SDM Esempio di VPN IPsec da sito a sito tra ASA/PIX e un router IOS

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per il tunnel IPsec da LAN a LAN (da sito a sito) tra le appliance di sicurezza Cisco (ASA/PIX) e un router Cisco IOS. Le route statiche vengono utilizzate per maggiore semplicità.

Per ulteriori informazioni sullo stesso scenario in cui la configurazione del tunnel IPsec da LAN a LAN di un router IOS esegue la versione software *7.x,* fare riferimento all'esempio di configurazione del tunnel IPsec da PIX/ASA 7.x.

Prerequisiti

Requisiti

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

- Prima di avviare questa configurazione, è necessario stabilire la connettività IP end-to-end.
- Ènecessario abilitare la licenza di Security Appliance per la crittografia DES (Data Encryption

Standard) (a un livello di crittografia minimo).

Componenti usati

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

- Cisco Adaptive Security Appliance (ASA) con versione 8.x e successive
- ASDM versione 6.x e successive
- Cisco 1812 router con software Cisco IOS® versione 12.3
- Cisco Security Device Manager (SDM) versione 2.5

Nota: per consentire all'ASDM di configurare l'appliance ASA, consultare il documento sull'autorizzazione dell'accesso HTTPS per ASDM.

Nota: per consentire al router di essere configurato dal modello SDM, consultare il documento sulla configurazione base del router utilizzando l'SDM.

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.

Nota: per ulteriori informazioni, fare riferimento al documento Configuration Professional: Esempio di VPN IPsec da sito a sito tra ASA/PIX e un router IOS per una configurazione simile con Cisco Configuration Professional sul router.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco PIX serie 500 Security Appliance, con versione 7.x e successive.

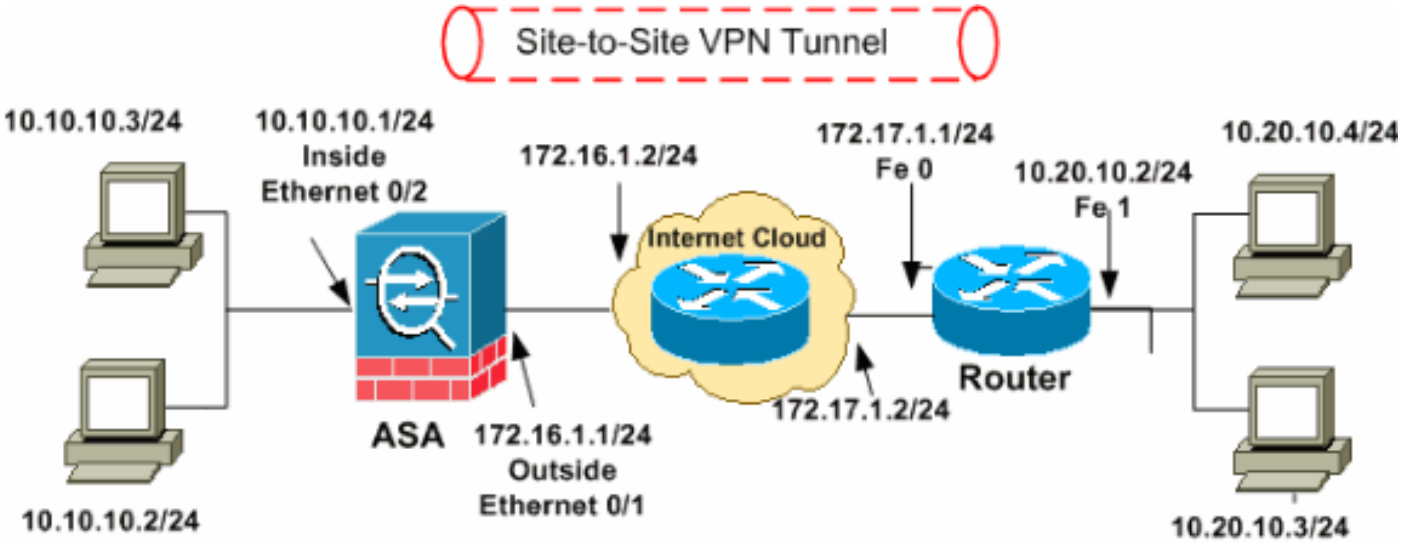
Convenzioni

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

Configurazione

Esempio di rete

Nel documento viene usata l'impostazione di rete mostrata nel diagramma.



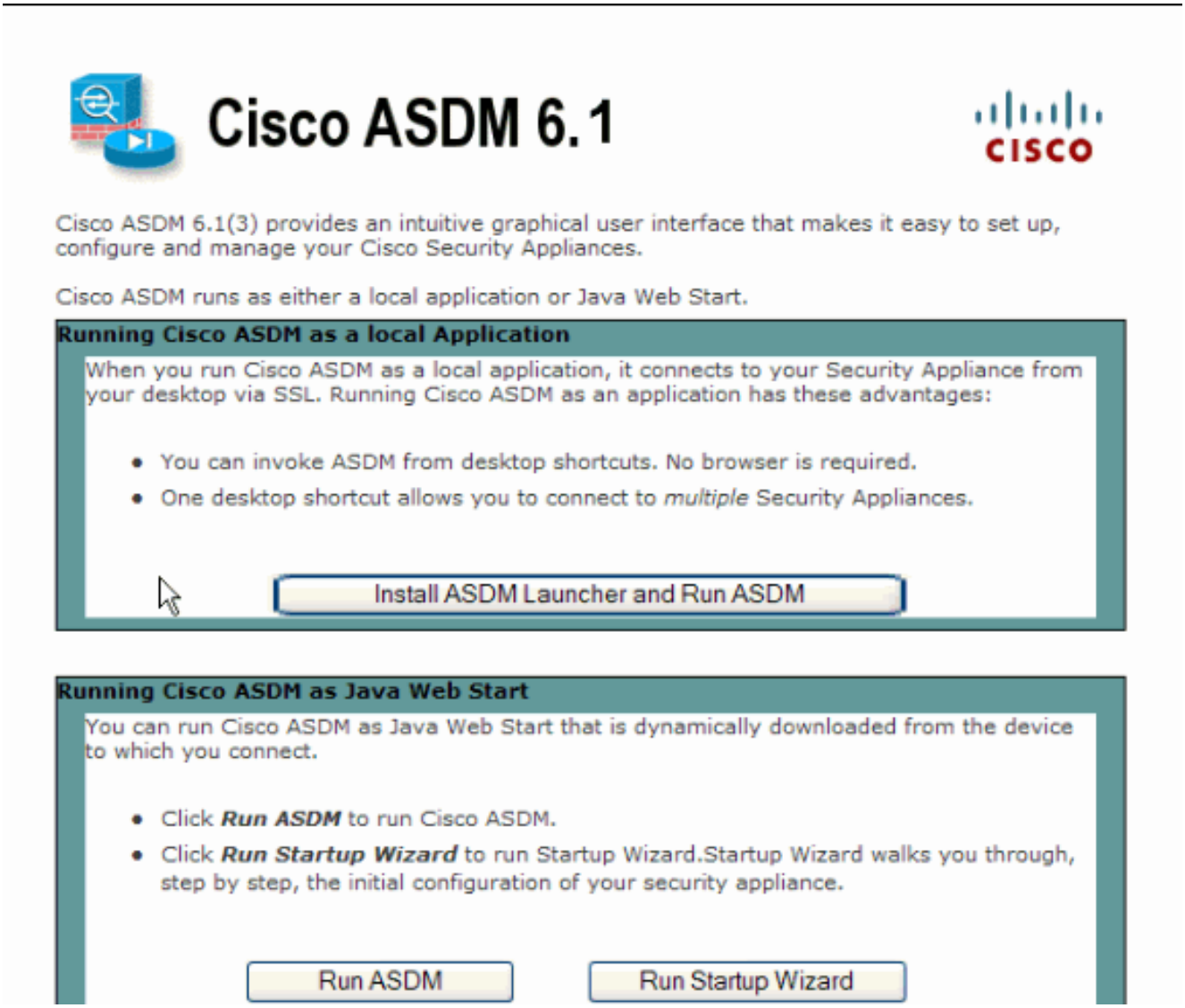
Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

- Configurazione ASDM tunnel VPN
- Configurazione SDM router
- Configurazione ASA CLI
- Configurazione CLI router

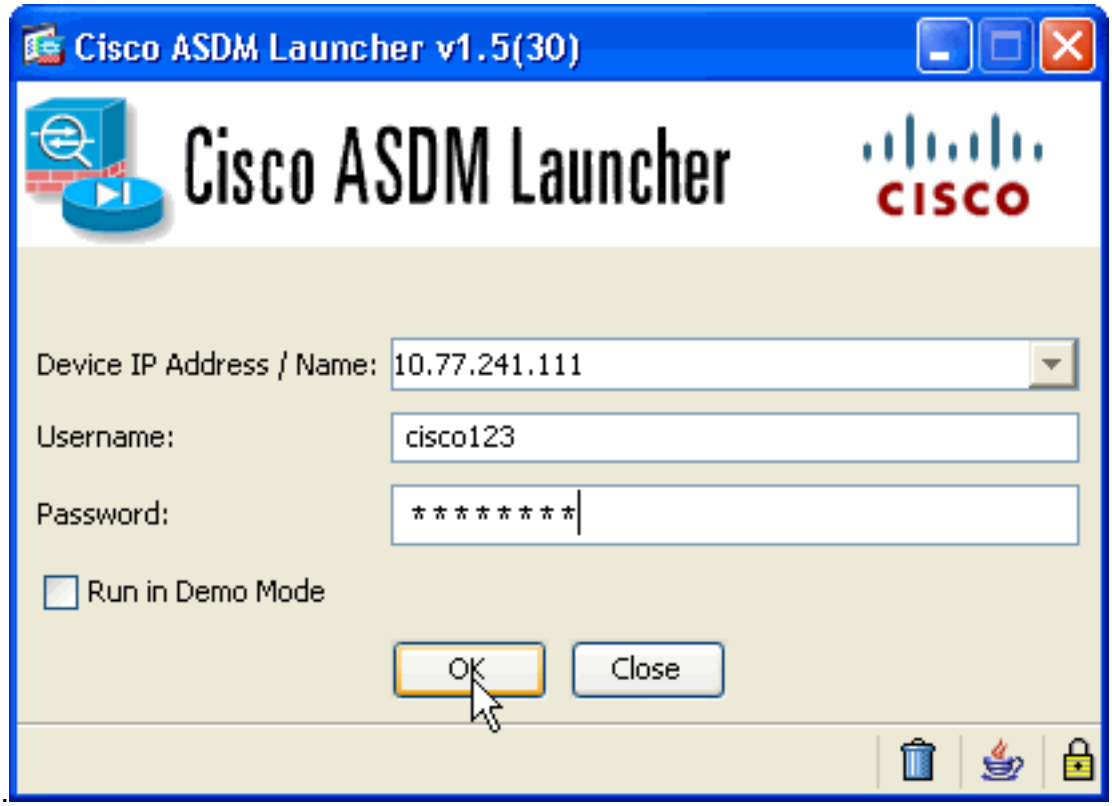
Configurazione ASDM tunnel VPN

Per creare il tunnel VPN, completare i seguenti passaggi:

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.

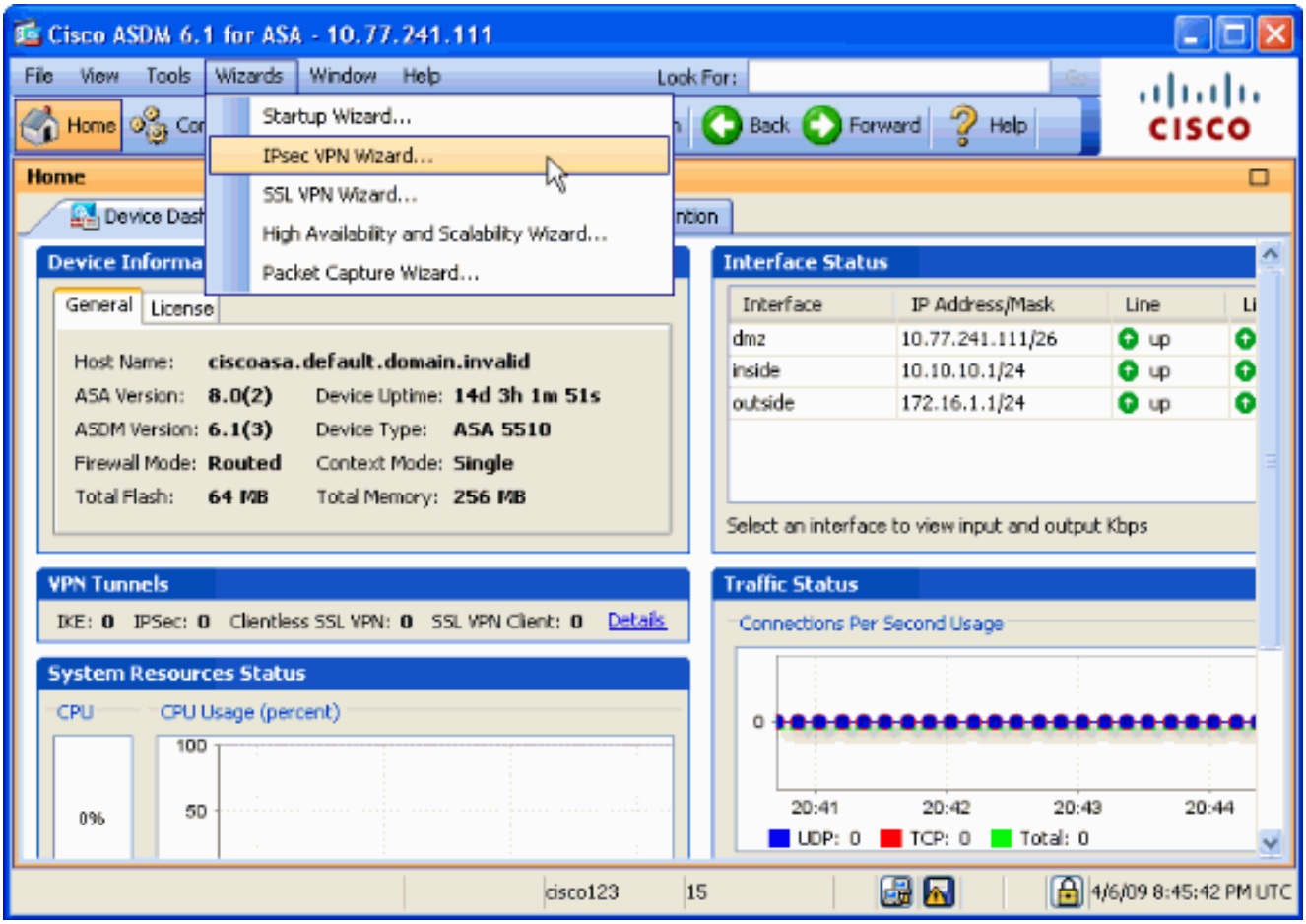


2. Per scaricare il programma di installazione dell'applicazione ASDM, fare clic su **Download ASDM Launcher** e su Start ASDM.
3. Una volta scaricato l'utilità di avvio ASDM, completare la procedura indicata dalle istruzioni per installare il software ed eseguire l'utilità di avvio Cisco ASDM.
4. Immettere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

