ASA/PIX: Esempio di server VPN remoto con NAT in entrata per il traffico dei client VPN con CLI e ASDM

Sommario

Introduzione

Questo documento descrive come configurare Cisco serie 5500 Adaptive Security Appliance (ASA) in modo che agisca come server VPN remoto usando Adaptive Security Device Manager (ASDM) o CLI e NAT per il traffico del client VPN in entrata. ASDM offre funzionalità di monitoraggio e gestione della sicurezza di altissimo livello attraverso un'interfaccia di gestione intuitiva e basata su Web. Una volta completata la configurazione di Cisco ASA, è possibile verificarla tramite il client VPN Cisco.

Prerequisiti

Requisiti

In questo documento si presume che l'ASA sia completamente operativa e configurata per consentire a Cisco ASDM o CLI di apportare modifiche alla configurazione. Si presume che l'ASA sia configurata anche per il protocollo NAT in uscita. Per ulteriori informazioni su come configurare il protocollo NAT in uscita, fare riferimento a Consenti accesso degli host interni alle reti esterne con l'utilizzo del protocollo PAT.

Nota: per ulteriori informazioni, fare riferimento al documento sull'autorizzazione dell'accesso HTTPS per ASDM o PIX/ASA 7.x: Esempio di configurazione dell'interfaccia interna ed esterna per consentire la configurazione remota del dispositivo da parte di ASDM o Secure Shell (SSH).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco Adaptive Security Appliance versione 7.x e successive
- Adaptive Security Device Manager versione 5.x e successive
- Cisco VPN Client versione 4.x e successive

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.x e successive.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Le configurazioni di accesso remoto forniscono accesso remoto sicuro per i client VPN Cisco, ad esempio gli utenti mobili. Una VPN ad accesso remoto consente agli utenti remoti di accedere in modo sicuro alle risorse di rete centralizzate. Il client VPN Cisco è conforme al protocollo IPSec ed è progettato in modo specifico per l'utilizzo con l'appliance di sicurezza. L'appliance di sicurezza può tuttavia stabilire connessioni IPSec con molti client conformi al protocollo. Per ulteriori informazioni su IPSec, consultare le guide alla configurazione delle appliance ASA.

I gruppi e gli utenti sono concetti fondamentali nella gestione della sicurezza delle VPN e nella configurazione dell'appliance di sicurezza. Specificano gli attributi che determinano l'accesso e l'utilizzo della VPN da parte degli utenti. Un gruppo è una raccolta di utenti trattati come un'unica entità. Gli utenti ottengono gli attributi dai criteri di gruppo. I gruppi di tunnel identificano i Criteri di gruppo per connessioni specifiche. Se non si assegna un determinato criterio di gruppo agli utenti, verrà applicato il criterio di gruppo predefinito per la connessione.

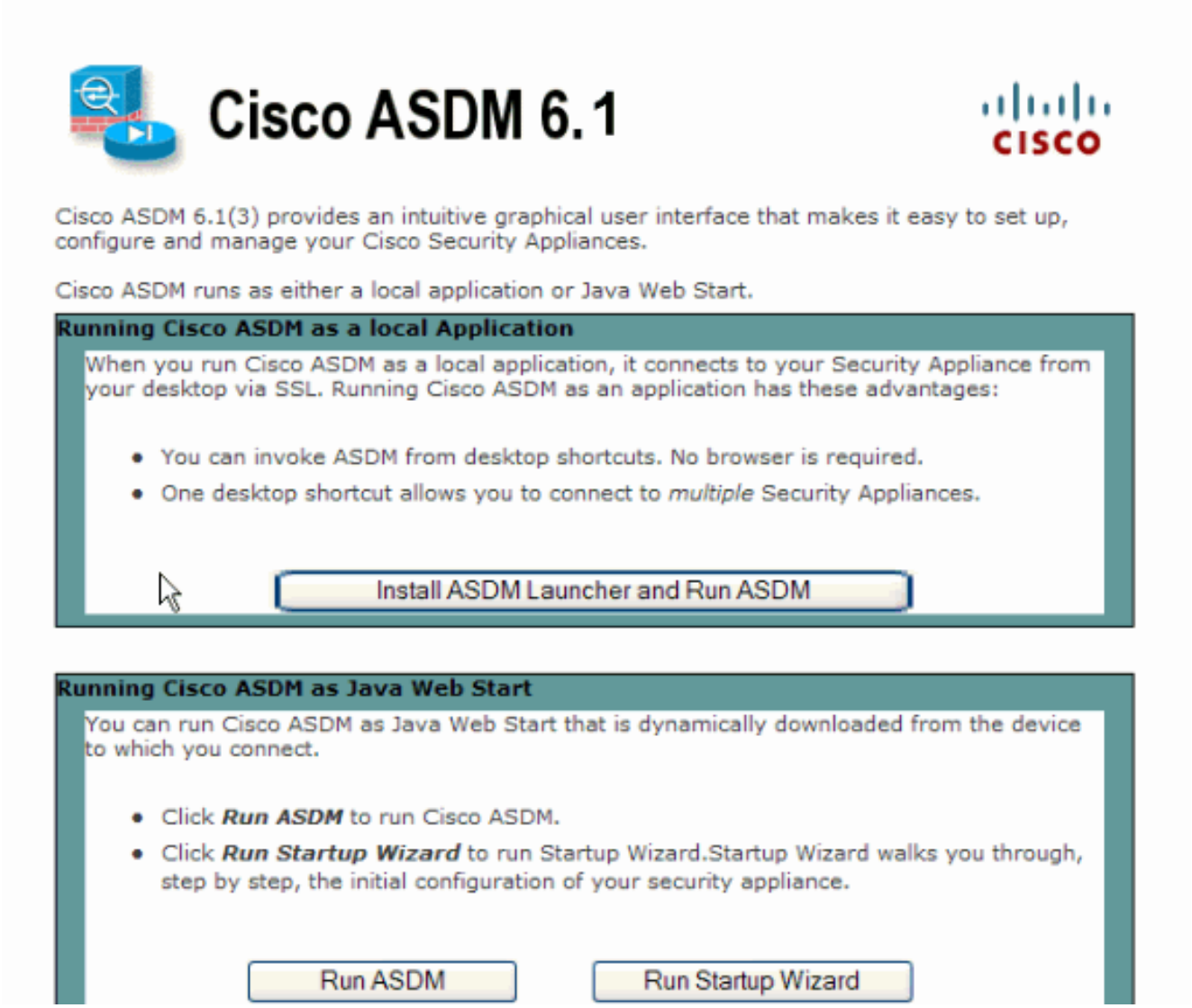
Un gruppo di tunnel è costituito da un set di record che determina i criteri di connessione al tunnel. Questi record identificano i server a cui gli utenti del tunnel sono autenticati, nonché gli eventuali server di accounting a cui vengono inviate le informazioni di connessione. Identificano inoltre un criterio di gruppo predefinito per le connessioni e contengono parametri di connessione specifici del protocollo. I gruppi di tunnel includono un piccolo numero di attributi relativi alla creazione del tunnel stesso. I gruppi di tunnel includono un puntatore a un criterio di gruppo che definisce gli attributi orientati all'utente.

Configurazioni

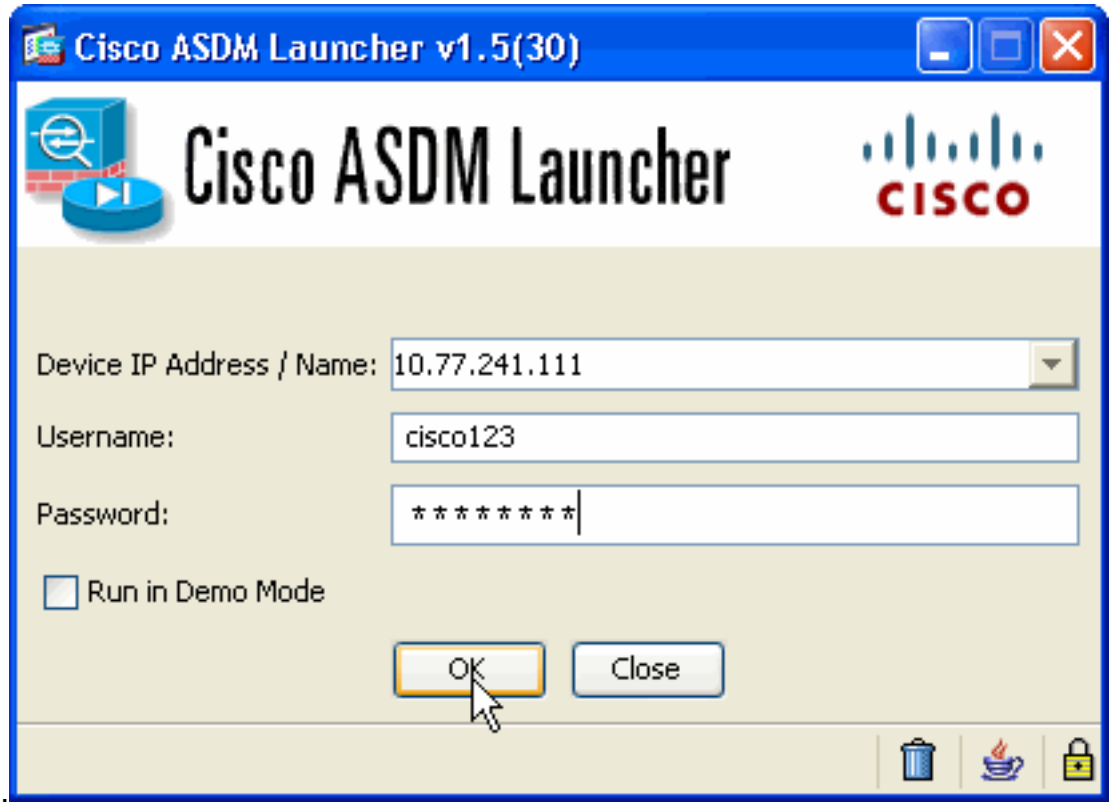
Configurazione di ASA/PIX come server VPN remoto con ASDM

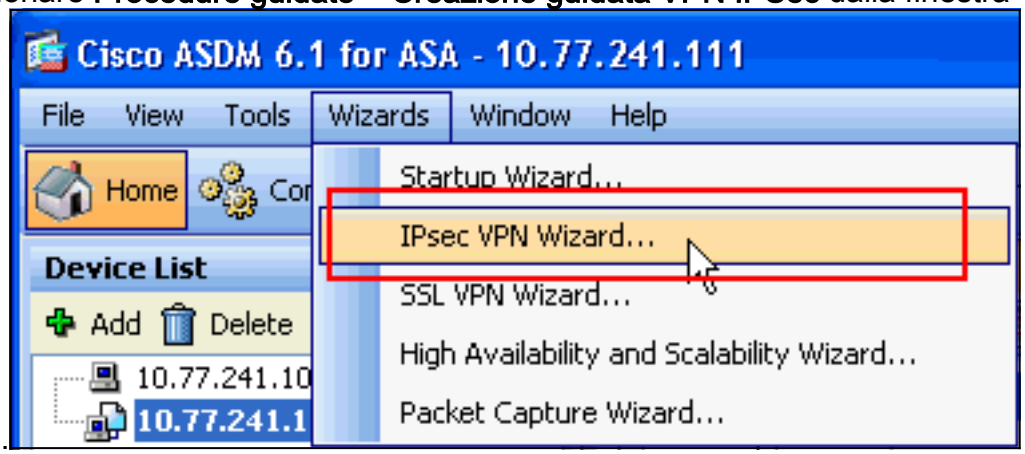
Per configurare Cisco ASA come server VPN remoto con ASDM, completare la procedura seguente:

1. Aprire il browser e immettere **https://<IP_Address> dell'interfaccia dell'ASA configurata per l'accesso ASDM>** per accedere all'ASDM sull'appliance.Accertarsi di autorizzare gli avvisi che il browser visualizza relativi all'autenticità del certificato SSL. Il nome utente e la password predefiniti sono entrambi vuoti.L'appliance ASA visualizza questa finestra per consentire il download dell'applicazione ASDM. In questo esempio l'applicazione viene caricata nel computer locale e non viene eseguita in un'applet Java.

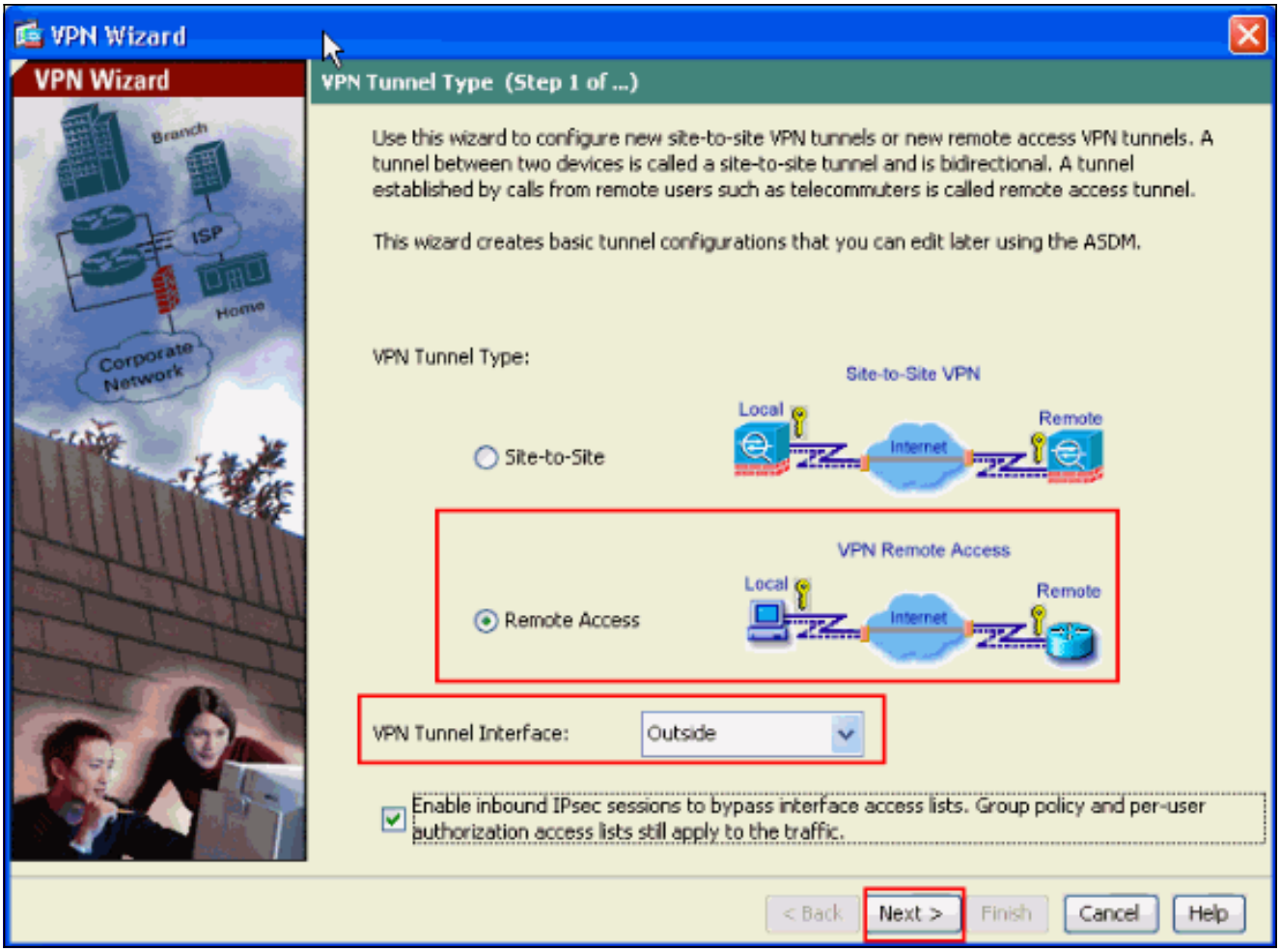


2. Per scaricare il programma di installazione dell'applicazione ASDM, fare clic su **Download ASDM Launcher** e su Start ASDM.
3. Una volta scaricato l'utilità di avvio ASDM, completare la procedura indicata dalle istruzioni per installare il software ed eseguire l'utilità di avvio Cisco ASDM.
4. Immettere l'indirizzo IP dell'interfaccia configurata con il comando **http -**, nonché un nome utente e una password, se specificati.In questo esempio viene utilizzato **cisco123** come nome utente e **cisco123** come

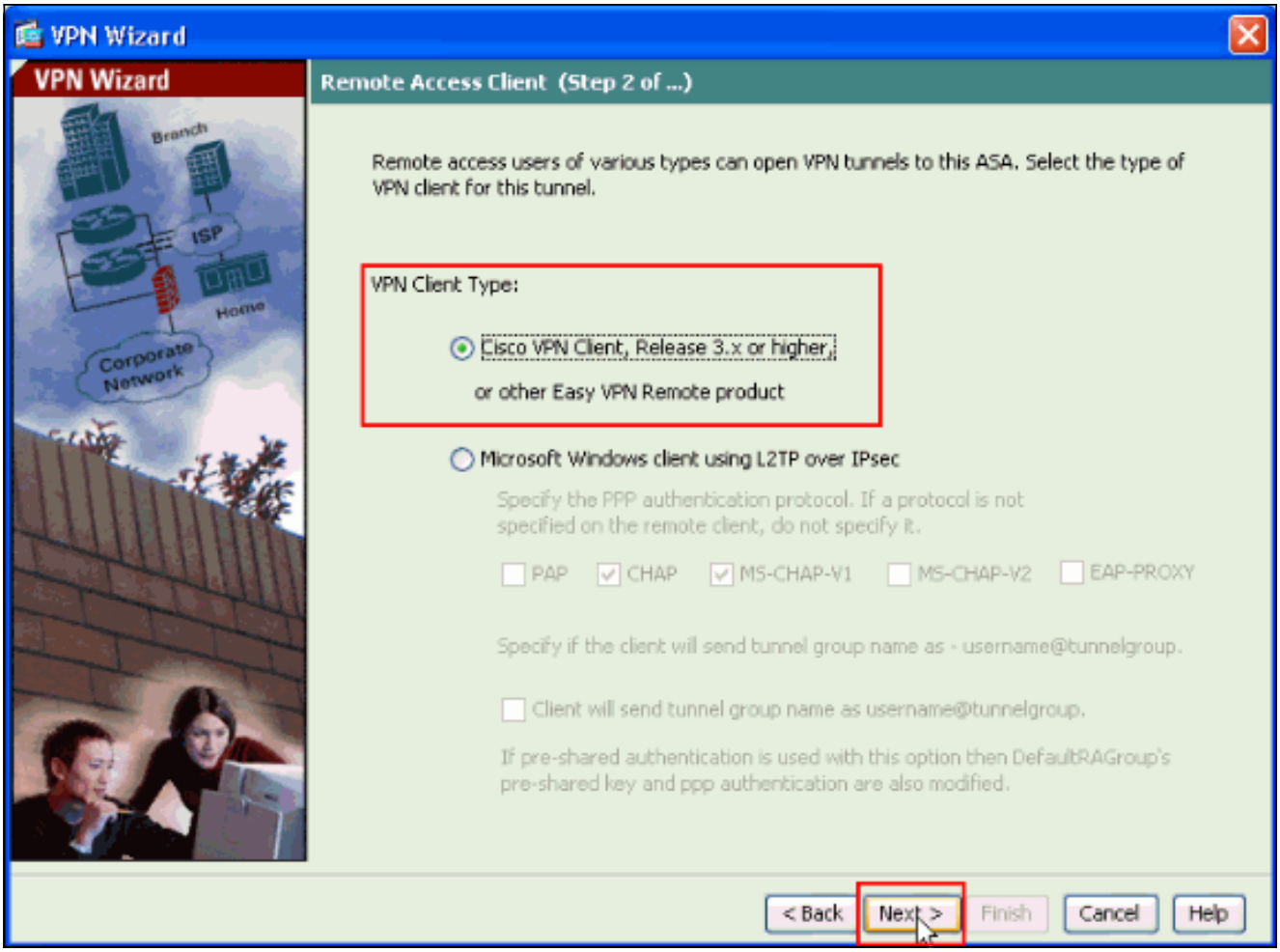
password. 

5. Selezionare **Procedure guidate > Creazione guidata VPN IPSec** dalla finestra Home. 

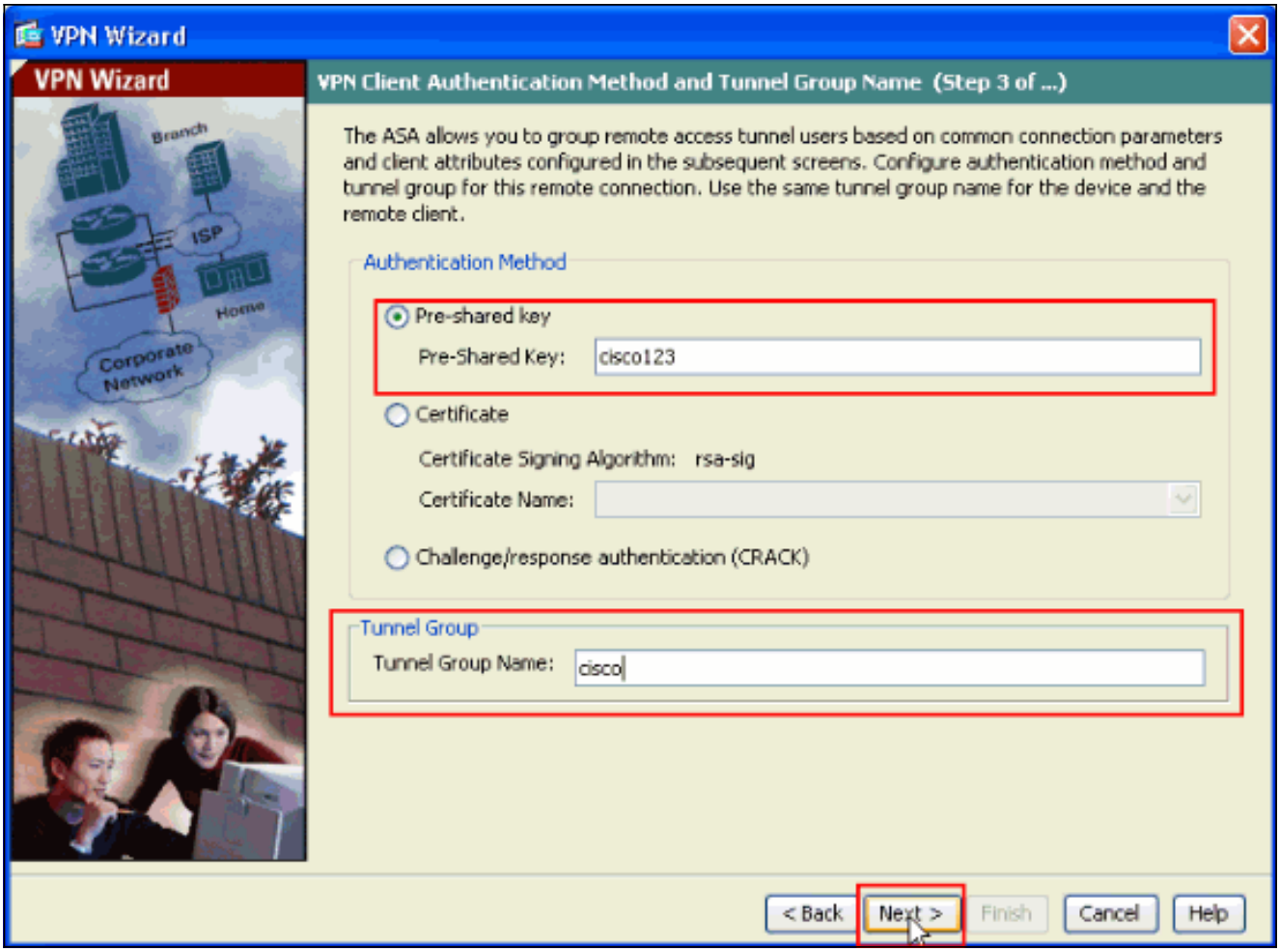
6. Selezionare il tipo di tunnel VPN di **accesso remoto** e verificare che l'interfaccia tunnel VPN sia impostata come desiderato, quindi fare clic su **Avanti** come mostrato di seguito.



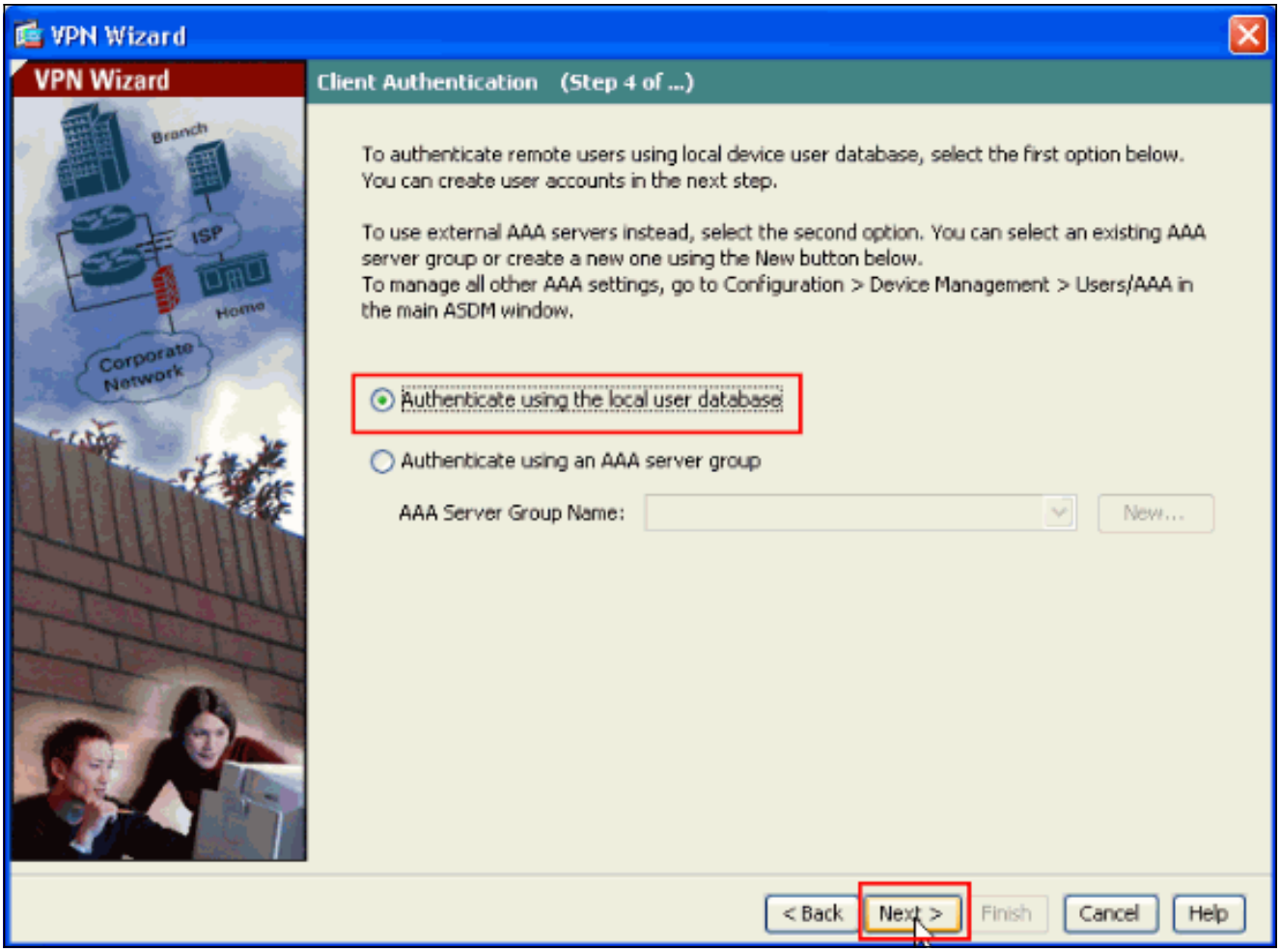
7. Viene scelto il tipo di client VPN, come mostrato. **Cisco VPN Client** è scelto qui. Fare clic su **Next**
(Avanti).



