Criação de túnel redundante entre firewalls usando PDM

Contents

Introduction

Este documento descreve o procedimento usado para configurar túneis entre dois firewalls PIX usando o Cisco PIX Device Manager (PDM). Os PIX Firewalls são colocados em dois locais diferentes. Em caso de falha ao alcançar o caminho principal, é desejável lançar o túnel através de um link redundante. 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 existem requisitos específicos para este documento.

Componentes Utilizados

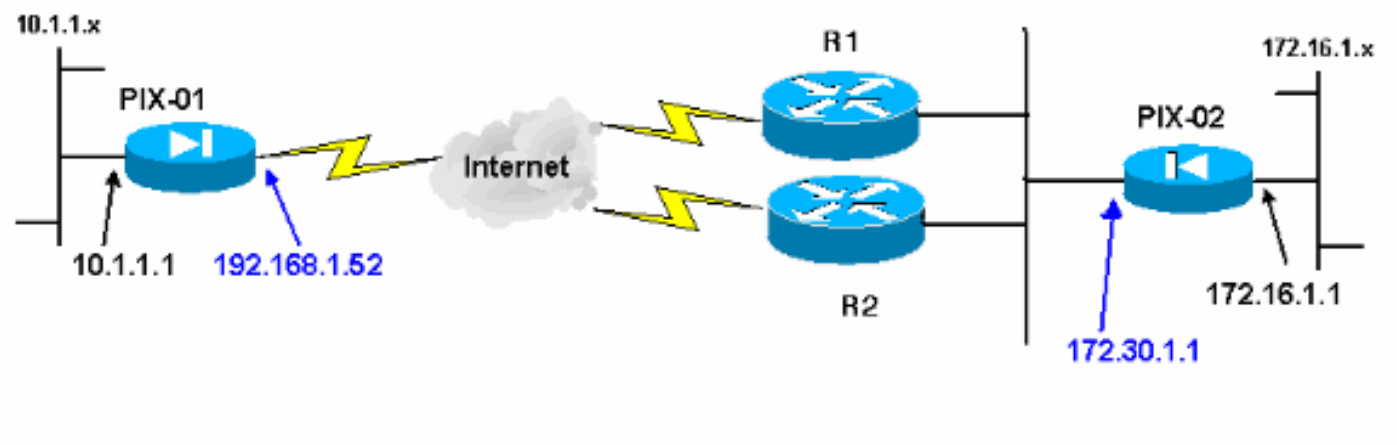
As informações neste documento são baseadas nestas versões de software e hardware:

- Firewalls Cisco Secure PIX 515E com 6.x e PDM versão 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 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).

Um túnel de IPSec é iniciado por um tráfego interessante. O tráfego é considerado interessante quando ele é transmitido entre os peers IPSec.

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).

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.

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.

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.

Configuração

Este procedimento o orienta na configuração de um dos firewalls PIX para disparar o túnel quando houver tráfego interessante. Essa configuração também ajuda a estabelecer o túnel através do link de backup através do roteador 2 (R2), quando não há conectividade entre o PIX-

01 e o PIX-02 através do roteador 1 (R1). Este documento mostra a configuração do PIX-01 usando PDM. Você pode configurar PIX-02 em linhas semelhantes.

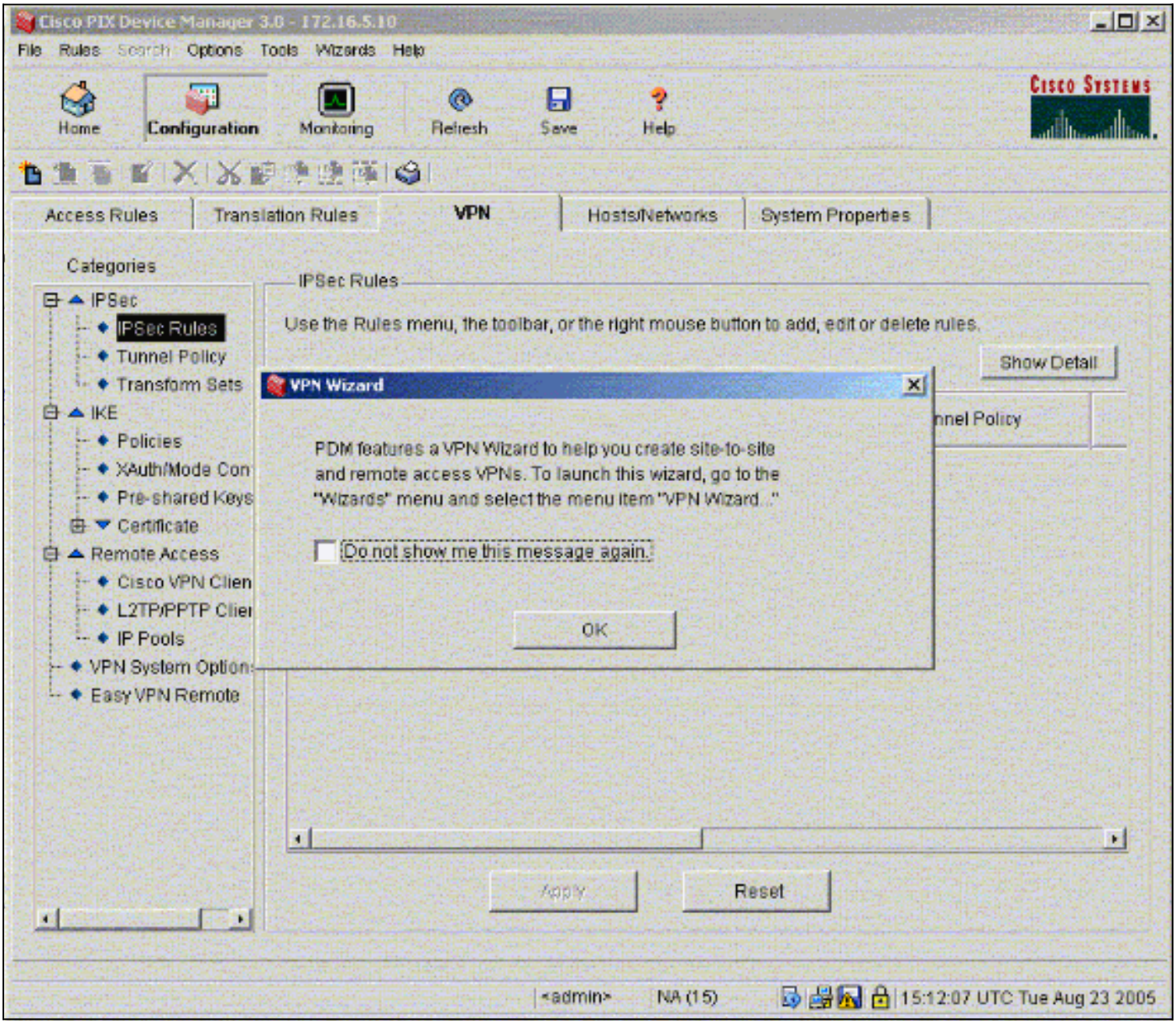
Este documento pressupõe que você já configurou o roteamento.

Para apenas um link estar ativo por vez, faça com que R2 anuncie uma métrica pior para a rede 192.168.1.0 e para a rede 172.30.0.0. Por exemplo, se você usa o RIP para o roteamento, o R2 tem essa configuração além de outros anúncios de rede:

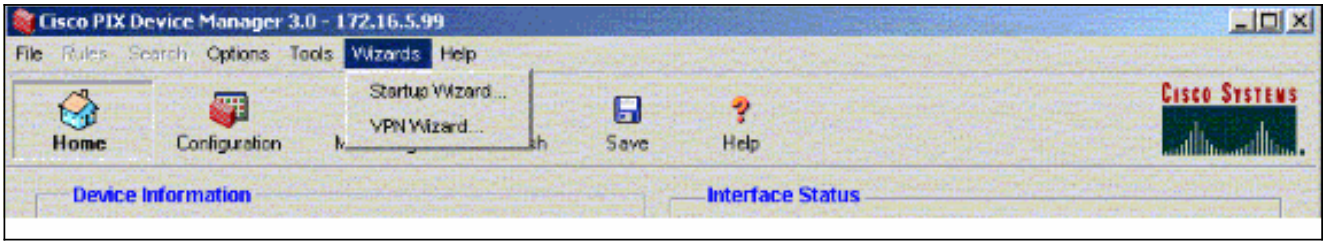
```
R2(config)#router rip
R2(config-router)#offset-list 1 out 2 s1
R2(config-router)#offset-list 2 out 2 e0
R2(config-router)#exit
R2(config)#access-list 1 permit 172.30.0.0 0.0.255.255
R2(config)#access-list 2 permit 192.168.1.0 0.0.0.255
```

Procedimento de configuração

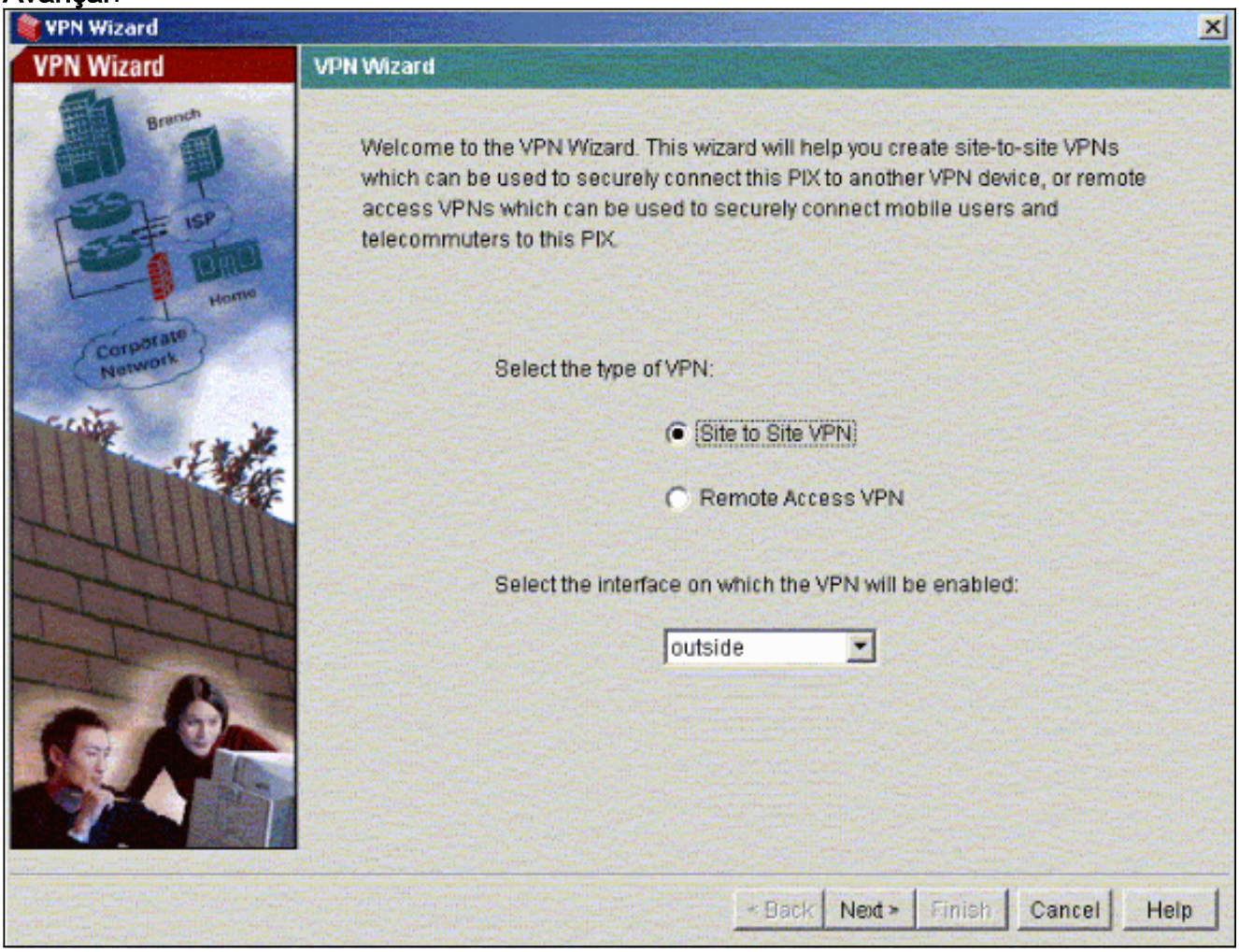
Quando você digita **https://<Inside_IP_Address_on_PIX>** para iniciar o PDM e clicar na guia VPN pela primeira vez, as informações sobre o Assistente automático de VPN são exibidas.



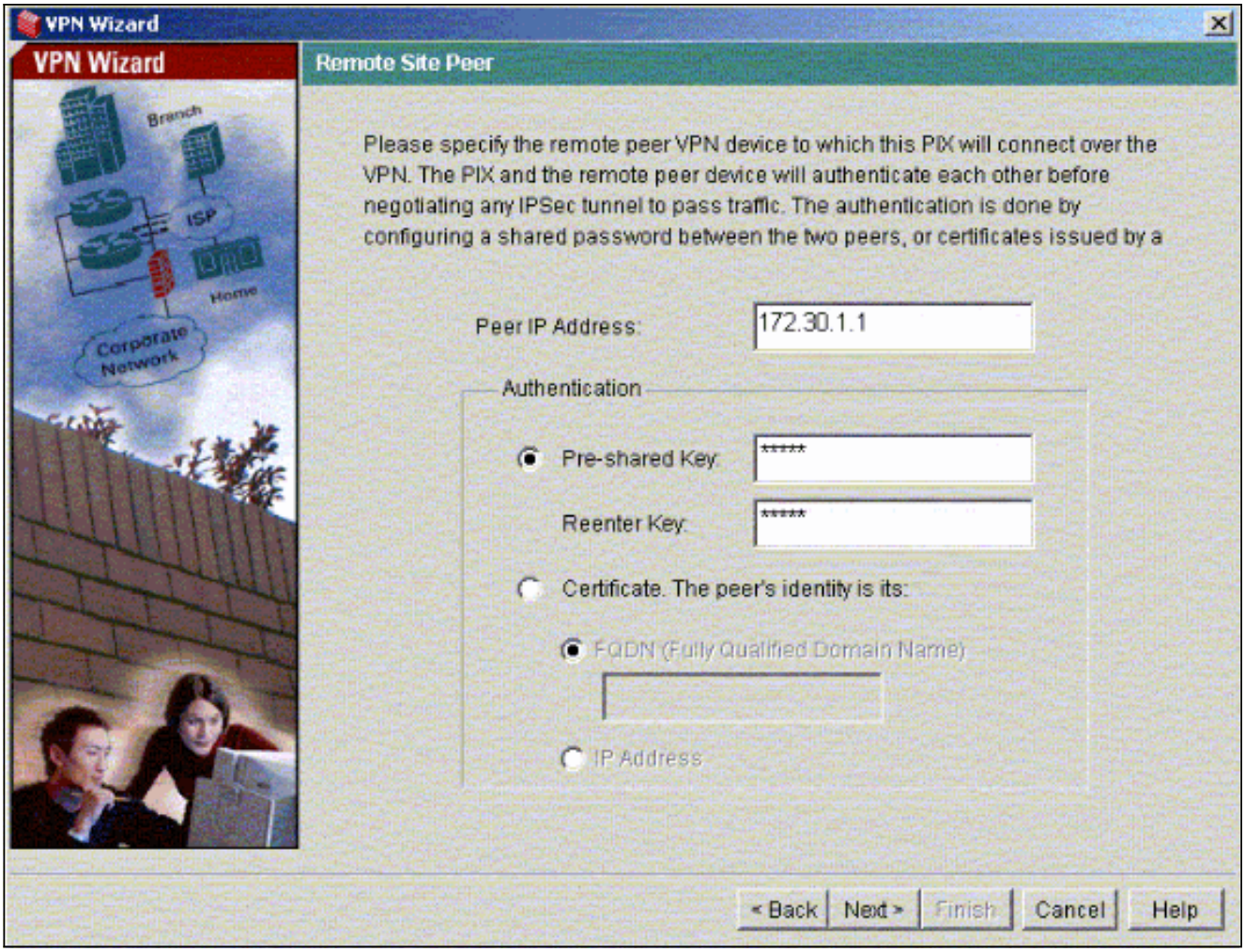
1. Selecione **Assistentes > Assistente de VPN**.



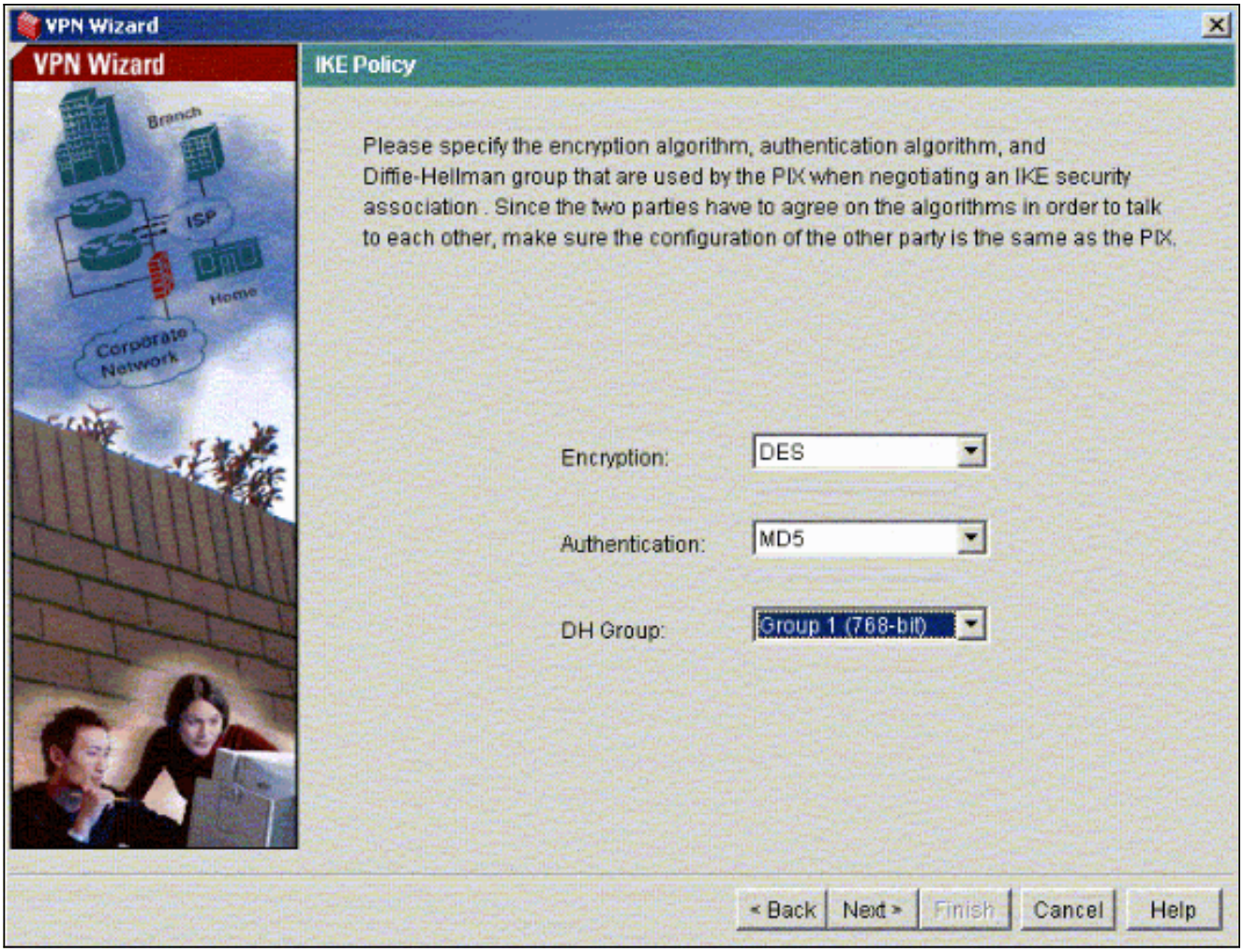
2. O assistente VPN é iniciado e solicita o tipo de VPN que você deseja configurar. Escolha **VPN site a site**, selecione a interface **externa** como a interface na qual a VPN será habilitada e clique em **Avançar**.



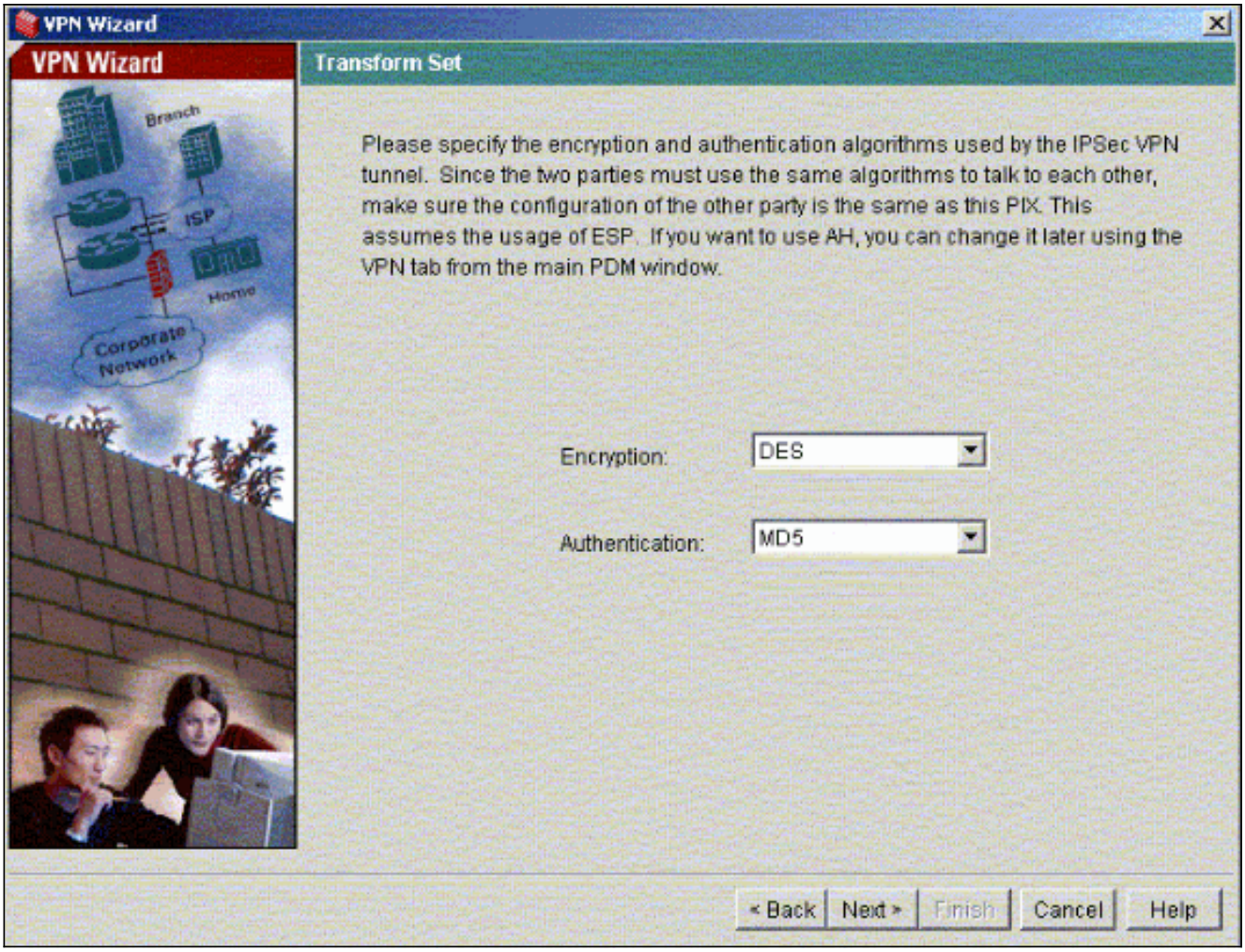
3. Digite o endereço IP do peer, onde o túnel IPsec deve terminar. Neste exemplo, o túnel termina na interface externa do PIX-02. Clique em **Next**.



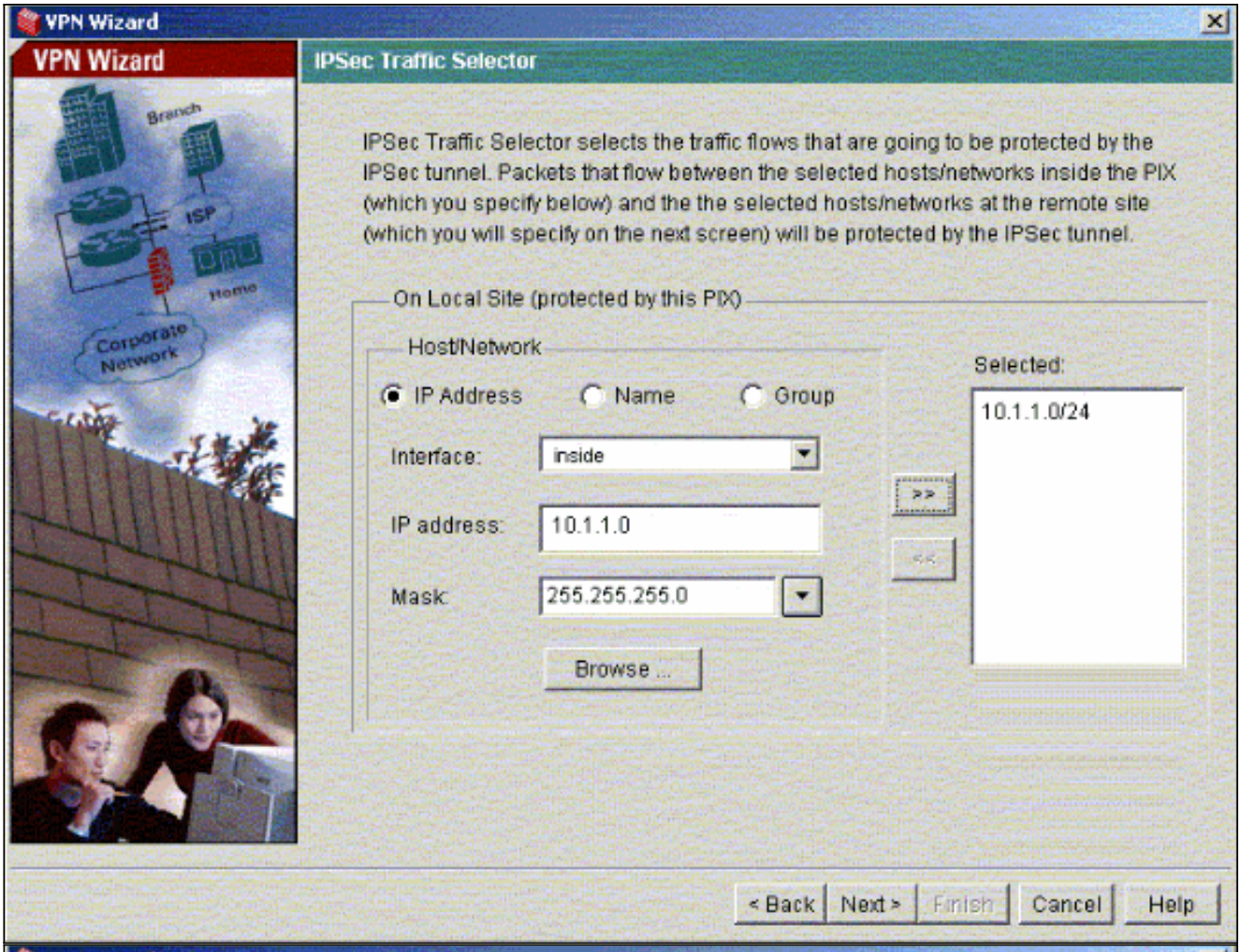
4. Insira os parâmetros da política IKE que você escolhe para usar e clique em **Avançar**.

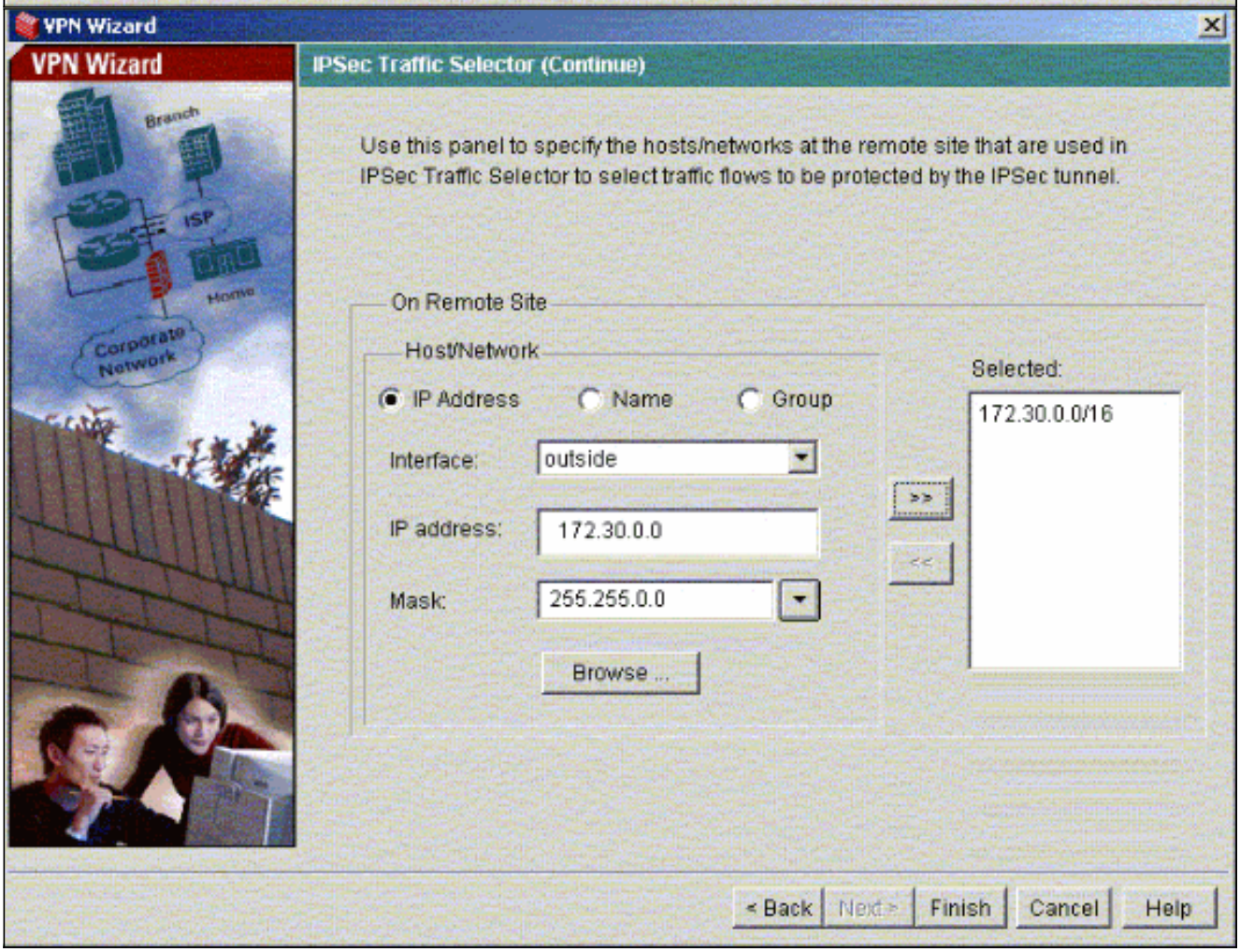


5. Forneça os parâmetros de criptografia e autenticação para o conjunto de transformações e clique em
Avançar.



6. Selecione a rede local e as redes remotas que você precisa proteger usando o IPsec para selecionar o tráfego interessante que você precisa 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

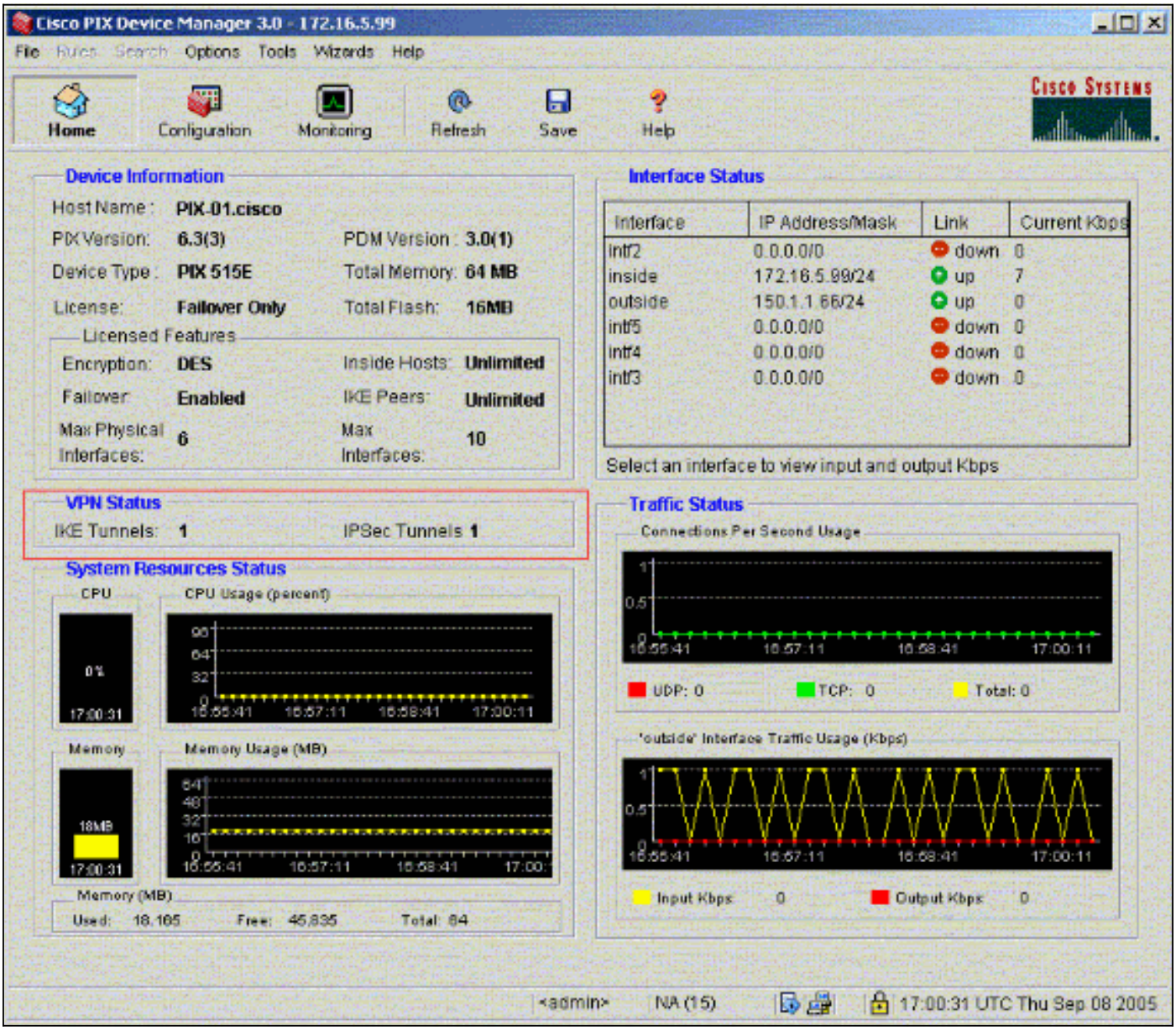

VPN Wizard
VPN Wizard
IPSec Traffic Selector (Continue)
Branch
ISP
Home
Corporate Network
Use this panel to specify the hosts/networks at the remote site that are used in IPSec Traffic Selector to select traffic flows to be protected by the IPSec tunnel.
On Remote Site
Host/Network
IP Address
Name
Group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

Verificar

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

Para verificar isso, desligue a interface serial R1 para a qual o túnel está estabelecido entre PIX-01 e PIX-02 via R2 quando o tráfego interessante existe.

Visualize o **Status da VPN** em **Home** no PDM (realçado 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.

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.

Consulte o Cisco PIX Device Manager 3.0 para obter mais informações sobre a configuração do PIX Firewall usando PDM.

Troubleshoot

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

Informações Relacionadas

- Configurando um túnel PIX para PIX VPN simples usando IPSec
- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems