LAN-to-LAN-VPN-Tunnel zwischen zwei PIXs unter Verwendung von PDM-Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird das Verfahren zur Konfiguration von VPN-Tunneln zwischen zwei PIX-Firewalls mithilfe des Cisco PIX Device Manager (PDM) beschrieben. PDM ist ein browserbasiertes Konfigurationstool, das Sie beim Einrichten, Konfigurieren und Überwachen Ihrer PIX-Firewall über eine grafische Benutzeroberfläche unterstützt. PIX-Firewalls werden an zwei verschiedenen Standorten platziert.

Ein Tunnel wird mithilfe von IPsec gebildet. IPsec ist eine Kombination offener Standards, die Datensicherheit, Datenintegrität und Datenursprungsauthentifizierung zwischen IPsec-Peers bieten.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine Anforderungen.

Verwendete Komponenten

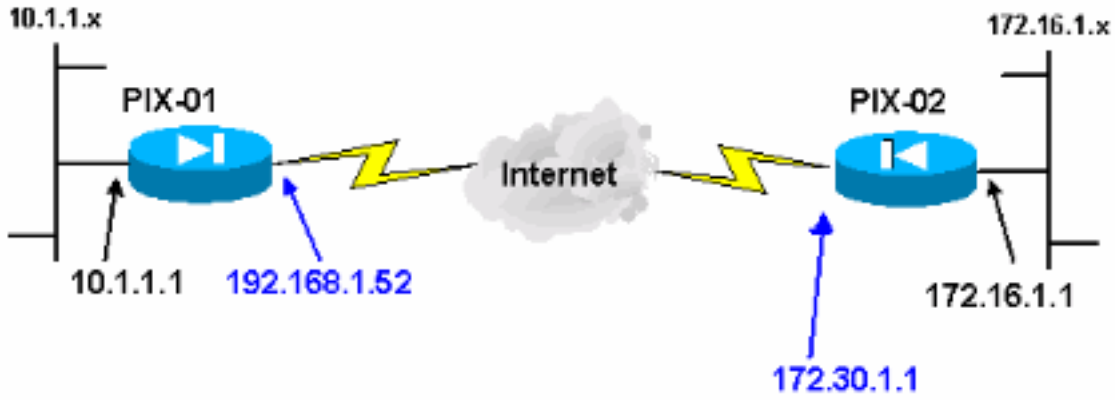
Die Informationen in diesem Dokument basieren auf Cisco Secure PIX 515E-Firewalls mit 6.x und PDM Version 3.0.

Ein Konfigurationsbeispiel für die Konfiguration eines VPN-Tunnels zwischen zwei PIX-Geräten über die Befehlszeilenschnittstelle (CLI) finden Sie unter Konfigurieren eines einfachen PIX-zu-PIX-VPN-Tunnels mit IPsec.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Die IPsec-Aushandlung kann in fünf Schritte unterteilt werden und umfasst zwei IKE-Phasen (Internet Key Exchange).

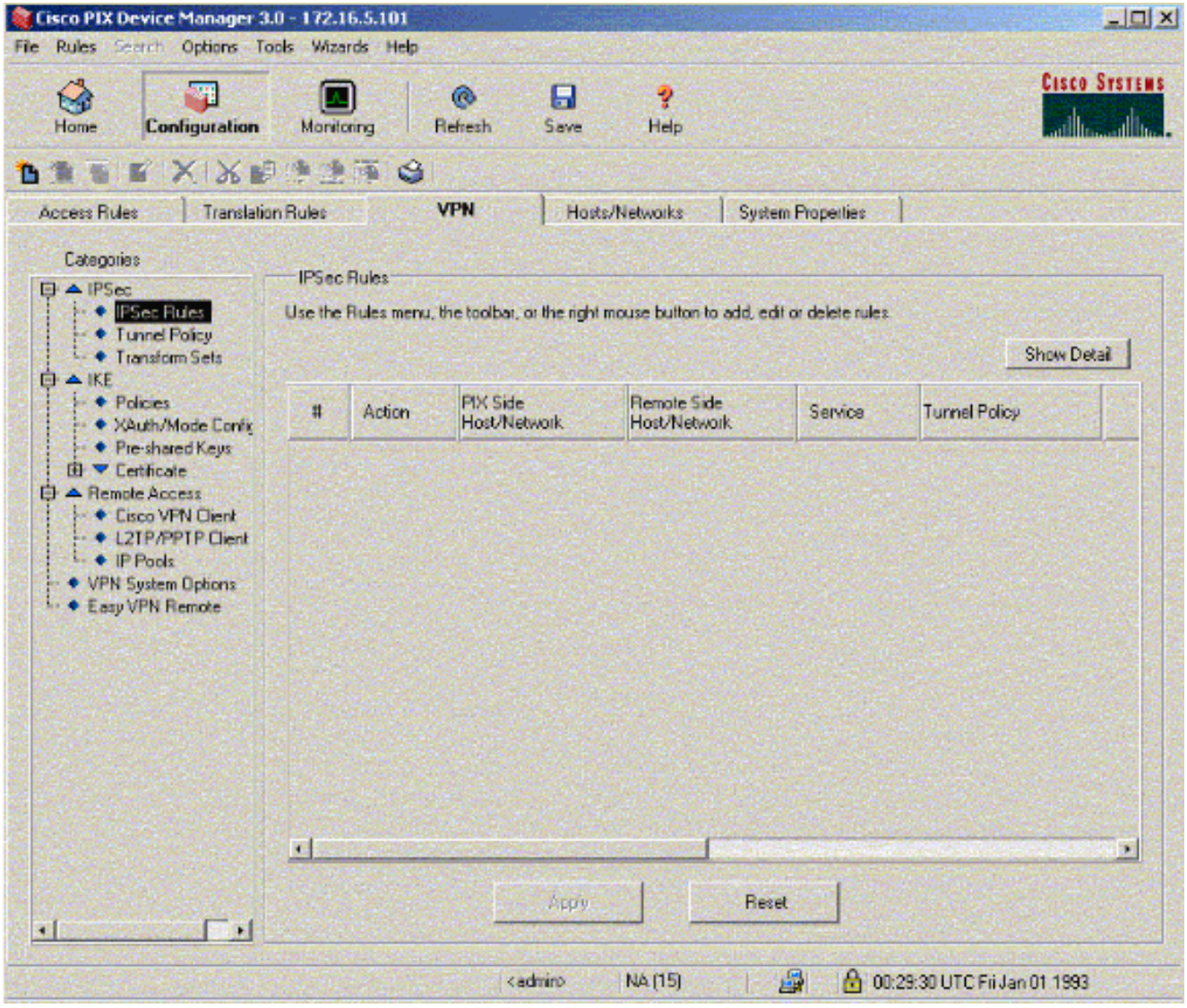
1. Ein IPsec-Tunnel wird durch interessanten Datenverkehr initiiert. Datenverkehr gilt als interessant, wenn er zwischen den IPsec-Peers übertragen wird.
2. In IKE Phase 1 handeln die IPsec-Peers die etablierte IKE Security Association (SA)-Richtlinie aus. Nach der Authentifizierung der Peers wird ein sicherer Tunnel mithilfe von Internet Security Association und Key Management Protocol (ISAKMP) erstellt.
3. In IKE Phase 2 verwenden die IPsec-Peers den authentifizierten und sicheren Tunnel, um IPsec-SA-Transformationen auszuhandeln. Die Aushandlung der freigegebenen Richtlinie bestimmt, wie der IPsec-Tunnel eingerichtet wird.
4. Der IPsec-Tunnel wird erstellt, und Daten werden zwischen den IPsec-Peers übertragen, basierend auf den in den IPsec-Transformationssätzen konfigurierten IPsec-Parametern.
5. Der IPsec-Tunnel endet, wenn die IPsec-SAs gelöscht werden oder ihre Lebensdauer abläuft.**Hinweis:** Die IPsec-Aushandlung zwischen den beiden PIXs schlägt fehl, wenn die SAs in beiden IKE-Phasen auf den Peers nicht übereinstimmen.

