Installation and Configuration Guide for IPS Deployments of IBM Proventia Network IPS on Crossbeam X-Series Systems

Part Number 005245A
May 2008

Copyright and Trademark Information

Copyright © 2008 by Crossbeam Systems
Boxborough, MA, USA

All Rights Reserved

The products, specifications, and other technical information regarding the products contained in this document are subject to change without notice. All information in this document is believed to be accurate and reliable, but is presented without warranty of any kind, expressed or implied, and users must take full responsibility for their application of any products specified in this document. Crossbeam Systems disclaims responsibility for errors that may appear in this document, and it reserves the right, in its sole discretion and without notice, to make substitutions and modifications in the products and practices described in this document.

This material is protected by the copyright and trade secret laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Crossbeam Systems), except in accordance with applicable agreements, contracts, or licensing, without the express written consent of Crossbeam Systems.

For permission to reproduce or distribute please contact your Crossbeam Systems account executive.

This product includes software developed by the Apache Software Foundation: www.apache.org.

“Crossbeam,” “Crossbeam Systems,” “iBeam,” X40, X45, X80 and any logos associated therewith are trademarks or registered trademarks of Crossbeam Systems, Inc. in the U.S. Patent and Trademark Office, and several international jurisdictions.

All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

Contents

About This Guide

IBM Proventia® Network IPS v.2.0 for Crossbeam stops Internet threats before they impact your business network, and delivers complete protection to all three layers of the network: core, perimeter, and remote segments. The Proventia Network IPS employs multiple intrusion prevention technologies which are all highly integrated to work in tandem, providing unprecedented correlation and protection mechanisms. These core technologies enable pre-emptive protection of the network against a wide variety of Internet threats.

The Crossbeam X-Series system's unique, modular architecture lets you:

- Consolidate your security solutions — You can run the Proventia Network IPS application side-by-side with other best-of-breed security applications running on separate Application Processor Modules (APMs) in the same X-series chassis.
- Scale the application's performance — You can scale up the performance of the Proventia Network IPS application by running the application on multiple APMs simultaneously.
- Provide users with hardware and software high availability — When you deploy the Proventia Network IPS application on multiple APMs, each APM provides both hardware and software redundancy for the others. In addition, you can install an extra APM in the X-series chassis and use it as a replacement for any APM that fails while running the Proventia Network IPS application.

  The hardware high availability features in the X-series system also include redundant switch fabrics and a passive backplane, as well as redundant hot swappable fans, power supplies, and modules. In addition, you can deploy Crossbeam X-series systems in active/active or active/standby modes with either Single-Box High Availability (SBHA) and/or Dual-Box High Availability (DBHA) modes.

The combined solution is jointly engineered, tested, and certified by both IBM and Crossbeam, ensuring compatibility of the Proventia Network IPS application with all Crossbeam X-series chassis.

This guide explains how to install and configure the IBM Proventia Network IPS application for Intrusion Prevention System (IPS) deployments on Crossbeam X-series systems.

IMPORTANT: This guide covers only IPS deployments of the Proventia Network IPS application. For information on installing and configuring the application as an Intrusion Detection System (IDS), refer to the Installation and Configuration Guide for *IDS Deployments of IBM Proventia Network IPS on Crossbeam X-Series Systems*.

Intended Audience

This guide is intended for system integrators and other qualified service personnel responsible for installing, configuring, and managing software on Crossbeam X-Series systems.

Related Documentation

Crossbeam Systems Documentation

The following documents are provided on the Crossbeam Systems Documentation CD and are available on the Crossbeam Systems Customer Support web site located at http://www.crossbeam.com/services/online_support.php.

- *X40-X80 Security Services Switch Hardware Installation Guide*
- *X45 Security Services Switch Hardware Installation Guide*
- *XOS Configuration Guide*
- *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 Power NGX R65*
- *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 Power VSX NGX R65*
- *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 NGX Layer-2 Firewall*
- *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 Power VSX NGX R65 with Bridged Virtual Systems*
- *XOS Command Reference Guide*
- *Install Server User Guide*
- *XOS V8.1 Release Notes*

IBM Documentation

The following documents are available on the IBM Internet Security Systems (ISS) documentation web site located at http://www.iss.net/support/documentation.

- *Installation and Configuration Guide for IDS Deployments of Proventia Network IPS on Crossbeam X-Series Systems*
- *Proventia Network IPS for Crossbeam X-Series Hardware User Guide*
- *Proventia Network IPS Data Sheet*
- *Proventia Network IPS Frequently Asked Questions*
- *SiteProtector System Requirements*
- *SiteProtector Installation Guide*
- *SiteProtector Configuration Guide*
- *SiteProtector Technical Reference Guide*

You can also access the Proventia Network IPS Help System via the Proventia Manager or via SiteProtector's Proventia Network IPS Policy Editor, and you can access the SiteProtector Help System via the SiteProtector Console.

The IBM ISS support knowledgebase is another valuable source of information. Visit the knowledgebase at http://www.iss.net/support/knowledgebase. You can search the knowledgebase using key words or Answer IDs.

For the most current information about product issues and updates, and for information on contacting IBM Customer Support, download the Readme file at http://www.iss.net/download.

Conventions

Typographical Conventions

For paragraph text conventions, see Table 1 on page 9.

For command-line text conventions, see Table 2 on page 10.

Table 1. Typographical Conventions Used in Paragraph Text

Typographical Convention	Types of Information	Usage Examples
Bold	Elements on the graphical user interface.	In the **IP Address** field, type the IP address of the first VAP in the group. Click **OK** to close the dialog. Select the **Print to File** check box.
`Courier`	Keys on the keyboard. File names, folder names, and command names. Any information that you must type exactlly as shown. Program output text.	Press `Esc` to return to the main menu. Save the `user.txt` file in the `user_install` directory. Use the `start` command to start the application. In the **Username** field, type `Administrator`. The XOS CLI `show calendar` command displays the system calendar: `Fri Mar  7 13:32:03 2008`
`Courier Italic`	File names, folder names, command names, or other information that you must supply.	In the **Version Number** field, type `8.1.`*`patch_number`*.
>	A sequence of commands from the task bar or menu bar.	From the taskbar, choose **Start > Run**. From the main menu, choose **File > Save As...** Right-click on the desktop and choose **Arrange Icons By > Name** from the pop-up menu.

Table 2. Typographical Conventions Used in Command-Line Text

Typographical Convention	Types of Information	Usage Examples
`Courier`	User prompts and program output text.	`CBS# show calendar` `Fri Mar 7 13:32:03 2008`
`Courier Bold`	Information that you must type in exactly as shown.	`[root@xxxxx]# md crossbeam`
`<Courier Italic>`	Angle brackets surrounding Courier italic text indicate file names, folder names, command names, or other information that you must supply.	`[root@xxxxx]# md <your_folder_name>`
[ ]	Square brackets contain optional information that may be supplied with a command.	`[root@xxxxx]# dir [drive:] [path] [<filename>] [/P] [/W] [/D].`
|	Separates two or more mutually exclusive options.	`[root@xxxxx]# verify [ON|OFF]`
{ }	Braces contain two or more mutually exclusive options from which you must choose one.	`CBS# configure vap-group <VAP_group_name>` `CBS(config-vap-grp)# raid {0|1}`

Cautions, Warnings, and Notes

Caution: Lists precautions that you must take to avoid temporary data loss or data unavailability.

Warning: Lists precautions that you must take to avoid personal injury, permanent data loss, or equipment damage.

IMPORTANT: Lists important steps that you must perform properly or important information that you must take into consideration to avoid performing unnecessary work.

NOTE: Provides special information or tips that help you properly understand or carry out a task.

Crossbeam Systems Customer Support

Crossbeam Systems offers a variety of service plans designed to meet your specific technical support requirements. For information on purchasing a service plan for your organization, please contact your account representative or refer to http://www.crossbeam.com/services/support_overview.php.

If you have purchased a Crossbeam Systems product service plan and need technical assistance, you can report issues by telephone:

United States: +1 800-331-1338 **OR** +1 978-318-7595

EMEA: + 33 4 9228 8989 (during normal working hours)
+1 978-318-7595 (outside office hours and on public holidays, if applicable)

Asia Pacific: +1 978-318-7595

You can also report issues via email to support@crossbeamsystems.com.

In addition, all of our service plans include access to the Crossbeam Online Support web site located at http://www.crossbeam.com/services/online_support.php.

The Crossbeam Online Support web site provides you with access to a variety of resources, including Customer Support Knowledgebase articles, technical bulletins, product documentation, and release notes. You can also access our real-time problem reporting application, which lets you submit new technical support requests and view all your open requests.

Crossbeam Systems also offers extensive customer training on all of its products. Please refer to the Crossbeam Training and Education web site located at http://www.crossbeam.com/services/training_education.php for current course offerings and schedules.

IBM Customer Support

IBM ISS provides technical support through its Web site, by email, and by telephone.

The IBM Internet Security Systems (IBM ISS) Resource Center Web site, located at, http://www.iss.net/support, provides direct access to online user documentation, current firmware version listings, detailed product literature, white papers, and the Technical Support Knowledgebase.

Support levels IBM ISS offers three levels of support:

- Standard
- Select
- Premium

Each level provides you with 24x7 telephone and electronic support. Select and Premium services provide more features and benefits than the Standard service. Contact Client Services at clientservices@iss.net if you do not know the level of support your organization has selected.

Table 3 on page 12 provides IBM ISS Technical Support contact information and hours of operation for the Americas and other locations.

Table 3. IBM ISS Customer Support Contact Info and Hours of Operation

Location	Electronic Support	Telephone Numbers	Hours of Operation
North America	Connect to the MYISS section of the Web site: http://www.iss.net	Standard: (1) (888) 447-4861 (toll free) (1) (404) 236-2700 Select and Premium: Refer to your Welcome Kit or call your Primary Designated Contact for this information.	24 hours a day
Latin America	support@iss.net	(1) (888) 447-4861 (toll free) (1) (404) 236-2700	
Europe, Middle East, and Africa	support@iss.net	(44) (1753) 845105	Monday through Friday, 9:00 A.M. to 6:00 P.M. local time, excluding IBM ISS published holidays **Note:** If your local support office is located outside the Americas, you may call or send an email to the Americas office for help during off-hours.
Asia-Pacific, Australia, and the Philippines	support@iss.net	(1) (888) 447-4861 (toll free) (1) (404) 236-2700	
Japan	support@isskk.co.jp	Domestic: (81) (3) 5740-4065	

1

Introduction to the Proventia Network IPS v.2.0 for Crossbeam

This chapter describes how the Proventia Network IPS application operates on the Crossbeam X-Series platform, and describes the configuration options available for the IBM Proventia Network IPS v.2.0 for Crossbeam.

This chapter contains the following sections:

Proventia Network IPS v.2.0 for Crossbeam

IBM Proventia® Network IPS v.2.0 for Crossbeam stops Internet threats before they impact your business network, and delivers complete protection to all three layers of the network: core, perimeter, and remote segments. The Proventia Network IPS employs multiple intrusion prevention technologies which are all highly integrated to work in tandem, providing unprecedented correlation and protection mechanisms. These core technologies enable pre-emptive protection of the network against a wide variety of Internet threats.

The Crossbeam X-Series system's unique, modular architecture lets you:

- Consolidate your security solutions.
- Scale the application's performance.
- Provide users with hardware and software high availability.

The combined solution is jointly engineered, tested, and certified by both IBM and Crossbeam, ensuring compatibility of the Proventia Network IPS application with all Crossbeam X-series chassis.

This section explains the Crossbeam X-Series system architecture and explains how the Proventia Network IPS application operates on an X-Series system.

X-Series System Architecture Overview

The Crossbeam X-Series system running the XOS software is an open-networked application platform designed to deliver enhanced application services while providing high performance and high availability. The X-Series system's modular design allows it to run multiple applications, while providing multi-gigabit throughput performance for all applications.

The Crossbeam X-Series system has a unique, modular architecture design, which provides performance scalability for applications running on the X-Series system, and which provides high availability in case of module failure.

Each X-Series system contains three types of hardware modules:

- Control Processor Module (CPM) maintains overall system configuration, management, and integrity.
- Application Processor Module (APM) hosts a Virtual Application Processor (VAP). A VAP is a set of applications, such as the Proventia Network IPS, which process packets belonging to individual flows.

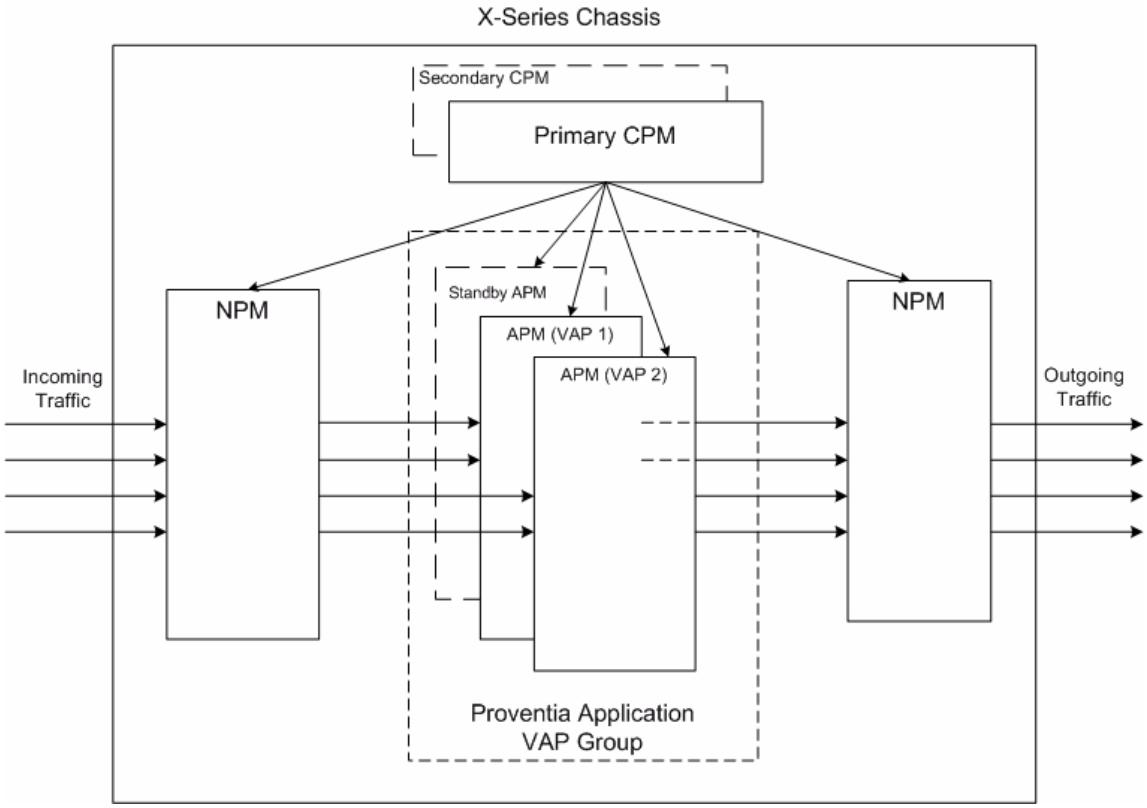
  You install the Proventia Network IPS on a VAP group, which may contain one or more VAPs. If the application's VAP group contains multiple VAPs, you can configure the X-Series system to load-balance traffic across all VAPs in the group.
- Network Processor Module (NPM) provides network connectivity for the X-Series system, classifies packets, and load-balances flows among groups of APMs.

An X-Series system can be configured to provide high availability for all three types of modules and to provide performance scalability for NPMs and APMs.

Refer to Hardware Requirements on page 27 for information about the X-Series chassis and modules that are supported for use with the Proventia Network IPS application.

Figure 1 on page 14 shows how traffic flows through an X-Series system with the Proventia Network IPS application installed on two APMs in an X-Series chassis that contains two CPMs, two NPMs, and three APMs.

Figure 1. High-Level X-Series System Architecture



Proventia Network IPS Application VAPs and VAP Groups

A Virtual Application Processor (VAP) is an application operating environment that runs on an APM. A VAP consists of the OS, system software, and a set of applications (such as the Proventia Network IPS) that run concurrently.

A VAP group is a collection of APMs configured to provide load-balanced network services to run applications installed on the VAP group and to provide high availability to those applications in the event of an APM failure.

The Proventia Network IPS application is installed on a VAP group that consists of one or more VAPs. Each VAP on which the Proventia Network IPS application is installed can function as a single Proventia GC1200 appliance, but if the VAP group contains more than one VAP, all of the appliances (VAPs) in the group act in concert with each other, creating a virtual processing engine comprised of APMs.

The NPM load-balances packet flows among all functioning VAPs in the group, as shown in Figure 1 on page 14; therefore, application performance increases significantly each time an APM is added to the VAP group.

Before you install the Proventia Network IPS application, you must first use the XOS CLI to configure a VAP group, defining the number of VAPs in the group by setting the VAP count and using other parameter settings to control the assignment of VAPs to physical APMs. Refer to Creating and Configuring a VAP Group for the Proventia Application on page 35 for more information.

XOS Configuration of Application Data and Management Interfaces

Before installing the Proventia Network IPS application, you must use the XOS CLI to configure the interfaces that the application will use to monitor traffic and respond to network security threats. You must also use the CLI to configure the interface that Proventia Manager and SiteProtector will use to manage the application. Refer to Basic XOS Configuration Procedures on page 34 for information about configuring interfaces in XOS.

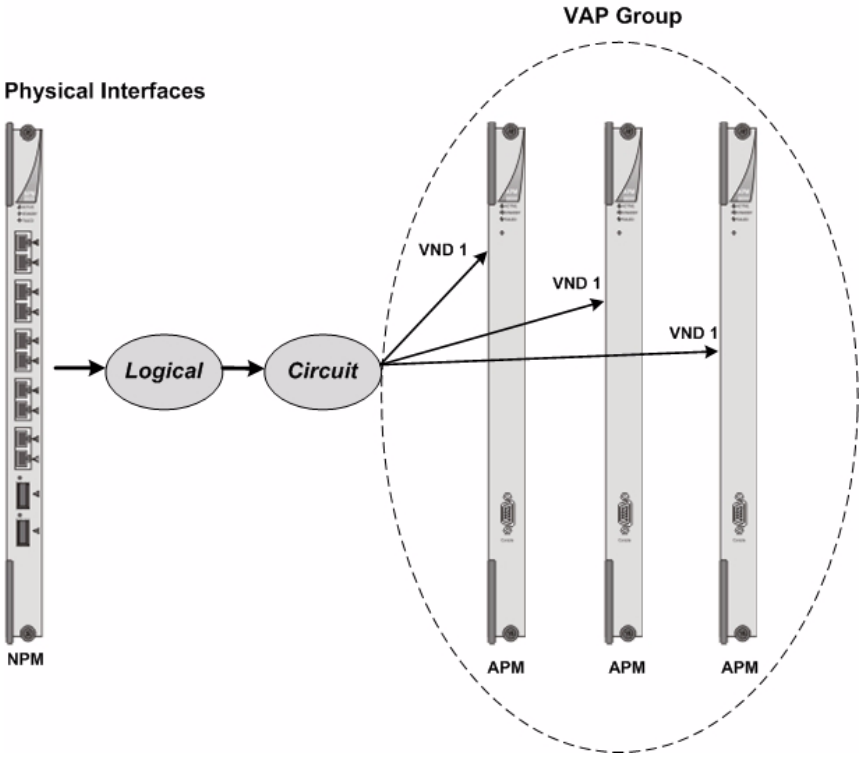
Within XOS, application management and data interfaces have four types of components: physical interfaces, logical interfaces, circuits, and Virtual Network Devices (VNDs). Within XOS, each physical interface on the NPM that is to be used to pass traffic in or out of the VAP group must be mapped to one or more logical interfaces. Each logical interface is then mapped to a circuit.

In addition, some circuits may be defined and configured to pass traffic between multiple VAP groups installed on the same X-Series system. These circuits do not need to be mapped to physical interfaces on the NPM unless the circuits will also be used to pass traffic to and from the X-Series system, since all APMs are connected by a shared data plane.

VAPs see all circuits as VNDs.

Figure 2 on page 16 shows the different components of an XOS configuration of a management or data interface.

Figure 2. XOS Configuration Components of an Application Data or Management Interface



The Proventia Network IPS application treats VNDs as adapter ports on the Proventia GC1200 appliance. Each VAP functions as a separate Proventia GC1200 appliance, while each VAP group functions as an appliance group, or cluster.

NOTE: Although the Proventia Network IPS application treats all VNDs as “adapter ports”, the number of VNDs is often not equal to the number of physical ports on the NPM. Some physical ports on the NPM may be mapped to multiple circuits, and any circuits configured solely to pass traffic between VAP groups within the same X-Series system are not mapped to any physical interface.

In Proventia Manager and SiteProtector, all circuits configured in XOS are represented as VNDs, and all individual physical interfaces configured as part of a single “group interface” for a Multi-Link Trunk (MLT) are also represented at VNDs.

IPS Configuration Options

Before installing the IBM Proventia Network IPS, you must decide how you are going to configure the application. The following sections describe the supported configuration options for the Proventia Network IPS application when it is deployed as an Intrusion Prevention System (IPS) on one or more Crossbeam X-series systems.

IPS Modes of Operation

This section describes the following supported Intrusion Prevention System (IPS) modes of operation :

For more information on these modes, refer to the *Proventia Network IPS for Crossbeam X-Series Hardware User Guide* located on the ISS documentation web site located at http://www.iss.net/support/documentation.

Inline Simulation Mode

In Inline Simulation mode, the application monitors the network passively, without affecting traffic patterns.

While in this mode, the application uses the traditional Block response and the Quarantine response, but it does not drop packets when they trigger these responses. By default, the application also does not send TCP Reset packets to stop a connection if the application detects suspicious TCP network activity.

You can use Inline Simulation mode to baseline and test your security policy without affecting network traffic.

Inline Protection Mode

In Inline Protection mode, the application monitors the network and actively responds to events.

While in this mode, the application uses the Block and Quarantine responses, enforces all firewall rules, and applies all security policies that you define for the application.

Software Bypass Modes of Operation

When the Proventia Network IPS application cannot analyze packets, it may enter one of two Software Bypass modes of operation:

- **Forward Unanalyzed Packets:** Forward packets without processing them; fail open.
- **Drop Unanalyzed Packets:** Drop packets without processing them; fail closed.

The application resumes normal packet analysis as soon as all problems/conditions are resolved.

When installed on a Crossbeam X-series system, the Proventia Network IPS application enters a Software Bypass mode of operation when one or more of the following conditions occur:

- The throughput on the X-series chassis exceeds the application's ability to examine all the packets.
- The application fails to extract packets for examination for the amount of time specified (via Proventia Manager or SiteProtector) for an Application Stall event.
- The application restarts; application restarts occur during the following events:
  - Any of the following policies are configured.
    - Quarantined Intrusions
    - Responses
    - Connection Events
    - User Defined Events
    - OpenSignature Events
    - Global Tuning Parameters
    - Firewall Settings
    - Local Tuning Parameters
  - The user applies security content updates.
  - The user applies firmware updates.

By default, the Proventia Network IPS application's Software Bypass mode is set to Forward Unanalyzed Packets, but you can change this setting via the **Local Tuning Parameters** page in Proventia Manager or SiteProtector. See the *Proventia Network IPS for Crossbeam X-Series Hardware User Guide* for more information on configuring the Software Bypass mode for the Proventia Network IPS application.

Network Topology Configuration Options

The following sections describe the supported network topology configuration options for the Proventia Network IPS application when it is deployed an Intrusion Prevention System (IPS) on a Crossbeam X-series system:

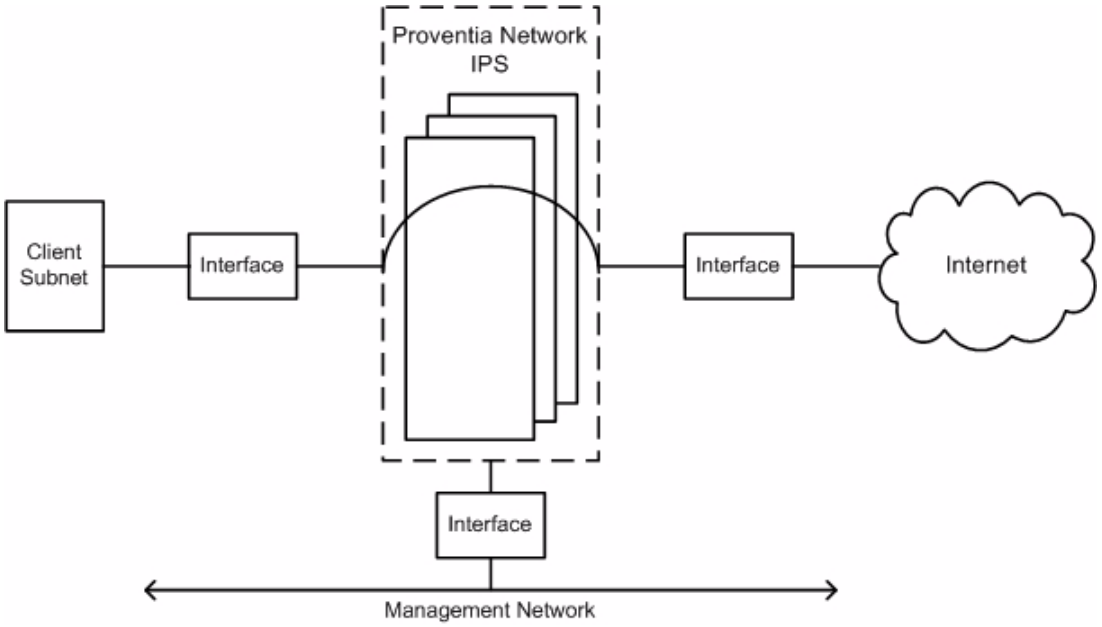
- Standalone IPS on page 19
- Standalone IPS with Dual-Box High Availability (DBHA) on page 20
- Serialization with Proventia Network IPS and Check Point VPN-1 Power NGX R65 on page 21
- Serialization with Proventia Network IPS and Check Point VPN-1 Power VSX NGX R65 on page 22
- Serialization with Proventia Network IPS and Check Point VPN-1 NGX Layer-2 Firewall on page 23
- Serialization with Proventia Network IPS and Check Point VPN-1 Power VSX NGX R65 with Bridged Virtual Systems on page 24
- Serialization with Two Proventia Network IPS VAP Groups and One Check Point VPN-1 Power VSX NGX R65 VAP Group on page 25

Standalone IPS

In this scenario, Proventia Network IPS is the only application running on the system. The application can be running in Inline Simulation or Inline Protection mode.

Figure 3 on page 19 shows a topology diagram that illustrates this option.

Figure 3. Standalone IPS



This topology may include any of the following types of bridge interfaces:

- Simple Interface — Defined as a single circuit mapped to a single physical interface.
- Simple Interface with redundancy
- Multi-Link Trunk (MLT)
- VLAN Trunk (802.1q) (up to 4094 VLANs)
- VLAN Trunk over MLT

You can configure a maximum of 128 bridges.

See Creating and Configuring Bridge Circuits on page 38 for basic syntax on configuring bridges.

See Standalone IPS Examples on page 50 for examples of configuring bridges in XOS for the types of interfaces supported for this network topology.

Standalone IPS with Dual-Box High Availability (DBHA)

In this scenario, Proventia Network IPS is installed standalone on two systems in a network environment configured for Dual-Box High Availability (DBHA). The Proventia Network IPS application may be operating in Inline Simulation or Inline Protection mode.

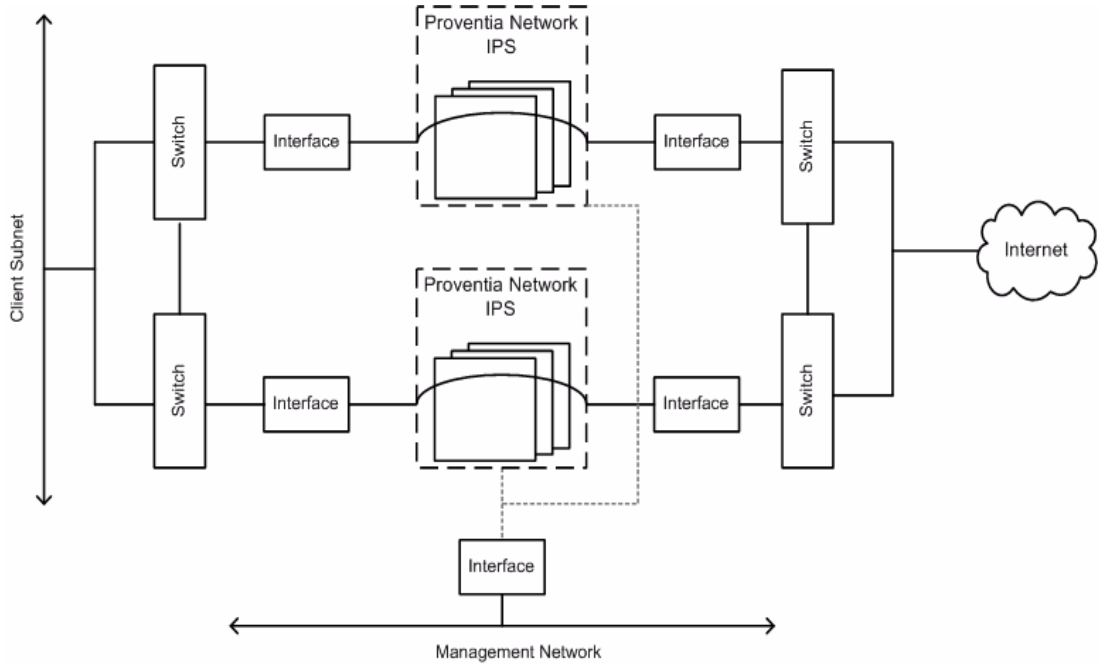
NOTE: While this model does provide DBHA, each system is autonomous, without any knowledge of the other system, its state, or its health.

A successful DBHA configuration depends upon external devices configured to provide failure detection and traffic failover in the event that one X-Series system fails. These external devices must provide this functionality by using a dynamic routing protocol or by using a redundant path protocol, such as Spanning Tree Protocol (STP).

External systems must be configured to ensure that all packets in a flow are sent to a single X-series system. The application will not inspect asymmetric traffic because the application's stateful inspection functionality requires that every packet in a flow be inspected by a single Proventia Network IPS appliance.

Figure 4 shows a topology diagram that illustrates this option.

Figure 4. Standalone IPS with Dual-Box High Availability



You must manually configure SiteProtector to put both chassis in the same SiteProtector group and push the same policies to both chassis; SiteProtector will not do this automatically.

This topology may include any of the following types of bridge interfaces; you can configure up to 128 bridges.

- Simple Interface — Defined as a single circuit mapped to a single physical interface.
- Simple Interface with redundancy
- Multi-Link Trunk (MLT)
- VLAN Trunk (802.1q) (up to 4094 VLANs)
- VLAN Trunk over MLT

See Creating and Configuring Bridge Circuits on page 38 for basic syntax on configuring bridges.

See Standalone IPS with Dual-Box High Availability (DBHA) Example on page 54 for an example of configuring bridges in XOS to support this network topology.

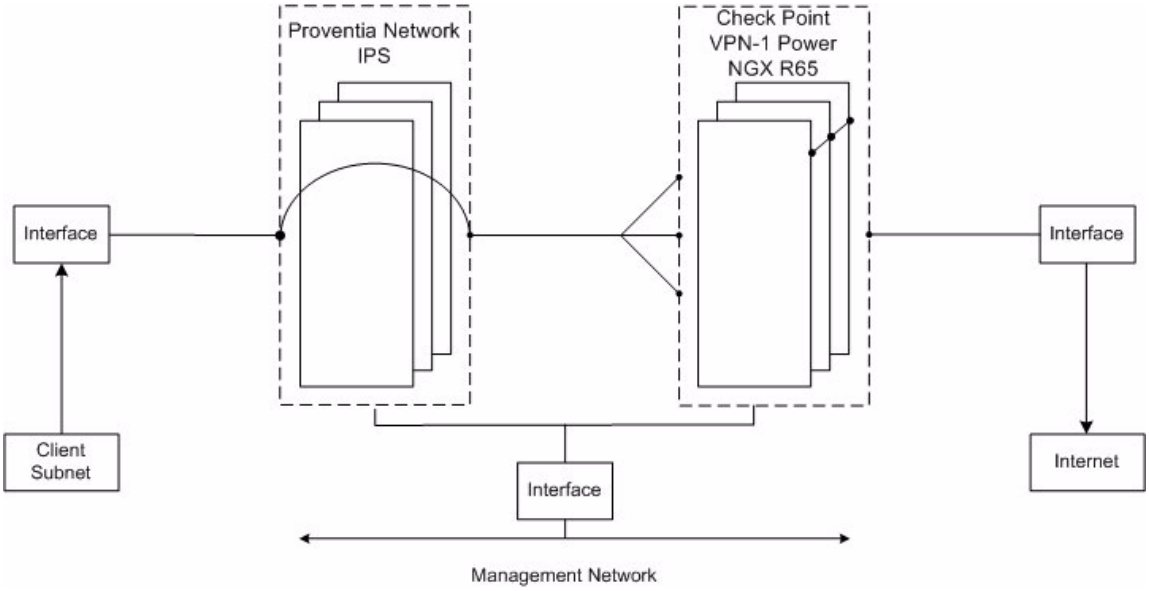
Serialization with Proventia Network IPS and Check Point VPN-1 Power NGX R65

In this scenario, the Proventia Network IPS is serialized with a Layer 3 deployment of the Check Point VPN-1 Power NGX R65 application running on the same X-series system. The Proventia application may be operating in Inline Simulation or Inline Protection mode.

See *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 Power NGX R65* for more information about this topology configuration option.

Figure 5 on page 21 shows a topology diagram of this option.

