Configuring Server Access Settings on Firewall Devices

The Server Access section contains pages for configuring server access on firewall devices; Server Access is under Device Admin in the Device or Policy selector.

This chapter contains the following topics:

AUS Page

The AUS page lets you configure remote updating of a security appliance from a server that supports the Auto Update specification. Auto Update applies configuration changes and software updates to the appliance automatically from the remote server.

Note The server you identify on this page must be the same server you identify in the Auto Update section of the Device Properties (from the Tools menu, choose Device Properties). The Device Properties information identifies the AUS server to which Security Manager sends configuration updates, whereas the information on this page defines for the server the device will contact for updates. Also, the Device Identity you provide in the Device Properties must match the Device ID on this page.

If you change AUS servers, note that the device will continue to use the AUS server defined in its current configuration until it receives a new configuration. Thus, you should change the AUS policy but deploy the configuration using the previous AUS server. After deployment is successful, change the Device Properties to point to the new server. For more information on deploying to AUS, see Deploying Configurations Using an Auto Update Server or CNS Configuration Engine.

Navigation Path

- (Device view) Select **Platform > Device Admin > Server Access > AUS** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Server Access > AUS** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- Add and Edit Auto Update Server Dialog Boxes , on page 3

Field Reference

Table 1: AUS Page

Element	Description
Auto Update Servers table	This table lists currently configured Auto Update servers. Use the buttons below the table to manage these entries. The entries are listed in order of precedence for contacting AUS servers. Use the Up and Down arrow buttons to change the ordering of the list by moving the selected entry up or down. Use the Add Row, Edit Row, and Delete Row buttons to add, edit or delete entries. Add Row opens the Add Auto Update Server dialog box, while Edit Row opens the Edit Auto Update Server dialog box for the selected row. See Add and Edit Auto Update Server Dialog Boxes , on page 3 for information about these dialog boxes. **Note** The URL for contacting this AUS server is produced by concatenating the *Protocol* ://*Username* :*Password* *@IP IP Address* (:*Port*)/*Path* provided in the Add/Edit Auto Update Server dialog boxes. The Port is included only if you entered a port number other than the default 443.
Device ID Type	Choose the method used for identifying this device to the AUS server: • **Host Name** – The host name of this device, as provided in the Device Properties window (Tools > Device Properties). • **Serial Number** – The serial number of this device. • **IP Address** – The IP address of the specified interface. When you choose this option, an Interface field appears; enter or Select the desired device interface. • **MAC Address** – The MAC address of the specified interface. When you choose this option, an Interface field appears; enter or Select the desired device interface. • **User Defined** – A unique user-specified ID is used. When you choose this option, a User Defined field appears; enter any alphanumeric string. Note that this string must also appear in the Device Identity field in the Device Properties window (Tools > Device Properties).

Element	Description

Poll Type	Choose the method defining how often the AUS server is polled for updates:
	• **At Specified Frequency** – If you choose this option, the Poll Period field is displayed:
	  • **Poll Period** – Specify the number of minutes the device waits between polls of the AUS server; valid values are 1 to 35791.
	• **At Scheduled Time** – If you choose this option, the following fields are displayed (available only on ASA/PIX devices running version 7.2 or later):
	  • **Days of the week** – Select one or more days on which the device is to poll the AUS server.
	  • **Polling Start Time in Hours** – The hour at which polling is to begin on the selected days; based on a 24-hour clock.
	  • **Polling Start Time in Mins** – The minute within the chosen hour when polling is to begin.
	  • **Enable Randomization of the Start Time** – Select this option to specify a random polling window; the Randomization Window field is enabled.
	Randomization Window – The maximum number of minutes the device can use to randomize the specified polling time; valid values are 1 to 1439.

Retry Count	The number of times the device will try to poll the AUS server for new information. Optional; if you enter zero or leave this field blank, the device will not retry after a failed poll attempt.
Retry Period	If Retry Count is not zero or blank, the number of minutes the device will wait to re-poll the AUS server if the previous attempt failed; valid values are 1 to 35791. If Retry Count is not zero or blank and you leave this field blank, the value defaults to five minutes.
Disable Device After:	Selecting this option ensures that if no response is received from the AUS server within the specified Timeout period, the security appliance will stop passing traffic. • **Timeout** – The number of minutes the firewall device will wait to timeout if no response is received from the AUS server.

Add and Edit Auto Update Server Dialog Boxes

Use the Add Auto Update Server dialog box to configure a new AUS server definition. The security appliance will automatically poll this server for image and configuration updates.

The Auto Update specification allows the Auto Update server to either push configuration information and send requests for information to the security appliance, or to pull configuration information by causing the security appliance to periodically poll the Auto Update server. The Auto Update server can also send a command to the security appliance to send an immediate polling request at any time. Communication between the Auto Update server and the security appliance requires a communications path and local CLI configuration on each security appliance.

Note The URL for contacting this AUS server is produced by concatenating the *Protocol* ://*Username* :*Password* *@IP IP Address* (:*Port*)/*Path* provided in these dialog boxes. The Port is included only if you entered a port number other than the default 443.

With the exception of the title, the Edit Auto Update Server dialog box is identical to the Add Auto Update Server dialog box. The following descriptions apply to both.

Navigation Path

You can access the Add and Edit Auto Update Server dialog boxes from the AUS Page , on page 1.

Field Reference

Table 2: Add and Edit Auto Update Server Dialog Boxes

Element	Description
Protocol	The protocol used to communicate with the AUS server; choose **http** or **https**. **Note** If https is selected as the protocol to communicate with the Auto Update server, the security appliance will use SSL. This requires the security appliance to have a DES, 3DES, or AES license.
IP Address	Enter the IP address or Select a Networks/Hosts object representing this AUS server.
Port	Enter the number of the port on which communications with the AUS server take place. Defaults to 80 if http is chosen as the Protocol, and to 443 if https is chosen. If you enter an arbitrary port number, be sure the AUS server is configured to use the same port.
Path	The path to AUS services on the server. The standard path is autoupdate/AutoUpdateServlet ; change this to admin/auto-update only if the AUS server host is an ASA.
AUS Interface	Enter or Select the interface to use when polling the Auto Update server.
Verify Certificate	Select this option to require SSL verification from the AUS server. The certificate returned by the server will be checked against Certification Authority (CA) root certificates. This requires that the AUS Server and this device use the same Certification Authority.
Username	Enter a user name to be used for AUS authentication (optional).
Password	Enter the password to be used for AUS authentication (optional).
Confirm	Re-enter the password (optional).

DHCP Relay Page

Use the DHCP Relay page to configure DHCP relay services for security devices. Dynamic Host Configuration Protocol (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.

Note You cannot enable a DHCP relay agent on an interface where a DHCP relay server is configured. 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.

Beginning with Security Manager version 4.9, DHCP Relay IPv4 is supported for ASA cluster devices running the software version 9.4.0 or later.

For ASA-SM 9.1.2+ devices, you can configure DHCP relay servers per-interface, so requests that enter a given interface are relayed only to servers specified for that interface. 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. IPv6 is not supported for per-interface DHCP relay. For more information, see Add/Edit Interface Dialog Box: Advanced Tab (ASA/PIX 7.0+).

Navigation Path

- (Device view) Select **Platform > Device Admin > Server Access > DHCP Relay** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Server Access > DHCP Relay** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Field Reference

Table 3: DHCP Relay Page

Element	Description
DHCP Relay Agent table	This table lists the interfaces on which DHCP relay is configured. Use the Add Row, Edit Row, and Delete Row buttons to manage these entries. The Add Row button opens the Add DHCP Relay Agent Configuration dialog box, while Edit Row opens the Edit DHCP Relay Agent Configuration dialog box. See Add and Edit DHCP Relay Agent Configuration Dialog Boxes , on page 6 for more information.
DHCP Servers table	This table lists the global DHCP servers to which DHCP requests are relayed. Use the Add Row, Edit Row, and Delete Row buttons to manage these entries. The Add Row button opens the Add DHCP Relay Server Configuration dialog box, while Edit Row opens the Edit DHCP Relay Server Configuration dialog box. See Add and Edit DHCP Relay Server Configuration Dialog Boxes , on page 7 for more information.
Timeout (seconds)	Specify 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.

Element	Description
Trust Info (Option 82)	Specifies that you want to trust all DHCP client interfaces. You can configure interfaces as trusted interfaces to preserve DHCP Option 82. **Note** You can also specify interfaces to trust individually. For more information, see Add/Edit Interface Dialog Box: Advanced Tab (ASA/PIX 7.0+). 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.

Add and Edit DHCP Relay Agent Configuration Dialog Boxes

Use the Add DHCP Relay Agent Configuration dialog box to configure and enable a DHCP relay agent on an interface. Use the Edit DHCP Relay Agent Configuration dialog box to update an existing interface relay agent.

Note You cannot enable a DHCP relay agent on an interface where a DHCP relay server is configured. 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.

The Add DHCP Relay Agent Configuration dialog box and the Edit DHCP Relay Agent Configuration dialog box are virtually identical; the following descriptions apply to both.

Navigation Path

You can access the Add and Edit DHCP Relay Agent Configuration dialog boxes from the DHCP Relay Page , on page 4.

Related Topics

- Add and Edit DHCP Relay Server Configuration Dialog Boxes , on page 7

Field Reference

Table 4: Add and Edit DHCP Relay Agent Configuration Dialog Boxes

Element	Description
Interface	Enter or Select the name of the interface on which you want to configure a DHCP relay agent.
Enable DHCP Relay	When checked, the DHCP relay is enabled on the specified interface.

Element	Description
Set Route	Check this box to configure the DHCP relay agent to modify the default router address in the information returned from the DHCP server. When this option is selected, the DHCP relay agent substitutes the address of the selected interface for the default router address in the information returned from the DHCP server.

Add and Edit DHCP Relay Server Configuration Dialog Boxes

Use the Add DHCP Relay Server Configuration dialog box to define a new DHCP relay server; use the Edit DHCP Relay Server Configuration dialog box to update existing server information. 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.

Note PIX Firewalls running an OS earlier than 7.2 only support 4 DHCP relay servers.

The Add DHCP Relay Server Configuration dialog box and the Edit DHCP Relay Server Configuration dialog box are virtually identical; the following descriptions apply to both.

Navigation Path

You can access the Add and Edit DHCP Relay Server Configuration dialog boxes from the DHCP Relay Page , on page 4.

Related Topics

- Add and Edit DHCP Relay Agent Configuration Dialog Boxes , on page 6

Field Reference

Table 5: Add and Edit DHCP Relay Server Configuration Dialog Boxes

Element	Description
Server	Enter the IP address or Select a Networks/Hosts object representing the external DHCP server to which DHCP requests are forwarded.
Interface	Enter or Select the interface through which DHCP requests are forwarded to the external DHCP server.

DHCP Relay IPv6 Page

Use the DHCP Relay IPv6 page to configure DHCPv6 relay services for security devices. Dynamic Host Configuration Protocol v6 (DHCPv6) relay passes DHCPv6 requests received on one interface to an external DHCPv6 server located behind a different interface. To configure DHCPv6 relay, you need to specify at least one DHCPv6 relay server and then enable a DHCPv6 relay agent on the interface receiving DHCPv6 requests.

Note You cannot enable a DHCPv6 relay agent on an interface where a DHCPv6 relay server is configured. The DHCPv6 relay agent works only with external DHCPv6 servers; it will not forward DHCPv6 requests to a security appliance interface configured as a DHCPv6 server. Beginning with Security Manager version 4.9, DHCP Relay IPv6 is supported for ASA cluster devices running the software version 9.4.0 or later.

Navigation Path

- (Device view) Select **Platform > Device Admin > Server Access > DHCP Relay IPv6** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Server Access > DHCP Relay IPv6** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Note Two new interface settings have been introduced for DHCPv6: "managed-config-flag" and "other-config-flag." For more information, refer to Configuring IPv6 Interfaces (ASA/FWSM).

Field Reference

Table 6: DHCP Relay IPv6 Page

Element	Description
DHCP Relay IPv6 Agent table	This table lists the interfaces on which DHCP relay IPv6 is configured. Use the Add Row, Edit Row, and Delete Row buttons to manage these entries. The Add Row button opens the Add DHCP Relay IPv6 Agent Configuration dialog box, while Edit Row opens the Edit DHCP Relay IPv6 Agent Configuration dialog box. See Add and Edit DHCP Relay IPv6 Agent Configuration Dialog Boxes , on page 8 for more information.
DHCP Servers table	This table lists the interfaces on which DHCP relay IPv6 is configured. Use the Add Row, Edit Row, and Delete Row buttons to manage these entries. The Add Row button opens the Add DHCP Relay IPv6 Server Configuration dialog box, while Edit Row opens the Edit DHCP Relay IPv6 Server Configuration dialog box. See Add and Edit DHCP Relay IPv6 Server Configuration Dialog Boxes , on page 9 for more information.
Timeout (seconds)	Specify the amount of time, in seconds, allowed for DHCPv6 address negotiation. Valid values range from 1 to 3600 seconds; the default value is 60 seconds.

Add and Edit DHCP Relay IPv6 Agent Configuration Dialog Boxes

Use the Add DHCP Relay IPv6 Agent Configuration dialog box to configure and enable a DHCPv6 relay agent on an interface. Use the Edit DHCP Relay IPv6 Agent Configuration dialog box to update an existing interface relay agent.

Note You cannot enable a DHCPv6 relay agent on an interface where a DHCPv6 relay server is configured. The DHCPv6 relay agent works only with external DHCPv6 servers; it will not forward DHCPv6 requests to a security appliance interface configured as a DHCPv6 server.

The Add DHCP Relay IPv6 Agent Configuration dialog box and the Edit DHCP Relay IPv6 Agent Configuration dialog box are virtually identical; the following descriptions apply to both.

Navigation Path

You can access the Add and Edit DHCP Relay IPv6 Agent Configuration dialog boxes from the DHCP Relay IPv6 Page , on page 7.

Related Topics

- Add and Edit DHCP Relay IPv6 Server Configuration Dialog Boxes , on page 9

Field Reference

Table 7: Add and Edit DHCP Relay IPv6 Agent Configuration Dialog Boxes

Element	Description
Interface	Enter or Select the name of the interface on which you want to configure a DHCPv6 relay agent.
Enable DHCPv6 Relay	When checked, the DHCPv6 relay is enabled on the specified interface.
Set Route	Check this box to configure the DHCPv6 relay agent to modify the default router address in the information returned from the DHCPv6 server. When this option is selected, the DHCPv6 relay agent substitutes the address of the selected interface for the default router address in the information returned from the DHCPv6 server.

Add and Edit DHCP Relay IPv6 Server Configuration Dialog Boxes

Use the Add DHCP Relay IPv6 Server Configuration dialog box to define a new DHCPv6 relay server; use the Edit DHCP Relay IPv6 Server Configuration dialog box to update existing server information. You can define up to ten DHCPv6 relay servers.

Note The Add DHCP Relay IPv6 Server Configuration dialog box and the Edit DHCP Relay IPv6 Server Configuration dialog box are virtually identical; the following descriptions apply to both.

Navigation Path

You can access the Add and Edit DHCP Relay IPv6 Server Configuration dialog boxes from the DHCP Relay IPv6 Page , on page 7.

Related Topics

- Add and Edit DHCP Relay IPv6 Agent Configuration Dialog Boxes , on page 8

Field Reference

Table 8: Add and Edit DHCP Relay IPv6 Server Configuration Dialog Boxes

Element	Description
Server	Enter the IP address or Select a Networks/Hosts object representing the external DHCPv6 server to which DHCPv6 requests are forwarded.
Interface	Enter or Select the interface through which DHCPv6 requests are forwarded to the external DHCPv6 server.

Configuring DHCP Servers

A Dynamic Host Configuration Protocol (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 the 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. For more information about DHCP relay, see DHCP Relay Page , on page 4.

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

You can configure a DHCP server on each interface of the security appliance, and 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 DHCP server is enabled. Additionally, DHCP clients must be directly connected to the interface on which the server is enabled.

If your firewall is also acting as a DHCP client on the outside interface, you can enable auto-negotiated IP configuration. This allows the firewall to pass the DNS, WINS and domain name parameters it gets from the outside interface (as a DHCP client) to hosts on its inside network. Alternatively, you can manually specify the DNS, WINS and domain name parameters. If you specify those parameters manually and auto-configuration is on, your values take precedence over auto-configuration.

Use the DHCP Server Page , on page 10 to manage DHCP server definitions.

DHCP Server Page

Use the DHCP Server page to configure global DHCP server and dynamic DNS (DDNS) update options, to set up a DHCP server on one or more device interfaces, and to configure advanced server options.

Navigation Path

- (Device view) Select **Platform > Device Admin > Server Access > DHCP Server** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Server Access > DHCP Server** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- Configuring DHCP Servers , on page 10

Field Reference

Table 9: DHCP Server Page

Element	Description
Ping Timeout	Specify the amount of time, in milliseconds, that the firewall device waits to time out a DHCP ping attempt. To avoid address conflicts, firewall devices send two ICMP ping packets to an address before assigning that address to a DHCP client. Valid values range from 10 to 10000 milliseconds.
Lease Length	Specify 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).
Enable auto-configuration (PIX and ASA only)	Select this option to enable DHCP auto configuration. 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, the manually specified information takes precedence over the discovered information.
Interface	If Enable auto-configuration is checked, this field is available. Enter or Select the interface running the DHCP client that supplies the DNS, WINS, and domain name parameters.
Define settings (optional)	
Domain Name	Specify the DNS domain name for DHCP clients. Enter a valid DNS domain name; for example, example.com .
Primary DNS Server	Enter the IP address or Select a Networks/Hosts object representing the primary DNS server for a DHCP client.
Primary WINS Server	Enter the IP address or Select a Networks/Hosts object representing the primary WINS server for a DHCP client.
Secondary DNS Server	Enter the IP address or Select a Networks/Hosts object representing the alternate DNS server for a DHCP client.

Element	Description
Secondary WINS Server	Enter the IP address or Select a Networks/Hosts object representing the alternate WINS server for a DHCP client.
Dynamic DNS Update	
Enable Dynamic DNS Update	Check this box to define global DDNS update options: • Select the type of resource-record updating: **PTR Record** only, or **A Record and PTR Record**. • You also can select Override DHCP Client Request. If selected, DHCP server updates override any updates requested by DHCP clients. These options are available only on ASA/PIX 7.2 and later.
DHCP Server Interface Configuration table	
Interface table	This table lists device interfaces on which a DHCP server, DDNS updating, or both are configured. Use the Add Row, Edit Row, and Delete Row buttons to manage these entries. The Add Row button opens the Add DHCP Server Interface Configuration dialog box, while Edit Row opens the Edit DHCP Server Interface Configuration dialog box. See Add and Edit DHCP Server Interface Configuration Dialog Boxes , on page 12 for more information.
Advanced Options	
Advanced button	Opens the Add/Edit DHCP Server Advanced Configuration Dialog Box , on page 13.

Add and Edit DHCP Server Interface Configuration Dialog Boxes

Use these dialog boxes to enable DHCP and specify a DHCP address pool for a specified interface, and to enable dynamic DNS (DDNS) updating on the interface.

Note Other than the titles, the two dialog boxes are identical.

Navigation Path

You can access the Add DHCP Server Interface Configuration and Edit DHCP Server Interface Configuration dialog boxes from the DHCP Server Page , on page 10.

Related Topics

- Configuring DHCP Servers , on page 10

Field Reference

Table 10: Add/Edit DHCP Server Interface Configuration Dialog Boxes

Element	Description
Interface	Identifies the interface on which you are configuring a DHCP server. Enter an interface name, or select an interface object.
DHCP Address Pool	Enter an IP address or a range of addresses, separated by a hyphen, that the DHCP server will use when assigning IP addresses. The beginning and ending addresses in the range must be in the same subnet, and the beginning address cannot be greater than the ending address.
Enable DHCP Server	Check this box to enable a DHCP server on this interface.
Enable Dynamic DNS Update	Check this box to enable DDNS updating by this DHCP server. Specify the record(s) to be updated: • **PTR Record** only • **A Record and PTR Record** You also can select **Override DHCP Client Request**. If selected, DHCP server updates override any updates requested by DHCP clients.

Add/Edit DHCP Server Advanced Configuration Dialog Box

The Add/Edit DHCP Server Advanced Configuration dialog box lets you manage DHCP options configured for the DHCP server. These options 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.

Navigation Path

You can access the Add/Edit DHCP Server Advanced Configuration dialog box by clicking the Advanced button on the DHCP Server Page , on page 10.

Related Topics

• Configuring DHCP Servers , on page 10

Field Reference

Table 11: Add/Edit DHCP Server Advanced Configuration Dialog Box

Element	Description
Options table	This table lists configured DHCP server options. Use the Add Row, Edit Row, and Delete Row buttons to manage these entries. The Add Row button opens the Add DHCP Server Interface Configuration dialog box, while Edit Row opens the Edit DHCP Server Interface Configuration dialog box. See Add/Edit DHCP Server Option Dialog Box , on page 14 for more information.

Add/Edit DHCP Server Option Dialog Box

The Add and Edit DHCP Server Option dialog boxes let you configure DHCP server option parameters, 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.

Navigation Path

You can access the Add and Edit DHCP Server Option dialog boxes from the Add/Edit DHCP Server Advanced Configuration Dialog Box , on page 13.

Related Topics

- Configuring DHCP Servers , on page 10
- DHCP Server Page , on page 10

Field Reference

Table 12: Add/Edit DHCP Server Option Dialog Box

Element	Description
Option Code	Choose an option from the list of available option codes. All DHCP options (options 1 through 255) are supported except 1, 12, 50-54, 58-59, 61, 67, and 82. Detailed information about DHCP option codes is available on cisco.com: DHCP Options Reference.
Type	Choose the type of information the option returns to the DHCP client: • **IP** – Choosing this type specifies that one or two IP addresses are returned to the DHCP client. Provide up to two IP addresses. • **ASCII** – Choosing this type specifies that an ASCII value is returned to the DHCP client. Provide the ASCII character string, which cannot include spaces. • **HEX** – Choosing this type specifies that an hexadecimal value is returned to the DHCP client. Provide the HEX string with an even number of digits and no spaces; you do not need to use a 0x prefix.

DNS Page

Use the DNS page to configure DNS server groups. The firewall device uses these DNS servers to resolve fully-qualified domain names (host names) to IP addresses for SSL VPN, certificates, and FQDN network/host objects used in identity-aware firewall policies. Other features that define server names (such as AAA) do not support DNS resolution—you must enter the IP address or manually resolve the name to an IP address.

Tip The DefaultDNS server group is predefined on the ASA and is used for FQDN network/host object resolution. If you use FQDN objects, ensure that you configure DNS servers for this group; otherwise, the names cannot be resolved. To enhance security, ensure that you specify DNS servers that are trusted and that are preferably inside your network. For more information, see Requirements for Identity-Aware Firewall Policies.

Navigation Path

- (Device view) Select **Platform > Device Admin > Server Access > DNS** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Server Access > DNS** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- Add DNS Server Dialog Box , on page 17

Field Reference

Table 13: DNS Page

Element	Description
DNS Server Groups table	This table lists the currently defined DNS server groups. Use the Add Row, Edit Row and Delete Row buttons below the table to manage these group entries. The Add Row button opens the Add DNS Server Group dialog box, and the Edit Row button opens the Edit DNS Server Group dialog box; except for the titles these dialog boxes are identical. See Add DNS Server Group Dialog Box , on page 16 for more information.
DNS Lookup Interfaces	Lists the interfaces on which you want to enable DNS lookup. Enter or Select one or more interfaces or interface roles.
Enable DNS Guard (ASA/PIX 7.0(5), 7.2(x) and 8.x only)	Check this box to enable DNS Guard for the selected device or shared policy. DNS Guard tears down the DNS session associated with a DNS query as soon as the DNS reply is forwarded by the security appliance. DNS Guard also monitors the message exchange to ensure that the ID of the DNS reply matches the ID of the DNS query. This command is effective only on interfaces for which DNS inspection is disabled. When DNS inspection is enabled, the DNS Guard function is always performed. **Note** In releases prior to 7.0(5), the DNS Guard functions are always enabled regardless of the configuration of DNS inspection.

Element	Description
DefaultDNS Server Group (ASA 8.4(2)+)	Additional settings that apply to the DefaultDNS server group only. These settings are used when resolving FQDN network/host objects to IP addresses. • **Poll Timer**—The time, in minutes, of the polling cycle used to resolve FQDN network/host objects to IP addresses. FQDN objects are resolved only if they are used in a firewall policy. The timer determines the maximum time between resolutions; the DNS entry's time-to-live (TTL) value is also used to determine when to update to IP address resolution, so individual FQDNs might be resolved more frequently than the polling cycle. The default is 240 (four hours). The range is 1 to 65535 minutes. • **Expire Entry Timer**—The number of minutes after a DNS entry expires (that is, the TTL has passed) that the entry is removed from the DNS lookup table. Removing an entry requires that the table be recompiled, so frequent removals can increase the processing load on the device. Because some DNS entries can have very short TTL (as short as three seconds), you can use this setting to virtually extend the TTL. The default is 1 minute (that is, the entry is removed one minute after the TTL has passed). The range is 1 to 65535 minutes.

Add DNS Server Group Dialog Box

Use the Add DNS Server Group dialog box to define the DNS servers and settings for a DNS server group, used by security devices to resolve server names to IP addresses in policies that support name resolution.

Note With the exception of its title, the Edit DNS Server Group dialog box is identical to this one, and the following descriptions apply to both.

Navigation Path

You can access the Add DNS Server Group and Edit DNS Server Group dialog boxes from the DNS Page , on page 14.

Field Reference

Table 14: Add/Edit DNS Server Group Dialog Boxes

Element	Description
Name	Provide a name for the group of DNS servers. **Tip** The name DefaultDNS is predefined on the ASA and includes the servers used for policies that do not allow the selection of a specific group, such as for FQDN network/host object resolution.

Element	Description
DNS Servers	Lists the DNS servers in this group. You can specify up to six servers to which DNS requests can be forwarded. The security appliance tries each DNS server in top-to-bottom order until it receives a response. **Note** You also must specify at least one interface on which DNS is enabled in the DNS Lookup section of the DNS Page , on page 14. Use the buttons next to this list to manage the entries; from the top down, they are: • Add a DNS server to the list; opens the Add DNS Server Dialog Box , on page 17. • Delete the currently selected DNS server entry from the list. • Move the currently selected entry up one row. • Move the currently selected entry down one row.
Timeout	Specify the number of seconds, from 1 to 30, to wait before trying the next DNS server; the default is 2 seconds. Each time the security device retries the list of servers, this timeout doubles.
Retries	Specify the number of times, from 0 to 10, to retry the list of DNS servers when the security device does not receive a response.
Domain Name	Optionally, specify a valid DNS domain name for the server; for example, **dnsexample.com**.

Add DNS Server Dialog Box

Use the Add DNS Server dialog box to add a DNS server to the DNS servers list in the Add DNS Server Group or Edit DNS Server Group dialog boxes.

Navigation Path

You can access the Add DNS Server dialog box from the Add DNS Server Group or Edit DNS Server Group dialog boxes. For more information about these dialog boxes, see Add DNS Server Group Dialog Box , on page 16.

Related Topics

- DNS Page , on page 14

Field Reference

Table 15: Add DNS Server Dialog Box

Element	Description
DNS Server	The IP address, or the host network/host object that defines the address, of the DNS server. Enter the address or click **Select** to select the network/host object from a list or to create a new object.

Element	Description
Interface (ASA 9.5(1) or later)	Click select to choose an interface. The Interface selector dialog box lists only Interface Roles and not Physical Interfaces. Therefore you must add a Physical Interface to the Interface Role before selecting the Source Interface. There is no default value for the interface. This feature is available in Security Manager version 4.9 and later for devices running ASA version 9.5(1) or later.

Configuring DDNS

Dynamic DNS (DDNS) provides IP-address and domain-name mapping updates so hosts can find each other even though their DHCP-assigned IP addresses may change frequently. Also, beginning with the version 7.2(3), Cisco security appliances can generate DDNS updates. The DDNS page is where you configure this feature.

The DDNS mappings are maintained on the DHCP server in two types of resource records (RRs): the address or *A* records contain the name-to-IP-address mappings, while the pointer or *PTR* records map addresses to host names.

By automatically recording the association between assigned addresses and host names at 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.

Navigation Path

- (Device view) Select **Platform > Device Admin > Server Access > DDNS** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Server Access > DDNS** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Field Reference

Table 16: DDNS Page

Element	Description
Dynamic DNS Interface Settings	This table lists currently defined DDNS interface-update methods. Use the Add Row, Edit Row, and Delete Row buttons below the table to manage these methods; the Add Row and Edit Row buttons open the Add/Edit DDNS Interface Rule Dialog Box , on page 19.
DHCP Client requests DHCP Server to update records	The global setting on the appliance for DHCP client update requests. This option enables the client to send DDNS updates via the DHCP server, and specifies what is updated: the PTR resource record, both the A and PTR resource records, or neither. Choose **Not Selected**, **Only PTR Record**, **Both A and PTR Record**, or **No Update**.
DHCP Client ID Interface	Specify the interface(s) for global DHCP client update requests: enter an interface name or IP address, or Select an interface object.

Element	Description
Enable DHCP Client Broadcast	Select this option to allow DHCP clients on the device to broadcast DDNS updates. Available on ASA/PIX 7.2(3)+ devices only.

Add/Edit DDNS Interface Rule Dialog Box

Use the Add/Edit DDNS Interface Rule dialog box to manage rules for dynamic DNS updates. These rules are defined on a per-interface basis.

Navigation Path

You access the Add/Edit DDNS Interface Rule dialog box from the Configuring DDNS , on page 18.

Related Topics

- DDNS Update Methods Dialog Box , on page 19
- Add/Edit DDNS Update Methods Dialog Box , on page 20

Field Reference

Table 17: Add/Edit DDNS Interface Rule Dialog Box

Element	Description
Interface	Enter or Select the name of the interface on which DDNS is to be configured. **Note** DHCP must be enabled on the specified interface.
Method Name	Choose a previously defined method for DDNS update, or choose **Add/Edit Update Method** to define a new method; the DDNS Update Methods Dialog Box , on page 19 dialog box opens.
Hostname	Enter the name of the DDNS server host to which updates will be sent.
DHCP Client requests DHCP Server to update records	The setting on the interface for DHCP client update requests; specifies whether the DHCP server updates the PTR resource record, both the A and PTR records, or neither. Choose **Not Selected**, **Only PTR Record**, **Both A and PTR Record**, or **No Update**. Any choice other than Not Selected overrides the global setting on the Configuring DDNS , on page 18.

DDNS Update Methods Dialog Box

Use the DDNS Update Methods dialog box to manage methods for dynamic DNS updates. Each defined method specifies an update interval and the resource record(s) to be updated.

Navigation Path

You access the DDNS Update Methods dialog box by choosing **Add/Edit Update Method** from the Method Name drop-down list in the Add/Edit DDNS Interface Rule Dialog Box , on page 19.

Related Topics

- Configuring DDNS , on page 18

Field Reference

Table 18: DDNS Update Methods Dialog Box

Element	Description
Update Methods	This table lists the currently defined update methods. Use the buttons below the table to manage these entries.
Add Row button	Opens the Add/Edit DDNS Update Methods Dialog Box , on page 20 where you can define a new update method.
Edit Row button	Opens the Add/Edit DDNS Update Methods Dialog Box , on page 20, where you can edit the method currently selected in the table.
Delete Row button	Deletes the method currently selected in the Update Methods table; confirmation may be required.

Add/Edit DDNS Update Methods Dialog Box

Use the Add/Edit DDNS Update Methods dialog box to define or edit a DDNS update method; currently defined methods are listed in the DDNS Update Methods Dialog Box , on page 19.

Navigation Path

You access the Add/Edit DDNS Update Methods dialog box by clicking the Add Row or the Edit Row buttons in the DDNS Update Methods Dialog Box , on page 19.

Related Topics

- Configuring DDNS , on page 18

Field Reference

Table 19: Add/Edit DDNS Update Methods Dialog Box

Element	Description
Method Name	Provide an identifier for this method.
Update Interval	Specify how often records are to be updated for this method: provide a number of days, hours, minutes, and seconds. Note that while zero is the default value for hours, minutes and seconds, there is no default Day value: you must enter a number for Day.

Element	Description
Update Records	Specify the resource record(s) to be updated: select **Not Defined**, **A Records**, or **Both A and PTR Records**. Selecting A Records or Both A and PTR Records overrides the setting in the Add/Edit DDNS Interface Rule Dialog Box , on page 19.

NTP Page

Network Time Protocol (NTP) is used to implement a hierarchical system of servers that provide precisely synchronized timing for network systems. This kind of accuracy is required for time-sensitive operations, such as validating Certificate Revocation Lists (CRLs), which include a precise time stamp. You can configure multiple NTP servers. The security device chooses the server with the lowest stratum—a measure of how reliable the data is.

Note This page is not available on Catalyst 6500 service modules (the Firewall Services Module and the Adaptive Security Appliance Service Module).

Use the NTP page to enable NTP and manage the NTP servers used to dynamically set the time on a security device.

Note Time derived from an NTP server overrides any time set manually on the Clock page.

Navigation Path

- (Device view) Select **Platform > Device Admin > Server Access > NTP** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Server Access > NTP** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Field Reference

Table 20: NTP Page

Element	Description
Enable NTP Authentication	Enables or disables authentication with an NTP server. Disabling authentication does not alter the list of configured servers. If you enable authentication, the security appliance only communicates with an NTP server if it uses the correct trusted key in the packets. The security appliance also uses an authentication key to synchronize with the NTP server.
NTP Server Table	Lists the currently configured NTP servers. Use the Add Row, Edit Row and Delete Row buttons to manage this list; the Add Row and Edit Row buttons open the NTP Server Configuration Dialog Box , on page 22.

NTP Server Configuration Dialog Box

Use the NTP Server Configuration dialog box to add or edit an NTP server definition.

Navigation Path

You can access the NTP Server Configuration dialog box from the NTP Page , on page 21.

Note The NTP page is not available on Catalyst 6500 service modules (the Firewall Services Module and the Adaptive Security Appliance Service Module).

Field Reference

Table 21: NTP Server Configuration Dialog Box

Element	Description
IP Address	Enter or Select the IP address of the NTP server.
Preferred	If checked, this NTP server is the preferred server when multiple servers are similarly accurate. NTP uses an algorithm to determine which server is the most accurate and synchronizes to that one. If multiple servers are of similar accuracy, then this option specifies which of those servers to use. However, if a server is significantly more accurate than the preferred one, the security appliance uses the more accurate server. For example, the security appliance uses a server of stratum 2 over a server of stratum 3 that is preferred. We recommend that you configure an NTP server as preferred only when multiple servers are likely to have the same stratum.
Interface	Enter or Select the interface used for NTP traffic, if you want to override the default interface in to the routing table.
Authentication Type	Adding to MD5, the following authentication types are also supported in Cisco Security Manager starting from version 4.20 for ASA 9.13(1) and higher devices: • sha1 • sha256 • sha512 • cmac
Key Number	Enter the ID for this authentication key. The NTP server packets must also use this key ID. If you previously configured a key ID for another server, you can select it in the list; otherwise, type a number between 1 and 4294967295.
Trusted	Sets this key as a trusted key. You must select this option for authentication to work.
Key Value	Enter the authentication key as a string up to 32 characters in length.

Element	Description
Confirm	Re-enter the authentication key to verify it is correct.

SMTP Server Page

Use the SMTP Server page to specify the IP address of an SMTP server and optionally, the IP address of a backup server, to which e-mail alerts and notifications are sent in response to specific events.

Navigation Path

- (Device view) Select **Platform > Device Admin > Server Access > SMTP Server** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Server Access > SMTP Server** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Field Reference

Table 22: SMTP Server Page

Element	Description
Primary Server IP Address	Enter or Select the IP address of the SMTP server.
Secondary Server IP Address	Enter or Select the IP address of a back-up SMTP server.

TFTP Server Page

The Trivial File Transfer Protocol (TFTP) is a simple client/server file transfer protocol described in RFC783 and RFC1350 Rev. 2. You can use the TFTP Server page to configure the security appliance as a TFTP client so it can transfer a copy of its running configuration file to a TFTP server. In this way, you can back up and propagate configuration files to multiple security appliances. Only one server is supported.

Navigation Path

- (Device view) Select **Platform > Device Admin > Server Access > TFTP Server** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Server Access > TFTP Server** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Field Reference

Table 23: TFTP Server Page

Element	Description
Interface	Enter or Select the name of interface on which the TFTP server is accessed.
IP Address	Enter or Select the IP address of the TFTP server.
Directory	Enter the path on the TFTP server, beginning with a forward slash (/) and ending in the file name, to which the configuration files will be written (for example, **/tftpboot/asa/config3**). **Note** The path must begin with a forward slash (/).