Túnel VPN de LAN para LAN entre dois PIXs usando o exemplo de configuração de PDM

Contents

Introduction

Este documento descreve o procedimento para configurar túneis VPN entre dois PIX Firewalls usando o Cisco PIX Device Manager (PDM). O PDM é uma ferramenta de configuração baseada em navegador projetada para ajudá-lo a configurar, configurar e monitorar seu PIX Firewall com uma GUI. Os PIX Firewalls são colocados em dois locais diferentes.

Um túnel é formado usando IPsec. O IPsec é uma combinação de padrões abertos que fornece confidencialidade de dados, integridade de dados e autenticação de origem de dados entre pares IPsec.

Prerequisites

Requirements

Não há requisitos para este documento.

Componentes Utilizados

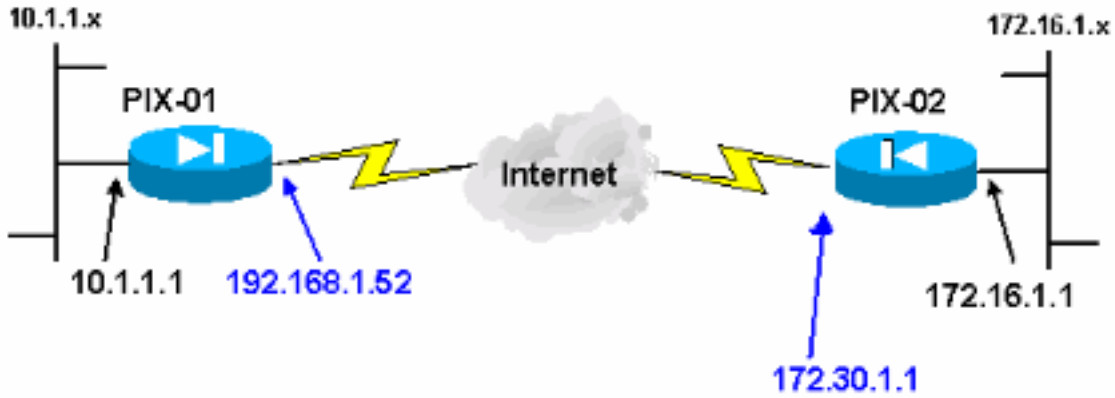
As informações neste documento são baseadas nos Cisco Secure PIX 515E Firewalls com 6.x e PDM versão 3.0.

Consulte Configurando um Túnel VPN PIX para PIX Simples Usando IPsec para obter um exemplo de configuração na configuração de um túnel VPN entre dois dispositivos PIX usando a CLI (Command Line Interface, Interface de Linha de Comando).

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 Rede

Este documento utiliza a seguinte configuração de rede:



Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

A negociação de IPsec pode ser dividida em cinco etapas e inclui duas fases de Internet Key Exchange (IKE).

1. Um túnel de IPSec é iniciado por um tráfego interessante. O tráfego é considerado interessante quando ele é transmitido entre os peers IPSec.
2. Na Fase 1 IKE, os correspondentes IPSec negociam a política de Associação de segurança (SA) IKE estabelecida. Quando os peers são autenticados, um túnel seguro é criado com o uso do Internet Security Association and Key Management Protocol (ISAKMP).
3. Em IKE Phase 2, os correspondentes de IPSec utilizam o túnel autenticado e seguro para negociar transformações de IPSec AS. A negociação da política compartilhada determina como o túnel de IPSec é estabelecido.
4. O túnel de IPSec é criado e os dados são transferidos entre peers de IPSec com base nos parâmetros de IPSec configurados em grupos de transformação do IPSec.
5. O túnel de IPSec finaliza quando os IPSec SAs são excluídos ou quando sua vida útil expira.**Observação:** a negociação de IPsec entre os dois PIXes falhará se os SAs em ambas as fases de IKE não coincidirem com os correspondentes.

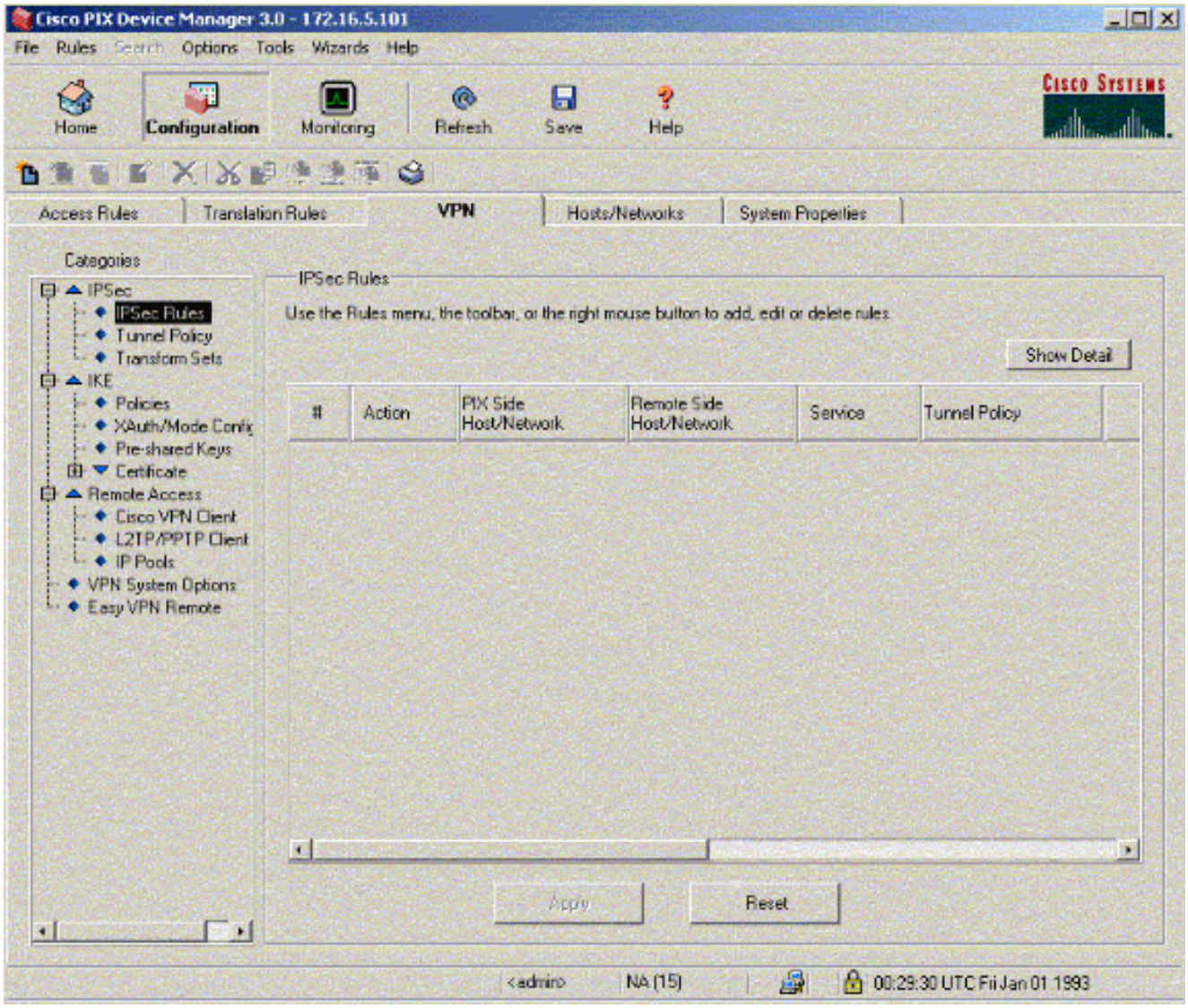
Procedimento de configuração

Além de outras configurações gerais na CLI do PIX para acessá-lo através da interface Ethernet