Konfigurationsverfahren

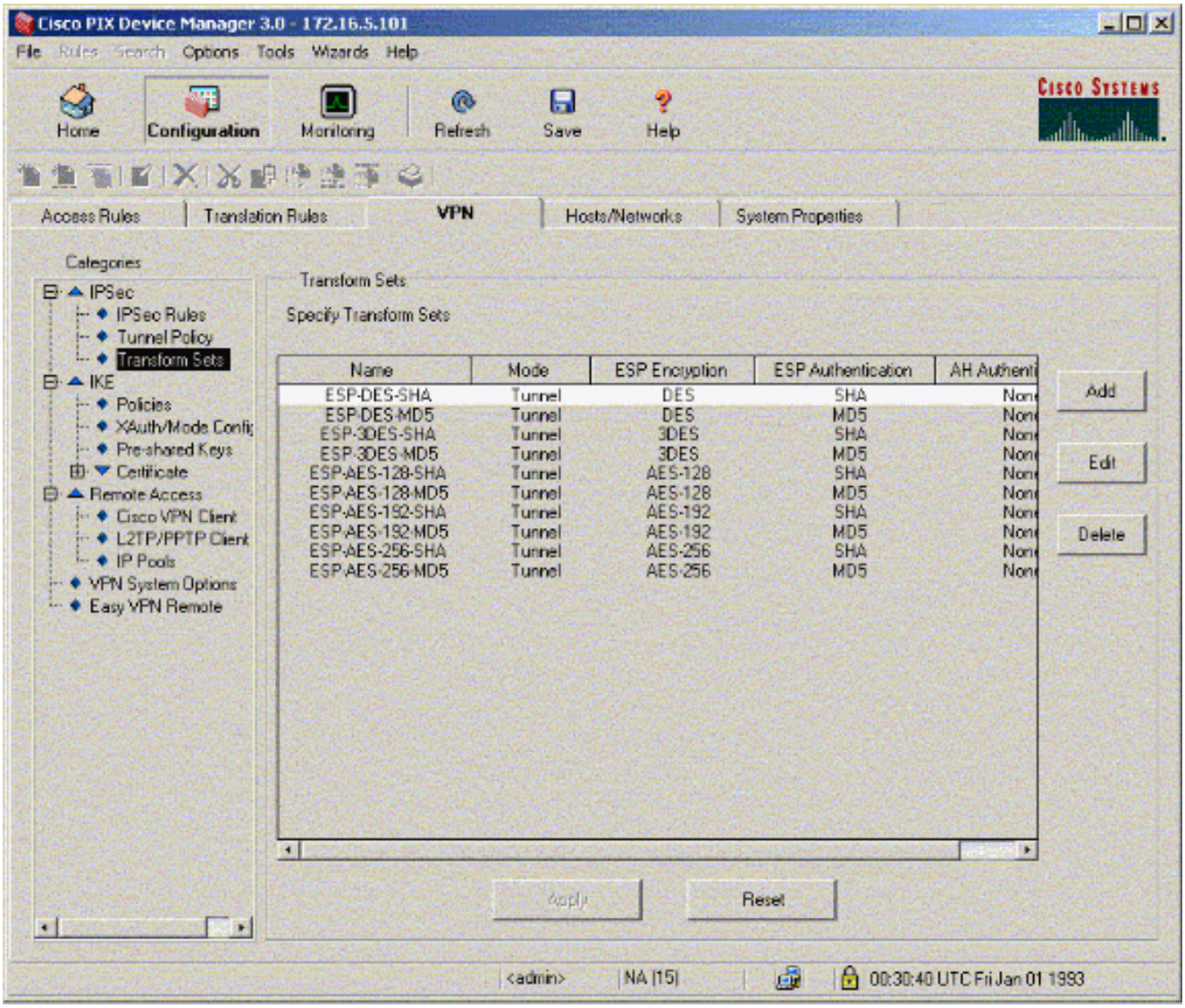
Neben anderen allgemeinen Konfigurationen in der CLI von PIX für den Zugriff auf die Schnittstelle Ethernet 0 verwenden Sie die Befehle **http server enable** und **http server <local_ip> <mask> <interface>**, wobei **<local_ip>** und **<mask> die IP-Adresse und die Maske der Workstation ist, auf der PDM installiert ist.** Die Konfiguration in diesem Dokument gilt für PIX-01. PIX-02 kann mit den gleichen Schritten und unterschiedlichen Adressen konfiguriert werden.

Gehen Sie wie folgt vor:

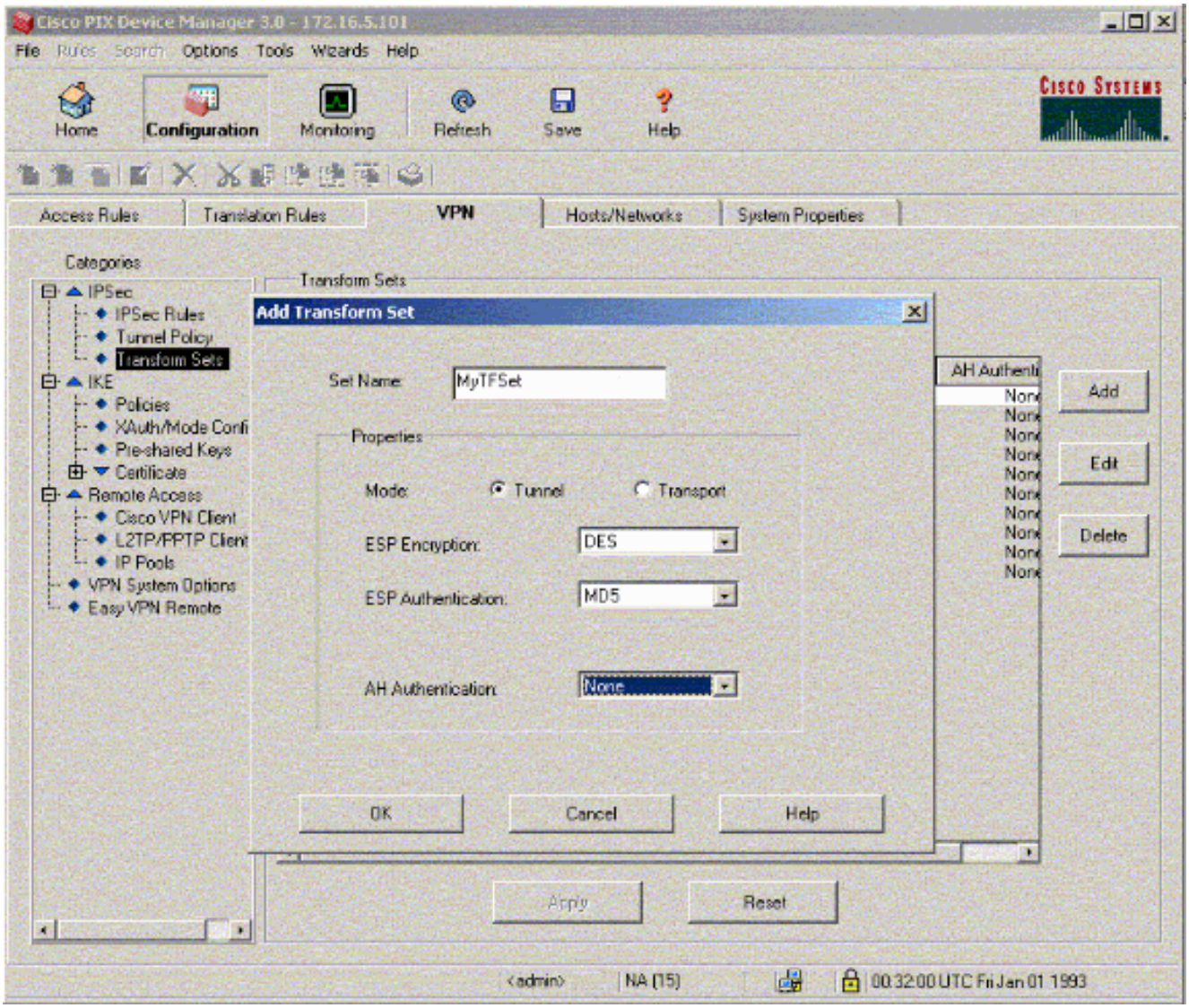
1. Öffnen Sie Ihren Browser, und geben Sie **https://<Inside_IP_Address_of_PIX>** ein, um auf das PIX in PDM zuzugreifen.
2. Klicken Sie auf **Konfiguration**, und wechseln Sie zur Registerkarte VPN.



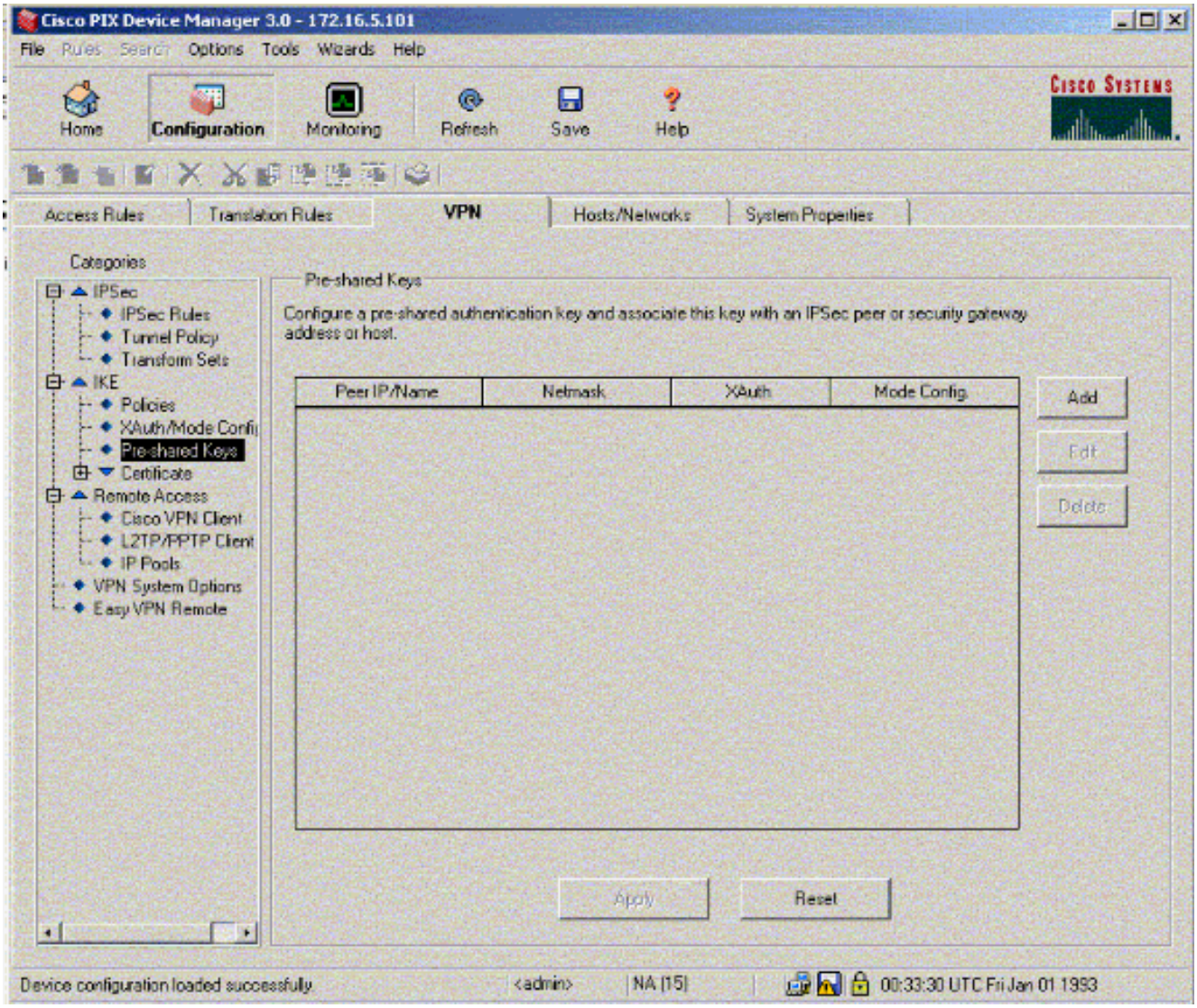
3. Klicken Sie unter IPSec auf **Transform Sets**, um einen Transform-Satz zu erstellen.



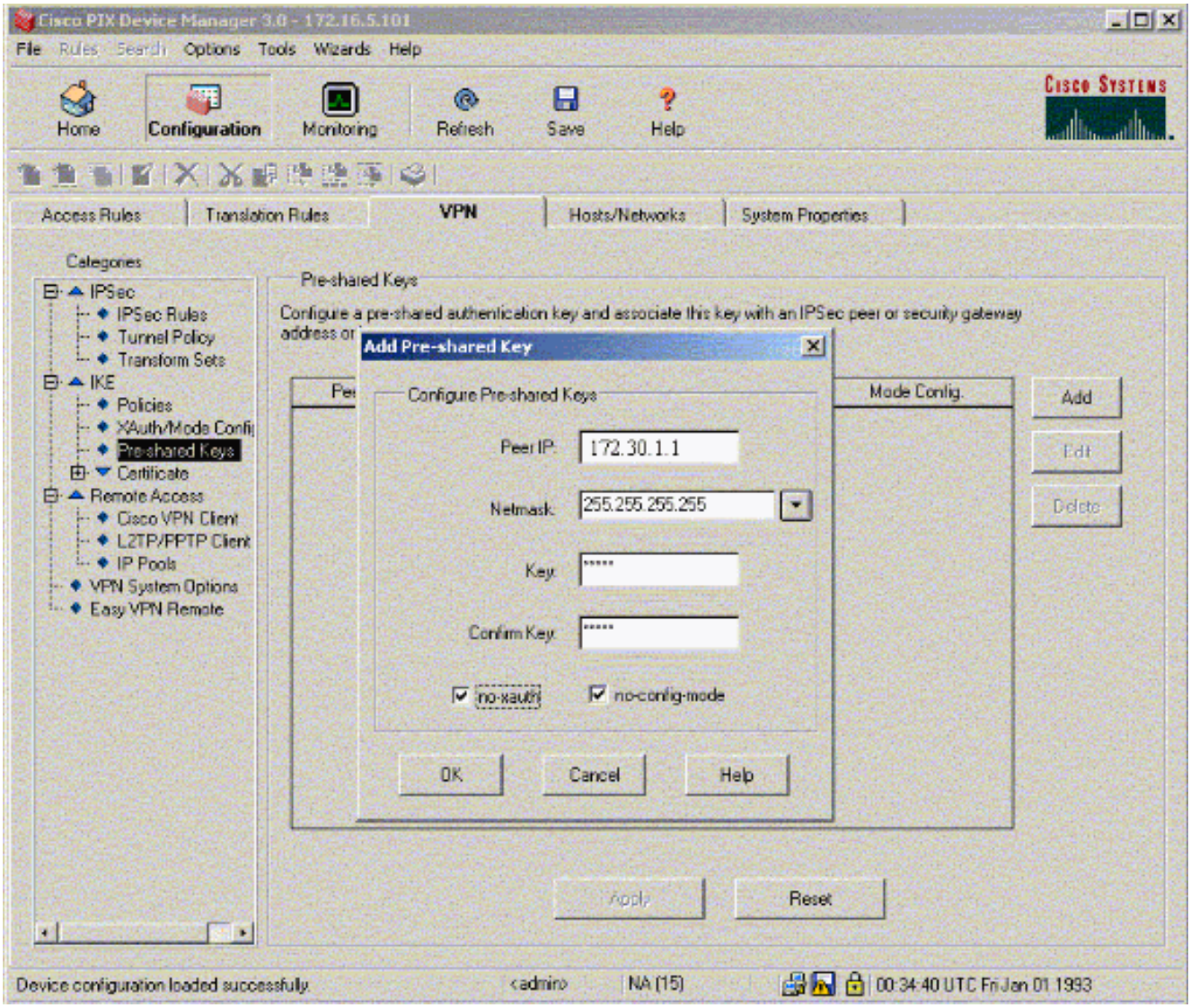
4. Klicken Sie auf **Hinzufügen**, wählen Sie alle entsprechenden Optionen aus, und klicken Sie auf **OK**, um einen neuen Transform-Satz zu erstellen.



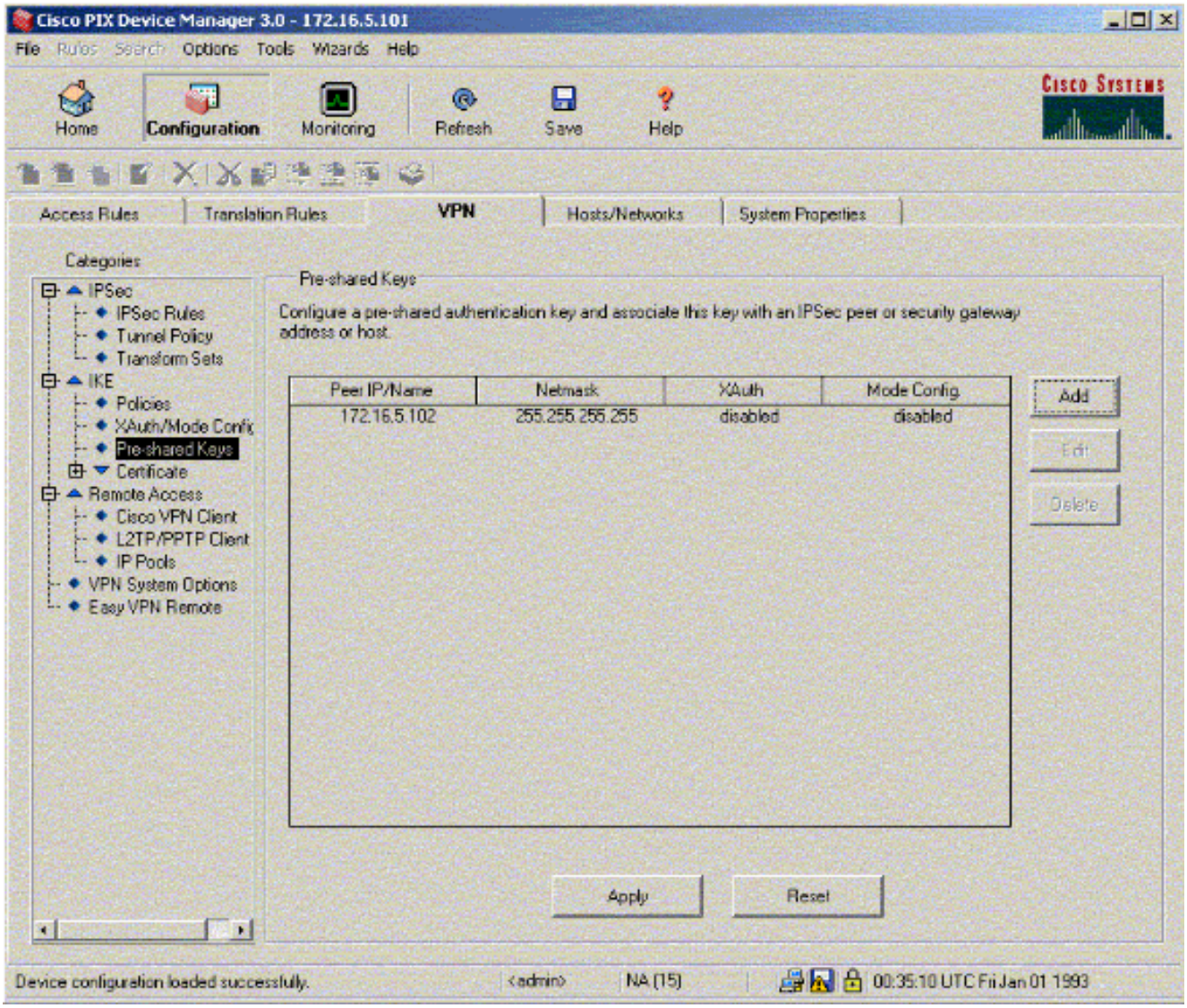
5. Klicken Sie unter IKE auf **Vorinstallierte Schlüssel**, um vorinstallierte Schlüssel zu konfigurieren.



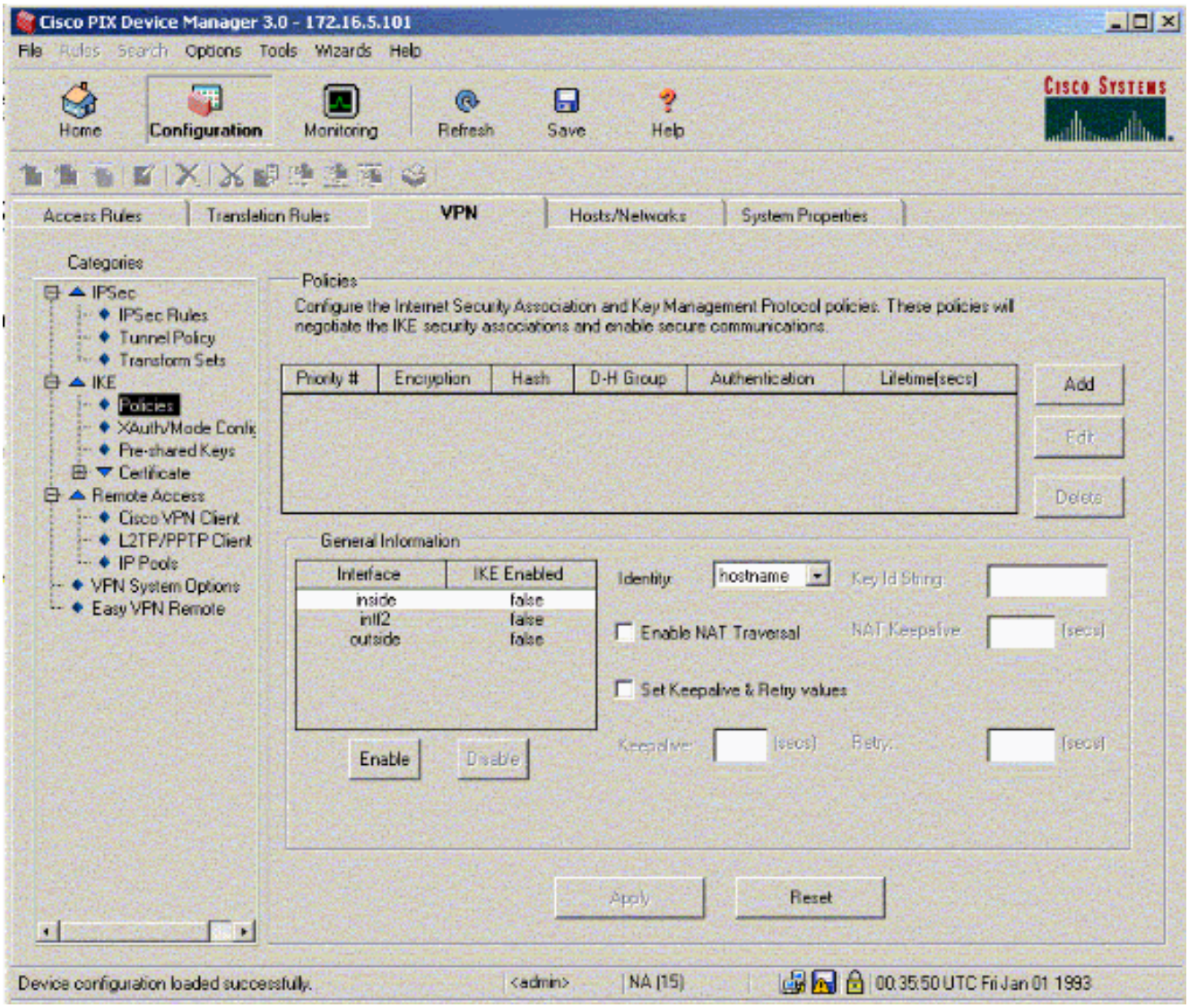
6. Klicken Sie auf **Hinzufügen**, um einen neuen vorinstallierten Schlüssel hinzuzufügen.



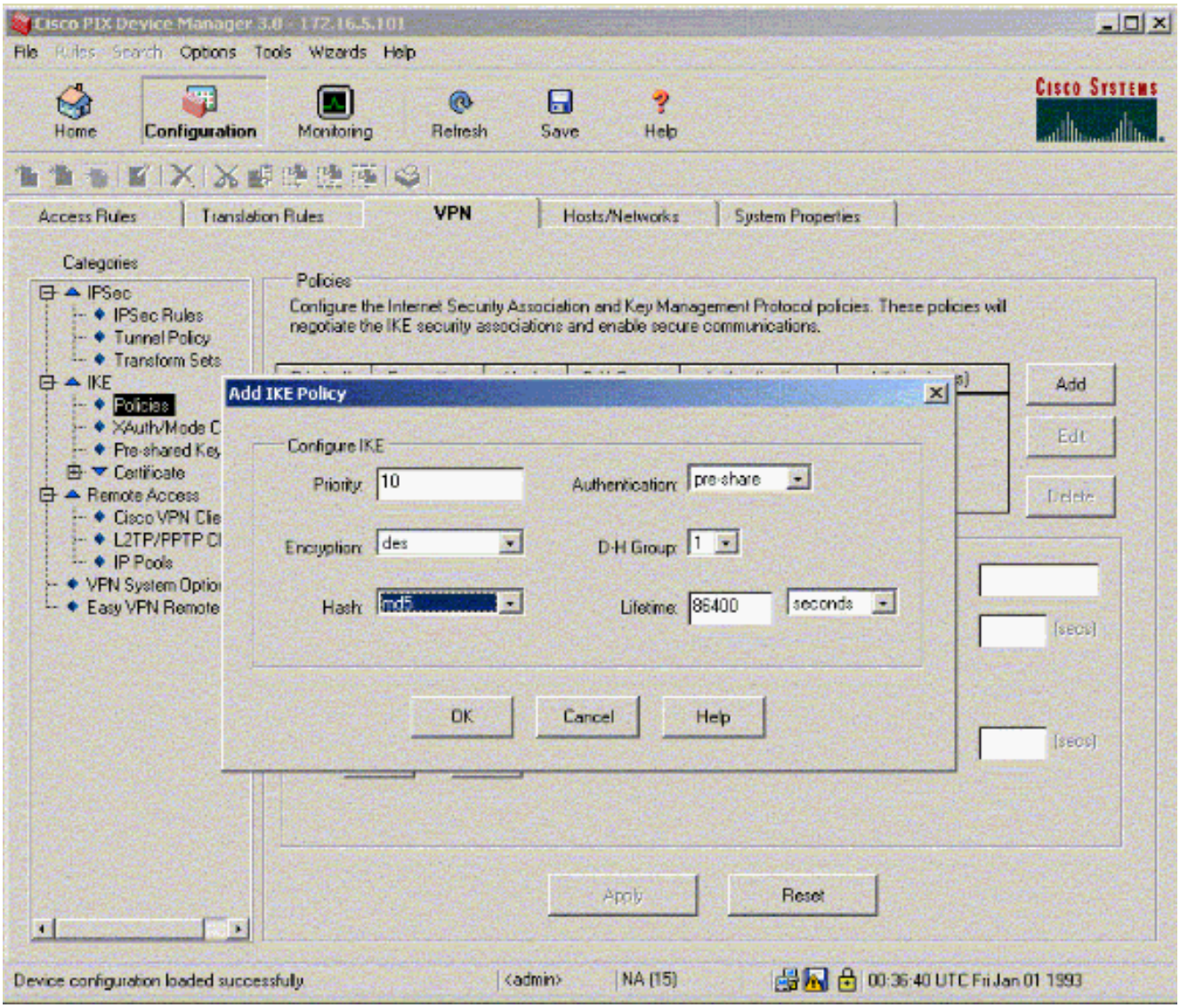
In diesem Fenster wird der Schlüssel angezeigt, d. h. das Kennwort für die Tunnelzuordnung. Dies muss auf beiden Seiten des Tunnels übereinstimmen.



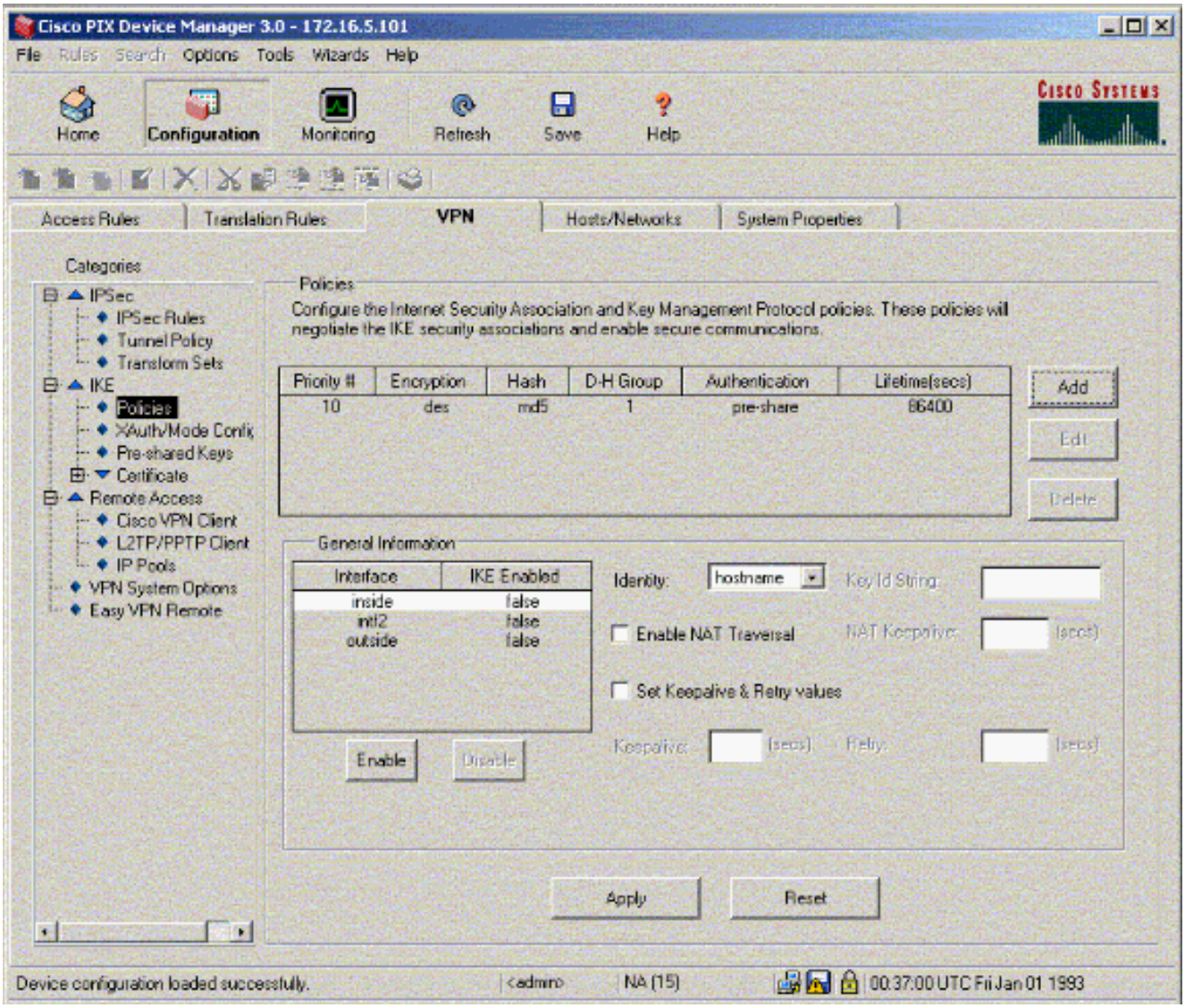
7. Klicken Sie unter IKE auf **Policies (Richtlinien)**, um Richtlinien zu konfigurieren.



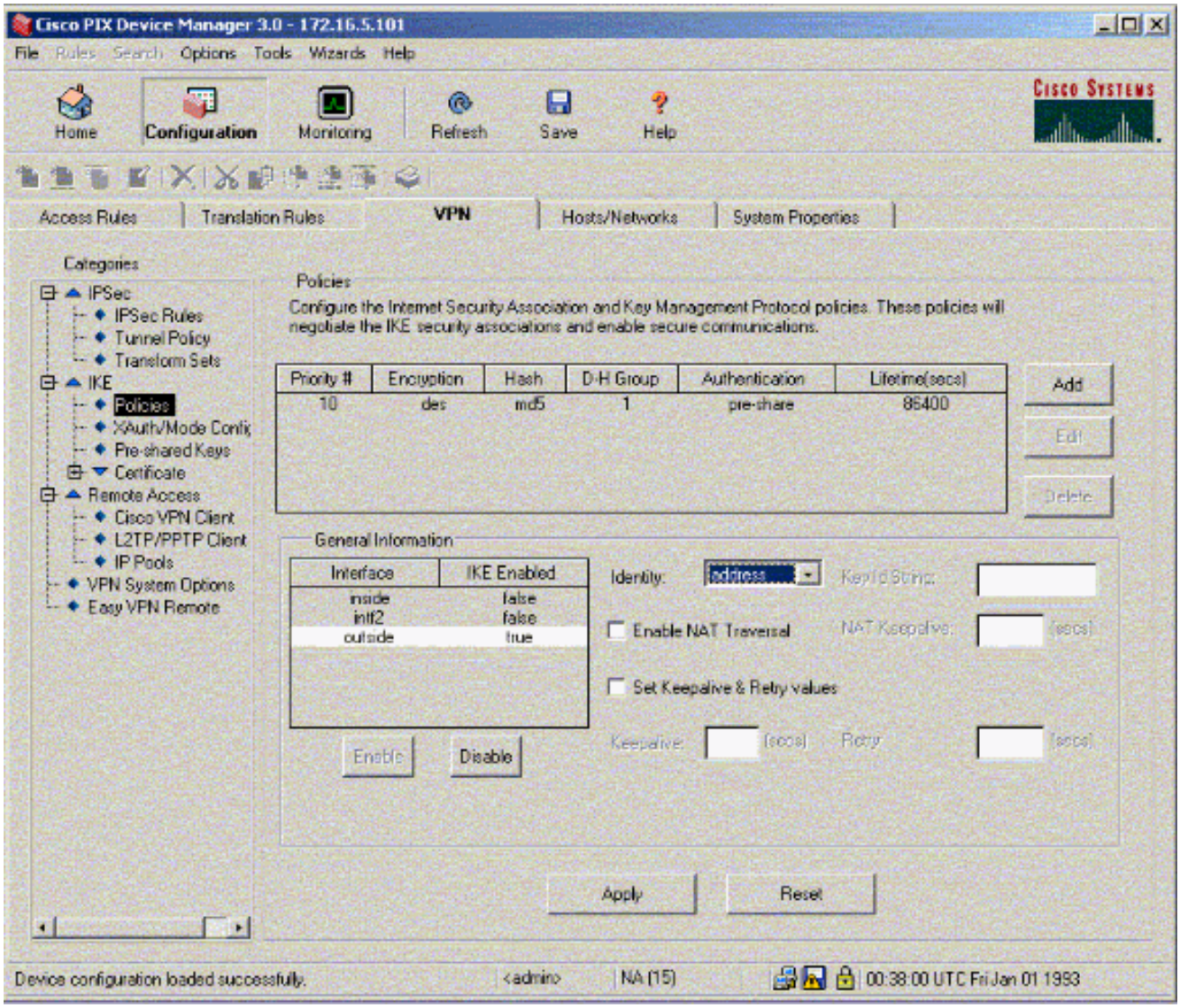
8. Klicken Sie auf **Hinzufügen**, und füllen Sie die entsprechenden Felder aus.



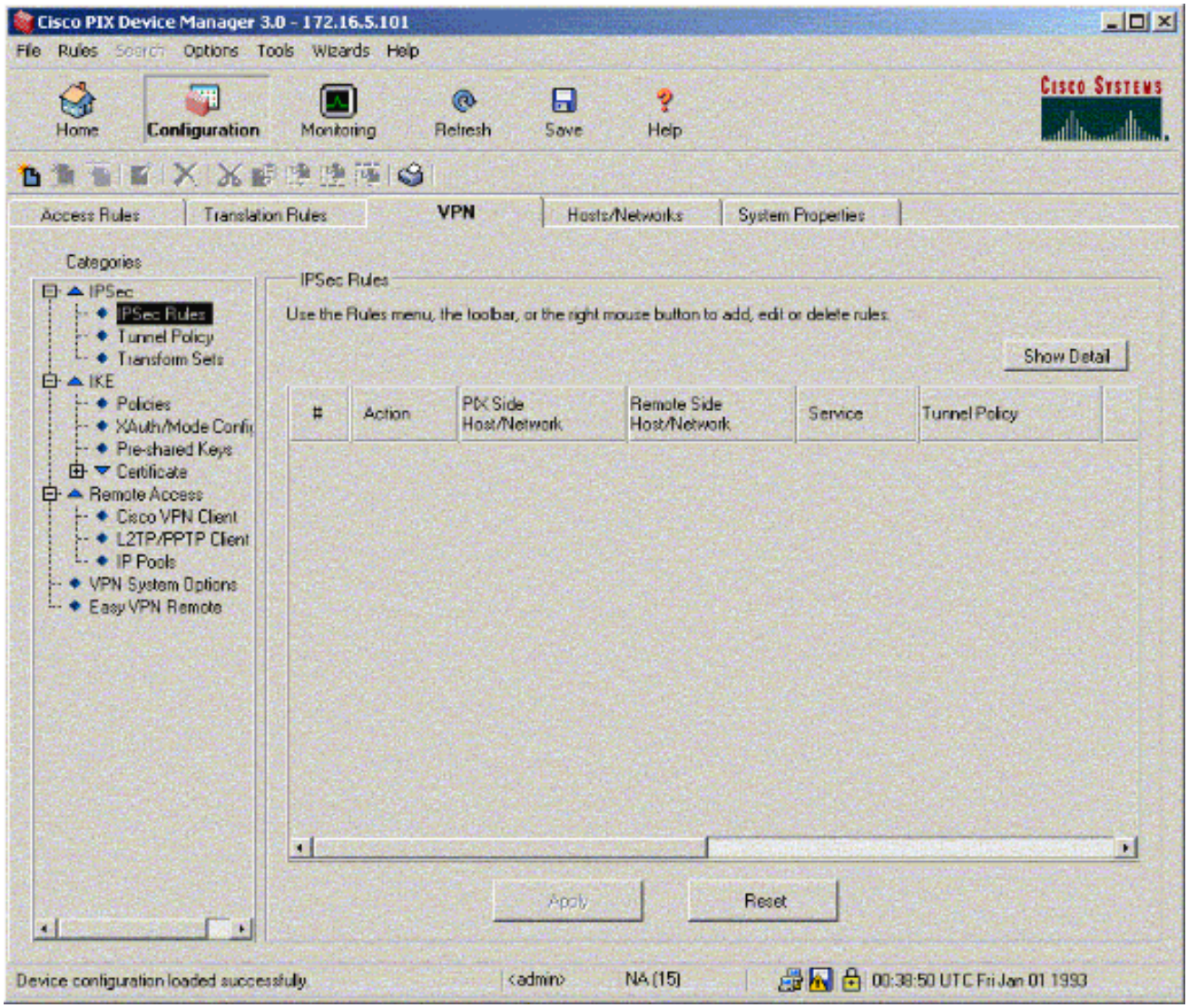
9. Klicken Sie auf **OK**, um eine neue Richtlinie hinzuzufügen.



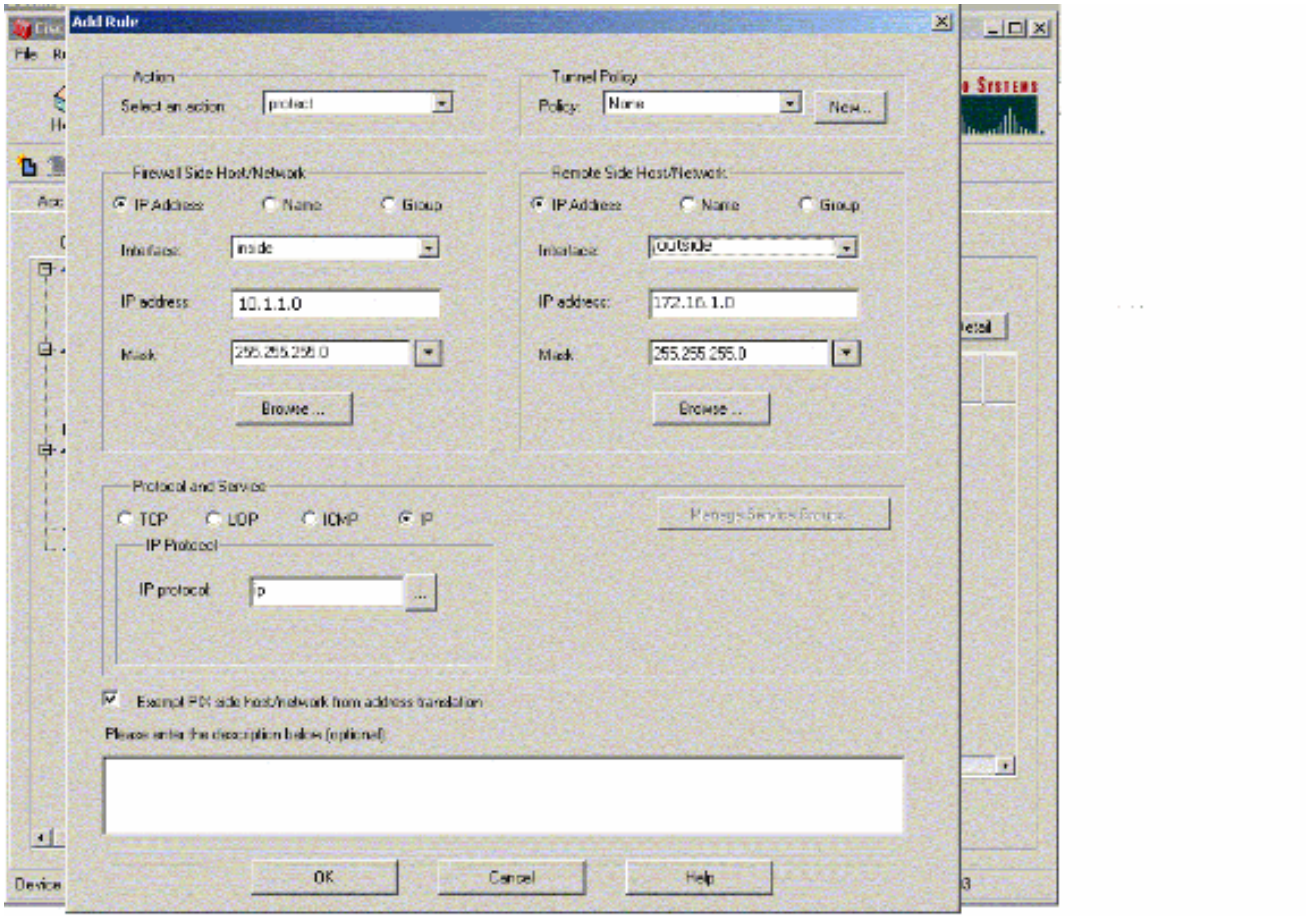
10. Wählen Sie die **externe** Schnittstelle aus, klicken Sie auf **Aktivieren**, und wählen Sie im Dropdown-Menü Identität die **Adresse aus**.



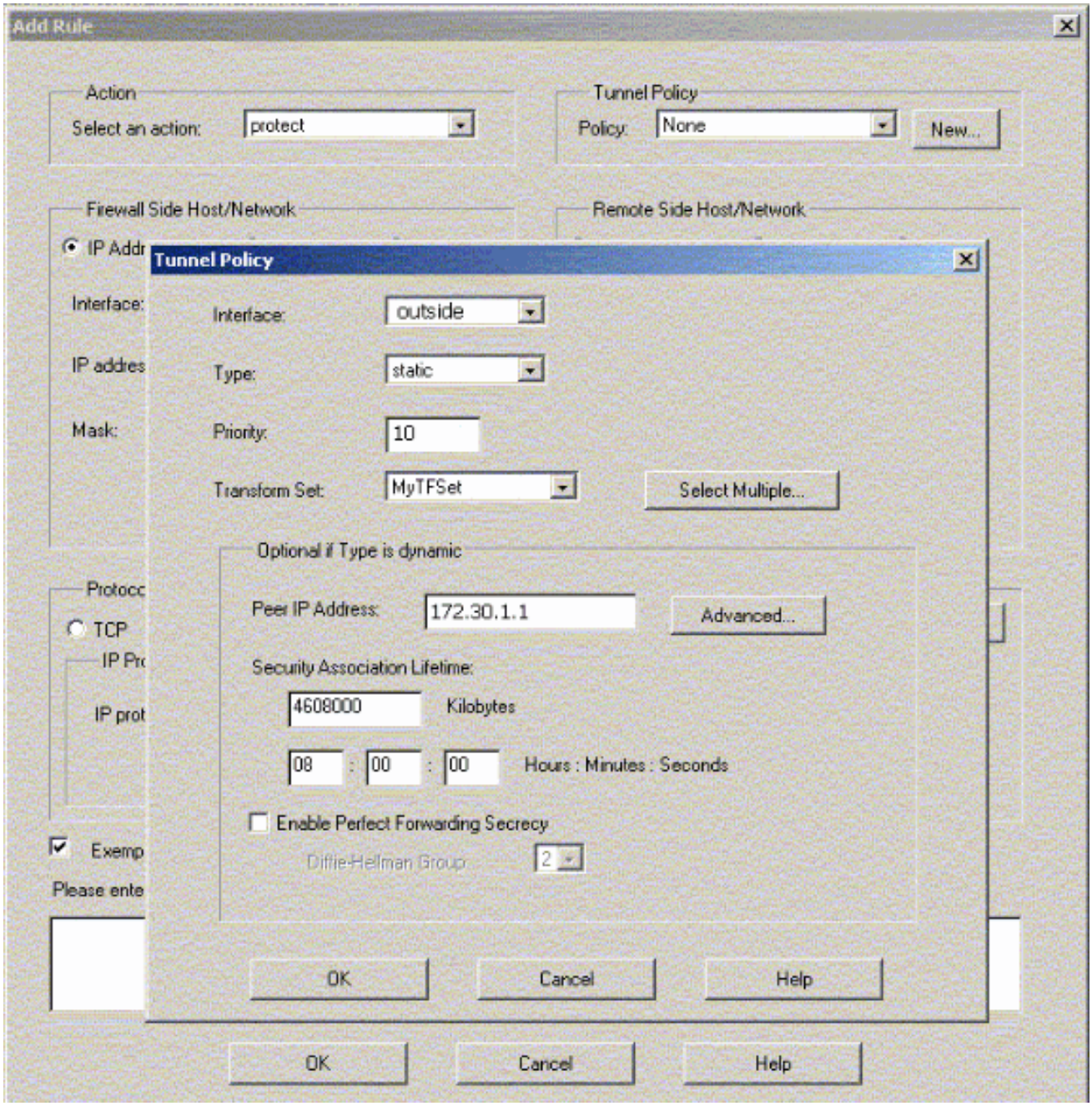
11. Klicken Sie unter IPSec auf **IPSec Rules**, um IPsec-Regeln zu erstellen.



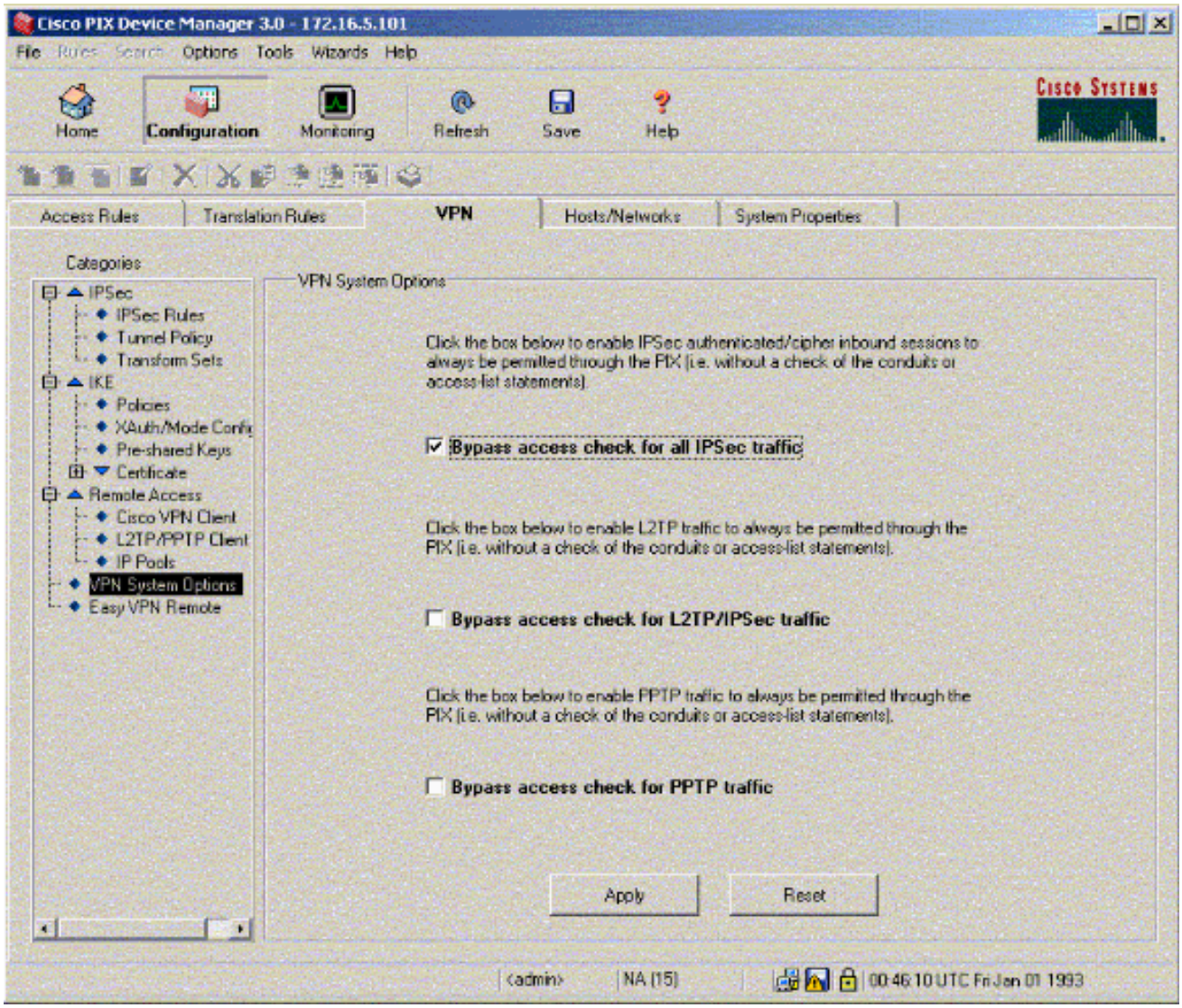
12. Füllen Sie die entsprechenden Felder aus.



13. Klicken Sie in der Tunnelrichtlinie auf **Neu**. Das Fenster Tunnel Policy (Tunnelrichtlinie) wird angezeigt. Füllen Sie die entsprechenden Felder
    aus.



14. Klicken Sie auf **OK**, um die konfigurierte IPsec-Regel anzuzeigen.
15. Klicken Sie auf **VPN-Systemoptionen**, und aktivieren Sie **die Option Zugriffsüberprüfung für den gesamten IPSec-Datenverkehr umgehen**.

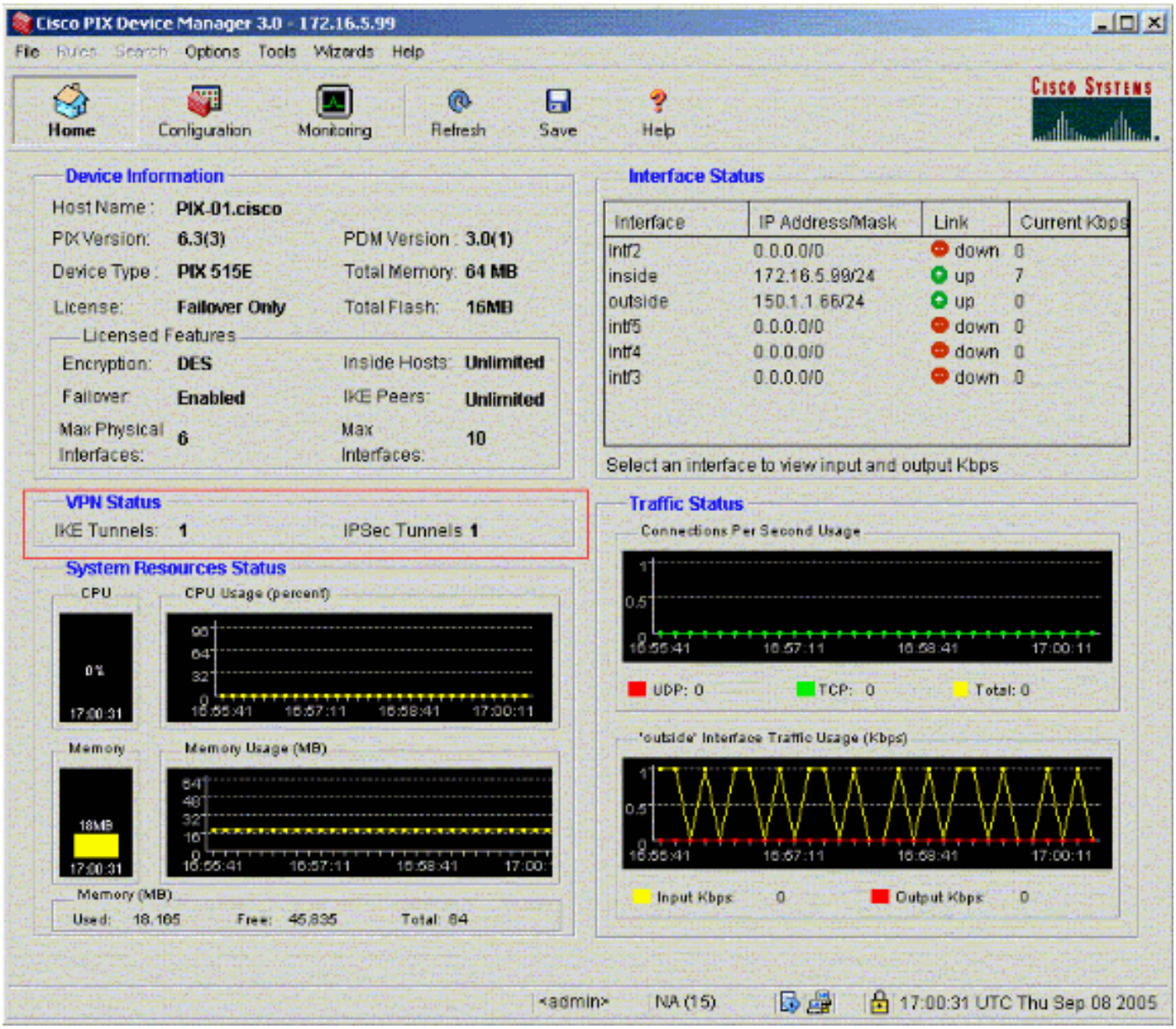


Überprüfen

Wenn ein interessanter Datenverkehr zum Peer besteht, wird der Tunnel zwischen PIX-01 und PIX-02 erstellt.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Zeigen Sie den VPN-Status im PDM unter "Home" (rot markiert) an, um die Bildung des Tunnels zu überprüfen.



Sie können auch die Bildung von Tunneln mithilfe der CLI im PDM unter Tools überprüfen. Geben Sie den Befehl **show crypto isakmp sa** ein, um die Bildung von Tunneln zu überprüfen und den Befehl **show crypto ipsec als** Befehl auszugeben, um die Anzahl der eingekapselten, verschlüsselten Pakete usw. zu beobachten.

Hinweis: Die interne Schnittstelle des PIX kann erst dann für die Tunnelbildung gepingt werden, wenn der Befehl **Management-Access** im globalen Bestätigungsmodus konfiguriert wurde.

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

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Redundante Tunnelerstellung zwischen Firewalls mithilfe von PDM
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Anforderungen für Kommentare (RFCs)
- Cisco PIX Firewall-Software