Title: Windows 98 and ME
With Netscreen Remote L2TP/IPSEC VPN to Netscreen
Document Number: VPN-260-005
Version: 0.1
OS Ver. this Paper Applies to: 2.60
HW Platforms this Paper Applies to: All
Audience (Internal or External): External

Purpose

The purpose of this paper is to assist a user in setting up a remote VPN tunnel using L2TP over IPSEC from a PC running Windows 98and ME with Netscreen Remote Client to a Netscreen VPN firewall device running ScreenOS 2.6.0.

Note: This does not apply with ScreenOS 3.0 or higher.

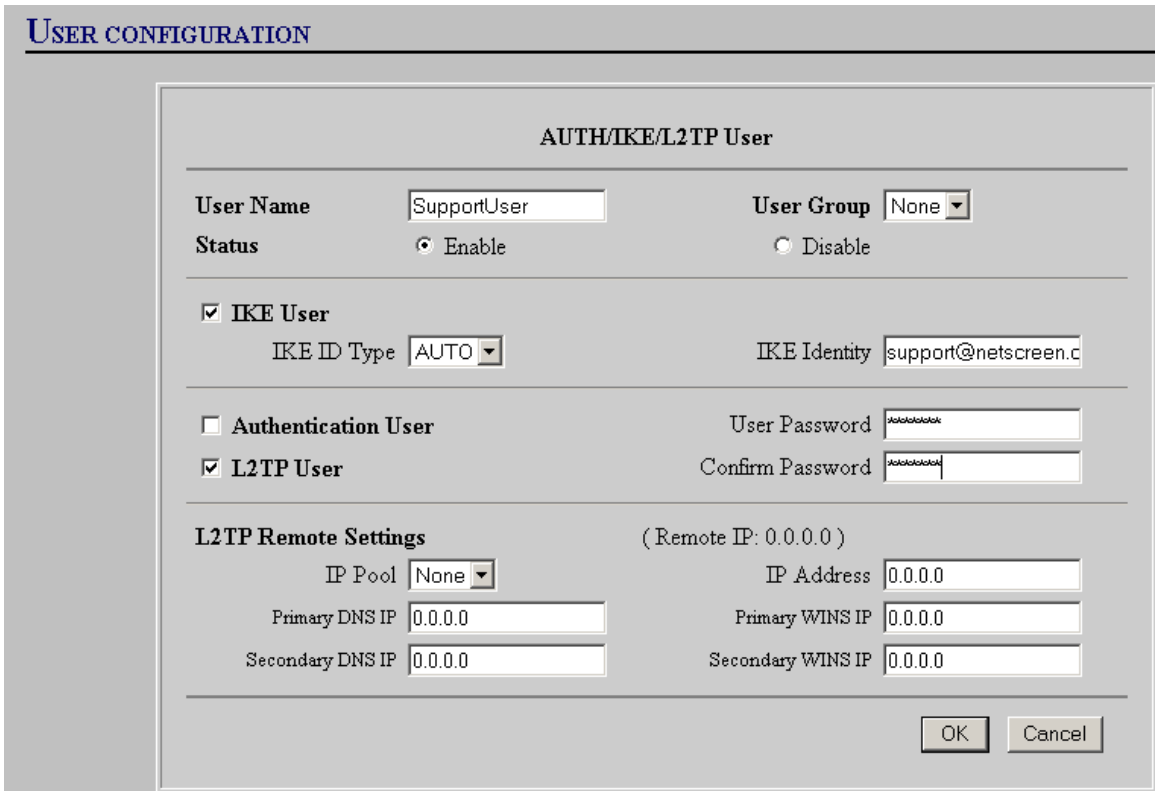
Overview

To configure a VPN using L2TP/IPSEC with Windows 98 and ME with Netscreen Remote Client, you must create a native Microsoft VPN connection within Windows and L2TP with pre-shared IKE on the Netscreen Remote Client to the Netscreen firewall. This paper will provide a procedure in how to configure a VPN via L2TP/IPSEC with either Windows 98 and ME and Netscreen Remote Client.

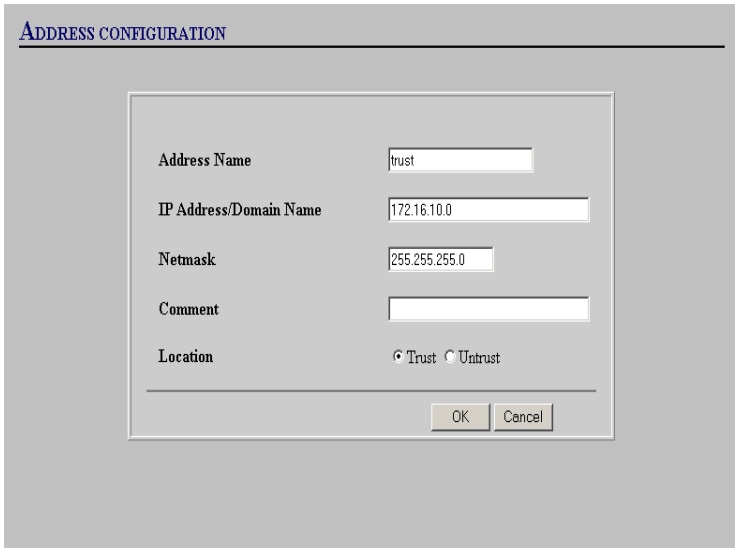
Setting Up the Netscreen for L2TP and IPSEC Pre-Shared IKE

1. First step is to create a IKE and L2TP user within the Netscreen through the WEBUI in the user section. The IKE identity must match the ID type in the Netscreen Remote Client in the MY Identity section.

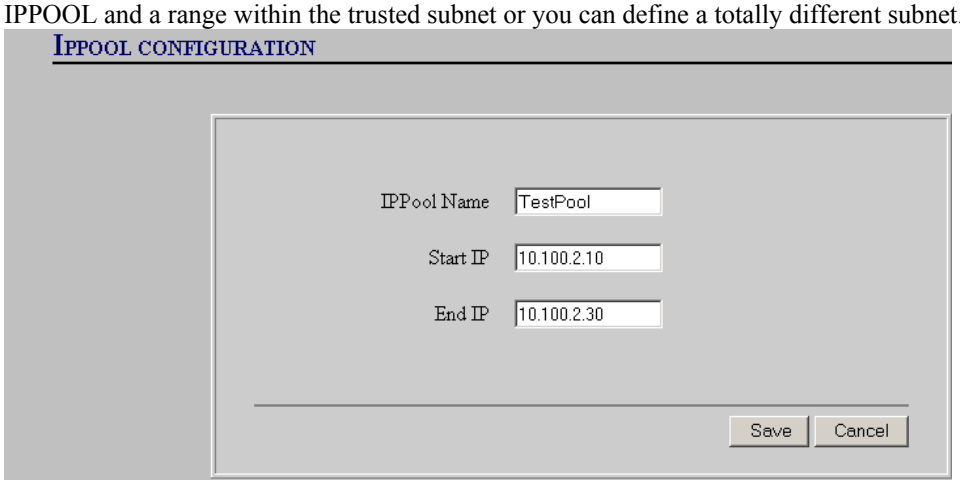
.



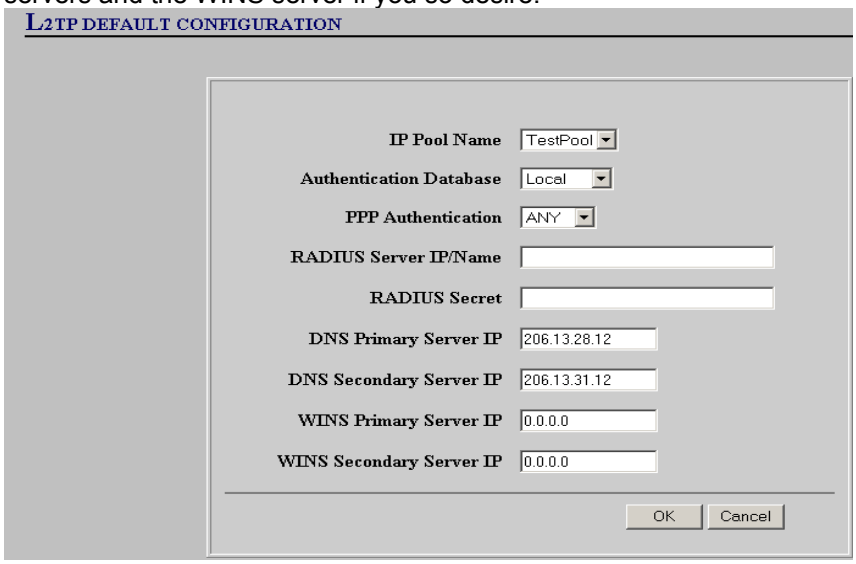
2. Go to the Address book and enter the Network Address of the trusted subnet that you want to access.



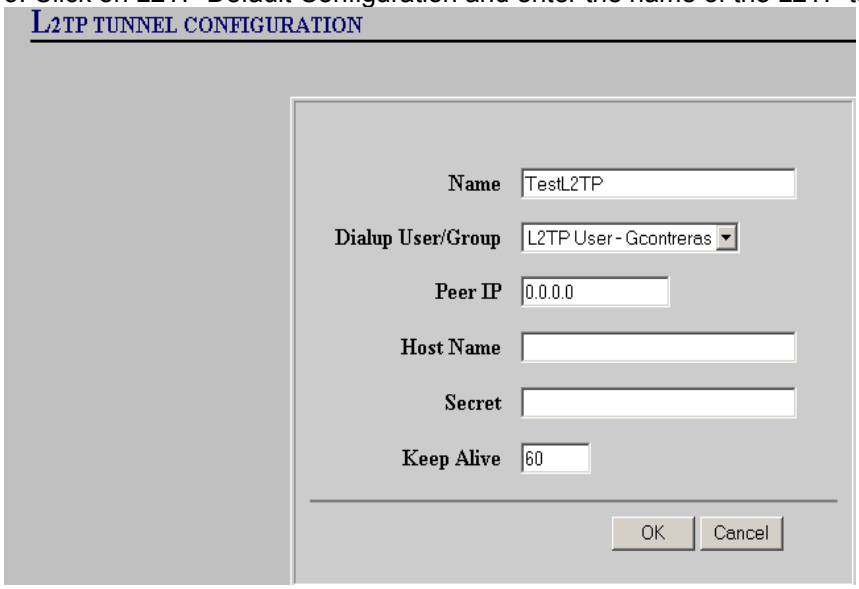
3. You must then go the VPN section and select IPPOOL, select New IPPOOL, enter the name of the IPPOOL and a range within the trusted subnet or you can define a totally different subnet.



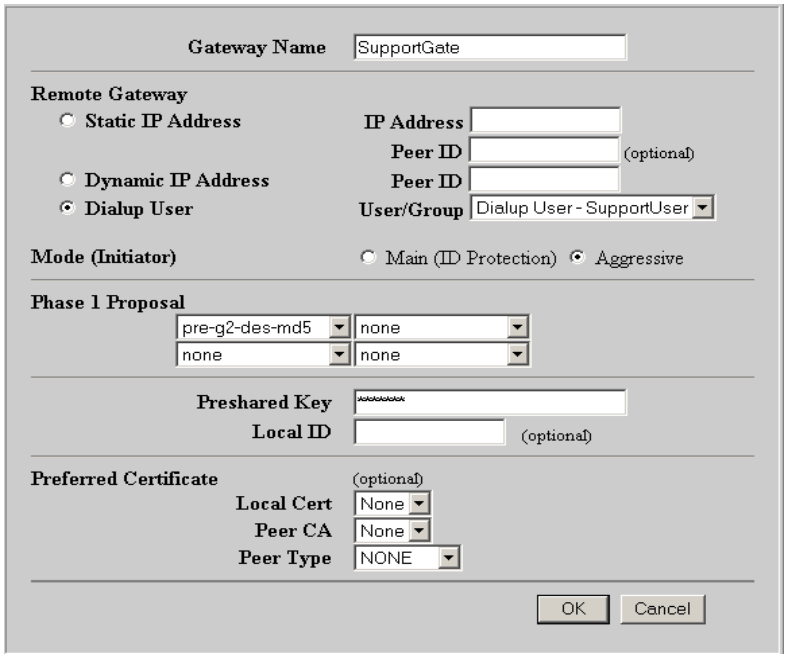
4. Click on the L2TP Default Configuration. You must enter the primary and secondary DNS servers and the WINS server if you so desire.



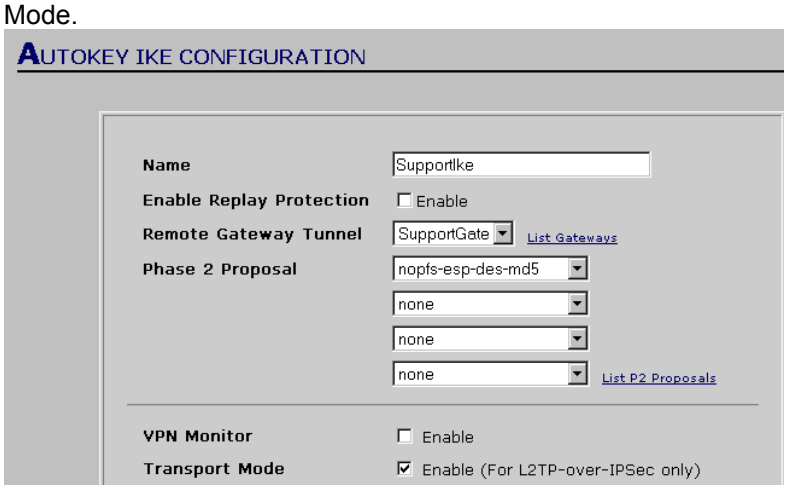
5. Click on L2TP Default Configuration and enter the name of the L2TP tunnel.



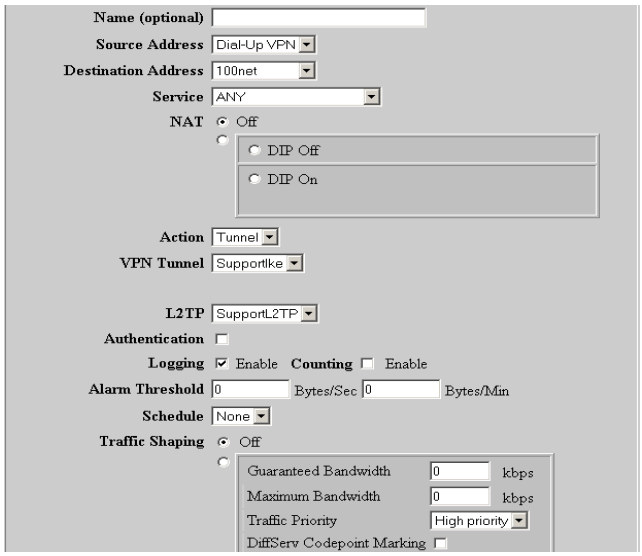
7. You must go to the VPN section of the Netscreen select gateway. Once you are there you must select the “Dialup User” then select the dialup user that you created, select Aggressive Mode, select the desired Phase 1 Proposal, and click OK. The remote client requires at least eight characters for the pre-shared key.



8. Click on the AutoKey IKE section, enter the desired name of the IKE Auto section, select the correct Remote Gateway Tunnel Name, then select desired Phase 2 proposal, select Transport Mode.



9. Click on the policy section, click on the incoming section, select “Dial-Up VPN” for the Source Address, select “Inside Any” or the address that you prefer for Destination Address, select “Any” for the service, click on “Tunnel” for the Action, select the correct tunnel for VPN Tunnel, select L2TP tunnel name for the L2TP section, and you can select Logging or Counting if you so desire. In ScreenOs 3.1 you will need to select from the Untrust Zone to Trust Zone before you configure the policies. If you created custom zones please make sure that there you have the correct routes set so the traffic can get to the correct zones. If you use the default Trust and Untrust zones you do not need to add any additional routes other than the default route “0.0.0.0 0.0.0.0 gate x.x.x.x”.



5. You must now configure the Dial-Up Connection for Safenet L2TP in the Windows 98 and ME section: Windows menu-dialog path:
My Computer=>Dial-Up Networking.
Before you can do these steps you must make sure that you load Microsoft VPN client. This can be done the right click on Network Neighborhood > Properties > add > client > VPN.

6. Click on Make New Connection then click on next

7. Under “Select a device” select Safenet VPN1 adapter then click on next.

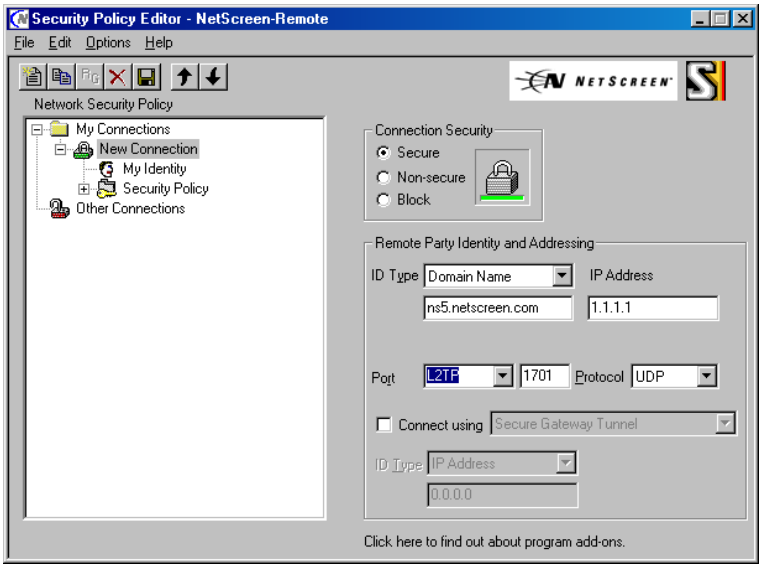
8. In the Host name or IP address: enter the IP address of the Netscreen’s Untrust interface click next then click on finish

9. Enter the Username and password of the L2TP user.

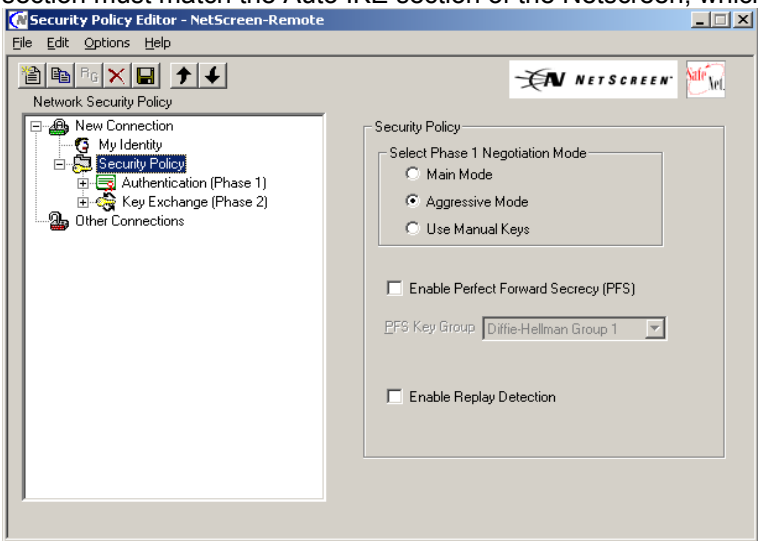
10. This completes the configuration of the L2TP user on the Windows 98 and ME. You must come back and click on connect when you are done with Netscreen Remote Client.

Netscreen Remote Client Setup

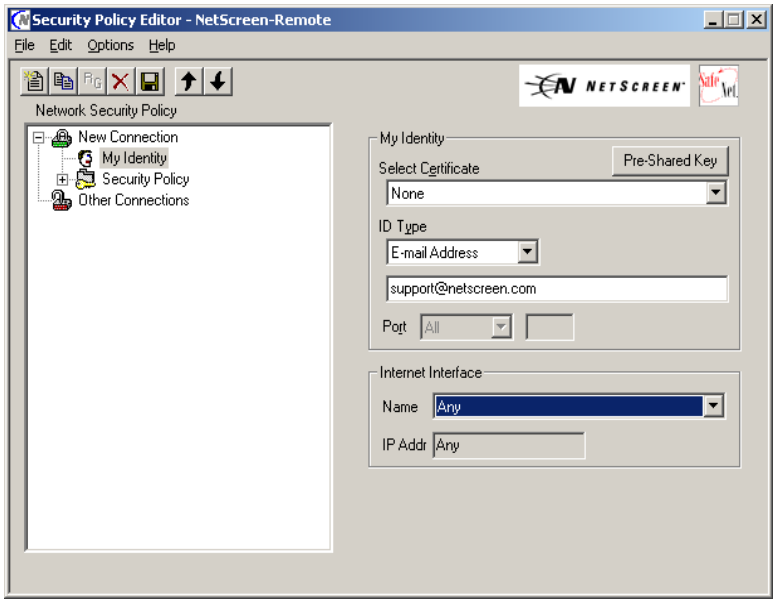
1.Bring up the Netscreen Remote Client Security Editor. Make sure that Secure is selected for the Connection Security, under the Remote part Identity and Addressing select domain name or IP address and input the domain name of the Netscreen or the IP address of the Netscreen, select L2TP for the port and UDP for the protocol.



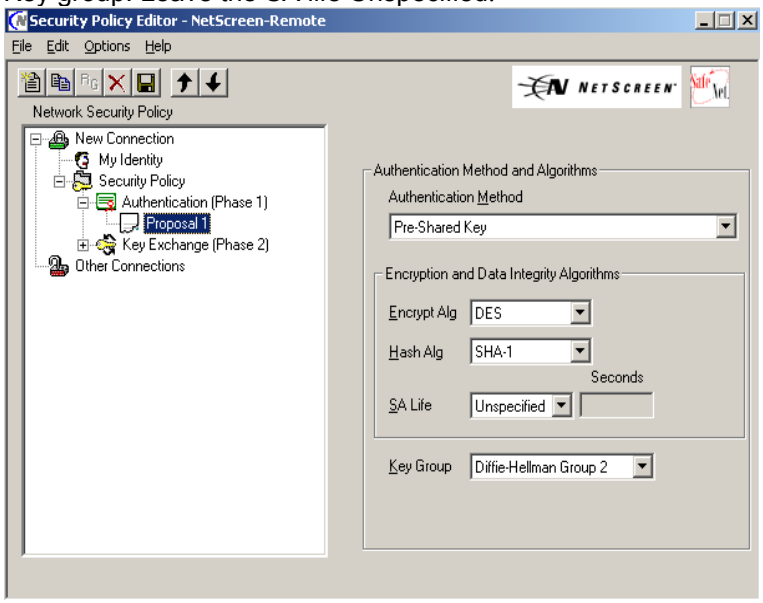
2. Double Click on the Security policy section and select aggressive mode. Remember that this section must match the Auto IKE section of the Netscreen, which is the second proposal.



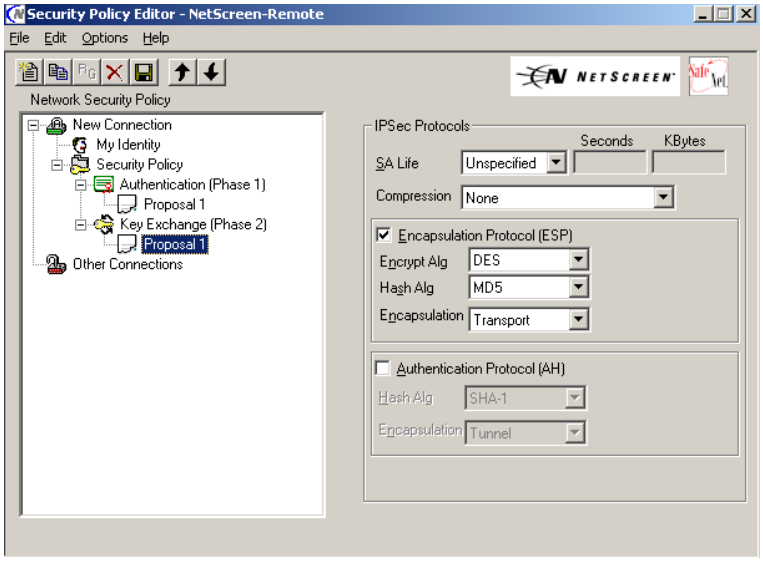
3. Go to the My Identity section, click on Pre-shared key and enter a password, select an ID type (This is very important because it must match the identity that you entered in the dialup users section. You can select “Internet Interface” and select the Name of the adapter, this is optional.



4. Make sure that Preshared key is selected under the Authentication Method, The Preshared key must be at least eight characters, select the desired encryption algorithm & hash algorithm & and Key group. Leave the SA life Unspecified.



5. Go the Key Exchange (Phase 2) Section and select Proposal 1. Select Encapsulation Protocol (ESP) and enter the desired Encryption and hash Algorithm. You must then select Transport for the Encapsulation. You must now save your configuration of the remote client by clicking on the floppy icon or going to file than selecting save.



Testing the Tunnel and Debugging
At this point, you are done with the initial configuration. You must go back to the connection you created for the WIN2K L2TP connection and enter the password to connect. You must have a connection to the internet or LAN to test this connection. If all goes well, you should be able to ping across to the trusted network. Typically, you will find the first 5-8 pings fail, but afterwards, a reply will come back after the tunnel has been created. To troubleshoot matters, on WIN2K to Netscreen useful debugging commands are

debug l2tp 1
debug ike 10

Note: For the ScreenOs 2.6.1 and above you have an option to debug ike basic, debug ike detail or debug ike trace

debug flow basic
get db stream.