



CHAPTER 9

DHCP and DNS Services

A DHCP server provides network configuration parameters, such as IP addresses, to DHCP clients. The security appliance can provide DHCP server or DHCP relay services to DHCP clients attached to 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.

The Domain Name System (DNS) is the system in the Internet that maps names of objects (usually host names) into IP numbers or other resource record values. The namespace of the Internet is divided into domains, and the responsibility for managing names within each domain is delegated, typically to systems within each domain. DNS client services allows you to specify DNS servers to which the security appliance sends DNS requests, request timeout period, and other parameters.

Dynamic DNS (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 host names at pre-defined intervals. DDNS allows frequently changing address-host name associations to be updated frequently. Mobile hosts, for example, can then move freely on a network without user or administrator intervention.

For information about configuring these services, see the following topics:

- [DHCP Relay](#)
- [DHCP Server](#)
- [DNS Client](#)
- [Dynamic DNS](#)

DHCP Relay

The DHCP Relay pane lets you configure DHCP relay services on the security appliance. DHCP relay passes DHCP requests received on one interface to an external DHCP server located behind a different interface. To configure DHCP relay, you need to specify at least one DHCP relay server and then enable a DHCP relay agent on the interface receiving DHCP requests.

Restrictions

- You cannot enable a DHCP relay agent on an interface that has a DHCP relay server configured for it.
- The DHCP relay agent works only with external DHCP servers; it will not forward DHCP requests to a security appliance interface configured as a DHCP server.

Prerequisites

Before you can enable a DHCP relay agent on an interface, you must have at least one DHCP relay server in the configuration.

Fields

- DHCP Relay Agent—*Display only*. Contains the fields for configuring the DHCP relay agent.
 - Interface—Displays the interface ID. Double-clicking an interface opens the Edit DHCP Relay Agent Settings dialog box, where you can enable the DHCP relay agent and configure the relay agent parameters.
 - DHCP Relay Enabled—Indicates whether the DHCP relay agent is enabled on the interface. This column displays “Yes” if the DHCP relay agent is enabled or “No” if the DHCP relay agent is not enabled on the interface.
 - Set Route—Indicates whether the DHCP relay agent is configured to modify the default router address in the information returned from the DHCP server. This column display “Yes” if the DHCP relay agent is configured to change the default router address to the interface address or “No” if the DHCP relay agent does not modify the default router address.
 - Edit—Opens the Edit DHCP Relay Agent Settings dialog box, where you can enable the DHCP relay agent and configure the relay agent parameters.
- DHCP Relay Server—Contains the fields for configuring the DHCP relay servers.
 - Timeout—Specifies the amount of time, in seconds, allowed for DHCP address negotiation. Valid values range from 1 to 3600 seconds. The default value is 60 seconds.
 - Server—*Display only*. Displays the IP address of a configured, external DHCP server. Double-clicking a server address opens the DHCP Relay - Edit DHCP Server dialog box, where you can edit the DHCP relay server settings.
 - Interface—*Display only*. Display the interface the specified DHCP server is attached to.
 - Add—Opens the DHCP Relay - Add DHCP Server dialog box, where you can specify a new DHCP relay server. You can define up to 4 DHCP relay servers on the security appliance. This button is unavailable if you already have 4 DHCP relay servers defined.
 - Edit—Opens the DHCP Relay - Edit DHCP Server dialog box, where you can edit the DHCP relay server settings.
 - Delete—Removes the selected DHCP relay server. The server is removed from the security appliance configuration when you apply or save your changes.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Edit DHCP Relay Agent Settings

You can enable the DHCP relay agent and configure the relay agent parameters for the selected interface in the Edit DHCP Relay Agent Settings dialog box.

Restrictions

- You cannot enable a DHCP relay agent on an interface that has a DHCP relay server configured for it.
- You cannot enable a DHCP relay agent on a security appliance that has DHCP server configured on an interface.

Prerequisites

Before you can enable a DHCP relay agent on an selected interface, you must have at least one DHCP relay server in the configuration.

Fields

- Enable DHCP Relay Agent—When checked, enables the DHCP relay agent on the selected interface. You must have a DHCP relay server defined before enabling the DHCP relay agent.
- Set Route—Specifies whether the DHCP relay agent is configured to modify the default router address in the information returned from the DHCP server. When this check box is checked, the DHCP relay agent substitutes the address of the selected interface for the default router address in the information returned from the DHCP server.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

DHCP Relay - Add/Edit DHCP Server

Define new DHCP relay servers in the DHCP Relay - Add DHCP Server dialog box or edit exiting server information in the DHCP Relay - Edit DHCP Server dialog box. You can define up to 4 DHCP relay servers.

Restrictions

You cannot define a DHCP relay server on an interface with a DHCP server enabled on it.

Fields

- DHCP Server—Specifies the IP address of the external DHCP server to which DHCP requests are forwarded.
- Interface—Specifies the interface through which DHCP requests are forwarded to the external DHCP server.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

DHCP Server

The DHCP Server pane lets you configure the security appliance interfaces as DHCP servers. You can configure one DHCP server per interface on the security appliance.



Note

You cannot configure a DHCP server on an interface that has DHCP relay configured on it. For more information about DHCP relay, see [DHCP Relay](#).

Fields

- **Interface**—*Display only*. Displays the interface ID. Double-clicking an interface ID opens the Edit DHCP Server dialog box, where you can enable DHCP on and assign a DHCP address pool to the selected interface.
- **DHCP Enabled**—*Display only*. Indicates whether DHCP is enabled on the interface. This column displays “Yes” if DHCP is enabled or “No” if DHCP is not enabled on the interface.
- **Address Pool**—*Display only*. Displays the range of IP addresses assigned to the DHCP address pool.
- **DNS Servers**—*Display only*. Displays the DNS servers configured for the interface.
- **WINS Servers**—*Display only*. Displays the WINS servers configured for the interface.
- **Domain Name**—*Display only*. Displays the domain name of the interface.
- **Ping Timeout**—*Display only*. Displays time in milliseconds that the security appliance will wait for an ICMP ping response on the interface.
- **Lease Length**—*Display only*. Displays the duration of time that the DHCP server configured on the interface allows DHCP clients to use the an assigned IP address.
- **Auto Interface**—*Display only*. Displays the interface on a DHCP client providing DNS, WINS, and domain name information for automatic configuration.
- **Options**—*Display only*. Displays advanced DHCP options configured for the interface.
- **Dynamic DNS Settings**—*Display only*. Displays
- **Edit**—Opens the Edit DHCP Server dialog box for the selected interface. You can enable DHCP and specify the DHCP address pool in the Edit DHCP Server dialog box.
- **Other DHCP Options**—Contains optional DHCP parameters.
 - **Enable Autoconfiguration on interface**—Check to enable DHCP auto configuration and select the interface from the menu.

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

- DNS Server 1—(Optional) Specifies the IP address of the primary DNS server for a DHCP client.
- DNS Server 2—(Optional) Specifies the IP address of the alternate DNS server for a DHCP client.
- Domain Name—(Optional) Specifies the DNS domain name for DHCP clients. Enter a valid DNS domain name, for example example.com.
- Lease Length—(Optional) Specifies the amount of time, in seconds, that the client can 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).
- Primary WINS Server—(Optional) Specifies the IP address of the primary WINS server for a DHCP client.
- Secondary WINS Server—(Optional) Specifies the IP address of the alternate WINS server for a DHCP client.
- Ping Timeout—(Optional) To avoid address conflicts, the security appliance sends two ICMP ping packets to an address before assigning that address to a DHCP client. The Ping Timeout field specifies the amount of time, in milliseconds, that the security appliance waits to time out a DHCP ping attempt. Valid values range from 10 to 10000 milliseconds. The default value is 50 milliseconds.
- Advanced—Opens the [Advanced DHCP Options](#) dialog box, where you can specify DHCP options and their parameters.
- Dynamic DNS Settings for DHCP Server—In this area, you can configure the DDNS update settings for the DHCP server.
 - Update DNS Clients—Check to specify that, besides the default action of updating the client PTR resource records, the DHCP server should also perform the following update actions (if selected):
 - Update Both Records—Check to specify that the DHCP server should update both the A and PTR RRs.
 - Override Client Settings—Check to specify that the DHCP server actions should override any update actions requested by the DHCP client.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Edit DHCP Server

You can enable DHCP and specify the DHCP address pool for the selected interface in the Edit DHCP Server dialog box.

Fields

- **Enable DHCP Server**—Check this check box to enable the DHCP server on the selected interface. Uncheck this check box to disable DHCP on the selected interface. Disabling the DHCP server on the selected interface does not clear the specified DHCP address pool.
- **DHCP Address Pool**—Enter the IP address pool used by the DHCP server. Enter the range of IP addresses from lowest to highest. The range of IP addresses must be on the same subnet as the selected interface and cannot contain the IP address of the interface itself.
- **Optional Parameters**—You can optionally configure the following parameters for the DHCP server:
 - **DNS Server 1**—Enter the IP address of the primary DNS server for a DHCP client.
 - **DNS Server 2**— Enter the IP address of the alternate DNS server for a DHCP client.
 - **Domain Name**—Enter the DNS domain name for DHCP clients. Enter a valid DNS domain name, for example example.com.
 - **Lease Length**—Enter the amount of time, in seconds, that the client can 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).
 - **Primary WINS Server**—Enter the IP address of the primary WINS server for a DHCP client.
 - **Secondary WINS Server**—Enter the IP address of the alternate WINS server for a DHCP client.
 - **Ping Timeout**—Enter the amount of time, in milliseconds, that the security appliance waits to time out a DHCP ping attempt. Valid values range from 10 to 10000 milliseconds. The default value is 50 milliseconds.
 - **Enable Autoconfiguration on interface**—Check to enable DHCP auto configuration and select the interface from the menu.
 - **Advanced**—Opens the [Advanced DHCP Options](#) dialog box, where you can specify DHCP options and their parameters.
- **Dynamic DNS Settings for DHCP Server**—In this area, you can configure the DDNS update settings for the DHCP server.
 - **Update DNS Clients**—Check to specify that, besides the default action of updating the client PTR resource records, the DHCP server should also perform the following update actions (if selected):
 - **Update Both Records**—Check to specify that the DHCP server should update both the A and PTR RRs.
 - **Override Client Settings**—Check to specify that DHCP server actions should override any update actions requested by the DHCP client.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Advanced DHCP Options

The Advanced DHCP Options dialog box lets you configure DHCP option parameters. You use DHCP options to provide additional information to DHCP clients. For example, DHCP option 150 and DHCP option 66 provide TFTP server information to Cisco IP Phones and Cisco IOS routers.

You can use that advanced DHCP options to provide DNS, WINS, and domain name parameters to DHCP clients. You can also use the DHCP auto configuration setting to obtain these values or manually specify them on the [DHCP Server](#) pane. When you use more than one method to specify this information, the information is passed to DHCP clients with the following preference:

1. Manually configured settings.
2. Advanced DHCP Options settings.
3. DHCP auto configuration.

For example, you can manually define the domain name that you want the DHCP clients to receive, and then enable DHCP auto configuration. Although DHCP auto configuration will discover the domain along with the DNS and WINS servers, the manually-defined domain name is passed to DHCP clients with the discovered DNS and WINS server names. The domain name discovered by the DHCP auto configuration process is discarded in favor of the manually-defined domain name.

Fields

- Option to be Added—Contains the fields used to configure a DHCP option.
 - Choose the option code—Lists the available option codes. All DHCP options (options 1 through 255) are supported except 1, 12, 50–54, 58–59, 61, 67, and 82. Choose the option 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 standard DHCP options, only the supported option value type is available. For example, if you choose DHCP Option 2 (Time Offset), you can only supply 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 options value type.
- Option Data—These options specify the type of information the option returns to the DHCP client. 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.
- IP Address—Choosing this value specifies that an IP address is returned to the DHCP client. You can specify up to two IP addresses.



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

- IP Address 1—An IP address in dotted-decimal notation.
- IP Address 2—(Optional) An IP address in dotted-decimal notation.
- ASCII—Choose this option specifies that an ASCII value is returned to the DHCP client.



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

- Data—An ASCII character string. The string cannot include white space.
- Hex—Selecting this option specifies that a hexadecimal value is returned to the DHCP client.



Note 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.

- Data—A hexadecimal string with an even number of digits and no spaces. You do not need to use a 0x prefix.
- Add—Adds the configured option to the DHCP option table.
- Delete—Removes the selected option from the DHCP option table.
- DHCP option table—Lists the DHCP options that have been configured.
 - Option Code—Shows the DHCP option code. For standard DHCP options, the option name appears in parentheses next to the option code.
 - Option Data—Shows the parameters that have been configured for the selected option.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

DNS Client

The DNS Client pane shows the DNS server groups and DNS lookup information for the security appliance, so it can resolve server names to IP addresses in your WebVPN configuration or certificate configuration. Other features that define server names (such as AAA) do not support DNS resolution. In those cases, you must enter the IP address or manually resolve the name to an IP address by adding the server name in the Network Objects/Groups pane.

Fields

- DNS Server Groups—Displays and manages the DNS server list. There can be up to six addresses to which DNS requests can be forwarded. The security appliance tries each DNS server in order until it receives a response. You must enable DNS on at least one interface in the DNS Lookup area before you can add a DNS server. The contents of the table in this area are as follows:
 - Name—*Display only*. Shows the name of each configured DNS server group.
 - Servers—*Display only*. Shows the IP addresses of the configured servers.
 - Timeout—*Display only*. Shows the number of seconds to wait before trying the next DNS server in the list, between 1 and 30 seconds. The default is 2 seconds. Each time the security appliance retries the list of servers, this timeout doubles.
 - Retries—*Display only*. Shows the number of seconds to wait before trying the next DNS server in the list.
 - Domain Name—*Display only*. Shows the number of times the security appliance retries the request.
- DNS Lookup—Enables or disables DNS lookup on an interface.
 - Interface—*Display only*. Lists all interface names.
 - DNS Enabled—*Display only*. Shows whether an interface supports DNS lookup, Yes or No.
 - Disable—Disables DNS lookup for the selected interface.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit DNS Server Group

The Add or Edit DNS Server Group pane lets you specify or modify one or more DNS servers for the security appliance so it can resolve server names to IP addresses in your WebVPN configuration or certificate configuration (See [Add/Edit Trustpoint Configuration > Enrollment Settings Tab](#) and [Add/Edit Trustpoint Configuration > CRL Retrieval Policy Tab](#)). Other features that define server names (such as AAA) do not support DNS resolution. For those, you must enter the IP address or manually resolve the name to an IP address by adding the server name in the Network Objects/Groups pane.

Fields

- Name—Specifies the server name. For the Edit function, this field is *Display only*.
- DNS Servers—Manages the DNS server list. You can specify up to six addresses to which DNS requests can be forwarded. The security appliance tries each DNS server in order until it receives a response. You must enable DNS on at least one interface in the DNS Lookup area before you can add a DNS server.
 - Server to be Added—Specifies the DNS server IP address.
 - Add—Adds a DNS server to the bottom of the list.
 - Delete—Deletes the selected DNS server from the list.
 - Servers—*Display only*. Shows the DNS server list.
 - Move Up—Moves the selected DNS server up the list.
 - Move down—Moves the selected DNS server down the list.
- Timeout—Specifies the number of seconds to wait before trying the next DNS server in the list, between 1 and 30 seconds. The default is 2 seconds. Each time the security appliance retries the list of servers, this timeout doubles.
- Retries—Sets the number of times the security appliance retries the request. The range is 1 through 10 retries.
- Domain Name—(Optional) Specifies the DNS domain name for the server. Enter a valid DNS domain name; for example example.com.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Dynamic DNS

Dynamic DNS provides address and domain name mappings so hosts can find each other even though their DHCP-assigned IP addresses change frequently. The DDNS name and address mappings are held on the DHCP server in two resource records: the A RR contains 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 security appliance supports the IETF method in this release.

The Dynamic DNS pane shows the configured DDNS update methods and the interfaces configured for DDNS. By automatically records the association between assigned addresses and host names at pre-defined intervals, DDNS allows frequently changing address-host name associations to be updated frequently. Mobile hosts, for example, can then move freely on a network without user or administrator intervention.

Fields

- Update Methods—Lists the DDNS update methods that are configured on the security appliance. This table includes:
 - Method Name—*Display only*. Shows the user-defined name for the DDNS update method.
 - Interval—*Display only*. Shows the time between DNS update attempts configured for the update method.
 - Update DNS Server Records—*Display only*. Shows whether the method updates both the A resource record (name to IP address) and the PTR resource record (IP address to name), or neither record.
 - Add/Edit—Displays the Add/Edit Dynamic DNS Update Methods dialog box.
 - Delete—Removes the currently selected update method from the table.
- Dynamic DNS Interface Settings—Lists the DDNS settings for each interface configured for DDNS.
 - Interface—*Display only*. Shows the names of the security appliance interfaces configured for DDNS.
 - Method Name—*Display only*. Shows the update methods assigned to each interface.
 - Hostname—*Display only*. Shows the hostname of the DDNS client.
 - Update DHCP Server Records—*Display only*. Shows whether the interface updates both the A and PTR resource records or neither.
 - Add/Edit—Displays the Add/Edit Dynamic DNS Interface Settings dialog box.
 - Delete—Removes the DDNS update settings for the selected interface.
- DHCP Clients Update DNS Records—This is the global setting specifying which records the DHCP client requests to be updated by the DHCP server. Click one of the following radio buttons:
 - Default (PTR Records) to specify that the client request PTR record updating by the server
 - or–
 - Both (PTR Records and A Records) to specify that the client request both the A and PTR DNS resource records by the server
 - or–
 - None to specify that the client request no updates by the server

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Add/Edit Dynamic DNS Update Methods

The Add/Edit Dynamic DNS Update Methods dialog box lets you add a new method or edit a previously added method. You can specify the method name (if adding a method), specify the interval between DDNS update attempts, and specify whether the DDNS client attempts to update both or neither of the two DNS records, the A record and the PTR record.

Fields

- Name—If you are adding a method, enter then name of the new method in this field. If you are editing an existing method, this field is *display-only* and shows the name of the method selected for editing.
- Update Interval—Specifies the time to elapse between update attempts. The interval ranges from 0 to nearly one year.
 - Days—Choose the number of days between update attempts from 0 to 364.
 - Hours—Choose the number of hours (in whole numbers) between update attempts from 0 to 23.
 - Minutes—Choose the number of minutes (in whole numbers) between update attempts from 0 to 59.
 - Seconds—Choose the number of minutes (in whole numbers) between update attempts from 0 to 59.
 - Update Records—Click Both (A and PTR Records) for the client to attempt updates to both the A and PTR DNS resource records, or click A Records Only to update just the A records. This is the individual method setting for DNS server records updated by the client.

These units are additive. That is, if you enter 0 days, 0 hours, 5 minutes and 15 seconds, the update method will attempt an update every 5 minutes and 15 seconds for as long as the method is active.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Add/Edit Dynamic DNS Interface Settings

The Add/Edit Dynamic DNS Interface Settings allows you to configure DDNS on a security appliance interface. You can assign an update method, specify the hostname, and configure DHCP server updating of both the A and PTR records by the client or neither.

Fields

- Interface—Choose an interface on which to configure DDNS from the menu.
- Update Method—Choose an available DDNS update method from the menu.
- Hostname—Enter the hostname of the DDNS client.

- DHCP Client—This area allows you to specify that the DHCP client updates both the A and PTR DNS records or neither. This interface setting overrides the global setting at Configuration > Properties > DNS > Dynamic DNS
- DHCP Client Updates DNS Records—Click one of the following radio buttons:
 - Default (PTR Records only) to specify that the client request only PTR record updating by the server
 - or–
 - Both (PTR Records and A Records) to specify that the client request both the A and PTR DNS resource records by the server
 - or–
 - 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 be effective.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

