PIX/ASA come server VPN remoto con autenticazione estesa utilizzando la CLI e la configurazione ASDM

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Prodotti correlati
Convenzioni
Premesse
Configurazioni
Configurazione di ASA/PIX come server VPN remoto con ASDM
Configurazione di ASA/PIX come server VPN remoto tramite CLI
Configurazione archiviazione password client VPN Cisco
Disabilita autenticazione estesa
Verifica
Risoluzione dei problemi
ACL di crittografia non corretto
Informazioni correlate

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 la CLI. 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 con il client VPN Cisco.

Per configurare la connessione VPN di accesso remoto tra un client VPN Cisco (4.x per Windows) e l'appliance di sicurezza PIX serie 500 7.x, fare riferimento agli esempi di configurazione dell'autenticazione PIX/ASA 7.x e Cisco VPN Client 4.x con Windows 2003 RADIUS (con Active Directory). L'utente client VPN remoto esegue l'autenticazione in Active Directory utilizzando un server RADIUS Microsoft Windows 2003 Internet Authentication Service (IAS).

Per configurare una connessione VPN di accesso remoto tra un client VPN Cisco (4.x per Windows) e l'appliance di sicurezza PIX serie 500 7.x con Cisco Secure Access Control Server (ACS versione 3.2) per l'autenticazione estesa (Xauth), fare riferimento agli esempi di configurazione di PIX/ASA 7.x e Cisco VPN Client 4.x per l'autenticazione ACS sicura (Cisco Secure ACS versione 3.2).

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.

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 a un utente, 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 ai quali vengono autenticati gli utenti del tunnel, nonché gli eventuali server di accounting ai quali vengono inviate le informazioni sulle connessioni. 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.

Nota: nella configurazione di esempio di questo documento, per l'autenticazione vengono utilizzati gli account utente locali. Per utilizzare un altro servizio, ad esempio LDAP e RADIUS, vedere Configurazione di un server RADIUS esterno per l'autorizzazione e l'autenticazione.

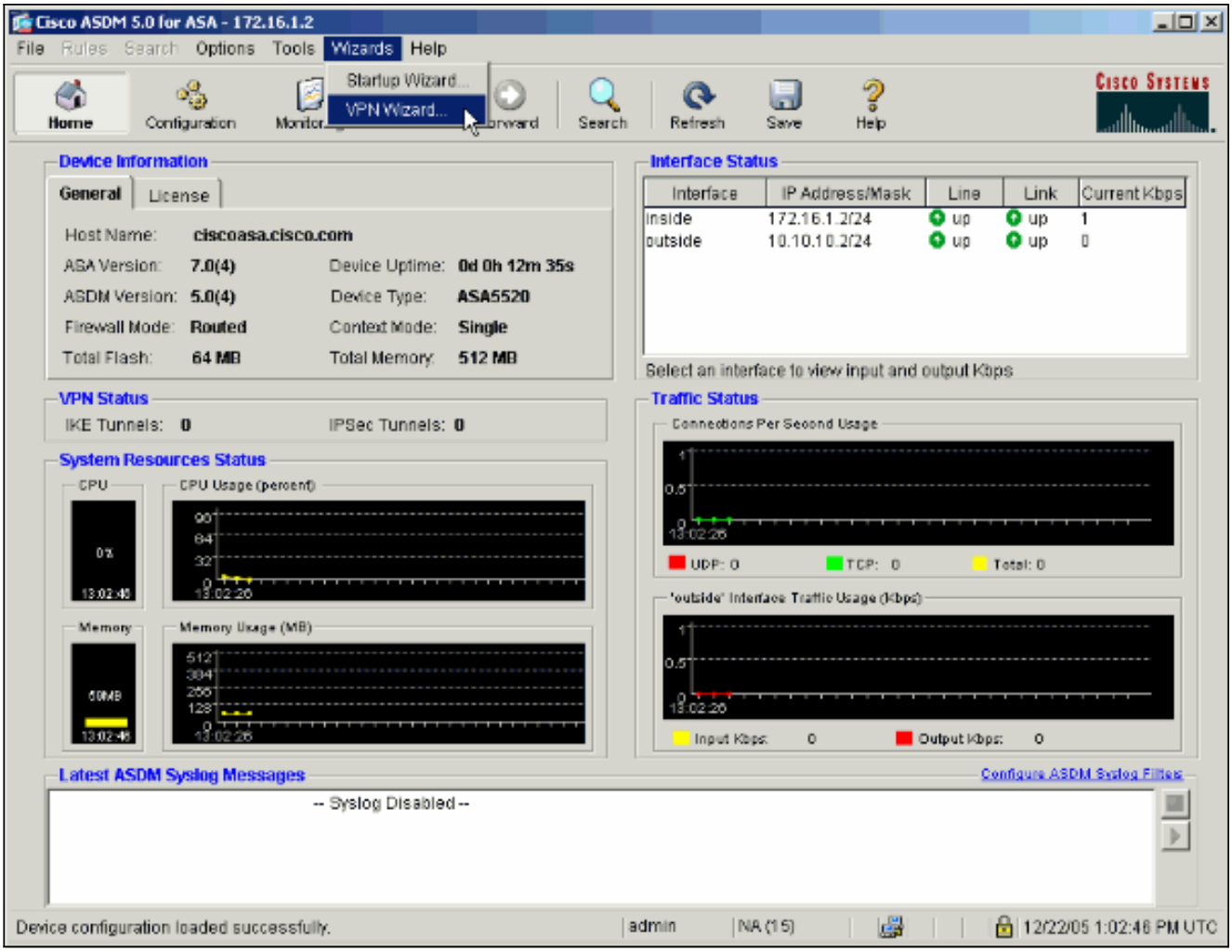
Il protocollo ISAKMP (Internet Security Association and Key Management Protocol), noto anche come IKE, è il protocollo di negoziazione che ospita la negoziazione su come creare un'associazione di protezione IPSec. Ogni negoziazione ISAKMP è divisa in due sezioni, Fase1 e Fase2. La Fase1 crea il primo tunnel per proteggere i messaggi di negoziazione ISAKMP successivi. La fase 2 crea il tunnel che protegge i dati che viaggiano attraverso la connessione protetta. per ulteriori informazioni su ISAKMP, fare riferimento a Parole chiave delle policy ISAKMP per i comandi CLI.

Configurazioni

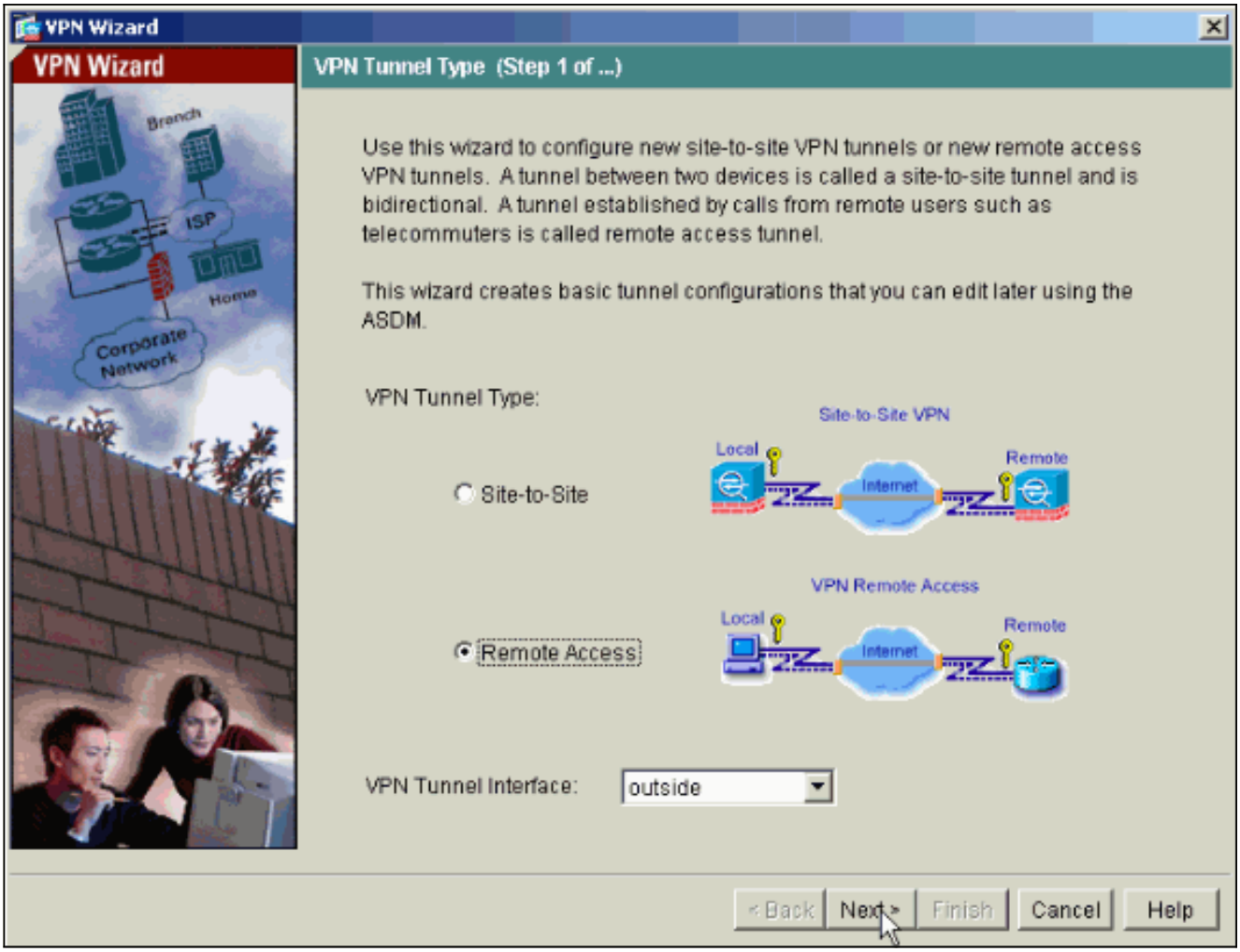
Configurazione di ASA/PIX come server VPN remoto con ASDM