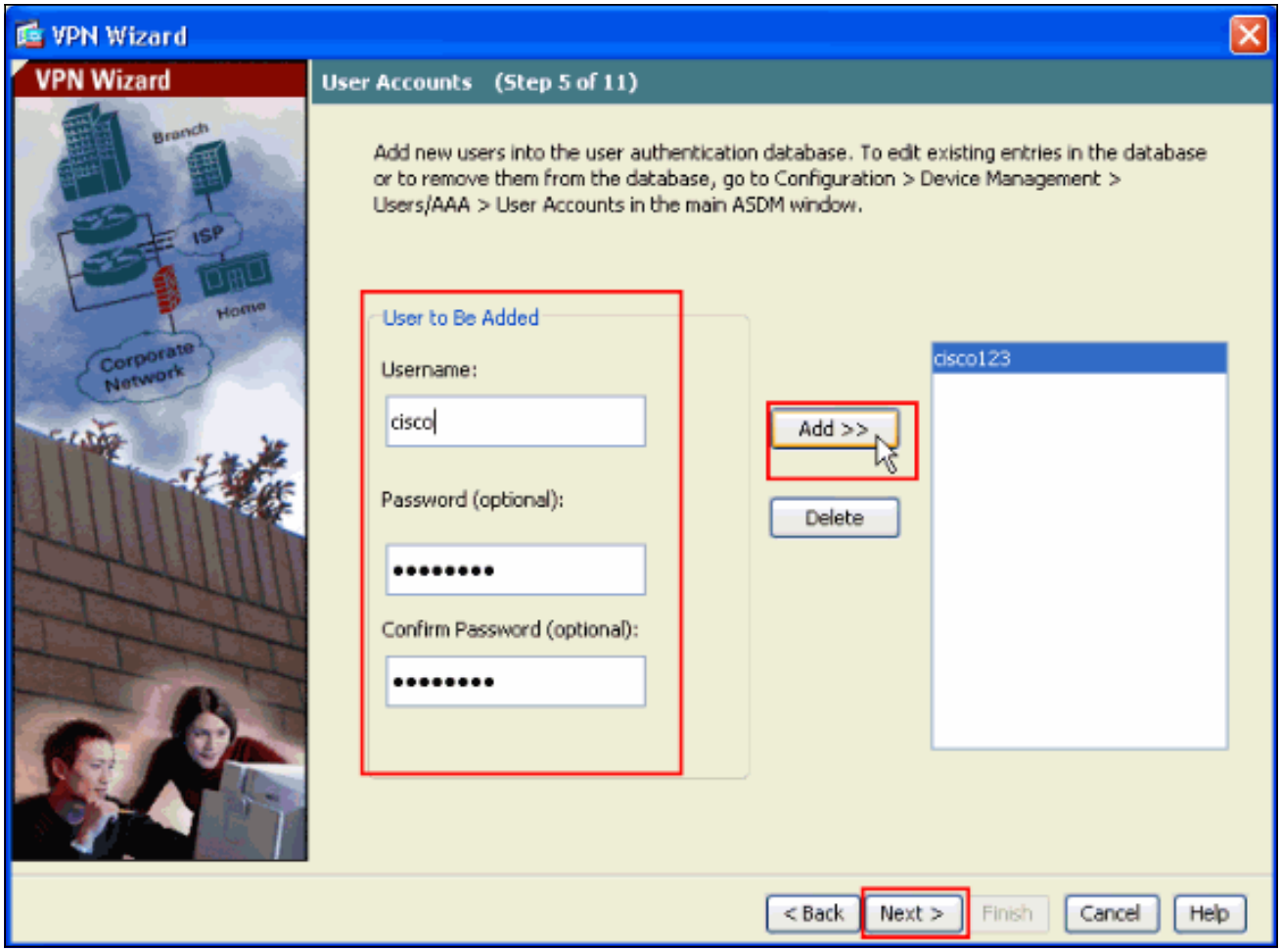
8. Immettere un nome per il **nome** del **gruppo di tunnel**. Immettere le informazioni di autenticazione da utilizzare, ovvero la **chiave già condivisa** in questo esempio. La chiave già condivisa utilizzata in questo esempio è **cisco123**. Il nome del gruppo di tunnel usato in questo esempio è **cisco**. Fare clic su **Next**
(Avanti).



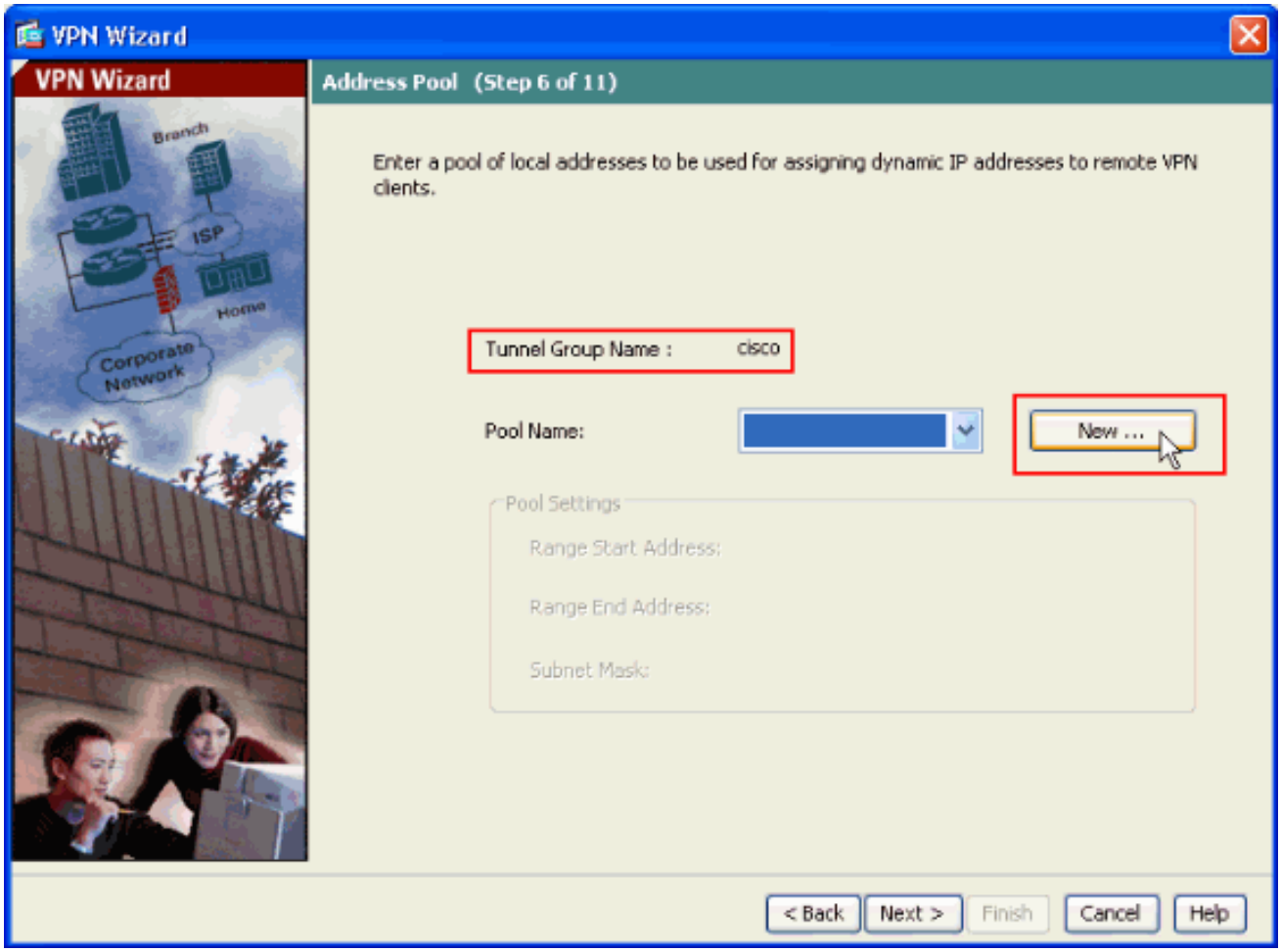
9. Specificare se si desidera che gli utenti remoti vengano autenticati nel database degli utenti locale o in un gruppo di server AAA esterno.**Nota:** aggiungere gli utenti al database locale nel passo 10.**Nota: per** informazioni su come configurare un gruppo di server AAA esterno con ASDM, fare riferimento all'[esempio di configurazione dell'autenticazione e dell'autorizzazione PIX/ASA 7.x per utenti VPN tramite]
ASDM.



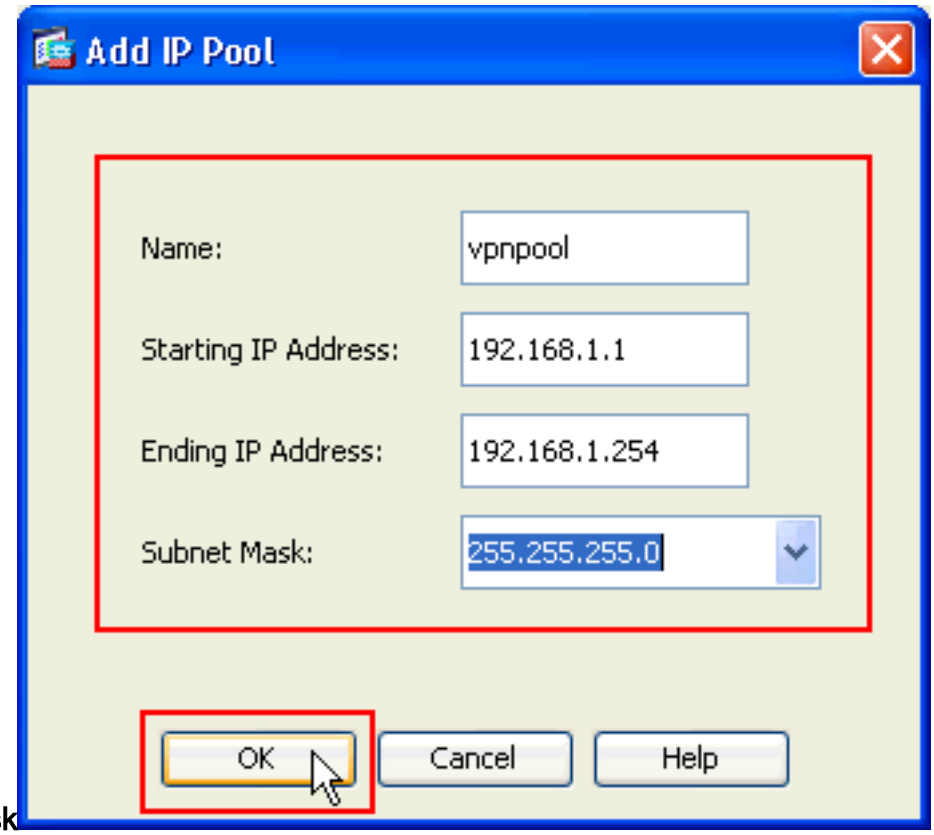
10. Fornire un **nome utente** e una **password** facoltativa e fare clic su **Aggiungi** per aggiungere nuovi utenti al database di autenticazione degli utenti. Fare clic su **Next** (Avanti).**Nota:** non rimuovere gli utenti esistenti da questa finestra. Selezionare **Configurazione > Gestione dispositivi > Utenti/AAA > Account utente** nella finestra principale di ASDM per modificare le voci esistenti nel database o rimuoverle dal database.



