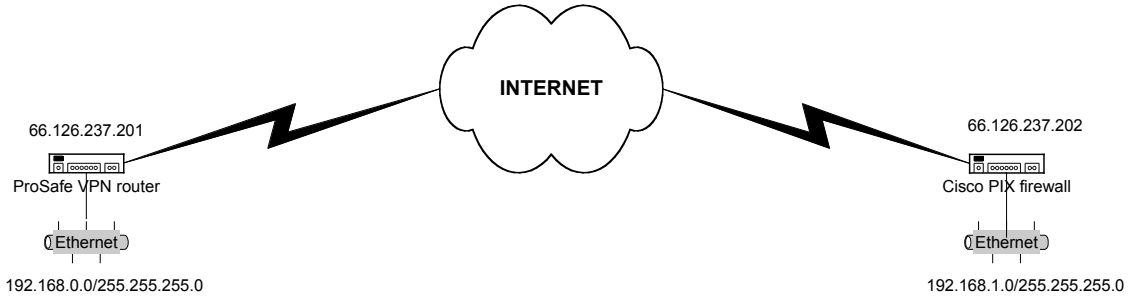
Netgear ProSafe VPN firewall (FVS318 or FVM318) to Cisco PIX firewall

This document is a step-by-step instruction for setting up VPN between Netgear ProSafe VPN firewall (FVS318 or FVM318) and Cisco PIX firewall.

The instruction is verified with FVS318 (firmware version v2.4), FVM318 (firmware version R1.2 Beta) and Cisco PIX 501 (firmware 6.3.3 and Pix Device Manager PDM 3.0).

Scenario:



Both the Netgear ProSafe VPN router and the Cisco PIX firewall are connection to Internet with a public IP address assigned to the WAN interface. The VPN is configure with the following parameters:

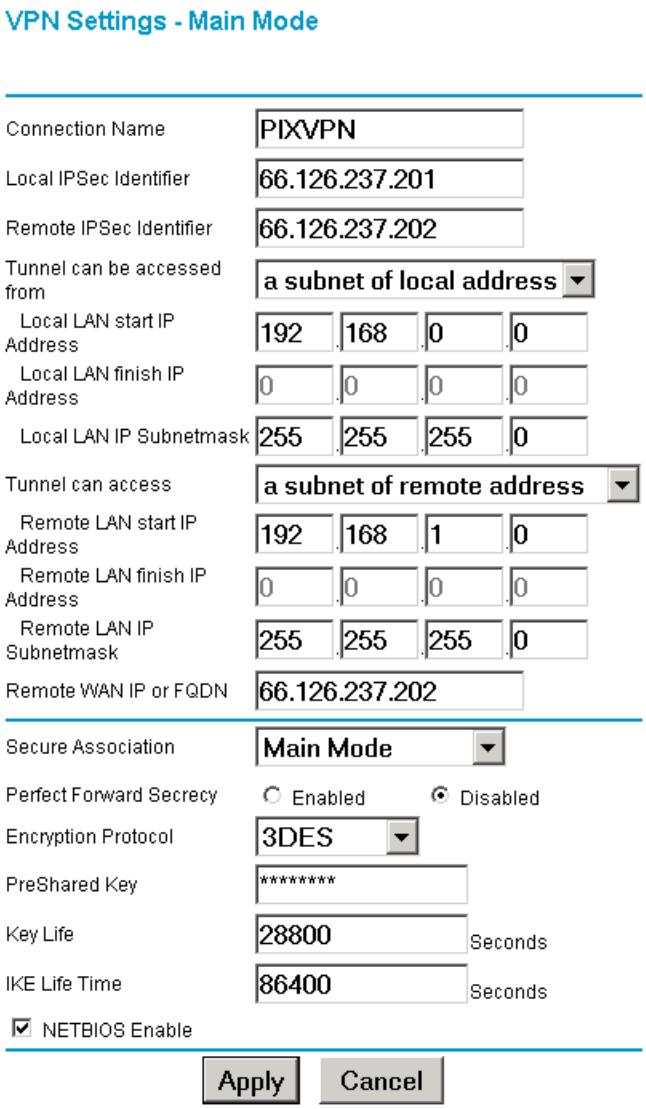
	Netgear ProSafe VPN Router	Cisco Pix Firewall
Local IKE identity	66.126.237.201	66.126.237.202
Remote IKE identity	66.126.237.202	66.126.237.201
Local VPN Subnet	192.168.0.0	192.168.1.0
Local VPN subnet netmask	255.255.255.0	255.255.255.0
Encryption algorithm	3DES	3DES
Authentication algorithm	MD5	MD5
Pre-shared key	12345678	12345678
IKE mode	Main mode	Main mode

The above parameters are specific to our network settings. User will most likely need to change the parameters to match their network setting such as IP addresses of the VPN gateways and the local area networks IP addresses. User can also choose a different encryption algorithm or authentication algorithm. A different pre-shared key is also recommended. The requirement is the same encryption/authentication algorithm and pre-shared key have to be specified in both the Netgear router's and PIX firewall's VPN policy.

I. Configure the Netgear ProSafe VPN router:

1. Log in to the Netgear ProSafe VPN router.
2. Click on **VPN Setting** under the Setup menu. Choose one of the unused policies and click Edit.

    a. Enter a descriptive name for the VPN policy in the **Connection Name** textbox. It is only being used to help user manage the VPN polices. For our example, PIXVPN.
    b. In the Local IPSEC Identifier textbox, enter the WAN IP address of the Netgear router.
    c. In the Remote IPSec Identifier textbox, enter the WAN IP address of the PIX firewall
    d. In the **Tunnel can be accessed from** box, choose **a subnet of local address**. Enter the LAN IP address of the Netgear router for **Local LAN start IP Address**. Enter the LAN subnet mask for **Local LAN IP Subnetmask**. IP information can be looked up from the LAN IP Setup menu.
    e. In the **Tunnel can access** box, choose **a subnet of remote address**. For **Remote LAN start IP address**, enter the LAN IP subnet behind the PIX firewall. For Remote LAN IP Subnetmask, enter the subnet mask of the LAN IP subnet behind the PIX firewall.
    f. In the **Remote WAN IP or FQDN** box, enter the PIX firewall's WAN IP address.
    g. For **Secure Association**, choose **Main Mode**.
    h. For **Perfect Forward Secrecy**, check **Disabled**.
    i. For **Encryption Protocol**, choose **3DES**.
    j. For **Pre-shared Key,** enter the pre-shared key "12345678".
    k. Enter 28800 seconds for **Key Life**.
    l. Enter 86400 for **IKE Life Time**.
    m. Check the box **NETABIOS Enable**.
    n. Click **Apply**.



There are three methods of creating VPN policy with a PIX firewall – command line interface, VPN configuration page within the PDM, VPN wizard within the PDM. We will describe step-by-step instruction for all three methods.

The instruction is tested with the PIX firewall in its factory default setting. We have only configured the firewall's WAN interface IP address and the default gateway before setting up VPN policy. Your PIX firewall may have existing configurations that need to be modified in order for the VPN to work. For example, firewall rules and NAT (network address translation) rules may interfere with your VPN. Please refer to your Cisco documentation for configuring those settings.

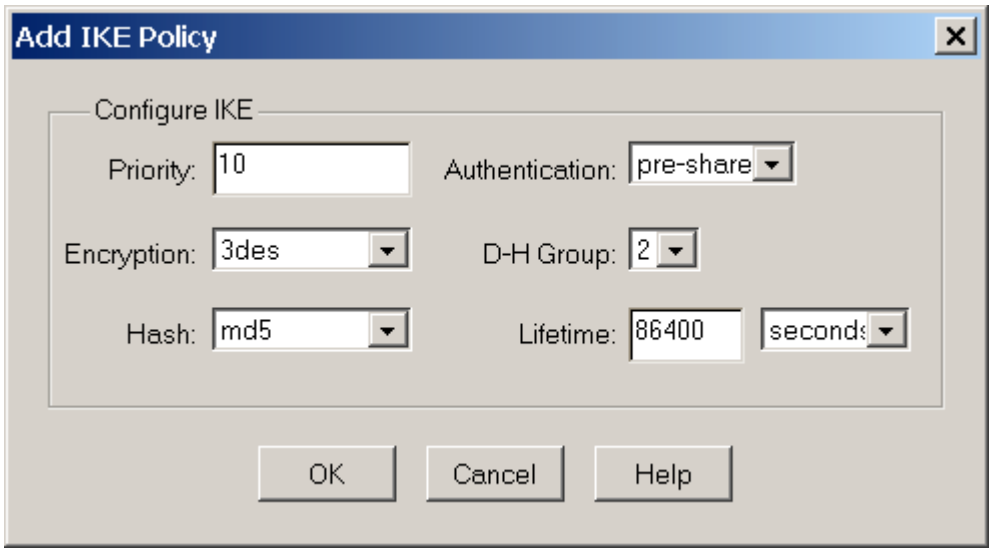
From the Cisco PIX command line interface:

1. Log into the command line interface through either console, telnet or ssh.
2. Type *enable* to enter enable mode. Enter your password when prompted.
3. Type *config t* to enter configuration mode.

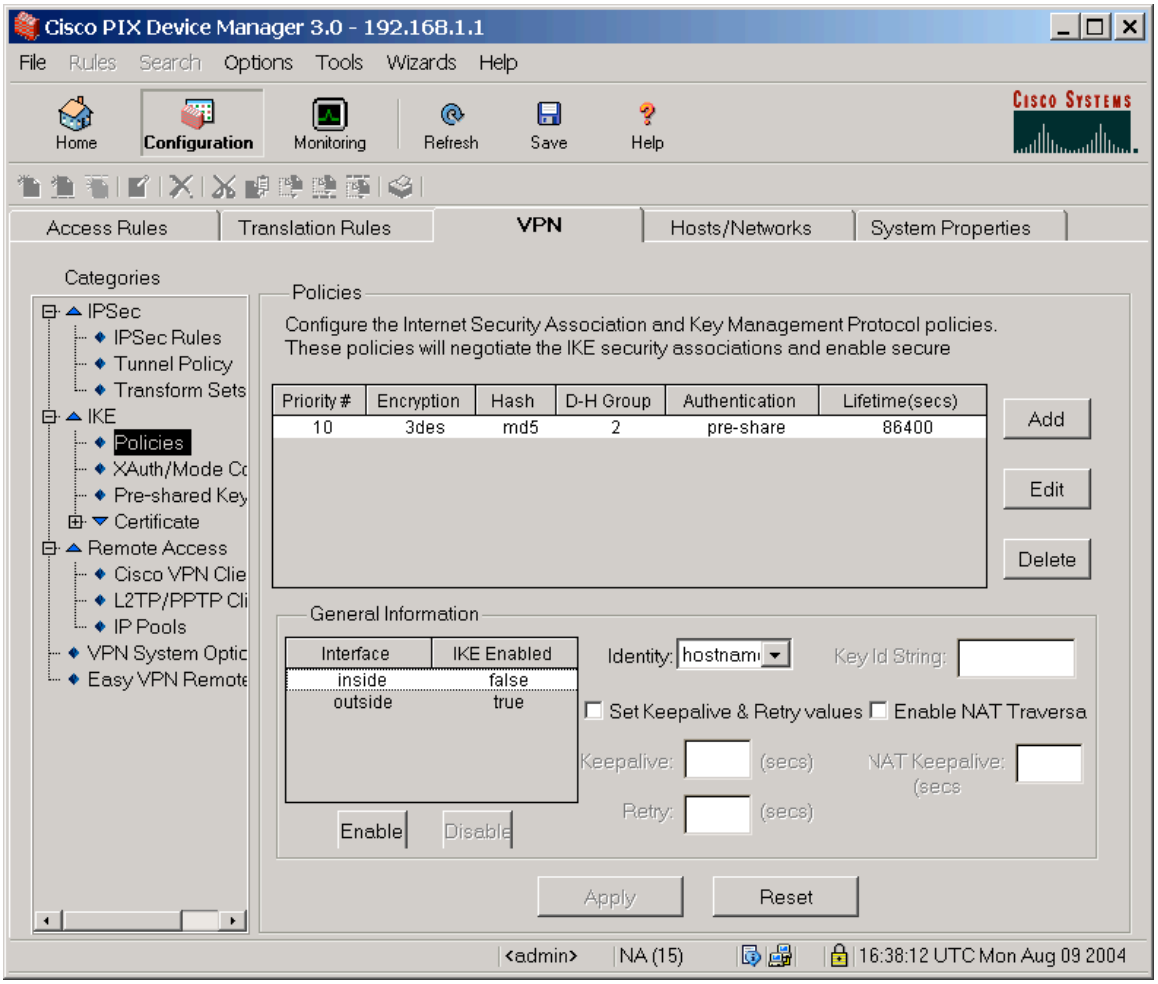
4. Create a name object for your local network – 192.168.0.0 in our example.
   name 192.168.0.0 remoteVPN
5. Create an access list to exclude from NAT, the access should specific traffic from your local network to the remote network.
   access-list inside_nat0_outbound permit ip 192.168.1.0 255.255.255.0 remoteVPN 255.255.255.0
6. Create an access list defining the traffic to be encrypted by the VPN.
   access-list outside_cryptomap_20 permit ip 192.168.1.0 255.255.255.0 remoteVPN 255.255.255.0
7. Create a NAT rule to not translate traffic between your local network and the remote network.
   nat (inside) 0 access-list inside_nat0_outbound
8. Enable IPSEC traffic to be permitted from the Internet.
   sysopt connection permit-ipsec
9. Create a transform set with the encryption and authentication algorithms you have chosen.
   crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
10. Create a crypt map using IPSEC ISAKMP.
    crypto map outside_map 20 ipsec-isakmp
11. Specify your VPN traffic, defined in step(6), for the crypto map.
    crypto map outside_map 20 match address outside_cryptomap_20
12. Specify the VPN peer – the Netgear router.
    crypto map outside_map 20 set peer 66.126.237.201
13. Specify the transform set – created in step (9).
    crypto map outside_map 20 set transform-set ESP-3DES-MD5
14. Apply the crypto map to the outside interface.
    crypto map outside_map interface outside
15. Enter the IKE parameters.
    isakmp enable outside
    isakmp policy 10 authentication pre-share
    isakmp policy 10 encryption 3des
    isakmp policy 10 hash md5
    isakmp policy 10 group 2
    isakmp policy 10 lifetime 86400
16. Define your pre-shared key. “12345678” in our example.
    *isakmp key ******** address 66.126.237.201 netmask 255.255.255.255 no-xauth no-config-mode*
17. Type *exit* to quit from configuration mode.
18. Type *write mem* to save the configuration into flash memory.

From the VPN configuration page in the PDM:

1. Under Categories, Click on IKE -> Policies and click on Add to add new IKE policy. Enter 10 as Priority. Choose pre-share as Authentication, 3des as Encryption, 2 as D-H Group, md5 as Hask and 86400 seconds as Lifetime. Click OK.

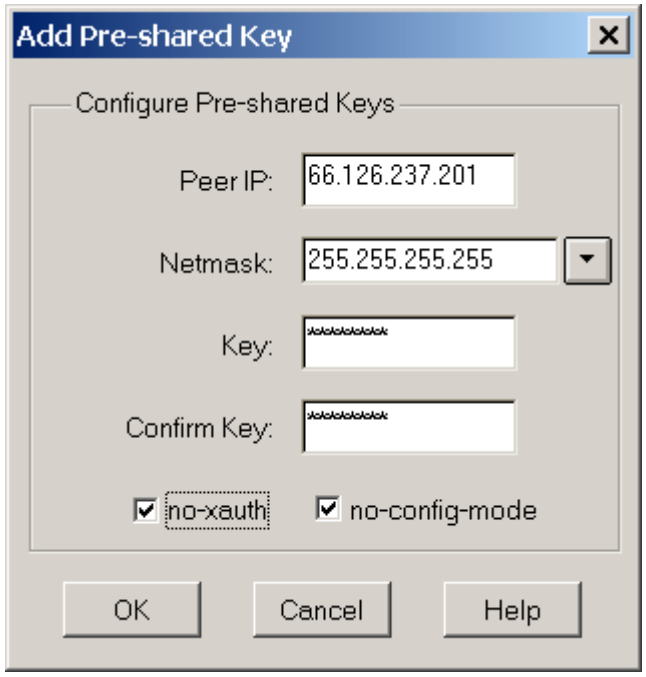


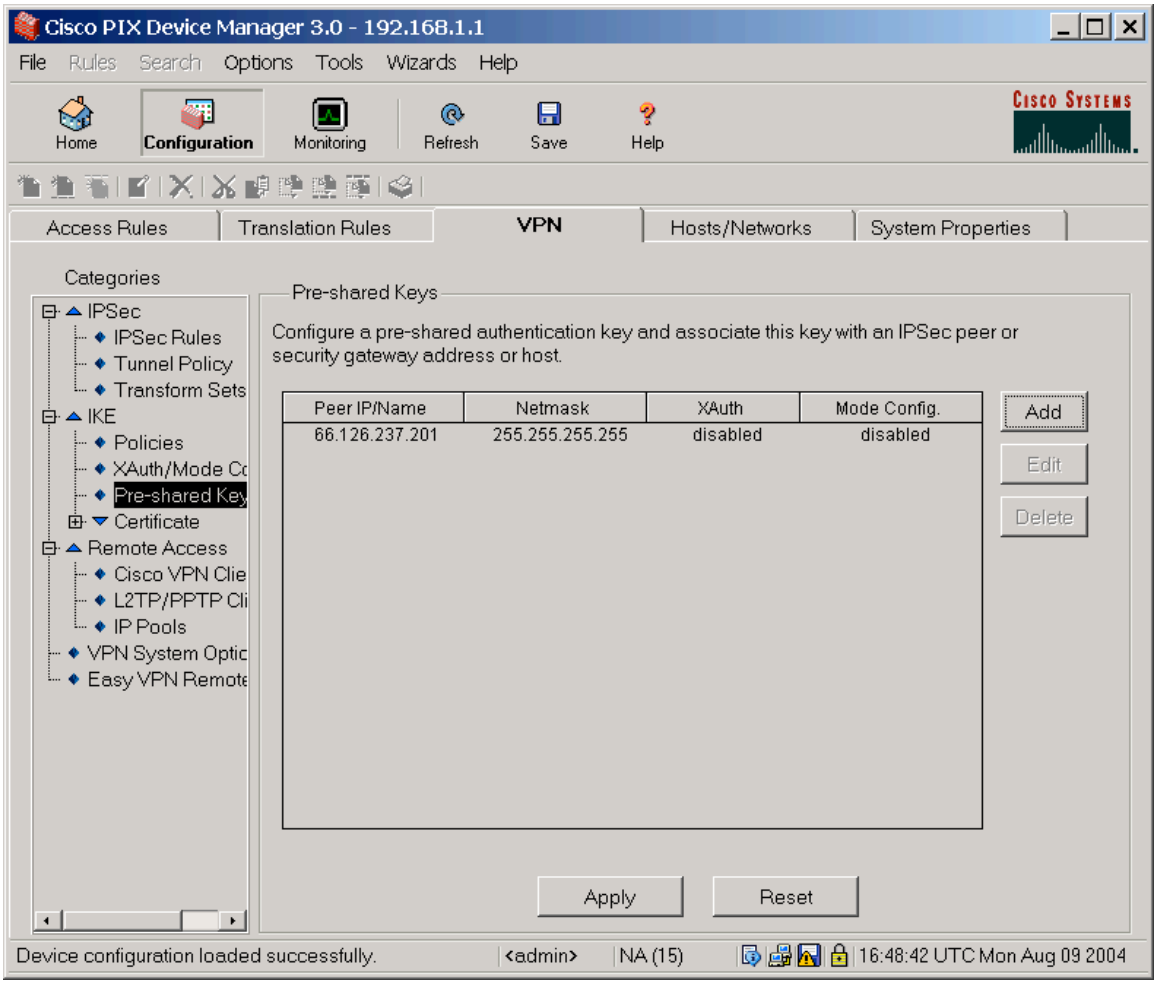
Under General information, highlight outside interface and click Enable.



Click Apply.

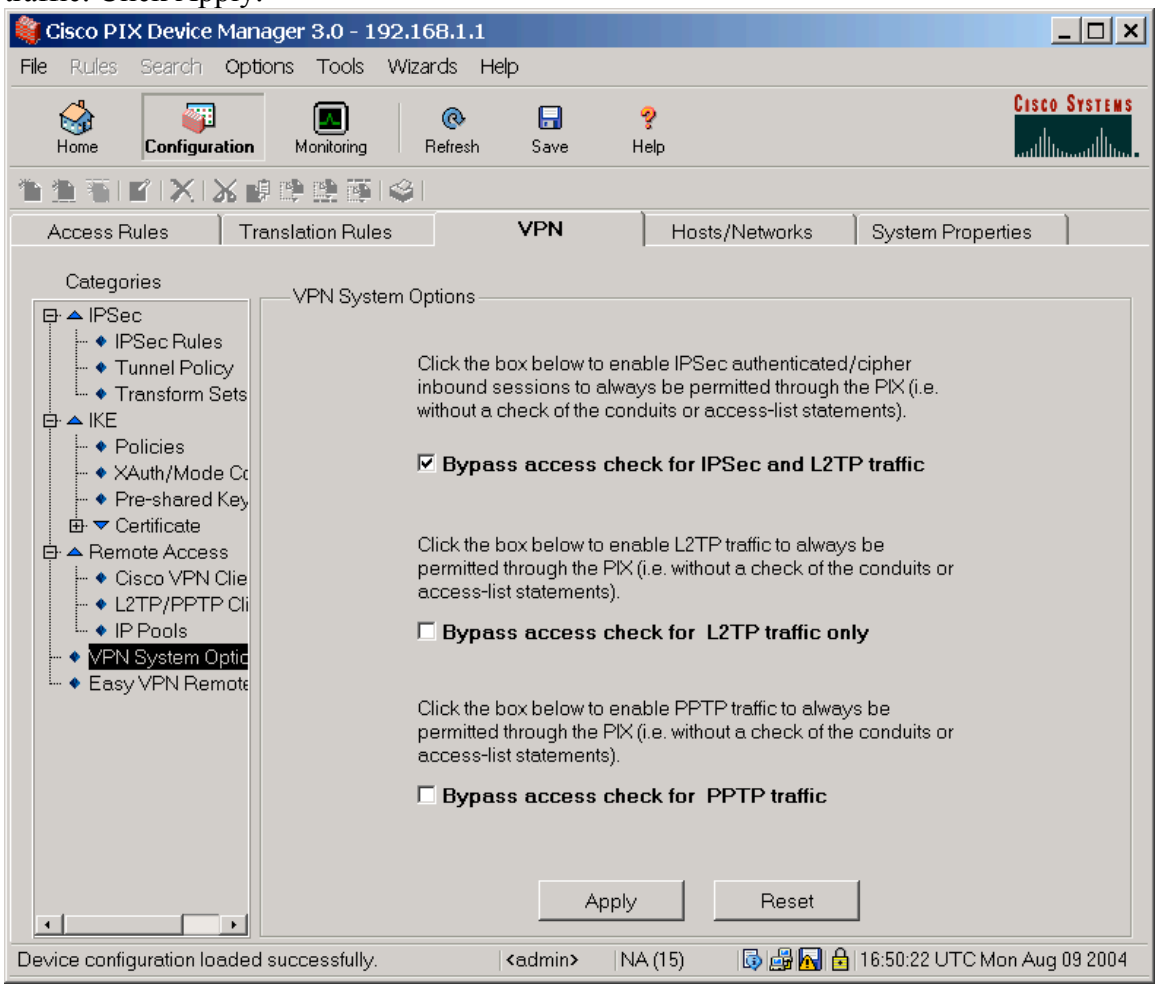
2. Choose Pre-shared Key under IKE. Click Add to add a new pre-share key. Enter 66.126.237.201 as Peer IP, 255.255.255.255 as Netmask, enter the pre-share key twice and check both the box for no-xauth and no-config-mode. Click OK.



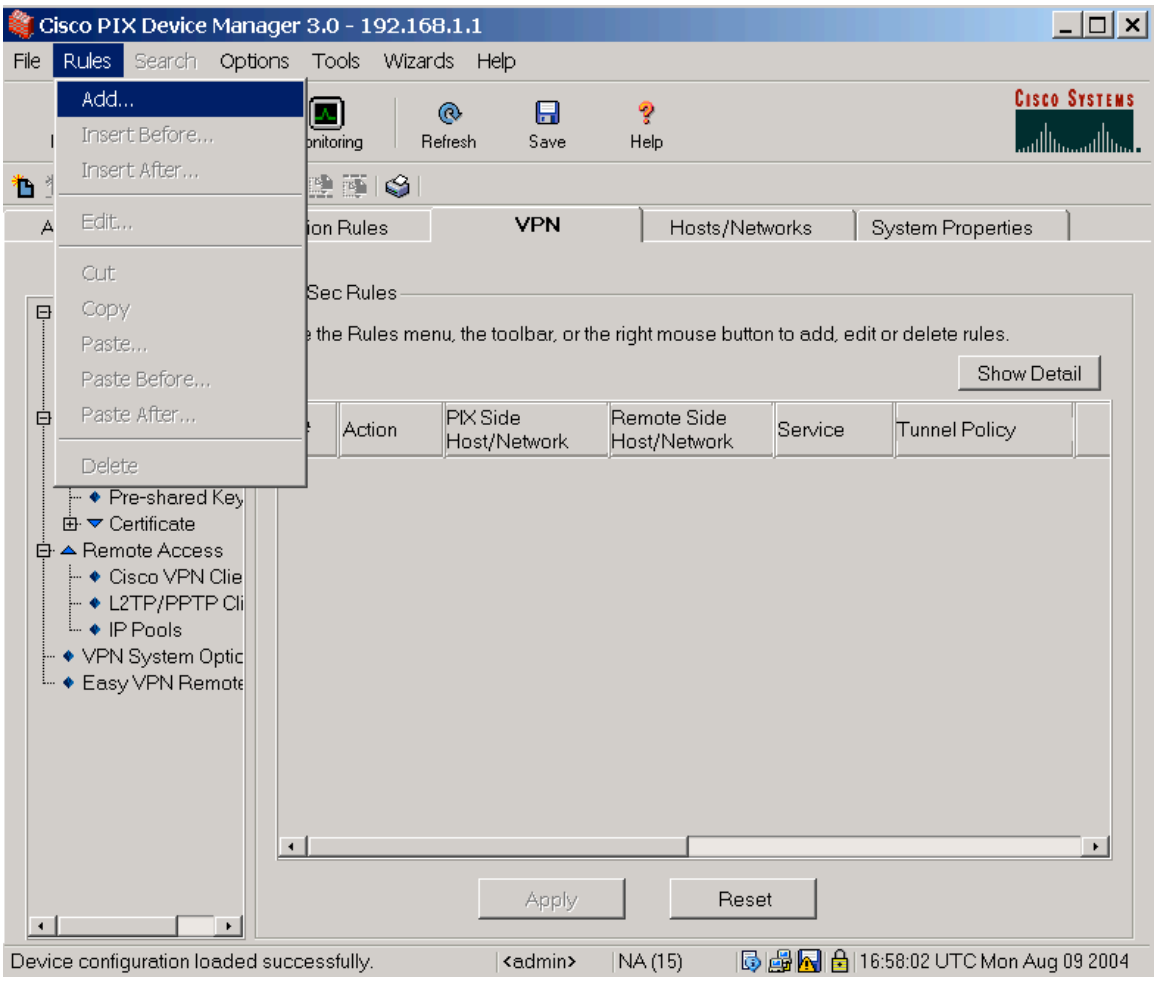

Cisco PIX Device Manager 3.0 - 192.168.1.1
File Rules Search Options Tools Wizards Help
Home Configuration Monitoring Refresh Save Help
Cisco Systems
Access Rules Translation Rules VPN Hosts/Networks System Properties
Categories
IPSec
IPSec Rules
Tunnel Policy
Transform Sets
IKE
Policies
XAuth/Mode Co
Pre-shared Key
Certificate
Remote Access
Cisco VPN Clie
L2TP/PPTP Cli
IP Pools
VPN System Optic
Easy VPN Remote
Pre-shared Keys
Configure a pre-shared authentication key and associate this key with an IPSec peer or security gateway address or host.
Peer IP/Name
Netmask
XAuth
Mode Config.
66.126.237.201
255.255.255.255
disabled
disabled
Add
Edit
Delete
Apply
Reset
Device configuration loaded successfully.
<admin>
NA (15)
16:48:42 UTC Mon Aug 09 2004

Click Apply.

3. Choose VPN System Options, check Bypass access check for IPSec and L2TP traffic. Click Apply.

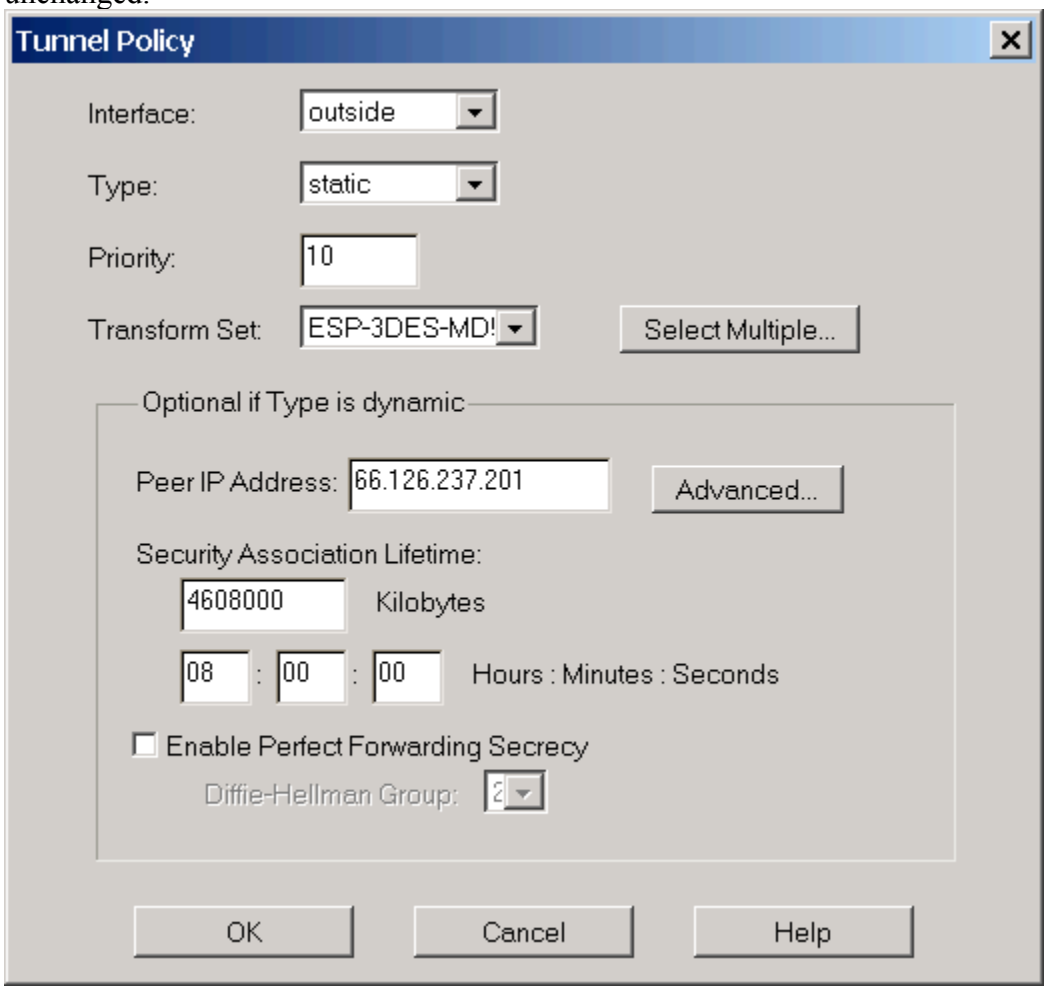


4. Highlight IPSec Rules under IPSec. Pull down the Rules menu and choose Add to add new IPSec Rule.

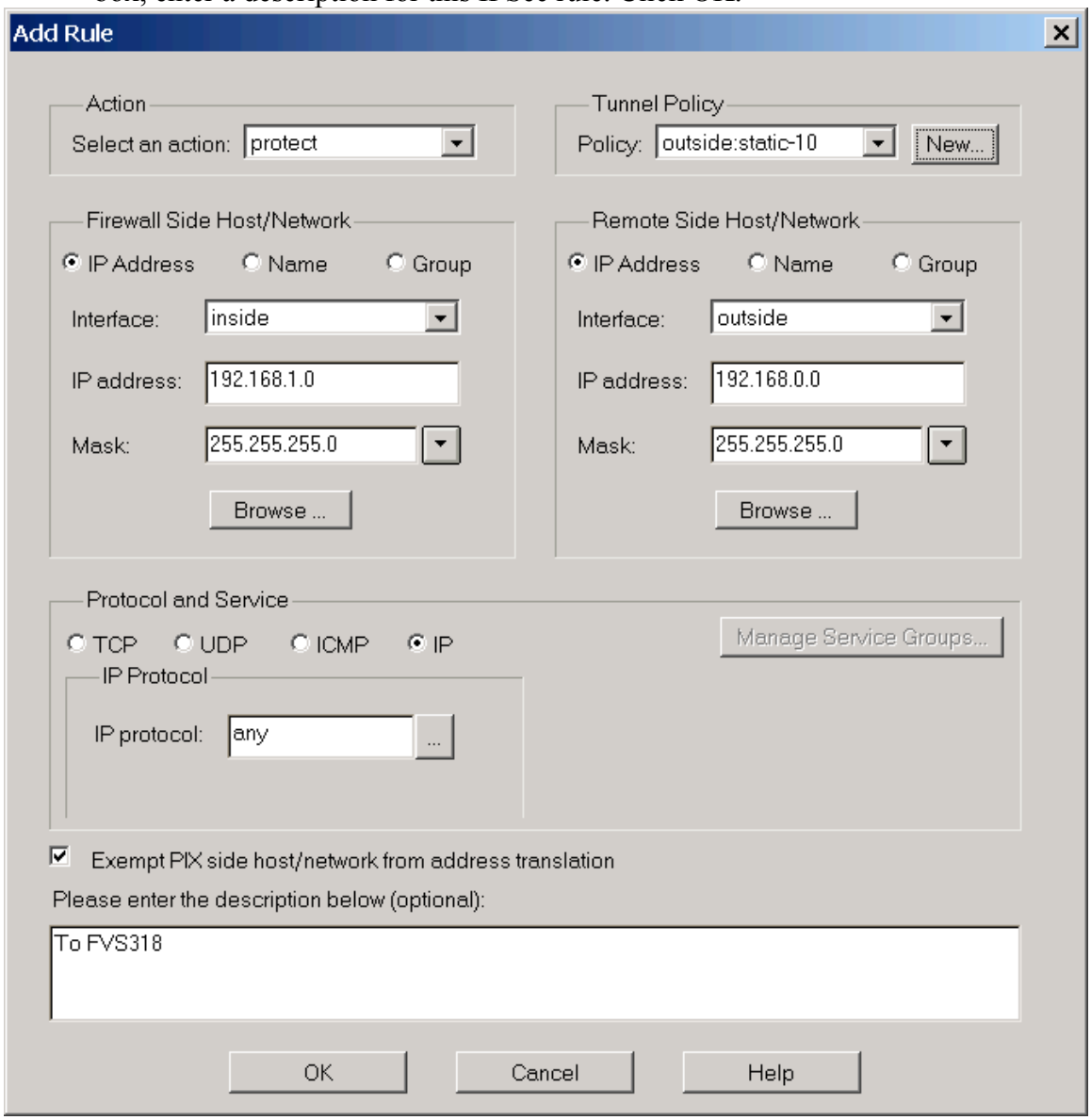


5. Click on the New button next to Tunnel Policy. Choose outside as Interface, choose static as Type, enter 10 as Priority, choose ESP-3DES-MD5 as Transform Set. Enter 66.126.237.201 as Peer IP Address and left the other parameter

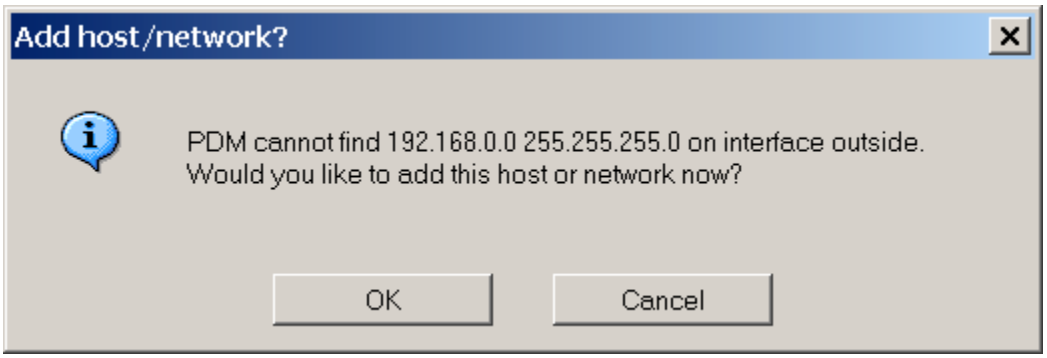
unchanged.


Tunnel Policy
Interface:
outside
Type:
static
Priority:
10
Transform Set:
ESP-3DES-MD!
Select Multiple...
Optional if Type is dynamic
Peer IP Address:
66.126.237.201
Advanced...
Security Association Lifetime:
4608000
Kilobytes
08
00
00
Hours : Minutes : Seconds
Enable Perfect Forwarding Secrecy
Diffie-Hellman Group:
OK
Cancel
Help

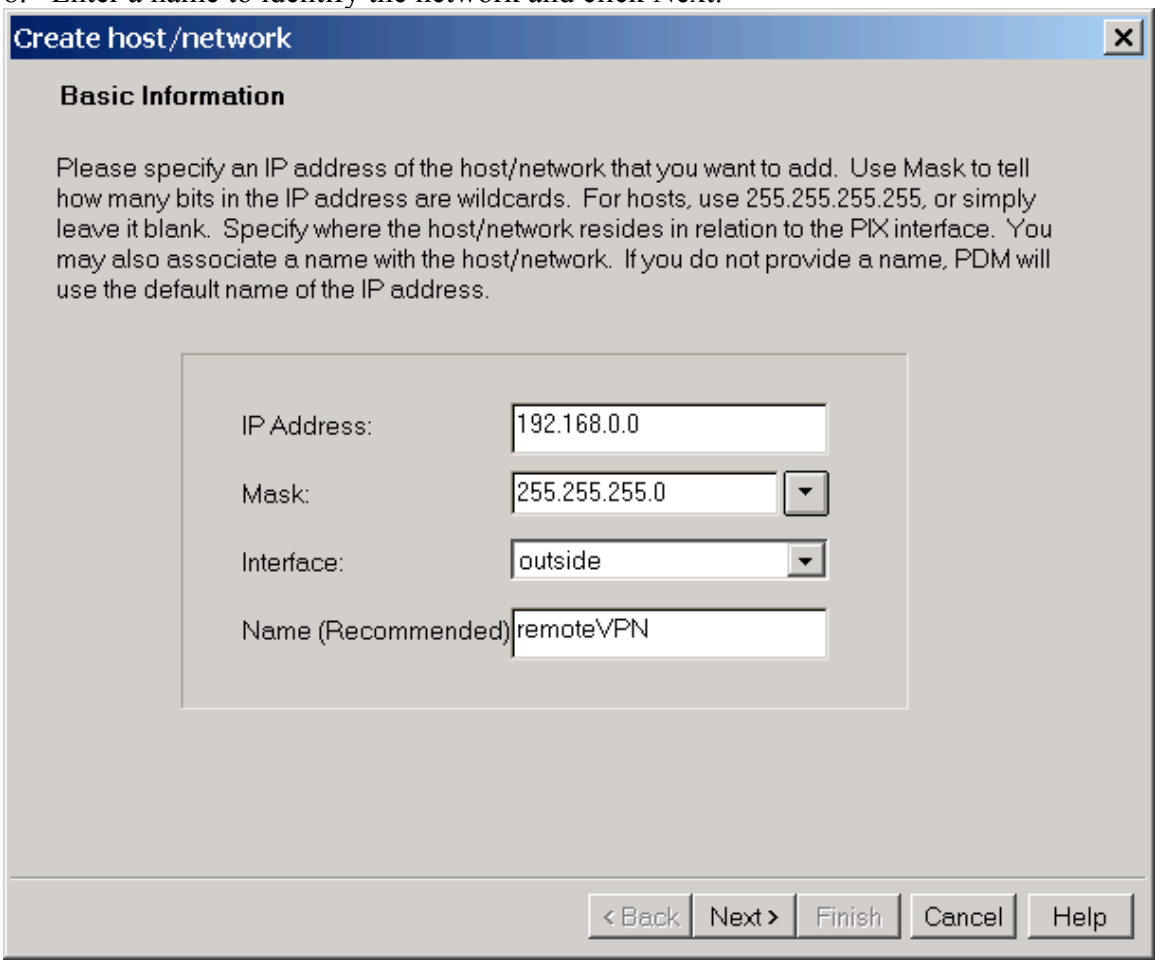
6. Choose protect under Action. Under Firewall Side Host/Network, choose IP Address, choose inside as Interface, enter 192.168.1.0 as IP address and 255.255.255.0 as Mask. Under Remote Side Host/Network, choose IP Address, choose outside as Interface, enter 192.168.0.0 as IP address and 255.255.255.0 as Mask. Under Protocol and Service, choose IP and any as IP protocol. Check the box Exempt PIX side host/network from address translation. In the description box, enter a description for this IPSec rule. Click OK.



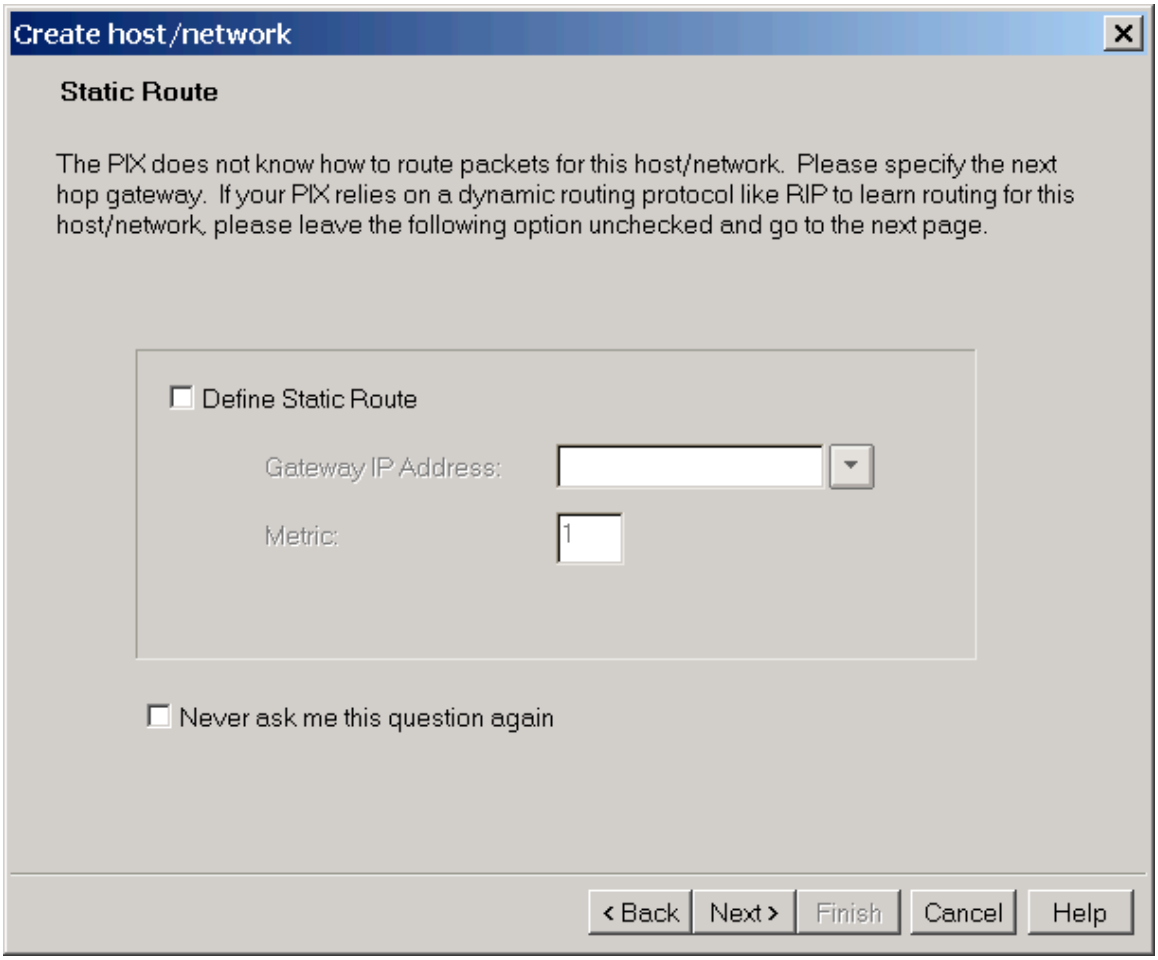
7. When ask to Add host/network, Click OK.



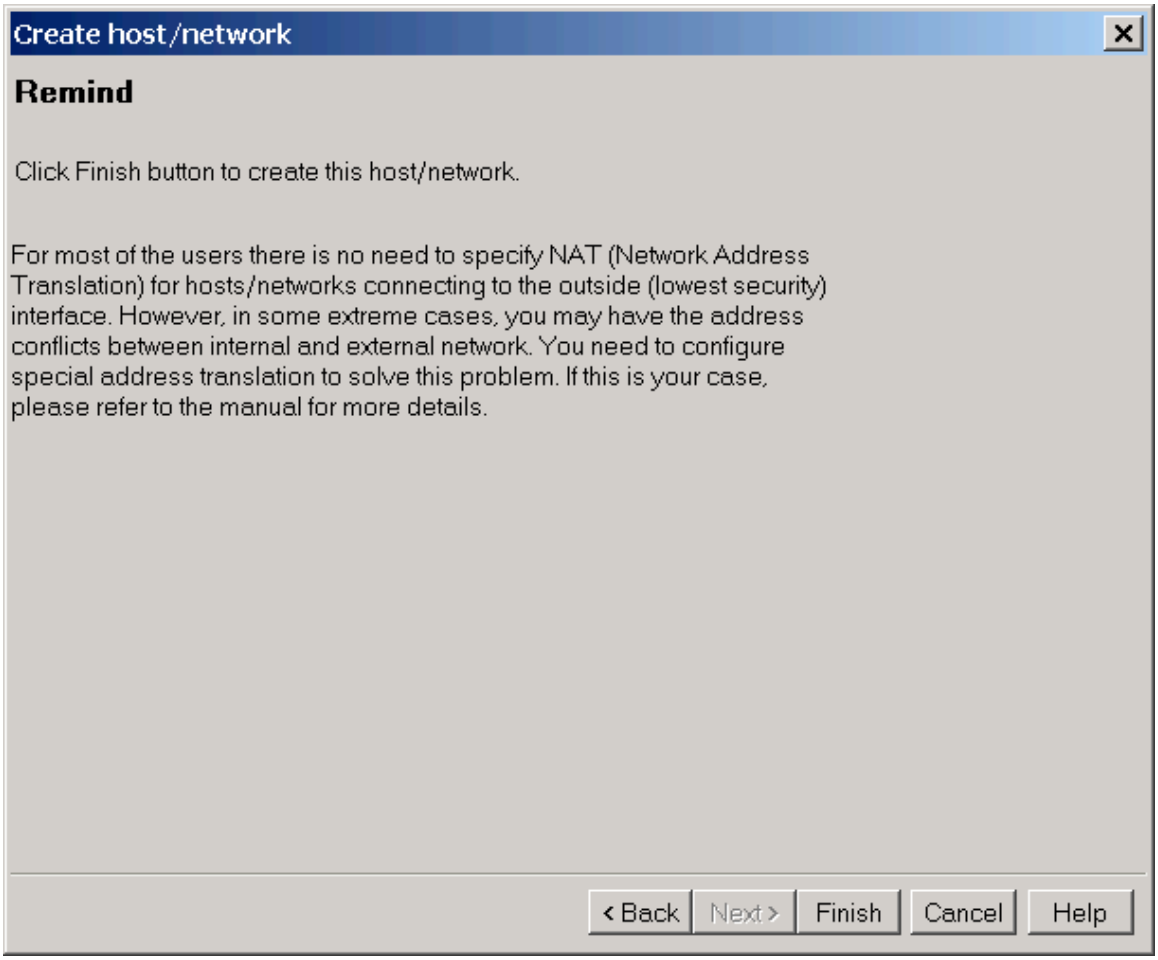
8. Enter a name to identify the network and click Next.



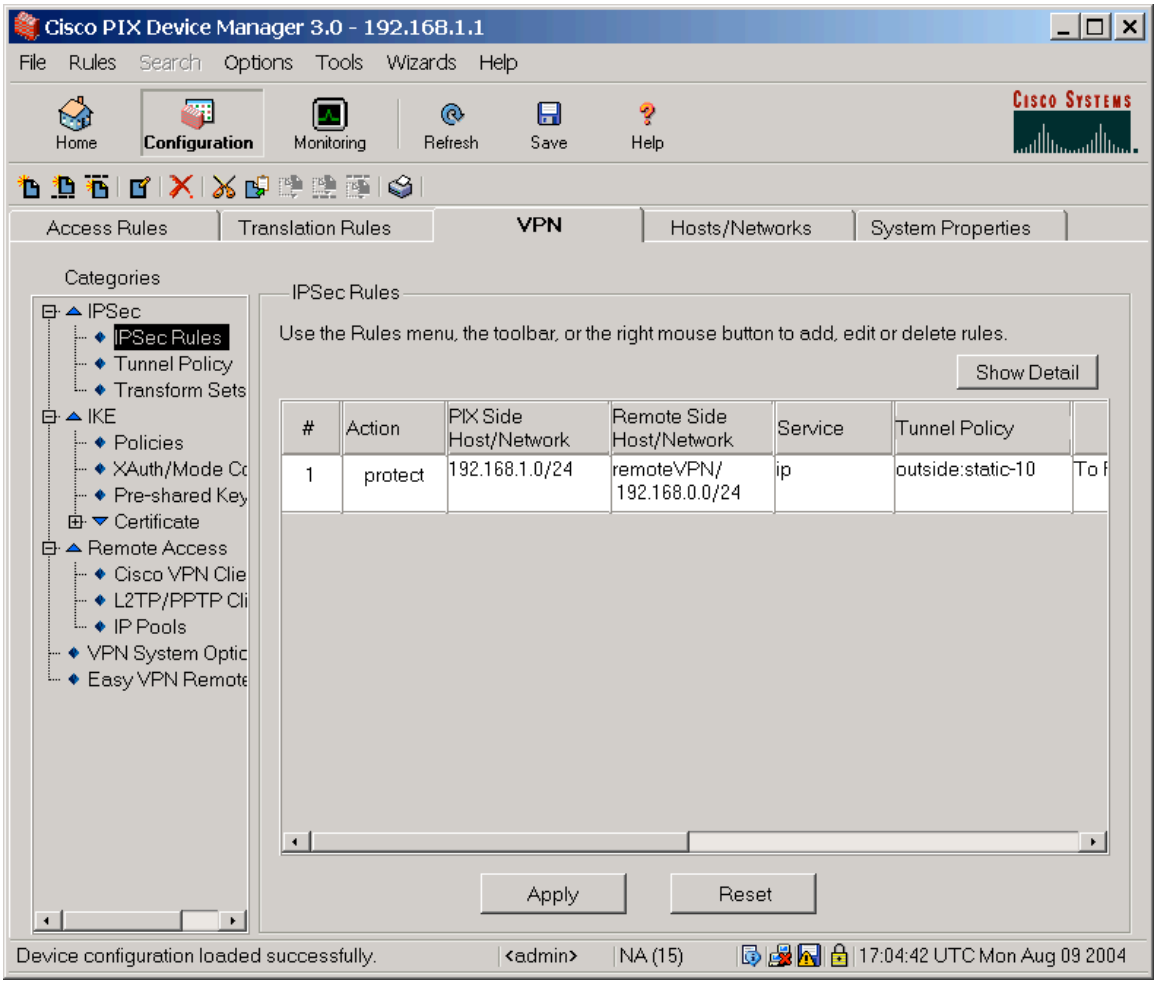
9. When ask about defining static route, just click Next.



10. Click Finish to finish creating network.

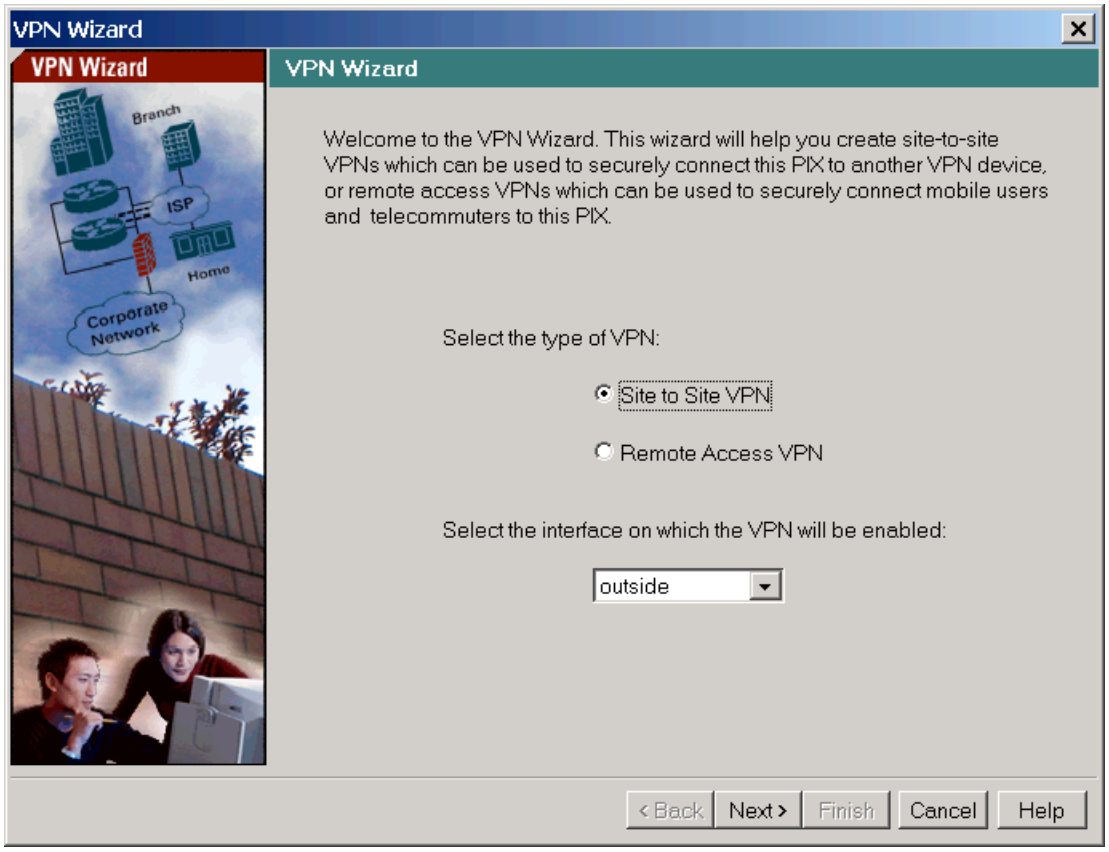


11. The IPSec Policy is created. Click Apply.

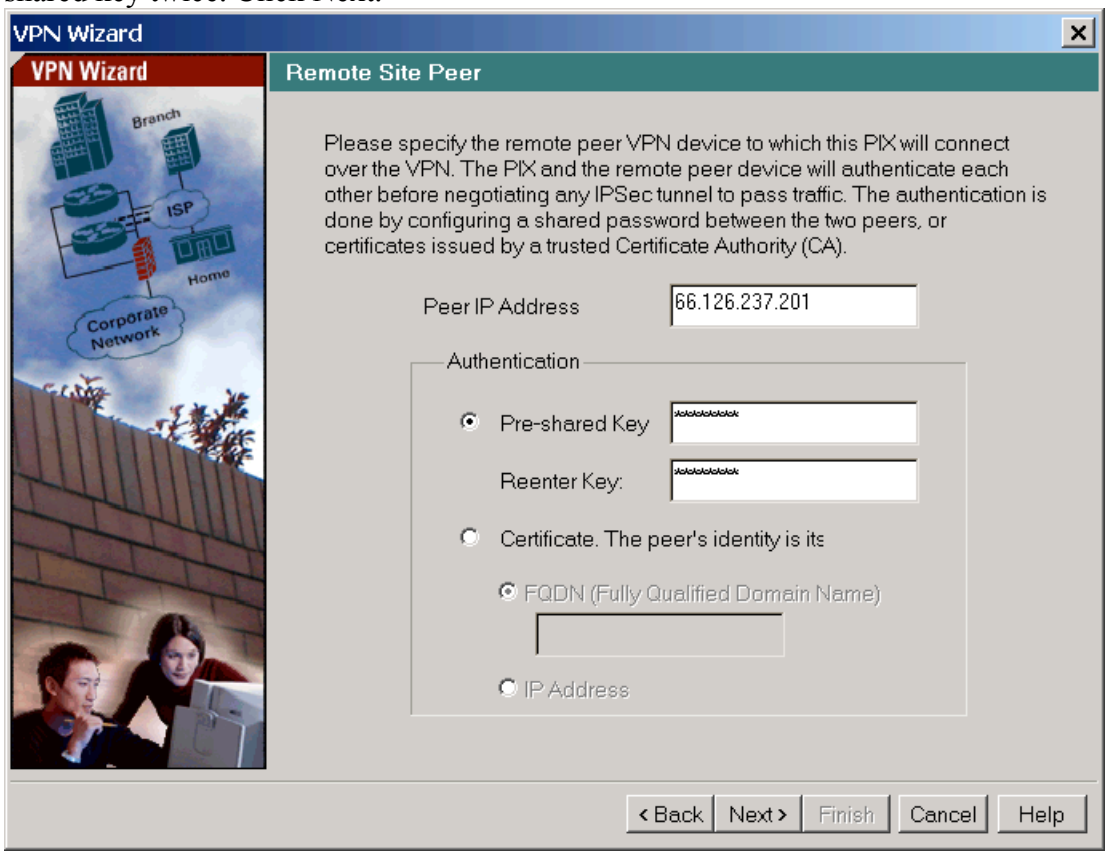


From VPN wizard in the PDM (choose VPN wizard from the Wizard pull down menu):

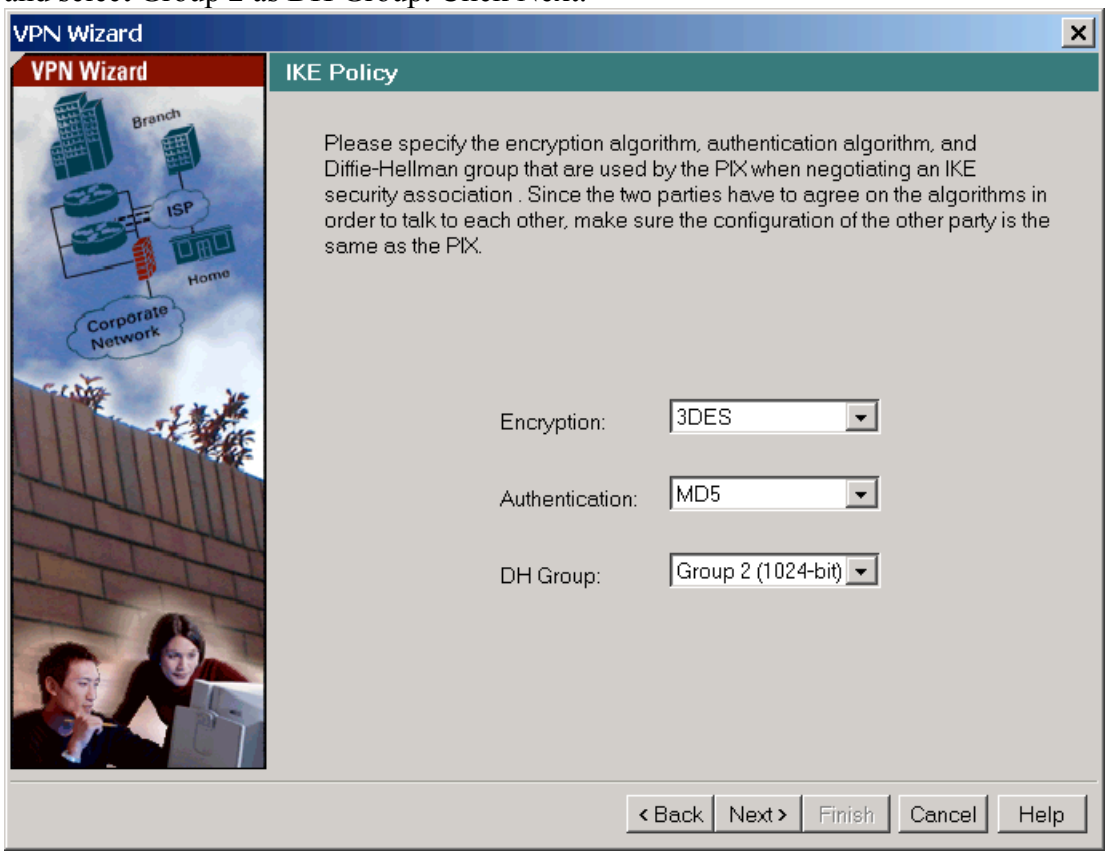
1. Select Site to Site VPN as type of VPN. Select outside as the interface on which the PVN will be enable.



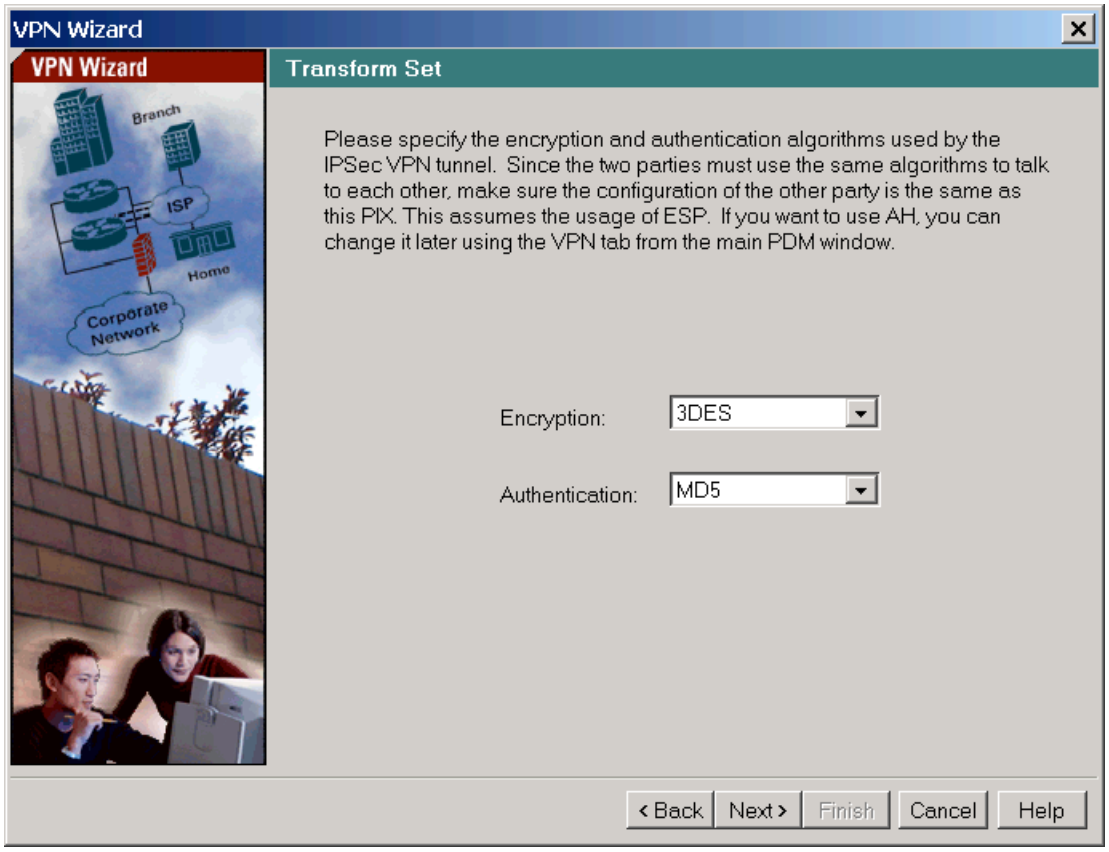
2. Enter 66.126.237.201 as Peer IP Address. Under Authentication, enter the Pre-shared key twice. Click Next.



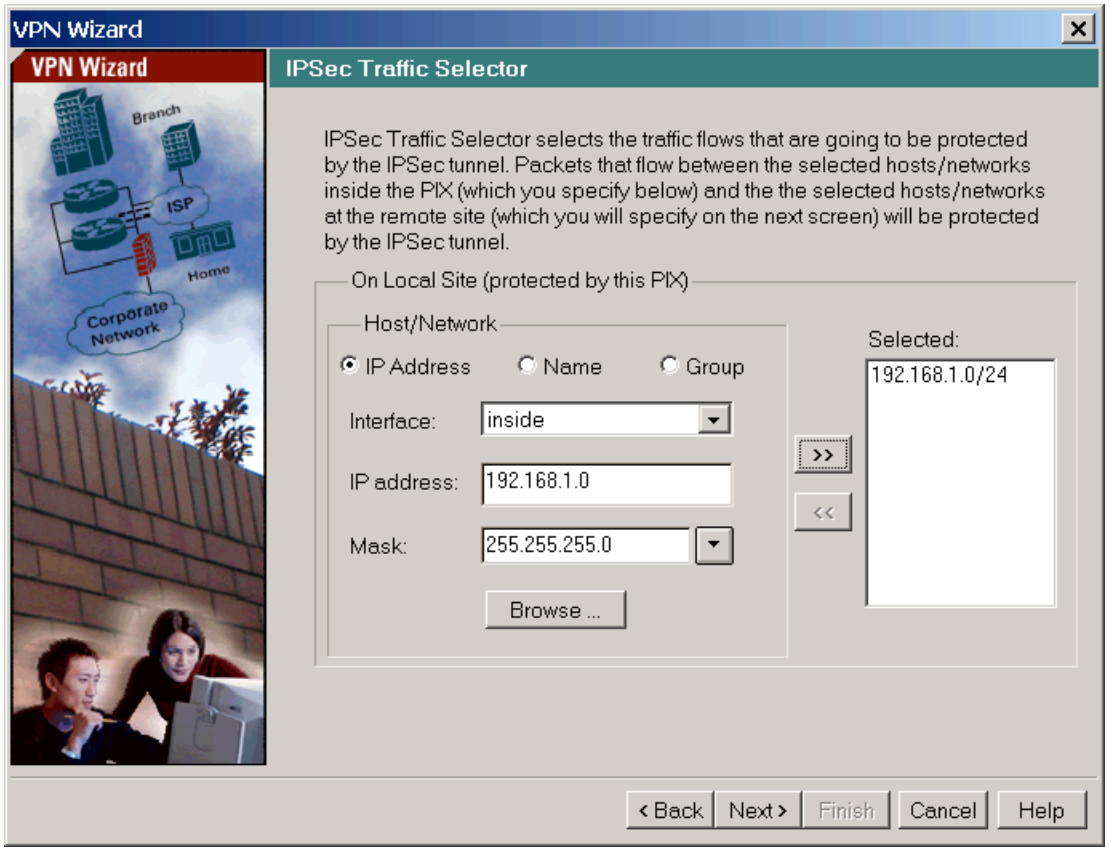
3. Select 3DES as Encryption algorithm, select MD5 as Authentication algorithm and select Group 2 as DH Group. Click Next.



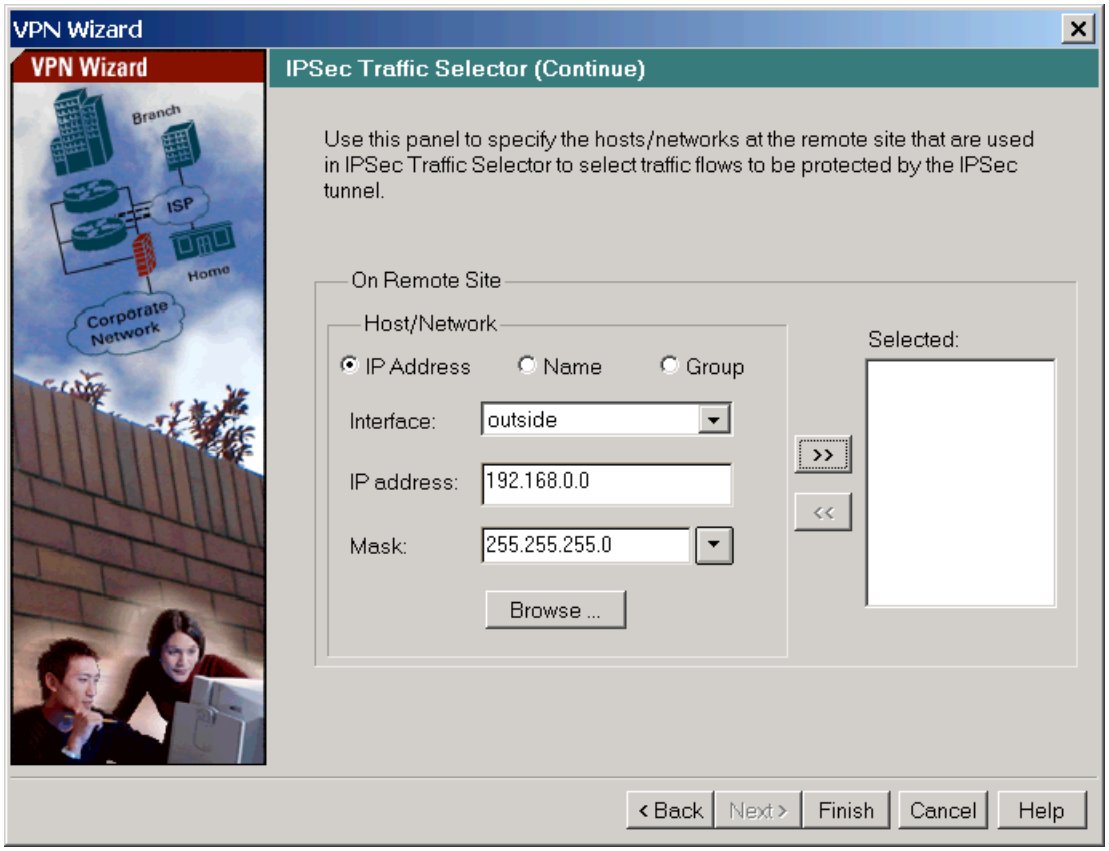
4. Select 3DES as Encryption algorithm. Select MD5 as Authentication algorithm. Click Next.



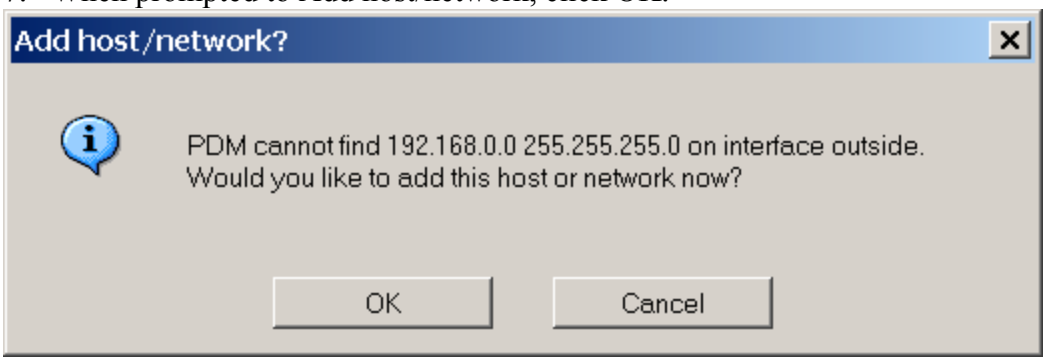
5. Select IP Address. Select inside as the interface. Enter 192.168.1.0 as IP address. Enter 255.255.255.0 as mask. Click on the >> button. Click Next.



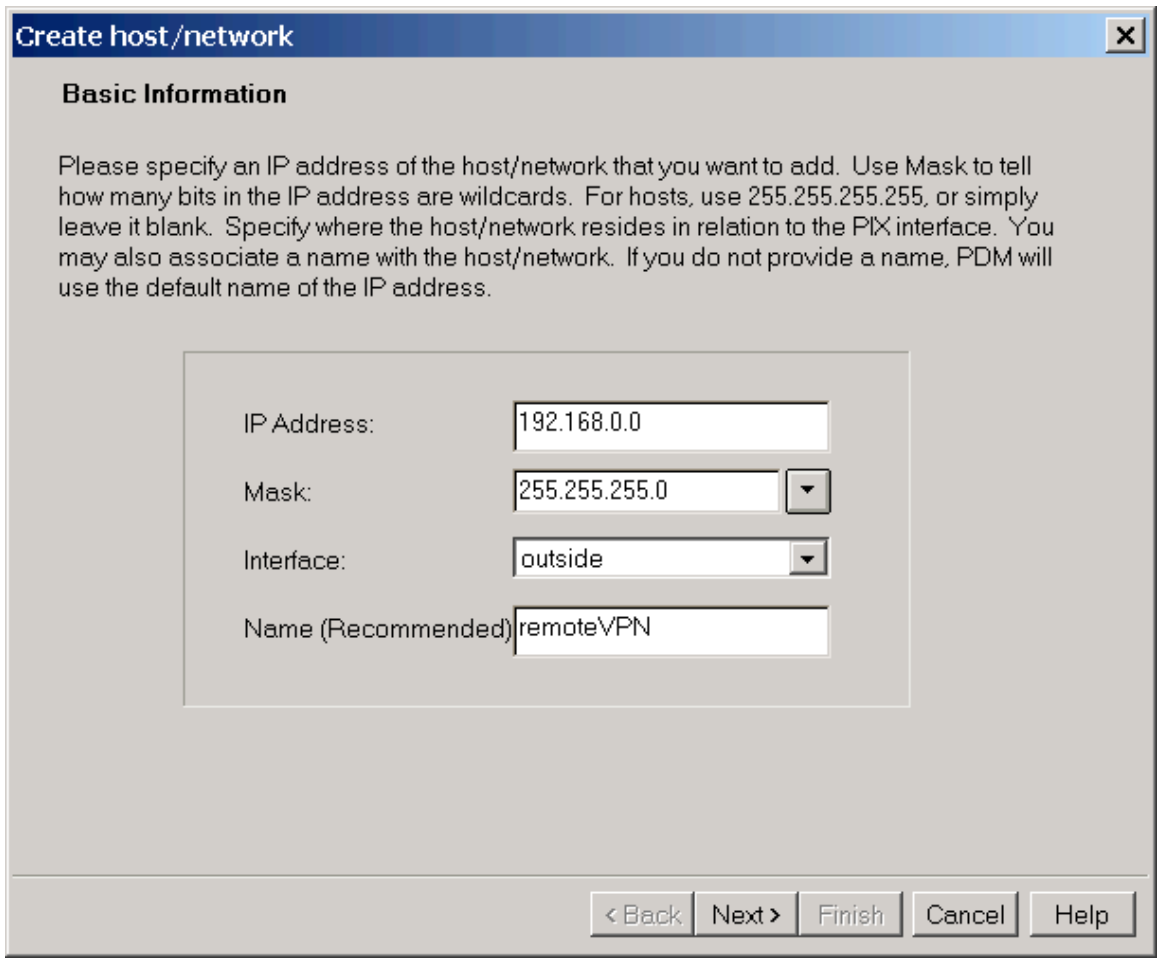
6. Select IP Address. Select outside as the Interface. Enter 192.168.0.0 as IP address. Enter 255.255.255.0 as Mask. Click on the >> button. Click Next.



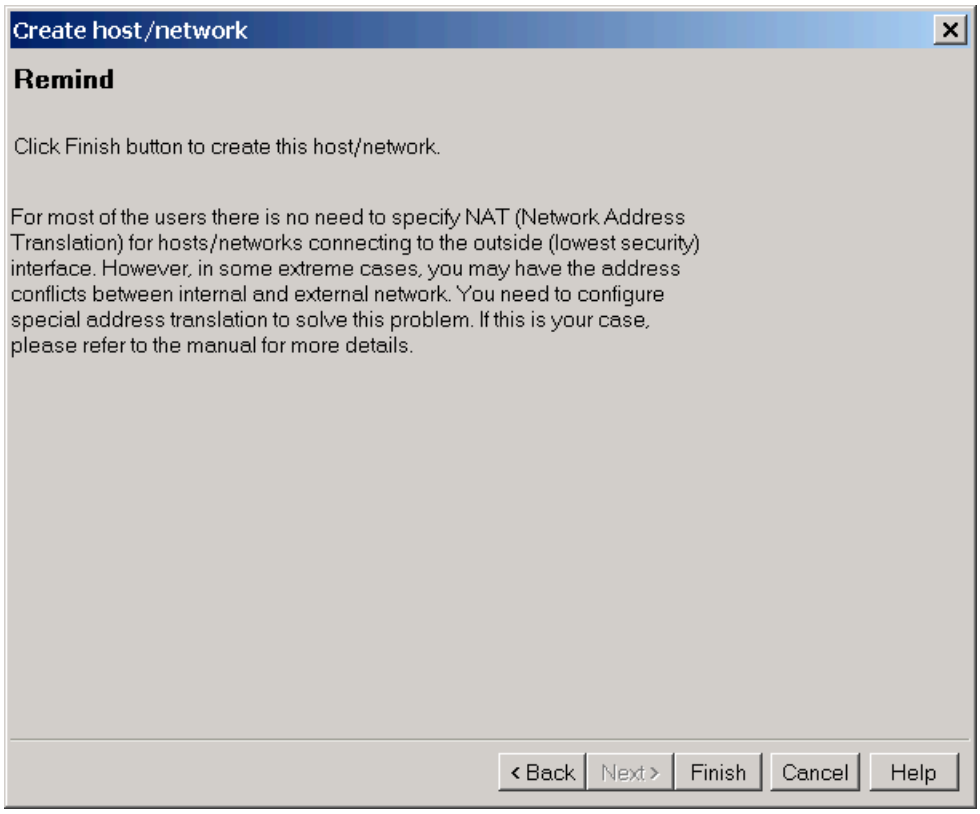
7. When prompted to Add host/network, click OK.



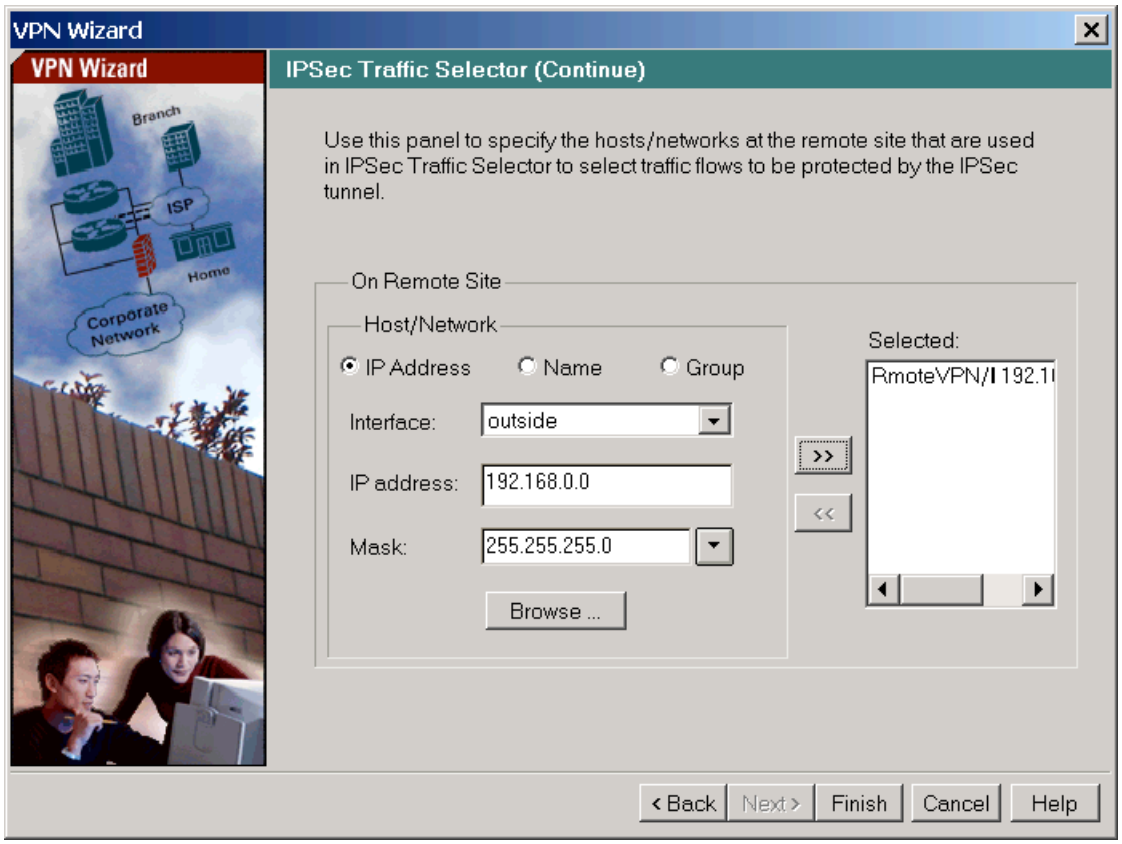
8. Enter a name for the new network. Click Next.


Create host/network
Basic Information
Please specify an IP address of the host/network that you want to add. Use Mask to tell how many bits in the IP address are wildcards. For hosts, use 255.255.255.255, or simply leave it blank. Specify where the host/network resides in relation to the PIX interface. You may also associate a name with the host/network. If you do not provide a name, PDM will use the default name of the IP address.
IP Address:
192.168.0.0
Mask:
255.255.255.0
Interface:
outside
Name (Recommended):
remoteVPN
< Back
Next >
Finish
Cancel
Help

9. Click Finish to create the network.



10. Click Finish to create the VPN connection.



.

Troubleshooting