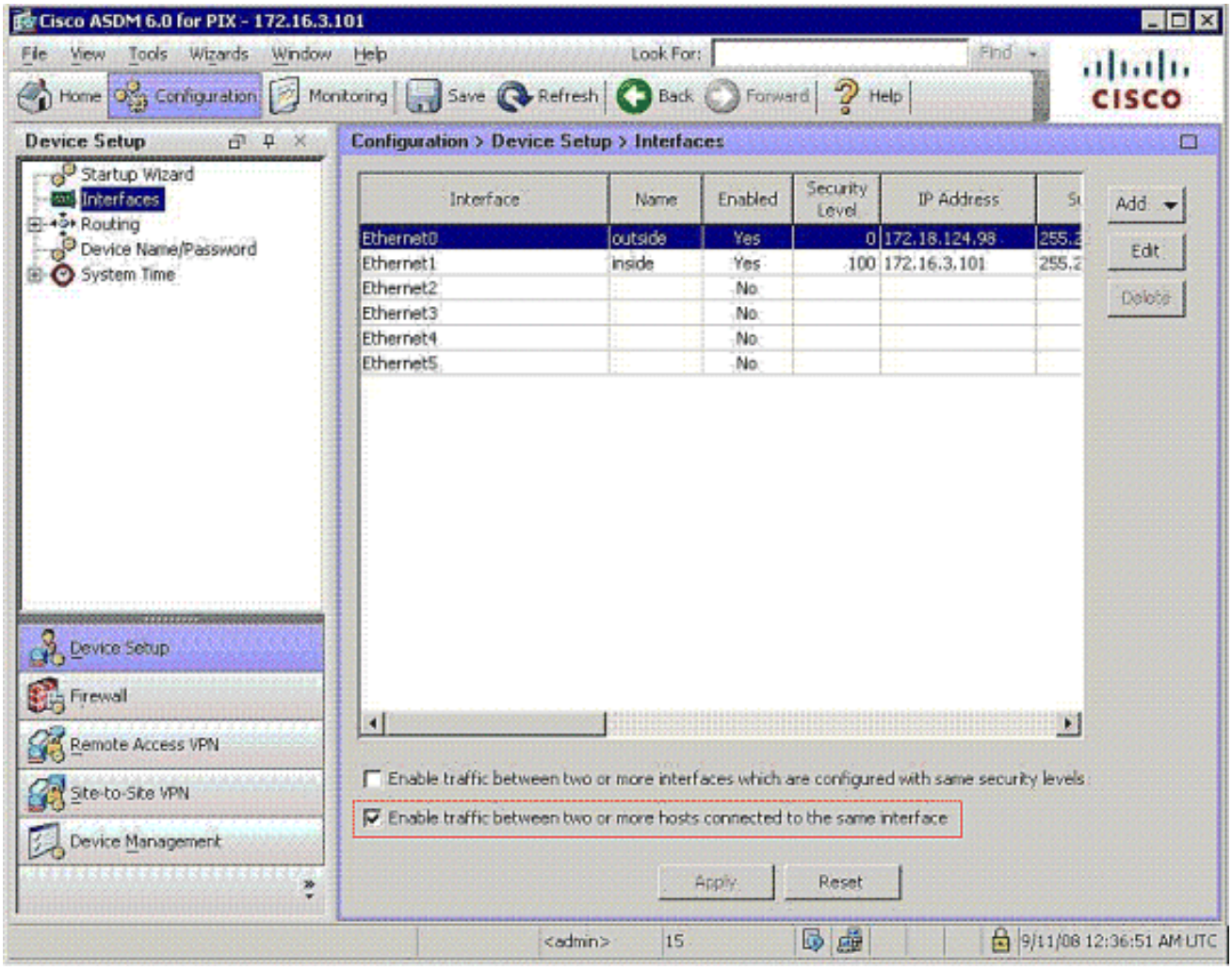
11. Specificare gli eventuali host interni o reti che possono essere esposti agli utenti VPN remoti.Se si lascia vuoto questo elenco, gli utenti VPN remoti possono accedere all'intera rete interna dell'appliance ASA.In questa finestra è anche possibile abilitare il tunneling suddiviso. Il tunneling ripartito cripta il traffico diretto alle risorse definite in precedenza in questa procedura e fornisce l'accesso non crittografato a Internet in senso lato evitando il tunneling del traffico. Se il tunneling suddiviso *non* è abilitato, tutto il traffico proveniente dagli utenti VPN remoti viene tunneling verso l'appliance ASA. In base alla configurazione, questa operazione può richiedere un uso intensivo della larghezza di banda e del processore.



