Cisco NGIPS for Blue Coat X-Series Installation and Configuration Guide

Version 5.4
June 23, 2014

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Introduction to Cisco NGIPS for Blue Coat X-Series

The FireSIGHT System combines the security of an industry-leading network intrusion protection system with the power to control access to your network based on many criteria, such as detected files and URLs. The Defense Center® provides a centralized management console and database repository for the FireSIGHT System. Managed devices installed on network segments monitor traffic for analysis.

Cisco NGIPS for Blue Coat X-Series provides a software-only version of the FireSIGHT System that you can install on your X-Series platform, with access control features, including file control and intrusion prevention. Cisco NGIPS for Blue Coat X-Series also provides network discovery functionality that lets you map and track hosts on your network, and correlate events affecting those hosts to quickly identify compromised hosts.

You can use Cisco NGIPS for Blue Coat X-Series as a managed device in a passive deployment to 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. You can monitor connections in a passive deployment for many characteristics, such as file types or protocols, file signatures, intrusion indicators, applications, users, network characteristics, URLs, and location data. However, you cannot block traffic in this deployment.

You can also use Cisco NGIPS for Blue Coat X-Series as a managed device in an inline deployment 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 the Defense Center configuration based on your deployment. Inline devices can be deployed as a simple intrusion prevention system.

Cisco NGIPS for Blue Coat X-Series uses several X-Series components:

- The Application Processor Module (APM) provides application processing and status monitoring, as well as standard and application-specific logging.

  You install Cisco NGIPS for Blue Coat X-Series on an APM.

- The Virtual Appliance Processor (VAP) consists of an operating system, system software, and an application run on an APM.

  A VAP functions like a managed device in the FireSIGHT System. You can group VAPs to provide redundancy (similar to clustering) or to load-balanced services to run applications.

- The Control Processor Module (CPM) provides all general system-functions.

  You load Cisco NGIPS for Blue Coat X-Series onto the CPM.

- The Network Processing Module (NPM) contains the physical interfaces of the X-Series platform.

This installation guide provides information about deploying, installing, and setting up Cisco NGIPS for Blue Coat X-Series. It also assumes familiarity with the features and nomenclature of the X-Series platform, the *XOS Command Reference Guide*, and the *XOS Configuration Guide*.

See the following sections for more information:

- Prerequisites for Installing Cisco NGIPS for Blue Coat X-Series, page 1-2 describes requirements you must fulfill to include Cisco NGIPS for Blue Coat X-Series in your FireSIGHT System deployment.
- Components of the FireSIGHT System, page 1-3 describes the key capabilities of the FireSIGHT System.
- Understanding Cisco NGIPS for Blue Coat X-Series Capabilities, page 1-5 describes the capabilities of the FireSIGHT System software on the X-Series platform.
- Licensing the FireSIGHT System, page 1-6 describes the various feature licenses available on the FireSIGHT System.
- Security, Internet Access, and Communication Ports, page 1-8 describes security considerations, access requirements, and communication ports for the FireSIGHT System.
- What's Next?, page 1-9 provides information on the content of this guide and outlines the steps for installing and configuring Cisco NGIPS for Blue Coat X-Series.

Prerequisites for Installing Cisco NGIPS for Blue Coat X-Series

The following sections detail the hardware and other requirements for including Cisco NGIPS for Blue Coat X-Series in your FireSIGHT System deployment.

You cannot update Cisco NGIPS for Blue Coat X-Series running Version 4.10.x of the FireSIGHT System directly to Version 5.4. Instead, you must uninstall the previous version and reinstall Version 5.4. Note that this results in the loss of all configuration and event data on the X-Series installation.

Tip If you want to retain essential configuration and event data, you can perform a limited migration of your entire deployment from Version 4.10.3.x (patch 4.10.3.5 or later) to Version 5.2.0.x, then update the migrated deployment to Version 5.4. Because Cisco NGIPS for Blue Coat X-Series is not supported with Version 5.2, you must update your Defense Center to Version 5.4 before you re-add Cisco NGIPS for Blue Coat X-Series. For more information on migration, contact Cisco Support.

Hardware and Operating System Requirements

Before you install Cisco NGIPS for Blue Coat X-Series on the X-Series platform, you must make sure that:

- the X-Series platform is installed and configured
- the X-Series platform is running XOS version 9.7.2 or later, or version 10.0 or later
- each Application Processor Module (APM) where you want to install the software has a minimum of 8GB of RAM and a local hard disk
- you know the IP address of the default gateway of the management network

Tip Cisco NGIPS for Blue Coat X-Series installations do **not** have a web interface. You must configure Cisco NGIPS for Blue Coat X-Series via console and command line, and you must manage Cisco NGIPS for Blue Coat X-Series with a Defense Center.

Supported Hardware Modules

You deploy Cisco NGIPS for Blue Coat X-Series on a combination of X-Series-based APM, CPM, and NPM hardware modules. For more information on X-Series hardware configuration options, see the *XOS Configuration Guide*.

You can deploy Cisco NGIPS for Blue Coat X-Series on the following APM modules:

Table 1-1 Supported APM Modules

Module	Options	X80	X60	X50	X30	X20
APM-8650	Dual CPU, 8GB RAM	yes	yes	no	no	no
	Dual CPU, 16BG RAM	yes	yes	no	no	no
APM-9600	Dual CPU, 12GB RAM	yes	yes	no	no	no
	Dual CPU, 24GB RAM	yes	yes	no	no	no
APM-2030	Dual CPU, 8GB RAM	no	no	no	yes	yes
APM-50	Dual CPU, 12GB RAM	no	no	yes	no	no

You can deploy Cisco NGIPS for Blue Coat X-Series on the following CPM and NPM modules:

Table 1-2 Supported CPM and NPM Modules

Module	X80	X60	X50	X30	X20
CPM-9600	yes	yes	yes	yes	yes
NPM-8620	yes	yes	no	no	no
NPM-8650	yes	yes	no	no	no
NPM-9610	yes	yes	no	no	no
NPM-9650	yes	yes	no	no	no
NPM-20	no	no	no	no	yes
NPM-30	no	no	no	yes	no
NPM-50	no	no	yes	no	no

Components of the FireSIGHT System

The topics 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:

- FireSIGHT, page 1-4
- Access Control, page 1-4

FireSIGHT

FireSIGHT™ is Cisco's discovery and awareness technology that collects information about hosts, operating systems, applications, users, files, networks, 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 can traverse your network. An access control policy determines how the system handles traffic on your network. You can use a policy that does not include access control rules to handle traffic in one of the following ways, using what is called the default action:

- block all traffic from entering your network
- trust all traffic to enter your network without further inspection
- allow all traffic to enter your network, and inspect the traffic with a network discovery policy only
- allow all traffic to enter your network, and inspect the traffic with intrusion and network discovery policies

You can include access control rules in an access control policy to further define how traffic is handled by targeted devices, from simple IP address matching to complex scenarios involving different users, applications, ports, and URLs. For each rule, you specify a rule action, that is, whether to trust, monitor, block, or inspect matching traffic with an intrusion or file policy.

For each access control policy, you can create a custom HTML page that users see when the system blocks their HTTP requests. Optionally, you can display a page that warns users, but also allows them to click a button to continue to the originally requested site.

As part of access control, the Security Intelligence feature allows you to blacklist (that is, deny traffic to and from) specific IP addresses before the traffic is subjected to analysis by access control rules.

Geolocation conditions are not supported, and you cannot block traffic based on user or application conditions using Cisco NGIPS for Blue Coat X-Series.

Access control includes intrusion detection and prevention, file control, and advanced malware protection. On Cisco NGIPS for Blue Coat X-Series, you cannot do advanced malware protection. For more information, see the next sections.

Intrusion Detection and Prevention

Intrusion detection and prevention allows you to monitor your network traffic for security violations and, in inline deployments, to block or alter malicious traffic.

Intrusion prevention is integrated into access control, where you can associate an intrusion policy with specific access control rules. If network traffic meets the conditions in a rule, you can analyze the matching traffic with an intrusion policy. You can also associate an intrusion policy with the default action of an access control policy.

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 Malware Protection

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

File control allows managed devices to detect and block your users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols. You configure file control as part of your overall access control configuration; file policies associated with access control rules inspect network traffic that meets rule conditions.

Network-Based Advanced Malware Protection (AMP)

Network-based advanced *malware protection* (AMP) allows the system to inspect network traffic for malware in several types of files. Note that advanced malware protection is not supported on Cisco NGIPS for Blue Coat X-Series.

Network File Trajectory

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; so, to track a file, the system must either:

- calculate the file's SHA-256 hash value and perform a malware cloud lookup using that value
- receive endpoint-based threat and quarantine data about that file, using the Defense Center's integration with your organization's FireAMP subscription

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.

Understanding Cisco NGIPS for Blue Coat X-Series Capabilities

Cisco NGIPS for Blue Coat X-Series supports most of the capabilities of the FireSIGHT System. However, 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 any of the system's hardware-based or advanced device management features, including the following features:
  - clustering

  - stacking
  - virtual switching
  - virtual routing
  - Cisco-based dynamic load balancing
  - Cisco-based high availability
  - site-to-site VPN
  - NAT
  - automatic application bypass
  - fast-path
  - user and application control
  - advanced malware protection
- 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

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.

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 1-3 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
DC2000	100,000
DC3000	100,000
DC3500	300,000
DC4000	600,000
virtual	50,000

You can use the following FireSIGHT System licenses on Cisco NGIPS for Blue Coat X-Series:

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. A Control license requires a Protection license. You cannot enable a Control license on Cisco NGIPS for Blue Coat X-Series to perform user and application control, switching, routing, or NAT.

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. You cannot enable a Malware license on Cisco NGIPS for Blue Coat X-Series to perform block malware or to store and submit files for further analysis.

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

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 from outside the firewall.

If the Defense Center and Cisco NGIPS for Blue Coat X-Series reside on the same network, you can connect the management interface on Cisco NGIPS for Blue Coat X-Series to the same protected internal network as the Defense Center. This allows you to securely control Cisco NGIPS for Blue Coat X-Series from the Defense Center.

Regardless of how you deploy your Cisco NGIPS for Blue Coat X-Series managed devices, intra-device communication is encrypted. However, you must still take steps to ensure that communications between Cisco NGIPS for Blue Coat X-Series managed devices 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 Cisco NGIPS for Blue Coat X-Series require an Internet connection. By default, all Cisco NGIPS for Blue Coat X-Series managed devices are configured to directly connect to the Internet. Additionally, the system requires certain ports remain open for basic intra-device communication, for secure device access, and so that specific system features can access the local or Internet resources they need to operate correctly.

For more information, see:

- Internet Access Requirements, page 1-8
- Communication Ports Requirements, page 1-8

Internet Access Requirements

By default, Cisco NGIPS for Blue Coat X-Series is configured to directly connect to the Internet. For more information, see the *FireSIGHT System User Guide*.

Note Cisco NGIPS for Blue Coat X-Series does **not** support proxy settings.

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:

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

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

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

For example, closing port 25/tcp (SMTP) outbound on a managed device blocks the device from sending email notifications for individual intrusion events (see the *FireSIGHT System User Guide*).

Note that the system allows you to 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.

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

Table 1-4 FireSIGHT System Open Communication Ports Requirements

Port	Description	Direction	To...
22/tcp	SSH/SSL	Bidirectional	allow a secure remote connection to the appliance.
25/tcp	SMTP	Outbound	send email notices and alerts from the appliance.
53/tcp	DNS	Outbound	use DNS.
162/udp	SNMP	Outbound	send SNMP alerts to a remote trap server.
514/udp	syslog	Outbound	send alerts to a remote syslog server.
8305/tcp	appliance comms.	Bidirectional	securely communicate between appliances in a deployment. **Required.**

What's Next?

The following chapters explain how to install and configure Cisco NGIPS for Blue Coat X-Series:

- Understanding Deployment, page 2-1 describes some of the ways you might want to deploy the FireSIGHT System within your network environment, depending on the capabilities of your X-Series platform and on the components you are licensed to use.
- Installing Cisco NGIPS for Blue Coat X-Series, page 3-1 explains how to install Cisco NGIPS for Blue Coat X-Series on your X-Series platform, how to make sure the Cisco Defense Center can communicate with the Cisco NGIPS for Blue Coat X-Series installations, and how to configure the X-Series platform so that Cisco NGIPS for Blue Coat X-Series receives network traffic. It also explains how to uninstall Cisco NGIPS for Blue Coat X-Series.
- Setting Up the Defense Center, page 4-1 explains how to set up a Cisco Defense Center to manage Cisco NGIPS for Blue Coat X-Series.
- Managing Cisco NGIPS for Blue Coat X-Series, page 5-1 explains how to perform tasks such as adding VAPs to a VAP group, changing interfaces for VAP groups, editing load-balanced VAP groups, and resetting the communications channel for a VAP. It also contains a command reference.

Understanding Deployment

A Cisco NGIPS for Blue Coat X-Series deployment depends on both X-Series-based and Cisco-specific components. Implement a basic deployment scenario using the following steps:

Step 1 Create and configure all VAPs and VAP groups on the X-Series platform. The name you give to each VAP is the name that appears in the Defense Center as the device name. See Preparing for the Installation, page 3-2 for more information.

Step 2 Install Cisco NGIPS for Blue Coat X-Series on each VAP on the X-Series platform. Each VAP appears on the Defense Center separately and functions as a managed device. See Installing Cisco NGIPS for Blue Coat X-Series, page 3-14 for more information.

Step 3 Deploy Cisco NGIPS for Blue Coat X-Series into your network. You can deploy each VAP individually, or deploy a VAP group to take advantage of redundancy and load balancing. See Understanding Deployment Scenarios, page 2-4 for more information.

Step 4 Configure remote management for each installation of Cisco NGIPS for Blue Coat X-Series on a Defense Center. See Adding Cisco NGIPS for Blue Coat X-Series to the Defense Center, page 4-1 for more information.

Step 5 Use the Defense Center to configure and apply an access control policy to each Cisco NGIPS for Blue Coat X-Series installation. See the *FireSIGHT System User Guide* for more information.

Your deployment options depend on the capabilities of your X-Series platform and the components of the FireSIGHT System you are licensed to use. For information on the requirements of your Cisco NGIPS for Blue Coat X-Series, see Prerequisites for Installing Cisco NGIPS for Blue Coat X-Series, page 1-2.

For a basic understanding of deployment options, see the following sections:

Understanding Sensing Circuits

Sensing circuits are connections between points in the chassis or to external interfaces. You create sensing circuits differently, depending on how Cisco NGIPS for Blue Coat X-Series is deployed:

- For passive deployments, create monitor (tap) circuits to ensure that a copy of the network traffic is sent to the VAP group for analysis.
- For inline deployments, create template (bridge) circuits and child circuits to provide logical connections through a VAP group and between network interfaces.

For more information on configuring and associating X-Series circuits for use in a Cisco NGIPS for Blue Coat X-Series installation, see Configuring Sensing Circuits, page 3-7, Configuring the Management Circuits, page 3-5, and Associating Physical Ports with Circuits, page 3-10.

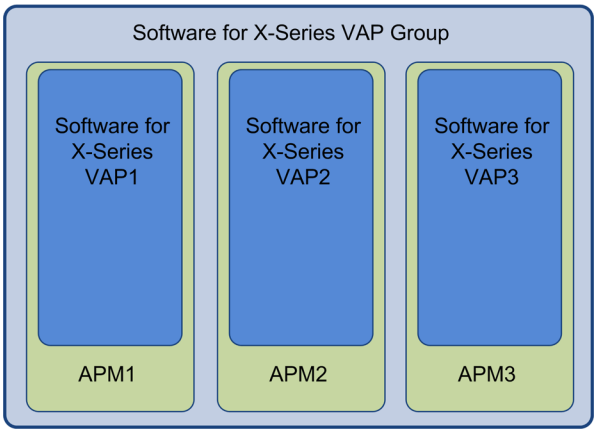
Understanding VAPs and VAP Groups

Cisco NGIPS for Blue Coat X-Series uses Virtual Appliance Processors (VAPs) and VAP groups hosted on Application Processor Modules (APMs) on blades of the X-Series platform, as described below:

- The X-Series platform can host one or more blades (APMs).
- Each APM can host one VAP.
- Each VAP can run one installation of Cisco NGIPS for Blue Coat X-Series.
- Each VAP functions like a managed device in the FireSIGHT System, and appears on its managing Defense Center as a device.
- A VAP group is a combination of VAPs, similar to physical device clustering, configured through the X-Series command line interface (CLI).

When you install Cisco NGIPS for Blue Coat X-Series on a VAP, the name you give to the VAP appears on the Defense Center web interface as the name of the device.

In the following diagram, three APMs (`APM1`, `APM2`, and `APM3`) each host one installation of Cisco NGIPS for Blue Coat X-Series on each VAP (`VAP1`, `VAP2`, and `VAP3`). These three APMs are configured as a single VAP group (`Cisco NGIPS for Blue Coat X-Series VAP Group`). In the Defense Center web interface, each VAP appears as a separate software device that you must add and configure individually.



If you use a device group on the FireSIGHT System, you can create a VAP group that parallels the structure of the device group. Use the same or similar names for VAP groups and their corresponding device groups to make management easier.

Understanding Redundancy and Load Balancing

The X-Series platform allows you to take advantage of its load balancing and redundancy benefits when you deploy Cisco NGIPS for Blue Coat X-Series in a multi-member VAP group, with each VAP running its own instance of Cisco NGIPS for Blue Coat X-Series.

Configuring Redundancy

If you want to take advantage of redundancy, deploy identically configured installations of Cisco NGIPS for Blue Coat X-Series in a multi-member VAP group. Use the Defense Center web interface to configure each Cisco NGIPS for Blue Coat X-Series identically. For example, to create a three-member VAP group, you create three VAPs, and configure each Cisco NGIPS for Blue Coat X-Series identically.

You cannot configure redundancy if the VAPs in your VAP group perform different functions (for example, one VAP monitors traffic on your internal network, and two VAPs monitor traffic on your DMZ). Instead, create multiple VAP groups, each with a specific function, to create redundancy on each VAP group.

Configuring Load Balancing

If you want to use two load-balanced Cisco NGIPS for Blue Coat X-Series installations to monitor IPv4 traffic, you create two identical VAPs, configure them to monitor the same Cisco NGIPS for Blue Coat X-Series sensing interfaces, and apply the same access control policy to each VAP. For more information, see the *XOS Configuration Guide*.

For all multi-member VAP groups, make sure that you add a flow rule with the `load-balance` action when you create the VAP group, as described in Creating and Configuring a VAP Group, page 3-4. Additionally, and especially for inline deployments, Cisco and Blue Coat recommend that you reserve one VAP in the group for failover.

When running on XOS V9.7.x (any operating mode) or on XOS V10.0 configured for Series-6 operating mode, you cannot load-balance IPv6 traffic across VAPs in a VAP group. IPv6 traffic can be load-balanced across multiple cores on a master VAP, reducing resource utilization and increasing throughput. For more information, see the *XOS Configuration Guide*.

When XOS V10.0 or later is configured for Series-9 operating mode and IPv6 is enabled for the VAP group, XOS supports load-balancing of IPv6 traffic across VAPs in a VAP group. For more information, see the XOS V10.0 Release Notes.

Understanding Access Control Policies

An access control policy determines how the FireSIGHT System handles traffic on your network. When you apply an access control policy, you configure Cisco NGIPS for Blue Coat X-Series to handle traffic on your network according to the rules specified in the applied access control policy.

A simple access control policy can filter traffic based on a variety of criteria, then use the policy's default action to handle traffic in a variety of ways, such as:

- block all traffic from entering your network
- trust all traffic to enter your network without further inspection
- allow all traffic to enter your network, and inspect all traffic according to additional policies

Note that you cannot block traffic based on user or application conditions with the Cisco NGIPS for Blue Coat X-Series.

You can configure one or more access control policies which you can then apply to one or more Cisco NGIPS for Blue Coat X-Series installations. Each Cisco NGIPS for Blue Coat X-Series can have only one currently applied policy.

After you configure your deployment, you apply an access control policy to each Cisco NGIPS for Blue Coat X-Series in the deployment, configuring subordinate intrusion and file policies as appropriate. See the *FireSIGHT System User Guide* for more information on how to configure policies, organize rules in a policy, and manage access control policies within the FireSIGHT System.

Understanding Deployment Scenarios

You can use Cisco NGIPS for Blue Coat X-Series in a passive deployment, either as a stand-alone VAP supporting an external tap, or in a multi-VAP or VAP group deployment supporting an internal tap. For more information on passive interfaces, see the *FireSIGHT System User Guide*. For more information on creating and configuring a VAP, VAP group, management circuits, and sensing circuits, see Preparing for the Installation, page 3-2.

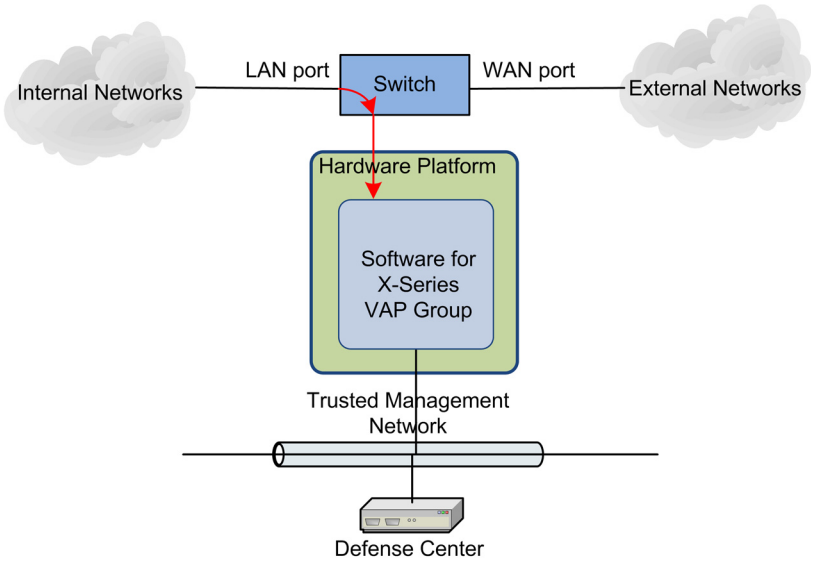
You apply an access control policy to each Cisco NGIPS for Blue Coat X-Series to handle traffic on your network according to the rules specified in the applied access control policy. For more information on access control policies, see the see the *FireSIGHT System User Guide*.

Using a Passive Deployment

Use a passive deployment for intrusion detection to analyze network traffic for potential intrusions and store attack data for analysis. A passive deployment receives all traffic unconditionally without retransmitting any traffic.

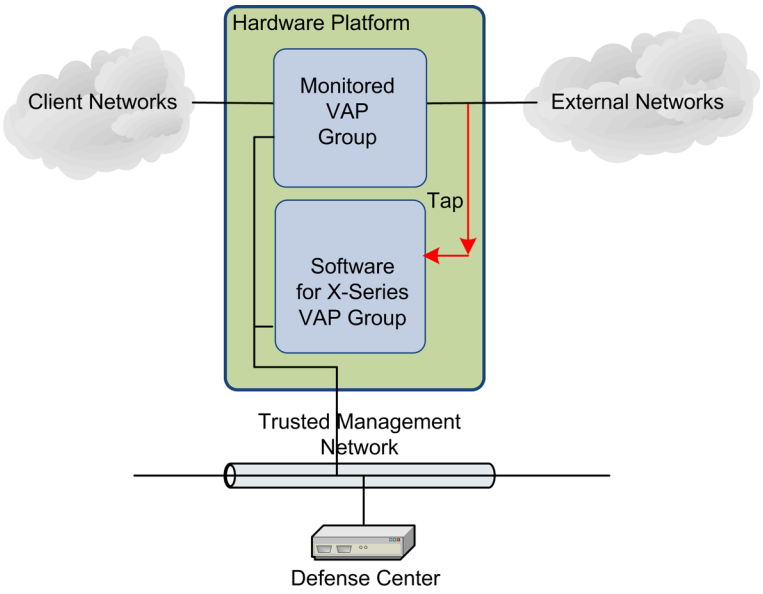
External Tap in a Passive Deployment

You can deploy Cisco NGIPS for Blue Coat X-Series in passive mode with an external tap to receive a copy of inline traffic passing through an external device, such as a physical network tap or a switch configured for port mirroring.



Internal Tap in a Passive Deployment

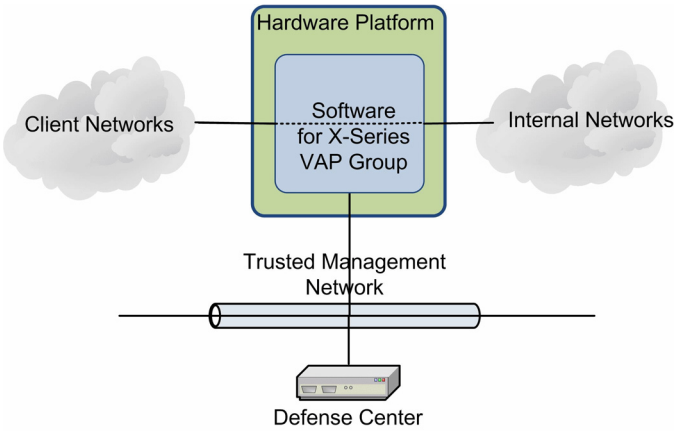
You can deploy Cisco NGIPS for Blue Coat X-Series in passive mode using an internal tap to receive copies of all packets passing through another application in the network. In this example, Cisco NGIPS for Blue Coat X-Series receives copies of all packets passing through an application hosted on a VAP in the VAP group called Monitored VAP Group.



Using an Inline Deployment

You can deploy as an inline access control system, where, in addition to trusting or monitoring traffic, you can block traffic based on access control rule criteria. You can also set up intrusion and file policies and select them in your access control policies to perform further analysis and, if needed, block traffic based on intrusion prevention and file control settings. If you deploy with a firewall, you can monitor traffic that is allowed inbound by the firewall policy or enters your network due to firewall misconfiguration. You can also detect and prevent attacks originating from hosts on the internal network.

Note Cisco NGIPS for Blue Coat X-Series does **not** support configurable bypass (called *inline with fail-open* in Version 4.10) interfaces.



Installing Cisco NGIPS for Blue Coat X-Series

After you determine how you will deploy Cisco NGIPS for Blue Coat X-Series, the next step is to create a Virtual Application Processor (VAP) group, configure circuits that allow network traffic to pass to (passive deployment) or through (inline deployment) the VAP group, then install Cisco NGIPS for Blue Coat X-Series.

You cannot update Cisco NGIPS for Blue Coat X-Series running Version 4.10.x of the FireSIGHT System directly to Version 5.3. Instead, you must uninstall the previous version and reinstall Version 5.3. Note that this results in the loss of all configuration and event data on Cisco NGIPS for Blue Coat X-Series installation.

Tip If you want to retain essential configuration and event data, you can perform a limited migration of your entire deployment from Version 4.10.3.x (patch 4.10.3.5 or later) to Version 5.2.0.x, then update the migrated deployment to Version 5.3. Because Cisco NGIPS for Blue Coat X-Series is not supported with Version 5.2, you must update your Defense Center to Version 5.3 before you re-add Cisco NGIPS for Blue Coat X-Series. For more information on migration, contact Cisco Support.

For more information, see:

Before You Begin

Before you begin the installation process, there are some important points you should keep in mind, as described in the following sections:

Uninstalling Previous Versions of Cisco NGIPS for Blue Coat X-Series

Before you load or perform a fresh install of Cisco NGIPS for Blue Coat X-Series, you **must** uninstall any previous versions and remove any existing Cisco software packages from the CPM. For information on uninstalling a previous version of the software, see the documentation delivered with that version.

After you complete and verify the installation, you **must**:

Step 1 Set up licensing and communication between Cisco NGIPS for Blue Coat X-Series and the Cisco Defense Center. For more information, see Setting Up the Defense Center, page 4-1.

Step 2 Log into to the Cisco Support site (https://support.sourcefire.com/) and check for updates to the FireSIGHT System. The release notes accompanying the update include instructions for installing the new software.

Pre-Staging Cisco NGIPS for Blue Coat X-Series

Pre-staging allows you to install Cisco NGIPS for Blue Coat X-Series on your CPM before all APM hardware is available. This is useful to prepare for additional hardware. When you pre-stage Cisco NGIPS for Blue Coat X-Series, the application installation runs on the CPM as if the APM were available. When you pre-stage your installation, confirm the following:

- there are more VAPs than APMs assigned to the VAP group
- the `vap-count` equals or exceeds the `max-load-count`
- the VAP must be running `xslinux_v5_64` for FireSIGHT System, Version 5.4

For more information on the `vap-count` and the `max-load-count`, see Creating and Configuring a VAP Group, page 3-4.

Keep in mind the capability for pre-staged application support while installing, uninstalling, and monitoring Cisco NGIPS for Blue Coat X-Series.

Preparing for the Installation

The Cisco NGIPS for Blue Coat X-Series installation is hosted on a VAP group that contains a management circuit to communicate with the managing Defense Center and sensing interfaces to pass traffic.

To prepare for the installation:

Step 1 Set up a Virtual Application Processor (VAP) group where you want to install Cisco NGIPS for Blue Coat X-Series.

Step 2 Create and configure the management circuits, and give each VAP in the VAP group a unique IP address.

Step 3 Create and configure bridges and circuits to use as sensing circuits.

Step 4 Assign the management and sensing circuits to the appropriate network interfaces.

For more information on how to perform each of these steps, see the following sections:

- Setting Up a VAP Group, page 3-3
- Configuring the Management Circuits, page 3-5

- Configuring Sensing Circuits, page 3-7
- Associating Physical Ports with Circuits, page 3-10

Setting Up a VAP Group

Before you configure the management and sensing circuits and install the application packages, use the X-Series platform CLI to set up a VAP group for Cisco NGIPS for Blue Coat X-Series.

For more information, see the following sections:

- Identifying APMs to Use, page 3-3
- Creating and Configuring a VAP Group, page 3-4

Identifying APMs to Use

Using the following commands can help you determine which APMs you can use to set up VAP groups for Cisco NGIPS for Blue Coat X-Series. A VAP where you load the software must be running on an APM with at least 8GB RAM and a local hard disk. Although there can be multiple APM types in a single Cisco NGIPS for Blue Coat X-Series, it is recommended that all of the APMs in a single VAP group include similar CPU, RAM capacity, hard disk drive, and so on. For more information, see Supported Hardware Modules, page 1-3:

- The **`show module status disk`** command displays which APMs have a local hard disk.
- The **`show module status memory`** command displays how much RAM is configured on each module.
- The **`show chassis`** command displays the module names and identifies which module is associated with which slot.

Note If you change an APM (for example you replace one APM in your configuration), you must reapply any policies on the APMs.

Step 1 To determine which APMs have a local hard disk, enter the following:

```
CBS# show module status disk
```

The system displays the disk status for each configured module similar to the information in the sample below:

```
Slot 5:
  Hard Disk                 450(GB)
  Second Hard Disk          NA
  Flash                     NA
  Hard Disk Drive Error     None
  Second Hard Drive Error   None
  RAID Status               Not Active, RAID none
```

Step 1 To determine how much RAM is installed on each APM, enter the following:

```
CBS# show module status memory
```

The system displays the memory for each configured module similar to the information in the sample below:

```
Slot 1:
  SDRAM 1 Size              1048576(KB)
```

```
SDRAM 2 Size                0(KB)
SDRAM 3 Size                1048576(KB)
SDRAM 4 Size                0(KB)
SDRAM Total Size            2097152(KB)
Reserved Memory             0(KB)
Total Memory                2097152(KB)
Used Memory                 1815924(KB)
Free Memory                 218228(KB)
Shared Memory               0(KB)
Buffers Memory              0(KB)
Cached Memeory              91344(KB)
Memory Utilization          82.23%
```

Step 1 To determine which APM is associated with which slot, enter the following:

```
CBS# show chassis
```

The system displays the chassis configuration similar to the information in the sample below:

```
Slot Present Module Name Module Type Status Uptime
1    Yes     np1         NPM9610     Up     119 days, 02:56
2    No      n/a         n/a         n/a
3    No      n/a         n/a         n/a
4    No      n/a         n/a         n/a
5    Yes     ap3         APM9600     Active 119 days, 02:40
6    Yes     ap4         APM9600     Active 119 days, 02:42
```

Creating and Configuring a VAP Group

The series of commands detailed in the following procedure creates a VAP group named `ABC` where the `max-load-count` value of 2 limits the active VAPs in the VAP group to two, and the `available-ap-list` specifies three VAPs which the VAP group can use (two VAPs host the active VAPs and you reserve the third for failover):

```
CBS# configure vap-group ABC xslinux_v5_64
CBS(config-vap-grp)# vap-count 2
CBS(config-vap-grp)# max-load-count 2
CBS(config-vap-grp)# available-ap-list ap1 ap2 ap5
CBS(config-vap-grp)# ip-flow-rule Inline_lb
CBS(ip-flow-rule)# action load-balance
CBS(ip-flow-rule)# activate
CBS(ip-flow-rule)# end
CBS#
```

To create and configure a VAP group:

Step 1 Create a VAP group by entering the following at the CLI prompt:

```
CBS# configure vap-group vap_group_name xslinux_v5_64
```

where *`vap_group_name`* is the name you want to give to the VAP group.

For example, to create a VAP group named ABC, enter the following command at the CLI prompt:

```
CBS# configure vap-group ABC xslinux_v5_64
```

You must verify that you want to create the new VAP group. The creation process takes several minutes.

Step 2 Set the `vap-count` and `max-load-count` to the same value for this VAP group by entering the following commands separately and in this sequence:

```
CBS(config-vap-grp)# vap-count vap-count-quantity
CBS(config-vap-grp)# max-load-count max-load-quantity
```

where *`vap-count-quantity`* is the number of VAPs you want to create for the VAP group, and *`max-load-quantity`* is the maximum number of VAPs the VAP group can contain.

Tip The *vap-count-quantity* and the *max-load-quantity* should be the same.

For example, if you have two licenses for Cisco NGIPS for Blue Coat X-Series, you can create two VAPs by entering the following commands:

```
CBS(config-vap-grp)# vap-count 2
CBS(config-vap-grp)# max-load-count 2
```

Step 3 Specify the APMs where you want the VAPs to run by entering the following:

```
CBS(config-vap-grp)# available-ap-list APM-names
```

where the *APM-names* is a list of the modules allowed to run the software.

Tip Confirm that the APMs meet your hardware requirements before running this command.

For example, the following command allows the software to run on two of the three modules (hosted on ap1, ap2, and ap5) and to reserve the third for common failover:

```
CBS(config-vap-grp)# available-ap-list ap1 ap2 ap5
```

Step 4 For IPv4 only: Create and assign a name to a flow rule to load-balance the traffic within the VAP group by entering the following commands separately and in this sequence:

```
CBS(config-vap-grp)# ip-flow-rule rule_name
CBS(ip-flow-rule)# action load-balance
CBS(ip-flow-rule)# activate
CBS(ip-flow-rule)# end
CBS#
```

where *rule_name* is the name of the flow rule. Because you want to load-balance the traffic, use the action `load-balance`. See the *XOS Command Reference Guide* for more options.

Note Do **not** use either the `no skip-port` or the `no skip-protocol` option when creating your flow rule.

For IPv6: Support for IPv6 load-balancing on the X-Series platform depends on the version of XOS installed. See Configuring IPv6 Detection, page 3-12 for more information.

Step 5 To create additional VAP groups, repeat steps 1 through 4.

Configuring the Management Circuits

You must create a management circuit, which the Cisco Defense Center and Cisco NGIPS for Blue Coat X-Series use to communicate. On the management circuit, you must assign an IP address to each VAP so that you can manage each instance of Cisco NGIPS for Blue Coat X-Series with the Defense Center. Note that if your trusted management circuit is on a different subnet from your Defense Center, you must create an IP route so that management traffic can cross subnets.

The following series of commands, detailed in the following procedure, creates a management circuit named `mgmt` and adds a VAP group named `ABC` to the circuit. It also assigns unique, consecutive (10.1.16.107 through 10.1.16.110) IP addresses to four VAPs: the two VAPs that compose the ABC VAP group.

```
CBS# configure circuit mgmt domain 2
CBS(conf-cct)# link-state-resistant
CBS(conf-cct)# device-name mgmt
CBS(conf-cct)# vap-group ABC
```

```
CBS(conf-cct-vapgroup)# management-circuit
CBS(conf-cct-vapgroup)# ip 10.1.16.107/24 10.1.16.255
    increment-per-vap 10.1.16.110
CBS(conf-cct-vapgroup-ip)# exit
CBS(conf-cct-vapgroup)# exit
CBS(conf-cct-vapgroup-ip)# end
CBS#
```

Note When XOS V10.0 or later is configured for Series-9 operating mode, the `increment-per-vap parameter` supports IPv4 or IPv6 addresses. For more information, see the XOS V10.0 Release Notes.

To configure the management circuit:

Step 1 Create a management circuit by entering:

```
CBS# configure circuit mgmt domain_ID
```

where *domain_ID* is the name of the management circuit.

If the sensing circuit monitors management traffic, Cisco and Blue Coat recommend specifying an alternate *domain_ID* for the management circuit. By default, all circuits belong to `domain 1`. The following example uses `domain 2` as the domain ID:

```
CBS# configure circuit mgmt domain 2
```

Step 2 Set the circuit type for the management circuit to `link-state-resistant` and assign a device name, by entering the following commands separately and in this sequence:

```
CBS(conf-cct)# link-state-resistant
CBS(conf-cct)# device-name device_name
```

where *device_name* is the name of the device.

For example, to set the circuit type to `link-state-resistant` and set the device name to `mgmt`, enter the following:

```
CBS(conf-cct)# link-state-resistant
CBS(conf-cct)# device-name mgmt
```

Caution Do **not** create a circuit or device name that starts with a numeric character.

Step 3 Add a VAP group to the circuit you just created by entering the following:

```
CBS(conf-cct)# vap-group vap_group_name
```

where *vap_group_name* is the name of the VAP group you want to add to the circuit.

For example, to add the VAP group named `ABC`, enter the following:

```
CBS(conf-cct)# vap-group ABC
```

Step 4 Mark the circuit as a management circuit by entering the following command:

```
CBS(conf-cct-vapgroup)# management-circuit
```

Step 5 Assign IP addresses to the VAPs in the VAP group you just added to the management circuit, by entering the following command:

```
CBS(conf-cct-vapgroup)# ip vap_ip+subnet_mask
    broadcast_address increment-per-vap last_ip_in_subnet
```

where *vap_ip+subnet_mask* is the first IP address and subnet mask you want to assign to the VAP, *broadcast_address* is the broadcast address of that IP address, and *last_ip_in+subnet* is the last IP address you want to use in that VAP group.

In this scenario, there are two VAPs in the VAP group named `ABC`, and you must assign two IP addresses. You also want to preserve two additional IP addresses for potential expansion of the VAP group.

For this example, the following command sets the first available IP address to `10.1.16.107` and the second available IP address to `10.1.16.108`, then sets aside two additional IP addresses (`10.1.16.109` and `10.1.16.110`) for VAP group expansion:

```
CBS(conf-cct-vapgroup)# ip 10.1.16.107/24 10.1.16.255
    increment-per-vap 10.1.16.110
```

When XOS V10.0 or later is configured for Series-9 operating mode, the `increment-per-vap` parameter supports IPv4 or IPv6 addresses. For more information, see the XOS V10.0 Release Notes.

Tip Blue Coat recommends increasing the outside range by two or three unused IP addresses to allow for possible future expansion of the VAP group.

Step 6 Exit to the `conf-cct` context, by entering the following commands separately and in this sequence:

```
CBS(conf-cct-vapgroup-ip)# exit
CBS(conf-cct-vapgroup)# exit
```

Configuring Sensing Circuits

Sensing circuits are connections between points in the chassis or to external interfaces. You create sensing circuits differently, depending on how Cisco NGIPS for Blue Coat X-Series is deployed:

- For passive deployments, create monitor (tap) circuits to ensure that a copy of the network traffic is sent to the VAP group for analysis.
- For inline deployments, create template (bridge) circuits and child circuits to provide logical connections through a VAP group and between network interfaces.

In either deployment, you must configure sensing circuits to ignore physical interface state by using the `link-state-resistant` command.

Note Cisco NGIPS for Blue Coat X-Series does **not** support configurable bypass (called *inline with fail-open* in the FireSIGHT System, Version 4.10) interfaces.

Note that if a sensing circuit goes down, Cisco NGIPS for Blue Coat X-Series stops analyzing network traffic until either the circuit comes up on its own or you remove the circuit from its interface on the Defense Center. You can avoid this interruption in traffic by configuring redundancy for your VAP group. For more information, see Understanding VAPs and VAP Groups, page 2-2.

Use an easy-to-remember naming convention for bridge, child, and monitor circuits that best suits your deployment. In the procedures that follow, the NPM_1 Gigabit Ethernet port 3 is named `n1e3`.

Caution Do **not** create a circuit or device name that starts with a numeric character.

For more information, see the following sections:

- Creating Monitor Circuits, page 3-8
- Creating Template Circuits, page 3-8
- Creating Child Circuits, page 3-9
- Configuring Bridge-Mode Bridges, page 3-10

Creating Monitor Circuits

For passive deployments, you must create monitor circuits for the sensing circuits. Monitor circuits ensure that a copy of the network traffic is sent to the VAP group for analysis. You must configure monitor circuits, sometimes called taps, using `promiscuous-mode`.

For a passive deployment of Cisco NGIPS for Blue Coat X-Series, the following series of commands creates a monitor circuit named `n1e1` on the device named `n1e1` hosted on the VAP group named `XYZ`:

```
CBS# configure circuit n1e1
CBS(conf-cct)# link-state-resistant
CBS(conf-cct)# device-name n1e1
CBS(conf-cct)# vap-group XYZ
CBS(conf-cct-vapgroup)# promiscuous-mode
CBS(conf-cct-vapgroup)# end
CBS#
```

To configure monitor circuits:

Step 1 Create monitor circuits for passive interfaces by entering the following commands separately and in sequence:

```
CBS# configure circuit circuit_name
CBS(conf-cct)# link-state-resistant
CBS(conf-cct)# device-name device_name
CBS(conf-cct)# vap-group vap_group_name
CBS(conf-cct-vapgroup)# promiscuous-mode
CBS(conf-cct-vapgroup)# end
CBS#
```

where *`circuit_name`* is the name you assign to the circuit, *`device_name`* is the name of the device hosting the circuit, and *`vap_group_name`* is the name of the VAP group hosting the device.

Repeat for each monitor circuit in all passive interfaces.

Creating Template Circuits

For inline deployments, you must create template circuits and child circuits for the sensing circuits. The series of commands, detailed in the following procedure, creates a template circuit named `bridge_one` for the VAP group named `ABC`:

```
CBS# configure circuit bridge_one
CBS(conf-cct)# vap-group ABC
CBS(conf-cct-vapgroup)# end
CBS#
```

Later, you will configure template circuits as `bridge-mode` bridges and associate them with the appropriate child circuits.

To create template circuits:

Step 1 Create a template circuit that will serve as an inline sensing circuit by entering the following commands separately and in this sequence:

```
CBS# configure circuit bridge_circuit_name
CBS(conf-cct)# vap-group vap_group_name
CBS(conf-cct-vapgroup)# end
CBS#
```

where *bridge_circuit_name* is the name of the bridge circuit you are creating, and *vap_group_name* is the name of the VAP group you want to create and assign to that bridge circuit. For example, to create and assign a VAP group named ABC to a new template circuit named bridge_one, enter the following:

```
CBS# configure circuit bridge_one
CBS(conf-ct)# vap-group ABC
CBS(conf-cct-vapgroup)# end
CBS#
```

Repeat this step for all inline sensing circuits associated with the VAP group. Then repeat the step for each inline sensing circuit on the VAP group. For example, if you want to use two inline sensing circuits on the VAP group, you can create the following template circuits:

- bridge_one_1
- bridge_one_2

Tip You **must** create all template circuits before creating child circuits to ensure that system resources are properly distributed.

Creating Child Circuits

For inline deployments, child circuits provide a logical connection, or a bridge, through a VAP group and between network interfaces. You must configure child circuits using promiscuous-mode active. Later you will connect the child circuits as a bridge-mode bridge configured in transparent mode, as described in Configuring Bridge-Mode Bridges, page 3-10.

The series of commands, detailed in the following procedure, creates two child circuits (a circuit named n1e1 on a device named n1e1, and a circuit named n1e3 on a device named n1e3) for an inline deployment of Cisco NGIPS for Blue Coat X-Series on the VAP group named ABC:

```
CBS# configure circuit n1e1
CBS(conf-cct)# link-state-resistant
CBS(conf-cct)# device-name n1e1
CBS(conf-cct)# vap-group ABC
CBS(conf-cct-vapgroup)# promiscuous-mode active
CBS(conf-cct-vapgroup)# end
CBS# configure circuit n1e3
CBS(conf-cct)# link-state-resistant
CBS(conf-cct)# device-name n1e3
CBS(conf-cct)# vap-group ABC
CBS(conf-cct-vapgroup)# promiscuous-mode active
CBS(conf-cct-vapgroup)# end
CBS#
```

To configure child circuits:

Step 1 Create child circuits for inline interfaces by entering the following commands separately and in sequence:

```
CBS# configure circuit circuit_name
CBS(conf-cct)# link-state-resistant
CBS(conf-cct)# device-name device_name
CBS(conf-cct)# vap-group vap_group_name
CBS(conf-cct-vapgroup)# promiscuous-mode active
CBS(conf-cct-vapgroup)# end
CBS#
```

where *circuit_name* is the name you assign to the circuit, *device_name* is the name of the device hosting the circuit, and *vap_group_name* is the name of the VAP group hosting the device.

Repeat for each child circuit in for all inline interfaces.

Tip Assign easy-to-remember device and circuit names, such as `n1e1`.

Configuring Bridge-Mode Bridges

You create the path from one side of an inline interface through a VAP group to the other side of the inline interface by connecting child circuits in a bridge. The path must be a `bridge-mode` bridge configured in transparent mode. The series of commands, detailed in the following procedure, creates a `bridge-mode` bridge by connecting `n1e1` and `n1e3` on the previously created template circuit called `bridge_one`:

```
CBS# configure bridge-mode bridge_one transparent
CBS(conf-bridge-mode)# circuit n1e1
CBS(conf-bridge-mode)# circuit n1e3
CBS(conf-bridge-mode)# end
CBS#
```

To configure a bridge-mode bridge:

Step 1 Create a `bridge-mode` bridge by using a previously created template circuit and designate it for transparent operation. For example:

```
CBS# configure bridge-mode bridge_circuit_name transparent
```

where *`bridge_circuit_name`* is the name of the template circuit.

Step 2 Add the appropriate circuits to the `bridge-mode` bridge to join the interfaces on each side of the bridge by using the following commands:

```
CBS(conf-bridge-mode)# circuit circuit_name_1
CBS(conf-bridge-mode)# circuit circuit_name_2
CBS(conf-bridge-mode)# end
CBS#
```

where *`circuit_name_1`* and *`circuit_name_2`* are the names of the circuits you want to use on the bridge.

Step 3 Repeat steps 1 and 2 for each inline interface you want to configure.

Associating Physical Ports with Circuits

After you create management and sensing circuits, you must identify which physical ports are used by each circuit. In the example in this chapter:

- the `n1e1` circuit uses ethernet 1/1
- the `n1e3` circuit uses ethernet 1/3
- the `n1e5` circuit uses ethernet 1/5
- the `mgmt` circuit uses ethernet 1/10

The following series of commands, detailed in the following procedure, associates the circuits you created with the correct physical ports:

```
CBS# configure interface ethernet 1/1
CBS(config-intf-gig)# logical n1e1
CBS(intf-gig-logical)# circuit n1e1
CBS(intf-gig-log-cct)# end
CBS# configure interface ethernet 1/3
```

```
CBS(config-intf-gig)# logical n1e3
CBS(intf-gig-logical)# circuit n1e3
CBS(intf-gig-log-cct)# end
CBS# configure interface ethernet 1/5
CBS(config-intf-gig)# logical n1e5
CBS(intf-gig-logical)# circuit n1e5
CBS(intf-gig-log-cct)# end
CBS# configure interface ethernet 1/10
CBS(config-intf-gig)# logical mgmt
CBS(intf-gig-logical)# circuit mgmt
CBS(intf-gig-log-cct)# end
```

To associate physical ports with circuits:

Step 1 Configure an interface.

For example, if you are using the tenth port on the NPM to connect your trusted management network to the **mgmt** circuit, and that port is configured as a Gigabit Ethernet, enter the following command:

```
CBS# configure interface ethernet 1/10
```

Step 2 Define a logical interface for the physical port. You have three options:

– For the management circuit and sensing circuits that do **not** carry VLAN traffic, define the logical interface as follows:

```
CBS(config-intf-gig)# logical logical_circuit_name
```

where *logical_circuit_name* is the name of the logical circuit. For example, if the logical circuit name is `mgmt`, enter the following:

```
CBS(config-intf-gig)# logical mgmt
```

– For sensing circuits that carry VLAN traffic where you want to use the circuit to monitor all the VLAN traffic regardless of the VLAN tag, or where you want to monitor all of the VLANs whose traffic is not being monitored by other, assigned circuits, define the logical interface as follows:

```
CBS(config-intf-gig)# logical-all logical_circuit_name
```

For example, if the logical circuit name is `outside`, enter the following:

```
CBS(config-intf-gig)# logical-all outside
```

– For sensing circuits that carry VLAN traffic where you want to use the circuit to monitor specific VLAN traffic, define the logical interface as follows:

```
CBS(config-intf-gig)# logical logical_circuit_name ingress-vlan-tag low_tag high_tag
```

where *low_tag* and *high_tag* are, respectively, the low and high VLAN channel values. For example, the following command configures the `outside` logical interface to pass traffic that has a VLAN tag of 100:

```
CBS(config-intf-gig)# logical outside ingress-vlan-tag 100 100
```

You can create as many logical interfaces as there are VLAN channels, and map each one to a separate sensing circuit. For more information on configuring circuits to carry VLAN traffic, see the *XOS Configuration Guide*.

Note that although it is not required, Blue Coat recommends naming the circuit and device identically for ease of diagnostics and troubleshooting.

Step 3 Attach the circuit that you created earlier to the logical interface:

```
CBS(intf-gig-logical)# circuit logical_circuit_name
CBS(intf-gig-log-cct)# end
```

where *logical_circuit_name* is the name of the logical circuit. For example, if the logical circuit name is `mgmt`, enter the following:

```
CBS(intf-gig-logical)# circuit mgmt
CBS(intf-gig-log-cct)# end
```

Step 4 Repeat steps 1 through 3 for the other circuits you need to associate with physical ports.

Using Optional Settings

In certain cases, you may need to use optional settings to correctly support your installation:

- If your management circuit is on a different subnet from your Defense Center, create an IP route, as described in Configuring IP Routes, page 3-12.
- If you intend to monitor IPv6 traffic, add support for it as described in Configuring IPv6 Detection, page 3-12.
- If you intend to monitor jumbo frame traffic, add support for it as described in Configuring Jumbo Frame Support, page 3-13.

Configuring IP Routes

If your management circuit is on a different subnet from your Defense Center, you must create an IP route so management traffic can cross subnets.

Step 1 To create an IP route, use the following commands:

```
CBS# configure
CBS(config)# ip
CBS(config-ip)# route vap-group vap_group_name 0.0.0.0/0 gateway_address domain_ID
```

where *vap_group_name* is the name of the VAP group you want to configure and *gateway_address* is the default gateway address for the subnet on which the management circuit resides, and *domain_ID* is the domain ID.

Note If you configured your management circuit to use an alternate domain ID, then, when creating an IP route for that management circuit, the domain ID (`domain 2` in our example) is a necessary part of the command.

For example, the VAP group you set up earlier is on the 10.1.16.0/24 subnet. If your Defense Center is on a different subnet (such as 10.1.17.0/24), you could use the following commands to set up an IP route for the VAP group named `ABC`:

```
CBS# configure
CBS(config)# ip
CBS(config-ip)# route vap-group ABC 0.0.0.0/0 10.1.16.1
    domain 2
CBS(config-ip-route)# exit
CBS(config-ip-route)# end
```

Configuring IPv6 Detection

If your network traffic is predominantly IPv4 with some IPv6, you should use the following configuration to detect the IPv6. This configuration also detects most IPv6 routing protocols and IPv4 to IPv6 transition and tunneling mechanisms.

IPv6 detection is disabled by default. You must enable it through the X-Series CLI on each VAP where you intend to use it.

The procedures used on the Defense Center for IPv6 detection are the same as those used with all devices.

To enable IPv6 support:

Step 1 Enable IPv6 support on for a specific VAP group. For example, enter:

```
CBS# configure vap-group vap_group_name
CBS(config-vap-grp)# enable-ipv6
CBS(config-vap-grp)# end
CBS#
```

where *vap_group_name* is the name of the VAP group you want to configure.

Note that the following information is automatically added to your VAP configuration when you enable IPv6:

```
non-ip-flow-rule ipv6_rule
encapsulation ethernet type 34525
action pass-to-master
activate
```

This information is only created when in Series-6 operating mode. In Series-9 operating mode, this information is no longer seen.

When XOS V10.0 or later is configured for Series-9 operating mode and IPv6 is enabled for the VAP group, IPv6 packets are handled as IP flows and non-IP flow rules do not apply, enabling IPv6 traffic to be load-balanced across VAPs in a VAP group, the same way IPv4 traffic is processed. For more information, see the *XOS Command Reference Guide*.

Configuring Jumbo Frame Support

Unlike configuring jumbo frame settings for other Cisco devices, you do **not** use the Defense Center to configure jumbo frame support for Cisco NGIPS for Blue Coat X-Series.

Instead, if your network traffic uses jumbo frames and you want to properly detect those frames, enable jumbo frame support on each VAP group where you intend to use it. Set the Maximum Transfer Unit (MTU) size to a value from 68 to 9,000 (IPv4) or 1280 to 9,000 (IPv6) on each applicable circuit in the VAP group and then reload the VAP group. The default MTU is 1500. Note that APMs with four cores or less cannot support jumbo frames.

Tip After you initially enable jumbo frames and reload the VAP group, you can change the MTU size without reloading the VAP group.

To enable jumbo frame support:

Step 1 Enable jumbo frame support for the VAP group by entering the following commands separately and in sequence:

```
CBS# configure vap-group vap_group_name
CBS(config-vap-grp)# enable jumbo-frame
CBS(config-vap-grp)# end
CBS#
```

where *vap_group_name* is the name of the VAP group.

Step 2 Set the MTU size for every circuit (including template circuits) in the VAP group. For example:

```
CBS# configure circuit circuit_name
CBS(conf-cct)# vap-group vap_group_name
CBS(conf-cct-vapgroup)# mtu MTU_size
CBS(conf-cct-vapgroup)# end
CBS#
```

where *circuit_name* is the name of the circuit, *vap_group_name* is the name of the VAP group and *MTU_size* is the MTU size. For example, to set the MTU to 9000 on the circuit named `n6g7` on a VAP group named `ABC`, enter the following:

```
CBS# configure circuit n6g7
CBS(conf-cct)# vap-group ABC
CBS(conf-cct-vapgroup)# mtu 9000
CBS(conf-cct-vapgroup)# end
CBS#
```

Note You must configure both circuits in a bridge with identical MTU sizes.

Step 3 To complete the process of enabling jumbo frame support, reload the VAP group by entering the following:

```
CBS# reload vap-group vap_group_name
```

where *vap_group_name* is the name of the VAP group.

For more information, see the *XOS Command Reference Guide*.

Installing Cisco NGIPS for Blue Coat X-Series

To install Cisco NGIPS for Blue Coat X-Series, you must perform the following steps:

- Transfer the application to the Control Processor Module (CPM), as described in Loading Cisco NGIPS for Blue Coat X-Series on the CPM, page 3-14.
- Install and configure the application on the VAP groups, as described in Installing Cisco NGIPS for Blue Coat X-Series on a VAP Group, page 3-15.
- Verify the installation, as described in Verifying the Installation, page 3-16.

In this section, the Cisco NGIPS for Blue Coat X-Series package displays `3D Sensor` on the monitor as the application name of the Cisco NGIPS for Blue Coat X-Series application. It is not the name you give the device, VAP, or VAP groups you create.

Note After you complete the installation process and set up licensing and communication between Cisco NGIPS for Blue Coat X-Series and the Defense Center, you must log onto the Cisco Support site (https://support.sourcefire.com/) and check for updates to the FireSIGHT System, which you can apply using the Defense Center. The release notes accompanying each update include instructions for installing the new software.

Loading Cisco NGIPS for Blue Coat X-Series on the CPM

After you set up VAP groups and circuits, load Cisco NGIPS for Blue Coat X-Series onto the X-Series Control Processor Module (CPM).

To load the software package:

Step 1 Log in to the X-Series platform as `root`:

```
CBS# unix su
```

When prompted, enter the password for your appliance.

Step 2 Copy the Cisco NGIPS for Blue Coat X-Series package `(SF3DSensor-5.4-#.cbi)` to the `/crossbeam/apps/archive` directory on the CPM, where `#` is the build number of Cisco NGIPS for Blue Coat X-Series.

You can use either FTP or SCP to copy the file.

Installing Cisco NGIPS for Blue Coat X-Series on a VAP Group

After you have loaded the Cisco NGIPS for Blue Coat X-Series package on the CPM, install it onto the appropriate VAP group.

Note If you reconfigure your VAP group to use RAID, you must reload the VAP group. The symbolic link to Cisco NGIPS for Blue Coat X-Series is not re-established until the RAID configuration is complete. This can be as long as ten minutes.

To install Cisco NGIPS for Blue Coat X-Series on a VAP group:

Step 1 Enter the following command to display the loaded applications:

```
CBS# show application
```

A list of applications appears. For example:

```
App ID          : Sf3DSensor
Name            : 3D Sensor
Version         : 5.4
Release         : 571
CBI Version     : 1.6.0.0
```

Step 2 Install the software as follows:

```
CBS# application Sf3DSensor version version_number vap-group    vap_group_name install
```

where *`vap_group_name`* is the name of the VAP group where you want to install the software and *`version_number`* is the version you want to install.

For example, to install Version 5.4 on a VAP group named `ABC`, enter the following:

```
CBS# application Sf3DSensor version 5.4 vap-group ABC    install
```

A system check message appears, followed by the end user license agreement (EULA).

Step 3 Read the EULA, then type **y** to accept it.

Step 4 When prompted, enter the name of the management interface.

If you are following the example in this chapter, enter `mgmt`, which is the device name of the `mgmt` circuit that you set up in Configuring the Management Circuits, page 3-5.

Step 5 When prompted, enter the IP address or host name of the Defense Center you will use to manage Cisco NGIPS for Blue Coat X-Series.

Note that to use the host name of the Defense Center, the host name must be resolvable by DNS, and you must have the IP address of at least one DNS server specified in your running configuration. In addition, you must configure the DNS server for each VAP group by entering the following:

```
configure dns server server_ip_address vap-group    vap_group_name
```

where *server_ip_address* is the IP address of the DNS server and *vap_group_name* is the name of the VAP group where you have installed the software. For more information, see the *XOS Configuration Guide*.

Step 6 When prompted, set a registration key for each VAP in the VAP group.

A registration key is a required alphanumeric value you define. Remember your registration keys; you must provide them when adding software devices to the Defense Center.

If you are planning to install Cisco NGIPS for Blue Coat X-Series on multiple VAPs (that is, you have a VAP group with more than one member, or you are creating more than one VAP group), and you are registering the software devices to the same Defense Center, the registration key for each VAP **must** be unique.

Step 7 If a NAT device separates your Cisco NGIPS for Blue Coat X-Series from the Defense Center, follow the prompt to set a unique NAT ID for each VAP in the VAP group.

Unique NAT IDs are used in a network environment with network address translation (NAT). Remember your unique NAT IDs; you must provide them when adding software devices to the Defense Center.

If you plan to install Cisco NGIPS for Blue Coat X-Series on multiple VAPs and you are registering the software devices to the same Defense Center, the NAT ID for each VAP **must** be unique.

Step 8 Press Enter to confirm that you have finished specifying your installation options.

Cisco NGIPS for Blue Coat X-Series is installed.

Step 9 If prompted, reload all VAPs by entering the following command:

```
CBS# reload vap-group vap_group_name
```

where *vap_group_name* is the name of the VAP group where you want to install the software.

Tip The reload prompt appears when you install Cisco NGIPS for Blue Coat X-Series on an existing VAP.

Step 10 Repeat steps 2 through 9 for each VAP group where you are installing Cisco NGIPS for Blue Coat X-Series.

Verifying the Installation

After you install Cisco NGIPS for Blue Coat X-Series, you can verify that it is installed on each of the VAPs where you installed it. If application monitoring is enabled (the default) for a VAP Group, the `show application` command shows you information about the application. The operational state for a VAP can be either **up** or **down**. An operational state of **up** indicates that all VAPs in the VAP group are running and an operational state of **down** indicates that one or more VAPs are not running, or none have been defined. For more information about application monitoring, see Changing Application Monitoring Status, page 5-6.

To verify that Cisco NGIPS for Blue Coat X-Series is running:

Step 1 Show the application information by entering the following command:

```
show application vap-group vap_group_name
```

where *vap_group_name* is the name of the VAP group where the software is installed. For example, to check the state of the application on the VAP group named `ABC`, enter:

```
show application vap-group ABC
```

Step 2 If Cisco NGIPS for Blue Coat X-Series is properly installed the application identity and name are displayed. For example:

```
VAP Group         : ABC
App ID            : Sf3DSensor
Name              : 3D Sensor
Version           : 5.4
Release           : 571
Start on Boot     : yes
App Monitor       : on
Reload on Failure : off
App State (ABC_1) : up
```

If the application identity and name are not correctly displayed, confirm that your Cisco NGIPS for Blue Coat X-Series configuration is correct, then uninstall and reinstall Cisco NGIPS for Blue Coat X-Series. If you continue to have problems, contact Blue Coat support.

Uninstalling Cisco NGIPS for Blue Coat X-Series

If you need to uninstall Cisco NGIPS for Blue Coat X-Series, you can remove it from a VAP group and from an X-Series platform.

To uninstall Cisco NGIPS for Blue Coat X-Series:

Step 1 Uninstall the application from a VAP group by entering the following command:

```
CBS# application Sf3DSensor vap-group vap_group_name uninstall
```

where *vap_group_name* is the name of the VAP group where the software is installed. For example, to uninstall the software on a VAP group named `ABC`, enter the following:

```
CBS# application Sf3DSensor vap-group ABC uninstall
```

At the prompt, enter `Y` to confirm that you want to uninstall the application, or `N` to cancel the `uninstall` command, and receive the following confirmation: `Command canceled by user`

Step 2 Reload all VAPs by entering the following command:

```
CBS# reload vap-group vap_group_name
```

For example, to reload all VAPs on the VAP group named `ABC`, enter the following:

```
CBS# reload vap-group ABC
```

Step 3 If you have uninstalled Cisco NGIPS for Blue Coat X-Series from all the VAP groups in your X-Series platform and have no need to install it to other VAP groups in the future, remove the CBI package with the command:

```
CBS# application-remove Sf3DSensor
```

At the prompt, enter `Y` to confirm that you want to remove the application, or `N` to cancel the `remove` command and receive the following confirmation: `Command canceled by user`

Setting Up the Defense Center

After you install Cisco NGIPS for Blue Coat X-Series, you must set up a Cisco Defense Center to manage the software. These steps include obtaining the proper licenses, adding Cisco NGIPS for Blue Coat X-Series to the Defense Center, and configuring the interfaces.

For more information, see:

- Licensing the FireSIGHT System in the *FireSIGHT System User Guide*
- Adding Cisco NGIPS for Blue Coat X-Series to the Defense Center, page 4-1
- Configuring Security Zones and Inline Sets, page 4-3

For more information on configuring the FireSIGHT System, including access control policies and so on, see the *FireSIGHT System User Guide.*

Adding Cisco NGIPS for Blue Coat X-Series to the Defense Center

You **must** use a Defense Center to manage Cisco NGIPS for Blue Coat X-Series. You use at least two of three fields for configuring communications between appliances:

- **Management Host** — the hostname or IP address
- **Registration Key** — the registration key
- **Unique NAT ID (optional)** — a unique alphanumeric ID (use if a NAT device separates your Cisco NGIPS for Blue Coat X-Series installation from the Defense Center)

Valid combinations include:

- **Management Host** and **Registration Key** on both the Defense Center and Cisco NGIPS for Blue Coat X-Series.
- **Registration Key** and **Unique NAT ID** on Cisco NGIPS for Blue Coat X-Series with **Host, Registration Key,** and **Unique NAT ID** on the Defense Center.
- **Management Host**, **Registration Key**, and **Unique NAT ID** on Cisco NGIPS for Blue Coat X-Series with **Registration Key** and **Unique NAT ID** on the Defense Center.

If you are using VAP groups, consider using device groups to parallel your VAP group configuration.

After you add Cisco NGIPS for Blue Coat X-Series to the Defense Center, use the Defense Center to configure the interfaces, as described in Configuring Security Zones and Inline Sets, page 4-3. For more information on configuring the FireSIGHT System, see the *FireSIGHT System User Guide.*

Tip Obtain and add all licenses to the Defense Center before you add Cisco NGIPS for Blue Coat X-Series to the Defense Center so that you can add licenses when you add the devices to the Defense Center. For information on licensing, see Licensing the FireSIGHT System in the *FireSIGHT System User Guide.*

To add Cisco NGIPS for Blue Coat X-Series to a Defense Center:

Step 1 Log into the Defense Center's web interface using a user account with Administrator access, and select **Devices > Device Management**.

The Device Management page appears.

Step 2 From the **Add** drop-down menu, select **Add Device**.

The Add Device pop-up window appears.

Step 3 In the **Host** field, type the IP address of Cisco NGIPS for Blue Coat X-Series you want to add. This is the IP address that you assigned in Configuring the Management Circuits, page 3-5.

Step 4 In the **Registration Key** field, type the same registration key you set in step 6 of Installing Cisco NGIPS for Blue Coat X-Series on a VAP Group, page 3-15.

Step 5 Optionally, add the device to a device group by selecting the group from the **Group** drop-down list.

You can configure device groups to correspond to VAP groups to make it easier to manage devices. For more information about device groups, see Managing Device Groups in the *FireSIGHT System User Guide*.

Step 6 From the **Access Control Policy** drop-down list, select an initial policy to apply to the device:

- The **Default Access Control** policy blocks all traffic from entering your network.
- The **Default Intrusion Prevention** policy allows all traffic that is also passed by the Balanced Security and Connectivity policy.
- The **Default Network Discovery** policy allows all traffic, which is inspected by network discovery only.
- You can select any existing user-defined access control policy.

For more information, see Using Access Control Policies in the *FireSIGHT System User Guide*.

Step 7 Select licenses to enable on the device. Note that:

- Control and Malware licenses are not supported on Cisco NGIPS for Blue Coat X-Series.
- the URL Filtering license requires a Protection license.
- Although you can enable a Control license on Cisco NGIPS for Blue Coat X-Series, Cisco NGIPS for Blue Coat X-Series does not support fast-path rules, switching, routing, clustering, or NAT.
- Although a FireSIGHT license is enabled on Cisco NGIPS for Blue Coat X-Series, Cisco NGIPS for Blue Coat X-Series does not support geolocation.

For more information, see Licensing the FireSIGHT System in the *FireSIGHT System User Guide*.

Step 8 If you used a NAT ID to identify the Cisco NGIPS for Blue Coat X-Series installation when you configured it to be managed by the Defense Center, expand the **Advanced** section and enter the same NAT ID in the **Unique NAT ID** field.

Step 9 To allow the device to transfer packets to the Defense Center, select the **Transfer Packets** check box.

This option is enabled by default. If you disable it, you completely prohibit packet transfer to the Defense Center.

Step 10 Click **Register**.

The device is added to the Defense Center. Note that it may take up to two minutes for the Defense Center to verify the device's heartbeat and establish communication. You can track the progress of the registration in the task status page (**System > Task Status**). You must add each VAP group member (VAPs) as a device separately. Check the Task Status page to make sure each device is completely installed on the Defense Center before adding the next device.

Cisco NGIPS for Blue Coat X-Series is added to the Defense Center. It can take up to two minutes for the Defense Center to establish communication. You can view the status of Cisco NGIPS for Blue Coat X-Series on the Device Management page (**Devices > Device Management**).

Step 11 Repeat steps 2 through 9 for each software device you want to manage with the Defense Center.

Configuring Security Zones and Inline Sets

Use the web interface of the Defense Center to configure security zones on passive and inline interfaces, and the inline set for inline interfaces.

You create passive and inline sensing interfaces when you install Cisco NGIPS for Blue Coat X-Series, or from the X-Series command line interface (CLI). These interfaces are prepopulated when you add Cisco NGIPS for Blue Coat X-Series to the Defense Center.

You cannot reconfigure any interfaces using the Defense Center. To reconfigure passive or inline interfaces, you must delete and recreate the interface using the X-Series CLI. For more information, see Reconfiguring Interfaces, page 4-4. To reconfigure the management interface, see Changing the Management Interface, page 5-4. For more information on interfaces, see the *FireSIGHT System User Guide*.

To configure the Security Zone or Inline Set on an interface:

Step 1 Log into the Defense Center's web interface using a user account with Administrator access, and select **Devices > Device Management**.

The Device Management page appears.

Step 2 Next to the Cisco NGIPS for Blue Coat X-Series installation that contains the interfaces you want to configure, click the edit icon ( ).

The Interfaces page appears. The inline and passive interfaces you created when you installed Cisco NGIPS for Blue Coat X-Series are prepopulated in the list of interfaces.

Note that for Cisco NGIPS for Blue Coat X-Series, Link always appears up ( ).

Step 3 On the **Interfaces** tab, next to the sensing interface (Inline or Passive) that you want to configure, click the edit icon ( ).

The inline or passive pop-up window appears.

Note You cannot edit the management interface using the Defense Center. To edit the management interface, see Changing the Management Interface, page 5-4.

Step 4 From the **Security Zone** drop-down list, select a existing security zone or select **New** to add a new security zone. For more information on security zones, see the *FireSIGHT System User Guide*.

Step 5 For an inline interface only, from the **Inline Set** drop-down list, select an existing inline set or select **New** to add a new inline set.

Note that if you add a new inline set, you must configure it on the Device Management page (**Devices > Device Management > Inline Sets**) after you set up the inline interface. For more information, see the *FireSIGHT System User Guide.*

Step 6 Click **Save**.

The interface is configured. Note that your changes do not take effect until you apply the device configuration by clicking **Apply Changes** at the top right of the menu bar. See Applying Changes to Devices in the *FireSIGHT System User Guide* for more information.

Reconfiguring Interfaces

You reconfigure an interface by deleting the interface from the Defense Center, deleting the interface from the X-Series platform, then recreating the interface as either passive or inline using the X-Series CLI. You cannot reconfigure an interface from the Defense Center.

Caution Before you use the X-Series CLI to either delete or edit the sensing interfaces in an interface, you **must** use the Defense Center's web interface to delete the interface. You can create a new interface using the Defense Center's web interface after you use the X-Series CLI to configure the sensing interfaces according to the needs of your organization.

To delete an interface from the Defense Center:

Step 1 Log into the Defense Center's web interface using a user account with Administrator access, and select **Devices > Device Management**.

The Device Management page appears.

Step 2 Next to the interface you want to configure, click the edit icon ( ).

The inline or passive interface pop-up window appears.

Step 3 Select **None** from the **None/Passive** or **None/Inline** option, click **Save**, then click **Apply Changes** at the top right of the menu bar for your changes to take effect.

After deleting the interface from the Defense Center, delete the interface using the X-Series CLI, then create a new interface as either passive or inline. See Installing Cisco NGIPS for Blue Coat X-Series, page 3-14, the *XOS Command Reference Guide*, and the *XOS Configuration Guide* for more information.

Managing Cisco NGIPS for Blue Coat X-Series

As a user of Cisco NGIPS for Blue Coat X-Series, you can perform the following tasks using X-Series command line interface (CLI) and the Cisco 3D Sensor Configuration Menu:

- Add additional VAPs to a VAP group. For more information, see Adding Additional VAPs to a VAP Group, page 5-1.
- Edit load-balanced VAP groups. For more information, see Editing Load-Balanced VAP Groups, page 5-2.
- Use the Cisco 3D Sensor Configuration Menu to change various settings for all VAPs in a VAP group. For more information, see Using the Configuration Menu, page 5-3:
  - To change the management interface, see Changing the Management Interface, page 5-4.
  - To change the managing Defense Center, see Changing the Managing Defense Center, page 5-4.
  - To change the registration key, see Changing the Registration Key, page 5-5.
  - To change the unique NAT ID, see Changing the Unique NAT ID, page 5-5.
- To enable or disable application monitoring status, see Changing Application Monitoring Status, page 5-6.
- Learn some useful commands you can perform on your X-Series platform to manage Cisco NGIPS for Blue Coat X-Series. For more information, see Command Reference, page 5-7.

Adding Additional VAPs to a VAP Group

When you add additional VAPs to a VAP group, Cisco recommends that you configure load balancing to include only the existing VAPs. After you configure and apply policies to the additional VAPs, you can reconfigure load balancing to include all VAPs.

VAPs in the VAP group are identified only by number. For example, if you have two VAPs in the VAP group named `ABC`, these two VAPs are identified as `1` and `2`.

To add additional VAPs to a VAP group:

Step 1 Set the `available-vap-list` to include only the existing VAPs by entering the following command:

```
CBS# configure vap-group vap_group_name 1
available-vap-list vap_1 vap_2
```

where *vap_group_name* is the name of the VAP group and *vap_1* is the first VAP in the VAP group, and *vap_2* is the second VAP in the same VAP group, separated by a space. For example, to restrict load balancing to the existing two VAPs on the ABC VAP group, enter the following commands separately and in sequence:

```
CBS# configure vap-group ABC
CBS(config-vap-grp)# available-vap-list 1 2
```

Step 2 Increase the vap-count and the max-load-count by entering the following commands separately and in sequence:

```
CBS(config-vap-grp)# vap-count vap-count-quantity
CBS(config-vap-grp)# max-load-count max-load-quantity
CBS(config-vap-grp)# end
```

where *vap-count-quantity* is the total number of VAPs you want in the VAP group and *max-load-quantity* is the maximum number of VAPs you want in the VAP group. For example, if you have two VAPs in the ABC load-balanced group and want to add two new VAPs, you can increase the vap-count and the max-load-count to 4 by entering the following commands separately and in sequence:

```
CBS(config-vap-grp)# vap-count 4
CBS(config-vapvgrp)# max-load-count 4
CBS(config-vap-grp)# end
```

Step 3 After the new VAPs boot, use the application-update command to install Cisco NGIPS for Blue Coat X-Series:

```
application-update vap-group vap_group_name
```

where *vap_group_name* is the name of the VAP group. For example, you can update the VAP group named ABC by entering the following command:

```
application-update vap-group ABC
```

Step 4 Provide the management interface, sensing interfaces, and management host IP address for the new VAPs.

Step 5 Reload the new VAPs in the VAP group by entering the following command:

```
CBS# reload vap-group vap_group_name vap_3 vap_4
```

where *vap_group_name* is the name of the VAP group, and *vap_3* and *vap_4* are the number that identify the two new VAPs. For example, add the two new VAPs to the VAP group named ABC by entering the following command:

```
CBS# reload vap-group ABC 3 4
```

Step 6 Register Cisco NGIPS for Blue Coat X-Series with the Defense Center and create interfaces. For more information, see Setting Up the Defense Center, page 4-1.

Step 7 Push the appropriate policies to the new VAPs using the user interface on the Defense Center that manages the device. See the *FireSIGHT System User Guide* for more information.

Step 8 Set the available-vap-list back to include all VAPs by entering the following command:

```
CBS# configure vap-group vap_group_name
    available-vap-list vap_1 vap_2 vap_3 vap_3
```

where *vap_group_name* is the name of the VAP group and *vap_1*, *vap_2*, *vap_3* and *vap_4* are the numbers that identify the VAPs. For example:

```
CBS# configure vap-group ABC
    available-vap-list 1 2 3 4
```

Editing Load-Balanced VAP Groups

You may want to add or remove a VAP from a load-balanced VAP group.

To ensure that all packets are processed and not simply passed, you should use multiple VAPs in a load-balanced VAP group. However, you may need to service a VAP, which could cause the VAP to pause in processing while the VAP restarts.

You can prevent traffic from going the a VAP you are servicing by removing the VAP from the available VAP list until you have finished servicing the VAP. Then you can add the VAP to the VAP group and rebalance the load. Make sure you plan these actions for times when they will have the least impact on your deployment.

To edit a load-balanced group:

Step 1 Use the `available-vap-list` command to restrict load balancing to only those VAPs you specify by entering the following commands separately and in sequence:

```
CBS# config vap-group vap_group_name
CBS(config-vap-grp)# available-vap-list vap_1 vap_2 vap_4
CBS(config-vap-grp)# end
```

where *vap_group_name* is the name of the VAP group and *vap_1*, *vap_2*, and *vap_4* are the numbers that identify the VAPs you want to use for load balancing. For example, if you have four VAPs in the `ABC` load-balanced group, but want to exclude *vap_3*, enter the following commands separately and in sequence:

```
CBS# config vap-group ABC
CBS(config-vap-grp)# available-vap-list 1 2 4
CBS(config-vap-grp)# end
```

When you want to reinstate the VAP you removed from the list, add the VAP back to the list by entering the following commands separately and in sequence:

```
CBS# config vap-group ABC
CBS(config-vap-grp)# available-vap-list 1 2 3 4
CBS(config-vap-grp)# end
```

Tip If you cannot remember which device in the Defense Center web interface corresponds to which VAP in your VAP group, you can issue the `show ip addresses` command from the X-Series CLI. Keep in mind that when you assign your devices sequential IP addresses, they are assigned in VAP-group order. For example, if you assign 10.1.1.1 through 10.1.1.10 to VAPs in a group named `ABC`, you know that `ABC_1` has an IP address of 10.1.1.1, and so on. You might also want to use the Device Management page on the Defense Center web interface to name your software devices according to their VAP number.

Using the Configuration Menu

The configuration menu allows you to make several changes to the VAP settings. After you use the X-Series CLI, the following menu is displayed:

```
3D Sensor Configuration Menu
1. Configure Management Interface
2. Configure Defense Center
3. Configure the Registration Key
4. Configure the NAT ID
5. Exit
Enter choice [5]:
```

Enter the configuration menu, then use the configuration menu to change the following settings for VAPs in a VAP group:

To enter the configuration menu :

Step 1 Enter the following command at the X-Series CLI prompt:

```
application Sf3DSensor vap-group vap_group_name config
```

where *vap_group_name* is the name of the VAP group where Cisco NGIPS for Blue Coat X-Series is installed.

Follow the procedures to change your configuration:

- To change the management interface, see Changing the Management Interface, page 5-4.
- To change the managing Defense Center, see Changing the Managing Defense Center, page 5-4.
- To change the registration key, see Changing the Registration Key, page 5-5.
- To change the NAT ID, see Changing the Unique NAT ID, page 5-5.

Changing the Management Interface

The following procedure explains how to change the management interface for a VAP group.

To change the management interface:

Step 1 From the Configuration Menu, select **1 Configure Management Interface** to change the management interface.

Step 2 When prompted, enter the device name configured for the new management interface. This is the device name attached to the circuit.

Step 3 From the Configuration Menu, select **5 Exit** to quit.

Step 4 Modify the corresponding circuit to use the new device name.

For more information, see Configuring the Management Circuits, page 3-5.

Step 5 Enter the following command to restart the application:

```
application Sf3DSensor vap-group vap_group_name restart
```

where *vap_group_name* is the name of the VAP group.

Changing the Managing Defense Center

The following procedure explains how to change the managing Defense Center for a VAP group using the following steps:

Step 1 Delete Cisco NGIPS for Blue Coat X-Series from its managing Defense Center using the Device Management page (**Devices > Device Management**). See the *FireSIGHT System User Guide* for more information.

Step 2 Change the managing Defense Center for the VAP group using the procedure described in this section.

Step 3 Re-add Cisco NGIPS for Blue Coat X-Series to the new managing Defense Center as described in Adding Cisco NGIPS for Blue Coat X-Series to the Defense Center, page 4-1.

Note You **must** delete managed Cisco NGIPS for Blue Coat X-Series installations from the Defense Center before changing the managing Defense Center for a VAP group.

To change the managing Defense Center:

Step 1 From the Configuration Menu, select **2 Configure Defense Center**.

Step 2 When prompted, enter the IP address or host name of the Defense Center you want to manage Cisco NGIPS for Blue Coat X-Series.

Note that to use the host name of the Defense Center, the host name must be resolvable by DNS, and you must have the IP address of at least one DNS server specified in your running configuration. In addition, you must configure the DNS server for each VAP group (`configure dns server` *`server_ip_address`* `vap-group` *`vap_group_name`*). For more information, see the *XOS Configuration Guide*.

Step 3 From the Configuration Menu, select **5 Exit** to quit.

Changing the Registration Key

A registration key is a required alphanumeric value you define that you must provide when you add a device to the Defense Center.

If you install Cisco NGIPS for Blue Coat X-Series on multiple VAPs (that is, you have a VAP group with more than one member, or you are creating more than one VAP group), and you are registering the software devices to the same Defense Center, the registration key for each VAP **must** be unique.

Note If you change the registration key, you must re-register the device to the Defense Center. Changing the registration key breaks the connection between the device and its managing Defense Center.

To change the registration key:

Step 1 From the Configuration Menu, select **3 Configure the Registration Key** to change the registration key.

Step 2 When prompted, enter the registration key.

If there are multiple VAPs in the VAP group, enter the registration key for each VAP in the VAP group.

Step 3 From the Configuration Menu, select **5 Exit** to quit.

Changing the Unique NAT ID

A unique NAT ID is an alphanumeric value used in a network environment that uses network address translation (NAT).

If you install Cisco NGIPS for Blue Coat X-Series on multiple VAPs (that is, you have a VAP group with more than one member, or you are creating more than one VAP group), and you are registering the software devices to the same Defense Center, the unique NAT ID for each VAP **must** be unique.

Note If you change the NAT ID, you must re-register the device to the Defense Center. Changing the NAT ID breaks the connection between the device and its managing Defense Center.

To change the Unique NAT ID:

Step 1 From the Configuration Menu, select **4 Configure the NAT ID** to change the Unique NAT ID.

Step 2 When prompted, enter the unique NAT ID.

If there are multiple VAPs in the VAP group, enter the NAT ID for each VAP in the VAP group.

Step 3 From the Configuration Menu, select **5 Exit** to quit.

Changing Application Monitoring Status

Application monitoring tracks whether your VAPs are running and halts load balancing of new flows to VAPs with failed VAPs.

If application monitoring is enabled (the default) for a VAP group, the operational state for a VAP can be either **up** or **down**. An operational state of **up** indicates that all the VAP are running. With application monitoring enabled, an operational state of **down** indicates that at least one of the VAP has failed, or that Cisco NGIPS for Blue Coat X-Series running on the VAP group was stopped manually.

If application monitoring is disabled, the X-Series platform displays the operational state as **Not Monitored** and sends flows to the VAP, regardless of the actual operational state.

You may want to disable application monitoring in a few situations, including:

- deployments where you are using more than one interface per VAP

  In this situation, if you disable application monitoring and an interface fails, the X-Series platform continues to send flows to the VAP and the other interfaces on the VAP can continue their analysis. However, note that flows directed to the failed interface will not be analyzed.

  On the other hand, if you are taking advantage of the load balancing and redundancy benefits of the X-Series platform by deploying intrusion prevention on multiple identically-configured VAPs, you may want to leave application monitoring enabled. You may experience some packet loss as old flows directed to the degraded VAP time out, but the X-Series platform will load-balance new flows to the other VAPs in the VAP group.
- if you have deployed Cisco NGIPS for Blue Coat X-Series inline, and you need to stop the application on the VAP group

  This avoids the situation where the X-Series platform halts traffic to the VAP group when you stop the application. Halting traffic in an inline deployment can cause a network outage.

To check and change application monitoring status:

Step 1 Check the application monitoring state by entering the following command:

```
show vap-group vap_group_name
```

where *vap_group_name* is the name of the VAP group where Cisco NGIPS for Blue Coat X-Series is installed.

Locate *Application Monitoring (true/false):* near the bottom of the output and ensure that state is: *t* (for true)

Step 2 If application monitoring is disabled and you to enable it, enter the command:

```
configure vap-group vap_group_name application-monitor
```

Step 3 If application monitoring is enabled and you to disable it, enter the command:

```
configure vap-group vap_group_name no application-monitor
```

Command Reference

The following table lists useful commands for controlling Cisco NGIPS for Blue Coat X-Series. Note that *vap_group_name* is the name of the VAP group where the software is installed.

Table 5-1 Command Reference

To...	Enter the following commands...
start Cisco NGIPS for Blue Coat X-Series	`application Sf3DSensor vap-group vap_group_name start`
stop Cisco NGIPS for Blue Coat X-Series	`application Sf3DSensor vap-group vap_group_name stop`
restart Cisco NGIPS for Blue Coat X-Series	`application Sf3DSensor vap-group vap_group_name restart`
uninstall Cisco NGIPS for Blue Coat X-Series	`application Sf3DSensor vap-group vap_group_name uninstall` After you uninstall the application, reload the VAP group (`reload vap-group vap_group_name`). For more information, see Uninstalling Cisco NGIPS for Blue Coat X-Series, page 3-17.
install the software on unconfigured VAPs	`application-update vap-group vap_group_name` The update command is used when the VAP count of the VAP group is incremented, after the application configuration. When the update completes, you must reload the VAP group with the command: *reload vap-group vap_group_name vap#.* For more information, see Adding Additional VAPs to a VAP Group, page 5-1.
display all applications installed on a VAP group and to show their state as up or down	`show application vap-group vap_group_name`

log into an active VAP	`CBS# unix su`
	`[root@machine admin]# rsh vap_group_name_index_number`
	where *index_number* is an index number of the VAP.
	Note that this is a concatenation of the terms *vap_group_name* and *index_number* and that the underbar is required. For example, `SF_1` or `SF_2` where `SF` is the *vap_group_name* and `1` and `2` are the `index_number`.

run Cisco-specific commands	`source /opt/sf/profile` Run this command prior to running other Cisco commands on the Cisco command line interface. For example, if you need to run Cisco-specific commands for troubleshooting, first source the correct profile with this command.