使用PDM配置的兩個PIX之間的LAN到LAN VPN隧道示例

目錄

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VPN隧道的過程。PDM是一種基於瀏覽器的配置工具，旨在幫助您使用GUI設定、配置和監控PIX防火牆。PIX防火牆位於兩個不同的站點。

使用IPsec形成隧道。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

本檔案沒有需求。

採用元件

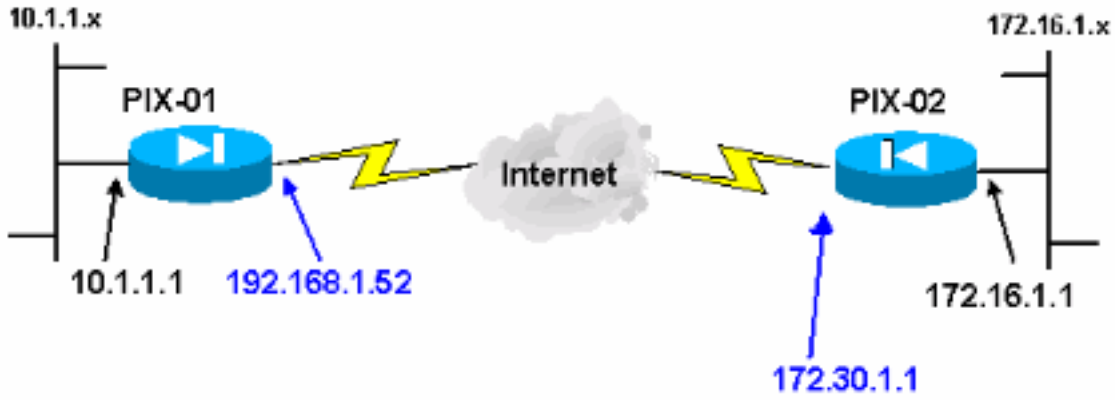
本文檔中的資訊基於具有6.x和PDM 3.0版的Cisco Secure PIX 515E防火牆。

有關使用命令列介面(CLI)在兩個PIX裝置之間配置VPN隧道的配置示例，請參閱使用IPsec配置簡單PIX到PIX VPN隧道。

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。

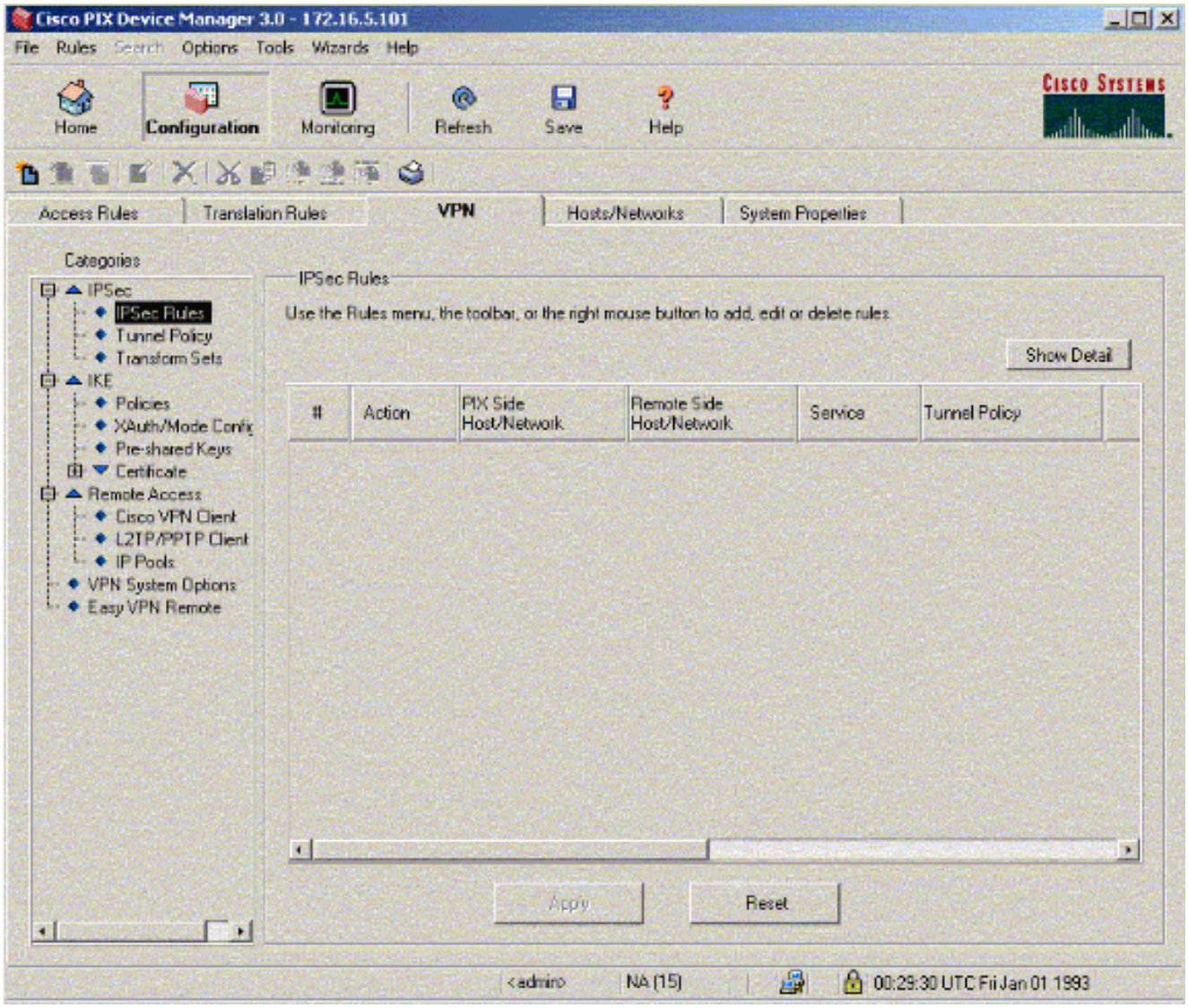
1. IPsec隧道由相關流量發起。流量在IPsec對等路由器之間傳輸時，會被視為有趣。
2. 在IKE第1階段，IPsec對等體協商已建立的IKE安全關聯(SA)策略。對等點通過驗證後，會使用網際網路安全性關聯和金鑰管理通訊協定(ISAKMP)建立安全通道。
3. 在IKE第2階段，IPsec對等使用經過身份驗證的安全隧道協商IPsec SA轉換。共用策略的協商確定如何建立IPsec隧道。
4. 將建立IPsec隧道，並根據IPsec轉換集中配置的IPsec引數在IPsec對等體之間傳輸資料。
5. IPsec隧道在IPsec SA被刪除或其生存期到期時終止。**注意**：如果兩個IKE階段上的SA在對等方上不匹配，則兩個PIX之間的IPsec協商失敗。

設定程式

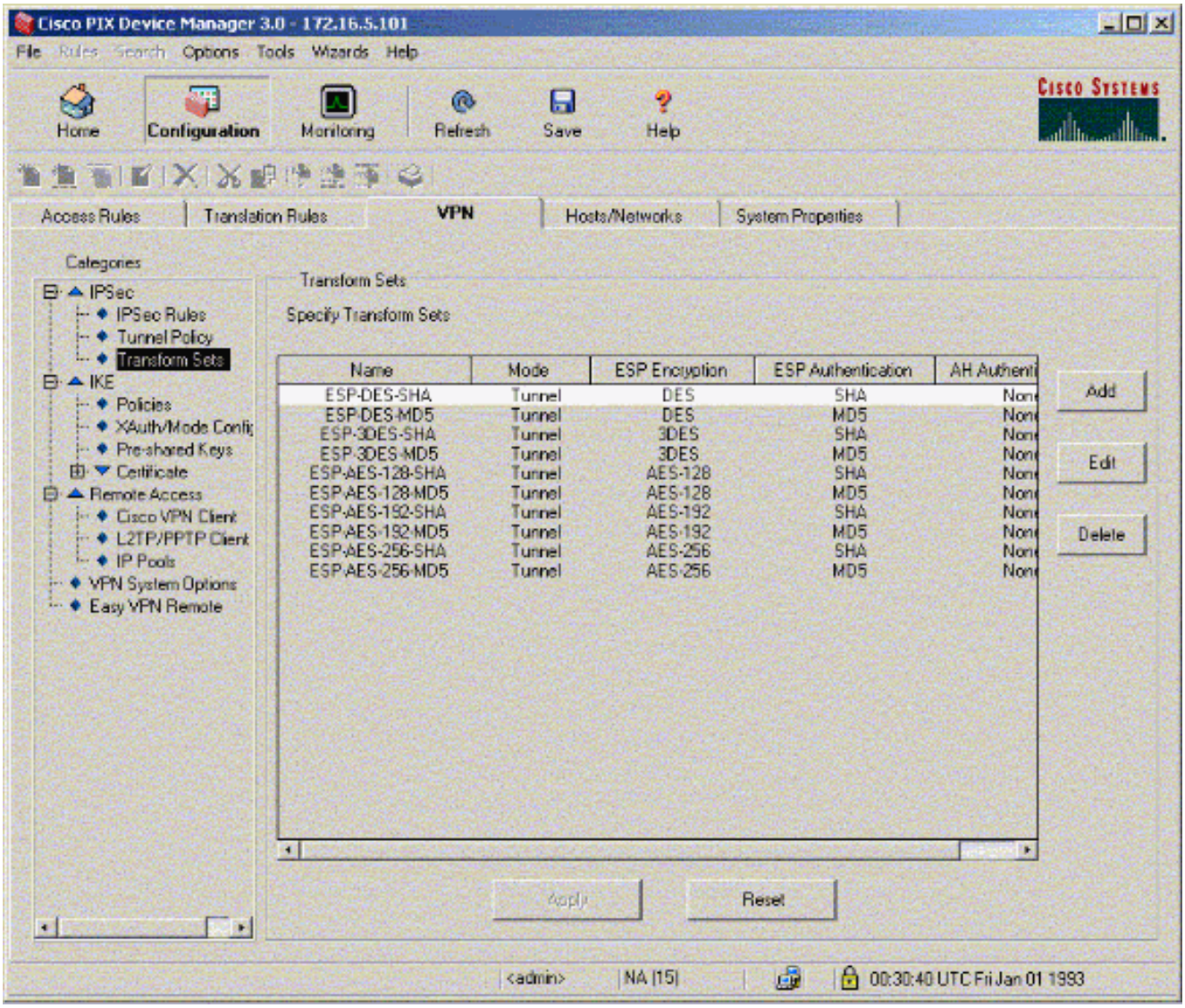
除了PIX的CLI上的其他常規配置來通過Ethernet 0介面訪問它外，還可以使用**http server enable**和**http server <local_ip> <mask> <interface>**命令，其中*<local_ip>* 和*<mask>* 是安裝PDM的工作站的IP地址和掩碼。本文檔中的配置用於PIX-01。可以使用不同地址的相同步驟配置PIX-02。

請完成以下步驟：

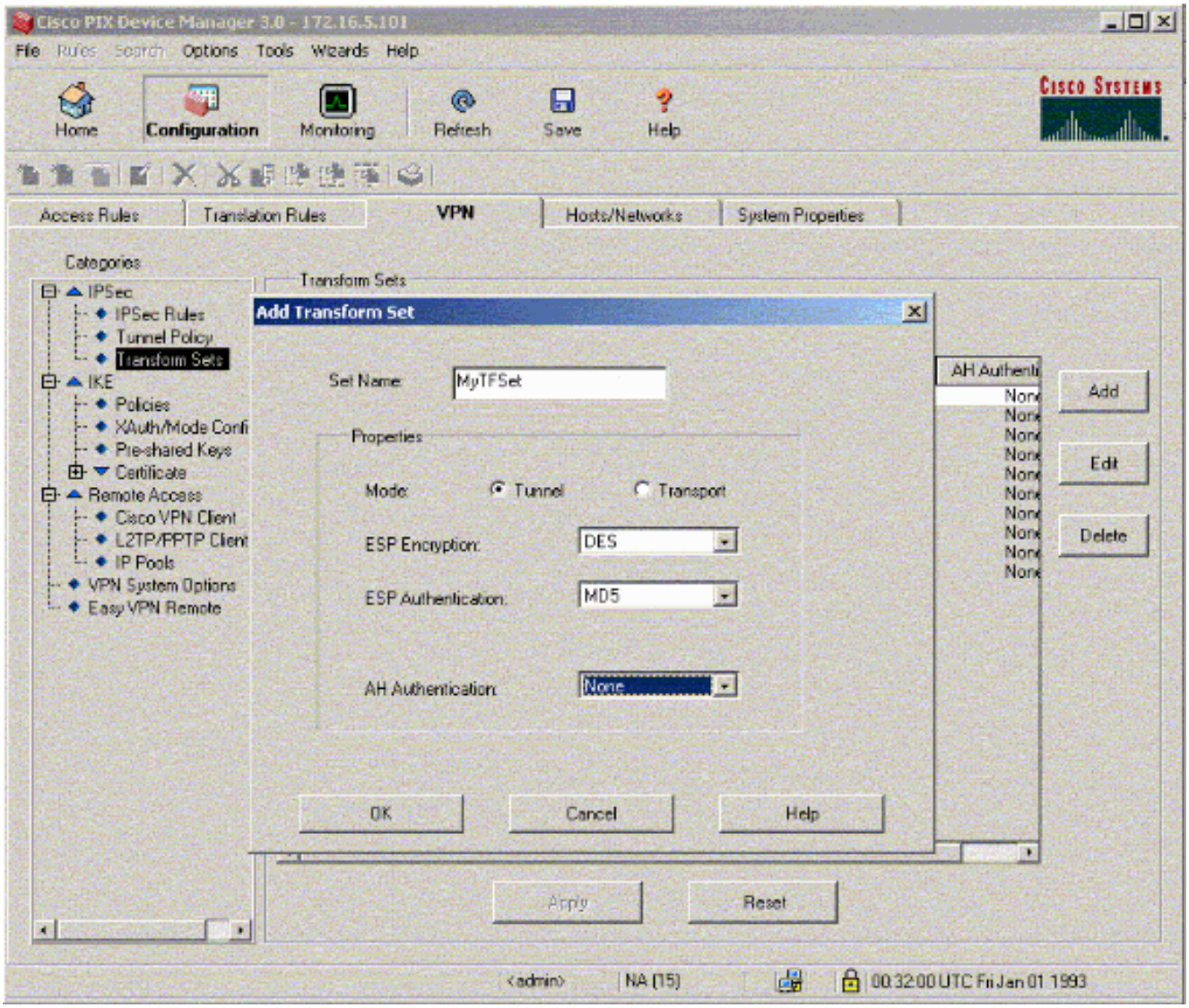
1. 開啟瀏覽器並鍵入**https://<Inside_IP_Address_of_PIX>**以訪問PDM中的PIX。
2. 按一下**Configuration**並轉到VPN頁籤。



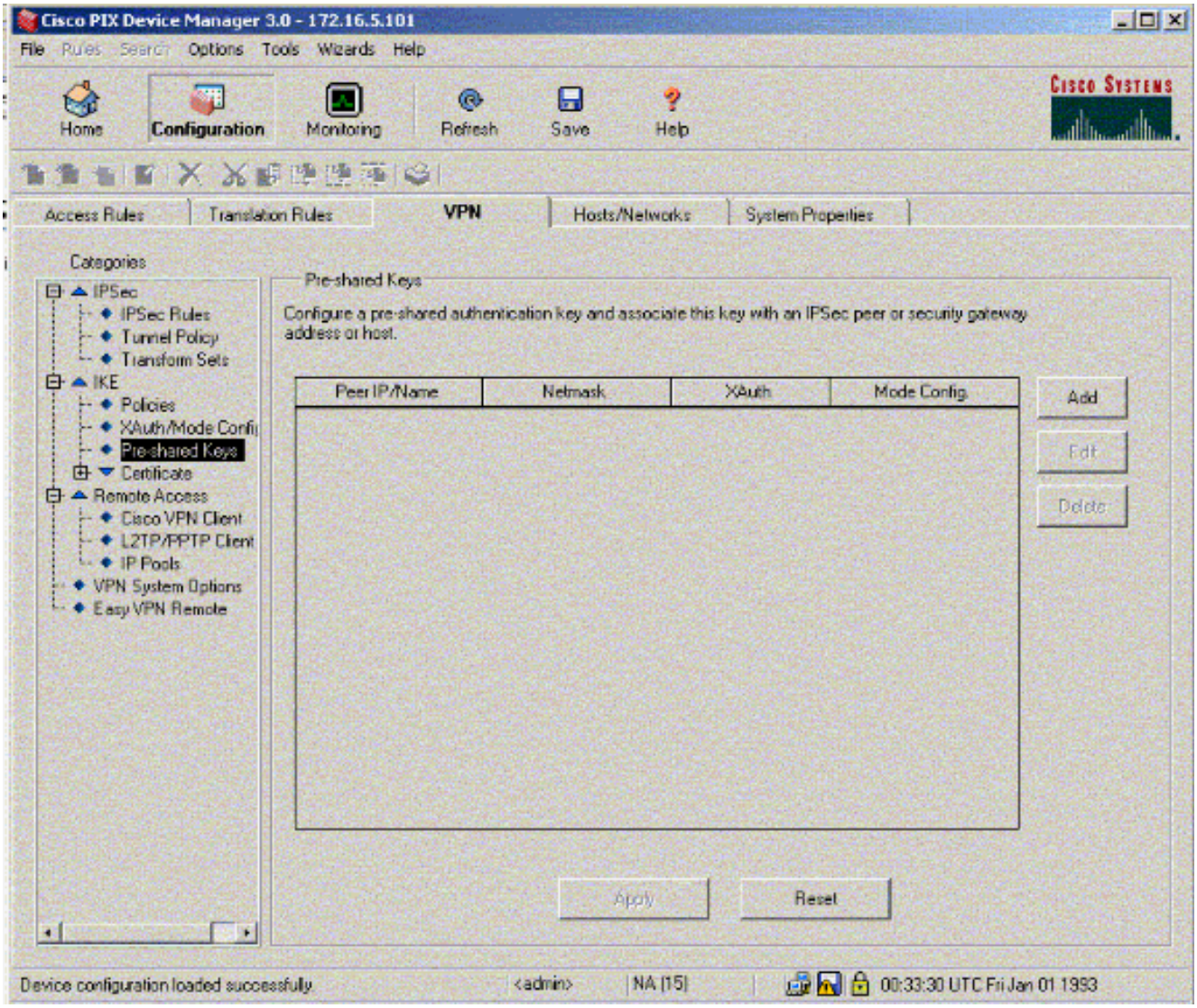
3. 按一下IPSec下的**Transform Sets**以建立轉換集。



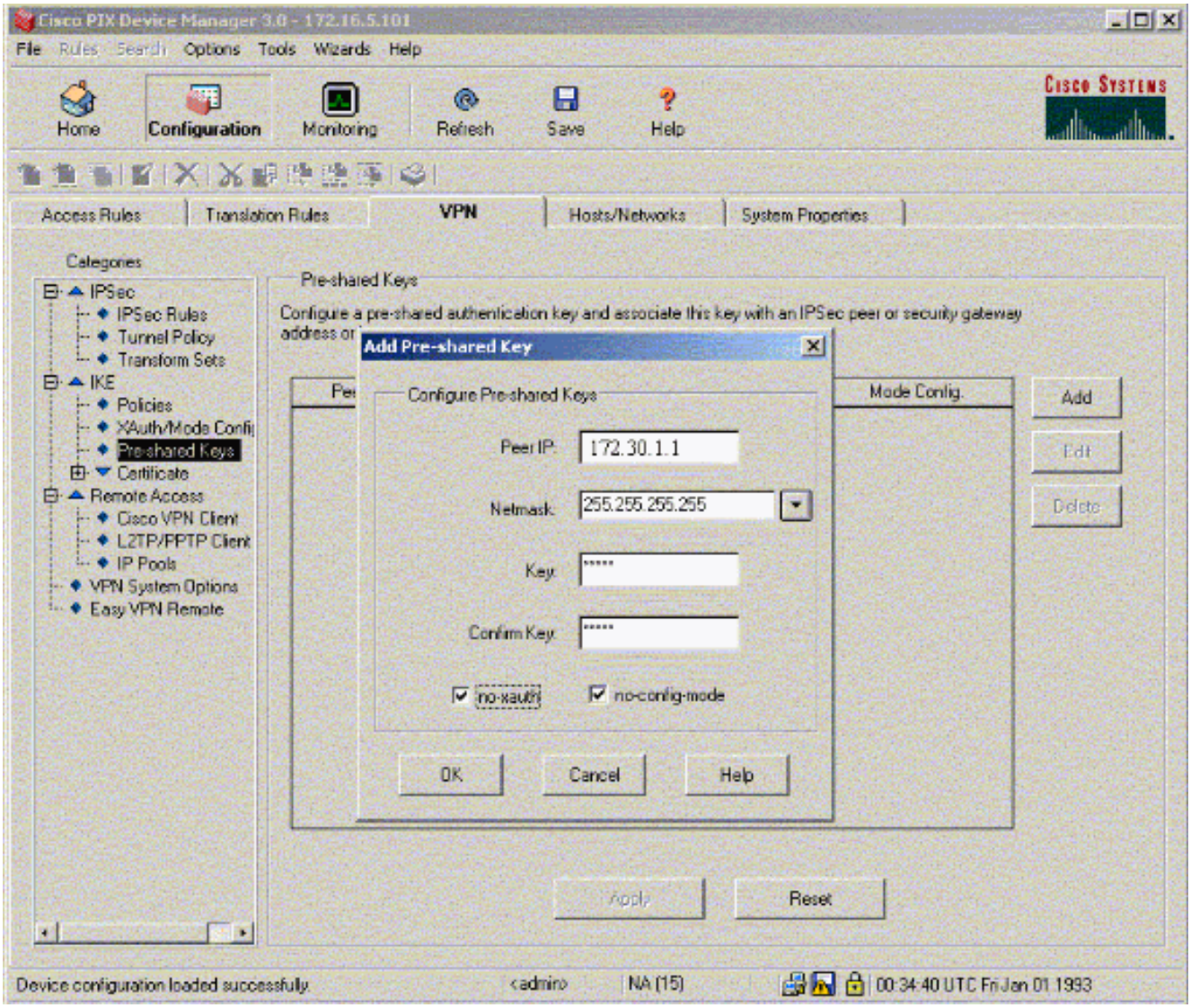
4. 按一下**Add**，選擇所有適當的選項，然後按一下**OK**以建立新的轉換集。



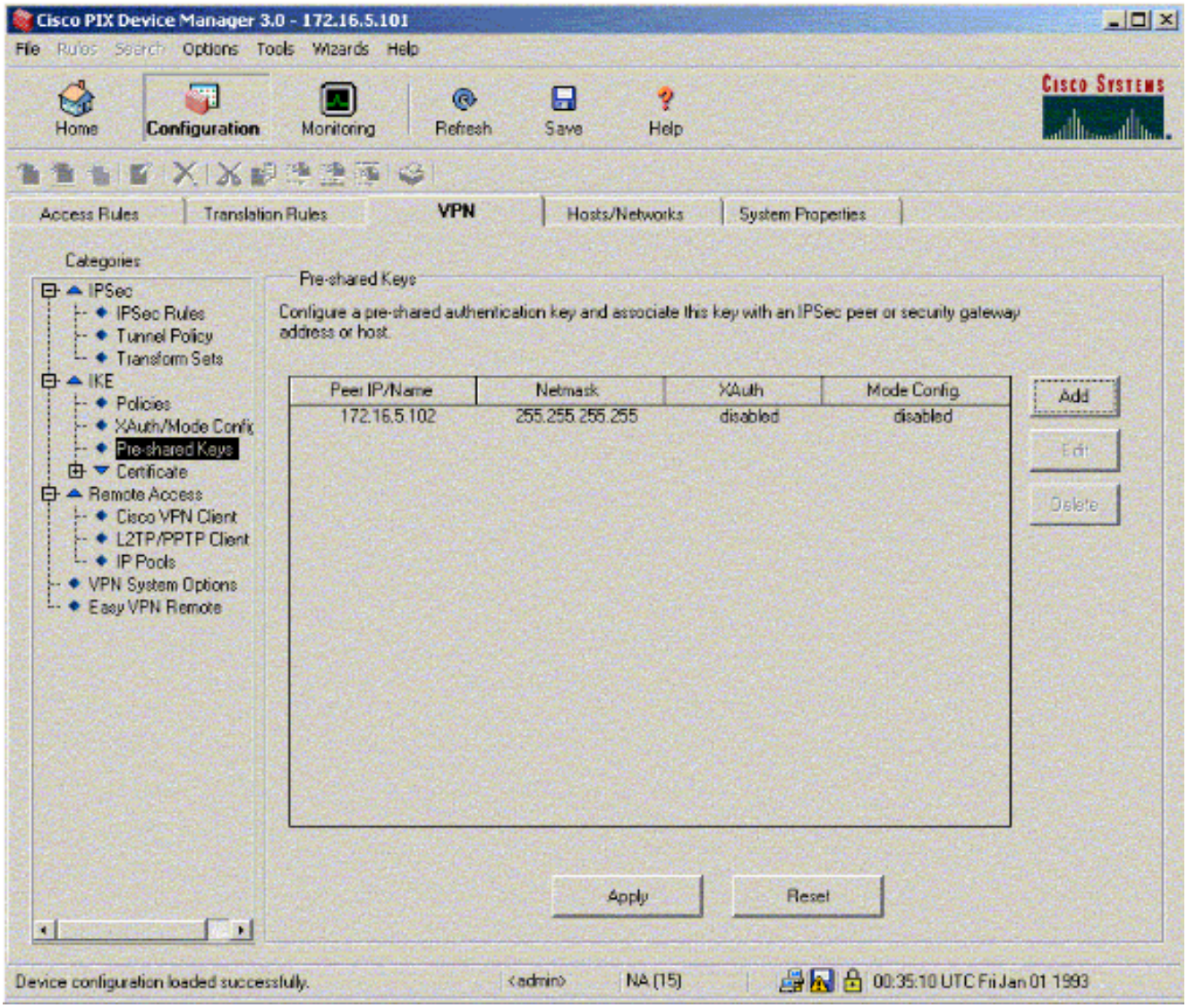
5. 按一下IKE下的**Pre-Shared Keys**以配置預共用金鑰。



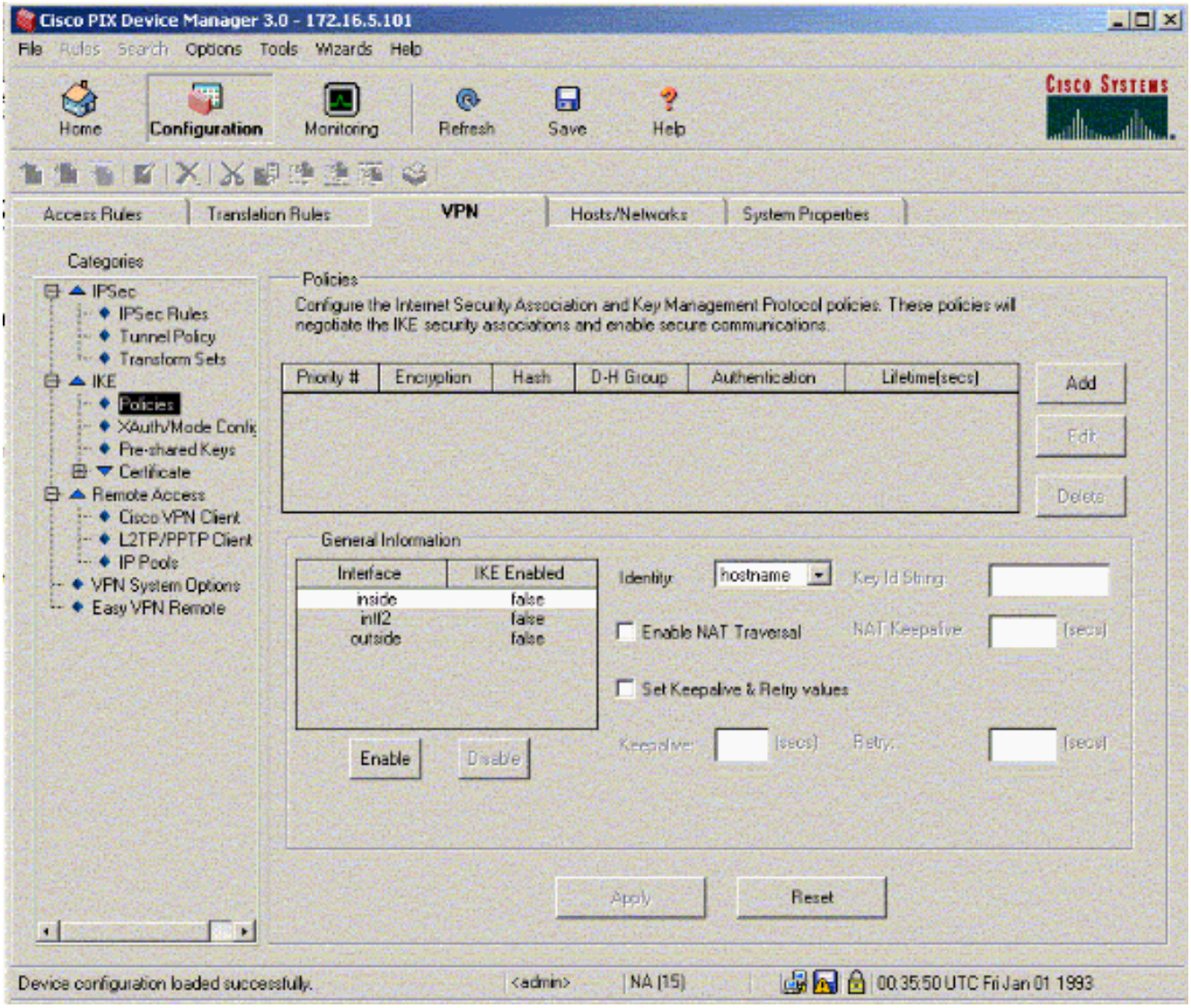
6. 按一下Add以新增新的預共用金鑰。



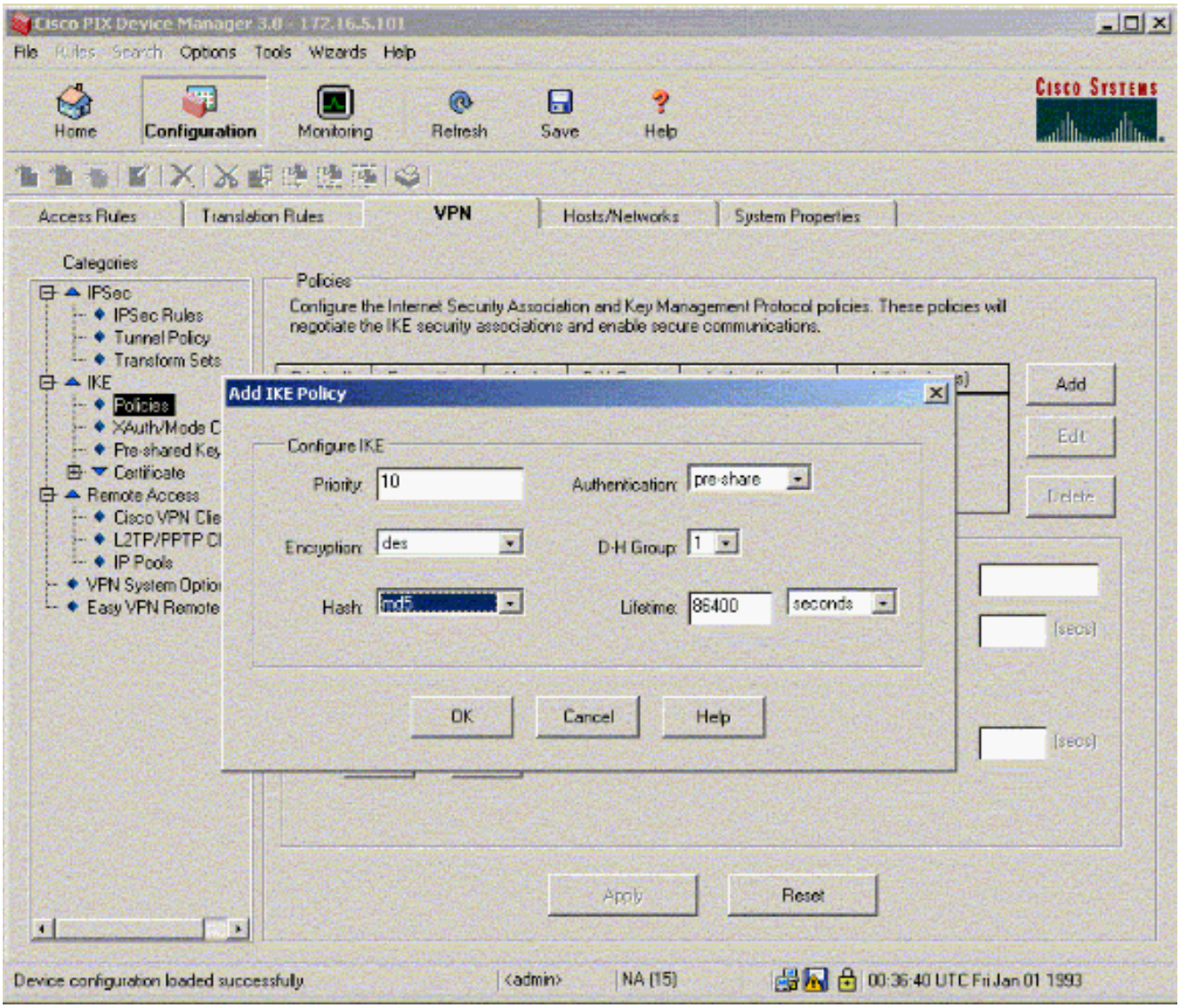
此視窗顯示金鑰，即隧道關聯的密碼。此值必須在通道的兩端相符。



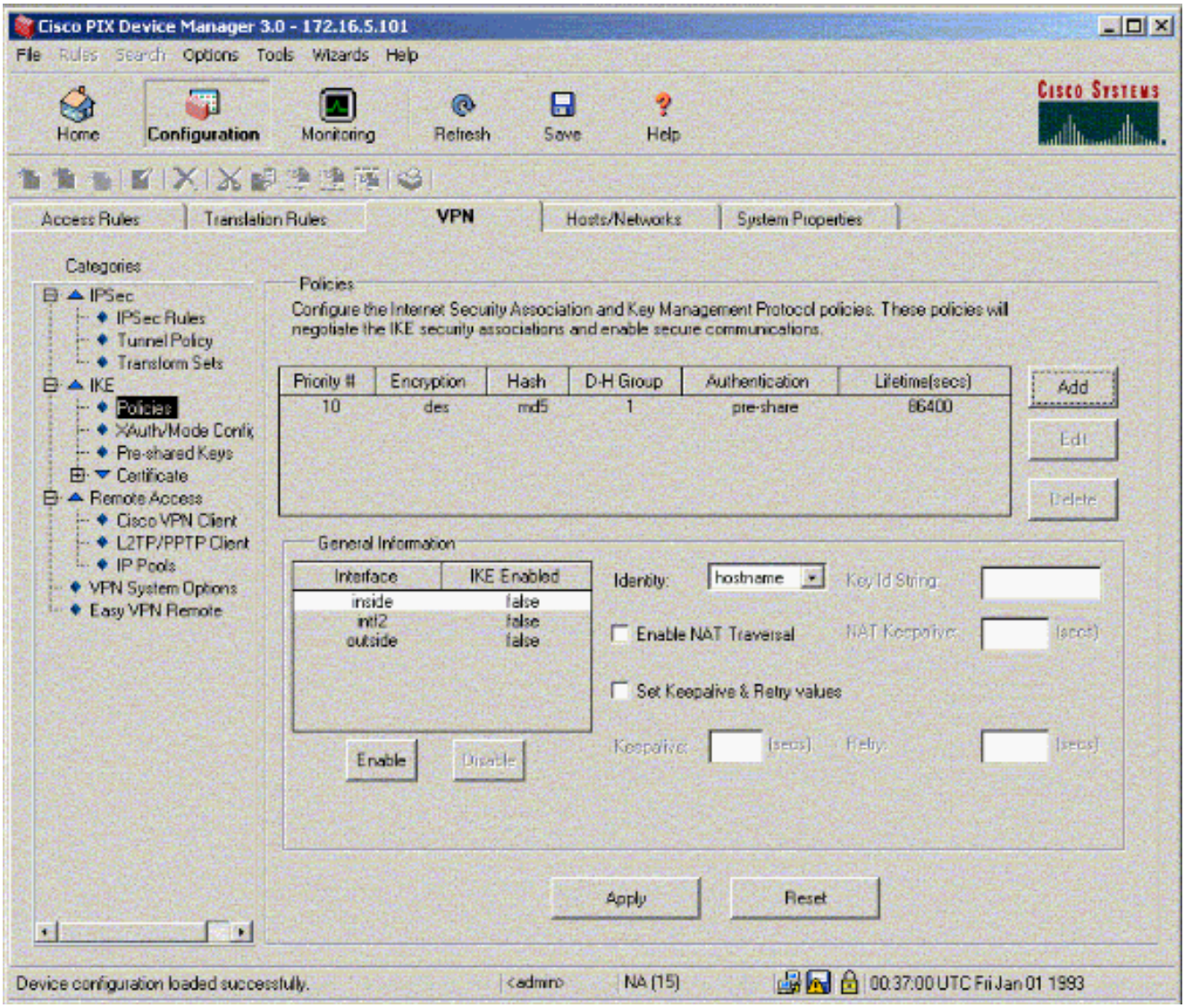
7. 按一下IKE下的**Policies**配置策略。



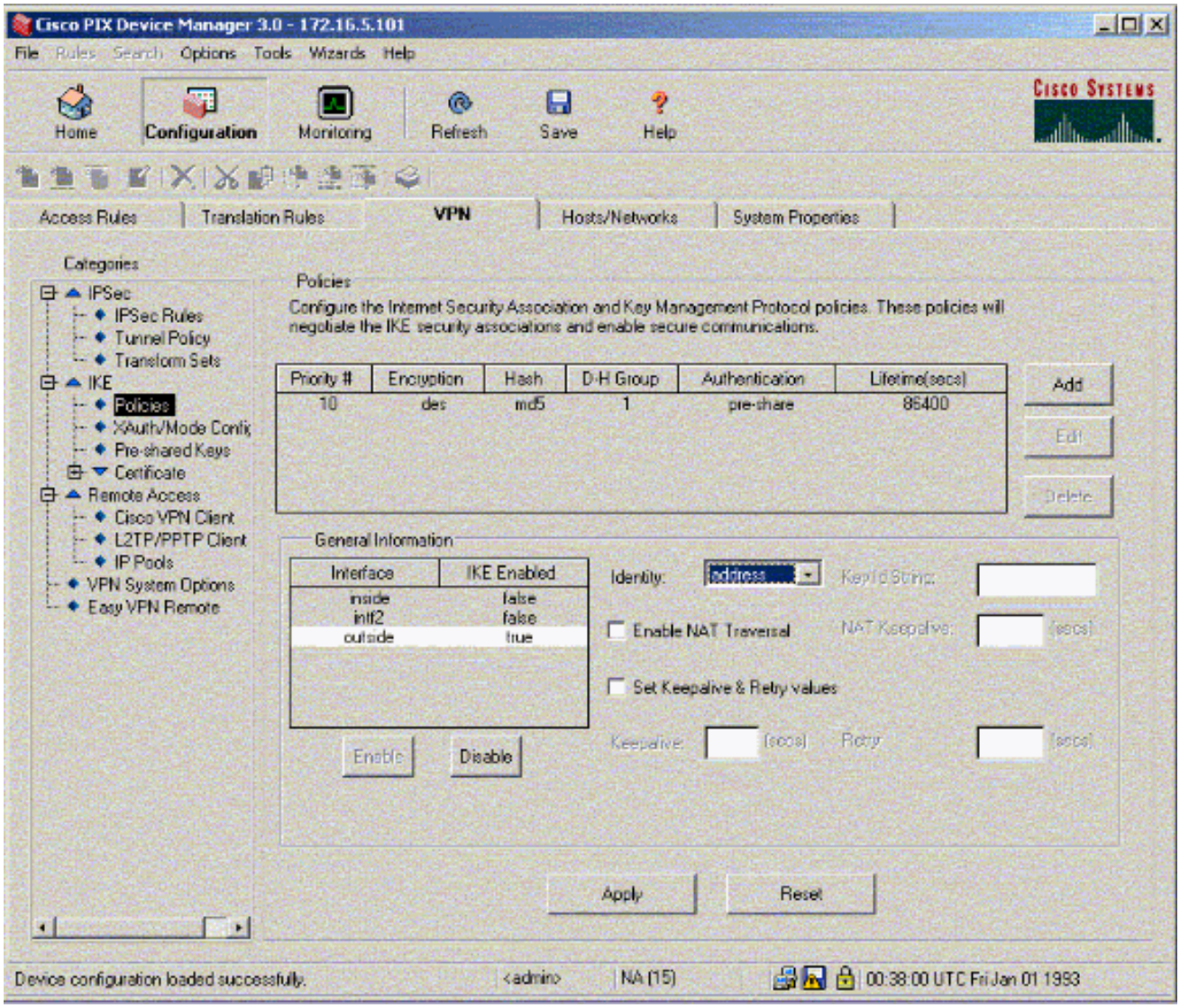
8. 按一下「**Add**」，然後填寫相應的欄位。



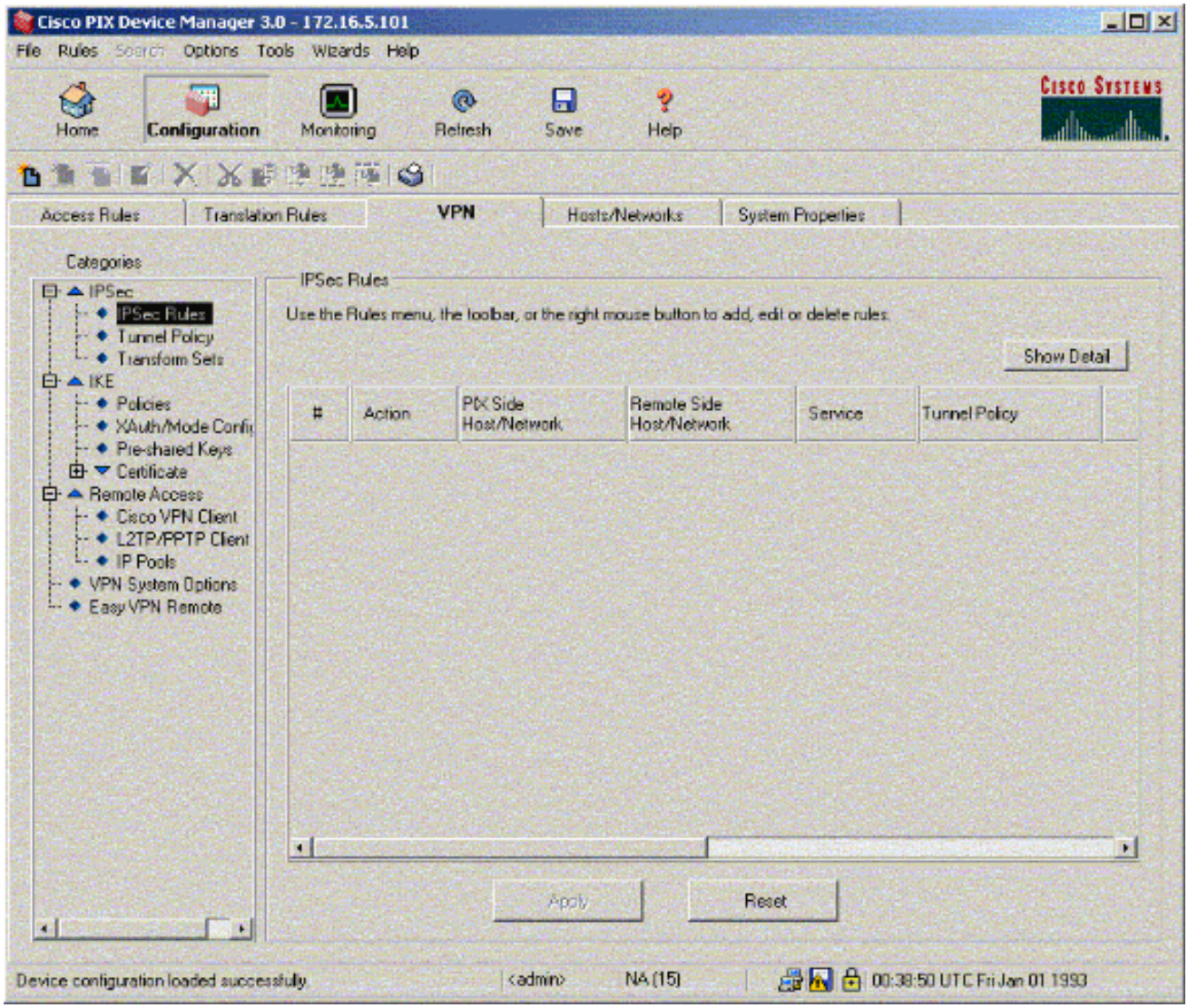
9. 按一下**OK**新增新策略。



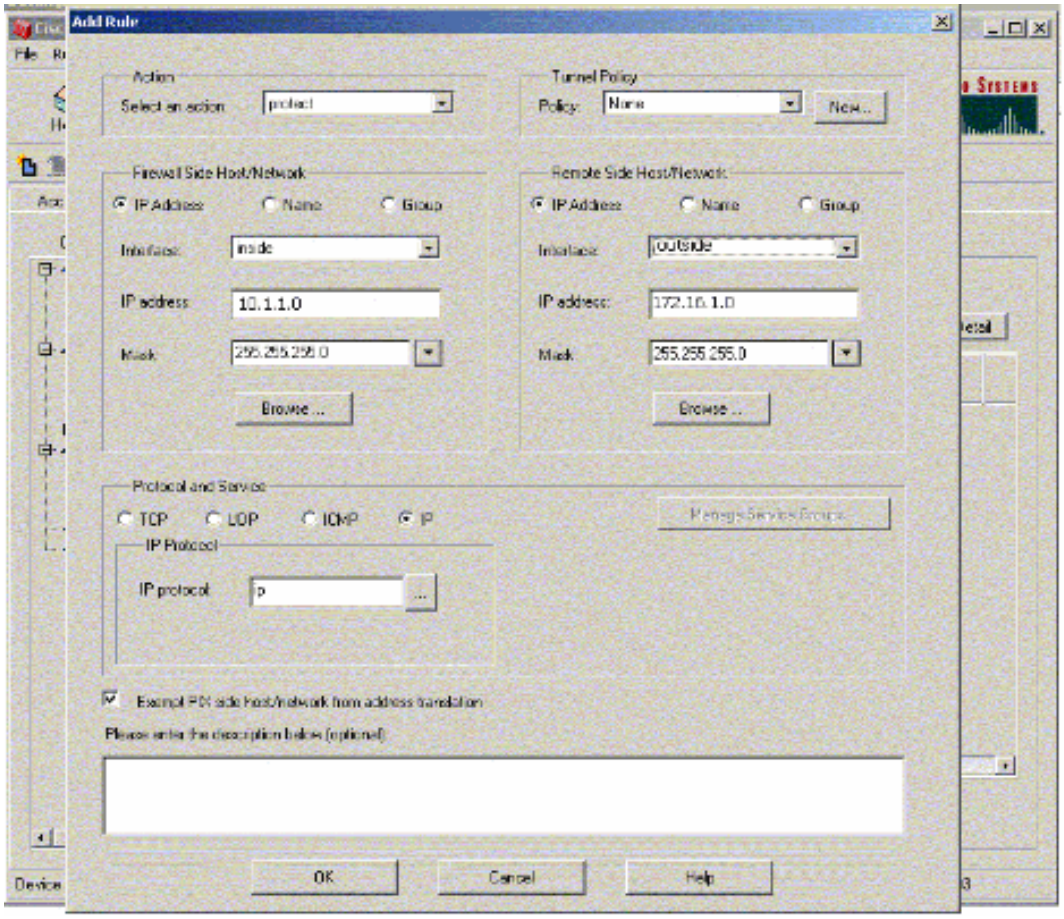
10. 選擇**outside**介面，按一下**Enable**，然後從Identity下拉選單中選擇**address**。



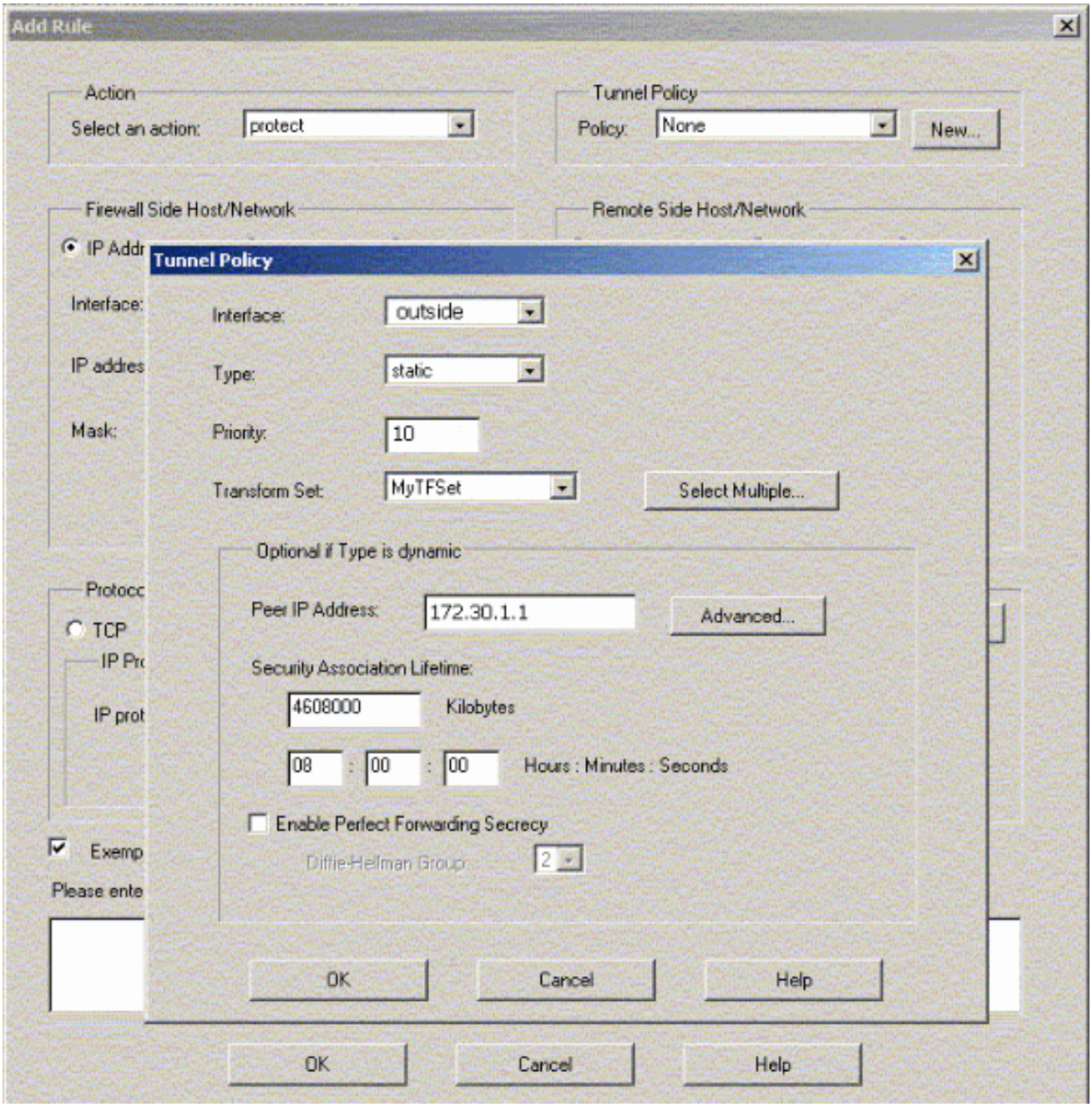
11. 按一下IPSec下的**IPSec Rules**以建立IPsec規則。


Cisco PIX Device Manager 3.0 - 172.16.5.101
File Rules Search Options Tools Wizards Help
Home
Configuration
Monitoring
Refresh
Save
Help
Cisco Systems
Access Rules
Translation Rules
VPN
Hosts/Networks
System Properties
Categories
IPSec
IPSec Rules
Tunnel Policy
Transform Sets
IKE
Policies
XAuth/Mode Config
Pre-shared Keys
Certificate
Remote Access
Cisco VPN Client
L2TP/PPTP Client
IP Pools
VPN System Options
Easy VPN Remote
IPSec Rules
Use the Rules menu, the toolbar, or the right mouse button to add, edit or delete rules.
Show Detail
#
Action
PIX Side Host/Network
Remote Side Host/Network
Service
Tunnel Policy
Apply
Reset
Device configuration loaded successfully.
<admin>
NA (15)
00:38:50 UTC Fri Jan 01 1993

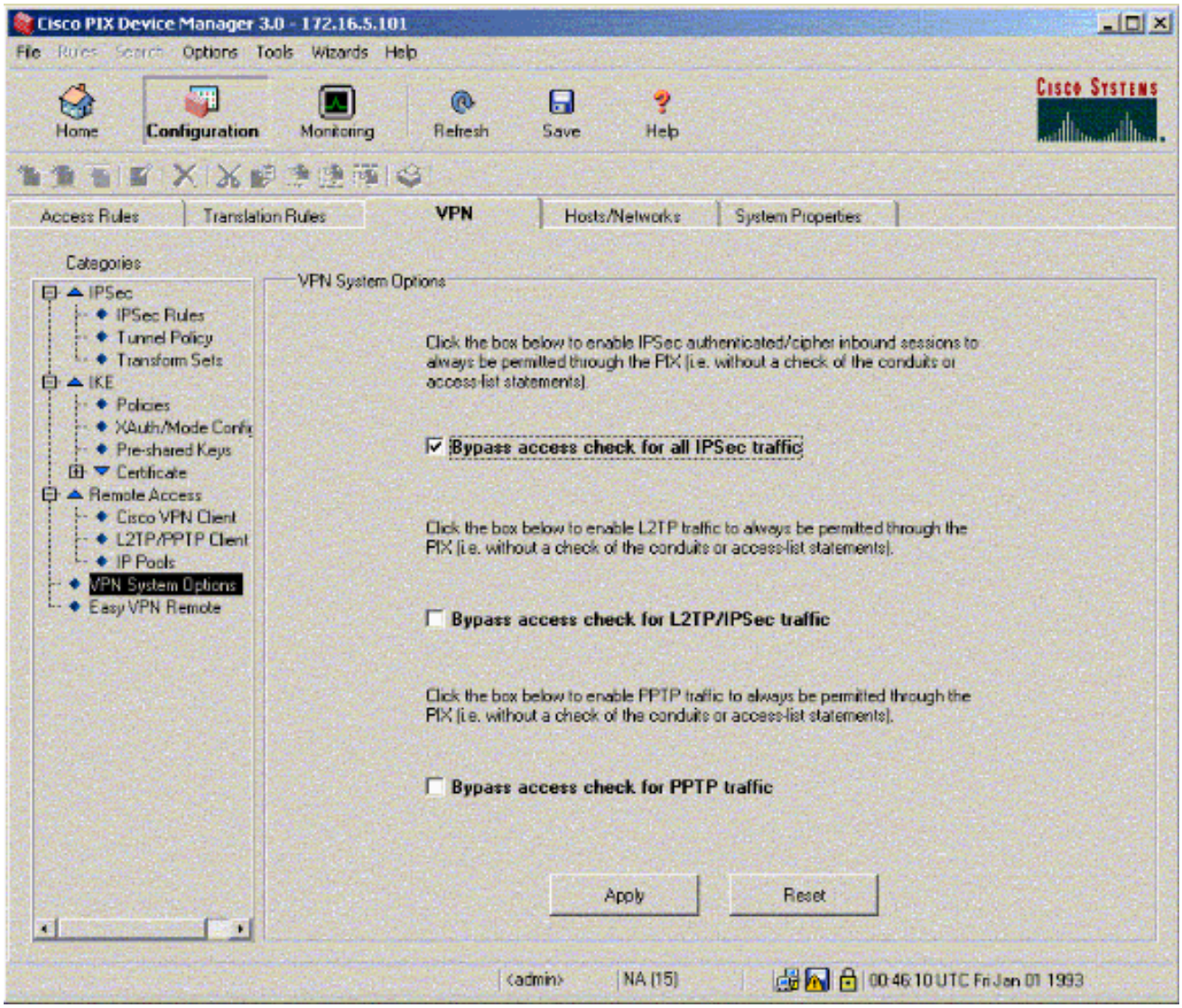
12. 填寫相應欄位。



13. 在Tunnel Policy中按一下**New**。出現「Tunnel Policy（隧道策略）」視窗。填寫相應欄位。



14. 按一下**OK**檢視配置的IPsec規則。
15. 按一下**VPN Systems Options**，然後選中**Bypass access check for all IPSec traffic**。

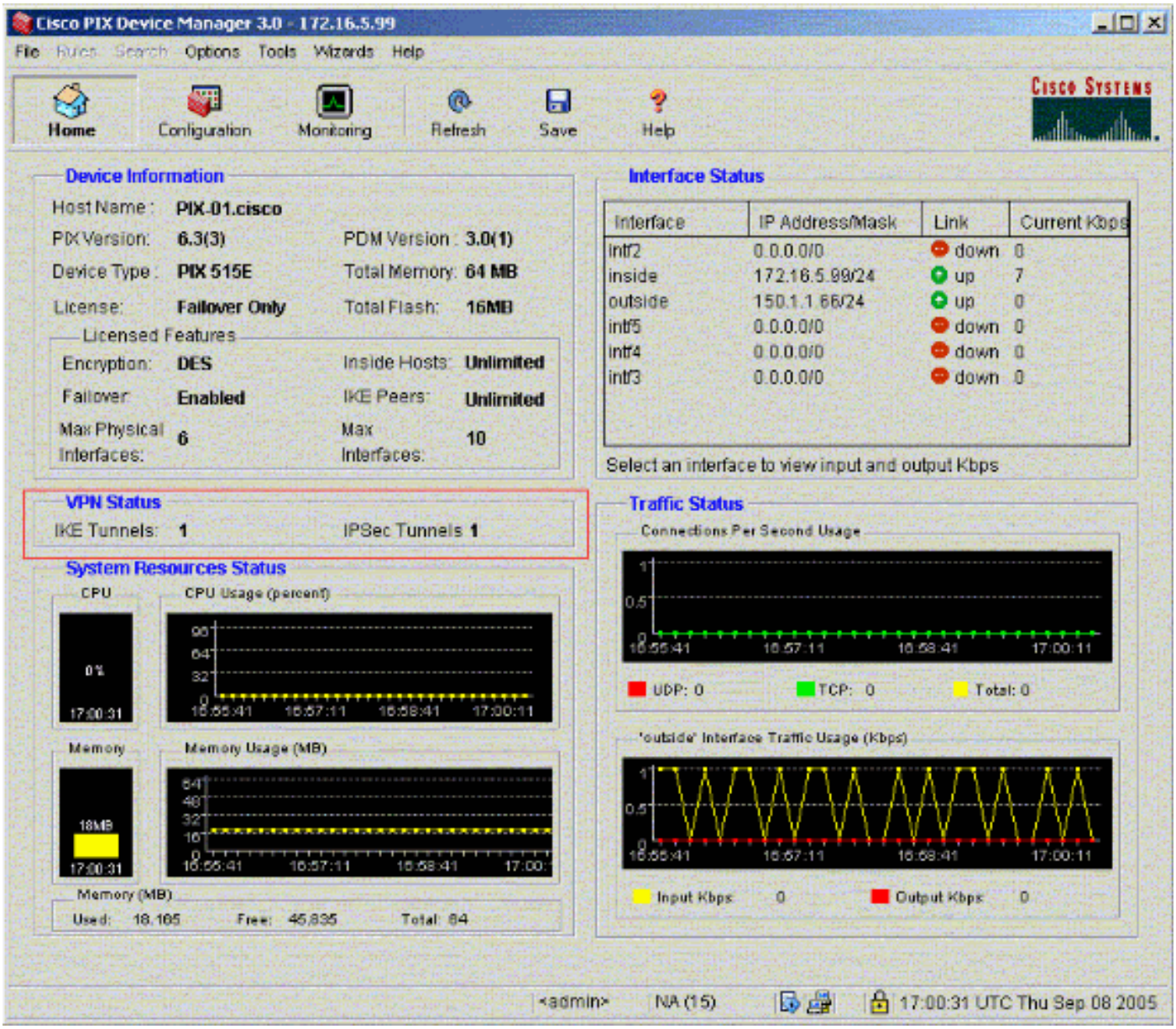


驗證

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。

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。

檢視PDM中Home下的VPN Status（以紅色突出顯示），以驗證隧道的形成。



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。

注意：除非在全域性配置模式下配置了[management-access](#)命令，否則無法ping通PIX的內部介面以形成隧道。

```
PIX-02(config)#management-access inside
PIX-02(config)#show management-access
management-access inside
```

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PDM在防火牆之間建立冗餘隧道]
- [Cisco Secure PIX防火牆命令參考]

- 要求建議 (RFC)
- Cisco PIX防火牆軟體