Redundant Tunnel Creation between Firewalls using PDM

Document ID: 66166

Contents

Introduction

This document describes the procedure you use to configure tunnels between two PIX firewalls using Cisco PIX Device Manager (PDM). PIX firewalls are placed at two different sites. In case of a failure to reach the primary path, it is desirable to kick off the tunnel through a redundant link. IPsec is a combination of open standards that provide data confidentiality, data integrity, and data origin authentication between IPsec peers.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

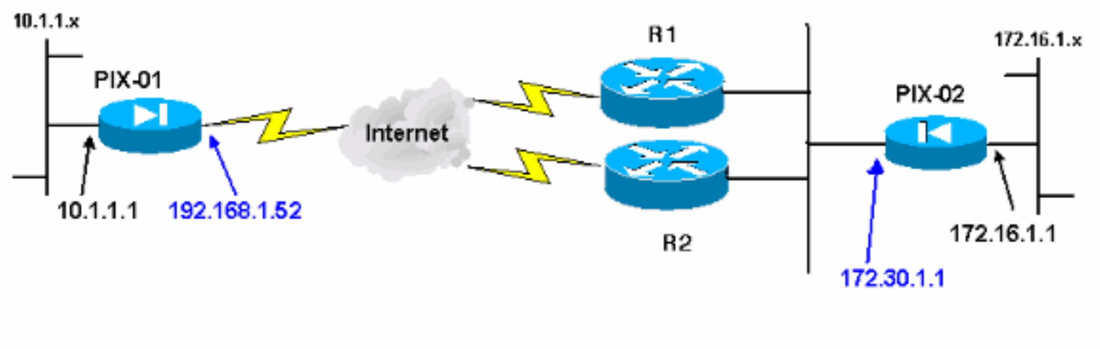
The information in this document is based on these software and hardware versions:

- Cisco Secure PIX 515E Firewalls with 6.x and PDM version 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.

Network Diagram

This document uses this network setup:



Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

IPsec negotiation can be broken down into five steps, and includes two Internet Key Exchange (IKE) phases.

An IPsec tunnel is initiated by interesting traffic. Traffic is considered interesting when it travels between the IPsec peers.

In IKE Phase 1, the IPsec peers negotiate the established IKE Security Association (SA) policy. Once the peers are authenticated, a secure tunnel is created using Internet Security Association and Key Management Protocol (ISAKMP).

In IKE Phase 2, the IPsec peers use the authenticated and secure tunnel to negotiate IPsec SA transforms. The negotiation of the shared policy determines how the IPsec tunnel is established.

The IPsec tunnel is created and data is transferred between the IPsec peers based on the IPsec parameters configured in the IPsec transform sets.

The IPsec tunnel terminates when the IPsec SAs are deleted or when their lifetime expires.

Note: IPsec negotiation between the two PIXes fails if the SAs on both of the IKE phases do not match on the peers.

Configuration

This procedure guides you through the configuration of one of the PIX firewalls to trigger the tunnel when interesting traffic exists. This configuration also helps you establish the tunnel through the backup link through router 2 (R2), when there is no connectivity between the PIX−01 and PIX−02 through router 1 (R1). This document shows the configuration of PIX−01 using PDM. You can configure PIX−02 on similar lines.

This document assumes that you have already configured the routing.

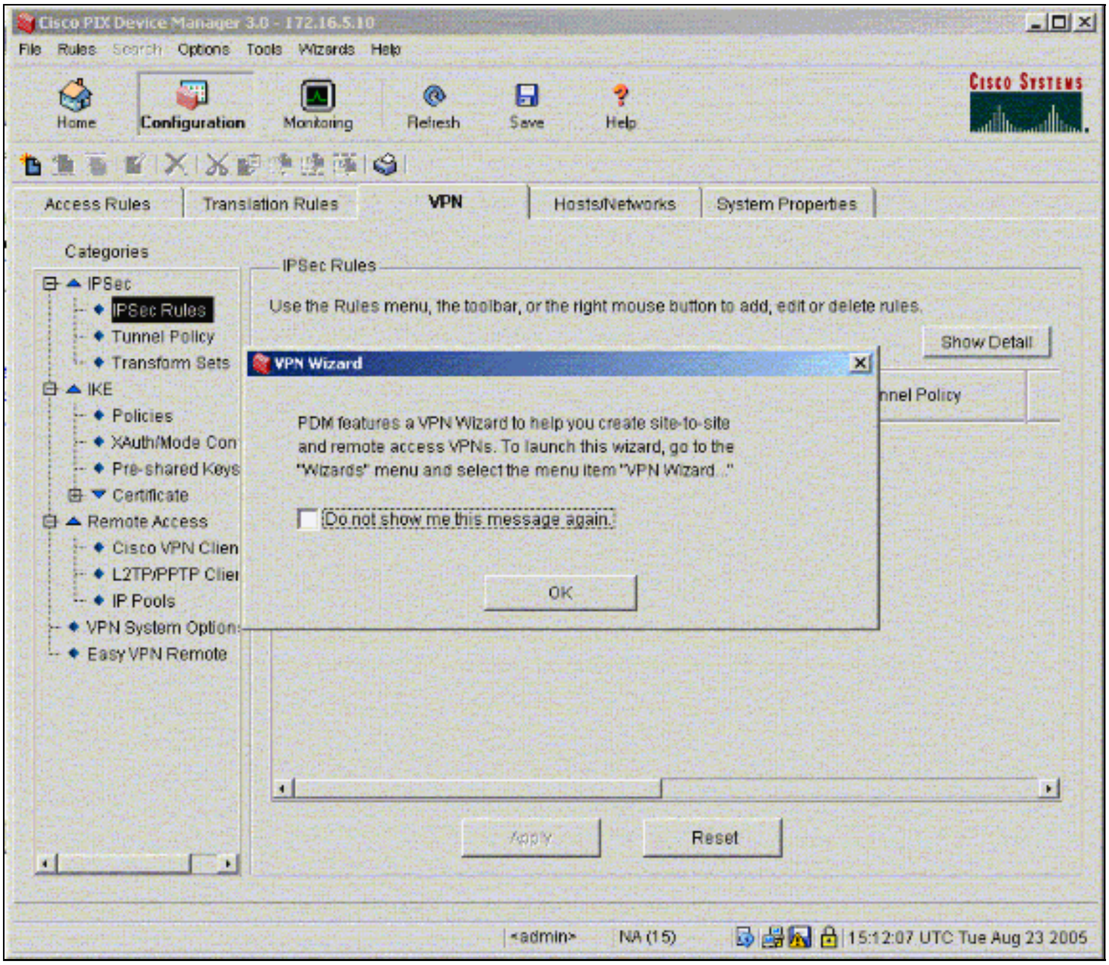
For only one link to be up at a time, make R2 advertize a worse metric for the 192.168.1.0 network as well as for the 172.30.0.0 network. For example, if you use RIP for the routing, R2 has this configuration apart from other network advertisements:

```
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
```

Configuration Procedure

When you type **https://<Inside_IP_Address_on_PIX>** in order to launch PDM and click the VPN tab for the first time, information about the automatic VPN Wizard displays.

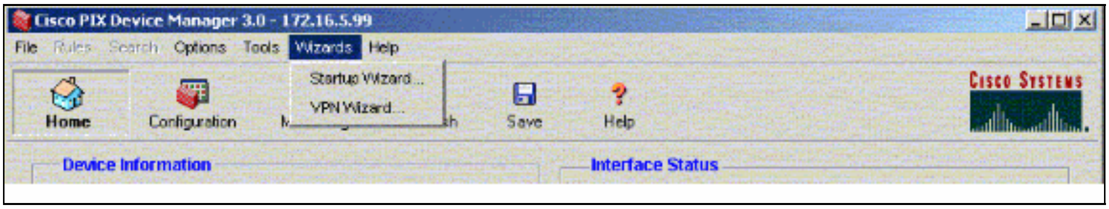


Use the Rules menu, the toolbar, or the right mouse button to add, edit or delete rules.

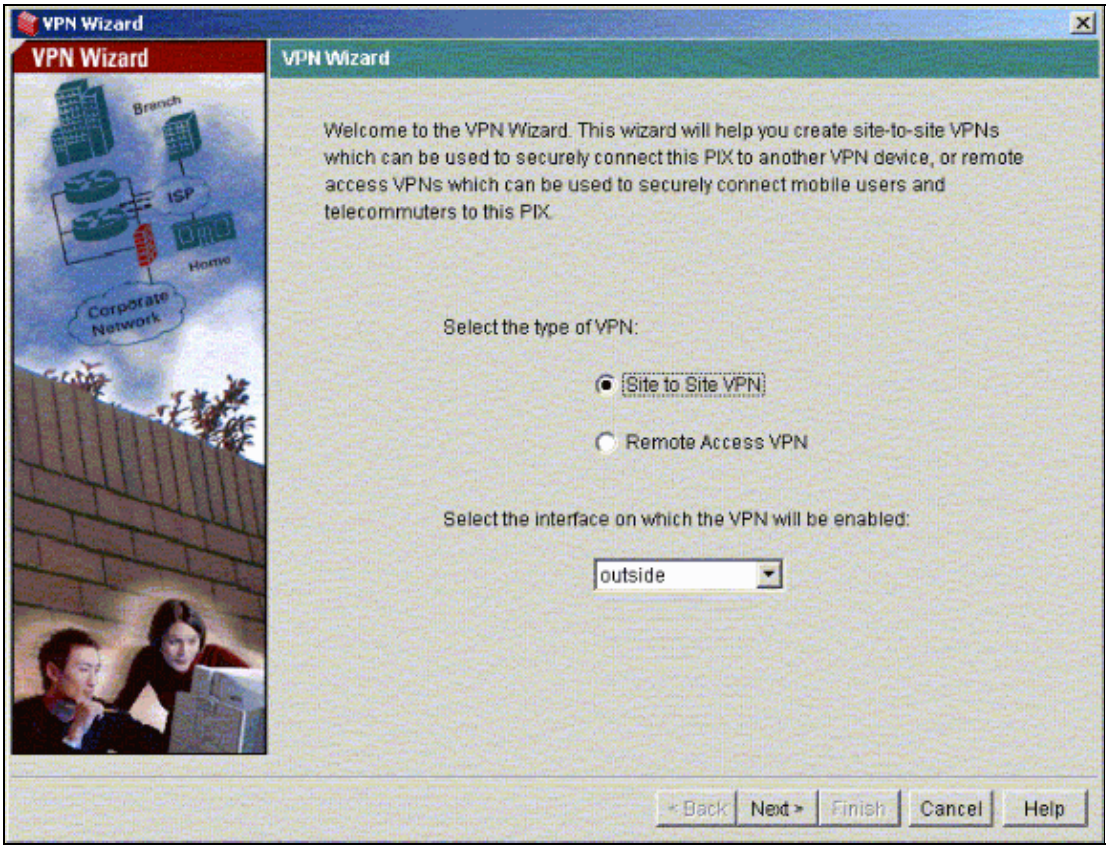
PDM features a VPN Wizard to help you create site-to-site and remote access VPNs. To launch this wizard, go to the "Wizards" menu and select the menu item "VPN Wizard..."

□ Do not show me this message again.

1. Select **Wizards > VPN Wizard**.



2. The VPN wizard starts and prompts you for the type of VPN you want to configure. Choose **Site−to−Site VPN**, select the **outside** interface as the interface on which the VPN will be enabled, and click **Next**.



VPN Wizard

Welcome to the VPN Wizard. This wizard will help you create site-to-site VPNs which can be used to securely connect this PIX to another VPN device, or remote access VPNs which can be used to securely connect mobile users and telecommuters to this PIX.

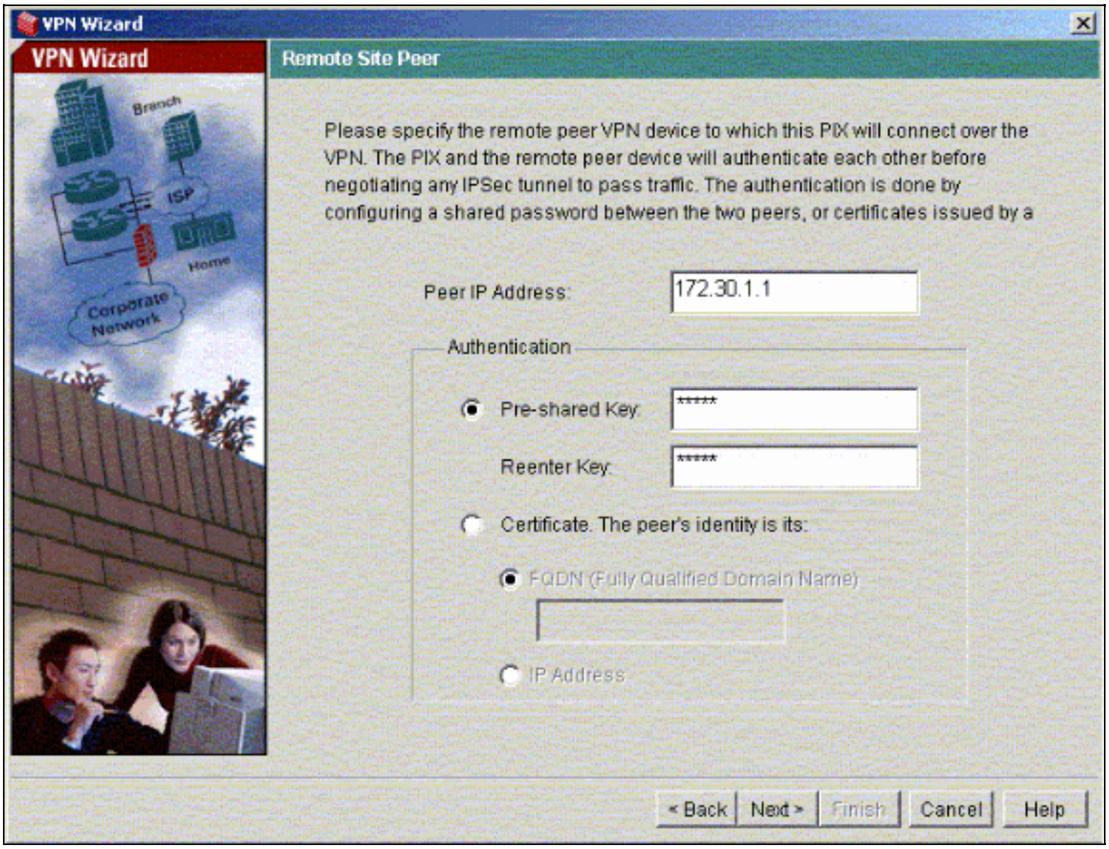
Select the type of VPN:

● Site to Site VPN

○ Remote Access VPN

Select the interface on which the VPN will be enabled: outside

3. Enter the Peer IP address, where the IPsec tunnel should end. In this example, the tunnel ends on the outside interface of PIX−02. Click **Next**.



Remote Site Peer

Please specify the remote peer VPN device to which this PIX will connect over the VPN. The PIX and the remote peer device will authenticate each other before negotiating any IPSec tunnel to pass traffic. The authentication is done by configuring a shared password between the two peers, or certificates issued by a

Peer IP Address: 172.30.1.1

Authentication

● Pre-shared Key: *****

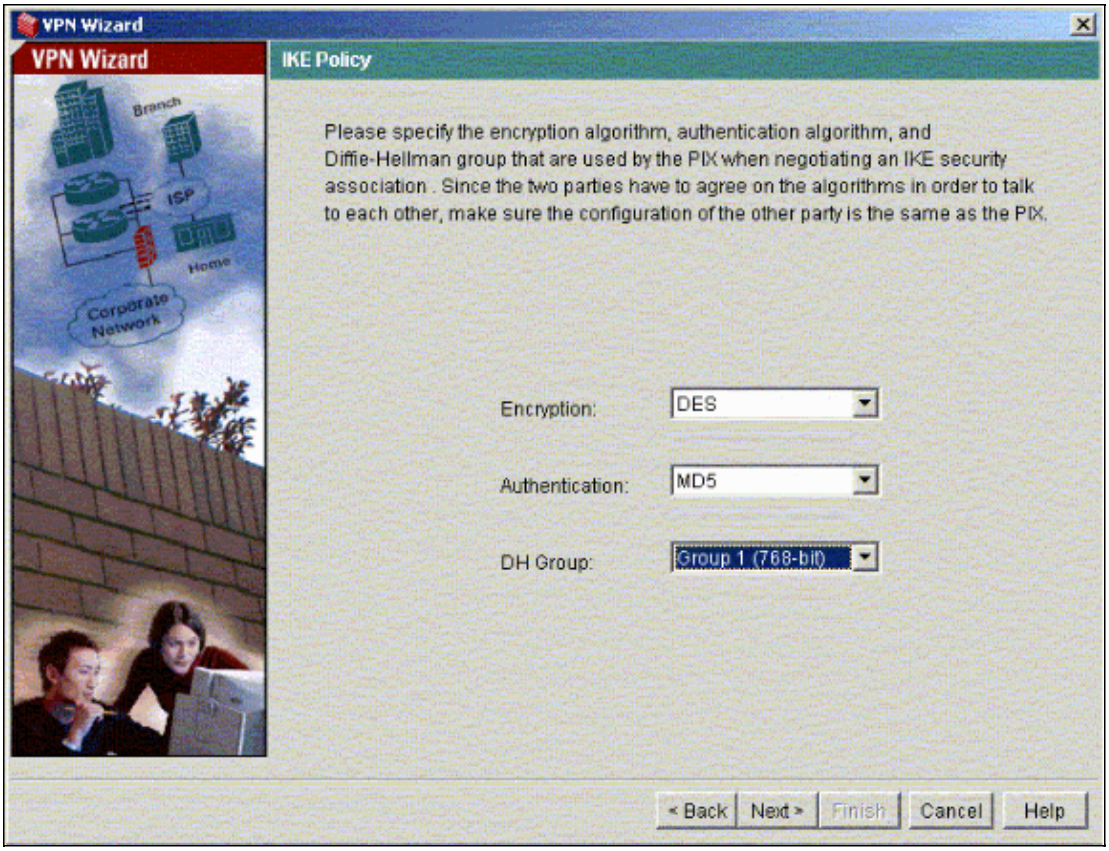
Reenter Key: *****

○ Certificate. The peer's identity is its:

● FQDN (Fully Qualified Domain Name)

○ IP Address

4. Enter the IKE Policy parameters that you choose to use and click **Next**.



IKE Policy

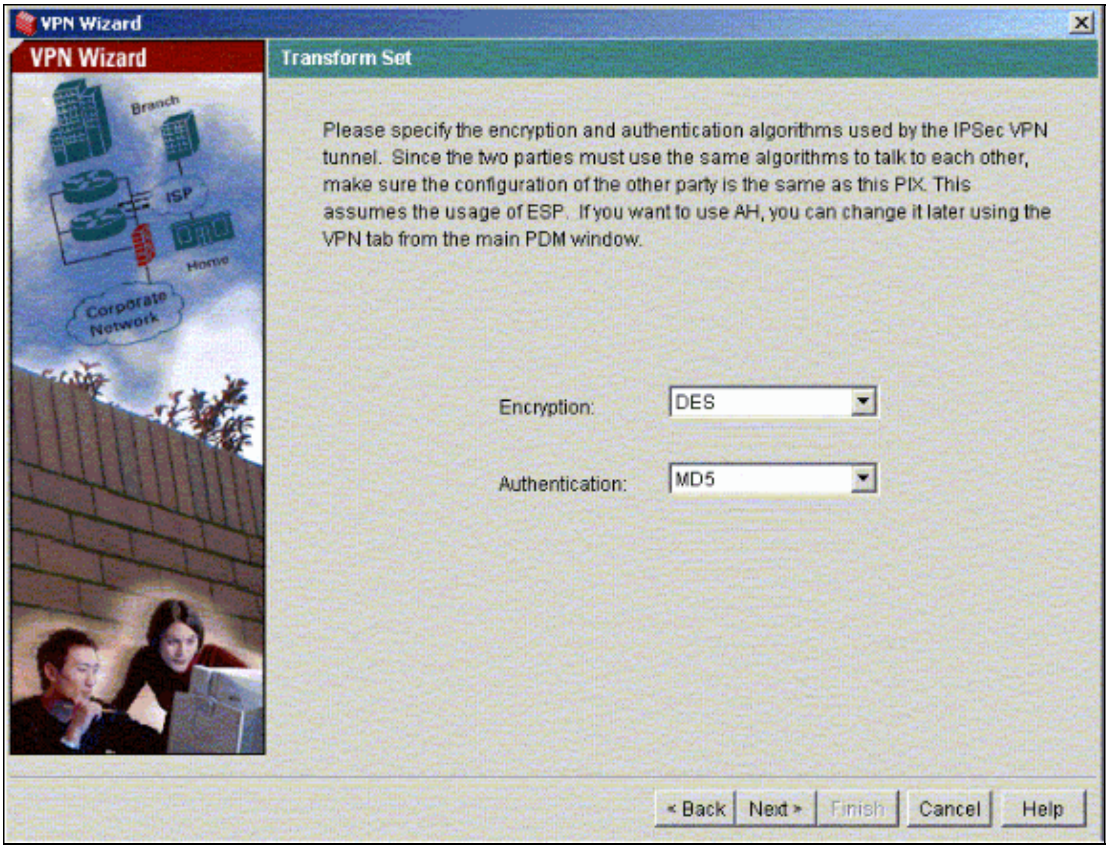
Please specify the encryption algorithm, authentication algorithm, and Diffie-Hellman group that are used by the PIX when negotiating an IKE security association . Since the two parties have to agree on the algorithms in order to talk to each other, make sure the configuration of the other party is the same as the PIX.

Encryption: DES

Authentication: MD5

DH Group: Group 1 (768-bit)

5. Provide the Encryption and Authentication parameters for the Transform Set and click **Next**.



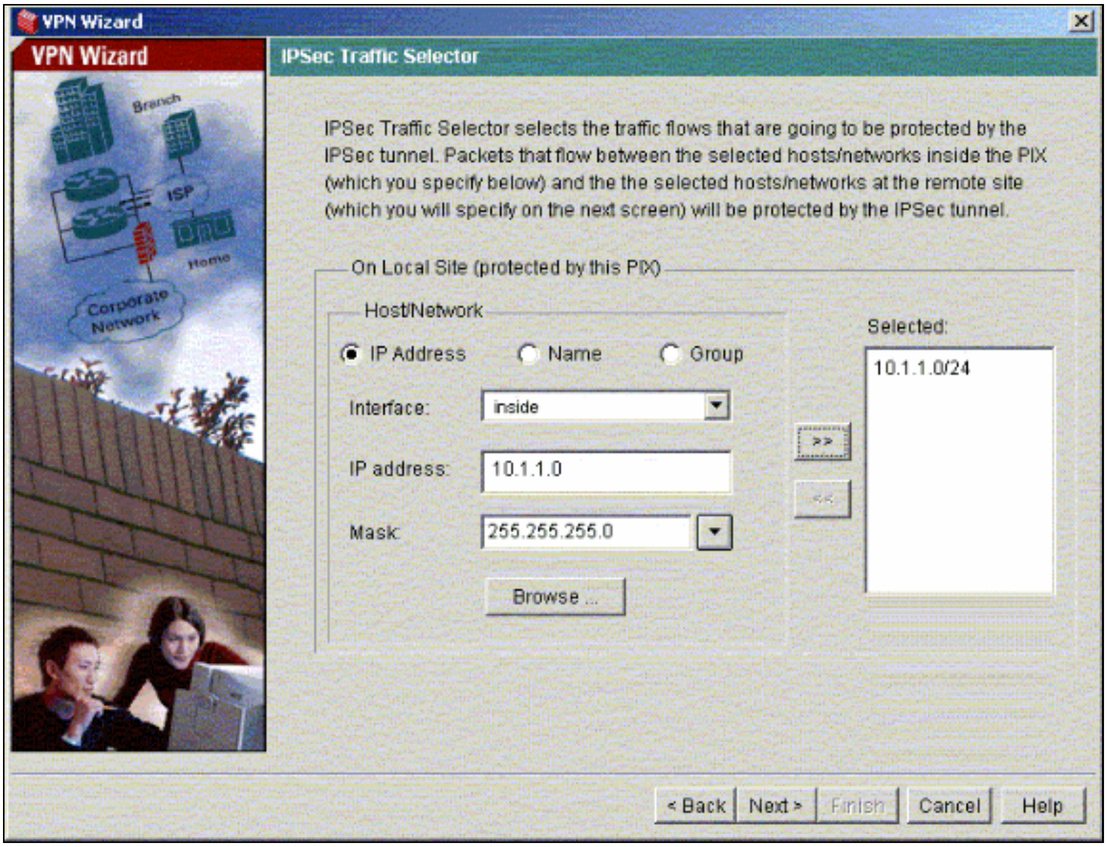
Transform Set

Please specify the encryption and authentication algorithms used by the IPSec VPN tunnel. Since the two parties must use the same algorithms to talk to each other, make sure the configuration of the other party is the same as this PIX. This assumes the usage of ESP. If you want to use AH, you can change it later using the VPN tab from the main PDM window.

Encryption: DES

Authentication: MD5

6. Select the local network and the remote networks you need to protect using IPsec in order to select the interesting traffic that you need to protect.



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: inside

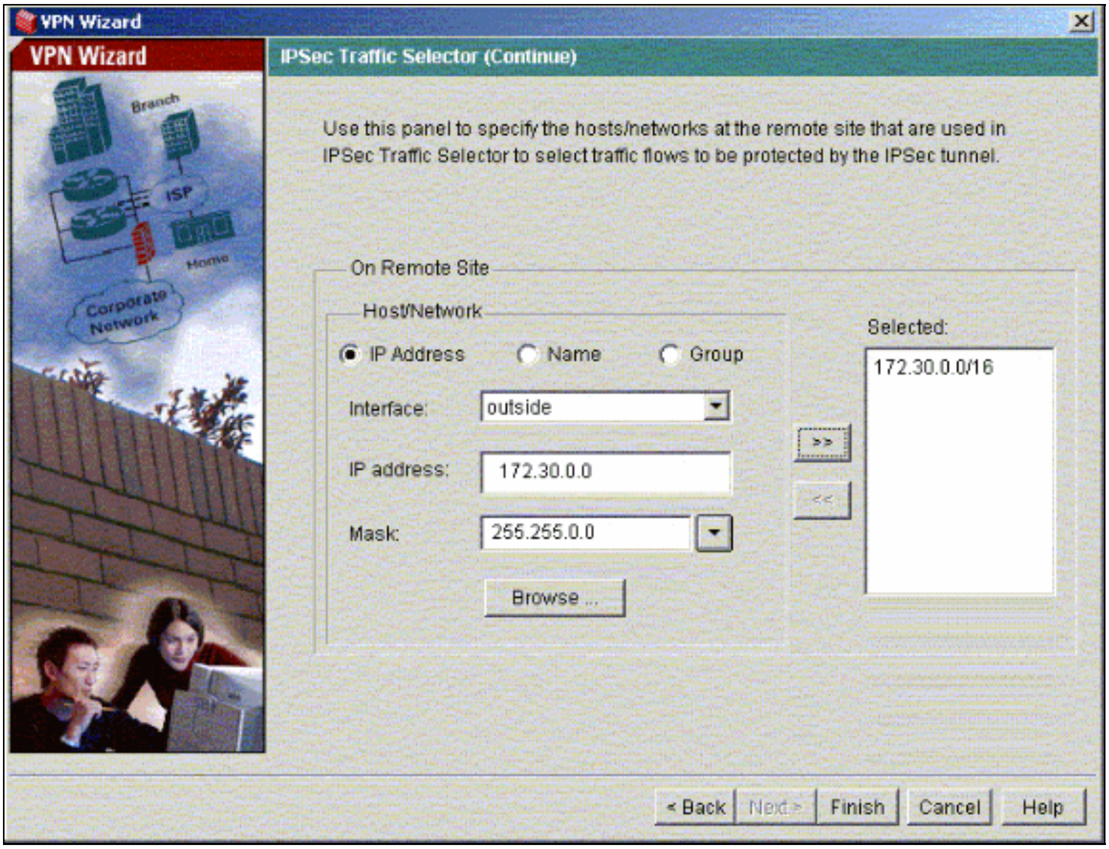
IP address: 10.1.1.0

Mask: 255.255.255.0

Browse ...

Selected:

10.1.1.0/24



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: outside

IP address: 172.30.0.0

Mask: 255.255.0.0

Browse ...

Selected:

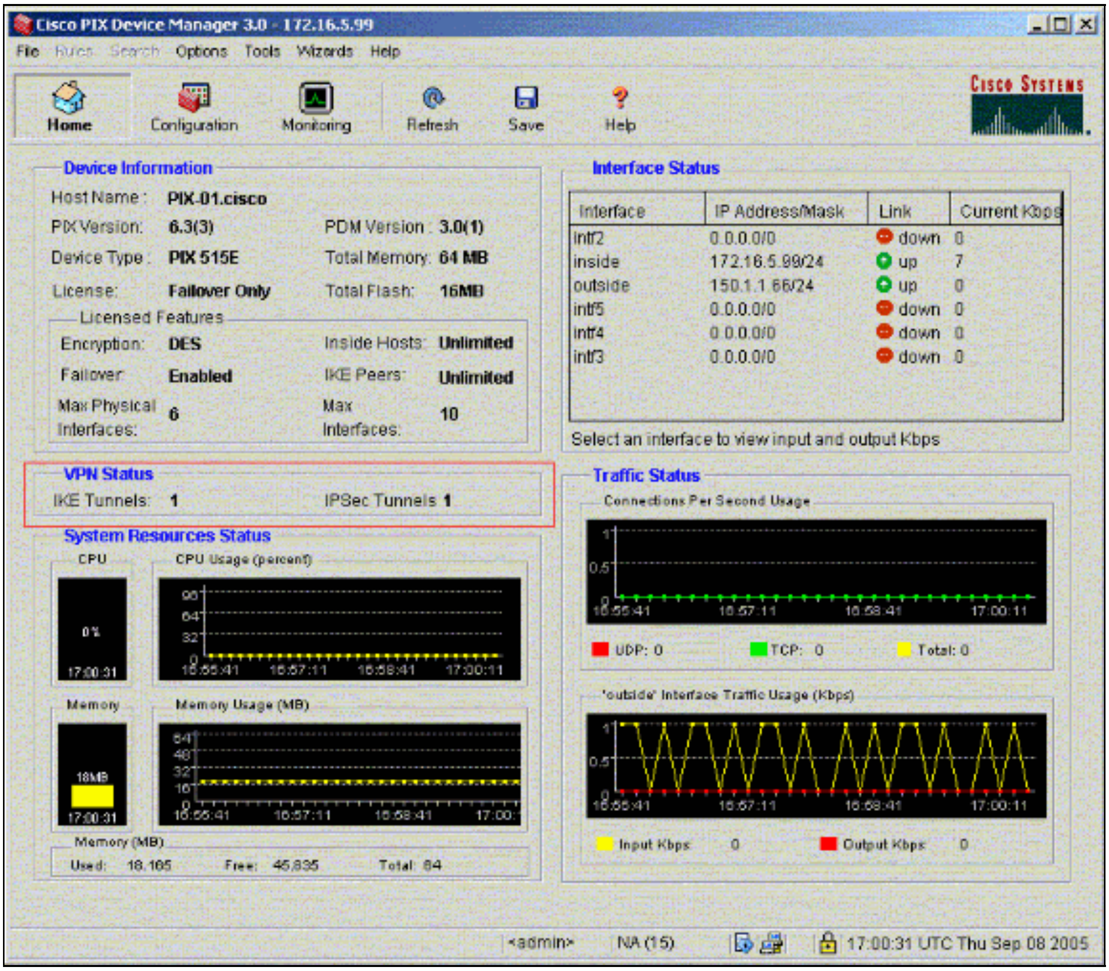
172.30.0.0/16

Verify

If there is interesting traffic to the peer, the tunnel is established between PIX−01 and PIX−02.

In order to verify this, shut down the R1 serial interface for which the tunnel is established between PIX−01 and PIX−02 via R2 when the interesting traffic exists.

View the **VPN Status** under **Home** in the PDM (highlighted in red) in order to verify the formation of the tunnel.



Device Information

Host Name: PIX-01.cisco

PIX Version: 6.3(3) PDM Version: 3.0(1)

Device Type: PIX 515E Total Memory: 64 MB

License: Failover Only Total Flash: 16MB

Licensed Features

Encryption: DES Inside Hosts: Unlimited

Failover: Enabled IKE Peers: Unlimited

Max Physical Interfaces: 6 Max Interfaces: 10

Interface Status

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

Select an interface to view input and output Kbps

VPN Status

IKE Tunnels: 1 IPSec Tunnels: 1

System Resources Status

Memory (MB)

Used: 18.165 Free: 45.835 Total: 64

Traffic Status

<admin> NA (15) 17:00:31 UTC Thu Sep 08 2005

You can also verify the formation of tunnels using CLI under Tools in the PDM. Issue the **show crypto isakmp sa** command to check the formation of tunnels and issue the **show crypto ipsec sa** command to observe the number of packets encapsulated, encrypted, and so forth.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Refer to Cisco PIX Device Manager 3.0 for more information on the configuration of the PIX Firewall using PDM.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Configuring a Simple PIX−to−PIX VPN Tunnel Using IPsec**
- **Cisco PIX Firewall Software**
- **Cisco Secure PIX Firewall Command References**

- **Requests for Comments (RFCs)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Feb 02, 2006 Document ID: 66166