ADTRAN

TECHNICAL SUPPORT NOTE

Using the GUI to Configure a VPN Tunnel Between a NetVanta 2000 Series Router and the NetVanta VPN Client using Mode-Config.

Featuring ADTRAN OS and the web GUI

Introduction

This Technical Support Note explains how to configure a VPN tunnel between a NetVanta 2000 series second-generation router, running the Enhanced ADTRAN OS, and the NetVanta VPN client software using Mode-Config. Mode-Config simplifies client configuration by dynamically assigning the VPN client an IP address for VPN traffic. Mode config allows the administrator to import the same security policy to each VPN client.

Included on this document:

- Step by step instructions, with screen shots, to configure VPN in the AOS web GUI on a NetVanta 2000 series router.
- Step by step instructions, with screen shots, to configure VPN client on a PC.

Before You Begin

This Tech Note assumes the NetVanta router is already installed and has connectivity to the Internet. It further assumes that the client software is already installed on the user's PC and the PC has Internet access. It is very important to verify with your ISP that ESP traffic (protocol 50) and AU (protocol 51) are allowed through their network. ESP is the protocol that carries the encrypted data of your VPN across the Internet.

Figure 1, is a network diagram that will be used as an example for this document. On the left is a user needing access to the 2054 LAN. The NetVanta 2054 and client software will be setup using mode config. Mode config allows the NetVanta 2054 to dynamically assign an IP address to the VPN client. The dynamic IP address range for this example will be 172.30.0.0 through 172.30.0.255. On the right is a NetVanta 2054 with a WAN IP address of 10.19.219.54 and a mask of 255.255.255.0. The LAN network behind the NetVanta 2100 is also a private network 10.10.10.0 with a mask of 255.255.255.0.

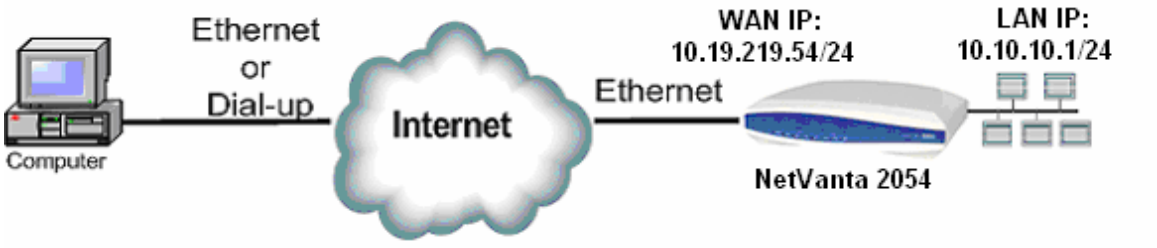


Figure 1 Sample Network Diagram

NetVanta 2054 configuration

1. VPN Wizard

From the main page of the web GUI choose "**VPN Wizard**" on the left hand side under "VPN". This will display a dialog box such as the one shown in Figure 2. If it is not already selected, choose "Typical Setup" and the click **Next**.

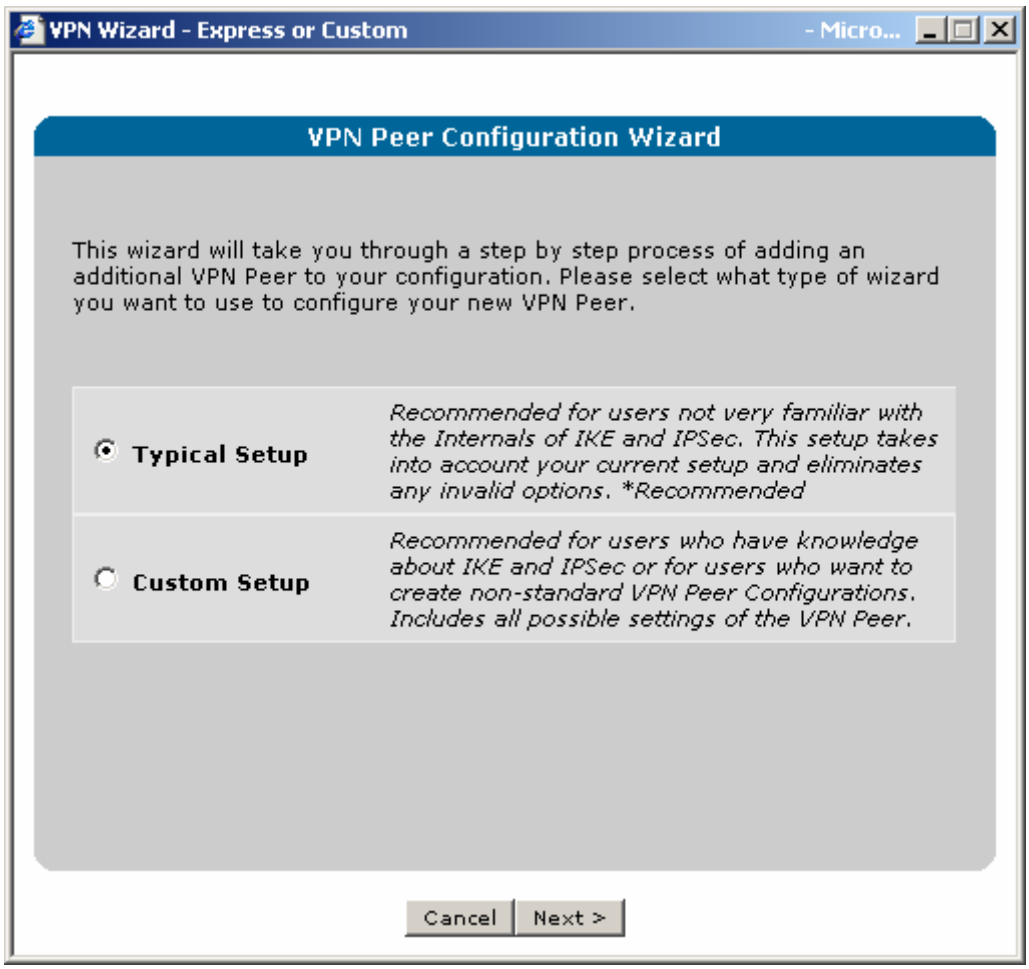


Figure 2 VPN Wizard

2. VPN Name

The dialog box, as shown in Figure 3, should now be prompting you to enter a name for your VPN connection. This name is used to describe the VPN connection. For our example we are going to call it "VPN Client Users".

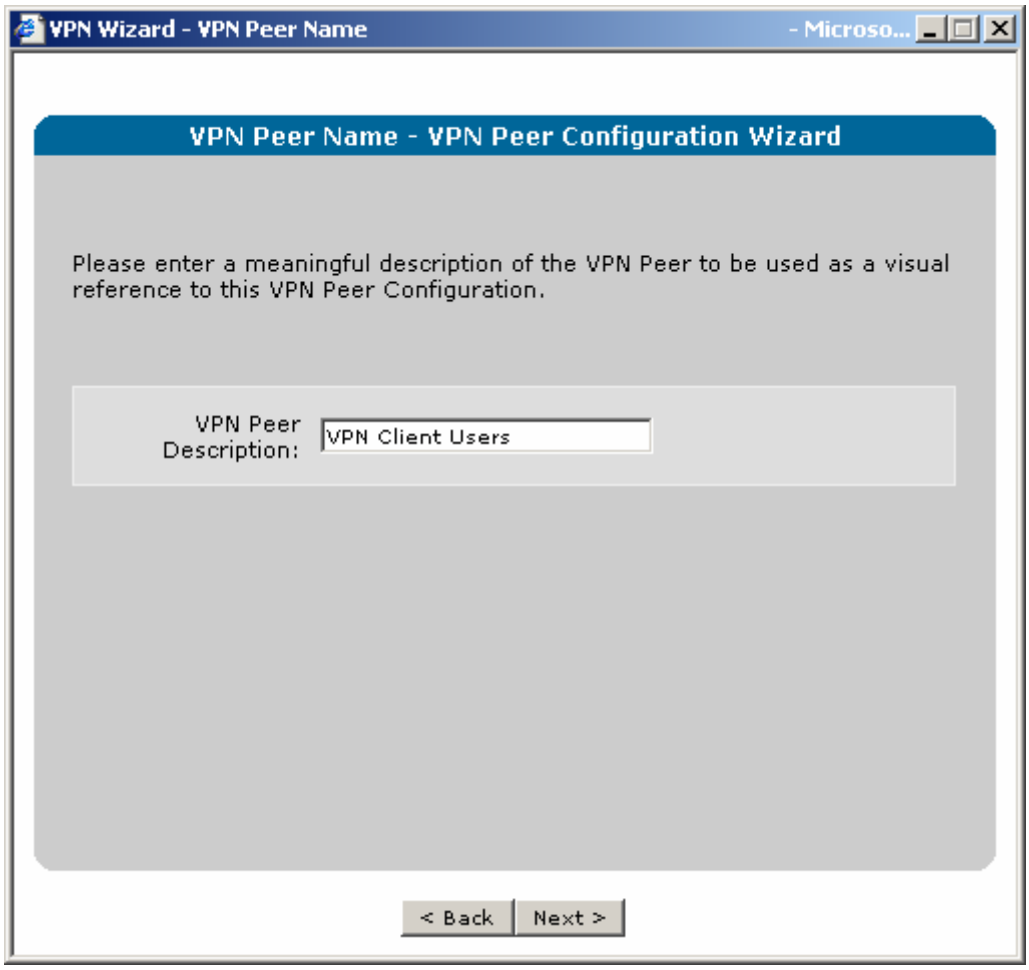


Figure 3 VPN Peer Description

3. Public Interface

Now we will need to choose from the drop down box which interface the vpn users will connect to. If this unit is connected to the Internet you will want to choose your Public interface (the interface connected to your ISP). In our example we will choose the interfaced label public with the IP address of 10.19.219.54.

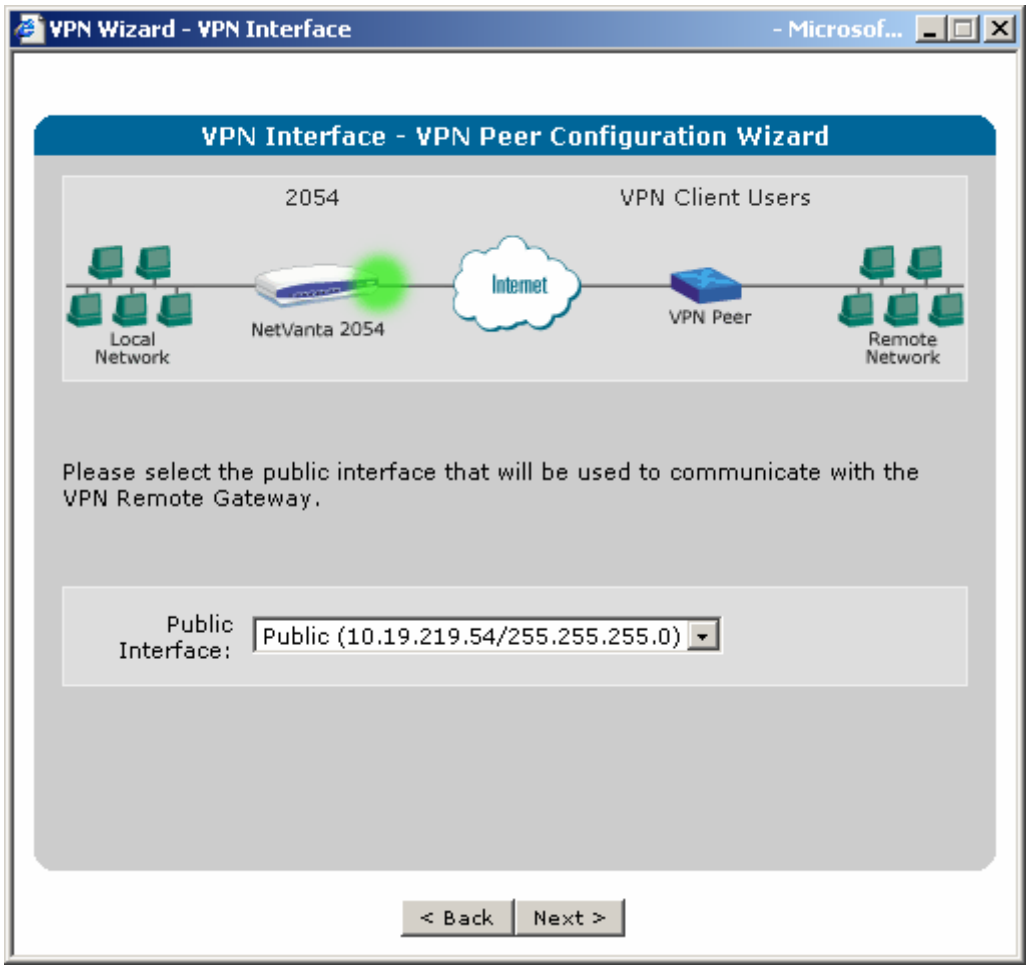


Figure 4 Choosing Your Public Interface

4. VPN Type

In the next dialog box, as shown in , we will be choosing the type of VPN connection we would like to configure. We want to choose "**Mobile Peer**", a mobile peer is someone who will connect with the NetVanta VPN client software.

