

## Chapter Twenty (e): SafeNet SoftRemote Client

### Summary of Chapter:

- How to add a VPN tunnel via SafeNet SoftRemote Client.

### What you need:

- SafeNet SoftRemote Client software installed on your PC.
- An IPSec Road Warrior profile set-up on the Pilot.
- VPN installed on your Pilot. Please see Chapter 20(d) for further information.

### Software Revision Required:

- Applicable to software revision 5.2.0 > NetPilots

(NetPilot will be referred to as 'Pilot'. All image examples are of a NetPilot.)

### Entering your Connections Details:

- Open the 'Security Policy Editor'.



- If the 'S' symbol in the taskbar is grey, (as shown left) right click this symbol and select 'Activate Security Policy' from the menu given. The symbol will become yellow.

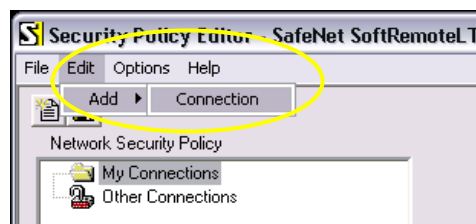


- If the 'S' symbol is yellow, (as shown left) double click the symbol to open the Editor.

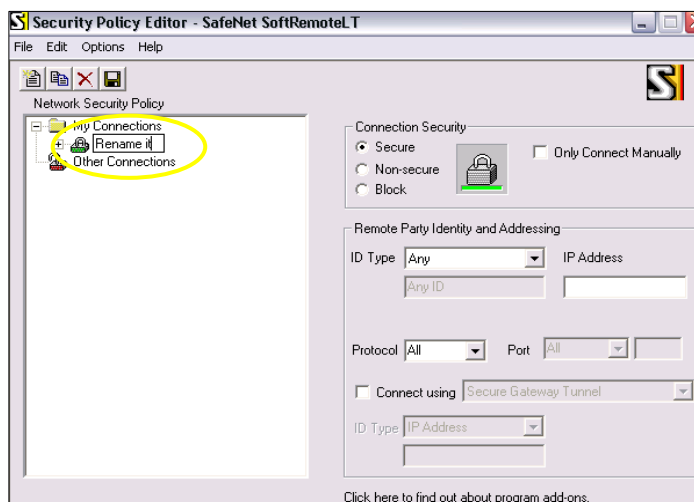
- You will be presented with the below screen:



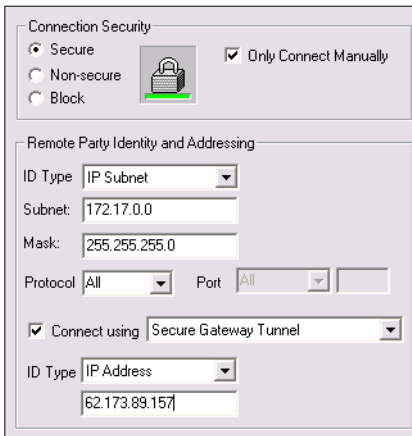
- To add a new connection, select 'Edit', 'Add' and then 'Connection' from the toolbar, as shown below:



- The Editor window will look similar as below. Rename the new connection as shown.



On the right side of the window, enter in the following details:



**‘Connection Security’ panel:**

‘Only Connect Manually’: put a tick in the box.

**‘Remote Party Identity and Addressing’ panel:**

‘ID Type’: Select ‘IP Subnet’

‘Subnet/Mask’: Enter the Pilots ‘LAN 1’ IP address

‘Connect using’: put a tick in the box.

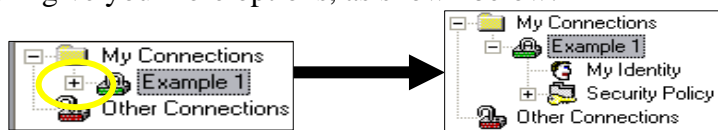
In the drop down text box next to the ‘Connect using’ tick box select ‘Secure Gateway Tunnel’

‘ID Type’: select ‘IP Address’ from the drop down box.

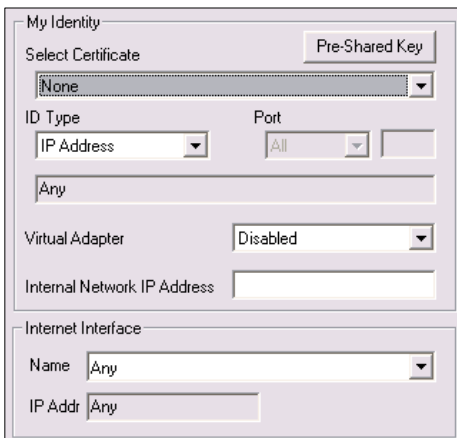
In the text box, enter the ‘LAN 2’ IP Address of the Pilot.

**Entering Further Details:**

Select the plus sign next to the new connection that you have added in the left-hand column; this will give you more options, as shown below:



Select ‘My Identity’ and you will be presented with two panels, as shown below:

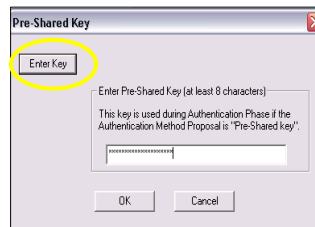


Enter the following details.

**‘My Identity’ panel**

‘Select Certificate’: Select ‘None’, a new button will appear on the window.

‘Pre-Shared Key: this button will open a new window.



Select the ‘Enter Key’ button, and enter your pre-shared key in the text box provided and select ‘OK’.

‘Virtual Adapter’: in the drop down box choose ‘Required’

‘Internal Network IP Address’: enter a unique IP Address from the scope which you have entered into the Pilot Roadwarrior Profile on the ‘Static Route’ screen.

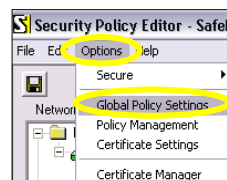


Enter a unique IP Address that is not being used on the Pilot!!



If you do not have the ‘Internal Network IP Address’ text box as an option in the above screen, please follow the below instructions.

Select ‘Options’ and then ‘Global Policy Settings’ from the toolbar, as shown right.



A new window will appear as shown left.

Enter in the following:

‘Retransmit Interval (seconds)’: 15

‘Number of retries’: 3

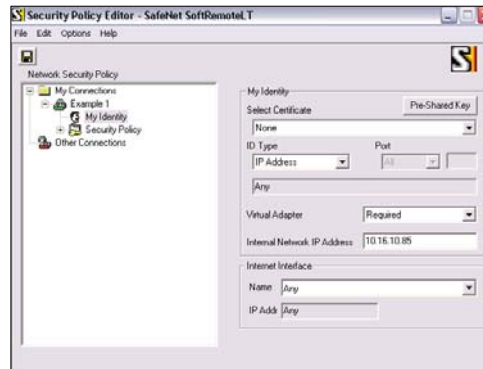
Tick the following boxes:

‘Send status notifications to peer hosts’

‘Allow to Specify Internal Network Address’

Select ‘OK’ to confirm.

Once you have entered in the correct details the screen will look similar as below:

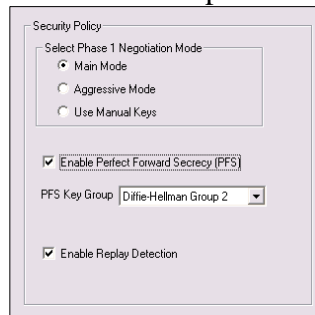


## Setting the Security Policy:

Select the 'Security Policy' option in the left-hand column as shown below:



You will be presented with the below screen:



'Enable Perfect Forward Security' put a tick in the box.

'PFS Key Group', in the drop down text box select 'Diffie-Hellman Group 2'.

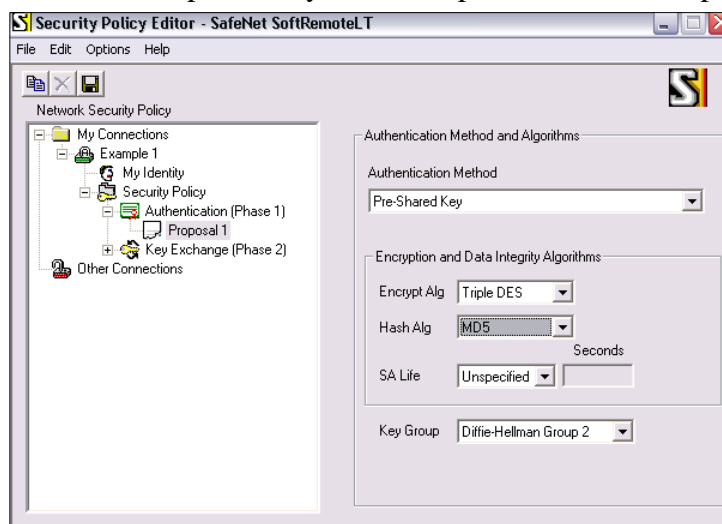
## Setting the Authentication Method:

Select the plus sign next to 'Security Policy' in the left-hand column, as shown below:



Select 'Authentication (Phase 1)'; this will give you another option called 'Proposal 1'.

Select 'Proposal 1', you will be presented with the panel shown below:



Select the following:

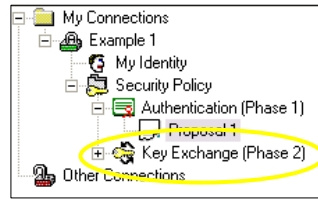
'Encrypt Alg': Triple DES

'Hash Alg': MD5

'SA Life': Unspecified

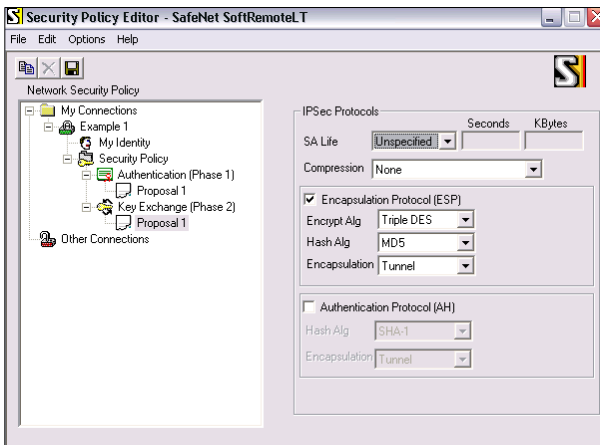
## Setting IPsec Protocols:

1. Select the plus sign next to 'Key Exchange (Phrase 2)' in the left-hand column, as highlighted below:



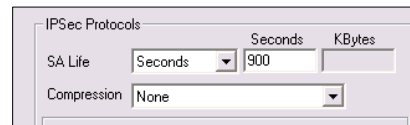
2. This will give you another option called 'Proposal 1'.

3. When you select 'Proposal 1' you will be presented with a similar screen as below:



Select the following:

4. 'SA Life': You can leave this as 'Unspecified' or select 'Seconds' and specify the amount as shown below. (8 hours is the maximum time limit)



5. 'Compression': None

6. 'Encrypt Alg': Triple DES

7. 'Hash Alg': MD5

8. 'Encapsulation': Tunnel

## Saving:

9. To save the profile you have created, select the save icon, which is located in the top left corner and highlighted below:



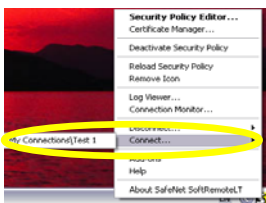
10. Or you can select 'File' and 'Save' from the toolbar.

11. Once you have saved the profile, close the 'Security policy Editor' window.

## Testing:

12. Connect to the Internet and browse to any web site, to test the connection.

13. Right hand click on the 'S' symbol in the taskbar and select 'Connect', your profile will be shown here.



Once you have selected the profile, which you created earlier, the software will try to connect you and you will be presented with a pop up window. This window will tell you if your connection was successful or failed to connect. Once you have established this select 'OK'.



**Tip!** If the connection does not work, please check that the shared keys entered are the same on the Pilot and on the Client.

14. If it is successful and you would like to test the connection, ping the Pilots 'LAN 1' IP address. To do this, open a 'Command prompt' (To select this go to 'Start', 'All Programs', and 'Accessories'). Once you've selected this, ping the 'LAN 1' IP address of the Pilot. (The default LAN is 10.0.0.1, but you may have changed this).



**Information** On the NAT device allow port 4500 UDP and 500 UDP out. If you are not sure on how to do this, please contact your network administrator.