



NetScreen-Security Manager

Release Notes

Release 2006.1
7-25-2006

Contents

- 1 Version Summary on page 2
- 2 New Features on page 2
- 3 Changes to Default Behavior on page 3
- 4 System Requirements on page 4
- 5 Upgrade Considerations on page 4
- 6 Addressed Issues on page 4
- 7 Known Issues on page 8
 - 7.1 Limitations of Features on page 9
 - 7.2 Known Issues on page 9
 - 7.3 Known Issues in ScreenOS 5.x That Affect NetScreen-Security Manager on page 13
- 8 Getting Help on page 15

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 093-1754-000 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, 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.

- **IDP Sensor Support**—Includes all IDP functions.
- **IDP Sensor/Cluster Monitoring**—NSM can now monitor the state and status of IDP Sensors and IDP Sensor clusters.
- **Standalone IDP Migration**—Migration of all configuration data and logs from IDP Manager to NSM. Upgrade of IDP Sensors to IDP 4.0.
- **Profiler**—Analyzes your network and automatically learns about the elements that comprise it, including hosts, peers (which host is talking to which other host), ports (non-IP protocols, TCP/UDP ports, RPC programs), and data from layer-7 that uniquely identifies hosts, applications, commands, users, and filenames.
- **Security Explorer**—The Security Explorer is a dynamic graphical tool that enables you to visualize network behavior based on profile, log, and report data. The main component is a touch graph that represents the relationships among data objects on multiple levels including hosts, services, and attacks. The Security Explorer also displays a Tool Area, Log Viewer, and Reports within contexts of the viewed graph.
- **IDP Policy Wizard**—Easily create a new IDP policy.
- **IDP Admin Role**—A new default role designed for IDP administrators, provides usability by showing IDP-relevant parts of UI only.
- **Audit Log Filtering and Sorting**—Provides a usable method for looking for changes made by a specific admin or changes made to a specific device.
- **View Logged in Admins**—Show name and contact information, idle time, and any locks currently held.
- **Enhanced RADIUS Support**—NSM role assignments via RADIUS now supported. NSM now supports two RADIUS servers.
- **Scalability**—100 IDP Sensors (20 of them running Profiler) with 2000 FW/VPN devices; or 6000 FW/VPN devices.

- **Recommended Attack Filter**—NSM now allows you to filter for Recommended attack objects when creating a custom group. Juniper Networks flags an attack as Recommended when it is currently circulating, represents a high risk of damage, or represents a common vulnerability. In addition, there is a new predefined attack group called Recommended which contains all attack objects with this flag on.

Custom attack objects may also be tagged as Recommended.

- **Out of Band Upgrade**—As part of the IDP Sensor migration process, you may upgrade IDP Sensors to 4.0 by loading the IDP 4.0 image directly on the Sensor. When the upgrade occurs, NSM will determine if the Sensor has already been upgraded. If it has not, the previous procedure will be followed, with NSM downloading the 4.0 image to the Sensor and having it execute the upgrade.
- **Dashboard**—Allows you to see your Destination Watchlist, Source WatchList, Top 10 Attacks all over past 1 hour, and device status.
- **New Predefined Log Views**—Under the Log Viewer node, you will now see three new sub-nodes: Backdoor, Scans, and Profiler. These predefined log views existed in IDP Manager and are convenient ways to view IDP-related logs.
- **New Attack Object Viewer/Editor**—The Attack Object viewer has been redesigned. Although predefined attack objects are still not editable, the Edit button in the viewer copies the object, then makes the copy editable in the view dialog. Use this same dialog to modify existing custom Attack Objects.
- **View Attacks by Service**—In the Policy Editor, see attacks within a rule grouped by their default service.
- **Policy Template Improvements**—IDP policy templates have been modified based on customer recommendations. Since IDP policies may be pushed to ISG or standalone IDP devices, the templates have a firewall rulebase by default. Standalone IDP Sensor ignore the firewall rulebase. Less commonly used rulebases are no longer part of the templates, but they can be easily added to any policy.
- **Audit Log Disk Space Management**—Logger can purge old entries before adding new ones to better manage disk space usage.
- **Block Logins**—Ability to block logins by IP address after specified number of consecutive failed attempts.

3 Changes to Default Behavior

- NetScreen-Security Manager now manages standalone IDP Sensors. The IDP Management Server and IDP UI cannot manage IDP 4.0 Sensors. See the IDP-NSM Migration Guide for a complete description of the changes.
- The Anomalies default log view is no longer available in NSM.

4 System Requirements

NetScreen-Security Manager 2006.1 requires one of the following operating systems:

- Red Hat ES/AS 3.0 with Update 5
- Red Hat ES/AS 4.0 with Update 1
- Solaris 8 or 9 with current recommended patches from Sun

Refer to the NetScreen-Security Manager Installer Guide for detailed installation requirements and procedures.

5 Upgrade Considerations

The follow items need to be taken into account when upgrading:

- If user “nsm” already exists, a shell needs to be defined for this user.

6 Addressed Issues

The following issues are addressed in this release:

Import/Update/Export

- **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.

Security Policies

- **7889**—Application errors appear when selecting attacks in some IDP rulebases.

Log Viewer

- **8933**—Error messages when accessing Log Actions Menu without "View Action Attributes" permission.

Management Servers

- **9767**—Core dump on Device Server.
- **9593**—Devices unable to connect to DevSvr if DevSvr management port is changed.
- **9485**—Core dump due to race condition.
- **9346**—Core dump due to race condition.

- 9002—Unable to select loaded CA Cert in Cert request dialog.
- 8990—fopen gives error "too many files open."
- 6477—Unable to get entire output for "get tech" through NSM.

IDP/DI

- 9475—Unable to update attack objects.
- 8479—Last modified date for attack signatures change with every sigupdate.
- 8024—Error when viewing copied attack object.
- 7984—NSM not updating attack db version for device in GUI view.
- 7889—Errors in NSM GUI when trying to choose IDP attacks in policy.
- 7046—31 character limit on key length in Signature.
- 6879—Pushing DI policy w/ unknown attack group clears existing attack objects.

IDP Management Server

- 9410—IDP Manager did not support localization (date formats).

Clusters/High Availability/NSRP

- 27923—NSRP cluster members display identical IP addresses for master and backup.
- 26796/22489—Connection status for VSYS cluster members is inconsistent.
- 9854—Core dump during startup while in HA configuration.
- 9528—Unable to unset default route on only one member of a cluster. Route unset on all members.
- 9339—NSRP monitor and device statistics not working.
- 9336—Deleting one cluster deletes members of another cluster.
- 9179—Cannot use "&" in password between GUI Server and Device Server.
- 8705—"received a heartbeat message with older timestamp" message even though local time was synchronized using NTP. Message occurred because heartbeat packets were not received in the same order they were sent.
- 8435—NSM does not allow modification of HA interface on member of a cluster.
- **7820**—NetScreen-Security Manager with VSYS cluster members may experience performance issues at login time.

Reporting

- 8558—Session Utilization graphs hover-over calculation off by decimal point.

Upgrade

- 9368—On update to 2005.3, GUI Server attempted to replicate data to secondary server even though both servers were sharing the disk.
- 9341—GuiSvr java process does not start after upgrade from FP3r1- 2005.3r2 in NSM HA environment.
- 9157—Interface bandwidth errors after upgrade.
- 8425—Unable to log in to UI after upgrade to 2005.3 unless setperms is re-run.
- 7820—Login to GUI Server takes 5 minutes after upgrade.

User Interface

- 9872—Admin Guide had incorrect multi-select instructions.
- 9382—NSM incorrectly allows user to define the rule options on their rule group name.
- 9373—Policy display becomes blank when changes are made by other user.
- 9169—NSM services fails to start due to the open file limits.
- 8980—All files do not get deleted when a job is removed from the UI.
- 8883—Unable to use numbers on the numeric key pad.
- 8594—When choosing to view Display Policy Usage for an Attack object, UI gives error "There are no references of this object in any Policy" even though object is used in Policy.
- 8306—No search function available in “add address to an address group” window.

Installation

- 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.

Monitoring

- 6477—Get tech output for ScreenOS 4.0 devices may be truncated when retrieved through the NetScreen-Security Manager troubleshooting window.

Objects

- 9193—Address Object names starting with Capital W are truncated.

Directives

- 9483—"set zone null shared" appears on Delta config.
- 9229—NSM does not unset VSI interface when changing VLAN tag on local interface.
- 9044—NSM 2005.3 pushes improper SNMP command to 4.0.3r8 devices.
- 8979—Jobs not getting executed due to inode limit.

Device Management

- 9766—Cannot configure SNMP on ScreenOS FIPS devices via NSM.
- 9736—Assertion failure caused failover to backup server.
- 9718—NSM SSG patch doesn't work on Solaris because cp -v option not supported.
- 9698—NSM does not adjust cluster object "Running OS" after adjust OS of members.
- 9634—Capital letters not accepted for zone names.
- 9599—Deleting one SNMP host entry deleted all SNMP host entries.
- 9505—NSM lists SSG maximum number of routes incorrectly as 4096.
- 9375—Cannot add email address logging notification on backdoor IDP policy.
- 9209—Update fails for all devices after upgrade to 5.3r2.
- 9165—NSM will not allow creation of VIP on a VSI interface in the untrust zone.
- 9039—Anti-virus updates using NSM2005.r3 fail when URL changed.
- 8892—Update from NSM fails if the subnet mask for SNMP host is changed.
- 8680—MGT Interface IP Address not being unset.
- 8593—NSM SurfControl Redirect should be selectable without a UF license.
- 8502—NSM sets route mode for the tunnel interface whereas ScreenOS does not.
- 8447—Java exception on firmware update. Firmware was updated anyway.
- 8112—Sub-interface not showing up for ISG2000 cluster.
- 8022—Device Server crashed due to an assertion failure.
- 8012—Columns do not size correctly in the table view of the Anti-Spam screen.
- 7701—Device Update fails if the Address Object has 2 white spaces.

- 7375—Can't unset a route-map once configured for dynamic routing in template.
- 7368—NSM allows two different admins to import same device at same time.
- 6926—NSM does not push a loopback group assignment when the assigned interface is a VSI.
- 6883—NSM and SRS do not report device downtime accurately.
- 3399—Local name resolution used global domain address list.

Scheduled Security Update

- 8025—Insufficient information about how to use the guiSvrCli.sh script.

SRS

- 9335—SRS missing device uptime/downtime data for few hours every day.
- 8634—NSM sends negative VPN uptime values to SRS.
- 8633—SRS displays FW CPU Utilization as greater than 100 %.
- 8516—SRS does not report stats for ethernet and vpn latency on some devices.

VSYS

- 9751—NSM unsets int ip manageable for vsys cluster members.
- 8932—When changing the vsys cluster object name in NSM, the default virtual router for the vsys is changed to trust-vr without any notification.
- 8825—When importing and renaming VSYS, the default router is changed back to trust-vr.
- 8230—Renaming root device breaks VSYS communication.
- 8218—When deleting a VSYS, interface still appears to be used.

7 Known Issues

This section describes known issues with the current release.

“Limitations of Features” identifies features that are not fully functional at the present time, and are not supported for this release.

“Known Issues” describes deviations from intended product behavior in IDP as identified by Juniper Test Technologies through their verification procedures. Whenever possible, information is provided to assist the customer in avoiding or otherwise working around the issue.

7.1 **Limitations of Features**

- None.

7.2 **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:”.

Upgrade

- **10175**—Solaris only. Upgrade script does not indicate what version of NSM was running previously, and does not indicate what version of NSM will be installed.
- **10174**—Linux only. Upgrade script refers to internal project code name instead of the real release version (2006.1).

Import/Update/Export

- **7774**—Import of a device config larger than 2 Megabytes may fail. The device will truncate the output.

Security Policies

- **6937**—Rule grouping is only available for zone-based rulebases.
- **gl27120**—Not all configured log actions appear enabled in the main rule view.

W/A: Open Notification dialogs to see which log actions are configured.
- **26972**—A predefined group with no members other than a custom attack generates a warning in a policy rule indicating it is empty.

IDP/DI

- **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.

- **29074**—Retry Push feature doesn’t work for IDP devices in NSM.
- **gl29051**—Policy push failed while during Profiler restart.

W/A: Do not push policies while Profiler is restarting.

- **gl29042**—IDP clusters in 3rd party HA configuration show status of Failed at all times. IDP clusters in stand-alone HA mode show correct status.
- **gl29021**—DI pack and detector versions not displayed correctly after attack object download. Sometimes after updating the attack object database, the UI does not show detector versions and DI signature pack versions correctly.

W/A: Log out and log back in.

- **gl28938**—Failed to push a large policy under high load conditions. Push time and compile time exceeded timeout (40 minutes).
- **gl28770**—Profiler permitted objects Apply button is not enabled after edit. After a permitted object used by the Violation Viewer is edited, the Apply button is not enabled.

W/A: Click on the Refresh icon button to refresh the Violation Viewer.

Log Viewer/Log Investigator/Audit Logs

- **gl29168**—Log-to-policy hyperlink does not work in migrated logs. Logs migrated from IDP lose the connection to the policy that generated them. Logs generated after the migration work as normal.
- **gl28807**—The log-to-policy jump is not disabled in the GUI for logs where it is not relevant, such as logs in the screen, config, and alarm categories.
- **gl28181**—Some audit logs for read-only events appear to be duplicates. In actuality, they are separate events because in some cases, the same command impacts more than one domain.
- **7977/gl28440**—Max log count constraint appears not to work in Log Investigator. However, the number of logs shown on the Log Investigator result table includes the repeat count of every log that meets the filter criteria, even though only the number of logs traversed does not exceed the max log count.

Reporting

- **gl28521**—Scheduled reports run on the global domain do not include logs from subdomains.

Clusters/High Availability/NSRP

- **8021**—Cluster objects do not show updated minor OS version running on a cluster that has been upgraded.

VPN

- **8585**—VPN Monitor displays wrong information for A/P cluster. VPNs between passive devices in NSRP clusters appear as "down" in VPN Monitor.
- **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.

User Interface

- **9450**—NSM GUI hangs when viewing audit logs with rb_firewall reference. When an audit logs entry contains the firewall rulebase, double-clicking on the entry hangs the GUI.
- **8981**—Warning displayed when RIP is enabled on a virtual router. However, the RIP config does get generated correctly and pushed to the device.

Upgrade

- 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.

Scheduled Security Updates

- gl28460—GuiSvrCli Retry option does not work. If a Scheduled Security Update fails due to a device being offline, the retry update function (if used) does not attempt the update when the device reconnects.

IDP Migration

- gl29141—IDP Migration fails on NSM GUI Server due to permission issues.

W/A: Change the permissions of the /var files on both GUI Servers to rwxrwxrwx before migrating, then change the permissions back after migrating. Refer to the *IDP-NetScreen-Security Manager Migration Guide* for complete procedures.

- gl28825—The following attacks show up as unNamed in log viewer after migration. These attacks have been deprecated, and the relevant signatures incorporated into different attack objects.

HTTP:STC:IMG:JPEG-HEADER-UF
HTTP:STC:MOZILLA:HOST-MAL-IDN
HTTP:STC:OUTLOOK:MAILTO-QUOT
HTTP:STC:IE:ADOBE-ACTIVEX
HTTP:STC:MOZILLA:RSS-SCRIPT-INJ
HTTP:OMNI:SRC-DISC
HTTP:CGI:SQL-INJECT
HTTP:IIS:EXAIR-DOS-1
HTTP:IIS:CODEBRWS-ASP
HTTP:NOVELL:NETBASIC-TRVRS
SMTP:OVERFLOW:SQRLMAIL-HDR-INJ
SMTP:MAL:DSHOW-BIGCHUNK-SMTP
IMAP:OVERFLOW:NETMAIL-CONT-OF
APP:DSHOW-BIGCHUNK-SMB
WORM:NACHI:INFECTION-PING
SMB:OF:PNP-OF
SMB:EXPLOIT:SMB-OF-0045

- gl28186—Don't see IDP sensor after IDP migration. Sometimes a sensor does not show up in the device list after it has been migrated.

W/A: Log out of the GUI, then log back in. The sensor will appear.

VSYS

- 9585—NSM VSYS cluster doesn't show all static routes in the GUI. When VSYS are in different subdomains and have their local routes in the same shared router, some of the local routes do not show in subdomains.

W/A: Call JTAC for assistance.

Device Management

- **gl29110**—Firmware must be loaded in subdomain in order to perform firmware update in subdomain.

- **gl28681**—Update fails if you unset multilink interface encapsulation from NSM.

W/A: When changing the encap setting to none, change the previous WAN fields to default values. This will prevent device update failure.

- **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.

- **10012**—The option for null interface in the Routing Table is missing in NSM.

W/A: Configure the null interface via CLI on the device. Import the device, edit the imported route, and uncheck the "Gateway Tracking On" check box. Then select "null" as the interface. Save. After that, device and server are in sync and device update will not change this route.

- **8411**—NSM cannot move zone untrust in untrust-vr if using DHCP or PPPOE. When modeling or RMA/activating a firewall that has the untrust zone into the untrust-vr and the untrust interface has a dynamic ip address with DHCP or PPPOE, it will fail to update the device after first connection with NSM.

W/A: From NSM, disable DHCP client on untrust interface, then update the device. Once it's done, enable DHCP client on untrust interface, update device again.

- **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.

7.3 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:

- **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.
- **53035**—NSRD in transparent mode is not functional 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

8 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 © 2006 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: Mark Schlagenhauf