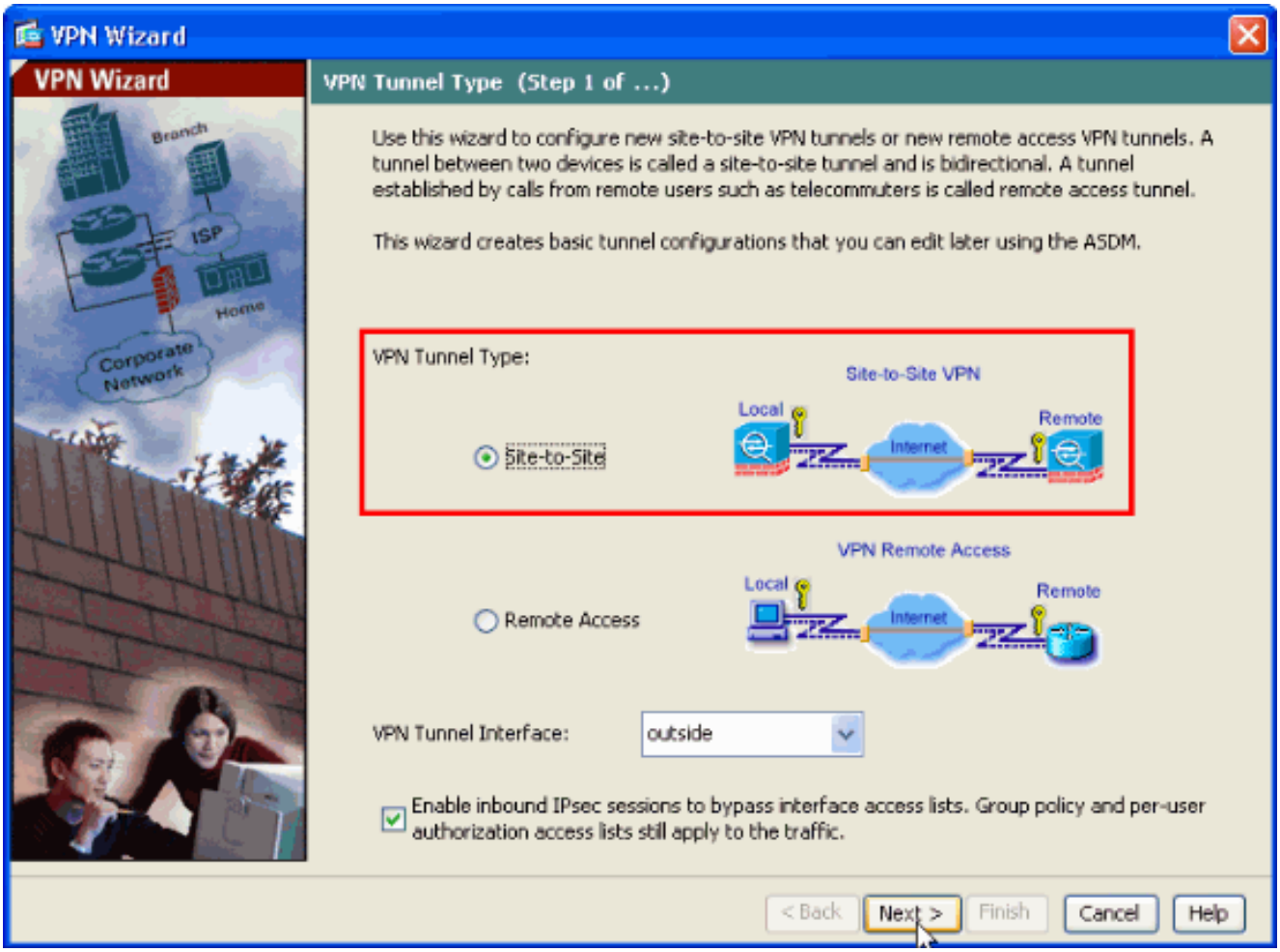


password.

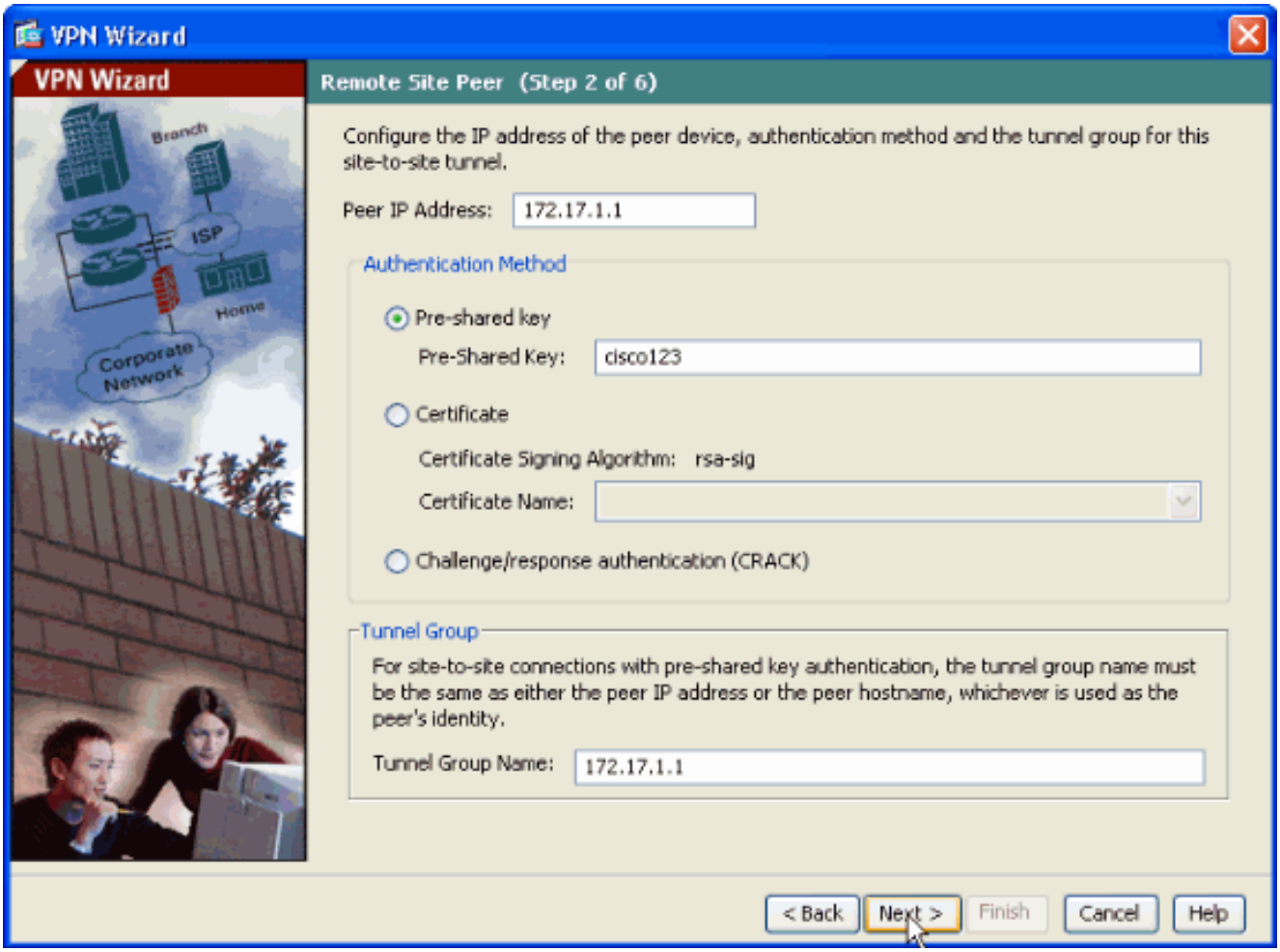
5. Eseguire la **Creazione guidata VPN IPsec** quando l'applicazione ASDM si connette all'appliance
ASA.



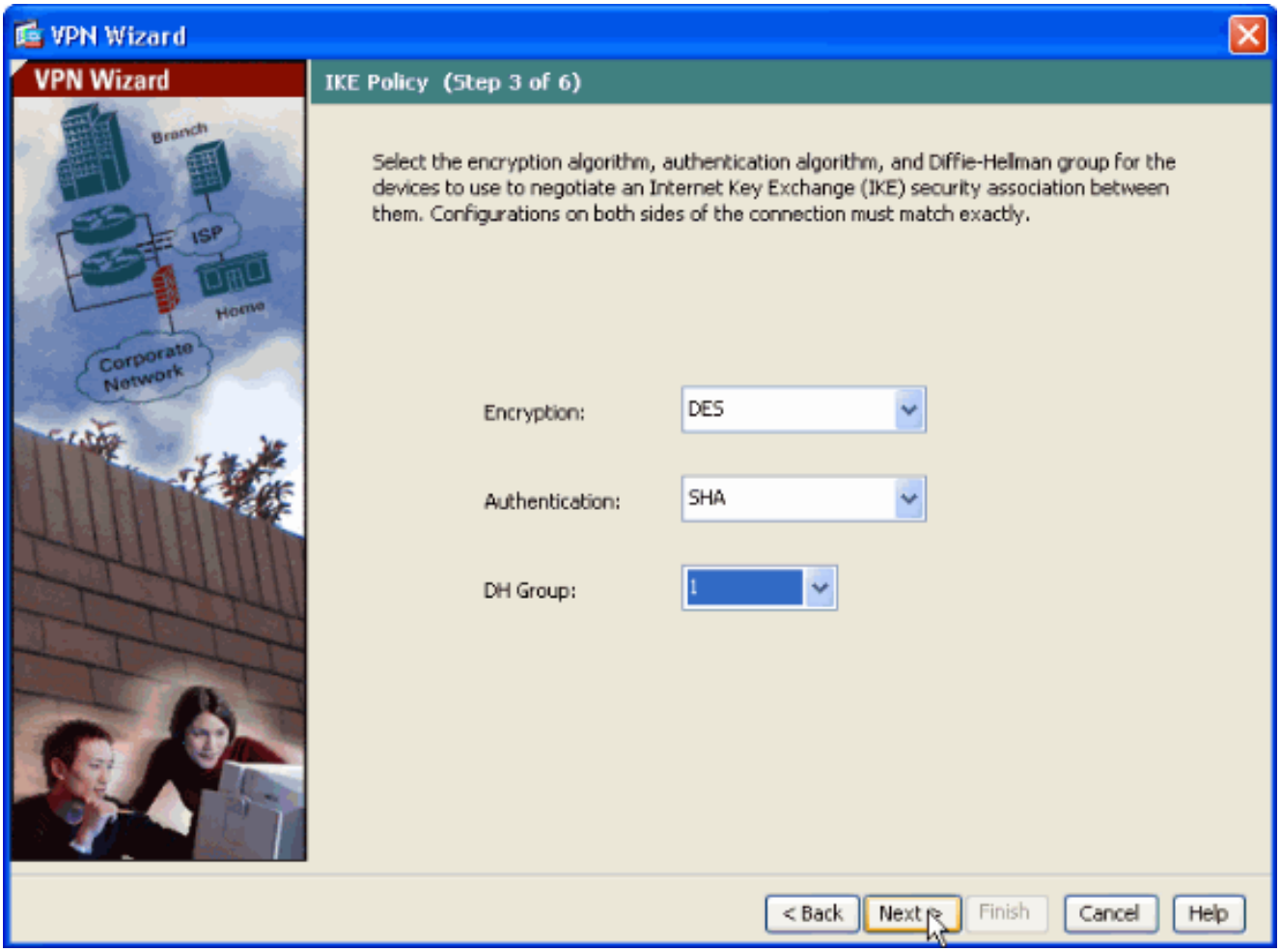
6. Scegliere il tipo di tunnel VPN IPsec **da sito a sito** e fare clic su **Avanti** come mostrato di seguito.



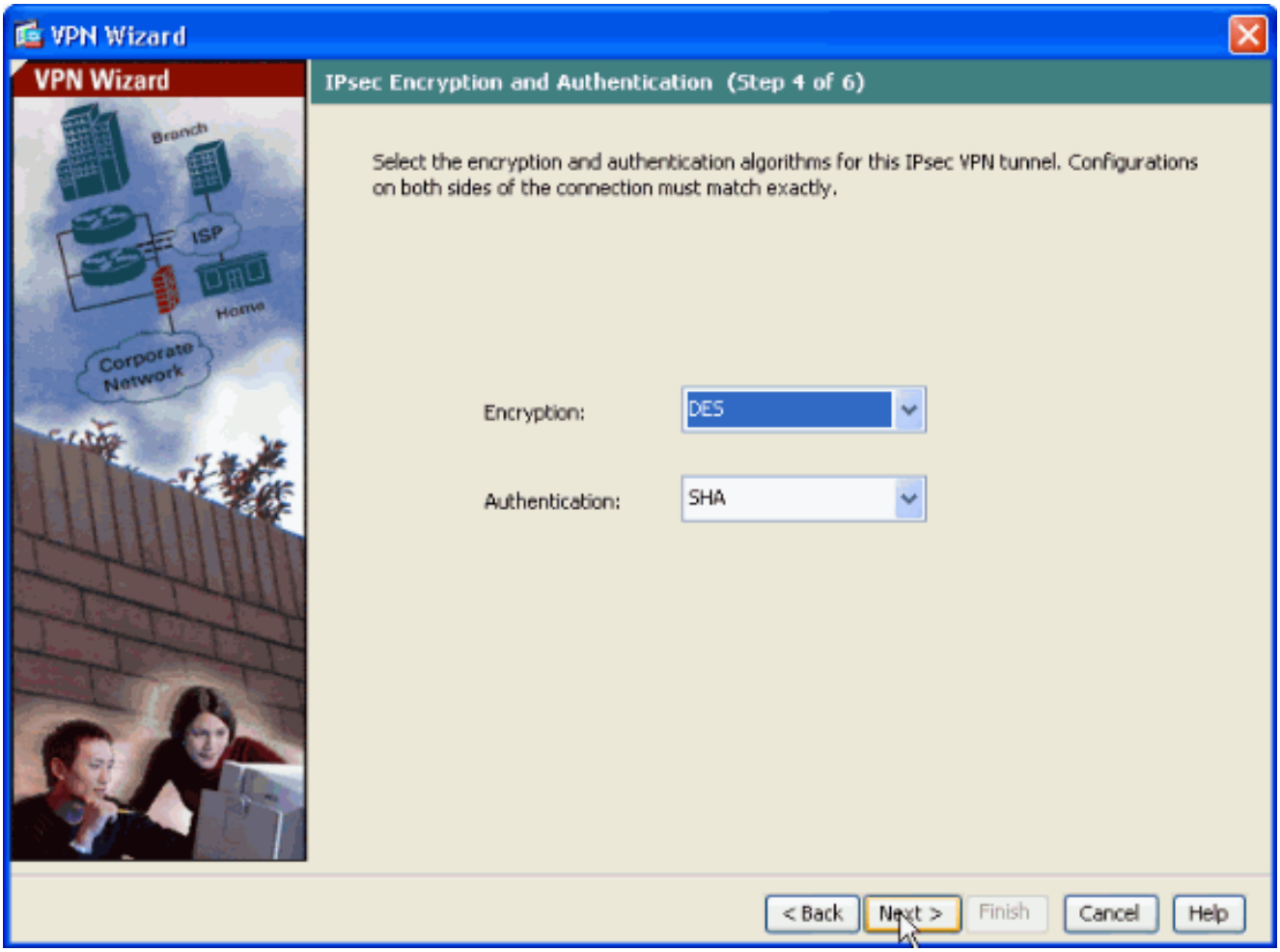
7. Specificare l'indirizzo IP esterno del peer remoto. Immettere le informazioni di autenticazione da utilizzare, ovvero la chiave già condivisa in questo esempio. La chiave già condivisa utilizzata in questo esempio è **cisco123**. Il **nome del gruppo di tunnel** sarà l'indirizzo IP esterno per impostazione predefinita se si configura la VPN L2L. Fare clic su **Next** (Avanti).



