Security, Internet Access, and Communication Ports

To safeguard the ASA FirePOWER module, you should install it on a protected internal network. Although the ASA FirePOWER module is configured to have only the necessary services and ports available, you must make sure that attacks cannot reach it from outside the firewall.

Also note that specific features of the ASA FirePOWER module require an Internet connection. By default, the ASA FirePOWER module is configured to directly connect to the Internet. Additionally, the system requires certain ports remain open for secure appliance access and so that specific system features can access the local or Internet resources to operate correctly.

For more information, see:

Internet Access Requirements

By default, the ASA FirePOWER module is configured to directly connect to the Internet on ports 443/tcp (HTTPS) and 80/tcp (HTTP), which are open by default on the ASA FirePOWER module; see Communication Ports Requirements, page D-2.

The following table describes the Internet access requirements of specific features of the ASA FirePOWER module.

Table D-1 ASA FirePOWER module Feature Internet Access Requirements

Feature	Internet access is required to...
intrusion rule, VDB, and GeoDB updates	download or schedule the download of a intrusion rule, GeoDB, or VDB update directly to an appliance.
network-based AMP	perform malware cloud lookups.
Security Intelligence filtering	download Security Intelligence feed data from an external source, including the Intelligence Feed.
system software updates	download or schedule the download of a system update directly to an appliance.

Table D-1 ASA FirePOWER module Feature Internet Access Requirements (continued)

Feature	Internet access is required to...
URL filtering	download cloud-based URL category and reputation data for access control, and perform lookups for uncategorized URLs.
whois	request whois information for an external host.

Communication Ports Requirements

Open ports allow:

- access to an appliance's user interface
- secure remote connections to an appliance
- certain features of the system to access the local or Internet resources they need to function correctly

In general, feature-related ports remain closed until you enable or configure the associated feature.

Caution Do **not** close an open port until you understand how this action will affect your deployment.

For example, closing port 25/tcp (SMTP) outbound on a manage device blocks the device from sending email notifications for individual intrusion events (see Configuring External Alerting for Intrusion Rules, page 39-1).

The following table lists the open ports required so that you can take full advantage of ASA FirePOWER module features.

Table D-2 Default Communication Ports for ASA FirePOWER module Features and Operations

Port	Description	Direction	Is Open to...
22/tcp	SSH/SSL	Bidirectional	allow a secure remote connection to the appliance.
25/tcp	SMTP	Outbound	send email notices and alerts from the appliance.
53/tcp	DNS	Outbound	use DNS.
67/udp 68/udp	DHCP	Outbound	use DHCP. **Note** These ports are **closed** by default.
		Bidirectional	update custom and third-party Security Intelligence feeds via HTTP. download URL category and reputation data (port 443 also required).
161/udp	SNMP	Bidirectional	allow access to an appliance's MIBs via SNMP polling.
162/udp	SNMP	Outbound	send SNMP alerts to a remote trap server.
389/tcp 636/tcp	LDAP	Outbound	communicate with an LDAP server for external authentication.
389/tcp 636/tcp	LDAP	Outbound	obtain metadata for detected LDAP users.

Table D-2 Default Communication Ports for ASA FirePOWER module Features and Operations

Port	Description	Direction	Is Open to...
443/tcp	HTTPS	Inbound	access an appliance's user interface.
443/tcp	HTTPS cloud comms.	Bidirectional	obtain: • software, intrusion rule, VDB, and GeoDB updates • URL category and reputation data (port 80 also required) • the Intelligence Feed and other secure Security Intelligence feeds • malware dispositions for files detected in network traffic
			download software updates using the device's local user interface.
514/udp	syslog	Outbound	send alerts to a remote syslog server.
8305/tcp	appliance comms.	Bidirectional	securely communicate between appliances in a deployment. **Required.**
8307/tcp	host input client	Bidirectional	communicate with a host input client.