



## Installation Guide

Revision C

# McAfee Firewall Enterprise 8.3.x

on Crossbeam X-Series Platforms

## **COPYRIGHT**

Copyright © 2014 McAfee, Inc. Do not copy without permission.

## **TRADEMARK ATTRIBUTIONS**

McAfee, the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

Product and feature names and descriptions are subject to change without notice. Please visit [mcafee.com](http://mcafee.com) for the most current products and features.

## **LICENSE INFORMATION**

### **License Agreement**

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

# Contents

<b>Preface</b>	<b>7</b>
About this guide . . . . .	7
Audience . . . . .	7
Conventions . . . . .	7
Find product documentation . . . . .	8
<b>1 Introduction</b>	<b>9</b>
Firewall Enterprise overview . . . . .	9
Firewall Enterprise on X-Series Platforms . . . . .	9
Management . . . . .	9
Unsupported features on X-Series Platforms . . . . .	9
Understanding X-Series Platform architecture . . . . .	10
Hardware modules . . . . .	10
Hosted applications . . . . .	11
Application data and management interfaces . . . . .	12
Single chassis fault-tolerance and performance features . . . . .	12
Dual-Box High Availability . . . . .	13
Network integration options . . . . .	14
Network interconnection modes . . . . .	14
Interface types . . . . .	15
Deployment examples . . . . .	16
Single chassis deployment example . . . . .	16
Dual-Box High Availability deployment example . . . . .	16
Serialization . . . . .	18

## Planning

<b>2 Hardware and software requirements</b>	<b>21</b>
X-Series Platform requirements . . . . .	21
Hardware and software requirements . . . . .	21
Configuration prerequisites . . . . .	22
Firewall Enterprise management requirements . . . . .	22
<b>3 Preparation</b>	<b>25</b>
Download the Firewall Enterprise CBI package . . . . .	25
Plan your network integration . . . . .	25
Determine the appropriate installation method . . . . .	26
Use the Automated Workflow System . . . . .	27
Manually install the firewall . . . . .	27

## Installation

<b>4 Single chassis AWS installation</b>	<b>31</b>
AWS installation prerequisites . . . . .	31

Prepare your interview responses . . . . .	31
Install Firewall Enterprise . . . . .	32
Finalize installation . . . . .	33
Configure a default route for Firewall Enterprise . . . . .	33
Verify the default route for the CPM . . . . .	34
Configure an NTP server on the CPM . . . . .	34
Configure DNS . . . . .	34
Configure the time zone . . . . .	35
Save the configuration . . . . .	36

**5 Single chassis manual installation 37**

Manual installation requirements . . . . .	37
Prepare your X-Series Platform . . . . .	37
Create incoming circuit groups . . . . .	38
Create a VAP group for Firewall Enterprise . . . . .	38
Create circuits . . . . .	40
Configure default routes and NTP . . . . .	43
Configure DNS . . . . .	44
Save the configuration . . . . .	45
Install Firewall Enterprise . . . . .	45
Install the Firewall Enterprise application . . . . .	45
Finalize the installation . . . . .	47
Configure the time zone . . . . .	49
Example configuration file . . . . .	50

**6 Dual-Box High Availability installation 53**

DBHA installation prerequisites . . . . .	53
Prepare each X-Series Platform for active-standby DBHA . . . . .	53
Connect your X-Series chassis interfaces . . . . .	54
Configure system identifiers . . . . .	55
Create incoming circuit groups . . . . .	55
Create a VAP group for Firewall Enterprise . . . . .	56
Create circuits . . . . .	57
Create a failover group for the Firewall Enterprise VAP group . . . . .	61
Create a virtual router for each circuit . . . . .	61
Enable VRRP on the Firewall Enterprise VAP group . . . . .	63
Configure default routes and NTP . . . . .	64
Configure DNS . . . . .	65
Save the configuration . . . . .	65
Install Firewall Enterprise on each X-Series Platform . . . . .	65
Install the Firewall Enterprise application . . . . .	66
Finalize the installation . . . . .	67
Configure the time zone . . . . .	69
Example configuration files . . . . .	70
Chassis A . . . . .	70
Chassis B . . . . .	72

## Management and integration

**7 Control Center registration 77**

Managing your firewall VAP group . . . . .	77
Register the Firewall Enterprise VAP group to the Control Center . . . . .	77
Configure audit archiving to Control Center . . . . .	78
Unlock the FTP user account . . . . .	78
Create an audit export policy . . . . .	79
Associate the audit export policy with your Firewall Enterprise VAP group . . . . .	79

	Validate and apply policy to the Firewall Enterprise VAP group . . . . .	80
<b>8</b>	<b>Network integration</b>	<b>81</b>
	Connect a firewall VAP group to a non-VLAN network . . . . .	81
	Create incoming circuit groups . . . . .	81
	Create a circuit . . . . .	82
	Configure an interface . . . . .	83
	Create a virtual router for each circuit . . . . .	84
	Save the configuration . . . . .	84
	Connect a firewall VAP group to a VLAN network . . . . .	85
	Create incoming circuit groups . . . . .	85
	Create a circuit for each VLAN . . . . .	85
	Configure an interface . . . . .	86
	Create a virtual router for each circuit . . . . .	87
	Save the configuration . . . . .	88
	Bridge two networks . . . . .	88
	Create incoming circuit groups for bridged networks . . . . .	89
	Create circuits for bridged networks . . . . .	89
	Configure interfaces . . . . .	90
	Create the bridge . . . . .	91
	Save the configuration . . . . .	92
<b>9</b>	<b>Dynamic routing configuration</b>	<b>93</b>
	How dynamic routing on Crossbeam X-Series Platforms works . . . . .	93
	Requirements for dynamic routing . . . . .	94
	Enable dynamic routing on Firewall Enterprise on Crossbeam X-Series Platforms . . . . .	94
	Configure VAP group interfaces for dynamic routing . . . . .	94
	Configure IP flow rules for dynamic routing agent protocol traffic . . . . .	95
	Enable and configure dynamic routing on Firewall Enterprise . . . . .	96
<b>10</b>	<b>VPN creation</b>	<b>97</b>
	Requirements for VPN . . . . .	97
	Create a VPN on your Firewall Enterprise VAP group . . . . .	97
<b>A</b>	<b>Appendix: Maintenance</b>	<b>99</b>
	Manage a firewall VAP group using the XOS command line interface . . . . .	99
	Monitor Firewall Enterprise and the X-Series Platform . . . . .	100
	Monitor using the Greenlight Element Manager . . . . .	100
	Monitor using the XOS command line interface . . . . .	101
	Add a VAP to a Firewall Enterprise VAP group . . . . .	102
	Prepare for installation . . . . .	102
	Install Firewall Enterprise on a new VAP . . . . .	102
	Verify installation . . . . .	103
	Remove a VAP from a Firewall Enterprise VAP group . . . . .	104
	Remove the VAP from the VAP group . . . . .	104
	Delete the VAP from your Control Center Management Server . . . . .	105
	Uninstall Firewall Enterprise from a VAP group . . . . .	105
	Uninstall the VAP group from your X-Series Platform . . . . .	105
	Delete the VAP group from your Control Center Management Server . . . . .	106
	Delete a Firewall Enterprise zone . . . . .	107
	Upgrade a firewall on a Crossbeam X-Series Platform . . . . .	108
	Upgrade Control Center . . . . .	108
	Upgrade or install your Crossbeam X-Series Platform . . . . .	108
	Install the Firewall Enterprise CBI package . . . . .	108



# Preface

This guide provides the information you need to install your McAfee product.

## Contents

- ▶ [About this guide](#)
- ▶ [Find product documentation](#)

---

## About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

## Audience





McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

## Conventions

This guide uses these typographical conventions and icons.

<i>Book title, term, emphasis</i>	Title of a book, chapter, or topic; a new term; emphasis.
<b>Bold</b>	Text that is strongly emphasized.
User input, code, message	Commands and other text that the user types; a code sample; a displayed message.
<b>Interface text</b>	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
	<b>Note:</b> Additional information, like an alternate method of accessing an option.
	<b>Tip:</b> Suggestions and recommendations.
	<b>Important/Caution:</b> Valuable advice to protect your computer system, software installation, network, business, or data.
	<b>Warning:</b> Critical advice to prevent bodily harm when using a hardware product.

---

## Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

### Task

- 1 Go to the McAfee ServicePortal at <http://support.mcafee.com> and click **Knowledge Center**.
- 2 Enter a product name, select a version, then click **Search** to display a list of documents.



# 1

## Introduction

McAfee® Firewall Enterprise (hereinafter Firewall Enterprise) is a next-generation firewall that runs on Crossbeam X-Series Platforms to provide superior performance, scalability, and flexibility.

### Contents

- ▶ *Firewall Enterprise overview*
- ▶ *Firewall Enterprise on X-Series Platforms*
- ▶ *Understanding X-Series Platform architecture*
- ▶ *Network integration options*
- ▶ *Deployment examples*

---

## Firewall Enterprise overview

Firewall Enterprise allows you to protect your network from unauthorized users and attackers, and to protect internal users as they access the Internet. Firewall Enterprise features provide powerful configuration options that allow you to control your users' access to almost any publicly available service on the Internet, while mitigating threats to your organization.

---

## Firewall Enterprise on X-Series Platforms

McAfee® Firewall Enterprise running on Crossbeam X-Series Platforms allows you to protect your network from unauthorized users and attackers, and to protect internal users as they access the Internet. Firewall Enterprise combines an application-layer firewall, user-based policy, IPsec VPN capabilities, SSL decryption, and Global Threat Intelligence™ into one security appliance that is designed to offer centralized perimeter security.

### Management

A standalone McAfee® Firewall Enterprise Control Center (Control Center) Management Server is required to manage Firewall Enterprise on X-Series Platforms.

### Unsupported features on X-Series Platforms

When installed on Crossbeam X-Series Platforms, Firewall Enterprise does not support these features.

- Firewall Enterprise Admin Console



Use a standalone Firewall Enterprise Control Center (Control Center) Management Server to manage Firewall Enterprise on X-Series Platforms.

- Multicast dynamic routing using the PIM-SM protocol
- Hybrid mode (configuring standard and transparent mode on the same firewall)

- Default route failover
- Quality of Service (QoS)
- Transparent (bridged) mode for these configurations:
  - Dual-Box High Availability
  - Multi-application serialization
- Dual-Box High Availability active-active mode



Active-standby DBHA is supported.

- X-Series Operating System (XOS) features:
  - VAP group hide-vlan-header parameter
  - Equal-cost multi-path routing
  - Configuration of the VRRP MAC address



If you need functionality similar to the VRRP MAC address, Crossbeam recommends configuring a user-defined MAC address on each traffic circuit/interface pair included in the VRRP failover group. For more information and the configuration procedure, refer to Crossbeam Technical Support Knowledgebase article 0004069.

---

## Understanding X-Series Platform architecture

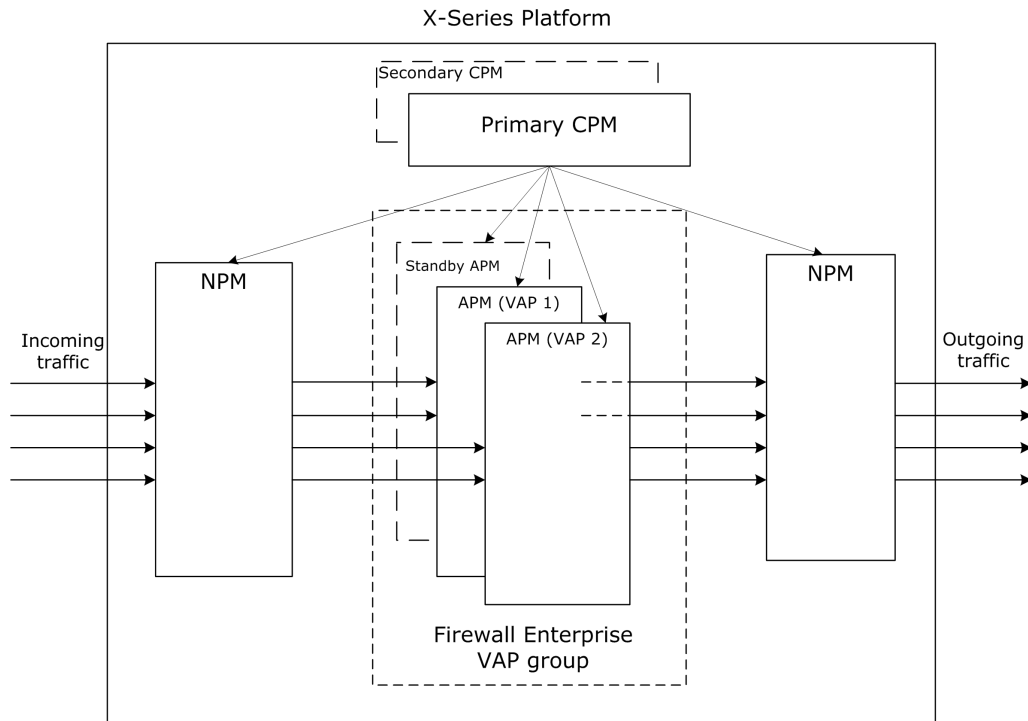
The Crossbeam X-Series Platform running XOS software is an open-networked application platform designed to deliver enhanced application services while providing high performance and High Availability. The modular design of the X-Series Platform allows it to run multiple applications while providing multi-gigabit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

### Hardware modules

Each X-Series Platform 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)
- **Network Processor Module (NPM)** — Provides network connectivity for the X-Series Platform, classifies packets, and load-balances flows among groups of APMs

The diagram shows how traffic flows through an X-Series Platform with Firewall Enterprise installed on two APMs in an X-Series chassis that contains two CPMs, two NPMs, and three APMs.



**Figure 1-1 High-level X-Series Platform architecture**

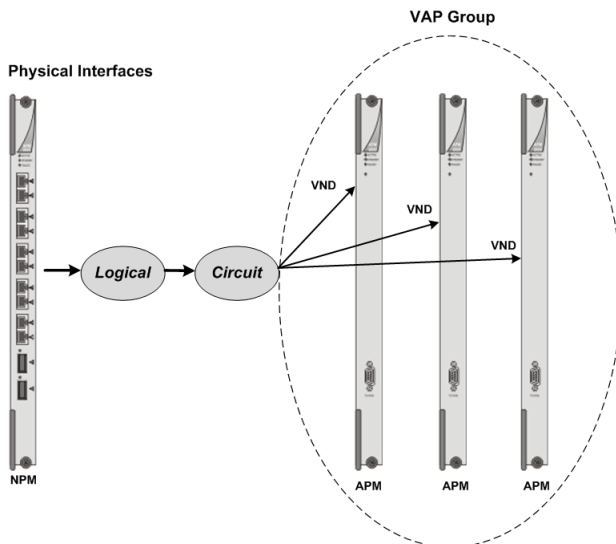
## Hosted applications

Applications that run on X-Series Platforms are made up of VAPs that are organized into VAP groups.

- **Virtual Application Processor (VAP)** — The application operating environment hosted by an APM, which consists of the operating system, system software, and one application (Firewall Enterprise)
- **VAP group** — A collection of VAPs running the same application that are grouped together to provide redundancy and increased throughput

## Application data and management interfaces

Applications are connected to physical networks by management and data interfaces. Figure 1-2 shows the components of an XOS interface.



**Figure 1-2 XOS components of an application interface**

A VAP group interface has four parts:

- **Physical interface** — An Ethernet port on an NPM that you configure to pass traffic between the X-Series Platform and an external network
- **Logical interface** — An interface that logically links circuit VNDs to a physical interface on an NPM
  - You can map only one circuit to each logical interface. However, you can map multiple logical interfaces to the same physical interface, allowing multiple circuits to pass traffic over a single physical interface.
  - You can also use link aggregation to bond multiple physical interfaces to a single logical interface, allowing one circuit to pass traffic over multiple physical interfaces.
- **Circuit** — A virtualized Ethernet connection configured for members of a VAP group  
Circuits provide a connection between the members of a VAP group and a physical interface, or an internal connection between VAP group members.



To create a Firewall Enterprise zone for a circuit, assign an incoming circuit group (ICG) to that circuit.

- **Virtual Network Device (VND)** — A virtual interface that represents a circuit that is assigned to a VAP group

## Single chassis fault-tolerance and performance features

The X-Series Platform provides several mechanisms that improve performance and help provide continuous operation in the event of a failure.

- **CP Redundancy** — Each chassis can contain two Control Processor Modules (CPMs). When two CPMs are present, one can be configured as Active and the other as Standby.
- **Interface Redundancy** — A physical interface can be configured as a backup to another physical interface. Failover occurs quickly and is transparent to the application.
- **LACP (Link Aggregation Control Protocol)** — Multiple physical interfaces can be combined into one interface. A failure of one physical link does not prevent traffic flow.

- **Virtual Application Processor (VAP) Load Balancing** — In a VAP group, each VAP runs an instance of the application, and traffic is load balanced among the VAPs. If a hardware or software failure occurs on a VAP, the system automatically redistributes the traffic flow among the remaining VAPs.
- **Standby VAP** — APMs that are not assigned to a VAP group are automatically configured as standby VAPs. If a VAP in any VAP group fails, a standby VAP automatically joins that group.
- **APM Preemption Mode** — Applications are assigned a priority. If a higher-priority application has a VAP failure, it can take a VAP from a lower-priority application.

The X-Series Platform can be configured to provide High Availability for all three types of modules and performance scalability for NPMs and APMs.

## Dual-Box High Availability

Dual-Box High Availability (DBHA) allows two or more X-Series Platforms to work together to provide fault tolerance. Firewall Enterprise supports active-standby DBHA across two Crossbeam X-Series Platforms.

DBHA is implemented using the following mechanisms.

### Virtual Router Redundancy Protocol (VRRP)

Using VRRP, configure two X-Series chassis so network traffic reroutes from a primary chassis to a standby chassis if a failure or unwanted change occurs on the primary chassis in any of these areas.

- Application Monitor
- Circuit
- Interface (physical or logical)
- VAP Group
- IP Address
- Next Hop IP Address
- Multi-Link Trunking Interface

### Failover groups

A failover group is a grouping of one or more virtual routers (VRs). A VR identifies the circuits and associated VAP groups for High Availability. Only a failover group— not the entire system or an individual VAP group— can fail over to a standby failover group on another system.

### Virtual router (VR)

A *virtual router* can be attached to a single circuit only and can include only one VAP group attached to that circuit.

In addition, the VR can assign individual IP addresses to the circuit and the VAP group interface. For circuits already configured with an IP address, the VR can also assign a virtual IP address. This virtual IP address allows you to configure failover groups using the same virtual IP address on other systems. Each virtual router can be configured to verify the state of the next hop IP address before using it.

### VRRP priority

Each failover group is assigned a VRRP priority. Typically failover groups are defined in pairs and the failover group with the higher priority is designated the Master. Both failover groups in a pair must have the same ID.

A failure within a chassis does not necessarily cause a failover from one failover group to another. Instead, the VRRP priority is reduced by a preconfigured value, called a priority-delta. Failover occurs only if the priority is reduced below the priority of the backup failover group. This minimizes or eliminates the problem of failing over to a chassis that has greater diminished capacity. After any failure is rectified, the VRRP priority increases by the same amount it was decremented by when that failure occurred. When all failures are rectified, the priority returns to the originally configured value.

## Control Link port (HA Port) and Management interfaces

The X-Series Platform requires a communication link between all X-Series Platforms in a High Availability (HA) configuration.

Crossbeam recommends using the CPM Control Link port and both Management ports on the primary CPMs and both Management ports on the secondary CPMs when connecting between chassis. In a dual-system configuration, each pair of ports (HA, Management 1, and Management 2) is connected to separate network broadcast domains. Crossbeam recommends that customers do not connect the Control Link ports or Management ports directly to each other. Connecting the ports directly can lead to scenarios that do not provide full redundancy.



Typically, you configure Control Link and Management ports for auto-negotiation. If you connect any of these ports to a switch and auto-negotiation does not work, use the `configure management high-availability or configure management ethernet` command to manually set up the communication parameters.

---

## Network integration options

Firewall Enterprise supports two network interconnection modes and several interface types that allow you to integrate the firewall into your network.

### Network interconnection modes

Firewall Enterprise supports these network interconnection modes.

- Standard (routed) mode
- Transparent (bridged) mode



Hybrid mode (combining standard and transparent mode on the same firewall) is not supported on Crossbeam X-Series Platforms.

### Standard (routed) mode

In this mode, a standard network interface connects the firewall to each network. Each firewall interface is assigned a unique IP address and associated with a security zone.

Hosts in a protected network communicate with other networks using the firewall IP address as the gateway. When traffic attempts to cross from one zone to another, the configured security policy is enforced. If the security policy allows the traffic, the firewall passes it between the networks like a router.

### Transparent (bridged) mode

In this mode, two interfaces are connected inside a single network and bridged to form a transparent interface. Each member interface is assigned to a unique zone, and the transparent interface is assigned an IP address for management and network address translation (NAT).

When traffic attempts to cross the bridge (from one zone to another), the configured security policy is enforced. If the security policy allows the traffic, the firewall passes it to the other zone. The traffic will be translated if NAT is enabled





A transparent interface can be configured with a single VLAN ID.

## Interface types

Firewall Enterprise supports several interface types that offer different functionality. The following table summarizes the available interface types and associates them with the equivalent Crossbeam XOS terminology.

**Table 1-1 Available interface types**

Firewall Enterprise interface type	Crossbeam XOS equivalent	Description
Standard interface based on a single NIC or VLAN	Logical interface and corresponding circuit	<p>Connects the firewall to a single network</p> <ul style="list-style-type: none"> <li>The interface is assigned a unique IP address in the connected subnet.</li> <li>Hosts in the connected network communicate with other networks using the firewall IP address as the gateway.</li> <li>The firewall allows traffic to pass between the networks like a router, enforcing your security policy.</li> </ul> <p> You cannot combine VLAN and non-VLAN logical interfaces on the same physical interface.</p>
Standard interface based on an aggregate NIC group	Multi-link group interface	<p>Combines multiple physical interfaces into a single virtual interface</p> <ul style="list-style-type: none"> <li>Aggregate groups use the Link Aggregation Control Protocol (LACP) and the Marker protocols defined by IEEE 802.1AX (formerly known as IEEE 802.3ad).</li> <li>The available bandwidth does not increase for a single conversation. All packets associated with a conversation are transmitted on the same link to maintain the packet order. Aggregate mode achieves a high bandwidth only when there are multiple, simultaneous conversations.</li> </ul>
Transparent interface	Bridge-mode bridge	<p>Bridges two interfaces</p> <ul style="list-style-type: none"> <li>Each interface that is a member of the bridge connected inside a single network and assigned a unique zone.</li> <li>Traffic passes through the firewall like a layer 2 switch, allowing you to enforce security policy inside the network without re-addressing the network.</li> </ul> <p> The firewall supports a maximum of one configured transparent interface (bridge) connecting two circuits. If a transparent interface is configured, additional traffic interfaces are not supported.</p>

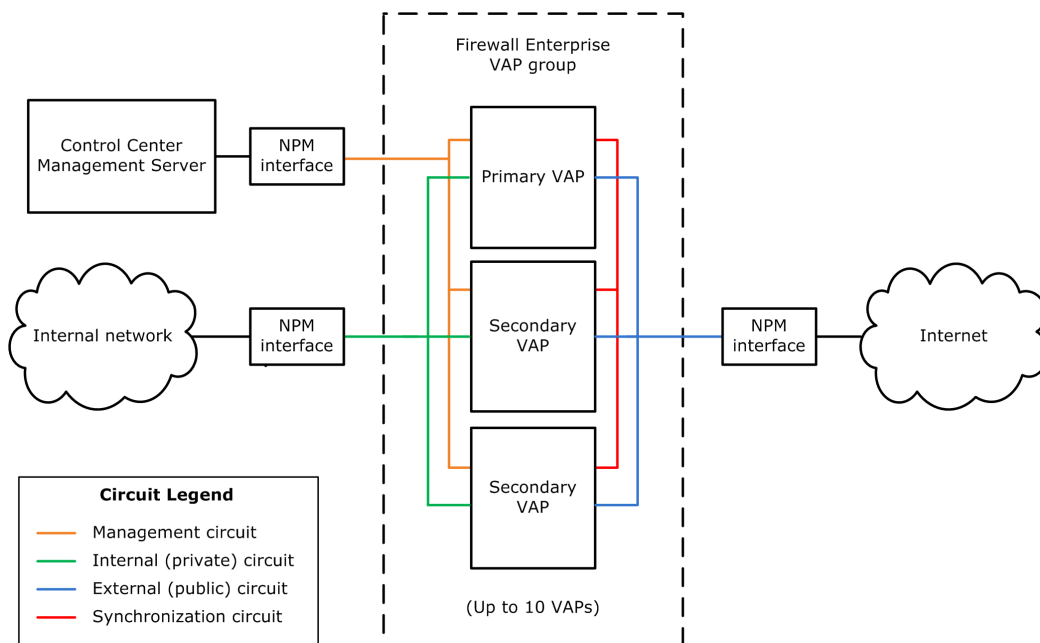
## Deployment examples

This section illustrates examples of single chassis, DBHA, and serialization deployments.

### Single chassis deployment example

The diagram shows a basic Firewall Enterprise on X-Series Platforms deployment. In this example, Firewall Enterprise is installed on a single X-Series Platform chassis.

- The Firewall Enterprise VAP group contains three VAPs.
- Network traffic flows through the firewall VAP group over the internal and external circuits.
- A Control Center Management Server manages the firewall VAP group over the management circuit.
- Individual firewall VAPs communicate with each other over the synchronization circuit.



**Figure 1-3 Example deployment**

#### See also

[Example configuration file on page 50](#)

### Dual-Box High Availability deployment example

The figure shows an example active-standby DBHA deployment.



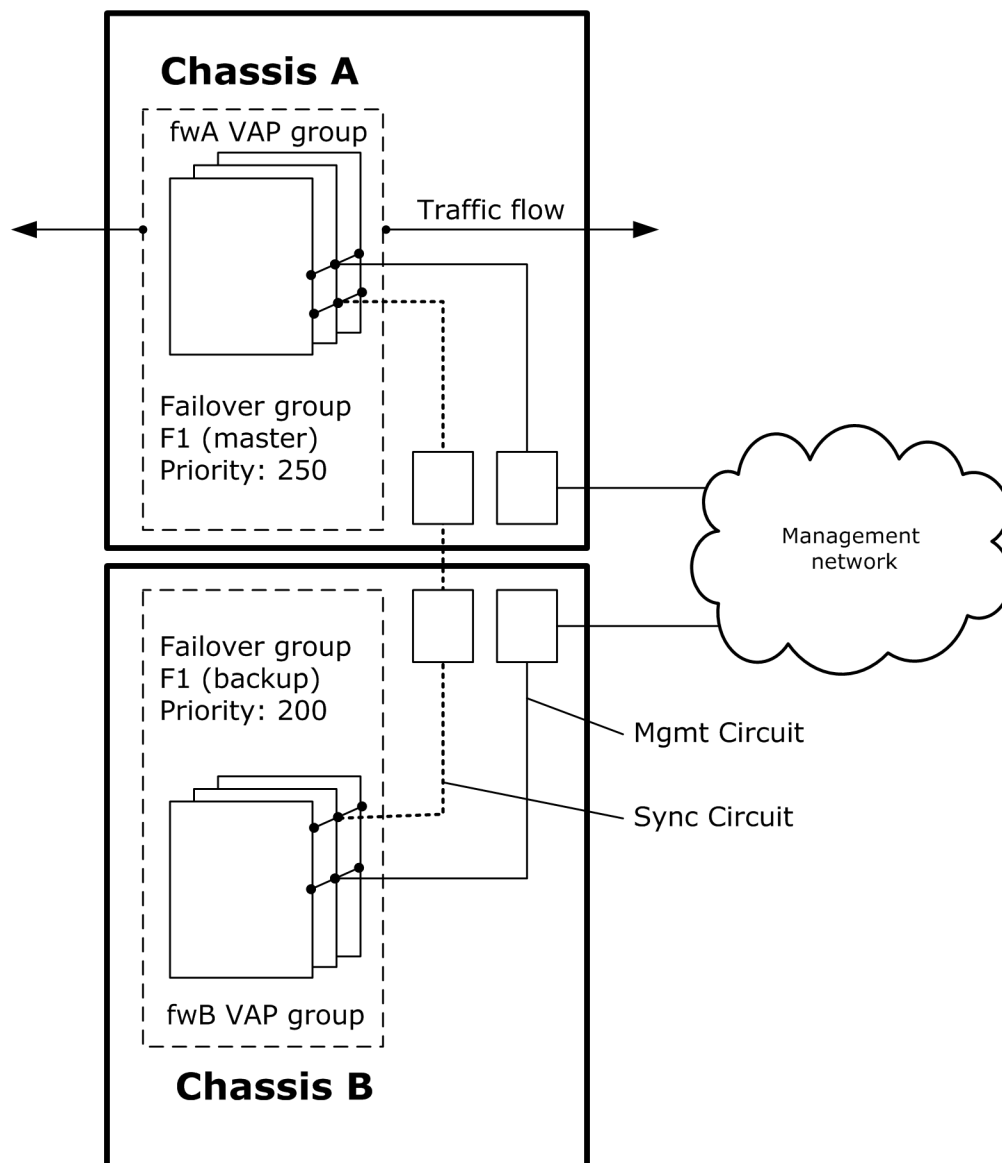
This example omits the Control Center Management Server and internal and external circuits to reduce complexity.

In this example, Firewall Enterprise is installed on two X-Series Platform chassis. Under normal conditions, all of the traffic is handled by chassis A. When a failover occurs, the standby chassis begins processing traffic. When the failure condition is resolved, the original roles might be restored depending on the configuration.



Firewall Enterprise is installed on the fwA and fwB VAP groups. On each chassis:

- The circuit configuration and circuit names are the same.
- Firewall VAPs and VAP groups communicate with each other over the synchronization circuit.
- Failover group F1 is associated with the fwA and fwB VAP groups.
  - The master failover group on chassis A has a higher priority, so chassis A handles all traffic under normal conditions.
  - The backup failover group on chassis B has a lower priority, so chassis B handles no traffic until a failover occurs.
- When any failure occurs, the actual VRRP priority of the failover groups is compared not the configured VRRP priority. If both chassis have experienced failures, the failover group with the higher actual priority is designated as master.



**Figure 1-4 Active-standby DBHA**

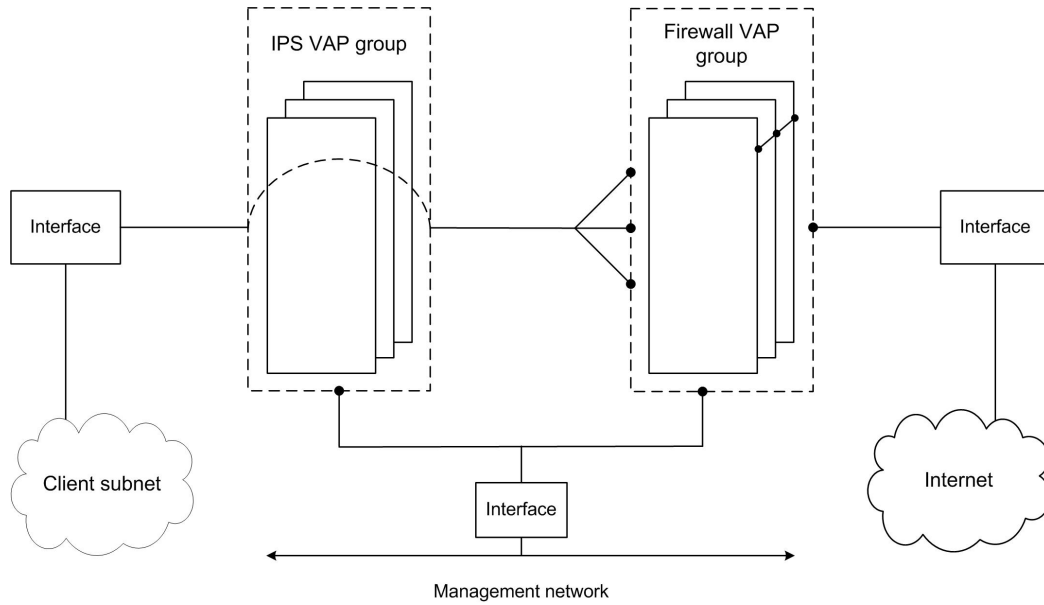
**See also**

*Example configuration files on page 70*

## Serialization

Firewall Enterprise can be deployed in series with other applications hosted by the X-Series Platform, allowing traffic to be inspected by both applications. In this example, Firewall Enterprise is deployed in-line with an IPS application on a single chassis.

For more information and configuration instructions, see the *Crossbeam Multi-Application Serialization Configuration Guide: IPS and Firewall*.



**Figure 1-5 Firewall Enterprise deployed in series with an IPS application**

# Planning

---

Chapter 2 *Hardware and software requirements*

Chapter 3 *Preparation*



# 2

## Hardware and software requirements

Make sure that your X-Series Platform fulfils the hardware, software, and configuration needs.

### Contents

- ▶ *X-Series Platform requirements*
- ▶ *Firewall Enterprise management requirements*

---

### X-Series Platform requirements

Before installing Firewall Enterprise, make sure that your X-Series Platform meets hardware, software, and configuration requirements.

### Hardware and software requirements

Firewall Enterprise is supported by specific X-Series Platforms and modules as shown in the table.

**Table 2-1 Hardware requirements summary**

Component	Requirement	Minimum quantity	Maximum quantity
X-Series Platform	One of the following: <ul style="list-style-type: none"><li>• X50 Platform</li><li>• X60 Platform</li><li>• X80-S Platform</li></ul>	1	2 (High Availability)
Control Processor Module (CPM)	CPM-9600	1	2 per chassis
Application Processor Module (APM)	APM-50	1	2 per chassis
	APM-9600	1	10 per chassis
Network Processor Module (NPM)	NPM-50	1	1 per chassis
	NPM-86x0	1	4 per chassis
	NPM-96x0	1	4 per chassis

All models of CPMs, NPMs, and APMs included in the same X-Series Platform must be compatible with one another. For detailed module compatibility matrices, see the hardware installation guide for your X-Series Platform.

## Application Processor Module (APM) requirements

Each APM module must meet these requirements.

- **Local disk** — At least one local disk
  - RAID 0 and RAID 1 disk configurations are also supported.
  - Two-disk, non-RAID configurations are not supported for Firewall Enterprise.
- **Memory** — A minimum of 12 GB  
Crossbeam strongly recommends that all APMs in a VAP group have the same memory configuration.

## Control Processor Module (CPM) requirements

The appropriate XOS version must be installed on each CPM in the X-Series chassis.

- Firewall Enterprise version 8.3.0 — XOS version 9.6.x, 9.7.1 and later, 9.9.x, or 10.0
- Firewall Enterprise version 8.3.1 or 8.3.2 — XOS version 9.6.5 and later, 9.7.1 and later, 9.9.x, or 10.0

## Network Processor Module (NPM) requirements

The X60 chassis can accommodate up to two NPMs, while the X80-S can accommodate up to four NPMs. The X50 chassis supports a single NPM-50. No other NPMs are supported in the X50 chassis.

## Configuration prerequisites

Before you can install Firewall Enterprise, the following X-Series configuration prerequisites must be met.

- The X-Series Platform must be installed as described in the appropriate hardware installation guide:
  - *Crossbeam X50 Platform Hardware Installation Guide*
  - *Crossbeam X60 Platform Hardware Installation Guide*
  - *Crossbeam X80 Platform Hardware Installation Guide*
- The X-Series Platform must be assigned an initial configuration as described in the *Crossbeam XOS Configuration Guide*.
- All physical network connections required to support the Firewall Enterprise deployment and configuration options must be connected and functioning normally.

---

## Firewall Enterprise management requirements

A standalone Firewall Enterprise Control Center Management Server is required to manage Firewall Enterprise on X-Series Platforms.

To manage Firewall Enterprise on X-Series Platforms, you need the following:

- Management Server at version 5.3.0 or later



The Management Server must be connected to a network reachable by the Firewall Enterprise management interface.

- Microsoft Windows-based computer to host the Control Center Client application
- Documentation

**Table 2-2 Required documents**

Source	Documents
McAfee	<ul style="list-style-type: none"> <li>• Grant letter (contains download, activation, and support information)</li> <li>• <i>McAfee Firewall Enterprise Release Notes</i></li> <li>• <i>McAfee Firewall Enterprise Product Guide</i></li> <li>• <i>McAfee Firewall Enterprise Control Center Quick Start Guide</i></li> <li>• <i>McAfee Firewall Enterprise Control Center Product Guide</i></li> </ul>
Crossbeam	<ul style="list-style-type: none"> <li>• Crossbeam hardware installation guide for your X-Series Platform:                             <ul style="list-style-type: none"> <li>• <i>Crossbeam X50 Platform Hardware Installation Guide</i></li> <li>• <i>Crossbeam X60 Platform Hardware Installation Guide</i></li> <li>• <i>Crossbeam X80 Platform Hardware Installation Guide</i></li> </ul> </li> <li>• <i>Crossbeam XOS Configuration Guide</i></li> <li>• <i>Crossbeam XOS Command Reference Guide</i></li> </ul>

The following Control Center features must be configured from the XOS command line interface:

- Static routing
- Interfaces
- Link aggregation (aggregate interfaces appear as normal interfaces in Control Center)
- Static ARP
- DNS (unless using firewall-hosted DNS)





# 3

## Preparation

Prepare and install Firewall Enterprise using the appropriate installation method.

### Contents

- ▶ *Download the Firewall Enterprise CBI package*
- ▶ *Plan your network integration*
- ▶ *Determine the appropriate installation method*

---

## Download the Firewall Enterprise CBI package

Download the CBI package.

### Task

- 1 Visit [support.mcafee.com](https://support.mcafee.com).
- 2 Click on the **Downloads** tab, then select the appropriate type of download.
- 3 Provide your grant number, then navigate to the appropriate product and version.



Your grant number is included in the grant letter you received from McAfee.

- 4 Download the .cbi file to your management computer.

---

## Plan your network integration

Decide which network interconnection mode and interface types are most appropriate for your network topology. You will use this information during the installation process.

### Task

- 1 Review the available network interconnection modes and interface types. See Network integration options.
- 2 Select a network interconnection mode. Use the following table to determine the action you need to take to configure the appropriate mode.

**Table 3-1 Network interconnection mode configuration methods**

Network interconnection mode	Configuration action based on installation method
Standard (routed)	<ul style="list-style-type: none"> <li>• <b>Manual installation</b> — Create standard interfaces for each network.</li> <li>• <b>Automated Workflow System (AWS) installation</b> — Choose the L3 topology during the AWS interview.</li> </ul>
Transparent (bridged)	<ul style="list-style-type: none"> <li>• <b>Manual installation</b> — Create a bridge that references both network segments.</li> <li>• <b>Automated Workflow System (AWS) installation</b> — Choose the L2 topology during the AWS interview.</li> </ul>

- 3 Determine which interface types are appropriate for your network.



If you chose transparent mode in the previous step, you must create an XOS bridge, which appears on the firewall as a transparent interface.

**See also**

[Network integration options on page 14](#)

## Determine the appropriate installation method

Use the following table to select the installation method that is appropriate for your situation.

**Table 3-2 Installation methods**

If...	Then use this installation method
All of these conditions are met: <ul style="list-style-type: none"> <li>• You are installing Firewall Enterprise on a single chassis.</li> <li>• No applications are installed on the X-Series Platform.</li> <li>• No XOS options are configured on the X-Series Platform.</li> </ul>	AWS installation
One or more of these conditions are met: <ul style="list-style-type: none"> <li>• You are configuring Firewall Enterprise for Dual-Box High Availability.</li> <li>• Other applications are installed on the X-Series Platform.</li> <li>• XOS options are configured on the X-Series Platform.</li> </ul>	Manual installation

**Tasks**

- [Use the Automated Workflow System on page 27](#)  
AWS provides automated installation based on information you provide.
- [Manually install the firewall on page 27](#)  
Install and register Firewall Enterprise.

## Use the Automated Workflow System

AWS provides automated installation based on information you provide.

After you complete the installation interview, AWS performs the following tasks:

- XOS configuration, including:
  - VAP group
  - Incoming circuit groups
  - Circuits
  - Interfaces
- Firewall Enterprise installation on the specified VAP group

To use the AWS installation method, perform these tasks:

### Task

- 1 Install Firewall Enterprise on the X-Series Platform.
- 2 Register the firewall to your Control Center Management Server.
- 3 [Optional] Perform post-setup tasks.
  - a Connect your firewall to additional networks.
  - b Create a VPN.

### See also

[Single chassis AWS installation on page 3](#)

[Control Center registration on page 4](#)

[Network integration on page 5](#)

[VPN creation on page 5](#)

## Manually install the firewall

Install and register Firewall Enterprise.

### Task

- 1 Install Firewall Enterprise.
  - **Single chassis**
  - **Dual-Box HA**
- 2 Register the firewall to your Control Center Management Server.
- 3 [Optional] Perform post-setup tasks.
  - a Connect your firewall to additional networks.
  - b Create a VPN.

### See also

[Single chassis manual installation on page 4](#)

[Dual-Box High Availability installation on page 4](#)

[Control Center registration on page 4](#)

[Network integration on page 5](#)

[VPN creation on page 5](#)

**Preparation**

Determine the appropriate installation method

# Installation

- 
- Chapter 4 *Single chassis AWS installation*
  - Chapter 5 *Single chassis manual installation*
  - Chapter 6 *Dual-Box High Availability installation*



# 4

## Single chassis AWS installation

Install Firewall Enterprise with Automated Workflow System (AWS).

### Contents

- ▶ *AWS installation prerequisites*
- ▶ *Prepare your interview responses*
- ▶ *Install Firewall Enterprise*
- ▶ *Finalize installation*

---

### AWS installation prerequisites

To install Firewall Enterprise with AWS, your X-Series Platform configuration cannot contain any of these elements.

- VAP groups
- Circuits
- Incoming-circuit-groups
- Interfaces
- Internal interfaces
- Group interfaces

If your X-Series Platform contains any of these elements, use the manual installation method.

---

### Prepare your interview responses

Plan your configuration to prepare for the AWS installation interview.

The interview asks for this information.

- IP addresses and optional VLANs for the management, synchronization, internal, and external interfaces
- Physical ports for the interfaces
- VAP group information
  - VAP group name
  - VAP count
  - Max load count
- Shared cluster password
- Firewall Enterprise serial number (refer to your McAfee grant letter)

## Install Firewall Enterprise

Install Firewall Enterprise, start AWS, and complete the installation interview.

### Task

- 1 Transfer the .cbi file to the /crossbeam/apps/archive directory on each X-Series CPM.
- 2 Establish a command line connection to the X-Series CPM using SSH (recommended) or Telnet, then log on.
- 3 Enter this XOS command to verify that the Firewall Enterprise CBI package is loaded in the correct directory (/crossbeam/apps/archive) on the X-Series Platform.

```
CBS# show application
App ID       : MFE
Name        : McAfee Firewall Enterprise
Version     : <firewall_version_number>
Release     : <release_number>
CBI Version  : <version_number>
```

- 4 Start AWS.

```
CBS# automated-workflow-menu

Welcome to the X-Series Platform Automated Workflow System!
Version: <version_number>

1. Configure XOS...
2. Upgrade XOS software and firmware...
3. View system configuration and status...
4. Applications...
5. Custom...

Select a submenu to view available automated workflows.
Enter x to exit or ? for help.

Please Enter Selection:
```

- 5 Enter option 4.

```
Please Enter Selection: 4
```

- 6 Verify that Firewall Enterprise is one of the application options.

```
.
.
<n>. MFE      Version <firewall_version_number> Release <number>
.
.
```



- 7 Enter the number that corresponds to Firewall Enterprise.

```
Please Enter Selection: <n>
```

The AWS installation interview begins.

- 8 Complete the AWS interview.



Your response to the question, Would you like to configure a L2 or L3 topology?, determines the network interconnection mode. To configure standard mode, choose L3. To configure transparent mode, choose L2.



Press ? at any time during the interview for assistance.

AWS notifies you when the configuration and installation process is complete.

## Finalize installation

Perform these tasks after the AWS installation process is complete.

### Tasks

- [Configure a default route for Firewall Enterprise on page 33](#)  
Firewall Enterprise sends traffic to the gateway specified by the default route if no other known route exists for the destination address.
- [Verify the default route for the CPM on page 34](#)  
During the initial configuration interview for the X-Series chassis, you specify the IP address for the management default gateway. This gateway is required for the CPM to connect to external networks.
- [Configure an NTP server on the CPM on page 34](#)  
Configure an NTP server on the CPM to ensure that correct time is supplied to the Firewall Enterprise VAP group.
- [Configure DNS on page 34](#)  
Configure DNS servers and host names for email.
- [Configure the time zone on page 35](#)  
While the firewall VAP group receives system time from XOS, the time zone is configured separately. Perform this procedure to set the time zone for the firewall VAP group.
- [Save the configuration on page 36](#)  
Save all of the configuration changes you made.

### Configure a default route for Firewall Enterprise

Firewall Enterprise sends traffic to the gateway specified by the default route if no other known route exists for the destination address.

```
CBS# configure ip route 0.0.0.0/0 <gateway_IP_address> vap-group <VAP_group_name>
CBS(config-ip-route)# end
CBS#
```

## Verify the default route for the CPM

During the initial configuration interview for the X-Series chassis, you specify the IP address for the management default gateway. This gateway is required for the CPM to connect to external networks.

To verify that the management gateway is configured on the X-Series chassis, enter this command:

```
CBS# search gateway show running-config
```

In the output of the command, verify that this line appears:

```
.
.
management default-gateway <IP_address>
.
.
```

If you do not see this line, configure the gateway using this command:

```
CBS# configure management default-gateway <IP_address>
```



The IP address that you configure must be consistent with the network segment the CPM management interface is connected to.

## Configure an NTP server on the CPM

Configure an NTP server on the CPM to ensure that correct time is supplied to the Firewall Enterprise VAP group.

```
CBS# configure ntp server <IP_address_of_NTP_server>
```

## Configure DNS

Configure DNS servers and host names for email.

### Tasks

- [Configure DNS servers for Firewall Enterprise on page 34](#)  
You can use the following command to configure a DNS server for the firewall VAP group.
- [Configure host names for email on page 34](#)  
Configure the `dns search-name` command to allow sendmail to resolve the host name of each VAP.

### Configure DNS servers for Firewall Enterprise

You can use the following command to configure a DNS server for the firewall VAP group.

```
CBS# configure dns server <server_IP> vap-group <VAP_group>
```



If you choose to configure firewall-hosted DNS using Control Center, the firewall VAP group ignores any DNS commands run at the XOS command line interface.

### Configure host names for email

Configure the `dns search-name` command to allow sendmail to resolve the host name of each VAP.

```
CBS# configure dns search-name <dns_domain> vap-group <VAP_group>
```

This command causes sendmail to use the host name *VAP\_name.domain* for each VAP.



Sendmail converts underscores (\_) in the firewall host names to dashes (-).

## Configure the time zone

While the firewall VAP group receives system time from XOS, the time zone is configured separately. Perform this procedure to set the time zone for the firewall VAP group.

### Task

- 1 Verify the XOS time zone.

```
CBS# show timezone
```

- 2 Determine which firewall VAP is the current master.

```
CBS# show ap-vap-mapping
```



The Master column is "true" for the current master VAP.

- 3 Access the console of the master VAP.

- a Access the Linux shell.

```
CBS# unix su
Password:
[root@<system-id> admin]#
```

- b Establish an rsh connection to the master VAP.

```
[root@<system-id> admin]# rsh <VAP_group>_<index_of_master>
<VAP_group>_<index_of_master> (<system-id>): ~#
```

- c Start a virtual console for the VAP.

```
<VAP_group>_<index_of_master> (<system-id>): ~# virsh console crbm_vm
Connected to domain crbm_vm
Escape character is ^]
```

- d Press **Enter**. The firewall login prompt appears.

```
SecureOS/amd64 (<VAP_group>_<index>VA.local) (ttyd0)
login:
```

- 4 Log on to the firewall VAP using the administrator account you created during installation.

- 5 Run the `srole` command to change to the Admn domain.

```
<VAP_group>_<index>VA:User {1} % srole
You have mail.
<VAP_group>_<index>VA:Admn {1} %
```

- 6 Configure the firewall time zone.

- a Run the `cf timezone list` command to view available time zone combinations.
- b Use the `cf timezone set` command to set the time zone.



For help, view the `cf_timezone` man page by running the `man cf_timezone` command.

7 After the time zone is set, exit to the XOS command line interface.

a Leave the Admn domain.

```
<VAP_group>_<index>VA:Admn {3} % exit
```

b Log off of the firewall console.

```
<VAP_group>_<index>VA:User {2} % exit
```

c Press **Control+]** to close the virtual console.

d Run the `exit` command to close the rsh session.

e Run the `exit` command to leave the Linux shell.

## Save the configuration

Save all of the configuration changes you made.

```
CBS# wr

Saving configuration ... Please be patient...
CBS#
```



You can also save a copy of your configuration to a file by running the command `copy running-config <path/filename>`.

# 5

## Single chassis manual installation

Manually install Firewall Enterprise on a single chassis.

### Contents

- ▶ [Manual installation requirements](#)
- ▶ [Prepare your X-Series Platform](#)
- ▶ [Install Firewall Enterprise](#)
- ▶ [Example configuration file](#)

---

## Manual installation requirements

Before you install Firewall Enterprise, make sure that your X-Series Platform meets the following requirements:

- The appliance meets the requirements listed in chapter 2, *Hardware and software requirements*.
- The appliance is installed and configured as described in the hardware installation guide for your Crossbeam X-Series Platform.

---

## Prepare your X-Series Platform

Perform the following tasks to prepare your X-Series Platform for installation.

### Tasks

- [Create incoming circuit groups on page 38](#)  
Incoming circuit groups (ICGs) associate circuits (firewall interfaces) with Firewall Enterprise security zones.
- [Create a VAP group for Firewall Enterprise on page 38](#)  
Create a VAP group for Firewall Enterprise, configure its attributes, and create the required IP flow rules.
- [Create circuits on page 40](#)  
You must create a circuit for each incoming circuit group you defined.
- [Configure default routes and NTP on page 43](#)  
Configure default routes for Firewall Enterprise and the CPM to ensure that network traffic flows correctly. Configure NTP on the CPM to ensure correct time is maintained.
- [Configure DNS on page 44](#)  
Configure DNS servers and host names for email.
- [Save the configuration on page 45](#)  
Save all of the configuration changes you made.

### See also

[Hardware and software requirements on page 3](#)

## Create incoming circuit groups

Incoming circuit groups (ICGs) associate circuits (firewall interfaces) with Firewall Enterprise security zones.

To install Firewall Enterprise, a minimum of four ICGs must be configured:

- **Management** — Allows Firewall Enterprise Control Center to manage the Firewall Enterprise VAP group; must be named *mgmt*
- **Synchronization** — Allows the nodes within the firewall VAP group to communicate with each other; must be named *sync*
- **Internal** — Represents a network behind the firewall
- **External** — Represents a network outside the firewall



The ICG names must be the same on both X-Series chassis.

Create the required ICGs.

### Task

- 1 Establish a command line interface connection to the X-Series CPM using SSH (recommended) or Telnet.
- 2 View the existing incoming circuit groups and record which ICG numbers are already in use.

```
CBS# show incoming-circuit-group-name
```



Do not use an ICG number that is already in use; doing so overwrites the existing number.

- 3 Create an ICG for management with the number 2 and the name *mgmt*.



Valid ICG numbers are 2–255.

```
CBS# configure incoming-circuit-group-name 2 mgmt
```

- 4 Create an ICG for synchronization with the number 3 and the name *sync*.

```
CBS# configure incoming-circuit-group-name 3 sync
```

- 5 Create an ICG for the network outside the firewall.

This example command creates an ICG with the number 4 and the name *external*.

```
CBS# configure incoming-circuit-group-name 4 external
```

- 6 Create an ICG for the network behind the firewall.

This example command creates an ICG with the number 5 and the name *internal*.

```
CBS# configure incoming-circuit-group-name 5 internal
```

- 7 [Optional] Create an additional ICG for each network that will connect to Firewall Enterprise.

## Create a VAP group for Firewall Enterprise

Create a VAP group for Firewall Enterprise, configure its attributes, and create the required IP flow rules.



The Firewall Enterprise VAP group on each chassis must have a unique name.

**Task**

- 1 Create a VAP group for Firewall Enterprise, and configure it to use the xsve virtualized environment VAP OS.

```
CBS# configure vap-group <VAP_group_name> xsve
Are you sure you want to create a new vap-group with OS version xsve? <Y or N>: y
Creating vap-group <VAP_group_name>. May take several minutes...
CBS(config-vap-grp)#
```

- 2 Configure the number of VAPs in the group.

```
CBS(config-vap-grp)# vap-count <number_of_VAPs_in_group>
Are you sure you want to adjust vap-count to <new_VAP_count>? <Y or N> [Y]: y
Adjusting vap-count. May take several minutes...
CBS(config-vap-grp)#
```

- 3 Set the max load count to the number of active VAP members in the VAP group.

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

- 4 Configure the flow-proxy option.

```
CBS(config-vap-grp)# flow-proxy
```

- 5 Configure the master-failover-trigger so a change in application status selects a new master VAP.

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

- 6 Configure the APM list for the VAP group.

```
CBS(config-vap-grp)# ap-list <apm_module_name1> [<apm_module_name2>]
 [<apm_module_name3>] ...
```

where *<apm\_module\_nameN>* is the name that the X-Series Platform assigned to the APM (example: ap3 or ap4).



APMs do not need to be active or present during installation. However, the APMs must be active to manage the Firewall Enterprise VAP group using Firewall Enterprise Control Center.

- 7 [Conditional] If you are planning to assign IPv6 addresses to the VAP group traffic circuits, enable IPv6.

```
CBS(config-vap-grp)# enable-ipv6
```

- 8 Configure a load balance IP flow rule for the VAP group.

```
CBS(config-vap-grp)# ip-flow-rule <load_balance_IP_flow_rule_name>
CBS(ip-flow-rule)# action load-balance
CBS(ip-flow-rule)# incoming-circuit-group any
CBS(ip-flow-rule)# activate
CBS(ip-flow-rule)# exit
CBS(config-vap-grp)#
```



You can use the timeout parameter to specify a custom timeout value. To avoid connection disruption, the ip flow timeout should be greater than the idle connection timeout configured for that flow on the firewall.

## 9 Configure an IP flow rule for intra-VAP group synchronization traffic.

```
CBS(config-vap-grp)# ip-flow-rule synchronization_flow_rule_name>
CBS(ip-flow-rule)# action broadcast
CBS(ip-flow-rule)# priority 30
CBS(ip-flow-rule)# incoming-circuit-group <number_of_synchronization_group>
CBS(ip-flow-rule)# destination-addr 239.255.0.0/24
CBS(ip-flow-rule)# activate
CBS(ip-flow-rule)# end
CBS#
```

## Create circuits

You must create a circuit for each incoming circuit group you defined.

Perform these tasks to create the required circuits:

### Tasks

- [Create a management circuit on page 40](#)  
Create a circuit and interface for management traffic.
- [Create a synchronization circuit on page 41](#)  
The synchronization circuit allows the Firewall Enterprise VAPs to communicate with each other.
- [Create internal and external circuits on page 42](#)  
You must create two circuits (internal and external) to allow network traffic to flow through the firewall.

## Create a management circuit

Create a circuit and interface for management traffic.

### Task

- 1 Create a management circuit.



McAfee recommends using the name **mgmt** for your management circuit.

```
CBS# configure circuit <management_circuit_name>
```

- 2 Assign a device name to the circuit.



To avoid confusion, the device name should be the same as, or based on, the circuit name.

```
CBS(conf-cct)# device-name <management_circuit_device_name>
```

- 3 Assign the management ICG to the management circuit.

```
CBS(conf-cct)# incoming-circuit-group <number_of_management_ICG>
```

- 4 Configure the management circuit as link state resistant.



This parameter causes the circuit between VAPs to stay up in the event that the external interface linking it to the Control Center Management Server goes down.

```
CBS(conf-cct)# link-state-resistant
```

- 5 Assign the Firewall Enterprise VAP group to the management circuit.

```
CBS(conf-cct)# vap-group <VAP_group_name>
CBS(conf-cct-vapgroup)#
```



- 6 Use increment-per-vap to assign a unique IP address for 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-ip)#
```



The increment-per-vap parameter must be used even if the VAP group contains only one APM.



McAfee recommends leaving some unused IP addresses so that additional APMs and VAPs can be added as the platform grows.

- 7 Configure a floating alias IP address for the master VAP in the Firewall Enterprise VAP group.

```
CBS(config-cct-vapgroup-ip)# alias <alias_ip_address>/<netmask>  
CBS(config-cct-vapgroup-alias)# floating  
CBS(config-cct-vapgroup-alias)# end  
CBS#
```

- 8 Configure a physical interface and assign it to the circuit.

```
CBS# configure interface ethernet <NPM_slot_number>/<port_number>  
CBS(conf-intf-ether)# logical <logical_name>  
CBS(intf-ether-logical)# circuit <management_circuit_name>  
CBS(intf-ether-log-cct)# end
```



The <management\_circuit\_name> parameter must be the circuit name that you assigned in step 1.

## Create a synchronization circuit

The synchronization circuit allows the Firewall Enterprise VAPs to communicate with each other.

### Task

- 1 Create a synchronization circuit.



McAfee recommends using the name **sync** for your synchronization circuit.

```
CBS# configure circuit <synchronization_circuit_name>
```

- 2 Assign a device name to the circuit.



To avoid confusion, the device name should be the same as, or based on, the circuit name.

```
CBS(conf-cct)# device-name <synchronization_circuit_device_name>
```

- 3 Assign the synchronization ICG to the synchronization circuit.

```
CBS(conf-cct)# incoming-circuit-group <number_of_synchronization_ICG>
```

- 4 Assign the Firewall Enterprise VAP group to the synchronization circuit.

```
CBS(conf-cct)# vap-group <VAP_group_name>  
CBS(conf-cct-vapgroup)#
```

- 5 Use increment-per-vap to assign a unique IP address for 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-ip)#
```



The increment-per-vap parameter must be used even if the VAP group contains only one APM.



McAfee recommends leaving some unused IP addresses so that additional APMs and VAPs can be added as the platform grows.

- 6 Configure a floating alias IP address for the master VAP in the Firewall Enterprise VAP group.

```
CBS(config-cct-vapgroup-ip)# alias <alias_ip_address>/<netmask>
CBS(config-cct-vapgroup-alias)# floating
CBS(config-cct-vapgroup-alias)# end
CBS#
```

- 7 Create an internal interface for the circuit.

```
CBS# configure interface-internal <interface_name>
CBS(conf-intf-internal)# logical-all <logical_name>
CBS(conf-intf-internal-log-all)# circuit <synchronization_circuit_name>
CBS(conf-intf-int-log-all-cct)# end
CBS#
```

## Create internal and external circuits

You must create two circuits (internal and external) to allow network traffic to flow through the firewall.



This task contains instructions on how to create a circuit that connects to a standard, non-VLAN interface. For instructions on creating VLAN interfaces, multi-link group interfaces, or bridges, refer to Chapter 8, Network integration.

Perform these steps for each circuit you need to configure.

### Task

- 1 Create the circuit.

```
CBS# configure circuit <circuit_name>
CBS(conf-cct)#
```

- 2 Assign a device name to the circuit.



To avoid confusion, the device name should be the same as, or based on, the circuit name.

```
CBS(conf-cct)# device-name <circuit_device_name>
```

- 3 Assign the appropriate ICG to the circuit.

```
CBS(conf-cct)# incoming-circuit-group <number_of_ICG>
```

- 4 Assign the Firewall Enterprise VAP group to the circuit.

```
CBS(conf-cct)# vap-group <VAP_group_name>
CBS(conf-cct-vapgroup)#
```

## 5 Configure an IPv4 or IPv6 address for the circuit.



If you intend to combine IPv4 and IPv6 addresses on the circuit, the first address you specify must be IPv4.

```
CBS(conf-cct-vapgroup) # ip <IP_address/mask>
CBS(conf-cct-vapgroup-ip) #
```

## 6 [Optional] Configure an alias IPv4 or IPv6 address for the circuit.

```
CBS(conf-cct-vapgroup-ip) # alias <alias_IP_address/mask>
CBS(conf-cct-vapgroup-alias) # endCBS#
```



Repeat this step as necessary to configure additional alias IP addresses.

## 7 Configure a physical interface.

```
CBS# configure interface ethernet <slot/port>
CBS(conf-intf-ether) #
```

## 8 Create a logical interface and associate it with the circuit.

```
CBS(conf-intf-ether) # logical <logical_name> circuit <circuit_name>
CBS(intf-ether-log-cct) # endCBS#
```

### See also

[Network integration on page 5](#)

## Configure default routes and NTP

Configure default routes for Firewall Enterprise and the CPM to ensure that network traffic flows correctly. Configure NTP on the CPM to ensure correct time is maintained.

### Tasks

- [Configure a default route for Firewall Enterprise on page 43](#)  
Firewall Enterprise sends traffic to the gateway specified by the default route if no other known route exists for the destination address.
- [Verify the default route for the CPM on page 44](#)  
During the initial configuration interview for the X-Series chassis, you specify the IP address for the management default gateway. This gateway is required for the CPM to connect to external networks.
- [Configure an NTP server on the CPM on page 44](#)  
Configure an NTP server on the CPM to ensure that correct time is supplied to the Firewall Enterprise VAP group.

## Configure a default route for Firewall Enterprise

Firewall Enterprise sends traffic to the gateway specified by the default route if no other known route exists for the destination address.

```
CBS# configure ip route 0.0.0.0/0 <gateway_IP_address> vap-group <VAP_group_name>
CBS(config-ip-route) # end
CBS#
```

## Verify the default route for the CPM

During the initial configuration interview for the X-Series chassis, you specify the IP address for the management default gateway. This gateway is required for the CPM to connect to external networks.

To verify that the management gateway is configured on the X-Series chassis, enter this command:

```
CBS# search gateway show running-config
```

In the output of the command, verify that this line appears:

```
.
.
management default-gateway <IP_address>
.
.
```

If you do not see this line, configure the gateway using this command:

```
CBS# configure management default-gateway <IP_address>
```



The IP address that you configure must be consistent with the network segment the CPM management interface is connected to.

## Configure an NTP server on the CPM

Configure an NTP server on the CPM to ensure that correct time is supplied to the Firewall Enterprise VAP group.

```
CBS# configure ntp server <IP_address_of_NTP_server>
```

## Configure DNS

Configure DNS servers and host names for email.

### Tasks

- [Configure DNS servers for Firewall Enterprise on page 44](#)  
You can use the following command to configure a DNS server for the firewall VAP group.
- [Configure host names for email on page 44](#)  
Configure the `dns search-name` command to allow sendmail to resolve the host name of each VAP.

## Configure DNS servers for Firewall Enterprise

You can use the following command to configure a DNS server for the firewall VAP group.

```
CBS# configure dns server <server_IP> vap-group <VAP_group>
```



If you choose to configure firewall-hosted DNS using Control Center, the firewall VAP group ignores any DNS commands run at the XOS command line interface.

## Configure host names for email

Configure the `dns search-name` command to allow sendmail to resolve the host name of each VAP.

```
CBS# configure dns search-name <dns_domain> vap-group <VAP_group>
```

This command causes sendmail to use the host name `VAP_name.domain` for each VAP.



Sendmail converts underscores (`_`) in the firewall host names to dashes (`-`).

## Save the configuration

Save all of the configuration changes you made.

```
CBS# wr

Saving configuration ... Please be patient...
CBS#
```



You can also save a copy of your configuration to a file by running the command `copy running-config <path/filename>`.

## Install Firewall Enterprise

Perform these tasks to install Firewall Enterprise on your X-Series Platform.



Before you install Firewall Enterprise, make sure no application is installed on the target VAP group.

### Tasks

- [Install the Firewall Enterprise application on page 45](#)  
Install Firewall Enterprise on the VAP group you created.
- [Finalize the installation on page 47](#)  
After you have completed the installation interview, reload the VAP group and verify that Firewall Enterprise installed correctly.
- [Configure the time zone on page 49](#)  
While the firewall VAP group receives system time from XOS, the time zone is configured separately. Perform this procedure to set the time zone for the firewall VAP group.

## Install the Firewall Enterprise application

Install Firewall Enterprise on the VAP group you created.



To obtain help for any question during the installation interview, enter a question mark (?).

### Task

- 1 Transfer the .cbi file to the /crossbeam/apps/archive directory on each X-Series CPM.
- 2 Establish a command line connection to the X-Series CPM using SSH (recommended) or Telnet, then log on.
- 3 Enter the following XOS command to verify that the Firewall Enterprise CBI package is loaded in the correct directory (/crossbeam/apps/archive) on the X-Series Platform:

```
CBS# show application
App ID       : MFE
Name        : McAfee Firewall Enterprise
Version     : <firewall_version_number>
Release     : <release_number>
CBI Version  : <version_number>
```

- 4 Enter the following XOS command to install the application on the VAP group you created, where `<VAP_group_name>` is the name of the Firewall Enterprise VAP group you created.

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

XOS checks the integrity of the CBI package and its dependencies. These progress messages appear:

```
Checking Integrity: [=====] 100% [ ok ]
Checking Dependencies: [=====] 100% [ ok ]
```

After the integrity check is complete, XOS displays the Firewall Enterprise license agreement.

- 5 Read the license agreement.



Press the spacebar to move through the license agreement or press **q** to skip it.

When you reach the end of the license agreement, the following prompt appears:

```
Do you accept the license agreement? [n]:
```

- 6 Use the following table to complete the installation interview.

Press **Enter** after each entry.

**Table 5-1 Installation interview responses**

Prompt	Entry
Do you accept the license agreement? [n]:	Press <b>Y</b> .
Enter the interface name from which you want to manage the system. [ ]:	Type the device name of the management circuit.
Enter the interface name for the synchronization network [ ]:	Type the device name of the synchronization circuit.
Please enter Shared Cluster Password below Password:	Type and confirm a password that the firewall VAPs will use to communicate with each other.
Serial number (See Activation Certificate) [ ]:	Type the Firewall Enterprise serial number provided in your McAfee grant letter.
First Name through License Comments	Enter your registration information.
external (internet) zone name [external]:	Type the name of the external ICG.
internal zone name [internal]:	Type the name of the internal ICG.
Internal mail host (example: mail.example.com) [ ]:	Type the host name of your email server.
Username (example: admin) [ ]:	Type the name of the firewall administrator.
Please enter Password below Password:	Enter and confirm a password for the firewall administrator.
Administrator's email address (optional - press 'Enter' to omit) (example: me@mail.example.com) [ ]:	Type an email address for the administrative account, or press <b>Enter</b> to omit it.

**Table 5-1 Installation interview responses** (continued)

Prompt	Entry
Are any changes needed? [n]:	<ul style="list-style-type: none"> <li>To modify your answers, press <b>Y</b>.</li> <li>To accept the answers and proceed with the installation, press <b>N</b>.</li> </ul> <p>XOS installs Firewall Enterprise on the VAP group that you specified and displays the progress of the application installation on each VAP.</p>
Do you want to save it to startup-config? <Y or N>[Y]:	Press <b>Y</b> .

## Finalize the installation

After you have completed the installation interview, reload the VAP group and verify that Firewall Enterprise installed correctly.

### Tasks

- [Reload the Firewall Enterprise VAP group on page 47](#)  
Reload the Firewall Enterprise VAP group for the installation to take effect.
- [Verify installation on page 47](#)  
Verify the application is running.

## Reload the Firewall Enterprise VAP group

Reload the Firewall Enterprise VAP group for the installation to take effect.

### Task

- 1 Reload the Firewall Enterprise VAP group.

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

The following prompt appears:

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

- 2 Press **Y**, then press **Enter**.

## Verify installation

Verify the application is running.

Enter this command.

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

VAP group information is provided.


For example, the following text is displayed for Firewall Enterprise VAP group *cybele*, which contains three VAPs.

```
CBS# show application vap-group cybele
VAP Group      : cybele
App ID        : MFE
Name          : McAfee Firewall Enterprise
Version       : <firewall_version_number>
Release      : <release_number>
Start on Boot : yes
App Monitor   : on
```

```
Reload on Failure      : off
App State (cybele_1)  : Up
App State (cybele_2)  : Up
App State (cybele_3)  : Up
```

For a description of each parameter in the output, refer to the table.

**Table 5-2 VAP group application information**

Parameter	Description
VAP Group	Displays the VAP group the application is installed on.
App ID	Displays the application identifier assigned to the application.
Name	Displays the application name.
Version	Displays the application version.
Release	Displays the application release number.
Start on boot	Indicates whether the application automatically starts running when you boot the VAP group: <ul style="list-style-type: none"> <li>• <b>yes</b> — The application starts automatically when you boot the VAP group.</li> <li>• <b>no</b> — The application does not start automatically when you boot the VAP group.</li> </ul>
App Monitor	Indicates whether application monitoring is enabled (on) or disabled (off) for the VAP group the application is installed on; by default, application monitoring is enabled (on). <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  If application monitoring is enabled (on) and 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 load balance list. </div>
App State	Indicates the current state of the application on the VAP with the VAP index number <i>n</i> . Possible application states are: <ul style="list-style-type: none"> <li>• <b>Up</b> — Application is running on the VAP.</li> <li>• <b>Down</b> — Application is not running on the VAP, but the APM the VAP is loaded on is functional.</li> <li>• <b>Initializing</b> — The application is rebooting.</li> <li>• <b>Not Monitored</b> — Application monitoring is disabled on the VAP group the application is installed on. Therefore, XOS is unable to determine the current state of the application on any VAP.</li> </ul>

## Troubleshoot installation problems

If you experience problems during the installation, you can check the log messages and errors.

- Examine the `/var/log/messages` file the CPM.
- View the installation error and warning messages by entering the following command:

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



## Configure the time zone

While the firewall VAP group receives system time from XOS, the time zone is configured separately. Perform this procedure to set the time zone for the firewall VAP group.

### Task

- 1 Verify the XOS time zone.

```
CBS# show timezone
```

- 2 Determine which firewall VAP is the current master.

```
CBS# show ap-vap-mapping
```



The Master column is "true" for the current master VAP.

- 3 Access the console of the master VAP.

- a Access the Linux shell.

```
CBS# unix su
Password:
[root@<system-id> admin]#
```

- b Establish an rsh connection to the master VAP.

```
[root@<system-id> admin]# rsh <VAP_group>_<ndex_of_master>
<VAP_group>_<index_of_master> (<system-id>): ~#
```

- c Start a virtual console for the VAP.

```
<VAP_group>_<index_of_master> (<system-id>): ~# virsh console crbm_vm
Connected to domain crbm_vm
Escape character is ^]
```

- d Press **Enter**. The firewall login prompt appears.

```
SecureOS/amd64 (<VAP_group>_<index>VA.local) (ttyd0)
login:
```

- 4 Log on to the firewall VAP using the administrator account you created during installation.

- 5 Run the `srole` command to change to the Admn domain.

```
<VAP_group>_<index>VA:User {1} % srole
You have mail.
<VAP_group>_<index>VA:Admn {1} %
```

- 6 Configure the firewall time zone.

- a Run the `cf timezone list` command to view available time zone combinations.
- b Use the `cf timezone set` command to set the time zone.



For help, view the `cf_timezone` man page by running the `man cf_timezone` command.

- 7 After the time zone is set, exit to the XOS command line interface.

- a Leave the Admn domain.

```
<VAP_group>_<index>VA:Admn {3} % exit
```

- b Log off of the firewall console.

```
<VAP_group>_<index>VA:User {2} % exit
```

- c Press **Control+]** to close the virtual console.
- d Run the `exit` command to close the rsh session.
- e Run the `exit` command to leave the Linux shell.

## Example configuration file

The following configuration file example approximates the single chassis deployment example.

```
ntp server 10.65.240.40

vap-group firewall xsve
vap-count 3
max-load-count 3
ap-list ap2 ap3 ap4
load-balance-vap-list 1 2 3 4 5 6 7 8 9 10
master-failover-trigger application
flow-proxy
ip-flow-rule load_balance
  action load-balance
  incoming-circuit-group any
activate
ip-flow-rule firewall_sync
  action broadcast priority 30
  incoming-circuit-group 5
  destination-addr 239.255.0.0/24
activate

dns server 192.168.215.100 vap-group firewall
dns server 192.168.215.200 vap-group firewall

incoming-circuit-group-name 2 external
incoming-circuit-group-name 4 mgmt
incoming-circuit-group-name 5 sync
incoming-circuit-group-name 3 internal

circuit external circuit-id 1026
device-name external
incoming-circuit-group 2
vap-group firewall
ip 10.66.146.11/24 10.66.146.255

circuit mgmt circuit-id 1025
device-name mgmt
incoming-circuit-group 4
vap-group firewall
ip 10.69.153.131/24 10.69.153.255 increment-per-vap 10.69.153.133
alias 10.69.153.130/24 10.69.153.255
floating

circuit sync circuit-id 1029
device-name sync
incoming-circuit-group 5
link-state-resistant
vap-group firewall
ip 10.69.157.131/24 10.69.157.255 increment-per-vap 10.69.157.133
alias 10.69.157.130/24 10.69.157.255
floating

circuit internal circuit-id 1027
device-name internal
incoming-circuit-group 3
vap-group firewall
```

```
ip 10.66.144.10/24 10.66.144.255

interface ethernet 1/2
  logical external
  circuit external

interface ethernet 1/3
  logical internal
  circuit internal

interface ethernet 1/6
  logical mgmt
  circuit mgmt

interface-internal sync
  logical-all sync
  circuit sync

ip route 0.0.0.0 0.0.0.0 10.69.153.30 circuit mgmt

management default-gateway 10.69.153.30
```

**See also**

*Single chassis deployment example on page 16*



# 6

## Dual-Box High Availability installation

Prepare each chassis to configure Firewall Enterprise for Dual-Box High Availability (DBHA) installation.

### Contents

- ▶ *DBHA installation prerequisites*
- ▶ *Prepare each X-Series Platform for active-standby DBHA*
- ▶ *Install Firewall Enterprise on each X-Series Platform*
- ▶ *Example configuration files*

---

### DBHA installation prerequisites

Before you install Firewall Enterprise, make sure both X-Series Platforms meet the necessary requirements and are configured appropriately.

- The appliances must meet the requirements listed in Chapter 2, *Hardware and software requirements*.
- The appliances must be installed and configured as described in the hardware installation guide for your Crossbeam X-Series Platform.



The optional `vrrp-mac` command is not supported on the xsve VAP operating system required for Firewall Enterprise on X-Series Platforms. If your multi-system High Availability configuration requires a shorter recovery time than what the `vrrp-mac` command provides, Crossbeam recommends configuring a user-defined MAC address on each traffic circuit/interface pair included in the VRRP failover group. For more information and the configuration procedure, refer to Crossbeam Technical Support Knowledgebase article 0004069.

### See also

*Hardware and software requirements on page 3*

---

### Prepare each X-Series Platform for active-standby DBHA

Perform these tasks on each chassis that will participate in the DBHA configuration.

**Tasks**

- [Connect your X-Series chassis interfaces on page 54](#)  
To avoid a single point of failure, both the primary and standby CPMs in each of the two chassis in a Dual-Box High Availability configuration should be connected in more than one way.
- [Configure system identifiers on page 55](#)  
You must configure system identifiers on each chassis.
- [Create incoming circuit groups on page 55](#)  
Incoming circuit groups (ICGs) associate circuits (firewall interfaces) with Firewall Enterprise security zones.
- [Create a VAP group for Firewall Enterprise on page 56](#)  
Create a VAP group for Firewall Enterprise, configure its attributes, and create the required IP flow rules.
- [Create circuits on page 57](#)  
Circuits attached to the Virtual Environment (VE) VAP appear as individual interfaces to Firewall Enterprise. Create a circuit for each incoming circuit group you defined in *Create incoming circuit groups*.
- [Create a failover group for the Firewall Enterprise VAP group on page 61](#)  
Create a failover group for the Firewall Enterprise VAP group on each X-Series chassis.
- [Create a virtual router for each circuit on page 61](#)  
Create a virtual router for each circuit you created, and associate it with the failover group.
- [Enable VRRP on the Firewall Enterprise VAP group on page 63](#)  
VRRP monitors the Firewall Enterprise VAP group for failure of individual VAPs.
- [Configure default routes and NTP on page 64](#)  
Configure default routes for Firewall Enterprise and the CPM to ensure that network traffic flows correctly. Configure NTP on the CPM to ensure correct time is maintained.
- [Configure DNS on page 65](#)  
Configure DNS servers and host names for email.
- [Save the configuration on page 65](#)  
Save all of the configuration changes you made.

**Connect your X-Series chassis interfaces**

To avoid a single point of failure, both the primary and standby CPMs in each of the two chassis in a Dual-Box High Availability configuration should be connected in more than one way.

Crossbeam recommends that the two chassis be interconnected using these interfaces on all CPMs:

- High Availability (HA) ports
- Management 1 ports
- Management 2 ports



Do not connect these ports directly. Instead, use separate network broadcast domains for each type of port (the HA ports, the Management 1 ports, and the Management 2 ports) on both the Primary CPMs and the Secondary CPMs.

## Configure system identifiers

You must configure system identifiers on each chassis.

### Task

- 1 Establish a command line interface connection to the X-Series CPM using SSH (recommended) or Telnet.
- 2 Configure a unique local system identifier.
  - a Specify a unique system identifier. The valid range is 1–255.

```
CBS# configure system-identifier <ID number>
Each chassis a must have a unique system ID.
```

- b Activate the new system identifier.

```
CBS# reload all
This command may take a few minutes.
Any unsaved configuration will be lost.
Do you want to save it to startup-config? <Y or N>[Y]:y
#Start Configuration Validation
##
#End Configuration Validation
Do you still want to save the current configuration? <Y or N>[Y]:y
Proceed with reload? <Y or N> [Y]:y
```

- 3 Specify the system identifier of the remote chassis.

```
CBS# configure remote-box <remote_system_ID> <HA_IP_of_remote_CPM>
CBS(conf-remote-box)# end
```



Crossbeam recommends configuring additional management IP addresses for each remote CPM.

## Create incoming circuit groups

Incoming circuit groups (ICGs) associate circuits (firewall interfaces) with Firewall Enterprise security zones.

To install Firewall Enterprise, a minimum of four ICGs must be configured:

- **Management** — Allows Firewall Enterprise Control Center to manage the Firewall Enterprise VAP group; must be named *mgmt*
- **Synchronization** — Allows the nodes within the firewall VAP group to communicate with each other; must be named *sync*
- **Internal** — Represents a network behind the firewall
- **External** — Represents a network outside the firewall



The ICG names must be the same on both X-Series chassis.

Create the required ICGs.

### Task

- 1 Establish a command line interface connection to the X-Series CPM using SSH (recommended) or Telnet.

- 2 View the existing incoming circuit groups and record which ICG numbers are already in use.

```
CBS# show incoming-circuit-group-name
```



Do not use an ICG number that is already in use; doing so overwrites the existing number.

- 3 Create an ICG for management with the number 2 and the name *mgmt*.



Valid ICG numbers are 2–255.

```
CBS# configure incoming-circuit-group-name 2 mgmt
```

- 4 Create an ICG for synchronization with the number 3 and the name *sync*.

```
CBS# configure incoming-circuit-group-name 3 sync
```

- 5 Create an ICG for the network outside the firewall.

This example command creates an ICG with the number 4 and the name *external*.

```
CBS# configure incoming-circuit-group-name 4 external
```

- 6 Create an ICG for the network behind the firewall.

This example command creates an ICG with the number 5 and the name *internal*.

```
CBS# configure incoming-circuit-group-name 5 internal
```

- 7 [Optional] Create an additional ICG for each network that will connect to Firewall Enterprise.

## Create a VAP group for Firewall Enterprise

Create a VAP group for Firewall Enterprise, configure its attributes, and create the required IP flow rules.



The Firewall Enterprise VAP group on each chassis must have a unique name.

### Task

- 1 Create a VAP group for Firewall Enterprise, and configure it to use the xsve virtualized environment VAP OS.

```
CBS# configure vap-group <VAP_group_name> xsve
Are you sure you want to create a new vap-group with OS version xsve? <Y or N>: y
Creating vap-group <VAP_group_name>. May take several minutes...
CBS(config-vap-grp)#
```

- 2 Configure the number of VAPs in the group.

```
CBS(config-vap-grp)# vap-count <number_of_VAPs_in_group>
Are you sure you want to adjust vap-count to <new_VAP_count>? <Y or N> [Y]: y
Adjusting vap-count. May take several minutes...
CBS(config-vap-grp)#
```



- 3 Set the max load count to the number of active VAP members in the VAP group.

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

- 4 Configure the flow-proxy option.

```
CBS(config-vap-grp)# flow-proxy
```

- 5 Configure the master-failover-trigger so a change in application status selects a new master VAP.

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

- 6 Configure the APM list for the VAP group.

```
CBS(config-vap-grp)# ap-list <apm_module_name1> [<apm_module_name2>]  
 [<apm_module_name3>] ...
```

where *<apm\_module\_nameN>* is the name that the X-Series Platform assigned to the APM (example: ap3 or ap4).



APMs do not need to be active or present during installation. However, the APMs must be active to manage the Firewall Enterprise VAP group using Firewall Enterprise Control Center.

- 7 [Conditional] If you are planning to assign IPv6 addresses to the VAP group traffic circuits, enable IPv6.

```
CBS(config-vap-grp)# enable-ipv6
```

- 8 Configure a load balance IP flow rule for the VAP group.

```
CBS(config-vap-grp)# ip-flow-rule <load_balance_IP_flow_rule_name>  
CBS(ip-flow-rule)# action load-balance  
CBS(ip-flow-rule)# incoming-circuit-group any  
CBS(ip-flow-rule)# activate  
CBS(ip-flow-rule)# exit  
CBS(config-vap-grp)#
```



You can use the timeout parameter to specify a custom timeout value. To avoid connection disruption, the ip flow timeout should be greater than the idle connection timeout configured for that flow on the firewall.

- 9 Configure an IP flow rule for intra-VAP group synchronization traffic.

```
CBS(config-vap-grp)# ip-flow-rule <synchronization_flow_rule_name>  
CBS(ip-flow-rule)# action broadcast  
CBS(ip-flow-rule)# priority 30  
CBS(ip-flow-rule)# incoming-circuit-group <number_of_synchronization_group>  
CBS(ip-flow-rule)# destination-addr 239.255.0.0/24  
CBS(ip-flow-rule)# activate  
CBS(ip-flow-rule)# end  
CBS#
```

## Create circuits

Circuits attached to the Virtual Environment (VE) VAP appear as individual interfaces to Firewall Enterprise. Create a circuit for each incoming circuit group you defined in *Create incoming circuit groups*.

Perform these tasks to create the required circuits.

## Tasks

- [Create a management circuit on page 58](#)  
Create and configure a management interface, then map the circuit to use a unique IP address to access each VAP in the group.
- [Create a synchronization circuit on page 59](#)  
The synchronization circuit allows the Firewall Enterprise VAPs to communicate with each other.
- [Create internal and external circuits on page 60](#)  
You must create two circuits (internal and external) to allow network traffic to flow through the firewall.

## Create a management circuit

Create and configure a management interface, then map the circuit to use a unique IP address to access each VAP in the group.

### Task

- 1 Create a management circuit.

```
CBS# configure circuit <mgmt_circuit_name>
```

- 2 Assign a device name to the circuit.



The device name must be the same on both X-Series Platforms.



To avoid confusion, the device name should be the same as, or based on, the circuit name.

```
CBS(conf-cct)# device-name <management_circuit_device_name>
```

- 3 Assign the management ICG to the management circuit.

```
CBS(conf-cct)# incoming-circuit-group <number_of_management_ICG>
```

- 4 Configure the management circuit as link state resistant.



This parameter causes the circuit between VAPs to stay up in the event that the external interface linking it to the Control Center Management Server goes down.

```
CBS(conf-cct)# link-state-resistant
```

- 5 Assign the Firewall Enterprise VAP group to the management circuit.

```
CBS(conf-cct)# vap-group <VAP_group_name>
CBS(conf-cct-vapgroup)#
```

- 6 Use `increment-per-vap` to assign a unique IP address for 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-ip)#
```



The `increment-per-vap` parameter must be used even if the VAP group contains only one APM.



McAfee recommends leaving some unused IP addresses so that additional APMs and VAPs can be added as the platform grows.

## 7 Configure a physical interface and assign it to the circuit.

```
CBS# configure interface ethernet <NPM_slot_number>/<port_number>
CBS(conf-intf-ether)# logical <logical_name>
CBS(intf-ether-logical)# circuit <management_circuit_name>
CBS(intf-ether-log-cct)# end
```



The <management\_circuit\_name> parameter must be the circuit name you assigned in step 1.

## Create a synchronization circuit

The synchronization circuit allows the Firewall Enterprise VAPs to communicate with each other.

### Task

#### 1 Create a synchronization circuit.



McAfee recommends using the name **sync** for your synchronization circuit.

```
CBS# configure circuit <synchronization_circuit_name>
```

#### 2 Assign a device name to the circuit.



The device name must be the same on both X-Series Platforms.



To avoid confusion, the device name should be the same as, or based on, the circuit name.

```
CBS(conf-cct)# device-name <synchronization_circuit_device_name>
```

#### 3 Assign the synchronization ICG to the synchronization circuit.

```
CBS(conf-cct)# incoming-circuit-group <number_of_synchronization_ICG>
```

#### 4 Configure the sync circuit as link state resistant.



This parameter causes the circuit between VAPs to stay up in the event that the external interface goes down.

```
CBS(conf-cct)# link-state-resistant
```

#### 5 Assign the Firewall Enterprise VAP group to the synchronization circuit.

```
CBS(conf-cct)# vap-group <VAP_group_name>CBS(conf-cct-vapgroup)#
```

#### 6 Use increment-per-vap to assign a unique IP address for 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-ip)#
```



The increment-per-vap parameter must be used even if the VAP group contains only one APM.



McAfee recommends leaving some unused IP addresses so that additional APMs and VAPs can be added as the platform grows.

## 7 Configure an interface and a logical line to connect the sync circuits on both chassis.

```
CBS# configure interface ethernet <slot/port> logical <logical_name>
CBS(intf-ether-logical)# circuit <synchronization_circuit_name>
CBS(intf-ether-log-cct)# end
CBS#
```

### Create internal and external circuits

You must create two circuits (internal and external) to allow network traffic to flow through the firewall.



This task contains instructions on how to create a circuit that connects to a standard, non-VLAN interface. For instructions on creating VLAN interfaces, multi-link group interfaces, or bridges, refer to Chapter 8, *Network integration*.

Perform these steps for each circuit you need to configure.

#### Task

##### 1 Create the circuit.

```
CBS# configure circuit <circuit_name>
CBS(conf-cct)#
```

##### 2 Assign a device name to the circuit.



The device name must be the same on both X-Series Platforms.



To avoid confusion, the device name should be the same as, or based on, the circuit name.

```
CBS(conf-cct)# device-name <circuit_device_name>
```

##### 3 Assign the appropriate ICG to the circuit.

```
CBS(conf-cct)# incoming-circuit-group <number_of_ICG>
```

##### 4 Assign the Firewall Enterprise VAP group to the circuit.

```
CBS(conf-cct)# vap-group <VAP_group_name>
CBS(conf-cct-vapgroup)#
```

##### 5 Configure an interface and a logical line.

```
CBS# configure interface ethernet <slot/port> logical <logical_name>
CBS(intf-ether-logical)# circuit <circuit_name>
CBS(intf-ether-log-cct)# end
CBS#
```

#### See also

[Network integration on page 5](#)

## Create a failover group for the Firewall Enterprise VAP group

Create a failover group for the Firewall Enterprise VAP group on each X-Series chassis.

### Task

- 1 Create a failover group by assigning it a name and ID number.

```
CBS# configure vrrp failover-group <failover_group_name> failover-group-id <1-255>
CBS(conf-vrrp-group) #
```



The failover group ID must be the same on both chassis.

- 2 Specify the VRRP priority for the failover group.



VRRP priority should be different for each chassis; the failover group with the higher priority is the master. Certain events such as an interface failure or a change in VAP group member count can be configured to decrement the VRRP priority. A chassis failover occurs when the VRRP priority value of one failover group drops below the priority of the failover group on the other chassis.

```
CBS(conf-vrrp-group) # priority <1-255>
CBS(conf-vrrp-group) #
```

## Create a virtual router for each circuit

Create a virtual router for each circuit you created, and associate it with the failover group.

### Tasks

- [Create a virtual router for the management circuit on page 61](#)  
Perform this task to create a virtual router for the management circuit.
- [Create a virtual router for the sync circuit on page 62](#)  
Perform this task to create a virtual router for the synchronization circuit.
- [Create a virtual router for each traffic circuit on page 62](#)  
Perform this task to create a virtual router for each traffic circuit you created.

## Create a virtual router for the management circuit

Perform this task to create a virtual router for the management circuit.

### Task

- 1 Add the virtual router to the failover group you created.

```
CBS#
configure vrrp failover-group <failover_group_name> failover-group-id <1-255>
CBS(conf-vrrp-group) #
```

- 2 Create a virtual router, assign it an ID, and attach it to the management circuit.

```
CBS(conf-vrrp-group) # virtual-router vrrp-id <1-4096> circuit
<management_circuit_name>
CBS(conf-vrrp-failover-vr) #
```

- 3 Assign the virtual router to the Firewall Enterprise VAP group.

```
CBS(conf-vrrp-failover-vr) # vap-group<VAP_group_name>
CBS(conf-vrrp-vr-vapgroup) #
```

- Assign a floating virtual IP address to the virtual router.

```
CBS(conf-vrrp-vr-vapgroup)# virtual-ip <IP/netmask>
CBS(conf-vrrp-vr-virtual-ali)# floating
```

- Run the `exit` command until you return to the `CBS#` prompt.

## Create a virtual router for the sync circuit

Perform this task to create a virtual router for the synchronization circuit.

### Task

- Add the virtual router to the failover group you created.

```
CBS#
configure vrrp failover-group <failover_group_name> failover-group-id <1-255>
CBS(conf-vrrp-group)#
```

- Create a virtual router, assign it an ID, and attach it to the synchronization circuit.

```
CBS(conf-vrrp-group)# virtual-router vrrp-id <1-4096> circuit
<synchronization_circuit_name>
CBS(conf-vrrp-failover-vr)#
```

- Assign the virtual router to the Firewall Enterprise VAP group.

```
CBS(conf-vrrp-failover-vr)# vap-group<VAP_group_name>
CBS(conf-vrrp-vr-vapgroup)#
```

- Assign a floating virtual IP address to the virtual router.

```
CBS(conf-vrrp-vr-vapgroup)# virtual-ip <IP/netmask>
CBS(conf-vrrp-vr-virtual-ali)# floating
```

- Run the `exit` command until you return to the `CBS#` prompt.

## Create a virtual router for each traffic circuit

Perform this task to create a virtual router for each traffic circuit you created.

### Task

- Add the virtual router to the failover group you created.

```
CBS# configure vrrp failover-group <failover_group_name> failover-group-id <1-255>
CBS(conf-vrrp-group)#
```

- Create a virtual router, assign it an ID, and attach it to the traffic circuit.

```
CBS(conf-vrrp-group)# virtual-router vrrp-id <1-4096> circuit <circuit_name>
CBS(conf-vrrp-failover-vr)#
```

- Assign a priority-delta value to the virtual router.

When a virtual router fails, the associated failover group's priority value is decremented by the priority-delta value. The priorities of the failover groups on the two chassis are compared; if the priority of the master failover group has a lower priority than the standby failover group, the standby chassis becomes the master. The priority-delta value is added back to the priority when the VR recovers.

```
CBS(conf-vrrp-failover-vr)# priority-delta <1-255>
CBS(conf-vrrp-failover-vr)#
```

- 4 Enable the backup-stay-up option to keep the virtual router circuit interface up when the failover group is in backup mode.

```
CBS(conf-vrrp-failover-vr)# backup-stay-up
CBS(conf-vrrp-failover-vr)#
```

- 5 Assign the virtual router to the Firewall Enterprise VAP group.

```
CBS(conf-vrrp-failover-vr)# vap-group<uicontrol> <VAP_group_name>
CBS(conf-vrrp-vr-vapgroup)#
```

- 6 Assign an IP address to the virtual router.

```
CBS(conf-vrrp-vr-vapgroup)# ip <IP/netmask>
CBS(conf-vrrp-vr-vapgroup)#
```

- 7 Run the `exit` command until you return to the CBS# prompt.

## Enable VRRP on the Firewall Enterprise VAP group

VRRP monitors the Firewall Enterprise VAP group for failure of individual VAPs.

By setting the `active-vap-threshold` and the `priority-delta`, individual VAP failures can decrement VRRP priority and cause a comparison with the VRRP priority on the remote chassis. Failover occurs when the `priority-delta` value decrements the priority value of the master failover group below the priority value of the associated failover group on the remote chassis.

To configure the Firewall Enterprise VAP group for failover:

### Task

- 1 Enable VRRP on the Firewall Enterprise VAP group.

```
CBS# configure vrrp vap-group <VAP_group_name>
CBS(conf-vrrp-vap-group)#
```

- 2 Assign the VRRP-enabled Firewall Enterprise VAP group to the failover group you created.

```
CBS(conf-vrrp-vap-group)# failover-group-list <failover_group>
CBS(conf-vrrp-vap-group)#
```

- 3 Set the `priority-delta` value for the VAP group.



VRRP decrements the priority of the failover group whenever the number of active VAPs falls below the `active-vap-threshold`. When the VAP returns to the Active state, the `priority-delta` value is added back to the priority value.

```
CBS(conf-vrrp-vap-group)# priority-delta <1-255>
CBS(conf-vrrp-vap-group)# exit
```

## Configure default routes and NTP

Configure default routes for Firewall Enterprise and the CPM to ensure that network traffic flows correctly. Configure NTP on the CPM to ensure correct time is maintained.

### Tasks

- [Configure a default route for Firewall Enterprise on page 64](#)  
Firewall Enterprise sends traffic to the gateway specified by the default route if no other known route exists for the destination address.
- [Verify the default route for the CPM on page 64](#)  
During the initial configuration interview for the X-Series chassis, you specify the IP address for the management default gateway. This gateway is required for the CPM to connect to external networks.
- [Configure an NTP server on the CPM on page 64](#)  
Configure an NTP server on the CPM to ensure that correct time is supplied to the Firewall Enterprise VAP group.

### Configure a default route for Firewall Enterprise

Firewall Enterprise sends traffic to the gateway specified by the default route if no other known route exists for the destination address.

```
CBS# configure ip route 0.0.0.0/0 <gateway_IP_address> vap-group <VAP_group_name>
CBS(config-ip-route)# end
CBS#
```

### Verify the default route for the CPM

During the initial configuration interview for the X-Series chassis, you specify the IP address for the management default gateway. This gateway is required for the CPM to connect to external networks.

To verify that the management gateway is configured on the X-Series chassis, enter this command:

```
CBS# search gateway show running-config
```

In the output of the command, verify that this line appears:

```
.
.
management default-gateway <IP_address>
.
.
```

If you do not see this line, configure the gateway using this command:

```
CBS# configure management default-gateway <IP_address>
```



The IP address that you configure must be consistent with the network segment the CPM management interface is connected to.

### Configure an NTP server on the CPM

Configure an NTP server on the CPM to ensure that correct time is supplied to the Firewall Enterprise VAP group.

```
CBS# configure ntp server <IP_address_of_NTP_server>
```



## Configure DNS

Configure DNS servers and host names for email.

### Tasks

- [Configure DNS servers for Firewall Enterprise on page 65](#)  
You can use the following command to configure a DNS server for the firewall VAP group.
- [Configure host names for email on page 65](#)  
Configure the `dns search-name` command to allow sendmail to resolve the host name of each VAP.

### Configure DNS servers for Firewall Enterprise

You can use the following command to configure a DNS server for the firewall VAP group.

```
CBS# configure dns server <server_IP> vap-group <VAP_group>
```



If you choose to configure firewall-hosted DNS using Control Center, the firewall VAP group ignores any DNS commands run at the XOS command line interface.

### Configure host names for email

Configure the `dns search-name` command to allow sendmail to resolve the host name of each VAP.

```
CBS# configure dns search-name <dns_domain> vap-group <VAP_group>
```

This command causes sendmail to use the host name `VAP_name.domain` for each VAP.



Sendmail converts underscores (`_`) in the firewall host names to dashes (`-`).

## Save the configuration

Save all of the configuration changes you made.

```
CBS# wr

Saving configuration ... Please be patient...
CBS#
```



You can also save a copy of your configuration to a file by running the command `copy running-config <path/filename>`.

---

## Install Firewall Enterprise on each X-Series Platform

Perform several tasks on both X-Series Platforms to install Firewall Enterprise.

## Tasks

- [Install the Firewall Enterprise application on page 66](#)  
Install Firewall Enterprise on the VAP group you created.
- [Finalize the installation on page 67](#)  
After you have completed the installation interview, reload the VAP group and verify that Firewall Enterprise installed correctly.
- [Configure the time zone on page 69](#)  
While the firewall VAP group receives system time from XOS, the time zone is configured separately. Perform this procedure to set the time zone for the firewall VAP group.

## Install the Firewall Enterprise application

Install Firewall Enterprise on the VAP group you created.



To obtain help for any question during the installation interview, enter a question mark (?).

### Task

- 1 Transfer the .cbi file to the /crossbeam/apps/archive directory on each X-Series CPM.
- 2 Establish a command line connection to the X-Series CPM using SSH (recommended) or Telnet, then log on.
- 3 Enter the following XOS command to verify that the Firewall Enterprise CBI package is loaded in the correct directory (/crossbeam/apps/archive) on the X-Series Platform:

```
CBS# show application
App ID       : MFE
Name        : McAfee Firewall Enterprise
Version     : <firewall_version_number>
Release     : <release_number>
CBI Version  : <version_number>
```

- 4 Enter the following XOS command to install the application on the VAP group you created, where <VAP\_group\_name> is the name of the Firewall Enterprise VAP group you created.

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

XOS checks the integrity of the CBI package and its dependencies. These progress messages appear:

```
Checking Integrity: [=====] 100% [ ok ]
Checking Dependencies: [=====] 100% [ ok ]
```

After the integrity check is complete, XOS displays the Firewall Enterprise license agreement.

- 5 Read the license agreement.



Press the spacebar to move through the license agreement or press q to skip it.

When you reach the end of the license agreement, the following prompt appears:

```
Do you accept the license agreement? [n]:
```

- 6 Use the following table to complete the installation interview.  
Press **Enter** after each entry.

**Table 6-1 Installation interview responses**

Prompt	Entry
Do you accept the license agreement? [n]:	Press <b>Y</b> .
Enter the interface name from which you want to manage the system. [ ]:	Type the device name of the management circuit.
Enter the interface name for the synchronization network [ ]:	Type the device name of the synchronization circuit.
Please enter Shared Cluster Password below Password:	Type and confirm a password that the firewall VAPs will use to communicate with each other.
Serial number (See Activation Certificate) [ ]:	Type the Firewall Enterprise serial number provided in your McAfee grant letter.
First Name through License Comments	Enter your registration information.
external (internet) zone name [external]:	Type the name of the external ICG.
internal zone name [internal]:	Type the name of the internal ICG.
Internal mail host (example: mail.example.com) [ ]:	Type the host name of your email server.
Username (example: admin) [ ]:	Type the name of the firewall administrator.
Please enter Password below Password:	Enter and confirm a password for the firewall administrator.
Administrator's email address (optional - press 'Enter' to omit) (example: me@mail.example.com) [ ]:	Type an email address for the administrative account, or press <b>Enter</b> to omit it.
Are any changes needed? [n]:	<ul style="list-style-type: none"> <li>To modify your answers, press <b>Y</b>.</li> <li>To accept the answers and proceed with the installation, press <b>N</b>.</li> </ul> <p>XOS installs Firewall Enterprise on the VAP group that you specified and displays the progress of the application installation on each VAP.</p>
Do you want to save it to startup-config? <Y or N>[Y]:	Press <b>Y</b> .

## Finalize the installation

After you have completed the installation interview, reload the VAP group and verify that Firewall Enterprise installed correctly.

### Tasks

- [Reload the Firewall Enterprise VAP group on page 68](#)  
Reload the Firewall Enterprise VAP group for the installation to take effect.
- [Verify installation on page 68](#)  
Verify the application is running.

## Reload the Firewall Enterprise VAP group

Reload the Firewall Enterprise VAP group for the installation to take effect.

### Task

- 1 Reload the Firewall Enterprise VAP group.

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

The following prompt appears:

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

- 2 Press **Y**, then press **Enter**.

## Verify installation

Verify the application is running.

Enter this command.

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

VAP group information is provided.

For example, the following text is displayed for Firewall Enterprise VAP group *cybele*, which contains three VAPs.


```
CBS# show application vap-group cybele
VAP Group           : cybele
App ID              : MFE
Name                : McAfee Firewall Enterprise
Version             : <firewall_version_number>
Release             : <release_number>
Start on Boot       : yes
App Monitor         : on
Reload on Failure   : off
App State (cybele_1) : Up
App State (cybele_2) : Up
App State (cybele_3) : Up
```

For a description of each parameter in the output, refer to the table.

**Table 6-2 VAP group application information**

Parameter	Description
<b>VAP Group</b>	Displays the VAP group the application is installed on.
<b>App ID</b>	Displays the application identifier assigned to the application.
<b>Name</b>	Displays the application name.
<b>Version</b>	Displays the application version.
<b>Release</b>	Displays the application release number.
<b>Start on boot</b>	Indicates whether the application automatically starts running when you boot the VAP group: <ul style="list-style-type: none"> <li>• <b>yes</b> — The application starts automatically when you boot the VAP group.</li> <li>• <b>no</b> — The application does not start automatically when you boot the VAP group.</li> </ul>

**Table 6-2 VAP group application information** (continued)

Parameter	Description
App Monitor	<p>Indicates whether application monitoring is enabled (on) or disabled (off) for the VAP group the application is installed on; by default, application monitoring is enabled (on).</p> <p> If application monitoring is enabled (on) and 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 load balance list.</p>
App State	<p>Indicates the current state of the application on the VAP with the VAP index number <i>n</i>. Possible application states are:</p> <ul style="list-style-type: none"> <li>• <b>Up</b> — Application is running on the VAP.</li> <li>• <b>Down</b> — Application is not running on the VAP, but the APM the VAP is loaded on is functional.</li> <li>• <b>Initializing</b> — The application is rebooting.</li> <li>• <b>Not Monitored</b> — Application monitoring is disabled on the VAP group the application is installed on. Therefore, XOS is unable to determine the current state of the application on any VAP.</li> </ul>

## Troubleshoot installation problems

If you experience problems during the installation, you can check the log messages and errors.

- Examine the `/var/log/messages` file the CPM.
- View the installation error and warning messages by entering the following command:

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

## Configure the time zone

While the firewall VAP group receives system time from XOS, the time zone is configured separately. Perform this procedure to set the time zone for the firewall VAP group.

### Task

- 1 Verify the XOS time zone.

```
CBS# show timezone
```

- 2 Determine which firewall VAP is the current master.

```
CBS# show ap-vap-mapping
```



The Master column is "true" for the current master VAP.

- 3 Access the console of the master VAP.
  - a Access the Linux shell.

```
CBS# unix su
Password:
[root@<system-id> admin]#
```

- b Establish an rsh connection to the master VAP.

```
[root@<system-id> admin]# rsh <VAP_group>_<index_of_master>
<VAP_group>_<index_of_master> (<system-id>): ~#
```

- c Start a virtual console for the VAP.

```
<VAP_group>_<index_of_master> (<system-id>): ~# virsh console crbm_vm
Connected to domain crbm_vm
Escape character is ^]
```

- d Press **Enter**. The firewall login prompt appears.

```
SecureOS/amd64 (<VAP_group>_<index>VA.local) (ttyd0)
login:
```

- 4 Log on to the firewall VAP using the administrator account you created during installation.

- 5 Run the `srole` command to change to the Admn domain.

```
<VAP_group>_<index>VA:User {1} % srole
You have mail.
<VAP_group>_<index>VA:Admn {1} %
```

- 6 Configure the firewall time zone.

- a Run the `cf timezone list` command to view available time zone combinations.

- b Use the `cf timezone set` command to set the time zone.



For help, view the `cf_timezone` man page by running the `man cf_timezone` command.

- 7 After the time zone is set, exit to the XOS command line interface.

- a Leave the Admn domain.

```
<VAP_group>_<index>VA:Admn {3} % exit
```

- b Log off of the firewall console.

```
<VAP_group>_<index>VA:User {2} % exit
```

- c Press **Control+]** to close the virtual console.  
d Run the `exit` command to close the rsh session.  
e Run the `exit` command to leave the Linux shell.

## Example configuration files

This section contains example configuration files for a Firewall Enterprise active-standby DBHA configuration.

### See also

[Dual-Box High Availability deployment example](#) on page 16

## Chassis A

```
#
system-identifier 249
#
```

```
remote-box 246 192.168.69.245 192.168.69.246 100.100.100.2 100.100.100.4 1.1.246.20
#
#
vap-group mfw xsve
  vap-count 2
  max-load-count 2
  backup-mode group
  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
  master-failover-trigger application
  flow-proxy
  ip-flow-rule LoadBalance
    action load-balance
    incoming-circuit-group any
    activate
  ip-flow-rule sync
    action broadcast
    priority 30
    incoming-circuit-group 2
    destination-addr 239.255.0.0 239.255.0.255
    activate
#
incoming-circuit-group-name 5 mgmt
incoming-circuit-group-name 2 sync
incoming-circuit-group-name 3 internal
incoming-circuit-group-name 4 out
#
circuit gig1 circuit-id 1025
  device-name gig1
  incoming-circuit-group 3
  vap-group mfw
circuit gig2 circuit-id 1026
  device-name gig2
  incoming-circuit-group 4
  vap-group mfw
circuit mngFW circuit-id 1027
  device-name mngFW
  incoming-circuit-group 5
  vap-group mfw
  ip 192.168.69.225/24 192.168.69.255 increment-per-vap 192.168.69.233
circuit sync circuit-id 1031
  device-name sync
  incoming-circuit-group 2
  link-state-resistant
  vap-group mfw
  ip 193.0.0.1/24 193.0.0.255 increment-per-vap 193.0.0.10
#
interface ethernet 1/1
  logical gig1
  circuit gig1
interface ethernet 1/2
  logical gig2
  circuit gig2
interface ethernet 2/7
  logical mngFW
  circuit mngFW
interface ethernet 2/8
  logical sync
  circuit sync
#
vrrp failover-group odin failover-group-id 1
  virtual-router vrrp-id 103 circuit mngFW
  priority-delta 2
  vap-group mfw
  virtual-ip 192.168.69.234/24 192.168.69.255
  floating
virtual-router vrrp-id 104 circuit sync
  priority-delta 0
  vap-group mfw
  virtual-ip 193.0.0.100/24 193.0.0.255
  floating
virtual-router vrrp-id 100 circuit gig1
  priority-delta 2
  backup-stay-up
```

```

    vap-group mfw
      ip 192.100.10.100/24 192.100.10.255
virtual-router vrrp-id 101 circuit gig2
  priority-delta 2
  backup-stay-up
  vap-group mfw
    ip 192.101.10.100/24 192.101.10.255
#
vrrp vap-group mfw
  failover-group-list odin
  hold-down-timer 1
  priority-delta 2
#
ip route 192.168.66.0/24 192.168.69.1 vap-group mfw circuit mngFW
ip route 192.168.68.0/24 192.168.69.1 vap-group mfw circuit mngFW
ip route 192.168.71.0/24 192.168.69.1 vap-group mfw circuit mngFW
ip route 10.0.0.0/8 192.168.69.1 vap-group mfw circuit mngFW
#

```

## Chassis B

```

#
system-identifier 246
#
remote-box 249 192.168.69.248 192.168.69.249 100.100.100.1 1.1.249.20
#
access-list 1 permit ip source-ip 0.0.0.0 255.255.255.255 destination-ip 0.0.0.0
255.255.255.255
#
#
vap-group fw xsve
  vap-count 3
  max-load-count 2
  backup-mode group
  ap-list ap1 ap2 ap3 ap4 ap5 ap6 ap7 ap8 ap9 ap10
  load-balance-vap-list 3 4 5 6 7 8 9 10 2 1
  master-failover-trigger application
  flow-proxy
  ip-flow-rule LoadBalance
    action load-balance
    incoming-circuit-group any
    activate
  ip-flow-rule sync
    action broadcast
    priority 30
    incoming-circuit-group 2
    destination-addr 239.255.0.0 239.255.0.255
    activate
#
incoming-circuit-group-name 2 sync
incoming-circuit-group-name 3 internal
incoming-circuit-group-name 4 out
incoming-circuit-group-name 5 mgmt
#
circuit gig1 circuit-id 1025
  device-name gig1
  incoming-circuit-group 3
  vap-group fw
circuit gig2 circuit-id 1026
  device-name gig2
  incoming-circuit-group 4
  vap-group fw
circuit sync circuit-id 1030
  device-name sync
  incoming-circuit-group 2
  link-state-resistant
  vap-group fw
    ip 193.0.0.11/24 193.0.0.255 increment-per-vap 193.0.0.14
circuit mngFW circuit-id 1031
  device-name mngFW
  incoming-circuit-group 5

```



```
vap-group fw
  ip 192.168.69.222/24 192.168.69.255 increment-per-vap 192.168.69.224
#
interface ethernet 1/3
  logical gig1
  circuit gig1
interface ethernet 1/4
  logical gig2
  circuit gig2
interface ethernet 2/9
  logical sync
  circuit sync
interface ethernet 2/10
  logical mngFW
  circuit mngFW
#
vrrp failover-group odin failover-group-id 1
  priority 101
  virtual-router vrrp-id 100 circuit gig1
    priority-delta 2
    backup-stay-up
    vap-group fw
      ip 192.100.10.100/24 192.100.10.255
  virtual-router vrrp-id 101 circuit gig2
    priority-delta 2
    backup-stay-up
    vap-group fw
      ip 192.101.10.100/24 192.101.10.255
  virtual-router vrrp-id 103 circuit mngFW
    priority-delta 2
    vap-group fw
      virtual-ip 192.168.69.234/24 192.168.69.255
      floating
  virtual-router vrrp-id 104 circuit sync
    priority-delta 0
    vap-group fw
      virtual-ip 193.0.0.100/24 193.0.0.255
      floating
#
vrrp vap-group fw
  failover-group-list odin
  hold-down-timer 10
  priority-delta 2
#
ip route 192.168.68.0/24 192.168.69.1 vap-group fw circuit mngFW
ip route 10.0.0.0/8 192.168.69.1 vap-group fw circuit mngFW
ip route 192.168.71.0/24 192.168.69.1 vap-group fw circuit mngFW
#
```



# Management and integration

- 
- Chapter 7 *Control Center registration*
  - Chapter 8 *Network integration*
  - Chapter 9 *Dynamic routing configuration*
  - Chapter 10 *VPN creation*



# 7

## Control Center registration

You can manage your Firewall Enterprise VAP group with a Control Center Management Server.

### Contents

- ▶ *Managing your firewall VAP group*
- ▶ *Register the Firewall Enterprise VAP group to the Control Center*
- ▶ *Configure audit archiving to Control Center*
- ▶ *Validate and apply policy to the Firewall Enterprise VAP group*

---

## Managing your firewall VAP group

To manage your Firewall Enterprise VAP group with your Control Center Management Server, you must complete several tasks.

- Register the firewall VAP group with the Control Center Management Server.
- Configure the firewall VAP group to archive audit data to the Control Center Management Server.
- Validate and apply policy from the Control Center Management Server to the firewall VAP group.



Before you perform the tasks described in this chapter, you must set up your Control Center Management Server as described in the *McAfee Firewall Enterprise Control Center Quick Start Guide*.

---

## Register the Firewall Enterprise VAP group to the Control Center

Perform this task from your Control Center client computer.

### Task

- 1 Use the Control Center Client application to connect to your Control Center Management Server.
- 2 In the navigation bar, click **Policy**.
- 3 In the **Policy** tree, right-click **Clusters**, then select **Add Object**. The **Add New Cluster Wizard** appears.
- 4 Specify the attributes of your Firewall Enterprise VAP group.
  - a In the **Cluster name** field, type a name for the Firewall Enterprise VAP group.
  - b In the **Cluster management address** field, type the floating IP address that you added to the management circuit.
  - c From the **Version** drop-down list, select the firewall version.
  - d Click **Next**. The **Firewall Registration** page appears.

- 5 Specify registration credentials for your Firewall Enterprise VAP group.
  - a Select **Register the firewall with this Management Server**.
  - b In the **SSH username** field, type the name of the firewall administrator you created when you installed the firewall.
  - c In the **Password** field, type the password for the firewall administrator account.
  - d Click **Next**. The **Summary** page appears.
- 6 Review the summary.
  - To modify the configuration, click **Back**.
  - To continue, click **Register**.

The Control Center Management Server contacts your Firewall Enterprise VAP group. When the operation is complete, a registration complete message appears.
- 7 Click **Next**. The **Retrieval of the Firewall into Control Center** page appears.
- 8 Confirm that all items in the **Retrieval Items** list are selected, then click **Finish**. A pop-up window appears.
- 9 Click **OK**. The Control Center Management Server retrieves policy from the Firewall Enterprise VAP group.

After registration is complete, the Firewall Enterprise VAP group appears under the **Clusters** node in the **Policy** tree.

---

## Configure audit archiving to Control Center

Because disk space is limited on the X-Series Platform, McAfee recommends configuring the firewall VAP group to automatically archive audit data to the Control Center Management Server.

### Unlock the FTP user account

Use the Control Center command line interface to unlock the FTP user account.

#### Task

- 1 Obtain command line access to the Control Center Management Server using one of these methods:
  - Connect to the Control Center Management Server using SSH.
  - Use the system console.
- 2 Log on using the mgradmin account. The following prompt is displayed:

```
[ mgradmin@cchostname ~]$
```

- 3 Run the following command to switch to the SSO account:

```
su - sso
```

- 4 Type the SSO account password.

- 5 Run the following command to unlock the FTP account:

```
/usr/sbin/cg_usermod -s /bin/bash ftp
```

- 6 [Optional] To specify a new password for the FTP account, run the following command:

```
/usr/sbin/cg_usermod -s /bin/bash -p password ftp
```

- 7 Run the `exit` command to exit the SSO account.

## Create an audit export policy

Create an audit export policy that sends audit data to the Control Center Management Server.

### Task

- 1 In the navigation bar, click **Policy**.
- 2 In the lower left area of the window, click the **Firewall Settings** tab.
- 3 Double-click the **Audit Export** node. The **Audit Export** window appears.
- 4 Configure audit export to the Control Center.
  - a In the **Name** field, type a name that identifies the export location (Control Center).
  - b Select **Export to Control Center**.
  - c In the **Password** and **Confirm Password** fields, specify the password for the Control Center ftp user account.
  - d [Optional] Click the **Frequency** tab to configure how often the audit export takes place. The default is hourly.
  - e Click **OK**.

## Associate the audit export policy with your Firewall Enterprise VAP group

Configure your firewall VAP group to use the audit export policy.

### Task

- 1 In the **Policy** tree, expand the **Clusters** node.
- 2 Right-click the Firewall Enterprise VAP group, then select **Edit Cluster Settings**. The **Cluster** window appears.
- 3 In the navigation tree, click **Offbox**.
- 4 In the **Audit Export** area, select the audit export policy you created from the drop-down list.
- 5 Click **OK**. The **Cluster** window closes.



The audit export policy does not take effect until you apply policy to the firewall VAP group.

---

## Validate and apply policy to the Firewall Enterprise VAP group

Validate the policy on the Control Center Management Server and apply it to the firewall VAP group.

### Task

- 1 Validate the policy retrieved from the firewall VAP group.
  - a In the navigation bar, click **Validate**. The **Validate Configuration** window appears.
  - b In the **Firewalls** list, select your Firewall Enterprise VAP group.
  - c Click **OK**.
    - If any warnings are detected, the **Validation Warnings** window appears. Proceed with the validation process, or cancel and correct the error.
    - If no warnings are detected, the status for the firewall VAP group changes to *Completed* on the **Validation Status** page.
- 2 Apply policy to the firewall VAP group.
  - a Click **Apply**. The **Apply Configuration** window appears.
  - b In the **Firewalls** list, select your Firewall Enterprise VAP group.
  - c Click **OK**. Progress is displayed as the Control Center applies policy to the firewall VAP group. When the policy apply is complete, the **Pending Status** changes to *Completed* on the **Configuration Status** page.

After the policy is applied, you can create new policy on the Control Center Management Server and apply it to the firewall VAP group as needed.



# 8

## Network integration

You can use these instructions to connect your firewall VAP group to an additional network, or to bridge networks.

### Contents

- ▶ [Connect a firewall VAP group to a non-VLAN network](#)
- ▶ [Connect a firewall VAP group to a VLAN network](#)
- ▶ [Bridge two networks](#)

---

## Connect a firewall VAP group to a non-VLAN network

You must perform several tasks to connect your firewall VAP group to an additional network.



If you are connecting a DBHA firewall VAP group to a non-VLAN network, you must perform these tasks on each X-Series Platform.

### Tasks

- [Create incoming circuit groups on page 81](#)  
Incoming circuit groups (ICGs) associate circuits with Firewall Enterprise security zones.
- [Create a circuit on page 82](#)  
Create a circuit to associate the firewall VAP group with the ICG and physical interface.
- [Configure an interface on page 83](#)  
Create the appropriate interface type and associate it with the circuit you created.
- [Create a virtual router for each circuit on page 84](#)  
If you are connecting a DBHA firewall VAP group to a VLAN network, perform this task to create a virtual router for the circuit you created.
- [Save the configuration on page 84](#)  
Save all of the configuration changes you made.

## Create incoming circuit groups

Incoming circuit groups (ICGs) associate circuits with Firewall Enterprise security zones.

- If you want to isolate each VLAN on the network, create an ICG for each VLAN.
- If you want to apply the same security policy to all VLANs on the network, create a single ICG.

**Task**

- 1 Establish a command line interface connection to the X-Series CPM using SSH (recommended) or Telnet.
- 2 Create a new ICG for the network.

```
CBS# configure incoming-circuit-group-name <icg_number> <icg_name>
CBS#
```

**Create a circuit**

Create a circuit to associate the firewall VAP group with the ICG and physical interface.

**Task**

- 1 Create the circuit.

```
CBS# configure circuit <circuit_name>CBS(conf-cct)#
```

- 2 Assign a device name to the circuit.



The device name is used as the Firewall Enterprise interface name. To avoid confusion, the device name should be the same as, or based on, the circuit name.

```
CBS(conf-cct)# device-name <circuit_device_name>
```

- 3 Assign the appropriate ICG to the circuit.

```
CBS(conf-cct)# incoming-circuit-group <number_of_ICG>
```

- 4 Assign the Firewall Enterprise VAP group to the circuit.

```
CBS(conf-cct)# vap-group <VAP_group_name>
CBS(conf-cct-vapgroup)#
```

- 5 [Single chassis only] Configure an IPv4 or IPv6 address for the circuit.



If you intend to combine IPv4 and IPv6 addresses on the circuit, the first address you specify must be IPv4.

```
CBS(conf-cct-vapgroup)# ip <IP_address/mask>
CBS(conf-cct-vapgroup-ip)#
```

- 6 [Optional, single chassis only] Configure an alias IPv4 or IPv6 address for the circuit.

```
CBS(conf-cct-vapgroup-ip)# alias <alias_IP_address/mask>
CBS(conf-cct-vapgroup-alias)# end
CBS#
```



Repeat this step as necessary to configure additional alias IP addresses.

## Configure an interface

Create the appropriate interface type and associate it with the circuit you created.

### Tasks

- [Create a single physical interface on page 83](#)  
You can create a non-VLAN interface.
- [Create a multi-link group interface on page 83](#)  
You must perform several steps to create a multi-link group interface.

### Create a single physical interface

You can create a non-VLAN interface.

#### Task

- 1 Configure a physical interface.

```
CBS# configure interface ethernet <slot/port>
CBS(conf-intf-ether)#
```

- 2 Create a logical interface and associate it with the circuit.

```
CBS(conf-intf-ether)# logical <logical_name> circuit <circuit_name>
CBS(intf-ether-log-cct)# end
CBS#
```

### Create a multi-link group interface

You must perform several steps to create a multi-link group interface.

#### Task

- 1 Create the group interface.

```
CBS# configure group-interface <group_interface_name>
CBS(conf-group-intf)#
```

- 2 Configure the interface type and return to the interface configuration context.

```
CBS(conf-group-intf)# interface-type ethernet
CBS(conf-grp-intf-ether)# exit
CBS(conf-group-intf)#
```

- 3 Define the interface mode as multi-link and associate it with the circuit.

```
CBS(conf-group-intf)# mode multi-link circuit <circuit_name>
```

- 4 Assign physical interfaces to the group interface and exit the configuration mode.

- a For each physical interface you want to associate with the group interface, specify the interface you want.

```
CBS(conf-group-intf)# interface <slot/port>
CBS(conf-grp-intf-intf)# exit
CBS(conf-group-intf)#
```

- b When you are finished, run the command `end` to return to the main command line interface context.

## Create a virtual router for each circuit

If you are connecting a DBHA firewall VAP group to a VLAN network, perform this task to create a virtual router for the circuit you created.

### Task

- 1 Add the virtual router to the failover group.

```
CBS# configure vrrp failover-group <failover_group_name> failover-group-id <1-255>
CBS(conf-vrrp-group) #
```

- 2 Create a virtual router, assign it an ID, and attach it to the circuit.

```
CBS(conf-vrrp-group) # virtual-router vrrp-id <1-4096> circuit <circuit_name>
CBS(conf-vrrp-failover-vr) #
```

- 3 Assign a priority-delta value to the virtual router.

When a virtual router fails, the associated failover group's priority value is decremented by the priority-delta value. The priorities of the failover groups on the two chassis are compared; if the priority of the master failover group has a lower priority than the standby failover group, the standby chassis becomes the master. The priority-delta value is added back to the priority when the VR recovers.

```
CBS(conf-vrrp-failover-vr) # priority-delta <1-255>
CBS(conf-vrrp-failover-vr) #
```

- 4 Enable the backup-stay-up option to keep the virtual router circuit interface up when the failover group is in backup mode.

```
CBS(conf-vrrp-failover-vr) # backup-stay-up
CBS(conf-vrrp-failover-vr) #
```

- 5 Assign the virtual router to the Firewall Enterprise VAP group.

```
CBS(conf-vrrp-failover-vr) # vap-group<uicontrol>
CBS(conf-vrrp-vr-vapgroup) #
```

- 6 Assign an IP address to the virtual router.

```
CBS(conf-vrrp-vr-vapgroup) # ip <IP/netmask>
CBS(conf-vrrp-vr-vapgroup) #
```

- 7 Run the exit command until you return to the CBS# prompt.

## Save the configuration

Save all of the configuration changes you made.

```
CBS# wr

Saving configuration ... Please be patient...
CBS#
```

After a few minutes, the corresponding VAP group interface(s) and zone(s) appear in the Control Center Management Server.

## Connect a firewall VAP group to a VLAN network

Perform several tasks to connect your firewall VAP group to an additional network.



If you are connecting a DBHA firewall VAP group to a VLAN network, you must perform these tasks on each X-Series Platform.

### Tasks

- [Create incoming circuit groups on page 85](#)  
Incoming circuit groups (ICGs) associate circuits with Firewall Enterprise security zones.
- [Create a circuit for each VLAN on page 85](#)  
You must perform several steps for each circuit you need to configure.
- [Configure an interface on page 86](#)  
Create the appropriate VLAN interface type and associate it with the circuit you created.
- [Create a virtual router for each circuit on page 87](#)  
If you are connecting a DBHA firewall VAP group to a VLAN network, perform this task to create a virtual router for the circuit you created.
- [Save the configuration on page 88](#)  
Save all of the configuration changes you made.

## Create incoming circuit groups

Incoming circuit groups (ICGs) associate circuits with Firewall Enterprise security zones.

- If you want to isolate each VLAN on the network, create an ICG for each VLAN.
- If you want to apply the same security policy to all VLANs on the network, create a single ICG.

### Task

- 1 Establish a command line interface connection to the X-Series CPM using SSH (recommended) or Telnet.
- 2 Create a new ICG for the network.

```
CBS# configure incoming-circuit-group-name <icg_number> <icg_name>
CBS#
```

## Create a circuit for each VLAN

You must perform several steps for each circuit you need to configure.

### Task

- 1 Create the circuit.

```
CBS# configure circuit <circuit_name>
CBS(conf-cct)#
```

- 2 Assign a device name to the circuit.



The device name is used as the Firewall Enterprise interface name. To avoid confusion, the device name should be the same as, or based on, the circuit name.

```
CBS(conf-cct)# device-name <circuit_device_name>
```

- 3 Assign the appropriate ICG to the circuit.

```
CBS(conf-cct)# incoming-circuit-group <number_of_ICG>
```

#### 4 Assign the Firewall Enterprise VAP group to the circuit.

```
CBS(conf-cct)# vap-group <VAP_group_name>
CBS(conf-cct-vapgroup)#
```

#### 5 Specify the VLAN ID.

```
CBS(conf-cct-vapgroup)# default-egress-vlan-tag <VLAN_ID>
CBS(conf-cct-vapgroup)#
```

#### 6 [Single chassis only] Configure an IPv4 or IPv6 address for the circuit.



If you intend to combine IPv4 and IPv6 addresses on the circuit, the first address you specify must be IPv4.

```
CBS(conf-cct-vapgroup)# ip <IP_address/mask>
CBS#
```

#### 7 [Optional, single chassis only] Configure an alias IPv4 or IPv6 address for the circuit.

```
CBS(conf-cct-vapgroup-ip)# alias <alias_IP_address/mask>
CBS(conf-cct-vapgroup-alias)# end
CBS#
```



Repeat this step as necessary to configure additional alias IP addresses.

## Configure an interface

Create the appropriate VLAN interface type and associate it with the circuit you created.

### Tasks

- [Create a single physical interface with VLANs on page 86](#)  
You must perform these steps to create a VLAN interface.
- [Create a multi-link group interface with VLANs on page 87](#)  
You must perform several steps to create a multi-link group interface.

### Create a single physical interface with VLANs

You must perform these steps to create a VLAN interface.

#### Task

##### 1 Configure a physical interface.

```
CBS# configure interface ethernet <slot/port>
CBS(conf-intf-ether)#
```

##### 2 For each VLAN that you want to create, create a logical interface for the VLAN and associate it with the appropriate circuit.

```
CBS(conf-intf-ether)# logical <logical_name> ingress-vlan-tag <VLAN_ID> circuit
<circuit_name>
CBS(intf-ether-log-cct)# exit
CBS(conf-intf-ether)#
```

## Create a multi-link group interface with VLANs

You must perform several steps to create a multi-link group interface.

### Task

- 1 Create a circuit for non-VLAN traffic and associate it with the firewall VAP group.

```
CBS# configure circuit <circuit_name> vap-group <VAP_group_name>
CBS(conf-cct-vapgroup)# end
CBS(conf-cct)#
```

- 2 Create the group interface.

```
CBS# configure group-interface <group_interface_name>
CBS(conf-group-intf)#
```

- 3 Configure the interface type and return to the interface configuration context.

```
CBS(conf-group-intf)# interface-type ethernet
CBS(conf-grp-intf-ether)# exit
CBS(conf-group-intf)#
```

- 4 Define the interface mode as multi-link and associate it with the non-VLAN circuit you created in step 1.

```
CBS(conf-group-intf)# mode multi-link circuit <circuit_name>
CBS(conf-group-intf)#
```

- 5 Assign physical interfaces to the group interface and exit the configuration mode. Specify each physical interface you want to associate with the group interface.

```
CBS(conf-group-intf)# interface <slot/port>
CBS(conf-grp-intf-intf)# exit
CBS(conf-group-intf)#
```

- 6 For each VLAN that you want to create:

- a Create a logical interface for the VLAN and associate it with the multi-link group interface.

```
CBS(conf-group-intf)# logical <logical_name> ingress-vlan-tag <VLAN_ID> circuit
<circuit_name>
CBS(conf-group-intf-cct)# exit
CBS(conf-group-intf)#
```

- b When you are finished, run the command `end` to return to the main command line interface context.

## Create a virtual router for each circuit

If you are connecting a DBHA firewall VAP group to a VLAN network, perform this task to create a virtual router for the circuit you created.

### Task

- 1 Add the virtual router to the failover group.

```
CBS# configure vrrp failover-group <failover_group_name> failover-group-id <1-255>
CBS(conf-vrrp-group)#
```

- 2 Create a virtual router, assign it an ID, and attach it to the circuit.

```
CBS(conf-vrrp-group)# virtual-router vrrp-id <1-4096> circuit <circuit_name>
CBS(conf-vrrp-failover-vr)#
```

- 3 Assign a priority-delta value to the virtual router.

When a virtual router fails, the associated failover group's priority value is decremented by the priority-delta value. The priorities of the failover groups on the two chassis are compared; if the priority of the master failover group has a lower priority than the standby failover group, the standby chassis becomes the master. The priority-delta value is added back to the priority when the VR recovers.

```
CBS(conf-vrrp-failover-vr)# priority-delta <1-255>
CBS(conf-vrrp-failover-vr)#
```

- 4 Enable the backup-stay-up option to keep the virtual router circuit interface up when the failover group is in backup mode.

```
CBS(conf-vrrp-failover-vr)# backup-stay-up
CBS(conf-vrrp-failover-vr)#
```

- 5 Assign the virtual router to the Firewall Enterprise VAP group.

```
CBS(conf-vrrp-failover-vr)# vap-group<uicontrol>
CBS(conf-vrrp-vr-vapgroup)#
```

- 6 Assign an IP address to the virtual router.

```
CBS(conf-vrrp-vr-vapgroup)# ip <IP/netmask>
CBS(conf-vrrp-vr-vapgroup)#
```

- 7 Run the exit command until you return to the CBS# prompt.

## Save the configuration

Save all of the configuration changes you made.

```
CBS# wr

Saving configuration ... Please be patient...
CBS#
```

After a few minutes, the corresponding VAP group interface(s) and zone(s) appear in the Control Center Management Server.

## Bridge two networks

When you bridge two network segments, a transparent interface is created on the firewall.



The firewall supports only one configured transparent interface (bridge) at a time. If a transparent interface is configured, additional traffic interfaces are not supported.

Perform the following steps to bridge two networks.



## Tasks

- [Create incoming circuit groups for bridged networks on page 89](#)  
Create an ICG for each network that will be bridged to represent the Firewall Enterprise security zone that will contain the network.
- [Create circuits for bridged networks on page 89](#)  
Create three circuits: one circuit for the bridge and an additional circuit for each network segment that will be bridged.
- [Configure interfaces on page 90](#)  
Create the appropriate interface type for each network circuit in the bridge.
- [Create the bridge on page 91](#)  
Bridge the circuits together.
- [Save the configuration on page 92](#)  
Save all of the configuration changes you made.

## Create incoming circuit groups for bridged networks

Create an ICG for each network that will be bridged to represent the Firewall Enterprise security zone that will contain the network.

### Task

- 1 Establish a command line interface connection to the X-Series CPM using SSH (recommended) or Telnet.
- 2 Create an ICG for the first network.

```
CBS# configure incoming-circuit-group-name <icg_number> <icg_name>
CBS#
```

- 3 Create an ICG for the second network.

```
CBS# configure incoming-circuit-group-name <icg_number> <icg_name>
CBS#
```

## Create circuits for bridged networks

Create three circuits: one circuit for the bridge and an additional circuit for each network segment that will be bridged.

### Task

- 1 Create a template circuit for the bridge.
  - a Define the circuit.

```
CBS# configure circuit <template_circuit_name>
CBS (conf-cct) #
```

- b Configure a device name for the bridge circuit.

```
CBS (conf-cct) # device-name <circuit_device_name>
CBS (conf-cct) #
```

- c Assign the Firewall Enterprise VAP group to the bridge circuit.

```
CBS (conf-cct) # vap-group <VAP_group_name>
CBS (conf-cct-vapgroup) #
```

- d Configure an IPv4 or IPv6 address for the bridge circuit.

```
CBS(conf-cct-vapgroup)# ip <IP_address/mask>
CBS(conf-cct-vapgroup-ip)# end
CBS#
```

- 2 Create a circuit for the each network segment.

- a Create the circuit.

```
CBS# configure circuit <circuit_name1>
CBS(conf-cct)#
```

- b Assign a device name to the circuit.

```
CBS(conf-cct)# device-name <circuit_device_name>
```

- c Assign the appropriate ICG to the circuit.

```
CBS(conf-cct)# incoming-circuit-group <number_of_ICG>
```

- d Assign the Firewall Enterprise VAP group to the circuit.

```
CBS(conf-cct)# vap-group <VAP_group_name>
CBS(conf-cct-vapgroup)#
```

- e [VLAN only] Specify the VLAN ID.

```
CBS(conf-cct-vapgroup)# default-egress-vlan-tag <VLAN_ID>
```



A bridge supports a single VLAN ID.

- f Enable promiscuous mode.

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

## Configure interfaces

Create the appropriate interface type for each network circuit in the bridge.



Do not configure an interface for the bridge circuit.

### Tasks

- [Create a single physical interface on page 90](#)  
You must perform several steps to create a single interface.
- [Create a multi-link group interface on page 91](#)  
You must perform several steps to create a multi-link group interface.

### Create a single physical interface

You must perform several steps to create a single interface.

#### Task

- 1 Configure a physical interface.

```
CBS# configure interface ethernet <slot/port>
CBS(conf-intf-ether)#
```

2 Create a logical interface and associate it with the circuit.

- **Non-VLAN interface** — Run the following commands.

```
CBS(conf-intf-ether)# logical <logical_name> circuit <circuit_name>
CBS(intf-ether-log-all-cct)# end
CBS#
```

- **VLAN interface** — Run the following commands.

```
CBS(conf-intf-ether)# logical <logical_name> ingress-vlan-tag <VLAN_ID> circuit
<circuit_name>
CBS(intf-ether-log-all-cct)# end
CBS#
```

## Create a multi-link group interface

You must perform several steps to create a multi-link group interface.

### Task

1 Create the group interface.

```
CBS# configure group-interface <group_interface_name>
CBS(conf-group-intf)#
```

2 Configure the interface type and return to the interface configuration context.

```
CBS(conf-group-intf)# interface-type ethernet
CBS(conf-grp-intf-ether)# exit
CBS(conf-group-intf)#
```

3 Define the interface mode as multi-link and associate it with the circuit.

```
CBS(conf-group-intf)# mode multi-link circuit <circuit_name>
```

4 Assign physical interfaces to the group interface and exit the configuration mode.

- a For each physical interface you want to associate with the group interface, specify the interface you want.

```
CBS(conf-group-intf)# interface <slot/port>
CBS(conf-grp-intf-intf)# exit
CBS(conf-group-intf)#
```

- b When you are finished, run the command `end` to return to the main command line interface context.

## Create the bridge

Bridge the circuits together.

### Task

1 Create the bridge and associate it with the template circuit.

```
CBS# configure bridge-mode <template_circuit_name>
CBS(conf-bridge-mode)#
```

2 Specify the first network circuit.

```
CBS(conf-bridge-mode)# circuit <circuit1>
CBS(conf-bridge-mode)#
```

### 3 Specify the second network circuit

```
CBS(conf-bridge-mode)# circuit <ircuit2>
CBS(conf-bridge-mode)# end
CBS#
```

## Save the configuration

Save all of the configuration changes you made.

```
CBS# wr

Saving configuration ... Please be patient...
CBS#
```

After a few minutes, the corresponding VAP group interface(s) and zone(s) appear in the Control Center Management Server.

# 9

## Dynamic routing configuration

You need to configure the firewall to enable dynamic routing on Crossbeam X-Series Platform.

### Contents

- ▶ *How dynamic routing on Crossbeam X-Series Platforms works*
- ▶ *Requirements for dynamic routing*
- ▶ *Enable dynamic routing on Firewall Enterprise on Crossbeam X-Series Platforms*

### How dynamic routing on Crossbeam X-Series Platforms works

On the Crossbeam X-Series Platform, the XOS circuit connects with dynamic routing agent peers, and all dynamic routing agent protocol traffic is directed to the master VAP.

The master VAP runs the Firewall Enterprise application, which controls the dynamic routing agent and agent configuration. The master VAP synchronizes the routes across all VAPs in the VAP group.

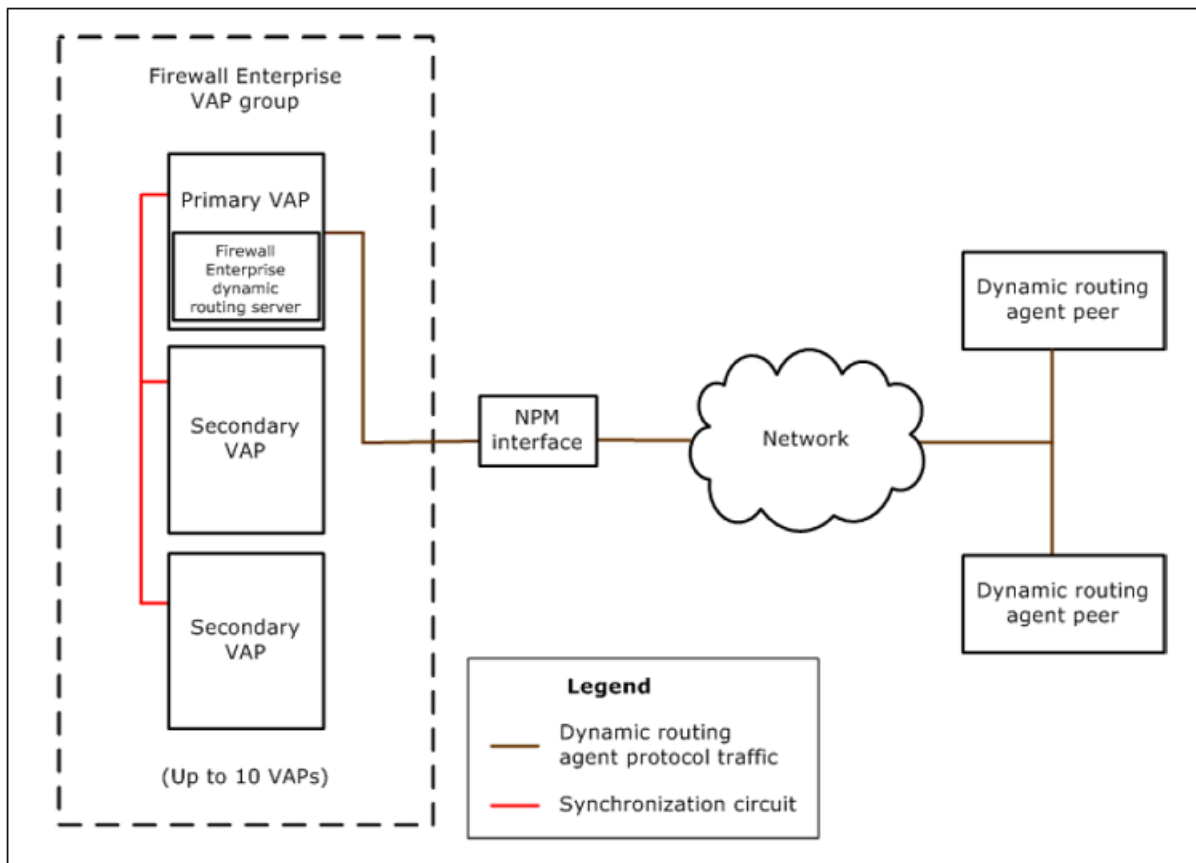


Figure 9-1 Dynamic routing traffic flow

## Requirements for dynamic routing

To enable dynamic routing on your Firewall Enterprise on Crossbeam X-Series Platform, several requirements must be met.

- The firewall must appear as a single host to any dynamic routing agent peers. The XOS circuit that connects with dynamic routing agent peers must be configured with either a shared IP address for the VAP group or a floating IP address.
- The VAP group must be configured to redirect all dynamic routing agent protocol traffic to the master VAP.



The dynamic routing protocols supported on Firewall Enterprise on Crossbeam X-Series Platform are BGP, BGP IPv6, OSPF, OSPF IPv6, and RIP. Multicast dynamic routing using the PIM-SM protocol is not supported.

## Enable dynamic routing on Firewall Enterprise on Crossbeam X-Series Platforms

Using dynamic routing on Firewall Enterprise on Crossbeam X-Series Platforms requires configuration on the XOS command line interface and the Firewall Enterprise Control Center Client application.

To enable dynamic routing on Firewall Enterprise on Crossbeam X-Series Platforms, you must complete several tasks.

### Tasks

- [Configure VAP group interfaces for dynamic routing on page 94](#)  
For each circuit that the Firewall Enterprise VAP group will use for dynamic routing, configure the circuit to use a shared IP address for the VAP group or configure a floating IP address.
- [Configure IP flow rules for dynamic routing agent protocol traffic on page 95](#)  
Dynamic routing servers run only on the master VAP within a VAP group. Configure IP flow rules for each routing protocol in use to ensure delivery of the dynamic routing agent protocol traffic to the master VAP.
- [Enable and configure dynamic routing on Firewall Enterprise on page 96](#)  
Enable and configure dynamic routing on Firewall Enterprise using the Control Center Client application.

## Configure VAP group interfaces for dynamic routing

For each circuit that the Firewall Enterprise VAP group will use for dynamic routing, configure the circuit to use a shared IP address for the VAP group or configure a floating IP address.

### Task

- 1 At the XOS command prompt, switch to the `conf-cct-vapgroup` context for the circuit.

```
CBS# configure circuit <circuit_name>
CBS(conf-cct)# vap-group <VAP_group_name>
CBS(conf-cct-vapgroup)#
```

- 2 Configure a shared IP address or floating IP address for the circuit.

- To assign a shared IP address:

```
CBS(conf-cct-vapgroup)# ip <IP_address>/<mask>
CBS(conf-cct-vapgroup-ip)# end
```

- To assign a shared IP address along with a unique address for each cluster member (VAP):

```
CBS(conf-cct-vapgroup)# ip <IP_address_in_range>/<mask> increment-per-vap
<last_IP_address_in_range>
CBS(conf-cct-vapgroup-ip)# alias <shared_IP_address>/<mask>
CBS(conf-cct-vapgroup-alias)# end
```

- To assign a floating IP address owned by the master VAP:

```
CBS(conf-cct-vapgroup)# ip <IP_address>/<mask>
CBS(conf-cct-vapgroup-ip)# alias <alias_IP_address>/<mask>
CBS(conf-cct-vapgroup-alias)# floating
CBS(conf-cct-vapgroup-alias)# end
```

## Configure IP flow rules for dynamic routing agent protocol traffic

Dynamic routing servers run only on the master VAP within a VAP group. Configure IP flow rules for each routing protocol in use to ensure delivery of the dynamic routing agent protocol traffic to the master VAP.

### Task

- 1 At the XOS command prompt, switch to the `config-vap-grp` context for the VAP group.

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

- 2 Add an IP flow rule for each dynamic routing protocol.

```
CBS(config-vap-grp)# ip-flow-rule <rule_name>
CBS(ip-flow-rule)# action pass-to-master
CBS(ip-flow-rule)# incoming-circuit-group any
CBS(ip-flow-rule)# destination-port <start_port_#> <end_port_#>
CBS(ip-flow-rule)# protocol <start_proto_#> <end_proto_#>
CBS(ip-flow-rule)# activate
```

The default protocols and ports for each dynamic routing protocol are:



- **RIP** — UDP protocol 17 on port 520
- **OSPF** — Protocol 89
- **BGP** — TCP protocol 6 on port 179

Example IP flow rule for RIP:

```
ip-flow-rule rip_rule
action pass-to-master
priority 25
incoming-circuit-group any
destination-port 520 520
protocol 17 17
activate
```



For information about configuring IP flow rules for IPv6 traffic, when using XOS version 10.0 or later configured for Series-9 operating mode, see the XOS release notes.

## Enable and configure dynamic routing on Firewall Enterprise

Enable and configure dynamic routing on Firewall Enterprise using the Control Center Client application.

The high-level steps to set up dynamic routing are:

### Task

- 1 Configure rules to enable the dynamic routing servers and to allow dynamic routing agent protocol traffic to reach the servers.
- 2 Configure the dynamic routing server network information and processing options. The dynamic routing server configuration files must reflect the networks and interfaces of the VAP group.

For detailed instructions, see also:

- *McAfee Firewall Enterprise Product Guide, Routing* chapter
- *McAfee Firewall Enterprise Control Center Product Guide, Firewalls* chapter



# 10 VPN creation

You must create a VPN on your Firewall Enterprise VAP group to connect to a remote peer.

## Contents

- ▶ *Requirements for VPN*
- ▶ *Create a VPN on your Firewall Enterprise VAP group*

---

## Requirements for VPN

To create a VPN on your Firewall Enterprise VAP group, several requirements must be met.

- A floating IP address must be defined for the XOS circuit where the remote VPN peer is located.
- The floating IP address must be used as the local gateway in the VPN definition.
- If the local identity type is the gateway IP address, the floating IP address must be manually specified.



McAfee recommends using IKE v2 for VPNs terminated by a Firewall Enterprise VAP group.

---

## Create a VPN on your Firewall Enterprise VAP group

You must perform several steps to create a VPN.

### Task

- 1 At the XOS command prompt, create a floating IP address for the VPN gateway address.
  - a Switch to the `conf-cct-vapgroup` context for the circuit that will host the VPN gateway address.

```
CBS# configure circuit <circuit_name>
CBS(conf-cct)# vap-group <VAP_group_name>
CBS(conf-cct-vapgroup)#
```

- b Switch to the `config-cct-vapgroup-ip` context.



To reach this context, you must re-specify the IP address for the circuit.

```
CBS(conf-cct-vapgroup)# ip <IP_address/mask>
CBS(config-cct-vapgroup-ip)#
```

**c** Create a floating alias IP address.

```
CBS(config-cct-vapgroup-ip)# alias <alias_ip_address>/<netmask>
CBS(config-cct-vapgroup-alias)# floating
CBS(config-cct-vapgroup-alias)# end
CBS#
```

**d** Save your changes.

```
CBS# wr

Saving configuration ... Please be patient...
CBS#
```

**2** Use the Control Center **VPN Wizard** to create the VPN. Note the following:

- You must specify the floating IP address you configured in step 1 as the gateway IP address for the firewall VAP group.
- If you are using the gateway IP address as the identity of the firewall VAP group, you must manually specify the floating IP address.



Do not use the **Use gateway IP address as identity** option.

# A

## Appendix: Maintenance

Maintain Firewall Enterprise on the Crossbeam X-Series Platform.

### Contents

- ▶ *Manage a firewall VAP group using the XOS command line interface*
- ▶ *Monitor Firewall Enterprise and the X-Series Platform*
- ▶ *Add a VAP to a Firewall Enterprise VAP group*
- ▶ *Remove a VAP from a Firewall Enterprise VAP group*
- ▶ *Uninstall Firewall Enterprise from a VAP group*
- ▶ *Delete a Firewall Enterprise zone*
- ▶ *Upgrade a firewall on a Crossbeam X-Series Platform*

---


## Manage a firewall VAP group using the XOS command line interface

Use the commands in the following table at the XOS command prompt to perform basic management. For more information on using the XOS command line interface to manage applications, see the *Crossbeam XOS Command Reference Guide* and the *Crossbeam XOS Configuration Guide*.

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

- The primary CPM, the NPM(s), and the application VAP group are *Up*.
- The management circuit is configured, and the physical link to the management interface is *Up*.

**Table A-1 Basic VAP group management commands**

Action	Command
Start a Firewall Enterprise VAP group	<pre>CBS# application mfe vap-group &lt;VAP_group_name&gt; start</pre>
Stop a Firewall Enterprise VAP group	<pre>CBS# application mfe vap-group &lt;VAP_group_name&gt; stop</pre> <div data-bbox="932 1619 1511 1682"> The VAP group remains stopped until you start it.</div>
Restart a Firewall Enterprise VAP group	<pre>CBS# application mfe vap-group &lt;VAP_group_name&gt; restart</pre>
Reload a Firewall Enterprise VAP group (restart all APMs in the group)	<pre>CBS# reload vap-group &lt;VAP_group_name&gt;</pre>
Install Firewall Enterprise on any new VAPs you added to the group after initial configuration	<pre>CBS# application-update vap-group &lt;VAP_group_name&gt;</pre>

**Table A-1 Basic VAP group management commands** *(continued)*

Action	Command
Display Firewall Enterprise status on a specified VAP group	CBS# show application vap-group <VAP_group_name>
Configure console settings or restart the firewall VM on individual VAPs	CBS# application mfe vap-group <VAP_group_name> configure

## Monitor Firewall Enterprise and the X-Series Platform

Monitor system health using the Greenlight Element Manager or the XOS command line interface.

### Tasks

- [Monitor using the Greenlight Element Manager on page 100](#)  
Use the Greenlight Element Manager (GEM) to view the components and health of your X-Series Platform.
- [Monitor using the XOS command line interface on page 101](#)  
Use these basic XOS commands for monitoring.

### Monitor using the Greenlight Element Manager

Use the Greenlight Element Manager (GEM) to view the components and health of your X-Series Platform.

GEM is a web application that displays system and component operational information in an easy-to-reference format. GEM provides system monitoring capabilities only; it does not allow you to configure your system.



If GEM is not enabled on your X-Series Platform, run the `configure web-server` command at the XOS command prompt to enable it. For more information, refer to the *Crossbeam XOS Configuration Guide*.



Make sure your client system meets the GEM requirements listed in the *Crossbeam XOS Configuration Guide*.

### Tasks

- [Access GEM from the Control Center Client application on page 100](#)  
Launch GEM from the Control Center Client application.
- [Access GEM from a web browser on page 101](#)  
Navigate to and logon to the Greenlight Element Manager (GEM).

### Access GEM from the Control Center Client application

Launch GEM from the Control Center Client application.

#### Task

- 1 [First time only] If you have not already done so, specify the IP address of the CPM.
  - a In the navigation bar, select **Policy**.
  - b In the **Policy** tree, expand the **Clusters** node.
  - c Right-click the Firewall Enterprise VAP group, then select **Edit Cluster Settings**. The **Cluster** window appears.
  - d In the navigation tree, click **General**.

- e In the **Appliance Address** area, specify the IP address or host name of the CPM.



The Control Center Client application connects to this address when you launch GEM.

- f Click **OK**. The **Cluster** window closes.
- 2 Open GEM from the Control Center Client application.
    - a In the navigation bar, select **Policy**.
    - b In the **Policy** tree, expand the **Clusters** node.
    - c Right-click the Firewall Enterprise VAP group, then select **Launch UI**. A security alert message appears.
    - d Click **Yes** to proceed. The Greenlight Element Manager logon page is displayed within the Client work area.
    - e Specify your user name and password, then click **Login**. The Greenlight Element Manager appears.
    - f When you have finished, click **Sign out**.

### Access GEM from a web browser

Navigate to and logon to the Greenlight Element Manager (GEM).

#### Task

- 1 In a web browser, go to `https://<IP_of_CPM>`. A security alert message appears.
- 2 Click **Yes** to proceed. The Greenlight Element Manager logon page is displayed in the Client work area.
- 3 Specify your user name and password, then click **Login**. The Greenlight Element Manager appears.
- 4 When you have finished, click **Sign out**.

### Monitor using the XOS command line interface

Use these basic XOS commands for monitoring.

For complete information, refer to the *Crossbeam XOS Command Reference Guide*.

**Table A-2 Basic XOS monitoring commands**

Action	Command
Display the number of flows that each NPM has assigned to each VAP and the rates that new and existing flows are assigned	<code>CBS# show flow distribution</code>
Display information on flows passing through the X-Series Platform	<code>CBS# show flow active</code>
Display information about the applications loaded on the CPM	<code>CBS# show application</code>
Display information about the application installed on the specified VAP group	<code>CBS# show application vap-group &lt;VAP_group_name&gt;</code>
Disable application monitoring for the specified VAP group	<code>CBS# configure vap-group &lt;VAP_group_name&gt; no application-monitor</code>
Enable application monitoring for the specified VAP group	<code>CBS# configure vap-group &lt;VAP_group_name&gt; application-monitor</code>

## Add a VAP to a Firewall Enterprise VAP group

Add a VAP to an already configured VAP group.

### Tasks

- [Prepare for installation on page 102](#)  
Before you add a VAP to a Firewall Enterprise VAP group, install an APM and make the necessary modifications to the management and synchronization circuits.
- [Install Firewall Enterprise on a new VAP on page 102](#)  
Use the following commands to install Firewall Enterprise on a new VAP.
- [Verify installation on page 103](#)  
After the VAP reboot is complete, verify that Firewall Enterprise correctly installed, then add it back into to the load balance list.

### Prepare for installation

Before you add a VAP to a Firewall Enterprise VAP group, install an APM and make the necessary modifications to the management and synchronization circuits.

#### Task

- 1 Acquire and install an APM.



Make sure that the new APM meets the requirements listed in X-Series Platform requirements. The hardware configuration of the new APM must match the hardware configuration of all other APMs in the VAP group.

- 2 If necessary, increment the IP address range for the management circuit.

```
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-ip)# end
CBS#
```

- 3 If necessary, increment the IP address range for the synchronization circuit.

```
CBS# configure circuit <synchronization_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-ip)# end
CBS#
```

### Install Firewall Enterprise on a new VAP

Use the following commands to install Firewall Enterprise on a new VAP.

#### Task

- 1 Reconfigure the APM list for the VAP group to add the new APM to the group.

```
CBS# configure vap-group <VAP_group_name>
CBS(config-vap-grp)# ap-list <apm_module_name1> [<apm_module_name2>]
[<apm_module_name3>] ...
```

where `<apm_module_nameN>` is the name XOS assigned to the APM (example: ap3 or ap4).



To determine the assigned names of the APMs in your chassis, exit the config-vap-grp context, then run the show chassis command.

**2** Increment the VAP count of the Firewall Enterprise VAP group.

```
CBS(config-vap-grp)# vap-count <new_VAP_count>
Are you sure you want to adjust vap-count to <new_VAP_count>? <Y or N> [Y]: y

Adjusting vap-count. May take several minutes...
CBS(config-vap-grp)#
```

**3** Set the max load count to the number of active VAP members.

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

**4** Configure the VAP group load-balance VAP list so the new VAP does not receive any flows.

The new APM has 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>[<index3>] ...
CBS(config-vap-grp)# end
CBS#
```

**5** Verify that the status of the VAP is Up and note the slot number.

```
CBS# show ap-vap-mapping
```

**6** Install Firewall Enterprise on the new VAP.

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

**7** Reboot the new VAP so the installation can take effect.

```
CBS# reload module <VAP_slot_number>
```

## Verify installation

After the VAP reboot is complete, verify that Firewall Enterprise correctly installed, then add it back into to the load balance list.

### Task

**1** Verify that Firewall Enterprise is running on the new VAP.

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

The App State for each VAP group member should be *Up*.

**2** Add the new VAP back into the load-balance VAP list.

```
CBS# configure vap-group <VAP_group_name>
CBS(config-vap-grp)# load-balance-vap-list <index1> <index2> [<index3>] ...
CBS(config-vap-grp)# end
```

After a few minutes, the new VAP appears in the Control Center Management Server as part of the Firewall Enterprise VAP group.

## Remove a VAP from a Firewall Enterprise VAP group

Remove the VAP using the XOS command line interface, then delete the VAP from the Control Center Management Server.

### Tasks

- [Remove the VAP from the VAP group on page 104](#)  
Use the XOS command line interface to remove the VAP from the Firewall Enterprise VAP group.
- [Delete the VAP from your Control Center Management Server on page 105](#)  
After you remove the VAP using the XOS command line interface, delete it from your Control Center Management Server.

## Remove the VAP from the VAP group

Use the XOS command line interface to remove the VAP from the Firewall Enterprise VAP group.

### Task

- 1 Remove the VAP from the load-balance VAP list so it no longer receives new flows.



You can remove only 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> [<index3>] ...
```

- 2 Reconfigure the APM list for the VAP group; list the APMs that you want to keep and omit the APM that you want to remove.

```
CBS(config-vap-grp)# ap-list <apm_module_name1> [<apm_module_name2>]
 [<apm_module_name3>] ...
```

where `<apm_module_nameN>` 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.

- 3 Decrement the VAP count of the Firewall Enterprise VAP group.

```
CBS(config-vap-grp)# vap-count <new_VAP_count>
Are you sure you want to adjust vap-count to <new_VAP_count>? <Y or N> [Y]: y

Adjusting vap-count. May take several minutes...
CBS(config-vap-grp)# end
CBS#
```

- 4 [Optional] Reconfigure the management and synchronization circuits to reclaim the IP addresses of the VAP you removed.

```
CBS# configure circuit <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-ip)# end
CBS#
```



## Delete the VAP from your Control Center Management Server

After you remove the VAP using the XOS command line interface, delete it from your Control Center Management Server.

### Task

- 1 Use the Control Center Client application to connect to your Control Center Management Server.
- 2 In the **Policy** tree, expand the **Clusters** node.
- 3 Expand the Firewall Enterprise VAP group.
- 4 Delete the cluster member (VAP) you removed from the VAP group.
  - a Right-click the appropriate cluster member (VAP), then select **Remove Object(s)**. A confirmation message appears.
  - b Click **Yes**. The **Delete Firewall** window appears.
  - c Select the objects you want to delete, then click **Delete Firewall**. A message appears.
  - d Click **OK**. A message appears that recommends you apply changes.
  - e Click **Yes**. The **Apply Configuration** window appears.
  - f Select the Firewall Enterprise VAP group, then click **OK**.

The Control Center Management Server applies policy to the remaining VAPs in the VAP group.

---

## Uninstall Firewall Enterprise from a VAP group

Uninstall the VAP group using the XOS command line interface, then delete the VAP group from the Control Center Management Server.

### Tasks

- [Uninstall the VAP group from your X-Series Platform on page 105](#)  
Use the XOS command line interface to uninstall Firewall Enterprise.
- [Delete the VAP group from your Control Center Management Server on page 106](#)  
Use the Control Center Client application to delete the Firewall Enterprise VAP group from the Control Center Management Server.

## Uninstall the VAP group from your X-Series Platform

Use the XOS command line interface to uninstall Firewall Enterprise.

### Task

- 1 Establish a command line interface connection to the CPM using SSH (recommended) or Telnet.
- 2 Uninstall Firewall Enterprise from the VAP group.

```
CBS# application mfe vap-group <VAP_group_name> uninstall  
Are you sure you want to uninstall application? <Y or N> [Y]:
```

- 3 Press **Y**, then press **Enter** to confirm. Progress appears as Firewall Enterprise is uninstalled from the VAP group. When the operation is complete, the following text appears:

```
A VAP reload is required for the change(s) to take effect. Please run the CLI command
"reload vap-group <VAP_group_name>"
```

```
In order to successfully complete the application uninstall, the XOS configuration must
be saved.
```

```
Any unsaved configuration will be lost.
Do you want to save it to startup-config? <Y or N>[Y]:
```

- 4 Press **Y**, then press **Enter** to save.

- 5 Reload the VAP group.

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

If you see a message indicating that the uninstallation failed:

- View the `/var/log/messages` file on the CPM
- View the uninstallation error and warning messages by entering the following command:

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

## Delete the VAP group from your Control Center Management Server

Use the Control Center Client application to delete the Firewall Enterprise VAP group from the Control Center Management Server.

### Task

- 1 Use the Control Center Client application to connect to your Control Center Management Server.
- 2 In the **Policy** tree, expand the **Clusters** node.
- 3 Delete the Firewall Enterprise VAP group.
  - a Right-click the Firewall Enterprise VAP group, then select **Remove Object(s)**. A confirmation message appears.
  - b Click **Yes**. The **Delete Firewall** window appears.
  - c Select the objects you want to delete, then click **Delete Firewall**. A confirmation message appears.
  - d Click **OK**.

The Firewall Enterprise VAP group is removed from your Control Center Management Server.

---

## Delete a Firewall Enterprise zone

Delete a zone if the network no longer requires a unique security policy.

### Task

- 1 Make sure the zone is not in use in the firewall policy. You must remove the zone from use before you can delete it.
  - a Use the Control Center Client application to connect to your Control Center Management Server.
  - b In the navigation bar, select **Policy**.
  - c In the lower left area of the window, click the **Rule Objects** tab.
  - d Expand the **Network Objects** node.
  - e Expand the **Zones** node.
  - f Right-click the zone and select **Show Usage** to display a list of every area where the zone is currently used.
  - g Access each area listed and remove the zone from use.
- 2 Apply the updated policy to the firewall VAP group.
  - a Use the Control Center Client application to connect to your Control Center Management Server.
  - b In the navigation bar, click **Apply**. The **Apply Configuration** window appears.
  - c In the **Firewalls** list, select your Firewall Enterprise VAP group.
  - d Click **OK**. Progress is displayed as the Control Center applies policy to the firewall VAP group.
- 3 Delete the X-Series incoming circuit group (ICG) associated with the zone.
  - a Establish a command line connection to the X-Series CPM using SSH (recommended) or Telnet, then log on.
  - b At the XOS command prompt, run the following command to determine the ICG name and number associated with the zone:

```
CBS# show incoming-circuit-group-name
```
  - c Make sure the ICG is not in use by any circuit. You must remove the ICG from use before you can delete it.
  - d Delete the ICG.

```
CBS# config no incoming-circuit-group-name <ICG_number> <ICG_name>
```
- 4 Delete the zone.
  - a Establish a command line connection to the console of the primary firewall of the VAP group, then log on.
  - b Run the `srole` command to change to the Admn domain.
  - c Run the following command:

```
cf zone delete name=<zone_name>
```
- 5 Retrieve the Firewall Dialog Information component in Control Center.
  - a Use the Control Center Client application to connect to your Control Center Management Server.
  - b In the navigation bar, select **Policy**.

- c Expand the **Clusters** node.
- d Right-click the Firewall Enterprise VAP group and select **Retrieve Cluster Objects**. The **Cluster Retrieval Options** window appears.
- e Select **Firewall Dialog Information**.
- f Click **OK**.

---

## Upgrade a firewall on a Crossbeam X-Series Platform

Upgrade Firewall Enterprise on a Crossbeam X-Series Platform.

### Tasks

- [Upgrade Control Center on page 108](#)  
To upgrade Control Center, see the *McAfee Firewall Enterprise Control Center Release Notes*.
- [Upgrade or install your Crossbeam X-Series Platform on page 108](#)  
Make sure you are running a supported version of XOS by upgrading or performing a new XOS installation.
- [Install the Firewall Enterprise CBI package on page 108](#)  
Download the Firewall Enterprise CBI package and load it on your Crossbeam X-Series Platform.

## Upgrade Control Center

To upgrade Control Center, see the *McAfee Firewall Enterprise Control Center Release Notes*.

## Upgrade or install your Crossbeam X-Series Platform

Make sure you are running a supported version of XOS by upgrading or performing a new XOS installation.

See the *Crossbeam XOS Configuration Guide* for more information.

## Install the Firewall Enterprise CBI package

Download the Firewall Enterprise CBI package and load it on your Crossbeam X-Series Platform.



This procedure updates the Firewall Enterprise CBI that is present on the CPM, which is used to provision new VAPs. Performing this procedure will not modify firewall VAPs that are already installed.

### Task

- 1 Download the Firewall Enterprise CBI package.
  - a In a web browser, navigate to [support.mcafee.com](http://support.mcafee.com).
  - b Click the **Downloads** tab, then select the appropriate type of download.
  - c Enter your grant number, then navigate to the appropriate product and version.
  - d Download the Crossbeam installer (.cbi) file for the version.
- 2 Transfer the .cbi file to the \crossbeam\apps\archive directory on each X-Series CPM.

- 3 Run the following command for the firewall VAP group:

```
CBS# application-upgrade mfe vap-group <VAP_group_name>
```

- 4 Accept the prompts.



# Index

## A

about this guide [7](#)  
Application Processor Module [10](#)  
applications [11](#)  
AWS (Automated Workflow System [27](#), [31](#))

## B

bridged mode [14](#)

## C

circuit [12](#)  
configuration, saving [36](#), [45](#), [65](#)  
control link [14](#)  
Control Processor Module [10](#)  
conventions and icons used in this guide [7](#)

## D

default route  
    configuring [33](#), [43](#), [64](#)  
    configuring CPM [34](#), [44](#), [64](#)  
documentation  
    audience for this guide [7](#)  
    product-specific, finding [8](#)  
    typographical conventions and icons [7](#)  
dynamic routing [9](#)

## F

failover [13](#)  
fault tolerance [12](#), [13](#)  
Firewall Enterprise, installing [32](#), [45](#), [65](#)

## H

hardware [10](#)  
High Availability [13](#)  
host names, configuring for email [34](#), [44](#), [65](#)  
hybrid mode [14](#)

## I

installation requirements  
    DBHA [53](#)  
    manual [37](#)  
interface types [15](#)

## M

McAfee ServicePortal, accessing [8](#)  
multi-link [15](#)

## N

network integration  
    options [14](#)  
    planning [25](#)  
network modes [14](#)  
Network Processor Module [10](#), [22](#)

## O

overview  
    Crossbeam [9](#)  
    Firewall Enterprise [9](#)

## P

performance [12](#)  
prerequisites  
    Crossbeam configuration [22](#)  
    installing AWS [31](#)

## R

requirements  
    hardware and software [21](#)  
    Network Processor Module [22](#)  
responses, preparing for AWS installation [31](#)

## S

ServicePortal, finding product documentation [8](#)  
single chassis [12](#)  
single circuit [13](#)  
standalone [9](#)  
standard (routed) mode [14](#)

## T

technical support, finding product information [8](#)  
time zone, configuring [35](#), [49](#), [69](#)  
transparent (bridged) mode [14](#)

**V**

VAP [35](#), [45](#), [49](#), [66](#), [69](#)  
VAP groups [11](#)  
virtual router [13](#)  
VLAN [15](#)  
VRRP [13](#)

**X**

X-Series [12](#)  
XOS [9](#), [35](#), [49](#), [69](#)  
XOS command [32](#)



