Esempio di tunnel VPN da LAN a LAN tra due PIX con configurazione PDM

Sommario

Introduzione

Questo documento descrive la procedura per configurare i tunnel VPN tra due firewall PIX con Cisco PIX Device Manager (PDM). PDM è uno strumento di configurazione basato su browser progettato per semplificare la configurazione, la configurazione e il monitoraggio del firewall PIX tramite un'interfaccia utente grafica. I firewall PIX si trovano in due siti diversi.

Tunnel formato tramite IPsec. IPsec è una combinazione di standard aperti che forniscono riservatezza, integrità e autenticazione dell'origine dei dati tra peer IPsec.

Prerequisiti

Requisiti

Nessun requisito previsto per questo documento.

Componenti usati

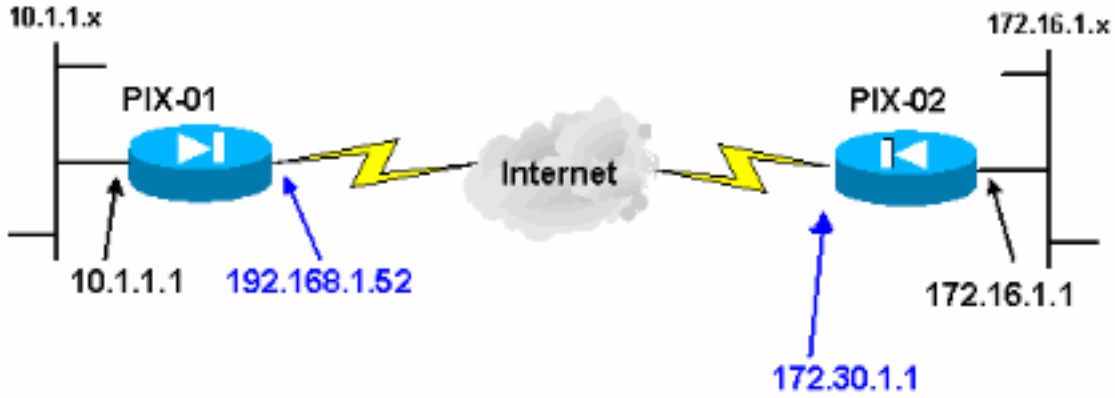
Le informazioni di questo documento si basano sui firewall Cisco Secure PIX 515E con 6.x e PDM versione 3.0.

Per un esempio sulla configurazione di un tunnel VPN tra due dispositivi PIX tramite l'interfaccia della riga di comando (CLI), fare riferimento a Configurazione di un tunnel VPN da PIX a PIX semplice con IPsec.

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).

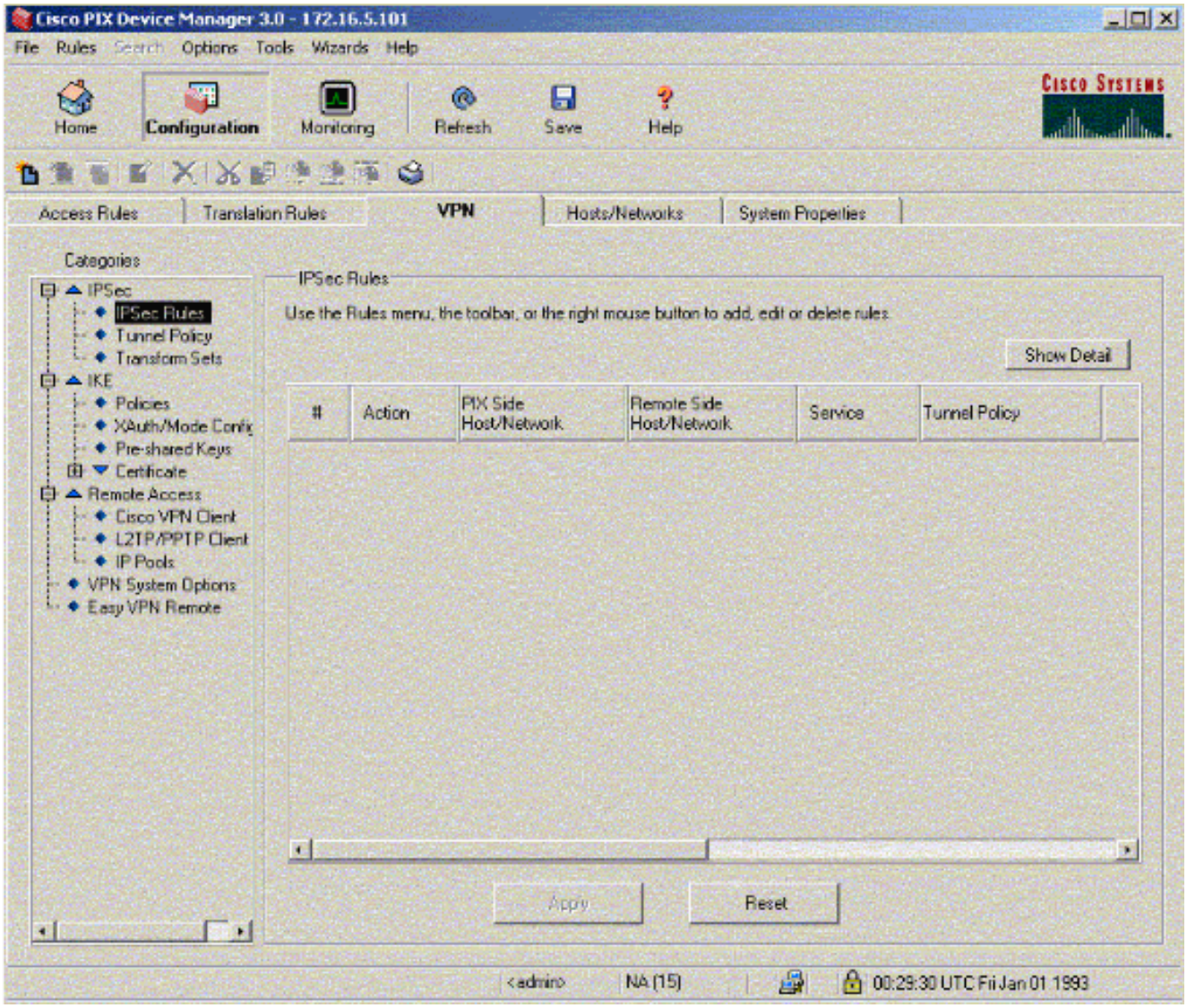
1. Un tunnel IPsec viene avviato da traffico interessante. Il traffico è considerato interessante quando avviene tra peer IPsec.
2. Nella fase 1 di IKE, i peer IPsec negoziano il criterio SA (Security Association) IKE stabilito. Dopo l'autenticazione dei peer, viene creato un tunnel protetto utilizzando Internet Security Association and Key Management Protocol (ISAKMP).
3. 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.
4. 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.
5. 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.

Procedura di configurazione

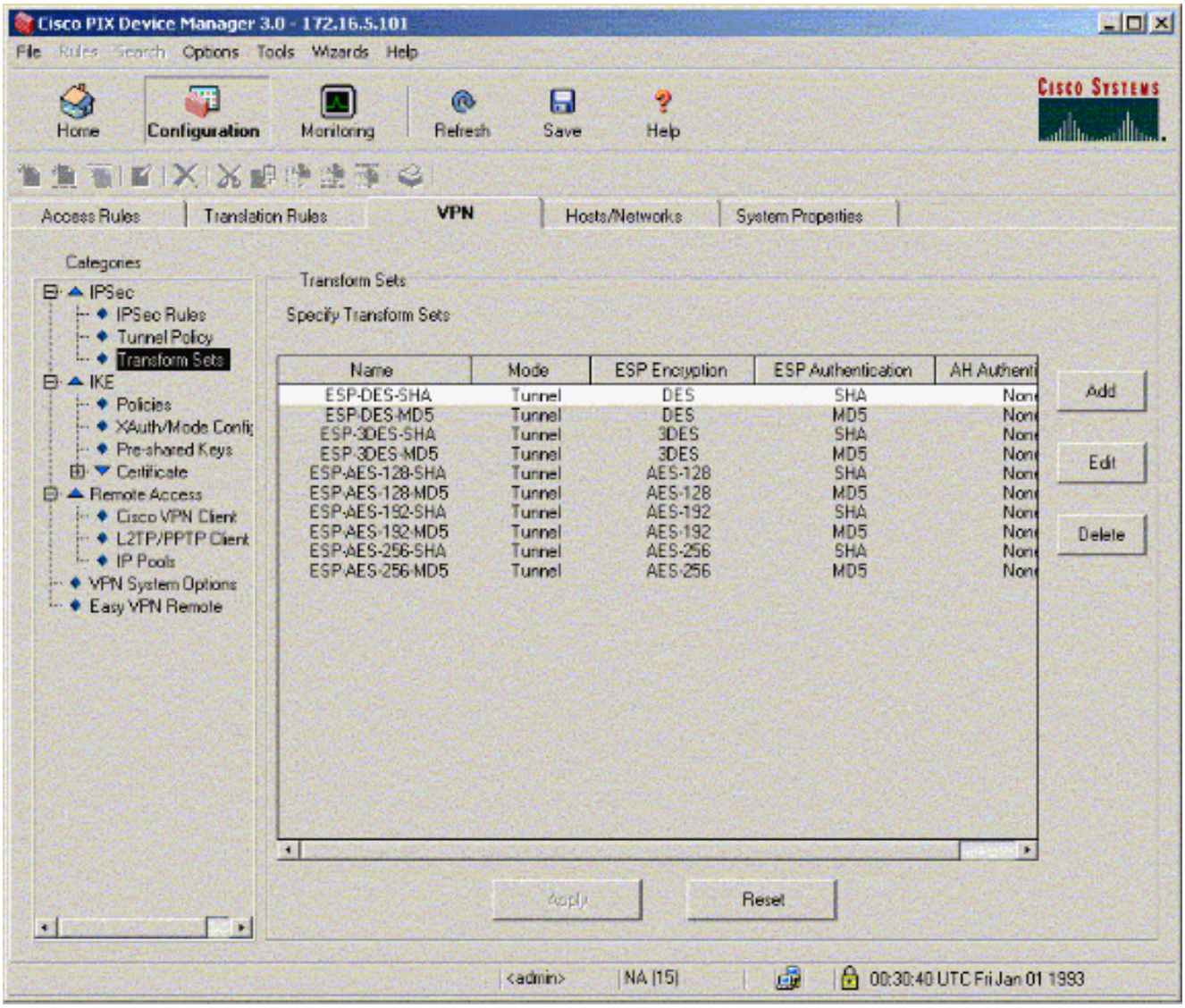
A parte altre configurazioni generali nella CLI di PIX per accedere tramite l'interfaccia Ethernet 0, usare i comandi **http server enable** e **http server <ip_locale> <mask> <interface>** dove *<ip_locale>* e *<mask>* è l'indirizzo IP e la maschera della workstation su cui è installato PDM. La configurazione di questo documento è per PIX-01. PIX-02 può essere configurato usando gli stessi passaggi con indirizzi diversi.

Attenersi alla seguente procedura:

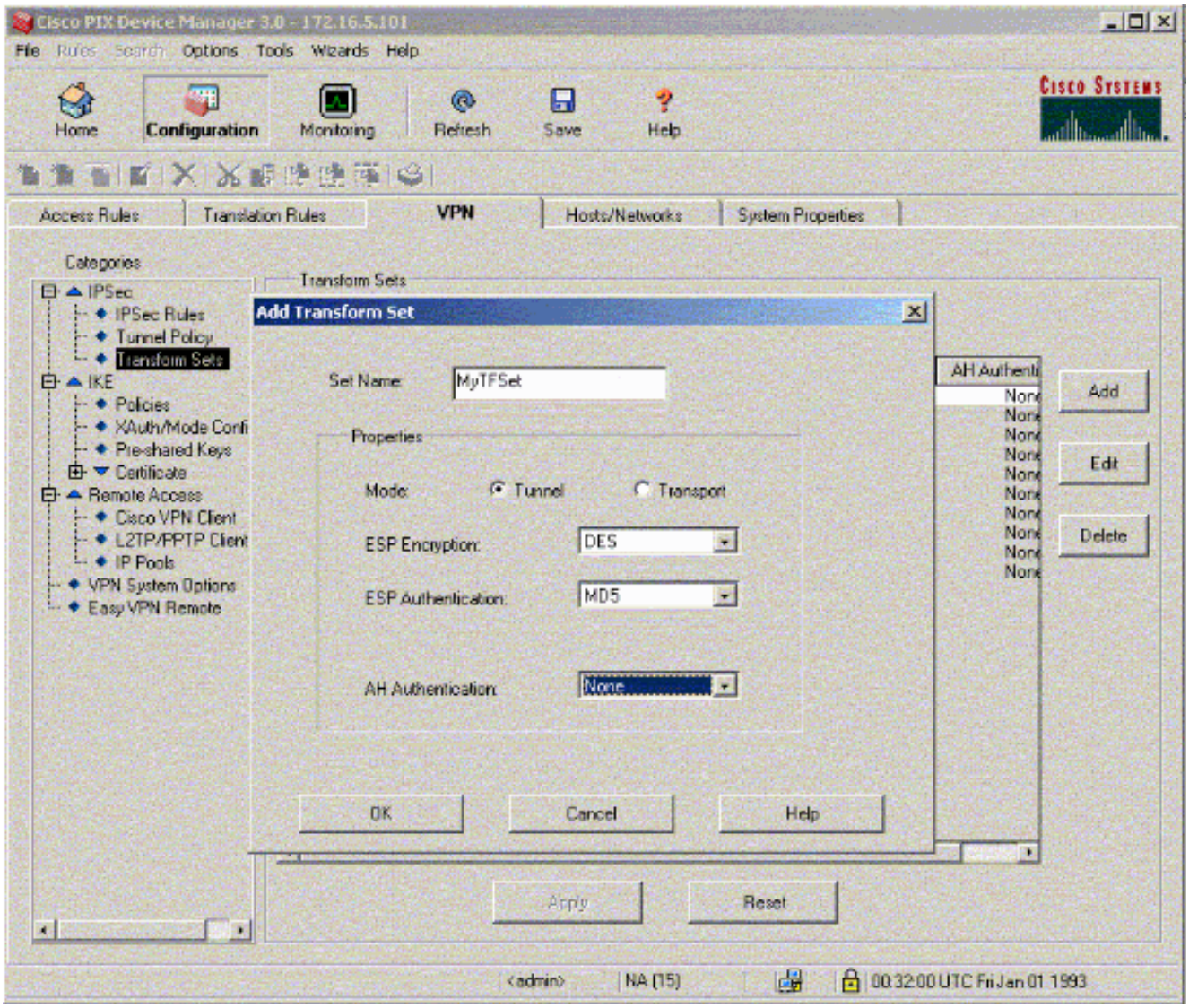
1. Aprire il browser e digitare **https://<Inside_IP_Address_of_PIX>** per accedere al PIX in PDM.
2. Fare clic su **Configuration** (Configurazione) e andare alla scheda VPN.



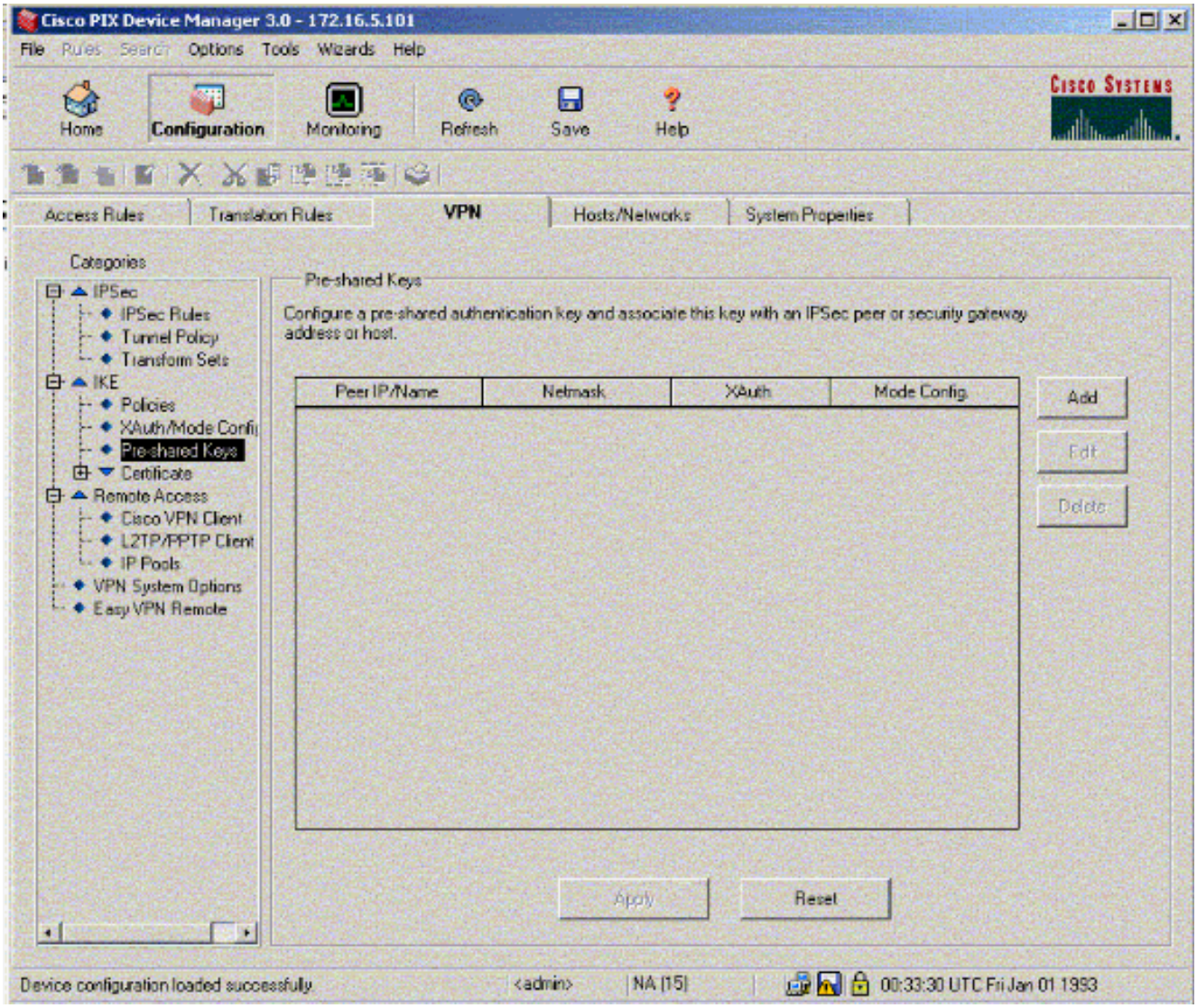
3. Fare clic su **Set di trasformazioni** in IPSec per creare un set di trasformazioni.



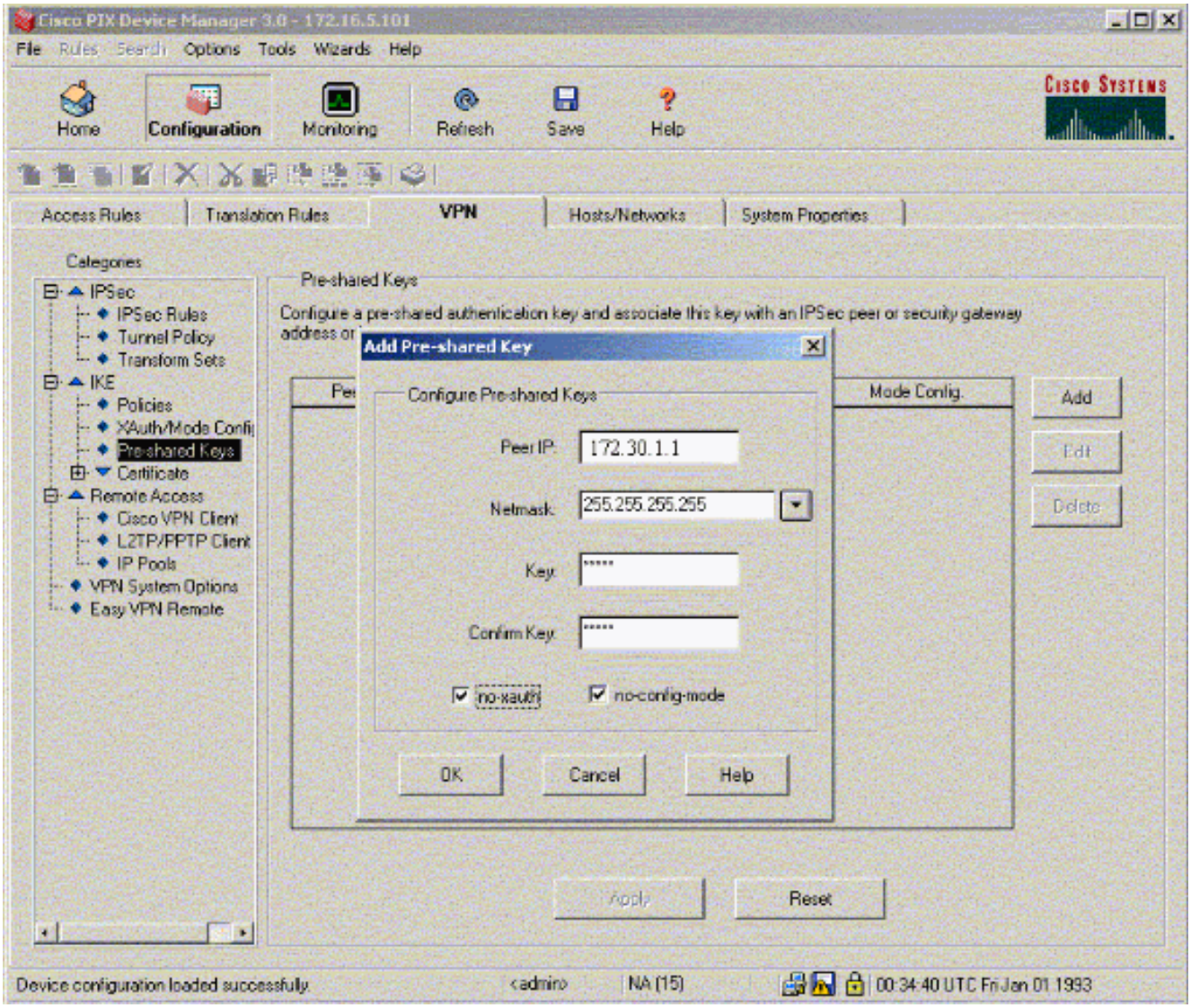
4. Fare clic su **Aggiungi**, selezionare tutte le opzioni appropriate e fare clic su **OK** per creare un nuovo set di trasformazione.



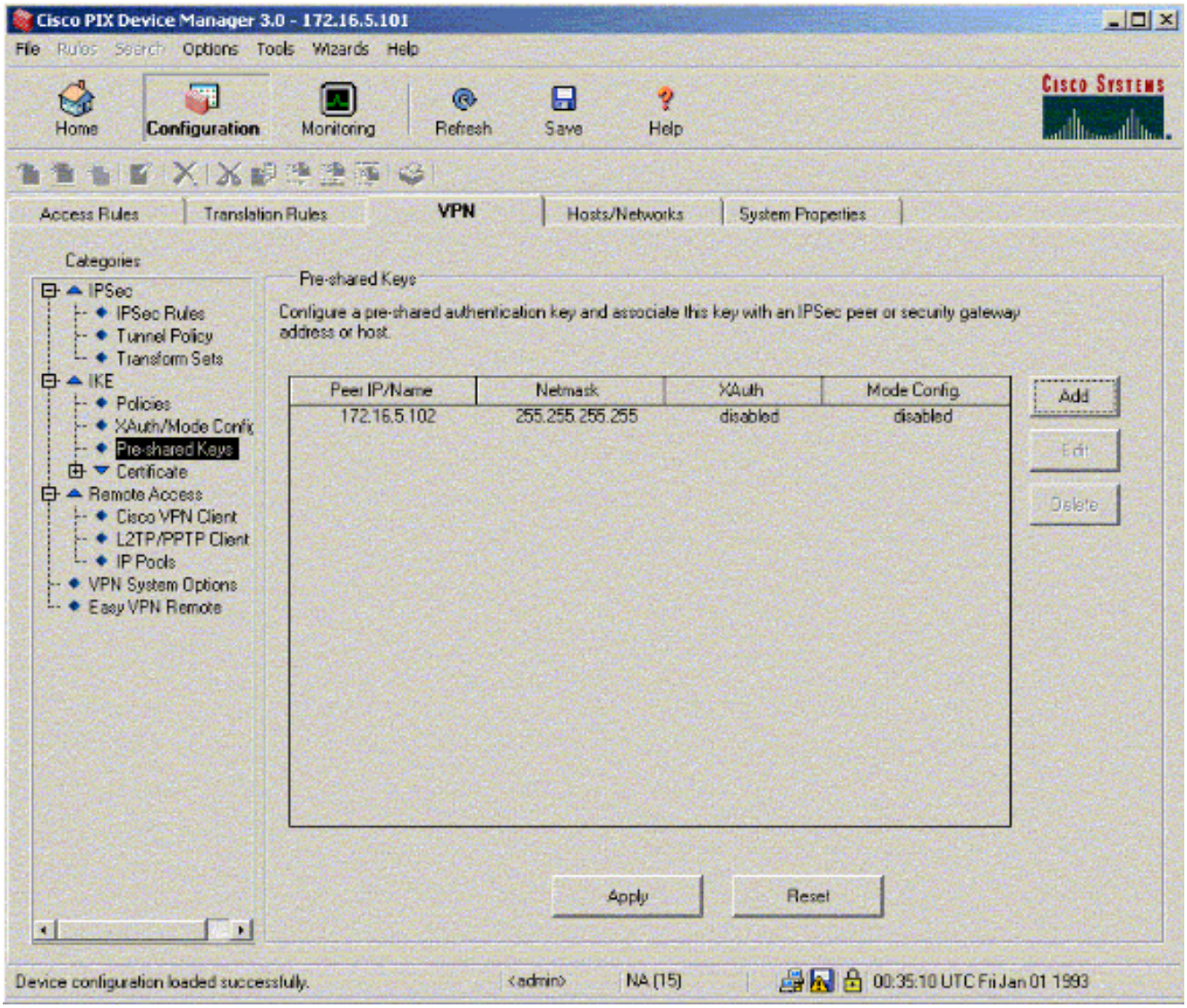
5. Fare clic su **Chiavi già condivise** in IKE per configurare le chiavi già condivise.



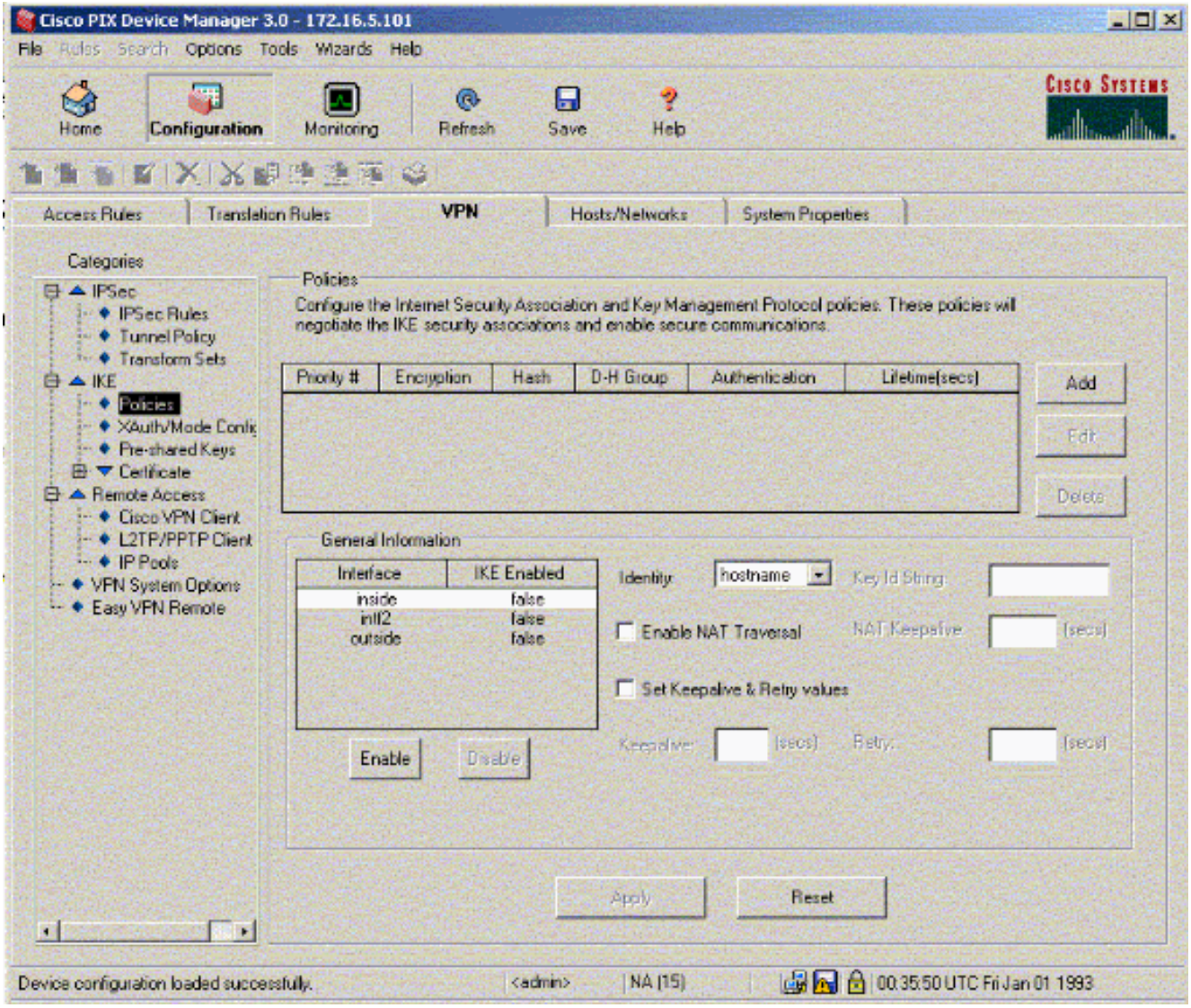
6. Fare clic su **Add** (Aggiungi) per aggiungere una nuova chiave già condivisa.



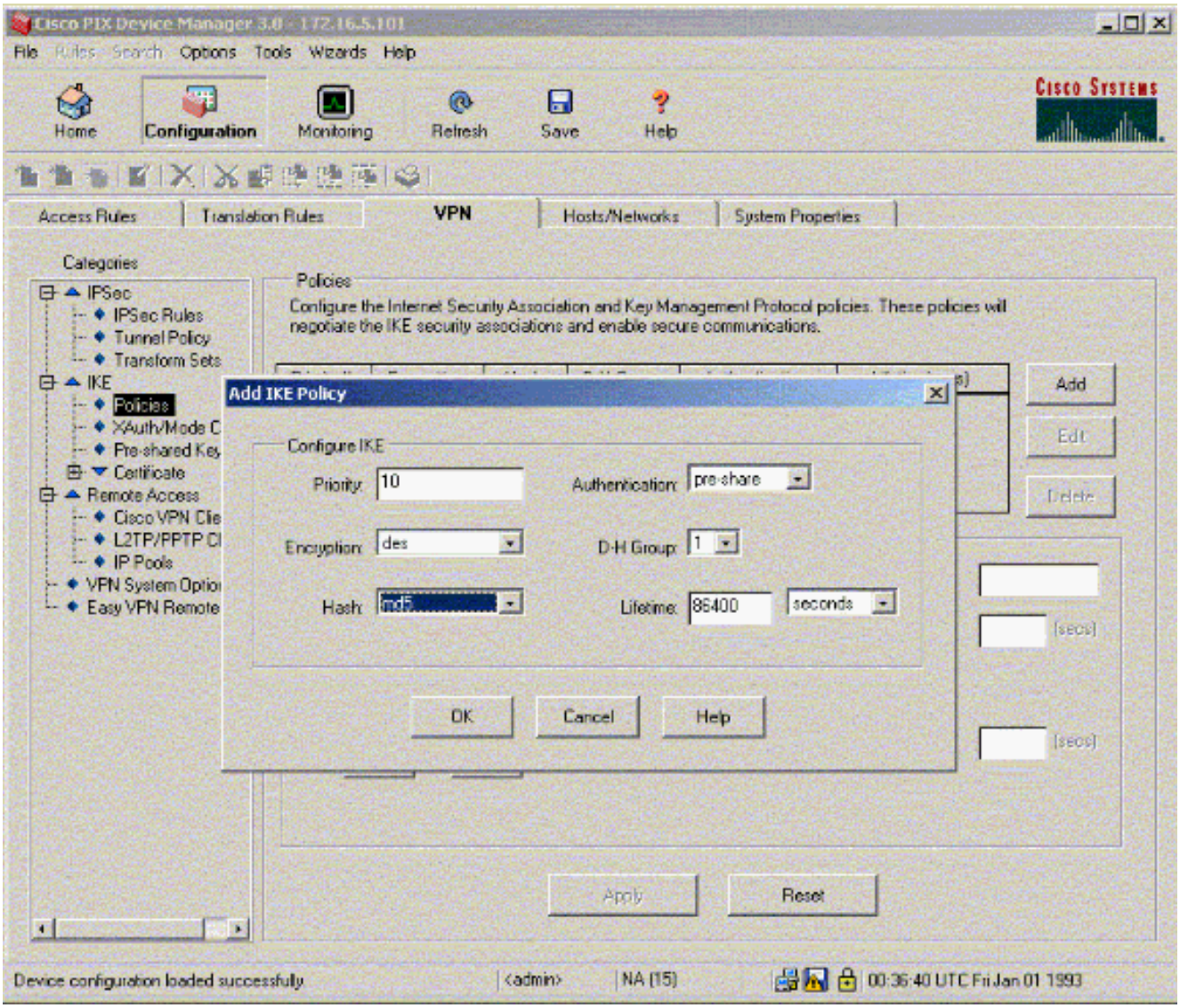
In questa finestra viene visualizzata la chiave, ovvero la password per l'associazione del tunnel. Deve essere uguale su entrambi i lati del
tunnel.



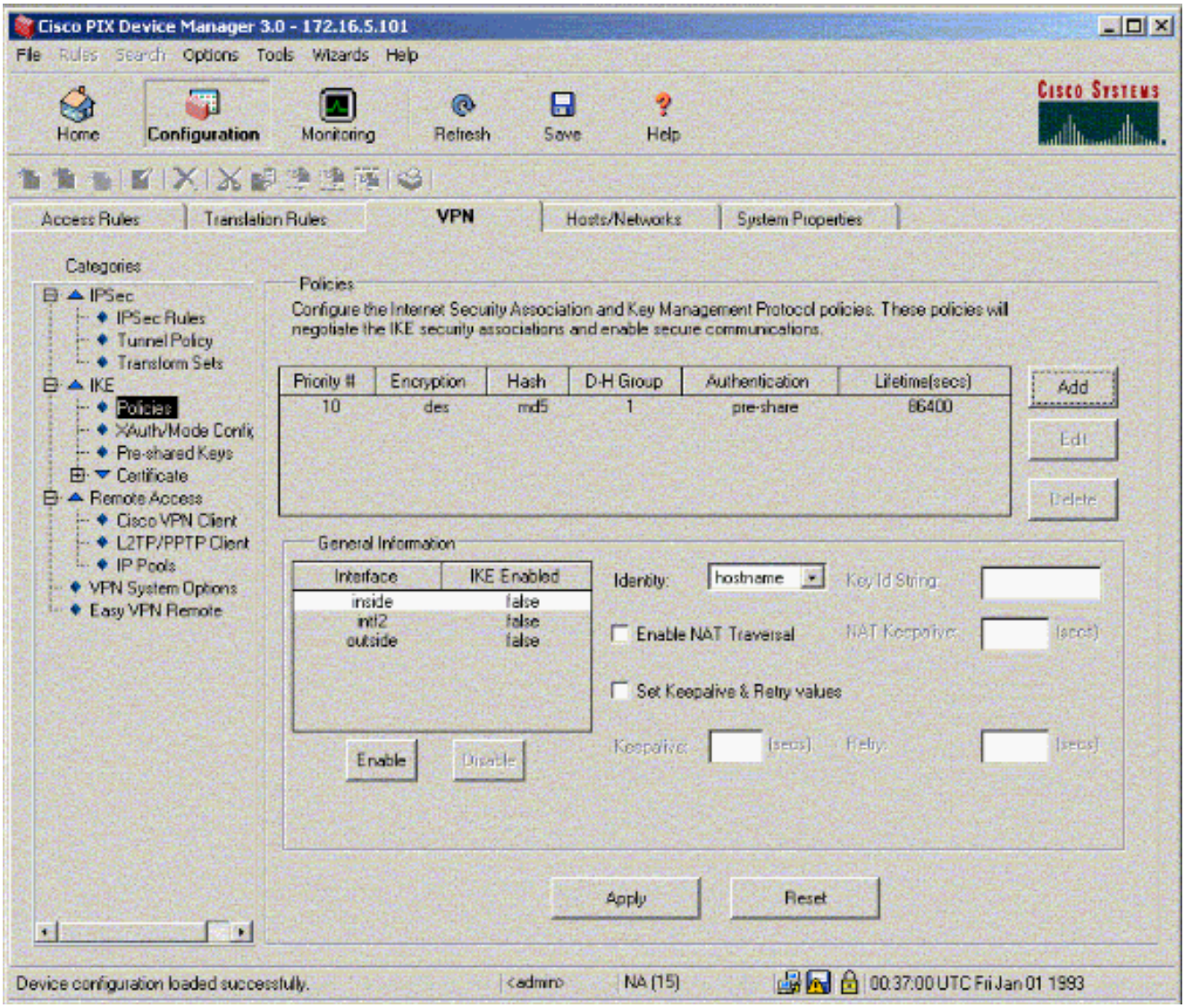
7. Fare clic su **Criteri** in IKE per configurare i criteri.



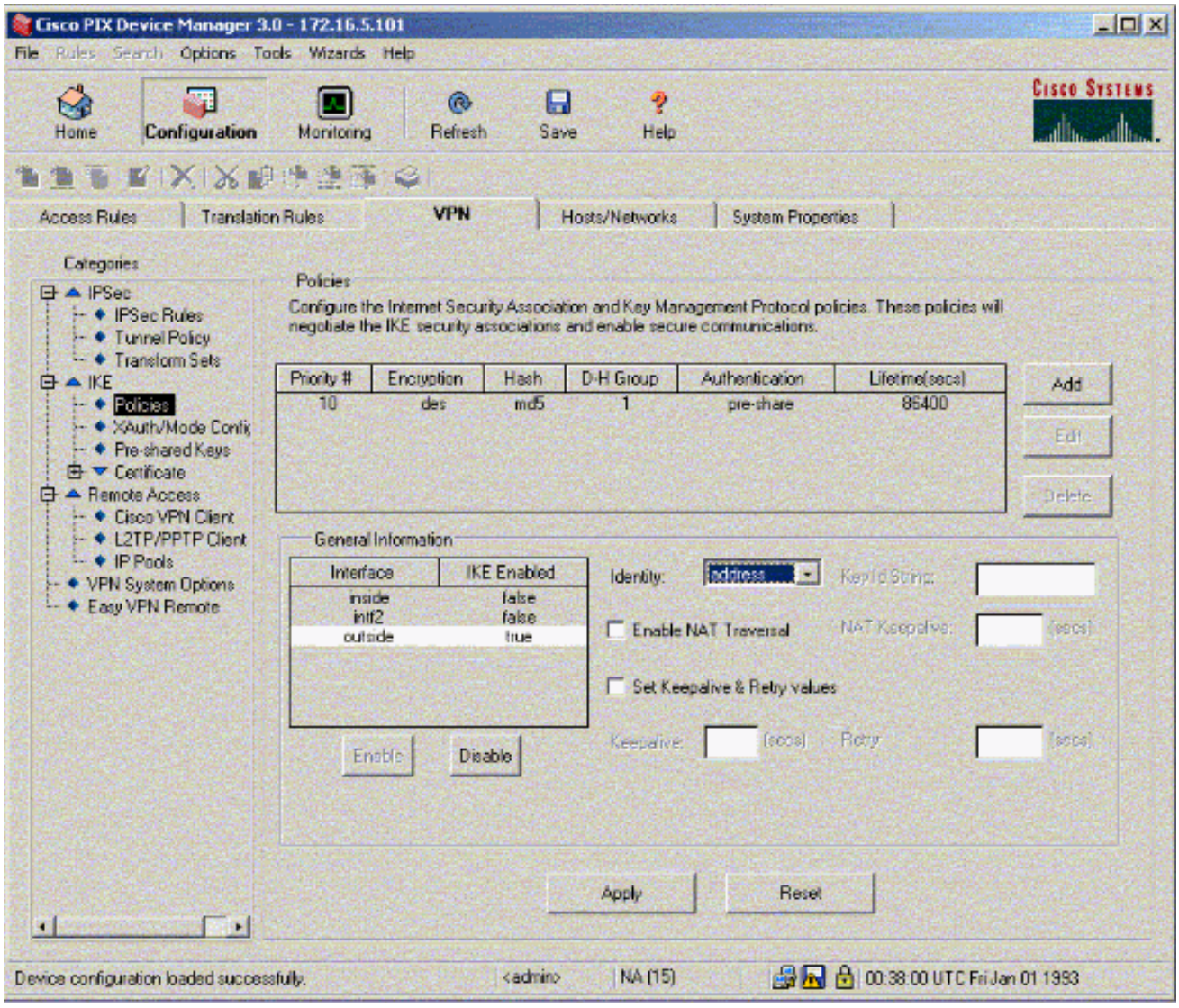
8. Fare clic su **Add** (Aggiungi) e compilare i campi appropriati.



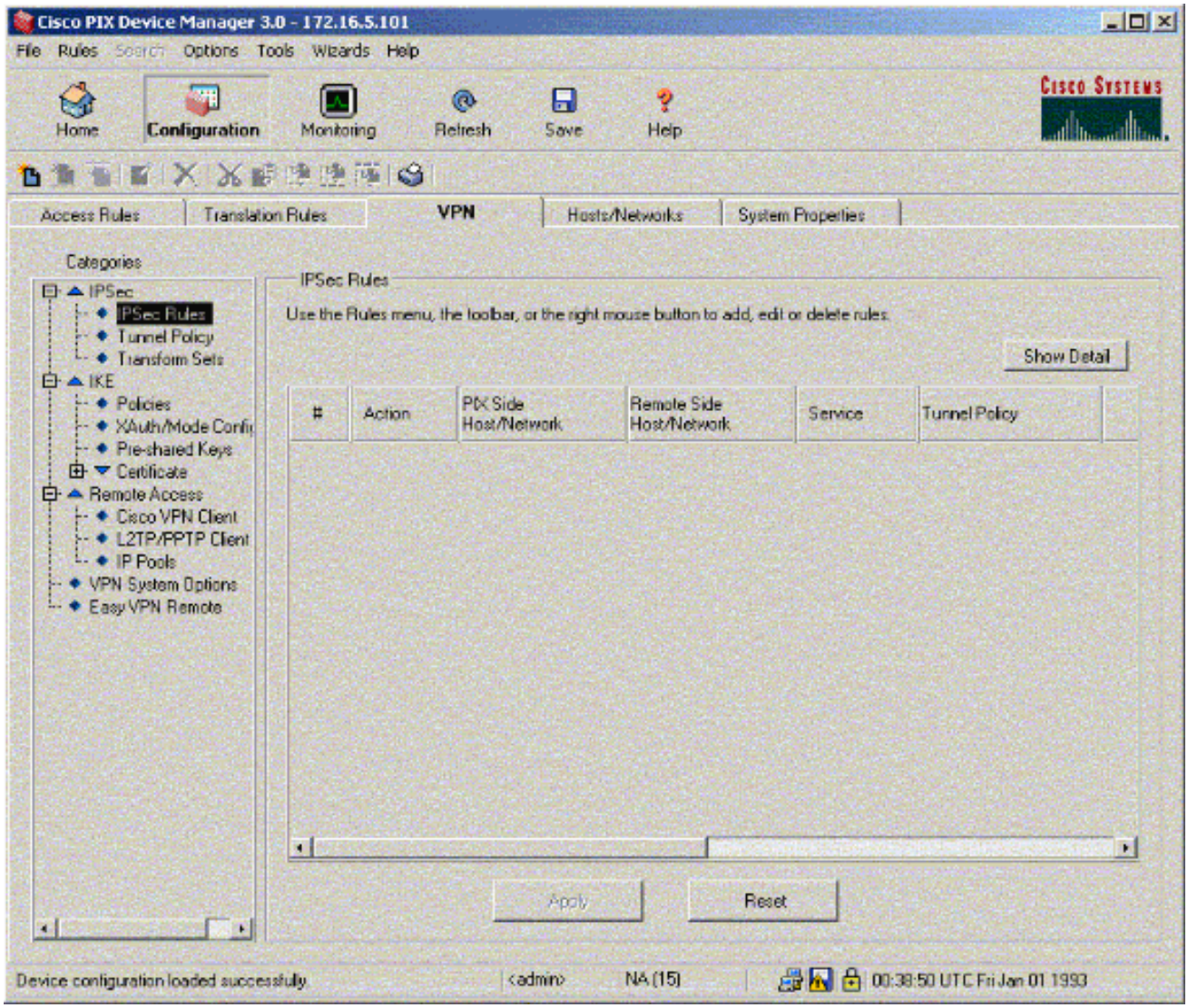
9. Fare clic su **OK** per aggiungere un nuovo criterio.



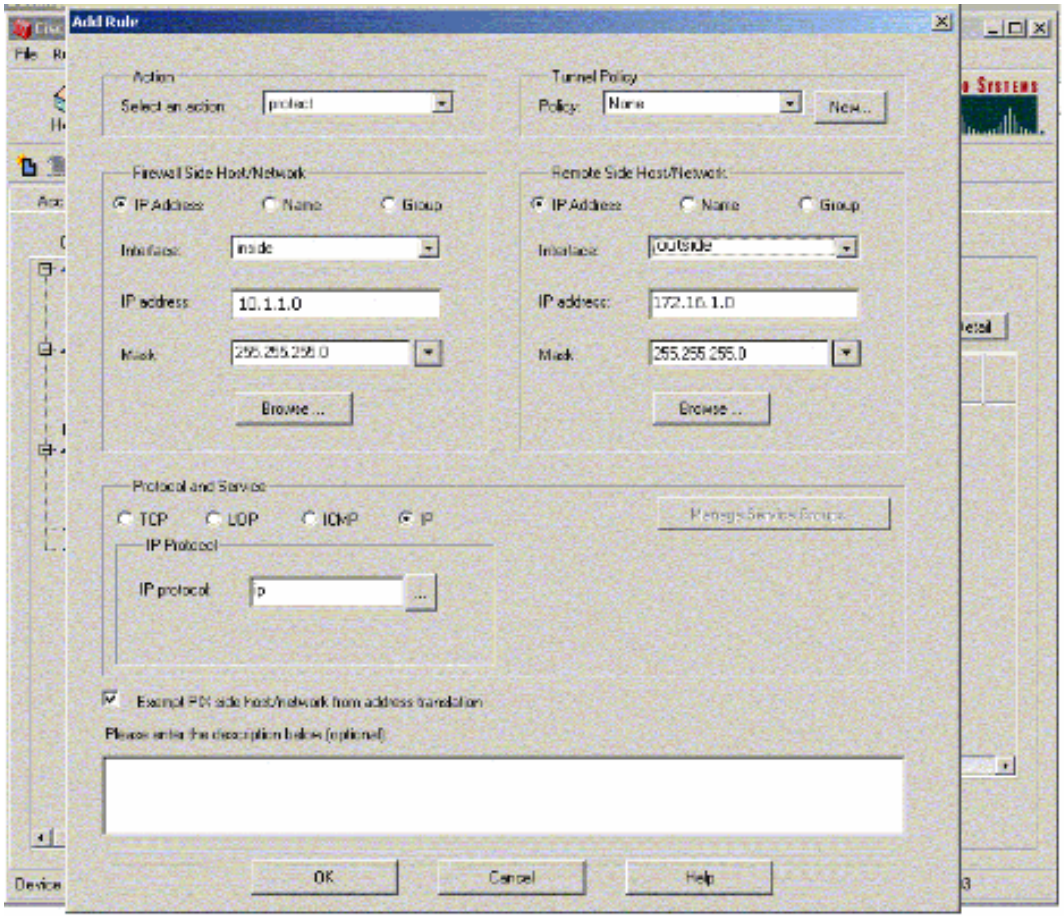
10. Selezionare l'interfaccia **esterna**, fare clic su **Attiva**, quindi dal menu a discesa Identità selezionare
indirizzo.



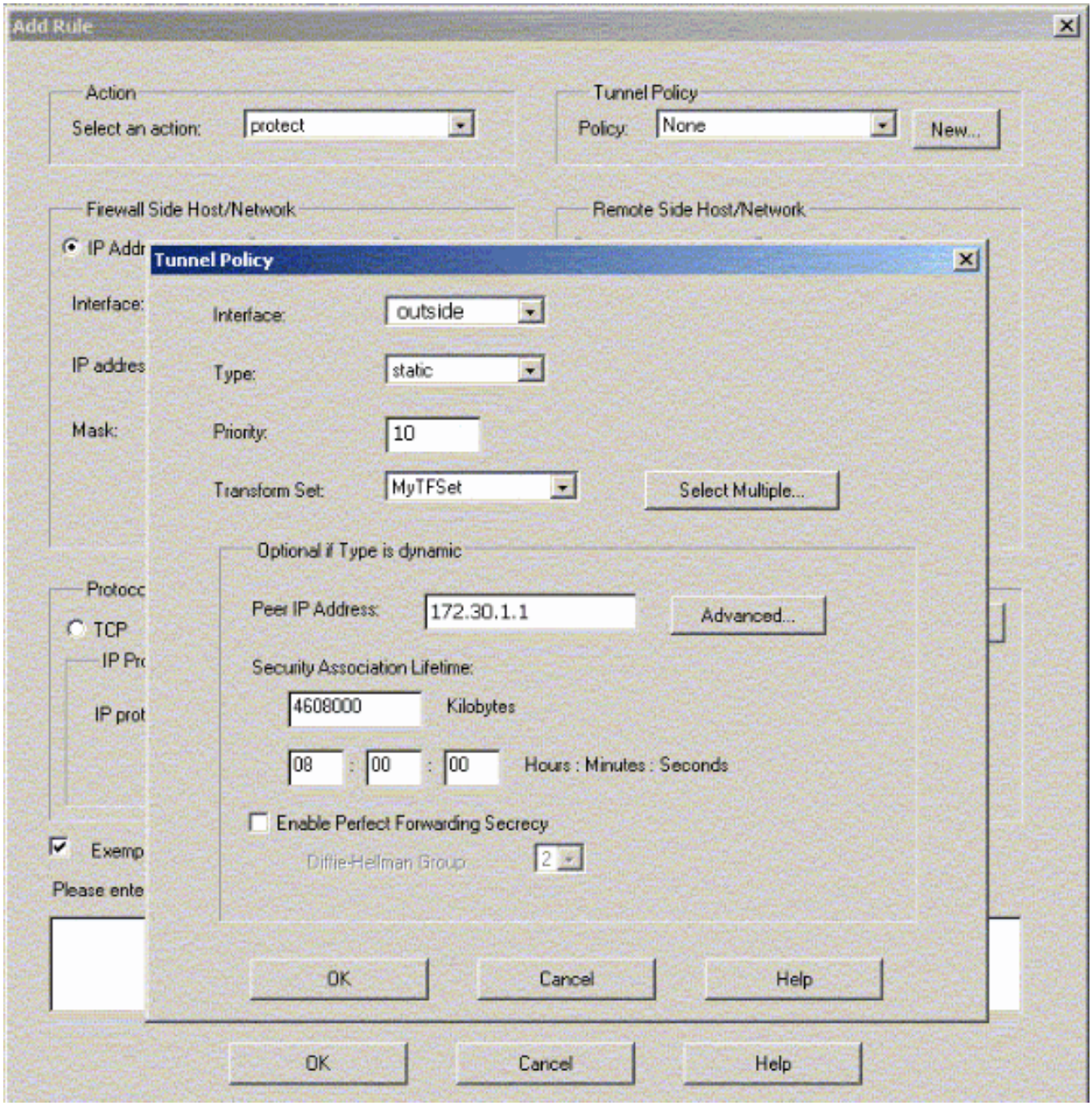
11. Fare clic su **Regole IPSec** in IPSec per creare le regole IPSec.



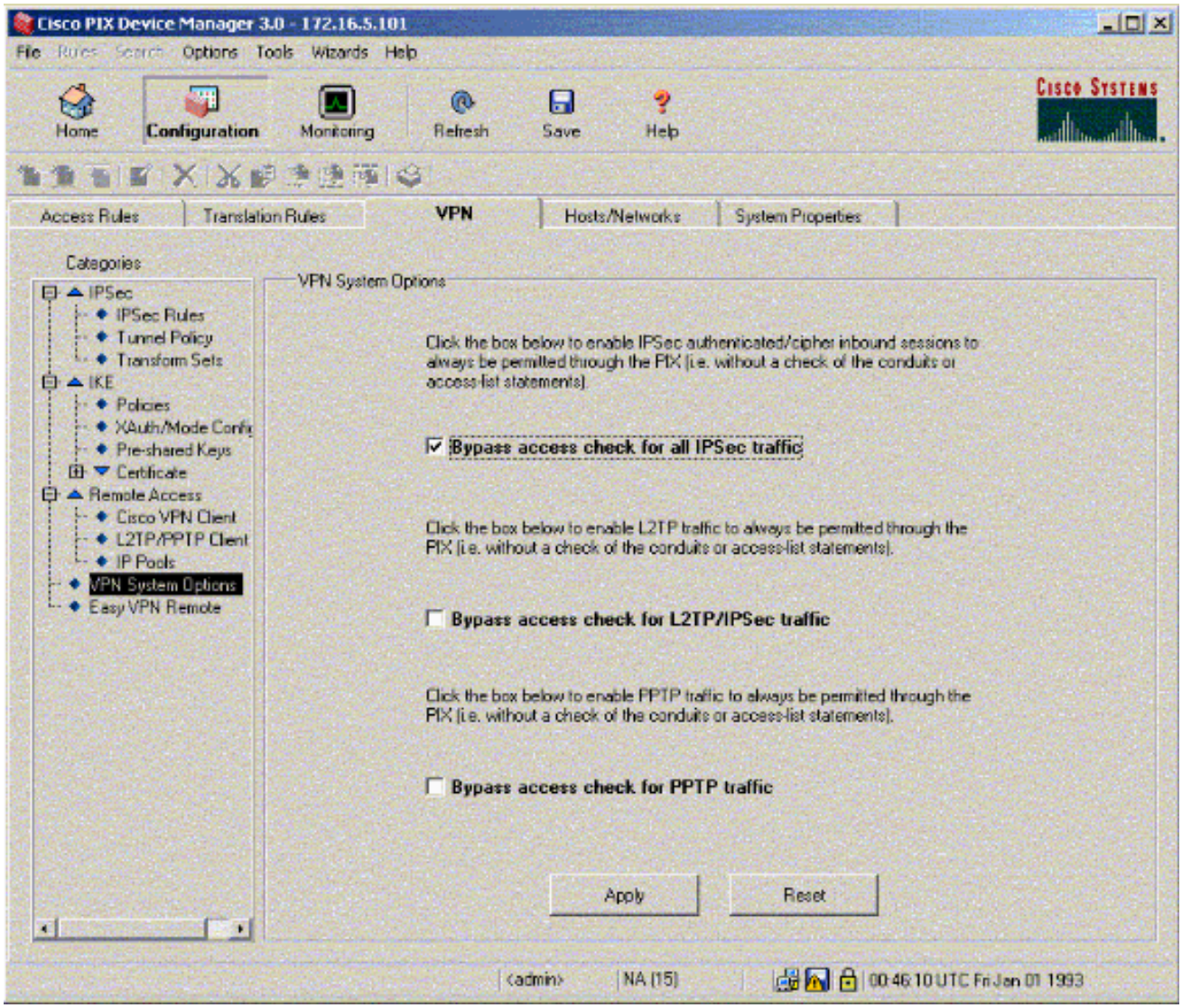
12. Compilare i campi appropriati.



13. Fare clic su **Nuovo** in Criteri tunnel. Viene visualizzata la finestra Criteri tunnel. Compilare i campi
appropriati.



14. Fare clic su **OK** per visualizzare la regola IPSec configurata.
15. Fare clic su **VPN Systems Options** (Opzioni di sistema VPN) e selezionare **Bypass access check (Ignora controllo accesso) per tutto il traffico IPSec**.

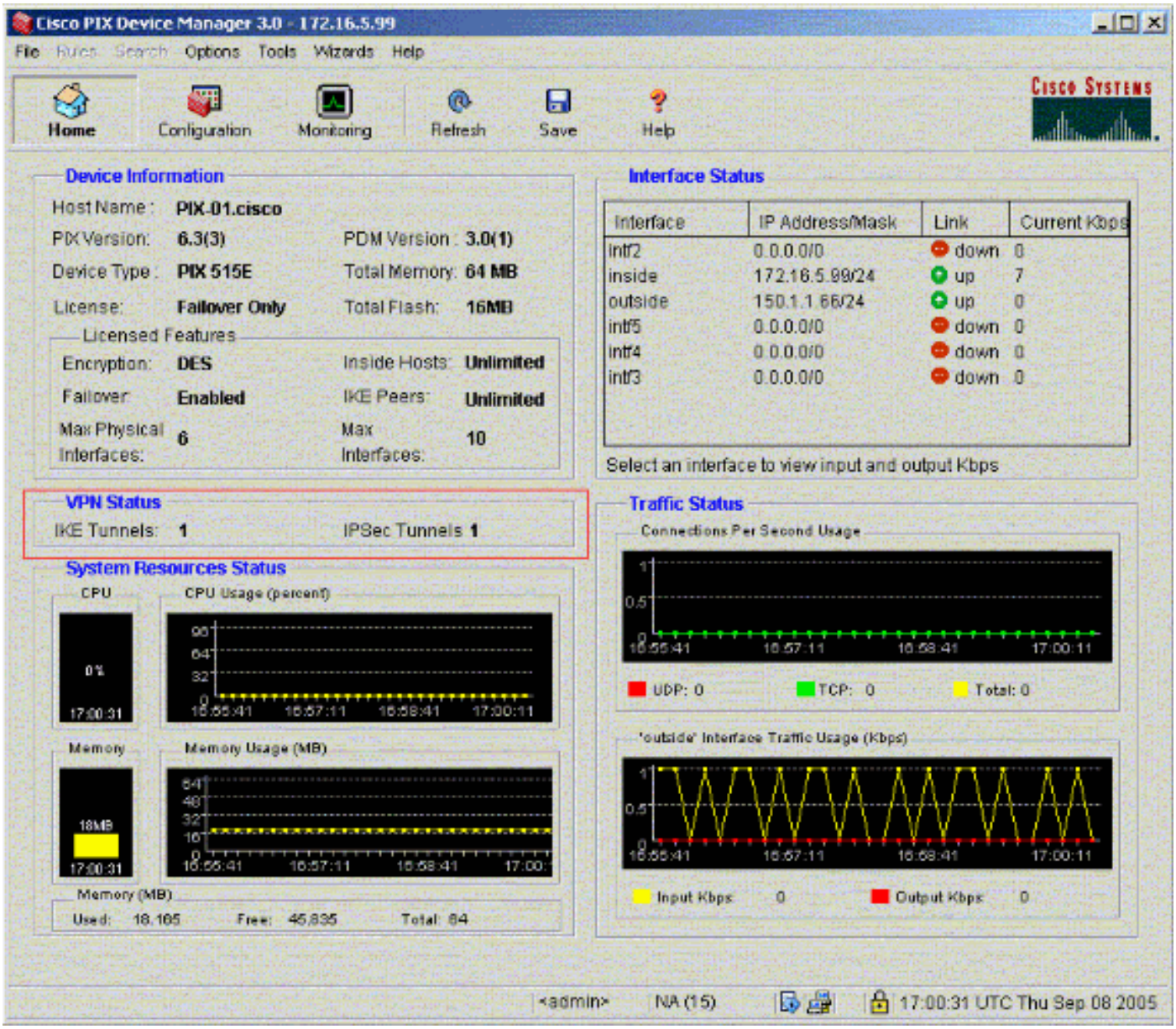


Verifica

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

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

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



Èinoltre 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.

Nota: non è possibile eseguire il ping dell'interfaccia interna del PIX per la formazione del tunnel a meno che il comando management-access non sia configurato in modalità di conferma globale.

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

Risoluzione dei problemi

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

Informazioni correlate

- Creazione di tunnel ridondanti tra firewall tramite PDM

- Riferimenti per i comandi di Cisco Secure PIX Firewall
- RFC (Requests for Comments)
- Software Cisco PIX Firewall