DHCP and DDNS Services for Threat Defense

The following topics explain DHCP and DDNS services and how to configure them on Threat Defense devices.

About DHCP and DDNS Services

The following topics describe the DHCP server, DHCP relay agent, and DDNS update.

About the DHCPv4 Server

DHCP provides network configuration parameters, such as IP addresses, to DHCP clients. The Firepower Threat Defense device can provide a DHCP server to DHCP clients attached to Firepower Threat Defense device interfaces. The DHCP server provides network configuration parameters directly to DHCP clients.

An IPv4 DHCP client uses a broadcast rather than a multicast address to reach the server. The DHCP client listens for messages on UDP port 68; the DHCP server listens for messages on UDP port 67.

The DHCP server for IPv6 is not supported; you can, however, enable DHCP relay for IPv6 traffic.

DHCP Options

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. The configuration parameters are carried in tagged items that are stored in the Options field of the DHCP message and the data are also called options. Vendor information is also stored in Options, and all of the vendor information extensions can be used as DHCP options.

For example, 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.
- DHCP option 3 sets the default route.

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

You can use advanced DHCP options to provide DNS, WINS, and domain name parameters to DHCP clients; DHCP option 15 is used for the DNS domain suffix.You can also use the DHCP automatic configuration setting to obtain these values or define them manually. When you use more than one method to define this information, it is passed to DHCP clients in the following sequence:

1. Manually configured settings.
2. Advanced DHCP options settings.
3. DHCP automatic configuration settings.

For example, you can manually define the domain name that you want the DHCP clients to receive and then enable DHCP automatic configuration. Although DHCP automatic configuration discovers the domain together with the DNS and WINS servers, the manually defined domain name is passed to DHCP clients with the discovered DNS and WINS server names, because the domain name discovered by the DHCP automatic configuration process is superseded by the manually defined domain name.

About the DHCP Relay Agent

You can configure a DHCP relay agent to forward DHCP requests received on an interface to one or more DHCP servers. DHCP clients use UDP broadcasts to send their initial DHCPDISCOVER messages because they do not have information about the network to which they are attached. If the client is on a network segment that does not include a server, UDP broadcasts normally are not forwarded by the Firepower Threat Defense device because it does not forward broadcast traffic. The DHCP relay agent lets you configure the interface of the Firepower Threat Defense device that is receiving the broadcasts to forward DHCP requests to a DHCP server on another interface.

About DDNS

DDNS update integrates DNS with DHCP. The two protocols are complementary: DHCP centralizes and automates IP address allocation; DDNS update automatically records the association between assigned addresses and hostnames at predefined intervals. DDNS allows frequently changing address-hostname associations to be updated frequently. Mobile hosts, for example, can then move freely on a network without user or administrator intervention. DDNS provides the necessary dynamic update and synchronization of the name-to-address mapping and address-to-name mapping on the DNS server.

The DDNS name and address mapping is held on the DHCP server in two resource records (RRs): the A RR includes the name-to-IP address mapping, while the PTR RR maps addresses to names. Of the two methods for performing DDNS updates—the IETF standard defined by RFC 2136 and a generic HTTP method—the Firepower Threat Defense device supports the IETF method.

Note DDNS is not supported on the BVI or bridge group member interfaces.

DDNS Update Configurations

The two most common DDNS update configurations are the following:

- The DHCP client updates the A RR, while the DHCP server updates the PTR RR.

- The DHCP server updates both the A RR and PTR RR.

In general, the DHCP server maintains DNS PTR RRs on behalf of clients. Clients may be configured to perform all desired DNS updates. The server may be configured to honor these updates or not. The DHCP server must know the fully qualified domain name (FQDN) of the client to update the PTR RR. The client provides an FQDN to the server using a DHCP option called Client FQDN.

UDP Packet Size

DDNS allows DNS requesters to advertise the size of their UDP packets and facilitates the transfer of packets larger than 512 octets. When a DNS server receives a request over UDP, it identifies the size of the UDP packet from the OPT RR and scales its response to contain as many resource records as are allowed in the maximum UDP packet size specified by the requester. The size of the DNS packets can be up to 4096 bytes for BIND or 1280 bytes for the Windows 2003 DNS Server.

Guidelines for DHCP and DDNS Services

This section includes guidelines and limitations that you should check before configuring DHCP and DDNS services.

Firewall Mode

- DHCP Relay is not supported in transparent firewall mode or in routed mode on the BVI or bridge group member interface.
- DHCP Server is supported in transparent firewall mode on a bridge group member interface. In routed mode, the DHCP server is supported on the BVI interface, not the bridge group member interface. The BVI must have a name for the DHCP server to operate.
- DDNS is not supported in transparent firewall mode or in routed mode on the BVI or bridge group member interface.

IPv6

Does not support IPv6 for DHCP server; IPv6 for DHCP relay is supported.

DHCPv4 Server

- The maximum available DHCP pool is 256 addresses.
- You can configure only one DHCP server on each interface. Each interface can have its own pool of addresses to use. 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 service 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.
- Firepower Threat Defense device does not support QIP DHCP servers for use with the DHCP proxy service.
- The relay agent cannot be enabled if the DHCP server is also enabled.

- The DHCP server does not support BOOTP requests.

DHCP Relay

- You can configure a maximum of 10 DHCPv4 relay servers, global and interface-specific servers combined, with a maximum of 4 servers per interface.
- You can configure a maximum of 10 DHCPv6 relay servers. Interface-specific servers for IPv6 are not supported.
- The relay agent cannot be enabled if the DHCP server feature is also enabled.
- DHCP relay services are not available in transparent firewall mode. You can, however, allow DHCP traffic through using an access rule. To allow DHCP requests and replies through the Firepower Threat Defense device, you need to configure two access rules, one that allows DCHP requests from the inside interface to the outside (UDP destination port 67), and one that allows the replies from the server in the other direction (UDP destination port 68).
- For IPv4, clients must be directly-connected to the Firepower Threat Defense device and cannot send requests through another relay agent or a router. For IPv6, the Firepower Threat Defense device supports packets from another relay server.
- The DHCP clients must be on different interfaces from the DHCP servers to which the Firepower Threat Defense device relays requests.
- You cannot enable DHCP Relay on an interface in a traffic zone.

Configure the DHCP Server

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	N/A	FTD	Any	Access Admin Administrator Network Admin

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the FTD device.

Step 2 Select **DHCP > DHCP Server**.

Step 3 Configure the following DHCP server options:

- **Ping Timeout**—The amount of time in milliseconds that Firepower Threat Defense device waits to time out a DHCP ping attempt. Valid values range from 10 to 10000 milliseconds. The default value is 50 milliseconds.

  To avoid address conflicts, the Firepower Threat Defense device sends two ICMP ping packets to an address before assigning that address to a DHCP client.

- **Lease Length**—The amount of time in seconds that the client may use its allocated IP address before the lease expires. Valid values range from 300 to 1048575 seconds. The default value is 3600 seconds (1 hour).
- (Routed mode) **Auto-configuration**—Enables DHCP auto configuration on the Firepower Threat Defense device. Auto-configuration enables the DHCP server to provide the DHCP clients with the DNS server, domain name, and WINS server information obtained from a DHCP client running on the specified interface. Otherwise, you can disable auto configuration and add the values yourself in Step 4.
- (Routed mode) **Interface**—Specifies the interface to be used for auto configuration.

Step 4 To override auto-configured settings, do the following:

- Enter the domain name of the interface. For example, your device may be in the Your_Company domain.
- From the drop-down list, choose the DNS servers (primary and secondary) configured for the interface. To add a new DNS server, see Creating Network Objects.
- From the drop-down list, choose the WINS servers (primary and secondary) configured for the interface. To add a new WINS server, see Creating Network Objects.

Step 5 Select the **Server** tab, click **Add**, and configure the following options:

- **Interface**—Choose the interface from the drop-down list. In transparent mode, specify a named bridge group member interface. In routed mode, specify a named routed interface or a named BVI; do not specify the bridge group member interface. Note that each bridge group member interface for the BVI must also be named for the DHCP server to operate.
- **Address Pool**—The range of IP addresses from lowest to highest that is used by the DHCP server. The range of IP addresses must be on the same subnet as the selected interface and cannot include the IP address of the interface itself.
- **Enable DHCP Server**—Enables the DHCP server on the selected interface.

Step 6 Click **OK** to save the DHCP server configuration.

Step 7 (Optional) Select the **Advanced** tab, click **Add**, and specify the type of information you want the option to return to the DHCP client:

- **Option Code**—The Firepower Threat Defense device supports the DHCP options listed in RFC 2132, RFC 2562, and RFC 5510 to send information. All DHCP options (1 through 255) are supported except for 1, 12, 50–54, 58–59, 61, 67, and 82. See About the DHCPv4 Server, on page 1for more information on DHCP option codes.

  Note The Firepower Threat Defense device 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 more information about option codes and their associated types and expected values, see RFC 2132.

- **Type**—DHCP option type. Available options include **IP**, **ASCII**, and **HEX**. If you chose IP, you must add IP addresses in the IP Address fields. If you chose ASCII, you must add the ASCII value in the ASCII field. If you chose HEX, you must add the HEX value in the HEX field.
- **IP Address 1** and **IP Address 2**—The IP address(es) to be returned with this option code. To add a new IP address, see Creating Network Objects.

- **ASCII**—The ASCII value that is returned to the DHCP client. The string cannot include spaces.
- **HEX**—The HEX value that is returned to the DHCP client. The string must have an even number of digits and no spaces. You do not need to use a 0x prefix.

Step 8 Click **OK** to save the option code configuration.

Step 9 Click **Save** on the DHCP page to save your changes.

Configure the DHCP Relay Agent

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	N/A	FTD	Any	Access Admin Administrator Network Admin

You can configure a DHCP relay agent to forward DHCP requests received on an interface to one or more DHCP servers. DHCP clients use UDP broadcasts to send their initial DHCPDISCOVER messages because they do not have information about the network to which they are attached. If the client is on a network segment that does not include a server, UDP broadcasts normally are not forwarded by the Firepower Threat Defense device because it does not forward broadcast traffic.

You can remedy this situation by configuring the interface of the Firepower Threat Defense device that is receiving the broadcasts to forward DHCP requests to a DHCP server on another interface.

Note DHCP Relay is not supported in transparent firewall mode.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the FTD device.

Step 2 Select **DHCP** > **DHCP Relay**.

Step 3 In the **Timeout** field, enter the amount of time in seconds that the Firepower Threat Defense device waits to time out the DHCP relay agent. Valid values range from 1 to 3600 seconds. The default value is 60 seconds.

The timeout is for address negotiation through the local DHCP Relay agent.

Step 4 On the **DHCP Relay Agent** tab, click **Add**, and configure the following options:

- **Interface**—The interface connected to the DHCP clients.
- **Enable IPv4 Relay**—Enables IPv4 DHCP Relay for this interface.
- **Set Route**—(For IPv4) Changes the default gateway address in the DHCP message from the server to that of the Firepower Threat Defense device interface that is closest to the DHCP client, which relayed the original DHCP request. This action allows the client to set its default route to point to the Firepower

Threat Defense device even if the DHCP server specifies a different router. If there is no default router option in the packet, the Firepower Threat Defense device adds one containing the interface address.

- **Enable IPv6 Relay**—Enables IPv6 DHCP Relay for this interface.

Step 5 Click **OK** to save the DHCP relay agent changes.

Step 6 On the **DHCP Servers** tab, click **Add**, and configure the following options:

Add the IPv4 and IPv6 server addresses as separate entries, even if they belong to the same server.

- **Server**—The IP address of the DHCP server. Chose an IP address from the drop-down list. To add a new one, see Creating Network Objects
- **Interface**—The interface to which the specified DHCP server is attached. The DHCP Relay agent and the DHCP server cannot be configured on the same interface.

Step 7 Click **OK** to save the DHCP server changes.

Step 8 Click **Save** on the DHCP page to save your changes.

Configure DDNS

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	N/A	FTD	Any	Access Admin Administrator Network Admin

Dynamic DNS (DDNS) update integrates DNS with DHCP. DDNS update automatically records the association between assigned addresses and hostnames, which allows frequently changing address-hostname associations to be updated efficiently.

Before you begin

- For overview information, see About DDNS, on page 2.
- DDNS is not supported in transparent firewall mode.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the FTD device.

Step 2 Select **DHCP** > **DDNS**, and configure the following DDNS options:

- **DHCP Client Requests DHCP Server to update Records**—Configures the DHCP client to request that it update the specified records. Available options are **Not Selected**, **No Update**, **Only PTR**, and **Both A and PTR Records**. See About DDNS, on page 2 for a description of A and PTR records.
- **Enable DHCP Client Broadcast**—Enables the DHCP client to use a broadcast address to reach the DHCP server.

- **Dynamic DNS Update**—Which records to update for the DDNS updates for the DHCP server. Available options are **Not Selected**, **Only PTR**, and **Both A and PTR Records** .
- **Override DHCP Client Requests**—Specifies that the DHCP server actions should override any update actions requested by the DHCP client.

Step 3 On the **DHCP Client ID Interface** tab, choose the interface from the **Available Interfaces** list, and then click **Add** to move it to the **Selected Interfaces** list.

Step 4 On the **DDNS Interface Settings** tab, click **Add**, and configure the following options:

- **Interface**—Choose the interface from the drop-down list to add DDNS settings for each configured interface .
- **Method Name**—The DDNS update method assigned to the interface.
- **Host Name**—The host name of the DDNS client.
- **DHCP Client requests DHCP server to update requests**—Configures the DHCP client to request that it update the specified records. Available options are **Not Selected**, **No Update**, **Only PTR**, and **Both A and PTR Records**. See About DDNS, on page 2 for a description of A and PTR records.
- **Dynamic DNS Update**—Which records to update for the DDNS updates for the DHCP server. Available options are **Not Selected**, **Only PTR**, and **Both A and PTR Records** .
- **Override DHCP Client Requests**—Specifies that the DHCP server actions should override any update actions requested by the DHCP client.

Step 5 Click **OK** to save the DDNS interface changes.

Step 6 On the **DDNS Update Methods** tab, click **Add**, and configure the following options:

- **Method Name**—The DDNS update method assigned to the interface.
- **Update Interval**—The update interval in whole numbers between DNS update attempts configured for the update method in days (0 to 364), hours (0 to 23), minutes (0 to 59), and seconds (0 to 59). These units are additive. That is, if you enter 0 days, 0 hours, 5 minutes and 15 seconds, the update method tries an update every 5 minutes and 15 seconds for as long as the method is active.
- **Update Records**—Stores server resource record updates that the DNS client updates. Available options are **Not Defined**, **Both A and PTR Records**, and **A Records**.

Step 7 Click **OK** to save the DDNS update methods changes.

Step 8 Click **Save** on the DHCP page to save your changes.