7000 Series

A group of Series 3 FirePOWER managed devices. The devices in this series include the 70xx Family (the 3D7010, 3D7020, 3D7030, 3D7050 models) and the 71xx Family (the 3D7110, 3D7115, 3D7120, 3D7125, AMP7150 models).

8000 Series

A group of Series 3 FirePOWER managed devices. The devices in this series include the 81xx Family (the 3D8120, 3D8130, 3D8140, AMP8150 models), the 82xx Family (the 3D8250, 3D8260, 3D8270, 3D8290 models), and the 83xx Family (the 3D8350, 3D8360, 3D8370, 3D8390 models). 8000 Series devices are generally more powerful than the 7000 Series devices.

access control

A feature of the FireSIGHT System that allows you to specify, inspect, and log the traffic that can traverse your network. Access control includes the intrusion detection and prevention, file control, and advanced malware protection features, and also determines the traffic you can inspect with the discovery feature.

access control policy

A policy that you apply to managed devices to perform access control on the network traffic monitored by those devices. An access control policy may include multiple access control rules; it also specifies a default action, which determines the handling and logging of traffic that does not meet the criteria of any of those rules. An access control policy can also specify HTTP response page, Security Intelligence, and other advanced settings.

access control rule

A set of conditions the FireSIGHT System uses to examine your monitored network traffic and which allows you to achieve granular access control. Access control rules, which populate an access control policy, may perform simple IP address matching, or may characterize complex connections involving different users, applications, ports, and URLs. The access control rule action determines how the system handles traffic that meets the rule's conditions. Other rule settings determine how (and whether) the connection is logged, and whether an intrusion policy or file policy inspects matching traffic.

access list

A list of IP addresses, configured in the system policy, that represents the hosts that can access an appliance. By default, anyone can access the web interface of an appliance using port 443 (HTTPS), as well as the command line using port 22 (SSH). You can also add SNMP access using port 161.

advanced malware protection

Abbreviated AMP, the FireSIGHT System's network-based malware detection and malware cloud lookup feature. Compare this functionality with FireAMP, Cisco's endpoint-based AMP tool that requires a FireAMP subscription.

advanced setting

A preprocessor or other intrusion policy feature that requires specific expertise to configure. Advanced settings typically require little or no modification and are not common to every deployment.

alert

A notification that the system has generated a specific event. You can alert based on intrusion events (including their impact flags), discovery events, malware events, correlation policy violations, health status changes, and connections logged by specific access control rules. In most cases, you can alert via email, syslog, or SNMP trap.

appliance

A Defense Center or managed device. An appliance can be physical or virtual.

application

A detected network asset, communications method, or HTTP content against which you can write access control rules. The system detects three types of application: application protocol, client application, and web application.

application control

A feature that, as part of access control, allows you to specify which application traffic can traverse your network.

application protocol

A type of application that represents application protocol traffic detected during communications between server and client applications on hosts; for example, SSH or HTTP.

apply

The action you take to have a policy, or changes to that policy, take effect. You apply most policies from the Defense Center to its managed devices; however, you activate and deactivate correlation policies because they do not involve changes to the configuration of managed devices.

ASA FirePOWER

The short name for Cisco ASA with FirePOWER Services.

bypass mode

A characteristic of an inline set that allows traffic to continue flowing if the sensing interfaces in the set fail for any reason.

Cisco ASA with FirePOWER Services

A group of Cisco Adaptive Security Appliance (ASA) managed devices. The devices in this series include the ASA5506-X, ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X, ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, and ASA5585-X-SSP-60 models.

Cisco cloud

Sometimes called *cloud services*, a Cisco-hosted external server where the Defense Center can obtain up-to-date, relevant information including malware, Security Intelligence, and URL filtering data. See also malware cloud lookup.

Cisco Intelligence Feed

A collection of regularly updated lists of IP addresses determined by the Cisco VRT to have a poor reputation. Each list in the feed represents a specific category: open relays, known attackers, bogus IP addresses (bogon), and so on. In an access control policy, you can blacklist any or all of the categories using Security Intelligence. Because the intelligence feed is regularly updated, using it ensures that the system uses up-to-date information to filter your network traffic.

Cisco VRT

Cisco's Vulnerability Research Team.

CLI

See command line interface.

client

Also called a client application, an application that runs on one host and relies on another host (a server) to perform some operation. For example, email clients allow you to send and receive email. When the system detects that a user on a host is using a specific client to access another host, it reports that information in the host profile and network map, including the name and version (if available) of the client.

client application

See client.

clustering

A feature that allows you to achieve redundancy of networking functionality and configuration data between two peer Series 3 devices or stacks. Clustering provides a single logical system for policy applies, system updates, and registration. Compare with high availability, which allows you to configure redundant Defense Centers.

command line interface

A restricted text-based interface on Series 3 and virtual devices. The commands that CLI users can run depend on the users' assigned level of access.

configurable bypass

A characteristic of an inline set that allows you to configure bypass mode.

connection

A monitored session between two hosts. You can log connections detected by managed devices in the access control policy; you configure NetMod connection logging in the network discovery policy.

Context Explorer

A page that displays detailed, interactive graphical information about your monitored network, using intrusion, connection, file, geolocation, malware, and discovery policy. Distinct sections present information in the form of vivid line, bar, pie, and donut graphs, accompanied by detailed lists. You can easily create and apply custom filters to fine-tune your analysis, and you can examine data sections in more detail by clicking or hovering your cursor over graph areas. Compared with a dashboard, which is highly customizable, compartmentalized, and updates in real time, the Context Explorer is manually updated, designed to provide broader context for its data, and has a single, consistent layout designed for active user exploration.

context menu

A pop-up menu, available on many of the pages in the web interface, that you can use as a shortcut for accessing other features in the FireSIGHT System. The contents of the menu depend on several factors, including the page you are viewing, the specific data you are investigating, and your user role. Context menu options include links to intrusion rule, event, and host information; various intrusion rule settings, quick links to the Context Explorer; options to add a host to the Security Intelligence global blacklist or global whitelist by its IP address; and options to add a file to the global whitelist by its SHA-256 hash value.

Control license

A license that allows you to implement user control and application control by adding user and application conditions to access control rules. It also allows you to configure your managed devices to perform switching and routing (including DHCP relay and NAT), as well as clustering managed devices.

correlation

A feature you can use to build a correlation policy that responds in real time to threats on your network. The remediation component of correlation provides a flexible API that allows you to create and upload your own custom remediation modules to respond to policy violations.

custom user role

A user role with specialized access privileges. Custom user roles may have any set of menu-based and system permissions, and may be completely original or based on a predefined user role.

dashboard

A display that provides at-a-glance views of current system status, including data about the events collected and generated by the system. To augment the dashboards delivered with the system, you can create multiple custom dashboards, populated with the dashboard widgets you choose. Compare with the Context Explorer, which offers a broad, brief, and colorful picture of how your monitored network looks and acts.

dashboard widget

A small, self-contained dashboard component that provides insight into an aspect of the FireSIGHT System.

database access

A feature that allows read-only access to the Defense Center database by a third-party client.

decoder

A component of intrusion detection and prevention that places sniffed packets into a format that can be understood by a preprocessor.

default action

As part of an access control policy, determines how to handle traffic that does not meet the conditions of any rule in the policy. When you apply an access control policy that does not contain any access control rules or Security Intelligence settings, the default policy action determines how non-fast-pathed traffic on your network is handled. You can set the default action to block or trust traffic without further inspection, or inspect it with a network discovery policy or intrusion policy.

Defense Center

A central management point that allows you to manage devices and automatically aggregate and correlate the events they generate.

device

A fault-tolerant, purpose-built appliance available in a range of throughputs. Depending on the licensed capabilities you enable on your devices, you can use them to passively monitor traffic to build a comprehensive map of your network assets, application traffic, and user activity, perform intrusion detection and prevention, perform access control, and configure switching and routing. You must manage devices with a Defense Center.

device clustering

See clustering.

device stacking

See stacking.

discovery

A component of the FireSIGHT System that uses managed devices to monitor your network and provide you with a complete, persistent view of your network. Network discovery determines the number and types of hosts (including network devices and mobile devices) on your network, as well as information about the operating systems, active applications, and open ports on those hosts. You can also configure Cisco managed devices to monitor user activity on your network, which allows you to identify the source of policy breaches, attacks, or network vulnerabilities.

discovery policy

See network discovery policy.

endpoint

A computer or mobile device where your users install a FireAMP Connector as part of your organization's advanced malware protection strategy.

eStreamer

A component of the FireSIGHT System that allows you to stream event data from a Defense Center or managed device to external client applications.

event

A collection of details about a specific occurrence that you can view in the event viewer, using workflows. Events may represent attacks on your network, changes in your detected network assets, violations of your organization's security and network use policies, and so on. The system also generates events that contain information about the changing health status of appliances, your use of the web interface, rule updates, and launched remediations. Finally, the system presents certain other information as events, even though these "events" do not represent particular occurrences. For example, you can use the event viewer to view detailed information about detected hosts, applications, and their vulnerabilities.

Event Streamer

See eStreamer.

event traffic channel

See traffic channel.

event viewer

A component of the system that allows you to view and manipulate events. The event viewer uses workflows to present a broad, then a more focused event view that contains only the events of interest to you. You can constrain the events in an event view by drilling down through the workflow, or by using a search.

fast-path rule

A rule that you configure at a device's hardware level, using a limited set of criteria, to allow traffic that does not need to be analyzed to bypass processing.

feed

See Security Intelligence feed.

file control

A feature that, as part of access control, allows you to specify and log the types of files that can traverse your network.

file policy

A policy that the system uses to perform file control and advanced malware protection. Populated by file rules, a file policy is invoked by an access control rule within an access control policy.

file trajectory

See network file trajectory.

file type

A specific type of file format, such as PDF, EXE, or MP3.

FireAMP

Cisco's enterprise-class, endpoint-based, advanced malware analysis and protection solution that discovers, understands, and blocks malware outbreaks, persistent threats, and targeted attacks. If your organization has a FireAMP subscription, individual users install lightweight FireAMP Connectors on endpoints (computers, mobile devices), which then communicate with the Cisco cloud. This allows you to quickly identify and quarantine malware, as well as identify outbreaks when they occur, track their trajectory, understand their effects, and learn how to successfully recover. You can also use the FireAMP portal to create custom protections, block execution of certain applications, and create custom whitelists. Compare with network-based advanced malware protection.

FireAMP Connector

A lightweight agent that users in a subscription-based FireAMP deployment install on endpoints, such as computers and mobile devices. Connectors communicate with the Cisco cloud, exchanging information that allow you to quickly identify and quarantine malware throughout your organization.

FireAMP portal

The website, http://amp.sourcefire.com/, where you can configure your organization's subscription-based FireAMP deployment.

FireAMP subscription

A separately purchased subscription that allows your organization to use FireAMP as an advanced malware protection (AMP) solution. Compare with a Malware license, which you enable on managed devices to perform network-based AMP.

FireSIGHT license

The default license on the Defense Center, which allows you to perform host, application, and user discovery. The FireSIGHT license also determines how many individual hosts and users you can monitor with the Defense Center and its managed devices, as well as the number of access-controlled users you can use in access control rules to perform user control.

GeoDB

See geolocation database.

geolocation

A feature that provides data on the geographical source of routable IP addresses detected in traffic on your monitored network including connection type, internet service provider, and so on. You can see geolocation information which is stored in the geolocation database, in connection events, intrusion events, file events, and malware events, as well as in host profiles.

geolocation database

Also called the GeoDB, a regularly updated database of known geolocation data associated with routable IP addresses.

health module

A test of a particular performance aspect, such as CPU usage or available disk space, of the appliances in your deployment. Health modules, which you enable in a health policy, generate health events when the performance aspects they monitor reach a certain level.

health monitor

A feature that continuously monitors the performance of the appliances in your deployment. The health monitor uses health modules within an applied health policy to test the appliances.

health policy

The criteria used when checking the health of an appliance in your deployment. Health policies use health modules to indicate whether your FireSIGHT System hardware and software are working correctly. You can use the default health policy or create your own.

high availability

A feature that allows you to configure redundant physical Defense Centers to manage groups of devices. Event data streams from managed devices to both Defense Centers and most configuration elements are maintained on both Defense Centers. If your primary Defense Center fails, you can monitor your network without interruption using the secondary Defense Center. Compare with clustering, which allows you to designate redundant devices.

host

A device that is connected to a network and has a unique IP address. To the FireSIGHT System, a host is any identified host that is not categorized as a mobile device, bridge, router, NAT device, or logical interface.

host input

A feature that allows you to import data from third-party sources using scripts or command-line files to augment the information in the network map. The web interface also provides some host input functionality; you can modify operating system or application protocol identities, validate or invalidate vulnerabilities, and delete various items from the network map, including clients and server ports.

hybrid interface

A logical interface on a managed device that allows the system to bridge traffic between a virtual router and a virtual switch.

import

A method that you can use to transfer various configurations from appliance to appliance. You can import configurations that you previously exported from another appliance of the same type.

inline deployment

A deployment of the FireSIGHT System where your managed devices are placed inline on a network. In this configuration, devices can affect network traffic flow using switching, routing, access control, and intrusion detection and prevention.

inline interface

A sensing interface configured to handle traffic in an inline deployment. You must add inline interfaces to inline sets in pairs.

inline set

One or more pairs of inline interfaces.

intrusion

A security breach, attack, or exploit that occurs on your network.

intrusion detection and prevention

The monitoring of your network traffic for security policy violations, and, in inline deployments, the ability to block or alter malicious traffic. In the FireSIGHT System, you perform intrusion detection and prevention when you associate an intrusion policy with an access control rule or default action.

intrusion event

An event that records an intrusion policy violation. Intrusion event data includes the date, time, and the type of exploit, as well as other contextual information about the attack and its target.

intrusion policy

A variety of components that you can configure to inspect your network traffic for intrusions and security policy violations. These components include intrusion rules that inspect the protocol header values, payload content, and certain packet size characteristics; variables commonly used in intrusion rules; a FireSIGHT recommended rules configuration; advanced settings such as preprocessors and other detection and performance features; and preprocessor rules that allow you to generate events for associated preprocessor options. When your network traffic meets the conditions in an access control rule, you can inspect that traffic with an intrusion policy; you can also associate an intrusion policy with the default action.

intrusion rule

A set of keywords and arguments that, when applied to monitored network traffic, identify potential intrusions, security policy violations, and security breaches. The system compares packets against rule conditions. If the packet data matches the conditions, the rule triggers and generates an intrusion event. Intrusion rules include drop rules and pass rules.

layer

A complete set of intrusion rule, preprocessor rule, and advanced setting configurations within an intrusion policy. You can add custom user layers to the built-in layer or layers in your policy. A setting in a higher layer in an intrusion policy overrides a setting in a lower layer.

LDAP authentication

A form of external authentication that verifies user credentials by comparing them to a Lightweight Directory Access Protocol (LDAP) directory stored on an LDAP directory server.

Lights-Out-Management (LOM)

A Series 3 feature that allows you to use an out-of-band Serial over LAN (SOL) management connection to remotely monitor or manage appliances without logging into the web interface of the appliance. You can perform limited tasks, such as viewing the chassis serial number or monitoring such conditions as fan speed and temperature.

link state propagation

An option for inline sets in bypass mode that automatically brings down the second interface in a pair when one of the interfaces in an inline set goes down. When the downed interface comes back up, the second interface automatically comes back up also. In other words, if the link state of a paired interface changes, the link state of the other interface changes automatically to match it.

list

See Security Intelligence list.

logical interface

A virtual subinterface that you define to handle traffic with specific VLAN tags as the tagged traffic passes through a physical interface.

malware blocking

A component of Cisco's network-based advanced malware protection (AMP) solution. After malware detection yields a malware disposition for a detected file, you can either block the file or allows its upload or download. Compare this functionality with FireAMP, Cisco's endpoint-based AMP tool that requires a FireAMP subscription.

malware cloud lookup

A process by which the Defense Center communicates with the Cisco cloud to determine the malware disposition of a file detected in network traffic, based on the file's SHA-256 hash value.

malware detection

A component of Cisco's network-based advanced malware protection (AMP) solution. File policies applied to managed devices as part of your overall access control configuration inspect network traffic. The Defense Center then performs malware cloud lookups for specific detected file types, and generates events that alert you to the files' malware dispositions. AMP malware blocking follows and either blocks the file or allows its upload or download. Compare this functionality with FireAMP, Cisco's endpoint-based AMP tool that requires a FireAMP subscription.

malware event

An event generated by one of Cisco's advanced malware protection solutions. Network-based malware events are generated when the Cisco cloud returns a malware disposition for a file detected in network traffic; retrospective malware events are generated when that disposition changes. Compare with endpoint-based malware events, which are generated when a deployed FireAMP Connector detects a threat, blocks malware execution, or quarantines or fails to quarantine malware.

Malware license

A license that allows you to perform advanced malware protection (AMP) in network traffic. Using a file policy, you can configure the system to perform malware cloud lookups on specific file types detected by managed devices. Compare with FireAMP subscription.

malware protection

See advanced malware protection.

managed device

See device.

management interface

The network interface that you use to administer a FireSIGHT System appliance. In most deployments, the management interface is connected to an internal protected network. Compare with sensing interface.

management traffic channel

See traffic channel.

mobile device

In the FireSIGHT System, a host identified by the discovery feature as a mobile, handheld device (such as a mobile phone or tablet). The system can often detect whether a mobile device is jailbroken.

monitor

In an access control policy, a way to log traffic that matches a Security Intelligence blacklist or access control rule, but allows the system to continue to evaluate the traffic rather than immediately allowing or blocking it.

multiple management interfaces

Additional management interfaces on Series 3 appliances that you can configure to either separate traffic into traffic channels to improve performance, or to create a route to an additional network to allow your Defense Center to isolate traffic on different networks. You can also route traffic channels to separate networks to increase throughput capacity. See management interface.

NAT

Network address translation, a feature most commonly used to share a single internet connection among multiple hosts on a private network. Using discovery, the system can identify network devices as logical interfaces. In addition, in a Layer 3 deployment of the FireSIGHT System, you can configure routing with NAT using a NAT policy.

NAT policy

A policy that uses NAT rules to perform routing with NAT.

NetMod

A module that you install in the chassis of a managed device that contains the sensing interfaces for that device.

network device

In the FireSIGHT System, a host identified as a bridge, router, NAT device, or logical interface.

network discovery

See discovery.

network discovery policy

A policy that specifies the kinds of discovery policy (including host, user, and application data) the system collects for specific network segments, including networks monitored by NetMod-enabled devices. The network discovery policy also manages import resolution preferences and active detection source priorities.

network file trajectory

A visual representation of a file's path as hosts transfer it across your network. For any file with an associated SHA-256 hash value, the trajectory map displays the IP addresses of all hosts that have transferred the file, the time the file was detected, the file's malware disposition, associated file events and malware events, and so on.

network map

A detailed representation of your network. The network map allows you to view your network topology in terms of the hosts, mobile devices, and network devices running on your network, as well as their associated host attributes, application protocols, and vulnerabilities.

non-bypass mode

A characteristic of an inline set that blocks traffic if the sensing interfaces in the set fail for any reason.

passive detection

The collection of discovery policy through analysis of traffic passively collected by managed devices. Compare with active detection.

passive interface

A sensing interface configured to analyze traffic in a passive deployment.

physical interface

An interface that represents a physical port on a NetMod.

policy

A mechanism for applying settings, most often to an appliance. See access control policy, correlation policy, file policy, health policy, intrusion policy, network discovery policy, and system policy.

preprocessor

A feature that normalizes traffic inspected by an intrusion policy and that helps identify network layer and transport layer protocol anomalies by identifying inappropriate header options, defragmenting IP datagrams, providing TCP stateful inspection and stream reassembly, and validating checksums. Preprocessors can also render specific types of packet data in a format that the system can analyze; these preprocessors are called data normalization preprocessors, or application layer protocol preprocessors. Normalizing application layer protocol encoding allows the system to effectively apply the same content-related intrusion rules to packets whose data is represented differently and obtain meaningful results. Preprocessors generate preprocessor rules whenever packets trigger preprocessor options that you configure.

preprocessor rule

An intrusion rule associated with a preprocessor or with the portscan flow detector. You must enable preprocessor rules if you want them to generate events. Preprocessor rules have a preprocessor-specific GID (generator ID).

protected network

Your organization's internal network that is protected from users of other networks by a device such as a firewall. Many of the intrusion rules delivered with the FireSIGHT System use variables to define the protected network and the unprotected (or outside) network.

Protection license

A license for Series 3 and virtual devices that allows you to perform intrusion detection and prevention, file control, and Security Intelligence filtering. Without a license, Series 2 devices automatically have Protection capabilities, with the exception of Security Intelligence.

RADIUS authentication

Remote Authentication Dial In User Service, a service used to authenticate, authorize, and account for user access to network resources. You can create an external authentication object to allow FireSIGHT System users to authenticate through a RADIUS server.

remediation

An action that mitigates potential attacks on your system. You can configure remediations and, within a correlation policy, associate them with correlation rules and compliance white lists so that when they trigger, the Defense Center launches the remediation. 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. The Defense Center ships with predefined remediation modules, and you also can use a flexible API to create custom remediations.

reputation (IP address)

See Security Intelligence.

routed interface

An interface that routes traffic in a Layer 3 deployment. You can set up physical routed interfaces for handling untagged VLAN traffic, and logical routed interfaces for handling traffic with designated VLAN tags. You can also add static Address Resolution Protocol (ARP) entries to routed interfaces.

router

A network device, located at a gateway, that forwards packets between networks. Using network discovery, the system can identify routers. In addition, you can configure managed devices as virtual routers that route traffic between two or more interfaces.

rule

A construct, usually within a policy, that provides criteria against which network traffic is examined.

rule action

A setting that determines how the system handles network traffic that meets the conditions of a rule. See access control rule and file rule action.

rule state

Whether an intrusion rule is enabled (set to Generate Events or Drop and Generate Events), or disabled (set to Disable) within an intrusion policy. If you enable a rule, it is used to evaluate your network traffic; if you disable a rule, it is not used.

rule update

An as-needed intrusion rule update that contains new and updated standard text rules, shared object rules, and preprocessor rules. A rule update may also delete rules, modify default intrusion policy settings, and add or delete system variables and rule categories.

scheduled task

An administrative task that you can schedule to run once or at recurring intervals.

Security Intelligence

A feature that allows you to specify the traffic that can traverse your network, per access control policy, based on the source or destination IP address. This is especially useful if you want to blacklist—deny traffic to and from—specific IP addresses, before the traffic is subjected to analysis by access control rules. Optionally, you can use a monitor setting for Security Intelligence filtering, which allows the system to analyze connections that would have been blacklisted, but also logs the match to the blacklist.

Security Intelligence feed

One of the types of Security Intelligence objects, a dynamic collection of IP addresses that the system downloads on a regular basis, at an interval you configure. Because feeds are regularly updated, using them ensures that the system uses up-to-date information to filter your network traffic using the Security Intelligence feature. See also Cisco Intelligence Feed.

Security Intelligence list

A simple static collection of IP addresses that you manually upload to the Defense Center as a Security Intelligence object. Use lists to augment and fine-tune Security Intelligence feeds as well as the global blacklist and global whitelist.

security policy

An organization's guidelines for protecting its network. For example, your security policy might forbid the use of wireless access points. A security policy may also include an acceptable use policy (AUP), which provides employees with guidelines of how they may use their organization's systems.

security policy violation

A security breach, attack, exploit, or other misuse of your network.

security zone

A grouping of one or more inline, passive, switched, or routed interfaces that you can use to manage and classify traffic flow in various policies and configurations. The interfaces in a single zone may span multiple devices; you can also configure multiple security zones on a single device. You must assign each interface you configure to a security zone before it can handle traffic, and each interface can belong to only one security zone.

sensing interface

A network interface on a device that you use to monitor a network segment. Compare with management interface.

Series 2

The second series of Cisco appliance models. Because of resource, architecture, and licensing limitations, Series 2 appliances support a restricted set of FireSIGHT System features. Series 2 devices include the 3D500, 3D1000, 3D2000, 3D2100, 3D2500, 3D3500, 3D4500, 3D6500, and 3D9900. Series 2 Defense Centers include the DC500, DC1000, and DC3000.

Series 3

The third series of Cisco appliance models. Series 3 appliances include 7000 Series and 8000 Series devices, as well as the DC750, DC1500, DC2000, DC3500, and DC4000 Defense Centers.

server

The server application (compare with client application) installed on a host, identified by application protocol traffic.

SFP module

A small form-factor pluggable transceiver that is inserted into a network module on a 71xx Family device. Sensing interfaces on SFP modules do not allow configurable bypass.

stack

Two to four connected devices that share detection resources.

stacking

A feature that allows you to increase the amount of traffic inspected on a network segment by connecting two to four physical devices in a stacked configuration. When you establish a stacked configuration, you combine the resources of each stacked device into a single, shared configuration.

switch

A network device that acts as a multiport bridge. Using network discovery, the system identifies switches as bridges. In addition, you can configure managed devices as virtual switches, performing packet switching between two or more networks.

switched interface

An interface that you want to use to switch traffic in a Layer 2 deployment. You can set up physical switched interfaces for handling untagged VLAN traffic, and logical switched interfaces for handling traffic with designated VLAN tags.

system policy

Settings that are likely to be similar for multiple appliances in a deployment, such as mail relay host preferences and time synchronization settings. Use the Defense Center to apply a system policy to itself and its managed devices.

table view

A type of workflow page that displays event information, with one column for each of the fields in the database table. When performing event analysis, you can use drill-down pages to constrain the events you want to investigate before moving to the table view that shows you the details about the events you are interested in. The table view is often the next-to-last page in workflows delivered with the system.

tap mode

An advanced inline set option available on 3D9900 and Series 3 devices where a copy of each packet is analyzed and the network traffic flow is undisturbed instead of passing through the device. Because you are working with copies of packets rather than the packets themselves, the device cannot affect the packet stream even if you configure access control and intrusion policies to drop, modify, or block traffic.

task queue

A queue of jobs that the appliance needs to perform. When you apply a policy, install software updates, and perform other long-running jobs, the jobs are queued and their status reported on the Task Status page. The Task Status page provides a detailed list of jobs and refreshes every ten seconds to update their status.

traffic channel

A connection you can configure on the management interface of a Series 3 appliance or virtual Defense Center to carry either management or event traffic. The event traffic channel carries only externally generated traffic (such as web browsers and so on) and the management traffic channel carries only internally generated traffic (that is, management traffic between the Defense Center and the device). See multiple management interfaces.

transparent inline mode

An advanced inline set option that allows a device to act as a “bump in the wire” and to forward all the network traffic it sees, regardless of its source and destination.

URL category

A general classification for a URL, such as malware or social networking.

URL filtering

A feature that allows you to write access control rules that determine the traffic that can traverse your network based on URLs requested by monitored hosts, correlated with URL category and URL reputation information about those URLs, which is obtained from the Cisco cloud by the Defense Center. You can also achieve more granular, custom control over web traffic by specifying individual URLs or groups of URLs to allow or block.

URL Filtering license

A license that allows you to perform URL filtering based on URL category and URL reputation information. URL Filtering licenses may expire.

user

A user whose network activity has been detected by a managed device or User Agent.

user activity

An event generated when the system detects a user login (optionally, including some failed login attempts) or the addition or deletion of a user record from the Defense Center database.

User Agent

An agent you install on a server to monitor users as they log into the network or when they authenticate against Active Directory credentials for any other reason. User activity for access-controlled users is used for access control only when reported by a User Agent.

user awareness

A feature that allows your organization to correlate threat, endpoint, and network intelligence with user identity information, and that allows you to perform user control.

user control

A feature that, as part of access control, allows you to specify and log the user-associated traffic that can enter your network, exit it, or cross from within without leaving it.

user role

The level of access granted to a user of the FireSIGHT System. For example, you can grant different access privileges to the web interface for event analysts, the administrator managing the FireSIGHT System, users accessing the Defense Center database using third-party tools, and so on. You can also create custom roles with specialized access privileges.

UTC time

Coordinated Universal Time. Also known as Greenwich Mean Time (GMT), UTC is the standard time common to every place in the world. The FireSIGHT System uses UTC, although you can set the local time using the Time Zone feature.

VDB

See vulnerability database.

virtual Defense Center

A Defense Center that you can deploy on your own equipment in a virtual hosting environment.

virtual device

A managed device that you can deploy on your own equipment in a virtual hosting environment. You cannot configure a virtual device as a virtual switch or virtual router.

virtual router

A group of routed interfaces that route Layer 3 traffic. In a Layer 3 deployment, you can configure virtual routers to route packets by making packet forwarding decisions according to the destination IP address. You can define static routes, configure Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) dynamic routing protocols, as well as implement Network Address Translation (NAT).

virtual switch

A group of switched interfaces that process inbound and outbound traffic through your network. In a Layer 2 deployment, you can configure virtual switches on managed devices to operate as standalone broadcast domains, dividing your network into logical segments. A virtual switch uses the media access and control (MAC) address from a host to determine where to send packets.

VLAN

Virtual local area network. VLANs map hosts not by geographic location, but by some other criterion, such as by department or primary use. A monitored host's host profile shows any VLAN information associated with the host. VLAN information is also included in intrusion events, as the innermost VLAN tag in the packet that triggered the event. You can filter intrusion policies by VLAN and target compliance white lists by VLAN. In Layer 2 and Layer 3 deployments, you can configure virtual switches and virtual routers on managed devices to appropriately handle VLAN-tagged traffic.

VPN

A feature that 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.

VPN license

A license that 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.

VRT

See Cisco VRT.

vulnerability

A description of a specific compromise to which a host is susceptible. The Defense Center provides information on the vulnerabilities to which each of your hosts is vulnerable in the hosts' host profiles. In addition, you can use the vulnerabilities network map to obtain an overall view of the vulnerabilities that the system has detected on your entire monitored network. If you deem a host or hosts no longer vulnerable to a specific compromise, you can deactivate, or mark as invalid, a specific vulnerability.

vulnerability database

Also called the VDB, a database of known vulnerabilities to which hosts may be susceptible. The system correlates the operating system, application protocols, and clients detected on each host with the VDB to help you determine whether a particular host increases your risk of network compromise. VDB updates may contain new and updated vulnerabilities, as well as new and updated application detectors.

web application

A type of application that represents the content of, or requested URL for, HTTP traffic.

widget

See dashboard widget.

zone

See security zone.