CHAPTER 8

Configuring DHCP

This chapter describes how to configure the DHCP server, and includes the following topics:

Information About DHCP

DHCP provides network configuration parameters, such as IP addresses, to DHCP clients. The adaptive security appliance can provide a DHCP server or DHCP relay services to DHCP clients attached to adaptive security appliance interfaces. The DHCP server provides network configuration parameters directly to DHCP clients. DHCP relay passes DHCP requests received on one interface to an external DHCP server located behind a different interface.

Licensing Requirements for DHCP

Table 8-1 shows the licensing requirements for DHCP.

Table 8-1 Licensing Requirements

Model	License Requirement
All models	Base License.

For the Cisco ASA 5505 adaptive security appliance, the maximum number of DHCP client addresses varies depending on the license:

- If the limit is 10 hosts, the maximum available DHCP pool is 32 addresses.
- If the limit is 50 hosts, the maximum available DHCP pool is 128 addresses.

- If the number of hosts is unlimited, the maximum available DHCP pool is 256 addresses.

Note By default, the Cisco ASA 5505 adaptive security appliance ships with a 10-user license.

Guidelines and Limitations

Use the following guidelines to configure the DHCP server:

- You can configure a DHCP server on each interface of the adaptive security appliance. Each interface can have its own pool of addresses to draw from. However the other DHCP settings, such as DNS servers, domain name, options, ping timeout, and WINS servers, are configured globally and used by the DHCP server on all interfaces.
- You cannot configure a DHCP client or DHCP relay services on an interface on which the server is enabled. Additionally, DHCP clients must be directly connected to the interface on which the server is enabled.
- The adaptive security appliance does not support QIP DHCP servers for use with DHCP proxy.
- When it receives a DHCP request, the adaptive security appliance sends a discovery message to the DHCP server. This message includes the IP address (within a subnetwork) configured with the **dhcp-network-scope** command in the group policy. If the server has an address pool that falls within that subnetwork, the server sends the offer message with the pool information to the IP address—not to the source IP address of the discovery message.
- For example, if the server has a pool in the range of 209.165.200.225 to 209.165.200.254, mask 255.255.255.0, and the IP address specified by the **dhcp-network-scope** command is 209.165.200.1, the server sends that pool in the offer message to the adaptive security appliance.

Failover Guidelines

Supports Active/Active and Active/Standby failover.

Firewall Mode Guidelines

Supported in routed and transparent firewall modes.

Context Mode Guidelines

Supported in single mode and multiple context mode.

Configuring a DHCP Server

This section describes how to configure a DHCP server provided by the adaptive security appliance, and includes the following topics:

- Enabling the DHCP Server, page 8-3
- Configuring DHCP Options, page 8-4
- Using Cisco IP Phones with a DHCP Server, page 8-6
- DHCP Monitoring Commands, page 8-8

Enabling the DHCP Server

The adaptive security appliance can act as a DHCP server. DHCP is a protocol that provides network settings to hosts, including the host IP address, the default gateway, and a DNS server.

Note The adaptive security appliance DHCP server does not support BOOTP requests. In multiple context mode, you cannot enable the DHCP server or DHCP relay on an interface that is used by more than one context.

To enable the DHCP server on a adaptive security appliance interface, perform the following steps:

	Command	Purpose
Step 1	**dhcpd address** *ip_address*-*ip_address interface_name* **Example:** `hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside`	Create a DHCP address pool. The adaptive security appliance assigns a client one of the addresses from this pool to use for a given length of time. These addresses are the local, untranslated addresses for the directly connected network. The address pool must be on the same subnet as the adaptive security appliance interface.
Step 2	**dhcpd dns** *dns1* [*dns2*] **Example:** `hostname(config)# dhcpd dns 209.165.201.2 209.165.202.129`	(Optional) Specifies the IP address(es) of the DNS server(s).
Step 3	**dhcpd wins** *wins1* [*wins2*] **Example:** `hostname(config)# dhcpd wins 209.165.201.5`	(Optional) Specifies the IP address(es) of the WINS server(s). You can specify up to two WINS servers.
Step 4	**dhcpd lease** *lease_length* **Example:** `hostname(config)# dhcpd lease 3000`	(Optional) Change the lease length to be granted to the client. This lease equals the amount of time (in seconds) the client can use its allocated IP address before the lease expires. Enter a value between 0 to 1,048,575. The default value is 3600 seconds.
Step 5	**dhcpd domain** *domain_name* **Example:** `hostname(config)# dhcpd domain example.com`	(Optional) Configures the domain name.
Step 6	**dhcpd ping_timeout** *milliseconds* **Example:** `hostname(config)# dhcpd ping timeout 20`	(Optional) Configures the DHCP ping timeout value. To avoid address conflicts, the adaptive security appliance sends two ICMP ping packets to an address before assigning that address to a DHCP client. This command specifies the timeout value for those packets.

	Command	Purpose
Step 7	**dhcpd option 3 ip** *gateway_ip* **Example:** `hostname(config)# dhcpd option 3 ip 10.10.1.1`	(Transparent Firewall Mode) Defines a default gateway that is sent to DHCP clients. If you do not use the DHCP option 3 to define the default gateway, DHCP clients use the IP address of the management interface. The management interface does not route traffic.
Step 8	**dhcpd enable** *interface_name* **Example:** `hostname(config)# dhcpd enable outside`	Enables the DHCP daemon within the adaptive security appliance to listen for DHCP client requests on the enabled interface.

Configuring DHCP Options

You can configure the adaptive security appliance to send information for the DHCP options listed in RFC 2132. The DHCP options include the following three categories:

- Options that Return an IP Address, page 8-4
- Options that Return a Text String, page 8-4
- Options that Return a Hexadecimal Value, page 8-5

The adaptive security appliance supports all three categories. To configure a DHCP option, choose one of the following commands:

Options that Return an IP Address

Command	Purpose
dhcpd option *code* **ip** *addr_1* [*addr_2*] **Example:** `hostname(config)# dhcpd option 2 ip 10.10.1.1 10.10.1.2`	Configures a DHCP option that returns one or two IP addresses.

Options that Return a Text String

Command	Purpose
dhcpd option *code* **ascii** *text* **Example:** `hostname(config)# dhcpd option 2 ascii examplestring`	Configures a DHCP option that returns a text string.

Options that Return a Hexadecimal Value

Command	Purpose
dhcpd option *code* **hex** *value* **Example:** hostname(config)# dhcpd option 2 hex 22.0011.01.FF1111.00FF.0000.AAAA.1111.1111 .1111.11	Configures a DHCP option that returns a hexadecimal value.

Note The adaptive security appliance does not verify that the option type and value that you provide match the expected type and value for the option code as defined in RFC 2132. For example, you can enter the dhcpd option 46 ascii hello command, and the adaptive security appliance accepts the configuration, although option 46 is defined in RFC 2132 to expect a single-digit, hexadecimal value. For more information about the option codes and their associated types and expected values, see RFC 2132.

Table 8-2 shows the DHCP options that are not supported by the **dhcpd option** command.

Table 8-2 Unsupported DHCP Options

Option Code	Description
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

DHCP options 3, 66, and 150 are used to configure Cisco IP Phones. For more information about configuring these options, see the "Using Cisco IP Phones with a DHCP Server" section on page 8-6.

Using Cisco IP Phones with a DHCP Server

Enterprises with small branch offices that implement a Cisco IP Telephony Voice over IP solution typically implement Cisco CallManager at a central office to control Cisco IP Phones at small branch offices. This implementation allows centralized call processing, reduces the equipment required, and eliminates the administration of additional Cisco CallManager and other servers at branch offices.

Cisco IP Phones download their configuration from a TFTP server. When a Cisco IP Phone starts, if it does not have both the IP address and TFTP server IP address preconfigured, it sends a request with option 150 or 66 to the DHCP server to obtain this information.

- DHCP option 150 provides the IP addresses of a list of TFTP servers.
- DHCP option 66 gives the IP address or the hostname of a single TFTP server.

Note Cisco IP Phones might also include DHCP option 3 in their requests, which sets the default route.

A single request might include both options 150 and 66. In this case, the adaptive security appliance DHCP server provides values for both options in the response if they are already configured on the adaptive security appliance.

You can configure the adaptive security appliance to send information for most options listed in RFC 2132. The following examples show the syntax for any option number, as well as the syntax for options 3, 66, and 150:

Command	Purpose
dhcpd option *number value* **Example:** `hostname(config)# dhcpd option 2`	Provides information for DHCP requests that include an option number as specified in RFC-2132.

Command	Purpose
dhcpd option 66 ascii *server_name* **Example:** `hostname(config)# dhcpd option 66 ascii exampleserver`	Provides the IP address or name of a TFTP server for option 66.

Command	Purpose
dhcpd option 150 ip *server_ip1* [*server_ip2*] **Example:** `hostname(config)# dhcpd option 150 ip 10.10.1.1`	Provides the IP address or names of one or two TFTP servers for option 150. The *server_ip1* is the IP address or name of the primary TFTP server while *server_ip2* is the IP address or name of the secondary TFTP server. A maximum of two TFTP servers can be identified using option 150.

Command	Purpose
dhcpd option 3 ip *router_ip1* **Example:** `hostname(config)# dhcpd option 3 ip 10.10.1.1`	Sets the default route.

Configuring DHCP Relay Services

A DHCP relay agent allows the adaptive security appliance to forward DHCP requests from clients to a router connected to a different interface.

The following restrictions apply to the use of the DHCP relay agent:

- The relay agent cannot be enabled if the DHCP server feature is also enabled.
- DHCP clients must be directly connected to the adaptive security appliance and cannot send requests through another relay agent or a router.
- For multiple context mode, you cannot enable DHCP relay on an interface that is used by more than one context.
- DHCP Relay services are not available in transparent firewall mode. A adaptive security appliance in transparent firewall mode only allows ARP traffic through; all other traffic requires an access list. To allow DHCP requests and replies through the adaptive security appliance in transparent mode, you need to configure two access lists, one that allows DCHP requests from the inside interface to the outside, and one that allows the replies from the server in the other direction.
- When DHCP relay is enabled and more than one DHCP relay server is defined, the adaptive security appliance forwards client requests to each defined DHCP relay server. Replies from the servers are also forwarded to the client until the client DHCP relay binding is removed. The binding is removed when the adaptive security appliance receives any of the following DHCP messages: ACK, NACK, or decline.

Note You cannot enable DHCP Relay on an interface running DHCP Proxy. You must Remove VPN DHCP configuration first or you will see an error message. This error happens if both DHCP relay and DHCP proxy are enabled. Ensure that either DHCP relay or DHCP proxy are enabled, but not both.

To enable DHCP relay, perform the following steps:

	Command	Purpose
Step 1	**dhcprelay server** *ip_address if_name* **Example:** `hostname(config)# dhcprelay server 201.168.200.4`	Set the IP address of a DHCP server on a different interface from the DHCP client. You can use this command up to four times to identify up to four servers.
Step 2	**dhcprelay enable** *interface* **Example:** `hostname(config)# dhcprelay enable inside`	Enables DHCP relay on the interface connected to the clients.

	Command	Purpose
Step 3	**dhcprelay timeout** *seconds* **Example:** `hostname(config)# dhcprelay timeout 25`	(Optional) Set the number of seconds allowed for relay address negotiation.
Step 4	**dhcprelay setroute** *interface_name* **Example:** `hostname(config)# dhcprelay setroute inside`	(Optional) Change the first default router address in the packet sent from the DHCP server to the address of the adaptive security appliance interface. This action allows the client to set its default route to point to the adaptive security appliance even if the DHCP server specifies a different router. If there is no default router option in the packet, the adaptive security appliance adds one containing the interface address.

DHCP Monitoring Commands

To monitor DHCP, enter one of the following commands:

Command	Purpose
show running-config dhcpd	Shows the current DHCP configuration.
show running-config dhcprelay	Shows the current DHCP relay services status.

Feature History for DHCP

Table 8-3 lists the release history for this feature.

Table 8-3 Feature History for DHCP

Feature Name	Releases	Description
DHCP	7.0(1)	This feature was introduced. The following commands were introduced: **dhcp client update dns**, **dhcpd address**, **dhcpd domain**, **dhcpd enable**, **dhcpd lease**, **dhcpd option**, **dhcpd ping timeout**, **dhcpd update dns**, **dhcpd wins**, **dhcp-network-scope**, **dhcprelay enable**, **dhcprelay server**, **dhcprelay setroute**, **dhcprelay trusted**, **dhcp-server**. **show running-config dhcpd**, and **show running-config dhcprelay**.