

# Firefly Perimeter Getting Started Guide for KVM



---

Published: 2014-02-16

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 Getting Started Guide for KVM*

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
	Understanding Firefly Perimeter with KVM . . . . .	3
	Features Supported on Firefly Perimeter with KVM . . . . .	4
<b>Chapter 2</b>	<b>System Requirements . . . . .</b>	<b>27</b>
	System Requirements for Firefly Perimeter with KVM . . . . .	27
	Firefly Perimeter Installation Specifications . . . . .	27
	Supported KVM Hypervisors for Firefly Perimeter . . . . .	29
	Firefly Perimeter Basic Settings . . . . .	29
<b>Part 2</b>	<b>Installation</b>	
<b>Chapter 3</b>	<b>Firefly Perimeter Installation . . . . .</b>	<b>33</b>
	Installing Firefly Perimeter with KVM . . . . .	33
	Downloading the Firefly Perimeter JVA Package and Deploying Firefly Perimeter Instances . . . . .	33
<b>Part 3</b>	<b>Configuration</b>	
<b>Chapter 4</b>	<b>Firefly Perimeter Configurations . . . . .</b>	<b>39</b>
	Firefly Perimeter Configuration Using the J-Web Interface . . . . .	39
	Accessing the J-Web Interface and Configuring Firefly Perimeter . . . . .	39
	Applying the Configuration . . . . .	42
	Firefly Perimeter Configuration Using the CLI Interface . . . . .	43
<b>Part 4</b>	<b>Index</b>	
	Index . . . . .	49



# List of Figures

<b>Part 3</b>	<b>Configuration</b>	
<b>Chapter 4</b>	<b>Firefly Perimeter Configurations</b>	<b>39</b>
	Figure 1: J-Web Setup Wizard Page	39
	Figure 2: J-Web Configuration Page	40
	Figure 3: Firefly Perimeter Configuration Summary	42



# 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 1</b>	<b>Firefly Perimeter Overview</b> . . . . .	<b>3</b>
	Table 3: Features Supported on Firefly Perimeter . . . . .	4
	Table 4: Firefly Feature Support Information . . . . .	24
<b>Chapter 2</b>	<b>System Requirements</b> . . . . .	<b>27</b>
	Table 5: Specifications for Firefly Perimeter . . . . .	27
	Table 6: Hardware Specifications for Host Machine . . . . .	27
	Table 7: Supported Versions of KVM hypervisor . . . . .	29
	Table 8: Supported Version of Operating System . . . . .	29
	Table 9: Basic Settings for Interfaces . . . . .	30
	Table 10: Basic Settings for Security Policies . . . . .	30
	Table 11: Basic Settings for NAT Rule . . . . .	30
<b>Part 2</b>	<b>Installation</b>	
<b>Chapter 3</b>	<b>Firefly Perimeter Installation</b> . . . . .	<b>33</b>
	Table 12: Options for Firefly Perimeter VM . . . . .	34
<b>Part 3</b>	<b>Configuration</b>	
<b>Chapter 4</b>	<b>Firefly Perimeter Configurations</b> . . . . .	<b>39</b>
	Table 13: Device Name and User Account Information . . . . .	41
	Table 14: System Time Options . . . . .	41





# 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>
<code>Fixed-width text like this</code>	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 27](#)



## CHAPTER 1

# Firefly Perimeter Overview

- [Understanding Firefly Perimeter on page 3](#)
- [Understanding Firefly Perimeter with KVM on page 3](#)
- [Features Supported on Firefly Perimeter with KVM on page 4](#)

## 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*
- [Firefly Perimeter Basic Settings on page 29](#)
- *Installation Requirements for Firefly Perimeter with VMware*

## Understanding Firefly Perimeter with KVM

---

The kernel-based virtual machine (KVM) is a virtualization infrastructure that is used for the Linux kernel. KVM is an open source software that can be used to create multiple VMs and to install security and networking appliances.

The basic components of KVM include:

- A loadable kernel module that provides the basic virtualization infrastructure
- A processor-specific module

When loaded into the Linux kernel, the KVM software acts like a hypervisor. KVM supports multitenancy and allows multiple VMs to run concurrently on its host, whose resources it manages and shares. Every VM has its distinct virtualized hardware.

**Related  
Documentation**

- [Understanding Firefly Perimeter on page 3](#)
- [Installing Firefly Perimeter with KVM on page 33](#)

## Features Supported on Firefly Perimeter with KVM

Firefly Perimeter inherits many features from the SRX Series product line. However, because some SRX Series features are not directly applicable in a virtualized environment, they have been excluded from the Firefly Perimeter product line. [Table 3 on page 4](#) describes the available features on Firefly Perimeter as of Junos OS Release 12.1X46-D10. For feature roadmap details, contact your Juniper Networks representative.

**Table 3: Features Supported on Firefly Perimeter**

Feature	Support on Firefly Perimeter
<b>Address Books and Address Sets:</b>	
Address books	Yes
Address sets	Yes
Global address objects or sets	Yes
Nested address groups	Yes
<b>Administrator Authentication:</b>	
Local authentication	Yes
RADIUS	Yes
TACACS+	Yes
<b>Alarms:</b>	
Chassis alarms	Yes
Interface alarms	Yes
System alarms	Yes



Table 3: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
<b>Application Layer Gateways:</b>	
DNS ALG	Yes
DNS doctoring support	No
DNS, FTP, RTSP, and TFTP ALGs (Layer 2) with chassis clustering	No
DSCP marking for SIP, H.323, MGCP, and SCCP ALGs	Yes
FTP	Yes
H.323	Yes
Avaya H.323	Yes
IKE	Yes
MGCP	Yes
PPTP	Yes
RSH	Yes
RTSP	Yes
SCCP	Yes
SIP	Yes
SIP ALG–NEC	Yes
SQL	Yes
MS RPC	Yes
SUN RPC	Yes
TALK	Yes
TFTP	Yes
<b>Attack Detection and Prevention:</b>	
Bad IP option	Yes
Block fragment traffic	Yes

Table 3: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
FIN flag without ACK flag set protection	Yes
ICMP flood protection	Yes
ICMP fragment protection	Yes
IP address spoof	Yes
IP address sweep	Yes
IP record route option	Yes
IP security option	Yes
IP stream option	Yes
IP strict source route option	Yes
IP timestamp option	Yes
Land attack protection	Yes
Large size ICMP packet protection	Yes
Loose source route option	Yes
Ping of death attack protection	Yes
Port scan	Yes
Source IP-based session limit	Yes
SYN-ACK-ACK proxy protection	Yes
SYN and FIN flags set protection	Yes
SYN flood protection	Yes
SYN fragment protection	Yes
TCP address sweep	Yes
TCP packet without flag set protection	Yes
Teardrop attack protection	Yes

Table 3: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
UDP address sweep	Yes
UDP flood protection	Yes
Unknown IP protocol protection	Yes
Whitelist for SYN flood screens	Yes
WinNuke attack protection	Yes
<b>Autoinstallation:</b>	
Autoinstallation	Yes
<b>Class of Service:</b>	
Classifiers	Yes
Code-point aliases	Yes
Egress interface shaping	Yes
Forwarding classes	Yes
High-priority queue on Services Processing Card	No
Ingress interface policer	Yes
Schedulers	Yes
Simple filters	Yes
Transmission queues	Yes
Tunnels	Yes
<b>NOTE:</b> GRE and IP-IP tunnels only.	
Virtual channels	Yes
<b>Diagnostics Tools:</b>	
CLI terminal	Yes
Flow monitoring cflowd version 5 and flow monitoring cflowd version 8	Yes
Flow monitoring cflowd version 9	No

Table 3: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
Ping host	Yes
Ping MPLS	Yes
Traceroute	Yes
Ping Ethernet (CFM)	No
Traceroute Ethernet (CFM)	No
<b>DNS Proxy:</b>	
DNS proxy cache	Yes
DNS proxy with split DNS	Yes
Dynamic DNS	No
<b>Dynamic Host Configuration Protocol:</b>	
DHCPv6 client	No
DHCPv4 client	Yes
DHCPv6 relay agent	No
DHCPv4 relay agent	Yes
DHCPv6 server	Yes
DHCPv4 server	Yes
DHCP server address pools	Yes
DHCP server static mapping	Yes
<b>Ethernet Link Aggregation:</b>	
<b>Routing mode:</b>	
LACP in chassis cluster pair	No
LACP in standalone device	No
Layer 3 LAG on routed ports	No
Static LAG in chassis cluster mode	No

Table 3: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
Static LAG in standalone mode	No
<b>Ethernet Link Fault Management:</b>	
<b>Interfaces supported:</b>	
LACP in chassis cluster pair	No
LACP in standalone mode	No
Static LAG in chassis cluster mode	No
Static LAG in standalone mode	No
<b>Physical interface (encapsulations):</b>	
ethernet-ccc	No
extended-vlan-ccc	No
ethernet-tcc	No
extended-vlan-tcc	No
<b>Interface family:</b>	
inet	Yes
mpls	Yes
ccc	No
tcc	No
iso	Yes
ethernet-switching	No
inet6	Yes
<b>Aggregated Ethernet interface:</b>	
Static LAG	No
LACP enabled LAG	No
<b>Interface family:</b>	

Table 3: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
ethernet-switching	No
inet	Yes
inet6	Yes
iso	Yes
mpls	Yes
<b>File Management:</b>	
Clean up unnecessary files	Yes
Delete backup software image	Yes
Delete individual files	Yes
Download system files	Yes
Encrypt/decrypt configuration files	Yes
Manage account files	Yes
Rescue	Yes
System zeroize	Yes
Monitor start	Yes
Archive files	Yes
Calculate checksum	Yes
Compare files	Yes
Rename files	Yes
<b>Firewall Authentication:</b>	
Firewall authentication on Layer 2 transparent authentication	No
LDAP authentication server	Yes
Local authentication server	Yes
Pass-through authentication	Yes

Table 3: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
RADIUS authentication server	Yes
SecurID authentication server	Yes
Web authentication	Yes
<b>Flow-Based and Packet-Based Processing:</b>	
Alarms and auditing	Yes
End-to-end packet debugging	No
Flow-based processing	Yes
Network processor bundling	No
Packet-based processing	Yes
Selective stateless packet-based services	Yes
<b>Interfaces:</b>	
<b>Physical and Virtual Interface:</b>	
Ethernet interface	Yes
Gigabit Ethernet interface	Yes
<b>Services:</b>	
Aggregated Ethernet interface	No
GRE interface	Yes
IEEE 802.1X dynamic VLAN assignment	No
IEEE 802.1X MAC bypass	No
IEEE 802.1X port-based authentication control with multisuppliant support	No
Interleaving using MLFR	No
Internally configured interface used by the system as a control path between the WXC Integrated Services Module and the Routing Engine	No
Internally generated GRE interface (gr-0/0/0)	Yes

Table 3: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
Internally generated IP-over-IP interface (ip-0/0/0)	Yes
Internally generated link services interface	Yes
Internally generated Protocol Independent Multicast de-encapsulation interface	Yes
Internally generated Protocol Independent Multicast encapsulation interface	Yes
Link fragmentation and interleaving interface	Yes
Link services interface	Yes
Loopback interface	Yes
Management interface	Yes
PPP interface	No
PPPoE-based radio-to-router protocol	No
PPPoE interface	No
Promiscuous mode on interfaces	Yes  <b>NOTE:</b> Promiscuous mode needs to be enabled on hypervisor.
Secure tunnel interface	Yes
<b>IP Monitoring:</b>	
IP monitoring with route failover (for standalone devices and redundant Ethernet interfaces)	Yes
IP monitoring with interface failover (for standalone devices)	Yes
Track IP enhancements (IP Monitoring using RPM)	No
<b>IP Security:</b>	
Acadia - Clientless VPN	No
AH protocol	Yes
Alarms and auditing	Yes



Table 3: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
Antireplay (packet replay attack prevention)	Yes
Authentication	Yes
Authentication Header (AH)	Yes
Autokey management	Yes
Automated certificate enrollment using SCEP	Yes
Automatic generation of self-signed certificates	Yes
Bridge domain and transparent mode	No
Certificate - Configure local certificate sent to peer	Yes
Certificate - Configure requested CA of peer certificate	Yes
Certificate - Encoding: PKCS7, X509, PEM, DERs	Yes
Certificate - RSA signature	Yes
Chassis clusters (active/backup and active/active)	No
Class of service	Yes
CRL update at user-specified interval	Yes
Config Mode (draft-dukes-ike-mode-cfg-03)	Yes
Dead peer detection (DPD)	Yes
Diffie-Hellman (PFS) Group 1	Yes
Diffie-Hellman (PFS) Group 2	Yes
Diffie-Hellman (PFS) Group 5	Yes
Diffie-Hellman Group 1	Yes
Diffie-Hellman Group 2	Yes
Diffie-Hellman Group 5	Yes
Digital signature generation	Yes

Table 3: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
Dynamic IP address	Yes
Dynamic IPsec VPNs	No
Encapsulating Security Payload (ESP) protocol	Yes
Encryption algorithms 3DES	Yes
Encryption algorithms AES 128, 192, and 256	Yes
Encryption algorithms DES	Yes
Encryption algorithms NULL (authentication only)	Yes
Entrust, Microsoft, and Verisign certificate authorities (CAs)	Yes
External Extended Authentication (Xauth) to a RADIUS server for remote access connections	Yes
Group Encrypted Transport (GET VPN)	No
Group VPN with dynamic policies	No
Hard lifetime limit	Yes
Hardware IPsec (bulk crypto) Cavium/RMI	No
Hash algorithms MD5	Yes
Hash algorithms SHA-1	Yes
Hash algorithms SHA-2 (SHA-256)	Yes
Hub & spoke VPN	Yes
Idle timers for IKE	Yes
Improvements in VPN debug capabilities	Yes
Initial contact	Yes
Invalid SPI response	Yes
IKE Diffie-Hellman Group 14 support	Yes
IKE Phase 1	Yes

Table 3: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
IKE Phase 1 lifetime	Yes
IKE Phase 2	Yes
IKE Phase 2 lifetime	Yes
IKE and IPsec predefine proposal sets to work with dynamic VPN client	No
IPsec tunnel termination in routing-instances	Yes
IKE support	Yes
IKEv1	Yes
IKEv1 authentication, preshared key	Yes
IKEv2	Yes
Local IP address management - VPN XAuth support	Yes
Local IP address management support for DVPN	No
Manual installation of DER-encoded and PEM-encoded CRLs	Yes
Manual key management	Yes
Manual proxy-ID (Phase 2 ID) configuration	Yes
NHTB - Next Hop Tunnel Binding	Yes
New IPsec Phase 2 authentication algorithm	Yes
Online CRL retrieval through LDAP and HTTP	Yes
Package dynamic VPN client	No
Policy-based VPN	Yes
Preshared key (PSK)	Yes
Prioritization of IKE packet processing	Yes
Reconnect to dead IKE peer	Yes
Remote access	Yes

**Table 3: Features Supported on Firefly Perimeter (*continued*)**

Feature	Support on Firefly Perimeter
Remote access user IKE peer	Yes
Remote access user-group IKE peer - group IKE ID	Yes
Route-based VPN	Yes
SHA-2 IPsec support	Yes
Soft lifetime	Yes
Static IP address	Yes
Suites: standard, compatible, basic, and custom-created	Yes
Support for NHTB when the st0.x interface is bound to a routing instance	Yes
Support for remote access peers with shared IKE identity + mandatory XAuth	Yes
Support group IKE IDs for dynamic VPN configuration	No
TOS/DSCP honoring/coloring (inner/outer)	Yes
Tunnel mode with clear/copy/set Don't Fragment bit	Yes
UAC Layer 3 enforcement	Yes
Virtual router support for route-based VPNs	Yes
VPN monitoring (proprietary)	Yes
X.509 encoding for IKE	Yes
XAuth (draft-beaulieu-ike-xauth-03)	Yes
<b>IPv6 Support:</b>	
<b>Flow-based forwarding and security features:</b>	
Advanced flow	Yes
DS-Lite concentrator (aka AFTR)	No
DS-Lite initiator (aka B4)	No
Firewall filters	Yes

Table 3: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
Forwarding option: flow mode	Yes
Multicast flow	Yes
Screens	Yes
Security policy (firewall)	Yes
Security policy (IDP)	No
Security policy (user role firewall)	No
Zones	Yes
<b>IPv6 ALG support for FTP:</b> Routing, NAT, NAT-PT support	Yes
<b>IPv6 ALG support for ICMP:</b> Routing, NAT, NAT-PT support	Yes
<b>IPv6 NAT:</b> NAT-PT, NAT support	Yes
IPv6 NAT64	Yes
<b>IPv6--related protocols:</b> BFD, BGP, ECMPv6, ICMPv6, ND, OSPFv3, RIPng	Yes
IPv6 ALG support for TFTP	Yes
<b>System services:</b> DHCPv6, DNS, FTP, HTTP, ping, SNMP, SSH, syslog, Telnet, traceroute	Yes
<b>Packet-based forwarding and security features:</b>	
Class of service	Yes
Firewall filters	Yes
Forwarding option: packet mode	Yes
<b>IPv6 IP Security:</b>	

Table 3: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
4in4 and 6in6 policy-based site-to-site VPN, AutoKey IKEv1	No
4in4 and 6in6 policy-based site-to-site VPN, manual key	No
4in4 and 6in6 route-based site-to-site VPN, AutoKey IKEv1	No
4in4 and 6in6 route-based site-to-site VPN, manual key	No
<b>Log File Formats:</b>	
<b>System (control plane) log file formats:</b>	
Binary format (binary)	No
Structured syslog (sd-syslog)	Yes
Syslog (syslog)	Yes
WebTrends Enhanced Log Format (WELF)	No
<b>Security (data plane) log file formats:</b>	
Binary format (binary)	Yes
Structured syslog (sd-syslog)	Yes
Syslog (syslog)	Yes
WebTrends enhanced log format (WELF)	Yes
<b>MPLS:</b>	
CCC and TCC	No
CLNS	Yes
Interprovider and carrier-of-carriers VPNs	Yes
Layer 2 VPNs for Ethernet connections	Yes  <b>NOTE:</b> Promiscuous mode needs to be enabled on hypervisor.
Layer 3 MPLS VPNs	Yes
LDP	Yes

Table 3: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
MPLS VPNs with VRF tables on provider edge routers	Yes
Multicast VPNs	Yes
OSPF and IS-IS traffic engineering extensions	Yes
P2MP LSPs	Yes
RSVP	Yes
Secondary and standby LSPs	Yes
Standards-based fast reroute	Yes
<b>Multicast:</b>	
Filtering PIM register messages	Yes
IGMP	Yes
PIM RPF routing table	Yes
Primary routing mode (dense mode for LAN and sparse mode for WAN)	Yes
Protocol Independent Multicast Static RP	Yes
Session Announcement Protocol (SAP)	Yes
SDP	Yes
<b>Multicast VPN:</b>	
Basic multicast features in C-instance	Yes
Multicast VPN membership discovery with BGP	Yes
P2MP LSP support	Yes
P2MP OAM - P2MP LSP ping	Yes
Reliable multicast VPN routing information exchange	Yes
<b>Network Address Translation:</b>	
Destination IP address translation	Yes
Disabling source NAT port randomization	Yes

**Table 3: Features Supported on Firefly Perimeter (*continued*)**

Feature	Support on Firefly Perimeter
Interface source NAT pool port	Yes
NAT address pool utilization threshold status	Yes
NAT traversal (NAT-T) for site-to-site IPsec VPNs (IPv4)	Yes
Persistent NAT	Yes
Persistent NAT binding for wildcard ports	Yes
Persistent NAT hairpinning	Yes
Maximize persistent NAT bindings	No
Pool translation	Yes
Proxy ARP (IPv4)	Yes
Proxy NDP (IPv6)	Yes
Removing persistent NAT query bindings	Yes
Rule-based NAT	Yes
Rule translation	Yes
Source address and group address translation for multicast flows	Yes
Source IP address translation	Yes
Static NAT	Yes
<b>Network Operations and Troubleshooting:</b>	
Event policies	Yes
Event scripts	Yes
Operation scripts	Yes
XSLT commit scripts	Yes
<b>Network Time Protocol:</b>	
NTP support	Yes
<b>Packet Capture:</b>	



Table 3: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
Packet capture	Yes
<p><b>NOTE:</b> Packet capture, in this context, refers to standard interface packet capture. It is not part of the IDP. Packet capture is supported only on physical interfaces and tunnel interfaces; for example, <i>gr</i>, <i>ip</i>, <i>st0</i>, <i>lsq</i>-/ls-. Packet capture is not supported on redundant Ethernet interfaces (<i>reth</i>).</p>	
<b>Real-Time Performance Monitoring Probe:</b>	
RPM probe	Yes
One-way timestamps	Yes
<b>Routing:</b>	
BGP	Yes
BGP extensions for IPv6	Yes
BGP Flowspec	No
Compressed Real-Time Transport Protocol (CRTP)	No
ECMP flow-based forwarding	No
Internet Group Management Protocol (IGMP)	Yes
IPv4 options and broadcast Internet diagrams	Yes
IPv6 routing, forwarding, global address configuration, and Internet Control Message Protocol (ICMP)	Yes
IS-IS	Yes
Multiple virtual routers	Yes
Neighbor Discovery Protocol (NDP) and Secure NDP	Yes
OSPF v2	Yes
OSPF v3	Yes
RIP next generation (RIPng)	Yes
RIP v1, v2	Yes
Static routing	Yes

**Table 3: Features Supported on Firefly Perimeter (*continued*)**

Feature	Support on Firefly Perimeter
Virtual Router Redundancy Protocol (VRRP)	Yes
<b>Secure Web Access:</b>	
CAs	Yes
HTTP	Yes
HTTPS	Yes
<b>Security Policy Support:</b>	
Address books/address sets	Yes
Custom policy applications	Yes
Global policy	Yes
Policy application timeouts	Yes
Policy applications and application sets	Yes
Policy hit-count tracking	Yes
Schedulers	Yes
Security policies for self-traffic	Yes
SSL proxy	No
User role firewall	No
Common predefined applications	Yes
Shadow policy	Yes
<b>Security Zone:</b>	
Functional zone	Yes
Security zone	Yes
<b>Session Logging:</b>	
Accelerating security and traffic logging	Yes
Aggressive session aging	Yes
Getting information about sessions	Yes

Table 3: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
Logging to a single server	Yes
Session logging with NAT information	Yes
<b>SMTP:</b>	
SMTP support	Yes
<b>SNMP:</b>	
SNMP support	Yes
<b>Stateless Firewall Filters:</b>	
Stateless firewall filters (ACLs)	Yes
Stateless firewall filters (simple filter)	No
<b>System Log Files:</b>	
Archiving system logs	Yes
Configuring system log messages	Yes
Disabling system logs	Yes
Filtering system log messages	Yes
Multiple system log servers (control-plane logs)	Yes
Sending system log messages to a file	Yes
Sending system log messages to a user terminal	Yes
Viewing data plane logs	Yes
Viewing system log messages	Yes
<b>Upgrading and Rebooting:</b>	
Autorecovery	No
Boot device configuration	No (N.A.)
Boot device recovery	No (N.A.)
Chassis components control	Yes
Chassis restart	Yes

**Table 3: Features Supported on Firefly Perimeter (*continued*)**

Feature	Support on Firefly Perimeter
Download manager	Yes
Dual-root partitioning	No
In-band cluster upgrade	No
Low-impact cluster upgrades	No
Software upgrades and downgrades	Yes
<b>User Interfaces:</b>	
CLI	Yes
J-Web user interface	Yes
Junos XML protocol	Yes
Network and Security Manager	No
Junos Space Security Director	Yes
SRC application	No
Junos Space Virtual Director	Yes
<b>Authentication with IC Series Devices</b>	
Captive Portal	Yes
Junos OS Enforces in UAC deployments	Yes
<b>VPLS</b>	
Filtering and Policing (Packet-Based)	Yes

[Table 4 on page 24](#) lists additional features that are not supported on Firefly.

**Table 4: Firefly Feature Support Information**

Feature	Firefly
Application Identification (Junos OS)	No
Authentication with IC Series Devices	No
General Packet Radio Service	No

Table 4: Firefly Feature Support Information (*continued*)

Feature	Firefly
Intrusion Detection and Prevention	No
Layer 2 Mode	No
Logical Systems	No
Power over Ethernet	No
Public Key Infrastructure	No
Remote Device Access	No
Route Reflector	No
RPM Probe	No
Services Offloading	No
Transparent Mode	No
Unified Threat Management	No
USB Modem	No
Voice over Internet Protocol with Avaya	No
Wireless Local Area Network	No
Group VPN	No
Multicast for AutoVPN	No
Dynamic VPN (DVPN).	No

**Related  
Documentation**

- [Understanding Firefly Perimeter on page 3](#)
- [Specifications for Firefly Perimeter Installation](#)
- [Firefly Perimeter Basic Settings on page 29](#)



## CHAPTER 2

# System Requirements

- [System Requirements for Firefly Perimeter with KVM on page 27](#)
- [Firefly Perimeter Basic Settings on page 29](#)

### System Requirements for Firefly Perimeter with KVM

---

- [Firefly Perimeter Installation Specifications on page 27](#)
- [Supported KVM Hypervisors for Firefly Perimeter on page 29](#)

### Firefly Perimeter Installation Specifications

[Table 5 on page 27](#) lists the specifications for Firefly Perimeter.

**Table 5: Specifications for Firefly Perimeter**

Component	Specification
Memory	2 GB
Disk space	2 GB
vCPUs	2
vNICs	Up to 10
Virtual NIC type	Virtio (default)

**NOTE:** No chassis cluster support available for Virtio.

[Table 6 on page 27](#) lists the hardware specifications for the host machine that runs Firefly Perimeter VM.

**Table 6: 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 a multi-core CPU.

---



## Supported KVM Hypervisors for Firefly Perimeter

Table 7 on page 29 lists the supported versions of KVM hypervisors for Firefly Perimeter.

**Table 7: Supported Versions of KVM hypervisor**

KVM Hypervisor	Hypervisor Version	Download Link
Bash	Not Applicable	<a href="http://www.gnu.org/software/bash/">http://www.gnu.org/software/bash/</a> .
KVM	0.12.1	<a href="http://wiki.qemu.org/Download">http://wiki.qemu.org/Download</a> .
Libvirt	0.9.10	<a href="http://libvirt.org/downloads.html#releases">http://libvirt.org/downloads.html#releases</a> .
Virsh (mandatory)	Not Applicable	<a href="http://libvirt.org/virshcmdref.html#downloading">http://libvirt.org/virshcmdref.html#downloading</a> .
Virt-manager (Recommended)	Not Applicable	<a href="http://virt-manager.org/download.html">http://virt-manager.org/download.html</a> .

Table 8 on page 29 lists the supported operating system version for Firefly Perimeter with KVM.

**Table 8: Supported Version of Operating System**

Operating System	Operating System Version
CentOS	6.3

### Related Documentation

- [Understanding Firefly Perimeter on page 3](#)
- [Firefly Perimeter Basic Settings on page 29](#)

## 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 9 on page 30 lists the basic settings for interfaces.

**Table 9: 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 10 on page 30 lists the basic settings for the security policies.

**Table 10: Basic Settings for Security Policies**

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

Table 11 on page 30 lists the basic settings for the NAT rule.

**Table 11: 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*
- *Installation Requirements for Firefly Perimeter with VMware*

## PART 2

# Installation

- [Firefly Perimeter Installation on page 33](#)



## CHAPTER 3

# Firefly Perimeter Installation

- Installing Firefly Perimeter with KVM on page 33

## Installing Firefly Perimeter with KVM

---

- Downloading the Firefly Perimeter JVA Package and Deploying Firefly Perimeter Instances on page 33

## Downloading the Firefly Perimeter JVA Package and Deploying Firefly Perimeter Instances

1. Download the Firefly Perimeter JVA package from the Juniper software download site.

<http://www.juniper.net/support/downloads/>.

The .jva file is a Firefly Perimeter self-extracting package file. It contains a disk image file of a Firefly Perimeter KVM virtual machine (VM) along with a VM XML template file. This package file can be used to deploy multiple VMs of Firefly Perimeter on a KVM hypervisor locally or remotely.

2. Make sure you have already installed KVM, QEmu and virsh and have configured the required virtual networks and storage pool.
3. Deploy the VM by executing the .jva file as a bash script. For example:

```
user@host>bash junos-vsrx-<version>-domestic.jva
```

- The following CLI command shows detailed instructions.

```
user@host>bash junos-vsrx-<version>-domestic.jva Firewall1 -i  
4::VNET1,VNET2,VNET3,VNET4 -s vm_storage
```

- This CLI command deploys a VM called Firewall1, which has four interfaces that are connected to four networks called VNET1, VNET2, VNET3 and VNET4, respectively. The image will be stored in a directory called **vm\_storage**.

[Table 12 on page 34](#) describes the options for the Firefly Perimeter VM.

- Deploy a Firefly Perimeter instance:

```
user@host>junos-vsrx-<version>-domestic.jva <VM name>[options].
```

A Firefly Perimeter virtual machine instance named <VM name> will be created.

Table 12: Options for Firefly Perimeter VM

Option	Description	Default Specification
<b>-i &lt;interface options&gt;</b>	Specifies network interfaces. The options are specified by a string consisting of three parts delimited by : (no spaces allowed).	NA
<b>&lt;number&gt;:&lt;driver type&gt;:&lt;virtual networks&gt;</b>		
<b>&lt;number&gt;</b>	Specifies number of vNICs.	2–10  If this information missing, a value of 2 is assumed.
<b>&lt;driver type&gt;</b>	Specifies the type of driver used.	virtio  If this information is unavailable, virtio is assumed.
<b>&lt;virtual networks&gt;</b>	Specifies a list of virtual network names separated by a comma. No spaces are allowed.	If this information is unavailable, default network is assumed.  See <a href="#">“Note” on page 35</a> .
<b>-r &lt;usr&gt;@&lt;host IP or DNS name&gt;</b>		
<b>&lt;usr&gt;</b>	Specifies the user who must be authorized to create VMs on the remote host.  User will create and deploy a Firefly Perimeter instance on a remote hypervisor host.	If this option is unavailable, the hypervisor host is assumed to be the local host and the user is assumed to be the current user.  <b>WARNING:</b> This tool uses ssh to access the remote host multiple times. Deploy ssh public key of the local host to the remote host to avoid repeatedly entering a password.
<b>-s &lt;storage name&gt;</b>	Specifies the storage in which the Firefly Perimeter instance's disk image will be stored.  The named storage must be managed by the hypervisor the Firefly instance will be hosted.	If this option is unavailable, the default storage of the host will be assumed.

**NOTE:**

- If the number of vnets listed equals the number of vNICs, vNICs will be added to the networks sequentially.

2:e1000:VNET1,VNET2

Two vNICs of e1000 type will be created for the Firefly VM. The first vNIC will be in VNET1, second in VNET2.

- If the number of vnets listed is greater than the number of vNICs, vNICs will also be added to the networks sequentially but remaining vnets will be ignored.

Example 1: 4::VNET1,VNET2,VNET3

Four vNICs of virtio type will be created for the Firefly VM. The first vNIC will be in VNET1, second in VNET2 and the last two vNICs in VNET3.

Example 2: 2:virtio:

Two vNICs of virtio type will be created for the Firefly VM. Both vNIC will be in the default vnet.

- If number of vnets listed is smaller than the number of vNICs, vNICs will be added to the networks sequentially but the remaining vNICs will be put into the last vnet in the list.

VNET1

Two vNICs of virtio type will be created for the Firefly VM. Both vNICs will be in VNET1.

The VM created hereby has only two network interfaces, both in the default virtual network. Edit the VM to change networks and/or add more interfaces to meet your networking requirements.

The VM can be managed and started up using various tools. Here is an example using virsh, which also allows you to make a connection to the console of the VM.

**virsh # list --all**

```
user@host> virsh # list --all
ID Name      State
-  vSRX-kvm-2  shut off
```

**virsh # start vSRX-kvm-2**

```
user@host>virsh # start vSRX-kvm-2
Domain vSRX-kvm-2 started
```

**virsh # list**

```
user@host> virsh # list
ID Name      State
2  vSRX-kvm-2  running
```

#### virsh # console vSRX-kvm-2

```
user@host>virsh # console vSRX-kvm-2  
Connected to domain vSRX-kvm-2
```

#### Related Documentation

- [Understanding Firefly Perimeter on page 3](#)
- [System Requirements for Firefly Perimeter with KVM on page 27](#)
- [Firefly Perimeter Basic Settings on page 29](#)



## PART 3

# Configuration

- [Firefly Perimeter Configurations on page 39](#)



## CHAPTER 4

# Firefly Perimeter Configurations

- Firefly Perimeter Configuration Using the J-Web Interface on page 39
- Firefly Perimeter Configuration Using the CLI Interface on page 43

## Firefly Perimeter Configuration Using the J-Web Interface

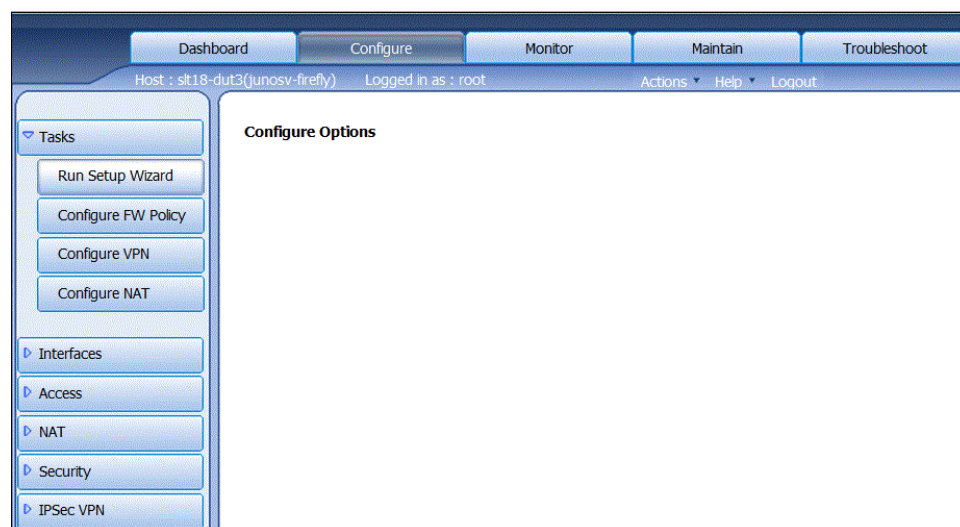
- Accessing the J-Web Interface and Configuring Firefly Perimeter on page 39
- Applying the Configuration on page 42

### 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 39](#).

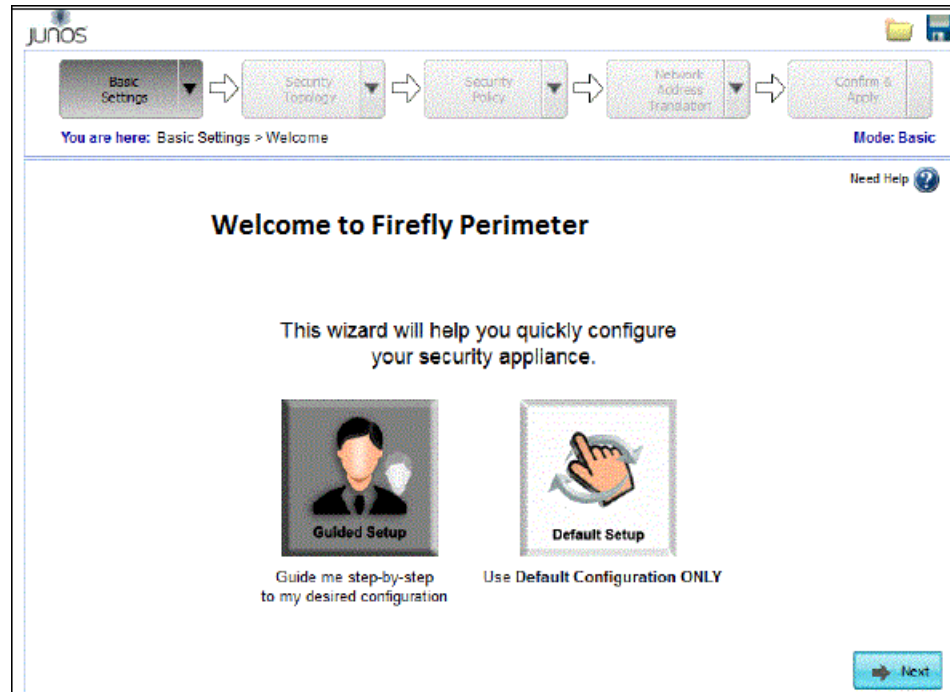
Figure 1: J-Web Setup Wizard Page



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 40](#).

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 13 on page 41](#).

- Device name and user account information

**Table 13: 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 14 on page 41](#) lists the system time options.

**Table 14: 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:

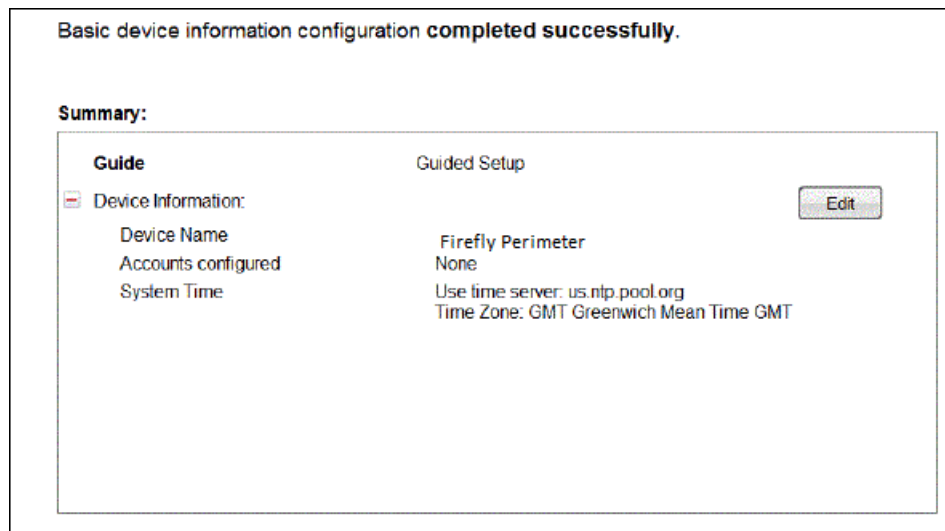
Select **Expert** to configure the basic options as well as the following advanced options:

- 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 42](#).

**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 29](#)
- [Powering On/Off the Device](#)
- [Firefly Perimeter Configuration Using the CLI Interface on page 43](#)

## 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 29](#)
- [Powering On/Off the Device](#)
- [Firefly Perimeter Configuration Using the J-Web Interface on page 39](#)



## 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.....	29
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.....	43
J-Web Interface.....	39
conventions	
text and syntax.....	x
curly braces, in configuration statements.....	xi
customer support.....	xi
contacting JTAC.....	xi

## D

documentation	
comments on.....	xi

## F

font conventions.....	x
-----------------------	---

## M

manuals	
comments on.....	xi

## P

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

## S

support, technical See technical support	
syntax conventions.....	x

## T

technical support	
contacting JTAC.....	xi

## U

Understanding	
Firefly.....	3

