NORTEL SWITCHED FIREWALLS 5100 Series
Software Release 2.4.2

1. Release Summary

Release Date : July 2008.
Purpose : Software maintenance release to address customer software issues.

2. Important Notes Before Upgrading to This Release

Upgrade to 2.4.2 is supported from 2.2.7 or later versions. 2.4.2 requires 500 MBytes free space on the /isd partition. To check the available free space, login as root, run "df –H /isd" and look under the "Avail" column. If you do not have enough free space, you will get an error saying "Failed to unpack software …" when you try to download the .pkg file.

If there is not enough free space to upgrade, please export the current configuration using "/cfg/ptcfg", do a clean install from CD, and then import the configuration using "/cfg/gtcfg".

Pre upgrade checks:
New validations have been added for some CLI commands. If these parameters are not configured properly, upgrade to 2.4.2 will fail due to the new validation checks. Please refer to the CR# Q01475332 for all the new validations.

To upgrade, first download the appropriate 2.4.2 upgrade package to the cluster. This can be done over the network using "/boot/software/download" or from the CD-ROM using "/boot/software/cdrom". Run "/boot/software/cur" to make sure the new version was downloaded successfully. You can then activate the new version using "/boot/software/activate".

Upgrade procedure in cluster mode from CLI

- Get the NSF5100_2.4.2.0_Rxx.pkg file and copy it to an ftp server or in a CD.
- Download the new upgrade image via ftp/CDROM using /boot/software/download or */boot/software/cdrom* command from the CLI. This should be done only in one Director.
- After the download is complete, check the current versions of the software and you will see that the version you downloaded has a status 'unpacked'.
- Check if any access list entries are configured on the Firewall. If access lists are configured for networks other than the SSI network, add a new access list entry for SSI network (it's mandatory for NSF 2.4.2.0 upgrade process to have entries for the SSI network as well).
- Activate the new (unpacked) version software by running the following command in the CLI: /boot/software/activate.
- At this time, both firewalls will be rebooted twice to make the post upgrade changes effective.
- Wait for a minute or two for the firewalls to initialize all system components.

- Check the firewall status by executing /info/sum command from the CLI and make sure you see both firewalls as 'up'.
- Check the CP sync status. This should show both the iSDs as 'active'.

Note: *Upgrade to 2.4.2_R65 from any previous version is not supported from BBI. Only CLI upgrade is supported.*

Upgrade procedure in standalone mode from CLI

- Get the NSF5100_2.4.2.0_Rxx.pkg file and copy it to an ftp server or in a CD.
- Download the new upgrade image via ftp/CDROM using /boot/software/download or */boot/software/cdrom* command from the CLI.
- Once the download is complete, check the current versions of the software and you will see that the version you downloaded has a status 'unpacked'.
- Activate the new (unpacked) version software by running the following command in the CLI: */boot/software/activate.*
- At this time, both firewalls will be rebooted twice to make the post upgrade changes effective.
- Wait for a minute or two for the firewall to initialize all system components
- Check the firewall status by executing /info/sum command from the CLI and make sure you are seeing the firewall status as 'up'

Note: *Upgrade to 2.4.2_R65 from any previous version is not supported from BBI. Only CLI upgrade is supported.*

3. Platforms Supported

Hardware platforms supported

The Nortel Switched Firewall 5100 Series Release 2.4.2 supports the following hardware platforms:

Hardware Model	PEC
NSF 5111-NE1	EB1639127, EB1639127E5
NSF 5114-NE1	EB1639128, EB1639128E5
NSF 5124-NE1	EB1639129, EB1639129E5

Hardware Models with their Product Equipment Code

Supported Check Point applications

Nortel Switched Firewall 5100 Series 2.4.2 supports the following *Check Point applications:
• Firewall-1®
• ISP Redundancy
• User Authority®
• VPN-1®
• SmartDefense™
• NAT
• Authentication
• Content Security
• ClusterXL®
• Policy Server
Floodgate-1®
• Management Tools
• SmartView Monitor™
• SmartCenter™ Server
• Smart Portal
• Eventia Reporter

Configure the following management tools outside the NSF 2.4.2 software:
• SmartDashboard™
• SmartView Tracker™
• SmartView Status™

4. Notes For Upgrade

File names for this release

File Name	Module or File Type	File Size(K.B)
NSF5100_2.4.2.0_R60.iso	.iso (contains .img and .pkg files)	433568
NSF5100_2.4.2.0_R65.iso	.iso (contains .img and .pkg files)	593280

File Name	MD5 Checksum
NSF5100_2.4.2.0_R60.iso	.iso (contains .img and .pkg files)
NSF5100_2.4.2.0_R65.iso	.iso (contains .img and .pkg files)

5. Version of Previous Release

Software version 2.4.1, Release date - March 31, 2008

6. Compatibility

N/A

7. Changes in This Release

Problems solved in this release: 2.4.2

Q01857817	When configured the 5100 firewall cluster as 'Check Point UTM Gateway (option # 3 during 'new') and add a sync interface, the cluster is not going for a reboot. Because of this reboot failure the sync is not started properly. SIC (Secure Internal Communication) cannot be established if once we hard reboot the iSDs. This issue occurs only with R65 CP version and is caused because of the incorrect setting of installation mode in the config script. This issue is fixed in 2.4.2 release by correcting the mode of installation to distributed mode.
Q01848535	A new enhancement is added in the 2.4.2 release to include /var/tmp/monitor/log files in the tsdump, as these are useful to know more details about memory and system information.
Q01851636	In NE1 5124 platform, upgrading from pre 2.3.6 releases to any higher release was failing. This is due to the introduction of CPacc4 module (new module of Checkpoint for RoHS compliant BCM5823 cards which can also support older BCM5822 VPN accelerator cards) from 2.3.6.1 onwards. This new driver fails to install over an existing old driver. The issue is fixed in the release 2.4.2 by correcting the installation procedure to uninstall any pre-existing acc3 modules before upgrading to the acc4 module.
Q01843354	In a cluster setup, whenever static routes are added, sync is going down. This issue happens because both MIP owner and NON-MIP owner are trying to update the SSI registry database at a time, which is leading to SSI crash. This issue is fixed in 2.4.2 by stopping the Non-MIP owner from updating the database, there by only MIP owner updates the database and the updated info will be propagated to cluster members.
Q01849045	If a loop back IP or multicast IP or IP having 0 or 255 in one of the octets is added to the access list, then changes don't get applied. IP address validation doesn't allow having a '0' or '255' in any octet of the IP address. This issue is fixed by removing the IP address validation.
Q01880731	The user additions from /cfg/sys/usr/add are allowed even without specifying a password whereas the same operation from the BBI would throw error. This

issue is addressed in 2.4.2 by adding a check for the password as soon as a user is created.

Q01885243 Traffic is affected in a tunnel where BCM5822 VPN card with CPacc4 driver module or BCM5823 VPN card with CPacc3 driver module is installed. This issue is fixed in 2.4.2 release by installing proper modules to corresponding VPN cards. i.e., CPacc3 module for BCM5822 and CPacc4 module for BCM5823.

Q01871064 Synch network is going down whenever any interface is added or deleted in a cluster setup. This issue happens only in a setup where L2 bridge was configured and removed later. This is because of not proper cleaning up of previous bridge settings in NON-MIP owner's registry database. This issue is resolved in the release 2.4.2 by proper deletion of the bridge settings from the Non-MIP owner also.

8. New Outstanding Issues

Q01798595 Hardware Installation Manual doesn't include information about the system status LED's glow color "solid Amber". The system status LEDs indicate the operational status of four fans, chassis, CPU temperature, ambient temperature and the voltages(+5V and +12V). The different glow states of LEDs are,

1. If the system is reset then the LED doesn't glow.
2. If system detects any problem with any of the CPU temperature, fan speed, system voltages then LED glows amber.
3. If the system is working LED glows in solid green.
4. If the system halts then LED flashes.

Q01888674 All existing voice calls are getting terminated when a CP policy with SIP (Session Initiation protocol) is added to the rule base and the same is pushed to firewall. As a work around to this issue, a rule with host Ips of specific source and specific destination has to be mentioned in the rule base instead of the network addresses with service "ANY".

Q01889322 Following issues are noticed with Hide/Static NAT'd voice calls with SIP enabled CP policy.

1. About 50% of the voice calls gets failed. A voice call to the destination phone will make it ring. But even that call is accepted, the caller doesn't hear any voice and it appears to the caller as if the call is not accepted. Also the caller is intimated with an error message Declined: Temporarily Unavailable". All non-NAT'd calls are successful.
2. Any voice calls through the hard phones would fail if tried to initialize after an idle period of 10 or more minutes (enters into HANGUP mode). A soft or hard reboot of the hard phone can be used as a workaround to end this problem.
3. No voice call is allowed on SIP soft phones. An attempt to initiate a call will end up with an error message stating "Proxy authentication required".

SIP with no-NAT doesn't exhibit any of the above errors.

Q01889319	If the status of the NAT is changed from no NAT to NAT enabled or from with NAT to without NAT and a CP policy is pushed then no more calls can be made.

9. New Known Limitations

N/A

For information on previous releases, please refer to the 2.4.1 Read Me file.

For other known issues, please refer to the product release notes and technical documentation available from the Nortel Technical Support web site at: http://www.nortel.com/support.