

vGW Series 5.5

Release Notes

Release 5.5 - (Summary of Known Issues – All Hot Fixes and Maintenance Releases)

Last Updated October 30, 2014 (Document Rev. W)

Contents

Contents	i
SOFTWARE LICENSE	1
END USER LICENSE AGREEMENT	1
Release Overview	4
VMware Version Compatibility	4
Security Design vGW	4
vGW Security VM.....	16
vGW Endpoint	17

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE.

BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. The Parties. The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. The Software. In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. License Grant. Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services. The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. Use Prohibitions. Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. Audit. Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. Confidentiality. The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. Ownership. Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. Warranty, Limitation of Liability, Disclaimer of Warranty. The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties. **9. Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. Taxes. All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. Export. Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. Commercial Computer Software. The Software is “commercial computer software” and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. Interface Information. To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. Third Party Software. Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License (“GPL”) or the GNU Library General Public License (“LGPL”)), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. Miscellaneous. This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Release Overview

This document describes the known issues and available fixes for each of the Juniper vGW Series components. There are separate sections for each component, including: the Security Design vGW management system (SD vGW or vGW SDC), the vGW Security VM (vGW SVM) on each ESX/ESXi host, and the vGW Endpoint (installed in Guest VMs when On-Access AV protection is desired).

VMware Version Compatibility

The following table describes the compatible VMware versions and vGW (Security Design vGW and vGW Security VM)

Versions of VMware	Compatible Versions of vGW
vSphere 4.0 and 4.1 (all Updates)	End of Life (EOL)
vSphere 5.0 and 5.0 (all Updates)	vGW 5.0R2 or later (including all versions of vGW 5.5). Warning: Upgrading to ESXi 5.0 Update 2 prior to vGW 5.5R4 being installed can cause issues with vGW SVM's associating properly to hosts (blank ESX Host field in GUI). This occurs b/c the UUID changes during the upgrade (related to modifications VMware made to UUID behavior & noted in their release notes (http://www.vmware.com/support/vsphere5/doc/vsp_esxi50_u2_rel_notes.html)). See also PR849657.
vSphere 5.1 (all Updates)	vGW 5.0R4 or later (including all versions of vGW 5.5)
vSphere 5.5	Firefly Host 6.0

Security Design vGW

The following table summarizes each of the releases for the Security Design vGW management center. The date of the release and build number are noted as well as a summary of the fix or open issue.

Release Date October-30-2014 (5.5R7)

Build Number	Summary of Fixes and/or Open Issues
5.5.c-17-2	
Item 1 - PR984437	<u>Resolved</u> - Fixed incomplete group purging, which caused an SDC error on startup.
Item 2 - PR1022507	<u>Resolved</u> - 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.
Item 3 - PR 1029345	<u>Resolved</u> - Fixed the following vulnerabilities: CVE- 2014-6271, CVE- 2014-7169 (Shellshock).

Release Date July-9-2014 (5.5R6)

Build Number 5.5.c-17	Summary of Fixes and/or Open Issues
Item 1 - PR951358	<u>Resolved</u> – Fixed the unexpected packet drops reported for more than 500 VMs.
Item 2 - PR955293	<u>Resolved</u> – Included additional logs for – sync/policy/machine/nic.
Item 3 - PR956064	<u>Resolved</u> – Fixed the issue of IP address removal in incremental sync.
Item 4 - PR952623	<u>Resolved</u> – Fixed the issue of frequent tomcat server restart.
Item 5 - PR955289	<u>Resolved</u> – Fixed the issue of attribute redundant notification during full synchronization.
Item 6 - PR969138	<u>Resolved</u> – Fixed the issue of High CPU and Delayed response from SDC.
Item 7 - PR999842	<u>Resolved</u> – Fixed the following vulnerabilities: CVE-2014-0224, CVE-2014-0221, CVE-2014-0195, CVE-2014-0198, CVE-2010-5298 and CVE-2014-3470.
Item 8 - PR976155	<u>Resolved</u> – Fixed the issue of erroneous disk mounting in DOS extended partitions.
Item 9 - PR978452	<u>Resolved</u> – Purge or removed objects from the SDC.

Release Date Jan-7-2014 (5.5R5)

Build Number 5.5.c-9-16	Summary of Fixes and/or Open Issues
Item 1 – Update Notification!	Updates from 5.0 to 5.5 may require a manual reboot of the Security Design vGW management center. Monitor the center after the update occurs to make sure it reboots after the update completes, if it doesn't initiate a reboot. Please see the items listed in the 5.5 R4 HF2,3 and 4 sections for additional known issues
Item 2 – Update Notification! & PR951770	Crucial Known Issue – An SSL certificate is used to encrypt communications between vGW components. This certificate expired on Jan 1 2014 and thus communication breaks between systems. The issue is described in Juniper KB 28666. This build fixes the issue completely for a new install. For customers who are updating to this build, they will still need to follow the procedures listed to reset the CA and re-config the SVM's described in KB 28666 (no downloading of files will be necessary but the other steps are still required).
Item 4 – PR950786	<u>Resolved</u> – Fixed an issue in which a rule wouldn't be enforced properly in an upgrade from 5.0 to 5.5 if you had overlapping sources.
Item 4 – PR948508	<u>Resolved</u> – Clarification that anytime a VM is a member of a policy group it will be excluded from the default policy group. Also created a new saveEmpty method in InstalledPolicy that receives updated group order
Item 5 – PR945665	<u>Resolved</u> – Default policy will be added to the nic policy if the nic is not a member of a manual group and not a member of applied auto-push group. The default policy will be added regardless of existence of in/outbound rules. It is enough that a nic belongs to a manual policy group or an applied auto-push policy group to exclude the nic from the default policy.

Release Date Dec-10-2013 (5.5R4 HF4)

Build Number	Summary of Fixes and/or Open Issues
--------------	-------------------------------------

5.5.c-9-15	
Item 1 – Update Notification!	<p>Updates from 5.0 to 5.5 may require a manual reboot of the Security Design vGW management center. Monitor the center after the update occurs to make sure it reboots after the update completes, if it doesn't initiate a reboot.</p> <p>Please see the items listed in the 5.5 R4 HF2 and HF3 sections (all of those are relevant with HF3). This is minor update to fix one item as listed below)</p>
Item 2 – PR945665	<p><u>Resolved</u>– The Security Design Management Center could fail to properly recognize the IP address of a VM which was to be protected. This failure could cause incomplete firewall rule to be applied.</p>

Release Date Nov-20-2013 (5.5R4 HF3)

Build Number 5.5.c-9-14	Summary of Fixes and/or Open Issues
Item 1 – Update Notification!	<p>Updates from 5.0 to 5.5 may require a manual reboot of the Security Design vGW management center. Monitor the center after the update occurs to make sure it reboots after the update completes, if it doesn't initiate a reboot.</p> <p>Please see the items listed in the 5.5 R4 HF2 section (all of those are relevant with HF3). This is minor update to fix one items as listed below and list two more as known.</p>
Item 2 – PR940510	<p><u>Known</u>– When creating an application of type 'other' instead of displaying 'Other' in the Type field and the relevant IP Protocol in the 'Port / Info' field, the IP Protocol is incorrectly listed in the Type field.</p>
Item 3 – PR940927	<p><u>Known</u> – Tool tips in the left hand side inventory can sometimes fail to appear/appear only after a delay (this is an issue for internal automation tests but generally shouldn't impact regular users).</p>
Item 4 – PR939938	<p><u>Resolved</u> – Global policy application was failing on auto-push policy configured systems using cloned VMs (we were transferring only part of the rule base)</p>

Release Date Oct-3-2013 (5.5R4 HF2)

Build Number 5.5.c-9-13	Summary of Fixes and/or Open Issues
Item 1 – Update Notification!	<p>Updates from 5.0 to 5.5 may require a manual reboot of the Security Design vGW management center. Monitor the center after the update occurs to make sure it reboots after the update completes, if it doesn't initiate a reboot.</p>
Item 2 – PR922283	<p><u>New</u> – Synchronization stability improvements and a new internal support flag which can be used to control heartbeat and incremental synch (center.enable.identical.heartbeat)</p>
Item 3 – PR923911	<p><u>New</u> – Added dvSwitch port group options to Auto Deploy so this feature can be used with vSphere Distributed Switch</p>
Item 4 – PR917588	<p><u>Known</u> – IE8 can fail to show external machines in the list to add policies. Workaround is to use different browser.</p>
Item 5 – PR914072	<p><u>Known</u> – The backup settings can incorrectly revert to previous configurations.</p>
Item 6 – PR919038	<p><u>Known</u> – It's not possible to save any new policy rule on a brand new installation when no SVM exists. Workaround is to properly install at least one SVM.</p>

Item 7 – PR910058	<u>Known</u> – Confirmation popup box when adding a default policy rule disappeared with IPv6 changes.
Item 8 – PR916575	<u>Known</u> – Error message in catalina.out.log file about NullPointerException seen when doing log collection. No impact to system.
Item 9 – PR920818, PR916609	<u>Known</u> – A protected host can be shown as unprotected if it's moved out of a cluster. Can re-secure the host to eliminate this.
Item 10 – PR920910	<u>Known</u> – If a vm which doesn't contain any vNIC's can appear under the 'secured vm' display.
Item 11 – PR921141	<u>Known</u> – When a policy group contains rules that are ALL disabled, applying the policy can still show as not applied. This is because no rules were actually pushed. No effect on the applied policy just needs more gui clarification to explain it's not applied b/c there are no rules to push.
Item 12 – PR921681, PR921715	<u>Known</u> – On-access AV scans will scan an archived file regardless of the 'Scan Archives' checkbox. Also high priority group setting may not work with dynamic groups.
Item 13 – PR926669, PR926957	<u>Resolved</u> – Improvements to better resist any failures in connectivity between vCenter and the Security Design vGW Management system.
Item 14 – PR923850, PR923931, PR924170, PR923927, PR920411	<u>Resolved</u> – Null check in inventory.java and other locations which, could lead to unforeseen issues. Fixed additional memory, locking and sync items. Also improved the handling of powering on SVM's to avoid deadlocks.
Item 15 – PR922889, PR924376	<u>Resolved</u> – Improved behavior on full synchronizations so that the apply policy screen is displayed accurately and proper policy enforcement can be done. Also improvements to caching mechanisms.
Item 16 – PR921164	<u>Resolved</u> – vCloud Director integration not seeing changes made during Security Design Center down time.
Item 17 – PR921913, PR921916	<u>Resolved</u> – Improved the ability to detect newly cloned VMs (including updating alarm messaging)
Item 18 – PR921902	<u>Resolved</u> – Null pointer verification when getting heartbeat with unknown machine id's.
Item 19 – PR920826	<u>Resolved</u> – Event propagating on datacenter changes for a VM are more reliable.
Item 20 – PR920904, P922497	<u>Resolved</u> – Several VI Attribute values not always updating correctly including the following: vi.host.vmkernel.isolated.vlan, vi.host.vmkernel.isolated.vswitch, vi.indep.nonpersist.disk.ct, vi.ipv4, vi.ipv6, vi.snapshots.count, vi.pg.security.forgedtransmits, vi.pg.security.macchanges, vi.pg.security.promiscuous, vi.portgroup, vi.portgroup.all, vi.pvlan, vi.pvlan.all, vi.vlan, vi.vlan.all, vi.vhci.enabled, vi.vnic.count, vi.vswitch, vi.folder, vi.cluster, vi.pvlan Also removed viname which was duplicate of name
Item 21 – PR919591	<u>Resolved</u> – Standby center creation in HA scenario can hang at 59%
Item 22 – PR920448	<u>Resolved</u> – An SVM can appear as not communicating in the GUI even though communication is actually established and working properly. This can occur when AV settings are changed.
Item 23 – PR916580	<u>Resolved</u> – Removing a vNIC from a protected VM can cause RuntimeException in error.log node is null.
Item 24 – PR920564	<u>Resolved</u> – Alert not being generated correctly for VM's which are not properly protected (alert initially appears in management center interface but doesn't persist longer than an hour as it should)
Item 25 – PR921164	<u>Resolved</u> – vCloud Director integration can miss changes during SDC down time.
Item 26 – PR889510, PR917682	<u>Resolved</u> – Null pointer exceptions can occur in the handling of enforced policies.

Item 27 – PR908393	<u>Resolved</u> – Secured VM's are not presented correctly in 'Security VMs Settings' table on an import of the SVM.
Item 28 – PR909605	<u>Resolved</u> – Incorrect global policy status for specific VM (apply policy action worked but, the GUI of the management center isn't updated properly)
Item 29 – PR909710	<u>Resolved</u> – Upgrade to 5.5R4 results in unstable management center connection and disconnected Firewalls
Item 30 – PR910386	<u>Resolved</u> – SVM's protected field is empty (0 VMs) after Security VM IP Configuration update action. Workaround is to restart the management center.
Item 31 – PR912733, PR916746	<u>Resolved</u> – Upgrade to 5.5R4H1 can incorrectly result in vm's getting default reject policy. Restrictive policy sent to vm after it's created causing unintended down time. Global or default policy of any accept can be used to recover.
Item 32 – PR916304, PR915609	<u>Resolved</u> – Deleting and re-adding a vNIC, VM or SVM can result in the management center gui failing.
Item 33 – PR916568	<u>Resolved</u> – Unexpected exceptions in error.log when running "Import SVM" scenario
Item 34 – PR916585	<u>Resolved</u> – Group priority null pointer exception can cause exceptions in error.log
Item 35 – PR917044	<u>Resolved</u> – Static Group members after upgrade aren't applied correctly
Item 36 – PR917892	<u>Resolved</u> – Autosecure policy Smart Groups did not generate policy change notifications and could cause null or incorrect policy to be sent.

Release Date July-30-2013 (5.5R4 HF1). **REVIEW ITEM #1 FOR IMPORTANT INFORMATION PRIOR TO UPDATING**

Build Number 5.5.c-8-4	Summary of Fixes and/or Open Issues
Item 1 – Update Notification!	<p>There are some important items to be aware of when using this release. It should only be used in clean installations. The online update server has been disabled until the below items are fixed (PR914288). The following items should be avoided even in a clean installation:</p> <ol style="list-style-type: none"> 1. Avoid deleting/re-adding a VM or VM NIC – This can currently cause synchronization issues 2. Avoid Pressing on the Settings->vCenter integration -> Update VMs button or running the corresponding operation via XML-RPC APIs. 3. Before applying a policy, check the content of smart groups in its source/destination <ul style="list-style-type: none"> – Settings->Groups edit group, check the VMs in it are the expected ones – Click on Test and see that the number of matching VMs is the same as in the saved group <p>A fix (HF2) is expected by Mid to Late Sept 2013.</p> <p>Also note for any customer who updated to this build already from previous posting of you should avoid use of auto-secure, auto push policy groups and make sure your vGW elements (management center and SVM) aren't auto-protected.</p>
Item 2 – PR889510, PR917682	<u>Known</u> – Null pointer exceptions can occur in the handling of enforced policies.
Item 3 – PR908393	<u>Known</u> – Secured VM's are not presented correctly in 'Security VMs Settings' table on an import of the SVM.
Item 4 – PR909605	<u>Known</u> – Incorrect global policy status for specific VM (apply policy action worked but, the GUI of the management center isn't updated properly)
Item 5 – PR909710	<u>Known</u> – Upgrade to 5.5R4 results in unstable management center connection and disconnected Firewalls

Item 6 – PR910386	<u>Known</u> – SVM's protected field is empty (0 VMs) after Security VM IP Configuration update action. Workaround is to restart the management center.
Item 7 – PR912733, PR916746	<u>Known</u> – Upgrade to 5.5R4H1 can incorrectly result in vm's getting default reject policy. Restrictive policy sent to vm after it's created causing unintended down time. Global or default policy of any accept can be used to recover.
Item 8 – PR916304, PR915609	<u>Known</u> – Deleting and re-adding a vNIC, VM or SVM can result in the management center gui failing.
Item 9 – PR916568	<u>Known</u> – Unexpected exceptions in error.log when running "Import SVM" scenario
Item 10 – PR916585	<u>Known</u> – Group priority null pointer exception can cause exceptions in error.log
Item 11 – PR917044	<u>Known</u> – Static Group members after upgrade aren't applied correctly
Item 12 – PR917892	<u>Known</u> – AutoPush policy Smart Groups did not generate policy change notifications and could cause null or incorrect policy to be sent.
Item 13 – PR907952	<u>Resolved</u> – vGW Security VM's (SVM's) were not showing protected vm's after an upgrade to 5.5 R4. This was do to a race condition in the heartbeat mechanism for 5.5R4. The race condition can clear itself but 5.5R4HF1 changes the calculation process to avoid the condition all together.
Item 14 – PR895906	<u>Resolved</u> – Debug modifications for 'updatedAPPGroupsOnly -InstalledPolicy is null for node' messages.
Item 15 – PR899543	<u>Resolved</u> – Compliance dashboard for vm with machined_id=1 shows all rules
Item 16 – PR901493	<u>Resolved</u> – Default policy was being pushed to vGW Security VM's (SVM's) when they should not have been. This happened in a race condition when vNIC object changes occurred while a system sync was in process.
Item 17 – PR904539	<u>Resolved</u> - In rare occasions on upgrades, IPv6 Traffic can be blocked unexpectedly because of a cache issue in the policy synchronization procedure. The workaround was to disable and renable ipv6 on the SVM. With this version no workaround is required.

Release Date July-25-2013 (5.5R4)

Build Number 5.5.c-8-3	Summary of Fixes and/or Open Issues
Item 1 – Update Notification!	<p>Warning: The IDS Configuration was completely replaced in 5.5 R3 and on-ward. The new version requires all signatures to be reconfigured. See the 5.5 R3 release notes for further information. All existing IDS customers must upgrade to this version before year-end to keep receiving feeds properly.</p> <p>In some cases, upgrading the vGW management system from a previous vGW version will not perform a proper reboot after the update completes. When the update completes you will see a message stating 'Rebooting in x minutes...' however the reboot never actually occurs. You must monitor the update and make sure that the vGW management center reboots when this message is displayed. Do not reboot it during the update prior to seeing this message. It's strongly recommended you backup the system prior to performing the update.</p> <p>The vGW Security Design management server should be updated prior to updating any Security VM's!</p>
Item 2 – PR881933	<p>New – We now fully support VMware AutoDeploy with a gui configurable section in Settings -> Install Settings. You can define which hosts will have the SVM deployed out after VMware installs the host.</p> <p>More details available in the product and SDK documentation.</p> <p>http://www.juniper.net/support/downloads/?p=vgw#docs</p>

Item 3 – PR904539	<u>Known</u> – In rare occasions on upgrades, IPv6 Traffic can be blocked unexpectedly because of a cache issue in the policy synchronization procedure. The workaround is to disable and enable ipv6 on the SVM.
Item 4 – PR818017	<u>Known</u> – An unexpected alert when saving a backup location on a new Security Design vGW center VM can occur. Workaround is to re-try the save.
Item 5 – PR817723	<u>Known</u> – Introspection “Image Enforcer” profile option “Apps matching previous scan are acceptable” is lost (unselected) after a restart of the Security Design vGW center VM. Failed to reproduce
Item 6 – PR815880	<u>Known</u> – On-demand AV scans and introspection can fail to delete snapshots on disks which required ‘snapshot consolidation’.
Item 7 – PR831653	<u>Known</u> – On-access scans in which the protected vm’s have pending authentication requests can cause high cpu utilization (workaround is to disable authentication).
Item 8 – PR876398	<u>Known</u> – Batch updates from 5.5 R2 to R3 can fail. Workaround is to do updates individually.
Item 9 – PR808516	<u>Known</u> – Group policy not being applied correctly to a VM in a rare case. More debug information added in order to try and determine root cause. Failed to reproduce
Item 10 – PR817487, PR817715, PR831939	<u>Resolved</u> – vGW 5.5 requires all SVM’s to be on version 5.5 in order to fully activate IPv6 functionality. Once all SVM’s are updated to 5.5 the vGW SD VM changes mode to allow policy push of IPv6 objects. If subsequently an older (non-5.5) SVM is imported into the center the vGW SD VM will fail to push security policy. The workaround is to upgrade the older SVM to 5.5. Also, firewall rules with IPv6 protocols should not be created and saved until all SVM’s are of version 5.5 or later (unexpected parsing errors may occur). In general if you wish to use IPv6 run an entire vGW 5.5 environment (no 5.0).
Item 11 – PR868700	<u>Resolved</u> – Logging into the Security Design vGW Center can take multiple minutes. As a workaround Compliance rules can be disabled.
Item 12 – PR880494	<u>Resolved</u> – External inspection devices now get ipv4 address in addition to ipv6 addresses correctly. Devices are now always sent. Fixes External Device break from previous build
Item 13 – PR713852	<u>Resolved</u> – Small gui edit in alert settings so they can’t be changed without being enabled.
Item 14 – PR849657	<u>Resolved</u> – SVM’s not associating with any ESXi hosts after patching the host to update 2. Improved gui related to association process.
Item 15 – PR844033, PR723730, PR844565	<u>Resolved</u> – VC sync improvements and new mechanism for policy calculations during apply and status checks. New heartbeat mechanism (performance and scale enhancements).
Item 16 – PR883115	<u>Resolved</u> – Updated fallback installer to include esxi 5 commands.
Item 17 – PR883374	<u>Resolved</u> – Added API for updating VM by viid or uuid (updateVM). Helps avoid vm sync if vm creation race condition occurs.
Item 18 – PR869296, PR865836	<u>Resolved</u> – Various setup wizard and gui improvements (text changes, copyright, etc.)
Item 19 – PR885023, PR893542	<u>Resolved</u> – SRX Zone synch is now fixed. (Changed the AD username input field to not collide with the username of the SRX Zone definition).
Item 20 – PR886062, PR723730	<u>Resolved</u> – Null pointer exceptions on os == null and managedobject references.
Item 21 – PR886757	<u>Resolved</u> – Added a configurable parameter (center.fw.policy.rate) to tune the firewall status checker (controlling policy check rates). The value is in minutes and default is 5.
Item 22 – PR886799	<u>Resolved</u> – When changing the protocol after editing the text below, for icmp6 the text remains upon return and for the rest the text disappears.
Item 23 – PR870400	<u>Resolved</u> – Improved VMware Tools handling and cache interaction. IP’s were being removed improperly from vGW and not being readed.

Item 24 – PR885928	<u>Resolved</u> – Improved the security of logging commands to system files.
Item 25 – PR868961	<u>Resolved</u> – Fixed issue in which kernel update failed stating “The format of the VIB is invalid”
Item 26 – PR888950	<u>Resolved</u> – Fixed ‘Unable to locate data center id’ error on installation.
Item 27 – PR880591	<u>Resolved</u> – Smart Group lost policy and needed to be re-installed for traffic to flow again.
Item 28 – PR890922	<u>Resolved</u> – When trying to disable traffic monitoring there’s a check that if console monitoring is on at least one vSwitch is selected. This check done only on save of console monitoring.
Item 29 – PR893058	<u>Resolved</u> – SVM removal step progress not showing correct percentage.
Item 30 – PR893539, PR894621	<u>Resolved</u> – VM’s not automatically added to a dynamic group on vi.resourcepool changes. Also issue on vf.has.installed.policy.
Item 31 – PR894498	<u>Resolved</u> – vCloud Integration issue reading any vCenter attributes after reboot of the Security Design vGW center VM.
Item 32 – PR890770, PR895561	<u>Resolved</u> – Added back IDS sig data so ‘internal error’ won’t occur on old alerts. Also fix for ‘firewall was unable to process the policy when applying IDS policy’.
Item 33 – PR893837	<u>Resolved</u> – Resolve hostnames in the update file only if auto-check for updates is enabled. Alert about specific hostnames on unknown host exceptions.

Release Date May-6-2013 (5.5R3)

Build Number 5.5.c-4-6	Summary of Fixes and/or Open Issues
Item 1 – Update Notification!	<p>Warning: The IDS Configuration has been completely replaced. The new version requires all signatures to be re configured. See Item #2 below prior to updating to 5.5 R3. All existing IDS customers must upgrade to this version before year-end to keep receiving feeds properly.</p> <p>In some cases, upgrading the vGW management system from a previous vGW version will not perform a proper reboot after the update completes. When the update completes you will see a message stating ‘Rebooting in x minutes...’ however the reboot never actually occurs. You must monitor the update and make sure that the vGW management center reboots when this message is displayed. Do not reboot it during the update prior to seeing this message. It’s strongly recommended you backup the system prior to performing the update.</p> <p>The vGW Security Design management server should be updated prior to updating any Security VM’s!</p>
Item 2 – PR854796	<p><u>New</u> – IDS Configuration and Signature Replacement. The signature mechanism and feed has been changed. A new feed and signature selection mechanism is defined in the documentation update.</p> <p>http://www.juniper.net/techpubs/en_US/vgw/information-products/pathway-pages/vgw-series/product/</p>
Item 3 – PR856242	<p><u>New</u> – A new vCloud Director integration feature is available for mapping information to vcd.tag smart group attribute. Refer to the documentation updates at above link for details on activating and using this new feature.</p>
Item 4 – PR831711	<u>Resolved</u> – On-demand scans can fail for very large disks
Item 5 – PR841264	<u>Resolved</u> – Primary Security Design Center could fail to connect to database. Occurred in situation in which disk filled improperly.
Item 6 – PR811944	<u>Resolved</u> – AV screens contained tables which weren’t displayed properly

Item 7 – PR833978	<u>Resolved</u> – Protocol groups with IPv6 were being allowed improperly after upgrades.
Item 8 – PR727088	<u>Resolved</u> – Policy maintenance could fail with internal error 500 on non-secured VM's.
Item 9 – PR836421	<u>Resolved</u> – Editing administrator without changing its password could corrupt the original password.
Item 10 – PR837255	<u>Resolved</u> – Delegate center wasn't getting AV Scanner Config properly.
Item 11 – PR835365	<u>Resolved</u> – Autostart delay parameter milliseconds vs seconds mismatch
Item 12 – PR839033, PR840965, PR811925, PR837958, PR847541	<u>Resolved</u> – Various minor gui element fixes (reporting popups, table alignment, setting registry values, etc.)
Item 13 – PR830468, PR855237	<u>Resolved</u> – Memory leak fix caused by uuidvm's function. Also memory leak in some underlying rAPA functions.
Item 14 – PR840559	<u>Resolved</u> – No longer possible to allow src/dst with empty values (due to update issues or api calls)
Item 15 – PR844033, PR844561, PR844565, PR852815	<u>Resolved</u> – vCenter Sync improvements for scale and stability. Improvements in Heartbeat mechanisms and other scale enhancements. Policy status performance improvements. AgentConfig caching added.
Item 16 – PR843754	<u>Resolved</u> – ICMP filter report causing Null Pointer Exception
Item 17 – PR723730	<u>Resolved</u> – NTP value checking behavior changes to avoid notify errors.
Item 18 – PR854330	<u>Resolved</u> – Added hourly memory tracking log
Item 19 – PR855240, PR855522, PR856358, PR859254, PR859408	<u>Resolved</u> – Various checks to make SVM, Host tracking and monitoring more robust.
Item 20 – PR844030	<u>Resolved</u> – Removed 4 minute limitation on log filtering.
Item 21 – PR864347	<u>Resolved</u> – Status Tab changes for high availability configuration.
Item 22 – PR843714	<u>Resolved</u> – ICMPv6 logs were not being filtered correctly in the logs.
Item 23 – PR873454	<u>Resolved</u> – Calling Machine.ipAddressList instead of Machine.ipAddress to get the current ip addresses the machine holds. Fixes ip update event with multiple IPs
Item 24 – PR877173	<u>Resolved</u> – Various locking and synch improvements.
Item 25 – PR817487, PR817715, PR831939	<u>Known</u> – vGW 5.5 requires all SVM's to be on version 5.5 in order to fully activate IPv6 functionality. Once all SVM's are updated to 5.5 the vGW SD VM changes mode to allow policy push of IPv6 objects. If subsequently an older (non-5.5) SVM is imported into the center the vGW SD VM will fail to push security policy. The workaround is to upgrade the older SVM to 5.5. Also, firewall rules with IPv6 protocols should not be created and saved until all SVM's are of version 5.5 or later (unexpected parsing errors may occur). In general if you wish to use IPv6 run an entire vGW 5.5 environment (no 5.0).
Item 26 - PR808516	<u>Known</u> – Group policy not being applied correctly to a VM in a rare case. More debug information added in order to try and determine root cause. Failed to reproduce
Item 27 – PR818017	<u>Known</u> – An unexpected alert when saving a backup location on a new SD vGW VM can occur. Workaround is to re-try the save.
Item 28 – PR817723	<u>Known</u> – Introspection "Image Enforcer" profile option "Apps matching previous scan are acceptable" is lost (unselected) after a restart of the Security Design vGW VM. Failed to reproduce
Item 29 – PR815880	<u>Known</u> – On-demand AV scans and introspection can fail to delete snapshots on disks which required 'snapshot consolidation'.

Item 30 – PR831653	<u>Known</u> – On-access scans in which the protected vm's have pending authentication requests can cause high cpu utilization (workaround is to disable authentication).
Item 31 – PR868700	<u>Known</u> – Logging into the Security Design vGW Center can take multiple minutes. As a workaround Compliance rules can be disabled.
Item 32 – PR876398	<u>Known</u> – Batch updates from 5.5 R2 to R3 can fail. Workaround is to do updates individually.

Release Date November-19-2012 (5.5R2)

Build Number 5.5.c-2-8	Summary of Fixes and/or Open Issues
Item 1 – Update Notification!	In some cases, upgrading the vGW management system from a previous vGW version will not perform a proper reboot after the update completes. When the update completes you will see a message stating 'Rebooting in x minutes...' however the reboot never actually occurs. You must monitor the update and make sure that the vGW management center reboots when this message is displayed. Do not reboot it during the update prior to seeing this message. It's strongly recommended you backup the system prior to performing the update. The vGW Security Design management server should be updated prior to updating any Security VM's!
Item 2 - PR816047	<u>Resolved</u> – Backup from restoration file could fail unexpectedly.
Item 3 - PR821774	<u>Resolved</u> – Security VM's showing "fastpath status = not ok". Caused by a large number of deleted vm's not being purged correctly in the vGW Center database.
Item 4 - PR821310	<u>Resolved</u> – Statistics in dropped connections not being reset correctly in all cases.
Item 5 - PR823722	<u>Resolved</u> – Compliance rule for vi.ipv4 behavior different than behavior in 4.5. The vi.ipv4 attribute was changed to report back properly.
Item 6 - PR823526	<u>Resolved</u> – Additional messaging added to notify users about upgrade process (to avoid update attempts between untested versions).
Item 7 - PR825716	<u>Resolved</u> – Log collections didn't contain all information related to pgsqL.
Item 8 - PR814506	<u>Resolved</u> – vGW Center upgrades from centers that were originally very old (3.0, 4.0) could fail.
Item 9 - PR823386	<u>Resolved</u> – Registry value scans could fail if they contained the "/" character
Item 10 – PR818769	<u>Resolved</u> – IDS alerts under load for warnings related to the number of dropped packets can be incorrectly formatted causing an exception 'Format specifier 'o' in the error logs.
Item 11 – PR818976	<u>Resolved</u> – The event and status alert words 'High', 'Medium' are truncated to 'Hig', 'Mediu'
Item 12 – PR818945	<u>Resolved</u> – The 'Search' text doesn't disappear in the left hand screen when searching for objects (though the search still works fine).
Item 13 – PR818771	<u>Resolved</u> – The Main->Quarantine screen has three filter selection check boxes (AntiVirus, Compliance, Image Enforcer) de-selection of any option automatically re-selects the option.
Item 14 – PR818770	<u>Resolved</u> – The events and alerts 'Consolidated Search' doesn't work properly unless 'all machines' is selected in the left hand navigation screen (an error stating failed to load page error in processing) is displayed.
Item 15 – PR817871	<u>Resolved</u> – Selecting an individual vNIC can cause a 'server error 500'
Item 16 – PR751592	<u>Resolved</u> – Race condition in which vNIC in the left side navigation tree wasn't rendering properly before being able to be highlighted as the selected element.

Item 17 – PR819120, PR751592, PR828366	<u>Resolved</u> – Various GUI improvements (Missing label tag on radio button in Active Directory setup, AV quarantine file display, vNIC message display improvements, folder toggling behavior fix, Compliance alignment issues)
Item 18 – PR811944	<u>Resolved</u> – AntiVirus table on dashboard not lining up correctly.
Item 19 – PR814258, PR817752, PR792719, PR815843	<u>Resolved</u> – After activating the ‘Enable Monitoring-Only option for VMsafe’ then disabling it you will only be able to deploy in monitor-only mode. To workaround this issue reactivate monitor-only mode again which will give you back both Monitor and Firewall+Monitor modes and allow you to deploy in either mode. Also resolved issue in which VM’s were not moved to monitored network properly (VM is being unsecured after deploying in monitoring mode).
Item 20 – PR818768	<u>Resolved</u> – Error message ‘null protocol in rule x’ which occurred when the negate policy action was used and then protocols were added and removed.
Item 21 – PR816663	<u>Resolved</u> – Null pointer exception when trying to activate a backup without first saving a configuration.
Item 22 – PR820377	<u>Resolved</u> – Incorrectly printing “Last update failed for <svm name>”.
Item 23 – PR818970	<u>Resolved</u> – Introspection edit profile selection options not always working properly.
Item 24 – PR819070	<u>Resolved</u> – New vNIC adds to a VM (which is already secured) not resulting in the new vNIC being secured automatically.
Item 25 – PR826277	<u>Resolved</u> – After on-access scan and subsequent display of ‘Internal Error’ (resulting from a memory leak).
Item 26 – PR827886	<u>Resolved</u> – Potential for constantly retrying to reconfigure a protected vm if unsecure flag was modified in vmx file for a specific vnic.
Item 27 – PR828561	<u>Resolved</u> – Introspection Image Enforcer wrongly showing 100% when there are no matching VM’s
Item 28 – PR810972, PR830067	<u>Resolved</u> – vGW Center 5.5 wasn’t properly pushing policy to vGW SVM’s prior to 5.5R
Item 29 – PR831072	<u>Resolved</u> – Fixed policy save problem which was resulting in message stating ‘could not save policy due to the following reason: already in map:1’
Item 30 – PR831299	<u>Resolved</u> – Cloud SDK was returning ‘any-ipvx’ instead of ‘any’ on get policies (src/dst values)
Item 31 – PR808044	<u>Resolved</u> – If only on-access AV is configured it is now possible to move a vm out of infected status by making sure there are no infected files in the quarantine. (a clean run from on-demand is not necessary to allow the vm back into a clean state).
Item 32 – PR824967	<u>Resolved</u> – Removed error messages in the log collection which appear when Security VM’s don’t have internet access. The ‘auto update’ flag in Settings->Updates will now disable SVM update check in batch update. If the flag is unchecked, the SVM status should also say that checks are disabled along with the last check status.
Item 33 – PR817487, PR817715, PR831939	<u>Known</u> – vGW 5.5 requires all SVM’s to be on version 5.5 in order to fully activate IPv6 functionality. Once all SVM’s are updated to 5.5 the vGW SD VM changes mode to allow policy push of IPv6 objects. If subsequently an older (non-5.5) SVM is imported into the center the vGW SD VM will fail to push security policy. The workaround is to upgrade the older SVM to 5.5. Also, firewall rules with IPv6 protocols should not be created and saved until all SVM’s are of version 5.5 or later (unexpected parsing errors may occur). In general if you wish to use IPv6 run an entire vGW 5.5 environment (no 5.0).
Item 34 – PR808516	<u>Known</u> – Group policy not being applied correctly to a VM in a rare case. More debug information added in order to try and determine root cause.
Item 35 – PR818017	<u>Known</u> – An unexpected alert when saving a backup location on a new SD vGW VM can occur. Workaround is to re-try the save.
Item 36 – PR817723	<u>Known</u> – Introspection “Image Enforcer” profile option “Apps matching previous scan are acceptable” is lost (unselected) after a restart of the Security Design vGW VM.

Item 37 – PR815880	<u>Known</u> – On-demand AV scans and introspection can fail to delete snapshots on disks which required 'snapshot consolidation'.
Item 38 – PR831653	<u>Known</u> – On-access scans in which the protected vm's have pending authentication requests can cause high cpu utilization (workaround is to disable authentication).
Item 39 – PR831711	<u>Known</u> – On-demand scans can fail for very large disks

Release Date September-24-2012 (5.5R1)

Warning: Customers updating from vGW 5.0 should only implement Security Design vGW 5.5 R2 or later (Security Design vGW 5.5 R1 can't manage both vGW 5.0 and vGW 5.5 SVM's at the same time).

Build Number 5.5.c-2-7	Summary of Fixes and/or Open Issues
Item 1 – Update Notification!	In some cases, upgrading the vGW management system from a previous vGW version will not perform a proper reboot after the update completes. When the update completes you will see a message stating 'Rebooting in x minutes...' however the reboot never actually occurs. You must monitor the update and make sure that the vGW management center reboots when this message is displayed. Do not reboot it during the update prior to seeing this message. It's strongly recommended you backup the system prior to performing the update. The vGW Security Design management server should be updated prior to updating any Security VM's!
Item 1 – PR806937	<u>Known</u> – After un-securing a VM the status window can stick. Workaround is to just click on a different page within the user interface.
Item 2 – PR807256	<u>Known</u> – Compliance and non-compliance state changes for Image Enforcer not updating automatically (you have to actually click inventory tree)
Item 3 – PR810704	<u>Known</u> – A message stating "Virtual ethernet card 'Network adapter 1' is not supported. This is not a limitation of the host in general, but of the virtual machine's configured guest OS on the selected host." can occur if the VMware Hardware version is not updated. Please see KB20798 for a workaround.
Item 4 – PR810800	<u>Known</u> – Apply policy can fail if there are switches between static and dhcp interface use and policy per vNIC. Additional attempts should work
Item 5 – PR814258, PR817752	<u>Known</u> – After activating the 'Enable Monitoring-Only option for VMsafe' then disabling it you will only be able to deploy in monitor-only mode. To workaround this issue reactivate monitor-only mode again which will give you back both Monitor and Firewall+Monitor modes and allow you to deploy in either mode.
Item 6 – PR814964	<u>Known</u> – AV On-Demand scans can very rarely fail with a 'General Error' displayed in the AV status viewer. The workaround is to re-scan the VM (the cause is an exception in mounting the virtual disk).
Item 7 – PR815159, PR815552	<u>Known</u> – Foreign languages in the Introspection results aren't displayed correctly. Also it's possible to have day of month displayed as '0 th '
Item 8 – PR815880	<u>Known</u> – Introspection and AV On-Demand scans and AV authentication rely on snapshots. If a VM is in a state saying "Configuration issues: Virtual machine disks consolidation needed", vGW can fail to remove all relevant snapshots. This becomes particularly visible in AV situations. To avoid this, please see VMware directions on 'Snapshot Consolidation' (http://blogs.vmware.com/vsphere/2011/08/consolidate-snapshots.html)
Item 9 – PR817487, PR817715	<u>Known</u> – vGW 5.5 requires all SVM's to be on version 5.5 in order to fully activate IPv6 functionality. Once all SVM's are updated to 5.5 the vGW SD VM changes mode to allow policy push of IPv6 objects. If subsequently an older (non-5.5) SVM is imported into the center the vGW SD VM will fail to push security policy. The workaround is to upgrade the older SVM to 5.5. Also, firewall rules with IPv6 protocols should not be created and saved until all SVM's are of version 5.5 or later (unexpected parsing errors may occur).

Item 10 – PR817723	<u>Known</u> – Introspection “Image Enforcer” profile option “Apps matching previous scan are acceptable” is lost (unselected) after a restart of the Security Design vGW VM.
Item 11 – PR817871	<u>Known</u> – Selecting an individual vNIC then navigating to the Introspection module can cause a ‘server error 500’
Item 12 – PR818017	<u>Known</u> – An unexpected alert when saving a backup location on a new SD vGW VM can occur. Workaround is to re-try the save.
Item 13 – PR818770	<u>Known</u> – The events and alerts ‘Consolidated Search’ doesn’t work properly unless ‘all machines’ is selected in the left hand navigation screen (an error stating failed to load page error in processing) is displayed.
Item 14 – PR818771	<u>Known</u> – The Main->Quarantine screen has three filter selection check boxes (AntiVirus, Compliance, Image Enforcer) de-selection of any option automatically re-selects the option.
Item 15 – PR818945	<u>Known</u> – The ‘Search’ text doesn’t disappear in the left hand screen when searching for objects (though the search still works fine).
Item 16 – PR818976	<u>Known</u> – The event and status alert words ‘High’, ‘Medium’ are truncated to ‘Hig’, ‘Mediu’
Item 17 – PR818769	<u>Known</u> – IDS alerts under load for warnings related to the number of dropped packets can be incorrectly formatted causing an exception ‘Format specifier ‘o’ in the error logs.

vGW Security VM

The below table summarizes each of the releases for the vGW Security VM. The date of the release and build number are noted as well as a summary of the fix or open issue.

Release Date May-6-2013 (5.5R3). Notes this is latest version also compatible with 5.5R4 Center

Updating to this version from 5.0 will subsequently update the vGW Kernel Module on the ESX/ESXi host. This operation will require the host be placed into maintenance mode (which vGW will attempt to do automatically). Clean installations of this version will not require maintenance mode.

Build Number 5.5.a-5-1	Summary of Fixes and/or Open Issues
Item 1 – PR863414	<u>New</u> – The Security VM (SVM) deployed on each host now requires 1GB vRAM instead of 512MB
Item 2 – PR862446	<u>Resolved</u> – Packet truncation issue in IDS processing.
Item 3 – PR821831	<p><u>Known</u> – High CPU utilization / frequent AV scan’s can occur if there are any processes in VM’s marked for AV protection which constantly access files (for example disk defragment tools). A workaround is to disable these tools during AV protection. Also see ‘Disable the Windows Customer Experience Improvement Program’ (see VMware View documentation or Microsoft documentation for disabling this).</p> <p>http://pubs.vmware.com/view-51/index.jsp?topic=%2Fcom.vmware.view.administration.doc%2FGUID-BE82165B-13BC-4FD9-A9CF-FBEF6343D98A.html</p>

Release Date February-6-2013 (5.5R2)

Updating to this version will subsequently update the vGW Kernel Module on the ESX/ESXi host. This operation will require the host be placed into maintenance mode (which vGW will attempt to do automatically). Clean installations of this version will not require maintenance mode.

Build Number 5.5.a-2-1	Summary of Fixes and/or Open Issues
Item 1 – PR807233, PR825716	<u>Resolved</u> – Log rotation changed to run hourly rather than daily.
Item 2 – PR824135, PR821831, PR748820	<u>Resolved</u> – Extremely large groups/policy objects (1000's) for a single SVM could result in error messages that are too large being passed from daemon to kernel. This could result in abnormally high CPU utilization on the SVM.
Item 3 – PR827863, PR828179, PR828352, PR839075	<u>Resolved</u> – IPv6 address ranges in policy and dynamic groups needed to use network order layout b/c otherwise there could be incorrect source and destination information in the connection logs and NetFlow transmissions (packet stats wrong for IPv6). Also fixed issues in complex connections with wrong src/dst.
Item 4 – PR815551	<u>Resolved</u> – Increased protections against malformed packets
Item 5 – PR821831	<u>Known</u> – High CPU utilization / frequent AV scan's can occur if there are any processes in VM's marked for AV protection which constantly access files (for example disk defragment tools). A workaround is to disable these tools during AV protection. Also see 'Disable the Windows Customer Experience Improvement Program' (see VMware View documentation or Microsoft documentation for disabling this). http://pubs.vmware.com/view-51/index.jsp?topic=%2Fcom.vmware.view.administration.doc%2FGUID-BE82165B-13BC-4FD9-A9CF-FBEF6343D98A.html

Release Date September-24-2012 (5.5R1)

Updating to this version will subsequently update the vGW Kernel Module on the ESX/ESXi host. This operation will require the host be placed into maintenance mode (which vGW will attempt to do automatically). Clean installations of this version will not require maintenance mode.

Build Number 5.5.a-1-2	Summary of Fixes and/or Open Issues
No known issues.	No known issues.

vGW Endpoint

The below table summarizes each of the releases for the vGW Endpoint software. The date of the release and build number are noted as well as a summary of the fix or open issue.

Note: The vGW Endpoint software is available as a link in Settings -> AV Settings within SD vGW interface. However, it's best to download the very latest from Juniper web site (<https://www.juniper.net/support/products/vgw/#sw>)

There is not a new version of vGW Endpoint for vGW 5.5 (the below is compatible with both 5.5 and 5.0 vGW Center and SVM)

Release Date July -9 -2014 (6.0R1)

Build Number 6.0-R1-22824	Summary of Fixes and/or Open Issues
Item 1 - PR:998211	<u>Resolved</u> : Fixed the issue of upgrading endpoint version from 21848 to 22805.
Item 2 - PR 996131	<u>Resolved</u> : Fixed the issue of file scan filter.

Item 3 - PR 988753	<u>Resolved</u> : Fixed the issue of AV Endpoint vGW 5.5 uninstallation.
Item 4 - PR 989418	<u>Resolved</u> : Fixed the issue of endpoint major version string.
Item 5 - PR 987079	<u>Resolved</u> : Fixed the issue of blue screen after upgrading vGW 5.5 to Host 6.0.

Release Date January-24-2012 (5.0R2)

Build Number 5.0-R2-17233	Summary of Fixes and/or Open Issues
Item 1 - #726733	<u>Known</u> – vGW Endpoint doesn't currently stop installation execution on unsupported operating systems. The install may appear to work or fail silently and leave the system in an unexpected state. Until this behavior is changed please examine the supported operating system table (listed below) carefully.
Item 2 - #724172, #716629, #R16986	<u>Known</u> – Occasionally installations on Windows 2008 R2 x64 will report that the driver failed to load even though it has worked normally. Re-trying will clear the notification issue. Network Access Protection not tested in Windows 2008 R2 64 Bit.
Item 3 - #730957	<u>Known</u> – The vGW Endpoint package was not signed by Juniper and will therefore appear as an unknown publisher upon installation (and removal). This error message can be safely ignored (verify the md5sum of the download site and package or use the package within the vGW SD management system).
Item 4 - #4228, #4156, PR814027	<u>Fixed</u> - improper version display on the vGW Endpoint interface
Item 5 - PR805817	<u>Known</u> - vGW Endpoint can not be used in IPv6 only environments. IPv4 is required for on-access scans via vGW Endpoint.

vGW Endpoint Operating System Coverage – Build 5.0-R2-17233

All Supported Operating Systems	Windows Security Center Integration	Certified Windows Compatible (Winqual)	Package Signature by Juniper
Windows XP 32-Bit	N/A	No	No
Windows XP 64-Bit	N/A	No	No
Windows 7 32-Bit	Yes	Yes	No
Windows 7 64-Bit	Yes	Yes	No
Windows 2003 32-Bit	N/A	No	No
Windows 2003 64-Bit	N/A	No	No
Window 2008 R2 64-Bit	No	Yes	No