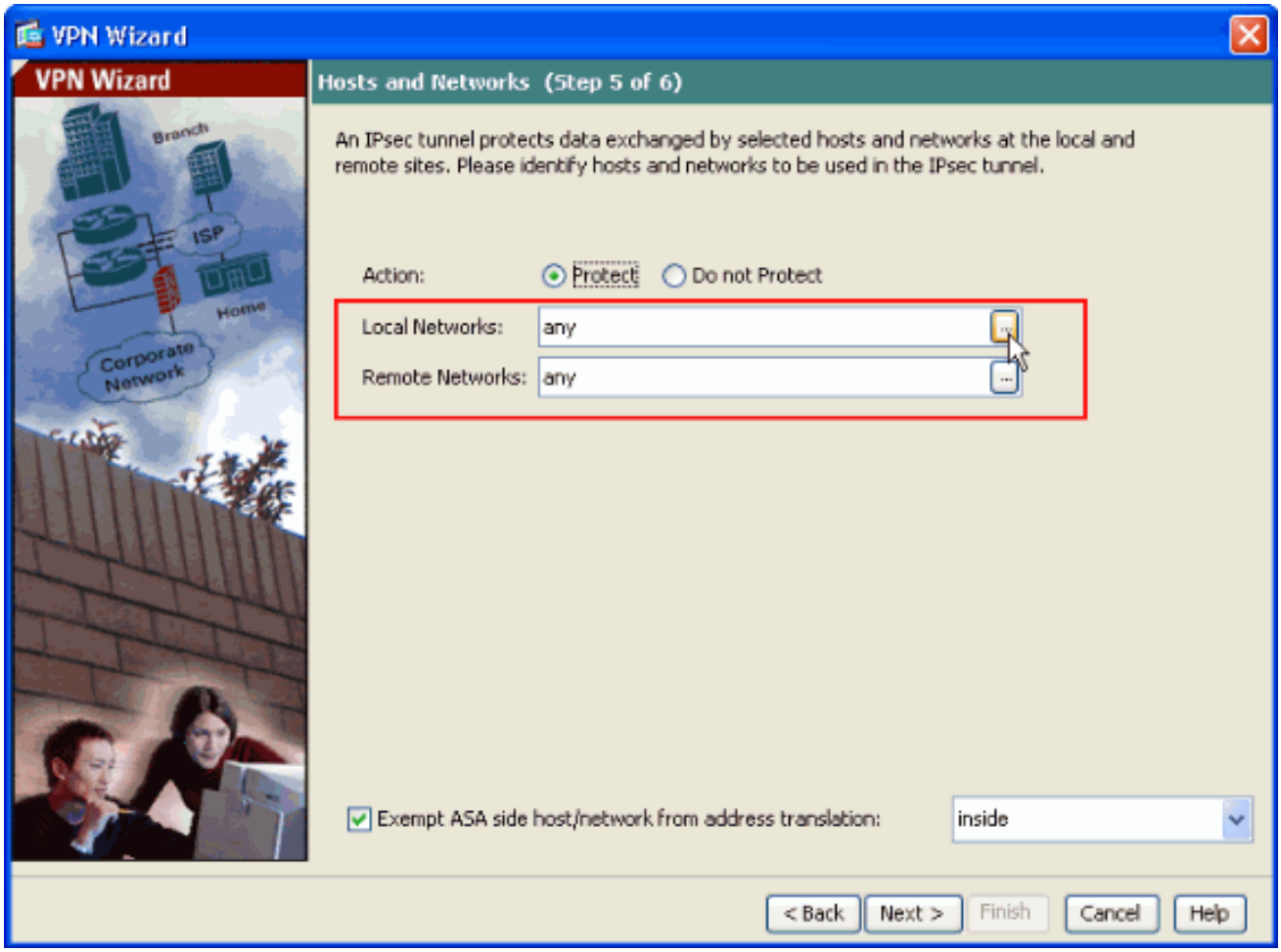
8. Specificare gli attributi da utilizzare per IKE, noti anche come fase 1. Questi attributi devono essere gli stessi sia sull'ASA che sul router IOS. Fare clic su **Next** (Avanti).



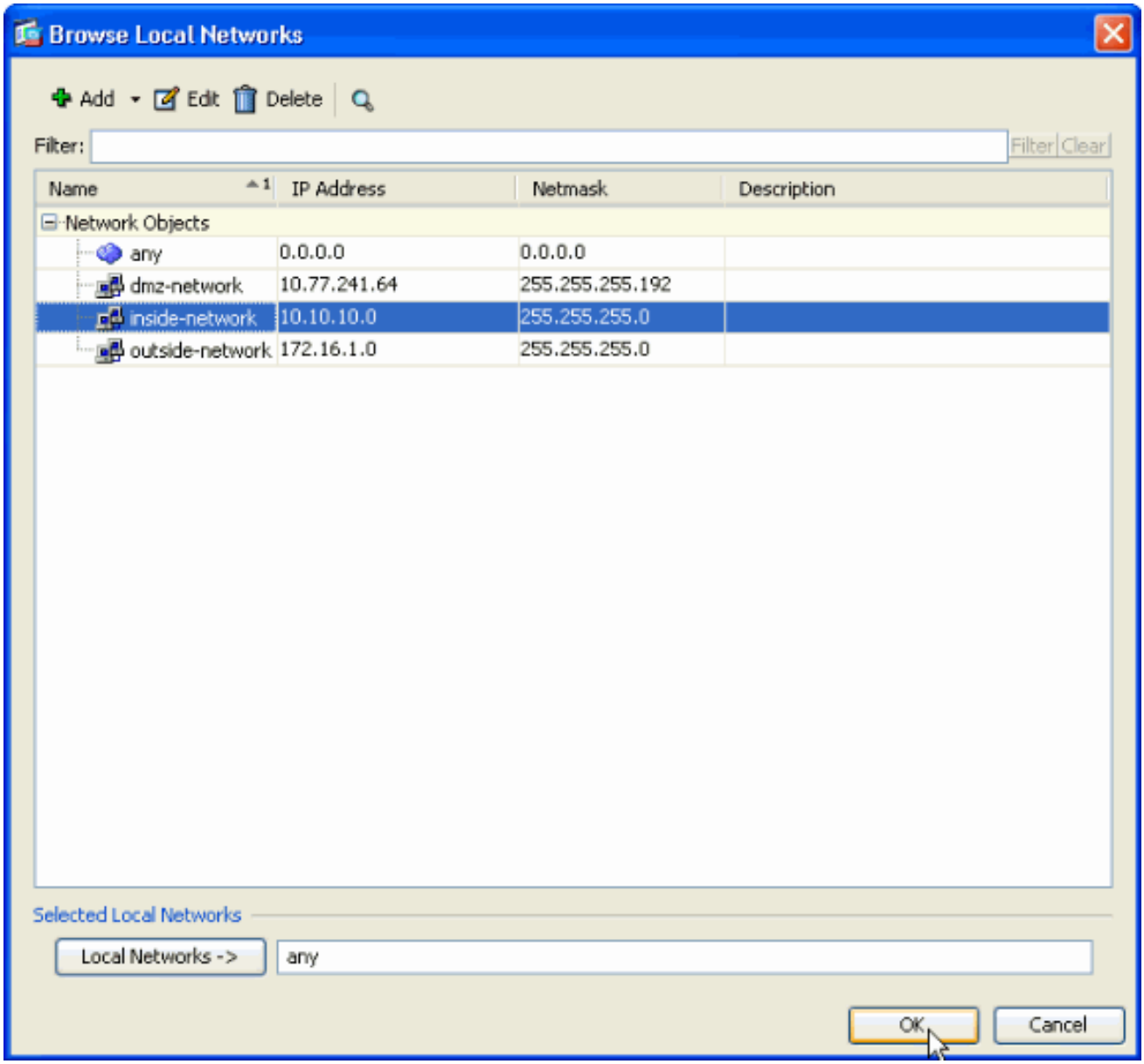
9. Specificare gli attributi da utilizzare per IPsec, noti anche come fase 2. Questi attributi devono corrispondere sia sull'appliance ASA sia sul router IOS. Fare clic su **Next** (Avanti).



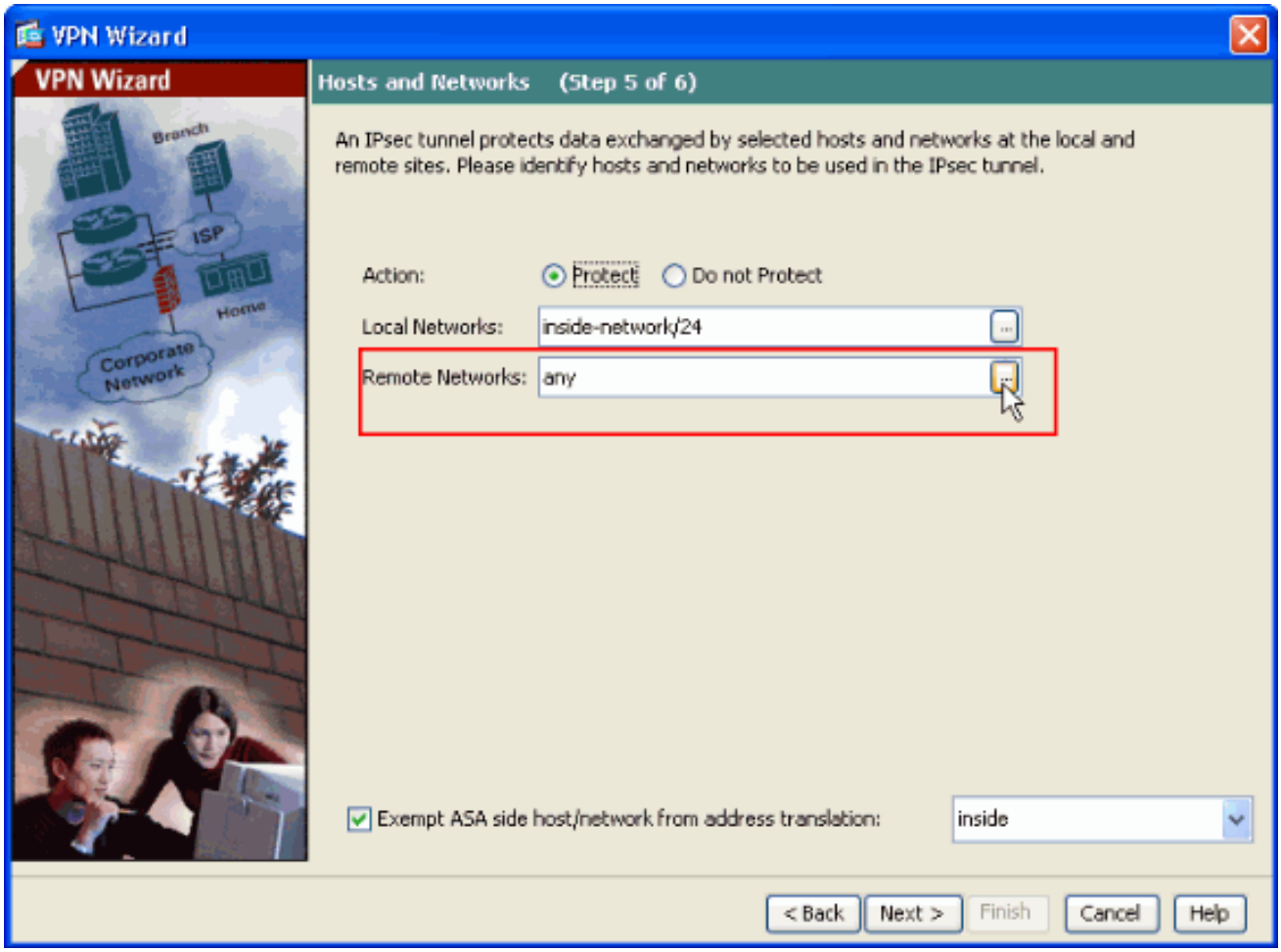
10. Specificare gli host il cui traffico deve poter passare attraverso il tunnel VPN. In questo passaggio, è necessario fornire le **reti locale** e **remota** per il tunnel VPN. Fare clic sul pulsante accanto a **Reti locali** come mostrato di seguito per scegliere l'indirizzo di rete locale dall'elenco a
discesa.



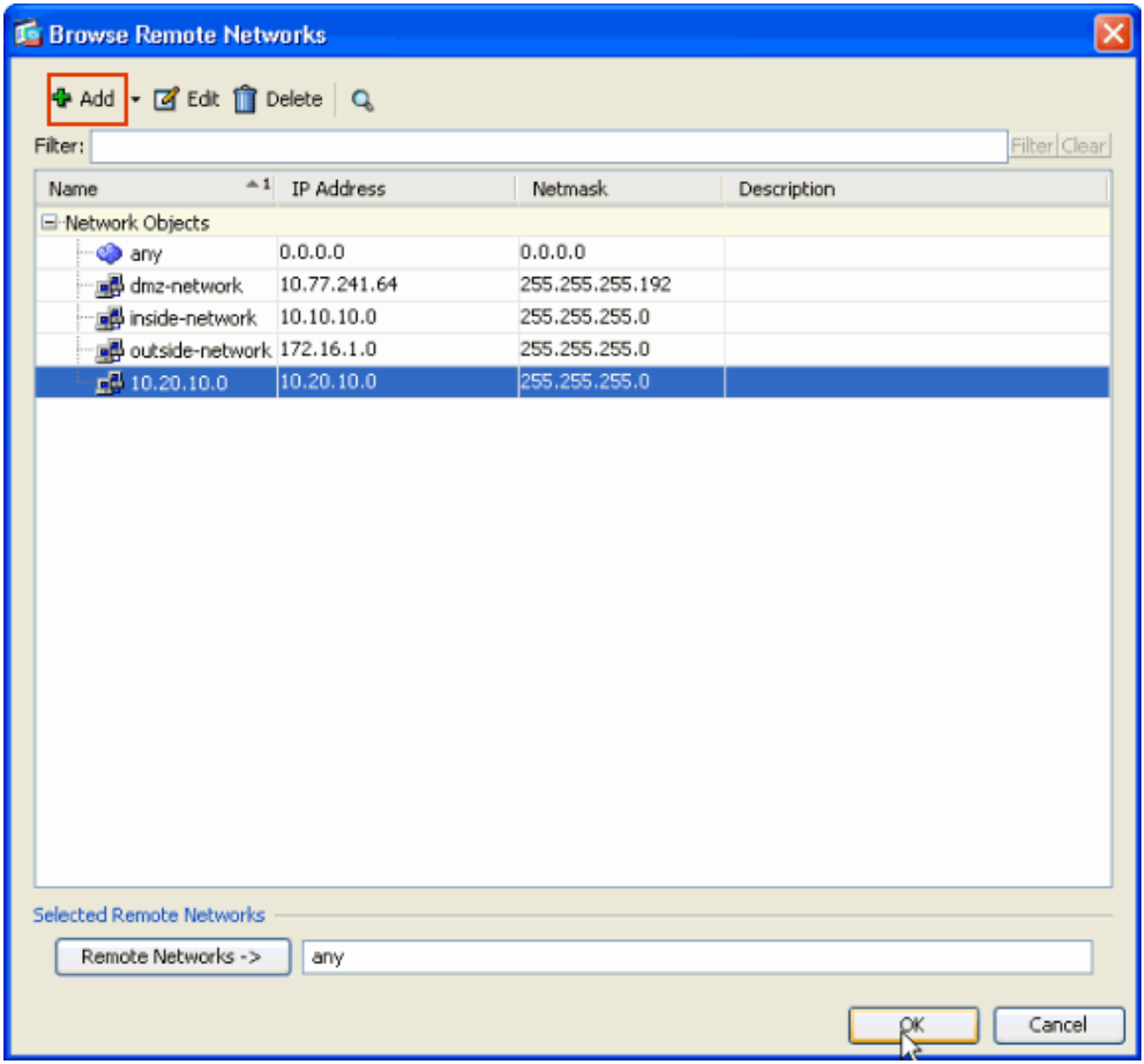
11. Scegliere l'indirizzo **di rete locale**, quindi fare clic su **OK** come mostrato di seguito.



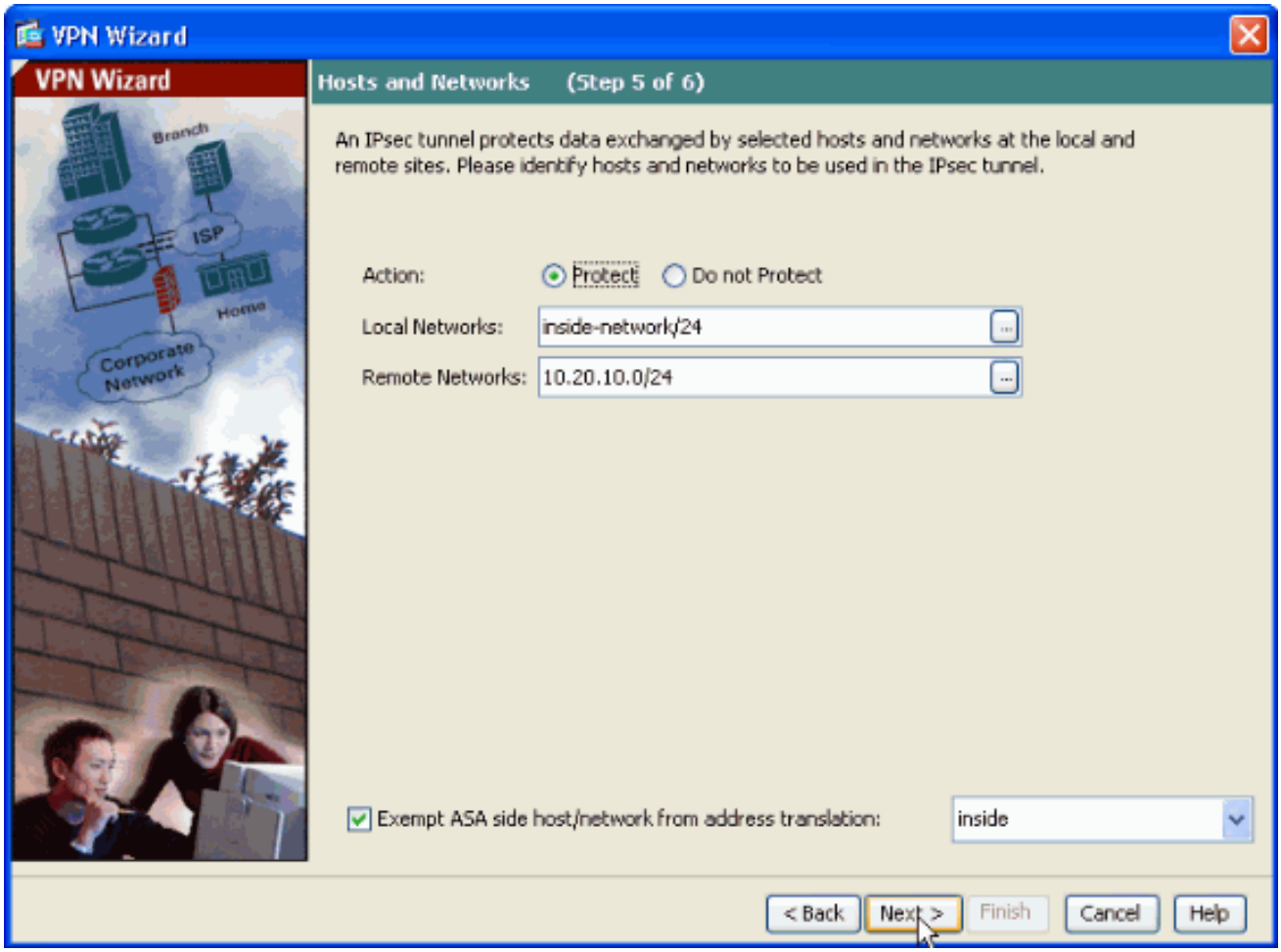
12. Fare clic sul pulsante accanto a **Reti remote** come mostrato di seguito per scegliere l'indirizzo di rete remoto dall'elenco a discesa.



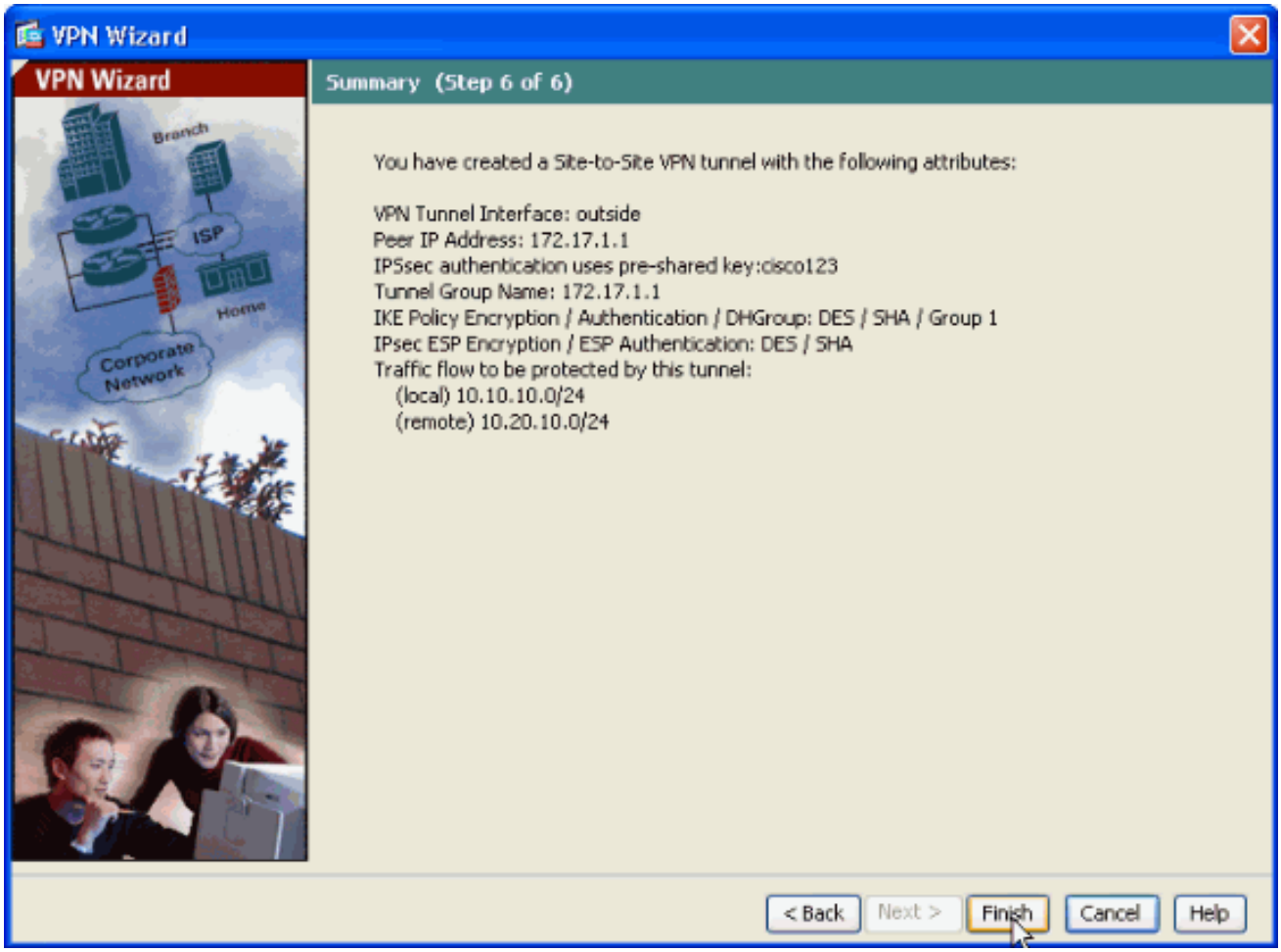
13. Scegliere l'indirizzo di **rete remota**, quindi fare clic su **OK** come mostrato di seguito.**Nota:** se la rete remota non è presente nell'elenco, è necessario aggiungerla all'elenco facendo clic su
Aggiungi.



14. Per evitare che il traffico del tunnel venga **convertito** dall'indirizzo di **rete,** selezionare la casella di controllo **Esenzione host/rete lato ASA dalla conversione degli indirizzi**. Fare quindi clic su
Avanti.



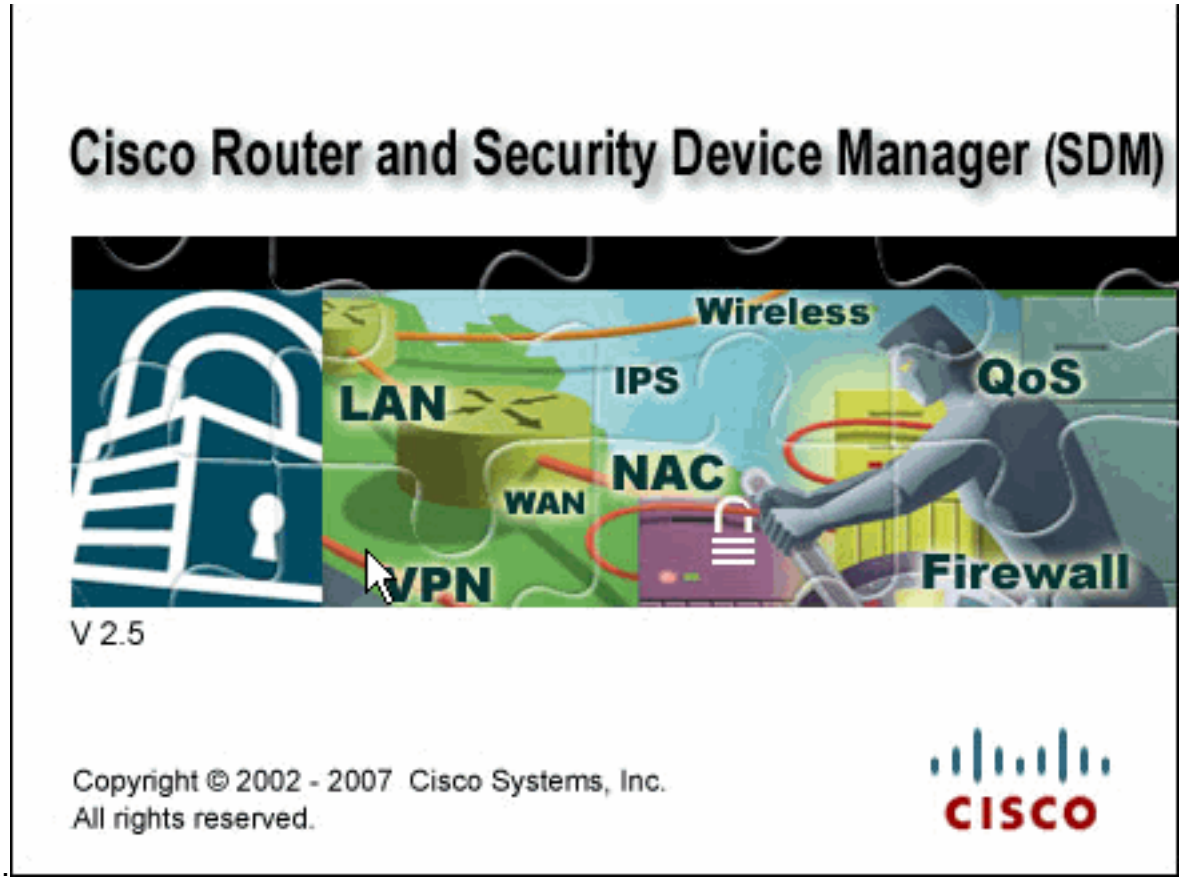
15. In questo riepilogo vengono visualizzati gli attributi definiti dalla Creazione guidata VPN. Verificare la configurazione e fare clic su **Finish** (Fine) quando le impostazioni sono corrette.



Configurazione SDM router

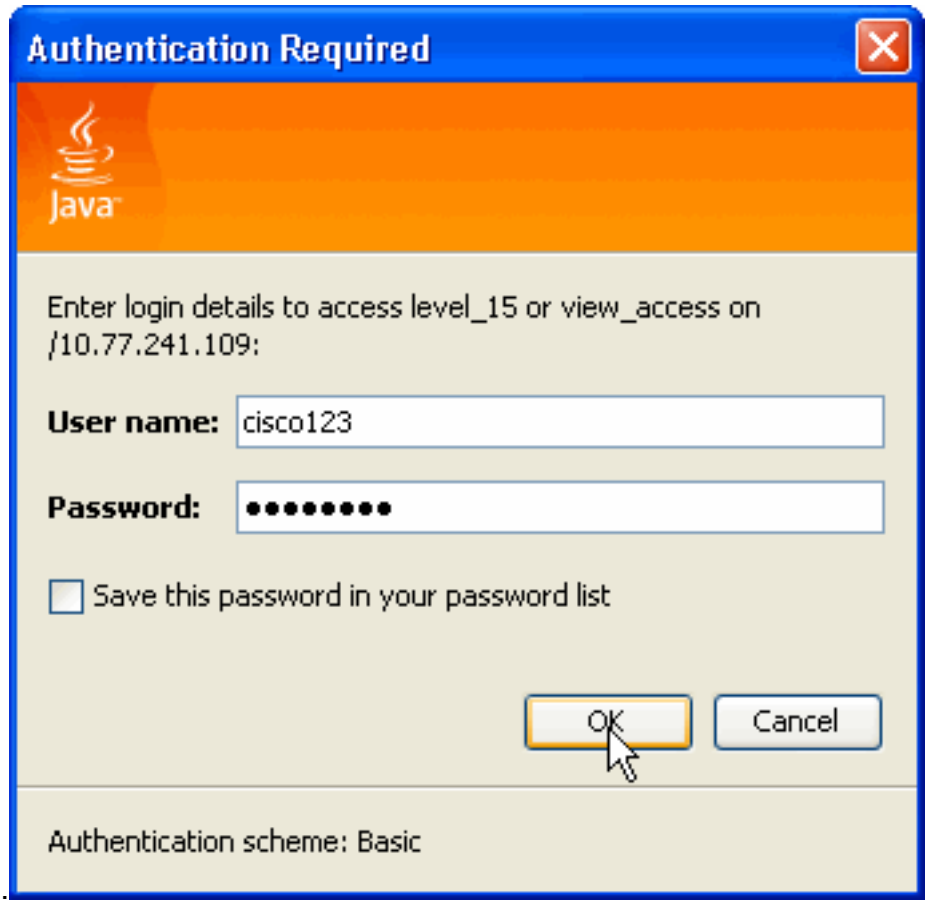
Completare questa procedura per configurare il tunnel VPN da sito a sito sul router Cisco IOS:

1. Aprire il browser e immettere **https://<Indirizzo_IP dell'interfaccia del router configurata per l'accesso SDM>** per accedere al modulo SDM sul router.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.Il router visualizza questa finestra per consentire il download dell'applicazione SDM. In questo esempio l'applicazione viene caricata nel computer locale e non viene eseguita in un'applet



Java.

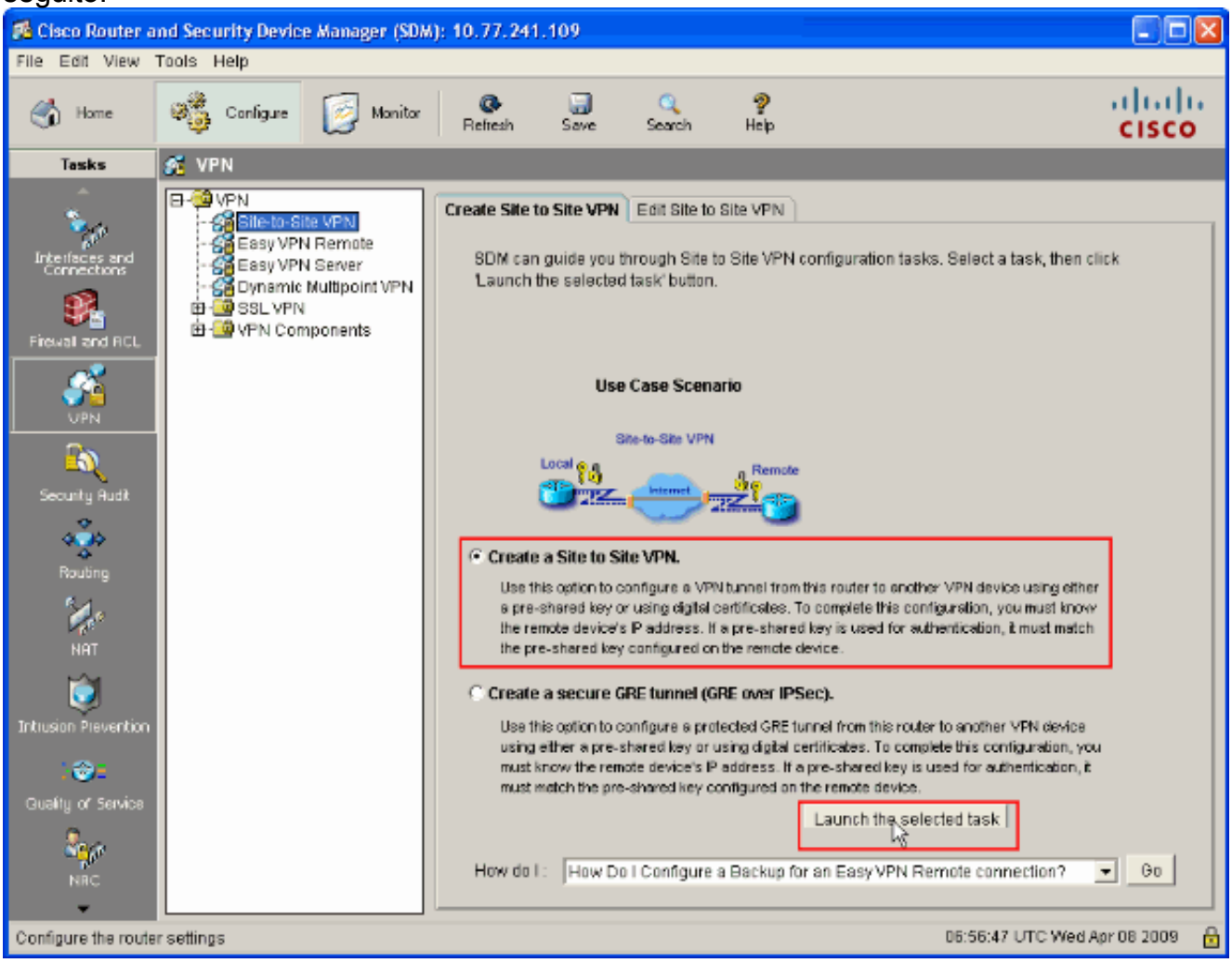
2. Il download dell'SDM ha inizio ora. Una volta scaricato l'utilità di avvio SDM, completare la procedura indicata dalle istruzioni per installare il software ed eseguire l'utilità di avvio SDM di Cisco.
3. Immettere il **Nome utente** e la **Password**, se specificati, e fare clic su **OK**.In questo esempio viene utilizzato **cisco123** come nome utente e **cisco123** come



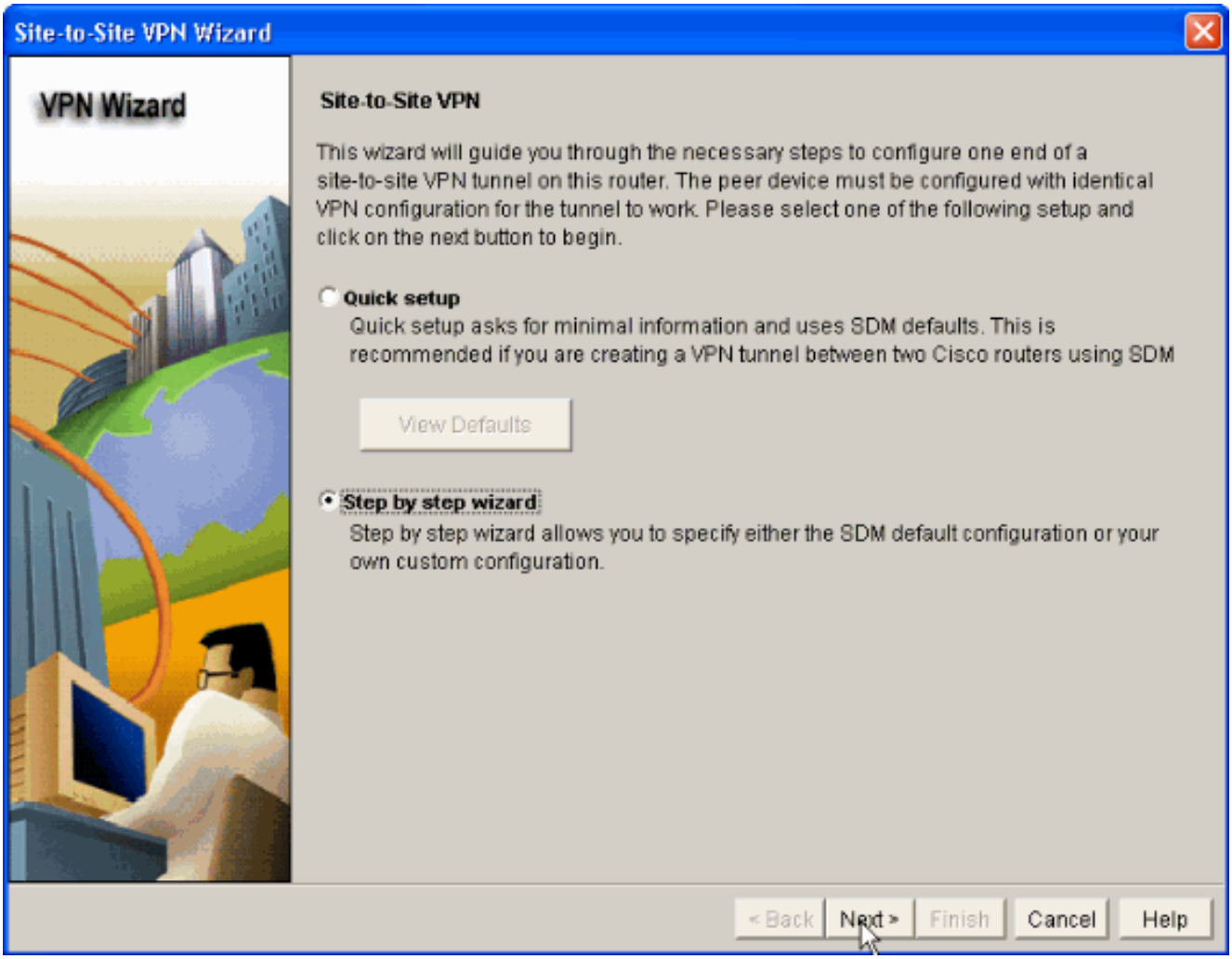
password.

4. Scegliere **Configurazione->VPN->da sito a sito VPN** e fare clic sul pulsante di opzione

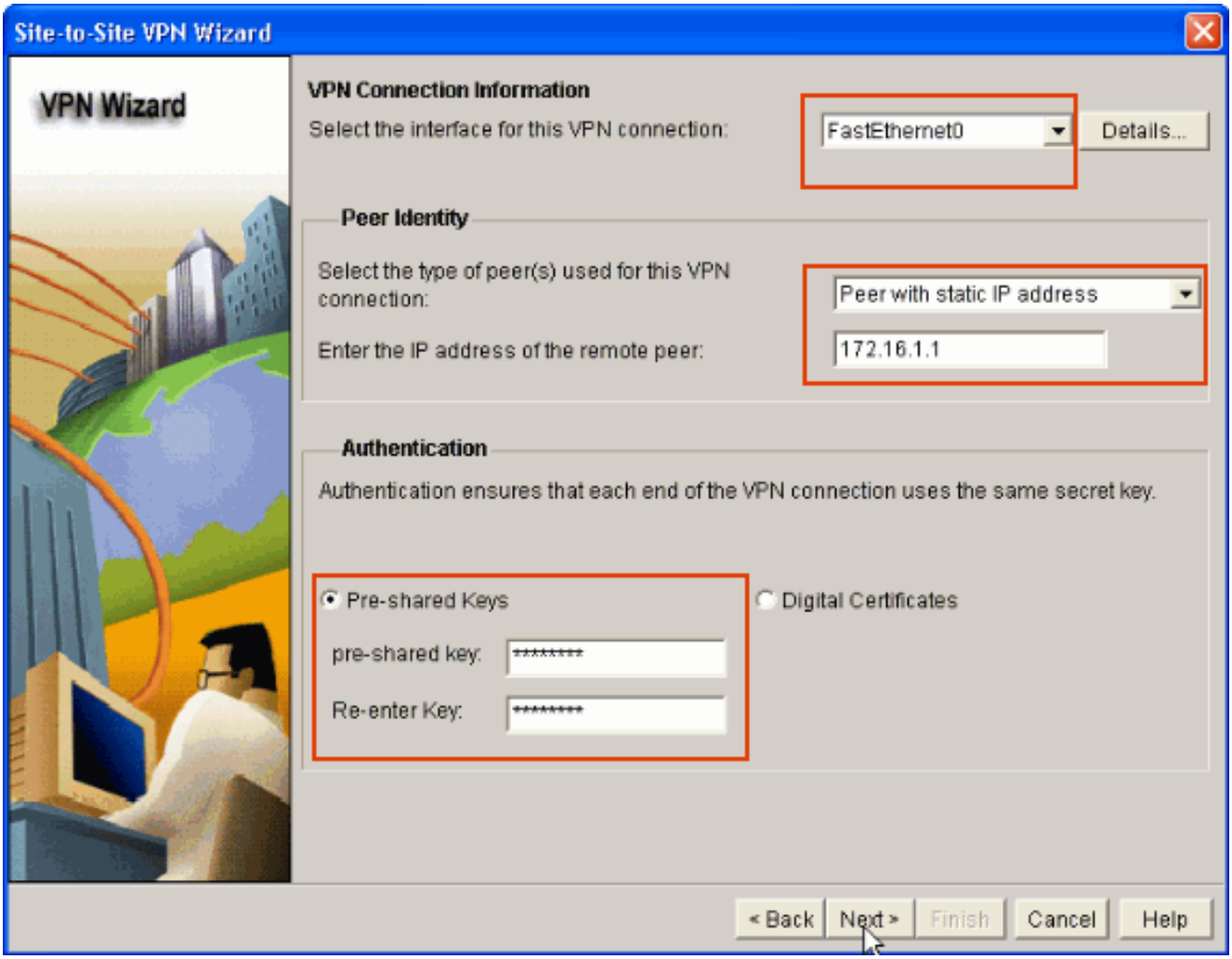
accanto a **Crea VPN da sito a sito** nella home page SDM. Fare quindi clic su **Avvia l'attività selezionata** come illustrato di
seguito:



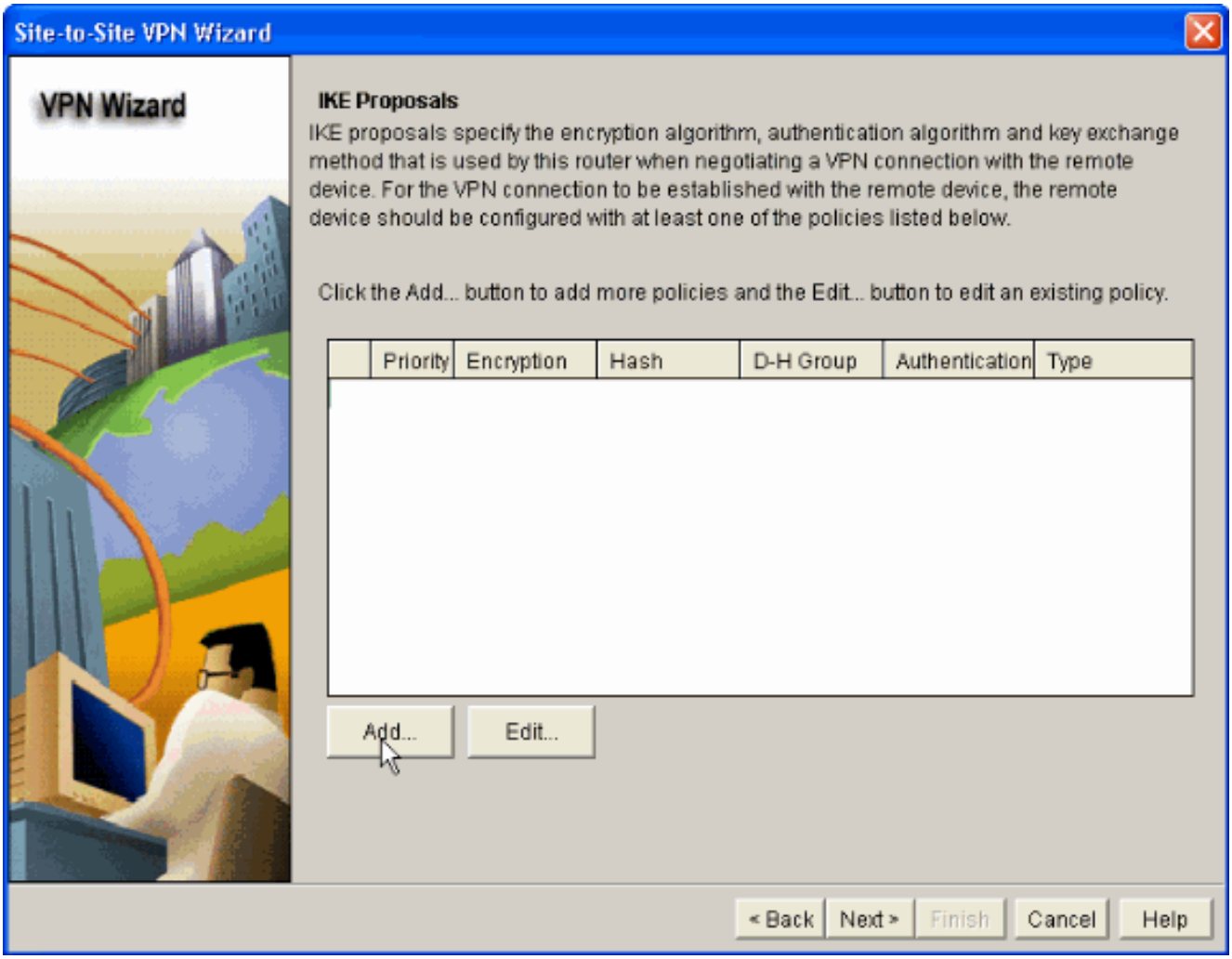
5. Scegliere **Procedura guidata dettagliata** per procedere con la configurazione:



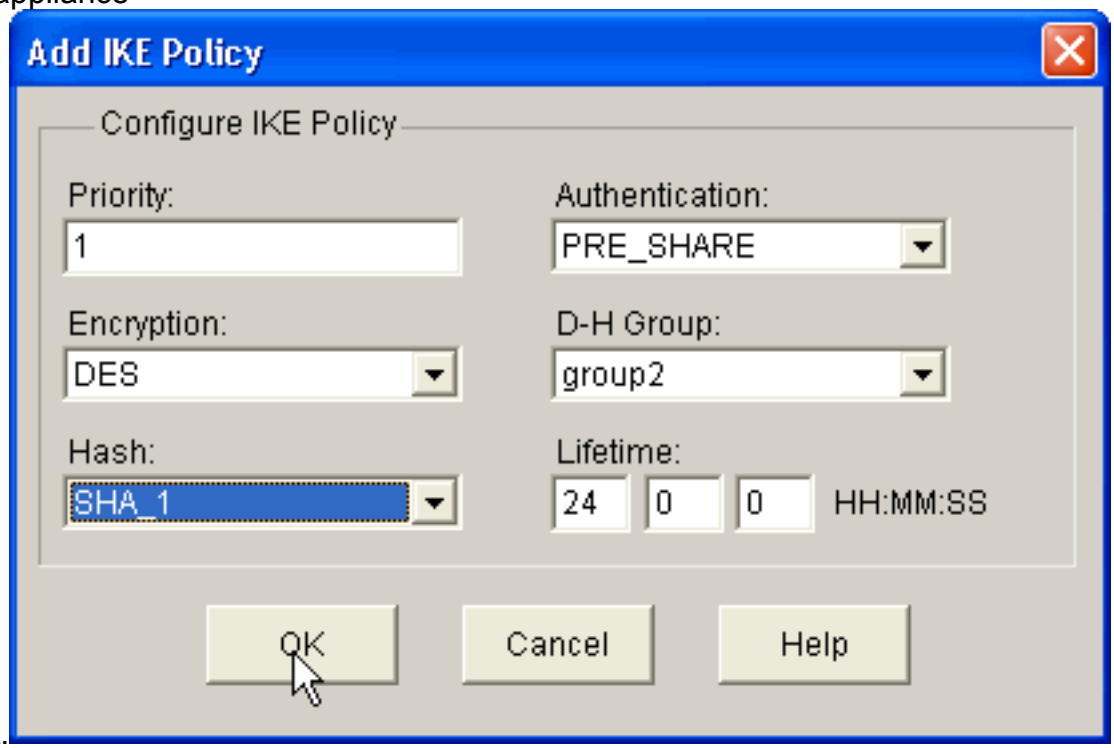
6. Nella finestra successiva fornire le **informazioni sulla connessione VPN** negli spazi corrispondenti. Selezionare l'interfaccia del tunnel VPN dall'elenco a discesa. In questo caso, viene scelto **FastEthernet0**. Nella sezione **Identità peer**, scegliere **Peer con indirizzo IP statico** e fornire l'indirizzo IP del peer remoto. Quindi, fornire la **chiave già condivisa** (**cisco123** nell'esempio) nella sezione Authentication (Autenticazione) come mostrato. Fare quindi clic su
Avanti.



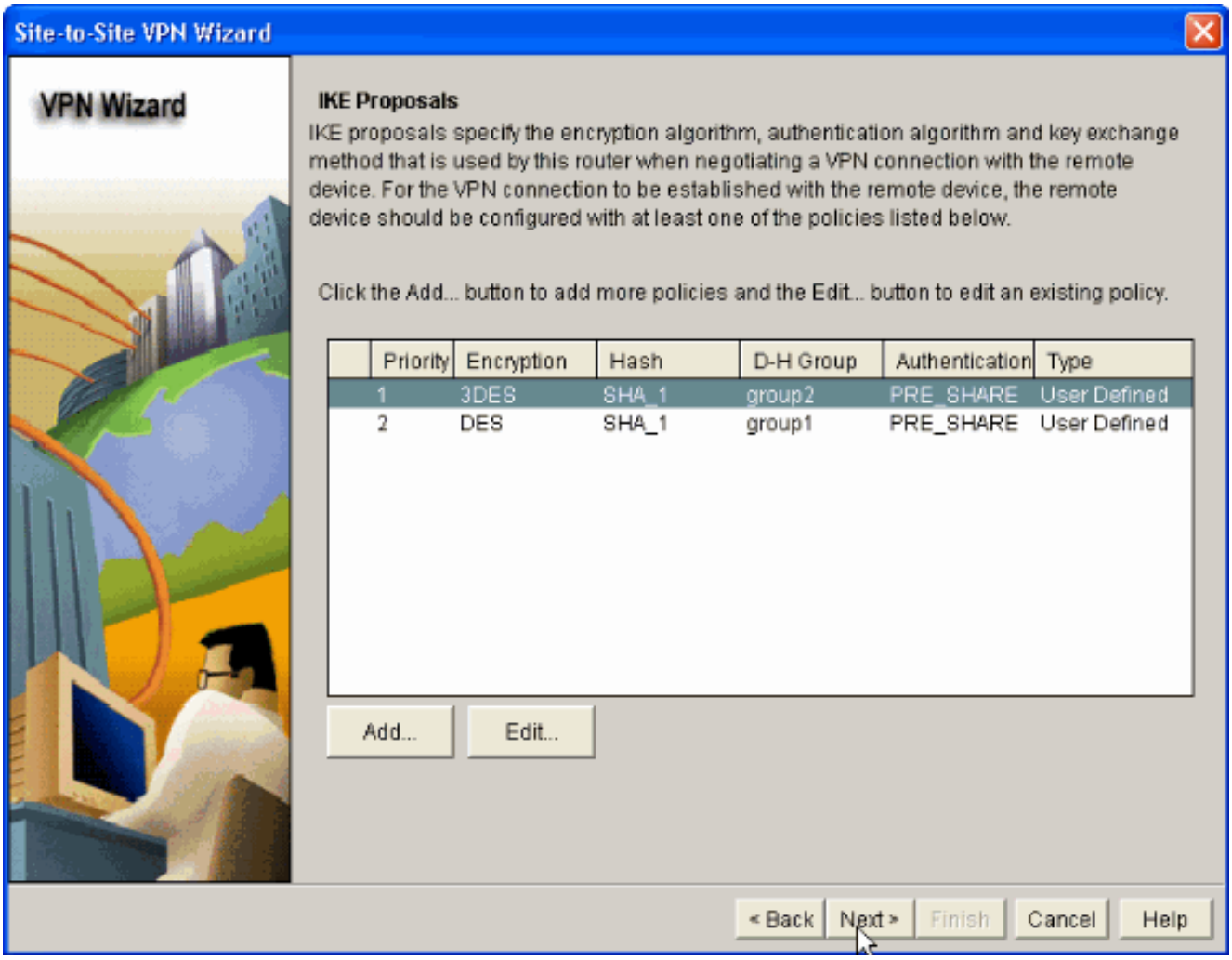
7. Fare clic su **Add** per aggiungere le proposte IKE che specificano l'**algoritmo di crittografia, l'algoritmo di autenticazione** e il **metodo di scambio chiave**.



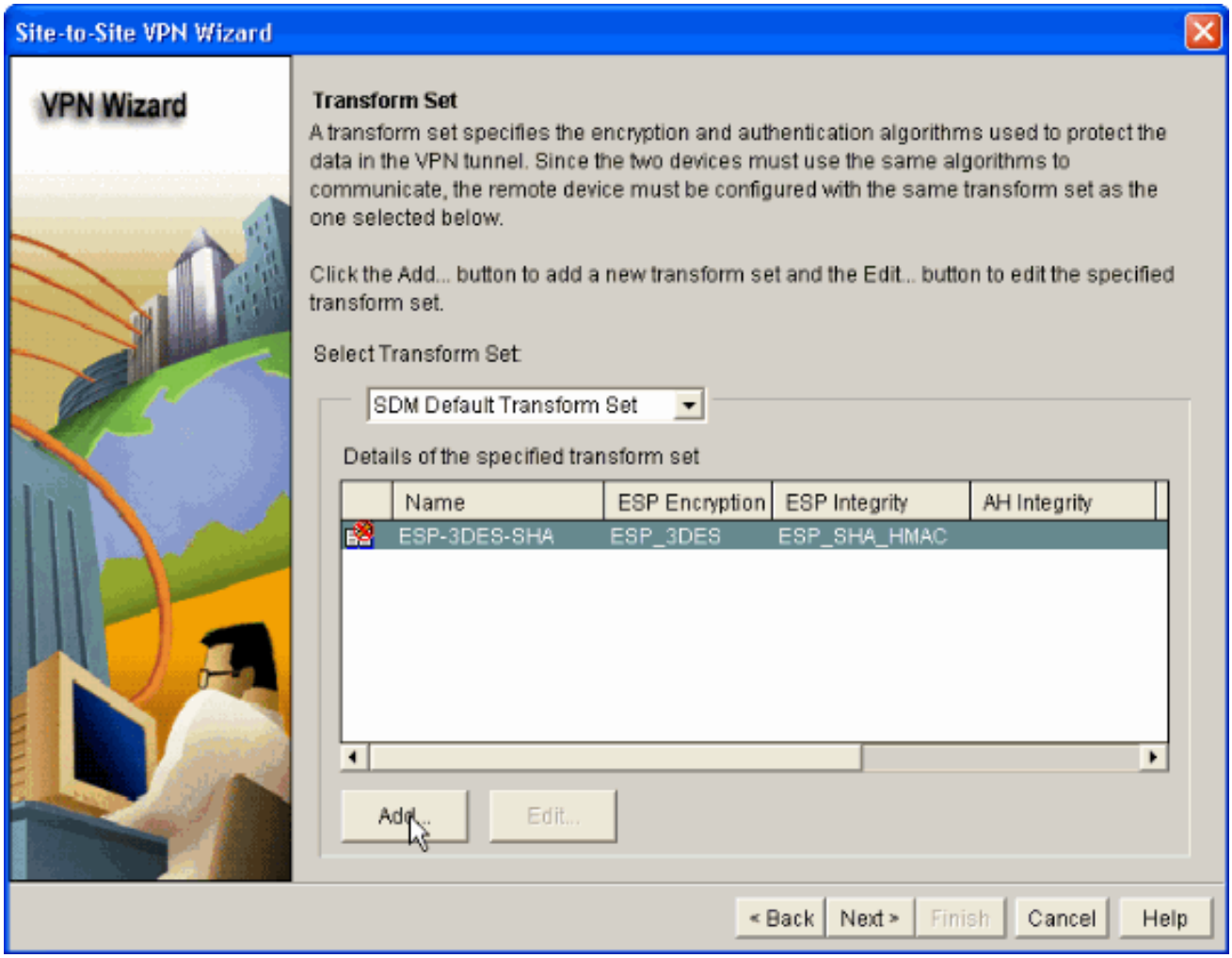
8. Specificare **Algoritmo di crittografia**, **Algoritmo di autenticazione** e il **metodo di scambio chiavi**, come mostrato di seguito, quindi fare clic su **OK**. I valori **Encryption Algorithm**, **Authentication Algorithm** e il metodo **Key Exchange** devono corrispondere ai dati forniti nell'appliance ASA.



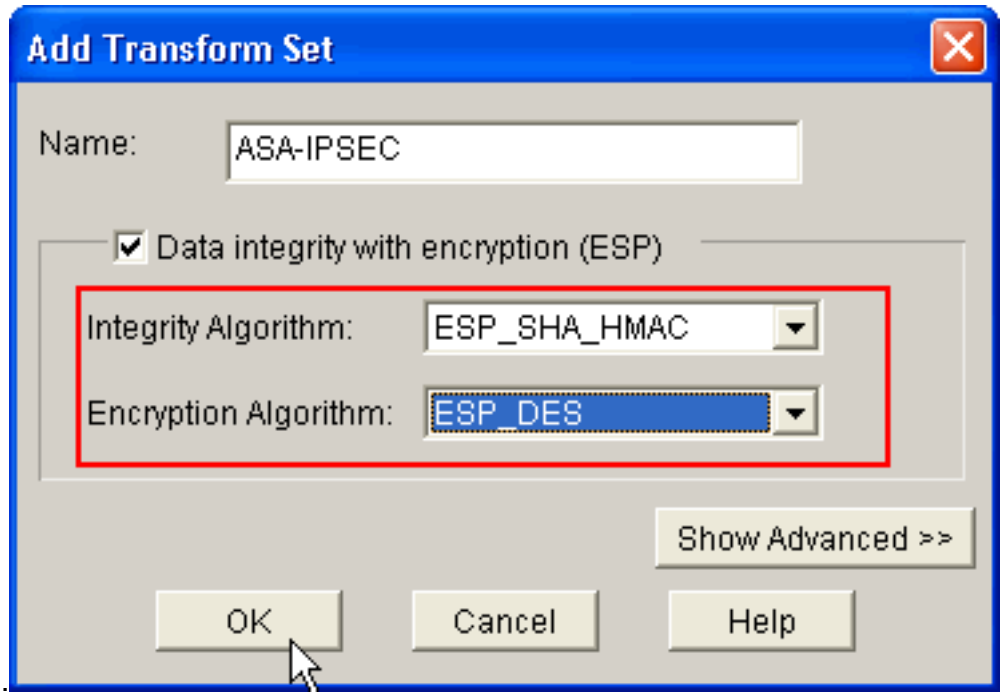
9. Fare clic su **Next** (Avanti) come mostrato di seguito.



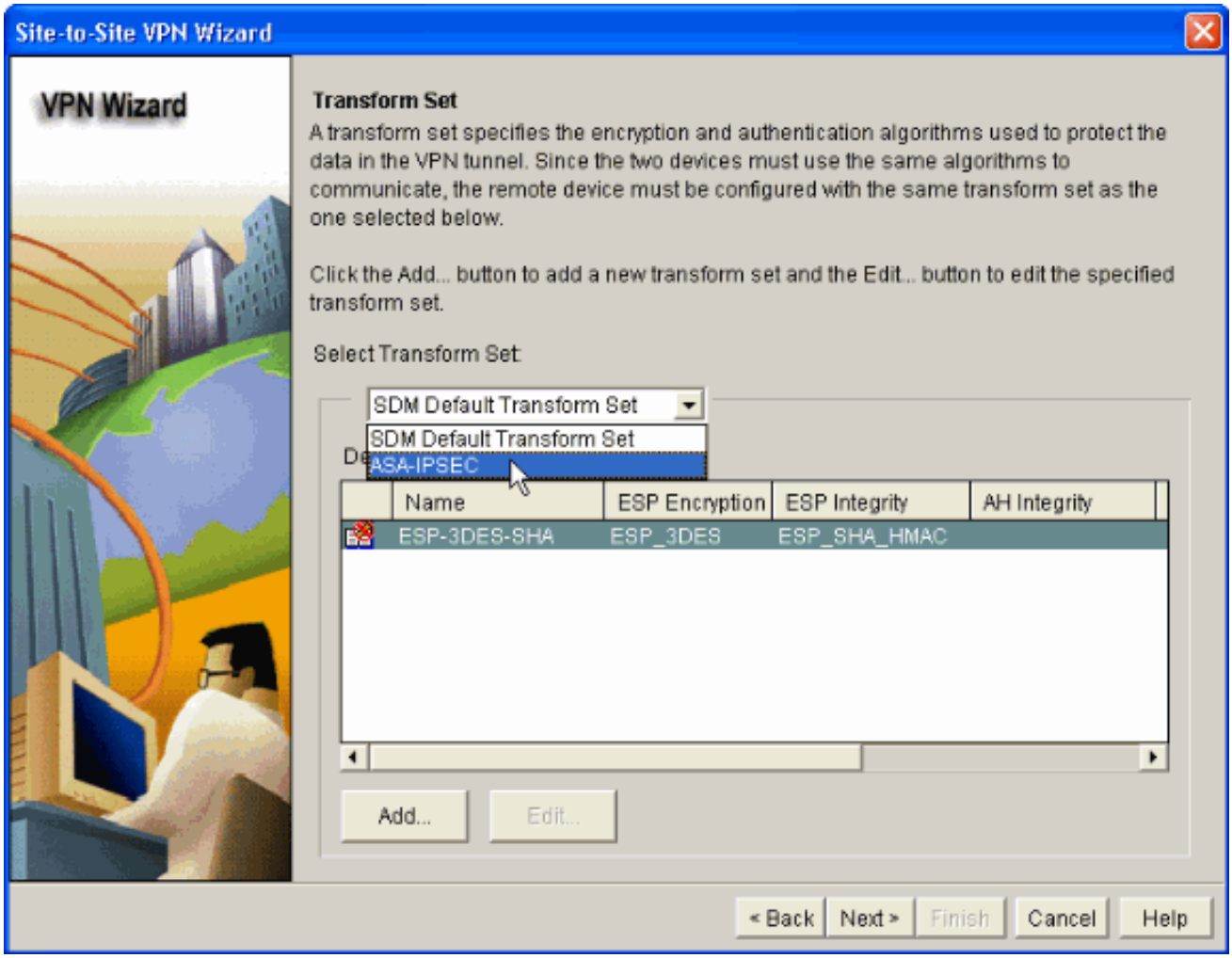
10. In questa nuova finestra devono essere forniti i dettagli **Set di trasformazioni**. Il set di trasformazioni specifica gli algoritmi di **crittografia** e **autenticazione** utilizzati per proteggere **i dati nel tunnel VPN**. Quindi, fare clic su **Add** (Aggiungi) per specificare i dettagli. È possibile aggiungere qualsiasi numero di set di trasformazioni in base alle esigenze facendo clic su **Aggiungi** e fornendo i
dettagli.



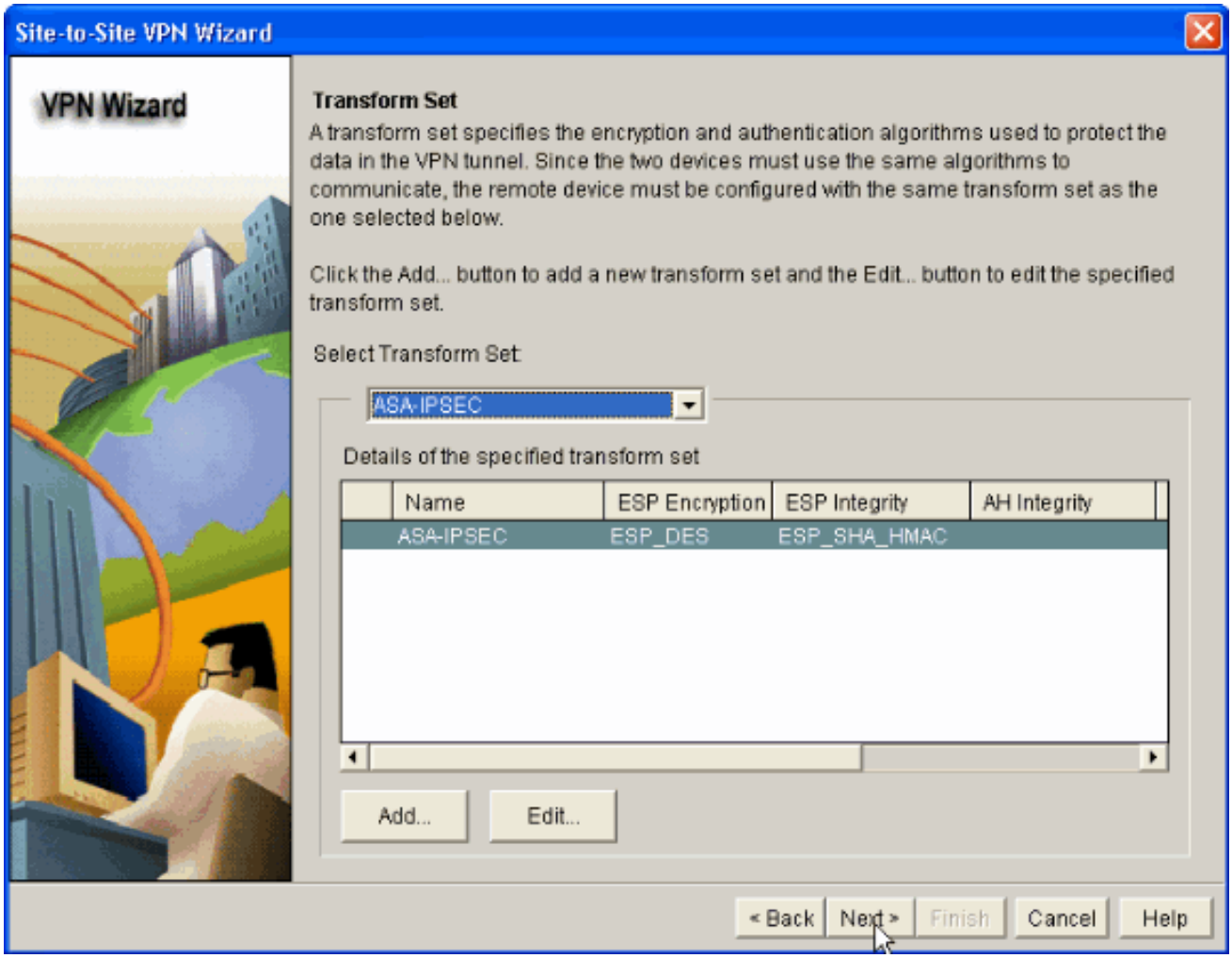
11. Specificare i dettagli del **set di trasformazioni** (**algoritmo di crittografia e autenticazione**) e fare clic su **OK** come mostrato.



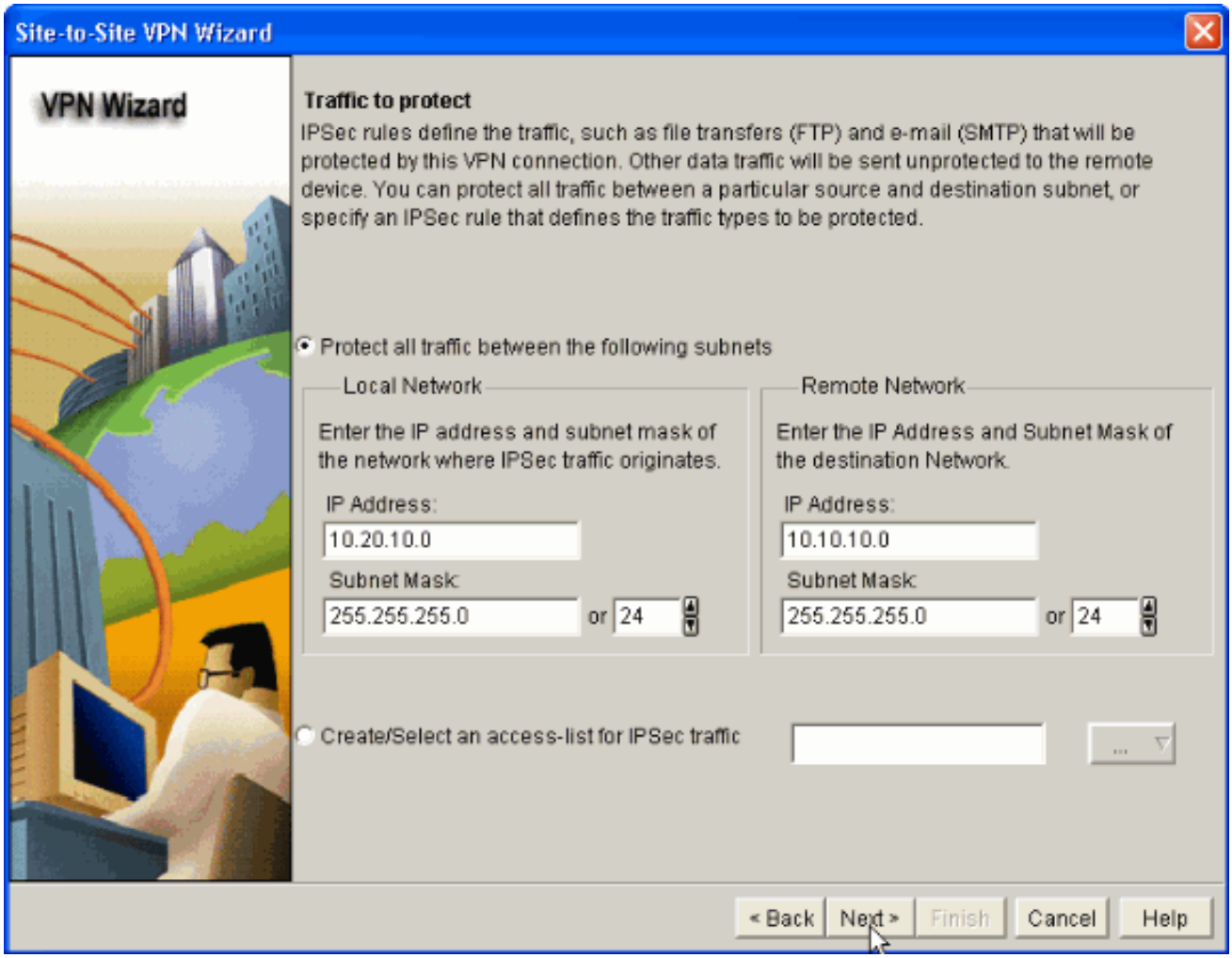
12. Selezionate il **set di trasformazioni** richiesto da utilizzare dall'elenco a discesa come mostrato.



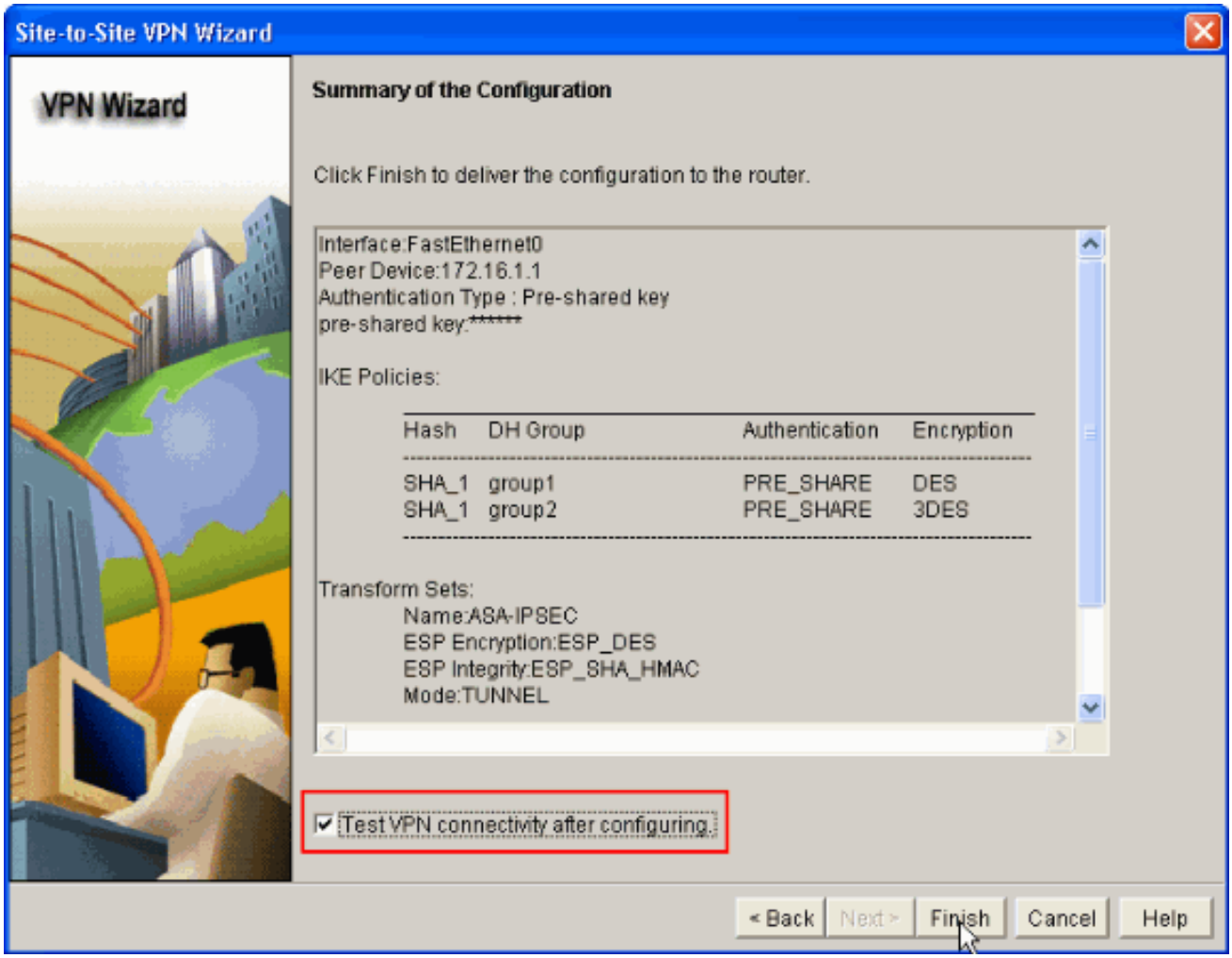
13. Fare clic su **Next** (Avanti).



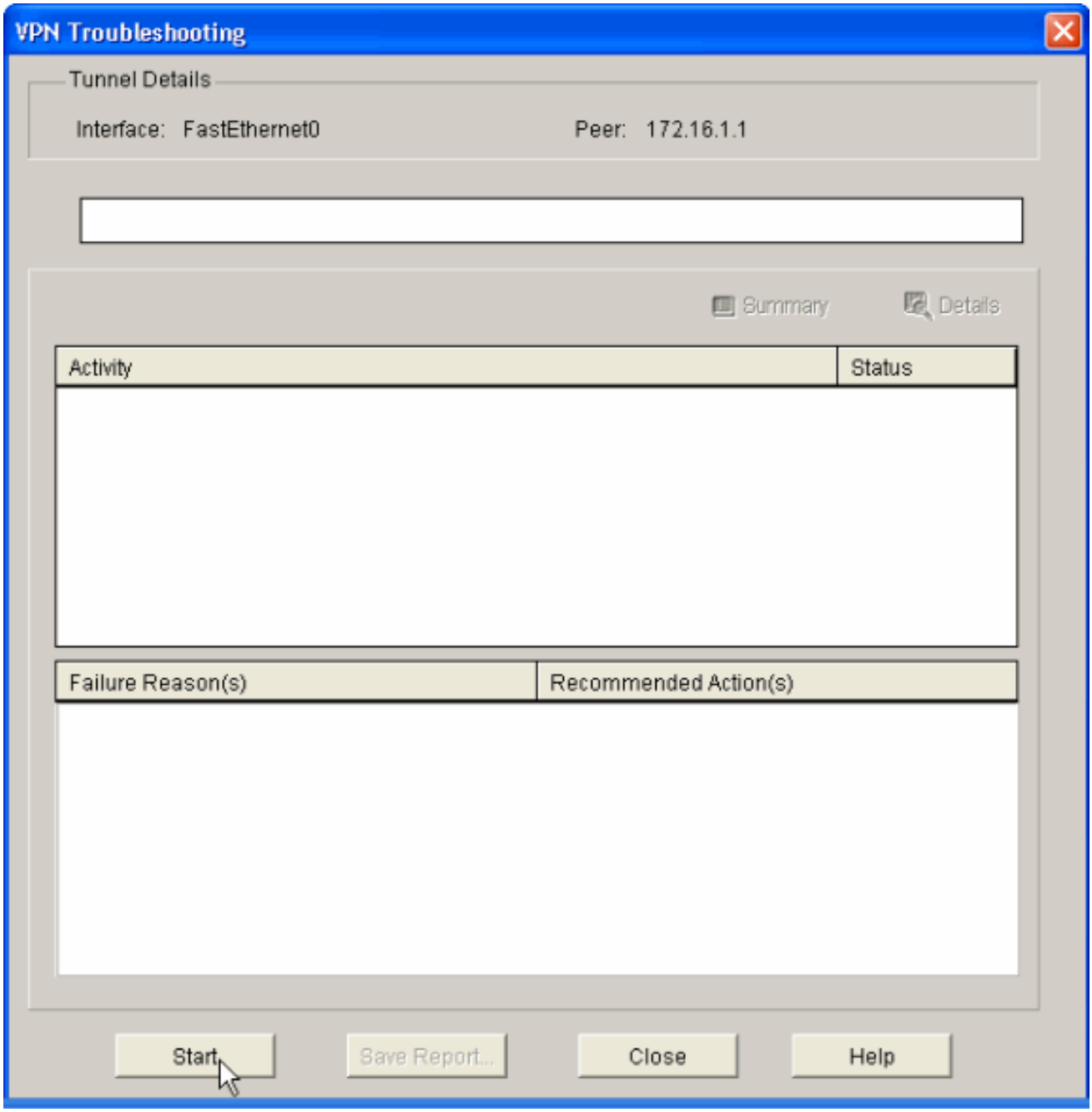
14. Nella finestra seguente vengono forniti i dettagli sul **traffico da proteggere** tramite il tunnel VPN. Specificare le **reti di origine e di destinazione** del traffico da proteggere in modo che il traffico tra le reti di origine e di destinazione specificate sia protetto. Nell'esempio, la rete di origine è 10.20.10.0 e la rete di destinazione è 10.10.10.0. Quindi, fare clic su **Avanti**.



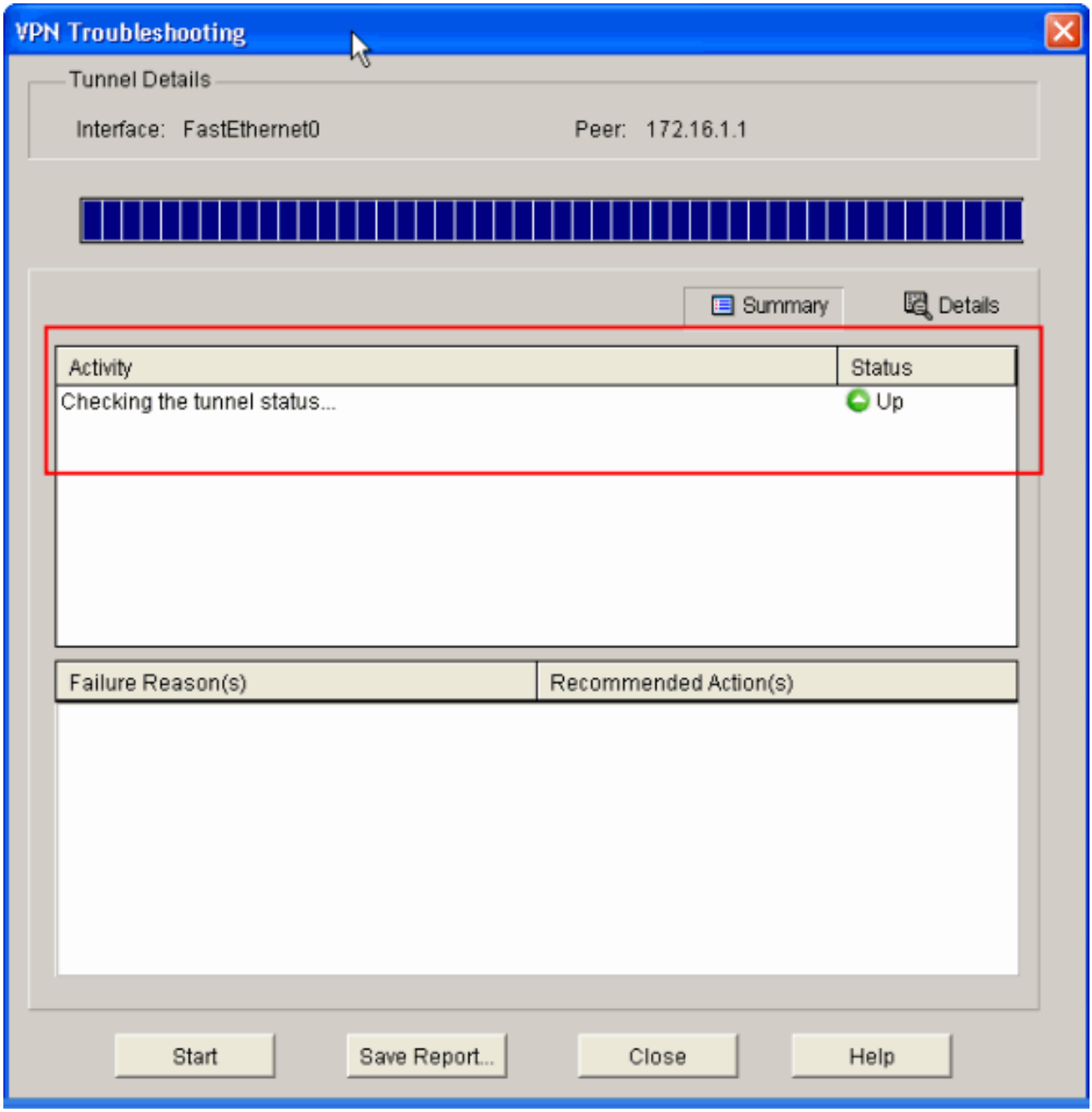
15. In questa finestra viene visualizzato il riepilogo della configurazione della VPN da sito a sito eseguita. Selezionare la casella di controllo **Test connettività VPN dopo la configurazione** se si desidera verificare la connettività VPN. In questo caso, la casella è selezionata in quanto è necessario selezionare la connettività. Fare quindi clic su **Fine**.



16. Fare clic su **Start** come mostrato per controllare la connettività VPN.



17. Nella finestra successiva viene fornito il risultato del **test di connettività VPN**. Qui potete vedere se il tunnel è **Su** o **Giù**. In questa configurazione di esempio, il tunnel è **attivo**, come mostrato in
verde.



La configurazione sul router Cisco IOS è stata completata.

Configurazione ASA CLI

ASA

```
ASA#show run
: Saved
ASA Version 8.0(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
!--- Configure the outside interface. ! interface
Ethernet0/1 nameif outside security-level 0 ip address
172.16.1.1 255.255.255.0 !--- Configure the inside
interface. ! interface Ethernet0/2 nameif inside
security-level 100 ip address 10.10.10.1 255.255.255.0
!-- Output suppressed ! passwd 2KFQnbNIdI.2KYOU
```

```
encrypted ftp mode passive dns server-group DefaultDNS
domain-name default.domain.invalid access-list 100
extended permit ip any any access-list
inside_nat0_outbound extended permit ip 10.10.10.0
255.255.255.0
10.20.10.0 255.255.255.0
!--- This access list (inside_nat0_outbound) is used !--
- with the nat zero command. This prevents traffic which
!--- matches the access list from undergoing network
address translation (NAT). !--- The traffic specified by
this ACL is traffic that is to be encrypted and !---
sent across the VPN tunnel. This ACL is intentionally !-
-- the same as (outside_1_cryptomap). !--- Two separate
access lists should always be used in this
configuration.

access-list outside_1_cryptomap extended permit ip
10.10.10.0 255.255.255.0
10.20.10.0 255.255.255.0
!--- This access list (outside_cryptomap) is used !---
with the crypto map outside_map !--- to determine which
traffic should be encrypted and sent !--- across the
tunnel. !--- This ACL is intentionally the same as
(inside_nat0_outbound). !--- Two separate access lists
should always be used in this configuration.

pager lines 24
mtu inside 1500
mtu outside 1500
no failover
asdm image disk0:/asdm-613.bin
asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 10.10.10.0 255.255.255.0

nat (inside) 0 access-list inside_nat0_outbound
!--- NAT 0 prevents NAT for networks specified in !---
the ACL inside_nat0_outbound.


access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.2 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
http server enable
http 0.0.0.0 0.0.0.0 dmz
no snmp-server location
no snmp-server contact

!--- PHASE 2 CONFIGURATION ---! !--- The encryption
types for Phase 2 are defined here. crypto ipsec
transform-set ESP-DES-SHA esp-des esp-sha-hmac
!--- Define the transform set for Phase 2. crypto map
outside_map 1 match address outside_1_cryptomap
!--- Define which traffic should be sent to the IPsec
peer. crypto map outside_map 1 set peer 172.17.1.1
!--- Sets the IPsec peer crypto map outside_map 1 set
```

```
transform-set ESP-DES-SHA
!--- Sets the IPsec transform set "ESP-AES-256-SHA" !---
to be used with the crypto map entry "outside_map".
crypto map outside_map interface outside
!--- Specifies the interface to be used with !--- the
settings defined in this configuration. !--- PHASE 1
CONFIGURATION ---! !--- This configuration uses isakmp
policy 10. !--- The configuration commands here define
the Phase !--- 1 policy parameters that are used. crypto
isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption des
 hash sha
 group 1
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!



tunnel-group 172.17.1.1 type ipsec-l2l
!--- In order to create and manage the database of
connection-specific !--- records for ipsec-l2l-IPsec
(LAN-to-LAN) tunnels, use the command !--- tunnel-group
in global configuration mode. !--- For L2L connections
the name of the tunnel group MUST be the IP !--- address
of the IPsec peer.



tunnel-group 172.17.1.1 ipsec-attributes
 pre-shared-key *
!--- Enter the pre-shared-key in order to configure the
!--- authentication method. telnet timeout 5 ssh timeout
5 console timeout 0 threat-detection basic-threat
threat-detection statistics access-list ! class-map
inspection_default match default-inspection-traffic ! !
!-- Output suppressed! username cisco123 password
ffIRPGpDSOJh9YLq encrypted privilege 15
Cryptochecksum:be38dfaef777a339b9e1c89202572a7d : end
```

Configurazione CLI router

Router

```
Building configuration...

Current configuration : 2403 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
```

```
boot-start-marker
boot-end-marker
!
no logging buffered
!
username cisco123 privilege 15 password 7
1511021F07257A767B
no aaa new-model
ip subnet-zero
!
!
ip cef
!
!
ip ips po max-events 100
no ftp-server write-enable
!

!--- 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 2
 authentication pre-share

!--- Specifies the pre-shared key "cisco123" which
should !--- be identical at both peers. This is a global
!--- configuration mode command. crypto isakmp key
cisco123 address 172.16.1.1
!
!
!--- 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 ASA-IPSEC
esp-des esp-sha-hmac
!

!--- !--- Indicates that IKE is used to establish !---
the IPsec Security Association for protecting the !---
traffic specified by this crypto map entry. crypto map
SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to172.16.1.1

!--- !--- Sets the IP address of the remote end. set
peer 172.16.1.1

!--- !--- Configures IPsec to use the transform-set !---
"ASA-IPSEC" defined earlier in this configuration. set
transform-set ASA-IPSEC

!--- !--- Specifies the interesting traffic to be
encrypted. match address 100
!
!
!
!--- Configures the interface to use the !--- crypto map
"SDM_CMAP_1" for IPsec. interface FastEthernet0 ip
address 172.17.1.1 255.255.255.0 duplex auto speed auto
crypto map SDM_CMAP_1
!
interface FastEthernet1
 ip address 10.20.10.2 255.255.255.0
```

```
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
!
interface Vlan1
 ip address 10.77.241.109 255.255.255.192
!
ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.233.0 255.255.255.0 10.77.241.65
ip route 172.16.1.0 255.255.255.0 172.17.1.2
!
!
ip nat inside source route-map nonat interface
FastEthernet0 overload
!
ip http server
ip http authentication local
ip http secure-server
!
!--- Configure the access-lists and map them to the
Crypto map configured. access-list 100 remark SDM_ACL
Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
!
!
!
!--- This ACL 110 identifies the traffic flows using
route map access-list 110 deny ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
access-list 110 permit ip 10.20.10.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 110
!
control-plane
!
!
line con 0
 login local
line aux 0
line vty 0 4
 privilege level 15
 login local
 transport input telnet ssh
!
end
```

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**.

- PIX Security Appliance - Comandi **show**
- Router IOS remoto - Comandi **show**

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: 172.17.1.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

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

```
ASA#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

      local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
      current_peer: 172.17.1.1

     #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
      #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 9, #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.: 172.16.1.1, remote crypto endpt.: 172.17.1.1

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 434C4A7F

    inbound esp sas:
      spi: 0xB7C1948E (3082917006)
         transform: esp-des esp-sha-hmac none
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 12288, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/3588)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x434C4A7F (1129073279)
         transform: esp-des esp-sha-hmac none
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 12288, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/3588)
         IV size: 8 bytes
         replay detection support: Y
```

Router IOS remoto - Comandi show

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

```
Router#show crypto isakmp sa

dst             src             state          conn-id slot status
172.17.1.1      172.16.1.1      QM_IDLE              3    0 ACTIVE
```

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

```
Router#show crypto ipsec sa
interface: FastEthernet0
    Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
   current_peer 172.16.1.1 port 500
     PERMIT, flags={origin_is_acl,}
  #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68
    #pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
     path mtu 1500, ip mtu 1500
     current outbound spi: 0xB7C1948E(3082917006)

     inbound esp sas:
      spi: 0x434C4A7F(1129073279)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3004)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB7C1948E(3082917006)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3002)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

- **show crypto engine connections active**: visualizza le connessioni correnti e le informazioni sui pacchetti crittografati e decrittografati (solo router).

```
Router#show crypto engine connections active

  ID Interface            IP-Address      State  Algorithm           Encrypt  Decrypt
   3 FastEthernet0        172.17.1.1      set    HMAC_SHA+DES_56_CB        0        0
2001 FastEthernet0        172.17.1.1      set    DES+SHA                   0       59
2002 FastEthernet0        172.17.1.1      set    DES+SHA                  59        0
```

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**.

Nota: consultare le informazioni importanti sui comandi di debug e sulla risoluzione dei problemi di sicurezza IP - Comprensione e uso dei comandi di debug prima di usare i comandi di **debug**.

- **debug crypto ipsec 7**: visualizza le negoziazioni IPsec della fase 2.**debug crypto isakmp 7**: visualizza le negoziazioni ISAKMP della fase 1.
- **debug crypto ipsec**: visualizza le negoziazioni IPsec della fase 2.**debug crypto isakmp**: visualizza le negoziazioni ISAKMP della fase 1.

Per ulteriori informazioni sulla risoluzione dei problemi relativi alla VPN da sito a sito, fare riferimento alle soluzioni di risoluzione dei problemi più comuni per VPN IPSec da sito a sito e da accesso remoto.

Informazioni correlate

- Software Cisco PIX Firewall
- Cisco Adaptive Security Device Manager
- Cisco ASA serie 5500 Adaptive Security Appliance
- Configuration Professional: Esempio di VPN IPsec da sito a sito tra ASA/PIX e una configurazione di router IOS
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Cisco Router e Security Device Manager
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems