Configuring Public Servers

This section describes how to configure public servers, and includes the following topics:

Information About Public Servers

The Public Servers pane enables an administrator to provide internal and external users access to various application servers. This pane displays a list of public servers. internal and external addresses, the interfaces to which the internal or external addresses apply, the ability to translate the addresses, and the service that is exposed. You can add, edit, delete, or modify settings for existing public servers.

Licensing Requirements for Public Servers

Model	License Requirement
All models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

Adding a Public Server that Enables Static NAT

To add a public server that enables static NAT and creates a fixed translation of a real address to a mapped address, perform the following steps:

Step 1 In the Configuration > Firewall > Public Servers pane, click **Add** to add a new server.

The Add Public Server dialog box appears.

Step 2 From the Private Interface drop-down menu, select the name of the private interface to which the real server is connected.

Step 3 In the Private IP address field, enter the real IP address of the server (IPv4 only).

Step 4 In the Private Service field, click **Browse** to display the Browse Service dialog box, choose the actual service that is exposed to the outside, and click **OK**.

Optionally, from the Browse Service dialog box you can click **Add** to create a new service or service group. Multiple services from various ports can be opened to the outside. For more information about service objects and service groups, see the "Configuring Service Objects and Service Groups" section on page 25-4.

Step 5 From the Public Interface drop-down menu, enter the interface through which users from the outside can access the real server.

Step 6 In the Public Address field, enter the mapped IP address of the server, which is the address that is seen by the outside user.

Step 7 (Optional) To enable static PAT, check the **Specify if Public Service is different from private service** check box .

Step 8 Click **OK**. The configuration appears in the main pane.

Step 9 Click **Apply** to generate static NAT and a corresponding access rule for the traffic flow and to save the configuration.

For information about static NAT, see the "Information About Static NAT" section on page 32-3.

Adding a Public Server that Enables Static NAT with PAT

To add a public server that lets you specify a real and mapped protocol (TCP or UDP) to a port, perform the following steps:

Step 1 Choose **Configuration > Firewall > Public Servers**, then click **Add**.

The Add Public Server dialog box appears.

Step 2 From the Private Interface drop-down menu, choose the name of the private interface to which the real server is connected.

Step 3 In the Private IP address field, enter the real IP address of the server (only IPv4 is supported).

Step 4 In the Private Service field, click **Browse** to display the Browse Service dialog box

Step 5 Choose the actual service that is exposed to the outside, and click **OK**.

Optionally, from the Browse Service dialog box, click **Add** to create a new service or service group. Multiple services from various ports can be opened to the outside. For more information about service objects and service groups, see the "Configuring Service Objects and Service Groups" section on page 25-4.

Step 6 From the Public Interface drop-down menu, enter the interface through which users from the outside can access the real server.

Step 7 In the Public Address field, enter the mapped IP address of the server, which is the address that the outside user sees.

Step 8 Check the **Specify Public Service if different from Private Service** check box to enable static PAT.

In the Public Service field, enter the mapped protocol (TCP or UDP only), or click **Browse** to choose a protocol from the list.

Optionally, to specify a custom port for TCP or UDP, enter the port number as *tcp/<port number>* or *udp/<port number>* in the Public Service field.

Step 9 Click **OK**.

Step 10 Click **Apply** to generate static NAT with PAT and a corresponding access rule for the traffic flow, and to save the configuration.

For information about static NAT with port address translation, see the "Information About Static NAT with Port Translation" section on page 32-4.

Editing Settings for a Public Server

To edit the settings for a public server, perform the following steps:

Step 1 Choose **Configuration > Firewall > Public Servers**, choose an existing public server, then click **Edit**.

The Edit Public Server dialog box appears.

Step 2 Make any necessary changes to the following settings:

- Private Interface—The interface to which the real server is connected.
- Private IP Address—The real IP address of the server.
- Private Service—The actual service that is running on the real server.
- Public Interface—The interface through which outside users can access the real server.
- Public Address—The IP address that is seen by outside users.
- Public Service—The service that is running on the translated address.

Step 3 Click **OK**, then click **Apply** to save your changes.

Feature History for Public Servers

Table 55-1 lists each feature change and the platform release in which it was implemented. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 55-1 Feature History for Public Servers

Feature Name	Platform Releases	Feature Information
Public Servers	8.3(1)	Public servers provide internal and external users access to various application servers. We introduced the following screen: Configuration > Firewall > Public Servers