PDM を使用したファイアウォール間の冗長トンネルの作成

内容

概要

このドキュメントでは、Cisco PIX Device Manager（PDM）を使用して、2 つの PIX Firewall 間にトンネルを設定するために使用する手順について説明します。PIX Firewall は、2 つの異なるサイトに配置されます。プライマリ パスに到達できない場合は、冗長リンクを経由するトンネルを開始することを推奨します。IPSec とは、IPSec ピア間でデータの機密性、データの完全性、およびデータの発信元の認証を提供するオープン スタンダードの組み合わせです。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

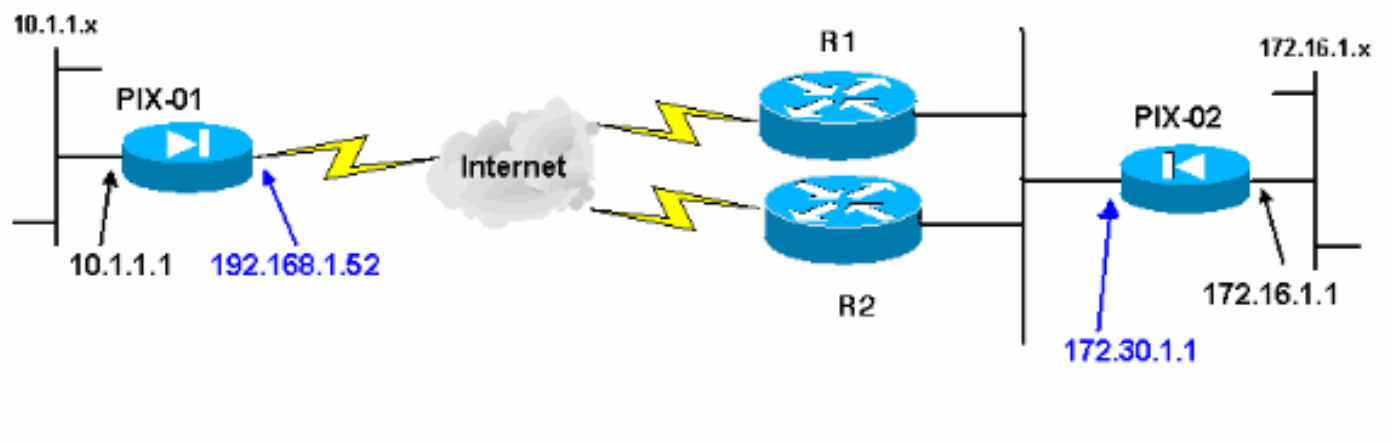
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 6.xおよびPDMバージョン3.0が稼働するCisco Secure PIX 515E Firewall

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

IPsecネゴシエーションは5つのステップに分けられ、2つのInternet Key Exchange（IKE；インターネット鍵交換）フェーズが含まれます。

対象トラフィックによって IPsec トンネルが開始されます。IPsec ピアの間を転送されるトラフィックは、対象トラフィックとみなされます。

IKE フェーズ 1 では、IPsec ピア同士が、IKE セキュリティ アソシエーション（SA）ポリシーについてネゴシエートします。ピアが認証されると、Internet Security Association and Key Management Protocol（ISAKMP）を使用して安全なトンネルが作成されます。

IKE フェーズ 2 では、IPsec ピア同士が認証済みの安全なトンネルを使用して、IPsec SA トランスフォームをネゴシエートします。共有ポリシーのネゴシエーションによって、IPsec トンネルの確立方法が決まります。

IPsec トンネルが作成され、IPsec トランスフォーム セットに設定された IPsec パラメータに基づいて、IPsec 間でデータが伝送されます。

IPsec SA が削除されるか、そのライフタイムの有効期限が切れると、IPsec トンネルは終了します。

注：ピアで両方のIKEフェーズのSAが一致しない場合、2つのPIX間のIPSecネゴシエーションは失敗します。

コンフィギュレーション

この手順では、対象トラフィックが存在する場合にトンネルをトリガーするPIXファイアウォールの1つの設定について説明します。この設定は、PIX-01とPIX-02の間にルータ1(R1)を経由する

接続がない場合に、ルータ2(R2)を経由するバックアップリンクを介したトンネルの確立にも役立ちます。 このドキュメントでは、PDMを使用したPIX-01の設定について説明します。PIX-02は同様の回線で設定できます。

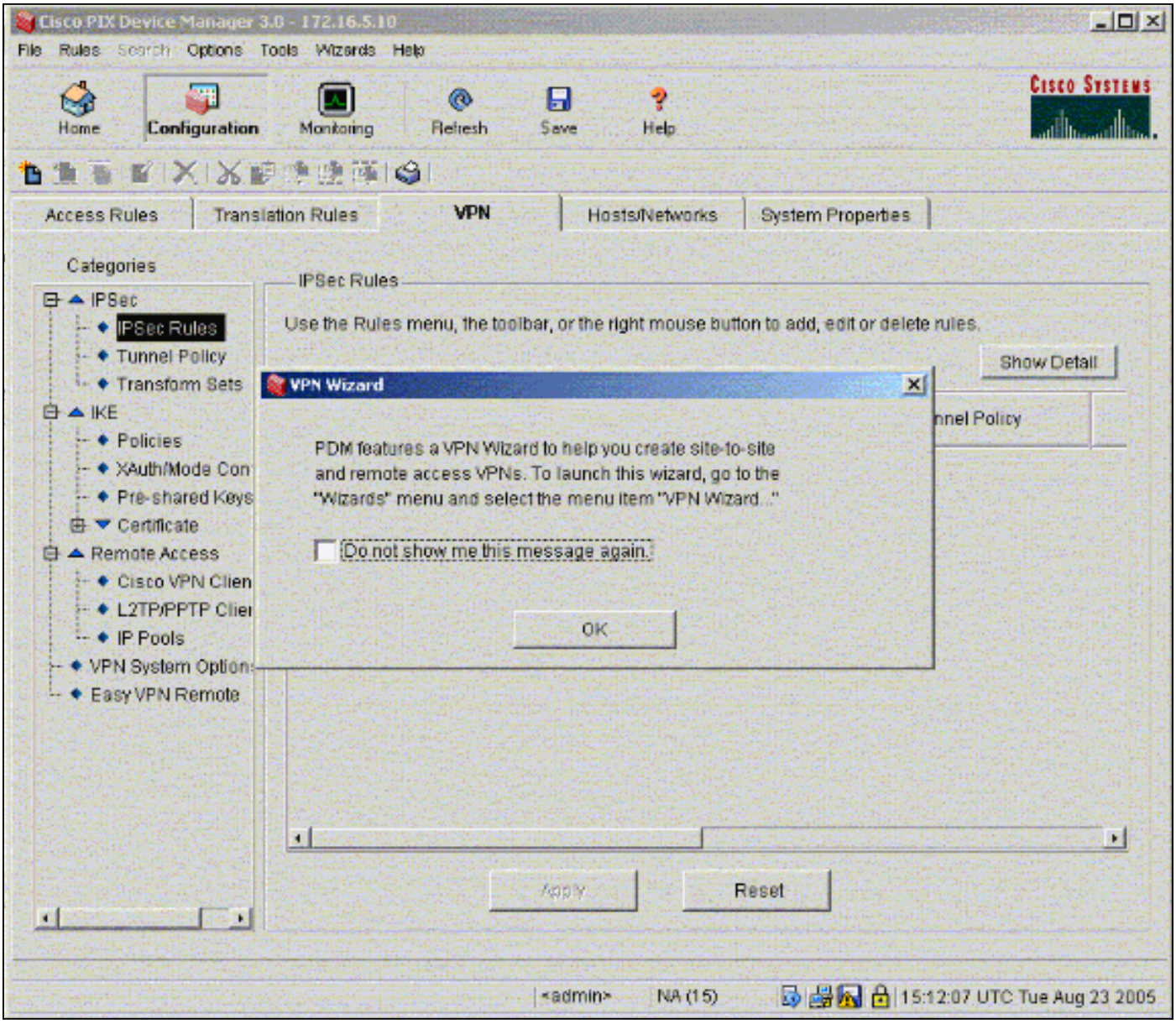
このドキュメントでは、ルーティングがすでに設定されていることを前提としています。

一度に1つのリンクしかアップ状態にならない場合は、R2が192.168.1.0ネットワークおよび172.30.0.0ネットワークに対して、より悪いメトリックをアドバタイズするようにします。たとえば、ルーティングにRIPを使用する場合、R2は他のネットワークアドバタイズメントとは別に次の設定になります。

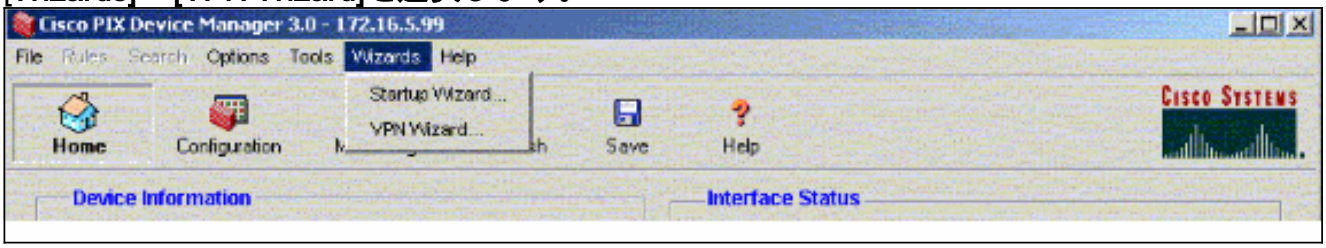
```
R2(config)#router rip
R2(config-router)#offset-list 1 out 2 s1
R2(config-router)#offset-list 2 out 2 e0
R2(config-router)#exit
R2(config)#access-list 1 permit 172.30.0.0 0.0.255.255
R2(config)#access-list 2 permit 192.168.1.0 0.0.0.255
```

構成手順

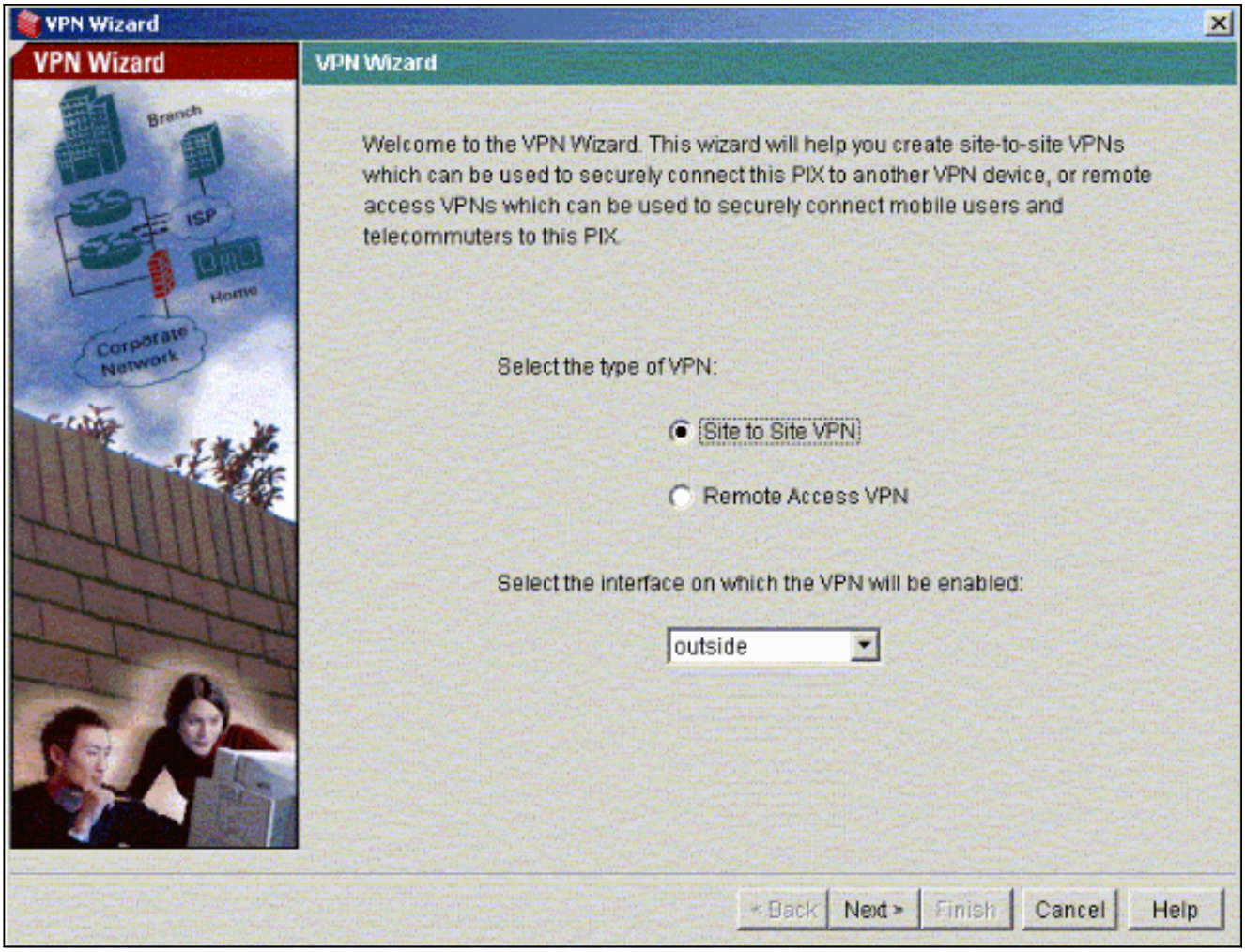
https://<Inside_IP_Address_on_PIX>と入力してPDMを起動し、初めて[VPN]タブをクリックすると、自動VPNウィザードに関する情報が表示されます。



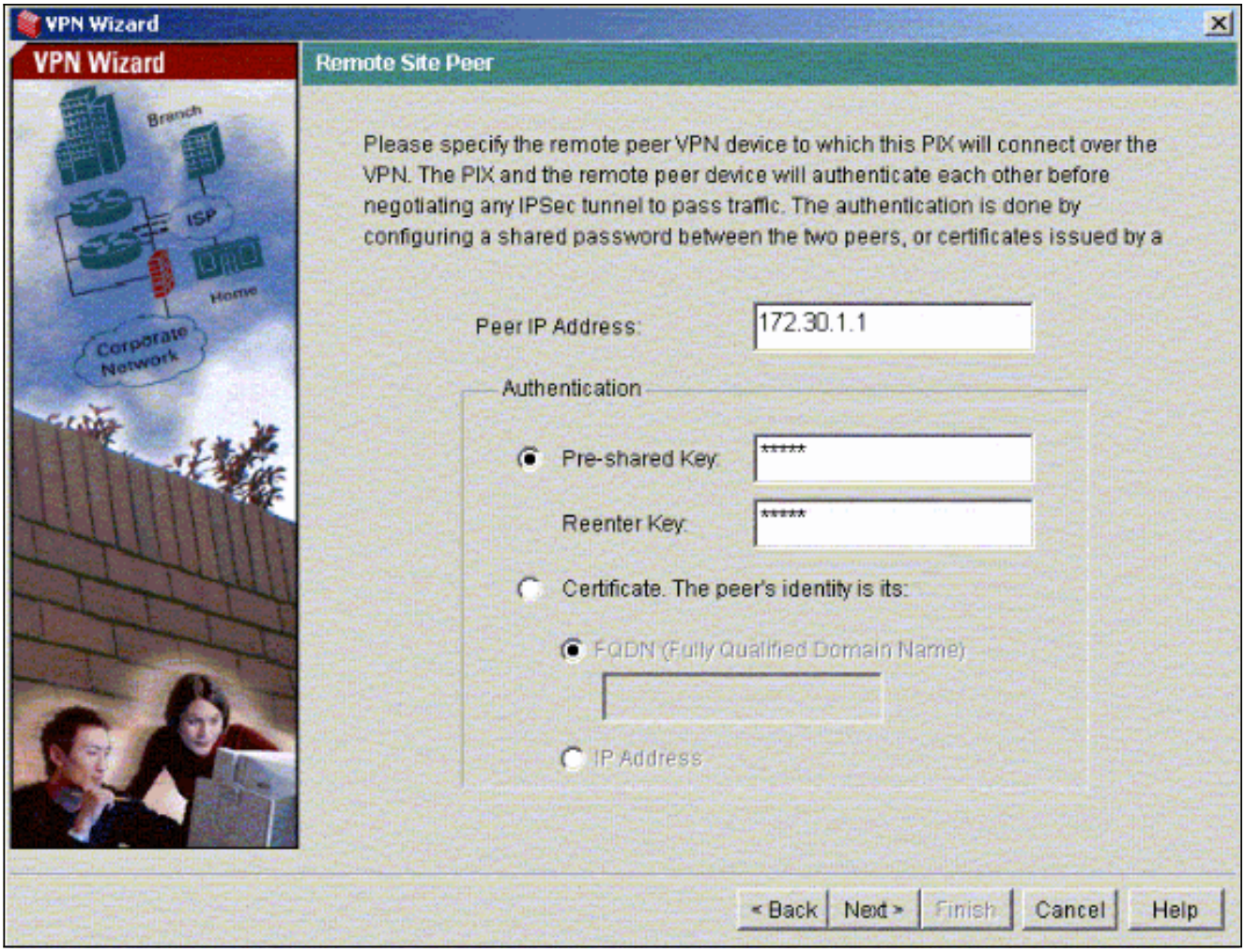
1. **[Wizards] > [VPN Wizard]を選択します。**



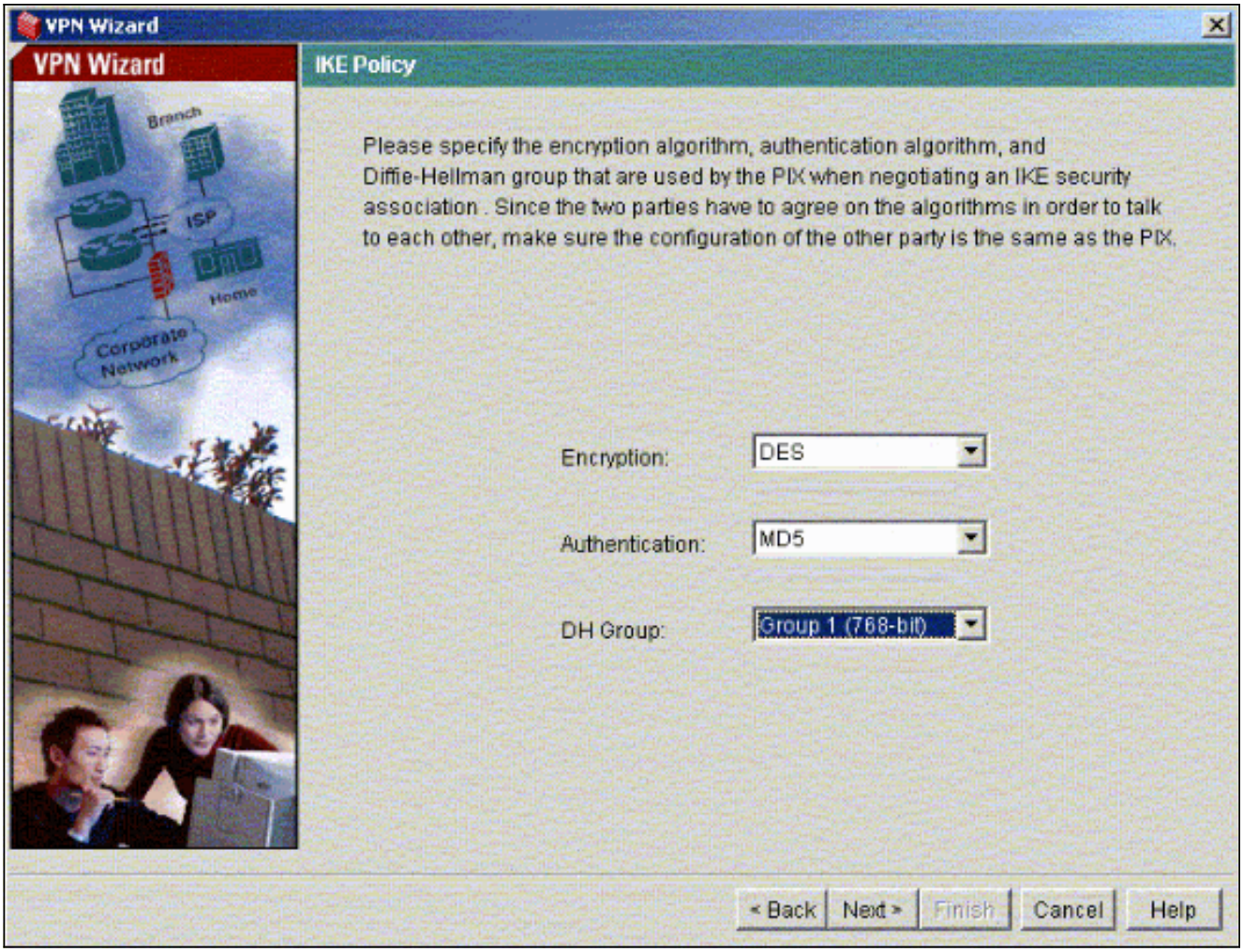
2. VPNウィザードが起動し、設定するVPNのタイプを入力するように求められます。**Site-to-Site VPN**を選択し、VPNを有効にする**インターフェイス**としてoutsideインターフェイスを選択し、**Nextをクリックします。**



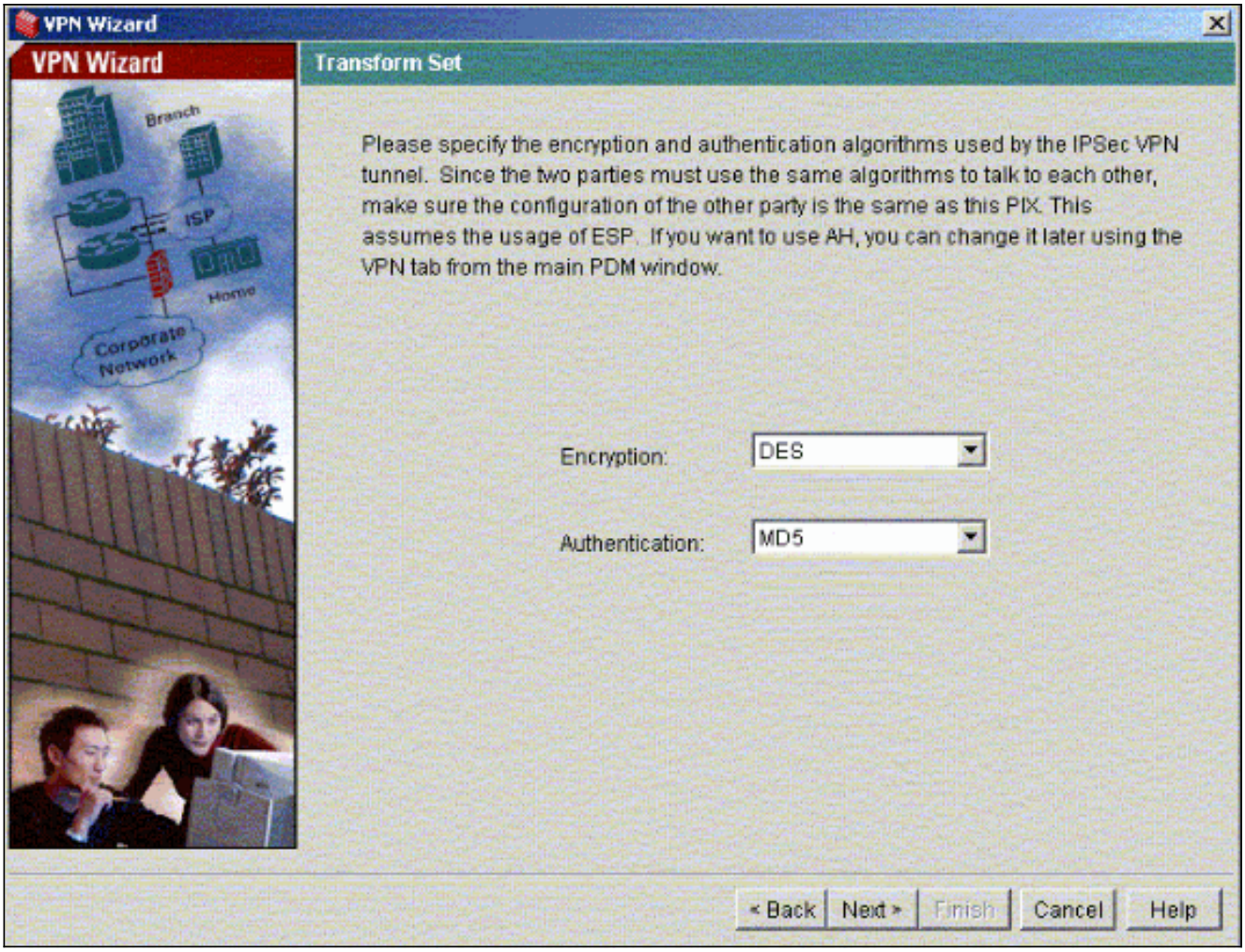
3. IPsecトンネルが終了するピアIPアドレスを入力します。この例では、トンネルはPIX-02の外部インターフェイスで終了します。[**Next**]をクリックします。



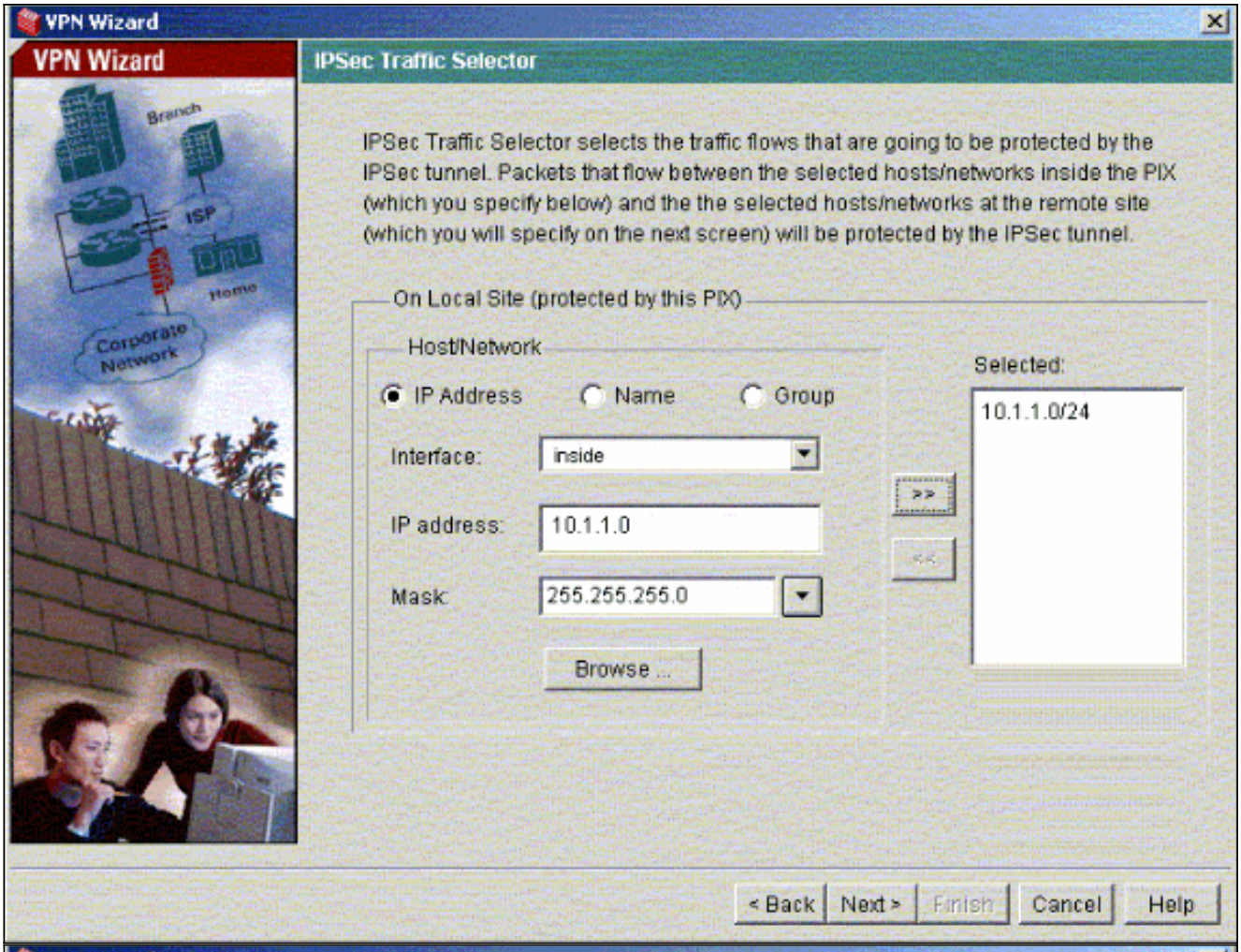
4. 使用するIKEポリシーパラメータを入力し、[Next]をクリックします。

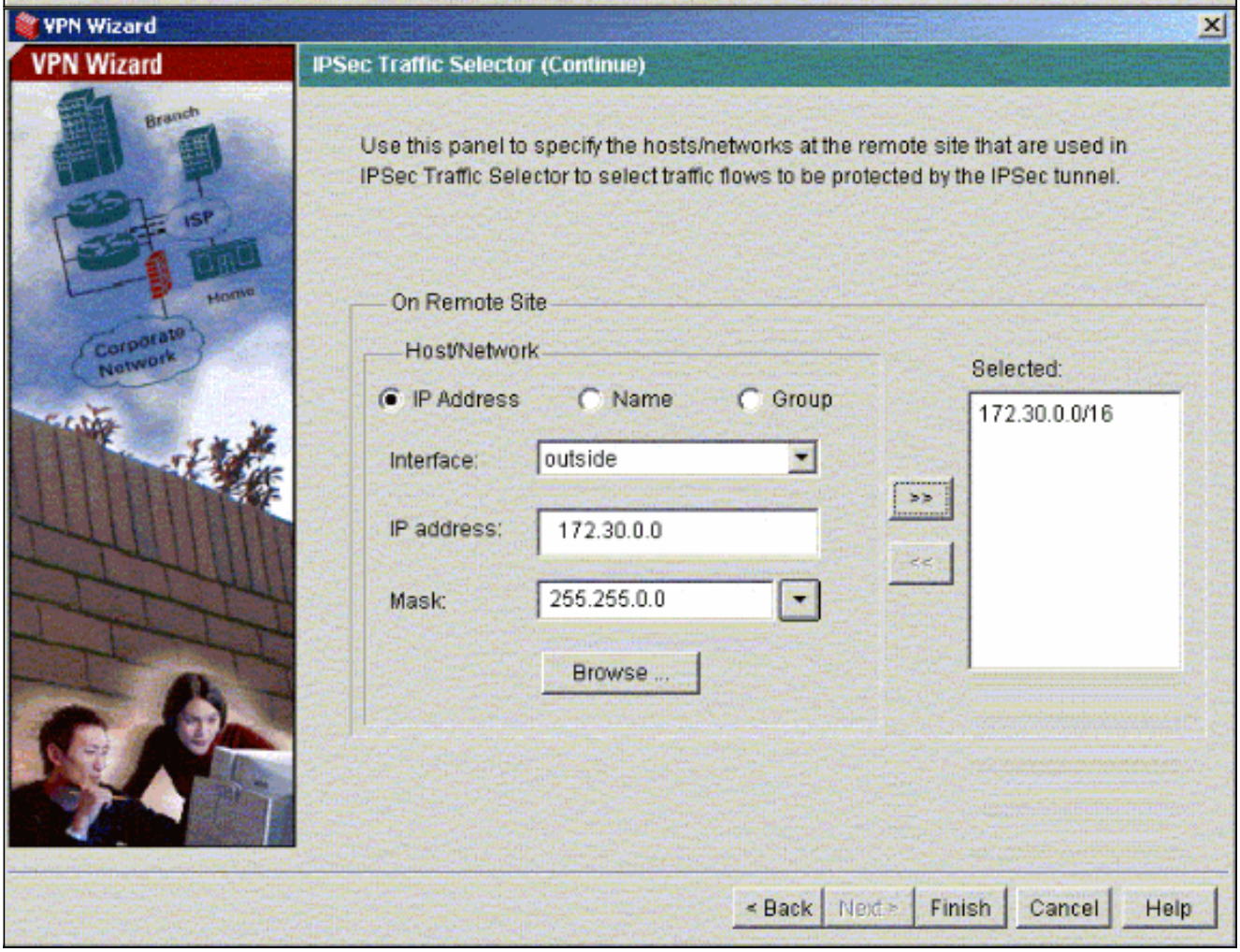


5. トランスフォームセットの暗号化パラメータと認証パラメータを指定し、**[Next]をクリックします**。



6. 保護する必要がある対象トラフィックを選択するには、IPsecを使用して保護する必要があるローカルネットワークとリモートネットワークを選択します。


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

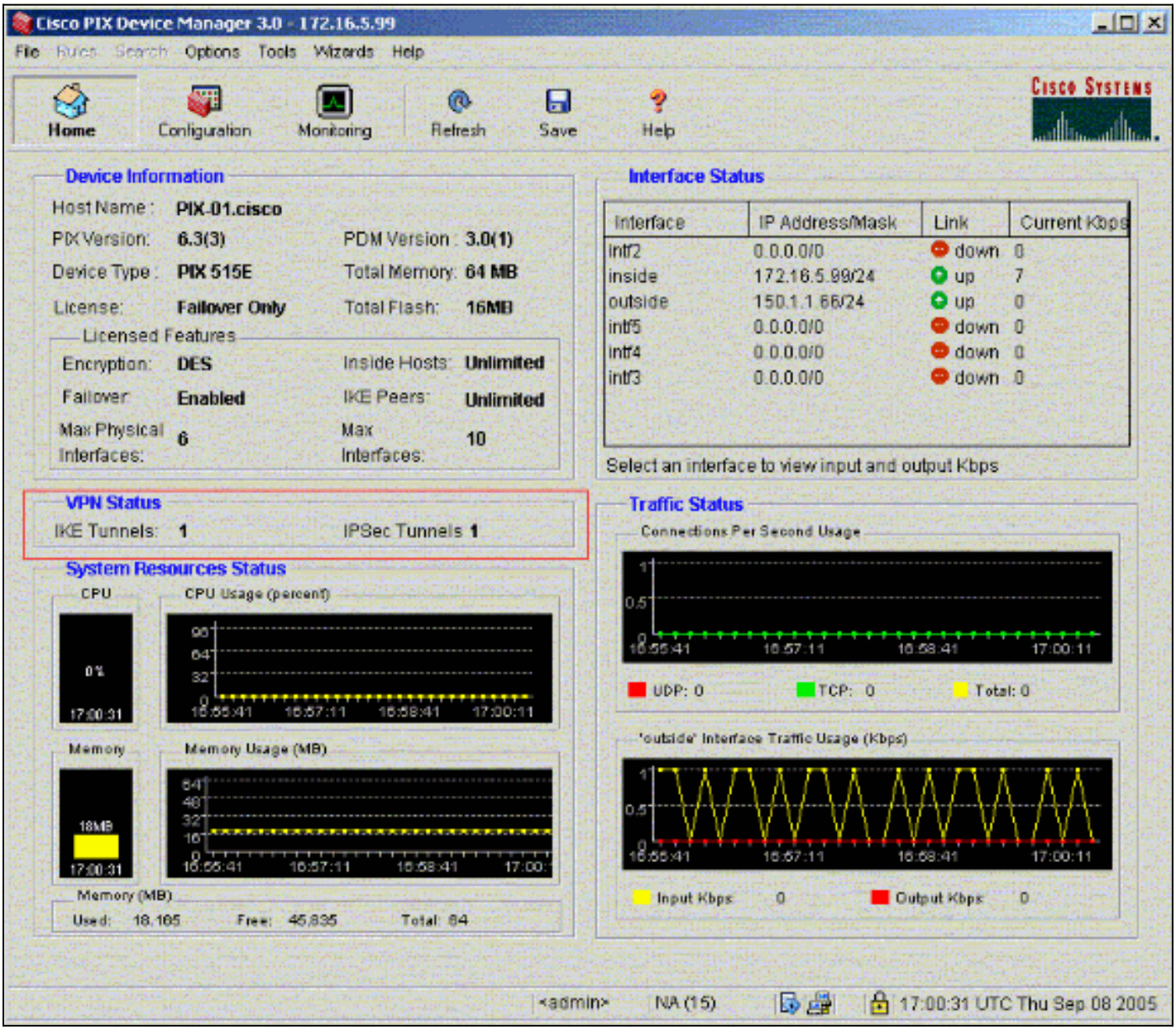

VPN Wizard
VPN Wizard
IPSec Traffic Selector (Continue)
Branch
ISP
Home
Corporate Network
Use this panel to specify the hosts/networks at the remote site that are used in IPSec Traffic Selector to select traffic flows to be protected by the IPSec tunnel.
On Remote Site
Host/Network
IP Address
Name
Group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

確認

ピアへの対象トラフィックがある場合、トンネルはPIX-01とPIX-02の間に確立されます。

これを確認するには、対象トラフィックが存在する場合に、R2経由でPIX-01とPIX-02の間にトンネルが確立されているR1シリアルインターフェイスをシャットダウンします。

トンネルの形成を確認**するために**、PDMの[Home]（**赤で強調表示**）の下の[VPN Status]を表示します。



PDMの[Tools]の下にあるCLIを使用して、トンネルの形成を確認することもできます。**show crypto isakmp sa**コマンドを発行してトンネルの形成を確認し、**show crypto ipsec saコマンドを発行してカプセル化、暗号化などのパケットの数を調**べます。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

PDMを使用したPIX Firewallの設定の詳細は、『Cisco PIX Device Manager 3.0』を参照してください。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- IPSec を使用した簡単な PIX-to-PIX VPN トンネル設定
- Cisco PIX Firewall ソフトウェア
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems