IP Addresses for VPNs

Configure 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 the following methods to specify a way to assign IP addresses to remote access clients.

Configure IP Address Assignment Options

Procedure

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 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 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**.

View Address Assignment Methods

Procedure

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

Configure Local IP Address Pools

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

Configure Local IPv4 Address Pools

The IP Pool area shows the configured address pools 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.

Procedure

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, choose 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**.

Configure Local IPv6 Address Pools

The IP Pool area shows the configured address pools 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.

Procedure

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, choose 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, that are in the pool.

Step 4 Click **Apply**.

Step 5 Click **OK**.

Assign Internal Address Pools to Group Policies

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.

Procedure

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**.

Configure 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.

The following example defines the DHCP server at 172.33.44.19 for the connection profile named **firstgroup**. The example also defines a DHCP network scope of 10.100.10.1 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.

Before you begin

You can only use an IPv4 address to identify a DHCP server to assign client addresses. In addition, DHCP options are not forwarded to users, they receive an address assignment only.

Procedure

Step 1 Configure your DHCP servers.

You cannot assign IPv6 addresses to Secure Clients using a DHCP server.

a) Verify that DHCP is enabled on **Configuration** > **Remote Access VPN** > **Network (Client) Access** > > **Address Assignment** > **Assignment Policy**.
b) Configure your DHCP servers by selecting **Configuration** > **Remote Access VPN** > **DHCP Server**.

Step 2 Define the DHCP server in the connection profile.

a) Select **Configuration** > **Remote Access VPN** > **Network (Client) Access > Secure Client Connection Profiles**.
b) In the Connection Profiles Area click **Add** or **Edit**.
c) Click **Basic** in the configuration tree for the connection profile.
d) 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 3 Edit the group-policy associated with the connection profile to define the DHCP scope.

a) Select **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.
b) Double-click the group policy you want to edit.
c) Click **Server**in the configuration tree.
d) Expand the **More Options** area by clicking the down arrow.
e) Uncheck DHCP Scope **Inherit** and define the DHCP scope.

If you configure DHCP servers for the address pool in the connection profile, the DHCP scope identifies the subnets to use for the pool for this group. The DHCP server must also have addresses in the same

subnet identified by the scope. The scope allows you to select a subset of the address pools defined in the DHCP server to use for this specific group.

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.

To specify a scope, enter a routeable address on the same subnet as the desired pool, but not within the pool. The DHCP server determines which subnet this IP address belongs to and assigns an IP address from that pool.

We recommend using the IP address of an interface whenever possible for routing purposes. For example, if the pool is 10.100.10.2-10.100.10.254, and the interface address is 10.100.10.1/24, use 10.100.10.1 as the DHCP scope. Do not use the network number. You can use DHCP for IPv4 addressing only. If the address you choose is not an interface address, you might need to create a static route for the scope address.

f) Click **OK**.
g) Click **Apply**.

Assign IP Addresses to Local Users

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

Before you begin

To add or edit a user, choose **Configuration > Remote Access VPN > AAA/Local Users > Local Users** and click **Add** or **Edit**.

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 the IP address settings. See Configure VPN Policy Attributes for a Local User for full configuration details.

Procedure

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

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

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

Step 4 To set a dedicated IPv4 address for this user, enter an IPv4 address and subnet mask in the **Dedicated IPv4 Address (Optional)** area.

Step 5 To set a dedicated IPv6 address for this user, enter an IPv6 address with an IPv6 prefix in the **Dedicated IPv6 Address (Optional)** area. The IPv6 prefix indicates the subnet on which the IPv6 address resides.

Step 6 Click**Apply** to save the changes to the running configuration.