



NetScreen-Security Manager Release Notes

Release 2005.3r2
4-11-06

Contents

- 1 “Version Summary” on page 2
- 2 “Changes in Default Behavior” on page 2
- 3 “System Requirements” on page 2
- 4 “Addressed Issues” on page 2
- 5 “Known Issues” on page 6
 - 5.1 “Limitations of Features” on page 6
 - 5.2 “Compatibility Issues” on page 6
 - 5.3 “Known Issues” on page 7
 - 5.4 “Known Issues in ScreenOS 5.x That Affect NetScreen-Security Manager 2005.3r2” on page 11
- 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: 093-1805-000 Rev B

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 and virtual private network (VPN) appliances and systems. NSM 2005.3r2 is a maintenance release supporting NSM 2005.3.

2 Changes in Default Behavior

The following are changes in the default behavior of NSM 2005.3r2:

- Preferred Ids in security policies start from 1, instead of zero.

3 System Requirements

NetScreen-Security Manager 2005.3 no longer provides support for Red Hat Linux 8 or 9. If you want to install NetScreen-Security Manager 2005.3, you must install or upgrade the operating system to either Red Hat Enterprise Linux 3 or 4, before installing or upgrading to NetScreen-Security Manager 2005.3.

The NetScreen-Security Manager 2005.3 system update utility is compatible with Red Hat Enterprise Linux 3.0 Update 5 and Red Hat Enterprise Linux 4.0 Update 1.

4 Addressed Issues

This section describes addressed issues in the current release:

Import/Update/Export

The following are addressed issues with Import/Update in this release of NetScreen-Security Manager:

- **8006**—You could not import a security device running ScreenOS 4.0 using NACN if telnet was not enabled.
- **8017**—For NS5200 devices running ScreenOS 4.0 clusters configured with vsys, NSM failed to update devices with policies configured with MIPs.
- **8038**—Non-printing characters appeared in the update device dialog box.
- **8379**—If a service group from global domain was used in a subdomain policy rule, NSM failed to update any change to that policy rule.
- **8446**—When a VSYS was updated, an invalid CLI was sent that attempts to unset a management interface IP address.
- **8596**—ICMP Services were incorrectly unset when devices were updated.
- **8716**—Redundant SNMP community config caused update failure.
- **8863**—Updates appeared to fail due to policy save failures. See also ID 8496.

- **26023**— NSM now dynamically updates attack groups based on the contents of the security update. NSM also trims unsupported groups based on device type when doing an update to a device.

Security Policies

The following are addressed issues with security policies in this release of NetScreen-Security Manager:

- **8496**—At random intervals, NSM failed to save a change in policy and prompted admins to save the policy upon exiting.
- **26627**—Permissions to create and delete security policies did not automatically select permissions to the following:
 - create/edit Backdoor rulebase
 - create/edit Firewall rulebase
 - create/edit IDP rulebase
 - create/edit Multicast rulebase
- **27814**—When a new policy rule was added for the first time, the preferred ID started with number 0, instead of 1.

Log Viewer

The following is an addressed issue with the Log Viewer in this release of NetScreen-Security Manager:

- **8354**—Devices with VPN policies did not show the correct rule number on log records displayed in the Log Viewer.

Directives

The following are addressed issues with Directives in this release of NetScreen-Security Manager:

- **7552**—The RMA and activate process failed if a device was not in the down state.
- **8613**—Directives failed with the message "Connection to Device Server dropped" because the GUI Server processes were not completely started.

Validation

The following are addressed issues with Validation in this release of NetScreen-Security Manager:

- **7775**—Validation was needed to prevent a user from adding l2 to a zone name in a transparent device. L2 is automatically prepended by NSM in this case at device update time.

- **8378**—An erroneous validation and a null pointer exception appeared in the Policy Manager when a custom service object in the global domain was referenced in a policy in a subdomain.
- **8553**—An ISG1000 device running ScreenOS 5.3 incorrectly listed GTP as a service resulting in a validation error.

Monitoring

The following are addressed issues with monitoring in this release of NetScreen-Security Manager:

- **7792**—The NSRP Monitor was not updated for 2 hours after device failover.
- **7291**—Device statistics did not appear in the NSRP Monitor in cases where the device serial number was not saved properly.
- **8041**—When a device was deleted and re-added, the device names were not updated in the NSRP Monitor.
- **8887**—Device connections were listed as Up and Managed even when the device connection was down.

Management System

The following are addressed issues with the management system in this release of NetScreen-Security Manager:

- **8011**—Multiple invocations of Scheduled Security Update caused excessive memory consumption in the NSM management system.
- **8150**—The GUI Server crashed due to a failure during error handling at login time.
- **8167**—Device Server crashed due to a failure to recover from an error condition. This problem can happen when a device disconnects from the Device Server during a write operation.
- **8550**—Some NSM processes failed to start because of missing "whoami" command on Solaris systems.
- **8656**—The GUI Server crashed on some Solaris systems due to a failure to de-reference memory appropriately that caused a null value to be inserted in a printf() statement.
- **8849**—Ungraceful device disconnects caused the Device Server to crash.

High Availability

The following are addressed issues with High Availability (HA) in this release of NetScreen-Security Manager:

- **7892**—When NSM was not run as the root user, the HA process did not set startToken and completeToken correctly.

- **7906**—When an NSM management system running HA with a shared disk on Solaris failed over, the secondary system was not able to mount the shared disk.
- **7996**—HA replication failed if NSM management system was not running as the root user.
- **8735**—HA operations on large databases failed due to a low default timeout value.
- **8862**—It was not possible to select the MIP Address for the secondary NSM server in an HA environment.

VPN

The following are addressed issues with VPNs in this release of NetScreen-Security Manager:

- **8016**—A phase 2 proposal configured with SHA-1, appeared as MD5.
- **8191**—Deleting a tunnel interface did not correctly delete its references from all routes.

Upgrade

The following are addressed issues with upgrading in this release of NetScreen-Security Manager:

- **8353**—Upgrading from NSM 2005.2 to NSM 2005.3 on Solaris resulted in errors due to older version of the tar command. The newer version is now included in the system update.
- **8093**—Upgrading from NSM 2005.1 to NSM 2005.3r1 resulted in missing device server IP address from the "Startup" section of the device editor and a validation error was displayed.
- **27277**—Firmware upgrade from ScreenOS 5.0 to ScreenOS 5.1 was not available for NS-HSC devices via NSM.
- **27950**—File permissions were modified during upgrade so that users wishing to run NSM as a non-root process would need to run setperms.sh script again after upgrade.

Device Configuration

The following are addressed issues with device configuration in this release of NetScreen-Security Manager:

- **7375**—You could not unset route map once it was configured for dynamic routing.
- **8346**—Setting a VIP with a separate address on an untrust interface resulted in NSM pushing an incorrect VIP reference to a device when the VIP is used in a policy.

- **8500**—If a DIP or a MIP was in use by a policy and a modification was needed, the DIP or MIP had to be first removed from the policy and modified and then added back to the policy. This procedure required two updates to complete the configuration change.
- **8646**—You could not assign a redundant sub-interface to a VSI.
- **8678**—The JUNIPER-SMI.MIB was not included in previous releases of NSM.
- **8751**—NSM attempted to set the management interface IP address on a VSYS if vsd-group id 0 was unset in the associated cluster.

Report Manager

The following are addressed issues with the Report Manager in this release of NetScreen-Security Manager:

- **8336**—CLI generated reports always showed null for the dest port.
- **26585**—Report Manager performance was improved.

Miscellaneous

The following are miscellaneous addressed issues in this release of NetScreen-Security Manager:

- **8094**—The Find Usage function returned unused Custom proposals.
- **8198**—NACN certificate generation failed on Solaris systems due to missing "whoami" command.
- **26596**—Migration from a previous release of NetScreen-Security Manager resulted in inconsistencies in the device UP or DOWN status.
- **26915**—Repair install option with reconfigure option selected as true failed with an error.
- **27396**—The libstdc + +.so.5 library was missing from the system update for RedHat Linux ES 4.0.
- **27578**—A security update did not prevent the downgrade of the detector.so file.

5 Known Issues

This section describes known issues with the current release.

5.1 Limitations of Features

None.

5.2 Compatibility Issues

None.

5.3 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:”

Import/Update/Export

The following are known issues with import/update/export functionality in this release of NetScreen-Security Manager:

- **7774**—Import of a device config larger than 2 Megabytes may fail. The device will truncate the output.
- **7701**—Device Update fails if the Address Object name has multiple interior adjacent white spaces. i.e.: "abc < sp > < sp > 123".
- **6879/6185**—NetScreen-Security Manager cannot distinguish which devices contain which DI signatures. Updates may fail if unsupported signatures are included in a policy rule.
- **26363**—Import of device configurations larger than 2 MB fails (ScreenOS limitation).

Security Policies

The following are known issues with security policies in this release of NetScreen-Security Manager:

- **7889**—Application errors appear when selecting attacks in some IDP rulebases.
- **7617**—Currently the UI displays only changes to a policy (i.e. adding/removing of rulebases from policy). Changes to rulebases (adding/removing/modifying rules) are logged in audit log but can not be displayed using the Policy Editor.
- **6937**—Rule grouping is only available for zone-based rulebases.
- **6013**—When a policy rule is cut, it disappears until it is pasted.
- **26972**—A predefined group with no members other than a custom attack generates a warning in a policy rule indicating it is empty.
- **27135**—Duplicate entries appear in the "Select Services" dialog in Policy Manager.
- **28045**—An incorrect validation error with a NullPointerException is seen when entering a source NAT in Policy Manager.

Device Configuration

The following are known issues with device configuration in this release of NetScreen-Security Manager:

- **8036**—Routing table default metric that appears in NetScreen-Security Manager does not match the ScreenOS default.

- **8024**—The direction for an attack object is set as "any" when it is copied to a custom attack object.

W/A: Set the direction as "client to server" or "server to client".

- **8015**—Custom service objects do not sort correctly based on the non-ICMP column.
- **7984**—NetScreen-Security Manager sometimes displays an incorrect attack database version.
- **8025**—The domain path for the guiSvrCli.sh script should be specified as: global[. <subdomain-name >].
- **8012**—Columns do not size correctly in the table view of the Anti-Spam screen.
- **7744**—NetScreen-Security Manager does not set webauth on a ScreenOS 4.0 transparent device interface.
- **5425**—NetScreen-Security Manager unsets dynamically learned DNS settings.
- **26079**—There is an issue with enabling PIM-SM and IGMP together on an interface. In some cases, when you enable IGMP, PIM-SM settings will be disabled.

W/A: Unset IGMP (Uncheck "Enable", Select IGMP type "None"), save and then return to configure PIM-SM settings.

- **25190**—If an aggregate interface with a single member has that member replaced, an update failure will occur.

W/A: First add the second member and update the device. Then you can remove the first member without issues.

- **28030**—The MGCP pre-defined service group is missing from NSM.
- **27255**—When viewing the "Compound Attack Members" tab in the "Attack Version" dialog for a custom compound attack, some entries in the "Compound Attacks" column are blank. This is the case if there is more than one entry in the table.
- **27869**—The "to e-mail address" field in the "Action Parameters" screen is empty.

W/A: Double-click the entry to open the "Action Parameters" dialog which displays this value.

VPN

The following are known issues with VPNs in this release of NetScreen-Security Manager:

- **8189**—If a Route Based VPN is created at the device level without using a VPN abstraction and the related tunnel interface has the same name in two or more devices, deletion of this tunnel on a single device results in the deletion of the reference to this tunnel on all devices that use the same tunnel interface name.

W/A: Delete all the routes that utilize this specific tunnel interface. Alternatively, contact JTAC to assist in manually deleting this tunnel interface from the NetScreen-Security Manager database.

- **7143**—The preshared key for a VPN is displayed in clear text. There should be a way to encrypt it.
- **5353**—Config Sync does not report changes on VPN Manager.

NSRP

The following are known issues with NSRP in this release of NetScreen-Security Manager:

- **8021**—Cluster objects do not show updated minor OS version running on a cluster that has been upgraded.
- **7820**—NetScreen-Security Manager with VSYS cluster members may experience performance issues at login time.

W/A (Partial): Open and save VSYS cluster objects to remove some redundant data.

- **26796/22489**—Connection status for VSYS cluster members is inconsistent.
- **27923**—NSRP cluster members display identical IP addresses for master and backup.
- **28464**—It is not possible to update the Deep Inspection attack database using NSM for devices in NSRP cluster configurations that are running ScreenOS 5.1 and above.

W/A: Use the "exec attack-db update" command on the CLI, use the WebUI or contact JTAC for patch.

Monitoring

The following are known issues with monitoring in this release of NetScreen-Security Manager:

- **6477**—Get tech output for ScreenOS 4.0 devices may be truncated when retrieved through the NetScreen-Security Manager troubleshooting window.
- **5470**—The Realtime Monitor is not properly enabled after migration from NetScreen-Global PRO.
- **27981**—Duplicate entries may appear in the NSRP Monitor, if devices are deleted and re-added.

Installation

The following is a known issue with installation in this release of NetScreen-Security Manager:

- **7939**—The `restoreDbFromBackup.sh` requires the `/var/netscreen/GuiSvr` directory to be present. If this directory is not present, then the restore script reports success output but nothing is restored.

Upgrade

The following are known issues with upgrades in this release of NetScreen-Security Manager:

- **6113**—If an upgrade from one release of NetScreen-Security Manager to another does not include version migration, it is impossible to migrate any versions in a future upgrade.

W/A: You must delete domain versions after any upgrade where they are not migrated.

- **26668**—Firmware Upgrades from ScreenOS 4.0 to ScreenOS 5.1/5.2/5.3 should be blocked.
- **9341**—If you are not running the NSM server processes as root, and you upgrade to NetScreen-Security Manager 2005.3r2 configured with HA, java processes on the management system do not start.

W/A: After upgrade and running of `setperms.sh`, you must manually modify `haSvr.cfg` to the root user.

Statistical Report Server

The following are known issues with the Statistical Report Server in this release of NetScreen-Security Manager:

- **7315**—The Statistical Report Server fails to save the IP address for a second GUI Server.
- **6883**—The Statistical Report Server does not report device downtime accurately.

Management System

The following are known issues with the management system in this release of NetScreen-Security Manager:

- **8998**—Database replication failed on Solaris systems when you launched NSM server processes using the Bourne Shell.

W/A: Contact JTAC for patch.

- **7233**—If the GUI Server is not configured in HA mode, then the Device Server will not failover if it is configured in HA mode.
- **7035**—The GUI Server directive handler process stops under heavy load.

5.4 Known Issues in ScreenOS 5.x That Affect NetScreen-Security Manager 2005.3r2

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

- **55015**—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.
- **7488**—NetScreen-Security Manager reports an error when trying to set link-down an interface on an ISG 2000 device.
- **3723**—It is not possible to create a configlet for a device in transparent mode.
- **53891**—When upgrading a device from ScreenOS 5.0r10 and lower to ScreenOS 5.3, devices crash.
- **53871**—Devices running ScreenOS 5.3 may crash when generating Deep Inspection logs.
- **53854**—Wireless interface zone settings on devices running ScreenOS 5.3 are always displayed as "none" in the NetScreen-Security Manager UI.
- **53710**—It is not possible to set the bandwidth on interfaces for a VSYS in ScreenOS 5.3.
- **53595**—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.

- **53312**—You can not nest local user groups in ScreenOS 5.3.
- **48987**—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.

- **45418/48460**—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.

- **43001**—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 © 2005 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.