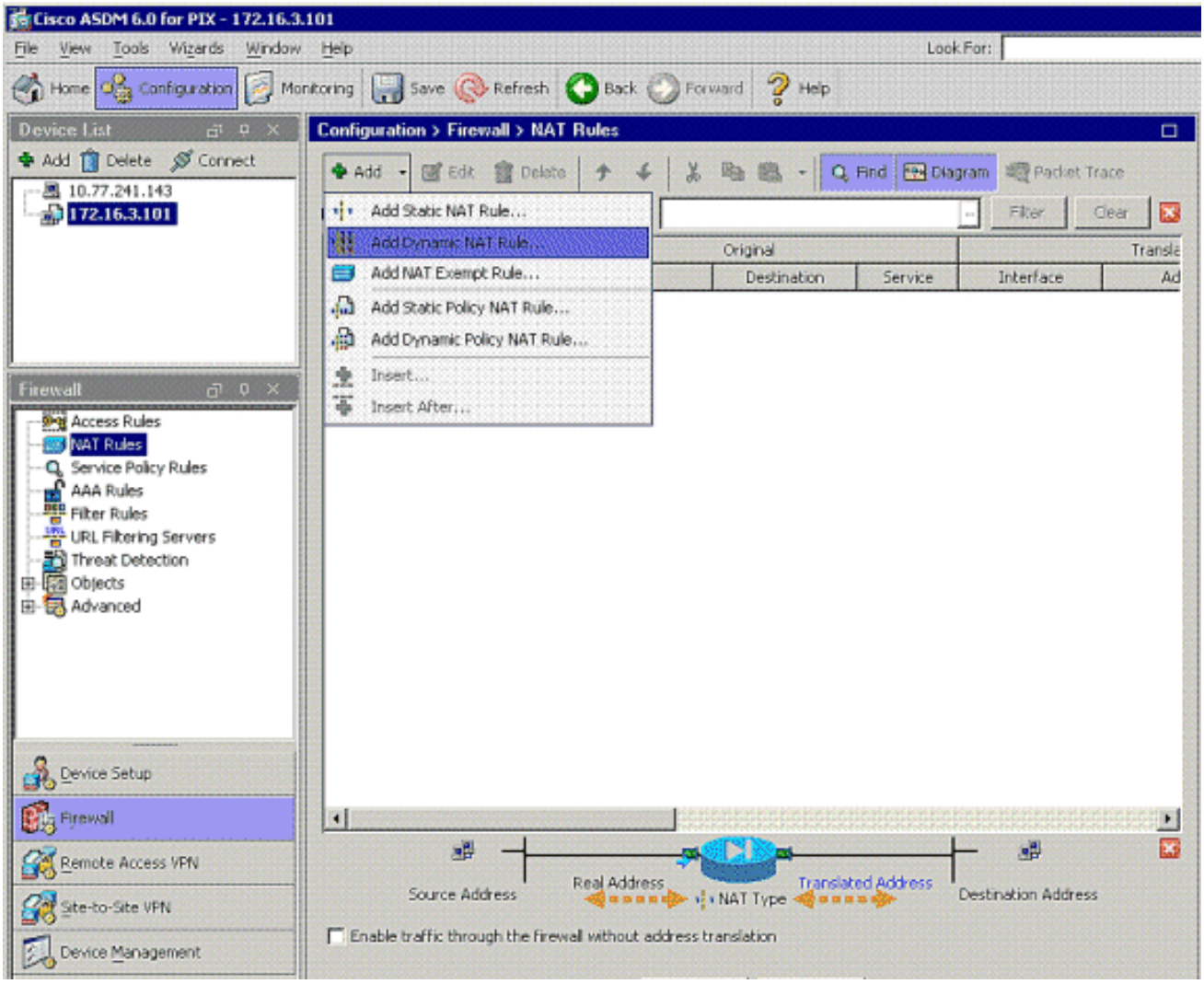
12. Questa finestra mostra un riepilogo delle azioni intraprese. Se la configurazione è soddisfacente, fare clic su
Fine.



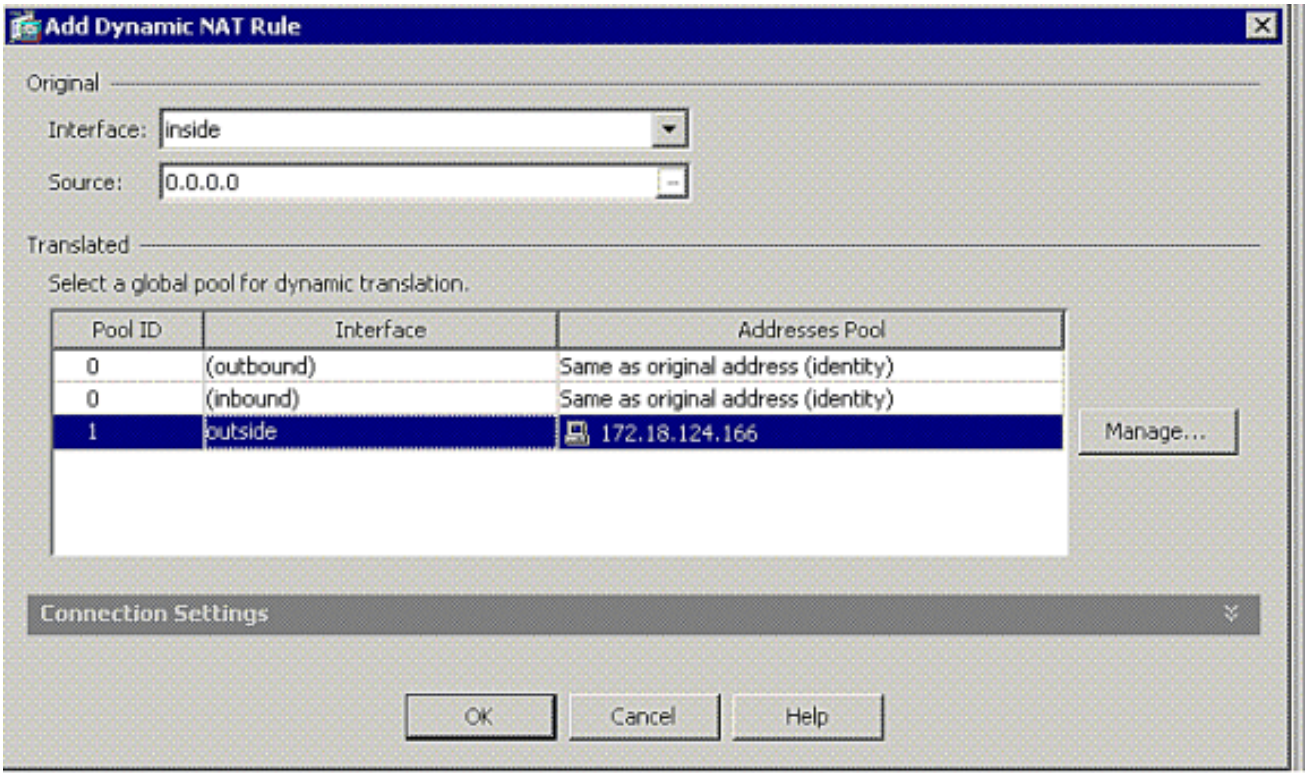
13. Configurare il comando **same-security-traffic** per abilitare il traffico tra due o più host connessi alla stessa interfaccia quando si seleziona la casella di controllo come mostrato:



14. Scegliere **Configurazione > Firewall > Regole NAT**, quindi fare clic su **Aggiungi regola NAT dinamica** per creare questa traduzione dinamica con l'uso di ASDM.

