两个PIXes之间使用PDM的LAN到LAN VPN隧道配置示例

目录

简介

本文档介绍使用 Cisco PIX Device Manager (PDM) 在两个 PIX 防火墙之间配置 VPN 隧道的过程。PDM 是一种基于浏览器的配置工具，专用于帮助您通过 GUI 来设置、配置并监控 PIX 防火墙。PIX 防火墙放置在两个不同的站点。

可以使用 IPsec 形成隧道。IPsec 是在 IPsec 对等体之间提供数据机密性、数据完整性和数据原始身份验证的开放标准组合。

先决条件

要求

本文档没有任何要求。

使用的组件

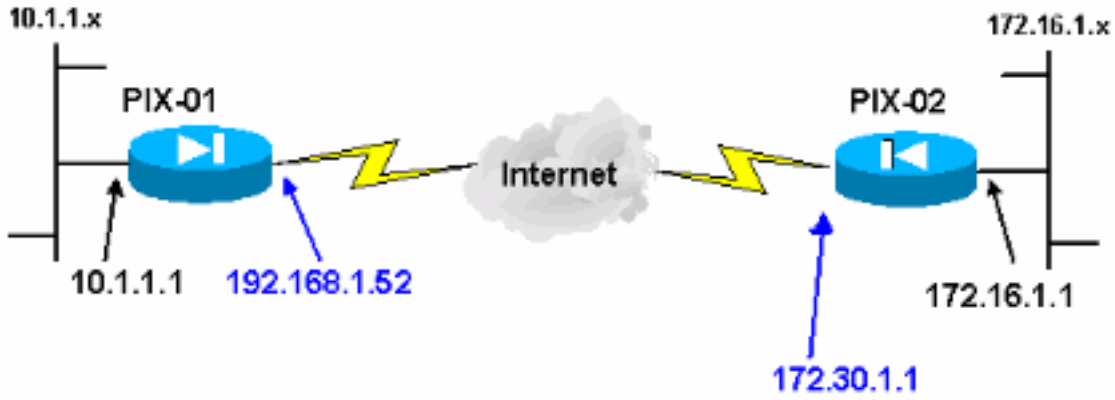
本文档中的信息基于具有 6.x 和 PDM 版本 3.0 的 Cisco Secure PIX 515E 防火墙。

请参阅使用 IPSec 配置简单的 PIX 到 PIX VPN 隧道，获取有关使用命令行界面 (CLI) 在两个 PIX 设备之间配置 VPN 隧道的配置示例。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

网络图

本文档使用以下网络设置：



规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

IPsec 协商可分为五个步骤，并且包括两个 Internet 密钥交换 (IKE) 阶段。

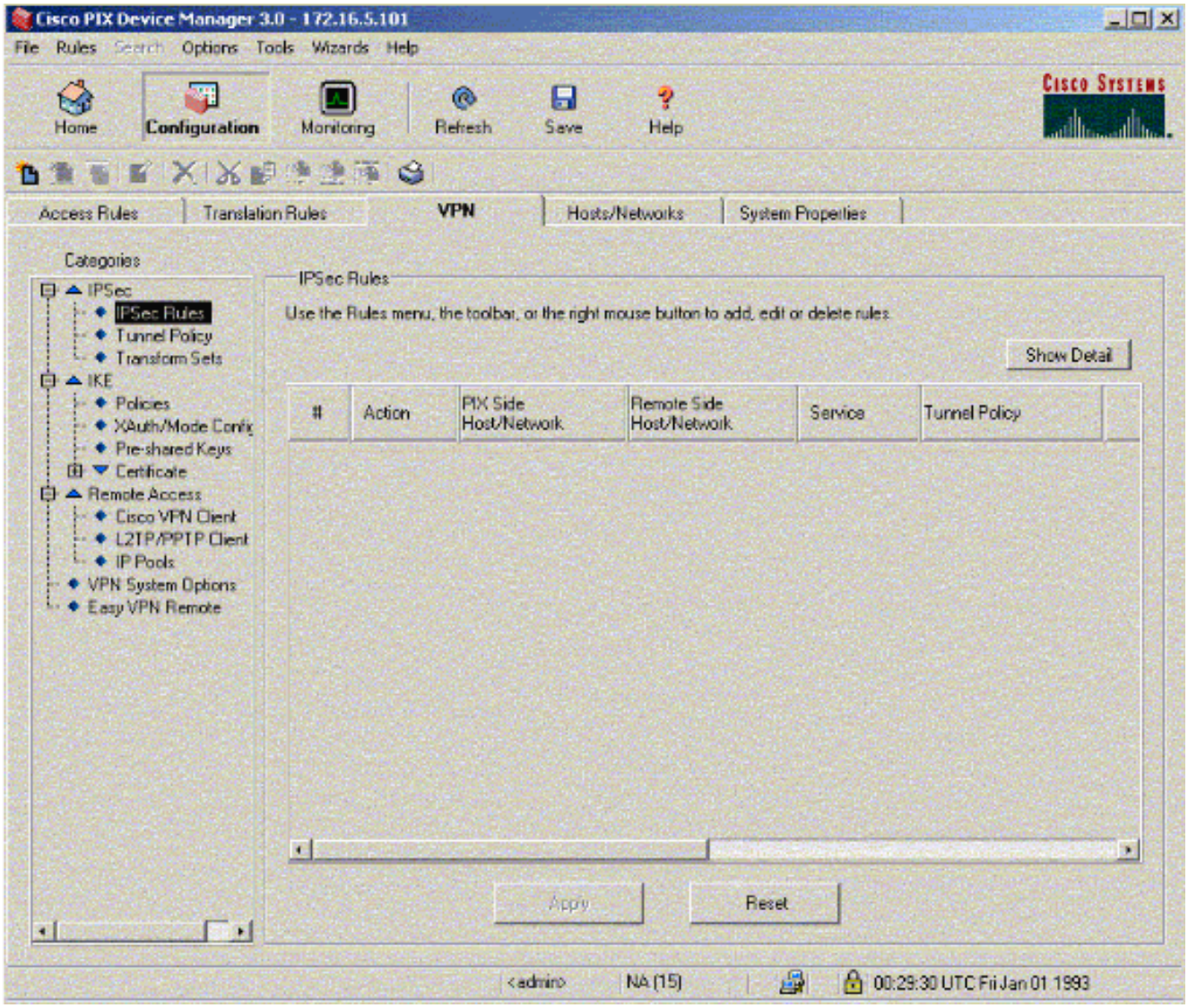
1. IPsec 隧道由相关数据流启动。如果数据流在 IPsec 对等体之间传输，则它会被认为是相关数据流。
2. 在 IKE 第 1 阶段中，IPsec 对等体对建立的 IKE 安全关联 (SA) 策略进行协商。对等体经过身份验证后，会使用 Internet 安全关联和密钥管理协议 (ISAKMP) 创建安全隧道。
3. 在 IKE 第 2 阶段中，IPsec 对等体使用经身份验证的安全隧道对 IPsec SA 转换进行协商。共享策略的协商决定建立 IPsec 隧道的方式。
4. 根据 IPsec 转换集中配置的 IPsec 参数，将在 IPsec 对等体之间创建 IPsec 隧道并传输数据。
5. 如果删除了 IPsec SA，或者 IPsec SA 的生存时间到期，则 IPsec 隧道将终止。**注意：**如果两个IKE阶段上的SA在对等体上不匹配，则两个PIX之间的IPsec协商失败。

配置过程

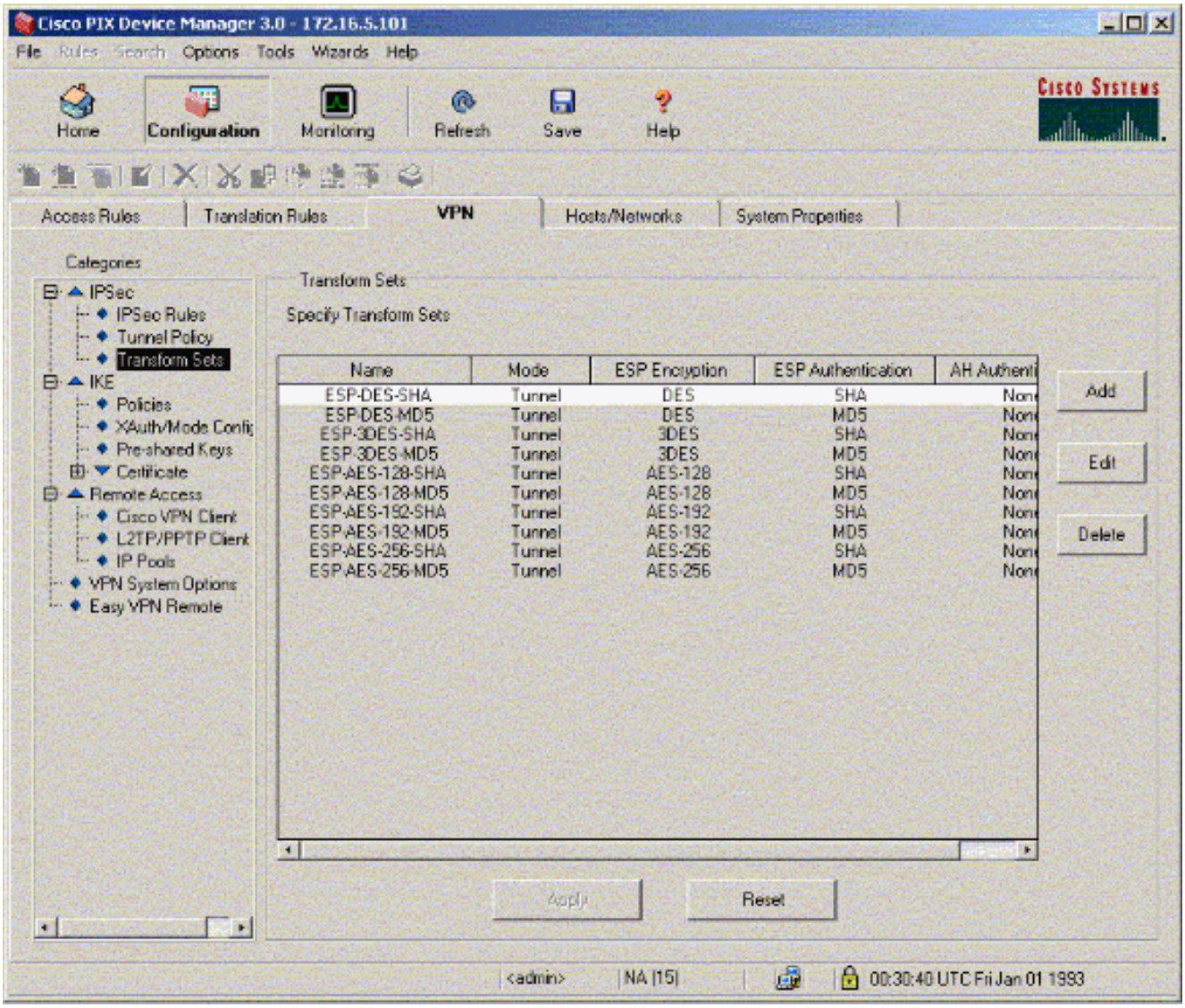
除通过以太网 0 接口访问的 PIX 的 CLI 其他一般配置外，使用命令 http server enable 和 **http server <local_ip> <mask> <interface>，其中 <local_ip> 和 <mask> 是 IP 地址以及安装 PDM 的工作站的掩码。**本文档中的配置针对PIX-01。PIX-02可以使用不同地址的相同步骤进行配置。

请完成以下步骤：

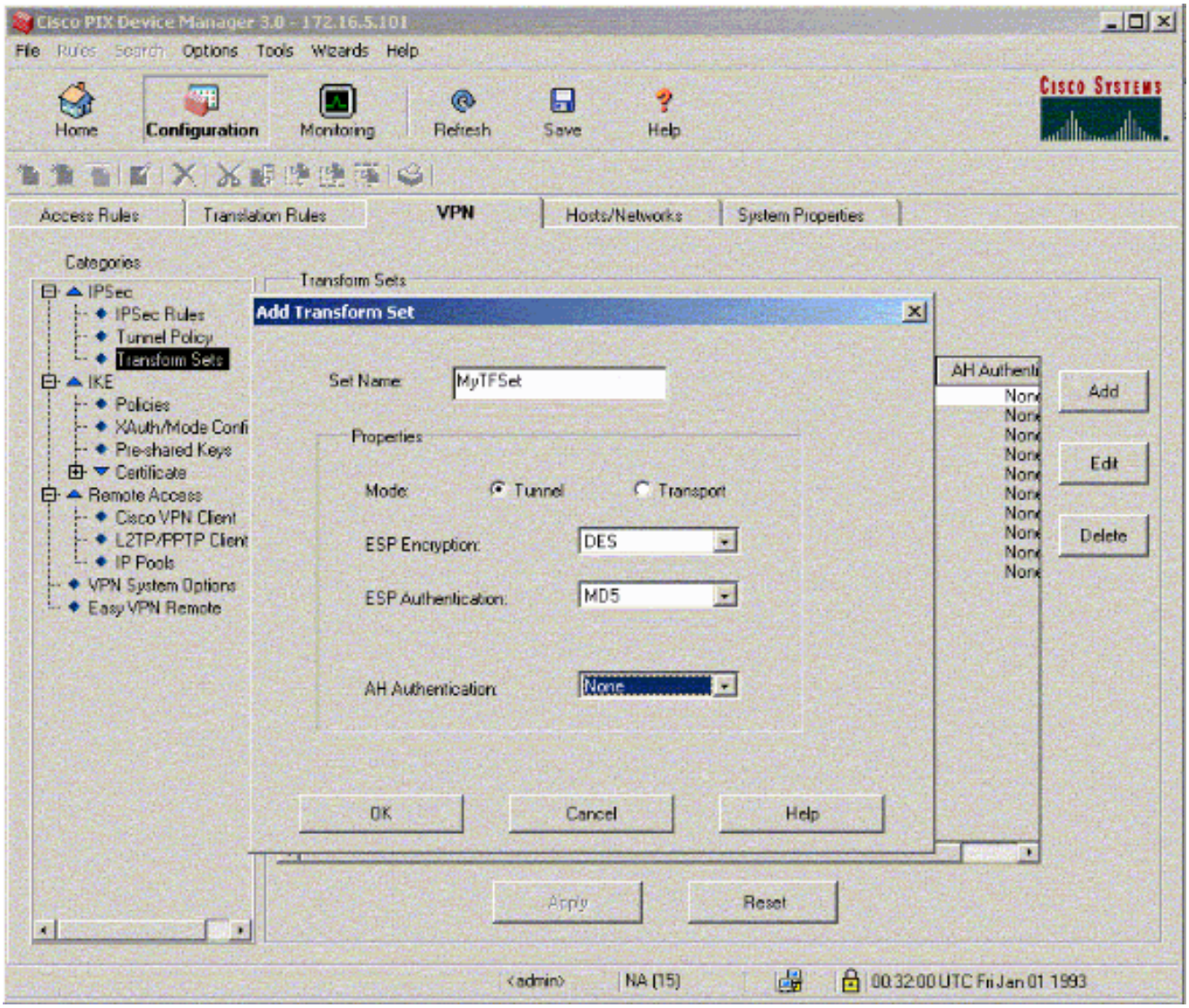
1. 打开浏览器并键入 **https:// <Inside_IP_Address_of_PIX>** 以访问 PDM 中的 PIX。
2. 单击 **Configuration，然后转至 VPN 选项卡。**



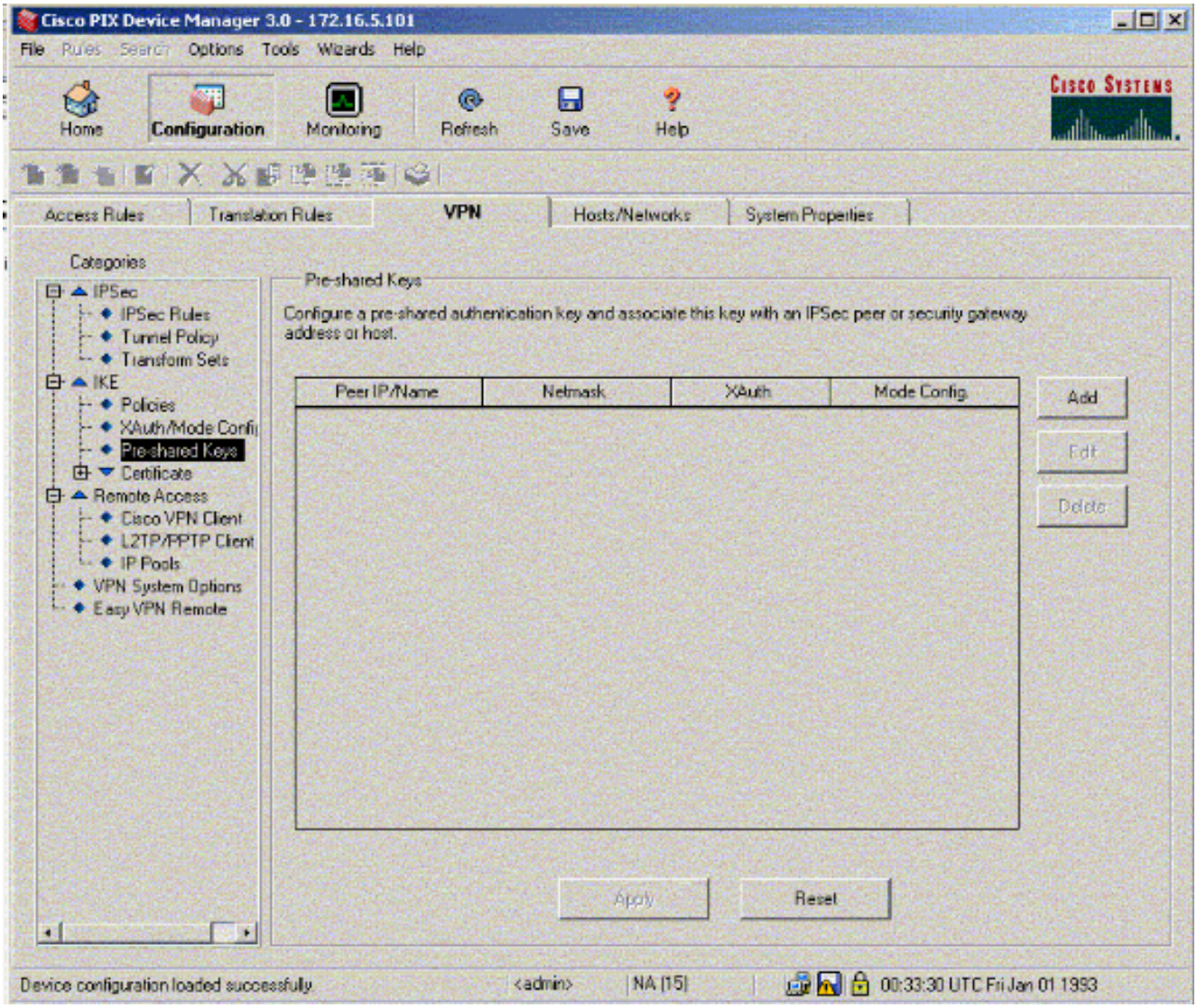
3. 单击 IPSec 下的 **Transform Sets 以创建转换集。**



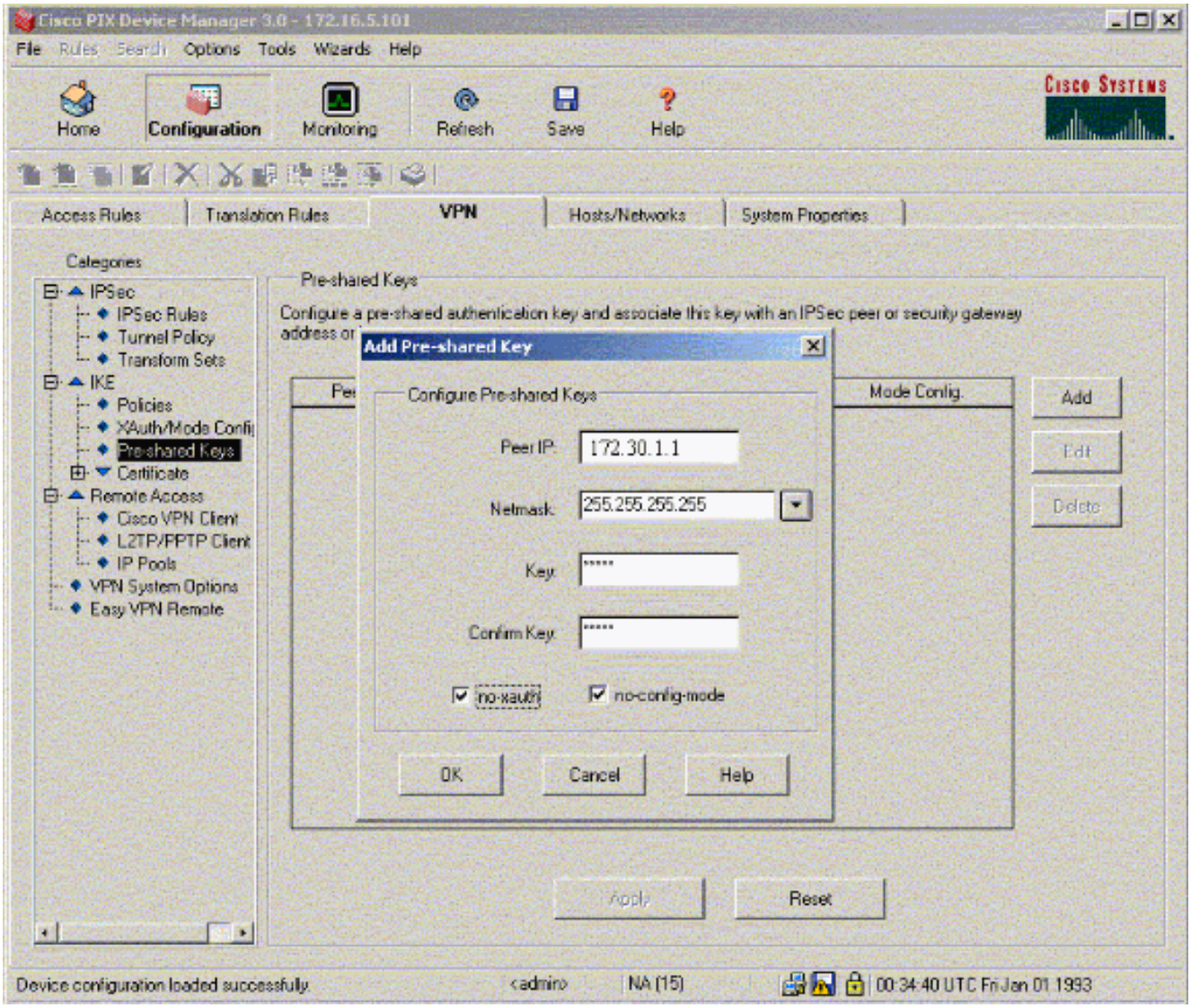
4. 单击 **Add**，选择所有适用选项，然后单击 **OK 创建新的转换集。**



