CHAPTER 7

Using the Startup Wizard

The ASDM Startup Wizard guides you through the initial configuration of the FWSM, and helps you define the following settings for the FWSM:

- The hostname
- The domain name
- A password to restrict administrative access through ASDM or the CLI
- The IP address information of the outside interface
- Other interfaces, such as the inside or DMZ interfaces
- NAT or PAT rules
- DHCP settings for the inside interface, for use with a DHCP server

To access the Startup Wizard from the main ASDM application window, choose one of the following:

- **Wizards > Startup Wizard**.
- **Configuration > Device Setup > Startup Wizard,** and then click **Launch Startup Wizard**.

For more information, see the "Starting ASDM from a Web Browser" section on page 6-5.

Modes

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

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

Startup Wizard Screens

Table 7-1 lists all of the required Startup Wizard screens. The actual sequence of screens is determined by your specified configuration selections. The Description column describes the function that each screen performs in the configuration process. The Availability column lists the mode or modes in which each screen appears and provides additional configuration information. Click the name to view information for the selected screen.

Table 7-1 Startup Wizard Screens

Screen Name	Description	Availability
Welcome, page 7-2	Explains the function of the Startup Wizard. Starts with the current running configuration.	All modes.
Basic Configuration, page 7-3	Lets you retain or modify the existing configuration.	
Auto Update Server, page 7-4	Lets you manage the adaptive security appliance remotely from an Auto Update server.	Single routed and single transparent modes. If enabled in single transparent mode, the Interface Configuration and DHCP Server screens are not available.
Management IP Address Configuration, page 7-6	Lets you configure the management IP address of the host for this context.	Single transparent mode only.
Outside Interface Configuration, page 7-6	Lets you configure the outside interfaces.	Single routed mode only.
Interface Configuration, page 7-4	Lets you configure the remaining interfaces.	
Static Routes, page 7-7	Lets you create, edit, and remove static routes that will access networks connected to a router on any interface.	All modes.
DHCP Server, page 7-7	Lets you configure the FWSM as a DHCP server to hosts on the inside interface.	Single routed mode only.
Address Translation (NAT/PAT), page 7-8	Lets you configure either NAT or PAT for address translation on the FWSM.	All modes
Administrative Access, page 7-9	Lets you configure host or network access to the FWSM.	
Startup Wizard Summary, page 7-11	Lists all settings that you have configured for the FWSM.	

Welcome

In the Welcome screen, perform the following steps:

Step 1 To change the existing configuration, choose **Modify existing configuration**.

Step 2 To set the configuration at the factory default values for the inside interface, choose **Reset configuration to factory defaults**.

Step 3 To configure the IP address and subnet mask of the management interface, check the **Configure the IP address of the management interface** check box.

Step 4 Specify the IP address of the management interface.

Step 5 Choose the subnet mask of the management interface from the drop-down list.

Note If you reset the configuration to factory defaults, you cannot undo these changes by clicking **Cancel** or by closing this screen.

Step 6 Click **Next** to continue.

Modes

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

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

Basic Configuration

In the Basic Configuration screen, perform the following steps:

Step 1 Specify a hostname for the FWSM. The hostname can be up to 63 alphanumeric characters in mixed case.

Step 2 Specify the IPsec domain name of the FWSM, which can be used for certificates. The domain name can be a maximum of 63 alphanumeric characters, with no special characters or spaces.

The Privileged Mode (Enable) Password section allows you to restrict administrative access to the FWSM through ASDM or the CLI.

Note If you leave the password field blank, a Password Confirmation dialog box appears to notify you that to do so is a high security risk.

Step 3 To change the current privileged mode (enable) password, check the **Change privileged mode (enable) password** check box.

Step 4 Specify the old enable password, if one exists.

Step 5 Specify the new enable password. The password is case-sensitive and can be up to 32 alphanumeric characters.

Step 6 Reenter the new enable password.

Step 7 Click **Next** to continue.

Modes

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

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

Auto Update Server

In the Auto Update Server screen, perform the following steps:

Step 1 To enable communication between the FWSM and an Auto Update server, check the **Enable Auto Update** check box.

Step 2 From the drop-down list, choose either HTTPS or HTTP to define the beginning of the URL for the Auto Update Server.

Step 3 To confirm that an SSL certificate is enabled on the Auto Update Server, check the **Verify server's SSL certificate** check box.

Step 4 Specify the username to log in to the Auto Update server.

Step 5 Specify the password to log in to the Auto Update server.

Step 6 Reenter the password to confirm it.

Step 7 To uniquely identify the FWSM, choose the type of ID from the Device ID Type drop-down list. To enable the Device ID field, choose **User-defined name**, in which you specify a unique ID.

Step 8 Specify a unique string to use as the FWSM device ID.

Step 9 Click **Next** to continue.

Modes

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

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

Interface Configuration

To configure the remaining interfaces, perform the following steps:

Step 1 Choose an interface to change from the list, and click **Edit**. For more information, see Edit Interface, page 7-5.

Step 2 To enable traffic between two or more interfaces with the same security level, check the **Enable traffic between two or more interfaces with the same security level** check box.

Step 3 To enable traffic between two or more hosts connected to the same interface, check the **Enable traffic between two or more hosts connected to the same interface** check box.

Note IP address-related fields are not available in transparent mode.

Step 4 Click **Next** to continue.

Modes

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

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

Edit Interface

To change the configuration of an interface, perform the following steps:

Step 1 Specify the name of the selected interface to edit.

Step 2 Specify the name of the selected interface, or change the name of the interface, if required.

Step 3 Specify the security level of the selected interface. If you change the security level of the interface to a lower level, a warning message appears.

Step 4 To enter a specific IP address for an interface, check the **Uses the following IP address** check box.

Step 5 Change the IP address of the interface.

Step 6 Choose an existing subnet mask from the drop-down list, and then click **OK** to close this dialog box.

Modes

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

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

Outside Interface Configuration

Note With a full license, the FWSM supports up to five interfaces, with a maximum of three outside interfaces. In restricted mode, the FWSM supports up to three interfaces, and in transparent mode, the FWSM supports up to two interfaces. After you have created the maximum number of interfaces, or the maximum number of interfaces has already been named, you may not be able to create a new VLAN, and must select an existing one.

To configure the outside interface by specifying an IP address, perform the following steps:

Step 1 Choose an interface from the drop-down list.

Step 2 Add a name to a new interface, or choose the name associated with an existing interface.

Step 3 To activate the interface in privileged mode, check the **Enable interface** check box.

Step 4 Specify the security level range for the interface from 0 to 100, with 100 assigned to the inside interface and 0 assigned to the outside interface. Perimeter interfaces can have any number between 1 and 99. Security levels between 0 and 100 for perimeter interfaces are not set by default.

Step 5 To specify an IP address manually for the interface, click **Use the following IP address**. This field is not visible in transparent mode.

Step 6 Specify an IP address for an outside interface. This field is not visible in transparent mode.

Step 7 Choose a subnet mask for an outside interface from the drop-down list.

Step 8 Click **Next** to continue.

Modes

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

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

Management IP Address Configuration

In the Management IP Address Configuration screen, perform the following steps:

Step 1 Specify the management IP address of the host that can access this context using ASDM or a session protocol.

Step 2 Specify the subnet mask for the management IP address.

Step 3 Click **Next** to continue.

Modes

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

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

Static Routes

You can add, edit, and remove static routes that access networks connected to a router on any interface. For more information, see Configuring Static Routes, page 11-41 and Add/Edit Static Route, page 7-7.

Modes

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

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

Add/Edit Static Route

You can add or edit a static route. For more information, see Add/Edit Static Route, page 11-42.

DHCP Server

To configure the DHCP server for other interfaces from the main ASDM application window, choose **Configuration> Device Management > DHCP > DHCP Server**. For more information, see DHCP Server, page 13-4.

To configure the FWSM as a DHCP server, perform the following steps:

Step 1 To allow connection to the DHCP server from the inside interface, check the **Enable DHCP server on the inside interface** check box.

Step 2 Specify the starting range of the DHCP server pool in a block of IP addresses from the lowest to highest.

Note The FWSM supports up to 256 IP addresses.

Step 3 Specify the ending range of the DHCP server pool in a block of IP addresses from the lowest to highest.

Step 4 Check the **Enable auto-configuration from interface** check box to allow automatic configuration of the following settings:

- The IP address of the DNS server.

- The IP address of the WINS server.
- The IP address of the alternate DNS server.
- The IP address of the alternate WINS server.
- The amount of time (in seconds) that the client can use its allocated IP address before the lease expires. The default value is 3600 seconds (1 hour).
- The parameters for the ping timeout value in milliseconds.
- The domain name of the DNS server to use DNS.

Step 5 To enable DHCP auto-configuration, check the **Enable auto-configuration from interface** check box, and then select the interface from the list. The values you specified in the previous sections of the screen take precedence over the auto-configured values.

Step 6 Click **Next** to continue.

Modes

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

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

Address Translation (NAT/PAT)

PAT lets you set up a single IP address for use as the global address. In addition, you can set multiple outbound sessions to appear as if they originate from a single IP address. PAT lets up to 65,535 hosts start connections through a single outside IP address.

When you use PAT, be aware of the following:

- PAT does not work with caching name servers.
- You may need to enable the corresponding inspection engine to pass multimedia application protocols through the FWSM.
- PAT does not work with the **established** command.
- With passive FTP, use the **inspect protocol ftp strict** command with the **access-list** command to allow outbound FTP traffic.
- A DNS server on a higher level security interface cannot use PAT.

If you decide to use NAT, enter an address range to use for translating all addresses on the inside interface to addresses on the outside interface. The global addresses in the pool provide an IP address for each outbound connection, and for those inbound connections resulting from outbound connections.

To configure NAT or PAT, perform the following steps:

Step 1 To enable NAT and a range of IP addresses to be used for translation, choose **Use Network Address Translation (NAT)**.

Step 2 Specify the first IP address in a range of IP addresses to be used for translation.

Step 3 Specify the last IP address in a range of IP addresses to be used for translation.

Step 4 Specify the subnet mask for the range of IP addresses to be used for translation.

Step 5 To enable PAT, choose **Use Port Address Translation (PAT)**. Complete the following if you select this option:

- To use the IP address of the outside interface for PAT, choose **Use the IP address on the outside interface**.
- Enter an IP address for the outside interface to be used for PAT.
- Choose a subnet mask from the drop-down list.
- To allow traffic through the firewall without translation, choose **Enable traffic through the firewall without address translation**.

Step 6 Click **Next** to continue.

Modes

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

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

Administrative Access

To configure host or network access, perform the following steps:

Step 1 Specify how the host or network is accessing the FWSM— through HTTP over SSL in ASDM, SSH, or Telnet.

Step 2 Specify the host or network name.

Step 3 Specify the IP address of the host or network.

Step 4 Specify the subnet mask of the host or network.

Step 5 To enable a secure connection to an HTTP server to access ASDM, check the **Enable HTTP server for HTTPS/ASDM access** check box.

Note Unchecking this check box will prevent ASDM access to the FWSM.

Step 6 To add the access type, an interface, and then specify the IP address and netmask of the host network that may connect to that interface for management purposes only, click **Add**. To change an interface, click **Edit**. To remove an interface, click **Delete**. For more information, see Add/Edit Administrative Access Entry, page 7-10.

Step 7 To allow ASDM to collect and display statistics, check the **Enable ASDM history metrics** check box.

Step 8 Click **Next** to continue.

Modes

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

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

Add/Edit Administrative Access Entry

To access the Add/Edit Administrative Access Entry dialog box from the main ASDM application window, choose one of the following:

- **Configuration > Device Management > Management Access > HTTPS/ASDM**.
- **Configuration > Device Management > Management Access > Command-Line (CLI)> Telnet**.
- **Configuration > Device Management > Management Access > Command-Line (CLI) > Secure Shell (SSH)**.
- **Configuration > Device Management > Advanced > History Metrics**.

To add or edit the host configuration, perform the following steps:

Step 1 Specify one of the types of preconfigured connections—ASDM/HTTPS, SSH, or Telnet—for the CLI console sessions from the drop-down list.

Note ASDM uses HTTP over SSL for all communication with the FWSM.

Step 2 Choose from a drop-down list of predetermined interfaces (for example, inside or outside).

Step 3 Specify an IP address for the interface.

Step 4 Choose the subnet mask IP address for the interface from a drop-down list, and then click **OK** to close this dialog box.

Modes

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

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

Startup Wizard Summary

To complete the Startup Wizard, perform the following steps:

Step 1 To change any of the settings in previous screens, click **Back**.

Step 2 If you started the Startup Wizard directly from a browser, when you click **Finish**, the configuration that you created through the wizard is sent to the FWSM and saved in flash memory automatically. If you ran the Startup Wizard from within ASDM, you must explicitly save the configuration in flash memory.

Step 3 To exit the wizard, click **Finish**.

Modes

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

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