


# SafeNet SoftRemote Documentation Profiles for IPSec Interoperability

SafeNet SoftRemote  
Version 8.0  
July 25, 2002

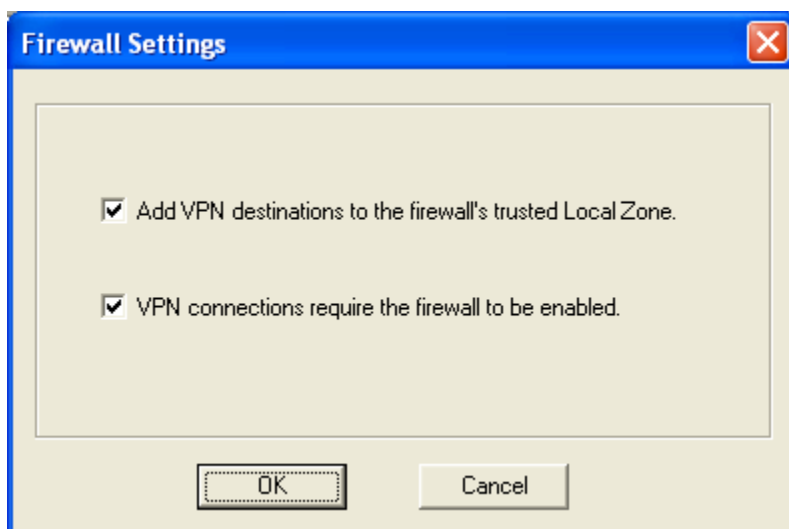
---

## Scenario 1: Remote Client-to-gateway with preshared secrets

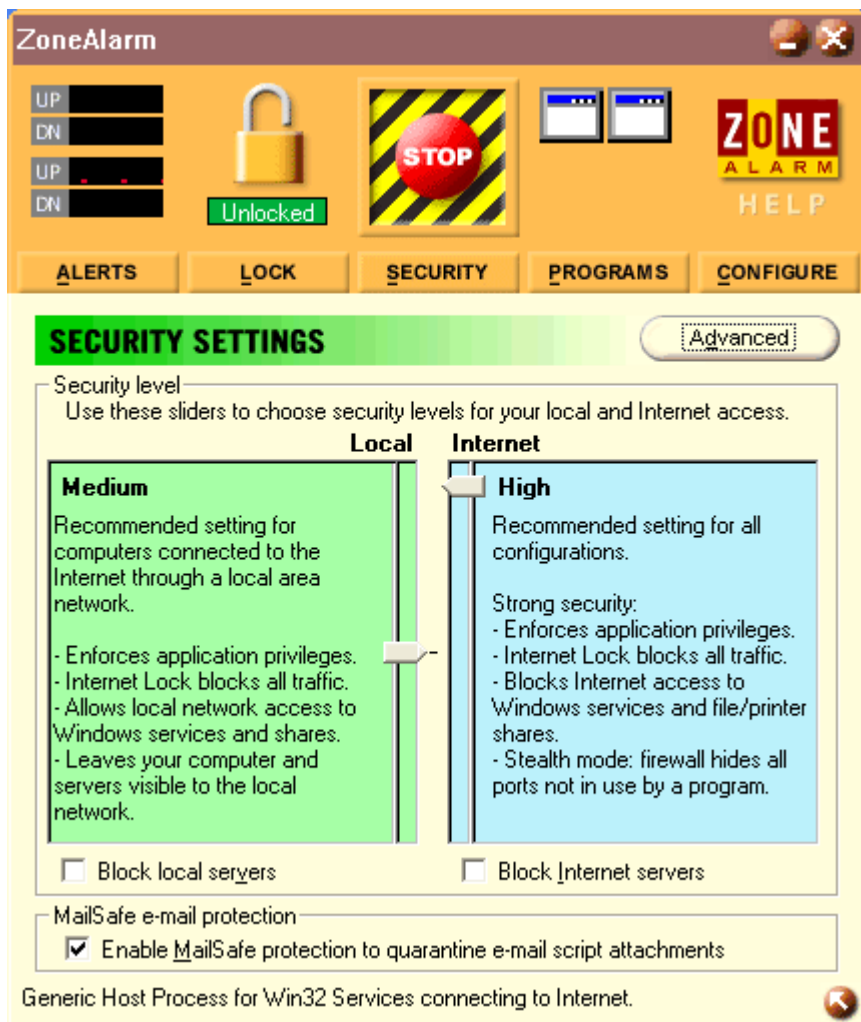
### A. Configure SoftRemote Firewall Settings

1. Open SafeNet SoftRemote Security Policy Editor by double clicking the SoftRemote system tray icon. 
2. Select Firewall Settings from the Options dropdown.
3. Choosing Add VPN destinations to the Firewall's Trusted Local Zone will automatically map all VPN destinations in the policy Trusted Local Zone. This will avoid blocked traffic; warning messages or prompts if unchecked. See Local Zone Properties and samples below.
4. Choosing VPN connections require the firewall to be enabled, will block VPN traffic if the Firewall is shutdown.

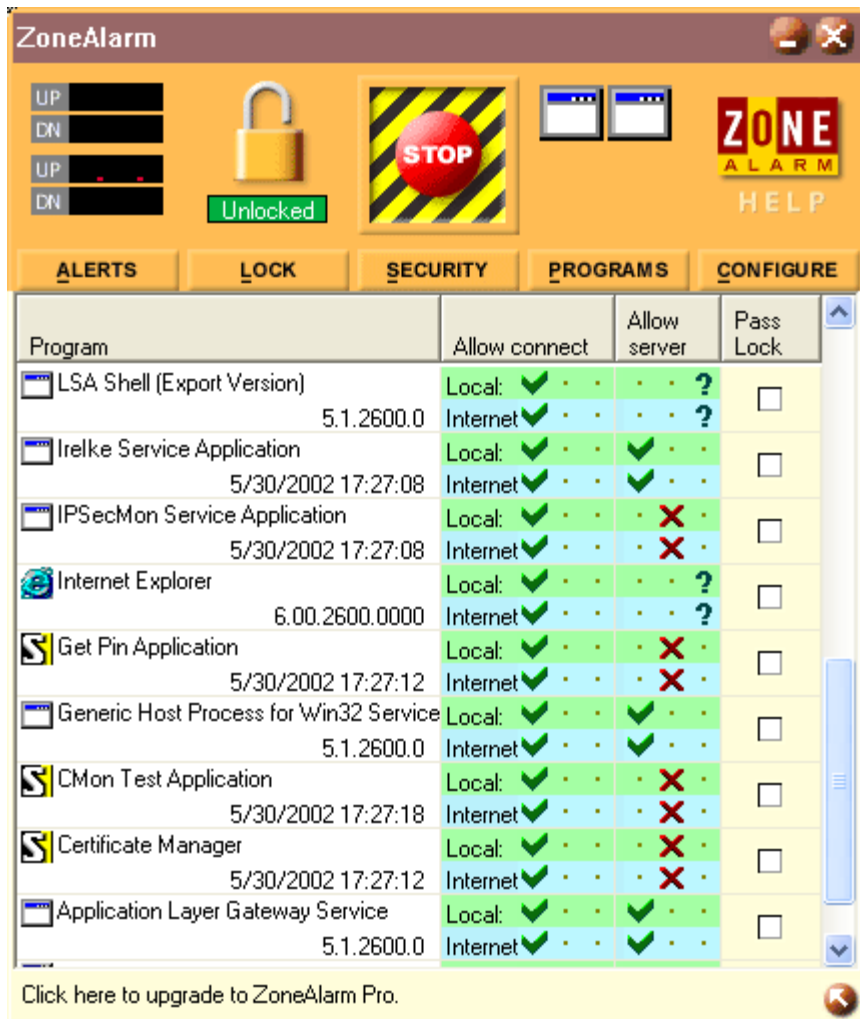
### Policy Editor Firewall Options Settings sample



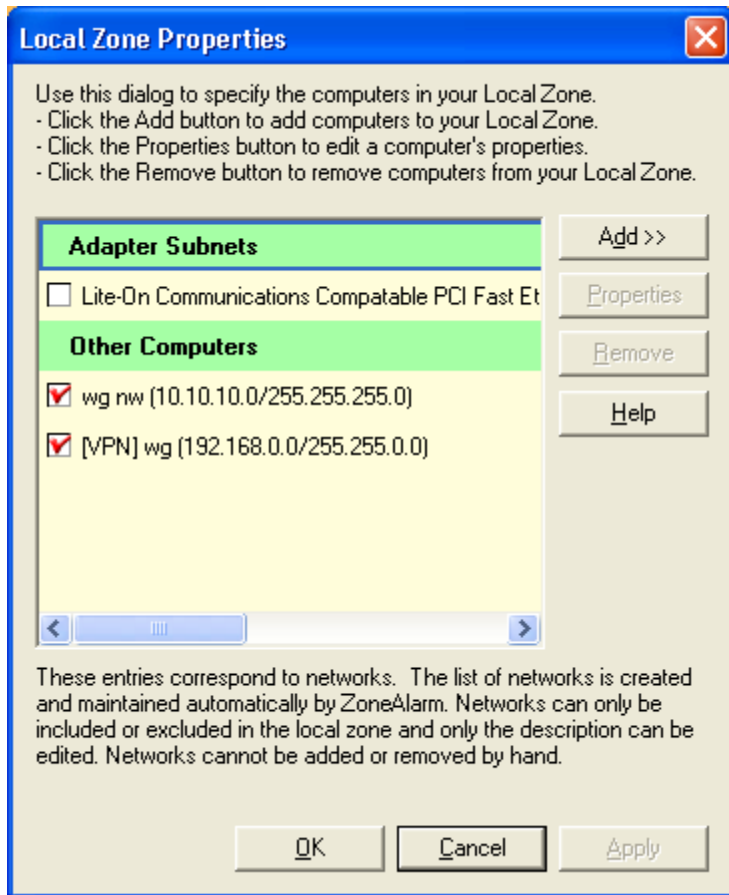
### ZoneAlarm Security Settings sample



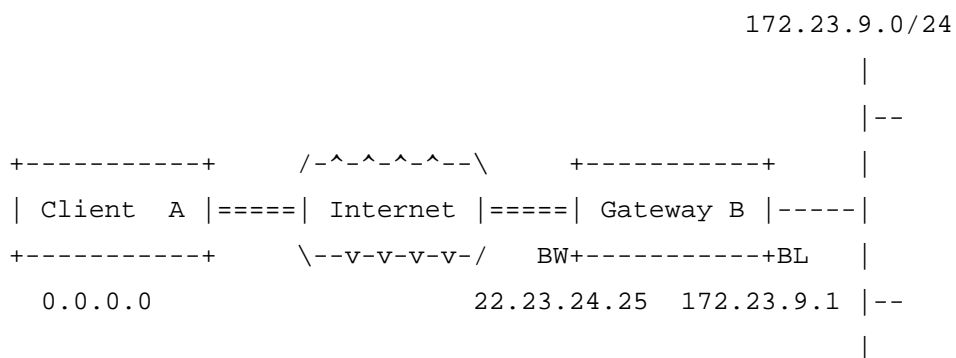
ZoneAlarm Programs settings sample



**ZoneAlarm Local Zone Properties sample**



The following is a typical client-to-gateway VPN that uses a preshared secret for authentication.




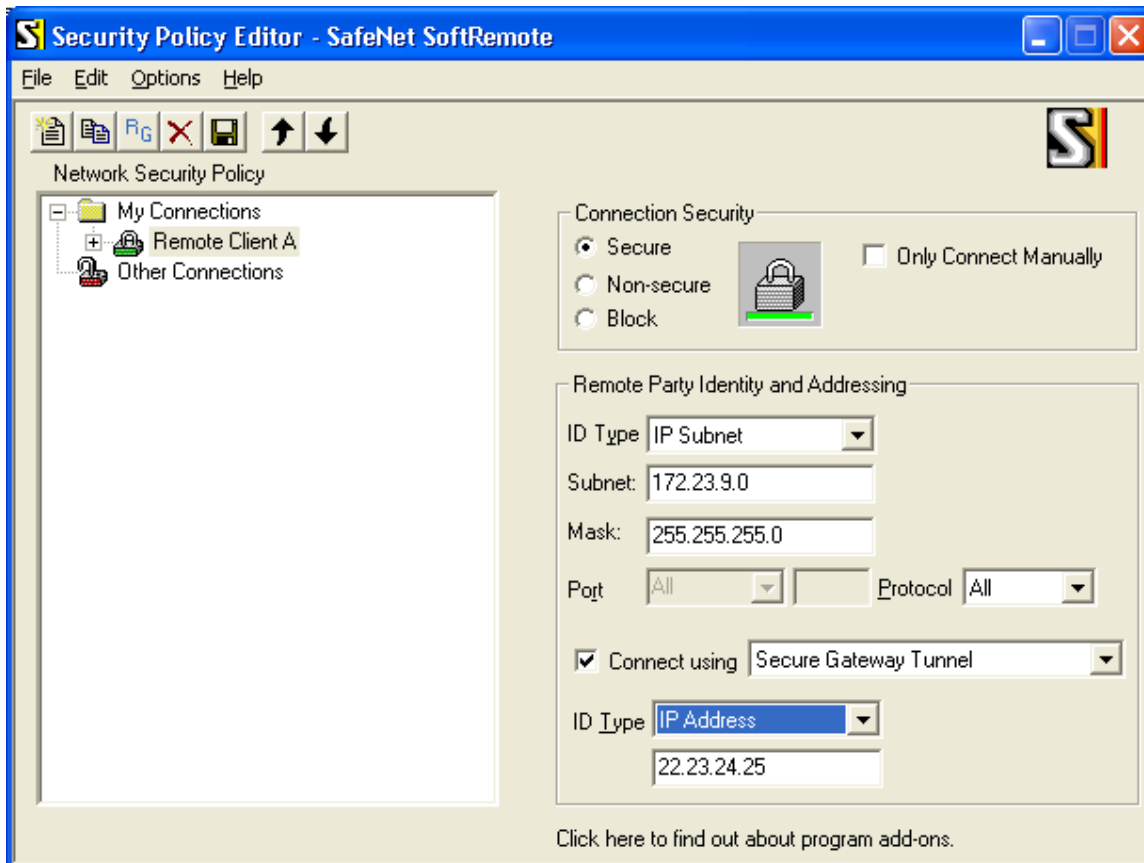
Client A connects to the internal LAN 172.23.9.0/24 via the Internet through Gateway B's WAN interface 22.23.24.25. Gateway B is to be configured for RAS clients with dynamic IP addressing. In other configurations static IP addressing could be used, such as LAN, PPPoE, ISDN, and NT RAS connections.

The **IKE Phase 1 parameters** used in Scenario 1 are:

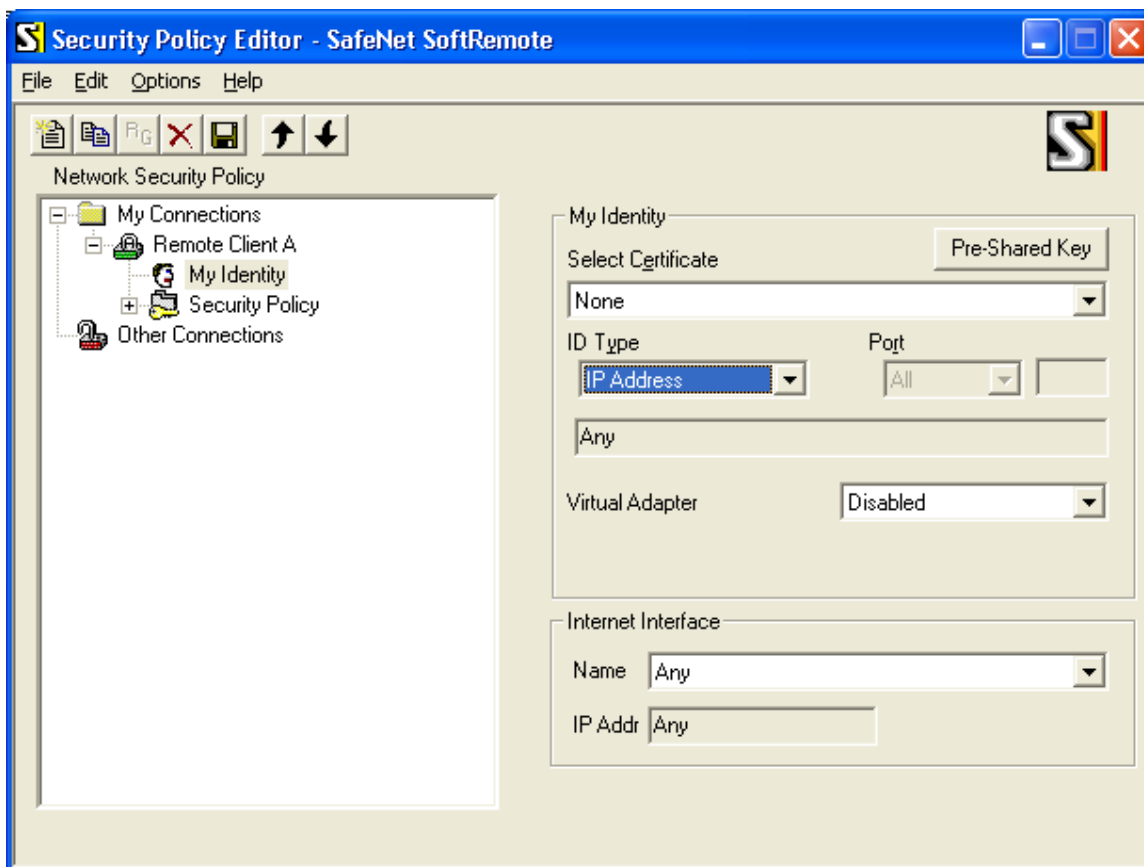
- Main mode
- TripleDES
- SHA-1
- MODP group 2 (1024 bits)
- pre-shared secret of "hr5xb8416aa9r6"
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying

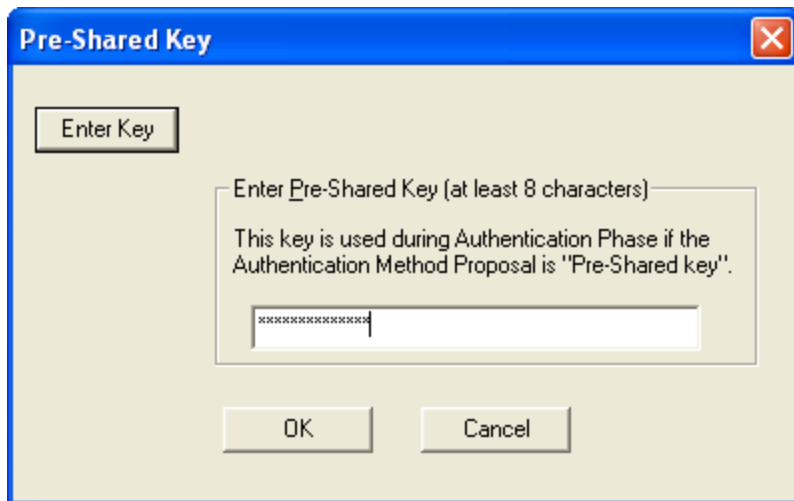
To set up client policy Phase1 for Gateway B for this scenario, use the following steps:

1. Open SafeNet SoftRemote Security Policy Editor by double clicking the SoftRemote system tray icon. 
2. To Add a new connection right click on My Connections, choose add – connection.
3. Name the new connection Remote Client A.
4. Set Connection Security to Secure.
5. Set the ID Type to IP subnet in Remote Party Identity and Addressing.
6. Set the Subnet and Mask to 172.23.9.0 / 255.255.255.0 in Remote Party Identity and Addressing.
7. Set Protocol and Port to All, default setting.
8. Check the box Connect using “Secure Gateway Tunnel”.
9. Set Gateway ID type to IP Address and enter the Gateways IP address 22.23.24.25.

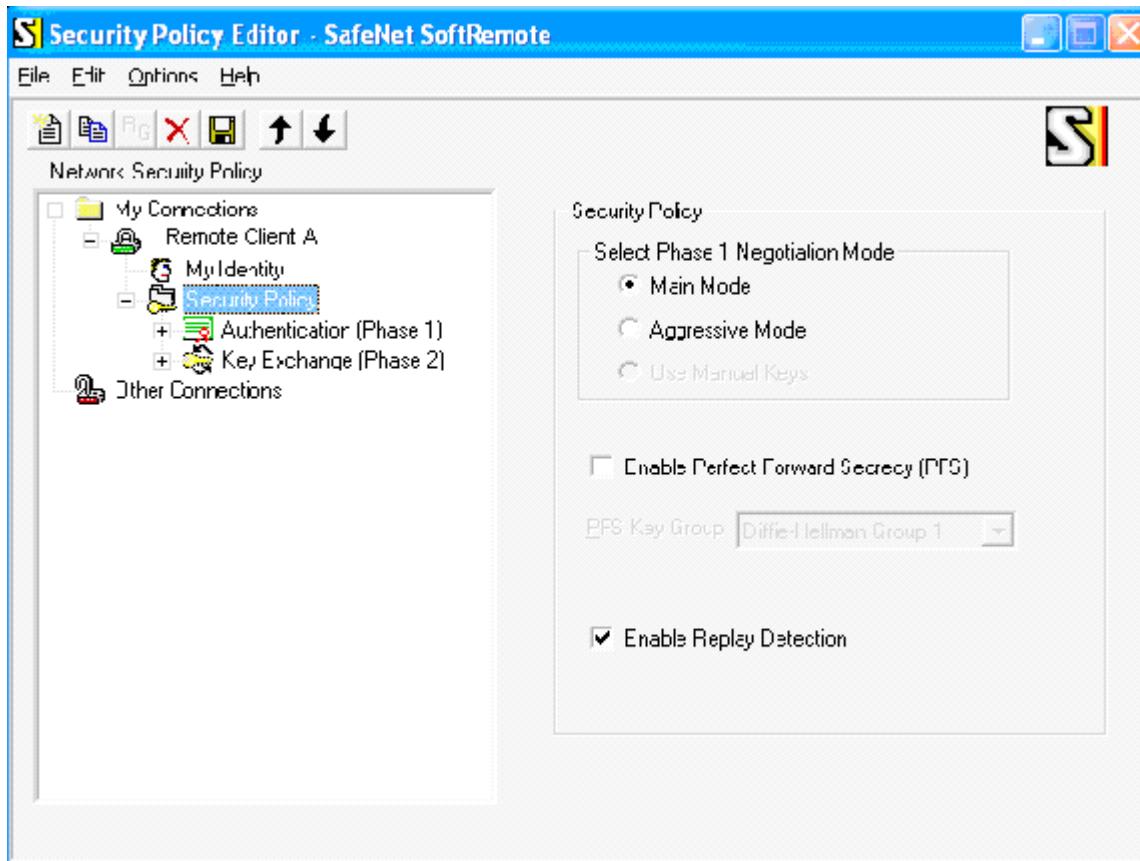


10. Open the My Identity Section of the connection by double clicking Remote Client A or clicking on the + next to Remote Client A.
11. Set the Select Certificate to "None" for Pre-Shared Key in the My Identity field
12. Click on the Pre-Shared Key button.
13. Click on the Enter Key button and enter the Pre-Shared Key "hr5xb84l6aa9r6" in the field provided, then click OK.
14. The ID type and name will default IP Address and name "Any" is grayed out below IP Address.
15. Port will default to All due to the previous port and protocol settings to All.
16. Set the Virtual Adapter to Disabled, to use the VA set it to Preferred or Required, this will require a Gateway that does Mode Config.
17. Set the Internet Interface to Any which will default the IP address to Any.

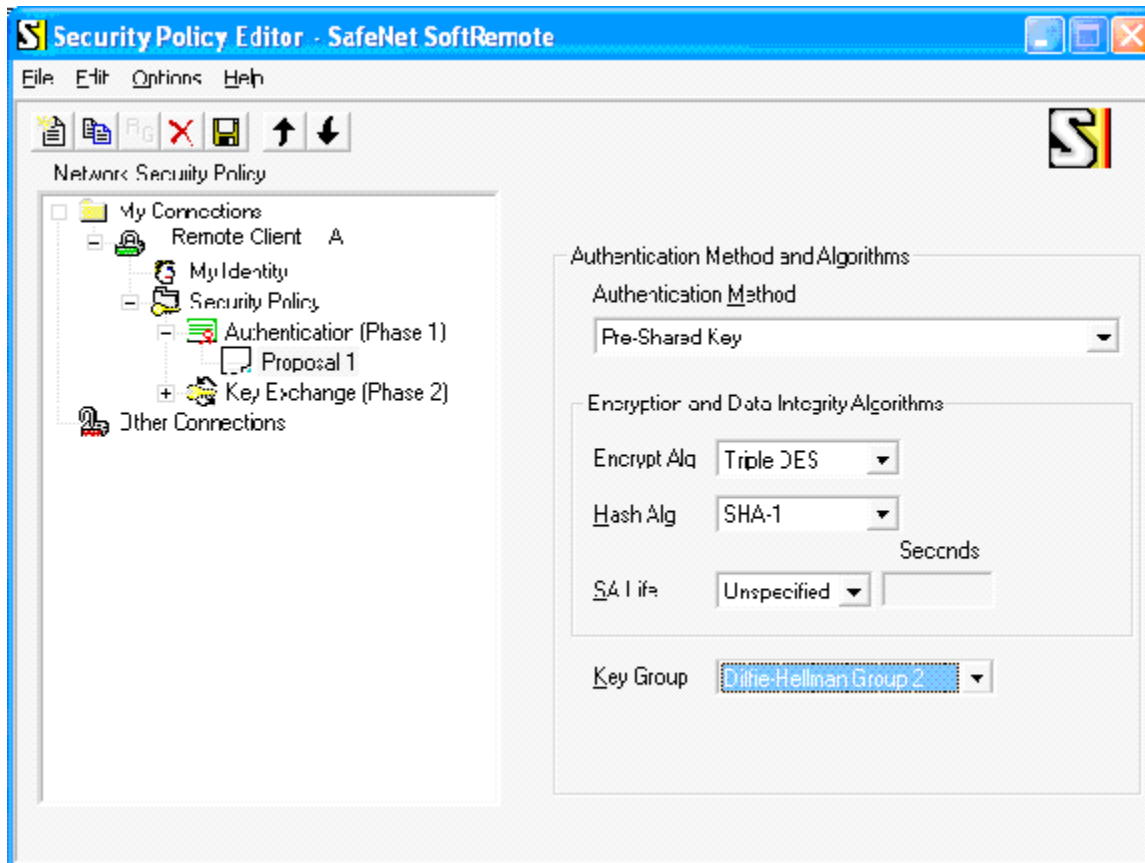




18. Open the Security Policy section of connection Remote Client A.
19. Set the Security Policy Phase 1 Negotiation Mode to Main Mode.
20. Leave Enable PFS unchecked since it is not being used by the Gateway. To use PFS, check the box Enable PFS and select DH group 2.
21. Check Enable Replay Detection.





22. Open Proposal 1 of Authentication (Phase 1) by double clicking Security Policy then double clicking Authentication (Phase1).
23. Authentication Method and Algorithms will default to Pre-Shared Key due to our previous selection in “My Identity”.
24. Set Encryption Algorithm to Triple DES.
25. Set Hash Algorithm to SHA-1
26. Set the SA Life to Seconds and enter 28800 seconds, this field can be left Unspecified since the client will respond to Gateway initiated re-keying.
27. Set the Key Group to DH Group 2.

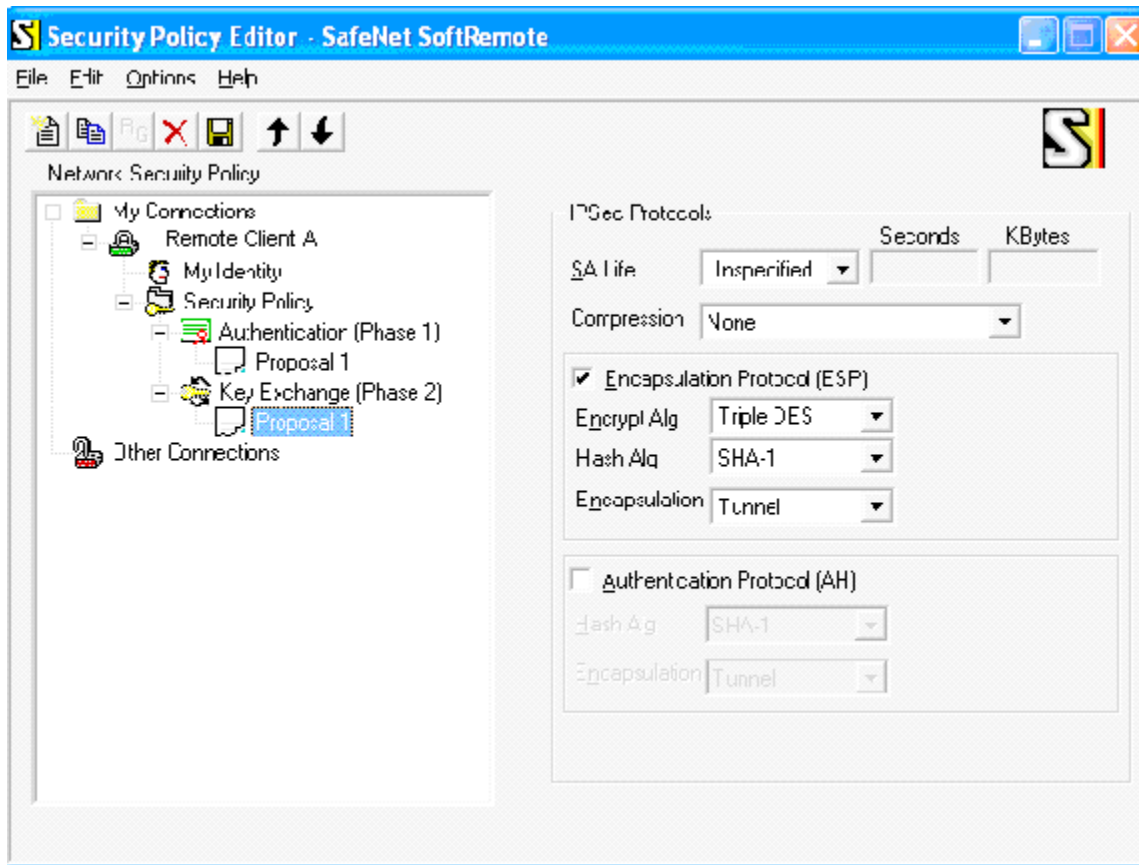


The **IKE Phase 2 parameters** used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying
- Selectors for all IP protocols, all ports, between 0.0.0.0 and 172.23.9.0/24, using IPv4 subnets

To set up client policy Phase2 for Gateway B for this scenario, use the following steps:

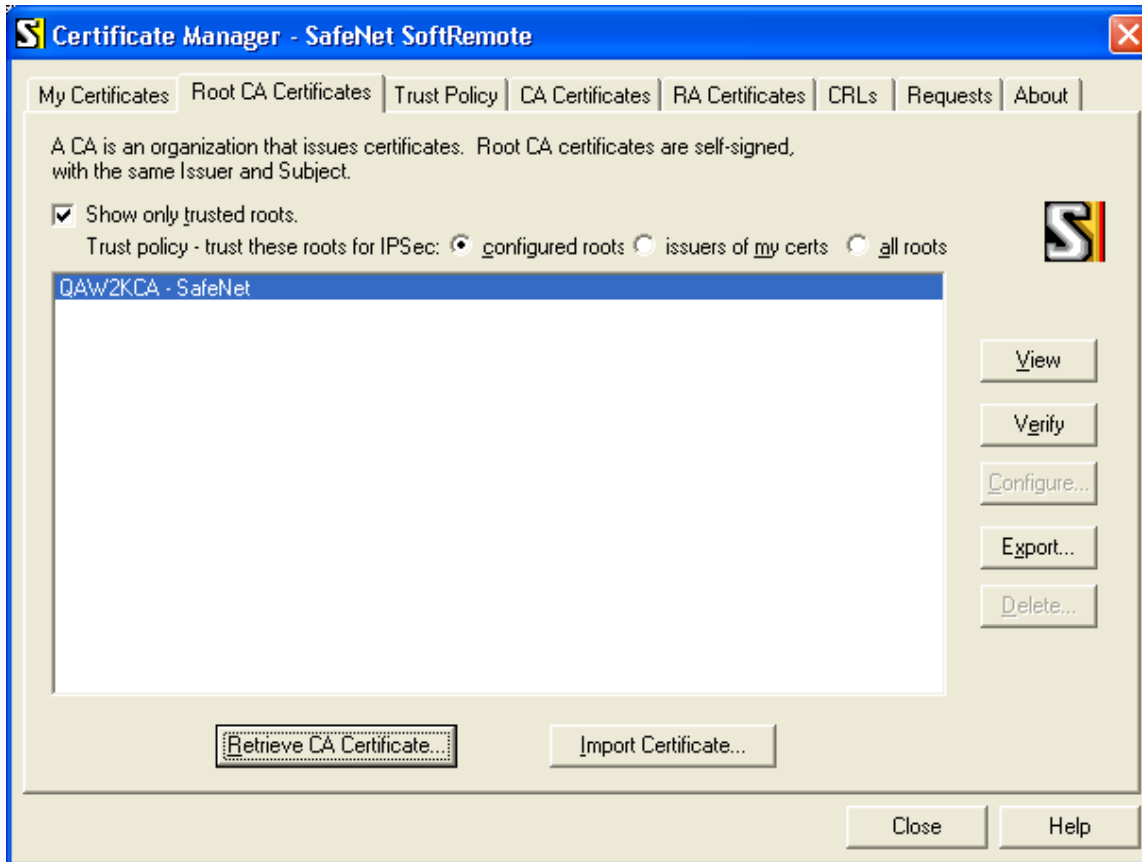
28. Open Proposal 1 of Key Exchange (Phase 2) of Remote Client A by double clicking Key Exchange (Phase 2) or clicking on the + of Key Exchange (Phase 2).
29. Set the IPSec Protocols SA Life to Seconds and enter 3600 seconds, this field can be left Unspecified since the client will respond to Gateway initiated re-keying.
30. Leave Compression set to None.
31. Check the box Encapsulation Protocol (ESP).
32. Set the Encryption Algorithm to Triple DES
33. Set the Hash Algorithm to SHA-1.
34. Set Encapsulation to Tunnel.
35. Save the policy by clicking on the diskette image  or click on the File tab and save changes.
36. To connect to the 172.23.9.0 network, first connect to the Internet, then ping or ftp a host behind the Gateway, use the connection monitor and log viewer to monitor the session establishment. Look for the system tray icon to get a key and a green bar will indicate when secure traffic passes. 



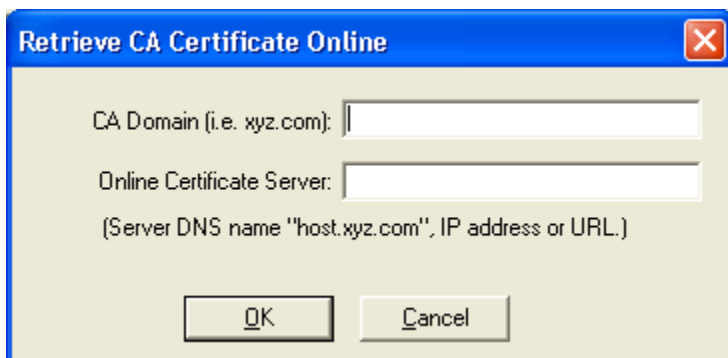
## Scenario 2: Client-to-gateway with certificates

The following is a typical Client-to-gateway VPN that uses PKIX certificates for authentication.

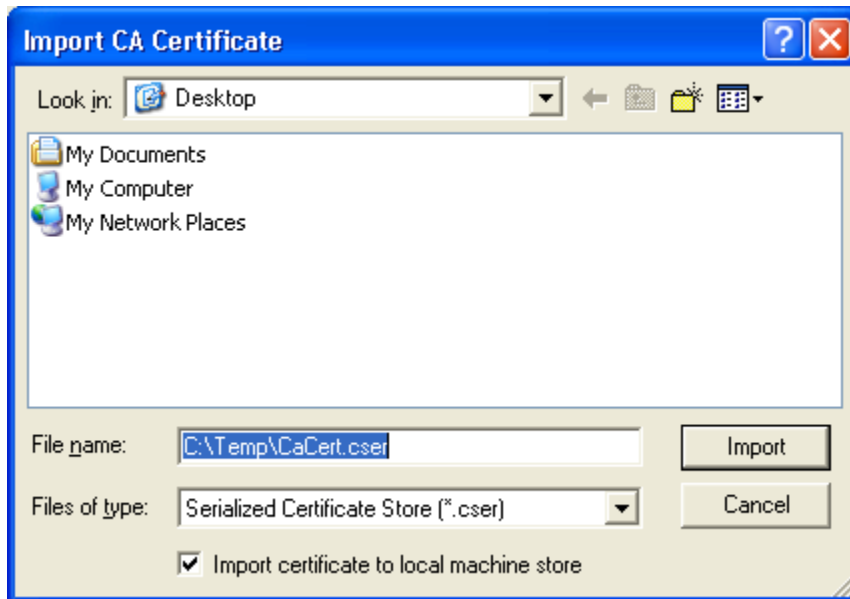




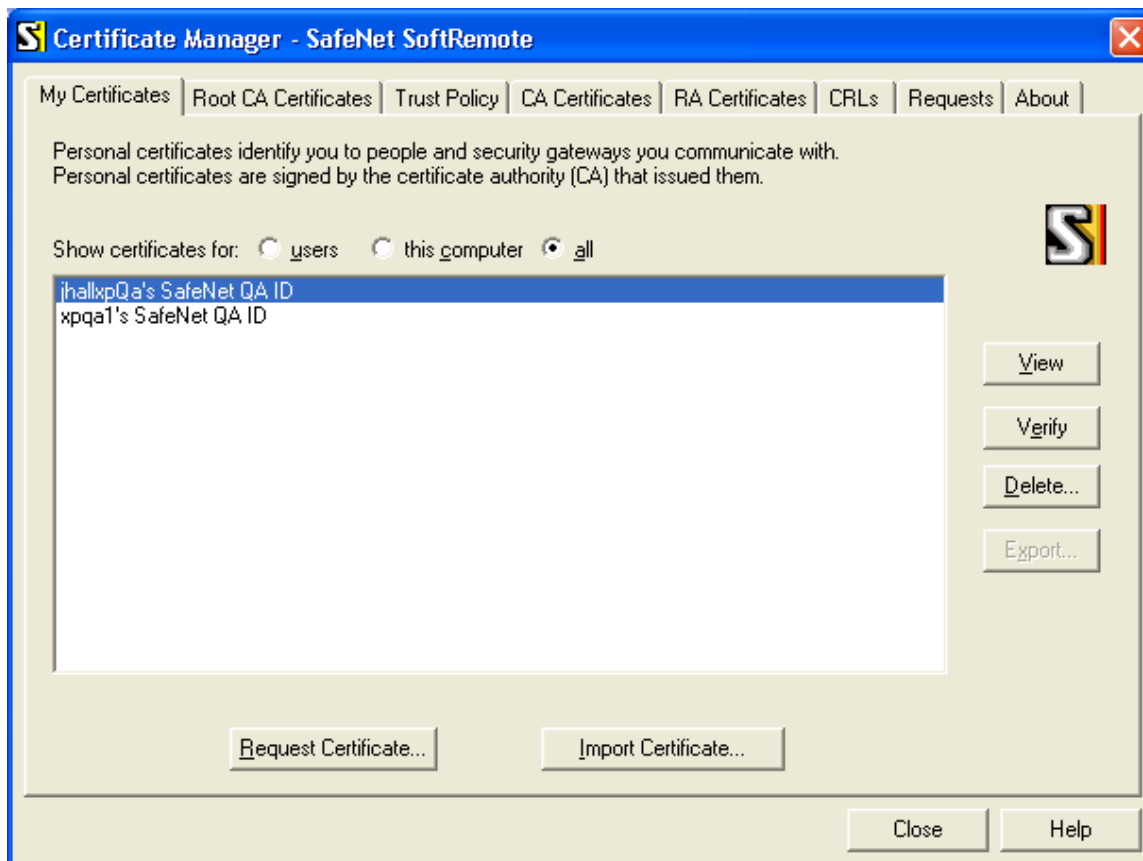
2. Online CA retrieval, enter CA domain name and path to CA server such as an IP address or URL. Once the CA cert has been imported or retrieved it can be viewed or verified with the tabs on the right side of Root CA Certificates.



3. To import the CA certificate from a file or local machine store use the import CA cert option.



4. With a valid CA Certificate a Personal Certificate can now be retrieved or imported from the options under the My Certificates tab.



5. Use the Online Certificate request form for SCEP request. Enter the Subject Name, Subject Alternate Name information as required by your CA. Enter a Challenge Phase, select the Issuing CA, set the Key Generation Option if desired, choose an enrollment method (Online is default). Under the Advanced tab the Cert Key size can be specified and the CSP can be specified in the case of Smart cards or other special CSP requirements. The Advanced option in most cases can be left at the default setting.

Online Certificate Request - SafeNet SoftRemote

Generate a Private/Public key pair and request a personal certificate.

Subject Name

Enter Subject Name in LDAP format

\*Name:

Department:

Company:

State:  Country:

Key Generation Options:

Generate exportable key

Enrollment Method:

Online

File-based

Subject Alternate Name

Email:

Domain Name:

IP Address:  \*Required Fields

Advanced...

Online Request Information

Challenge Phrase:

Confirm Challenge:

Issuing CA:

OK

Cancel

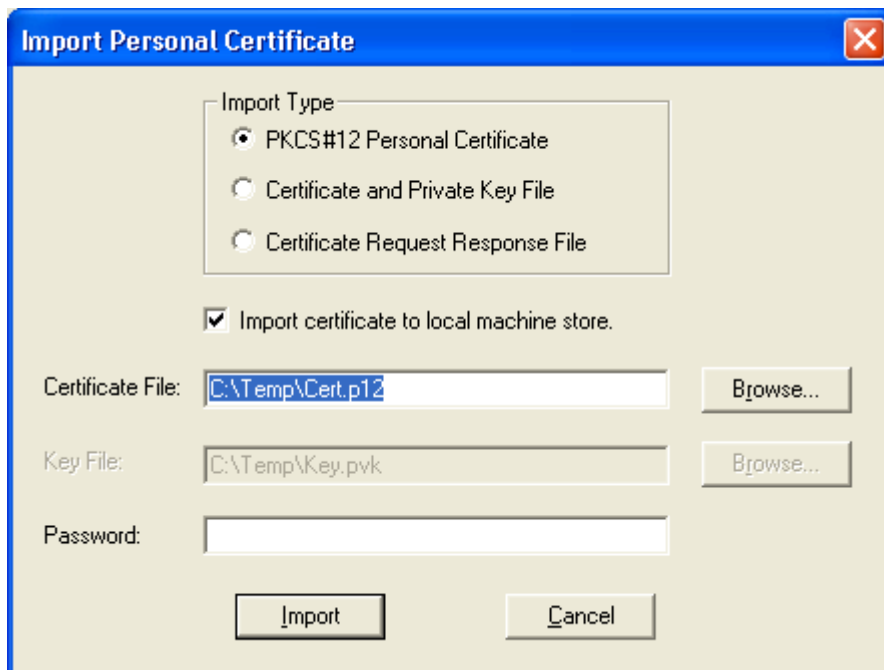
6. Optional File based Certificate Request Form.

**S** File-based Certificate Request - SafeNet SoftRemote ✕

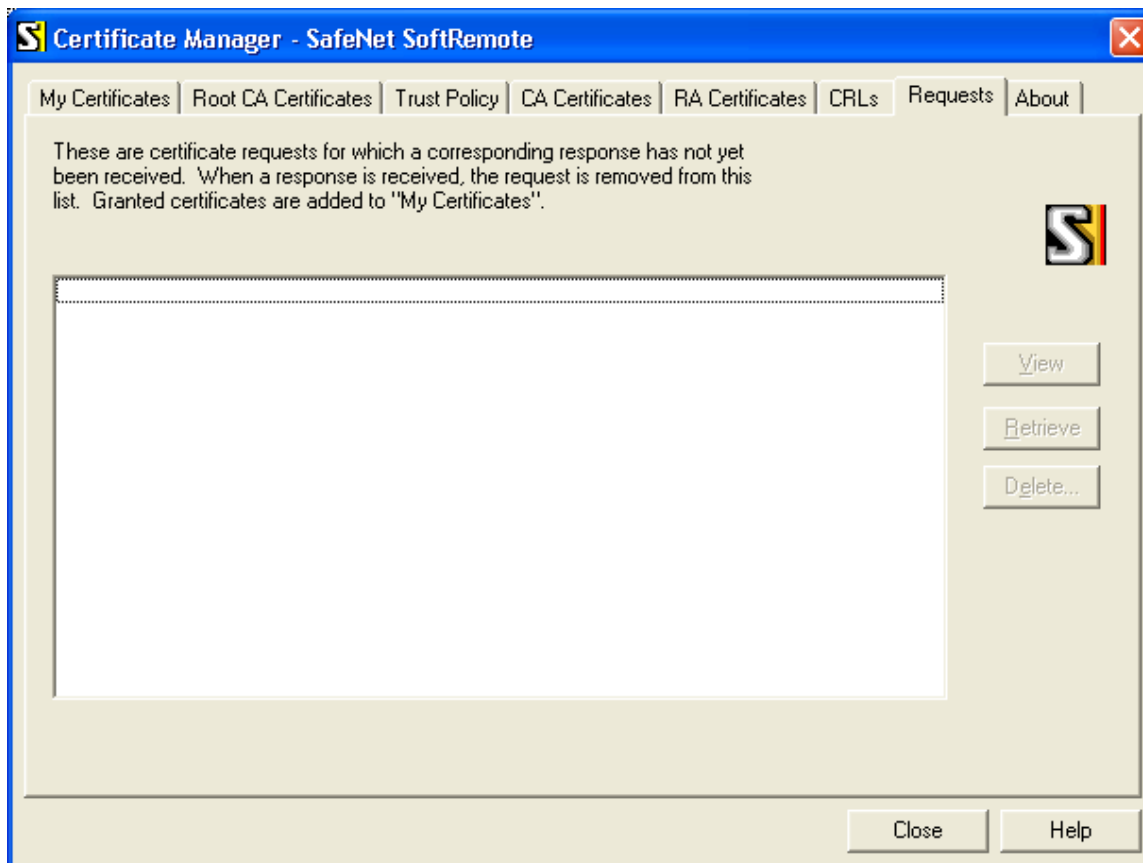
Generate a Private/Public key pair and request a personal certificate.

<p>Subject Name</p> <p><input type="checkbox"/> Enter Subject Name in LDAP format</p> <p>*Name: <input type="text"/></p> <p>Department: <input type="text"/></p> <p>Company: <input type="text"/></p> <p>State: <input type="text"/> Country: <input type="text"/></p>	<p>Key Generation Options:</p> <p><input type="checkbox"/> Generate exportable key</p>
<p>Subject Alternate Name</p> <p>Email: <input type="text"/></p> <p>Domain Name: <input type="text"/></p> <p>IP Address: <input type="text"/> *Required Fields</p>	<p>Advanced...</p>
<p>Request File</p> <p>Filename: <input type="text"/></p> <p>Browse...</p>	<p>OK</p> <p>Cancel</p>

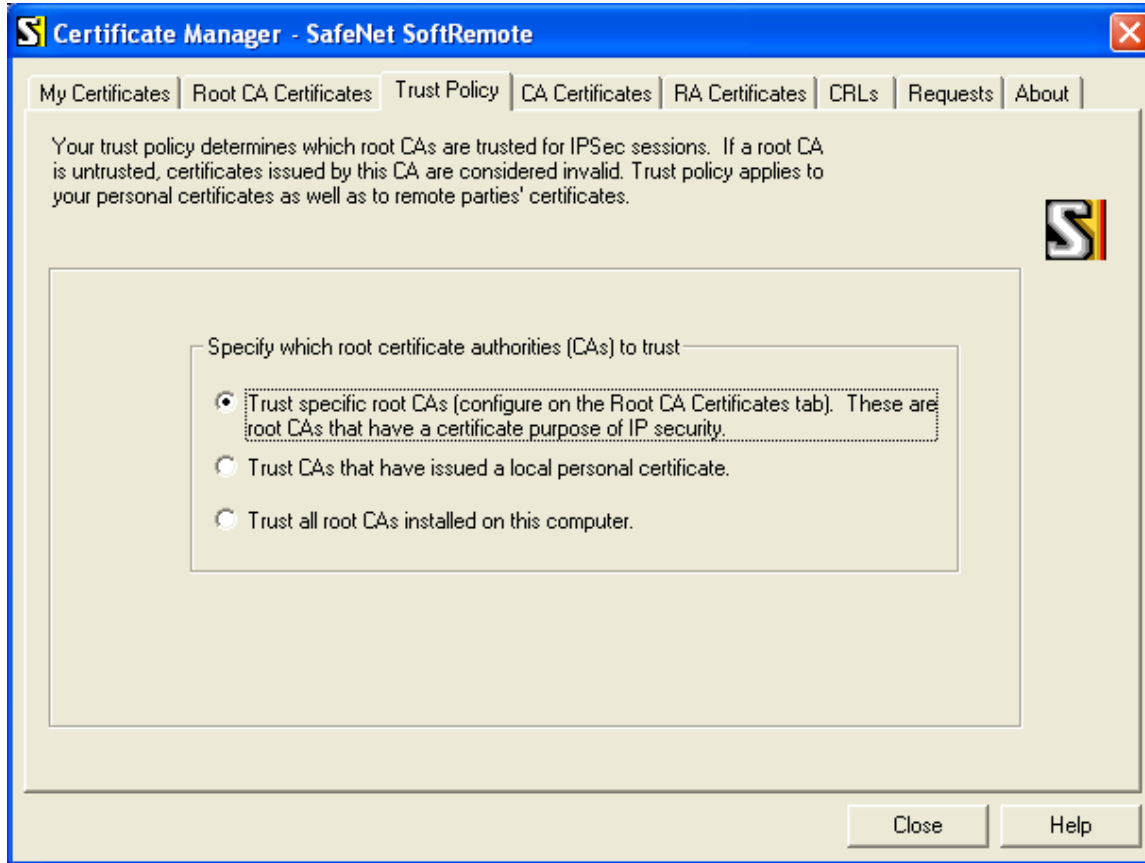
7. Manual Personal Import Certificate Form.



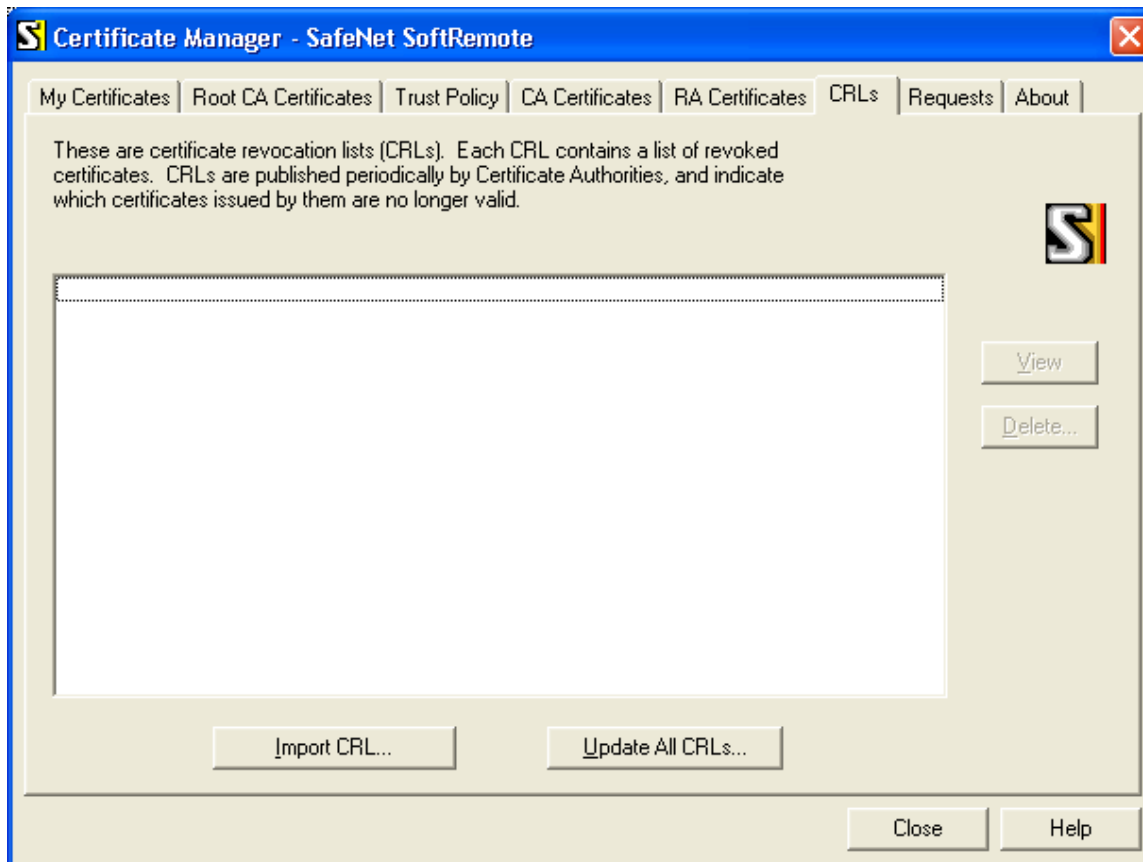
8. Use the Request tab in Certificate Manager to Retrieve Personal Certificate Requests for CA's that do manual cert approvals.




9. Set the CA Trust settings according to your security officer's recommendations, Trust specific root CA's is the default.

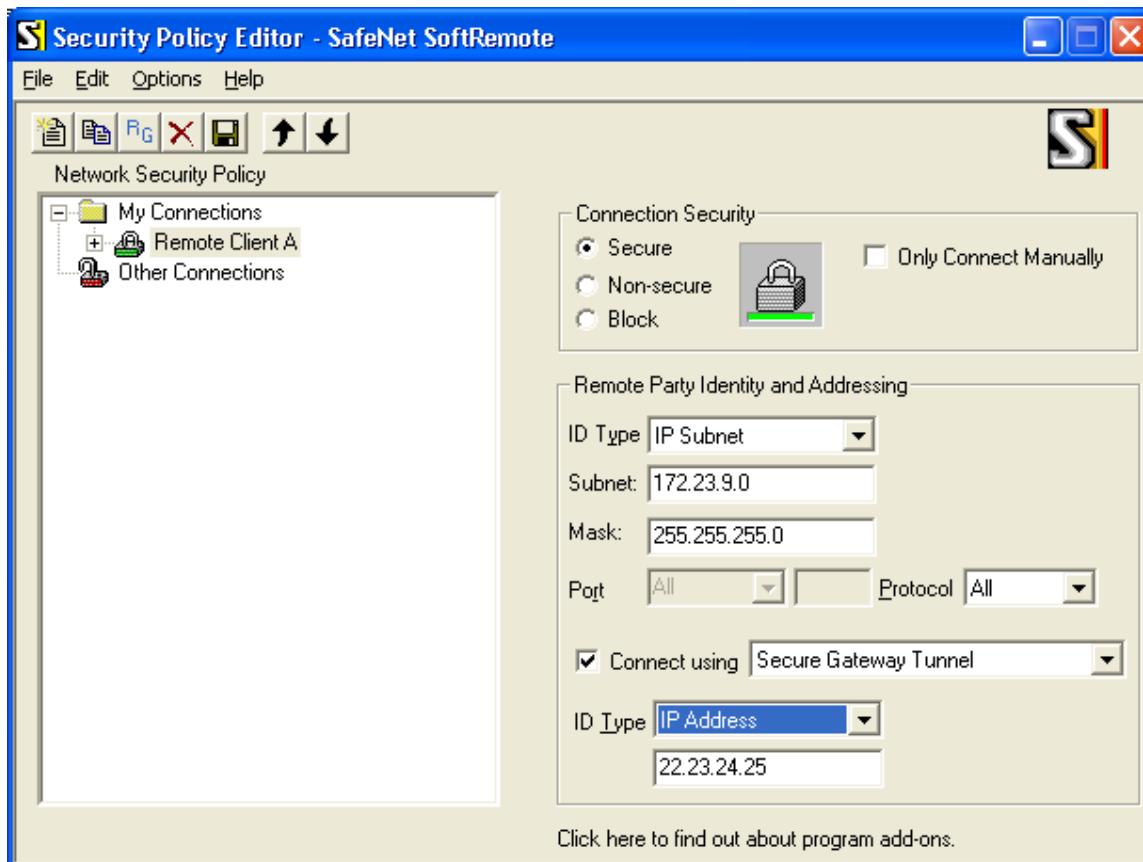


10. Use the CRLs option in Certificate Manager if your CA supports importing or updating CRLs.

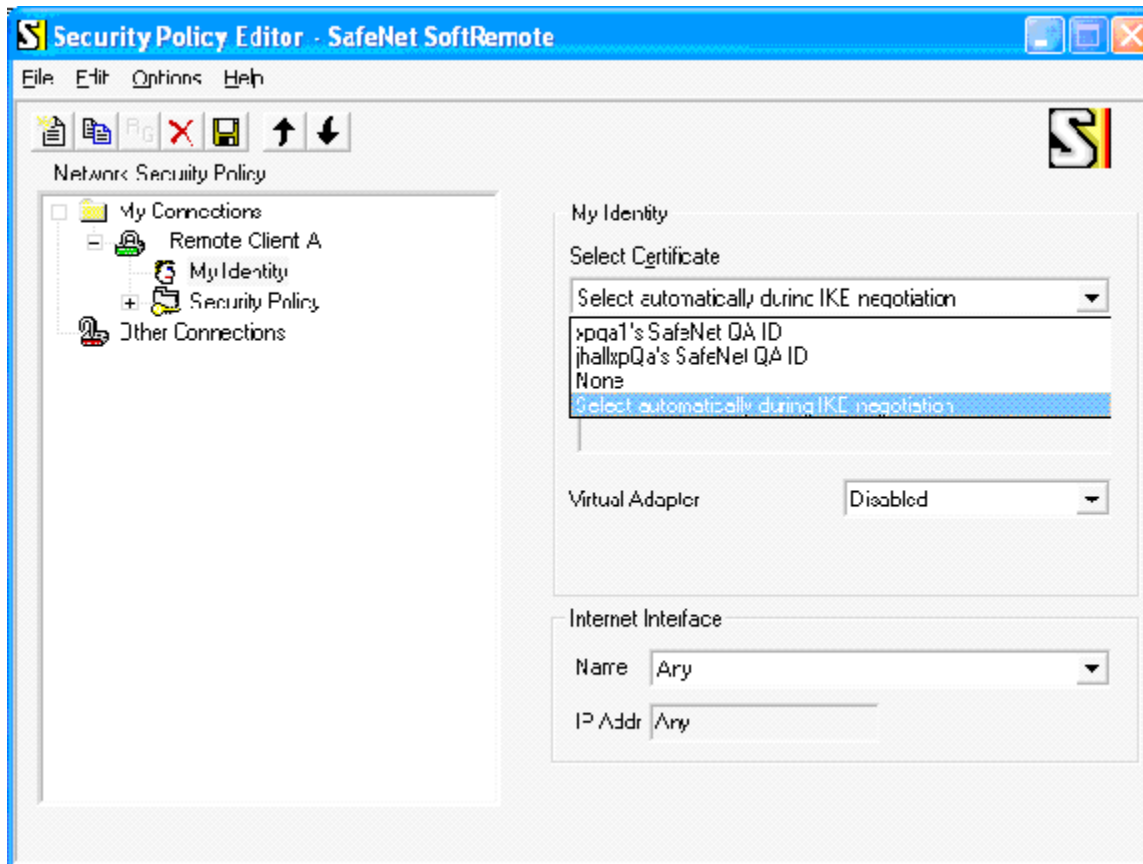


To set up client policy Phase1 for Gateway B for this scenario, use the following steps:

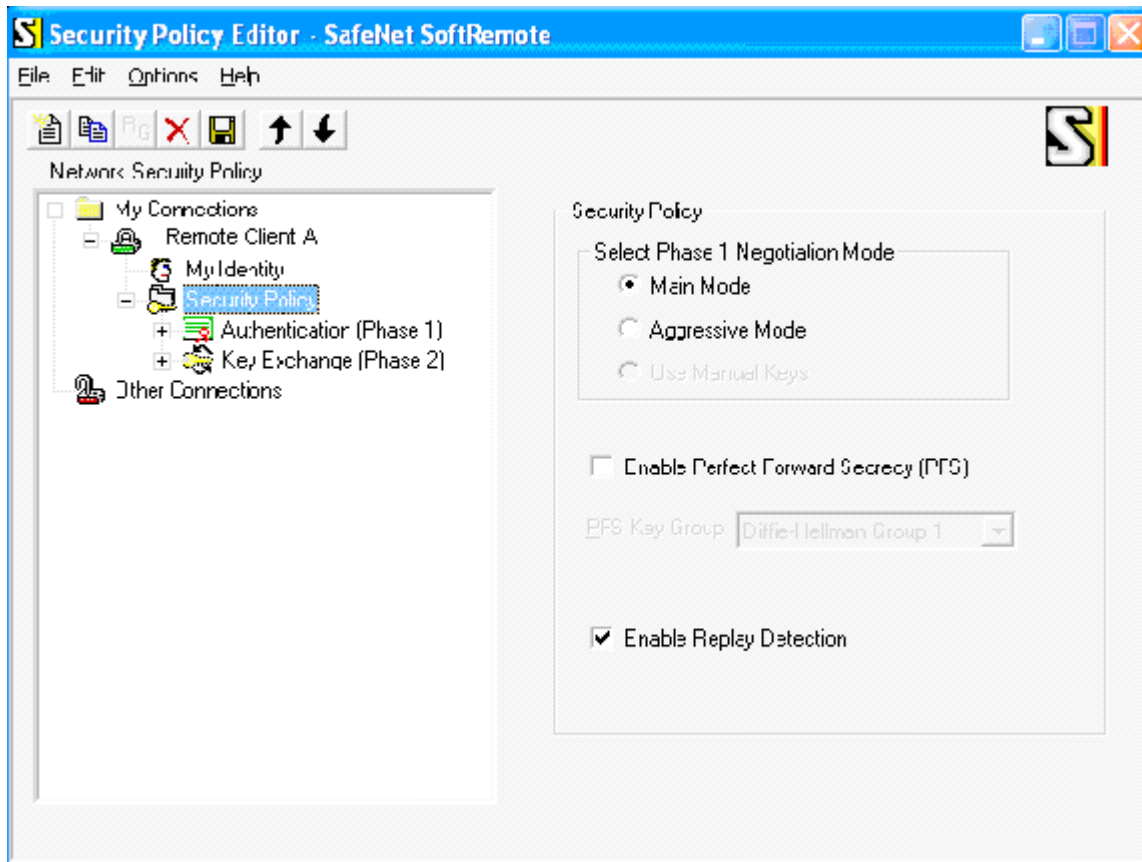
1. Open SafeNet SoftRemote Security Policy Editor by double clicking the SoftRemote system tray icon.  

2. To Add a new connection right click on My Connections, choose add – connection.
3. Name the new connection Remote Client A.
4. Set Connection Security to Secure.
5. Set the ID Type to IP subnet in Remote Party Identity and Addressing.
6. Set the Subnet and Mask to 172.23.9.0 / 255.255.255.0 in Remote Party Identity and Addressing.
7. Set Protocol and Port to All, default setting.
8. Check the box Connect using “Secure Gateway Tunnel”.
9. Set Gateway ID type to IP Address and enter the Gateways IP address 22.23.24.25.



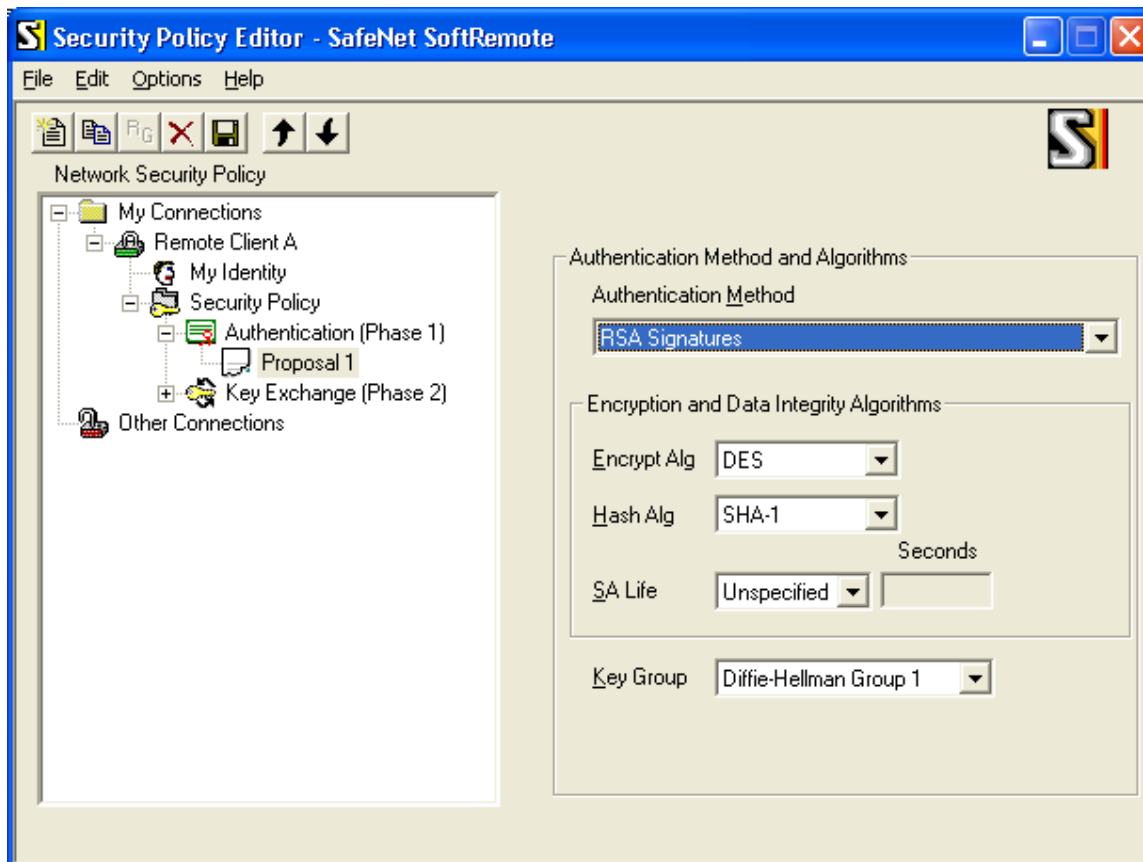
10. Open the My Identity Section of the connection by double clicking Remote Client A or clicking on the + next to Remote Client A.
11. Set the Select Certificate to a specific PKIX certificate or set to Select automatically during IKE negotiation in the My Identity field
12. Set the ID type and name that matches your Certificate requirements.
13. Port will default to All due to the previous port and protocol settings to All.
14. Set the Virtual Adapter to Disabled, to use the VA set it to Preferred or Required, this will require a Gateway that does Mode Config.
15. Set the Internet Interface to Any which will default the IP address to Any.



16. Open the Security Policy section of connection Remote Client A.
17. Set the Security Policy Phase 1 Negotiation Mode to Main Mode.
18. Leave Enable PFS unchecked since it is not being used by the Gateway. To use PFS, check the box Enable PFS and select the desired DH group type.
19. Check Enable Replay Detection.



20. Open Proposal 1 of Authentication (Phase 1) by double clicking Security Policy then double clicking Authentication (Phase1).
21. Authentication Method and Algorithms will default to RSA Signatures due to our previous certificate selection in “My Identity”.
22. Set Encryption Algorithm to Triple DES.
23. Set Hash Algorithm to SHA-1
24. Set the SA Life to Seconds and enter 28800 seconds, this field can be left Unspecified since the client will respond to Gateway initiated re-keying.
25. Set the Key Group to DH Group 2.




The **IKE Phase 2 parameters** used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying
- Selectors for all IP protocols, all ports, between 0.0.0.0 and 172.23.9.0/24, using IPv4 subnets

To set up client policy Phase2 for Gateway B for this scenario, use the following steps:

26. Open Proposal 1 of Key Exchange (Phase 2) of Remote Client A by double clicking Key Exchange (Phase 2) or clicking on the + of Key Exchange (Phase 2).
27. Set the IPsec Protocols SA Life to Seconds and enter 3600 seconds, this field can be left Unspecified since the client will respond to Gateway initiated re-keying.
28. Leave Compression set to None.
29. Check the box Encapsulation Protocol (ESP).
30. Set the Encryption Algorithm to Triple DES
31. Set the Hash Algorithm to SHA-1.
32. Set Encapsulation to Tunnel.

33. Save the policy by clicking on the diskette image  or click on the File tab and save changes.
34. To connect to the 172.23.9.0 network, first connect to the Internet, then ping or ftp a host behind the Gateway, use the connection monitor and log viewer to monitor the session establishment. Look for the system tray icon to get a key and a green bar will indicate when secure traffic passes. 