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

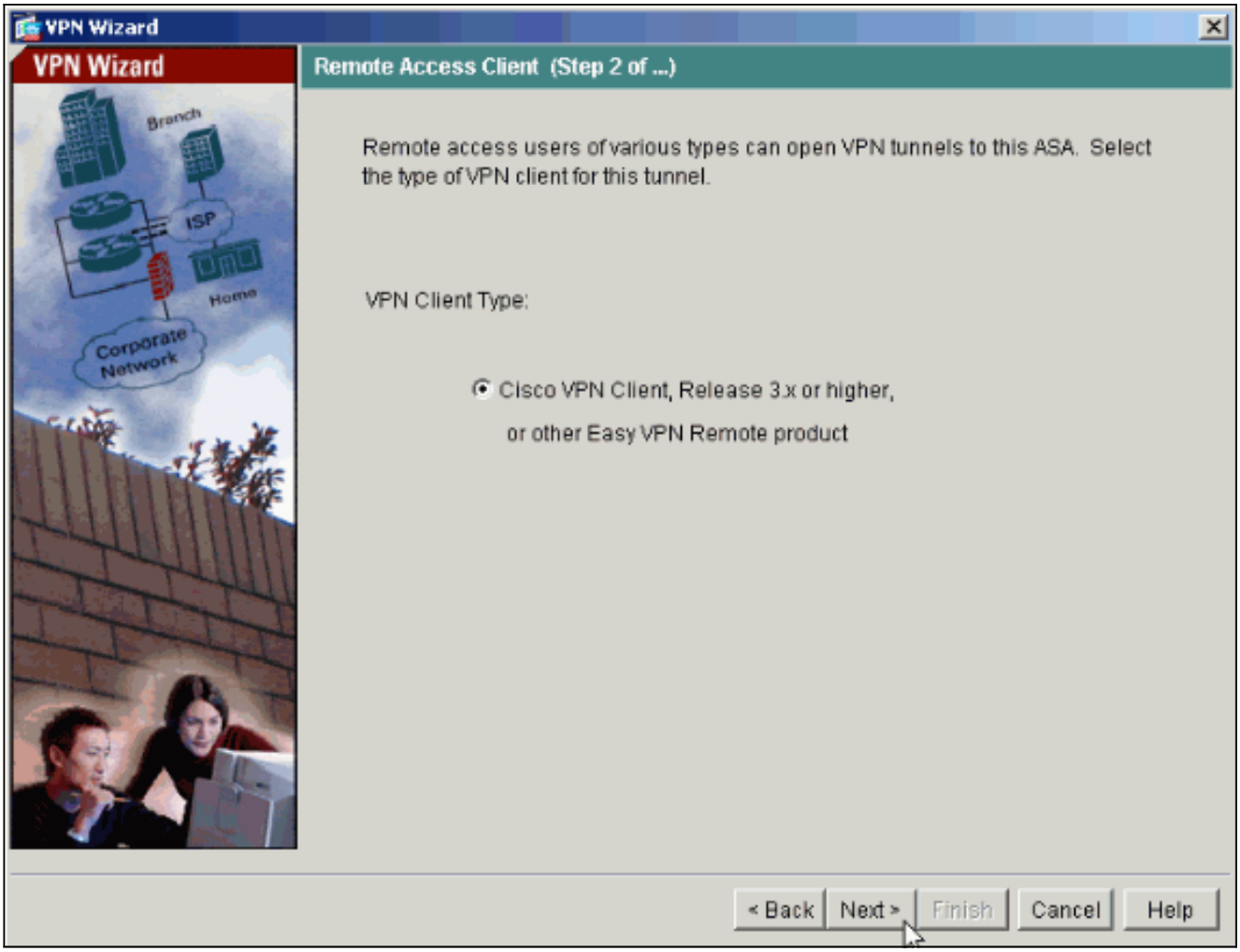
1. Selezionare **Procedure guidate > Creazione guidata VPN** dalla finestra Home.



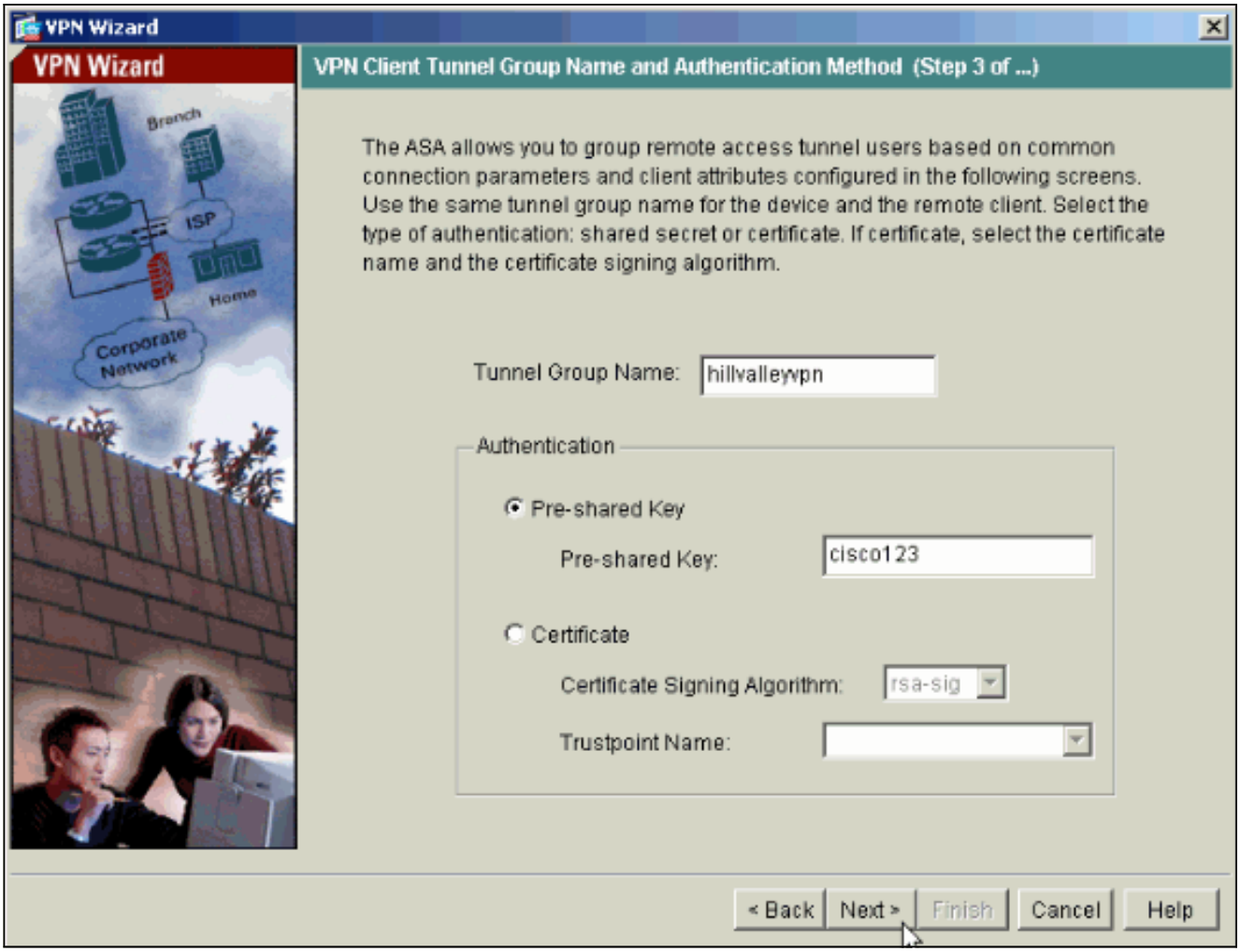
2. Selezionare il tipo di tunnel VPN di **accesso remoto** e verificare che l'interfaccia tunnel VPN sia impostata come
desiderato.



