Exemple de configuration d'un tunnel VPN LAN à LAN entre deux PIX à l'aide de PDM

Contenu

Introduction

Ce document décrit la procédure de configuration des tunnels VPN entre deux pare-feu PIX à l'aide de Cisco PIX Device Manager (PDM). PDM est un outil de configuration basé sur navigateur conçu pour vous aider à configurer, configurer et surveiller votre pare-feu PIX à l'aide d'une interface utilisateur graphique. Les pare-feux PIX sont placés à deux endroits différents.

Un tunnel est formé utilisant IPsec. IPSec est une combinaison de normes ouvertes qui fournissent la confidentialité des données, l'intégrité des données et l'authentification de l'origine des données entre des homologues IPSec.

Conditions préalables

Conditions requises

Il n'y a aucune exigence pour ce document.

Components Used

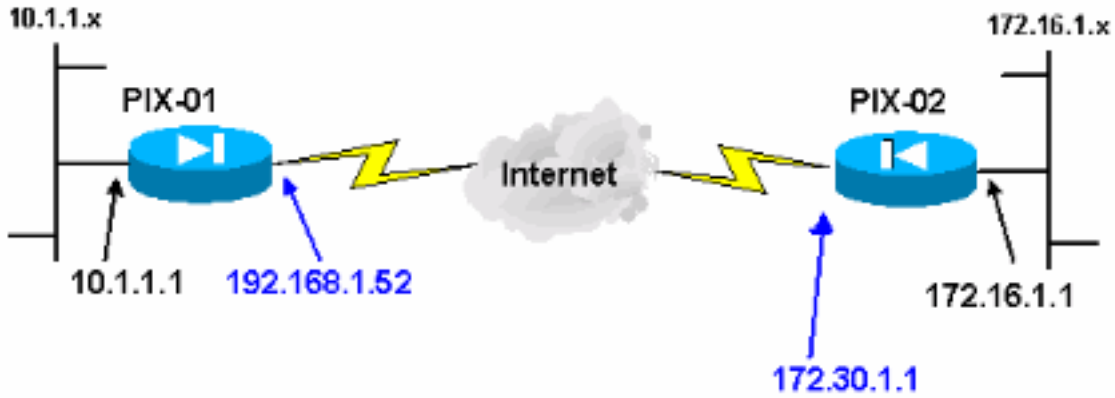
Les informations de ce document sont basées sur les pare-feu Cisco Secure PIX 515E avec 6.x et PDM version 3.0.

Référez-vous à Configuration d'un tunnel VPN PIX à PIX simple à l'aide d'IPsec pour un exemple de configuration sur la configuration d'un tunnel VPN entre deux périphériques PIX à l'aide de l'interface de ligne de commande (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.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

La négociation IPSec peut être décomposée en cinq étapes et inclut deux phases d'échange de clés Internet (IKE).

1. Un tunnel IPSec est lancé par un trafic intéressant. Le trafic est considéré comme intéressant quand il transite entre les homologues IPSec.
2. Dans la phase 1 d'IKE, les homologues IPSec négocient la stratégie d'association de sécurité IKE. Une fois que les homologues sont authentifiés, un tunnel sécurisé est créé en utilisant Internet Security Association and Key Management Protocol (ISAKMP).
3. Dans la phase 2 d'IKE, les homologues IPSec utilisent le tunnel authentifié et sécurisé pour négocier des transformations d'association de sécurité IPSec. La négociation de la stratégie partagée détermine comment le tunnel IPSec est établi.
4. Le tunnel IPSec est créé et les données sont transférées entre les homologues IPSec en fonction des paramètres IPSec configurés dans les jeux de transformations IPSec.
5. Le tunnel IPSec se termine quand les associations de sécurité IPSec sont supprimées ou quand leur durée de vie expire.**Remarque :** la négociation IPsec entre les deux PIXes échoue si les SA des deux phases IKE ne correspondent pas sur les homologues.

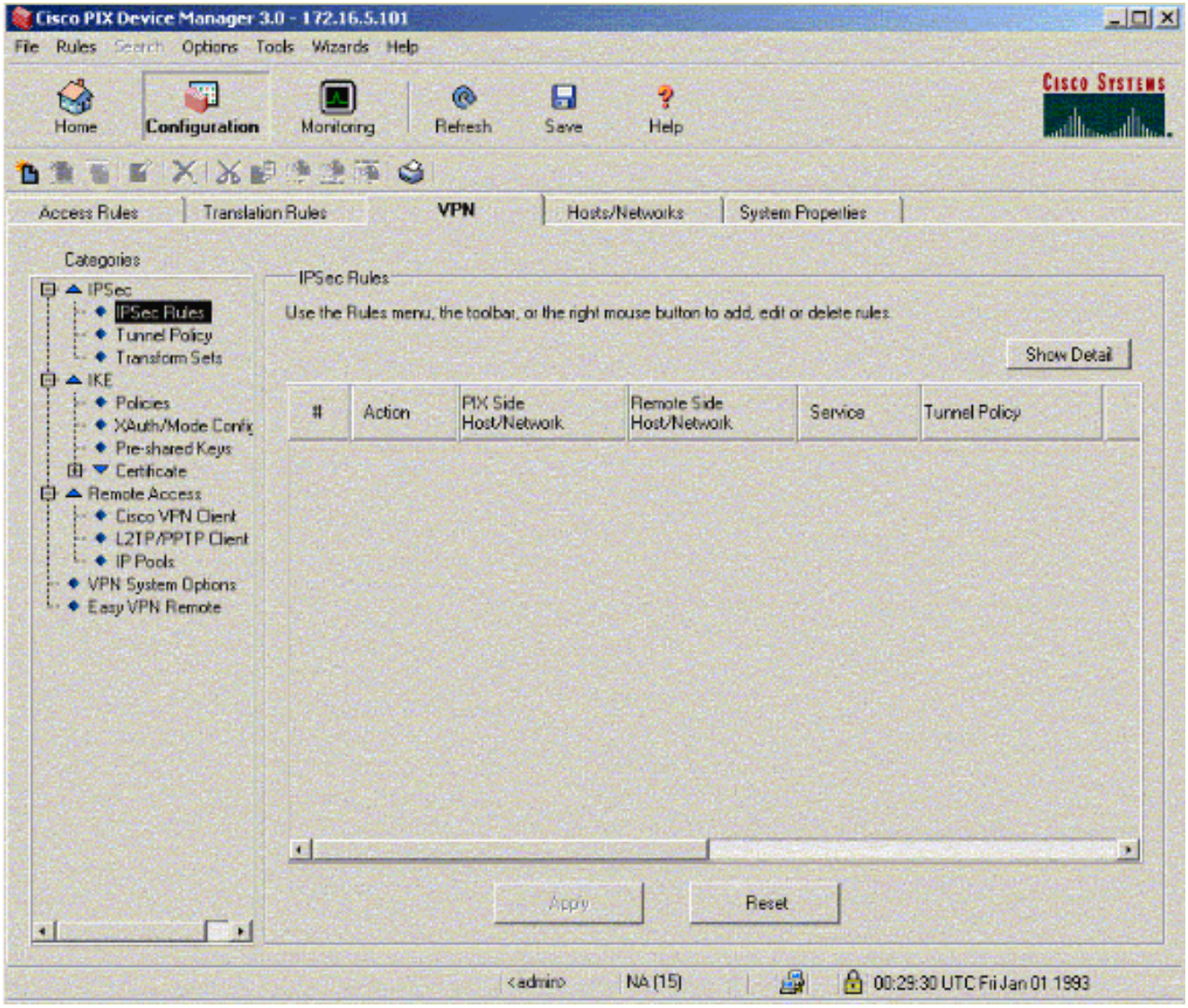
Procédure de configuration

Outre d'autres configurations générales sur l'interface de ligne de commande de PIX pour y

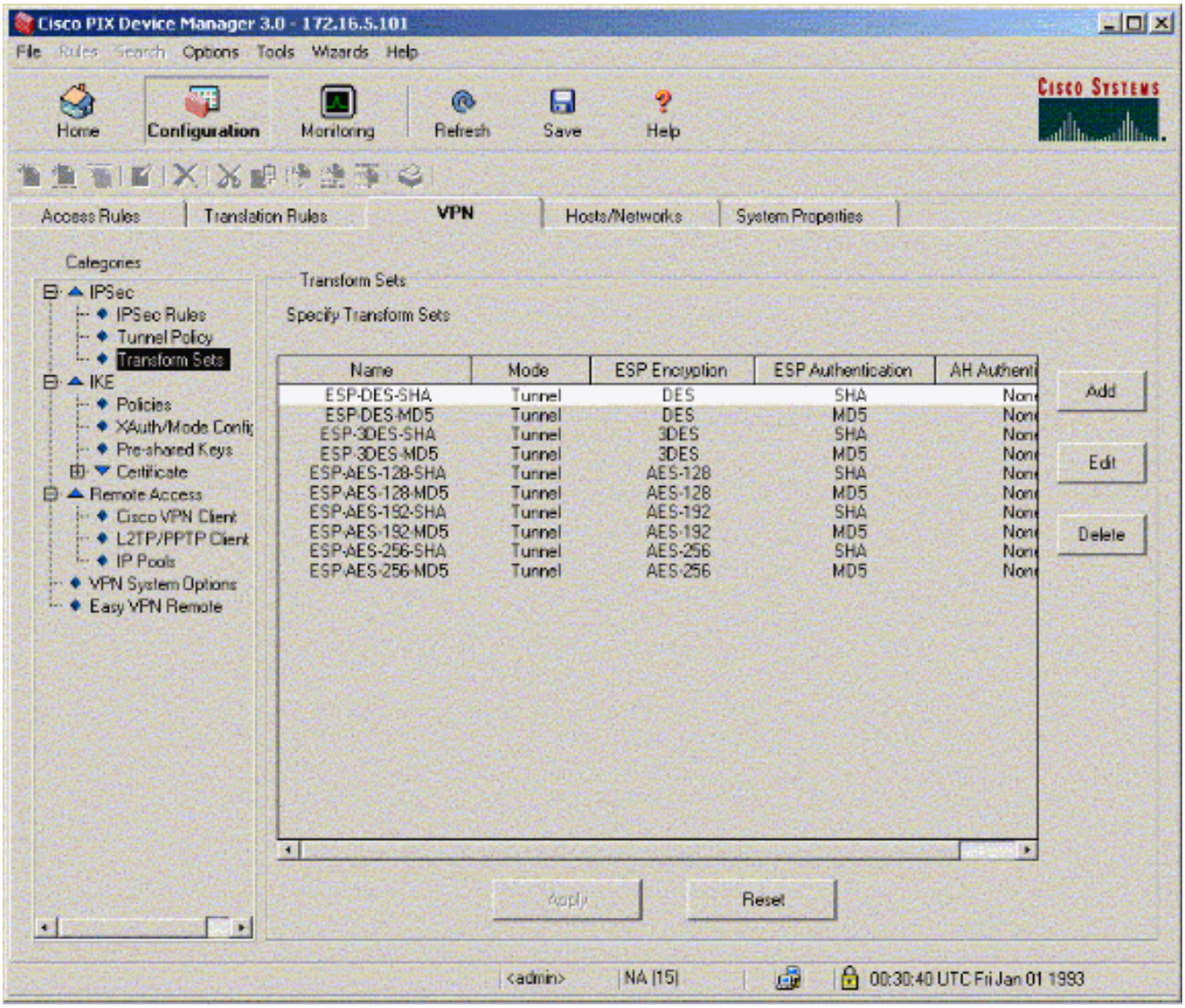
accéder via l'interface Ethernet 0, utilisez les commandes **http server enable** et **http server <ip_locale> <masque> <interface>** où *<ip_locale>* et *<masque>* sont l'adresse IP et le masque de la station de travail sur laquelle PDM est installé. La configuration de ce document est pour PIX-01. PIX-02 peut être configuré en utilisant les mêmes étapes avec des adresses différentes.

Procédez comme suit :

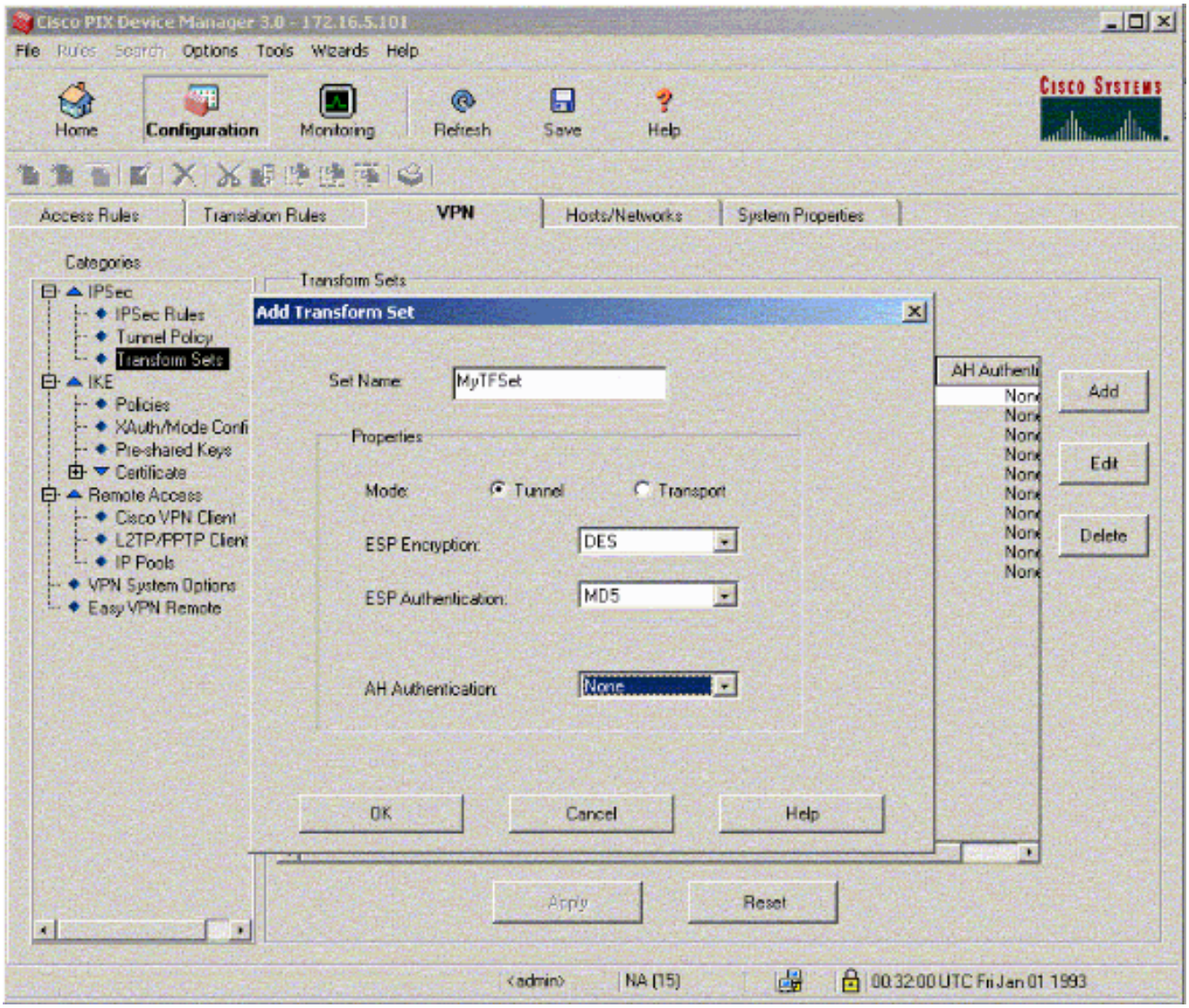
1. Ouvrez votre navigateur et tapez **https://<Inside_IP_Address_of_PIX>** pour accéder au PIX dans PDM.
2. Cliquez sur **Configuration** et accédez à l'onglet VPN.



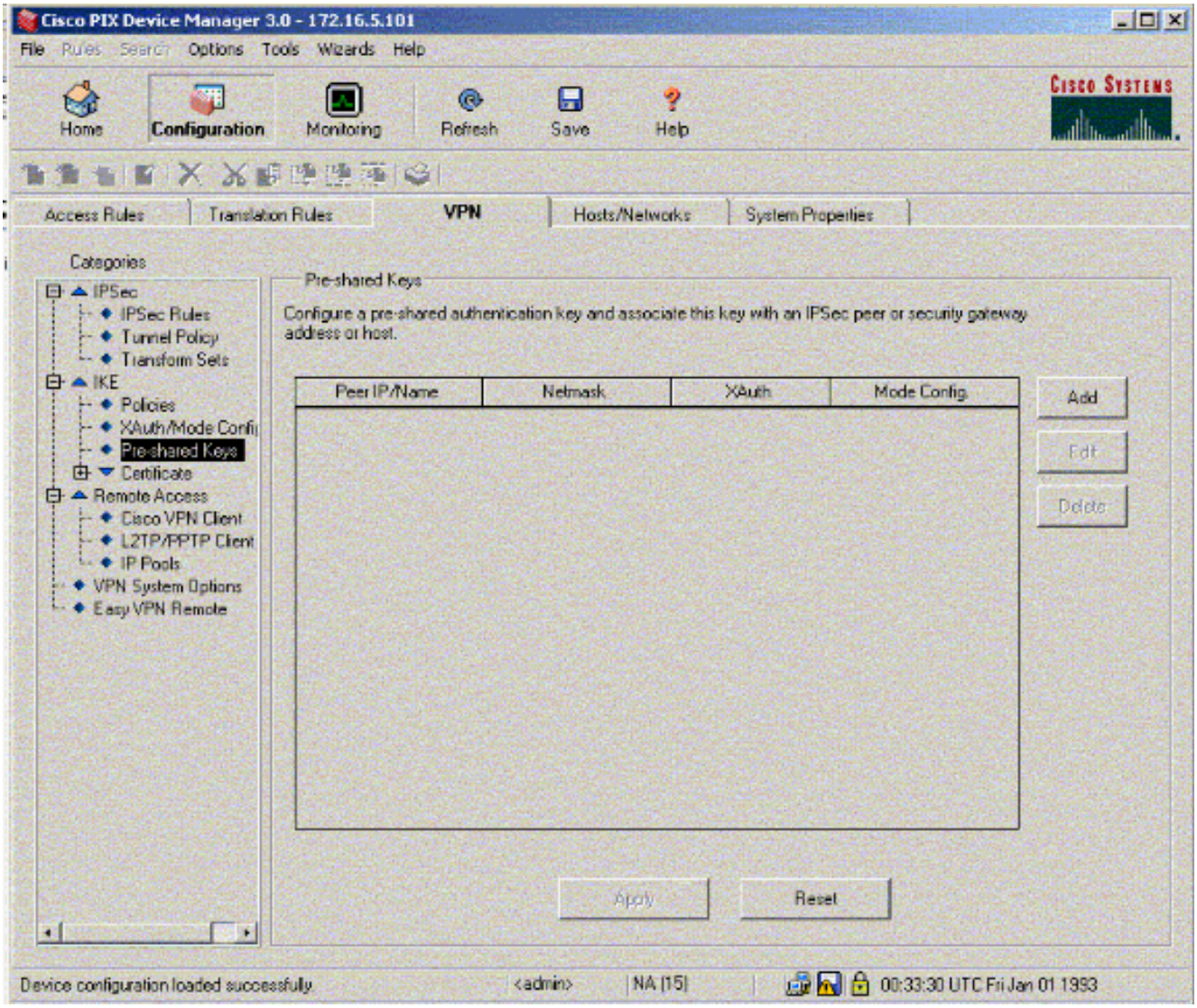
3. Cliquez sur **Transform Sets** sous IPSec pour créer un jeu Transform.



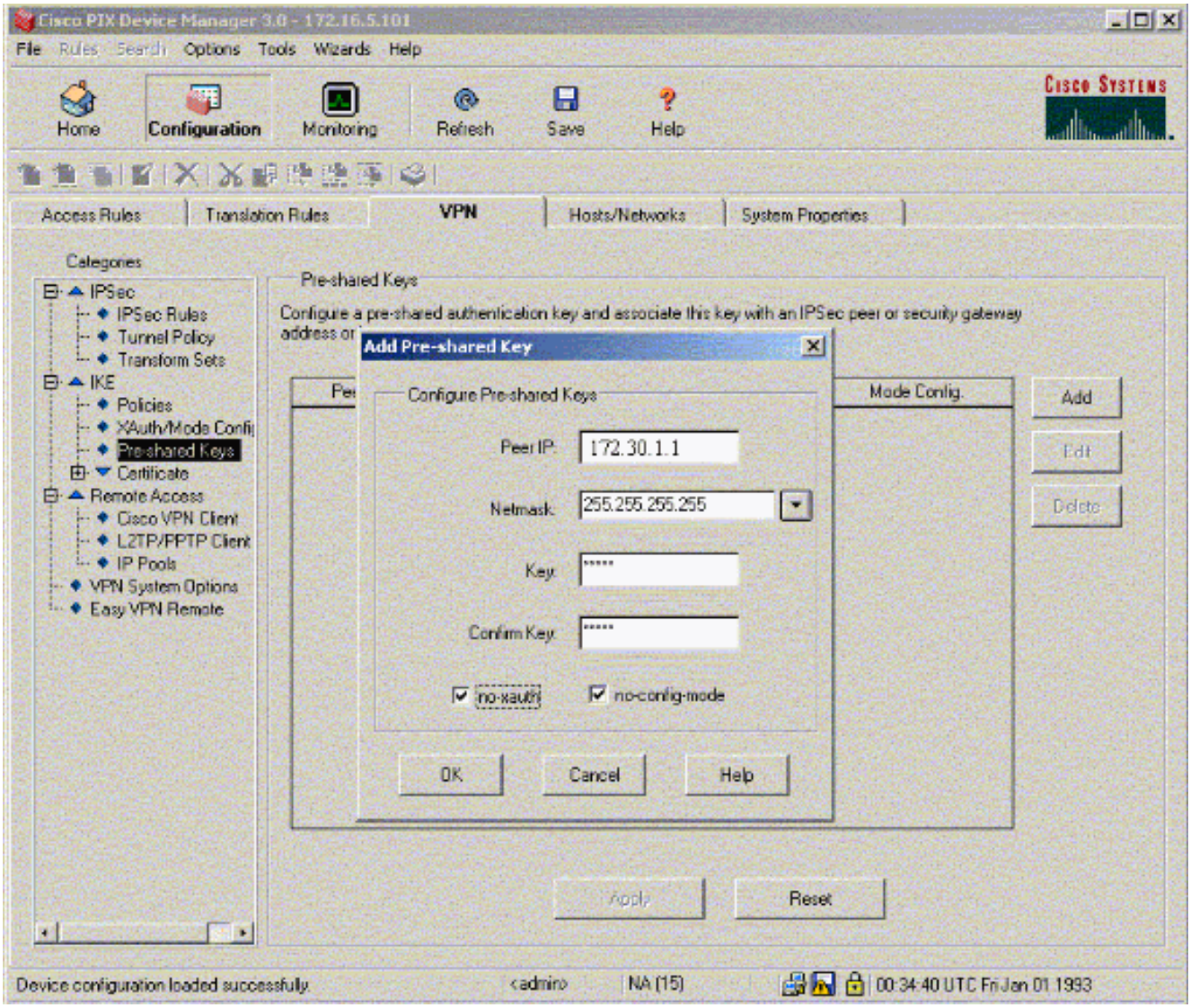
4. Cliquez sur **Ajouter**, sélectionnez toutes les options appropriées et cliquez sur **OK** pour créer un jeu de
transformation.



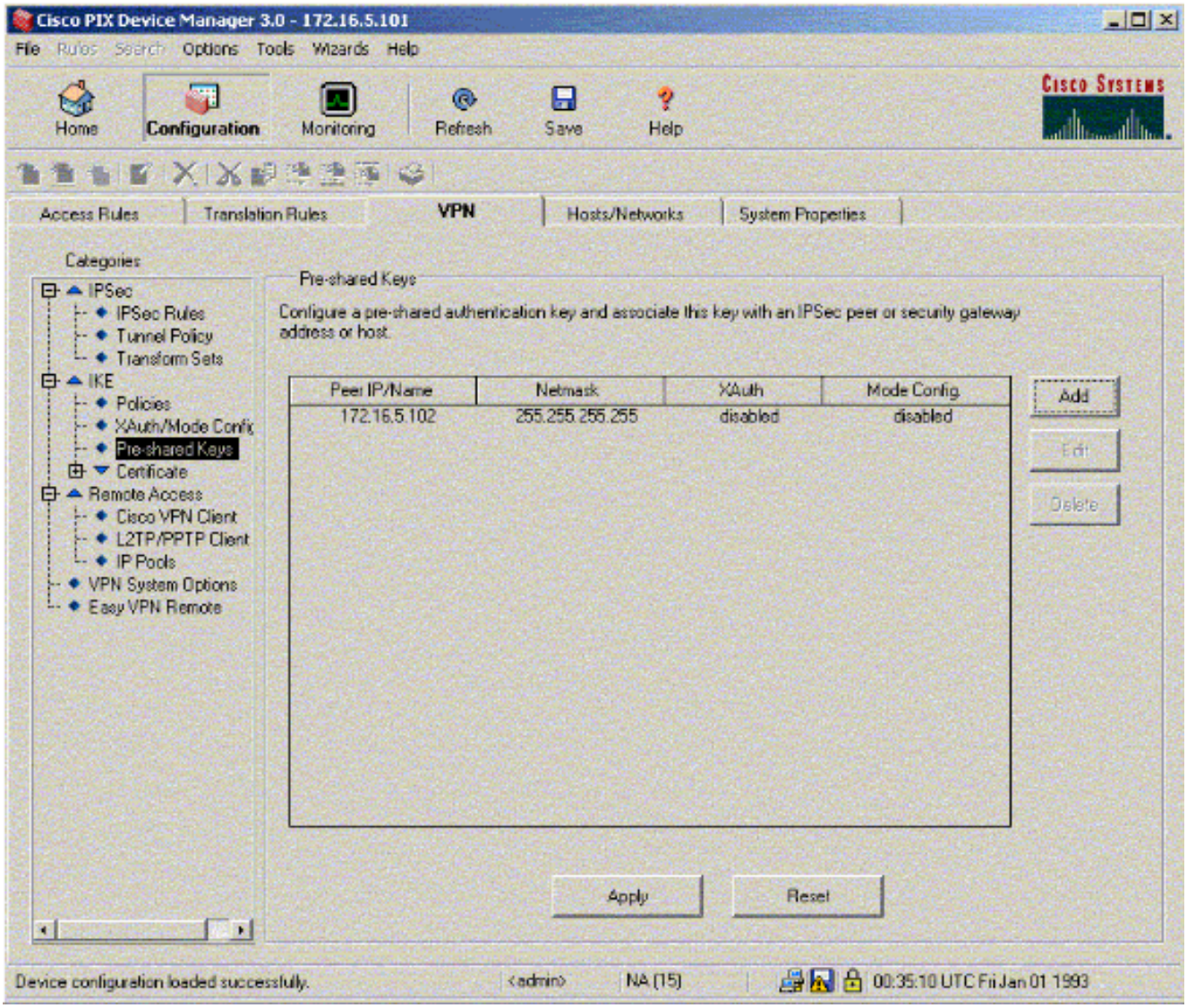
5. Cliquez sur **Clés prépartagées** sous IKE pour configurer les clés prépartagées.



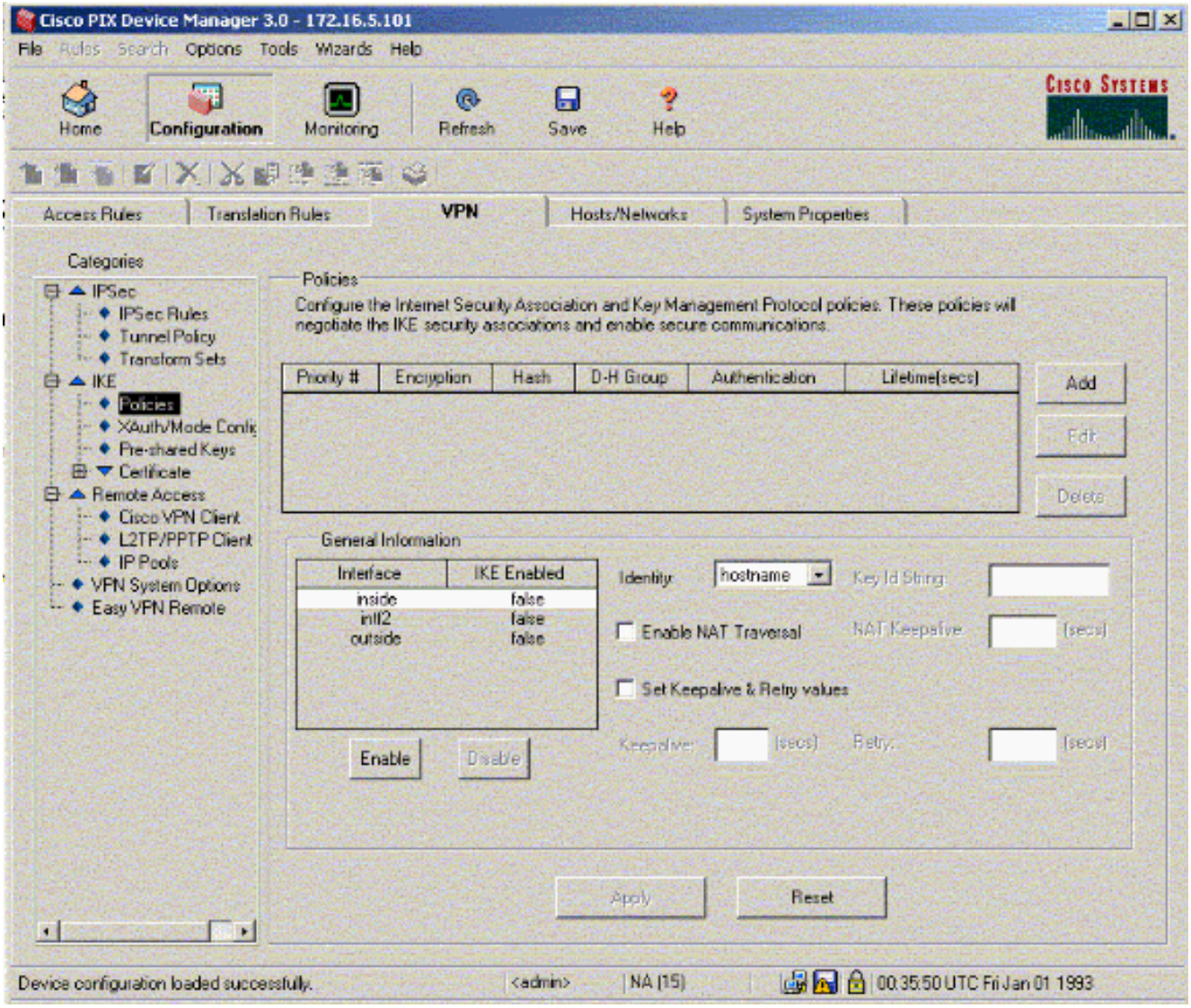
6. Cliquez sur **Ajouter** pour ajouter une nouvelle clé pré-partagée.



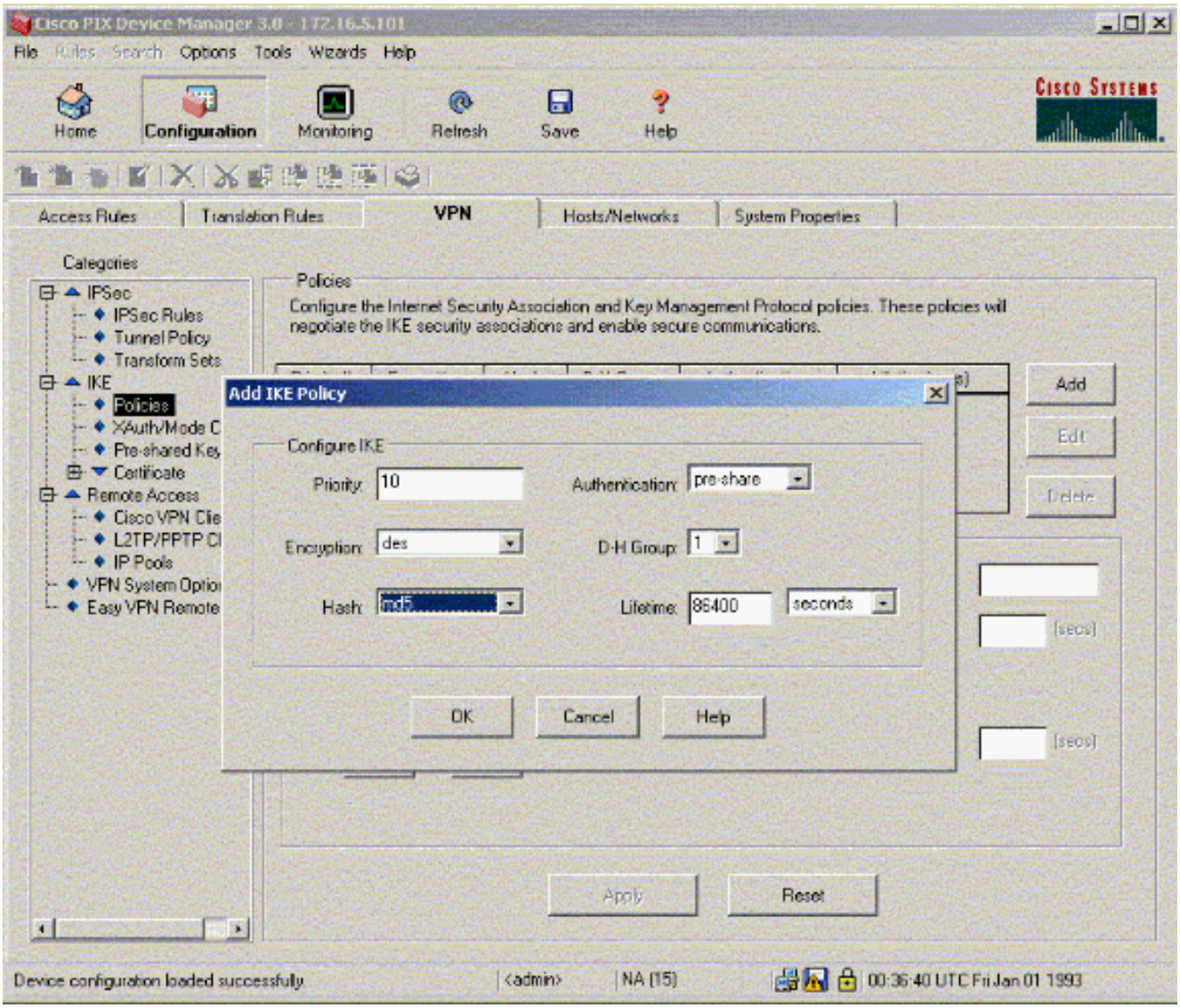
Cette fenêtre affiche la clé, qui est le mot de passe de l'association de tunnel. Cela doit correspondre des deux côtés du
tunnel.



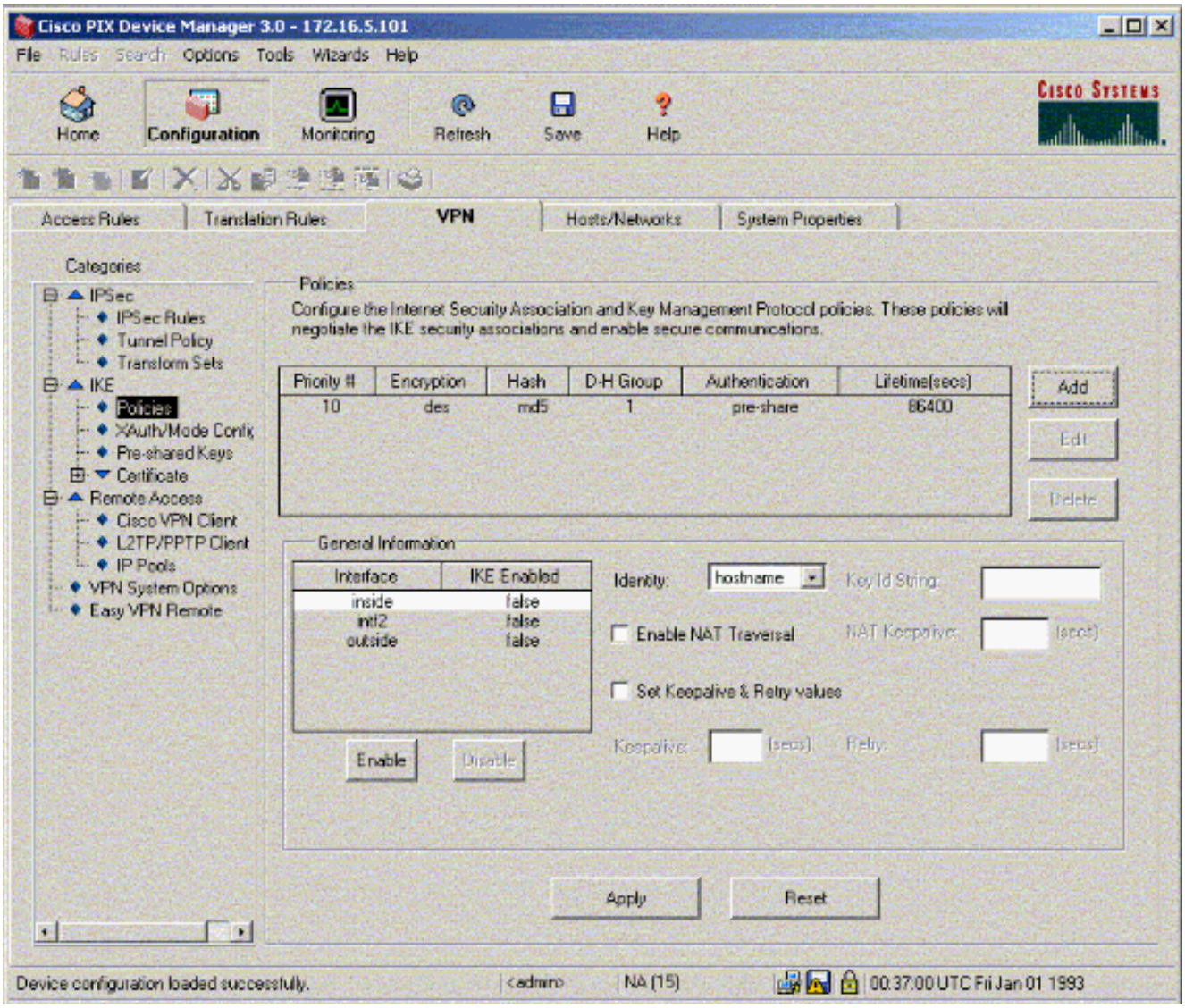
7. Cliquez sur **Stratégies** sous IKE pour configurer des stratégies.



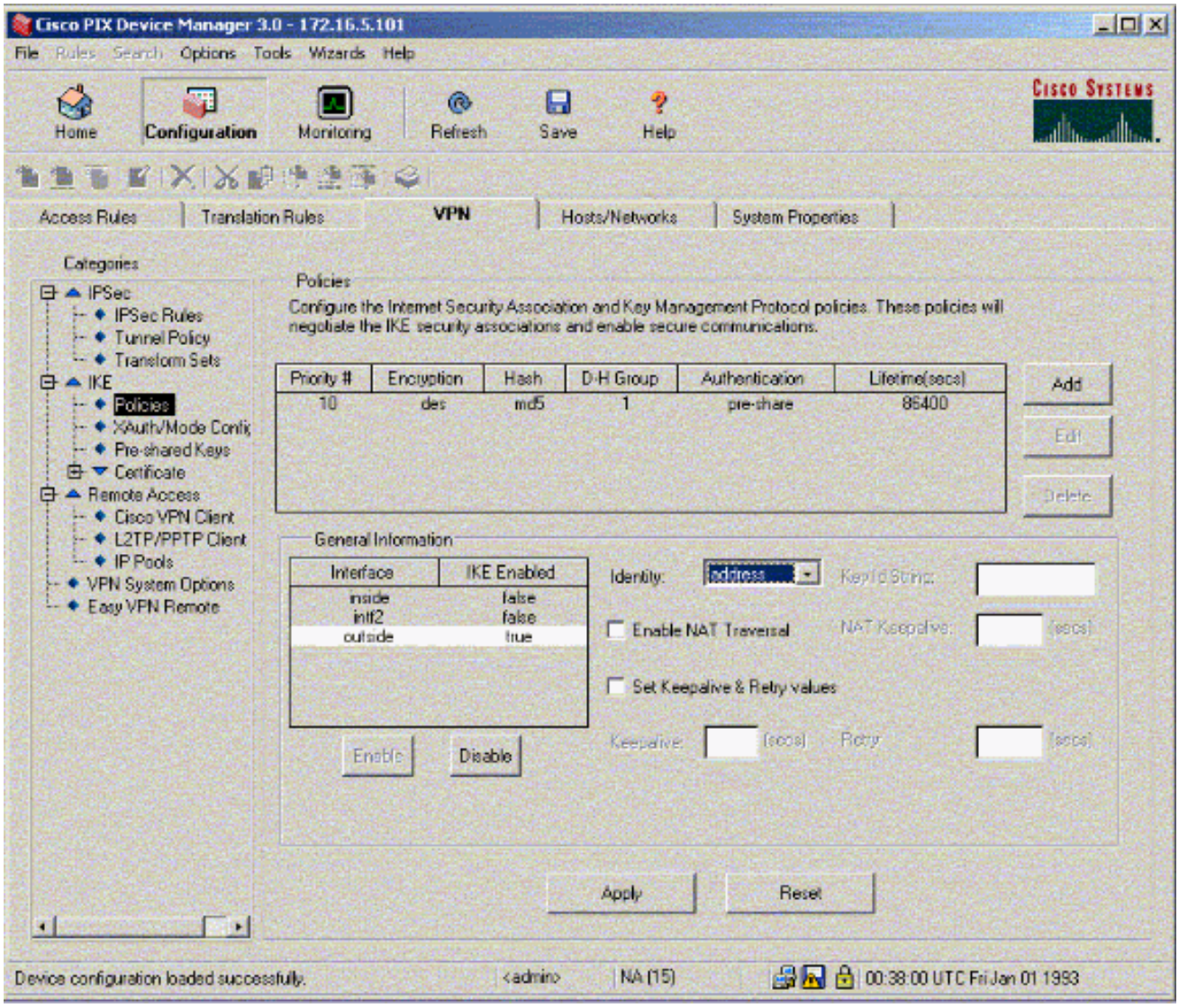
8. Cliquez sur **Ajouter** et renseignez les champs appropriés.



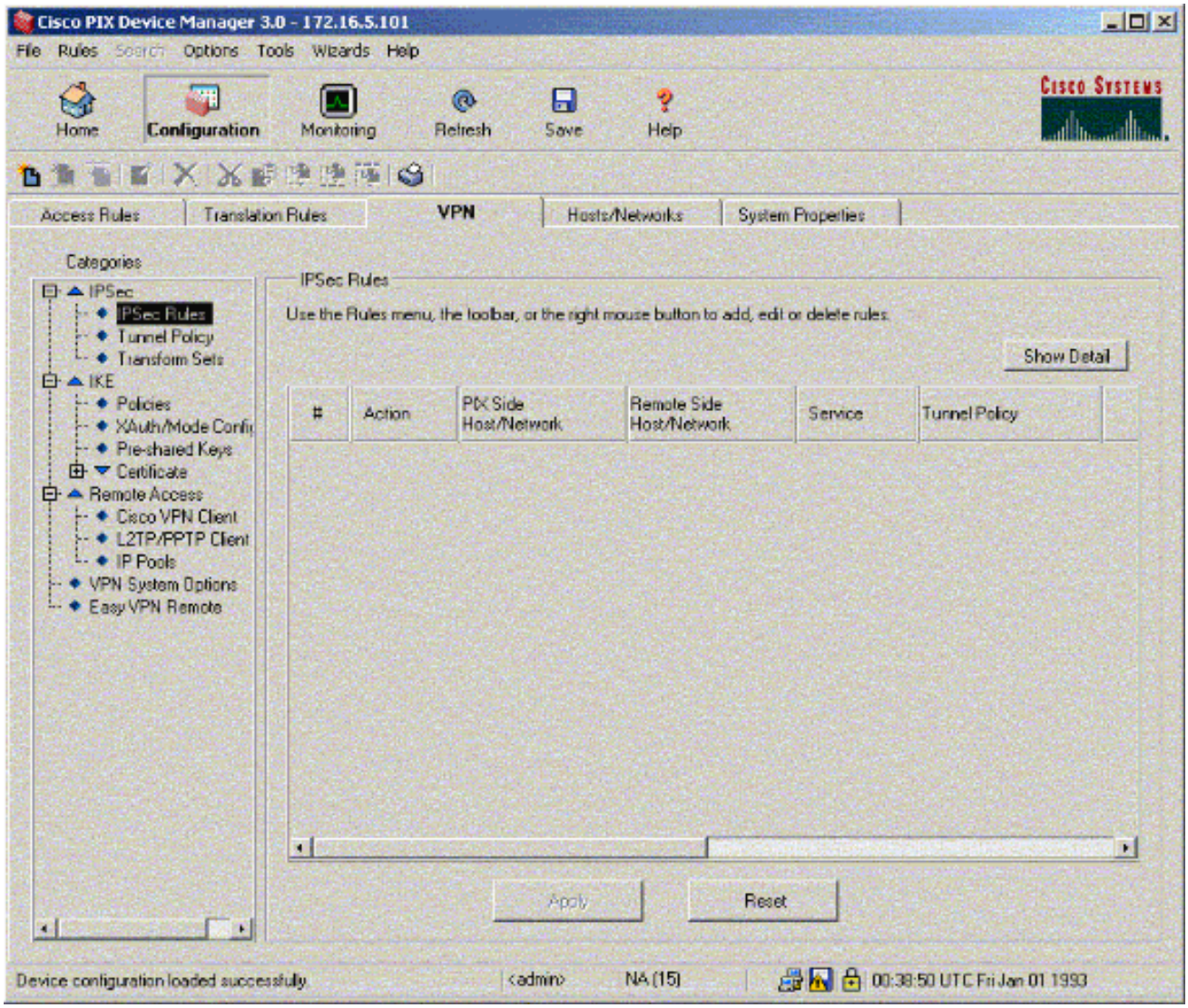
9. Cliquez sur **OK** pour ajouter une nouvelle stratégie.



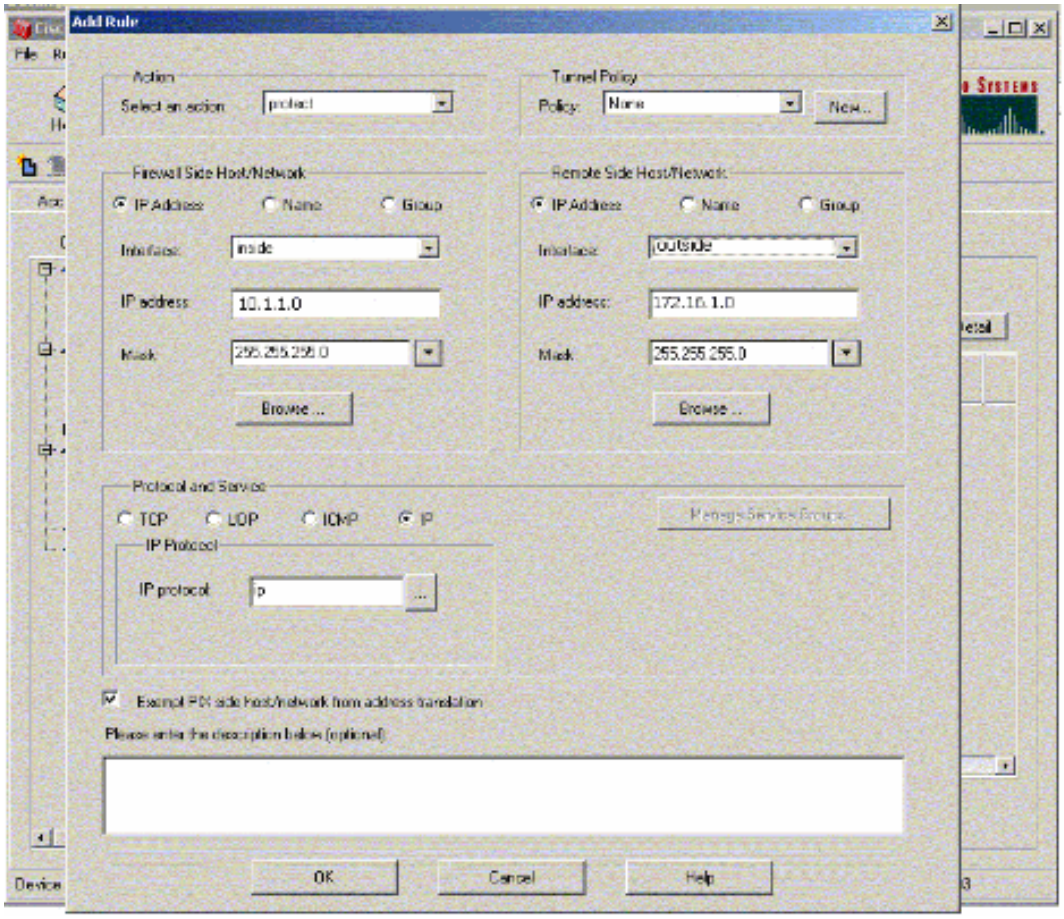
10. Sélectionnez l'interface **externe**, cliquez sur **Activer**, et dans le menu déroulant Identité, sélectionnez
adresse.



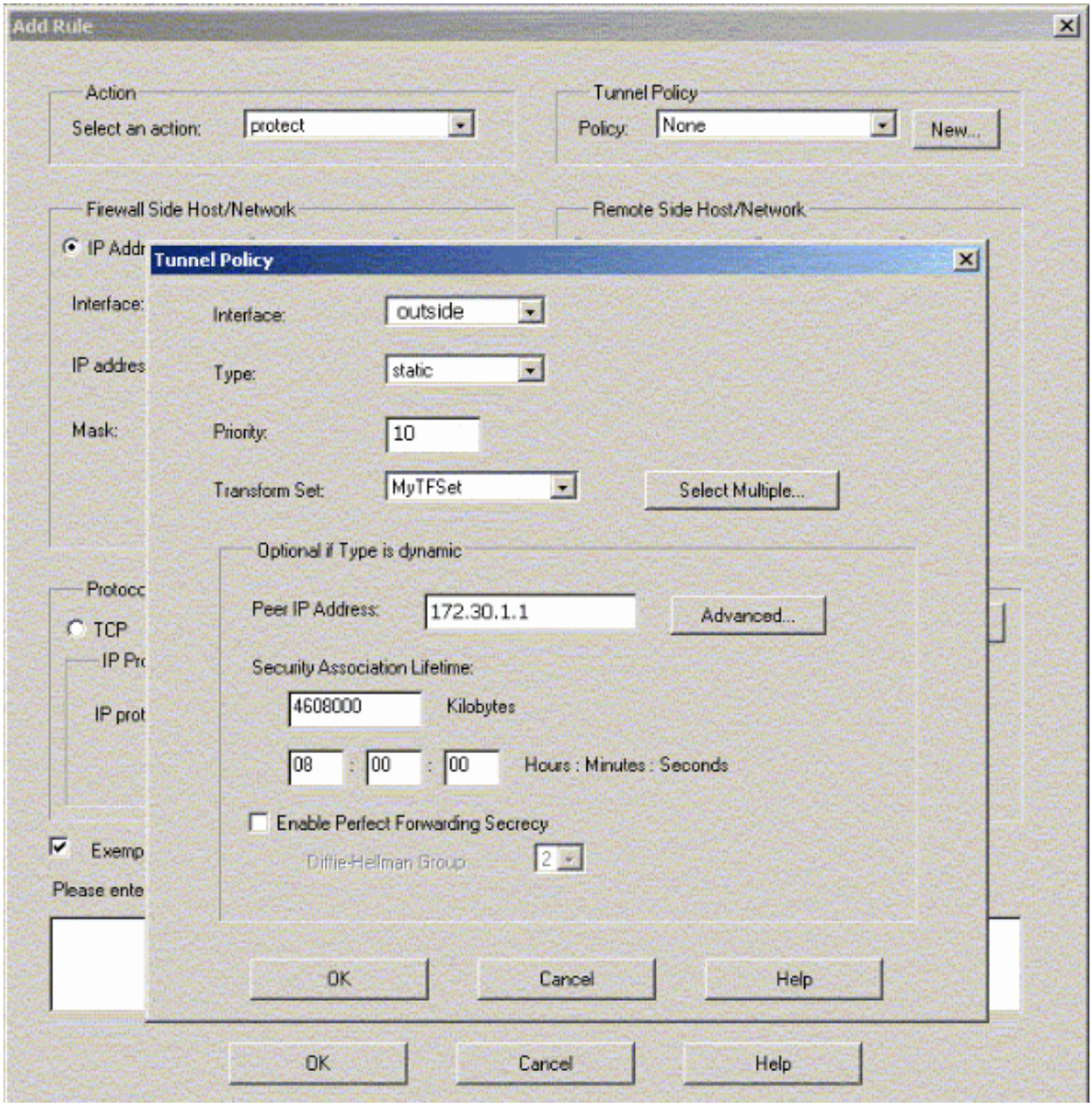
11. Cliquez sur **Règles IPSec** sous IPSec pour créer des règles IPsec.



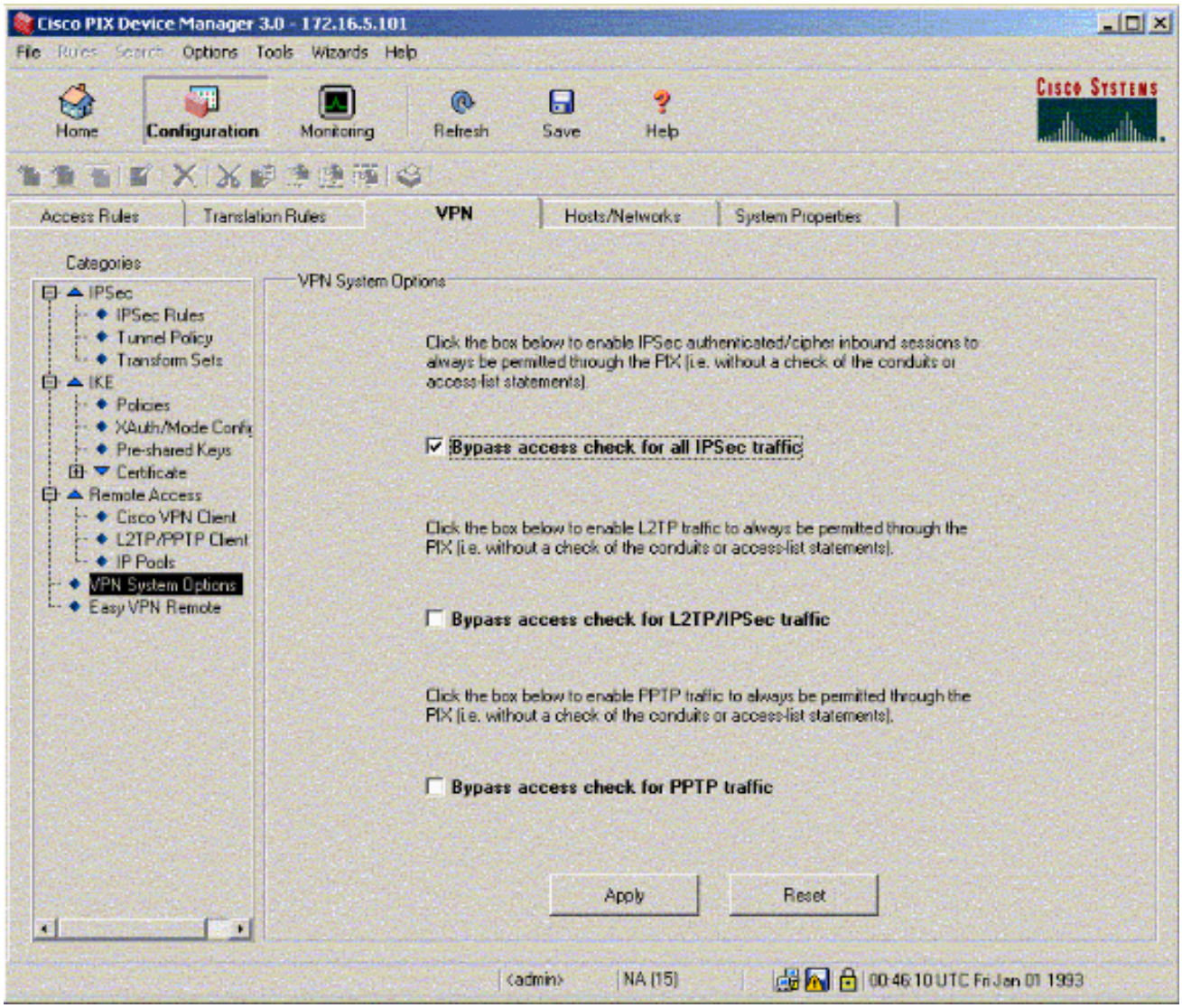
12. Renseignez les champs appropriés.



13. Cliquez sur **Nouveau** dans la stratégie de tunnel. Une fenêtre Tunnel Policy s'affiche. Renseignez les champs
    appropriés.



14. Cliquez sur **OK** pour afficher la règle IPsec configurée.
15. Cliquez sur **Options des systèmes VPN** et cochez **la case Contourner l'accès pour tout le trafic IPSec**.

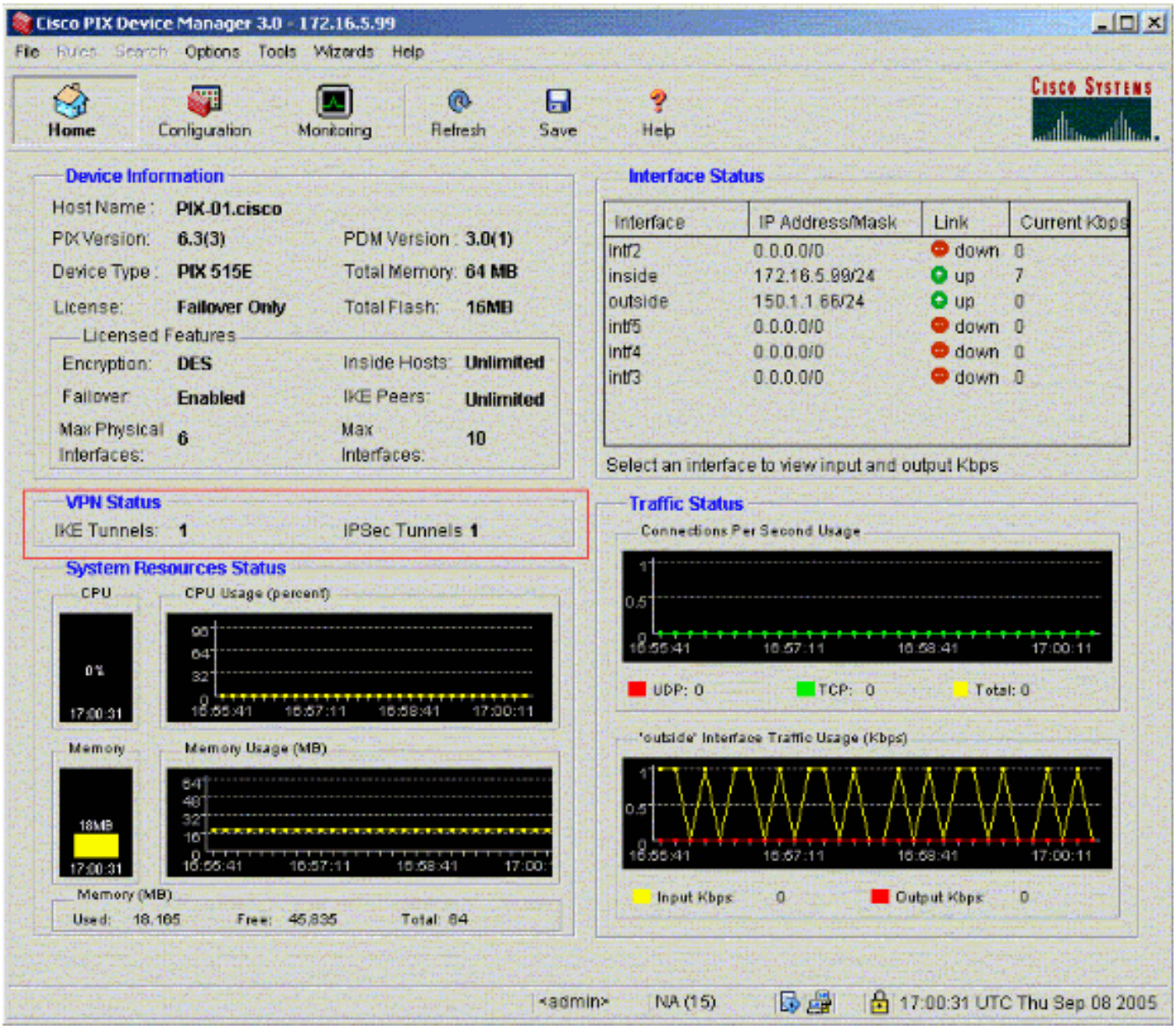


Vérification

S'il y a du trafic intéressant à l'homologue, le tunnel est établi entre pix-01 et PIX-02.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Affichez l'état du VPN sous Accueil dans le PDM (mis en surbrillance en rouge) afin de vérifier la formation du tunnel.



Vous pouvez également vérifier la formation des tunnels à l'aide de l'interface de ligne de commande sous Outils dans le PDM. Exécutez la commande **show crypto isakmp sa pour vérifier la formation des tunnels et exécutez la commande show crypto ipsec sa pour observer le nombre de paquets encapsulés, chiffrés, etc.**

Remarque : L'interface interne du PIX ne peut pas être envoyée par ping pour la formation du tunnel, sauf si la commande management-access est configurée en mode de confirmation globale.

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

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Création de tunnels redondants entre pare-feu à l'aide de PDM
- Références des commandes du pare-feu Cisco Secure PIX
- Demandes de commentaires (RFC)
- Logiciels pare-feu Cisco PIX