

Release Notes: Firefly Perimeter

12.1X46-D25 Release Notes

Release 12.1X46-D25
28 March 2016
Revision 3

The Firefly Suite is designed to address the need for compelling and robust security for diverse virtualized environments by bringing together three products - Firefly Perimeter, Firefly Host, and Junos Space Virtual Director. These release notes accompany Release 12.1X46-D25 for Firefly Perimeter. They describe supported features and known issues with Firefly Perimeter.

For the latest, most complete information about outstanding and resolved issues with Firefly Perimeter, see the Juniper Networks online software defect search application at <http://www.juniper.net/prsearch>.

You can also find these release notes on the Firefly Perimeter Documentation webpage, which is located at <https://www.juniper.net/techpubs/firefly-perimeter>.

Contents

Release Notes for Firefly Perimeter	3
Upgrading from Prior Releases of Firefly Perimeter	3
Optional Instructions for Validating Security Signatures	3
Validating the Firefly Perimeter OVA Image	4
Validating the Firefly Perimeter JVA Image using Linux commands	6
Features Supported on Firefly Perimeter	8
Changes in Default Behavior and Syntax in Release 12.1X46-D25 for Firefly Perimeter	31
Known Limitations in Release 12.1X46-D25 for Firefly Perimeter	31
Outstanding Issues in Release 12.1X46-D25 for Firefly Perimeter	31
Chassis Cluster	31
Command-Line Interface (CLI)	31
Flow and Processing	32
Interfaces and Routing	33
Junos OS Documentation and Release Notes	34
Documentation Feedback	34
Requesting Technical Support	34
Self-Help Online Tools and Resources	35
Opening a Case with JTAC	35

Revision History	35
------------------------	----

Release Notes for Firefly Perimeter

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

Firefly Perimeter is built on Junos OS and delivers similar security and networking features available on branch SRX Series devices.

These release notes include:

- [Upgrading from Prior Releases of Firefly Perimeter on page 3](#)
- [Optional Instructions for Validating Security Signatures on page 3](#)
- [Features Supported on Firefly Perimeter on page 8](#)
- [Changes in Default Behavior and Syntax in Release 12.1X46-D25 for Firefly Perimeter on page 31](#)
- [Known Limitations in Release 12.1X46-D25 for Firefly Perimeter on page 31](#)
- [Outstanding Issues in Release 12.1X46-D25 for Firefly Perimeter on page 31](#)

Upgrading from Prior Releases of Firefly Perimeter

You can upgrade to Firefly Perimeter Release 12.1X46-D25 from Release 12.1X46-D10 or later, using the 12.1X46-D25 TGZ image. For new installations you can use the OVA or JVA images.

Optional Instructions for Validating Security Signatures

This section includes instructions for validating security signatures.



.....

CAUTION: During the Firefly Perimeter installation or upgrade process, do not modify the filename of the software image that you download from the Juniper Networks support site. If you modify the filename, then the installation or upgrade will fail.

.....

- [Validating the Firefly Perimeter OVA Image](#)
- [Validating the Firefly Perimeter JVA Image using Linux commands](#)

Validating the Firefly Perimeter OVA Image

Starting with Firefly Perimeter 12.1X46-D25 and later, the Firefly Perimeter Open Virtualization Format Archive (OVA) image is securely signed. You can validate the OVA image, if necessary. However, you can install or upgrade Firefly Perimeter without validating the OVA image. Before you validate the OVA image, ensure that the Linux/UNIX PC on which you are performing the validation has the following utilities available: tar, openssl, and ovftool. You can download the VMware Open Virtualization Format (OVF) tool from the following location: <https://my.vmware.com/web/vmware/details?productId=353&downloadGroup=OVFTOOL351>

To validate the OVA image:

1. Download the Firefly Perimeter OVA image and the Juniper Networks Root certificate file (**JuniperRootRSACA.pem**) from the Firefly Perimeter downloads page at <https://www.juniper.net/support/downloads/?p=firefly#sw>



NOTE: You only need to download the Juniper Networks Root certificate file once; you can use the same file to validate OVA images for future releases of Firefly Perimeter.

2. (Optional) If you downloaded the OVA image and the certificate file to a PC running Windows, copy the two files to a temporary directory on a PC running Linux or UNIX. You can also copy the OVA image and the certificate file to a temporary directory (**/var/tmp** or **/tmp**) on a Firefly Perimeter node.

Ensure that the OVA image file and the Juniper Networks Root certificate file are not modified during the validation procedure. You can do this by providing write access to these files only to the user performing the validation procedure. This is especially important if you use an accessible temporary directory, such as **/tmp** or **/var/tmp**, because such directories can be accessed by several users. Take precautions to ensure that the files are not modified by other users during the validation procedure.

3. Navigate to the directory containing the OVA image.
4. Unpack the OVA image by running the following command:

```
tar xf ova-filename
```

where *ova-filename* is the filename of the previously downloaded OVA image.

5. Verify that the unpacked OVA image contains a certificate chain file (**certchain.pem**) and a signature file (**vsrx.cert**).
6. Validate the signature in the unpacked OVF file (extension .ovf) by running the following command:

```
ovftool ovf-filename
```

where *ovf-filename* is the filename of the unpacked OVF file contained within the previously downloaded OVA image.

- After the unpacked OVF file is validated, validate the signing certificate with the Juniper Networks Root CA file by running the following command:

```
openssl verify -CAfile JuniperRootRSACA.pem -untrusted Certificate-Chain-File
Signature-file
```

where **JuniperRootRSACA.pem** is the Juniper Networks Root CA file, *Certificate-Chain-File* is the filename of the unpacked certificate chain file (extension **.pem**) and *Signature-file* is the filename of the unpacked signature file (extension **.cert**).

If the validation is successful, a message indicating that the validation is successful is displayed.

A sample of the validation procedure is as follows:

```
-bash-4.1$ ls
JuniperRootCA.pem junos-vsrx-12.1X46-D25.7-domestic.ova
-bash-4.1$ mkdir tmp
-bash-4.1$ cd tmp
-bash-4.1$ tar xf ../junos-vsrx-12.1X46-D25.7-domestic.ova
-bash-4.1$ ls
certchain.pem junos-vsrx-12.1X46-D25.7-domestic.cert
junos-vsrx-12.1X46-D25.7-domestic-disk1.vmdk junos-vsrx-12.1X46-D25.7-domestic.mf
junos-vsrx-12.1X46-D25.7-domestic.ovf
-bash-4.1$ /usr/lib/vmware-ovftool/ovftool junos-vsrx-12.1X46-D25.7-domestic.ovf
OVF version: 1.0
VirtualApp: false
Name: Firefly Perimeter
Version: JUNOS 12.1
Vendor: Juniper Networks Inc.
Product URL:
  http://www.juniper.net/us/en/products-services/software/security/vsrxseries/
Vendor URL: http://www.juniper.net/
Download Size: 227.29 MB

Deployment Sizes:
Flat disks: 2.00 GB
Sparse disks: 265.25 MB

Networks:
Name: VM Network
Description: The VM Network network

Virtual Machines:
Name: Juniper Virtual SRX
Operating System: freebsdguest
Virtual Hardware:
Families: vmx-07
Number of CPUs: 2
Cores per socket: 1
Memory: 2.00 GB

Disks:
Index: 0
Instance ID: 5
```

Capacity: 2.00 GB
Disk Types: IDE

NICs:
Adapter Type: E1000
Connection: VM Network

Adapter Type: E1000
Connection: VM Network

Deployment Options:

Id: 2GvRAM
Label: 2G vRAM
Description:
2G Memory

```
-bash-4.1$ openssl verify -CAfile ../JuniperRootCA.pem -untrusted certchain.pem
junos-vsrx-12.1X46-D25.7-domestic.cert
junos-vsrx-12.1X46-D25.7-domestic.cert: OK
```

8. (Optional) If the validation is not successful, perform the following tasks:
 - a. Determine if the contents of the OVA image have been modified. If the contents have been modified, download the OVA image from the Firefly Perimeter downloads page.
 - b. Determine whether the Juniper Networks Root CA file is corrupted or modified. If it was corrupted or modified, download the certificate file from the Firefly Perimeter downloads page.
 - c. Retry the preceding validation steps using one or both new files.

Validating the Firefly Perimeter JVA Image using Linux commands

The Firefly Perimeter.jva format includes an embedded digital signature that can be validated to ensure authenticity of the content. In order to do so, along with the .jva file, you will need a copy of Juniper's root certificate. Once you have downloaded both, you will need to run a set of commands to extract the contents within the .jva file, authenticate the embedded signature with the signing certificate, and authenticate the signing certificate with Juniper's root certificate.

Once you have the .jva file and Juniper root certificate file in the same directory, use the following commands:

1. **bash junos-vsrx-12.1X46-D25.7-domestic.jva -x** (hit 'y' to accept the EULA)
2. **ls** (to show the newly created directory containing the .jva contents)
3. **cd**(to enter into the newly created directory containing .jva contents)
4. **openssl x509 -pubkey -noout -in vsrx.cert > public.pem** (this extracts the public key from the signing certificate)
5. **head -1 vsrx.cert | awk '{print \$2}' | xxd -p -r > signature.binary** (this converts the hex-encoded signature to binary format)

6. **openssl dgst -sha1 -verify public.pem -signature signature.binary vsrx.sig** (This command will validate the signature with the signing certificate. A successful validation will result in the message 'Verified OK'.)
7. **openssl verify -CAfile ../JuniperRootCA.pem -untrusted certchain.pem vsrx.cer** (This command will validate the signing certificate with Juniper's root certificate. A successful validation will result in message 'vsrc.cert: OK')

A sample of the JVA signature validation procedure using Linux commands is as follows:

```
-bash-4.1$ ls
JuniperRootCA.pem junos-vsrc-12.1X46-D25.7-domestic.jva
-bash-4.1$ bash junos-vsrc-12.1X46-D25.7-domestic.jva -x
Accept?[y/n]y
Extracting ...
Image dumped:
junos-vsrc-12.1X46-D25.7-domestic/junos-vsrc-12.1X46-D25.7-domestic.img
-rw-r--r-- 1 dkan nscn 278659072 Aug 15 10:05
junos-vsrc-12.1X46-D25.7-domestic/junos-vsrc-12.1X46-D25.7-domestic.img
-bash-4.1$ ls
JuniperRootCA.pem junos-vsrc-12.1X46-D25.7-domestic
junos-vsrc-12.1X46-D25.7-domestic.jva
-bash-4.1$ cd junos-vsrc-12.1X46-D25.7-domestic
-bash-4.1$ ls
certchain.pem junos-vsrc-12.1X46-D25.7-domestic.img vsrc.cert vsrc.sig vsrc.xml
-bash-4.1$ openssl verify -CAfile ../JuniperRootCA.pem -untrusted certchain.pem vsrc.cert
vsrc.cert: OK
-bash-4.1$ openssl x509 -pubkey -noout -in vsrc.cert > public.pem
-bash-4.1$ head -1 vsrc.cert | awk '{print $2}' | xxd -p -r > signature.binary
-bash-4.1$ openssl dgst -sha1 -verify public.pem -signature signature.binary vsrc.sig
Verified OK
```

Features Supported on Firefly Perimeter

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 1 on page 8](#) describes the available features on Firefly Perimeter as of Release 12.1X46-D25. For feature roadmap details, contact your Juniper Networks representative.

Table 1: Features Supported on Firefly Perimeter

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

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
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
Attack Detection and Prevention:	
Bad IP option	Yes
Block fragment traffic	Yes
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

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
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
UDP address sweep	Yes
UDP flood protection	Yes
Unknown IP protocol protection	Yes
Whitelist for SYN flood screens	Yes
WinNuke attack protection	Yes
Authentication with IC Series Devices:	
Captive Portal	Yes
Junos OS enforces in UAC deployments	Yes

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
Autoinstallation:	
Autoinstallation	Yes
Chassis Cluster (Support on VMware):	
Active/active chassis cluster	Yes
ALGs	Yes
Chassis cluster formation	Yes
Control plane failover	Yes
Dampening time between back-to-back redundancy group failover	Yes
Data plane failover	Yes
Dual control links	No
Dual fabric links	Yes
In-band cluster upgrade	No
Junos OS flow-based routing functionality	Yes
Layer 2 Ethernet switching capacity	No
Layer 2 LAG	No
Layer 3 LAG	No
LACP support for Layer 2	No
LACP support for Layer 3	No
Low-impact cluster upgrade (ISSU Light)	No
Low latency firewall	No
Multicast routing	Yes
PPPoE over redundant Ethernet interface	No
Redundant Ethernet interfaces	Yes
Redundant Ethernet interface LAGs	No

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
Redundant Ethernet or aggregate Ethernet interface monitoring	Yes
Redundancy group 0 (backup for Routing Engine)	Yes
Redundancy group 1 through 128	Yes
Upstream device IP address monitoring	Yes
Upstream device IP address monitoring on a backup interface	Yes
Chassis Management (Support on VMware):	
Chassis management	Yes
Class of Service:	
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
NOTE: GRE and IP-IP tunnels only.	
Virtual channels	Yes
Diagnostics Tools:	
CLI terminal	Yes
Flow monitoring cflowd version 5 and flow monitoring cflowd version 8	Yes
Flow monitoring cflowd version 9	No
Ping host	Yes

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
Ping MPLS	Yes
Traceroute	Yes
Ping Ethernet (CFM)	No
Traceroute Ethernet (CFM)	No
DNS Proxy:	
DNS proxy cache	Yes
DNS proxy with split DNS	Yes
Dynamic DNS	No
Dynamic Host Configuration Protocol:	
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
Ethernet Link Aggregation:	
Routing mode:	
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
Static LAG in standalone mode	No
Ethernet Link Fault Management:	

Table 1: Features Supported on Firefly Perimeter (*continued*)

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

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
inet6	Yes
iso	Yes
mpls	Yes
File Management:	
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
Firewall Authentication:	
Firewall authentication on Layer 2 transparent authentication	No
LDAP authentication server	Yes
Local authentication server	Yes
Pass-through authentication	Yes
RADIUS authentication server	Yes
SecurID authentication server	Yes

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
Web authentication	Yes
Flow-Based and Packet-Based Processing:	
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
Interfaces:	
Physical and Virtual Interface:	
Ethernet interface	Yes
Gigabit Ethernet interface	Yes
Services:	
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
Internally generated IP-over-IP interface (ip-0/0/0)	Yes
Internally generated link services interface	Yes

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
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 NOTE: Promiscuous mode needs to be enabled on hypervisor.	Yes
Secure tunnel interface	Yes
IP Monitoring:	
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
IP Security:	
Acadia - Clientless VPN	No
Alarms and auditing	Yes
Antireplay (packet replay attack prevention)	Yes
Authentication	Yes
Authentication Header (AH)	Yes
Autokey management	Yes

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
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)	Yes
NOTE: VMware platform only.	
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
Dynamic IP address	Yes
Dynamic IPsec VPNs	No
Encapsulating Security Payload (ESP) protocol	Yes
Encryption algorithms 3DES	Yes

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
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
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

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
IPsec tunnel termination in routing-instances	Yes NOTE: Supported on Virtual Router, only.
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
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

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
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
IPv6 Support:	
Flow-based forwarding and security features:	
Advanced flow	Yes
DS-Lite concentrator (aka AFTR)	No
DS-Lite initiator (aka B4)	No
Firewall filters	Yes
Forwarding option: flow mode	Yes
Multicast flow	Yes
Screens	Yes
Security policy (firewall)	Yes

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
Security policy (IDP)	No
Security policy (user role firewall)	No
Zones	Yes
IPv6 ALG support for FTP: Routing, NAT, NAT-PT support	Yes
IPv6 ALG support for ICMP: Routing, NAT, NAT-PT support	Yes
IPv6 NAT: NAT-PT, NAT support	Yes
IPv6 NAT64	Yes
IPv6--related protocols: BFD, BGP, ECMPv6, ICMPv6, ND, OSPFv3, RIPng	Yes
IPv6 ALG support for TFTP	Yes
System services: DHCPv6, DNS, FTP, HTTP, ping, SNMP, SSH, syslog, Telnet, traceroute	Yes
Packet-based forwarding and security features:	
Class of service	Yes
Firewall filters	Yes
Forwarding option: packet mode	Yes
Chassis cluster (VMware platform only)	
Active-active	Yes
Active-passive	Yes
Multicast flow	Yes
IPv6 IP Security:	
4in4 and 6in6 policy-based site-to-site VPN, AutoKey IKEv1	No

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
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
Log File Formats:	
System (control plane) log file formats:	
Binary format (binary)	No
Structured syslog (sd-syslog)	Yes
Syslog (syslog)	Yes
WebTrends Enhanced Log Format (WELF)	No
Security (data plane) log file formats:	
Binary format (binary)	Yes
Structured syslog (sd-syslog)	Yes
Syslog (syslog)	Yes
WebTrends enhanced log format (WELF)	Yes
MPLS:	
CCC and TCC	No
CLNS	Yes
Interprovider and carrier-of-carriers VPNs	Yes
Layer 2 VPNs for Ethernet connections	Yes
Layer 3 MPLS VPNs	Yes
LDP	Yes
MPLS VPNs with VRF tables on provider edge routers	Yes
Multicast VPNs	Yes
OSPF and IS-IS traffic engineering extensions	Yes

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
P2MP LSPs	Yes
RSVP	Yes
Secondary and standby LSPs	Yes
Standards-based fast reroute	Yes
Multicast:	
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
Multicast VPN:	
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
Network Address Translation:	
Destination IP address translation	Yes
Disabling source NAT port randomization	Yes
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

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
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
Network Operations and Troubleshooting:	
Event policies	Yes
Event scripts	Yes
Operation scripts	Yes
XSLT commit scripts	Yes
Network Time Protocol:	
NTP support	Yes
Packet Capture:	
Packet capture	Yes
<p>NOTE: 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>	

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
Routing:	
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
Virtual Router Redundancy Protocol (VRRP)	Yes
Secure Web Access:	
CAs	Yes
HTTP	Yes
HTTPS	Yes
Security Policy Support:	
Address books/address sets	Yes

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
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
Security Zone:	
Functional zone	Yes
Security zone	Yes
Session Logging:	
Accelerating security and traffic logging	Yes
Aggressive session aging	Yes
Getting information about sessions	Yes
Logging to a single server	Yes
Session logging with NAT information	Yes
SMTP:	
SMTP support	Yes
SNMP:	
SNMP support	Yes
Stateless Firewall Filters:	

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
Stateless firewall filters (ACLs)	Yes
Stateless firewall filters (simple filter)	No
System Log Files:	
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
Upgrading and Rebooting:	
Autorecovery	No
Boot device configuration	No
Boot device recovery	No
Chassis components control	Yes
Chassis restart	Yes
Download manager	Yes
Dual-root partitioning	No
In-band cluster upgrade	No
Low-impact cluster upgrades	No
Software upgrades and downgrades	Yes
User Interfaces:	
CLI	Yes

Table 1: Features Supported on Firefly Perimeter (*continued*)

Feature	Support on Firefly Perimeter
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 Note: Supported on VMware only and not on KVM.
VPLS:	
Filtering and policing (Packet-Based)	Yes

Table 2 on page 30 lists additional features that are not supported on Firefly.

Table 2: Firefly Feature Support Information

Feature	Firefly
Application Identification (Junos OS)	No
Dynamic VPN (DVPN)	No
General Packet Radio Service	No
Group VPN	No
Intrusion Detection and Prevention	No
Layer 2 Mode	No
Logical Systems	No
Multicast for AutoVPN	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

Changes in Default Behavior and Syntax in Release 12.1X46-D25 for Firefly Perimeter

- A new static product image is added for the Firefly Perimeter Chassis View on the J-Web Dashboard.
- Firefly Perimeter does not need a license activation key.

In order to use Firefly Perimeter after a 60 day evaluation period, a purchase is required. Enforcement and auditing are possible for anyone using the product as per Juniper EULA agreement and Software Advantage model.
- Performance on VMware 5.5 update 2 or 3 can degrade significantly (25 percent) from previous versions because of an e1000 driver issue.

Known Limitations in Release 12.1X46-D25 for Firefly Perimeter

The known limitations in Firefly Perimeter are as follows:

- Firefly Perimeter requires a configuration with 2 vCPUs, up to 10 vNICs, and 2GB RAM.
- Firefly Perimeter supports only ESXi 5.0 and 5.1.
- VM hardware version cannot be upgraded through vSphere client.
- On Firefly Perimeter, *family ethernet-switching* and *services unified-access-control* are not supported.
- On Firefly Perimeter, configuring an interface to do traffic loopback is not supported due to VMware e1000 NIC emulation limitation.

Outstanding Issues in Release 12.1X46-D25 for Firefly Perimeter

The following problems currently exist in Juniper Networks Firefly Perimeter. The identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

Chassis Cluster

- On Firefly Perimeter, when enabling chassis cluster on VMware ESXi version 5.1-update2 hypervisor, the control link does not make a connection and you might see the log **fxp1 watchdog timeout** on the console.

VMware ESXi 5.1u2 does not support chassis cluster on Firefly Perimeter. [PR 936992]

Command-Line Interface (CLI)

- Upgrading from 12.1X44-D20.3 to 12.1Q1_X46 with the `validate` option produces an error.

Workaround: Use `request system software add firefly-perimeter.tgz image no-validate` to upgrade the image. [PR 941123]

Flow and Processing

- The Remote Shell (RSH) session fails when RSH is done from a PC to the Firefly Perimeter towards an IP address that does not belong to the closest interface.

This error happens because the data session initiated by Firefly Perimeter has the outgoing interface's IP address as its source IP, which is not the same IP address that the PC directed the control session to. [PR 738835]

- When a huge configuration is loaded and committed, the Firefly Perimeter becomes unresponsive for a short time. [PR 749206]
- If the disk is full on Firefly Perimeter, then HTTP becomes out of service and displays the **"Access Error: 503 -- Service Unavailable"** error message.

Workaround: Create space in the disk by using the **request system storage cleanup** command. [PR 774387]

- IPsec does not display for the VPLS configuration on Firefly Perimeter. [PR 783735]
- On Firefly Perimeter, password recovery does not work through the VMware vSphere console.

If you do not have a serial connection, then you must deploy a new Firefly Perimeter instance. [PR 818987]

- Existing protected resource access might get stopped during the reboot of a primary node of a Firefly Perimeter active/passive cluster.

UAC authenticated Telnet access gets disconnected upon a primary node reboot in active/backup setup. [PR 911542]

- If the Firefly Perimeter is configured with a number of vNICs and you delete a few using VMware console, then you might notice performance degradation.

Workaround: Delete the remaining interfaces and security configuration from Firefly Perimeter and then add them back. [PR 912817]

- Internet Key Exchange (IKE) security association might not negotiate successfully after a RGO failover and switching between *establish-tunnels no-traffic* and *establish-tunnels immediately*. [PR 913961]

- You can see a performance degradation with more Firefly Perimeter instances when compared with a single Perimeter instance, running under a single VMware ESX host.

The KVM density of Firefly Perimeter running under the host degrades the performance; each Firefly Perimeter throughput is relatively lower when compared to the throughput of a single Firefly Perimeter running under the host (see PR 930500). [PR 914280]

- On Firefly Perimeter, unidirectional latency is almost double the bidirectional latency.

The number of packets transmitted in bidirectional mode is more than the number of packets transmitted in unidirectional mode. Latency is high with unidirectional traffic in firewall mode (see PR 751987). [PR 925123]

- On Firefly Perimeter, packets are not distributed evenly across all four queues and eight queues for a KVM Virtio interface.

The bandwidth of the lower priority queue cannot be occupied by strict-high queue (see PR 938362). Traffic shaping (QoS) on a Firefly Perimeter fails on the reth interface (see PR 908995).

The priority queuing of a class-of-service scheduler does not work well on a Perimeter platform as its process relates to interface speed. The interface speed of a Perimeter does not precisely comply with the real transmission capability, which is controlled by a vNIC and hypervisor does not implement Physical Layer of vNIC. [PR 925300]

- The egress statistics will display wrong numbers.

Schedule monitoring should be disabled in higher traffic environments for active-passive mode. In *active-active* mode the maximum throughput supported is 1.3 Gbps only. You can ignore the output of egress statistics. [PR 950223]

Interfaces and Routing

- The **show interfaces** command in Firefly Perimeter generates inaccurate data under heavy traffic conditions. [PR 740145]
- If the Virtual Router Redundancy Protocol (VRRP) is configured on Firefly Perimeter running on a VMware hypervisor, you cannot ping the virtual IP address.

A VRRP ping to a virtual IP fails even though promiscuous mode is enabled on the hypervisor (see PR 917549). This issue occurs because the vSwitch in the VMware ESXi host does not update the Layer 2 forwarding table for the Gratuitous Address Resolution Protocol (GARP).

Workaround: Set virtual MAC for member interfaces on both VRRP nodes. [PR 753715]

- On Firefly Perimeter, there is nonstatic mapping between vNICs and Junos OS interfaces. Hence, you must reconfigure interfaces and other related configuration commands to delete a vNIC. [PR 813391]
- On Firefly Perimeter high availability, you might not get all the reth interface statistics after an interface-monitor failover. [PR 925715]
- The link speed and link mode settings of a Gigabit interface on a Firefly Perimeter are irrelevant.

The hypervisor does not implement the Physical Layer on a vNIC adapter. The vNIC adapter always transmits packets with best effort. [PR 933973]

- When the traffic is heavy and you are continuously doing multiple manual failovers on Firefly Perimeter, one of the nodes goes into disable state.

Workaround: Increase the heartbeat interval to 5 seconds. [PR 946071]

- When Firefly Perimeter is in packet mode, a warning message is still displayed on commit after configuring an interface with family inet.

You can ignore the message as it does not affect any functionality. [PR 949472]

Junos OS Documentation and Release Notes

For a list of related Junos OS documentation, see <http://www.juniper.net/techpubs/software/junos/>.

If the information in the latest release notes differs from the information in the documentation, follow the *Junos OS 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/>.

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at <http://www.juniper.net/books>.

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, 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 Partner Support Service 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: <http://kb.juniper.net/InfoCenter/>
- 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>.

Revision History

28 March 2016—Revision 2, Firefly Perimeter - Release 12.1X46-D25.

28 August 2014—Revision 1, Firefly Perimeter - Release 12.1X46-D25.

Copyright © 2016, 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.