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

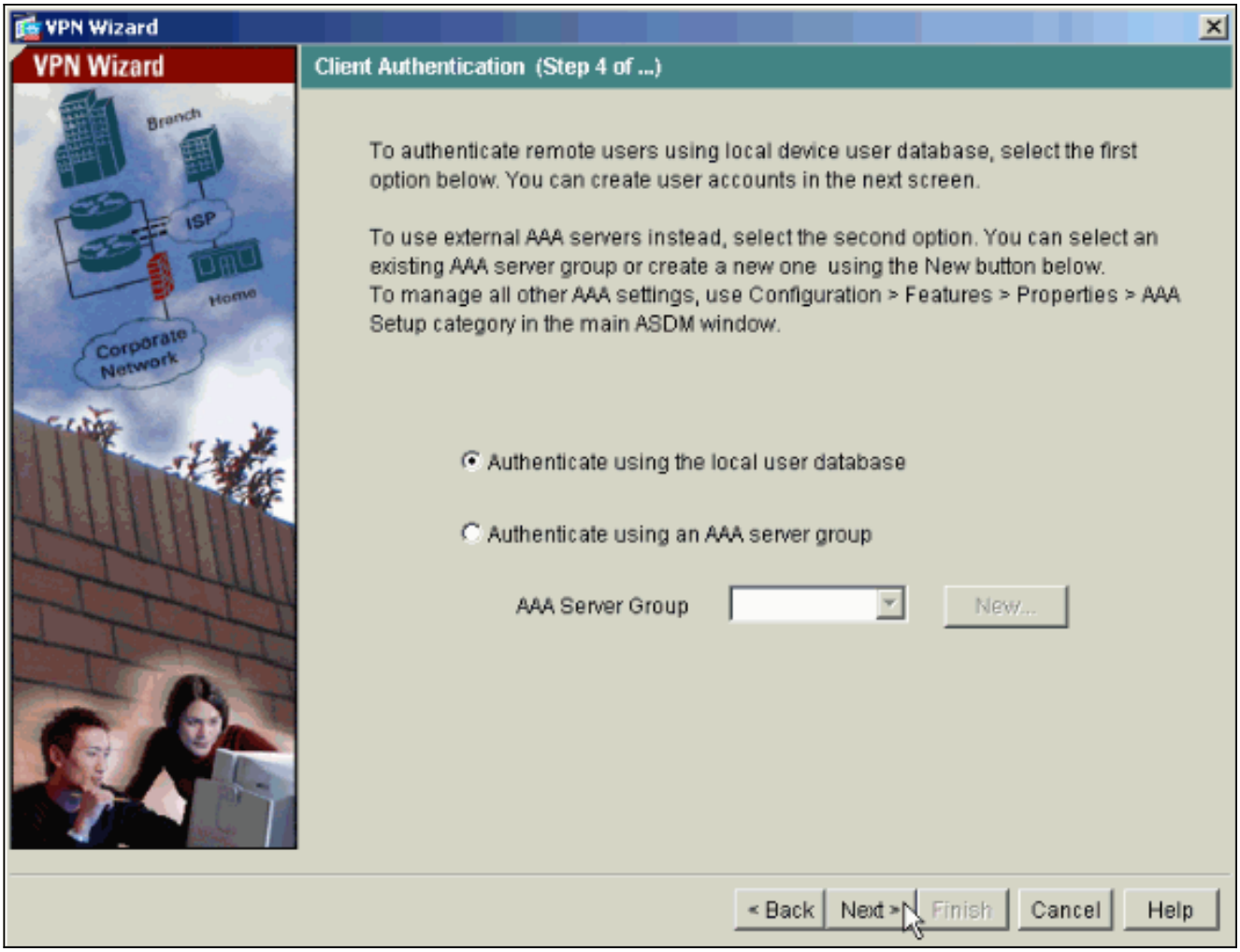


4. Immettere un nome per il nome del gruppo di tunnel. Specificare le informazioni di autenticazione da utilizzare.In questo esempio è selezionata la **chiave già condivisa**.

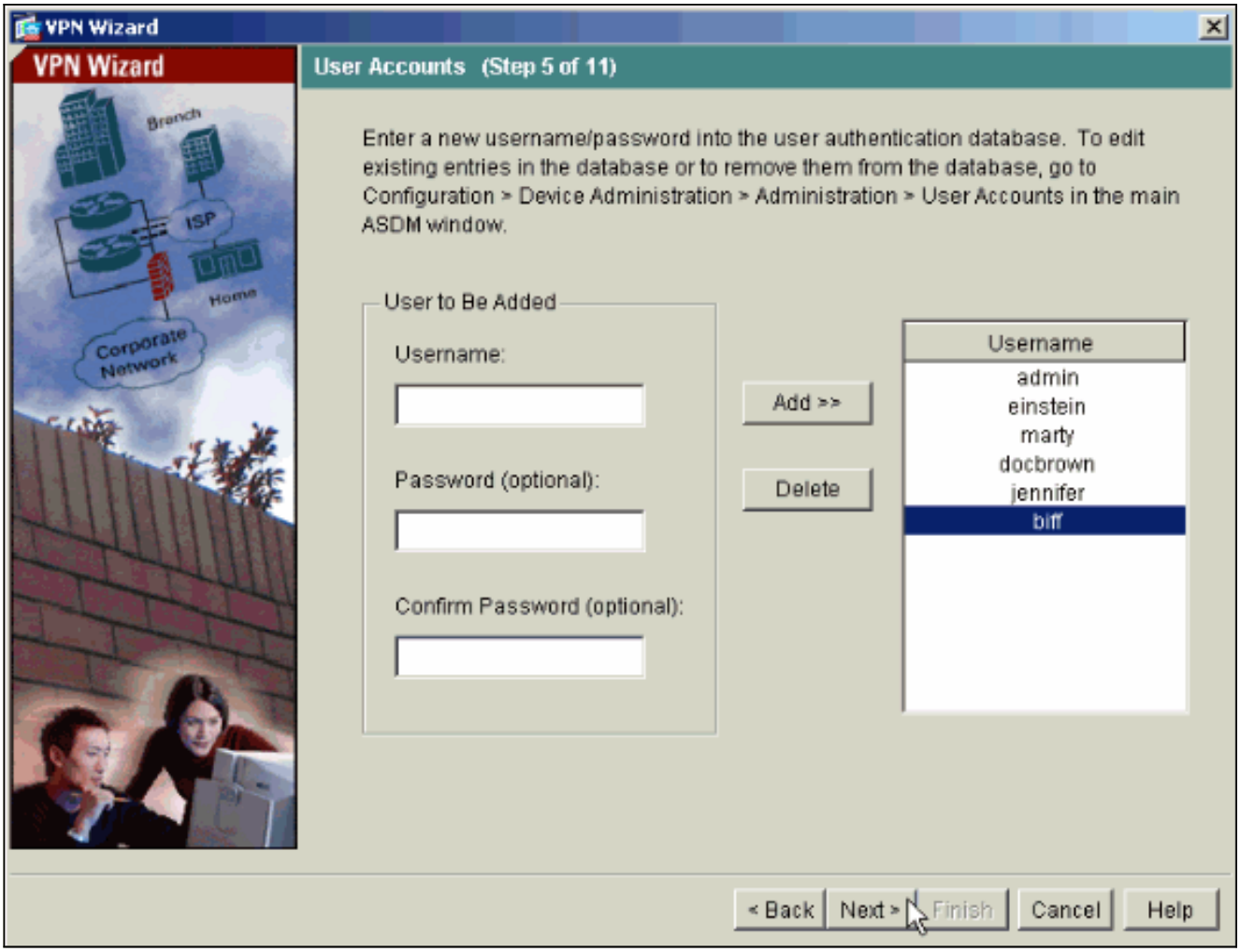


Nota: non è possibile nascondere/crittografare la chiave già condivisa sull'ASDM. La ragione è che l'ASDM deve essere utilizzata solo da utenti che configurano l'ASA o da utenti che assistono il cliente nella configurazione.

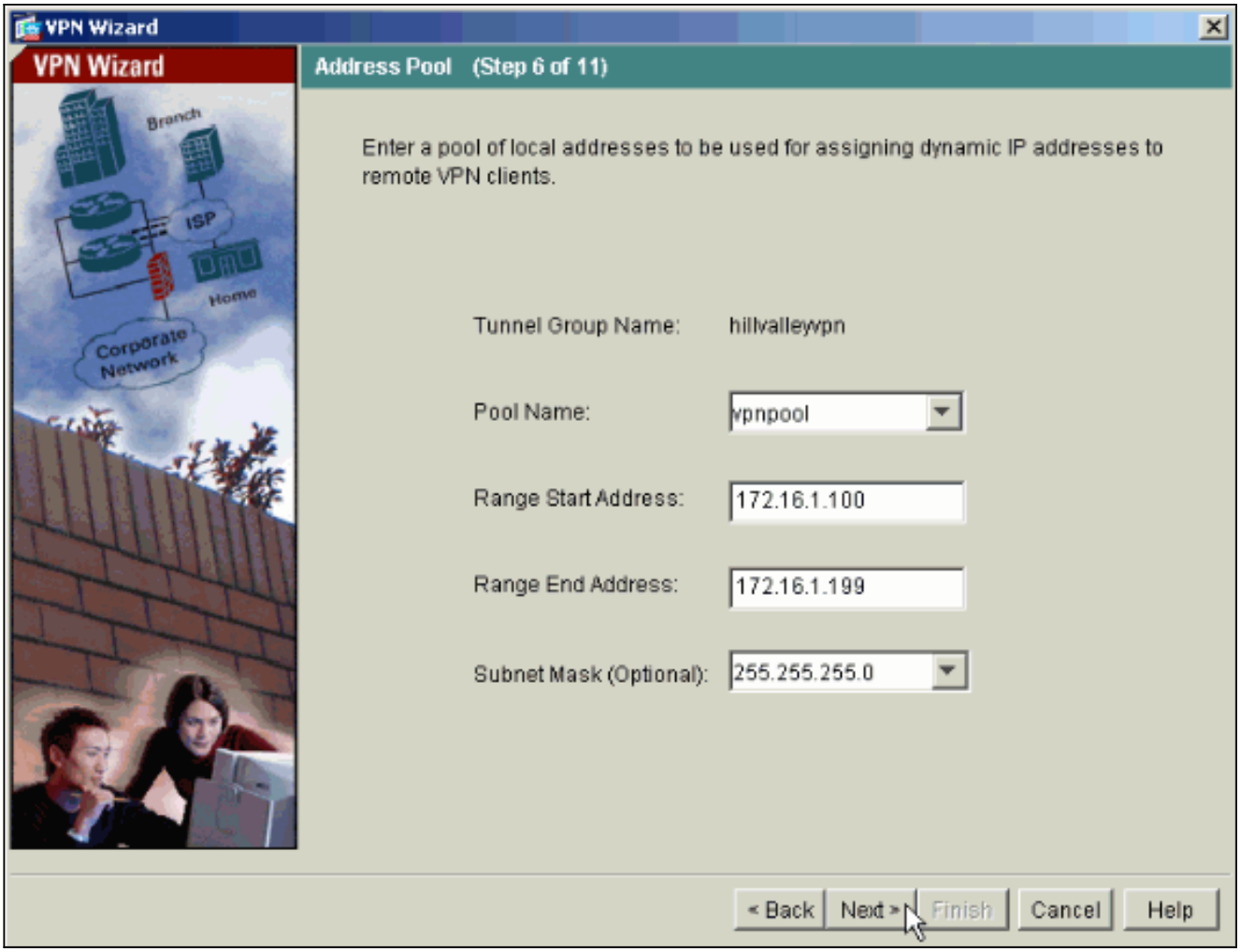
5. Specificare se si desidera che gli utenti remoti vengano autenticati nel database degli utenti locale o in un gruppo di server AAA esterno.**Nota:** aggiungere gli utenti al database locale nel passo 6.**Nota: per** informazioni su come configurare un gruppo di server AAA esterno tramite ASDM, fare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



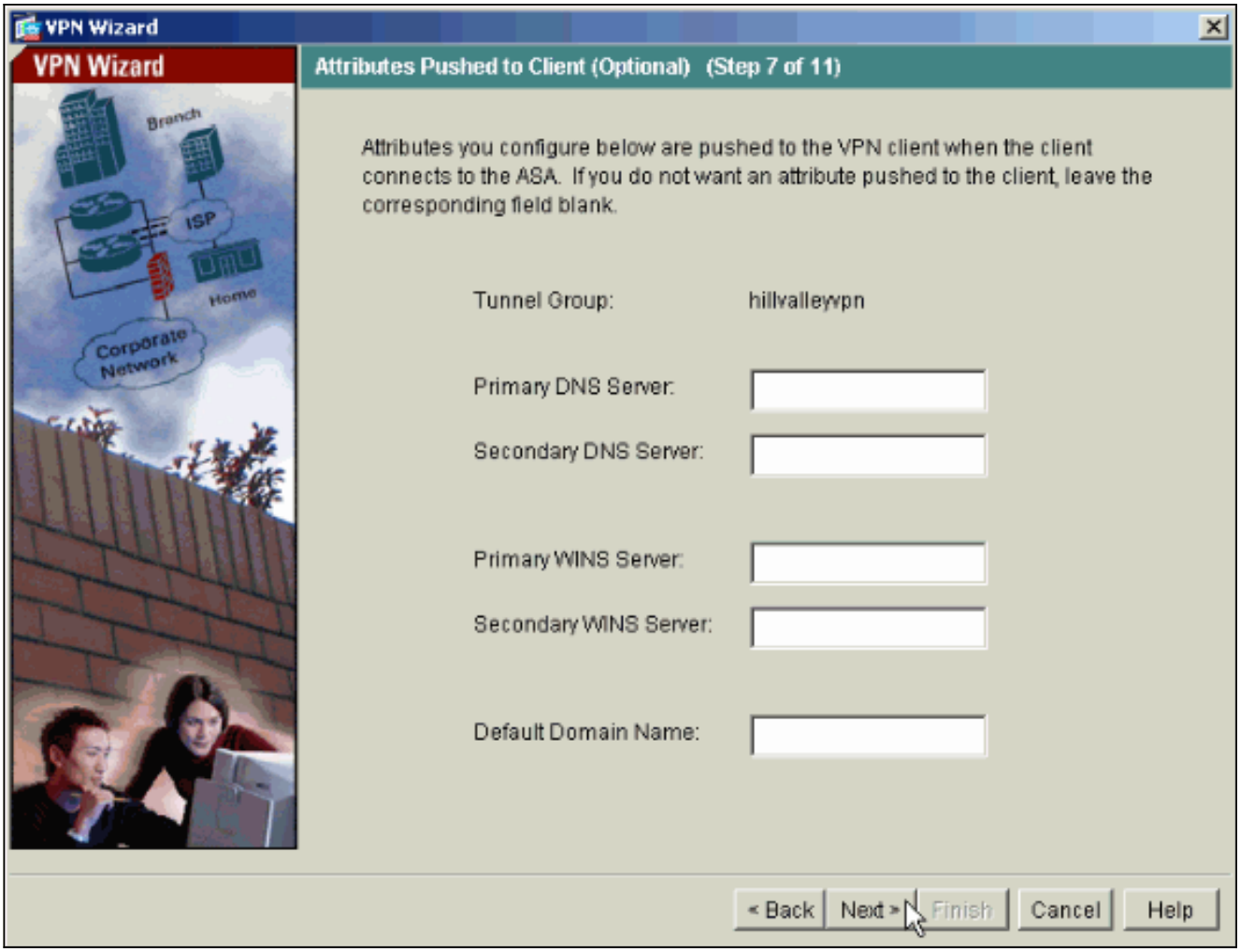
6. Se necessario, aggiungere utenti al database locale.**Nota:** non rimuovere gli utenti esistenti da questa finestra. Selezionare **Configurazione > Amministrazione dispositivi > Amministrazione > Account utente nella finestra principale di ASDM** per modificare le voci esistenti nel database o rimuoverle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



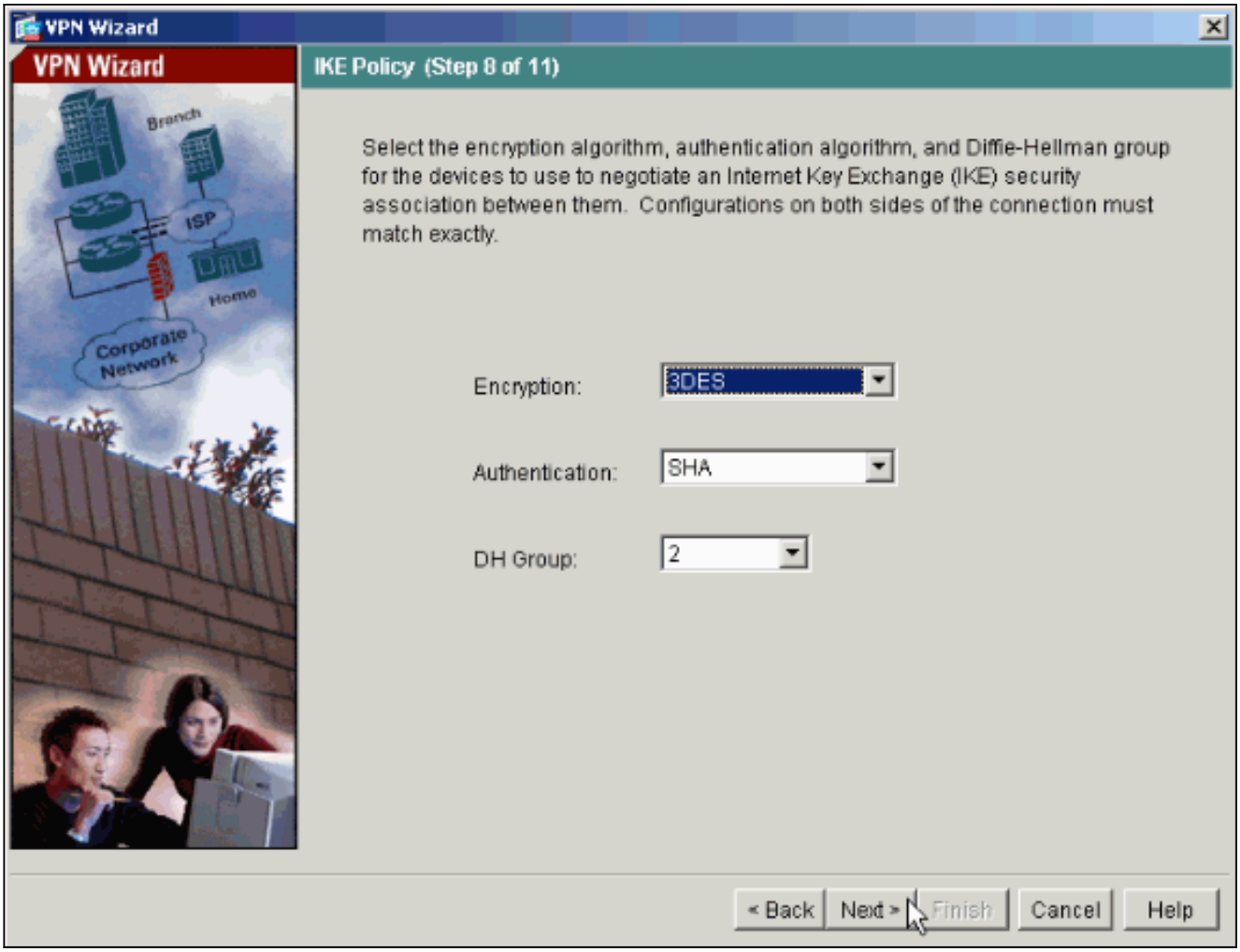
7. Definire un pool di indirizzi locali da assegnare dinamicamente ai client VPN remoti quando si
connettono.



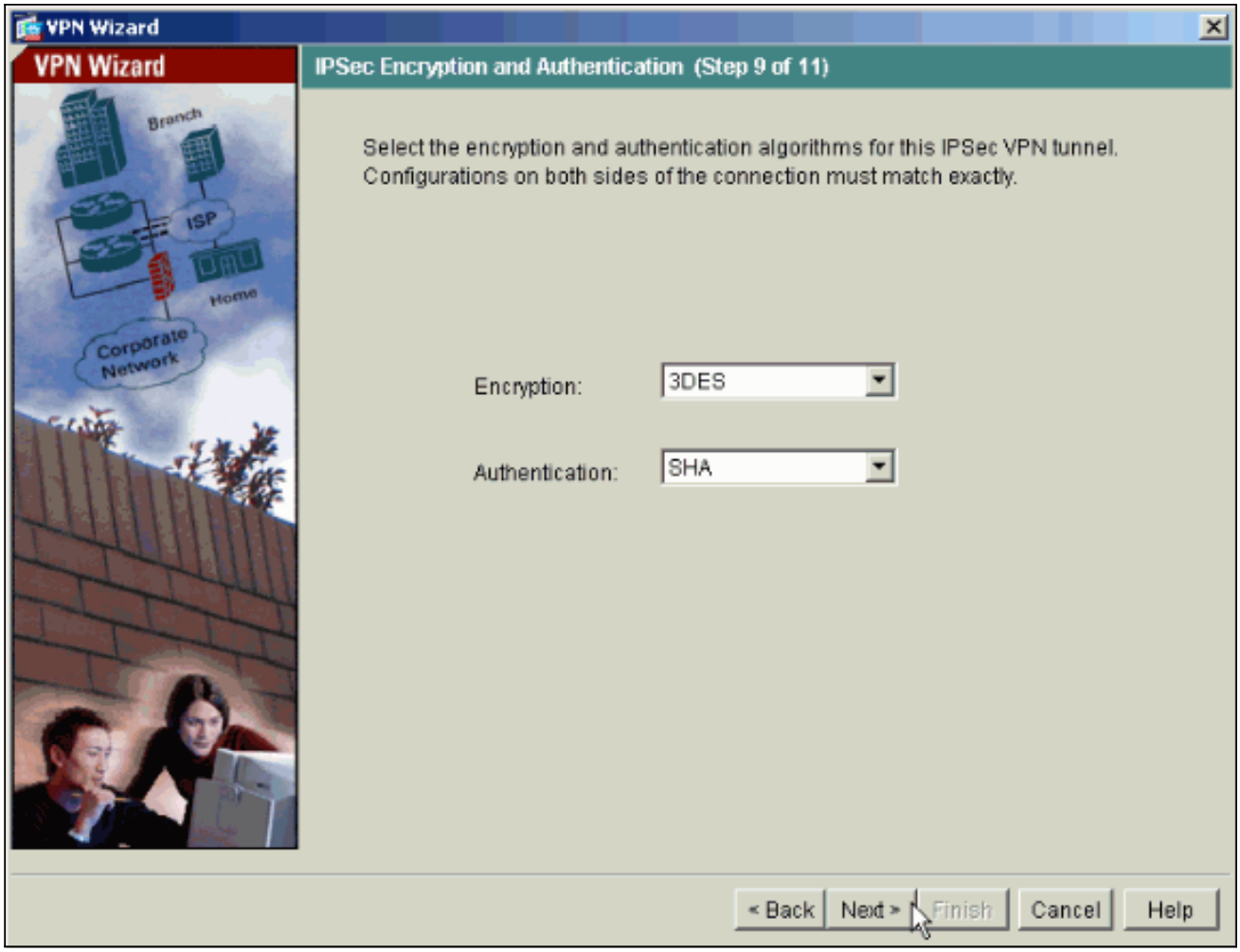
8. *Facoltativo:* Specificare le informazioni sui server DNS e WINS e un nome di dominio predefinito da inserire nei client VPN
remoti.



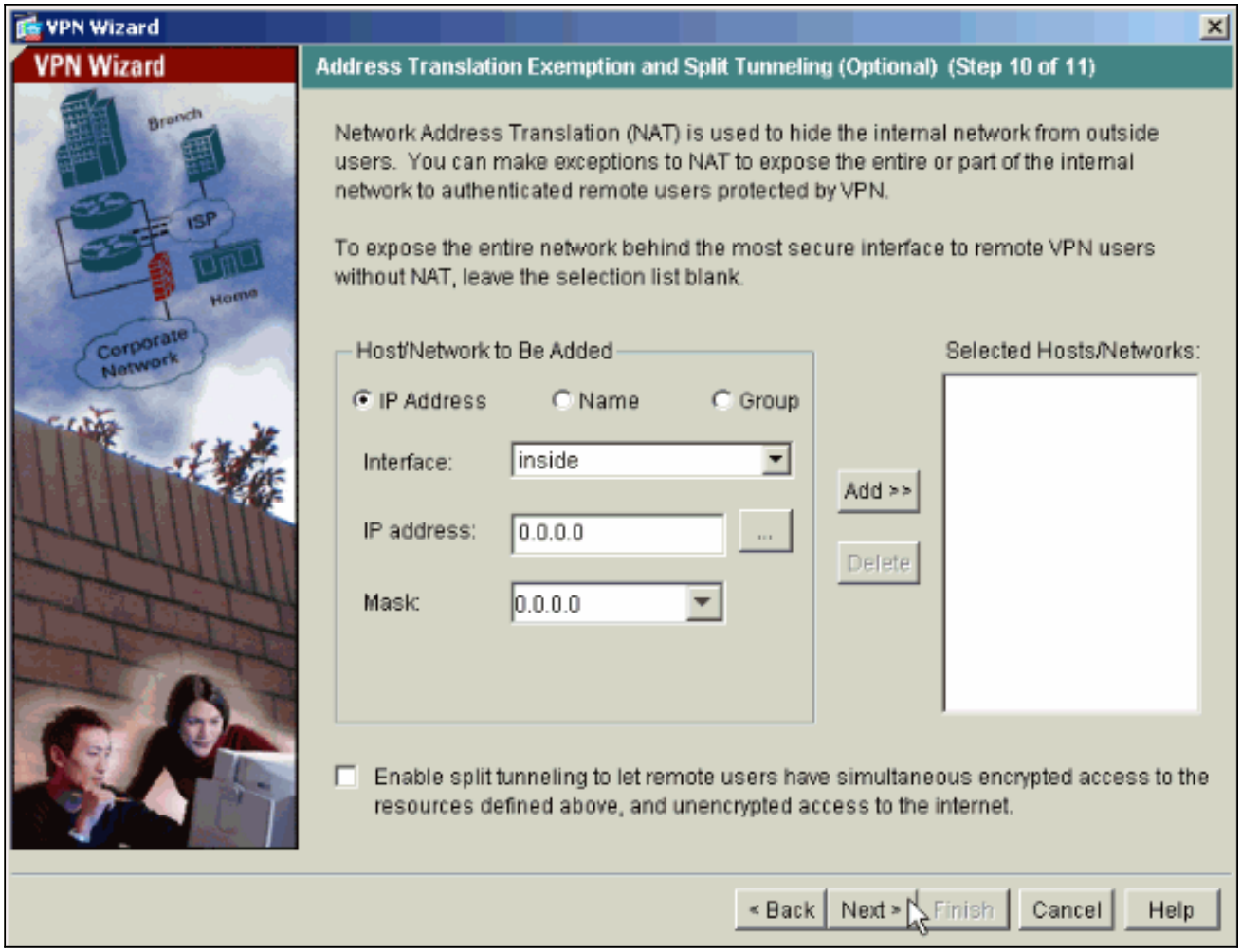
9. Specificare i parametri per IKE, noto anche come IKE fase 1.Le configurazioni su entrambi i lati del tunnel devono corrispondere esattamente. Tuttavia, il client VPN Cisco seleziona automaticamente la configurazione corretta. Non è pertanto necessaria alcuna configurazione IKE sul PC
client.



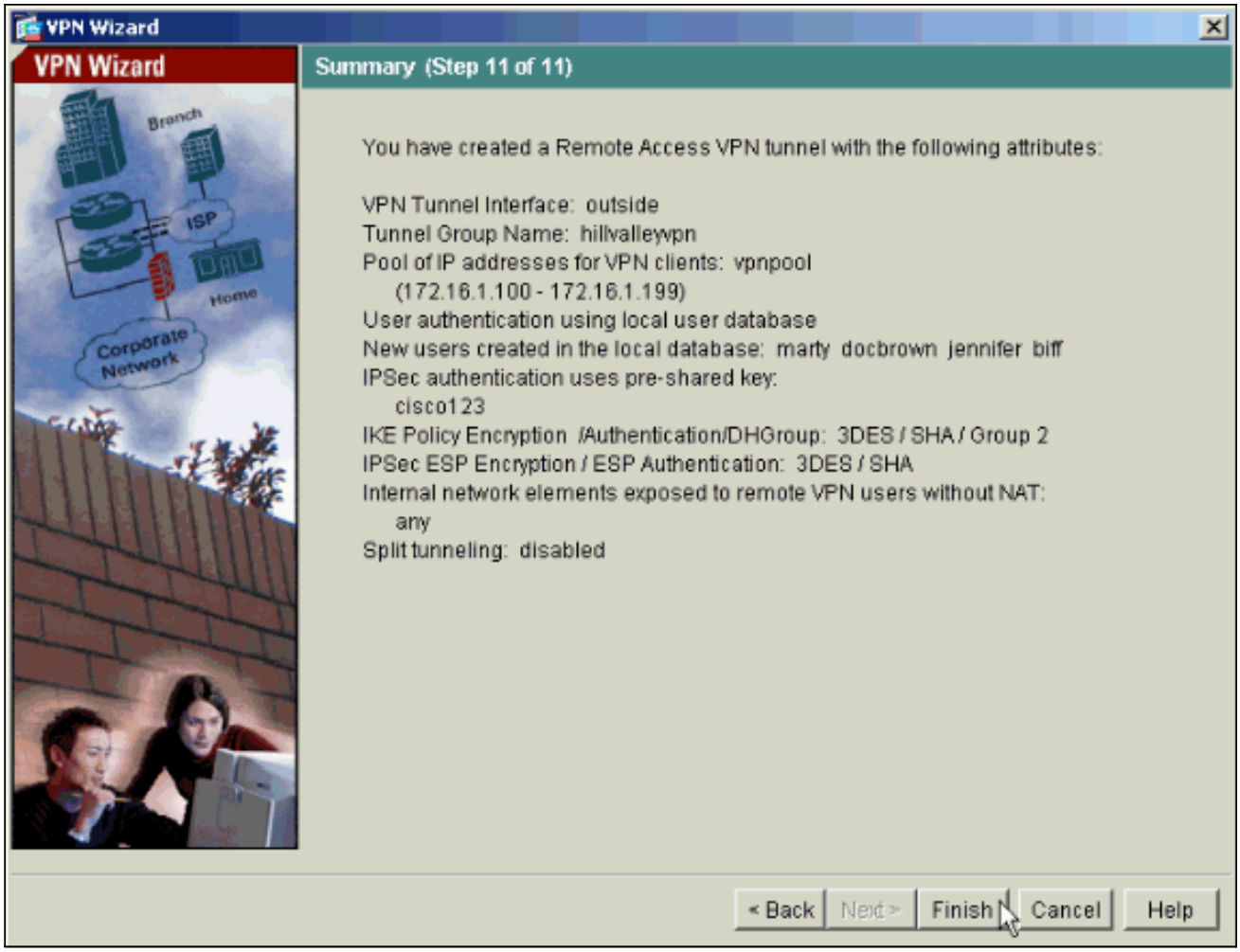
10. Specificare i parametri per IPSec, noto anche come IKE fase 2.Le configurazioni su entrambi i lati del tunnel devono corrispondere esattamente. Tuttavia, il client VPN Cisco seleziona automaticamente la configurazione corretta. Non è pertanto necessaria alcuna configurazione IKE sul PC
client.



11. Specificare gli eventuali host interni o reti da esporre 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.



Configurazione di ASA/PIX come server VPN remoto tramite CLI

Completare questa procedura per configurare un server di accesso VPN remoto dalla riga di comando. Per ulteriori informazioni su ciascun comando usato, consultare il documento sulla configurazione delle VPN di accesso remoto o sulla guida di riferimento dei comandi di Cisco ASA serie 5500 Adaptive Security Appliance.

1. Per configurare i pool di indirizzi IP da utilizzare per i tunnel di accesso remoto VPN, immettere il comando **ip local pool** in modalità di configurazione globale. Per eliminare i pool di indirizzi, immettere la forma no di questo comando.L'appliance di sicurezza utilizza pool di indirizzi basati sul gruppo di tunnel per la connessione. Se si configurano più pool di indirizzi per un gruppo di tunnel, l'appliance di sicurezza li utilizza nell'ordine in cui sono configurati. Per creare un pool di indirizzi locali da utilizzare per assegnare indirizzi dinamici ai client VPN di accesso remoto, eseguire questo comando:
   ```
   ASA-AIP-CLI(config)#ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
     255.255.255.0
   ```

2. Immettere questo comando
   ```
   ASA-AIP-CLI(config)#username marty password 12345678
   ```

3. Utilizzare questo gruppo di comandi per configurare il tunnel specifico:ASA-AIP-CLI(config)**#isakmp criterio 1 autenticazione pre-condivisione**ASA-AIP-CLI(config)**#isakmp policy 1 crittografia 3des**ASA-AIP-CLI(config)**#isakmp policy 1 hash sha**ASA-AIP-CLI(config)**#isakmp criterio 1 gruppo 2**ASA-AIP-CLI(config)**#isakmp criterio 1 durata 43200**ASA-AIP-CLI(config)**#isakmp abilitazione esterna**ASA-AIP-CLI(config)**#crypto ipsec**

transform-set ESP-3DES-SHA esp-3des esp-sha-hmacASA-AIP-CLI(config)#**crypto dynamic-map outside_dyn_map 10 set transform-set ESP-3DES-SHA**ASA-AIP-CLI(config)#**crypto dynamic-map outside_dyn_map 10 impostata su reverse-route**ASA-AIP-CLI(config)#**crypto dynamic-map outside_dyn_map 10 impostazione della durata dell'associazione di sicurezza in secondi 28800**ASA-AIP-CLI(config)#**crypto map_outside_map 10 ipsec-isakmp dynamic_outside_dyn_map**ASA-AIP-CLI(config)#**crypto map_outside_map interface outside**ASA-AIP-CLI(config)#**crypto isakmp nat-traversal**

4. *Facoltativo:* Se si desidera che la connessione ignori l'elenco degli accessi applicato all'interfaccia, usare questo comando:
   ASA-AIP-CLI(config)#**sysopt connection permit-ipsec**

   Nota: questo comando funziona su immagini 7.x precedenti alla 7.2(2). Se si usa l'immagine 7.2(2), usare il comando ASA-AIP-CLI(config)#syspot connection allow-vpn.
5. Immettere questo comando
   ASA-AIP-CLI(config)#**group-policy hillvalleyvpn internal**

6. Per configurare le impostazioni di connessione client, eseguire questi comandi:**Attributi** ASA-AIP-CLI(config)#**group-policy hillvalleyvpn**ASA-AIP-CLI(config)#(config-group-policy)#**dns-server valore 172.16.1.11**ASA-AIP-CLI(config)#(config-group-policy)#**vpn-tunnel-protocol-IPSec**ASA-AIP-CLI(config)#(config-group-policy)#**default-domain valore test.com**
7. Immettere questo comando
   ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn ipsec-ra**

8. Immettere questo comando
   ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn ipsec-attributes**

9. Immettere questo comando
   ASA-AIP-CLI(config-tunnel-ipsec)#**pre-shared-key cisco123**

10. Immettere questo comando
    ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn general-attributes**

11. Utilizzare questo comando per fare riferimento al database degli utenti locale per l'autenticazione.
    ASA-AIP-CLI(config-tunnel-general)#**authentication-server-group LOCAL**

12. Associare i Criteri di gruppo al gruppo di tunnel
    ASA-AIP-CLI(config-tunnel-ipsec)# **default-group-policy hillvalleyvpn**

13. Usare questo comando nella modalità general-attributes del gruppo del tunnel hillvalleyvpn per assegnare il pool vpn creato nel passaggio 1 al gruppo hillvalleyvpn.
    ASA-AIP-CLI(config-tunnel-general)#**address-pool vpnpool**

Esecuzione della configurazione sul dispositivo ASA

```
ASA-AIP-CLI(config)#show running-config
ASA Version 7.2(2)
!
hostname ASAwAIP-CLI
domain-name corp.com
enable password WwXYvtKrnjXqGbu1 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
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name corp.com
pager lines 24
mtu outside 1500
mtu inside 1500
ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
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
group-policy hillvalleyvpn1 internal
group-policy hillvalleyvpn1 attributes
 dns-server value 172.16.1.11
 vpn-tunnel-protocol IPSec
 default-domain value test.com
username marty password 6XmYwQOO9tiYnUDN encrypted
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
sha-hmac
crypto dynamic-map outside_dyn_map 10 set transform-set
```

```
ESP-3DES-SHA
crypto dynamic-map outside_dyn_map 10 set security-
association lifetime seconds 288000
crypto map outside_map 10 ipsec-isakmp dynamic
outside_dyn_map
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp nat-traversal  20
tunnel-group hillvalleyvpn type ipsec-ra
tunnel-group hillvalleyvpn general-attributes
 address-pool vpnpool
 default-group-policy hillvalleyvpn
tunnel-group hillvalleyvpn ipsec-attributes
 pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:0f78ee7ef3c196a683ae7a4804ce1192
: end
ASA-AIP-CLI(config)#
```

Configurazione archiviazione password client VPN Cisco

Se si hanno numerosi client VPN Cisco, è molto difficile ricordare tutti i nomi utente e le password dei client VPN. Per memorizzare le password nel computer client VPN, configurare l'ASA/PIX e il client VPN come descritto in questa sezione.

