Safenet IPSEC VPN

Firmware V2.26

July 2002

Firmware V2.26
Client IPSec to VPN router

2.0 Setup Procedure

Test setup

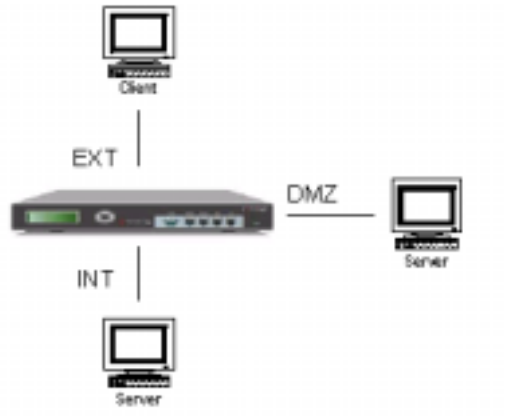


Diagram 1.1 – network equipment layout for Client IPSec to DFL-xxx VPN.

Setup assumes an internet connection has been provided and exists between the DFL-xxx external interface and the target client. The client's network has not been illustrated for it is generally under customer control and may be of numerous configurations (DSL modem, Cable modem, dialup Internet access, etc…) All configurations fall under two client configuration categories: Static client and Dynamic client.

2.1 Autokey IKE setup

DFL-xxx Autokey IKE setup

1. Go to **VPN > IPSEC > Autokey IKE**.
2. Select NEW to add a new Autokey IKE VPN tunnel.
3. Enter the VPN Tunnel Name, Remote Gateway, Keylife, and Authentication Key. When configuring **static** VPN client, enter the client IP address on the Remote Gateway; when configuring **dynamic** VPN client, enter 0.0.0.0 on the Remote Gateway.
4. Select the P1 Proposal and the P2 Proposal algorithms.
5. Select OK to save the Autokey IKE VPN tunnel.

Adding an Internal destination address: (Do not need a destination address for dynamic vpn client)

6. Go to **Firewall > Address > Internal**.
7. Select NEW to add a new internal address to the list.
8. Enter an Address Name, the IP Address, and the NetMask of the network to connect to the VPN.
9. Select OK to save the new internal address.

Adding an external destination address: (Do not need a destination address for dynamic vpn client)

10. Go to **Firewall > Address > External**.
11. Select NEW to add the address of the client.
12. Enter an Address Name, the static IP Address, and the Netmask of the client.
13. Select OK to save the destination address.

Complete the following procedure on the DFL-xxx VPN gateway to add the VPN policy. Do not need a policy for dynamic vpn client.

14. Go to **VPN > IPSEC > Policy**.
15. Select NEW to add a new IPSec VPN policy.
16. Select a Source address.
17. Select a Destination address.
18. Select the VPN Tunnel.
19. Select OK to save the VPN policy.

2.2 Manual key IPSec setup

DFL-xxx Manual key IPSec setup

1. Go to **VPN > IPSEC > Manual Key**.
2. Select NEW to add a new manual key VPN tunnel.
3. Enter the VPN Tunnel Name, Local SPI, Remote SPI, Remote gateway, Encrytion Algorithm and key, Authentication Algorithm and Key.
4. In the Remote Gateway field, enter the static IP address of the VPN client. To accept connections from more than one client, set the Remote Gateway address to 0.0.0.0.
5. Select OK to save the manual key VPN tunnel.

Adding an Internal destination address: (Do not need a destination address for dynamic vpn client)

6. Go to **Firewall > Address > Internal**.
7. Select New to add a new internal address to the list.
8. Enter an Address Name, the IP Address, and the NetMask of the network to connect to the VPN.
9. Select OK to save the new internal address.

Adding an External destination address: (Do not need a destination address for dynamic vpn client)

10. Go to **Firewall > Address > External**.
11. Select New to add the address of the client.
12. Enter an Address Name, the static IP Address, and the Netmask of the client.
13. Select OK to save the destination address.

Complete the following procedure on the DFL-xxx VPN gateway to add the VPN policy. Do not need a policy for dynamic vpn client.

14. Go to **VPN > IPSEC > Policy**.
15. Select NEW to add a new IPSec VPN policy.
16. Select a Source address.
17. Select a Destination address.
18. Select the VPN Tunnel.
19. Select OK to save the VPN policy.

3.0 Safenet Client IPSec setup

Safenet Client IPSec setup

The Security Policy Editor, shown in Figure 3-1, is the software module within the Safenet client where you create connections and their associated proposals.

Security Policy Editor

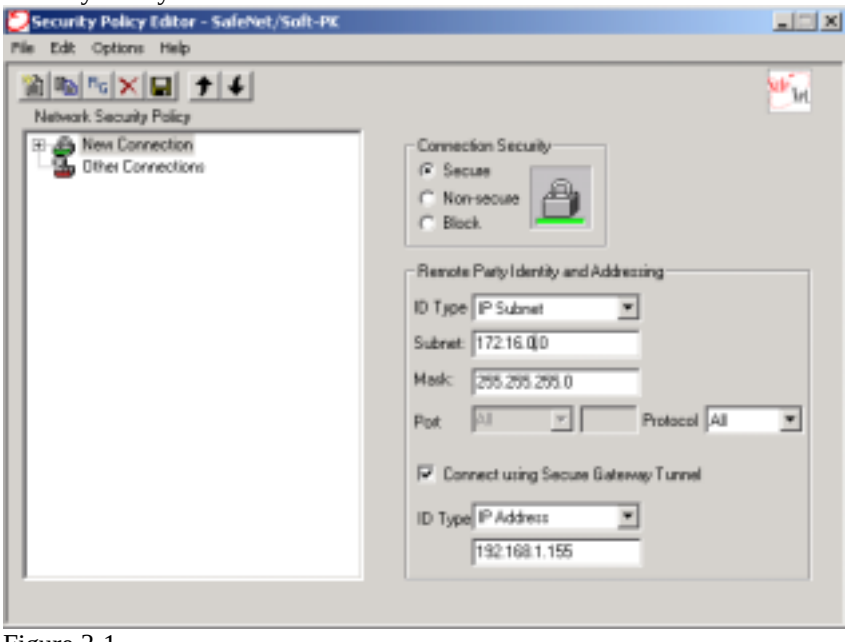


Figure 3-1

The Network Security Policy list displays a hierarchically ordered list of connections and their associated proposals.

The three Connection Security options refer to the type of security to apply to a connection:

1. **Secure:** This option secures communication for the connection.

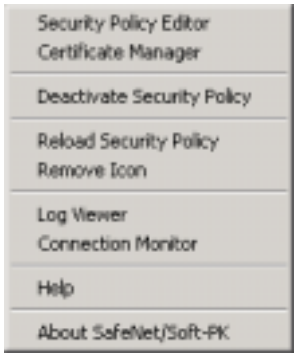

2. **Non-secure:** This option allows communication for the connection to pass through unsecured.

3. **Block:** This option does not allow any communication for the connection to pass through.

The Safenet icon appears in the status area of the taskbar in the lower-right corner of the Windows desktop, as shown below.

When you right-click the Safenet icon on the Windows taskbar, the Safenet shortcut menu pops up.

Safenet Shortcut Menu



Security Policy Editor opens the software module where you create and store connections and their associated proposals.

Certificate Manager opens the software module where you can request, import, and store digital certificates.

Deactivate Security Policy turns off the Safenet's monitoring of your communication activity so that no security policies are invoked when communicating with locations for which you have established a secure connection. When Safenet is deactivated, the **Deactivate Security Policy** command changes to **Activate Security Policy.**

Reload Security Policy replaces an existing security policy with a new security policy.

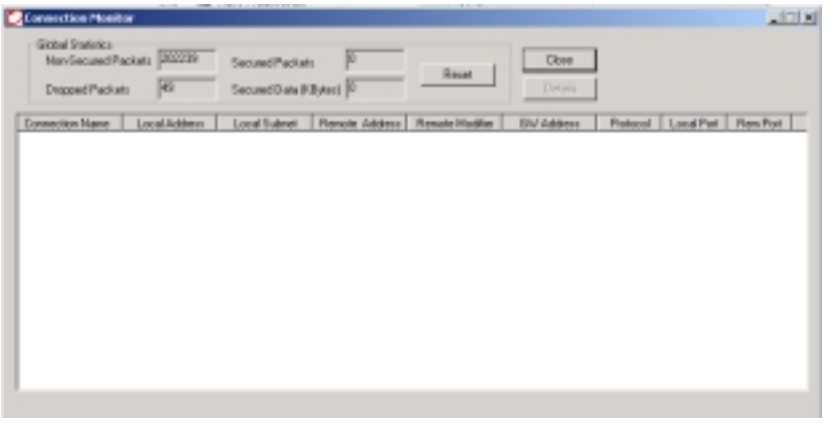
Note *Saving changes to the security policy of an active connection terminates that connection to implement the changes. To delay implementing the changes until you end the currently active connection, click* ***No*** *when Safenet prompts you to reset your active connection. Then click* ***Reload Security Policy*** *to put the changes into effect.*

Remove Icon removes the Safenet icon from the taskbar on your desktop. The icon reappears when you restart your computer.

Log Viewer opens the communication log, a diagnostic tool that lists Internet Key Exchange (IKE) negotiations as they occur.

Connection Monitor opens a window that displays statistical and diagnostic information for each active connection in the security policy. To see details, select a connection, and click **Details**.

Note *Safenet does not save log information; it is overwritten by ongoing IKE negotiations. To record log information, you must click* ***Freeze****, and then save or print it.*



3.1 Safenet Manual Key VPN

There are three steps to set up Safenet for a Manual Key VPN tunnel:

3.1.1 Creating a New Connection.

3.1.2 Defining the IPSec Protocols

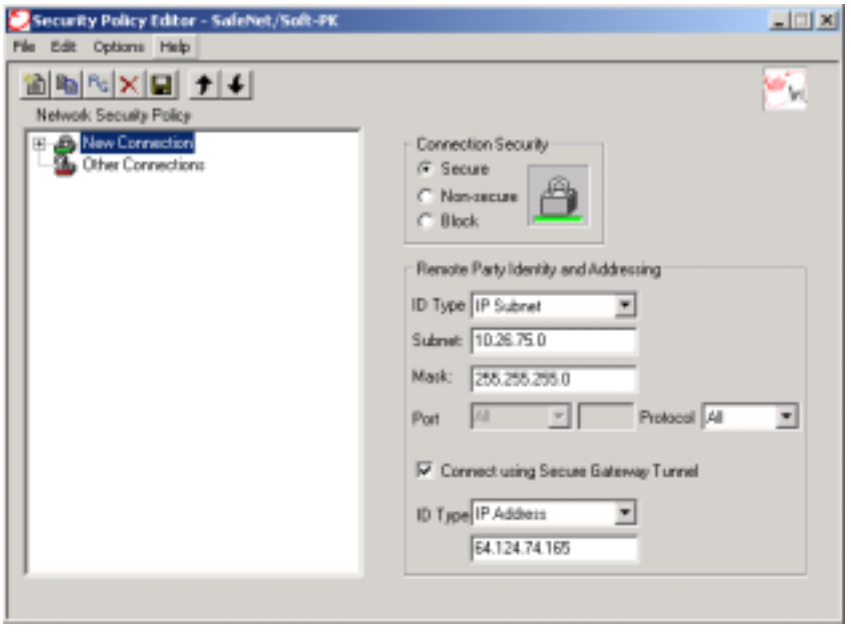
3.1.3 Creating the Inbound and Outbound Keys

3.1.1 Create a New Connection

Begin by initiating a new connection. Then name the connection, define its connection security, and determine the identification and location of the other end of the eventual VPN tunnel.

1. Double-click the **Safenet** icon, located on the Windows taskbar, to open the Security Policy Editor.
2. On the Edit menu, choose **Add,** then select **Connection**.

A new Connection icon appears in the Network Security Policy list, as shown below.



3. Give the new connection a unique name.
4. In the Connection Security area, select **Secure**.
5. In the Remote Party Identity and Addressing area, select an identifier for the other party from the ID Type list, and enter the required information.

   The choices are:

   IP Address—Enter the destination IP address in the IP address field.

Domain Name — Enter the domain name of the destination sub network.

E-mail Address — Enter the destination e-mail address.

IP Subnet — Enter the destination subnet IP address and subnet mask.

IP Address Range — Enter the start and end of the destination IP address range.

Distinguished Name — Click **Edit Name**, and enter information in the Subject Information fields. The information entered is linked together to create the distinguished name of the destination.

6. Define the protocol to use for the connection. The choices are:

   All — Allows the connection to use all of the following protocols.

   TCP — Transmission Control Protocol, the protocol that controls data transfer on the Internet

   UDP — User Datagram Protocol, a protocol within the TCP/IP protocol suite that provides very few error recovery services (for example, a lost packet is simply ignored) and is used primarily for broadcasting

   ICMP — Internet Control Message Protocol, a protocol tightly integrated with the Internet Protocol (IP) that supports packets containing error, control, and informational messages related to network operations

   GRE — Generic Routing Encapsulation, a protocol that encapsulates the packets of one kind of protocol within GRE packets, which can then be contained within the packets of another kind of protocol

Note *Entering an IP address in addition to the domain name, e-mail address, or distinguished name is optional. If "Connect using Secure Gateway Tunnel" is not selected, use any of the six ID types. If it is selected, however, only use IP Address, IP Subnet, or IP Address* Range.

7. If the other end of the eventual VPN tunnel is protected by a security gateway, select **Connect using Secure Gateway Tunnel**. The Secure Gateway Tunnel ID Type and IP Address fields become available.
8. For ID Type, select an identifier for the other party from the ID Type list, and enter the required information. The choices are:

   IP Address — Enter the security gateway IP address in the IP address field.

   Domain Name — Enter the domain name of the security gateway.

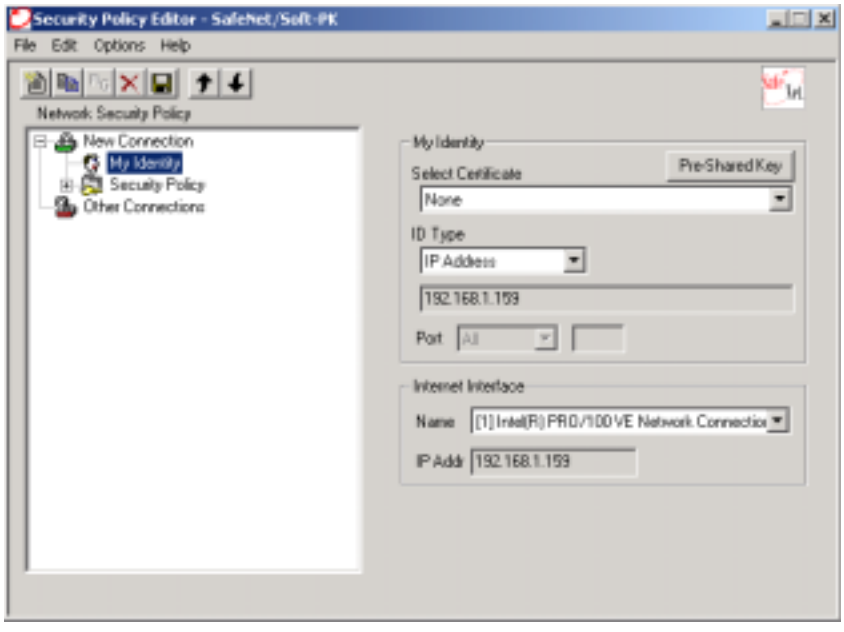
Distinguished Name — Click **Edit Name**, and enter information in the Subject Information fields. The information you enter is linked together to create the distinguished name of the security gateway.

3.1.2 Define IPSec Protocols

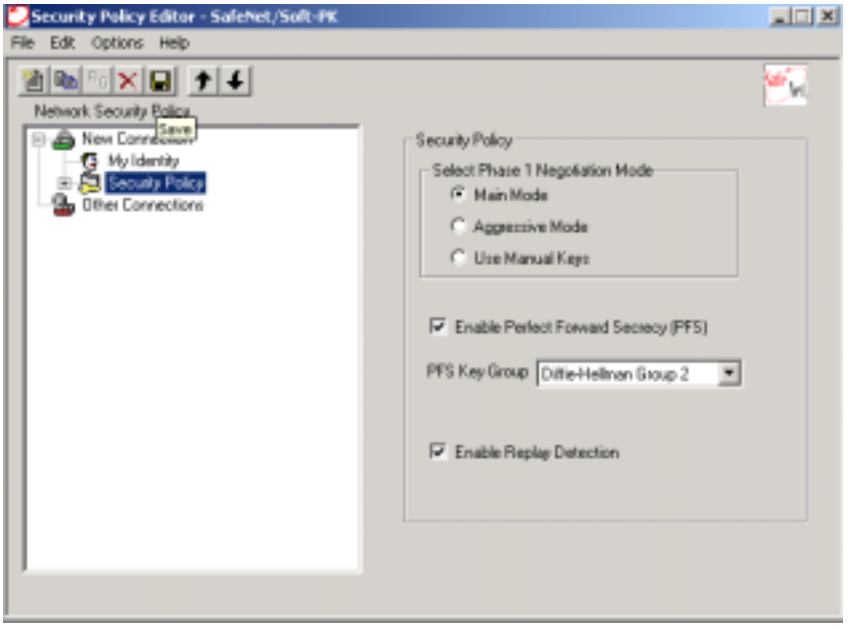
In this procedure, using Manual Keys will be specified, and then define the Internet Protocol Security (IPSec) protocols for securing the VPN tunnel.

1. Double-click the icon of the new connection that was created in the previous procedure. Icons for My Identity and Security Policy appear in the Network Security Policy list, as shown below.

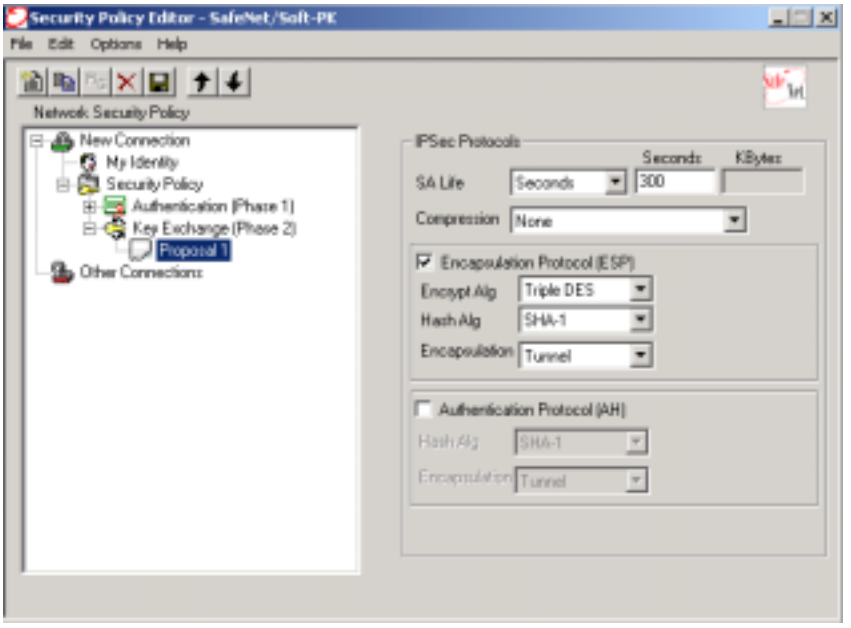
Note *Because the use of Manual Keys eliminates the Authentication phase of establishing a VPN tunnel, there is no need to set any identity authentication parameters.*



2. Double-click the **Security Policy** icon. The Security Policy area appears on the right, and icons for Authentication (Phase 1) and Key Exchange (Phase 2) appear in the Network Security Policy list, as shown below.



3. Select **Use Manual Keys** in the Security Policy area. The Enable Perfect Forward Secrecy (PFS) and Enable Replay Detection options become unavailable.
4. In the Network Security Policy list, double-click **Key Exchange (Phase 2**). Proposal 1 appears in the Network Security Policy list.
5. Click **Proposal 1** to display the IPSec Protocols area, as shown below.



6. Because the Security Association (SA) life for Manual Keys is unlimited, leave SA Life set as **Unspecifie**d.
7. To enable compression, choose **Deflate** from the drop-down list. To disable it, choose **None.** Compression reduces packet sizes to expedite transmission.

Note *Because the devices on both ends of the VPN tunnel must support this feature to be able to use it, leave the setting at* ***Non****e.*

8. Select **Encapsulation Protocol (ESP)** or **Authentication Protocol (AH)**. ESP provides encryption, authentication, and an integrity check for IP packet. AH provides authentication and an integrity check for IP packets
9. If **Encapsulation Protocol (ESP**) is selected, then select one of the following from the Encryption Algorithm drop-down list:

   DES — Data Encryption Standard is a cryptographic block algorithm with a 56-bit key.

   Triple DES — This is a more powerful version of DES in which the original DES algorithm is applied in three rounds, using a 168-bit key.

   NULL — No cryptographic algorithm is applied. (Safenet require you to enter a key even if you select **NULL**. Because the key is not used, its content does not matter and can be anything.) In the Hash Algorithm drop-down list, select one of the following:

MD5 — Message Digest version 5 is an algorithm that produces a 128-bit message digest or hash from a message of arbitrary length. The resulting hash is used, like a fingerprint of the input, to verify authenticity.

SHA-1 — Secure Hash Algorithm-1 is an algorithm that produces a 160-bit hash from a message of arbitrary length. It is generally regarded as more secure than MD5 because of the larger hashes it produces.

DES-MAC — Data Encryption Standard–Message Authentication Code is an authentication tag or checksum derived by using the final block of a DES-encrypted cipher text as the checksum.

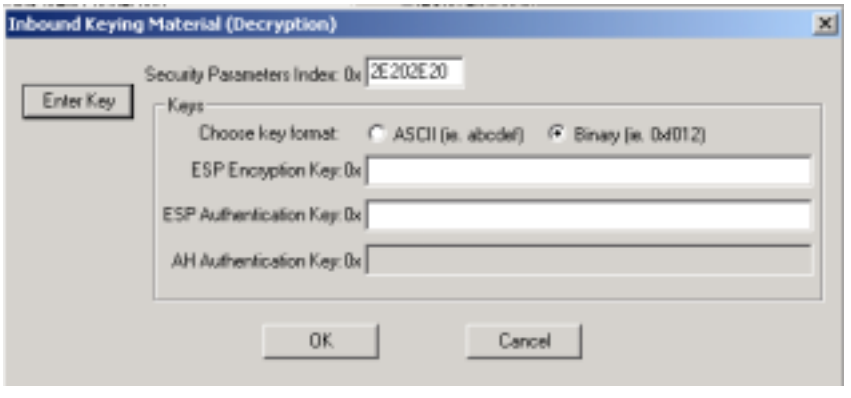
Note *Export versions of Safenet (designated with an* e *after the version number) are to be used outside the US. Because use of triple-DES is prohibited outside the US, export versions do not contain this option. In this case, DES is an acceptable option.*

If **Authentication Protocol (AH**) is selected, choose either **MD5** or **SHA-1** from the Hash Algorithm drop-down list. Then select the Encapsulation method. If you select **Connect using Secure Gateway Tunnel** when defining Remote Party Identity and Addressing, the encapsulation method must be **Tunnel**—no other option is available. If the other end of the VPN does not terminate at a secure gateway, you can select either **Tunnel** or **Transport**.

3.1.3 Create Inbound and Outbound Keys

In this procedure, one creates two pairs of keys: one pair to decrypt inbound messages and another pair to encrypt outbound messages.

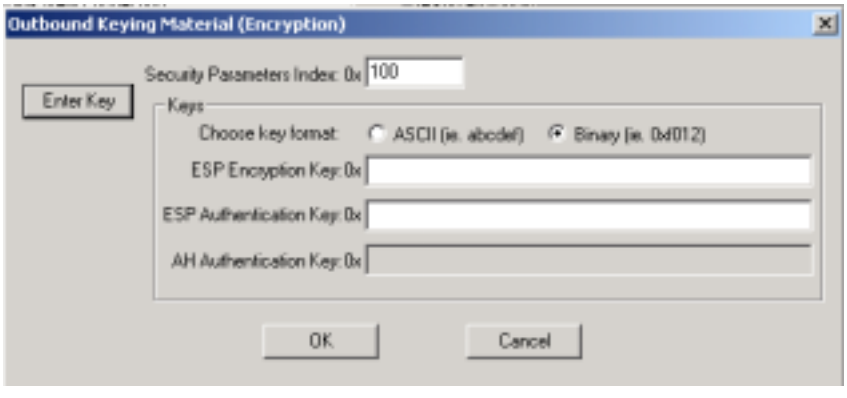
1. Click **Inbound Keys** at the bottom of the Security Policy Editor window. The Inbound Keying Material (Decryption) dialog box appears.



2. Click **Enter Key** to open the Key fields. If Encapsulation Protocol (ESP) in the IPSec Protocols area is selected, only the ESP fields become available—the AH Authentication Key field remains dimmed. The reverse is true if you selected Authentication Protocol (AH).
3. In the Security Parameters Index (SPI) field, enter a unique identifying value of 8 hexadecimal characters. The DFL-xxx security gateway uses the SPI, which is carried in the header of the Security Protocol (ESP or AH), to identify the Safenet user's VPN tunnel proposal. This allows the remote user to make a connection from either a fixed IP address or a dynamically assigned IP address.
4. For the key format, select either **ASCII** or **Binary**.

   ASCII — American Standard Code for Information Interchange is a binary coding system for the set of letters, numbers, and symbols on a standard keyboard.

   Binary — This base-16 (or hexadecimal) numbering system represents binary numbers with 16 characters: 1234567890abcdef.
5. Enter keys in the available Key fields, depending on the protocol that is selected.
6. Click **OK** to save the settings.
7. Click **Outbound Keys** at the bottom of the Security Policy Editor window. The Outbound Keying Material (Encryption) dialog box appears.



8. Click **Enter Key** to activate the ESP Encryption Key and Authentication Key fields or the AH Authentication Key field, depending on which IPSec Protocol (ESP or AH) is selected.
9. In the Security Parameters Index (SPI) field, enter a unique identifying value of 8 hexadecimal characters.
10. For the key format, select either **ASCII** or **Binary**.
11. In the Key field(s), type the same key(s) that you used for the Inbound Keys.
12. Click **OK** to save the settings. The Outbound Keying Material (Encryption) dialog box closes.
13. Click the **Save** icon or choose **Save Changes** from the File menu. The configuration for the DFL-xxx end of a Manual Key VPN tunnel is complete.

3.2 Safenet Pre-Shared Key VPN

There are three steps to set up Safenet for a VPN tunnel with a Pre-Shared Key:

3.2.1 Creating a New Connection

3.2.2 Creating the Pre-Shared Key

3.2.3 Defining the IPSec Protocols

3.2.1 Create a New Connection

Begin by initiating a new connection. Then name the connection, define it as secure, and determine the identification and location of the other end of the eventual VPN tunnel.

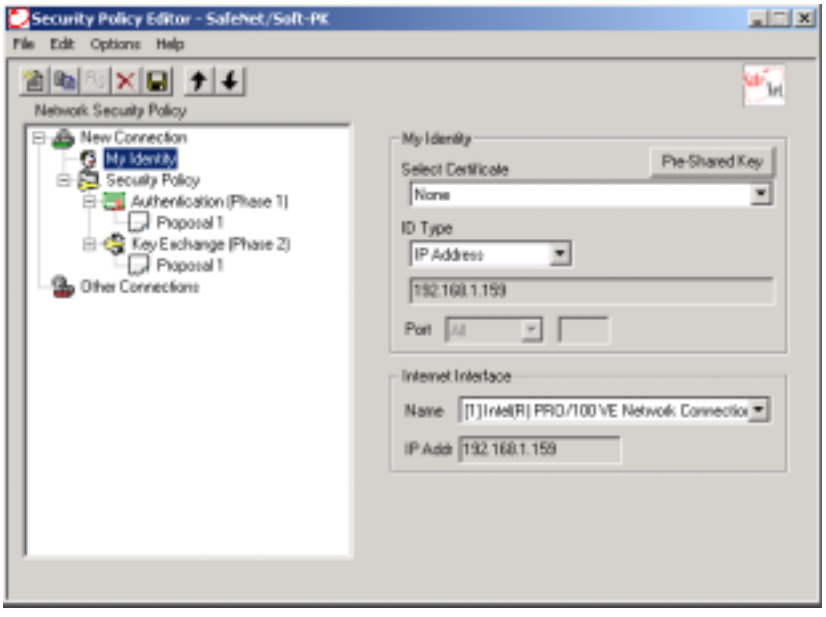
1. Double-click the **Safenet** icon, located on the Windows taskbar, to open the Security Policy Editor.
2. On the File menu, choose **New Connection**.
3. Give the new connection a unique name.
4. In the Connection Security area (to the right of the Network Security Policy list), select **Secure**.
5. In the Remote Party Identity and Addressing area, select an identifier for the other party from the ID Type list, and enter the required information. Choose either IP Address or IP Subnet. Other choices will not work.
6. Define the protocol you want to use for the Connection: All, TCP, UDP, ICMP, or GRE.
7. If the other end of the eventual VPN tunnel is protected by a security gateway, select **Connect using Secure Gateway Tunnel**. The Secure Gateway Tunnel ID Type and IP Address fields become available.

8. For ID Type, select **IP Address** as an identifier for the other party from the ID Type list, and enter the required information. No other option can be selected for pre-shared key IKE.

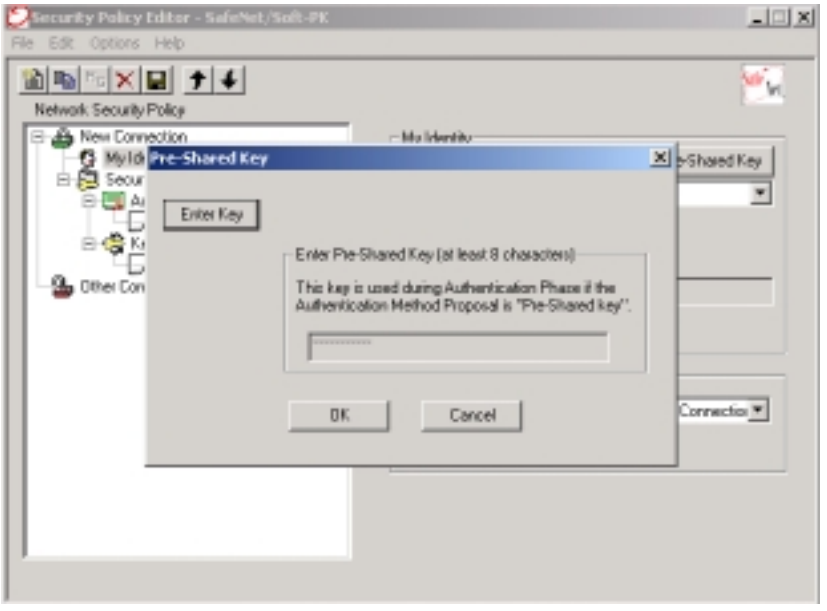
3.2.2 Create Pre-Shared Key

Create the Pre-Shared Key to be used in identifying the communicating parties during the Phase 1 negotiations.

1. Double-click the icon for the new connection. **My Identity** and **Security Policy** icons appear in the Network Security Policy list.
2. Click **My Identity**. The **My Identity** and Internet Interface areas appear to the right of the Network Security Policy list, as shown below.



3. In the **My Identity** area, select **NONE** from the Select Certificate drop-down list.
4. Click **Pre-Shared Key**.

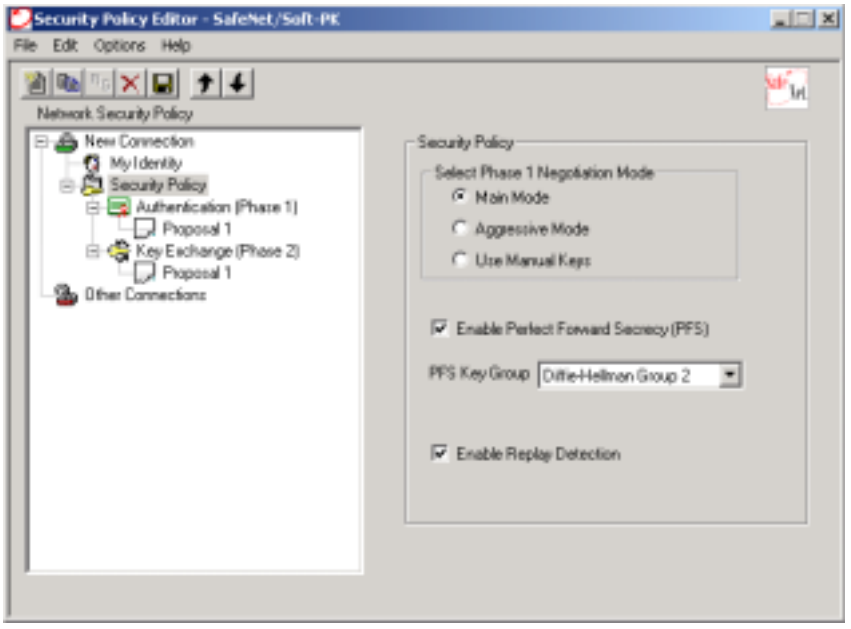


5. Click **Enter Key** to make the Pre-Shared Key field available.
6. Type a key with a length between 8 and 58 characters. A longer key length results in stronger encryption.
7. Click **OK** to save the entry.

3.2.3 Define IPSec Protocols

Define the Internet Protocol Security (IPSec) protocols for securing the VPN tunnel.

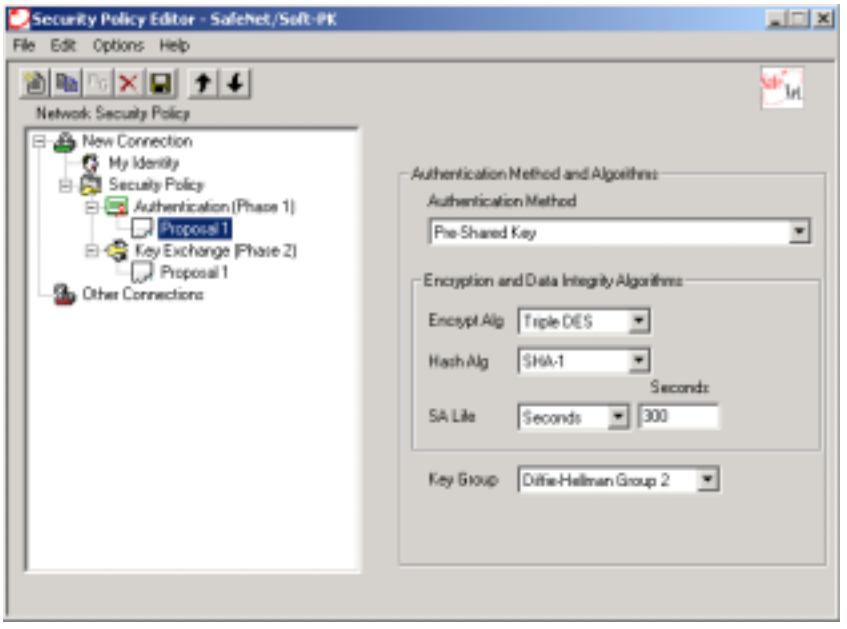
1. Double-click **Security Policy** in the Network Security Policy list. The Security Policy area appears on the right, and the Authentication (Phase 1) icon and Key Exchange (Phase 2) icon appear in the Network Security Policy list, as shown below.



2. Select **Main Mode** in the Security Policy area if a dynamic IP is being used.
3. Select **Enable Perfect Forward Secrecy (PFS)** and **Enable ReplayDetection** to employ these options.

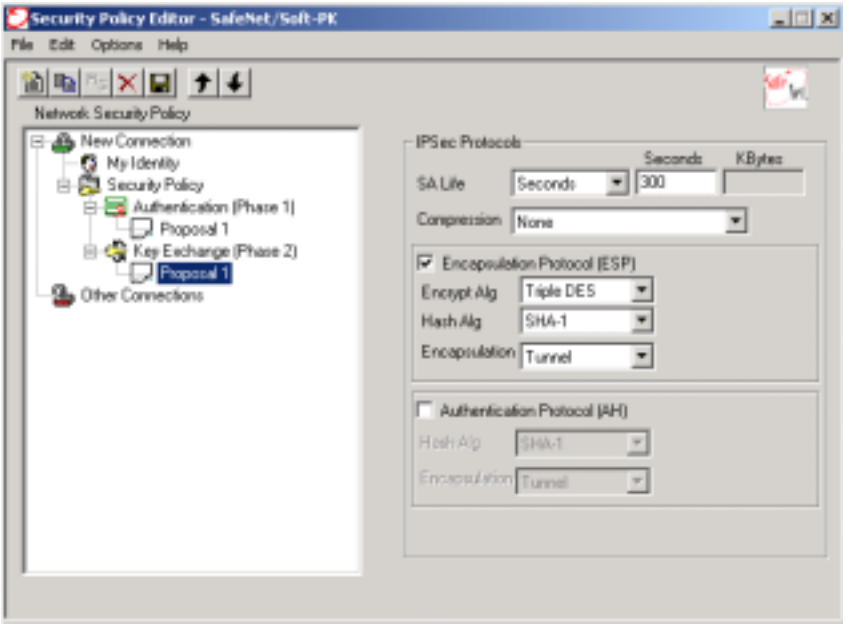
   Perfect Forward Secrecy (PFS) is a method that allows the generation of a new encryption key independent from and unrelated to the preceding key.

   Replay Detection is a service in the Authentication Header that detects replay attacks, in which an attacker intercepts a sequence of packets, and then replays them later to gain access to network resources.
4. In the Network Security Policy list, double-click the **Authentication (Phase 1)** icon. Proposal 1 appears below the Authentication (Phase 1) icon.
5. Select **Proposal 1** to display the Authentication Method and Algorithms area, as shown below.



6. In the **Authentication Method and Algorithms** area, define the Encryption Algorithm, the Hash Algorithm, and the Security Association (SA) Life. Because Pre-Shared Key is selected, it appears in the **Authentication Method** field. Although there is a drop-down list, no other choices are available.
7. In the Key Group drop-down list, select **Diffie-Hellman Group 1**, **Diffie-Hellman Group 2**, or **Diffie-Hellman Group 5**. Diffie-Hellman is a key-exchange protocol allowing the participants to agree on a key over an insecure channel.

   Select **Diffie-Hellman Group 2.**
8. Double-click the **Key Exchange (Phase 2)** icon.Proposal 1 appears below the Key Exchange (Phase 2) icon.
9. Select **Proposal 1** to display the IPSec Protocols area.



10. In the IPSec Protocols area, define the **SA Life** (that is, the lifetime of the Security Association) in either seconds or bytes, or leave it as **Unspecified.**
11. The Compression feature reduces packet sizes to expedite transmission. To enable compression, choose **Deflate** from the drop-down list; to disable it, choose **None**.
12. Select either **Encapsulation Protocol (ESP)** or **AuthenticationProtocol (AH)**, and specify the desired protocols.

    ESP provides encryption, authentication, and an integrity check for IP datagrams

    AH provides authentication and an integrity check for IP datagrams

    If you select the **Connect using Secure Gateway Tunnel** check box when defining Remote Party Identity and Addressing, the encapsulation method must be **Tunnel** — no other option is available. If the other end of the VPN does not terminate at a secure gateway, either **Tunnel** or **Transport** can be selected.
13. Click **Save** in the toolbar, or choose **Save Changes** from the File menu. The configuration for the Safenet end of an eventual VPN tunnel using a Pre-Shared Key is complete.