

Juniper Networks Release Notes

Product: NetScreen-Security Manager

Version: NetScreen-Security Manager 2004 FP3r2

Release Status: Public

Part Number: 093-1622-000, Rev. C

Date: 6-15-05

Contents

1. "Version Summary" on page 2
2. "New Features in NetScreen-Security Manager 2004 FP3" on page 2
3. "Changes to Default Behavior" on page 3
4. "Upgrade and Migration Notes" on page 3
 - Section 4.1 "Migration Path"
 - Section 4.2 "Upgrade Failure Warning"
5. "Addressed Issues" on page 4
6. "Known Issues" on page 7
 - Section 6.1 "Limitations of Features"
 - Section 6.2 "Compatibility Issues"
 - Section 6.3 "Known Issues in NetScreen-Security Manager 2004 FP3r2"
 - Section 6.4 "Known Issues in ScreenOS 5.1r3 That Affect NetScreen-Security Manager 2004 FP3r2"
 - Section 6.5 "Known Issues in ScreenOS 5.0 That Affect NetScreen-Security Manager 2004 FP3r2"
7. "Getting Help" on page 20

1. Version Summary

This is the r2 version of Juniper Networks NetScreen-Security Manager 2004 Feature Pack 3 (FP3). This Feature Pack includes new features and functionality supporting comprehensive security management of device, network, and security configurations for integrated firewall and virtual private network (VPN) appliances and systems.

2. New Features in NetScreen-Security Manager 2004 FP3

The following is a partial list of new features and enhancements in this release of NetScreen-Security Manager:

- **Support for ScreenOS 5.1r3:** NetScreen-Security Manager 2004 FP3 provides support for FW/VPN devices running ScreenOS 5.1r3 and above. Please note that devices running ScreenOS 5.1r1 and ScreenOS 5.1r2 are **not** supported. Refer to [Section 6.1 “Limitations of Features”](#) for more information on upgrading the device firmware from ScreenOS 5.0 to ScreenOS 5.1.
- **Atomic Configuration Push:** This release enables FW/VPN devices running ScreenOS 5.1 to receive an entire modeled configuration (i.e., a complete set of commands) before execution of those commands. This provides the ability for administrators to make changes to their configurations that could temporarily cut communication to the management system.
- **Configuration Synchronization:** NetScreen-Security Manager now monitors the status of the physical configuration of FW/VPN devices running ScreenOS 5.1, in relation to the configuration modeled in the NetScreen-Security Manager database. This enables administrators to better synchronize the configuration of the managed devices in their network.
- **Removal of TFTP:** This release enables migration of certificate and CRL loading from TFTP to the SSP connection. With this change, all communication between NetScreen-Security Manager and FW/VPN devices running ScreenOS 5.1 utilizes SSP.
- **Extended Scalability:** NetScreen-Security Manager 2004 FP3 increases the number of devices that can be managed to 2000 devices, and the number of UI clients to 25.
- **Custom Reports:** You can now define and save your own reports using custom criteria, including all filters.
- **Quick Reports:** You can now generate a “quick” report directly from data displayed in the Log Viewer.

- **Object Search:** NetScreen-Security Manager now enables you to search for an object by name, string within a name, or IP address.
- **Duplicate Object Creation Validation:** NetScreen-Security Manager validates against the creation of duplicate objects and displays a warning message when this situation occurs.
- **Object Creation in Policy View:** You can now create a new address object while editing a policy.
- **Enhanced Log Viewer Filtering:** You can now filter on an address object name in the Log Viewer.
- **Policy Enhancements:** You can now negate address objects in the source or destination columns of a rule. You can now configure “reject” as a firewall action in a firewall rule. You can also set a preferred ID for each rule; this ID number uniquely identifies the rule within the rulebase and security policy. You can also enable session rematch when installing a security policy on managed devices running ScreenOS 5.1.
- **Display of Administrator Name for Locked Objects:** when an administrator attempts to open an object which is already being edited by another administrator, the system will display the name of the administrator holding the lock for that object.
- **Address Replacement Enhancement:** When replacing an address object from the Address Table, you now have the option of deleting the former address object.

