

Creazione di tunnel ridondanti tra firewall tramite PDM

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Convenzioni](#)

[Premesse](#)

[Configurazione](#)

[Procedura di configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

Questo documento descrive la procedura da utilizzare per configurare i tunnel tra due firewall PIX con Cisco PIX Device Manager (PDM). I firewall PIX si trovano in due siti diversi. In caso di mancato raggiungimento del percorso principale, è consigliabile avviare il tunnel tramite un collegamento ridondante. IPsec è una combinazione di standard aperti che forniscono riservatezza, integrità e autenticazione dell'origine dei dati tra peer IPsec.

[Prerequisiti](#)

[Requisiti](#)

Nessun requisito specifico previsto per questo documento.

[Componenti usati](#)

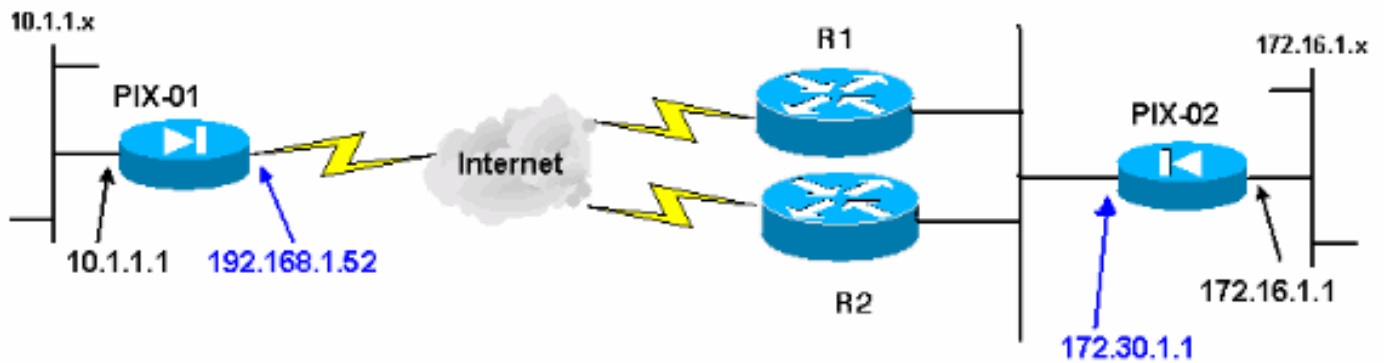
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure PIX 515E Firewall con 6.x e PDM versione 3.0

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.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Convenzioni

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.](#)

Premesse

La negoziazione IPsec può essere suddivisa in cinque fasi e include due fasi IKE (Internet Key Exchange).

Un tunnel IPsec viene avviato da traffico interessante. Il traffico è considerato interessante quando avviene tra peer IPsec.

Nella fase 1 di IKE, i peer IPsec negoziano il criterio SA (Security Association) IKE stabilito. Dopo l'autenticazione dei peer, viene creato un tunnel protetto utilizzando Internet Security Association and Key Management Protocol (ISAKMP).

In IKE fase 2, i peer IPsec utilizzano il tunnel autenticato e sicuro per negoziare le trasformazioni di associazione di sicurezza IPsec. La negoziazione del criterio condiviso determina la modalità di definizione del tunnel IPsec.

Il tunnel IPsec viene creato e i dati vengono trasferiti tra i peer IPsec in base ai parametri IPsec configurati nei set di trasformazioni IPsec.

Il tunnel IPsec termina quando le associazioni di protezione IPsec vengono eliminate o quando scade la loro durata.

Nota: la negoziazione IPsec tra i due PIX non ha esito positivo se le associazioni di protezione su entrambe le fasi IKE non corrispondono sui peer.

Configurazione

Questa procedura guida l'utente nella configurazione di uno dei firewall PIX per attivare il tunnel quando esiste traffico interessante. Questa configurazione consente anche di stabilire il tunnel

attraverso il collegamento di backup attraverso il router 2 (R2), quando non vi è connettività tra PIX-01 e PIX-02 attraverso il router 1 (R1). Questo documento mostra la configurazione di PIX-01 con PDM. È possibile configurare PIX-02 su linee simili.

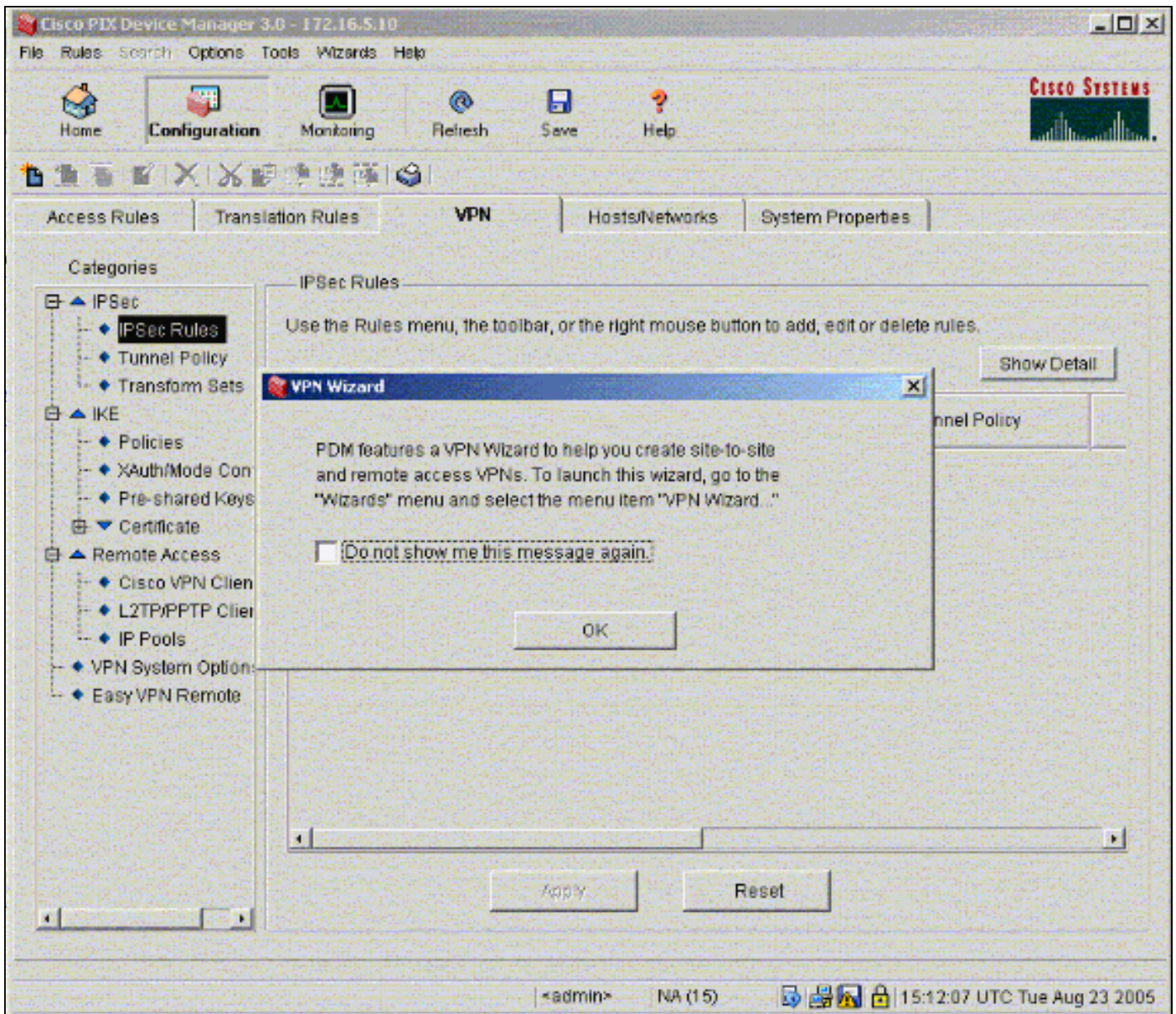
in questo documento si presume che il routing sia già stato configurato.

Affinché sia attivo un solo collegamento alla volta, rendere R2 pubblicizza una metrica peggiore per la rete 192.168.1.0 e per la rete 172.30.0.0. Ad esempio, se si utilizza RIP per il routing, R2 ha questa configurazione a parte altri annunci di rete:

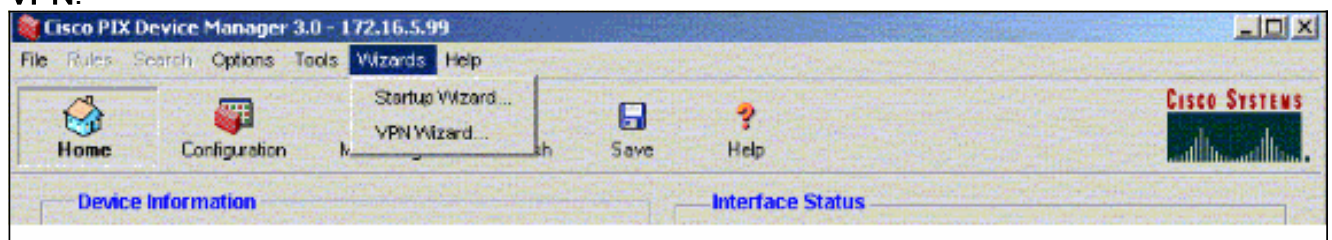
```
R2(config)#router rip
R2(config-router)#offset-list 1 out 2 s1
R2(config-router)#offset-list 2 out 2 e0
R2(config-router)#exit
R2(config)#access-list 1 permit 172.30.0.0 0.0.255.255
R2(config)#access-list 2 permit 192.168.1.0 0.0.0.255
```

[Procedura di configurazione](#)

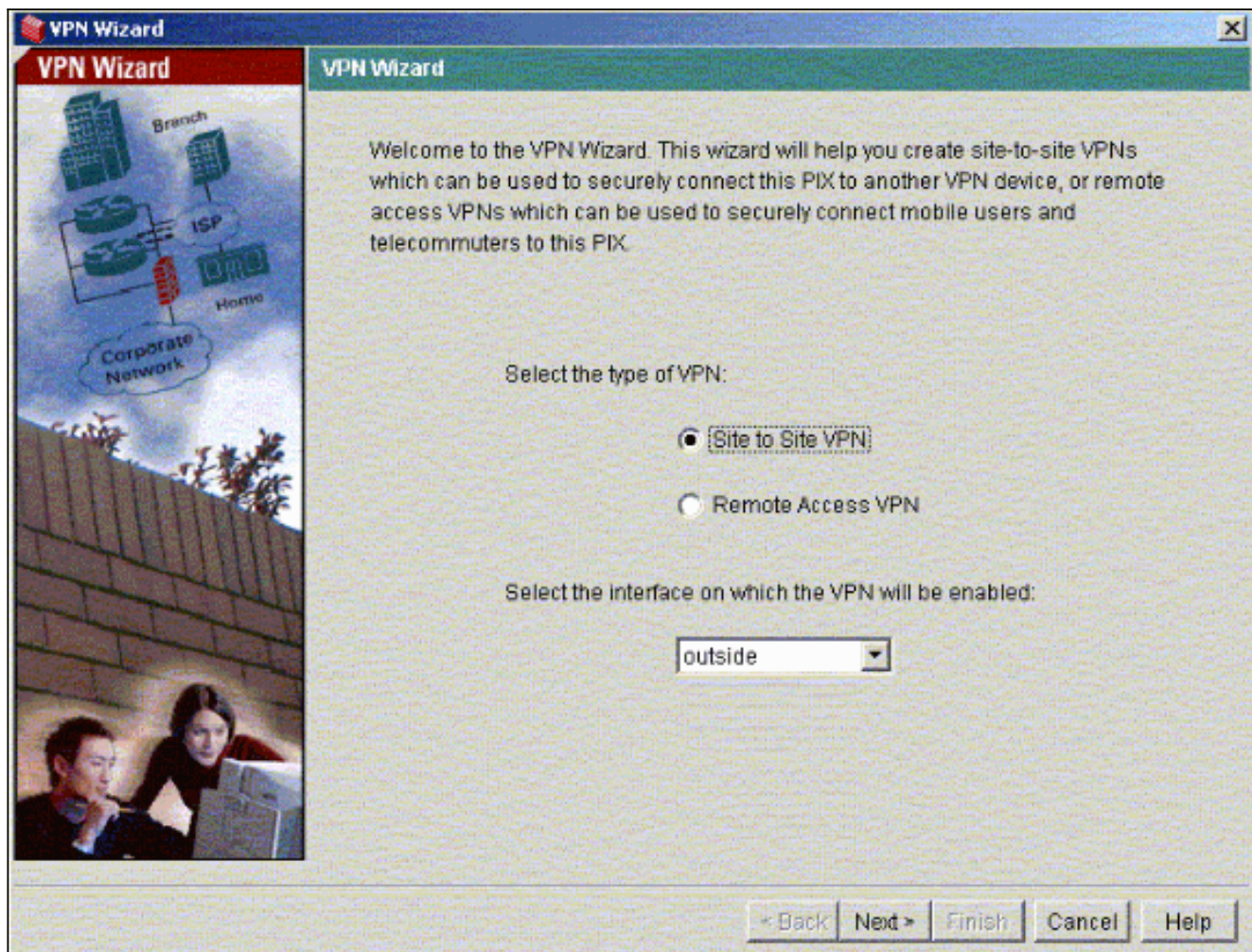
Quando si digita https://<Inside_IP_Address_on_PIX> per avviare PDM e si fa clic per la prima volta sulla scheda VPN, vengono visualizzate informazioni sulla Creazione guidata VPN automatica.



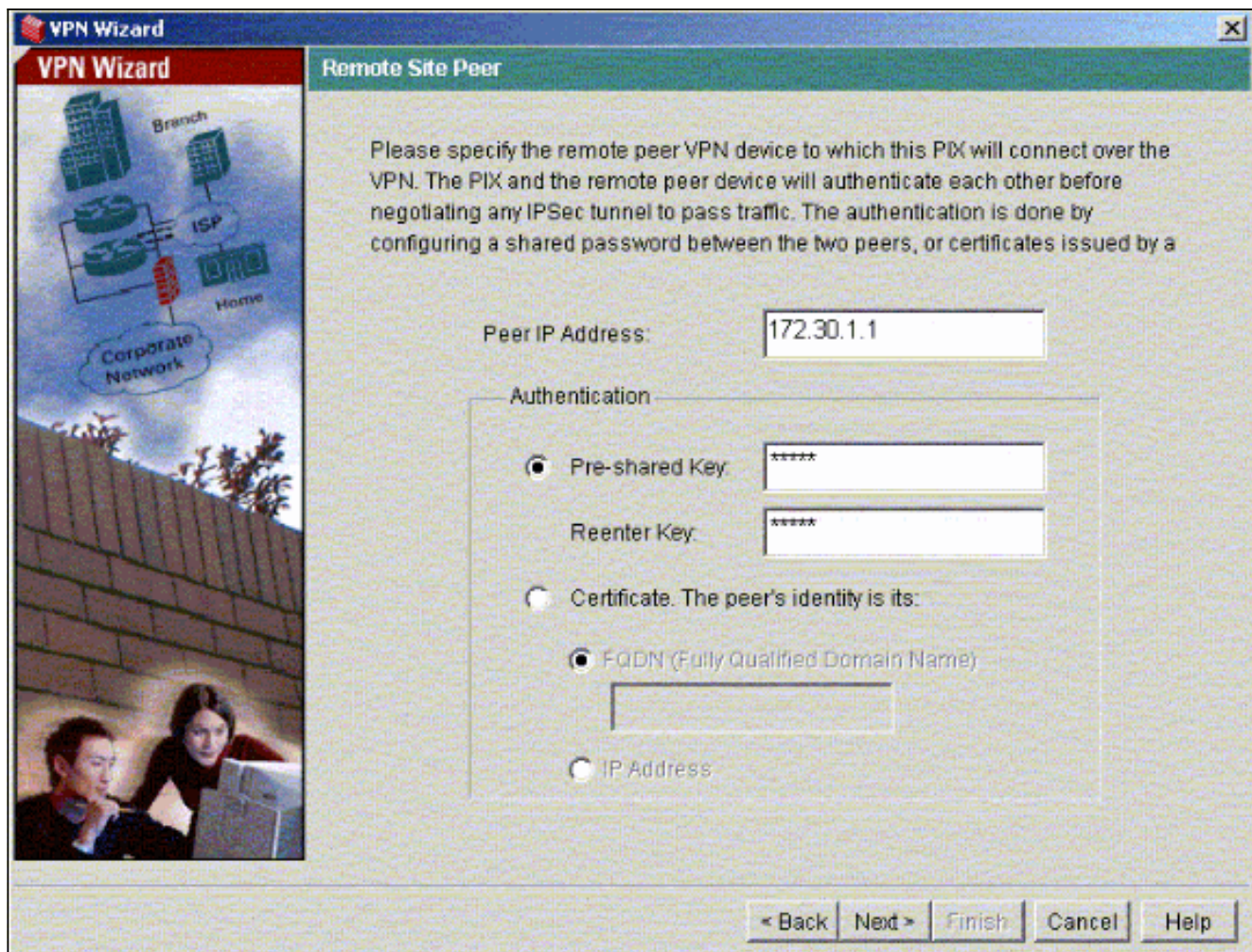
1. Selezionare **Procedure guidate > Creazione guidata VPN.**



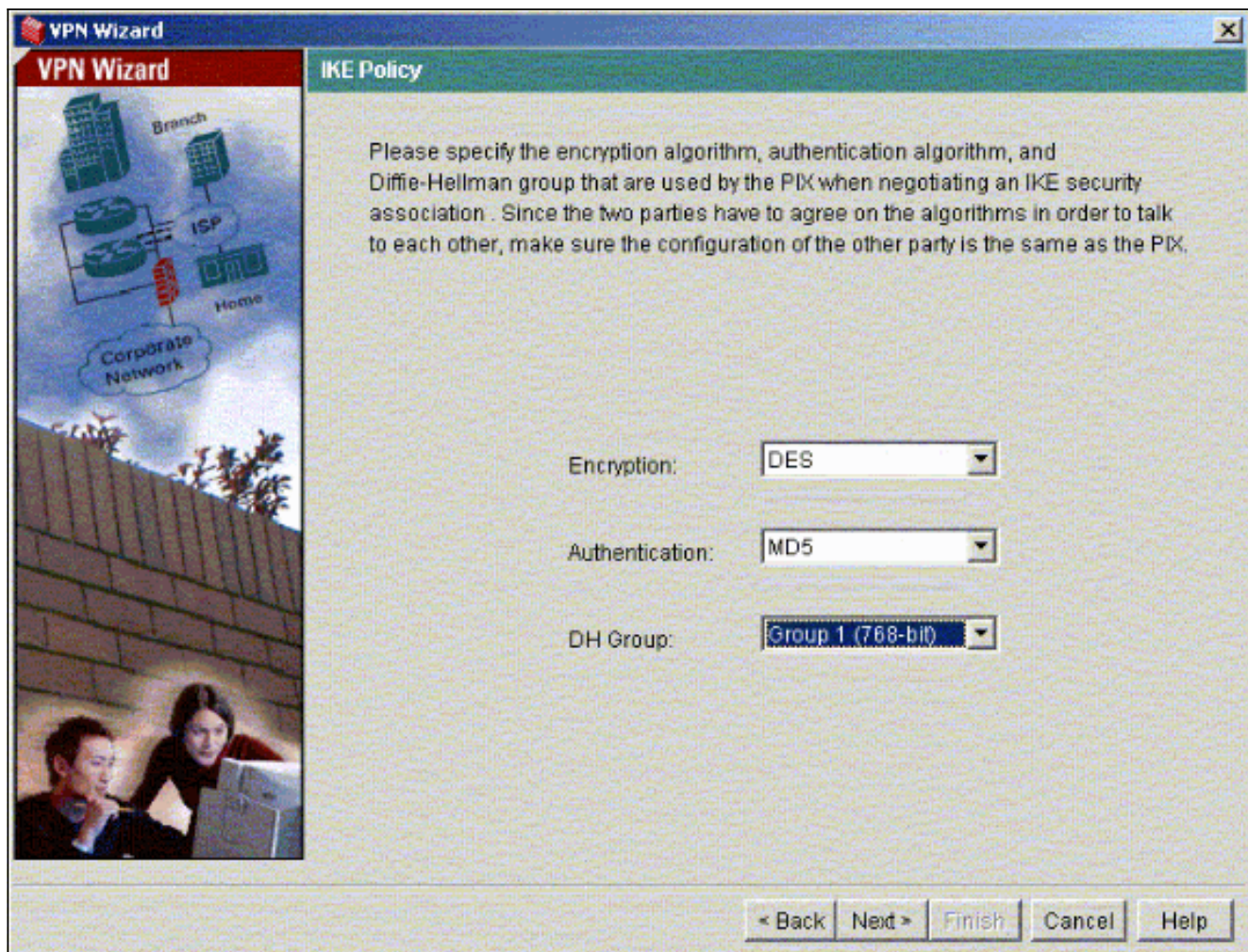
2. Verrà avviata la Creazione guidata VPN e verrà richiesto il tipo di VPN che si desidera configurare. Scegliere **VPN da sito a sito**, selezionare l'interfaccia **esterna** come interfaccia su cui verrà abilitata la VPN e fare clic su **Avanti.**



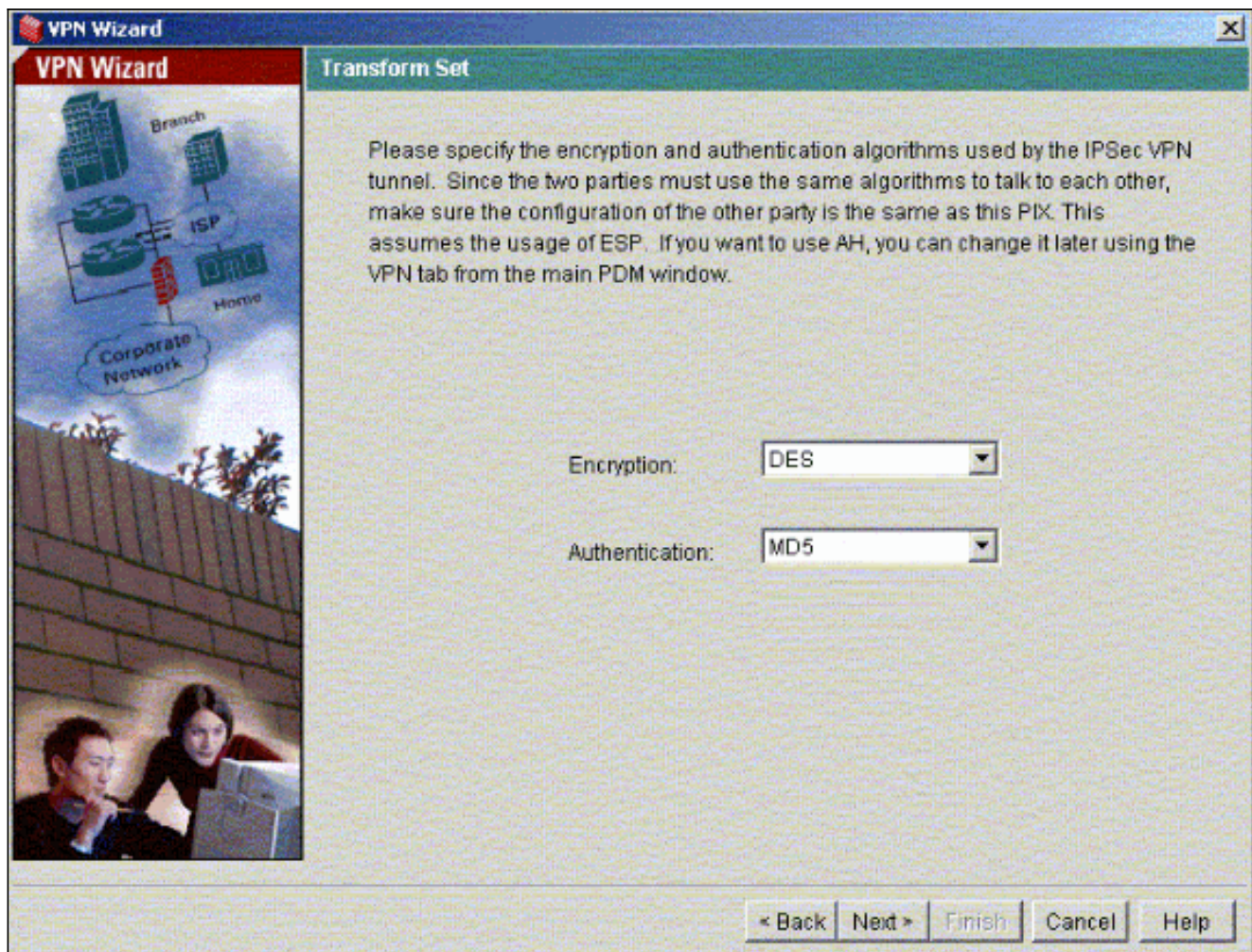
3. Immettere l'indirizzo IP del peer in cui deve terminare il tunnel IPsec. In questo esempio, il tunnel termina sull'interfaccia esterna del PIX-02. Fare clic su **Avanti**.



4. Immettere i parametri dei criteri IKE che si sceglie di utilizzare e fare clic su **Avanti**.




5. Specificare i parametri di crittografia e autenticazione per il set di trasformazioni e fare clic su **Avanti**.



6. Selezionare la rete locale e le reti remote da proteggere utilizzando IPsec per selezionare il traffico interessante da proteggere.

VPN Wizard X

VPN Wizard IPSec Traffic Selector



IPSec Traffic Selector selects the traffic flows that are going to be protected by the IPSec tunnel. Packets that flow between the selected hosts/networks inside the PIX (which you specify below) and the the selected hosts/networks at the remote site (which you will specify on the next screen) will be protected by the IPSec tunnel.

On Local Site (protected by this PIX)

Host/Network

IP Address
 Name
 Group

Interface:

IP address:

Mask:


Selected:

>>

<<

VPN Wizard X

VPN Wizard IPSec Traffic Selector (Continue)



Use this panel to specify the hosts/networks at the remote site that are used in IPSec Traffic Selector to select traffic flows to be protected by the IPSec tunnel.

On Remote Site

Host/Network

IP Address
 Name
 Group

Interface:

IP address:

Mask:

Selected:

>>

<<

Verifica

Se è presente traffico interessante verso il peer, il tunnel viene stabilito tra PIX-01 e PIX-02.

Per verificare questa condizione, chiudere l'interfaccia seriale R1 per la quale viene stabilito il tunnel tra PIX-01 e PIX-02 tramite R2 quando esiste il traffico interessato.

Visualizzare lo **stato VPN** in **Home** (Home) nel PDM (evidenziato in rosso) per verificare la formazione del tunnel.

The screenshot displays the Cisco PIX Device Manager 3.0 interface. The 'VPN Status' section is highlighted with a red box, showing 1 IKE Tunnel and 1 IPsec Tunnel. The 'Interface Status' table shows the following data:

Interface	IP Address/Mask	Link	Current Kbps
intf2	0.0.0.0/0	down	0
inside	172.16.5.99/24	up	7
outside	150.1.1.66/24	up	0
intf5	0.0.0.0/0	down	0
intf4	0.0.0.0/0	down	0
intf3	0.0.0.0/0	down	0

The 'System Resources Status' section shows CPU usage at 0% and memory usage at 18MB. The 'Traffic Status' section includes two graphs: 'Connections Per Second Usage' and ''outside' Interface Traffic Usage (Kbps)'. The status bar at the bottom indicates the user is <admin> on NA (15) at 17:00:31 UTC Thu Sep 08 2005.

È inoltre possibile verificare la formazione dei tunnel utilizzando CLI in Strumenti in PDM. Utilizzare il comando **show crypto isakmp sa** per controllare la formazione dei tunnel e il comando **show crypto ipsec sa** per osservare il numero di pacchetti incapsulati, crittografati e così via.

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

Fare riferimento a [Cisco PIX Device Manager 3.0](#) per ulteriori informazioni sulla configurazione del firewall PIX con PDM.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- [Configurazione di un tunnel VPN da PIX a PIX semplice con IPsec](#)
- [Software Cisco PIX Firewall](#)
- [Riferimenti per i comandi di Cisco Secure PIX Firewall](#)
- [RFC \(Requests for Comments\)](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)