LAN-to-LAN VPN-tunnelheid tussen twee PIX's met behulp van een PDM-configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft de procedure om VPN-tunnels tussen twee PIX-firewalls te configureren met Cisco PIX-apparaatbeheer (PDM). PDM is een op een browser gebaseerd configuratiegereedschap dat u moet helpen om uw PIX-firewall met een GUI in te stellen, te configureren en te bewaken. PIX-firewalls worden op twee verschillende locaties geplaatst.

Er wordt een tunnel gevormd met IPsec. IPsec vormt een combinatie van open standaarden die gegevensvertrouwelijkheid, gegevensintegriteit en verificatie van gegevensoorsprong tussen IPsec-peers bieden.

Voorwaarden

Vereisten

Dit document bevat geen eisen.

Gebruikte componenten

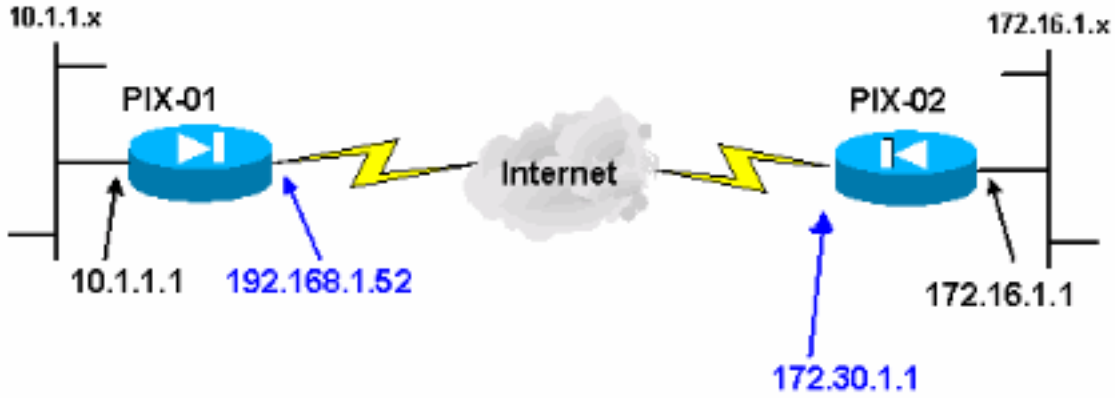
De informatie in dit document is gebaseerd op Cisco Secure PIX 515E Firewalls met 6.x en PDM versie 3.0.

Raadpleeg een Eenvoudige PIX-to-PIX VPN-tunnel configureren met IPsec voor een configuratievoorbeeld in de configuratie van een VPN-tunnel tussen twee PIX-apparaten die de Opdrachtlijn Interface (CLI) gebruiken.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

IPsec-onderhandeling kan in vijf stappen worden onderverdeeld en omvat twee IKE-fasen (Internet Key Exchange).

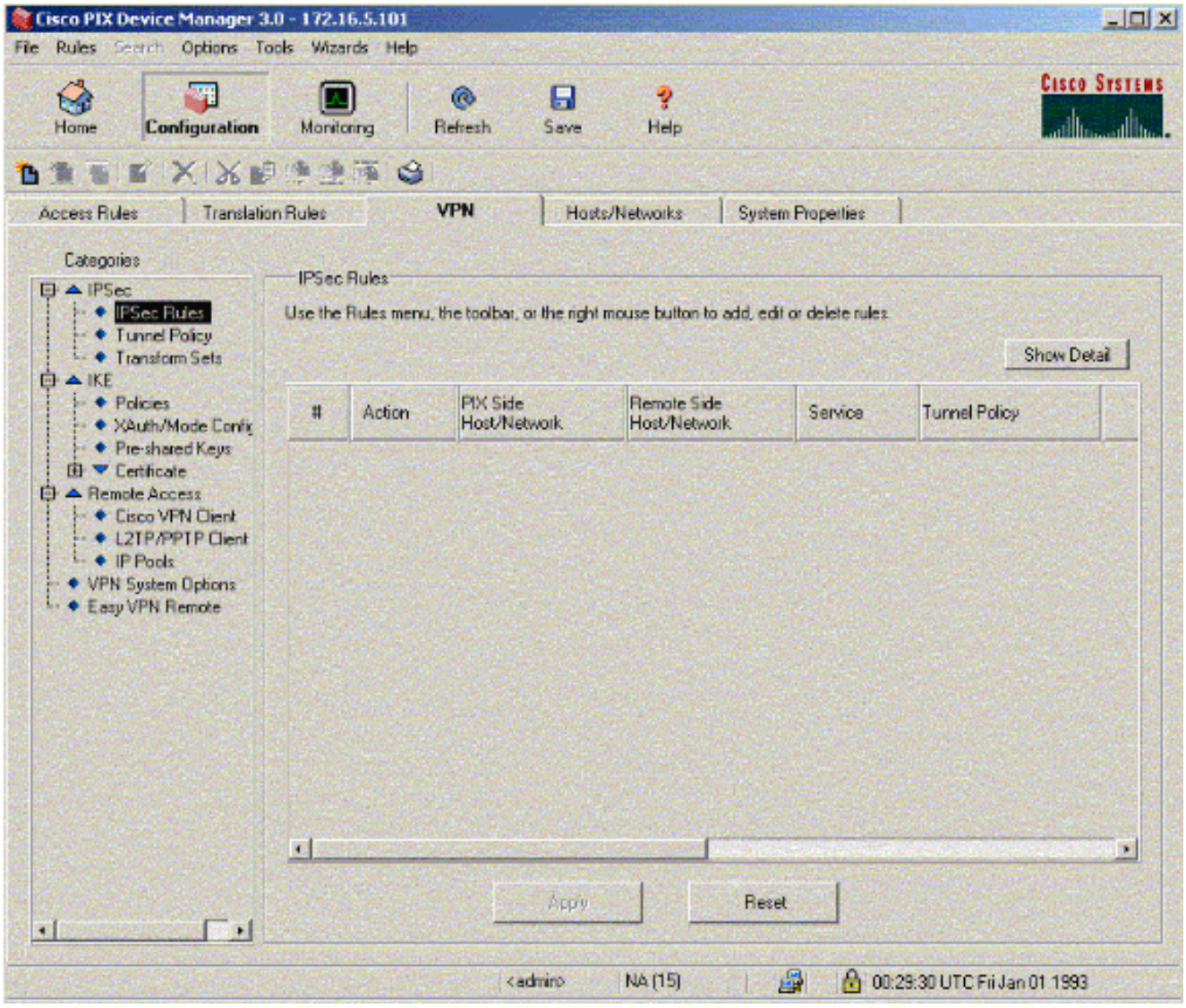
1. Een IPsec-tunnel wordt geïnitieerd door interessant verkeer. Het verkeer wordt als interessant beschouwd wanneer het tussen de IPsec-peers reist.
2. In IKE fase 1 onderhandelen de IPsec-peers over het vastgestelde beleid van de IKE Security Association (SA). Zodra de peers echt zijn bevonden, wordt er een beveiligde tunnel aangemaakt met behulp van Internet Security Association en Key Management Protocol (ISAKMP).
3. In IKE Fase 2, gebruiken de IPsec peers de geauthenticeerde en veilige tunnel om IPsec SA transformaties te onderhandelen. De onderhandelingen over het gedeelde beleid bepalen hoe de IPsec-tunnel tot stand wordt gebracht.
4. De IPsec-tunnel wordt gecreëerd en er worden gegevens tussen de IPsec-peers overgebracht, op basis van de IPsec-parameters die zijn ingesteld in de transformatiesets van IPsec.
5. De IPsec-tunnel eindigt wanneer de IPsec SA's worden verwijderd of wanneer hun levensduur verlopen.**Opmerking:** IPsec-onderhandeling tussen de twee PIX's mislukt als de SA's in beide IKE-fasen niet op de peers overeenkomen.

