



---

# Firefly Perimeter Administration Guide for VMware



---

Published: 2014-01-14

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

Copyright © 2014, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

*Firefly Perimeter Administration Guide for VMware*  
Copyright © 2014, Juniper Networks, Inc.  
All rights reserved.

The information in this document is current as of the date on the title page.

#### YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

#### END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

	About the Documentation . . . . .	ix
	Documentation and Release Notes . . . . .	ix
	Documentation Conventions . . . . .	ix
	Documentation Feedback . . . . .	xi
	Requesting Technical Support . . . . .	xi
	Self-Help Online Tools and Resources . . . . .	xii
	Opening a Case with JTAC . . . . .	xii
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Firefly Perimeter Overview . . . . .</b>	<b>3</b>
	Understanding Firefly Perimeter . . . . .	3
<b>Chapter 2</b>	<b>System Requirements . . . . .</b>	<b>5</b>
	Specifications for Firefly Perimeter Installation . . . . .	5
	Firefly Perimeter Basic Settings . . . . .	6
	Installation Requirements for Firefly Perimeter with VMware . . . . .	7
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 3</b>	<b>Firefly Perimeter Configurations . . . . .</b>	<b>11</b>
	Configuring and Deploying Firefly Perimeter Instances Using Junos Space Virtual Director . . . . .	11
	Firefly Perimeter Configuration Using the J-Web Interface . . . . .	11
	Accessing the J-Web Interface and Configuring Firefly Perimeter . . . . .	12
	Applying the Configuration . . . . .	15
	Firefly Perimeter Configuration Using the CLI Interface . . . . .	16
	Configuring Chassis Cluster for Firefly Perimeter . . . . .	18
	Chassis Cluster Overview . . . . .	18
	Understanding Chassis Cluster Formation . . . . .	19
	Chassis Cluster Quick Setup . . . . .	20
	Configuring Chassis Cluster . . . . .	23
	Firefly Chassis Cluster Configuration on VMware . . . . .	29
	Connecting Control Interface via Control vSwitch Using the VMware vSphere Client . . . . .	29
	Connecting Fabric Interface via Fabric vSwitch Using the VMware vSphere Client . . . . .	31
	Connecting Data Interface via Data vSwitch Using the VMware vSphere Client . . . . .	33
	Deploying Firefly Perimeter Chassis Cluster Nodes at Different ESXi Hosts Using dvSwitch . . . . .	34

<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 4</b>	<b>Firefly Perimeter Configuration and Management Tools . . . . .</b>	<b>39</b>
	Firefly Perimeter Configuration and Management Tools . . . . .	39
	Understanding Junos OS CLI and Junos Scripts . . . . .	39
	Understanding J-Web Interface . . . . .	39
	Understanding Junos Space Virtual Director . . . . .	40
	Understanding Junos Space Security Director . . . . .	41
<b>Chapter 5</b>	<b>Firefly Perimeter Management . . . . .</b>	<b>43</b>
	Monitoring and Managing Firefly Perimeter Instances Using Junos Space Virtual Director . . . . .	43
	Viewing Connection Status . . . . .	44
	Discover Devices . . . . .	44
	Managing Security Policies for VM Using Junos Space Security Director . . . . .	44
<b>Part 4</b>	<b>Index</b>	
	Index . . . . .	49

# List of Figures

<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 3</b>	<b>Firefly Perimeter Configurations</b>	<b>11</b>
	Figure 1: J-Web Setup Wizard Page	12
	Figure 2: J-Web Configuration Page	13
	Figure 3: Firefly Perimeter Configuration Summary	15
	Figure 4: vSwitch 1 Properties	30
	Figure 5: Virtual Machine Properties for Control vSwitch	30
	Figure 6: vSwitch 2 Properties	32
	Figure 7: Virtual Machine Properties for Fabric vSwitch	32
	Figure 8: Virtual Machine Properties for Data vSwitch	34
	Figure 9: dvPortGroup3 Settings	35
	Figure 10: dvPortGroup6 Settings	35
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 4</b>	<b>Firefly Perimeter Configuration and Management Tools</b>	<b>39</b>
	Figure 11: Virtual Director Topology	40



# List of Tables

	<b>About the Documentation</b> . . . . .	<b>ix</b>
	Table 1: Notice Icons . . . . .	x
	Table 2: Text and Syntax Conventions . . . . .	x
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 2</b>	<b>System Requirements</b> . . . . .	<b>5</b>
	Table 3: Specifications for Firefly Perimeter . . . . .	5
	Table 4: Hardware Specifications for Host Machine . . . . .	5
	Table 5: Basic Settings for Interfaces . . . . .	6
	Table 6: Basic Settings for Security Policies . . . . .	6
	Table 7: Basic Settings for NAT Rule . . . . .	7
	Table 8: Supported Version of VMware hypervisor . . . . .	7
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 3</b>	<b>Firefly Perimeter Configurations</b> . . . . .	<b>11</b>
	Table 9: Device Name and User Account Information . . . . .	14
	Table 10: System Time Options . . . . .	14
	Table 11: Add Chassis Cluster Setup Configuration Details . . . . .	22
	Table 12: Chassis Cluster Configuration Page Actions . . . . .	23
	Table 13: Chassis Cluster Configuration Page . . . . .	24
	Table 14: Add Node Setting Configuration Details . . . . .	25
	Table 15: Edit Node Setting Configuration Details . . . . .	28





# About the Documentation

- Documentation and Release Notes on page ix
- Documentation Conventions on page ix
- Documentation Feedback on page xi
- Requesting Technical Support on page xi

## Documentation and Release Notes

---

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

## Documentation Conventions

---

Table 1 on page x defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page x defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  <code>user@host&gt; configure</code>
<b>Fixed-width text like this</b>	Represents output that appears on the terminal screen.	<code>user@host&gt; show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies guide names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS CLI User Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name:  <code>[edit]</code> <code>root@# set system domain-name <i>domain-name</i></code>
<b>Text like this</b>	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the <code>[edit protocols ospf area area-id]</code> hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Encloses optional keywords or variables.	<code>stub &lt;default-metric <i>metric</i>&gt;;</code>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	<b>broadcast   multicast</b>  <i>(string1   string2   string3)</i>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	<b>community name members [ community-ids ]</b>
Indentation and braces ( { } )	Identifies a level in the configuration hierarchy.	<b>[edit]</b> routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
<b>GUI Conventions</b>		
<b>Bold text like this</b>	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

## Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

## PART 1

# Overview

- [Firefly Perimeter Overview on page 3](#)
- [System Requirements on page 5](#)



## CHAPTER 1

# Firefly Perimeter Overview

- [Understanding Firefly Perimeter on page 3](#)

## Understanding Firefly Perimeter

---

Firefly Perimeter is a virtual security appliance that provides security and networking services at the perimeter or edge in virtualized private or public cloud environments. Firefly Perimeter runs as a virtual machine (VM) on a standard x86 server.

Firefly Perimeter enables advanced security and routing at the network edge in a multitenant virtualized environment. Firefly Perimeter is built on Junos OS and delivers similar networking and security features available on SRX Series devices for the branch.

Some of the key benefits of Firefly Perimeter in virtualized private or public cloud multitenant environments include:

- Stateful firewall protection at the tenant edge
- Faster deployment of virtual firewalls
- Full routing, Virtual Private Network (VPN) and networking capabilities
- Complementary with the Juniper Networks Firefly Host for inter-VM security
- Centralized and local management

### Related Documentation

- [Specifications for Firefly Perimeter Installation on page 5](#)
- [Firefly Perimeter Basic Settings on page 6](#)
- [Installation Requirements for Firefly Perimeter with VMware on page 7](#)





## CHAPTER 2

# System Requirements

- [Specifications for Firefly Perimeter Installation on page 5](#)
- [Firefly Perimeter Basic Settings on page 6](#)
- [Installation Requirements for Firefly Perimeter with VMware on page 7](#)

### Specifications for Firefly Perimeter Installation

---

[Table 3 on page 5](#) lists the specifications for Firefly Perimeter.

**Table 3: Specifications for Firefly Perimeter**

Component	Specification
Memory	2 GB
Disk space	2 GB
vCPUs	2
vNICs	Up to 10
Virtual Network Interface Card type (NIC)	E1000

[Table 4 on page 5](#) lists the hardware specifications for the host machine that runs Firefly Perimeter VM.

**Table 4: Hardware Specifications for Host Machine**

Component	Specification
Host memory size	Minimum 4 GB
Host processor type	x86_64

**NOTE:**

- Ensure that the physical server includes multi-core CPU.
- The Host machine must support VMware.

For the Hardware Compatibility List, see:

[www.vmware.com](http://www.vmware.com).

**Related Documentation**

- [Understanding Firefly Perimeter on page 3](#)
- [Firefly Perimeter Basic Settings on page 6](#)
- [Installation Requirements for Firefly Perimeter with VMware on page 7](#)

## Firefly Perimeter Basic Settings

Firefly Perimeter is a security device that requires these basic configuration settings to function:

- Interfaces must be assigned IP addresses.
- Interfaces must be bound to zones.
- Policies must be configured between zones to permit or deny traffic.

Firefly Perimeter has the following default configurations set when you power it on for the first time.

[Table 5 on page 6](#) lists the basic settings for interfaces.

**Table 5: Basic Settings for Interfaces**

Interface	Security Zones	DHCP State
ge-0/0/0	trust	client
ge-0/0/1 to ge-0/0/3	trust	server

[Table 6 on page 6](#) lists the basic settings for the security policies.

**Table 6: Basic Settings for Security Policies**

Source Zone	Destination Zone	Policy Action
trust	untrust	permit
trust	trust	permit
untrust	trust	deny

Table 7 on page 7 lists the basic settings for the NAT rule.

**Table 7: Basic Settings for NAT Rule**

Source Zone	Destination Zone	Policy Action
trust	untrust	source NAT to untrust zone interface

**Related  
Documentation**

- [Understanding Firefly Perimeter on page 3](#)
- [Specifications for Firefly Perimeter Installation on page 5](#)
- [Installation Requirements for Firefly Perimeter with VMware on page 7](#)

## Installation Requirements for Firefly Perimeter with VMware

Table 8 on page 7 lists the supported version of VMware Hypervisor.

**Table 8: Supported Version of VMware hypervisor**

VMware Hypervisor	Hypervisor Version
VMware vSphere ESXi	5.0 and 5.1



**NOTE:** Create an account on the VMware website at [www.vmware.com](http://www.vmware.com) to access the downloads and to obtain the license key for VMware.

**Related  
Documentation**

- [Understanding Firefly Perimeter on page 3](#)
- [Specifications for Firefly Perimeter Installation on page 5](#)
- [Firefly Perimeter Basic Settings on page 6](#)



## PART 2

# Configuration

- [Firefly Perimeter Configurations on page 11](#)



## CHAPTER 3

# Firefly Perimeter Configurations

- [Configuring and Deploying Firefly Perimeter Instances Using Junos Space Virtual Director on page 11](#)
- [Firefly Perimeter Configuration Using the J-Web Interface on page 11](#)
- [Firefly Perimeter Configuration Using the CLI Interface on page 16](#)
- [Configuring Chassis Cluster for Firefly Perimeter on page 18](#)

## Configuring and Deploying Firefly Perimeter Instances Using Junos Space Virtual Director

---

Junos Space Virtual Director offers a provision template that allows you to configure Firefly Perimeter instances for individual or batch replicated deployment. The provision template defines all the parameters that a virtual machine requires to execute an instance of the Firefly Perimeter. It also includes the information about virtual machine parameters such as number of CPUs, memory size, disk space, number of NICs, network addresses, and a minimal amount of device startup configuration information.



**NOTE:** Virtual Director is one way to configure Firefly Perimeter. You can also configure Firefly Perimeter using other management tools like J-Web, CLI, and so on.

### Related Documentation

- [Junos Space Virtual Director Getting Started Guide.](#)
- [Understanding Firefly Perimeter on page 3](#)
- [Firefly Perimeter Configuration and Management Tools on page 39](#)

## Firefly Perimeter Configuration Using the J-Web Interface

---

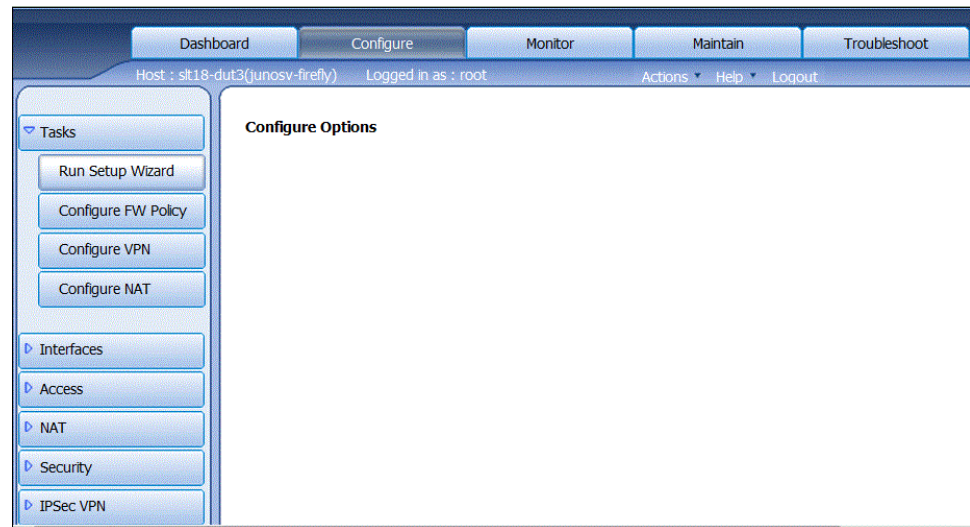
- [Accessing the J-Web Interface and Configuring Firefly Perimeter on page 12](#)
- [Applying the Configuration on page 15](#)

## Accessing the J-Web Interface and Configuring Firefly Perimeter

To configure Firefly Perimeter using the J-Web Interface:

1. Launch a Web browser from the management device.
2. Enter the Firefly Perimeter interface IP address in the Address box.
3. Specify the default username as root. Do not enter a value in the Password box.
4. Click **Log In**. The J-Web Setup Wizard page opens. See [Figure 1 on page 12](#).

**Figure 1: J-Web Setup Wizard Page**

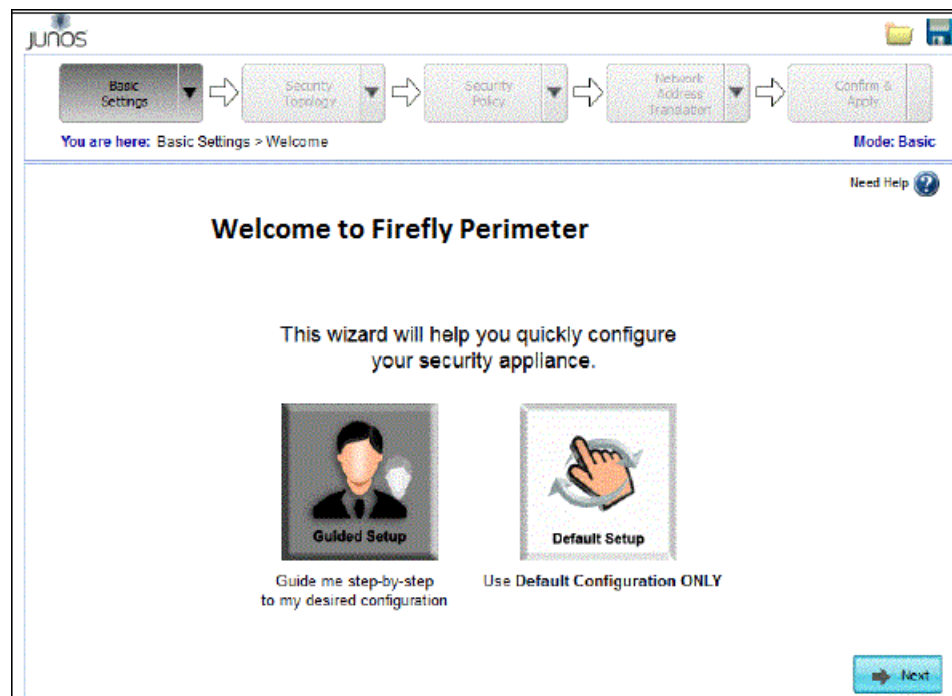


5. Click **Tasks > Run Setup Wizard**.

You can use the Setup Wizard to configure a device or edit an existing configuration. See [Figure 2 on page 13](#).



Figure 2: J-Web Configuration Page



- Select the **Edit Existing Configuration** if you have already configured the wizard using the factory mode.
- Select the **Create New Configuration** to configure a device using the wizard.

Two configuration options are available:

- To enable basic options

Select **Basic** to enable basic options. In Basic mode, you configure the device name and user account information as shown in [Table 9 on page 14](#).

- Device name and user account information

**Table 9: Device Name and User Account Information**

Field	Description
Device name	Type the name of the device. For example: <b>Firefly Perimeter</b> .
Root password	Create a default root user password.
Verify password	Verify the default root user password.
Operator	<p>Add an administrative account in addition to the root account, which is optional.</p> <p>User role options include:</p> <ul style="list-style-type: none"> <li>• <b>Super User:</b> This user has full system administration rights and can add, modify, and delete settings and users.</li> <li>• <b>Operator:</b> This user can perform system operations such as a system reset but cannot change the configuration or add or modify users.</li> <li>• <b>Read only:</b> This user can only access the system and view the configuration.</li> <li>• <b>Disabled:</b> This user cannot access the system.</li> </ul>

- Select either **Time Server** or **Manual**. [Table 10 on page 14](#) lists the system time options.

**Table 10: System Time Options**

Field	Description
<b>Time Server</b>	
Host Name	Type the hostname of the time server. For example: <b>us.ntp.pool.org</b>
IP	Type the IP address of the time server in the IP address entry field. For example: <b>192.168.1.254</b> .
<b>NOTE:</b> You can either enter the hostname or the IP address.	
<b>Manual</b>	
Date	Click the current date in the calendar.
Time	Set the hour, minute, and seconds. Choose <b>AM</b> or <b>PM</b> .
<b>Time Zone (mandatory)</b>	
Time Zone	Select the time zone from the list. For example: GMT Greenwich Mean Time GMT.

- To enable Advanced options:

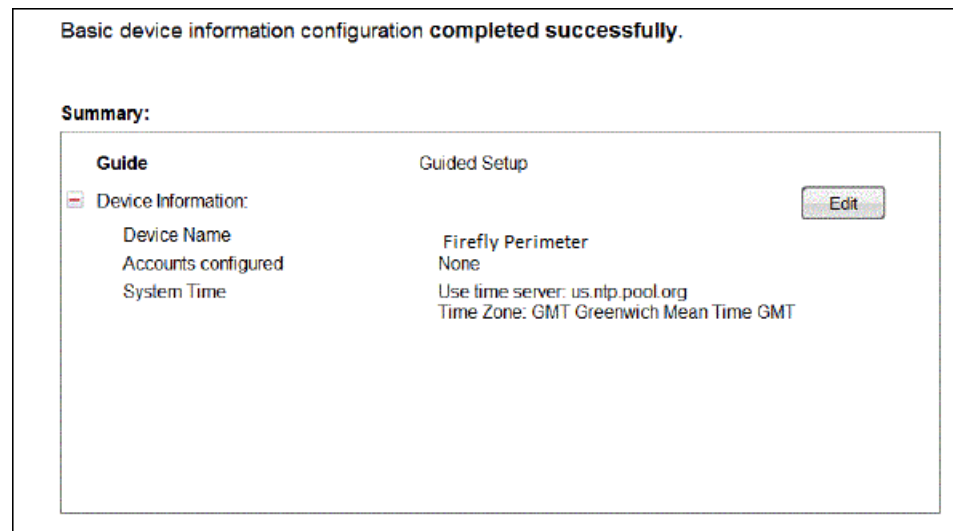
Select **Expert** to configure the basic options as well as the following advanced options:

- Four or more internal zones
- Internal zone services
- Application of security policies between internal zones
- A static IP address pool for Internet addressing
- An inbound static IP addressing pool for NAT

Click the **Need Help** icon available for detailed configuration information.

You see a success message after the basic configuration is complete. See [Figure 3 on page 15](#).

**Figure 3: Firefly Perimeter Configuration Summary**



## Applying the Configuration

To apply the configuration settings for Firefly Perimeter:

1. Review and ensure that the configuration settings are correct and click **Next**. The Commit Configuration page displays.
2. Click **Apply Settings** to apply the configuration changes to Firefly Perimeter.
3. Check the connectivity to Firefly Perimeter as you might lose connectivity if you have changed the management zone IP. Click the URL for reconnection instructions on how to reconnect to the device.
4. Click **Done** to complete the setup.

After successful completion of the setup, you are redirected to the J-Web interface.



**WARNING:** After you complete the initial setup configuration, you can relaunch the J-Web Setup wizard by clicking Tasks > Run Setup Wizard. You can either edit an existing configuration or create a new configuration. If you decide to create a new configuration, then all the current configuration in Firefly Perimeter will be deleted.

**Related  
Documentation**

- [Firefly Perimeter Basic Settings on page 6](#)
- [Powering On/Off the Device](#)
- [Firefly Perimeter Configuration Using the CLI Interface on page 16](#)

---

## Firefly Perimeter Configuration Using the CLI Interface

To configure Firefly Perimeter using the CLI Interface:

1. Verify that the device is powered on.
2. Log in as the root user. There is no password.
3. Start the CLI

```
root#cli
root@>
```
4. Enter configuration mode.

```
configure
[edit]
root@#
```
5. Set the root authentication password by entering a cleartext password, an encrypted password, or an SSH public key string (DSA or RSA).

```
[edit]
root@# set system root-authentication plain-text-password
New password: password
Retype new password: password
```
6. Configure an administrative account on the device.

```
[edit]
root@# set system login user admin class super-user authentication
plain-text-password
```
7. Commit the configuration to activate it on the device.

```
[edit]
root@# commit
```
8. Login as the administrative user you configured in Step 6.
9. Configure the name of the device. If the name includes spaces, enclose the name in quotation marks (" ").

```
configure
```

```
[edit]
admin@# set system host-name host-name
```

10. Configure the traffic interface.

```
[edit]
admin@# set interfaces ge-0/0/1 unit 0 family inet address address/prefix-length
```

11. Configure the default route.

```
[edit]
admin@# set routing-options static route 0.0.0.0/0 next-hop gateway
```

12. Configure basic security zones and bind them to traffic interfaces.

```
[edit]
admin@# set security zones security-zone untrust interfaces ge-0/0/1
```

13. Verify the configuration.

```
[edit]
admin@# commit check
configuration check succeeds
```

14. Commit the configuration to activate it on the device.

```
[edit]
admin@# commit
commit complete
```

15. Optionally, display the configuration to verify that it is correct.

```
[edit]
user@host# show
system {
  host-name devicea;
  domain-name lab.device.net;
  domain-search [ lab.device.net device.net ];
  backup-device ip
  time-zone America/Los_Angeles;
  root-authentication {
    ssh-rsa "ssh-rsa AAAAB3Nza...D9Y2gXF9ac==root@devicea.lab.device.net";
  }
  name-server {
    ip
  }
  services {
  }
  ntp {
    server ip
  }
}
interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        address ip
      }
    }
  }
}
```

```
lo0 {  
  unit 0 {  
    family inet {  
      address ip  
    }  
  }  
}
```

16. Commit the configuration to activate it on the device.

```
[edit]  
admin@# commit
```

17. Optionally, configure more properties by adding the necessary configuration statements. Then commit the changes to activate them on the device.

```
[edit]  
admin@host# commit
```

18. When you have finished configuring the device, exit configuration mode.

```
[edit]  
admin@host# exit  
admin@host>
```



**NOTE:** For additional configuration details, see:

[http://www.juniper.net/techpubs/en\\_US/junos12.1/information-products/pathway-pages/security/security-swconfig-initial-device-config.html#configuration](http://www.juniper.net/techpubs/en_US/junos12.1/information-products/pathway-pages/security/security-swconfig-initial-device-config.html#configuration)

---

#### Related Documentation

- [Firefly Perimeter Basic Settings on page 6](#)
- [Powering On/Off the Device](#)
- [Firefly Perimeter Configuration Using the J-Web Interface on page 11](#)

---

## Configuring Chassis Cluster for Firefly Perimeter

- [Chassis Cluster Overview on page 18](#)
- [Understanding Chassis Cluster Formation on page 19](#)
- [Chassis Cluster Quick Setup on page 20](#)
- [Configuring Chassis Cluster on page 23](#)
- [Firefly Chassis Cluster Configuration on VMware on page 29](#)
- [Deploying Firefly Perimeter Chassis Cluster Nodes at Different ESXi Hosts Using dvSwich on page 34](#)

### Chassis Cluster Overview

Chassis clustering provides network node redundancy by grouping a pair of the same kind of Firefly Perimeter instances into a cluster. The devices must be running the same

version of the Junos OS. The control ports on the respective nodes are connected to form a control plane that synchronizes the configuration and kernel state to facilitate the high availability of interfaces and services. Similarly, the data plane on the respective nodes is connected over the fabric ports to form a unified data plane. The fabric link allows for the management of cross-node flow processing and for the management of session redundancy.

The control plane software operates in active or backup mode. When configured as a chassis cluster, the two nodes back up each other, with one node acting as the primary device and the other as the secondary device, ensuring stateful failover of processes and services in the event of a system or hardware failure. If the primary device fails, the secondary device takes over processing of traffic.

The data plane software operates in active/active mode. In a chassis cluster, session information is updated as traffic traverses either device, and this information is transmitted between the nodes over the fabric link to guarantee that established sessions are not dropped when a failover occurs. In active/active mode, it is possible for traffic to ingress the cluster on one node and egress from the other node.

Chassis cluster functionality includes:

- Resilient system architecture, with a single active control plane for the entire cluster and multiple Packet Forwarding Engines. This architecture presents a single device view of the cluster.
- Synchronization of configuration and dynamic runtime states between nodes within a cluster.
- Monitoring of physical interfaces, and failover if the failure parameters cross a configured threshold.
- Support for generic routing encapsulation (GRE) and IP-over-IP (IP-IP) tunnels used to route encapsulated IPv4 or IPv6 traffic by means of two internal interfaces, `gr-0/0/0` and `ip-0/0/0`, respectively. These interfaces are created by Junos OS at system bootup and are used only for processing GRE and IP-IP tunnels.

At any given instant, a cluster can be in one of the following states: hold, primary, secondary-hold, secondary, ineligible, and disabled. A state transition can be triggered because of any event, such as interface monitoring, Services Processing Unit (SPU) monitoring, failures, and manual failovers.

For additional information, see:

[Interfaces for Security Devices](#)

## Understanding Chassis Cluster Formation

You create two Firefly Perimeter instances to form a chassis cluster, and then you set the cluster ID and node ID on each instance to join the cluster. When a device joins a cluster, it becomes a node of that cluster. With the exception of unique node settings and management IP addresses, nodes in a cluster share the same configuration.

You can deploy up to 15 chassis clusters in a Layer 2 domain. Clusters and nodes are identified in the following ways:

- A cluster is identified by a *cluster ID* specified as a number from 1 to 15.
- A cluster node is identified by a *node ID* specified as a number from 0 to 1.

Generally, on SRX Series devices, the cluster ID and node ID are written into EEPROM. However, the Firefly Perimeter VM does not emulate it. A location (`boot/loader.conf`) is required to save the IDs and read it out during initialization. Then the whole system (including BSD kernel) can know it is working in chassis cluster mode and does related initializations for chassis cluster.

The chassis cluster formation commands for node 0 and node 1 are as follows:

- `user@hostset chassis cluster cluster-id 1 node 0 reboot`
- `user@hostset chassis cluster cluster-id 1 node 1 reboot`

For additional information on chassis cluster, see:

[http://www.juniper.net/techpubs/en\\_US/junos12.1x45/information-products/pathway-pages/security/security-chassis-cluster.html](http://www.juniper.net/techpubs/en_US/junos12.1x45/information-products/pathway-pages/security/security-chassis-cluster.html)

## Chassis Cluster Quick Setup

You can use the J-Web interface to set up chassis cluster for both the Firefly Perimeter devices forming a cluster.

To set up chassis cluster:

1. Launch a Web browser from the management device.
2. Enter the Firefly interface IP address in the Address box.
3. Specify the default username as `root`. Do not enter a value in the Password box.
4. Click **Log In**. The J-Web Setup Wizard page opens.
5. Select **Configure>Chassis Cluster>Setup**. The Chassis Cluster Setup configuration page appears. [Table 11 on page 22](#) explains the contents of this page.
6. Configure chassis cluster using the options described in [Table 11 on page 22](#).
7. Click **Enable** to enable chassis cluster mode on the node.
8. Select one of the following options:
  - **Enable and Reboot**: Enables chassis cluster mode and reboots the node.  
A confirmation message says **Successfully enabled chassis cluster. Going to reboot now**.  
Click **OK**.
  - **Enable and No Reboot**: Enables chassis cluster mode without rebooting the node.  
A confirmation message is displayed.



Click **OK**.

- **Cancel**: Cancels your entries and returns to the main configuration page.
9. Click **Reset** to reset your entries to their original values or click **Disable** to disable chassis cluster mode on the node.

Table 11: Add Chassis Cluster Setup Configuration Details

Field	Function	Action
Cluster ID	Specifies the number by which a cluster is identified.	Enter a number from 0 through 15.
<b>Node</b>		
Node ID	Specifies the number by which a node is identified.	Enter a number from 0 through 1.
Node Management IP Address (fxp0.0)	Specifies the management IP address of a node.	Enter a valid IP address for the management interface.
<b>Control Link</b>		
FPC	Specifies the FPC control link.	Select the FPC number from the list.
Port	Specifies the port to configure for the control link.	Enter a number from 0 through 2.



**NOTE:** For detailed information on various options used for chassis cluster see:

[http://www.juniper.net/techpubs/en\\_US/junos12.1x45/information-products/pathway-pages/security/security-chassis-cluster.html](http://www.juniper.net/techpubs/en_US/junos12.1x45/information-products/pathway-pages/security/security-chassis-cluster.html)

## Configuring Chassis Cluster

You can use J-Web interface to configure the primary Firefly device.

Select **Configure>Chassis Cluster>Cluster Configuration**. The Chassis Cluster configuration page appears.

See [Table 12 on page 23](#) for the actions available on the Chassis Cluster configuration page.

[Table 13 on page 24](#) explains the contents of the configuration page.

See [Table 14 on page 25](#) for Node Setting configuration details.

**Table 12: Chassis Cluster Configuration Page Actions**

Action	Description
Add	Adds a new or duplicate chassis cluster configuration. Enter information as specified in <a href="#">Table 15 on page 28</a> .
Edit	Edits the selected chassis cluster configuration. Enter information as specified in <a href="#">Table 15 on page 28</a> .
Delete	Deletes the selected chassis cluster configuration.
Actions & Commit	Commits the configuration and returns to the main configuration page.
Cancel	Cancels your entries and returns to the main configuration page.

Table 13: Chassis Cluster Configuration Page

Field	Function
<b>Node Settings</b>	
Node ID	Displays the node ID.
Cluster ID	Displays the cluster ID configured for the node.
Host Name	Displays the name of the node.
Backup Router	Displays the IP address used while booting.
Management Interface	Displays the management interface of the node.
IP Address	Displays the management IP address of the node.
Status	Displays the state of the redundancy group. <ul style="list-style-type: none"> <li>• <b>Primary</b>—Redundancy group is active.</li> <li>• <b>Secondary</b>—Redundancy group is passive.</li> </ul>
<b>Chassis Cluster &gt; Cluster Settings &gt; Interfaces</b>	
Name	Displays the physical interface name.
Member Interfaces/IP Address	Displays the member interface name or IP address configured for an interface.
Redundancy Group	Displays the redundancy group.
<b>Chassis Cluster &gt; Cluster Settings &gt; Redundancy Group</b>	
Group	Displays the redundancy group identification number.
Preempt	Displays the selected Preempt option. <ul style="list-style-type: none"> <li>• <b>True</b>—Mastership can be preempted based on priority.</li> <li>• <b>False</b>—Mastership cannot be preempt based on priority.</li> </ul>
Gratuitous ARP Count	Displays the number of gratuitous ARP requests that a newly elected primary device in a chassis cluster sends out to announce its presence to the other network devices.
Node Priority	Displays the assigned priority for the redundancy group on that node. The eligible node with the highest priority is elected as primary for the redundant group.

Table 14: Add Node Setting Configuration Details

Field	Function	Action
<b>Fabric Link &gt; Fabric Link 0 (fab0)</b>		
Interface	Specifies fabric link 0.	Enter the interface IP fabric link 0.
Add	Adds fabric interface 0.	Click <b>Add</b> .
Delete	Deletes fabric interface 0.	Click <b>Delete</b> .
<b>Fabric Link &gt; Fabric Link 1 (fab1)</b>		
Interface	Specifies fabric link 1.	Enter the interface IP for fabric link 1.
Add	Adds fabric interface 1.	Click <b>Add</b> .
Delete	Deletes fabric interface 1.	Click <b>Delete</b> .
<b>Redundant Ethernet</b>		
Interface	Specifies a logical interface consisting of two physical Ethernet interfaces, one on each chassis.	Enter the logical interface.
IP	Specifies redundant Ethernet IP address.	Enter redundant Ethernet IP address.
Redundancy Group	Specifies redundancy group ID number in the chassis cluster.	Select a redundancy group from the list.
Add	Adds redundant Ethernet IP address.	Click <b>Add</b> .
Delete	Deletes redundant Ethernet IP address.	Click <b>Delete</b> .
<b>Add Redundancy Group</b>		
Redundancy Group	Specifies the redundancy group name.	Enter the redundancy group name.
Allow preemption of primaryship	Allows a node with a better priority to initiate a failover for a redundancy group.  <b>NOTE:</b> By default, this feature is disabled. When disabled, a node with a better priority does not initiate a redundancy group failover (unless some other factor, such as faulty network connectivity identified for monitored interfaces, causes a failover).	-

Table 14: Add Node Setting Configuration Details (*continued*)

Field	Function	Action
Gratuitous ARP Count	Specifies the number of gratuitous Address Resolution Protocol requests that a newly elected master sends out on the active redundant Ethernet interface child links to notify network devices of a change in mastership on the redundant Ethernet interface links.	Enter a value from 1 to 16. The default is 4.
node0 priority	Specifies the priority value of node0 for a redundancy group.	Enter the node priority number as 0.
node1 priority	Specifies the priority value of node1 for a redundancy group.	Select the node priority number as 1.
<b>Interface Monitor</b>		
Interface	Specifies the number of redundant Ethernet interfaces to be created for the cluster.	Select the interface from the list.
Weight	Specifies the weight for the interface to be monitored.	Enter a value from 1 to 125..
Add	Adds interfaces to be monitored by the redundancy group and their respective weights.	Click <b>Add</b> .
Delete	Deletes interfaces to be monitored by the redundancy group along with their respective weights.	Select the interface from the configured list and click <b>Delete</b> .
<b>IP Monitoring</b>		
Weight	Specifies the global threshold for IP monitoring.	Enter a value from 0 to 255.
Threshold	Specifies the global threshold for IP monitoring.	Enter a value from 0 to 255.
Retry Count	Specifies the number of retries needed to declare reachability failure.	Enter a value from 5 to 15.
Retry Interval	Specifies the time interval in seconds between retries.	Enter a value from 1 to 30.
<b>IPv4 Addresses to be monitored</b>		
IP	Specifies the IPv4 addresses to be monitored for reachability.	Enter the IPv4 addresses.

Table 14: Add Node Setting Configuration Details (*continued*)

Field	Function	Action
Weight	Specifies the weight for the redundancy group interface to be monitored.	Enter the weight.
Interface	Specifies the logical interface through which to monitor this IP address.	Enter the logical interface address.
Secondary IP address	Specifies the source address for monitoring packets on a secondary link.	Enter the secondary IP address.
Add	Adds the IPv4 addresses to be monitored.	Click <b>Add</b> .
Delete	Delete the IPv4 addresses to be monitored.	Select the item from the list and click <b>Delete</b> .

Table 15: Edit Node Setting Configuration Details

Field	Function	Action
<b>Node Settings</b>		
Host Name	Specifies the name of the host.	Enter the name of the host.
Backup Router	Specifies the backup router to be used during failover.	Specifies the backup router to be used during failover.
<b>Destination</b>		
IP	Adds the destination address.	Click <b>Add</b> .
Delete	Deletes the destination address.	Click <b>Delete</b> .
<b>Interface</b>		
Interface	Specifies the interfaces available for the router.  <b>NOTE:</b> Allows you to add and edit two interfaces for each fabric link.	Select an option.
IP	Specifies the interface IP address.	Enter the interface IP address.
Add	Adds the interface.	Click <b>Add</b> .
Delete	Deletes the interface.	Click <b>Delete</b> .



## Firefly Chassis Cluster Configuration on VMware

This topic provides information on Firefly Chassis Cluster Configuration using the VMware vSphere Client. This topic explains how to connect control interface via control vSwitch, fabric interface via fabric vSwitch and data interface via data vSwitch. Make sure that chassis cluster is set up for both the Firefly VMs.

For configuration examples on chassis cluster using CLI, see:

[http://www.juniper.net/techpubs/en\\_US/junos12.1x45/information-products/pathway-pages/security/security-chassis-cluster.html](http://www.juniper.net/techpubs/en_US/junos12.1x45/information-products/pathway-pages/security/security-chassis-cluster.html).

- [Connecting Control Interface via Control vSwitch Using the VMware vSphere Client on page 29](#)
- [Connecting Fabric Interface via Fabric vSwitch Using the VMware vSphere Client on page 31](#)
- [Connecting Data Interface via Data vSwitch Using the VMware vSphere Client on page 33](#)

---

### Connecting Control Interface via Control vSwitch Using the VMware vSphere Client

To connect the control interface via control switch:

1. Choose **Configuration->Networking**.
2. Click **Add Networking** to create a vSwitch for control link.

Choose the following attributes:

- Connection Type
  - Virtual Machines
- Network Access
  - Create a vSphere stand switch
  - No physical adapters
- Port Group Properties
  - Network Label: chassis cluster Control
  - VLAN ID: None(0)

After creating the control vSwitch, you can use the vSwitch default settings.

3. Click **Edit Settings** of both Firefly VMs to add the control interface (Network adapter 2) into control vSwitch.

See [Figure 4 on page 30](#) for vSwitch 1 Properties and [Figure 5 on page 30](#) for Virtual Machine Properties for Control vSwitch.

Figure 4: vSwitch 1 Properties

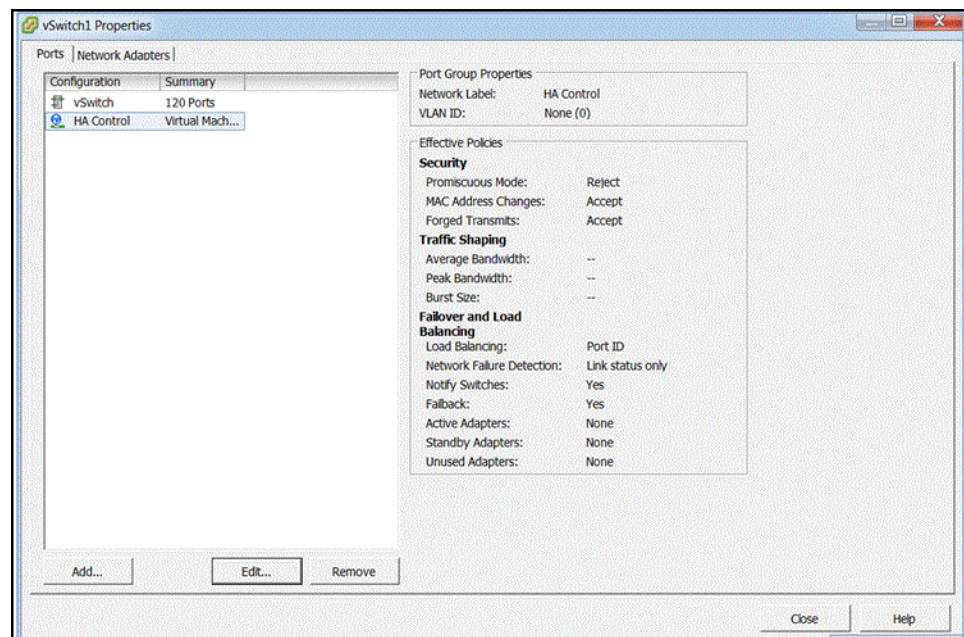
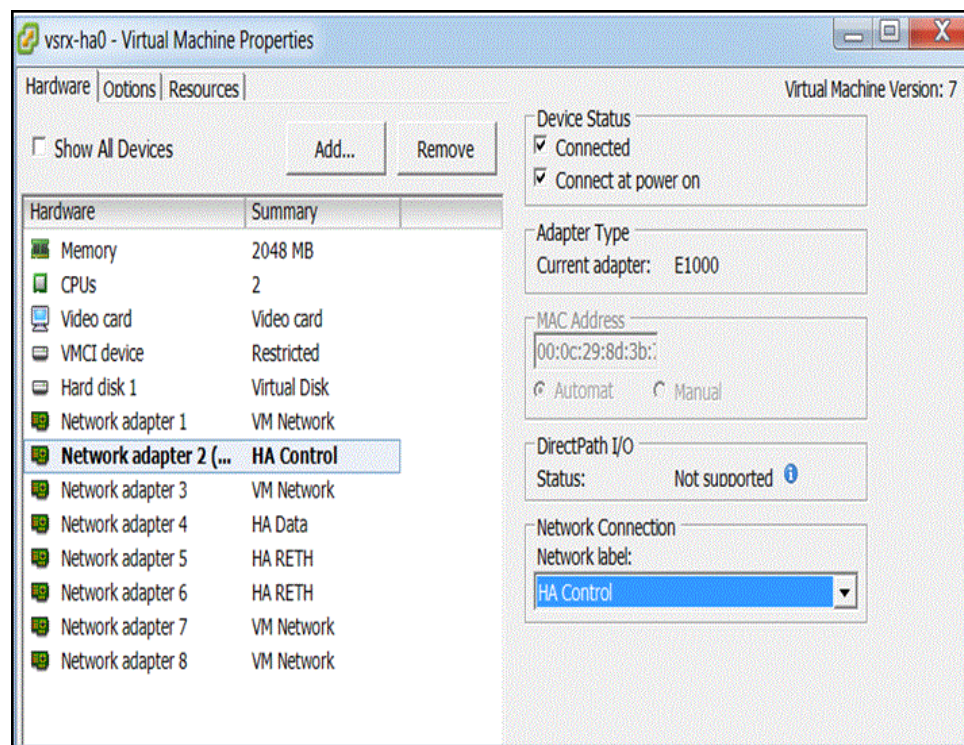


Figure 5: Virtual Machine Properties for Control vSwitch



The control interface will hence be connected via the control vSwitch using the above procedure.

### Connecting Fabric Interface via Fabric vSwitch Using the VMware vSphere Client

1. Choose **Configuration->Networking**.
2. Click **Add Networking** to create a vSwitch for fabric link.

Choose the following attributes:

- Connection Type
  - Virtual Machines
- Network Access
  - Create a vSphere stand switch
  - No physical adapters
- Port Group Properties
  - Network Label: chassis cluster Fabric
  - VLAN ID: None(0)

Click on **Properties** to turn on the following features:

- **General-> Advanced Properties:**
  - MTU: 9000
- **Security-> Effective Policies:**
  - MAC Address Changes: Accept
  - Forged Transmits: Accept

3. Click **Edit Settings** of both Firefly VMs to add the fabric interface into fabric vSwitch.



**NOTE:** Network adaptor 4 is used in this example, which is configurable in Junos.

See [Figure 6 on page 32](#) for vSwitch 2 Properties and [Figure 7 on page 32](#) for Virtual Machine Properties for Fabric vSwitch.



Figure 6: vSwitch 2 Properties

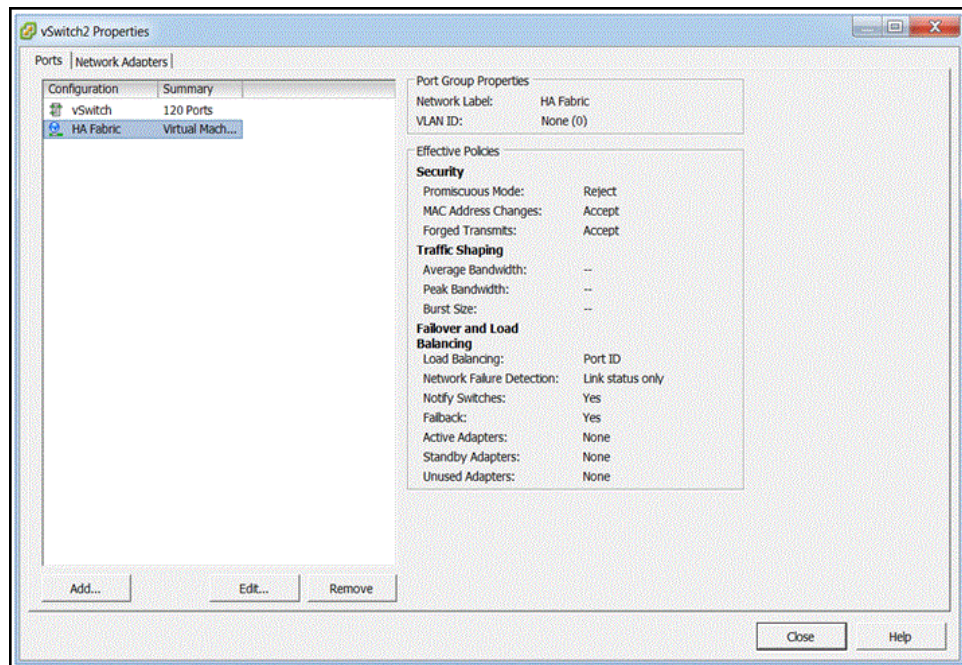
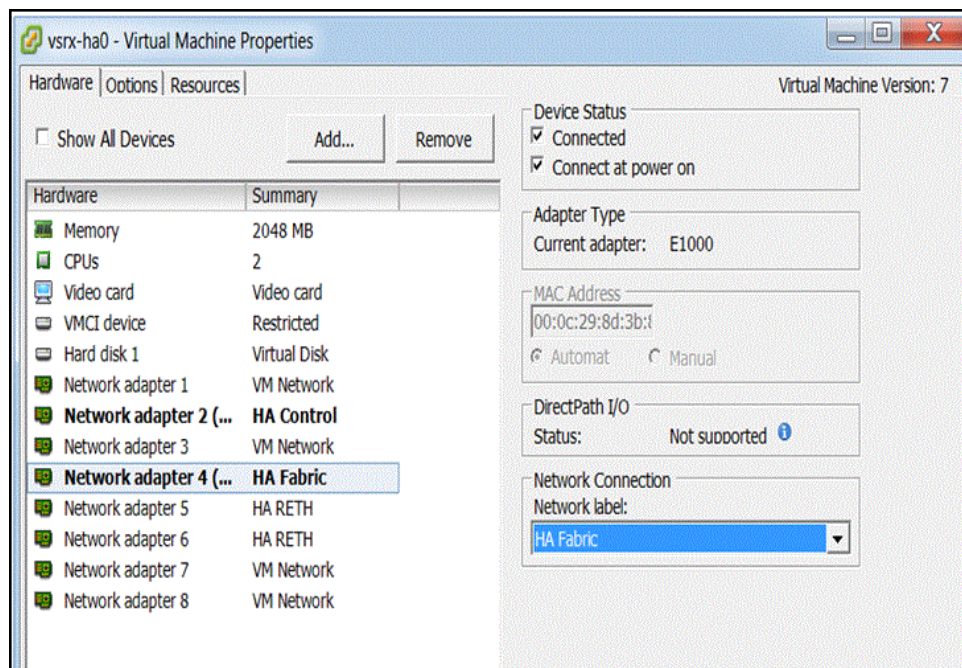


Figure 7: Virtual Machine Properties for Fabric vSwitch



The fabric interface will hence be connected via the fabric vSwitch using the above procedure.

### Connecting Data Interface via Data vSwitch Using the VMware vSphere Client

Add all the redundant interfaces into data traffic vSwitch like standalone mode.

1. Choose **Configuration->Networking**.
2. Click **Add Networking** to create a vSwitch for fabric link.

Choose the following attributes:

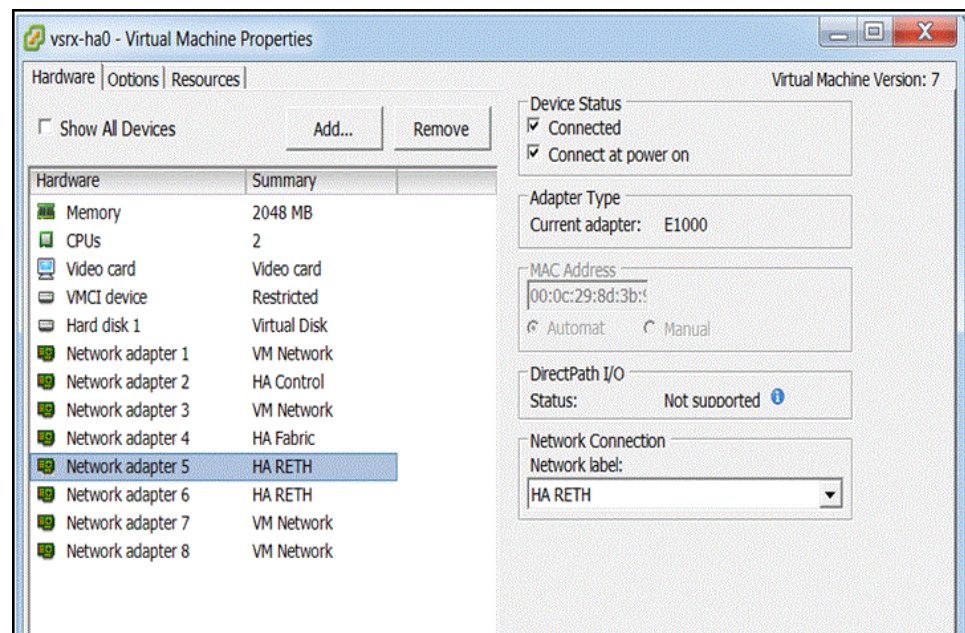
- Connection Type
  - Virtual Machines
- Network Access
  - Create a vSphere stand switch
  - No physical adapters
- Port Group Properties
  - Network Label: chassis cluster Reth
  - VLAN ID: None(0)

Click on **Properties** to turn on the following features:

- **General-> Advanced Properties:**
  - MTU: 9000
- **Security-> Effective Policies:**
  - MAC Address Changes: Accept
  - Forged Transmits: Accept

See [Figure 8 on page 34](#) for Virtual Machine Properties for Data vSwitch.

Figure 8: Virtual Machine Properties for Data vSwitch



The data interface will hence be connected via the data vSwitch using the above procedure.

### Deploying Firefly Perimeter Chassis Cluster Nodes at Different ESXi Hosts Using dvSwitch

In this method, we use the private vlan feature of dvSwitch. There is no need to change the external switch configurations.

On the VMware vSphere Client, for dvSwitch, there are two private VLAN IDs, the primary private VLAN ID and the secondary private VLAN ID.

Select **Community** in the drop down menu for secondary VLAN ID type.

Use the two secondary private VLAN IDs for Firefly Perimeter control and fabric link. See [Figure 9 on page 35](#) and [Figure 10 on page 35](#).



Figure 9: dvPortGroup3 Settings

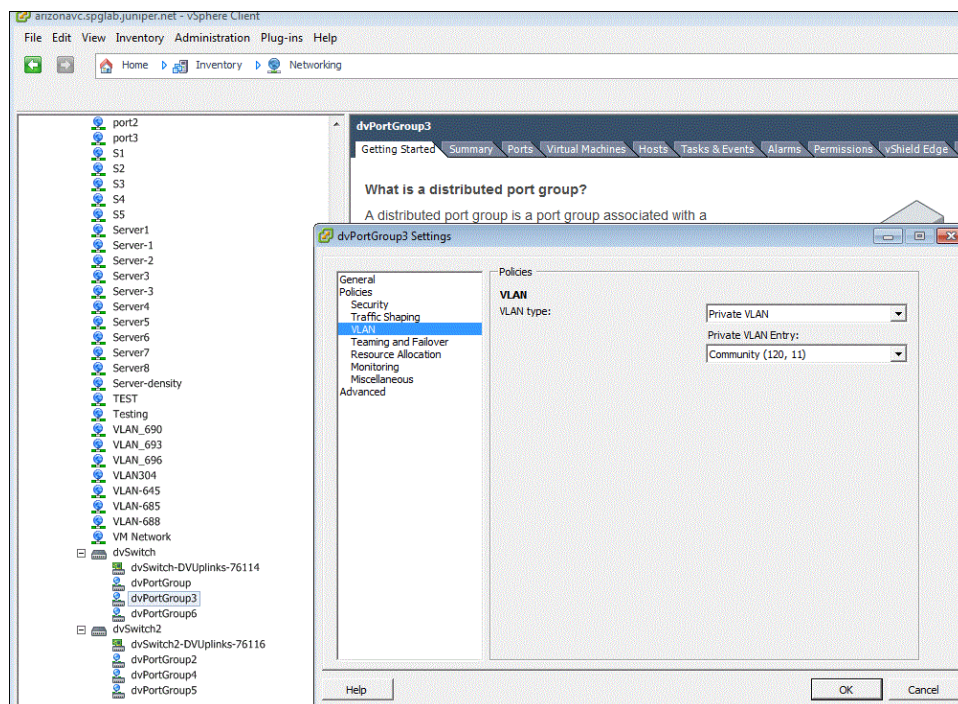
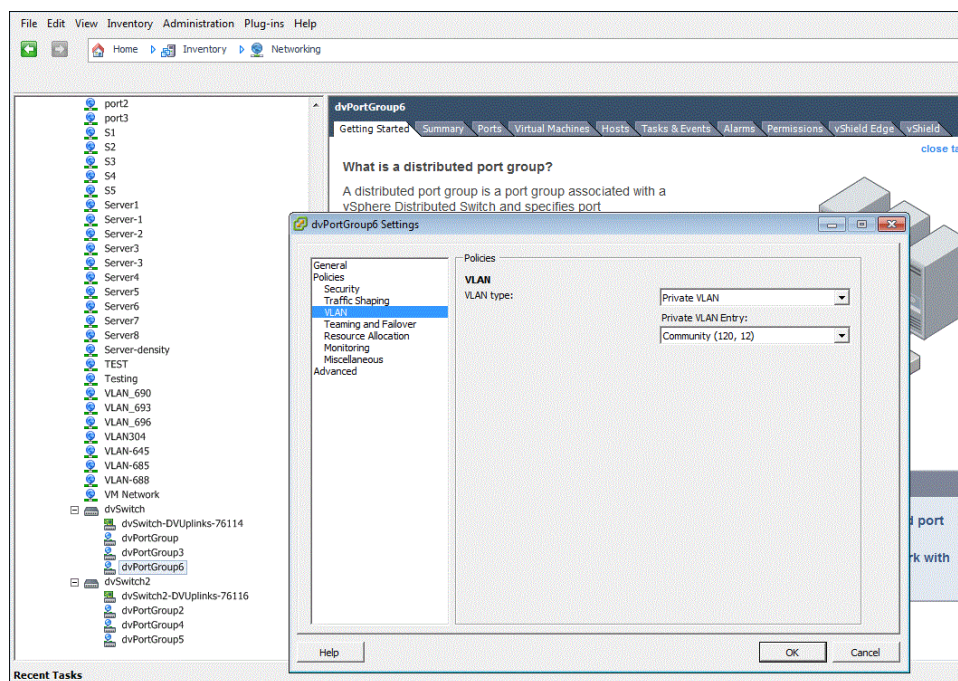


Figure 10: dvPortGroup6 Settings





NOTE: Configurations above are required at external switch, to which distributed switch uplinks are connected. If the link at external switch has native vlan, then distributed switch port group config can have vlan as none. Otherwise, vlan should be used.

**Related  
Documentation**

- [Understanding Firefly Perimeter on page 3](#)
- *Features Supported on Firefly Perimeter with VMware*



## PART 3

# Administration

- [Firefly Perimeter Configuration and Management Tools on page 39](#)
- [Firefly Perimeter Management on page 43](#)



## CHAPTER 4

# Firefly Perimeter Configuration and Management Tools

- Firefly Perimeter Configuration and Management Tools on page 39

## Firefly Perimeter Configuration and Management Tools

---

- Understanding Junos OS CLI and Junos Scripts on page 39
- Understanding J-Web Interface on page 39
- Understanding Junos Space Virtual Director on page 40
- Understanding Junos Space Security Director on page 41

### Understanding Junos OS CLI and Junos Scripts

Junos OS CLI is a Juniper Networks specific command shell that runs on top of a UNIX-based operating system kernel.

For detailed information, see

[https://www.juniper.net/techpubs/en\\_US/release-independent/junos/topics/concept/ex-series-cli-interface-overview.html](https://www.juniper.net/techpubs/en_US/release-independent/junos/topics/concept/ex-series-cli-interface-overview.html).

Built into the Junos OS, Junos script automation is an onboard toolset available on all Junos OS platforms, including routers, switches, and security devices.

For detailed information, see

<http://www.juniper.net/in/en/community/junos/script-automation/#overview>.

You can use the Junos OS CLI and the Junos OS scripts to configure, manage, administer, and troubleshoot Firefly Perimeter.

### Understanding J-Web Interface

The J-Web interface allows you to monitor, configure, troubleshoot, and manage the routing platform by means of a Web browser. J-Web provides access to all the configuration statements supported by the routing platform.

For detailed information, see [http://www.juniper.net/techpubs/en\\_US/junos12.1/information-products/pathway-pages/jweb/jweb.html](http://www.juniper.net/techpubs/en_US/junos12.1/information-products/pathway-pages/jweb/jweb.html).

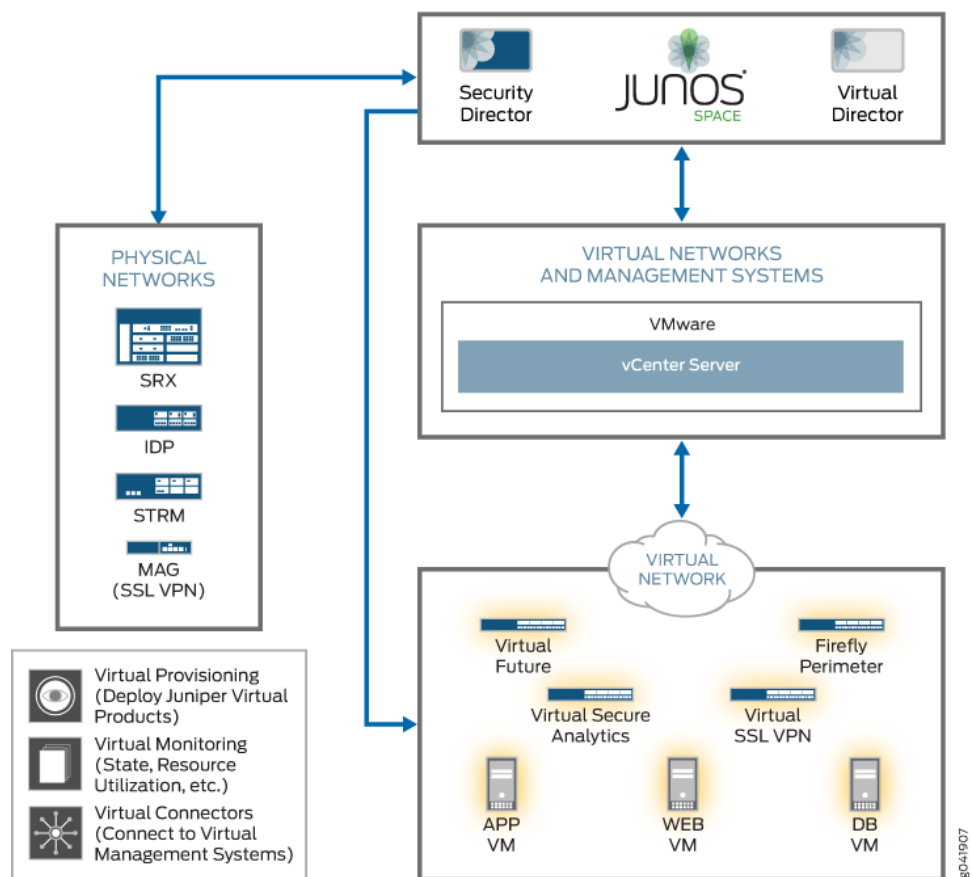
You can use J-Web to configure, manage, administer and troubleshoot Firefly Perimeter.

## Understanding Junos Space Virtual Director

Junos Space Virtual Director is dedicated to provisioning, bootstrapping, monitoring, and lifecycle management of a variety of Juniper virtual appliances and related virtual security solutions. Virtual Director can be used to deploy, manage, and monitor instances of Firefly Perimeter, which provides security and networking services at the perimeter in a virtualized private or public cloud environment. Virtual Director also registers each instance of Firefly Perimeter with the Junos Space Platform to allow other Junos Space applications, such as Security Director, to configure security policies.

Figure 11 on page 40 illustrates the Virtual Director topology.

Figure 11: Virtual Director Topology



Virtual Director supports Firefly Perimeter on VMware and offers the following lifecycle management features for Firefly Perimeter:

- **Provisioning**—Provides support for multiple vCenters, imports a Firefly Perimeter image file into VMware, and uses templates to build instances.
- **Bootstrapping**—Injects settings into the newly instantiated virtual machine so that it can be managed and registered into Junos Space automatically.

- Basic Monitoring—Groups the deployed Firefly Perimeter instances and displays the details of instances and resources.

2

For information regarding deploying VM templates using Virtual Director, see *Junos Space Virtual Director Getting Started Guide*.

## Understanding Junos Space Security Director

Managing enterprise security policy has become extremely complex. The growth in network traffic, including mobile traffic and BYOD, and the emergence of cloud services, have combined into a new array of opportunities for malicious hackers.

Security management can become error-prone and time-consuming if management solutions are slow, difficult to use, or restricted in their granularity of control. Resulting misconfigurations can make the enterprise vulnerable to threats and noncompliant with regulations and policies.

As one of the Junos Space Management Applications, Junos Space Security Director\* helps organizations improve the reach, ease, and accuracy, of security policy administration with a scalable, GUI-based management tool. It automates security provisioning through one centralized web-based interface to help administrators manage all phases of security policy lifecycle more quickly and intuitively, from policy creation to remediation.

For additional information, see

<http://www.juniper.net/us/en/products-services/network-management/junos-space-applications/security-director/#overview>.

### Related Documentation

- [Understanding Firefly Perimeter on page 3](#)
- *Installing Firefly Perimeter with VMware vSphere Client*



## CHAPTER 5

# Firefly Perimeter Management

- [Monitoring and Managing Firefly Perimeter Instances Using Junos Space Virtual Director on page 43](#)
- [Managing Security Policies for VM Using Junos Space Security Director on page 44](#)

### Monitoring and Managing Firefly Perimeter Instances Using Junos Space Virtual Director

Once the Firefly Perimeter instance is deployed within the virtual machine host provider, Virtual Director monitors and displays the virtual machine characteristics of each instance. On the Virtual Director user interface, when you click a particular virtual machine from the list, Virtual Director will display all the configured attributes for that virtual machine, a snapshot of all the performance data, and a snapshot of the statistical performance data for the Firefly Perimeter.

When the user clicks the group name for the group of virtual machines, Virtual Director will display a table of all data for the virtual machines in that group. Virtual Director will monitor and display information such as virtual machine status, memory allocated, number of vCPUs, number of vNICs, folder, host, data center, resource pool, CPU usage, and memory usage.

For the configured attribute changes, the monitoring module will receive a notification from the virtualization provider and the cache will be updated with the new changes.

Switch to monitor perspective by selecting **Virtual Director > Monitor Devices > VM Connection Status** to view the virtual device connection status.

This topic includes:

- [Viewing Connection Status on page 44](#)
- [Discover Devices on page 44](#)

## Viewing Connection Status

To view the connection status of a virtual device:

1. Select **Virtual Director > Monitor Devices > VM Connection Status**.

The virtual machine connection status page displays a list of all the virtual machines, and provides details such as host, vCenter, data center, cluster, and resource pool. Use the Columns Cascading menu to select the attribute to appear on the inventory table. You can then monitor the status of a virtual device for the selected attributes.

## Discover Devices

To discover a device:

1. Select **Virtual Director > Monitor Devices > VM Connection Status**.
2. Click **Actions > Discover Device** on the inventory page banner.

The Configure VM Instances for Discovery page appears.

3. Enter the IP, Subnet, and Root Password.
4. Click **Submit** to configure the virtual machine instance.

### Related Documentation

- *Junos Space Virtual Director Getting Started Guide*.
- [Understanding Firefly Perimeter on page 3](#)
- [Firefly Perimeter Configuration and Management Tools on page 39](#)

---

## Managing Security Policies for VM Using Junos Space Security Director

Managing enterprise security policy has become extremely complex. The growth in network traffic, including mobile traffic and BYOD, and the emergence of cloud services, have combined into a new array of opportunities for malicious hackers.

Security management can become error-prone and time-consuming if management solutions are slow, difficult to use, or restricted in their granularity of control. Resulting misconfigurations can make the enterprise vulnerable to threats and noncompliant with regulations and policies.

As one of the Junos Space Management Applications, Junos Space Security Director\* helps organizations improve the reach, ease, and accuracy, of security policy administration with a scalable, GUI-based management tool. It automates security provisioning through one centralized web-based interface to help administrators manage all phases of security policy lifecycle more quickly and intuitively, from policy creation to remediation:

For additional information, see

<http://www.juniper.net/us/en/products-services/network-management/junos-space-applications/security-director/#overview>



For information pertaining to managing security policies for VM, using Junos Space Security Director, see:

[http://www.juniper.net/techpubs/en\\_US/junos-space13.1/  
junos-space-security-design-sub-index.html](http://www.juniper.net/techpubs/en_US/junos-space13.1/junos-space-security-design-sub-index.html)

**Related  
Documentation**

- [Understanding Firefly Perimeter on page 3](#)



## PART 4

# Index

- [Index on page 49](#)



# Index

## Symbols

#, comments in configuration statements.....	xi
( ), in syntax descriptions.....	xi
< >, in syntax descriptions.....	x
[ ], in configuration statements.....	xi
{ }, in configuration statements.....	xi
(pipe), in syntax descriptions.....	xi

## B

Basic Settings	
Firefly.....	6
braces, in configuration statements.....	xi
brackets	
angle, in syntax descriptions.....	x
square, in configuration statements.....	xi

## C

comments, in configuration statements.....	xi
Configuration	
Firefly	
CLI Interface.....	16
J-Web Interface.....	12
conventions	
text and syntax.....	x
curly braces, in configuration statements.....	xi
customer support.....	xi
contacting JTAC.....	xi

## D

documentation	
comments on.....	xi

## F

Firefly Perimeter	
administer.....	39
configure.....	39
manage.....	39
troubleshoot.....	39
font conventions.....	x

## I

Installation Requirements	
Firefly.....	7

## M

manuals	
comments on.....	xi
Monitoring.....	43

## P

parentheses, in syntax descriptions.....	xi
--	----

## S

Specifications	
Firefly.....	5
support, technical See technical support	
syntax conventions.....	x

## T

technical support	
contacting JTAC.....	xi

## U

Understanding	
Firefly.....	3

