DHCP and DDNS Services

This chapter describes how to configure the DHCP server or DHCP relay as well as dynamic DNS (DDNS) update methods.

- About DHCP and DDNS Services, on page 1
- Guidelines for DHCP and DDNS Services, on page 3
- Configure the DHCP Server, on page 5
- Configure the DHCP Relay Agent, on page 9
- Configure DDNS, on page 10
- Monitoring DHCP and DDNS Services, on page 11
- History for DHCP and DDNS Services, on page 13

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 ASA can provide a DHCP server to DHCP clients attached to ASA 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.

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 DHCPv6 Stateless Server**

For clients that use StateLess Address Auto Configuration (SLAAC) in conjunction with the Prefix Delegation feature (Enable the IPv6 Prefix Delegation Client), you can configure the ASA to provide information such as the DNS server or domain name when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients.

**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 ASA because it does not forward broadcast traffic. The DHCP relay agent lets you configure the interface of the ASA 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 ASA 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.

Several additional **message-length maximum** commands are available:

- The existing global limit: `message-length maximum 512`
- A client or server specific limit: `message-length maximum client 4096` and `message-length maximum server 4096`
- The dynamic value specified in the OPT RR field: `message-length maximum client auto`

If the three commands are present at the same time, the ASA allows the automatically configured length up to the configured client or server maximum. For all other DNS traffic, the message-length maximum is used.

### Guidelines for DHCP and DDNS Services

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

**Context Mode**

- DHCPv6 stateless server is not supported in multiple context mode.
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.
- DHCPv6 stateless server is not supported in transparent firewall mode or in routed mode on the BVI or bridge group member interface.

Clustering

- DHCPv6 stateless server is not supported with clustering.

IPv6

 supports IPv6 for DHCP stateless server and DHCP Relay.

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.
- ASA 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.

DHCPv6 Server

The DHCPv6 Stateless server cannot be configured on an interface where the DHCPv6 address, Prefix Delegation client, or DHCPv6 relay is configured.

DHCP Relay

- You can configure a maximum of 10 DHCPv4 relay servers in single mode and per context, global and interface-specific servers combined, with a maximum of 4 servers per interface.
- You can configure a maximum of 10 DHCPv6 relay servers in single mode and per context. Interface-specific servers for IPv6 are not supported.
- The relay agent cannot be enabled if the DHCP server feature is also enabled.
Configure the DHCP Server

This section describes how to configure a DHCP server provided by the ASA.

Procedure

Step 1  Enable the DHCPv4 Server, on page 5.
Step 2  Configure Advanced DHCPv4 Options, on page 7.
Step 3  Configure the DHCPv6 Stateless Server, on page 8.

Enable the DHCPv4 Server

To enable the DHCP server on an ASA interface, perform the following steps:

Procedure

Step 1  Choose Configuration > Device Management > DHCP > DHCP Server.
Step 2  Choose an interface, then click Edit.

In transparent mode, choose a bridge group member interface. In routed mode, choose a routed interface or a BVI; do not choose the bridge group member interface.

a) Check the Enable DHCP Server check box to enable the DHCP server on the selected interface.
b) Enter the range of IP addresses from lowest to highest that is used by the DHCP server in the DHCP Address Pool field. 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.
c) Set the following in the Optional Parameters area:
   • The DNS servers (1 and 2) configured for the interface.
   • The WINS servers (primary and secondary) configured for the interface.
The domain name of the interface.

The time in milliseconds that the ASA will wait for an ICMP ping response on the interface.

The duration of time that the DHCP server configured on the interface allows DHCP clients to use an assigned IP address.

The interface on a DHCP client that provides DNS, WINS, and domain name information for automatic configuration if the ASA is acting as a DHCP client on a specified interface (usually outside).

Click Advanced to display the Advanced DHCP Options dialog box to configure more DHCP options. See Configure Advanced DHCPv4 Options, on page 7 for more information.

d) Check the Update DNS Clients check box in the Dynamic Settings for DHCP Server area to specify that in addition to the default action of updating the client PTR resource records, the selected DHCP server should also perform the following update actions:

• Check the Update Both Records check box to specify that the DHCP server should update both the A and PTR RRs.

