

使用PDM在防火牆之間建立冗餘隧道

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[網路圖表](#)

[慣例](#)

[背景資訊](#)

[組態](#)

[設定程式](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹使用Cisco PIX裝置管理器(PDM)在兩個PIX防火牆之間配置隧道的過程。PIX防火牆位於兩個不同的站點。如果無法到達主路徑，最好通過冗餘鏈路啟動隧道。IPsec是開放標準的組合，可在IPsec對等路由器之間提供資料機密性、資料完整性以及資料來源驗證。

必要條件

需求

本文件沒有特定需求。

採用元件

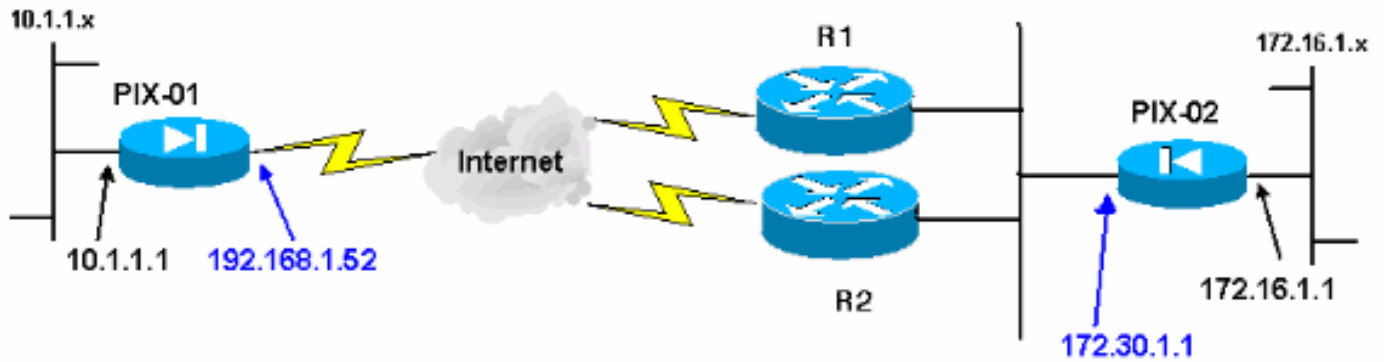
本文中的資訊係根據以下軟體和硬體版本：

- Cisco Secure PIX 515E防火牆，帶6.x和PDM 3.0版

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

網路圖表

本檔案會使用以下網路設定：



慣例

請參閱[思科技術提示慣例](#)以瞭解更多有關文件慣例的資訊。

背景資訊

IPsec交涉可分為五個步驟，並包括兩個網際網路金鑰交換(IKE)階段。

IPsec隧道由相關流量發起。流量在IPsec對等路由器之間傳輸時，會被視為有趣。

在IKE第1階段，IPsec對等體協商已建立的IKE安全關聯(SA)策略。對等點通過驗證後，會使用網際網路安全性關聯和金鑰管理通訊協定(ISAKMP)建立安全通道。

在IKE第2階段，IPsec對等使用經過身份驗證的安全隧道協商IPsec SA轉換。共用策略的協商確定如何建立IPsec隧道。

將建立IPsec隧道，並根據IPsec轉換集中配置的IPsec引數在IPsec對等體之間傳輸資料。

IPsec隧道在IPsec SA被刪除或其生存期到期時終止。

注意：如果兩個IKE階段上的SA在對等方上不匹配，則兩個PIX之間的IPsec協商失敗。

組態

此過程指導您完成一個PIX防火牆的配置，以便在存在相關流量時觸發隧道。當PIX-01和PIX-02之間沒有通過路由器1(R1)的連線時，此配置還有助於您通過路由器2(R2)的備用鏈路建立隧道。本文檔介紹使用PDM配置PIX-01。您可以在類似線路上配置PIX-02。

本檔案假設您已設定路由。

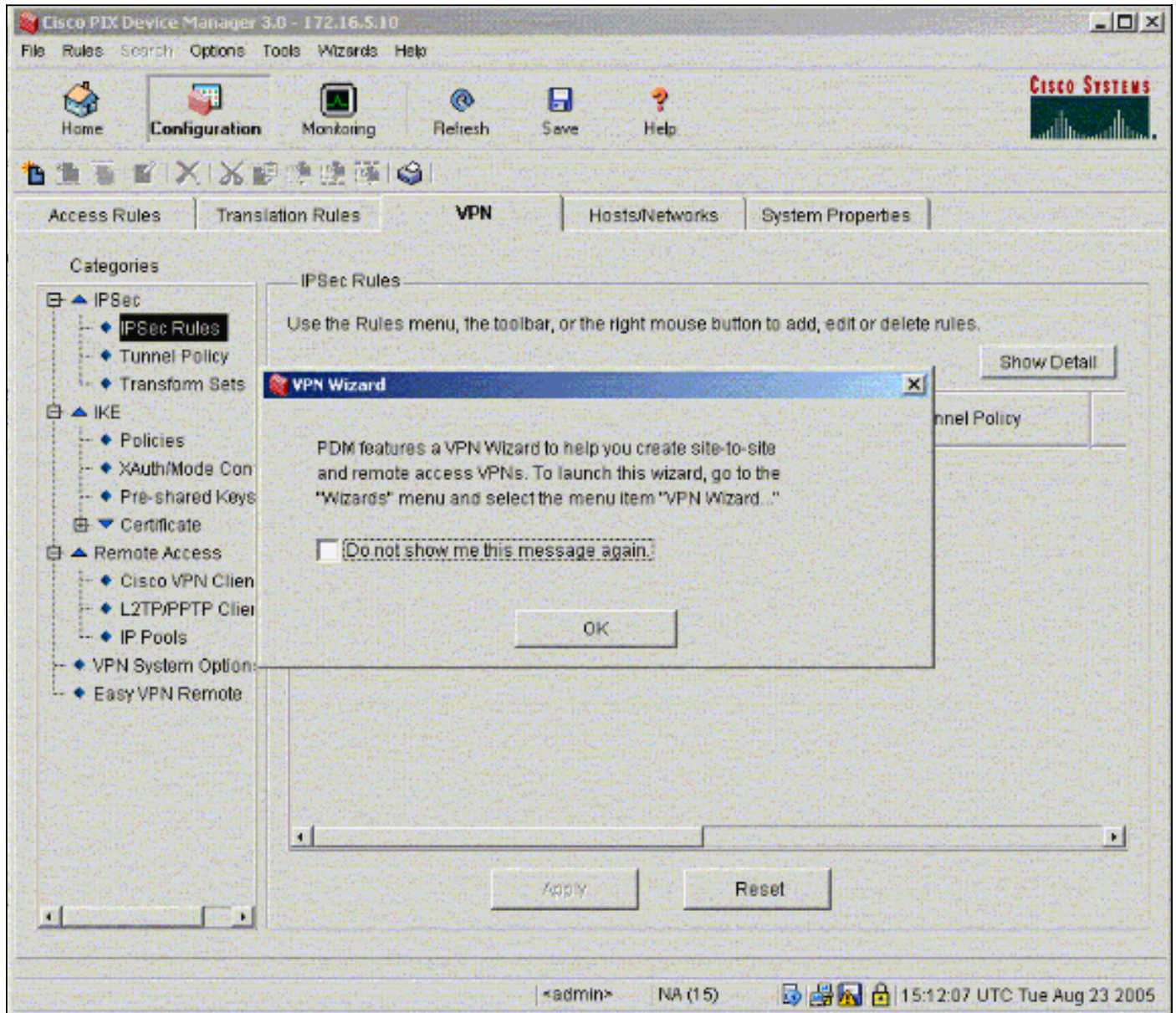
如果一次僅啟用一條鏈路，則使R2通告192.168.1.0網路和172.30.0.0網路的更差度量。例如，如果使用RIP進行路由，則R2除了其它網路通告外還具備以下配置：

```
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
```

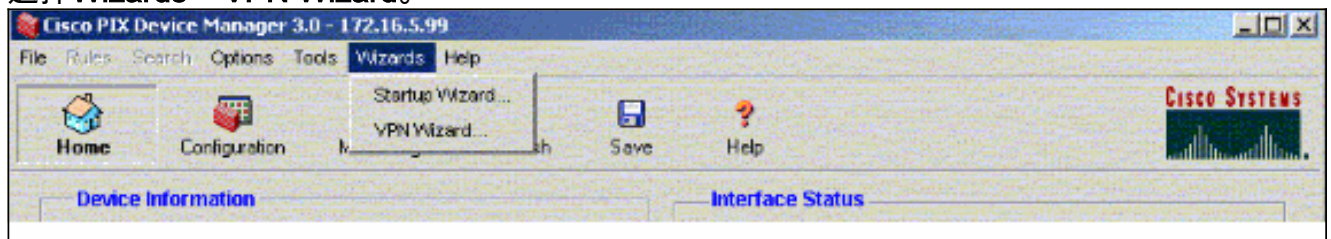
```
R2 (config) #access-list 2 permit 192.168.1.0 0.0.0.255
```

設定程式

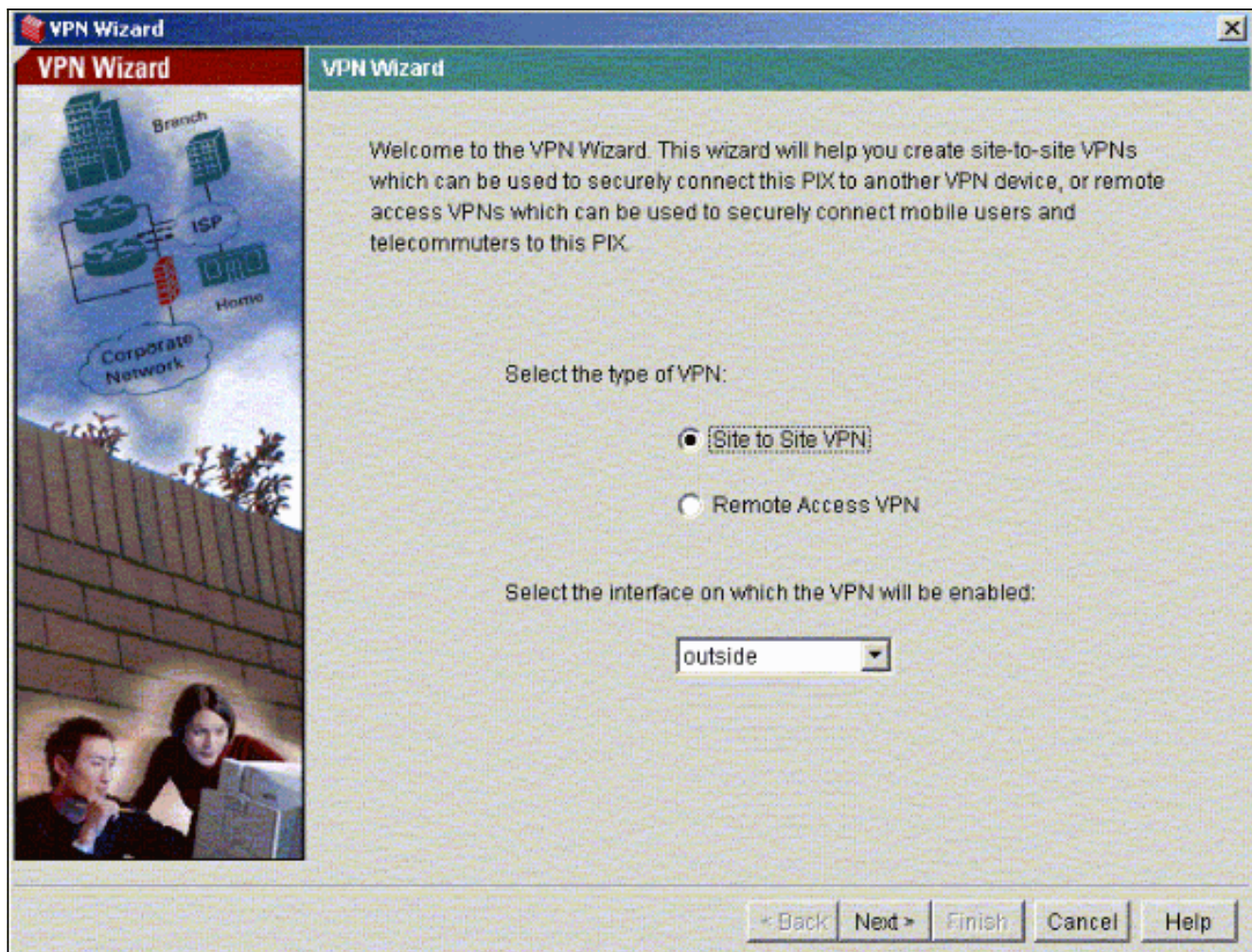
當鍵入https://<Inside_IP_Address_on_PIX>以啟動PDM並首次按一下VPN頁籤時，將顯示有關自動VPN嚮導的資訊。



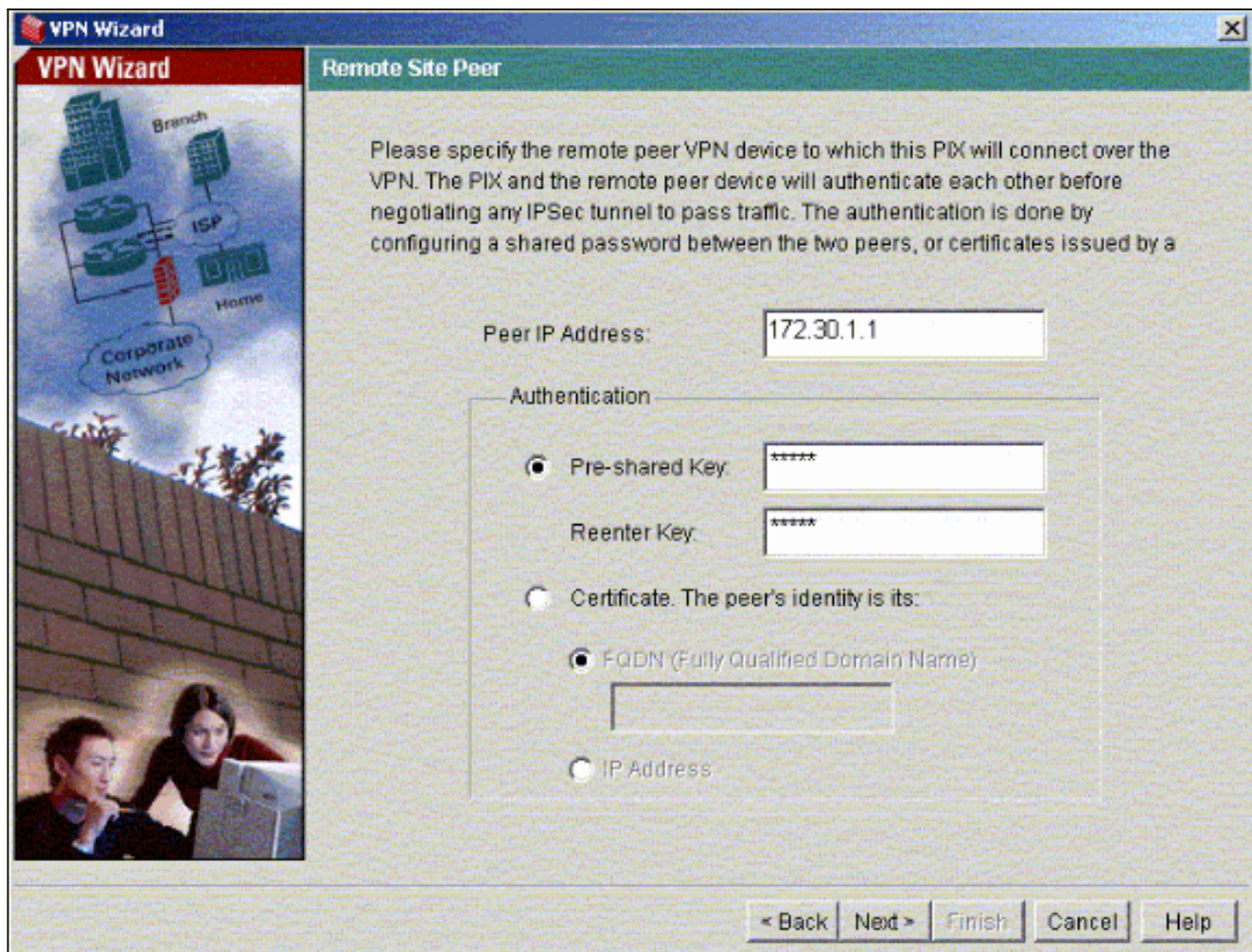
1. 選擇Wizards > VPN Wizard。



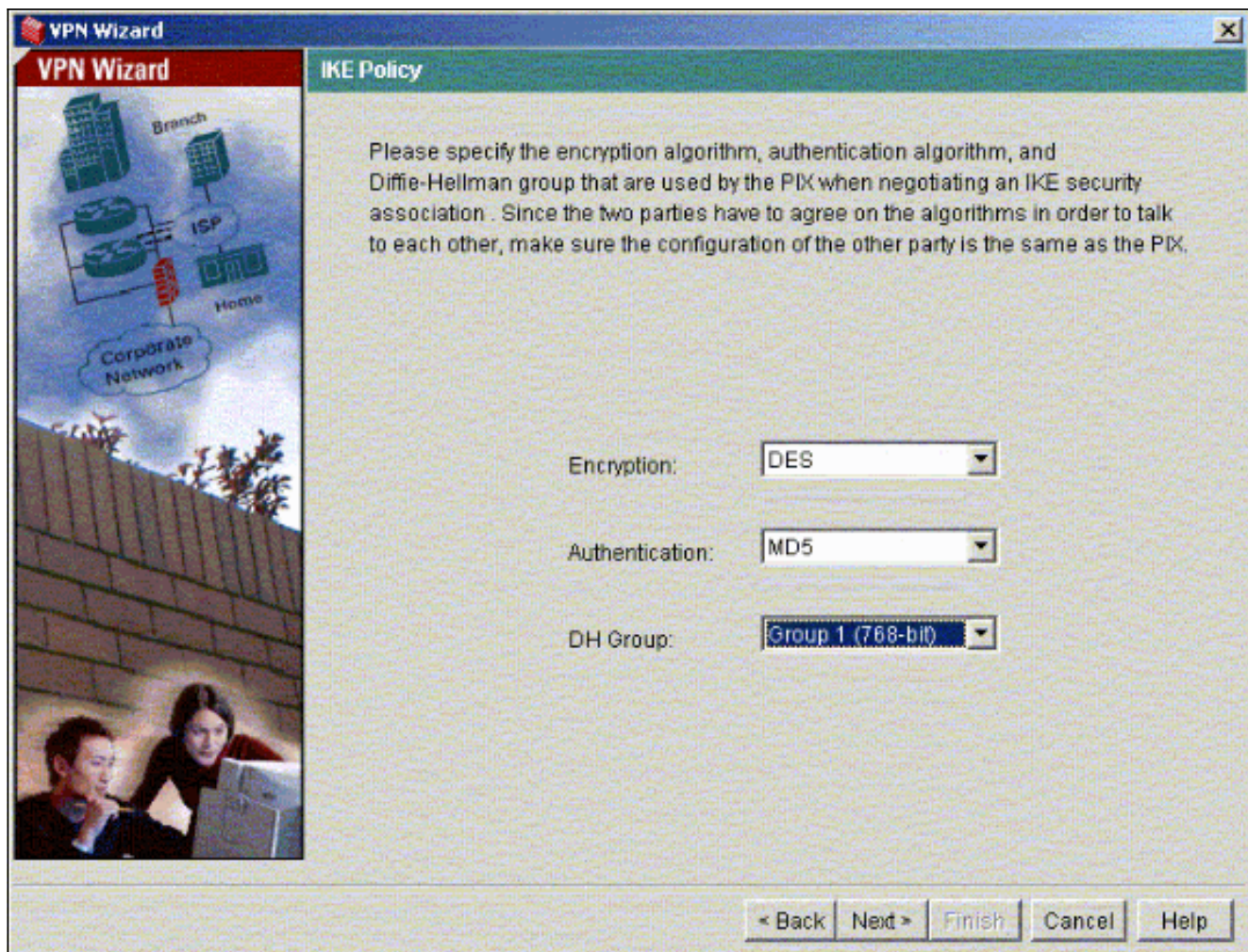
2. VPN嚮導將啟動並提示您輸入要配置的VPN型別。選擇Site-to-Site VPN，選擇outside介面作為啟用VPN的介面，然後按一下Next。



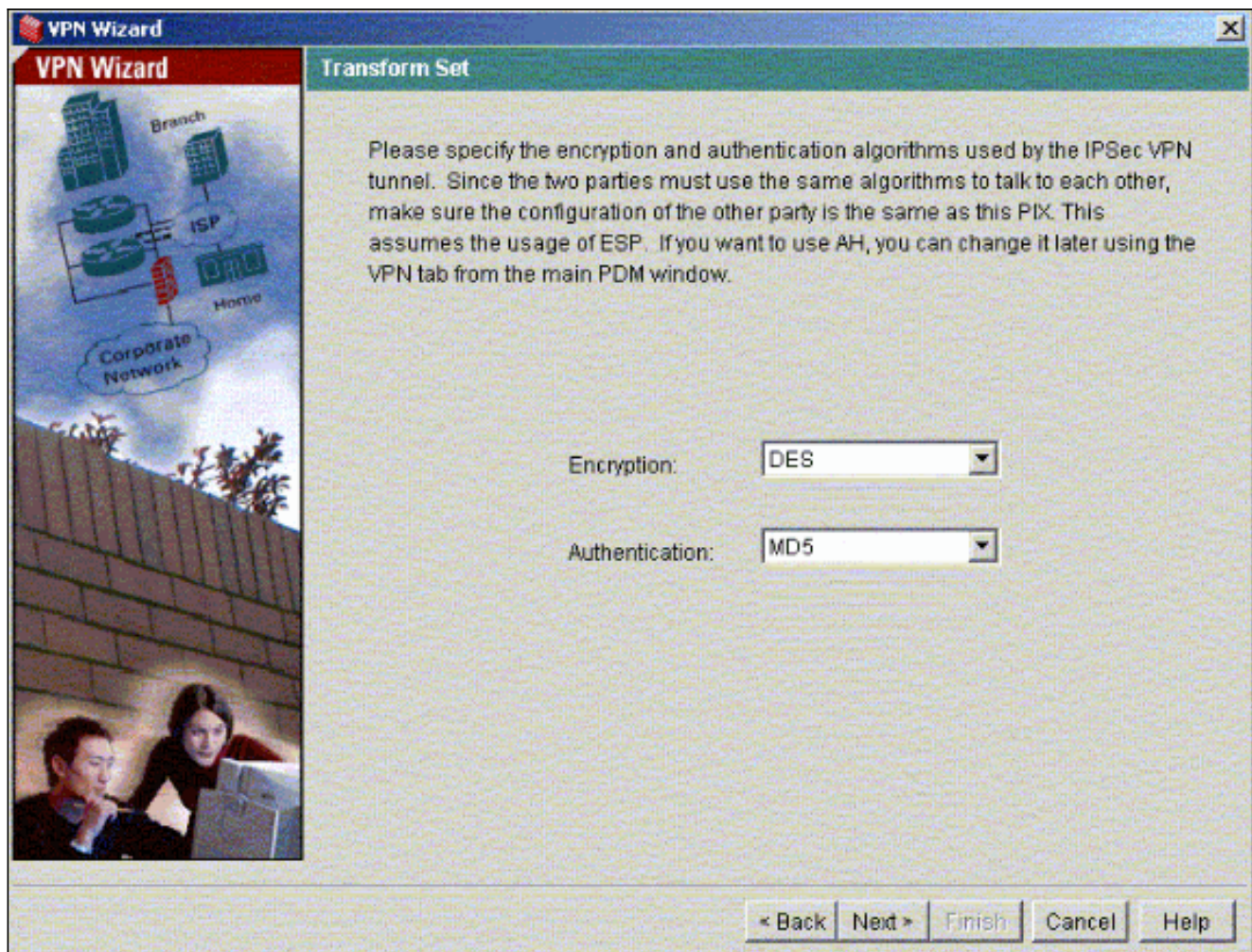
3. 輸入Peer IP地址，其中IPsec隧道應結束。在本示例中，隧道在PIX-02的外部介面上結束。按一下下一步。



4. 輸入要使用的IKE策略引數，然後按一下**Next**。




5. 為轉換集提供加密和身份驗證引數，然後按一下下一步。



6. 使用IPsec選擇需要保護的本地網路和遠端網路，以便選擇需要保護的相關流量。

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:

>>

<<

驗證

如果存在到對等體的相關流量，則在PIX-01和PIX-02之間建立隧道。

為了驗證這一點，請在存在相關流量時，關閉通過R2在PIX-01和PIX-02之間建立隧道的R1串列介面。

在PDM中檢視Home下的VPN Status (以紅色突出顯示)，以驗證通道的形成。

The screenshot displays the Cisco PIX Device Manager 3.0 interface for a device named PIX-01.cisco. The interface is divided into several sections:

- Device Information:** Host Name: PIX-01.cisco, PIX Version: 6.3(3), PDM Version: 3.0(1), Device Type: PIX 515E, Total Memory: 64 MB, License: Failover Only, Total Flash: 16MB.
- Interface Status:** A table showing the status of various interfaces. The 'inside' interface is up with 7 Kbps current traffic.
- VPN Status:** This section is highlighted with a red border. It shows 1 IKE Tunnel and 1 IPSec Tunnel.
- System Resources Status:** CPU usage is 0% and memory usage is 18MB.
- Traffic Status:** Two line graphs showing connections per second and interface traffic usage.

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

還可以在PDM中的「工具」(Tools)下使用CLI驗證隧道的形成。發出show crypto isakmp sa命令以檢查通道的形成，並發出show crypto ipsec sa命令以觀察封裝、加密等的資料包數量。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

有關使用PDM配置PIX防火牆的詳細資訊，請參閱[Cisco PIX裝置管理器3.0](#)。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

[相關資訊](#)

- [使用IPsec配置簡單的PIX到PIX VPN隧道](#)
- [Cisco PIX防火牆軟體](#)
- [Cisco Secure PIX防火牆命令參考](#)
- [要求建議 \(RFC\)](#)
- [技術支援與文件 - Cisco Systems](#)