



## Security, Internet Access, and Communication Ports

---

To safeguard the Defense Center, you should install it on a protected internal network. Although the Defense Center is configured to have only the necessary services and ports available, you must make sure that attacks cannot reach it (or any managed devices) from outside the firewall.

If the Defense Center and its managed devices reside on the same network, you can connect the management interfaces on the devices to the same protected internal network as the Defense Center. This allows you to securely control the devices from the Defense Center. You can also configure multiple management interfaces to allow the Defense Center to manage and isolate traffic from devices on other networks.

Regardless of how you deploy your appliances, intra-appliance communication is encrypted. However, you must still take steps to ensure that communications between FireSIGHT System appliances cannot be interrupted, blocked, or tampered with; for example, with a distributed denial of service (DDoS) or man-in-the-middle attack.

Also note that specific features of the FireSIGHT System require an Internet connection. By default, all FireSIGHT System appliances are configured to directly connect to the Internet. Additionally, the system requires certain ports remain open for basic intra-appliance communication, for secure appliance access, and so that specific system features can access the local or Internet resources they need to operate correctly.



**Tip**

---

With the exception of Cisco NGIPS for Blue Coat X-Series, FireSIGHT System appliances support the use of a proxy server. For more information, see [Configuring Management Interfaces, page 64-8](#) and [http-proxy, page D-35](#).

---

For more information, see:

- [Internet Access Requirements, page E-2](#)
- [Communication Ports Requirements, page E-3](#)

# Internet Access Requirements

By default, FireSIGHT System appliances are configured to directly connect to the Internet on ports 443/tcp (HTTPS) and 80/tcp (HTTP), which are open by default on all FireSIGHT System appliances; see [Communication Ports Requirements, page E-3](#). Note that most FireSIGHT System appliances support use of a proxy server; see [Configuring Management Interfaces, page 64-8](#). Note also that a proxy server cannot be used for whois access.

To ensure continuity of operations, both Defense Centers in a high availability pair must have Internet access. For specific features, the primary Defense Center contacts the Internet, then shares information with the secondary during the synchronization process. Therefore, if the primary fails, you should promote the secondary to Active as described in [Monitoring and Changing High Availability Status, page 4-15](#).

The following table describes the Internet access requirements of specific features of the FireSIGHT System.

**Table E-1** *FireSIGHT System Feature Internet Access Requirements*

| Feature                                | Internet access is required to...  | Appliances                              | High Availability Considerations  |
|--|--|---|---|
| dynamic analysis: querying             | query the cloud for threat scores of files previously submitted for dynamic analysis.                  | Defense Center                          | Paired Defense Centers query the cloud for threat scores independently.   |
| dynamic analysis: submitting           | submit files to the cloud for dynamic analysis.  | Any device except Series 2 and X-Series | n/a   |
| FireAMP integration                    | receive endpoint-based (FireAMP) malware events from the Cisco cloud.                                  | Defense Center                          | Cloud connections are not synchronized. Configure them on both Defense Centers.   |
| intrusion rule, VDB, and GeoDB updates | download or schedule the download of an intrusion rule, GeoDB, or VDB update directly to an appliance. | Defense Center                          | Intrusion rule, GeoDB, and VDB updates are synchronized.  |
| network-based AMP                      | perform malware cloud lookups.   | Defense Center                          | Paired Defense Centers perform cloud lookups independently.   |
| RSS feed dashboard widget              | download RSS feed data from an external source, including Cisco.                                       | Any except virtual devices and X-Series | Feed data is not synchronized.  |
| Security Intelligence filtering        | download Security Intelligence feed data from an external source, including the Intelligence Feed.     | Defense Center                          | The primary Defense Center downloads feed data and shares it with the secondary. In case of primary failure, promote the secondary to active. |
| system software updates                | download or schedule the download of a system update directly to an appliance.                         | Any except virtual devices and X-Series | System updates are not synchronized.  |

Table E-1 FireSIGHT System Feature Internet Access Requirements (continued)

| Feature       | Internet access is required to...   | Appliances                              | High Availability Considerations   |
|---------------|---|---|--|
| URL filtering | download cloud-based URL category and reputation data for access control, and perform lookups for uncategorized URLs. | Defense Center                          | The primary Defense Center downloads URL filtering data and shares it with the secondary. In case of primary failure, promote the secondary to active. |
| whois         | request whois information for an external host.   | Any except virtual devices and X-Series | Any appliance requesting whois information must have Internet access.  |

## Communication Ports Requirements

FireSIGHT System appliances communicate using a two-way, SSL-encrypted communication channel, which by default uses port 8305/tcp. The system **requires** this port remain open for basic intra-appliance communication. Other open ports allow:

- access to an appliance's web 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. For example, until you connect the Defense Center to a User Agent, the agent communications port (3306/tcp) remains closed. As another example, port 623/udp remains closed on Series 3 appliances until you enable LOM.



### 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 44-1](#)). As another example, you can disable access to a physical managed device's web interface by closing port 443/tcp (HTTPS), but this also prevents the device from submitting suspected malware files to the cloud for dynamic analysis.

Note that the system allows you to change some of its communication ports:

- You can specify custom ports for LDAP and RADIUS authentication when you configure a connection between the system and the authentication server; see [Identifying the LDAP Authentication Server, page 61-18](#) and [Configuring RADIUS Connection Settings, page 61-34](#).
- You can change the management port (8305/tcp); see [Configuring Management Interfaces, page 64-8](#). However, Cisco **strongly** recommends that you keep the default setting. If you change the management port, you must change it for all appliances in your deployment that need to communicate with each other.
- You can use port 32137/tcp to allow upgraded Defense Centers to communicate with the Cisco cloud. However, Cisco recommends you switch to port 443, which is the default for fresh installations of Version 5.3 and later. For more information, see [Enabling Cloud Communications, page 64-27](#).

The following table lists the open ports required by each appliance type so that you can take full advantage of FireSIGHT System features.

**Table E-2** *Default Communication Ports for FireSIGHT System Features and Operations*

| Port    | Description                   | Direction     | Is Open on...                           | To...  |
|---------|-------------------------------|---------------|---|--|
| 22/tcp  | SSH/SSL                       | Bidirectional | Any                                     | allow a secure remote connection to the appliance.   |
| 25/tcp  | SMTP                          | Outbound      | Any                                     | send email notices and alerts from the appliance.  |
| 53/tcp  | DNS                           | Outbound      | Any                                     | use DNS.   |
| 67/udp  | DHCP                          | Outbound      | Any except X-Series                     | use DHCP.  |
| 68/udp  |                               |               |   | <b>Note</b> These ports are <b>closed</b> by default.  |
| 80/tcp  | HTTP                          | Outbound      | Any except virtual devices and X-Series | allow the RSS Feed dashboard widget to connect to a remote web server.   |
|         |                               | Bidirectional | Defense Center                          | update custom and third-party Security Intelligence feeds via HTTP.<br>download URL category and reputation data (port 443 also required).   |
| 161/udp | SNMP                          | Bidirectional | Any except X-Series                     | allow access to an appliance's MIBs via SNMP polling.  |
| 162/udp | SNMP                          | Outbound      | Any                                     | send SNMP alerts to a remote trap server.  |
| 389/tcp | LDAP                          | Outbound      | Any except virtual devices and X-Series | communicate with an LDAP server for external authentication.   |
| 636/tcp |                               |               |   |  |
| 389/tcp | LDAP                          | Outbound      | Defense Center                          | obtain metadata for detected LDAP users.   |
| 636/tcp |                               |               |   |  |
| 443/tcp | HTTPS                         | Inbound       | Any except virtual devices and X-Series | access an appliance's web interface.   |
| 443/tcp | HTTPS<br>AMQP<br>cloud comms. | Bidirectional | Defense Center                          | obtain: <ul style="list-style-type: none"> <li>software, intrusion rule, VDB, and GeoDB updates</li> <li>URL category and reputation data (port 80 also required)</li> <li>the Intelligence Feed and other secure Security Intelligence feeds</li> <li>endpoint-based (FireAMP) malware events</li> <li>malware dispositions for files detected in network traffic</li> <li>dynamic analysis information on submitted files</li> </ul> |
|         |                               |               | Series 2 and Series 3 devices           | download software updates using the device's local web interface.  |
|         |                               |               | Series 3 and virtual devices            | submit files to for dynamic analysis.  |
| 514/udp | syslog                        | Outbound      | Any                                     | send alerts to a remote syslog server.   |

Table E-2 Default Communication Ports for FireSIGHT System Features and Operations (continued)

| Port                 | Description       | Direction     | Is Open on...                           | To...  |
|----------------------|-------------------|---------------|---|--|
| 623/udp              | SOL/LOM           | Bidirectional | Series 3                                | allow you to perform Lights-Out Management using a Serial Over LAN (SOL) connection.           |
| 1500/tcp<br>2000/tcp | database access   | Inbound       | Defense Center                          | allow read-only access to the database by a third-party client.                                |
| 1812/udp<br>1813/udp | RADIUS            | Bidirectional | Any except virtual devices and X-Series | communicate with a RADIUS server for external authentication and accounting.                   |
| 3306/tcp             | User Agent        | Inbound       | Defense Center                          | communicate with User Agents.  |
| 8302/tcp             | eStreamer         | Bidirectional | Any except virtual devices and X-Series | communicate with an eStreamer client.  |
| 8305/tcp             | appliance comms.  | Bidirectional | Any                                     | securely communicate between appliances in a deployment. <b>Required.</b>                      |
| 8307/tcp             | host input client | Bidirectional | Defense Center                          | communicate with a host input client.  |
| 32137/tcp            | cloud comms.      | Bidirectional | Defense Center                          | allow upgraded Defense Centers to communicate with the Collective Security Intelligence Cloud. |