• Check the Override Client Settings check box to specify that DHCP server actions should override any update actions requested by the DHCP client.

e) Click OK to close the Edit DHCP Server dialog box.

Step 3 (Optional) (Routed mode) Check the Enable Auto-configuration from interface check box in the Global DHCP Options area below the DHCP Server table to enable DHCP auto configuration only if the ASA is acting as a DHCP client on a specified interface (usually outside).

DHCP auto configuration enables the DHCP Server to provide DHCP clients with DNS server, domain name, and WINS server information obtained from a DHCP client that is running on the specified interface. If information obtained through auto configuration is also specified manually in the Global DHCP Options area, the manually specified information takes precedence over the discovered information.

Step 4 Choose the auto-configuration interface from the drop-down list.

Step 5 Check the Allow VPN override check box to override the interface DHCP or PPPoE client WINS parameter with the VPN client parameter.

Step 6 Enter the IP address of the primary DNS server for a DHCP client in the DNS Server 1 field.

Step 7 Enter the IP address of the alternate DNS server for a DHCP client in the DNS Server 2 field.

Step 8 Enter the DNS domain name for DHCP clients (for example, example.com) in the Domain Name field.

Step 9 Enter the amount of time, in seconds, in the Lease Length field 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).

Step 10 Enter the IP address of the primary WINS server for a DHCP client in the Primary WINS Server field.

Step 11 Enter the IP address of the alternate WINS server for a DHCP client in the Secondary WINS Server field.

Step 12 To avoid address conflicts, the ASA sends two ICMP ping packets to an address before assigning that address to a DHCP client. Enter the amount of time, in milliseconds, in the Ping Timeout field that the ASA waits to time out a DHCP ping attempt. Valid values range from 10 to 10000 milliseconds. The default value is 50 milliseconds.

Step 13 Click Advanced to display the Configuring Advanced DHCP Options dialog box to specify additional DHCP options and their parameters. For more information, see Configure Advanced DHCPv4 Options, on page 7.
Step 14 You configure the DDNS update settings for the DHCP server in the Dynamic DNS Settings for DHCP Server area. Check the Update DNS Clients check box to specify that, in addition to the default action of updating the client PTR resource records, the selected DHCP server should also perform the following update actions:

- Check the Update Both Records check box to specify that the DHCP server should update both the A and PTR RRs.
- Check the Override Client Settings check box to specify that the DHCP server actions should override any update actions requested by the DHCP client.

Step 15 Click Apply to save your changes.

Configure Advanced DHCPv4 Options

The ASA 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.

Procedure

Step 1 Choose Configuration > Device Management > DHCP > DHCP Server, then click Advanced.

Step 2 Choose the option code from the drop-down list.

Step 3 Choose the options that you want to configure. Some options are standard. For standard options, the option name is shown in parentheses after the option number and the option parameters are limited to those supported by the option. For all other options, only the option number is shown and you must choose the appropriate parameters to supply with the option. For example, if you choose DHCP Option 2 (Time Offset), you can only enter a hexadecimal value for the option. For all other DHCP options, all of the option value types are available and you must choose the appropriate one.

Step 4 Specify the type of information that the option returns to the DHCP client in the Option Data area. For standard DHCP options, only the supported option value type is available. For all other DHCP options, all of the option value types are available. Click Add to add the option to the DHCP option list. Click Delete to remove the option from the DHCP option list.

- Click IP Address to indicate that an IP address is returned to the DHCP client. You can specify up to two IP addresses. IP Address 1 and IP Address 2 indicate an IP address in dotted-decimal notation.

  Note The name of the associated IP address fields can change based on the DHCP option that you chose. For example, if you choose DHCP Option 3 (Router), the fields names change to Router 1 and Router 2.

- Click ASCII to specify that an ASCII value is returned to the DHCP client. Enter an ASCII character string in the Data field. The string cannot include spaces.

  Note The name of the associated Data field can change based on the DHCP option that you chose. For example, if you choose DHCP Option 14 (Merit Dump File), the associated Data field names change to File Name.

- Click Hex to specify that a hexadecimal value is returned to the DHCP client. Enter a hexadecimal string with an even number of digits and no spaces in the Data field. You do not need to use a 0x prefix.
The name of the associated Data field can change based on the DHCP option you chose. For example, if you choose DHCP Option 2 (Time Offset), the associated Data field becomes the Offset field.

**Step 5**  
Click **OK** to close the Advanced DHCP Options dialog box.

**Step 6**  
Click **Apply** to save your changes.

---

## Configure the DHCPv6 Stateless Server

For clients that use StateLess Address Auto Configuration (SLAAC) in conjunction with the Prefix Delegation feature (Enable the IPv6 Prefix Delegation Client), you can configure the ASA to provide information such as the DNS server or domain name when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients.

**Before you begin**

This feature is only supported in single, routed mode. This feature is not supported in clustering.

**Procedure**

**Step 1**  
Configure the IPv6 DHCP pool that contains the information you want the DHCPv6 server to provide:

a) Choose **Configuration > Device Management > DHCP > DHCP Pool**, and click **Add**.

b) In the **DHCP Pool Name** field, enter a name.

c) For each parameter on each tab, either check the **Import** check box or manually enter a value in the field and click **Add**.

   The **Import** option uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface. You can mix and match manually-configured parameters with imported parameters; however, you cannot configure the same parameter manually and also specify **Import**.

   d) Click **OK**, and then **Apply**.

**Step 2**  
Choose **Configuration > Device Setup > Interface Settings > Interfaces**.

**Step 3**  
Choose an interface, and click **Edit**.

The **Edit Interface** dialog box appears with the **General** tab selected.

**Step 4**  
Click the **IPv6** tab.

**Step 5**  
In the **Interface IPv6 DHCP** area, click the **Server DHCP Pool Name** radio button, and enter the IPv6 DHCP pool name.

**Step 6**  
Check the **Hosts should use DHCP for non-address config** check box to set the Other Address Config flag in the IPv6 router advertisement packet.

This flag informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain additional information from DHCPv6, such as the DNS server address.

**Step 7**  
Click **OK**.

You return to the **Configuration > Device Setup > Interface Settings > Interfaces** pane.
Configure the DHCP Relay Agent

When a DHCP request enters an interface, the DHCP servers to which the ASA relays the request depends on your configuration. You may configure the following types of servers:

- Interface-specific DHCP servers—When a DHCP request enters a particular interface, then the ASA relays the request only to the interface-specific servers.
- Global DHCP servers—When a DHCP request enters an interface that does not have interface-specific servers configured, the ASA relays the request to all global servers. If the interface has interface-specific servers, then the global servers are not used.

Procedure

Step 1 Choose Configuration > Device Management > DHCP > DHCP Relay.

Step 2 Check the check boxes for the services you want for each interface in the DHCP Relay Agent area.

  - IPv4 > DHCP Relay Enabled.

  - IPv4 > Set Route—Changes the default gateway address in the DHCP message from the server to that of the ASA 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 ASA even if the DHCP server specifies a different router. If there is no default router option in the packet, the ASA adds one containing the interface address.

  - IPv6 > DHCP Relay Enabled.

  - Trusted Interface—Specifies a DHCP client interface that you want to trust. You can configure interfaces as trusted interfaces to preserve DHCP Option 82. DHCP Option 82 is used by downstream switches and routers for DHCP snooping and IP Source Guard. Normally, if the ASA DHCP relay agent receives a DHCP packet with Option 82 already set, but the giaddr field (which specifies the DHCP relay agent address that is set by the relay agent before it forwards the packet to the server) is set to 0, then the ASA will drop that packet by default. You can now preserve Option 82 and forward the packet by identifying an interface as a trusted interface. You can alternatively trust all interfaces by checking the Set dhcp relay information as trusted on all interfaces check box.

Step 3 Add one or more DHCP servers to which DHCP requests are relayed in the Global DHCP Relay Servers area,

  a) Click Add. The Add Global DHCP Relay Server dialog box appears.

  b) Enter the IPv4 or IPv6 address of the DHCP server in the DHCP Server field.

  c) Choose the interface to which the specified DHCP server is attached from the Interface drop-down list.

  d) Click OK.

  The newly added global DHCP relay server appears in the Global DHCP Relay Servers list.

Step 4 (Optional) In the IPv4 Timeout field, enter the amount of time, in seconds, allowed for DHCPv4 address handling. Valid values range from 1 to 3600 seconds. The default value is 60 seconds.
Configure DDNS

To configure dynamic DNS and update the DNS server, perform the following steps:

Procedure

Step 1 Choose Configuration > Device Management > DNS > Dynamic DNS.
Step 2 Click Add to display the Add Dynamic DNS Update Method dialog box.
Step 3 Enter the name for the DDNS update method.
Step 4 Specify the update interval between DNS update attempts configured for the update method in days, hours, minutes, and seconds.
  • Choose the number of days between update attempts from 0 to 364.
  • Choose the number of hours (in whole numbers) between update attempts from 0 to 23.
  • Choose the number of minutes (in whole numbers) between update attempts from 0 to 59.
  • Choose the number of seconds (in whole numbers) between update attempts from 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.

Step 5 Choose one of the following options to store server resource record updates that the DNS client updates:
  • Both the A resource record and the PTR resource record.
  • The A resource records only.
Step 6  Click **OK** to close the Add Dynamic DNS Update Method dialog box.

The new dynamic DNS client settings appear.

**Note**  When you edit an existing method, the Name field is *display-only* and shows the name of the selected method for editing.

Step 7  Click **Add** to display the Add Dynamic DNS Interface Settings dialog box to add DDNS settings for each interface configured.

Step 8  Choose the interface from the drop-down list.

Step 9  Choose the update method assigned to the interface from the drop-down list.

Step 10 Enter the hostname of the DDNS client.

Step 11 Choose one of the following options to store resource record updates:

- Default (PTR Records) to specify that the client request PTR record updating by the server.
- Both (PTR Records and A Records) to specify that the client request both the A and PTR DNS resource records by the server.
- None to specify that the client request no updates by the server.

**Note**  DHCP must be enabled on the selected interface for this action to take effect.

Step 12  Click **OK** to close the Add Dynamic DNS Interface Settings dialog box.

The new dynamic DNS interface settings appear.

Step 13  Click **Apply** to save your changes, or click **Reset** to discard them and enter new ones.

---

**Monitoring DHCP and DDNS Services**

This section includes the procedures to monitor both DHCP and DDNS services.

**Monitoring DHCP Services**

- **Monitoring > Interfaces > DHCP > DHCP Client Lease Information.**
  
  This pane displays configured DHCP client IP addresses.

- **Monitoring > Interfaces > DHCP > DHCP Server Table**
  
  This pane displays configured dynamic DHCP client IP addresses.

- **Monitoring > Interfaces > DHCP > DHCP Statistics**
  
  This pane displays DHCPv4 message types, counters, values, directions, messages received, and messages sent.

- **Monitoring > Interfaces > DHCP > IPV6 DHCP Relay Statistics**
  
  This pane displays DHCPv6 Relay message types, counters, values, directions, messages received, and messages sent.
• **Monitoring > Interfaces > DHCP > IPV6 DHCP Relay Binding**

  This pane displays DHCPv6 Relay bindings.

• **Monitoring > Interfaces > DHCP > IPV6 DHCP Interface Statistics**

  This screen displays DHCPv6 information for all interfaces. If the interface is configured for DHCPv6 stateless server configuration (see [Configure the DHCPv6 Stateless Server](#), on page 8), this screen lists the DHCPv6 pool that is being used by the server. If the interface has DHCPv6 address client or Prefix Delegation client configuration, this screen shows the state of each client and the values received from the server. This screen also shows message statistics for the DHCP server or client.

• **Monitoring > Interfaces > DHCP > IPV6 DHCP HA Statistics**

  This screen shows the transaction statistics between failover units, including how many times the DUID information was synced between the units.

• **Monitoring > Interfaces > DHCP > IPV6 DHCP Server Statistics**

  This screen shows the DHCPv6 stateless server statistics.

---

**Monitoring DDNS Status**

See the following commands for monitoring DDNS status. Enter the commands on **Tools > Command Line Interface**.

- **show running-config ddns**

  This command shows the current DDNS configuration.

- **show running-config dns server-group**

  This command shows the current DNS server group status.
# History for DHCP and DDNS Services

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
</table>
| IPv6 DHCP    | 9.6(2)            | The ASA now supports the following features for IPv6 addressing:  
  • DHCPv6 Address client—The ASA obtains an IPv6 global address and optional default route from the DHCPv6 server.  
  • DHCPv6 Prefix Delegation client—The ASA obtains delegated prefix(es) from a DHCPv6 server. The ASA can then use these prefixes to configure other ASA interface addresses so that Stateless Address Auto Configuration (SLAAC) clients can autoconfigure IPv6 addresses on the same network.  
  • BGP router advertisement for delegated prefixes  
  • DHCPv6 stateless server—The ASA provides other information such as the domain name to SLAAC clients when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients.  

We added or modified the following screens:  
**Configuration > Device Setup > Interface Settings > Interfaces > Add Interface > IPv6**  
**Configuration > Device Management > DHCP > DHCP Pool**  
**Configuration > Device Setup > Routing > BGP > IPv6 Family > Networks**  
**Monitoring > interfaces > DHCP**  

| DHCPv6 monitoring | 9.4(1) | You can now monitor DHCP statistics for IPv6 and DHCP bindings for IPv6.  
We introduced the following screens: DHCPv6 monitoring  
Monitoring > Interfaces > DHCP > IPv6 DHCP Statistics, Monitoring > Interfaces > DHCP > IPv6 DHCP Binding.  

| DHCP Relay server validates the DHCP Server identifier for replies | 9.2(4)/9.3(3) | If the ASA DHCP relay server receives a reply from an incorrect DHCP server, it now verifies that the reply is from the correct server before acting on the reply. We did not introduce or modify any commands. We did not modify any ASDM screens.  
We did not modify any ASDM screens.  

| DHCP rebind function | 9.1(4) | During the DHCP rebind phase, the client now tries to rebind to other DHCP servers in the tunnel group list. Before this release, the client did not rebind to an alternate server when the DHCP lease fails to renew.  
We did not modify any ASDM screens. |
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP trusted interfaces</td>
<td>9.1(2)</td>
<td>You can now configure interfaces as trusted interfaces to preserve DHCP Option 82. DHCP Option 82 is used by downstream switches and routers for DHCP snooping and IP Source Guard. Normally, if the ASA DHCP relay agent receives a DHCP packet with Option 82 already set, but the giaddr field (which specifies the DHCP relay agent address that is set by the relay agent before it forwards the packet to the server) is set to 0, then the ASA will drop that packet by default. You can now preserve Option 82 and forward the packet by identifying an interface as a trusted interface. We modified the following screen: Configuration &gt; Device Management &gt; DHCP &gt; DHCP Relay.</td>
</tr>
<tr>
<td>DHCP relay servers per interface (IPv4 only)</td>
<td>9.1(2)</td>
<td>You can now configure DHCP relay servers per-interface, so requests that enter a given interface are relayed only to servers specified for that interface. IPv6 is not supported for per-interface DHCP relay. We modified the following screen: Configuration &gt; Device Management &gt; DHCP &gt; DHCP Relay.</td>
</tr>
<tr>
<td>DHCP relay for IPv6 (DHCPv6)</td>
<td>9.0(1)</td>
<td>DHCP relay support for IPv6 was added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We modified the following screen: Configuration &gt; Device Management &gt; DHCP &gt; DHCP Relay.</td>
</tr>
<tr>
<td>DDNS</td>
<td>7.0(1)</td>
<td>We introduced this feature. We introduced the following screens: Configuration &gt; Device Management &gt; DNS &gt; DNS Client. Configuration &gt; Device Management &gt; DNS &gt; Dynamic DNS.</td>
</tr>
<tr>
<td>DHCP</td>
<td>7.0(1)</td>
<td>The ASA can provide a DHCP server or DHCP relay services to DHCP clients attached to ASA interfaces. We introduced the following screens: Configuration &gt; Device Management &gt; DHCP &gt; DHCP Relay. Configuration &gt; Device Management &gt; DHCP &gt; DHCP Server.</td>
</tr>
</tbody>
</table>