



NetScreen-Security Manager

Release Notes

Release 2005.2
09-21-05

Contents

- 1 “Version Summary” on page 2
- 2 “New Features” on page 2
- 3 “Changes to Default Behavior” on page 2
- 4 “Upgrade Considerations” on page 2
- 5 “Addressed Issues” on page 2
- 6 “Known Issues” on page 4
 - 6.1 “Limitations of Features” on page 5
 - 6.2 “Compatibility Issues” on page 5
 - 6.3 “Known Issues” on page 5
 - 6.4 “Known Issues in ScreenOS 5.0 That Affect NetScreen-Security Manager 2005.2” on page 9
- 7 “Getting Help” on page 11

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 093-1734-000 Rev C

1 Version Summary

Juniper Networks NetScreen-Security Manager 2005.2 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.

2 New Features

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

- **IDP Module Support for the ISG 1000** — NetScreen-Security Manager now supports IDP on the ISG 1000.

3 Changes to Default Behavior

- None

4 Upgrade Considerations

If you upgrade from NetScreen-Security Manager 2004 FP2 and below to NetScreen-Security Manager 2004 FP3 and later, you will notice changes in rule ID numbers for some policy rules. Rules that contain more than one service object are affected by this. This is caused by a change in the hashing algorithm that generates the rule ID. Performing an update on the device resolves this condition. During the update, policy rules are unset and then set again with the new ID.

As an alternative, you can also set the preferred ID field in the policy rule to match the rule ID on the device. In this case, you do not need to unset your rules. You can do this manually or by running the import directive on the device.

5 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:

- **6781**—You could not control the wireless WPA keys via template after re-import.
- **6774**—RIP values moved trust-vr to untrust-vr on re-import in the device nml file.
- **6730**—Update of the NetScreen-Security Manager attack database failed after upgrading.
- **6729**—Policy name was derived from the device name when the device was imported.

- **6038/24124**—Device export did not include IDP policy.
- **24563**—The NetScreen-Security Manager UI had performance problems when importing devices with VPNs and large number of VPN tunnels.
- **24792**—NetScreen-Security Manager checked the connection status for devices running ScreenOS 4.0, and did not permit an update if they were down. This was incorrect, since 4.0 connection status was not kept current.

Security Policies

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

- **6701**—Policy assignment could not be controlled by templates.

VPN

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

- **6649**—There were problems with reimporting a device if you had policy-based VPNs configured through the VPN Manager.
- **6243**—Performance degradation in updates were seen with large full mesh VPN configurations.

Virtual Systems

The following is an addressed issue with Virtual Systems in this release of NetScreen-Security Manager:

- **6776**—WLAN channel could not be controlled by template.

NSRP

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

- **6752**—NetScreen-Security Manager did not support NSRP with ScreenOS 4.0.1 SBR VSYS on NS5000 series.
- **6718**—SNMP hosts were not controllable through templates.

Delta Config Summary

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

- **6851**—Delta Config and Get running-config on devices running ScreenOS 4.0 failed intermittently.
- **6619**—Inaccurate delta config summary appeared intermittently.

Logging

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

- **6574**—Log Viewer performance was sluggish when internal address resolution is enabled.

Upgrade

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

- **6747**—Upgrade overwrote the configuration file parameters on the HA Server.

High Availability

The following is an addressed issue with High Availability (HA) in this release of NetScreen-Security Manager:

- **5692**—Manual shutdown of the HA Server failed to unmount the shared disk.

Miscellaneous

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

- **6561**—Backup on some systems may have failed due to dependency on awk version. Even though the backup failed, success was reported.
- **6746**—When editing slot information in a 5200 device, "Invalid enum value" error appeared.
- **6658**—It was not possible to unset RIP route map filters in NetScreen-Security Manager.
- **6716**—The route-map dialog box in the device editor did not size correctly.
- **6733**—NetScreen-Security Manager logs displayed WAP passphrase in plain text.

6 Known Issues

This section describes known issues with the current release.

Section 6.1 “Limitations of Features” identifies features that are not fully functional at the present time, and are not supported for this release.

Section 6.2 “Compatibility Issues” describes known compatibility issues with other products, including but not limited to specific Juniper Networks’ appliances, versions of ScreenOS, Internet browsers, and other vendor devices. Whenever possible, information is provided for ways to avoid the issue, minimize its impact, or in some manner work around it.

Section 6.3 “Known Issues” describes deviations from intended product behavior in NetScreen-Security Manager as identified by Juniper Networks Test Technologies through their verification procedures. Again, whenever possible, information is provided to assist the customer in avoiding or otherwise working around the issue.

Section 6.4 “Known Issues in ScreenOS 5.0 That Affect NetScreen-Security Manager 2005.2” describes deviations in ScreenOS 5.0 that affect this release of NetScreen-Security Manager as identified by Juniper Test Technologies through their verification procedures. Again, whenever possible, information is provided to assist the customer in avoiding or otherwise working around the issue.

6.1 Limitations of Features

This release contains the following feature limitations:

- NetScreen-Security Manager does not support the upgrade of NetScreen-500 and ISG 2000 security devices from ScreenOS 5.1 to ScreenOS 5.2. This migration requires a boot rom upgrade; for more details, refer to the *ScreenOS 5.2 Migration Guide*.
- NetScreen-Security Manager does not support ScreenOS 5.2r1 for NS5GT-ADSL security devices.

6.2 Compatibility Issues

This release has the following compatibility issues:

- The RPMs provided in the system update utility for RedHat Enterprise Linux require update 3 of RedHat Enterprise Linux version 3.

6.3 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:”.

Role-Based Administration

The following are known issues with Role-Based Administration in this release of NetScreen-Security Manager:

- **24574**—You must be a global domain administrator in order to run the Scheduled Security Update command properly.
- **24016**—The update config activity does not include update policy.

W/A: Add the update policy activity.

Policies

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

- **6135**—Sizing of columns in Policy Manager is inconsistent.

- **5343**—Policies support only one MIP per rule for ScreenOS 5.x devices.

Device Configuration

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

- **7277**—NetScreen-Security Manager does not have a wireless specific authentication server configuration for wireless 5GT devices. This results in failure to send authentication type 802.1x related CLI commands to the security device.

W/A: Using the UI, configure the authentication server of auth-type 802.1x. Edit the device, and then select the default authentication server to be the one configured for authentication type 802.1x.

- **25312**—Assigning a template value for the parameters listed below and then changing the template value does not change it on the device after update.
 - RIP and OSPF Authentication (when using single or multiple MD5 authentication on either an interface or virtual router)
 - Interface DHCP Mode (switching between client/server/relay/none)
 - VPN Phase1/2 Proposals (switching between predefined/user-defined)

W/A: Unassign the template from the device and then revert the template value. You can then set the template value to the new value and assign it to the device.

- **24534**—For a WLAN device in transparent mode, the L3 zone is displayed even though it is not accessible on the device.
- **24120**—The src-port range on ScreenOS for the service RSH/SIP/H.323 is different from the src-port range of NetScreen-Security Manager.

Import/Update

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

- **6638**—If you configure the "SMTP" service object, and update a device running ScreenOS 5.0.0rX, the update fails. This is because the SMTP service object is included in ScreenOS 5.1 and above.
- **24034**—When a device is imported, NetScreen-Security Manager removes device object values that match the default values (or template-provided values). If there is no default, the imported value is retained in the device object data. If you add a template that sets one of these fields, the device object value overrides the template value.

W/A: Right click on the field label and choose to Revert the value to the template or default value.

Firmware Upgrade

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

- **6134**—When upgrading the image for a NetScreen-Hardware Security Client, you need to rename the file name for any ScreenOS 5.x image. (e.g. ns5gt.5.0.0r8.1 needs to be renamed to ns-hsc.5.0.0r8.1).
- **24243**—If you add a security device running ScreenOS 5.0, and then upgrade the firmware version to ScreenOS 5.1, or if you create a device running ScreenOS 5.1 and upgrade the firmware version to ScreenOS 5.2, the following verification error appears when you update the device.

Verification failed

The following parameters did not get updated to the device:

```
set service H.323 timeout 0
```

The device still has the following parameters which should have been modified

```
set service H.323 timeout 30
```

The verification error is not harmful and you can disregard it. However, if you want to clear the error you can either: import the device; change the H.323 timeout value to 30 minutes (for devices running ScreenOS 5.1) on the “Advanced-> Predefined Service Timeout” screen in the device object and update the device; or change the H.323 timeout value to “Default” (for devices running ScreenOS 5.2) on the “Advanced-> Predefined Service Timeout” screen in the device object and update the device.

Virtual Systems

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

- **4071**—Admins in a subdomain can not view shared interfaces in a vsys device.
- **24480**—Names for vsys must be unique throughout all domains.
- **22489/23440/23503/23827**—When a root device connection state changes, that change is not populated to all associated vsys devices. This can cause the UI to display an incorrect vsys connection state; however, all vsys features remain enabled.

NSRP

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

- **24479**—If you create a cluster device in NetScreen-Security Manager 2004 FP3r2 or before, and the cluster device contains MIP objects with a policy referring to the MIP objects, and you have unset (or delete) the vsd group 0, then after you import the device and perform a “Summarize Delta Config” action, the following error message appears in the Job window.

Error Text: Unable to create device DM.

Invalid mip object in rule No Details Available.

Error Details: No Details Available.

This issue is resolved this release of NetScreen-Security Manager. However, if you are migrating from NetScreen-Security Manager FP3r2 or before to NetScreen-Security Manager 2005.1, the error still appears.

W/A: Perform an "Import Device" action on the cluster device in NetScreen-Security Manager 2005.1.

- **23953**—Clusters do now show the correct minor version after a firmware upgrade.
- **23914**—Config sync does not show the device out of sync when the policy is deleted.

Logging

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

- **5528**—Setting the time received filter in the filter summary is inconsistent with the duration in the Log Investigator options dialog.
- **23599**—If you double-click on an Audit Log to see the Audit Log details, you can not access any further Audit Log screens until you restart the UI.
- **24467**—Only two pages of logs are supported for PDF exports.
- **24253**—NetScreen-Security Manager allows custom service object to have the same name (case-insensitive) while service objects created using CLI are case-sensitive.

Reports

The following is the known issue with Reports in this release of NetScreen-Security Manager:

- **25073**—No report for "Top FW/VPN Rules" in Global domain. The report manager may fail to generate a report if rule number is used in a filter. This issue is only seen with a Solaris based NetScreen-Security Manager server.
- **6235**—Log filter for custom reports does not remember the last IP/subnet mask entered.

Performance

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

- **6436**—Performance issues outside of NetScreen-Security Manager (e.g. Syslog) may cause syslog files to get piled up inside of the system.
- **6225**—Automatic back up may fail due to performance issue with large number of domain versions.

Miscellaneous

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

- **6279**—Adjust OS version does not work for modeled devices that are deployed with the not reachable workflow.
- **5843**—If a device is in multiple groups, the Job Manager will not display the correct %complete when a directive is run.
- **3723**—If you are using Rapid Deployment, you can not create a configlet for transparent mode devices.
- **24608**—Compound attacks with some members having direction “Server to Client” and others as “Client to Server” are displayed incorrectly under the general “Category” group. For example, attack AOL Admin Server Response (TROJAN:MISC:AOLADMIN-SRV-RESP) should be under “Response_TROJAN-Major”, but are listed under “Category_TROJAN-Major”. Performance is degraded significantly for attacks containing one or more members having direction “Server to Client”.

W/A: Place these attacks under the “Response” group.

- **24559**—Newly created SIP anomalies/signatures are categorized in the signature database under the VOIP:SIP categories. Since predefined groups in NetScreen-Security Manager filter on this category designation and are currently flattened to only one level of hierarchy, these attacks and signatures are in the VOIP category. When creating SIP custom Attacks, the category that NetScreen-Security Manager assigns the custom attacks is its “service”, which is part of the AppService_Table. Since there is an Appservice called SIP, when you create the custom attack, it is assigned to the “SIP” category corresponding to the service. Since there is not a predefined group called “SIP”, this attack does not appear under the category tree of pre-defined attacks.

W/A: Create a dynamic group and choose “SIP” as the filter for that group to have these attacks display.

6.4 Known Issues in ScreenOS 5.0 That Affect NetScreen-Security Manager 2005.2

The following are known issue in ScreenOS 5.0 that specifically affects this release of NetScreen-Security Manager:

- **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

7 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.