3. Changes to Default Behavior

None.

4. Upgrade and Migration Notes

Please note the following regarding migration and upgrades.

4.1 Migration Path

The migration of data from Juniper Networks NetScreen-Global PRO and Juniper Networks NetScreen-Global PRO Express is supported up to NetScreen-Security Manager 2004 FP2. After you have migrated your data successfully to NetScreen-Security Manager 2004 FP2, you can then upgrade to NetScreen-Security Manager 2004 FP3.

Refer to the documentation and Release Notes for NetScreen-Security Manager 2004 FP2 for more information on migrating your data to NetScreen-Security Manager.

4.2 Upgrade Failure Warning

If you have upgraded your previous installation of NetScreen-Security Manager to NetScreen-Security Manager 2004 FP3, and you receive any indication of a failure, **do not run the install shell archive script again**. Contact the Juniper Networks Technical Assistance Center for further instructions.

5. Addressed Issues

The following is an addressed issue in this release of NetScreen-Security Manager 2004 FP3r2.

Administration

The following is an addressed issue with role-based administration in NetScreen-Security Manager 2004 FP3r2:

- **4736** – Some permissions granted in the global domain were not propagated to a subdomain.

User Interface

The following are addressed issues with the User Interface in NetScreen-Security Manager 2004 FP3r2:

- **5142** – The "+" symbol in the main UI tree used to view individual items in the Policy Manager and VPN Manager did not always appear.
- **23170** – The 2005 copyright information in the UI installation splash screen was not updated.

Monitoring

The following is an addressed issue with monitoring in NetScreen-Security Manager 2004 FP3r2:

- **5033/4835** – The Server Monitor sometimes showed the GUI Server or Device Server as down for a few seconds when either were operational.

Validation

The following are addressed issues with validation in NetScreen-Security Manager 2004 FP3r2:

- **5032** – Empty DI profiles in policy rules resulted in validation errors after upgrade.
- **4878/4910** – When a new policy was added where the zone was global and the destination was MIP/DIP, an incorrect validation error occurred.

Directives

The following is an addressed issue with directives in NetScreen-Security Manager 2004 FP3r2:

- **5056** – Firmware upgrade failed for NetScreen-Security Manager 2004 FP3 on Solaris 8.

Device Configuration

The following are addressed issues with device configuration in NetScreen-Security Manager 2004 FP3r2:

- **5125** – Device update failed and some DHCP server options were incorrectly marked to be unset.
- **5120** – OSPF default link-type was not different for ScreenOS 5.0 and ScreenOS 5.1.
- **5087** – NetScreen-Security Manager did not support the command 'set/unset pki src-interface untrust'.
- **4965** – NetScreen-Security Manager unset values for vsd 1 monitor threshold and weight.

Delta Configuration Summary

The following are addressed issues with the Delta Configuration Summary in NetScreen-Security Manager 2004 FP3r2:

- **5122** – The Delta Config Summary reported a change in the track ip threshold when no such change was sent to the device.
- **4920** – The Delta Config Summary reported incorrect rule numbers in an error message.

Logging

The following are addressed issues with logging in NetScreen-Security Manager 2004 FP3r2:

- **5173** – The log count utility did not give per day information.
- **4943** – The log purge utility did not function correctly causing the Device Server to shut down when the disk became full.
- **3739** – The log purging mechanism occasionally malfunctioned and removed all logs except the current day's logs.

Policies

The following is an addressed issue with policies in NetScreen-Security Manager 2004 FP3r2:

- **5075** – The Global Firewall rulebase tab in the Policy Manager sometimes disappeared.

Objects

The following are addressed issues with VPNs in NetScreen-Security Manager 2004 FP3r2:

- **5044** – An invalid character was present in the Medium:HTTP:SIGS attack group.
- **4933** – You were not able to delete and then re-add an authorization server.

NSRP

The following are addressed issues with NSRP in NetScreen-Security Manager 2004 FP3r2:

- **5201** – The NSRP configuration synchronization flag did not prevent some route table entries from being synchronized when the flag was set to false.
- **5180** – You were not able to set individual SNMP system names on devices in an NSRP cluster.
- **4987** – The NSRP rto-sync option was incorrectly enabled for the NetScreen 25 device.
- **23169** – The monitor interface, zone and threshold features in ScreenOS 5.1 were not updated in an NSRP cluster configuration.

Upgrade

The following are addressed issues with upgrading in NetScreen-Security Manager 2004 FP3r2:

- **5245** – After upgrading from NetScreen-Security Manager 2004 FP2r3 to NetScreen-Security Manager 2004 FP3, you would get an error in the policy rule option for destination NAT, even if you did not configure the NAT option for these rules.

- **5144** – It was not possible to upgrade certain device firmware if you had upgraded from an earlier version of NetScreen-Security Manager.
- **4600** – Firmware upgrade to a device is reported as success even when the firmware upgrade fails.
- **3740** – Firmware upgrade would unset NSRP monitored interfaces (unset nsrp monitor interface) and manage-ip.

Migration

The following is an addressed issue with migration in NetScreen-Security Manager 2004 FP3r2:

- **5137** – Migration failed with certain obsolete forms of object references left over from NetScreen-Security Manager 2004 FP0 or NetScreen-Security Manager 2004 FP1.

High Availability

The following is an addressed issue with high availability in NetScreen-Security Manager 2004 FP3r2:

- **4885** – The HA Server backup.log file always reported a failure of the local backup, even if it was successful.

Miscellaneous

The following are miscellaneous addressed issues in NetScreen-Security Manager 2004 FP3r2:

- **4807** – SNMP traps did not use the correct EID code for Juniper Networks.
- **22354** – Bandwidth was displayed in Kbps and Holddown Time in msec.
- **22686** – While exporting a device configuration to file, the percentage of completion status on the Job Manager stopped at 90%, even though the job was successful.

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 NetScreen 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 in NetScreen-Security Manager 2004 FP3r2”](#) describes deviations from intended product behavior 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.
- [Section 6.4 “Known Issues in ScreenOS 5.1r3 That Affect NetScreen-Security Manager 2004 FP3r2”](#) describes deviations in ScreenOS 5.1r3 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.
- [Section 6.5 “Known Issues in ScreenOS 5.0 That Affect NetScreen-Security Manager 2004 FP3r2”](#) describes deviations in ScreenOS 5.0r9 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

The following limitations are present at the time of this release.

- **VPN Abstractions and Templates Per Device Limit.** The number of VPNs created in VPN Manager and templates must not exceed 63 per device.
- **Device Configuration Validation Does Not Cover All Cases.** When configuring a device, you may not always receive an error message if you enter an invalid configuration. In some cases, an error message appears even if an error did not occur. The error is only indicated during the device update process and only appears in the job results. The error does not have an adverse effect on the device.
- **Demo Mode is Not Fully Functional.** While running the NetScreen-Security Manager User Interface in “Demo Mode”, several features including log filtering, reports and role-based administration may not work properly.
- **Workaround for Local Signature Updates.** You are not able to use NetScreen-Security Manager to update the local attack database automatically. You must perform the update manually.

W/A: To update the local attack database: 1. Obtain both NSMFP3AttackUpdateInfo.dat and NSMFP3.zip from the Juniper website. 2. Save both files to a directory on the GUI Server that is accessible by root (i.e., /tmp/attackupdate/). 3. As a system administrator logged in to the UI, select Tools/Preferences/Attack Objects. 4. Change the URL field to a "file" based URL that points to the NSMFP3AttackUpdateInfo.dat file (i.e., file:///tmp/attackupdate/NSMFP3AttackUpdateInfo.dat). 5. Perform the attack update (Tools menu). Note: You can restore the URL inside the preference window by selecting "Restore Defaults".

