Configuring 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.

- Use authentication server — 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. You can configure AAA servers in the Configuration > AAA Setup pane.This method is available for IPv4 and IPv6 assignment policies.
- Use 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. If you use DHCP, configure the server in the Configuration > Remote Access VPN > DHCP Server pane. This method is available for IPv4 assignment policies.

- **Use an internal address pool —** Internally configured address pools are the easiest method of address pool assignment to configure. If you use this method, configure the IP address pools in Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools pane. 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, this is unchecked, meaning the ASA does not impose a delay. If you want one, check the box and enter the number of minutes in the range 1 - 480 to delay IP address reassignment.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 IP Address Assignment Options using ASDM

Configuring IP Address Assignment Options using ASDM

Step 1 Select **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy**

Step 2 In the IPv4 Policy area, check the address assignment method to enabled it or uncheck the address assignment method to disable it. These methods are enabled by default:

- Use Authentication server. Enables the use of a Authentication Authorization and Accounting (AAA) server you have configured to provide IP addresses.
- Use DHCP. Enables the use of a Dynamic Host Configuration Protocol (DHCP) server you have configured to provide IP addresses.
- Use internal address pools: Enables the use of a local address pool configured on the ASA.

If you enable **Use internal address pools**, you can also enable the reuse of an IPv4 address after it has been released. You can specify a range of minutes from 0-480 after which the IP v4 address can be reused.

Step 3 In the IPv6 Policy area, check the address assignment method to enable it or uncheck the address assignment method to disable it. These methods are enabled by default:

- Use Authentication server. Enables the use of a Authentication Authorization and Accounting (AAA) server you have configured to provide IP addresses.
- Use internal address pools: Enables the use of a local address pool configured on the ASA.

Step 4 Click **Apply**.

Step 5 Click **OK**.

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 and IPv6 Address Assignments using ASDM

Select **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy**

Configuring Local IP Address Pools

To configure IPv4 or IPv6 address pools for VPN remote access tunnels, open ASDM and select **Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools > Add/Edit IP Pool**. To delete an address pool, open ASDM and select **Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools**. Select the address pool you want to delete and click **Delete**.

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 ASDM, page 5-3
- Configuring Local IPv6 Address Pools Using ASDM, page 5-4

Configuring Local IPv4 Address Pools Using ASDM

The IP Pool area shows each configured address pool by name with their IP address range, for example: 10.10.147.100 to 10.10.147.177. If no pools exist, the area is empty. The ASA uses these pools in the order listed: if all addresses in the first pool have been assigned, it uses the next pool, and so on.

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.

Step 1 **Select Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools.**

Step 2 To add an IPv4 address, click **Add > IPv4 Address pool**. To edit an existing address pool, select the address pool in the address pool table and click **Edit**.

Step 3 In the Add/Edit IP Pool dialog box enter this information:

- Pool Name—Enter the name of the address pool. It can be up to 64 characters
- Starting Address—Enter the first IP address available in each configured pool. Use dotted decimal notation, for example: 10.10.147.100.
- Ending Address—Enter the last IP address available in each configured pool. User dotted decimal notation, for example: 10.10.147.177.
- Subnet Mask—Identifies the subnet on which this IP address pool resides.

Step 4 Click **Apply**.

Step 5 Click **OK**.

Configuring Local IPv6 Address Pools Using ASDM

The IP Pool area shows each configured address pool by name with a starting IP address range, the address prefix, and the number of addresses configurable in the pool. If no pools exist, the area is empty. The ASA uses these pools in the order listed: if all addresses in the first pool have been assigned, it uses the next pool, and so on.

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.

Step 1 **Select Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools.**

Step 2 To add an IPv6 address, click **Add > IPv6 Address pool**. To edit an existing address pool, select the address pool in the address pool table and click **Edit**.

Step 3 In the Add/Edit IP Pool dialog box enter this information:

- Name—Displays the name of each configured address pool.
- Starting IP Address—Enter the first IP address available in the configured pool. For example: 2001:DB8::1.
- Prefix Length— Enter the IP address prefix length in bits. For example 32 represents /32 in CIDR notation. The prefix length defines the subnet on which the pool of IP addresses resides.
- Number of Addresses—Identifies the number of IPv6 addresses, starting at the Starting IP Address, there are in the pool.

Step 4 Click **Apply**.

Step 5 Click **OK**.

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.

Assigning IP addresses using DHCP

Configure your DHCP servers, then create group policies that use those servers. When a user selects that that group policy, the DHCP server will assign an address for the VPN connection.

Configure Your DHCP Servers

DHCP server, configure the IP address Assignment policy to use DHCP follow the instructions below. You cannot assign IPv6 addresses to AnyConnect clients using a DHCP server.

Step 1 Connect to the ASA using ASDM.

Step 2 Verify that DHCP is enabled on Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy.

Step 3 Configure your DHCP servers by selecting Configuration > Remote Access VPN > DHCP Server.

Assign the DHCP IP Addressing to a Group Policy

Step 1 Select **Configuration > Remote Access VPN > Network (Client) Access> AnyConnect Connection Profiles**.

Step 2 In the Connection Profiles Area click **Add** or **Edit**.

Step 3 Click **Basic** in the configuration tree for the connection profile.

Step 4 In the Client Address Assignment area, enter the IPv4 address of the DHCP server you want to use to assign IP addresses to clients. For example, **172.33.44.19**.

Step 5 Edit the group-policy associated with the connection profile to define the DHCP scope. Select **Configuration > Remote Access VPN > Network (Client) Access> Group Policies.**

Step 6 Double-click the group policy you want to edit.

Step 7 Click **Servers** in the configuration tree.

Step 8 Expand the **More Options** area by clicking the down arrow.

Step 9 Uncheck DHCP Scope **Inherit**.

Step 10 Enter the IP network number or IP Address that identifies to the DHCP server which pool of IP addresses to use. For example, **192.86.0.0**.

Step 11 Click **OK**.

Step 12 Click **Apply**.

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 "Adding a User Account to the Local Database" in Chapter 42, Configuring AAA Servers and the Local Database in the *Cisco ASA 5500 Configuration Guide Using ASDM*.

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 Select 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 on 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.