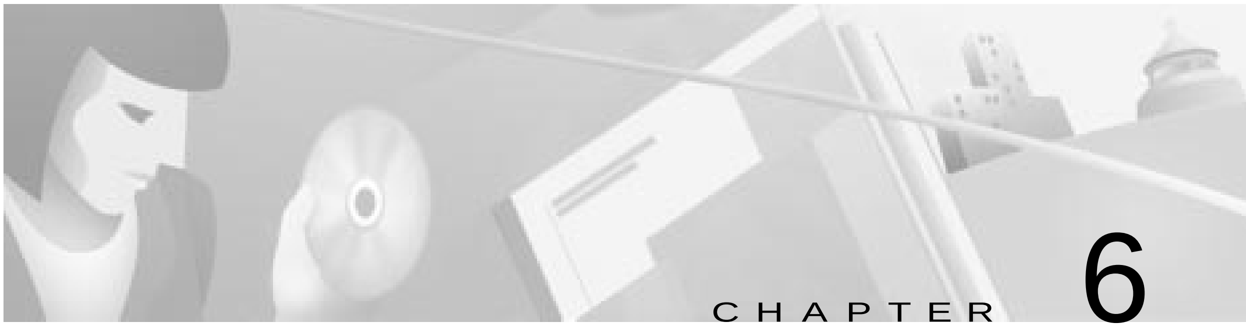


CHAPTER 6

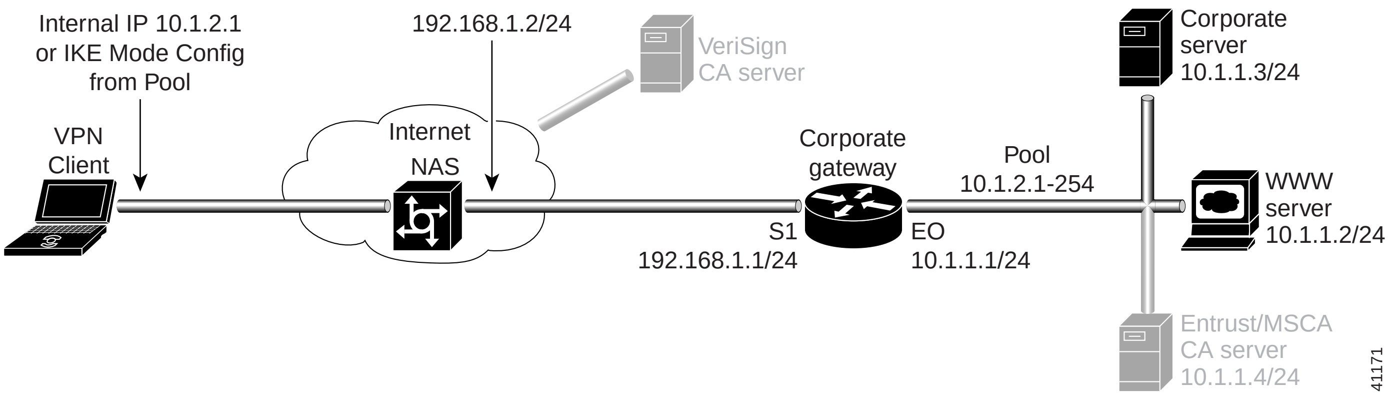
Configuring Digital Certification

This chapter describes how Cisco Secure VPN Client interoperates with Cisco networking devices using digital certificates in certification authority (CA) and Registration Authority (RA) modes with file-based enrollment and Simple Certificate Enrollment Protocol (SCEP). Using IPSec, digital certificates allow devices to be automatically authenticated to each other without manual key exchanges. This chapter includes the following sections:

- Task 1—Configuring Digital Certifications on the VPN Client
- Task 2—Configuring Digital Certification on the Gateway

Note Throughout this chapter, there are numerous configuration examples that include unusable IP addresses, passwords, and public key examples. Be sure to use your own IP addresses, passwords, and public keys when configuring your VPN Clients and gateway.

Figure 6-1 Digital Certificate Topology



Task 1—Configuring Digital Certifications on the VPN Client

- Importing the Root CA Certificate
- Creating a Public and Private Key Pair
- Sending the Certification Request to the CA Server
- Importing Your Signed Digital Certificate
- Configuring a New Gateway for a Security Policy
- Specifying the VPN Client's Identity
- Configuring Authentication on the VPN Client

Note Before configuring digital certification, it is recommended you configure pre-shared key authentication to establish VPN connectivity for debugging purposes. Once you have successfully established the VPN, then you can implement digital certification.

For details on configuring pre-shared keys, refer to Chapter 5, "Configuring a Pre-Shared Key or Wildcard Pre-Shared Key."

Importing the Root CA Certificate

To import the root CA certificate on the VPN Client, perform the following steps:

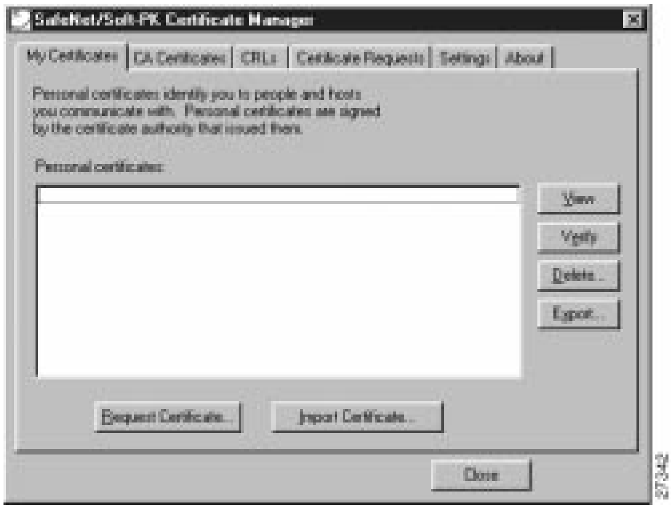
- Open the My Certificates Folder
- Open the CA Certificates Folder
- Import the Root CA Certificate
- Locate the Root CA File

To open the My Certificates folder

Click **Start**>**Programs**>**Cisco Secure VPN Client**>**Certificate Manager**.

The SafeNet/Soft-PK Certificate Manager dialog box appears with the My Certificates folder as a default, as shown in Figure 6-2. Table 6-1 describes the field descriptions for the My Certificates folder.

Figure 6-2 My Certificates Folder



Personal certificates identify you to people and hosts you communicate with. Personal certificates are signed by the certificate authority that issued them.

Personal certificates:

Table 6-1 My Certificates Folder Field Descriptions

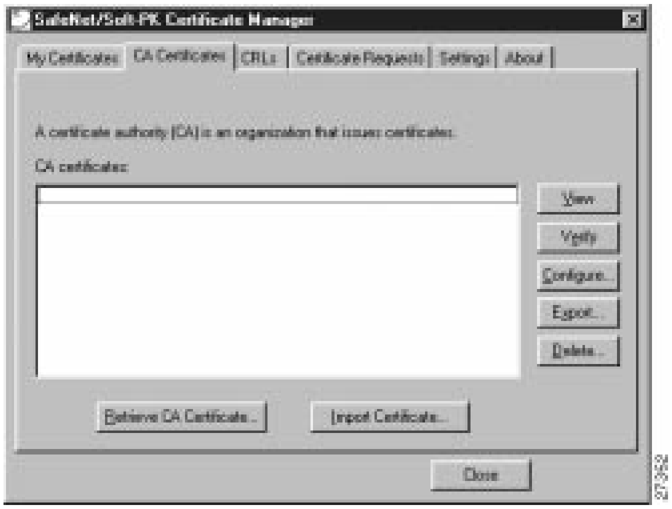
Field	Description
Certificate Manager	This folder allows you to request, import, and store the digital certificates that you receive from the certification authority (CA). There are two types of digital certificates: root CA certificates and personal certificates.
My Certificates	This folder shows the available personal certificates and provides options for certificate management.
Personal certificates	This box lists the personal digital certificates available for this VPN Client. You must have your own personal digital certificate from a CA, which verifies your identity to the IPSec peers with which you will communicate. **Note** You must have a root CA certificate before you can request a personal certificate.
• View • Verify • Delete • Export	• When clicked, this button allows you to view the contents of your digital certificate issued by the CA. • When clicked, this button prompts the VPN Client to check the validity dates and to check the digital certificate against its revocation list. An information window returns the current status of the certificate along with its content. • When clicked, this button allows you to delete a digital certificate. • When clicked, this button allows you to export or copy a digital certificate.
• Request Certificate • Import Certificate	• When clicked, this button allows you to request a certificate from a specified CA on the Internet. • When clicked, this button allows you to import a certificate.

To open the CA Certificates folder

Click the **CA Certificates** tab.

The CA Certificates Folder appears as shown in Figure 6-3. Table 6-2 describes the field descriptions for the CA Certificates folder.

Figure 6-3 CA Certificates Folder



A certificate authority (CA) is an organization that issues certificates.

CA certificates:

Table 6-2 CA Certificates Folder Field Descriptions

Field	Description
CA Certificates	This folder allows you to retrieve, import, view, verify, configure, export, or delete the certificates you receive from the CA.
CA certificates	This box lists the root CA digital certificates available for this VPN Client. Each CA you contact must provide you with its own root CA digital certificate, which verifies its identity. **Note** You must have a root CA certificate before you can request a personal certificate.

Table 6-2 CA Certificates Folder Field Descriptions (continued)

Field	Description
• View	• When clicked, this button allows you to view the contents of your digital certificate issued by the CA.
• Verify	• When clicked, this button prompts the VPN Client to check the validity dates and to check the digital certificate against its revocation list. An information window returns the current status of the certificate along with its content.
• Delete	• When clicked, this button allows you to delete a digital certificate.
• Export	• When clicked, this button allows you to export or copy a digital certificate.
• Request Certificate	• When clicked, this button allows you to request a certificate from a specified CA on the Internet.
• Import Certificate	• When clicked, this button allows you to import a certificate.

To import the Root CA certificate

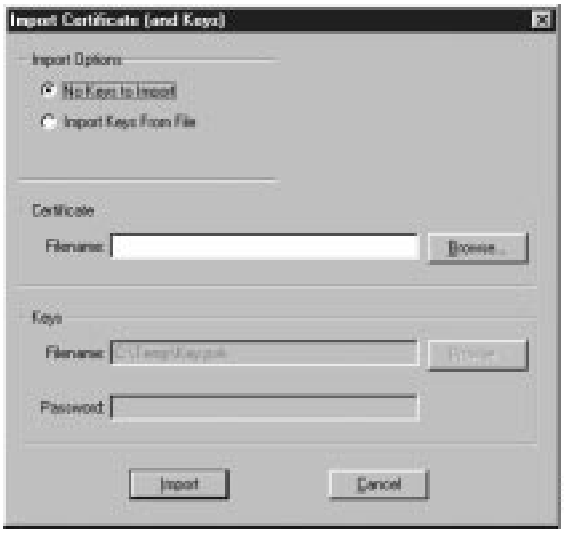
Step 1 In the CA Certificates Folder, click **Import Certificate**.

The Import Certificate (and Keys) dialog box appears as shown in Figure 6-4. Table 6-3 describes the field descriptions for the Import Certificate (and Keys) dialog box.

Step 2 Under Import Options, click the **No Keys to Import** option.

Step 3 Under Certificate, click **Browse**.

Figure 6-4 Import Certificate (and Keys) Dialog Box



Import Certificate (and Keys)

Import Options

● No Keys to Import

○ Import Keys From File

Certificate

Filename:

Keys

Filename: C:\temp\Key.pvk

Password:

Table 6-3 Import Certificate (and Keys) Dialog Box Field Descriptions

Field	Description
Import Certificate (and Keys)	This dialog box allows you to import a previously exported digital certificate or to import a recently downloaded digital certificate. Use this dialog box to obtain the root CA file from the system administrator, who should also supply you with the URL for IPSec CSR enrollment. The system administrator receives the root CA file and URL from the CA Administrator.
Import Options	Under Import Options, specify whether or not you want to import your keys by indicating either the No Keys to Import option or the Import Keys From File option.
• No Keys to Import	• This option indicates that you downloaded the CA certificate, or the CA sent a personal certificate to you in an e-mail, directed you to copy it from a server, or gave it to you on a floppy disk because you chose not to request one online. No keys require importing because the keys should be in the same file as the certificate.
• Import Keys From File	• This option indicates that you are importing a certificate file that you or your network administrator exported from the Certificate Manager window under My Identity. The keys for this personal certificate would have been copied to this file when you or your network administrator exported it.
Certificate	Under Certificate, specify the location of the certificate file using the Filename box.
• Filename	This box allows you to enter the certificate file's drive, directory, and filename, or use Browse to find it.
Keys	Under Keys, you can specify the location of the certificate file with keys.
• Filename	• This box is activated when you click the Import Keys From File option. Enter the filename to import a certificate file, or click Browse to find it.
• Password	• This box is activated when you click the Import Keys From File option. Enter the password to import a certificate file.
• Import	• When clicked, this button allows you to either import the digital certificate specified.

To locate the Root CA file

Step 1 From the CA Certificates Folder, click **Import**.

The Open dialog box appears, as shown in Figure 6-5. Use the Open dialog box to locate the root CA file on your hard drive. Open the root CA file for importing to the CA Certificates folder.

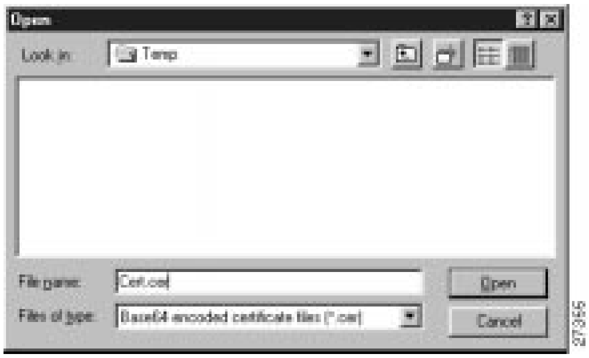
Step 2 In the Files of Type list, click **Base64 encoded certificate files**.

Step 3 Locate the root CA file (the *.cer* file), and then click **Open**.

The Import Certificate (and Keys) dialog box reappears, as shown in Figure 6-4.

Step 4 To add the certificate to the root store, click **Import.**

Figure 6-5 Open Dialog Box



Look in: Temp

File name: Cert.cer

Files of type: Base64 encoded certificate files (*.cer)

Creating a Public and Private Key Pair

To create a public and private key pair, perform the following tasks:

- Open My Certificates Folder
- Specify Online Certificate Request

To open the My Certificates folder

Click **Start**>**Programs**>**Cisco Secure VPN Client**>**Certificate Manager**.

The SafeNet/Soft-PK Certificate Manager dialog box appears with the My Certificates folder as a default, as shown in Figure 6-2. Table 6-1 describes the field descriptions for the My Certificates folder.

Note You must have your root CA certificate before requesting a personal certificate. Otherwise, only a file-based request is possible.

To specify On-line Certificate Request

Step 1 In the SafeNet/Soft-PK Certificate Manager, click **Request Certificate**.

Note To configure an online enrollment, you must click the **CA Certificate** tab in the Certificate Manager dialog box, and retrieve a CA certificate first.

The Online Certificate Request dialog box appears. Figure 6-6 shows the Online Certificate Request window. Table 6-4 describes the field descriptions for the Online Certificate Request window.

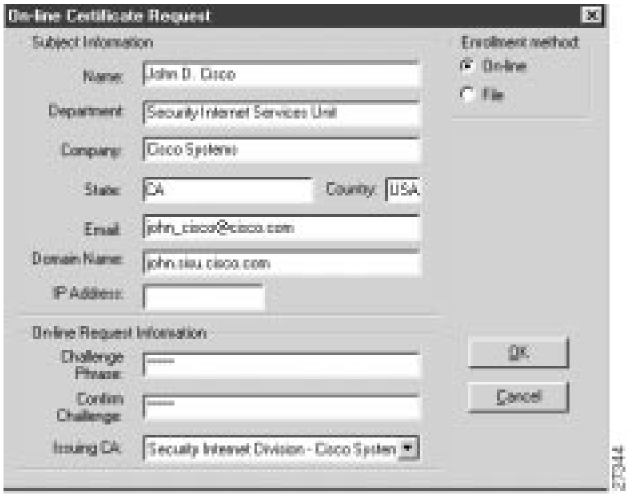
Step 2 In the Online Certificate Request dialog box, fill in the sections based on the identity of the owner of the certificate, and then click **OK**.

Figure 6-6 shows how these sections can be specified. Be sure to use your own identity specifications.

The client will generate public/private key pairs.

Note This information binds your identity to a public key that others will look for in a public key directory. Entering inaccurate or misleading information defeats the purpose of using public key.

Figure 6-6 Online Certificate Request



On-line Certificate Request

Subject Information

Name: John D. Cisco

Department: Security Internet Services Unit

Company: Cisco Systems

State: CA Country: USA

Email: john_cisco@cisco.com

Domain Name: john.siu.cisco.com

IP Address:

Online Request Information

Challenge Phrase: ******

Confirm Challenge: ******

Issuing CA: Security Internet Division - Cisco System

Enrollment method

● On-line

○ File

Table 6-4 Online Certificate Request

Field	Description
On-line Certificate Request	This dialog box allows you to specify public and private key pairs and enroll your personal certificate online. You can configure a certificate request for online or file-based enrollment.
Subject Information	Under Subject Information, specify the identity of the certificate owner, including Name, Department, Company, State, Email, Domain Name, and IP Address options.
• Name	• This box allows you to enter the certificate owner's name.
• Department	• This box allows you to enter the certificate owner's department.
• Company	• This box allows you to enter the certificate owner's company.
• State	• This box allows you to enter the state where the company headquarters is located.
• Email	• This box allows you to enter the certificate owner's email address.
• Domain Name	• This box allows you to enter the domain of the company.
• IP Address	• This box allows you to specify an IP address, but you need not enter anything here.

Table 6-4 Online Certificate Request (continued)

Field	Description
Online Request Information	Under Online Request Information, fill in the Challenge Phrase, Confirm Challenge, and Issuing CA box.
• Challenge Phrase	• This box allows you to enter a challenge phrase to be used to identify you in the event you choose to cancel or replace your digital certificate. You must remember this phrase.
• Confirm Challenge	• This box allows you to confirm your phrase.
• Issuing CA	• This box allows you to select a CA server issuing the certificate.

Sending the Certification Request to the CA Server

- To configure Entrust digital certificates, see Appendix A, "Configuring Entrust Digital Certificates."
- To configure Microsoft digital certificates, see Appendix B, "Configuring Microsoft Certificate Services."
- To configure VeriSign digital certificates, see Appendix C, "Configuring VeriSign Digital Certificates."

Importing Your Signed Digital Certificate

To import the signed digital certificate on the VPN Client, perform the following steps:

- Open the My Certificates Folder
- Import the Signed Digital Certificate
- Locate the Signed Digital Certificate
- Confirm Signed Digital Certificate

To open the My Certificates folder

Click **Start**>**Programs**>**Cisco Secure VPN Client**>**Certificate Manager**.

The SafeNet/Soft-PK Certificate Manager dialog box appears with the My Certificates folder as a default, as shown in Figure 6-2. Table 6-1 describes the field descriptions for the My Certificates folder.

To import the signed digital certificate

Step 1 In the My Certificates Folder, click **Import Certificate**.

Note The CA Administrator should have sent you a signed digital certificate through email.

The Import Certificate (and Keys) dialog box appears, as shown in Figure 6-4. Table 6-3 describes the field descriptions for the Import Certificate (and Keys) dialog box.

Step 2 In the Import Certificate (and Keys) dialog box, select the **No Keys to Import** option.

Step 3 Under Certificate, click **Browse**.

To locate and import the signed digital certificate

Step 1 From the My Certificates Folder, click **Import**.

The Open dialog box appears, as shown in Figure 6-5.

Step 2 In the Files of Type list, click **Base64 encoded certificate files**.

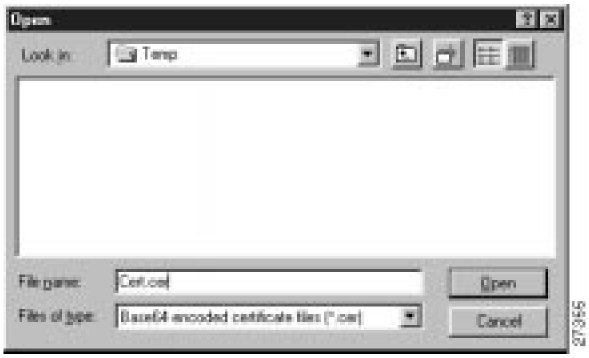
Step 3 Add your signed digital certificate, and then rename the file with a "**.cer**" filename extension.

Step 4 Select your signed digital certificate, and then, click **Open**.

The Import Certificate (and Keys) dialog box reappears.

Step 5 Click **Import**.

Figure 6-7 Open Dialog Box



Look in: Temp

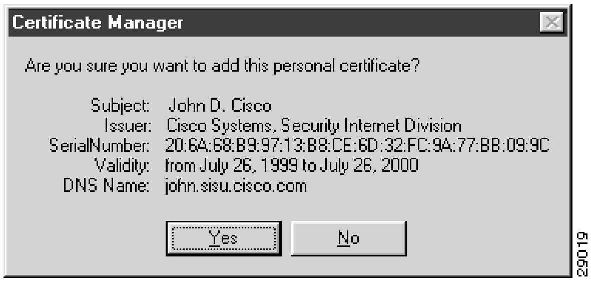
File name: Cert.cer

Files of type: Base64 encoded certificate files (*.cer)

To confirm signed digital certificate

After clicking Import, the Certificate Manager dialog box appears displaying the personal certificate to be added, as shown in Figure 6-8. To confirm that you want to add this personal certificate, click **Yes**.

Figure 6-8 Certificate Manager Dialog Box



Are you sure you want to add this personal certificate?

Subject: John D. Cisco
Issuer: Cisco Systems, Security Internet Division
SerialNumber: 20:6A:68:B9:97:13:B8:CE:6D:32:FC:9A:77:BB:09:9C
Validity: from July 26, 1999 to July 26, 2000
DNS Name: john.sisu.cisco.com

Configuring a New Gateway for a Security Policy

To configure a new gateway for a security policy on a VPN Client, perform the following tasks:

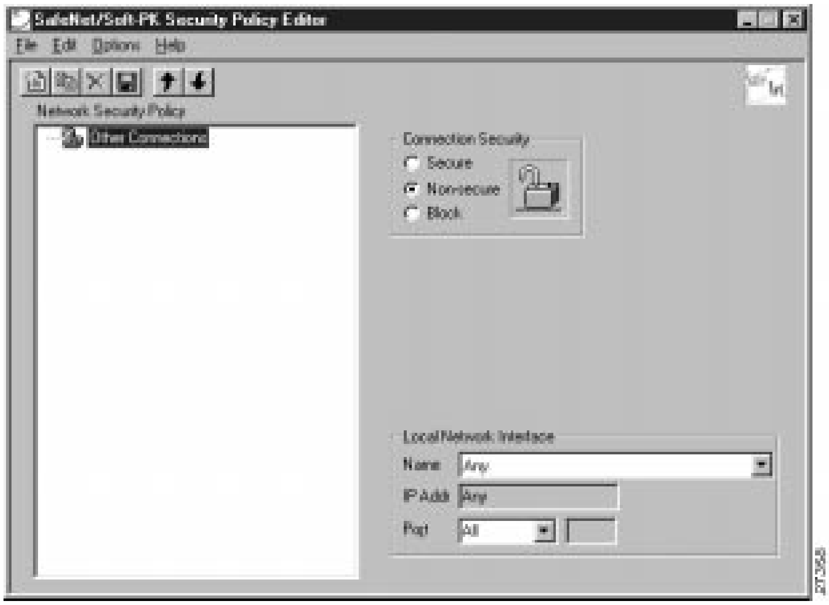
- Open the Security Policy Editor
- Configure Other Connections
- Create a New Connection
- Define the New Connection

To open the Security Policy Editor

Click **Start**>**Programs**>**Cisco Secure VPN Client**>**Security Policy Editor**.

The SafeNet/Soft-PK Security Policy Editor dialog box appears, as shown in Figure 6-9. Table 6-5 describes the field descriptions for the SafeNet/Soft-PK Security Policy Editor.

Figure 6-9 SafeNet/Soft-PK Security Policy Editor



Connection Security: ○ Secure ● Non-secure ○ Block

Local Network Interface
Name: Any
IP Addr: Any
Port: All

Table 6-5 SafeNet/Soft-PK Security Policy Editor Window Field Descriptions

Field	Description
Security Policy Editor	This window establishes connections and their associated proposals, and lists connections in a hierarchical order that defines an IP data communications security policy.
Other Connections	This object is a policy, or a default connection, and the first step in establishing security policies for individual connections.

Table 6-5 SafeNet/Soft-PK Security Policy Editor Window Field Descriptions (continued)

Field	Description
Connection Security	Under Connection Security, you can define IP access for this connection using Secure, Non-secure, and Block options.
• Secure	• This option secures the IP communications for this connection.
• Non-secure	• This option allows for IP communications to occur without encryption, and allows you to change any settings under your Internet Interface or Local Network Interface.
• Block	• This option denies all IP communications to the VPN Client.

To configure other connections

Step 1 From the **Options** menu, click **Secure**>**Specified Connections**.

In the left pane, **Other Connections** appears.

The Other Connections pane appears in the right pane. Use the Other Connections as the default for your security policy.

Step 2 In the right pane, under Connection Security, click the **Non-Secure** option. Leave all other fields as-is.

Figure 6-9 shows how this is displayed on the Other Connections pane. Table 6-6 describes the field descriptions for the Other Connections pane.

To create a new connection

Step 1 In the left pane, click **Other Connections**.

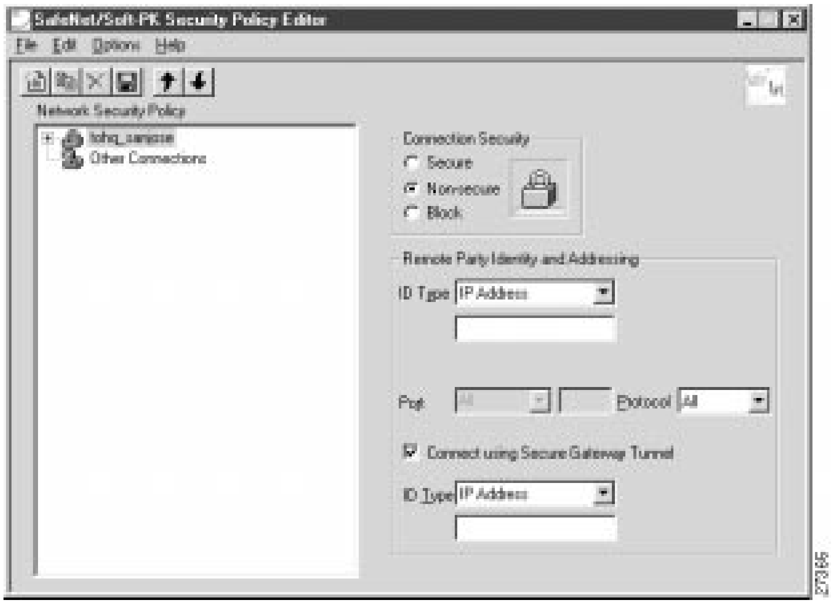
Step 2 On the **File** menu, click **New Connection**.

In the left pane, the default **New Connection** placeholder appears for the New Connection pane.

Step 3 Select **New Connection**, and in its place, define a unique name for the connection to your gateway.

For example, if your router name is `hq_sanjose`, you might rename the connection **`tohq_sanjose`**, as shown in Figure 6-10. Table 6-6 describes the field descriptions for the New Connection pane.

Figure 6-10 Renaming a New Connection



○ Secure
● Non-secure
○ Block

ID Type: IP Address

Port: All

Protocol: All

☑ Connect using Secure Gateway Tunnel

ID Type: IP Address

To define the new connection

Step 1 In the left pane, click your new connection. In this example, **tohq_sanjose** is clicked.

The New Connection pane appears in the right pane.

Step 2 In the right pane, under Connection Security, click the **Secure** option.

Step 3 In the right pane, under Remote Party Identity and Addressing, enter the following:

a. From the ID Type list, click **IP Subnet**. In this example, the IP address of the corporate subnet, **10.1.1.0** is entered.

b. In the Mask list, enter the subnet mask of the IP address of your corporate subnet. In this example, the subnet mask of the corporate subnet, **255.255.255.0** is entered.

c. The Port list and box are inactive as a default.

d. In the Protocol list, click **All**.

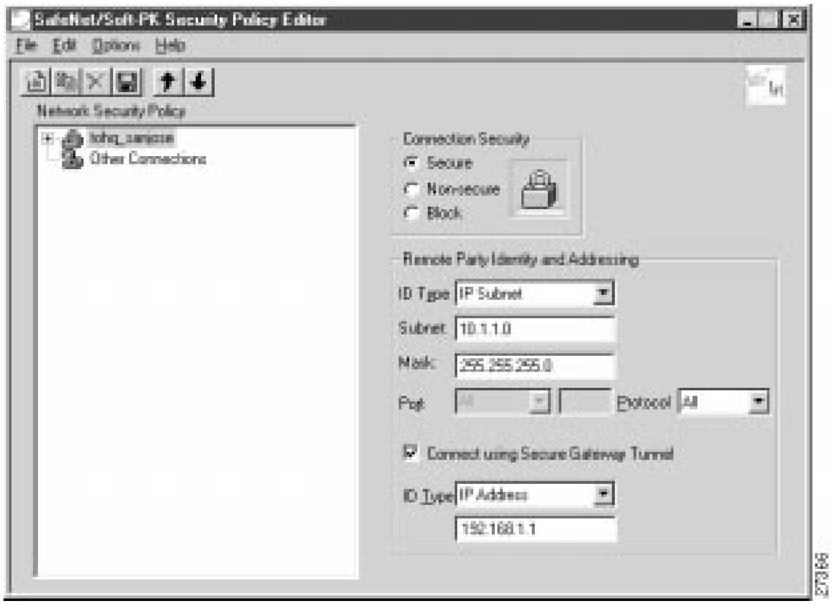
e. Select the **Connect using Secure Gateway Tunnel** check box.

f. In the ID_Type list, click **IP Address**.

g. In the ID_Type box, enter the IP address of the secure gateway. In this example the secure gateway, **192.168.1.1** is entered.

Figure 6-11 shows how this is displayed on the New Connection pane for digital certificates. Table 6-6 describes the field descriptions for the New Connection pane.

Figure 6-11 Defining a New Connection for Digital Certificates



Connection Security
● Secure
○ Non-secure
○ Block

Remote Party Identity and Addressing
ID Type: IP Subnet
Subnet: 10.1.1.0
Mask: 255.255.255.0
Port: All
Protocol: All
☑ Connect using Secure Gateway Tunnel
ID Type: IP Address
192.168.1.1

Table 6-6 New Connection Pane Field Descriptions

Field	Description
Network Security Policy	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed.
• New Connection	• This object is a set of security parameters that pertain to an individual remote IP connection. *New Connection* is the default connection name.
• Other Connections	• This object is a policy, or a default connection, and the first step in establishing security policies for individual connections. For all IP communications that do not adhere to the security policies defined in the individual connections, Other Connections acts as a default. Other Connections is always the last rule among security policies.
Connection Security	Under Connection Security, you can define IP access for this connection using Secure, Non-secure, and Block options.
• Secure	• This option secures the IP communications for this connection.
• Non-secure	• This option allows for IP communications to occur without encryption, and allows you to change any settings under your Internet Interface or Local Network Interface.
• Block	• This option denies all IP communications to the VPN Client.
Remote Party Identity and Addressing	Under Remote Party Identity and Addressing, define the IPSec peer with which the VPN Client will establish a secure tunnel.

Table 6-6 New Connection Pane Field Descriptions (continued)

Field	Description
ID Type	This list displays options for defining the IPSec peer identity including IP address, domain name, email address, IP subnet, IP address range, and distinguished name. IP subnet is the default option. Depending on the option you choose, different values will appear in the right pane.
• IP Address	• This option allows a static IP address to be configured on the VPN Client.
– IP address value	– In this box, specify the IP address value.
• Domain Name	• This option enables the domain name value box and the IP Address box.
– Domain name value	– In this box, specify the domain name value.
– IP Address	– In this box, specify the IP address of the domain, the organizational IP address.
• Email Address	• This option allows you to indicate the email address of the peer.
– Email value	– In this box, specify the e-mail value.
– IP address value	– In this box, specify the peer’s IP address.
• IP Subnet	• This option allows you to specify the IP subnet the client will be allowed to access using this peer.
– Subnet	– In this box, specify the subnet IP address.
– Mask	– In this box, specify the mask IP address.
• IP Address Range	• This option allows you to indicate the range of IP addresses to which this client will have access.
– From	– In this box, specify the beginning IP address.
– To	– In this box, specify the ending IP address.
• Distinguished Name	• This option allows you to specify the name, department, state, and country of the peer identity.
– Edit Name	– When clicked, this button allows you to specify the distinguished name settings.
– IP Address	– In this box, specify the peer’s IP address.
Port	This list shows the IPSec peer’s protocol ports. A default of *All* secures all protocol ports.
Connect using Secure Gateway Tunnel	If selected, this check box specifies that the IPSec peer is protected by a secure IPSec-compliant gateway, such as a firewall.

Table 6-6 New Connection Pane Field Descriptions (continued)

Field	Description
ID_Type	This list shows the identification type of the gateway including IP address, domain name, and distinguished name. IP Address is the default option. Depending on the option you choose, different values will appear in the right pane.
• IP Address	• This option enables the IP address value box.
– IP address value	– In this box, specify the IP address value.
– Domain Name	– This option enables the domain name value box and the IP Address box.
– Domain name value	– In this box, specify the domain name value.
– IP Address	– In this box, specify the IP Address of the domain.
• Distinguished Name	• This option allows you to specify the name, department, state, and country of the gateway.
– Edit Name	– When clicked, this button allows you to specify the distinguished name settings.
– IP Address	– In this box, specify the gateway's IP address.

Specifying the VPN Client's Identity

To specify the remote party's identity on a VPN Client, you must choose an identity, as follows:

To choose an identity

Step 1 In the left pane, double-click your new connection. In this example, **tohq_sanjose** is clicked.

The new connection expands with My Identity and Security Policy.

Step 2 Click **My Identity**.

The My Identity pane appears in the right pane. Figure 6-12 shows how this is displayed on the My Identity pane. Table 6-6 describes the field descriptions for the My Identity pane.

Step 3 In the right pane, Under My Identity, select the following:

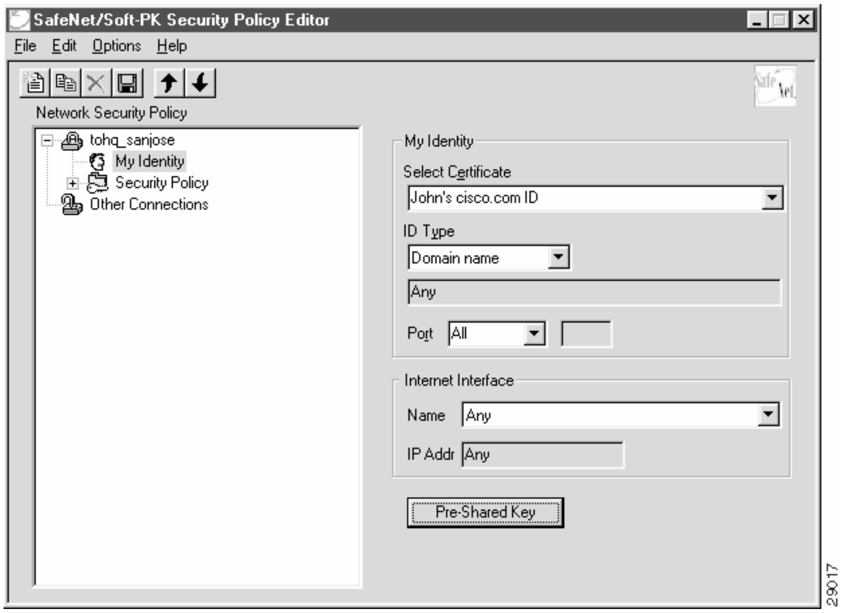
a. From the Select Certificate list, click your digital certificate. In this example, **John's example.com ID** is selected.

b. In the ID_Type list, click **Domain name**.

c. In the Port list, click **All**.

d. In the Name list, click **Any**. The IP Addr list is inactive as a default.

Figure 6-12 My Identity Pane



My Identity

Select Certificate: John's cisco.com ID

ID Type: Domain name

Any

Port: All

Internet Interface

Name: Any

IP Addr: Any

Table 6-7 My Identity Pane Field Descriptions

Field	Description
Network Security Policy • New Connection>My Identity	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed. • This pane allows you to specify the identity of the VPN Client. Choose an identification that will allow the other party to identify you during the key exchange phase.
My Identity	Under My Identity, specify options for determining the identity of the VPN Client. These options include Select Certificate, ID Type, Port and Name lists.
Select Certificate	If you are using digital certification, this list displays all the available digital certificates from which to choose. If you are not using digital certification, *None* is the default option.
ID_Type	This list indicates the IP address option for the VPN Client on the corporate subnet.
• Domain Name	• This box indicates that the VPN Client will be identified by the gateway using the domain name of the certificate identity. This is the default.
Port	This list shows the VPN Client's protocol ports. A default of *All* secures all protocol ports.

Table 6-7 My Identity Pane Field Descriptions (continued)

Field	Description
Local Network Interface	Under Local Network Interface, the hardware interface on the PC or laptop through which the connection will be established.
Name	This list indicates the names of the hardware interfaces on the PC or laptop. A default of *Any* enables all hardware interfaces.
IP Addr	This list indicates the IP addresses of the hardware interfaces on the PC or laptop. A default of *Any* enables all hardware interface IP addresses.
• Pre-Shared Key	• When clicked, this button enables the Pre-Shared Key dialog box. This button is not used while configuring digital certificates.

Configuring Authentication on the VPN Client

To configure authentication on the VPN Client, perform the following tasks:

- Specify Authentication Security Policy
- Specify Authentication for Phase 1 IKE
- Specify Authentication for Phase 2 IKE

To specify authentication security policy

Step 1 In the left pane, under My Identity, double-click **Security Policy**.

The Security Policy pane appears in the right pane.

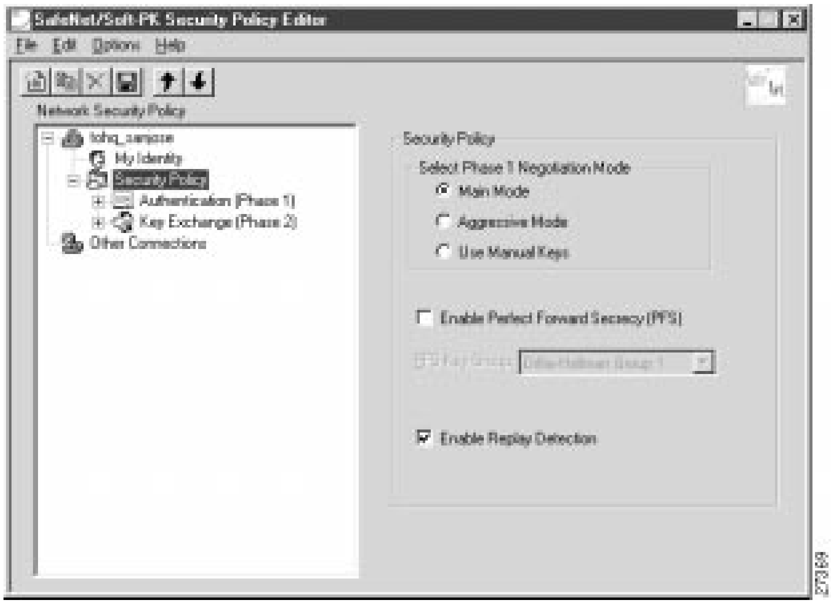
Step 2 In the right pane, under Security Policy, select the following:

a. Click **Main Mode**.

b. Select the **Enable Replay Detection** check box.

Figure 6-13 shows how this is displayed on the Security Policy pane. Table 6-8 describes the field descriptions for the Security Policy pane.

Figure 6-13 Security Policy Pane



Network Security Policy

- tohq_sanjose
  - My Identity
  - Security Policy
    - Authentication (Phase 1)
    - Key Exchange (Phase 2)
- Other Connections

Security Policy

Select Phase 1 Negotiation Mode

● Main Mode

○ Aggressive Mode

○ Use Manual Keys

□ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 1

☑ Enable Replay Detection

Table 6-8 Security Policy Pane Field Descriptions

Field	Description
Network Security Policy • New Connection>Security Policy	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed. • This pane allows you to specify authentication and data integrity.
Security Policy	Under Security Policy, define the Select Phase 1 Negotiation Mode, Enable Perfect Forward Secrecy, or Replay Detection options.
Select Phase 1 Negotiation Mode • Main Mode • Aggressive Mode • Use Manual Keys	Under Select Phase 1 Negotiation Mode, select the mode for authenticating ISAKMP SAs using Main Mode, Aggressive Mode, or Use Manual Key options. • This option allows identities to not be revealed until all secure communications have been established, which requires a longer processing time. • This option allows identities to viewed while secure communications are taking place, which makes for a faster processing time. • This option is available for troubleshooting purposes only.
Enable Perfect Forward Secrecy	When selected, this check box triggers an authentication method protects against repeat compromises of a shared secret key.
Enable Replay Detection	When selected, this check box sets a counter, which determines whether or not a packet is unique to prevent data from being falsified.

To specify authentication for Phase 1 IKE

Step 1 In the left pane, double-click **Security Policy**, and then double-click **Authentication (Phase 1)**. Under Authentication (Phase 1).

A new proposal appears called *Proposal 1*.

Step 2 The Proposal 1 pane appears in the right pane.

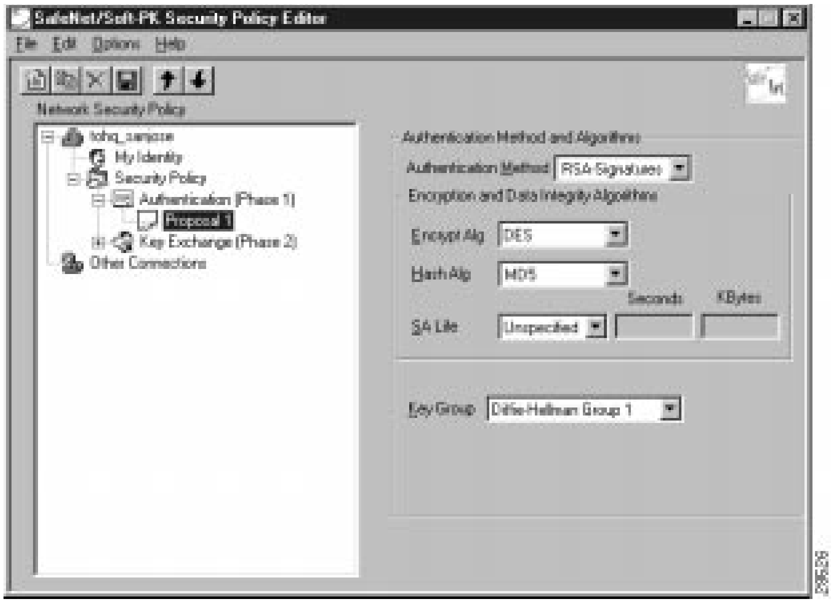
In the right pane, under Authentication Method and Algorithms, from the Authentication Method list, **RSA-Signatures** displays.

Step 3 In the right pane, under Authentication Method and Algorithms, select the following:

- **a.** In the Encrypt Alg list, click **DES**.
- **b.** In the Hash Alg list, click **MD5**.
- **c.** In the SA Life list, click **Unspecified**.
- **d.** In the Key Group list, click **Diffie-Hellman Group 1**.

Figure 6-14 shows how this is displayed on the Authentication Phase—Proposal 1 pane for pre-shared key. Table 6-9 describes the field descriptions for the Authentication Phase—Proposal 1 pane for pre-shared key.

Figure 6-14 Authentication (Phase 1)—Proposal 1 Pane



Authentication Method: RSA-Signatures

Encrypt Alg: DES

Hash Alg: MD5

SA Life: Unspecified

Key Group: Diffie-Hellman Group 1

Table 6-9 Authentication (Phase 1)—Proposal 1 Pane Field Descriptions

Field	Description
Network Security Policy • New Connection>Security Policy>Authentication (Phase 1)>Proposal 1	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed. • This pane allows you to specify authentication methods for Authentication Phase 1. During Authentication (Phase 1), you and your peer will reveal your identities and negotiate how they will secure Phase 2 communications. Before securing communications, the two peers involved negotiate the method they will use. Proposals are presented to the other peer in the order in which they are sequenced in the Network Security Policy list. You can reorder the proposals after you create them.
Authentication Method and Algorithms	Under Authentication Method and Algorithms, define the authentication method used and authentication and encryption algorithms.
Authentication Method • Pre-Shared Key • RSA Signatures	This list defines the authentication method being used, either Pre-Shared Key or RSA Signatures. The default is the method of authentication selected under My Identity. • This option appears if the method of authentication selected under My Identity is pre-shared key. • This option appears if the method of authentication selected under My Identity is digital certification.
Encryption and Data Integrity Algorithms	Under Encryption and Data Integrity Algorithms, define the algorithms to be used during Phase 1 negotiation including Encrypt Alg, Hash Alg, SA Life, and Key Group.
Encrypt Alg • DES • Triple-DES	This list allows you to specify encryption with DES or Triple DES options. • This option provides minimal security with 56-bit data encryption standard, which uses less processing time than does Triple-DES. • This option allows for maximum security with 168-bit data encryption standard, which uses more processing time than does DES. **Note** Triple DES is only supported within the U.S. domestic versions of both the Cisco IOS software and the VPN Client.

Table 6-9 Authentication (Phase 1)—Proposal 1 Pane Field Descriptions (continued)

Field	Description
Hash Alg	This list allows you to specify authentication with MD5 and SHA-1 options.
• MD5	• This option provides minimal authentication with 128-bit digest, which uses less processing time than does SHA.
• SHA-1	• This option allows for maximum authentication with 160-bit digest, which uses more processing time than does MD5. **Note** Cisco IOS software does not currently support the DES-MAC Hash Algorithm option.
SA Life	(Optional) This list allows you to specify the period for which the IKE SA is valid using Unspecified, Seconds, Kbytes, or Both options. **Note** When the VPN Client and gateway participate in IKE Phases 1 and 2 negotiation, the lowest SA life value offered by either device will be used as the agreed-upon value.
• Unspecified	• This option allows the other IPSec peer to indicate when IKE SA expires.
• Seconds	• This option allows you to specify SA life in seconds.
• Kbytes	• This option allows you to specify SA life in kilobytes.
• Both	• This option allows you to specify both seconds and kilobytes, whichever comes first, before an SA life expires.
Key Group	This list allows you to specify the Diffie-Hellman key exchange using Diffie-Hellman Group 1 or Diffie-Hellman Group 2 options. **Note** Cisco IOS software does not currently support Diffie-Hellman Group 5.
• Diffie-Hellman Group 1	• This option enables 768-bit encryption, which requires less processing time than does Diffie-Hellman Group 2.
• Diffie-Hellman Group 2	• This option enables 1024-bit encryption, which is more secure than Diffie-Hellman Group 1.

To specify authentication for phase 2 IKE

Step 1 In the left pane, under Authentication (Phase 1), double-click **Key Exchange (Phase 2)**.

In the left pane, under Key Exchange (Phase 2), a new proposal appears called *Proposal 1*.

Step 2 In the right pane, under IPSec Protocols, select the following:

a. In the **SA Life** list, click **Unspecified**.

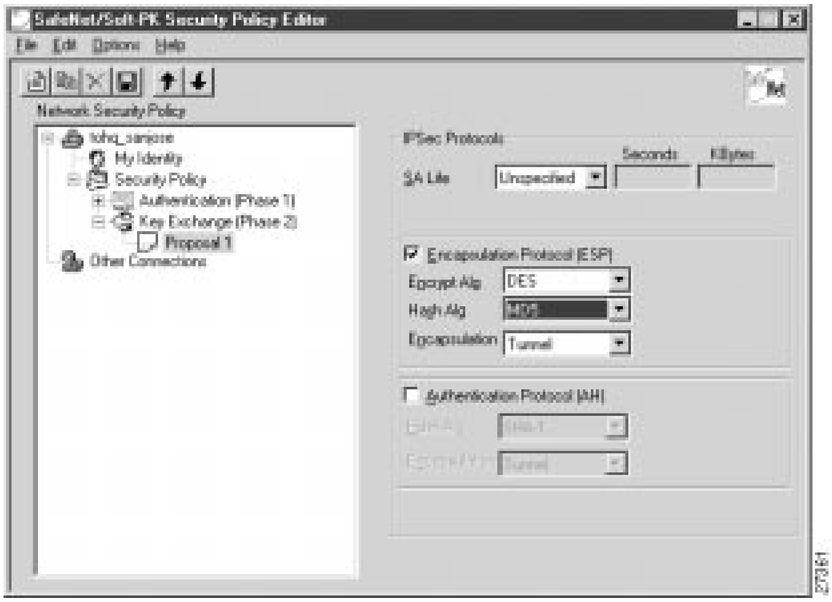
b. Select the **Encapsulation Protocol (ESP)** check box.

c. In the Encrypt Alg list, click **DES**.

d. In the Hash Alg list, click **MD5**.

e. In the Encapsulation list, click **Tunnel**.

Figure 6-15 Authentication (Phase 2)—Proposal 1 Pane



SA Life: Unspecified

☑ Encapsulation Protocol (ESP)

Encrypt Alg: DES

Hash Alg: MD5

Encapsulation: Tunnel

☐ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

Table 6-10 Authentication (Phase 2)—Proposal 1 Pane Field Descriptions

Field	Description
Network Security Policy • New Connection>Security Policy>Key Exchange (Phase 2)>Proposal 1	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed. • This pane allows you to specify authentication methods for Key Exchange (Phase 2). Set authentication requirements in the Security Policy pane. Negotiate which key exchange method of securing communications you and the other IPSec peer will use by establishing a proposal.
IPSec Protocols	Under IPSec Protocols, define the algorithms to be used during Phase 2 key exchange, including SA Life, Encrypt Alg, Hash Alg, and Encapsulation options.

Table 6-10 Authentication (Phase 2)—Proposal 1 Pane Field Descriptions (continued)

Field	Description
SA Life	This list allows you to specify the period for which the IKE SA is valid using Unspecified, Seconds, Kbytes, or Both options. **Note** When the VPN Client and gateway participate in IKE Phases 1 and 2 negotiation, the lowest SA life value offered by either device will be used as the agreed-upon value.
• Unspecified	• This option allows the other IPSec peer to indicate when IKE SA expires.
• Seconds	• This option allows you to specify SA life in seconds.
• Kbytes	• This option allows you to specify SA life in kilobytes.
• Both	• This option allows you to specify both seconds and kilobytes, whichever comes first, before an SA life expires.
Encapsulation Protocol	If selected, this check box indicates that encryption and authentication will be selected for this proposal.
Encrypt Alg	This list allows you to specify encryption with DES or Triple DES options.
• DES	• This option provides minimal security with 56-bit data encryption standard, which uses less processing time than does Triple-DES.
• Triple-DES	• This option allows for maximum security with 168-bit data encryption standard, which uses more processing time than does DES. **Note** Triple DES is only supported within the U.S. domestic versions of both the Cisco IOS software and the VPN Client.
Hash Alg	This list allows you to specify authentication with MD5 or SHA-1 options.
• MD5	• This option provides minimal authentication with 128-bit digest, which uses less processing time than does SHA. **Note** Cisco IOS software does not currently support the DES-MAC Hash Algorithm option.
• SHA-1	• This option allows for maximum authentication with 160-bit digest, which uses more processing time than does MD5.
Encapsulation	This list allows you to specify encapsulation method with Tunnel or Transport options.

Table 6-10 Authentication (Phase 2)—Proposal 1 Pane Field Descriptions (continued)

Field	Description
• Tunnel	• This option is the only method of secure encapsulation available for the Cisco Secure VPN Client.
• Transport	• This option allows non-IPSec protected encapsulation (when both peers are not using IPSec.) Otherwise, you *must* use the Tunnel option for maximum security.

To save your policy

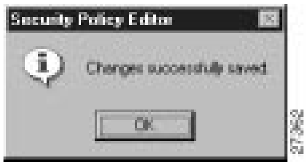
Step 1 On the **File** menu, click **Save Changes** to save the policy.

The Security Policy Editor dialog box appears. Before your policy is implemented, you must save your policy settings.

Step 2 Click **OK**.

Figure 6-16 shows how this is displayed in the Security Policy Editor dialog box.

Figure 6-16 Security Policy Editor



Changes successfully saved.

Task 2—Configuring Digital Certification on the Gateway

To configure digital certification on the gateway, perform the following steps:

- Configuring the Gateway
- Configuring ISAKMP
- Configuring IPSec
- Defining a Dynamic Crypto Map
- Declaring the CA
- Specifying a Public and Private Key

Configuring the Gateway

To configure the gateway, perform the following tasks, as described in Table 6-11:

- Configure the Gateway
- Define a Host Name
- Define a Name Server

Table 6-11 Configuring the Gateway

Command	Purpose
`router>` **`enable`**	To enter privileged EXEC mode, enter the **enable** user EXEC command.

`router#` **`configure terminal`**
`Enter configuration commands, one per line.`
`End with CNTL/Z.`
	To enter global configuration mode, enter the **configure** privileged EXEC command. To configure the terminal attached at console port, enter the **terminal** keyword.

`router(config)#` **`ip domain-name example.com`**	To define a default domain name that the Cisco IOS software uses to complete unqualified host names, use the **ip domain-name** global configuration command. An unqualified host name is a host name without a dotted-decimal domain name. In this example, *example.com* is defined as the default domain name.
`router(config)#` **`hostname hq_sanjose`**	To specify or modify the host name for the network server, enter the **hostname** global configuration command. The host name is used in prompts and default configuration filenames. In this example, *hq_sanjose* is defined as the host name. The *hq_sanjose* host name replaces the default *router* host name.

`hq_sanjose(config)#` **`ip name-server`**
`192.168.1.1`
	To specify the address of a name server to use for name and address resolution, enter the **ip name-server** global configuration command.
	In this example, the gateway is defined as the *IP name server*. The gateway's IP address is *192.168.1.1*.

Configuring ISAKMP

To configure ISAKMP on the gateway, perform the following tasks, as described in Table 6-12:

- Configure ISAKMP Policy
- Configure IKE RSA Signatures

Table 6-12 Configuring ISAKMP

Command	Purpose
`hq_sanjose(config)# crypto isakmp policy 3`	To define an IKE policy, use the **crypto isakmp policy** global configuration command. This command invokes the ISAKMP policy configuration (config-isakmp) command mode. IKE policies define a set of parameters to be used during the IKE negotiation. In this example, the ISAKMP policy is assigned a priority of *3*.
`hq_sanjose(config-isakmp)# encryption des`	To specify the encryption algorithm, use the **encryption (IKE policy)** ISAKMP policy configuration command. The options for encryption are the **des** and **3des** keywords. DES is configured by default for minimum security and fastest processing.
`hq_sanjose(config-isakmp)# hash sha`	To specify the hash algorithm, use the **hash (IKE policy)** ISAKMP policy configuration command. IKE policies define a set of parameters to be used during IKE negotiation. The options for hashing are **sha** and **md5** keywords. SHA is configured by default for maximum authentication with slower processing than MD5.
`hq_sanjose(config-isakmp)# authentication rsa-sig`	To specify the authentication method, use the **authentication (IKE policy**) ISAKMP policy configuration command. The options for authentication method are **rsa-sig**, **rsa-encr**, and **pre-share** keywords. To specify digital certificates as the authentication method, enter the **rsa-sig** keyword.
`hq_sanjose(config-isakmp)# exit`	To exit ISAKMP policy configuration (config-isakmp) command mode, enter the **exit** crypto transform configuration command.

Configuring IPSec

To configure IPSec on the gateway, perform the following tasks, as described in Table 6-13:

- Configure IPSec Transform Set
- Configure IPSec Encapsulation

Table 6-13 Configuring IPSec

Command	Purpose
`hq_sanjose(config)#` **`crypto ipsec transform-set vpn-transform esp-des esp-md5-hmac`**	To define a combination of security associations to occur during IPSec negotiations, enter the **crypto ipsec transform-set** global configuration command. This command invokes the crypto transform (cfg-crypto-trans) configuration mode. In this example, the transform set named *vpn-transform* is defined with two security algorithm keywords: **esp-des** and **esp-md5-hmac**. **Note** There are complex rules defining which entries you can use for the transform arguments. These rules are explained in the command description for the **crypto ipsec transform-set** command. You can also use the **crypto ipsec transform-set** global configuration command to view the available transform arguments.
`hq_sanjose(cfg-crypto-trans)#` **`mode tunnel`**	(Optional) To specify encapsulation between the gateway and the VPN Client, enter the **mode** crypto transform configuration command. The **mode** command is only applicable to traffic whose source and destination addresses are the IPSec peer addresses; it is ignored for all other traffic. (All other traffic is in tunnel mode only.) The options for encapsulation are **tunnel** and **transport** keywords. Tunnel is configured by default for IPSec encapsulation.
`hq_sanjose(cfg-crypto-trans)#` **`exit`**	To exit crypto transform (cfg-crypto-trans) configuration mode, enter the **exit** crypto transform configuration command.

Defining a Dynamic Crypto Map

To define a dynamic crypto map, perform the following tasks, as described in Table 6-14:

- Define a Dynamic Crypto Map Entry
- Add a Dynamic Crypto Map to the Static Crypto Map
- Apply the Crypto Map to the Gateway Interface

Table 6-14 Defining a Dynamic Crypto Map

Command	Purpose
`hq_sanjose(config)# crypto dynamic-map vpn-dynamic 1`	To define a dynamic crypto map entry, enter the **crypto dynamic-map** command. This command invokes the crypto map (config-crypto-map) configuration mode. In this example, the dynamic map name is *vpn-dynamic*, and the sequence number (or priority) is *1*.
`hq_sanjose(config-crypto-map)# set transform-set vpn-transform`	To specify which transform sets are allowed for the crypto map entry, enter the **set transform-set** crypto map configuration command. In this example, the transform set previously defined in Configuring IPSec, *vpn-transform* is applied to the *vpn-dynamic* dynamic crypto map. **Note** You can list multiple transform sets in order of priority (highest priority first).
`hq_sanjose(config-crypto-map)# set security-association lifetime seconds 2700`	(Optional) If you want the security associations for this crypto map to be negotiated using shorter IPSec SA lifetimes than the globally specified lifetimes, specify a key lifetime for the crypto map entry. Specify the IPSec lifetimes using one of the following keywords: **seconds** or **kilobytes**. In this example, the SA lifetime is *2700* seconds.
`hq_sanjose(config-crypto-map)# exit`	To exit crypto map (config-crypto-map) configuration mode, enter the **exit** crypto map configuration command.

Table 6-14 Defining a Dynamic Crypto Map (continued)

Command	Purpose
`hq_sanjose(config)#` **`crypto map vpnclient 1 ipsec-isakmp vpn-dynamic`**	To add a dynamic crypto map set to a static crypto map set, use the **crypto map** global configuration command. The crypto map entry references the dynamic crypto map sets. Set the crypto map entries referencing dynamic maps to be the lowest priority entries in a crypto map set (that is, have the highest sequence numbers). In this example, the dynamic map *vpn-dynamic* is added to the crypto map *vpnclient*. The **ipsec-isakmp** keyword indicates IPSec and IKE negotiations are being configured. The crypto map *vpnclient* references the dynamic map *vpn-dynamic* and has a priority of *1* because this is the only crypto map used for this security policy. Otherwise, a higher priority number would have been assigned to this crypto map.
`hq_sanjose(config)#` **`interface ethernet0/0`**	To configure an interface, enter the **interface** global configuration command. This command invokes the interface (config-if) configuration mode.
`hq_sanjose(config-if)#` **`ip address 10.1.1.1 255.255.255.0`**	To indicate an IP address to the interface, enter the **ip address** interface configuration command. In this example, *10.1.1.1* is specified as the IP address of the Ethernet 0/0 interface.
`hq_sanjose(config-if)#` **`crypto map vpnclient`**	To apply a previously defined crypto map set to an interface, enter the **crypto map** interface configuration command. In this example, crypto map *vpnclient* is applied to outbound packets from Ethernet interface 0/0.
`hq_sanjose(config-if)#` **`exit`**	To exit interface (config-if) configuration mode, enter the **exit** interface configuration command.

Declaring the CA

To enroll your certificate with a CA, perform the following tasks, as described in Table 6-15:

- Specify the CA
- Specify Compatibility with CA's RA
- Specify CA's Enrollment URL
- Specify LDAP Support
- Specify CRL Option

Table 6-15 Declare the CA

Command	Purpose
`hq_sanjose(config)#` **`crypto ca identity example.com`**	To declare the CA your router should use, enter the **crypto ca identity** global configuration command. This command invokes the ca-identity (cfg-ca-id) configuration mode. In this example, *example.com* is defined as the domain name for which this certificate is requested.
`hq_sanjose(cfg-ca-id)#` **`enrollment mode ra`**	To indicate compatibility with the CA's Registration Authority (RA) system, enter the **enrollment mode ra** ca-identity configuration command.
`hq_sanjose(cfg-ca-id)#` **`enrollment url http://ca-server`**	To specify the CA's location where your router should send certificate requests by indicating the CA's enrollment URL, enter the **enrollment url** ca-identity configuration command. In this example, *http://ca-server* is specified as the CA server.
`hq_sanjose(cfg-ca-id)#` **`query url http://ca-server`**	To specify Lightweight Directory Access Protocol (LDAP) support, enter the **query url** ca-identity configuration command. This command is required if your CA supports both RA and LDAP. LDAP is a query protocol used when the router retrieves certificates and CRLs. The default query protocol is Certificate Enrollment Protocol (CEP). In this example, *http://ca-server* is specified as the LDAP server.
`hq_sanjose(cfg-ca-id)#` **`crl optional`**	To allow other peers' certificates to still be accepted by your router even if the appropriate Certificate Revocation List (CRL) is not accessible to your router, use the **crl optional** ca-identity configuration command.
`hq_sanjose(cfg-ca-id)#` **`exit`**	To exit ca-identity (cfg-ca-id) configuration mode, enter the **exit** ca-identity configuration command.

Specifying a Public and Private Key

To specify a public and private key, perform the following tasks, as described in Table 6-16:

- Generate the Public and Private Key on the Gateway
- Receive the CA Public Key and CA Server Certificate
- Send the Gateway Public Key
- Receive the Signed Gateway Certificate
- Enroll the Gateway Certificate with the CA

Table 6-16 Specify a Public and Private Key

Command	Purpose

`hq_sanjose(config)#` **`crypto key generate rsa usage-keys`**
`mod 512 [signature key]`
`mod 512 [encryption key]`
	To generate the public and the private keys, enter the **crypto key generate rsa** global configuration command. This command creates two key-pairs for RSA:
	• One key-pair for digital signatures
	• One key-pair for encryption
	A key-pair refers to a public key and its corresponding secret key. If you do not specify the **usage-keys** keyword at the end of the command, the router will generate only one RSA key-pair and use it for both digital signatures and encryption.

`hq_sanjose(config)#` **`crypto ca authenticate example.com`**
`Certificate has the following attributes:`
`Fingerprint: 103FXXXX 9D64XXXX 0AE7XXXX 626AXXXX`
`% Do you accept this certificate? [yes/no]:`**`yes`**
	To receive the public key and CA server certificate and authenticate the CA (by receiving the CA's certificate), use the **crypto ca authenticate** global configuration command.
	In this example, *example.com* is defined as the domain name for which this certificate is authenticated.
	At this point the router has a copy of the CA's certificate.
	In this example, *yes* is entered to accept the certificate.

Table 6-16 Specify a Public and Private Key (continued)

Command	Purpose
hq_sanjose(config)# **crypto ca enroll example.com** Start certificate enrollment .. Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a proper note of it. Password:**cisco1234** Re-enter password:**cisco1234**	To send the gateway's public key and receive a signed certificate from the CA server, enter the **crypto ca enroll** global configuration command. In this example, *example.com* is defined as the domain name for which this certificate is received. **Note** This is message text. This text might contain information about what to enter after it prompts you.
% The subject name in the certificate will be: **hq_sanjose.example.com** % Include the router serial number in the subject name? [yes/no]: **yes** % The serial number in the certificate will be: 0431XXXX % Include an IP address in the subject name? [yes/no]: **yes** Interface: **ethernet0/0** Request certificate from CA? [yes/no]: **yes** % Certificate request sent to Certificate Authority % The certificate request fingerprint will be displayed. % The 'show crypto ca certificate' command will also show the fingerprint. Fingerprint: C767XXXX 4721XXXX 0D1EXXXX C27EXXXX	At this point, the enrollment request is sent to the CA and is pending for the CA administrator's approval. The router will be polling every 2 minutes for the availability of the certificate. In this example, *cisco1234* is entered as the challenge password. Should you choose to revoke your certificate, the CA must be provided with this challenge password. In this example, *hq_sanjose.example.com* is entered as the name server and domain name to which this digital certificate applies. In this example, *yes* is entered to indicate the router serial number is to be included in the subject name. The serial number is not used by IPSec or IKE but may be used by the CA to either authenticate certificates or to later associate a certificate with a particular router In this example, *yes* is entered to indicate the IP address is to be included in the subject name. Normally, you would not include the IP address because the IP address binds the certificate more tightly to a specific entity. Also, if the router is moved, you would need to issue a new certificate. Finally, a router has multiple IP addresses, any of which might be used with IPSec. In this example, the *ethernet 0/0* interface for the IP address specified is entered. This interface should correspond to the interface to which you apply your crypto map set. In this example, *yes* is entered to request the certificate. Wait until the router has retrieved the certificate. The router will display a message informing you that the certificate has been loaded.

Related Documentation

For more information on digital certification, refer to the “Digital Certification” section in Chapter 2, “Case Study for Layer 3 Authentication and Encryption.”

For more information on configuring Cisco IOS software commands, refer to the “Cisco IOS Software Documentation Set” section in the “Preface.”

For more information SCEP, refer to the following URL:

http://www.cisco.com/warp/public/cc/cisco/mkt/security/tech/scep_wp.htm