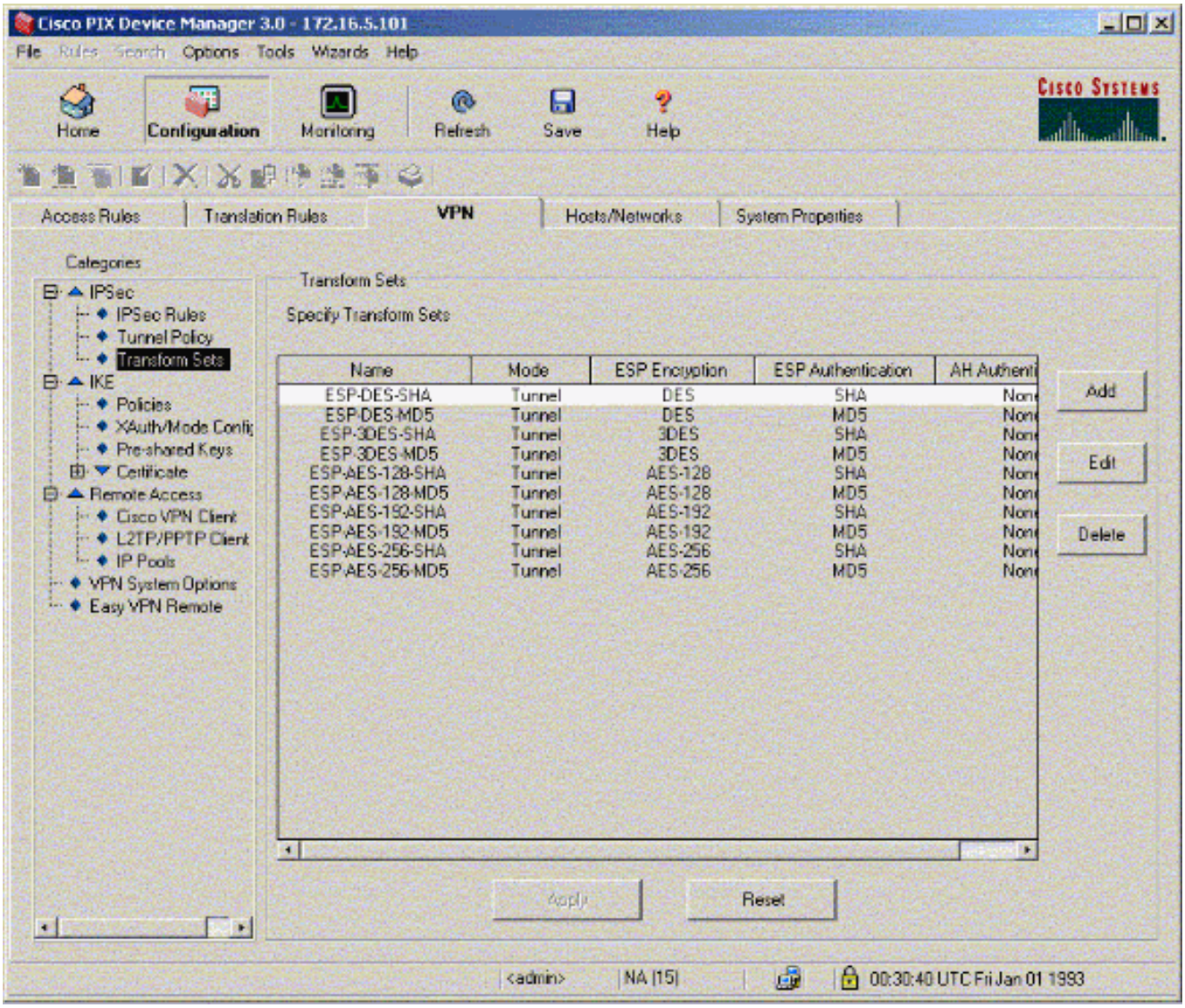
0, use os comandos **http server enable** e **http server <local_ip> <mask> <interface>** onde *<local_ip>* e *<mask>* são o endereço IP e a máscara da estação de trabalho na qual o PDM está instalado. A configuração neste documento é para PIX-01. O PIX-02 pode ser configurado usando as mesmas etapas com endereços diferentes.

Conclua estes passos:

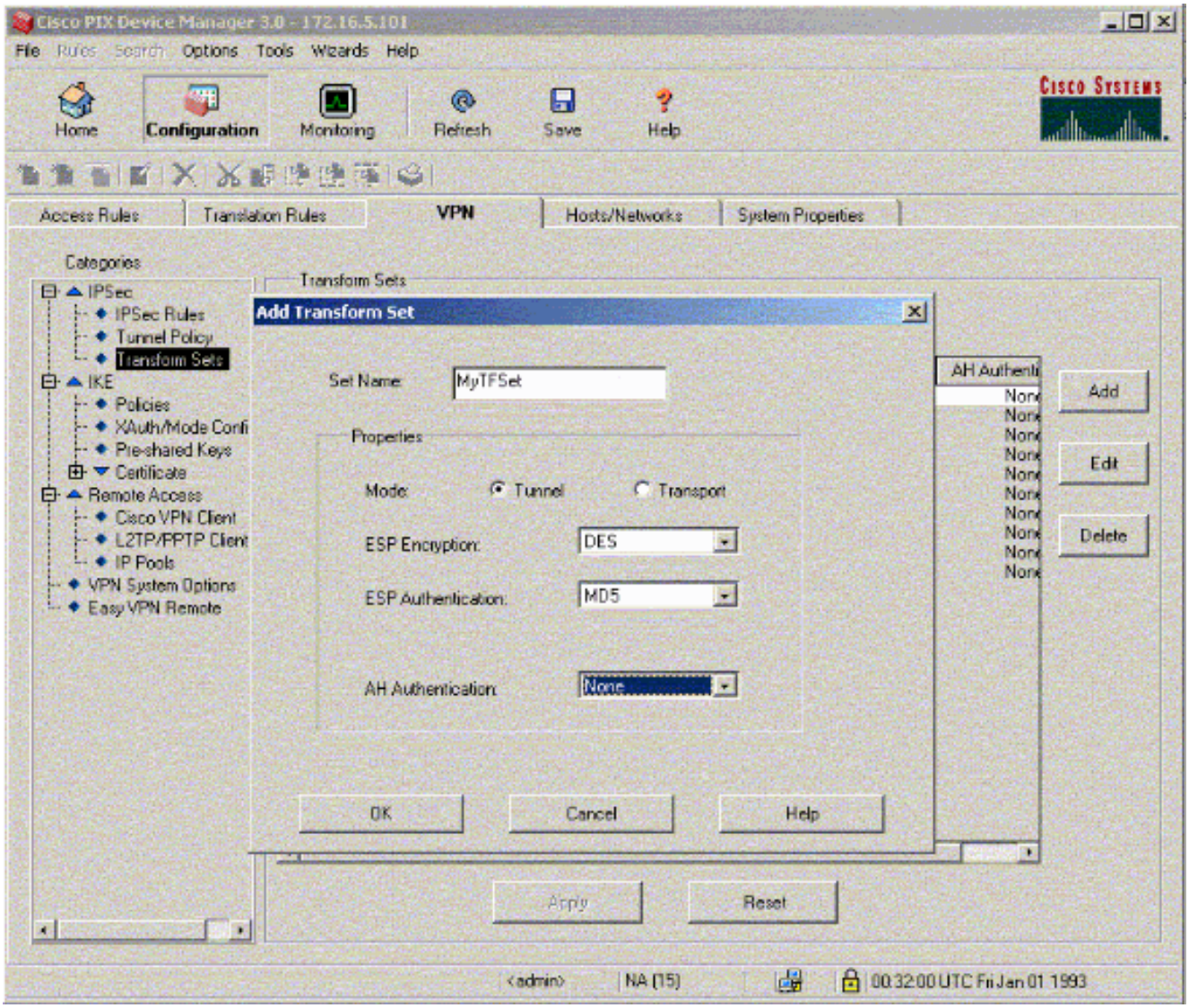
1. Abra o navegador e digite **https://<Inside_IP_Address_of_PIX>** para acessar o PIX no PDM.
2. Clique em **Configuração** e vá para a guia VPN.



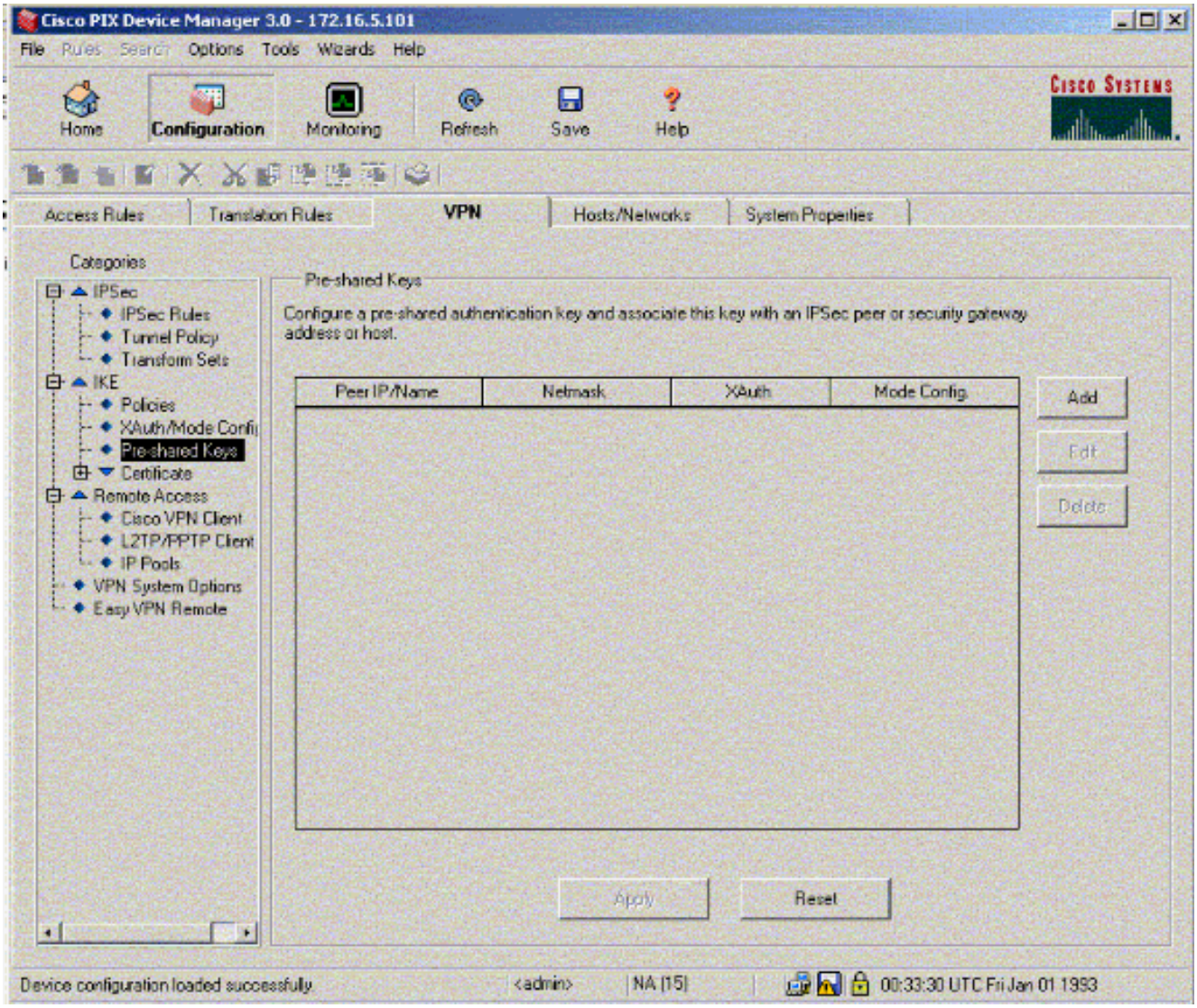
3. Clique em **Transform Sets** em IPSec para criar um conjunto de transformações.



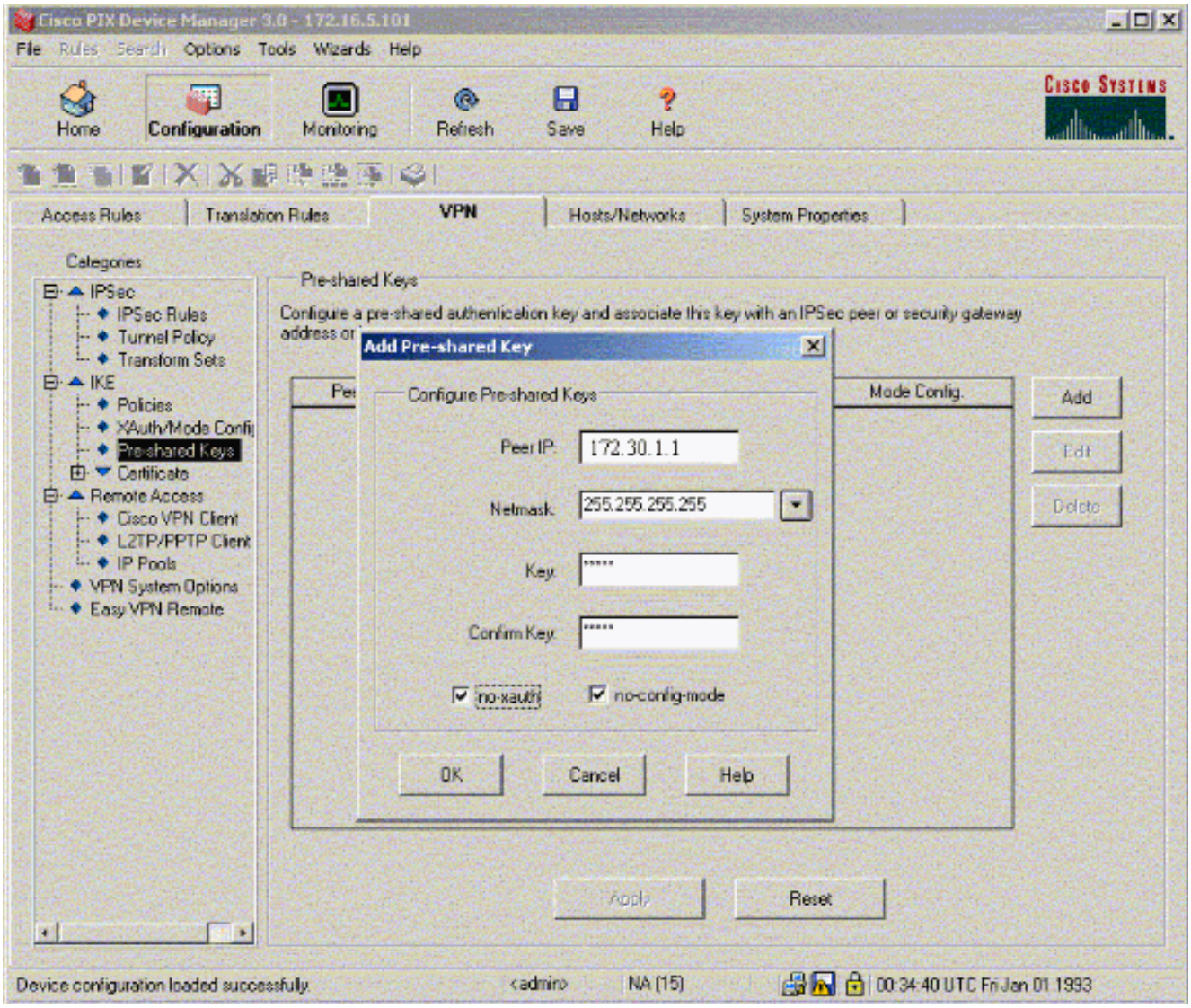
4. Clique em **Adicionar**, selecione todas as opções apropriadas e clique em **OK** para criar um novo conjunto de transformações.



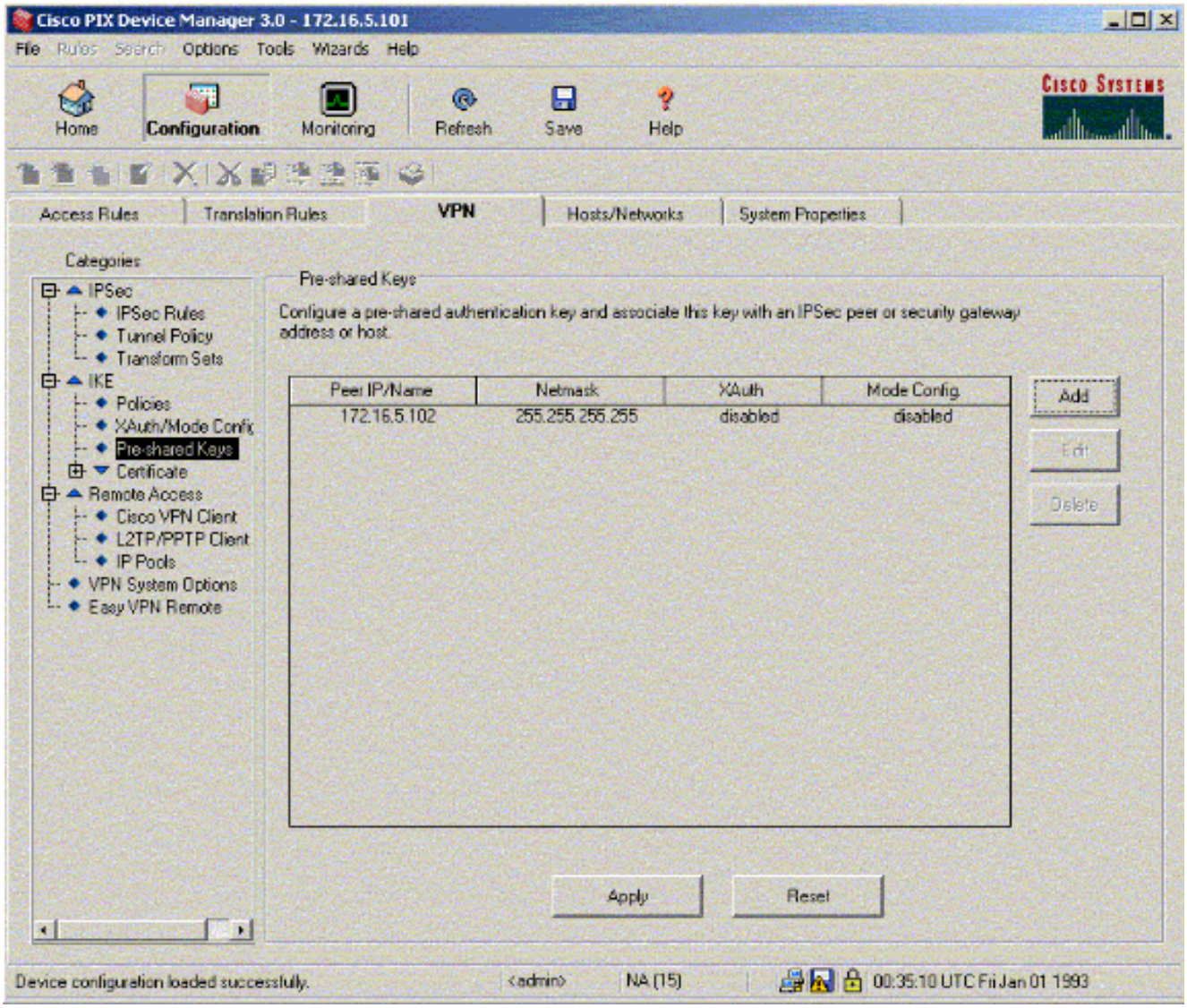
5. Clique em **Pre-Shared Keys** em IKE para configurar chaves pré-compartilhadas.



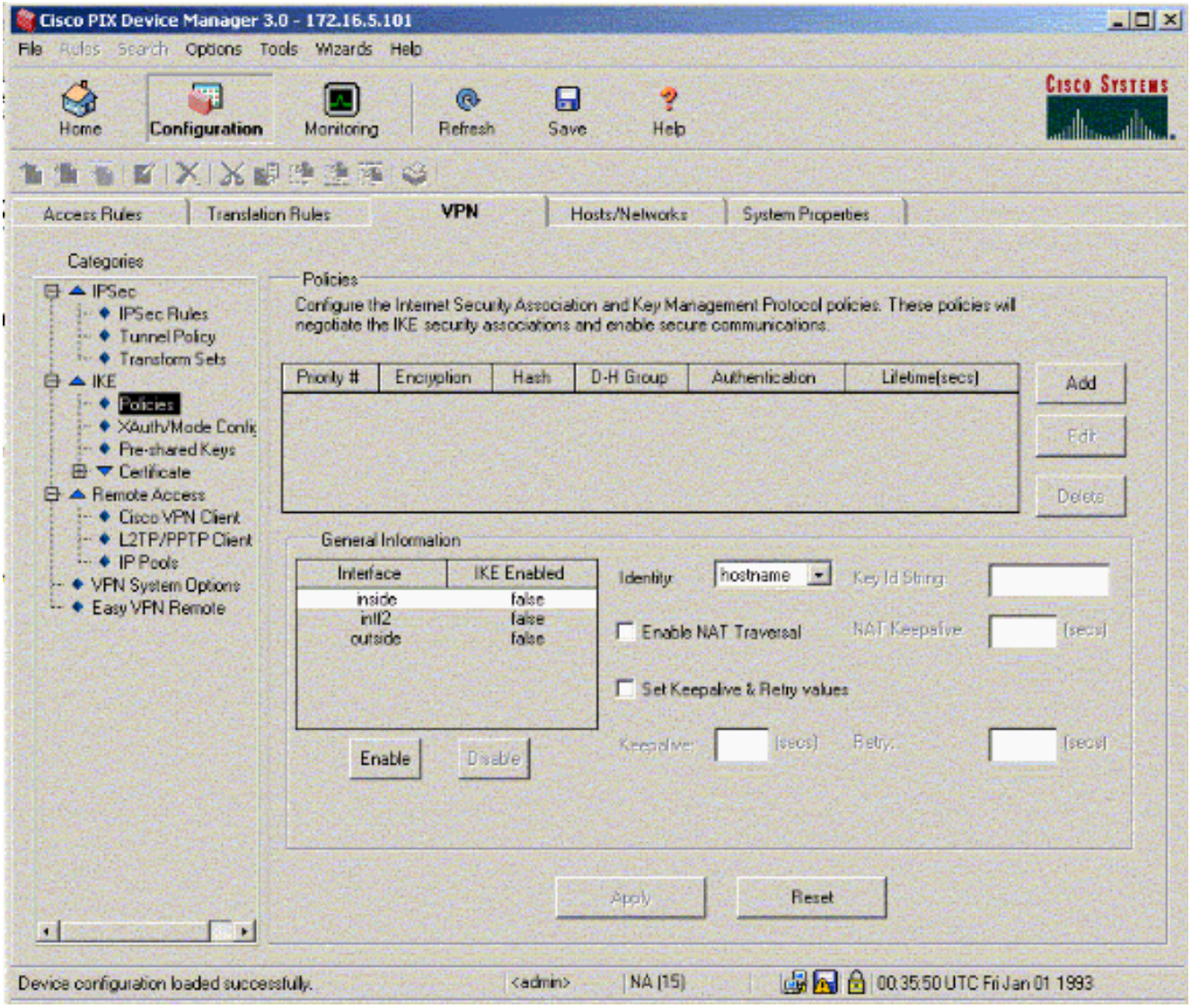
6. Clique em **Adicionar** para adicionar uma nova chave pré-compartilhada.



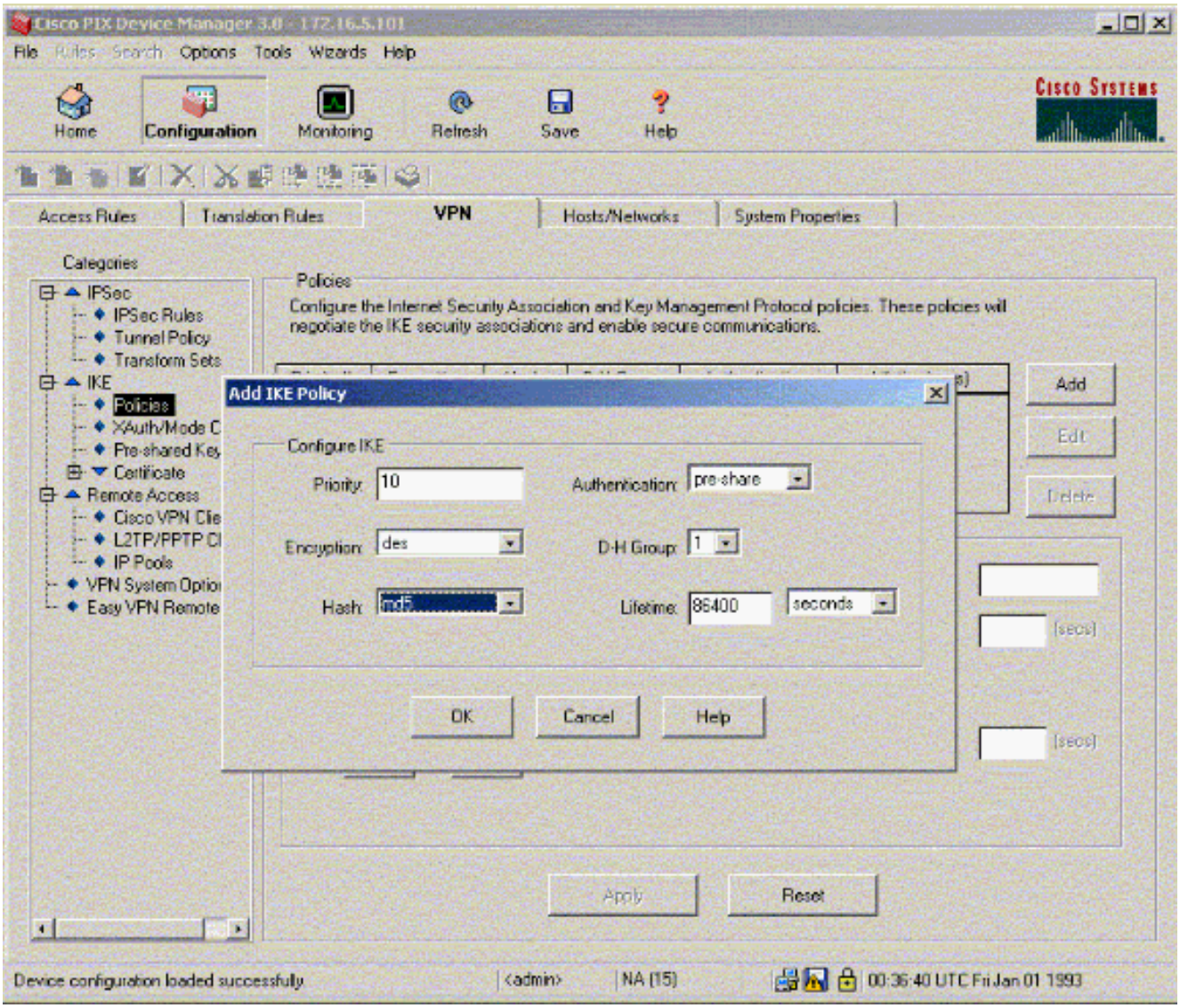
Esta janela mostra a chave, que é a senha para a associação do túnel. Isso tem que coincidir em ambos os lados do
túnel.



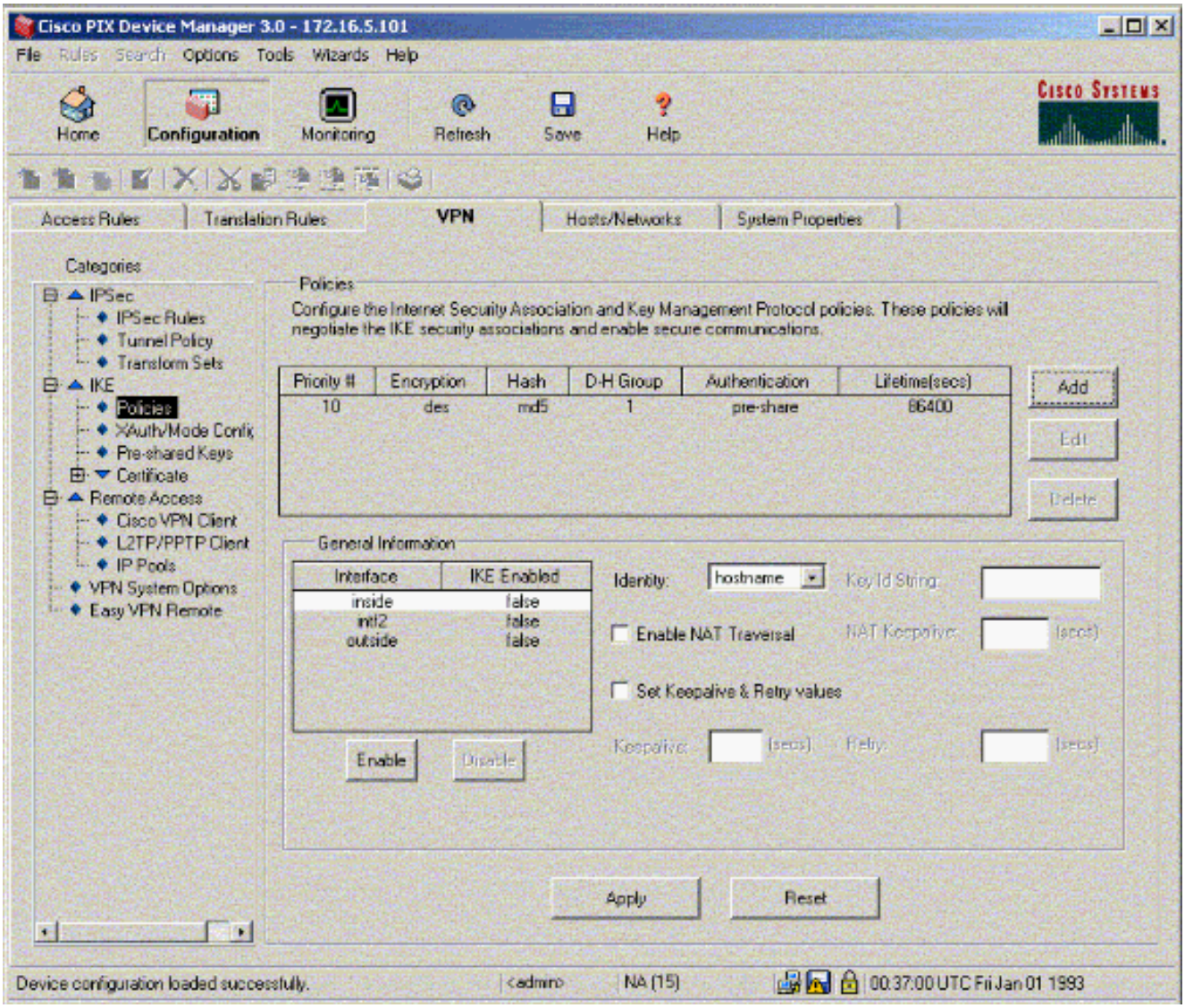
7. Clique em **Policies** em IKE para configurar políticas.



