



NetScreen-Security Manager Release Notes

Release 2007.1r3
6/19/07

Contents

- 1 Version Summary on page 2
- 2 Addressed Issues on page 2
- 3 Known Issues on page 4
 - 3.1 Limitations of Features on page 4
 - 3.2 Known Issues on page 4
 - 3.3 Known Issues in ScreenOS 5.x That Affect NetScreen-Security Manager on page 6
- 4 Getting Help on page 8

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 093-1875-000

1 Version Summary

Juniper Networks NetScreen-Security Manager is a comprehensive security management solution designed to manage device, network, and security configuration for integrated firewall, intrusion detection and prevention, and virtual private network (VPN) appliances, sensors, and systems.

2 Addressed Issues

The following issues are addressed in this release.

Attack Objects

- **223467/cs13001**—The existing custom attack objects could not be updated with the later detector version.

Device Management

- **223468/cs13002**—When VSD 0 is unset, an option to create the sub-interface on the cluster level was unavailable.
- **225142/cs13495**—When VSD 0 is unset, an interface could not be removed from the redundant group.
- **226685/cs13800**—NSM does not allow adding more than 3 outgoing interfaces in a multicast route group.
- **226770/cs13813**—Option to enable BGP on an interface is not available on a template, until the IP Address is defined.
- **227439/cs13969**—When VSD 0 is unset and the device config imported, overrides were displayed on the cluster members and also Routes could not be added using the VSI interfaces.
- **224005/cs13185**—An error is displayed with the bandwidth is set to 1000Mbps on the predefined ethernet1/1 to ethernet1/4 interfaces on an ISG 1000 with ScreenOS 5.3rX.

Device Directives

- **221406/cs12428**—Cert Hash on the Device and NSM were different since NSM did not account for all the values present in the Cert.
- **222294/cs12647**—Attack Object Updates to Standalone IDPs failed when performed via guiSvrCli.sh.
- **222605/cs12729**—Since the cert hash value did not match between NSM and ScreenOS, a cert would be deleted and re-added on update - see 221491.
- **222796/cs12775**—Device Update fails on an ISG-IDP device, when the device has an IDP key but does not have a security module.
- **223847/cs13131**—With ScreenOS 5.0, an incorrect format of the VIP command was updated to the device.

- **225533/cs13598**—Defining Proxy Settings via the Preferences fails to define these proxy settings.
- **226026/cs13702**—During an import, the mgt zone is changed to the untrust zone on a SSG550 with ScreenOS 5.4rX.

High Availability

- **224042/cs13196**—When the HA server fails over from the Primary to the Secondary server, the older transaction logs do not get deleted which causes the GUI Server not to start.
- **224512/cs13344**—If more than 1 RIP neighbor is configured, only the last entry will get updated to the device.
- **225070/cs13475**—Replication incorrectly reported a failure due to the temp files created by the log forwarding.

Profiler

- **224783/cs13410**—Profiler failed since the profiler database failed to recognize some timezones.

Installation/Upgrade

- **221123/cs12360**—Upgrade from NSM 2005.3rX or 2006.1rX corrupts custom admin roles.
- **222536/cs12717**—Install script used to check for a lower available disk space in the /tm directory.
- **223022/cs12823**—After an upgrade from a release earlier to 2007.1r1, the Install script failed to delete the older files used in 2007.1r1 and below, only when the default directory of /var/netscreen/GuiSvr was not chosen.
- **224790/cs13417**—When an upgrade failed for the first time and refreshed, the var directory of the HA server got deleted.

Logs & Reports

- **220643/cs12254**—Forwarding of IDP logs to the syslog server stopped at 0000hrs and restarted at 0200hrs.
- **223384/s12990**—Log retention was to be scheduled via a cron job as the internal 24 hour timer did not function.

Monitoring

- **221908/cs12572**—On a Red Hat linux system with 4 CPU's the status monitor used to display the CPU always at 100%.

Policies

- **223083/cs12875**—Certain rules in the rule groups did not show up until the UI was restarted.

VPN

- **225016/cs13460**—NSM did not allow selecting a NULL ESP for the Phase 2 proposal.

3 Known Issues

This section describes known issues with the current release. Known issues updates are released bi-monthly. You can subscribe to the updates by going to <http://www.juniper.net/customers/support> and selecting the Subscribe to Technical Bulletins option.

3.1 Limitations of Features

None

3.2 Known Issues

The following are known deficiencies at the time of this release. Whenever possible, a work-around is suggested following the description of the problem. Workaround information starts with "W/A:".

- **209464/cs10015**—Invalid reference when trying to delete redundant sub-interface.
- **209934/gl29223**—Secondary NSM server is not configured on the IDP Sensor when the device is added to NSM. Sensor disconnects from NSM if primary server fails over to backup.

W/A: Use ACM to specify secondary server for each Sensor.

- **210073/cs10125**—Import of the device fails if keyword "admin" is used in the configuration.
- **210914/cs10348**—When filtering by "device group" under Log Viewer for the devices column, no logs are returned from the filter.
- **215443/cs11327**—Audit "Log Viewer does not show the policy changes correctly."
- **216303/cs11962**—A route created in shared vr of a custom vsys is not available in the routing table of root vsys.
- **219227/cs11955**—NSM appends `_zone` to the address name when the object name is the same in multiple zones.
- **219303/cs11962**—Custom attack signatures do not allow you to modify the supported platforms.
- **219702/cs12052**—NSRP Monitor does not show correct information when one of the NSRP peer devices is powered off.
- **219858/cs12052**—VPN monitor should display the cluster name instead of cluster members.

- **212199/cs10718**—If you update a device and the update is unsuccessful, the Audit Log Viewer "device" value is NULL.
- **221479/cs12446**—NSM does not allow changing VSD group for NSRP lite.
- **222554/gl32416**—While re-installing the management system, the "Refresh" option does not prompt you to change previously configured server parameters.
- **223131/cs12893**—NSM GUI does not allow creation of a sub-interface on a cluster level when VSD 0 is unset.

W/A: Contact JTAC for a workaround.

- **223176/cs12905**—Templates do not function when the zones and VR's belong to different templates.

W/A: Define VR & zones in the same template.

- **223234/cs12933**—When uploading firmware 5.4r2tmav and 5.4r2av-k to NSM, the incorrect version is updated to the device.

W/A: Do not upload both the firmware images at the same time. Select the one that needs to be updated to the device.

- **223518/cs13020**—Using custom CA certificates, when Best effort for Revocation checking method is used, these CLI's do not get updated to the device.

- **223661/cs13079**—NSM does not allow defining Supplemental CLI commands on a Cluster.

- **224319/cs13284**—Log Investigator times out when the NSM GUI has been idle for 30 minutes and an error "Index Timed Out" is displayed.

W/A: Ignore the error and select OK for the query to happen again.

- **225020/cs13464**—Device Statistics are not shown as a part of NSM Realtime Monitor.

- **225574/cs13611**—Unable to select a local interface on the cluster members for setting the syslog parameters.

- **226083/cs13721**—After upgrade to 2007.1r2, the setperms.sh script has to be executed such that all the processes are started as a non-root user.

- **226080/cs13718**—Installer exits with a -1 error when the /etc/sysctl.conf parameters are not updated.

W/A: Add the Shared memory shmmax values in the respective configuration & reboot the NSM server before starting the upgrade.

- **226228/cs13741**—Duplicate CLI's are sent to the device when the "Supplemental CLI" commands are configured using a template.

- **226961/cs13865**—Sensor cannot be added to the device using a MIP address. The actual interface address of the Sensor needs to be used when adding a sensor.
- **227045/cs13883**—Device update unsets the source based routes after the firmware is upgraded from 5.0 to 5.
W/A: Contact JTAC for a workaround.
- **227616/cs14020**—Device Log action does not get triggered logs generated on match with custom attack objects.

3.3 *Known Issues in ScreenOS 5.x That Affect NetScreen-Security Manager*

The following are known issue in ScreenOS 5.x that specifically affects this release of NetScreen-Security Manager:

- **220967/os67938**—NSM is unable to add a device running ScreenOS 5.4r3 code if telnet is used as the method of initial connection.
W/A: Reboot the device and re-add the device in NSM.
- **197124/os55015**—While using NetScreen-Security Manager with DI enabled on an NS-500 device running ScreenOS 5.3, you may experience issues when downloading configurations larger than 1.7MB.
- **195025/cs07488**—NetScreen-Security Manager reports an error when trying to set link-down an interface on an ISG 2000 device.
- **171897/cs3723**—It is not possible to create a configlet for a device in transparent mode.
- **194320/os53891**—When upgrading a device from ScreenOS 5.0r10 and lower to ScreenOS 5.3, devices crash.
- **194266/os53871**—Devices running ScreenOS 5.3 may crash when generating Deep Inspection logs.
- **194211/os53854**—Wireless interface zone settings on devices running ScreenOS 5.3 are always displayed as "none" in the NetScreen-Security Manager UI.
- **193924/os53710**—It is not possible to set the bandwidth on interfaces for a VSYS in ScreenOS 5.3.
- **193654/os53595**—If you change the Device Server IP address, devices running ScreenOS 5.3 are not able to connect.
W/A: Perform an "RMA Device" and "Activate Device" workflow to continue managing the device.
- **193175/os53312**—You can not nest local user groups in ScreenOS 5.3.
- **192644/os53035**—NSRD in transparent mode is not functional in ScreenOS 5.3.

- **185847/os48987**—Using NetScreen-Security Manager to upgrade security devices running ScreenOS 5.0.0 over a slow network connection (if the image download takes over 5 minutes), occasionally causes updates to time out.

W/A: In most cases, upgrading to ScreenOS 5.0.0 r10 resolves this issue. Refer to the table below for more information describing resolution of this issue in specific branches of ScreenOS.

- **179994/os45418 and 185048/cs48460**—Devices are not able to save the key used to connect to the NetScreen-Security Manager Device Server. This causes the NSM agent on the security device to have to re-negotiate the key every time the security device restarts. The key re-negotiation process can take up to 15 seconds. One side effect of this issue is that when you restart the Device Server, this will also cause key renegotiation for all other security devices running it manages. This may cause system performance degradation that then affects the management of all security devices.

W/A: In most cases, upgrading to ScreenOS 5.0.0 r10 resolves this issue. Refer to the table below for more information describing resolution of this issue in specific branches of ScreenOS.

- **174051/os43001**—If you use NetScreen-Security Manager to upgrade the firmware on a device from ScreenOS 5.0.0 to ScreenOS 5.1, the security device crashes.

W/A: In most cases, upgrading to ScreenOS 5.0.0 r10 resolves this issue. Refer to the table below for more information describing resolution of this issue in specific branches of ScreenOS.

The table below describes specific releases of ScreenOS that resolve the issues referenced above, or provides other workaround information:

Issue	5.0.0	5.0.0 r9 for 5000 M2	5.0.0-GPRS.r8.5	5.0.0 WLAN	5.0.0 r9 for ISG 1000/ISG 2000	5.0.0IDP1
185847/os48987	5.0.0 r10	Upgrade the device firmware out-of-band using the CLI or WebUI.	Upgrade the device firmware out-of-band using the CLI or WebUI.	5.0.0 r10	5.0.0 r10	5.0.0IDP1 r2
179994/os45418 and 185048/cs48460	5.0.0 r10	Upgrade the device firmware out-of-band using the CLI or WebUI.	Upgrade the device firmware out-of-band using the CLI or WebUI.	5.0.0 r10	5.0.0 r10	5.0.0IDP1 r2
174051/os43001	5.0.0 r10	5.2	5.2	5.0.0 r10	5.0.0 r10	5.0.0IDP1 r2

4 Getting Help

For more assistance with Juniper Networks products, visit:

www.juniper.net/support

Juniper Networks occasionally provides maintenance releases (updates and upgrades) for ScreenOS firmware. To have access to these releases, you must register your NetScreen device with Juniper Networks at the above web address.

Copyright © 2007 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

Juniper Networks, Inc.
ATTN: General Counsel
1194 N. Mathilda Ave.
Sunnyvale, CA 94089
U.S.A.

www.juniper.net

Writer: Patricia Wright