- **Workaround for Upgrades.** Due to an issue with ScreenOS, you are not able to use NetScreen-Security Manager to upgrade the device firmware from ScreenOS 5.0r1-r9 to 5.1.

W/A: An interim firmware upgrade "step" image is available for all devices enabling you to upgrade to ScreenOS 5.1 from ScreenOS 5.0. One limitation of this upgrade image however, exists if your overall configuration has an NSRP cluster with only one device. In this case, you must upgrade the firmware on that one device using the CLI. Contact JTAC for more information on obtaining the firmware upgrade "step" image.

- **Workaround for Downgrades.** You are not able to use NetScreen-Security Manager to downgrade the device firmware.

W/A: Downgrade the device firmware out-of-band using the CLI. Note that there are additional requirements for downgrading the firmware on a device from ScreenOS 5.X to ScreenOS 4.X.

To downgrade from a 5.x release to a 4.x release, you must first delete the NetScreen-Security Manager connection parameters from the flash memory on the device:

1. Connect to the device using the console, telnet or SSH.
2. Enter these commands at the CLI:

```
unset nsm enable
unsetnsm init otp
unset nsm init id
unset nsm server primary
delete nsm keys
save
```

To complete the downgrade:

1. Place the firmware image in the TFTP server directory. You can use any TFTP server. To make use of the existing TFTP server on the management system, place the image in the directory `/usr/netscreen/DevSvr/var/cache/firmware` on the Device Server.
2. Save the firmware image to flash on the device with the following command:

```
save software from tftp <tftp-server-ip>
<path-to-firmware> to flash
```
3. Substitute your TFTP server IP address and firmware image name (ex: `save software from tftp 192.168.1.1 firmware/ns5xt.4.0.3r4.0 to flash`). A warning appears that the firmware has a different major version number
4. Press 'y' to accept.
5. Downgrade the device. You can do so by entering the following command:

```
exec downgrade
```
6. Press 'y' twice to confirm the downgrade and flash reformatting. The device automatically reboots once the downgrade is complete.
7. In the NetScreen-Security Manager UI, delete and re-add the device.

6.2 Compatibility Issues

Failover Occurs Only When Management Enabled Locally – If you have installed and configured NetScreen-Security Manager with HA enabled, you must run the `set nsmmgt enable` command locally on devices running ScreenOS 5.0r1 through 5.0r8 to ensure that these devices fail over to the secondary device server. This must be done immediately after adding the device to NetScreen-Security Manager or after enabling the secondary Device Server.

6.3 Known Issues in NetScreen-Security Manager 2004 FP3r2

The following are known deficiencies in features 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:”

Administration

The following are known issues with role-based administration in NetScreen-Security Manager 2004 FP3r2:

- **5155** – Every time you change a device admin password, the admin is reset with the new password generating a log entry in the Log Viewer. The log entry however only indicates that the admin has been deleted. No entry is found when the account is re-added.
- **4579/5216** – NetScreen-Security Manager does not correctly calculate the set of roles that should be visible in the administrator management dialog. If an administrator has permission to view all activities that a particular role has, then he or she should be able to see that role. You must currently assign a role to an administrator explicitly in order for him or her to see it. This leads to validation errors in the administrator table.
- **4123** – When a domain is deleted, admin permissions to that domain are not removed.
- **22865** – A sub-domain administrator can not edit a VSYS cluster, if it has no members, and if its root in the global domain also has no members.

W/A - Add a member to the root in the global domain and re-login as the sub domain administrator.

- **18798** – A versioned sub-domain incorrectly points to the current global domain as the sub-domain's parent instead of the versioned global domain.

User Interface

The following are known issues with the User Interface (UI) in NetScreen-Security Manager 2004 FP3r2:

- **4647** – The default value of 'keepalive' in relation to hold-time is not managed properly due to an incorrect default definition in the database.