Configuratieprocedure

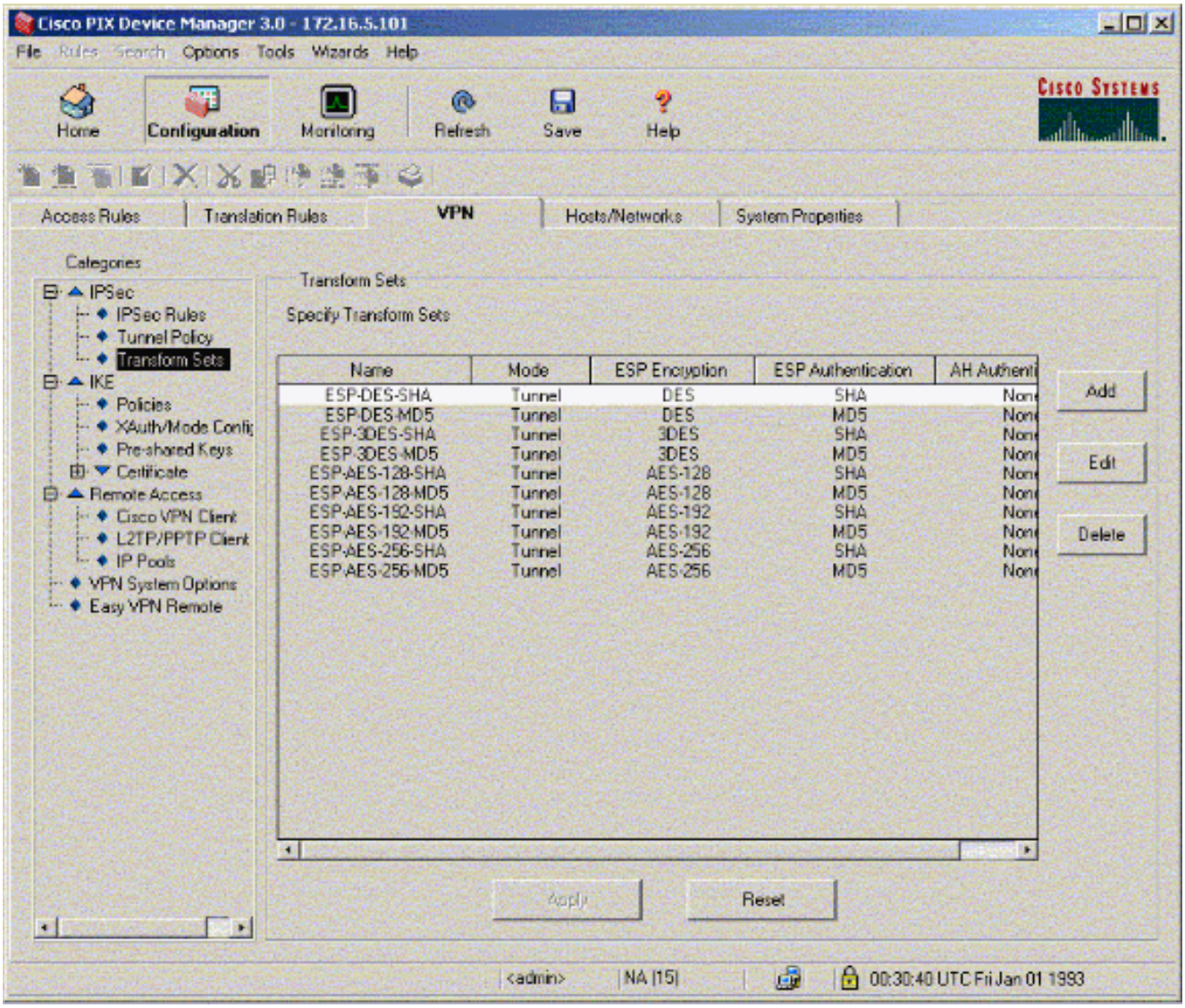
Naast andere algemene configuratie op de CLI of PIX om toegang tot de opdracht via de Ethernet 0-interface te krijgen, gebruikt u de opdrachten **http server** en **http server <local_ip> <mask>** ***<local_ip>*** en **masker> het IP-adres en het masker van het werkstation waarop PDM is geïnstalleerd.** De configuratie in dit document is voor PIX-01. PIX-02 kan worden geconfigureerd met behulp van dezelfde stappen met verschillende adressen.

Voer de volgende stappen uit:

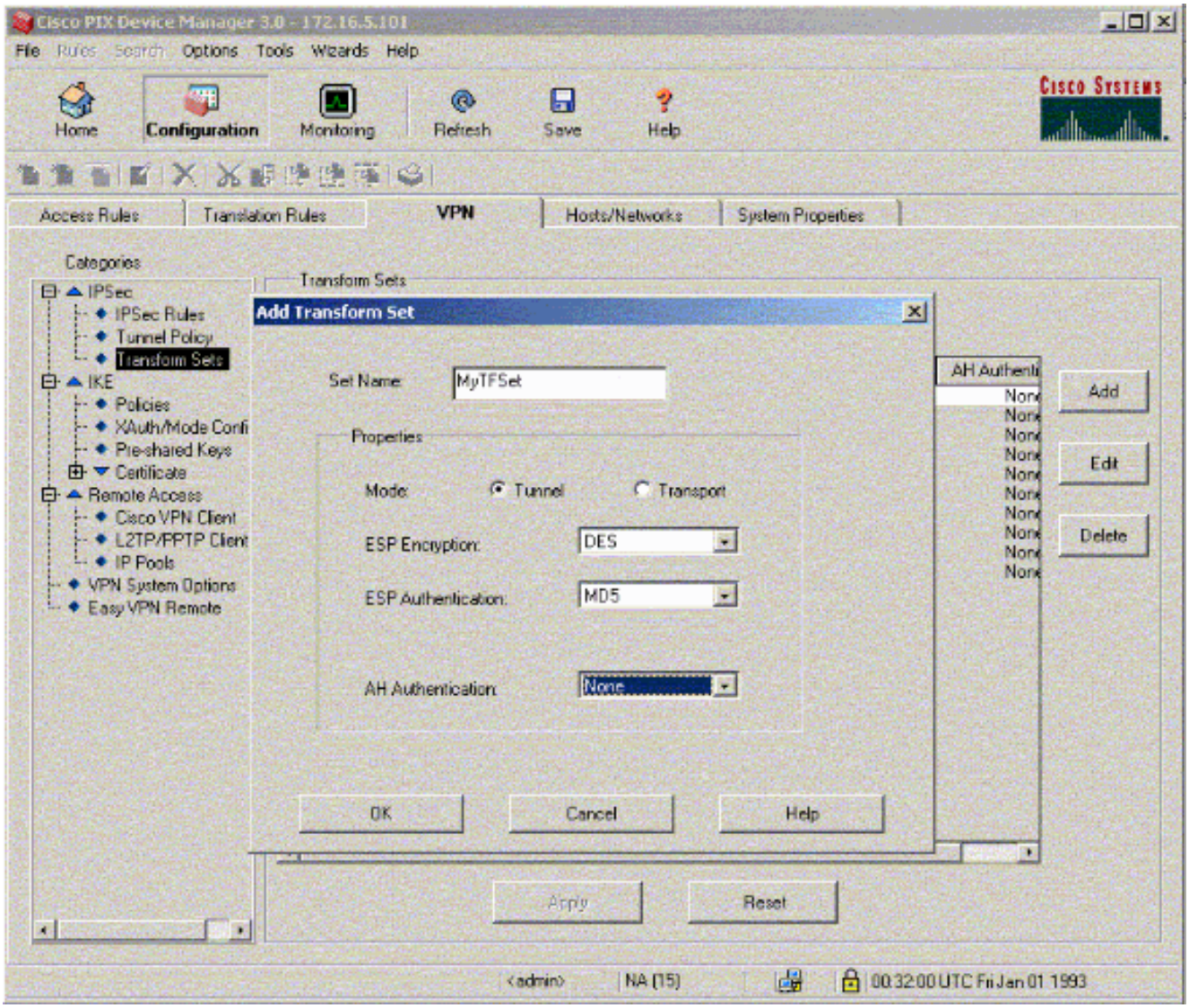
1. Open uw browser en type **<Inside_IP_Address_of_PIX>**om de PIX in PDM te gebruiken.
2. Klik op **Configuration** en ga naar het tabblad VPN.



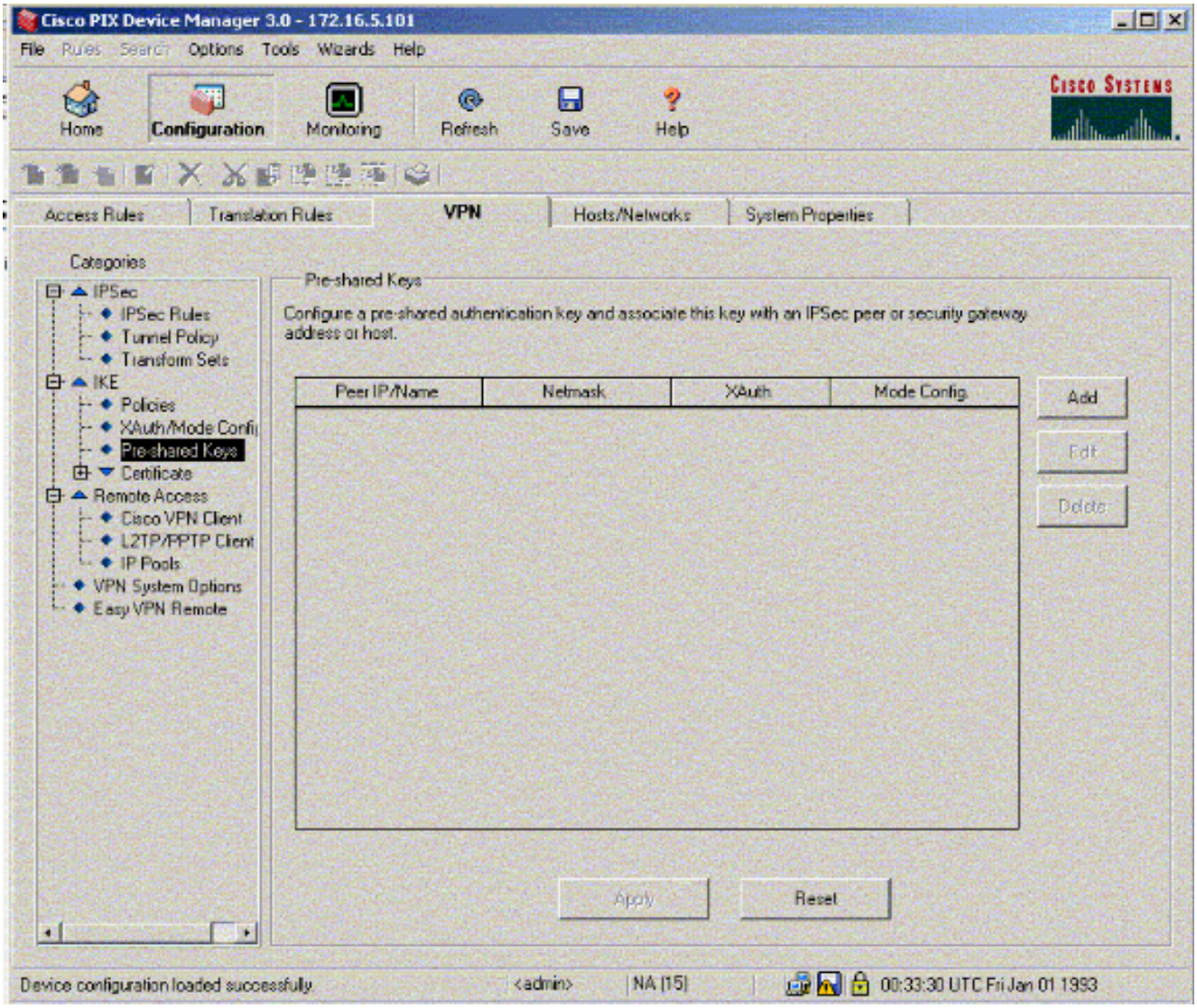
3. Klik op **Omzetten** om onder IPSec een set van transformaties te maken.



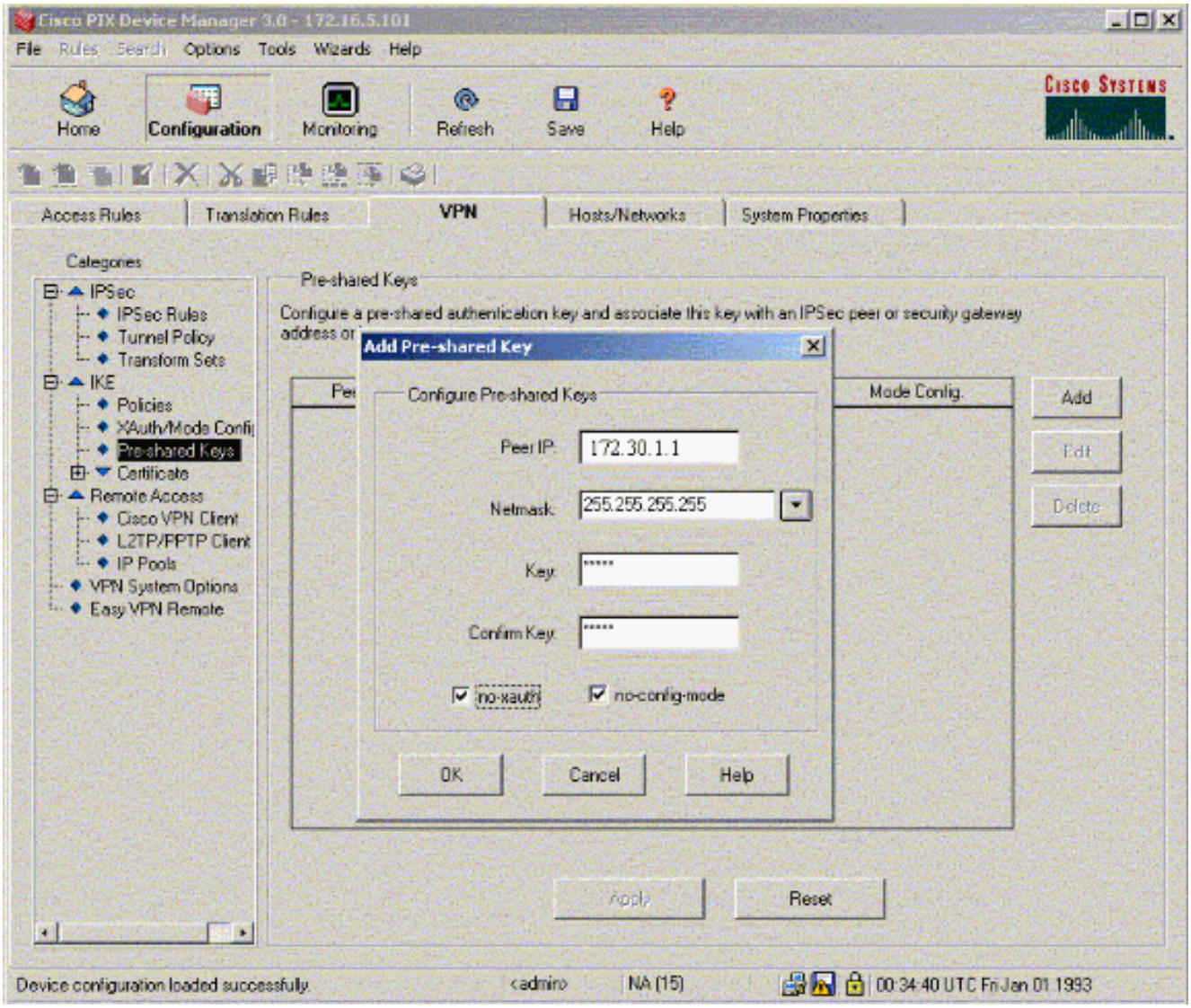
4. Klik op **Toevoegen**, selecteer alle gewenste opties en klik op **OK** om een nieuwe serie Omzetten te
maken.



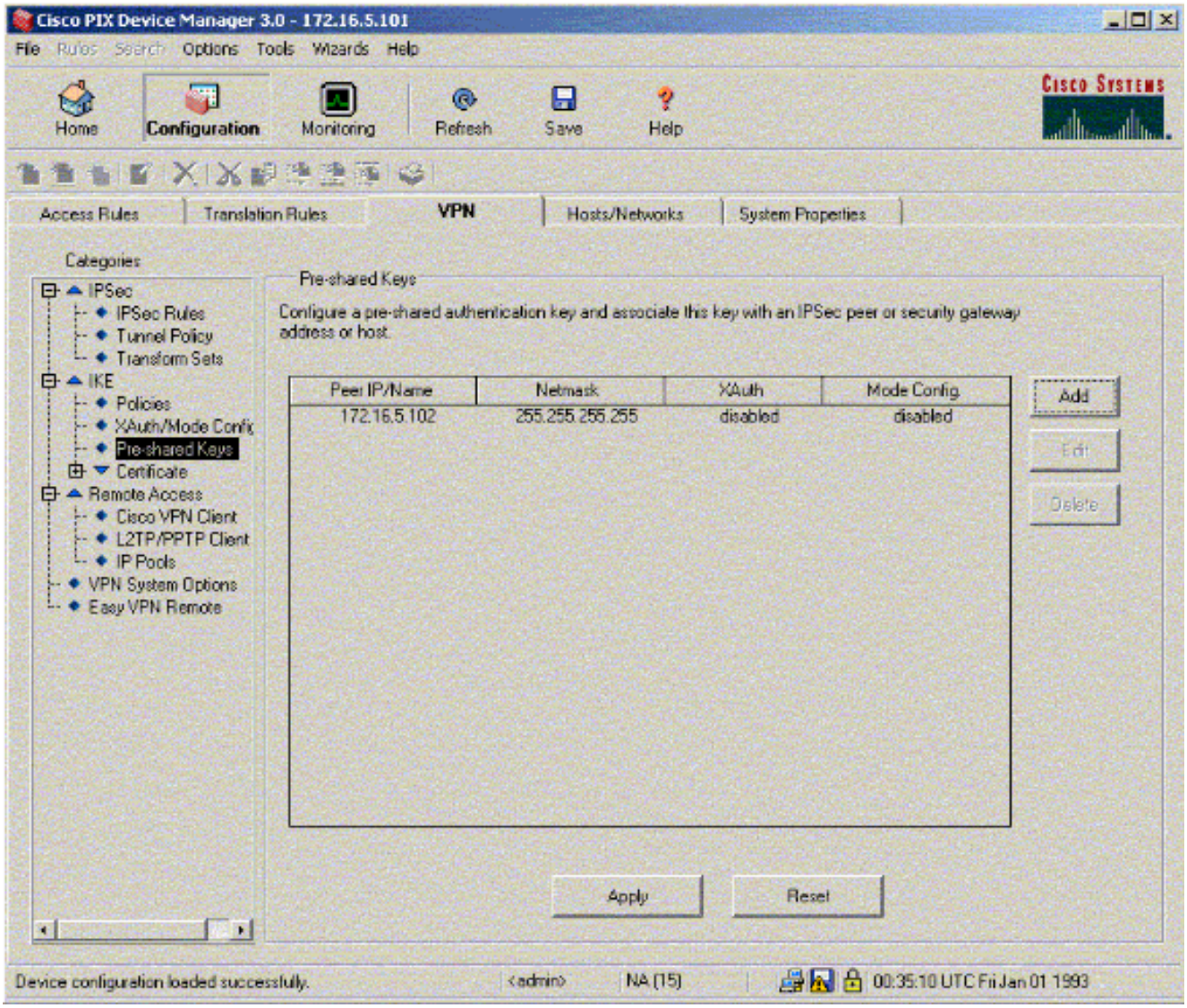
5. Klik op **Vooraf gedeelde toetsen** onder IKE om voorgedeelde toetsen te configureren.



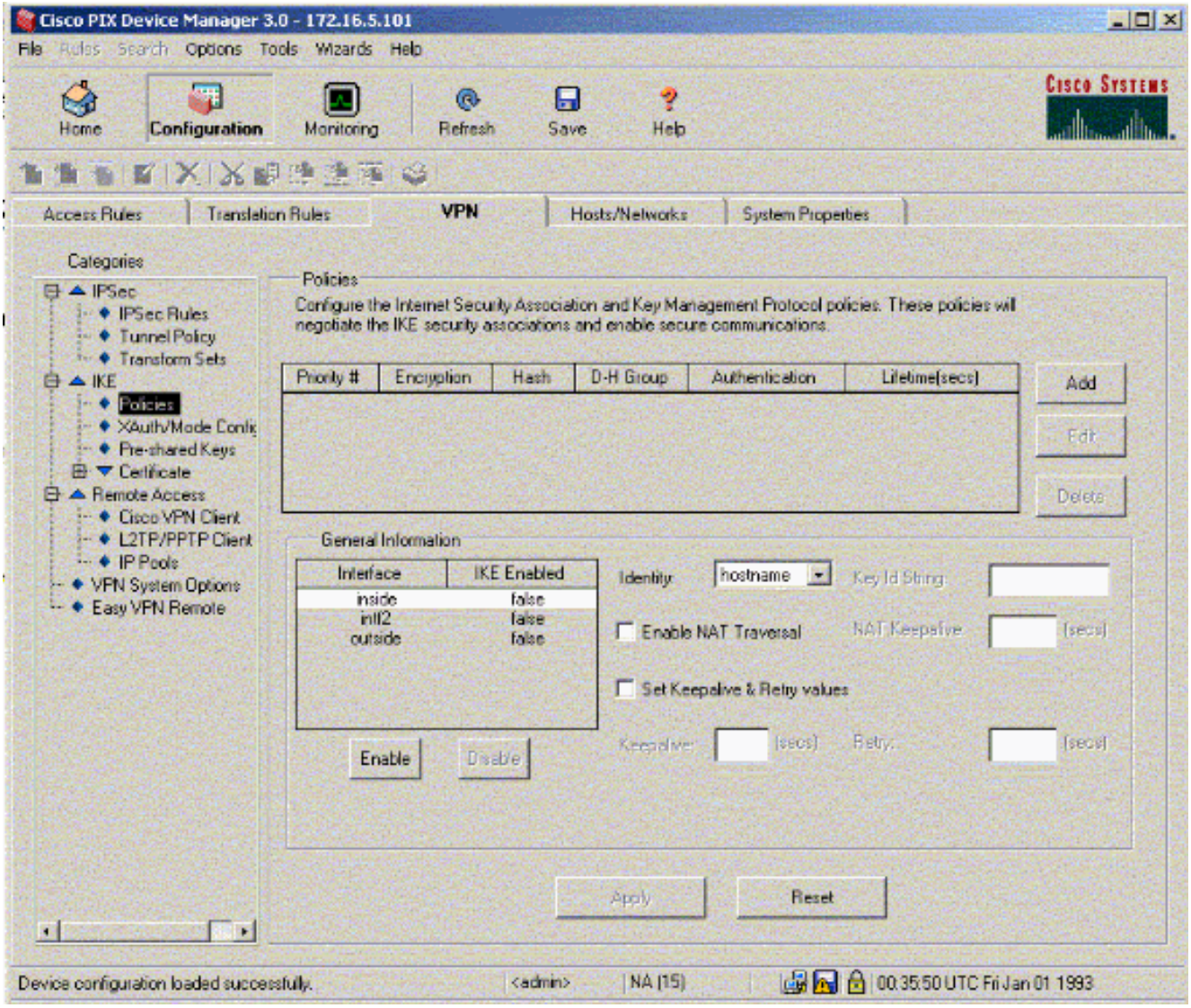
6. Klik op **Add** om een nieuwe voorgedeelde toets toe te voegen.



