Creación de túneles redundantes entre firewalls mediante PDM

Contenido

Introducción

Este documento describe el procedimiento que utiliza para configurar túneles entre dos firewalls PIX mediante Cisco PIX Device Manager (PDM). Los firewalls PIX se colocan en dos sitios diferentes. En caso de que no se alcance la trayectoria principal, es deseable iniciar el túnel a través de un link redundante. 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 específicos para este documento.

Componentes Utilizados

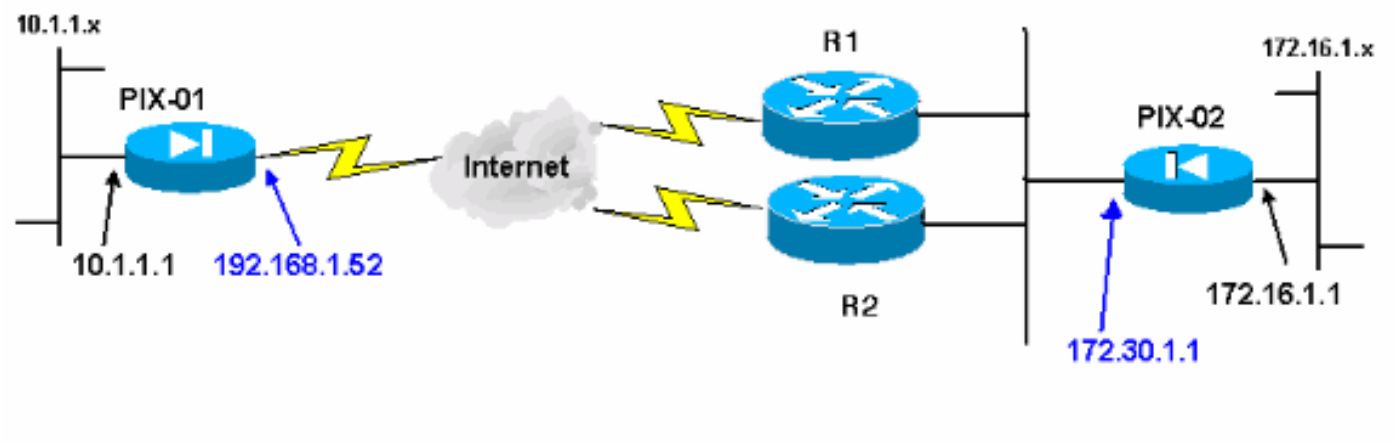
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Firewalls Cisco Secure PIX 515E con 6.x y PDM versión 3.0

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).

Un túnel IPSec es iniciado por un tráfico interesado. Se considera que el tráfico es interesante cuando se transmite entre los pares IPSec.

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).

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.

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.

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.

Configuración

Este procedimiento le guía a través de la configuración de uno de los firewalls PIX para activar el túnel cuando existe tráfico interesante. Esta configuración también le ayuda a establecer el túnel a través del link de respaldo a través del router 2 (R2), cuando no hay conectividad entre el PIX-01

y el PIX-02 a través del router 1 (R1). Este documento muestra la configuración de PIX-01 usando PDM. Puede configurar PIX-02 en líneas similares.