W/A: Whenever the hold-time value is not 180, you must set the 'keepalive' value to one third of the hold-time value.

- **14246** – Changes in "Enable Timeout and User Inactivity Timeout" (under Preference>Global Properties) do not take effect until you restart the UI.

W/A: Close and re-open the UI.

Monitoring

The following are known issues with monitoring in NetScreen-Security Manager 2004 FP3r2:

- **4583** – The NSRP Monitor VSD Summary does not indicate the master and backup firewall of the cluster.
- **2170** – The VPN Monitor in the Realtime Monitor displays inactive VPNs on the backup device in a HA (High Availability) cluster.
- **22041** – It may take 5-7 minutes for the Device Monitor to display a down device if the connection between the management system and the device is lost.

Import/Update

The following are known issues with importing and updating in NetScreen-Security Manager 2004 FP3r2:

- **5160** – In ScreenOS 5.1r3, the polling interval value for demand circuit is configured in seconds. NetScreen-Security Manager however, displays them in minutes and attempts to update the device with a value that is in minutes.

W/A: Configure the polling interval using seconds even though the field indicates that the value is in minutes.

- **5125** – If DHCP options are set to the default values, update incorrectly attempts to unset them.
- **5080** – The first time you update a modeled device may fail with av errors. Subsequent updates will not fail.
- **4926** – Device update fails when you enable URL filtering.

W/A: Enable URL Websense, then perform an update. Enable URL sc-cpa, and then perform an update again. This switching process causes the device updates to succeed.

- **3668** – Import of a deny policy with service FTP-Put, FTP-Get shows as permit.
- **3636** – If the ISP name in the Network>Modem section contains a space, the update fails.
- **23182** – Device update fails when you enable DHCP Relay.
- **22921** – A MIP policy gets unset during an update when the vsd-group 0 is unset.

W/A: In the Object Manager, select the MIP that is being used by the policy and assign it to the cluster member directly, instead of the MIP assigned to the cluster name.

- **17764** – Device update fails when you assign Track-IP to interface Ethernet 2 and then change a zone bound to the interface from Untrust to Mgt because NetScreen-Security Manager does not remove the Track-IP designation on the Mgt zone which does not support that feature.
- **14488** – The NetScreen-Security Manager data model does not support the defining of the same address name in multiple zones with different contents. During an import, NetScreen-Security Manager imports only one address causing policies associated with the address object to bind to the wrong address.
- **12002** – Configuration changes to objects (such as group expressions and authentication servers) that exceed maximum limits on the device, are rejected during updates. Information about objects that are rejected are indicated in the Update Summary only.

W/A: Verify that you have successfully updated every object in the Update Summary. If the update rejects an object because it exceeds device limits, you will need to reconfigure the object and perform the update again.

Device Configuration

The following are known issues with device configuration in NetScreen-Security Manager 2004 FP3r2:

- **4985/22929** – Web management is not seen in the template editor.
W/A: You must configure web management individually for each device.
- **4839** – After adding a dynamic IP device (NACN), the "connect with" option must be manually set to SSH regardless of whether the drop down already shows SSH or not (if telnet is disabled but scs is enabled on the device). This must be done before setting CLI commands generated by "Show Device Commands" on the device console.
- **4438** – For a modeled device, selecting the SSH version on the activate page, does not change the connection setting in the device configuration.
- **3830** – You are not able to specify an SNMP interface as physical (when VSD 0 has been unset).
- **22433** – BGP keep-alive time keep always has the default value.
- **20467** – In order to set the 'set vlink md5' command, you must enable the active md5 key.
- **19746** – The ISP name in the modem section of the device editor may not contain a space.
- **17397** – NetScreen-Security Manager does not support the NAT Fixed Port.

- **11794** – When configuring OSPF global parameters for dynamic routing, the dead-interval is typically 4 times greater than the hello-interval. But in NetScreen-Security Manager, if you change the hello-interval, there is no such effect on the dead-interval.

W/A: You need to manually reconfigure the dead-interval in the User Interface.

Delta Config Summary

The following are known issues with the Delta Config Summary in NetScreen-Security Manager 2004 FP3r2:

- **4921** – The Delta Config Summary may fail if the keyword "password" is used as a proper name that appears in the Job Manager CLI.
- **3660** – NetScreen-Security Manager deletes pre-existing CA certificates in a device, if the certificate is not defined in NetScreen-Security Manager for the device. The Delta Configuration Summary does not give you a warning.
- **3312** – Sometimes in the “Config on Device but not on NSM:” section in a Delta Configuration Summary, NetScreen-Security Manager displays invalid commands. As long as these commands do not occur in the “Config to be sent to the Device on next Update Device:” section, you can disregard them.

Policies

The following are known issues with policies in NetScreen-Security Manager 2004 FP3r2:

- **4453** – Rules that are disabled due to scheduler are not marked as disabled.
- **22938** - Security Policies open in a new window preventing access to the rest of the UI until closed in the following scenario - you open a Security Policy by selecting Security Policies from the navigation tree, then highlight the policy in the window on the right, and either double-click on the Policy Name or click on the 'Edit' button or use the Alt-E hotkey.
- **19406** – Multi-line cells do not display correctly in policy rules.

Log Viewer

The following are known issues with the Log Viewer in NetScreen-Security Manager 2004 FP3r2:

- **4671** – The Log Viewer may stop displaying logs.

W/A: Restart the Device Server.

- **3399** – Local name resolution in the Log Viewer comes from the global domain even when viewing logs in the subdomain.
- **20502/20503** – When printing logs from the Log Viewer, you can only print a maximum of 20 pages.
- **20003** – The Log Viewer currently handles zeroes and null values equally. This causes some filters to not work correctly.

Logs

The following are known issues with logs in NetScreen-Security Manager 2004 FP3r2:

- **5174** – Traffic logs from a cluster (only) show firewall policy as rule # as all zeros.
- **21867** – After you delete a device, logs created by the device show the policy and device columns as unknown.

Reports

The following are known issues with reports in NetScreen-Security Manager 2004 FP3r2:

- **5397** – Syslog settings are changed when you upgrade the firmware from ScreenOS 4.0 to ScreenOS 5.0.
- **22831** – When a combination of fields are included in a report, the drill-down window displays an incorrect result (i.e., when "Action", "Alert", and "Category" together). A set of enumerated fields causes a problem.

Virtual Systems

The following are known issues with virtual systems (VSYS) in NetScreen-Security Manager 2004 FP3r2:

- **5253** – You cannot use sub-interfaces on VSYS to add a VSI interface.
- **3860** – After making an out of band change to the device console, you need to import the device to use that change in NetScreen-Security Manager. If you have added a VSYS out-of-band, you need to import the device.
- **20306/21687** – The physical interface of a VSYS may be missing after a reimport.

W/A: Immediately after creating an aggregate interface in the root device, update the device. Go to the VSYS and import the aggregate interface, edit the configuration and then run an update for the VSYS.

- **20033** – Device administrators get cleared from the VSYS device if you do not do an import immediately following migration to NetScreen-Security Manager FP2.
- **19737** – NetScreen-Security Manager currently cannot import aggregate interfaces to a VSYS device.
- **13049** – You cannot update two virtual systems at the same time.

W/A: Ensure that you update one virtual system, before starting the update on the second virtual system.

NSRP

The following are known issues with NSRP in NetScreen-Security Manager 2004 FP3r2:

- **5215** – In a clustered Vsys where a local NAT is assigned to a shared interface from root, you get an "Invalid nat-dip object in rule" error during updates and summarize delta config directives. The directive then fails.
- **22809** – If you have upgraded from NetScreen-Security Manager 2004 FP2 to FP3, updating an NSRP cluster fails when a policy is added with a MIP defined on a local interface of the cluster member.

W/A: Edit the Global MIP object and change the device reference from the cluster to cluster member.

- **22761** – If all members are deleted from a cluster, but the cluster member is not deleted, that cluster can not be used again to add new members.

W/A – Delete cluster and create a new one.

- **21288** – You cannot use the 'set vr tr nsrp-config-sync' command.
- **16733** – If a cluster is modeled first and then updated to a device, the cluster's information does not appear in the NSRP monitor.

W/A: Close and re-open the UI.

Installation

The following is a known issue with installation in NetScreen-Security Manager 2004 FP3r2:

- **17059** – After installing the Linux bin and then attempting to log in, the Linux client incorrectly displays a run or display button.

Migration

The following are known issues with migration in NetScreen-Security Manager 2004 FP3r2:

- **22808** – If you enable the 'ethernet' option for the OSPF link type and then upgrade to NetScreen-Security Manager 2004 FP3, the configuration will not be migrated since this is not a valid configuration.

W/A - Update this parameter in the UI to a valid configuration option.

High Availability

The following are known issues with high availability in NetScreen-Security Manager 2004 FP3r2:

- **21684** – The UI does not report that HA replication failed in the Server Monitor.
- **21484** – After the failover of a large database, it may take a few minutes before UI clients can log back in to the backup server.
- **21316** – The initial replication of a large database between the primary and secondary HA server may take more than a few minutes. During that time, the devices may lose connection to the Device Server due to a heartbeat timeout, but they will reconnect. This is unlikely to occur during subsequent synchronization processes because they are incremental and much quicker.

Rapid Deployment (RD)

The following are known issues with rapid deployment in NetScreen-Security Manager 2004 FP3r2:

- **3723** – If you are using Rapid Deployment, you can not create a configlet for transparent mode devices.
- **18834** – Rapid Deployment does not support clusters and groups.

Management System

The following are known issues with the management system in NetScreen-Security Manager 2004 FP3r2:

- **19221** – If you configure a shared disk system with both the GUI Server and Device Server on the same server with remote backup replication enabled, backups always report a failure if the database backup directory was on the shared disk.

- **5211** – When you are managing large numbers of devices running ScreenOS 5.1, it may not be possible to communicate with the devices for several hours after restarting the Device Server.

W/A: Edit the NSPMessageParserThreads parameter inside NSPPProperties in /usr/netscreen/DevSvr/var/be/cfg/devCommProp.cfg, so that the value for the number of threads is 5. Make the same change in the GUI Server. Restart both servers when done.

- **4048** – When restarting management system processes on Solaris from an "sh" shell, the MC/DC and Directive Handler processes were seen to stop after running for several hours. This is an intermittent problem. Other shells (tcsh and bash) do not have a problem.
- **3384** – The management system creates core files when the server processes are intentionally shut down. This is harmless behavior by the management system.

6.4 Known Issues in ScreenOS 5.1r3 That Affect NetScreen-Security Manager 2004 FP3r2

The following is a known issue in ScreenOS 5.1r3 that specifically affects this release of NetScreen-Security Manager:

- **44586** – In devices that support virtual systems (vsys), if the secondary banner is set at the root level, updating a vsys through NetScreen-Security Manager fails. The UI displays an error message indicating that the secondary banner is set at the vsys level, even if this option is not available.

W/A: Unset the secondary banner at the root level.

6.5 Known Issues in ScreenOS 5.0 That Affect NetScreen-Security Manager 2004 FP3r2

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, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: Deep Inspection, ERX, ESP, Instant Virtual Extranet, Internet Processor, J-Protect, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-IDP 1000, IDP 50, IDP 200, IDP 600, IDP 1100, ISG 1000, ISG 2000, NetScreen-Global Pro Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, GigaScreen ASIC, GigaScreen-II ASIC, NMC-RX, SDX, Stateful Signature, T320, T640, and T-series. All other trademarks and registered trademarks are the property of their respective companies.

Information in this document is subject to change 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