ASA/PIX

Utilizzare il comando **group-policy attributes** in modalità di configurazione globale:

```
group-policy VPNusers attributes
  password-storage enable
```

Cisco VPN Client

Modificate il **file .pcf** e i seguenti parametri:

```
SaveUserPassword=1
UserPassword=
```

Disabilita autenticazione estesa

In modalità tunnel group, immettere questo comando per disabilitare l'autenticazione estesa, abilitata per impostazione predefinita, su PIX/ASA 7.x:

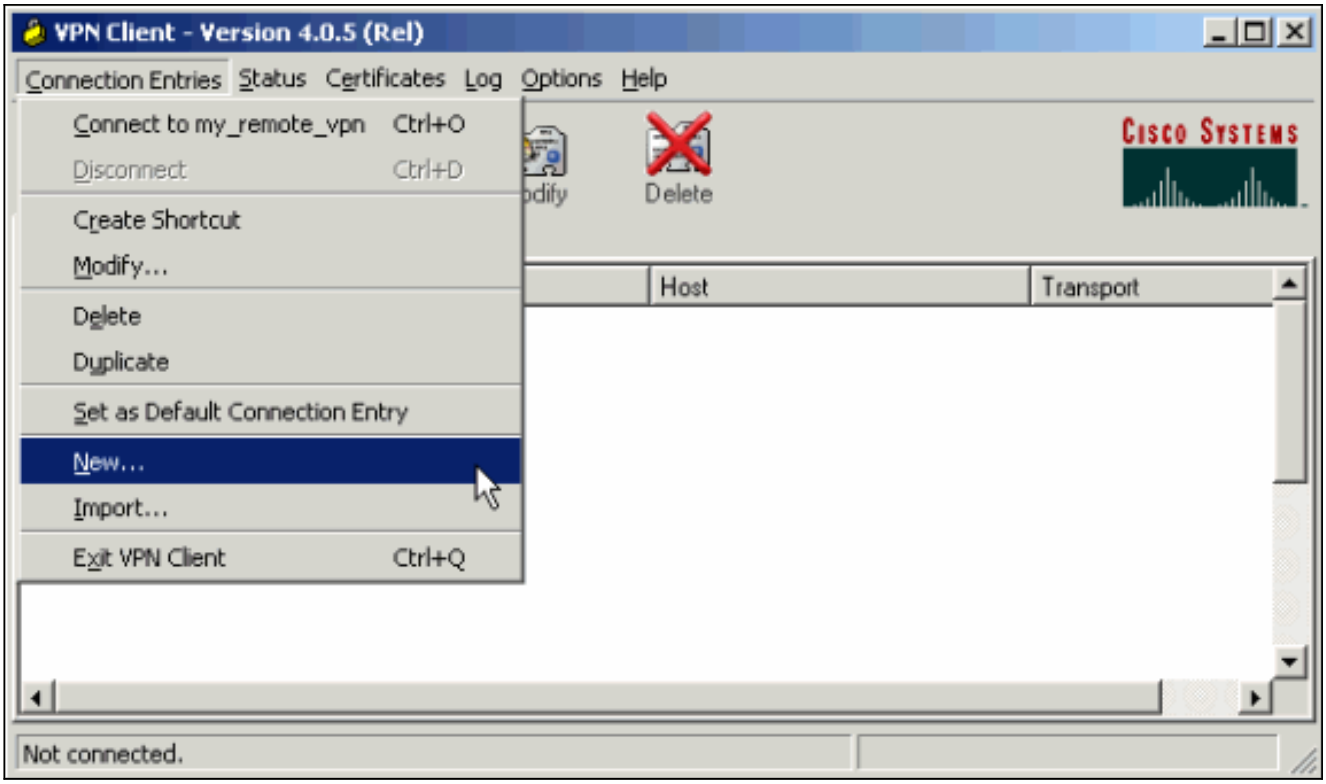
```
asa(config)#tunnel-group client ipsec-attributes
asa(config-tunnel-ipsec)#isakmp ikev1-user-authentication none
```

Dopo aver disabilitato l'autenticazione estesa, i client VPN non visualizzano un nome utente/password per un'autenticazione (Xauth). Pertanto, l'appliance ASA/PIX non richiede la configurazione di nome utente e password per autenticare i client VPN.

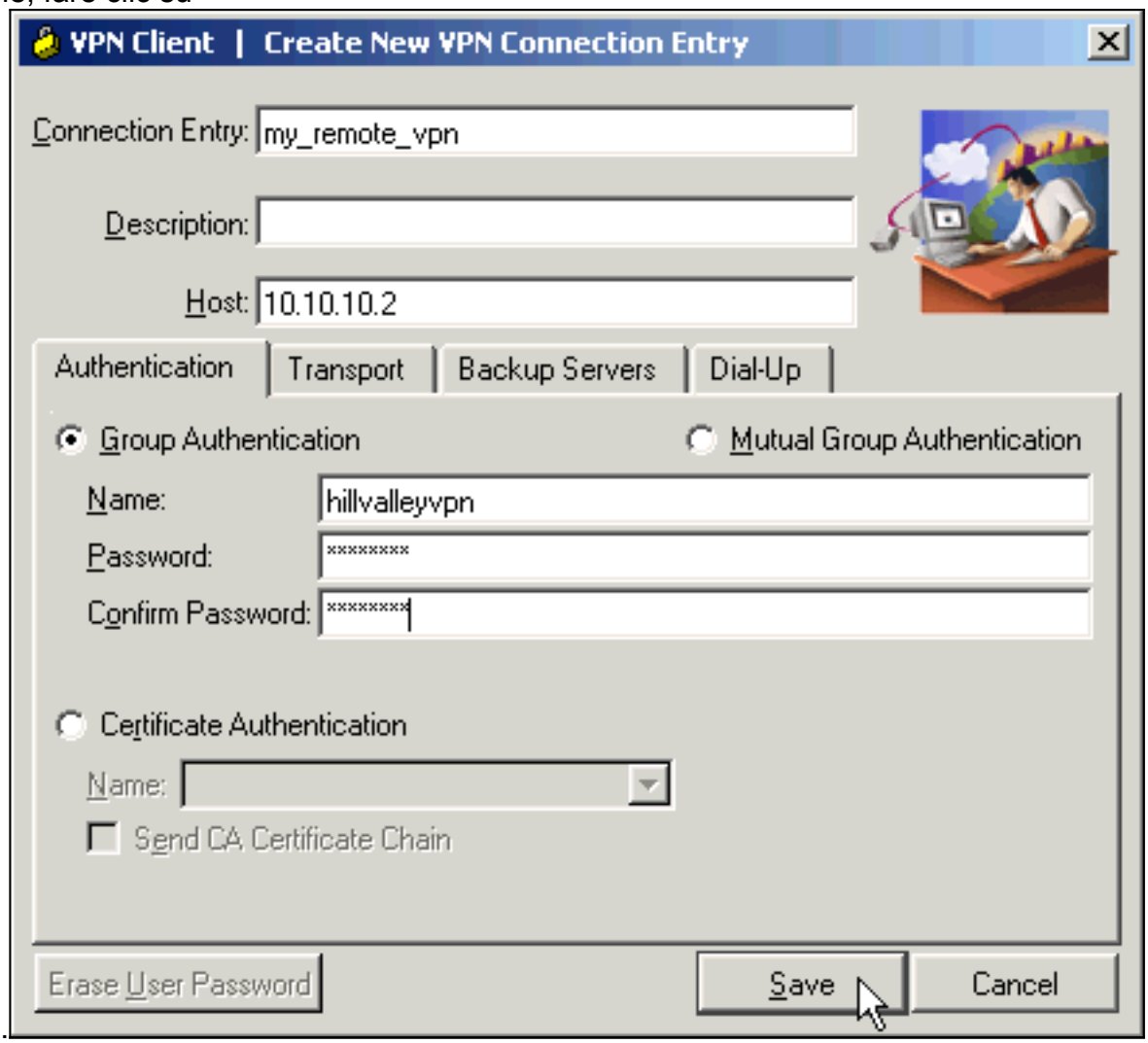
Verifica

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

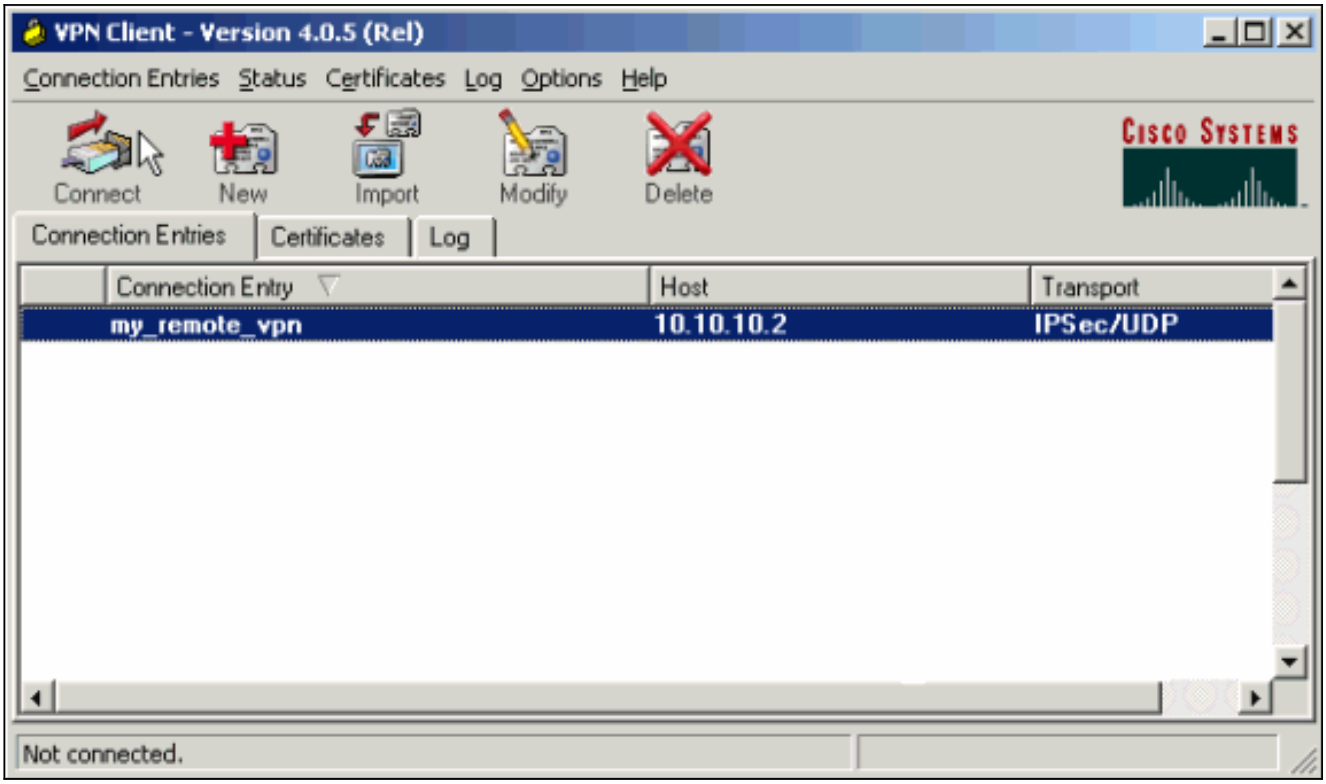
1. Selezionare **Voci di connessione > Nuovo**.



