

Configuring Manual Configuration

This chapter describes how to manually configure internal corporate IP addresses on a Cisco Secure VPN Client (VPN Client). With manual configuration, you can assign a static, internal IP address to a client, making it easier to administer IP Security Protocol (IPSec) policy from the Cisco router (gateway) to the VPN Client. This chapter includes the following sections:

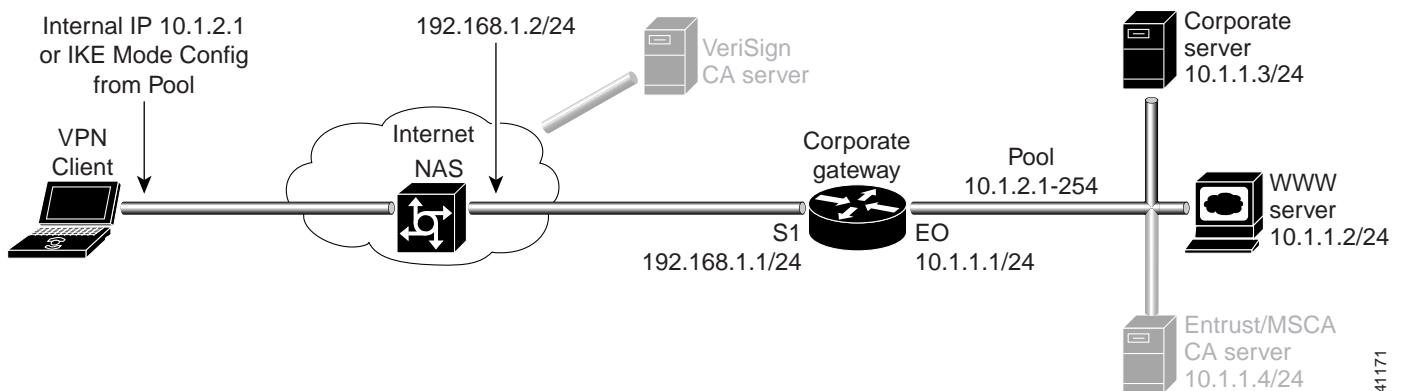
- Task 1—Configuring Manual Configuration on the VPN Client
- Task 2—Configuring Manual Configuration on the Gateway
- Related Documentation



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 3-1 Manual Configuration Topology



41171

Task 1—Configuring Manual Configuration on the VPN Client

To configure manual configuration between a VPN Client and a Cisco router, perform the following tasks:

- Specifying an Internal Network Address on the VPN Client
- Configuring New Gateway for Security Policy
- Specifying the VPN Client's Identity

Specifying an Internal Network Address on the VPN Client

To specify an internal network address on a VPN Client, perform the following tasks:

- Open the Security Policy Editor
- Open and Define Global Policy Settings

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 3-2. Table 3-2 describes the field descriptions for the SafeNet/Soft-PK Security Policy Editor.

Figure 3-2 SafeNet/Soft-PK Security Policy Editor



Table 3-1 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 <ul style="list-style-type: none"> • Secure • Non-secure • Block 	<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"> • This option secures the IP communications for this connection. • This option allows for IP communications to occur without encryption, and allows you to change any settings under your Internet Interface. This is the default. • This option denies all IP communications to the VPN Client.

To open and define Global Policy Settings

Step 1 On the **Options** menu, click **Global Policy Settings**.

The Global Policy Settings window appears, as shown in Figure 3-3. Table 3-2 describes the field descriptions for the Global Policy Settings window.

Step 2 Select the **Allow to Specify Internal Network Address** check box, and then click **OK**.

Figure 3-3 Global Policy Settings Window

Table 3-2 Global Policy Settings Window Field Descriptions

Field	Description
Global Policy Settings	Using this window, set preferences for all transmissions.
Retransmit Interval (seconds)	In this box, specify the amount of time your computer waits before it retransmits a protocol packet to which a device has not responded. The default interval is 15 seconds.
Number of retries	In this box, specify the number of times your computer retransmits a protocol packet before abandoning the exchange. The default is 3 retries.
Send status notifications to peer hosts	If selected, this check box sends messages that inform communicating parties whether their security proposals have been accepted or rejected, and the timeout periods.
Enable Non-IP Connections	If selected, this option allows your computer to transmit non-IP data without security. As a default, the VPN Client secures IP data and discards all non-IP data.
Allow to Specify Internal Network Address	If selected, this option allows you to enter the exact IP address under My Identity. An internal network address is the actual IP address for the VPN Client behind a network firewall. Use this option to specify that you want to indicate an internal network address. This allows you to enter the IP address in the Network Security Policy window under My Identity in the Internal Network IP Address box.

Configuring New Gateway for Security Policy

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

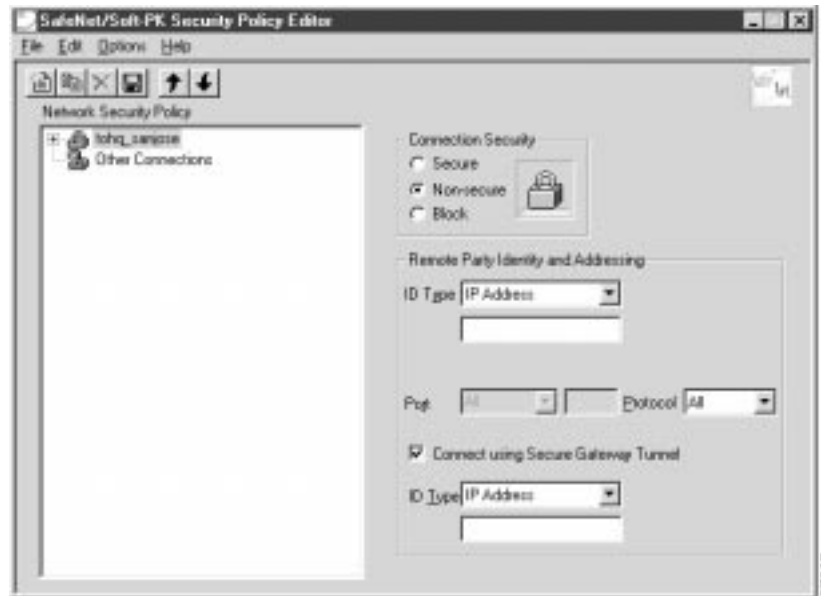
- Create a New Connection
- Define the New Connection

To create a new connection

-
- Step 1** In the left pane, click **Other Connections**.
- Step 2** On the **File** menu, click **New Connection**.
- Step 3** In the left pane, the default **New Connection** placeholder appears for the New Connection pane.
- Step 4** 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 3-4. Table 3-3 describes the field descriptions for the New Connection pane.

Figure 3-4 Renaming a New Connection Pane



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, under Connection Security, click **Secure**.
- Step 3** In the right pane, under Remote Party Identity and Addressing, enter the following:
- In the ID Type list, click **IP Subnet**.
 - In the Subnet box, enter the IP address of your corporate subnet. In this example, the IP address of the corporate subnet, **10.1.1.0** is entered.
 - 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.
 - The Port list and box are inactive as a default. In the Protocol list, click **All**.
 - Select the **Connect using Secure Gateway Tunnel** check box.
 - In the ID_Type list, click **IP Address**. 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 3-5 shows how this is displayed on the New Connection pane. Table 3-3 describes the field descriptions for the New Connection pane.

Figure 3-5 New Connection Pane



Table 3-3 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.
<ul style="list-style-type: none"> New Connection Other Connections 	<ul style="list-style-type: none"> 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. This object is the 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, <i>Other Connections</i> acts as a default. <i>Other Connections</i> is always the last rule among security policies.
Connection Security	Under Connection Security, you can define IP access for this connection.
<ul style="list-style-type: none"> Secure Non-secure Block 	<ul style="list-style-type: none"> This option secures the IP communications for this connection. This option allows for IP communications to occur without encryption, and you to change any settings under your Internet Interface. This is the default. 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 3-3 *New Connection Pane Field Descriptions (continued)*

Field	Description
<p>ID Type</p> <ul style="list-style-type: none"> • IP Address <ul style="list-style-type: none"> – IP address value • Domain Name <ul style="list-style-type: none"> – Domain name value – IP Address • Email Address <ul style="list-style-type: none"> – Email value – IP address value • IP Subnet <ul style="list-style-type: none"> – Subnet – Mask 	<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"> • 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"> – In this box, specify the IP address value. • This option enables the domain name value box and the IP Address box. <ul style="list-style-type: none"> – In this box, specify the domain name value. – In this box, specify the IP address of the domain, the organizational IP address. • This option allows you to indicate the email address of the peer. <ul style="list-style-type: none"> – In this box, specify the e-mail value. – In this box, specify the peer's IP address. • 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"> – In this box, specify the subnet IP address. – In this box, specify the mask IP address.
<ul style="list-style-type: none"> • IP Address Range <ul style="list-style-type: none"> – From – To • Distinguished Name <ul style="list-style-type: none"> – Edit Name – IP Address 	<ul style="list-style-type: none"> • This option allows you to indicate the range of IP addresses to which this client will have access. <ul style="list-style-type: none"> – In this box, specify the beginning IP address. – In this box, specify the ending IP address. • This option allows you to specify the name, department, state, and country of the peer identity. <ul style="list-style-type: none"> – Using this button, specify the distinguished name settings. – In this box, specify the peer's IP address.
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.

Table 3-3 *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. Depending on the option you choose, different values will appear in the right pane.
<ul style="list-style-type: none"> • IP Address <ul style="list-style-type: none"> – IP address value • Domain Name <ul style="list-style-type: none"> – Domain name value – IP Address • Distinguished Name <ul style="list-style-type: none"> – Edit Name – IP Address 	<ul style="list-style-type: none"> • This option enables the IP address value box. This is the default. <ul style="list-style-type: none"> – In this box, specify the IP address value. • This option enables the domain name value box and the IP Address box. <ul style="list-style-type: none"> – In this box, specify the domain name value. – In this box, specify the IP address of the domain. • This option allows you to specify the name, department, state, and country of the gateway. <ul style="list-style-type: none"> – Using this button, specify the distinguished name settings. – 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, perform the following tasks:

- Choose an Identity
- Specify Authentication

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:
- a. If you are using digital certificates, select your digital certificate in the Select Certificate list. If you are not using digital certificates, then leave this field as-is.
 - b. In the ID_Type list, click **IP Address**.
 - c. In the Internal Network IP Address box enter VPN Client static IP address. In this example, **10.1.2.1** is entered.
 - d. In the Port list, click **All**.
 - e. In the Name list, click **Any**. The IP Addr list is inactive as a default.
 - f. If you are using pre-shared keys, click **Pre-shared**. Enter the key to be used during the Authentication Phase. Click **OK** when done. If you are not using pre-shared keys, then leave this field as-is.

Figure 3-6 shows how this is displayed on the My Identity pane. Table 3-4 describes the field descriptions for the My Identity pane.

Figure 3-6 My Identity Pane



Table 3-4 My Identity Pane Field Descriptions

Field	Description
My Identity	This pane allows you to specify the identity of the VPN Client. Choose an identification that will allow the IPsec peer to identify you during the key exchange phase in the My Identity pane.
My Identity	Under My Identity, specify options for determining the identity of the VPN Client. These options include selecting certificate or pre-shared key, 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	This list indicates the IP address option for the VPN Client on the corporate subnet. <ul style="list-style-type: none"> IP Address <ul style="list-style-type: none"> Internal Network IP Address
Port	This list shows the VPN Client's protocol ports. A default of <i>All</i> secures all protocol ports.

Table 3-4 My Identity Pane Field Descriptions (continued)

Field	Description
Local Network Interface or Internet Interface	Under Local Network Interface or Internet Interface, the hardware interface on the PC or laptop through which the connection will be established.
Name	This list indicates the name of the hardware interface. A default of <i>Any</i> enables all hardware interfaces.
IP Addr	A default of <i>Any</i> enables all hardware interface IP addresses.
Pre-shared Key	The Pre-shared Key button enables the Pre-shared Key window. To specify a pre-shared key or a wildcard pre-shared key, enter the key to be used during the Authentication Phase in the Pre-shared Key window.

To specify authentication

- To configure authentication on a VPN Client using pre-shared key or wildcard pre-shared key, see “Task 2—Configuring a Pre-Shared Key or Wildcard Pre-Shared Key on the Gateway” in Chapter 5, “Configuring a Pre-Shared Key or Wildcard Pre-Shared Key.”
- To configure authentication on a VPN Client using digital certification, see “Task 2—Configuring Digital Certification on the Gateway” in Chapter 6, “Configuring Digital Certification.”

Task 2—Configuring Manual Configuration on the Gateway

To configure manual configuration on the gateway, perform the following tasks:

- Configuring the Gateway
- Defining an IPSec Transform Set
- 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 3-5:

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

Table 3-5 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, <i>example.com</i> 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, <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)# 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 <i>IP name server</i> . The gateway's IP address is <i>192.168.1.1</i> .

Defining an IPSec Transform Set

To define an IPSec transform set on the gateway, perform the following tasks, as described in Table 3-6:

- Define IPSec Negotiation Security Associations
- Specify IPSec Encapsulation Method

Table 3-6 Defining an IPSec Transform Set


Command	Purpose
<pre>hq-sanjose(config)# crypto ipsec transform-set vpn-transform esp-des ah-md5-hmac</pre>	<p>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.</p> <p>In this example, the transform set named <i>vpn-transform</i> is defined with two security algorithm keywords: esp-des and ah-md5-hmac.</p> <p> 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.</p>
<pre>hq-sanjose(cfg-crypto-trans)# mode tunnel</pre>	<p>To specify IPSec 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.)</p> <p>In this example, the tunnel mode is configured for <i>vpn-transform</i> for an IPSec encrypted tunnel.</p>
<pre>hq-sanjose(cfg-crypto-trans)# exit</pre>	<p>To exit crypto transform (cfg-crypto-trans) configuration mode, enter the exit crypto transform configuration command.</p>

Defining a Dynamic Crypto Map

To define a dynamic crypto map, perform the following tasks, as described in Table 3-7:

- Define a Dynamic Crypto Map Entry
- Specify an IPSec Transform Set
- Define an Extended Access List
- Specify the IPSec Peer

Table 3-7 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, enter the crypto dynamic-map command. This command invokes the crypto map (config-crypto-map) configuration mode.</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 set transform-set crypto map configuration command.</p> <p>In this example, the transform set previously defined in “Defining an IPSec Transform Set,” <i>vpn-transform</i> is applied to the <i>vpn-dynamic</i> dynamic crypto map.</p> <p> Note You can list multiple transform sets in order of priority (highest priority first).</p>
<pre>hq_sanjose(config-crypto-map)# match address 101</pre>	<p>To specify an extended access list for a crypto map entry, enter the match address crypto map configuration command. This access list determines which traffic should or should not be protected by IPSec. If this is configured, the data flow identity proposed by the IPSec peer must fall within a permit statement for this crypto access list. If this is not configured, the router will accept any data flow identity proposed by the IPSec peer. However, if this is configured but the specified access list does not exist or is empty, the router will drop all packets.</p>
<pre>hq_sanjose(config-crypto-map)# exit</pre>	<p>To exit crypto map (config-crypto-map) configuration mode, enter the exit crypto map configuration command.</p>

Defining a Static Crypto Map

To define a static crypto map, perform the following tasks, as described in Table 3-8:

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

Table 3-8 Defining a 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 crypto map 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 (parent) map.</p>
<pre>hq_sanjose(config)# access-list 101 permit ip 192.168.1.1 255.255.255.0 host 10.1.2.1</pre>	<p>To permit all IP traffic between the host and the gateway, use the extended version of the access-list global configuration command.</p> <p> Note An access-list must be configured for each VPN Client configured with static IP addresses on a corporate subnet.</p> <p>All IP traffic is permitted between the two IPsec peers.</p>
<pre>hq_sanjose(config)# crypto map vpn-dynamic local-address loopback0</pre>	<p>To specify and name an identifying interface to be used by the dynamic crypto map for IPsec traffic, use the crypto map local-address global configuration command.</p> <p>In this example, the address that the IPsec will use on the gateway interfaces is loopback0.</p> <p>The loopback0 interface is specified as the local IP address for encryption on the gateway.</p>

Related Documentation

For more information on manual configuration, refer to the “Manual Configuration (Static IP Addressing)” 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.”