Figure 5. Serialization with Proventia Network IPS and Check Point VPN-1 Power NGX R65



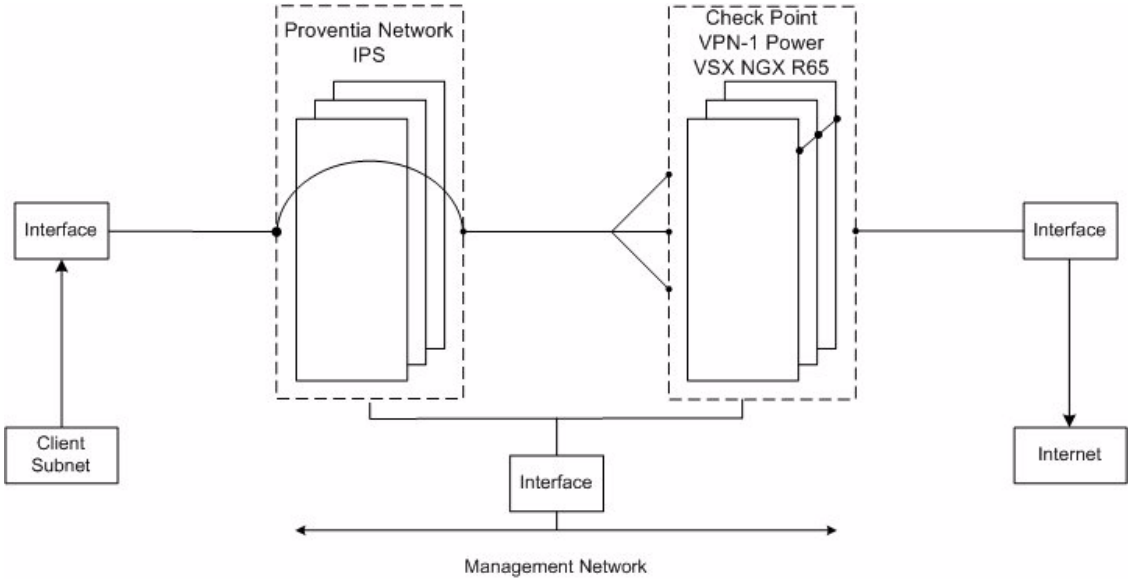
Serialization with Proventia Network IPS and Check Point VPN-1 Power VSX NGX R65

In this scenario, the Proventia Network IPS is serialized with a Layer 3 deployment of the Check Point VPN-1 Power VSX NGX R65 application running on the same X-series system. The Proventia application may be operating in Inline Simulation or Inline Protection mode.

See *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 Power VSX NGX R65* for more information about this topology configuration option.

Figure 6 on page 22 shows a topology diagram of this option.

Figure 6. Serialization with Proventia Network IPS and Check Point VPN-1 Power VSX NGX R65



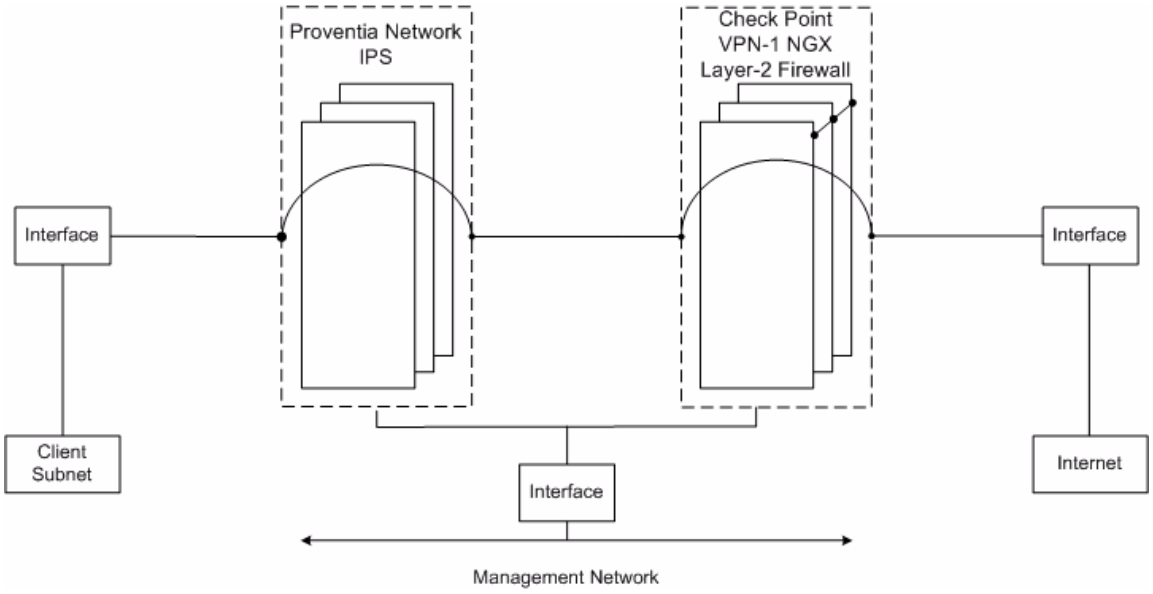
Serialization with Proventia Network IPS and Check Point VPN-1 NGX Layer-2 Firewall

In this scenario, the Proventia Network IPS application is serialized with the Check Point VPN-1 NGX Layer-2 Firewall application running on the same X-series system. The Proventia Network IPS application may be operating in Inline Simulation or Inline Protection mode.

See *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 NGX Layer-2 Firewall* for more information about this topology configuration option.

Figure 7 on page 23 shows a topology diagram that illustrates this option.

Figure 7. Serialization with Proventia Network IPS and Check Point VPN-1 NGX Layer-2 Firewall



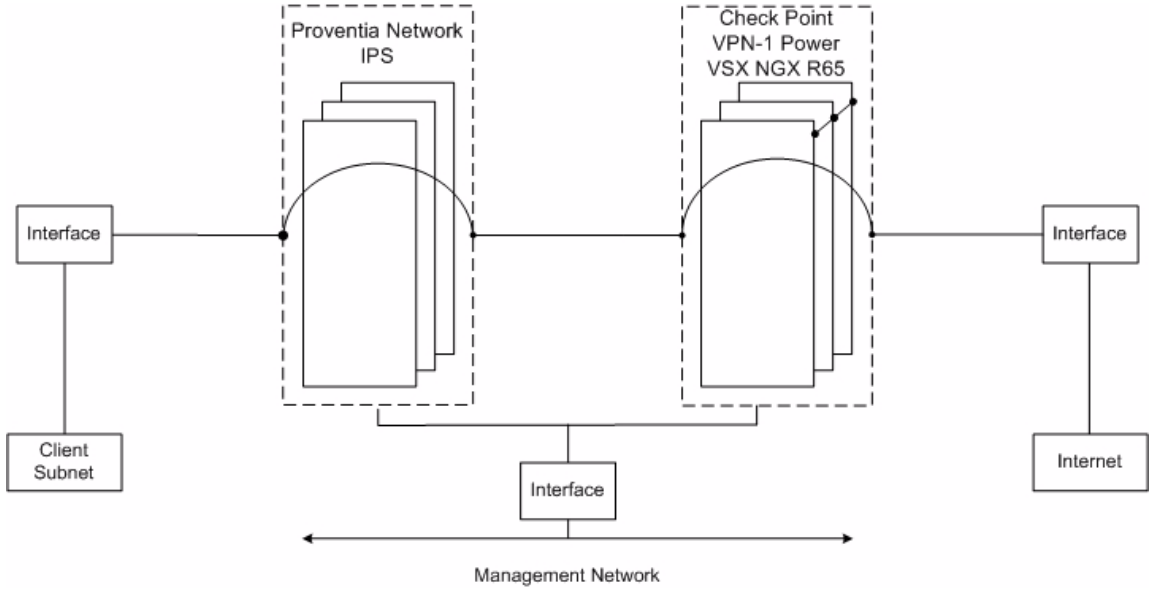
Serialization with Proventia Network IPS and Check Point VPN-1 Power VSX NGX R65 with Bridged Virtual Systems

In this deployment scenario, the Proventia Network IPS is serialized with a Layer 2 deployment of the Check Point VPN-1 Power VSX NGX R65 application running on the same X-series system. The Proventia Network IPS application may be operating in Inline Simulation or Inline Protection mode.

See *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 Power VSX NGX R65 with Bridged Virtual Systems* for more information about this topology configuration option.

Figure 8 on page 24 shows a topology diagram that illustrates this option.

Figure 8. Serialization with Proventia Network IPS and Check Point VPN-1 Power VSX NGX R65 with Bridged Virtual Systems



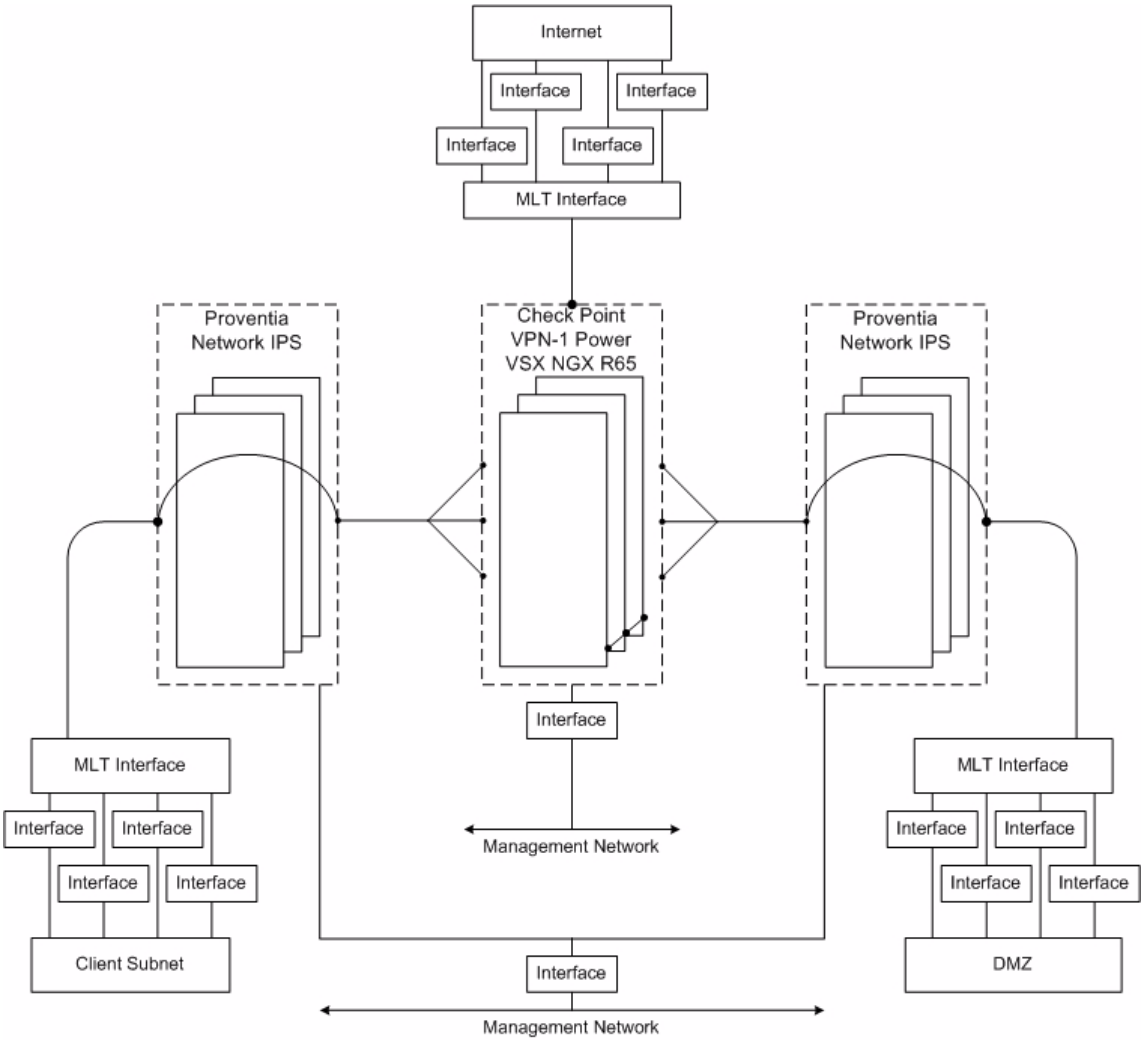
Serialization with Two Proventia Network IPS VAP Groups and One Check Point VPN-1 Power VSX NGX R65 VAP Group

In this scenario, two instances of the Proventia Network IPS application are serialized with a Layer 3 deployment of Check Point VPN-1 Power VSX NGX R65. Each instance of the Proventia Network IPS application may be operating in Inline Simulation or Inline Protection mode.

See *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 Power VSX NGX R65* for more information about this topology configuration option.

Figure 9 on page 25 shows a topology diagram that illustrates this option.

Figure 9. Serialization with Two Proventia Network IPS VAP Groups and One Check Point VPN-1 Power VSX NGX R65 VAP Group



2

Hardware, Software, and Network Requirements

This chapter provides a list of the hardware, software, and network configuration requirements for installing the IBM Proventia Network IPS application as an Intrusion Prevention System (IPS) on a Crossbeam X-Series system. This chapter contains the following sections:

Hardware Requirements

Before installing the Proventia Network IPS application, you must make sure the system meets the following hardware requirements.

General Requirements

- The system must include only the supported models of Crossbeam hardware components listed in Table 4 and Table 5 on page 28.
- All models of Control Processor Modules (CPMs), Network Processor Modules (NPMs), and Application Processor Modules (APMs) included in the same X-series chassis must be compatible with one another. Refer to the Crossbeam *X40/X80 Security Switch Hardware Installation Guide* and *X45 Security Switch Hardware Installation Guide* for detailed module compatibility matrices.

Network Processor Module (NPM) Requirements

- If the Proventia Network IPS is to be serialized with another application (such as a Check Point firewall), the X-Series system must be running in Series-6 NPM mode. Multi-application serialization deployments are not supported in Series-2 NPM mode.

Application Processor Module (APM) Requirements

- All of the Application Processor Modules (APMs) in a virtual application processor (VAP) group must be the same model. (Each VAP group must contain only APM-8400s or only APM-8600s.)
- Each APM must have a minimum of 2 GB of RAM. (4 GB is recommended.)

  NOTE: Crossbeam recommends that all APMs have the same amount and type of memory installed on them.

- Each APM on which the Proventia Network IPS application is installed must have at least one local hard drive installed on the module.

  NOTE: An APM-8600 can have two local hard drives installed on the module. In this case, the hard drives can be configured to use RAID 0, RAID 1, or no RAID at all. See the *XOS Configuration Guide* for more details on configuring RAID settings on local hard drives installed on APM-8600s.

- Each APM on which the Proventia Network IPS application is installed must have the same number of local hard drives installed on it. If the APMs have two local drives installed on them, each pair of drives must have the same RAID configuration (RAID 0, RAID 1, or no RAID).
- If a single local hard drive is installed on an APM-8600, that drive must be installed in the slot labeled “SATA 1”.

Table 4. Supported Chassis

Chassis	Supported Models	Additional Notes
X40 chassis	AC-1, AC-2, AC-3	None
X45 chassis	AC-3	AC-3 is supported only with NPM-8600, NPM-8200, NPM-8210, APM-8600, and CPM-8600 modules.
X80 chassis	AC-1, AC-2, AC-3, DC-1, DC-2	None

Table 5. Supported Modules

Module	Supported Models	Additional Notes
Control Processor Module (CPM)	CPM-8100, CPM-8400, CPM-8600	None
Network Processor Module (NPM)	NPM-8200, NPM-8210, NPM-8600	Multi-application serialization deployments are supported only with NPM-8600s.
Application Processor Module (APM)	APM-8400, APM-8600*	APM-8400 is supported only with dual CPUs. APM-8600 is supported with single and dual CPUs.

*Optimal performance is achieved with APM-8600s.

Software Requirements

Before installing the Proventia Network IPS application, you must make sure the system meets the XOS software version compatibility and configuration requirements listed in the following sections:

- Software Version Compatibility Requirements on page 29
- XOS Configuration Requirements on page 29
- Required Crossbeam Installation (CBI) Package on page 31

Software Version Compatibility Requirements

The Proventia Network IPS application is supported on Crossbeam X-Series systems that run XOS version 8.1 and later.

For information on Proventia Network IPS application version support, refer to the *XOS V8.1 Release Notes*.

XOS Configuration Requirements

Before installing the Proventia Network IPS application, you must complete the following XOS configuration procedures:

- Configure an IP domain name for the X-series system on which the application is to be installed.

  See Configuring an IP Domain Name for the X-Series System on page 35 for instructions.
- Create and configure a VAP group for the application.

  See Creating and Configuring a VAP Group for the Proventia Application on page 35 for instructions.
- If desired, configure the system to enable dual-box high availability (DBHA).

  See Configuring the System to Enable Dual-Box High Availability (DBHA) on page 36 for instructions.
- Create and configure a management circuit for the application and map the circuit to the application's VAP group.

  See Creating and Configuring a Management Circuit on page 37 for instructions.
- Create and configure the parent and child circuits for the bridge, and map all circuits to the application's VAP group.

  See Creating and Configuring Bridge Circuits on page 38 for instructions.

The above components of the XOS configuration must meet the requirements listed in the following sections:

VAP Group Configuration Requirements

- The VAP group on which you plan to install the application cannot have any other applications installed on it.
- The application's VAP group must be configured to use the `xslinux_v3` kernel (the default setting for a VAP group configuration).
- The application's VAP group must have a max load count equal to its VAP count.
- A DNS server must be configured for the VAP group on which the application is to be installed.
- All VAPs in the application's VAP group must be UP before the application can be installed.
- Crossbeam and IBM recommend that you configure a fully-qualified domain name (FQDN) for each VAP in the VAP group. SiteProtector and Proventia Manager will display each VAP's FQDN along with the IP address assigned to that VAP's management interface.

Circuit Configuration Requirements

- All circuits must be configured with user-specified device names, using the `device-name <device_name>` parameter. Device names are used to identify circuits displayed in SiteProtector and Proventia Manager.

Management Circuit Configuration Requirements

- If the X-Series system is running in Series-2 NPM mode, the management circuit must be configured with the `ip-flow-rule-no-failover` option.
- The management circuit must be configured with the `increment-per-vap` parameter, even if the VAP group contains only one VAP.
- The management circuit must be configured with the `management-circuit` option.
- The physical link to the management circuit must be UP before the application can be installed.

Bridge Circuit Configuration Requirements

- Each bridge parent circuit (also called a template circuit) can have only two bridge child circuits associated with it.
- All bridge child circuits must be configured with the `promiscuous-mode active` parameter.
- All bridges must be configured in transparent mode, using the `configure bridge-mode <bridge_parent_circuit_name> transparent` command.
- Because egress traffic is assigned to a specific SDP based on the bridge child circuit's ID number, Crossbeam recommends that you optimize egress traffic load-balancing by configuring all bridge child circuits with consecutive circuit IDs, using one of the following methods:
  - Allow XOS to assign all circuit IDs automatically. Configure the management circuit first, configure all bridge parent (template) circuits next, and configure all bridge child circuits last. This ensures that XOS will assign consecutive circuit IDs to all of the bridge child circuits.
  - Configure each circuit with the following command:

    `CBS# configure circuit <circuit_name> device-name <device_name> circuit-id <ID_number>`

    Make sure you assign consecutive circuit ID numbers to all bridge child circuits. For example, if you are configuring two bridges, you can manually assign circuit IDs 1024, 1025, 1026, and 1027 to the four bridge children.

Dual-Box High Availability (DBHA) Configuration Requirements

- You must create **identical** VAP group and IP flow rule configurations on the two X-Series systems.
- You must configure every circuit with **the same** circuit name, circuit ID, and device name on both X-Series systems.

NOTE: The following DBHA configuration requirements apply only when the Proventia Network IPS is deployed as a Standalone application and when the Proventia Network IPS is serialized with a Layer 2 deployment of a Check Point application.

- The network topology for the DBHA configuration must include external switches configured to distribute traffic between the two X-Series systems, and to provide redundancy functionality in the event that one X-Series system fails. These external devices must provide loop-prevention functionality by using a redundant path protocol such as Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP).
- You must configure a system-non-ip-flow-rule to direct the NPM to pass spanning-tree traffic from the external switches to the master VAP in the VAP group on each system:

- If the external switches utilize STP, RSTP, or Multiple Spanning Trees (MST), configure the following system-non-ip-flow-rule:

```
system-non-ip-flow-rule <flow_rule_name>
    encapsulation lsap any
    action pass-to-masters
    activate
```

- If the external switches utilize Per-VLAN Spanning Tree (PVST+) or Rapid Per-VLAN Spanning Tree (RPVST+), configure the following system-non-ip-flow-rule:

```
system-non-ip-flow-rule <flow_rule_name>
    encapsulation snap any
    action pass-to-masters
    activate
```

- If the application's VAP group contains more than one VAP, you must configure the VAP group with the `master-failover-trigger application` parameter. This parameter tells the system to re-elect a new master VAP if the application fails on the current master VAP, thereby preventing Layer 2 looping issues on the network.

Additional XOS Configuration Requirements

- If you wish to install the Proventia Network IPS application on multiple VAP groups on the same X-series system, you must install the application on each VAP group separately. You cannot install the application on multiple VAP groups at the same time.

Required Crossbeam Installation (CBI) Package

To run the CBI for the Proventia Network IPS application, you must first place the following CBI package into the `/crossbeam/apps/archive` directory on the CPM:

`issprovg-2.0-1.cbi`

See Copying the Crossbeam Installation (CBI) Package onto the X-Series System on page 41 for instructions on obtaining the CBI package.

Network Configuration Requirements

Before installing the Proventia Network IPS application, make sure your network meets the following configuration requirements:

- All physical network connections required to support the desired application deployment and configuration options must be functioning normally before the application is installed. (See IPS Configuration Options on page 17 and Advanced Configurations: Support for Communication between Internal Subnets on page 77 for a list of options you can choose.)
- The physical link to the management circuit must be UP before the application can be installed.
- The network topology for a DBHA configuration must include external switches configured to distribute traffic between the two X-Series systems, and to provide redundancy functionality in the event that one X-Series system fails. These external devices must provide loop-prevention functionality by using a redundant path protocol such as Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP).

  NOTE: This requirement applies only when the Proventia Network IPS is deployed as a Standalone application and when the Proventia Network IPS is serialized with a Layer 2 deployment of a Check Point application.

3

Preparing for Installation

This chapter describes the procedures that you must perform before installing the Proventia Network IPS on a Crossbeam X-series system.

NOTE: This chapter describes how to configure the XOS prior to installing Proventia Network IPS as a standalone application. For instructions on configuring XOS to enable a multi-application serialization deployment, see the following Crossbeam documents:

- *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 Power NGX R65*
- *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 Power VSX NGX R65*
- *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 NGX Layer-2 Firewall*
- *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 Power VSX NGX R65 with Bridged Virtual Systems*

This chapter contains the following sections:

Pre-Installation Procedure Overview

Before installing the IBM Proventia Network IPS, you must perform the following steps:

1. Read the Crossbeam Systems and IBM documents listed in Prerequisite Reading on page 34.

   You must have a thorough understanding of this material before attempting to install, configure, and run the IBM Proventia Network IPS application.

2. Make sure the X-series system meets all the requirements listed in Hardware Requirements on page 27 and Software Version Compatibility Requirements on page 29.

3. Choose the configuration options that you want to implement upon installation of the Proventia Network IPS application.

   See IPS Configuration Options on page 17 for descriptions of the specific options that you can choose.

4. Configure all the physical network connections required for the configuration options that you have chosen.

5. Configure the XOS to meet all the requirements listed in XOS Configuration Requirements on page 29 and Network Configuration Requirements on page 31.

   Basic XOS Configuration Procedures on page 34 contains instructions on configuring XOS to meet the basic requirements.

Prerequisite Reading

Before installing the Proventia Network IPS application on a Crossbeam X-series system, you must have a thorough understanding of the material presented in the following documents:

- Crossbeam documents available on the Crossbeam documentation CD and on the Crossbeam Customer Support web site located at http://www.crossbeamsystems.com/service-support/on-line.cfm:
  - *XOS Configuration Guide*
  - *XOS Release Notes*
- IBM documents available on the IBM ISS documentation web site located at http://www.iss.net/support/documentation:
  - *Proventia Network IPS for Crossbeam X-Series Hardware User Guide*
  - *Proventia Network IPS Data Sheet*
  - *Proventia Network IPS Frequently Asked Questions*

If the Proventia Network IPS application is to be serialized with a Check Point application, review the appropriate Crossbeam documentation for your network topology configuration. The following documents are located on the Crossbeam documentation CD and on the Crossbeam Customer Support web site located at http://www.crossbeamsystems.com/service-support/on-line.cfm:

- *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 Power NGX R65*
- *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 Power VSX NGX R65*
- *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 NGX Layer-2 Firewall*
- *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 Power VSX NGX R65 with Bridged Virtual Systems*

Basic XOS Configuration Procedures

To meet the basic XOS configuration requirements, you must perform the following tasks:

- Configure an IP domain name for the X-series system on which the application is to be installed.

  See Configuring an IP Domain Name for the X-Series System on page 35 for instructions.
- Create and configure a VAP group for the application.

  See Creating and Configuring a VAP Group for the Proventia Application on page 35 for instructions.
- If desired, configure the system to enable dual-box high availability (DBHA).

  See Configuring the System to Enable Dual-Box High Availability (DBHA) on page 36 for instructions.
- Create and configure a management circuit for the application and map the circuit to the application's VAP group.

  See Creating and Configuring a Management Circuit on page 37 for instructions.
- Create and configure the circuits for the bridge, and map all circuits to the application's VAP group.

  See Creating and Configuring Bridge Circuits on page 38 for instructions

Configuring an IP Domain Name for the X-Series System

Configure an IP domain name for the X-series system on which the application is to be installed:

```
CBS# configure ip domainname <domain_name>
```

where *<domain_name>* is an alphanumeric string, which may include characters, such as dashes and symbols.

For example:

```
CBS# configure ip domainname mycompany.com
```

Creating and Configuring a VAP Group for the Proventia Application

1. Create a VAP group for the Proventia Network IPS application and configure it to use the xslinux_v3 kernel:

   ```
   CBS# configure vap-group <VAP_group_name> xslinux_v3
   ```

2. Set the VAP count and the max load count for the VAP group to be equal to the number of APMs that you plan to include in the VAP group:

   ```
   CBS(config-vap-grp)# vap-count <number_of_APMs_in_group>
   CBS(config-vap-grp)# max-load-count <number_of_APMs_in_group>
   ```

3. Configure the AP list for the VAP group:

   ```
   CBS(config-vap-grp)# ap-list <ap_name1> [<ap_name2>] [<ap_name3>] ...
   ```

   where *<ap_name#>* is the name that the XOS has assigned to the APM.

   IMPORTANT: Make sure the AP list includes only APM-8400s or only APM-8600s. Use the `show chassis` command to determine the model numbers and assigned names of the APMs in your chassis.

4. If the VAP group contains APM-8600s, each APM has two local hard drives, and you wish to configure RAID 0 or 1, use the following command to do so:

   ```
   CBS(config-vap-grp)# raid {0|1}
   ```

5. Configure a basic IP flow rule for the VAP group:

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

6. Configure a DNS server for the VAP group:

   ```
   CBS# configure dns server <server_ip_addr> vap-group <VAP_group_name>
   ```

   where *<server_ip_addr>* is the DNS server's IP address and *<VAP_group_name>* is the name of the VAP group on which the Proventia Network IPS application is to be installed.

7. If desired, use the following command to configure a unique FQDN **for each VAP,** and map the FQDN to the IP address that you plan to assign to that VAP's management interface.

   ```
   CBS# configure host <management_ip_address> <hostname>.<domain_name>
   ```

   where:

   - *<management_ip_address>* is the IP address that you plan to assign to the management interface for this VAP.

     See Creating and Configuring a Management Circuit on page 37 for instructions on assigning IP addresses to the management interfaces for the VAPs in a VAP group.

   - *<hostname>* is the unique hostname assigned to the VAP.
   - *<domain_name>* is the IP domain name that you configured for the X-series system.

     See Configuring an IP Domain Name for the X-Series System on page 35 for instructions on configuring an IP domain name for the X-series system.

   When you configure an FQDN for a VAP, you can use Proventia Manager to login to that VAP by entering its hostname in a Web browser URL (`https://<FQDN>`). If you do not configure an FQDN for a VAP, when you want to use Proventia Manager to login to that VAP, you must enter the IP address assigned to the management circuit for that VAP (`https://<management_IP_address>`).

Configuring the System to Enable Dual-Box High Availability (DBHA)

NOTE: The following procedure is required to enable DBHA functionality only when the Proventia Network IPS is deployed as a Standalone application and when the Proventia Network IPS is serialized with a Layer 2 deployment of a Check Point application.

IMPORTANT: For a DBHA configuration to function, you must create **identical** VAP group and IP flow rule configurations on the two X-Series systems. In addition, you must configure every circuit with **the same** circuit name, circuit ID, and device name on both systems.

Perform the following steps **on each X-Series system**.

1. If the VAP group has more than one VAP, configure the VAP group with the following commands:

   ```
   CBS# configure vap-group <VAP_group_name>
   CBS(config-vap-grp)# master-failover-trigger application
   CBS(config-vap-grp)# end
   ```

2. Configure a system-non-ip-flow-rule to enable the external switches to direct traffic to the master VAP in the VAP group on each system:

   - If the external switches use STP, RSTP, or MST, configure the system-non-ip-flow-rule, as follows:

     ```
     CBS# configure system-non-ip-flow-rule <flow_rule_name>
     CBS(conf-system-non-ip-flow-rule)# encapsulation lsap any
     CBS(conf-system-non-ip-flow-rule)# action pass-to-masters
     CBS(conf-system-non-ip-flow-rule)# activate
     ```

   - If the external switches use PVST+ or RPVST+ , configure the system-non-ip-flow-rule, as follows:

     ```
     CB# configure system-non-ip-flow-rule <flow_rule_name>
     CBS(conf-system-non-ip-flow-rule)# encapsulation snap any
     CBS(conf-system-non-ip-flow-rule)# action pass-to-masters
     CBS(conf-system-non-ip-flow-rule)# activate
     ```

Creating and Configuring a Management Circuit

1. Create a management circuit, assign a device name to the circuit, and map the circuit to the application's VAP group:

   ```
   CBS# configure circuit <management_circuit_name> device-name
   <management_circuit_device_name>
   CBS(conf-cct)# vap-group <VAP_group_name>
   CBS(conf-cct-vapgroup)# management-circuit
   ```

   IMPORTANT: During installation, the value that you enter when prompted for the `Management Port Interface` must be the same as the value that you enter for *<management_circuit_device_name>* above. If these two values do not match, the management circuit will not work.

2. If the X-Series system is running in Series-2 NPM mode, configure the management circuit with the `ip-flow-rule-no-failover` option:

   ```
   CBS(conf-cct-vapgroup)# ip-flow-rule-no-failover
   ```

3. Configure the management circuit to use a unique IP address to access each VAP in the group:

   ```
   CBS(conf-cct-vapgroup)# ip <ip_address_of_first_VAP_in_group>/<netmask>
   <broadcast_address> increment-per-vap <ip_address_of_last_vap_in_group>
   CBS(conf-cct-vapgroup)# end
   ```

4. Assign the management circuit to a physical interface:

   ```
   CBS# configure interface {fastethernet | gigabitethernet | 10gigabitethernet}
   <NPM_slot_number>/<port_number>
   CBS(conf-intf-<iftype>)# logical <logical_name>
   CBS(intf-<iftype>-logical)# circuit <management_circuit_name>
   CBS(intf-<iftype>-logical)# end
   ```

   NOTE: On NPM-8600s, ports 11 and 12 support only 10 Gigabit Ethernet.

5. Configure a default IP route for the management circuit to use to communicate with the VAP group:

   ```
   CBS# configure ip route <first_ip_address_in_range>/<netmask>
   <next_hop_IP_address> vap-group <VAP_group_name> circuit
   <management_circuit_name>
   ```

   For example:

   ```
   CBS# configure ip route 190.1.1.0/24 192.213.212.111 vap-group
   iss circuit mgmt
   ```

Creating and Configuring Bridge Circuits

IMPORTANT: The bridge configuration described in this section does not support communication between internal subnets. To enable communication between internal subnets, use one of the two bridge configurations described in Advanced Configurations: Support for Communication between Internal Subnets on page 77.

NOTE: This section explains how to configure circuits for a bridge that uses two simple, non-redundant interfaces. For examples of bridge circuits configured to use more complex interfaces, see Example XOS Configurations for Supported Single-Application Use Cases on page 49.

Create and configure circuits with simple interfaces and create a bridge, as follows:

1. Create a bridge parent circuit (also called a template circuit), assign a device name to the circuit, and map the circuit to the application's VAP group:

```
CBS# configure circuit <bridge_parent_circuit_name>
CBS(conf-cct)# device-name <bridge_parent_circuit_device_name>
CBS(conf-cct)# vap-group <bridge_parent_circuit_VAP_group_name>
CBS(conf-cct-vapgroup)# end
```

2. Create a bridge child circuit for the ingress interface, assign a device name to the circuit, and map the circuit to the application's VAP group:

```
CBS# configure circuit <ingress_circuit_name>
CBS(conf-cct)# device-name <ingress_circuit_device_name>
CBS(conf-cct)# vap-group <VAP_group_name>
```

3. Place the circuit in promiscuous mode active, so that it functions as part of a bridge:

```
CBS(conf-cct-vapgroup)# promiscuous-mode active
CBS(conf-cct-vapgroup)# end
```

4. Create another bridge child circuit for the egress interface, assign a device name to the circuit, and map the circuit to the application's VAP group:

```
CBS# configure circuit <egress_circuit_name>
CBS(conf-cct)# device-name <egress_circuit_device_name>
CBS(conf-cct)# vap-group <egress_circuit_VAP_group_name>
```

5. Place the circuit in promiscuous mode active, so that it functions as part of a bridge:

```
CBS(conf-cct-vapgroup)# promiscuous-mode active
CBS(conf-cct-vapgroup)# end
```

6. Create the bridge by assigning the child circuits to the bridge parent (template) circuit.

   IMPORTANT: You must configure the bridge in transparent mode. If you configure the bridge in bridge mode, the application will not work properly.

```
CBS# configure bridge-mode <bridge_parent_circuit_name> transparent
CBS(conf-bridge-mode)# circuit <ingress_circuit_name>
CBS(conf-bridge-mode)# circuit <egress_circuit_name>
```

7. Assign the child circuits to physical interfaces:

```
CBS# configure interface {fastethernet | gigabitethernet | 10gigabitethernet}
<NPM_slot_number>/<port_number>
CBS(conf-intf-<iftype>)# logical <logical_name>
CBS(intf-<iftype>-logical)# circuit <ingress_circuit_name>
CBS(intf-<iftype>-logical)# end

CBS# configure interface {fastethernet | gigabitethernet | 10gigabitethernet}
<NPM_slot_number>/<port_number>
CBS(conf-intf-<iftype>)# logical <logical_name>
CBS(intf-<iftype>-logical)# circuit <egress_circuit_name>
CBS(intf-<iftype>-logical)# end
```

NOTE: On NPM-8600s, ports 11 and 12 support only 10 Gigabit Ethernet.

4

Installing the Application

This document describes how to install the Proventia Network IPS application.

This chapter contains the following sections:

Copying the Crossbeam Installation (CBI) Package onto the X-Series System

To load the application onto the X-series system, perform the following steps **on each CPM in the X-Series chassis:**

1. Download the CBI file, `issprovg-2.0-1.cbi`, from the IBM ISS download web site, located at http://www.iss.net/download/index.html, onto a remote Linux machine.
2. Copy the CBI file from the Linux machine onto the CPM. For example, you can use SCP to copy the file:

   ```
   [root@xxxxx admin]# scp issprovg-2.0-1.cbi admin@<ip_address_of_CPM>:
   admin@<ip_address_of_CPM>'s password: <admin_password_for_CPM>
   ```

   SCP displays a successful transfer, as follows:

   ```
   issprovg-2.0-1.cbi                              100%  100MB
   7.2MB/s   00:14
   ```

3. Log into your XOS system as root:

   ```
   CBS# unix su
   Password:<root_password>
   [root@xxxxx admin]#
   ```

4. Move the CBI file into the `/crossbeam/apps/archive/` directory. When the file is transfered to the CPM, the file will be located in `/tftpboot/.private/home/admin/`.

   ```
   [root@xxxxx admin]# mv issprovg-2.0-1.cbi /crossbeam/apps/archive/
   ```

5. Exit the unix shell to return to the CLI prompt:

   ```
   [root@xxxxx admin]# exit
   ```

6. Display the loaded applications:

   ```
   CBS# show application
   ```

   ```
   App ID          : issprovg
   Name            : IBM Proventia Network IPS
   Version         : 2.0
   Release         : 1
   CBI Version     : 1.1.0.0
   ```

Installing the CBI Application Bundle

IMPORTANT: The following conditions must be met or the installation will fail:

- The APMs in the application's VAP group must meet the requirements listed in Application Processor Module (APM) Requirements on page 27.
- The primary CPM, the NPM(s), and all APMs in the application's VAP group must be UP.
- The VAP count must be equal to the max load count.
- The management circuit must be configured, and the physical link to the management interface must be UP.

Use the CBI to install the Proventia Network IPS application, as follows:

1. At the XOS CLI prompt, enter the following command to run the Proventia Network IPS application CBI and begin the installation procedure:

   `CBS# application issprovg vap-group <VAP_group_name> install`

   For *<VAP_group_name>*, enter the name of the VAP group that you created for the Proventia Network IPS application.

2. The following text appears:

   ```
   IBM Internet Security Systems, IBM Proventia Network IPS 2.0  release 1
   ```

3. The XOS then checks the integrity of the CBI package and its dependencies, displaying the following text to show the progress of that operation:

   ```
   Checking Bundle Integrity: [####################] 100% [ ok ]
   Checking Dependencies: [####################] 100% [ ok ]
   ```

4. The XOS begins the CBI interview process by displaying the terms and definitions for the Proventia Network IPS application license agreement and prompting you to read the agreement:

   ```
   Press ENTER to read or 'q' to quit:
   ```

5. Press `Enter` to read the license agreement. When finished, type `y` and press `Enter` to accept the license agreement:

   ```
   [License agreement displayed here]
   Accept the license agreement? [n]: y
   ```

6. When prompted, enter the admin password for the Proventia Manager application.

   ```
   Answer the questions below to configure this application.  Type '?' for help.
   Change password for Proventia Manager user 'admin':
   Password:
   Confirm Password:
   ```

   The password must be between 6 and 99 characters long and cannot contain any of the following characters: `#&*()|"<>\;'``

   NOTE: The admin password for the Proventia Manager is NOT the same as the admin password for the XOS CLI or EMS.

7. When prompted, enter the agent name to be used by Proventia Manager and SiteProtector to reference the VAP group. The default agent name is `Proventia_GC1200`.

   ```
   Agent Name? [Proventia_GC1200]:
   ```

   The agent name must begin with a letter or number and can include letters, numbers, and the dash (-) and underscore (_) characters.

   The agent name has a maximum length of 100 characters (including VAP name).

   Proventia Manager and SiteProtector will append each VAP's name to the agent name that you choose.

   For example, if your VAP group name is `iss`, and you have 2 VAPs in the group, XOS will automatically name the VAPs `iss_1` and `iss_2`. If you specify the agent name, `Proventia`, the Proventia Manager and SiteProtector will refer to the VAPs as `Proventia_iss_1` and `Proventia_iss_2`.

8. When prompted, enter the letter that corresponds to the IPS mode in which you want the Proventia Network IPS application to operate. Refer to IPS Modes of Operation on page 17 for descriptions of these modes.

   ```
   Adapter Mode Configuration? [s]:
   ```

   - **`s`** - Intrusion Prevention System (IPS) Inline Simulation Mode (default option)
   - **`p`** - Intrusion Prevention System (IPS) Inline Protection Mode

9. When prompted for the management port interface, enter the device name that you assigned to the management circuit. (See Creating and Configuring a Management Circuit on page 37 for details.)

   ```
   Management Port Interface? [provgmgmt]
   ```

   IMPORTANT: The value that you enter when prompted for the `Management Port Interface` must be the same as the value that you entered for *`<management_circuit_device_name>`* when you configured the management circuit. If these two values do not match, the management circuit will not work.

   If the management circuit is not configured or if the physical link to the management interface is DOWN, the installation will prompt you to enter a different management interface name. You cannot proceed with the installation until you specify the correct device name for the management circuit, the management circuit is configured, and the physical link to the management interface is UP.

10. When prompted, if you want to change any configuration settings before installing the application, type `y` and press `Enter` to return to the first question in the installation interview. If you do not want to change configuration settings, press `Enter` to begin installing the application.

    ```
    Are any changes needed? [n]:
    ```

11. XOS installs the Proventia Network IPS application on the VAP group that you specified in step 1 of this procedure. XOS displays the progress of the application installation on each VAP.

    For example, the following text appears when the application is installed on a VAP group called `iss` that consists of two VAPs:

    ```
    Extracting Bundle: [####################] 100% [ ok ]

    Installing issprovg on VAP iss_2: [####################] 100% [ ok ]

    Installing issprovg on VAP iss_1: [####################] 100% [ ok ]

    A vap-group reload is required for the change(s) to take affect.
    Please run the CLI command "reload vap-group iss".
    ```

12. If desired, save the XOS configuration so that it runs on startup:

    ```
    CBS# copy running-config startup-config
    ```

13. Reboot the VAP group so that the installation can take effect:

    ```
    CBS# reload vap-group <VAP_group_name>
    ```

14. When prompted, press `Enter` to proceed with the reload:

    ```
    Proceed with reload? <Y or N> [Y]:
    ```

After the VAP has rebooted, the installation is complete, and you can begin using Proventia Manager to configure the application and to register with SiteProtector.

IMPORTANT: Once the initial installation is complete, if you change the IP address, FQDN, or device name (interface name) assigned to the management circuit for a VAP, you must reconfigure the management interface for that VAP. To do this, enter the following CLI command, and choose option `3` from the menu:

```
CBS# application issprovg vap-group <VAP_group_name> configure

IBM Proventia Network IPS Configuration Menu
1. Configure Proventia Manager Password
2. Configure Agent Name (requires application restart)
3. Configure Management Interface (requires application restart)
4. Exit

Enter choice: 3
```

Verifying the Installation

Use the following command to verify that the application is running:

```
CBS# show application vap-group <VAP_group_name>
```

where *<VAP_group_name>* is the name of the VAP group on which you have installed the application.

For example, if you install the Proventia Network IPS application on the VAP group, `iss`, which has two VAPs in the group, the following command:

```
CBS# show application vap-group iss
```

should produce the following output:

```
VAP Group      : iss
App ID         : issprovg
Name           : IBM Proventia Network IPS
Version        : 2.0
Release        : 1
Start on Boot  : yes
App Monitor    : on

iss_1          : running
iss_2          : running
```

Troubleshooting the Installation

If the installation fails before it is complete, you can view the log files in the following locations:

- **Syslog files —** On the CPM, in the `/var/log/messages/` directory
- **Log files** — On each VAP, in the `/tmp/issarchive/` directory

You can also view the installation error and warning messages in the `/var/log/messages` directory by issuing the following CLI command:

```
CBS# show logging console component cbi level error
```

If the installation completes, you can view the installation errors by looking at the `/var/iss/setup.log` file stored on each VAP. You can also download a VAP's `setup.log` file from the Proventia Manager web-based interface by accessing the IP address or host name assigned to the VAP's management interface.

5

Uninstalling the Application

This chapter explains how to uninstall the Proventia Network IPS application.

This chapter contains the following sections:

Uninstalling the CBI Application Bundle

IMPORTANT: The following conditions must be met or the uninstallation will fail:

- All VAPs must be unregistered from Site Protector. If any VAPs are registered with SiteProtector, the uninstallation fails. (Refer to Troubleshooting the Uninstallation on page 48 for information on error messages generated when this failure occurs.)
- The primary CPM, the NPM(s), and all APMs in the application's VAP group must be UP.
- The VAP count must be equal to the max load count.

To uninstall the application, perform the following steps:

1. From the CLI, enter the following command:
   `CBS# application issprovg vap-group <VAP_group_name> uninstall`
2. When prompted, press `Enter` to confirm the uninstallation.
   `Are you sure you want to uninstall application? <Y or N> [Y]:`
3. The XOS displays the following text:
   `IBM Internet Security Systems, IBM Proventia Network IPS 2.0  release 1`

   `Checking Dependencies: [####################] 100% [ ok ]`
4. The XOS then stops the application on each VAP in the group and displays the progress of these operations. For example, the following text appears when XOS stops the application on a VAP group called `iss` that contains two VAPs:
   `Stopping issprovg on VAP iss_2: [####################] 100% [ ok ]`

   `Stopping issprovg on VAP iss_1: [####################] 100% [ ok ]`

   NOTE: If the application was already stopped when you began the uninstallation, you may see some error or warning messages at this point; you can safely ignore these messages.
5. The XOS then uninstalls the application from each VAP in the group and displays the progress of these operations. For example, the following text appears when XOS uninstalls the application from a VAP group called `iss`, which contains two VAPs:
   `Uninstalling issprovg on VAP iss_2: [####################] 100% [ ok ]`

   `Uninstalling issprovg on VAP iss_1: [####################] 100% [ ok ]`

6. When the uninstallation is complete, the XOS displays the following text:

   ```
   A vap-group reload is required for the change(s) to take affect.
   Please run the CLI command "reload vap-group iss".*
   ```

7. Reboot the VAP group so that the uninstallation can take effect:

   ```
   CBS# reload vap-group <VAP_group_name>
   ```

8. When prompted, type `y` and press `Enter` to proceed with the reload:

   ```
   Proceed with reload? <Y or N> [Y]:
   ```

Troubleshooting the Uninstallation

If the uninstallation fails before it is complete, you can view the log files in the following locations:

- **Syslog files —** On the CPM, in the `/var/log/messages/` directory
- **Log files** — On each VAP, in the `/tmp/issarchive/` directory

You can also view the uninstallation error and warning messages in the `/var/log/messages` directory by issuing the following CLI command:

```
CBS# show logging console component cbi level error
```

NOTE: If the uninstallation fails because you have not unregistered all VAPs from SiteProtector before uninstalling the application, the above command displays the following error message:

```
This sensor appears to be managed by Site Protector. Uninstalling without
first unregistering from Site Protector can lead to orphaned sensors in
Site Protector. Before proceeding with the uninstall, please restart the
application and then unregister each VAP by accessing the VAP's Proventia
Manager web interface and unchecking the "Register with SiteProtector" box
in the System->Management page. If you wish to force the uninstall without
unregistering, you can remove the file /etc/lmi/spregistered from each VAP
in your VAP-group (this is not recommended).
```

6

Example XOS Configurations for Supported Single-Application Use Cases

This chapter provides topology diagrams that illustrate the single-application use cases supported for Proventia Network IPS applications installed on Crossbeam X-series systems and provides detailed XOS configuration examples for the supported use cases for each topology configuration option.

NOTE: The examples in this chapter are for basic single-bridge, single-application configurations.

For examples of more advanced multi-bridge, single-application configurations, refer to Advanced Configurations: Support for Communication between Internal Subnets on page 77.

For examples of multi-application serialization deployments, refer to the following Crossbeam Systems installation and configuration guides:

- *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 Power NGX R65*
- *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 Power VSX NGX R65*
- *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 NGX Layer-2 Firewall*
- *Deploying Multiple Security Services on the Crossbeam X-Series Platform: Using IBM Proventia Network IPS 2.0 for Crossbeam and Check Point™ VPN-1 Power VSX NGX R65 with Bridged Virtual Systems*

This chapter contains the following sections:

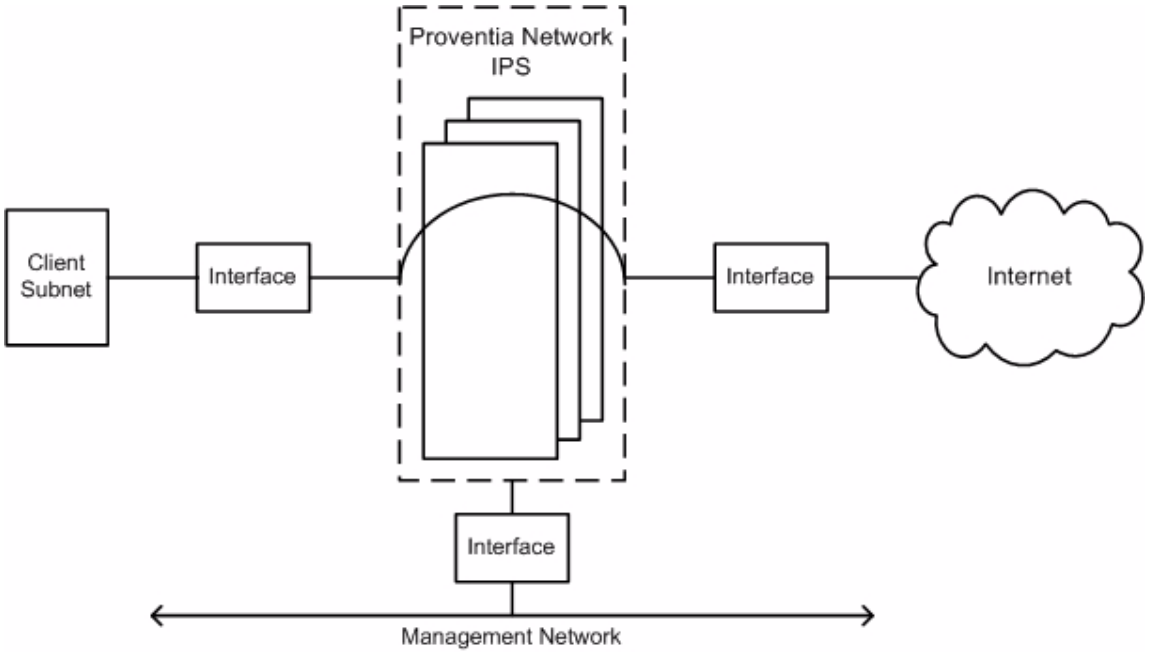
Standalone IPS Examples

In this scenario, Proventia Network IPS is the only application running on the system. The application may be running in Inline Simulation or Inline Protection mode.

Topology Diagram

The following figure illustrates the topology of a standalone IPS.

Figure 10. Standalone IPS (Inline Simulation or Inline Protection Mode)



XOS Configuration Examples

With a Standalone Proventia Network IPS deployment, you can configure a maximum of 128 bridges, and you can use any of the following five interface types.

- Simple Interface
- Simple Interface with redundancy
- Multi-Link Trunk (MLT)
- VLAN Trunk (802.1q) (up to 4094 VLANs)
- VLAN Trunk over MLT

This section contains examples that show how to use the XOS CLI to configure bridge circuits for each of the following three interface types:

- Simple Interface Example on page 51
- Multi-Link Trunk (MLT) Example on page 52
- VLAN Trunk Example on page 53

Simple Interface Example

1. Create the bridge parent circuit:

```
CBS# configure circuit bridge1 device-name bridge1
CBS(conf-cct)# vap-group iss
CBS(conf-cct-vapgroup)# end
```

2. Create the two child circuits that will form the bridge:

```
CBS# configure circuit lan device-name lan
CBS(conf-cct)# vap-group iss
CBS(conf-cct-vapgroup)# promiscuous-mode active
CBS(conf-cct-vapgroup)# end

CBS# configure circuit wan device-name wan
CBS(conf-cct)# vap-group iss
CBS(conf-cct-vapgroup)# promiscuous-mode active
CBS(conf-cct-vapgroup)# end
```

3. Create the bridge by assigning the circuits to the bridge parent.

```
CBS# configure bridge-mode bridge1 transparent
CBS(conf-bridge-mode)# circuit lan
CBS(conf-bridge-mode)# circuit wan
```

4. In this example, the bridge's physical interfaces will be two Gigabit Ethernet ports located on the NPM in slot 2 of the X-series chassis. Assign the bridge's child circuits to the two physical interfaces:

```
CBS# configure interface gigabitethernet 2/1
CBS(conf-intf-gig)# logical lan
CBS(intf-gig-logical)# circuit lan
CBS(intf-gig-logical)# end

CBS# configure interface gigabitethernet 2/2
CBS(conf-intf-gig)# logical wan
CBS(intf-gig-logical)# circuit wan
CBS(intf-gig-logical)# end
```

Multi-Link Trunk (MLT) Example

By default a Multi-Link Trunk allows the system to accept VLAN-tagged packets. This configuration allows all VLAN-tagged and untagged packets to be accepted. Refer to the *XOS 8.1 Configuration Guide* to limit the VLANs that are accepted, and to specify whether untagged packets are accepted.

1. Create the bridge parent circuit:

```
CBS# configure circuit bridge1 device-name bridge1
CBS(conf-cct)# vap-group iss
CBS(conf-cct-vapgroup)# end
```

2. Create the two child circuits that will form the bridge:

```
CBS# configure circuit lan device-name lan
CBS(conf-cct)# vap-group iss
CBS(conf-cct-vapgroup)# promiscuous-mode active
CBS(conf-cct-vapgroup)# end

CBS# configure circuit wan device-name wan
CBS(conf-cct)# vap-group iss
CBS(conf-cct-vapgroup)# promiscuous-mode active
CBS(conf-cct-vapgroup)# end
```

3. Create the bridge by assigning the circuits to the bridge parent.

```
CBS# configure bridge-mode bridge1 transparent
CBS(conf-bridge-mode)# circuit lan
CBS(conf-bridge-mode)# circuit wan
```

4. Assign the bridge's child circuits to the Multi-Link Trunks:

```
CBS# configure group-interface lan_group
CBS(conf-group-intf)# mode multi-link circuit lan
CBS(conf-group-intf)# interface-type gigabitethernet
CBS(conf-grp-intf-gig)# exit
CBS(conf-group-intf)# interface 1/1
CBS(conf-group-intf-intf)# exit
CBS(conf-group-intf)# interface 1/2
CBS(conf-group-intf-intf)# exit
CBS(conf-group-intf)# interface 1/3
CBS(conf-group-intf-intf)# exit
CBS(conf-group-intf)# interface 1/4
CBS(conf-group-intf-intf)# end

CBS# configure group-interface wan_group
CBS(conf-group-intf)# mode multi-link circuit wan
CBS(conf-group-intf)# interface-type gigabitethernet
CBS(conf-grp-intf-gig)# exit
CBS(conf-group-intf)# interface 1/5
CBS(conf-group-intf-intf)# exit
CBS(conf-group-intf)# interface 1/6
CBS(conf-group-intf-intf)# exit
CBS(conf-group-intf)# interface 1/7
CBS(conf-group-intf-intf)# exit
CBS(conf-group-intf)# interface 1/8
CBS(conf-group-intf-intf)# end
```

VLAN Trunk Example

Using `logical-all`, this configuration allows all VLAN-tagged and untagged packets to be accepted. Refer to the *XOS 8.1 Configuration Guide* to limit the VLANs that are accepted, and to specify whether untagged packets are accepted.

1. Create the bridge parent circuit:

```
CBS# configure circuit bridge1 device-name bridge1
CBS(conf-cct-vapgroup)# vap-group iss
CBS(conf-cct-vapgroup)# end
```

2. Create the two child circuits that will form the bridge:

```
CBS# configure circuit lan device-name lan
CBS(conf-cct)# vap-group iss
CBS(conf-cct-vapgroup)# promiscuous-mode active
CBS(conf-cct-vapgroup)# end

CBS# configure circuit wan device-name wan
CBS(conf-cct)# vap-group iss
CBS(conf-cct-vapgroup)# promiscuous-mode active
CBS(conf-cct-vapgroup)# end
```

3. Create the bridge by assigning the circuits to the bridge parent:

```
CBS# configure bridge-mode bridge1 transparent
CBS(conf-bridge-mode)# circuit lan
CBS(conf-bridge-mode)# circuit wan
```

4. Assign the bridge's child circuits to physical interfaces:

```
CBS# configure interface gigabitethernet 2/1
CBS(conf-intf-gig)# logical-all lan
CBS(intf-gig-logical)# circuit lan
CBS(intf-gig-logical)# end

CBS# configure interface gigabitethernet 2/2
CBS(conf-intf-gig)# logical-all wan
CBS(intf-gig-logical)# circuit wan
CBS(intf-gig-logical)# end
```

Standalone IPS with Dual-Box High Availability (DBHA) Example

In this scenario, the Proventia Network IPS application is installed on two systems in a network environment configured for Dual-Box High Availability (DBHA). The Proventia Network IPS application is the only application running on the two systems, and the application may be operating in Inline Simulation or Inline Protection mode.

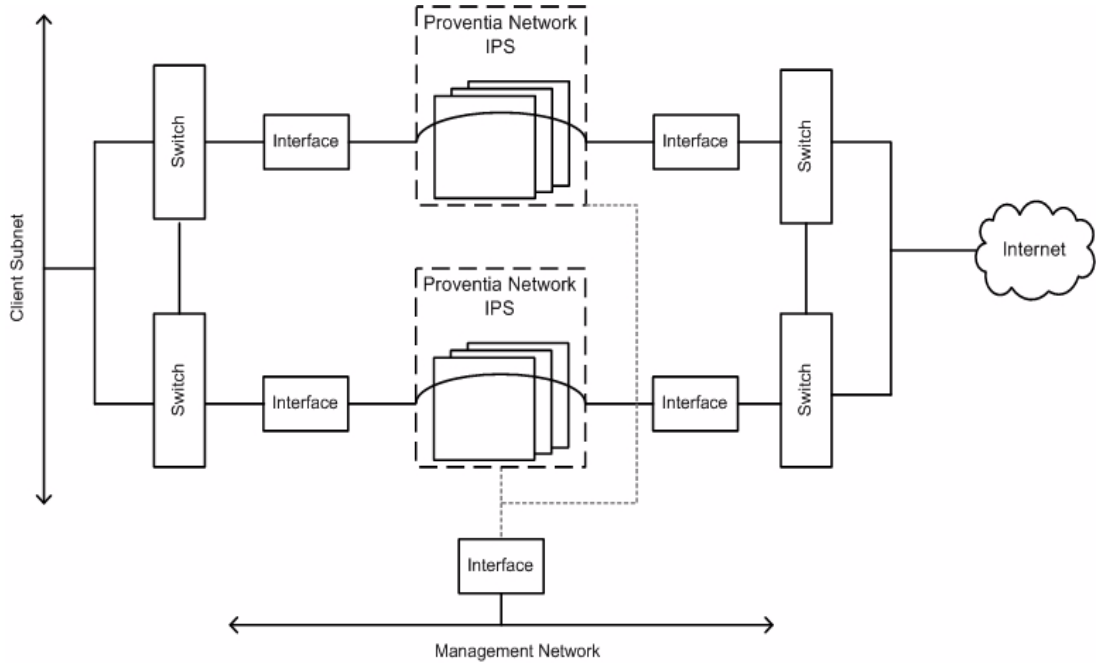
NOTE: A successful DBHA configuration depends upon external devices configured to provide failure detection and traffic failover in the event that one X-Series system fails. These external devices must provide this functionality by using a dynamic routing protocol or by using a redundant path protocol, such as Spanning Tree Protocol (STP).

External systems must be configured to ensure that all packets in a flow are sent to a single X-series system. The Proventia Network IPS application will not inspect asymmetric traffic because the application's stateful inspection requires that every packet in a flow be inspected by a single Proventia Network IPS appliance.

Topology Diagram

The following figure illustrates the topology of a Standalone IPS when it is installed on two X-series systems that are configured for dual-box high availability (DBHA).

Figure 11. Standalone IPS with Dual-Box High Availability



XOS Configuration Example

The Proventia Network IPS application supports up to 4094 VLANs in this configuration, and you can extend the MLT up to 8 ports.

You can use any combination of the following five interface types, which are supported for a Standalone IPS deployment:

- Simple Interface
- Simple Interface with redundancy
- Multi-Link Trunk (MLT)
- VLAN Trunk (802.1q) (up to 4094 VLANs)
- VLAN Trunk over MLT

The following example shows how to configure XOS to enable a dual-box, high-availability (DBHA) deployment of the Proventia Network IPS application. In this example, the X-Series systems are connected to external switches using VLAN Trunk over MLT interfaces. The switches are configured to use Spanning Tree Protocol (STP) to provide loop-prevention functionality for the two X-Series systems.

IMPORTANT: For a DBHA configuration to function, you must create **identical** VAP group and IP flow rule configurations on the two X-Series systems. In addition, you must configure every circuit with **the same** circuit name, circuit ID**,** and device name on both systems.

Perform the following steps **on each X-Series system**.

1. Use the following commands to create a VAP group for the Proventia Network IPS application.

```
CBS# configure vap-group iss xslinux_v3
CBS(config-vap-grp)# vap-count 2
CBS(config-vap-grp)# max-load-count 2
```

2. Configure the AP list and the load balance VAP list for the VAP group:

```
CBS(config-vap-grp)# ap-list ap6 ap7
CBS(config-vap-grp)# load-balance-vap-list 1 2
```

3. Because the VAP group has more than one VAP, you must configure the VAP group with the following command:

```
CBS(config-vap-grp)# master-failover-trigger application
```

4. Configure a basic IP flow rule for the VAP group:

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

5. Configure a DNS server for rhe VAP group:

```
CBS# configure dns server 192.168.35.50 vap-group iss
```

6. Configure the following system-non-ip-flow-rule to direct the NPM to pass STP packets directly to the master VAP in the VAP group:

```
CBS# configure system-non-ip-flow-rule ip_lsap
CBS(conf-system-non-ip-flow-rule)# encapsulation lsap any
CBS(conf-system-non-ip-flow-rule)# action pass-to-masters
CBS(conf-system-non-ip-flow-rule)# activate
CBS(conf-system-non-ip-flow-rule)# end
```

7. Create a management circuit, assign a device name to the circuit, and map the circuit to the application's VAP group:

```
CBS# configure circuit provgmgmt circuit-id 1020 device-name provgmgmt
CBS(conf-cct)# vap-group iss
CBS(conf-cct-vapgroup)# management-circuit
```

8. Configure the management circuit to use a unique IP address to access each VAP in the group:

```
CBS(conf-cct-vapgroup)# ip 172.30.253.11/24 172.30.253.255 increment-per-vap
172.30.253.12
CBS(conf-cct-vapgroup)# end
```

9. Assign the management circuit to a physical interface:

```
CBS# configure interface gigabitethernet 1/1
CBS(conf-intf-gig)# logical provgmgmt
CBS(intf-gig-logical)# circuit provgmgmt
CBS(intf-gig-logical)# end
```

10. Configure a default IP route for the management circuit to use to communicate with the VAP group:

```
CBS# configure ip route 0.0.0.0/0 172.30.253.1 vap-group
iss circuit provgmgmt
```

11. Create the bridge parent circuit:

```
CBS# configure circuit bridge1 circuit-id 1030 device-name bridge1
CBS(conf-cct)# vap-group iss
CBS(conf-cct-vapgroup)# end
```

12. Create the two child circuits that will form the bridge:

```
CBS# configure circuit lan circuit-id 1031 device-name lan
CBS(conf-cct)# vap-group iss
CBS(conf-cct-vapgroup)# promiscuous-mode active
CBS(conf-cct-vapgroup)# end

CBS# configure circuit wan circuit-id 1032 device-name wan
CBS(conf-cct)# vap-group iss
CBS(conf-cct-vapgroup)# promiscuous-mode active
CBS(conf-cct-vapgroup)# end
```

13. Create the bridge by assigning the circuits to the bridge parent.

```
CBS# configure bridge-mode bridge1 transparent
CBS(conf-bridge-mode)# circuit lan
CBS(conf-bridge-mode)# circuit wan
```

14. Assign the bridge's child circuits to the Multi-Link Trunks:

```
CBS# configure group-interface lan_group
CBS(conf-group-intf)# mode multi-link circuit lan
CBS(conf-group-intf)# interface-type gigabitethernet
CBS(conf-grp-intf-gig)# exit
CBS(conf-group-intf)# interface 1/2
CBS(conf-group-intf-intf)# exit
CBS(conf-group-intf)# interface 1/3
CBS(conf-group-intf-intf)# exit
CBS(conf-group-intf)# interface 1/4
CBS(conf-group-intf-intf)# end

CBS# configure group-interface wan_group
CBS(conf-group-intf)# mode multi-link circuit wan
```

```
CBS(conf-group-intf)# interface-type gigabitethernet
CBS(conf-grp-intf-gig)# exit
CBS(conf-group-intf)# interface 1/5
CBS(conf-group-intf-intf)# exit
CBS(conf-group-intf)# interface 1/6
CBS(conf-group-intf-intf)# exit
CBS(conf-group-intf)# interface 1/7
CBS(conf-group-intf-intf)# end
```

7

Application Configuration Requirements

The Proventia Network IPS application has the following Proventia Manager and SiteProtector configuration requirements:

- When applying policies or responses to sensors running on the X-Series platform, it is imperative that the same policy and response be loaded on all members of a VAP group. This will ensure that all load-balanced traffic will be inspected and handled identically across all members.

  For ease of management, it is recommended that all members of a VAP group are configured within the same SiteProtector group. Policies and responses should be applied to the group in order to keep VAP group members identical.

  For information on registering VAPs with SiteProtector, see SiteProtector on page 65. For information on using SiteProtector to manage the Proventia Network IPS application, see the *Proventia Network IPS for Crossbeam X-Series Hardware User Guide*, which is available for download from the IBM ISS documentation Web site located at http://www.iss.net/support/documentation.

- Before registering VAPs with SiteProtector, you must make sure SiteProtector is running with the latest database component updates. If the SiteProtector database component is out-of-date, SiteProtector registration may fail for one or more VAPs.

  For instructions on updating the SiteProtector database component, see the *IBM Proventia Management SiteProtector Configuration Guide*, which is available for download from the IBM ISS documentation Web site located at http://www.iss.net/support/documentation.

8

Managing and Monitoring the Application

This chapter describes the methods that you can use to manage and monitor the Proventia Network IPS application when it is installed on a Crossbeam X-series system. This chapter also describes the procedures that you can use to backup and restore the VAP group on which the Proventia Network IPS application is installed on a Crossbeam X-series system.

This chapter contains the following sections:

Managing the Application

The following sections describe the tools that you can use to manage the Proventia Network IPS application:

XOS Command-Line Interface (CLI)

IMPORTANT: With the exception of the `show application` command, the commands described in this section will work only if the following conditions are true:

- The primary CPM, the NPM(s), and all APMs in the application's VAP group are UP.
- The VAP count is equal to the max load count.
- The management circuit is configured, and the physical link to the management interface is UP.

You can use the following XOS CLI commands to perform basic application management. For more information on using the XOS CLI to manage applications, see the *XOS Command Reference Guide* and the *XOS Configuration Guide*.

- Start an application:

  `CBS# application issprovg vap-group <VAP_group_name> start`

  The following example shows the output when the above command is used to start the Proventia Network IPS application on a VAP group called `iss`, which has two VAPs in the group:

  ```
  IBM Internet Security Systems, IBM Proventia Network IPS 2.0  release 1

  Starting issprovg on VAP iss_2: [####################] 100% [ ok ]

  Starting issprovg on VAP iss_1: [####################] 100% [ ok ]
  ```

- Configure an application:

  `CBS# application issprovg vap-group <VAP_group_name> configure`

  This command provides you with access to the following menu, which lets you change your application installation configuration settings:

  ```
  IBM Proventia Network IPS Configuration Menu
  1. Configure Proventia Manager Password
  2. Configure Agent Name (requires application restart)
  3. Configure Management Interface (requires application restart)
  4. Exit

  Enter choice:
  ```

  NOTE: You must stop the application before reconfiguring either the agent name or the management interface.

  For more information on using the above configuration menu, refer to the *Proventia Network IPS for Crossbeam X-Series Hardware User Guide*, which is available for download from the IBM Internet Security Systems (ISS) documentation Web site located at http://www.iss.net/support/documentation.

- Stop an application:

  ```
  CBS# application issprovg vap-group <VAP_group_name> stop
  ```

  The following example shows the output when the above command is used to stop the Proventia Network IPS application on a VAP group called `iss`, which has two VAPs in the group:

  ```
  IBM Internet Security Systems, IBM Proventia Network IPS 2.0  release 1

  Stopping issprovg on VAP iss_2: [####################] 100% [ ok ]

  Stopping issprovg on VAP iss_1: [####################] 100% [ ok ]
  ```

- Restart an application:

  ```
  CBS# application issprovg vap-group <VAP_group_name> restart
  ```

  The following example shows the output when the above command is used to restart the Proventia Network IPS application on a VAP group called `iss`, which has two VAPs in the group:

  ```
  IBM Internet Security Systems, IBM Proventia Network IPS 2.0  release 1

  Stopping issprovg on VAP iss_2: [####################] 100% [ ok ]

  Stopping issprovg on VAP iss_1: [####################] 100% [ ok ]


  IBM Internet Security Systems, IBM Proventia Network IPS 2.0  release 1

  Starting issprovg on VAP iss_2: [####################] 100% [ ok ]

  Starting issprovg on VAP iss_1: [####################] 100% [ ok ]
  ```

- Update the VAP group to install the application on any new VAPs that you add to the VAP group after the initial application configuration:

  ```
  CBS# application-update vap-group <VAP_group_name>
  ```

  IMPORTANT: Once you install the Proventia Network IPS application on an X-series system, if you increase the number of VAPs in the application's VAP group, you must run the `application-update` command to install the application on the new VAPs.

- Display all applications installed on all VAP groups or a specified VAP group:

  ```
  CBS# show application [vap-group <VAP_group_name>]
  ```

  The following example shows the state of the application on a VAP group named `iss`, which has two VAPs in the group:

  ```
  VAP Group      : iss
  App ID         : issprovg
  Name           : IBM Proventia Network IPS
  Version        : 2.0
  Release        : 1
  Start on Boot  : yes
  App Monitor    : on

  iss_1          : running
  iss_2          : running
  ```

Proventia Manager

Proventia Manager is a web-based management interface used to manage the Proventia Network IPS application installed on a specific VAP.

If you plan to use SiteProtector to manage the application, you must use the Proventia Manager to register each VAP with SiteProtector.

You can also use the Proventia Manager to perform the following tasks for each specific VAP in the application's VAP group:

- Monitor the status of the application.
- Configure and manage application settings.
- View the quarantine table and apply changes to it.
- Review and manage application activities.

IMPORTANT: If you use the Proventia Manager to make configuration changes to one VAP, you must then make the same changes to each of the other VAPs in the VAP group. Therefore, if your VAP group contains more than one VAP, Crossbeam and IBM recommend using the SiteProtector central management system to make global configuration changes to the VAP group.

To log on to the Proventia Manager:

1. Start a web browser.
2. In the address field, enter the URL for the VAP that you wish to configure, using one of the following formats:

   ♦ **`https://`***`<xxx.xxx.xxx.xxx>`*

   where *`<xxx.xxx.xxx.xxx>`* is the IP address assigned to the management interface for the VAP on which you want to manage the application.

   Refer to Creating and Configuring a Management Circuit on page 37 for instructions on configuring the management IP address for each VAP in the Proventia application's VAP group.

   ♦ **`https://`***`<FQDN>`*

   where *`<FQDN>`* is the fully-qualified domain name (FQDN) that you configured for the VAP.

   Refer to Creating and Configuring a VAP Group for the Proventia Application on page 35 for instructions on configuring an FQDN for each VAP in the Proventia application's VAP group.

3. Login to Proventia Manager using the user name `admin` and the Proventia Manager password that you specified during the application installation.

   NOTE: Some Web browsers may prompt you to provide login and password information twice.

4. If a message informs you that you do not have Java Runtime Environment (JRE) installed, install version 1.5 of the JRE.

   NOTE: If you install JRE version 1.6, Proventia Manager may not work. To resolve this issue, prevent Java from caching Web data by disabling the **Keep Temporary Files on My Computer** setting in the Java control panel.

5. Click **Yes** to use the Getting Started procedures.

   NOTE: ISS recommends that you use these procedures to configure the application for the first time. You can also access the Getting Started procedures from the Proventia Manager Help.

6. Click **Launch Proventia Manager**.

   For more information on using Proventia Manager, see the *Proventia Network IPS for Crossbeam X-Series Hardware User Guide*, which is available for download from the IBM Internet Security Systems (ISS) documentation Web site located at http://www.iss.net/support/documentation.

SiteProtector

SiteProtector is the IBM ISS management console. With SiteProtector, you can manage components and appliances (VAPs), monitor events, and schedule reports.

By default, the Proventia Network IPS application is set up for you to manage it through Proventia Manager. However, if you are managing a VAP group that contains more than one VAP, Crossbeam and IBM recommend that you register each VAP with SiteProtector, place all VAPs in the same SiteProtector group, and then use SiteProtector to apply the same policies to all members of the VAP group.

NOTE: You must use the Proventia Manager to manage the following local functions on each VAP, even if the VAP group is registered with SiteProtector:

- Enabling and disabling SiteProtector management
- Viewing quarantined intrusions
- Deleting quarantine rules
- Performing firmware updates

IMPORTANT: Before registering VAPs with SiteProtector, make sure SiteProtector is running with the latest database component updates. If the database component is out-of-date, SiteProtector registration may fail.

For instructions on updating the SiteProtector database component, see the *IBM Proventia Management SiteProtector Configuration Guide*, which is available for download from the IBM ISS documentation Web site located at http://www.iss.net/support/documentation.

To use SiteProtector to manage the Proventia Network IPS application, perform the following steps **on each VAP in the VAP group:**

1. Use Proventia Manager to login to the VAP as `admin`.

   NOTE: Depending on which Web browser you are using, you may be prompted to provide login and password information twice.

2. From the Proventia Manager main menu, select **System > Management**.
3. Select the check box to register the VAP with SiteProtector.
4. If desired, select the **Local Settings Override SiteProtector Group Settings** option to have the VAP maintain any local settings that you have configured at the first heartbeat.

   If you do not select this option, the VAP inherits the settings of the SiteProtector group that you specify at the first heartbeat.

   NOTE: At the second heartbeat and each heartbeat thereafter, any policy settings you have changed at the SiteProtector group level are sent to the VAP.

5. Type the name of the SiteProtector group to which you wish to assign the VAP. If you do not specify a group, SiteProtector adds the VAP to the default “A or G Series” group.

   IMPORTANT: All VAPs must have the same policy settings at all times. Therefore, you should assign all the VAPs in the VAP group to the same SiteProtector group.

6. In the Heartbeat Interval field, enter the number of seconds that the VAP should wait between sending heartbeats to SiteProtector.

   NOTE: This value must be between 300 and 86,400 seconds. The default value is 3600 seconds.

7. Click **Save Changes**.
8. Add the Agent Manager(s) with which you want the VAP to communicate. (See the *Proventia Network IPS for Crossbeam X-Series Hardware User Guide* for instructions on configuring Agent Managers.)

9. When you finish registering each VAP with SiteProtector, open the SiteProtector console to start managing the VAP group.

   NOTE: When you register a VAP with SiteProtector, you may see several of the following messages in the `/var/log/messages` file:

   ```
   isshyd862_1 iss-spa[6208]: Error: mslLoader::LoadServiceLibrary():
   About to load library:  '/opt/ISS/lib/libissSessionConfigSvcs5.so'
   ```

   You can safely ignore these messages; they are purely informational and do not indicate any hardware or software malfunctions.

After you register the VAP group with SiteProtector, you *must* use SiteProtector to manage the following functions:

- Firewall settings
- Intrusion prevention settings
- Alert events

You can still manage update and installation settings in Proventia Manager or in SiteProtector.

NOTE: When you register a VAP with SiteProtector, some areas of Proventia Manager become read-only. When you unregister a VAP from SiteProtector, Proventia Manager again becomes fully functional on that VAP.

For more information on using SiteProtector, refer to the *Proventia Network IPS for Crossbeam X-Series Hardware User Guide*, which is available for download from the IBM Internet Security Systems (ISS) documentation Web site located at http://www.iss.net/support/documentation.

Monitoring the Application

The following sections describe the tools that you can use to monitor the Proventia Network IPS application once it is installed on an X-series system:

- XOS Application Monitoring on page 67
- SNMP Health Monitoring and SNMP Traps on page 67

XOS Application Monitoring

On an XOS system, the XOS health monitoring system polls application processes on each VAP in the VAP group every five seconds to verify that they are running.

You can use the following command to check the status of the application processes:

```
CBS# show application [vap-group <VAP_group_name>]
```

The following example shows the state of the application on a VAP group named `iss`, which has two VAPs in the group:

```
VAP Group       : iss
App ID          : issprovg
Name            : IBM Proventia Network IPS
Version         : 2.0
Release         : 1
Start on Boot   : yes
App Monitor     : on

iss_1           : stop
iss_2           : running
```

If the application is not running on a VAP, the health system notifies the NPM to stop new flows to the VAP. The NPM performs this process dynamically without modifying the VAP group's load balance list.

You can use the CLI `show flow distribution` command to verify that no new flows are directed to VAPs that are in a down state.

NOTE: Application monitoring cannot detect process hangs. If a process is not functioning, but the application is still running, the XOS health system will continue to report the application as running.

SNMP Health Monitoring and SNMP Traps

You can use the SNMP server embedded on the CPM to configure X-series chassis-specific SNMP health monitoring and SNMP traps.

You can also use the Proventia Network IPS application's SNMP servers, which are installed on each individual VAP, to configure application-specific SNMP health monitoring and SNMP traps for each VAP on which the application is installed.

The following sections explain how to configure SNMP health monitoring and SNMP traps for both the X-series chassis and the Proventia Network IPS application:

- Configuring SNMP Health Monitoring and SNMP Traps for the Crossbeam X-Series Chassis on page 68
- Configuring SNMP Health Monitoring and SNMP Traps for the Proventia Network IPS Application on page 68

Configuring SNMP Health Monitoring and SNMP Traps for the Crossbeam X-Series Chassis

You can use the SNMP server embedded on the CPM to configure chassis-specific SNMP health monitoring and SNMP traps.

To configure a trap destination, use the following command:

```
CBS# configure snmp-server host <host_ip_address> [traps|informs] [version 1|2c]
<community-string> [udp-port <port-number>]
```

To delete a host, use the following command:

```
CBS# configure no snmp-server host <host_ip_addr> <community-string>
```

To view the SNMP trap log, use the following command:

```
CBS# show traplog
```

For more information on using the CLI to configure SNMP health monitoring and SNMP traps for the X-series chassis and modules, refer to the *XOS Configuration Guide* and the *XOS Command Reference Guide*.

Configuring SNMP Health Monitoring and SNMP Traps for the Proventia Network IPS Application

The IBM ISS application SNMP responses use the `iss.mib` file; you can download this file from the IBM ISS download center located at http://www.iss.net/download. The Proventia application's SNMP health monitoring feature uses the following MIB files from the `net-snmp package`[8]:

- `/usr/share/snmp/mibs/UCD-SNMP-MIB.txt`
- `/usr/share/snmp/mibs/DISMAN_EVENT-MIB.txt`
- `/usr/share/snmp/mibs/IF-MIB.txt`
- `/usr/share/snmp/mibs/NET-SNMP-MIB.txt`
- `/usr/share/snmp/mibs/NET-SNMP-MIB-AGENT.txt`
- `/usr/share/snmp/mibs/HOST-RESOURCES-MIB.txt`

You can configure Proventia application-specific SNMP health monitoring and SNMP traps for each individual VAP. To configure application health monitoring and health alerts for a particular VAP, login to that VAP and issue the `provgSnmp` command. Then use the SNMP configuration menus to configure SNMP traps and SNMP polling for the VAP.

You can also configure SNMP health monitoring and SNMP traps using SiteProtector and Proventia Manager.

For more information on configuring Proventia application-specific SNMP health monitoring and SNMP traps, refer to the *Proventia Network IPS for Crossbeam X-Series Hardware User Guide*, which is available for download from the IBM Internet Security Systems (ISS) documentation Web site located at http://www.iss.net/support/documentation.

Logging Events

You can view events in two ways:

- Viewing Event Logs on page 69
- Obtaining Packet Captures from a Proventia Network IPS VAP on page 69

Viewing Event Logs

By default, event logs for each VAP are stored on the local hard drive(s) installed on each module. The event log files can be found in the directory, `/mnt/aplocaldisk`.

You can use either Proventia Manager or SiteProtector to configure event logging for each VAP.

For more information on configuring event logging, refer to the *Proventia Network IPS for Crossbeam X-Series Hardware User Guide*, which is available for download from the IBM Internet Security Systems (ISS) documentation Web site located at http://www.iss.net/support/documentation.

Obtaining Packet Captures from a Proventia Network IPS VAP

To obtain packet captures from a VAP on which the Proventia Network IPS application is installed, perform the following steps:

1. Use `rsh` to login to the VAP.
2. To obtain a packet capture for all circuits monitored by the Proventia Network IPS application, run the following command:

   `/etc/iss/usr/sbin/tcpdump -i provg_1`

   NOTE: There is no way to filter the packet capture information by VND or by bridge.
3. To obtain a packet capture for the management circuit, run the following command:

   `tcpdump -i` *`<management_circuit_device_name>`*

Performing VAP Group Backups and Restores

You can use the XOS CLI to create backup archives of the VAPs on which the Proventia Network IPS application is installed. In case of an application failure, you can use the backup archives that you create to restore the VAP group to a previous state in which the application is known to be fully functional.

NOTE: IBM recommends that you create a backup archive of the Proventia application's VAP group before installing any firmware updates.

The following sections describe the backup and restore functionality provided for the Proventia Network IPS application:

Restrictions

The VAP group backup and restore functionality has the following restrictions:

- This functionality is available only from the XOS CLI. You cannot use the EMS to perform application backups and restores.
- You cannot back up and restore a VAP group to or from a remote location.
- You cannot back up and restore the APM's local hard drive.
- You cannot back up and restore any VAP group on which the Proventia Network IPS application is not installed.
- You can store only one archive for each VAP group. If you back up a VAP group more than once, each successive archive overwrites the previous one.

Backing Up a VAP Group

You create a backup archive of a VAP group on which the Proventia Network IPS application is installed, as follows:

1. Enter the following CLI command:]

   ```
   CBS# archive-vap-group backup vap-group <VAP_group_name>
   ```

2. The XOS checks to be sure that you have enough disk space to perform the operation, and displays the following text as it performs this test:

   ```
   Calculating available and required space.......................... Done
   ```

3. A VAP group must be shut down during a backup operation. Therefore, the CLI prompts you to confirm the backup operation. Press `Enter` to confirm the backup operation, or type `N` and press `Enter` to abort the operation.

   ```
   During backup the vap-group will be disabled. Continue? <Y or N> [Y]:
   ```

4. If you have previously backed up this VAP group, the CLI prompts you to confirm that you want to overwrite the previous backup archive with the new one that you are creating. Press `Enter` to confirm the backup operation, or type `n` and press `Enter` to abort the operation.

   NOTE: The CLI can store only one backup archive of each VAP. Each time you back up a VAP group, the XOS overwrites the last VAP backup archive with the new one.

   ```
   An archive with the same name already exists. Do you want to overwrite it? (y)
   ```

5. The XOS executes the backup operation and displays the progress of the operation. For example, the following text appears as the XOS is backing up a VAP group named `iss` that contains two VAPs:

   NOTE: A backup operation may take a significant amount of time to complete. Please be patient.

   ```
   Waiting for vap group to go down ... Done
   Backing up iss_1..................................................... Done
   Backing up iss_2..................................................... Done
   Backing up iss_common................................................ Done
   CBS#
   ```

6. When the backup is complete, the VAP group archive will be stored in the following directory on the CPM:

   `/tftpboot/archives/<VAP_group_name>`

   This directory will contain the following:

   - A gzipped tar file containing each VAP's filesystem and the VAP group's common filesystem
   - A file containing information about the backup (`archive_info.txt`)

     IMPORTANT: Do NOT modify the `archive_info.txt` file. If you modify this file, you will be unable to restore the archive.

   NOTE: Crossbeam recommends that you copy the VAP group archive files onto another system.

Restoring a VAP Group

To restore a VAP group using a stored backup archive, perform the following steps:

1. Copy the VAP group archive files onto the CPM in the `/tftpboot/archives/<VAP_group_name>` directory.

1. Enter the following CLI command:

   `CBS# **archive-vap-group restore vap-group** <VAP_group_name>`

   IMPORTANT: Before entering this command, make sure the archive stored on the CPM was created from a VAP group with the same VAP group name, VAP count, XOS version, application name, application version, and application release as the VAP group you want to restore. The restore operation will fail if any of these parameters are not the same for the backup archive and the VAP group to be restored.

2. All of the VAPs in a VAP group must be shut down during a restore operation. Therefore, the CLI prompts you to confirm the restore operation. Press `Enter` to confirm the restore operation, or type `N` and press `Enter` to abort the operation.

   ```
   During restore the vap-group will be disabled. Continue? <Y or N> [Y]:
   ```

3. The XOS executes the restore operation and displays the progress of the operation. For example, the following text appears as the XOS is restoring a VAP group named `iss` that contains two VAPs:

   NOTE: A restore operation may take a significant amount of time to complete. Please be patient.

```
Waiting for vap group to go down ... Done
Restoring vap-group iss. This may take several minutes...
Removing old temporary files ... Done
Extracting iss_1 archive..................................... Done
Extracting iss_2 archive..................................... Done
Extracting iss_common archive................................ Done
Restoring VapGroup iss
iss_common restoration has completed
iss_1 restoration has completed
iss_2 restoration has completed
VAP Group iss restoration completed
Cleaning up temporary files.................................. Done
CBS#
```

4. After the VAP group has rebooted, use the following command to verify that the application has restarted (provided that the application is configured to start on boot):

   `CBS# **show application vap-group** *<VAP_group_name>*`

   The following example shows the status of an application that has successfully restarted on a VAP group named `iss`, which has two VAPs in the group:

```
VAP Group      : iss
App ID         : issprovg
Name           : IBM Proventia Network IPS
Version        : 2.0
Release        : 1
Start on Boot  : yes
App Monitor    : on

iss_1          : running
iss_2          : running
```

Deleting a VAP Group Archive

To delete a local VAP group archive, perform the following steps:

1. Enter the following CLI command:

   `CBS# **archive-vap-group delete vap-group** *<VAP_group_name>*`

2. The XOS deletes the VAP group's archive directory and all of the files in it, and displays the progress of the operation. For example, the following text appears as the XOS is deleting the archive for a VAP group called `iss`:

```
Deleting archive for VAP Group iss ... Done
CBS#
```

Displaying VAP Group Archive Information

You can use either of the following CLI commands to display information about the VAP group archives stored on the CPM:

- `CBS# **show archive-vap-group**`
- `CBS# **archive-vap-group show**`

These commands display information about all VAP group archives stored on the CPM. For example, the following data is displayed for two VAP groups named `iss1` and `iss2`, which are archived on a CPM:

```
vap-group : iss1
vap count : 3
vap OS version : xslinux_v3
XOS version : 8.1.0-75
application : issprovg
application Version : 2.0
application Release : 1
Date : Thu_Feb_21_10-10-10_EST_2008
Sys Time : 1203606610

Backup files are located in /tftpboot/archive/iss1/

vap-group : iss2
vap count : 2
vap OS version : xslinux_v3
XOS version : 8.1.0-75
application : issprovg
application Version : 2.0
application Release : 1
Date : Thu_Feb_21_10-10-10_EST_2008
Sys Time : 1225746283

Backup files are located in /tftpboot/archive/iss2/
```

You can also use the following command to display the above information for a specific VAP group's archive:

`CBS# **archive-vap-group show vap-group** *<VAP_group_name>*`

For example, the following data is displayed for the VAP group named `iss`, which is archived on a CPM:

```
vap-group : iss
vap count : 4
vap OS version : xslinux_v3
XOS version : 8.1.0-75
application : issprovg
application Version : 2.0
application Release : 1
Date : Thu_Feb_21_10-10-10_EST_2008
Sys Time : 1254356283

Backup files are located in /tftpboot/archive/iss/
```

Adding and Removing Proventia Application VAP Group Members

This section describes how to perform the following tasks:

Adding a VAP to a Proventia Application VAP Group

Perform the following steps to add a VAP to the Proventia Network IPS application's VAP group:

1. Acquire and install an APM.

   IMPORTANT: Make sure the new APM meets the requirements listed in Application Processor Module (APM) Requirements on page 27. The new APM's hardware configuration must match the hardware configuration of all other APMs in the VAP group.

2. Increment the management IP address range for the VAP group:

   ```
   CBS# configure circuit <management_circuit_name> vap-group <VAP_group_name>
   CBS(conf-cct-vapgroup)# ip <ip_address_of_first_VAP_in_group>/<netmask>
   <broadcast_address> increment-per-vap <ip_address_of_last_vap_in_group>
   CBS(conf-cct-vapgroup)# end
   ```

3. Increment the Proventia application VAP group's VAP count:

   ```
   CBS# configure vap-group <VAP_group_name>
   CBS(config-vap-grp)# vap-count <new_VAP_count>
   ```

4. Reconfigure the AP list for the VAP group to add the new APM to the group:

   ```
   CBS(config-vap-grp)# ap-list <ap_name1> [<ap_name2>] [<ap_name3>] ...
   ```

   where *<ap_name#>* is the name that the XOS has assigned to the APM. (Use the `show chassis` command to determine the assigned names of the APMs in your chassis.)

5. Configure the load-balance VAP list for the VAP group so that the new VAP does not receive any flows. The new APM will have the highest index number in the VAP group; leave this index number off the load-balance VAP list.

   ```
   CBS(config-vap-grp)# load-balance-vap-list <index1> <index2> [<indexn>] ...
   ```

6. Increment the Proventia application VAP group's max load count:

   ```
   CBS(config-vap-grp)# max-load-count <new_max_load_count>
   CBS# end
   ```

7. Use the following commands to verify that the new APM has the correct firmware installed on it. If the `revs_check` script prompts you to do so, follow the instructions in the *XOS Configuration Guide* to update the firmware on the new APM.

   ```
   CBS# unix su
   [root@xxxxx admin]# /crossbeam/bin/revs_check -u
   ```

8. Install the Proventia Network IPS on the new VAP by entering the following CLI command.

   IMPORTANT: Before running this command, make sure all APMs in the VAP group, including the APM for the new VAP, are UP. If any APMs in the group are not up, the installation will fail.

   ```
   CBS# application-update vap-group <VAP_group_name>
   ```

9. When the application update is complete, reload the new module:

```
CBS# reload module <module_name>
```

10. After the reload is complete, use the `show application vap-group <VAP_group_name>` command to verify that the application is running on the new VAP.

    For example, if a new VAP is added to a VAP group named `iss`, resulting in a VAP group with two VAPs, the `show application` command should have the following output:

```
CBS# show application vap-group iss
VAP Group       : iss
App ID          : issprovg
Name            : IBM Proventia Network IPS
Version         : 2.0
Release         : 1
Start on Boot   : yes
App Monitor     : on

iss_1           : running
iss_2           : running
```

11. Use Proventia Manager to configure the application on the new VAP, or register the new VAP with SiteProtector and add the new VAP to the VAP group's Site Protector group.

    IMPORTANT: If you have changed the IP address, FQDN, or device name (interface name) assigned to the management circuit for any VAP, you may be unable to access that VAP through Proventia Manager. If this happens, enter the following CLI command, and choose option `3` to reconfigure the management interface.

```
CBS# application issprovg vap-group <VAP_group_name> configure

IBM Proventia Network IPS Configuration Menu
1. Configure Proventia Manager Password
2. Configure Agent Name (requires application restart)
3. Configure Management Interface (requires application restart)
4. Exit

Enter choice: 3
```

12. Add the APM to the load-balance VAP list so that it can receive new flows:

```
CBS# configure vap-group <VAP_group_name>
CBS(config-vap-grp)# load-balance-vap-list <index1> <index2> [<indexn>] ...
```

Removing a VAP from a Proventia Application VAP Group

Perform the following steps to remove a VAP from a Proventia application VAP group.

1. Use Proventia Manager to log in to the VAP that you want to remove from the group, and unregister the VAP from SiteProtector.

2. Use the following commands to remove the VAP from the load-balance VAP list, so that it no longer receives new flows.

    NOTE: You can only remove the VAP with the highest index number. Exclude this VAP from the list.

```
CBS# configure vap-group <VAP_group_name>
CBS(config-vap-grp)# load-balance-vap-list <index1> <index2> [<indexn>] ...
```

3. Decrement the Proventia application VAP group's max load count:

```
CBS(config-vap-grp)# max-load-count <new_max_load_count>
```

4. Reconfigure the AP list for the VAP group to remove the APM from the group:

   ```
   CBS(config-vap-grp)# ap-list <ap_name1> [<ap_name2>] [<ap_name3>] ...
   ```

   where *<ap_name#>* is the name that the XOS has assigned to the APM. (Use the `show chassis` command to determine the assigned names of the APMs in your chassis.)

5. Decrement the Proventia application VAP group's VAP count:

   ```
   CBS(config-vap-grp)# vap-count <new_VAP_count>
   CBS(config-vap-grp)# end
   ```

6. Reconfigure the management IP address range to reclaim the IP address for the VAP that you have just removed from the VAP group:

   ```
   CBS# configure circuit <management_circuit_name> vap-group <VAP_group_name>
   CBS(conf-cct-vapgroup)# ip <ip_address_of_first_VAP_in_group>/<netmask>
   <broadcast_address> increment-per-vap <ip_address_of_last_vap_in_group>
   CBS(conf-cct-vapgroup)# end
   ```

   IMPORTANT: If you have changed the IP address, FQDN, or device name (interface name) assigned to the management circuit for any VAP, you may be unable to access that VAP through Proventia Manager. If this happens, enter the following CLI command, and choose option `3` to reconfigure the management interface.

   ```
   CBS# application issprovg vap-group <VAP_group_name> configure

   IBM Proventia Network IPS Configuration Menu
   1. Configure Proventia Manager Password
   2. Configure Agent Name (requires application restart)
   3. Configure Management Interface (requires application restart)
   4. Exit

   Enter choice: 3
   ```

Appendix A

Advanced Configurations: Support for Communication between Internal Subnets

This appendix describes two types of bridge configurations that you can use to enable communication between two or more internal subnets and provides an example XOS running configuration file for each type of bridge configuration.

This appendix contains the following sections:

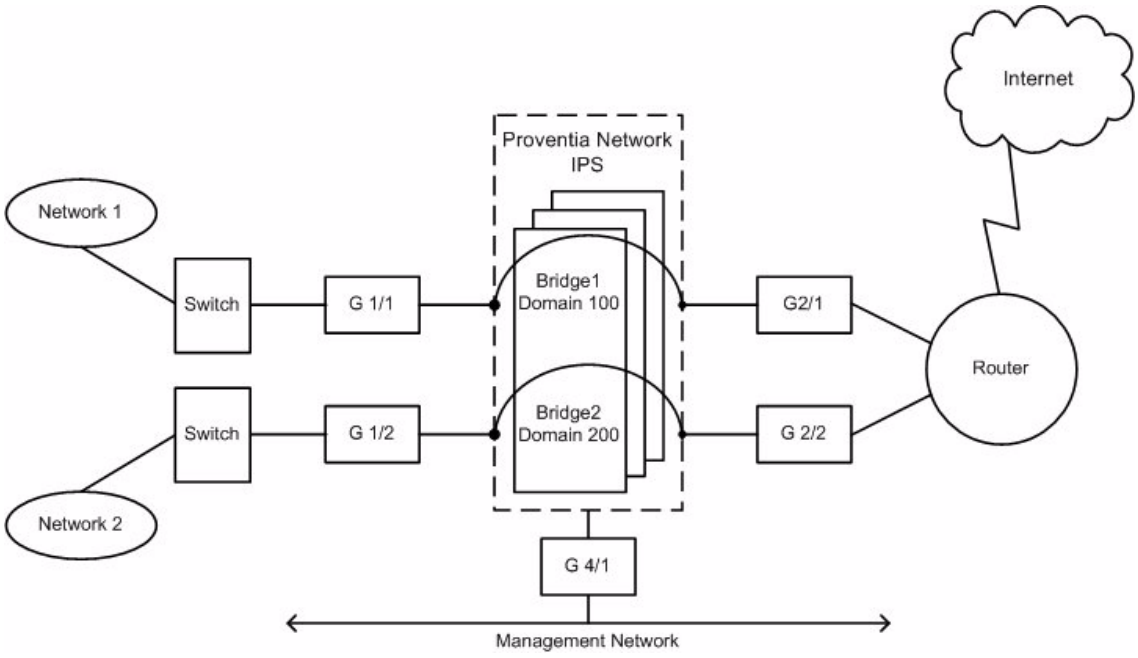
Configuring Bridges for Separate Physical Networks

To enable communication between two or more physical networks, configure the X-Series system to create a separate bridge for each network, assign a unique domain ID to each bridge, and assign a different pair of physical interfaces to each bridge.

Figure 12 on page 77 shows an example network topology that illustrates this type of bridge configuration.

See Example XOS Running Configuration: Configuring Bridges for Separate Physical Networks on page 78 for an example XOS configuration that implements this network topology.

Figure 12. Configuring Bridges for Separate Physical Networks



Example XOS Running Configuration: Configuring Bridges for Separate Physical Networks

```
vap-group ips xslinux_v3
  vap-count 2
  max-load-count 2
  ap-list ap1 ap2 ap3 ap4 ap5 ap6 ap7 ap8 ap9 ap10
  load-balance-vap-list 1 2 3 4 5 6 7 8 9 10
  ip-flow-rule ips_lb
    action load-balance
    activate
circuit lan1 circuit-id 1025 domain 100
  device-name lan1
  vap-group ips
    promiscuous-mode active
circuit wan1 circuit-id 1026 domain 100
  device-name wan1
  vap-group ips
    promiscuous-mode active
circuit bridge1 circuit-id 1027 domain 100
  device-name bridge1
  vap-group ips
circuit lan2 circuit-id 1028 domain 200
  device-name lan2
  vap-group ips
    promiscuous-mode active
circuit wan2 circuit-id 1029 domain 200
  device-name wan2
  vap-group ips
    promiscuous-mode active
circuit bridge2 circuit-id 1030 domain 200
  device-name bridge2
  vap-group ips
circuit mgmt circuit-id 1031
  device-name mgmt
  vap-group ips
    management-circuit
    ip 192.168.0.10/24 192.168.0.255 increment-per-vap 192.168.0.11
bridge-mode bridge1 transparent
  circuit lan1
  circuit wan1
bridge-mode bridge2 transparent
  circuit lan2
  circuit wan2
interface gigabitethernet 1/1
  logical lan1
    circuit lan1
interface gigabitethernet 1/2
  logical lan2
    circuit lan2
interface gigabitethernet 2/1
  logical wan1
    circuit wan1
interface gigabitethernet 2/2
  logical wan2
    circuit wan2
interface gigabitethernet 4/1
  logical mgmt
    circuit mgmt
```

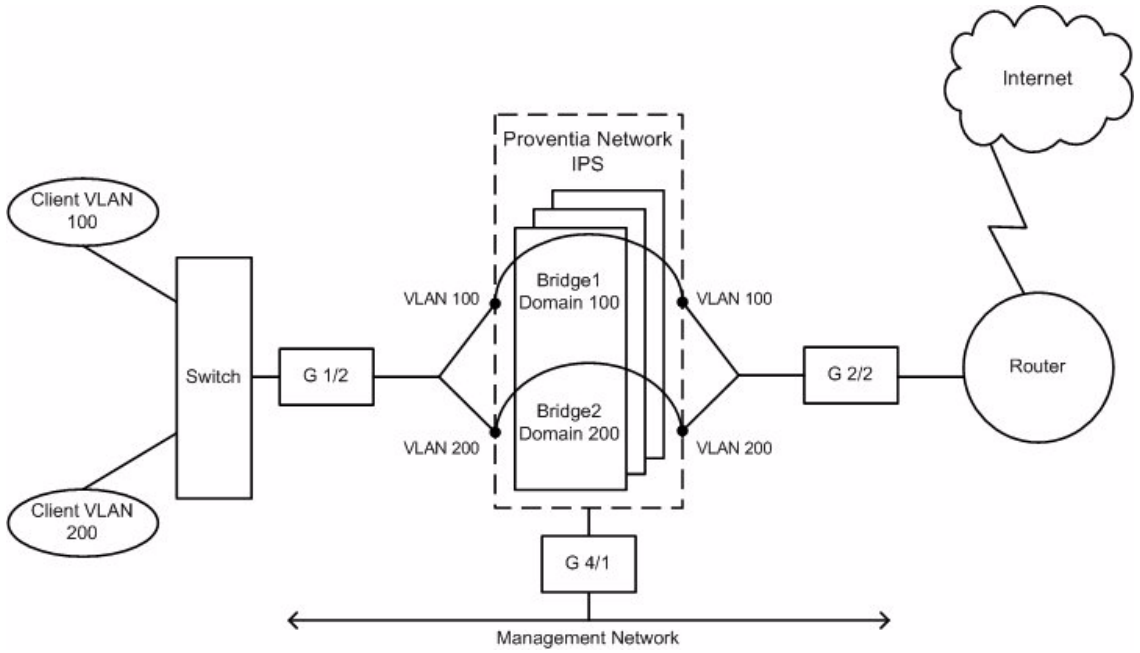
Configuring Bridges for a VLAN Trunk

To enable communication between two or more VLANs, configure a single pair of 802.1q VLAN trunk interfaces for all traffic passing through the Proventia Network IPS VAP group. Then, configure the X-Series system to create a separate bridge for each VLAN and assign a unique domain ID to each bridge.

Figure 13 on page 79 shows an example network topology that illustrates this type of bridge configuration.

See Example XOS Running Configuration: Configuring Bridges for a VLAN Trunk on page 79 for an example XOS configuration that implements this network topology.

Figure 13. Configuring Bridges for a VLAN Trunk



Example XOS Running Configuration: Configuring Bridges for a VLAN Trunk

```
vap-group ips xslinux_v3
  vap-count 2
  max-load-count 2
  ap-list ap1 ap2 ap3 ap4 ap5 ap6 ap7 ap8 ap9 ap10
  load-balance-vap-list 1 2 3 4 5 6 7 8 9 10
  ip-flow-rule ips_lb
    action load-balance
    activate
#
circuit bridge1 circuit-id 1027 domain 100
  device-name bridge1
  vap-group ips
circuit bridge2 circuit-id 1030 domain 200
  device-name bridge2
  vap-group ips
circuit mgmt circuit-id 1031
  device-name mgmt
  vap-group ips
    management-circuit
```

```
    ip 192.168.0.10/24 192.168.0.255 increment-per-vap 192.168.0.11
circuit lanv100 circuit-id 1025 domain 100
  device-name lanv100
  vap-group ips
    promiscuous-mode active
circuit wanv100 circuit-id 1026 domain 100
  device-name wanv100
  vap-group ips
    promiscuous-mode active
circuit lanv200 circuit-id 1028 domain 200
  device-name lanv200
  vap-group ips
    promiscuous-mode active
circuit wanv200 circuit-id 1029 domain 200
  device-name wanv200
  vap-group ips
    promiscuous-mode active
#
bridge-mode bridge1 transparent
  circuit lanv100
  circuit wanv100
bridge-mode bridge2 transparent
  circuit lanv200
  circuit wanv200
#
interface gigabitethernet 1/2
  logical lanv100 ingress-vlan-tag 100 100
    circuit lanv100
  logical lanv200 ingress-vlan-tag 200 200
    circuit lanv200
interface gigabitethernet 2/2
  logical wanv100 ingress-vlan-tag 100 100
    circuit wanv100
  logical wanv200 ingress-vlan-tag 200 200
    circuit wanv200
interface gigabitethernet 4/1
  logical mgmt
    circuit mgmt
```