

# Configuring a Pre-Shared Key or Wildcard Pre-Shared Key

This chapter describes how a Cisco Secure VPN Client (VPN Client) interoperates with a Cisco gateway using a pre-shared key or wildcard pre-shared key for Internet Key Exchange (IKE) authentication. With a pre-shared key, you can allow for one or more clients to use individual shared secret keys to authenticate encrypted tunnels to a gateway. With a wildcard pre-shared key, you can allow for one or more clients to use a shared secret key to authenticate encrypted tunnels to a gateway.

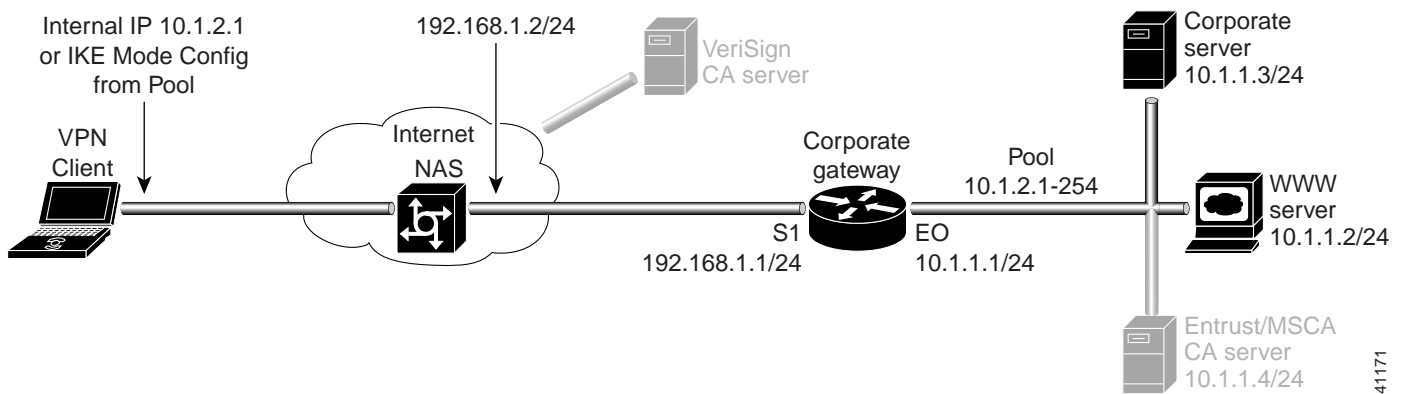
- Task 1—Configuring a Pre-Shared Key or Wildcard Pre-Shared Key on the VPN Client
- Task 2—Configuring a Pre-Shared Key or Wildcard Pre-Shared Key on the Gateway
- Related Documentation



**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 5-1 Pre-Shared Key Topology*



## Task 1—Configuring a Pre-Shared Key or Wildcard Pre-Shared Key on the VPN Client

- Configuring a New Gateway for Security Policy
- Specifying a VPN Client's Identity
- Configuring Authentication on the VPN Client

### Configuring a New Gateway for Security Policy

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

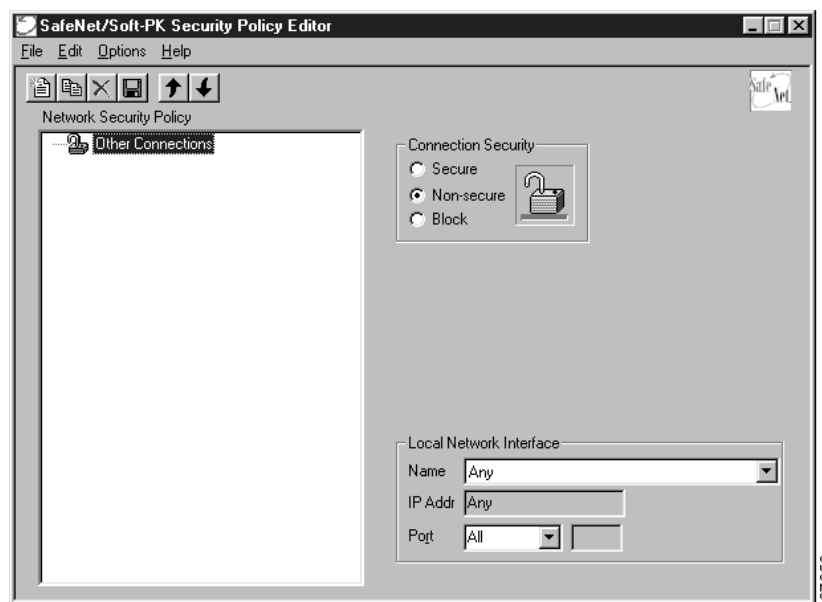
- Open the Security Policy Editor
- Configure Other Connections
- Create a New Connection
- Define the New Connection

To open the Security Policy Editor

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

The SafeNet/Soft-PK Security Policy Editor window appears, as shown in Figure 5-2. Table 5-1 describes the field descriptions for the SafeNet/Soft-PK Security Policy Editor.

*Figure 5-2 SafeNet/Soft-PK Security Policy Editor*



**Table 5-1 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.
Connection Security	Under Connection Security, you can define IP access for this connection using Secure, Non-secure, and Block options. <ul style="list-style-type: none"> <li>• Secure</li> <li>• Non-secure</li> <li>• Block</li> </ul>

**To configure other connections**

- 
- Step 1** On 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 5-2 shows how this is displayed on the Other Connections pane. Table 5-2 describes the field descriptions for the Other Connections pane.

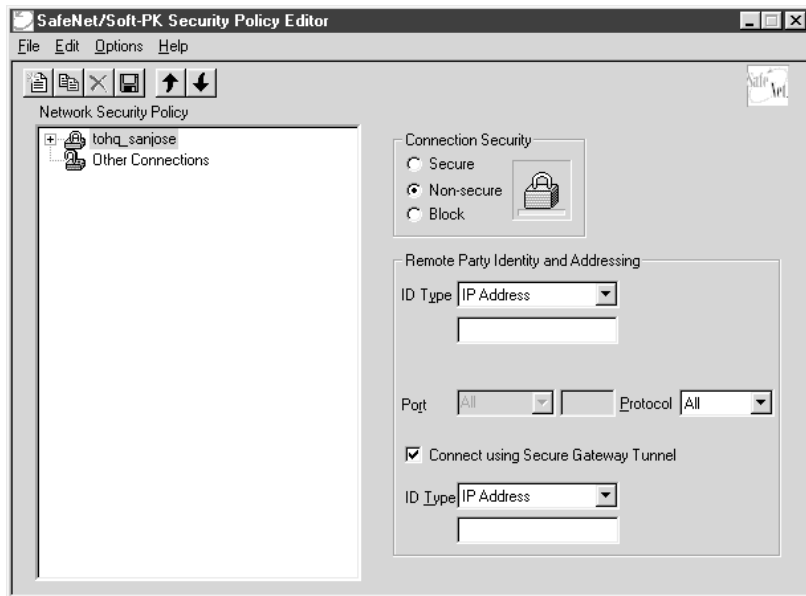


**Note** If you do not specify the Non-Secure option for the Other Connections pane, you *will not* be able to modify the Internet Interface or Local Network Interface to add the pre-shared key.

**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 5-3. Table 5-2 describes the field descriptions for the New Connection pane.
-

Figure 5-3 Renaming a New Connection




---

#### 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.
- Step 2** In the right pane, click the **Secure** option.
- Step 3** Either define the connection using a pre-shared key or wildcard pre-shared key.
- 

#### To define the connection for the VPN Client with a pre-shared key

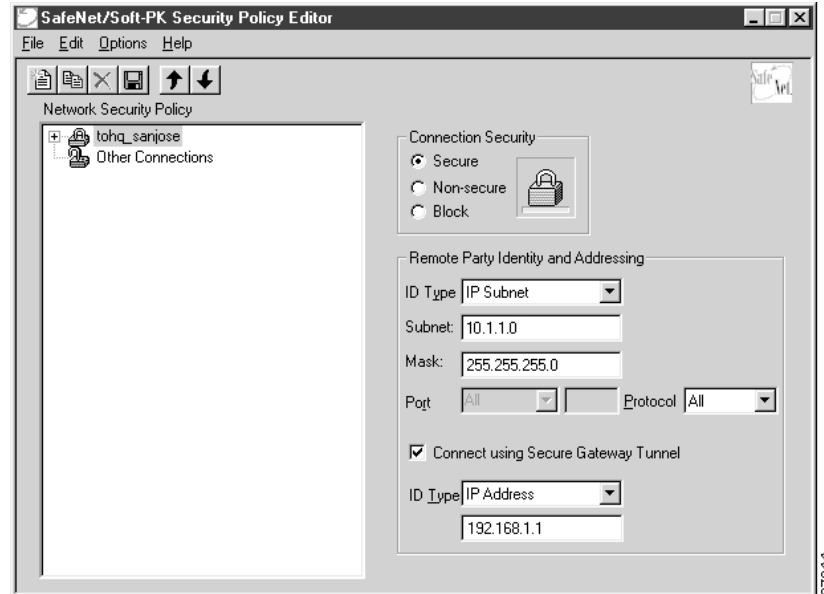
In the right pane, under Remote Party IP Addressing, enter the following parameters:

- Step 1** In the ID Type list, click **IP Subnet**.
- Step 2** In the Subnet box, enter your corporate subnet. In this example, the IP address of the corporate subnet, **10.1.1.0** is entered.
- Step 3** In the Mask box, 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.
- Step 4** The Port list and box are inactive as a default. In the Protocol list, click **All**.
- Step 5** Select the **Connect using Secure Gateway Tunnel** check box.
- Step 6** In the ID\_Type list, click **IP Address**.
- Step 7** 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 5-4 shows how this is displayed on the New Connection pane for pre-shared key. Table 5-2 describes the field descriptions for the New Connection pane.

---

Figure 5-4 Defining a New Connection for Pre-Shared Key



To define the connection for the VPN Client for a wildcard pre-shared key

In the right pane, under Remote Party IP Addressing, enter the following parameters:

- Step 1 In the ID Type list, click **IP Address**.
- Step 2 In the IP address value box, enter the wildcard IP address, **0.0.0.0**.
- Step 3 The Port list and box are inactive as a default. In the Protocol list, click **All**. Leave all other fields as-is.

Figure 5-5 shows how this is displayed on the New Connection pane for wildcard pre-shared key. Table 5-2 describes the field descriptions for the New Connection pane.

Figure 5-5 Defining a New Connection for Wildcard Pre-Shared Key

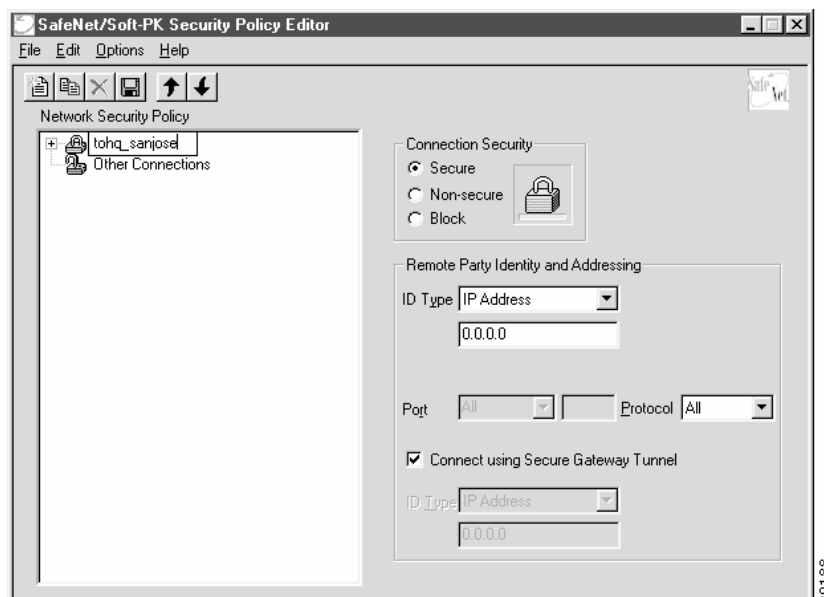


Table 5-2 New Connection Pane Field Descriptions

Field	Description
<p>Network Security Policy</p> <ul style="list-style-type: none"> <li>• New Connection</li> <li>• Other Connections</li> </ul>	<p>Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed.</p> <ul style="list-style-type: none"> <li>• This object is a set of security parameters that pertain to an individual remote IP connection. <i>New Connection</i> is the default connection name.</li> <li>• This object is a policy, or a default connection, and the first step in establishing security policies for individual connections.</li> </ul> <p>For all IP communications that do not adhere to the security policies defined in the individual connections, <i>Other Connections</i> acts as a default. <i>Other Connections</i> is always the last rule among security policies.</p>
<p>Connection Security</p> <ul style="list-style-type: none"> <li>• Secure</li> <li>• Non-secure</li> <li>• Block</li> </ul>	<p>Under Connection Security, you can define IP access for this connection using Secure, Non-secure, and Block options.</p> <ul style="list-style-type: none"> <li>• This option secures the IP communications for this connection.</li> <li>• This option allows for IP communications to occur without encryption, and you to change any settings under your Internet Interface or Local Network Interface.</li> <li>• This option denies all IP communications to the VPN Client.</li> </ul>
<p>Remote Party Identity and Addressing</p> <p>ID Type</p> <ul style="list-style-type: none"> <li>• IP Address <ul style="list-style-type: none"> <li>– IP address value</li> </ul> </li> <li>• Domain Name <ul style="list-style-type: none"> <li>– Domain name value</li> <li>– IP Address</li> </ul> </li> <li>• Email Address <ul style="list-style-type: none"> <li>– Email value</li> <li>– IP address value</li> </ul> </li> <li>• IP Subnet <ul style="list-style-type: none"> <li>– Subnet</li> <li>– Mask</li> </ul> </li> </ul>	<p>Under Remote Party Identity and Addressing, define the IPsec peer with which the VPN Client will establish a secure tunnel.</p> <p>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.</p> <p>Depending on the option you choose, different values will appear in the right pane.</p> <ul style="list-style-type: none"> <li>• This option allows a static IP address to be configured on the VPN Client. This is the default option. <ul style="list-style-type: none"> <li>– In this box, specify the IP address value.</li> </ul> </li> <li>• This option enables the domain name value box and the IP Address box. <ul style="list-style-type: none"> <li>– In this box, specify the domain name value.</li> <li>– In this box, specify the IP address of the domain, the organizational IP address.</li> </ul> </li> <li>• This option allows you to indicate the email address of the peer. <ul style="list-style-type: none"> <li>– In this box, specify the e-mail value.</li> <li>– In this box, specify the peer's IP address.</li> </ul> </li> <li>• This option allows you to specify the IP subnet the client will be allowed to access using this peer. <ul style="list-style-type: none"> <li>– In this box, specify the subnet IP address.</li> <li>– In this box, specify the mask IP address.</li> </ul> </li> </ul>

*Table 5-2 New Connection Pane Field Descriptions (continued)*

Field	Description
<ul style="list-style-type: none"> <li>• IP Address Range               <ul style="list-style-type: none"> <li>– From</li> <li>– To</li> </ul> </li> <li>• Distinguished Name               <ul style="list-style-type: none"> <li>– Edit Name</li> <li>– IP Address</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• This option allows you to indicate the range of IP addresses to which this client will have access.               <ul style="list-style-type: none"> <li>– In this box, specify the beginning IP address.</li> <li>– In this box, specify the ending IP address.</li> </ul> </li> <li>• This option allows you to specify the name, department, state, and country of the peer identity.               <ul style="list-style-type: none"> <li>– When clicked, this button allows you to specify distinguished name settings.</li> <li>– In this box, specify the peer’s IP address.</li> </ul> </li> </ul>
Port	This list shows the IPSec peer’s protocol ports. A default of <i>All</i> 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.
ID_Type	<p>This list shows the identification type of the gateway including IP address, domain name, and distinguished name.</p> <p>Depending on the option you choose, different values will appear in the right pane.</p>
<ul style="list-style-type: none"> <li>• IP Address               <ul style="list-style-type: none"> <li>– IP address value</li> </ul> </li> <li>• Domain Name               <ul style="list-style-type: none"> <li>– Domain name value</li> <li>– IP Address</li> </ul> </li> <li>• Distinguished Name               <ul style="list-style-type: none"> <li>– Edit Name</li> <li>– IP Address</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• This option enables the IP address value box. This is the default option.               <ul style="list-style-type: none"> <li>– In this box, specify the IP address value.</li> </ul> </li> <li>• This option enables the domain name value box and the IP Address box.               <ul style="list-style-type: none"> <li>– In this box, specify the domain name value.</li> <li>– In this box, specify the IP Address of the domain.</li> </ul> </li> <li>• This option allows you to specify the name, department, state, and country of the gateway.               <ul style="list-style-type: none"> <li>– When clicked, this button allows you to specify the distinguished name settings.</li> <li>– In this box, specify the gateway’s IP address.</li> </ul> </li> </ul>

## Specifying a VPN Client’s Identity

To specify the VPN Client’s identity, perform the following tasks:

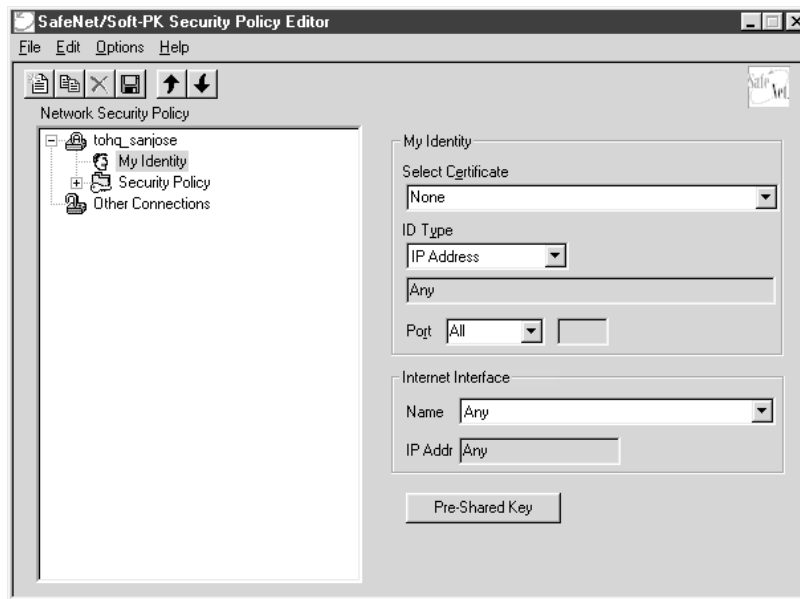
- Choose an Identity
- Enter the Pre-Shared Key

**To choose an identity**

- Step 1** In the left pane, double-click the new connection. In this example, **tohq\_sanjose** is double-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.
- Step 3** In the right pane, under My Identity, enter the following:
- In the ID\_Type list, click **IP Address**.
  - In the Port list, click **All**.
- Step 4** In the right pane, under Internet Interface (or Local Network Interface), enter the following:
- In the Name list, click **Any**. The IP Addr list is inactive as a default.
- Step 5** Click **Pre-Shared Key**.  
The Pre-Shared Key window appears.

Figure 5-6 shows how this is displayed on the My Identity pane for pre-shared key. Table 5-3 describes the field descriptions for the My Identity pane.

**Figure 5-6** My Identity Pane



**Table 5-3** My Identity 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.
<ul style="list-style-type: none"> <li>New Connection&gt;My Identity</li> </ul>	<ul style="list-style-type: none"> <li>This pane allows you to specify the identity of the VPN Client. This identity will allow the other peer to identify the device during the key exchange phase.</li> </ul>



Table 5-3 My Identity Pane Field Descriptions (continued)

Field	Description
My Identity	Under My Identity, specify options for determining the identity of the VPN Client. These options include Select Certificate, ID Type, and Port.
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, <i>None</i> is the default option.
ID_Type <ul style="list-style-type: none"> <li>IP Address</li> </ul>	This list indicates the IP address option for the VPN Client on the corporate subnet. <ul style="list-style-type: none"> <li>This field indicates that the VPN Client will be identified by the gateway using the VPN Client's statically or dynamically-assigned IP address.</li> </ul>
Port	This list shows the VPN Client's protocol ports. A default of <i>All</i> secures all protocol ports.
Local Network Interface: Version 1.0 <i>or</i> Internet Interface: Version 1.1	Under Local Network Interface or Internet Interface, specify the hardware interface on the PC or laptop through which the connection will be established. These options include Name and IP Addr options.
Name	This list indicates the names of the hardware interfaces on the PC or laptop. A default of <i>Any</i> enables all hardware interfaces.
IP Addr	This list indicates the IP addresses of the hardware interfaces on the PC or laptop. A default of <i>Any</i> enables all hardware interface IP addresses.
<ul style="list-style-type: none"> <li>Pre-Shared Key</li> </ul>	<ul style="list-style-type: none"> <li>This button enables the Pre-Shared Key dialog box.</li> </ul>

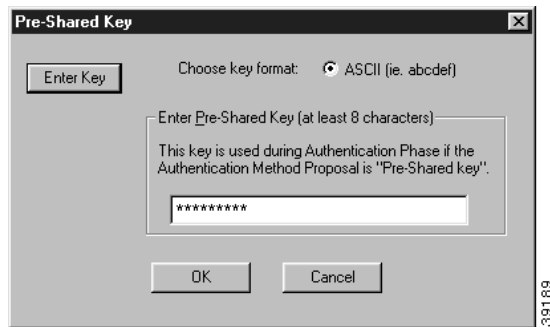
#### To enter the pre-shared key

- Step 1** In the Pre-Shared Key dialog box, under Enter Pre-Shared Key, enter the pre-shared keystring. The minimum keystring is 8 characters, and the maximum keystring is 128 characters. In this example, *cisco1234* is entered.
- To start the key exchange, both the VPN Client and the gateway must use the same public key.
- Step 2** Click **OK**.
- Figure 5-7 shows how this is displayed in the Pre-Shared Key dialog box.



**Note** In the Cisco Secure VPN Client Version 1.0, the pre-shared keystring is visible from the Pre-Shared Key dialog box. In Cisco Secure VPN Client Version 1.1, the pre-shared keystring is hidden.

Figure 5-7 Pre-Shared Key Dialog Box



## Configuring Authentication on the VPN Client

To configure authentication on the VPN Client for a pre-shared key or wildcard-preshared key, perform the following steps:

- 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, click **Main Mode**.

**Step 3** Select the **Enable Replay Detection** check box.

Figure 5-8 shows how this is displayed on the Security Policy pane. Table 5-4 describes the field descriptions for the Security Policy pane.

---

Figure 5-8 Security Policy Pane

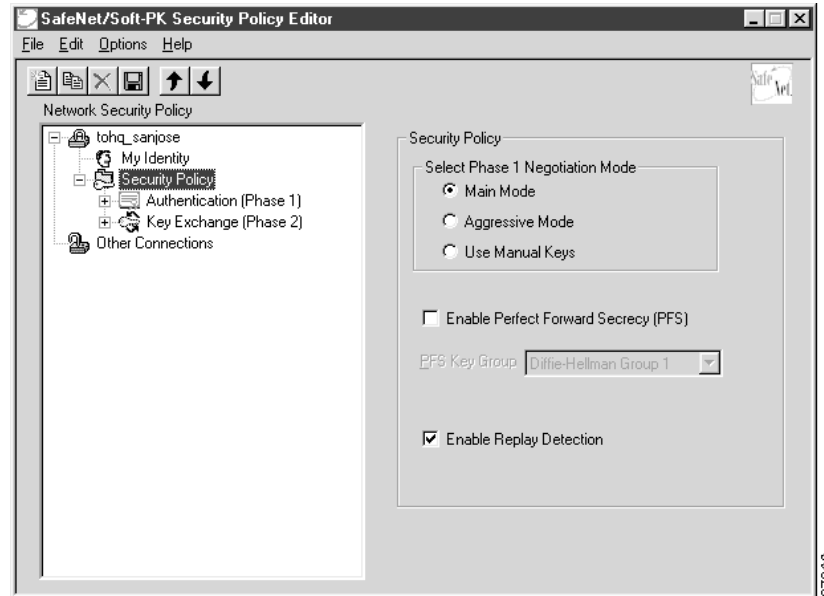


Table 5-4 Security Policy Pane Field Descriptions

Field	Description
Network Security Policy <ul style="list-style-type: none"> <li>New Connection&gt;Security Policy</li> </ul>	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed. <ul style="list-style-type: none"> <li>This pane allows you to specify authentication and data integrity.</li> </ul>
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 <ul style="list-style-type: none"> <li>Main Mode</li> <li>Aggressive Mode</li> <li>Use Manual Keys</li> </ul>	Under Select Phase 1 Negotiation Mode, select the mode for authenticating ISAKMP SAs using Main Mode, Aggressive Mode, or Use Manual Key options. <ul style="list-style-type: none"> <li>This option allows identities to not be revealed until all secure communications have been established, which requires a longer processing time.</li> <li>This option allows identities to viewed while secure communications are taking place, which makes for a faster processing time.</li> <li>This option is available for troubleshooting purposes only.</li> </ul>
Enable Perfect Forward Secrecy	When selected, this check box triggers an authentication method, which protects against repeat compromises of a shared secret key.
Enable Replay Detection	When selected, this check box sets a counter that 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*.

The Proposal 1 pane appears in the right pane.

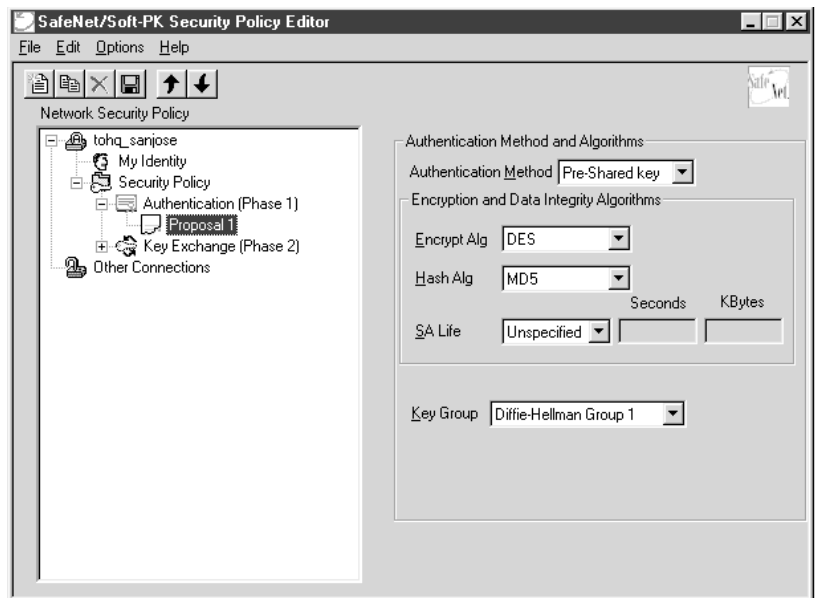
In the right pane, under Authentication Method and Algorithms, in the Authentication Method list, **Pre-Shared key** appears. Because you have already specified a pre-shared key, you cannot make a selection here.

**Step 2** 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 5-9 shows how this is displayed on the Authentication (Phase 1)—Proposal 1 pane for pre-shared key. Table 5-5 describes the field descriptions for the Authentication (Phase 1)—Proposal 1 pane for pre-shared key.

**Figure 5-9 Authentication (Phase 1)—Proposal 1 Pane**



*Table 5-5 Authentication (Phase 1)—Proposal 1 Pane Field Descriptions*





Field	Description
Network Security Policy <ul style="list-style-type: none"> <li>New Connection&gt;Security Policy&gt;Authentication (Phase 1)&gt;Proposal 1</li> </ul>	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed. <ul style="list-style-type: none"> <li>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.</li> </ul>
Authentication Method and Algorithms	Under Authentication Method and Algorithms, define the authentication method used and authentication and encryption algorithms.
Authentication Method <ul style="list-style-type: none"> <li>Pre-Shared Key</li> <li>RSA Signatures</li> </ul>	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. <ul style="list-style-type: none"> <li>This option appears if the method of authentication selected under My Identity is pre-shared key.</li> <li>This option appears if the method of authentication selected under My Identity is digital certification.</li> </ul>
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 <ul style="list-style-type: none"> <li>DES</li> <li>Triple-DES</li> </ul>	This list allows you to specify encryption with DES or Triple DES options. <ul style="list-style-type: none"> <li>This option provides minimal security with 56-bit data encryption standard, which uses less processing time than does Triple-DES.</li> <li>This option allows for maximum security with 168-bit data encryption standard, which uses more processing time than does DES.</li> </ul>
	 <p><b>Note</b> Triple DES is only supported within the U.S. domestic versions of both the Cisco IOS software and the VPN Client.</p>

Table 5-5 Authentication (Phase 1)—Proposal 1 Pane Field Descriptions (continued)

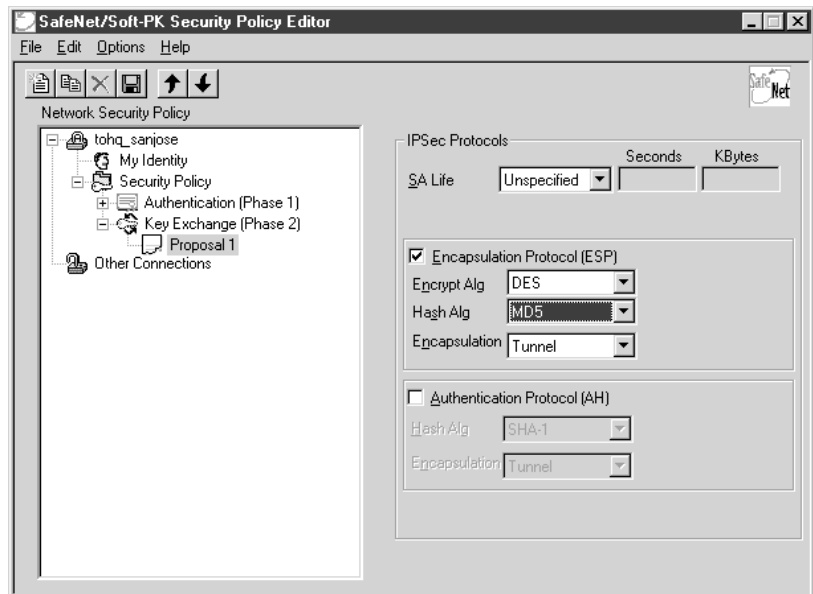
Field	Description
Hash Alg <ul style="list-style-type: none"> <li>• MD5</li> <li>• SHA-1</li> </ul>	This list allows you to specify authentication with MD5 and SHA-1 options. <ul style="list-style-type: none"> <li>• This option provides minimal authentication with 128-bit digest, which uses less processing time than does SHA.</li> <li>• This option allows for maximum authentication with 160-bit digest, which uses more processing time than does MD5.</li> </ul>  <hr/> <b>Note</b> Cisco IOS software does not currently support the DES-MAC Hash Algorithm option.
SA Life <ul style="list-style-type: none"> <li>• Unspecified</li> <li>• Seconds</li> <li>• Kbytes</li> <li>• Both</li> </ul>	(Optional) This list allows you to specify the period for which the IKE SA is valid using Unspecified, Seconds, Kbytes, or Both options.  <hr/> <b>Note</b> 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. <ul style="list-style-type: none"> <li>• This option allows the other IPSec peer to indicate when IKE SA expires.</li> <li>• This option allows you to specify SA life in seconds.</li> <li>• This option allows you to specify SA life in kilobytes.</li> <li>• This option allows you to specify both seconds and kilobytes, whichever comes first, before an SA life expires.</li> </ul>
Key Group <ul style="list-style-type: none"> <li>• Diffie-Hellman Group 1</li> <li>• Diffie-Hellman Group 2</li> </ul>	This list allows you to specify the Diffie-Hellman key exchange using Diffie-Hellman Group 1 or Diffie-Hellman Group 2 options.  <hr/> <b>Note</b> Cisco IOS software does not currently support Diffie-Hellman Group 5. <ul style="list-style-type: none"> <li>• This option enables 768-bit encryption, which requires less processing time than does Diffie-Hellman Group 2.</li> <li>• This option enables 1024-bit encryption, which is more secure than Diffie-Hellman Group 1.</li> </ul>

## 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:
- In the **SA Life** list, click **Unspecified**.
  - Select the **Encapsulation Protocol (ESP)** check box.
  - In the Encrypt Alg list, click **DES**.
  - In the Hash Alg list, click **MD5**.
  - In the Encapsulation list, click **Tunnel**.

Figure 5-10 shows how this is displayed on the Authentication (Phase 2)—Proposal 1 pane for pre-shared key. Table 5-6 describes the field descriptions for the Authentication (Phase 2)—Proposal 1 pane for pre-shared key.




**Figure 5-10 Authentication (Phase 2)—Proposal 1 Pane**



**Table 5-6 Authentication (Phase 2)—Proposal 1 Pane Field Descriptions**

Field	Description
Network Security Policy <ul style="list-style-type: none"> <li>New Connection&gt;Security Policy&gt;Key Exchange (Phase 2)&gt;Proposal 1</li> </ul>	Under Network Security Policy, the proposals that will be used to negotiate the authentication and encryption methods are displayed. <ul style="list-style-type: none"> <li>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.</li> </ul>

Table 5-6 Authentication (Phase 2)—Proposal 1 Pane Field Descriptions (continued)

Field	Description
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.
SA Life	<p>This list allows you to specify the period for which the IKE SA is valid using Unspecified, Seconds, Kbytes, or Both options.</p> <p> <b>Note</b> 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.</p> <ul style="list-style-type: none"> <li>• Unspecified</li> <li>• Seconds</li> <li>• Kbytes</li> <li>• Both</li> </ul> <ul style="list-style-type: none"> <li>• This option allows the other IPSec peer to indicate when IKE SA expires.</li> <li>• This option allows you to specify SA life in seconds.</li> <li>• This option allows you to specify SA life in kilobytes.</li> <li>• This option allows you to specify both seconds and kilobytes, whichever comes first, before an SA life expires.</li> </ul>
Encapsulation Protocol	If selected, this check box indicates that encryption and authentication will be selected for this proposal.
Encrypt Alg	<p>This list allows you to specify encryption with DES or Triple DES options.</p> <ul style="list-style-type: none"> <li>• DES</li> <li>• Triple-DES</li> </ul> <ul style="list-style-type: none"> <li>• This option provides minimal security with 56-bit data encryption standard, which uses less processing time than does Triple-DES.</li> <li>• This option allows for maximum security with 168-bit data encryption standard, which uses more processing time than does DES.</li> </ul> <p> <b>Note</b> Triple DES is only supported within the U.S. domestic versions of both the Cisco IOS software and the VPN Client.</p>
Hash Alg	<p>This list allows you to specify authentication with MD5 or SHA-1 options.</p> <ul style="list-style-type: none"> <li>• MD5</li> </ul> <ul style="list-style-type: none"> <li>• This option provides minimal authentication with 128-bit digest, which uses less processing time than does SHA.</li> </ul> <p> <b>Note</b> Cisco IOS software does not currently support the DES-MAC Hash Algorithm option.</p> <ul style="list-style-type: none"> <li>• SHA-1</li> <li>• This option allows for maximum authentication with 160-bit digest, which uses more processing time than does MD5.</li> </ul>



*Table 5-6 Authentication (Phase 2)—Proposal 1 Pane Field Descriptions (continued)*

Field	Description
Encapsulation	This list allows you to specify encapsulation method with Tunnel or Transport options.
<ul style="list-style-type: none"> <li>• Tunnel</li> <li>• Transport</li> </ul>	<ul style="list-style-type: none"> <li>• This option is the only method of secure encapsulation available for the Cisco Secure VPN Client.</li> <li>• This option allows non-IPSec protected encapsulation (when both peers are not using IPSec.) Otherwise, you <i>must</i> use the Tunnel option for maximum security.</li> </ul>

**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 5-11 shows how this is displayed in the Security Policy Editor dialog box.

*Figure 5-11 Security Policy Editor*

## Task 2—Configuring a Pre-Shared Key or Wildcard Pre-Shared Key on the Gateway

To configure a pre-shared key or wildcard pre-shared key on the gateway, perform the following steps:

- Configuring the Gateway
- Configuring ISAKMP
- Configuring IPSec
- Defining a Dynamic Crypto Map
- Defining a Static Crypto Map

## Configuring the Gateway

To configure the gateway, perform the following tasks, as described in Table 5-7:

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

**Table 5-7** Configuring the Gateway

Command	Purpose
router> <b>enable</b>	To enter privileged EXEC mode, enter the <b>enable</b> user EXEC command.
router# <b>configure terminal</b> Enter configuration commands, one per line. End with CNTL/Z.	To enter global configuration mode, enter the <b>configure</b> privileged EXEC command. To configure the terminal attached at console port, enter the <b>terminal</b> keyword.
router(config)# <b>ip domain-name example.com</b>	To define a default domain name that the Cisco IOS software uses to complete unqualified host names, use the <b>ip domain-name</b> global configuration command. An unqualified host name is a host name without a dotted-decimal domain name.  In this example, <i>example.com</i> is defined as the default domain name.
router(config)# <b>hostname hq_sanjose</b>	To specify or modify the host name for the network server, enter the <b>hostname</b> global configuration command. The host name is used in prompts and default configuration filenames.  In this example, <i>hq_sanjose</i> is defined as the host name. The <i>hq_sanjose</i> host name replaces the default <i>router</i> host name.
hq_sanjose(config)# <b>ip name-server 192.168.1.1</b>	To specify the address of a name server to use for name and address resolution, enter the <b>ip name-server</b> global configuration command.  In this example, the gateway is defined as the <i>IP name server</i> . The gateway's IP address is <i>192.168.1.1</i> .

## Configuring ISAKMP

To configure ISAKMP on the gateway, perform the following tasks, as described in Table 5-8:

- Configure ISAKMP Policy
- Configure Pre-Shared Key

*Table 5-8 Configuring ISAKMP*

Command	Purpose
hq_sanjose(config)# <b>crypto isakmp policy 3</b>	To define an IKE policy, use the <b>crypto isakmp policy</b> 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)# <b>encryption des</b>	(Optional) To specify the encryption algorithm, use the <b>encryption (IKE policy)</b> ISAKMP policy configuration command.  The options for encryption are the <b>des</b> and <b>3des</b> keywords. DES is configured by default for minimum security and fastest processing.
hq_sanjose(config-isakmp)# <b>hash sha</b>	(Optional) To specify the hash algorithm, use the <b>hash (IKE policy)</b> ISAKMP policy configuration command. IKE policies define a set of parameters to be used during IKE negotiation.  The options for hashing are the <b>sha</b> and <b>md5</b> keywords. SHA is configured by default for maximum authentication with slower processing than MD5.
hq_sanjose(config-isakmp)# <b>authentication pre-share</b>	To specify the authentication method, use the <b>authentication (IKE policy)</b> ISAKMP policy configuration command.  The options for authentication method are the <b>rsa-sig</b> , <b>rsa-encr</b> , and <b>pre-share</b> keywords. To specify pre-shared key as the authentication method, enter the <b>pre-share</b> keyword.
hq_sanjose(config-isakmp)# <b>group 1</b>	(Optional) To specify the Diffie-Hellman group identifier, use the group ISAKMP policy configuration command.  The options for Diffie-Hellman group are the <b>1</b> and <b>2</b> keywords. Diffie-Hellman Group 1 is configured by default for minimum security with the fastest processing time.

Table 5-8 Configuring ISAKMP (continued)

Command	Purpose
hq_sanjose(config-isakmp)# <b>lifetime 86400</b>	<p>(Optional) To specify the lifetime of an IKE SA before it expires, use the <b>lifetime</b> ISAKMP policy configuration command.</p> <p>The lifetime can be using an integer from <i>60</i> to <i>86,400</i> seconds. A day (86,400 seconds) is configured by default.</p>
hq_sanjose(config-isakmp)# <b>exit</b>	To exit ISAKMP policy configuration (config-isakmp) command mode, enter the <b>exit</b> ISAKMP policy configuration command.
<pre>hq_sanjose(config)# <b>crypto isakmp key</b> <b>cisco1234 address 10.1.2.1</b> or hq_sanjose(config)# <b>crypto isakmp key</b> <b>cisco1234 address 0.0.0.0</b></pre>	<p>To configure a pre-shared authentication key, use the <b>crypto isakmp key</b> global configuration command. You must configure this key whenever you specify pre-shared key in an IKE policy. Use any combination of alphanumeric characters between 8 and 128 bytes. This pre-shared key must be identical at both peers.</p> <p>The VPN Client pre-shared key and IP address are specified as follows:</p> <ul style="list-style-type: none"> <li>If configuring pre-shared key, specify a separate pre-shared key and static IP address for each VPN Client. <p>In the first example, one VPN Client is configured with <i>cisco1234</i> as the pre-shared key and <i>10.1.2.1</i> as static IP address of the VPN Client. The <b>address</b> keyword indicates an IP address will be used for authentication.</p> </li> <li>If configuring wildcard pre-shared key, specify one pre-shared key for each group of VPN Clients at the same level of authorization. Then, specify the wildcard IP address, <i>0.0.0.0</i>, for dynamic IP addressing. The <b>address</b> keyword indicates an IP address will be used for authentication. <p>In the second example, one or more VPN Client(s) is/are configured with <i>cisco1234</i> as the pre-shared key and <i>0.0.0.0</i> as wildcard IP address of the VPN Client.</p> </li> </ul>

**Caution**


For security purposes, you *must* distribute the pre-shared key (pre-shared key or wildcard pre-shared key) to remote users through a secure out-of-band channel. For more details, see “Authentication and Encryption Features” in Chapter 2, “Case Study for Layer 3 Authentication and Encryption.”

## Configuring IPSec

To configure IPSec on the gateway, perform the following tasks, as described in Table 5-9:

- Configure IPSec Transform Set
- Configure IPSec Encapsulation

*Table 5-9 Configuring IPSec*

Command	Purpose
<pre>hq_sanjose(config)# crypto ipsec transform-set vpn-transform esp-des esp-md5-hmac</pre>	<p>To define a combination of security associations to occur during IPSec negotiations, enter the <b>crypto ipsec transform-set</b> global configuration command. This command invokes the crypto transform (cfg-crypto-trans) configuration mode.</p> <p>In this example, the transform set named <i>vpn-transform</i> is defined with two security algorithm keywords: <b>esp-des</b> and <b>ah-md5-hmac</b>. This is the recommended combination for minimum encryption and authentication.</p> <p> <b>Note</b> There are complex rules defining which entries you can use for the transform arguments. These rules are explained in the command description for the <b>crypto ipsec transform-set</b> command. You can also use the <b>crypto ipsec transform-set</b> global configuration command to view the available transform arguments.</p>
<pre>hq_sanjose(cfg-crypto-trans)# mode tunnel</pre>	<p>(Optional) To specify encapsulation between the gateway and the VPN Client, enter the <b>mode</b> crypto transform configuration command. The <b>mode</b> 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.)</p> <p>The options for encapsulation are <b>tunnel</b> and <b>transport</b> keywords. Tunnel is configured by default for IPSec encapsulation.</p>
<pre>hq_sanjose(cfg-crypto-trans)# exit</pre>	<p>To exit crypto transform (cfg-crypto-trans) configuration mode, enter the <b>exit</b> crypto transform configuration command.</p>

## Defining a Dynamic Crypto Map

To define a dynamic crypto map, perform the following tasks, as described in Table 5-10:

- Define a Dynamic Crypto Map Entry
- Add a Dynamic Crypto Map to the Static Crypto Map

*Table 5-10 Defining a Dynamic Crypto Map*

Command	Purpose
<pre>hq_sanjose(config)# crypto dynamic-map vpn-dynamic 1</pre>	<p>To define a dynamic crypto map entry, use the <b>crypto dynamic-map</b> command. This command invokes the crypto map (config-crypto-map) configuration mode.</p> <p>The dynamic map entry will reference the static crypto map entry.</p> <p>In this example, the dynamic map name is <i>vpn-dynamic</i>, and the sequence number (or priority) is <i>1</i>.</p>
<pre>hq_sanjose(config-crypto-map)# set transform-set vpn-transform</pre>	<p>To specify which transform sets are allowed for the crypto map entry, enter the <b>set transform-set</b> crypto map configuration command.</p> <p>In this example, the transform set previously defined in Configuring IPSec, <i>vpn-transform</i>, is applied to the <i>vpn-dynamic</i> dynamic crypto map.</p> <p> <b>Note</b> You can list multiple transform sets in order of priority (highest priority first).</p>
<pre>hq_sanjose(config-crypto-map)# set security-association lifetime seconds 2700</pre>	<p>(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: <b>seconds</b> or <b>kilobytes</b>.</p> <p>The crypto map's security associations are negotiated according to the global lifetimes.</p> <p>In this example, the SA lifetime is <i>2700</i> seconds.</p>
<pre>hq_sanjose(config-crypto-map)# exit</pre>	<p>To exit crypto map (config-crypto-map) configuration mode, enter the <b>exit</b> crypto map configuration command.</p>

## Defining a Static Crypto Map

To define a static crypto map, perform the following tasks, as described in Table 5-11:

- Define a Static Crypto Map Entry
- Add a Dynamic Crypto Map to a Static Crypto Map
- Define an Access List for the VPN Client
- Apply the Crypto Map to the Gateway Interface

*Table 5-11 Defining Static Crypto Map*

Command	Purpose
<pre>hq_sanjose(config)# crypto map vpnclient 1 ipsec-isakmp vpn-dynamic</pre>	<p>To define a static crypto map and add a dynamic crypto map set to a static crypto map set, enter the <b>crypto map</b> global configuration command.</p> <p>In this example, the <i>vpn-dynamic</i> dynamic map (child) is applied to the <i>vpnclient</i> static crypto map (parent).</p>
<pre>hq_sanjose(config)# access-list 101 permit ip 192.168.1.1 255.255.255.224 host 10.1.1.1</pre>	<p>(Optional) To permit all IP traffic between the host and the gateway when using static IP addressing on the VPN Client, use the extended version of the <b>access-list</b> global configuration command.</p> <p> <b>Note</b> An access-list must be configured for each VPN Client configured with static IP addresses on a corporate subnet.</p> <p>In this example, all IP traffic is permitted between the two IPsec peers.</p>
<pre>hq_sanjose(config)# interface ethernet0/0</pre>	<p>To configure an interface, enter the <b>interface</b> global configuration command. This command invokes the interface (config-if) configuration mode.</p>
<pre>hq_sanjose(config-if)# ip address 10.1.1.1 255.255.255.0</pre>	<p>To indicate an IP address to the interface, enter the <b>ip address</b> interface configuration command.</p> <p>In this example, <i>10.1.1.1</i> is specified as the IP address of the Ethernet 0/0 interface.</p>
<pre>hq_sanjose(config-if)# crypto map vpnclient</pre>	<p>To apply a previously defined crypto map set to an interface, enter the <b>crypto map</b> interface configuration command.</p> <p>In this example, crypto map <i>vpnclient</i> is applied to outbound packets from Ethernet interface 0/0.</p>

## Related Documentation

For more information on pre-shared key and wildcard pre-shared key, refer to the “Pre-Shared Keys” section or “Wildcard Pre-Shared Keys” 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.”