VIRTUAL ACCESS
Service Provider Solutions

Service Managed Gateway™

How to Configure a VPN Client Against the Gateway

Issue 1.1

Date 14 August 2007

1 Introduction

1.1 What is a VPN client?

The VPN client is used to allow remote users to connect into an SMG headend box over a VPN IPSec tunnel. The VPN client resides on the remote user's laptop or PC and allows the remote user to access remote network security.

2 How to configure IPSec tunnels in the Expert Web of the Gateway

To configure an IPSec tunnel, you must configure 1 IKE policy and 2 SPD policies.

1. In the Expert View of the Gateway, select **system** – **vpn** – **ike**. The IKE Policy Configuration List page is displayed.

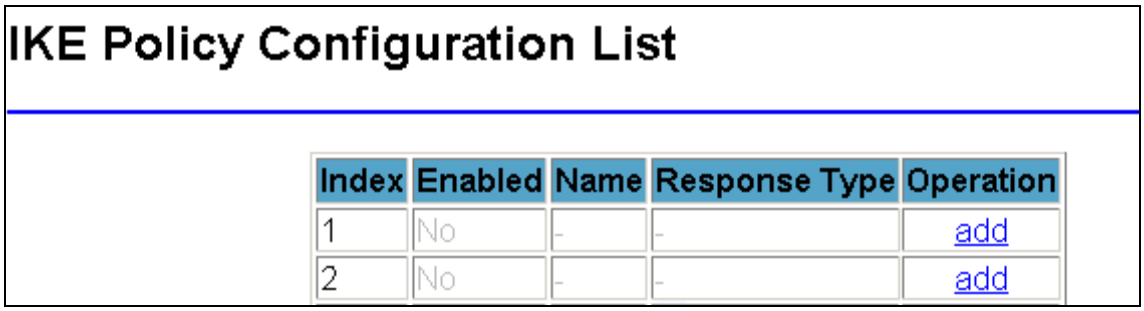

Figure 1: Click add in the row of an IKE that is available

2. Click **add** in the row of an IKE that is available. The IKE Policy Configuration page is displayed.

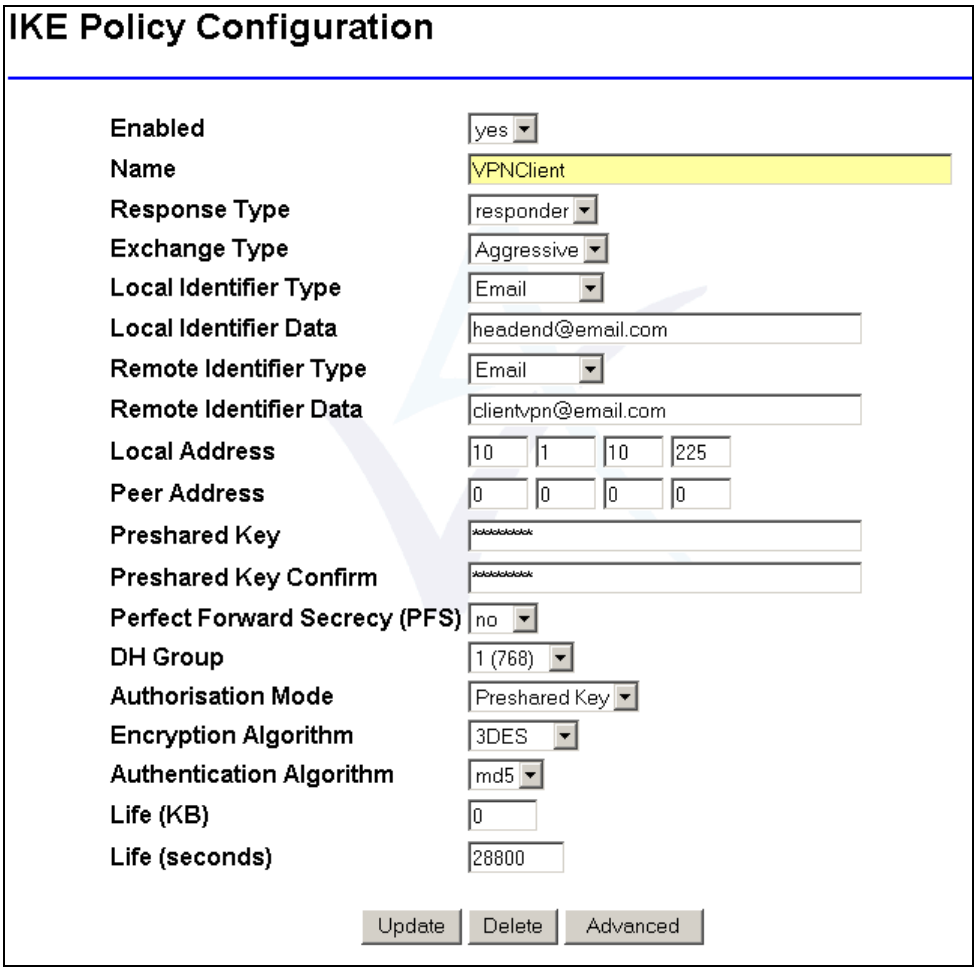

Figure 2: Specify the settings for the IKE policy

3. Specify the appropriate settings for the IKE policy. Figure 2 is an example. For more information about the settings, read the page on IKE Policy Configuration

in the **Full Reference Guide for the Expert Web of your Service Managed Gateway**.

4. In the Expert View of the Gateway, select **system** – **vpn** – **spd 1-50** or **system** – **vpn** – **spd 51-100**. The SPD Policy Configuration List is displayed.

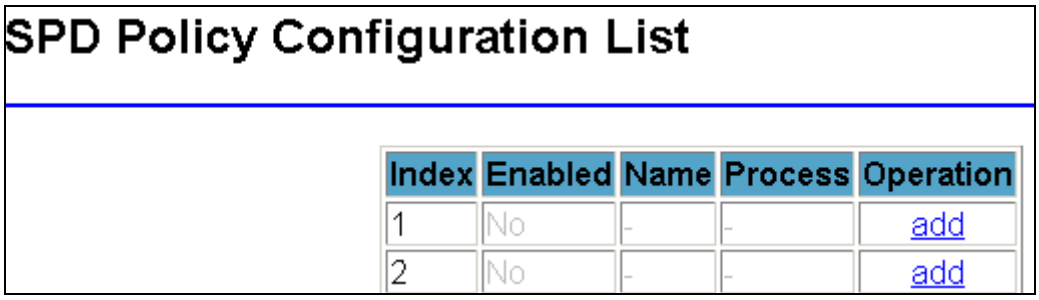

Figure 3: Click add in the row of an SPD policy that is available

5. Click **add** in the row of a policy that is available. The SPD Policy Configuration page is displayed.

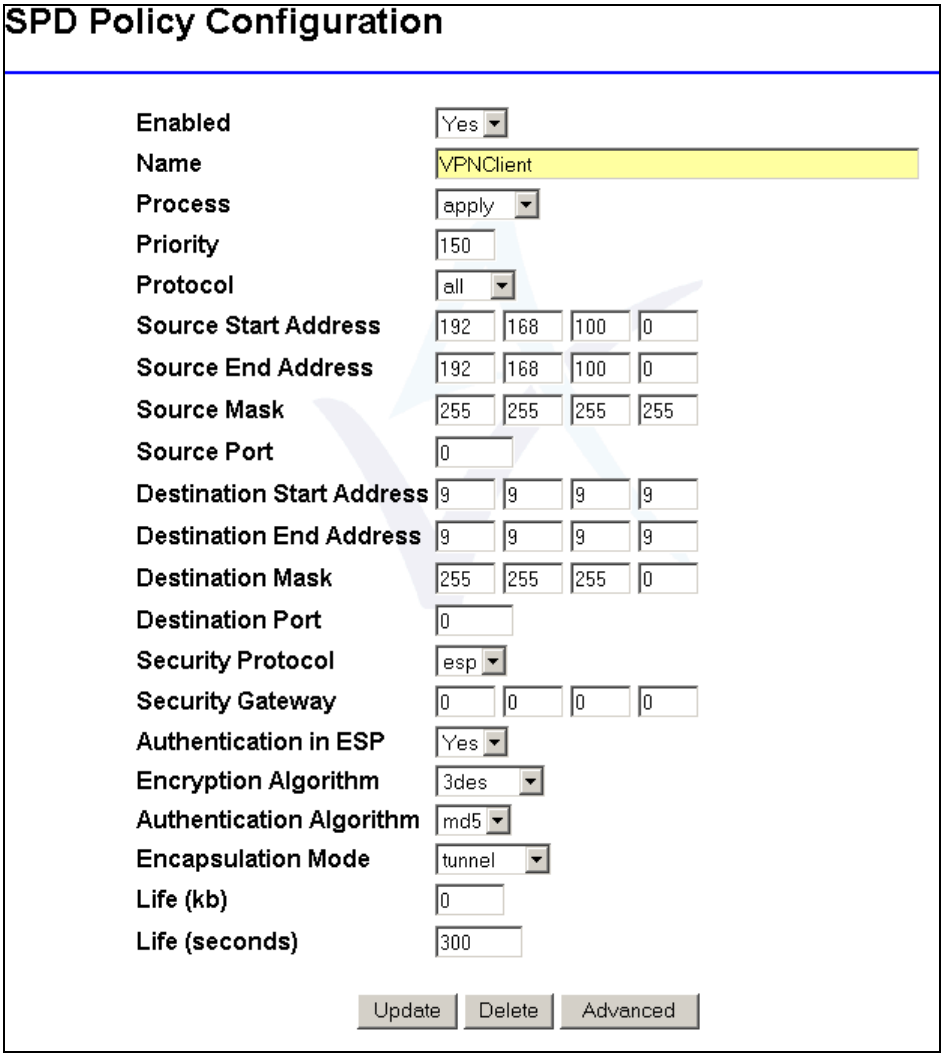

Figure 4: An example of settings for tunnel 1

6. Specify the appropriate settings for the first tunnel. Figure 4 is an example.

   For more information about the SPD policy settings, read the page on SPD Policy Configuration in the **Full Reference Guide for the Expert Web of your Service Managed Gateway**.

7. Click **Update**. The tunnel is configured.

8. In the SPD Policy Configuration List, click **add** in the row of a policy that is available. The SPD Policy Configuration page is displayed.

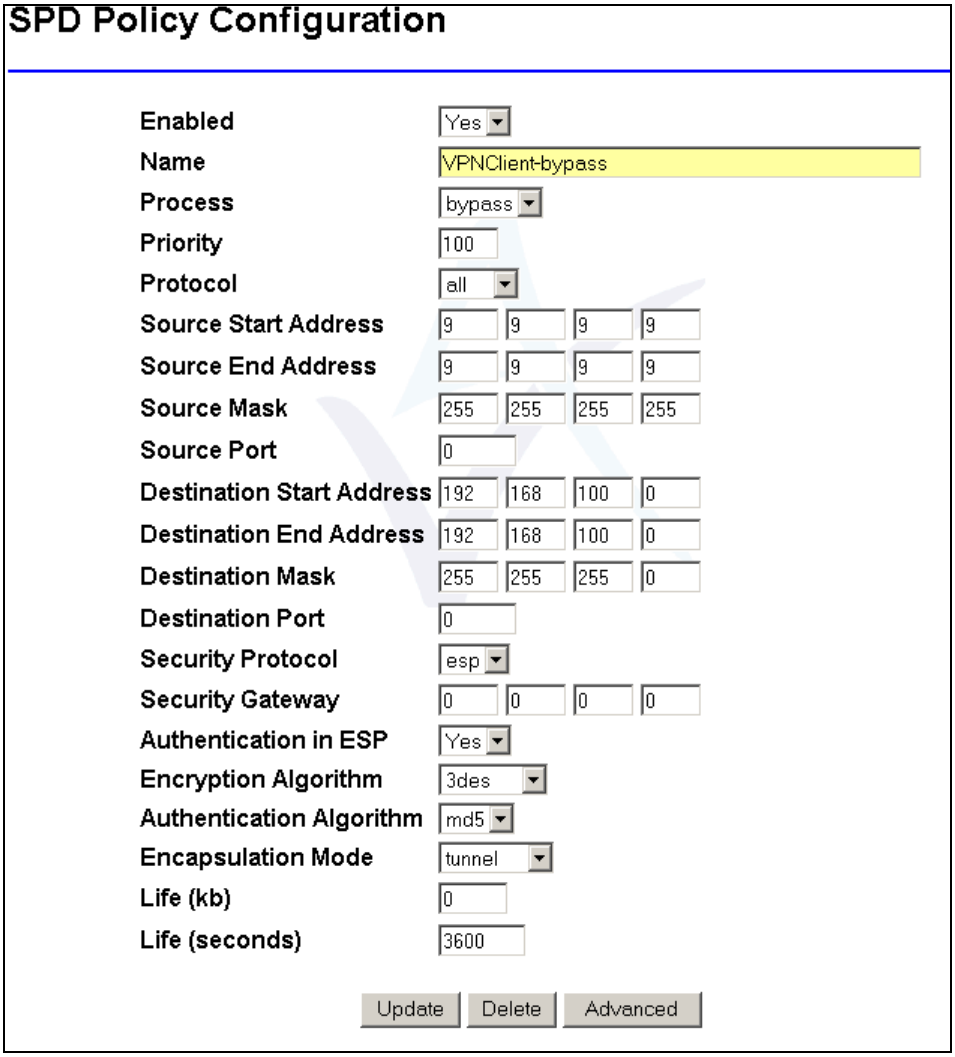

Figure 5: An example of the settings for tunnel 2

9. Specify the appropriate settings for the second tunnel. Figure 5 is an example.

   For more information about the SPD policy settings, read the page on SPD Policy Configuration in the **Full Reference Guide for the Expert Web of your Service Managed Gateway**.

10. Click **Update**. The tunnel is configured.

3 How to configure the SafeNet SoftRemote client

The VPN client software must be installed on your computer.

1. Open the SafeNet SoftRemote client. The Security Policy Editor window appears.

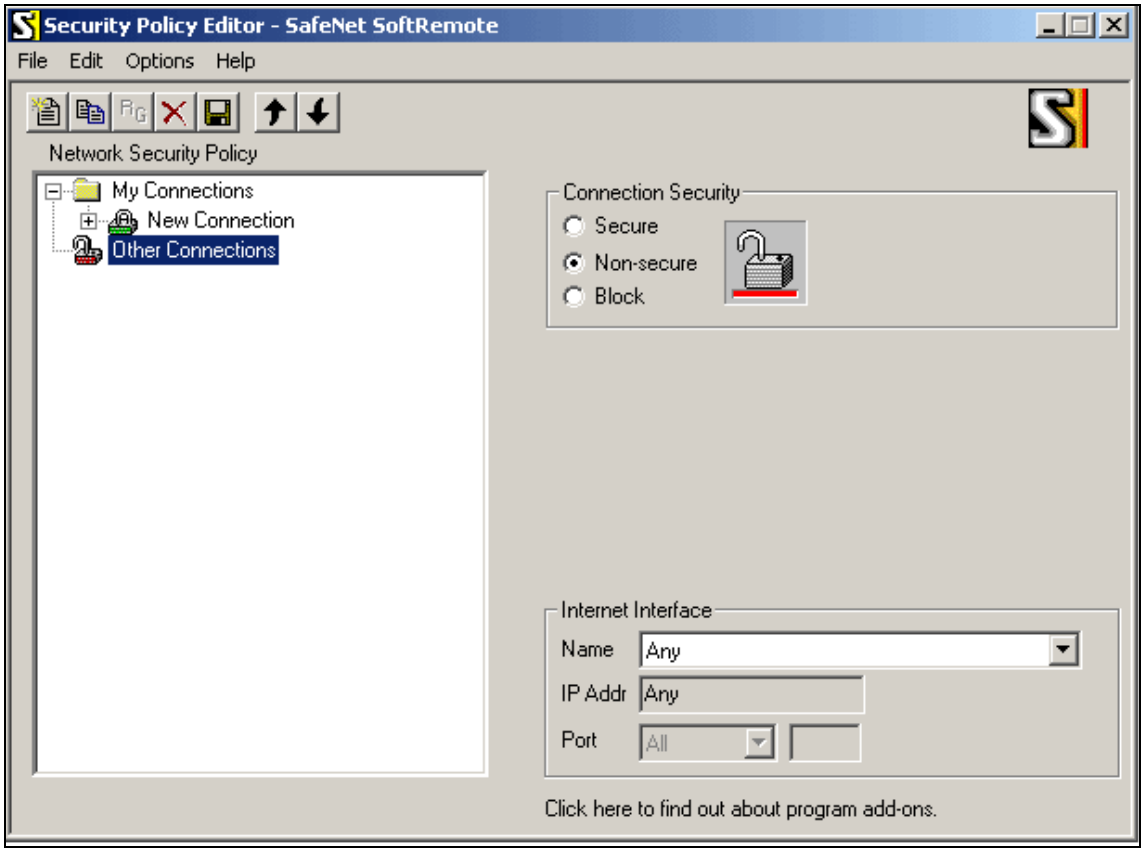

Figure 6: The Security Policy Editor

2. Right click **Other Connections** in the Network Security Policy window. Select **Add** from the pop-up menu.

3. Select **To VA Headend** in the menu.

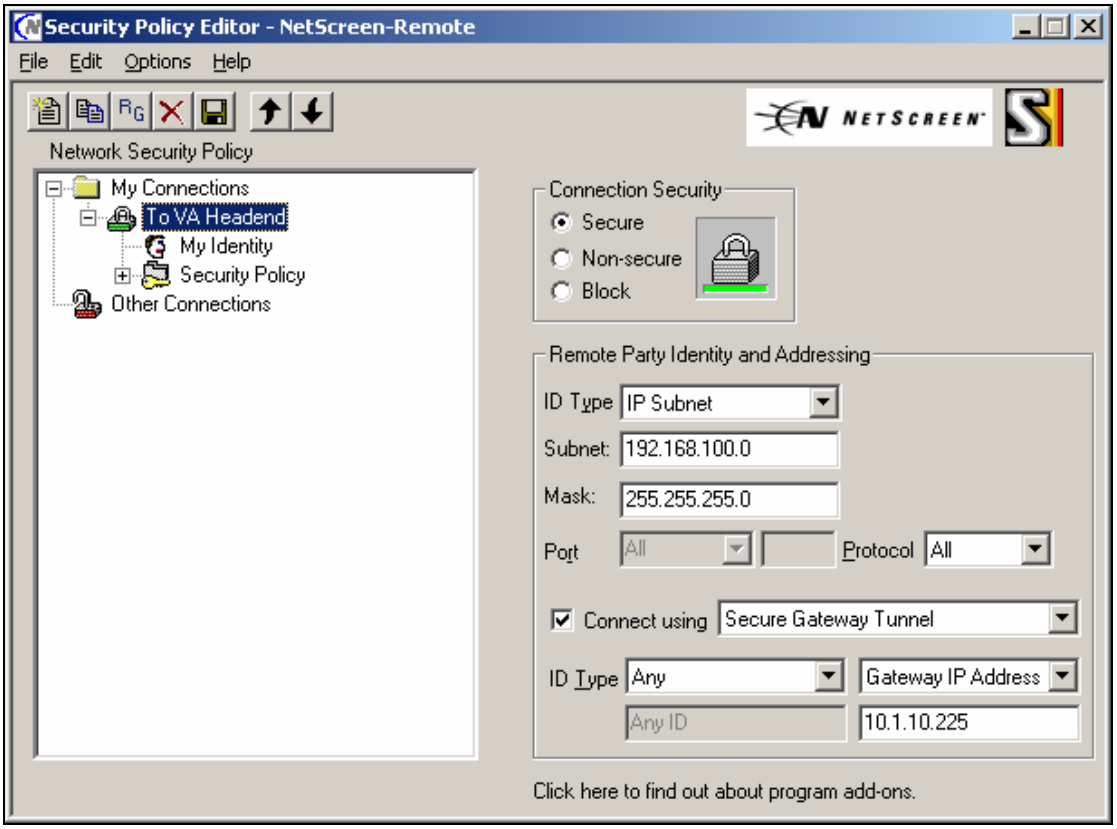

Figure 7: Select To VA Headend and specify the details

4. Select **Secure** in the Connection Security section of the window.
5. Specify the details in the Remote Party Identity and Addressing section of the window.

6. Select **My Identity** in the menu.

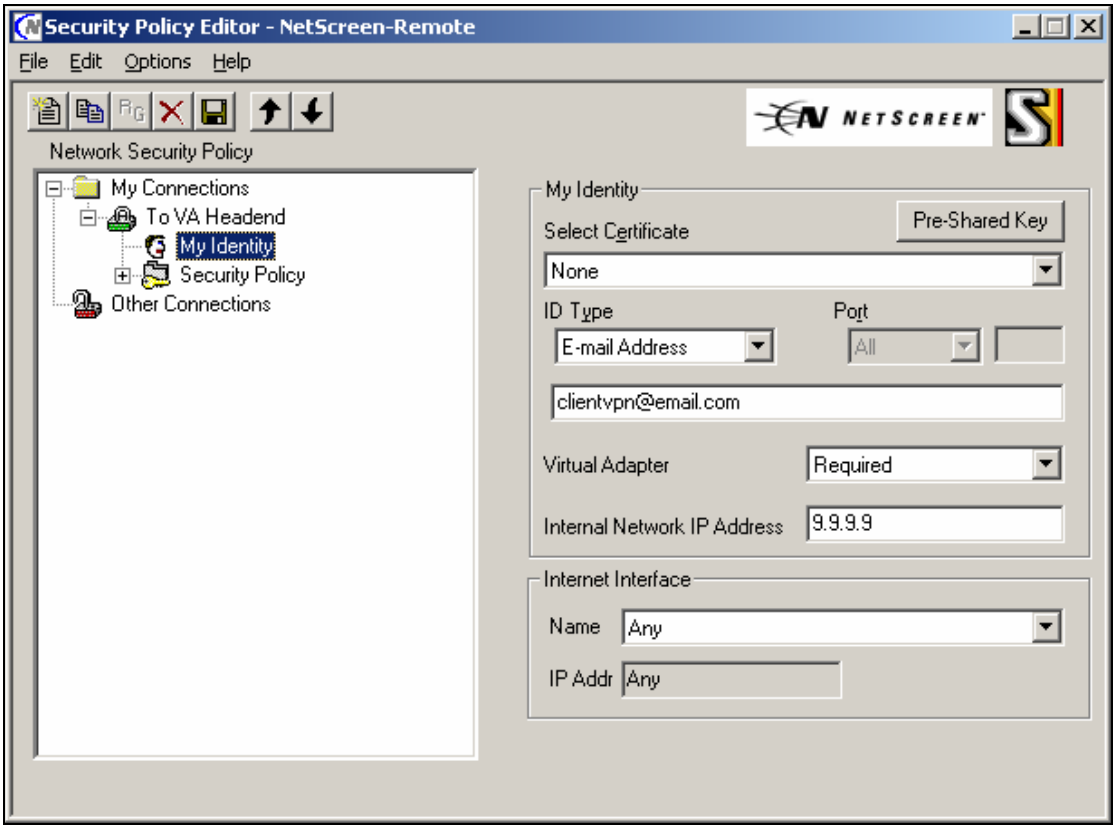

Figure 8: Select My Identity and specify the details

7. Specify the details in the My Identity section of the window.

8. Select **Security Policy** in the menu.

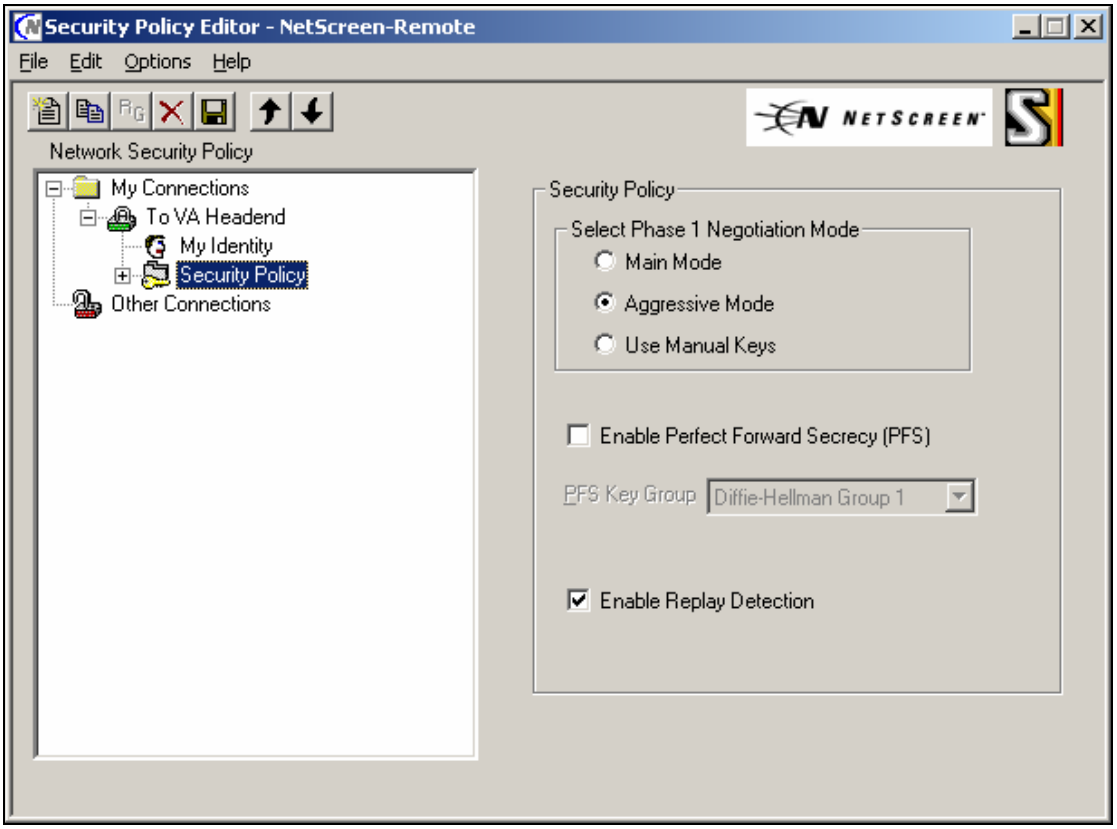

Figure 9: Select Security Policy in the menu and specify the details

9. Specify the details in the Security Policy section of the window.

4 How to configure the Microsoft VPN client

1. Install the Microsoft IPSec Policy Configuration Tool if it is not installed already. You can download the installation file from http://www.microsoft.com/downloads/details.aspx?FamilyID=7d40460c-a069-412e-a015-a2ab904b7361&displaylang=en.

2. To configure the tunnel from the client PC to the LAN, open a command prompt. At the prompt, type the command in Figure 10. Table 1 explains the arguments and parameters of the command.

```
ipsecpol –f A.B.C.D/255.255.255.255=A.B.C.D/
255.255.255.0 -t A.B.C.D -1s 3DES-MD5-2 -n ESP[3DES,MD5]3600S
-1p -a PRESHARE:xxxxxxxxxxxxxxxxx –lan
```

Figure 10: The command to configure an IPSec tunnel from a client PC to the LAN

Element in the command	Description
–f	Flag to specify the policy list.
First IP address: A.B.C.D/255.255.255.255	The address of the client PC.
Second IP address range: A.B.C.D/255.255.255.0	The address range of the LAN.
Third IP address: –t A.B.C.D	The address of the Gateway to the LAN.
–t	Flag to specify the tunnel list.
–s	Flag to specify the security method.
Security methods: • Encryption algorithm • Authentication algorithm	The security parameters. The parameters must match what is configured on the Gateway. Figure 10 shows the security parameters for a typical installation. These are equivalent to the IKE security settings on the Gateway.
–n	Flag to specify the IPSec policies.
VPN authentication and encryption parameters: • Encryption algorithm • Authentication algorithm • Life (seconds)	The VPN parameters. The parameters must match what is configured on the Gateway. Figure 10 shows the VPN parameters for a typical installation. These are equivalent to the SPD security settings on the Gateway.
-1p	Flag to enable perfect forward security for phase 1.
–a	Flag to enable the authentication method.
PRESHARE: followed by the preshared key.	Preshared Key. The preshared key must be at least 16 ASCII characters.
–lan	Flag to set the LAN policy

Table 1: Arguments and parameters for the ipsecpol command when you configure a tunnel from the client PC to the LAN

3. Press Return.

4. To configure the tunnel from the LAN to the client PC, at the command prompt, type the command in Figure 11. Table 2 explains the arguments and parameters of the command.

```
ipsecpol –f A.B.C.D/255.255.255.0=A.B.C.D/
255.255.255.255 -t A.B.C.D -1s 3DES-MD5-2 -n ESP[3DES,MD5]3600S
-1p -a PRESHARE:xxxxxxxxxxxxxxxxxx –lan
```

Figure 11: The command to configure an IPSec tunnel from the LAN to the client PC

Element in the command	Description
–f	Flag to specify the policy list.
First IP address: A.B.C.D/255.255.255.0	The address range of the LAN.
Second IP address range: A.B.C.D/255.255.255.255	The address of the client PC.
Third IP address: –t A.B.C.D	The address of the Gateway to the LAN.
–t	Flag to specify the tunnel list.
IP address: A.B.C.D	The address of the tunnel.
–s	Flag to specify the security method.
Security methods: • Encryption algorithm • Authentication algorithm	The security parameters. The parameters must match what is configured on the Gateway. Figure 10 shows the security parameters for a typical installation. These are equivalent to the IKE security settings on the Gateway.
–n	Flag to specify the IPSec policies.
VPN authentication and encryption parameters: • Encryption algorithm • Authentication algorithm • Life (seconds)	The VPN parameters. The parameters must match what is configured on the Gateway. Figure 10 shows the VPN parameters for a typical installation. These are equivalent to the SPD security settings on the SMG.
-1p	Flag to enable perfect forward security for phase 1.
–a	Flag to enable the authentication method.
PRESHARE: followed by the preshared key.	Preshared Key. The preshared key must be at least 16 ASCII characters.
–lan	Flag to set the LAN policy.

Table 2: Arguments and parameters for the ipsecpol command when you configure a tunnel from the LAN to the client PC

5. Press Return.

The tunnels are configured. You should be able to ping across the VPN tunnel.