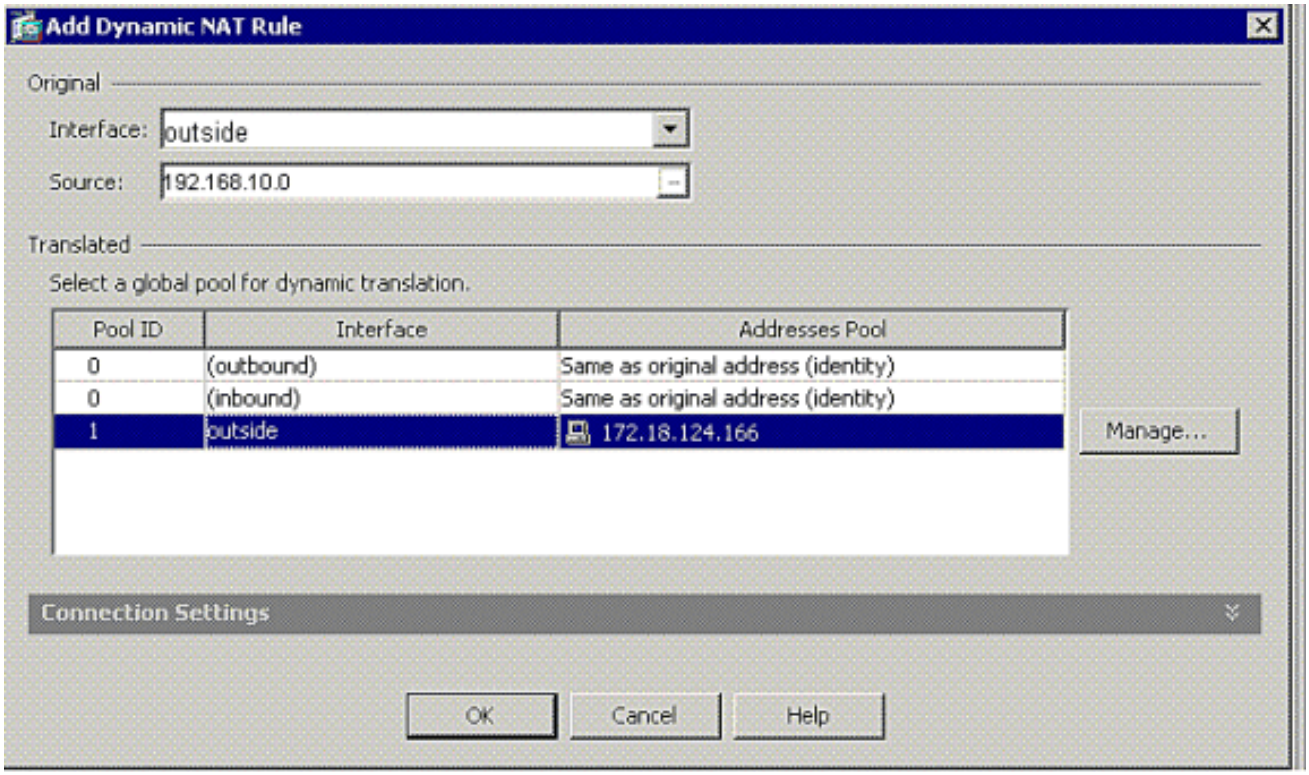


15. Scegliere **inside** come interfaccia di origine e immettere gli indirizzi che si desidera utilizzare per NAT. Per Traduci indirizzo su interfaccia, scegliete **esterno** e fate clic su **OK**.

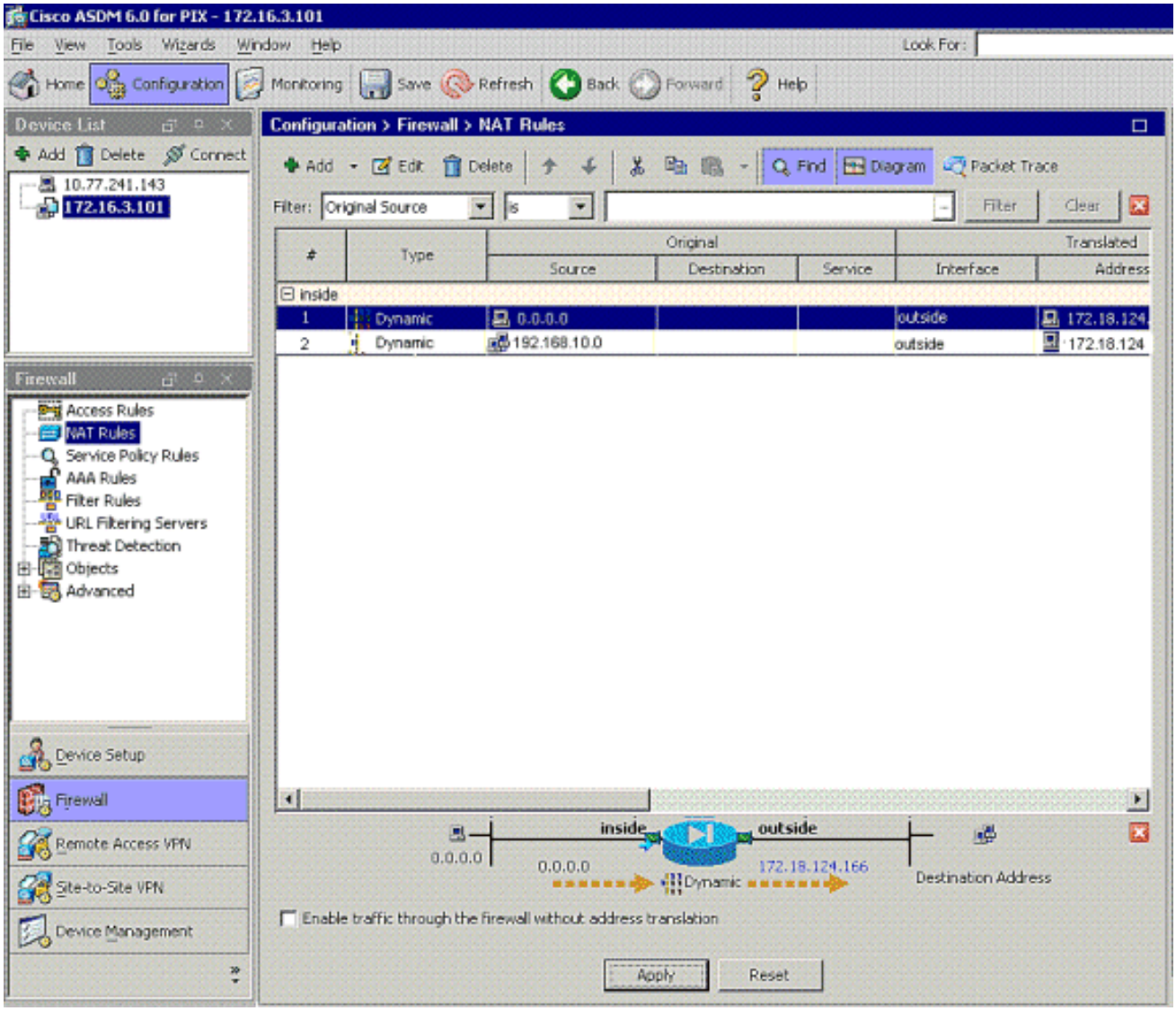


16. Scegliere **esterno** come interfaccia di origine e immettere gli indirizzi che si desidera utilizzare per NAT. Per Traduci indirizzo su interfaccia, scegliete **esterno** e fate clic su

OK.



17. La traduzione viene visualizzata in Regole di conversione in **Configurazione > Firewall > Regole NAT**.



Nota 1: È necessario configurare il comando [syspot connection allow-vpn](). Il comando [show running-config syspot]() verifica se è configurato.

Nota 2: Aggiungere questo output per il trasporto UDP opzionale:

```
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: Configurare questo comando nella configurazione globale dell'accessorio PIX per consentire ai client VPN di connettersi tramite IPsec su TCP:

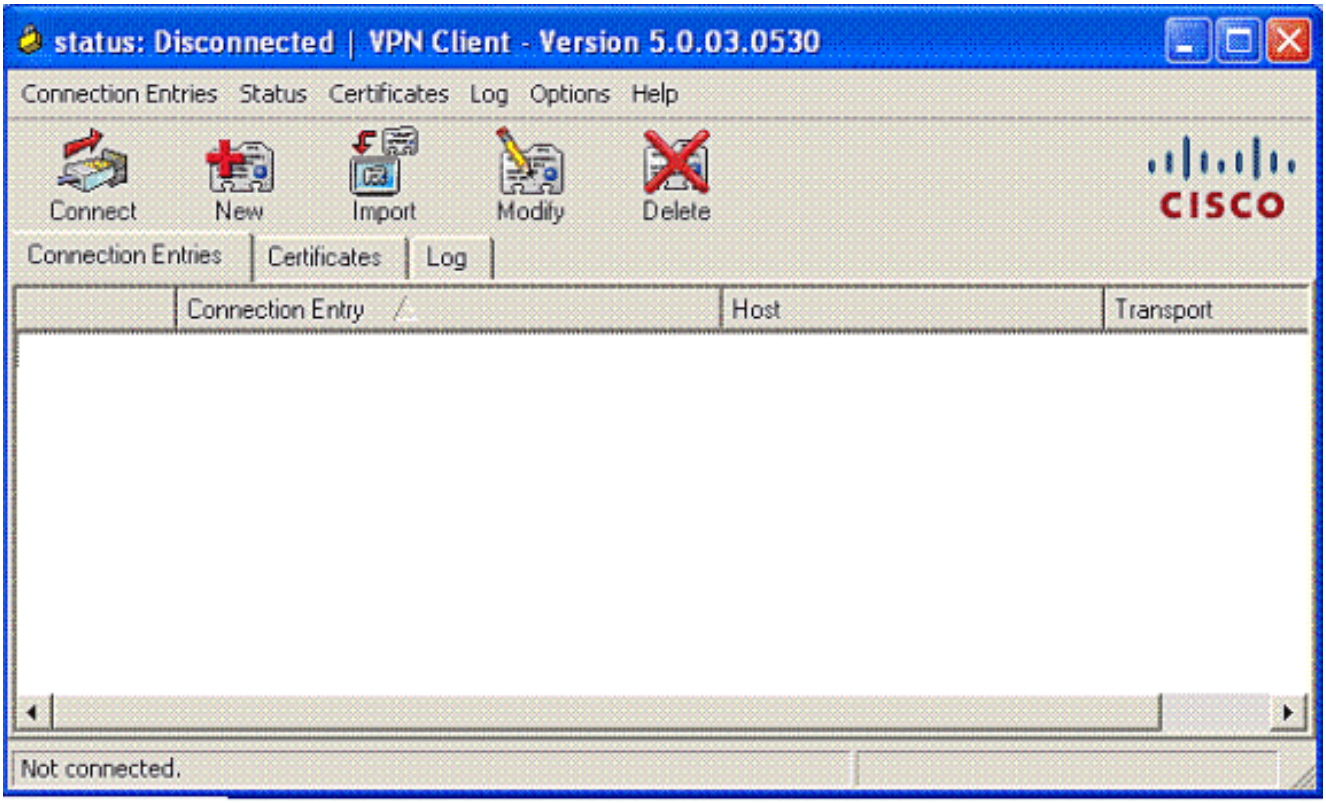
```
isakmp ipsec-over-tcp port 10000
```

Nota: fare riferimento al video Hair-Pinning su Cisco ASA per ulteriori informazioni su diversi scenari in cui è possibile utilizzare lo hair-pinning.

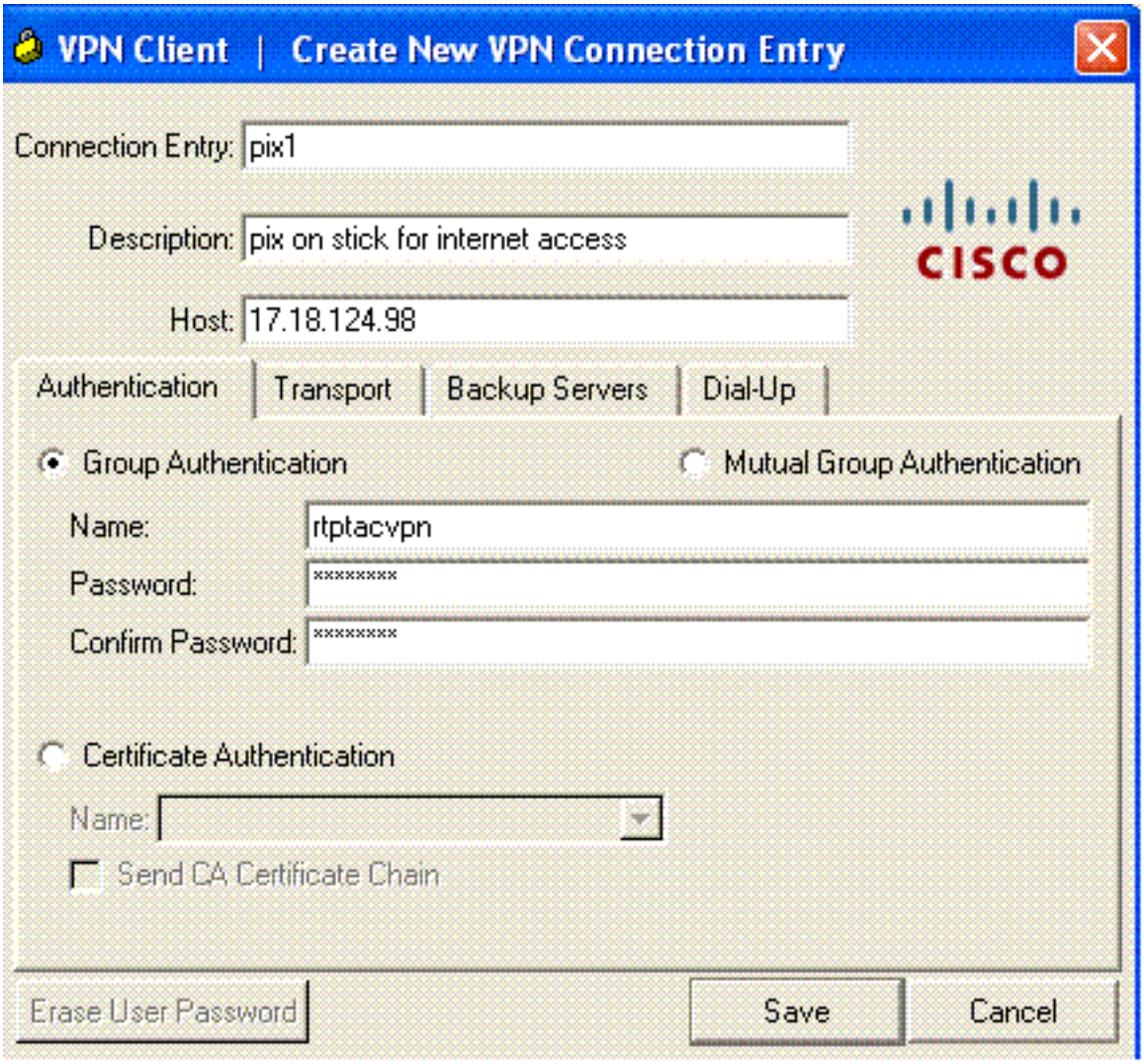
Configurazione client VPN

Completare questa procedura per configurare il client VPN:

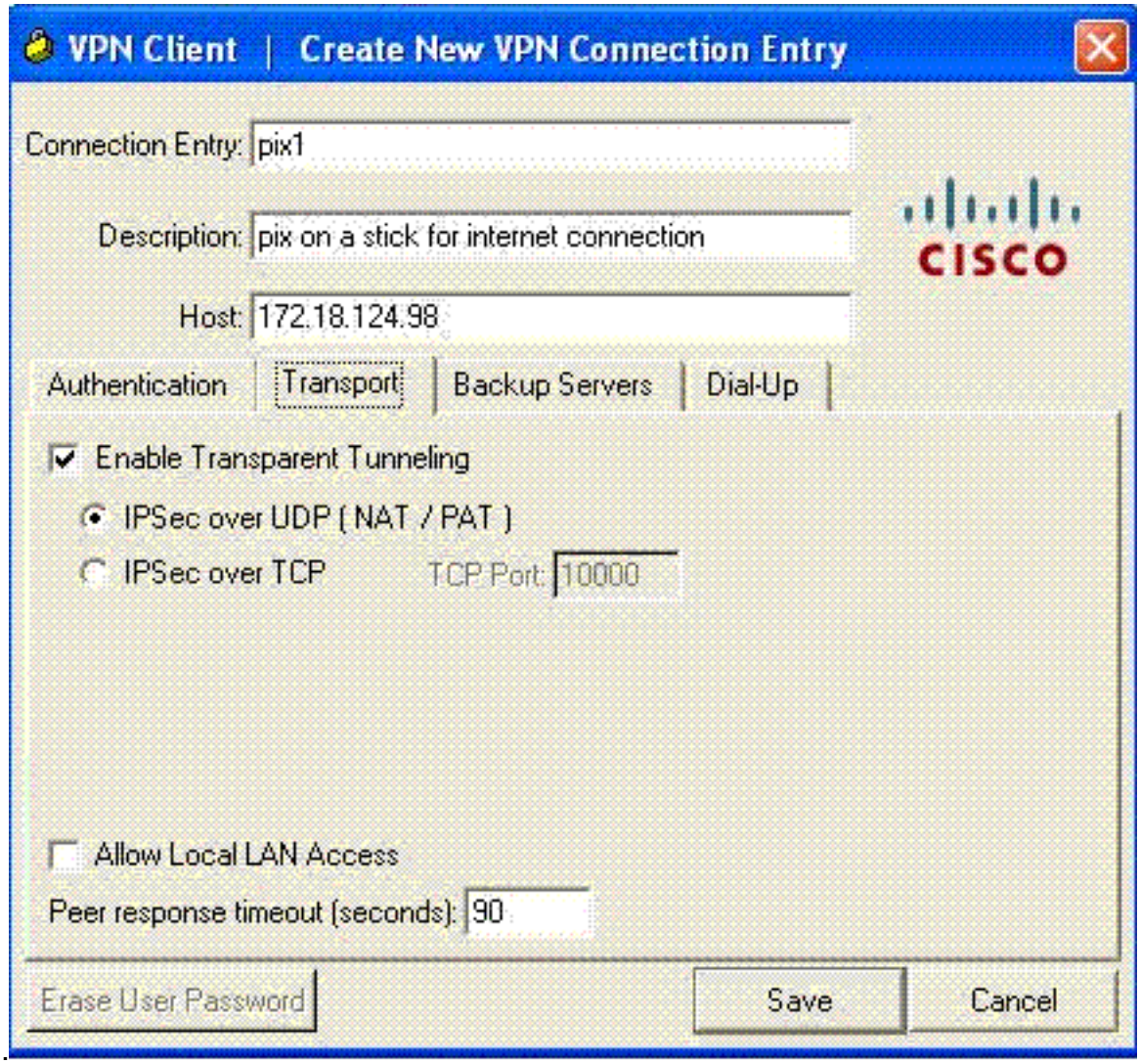
1. Scegliere
   Nuovo.



2. Immettere l'indirizzo IP dell'interfaccia esterna PIX e il nome del gruppo di tunnel insieme alla password di
   autenticazione.



