

IP Addresses for VPNs

- Configure an IP Address Assignment Policy, on page 1
- Configure Local IP Address Pools, on page 3
- Configure AAA Addressing, on page 5
- Configure DHCP Addressing, on page 6

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.

- 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.

Note When you configure both a DHCP server and a local IP address pool for address assignment, automatic fallback to the local pool (if the DHCP server is unavailable) works only for SSL-based remote access VPN connections.

For IPsec-based remote access VPN connections, this fallback may not complete in time if the DHCP server is unreachable, which can cause the connection to fail.

To avoid connection issues with IPsec-based remote access VPN, do one of the following:

- Make sure the DHCP server is reachable, or
- Use only a local IP address pool for address assignment.

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

Configure IPv4 Address Assignments

Procedure

Enable 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.

vpn-addr-assign {**aaa** | **dhcp** | **local** [**reuse-delay** *minutes*]}

Example:

For example, you can configure the reuse of an IP address for between 0 and 480 minutes after the IP address has been released.

```
hostname(config)#vpn-addr-assign aaa
hostname(config)#vpn-addr-assign local reuse-delay 180
```

This example uses the no form of the command to disable an address assignment method.

```
hostname(config)# no vpn-addr-assign dhcp
```

Configure IPv6 Address Assignments

Procedure

Enable 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.

ipv6-vpn-addr-assign {**aaa** | local}

Example:

```
hostname(config)# ipv6-vpn-addr-assign aaa
```

This example uses the no form of the command to disable an address assignment method.

```
hostname(config)# no ipv6-vpn-addr-assign local
```

View Address Assignment Methods

Procedure

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

- View IPv4 Address Assignments

  Show the configured address assignment method. The configured address method could be aaa, dhcp, or local.

  ```
  show running-config all vpn-addr-assign
  vpn-addr-assign aaa
  vpn-addr-assign dhcp
  vpn-addr-assign local
  ```

- View IPv6 Address Assignments

  Show the configured address assignment method. Configured address methods could be aaa or local.

  ```
  show running-config all ipv6-vpn-addr-assign
  ipv6-vpn-addr-assign aaa
  ipv6-vpn-addr-assign local reuse-delay 0
  ```

Configure 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.

Note When you modify existing address pools currently in use within an active tunnel-group (that is, open to end users for connections), you must perform the change in a change window and ensure the following:

- The connected users are logged off.
- The address pools are removed from the tunnel-group and modified as required.
- The modified address pools are then added back under the tunnel-group.

If an address pool is not modified in this manner, it may cause inconsistencies in the ASA's behaviour.

Configure Local IPv4 Address Pools

Note When you want to modify an existing address-pool currently in use within an active tunnel-group (i.e. open to end users for connections) on the CLI, it is recommended to perform this change in a change window. The users connected should be logged off, the address pool should be removed from the tunnel-group, modified as required and then added back under the tunnel-group. If not done in this manner, it may cause inconsistencies in the ASA's behavior.

Procedure

Step 1 Configure IP address pools as the address assignment method. Enter the **vpn-addr-assign** command with the **local** argument.

Example:

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

Step 2 Configure an address pool. The command names the pool, specifies a range of IPv4 addresses and the subnet mask.

ip local pool*poolname first_address-last_address***mask***mask*

Example:

This example configures an IP address pool named *firstpool*.The starting address is 10.20.30.40and the ending address is 10.20.30.50.The network mask is 255.255.255.0.

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

This example deletes the IP address pool named **firstpool**.

```
hostname(config)# no ip local pool firstpool
```

Configure Local IPv6 Address Pools

Procedure

Step 1 Configures IP address pools as the address assignment method, enter the ipv6-**vpn-addr-assign** command with the **local** argument.

Example:

```
hostname(config)# ipv6-vpn-addr-assign local
```

Step 2 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.

ipv6 local pool *pool_name starting_address prefix_length number_of_addresses*

Example:

This 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.

```
hostname(config)# ipv6 local pool ipv6pool 2001:DB8::1/32 100
```

This example deletes the IP address pool named *ipv6pool*.

```
hostname(config)# no ipv6 local pool ipv6pool
```

Configure 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)# authentication-server-group RAD2
```

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

Procedure

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)#
```

What to do next

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

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 IP address pools as the address assignment method.

vpn-addr-assign dhcp

Step 2 Establish the connection profile called **firstgroup** as a remote access connection profile.

tunnel-group firstgroup type remote-access

Step 3 Enter the general-attributes configuration mode for the connection profile so that you can configure a DHCP server.

tunnel-group firstgroup general-attributes

Step 4 Define the DHCP server by IPv4 address, then exit tunnel group configuration mode.

dhcp-server *IPv4_address_of_DHCP_server*

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 allows 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.

Example:

The example configures a DHCP server at IP address 172.33.44.19. Then, exit tunnel group configuration mode .

```
hostname(config-general)# dhcp-server 172.33.44.19
hostname(config-general)# exit
hostname(config)#
```

Step 5 If the group does not already exist, create an internal group policy called **remotegroup**.

```
hostname(config)# group-policy remotegroup internal
```

Step 6 (Optional.) Enter group-policy attributes configuration mode and define the DHCP network scope.

dhcp-network-scope *ip_address*

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.

Note
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.

Example:

The following example enters attribute configuration mode for remotegroup and sets the DHCP scope to 10.100.10.1.

```
hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.100.10.1
```

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 10.100.10.1
```