CHAPTER 5

IP Addresses for VPNs

This chapter describes IP address assignment methods.

IP addresses make internetwork connections possible. They are like telephone numbers: both the sender and receiver must have an assigned number to connect. But with VPNs, there are actually two sets of addresses: the first set connects client and server on the public network. Once that connection is made, the second set connects client and server through the VPN tunnel.

In ASA address management, we are dealing with the second set of IP addresses: those private IP addresses that connect a client with a resource on the private network, through the tunnel, and let the client function as if it were directly connected to the private network. Furthermore, we are dealing only with the private IP addresses that get assigned to clients. The IP addresses assigned to other resources on your private network are part of your network administration responsibilities, not part of VPN management. Therefore, when we discuss IP addresses here, we mean those IP addresses available in your private network addressing scheme that let the client function as a tunnel endpoint.

This chapter includes the following sections:

Configuring an IP Address Assignment Policy

The ASA can use one or more of the following methods for assigning IP addresses to remote access clients. If you configure more than one address assignment method, the ASA searches each of the options until it finds an IP address. By default, all methods are enabled.

- aaa — Retrieves addresses from an external authentication, authorization, and accounting server on a per-user basis. If you are using an authentication server that has IP addresses configured, we recommend using this method. This method is available for IPv4 and IPv6 assignment policies.
- dhcp — Obtains IP addresses from a DHCP server. If you want to use DHCP, you must configure a DHCP server. You must also define the range of IP addresses that the DHCP server can use. This method is available for IPv4 assignment policies.
- **local —** Internally configured address pools are the easiest method of address pool assignment to configure. If you choose local, you must also use the **ip-local-pool** command to define the range of IP addresses to use. This method is available for IPv4 and IPv6 assignment policies.

- – Allow the reuse of an IP address so many minutes after it is released—Delays the reuse of an IP address after its return to the address pool. Adding a delay helps to prevent problems firewalls can experience when an IP address is reassigned quickly. By default the ASA does not impose a delay. This configurable element is available for IPv4 assignment policies.

Use one of these methods to specify a way to assign IP addresses to remote access clients.

- Configuring IPv4 Address Assignments at the Command Line
- Configuring IPv6 Address Assignments at the Command Line

Configuring IPv4 Address Assignments at the Command Line

Command	Purpose

vpn-addr-assign {aaa | dhcp | local [reuse-delay *minutes*]}
Example:
`hostname(config)#` **`vpn-addr-assign aaa`**
Example:
`hostname(config)#` **`vpn-addr-assign local reuse-delay 180`**
Example:
`hostname(config)#` **`no vpn-addr-assign dhcp`**
	Enables an address assignment method for the ASA to use when assigning IPv4 address to VPN connections. The available methods to obtain an IP address are from a AAA server, DHCP server, or a local address pool. All of these methods are enabled by default.
	For local IP address pools, you can configure the reuse of an IP address for between 0 and 480 minutes after the IP address has been released.
	Use the no form of the command to disable an address assignment method.

Configuring IPv6 Address Assignments at the Command Line

Command	Purpose

ipv6-vpn-addr-assign {aaa | local}
Example:
`hostname(config)#` **`ipv6-vpn-addr-assign aaa`**
Example:
`hostname(config)#` **`no ipv6-vpn-addr-assign local`**
	Enables an address assignment method for the ASA to use when assigning IPv6 address to VPN connections. The available methods to obtain an IP address are from a AAA server or a local address pool. Both of these methods are enabled by default.
	Use the no form of the command to disable an address assignment method.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
			Multiple	
Routed	Transparent	Single	Context	System
•	—	•	—	—

Viewing Address Assignment Methods

Use one of these methods to view the address assignment method configured on the ASA:

Viewing IPv4 Address Assignments from the Command Line

Command	Purpose

show running-config all vpn-addr-assign
Example:
`hostname(config)# show running-config all vpn-addr-assign`
	Shows the configured address assignment method. Configured address methods could be aaa, dhcp, or local.
	`vpn-addr-assign aaa`
	`vpn-addr-assign dhcp`
	`vpn-addr-assign local`

Viewing IPv6 Address Assignments from the Command Line

Command	Purpose

show running-config all ipv6-vpn-addr-assign
Example:
`hostname(config)# show running-config all ipv6-vpn-addr-assign`
	Shows the configured address assignment method. Configured address methods could be aaa or local.
	`ipv6-vpn-addr-assign aaa`
	`ipv6-vpn-addr-assign local reuse-delay 0`

Configuring Local IP Address Pools

To configure IPv4 address pools to use for VPN remote access tunnels, enter the **ip local pool** command in global configuration mode. To delete address pools, enter the **no** form of this command.

To configure IPv6 address pools to use for VPN remote access tunnels, enter the **ipv6 local pool** command in global configuration mode. To delete address pools, enter the **no** form of this command.

The ASA uses address pools based on the connection profile or group policy for the connection. The order in which you specify the pools is important. If you configure more than one address pool for a connection profile or group policy, the ASA uses them in the order in which you added them to the ASA.

If you assign addresses from a non-local subnet, we suggest that you add pools that fall on subnet boundaries to make adding routes for these networks easier.

Use one of these methods to configure a local IP address pool:

- Configuring Local IPv4 Address Pools Using CLI, page 5-4
- Configuring Local IPv6 Address Pools Using CLI, page 5-4

Configuring Local IPv4 Address Pools Using CLI

	Command	Purpose
Step 1	**vpn-addr-assign local** **Example:** hostname(config)# **vpn-addr-assign local**	Configures IP address pools as the address assignment method, enter the **vpn-addr-assign** command with the **local** argument. See also Configuring IPv4 Address Assignments at the Command Line, page 5-2.
Step 2	**ip local pool** *poolname first_address–last_address* **mask** *mask* **Example:** hostname(config)# ip local pool **firstpool** **10.20.30.40-10.20.30.50** mask **255.255.255.0** **Example:** hostname(config)# no ip local pool **firstpool**	Configures an address pool. The command names the pool, specifies a range of IPv4 addresses and the subnet mask. The first example configures an IP address pool named **firstpool**. The starting address is **10.20.30.40** and the ending address is **10.20.30.50**. The network mask is **255.255.255.0**. The second example deletes the IP address pool named **firstpool**.

Configuring Local IPv6 Address Pools Using CLI

	Command	Purpose
Step 1	**ipv6-vpn-addr-assign local** **Example:** hostname(config)# **ipv6-vpn-addr-assign local**	Configures IP address pools as the address assignment method, enter the ipv6-**vpn-addr-assign** command with the **local** argument. See also Configuring IPv6 Address Assignments at the Command Line, page 5-2.
Step 2	**ipv6 local pool** *pool_name starting_address prefix_length number_of_addresses* **Example:** hostname(config)# **ipv6 local pool** *ipv6pool 2001:DB8::1/32 100* **Example:** hostname(config)# **no ipv6 local pool** *ipv6pool*	Configures an address pool. The command names the pool, identifies the starting IPv6 address, the prefix length in bits, and the number of addresses to use in the range. The first example configures an IP address pool named **ipv6pool**. The starting address is **2001:DB8::1** the prefix length is **32** bits and the number of addresses to use in the pool is **100**. The second example deletes the IP address pool named **ipv6pool**.

Assign Internal Address Pools to Group Policies in ASDM

The Add or Edit Group Policy dialog box lets you specify address pools, tunneling protocols, filters, connection settings, and servers for the internal Network (Client) Access group policy being added or modified. For each of the fields in this dialog box, checking the Inherit check box lets the corresponding setting take its value from the default group policy. Inherit is the default value for all the attributes in this dialog box.

You can configure both IPv4 and IPv6 address pools for the same group policy. If both versions of IP addresses are configured in the same group policy, clients configured for IPv4 will get an IPv4 address, clients configured for IPv6 will get an IPv6 address, and clients configured for both IPv4 and IPv6 addresses will get both an IPv4 and an IPv6 address.

Step 1 Connect to the ASA using ASDM and select **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

Step 2 Create a new group policy or the group policy you want to configure with an internal address pool and click **Edit**.

The General attributes pane is selected by default in the group policy dialog.

Step 3 Use the Address Pools field to specify an IPv4 address pool for this group policy. Click Select to add or edit an IPv4 address pool.

Step 4 Use the IPv6 Address Pools field to specify an IPv6 address pools to use for this group policy. Click Select to add or edit a IPv6 address pool.

Step 5 Click **OK**.

Step 6 Click **Apply**.

Configuring AAA Addressing

To use a AAA server to assign addresses for VPN remote access clients, you must first configure a AAA server or server group. See the **aaa-server protocol** command in the command reference.

In addition, the user must match a connection profile configured for RADIUS authentication.

The following examples illustrate how to define a AAA server group called RAD2 for the tunnel group named firstgroup. It includes one more step than is necessary, in that previously you might have named the tunnel group and defined the tunnel group type. This step appears in the following example as a reminder that you have no access to subsequent tunnel-group commands until you set these values.

An overview of the configuration that these examples create follows:

```
hostname(config)# vpn-addr-assign aaa
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)# authentication-server-group RAD2
```

To configure AAA for IP addressing, perform the following steps:

Step 1 To configure AAA as the address assignment method, enter the **vpn-addr-assign** command with the **aaa** argument:

```
hostname(config)# vpn-addr-assign aaa
hostname(config)#
```

Step 2 To establish the tunnel group called firstgroup as a remote access or LAN-to-LAN tunnel group, enter the **tunnel-group** command with the **type** keyword. The following example configures a remote access tunnel group.

```
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)#
```

Step 3 To enter general-attributes configuration mode, which lets you define a AAA server group for the tunnel group called firstgroup, enter the **tunnel-group** command with the **general-attributes** argument.

```
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)#
```

Step 4 To specify the AAA server group to use for authentication, enter the **authentication-server-group** command.

```
hostname(config-general)# authentication-server-group RAD2
hostname(config-general)#
```

This command has more arguments that this example includes. For more information, see the command reference.

Configuring DHCP Addressing

To use DHCP to assign addresses for VPN clients, you must first configure a DHCP server and the range of IP addresses that the DHCP server can use. Then you define the DHCP server on a connection profile basis. Optionally, you can also define a DHCP network scope in the group policy associated with a connection profile or username. This is either an IP network number or IP Address that identifies to the DHCP server which pool of IP addresses to use.

The following examples define the DHCP server at IP address 172.33.44.19 for the connection profile named **firstgroup**. They also define a DHCP network scope of 192.86.0.0 for the group policy called **remotegroup**. (The group policy called remotegroup is associated with the connection profile called firstgroup). If you do not define a network scope, the DHCP server assigns IP addresses in the order of the address pools configured. It goes through the pools until it identifies an unassigned address.

The following configuration includes more steps than are necessary, in that previously you might have named and defined the connection profile type as remote access, and named and identified the group policy as internal or external. These steps appear in the following examples as a reminder that you have no access to subsequent tunnel-group and group-policy commands until you set these values.

Guidelines and Limitations

You can only use an IPv4 address to identify a DHCP server to assign client addresses.

Configuring DHCP Addressing Using the CLI

	Command	Purpose
Step 1	`vpn-addr-assign dhcp`	Configures IP address pools as the address assignment method. Enter the **vpn-addr-assign** command with the **dhcp** argument. See also Configuring IPv4 Address Assignments at the Command Line, page 5-2.
Step 2	`tunnel-group firstgroup type remote-access`	Establishes the connection profile called firstgroup as a remote access connection profile. Enter the **tunnel-group** command with the **type** keyword and **remote-access** argument.
Step 3	`tunnel-group firstgroup general-attributes`	Enters the general-attributes configuration mode for the connection profile so that you can configure a DHCP server. Enter the **tunnel-group** command with the **general-attributes** argument.

Step 4	`dhcp-server IPv4_address_of_DHCP_server`
	Example:
	`hostname(config-general)# dhcp-server 172.33.44.19`
	`hostname(config-general)#`
		Defines the DHCP server by IPv4 address. You can not define a DHCP server by an IPv6 address. You can specify more than one DHCP server address for a connection profile.
		Enter the **dhcp-server** command. This command will allow you to configure the ASA to send additional options to the specified DHCP servers when it is trying to get IP addresses for VPN clients. See the **dhcp-server** command in the *Cisco Security Appliance Command Reference* guide for more information.
		The example configures a DHCP server at IP address 172.33.44.19.

Step 5	`hostname(config-general)# exit`
	`hostname(config)#`
		Exit tunnel-group mode.

Step 6	`hostname(config)# group-policy remotegroup internal`	Creates an internal group policy called **remotegroup**. Enter the **group-policy** command with the **internal** argument to make an internal group policy. The example configures an internal group.

	Command	Purpose
Step 7	hostname(config)# group-policy remotegroup **attributes** **Example:** hostname(config)# group-policy remotegroup **attributes** hostname(config-group-policy)#	(Optional) Enters group-policy attributes configuration mode, which lets you configure a subnetwork of IP addresses for the DHCP server to use. Enter the **group-policy** command with the **attributes** keyword. The example enters group policy attributes configuration mode for **remotegroup** group-policy.
Step 8	hostname(config-group-policy)# **dhcp-network-scope 192.86.0.0** hostname(config-group-policy)#	(Optional) To specify the range of IP addresses the DHCP server should use to assign addresses to users of the group policy called **remotegroup**, enter the **dhcp-network-scope** command. The example configures a network scope of 192.86.0.0. **Note** The dhcp-network-scope must be a routable IP address and not the subset of the DHCP pool. The DHCP server determines which subnet this IP address belongs to and assigns an IP address from that pool. We recommend that you use an interface of the ASA as a dhcp-network-scope for routing reasons. You can use any IP address as the dhcp-network-scope, but it may require that static routes be added to the network.

Example

A summary of the configuration that these examples create follows:

```
hostname(config)# vpn-addr-assign dhcp
hostname(config)# tunnel-group firstgroup type remote-access
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)# dhcp-server 172.33.44.19
hostname(config-general)# exit
hostname(config)# group-policy remotegroup internal
hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)# dhcp-network-scope 192.86.0.0
```

Assigning IP Addresses to Local Users

Local user accounts can be configured to use a group policy, and some AnyConnect attributes can also be configured. These user accounts provide fallback if the other sources of IP address fail, so administrators will still have access.

This section describes how to configure all the attributes of a local user.

Prerequisites

This procedure describes how to edit an existing user. To add a user select **Configuration > Remote Access VPN > AAA/Local Users > Local Users** and click **Add**. For more information, see the general operations configuration guide.

User Edits

By default, the **Inherit** check box is checked for each setting on the Edit User Account screen, which means that the user account inherits the value of that setting from the default group policy, DfltGrpPolicy.

To override each setting, uncheck the **Inherit** check box, and enter a new value. The detailed steps that follow describe each of the settings on the Edit User Account screen.

Detailed Steps

Step 1 Start ASDM and select **Configuration > Remote Access VPN > AAA/Local Users > Local Users**.

Step 2 Chose the user you want to configure and click **Edit**.

The Edit User Account screen opens.

Step 3 In the left pane, click **VPN Policy**.

Step 4 Specify a group policy for the user. The user policy will inherit the attributes of this group policy. If there are other fields in this screen that are set to **Inherit** the configuration from the Default Group Policy, the attributes specified in this group policy will take precedence over those in the Default Group Policy.

Step 5 Specify which tunneling protocols are available for the user, or whether the value is inherited from the group policy. Check the desired **Tunneling Protocols** check boxes to choose the VPN tunneling protocols that are available for use. Only the selected protocols are available for use. The choices are as follows:

- Clientless SSL VPN (VPN via SSL/TLS) uses a web browser to establish a secure remote-access tunnel to a VPN Concentrator; requires neither a software nor hardware client. Clientless SSL VPN can provide easy access to a broad range of enterprise resources, including corporate websites, web-enabled applications, NT/AD file shares (web-enabled), e-mail, and other TCP-based applications from almost any computer that can reach HTTPS Internet sites.
- The SSL VPN Client lets users connect after downloading the Cisco AnyConnect Client application. Users use a clientless SSL VPN connection to download this application the first time. Client updates then occur automatically as needed whenever the user connects.
- IPsec IKEv1—IP Security Protocol. Regarded as the most secure protocol, IPsec provides the most complete architecture for VPN tunnels. Both Site-to-Site (peer-to-peer) connections and Cisco VPN client-to-LAN connections can use IPsec IKEv1.
- IPsec IKEv2—IPsec IKEv2-Supported by the AnyConnect Secure Mobility Client. AnyConnect connections using IPsec with IKEv2 can make use of the same feature set available to SSL VPN Connections.
- L2TP over IPsec allows remote users with VPN clients provided with several common PC and mobile PC operating systems to establish secure connections over the public IP network to the ASA and private corporate networks.

Note If no protocol is selected, an error message appears.

Step 6 Specify which filter (IPv4 or IPv6) to use, or whether to inherit the value from the group policy. Filters consist of rules that determine whether to allow or reject tunneled data packets coming through the ASA, based on criteria such as source address, destination address, and protocol. To configure filters and rules, choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > General > More Options > Filter.**

Click **Manage** to display the ACL Manager pane, on which you can add, edit, and delete ACLs and ACEs.

Step 7 Specify whether to inherit the Connection Profile (tunnel group) lock or to use the selected tunnel group lock, if any. Selecting a specific lock restricts users to remote access through this group only. Tunnel Group Lock restricts users by checking if the group configured in the VPN client is the same as the users assigned group. If it is not, the ASA prevents the user from connecting. If the Inherit check box is not checked, the default value is None.

Step 8 Specify whether to inherit the Store Password on Client System setting from the group. Uncheck the **Inherit** check box to activate the Yes and No radio buttons. Click **Yes** to store the logon password on the client system (potentially a less-secure option). Click **No** (the default) to require the user to enter the password with each connection. For maximum security, we recommend that you *not allow* password storage.

Step 9 Specify an Access Hours policy to apply to this user, create a new access hours policy for the user, or leave the Inherit box checked. The default value is Inherit, or, if the Inherit check box is not checked, the default value is Unrestricted.

Click **Manage** to open the Add Time Range dialog box, in which you can specify a new set of access hours.

Step 10 Specify the number of simultaneous logons by the user. The Simultaneous logons parameter specifies the maximum number of simultaneous logons allowed for this user. The default value is 3. The minimum value is 0, which disables logon and prevents user access.

Note While there is no maximum limit, allowing several simultaneous connections could compromise security and affect performance.

Step 11 Specify the **maximum connection time** for the user connection time in minutes. At the end of this time, the system terminates the connection. The minimum is 1 minute, and the maximum is 2147483647 minutes (over 4000 years). To allow unlimited connection time, check the **Unlimited** check box (the default).

Step 12 Specify the Idle Timeout for the user in minutes. If there is no communication activity on the connection by this user in this period, the system terminates the connection. The minimum time is 1 minute, and the maximum time is 10080 minutes. This value does not apply to users of clientless SSL VPN connections.

Step 13 Configure the Session Alert Interval. If you uncheck the Inherit check box, the Default checkbox is checked automatically. This sets the session alert interval to 30 minutes. If you want to specify a new value, uncheck the Default check box and specify a session alert interval from 1 to 30 minutes in the minutes box.

Step 14 Configure the Idle Alert Interval. If you uncheck the Inherit check box, the Default checkbox is checked automatically. This sets the idle alert interval to 30 minutes. If you want to specify a new value, uncheck the Default check box and specify a session alert interval from 1 to 30 minutes in the minutes box.

Step 15 To set a dedicated IPv4 address for this user, enter an IPv4 address and subnet mask in the Dedicated IPv4 Address (Optional) area.

Step 16 To set a dedicated IPv6 address for this user, enter an IPv6 address with an IPv6 prefix in the Dedicated IPv6 Address (Optional) field. The IPv6 prefix indicates the subnet on which the IPv6 address resides.

Step 17 To configure clientless SSL settings, in the left pane, click **Clientless SSL VPN**. To override each setting, uncheck the **Inherit** check box, and enter a new value.

Step 18 Click **Apply**.

The changes are saved to the running configuration.