3. (*Facoltativo*) Fare clic su **Abilita tunneling trasparente** nella scheda Trasporto. (Questa operazione è opzionale e richiede la configurazione PIX/ASA aggiuntiva indicata nella [nota](#))



2).

4. Salvare il profilo.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- show crypto isakmp sa: visualizza tutte le associazioni di sicurezza IKE correnti in un peer.
- show crypto ipsec sa: visualizza tutte le SA correnti. Cercare i pacchetti crittografati e decrittografati sull'appliance ASA che definiscono il traffico del client VPN.

Tentare di eseguire il ping o di individuare un indirizzo IP pubblico dal client (ad esempio, www.cisco.com).

Nota: non è possibile eseguire il ping dell'interfaccia interna del PIX per la formazione di un tunnel a meno che il comando management-access non sia configurato in modalità di conferma globale.

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

management-access inside
```

Verifica client VPN

Completare questa procedura per verificare il client VPN.

1. Fare clic con il pulsante destro del mouse sull'icona di blocco del client VPN presente sulla barra delle applicazioni dopo una connessione riuscita e scegliere l'opzione per **le statistiche** per visualizzare le crittografie e le decrittografazioni.
2. Fare clic sulla scheda Dettagli percorso per verificare l'elenco dei tunnel non suddivisi trasmesso dall'accessorio.

Risoluzione dei problemi

Nota: per ulteriori informazioni su come risolvere i problemi relativi alla VPN, consultare il documento sulla risoluzione dei problemi relativi alla VPN.

Informazioni correlate

- Esempio di configurazione VPN Enhanced Spoke-to-Client per PIX Security Appliance versione 7.0
- Cisco VPN Client
- Negoziazione IPSec/protocolli IKE
- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- Fissaggio per capelli su Cisco ASA
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems