



Configuring Dynamic IP Addressing

This chapter describes how to configure IP addresses on multiple remote Cisco Secure VPN Clients (VPN Clients) using Internet Key Exchange Mode Configuration (IKE Mode Configuration). With IKE Mode Configuration, you can set up Virtual Private Networks (VPNs) with dynamic IP addressing from a Cisco router (gateway) to multiple VPN Clients for scalable IP Security Protocol (IPSec) policy. You can use IKE mode configuration to replace static or dynamic IP address on VPN Clients. This chapter contains the following sections:

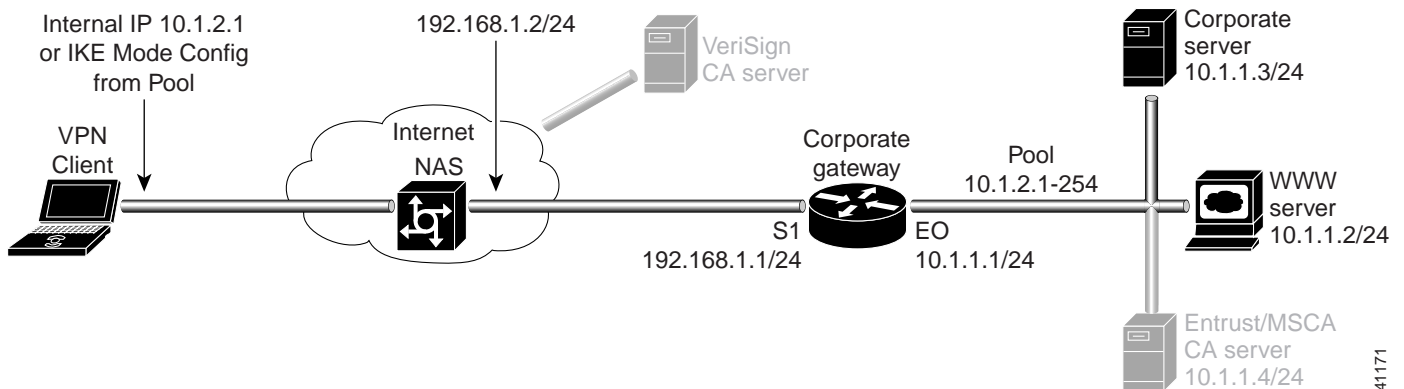
- Task 1—Configuring Dynamic IP Addressing on the VPN Client
- Task 2—Configuring Dynamic IP Addressing on the Gateway
- Related Documentation



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 4-1 Dynamic IP Addressing Topology



Task 1—Configuring Dynamic IP Addressing on the VPN Client

To configure IKE Mode Configuration on the VPN Client, you must specify an internal network address on the VPN Client. To do this, you must follow “Specifying an Internal Network Address on the VPN Client” in Chapter 3, “Configuring Manual Configuration.”

IKE Mode configuration is enabled by default on the VPN Client.

Task 2—Configuring Dynamic IP Addressing on the Gateway

To configure the gateway, perform the following tasks:

- Configuring the Gateway
- Defining an IPSec Transform Set
- Defining a Dynamic Crypto Map
- Defining the VPN Clients' IP Address Pool
- Defining a Static Crypto Map

Configuring the Gateway

To configure the gateway, perform the following tasks, as described in Table 4-1:

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

Table 4-1 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.

Defining an IPSec Transform Set

To define IPSec transform set on the gateway, perform the following tasks, as described in Table 4-2:

- Define IPSec Negotiation Security Associations
- Specify IPSec Encapsulation Method

Table 4-2 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 and enter crypto transform configuration mode, enter the crypto ipsec transform-set global configuration command.</p> <p>In this example, the transform set named <i>vpn-transform</i> is defined with two security algorithms: 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, <i>tunnel</i> 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 map 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 4-3:

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

Table 4-3 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 and enter the crypto map configuration mode, enter the crypto dynamic-map command.</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 be protected by IPsec and which traffic 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 configuration mode, enter the exit crypto map configuration command.</p>

Defining the VPN Clients' IP Address Pool

To define the VPN Clients' IP address pool, perform the following tasks, as described in Table 4-4:

- Define the VPN Client's Local IP Address Pool
- Reference the Local IP Address Pool to Reference IKE
- Specify Gateway-initiated IKE Mode Configuration

Table 4-4 Defining the VPN Clients' IP Address Pool


Command	Purpose
<pre>hq_sanjose(config)# ip local pool vpn-pool 10.1.2.1-10.1.2.254</pre>	<p>To define a local IP address pool for VPN Clients, enter the ip local pool command. You can use existing local address pools to define a set of addresses. The IP address pool must be within the IP range of the corporate subnet.</p> <p>In this example, the pool name is <i>vpn-pool</i>. This IP address pool has a range from <i>10.1.2.1—10.1.2.254</i>. The local address pool for VPN Clients is defined.</p>
<pre>hq_sanjose(config)# crypto isakmp client configuration address-pool local vpn-pool</pre>	<p>To configure the local IP address pool for VPN Clients to reference IKE on your router, use the crypto isakmp client configuration address-pool local global configuration command. In this example, the pool name is <i>vpn-pool</i>.</p> <p>The IP address pool for VPN Clients is set to reference IKE on your router.</p>
<pre>hq_sanjose(config)# crypto map vpnclient client configuration address initiate</pre>	<p>To configure IKE Mode Configuration on the static crypto map, use the crypto map client configuration address global configuration command. In this example, the crypto map is <i>vpnclient</i>. To indicate that IKE Mode Configuration is to be gateway-initiated, use the initiate keyword.</p> <p> Note Cisco supports gateway-initiated IKE Mode Configuration only. Client-initiated IKE Mode Configuration is not currently supported.</p> <p>A crypto map is defined for gateway-initiated IKE Mode Configuration.</p>
<pre>hq_sanjose(config)# exit</pre>	<p>To exit global configuration mode, enter the exit global configuration command.</p>

Defining a Static Crypto Map

To define a static crypto map, perform the following tasks, as described in Table 4-5:

- Defining a Static Crypto Map
- 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 4-5 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. 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>(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 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>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 interface 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 ip address 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 crypto map 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 IKE Mode Configuration, refer to the “IKE Mode Configuration (Dynamic 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.”