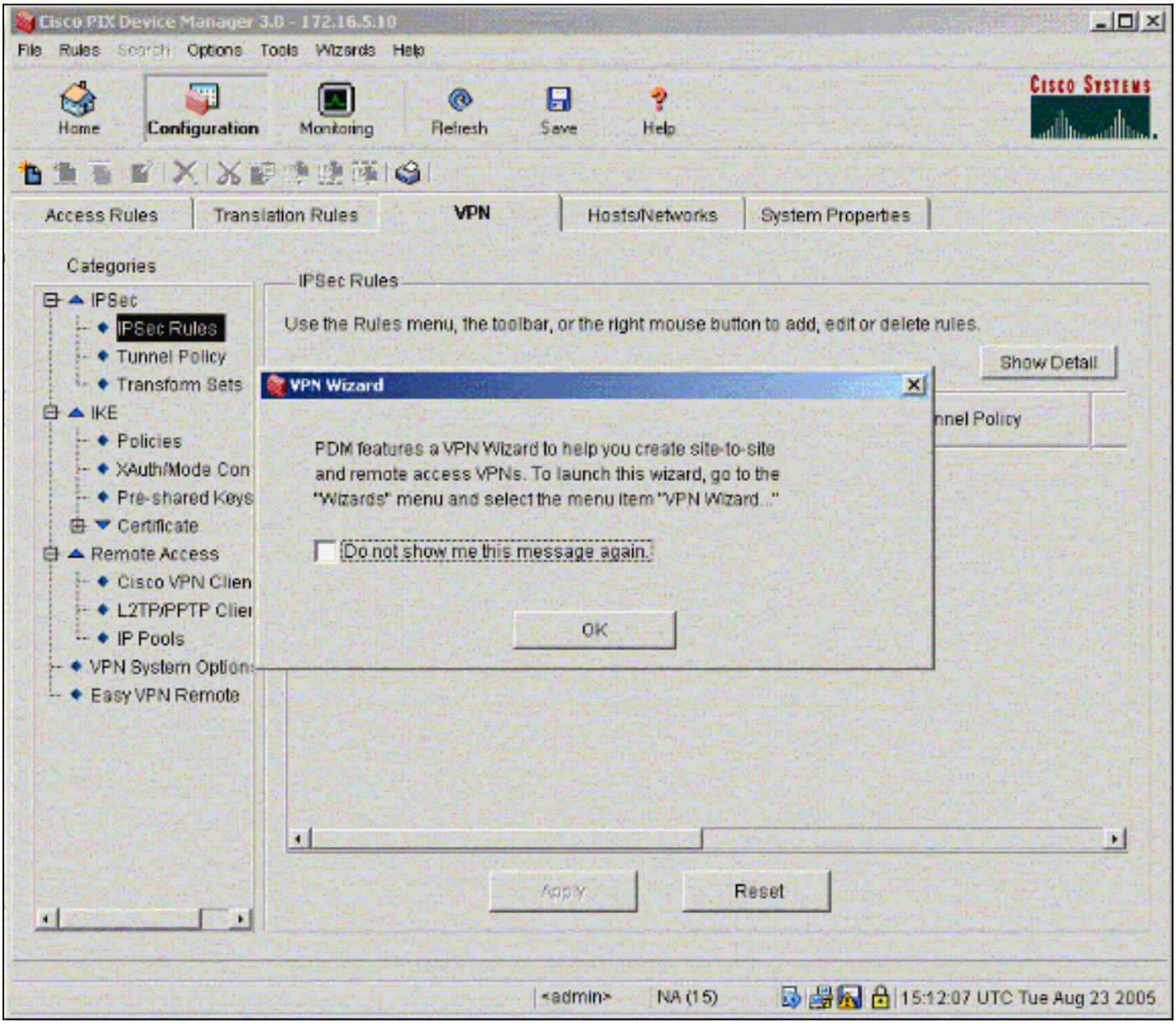
Este documento asume que ya ha configurado el ruteo.

Para que sólo un link esté activo a la vez, haga que R2 anuncie una métrica peor para la red 192.168.1.0 así como para la red 172.30.0.0. Por ejemplo, si utiliza RIP para el ruteo, R2 tiene esta configuración aparte de otros anuncios de red:

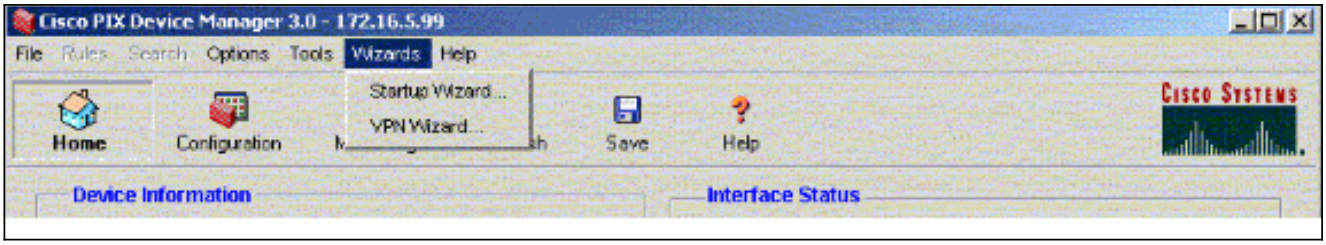
```
R2(config)#router rip
R2(config-router)#offset-list 1 out 2 s1
R2(config-router)#offset-list 2 out 2 e0
R2(config-router)#exit
R2(config)#access-list 1 permit 172.30.0.0 0.0.255.255
R2(config)#access-list 2 permit 192.168.1.0 0.0.0.255
```

Procedimiento de Configuración

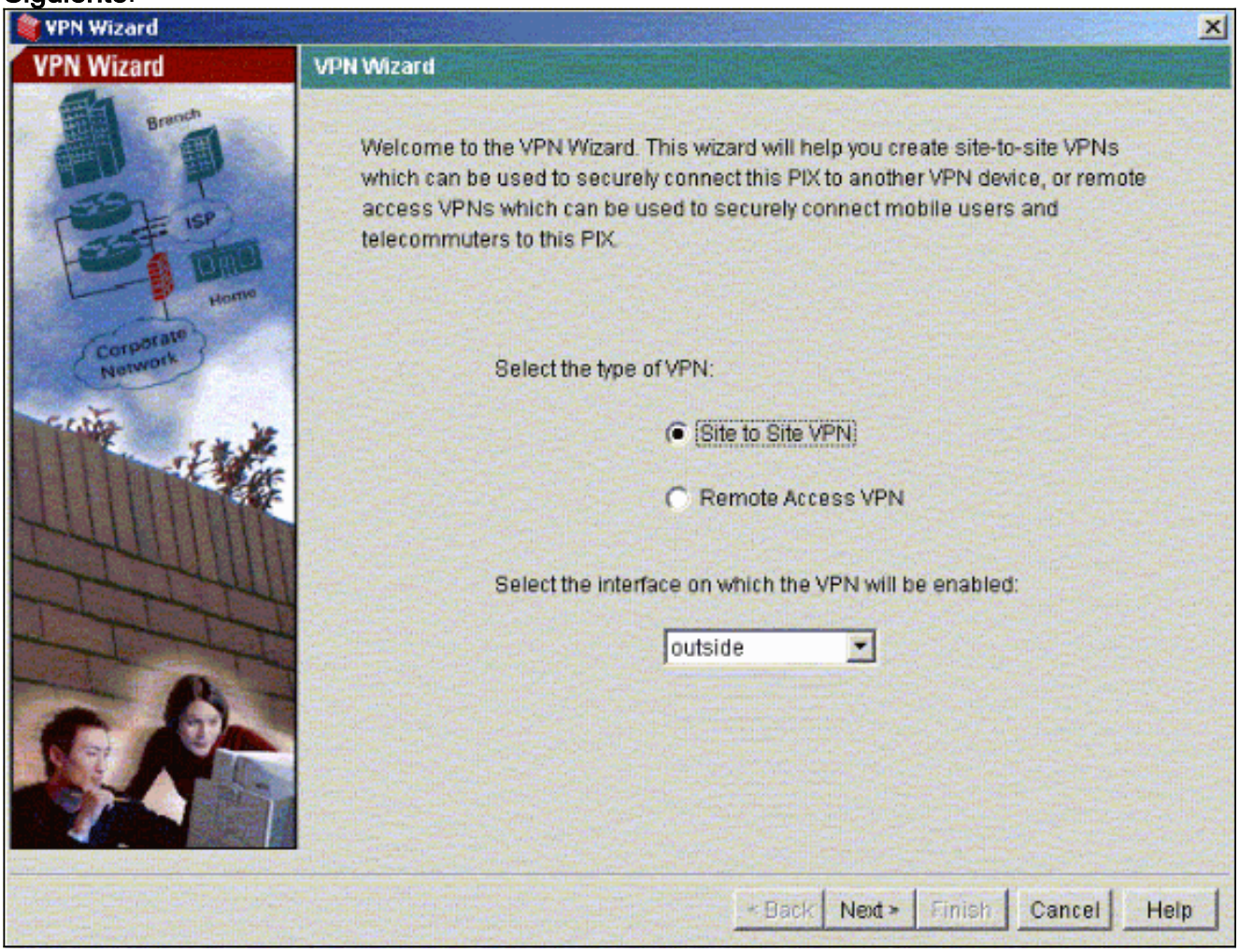
Cuando escribe **https://<Inside_IP_Address_on_PIX>** para iniciar PDM y hacer clic en la ficha VPN por primera vez, se muestra información sobre el asistente automático de VPN.



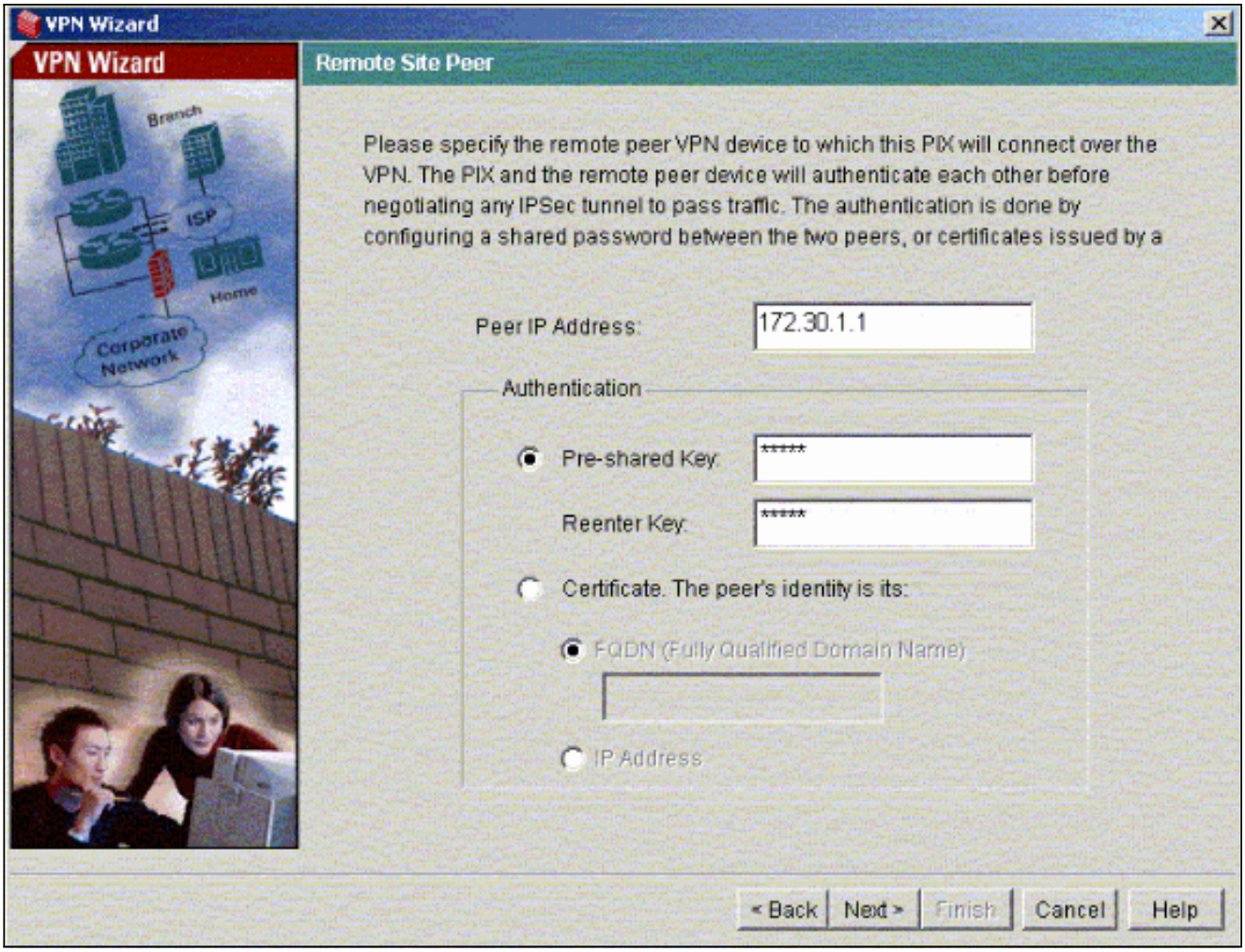
1. Seleccione **Asistentes > Asistente VPN**.



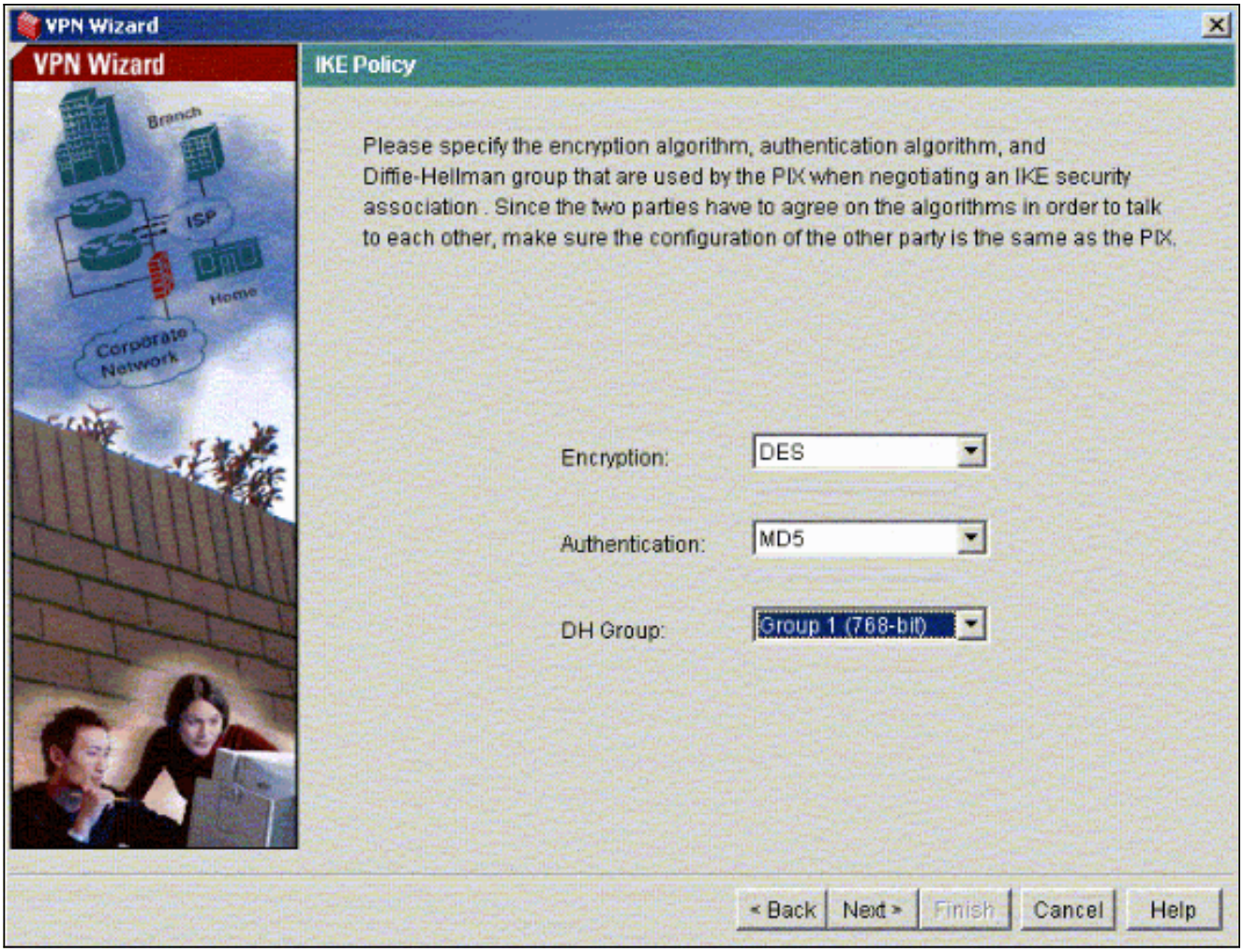
2. Se inicia el asistente de VPN y le solicita el tipo de VPN que desea configurar. Elija **VPN de sitio a sitio**, seleccione la **interfaz externa** como la interfaz en la que se habilitará la VPN y haga clic en **Siguiente**.



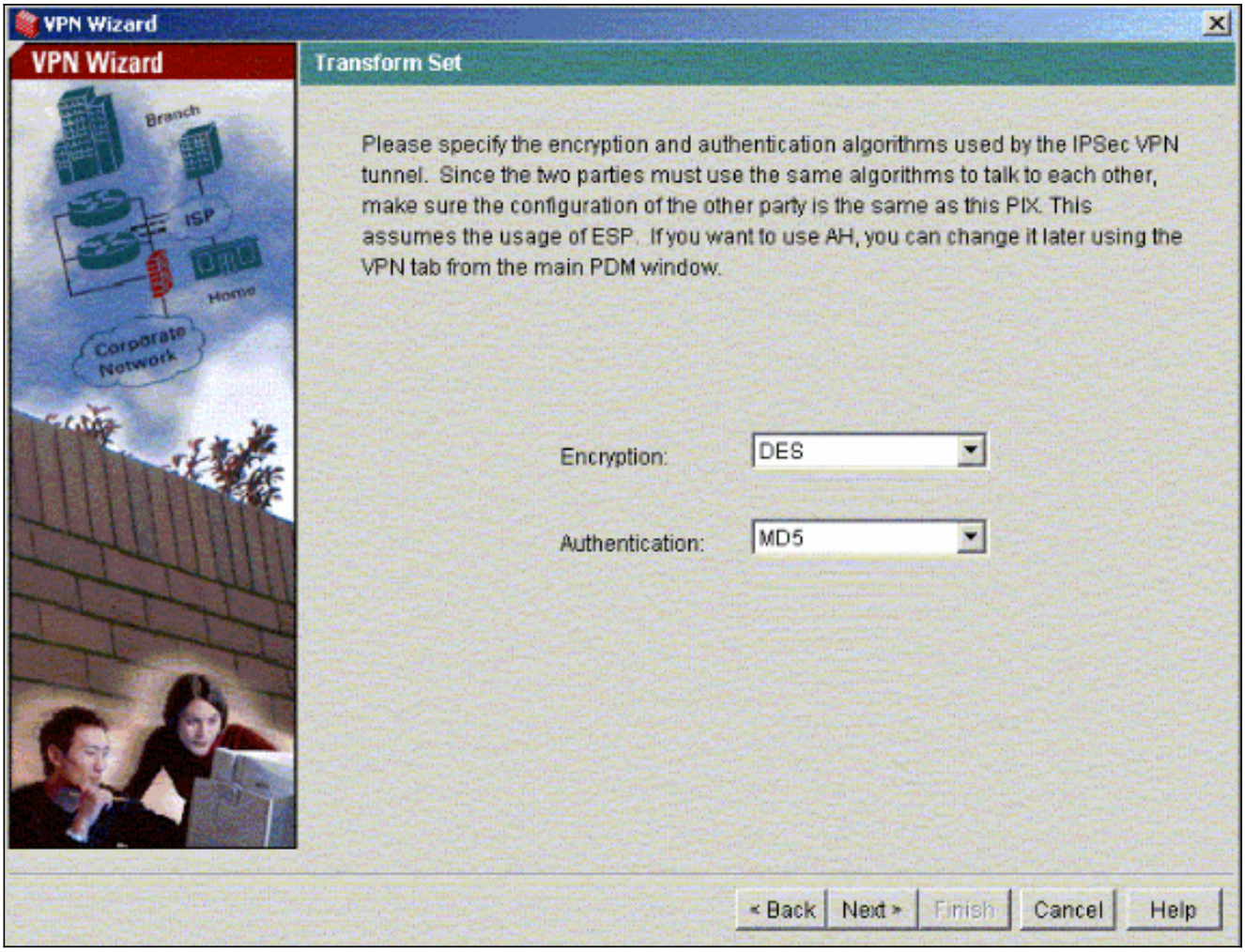
3. Introduzca la dirección IP del par, donde debe finalizar el túnel IPsec. En este ejemplo, el túnel termina en la interfaz exterior de PIX-02. Haga clic en Next (Siguiente).



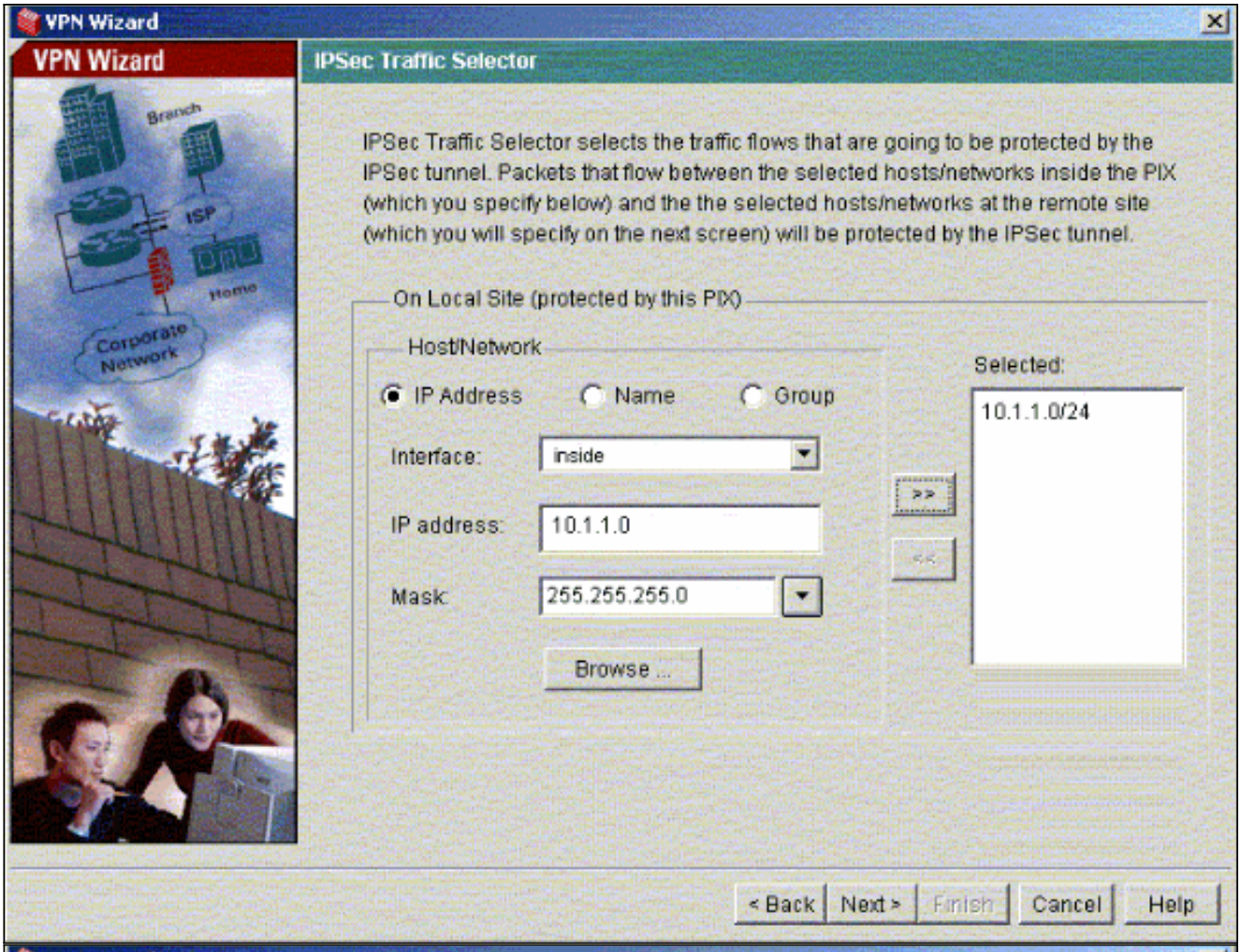
4. Ingrese los parámetros de política IKE que elija utilizar y haga clic en **Siguiente**.

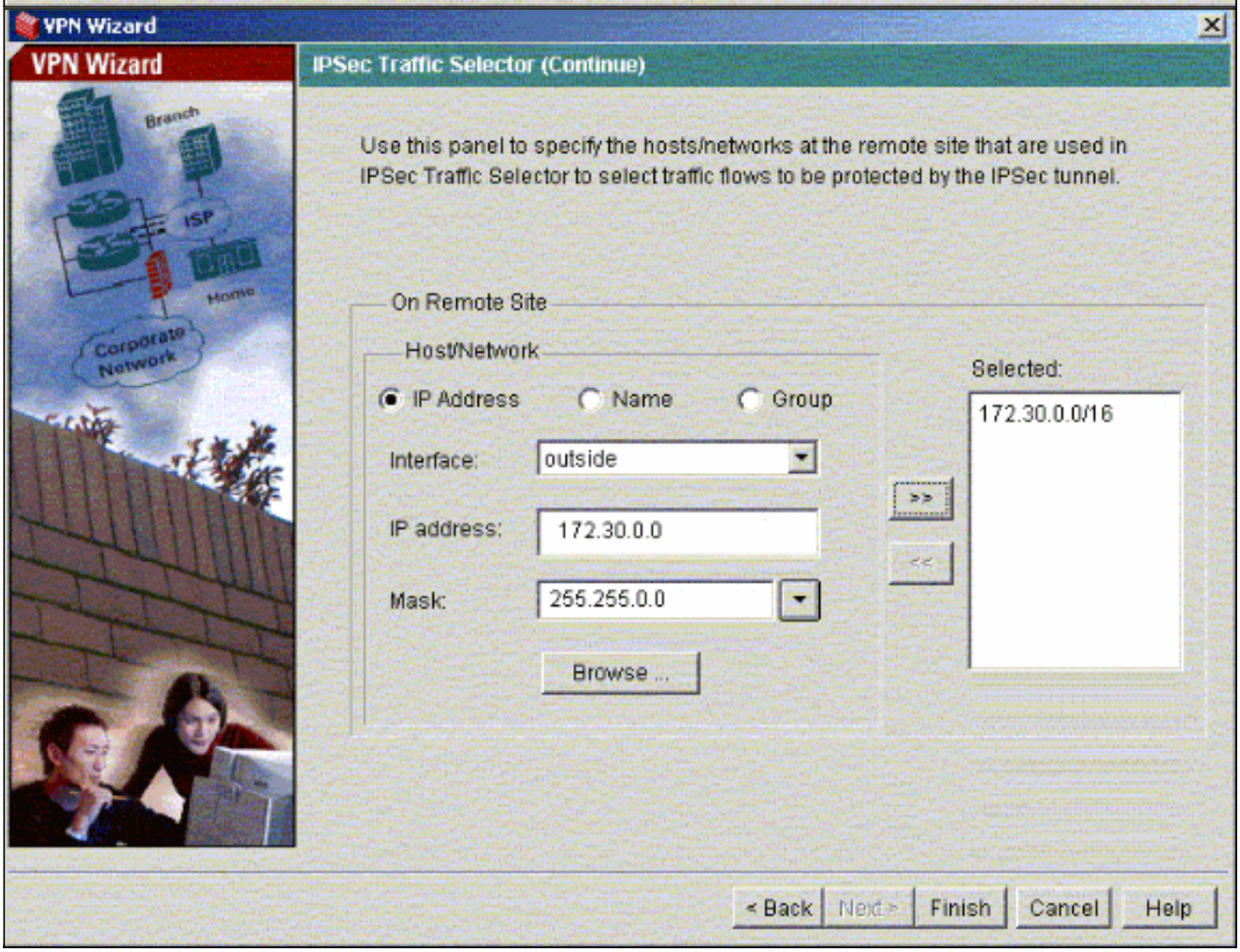


5. Proporcione los parámetros de cifrado y autenticación para el conjunto de transformación y haga clic en
Siguiente.



6. Seleccione la red local y las redes remotas que necesita proteger usando IPSec para seleccionar el tráfico interesante que necesita proteger.


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

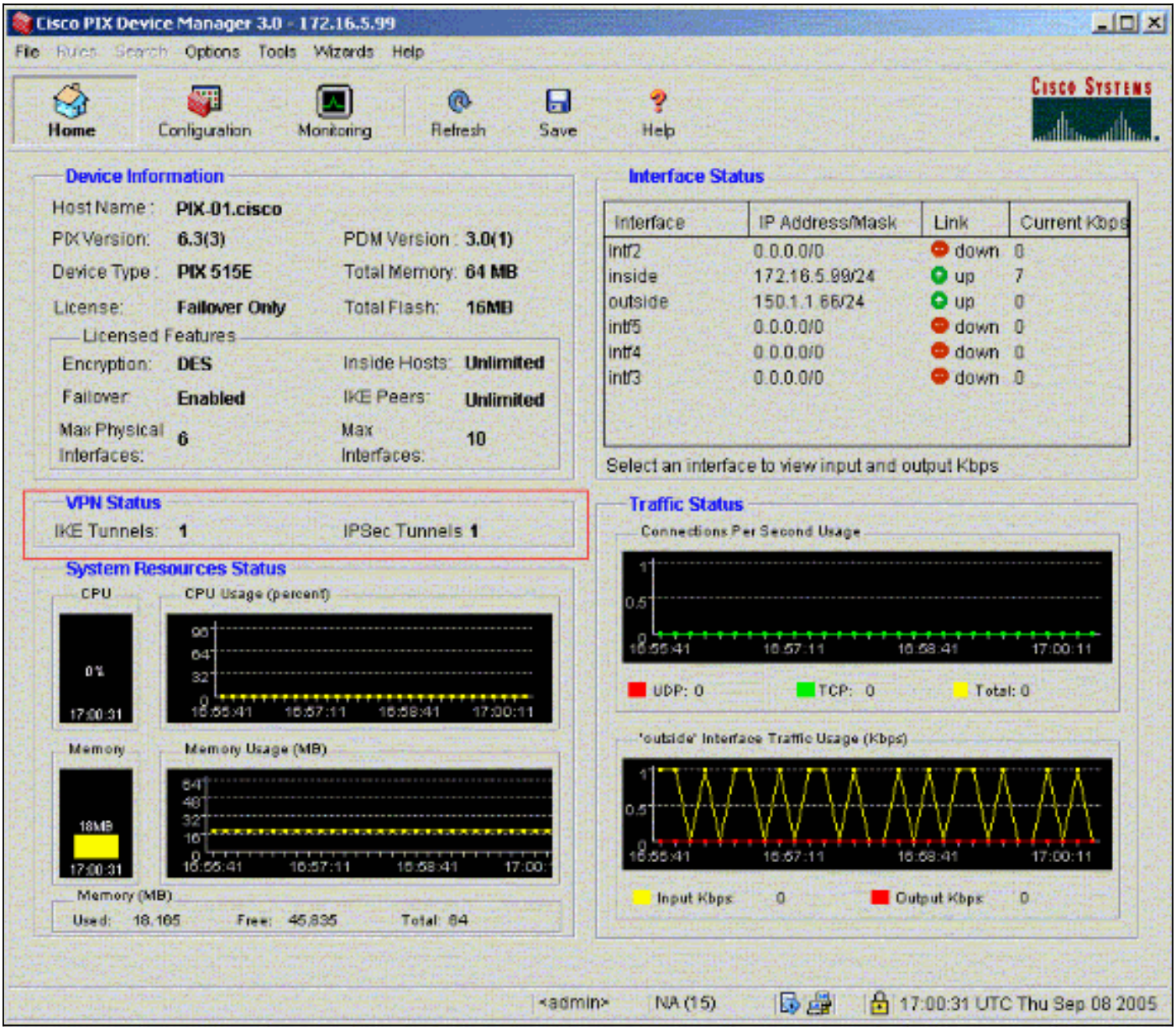

VPN Wizard
VPN Wizard
IPSec Traffic Selector (Continue)
Branch
ISP
Home
Corporate Network
Use this panel to specify the hosts/networks at the remote site that are used in IPSec Traffic Selector to select traffic flows to be protected by the IPSec tunnel.
On Remote Site
Host/Network
IP Address
Name
Group
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

Verificación

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

Para verificar esto, apague la interfaz serial R1 para la cual se establece el túnel entre PIX-01 y PIX-02 a través de R2 cuando existe el tráfico interesante.

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.

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.

Refiérase a Cisco PIX Device Manager 3.0 para obtener más información sobre la configuración del PIX Firewall con PDM.

Troubleshoot

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

Información Relacionada

- Configuración de un único túnel VPN PIX a PIX mediante IPSec
- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems