

Firefly Host Release Notes

Release 6.0R2
19 December 2014
Revision 1

The Firefly Suite is designed to address the need for compelling and robust security for diverse virtualized environments by bringing together three products - Firefly Host Release 6.0, Firefly Perimeter Release 12.1X46-D10, and Junos Space Virtual Director Release 1.0. These release notes accompany Release 6.0R2 of Firefly Host. They describe supported features and known issues with Firefly Host.

Contents

Release Notes for Firefly Host	2
Supported Features for Firefly Host	2
Firefly Host Compatibility	3
Known Issues in Release 6.0R2 for Firefly Host	4
Firefly Host Dashboard	4
Firefly Host VM	7
Resolved Issues in Release 6.0R2 for Firefly Host	8
Documentation and Release Notes	9
Documentation Feedback	9
Requesting Technical Support	10
Self-Help Online Tools and Resources	10
Opening a Case with JTAC	10
Revision History	11

Release Notes for Firefly Host

Firefly Host delivers complete virtualization security for multitenant public and private clouds, and clouds that are a hybrid of the two. Firefly Host is built off the vGW product line and replaces it. Firefly Host comprises the following three main components:

- Firefly Host Dashboard—Consists of a set of modules used to configure the Firefly Host features for your virtualized environment.
- Firefly Host VM—Remains attached to the ESX/ESXi host on which it is installed on and maintains policy and logging information.
- Firefly Host Module—All connections are processed and firewall security is enforced in the Firefly Host Module.

To obtain the most current version of Firefly Host technical documentation, see the [Firefly Host Documentation](#) page on the Juniper Networks website.

These release notes include:

- [Supported Features for Firefly Host on page 2](#)
- [Firefly Host Compatibility on page 3](#)
- [Known Issues in Release 6.0R2 for Firefly Host on page 4](#)
- [Resolved Issues in Release 6.0R2 for Firefly Host on page 8](#)

Supported Features for Firefly Host

[Table 1 on page 2](#) lists the main features that are supported on Firefly Host Release 6.0R2.

Table 1: Features Supported on Firefly Host

Feature	Description
Stateful virtual firewall enforces policy for group and individual VMs	Granular access control and VM isolation via policy enforcement for groups and individual VMs.
VMsafe implementation delivers breakthrough performance	Certified hypervisor-based security processing for breakthrough performance with more than 10x the throughput of non-VMsafe fast-path virtual firewalls.
VM Introspection gives X-ray view of VMs and OSes	X-ray view of VMs and their installed OSes, applications and services.
VM Image Enforcer ensures compliance with ideal VM configuration	Enforcement of the desired or ideal VM configuration with options for alerting and/or quarantining for VMs whose image deviates.
Virtualization-specific AV protects VM disks and files	On-demand and on-access scanning of VM disks and files with quarantining of infected entities.

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

Feature	Description
Intrusion detection system provides malware detection	Selectable, protocol and application-specific deep-packet inspection of allowed traffic for malware detection.
Smart Groups automates VM security for new VMs	Automated VM security for newly created or replicated VMs.
Network monitoring sees and monitors inter-VM and intra-VM traffic	Visibility and comprehensive auditing of inter-VM and intra-VM communications and Netflow-style data collection.
Highly scalable central management synchronizes security policies	Synchronization of security policies across vGW management centers for safe, large-scale, multi-tenant virtualization.
IPv6/IPv4 firewall enforcement and management	Greater flexibility and efficiency of traffic protection with the ability to manage the entire vGW infrastructure via IPv4 or IPv6 addresses.
Firefly Host Cloud API and SDK allows customization	Time and resource savings through customization and automation of security controls during VM provisioning.

Firefly Host Compatibility

Table 2 on page 3 describes the compatible versions of VMware and Firefly Host (Firefly Host Dashboard and Firefly Host VM).

Table 2: Firefly Host Compatibility with VMware Versions

VMware Version	vGW Series and Firefly Host Support
vSphere 5.0 (and all updates)	<p>vGW Series 5.0r2 and later releases including all versions of vGW 5.5 and Firefly Host 6.0R2.</p> <p>WARNING: Upgrading to ESXi 5.0 Update 2 prior to updating to vGW Series 5.5R4 installation can cause issues with vGW Security VMs/Host Security VMs associating properly to hosts. This occurs because of the UUID changes made during the upgrade. Issues are related to modifications VMware made to the UUID behavior as noted in their release notes. See PR849657. (http://www.vmware.com/support/vsphere5/doc/vsp_esxi50_u2_rel_notes.html)</p>
vSphere 5.1 (and all updates)	<p>vGW Series 5.0R4 or later including all versions of vGW 5.5 and Firefly Host.</p> <p>NOTE: vSphere 5.1 supports only ESXi hosts.</p>

Table 2: Firefly Host Compatibility with VMware Versions (*continued*)

VMware Version	vGW Series and Firefly Host Support
vSphere 5.5	Supported. See Juniper Networks Knowledge Base article - KB 28884 at http://kb.juniper.net/ .

Table 3 on page 4 describes the software compatibility and requirements for Firefly Host.

Table 3: Firefly Host Software Compatibility and Requirements

Software	Firefly Host
vSwitches	Firefly Host interoperates with the following types of switches: <ul style="list-style-type: none"> Standard VMware Virtual Switch VMware Distributed Virtual Switch (DVS) Cisco Nexus 1000V device
Browsers	Firefly Host requires one of the following supported Web browsers: <ul style="list-style-type: none"> Mozilla Firefox 3 or later <p>NOTE: Localized (non-English) versions of browsers, such as the Japanese version of IE7, are not fully supported. However most character sets including Japanese should display properly.</p>

Known Issues in Release 6.0R2 for Firefly Host

The following problems currently exist in the Juniper Networks Firefly Host components, which include Firefly Host Dashboard, Firefly Host VM, and Firefly Host Endpoint. The identifier after the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.



NOTE: This section lists the known issues for Firefly Host Release 6.0R2 only. It does not address vGW Series 5.5 issues.

Firefly Host Dashboard

Release Date: December-10-2014; Build Number: 6.0R2.c-1-3

- Primary and secondary SDCs fails to synchronize the database after the primary SDC upgrades to 6.0R2

Workaround: Log in to the SDC:

Run the following commands from the bash console:

- `bash-3.2$ psql -U sa vbrix_db -c "update property set value=2 where key='standby.c.conf.status'"`

Password for user sa:
UPDATE1

bash-3.2\$ psql -U sa vbrix_db -c "update property set value='10.159.27.128' where key='standby.c.ip'"

UPDATE1

Password for user sa:

2. **bash-3.2\$ sudo db/del_slony_conf.sh 10.159.27.238.10 10.159.27.128 standby
altorstandby**

Sending 'stop' command
No matching task or group
Reloading Process Monitor (god): Sending 'load' command with action 'leave'
The following tasks were affected:
exced
ntlmaps
tomcat
raa-web
raa-service
[OK]
slon: no process killed
<stdin>:16: PGRES_FATAL_ERROR select "_altor_standby" .uninstallNode(); -ERROR:
schema "_altor_standby" does not exist
Failed to exec unistallNode() for node 1
did not delete slony tables (may be were not created)
DROP ROLE
Stopping postgresql service: [OK]
Strating postgresql service: [OK]
Waiting for postgress to aaccept connection on port 5432
[OK]
Waiting for postgress scoket at /tmp/.s.PGSQL.5432
sucessful deletion of slony configuration

3. **bash-3.2\$ sudo db/del_slony_conf.sh 10.159.27.238.10 10.159.27.128 standby
altorstandby**

CREATE ROLE
Stopping postgresql service: [OK]
Strating postgresql service: [OK]
Waiting for postgress to aaccept connection on port 5432
[OK]
Waiting for postgress scoket at /tmp/.s.PGSQL.5432
sucessful_init_slony

4. **bash-3.2\$ sudo db/del_slony_conf.sh 10.159.27.238.10 10.159.27.128 standby
altorstandby**

<stdin>:18: NOTICE: subscribe set: omit_copy=f
<stdin>:18: NOTICE: subscribe set: omit_copy=f
CONTEXT: SQL statement "SELECT" "_altor_standby" .subscribeSet_int(\$1, \$2, \$3, \$4, \$5)"
PL/pgSQL fucntion "subscribe set" line 68 at PERFORM
<stdin>:19: NOTICE: subscribe set: omit_copy=f
<stdin>:19: NOTICE: subscribe set: omit_copy=f
CONTEXT: SQL statement "SELECT" "_altor_standby" .subscribeSet_int(\$1, \$2, \$3, \$4, \$5)"
PL/pgSQL fucntion "subscribe set" line 68 at PERFORM
<stdin>:20: NOTICE: subscribe set: omit_copy=f
<stdin>:20: NOTICE: subscribe set: omit_copy=f

```

CONTEXT: SQL statement "SELECT" "_altor_standby" .subscribeSet_int( $1, $2,
$3, $4, $5)"
PL/pgSQL fucntion "subscribe set" line 68 at PERFORM
<stdin:>21: NOTICE: subscribe set: omit_copy=f
<stdin:>21: NOTICE: subscribe set: omit_copy=f
CONTEXT: SQL statement "SELECT" "_altor_standby" .subscribeSet_int( $1, $2,
$3, $4, $5)"
PL/pgSQL fucntion "subscribe set" line 68 at PERFORM
<stdin:>22: NOTICE: subscribe set: omit_copy=f
<stdin:>22: NOTICE: subscribe set: omit_copy=f
CONTEXT: SQL statement "SELECT" "_altor_standby" .subscribeSet_int( $1, $2,
$3, $4, $5)"
PL/pgSQL fucntion "subscribe set" line 68 at PERFORM
<stdin:>23: NOTICE: subscribe set: omit_copy=f
<stdin:>23: NOTICE: subscribe set: omit_copy=f
CONTEXT: SQL statement "SELECT" "_altor_standby" .subscribeSet_int( $1, $2,
$3, $4, $5)"
PL/pgSQL fucntion "subscribe set" line 68 at PERFORM
Reloading Process Monitor (god)" Sending 'load' command with action 'leave'
The following tasks were affected:
exced
ntlmads
tomcat
raa-web
raa-service
[OK]
Sucessful start slony mirror

```

[PR 1048937]

- A VM can appear under the Secured VM display if it does not contain any vNICs. [PR 920910]
- Applied policy can still show as unapplied when all its rules are disabled as there are no rules to push. [PR 921141]
- An ESXi host cannot be unsecured when it runs a Firefly Host Dashboard VM and the dashboard appliance has an ISO image connected to its virtual CD-ROM drive. [PR 948650]
- Backup of the Firefly Host Dashboard appliance using the Common Internet File System (CIFS) is no longer supported. [PR 938074]
- The groups on *vi.pvlan*, and *vi.pvlan.all* might not get updated when changing dvPortGroup's pvlan. [PR 952013]
- When a VM is a member of an empty policy group (that is, a policy group without rules), you might see VMs as members in the user interface default policy group that do not belong there. [PR 952459]
- IDS signatures that reference other signatures might fail to generate an alert if all of the related signatures are not active. To determine if you are using signatures with dependencies, search on the description of the signature. The results will show all signatures using that description and all of them should be active. [PR 952014]
- The standby SDC cannot communicate with the primary SDC upon upgrade.
Workaround: Reconfigure the secondary SDC IP address through the SDC Web. [PR 954480]

- The Exception error seen while attempting to access XML-RPC getPolicy call with an ID of a node that does not exist. [PR 1030960]
- In security report there is no description. Workaround: In Reports, Select Add New Report click Security Report radio button. [PR 716538]
- The download page of Firefly Host 6.0 is directing to vGW. [PR 979103]
- Fixed the issue where after upgrading to Firefly Host 6.0, auto-push policy group changes resulted in incorrect static group policy enforcement for its member VMs (not all VMs). Workaround: Apply the policy manually for affected VMs. [PR 1022507]
- When connecting to external VMware and the target is unknown, Firefly IDS alert sources and targets report destinations and sources as "0.0.0.0" instead of the source IP address. [PR 1020031]
- AV installation on win-32 bit platform fails. [PR 1020239]
- Cannot unsecure VMs. [PR 1016783]
- The XML-RPC method "saveNetwork", does not validate the IP range is correct. [PR 1012536]
- Default server update.altornetworks.com is now changed to vgwudapte.juniper.net. [PR 1019320]
- Snort updates are prepared separately for vGW5.5 and Firefly Host 6.0. [PR 1021862]
- Inbound policy rule is not enforced properly. [PR 1019033]
- Resuming VMs sometimes may be suspended or throws unexpected exceptions. [PR 1017678]
- VM safe fail function configuration is not saved. [PR 1017858]
- Automated reply policy in smart group may not work. [PR 1016694]
- SDCs internal maps may sometimes contain old machine objects that represent old state of machines. [PR 1015796]
- During initialization of the simulator environment, the SDC would remain inactive if the simulator is not configured properly. [PR 1014674]
- Protected VMs list contains SVMs. [PR 1014612]

Firefly Host VM

Release Date: December-10-2014; Build Number: 6.0R2.a-1-1

- Firefly Host syslog information cannot be sent when TCP is used. [PR 746528]
- The Netflow time values are flipped. [PR 841343]
- IPv6 Neighbor Discovery packets are displayed with a double colon (::). [PR 793405]
- Low performance due to On Access Scanning. [PR 936192]

Resolved Issues in Release 6.0R2 for Firefly Host

- [CVE-2014-0224](#), [CVE-2014-0221](#), [CVE-2014-0195](#), [CVE-2014-0198](#), [CVE-2010-5298](#), and [CVE-2014-3470](#) are the vulnerabilities fixed. [PR 999842]
- [CVE-2014-6271](#), and [CVE-2014-7169](#)(Shellshock) are the vulnerabilities fixed. [PR 1029345]
- Fixed incomplete group purging, which caused an SDC error on startup. [PR 984437]
- Fixed the issue where after upgrading to Firefly Host 6.0, auto-push policy group changes resulted in incorrect static group policy enforcement for its member VMs (not all VMs). Workaround: Apply the policy manually for affected VMs.[PR 1022507]
- The Firefly Host dashboard Help file is updated from 5.5 to 6.0. [PR 1026952]
- Adding a VM through XML or GUI fails. [PR 1017807]
- While configuring the scanner, ADD AV button is disabled. [PR 1019028]
- When adding NIC card to EPVM, the VC loops the reconfigure actions. [PR 1021051]

Documentation and Release Notes

For a list of Firefly Host documentation, see [Firefly Host Documentation](#) page on the Juniper Networks website.

If the information in the documentation differs from the information in the latest release notes, follow the *Firefly Host 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 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/>

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

19 December 2014—Revision 1, Firefly Host - Release 6.0R2

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.