Ejemplo de Configuración de Túnel VPN de LAN a LAN entre Dos PIX que Utilizan PDM

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Diagrama de la red
Convenciones
Antecedentes
Procedimiento de Configuración
Verificación
Troubleshoot
Información Relacionada

Introducción

Este documento describe el procedimiento para configurar túneles VPN entre dos firewalls PIX utilizando Cisco PIX Device Manager (PDM). PDM es una herramienta de configuración basada en navegador diseñada para ayudarle a configurar, configurar y monitorear su PIX Firewall con una GUI. Los firewalls PIX se colocan en dos sitios diferentes.

Un túnel se forma usando IPSec. IPSec es una combinación de estándares abiertos que proporcionan confidencialidad de datos, integridad de datos y autenticación de origen de datos entre peers IPSec.

Prerequisites

Requirements

No hay requisitos para este documento.

Componentes Utilizados

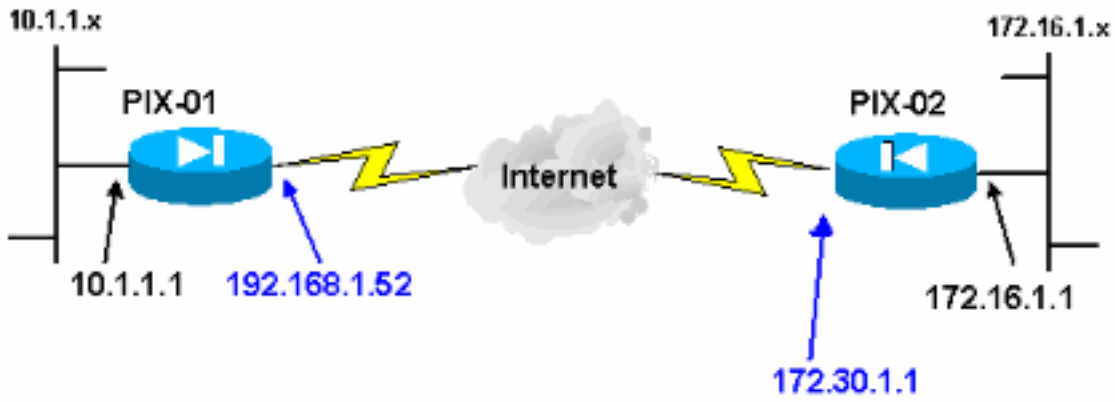
La información de este documento se basa en los firewalls Cisco Secure PIX 515E con 6.x y PDM versión 3.0.

Consulte Configuración de un Túnel VPN PIX a PIX Simple Usando IPSec para ver un ejemplo de configuración en la configuración de un túnel VPN entre dos dispositivos PIX usando la Interfaz de Línea de Comandos (CLI).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

La negociación IPSec se puede dividir en cinco pasos e incluye dos fases de intercambio de claves de Internet (IKE).

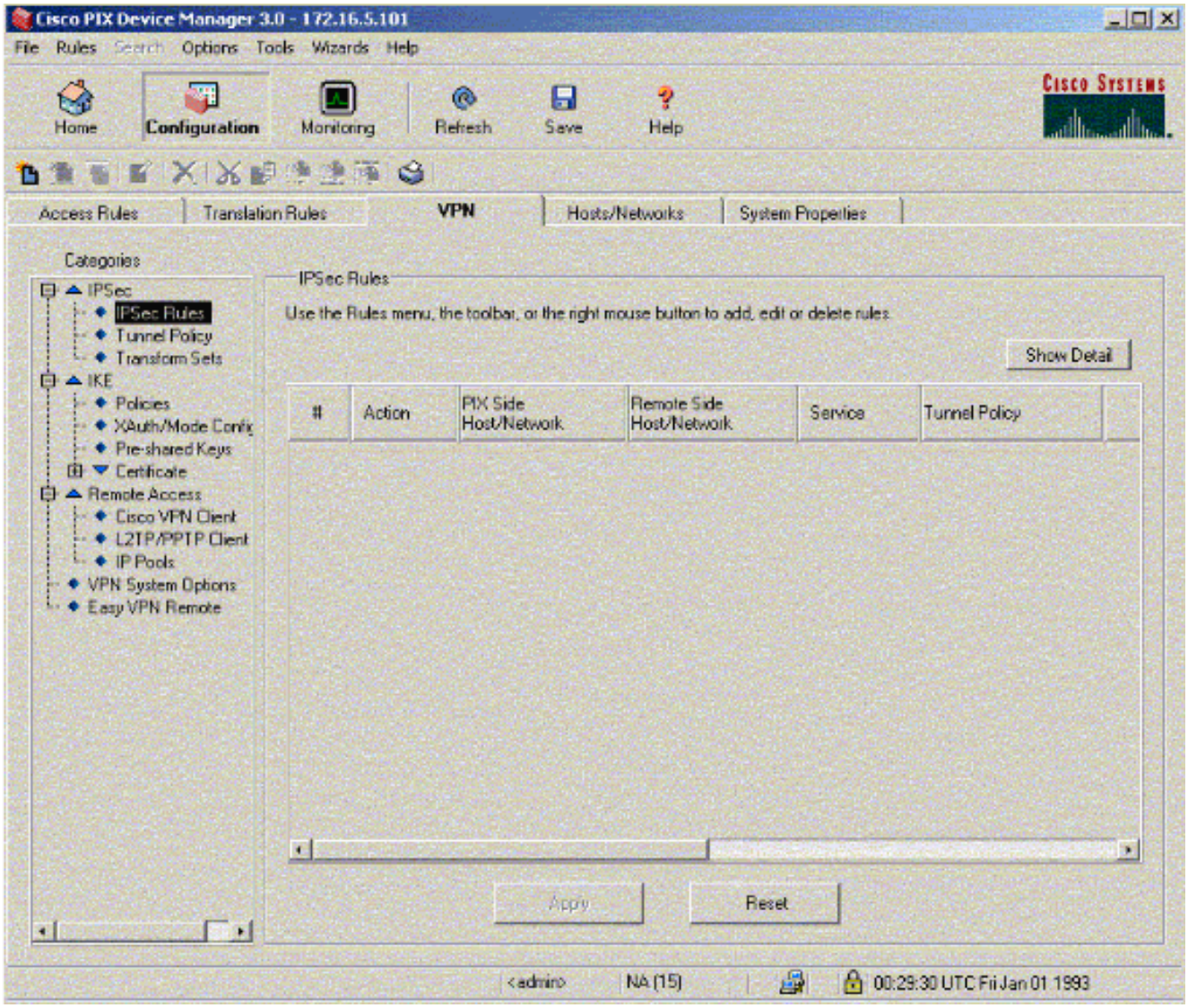
1. Un túnel IPSec es iniciado por un tráfico interesado. Se considera que el tráfico es interesante cuando se transmite entre los pares IPSec.
2. En la Fase 1 IKE, las entidades pares IPSec negocian la política establecida de la Asociación de seguridad (SA) IKE. Una vez que se autentican los pares, se crea un túnel seguro por medio de la Asociación de Seguridad en Internet y del Protocolo de administración de clave (ISAKMP).
3. En la fase 2 de IKE, los pares IPSec usan el túnel autenticado y seguro para negociar las transformaciones de IPSec SA. La negociación de la política compartida determina el modo en que se establece el túnel IPSec.
4. Se crea el túnel IPSec y los datos se transfieren entre los pares IPSec según los parámetros IPSec configurados en los conjuntos de transformaciones de IPSec.
5. El túnel IPSec termina cuando los IPSec SAs son borrados o cuando caduca su vigencia.**Nota:** La negociación IPSec entre los dos PIX falla si las SA en ambas fases IKE no coinciden en los pares.

Procedimiento de Configuración

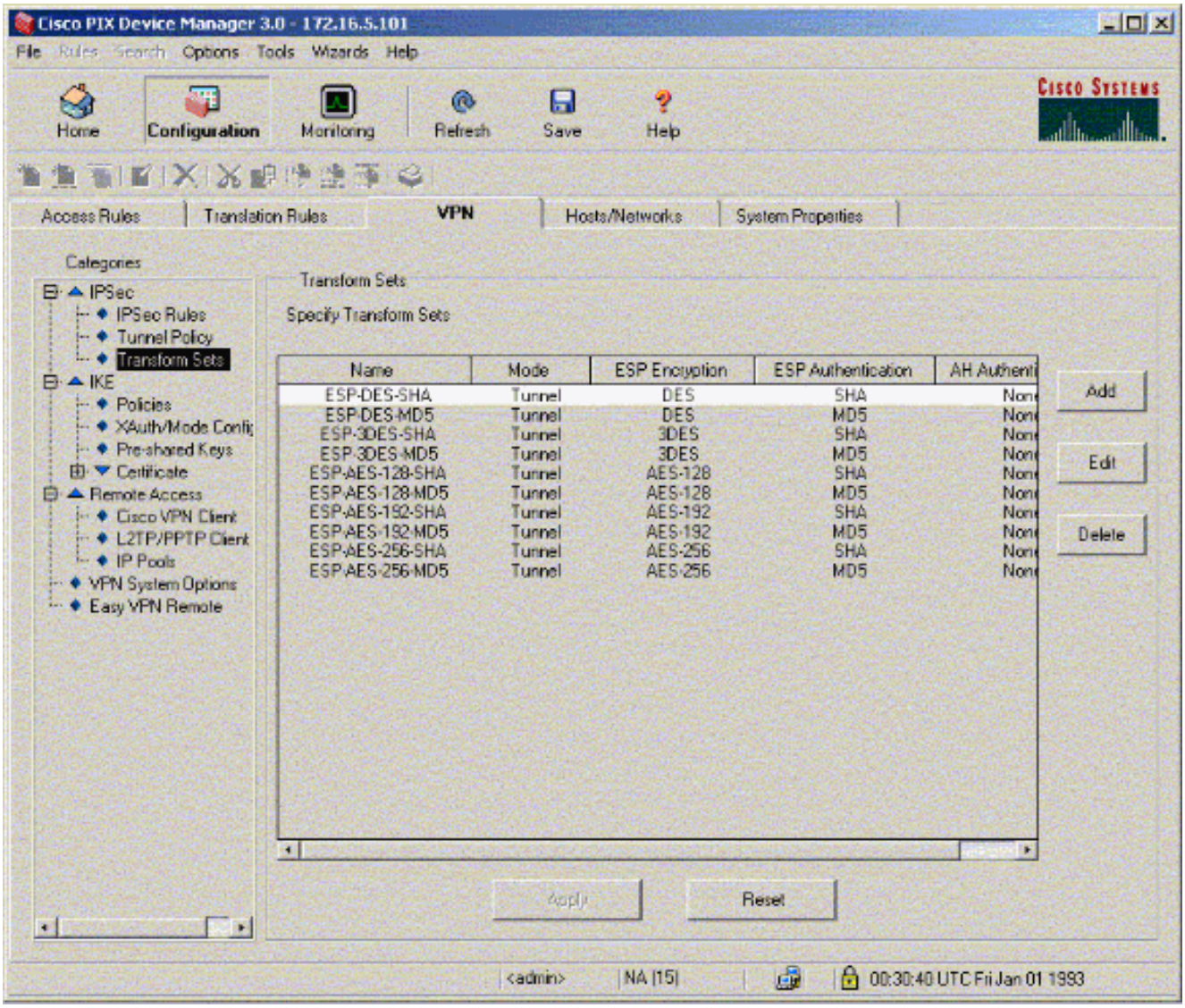
Aparte de otra configuración general en la CLI de PIX para acceder a ella a través de la interfaz Ethernet 0, utilice los comandos **http server enable** y **http server <local_ip> <mask> <interface>** donde *<local_ip>* y **<mask>** es la dirección IP y la máscara de la estación de trabajo en la que está instalado PDM. La configuración en este documento es para PIX-01. PIX-02 se puede configurar usando los mismos pasos con diferentes direcciones.

Complete estos pasos:

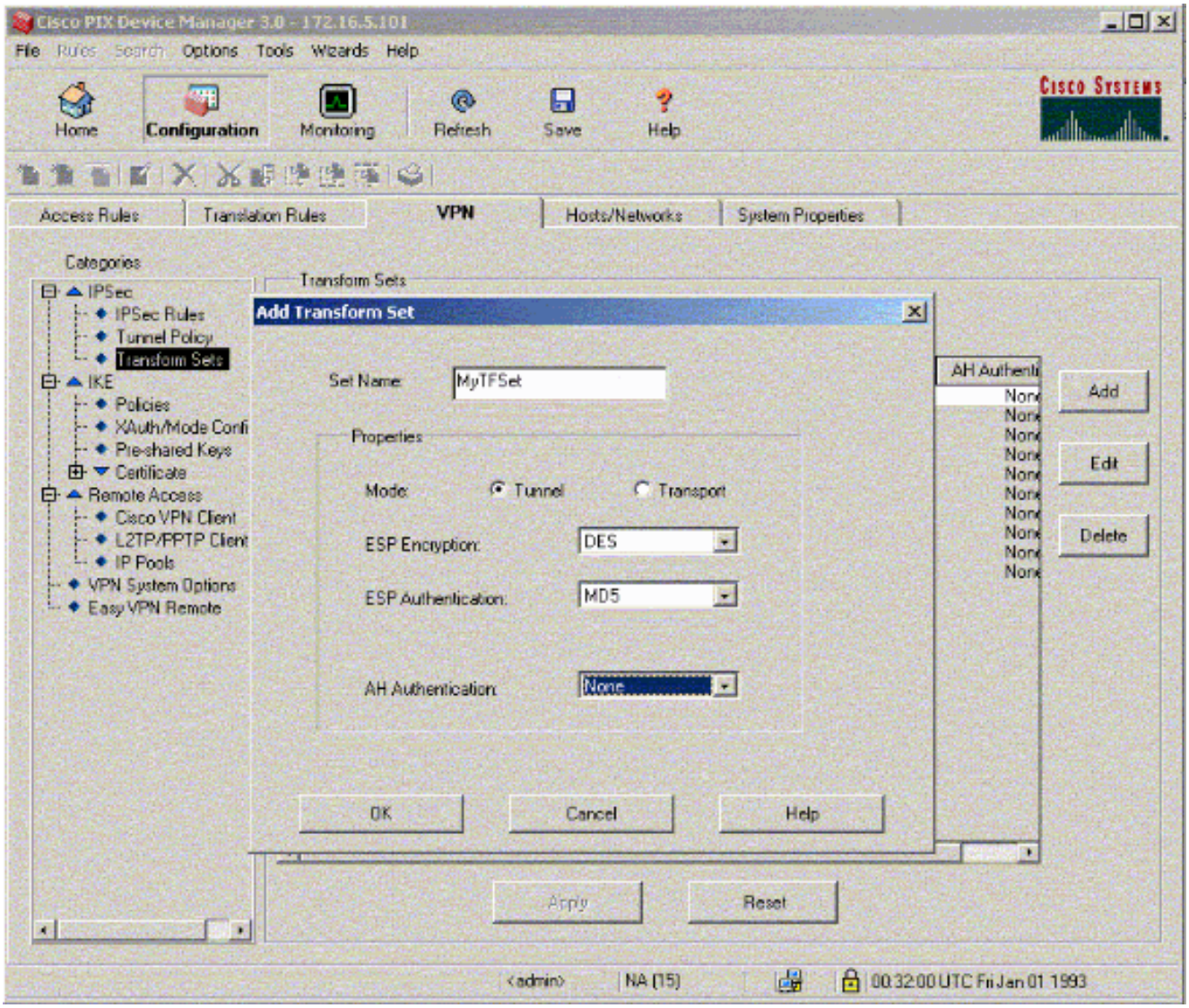
1. Abra su navegador y escriba **https://<Inside_IP_Address_of_PIX>** para acceder al PIX en PDM.
2. Haga clic en **Configuration** y vaya a la ficha VPN.



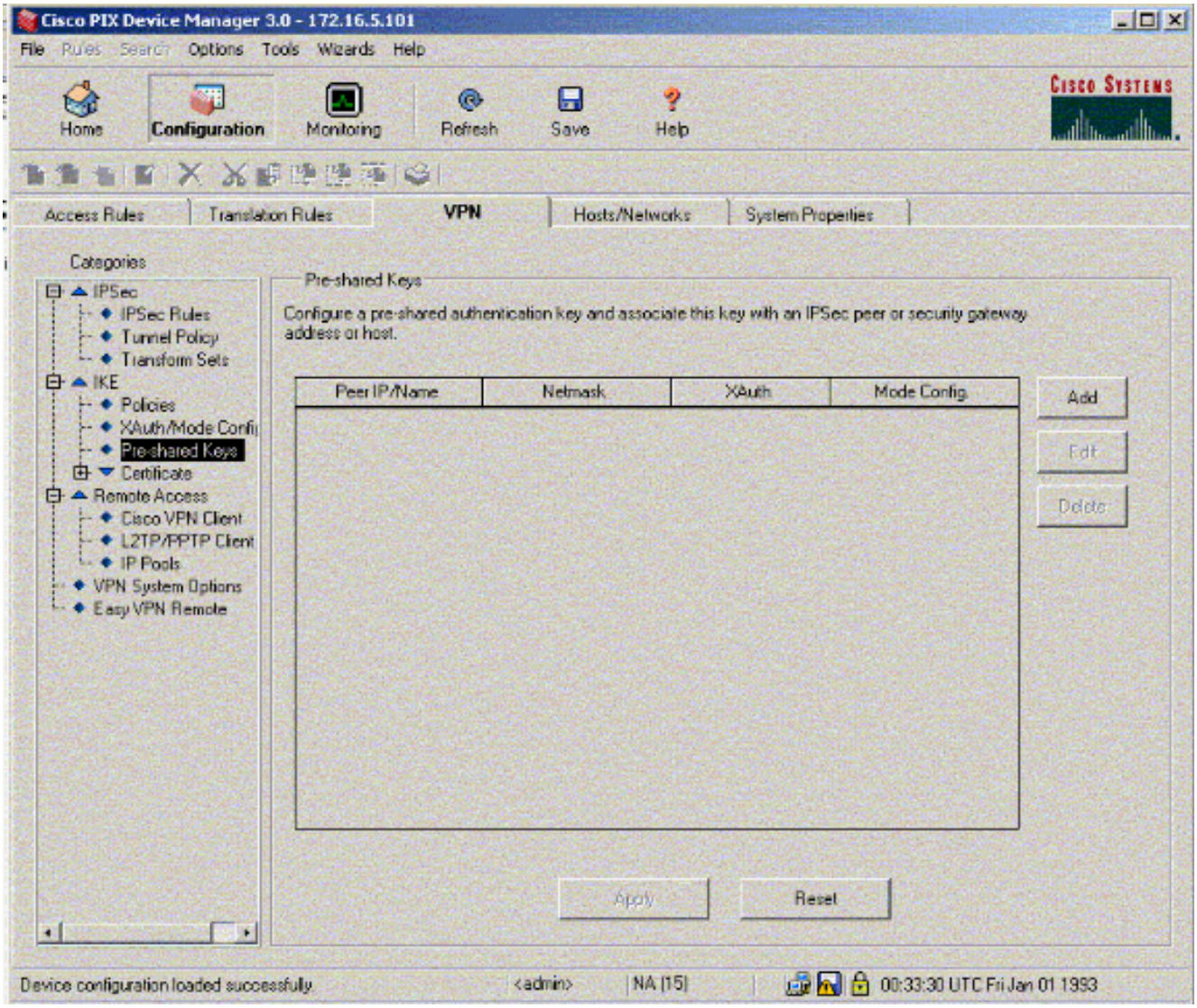
3. Haga clic en **Transformar conjuntos** en IPSec para crear un conjunto de transformación.



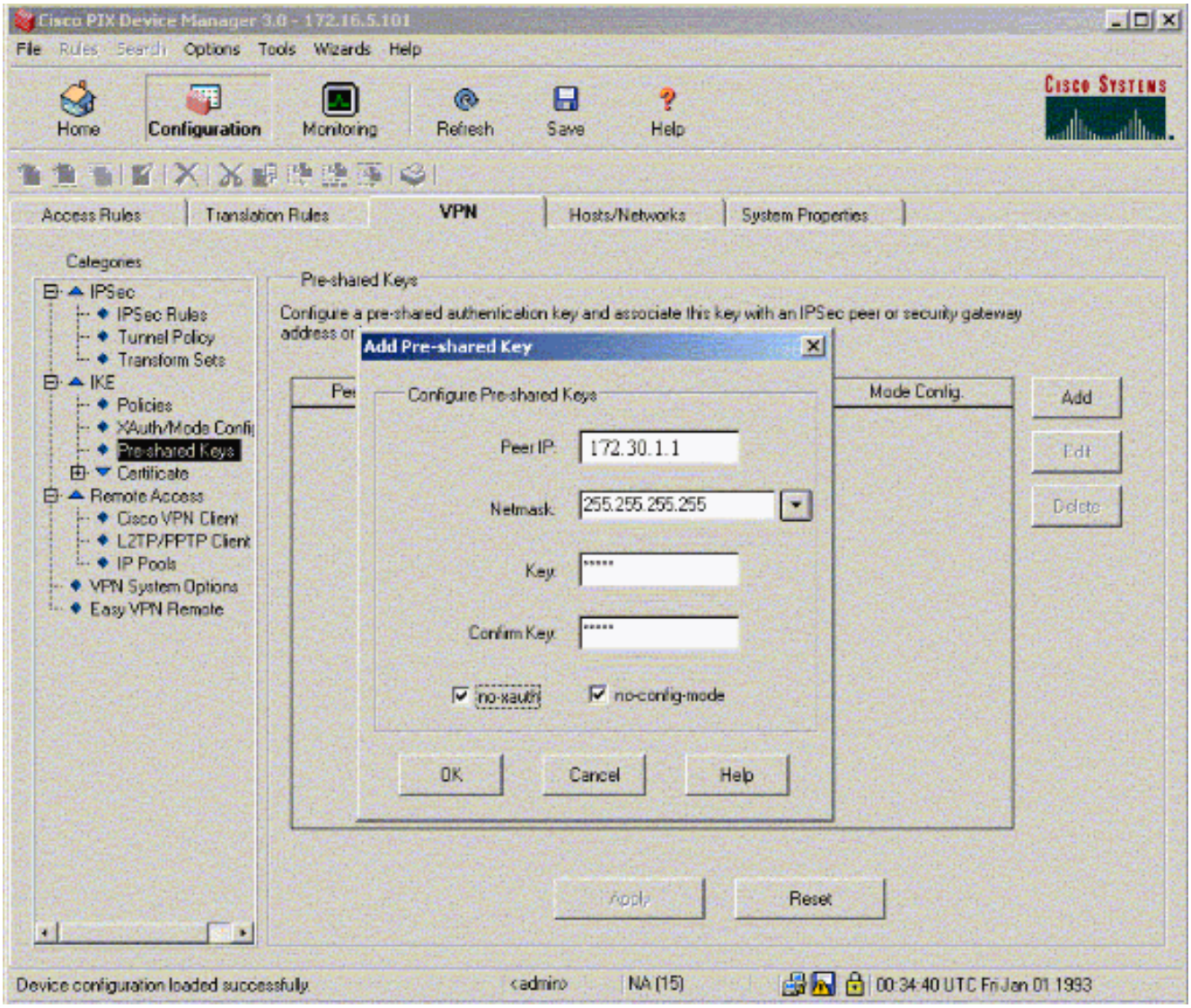
4. Haga clic en **Agregar**, seleccione todas las opciones apropiadas y haga clic en **Aceptar** para crear un nuevo conjunto de transformación.



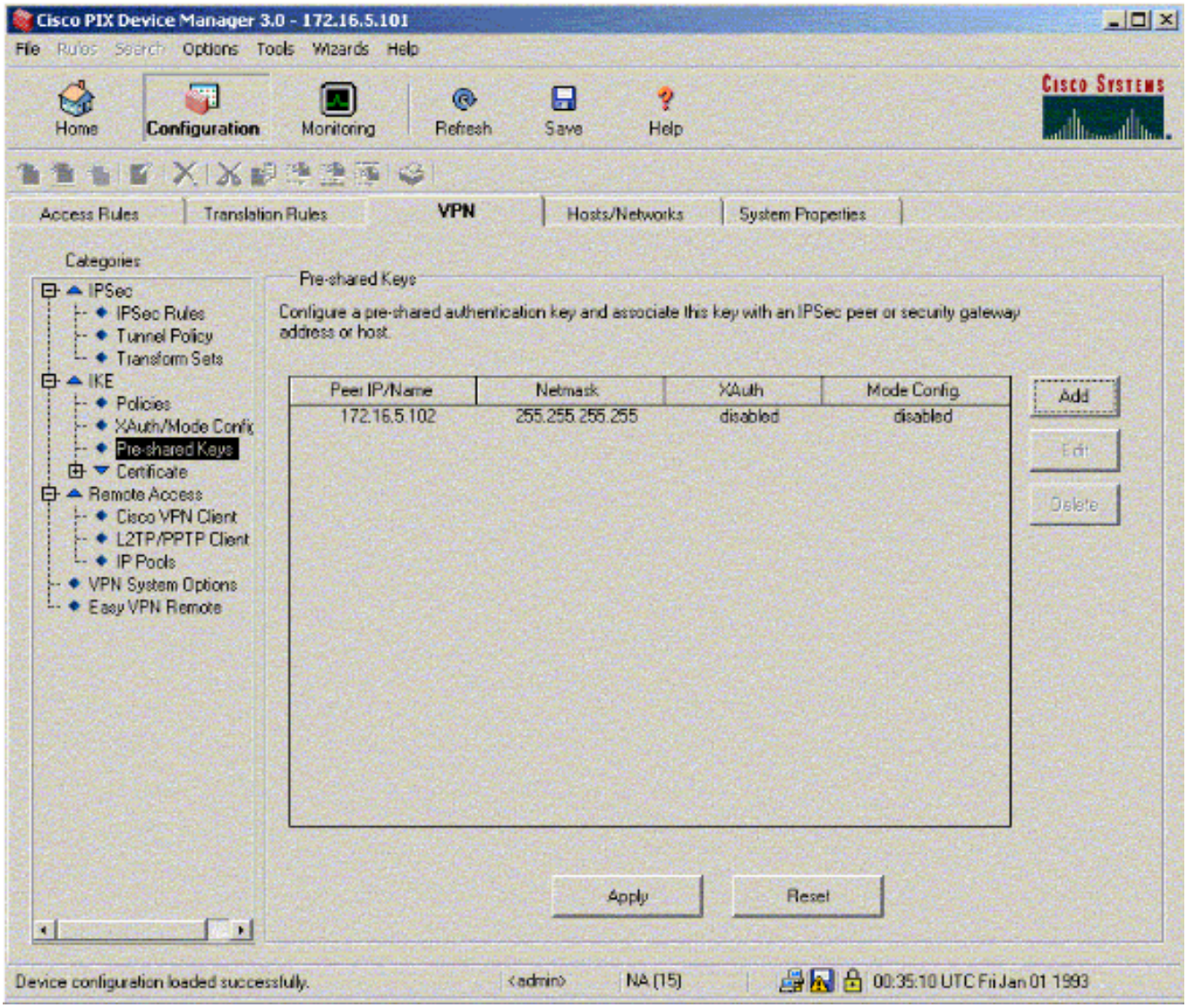
5. Haga clic en **Pre-Shared Keys** en IKE para configurar claves previamente compartidas.



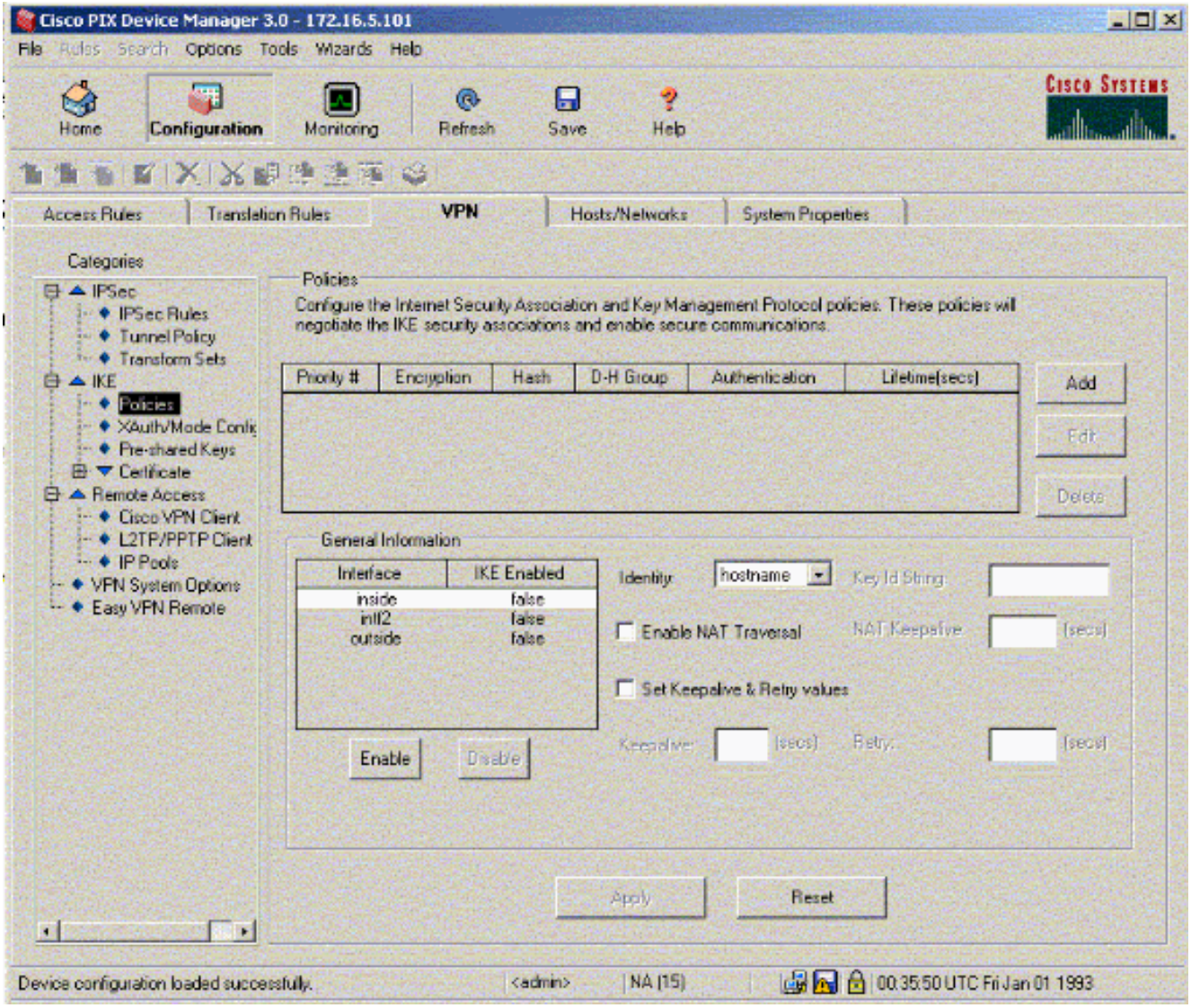
6. Haga clic en **Agregar** para agregar una nueva clave previamente compartida.



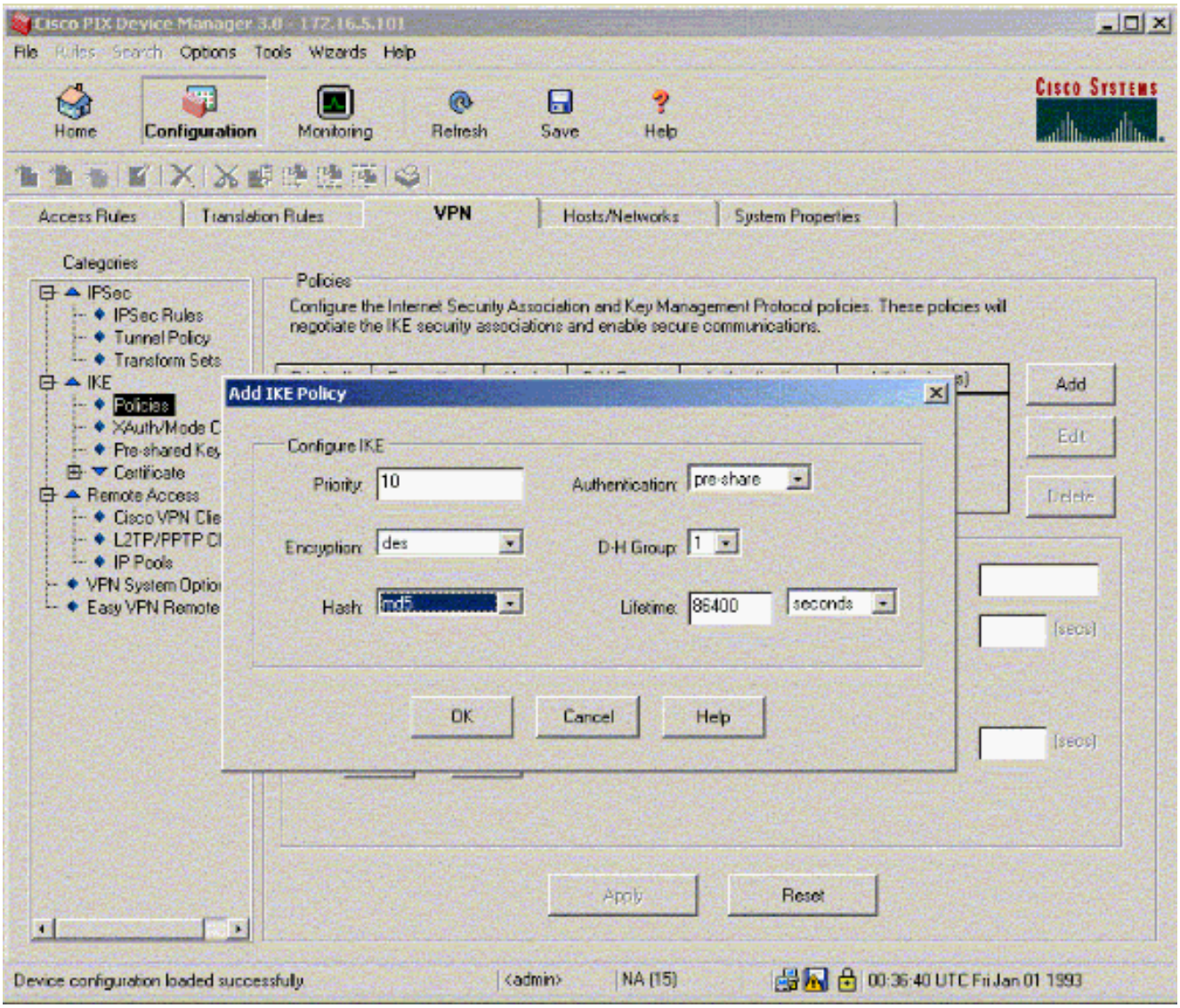
Esta ventana muestra la clave, que es la contraseña para la asociación de túnel. Esto tiene que coincidir en ambos lados del
túnel.



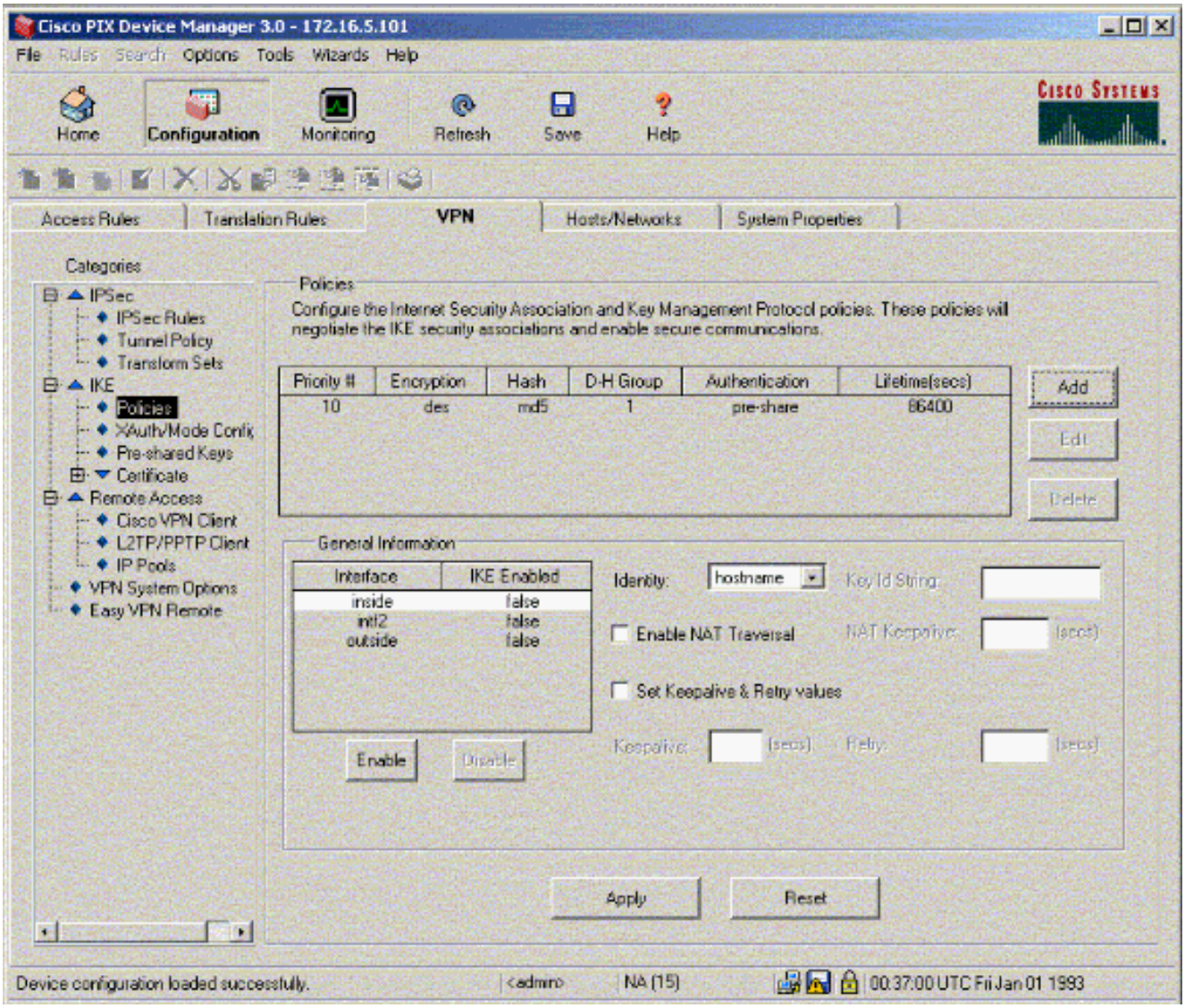
7. Haga clic en **Políticas** en IKE para configurar las políticas.



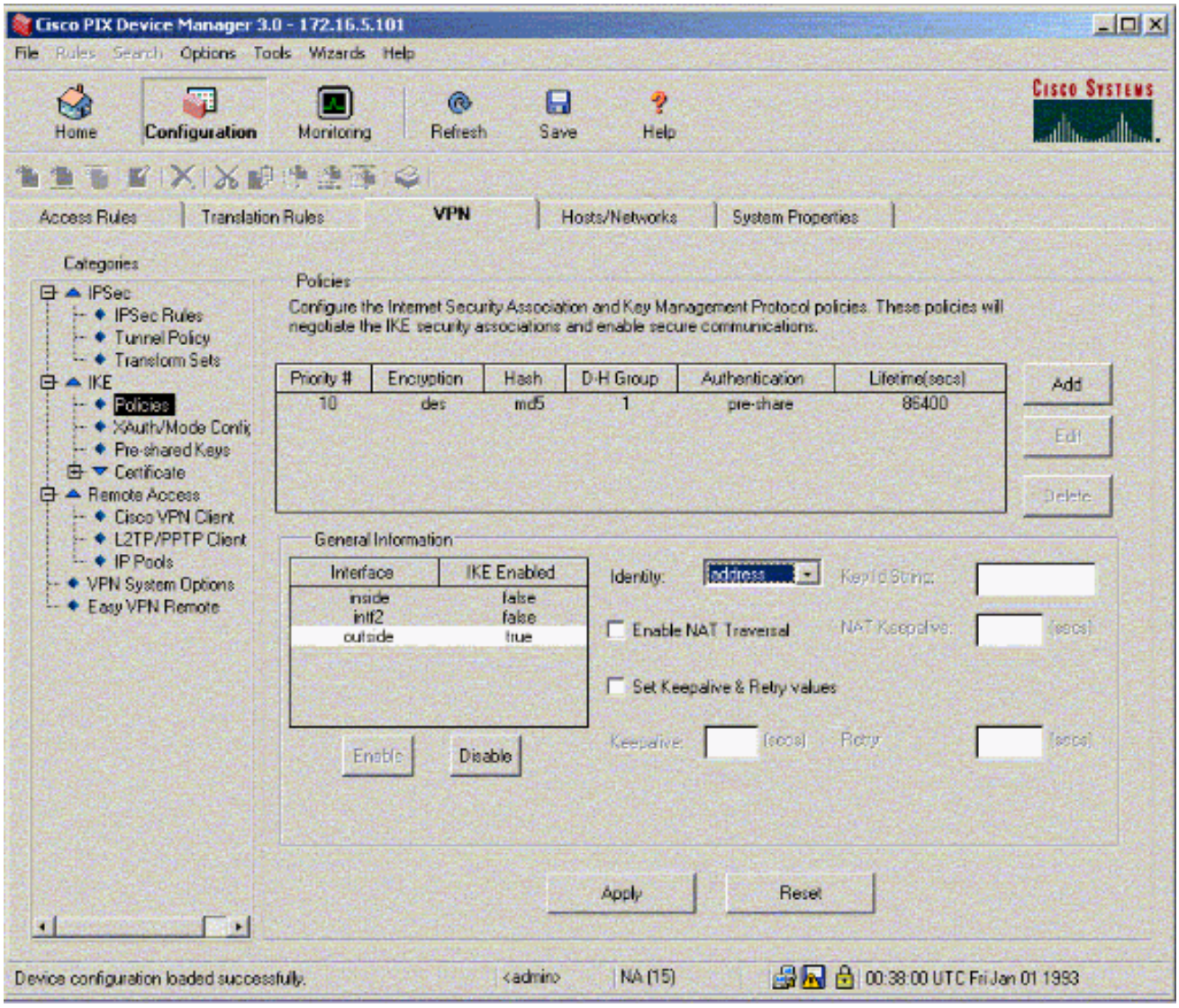
8. Haga clic en **Agregar** y rellene los campos correspondientes.



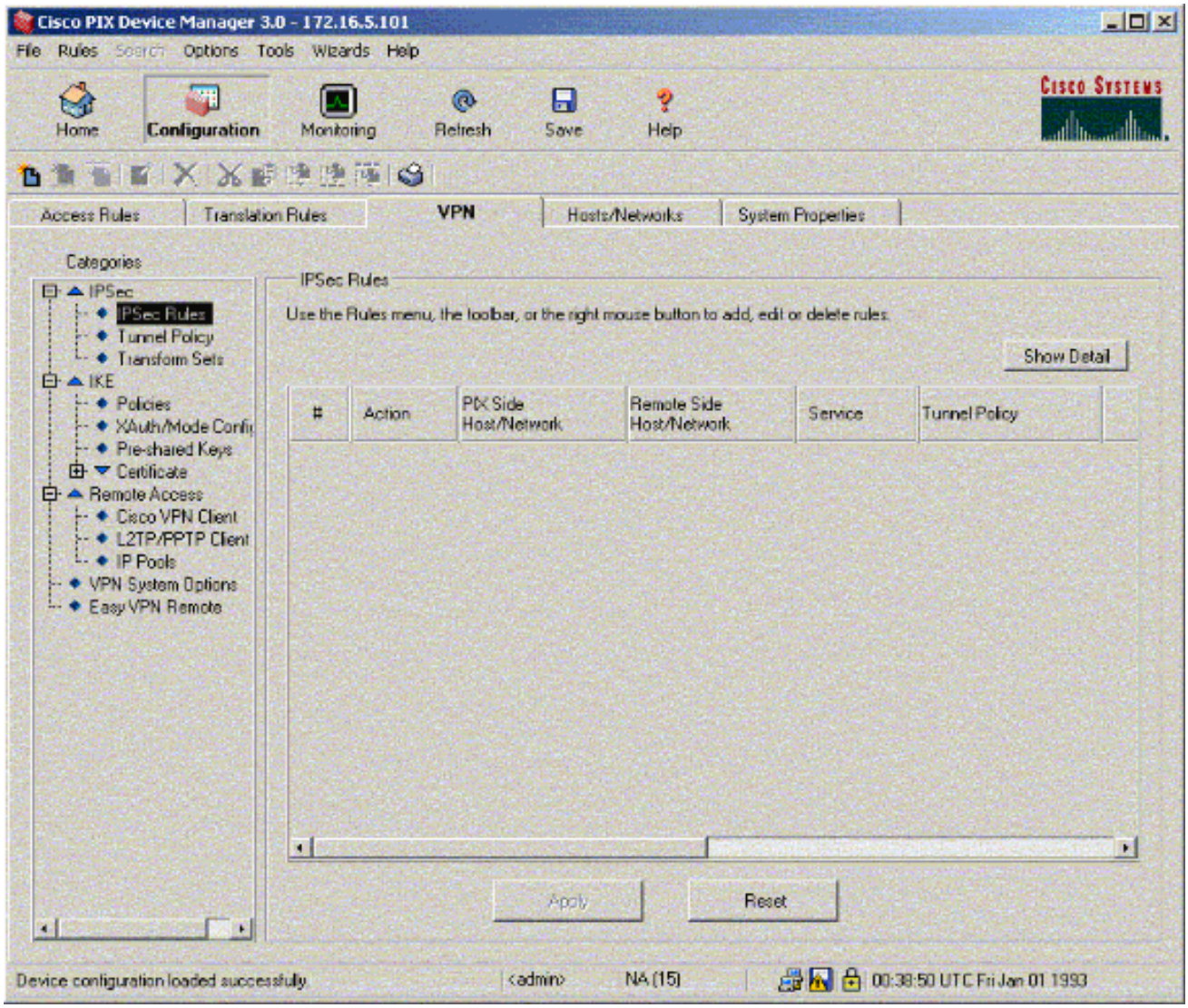
9. Haga clic en **Aceptar** para agregar una nueva política.



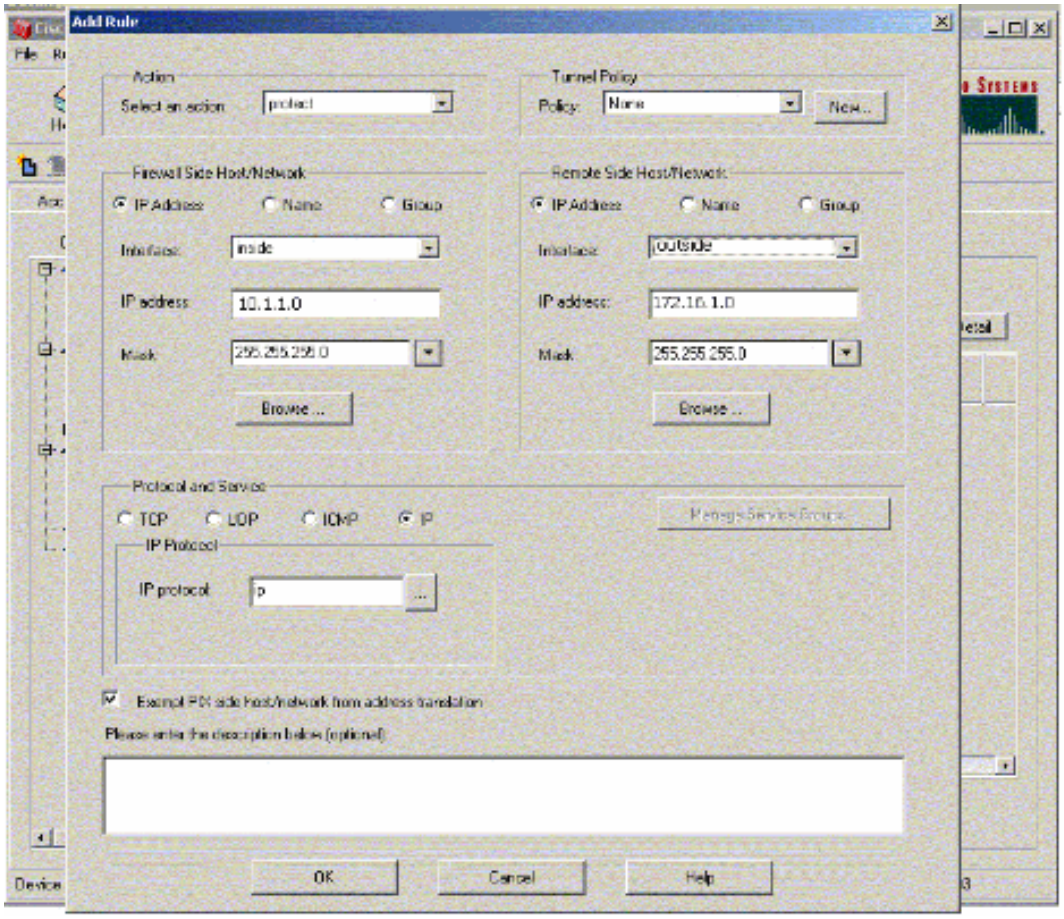
10. Seleccione la interfaz **externa**, haga clic en **Enable** y, en el menú desplegable Identity, seleccione **address**.



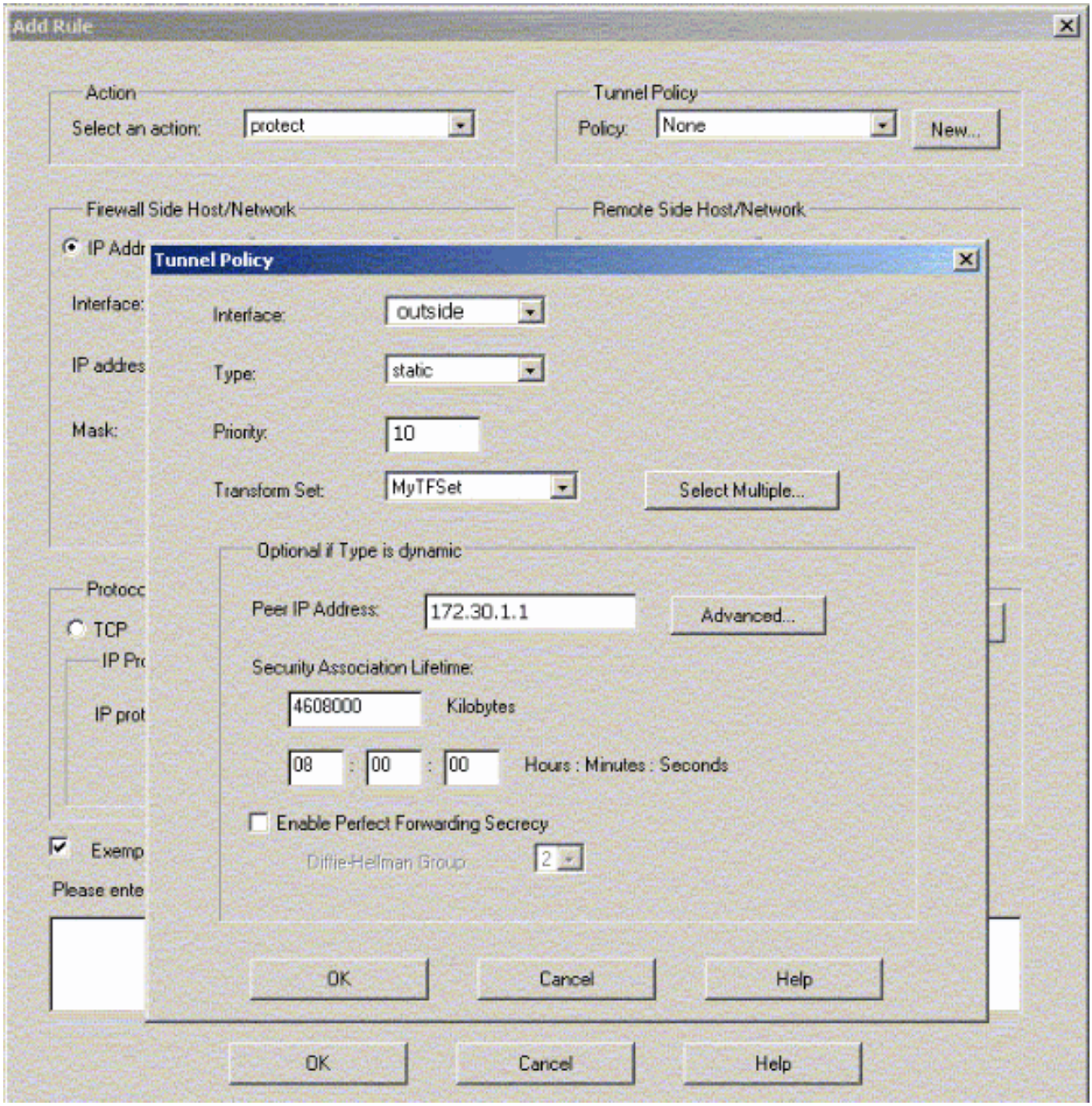
11. Haga clic en **Reglas IPSec** en IPSec para crear reglas IPSec.



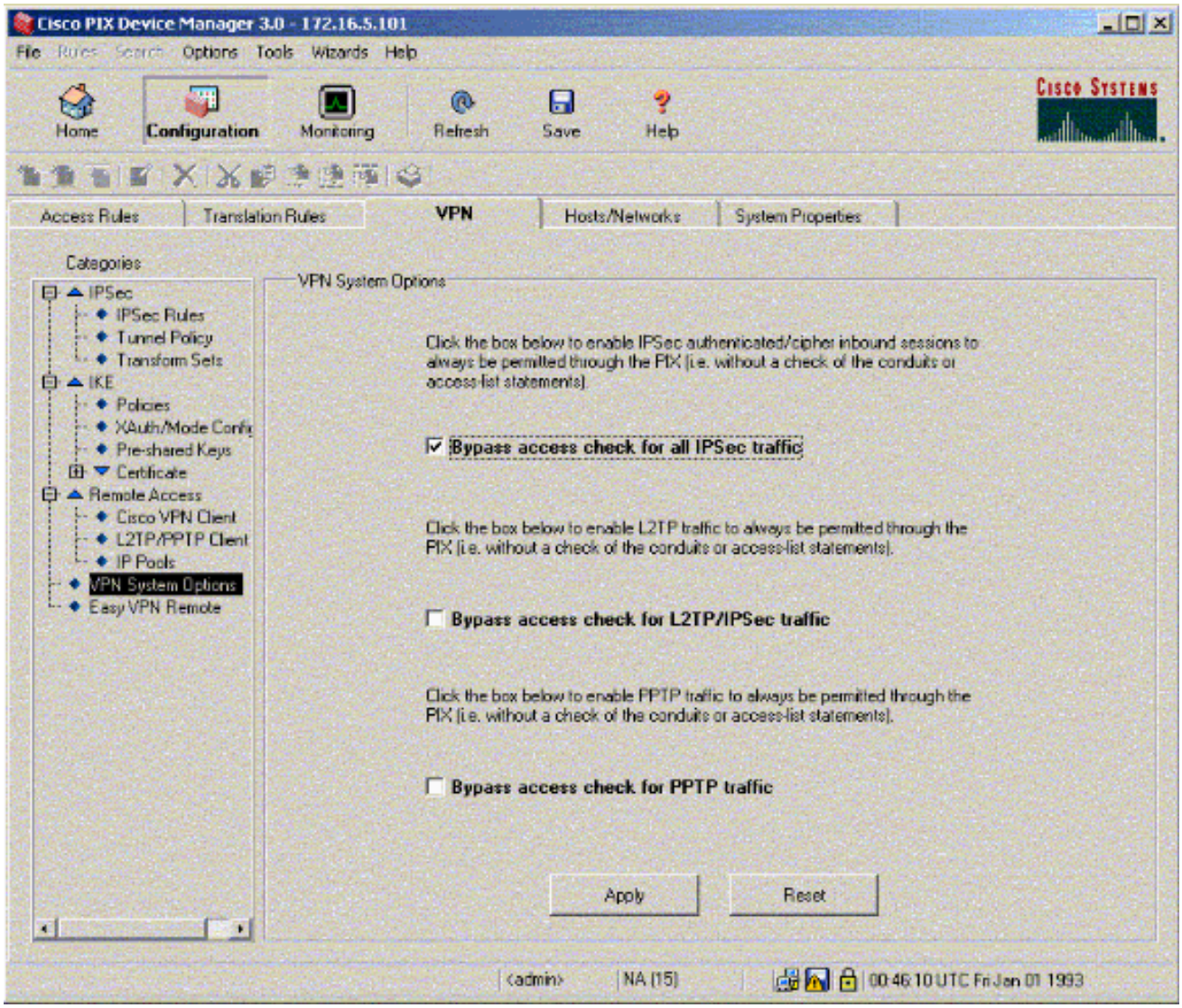
12. Rellene los campos correspondientes.



13. Haga clic en **Nuevo** en la Política de Túnel. Aparece una ventana Tunnel Policy . Rellene los campos correspondientes.



14. Haga clic en **Aceptar** para ver la regla IPsec configurada.
15. Haga clic en **Opciones de sistemas VPN** y marque **Omitir verificación de acceso para todo el tráfico IPSec**.

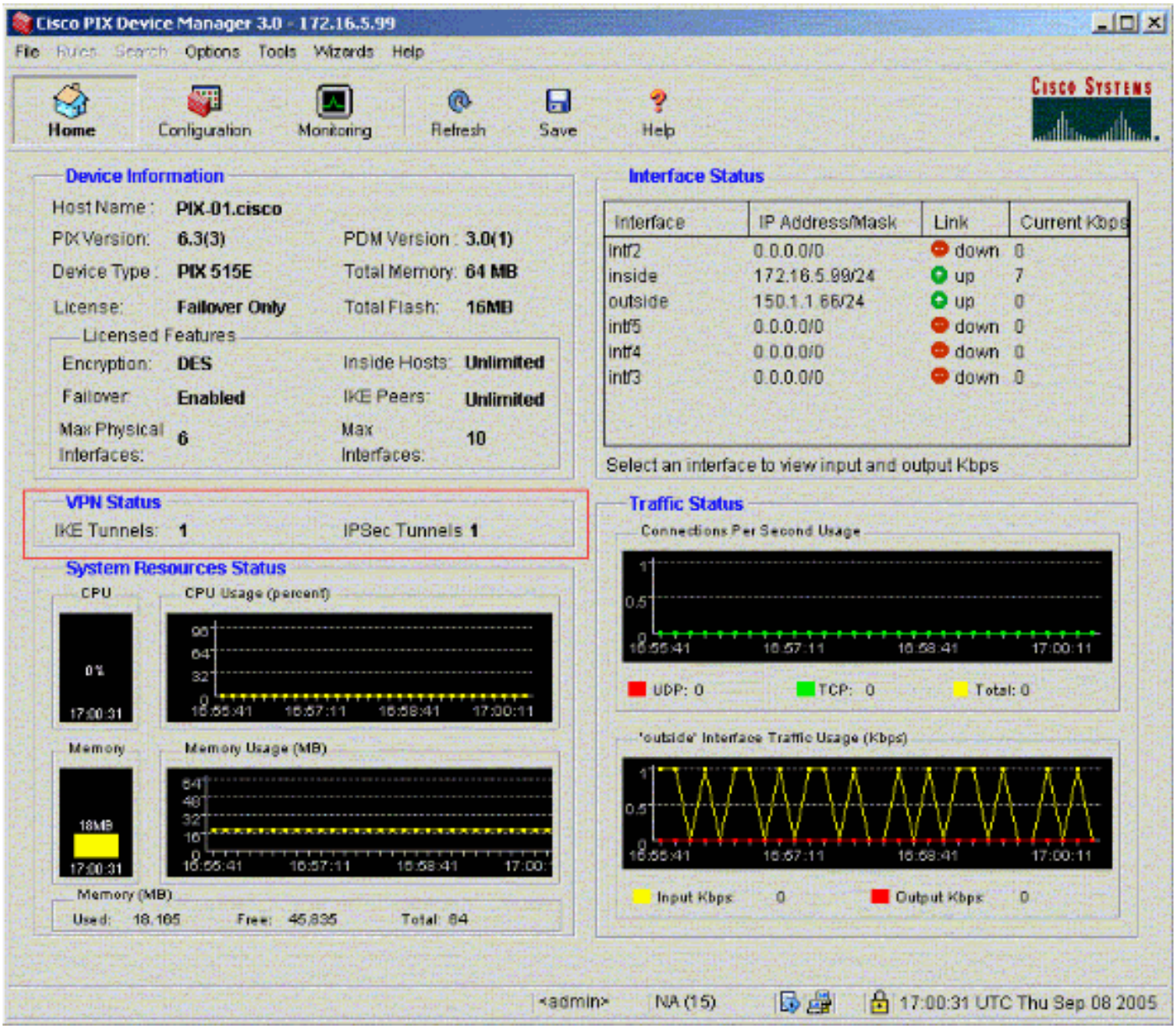


Verificación

Si hay tráfico interesante al par, el túnel se establece entre PIX-01 y PIX-02.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Vea el estado de VPN en Inicio en el PDM (resaltado en rojo) para verificar la formación del túnel.



También puede verificar la formación de túneles mediante CLI en Herramientas en el PDM. Ejecute el comando **show crypto isakmp sa** para verificar la formación de túneles y ejecute el comando **show crypto ipsec sa** para observar el número de paquetes encapsulados, cifrados, etc.

Nota: La interfaz interna del PIX no se puede hacer ping para la formación del túnel a menos que el comando management-access se configure en el modo de confirmación global.

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

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Creación de túneles redundantes entre firewalls mediante PDM
- Referencias de Comandos de Cisco Secure PIX Firewall

- Solicitudes de Comentarios (RFC)
- Cisco PIX Firewall Software