Redundant tunnelvorming tussen firewalls met PDM

Inhoud

Inleiding

Dit document beschrijft de procedure die u gebruikt om tunnels tussen twee PIX-firewalls te configureren met Cisco PIX-apparaatbeheer (PDM). PIX-firewalls worden op twee verschillende locaties geplaatst. In het geval van het niet bereiken van het primaire pad is het wenselijk om de tunnel uit te zetten door een overtollige verbinding. IPsec vormt een combinatie van open standaarden die gegevensvertrouwelijkheid, gegevensintegriteit en verificatie van gegevensoorsprong tussen IPsec-peers bieden.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

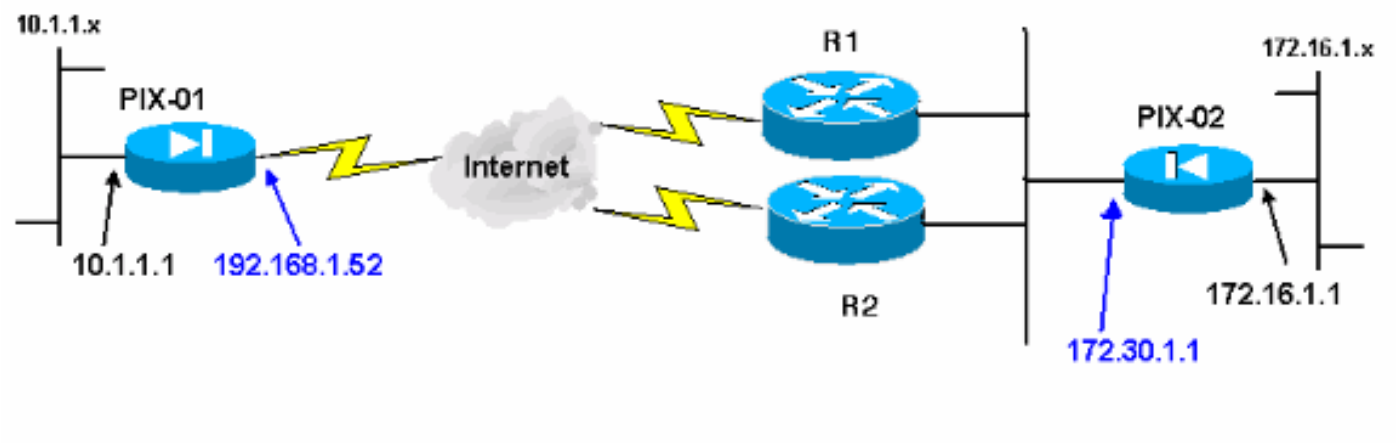
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure PIX 5150E firewalls met 6.x en PDM versie 3.0

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).

Een IPsec-tunnel wordt geïnitieerd door interessant verkeer. Het verkeer wordt als interessant beschouwd wanneer het tussen de IPsec-peers reist.

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).

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.

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.

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.

Configuratie

Deze procedure leidt je door de configuratie van één van de PIX-firewalls om de tunnel te activeren wanneer er interessant verkeer is. Deze configuratie helpt u ook de tunnel door de back-uplink door router 2 (R2) te creëren, wanneer er geen connectiviteit is tussen de PIX-01 en PIX-02

door router 1 (R1). Dit document toont de configuratie van PIX-01 met behulp van PDM. U kunt PIX-02 op soortgelijke lijnen configureren.

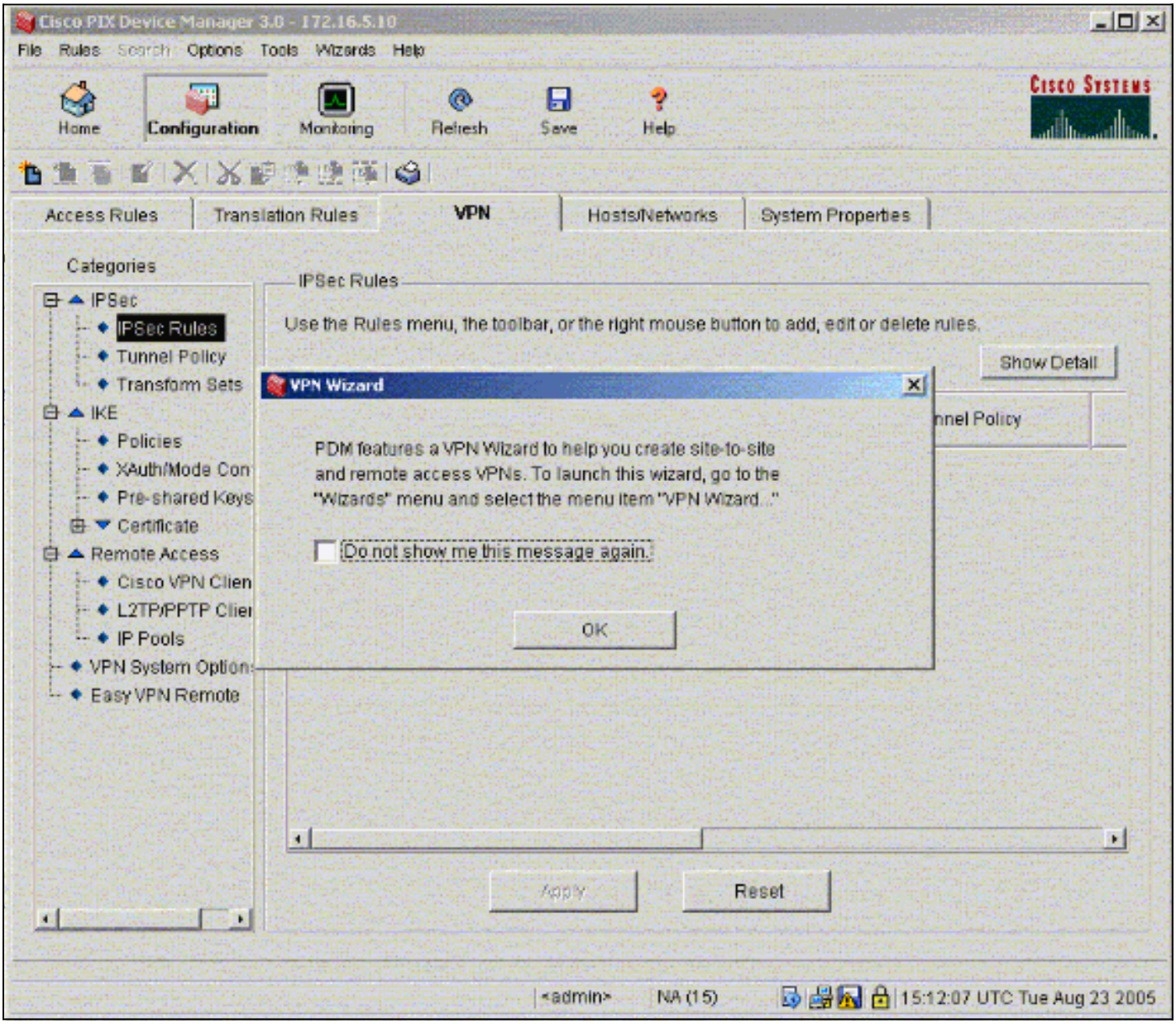
Dit document gaat ervan uit dat u de routing al hebt ingesteld.

Als slechts één verbinding in één keer omhoog moet zijn, maak R2 adverteer een erger metriek voor het 192.168.1.0 netwerk evenals voor het 172.30.0.0 netwerk. Als u bijvoorbeeld RIP voor het routing gebruikt, heeft R2 deze configuratie behalve andere netwerkadvertenties:

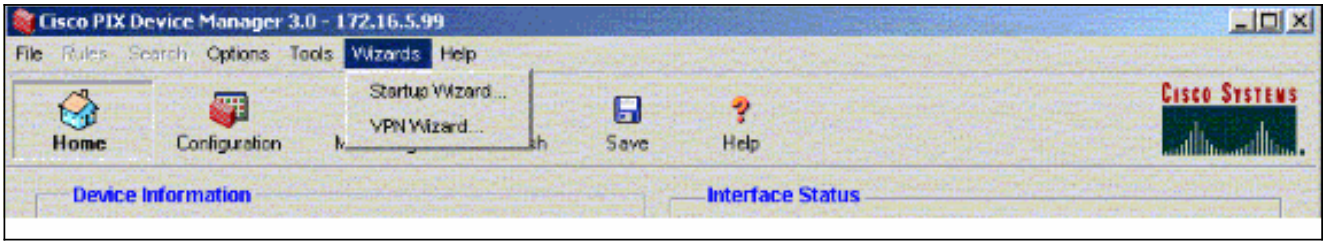
```
R2(config)#router rip
R2(config-router)#offset-list 1 out 2 s1
R2(config-router)#offset-list 2 out 2 e0
R2(config-router)#exit
R2(config)#access-list 1 permit 172.30.0.0 0.0.255.255
R2(config)#access-list 2 permit 192.168.1.0 0.0.0.255
```

Configuratieprocedure

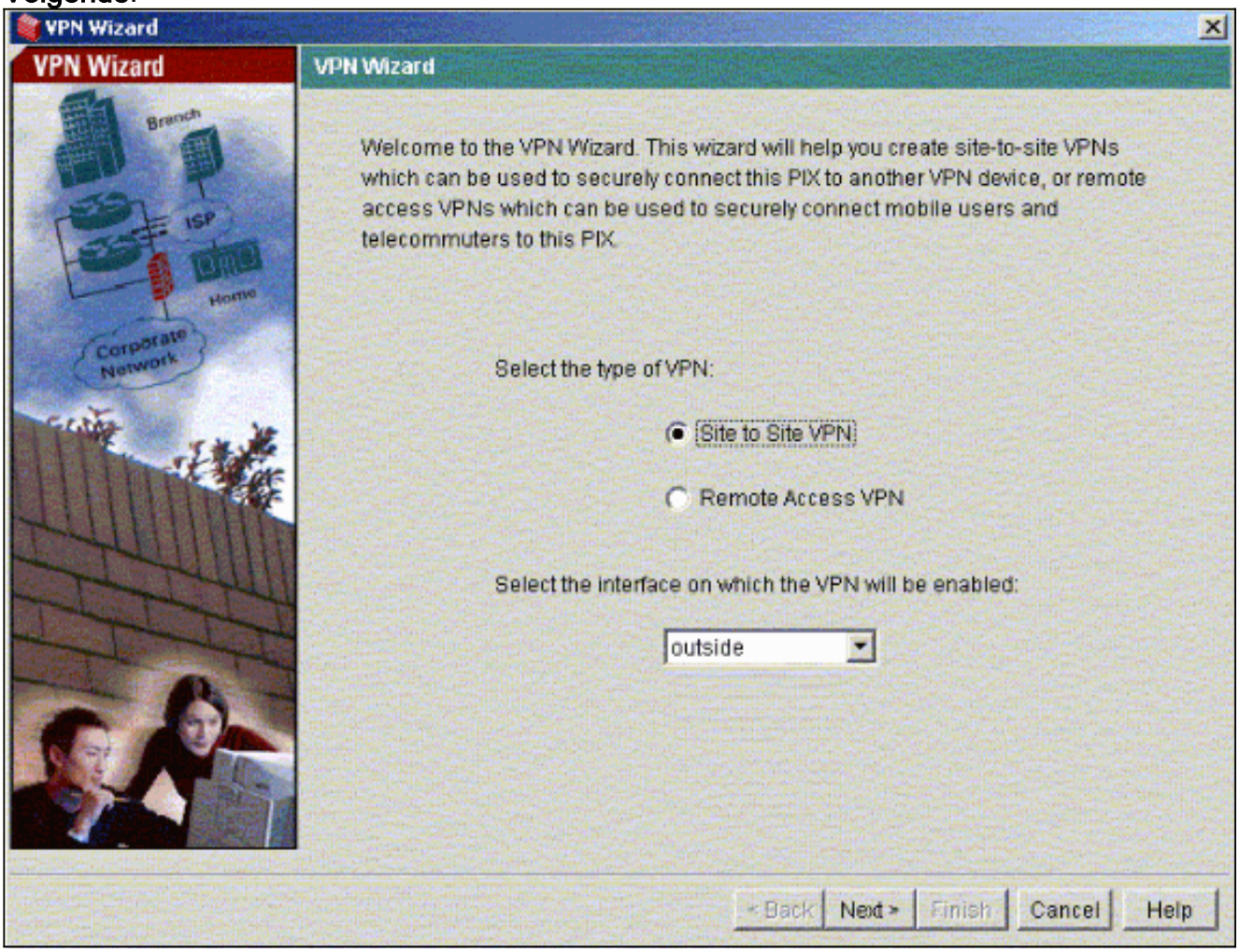
Wanneer u **https://<Inside_IP_Address_on_PIX>**typt om PDM te starten en voor het eerst op het tabblad VPN klikt, wordt informatie over de automatische VPN-wizard weergegeven.



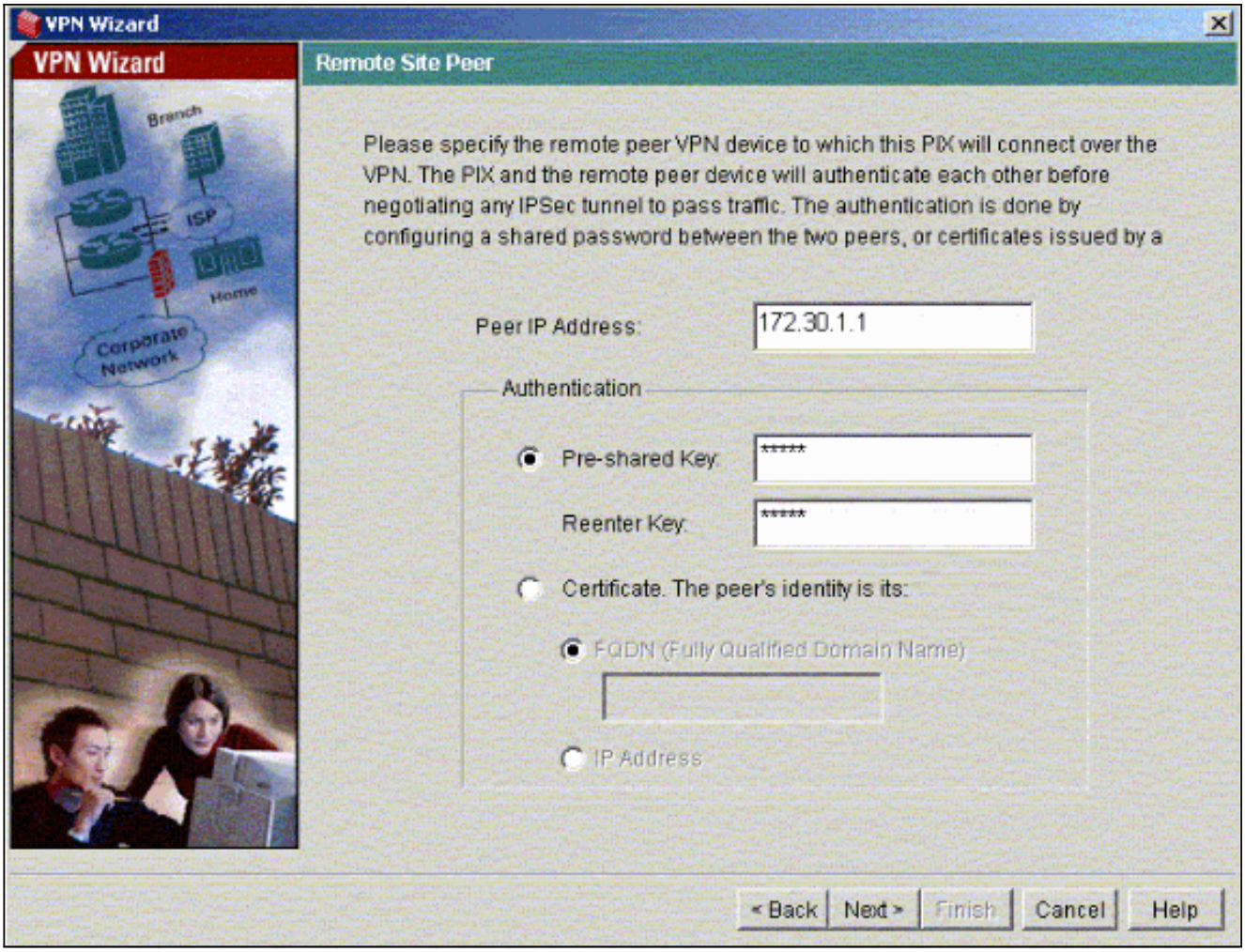
1. Selecteer **Wizard >**
   VPN.



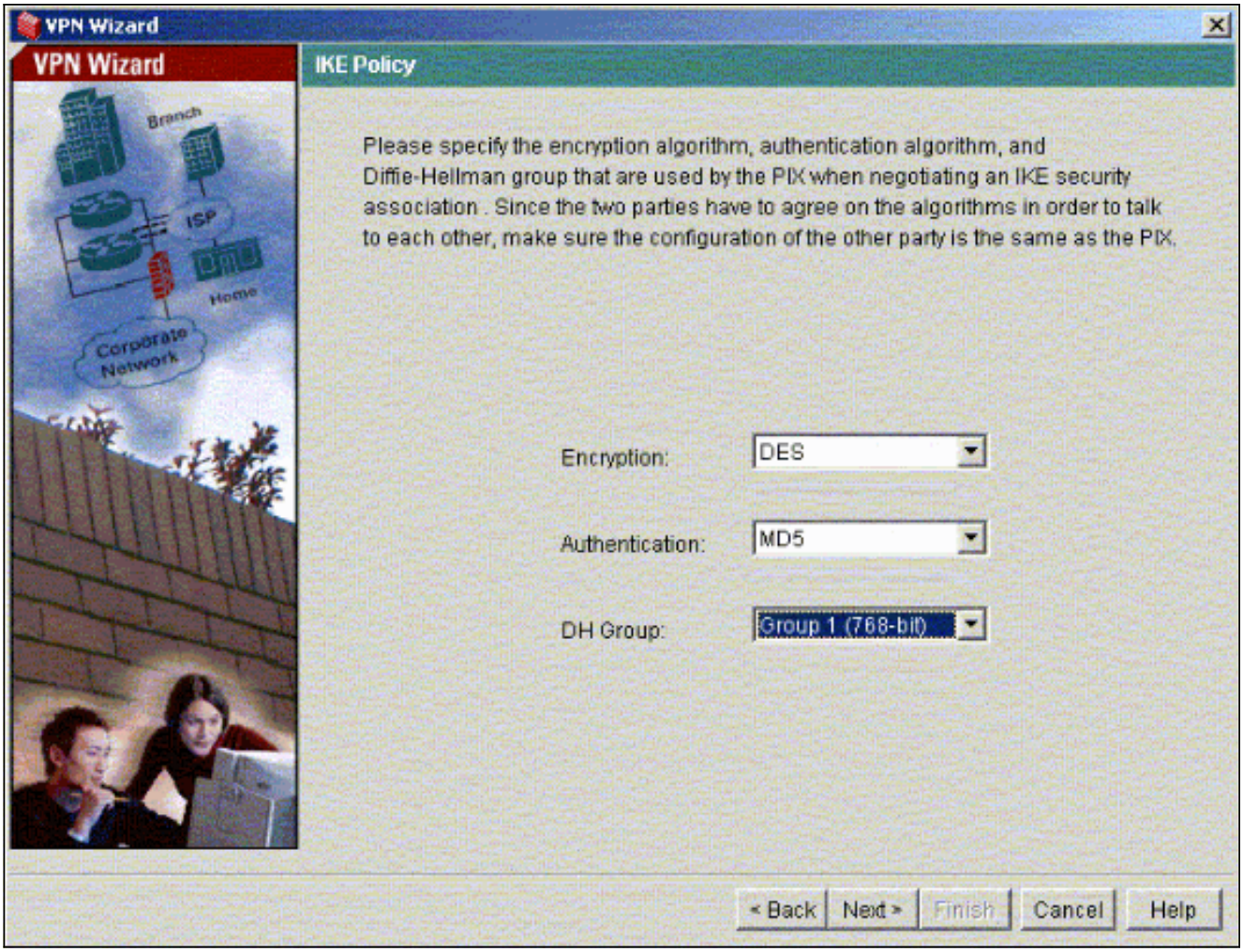
2. De wizard VPN start en vraagt u om het type VPN dat u wilt configureren. Kies **Site-to-Site VPN**, selecteer de **externe** interface als de interface waarop VPN ingeschakeld zal worden en klik op
   Volgende.



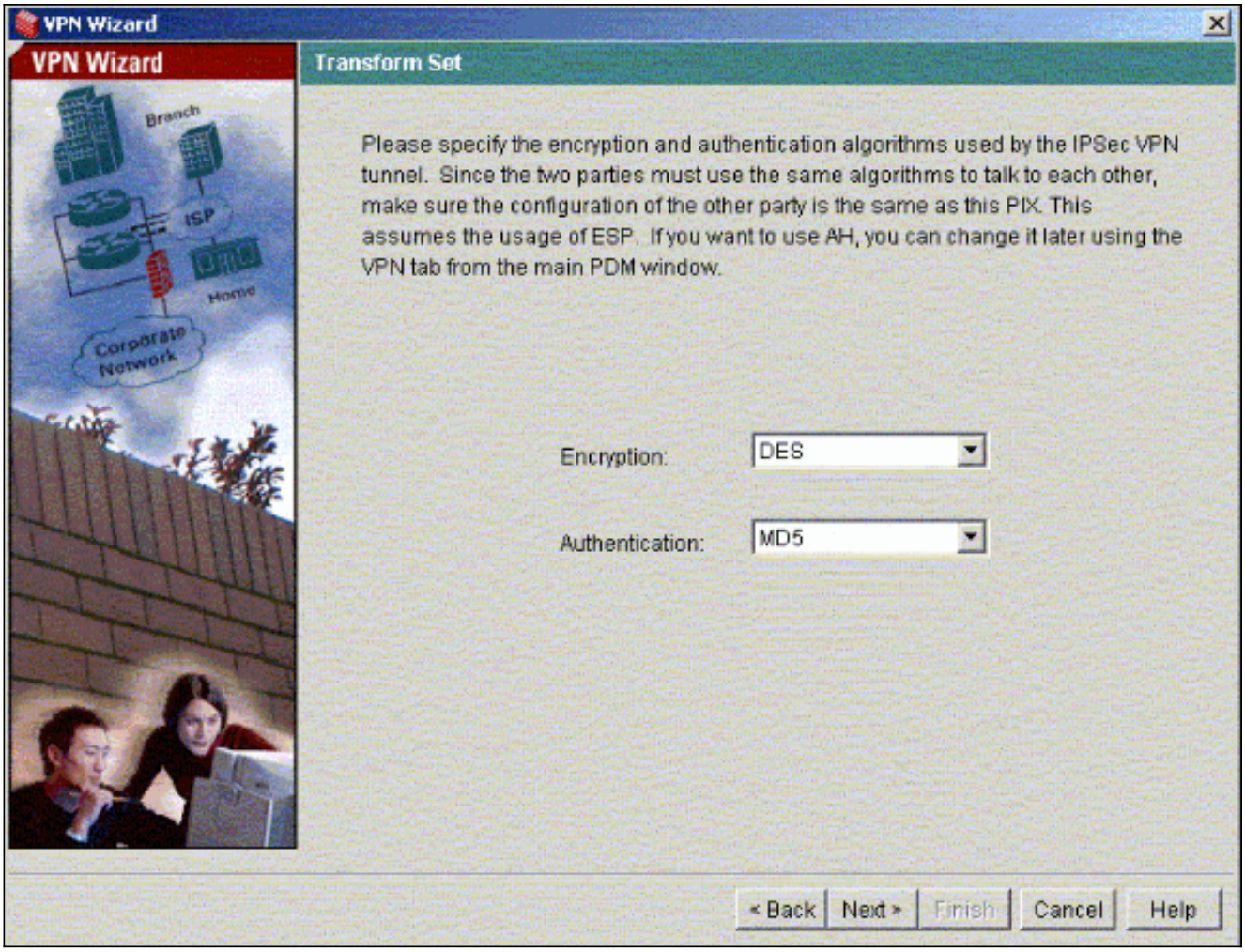
3. Voer het peer IP-adres in, waar de IPsec-tunnel moet stoppen. In dit voorbeeld eindigt de tunnel op de buiteninterface van PIX-02. Klik op
   Volgende.



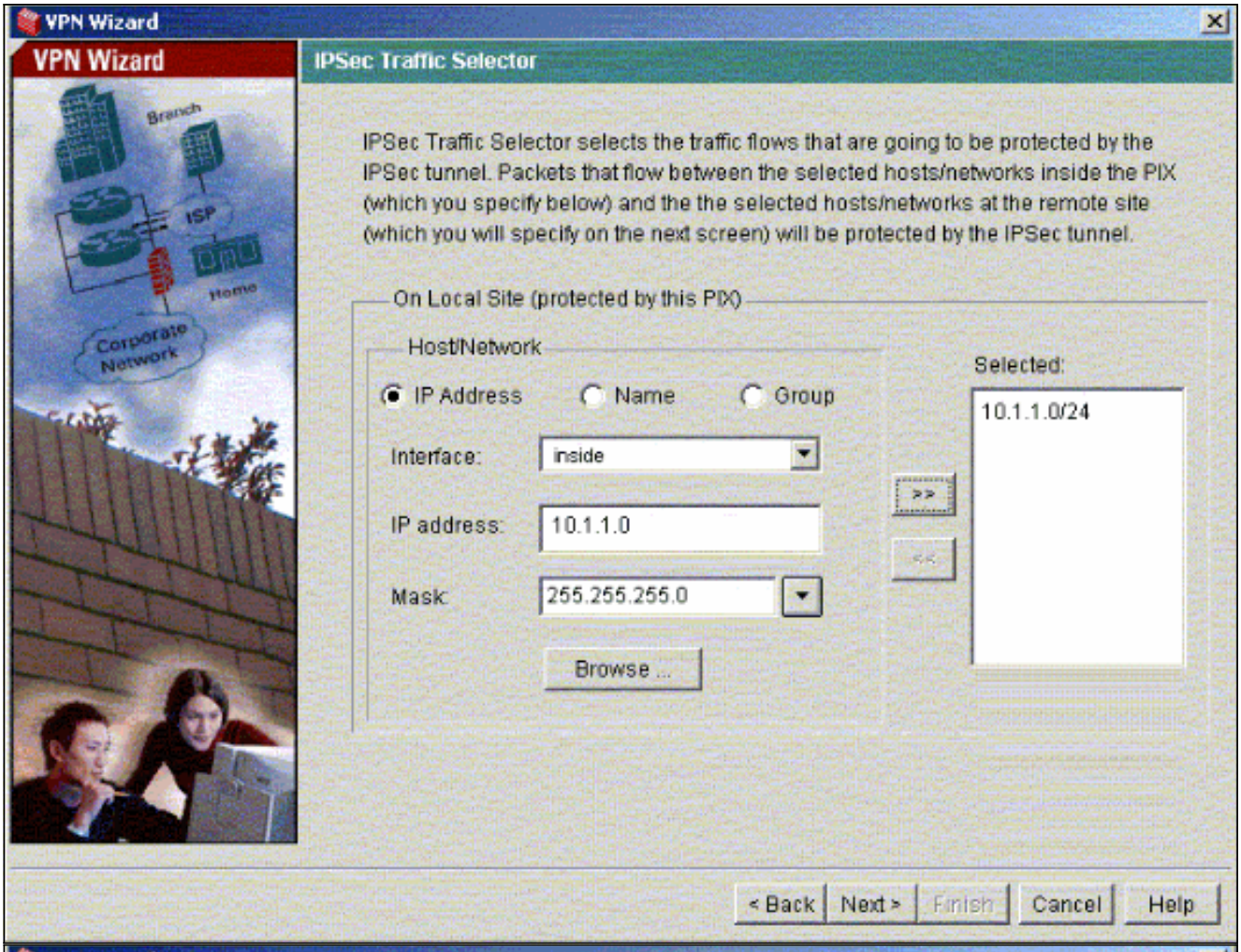
4. Typ de parameters voor IKE-beleid die u wilt gebruiken en klik op **Volgende**.

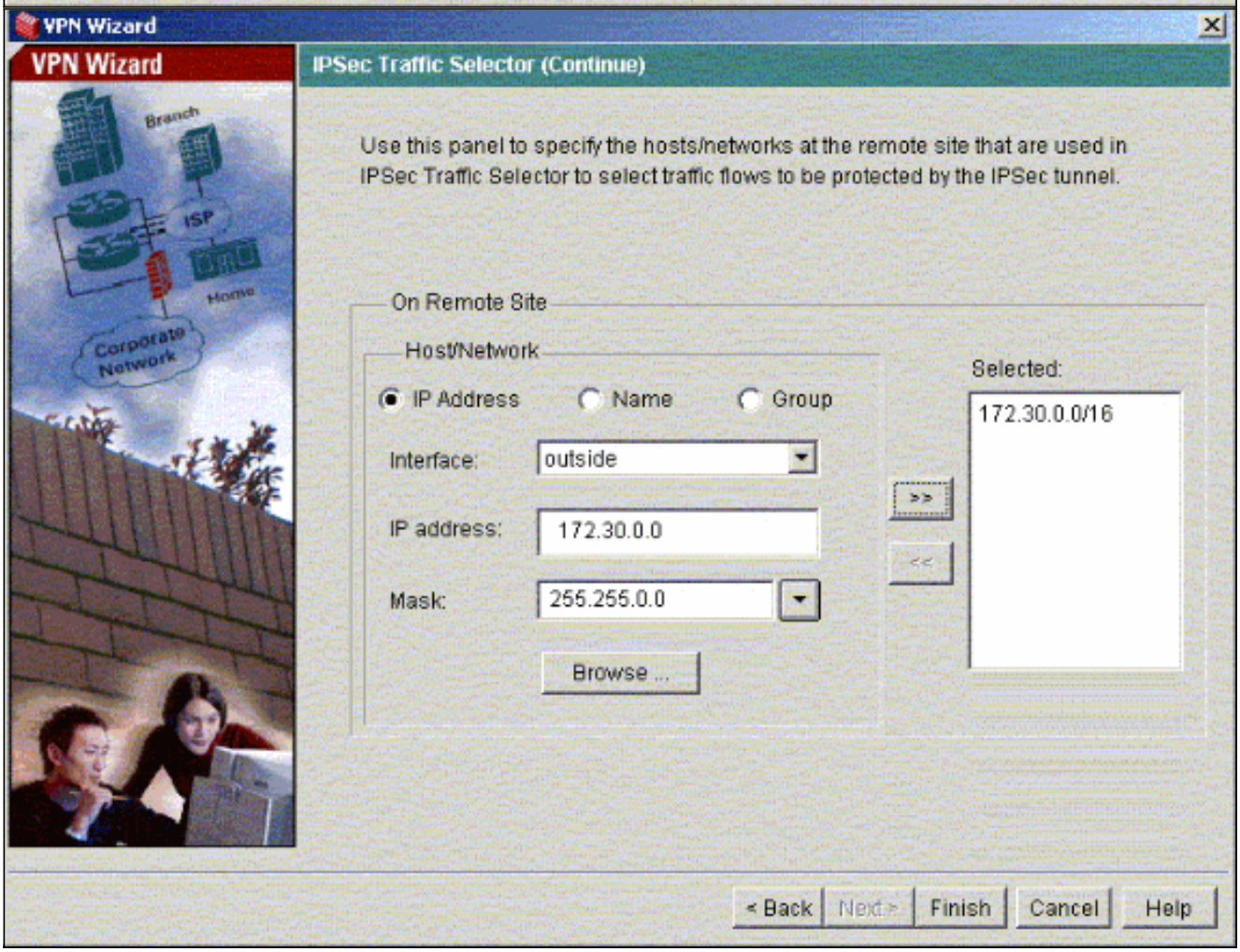


5. Geef de parameters Encryptie en verificatie op voor de verzameling van het formulier en klik op
Volgende.



6. Selecteer het lokale netwerk en de externe netwerken die u wilt beveiligen met IPsec om het interessante verkeer te selecteren dat u moet beveiligen.


VPN Wizard
VPN Wizard
IPSec Traffic Selector
Branch
ISP
Home
Corporate Network
IPSec Traffic Selector selects the traffic flows that are going to be protected by the IPSec tunnel. Packets that flow between the selected hosts/networks inside the PIX (which you specify below) and the the selected hosts/networks at the remote site (which you will specify on the next screen) will be protected by the IPSec tunnel.
On Local Site (protected by this PIX)
Host/Network
IP Address
Name
Group
Interface:
inside
IP address:
10.1.1.0
Mask:
255.255.255.0
Browse ...
Selected:
10.1.1.0/24
>>
<<
< Back
Next >
Finish
Cancel
Help

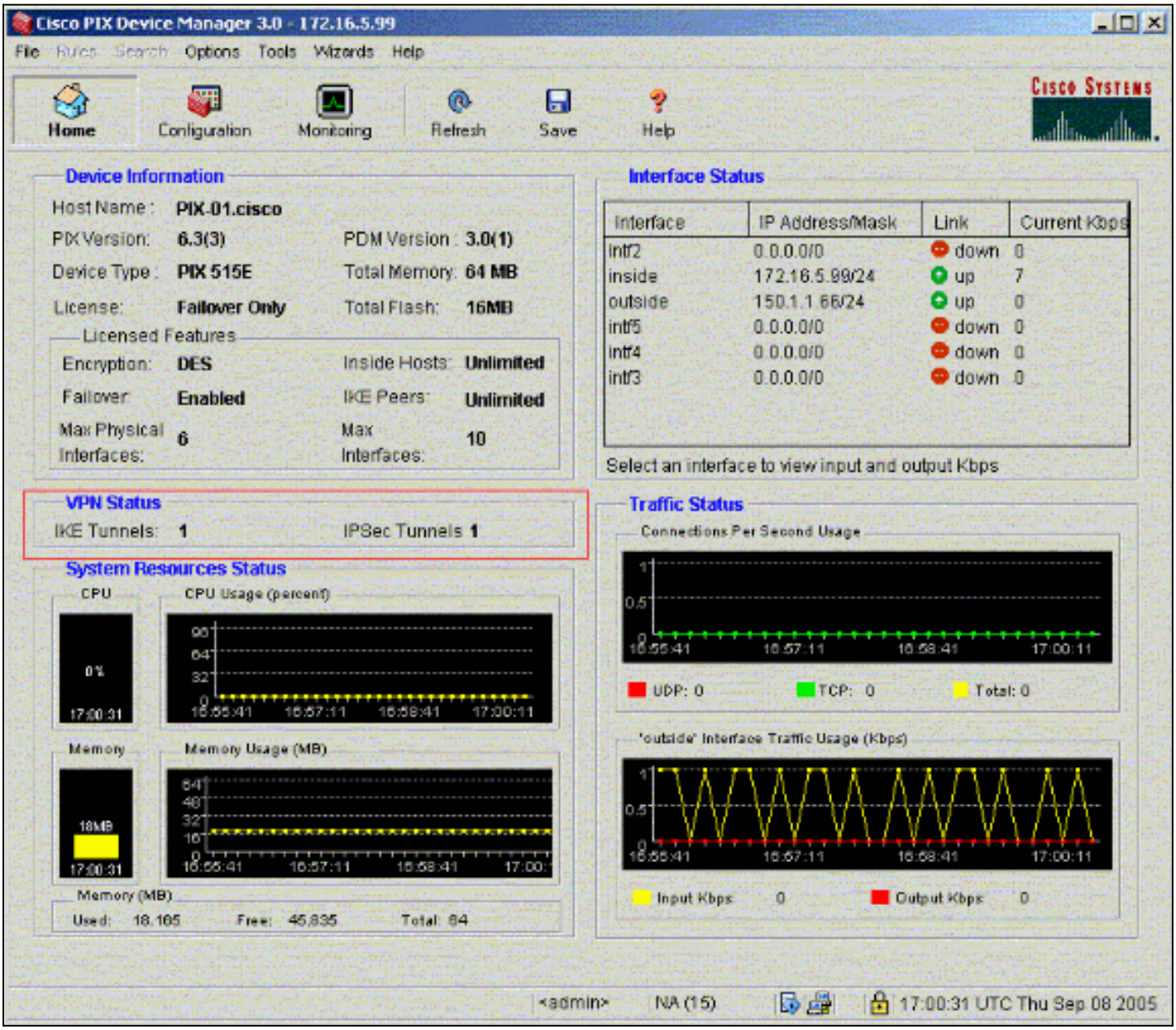

VPN Wizard
VPN Wizard
IPSec Traffic Selector (Continue)
Branch
ISP
Home
Corporate Network
Use this panel to specify the hosts/networks at the remote site that are used in IPSec Traffic Selector to select traffic flows to be protected by the IPSec tunnel.
On Remote Site
Host/Network
IP Address
Name
Group
Interface:
outside
IP address:
172.30.0.0
Mask:
255.255.0.0
Browse ...
Selected:
172.30.0.0/16
>>
<<
< Back
Next >
Finish
Cancel
Help

Verifiëren

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

Om dit te verifiëren, sluit de R1 seriële interface waarvoor de tunnel tussen PIX-01 en PIX-02 via R2 wordt ingesteld, wanneer het interessante verkeer bestaat.

Bekijk de **VPN-status** onder **Begin** 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.

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

Raadpleeg Cisco PIX-apparaatbeheer 3.0 voor meer informatie over de configuratie van de PIX-firewall met PDM.

Problemen oplossen

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

Gerelateerde informatie

- Een simpele PIX-to-PIX VPN-tuner configureren met IPsec
- Cisco PIX-firewallsoftware
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems