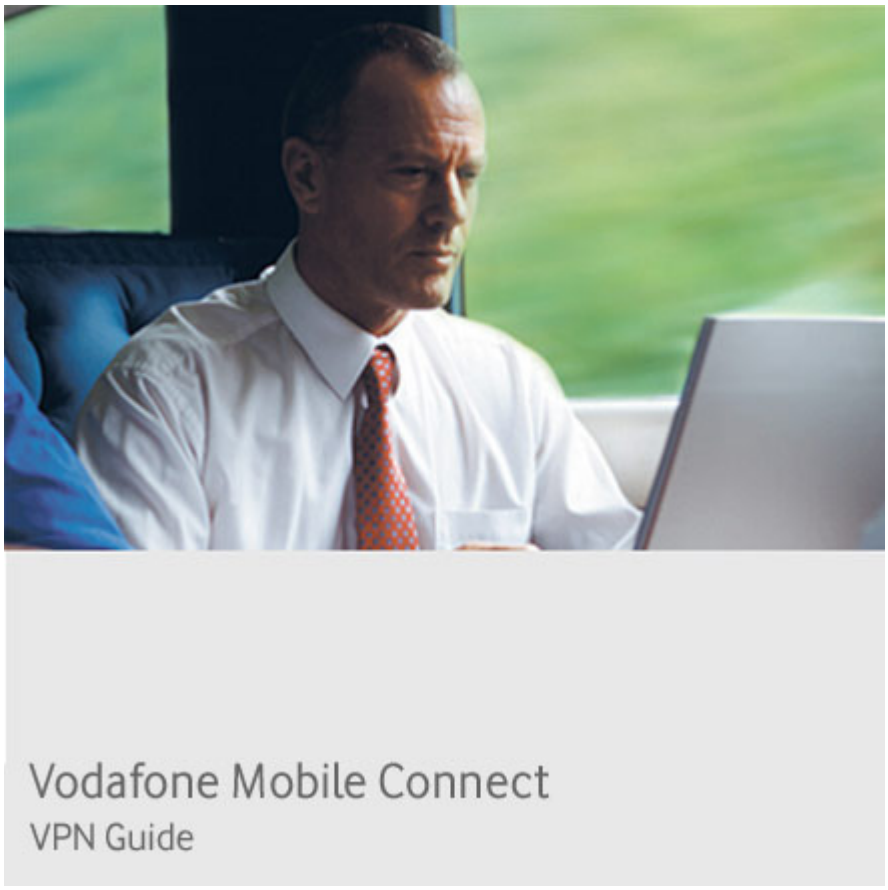
VPN End to End –Cisco PIX 501 Appendix

Appendix A: Cisco PIX 501

Technical Notes for use with Vodafone Mobile Connect services

Date: **3 May 2007**

Revision No: **3.0**



Scope

This document presents results of installation, configuration, and operations testing of VPN components with the Vodafone Mobile Connect service. The document is not intended to be a tutorial on VPN concepts nor does it supersede or replace the vendor's documentation. The reader is referred to the VPN vendor for definitive guidance on the proper and recommended use of their product. While Vodafone Group has taken care to ensure that the information contained herein is accurate, no responsibility can be accepted for errors, omissions, or inaccuracies.

Document History

Version	Date	Reason
1.0	October 2003	Initial release using GPRS network. Client documentation included in main document.
2.0	May 2007	Creation of separate document for client configuration. Update to new versions of VPN software and focus on 3G network performance.
3.0	May 2007	Final edits for web publication.

File Reference

VPN - Cisco ASA5510_Appendix_A_Concentrator.doc

Document Authors

Joerg Pfeffer, TECON Terenci
Peter Jaeger, TECON Terenci
Miroslaw Grzesica, TECON Terenci

Document Distribution

Public via websites of Vodafone, its Affiliates, and its Partner Networks

Contents

Tables & Figures

Nil

1 Executive summary

This Appendix is in addition to the detailed document for Cisco PIX 501 VPN Concentrator and describes the setup and update process in a detailed way with example screen shots taken from the initial processes.

Furthermore logging and additional functionality is available in the appropriate chapters.

2 Cisco PIX 501 Installation and Configuration (6.3)

The following description is intended for network administrators who are familiar with networking and IP concepts. The PIX has to be integrated into the internal company network. The PIX setup therefore has to comply with the configuration of the internal networking. This description is intended to allow a network administrator not yet familiar with the CISCO PIX to configure a VPN with UMTS/GPRS usage. Since this document is only describing the VPN aspects of the PIX, no firewall setups are described and should be addressed separately.

2.1 Initial setup

After unpacking the PIX install the device in your office environment with connecting power supply, internal and external network connections. Connect your PC to the internal network and enable DHCP on it. The Cisco PIX will use the internal IP address 192.168.1.1/24 and assign client IP addresses via DHCP.

2.2 Using the web-based Concentrator manager

Use a web browser to contact the PIX's internal address (https://192.168.1.1). Make sure to use https, not http. The PIX Device Manager requires one of the following browsers:

- A JavaScript and Java enabled browser. If these are not enabled in the browser, PDM guides you through how to enable them. PDM uses the native Java Virtual Machine (JVM) in your browser. It does not use the Java browser plug-in. (However, if you have the Java plug-in, it can remain installed with your browser, but it cannot be your default JVM. If you have the Java plug-in and cannot run PDM, refer to the troubleshooting matrix in Chapter 3, "Troubleshooting.")

- If you are using Microsoft Internet Explorer, be sure to use JDK Version 1.1.4. To check which version you have, launch PDM. In the main PDM menu, click Help>About Cisco PIX Device Manager. When the About PDM information window appears, it displays your browser specifications in a table, including your JDK version. If you have an older JDK version, you can get the latest JVM from Microsoft by downloading the product called Virtual Machine.

Make sure JavaScript and Java are enabled and popup windows are allowed.

Note the following when using PDM to access the PIX Firewall unit:

- *Minimum Disk Space Requirement*—PDM requires a minimum of at least 4 MB of temporary disk space to load into the browser.

- *Java Virtual Machine (JVM)*—PDM supports the native Internet Explorer JVM from Microsoft, and the native Java Development Kit (JDK), a Java Plug-in. PDM Version 3.0 supports the Java Plug-in 1.3.1, 1.4.0 and 1.4.1 (recommended). **Note:** Java Plug-in 1.4.0 includes some JVM bugs that cause it to display some error messages in the Java Console.

For best results, we recommend Internet Explorer. Whatever browser and version you use, install the latest patches and service packs for it.

If you are using Microsoft Internet Explorer, and it is necessary to disable the Java Plug-in for your configuration, perform the following steps:

1. Click Tools>Internet Options.
2. Click the Advanced tab.
3. In the Java (Sun) section, clear the Use Java 2 check box.

If you are using the Java Plug-in and accessing your PIX Firewall using an IP address instead of a host name, the performance of PDM is dramatically slower. This occurs if the PIX Firewall host name is not in DNS or in the local hosts file.

The workaround is to assure that the PIX Firewall host name is in DNS. If you are running Windows, and there is no DNS in your network or your DNS does not have the PIX Firewall entry, modify the “hosts” file.

- On Windows NT, 2000, and XP, the hosts file is located at C:\WINNT\system32\drivers\etc\hosts.
- On Windows 98 and ME, it is at C:\Windows\hosts.

Each line in the hosts file is in the format “<ip> <hostname>”. For example:

```
192.168.1.1 pixfirewall.example.com
```

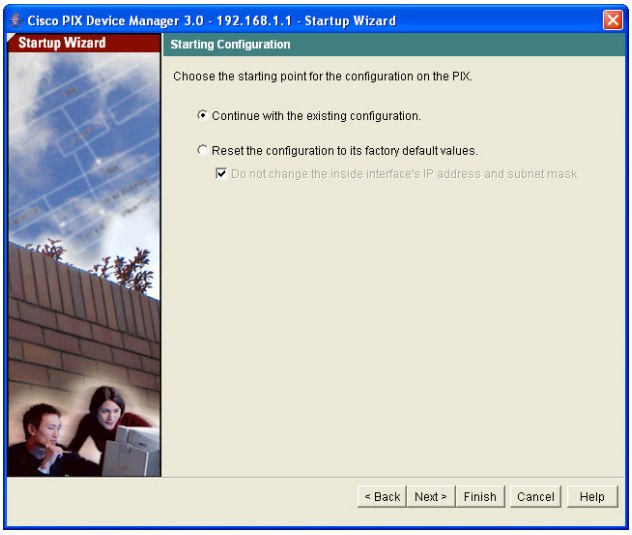
2.3 Basic settings

The first connection to the PIX is done via the Start-up Wizard. Open the web page https://192.168.1.1/startup.html to enter the Start-up Wizard.

Accept the certificate when the browser asks the respective dialog box.

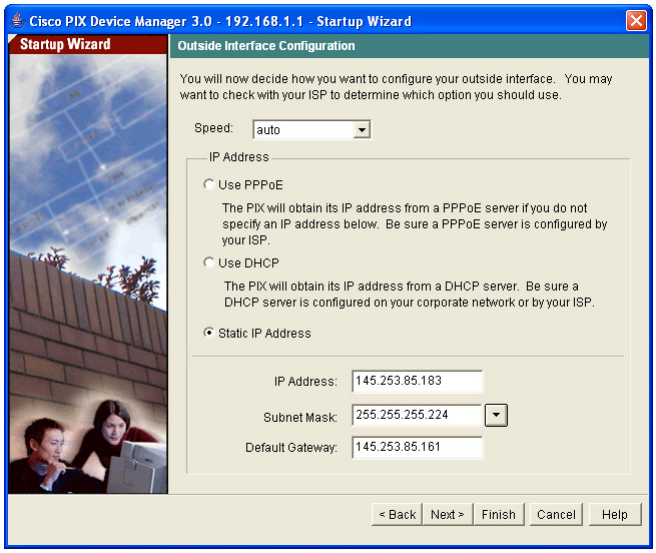
In the following authentication dialog, just click <Enter> to continue. Later, you must enter the configured admin user name and password here.

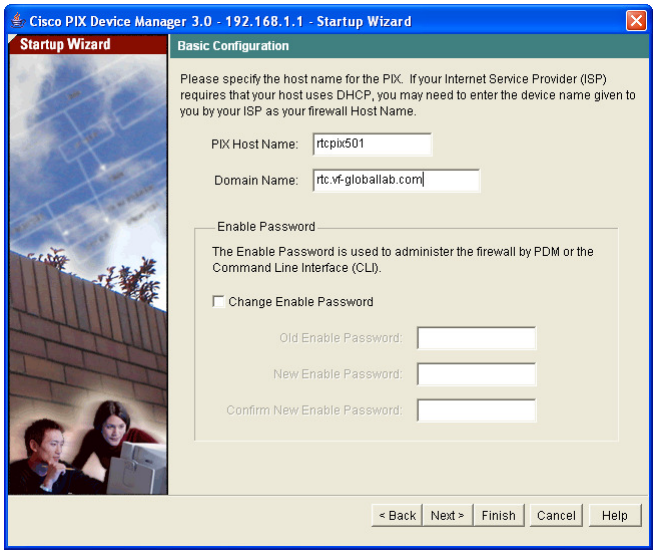
The Startup Wizard will open. Click <Next>.



In the following screen, you can select whether you want to continue with the previously setup configuration or if you want to start with the factory defaults. If you select “factory default”, the machine resets and you will need to start again until you come to this screen again.

Therefore, select “Continue” and click <Next>.

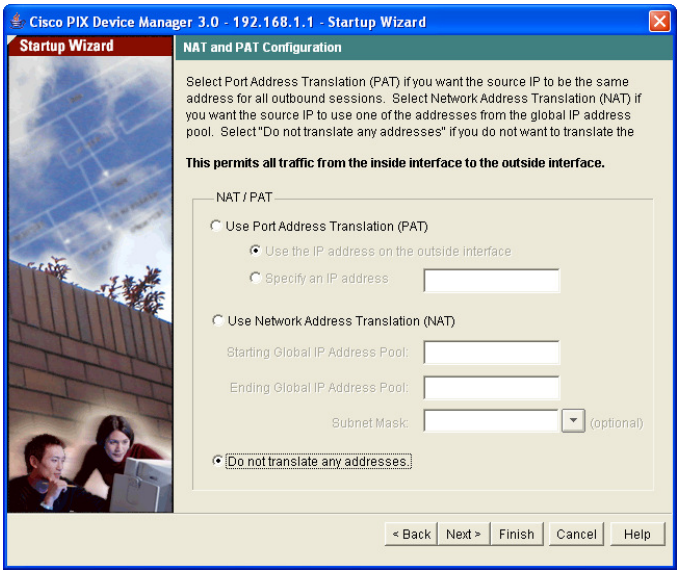


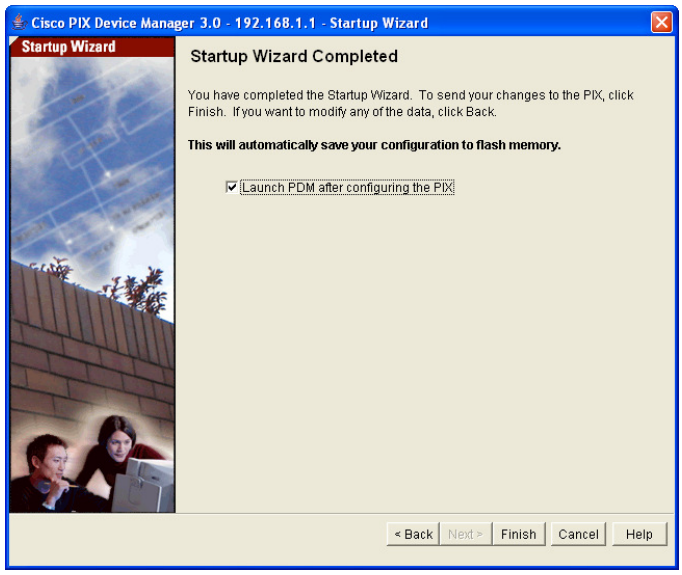


Enter the host name and domain at this point and click <Next>. Now configure the outside interface of the firewall. IP address and network parameters depend on your network setup. For client access, make sure the machine can be accessed from the outside via a fixed IP address or URL.

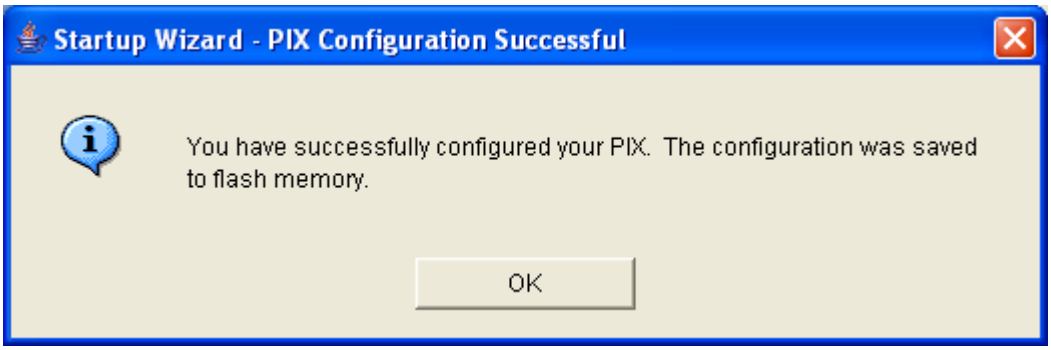
Do not enable Easy VPN Remote. Just click <Next>. Auto Update is also not configured. Just click <Next>.

The next screen shows an overview of the PIX interfaces. You may configure all interfaces **except** the one you are connected to (“inside”). Click <Next> when finished.





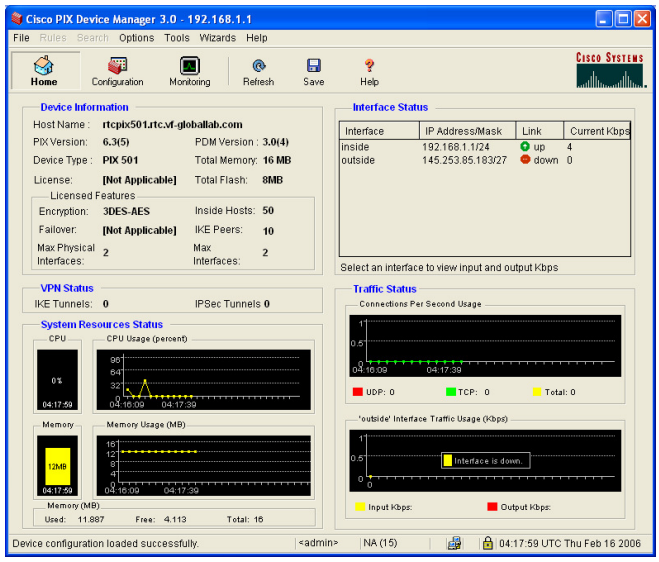
We don't need NAT/PAT for clear text packets at this point. Select "Do not translate any address" and click <Next>. Select "Launch PDM" in the following screen and click <Finish>. This concludes the Startup Wizard.



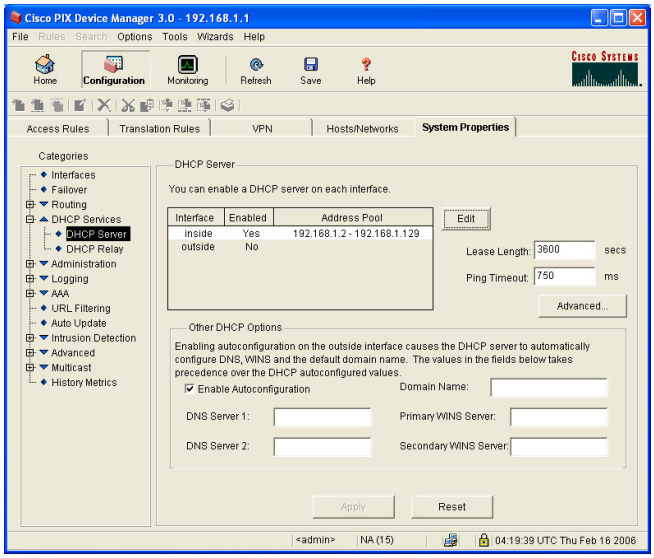
Next, the status screen of the PDM will open.

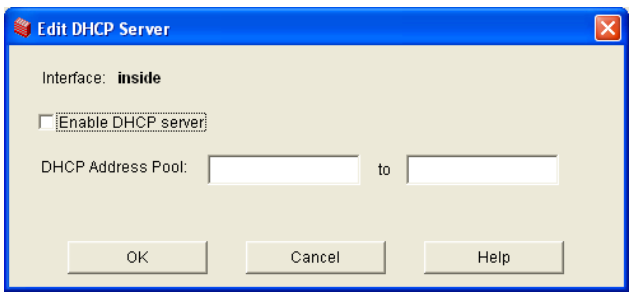
2.3.1 Changing the inside interface

Click on the <Configuration> button in the tool bar. There, change to the “System Properties” tab.



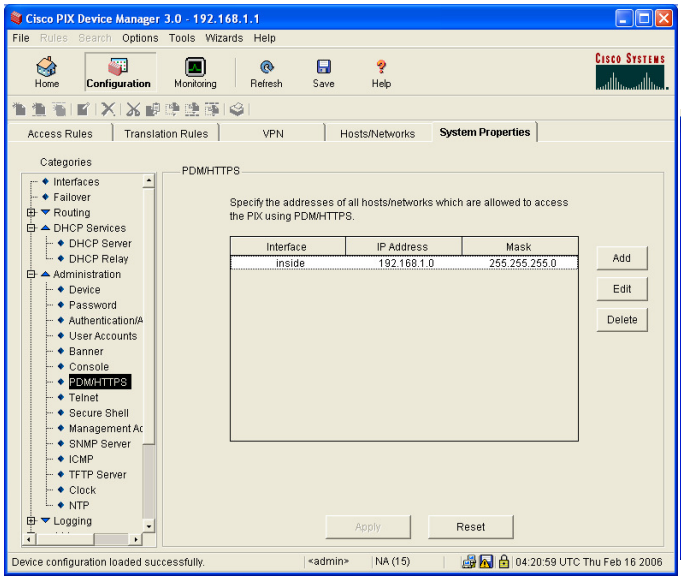
In the categories tree, select “DHCP Services > DHCP Server”. Here you can disable the DHCP address pool, which needs to be removed before the internal address can be changed. Select “inside” interface and click <Edit>. Deselect the “Enable DHCP server” box and remove the pool addresses. Click <OK>. In the previous screen, click <Apply> to download the changes to the PIX.

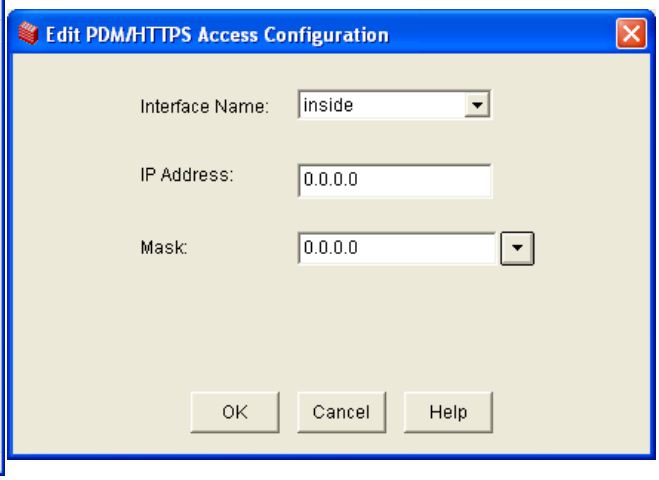




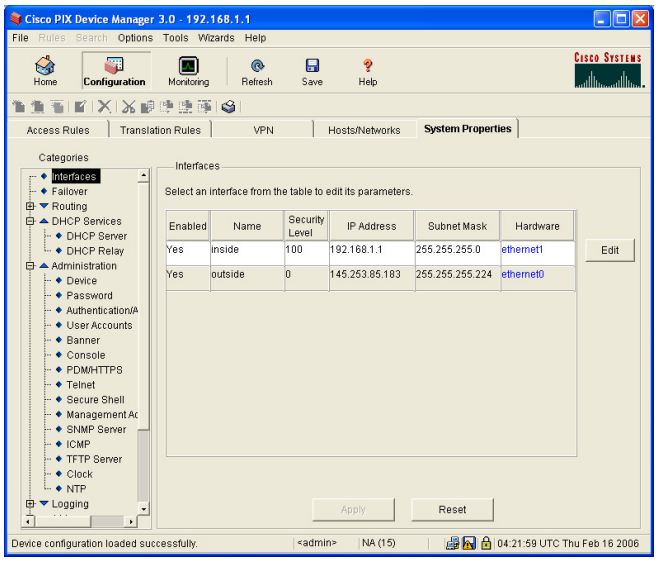
Next, select “Administration>PDM/HTTPS” in the categories tree. Before changing the inside interface IP address, you need to allow access to the PDM from other IP ranges. Otherwise, the machine will no longer be manageable via PDM. select the “inside” interface and click <Edit>. In the following dialog box enter IP address and mask 0.0.0.0,

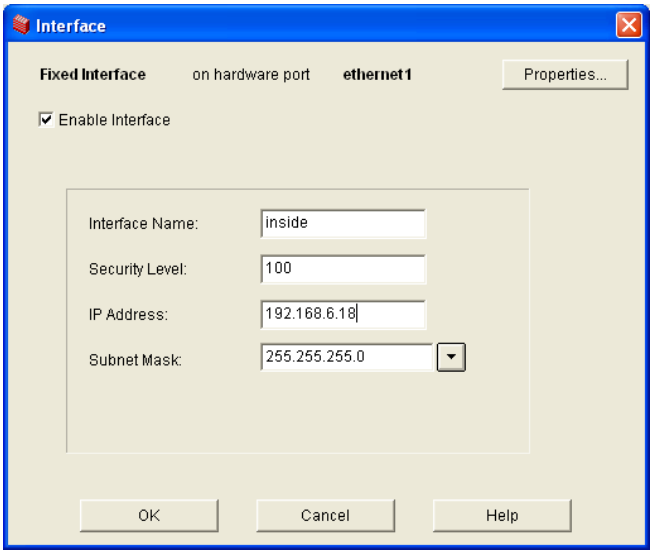
which will enable all addresses on the inside interface. Finish editing by clicking <OK>. After you returned to the previous screen, click <Apply> to download the changes to the PIX.



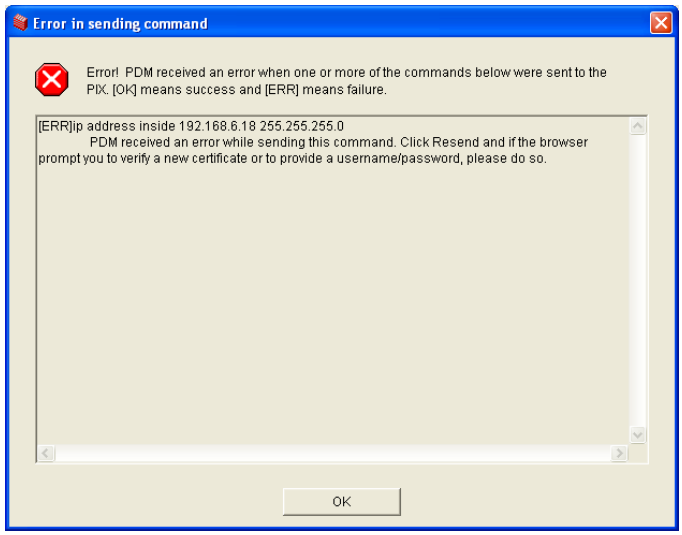


Now, select “interfaces” in the categories tree. The available interfaces are listed. Now, the internal IP address can be changed. Select the “inside” interface and click <Edit>.

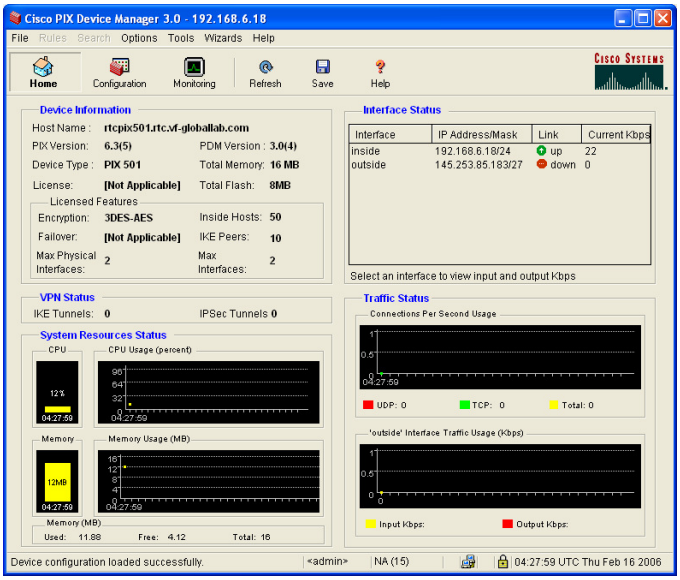




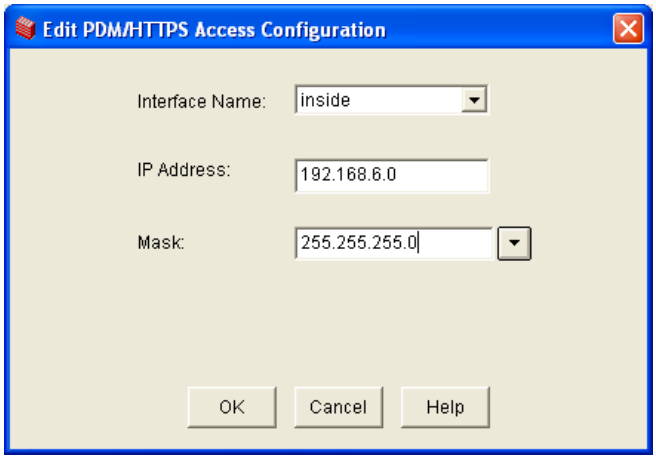
In the following Dialog box, enter the new IP parameters for the inside interface. When finished, click <OK>. The changed IP parameters will be shown in the list but are not yet valid on the PIX. Only when you click <Apply>, the configuration will be stored on the PIX. Since the change will be immediate, you will no longer be able to access the PIX via PDM, which will be shown by a PDM error message. Do not switch off the PIX at this time; otherwise you will lose the configuration changes.

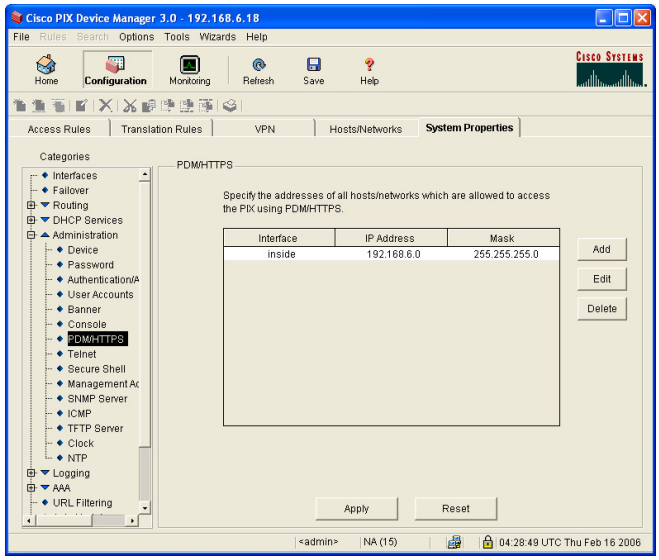


Nevertheless, the IP parameters were changed and the connection can be re-established by changing the client PC network setup to fit the IP parameters of the PIX. Then re-login via the new internal network interface IP address as web address, e.g. https://192.168.6.18/ . (Do not use the Startup Wizard any more).

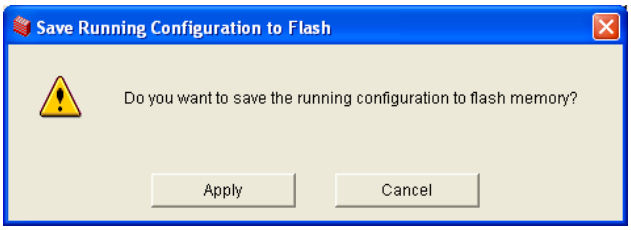


Now you can restrict the access to the PDM to the new address range of the internal interface again. Click on the configuration button in the tool bar, select the system tab and open “Administration>PDM/HTTPS” in the categories tree, as before. Enter an appropriate IP range that shall be allowed to use the PDM. Confirm the change by clicking <OK> and download the change to the PIX by clicking <Apply> in the previous screen.





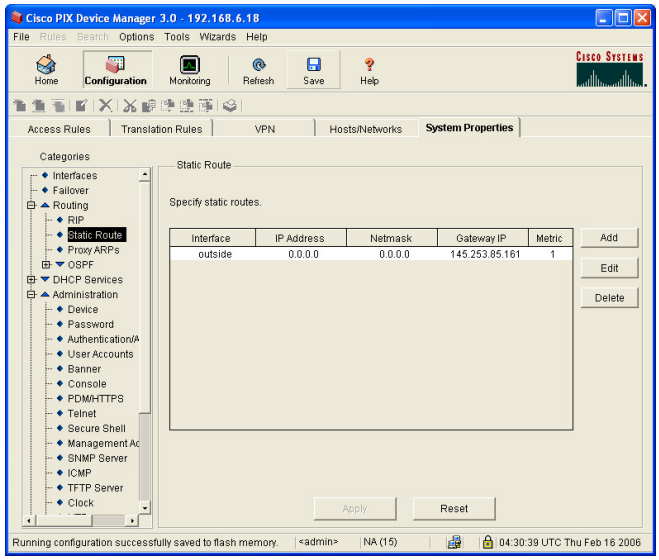
Now it is time to save the basic configuration permanently by clicking the <Save> button in the tool bar. Confirm the warning with <Apply> in the popup box.

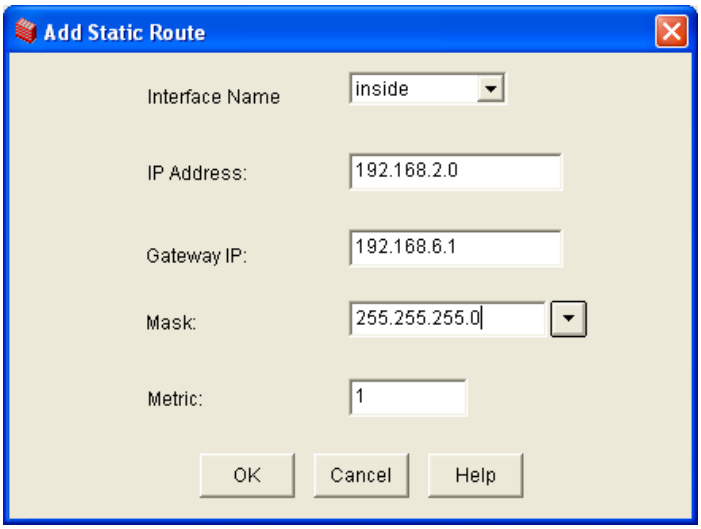


2.3.2 Routing Setup

When the Startup Wizard is used, the default route via the external interface is already setup to the gateway to the internet. If you want to configure any other networks not routed through the default gateway, you need to add those networks in the Routing setup. Here, we add a static route to an additional network via the inside interface.

Click <Configuration> in the tool bar. Click on the “System Properties” tab and select “Routing>Static Route” in the categories tree. Click <Add> to add a new route. In the following dialog box, enter the parameters of the new route and the interface name, which shall be used. Here, we use the inside interface.

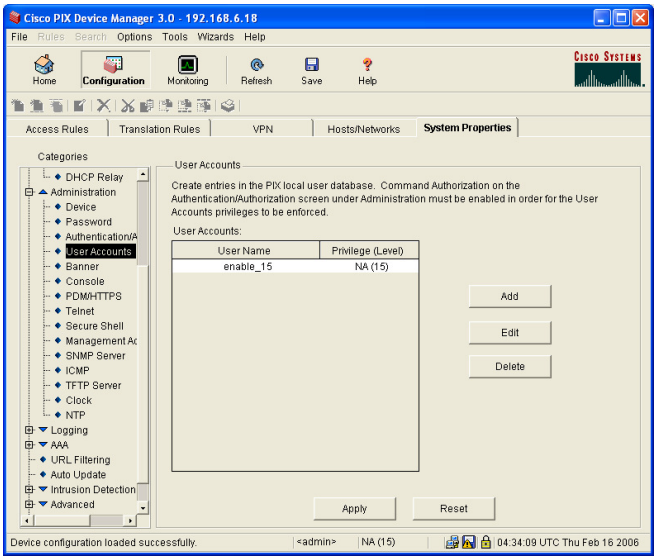


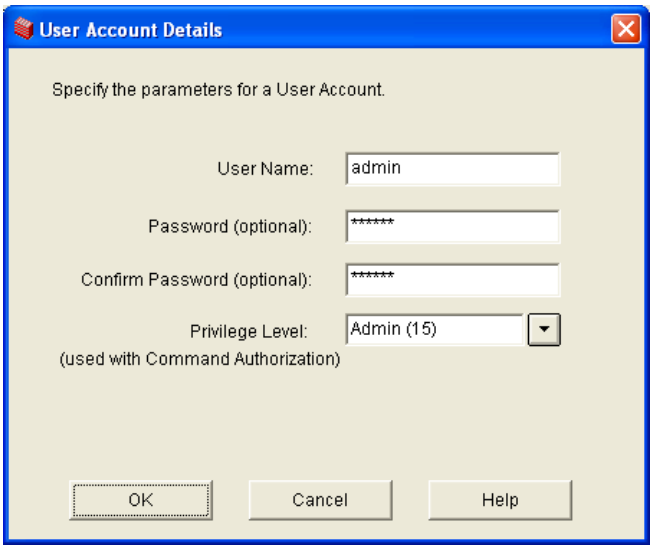


Click <OK> to close the box and accept the new route. Then click <Apply> in the previous screen. If the route needs to be permanent, click <Save> in the tool bar.

2.3.3 Local User Management

Administrators and users that shall be used as a local user data base for remote access can be defined with the PDM also. Click <Configuration> in the tool bar. Click on the “System Properties” tab and select “Administration>User Accounts” in the categories tree. Click <Add> to define user name, password and access rights for the new user.

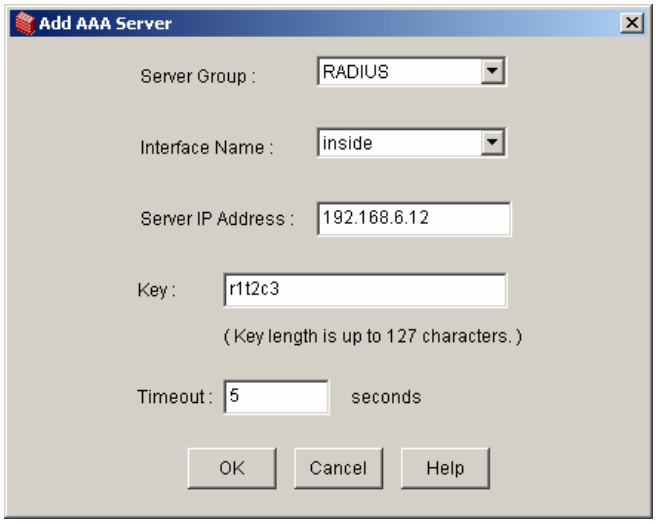


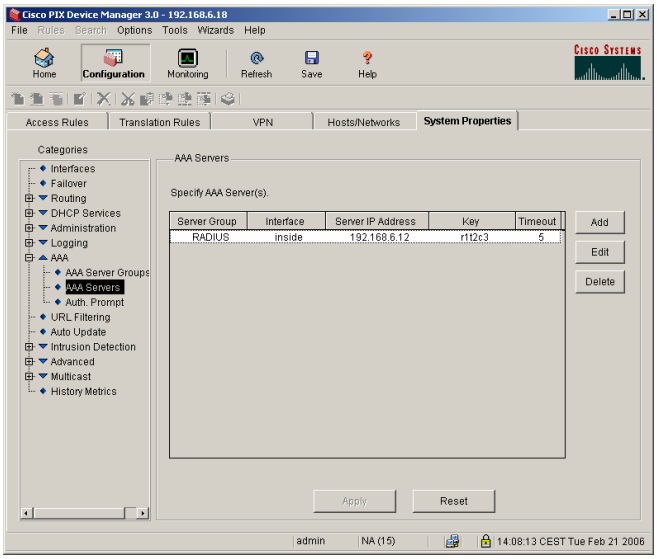


Click <OK> to close the box and accept the new user. Then click <Apply> in the previous screen. If the user needs to be permanent, click <Save> in the tool bar.

2.3.4 Authentication Setup

Authentication servers are set up in the AAA category of the system properties. Click <Configuration> in the tool bar. Click the “System Properties” tab. Select “AAA > AAA Servers” in the categories tree. Click <Add> to add another server. In this case, we configure a RADIUS server. Therefore, RADIUS is selected as Server Group. The RADIUS server is reached through the inside interface. Further, IP address and shared key are configured. Accept the values with <OK> to return to the previous screen.



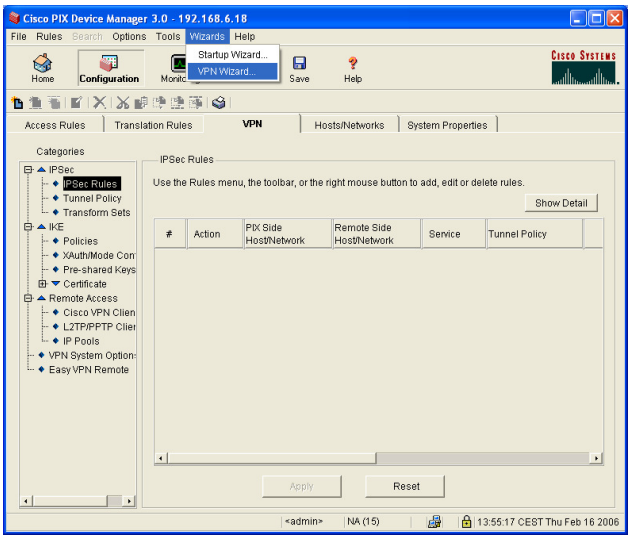


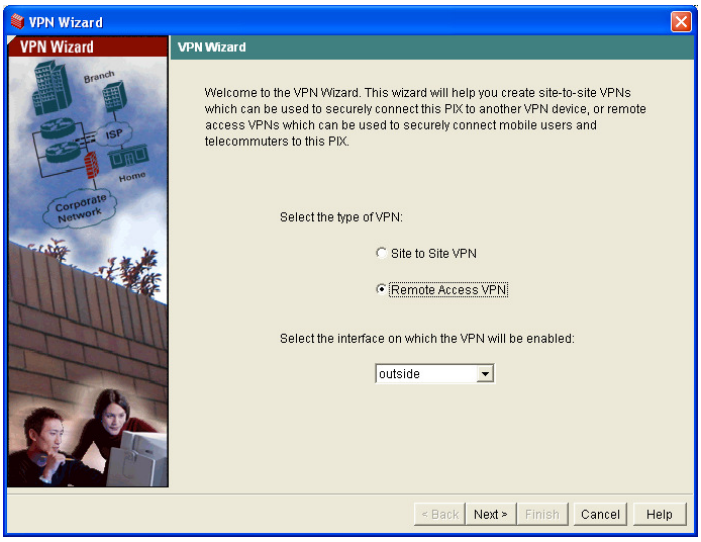
Make sure that the respective group, in this case RADIUS, is set up as the authentication means, when configuring the VPN client setup.

2.4 Advanced settings

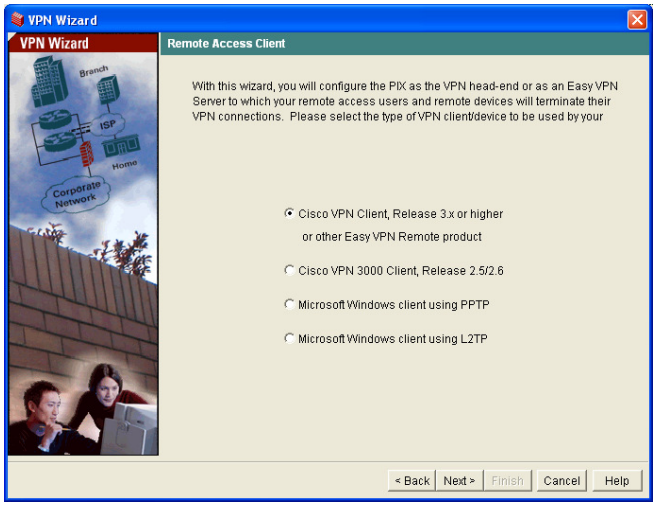
Since we are doing IPSec over an address translation we need to enable IPSec NAT-Traversal. Further it is necessary to enable “Keep Alive” telegrams.

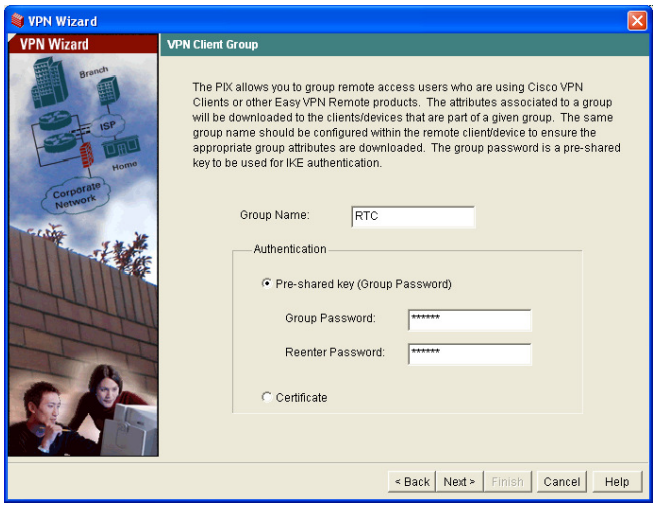
Click <Configuration> in the tool bar. Click the VPN tab. Select “Administration>User Accounts” in the categories tree. Now select “VPN Wizard” in the “Wizards” menu in the menu bar.



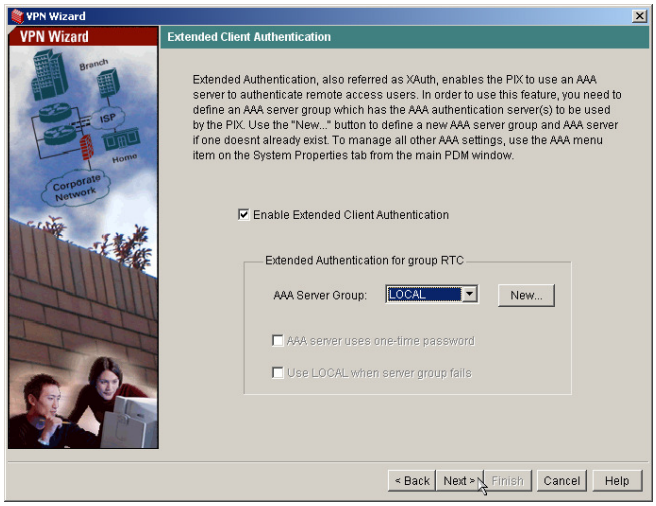


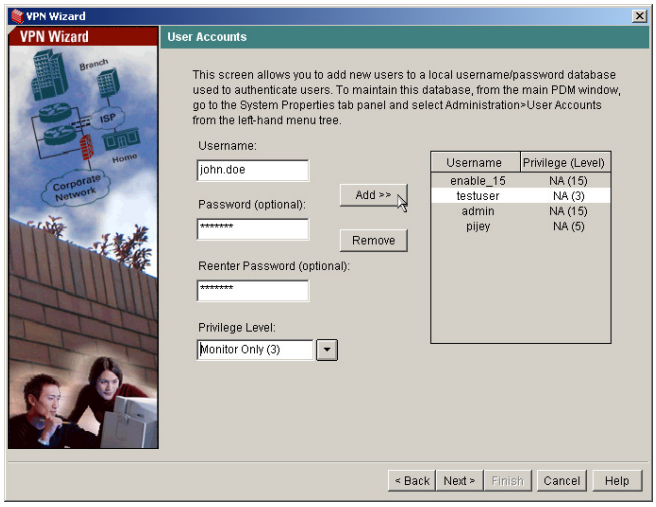
Select “Remote Access VPN” as the VPN type and select the outside interface to be the VPN-enabled interface. Click <Next>. Select the Cisco VPN client 3.x or higher as your VPN client. Then continue with <Next>.



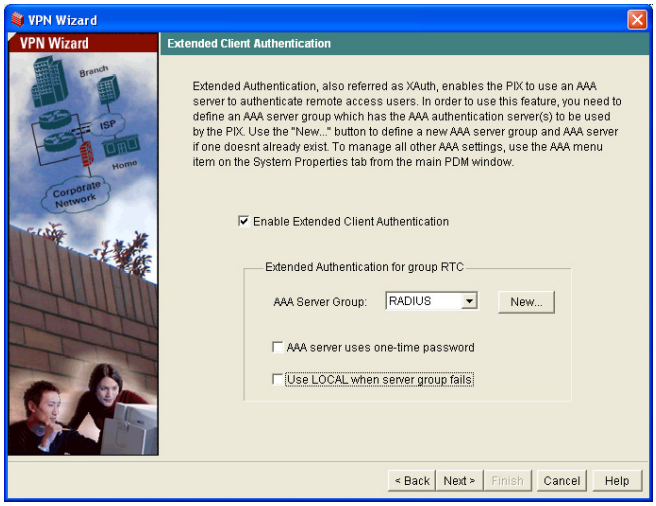


Setup the group name and select the authentication type. Here we use a group password. Enter it and then click <Next>. Enable Extended Authentication by checking the box and Select the AAA Server group. You can select either TACACS+ or RADIUS as external authenticators or LOCAL to use the internal user data base.

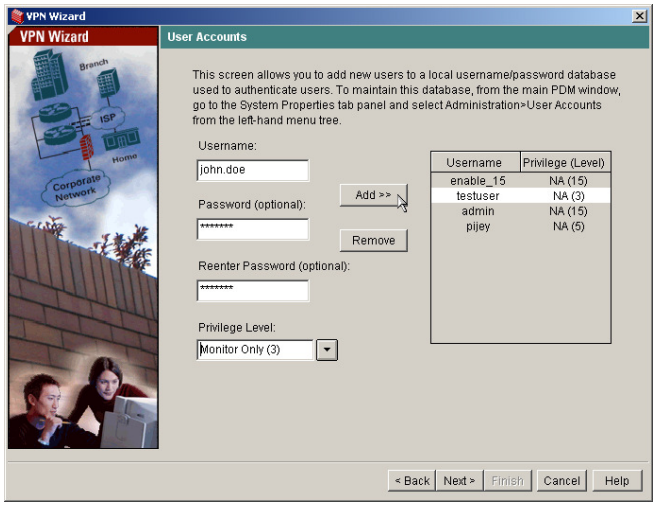


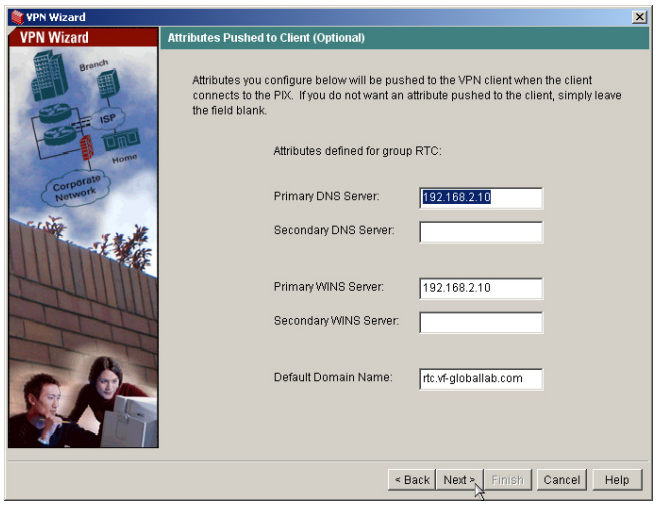


When local is selected, you can modify the local user data base after clicking <Next>. Alternatively, if selecting TACACS+ or RADIUS, the server must be configured in the System Properties, Category “AAA>AAA-Servers”.



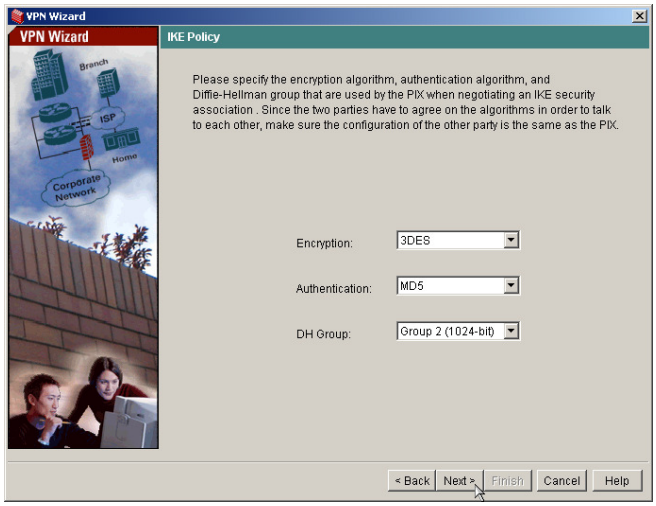
After selecting the authentication method, the address pool used in the clients must be entered. You can select either an already defined pool or enter a range in the dialog. Continue by selecting <Next>.

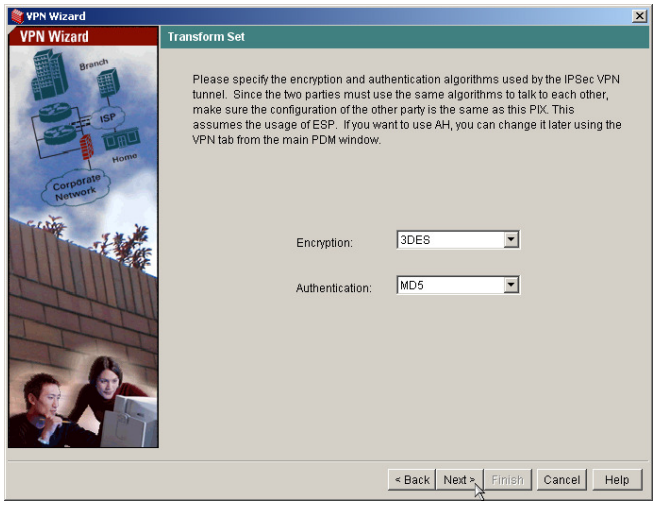




Next, the attributes, like DNS server, WINS server and domain that will be pushed to the client are configured. Continue by clicking <Next>.

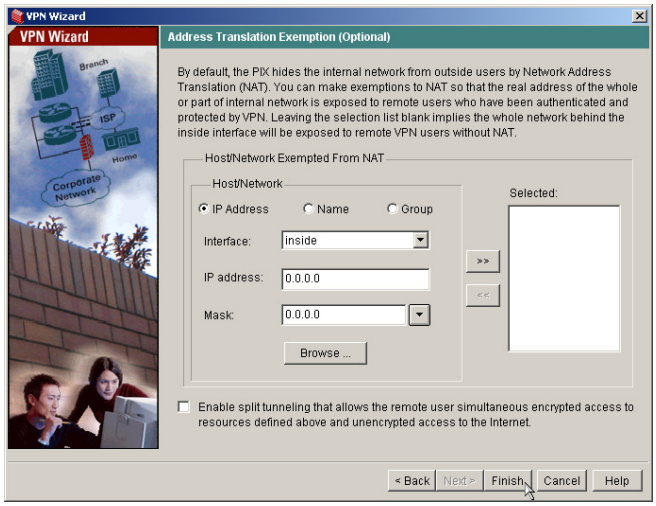
In the next two screens, the encryption method for authentication and encryption are defined. Continue by clicking <Next>.

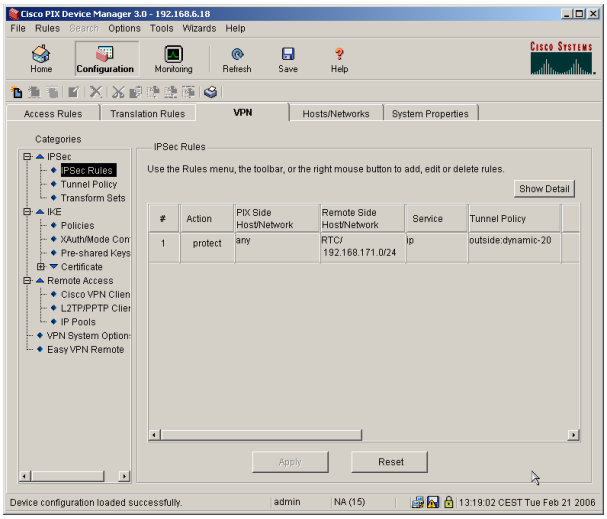




In the next screen, split tunnelling can be configured. If split tunnelling is desired, the networks which are entered into the list are the only networks transferred encrypted. All other networks will be allowed on the internet. Leave the checkbox to enable Split Tunnelling unchecked and click <Finish>. The wizard will generate all necessary entries and generate the IPSec Rule. Save the data to the PIX to make it permanent.

Note that split tunnelling is NOT recommended as it is a security vulnerability, but we cover it here for completeness.





2.5 IKE keep alive

The Keep Alive is configured in the IKE policy configuration. Click <Configuration> in the tool bar and then select the tab “VPN”. From the categories tree, select “IKE>Policies”. Here, in the General Information part, the following check boxes must be checked:

- Enable NAT Traversal
- Set Keepalive & Retry values

Set the NAT-Keepalive value to 60 seconds to get a stable connection over the usual 3G/GPRS networks. Set the Keepalive value to 30 seconds and the Retry value to 20 seconds.

Unfortunately, data compression is not supported on the current version of the PIX 501.

3 Configuration of Split Tunnelling

Split Tunnelling is supported and will be negotiated within connection phase by server push. The user cannot override server settings.

Enabling or disabling split tunnelling can be configured in the Group properties. All users assigned to this group will use this setting.

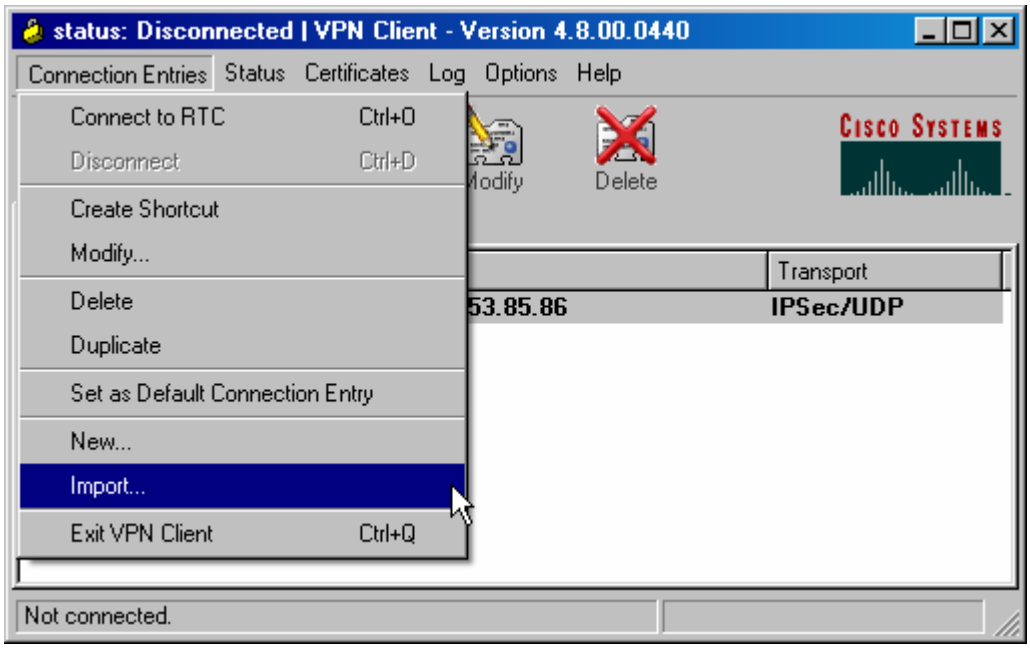
Note that split tunnelling is **NOT** recommended as it is a security vulnerability.

4 User Management and Profile Handling

Integrated user management and external authentication server such as RADUIS, SDI, NT- or AD-Domain are supported. You can choose it in the Configuration / System / Server / Authentication menu.

The connection profile is for the first time locally configured. After connecting to the PIX the profile will be updated automatically each time the Client connects. The Client application offers the possibility to import this profile.

Cisco VPN Client 4.8.00.0440



Profile configuration file (.pcf file) is placed in “C:\Program Files\Cisco Systems\VPN Client\Profiles”.

5 Logging

Event logging is available on the Monitoring / Filterable Event Logs screen. This screen shows the events in the current log file, lets you filter and display events by various criteria, and lets you manage the event log file.

*** End of Document ***