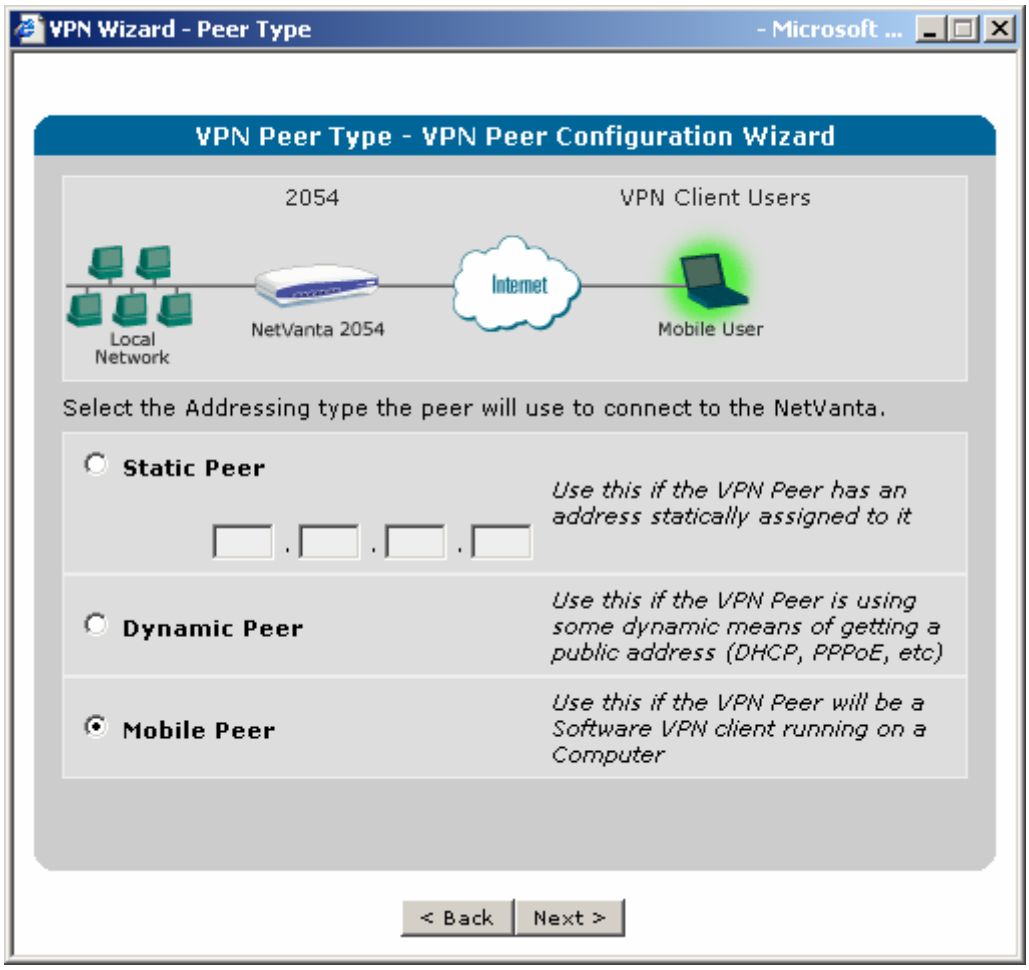


Figure 5 Peer Type

5. Mode Config Settings

Now we need configure the IP information that we will send to the mobile user. Figure 6 shows the dialog box that will apear that contains the settings we want to send to the client software. The "**IP Subnet**" and "**IP Netmask**" is the subnet of IP addresses that we wish to assign to the mobile users. Then we want to fill in the IP address of your DNS server in the "**Primary DNS Server**" field that your mobile users will use. You may optionally fill in a "**Secondary DNS Server**". If you have a WINS server (optional) on your network you may also enter in the IP address in the "**Primary WINS Server**" and also "**Secondary WINS Server**".

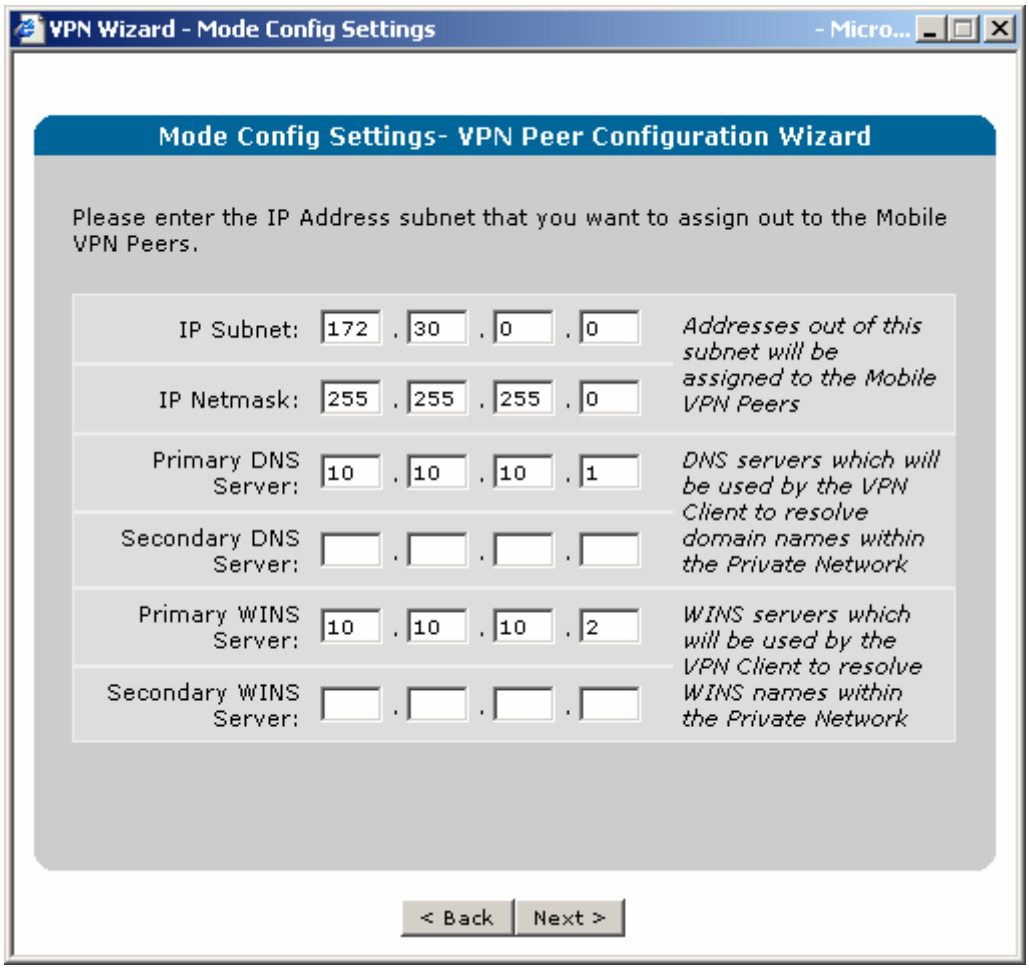


Figure 6 Mode Configuration Settings

6. Extended Authentication Mode

Next we will sepcify which extended authentication mode we will be using. In our example we will not be using any extended authentication sho we will choose "**Diable XAUTH**" from the drop down as show in Figure 7.

Figure 7 Extended Authentication

7. Local Network

Now we need to select the network(s) we would like the mobile users to have access to. You can select the network from the drop down as in Figure 8, or if you have multiple networks you would like them to access you can enter the network and mask in Local Subnet fields. In our example we only need access to the network that is behind the NetVanta so we choose the 10.10.10.0/255.255.255.0 network from the "**Use Network From:**" drop down.

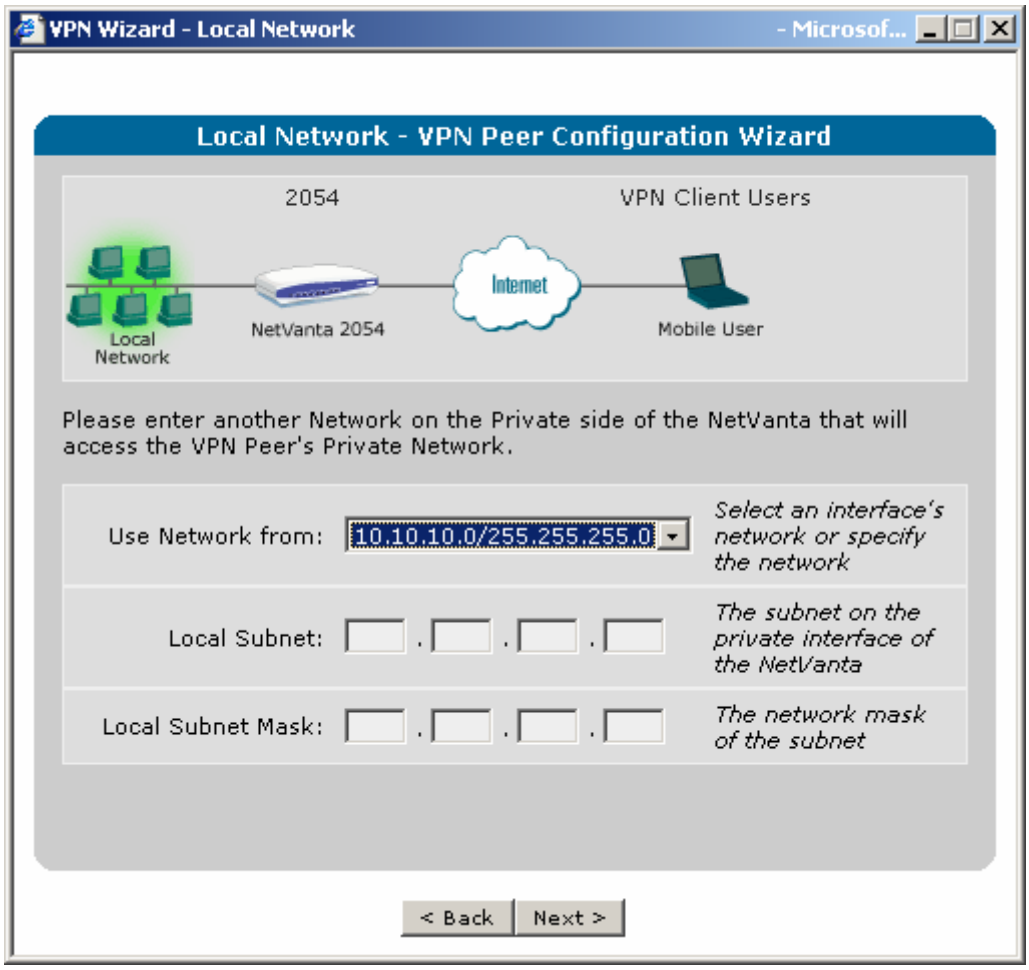


Figure 8 Local Network Selection

8. Authentication

Next we will select the authentication the mobile users will use to gain access via VPN. In most cases you will want to use "**Preshared Secret**". Once you select the option for preshared secret you can then type in your preshared secret key in the text box.

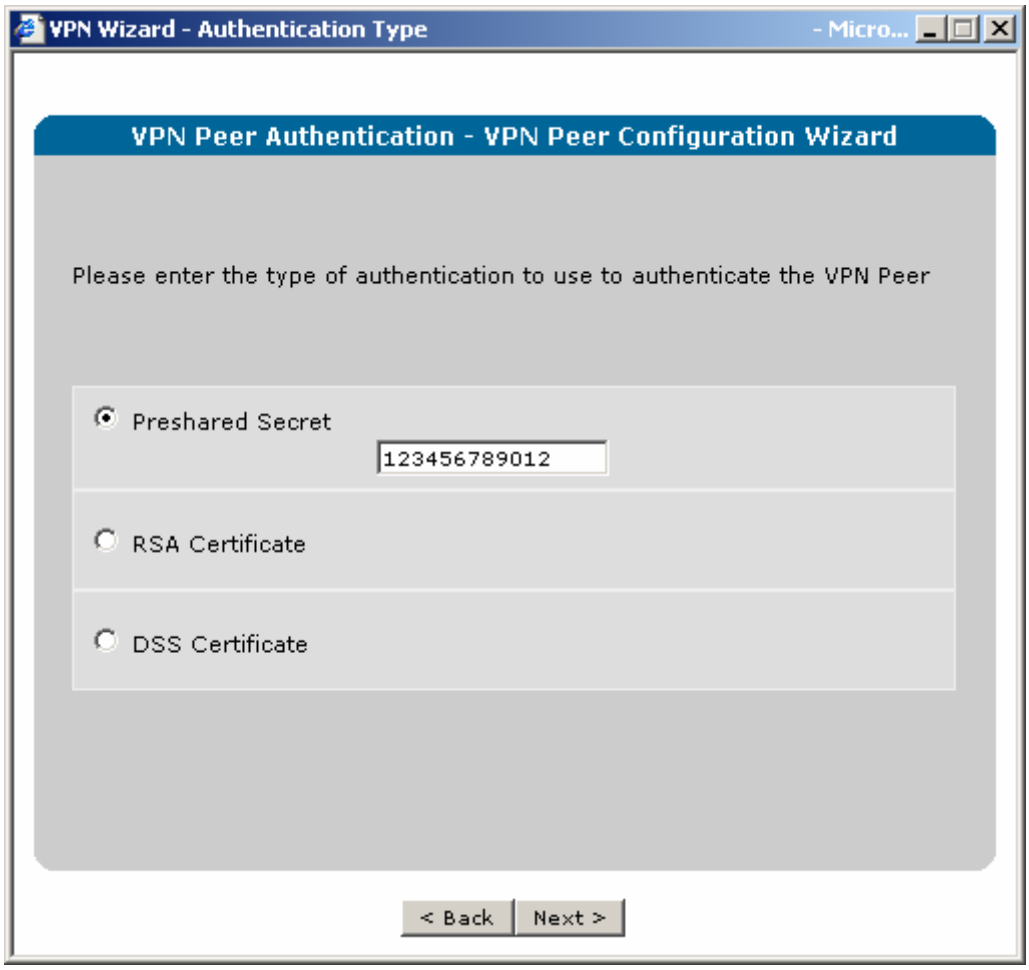


Figure 9 Authentication

9. Remote ID

Since we are using the NetVanta VPN Client softare to create the VPN session we will want to use "**Domain Name**" as our "**Remote ID Type**". In our example our mobile user will connect as remote1.adtran.com as his "**Remote ID Value**" but you can use any name you would like.

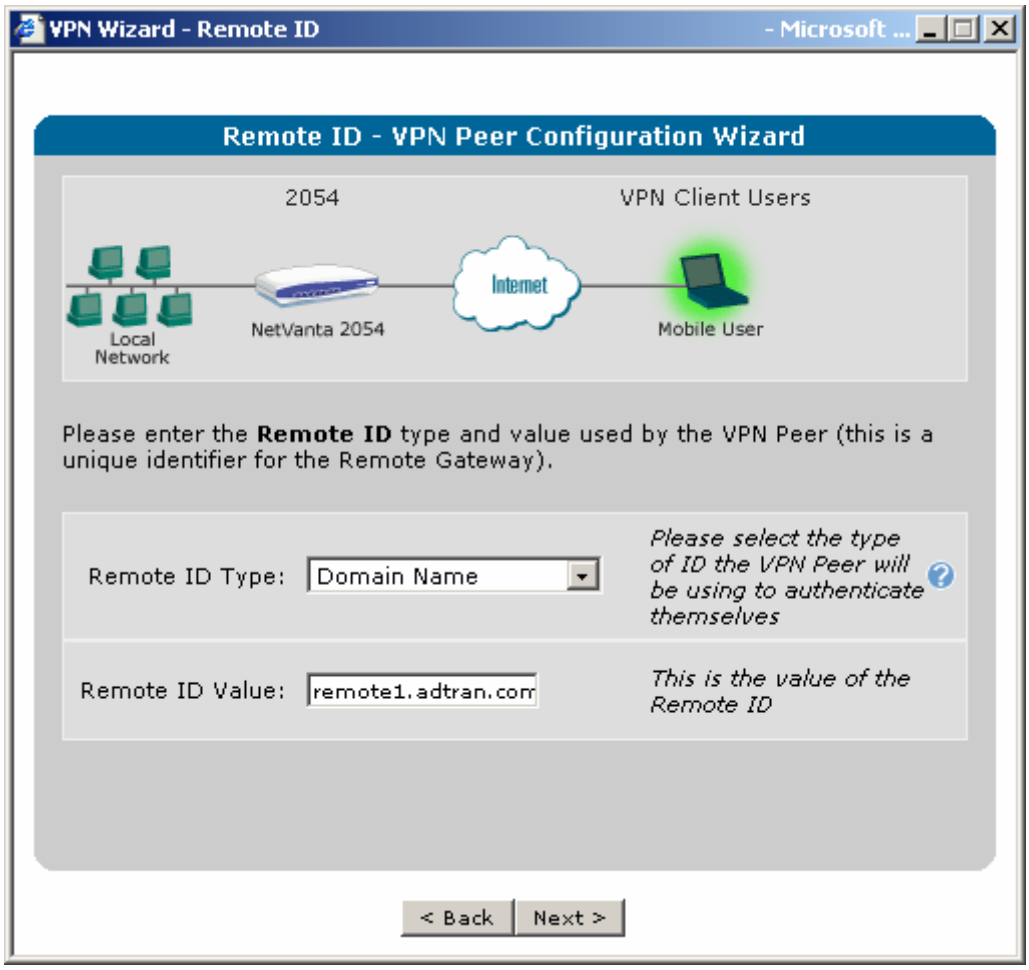


Figure 10 Remote ID

10. Local ID

Now we will specifiy what we will use as our Local ID. We our just going to use our public IP address as our local ID.

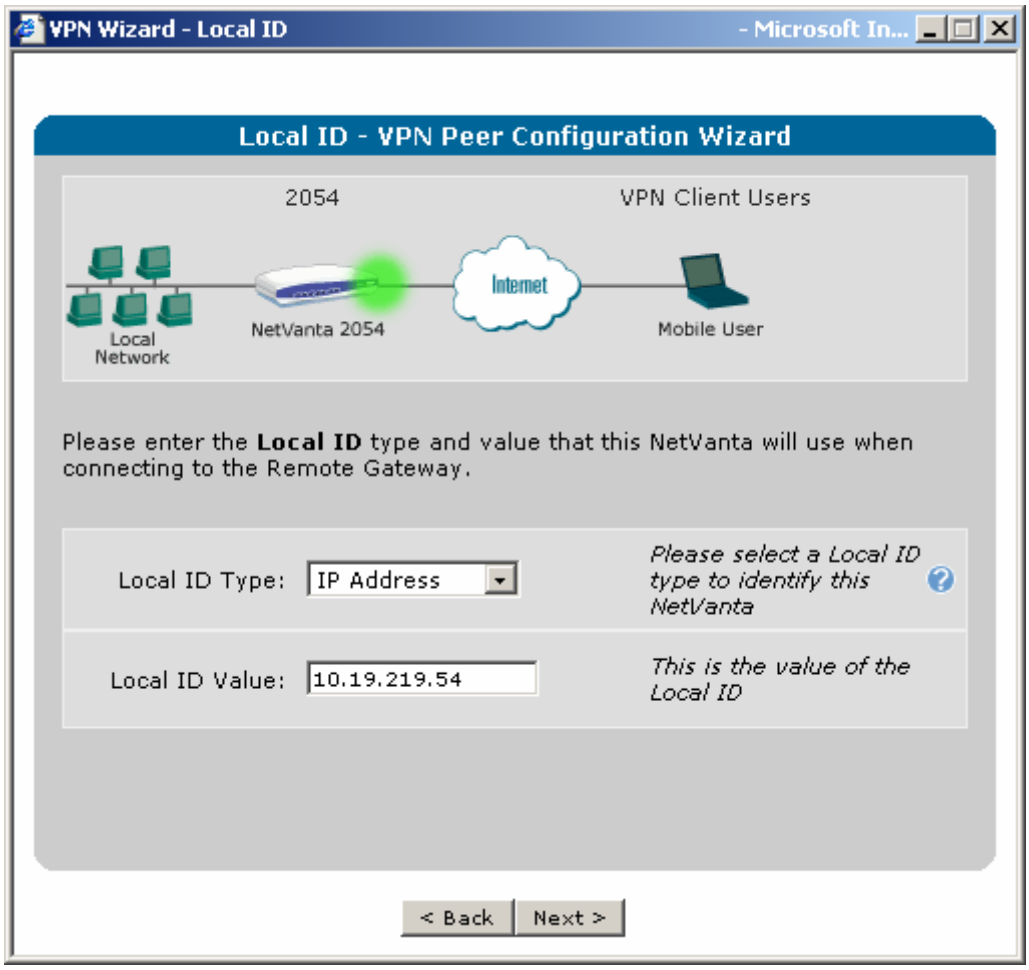


Figure 11 Local ID

10. Apply Configuration

At this point you should see a list of all the setting we choose above as shown in Figure 12. You can now choose "**Apply**" and your NetVanta should be configured to allow mobile users to VPN into your network.

Figure 12 Configuration Summary

1. Configure new connection

a) Start the Security Policy Editor by double-clicking on the Netvanta VPN Client icon in the Taskbar. Then select **Edit > Add > Connection** to create a New Connection.
b) Select **Secure** from the **Connection Security** list**.**
c) For **ID Type** choose **IP Subnet**. Then enter **10.10.10.0** and **255.255.255.0** for the **Subnet** and **Mask** (Netvanta 2054's Private LAN network).
d) Check **Connect using** and Select **Secure Gateway Tunnel**.
e) Under **ID type** select **IP Address** and below enter the WAN IP address of the Netvanta 2100.

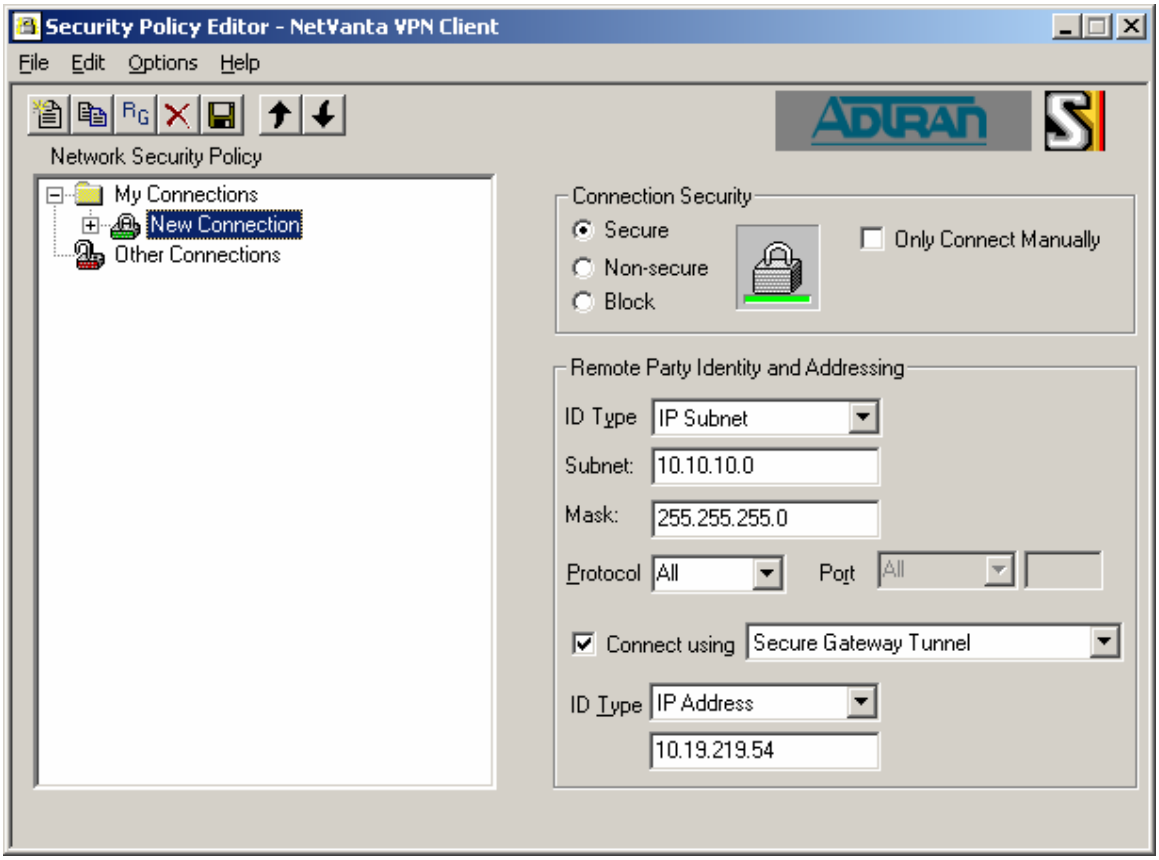


Figure 1

2. Configure Security Policy

a) Next, select Security Policy and under Security Policy select Aggressive Mode. See Figure 2.

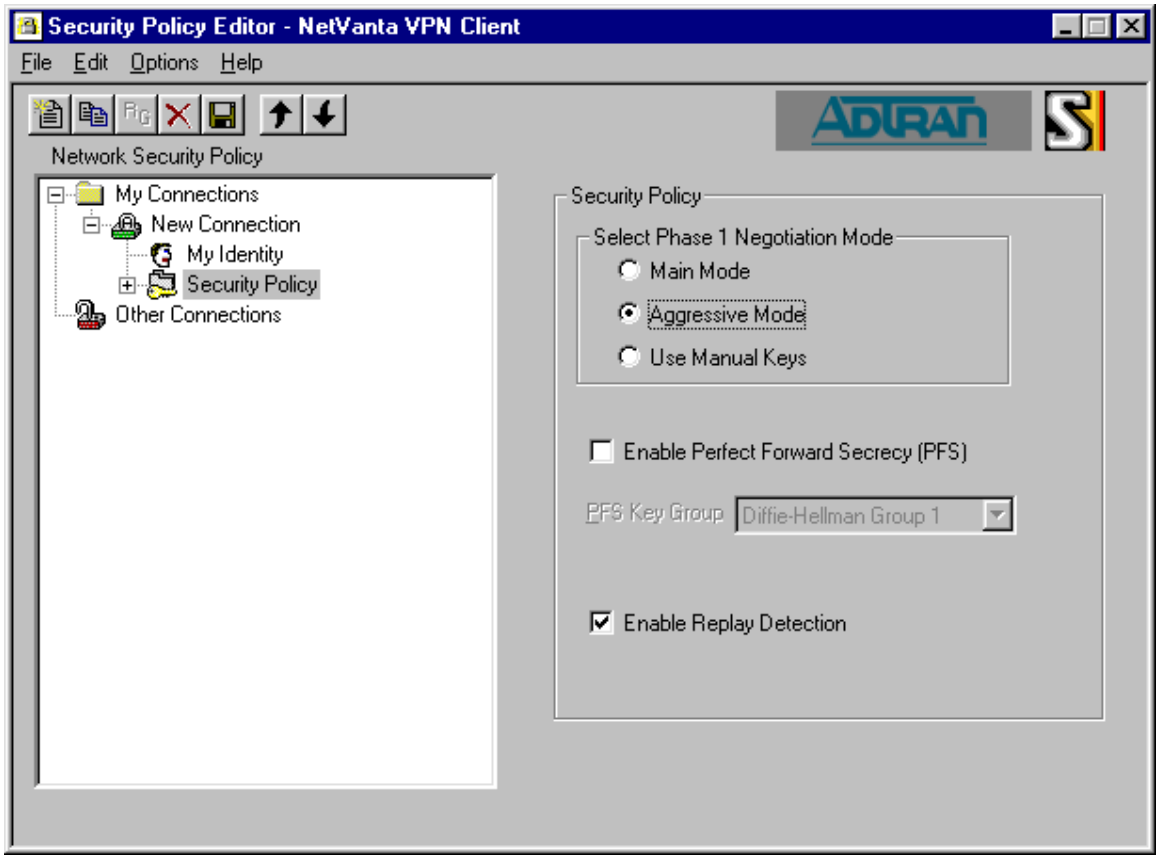


Figure 2

3. Set My Identy Parameters

Select **My Identity**. Under **ID Type** select **Domain Name** and type in the local ID (remote.com). This local ID data will be the Netvanta 2054 remote ID information. Select **Pre-Shared Key** and enter same key as entered into the Netvanta 2054. Select **Preferred** for **Virtual Adapter**. See Figure 6.

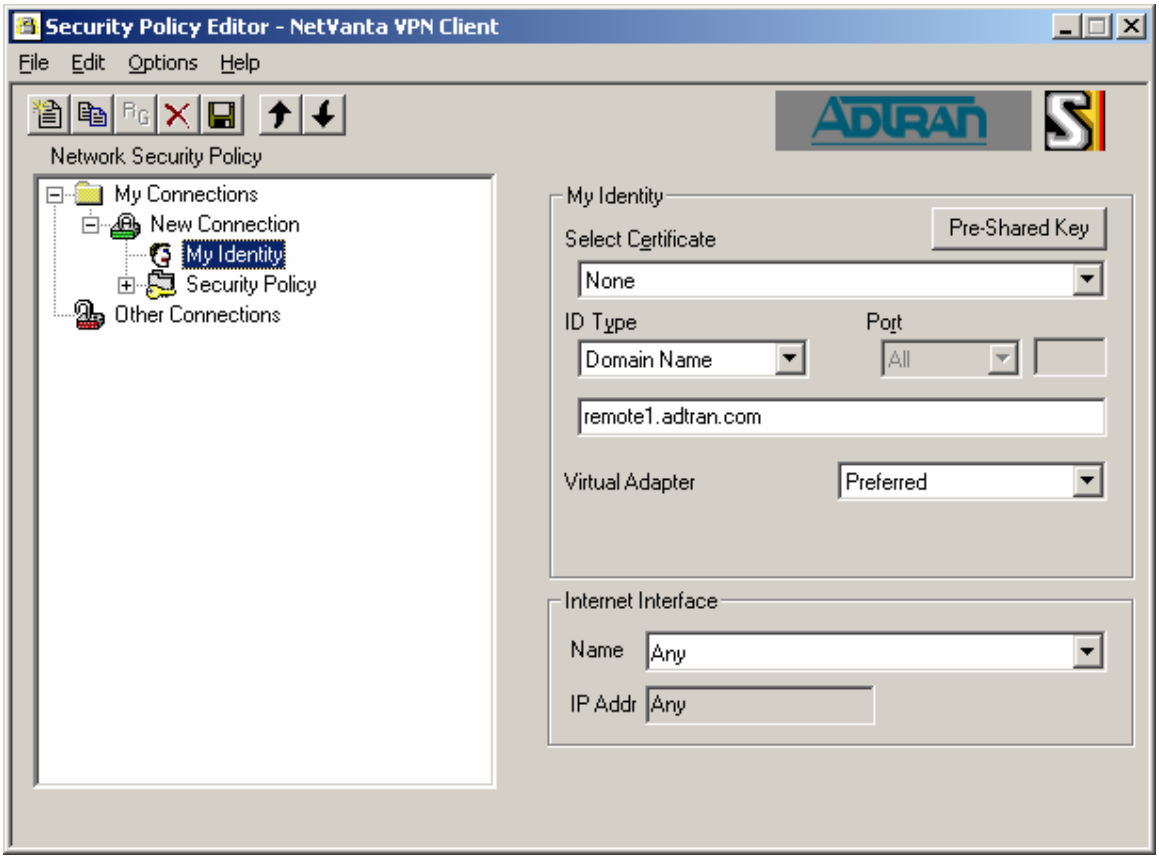


Figure 6

4. Configure IKE Parameters

Click on the plus **(+)** sign by **Security Policy**. Then click on the plus **(+)** sign by **Authentication (Phase 1)**. Click on **Proposal 1**. Select **Pre-Shared Key** for the **Authentication Method**. Select **Triple DES** for the **Encrypt Alg**. Select **MD5** for **Hash Alg**. Select **Seconds** for **SA Life** and enter **28800** (The IKE policy timeout from the Netvanta 2100). Select **Diffie-Hellman Group 1** for **Key Group**. See Figure 7.

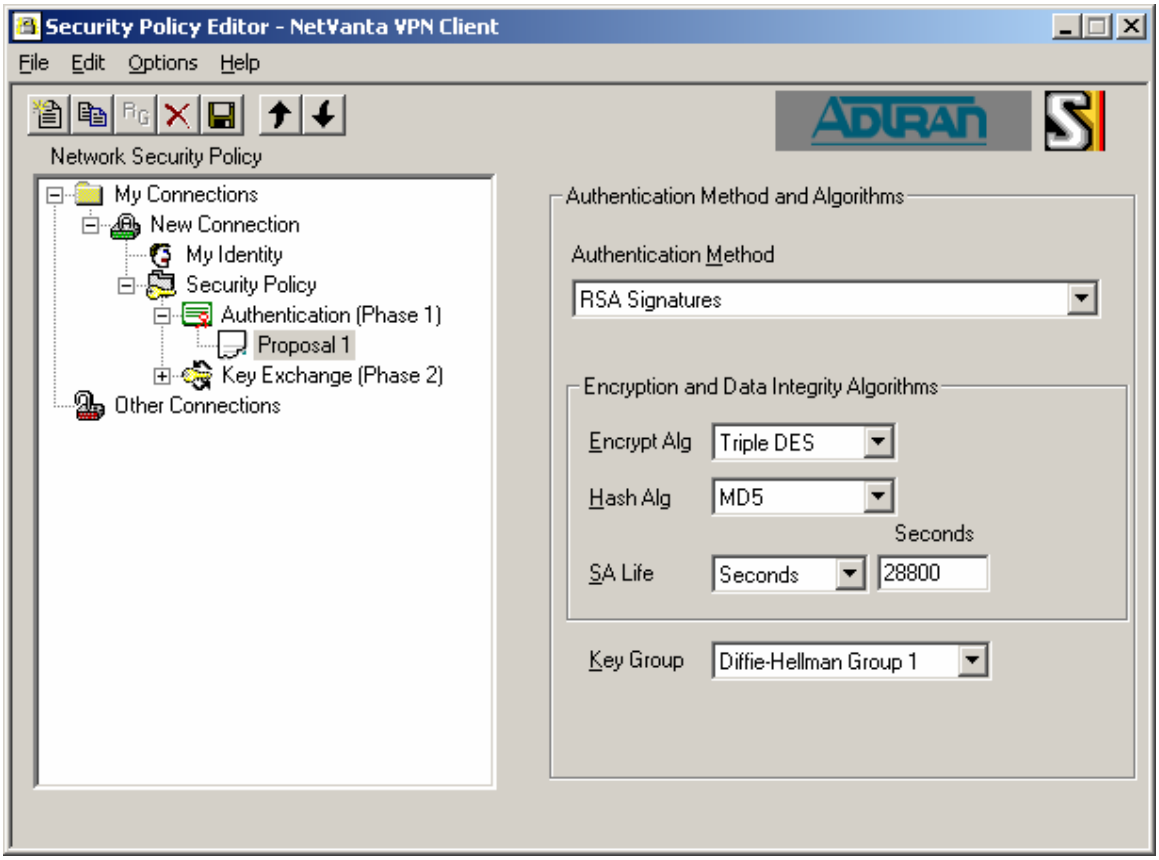


Figure 7

5. Configure IPSec Parameters

Click on the plus **(+)** sign by **Key Exchange (Phase 2)**. Then click on **Proposal 1.** Under **IPSec Protocols**, select **Seconds** for **SA life.** For **Seconds** enter **28800** (The IPSec Lifetime Secs of the Netvanta 2100). Check **Encapsulation Protocol (ESP)**. Select **Triple DES** for the **Encrypt Alg, MD5** for the **Hash Alg** and **Tunnel** for the **Encapsulation**. See Figure 8.

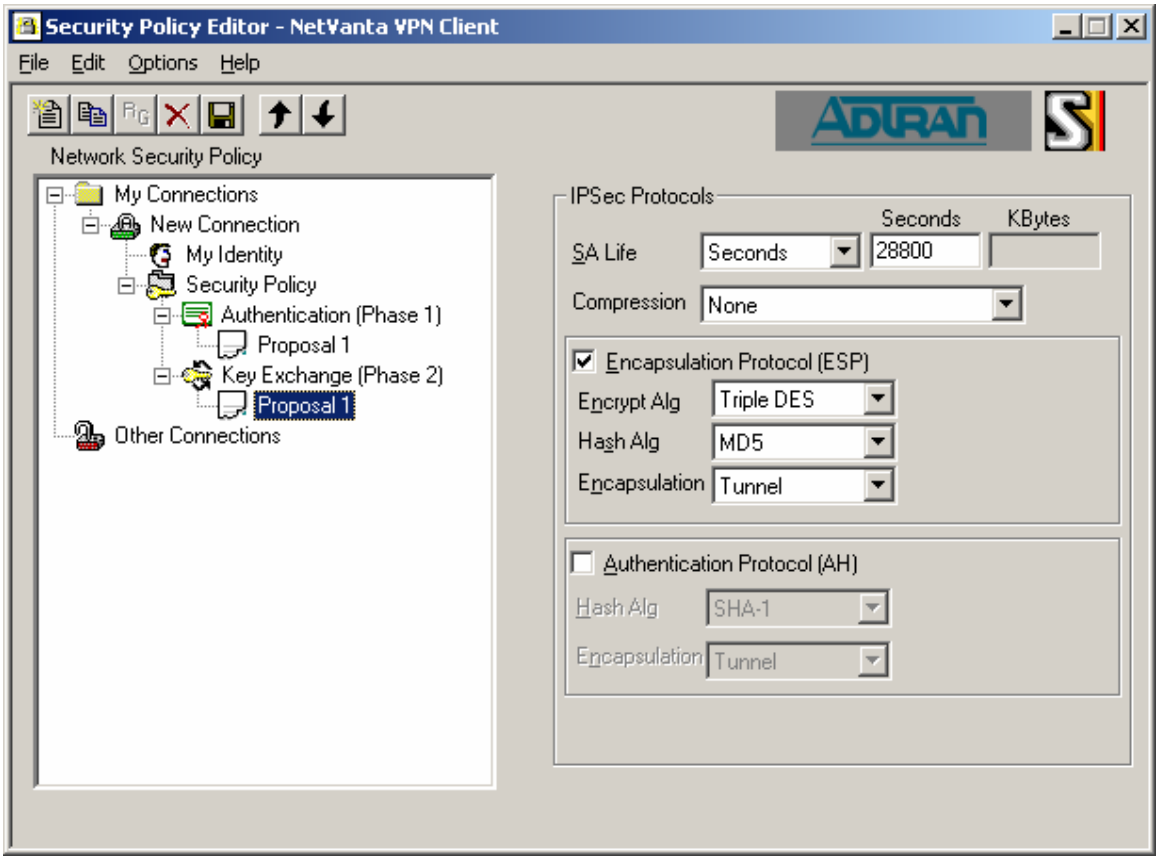
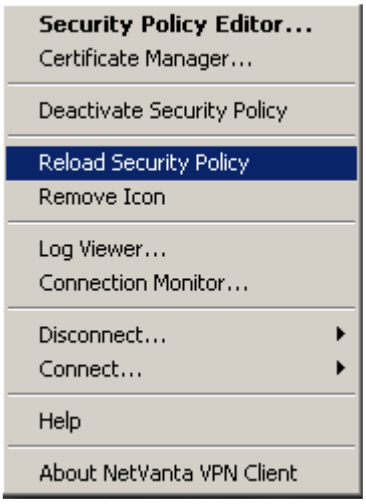


Figure 8

6. Save and Reload new Policy

Finally, click on **File** and then **Save**. Right-click on the Netvanta VPN Client icon and select **Reload Security Policy**. On the PC, open up a DOS prompt and type **ping 10.10.10.1**. This should activate the tunnel and you should get replies from 10.10.10.1



If you experience any problems using your ADTRAN product, please contact ADTRAN Technical Support.

DISCLAIMER

ADTRAN provides the foregoing application description solely for the reader's consideration and study, and without any representation or suggestion that the foregoing application is or may be free from claims of third parties for infringement of intellectual property rights, including but not limited to, direct and contributory infringement as well as for active inducement to infringe. In addition, the reader's attention is drawn to the following disclaimer with regard to the reader's use of the foregoing material in products and/or systems. That is:

ADTRAN SPECIFICALLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL ADTRAN BE LIABLE FOR ANY LOSS OR DAMAGE, AND FOR PERSONAL INJURY, INCLUDING BUT NOT LIMITED TO, COMPENSATORY, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.