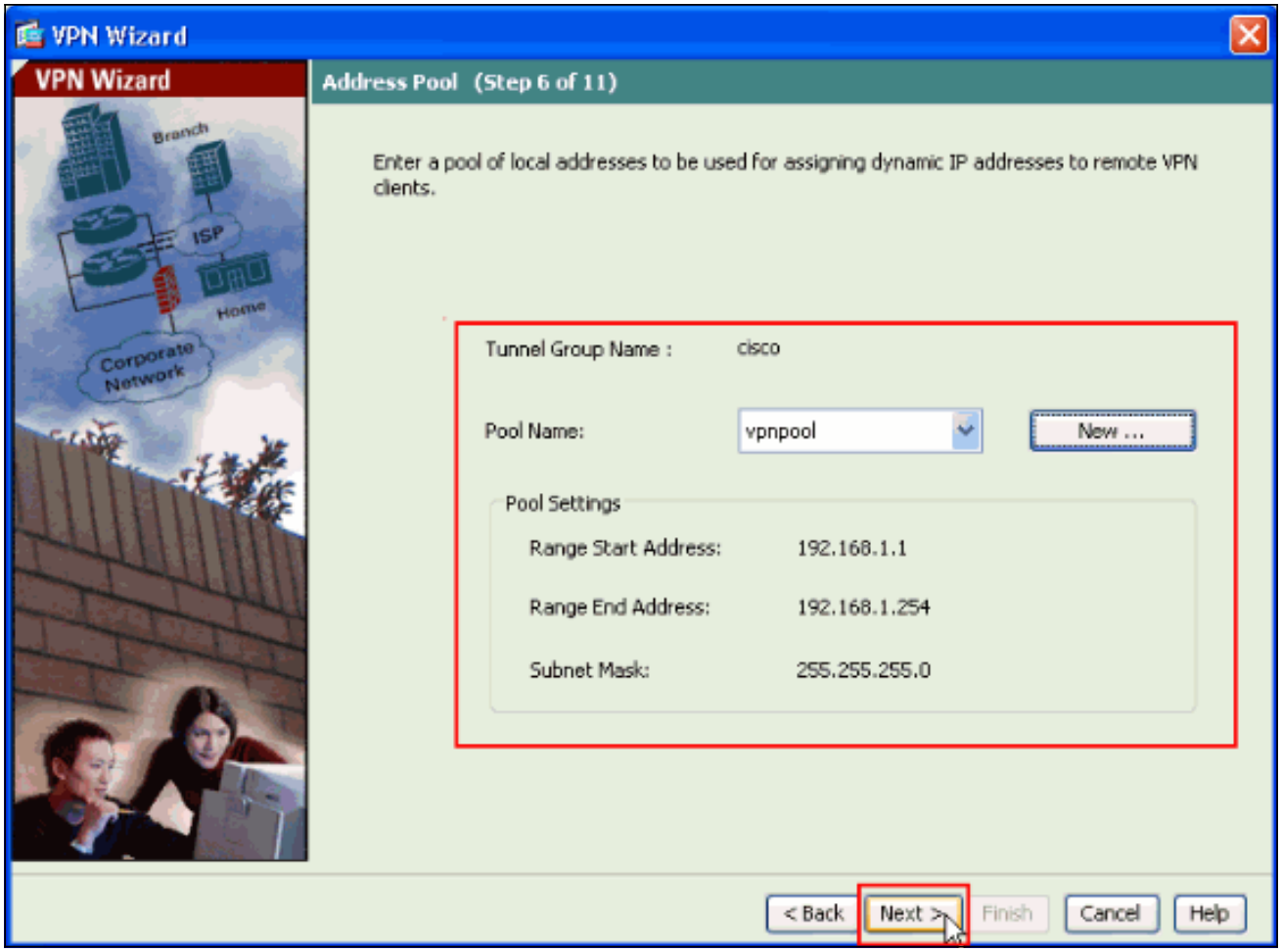
11. Per definire un pool di indirizzi locali da assegnare dinamicamente ai client VPN remoti, fare clic su **Nuovo** per creare un nuovo **pool IP**.



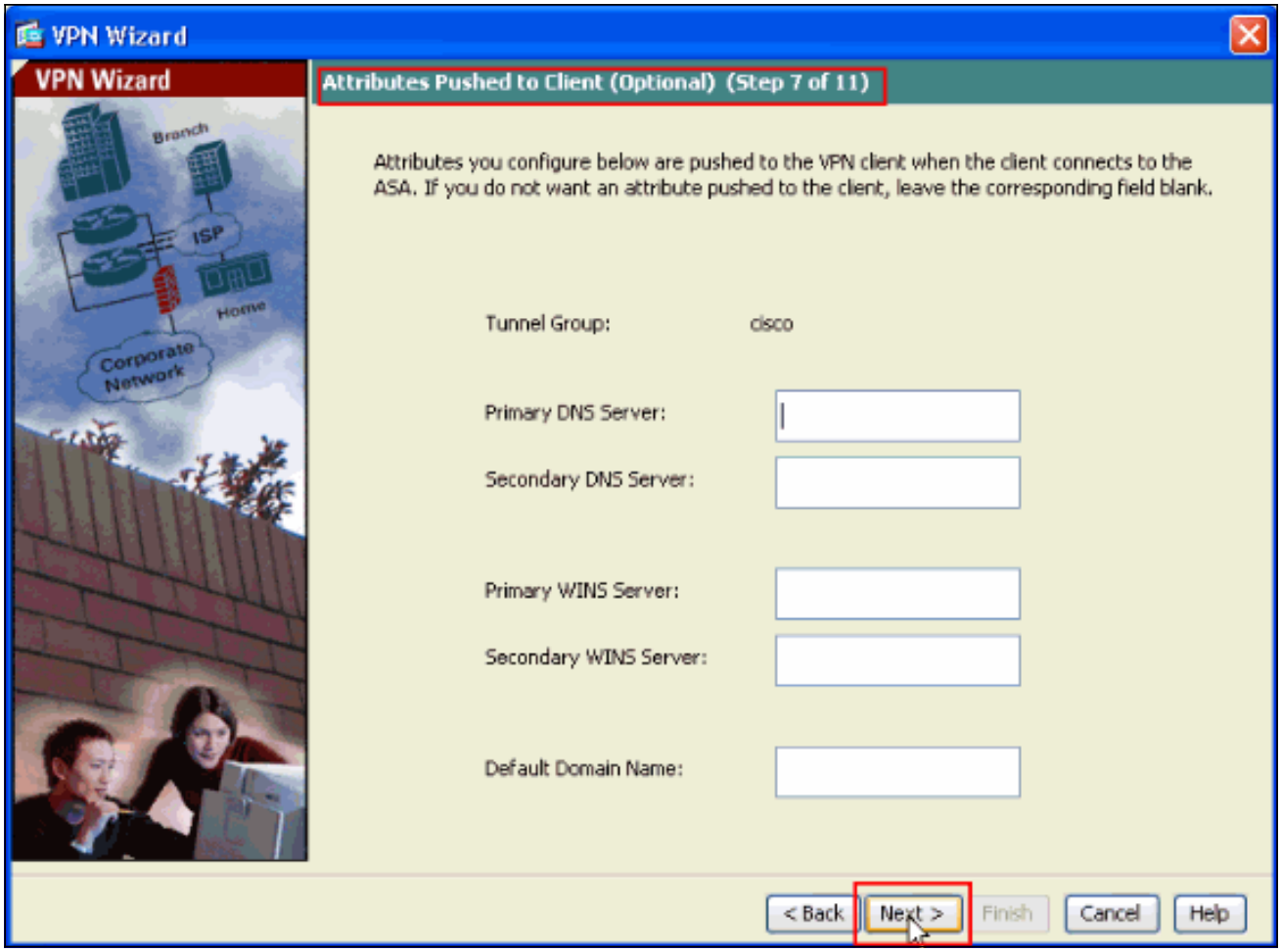
12. Nella nuova finestra **Add IP Pool** fornire queste informazioni e fare clic su **OK**.**Nome del pool IPIndirizzo IP inizialeIndirizzo IP finaleSubnet mask**



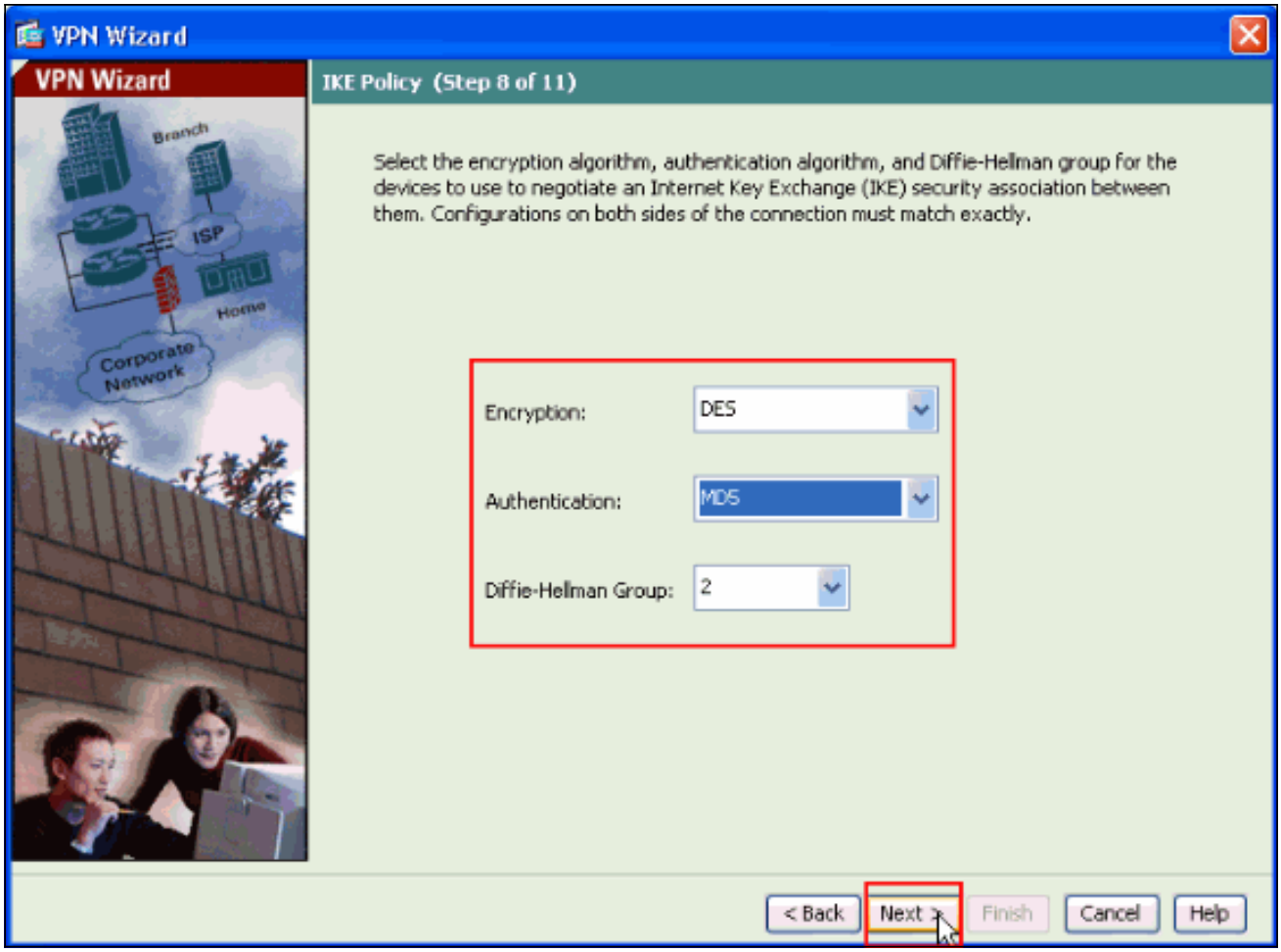
13. Dopo aver definito il pool di indirizzi locali da assegnare dinamicamente ai client VPN remoti quando si connettono, fare clic su **Avanti.**



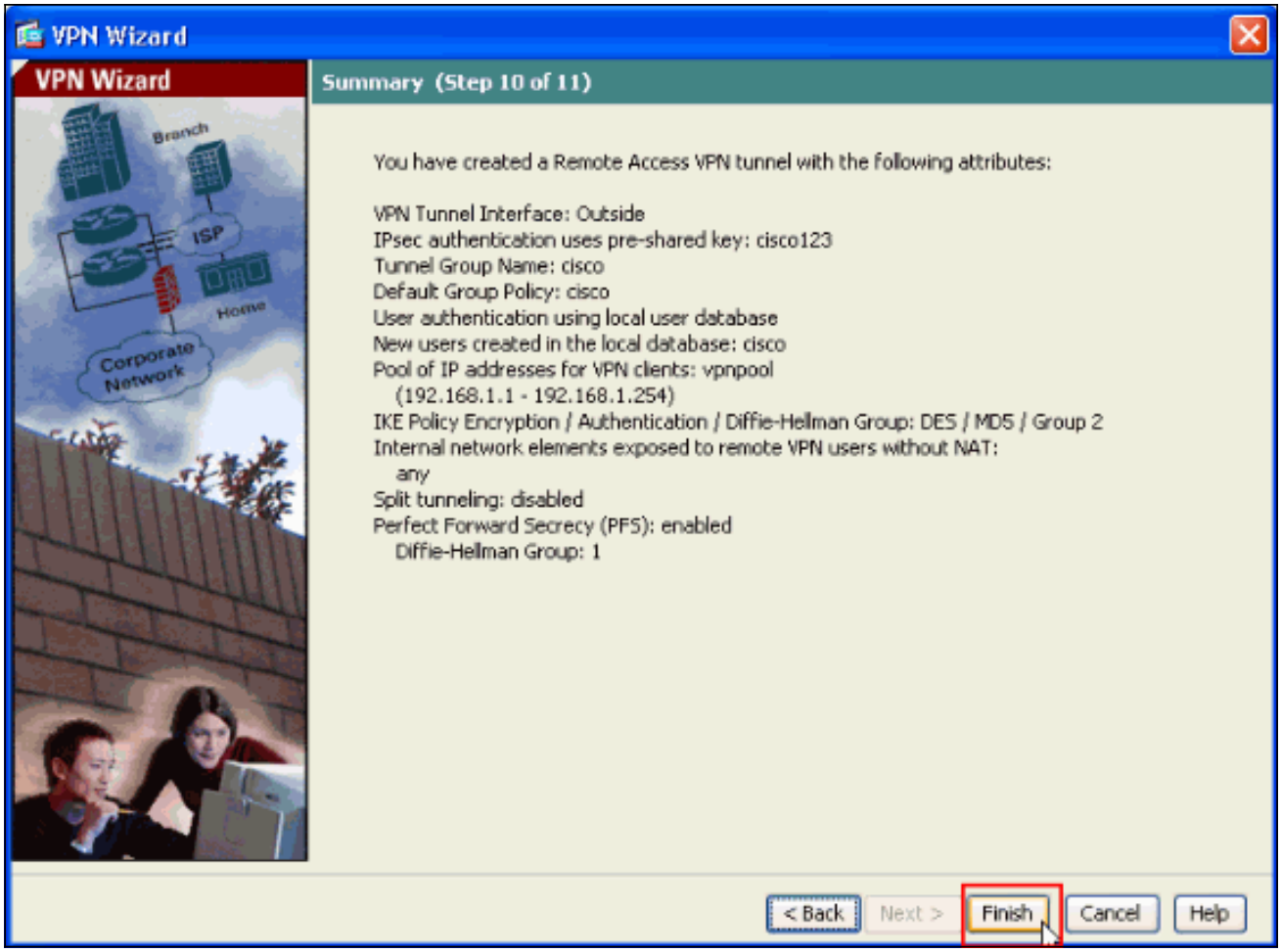
14. *Facoltativo:* Specificare le informazioni sui server DNS e WINS e un nome di dominio predefinito da inserire nei client VPN
remoti.



15. Specificare i parametri per IKE, noto anche come IKE fase 1.Le configurazioni su entrambi i lati del tunnel devono corrispondere esattamente. Tuttavia, il client VPN Cisco seleziona automaticamente la configurazione corretta. Non è pertanto necessaria alcuna configurazione IKE sul PC
client.



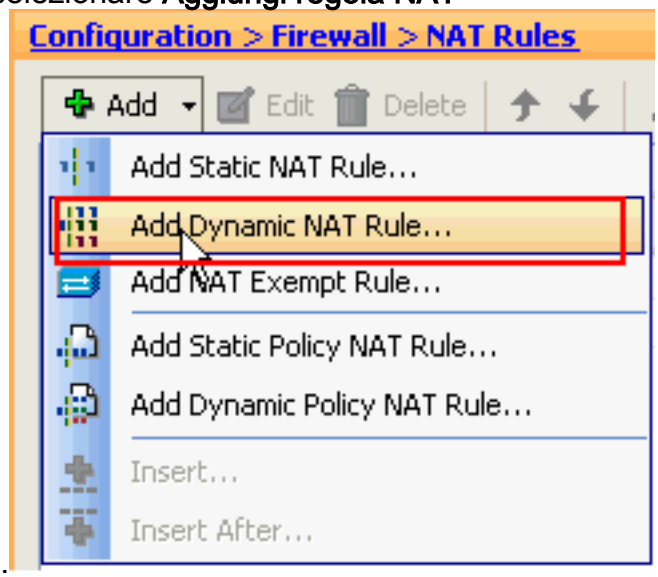
16. Questa finestra mostra un riepilogo delle azioni intraprese. Se la configurazione è soddisfacente, fare clic su **Fine**.



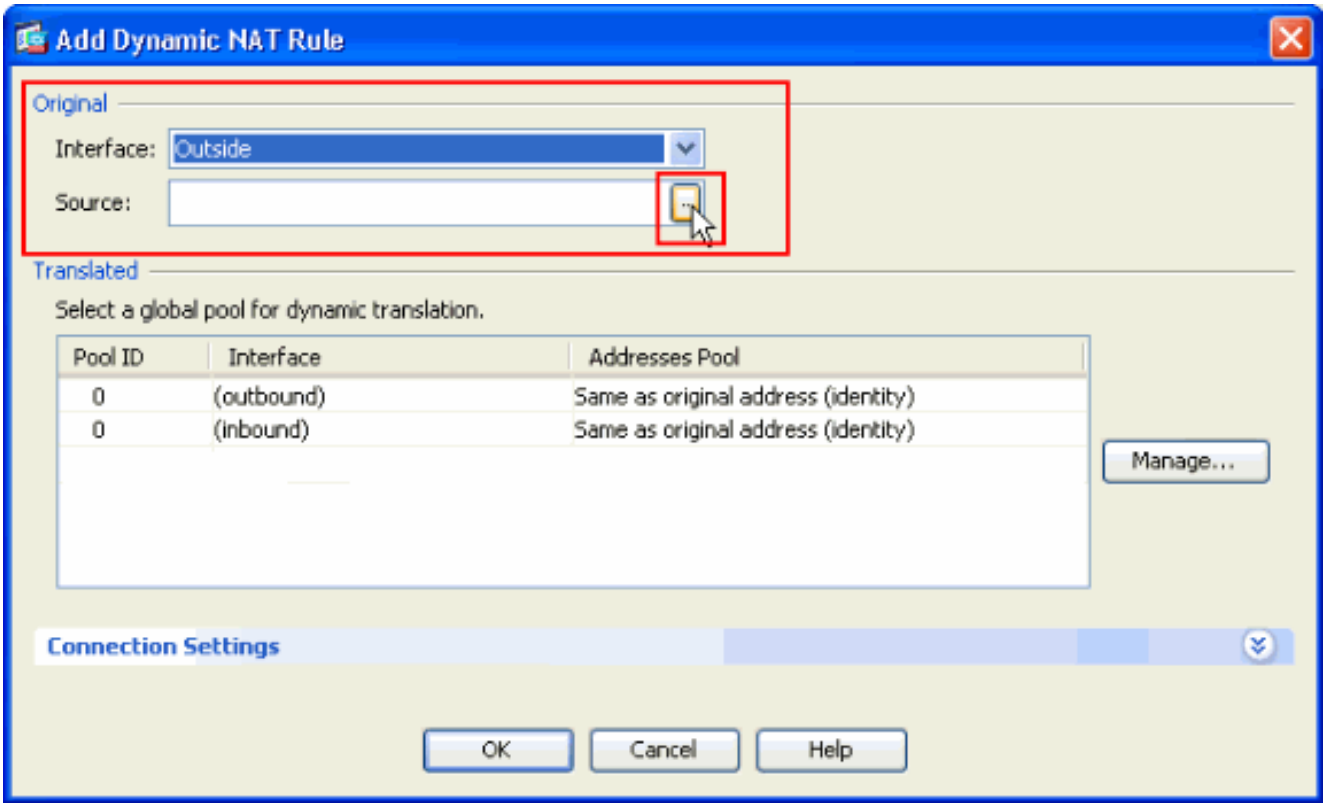
Configurazione di ASA/PIX per il traffico del client VPN in entrata NAT con ASDM

Completare questa procedura per configurare Cisco ASA per il traffico del client VPN in entrata NAT con ASDM:

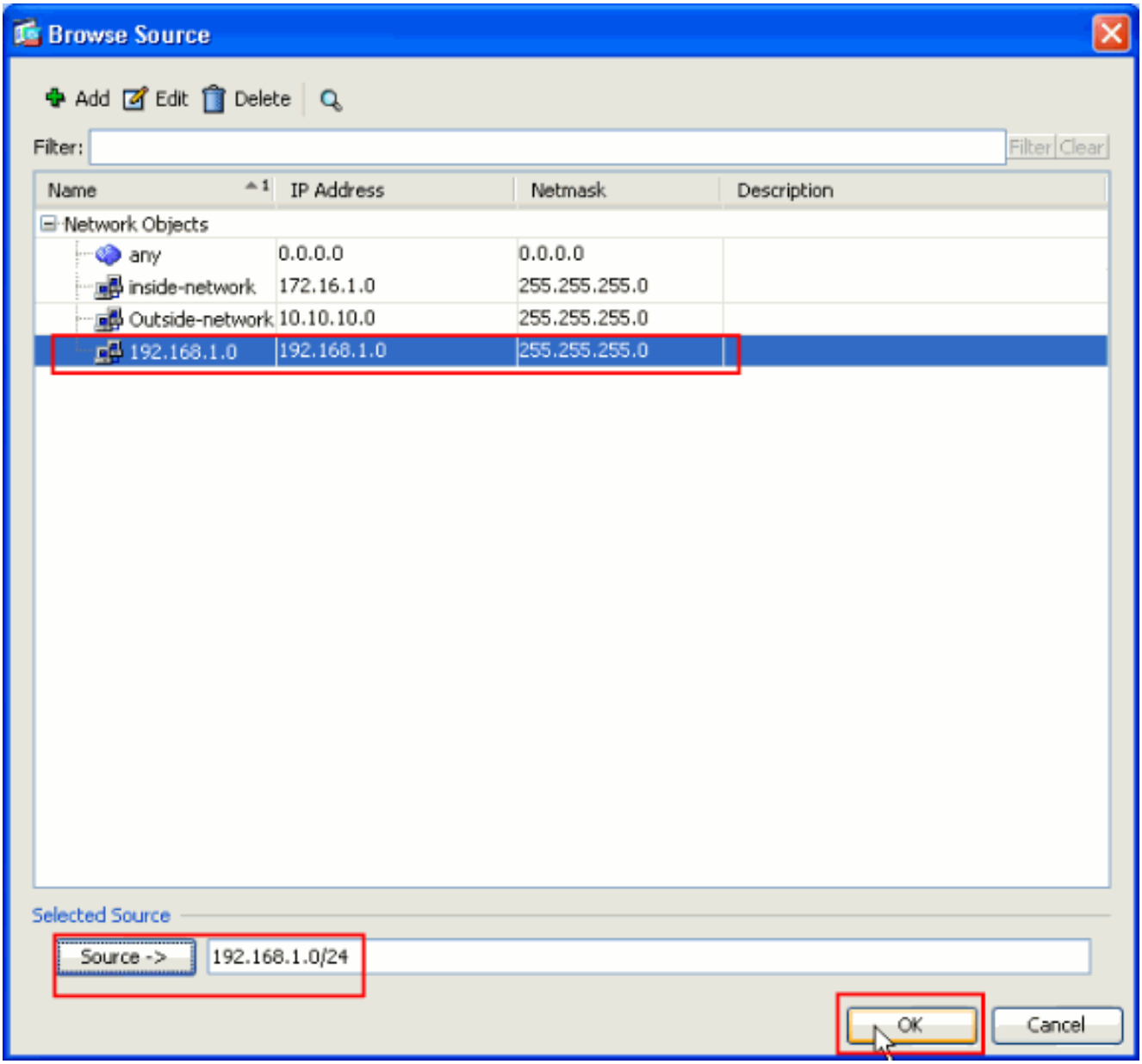
1. Scegliere **Configurazione > Firewall > Regole Nat**, quindi fare clic su **Aggiungi**. Nell'elenco a discesa selezionare **Aggiungi regola NAT dinamica**.



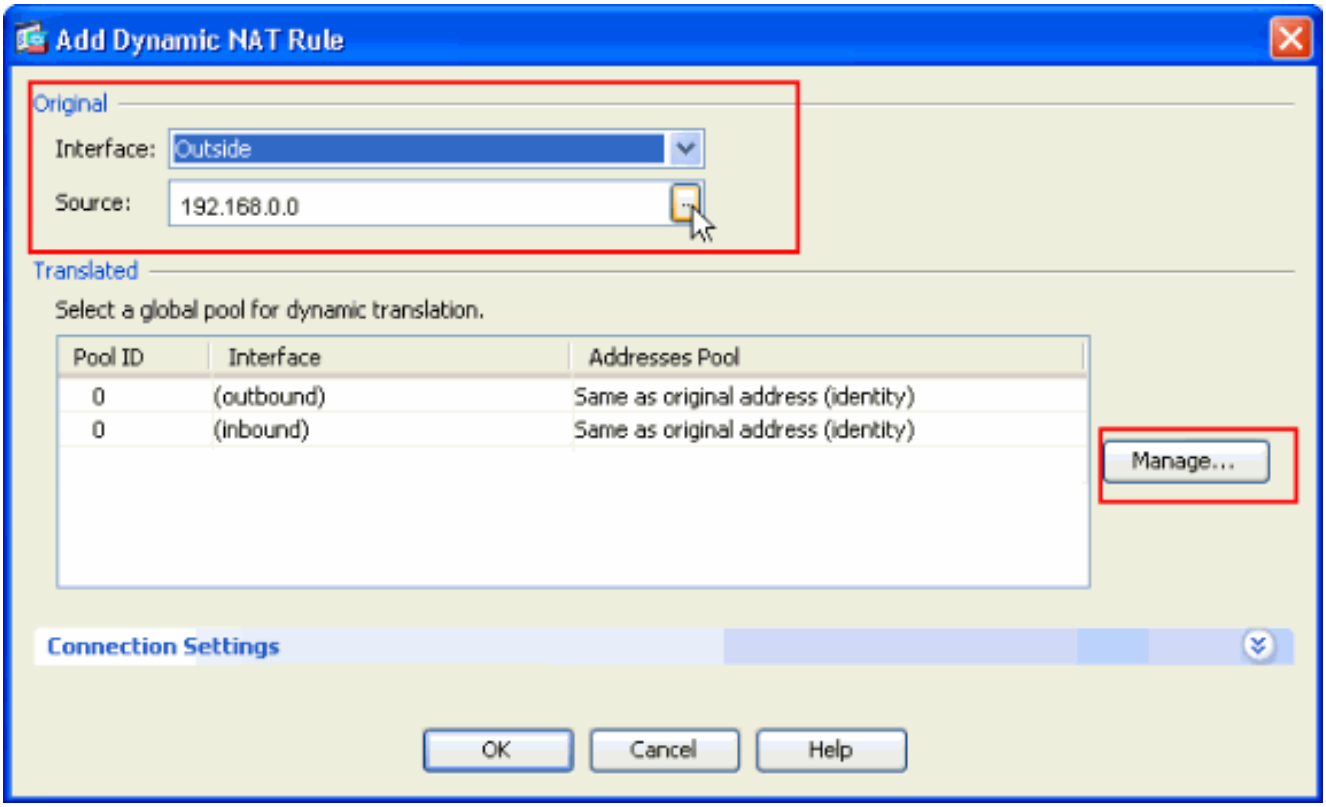
2. Nella finestra **Aggiungi regola NAT dinamica**, scegliere **Esterno** come interfaccia, quindi fare clic sul pulsante Sfoglia accanto alla casella **Origine**.



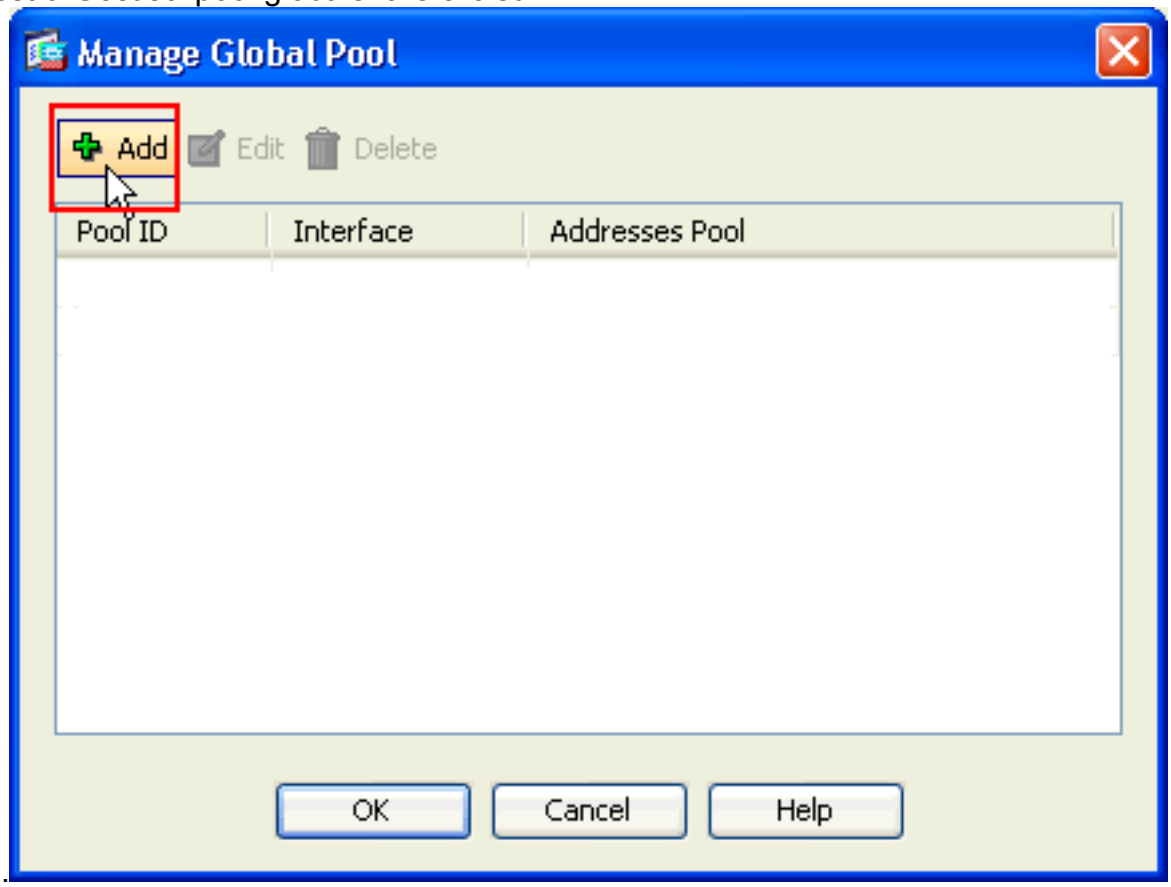
3. Nella finestra Sfoglia origine, selezionare gli oggetti di rete appropriati e scegliere l'**origine** nella sezione Origine selezionata, quindi fare clic su **OK**. In questo caso, viene scelto l'oggetto di rete
192.168.1.0.



4. Fare clic su **Gestisci**.

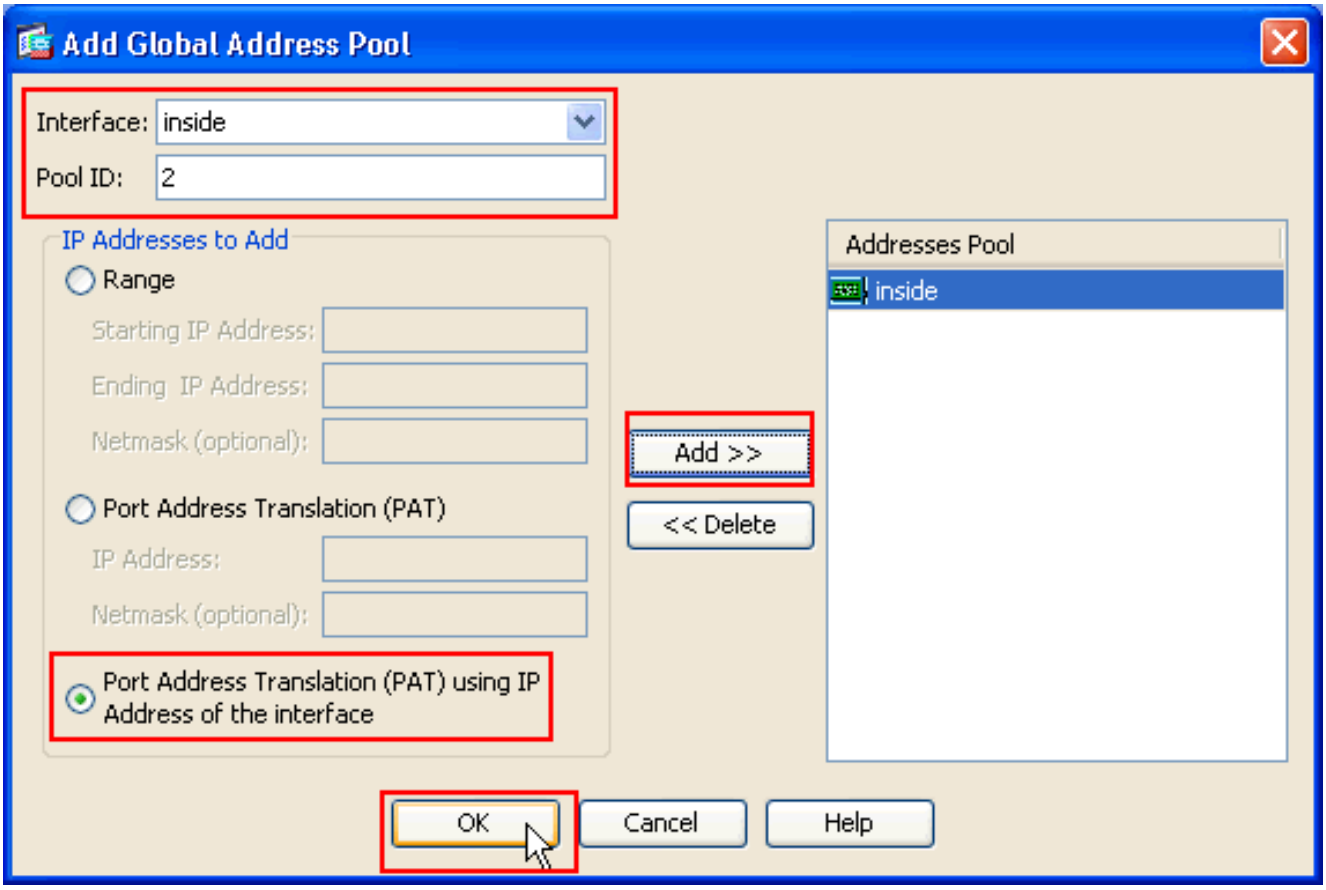


5. Nella finestra Gestisci pool globale fare clic su

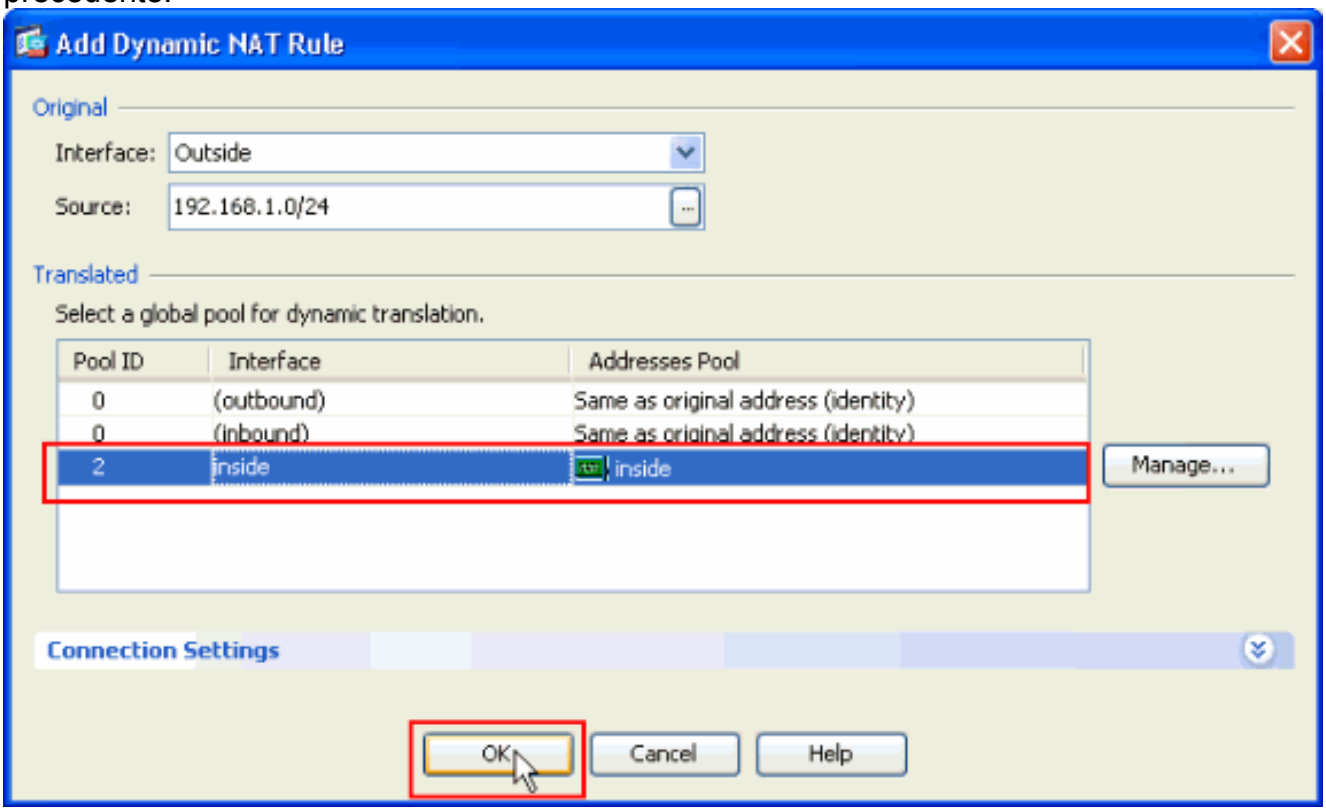


Aggiungi.

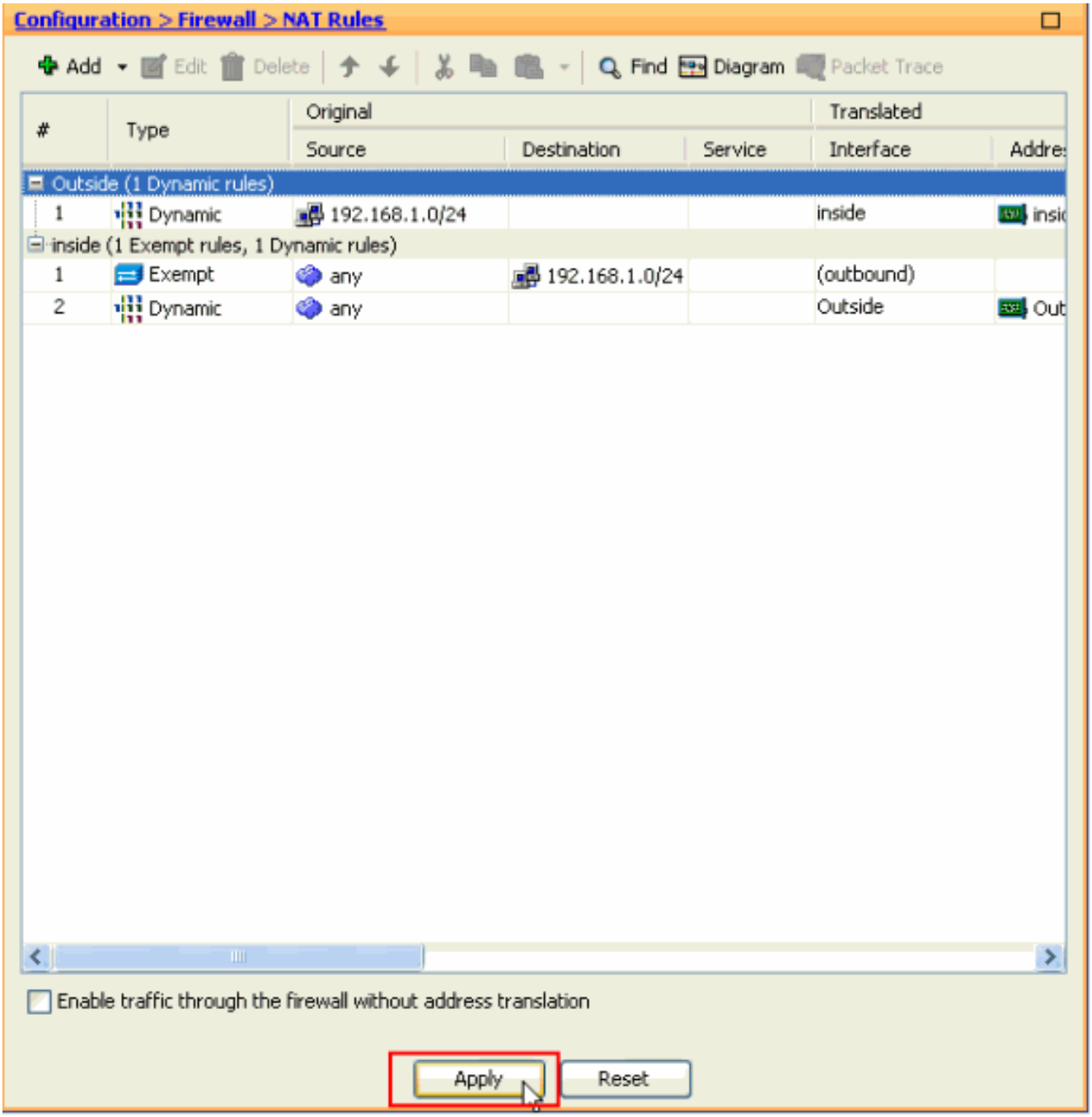
6. Nella finestra Aggiungi pool di indirizzi globale, scegliere **Interno** come interfaccia e **2** come **ID pool**. Verificare inoltre che il pulsante di opzione accanto a **PAT using IP Address of the interface (PAT che utilizza l'indirizzo IP dell'interfaccia)** sia selezionato. Fare clic su **Add>>**, quindi su
OK.



7. Fare clic su **OK** dopo aver selezionato il pool globale con l'**ID pool 2** configurato nel passaggio precedente.



8. A questo punto, fare clic su **Apply** (Applica) per applicare la configurazione all'appliance ASA. La configurazione è stata completata.



Configurare l'ASA/PIX come server VPN remoto e per il protocollo NAT in entrata con la CLI

Esecuzione della configurazione sul 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

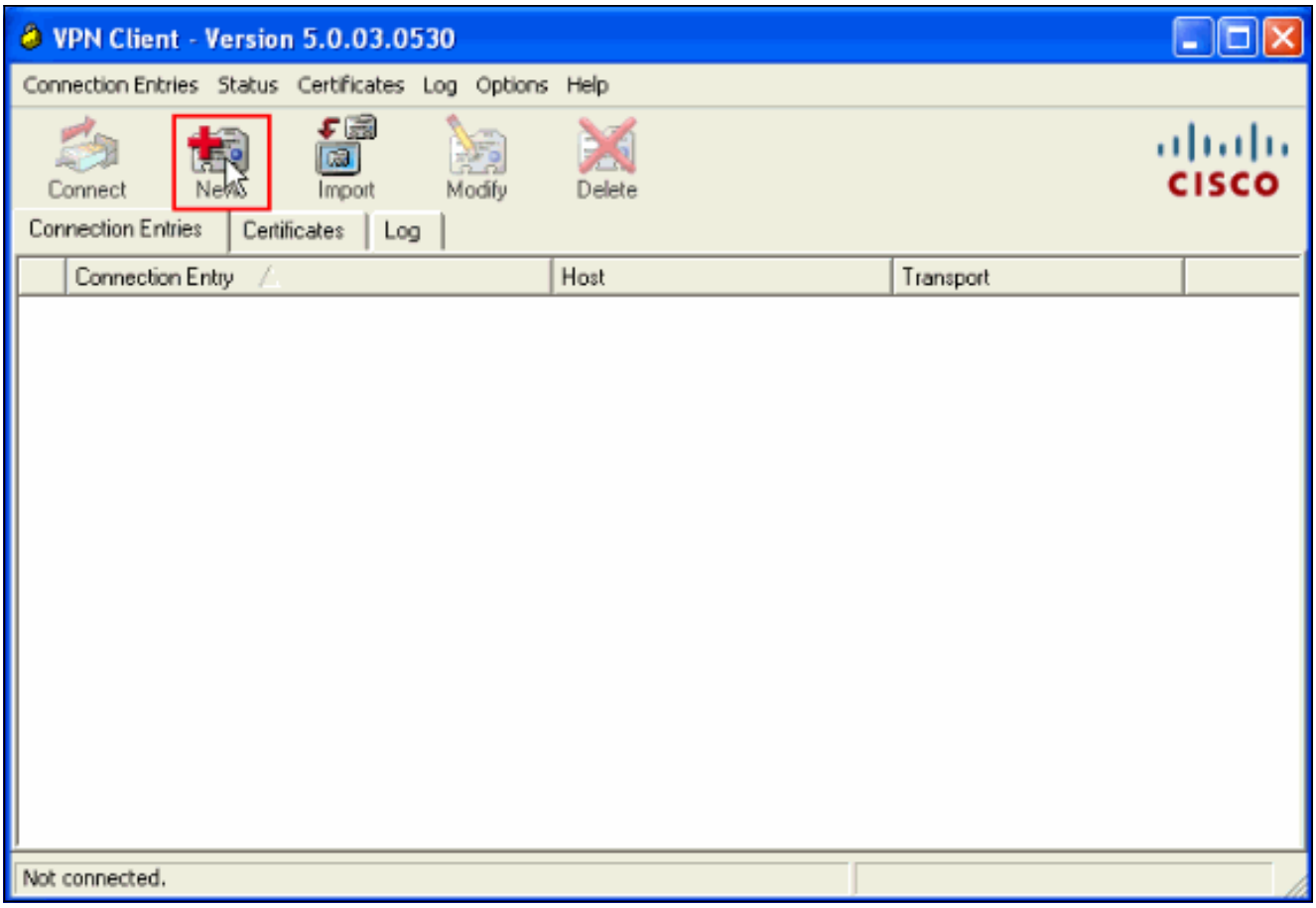
!--- Specifies the pre-shared key "cisco123" which must
!--- be identical at both peers. This is a global !---
configuration mode command. tunnel-group cisco ipsec-
attributes
 pre-shared-key *
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
 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#
```

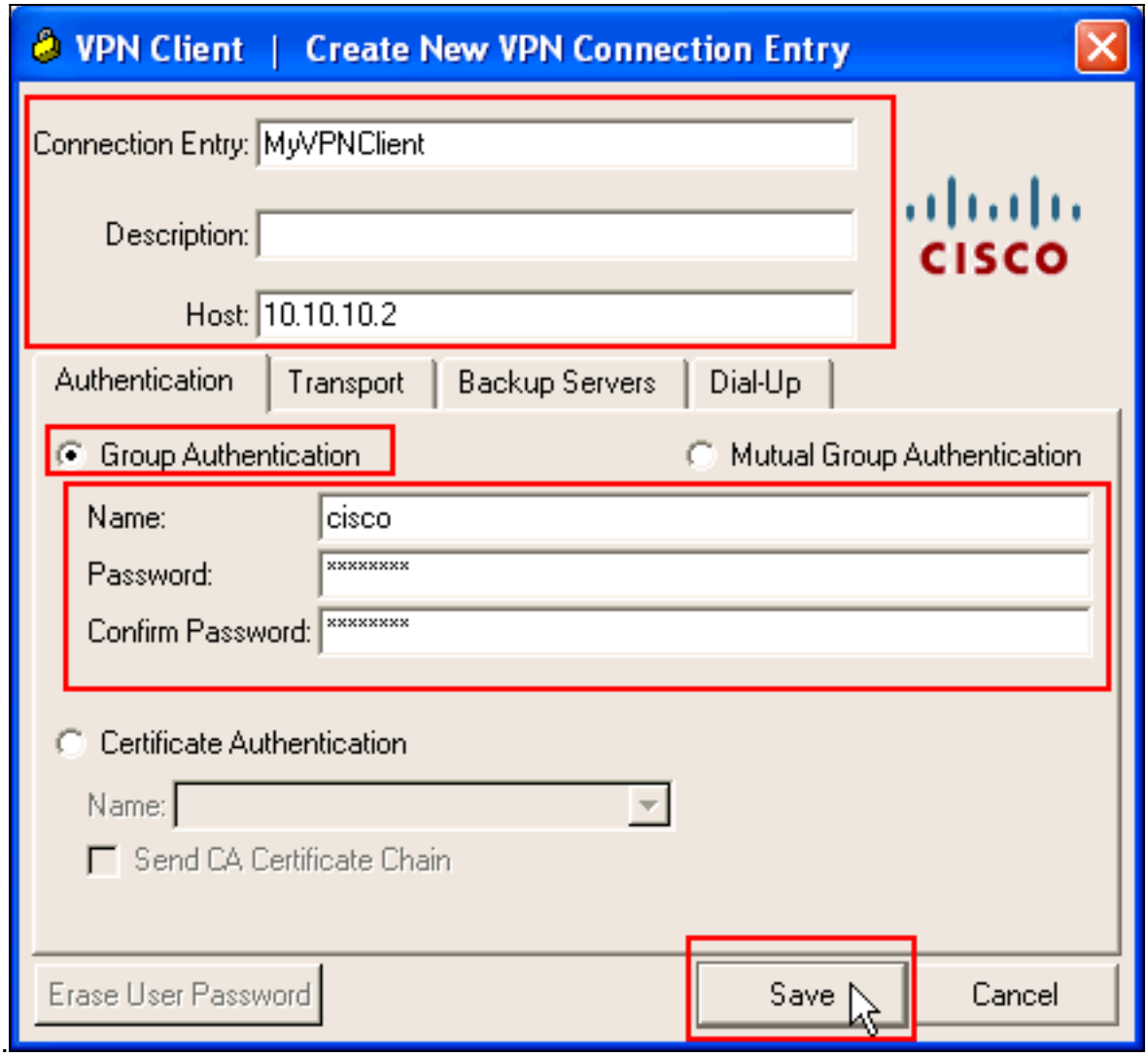
Verifica

Provare a connettersi all'appliance Cisco ASA tramite il client VPN Cisco per verificare che l'appliance ASA sia configurata correttamente.

1. Fare clic su
   New.

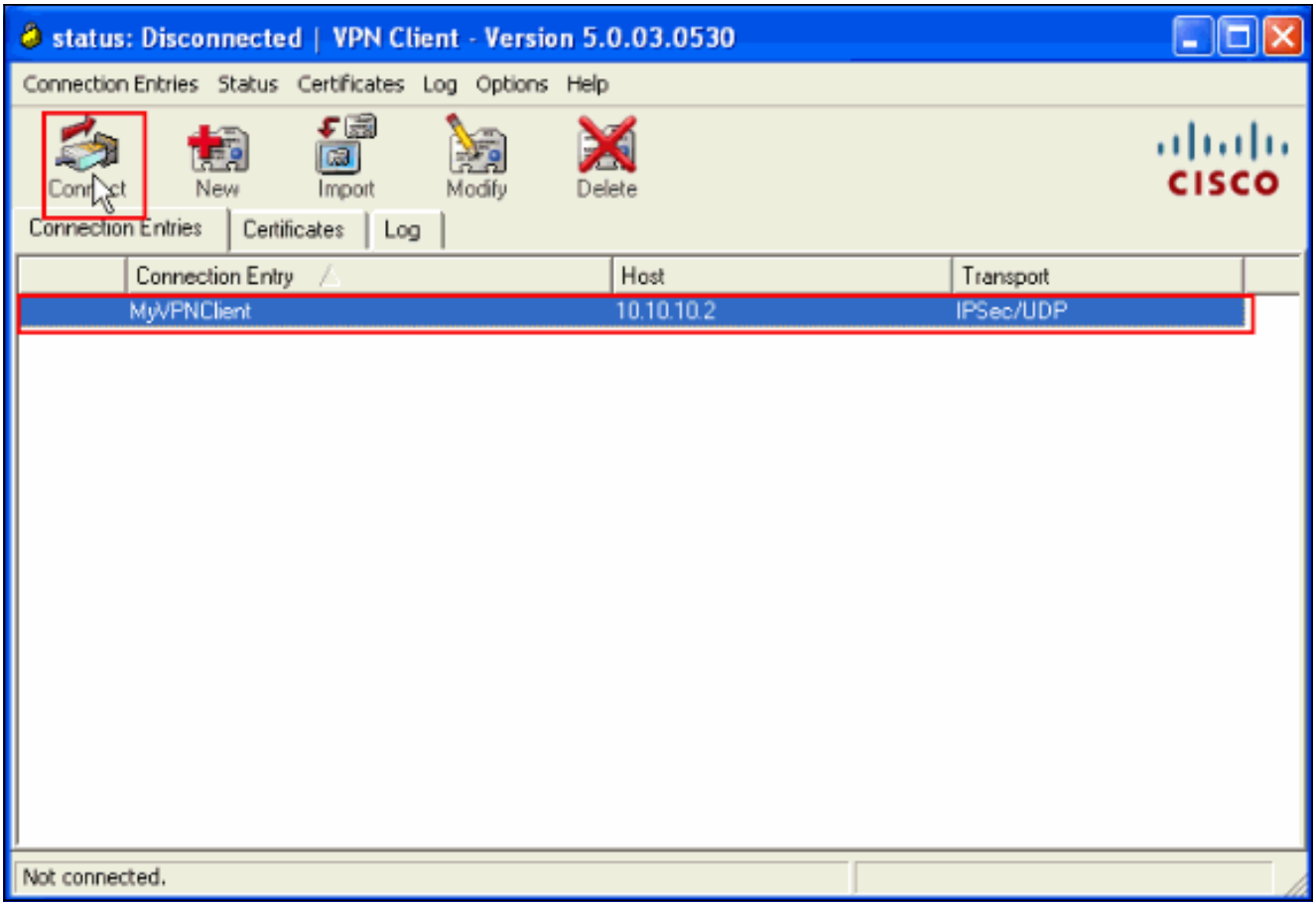


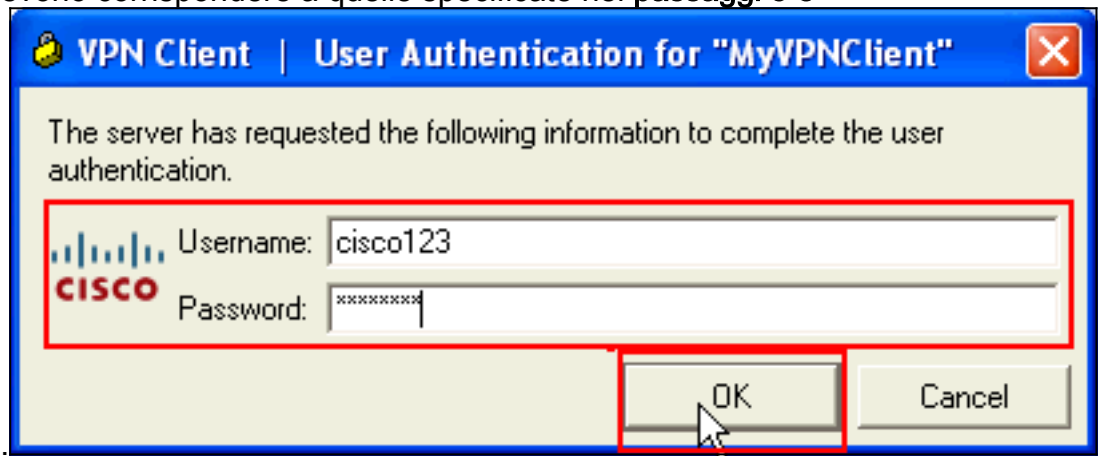
2. Specificare i dettagli della nuova connessione.Il campo Host deve contenere l'indirizzo IP o il nome host dell'appliance Cisco ASA configurata in precedenza. Le informazioni di autenticazione del gruppo devono corrispondere a quelle utilizzate nel **passaggio 4**. Al termine, fare clic su



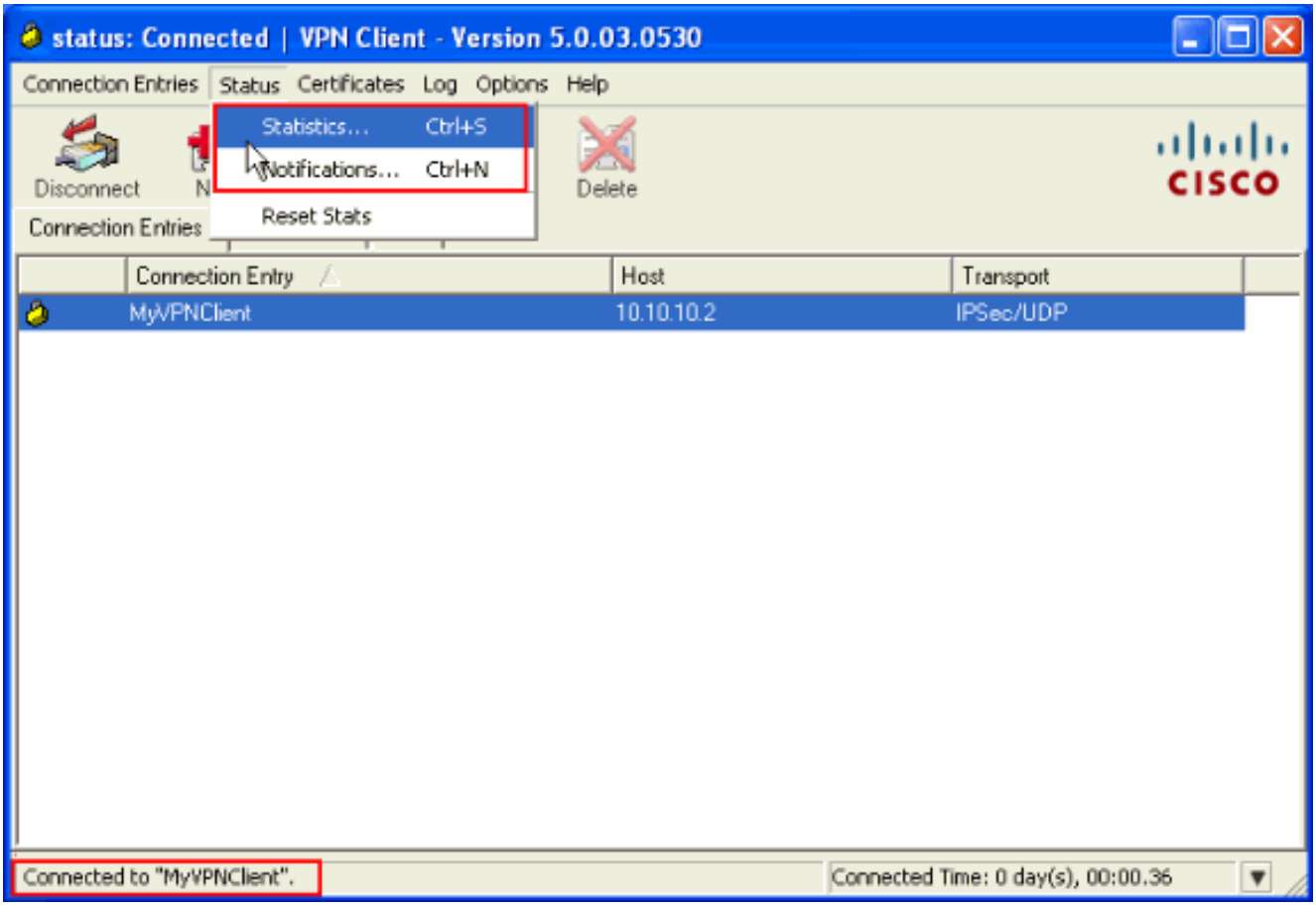
Salva.

3. Selezionare la connessione appena creata e fare clic su **Connetti**.

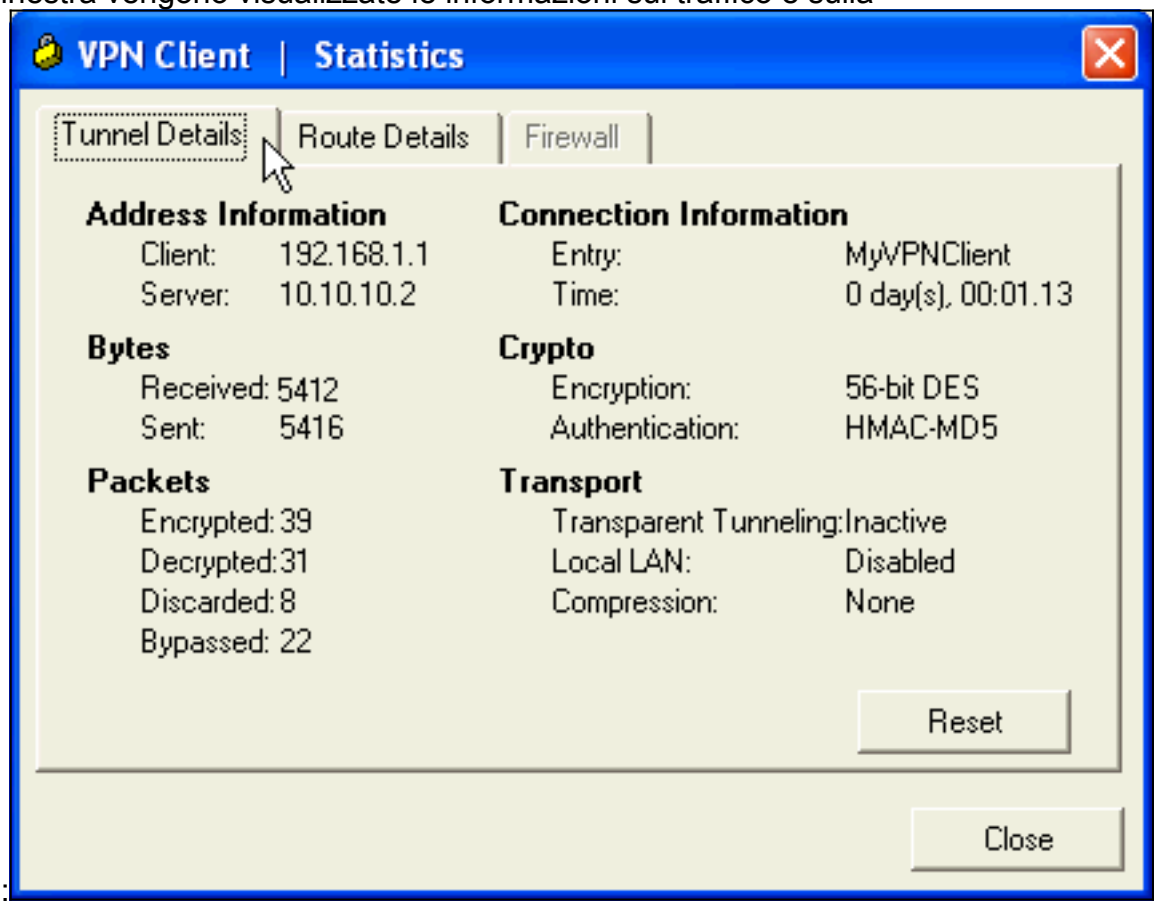


4. Immettere un nome utente e una password per l'autenticazione estesa. Queste informazioni devono corrispondere a quelle specificate nei **passaggi 5 e**


6.
5. Una volta stabilita la connessione, scegliere **Statistics** dal menu Status per verificare i dettagli del
tunnel.

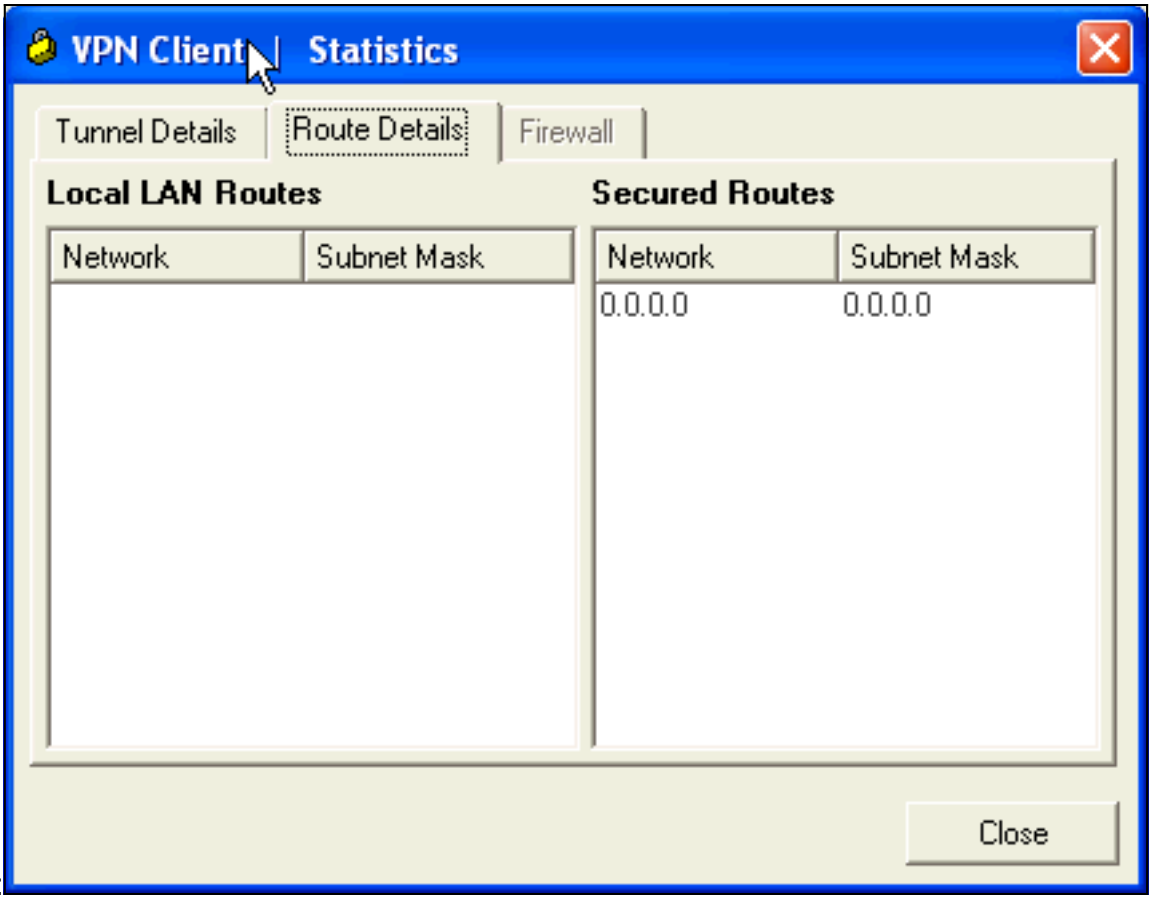


In questa finestra vengono visualizzate le informazioni sul traffico e sulla crittografia:



Questa finestra mostra le informazioni sul tunneling

suddiviso:



ASA/PIX Security Appliance - Comandi show

- **show crypto isakmp sa**: visualizza tutte le associazioni di protezione IKE correnti in un peer.

```
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
```

- **show crypto ipsec sa**: visualizza tutte le SA IPsec correnti in un peer.

```
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
  ```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

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

Per ulteriori informazioni su come risolvere i problemi relativi alla VPN da sito a sito, fare riferimento a L2L e alle soluzioni di risoluzione dei problemi per le VPN IPSec di accesso remoto più comuni.

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- Cisco Adaptive Security Device Manager
- Cisco ASA serie 5500 Adaptive Security Appliance - Risoluzione dei problemi e avvisi
  ```

- Documentazione e supporto tecnico – Cisco Systems