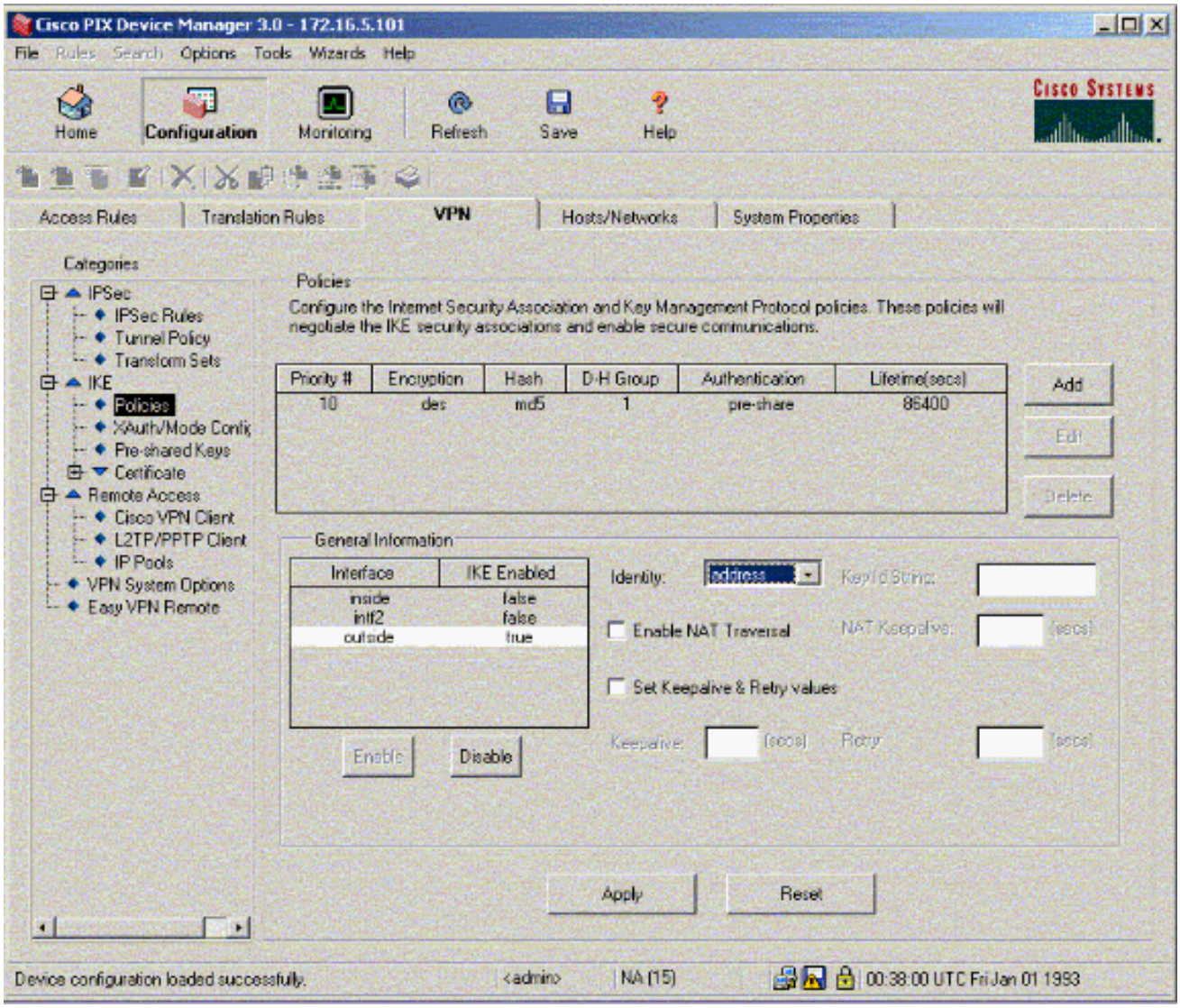
8. Clique em **Adicionar** e preencha os campos apropriados.



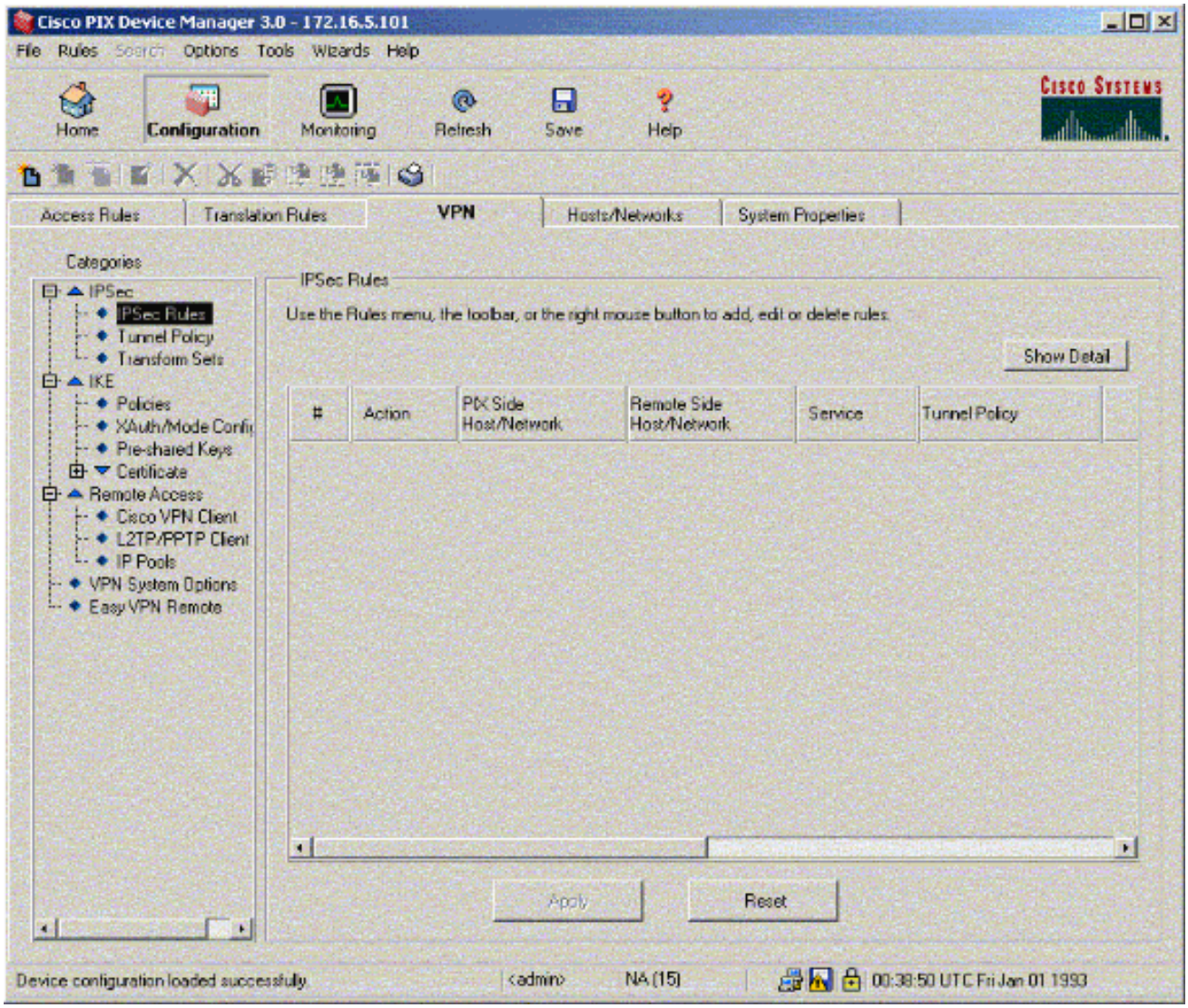
9. Clique em **OK** para adicionar uma nova política.