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.

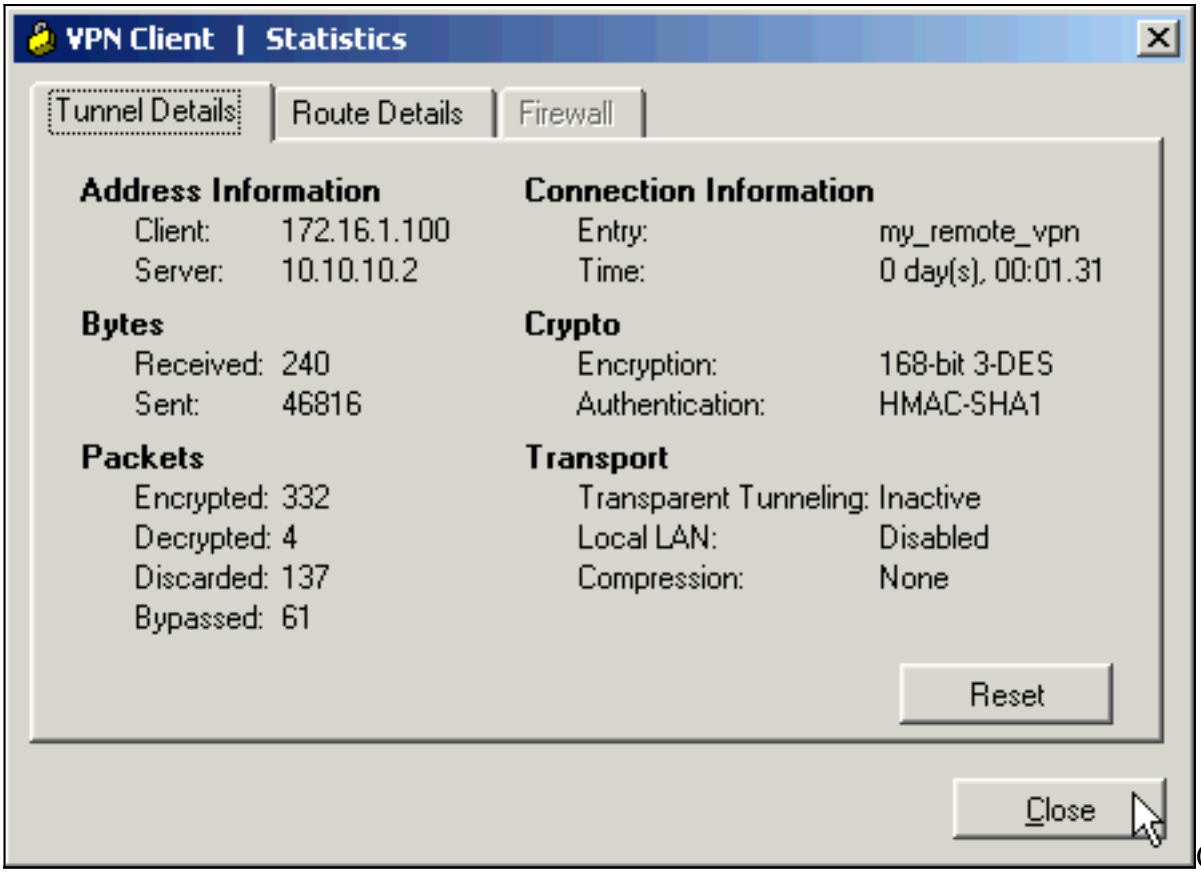


3. Selezionare la connessione appena creata e fare clic su **Connetti**.

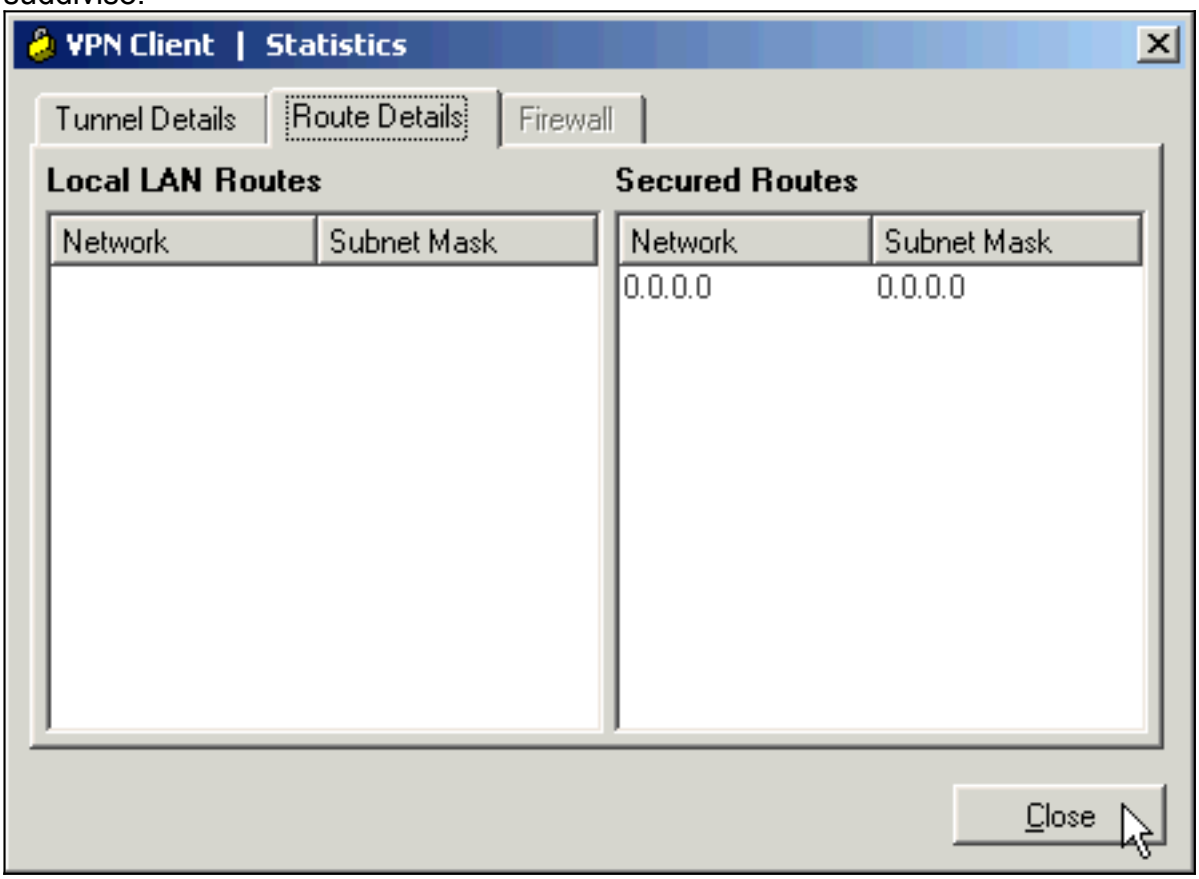


4. Immettere un nome utente e una password per l'autenticazione estesa. Queste informazioni devono corrispondere a quelle specificate nei passaggi 5 e 6.

5. Una volta stabilita la connessione, selezionare **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:



Risoluzione dei problemi

Utilizzare questa sezione per risolvere i problemi relativi alla configurazione.

ACL di crittografia non corretto

ASDM 5.0(2) è noto per creare e applicare un elenco di controllo di accesso (ACL) crittografico che può causare problemi ai client VPN che usano il tunneling suddiviso, nonché ai client hardware in modalità di estensione della rete. Per evitare questo problema, utilizzare ASDM versione 5.0(4.3) o successive. Per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCsc10806 (solo utenti registrati).

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- Soluzioni per la risoluzione dei problemi più comuni di VPN IPsec L2L e ad accesso remoto
- Cisco ASA serie 5500 Adaptive Security Appliance - Risoluzione dei problemi e avvisi
- Documentazione e supporto tecnico – Cisco Systems