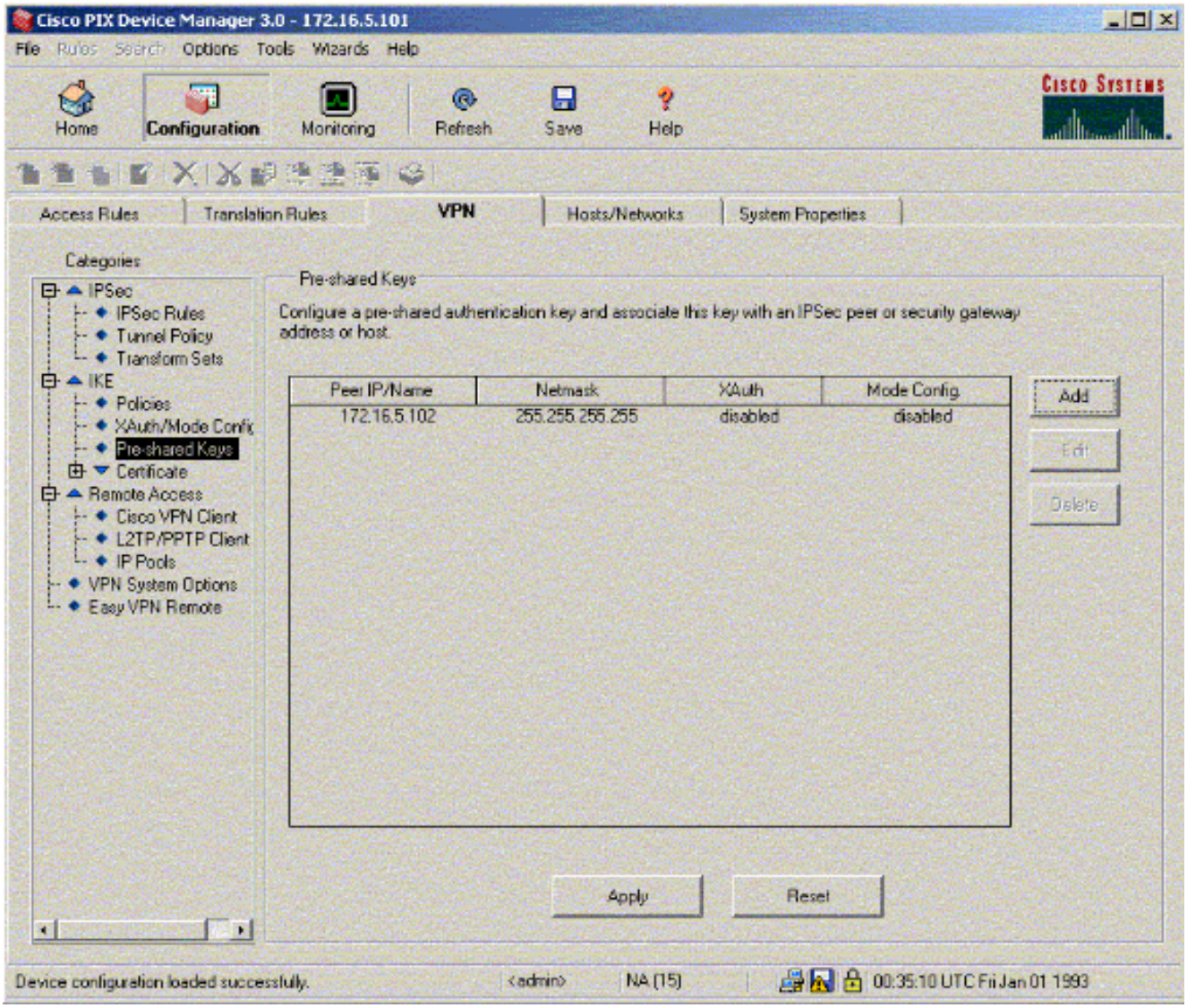
5. 单击 IKE 下的 **Pre-Shared Keys 以配置预共享密钥。**



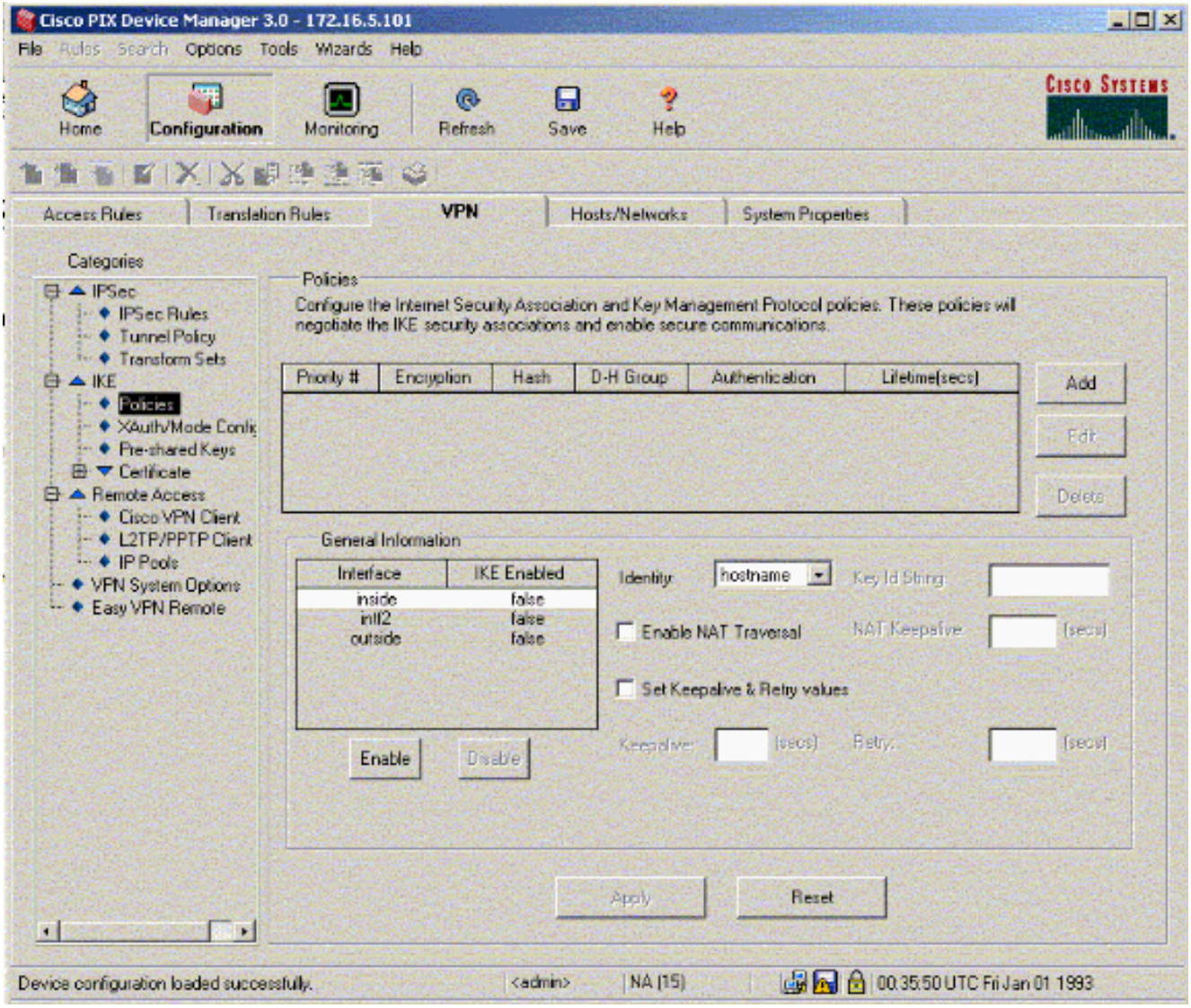
6. 单击 **Add** 以添加新的预共享密钥。



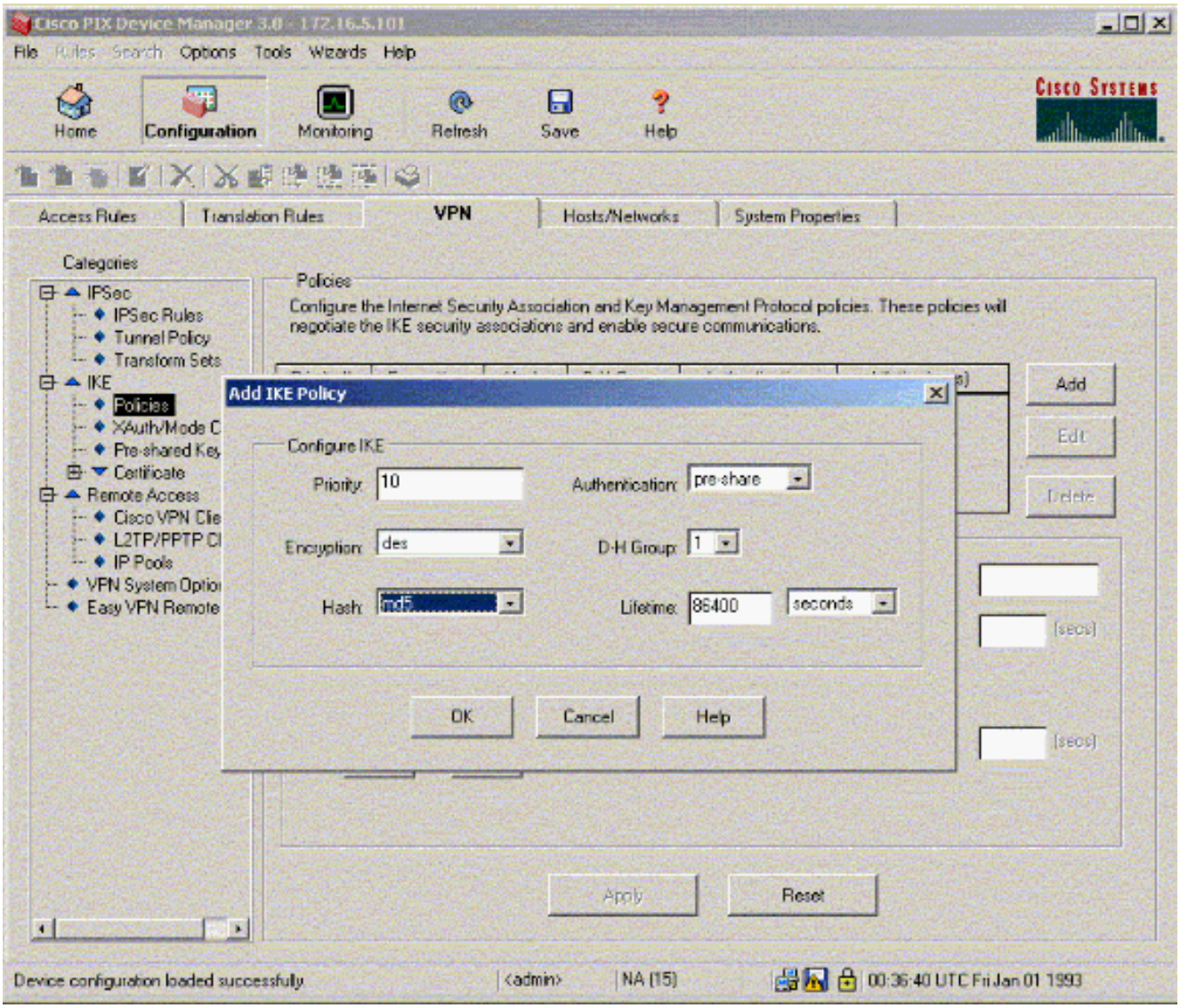
此窗口显示密钥，该密钥是隧道关联的口令。它在隧道的两端必须匹配。



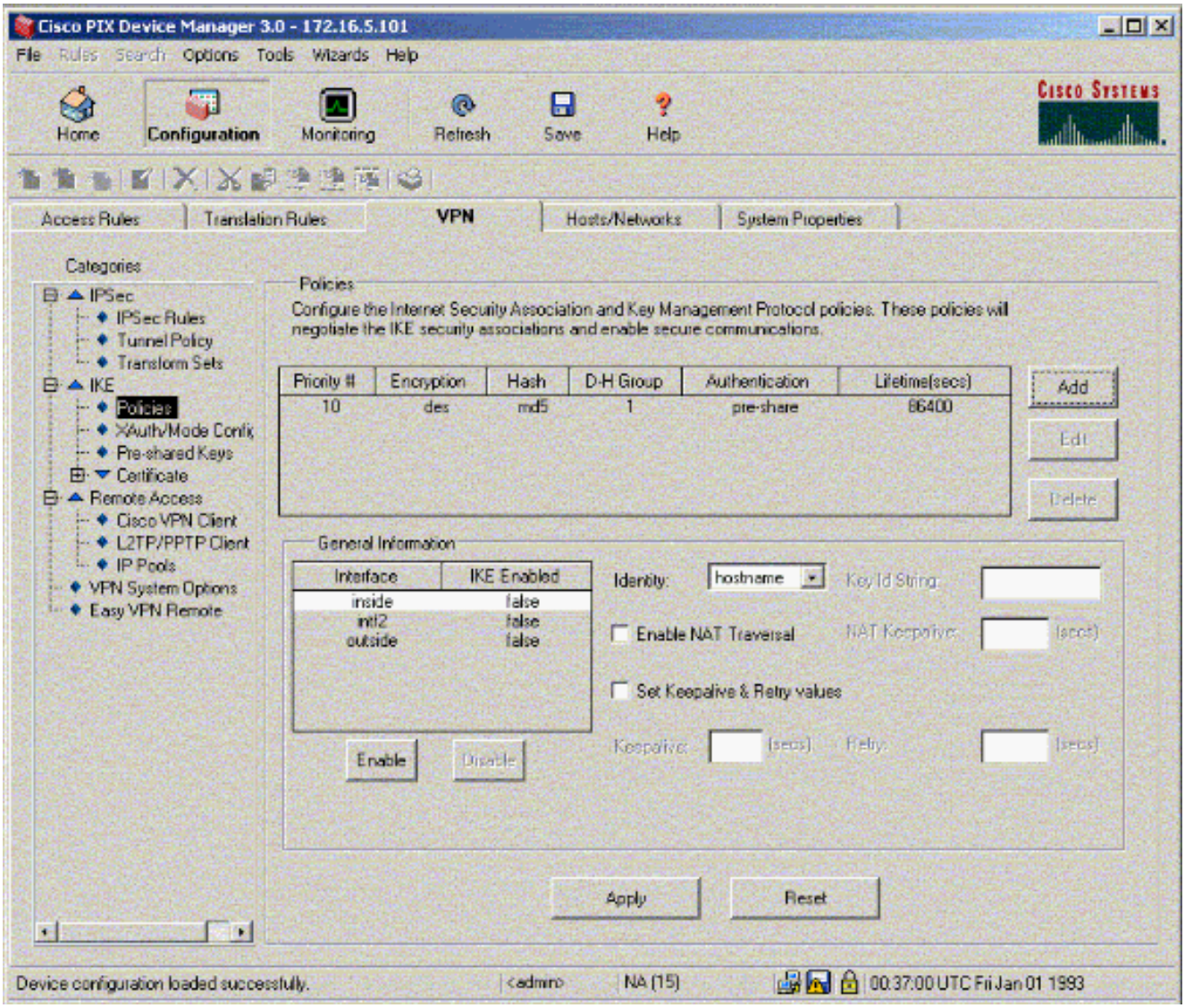
7. 单击 IKE 下的 **Policies 以配置策略。**



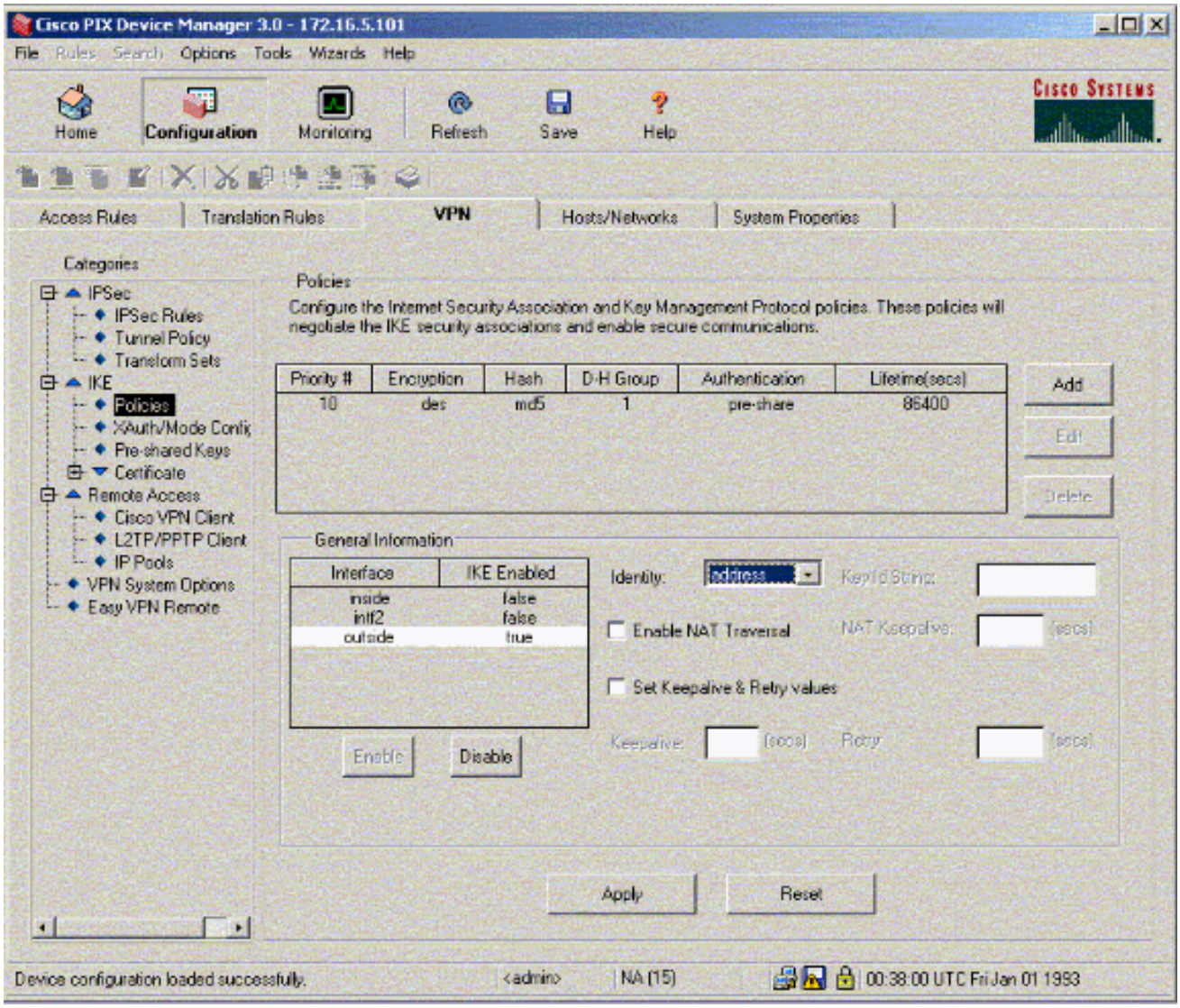
8. 单击 **Add** 并填写适当的字段。



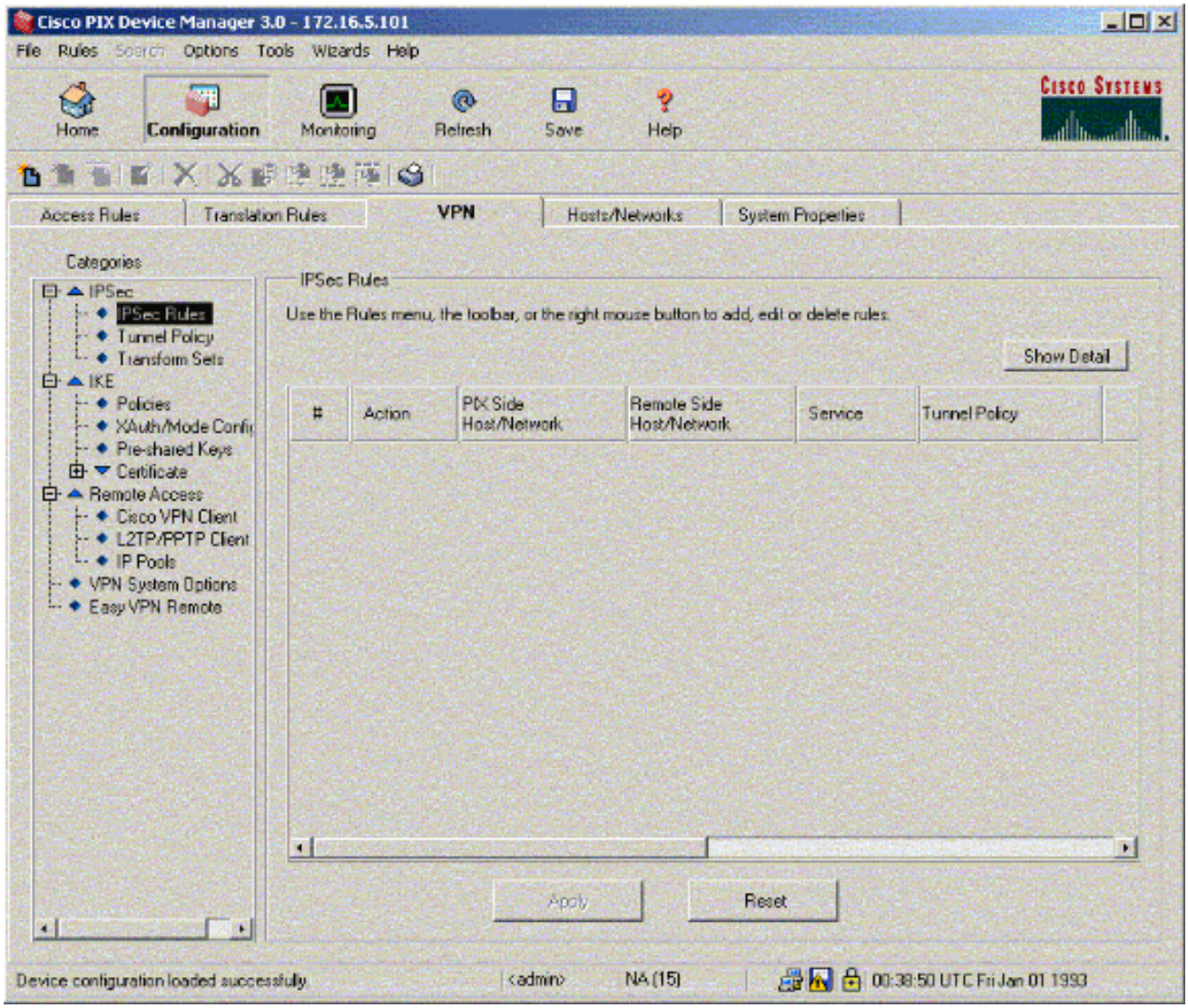
9. 单击 **OK 以添加新策略。**



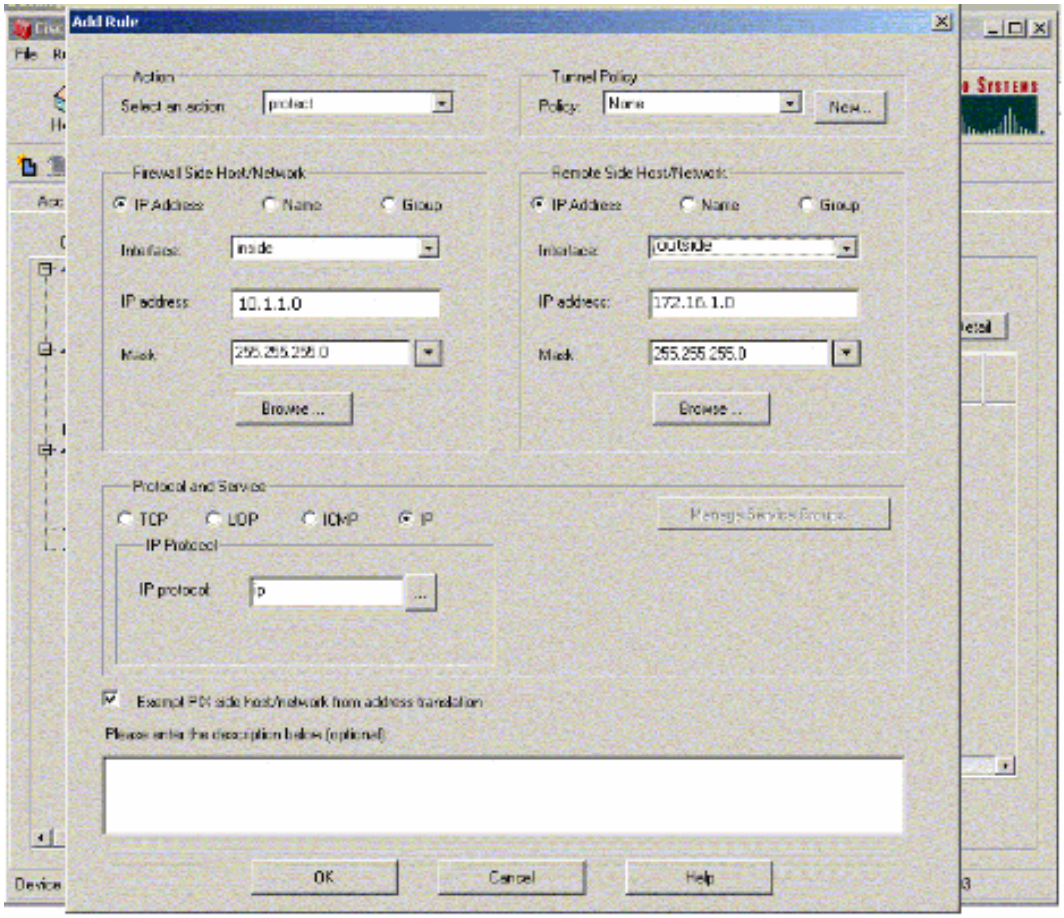
10. 选择 **outside interface，单击 Enable**，然后从 Identity 下拉菜单中选择 **address**。



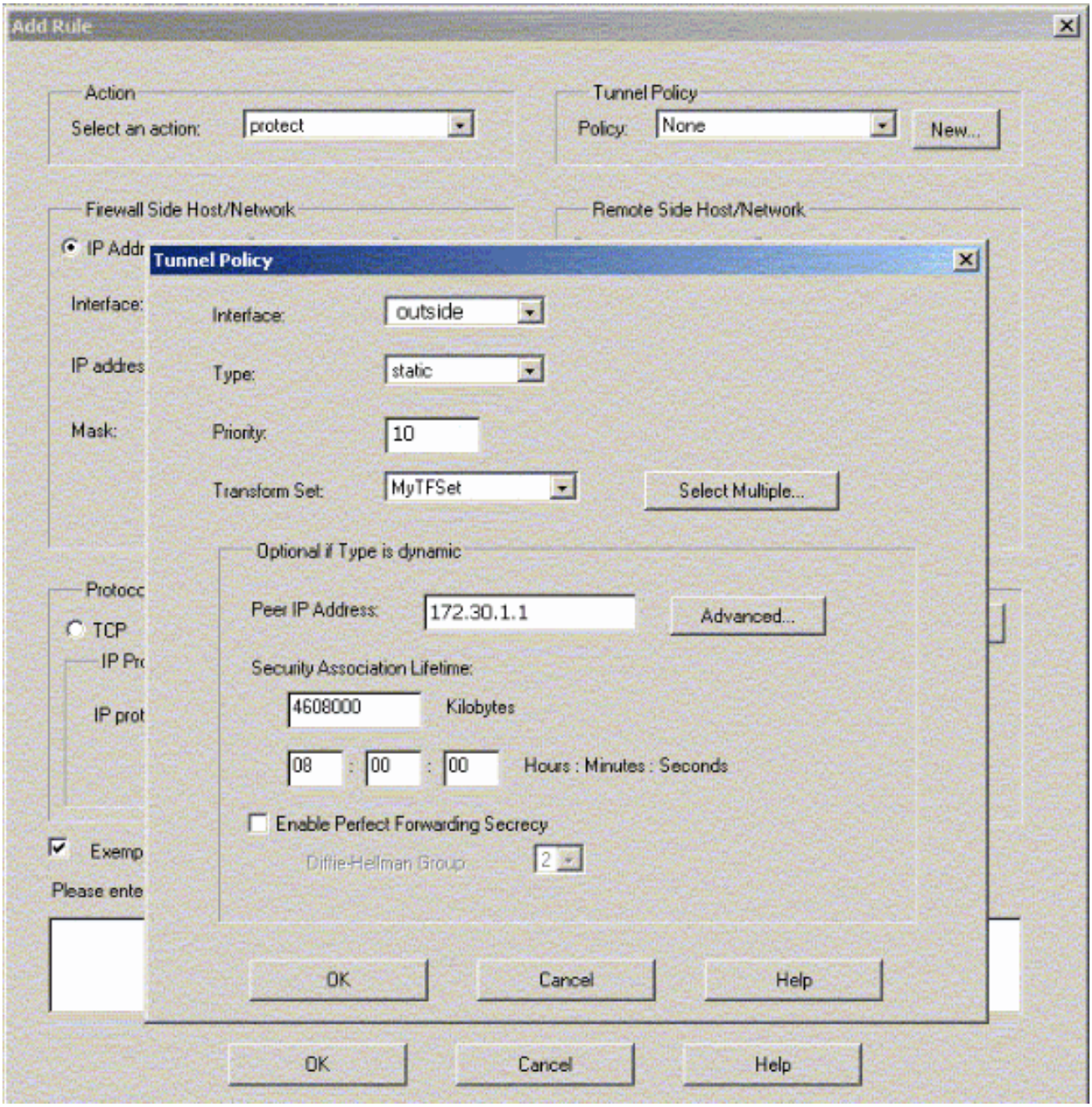
11. 单击 IPSec 下的 **IPSec Rules 以创建 IPsec 规则。**


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

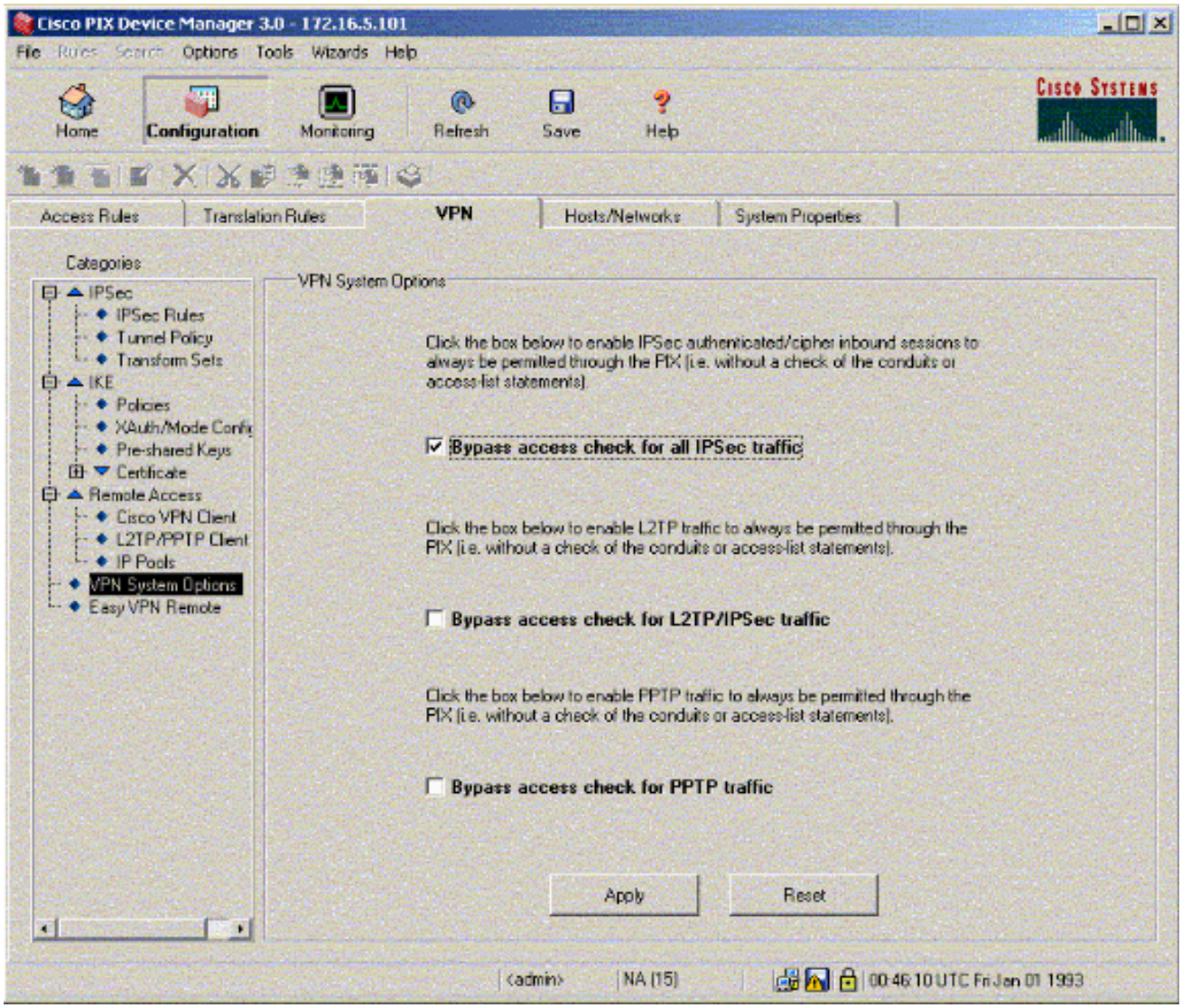
12. 填写适当的字段。



13. 单击 Tunnel Policy 中的 **New。**将出现 Tunnel Policy 窗口。填写适当的字段。



14. 单击 OK 以查看配置的 IPsec 规则。
15. 单击 VPN Systems Options 并选中 Bypass access check for all IPSec traffic。

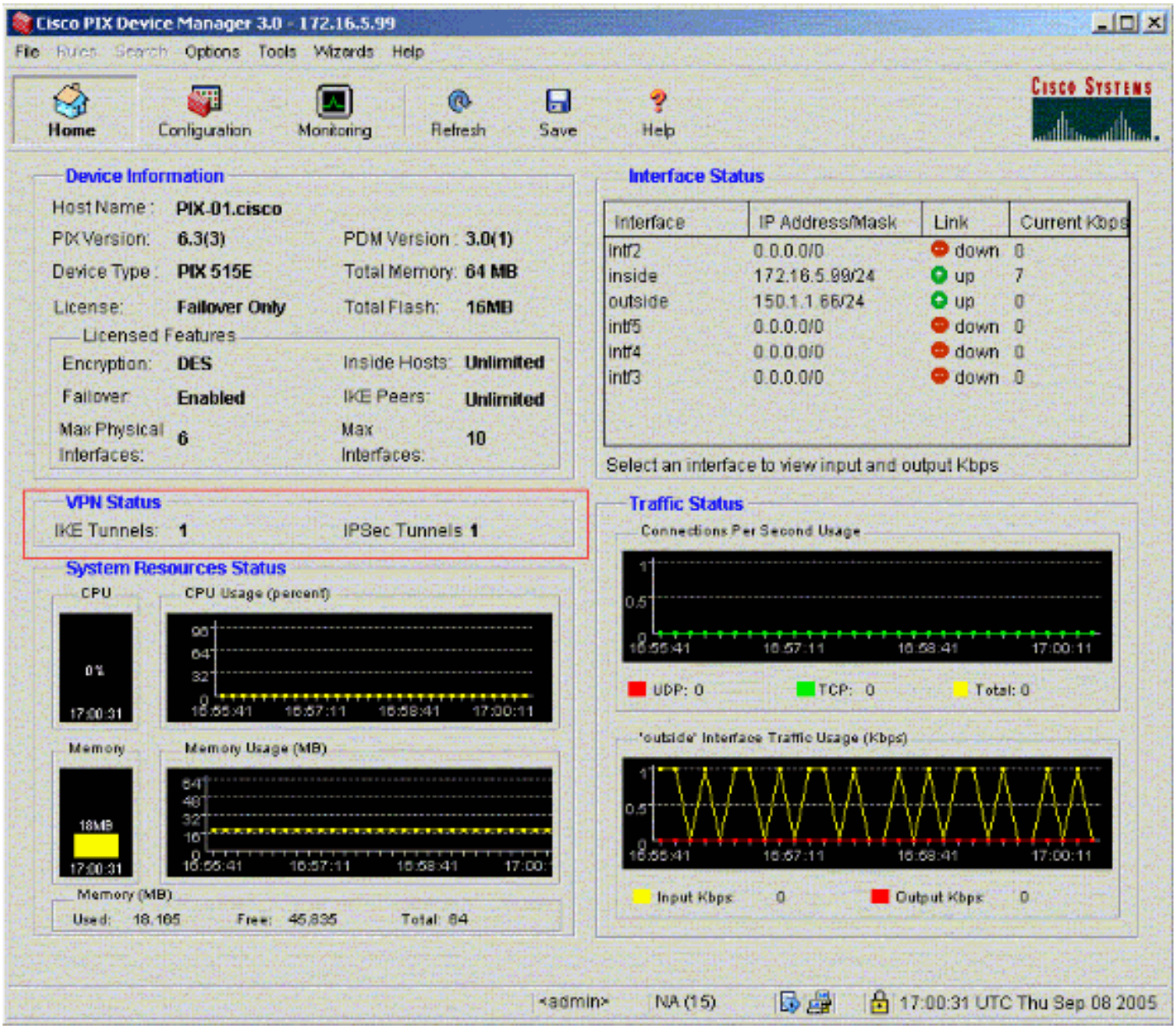


验证

如果有流向对等体的相关流量，则将在 PIX-01 和 PIX-02 之间建立隧道。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

在 PDM 中查看 Home 下的 VPN Status（以红色突出显示）以验证隧道是否已形成。



也可以使用 PDM 中 Tools 下的 CLI 来验证隧道是否已形成。发出 **show crypto isakmp sa 命令可检查隧道是否已形成，发出 show crypto ipsec sa 命令可观察已执行了封装、加密等操作的数据包的数量。**

注意：除非在全局配置模式下配置了management-access命令，否则无法对PIX的内[部接口](#)执行ping操作以形成隧道。

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

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- [在防火墙之间使用 PDM 创建冗余隧道]
- [Cisco Secure PIX 防火墙命令参考]

- 请求注解 (RFC)
- Cisco PIX 防火墙软件