Introduction to the FireSIGHT System

The Cisco FireSIGHT® System combines the security of an industry-leading network intrusion protection system with the power to control access to your network based on detected applications, users, and URLs. You can also use FireSIGHT System appliances to serve in a switched, routed, or hybrid (switched and routed) environment; to perform network address translation (NAT); and to build secure virtual private network (VPN) tunnels between the virtual routers of FirePOWER managed devices.

The FireSIGHT Defense Center® provides a centralized management console and database repository for the FireSIGHT System. Managed devices installed on network segments monitor traffic for analysis.

Devices in a passive deployment monitor traffic flowing across a network, for example, using a switch SPAN, virtual switch, or mirror port. Passive sensing interfaces receive all traffic unconditionally and no traffic received on these interfaces is retransmitted.

Devices in an inline deployment allow you to protect your network from attacks that might affect the availability, integrity, or confidentiality of hosts on the network. Inline interfaces receive all traffic unconditionally, and traffic received on these interfaces is retransmitted unless explicitly dropped by some configuration in your deployment. Inline devices can be deployed as a simple intrusion prevention system. You can also configure inline devices to perform access control as well as manage network traffic in other ways.

This installation guide provides information about deploying, installing, and setting up FireSIGHT System appliances (devices and Defense Centers). It also contains hardware specifications and safety and regulatory information for FireSIGHT System appliances.

Tip You can host virtual Defense Centers and devices, which can manage and be managed by physical appliances. However, virtual appliances do not support any of the system's hardware-based features: redundancy, switching, routing, and so on. For detailed information, see the *FireSIGHT System Virtual Installation Guide*.

The topics that follow introduce you to the FireSIGHT System and describe its key components:

FireSIGHT System Appliances

A FireSIGHT System *appliance* is either a traffic-sensing managed *device* or a managing *Defense Center*:

Physical devices are fault-tolerant, purpose-built network appliances available with a range of throughputs and capabilities. Defense Centers serve as central management points for these devices, and automatically aggregate and correlate the events they generate. There are several *models* of each physical appliance type; these models are further grouped into *series* and *family*. Many FireSIGHT System capabilities are appliance dependent.

Defense Centers

A Defense Center provides a centralized management point and event database for your FireSIGHT System deployment. Defense Centers aggregate and correlate intrusion, file, malware, discovery, connection, and performance data, assessing the impact of events on particular hosts and tagging hosts with indications of compromise. This allows you to monitor the information that your devices report in relation to one another, and to assess and control the overall activity that occurs on your network.

Key features of the Defense Center include:

- device, license, and policy management
- display of event and contextual information using tables, graphs, and charts
- health and performance monitoring
- external notification and alerting
- correlation, indications of compromise, and remediation features for real-time threat response
- custom and template-based reporting

For many physical Defense Centers, a high availability (redundancy) feature can help you ensure continuity of operations.

Managed Devices

Devices deployed on network segments within your organization monitor traffic for analysis. Devices deployed passively help you gain insight into your network traffic. Deployed inline, you can use FirePOWER devices to affect the flow of traffic based on multiple criteria. Depending on model and license, devices:

- gather detailed information about your organization's hosts, operating systems, applications, users, files, networks, and vulnerabilities
- block or allow network traffic based on various network-based criteria, as well as other criteria including applications, users, URLs, IP address reputations, and the results of intrusion or malware inspections
- have switching, routing, DHCP, NAT, and VPN capabilities, as well as configurable bypass interfaces, fast-path rules, and strict TCP enforcement
- have clustering (redundancy) to help you ensure continuity of operations, and stacking to combine resources from multiple devices

You **must** manage FirePOWER devices with a Defense Center.

Appliance Types

The FireSIGHT System can run on fault-tolerant, purpose-built *physical* network appliances available from Cisco. There are several *models* of each Defense Center and managed device; these models are further grouped into *series* and *family*.

Physical managed devices come in a range of throughputs and have a range of capabilities. Physical Defense Center also have a range of device management, event storage, and host and user monitoring capabilities.

You can also deploy the following software-based appliances:

- You can deploy 64-bit *virtual* Defense Centers and *virtual* managed devices as ESXi hosts using the VMware vSphere Hypervisor or vCloud Director environment.
- You can deploy Cisco NGIPS for Blue Coat X-Series on theBlue Coat X-Series platform; this functions as a managed device.

Either type of Defense Center (physical or virtual) can manage any type of device: physical, virtual, Cisco ASA with FirePOWER Services, and Cisco NGIPS for Blue Coat X-Series. Note, however, that many FireSIGHT System capabilities are appliance dependent.

For more information on FireSIGHT System appliances, including the features and capabilities they support, see:

- Series 2 Appliances, page 1-3
- Series 3 Appliances, page 1-4
- Virtual Appliances, page 1-4
- Cisco NGIPS for Blue Coat X-Series, page 1-4
- Cisco ASA with FirePOWER Services, page 1-5
- Appliances Delivered with Version 5.4, page 1-5
- Supported Capabilities by Defense Center Model, page 1-7
- Supported Capabilities by Managed Device Model, page 1-8

Series 2 Appliances

Series 2 is the second series of legacy physical appliances. Because of resource and architecture limitations, Series 2 devices support a restricted set of FireSIGHT System features.

Although Cisco no longer ships new Series 2 appliances, you can update or reimage Series 2 devices and Defense Centers running earlier versions of the system to Version 5.4. Note that reimaging results in the loss of almost **all** configuration and event data on the appliance. For more information, see the *FireSIGHT System Installation Guide*.

Tip You can migrate specific configuration and event data from a Version 4.10.3 deployment to a Version 5.2 deployment, which you can then update to Version 5.4. For more information, see the *Cisco FireSIGHT System Migration Guide* for Version 5.2.

Series 2 devices automatically have most of the capabilities associated with a Protection license: intrusion detection and prevention, file control, and basic access control. However, Series 2 devices cannot perform Security Intelligence filtering, advanced access control, or advanced malware protection, and they cannot inspect the contents of archived files. You also cannot enable other licensed capabilities on a Series 2 device. With the exception of the 3D9900, which supports fast-path rules, stacking, and tap mode, Series 2 devices do not support any of the hardware-based features associated with Series 3 devices: switching, routing, NAT, and so on.

When running Version 5.4, DC1000 and DC3000 Series 2 Defense Centers support all the features of the FireSIGHT System; the DC500 has more limited capabilities.

Series 3 Appliances

Series 3 is the third series of FirePOWER physical appliances. All 7000 Series and 8000 Series devices are Series 3 appliances. 8000 Series devices are more powerful and support a few features that 7000 Series devices do not.

Virtual Appliances

You can deploy 64-bit virtual Defense Center and managed devices as ESXi hosts using the VMware vSphere Hypervisor or vCloud Director environments.

Regardless of the licenses installed and applied, virtual appliances do not support any of the system's hardware-based features: redundancy and resource sharing, switching, routing, and so on. Also, virtual devices do not have web interfaces. For detailed information on virtual appliances, see the *FireSIGHT System Virtual Installation Guide*.

Cisco NGIPS for Blue Coat X-Series

You can install Cisco NGIPS for Blue Coat X-Series on a Blue Coat X-Series platform. This software-based appliance functions similarly to a virtual managed device. Regardless of the licenses installed and applied, Cisco NGIPS for Blue Coat X-Series does not support any of the following features:

- Cisco NGIPS for Blue Coat X-Series does not support the system's hardware-based features: clustering, stacking, switching, routing, VPN, NAT, and so on.
- You cannot use Cisco NGIPS for Blue Coat X-Series to filter network traffic based on its country or continent of origin or destination (geolocation-based access control).
- You cannot use the Defense Center web interface to configure Cisco NGIPS for Blue Coat X-Series interfaces.
- You cannot use the Defense Center to shut down, restart, or otherwise manage Cisco NGIPS for Blue Coat X-Series processes.
- You cannot use the Defense Center to create backups from or restore backups to Cisco NGIPS for Blue Coat X-Series.
- You cannot apply health or system policies to Cisco NGIPS for Blue Coat X-Series. This includes managing time settings.

Cisco NGIPS for Blue Coat X-Series does not have a web interface. However, it has a command line interface (CLI) unique to the X-Series platform. You use this CLI to install the system and to perform other platform-specific administrative tasks, such as:

- creating Virtual Appliance Processor (VAP) groups, which allow you to take advantage of the X-Series platform's load balancing and redundancy benefits (comparable to Cisco physical device clustering)
- configuring passive and inline sensing interfaces, including configuring the interface's maximum transmission unit (MTU)
- managing processes
- managing time settings, including NTP settings

Cisco ASA with FirePOWER Services

You can manage Cisco ASA with FirePOWER Services (ASA FirePOWER) devices with a Defense Center. In this deployment, the ASA device provides the first-line system policy and passes traffic to the FireSIGHT System for access control, intrusion detection and prevention, discovery, and advanced malware protection. See the Version 5.4 FireSIGHT System Appliances table for a list of supported ASA models.

Regardless of the licenses installed and applied, ASA FirePOWER devices do not support any of the following features through the FireSIGHT System:

- ASA FirePOWER devices do not support the FireSIGHT System's hardware-based features: clustering, stacking, switching, routing, VPN, NAT, and so on. However, the ASA platform does provide these features, which you can configure using the ASA CLI and ASDM. See the ASA documentation for more information.
- You cannot use the Defense Center web interface to configure ASA FirePOWER interfaces.
- You cannot use the Defense Center to shut down, restart, or otherwise manage ASA FirePOWER processes.
- You cannot use the Defense Center to create backups from or restore backups to ASA FirePOWER devices.
- You cannot write access control rules to match traffic using VLAN tag conditions.

The ASA FirePOWER device does not have a FireSIGHT web interface. However, it has software and a command line interface (CLI) unique to the ASA platform. You use these ASA-specific tools to install the system and to perform other platform-specific administrative tasks. See the ASA FirePOWER module documentation for more information.

The ASA FirePOWER module also includes the CLI for FirePOWER appliances. You can use the CLI to view, configure, and troubleshoot your FireSIGHT System. See the *FireSIGHT System User Guide* for more information.

Appliances Delivered with Version 5.4

The following table lists the appliances that Cisco delivers with Version 5.4 of the FireSIGHT System.

Table 1-1 Version 5.4 FireSIGHT System Appliances

Models/Family	Series	Form	Type
70xx Family: • 3D7010, 3D7020, 3D7030, 3D7050	Series 3 (7000 Series)	hardware	device
71xx Family: • 3D7110, 3D7120 • 3D7115, 3D7125 • AMP7150	Series 3 (7000 Series)	hardware	device
81xx Family: • 3D8120, 3D8130, 3D8140 • AMP8150	Series 3 (8000 Series)	hardware	device

Table 1-1 Version 5.4 FireSIGHT System Appliances (continued)

Models/Family	Series	Form	Type
82xx Family: • 3D8250 • 3D8260, 3D8270, 3D8290	Series 3 (8000 Series)	hardware	device
83xx Family: • 3D8350 • 3D8360, 3D8370, 3D8390	Series 3 (8000 Series)	hardware	device
64-bit virtual devices	n/a	software	device
Cisco NGIPS for Blue Coat X-Series	n/a	software	device
ASA FirePOWER: • ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, ASA5585-X-SSP-60	n/a	hardware	device
ASA FirePOWER: • ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X	n/a	software	device
Series 3 Defense Centers: • DC750, DC1500, DC3500, DC4000	Series 3	hardware	Defense Center
64-bit virtual Defense Centers	n/a	software	Defense Center

Although Cisco no longer ships new Series 2 appliances, you can update or reimage the following Series 2 devices and Defense Centers running earlier versions of the system to Version 5.4.

- 3D500, 3D1000, and 3D2000
- 3D2100, 3D2500, 3D3500, 3D4500
- 3D6500
- 3D9900
- DC500, DC1000, DC3000

Note that reimaging results in the loss of **all** configuration and event data on the appliance. See Restoring a FireSIGHT System Appliance to Factory Defaults, page 8-1 for more information.

Tip You can migrate specific configuration and event data from a Version 4.10.3 deployment to a Version 5.2 deployment, which you can then update to Version 5.4. For more information, see the *FireSIGHT System Migration Guide* for Version 5.2.

Supported Capabilities by Defense Center Model

When running Version 5.4, all Defense Centers have similar capabilities, with only a few model-based restrictions. The following table matches the major capabilities of the system with the Defense Centers that support those capabilities, assuming you are managing devices that support those features and have the correct licenses installed and applied.

In addition to the capabilities listed in the table, Defense Center models vary in terms of how many devices they can manage, how many events they can store, and how many hosts and users they can monitor. For more information, see the *FireSIGHT System User Guide*.

Also, keep in mind that although you can use any model of Defense Center running Version 5.4 of the system to manage any Version 5.4 device, many system capabilities are limited by the device model. For example, even if you have a Series 3 Defense Center, you cannot implement VPN unless your deployment also includes Series 3 devices. For more information, see Supported Capabilities by Managed Device Model, page 1-8.

Table 1-2 Supported Capabilities by Defense Center Model

Feature or Capability	Series 2 Defense Center	Series 3 Defense Center	VirtualDefense Center
collect discovery data (host, application, and user) reported by managed devices and build a network map for your organization	yes	yes	yes
view geolocation data for your network traffic	DC1000, DC3000	yes	yes
manage an intrusion detection and prevention (IPS) deployment	yes	yes	yes
manage devices performing Security Intelligence filtering	DC1000, DC3000	yes	yes
manage devices performing simple network-based control, including geolocation-based filtering	yes	yes	yes
manage devices performing application control	yes	yes	yes
manage devices performing user control	DC1000, DC3000	yes	yes
manage devices that filter network traffic by literal URL	yes	yes	yes
manage devices performing URL Filtering by category and reputation	DC1000, DC3000	yes	yes
manage devices performing simple file control by file type	yes	yes	yes
manage devices performing network-based advanced malware protection (AMP)	DC1000, DC3000	yes	yes
receive endpoint-based malware (FireAMP) events from your FireAMP deployment	yes	yes	yes
manage device-based hardware-based features: • fast-path rules • strict TCP enforcement • configurable bypass interfaces • tap mode • switching and routing • NAT policies • VPN	yes	yes	yes

Table 1-2 Supported Capabilities by Defense Center Model (continued)

Feature or Capability	Series 2 Defense Center	Series 3 Defense Center	VirtualDefense Center
manage device-based redundancy and resource sharing: • device stacks • device clusters • Cisco NGIPS for Blue Coat X-Series VAP groups • clustered stacks	yes	yes	yes
separate and manage internal and external traffic using traffic channels	no	yes	yes
isolate and manage traffic on different networks using multiple management interfaces	no	yes	yes
establish high availability	DC1000, DC3000	DC1500, DC3500, DC4000	no
install a malware storage pack	DC1000, DC3000	yes	no
connect to an eStreamer, host input, or database client	yes	yes	yes

Supported Capabilities by Managed Device Model

Devices are the appliances that handle network traffic; therefor, many FireSIGHT System capabilities are dependent on the model of your managed devices.

The following table matches the major capabilities of the system with the devices that support those capabilities, assuming you have the correct licenses installed and applied from the managing Defense Center.

Keep in mind that although you can use any model of Defense Center running Version 5.4 of the system to manage any Version 5.4 device, a few system capabilities are limited by the Defense Center model. For example, you cannot use the Series 2 DC500 to manage devices performing Security Intelligence filtering, even if the devices support that capability. For more information, see Supported Capabilities by Defense Center Model, page 1-7.

Table 1-3 Supported Capabilities by Managed Device Model

Feature or Capability	Series 2 Device	Series 3 Device	ASA FirePOWER	Virtual Device	X-Series
network discovery: host, application, and user	yes	yes	yes	yes	yes
intrusion detection and prevention (IPS)	yes	yes	yes	yes	yes
Security Intelligence filtering	no	yes	yes	yes	yes
access control: basic network control	yes	yes	yes	yes	yes
access control: geolocation-based filtering	no	yes	yes	yes	no
access control: application control	no	yes	yes	yes	yes
access control: user control	no	yes	yes	yes	yes
access control: literal URLs	no	yes	yes	yes	yes

Table 1-3 Supported Capabilities by Managed Device Model (continued)

Feature or Capability	Series 2 Device	Series 3 Device	ASA FirePOWER	Virtual Device	X-Series
access control: URL Filtering by category and reputation	no	yes	yes	yes	yes
file control: by file type	yes	yes	yes	yes	yes
network-based advanced malware protection (AMP)	no	yes	yes	yes	no
Automatic Application Bypass	yes	yes	no	yes	no
fast-path rules	3D9900	8000 Series	no	no	no
strict TCP enforcement	no	yes	no	no	no
configurable bypass interfaces	yes	except where hardware limited	no	no	no
tap mode	3D9900	yes	no	no	no
switching and routing	no	yes	no	no	no
NAT policies	no	yes	no	no	no
VPN	no	yes	no	no	no
device stacking	3D9900	3D8140 82xx Family 83xx Family	no	no	no
device clustering	no	yes	no	no	no
clustered stacks	no	3D8140 82xx Family 83xx Family	no	no	no
traffic channels	no	yes	no	no	no
multiple management interfaces	no	yes	no	no	no
malware storage pack	no	yes	no	no	no
restricted command line interface (CLI)	no	yes	yes	yes	no
external authentication	yes	yes	no	no	no
connect to an eStreamer client	yes	yes	yes	no	no

Series 3 Device Chassis Designations

The following section lists the 7000 Series and 8000 Series devices and their respective chassis hardware codes. The chassis code appears on the regulatory label on the outside of the chassis, and is the official reference code for hardware certifications and safety.

7000 Series Chassis Designations

The following table lists the chassis designations for the 7000 Series models available world-wide.

Table 1-4 7000 Series Chassis Models

3D Device Model	Hardware Chassis Code
3D7010, 3D7020, 3D7030	CHRY-1U-AC
3D7050	NEME-1U-AC
3D7110, 3D7120 (Copper)	GERY-1U-8-C-AC
3D7110, 3D7120 (Fiber)	GERY-1U-8-FM-AC
3D7115, 3D7125, AMP7150	GERY-1U-4C8S-AC

8000 Series Chassis Designations

The following table lists the chassis designations for the Series 3 models available world-wide.

Table 1-5 8000 Series Chassis Models

3D Device Model	Hardware Chassis Code
3D8120, 3D8130, 3D8140, AMP8150 (AC power)	CHAS-1U-AC
3D8120, 3D8130, 3D8140, AMP8150 (DC power)	CHAS-1U-DC
3D8250, 3D8260, 3D8270, 3D8290 (AC power)	CHAS-2U-AC
3D8250, 3D8260, 3D8270, 3D8290 (DC power)	CHAS-2U-DC
3D8350, 3D8360, 3D8370, 3D8390 (AC/DC power)	PG35-2U-AC/DC

FireSIGHT System Components

The sections that follow describe some of the key capabilities of the FireSIGHT System that contribute to your organization's security, acceptable use policy, and traffic management strategy.

Tip Many FireSIGHT System capabilities are appliance model, license, and user role dependent. Where needed, FireSIGHT System documentation outlines the requirements for each feature and task.

Redundancy and Resource Sharing

The redundancy and resource-sharing features of the FireSIGHT System allow you to ensure continuity of operations and to combine the processing resources of multiple physical devices:

- Defense Center high availability allows you to designate redundant DC1000, DC1500, DC3000, DC3500, or DC4000 Defense Centers to manage devices.
- Device stacking allows you to increase the amount of traffic inspected on a network segment by connecting two to four physical devices in a stacked configuration.
- Device clustering allows you to establish redundancy of networking functionality and configuration data between two or more Series 3 devices or stacks.

Multiple Management Interfaces

You can use *multiple management interfaces* on a Defense Center, device, or both, to improve performance by separating traffic into two traffic channels: the *management traffic channel* carries inter-device communication and the *event traffic channel* carries high volume event traffic such as intrusion events. Both traffic channels can be carried on the same management interface or split between two management interfaces, each interface carrying one traffic channel.

You can also create a route from a specific management interface on your Defense Center to a different network, allowing your Defense Center to isolate and manage device traffic on one network separately from device traffic on another network.

Additional management interfaces have many of the same capabilities as the default management interface (such as using high availability between the Defense Centers) with the following exceptions:

- You can configure DHCP on the default (`eth0`) management interface only. Additional (`eth1` and so on) interfaces require unique static IP addresses and hostnames.
- You must configure both traffic channels to use the same non-default management interface when your Defense Center and managed device are separated by a NAT device.
- You can use Lights-Out Management on the default management interface only.
- On the 70xx Family, you can separate traffic into two channels and configure those channels to send traffic to one or more management interfaces on the Defense Center. However, because the 70xx Family contains only one management interface, the device receives traffic sent from the Defense Center on only one management interface.

After your appliance installed, use the web browser to configure multiple management interfaces. See Multiple Management Interfaces in the *FireSIGHT System User Guide* for more information.

Network Traffic Management

The FireSIGHT System's network traffic management features allow Series 3 devices to act as part of your organization's network infrastructure. You can:

- configure a Layer 2 deployment to perform packet switching between two or more network segments
- configure a Layer 3 deployment to route traffic between two or more interfaces
- perform network address translation (NAT)
- build secure VPN tunnels from virtual routers on managed devices to remote devices or other third-party VPN endpoints

FireSIGHT

FireSIGHT™ is Cisco's discovery and awareness technology that collects information about hosts, operating systems, applications, users, files, networks, geolocation information, and vulnerabilities, in order to provide you with a complete view of your network.

You can use the Defense Center's web interface to view and analyze data collected by FireSIGHT. You can also use this data to help you perform access control and modify intrusion rule states. In addition, you can generate and track indications of compromise on hosts on your network based on correlated event data for the hosts.

Access Control

Access control is a policy-based feature that allows you to specify, inspect, and log the traffic that traverses your network. As part of access control, the Security Intelligence feature allows you to blacklist—deny traffic to and from—specific IP addresses before the traffic is subjected to deeper analysis.

After Security Intelligence filtering occurs, you can define which and how traffic is handled by targeted devices, from simple IP address matching to complex scenarios involving different users, applications, ports, and URLs. You can trust, monitor, or block traffic, or perform further analysis, such as:

- intrusion detection and prevention
- file control
- file tracking and network-based advanced malware protection (AMP)

Intrusion Detection and Prevention

Intrusion detection and prevention is a policy-based feature, integrated into access control, that allows you to monitor your network traffic for security violations and, in inline deployments, to block or alter malicious traffic. An intrusion policy contains a variety of components, including:

- rules that inspect the protocol header values, payload content, and certain packet size characteristics
- rule state configuration based on FireSIGHT recommendations
- advanced settings, such as preprocessors and other detection and performance features
- preprocessor rules that allow you to generate events for associated preprocessors and preprocessor options

File Tracking, Control, and Network-Based Advanced Malware Protection (AMP)

To help you identify and mitigate the effects of malware, the FireSIGHT System's file control, network file trajectory, and advanced malware protection components can detect, track, capture, analyze, and optionally block the transmission of files (including malware files) in network traffic.

File control is a policy-based feature, integrated into access control, that allows managed devices to detect and block your users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols.

Network-based *advanced malware protection* (AMP) allows the system to inspect network traffic for malware in several types of files. Appliances can store detected files for further analysis, either to their hard drive or (for some models) a malware storage pack.

Regardless of whether you store a detected file, you can submit it to the Cisco cloud for a simple known-disposition lookup using the files SHA-256 hash value. You can also submit files for *dynamic analysis*, which produces a threat score. Using this contextual information, you can configure the system to block or allow specific files.

FireAMP is Cisco's enterprise-class, advanced malware analysis and protection solution that discovers, understands, and blocks advanced malware outbreaks, advanced persistent threats, and targeted attacks. If your organization has a FireAMP subscription, individual users install FireAMP Connectors on their computers and mobile devices (also called endpoints). These lightweight agents communicate with the Cisco cloud, which in turn communicates with the Defense Center.

After you configure the Defense Center to connect to the cloud, you can use the Defense Center web interface to view endpoint-based malware events generated as a result of scans, detections, and quarantines on the endpoints in your organization. The Defense Center also uses FireAMP data to generate and track indications of compromise on hosts, as well as display network file trajectories.

The network file trajectory feature allows you to track a file's transmission path across a network. The system uses SHA-256 hash values to track files. Each file has an associated trajectory map, which contains a visual display of the file's transfers over time as well as additional information about the file.

Application Programming Interfaces

There are several ways to interact with the system using application programming interfaces (APIs):

- The Event Streamer (eStreamer) allows you to stream several kinds of event data from a FireSIGHT System appliance to a custom-developed client application.
- The database access feature allows you to query several database tables on a Defense Center, using a third-party client that supports JDBC SSL connections.
- The host input feature allows you to augment the information in the network map by importing data from third-party sources using scripts or command-line files.
- Remediations are programs that your Defense Center can automatically launch when certain conditions on your network are met. This can not only automatically mitigate attacks when you are not immediately available to address them, but can also ensure that your system remains compliant with your organization's security policy.

Licensing the FireSIGHT System

You can license a variety of features to create an optimal FireSIGHT System deployment for your organization. You must use the Defense Center to control licenses for itself and the devices it manages.

Cisco recommends you add the licenses your organization has purchased during the initial setup of your Defense Center. Otherwise, any devices you register during initial setup are added to the Defense Center as unlicensed. You must then enable licenses on each device individually after the initial setup process is over. For more information, see Setting Up a FireSIGHT System Appliance, page 5-1.

A FireSIGHT license is included with each Defense Center purchase, and is required to perform host, application, and user discovery. The FireSIGHT license on your Defense Center also determines how many individual hosts and users you can monitor with the Defense Center and its managed devices, as well as how many users you can use to perform user control. FireSIGHT host and user license limits are model specific, as listed in the following table.

Table 1-6 FireSIGHT Limits by Defense Center Model

Defense Center Model	FireSIGHT Host and User Limit
DC500	1000 (no user control)
DC750	2000
DC1000	20,000
DC1500	50,000
DC3000	100,000
DC3500	300,000
DC4000	600,000

If your Defense Center was previously running Version 4.10.x, you may be able to use legacy RNA Host and RUA User licenses instead of a FireSIGHT license. For more information, see Using Legacy RNA Host and RUA User Licenses, page 1-16.

Additional model-specific licenses allow your managed devices to perform a variety of functions, as follows:

Protection

A Protection license allows managed devices to perform intrusion detection and prevention, file control, and Security Intelligence filtering.

Control

A Control license allows managed devices to perform user and application control. It also allows devices to perform switching and routing (including DHCP relay), NAT, and to cluster devices and stacks. A Control license requires a Protection license.

URL Filtering

A URL Filtering license allows managed devices to use regularly updated cloud-based category and reputation data to determine which traffic can traverse your network, based on the URLs requested by monitored hosts. A URL Filtering license requires a Protection license.

Malware

A Malware license allows managed devices to perform network-based advanced malware protection (AMP), that is, to detect and block malware in files transmitted over your network. It also allows you to view trajectories, which track files transmitted over your network. A Malware license requires a Protection license.

VPN

A VPN license allows you to build secure VPN tunnels among the virtual routers on Cisco managed devices, or from managed devices to remote devices or other third-party VPN endpoints. A VPN license requires Protection and Control licenses.

SSL

An SSL license allows you to perform SSL inspection. If your system detects encrypted traffic, it can block the traffic without further inspection, inspect that traffic with access control, or decrypt the traffic for inspection with access control.

Because of architecture and resource limitations, not all licenses can be applied to all managed devices. In general, you cannot license a capability that a device does not support; see Supported Capabilities by Managed Device Model, page 1-8.

The following table summarizes which licenses you can add to your Defense Center and apply to each device model. The Defense Center rows (for all licenses except FireSIGHT) indicate whether that Defense Center can manage devices using those licenses. For example, you can use a Series 2 DC1000 to create a VPN deployment using Series 3 devices, but you cannot use a DC500 to perform category and reputation-based URL Filtering, regardless of the devices it manages. Note that `n/a` marks Defense Center-based licenses that are not relevant to managed devices.

Table 1-7 Supported Licenses by Model

Models	FireSIGHT	Protection	Control	URL Filtering	Malware	VPN	SSL
Series 2 devices: • 3D500, 3D1000, 3D2000 • 3D2100, 3D2500, 3D3500, 3D4500 • 3D6500 • 3D9900	n/a	automatic, no Security Intelligence	no	no	no	no	no
Series 3 devices: • 7000 Series • 8000 Series	n/a	yes	yes	yes	yes	yes	yes
virtual devices	n/a	yes	yes, but no support for hardware features	yes	yes	no	no
Cisco ASA with FirePOWER Services	n/a	yes	yes, but no support for hardware features	yes	yes	no	no
Cisco NGIPS for Blue Coat X-Series	n/a	yes	yes, but no support for hardware features	yes	yes	no	no
Series 2 Defense Center: • DC500	yes	yes, but no Security Intelligence	yes, but no user control	no	no	yes	no
Series 2 Defense Centers: • DC1000, DC3000	yes	yes	yes	yes	yes	yes	no
Series 3 Defense Centers: • DC750, DC1500, DC3500, DC4000	yes	yes	yes	yes	yes	yes	yes
virtual Defense Centers	yes	yes	yes	yes	yes	yes	no

In addition to the information in the table, note that:

- Series 2 devices automatically have Protection capabilities, with the exception of Security Intelligence filtering.
- Although you can enable a Control license on a virtual device, a virtual device does not support any of the hardware-based features granted by that license, such as switching or routing.
- Although the DC500 can manage devices with Protection and Control licenses, you cannot perform Security Intelligence filtering or user control.

For detailed information on licensing, see the Licensing the FireSIGHT System chapter in the *FireSIGHT System User Guide*.

Using Legacy RNA Host and RUA User Licenses

In Version 4.10.x of the FireSIGHT System, RNA Host and RUA User feature licenses determined your monitored host and user limits, respectively. If your Defense Center was previously running Version 4.10.x, you may be able to use your legacy host and user licenses instead of a FireSIGHT license.

Version 5.4 Defense Centers using legacy licenses use the RNA Host limit as the FireSIGHT host limit and the RUA User limit as both the FireSIGHT user and access-controlled user limit. The FireSIGHT Host License Limit health module alerts appropriately for your licensed limit.

Note that RNA Host and RUA User limits are cumulative. That is, you can add multiple licenses of each type to the Defense Center to monitor the total number of hosts or users allowed by the licenses.

If you later add a FireSIGHT license, the Defense Center uses the higher of the limits. For example, the FireSIGHT license on the DC1500 supports up to 50,000 hosts and users. If the RNA Host limit on your Version 4.10.x DC1500 was higher than 50,000, using that legacy host license on the same Defense Center running Version 5.4 gives you the higher limit. For your convenience, the web interface displays only the licenses that represent the higher limits.

Note Because FireSIGHT license limits are matched to the hardware capabilities of Defense Centers, Cisco does **not** recommend exceeding them when using legacy licensing. For guidance, contact Support.

Because there is no update path from Version 4.10.x to Version 5.4, you must use an ISO image to "restore" the Defense Center. Note that reimaging results in the loss of **all** configuration and event data on the appliance. You **cannot** import this data onto an appliance after a reimage. For more information, see Restoring a FireSIGHT System Appliance to Factory Defaults, page 8-1.

Note Only reimage your appliances during a maintenance window. Reimaging resets devices in an inline deployment to a non-bypass configuration and disrupts traffic on your network until you reconfigure bypass mode. For more information, see Traffic Flow During the Restore Process, page 8-2.

During the restore process, you are prompted to delete license and network settings. Keep these settings, although you can re-add them later if you accidentally delete them. Note that Version 5.4 Defense Centers cannot manage Version 4.10.x devices. You can, however, restore and update supported Version 4.10.x devices to the latest version. For more information, see Restoring a FireSIGHT System Appliance to Factory Defaults, page 8-1.

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 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 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 and Cisco ASA with FirePOWER Services, FireSIGHT System appliances support the use of a proxy server. For more information, see the *FireSIGHT System User Guide*.

For more information, see:

- Internet Access Requirements, page 1-17
- Communication Ports Requirements, page 1-18

Internet Access Requirements

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; see Communication Ports Requirements, page 1-18. Note that most FireSIGHT System appliances support use of a proxy server; see the Configuring Network Settings chapter in the *FireSIGHT System User Guide*. 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 the Managing Devices chapter in the *FireSIGHT System User Guide*.

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

Table 1-8 FireSIGHT System Feature Internet Access Requirements

Feature	Internet access is required to...	Appliances	High Availability Considerations
dynamic analysis: querying	query the Collective Security Intelligence 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 Collective Security Intelligence Cloud for dynamic analysis.	Managed devices	n/a
FireAMP integration	receive endpoint-based (FireAMP) malware events from the Collective Security Intelligence Cloud cloud.	Defense Center	Cloud connections are not synchronized. Configure them on both Defense Centers.

Table 1-8 FireSIGHT System Feature Internet Access Requirements (continued)

Feature	Internet access is required to...	Appliances	High Availability Considerations
intrusion rule, VDB, and GeoDB updates	download or schedule the download of a 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, X-Series, and ASA FirePOWER	Feed data is not synchronized.
Security Intelligence filtering	download Security Intelligence feed data from an external source, including the FireSIGHT System 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, X-Series, and ASA FirePOWER	System updates are not synchronized.
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, X-Series, and ASA FirePOWER	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 the *FireSIGHT System User Guide*). 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 the *FireSIGHT System User Guide*.
- You can change the management port (8305/tcp); see the *FireSIGHT System User Guide*. 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 Collective Security Intelligence Cloud cloud. However, Cisco recommends you switch to port 443, which is the default for fresh installations of Version 5.4 and later. For more information, see the *FireSIGHT System User Guide*.

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

Table 1-9 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 68/udp	DHCP	Outbound	Any except X-Series	use DHCP. **Note** These ports are **closed** by default.
80/tcp	HTTP	Outbound	Any except virtual devices, X-Series, and ASA FirePOWER	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. download URL category and reputation data (port 443 also required).
161/udp	SNMP	Bidirectional	Any except virtual devices, X-Series, and ASA FirePOWER	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 636/tcp	LDAP	Outbound	Any except virtual devices and X-Series	communicate with an LDAP server for external authentication.
389/tcp 636/tcp	LDAP	Outbound	Defense Center	obtain metadata for detected LDAP users.

Table 1-9 Default Communication Ports for FireSIGHT System Features and Operations (continued)

Port	Description	Direction	Is Open on...	To...
443/tcp	HTTPS	Inbound	Any except virtual devices, X-Series, and ASA FirePOWER	access an appliance's web interface.
443/tcp	HTTPS AMQP cloud comms.	Bidirectional	Defense Center	obtain: • software, intrusion rule, VDB, and GeoDB updates • URL category and reputation data (port 80 also required) • the Cisco Intelligence feed and other secure Security Intelligence feeds • endpoint-based (FireAMP) malware events • malware dispositions for files detected in network traffic • dynamic analysis information on submitted files
			Series 2 and Series 3 devices	download software updates using the device's local web interface.
			Series 3, virtual devices, X-Series, and ASA FirePOWER	submit files to the Cisco cloud for dynamic analysis.
514/udp	syslog	Outbound	Any	send alerts to a remote syslog server.
623/udp	SOL/LOM	Bidirectional	Series 3	allow you to perform Lights-Out Management using a Serial Over LAN (SOL) connection.
1500/tcp 2000/tcp	database access	Inbound	Defense Center	allow read-only access to the database by a third-party client.
1812/udp 1813/udp	RADIUS	Bidirectional	Any except virtual devices, X-Series, and ASA FirePOWER	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. **Required.**
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 Cisco cloud.

Preconfiguring Appliances

You can preconfigure multiple appliances devices and Defense Centers in a central location for later deployment at other sites. For considerations when preconfiguring appliances, see Preconfiguring FireSIGHT System Appliances, page E-1.