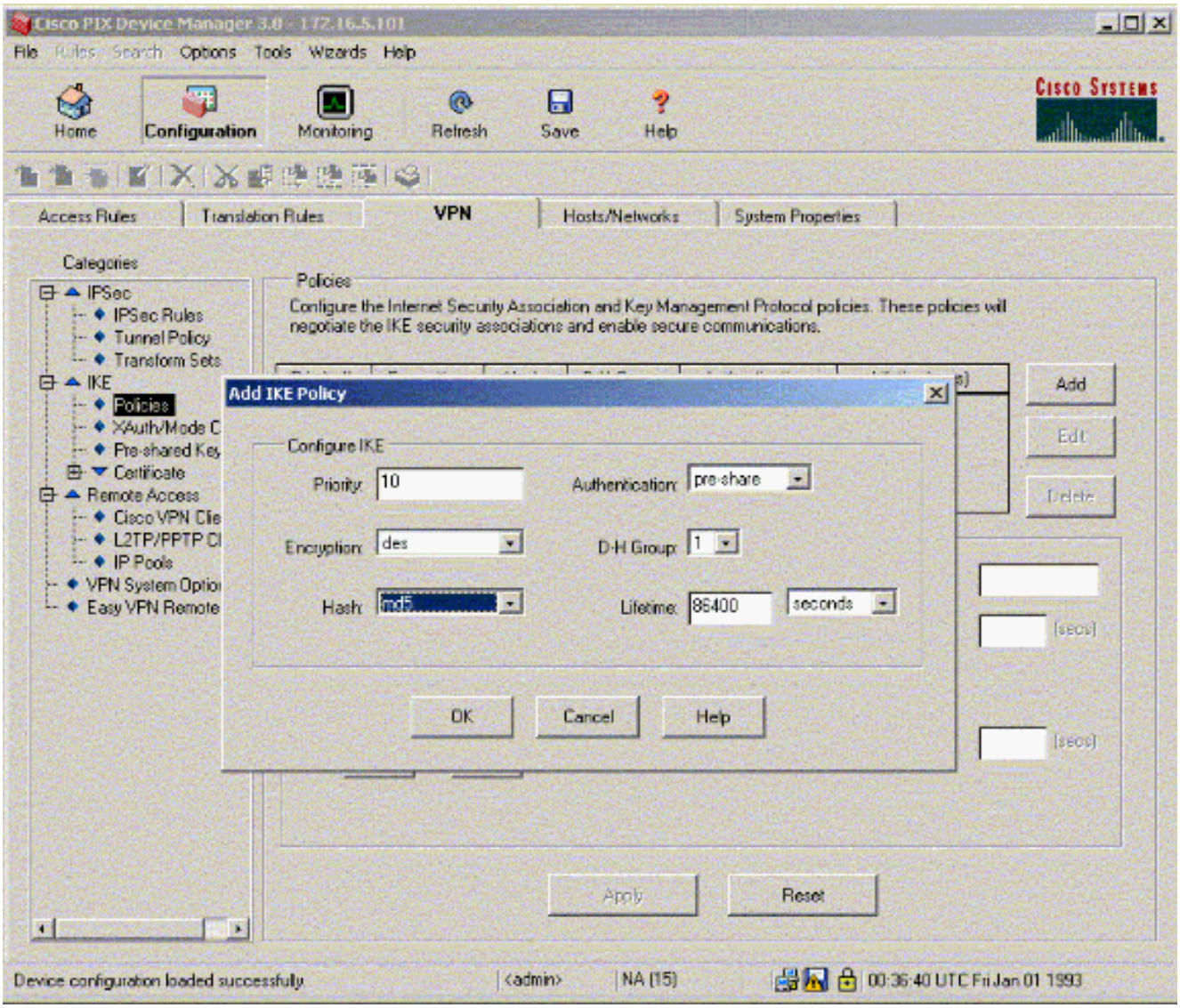
Dit venster toont de sleutel, het wachtwoord voor de tunnelassociatie. Dit moet aan beide zijden van de tunnel
passen.



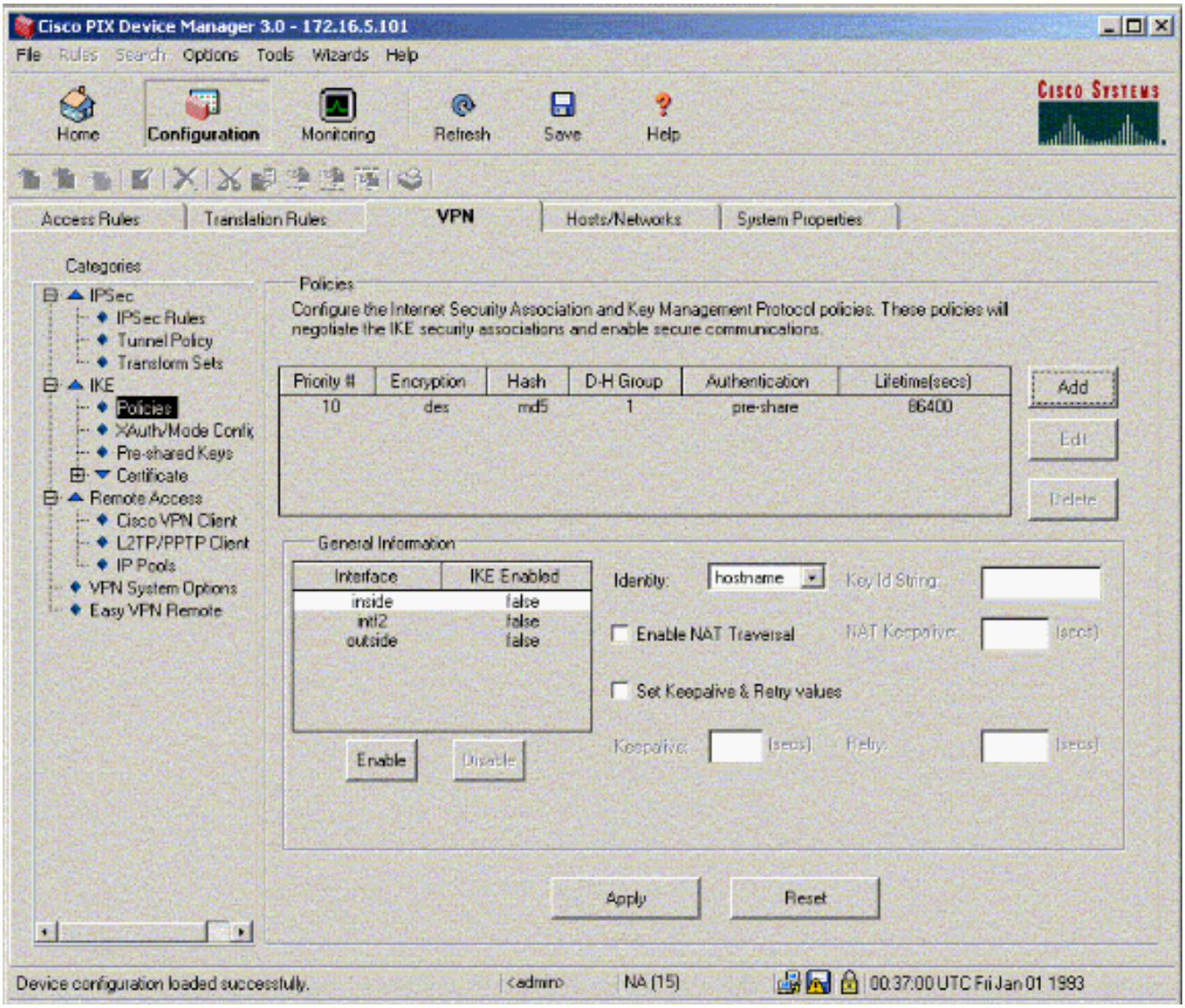
7. Klik onder IKE op **beleid** om het beleid te configureren.



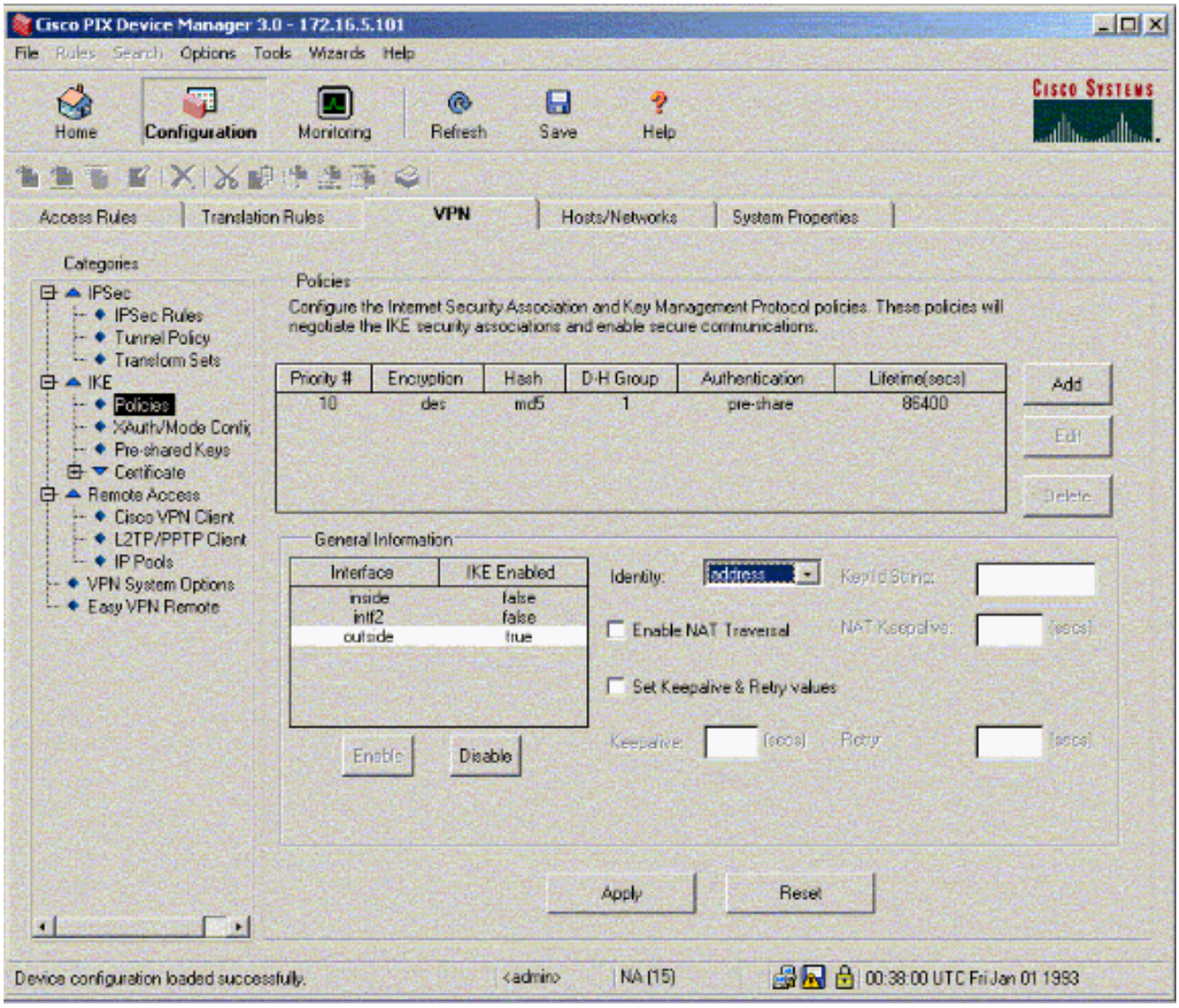
8. Klik op **Toevoegen** en invullen van de juiste velden.



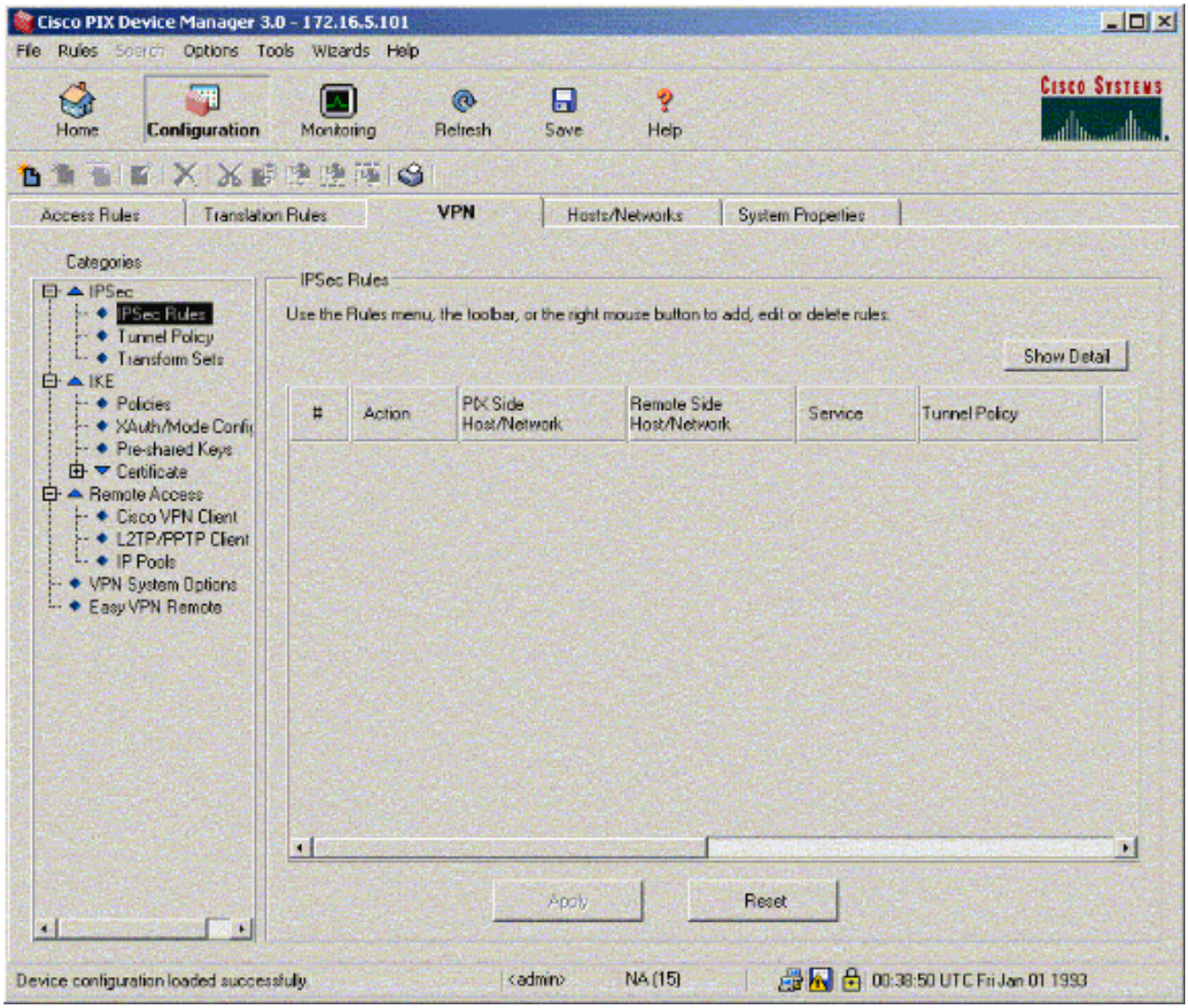
9. Klik op **OK** om een nieuw beleid toe te voegen.



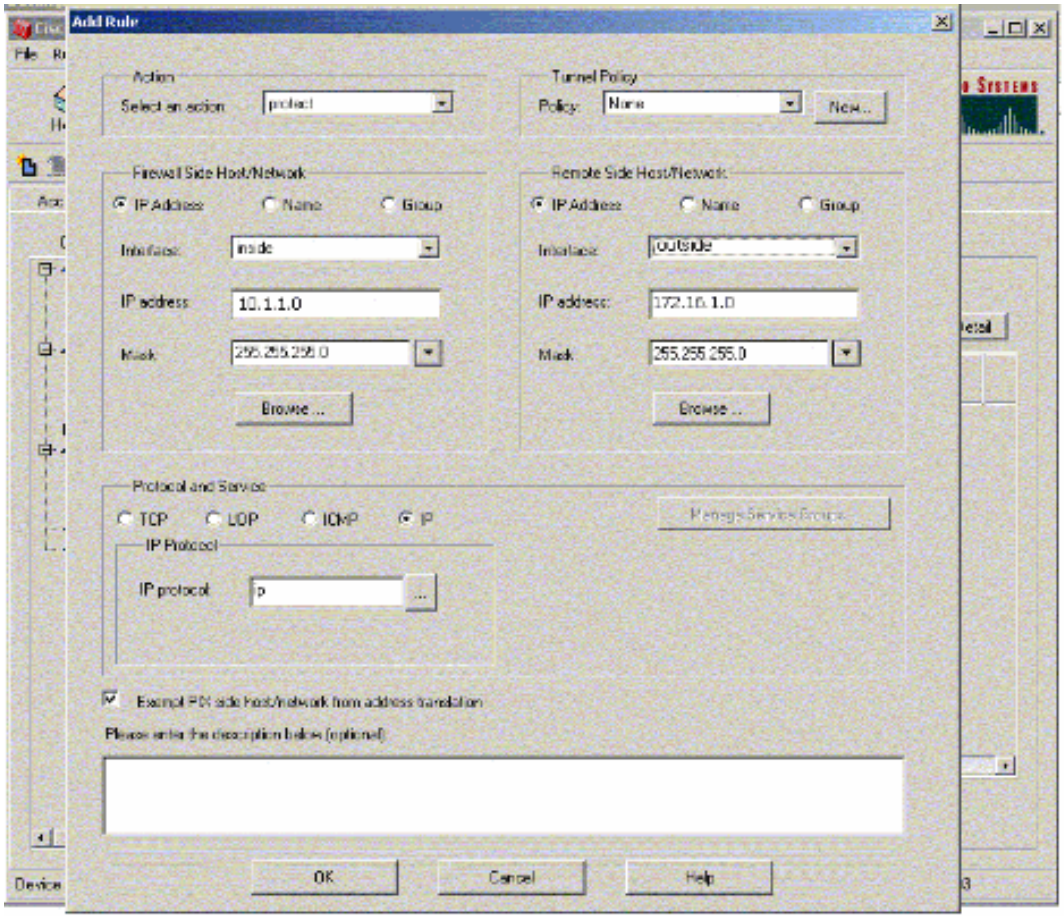
10. Selecteer de **externe** interface, klik op **Enable** en selecteer **adres** in het keuzemenu Identity.



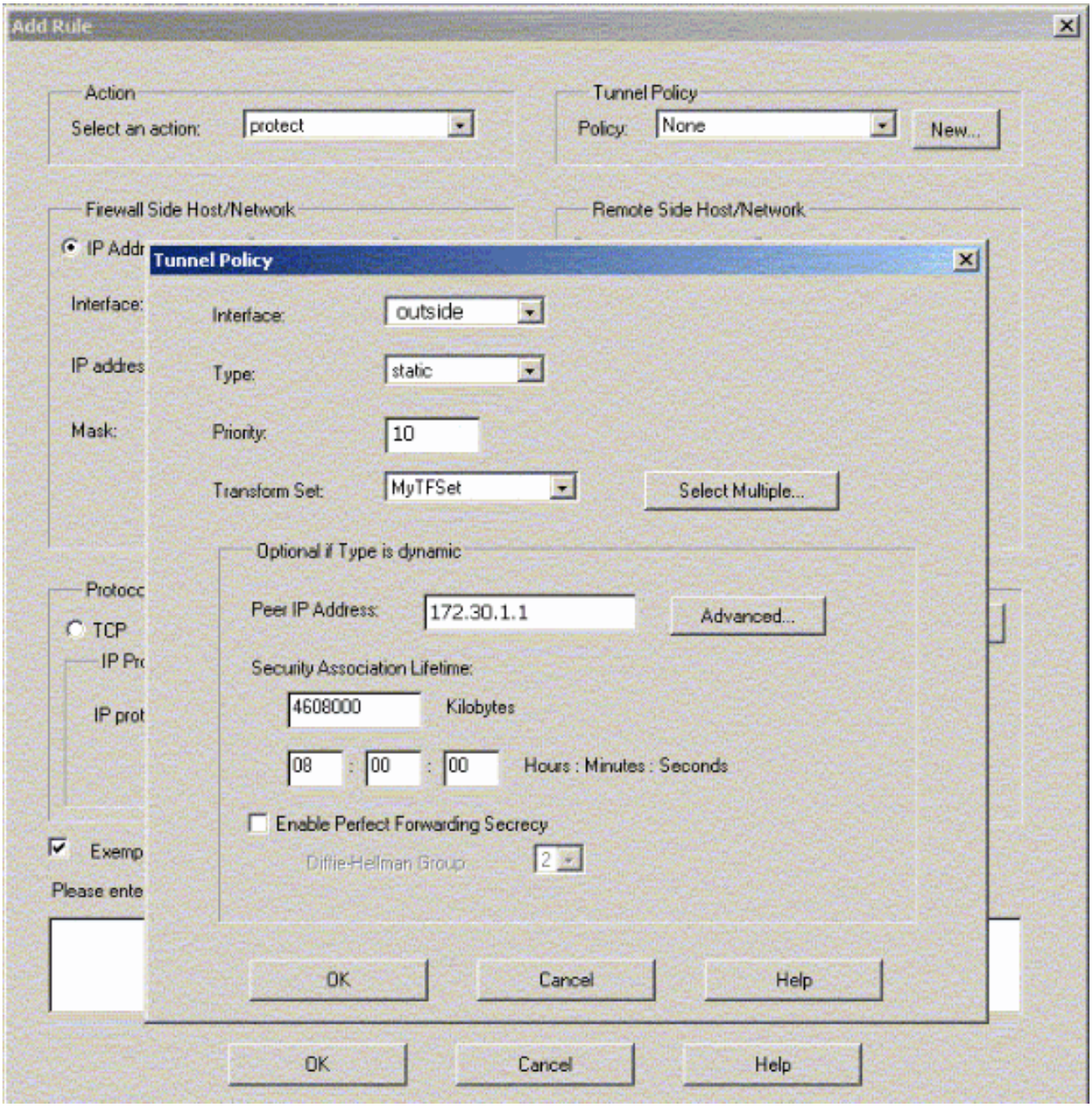
11. Klik op **IPsec-regels** onder IPSec om IPsec-regels te maken.



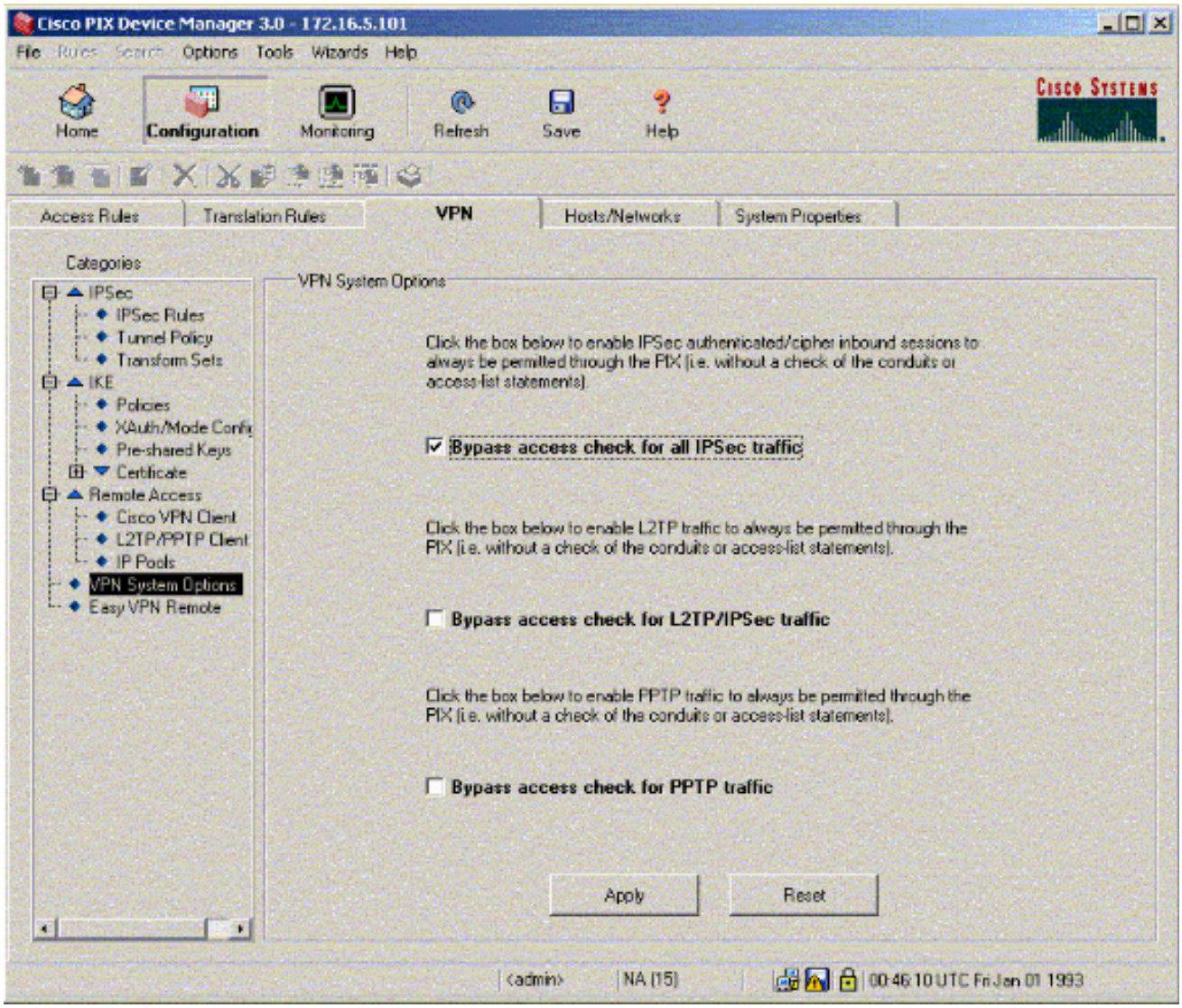
12. Vul de juiste velden in.



13. Klik op **Nieuw** in het Tunnelbeleid. Er verschijnt een venster voor tunnelbeleid. Vul de juiste velden
in.



14. Klik op **OK** om de geconfigureerde IPsec-regel te zien.
15. Klik op **VPN-systeemopties** en controleer **de toegangscontrole voor omzeilen voor al het IPSec-verkeer**.

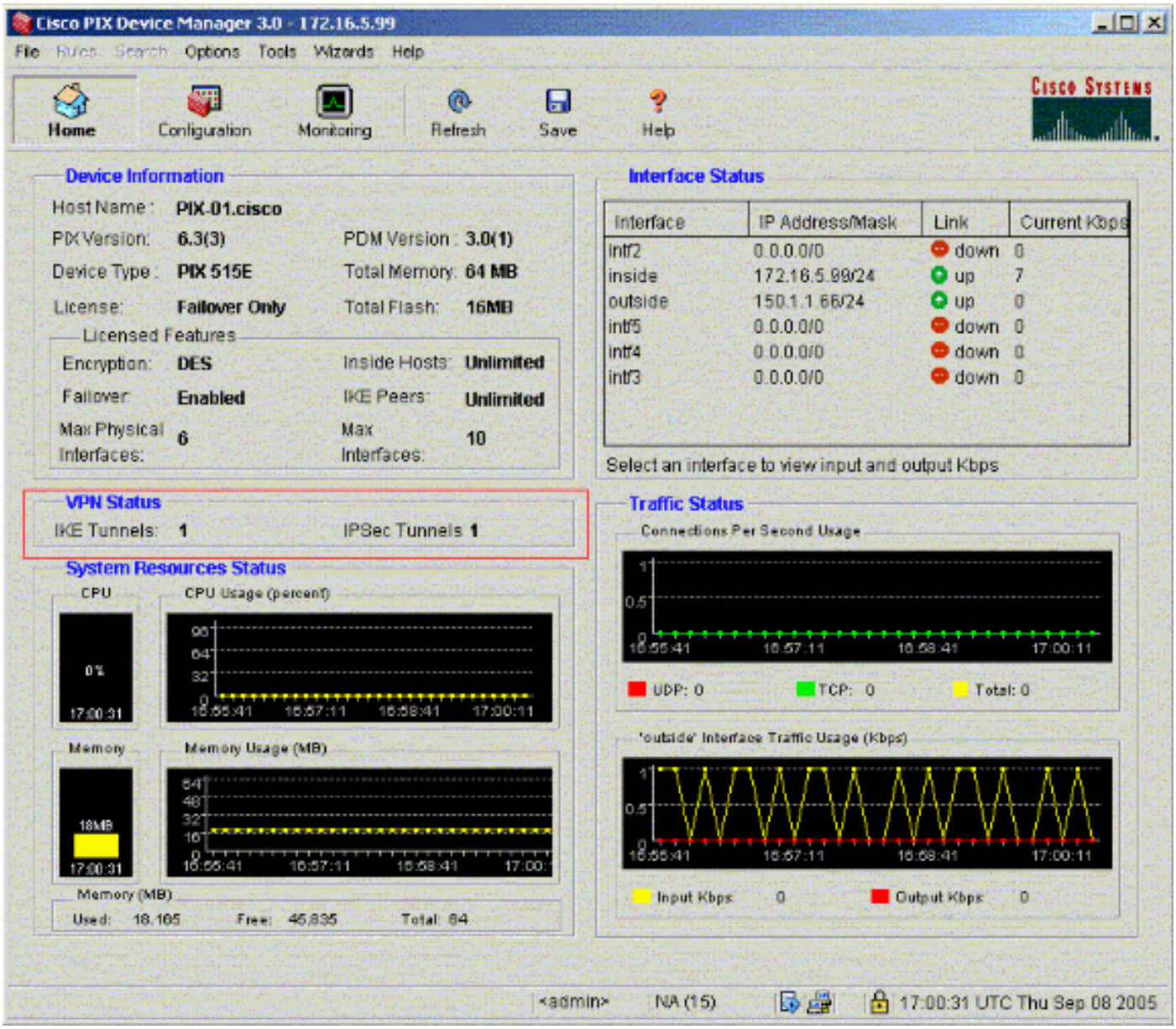


Verifiëren

Als er interessant verkeer naar de peer is, wordt de tunnel ingericht tussen PIX-01 en PIX-02.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Bekijk de VPN-status onder Start in de PDM (rood gemarkeerd) om de vorming van de tunnel te controleren.



U kunt ook de vorming van tunnels met CLI controleren onder Gereedschappen in de PDM. Geef de opdracht **show crypto isakmp als** opdracht uit om de vorming van tunnels te controleren en de **show crypto ipsec als** opdracht **uit** te **geven** om het aantal ingekapselde, gecodeerde pakketten, enzovoort te observeren.

Opmerking: De interne interface van de PIX kan niet worden gepingeld voor de samenstelling van de tunnel tenzij de opdracht **beheertoegang** is ingesteld in de wereldwijde bevestigingsmodus.

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

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Redundant tunnelvorming tussen firewalls met PDM

- Opdrachtreferenties van Cisco Secure PIX-firewall
- Verzoeken om opmerkingen (RFC's)
- Cisco PIX-firewallsoftware