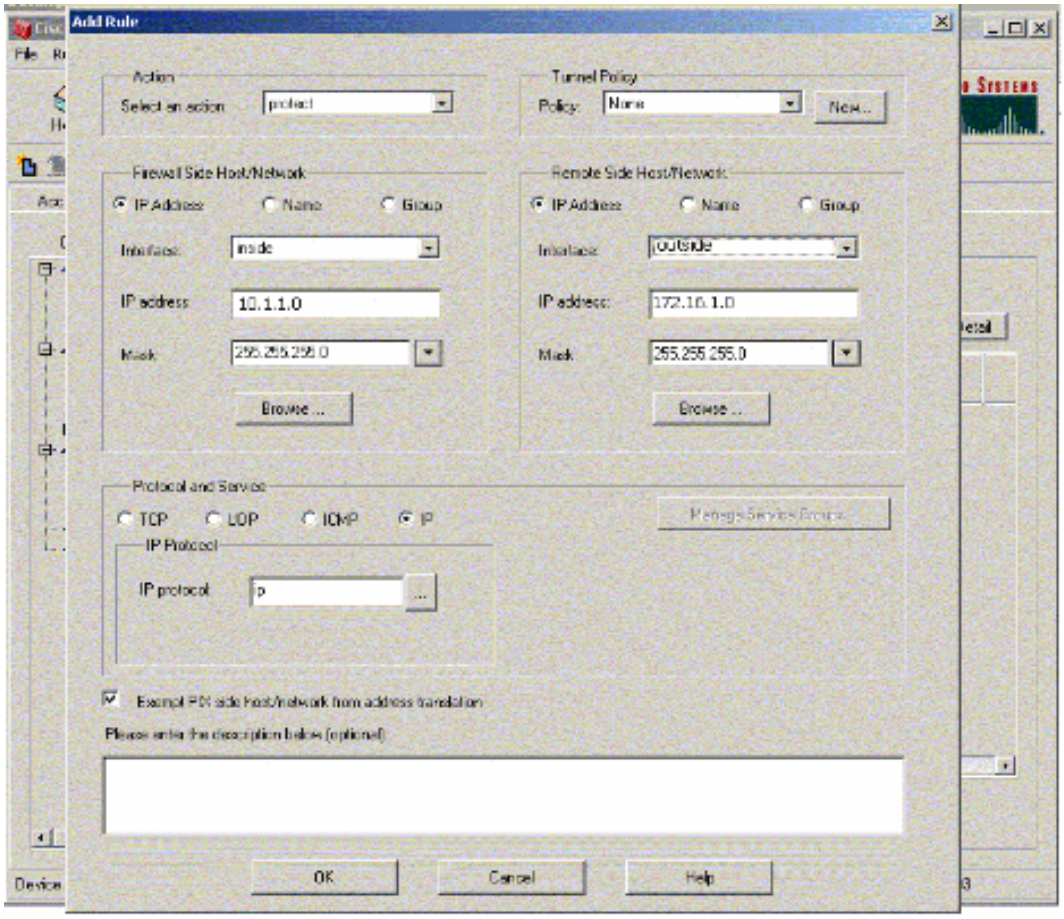
10. Selecione a interface **externa**, clique em **Enable** e, no menu suspenso Identity, selecione **address**.



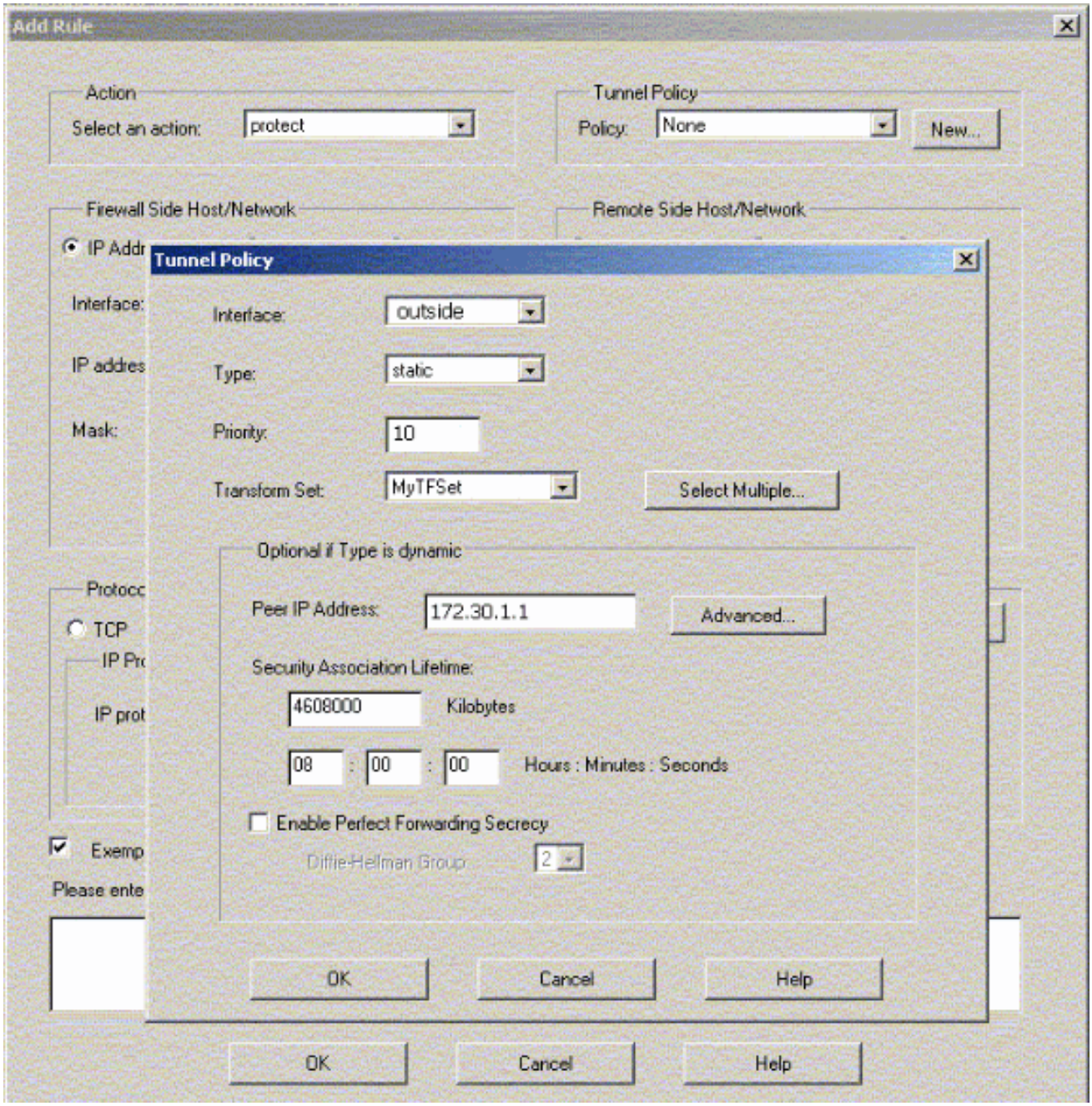
11. Clique em **IPSec Rules** em IPSec para criar regras IPsec.



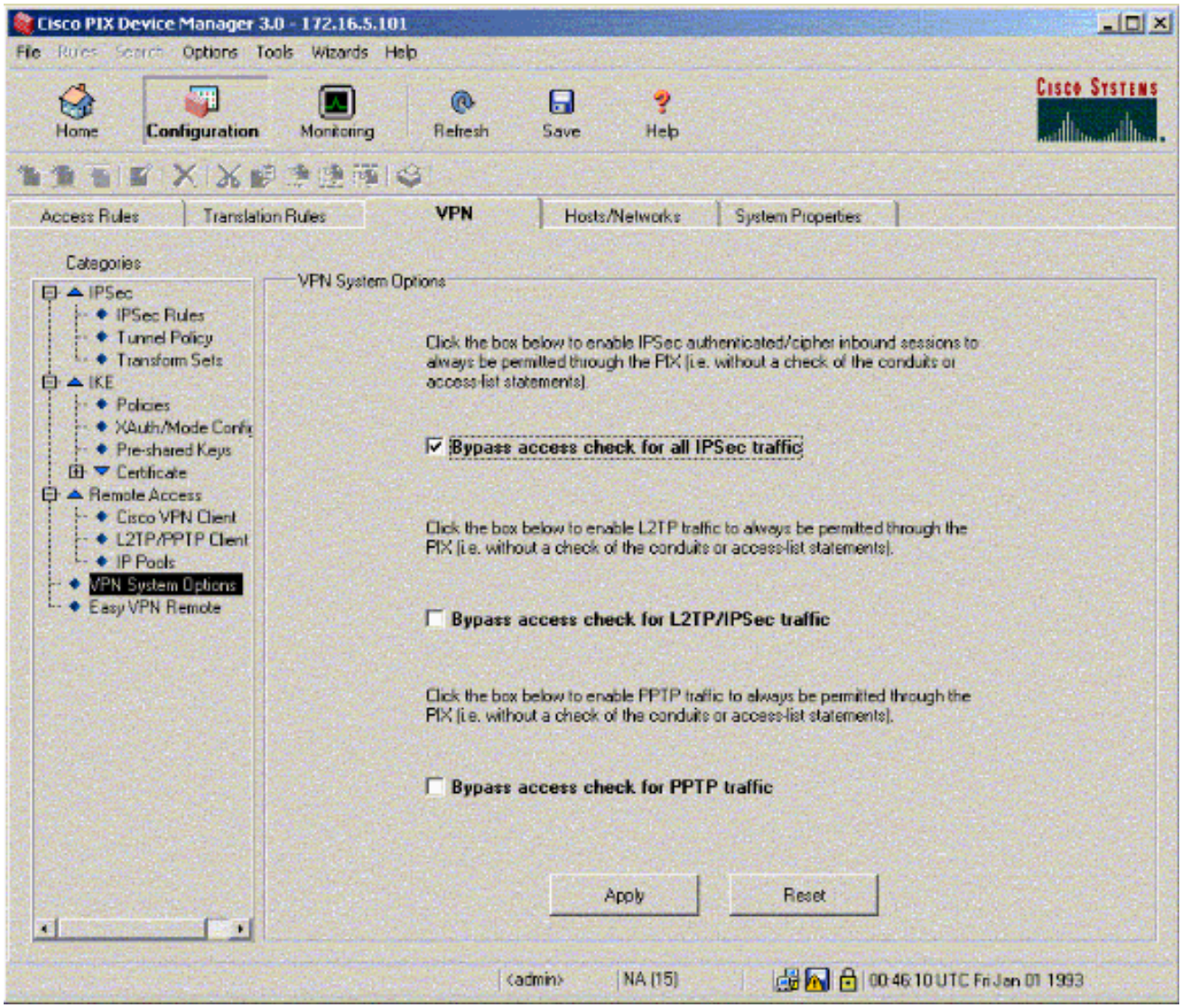
12. Preencha os campos apropriados.



13. Clique em **New** na Tunnel Policy (Política de túnel). Uma janela Política de túnel é exibida. Preencha os campos
apropriados.



14. Clique em **OK** para ver a regra IPsec configurada.
15. Clique em **Opções de sistemas VPN** e marque **Ignorar verificação de acesso para todo o tráfego IPSec**.

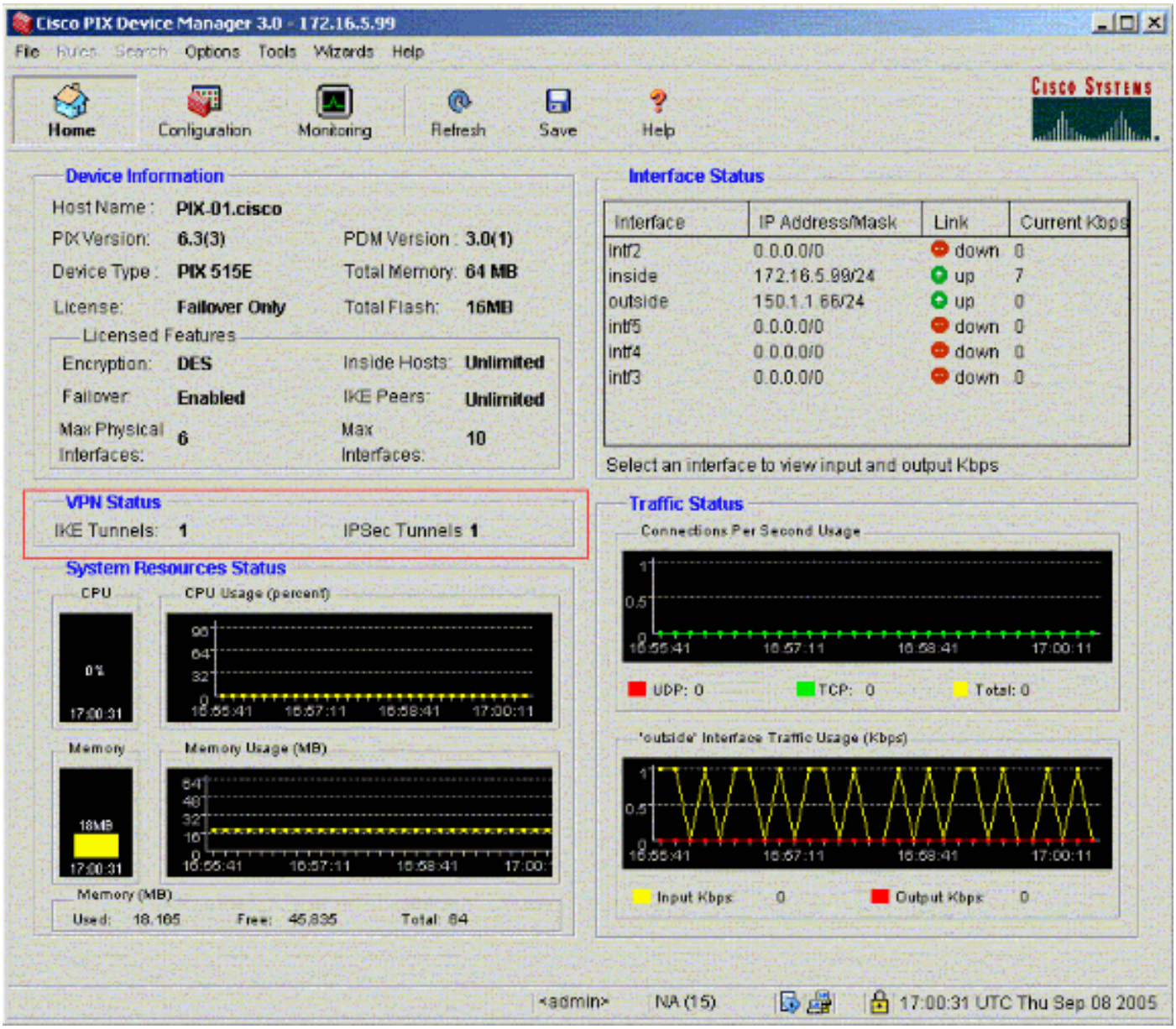


Verificar

Se houver tráfego interessante para o peer, o túnel é estabelecido entre PIX-01 e PIX-02.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Visualize o Status da VPN em Início no PDM (destacado em vermelho) para verificar a formação do túnel.



Você também pode verificar a formação de túneis usando CLI em Ferramentas no PDM. Emita o comando **show crypto isakmp sa** para verificar a formação de túneis e emita o comando **show crypto ipsec sa** para observar o número de pacotes encapsulados, criptografados e assim por diante.

Observação: a interface interna do PIX não pode receber ping para a formação do túnel, a menos que o comando management-access esteja configurado no modo de confirmação global.

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

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Criação de túnel redundante entre firewalls usando PDM
- Referências do comando Cisco Secure PIX Firewall
- Solicitações de Comentários (RFCs)
- Cisco PIX Firewall Software