



NetScreen-Security Manager

Release Notes

Release 2007.1
1/25/07

Contents

- 1 Version Summary on page 2
- 2 New Features on page 2
- 3 Changes to Default Behavior on page 4
- 4 Addressed Issues on page 5
- 5 Known Issues on page 9
 - 5.1 Limitations of Features on page 9
 - 5.2 Known Issues on page 9
 - 5.3 Known Issues in ScreenOS 5.x That Affect NetScreen-Security Manager on page 10
- 6 Getting Help on page 12

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 093-1836-000

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 New Features

The following is a list of new features and enhancements in this release of NSM:

- **Screen OS 5.4 Support**—You can now manage devices running ScreenOS 5.4. ScreenOS 5.4 includes the following new features:
 - Virtual System Limits, Reserves and Alarms
 - 802.1x support on NS-5GT
 - Hard Session Timeout for Authentication
 - 3GPP R6 IE Support
 - Simple Certificate Enrollment Protocol DNS
 - Next-Server-IP information in DHCP Header
 - ICMP Router Discovery Protocol (IRDP) on 5GT
 - WPA2, XR and SuperG support on 5GT Wireless
 - SCTP and SCCP Support
 - ICAP Anti-Virus Servers
 - Policy-Based Routing
 - Log Reason for Session Close
 - DI Signature Pack Selection
 - Infranet Controller Logs
 - Infranet - Captive Portal
 - ISG Profiler
 - Ability to define the source interface with the NSM agent

- **Extranet Device Enhancements**—You can now provide additional meta data to an Extranet Device. This data may include: credential info (user/password), IP, Interface List, comments, Action Script and other additional data. A new Shared Object called "Extranet Policy" has been added to provide you with this capability. In addition, the "Update Device" directive is enabled on the extranet device. When you update an extranet device, NSM invokes a specified script with the device configuration in XML format to be pushed to the device. The device update job now shows you the XML output with an option for the you to cancel.
- **New Fields in Policy Manager**—A new column has been added in the Policy Manager called "Optional Fields". You can view it in expanded mode. In the column you can place "Shared Objects for Policy" which you create in the Object Manager. These objects contain metadata information which will not be pushed to the device. You first define the fields of the Custom Objects in the Object Manager. You next create the Custom Objects, entering data for the fields you previously defined.
- **Auto-generate Routes**—NSM now has the functionality to automatically add virtual router information using the VPN Manager for each device based on the topology. When you create a route based VPN you specify the type of topology - "Site to Site" or "Hub and Spoke" - and enable route creation. When you select "Save" NSM will trigger the auto generation of device specific virtual router data for the configured topology.
- **Drag and Drop Objects**—The NSM Security Policy Editor now allows you to drag and drop shared objects into security policies. You can drag the objects from a pull down list of objects at the bottom of the panel and drop them into the security policies at the top of the panel.
- **Log Purging, Archiving and Retrieval**—You can now purge, archive and retrieve logs via the NSM UI.
- **Custom Report Grouping**—You can now group NSM Log Filters and Reports in custom folders that you create. For Reports, this feature is enabled by an editable "Save Report In" field at the bottom of the "Save Report" dialog. For Log Viewer, this feature is enabled by an editable "Save View In" field in the "New View" dialog.
- **Global Device Templates Available in Sub-Domains**—In previous NSM releases, device templates defined in the global domain were not accessible and could not be used in sub-domains. Global-domain templates are now available for reference in sub-domains.
- **Secure Proxy Server**—Your NSM server can now be installed in an internal network with no Internet connectivity and still get security updates. Your NSM server gets the security updates by connecting to a secure proxy server.
- **Troubleshooting Enhancements**—Troubleshooting has been enhanced with an expanded command set, easier device access, and the ability to create your own custom command set. Troubleshooting capability has also been added for ISG series devices.

- **"Replace With" Functionality for Service Objects**—The "replace with" functionality found in Address Objects is now available in Service Objects as well.
- **Log2Action Device Filter**—Previously NSM log2action did not give you any provision to filter device logs on a per device basis. Log2action's CLI now gives you the provision to filter logs based on device and forward them to existing facilities - syslog, snmp, xml, csv, script, smtp.
- **Combined "Summarize Delta Config" and "Update Device"**—You can now have NSM do a "Summarize Delta Config" on a device before you update the device. You can set this option in the Preferences dialog box or you can enable the option on the option dialog box that is displayed before you do the "Update Device" directive. You can cancel the "Update Device" directive if something does not look right to you in the "Summarize Config". You can also save the "Summarize Config" output by hitting the "Save Selected" button.
- **Firmware Manager support for IDP 4.1**—You can now use NSM Firmware Manager to upgrade IDP Sensor firmware. Firmware Manager can upgrade standalone IDP Sensors from any 4.0 release to 4.1, or from 4.1 to later releases, but it cannot upgrade Sensors from one 4.0 release to another 4.0 release.
- **Update IDP Policy Only**—You can now update IDP policies specifically for ISG 1000 and ISG 2000 devices with IDP security modules. This allows you to not push any changes to the zone-based and global firewall security policies on ISG devices.

3 Changes to Default Behavior

- NSM 2007.1 requires customers managing IDP 4.0 devices to perform the following steps in order for Profiler to display the core time stamps of logs:
 1. In the NSM UI, edit each IDP device that has profiler enabled, and input a GMT offset value in the device "info" page. It is important to touch this value and save it in NSM before re- importing the profiler data.
 2. If you have existing Profiler data, clear the profiler database from the Profiler view. You can do this by selecting **Security Monitor > Profiler** and then selecting the delete profiler button on the top right side view. All the old profiler information will be purged.
 3. ssh to the standalone idp device as admin. Use the su command to become root. Stop profiler on the device by execing "profiler.sh stop". Use "vi" to edit the /usr/idp/device/cfg/delta.set file so that it only contains the first ("and the last "), and save it. Start the profiler by executing "profiler.sh start". This will allow NSM to get all the profiler data from device.
 4. The operation to get all the profiler data from the device can be a time-consuming operation. In order to avoid profiler specific time-outs, restart the Device server processes after making the following changes to devSvr.cfg:

```
profilerMgr.receiver.pktIntTimeoutInSec 1800
```

profilerMgr.receiver.minPollTimeInSec 3600

Note: The NSM server will be updated with the recent profiler data on the IDP sensor.

5. NSM will now display the data with the right time stamp.
 6. After all the data has been fetched from the device, reset profilerMgr.receiver.pktIntTimeoutInSec and profilerMgr.receiver.minPollTimeInSec to the default values (300 secs) and restart the Device server processes.
- If you are upgrading the management system from NSM 2006.1 to NSM 2007.1 and applied the forward support schema update to manage ScreenOS 5.4 devices, you will be required to re-import these devices in NSM or make the same configuration in the NSM UI.

This step is required to ensure that all the new features of ScreenOS 5.4 managed via supplemental CLI commands are now being managed properly in NSM UI.

4 Addressed Issues

The following issues are addressed in this release.

Directives

- **cs12188**—Update failed with an SSG device upgrade from 5.1rX to 5.4rX related to cache size.
- **cs11906**—Device Update failed with a verification error when supplemental CLI "clear session" was defined.
- **cs11606**—Incorrect CLI's were generated when the device using 5.0.0r9 had the VIP configuration.
- **cs11507**—When you enabled OSPF on a shared virtual router and put a vsys interface in it, there was a logic which operated directly on internal data and caused template information of the interface to be lost. This made the root device think that the vsys interface belonged to itself, and generated wrong clis for it.
- **cs11410**—NSM did not generate commands when SNMP community settings were changed.
- **cs11387**—Selecting the NSM Secondary Server's MIP Address for the NSM agent configuration caused all the MIP addresses to be updated to the device.
- **cs11315**—Exception caught during device update when using supplemental CLI when "clear" commands were sent with the supplemental CLI.
- **cs11056**—Updating a device with the same detector.so version present on the device, returned an error that did not convey the right message.

- **cs11017**—Delta config displayed some difference in AV settings after upgrade to 5.4 related to ISG2000 & ISG1000.
- **cs10716**—Advertise Default Route with RIP was not being updated to the device.
- **cs9751**—Device update tried to unset interface "ip manageable" for vsys cluster members.
- **cs9698**—When Adjust OS was performed, the versions were not updated on the cluster when the upgrade version was a maintenance release on the same branch.

Install/Upgrade

- **cs11172**—NSM upgrade from 2005.3r2 to 2006.1 failed when the /tmp was limited to 512MB.
- **cs9784**—The UI timeout preferences were changed to default values after an upgrade.

Logs and Reporting

- **cs12184**—Duplicate columns for the same device were displayed in a report due to domain versions.
- **cs12093**—There was more than a three hour delay in forwarding of logs to a syslog server when the logging rate was more than 600 logs/sec.
- **cs11057**—Configuring action parameters was not possible for domains created prior to NSM 2005.2.
- **cs10954**—Log Viewer columns displayed a tool tip when the log was selected & highlighted.
- **cs10377**—Generating time based reports with guiSvrCli.sh did not work.

VSYS

- **cs9585**—NSM vsys cluster did not display all static routes in the UI.

Others

- **cs10273**—Unable to open online help in Linux Client due to an incorrect reference.

Policies

- **cs12374**—Policy Merge failed to merge certain rules.
- **cs11453**—You could not save a policy when copy and pasting a rule group then renaming it and editing the rule inside the group.
- **cs11271**—You could not add a group object in the Global firewall rulebase.

- **cs10963**—Adding a new rule after a filter was defined reverted to the default zones instead of the zones defined in the previous rule.
- **cs10934**—Policy Compilation failed on ES3 Update 8 and NSM 2006.1.
- **cs10668**—NSM did not always save or delete changes to Log Viewer views.
- **cs9811**—NSM could not copy/paste rule into security policy after a filter was applied to the policy.
- **cs9158**—Rule groups did not get expanded when a filter was applied.
- **cs8344**—Internal error occurred while editing options for a rule in policy due to incorrect roles defined for an admin user.

Monitoring

- **cs11431**—In the troubleshooting window of Device Monitor, executing the command 'get vsys' or 'get vsys name' returned no result.
- **cs10663**—Devices failed to report ethernet, flow & policy statistics when statistics were enabled as a part of the template and the same template was applied to the device.
- **cs10111**—Device Statistics did not list active session reliably.

VPN

- **cs11101**—NSM UI displayed error while configuring IKE gateway peer with an IKE ID of format ASN1-DN.
- **cs10898**—Changes in the VPN related to Phase 2 configuration would unset the VPN and set it.
- **cs10108**—Custom P1 proposals were displayed as **** in the Job Manager for non-super admins.
- **cs9180**—VPN was unset and set when an interface using DHCP was included in the route based VPN on a NS5GT.

Device Management

- **cs12039**—Applying templates failed when "Password Length Restriction" was selected and the password length was not defined.
- **cs11649**—Custom zones did not appear when defining the Zone Monitor under Whole Box Monitoring.
- **cs11392**—Errors when creating user with role: "Edit Devices, Device Groups, & Templates.
- **cs11378**—You could not edit interface management parameters for VSD-less cluster.

- **cs11296**—Screen settings via a template could not be applied for pre-defined zones.
- **cs11190**—NSM did not support using reverse solidus or back slash (\) for mal-url HTTP header pattern.
- **cs11134**—The "." key failed to work on a Dutch keyboard.
- **cs10988**—Unable to define a route to null interface using a template.
- **cs10964**—Subnet Mask on an interface could not be removed after the interface was unset from a zone.
- **cs10939**—Unable to create a MIP with the same IP as the untrust interface on a NS5GT.
- **cs10927**—Menu choice to set a secondary ip address on a sub-interface inside a VSYS was not available in NSM.
- **cs10676**—Copy/Paste of the devices present in the security device list view did not show all the details.
- **cs10669**—When routes on the trust-vr were pointed towards a tunnel interface, the same routes on different VSYS were displayed with an error.
- **cs10483**—When using device templates, an option to define different SNMP sysname and hostname were not present.
- **cs10448**—Unable to use the numeric key pad in the Security Devices view.
- **cs10085**—Unable to set DI attack DB url.
- **cs9664**—NSM did not support local sub interfaces in vsd-less cluster.
- **cs9450**—NSM UI hung when viewing audit logs with rb_firewall reference.
- **cs8448**—Errors shown when configuring speed/duplex settings on a mini-gb module on an ISG1000.
- **cs7640**—Source Interface selection could not be defined with the NSM agent configuration.

Objects

- **cs12193**—Update Device listed Attack objects as deprecated.
- **cs10014**—Changing the pre-defined service timeout on the device level and updating the device caused a verification failure.
- **cs9648**—Objects were not listed on their own once they were added to a group.
- **cs8015**—Service objects sort failed to list the correct order when sorted on the Non-ICMP column.

Validation

- **cs11187**—Adding more than 4 BGP neighbors was not allowed.

Crash

- **cs10574**—NSM GUI server Manager process crashed and resulted in core.
- **cs10629**—GUI Server dumped core due to database corruption.
- **cs11551**—GUI Server Database corruption.
- **cs11093**—GUI Server processes failed with a core when the port tcp/7801 was not available.

High Availability

- **cs11684**—HA Server processes failed to start when manually started using either the bourne shell or c shell.
- **cs11642**—NSM HA replication did not work for the first time after the server was restarted.

IDP

- **cs12185**—Replication failed due to the transaction logs on the profiler database being removed after the database was updated.

5 Known Issues

This section describes known issues with the current release.

5.1 Limitations of Features

None

5.2 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:”.

- **cs10015**—Invalid reference when trying to delete redundant sub-interface.
- **cs11327**—Audit Log Viewer does not show the policy changes correctly.
- **cs11440**—A route created in shared vr of a custom vsys is not available in the routing table of root vsys.
- **cs11955**—NSM appends `_zone` to the address name when the object name is the same in multiple zones.

- **cs11962**—Custom attack signatures do not allow you to modify the supported platforms.
- **cs12052**—NSRP Monitor does not show correct information when one of the NSRP peer devices is powered off.
- **cs12097**—VPN monitor should display the cluster name instead of cluster members.
- **cs12360**—Upgrade from NSM 2005.3r2 to 2006.1 corrupts custom admin roles.
- **cs12446**—NSM does not allow changing VSD group for NSRP lite.
- **cs12532**—Unable to update the sub interfaces configuration to NSRP Cluster when interface is created at member level.
- **cs12587**—VPN references are not removed when protected resource is deleted.

W/A: The workaround for this issue is: 1. Click the “Protected Resource” link to open the Protected Resource window. 2. Click “OK” to close the window. 3. Save the VPN.

- **cs10718**—If you update a device and the update is unsuccessful, the Audit Log Viewer "device" value is NULL.
- **gl32416**—While re-installing the management system, the "Refresh" option does not prompt you to change previously configured server parameters.
- **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.

- **cs10348**—When filtering by "device group" under Log Viewer for the devices column, no logs are returned from the filter.
- **cs10125**—Import of the device fails if keyword "admin" is used in the configuration.

5.3 **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:

- **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.

- **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.

- **cs7488**—NetScreen-Security Manager reports an error when trying to set link-down an interface on an ISG 2000 device.
- **cs3723**—It is not possible to create a configlet for a device in transparent mode.
- **os53891**—When upgrading a device from ScreenOS 5.0r10 and lower to ScreenOS 5.3, devices crash.
- **os53871**—Devices running ScreenOS 5.3 may crash when generating Deep Inspection logs.
- **os53854**—Wireless interface zone settings on devices running ScreenOS 5.3 are always displayed as "none" in the NetScreen-Security Manager UI.
- **os53710**—It is not possible to set the bandwidth on interfaces for a VSYS in ScreenOS 5.3.
- **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.

- **os53312**—You can not nest local user groups in ScreenOS 5.3.
- **os53035**—NSRD in transparent mode is not functional in ScreenOS 5.3.
- **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.

- **os45418/48460**—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.

- **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
48987	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
45418/ 48460	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
43001	5.0.0 r10	5.2	5.2	5.0.0 r10	5.0.0 r10	5.0.0IDP1 r2

6 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: Rick Wong

