

在防火墙之间使用 PDM 创建冗余隧道

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[网络图](#)

[规则](#)

[背景信息](#)

[配置](#)

[配置过程](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍使用 Cisco PIX Device Manager (PDM) 在两个 PIX 防火墙之间配置隧道的过程。PIX 防火墙放置在两个不同的站点。在无法到达主路径的情况下，需要通过冗余链路来开启隧道。IPsec 是在 IPsec 对等体之间提供数据机密性、数据完整性和数据原始身份验证的开放标准组合。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

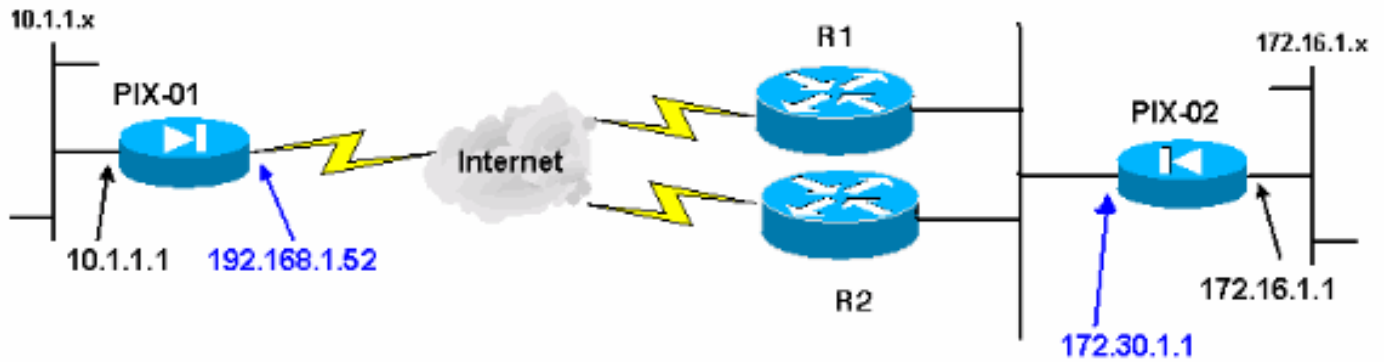
本文档中的信息基于以下软件和硬件版本：

- Cisco Secure PIX 515E 防火墙 6.x 以及 PDM 版本 3.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

网络图

本文档使用以下网络设置：



规则

有关文档约定的更多信息，请参考 [Cisco 技术提示约定](#)。

背景信息

IPsec 协商可分为五个步骤，并且包括两个 Internet 密钥交换 (IKE) 阶段。

IPsec 隧道由相关数据流启动。如果数据流在 IPsec 对等体之间传输，则它会被认为是相关数据流。

在 IKE 第 1 阶段中，IPsec 对等体对建立的 IKE 安全关联 (SA) 策略进行协商。对等体经过身份验证后，会使用 Internet 安全关联和密钥管理协议 (ISAKMP) 创建安全隧道。

在 IKE 第 2 阶段中，IPsec 对等体使用经身份验证的安全隧道对 IPsec SA 转换进行协商。共享策略的协商决定建立 IPsec 隧道的方式。

根据 IPsec 转换集中配置的 IPsec 参数，将在 IPsec 对等体之间创建 IPsec 隧道并传输数据。

如果删除了 IPsec SA，或者 IPsec SA 的生存时间到期，则 IPsec 隧道将终止。

注意：如果两个 IKE 阶段上的 SA 在对等体上不匹配，则两个 PIX 之间的 IPsec 协商失败。

配置

下面的过程将指导您完成其中一个 PIX 防火墙的配置，以便在存在相关流量时触发隧道。此配置还可帮助您在 PIX-01 与 PIX-02 之间没有通过路由器 1 (R1) 的连接时，建立通过备份链路的隧道，该备份链路通过路由器 2 (R2)。本文档说明如何使用 PDM 来配置 PIX-01。您可以按照类似方法来配置 PIX-02。

本文档假设您已配置路由。

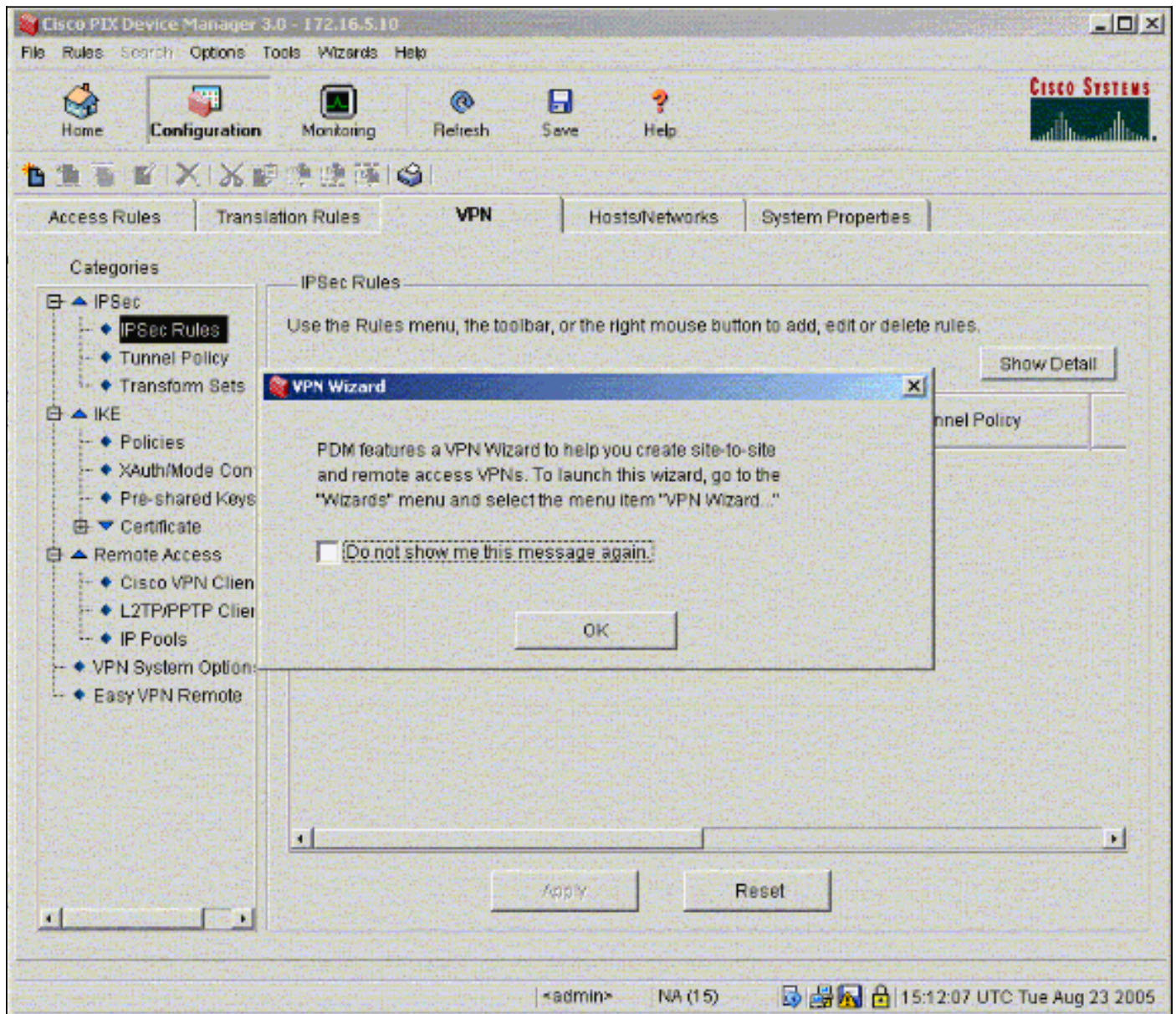
若要一次只接通一条链路，需要让 R2 为 192.168.1.0 网络和 172.30.0.0 网络通告一个更差度量。例如，如果您使用 RIP 进行路由，则除了其他网络通告外，R2 还具有下面的配置：

```
R2(config)#router rip
R2(config-router)#offset-list 1 out 2 s1
```

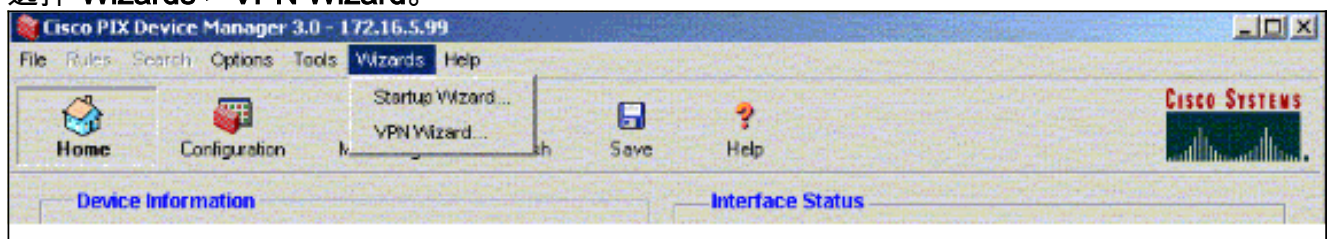
```
R2(config-router)#offset-list 2 out 2 e0
R2(config-router)#exit
R2(config)#access-list 1 permit 172.30.0.0 0.0.255.255
R2(config)#access-list 2 permit 192.168.1.0 0.0.0.255
```

配置过程

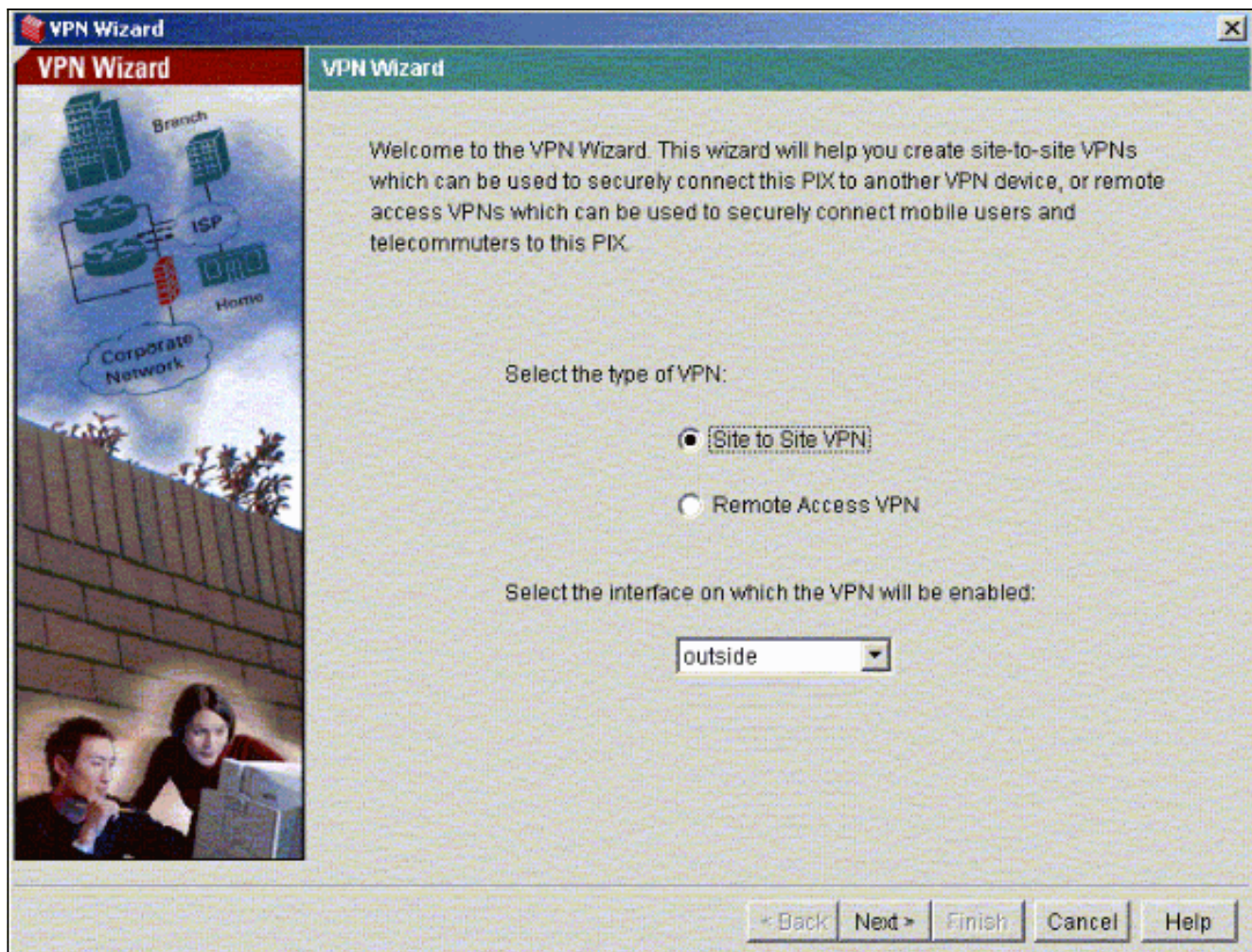
在首次键入 https://<Inside_IP_Address_on_PIX> 以启动 PDM 并单击 VPN 选项卡时，会显示有关自动 VPN 向导的信息。



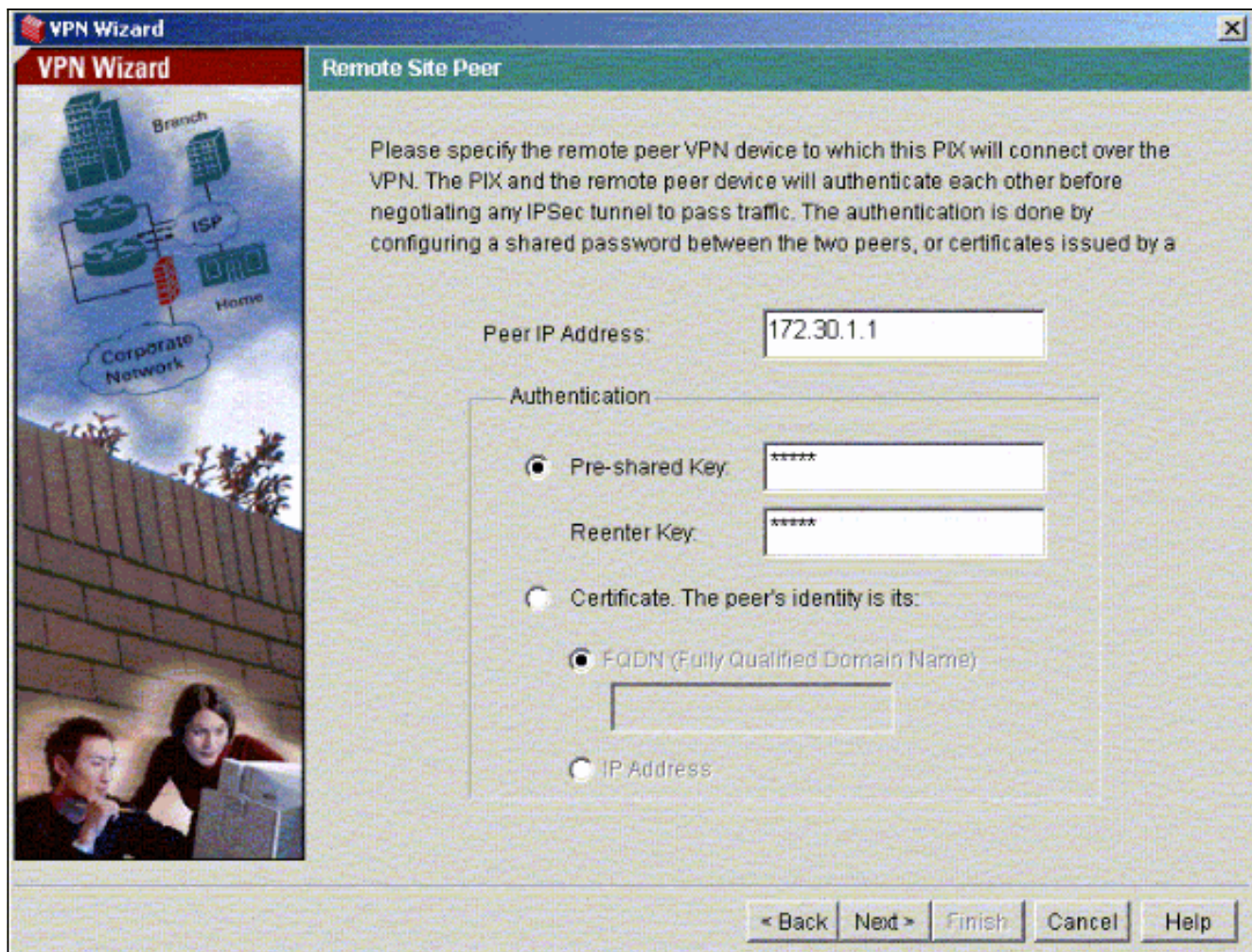
1. 选择 Wizards > VPN Wizard。



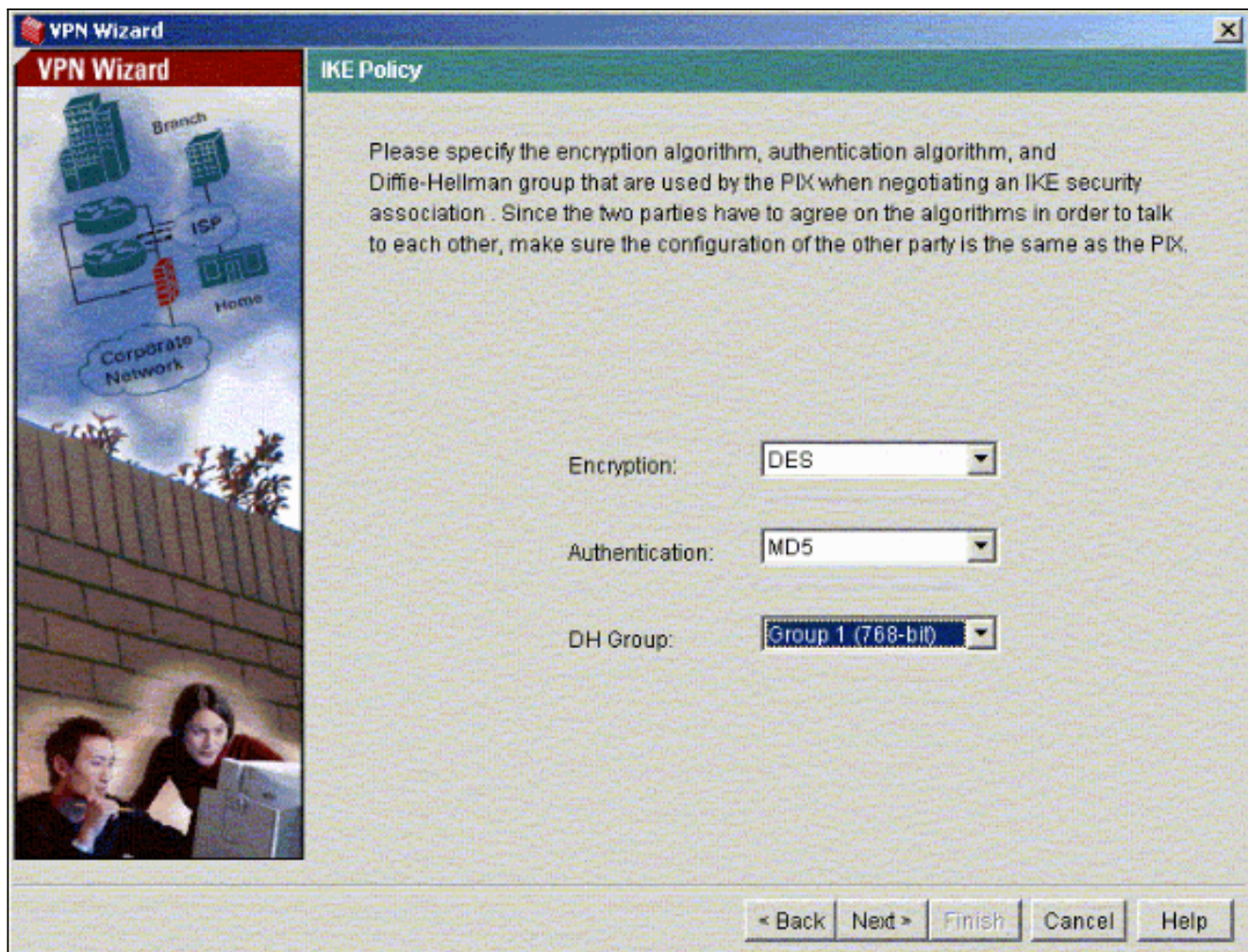
2. VPN 向导启动，并提示您选择要配置的 VPN 的类型。选择 Site-to-Site VPN，然后选择 outside 接口以作为将启用 VPN 的接口，然后单击 Next。



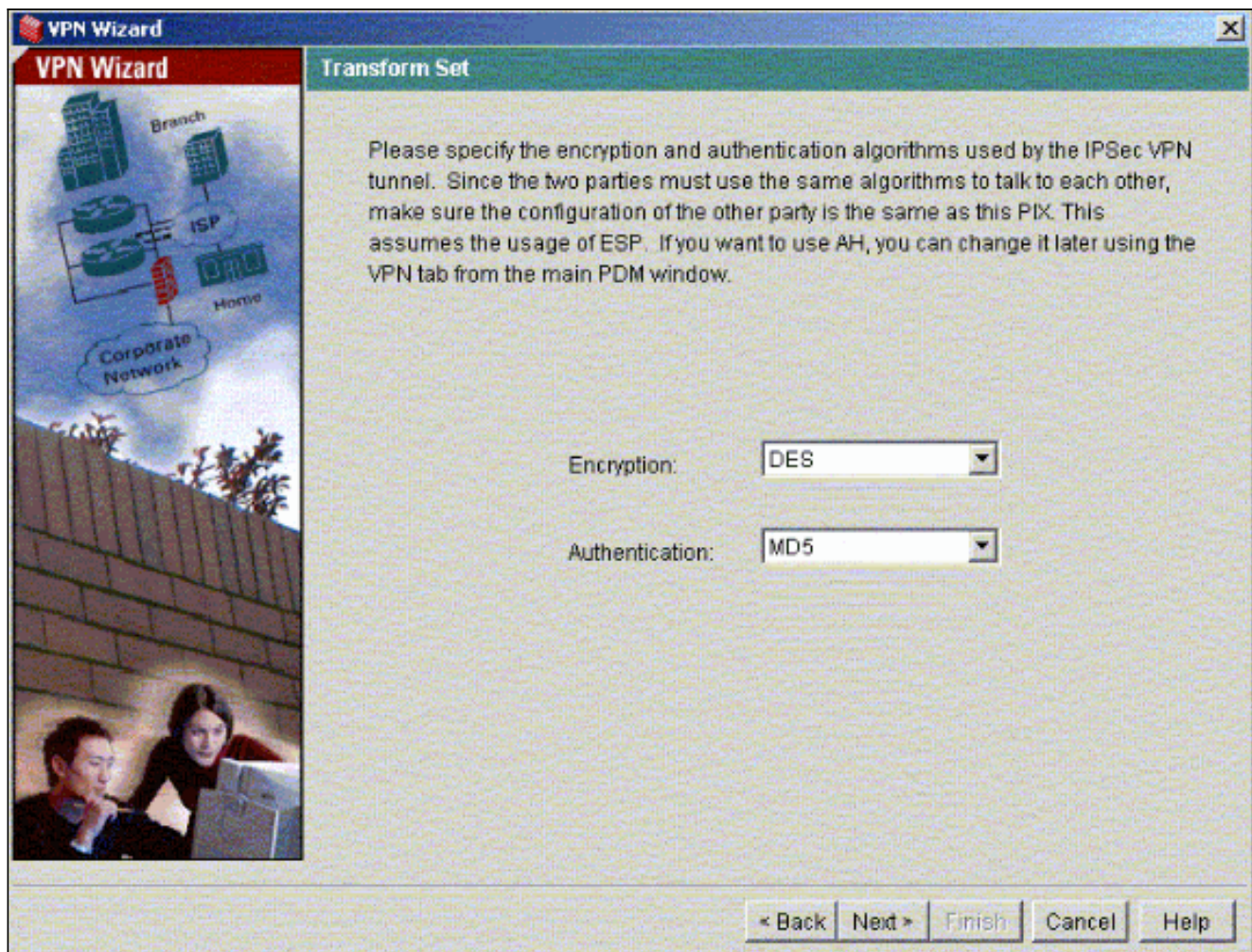
3. 输入对等体 IP 地址，IPsec 隧道应在此地址终止。在本示例中，隧道在PIX-02的外部接口上结束。单击Next。



4. 输入您选择使用的 IKE Policy 参数，然后单击 **Next**。




5. 为 Transform Set 提供 Encryption 和 Authentication 参数，然后单击 **Next**。



6. 为了选择需要保护的相关流量，请选择需要使用 IPsec 保护的本地网络和远程网络。

VPN Wizard X

VPN Wizard IPSec Traffic Selector



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:

IP address:


Mask:

Selected:

>> <<

VPN Wizard X

VPN Wizard IPSec Traffic Selector (Continue)



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:

IP address:

Mask:

Selected:

>> <<

验证

如果有流向对等体的相关流量，则将在 PIX-01 和 PIX-02 之间建立隧道。

为了验证这一点，请在存在相关流量时，关闭已在 PIX-01 和 PIX-02 之间建立通过 R2 的隧道的 R1 串行接口。

在 PDM 中查看 Home 下的 VPN Status (以红色突出显示) 以验证隧道是否已形成。

The screenshot displays the Cisco PIX Device Manager 3.0 interface. The 'VPN Status' section is highlighted with a red box, showing 1 IKE Tunnel and 1 IPSec Tunnel. The 'Interface Status' table is as follows:

Interface	IP Address/Mask	Link	Current Kbps
intf2	0.0.0.0/0	down	0
inside	172.16.5.99/24	up	7
outside	150.1.1.66/24	up	0
intf5	0.0.0.0/0	down	0
intf4	0.0.0.0/0	down	0
intf3	0.0.0.0/0	down	0

The 'System Resources Status' section shows CPU usage at 0% and Memory usage at 18MB. The 'Traffic Status' section includes graphs for Connections Per Second Usage and 'outside' Interface Traffic Usage (Kbps).

也可以使用 PDM 中 Tools 下的 CLI 来验证隧道是否已形成。发出 `show crypto isakmp sa` 命令可检查隧道是否已形成，发出 `show crypto ipsec sa` 命令可观察已执行了封装、加密等操作的数据包的数量。

[命令输出解释程序 \(仅限注册用户\) \(OIT\) 支持某些 show 命令。](#) 使用 OIT 可查看对 show 命令输出的分析。

有关使用 PDM 配置 PIX 防火墙的详细信息，请参阅 [Cisco PIX Device Manager 3.0](#)。

故障排除

目前没有针对此配置的故障排除信息。

[相关信息](#)

- [使用 IPsec 配置简单的 PIX 到 PIX VPN 隧道](#)
- [Cisco PIX 防火墙软件](#)
- [Cisco Secure PIX 防火墙命令参考](#)
- [请求注解 \(RFC\)](#)
- [技术支持和文档 - Cisco Systems](#)