>BUSINESS MADE **SIMPLE**

NORTEL

Nortel Security Solutions
Product Readme

Nortel Switched Firewall 6000 Series 4.1.x - Readme

Document Date: 14 September, 2007
Document Version: 2.1

Table of Contents

Change Log

Version	What	When	Who
1.0	Readme for 4.1.1 release	07/24/2005	Rajesh Vijayakumar
1.1	Added CR Q01113493	08/23/2005	Rajesh Vijayakumar
1.2	Readme for 4.1.2 release	03/22/2006	Ganesh Lakshmanan
1.3	Readme for 4.1.2.1 R61 release	07/07/2006	Ganesh Lakshmanan
1.4	Layout, documentation corrected	07/29/2006	Jürgen Luksch
1.5	Readme for 4.1.3 release	08/08/2006	Santhosh Balasubramanian
1.6	Readme for 4.1.3 release updated	09/01/2006	Santhosh Balasubramanian
1.7	Readme for 4.1.3.1 release	09/08/2006	Santhosh Balasubramanian
1.8	Readme for 4.1.3.4 R62 release	12/14/2006	Samuel Praveen
2.0	Readme for 4.1.4 release	04/30/2007	Samuel Praveen
2.1	Readme for 4.1.5 release	09/14/2007	Samuel Praveen

1 Introduction

This is the consolidated readme for all NSF 4.1.x releases. The objective of a single readme is to help the reader find and track the status and history of an issue more easily. In order to meet this objective, the document is organized in different sections as follows.

Section 2 contains a table that lists the status of all known issues found in 4.1.x releases. It shows the release where the issue was found, the current status of the issue, and the status of the issue in each 4.1.x software release. The following section (Section 3) describes the procedure to upgrade from an earlier release to a 4.1.x release.

The following sections present the detailed readme for each release (one section for each release). These sections describe the hardware platforms and Check Point software versions supported by each release. Finally, the list of all known issues with a brief description and work around (if any) is presented in Appendix A. The current status of each issue is also presented as part of the description.

2 Status of Known Issues and Limitations

All the known issues found and/or fixed in 4.1.x releases are summarized in the following table. The details of the issues are described in Appendix-A. Each row in the table corresponds to a known issue. A detailed explanation of the issue can be found by looking at the CR# (if available) in the Appendix. If a CR# is not available for an item, then search for the issue title in the Appendix for the specific update date. The known issues without the CR# are listed at the beginning of each sub-section for the specific update date.
If you are viewing this document on your computer, you can click on a description item to jump to the full description in Appendix A.

The current status and the status of the issue in different releases are also presented in the table. In the table, ☒ means the particular build is affected, ☑ means the issue is fixed in the particular build and 'blank' entry indicates that the CR existence is not verified in that particular build.

Table 1 Current status of all issues found in NSF-4.1.x releases.

CR #	Description of Issues and Limitations	Last Updated	Current Status	Status in Different Releases ☒							
				4.1.1	4.1.2	4.1.2.1	4.1.3	4.1.3.1	4.1.3.4	4.1.4	4.1.5
Q01528223	cfgd is getting crashed while resetting the switch when jumbo is enabled	08/31/2007	Closed				☒	☒	☒	☒	☑
Q01511878	Even though GOTO ID is greater than Filter ID, apply is successful	08/31/2007	Closed							☒	☑
Q01499951	GRE tunnel not operational when name exceeds 15 characters	08/31/2007	Closed				☒	☒	☒	☒	☑
Q01616071	NSF Telnet not working on newly joined SFD when telnet is enabled	08/31/2007	Closed				☒	☒	☒	☒	☑
Q01562278	Fatal error message displayed on screen when ssh is enabled for the first time	08/31/2007	Closed							☒	☑

Q01557635	Unable to join the new SFD in the cluster, after enabling sync in the existing SFD	08/31/2007	Closed							☒	☑
Q01342026	/maint/tsdump/export gets error if password contains '||' or a space	08/31/2007	Closed		☒	☒	☒	☒	☒	☒	☑
Q01508294	Wrong CLI display for idle timeout value	08/31/2007	Closed				☒	☒	☒	☒	☑
Q01137863-01	Dumping Accelerators ARP table via SNMP	08/31/2007	Closed		☒	☒	☒	☒	☒	☒	☑
Q01570767	/info/traffic displays wrong information after adding 3rd director	08/31/2007	Closed				☒	☒	☒	☒	☑
Q01488250	/info/sensor gives incorrect output	08/31/2007	Closed		☒	☒	☒	☒	☒	☒	☑
Q01679013	SNMP queries to firewall are returned with different source address or times out	08/31/2007	Closed				☒	☒	☒	☒	☑
Q01526868	Unable to add more than 1500 proxy arp entries	08/31/2007	Closed				☒	☒	☒	☒	☑
Q01468701	Accelerator '/i/slb/sess/help' description is incorrect	08/31/2007	Closed		☒	☒	☒	☒	☒	☒	☑
Q01049739	/i/clu displays error when the NSF cluster is idle for 1 or more weeks	08/31/2007	Closed	☒	☒	☒	☒	☒	☒	☒	☑
Q01531319	Auto Back-up feature on NSF products	08/31/2007	Closed		☒	☒	☒	☒	☒	☒	☑
Q01619202	NSF 4.1.x: Latency issues due to SP route cache filling up the ARP table	08/31/2007	Closed				☒	☒	☒	☒	☑

Q01687153	Hitless upgrade process should ask user to reset sic and push policy	08/31/2007	Closed							☒	☑
Q01512725	No options in filter to fix the maximum length of ip packet	08/31/2007	No Fix Planned				☒	☒	☒	☒	☒
Q01667113	'/info/capability' displays incorrect accelerator and aim connections	08/31/2007	Closed				☒	☒	☒	☒	☑
Q01691888	Adding additional entry in IPACL makes Acceleration OFF	08/31/2007	Closed							☒	☑
Q01691624	Accelerator fails to configure when a filter is associated to a port	08/31/2007	Closed							☒	☑
Q01692551	Invalid session table remains after SFA failover	08/31/2007	Closed							☒	☑
Q01450312	WEBUI: Accelerator display is not shown properly when we replace one accelerator	08/31/2007	Closed				☒	☒	☒	☒	☑
Q01616110	SSI Error is reported during join when SYNC is enabled prior to join	08/31/2007	Closed				☒	☒	☒	☒	☑
Q01451314	Radius configuration locks root user out of firewall	08/31/2007	Closed		☒	☒	☒	☒	☒	☑	
Q01425452	Panic on Accelerator after ASF power off	08/31/2007	Closed		☒	☒	☒	☒	☒	☑	
Q01685554	Unable to push the policy in R55 with HFA_20	09/07/2007	Open				☒	☒			
Q01742602	Backup/Restore fails for different CP Versions	09/07/2007	Open							☒	☒

Q01612783	TCP connections which use TCP window scaling option stall intermittently	09/12/2007	Open	☒	☒	☒	☒	☒	☒	☒	☒
Q01520395	Single fiber link failure of IAP does not fail over to copper	03/20/2007	Open	☒	☒	☒	☒	☒	☒	☒	☒
Q01540553	Some packets are dropped while a checkpoint policy is pushed to the firewall	09/12/2007	Open	☒	☒	☒	☒	☒	☒	☒	☒
Q01575439	NSF/inconsistencies between /info/acc and /info/det	08/31/2007	Closed		☒	☒	☒	☒	☒	☒	☑
Q01451288	Sync port down/up whenever accelerator is reconfigured	03/20/2007	Closed		☒	☒	☒	☒	☒	☑	
Q01460485	Cable unplugged on GBICs doesn't failover	03/20/2007	Closed	☒	☒	☒	☒	☒	☒	☑	
Q01535310	IAP failure creates 2 MIPs in a cluster	03/20/2007	Closed	☒	☒	☒	☒	☒	☒	☑	
Q01441056	cfgd crashes after installing HFA_04 (both 4.1.3 and 3.5.7 builds)	03/20/2007	Closed				☒	☒	☒	☑	
Q01488650	ASF prefers def gw advertised through ospf over def gw configured statically	03/20/2007	Closed					☒	☒	☑	
Q01525481	Accelerator is getting panic when we give -ive value for port statistics from ISD	03/20/2007	Closed				☒	☒	☒	☑	
Q01530663	Not able to install ASF image on NE isd with 160 GB HDD	03/20/2007	Closed				☒	☒	☒	☑	

Q01540529	SIC reset is needed after upgrade from 4.1.2 R60 to 4.1.3 R60	03/20/2007	No Fix Planned				☒	☒	☒	☒	☒
Q01460968	No Special Character Support for Admin password	03/20/2007	Open				☒	☒	☒	☒	☒
Q01587914	CLI command to enable/disable TCP sequence verification	03/20/2007	Closed				☒	☒	☒	☑	
Q01456570	Firewall leaking nonIP packets when IDSLB is enabled	03/20/2007	Closed					☒	☒	☑	
Q01469207	ASF6614 4.1.3/R60 - CheckPoint VPN is failing following HA failover	03/20/2007	Closed				☒	☒	☒	☑	
Q01539020	Websense UFP filtering stops due to lack of ports	03/20/2007	Closed				☒	☒	☒	☑	
Q01415915	Firewall Director locks up after several hours because of memory leak	09/14/2007	Open		☒	☒	☒	☒	☒	☒	☒
Q01496816	Large packets are getting dropped incorrectly	03/20/2007	Closed	☒	☒	☒	☒	☒	☒	☑	
Q01509522	Under stress condition, after rebooting the ISD's, sync is in "error state".	12/01/2006	Open						☒	☒	☒
Q01448475	IDSLB: Not able to set IDSLB group as 0 (to disable monitoring) on a particular VLAN.	09/08/2006	Closed				☒	☑			
Q01435035	IDSLB: IDS load balancing on NSF High Availability setup causes network loop	09/08/2006	Closed		☒	☒	☒	☑			

Q01104528	Switch reboots when we use /cfg/slb/isdfw/isd_no command in GOD mode	08/28/2006	Closed		☒	☒	☑				
Q01106902-03	Health Check Daemon and Config Daemon may not work properly after 248 days of uptime	08/28/2006	Closed		☒	☒	☑				
Q01410552	New HFAs are missing for R55 & R60	08/28/2006	Closed		☒	☒	☑				
Q01311541-01	Unable to add Proxy ARP	08/28/2006	Closed			☒	☑				
Q00910450-01	Oper group permissions	08/28/2006	Closed			☒	☑				
Q01317877	Validation should give error/warning msg when we delete the 10.10.1.0 from accesslist	08/28/2006	Closed				☑				
Q01340625	SFD always get panic when installing R60 HFA-03 with kdb mode on	08/28/2006	Closed			☒	☑				
Q01340625-01	SFD always get panic when installing new HFA version with kdb mode on.	08/28/2006	Open			☒	☒	☒	☒	☒	☒
Q01338741	JOIN fails when we try to add a member with 16 bit mask	08/28/2006	Closed				☑				
Q01095463	Not able to bring up copper gig port when we disable auto negotiation in 6600	08/28/2006	Closed			☒	☑				

Q01329192	Request to have an info cmd to view the CPU usage over a period of time	08/28/2006	Closed				☑				
Q01408009	NSF 6600 / 4.1.1 / RSA sdconf.rec file is deleted from /var/ace after reboot	08/28/2006	Closed				☑				
Q01266907	SSI Restarting	08/28/2006	Closed	☒	☒	☒	☑				
Q01445437	ASF continuously deleting and adding default route sent by Cisco	03/20/2007	Closed				☒	☒	☒	☑	
Q01427432	Oper user can be able to change the password of admin user	03/20/2007	Closed				☒	☒	☒	☑	
Q01435023	Hard disk usage calculation is wrong when we connect usb stick to the ISD	03/20/2007	Closed				☒	☒	☒	☑	
Q01435081	Upgrade: Switch panic while doing hitless Upgrade from 4.1.2.0 to 4.1.3.0	08/28/2006	Open				☒	☒	☒	☒	☒
Q01438644	Non MIP ISD remains in Passing State after the Upgradation to 4.1.3_R61	08/31/2007	Closed				☒	☒	☒	☑	
Q01448478	IDSLB: disable or enable IDS globally, there is a failover triggered always	08/28/2006	Open				☒	☒	☒	☒	☒
Q01437950	/cfg/acc/det and /info/det are not showing active accelerators	09/07/2007	Open				☒	☒	☒	☒	☒
Q01444801	ASF6414 - Clearing accelerator stats from the director	03/20/2007	Closed				☒	☒	☒	☑	

Q01434591	NSF 4.1.2_R60 SNMP queries, not returned	08/31/2007	Closed				☒	☒	☒	☒	☑
Q01437363	Radius user accounts on NSF	08/28/2006	Open				☒	☒	☒	☒	☒
Q01161524	SFD cannot detect SFA after disabling jumbo frame and enabling trunking	08/28/2006	Closed				☑				
Q01245413	Command /opt/tng/bin/lb is not giving the expected output	08/28/2006	No Fix Planned		☒	☒					
Q01231858	4.1.1 drops packets that arrive out of order	08/28/2006	Open	☒	☒	☒	☒	☒	☒	☒	☒
Q01418950	NSF/BBI or WebUI based port configuration is causing BBI problems	08/04/2006	Closed				☑				
Q01334782	Web Server did not work when adding new port or new filter	08/04/2006	Closed				☑				
Q01373575	WEBUI TICKER: Not able to view history while running ticker for more than 10 days	08/04/2006	Closed				☑				
Q01329143	WEBUI ticker : Throughput In and Out shown in Ebps when we do failover	08/04/2006	Closed				☑				
Q01351923	Hard disk space (/config) usage goes more than 70% after the upgrade	08/04/2006	Closed				☑				
Q01338725	HFA is not getting upgraded during software from 4.1.1.0_R55 to 4.1.2_R55	03/22/06	Closed	☒	☒	☒	☑				
Q01338744	mond.log file is not getting rotated when	03/22/06	Closed	☒	☒	☒	☑				

	we run the system more than 10 days										
Q01218241	Primary port failing to copper backup flips cluster	03/22/06	Closed	☒	☑						
Q01229738	snmpd process keeps restarting	03/22/06	Closed	☒	☑						
Q01208951	NTP server access is not restricted to SFD subnet	03/22/06	Closed	☒	☑						
Q01234723	NSF 4.1.1 Replacing a SFA shows 3 SFA's in /info/det	03/22/06	Closed	☒	☑						
Q01248760	unnecessary/confusing log message related to SFD status in single SFD SETUP	03/22/06	Closed	☒	☑						
Q01279395	Accelerator is 1 hour ahead of directors	08/31/07	No Fix Planned	☒	☒	☒	☒	☒	☒	☒	☒
Q01326194	L2 Vlan does not work properly	08/31/07	Closed		☒	☒	☒	☒	☒	☒	☑
Q01252655	/cfg/sys not available to change NAAP VLAN id on accelerator	03/22/06	Closed	☒	☑						
Q01284910	VPN Site to Site doesn't work	08/31/07	No Fix Planned		☒	☒	☒	☒	☒	☒	☒
Q01296879	bogus ERRORS ON PORTS 27 AND 28 OF THE ACCELERATOR	03/22/06	No Fix Planned	☒	☒	☒					
Q01335693	NSF /var/tmp/local_state file filling up	03/22/06	Closed	☒	☑						
Q01113493	FTP session fails when TCP sequence verification is enabled	03/22/06	Closed	☒	☒	☑					
	Sync thro vnic is not	03/22/06	No Fix	☒	☒	☒					

Q01061470	supported with VPN		Planned								
Q01050555	Using copper GBIC on dual ports of 6600	03/22/06	No Fix Planned	☒	☒	☒					
Q01104775	Proxy Arp entries above 1600 does not work	03/22/06	No Fix Planned	☒	☒	☒					
Q01052781	“Softdog driver open failure” message when accelerator boots up	03/22/06	No Fix Planned	☒	☒	☒					
Q01094577	Pimd restarts when ip address on pim enabled interface is changed	03/22/06	No Fix Planned	☒	☒	☒					
Q01089358	Changes made to routemaps do not take effect immediately	03/22/06	No Fix Planned	☒	☒	☒					
Q01142037	Issues related to large configurations	03/22/06	No Fix Planned	☒	☒	☒					
Q01117033	Incorrect UDP Blast behavior	03/22/06	No Fix Planned	☒	☒	☒					
Q01157944	Director runs out of memory during bootup	03/22/06	No Fix Planned	☒							
Q01174716	Dos attack traffic causes high MP CPU utilization on accelerator	03/22/06	Closed	☒	☑						
Q01164785	Error message for pmatch string longer than 40 characters is not clear	03/22/06	Closed	☒	☑						
Q01138787	Limit on number of virtual NICs	03/22/06	No Fix Planned	☒	☒	☒					
Q01159781	Changing subnet on RIP enabled interface requires restarting RIP	03/22/06	No Fix Planned	☒	☒	☒					
Q01158579	Static routes are lost after importing configuration	03/22/06	No Fix Planned	☒	☒	☒					
	No validation check	03/22/06	Closed	☒	☑						

Q01149215	to prevent invalid subnet mask for IP ACL										
Q01133343	/info/sensors show CPU and board temperature to be negative	08/31/2007	No Fix Planned	☒	☒	☒					
Q01150870	PIM: NSF does not support fragmented PIM messages	03/22/06	No Fix Planned	☒	☒	☒					
Q01157101	Validation error about accesslist after upgrade	08/31/07	Closed	☒	☒	☒	☑				
Q01160601	“asfcapture” does not capture packets simultaneously on accelerator and director	03/22/06	Closed	☒	☑						
Q01157140	Unable to configure accelerator after upgrade from 4.0.x	03/22/06	No Fix Planned	☒	☒	☒					

3 Upgrading to NSF 4.1.x

Upgrade to 4.1.x is supported from 4.0.1 or later versions. 4.1.5 requires 250 MBytes free space on the /isd partition. To check 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 for upgrade, please export the current configuration using “`/cfg/ptcfg`”, do a clean install from CD, and then import the configuration using “`/cfg/gtcfg`”. When configuration exported from 4.0.2 or below is imported into 4.1.1, you will lose all configured static routes. Please see Q01158579 on how to recover the static routes.

When upgrading from 4.0.x to 4.1.x, please keep the following things in mind. 4.1.x is a combined L2/L3 firewall. If you have multiple ports in the same VLAN, the default behavior of 4.1.x is to apply the firewall policy to traffic that is bridged between the ports. This is different from the 4.0.x behavior which applied the firewall policy only to routed traffic. If you would like to keep the 4.0.x behavior, please disable L2 firewall processing on these VLANs using the “`/cfg/net/vlan <n>/l2fw`” CLI item after upgrade.

To upgrade, first download the appropriate 4.1.x upgrade package to the cluster. This can be done over the

network using "/boot/software/download" or from the CR-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".

After the successful software upgrade, the following steps must be done:

1. Re-establish the trust for each director by,
   a. Reset sic on the firewall director (/cfg/fw/sic).
   b. Unload the default policy on the firewall director (/maint/diag/uldplcy).
   c. On the CP management server, Reset and re-initialize sic on the firewall director object.
2. Push the Check Point Firewall policy from the CP management server.

After upgrade from 4.0.x, please make sure the accelerators are configured by running "/info/det". If an error is reported, please see Q01157140 to recover.

The summary of the main steps for upgrading to NSF 4.1.5 is given in the following table

Upgrading to NSF 4.1.5

From	To	Upgrade Steps
4.0.1-x	4.1.5 R60 Or 4.1.5 R65	• Do a clean install using iso image.
4.0.2.0a	4.1.5 R60 (HFA 05) Or 4.1.5 R65	• Use "/boot/software/download" to download R60 or R65 upgrade package (NSF_Director_4.1.5_R60.pkg or NSF_Director_4.1.5_R65.pkg). This should be done only in one SFD. • Activate 4.1.5 image using "/boot/software/activate". This should be done only in one SFD. • Please wait until SFDs reboot and all upgrade process is complete. • Re-establish the trust for each director by, a. Reset sic on the firewall director (/cfg/fw/sic). b. Unload the default policy on the firewall director (/maint/diag/uldplcy). c. On the CP management server, Reset and re-initialize sic on the firewall director object. • Push the Check Point Firewall policy from the CP management server. • Do the post-upgrade verification.
4.0.3.0 4.0.4.0	4.1.5 R60 (HFA 05)	• Use "/boot/software/download" to download R60 or R65 upgrade package (NSF_Director_4.1.5_R60.pkg or

	Or 4.1.5 R65	upgrade package (NSF_Director_4.1.5_R60.pkg or NSF_Director_4.1.5_R65.pkg). • Activate 4.1.5 image using "/boot/software/activate". This should be done only in one SFD. • Please wait until SFDs reboot and all upgrade process is complete. • Re-establish the trust for each director by, a. Reset sic on the firewall director (/cfg/fw/sic). b. Unload the default policy on the firewall director (/maint/diag/uldplcy). c. On the CP management server, Reset and re-initialize sic on the firewall director object. • Push the Check Point Firewall policy from the CP management server. • Do the post-upgrade verification.
4.1.1	4.1.5 R60 (HFA 05) Or 4.1.5 R65	• Use "/boot/software/download" to download R60 or R65 upgrade package (NSF_Director_4.1.5_R60.pkg or NSF_Director_4.1.5_R65.pkg). • Activate 4.1.5 image using "/boot/software/activate". This should be done only in one SFD. • Please wait until SFDs reboot and all upgrade process is complete. • Re-establish the trust for each director by, a. Reset sic on the firewall director (/cfg/fw/sic). b. Unload the default policy on the firewall director (/maint/diag/uldplcy). c. On the CP management server, Reset and re-initialize sic on the firewall director object. • Push the Check Point Firewall policy from the CP management server. • Do the post-upgrade verification.
4.1.2	4.1.5 R60 (HFA 05) Or 4.1.5 R65	• Use "/boot/software/download" to download R60 or R65 upgrade package (NSF_Director_4.1.5_R60.pkg or NSF_Director_4.1.5_R65.pkg). • Activate 4.1.5 image using "/boot/software/activate". This should be done only in one SFD. • Please wait until SFDs reboot and all upgrade process is complete. • Re-establish the trust for each director by, a. Reset sic on the firewall director (/cfg/fw/sic). b. Unload the default policy on the firewall director

		(/maint/diag/uldplcy). c. On the CP management server, Reset and re-initialize sic on the firewall director object. • Push the Check Point Firewall policy from the CP management server. • Do the post-upgrade verification.
4.1.2.1	4.1.5 R60 (HFA 05) Or 4.1.5 R65	• Use "/boot/software/download" to download R60 or R65 upgrade package (NSF_Director_4.1.5_R60.pkg or NSF_Director_4.1.5_R65.pkg). • Activate 4.1.5 image using "/boot/software/activate". This should be done only in one SFD. • Please wait until SFDs reboot and all upgrade process is complete. • Re-establish the trust for each director by, a. Reset sic on the firewall director (/cfg/fw/sic). b. Unload the default policy on the firewall director (/maint/diag/uldplcy). c. On the CP management server, Reset and re-initialize sic on the firewall director object. • Push the Check Point Firewall policy from the CP management server. • Do the post-upgrade verification.
4.1.3	4.1.5 R60 (HFA 05) Or 4.1.5 R65	• Use "/boot/software/download" to download R60 or R65 upgrade package (NSF_Director_4.1.5_R60.pkg or NSF_Director_4.1.5_R65.pkg). • Activate 4.1.5 image using "/boot/software/activate". This should be done only in one SFD. • Please wait until SFDs reboot and all upgrade process is complete. • Re-establish the trust for each director by, a. Reset sic on the firewall director (/cfg/fw/sic). b. Unload the default policy on the firewall director (/maint/diag/uldplcy). c. On the CP management server, Reset and re-initialize sic on the firewall director object. • Push the Check Point Firewall policy from the CP management server. • Do the post-upgrade verification.
4.1.3.1	4.1.5 R60 (HFA 05) Or	• Use "/boot/software/download" to download R60 or R65 upgrade package (NSF_Director_4.1.5_R60.pkg or NSF_Director_4.1.5_R65.pkg).

	4.1.5 R65	• Activate 4.1.5 image using "/boot/software/activate". This should be done only in one SFD. • Please wait until SFDs reboot and all upgrade process is complete. • Re-establish the trust for each director by, a. Reset sic on the firewall director (/cfg/fw/sic). b. Unload the default policy on the firewall director (/maint/diag/uldplcy). c. On the CP management server, Reset and re-initialize sic on the firewall director object. • Push the Check Point Firewall policy from the CP management server. • Do the post-upgrade verification
4.1.3.4	4.1.5 R60 (HFA 05) Or 4.1.5 R65	• Use "/boot/software/download" to download R60 or R65 upgrade package (NSF_Director_4.1.5_R60.pkg or NSF_Director_4.1.5_R65.pkg). • Activate 4.1.5 image using "/boot/software/activate". This should be done only in one SFD. • Please wait until SFDs reboot and all upgrade process is complete. • Re-establish the trust for each director by, a. Reset sic on the firewall director (/cfg/fw/sic). b. Unload the default policy on the firewall director (/maint/diag/uldplcy). c. On the CP management server, Reset and re-initialize sic on the firewall director object. • Push the Check Point Firewall policy from the CP management server. • Do the post-upgrade verification.
4.1.4	4.1.5 R60 (HFA 05) Or 4.1.5 R65	• Use "/boot/software/download" to download R60 or R65 upgrade package (NSF_Director_4.1.5_R60.pkg or NSF_Director_4.1.5_R65.pkg). • Activate 4.1.5 image using "/boot/software/activate". This should be done only in one SFD. • Please wait until SFDs reboot and all upgrade process is complete. • Re-establish the trust for each director by, a. Reset sic on the firewall director (/cfg/fw/sic). b. Unload the default policy on the firewall director (/maint/diag/uldplcy). c. On the CP management server, Reset and re-initialize sic

		on the firewall director object. • Push the Check Point Firewall policy from the CP management server. • Do the post-upgrade verification

3.1 Pre-Upgrade Preparation

Backup configuration: You are strongly advised to backup the NSF configuration before doing the upgrade. Please use "`/cfg/ptcfg`" command to export the configuration. This should be done only in one SFD.

3.2 Downloading the upgrade Package

The upgrade package can be downloaded by two different ways. In the first method, the image can be downloaded via FTP using "`/boot/software/download`" CLI command. The CLI will prompt for all the details information, such as IP address of the server and the filename on the server, etc.

Since the NSF installation CD contains the upgrade files (i.e. pkg files), it can be used to import the pkg file to the SFD. User can also burn his/her own CD containing the pkg file. Note that upgrade process requires that file extension to be .pkg. The CD-ROM is automatically ejected at the end of the operation. This step should be done only in one SFD.

3.3 Activating the new software

Once the upgrade package is downloaded, "`/boot/software/cur`" can be used to display all the software versions in the SFD. The version that was just imported will have the status "unpacked." The new version (4.1.5) can now be activated using "`/boot/software/activate`". This should be done only in one SFD.

The activation process will upgrade both the Nortel software and the Check Point software to the same version as a clean install from the CD. There is no need to upgrade the Check Point software separately. Each SFD will reboot twice during the upgrade process: once after the upgrade of Nortel software and again after upgrading the Check Point software. The whole process could take somewhere between 15-20 minutes.

After the successful software upgrade, the following steps must be done:

1. Re-establish the trust for each director by,
    a. Reset sic on the firewall director (/cfg/fw/sic).
    b. Unload the default policy on the firewall director (/maint/diag/uldplcy).
    c. On the CP management server, Reset and re-initialize sic on the firewall director object.
2. Push the Check Point Firewall policy from the CP management server.

3.4 Post-Upgrade Verification

The following steps should be done to verify that the upgrade process was completed successfully. These steps are not required for a successful upgrade. However, it is recommended only for the purpose of verification.

- Login as root and run "`os-version`". You will get the output "1.5.1.3_tng.4.1.5_R60" or "1.5.1.3_tng.4.1.5_R65"
- Login as admin and check "`/info/cluster`" CLI to make sure that all the directors in the cluster are working fine.

4 Hitless Upgrade

If you have a high availability setup, consisting of 2 accelerators and 2 or more directors, you can upgrade the cluster with virtually no downtime. To start the hitless upgrade process, please use the "`/boot/software/hitless/activate`" CLI. For hitless upgrade to work smoothly, make sure the following conditions are met.

- Both the active and backup accelerators should have all the network links up
- Do not disconnect any network cables or reboot any accelerator or director while hitless upgrade is in progress.

Hitless upgrade works by upgrading one side of the cluster first, then failing over traffic to that side and upgrading the other side. Hitless upgrade will pause after upgrading one side and wait for you to re-establish the trust and push the policy to the upgraded side before failing over to that side.

Stateful session failover is not available during hitless upgrade because Check Point sync will not work between different versions.

Hitless Upgrade to NSF 4.1.5

From	To	Upgrade Steps
4.1.1	4.1.5 R60 (HFA 05) Or 4.1.5 R65	1) Use "/boot/software/download" to download R60 or R65 upgrade package (NSF_Director_4.1.5_R60.pkg or NSF_Director_4.1.5_R65.pkg). 2) Activate 4.1.5 image using "/boot/software/hitless/activate". This should be done only in one SFD. 3) Once upgrade is done to one side of the cluster please perform the following on the firewall director and the CP management server for the firewall to become operational

		and upgrade to continue to the other side, a. Reset sic on the firewall director (/cfg/fw/sic). b. Unload the default policy on the firewall director (/maint/diag/uldplcy). c. On the CP management server, Reset and re-initialize sic on the firewall director object. 4) Push the Check Point Firewall policy from the CP management server. 5) Once the other side is upgraded please perform steps 3 & 4 for HA to become operational
4.1.2	4.1.5 R60 (HFA 05) Or 4.1.5 R65	1) Use "/boot/software/download" to download R60 or R65 upgrade package (NSF_Director_4.1.5_R60.pkg or NSF_Director_4.1.5_R65.pkg). 2) Activate 4.1.5 image using "/boot/software/hitless/activate". This should be done only in one SFD. 3) Once upgrade is done to one side of the cluster please perform the following on the firewall director and the CP management server for the firewall to become operational and upgrade to continue to the other side a. Reset sic on the firewall director (/cfg/fw/sic). b. Unload the default policy on the firewall director (/maint/diag/uldplcy). c. On the CP management server, Reset and re-initialize sic on the firewall director object. 4) Push the Check Point Firewall policy from the CP management server. 5) Once the other side is upgraded please perform steps 3 & 4 for HA to become operational
4.1.2.1	4.1.5 R60 (HFA 05) Or 4.1.5 R65	1) Use "/boot/software/download" to download R60 or R65 upgrade package (NSF_Director_4.1.5_R60.pkg or NSF_Director_4.1.5_R65.pkg). 2) Activate 4.1.5 image using "/boot/software/hitless/activate". This should be done only in one SFD. 3) Once upgrade is done to one side of the cluster please perform the following on the firewall director and the CP management server for the firewall to become operational and upgrade to continue to the other side, a. Reset sic on the firewall director (/cfg/fw/sic).

		b. Unload the default policy on the firewall director (/maint/diag/uldplcy). c. On the CP management server, Reset and re-initialize sic on the firewall director object. 4) Push the Check Point Firewall policy from the CP management server. 5) Once the other side is upgraded please perform steps 3 & 4 for HA to become operational
4.1.3	4.1.5 R60 (HFA 05) Or 4.1.5 R65	1) Use "/boot/software/download" to download R60 or R65 upgrade package (NSF_Director_4.1.5_R60.pkg or NSF_Director_4.1.5_R65.pkg). 2) Activate 4.1.5 image using "/boot/software/hitless/activate". This should be done only in one SFD. 3) Once upgrade is done to one side of the cluster please perform the following on the firewall director and the CP management server for the firewall to become operational and upgrade to continue to the other side, a. Reset sic on the firewall director (/cfg/fw/sic). b. Unload the default policy on the firewall director (/maint/diag/uldplcy). c. On the CP management server, Reset and re-initialize sic on the firewall director object. 4) Push the Check Point Firewall policy from the CP management server. 5) Once the other side is upgraded please perform steps 3 & 4 for HA to become operational
4.1.3.1	4.1.5 R60 (HFA 05) Or 4.1.5 R65	1) Use "/boot/software/download" to download R60 or R65 upgrade package (NSF_Director_4.1.5_R60.pkg or NSF_Director_4.1.5_R65.pkg). 2) Activate 4.1.5 image using "/boot/software/hitless/activate". This should be done only in one SFD. 3) Once upgrade is done to one side of the cluster please perform the following on the firewall director and the CP management server for the firewall to become operational and upgrade to continue to the other side, a. Reset sic on the firewall director (/cfg/fw/sic). b. Unload the default policy on the firewall director (/maint/diag/uldplcy). c. On the CP management server, Reset and re-initialize sic on the firewall director object.

		4) Push the Check Point Firewall policy from the CP management server. 5) Once the other side is upgraded please perform steps 3 & 4 for HA to become operational
4.1.3.4	4.1.5 R60 (HFA 05) Or 4.1.5 R65	1) Use "/boot/software/download" to download R60 or R65 upgrade package (NSF_Director_4.1.5_R60.pkg or NSF_Director_4.1.5_R65.pkg). 2) Activate 4.1.5 image using "/boot/software/hitless/activate". This should be done only in one SFD. 3) Once upgrade is done to one side of the cluster please perform the following on the firewall director and the CP management server for the firewall to become operational and upgrade to continue to the other side, a. Reset sic on the firewall director (/cfg/fw/sic). b. Unload the default policy on the firewall director (/maint/diag/uldplcy). c. On the CP management server, Reset and re-initialize sic on the firewall director object. 4) Push the Check Point Firewall policy from the CP management server. 5) Once the other side is upgraded please perform steps 3 & 4 for HA to become operational
4.1.4	4.1.5 R60 (HFA 05) Or 4.1.5 R65	1) Use "/boot/software/download" to download R60 or R65 upgrade package (NSF_Director_4.1.5_R60.pkg or NSF_Director_4.1.5_R65.pkg). 2) Activate 4.1.5 image using "/boot/software/hitless/activate". This should be done only in one SFD. 3) Once upgrade is done to one side of the cluster please perform the following on the firewall director and the CP management server for the firewall to become operational and upgrade to continue to the other side, a. Reset sic on the firewall director (/cfg/fw/sic). b. Unload the default policy on the firewall director (/maint/diag/uldplcy). c. On the CP management server, Reset and re-initialize sic on the firewall director object. 4) Push the Check Point Firewall policy from the CP management server. 5) Once the other side is upgraded please perform steps 3 & 4 for HA to become operational

5 Nortel Switched Firewall, 4.1.1 (07/25/2005)

5.1 Supported Hardware Platforms

NSF 4.1.1 supports the following hardware platforms:

- NSF 6414 (6400 accelerator with 5014 director)
- NSF 6614 (6600 accelerator with 5014 director)
- NSF 6424 (6400 accelerator with 5024 director)
- NSF 6624 (6600 accelerator with 5024 director)
- NSF 6416 (6400 accelerator with 5016 director)
- NSF 6616 (6600 accelerator with 5016 director)
- NSF 6426 (6400 accelerator with 5026 director)
- NSF 6626 (6600 accelerator with 5026 director)

5.2 Supported Check Point Releases

NSF 4.1.1 supports the following Check Point versions:

- Check Point NG with Application Intelligence R54 (FP4) with HFA-414.
- Check Point NG with Application Intelligence R55 with HFA-12.

5.3 What's New

The following new features are supported in this release:

5.3.1 Integrated L2/L3 Firewall

NSF 4.1.x can operate either in L2 mode, L3 mode or combined L2/L3 mode depending on the configuration. To configure ports in L2 mode, define a VLAN and add the ports to the VLAN. Also make sure L2 firewall processing is enabled for the VLAN using "`/cfg/net/vlan <n>/l2fw`" CLI or "Config | Network | VLANs" page in WebUI. L2 firewall processing is enabled by default.

To configure the system in L3 mode, please disable L2 firewall processing for all VLANs that have multiple ports in them. For VLANs with only one associated port and for automatic VLANs, L2 firewall is always off.

To configure a VLAN in combined L2/L3 mode, define the VLAN, add at least 2 ports to the VLAN, enable L2 firewall processing for the VLAN, define an interface and add it to that VLAN. All bridged traffic between ports in the VLAN will go through L2 firewall processing and all routed traffic to another VLAN will go through L3 firewall processing.

5.3.2 Security Pack

Security Pack detects and prevents a number of attacks right on the accelerator.

- Protects against common DoS attacks like Smurf, LandAttack, Fraggle, NullScan, XmasScan, ScanSynFin, PortZero and Blat. This can be configured using "`/cfg/net/port <n>/sec/dos`" from the CLI or "Config | Network | Ports | Security" page in WebUI.
- Management processor rate limiting protects the MP on the accelerator by limiting the number of packets forwarded to it. This can be configured using "`/cfg/acc/mprlimit`" menu in the CLI or "Config | Cluster | Accelerator(s) | General" page in the WebUI.
- UDP blast protection protects UDP services from attack by limiting the amount of traffic on a per service basis. UDP blast settings can be configured using "`/cfg/sec/udpblast`" in the CLI or "Config | Security | UDP Blast" in the WebUI. UDP blast protection can be enabled on a per port basis using "`/cfg/net/port <n>/sec/udpblast`" in the CLI or "Config | Network | Ports | Security" page in WebUI.
- IP range access list (IP ACL) allows user to configure up to 5000 IP addresses to be blocked, for example an ISP black list. IP ACL can be configured using "`/cfg/sec/ipacl`" from the CLI or "Config | Security | IP ACL" from the WebUI and can be enabled on a per port basis using "`/cfg/net/port <n>/sec/ipacl`" in the CLI or "System | Network | Ports | Security" page in WebUI.
- Protocol rate limiting allows you to rate limit TCP, UDP or ICMP sessions. When the threshold rate is exceeded, new sessions will be dropped until the configured hold-down period exceeds. To use protocol rate limiting, you first define a filter using "`/cfg/net/adv/filt`" CLI or "Config | Network | Filters | Filters" page in WebUI. Then you can define how traffic matching that filter should be rate limited using "`/cfg/net/adv/filt <n>/adv/rlimit`" menu in CLI or "Config | Network | Filters | Rate Limiting" page in WebUI. Finally, apply the filter to specific ports using "`/cfg/net/port <n>/enf`" and "`/cfg/net/port <n>/filt`" in CLI or "Config | Network | Ports | General | Modify" page in WebUI.
- Pattern matching allows you to define filters that match the incoming packets against a simple string or a regular expression. To use pattern matching, first define a filter using "`/cfg/net/adv/filt`" CLI or "Config | Network | Filters | Filters" page in WebUI. Then you can define what pattern to search for using "`/cfg/net/adv/filt <n>/adv/pmatch`" menu in CLI or "Config | Network | Filters | Pattern Matching" page in WebUI. Finally, apply the filter to specific ports using "`/cfg/net/port <n>/enf`" and "`/cfg/net/port <n>/filt`" in CLI or "Config | Network | Ports | General | Modify" page in WebUI.

5.3.3 Hitless Upgrade

If you have a high availability setup, consisting of 2 accelerators and 2 or more directors, you can upgrade the cluster with virtually no downtime. To start the hitless upgrade process, please use the "`/boot/software/hitless/activate`" CLI. For hitless upgrade to work smoothly, make sure the following conditions are met.

- Both the active and backup accelerators should have all the network links up
- Do not disconnect any network cables or reboot any accelerator or director while hitless upgrade is in progress.

Hitless upgrade works by upgrading one side of the cluster first, then failing over traffic to that side and upgrading the other side. Hitless upgrade will pause after upgrading one side and wait for you to re-establish the trust and push the policy to the upgraded side before failing over to that side.

Stateful session failover is not available during hitless upgrade because Check Point sync will not work between different versions.

5.3.4 Packet Capture

NSF 4.1.x includes a packet capture utility to troubleshoot traffic related issues. It captures the packet at various points within the system as the packet flows through NSF. It supports ethereal like capture filters using the `–f` flag. To start the packet capture utility, login as root and run "`asfcapture –f <filter>`". Please run "`asfcapture –h`" for a brief help message.

5.3.5 Multicast Routing

NSF 4.1.x supports PIM-SM and IGMPv2 multicast routing. NSF can be used as a transit router or Rendezvous Point (RP). In this initial release, NSF cannot be used as an edge router for multicast. This means that multicast receivers and sources cannot be directly attached to NSF. NSF supports up to 31 outgoing VLANs per (S, G) and up to 63 multicast routes.
PIM can be configured using "`/cfg/net/routes/pim`" from the CLI or "Config | Network | Routes | PIM" from the WebUI.

5.3.6 WebUI Enhancements

The WebUI has a new look and feel with a navigation tree pane on the left which makes it easier to move around. The "Wizards" tab has a number of wizards which walk the user through various configuration tasks. There is also an "Initial configuration wizard" that can be launched immediately after initializing a cluster using the "new" item in the CLI, provided you specify a management interface IP address during "new".

The WebUI also includes a "Ticker", which is a Java applet that can be launched from the WebUI. The ticker displays all information needed to monitor NSF on a single screen and can also display charts over a period of time. Java 1.4.2._01 or newer is required for the ticker applet.

5.3.7 Detailed Explanation of Log Messages

Detailed online help is available for various syslog messages generated by the system. Each message contains an identifier (e.g. `CFGD_011`) which can be looked up from the CLI or WebUI to get more details about the message, possible causes and information on how to resolve it. This can be accessed in the CLI using "`/maint/logdetail`" and from the WebUI by navigating to "Config | Administration | Monitor | Syslog" page.

5.3.8 Enhanced Director Load balancing

NSF 4.1.x allows the user to select the load balancing metric to be used for load balancing traffic across the directors.

- iphash – Traditional load balancing metric using the source and destination IP addresses to select the director.
- ipporthash – Use the source port and destination port in addition to source IP and destination IP. Use this if a large portion of the traffic has the same source and destination IP.

You can also specify a weight between 0 and 15 for each director. You can also specify a weight for the MIP holder, which will override the weight specified for that director.

The load balancing options can be configured using "`/cfg/sys/lbopts`" menu in the CLI or "Config | Administration | Load Balancing" page in WebUI..

5.3.9 Gateway Persistency

When using multiple default gateways and round robin metric for load balancing the default gateways, gateway persistency can be enabled to ensure symmetric routing. Gateway persistency can be enabled on a port using "`/cfg/net/port <n>/gwp`" menu item in CLI or "Config | Network | Ports | General | Modify" page in WebUI.

5.3.10 UPS Support

NSF 4.1.x supports UPS devices manufactured by APC Corp. The directors can communicate with the UPS, detect power failure and shutdown cleanly before the UPS battery runs out. NSF can communicate with the UPS over USB cable or SNMP. UPS settings can be configured using "`/cfg/sys/ups`" menu in CLI or "Config | Administration | APC UPS" page in WebUI.

5.3.11 USB Device Support

You can use USB stick storage devices to transfer files from and to NSF. This includes transferring tsdumps, creating system backups, restoring from backups etc.

5.3.12 RADIUS Authentication

NSF 4.1.1 allows you to use an external RADIUS server for authentication for administrative login to NSF CLI or WebUI. RADIUS server authentication can be configured using "`/cfg/sys/adm/auth`" menu in the CLI or "Config | Administration | RADIUS" page in WebUI. The user name must exist on both NSF and the RADIUS server for the user to login successfully. It is recommended that the "fallback" option be enabled so you can login using the local username and password in case the RADIUS server is down.

5.3.13 OSPF Route Maps

Route maps allow you to exercise fine grained control over route redistribution in OSPF. You can define route maps using "`/cfg/net/route/rmap`" in the CLI or "Config | Network | Routes | RMAP" page in WebUI. These route maps can then be attached to "static", "connected" and "RIP" redistribution from OSPF.

5.3.14 Accelerated Sequence Number Verification

Sequence number verification is part of Check Point SmartDefense. Starting with 4.1.1, the accelerator supports sequence number verification. As a result, sequence number verification is done even for accelerated packets. Sequence number verification can be enabled or disabled from the SmartDefense tab of Check Point SmartDashboard.

5.3.15 SCP/SFTP Support

NSF 4.1.1 allows you to transfer files securely over the network using scp or sftp protocol. This can be used to export configuration, tsdumps, backup file etc.

6 Nortel Switched Firewall, 4.1.2 (03/24/2006)

6.1 Supported Hardware Platforms

NSF 4.1.2 supports the following hardware platforms:

- NSF 6414 (6400 accelerator with 5014 director)
- NSF 6614 (6600 accelerator with 5014 director)
- NSF 6424 (6400 accelerator with 5024 director)
- NSF 6624 (6600 accelerator with 5024 director)
- NSF 6416 (6400 accelerator with 5016 director)
- NSF 6616 (6600 accelerator with 5016 director)
- NSF 6426 (6400 accelerator with 5026 director)
- NSF 6626 (6600 accelerator with 5026 director)

6.2 Supported Check Point Releases

NSF 4.1.2 supports the following Check Point versions:

- Check Point NG with Application Intelligence R54 (FP4) with HFA-417
- Check Point NG with Application Intelligence R55 with HFA12 Or HFA-16
- Check Point NGX (R60)

6.3 What's New

There is no new feature added in 4.1.2.

6.4 Configuration of the Gateway Cluster Object for R60

Please refer to Check Point user guide for a detailed description of the procedure to configure R60 SmartDashboard. The following guidelines should be followed while configuring SmartDashboard for NSF:

- While creating cluster object, both VPN as well as ClusterXL in the "Gateway Cluster Properties" window are selected by default. Make sure to *unselect* ClusterXL from the list of Check Point products. Also, *unselect* VPN if it is not used.
- While defining the gateway cluster for the NSF in Check Point SmartDashboard, the "3rd Party Configuration" in the gateway cluster properties should be configured as follows:
    - Cluster Operation Mode: Load Sharing (mandatory)
    - 3rd Party Solution: OPSEC (mandatory)
    - Support non-sticky connections: Yes (mandatory)
    - Hide Cluster Members' outgoing traffic behind Cluster's IP Address: No
    - Forward Cluster's incoming traffic to Cluster Members' IP Address: No
    - Configure the Check Point synchronization interface in the topology page. This configuration used to be under "Synchronization" tab in "Gateway Cluster Properties" window for R54 and R55.

6.5 Bugs Fixed Since 4.1.1 Release

No bug fixes added

7 Nortel Switched Firewall, 4.1.2.1 (07/07/2006)

7.1 Supported Hardware Platforms

NSF 4.1.2.1 supports the following hardware platforms:

- NSF 6414 (6400 accelerator with 5014 director)
- NSF 6614 (6600 accelerator with 5014 director)
- NSF 6424 (6400 accelerator with 5024 director)
- NSF 6624 (6600 accelerator with 5024 director)
- NSF 6416 (6400 accelerator with 5016 director)
- NSF 6616 (6600 accelerator with 5016 director)
- NSF 6426 (6400 accelerator with 5026 director)
- NSF 6626 (6600 accelerator with 5026 director)

7.2 Supported Check Point Releases

NSF 4.1.2.1 supports the following Check Point versions:

- Check Point NGX (R61)

7.3 What's New

There is no new feature added in 4.1.2.1

7.4 Bugs Fixed Since 4.1.2 Release

No bug fixes added

8 Nortel Switched Firewall, 4.1.3 (08/28/2006)

8.1 Supported Hardware Platforms

NSF 4.1.3 supports the following hardware platforms:

- NSF 6414 (6400 accelerator with 5014 director)
- NSF 6614 (6600 accelerator with 5014 director)
- NSF 6424 (6400 accelerator with 5024 director)
- NSF 6624 (6600 accelerator with 5024 director)
- NSF 6416 (6400 accelerator with 5016 director)
- NSF 6616 (6600 accelerator with 5016 director)
- NSF 6426 (6400 accelerator with 5026 director)
- NSF 6626 (6600 accelerator with 5026 director)

8.2 Supported Check Point Releases

NSF 4.1.3 supports the following Check Point versions:

- Check Point NG with Application Intelligence R55 with HFA18
- Check Point NGX R60 with HFA-03
- Check Point NGX R61

8.3 What's New

The following new features are supported in this release:

8.3.1 CPU Usage

This feature provides a solution to view the average CPU usage using the CLI command "/info/clu". It computes the average CPU usage over a time period of 5 minutes collecting samples for each 30 seconds. The CPU Alarms which appeared during momentary peak CPU usage has also been corrected with this feature.

8.3.2 kept_conns

New CLI command requested for displaying SFD kept connections in AIM table and AIM accelerated connections. When the CLI command /maint/debug/aim/kept_conns is executed, a list of AIM accelerated and SFD kept connections are displayed from the AIM table.

8.3.3 WebUI Ticker Data Saving Functionality

The data saving functionality in NSF Ticker allows the user to save the cluster, host and accelerator data into text files. This functionality is enabled by default. The data is saved in text files under the users' home directory.

8.4 Bugs Fixed Since 4.1.2.1 Release

- Health Check Daemon and Config Daemon may not work properly after 248 days of uptime (Q01106902-03)
- NSF/BBI or Web UI based port configuration is causing BBI problems (Q01418950)
- Web Server did not work when adding new port or new filter (Q01334782)
- WEBUI TICKER: Not able to view history while running ticker for more than 10 days (Q01373575)
- WEBUI ticker : Throughput In and Out shown in Ebps when we do fail over (Q01329143)
- ISDLB : Switch reboots when we use /cfg/slb/isdfw/isd_no command in GOD mode (Q01104528)
- mond.log file is not getting rotated when we run the system more than 10 days (Q01338744)
- New HFAs are missing for R55 & R60 (Q01410552)
- Unable to add Proxy ARP (Q01311541-01)
- oper group permissions (Q00910450-01)
- Validation should give error/warning msg when we delete the 10.10.1.0 from accesslist (Q01317877)
- SFD always get panic when installing R60 HFA-03 with kdb mode on (Q01340625)
- HFA is not getting upgraded during software from 4.1.1.0_R55 to 4.1.2_R55 (Q01338725)
- JOIN fails when we try to add a member with 16 bit mask (Q01338741)
- Not able to bring up copper gig port when we disable auto negotiation in 6600 (Q01095463)
- NSF 6600 / 4.1.1 / RSA sdconf.rec file is deleted from /var/ace after reboot (Q01408009)
- SFD cannot detect SFA after disabling jumbo frame and enabling trunking (Q01161524)
- Command /opt/tng/bin/lb is not giving the expected output (Q01245413-01)
- Hard disk space (/config) usage goes more than 70% after the upgrade (Q01351923)
- CLI: Request to have an info cmd to view the CPU usage over a period of time (Q01329192)
- SSI Restarting (Q01266907)

9 Nortel Switched Firewall, 4.1.3.1 (09/08/2006)

9.1 Supported Hardware Platforms

NSF 4.1.3.1 supports the following hardware platforms:

- NSF 6414 (6400 accelerator with 5014 director)
- NSF 6614 (6600 accelerator with 5014 director)
- NSF 6424 (6400 accelerator with 5024 director)
- NSF 6624 (6600 accelerator with 5024 director)
- NSF 6416 (6400 accelerator with 5016 director)
- NSF 6616 (6600 accelerator with 5016 director)
- NSF 6426 (6400 accelerator with 5026 director)
- NSF 6626 (6600 accelerator with 5026 director)

9.2 Supported Check Point Releases

NSF 4.1.3.1 supports the following Check Point versions:

- Check Point NG with Application Intelligence R55 with HFA18
- Check Point NGX R60 with HFA-03
- Check Point NGX R61

9.3 What's New

There is no new feature added in 4.1.3.1

9.4 Bugs Fixed Since 4.1.3 Release

- `IDSLB: Not able to set IDSLB group as 0 (to disable monitoring) on a particular VLAN. (Q01448475)`
- `IDSLB:  IDS load balancing on NSF High Availability setup causes network loop. (Q01435035)`

10 Nortel Switched Firewall, 4.1.3.4 (12/11/2006)

10.1 Supported Hardware Platforms

NSF 4.1.3.4 supports the following hardware platforms:

- NSF 6414 (6400 accelerator with 5014 director)
- NSF 6614 (6600 accelerator with 5014 director)
- NSF 6424 (6400 accelerator with 5024 director)
- NSF 6624 (6600 accelerator with 5024 director)
- NSF 6416 (6400 accelerator with 5016 director)
- NSF 6616 (6600 accelerator with 5016 director)
- NSF 6426 (6400 accelerator with 5026 director)
- NSF 6626 (6600 accelerator with 5026 director)

10.2 Supported Check Point Releases

NSF 4.1.3.4 supports the following Check Point versions:

- Check Point VPN-1 <TM> & Firewall-1 <R> NGX (R62) – Build 120

10.3 What's New

There is no new feature added in 4.1.3.4

10.4 Bugs Fixed Since 4.1.3.1 Release

No bug fixes added

11 Nortel Switched Firewall, 4.1.4 (04/30/2007)

11.1 Notes on Newly Supported Features

The following features are added in this release.

11.1.1 SecurID

This is a new feature added for supporting SecurID authentication for SSH login to the NSF firewalls.

From 4.1.4 release onwards, logging in to the NSF CLI via SSH can be authenticated via the SecurID mechanism. In other words, whenever the user tries to login to the NSF CLI via the SSH, first the name username would be prompted. After this, instead of a regular password, a pass code needs to be entered. An ACE Agent, which is running on the NSF, would then send the login credentials to an ACE Server. After the successful authentication from the ACE server, the user would be logged in.

11.1.2 Mechanism for installing Checkpoint HFA's on NSF

A new CLI command, /boot/software/hfainstall, is added in release 4.1.4. This command provides an easy method for users to install Check Point HFAs on NSF from the admin CLI.

Executing this command from any SFD automatically installs the HFA on all cluster members.

11.1.3 Checkpoint R65

Release 4.1.4 supports Check Point NGX R65, version VPN-1(TM) & FireWall-1 (R) NGX (R65) – Build 427.

NGX R65 includes expanded intelligent inspection technologies in *VPN-1 Power and incorporates additional complex application support into state of the art stateful-inspection and application intelligence technology.

11.1.4 CLI command to enable/disable TCP sequence verification

If standard copper ports are used as NAAP ports, the SFA will add TCP sequence information to the normal frame, which may cause the frame size to cross 1500 bytes (jumbo frames) if the normal frame size is close to 1500 bytes. This makes the SFA to drop the frame without forwarding to SFD. In order to make the SFA send the jumbo frame to the SFD, TCP Sequence Verification should be disabled. Once disabled, the SFA will not add the TCP sequence information to the frame. In order to disable/enable TCP Sequence verification, CLI support has been added.

"/maint/diag/tcpseq" menu will enable and disable the TCP Sequence verification. This CLI menu also provides the warning message to the user to enable/disable the TCP Sequence verification on Check Point Management server. If the TCP Sequence verification option is enabled/disabled on the CLI, it should also be enabled/disabled on the Checkpoint management station. Ideally speaking, the TCP sequence verification option should be the same on the firewall and the checkpoint management station

11.2 Bugs Fixed Since 4.1.3.4 Release

- Sync port down/up whenever accelerator is reconfigured (CR Q01451288)
- Cable unplugged on GBICs doesn't failover (CR Q01460485)
- IAP failure creates 2 MIPs in a cluster (CR Q01535310)
- cfgd crashes after installing HFA_04 (both 4.1.3 and 3.5.7 builds)
- (CR Q01441056)
- ASF prefers def gw advertised through ospf over def gw configured statically
- (CR Q01488650)
- Accelerator is getting panic when we give –ive value for port statistics from ISD (Q01525481)

- Not able to install ASF image on NE isd with 160 GB HDD (CR Q01530663)
- SIC reset is needed after upgrade from 4.1.2 R60 to 4.1.3 R60 (CR Q01540529)
- CLI command to enable/disable TCP sequence verification (CR Q01587914)
- Firewall leaking nonIP packets when IDSLB is enabled (CR Q01456570)
- ASF6614 4.1.3/R60 - CheckPoint VPN is failing following HA failover
- (CR Q01469207)
- Websense UFP filtering stops due to lack of ports (CR Q01539020)

12 Nortel Switched Firewall 6000 Series, 4.1.5 (09/14/2007)

12.1 Notes on Newly Supported Features

The following features are added in this release.

12.1.1 Job Scheduling (Auto Backup Feature)

Nortel switched Firewalls provide the CLI for taking the backup of system configuration. With the current CLI implementation, users can take the backup only at present time, but there is no provision to take the backup at a scheduled time. For example if the user wants to take the backup at midnight, or on particular date (ex: 5th of every month), there is no option to schedule these tasks except for the user to execute the CLI command at the desired time.

To overcome this problem, a new feature called schedule backup is provided in 4.1.5 release, which lets the user schedule the backup any time he/she intends. User can backup the configuration to a remote server using the new CLI interface (/maint/schedule) and then restore the configuration back using the ‘restore’ command. The configuration file name that will be stored in the remote host would be of 'filename_isd ip_ddmmyyyy.tar' format. For example if the file name is ‘test’ then the final file name would be ‘test_10.10.1.1_16Jul2007.tar’.

This feature is supported only from CLI. There is no edit option to change the existing jobs configuration. The only option for the user is to delete and add a new job.

12.1.2 VPN CP ACC4 Driver for Broadcom's BCM5823 Card with ROHS compliance

Previously, the VPN acceleration in the 5026 was provided by the Broadcom ‘BCM5822’. Broadcom discontinued the manufacture of this card recently and replaced it with a newer model. The Broadcom VPN accelerator card ‘BCM5823’ has replaced the BCM5822 in newer models of the 5026.

The new card has slight modifications to the driver software and uses CPacc4 drivers. These drivers have

been added to version 4.1.5 of the software such that 4.1.5 supports both the older and newer versions of the VPN accelerator card.

12.1.3 *Supported SecurID feature in WEBUI*

In 4.1.4, SecurID support was offered only through CLI. From 4.1.5 onwards, SecurID authentication for SSH is supported from BBI as well. Please refer to the SecurID_NSF_BBI user guide in the Nortel Site for more information

12.2 Bugs Fixed Since 4.1.4 Release

- cfgd is getting crashed while resetting the switch when jumbo is enabled (Q01528223)
- Even though GOTO id greater than filter id, apply is successful (Q01511878)
- GRE tunnel not operational when name exceeds 15 characters (Q01499951)
- NSF Telnet not working on newly joined SFD when telnet is enabled (Q01616071)
- Fatal error message displayed on screen when ssh is enabled for the first time (Q01562278)
- Unable to join the new SFD in the cluster, after enabling sync in the existing SFD (Q01557635)
- "/maint/tsdump/export" gets error if password contains "||" or a space (Q01342026)
- Wrong CLI display for idle timeout value (Q01508294)
- Dumping Accelerators ARP table via SNMP (Q01137863-01)
- /info/traffic displays wrong information after adding 3rd director (Q01570767)
- /info/sensor gives incorrect output (Q01488250)
- SNMP queries to firewall are returned with different source address or times out (Q01679013)
- Unable to add more than 1500 proxy ARP entries (Q01526868)
- Accelerator '/i/slb/sess/help' description is incorrect (Q01468701)
- /i/clu displays error when the NSF cluster is idle for 1 or more weeks (Q01049739)
- Auto Back-up feature on NSF products (Q01531319)
- NSF 4.1.x: Latency issues due to SP route cache filling up the ARP table (Q01619202)
- Hitless upgrade process should ask user to reset sic and push policy (Q01687153)
- /info/capability displays incorrect Accelerator and AIM connections (Q01667113)

- Adding additional entry in IPACL makes Acceleration OFF (Q01691888)
- Accelerator fails to configure when a filter is associated to a port (Q01691624)
- Invalid session table remains after SFA failover (Q01692551)
- WEBUI: Accelerator display is not shown properly when we replace one accelerator (Q01450312)
- SSI Error is reported during join when SYNC is enabled prior to join (Q01616110)

13 Appendix A: List of Known Issues

This Appendix provides detailed explanation on all the issues found and/or fixed in 4.1.x releases. The following information is provided for each issue:

- Last update date
- Affected releases
- Current status
- Description of the problem
- Description of the work around or fix, if available

Issues Updated on 09/14/2007

cfgd is getting crashed while resetting the switch when jumbo is enabled

CR # Q01528223
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

Since the SSI was not operational, the registry was not initialized. After the fix, cfgd does not crash while resetting the switch when jumbo is enabled

Even though GOTO id greater than filter id, apply is successful

CR # Q01511878
Last Updated: 08/31/2007
Affected Releases: 4.1.x

Current Status: Closed

GOTO ID should be larger than the Filter ID. The current code works as per design. The NSF user guide which has the incorrect description as “Filter ID must be larger than the ID of the GOTO filter” has been corrected to “GOTO filter must be larger than the defined Filter ID”

GRE tunnel not operational when name exceeds 15 characters

CR # Q01499951
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

A Validation has been added in such a way that the user should specify the name for gre tunnel with a minimum length of 2 and a maximum length of 15. An error message would be displayed if the length is less than 2 (<2) or greater than 15 (>15) characters.

NSF Telnet not working on newly joined SFD when telnet is enabled

CR # Q01616071
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

When a new cluster is formed and telnet is enabled before the second SFD joins, telnet will be disabled on the second director. This is because the telnet daemon status was not set during fresh boot and join. This is fixed in 4.1.5 now.

Fatal error message displayed on screen when ssh is enabled for the first time

CR # Q01562278
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

After enabling SSH using ‘/cfg/sys/adm/ssh/ena’ command, the log message stating "fatal: cannot bind any address" appears on the CLI of both the ISDs. However the isd is accessible through ssh from the attached network client PCs. In 4.1.5, fix has been made to handle the ssh state during bootup, join and CLI modification.

Unable to join the new SFD in the cluster, after enabling sync in the existing SFD

CR # Q01557635
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

New SFD is not joining the cluster (cluster with 1 SFD and 2 SFA), after enabling sync in the existing SFD. While the ISD is joining the cluster, a new node entry is created in registry. Initially this entry contains empty values by default. So the sync device name value of a new node would be blank (empty string) at the time of ISD JOIN. Therefore it gives validation error and this prevents the new ISD to join a cluster.

The Sync device name validation should not be done during "Join" and this is taken care in 4.1.5, so that we can avoid the validation error thereby solving the ISD JOIN issue when sync is enabled.

/maint/tsdump/export gets error if password contains '||' or a space

CR # Q01342026
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

When exporting a tsdump file, if the password of FTP server contains two pipe symbols "||" or a space, this command will get an error and fails to upload the tsdump. This is because the logupload script reads the password argument wrongly (if password contains more than a word or special characters) from clicbd. This is fixed in 4.1.5

Wrong CLI display for idle timeout value

CR # Q01508294
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

'/cfg/sys/adm/idle' command was accepting the idle timeout value greater than 3600 even though the CLI display was 300-3600. This is because of the wrong CLI display, which has been changed to reflect the correct range (300-604800) in 4.1.5

Dumping Accelerators ARP table via SNMP

CR # Q01137863-01
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

SNMP MIB walk displayed the ARP entries only from a single accelerator in a cluster. This fix helps us to retrieve ARP table of both the accelerators in a cluster.

/info/traffic displays wrong information after adding 3rd director

CR # Q01570767
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

In a cluster with two or more directors when one director is powered down and a new one is added, Information from '/info/traffic' and '/info/clu' are dissimilar. The director which was shown 'down' from 'info/clu' is being shown as having connections from 'info/traffic'. After the fix in 4.1.5, '/info/traffic' and '/info/clu' are displaying the correct information

/info/sensor gives incorrect output

CR # Q01488250
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

The CLI command '/info/sensor' displays incorrect values for features like CPU temperature, Board temperature, RPM of Fan, etc.,. This is fixed in 4.1.5

SNMP queries to firewall are returned with different source address or times out

CR # Q01679013
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

When we make snmp queries to the firewall, the responses sent by the firewall have a different source address. The source ip address of snmp response are based on the 'cfg/sys/snmp/adv/trapsrcip'

configuration. In 4.1.5, the code has been modified in such a way that the trapscrip settings reflect only on the trap source ip address. The get response retains the interface ip address.

Unable to add more than 1500 proxy ARP entries

CR # Q01526868
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

When we add more than 1500 proxy ARP entries, the accelerators are not getting detected. '/info/det' shows the accelerators status as configuration failed. After the fix in 4.1.5, accelerators are detected properly and '/info/det' shows the correct output with more than 1500 proxy ARP entries

Accelerator '/i/slb/sess/help' description is incorrect

CR # Q01468701
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

The accelerator CLI command '/info/slb/sess/help' was showing incorrect information. This has been modified to reflect the correct accelerator session information

/i/clu displays error when the NSF cluster is idle for 1 or more weeks

CR # Q01049739
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

'/info/clu' error is caused because the Socket connection between SSI and CLICBD times out when some CLI command is executed after a week of idle time. The ssi_proto_server file is modified by the SSI team and the fix is part of 4.1.5 now

Auto Back-up feature on NSF products

CR # Q01531319
Last Updated: 08/31/2007

Affected Releases: 4.1.x
Current Status: Closed

At present, if the user wants to take config backup at midnight, user has to wait till that time and take the config backup; there is no provision to schedule the job. To overcome this problem, a new CLI has been added to schedule the jobs based on date, time, month etc. For more information please refer to the Job Scheduling Feature (section 12.1.1)

NSF 4.1.x: Latency issues due to SP route cache filling up the ARP table

CR # Q01619202
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

NSF 66xx and 64xx series have 8192 ARP entries limit per SP. In some heavily utilized networks, the ARP cache might fill-up to the maximum limit because of internet addresses being cached for SP route cache lookup. Whenever, a client/server traffic (typically tcp) is hashed to the SP where the ARP cache is full, users experience latency issue.

As a fix, a new CLI command '/c/acc/rtcache' has been added, which is enabled by default. When disabled, the SP will not cache sp routes in the IP_FDB, it will rely only on the SP route prefix table. This will help customers who fill the IP_FDB, which causes connectivity issues.

Hitless upgrade process should ask user to reset sic and push policy

CR # Q01687153
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

The messages that are prompted on the console during the hitless upgrade process are not descriptive enough to tell the user that he/she must reestablish sic, unload the policy from the firewall director and push the policy from the Checkpoint management server. This cosmetic change is addressed in 4.1.5. Please refer to the Hitless Upgrade section for more information

No options in filter to fix the maximum length of ip packet

CR # Q01512725
Last Updated: 08/31/2007

Affected Releases: 4.1.x
Current Status: No Fix Planned

The command '/cfg/net/adv/filt' does not have any option to fix the maximum length of the ip packet. Since the current switch design and implementation only supports the limited number of filter options, there is no plan to fix this CR

/info/capability displays incorrect Accelerator and AIM connections

CR # Q01667113
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

The Output of the command '/info/capability' displays the Accelerator Connections as 500000 wrongly. After the fix in 4.1.5, the Accelerator connections are displaying the correct value as 750000

Also if we change the AIM connections using '/cfg/fw/sxl/conns', the changed value will be reflected only after reboot. As a fix, a warning message has been added stating that the user needs to reboot the ISD's to get the modified AIM value.

Adding additional entry in IPACL makes Acceleration OFF

CR # Q01691888
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

Adding a second entry in IPACL makes Acceleration OFF. The fix has been made and the acceleration status is fine with adding additional entries in IPACL

Accelerator fails to configure when a filter is associated to a port

CR # Q01691624
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

When a filter is added to a port from the ISD, accelerator fails to configure the newly added filter to the

port and goes to NOT ACCELERATING state. This is fixed in 4.1.5

Invalid session table remains after SFA failover

CR # Q01692551
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

When the Master Accelerator is powered off, the ISD's sessions present in the master accelerator are not rebinded to the reachable ISDs. These sessions are found pointing to the original ISD though it is unreachable.

According to the normal behaviour, if any ISD goes down, 'ISD del' would be called which rebinds deleted ISD's sessions with another reachable ISD. 'ISD del' is not being called in the above scenario.

This issue occurs only with ICMP connections where all the packets traverse the firewall.

As a fix, all unreachable ISDs are deleted thereby rebinding the sessions to the reachable ISD when a switch failover happens

WEBUI: Accelerator display is not shown properly when we replace one accelerator

CR # Q01450312
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

When we replace an SFA with another, an error message "Unable to get Accelerators" is displayed on the system page of BBI. As a side effect, Ticker launch fails. After the fix in 4.1.5, the error message is not displayed and the ticker is launched properly

SSI Error is reported during join when SYNC is enabled prior to join

CR # Q01616110
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

New SFD is not joining the cluster (cluster with 1 SFD and 2 SFA), after enabling sync in the existing SFD. While the ISD is joining the cluster, a new node entry is created in registry. Initially this entry contains empty values by default. So the sync device name value of a new node would be blank (empty string) at the time of ISD JOIN. Therefore it gives validation error and this prevents the new ISD to join a cluster.

The Sync device name validation should not be done during "Join" and this is taken care in 4.1.5, so that we can avoid the validation error thereby solving the ISD JOIN issue when sync is enabled.

Radius configuration locks root user out of firewall

CR # Q01451314
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

This behavior is as designed and is documented in the firewall User's guide. Radius fallback is enabled by default, if it is disabled, then the firewall will not allow local authentication if radius authentication is not available. This is addressed in release 4.1.4 and higher so that if radius fallback is disabled, the following warning will be displayed on the console when the configuration is applied notifying the administrator of potentially being locked out of the firewall.

WARNING
Fallback is disabled. If Radius server is not reachable, login to the firewall may not be possible.

If the firewall cannot be administered due to this issue, the firewall can be re-imaged and re-configured using the firewall software iso cd image.

Panic on Accelerator after ASF power off

CR # Q01425452
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

When ASF running 4.1.2_R55 was powered OFF for some time and brought back up, it was found that there was no traffic flow. The problem seemed to disappear when the backup accelerator became master on rebooting the master accelerator. On analyzing the problem it was found that lot of panics happened on the accelerator.

The reason for panic was due to the memory allocation failure for ping process. This is already fixed in 4.1.4

Unable to push the policy in R55 with HFA_20

CR # Q01685554
Last Updated: 09/07/2007
Affected Releases: 4.1.x
Current Status: Open

After installing HFA 20 on a 4.1.3.0c R55 setup, configure the accelerator and interfaces and then push the policy. The policy push is successful since the isd has initial policy. But once we remove the policy from the isd by issuing "fw unloadlocal" and push the policy from the CP management server, it fails.

Even though it shows as policy installation failed in CP, we can still see the standard policy installed on the isd by executing 'fw stat' command.

Backup/Restore Fails for different CP Versions

CR # Q01742602
Last Updated: 09/07/2007
Affected Releases: 4.1.x
Current Status: Open

When configuration backup is taken using '/maint/backup' command from the firewall with one CP version (for example R60), cloning the firewall using the R60 backup file is not successful after re-imaging the firewall with different CP version (for example R65)

TCP connections which use TCP window scaling option stall intermittently

CR # Q01612783
Last Updated: 09/12/2007
Affected Releases: 4.1.x
Current Status: Open

TCP connections which use TCP window scaling option, as described in RFC 1323, stall intermittently when the session is established through Nortel Switched Firewall running version 4.1.1 / 4.1.2 R55. Problem has been seen with TCP connections originating from LINUX and Windows VISTA clients.

As a workaround 'TCP sequence verification' option can be disabled on the firewall to get rid of the problem.

Issues Updated on 04/30/2007

ISSUES WITH SYNC OVER VNIC:

Although NSF supports "Sync over VNIC" configuration, please note that for better performance it is always recommended to use a dedicated SFD port for Check Point state synchronization.

The Sync may be affected when there is heavy traffic. Under stress it may lead to memory leak and high CPU usage.

Single fiber link failure of IAP does not fail over to copper

CR # Q01520395
Last Updated: 04/30/2007
Affected Releases: 4.1.x
Current Status: Open

When a single Rx or Tx fiber is disconnected, the fiber link is reported DOWN by both the accelerators, but the copper link does not come UP. When both Rx & Tx fibers are disconnected, then the copper port becomes active.

This is a hardware limitation and switch architecture will not fail-over to the backup copper port when only a single fiber link is down.

Some packets are dropped while a checkpoint policy is pushed to the firewall

CR # Q01540553
Last Updated: 09/12/2007
Affected Releases: 4.1.x
Current Status: Open

While pushing a policy to the firewall, some packets are getting dropped. The packet drops causes an interruption in established connections/sessions that are going through the firewall. These connections must be re-established after the policy push.

As a work around, it's suggested to configure the policy settings during the maintenance window so that the failure can be minimized. Also, disabling TCP sequence verification seems to solve the issue.

Output displayed by /info/acc and /info/det commands is not consistent

CR # Q01575439
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

The output of the commands '/info/acc' and '/info/det' are not consistent from time to time. The IP address and SFA-MAC relation is NOT the same in the output of these commands. The issue happens on any type of accelerator model. This is only a display problem and it doesn't have any impact on the actual operation of the firewalls.

After the fix in 4.1.5, '/info/acc' and '/info/det' are displaying the correct output

Sync port down/up whenever accelerator is reconfigured

CR # Q01451288
Last Updated: 04/30/2007
Affected Releases: 4.1.x
Fixed in Release: 4.1.4
Current Status: Closed

Whenever an accelerator was reconfigured, the sync interface link goes down and comes up again.
In 4.1.4, the configuration daemon has been modified which checks if there's any sync configuration changes. Only then, the sync device is brought down and made up again.

Cable unplugged on GBICs doesn't failover

CR # Q01460485
Last Updated: 04/30/2007
Affected Releases: 4.1.x
Fixed in Release: 4.1.2
Current Status: Closed

When /info/link command was run from the backup accelerator, it shows the status of the primary's ports only. So when a port goes down, or is disconnected from the backup - /info/link does not show this link state change - even when directly connected to the backup. Also, no SNMP trap is generated for this event (backup accel link state change).

This issue was happening when the autoneg is set to 'off' on dual ports fiber link.

The underlying switch architecture doesn't support autoneg off settings on the dual ports fiber link. A validation function is added to prevent the user from disabling the autoneg and the problem is no longer seen.

IAP failure creates 2 MIPs in a cluster

CR # Q01535310
Last Updated: 04/30/2007
Affected Releases: 4.1.x
Current Status: Closed

In a specific cluster topology of 3 or more directors, two ore more directors connected to the backup accelerator, the IAP link failure was causing the cluster to be split into two.
Each cluster then elected a MIP and this causes OSPF daemon to run on both the directors.

In 4.1.4, a validation has been added to prevent the directors to become MIP if the accelerator connected to it is a backup. Hence only the Director that's connected to the master accelerator becomes the MIP and the other directors connected to the backup accelerators continue to be non-MIP.

cfgd crashes after installing HFA_04 (both 4.1.3 and 3.5.7 builds)

CR # Q01441056
Last Updated: 04/30/2007
Affected Releases: 4.1.x
Fixed in Release: 4.1.3
Current Status: Closed

After installing the HFA_04 and rebooting the Firewall, the cfg daemon was not running. Health check daemon tries to restart the cfg daemon but cfgd keeps crashing.

The issue was happening due to the less disk space allocated to the /config partition where all Check Point related configuration is stored.

The issue is fixed in 4.1.4 in the following method:

- Changed the /config partition size to 2GB, which is sufficient for the Check Point configuration in 4.1.4
- Check Point's "var-opt" directory moved from /config partition to /logs after confirming enough disk space on /logs
- The script will check whether we have sufficient disk space on var-opt directory before installing any HFAs

ASF prefers default gateway advertised through ospf over default gateway configured statically

CR # Q01488650
Last Updated: 04/30/2007
Affected Releases: 4.1.x

Fixed in Release: 4.1.4
Current Status: Closed

In a typical routing configuration where a default gateway is configured on the NSF CLI and also another default gateway learned through an external OSPF router, preference was given to the default route learned through OSPF.

Modified the routing code in 4.1.4 after which the statically configured gateway is given precedence over OSPF default route.

Entering negative port number for checking the port statistics causes the accelerator panic

CR # Q01525481
Last Updated: 04/30/2007
Affected Releases: 4.1.x
Fixed in Release: 4.1.4
Current Status: Closed

From the Firewall console, running the "/maint/debug/ac1/prtstat/stat -1" command caused the accelerator panic.

A validation check for the port number input has been added in 4.1.4 before trying to read the port statistics.

Not able to install iso image on NSF 6000 NE models with 160 GB HDD

CR # Q01530663
Last Updated: 04/30/2007
Affected Releases: 4.1.x
Fixed in Release: 4.1.4
Current Status: Closed

Installation fails when installing NSF600 iso image on NE models with 160 GB HDD. The latest NSF6000 NE models are shipped with 160GB HDD compared to 80GB HDD earlier. During installation process, necessary partitions are created and formatted. But all the previous install scripts are tuned to support 80GB HDD only. But with the increase in the HDD size, the installation times out while formatting the newly created partitions.

To address this issue, during the install process, the idle check daemon which handles the session time out is stopped. Also, since the installation can take longer time, a progress bar is added to the install script to indicate the installation status.

If you're running pre-4.1.4 release and would like to upgrade to 4.1.4, then this issue is not applicable. The happened only when the users try to re-install the software image on the box with 160GB HDD.

To verify whether your hardware has 160GB HDD and needs a re-install of image, please refer to the NSF6000 series firewall Release notes version 4.1.4.

Fore more information, please refer to the NSF6000 series firewalls customer support bulletin ID: 2007007922, Rev 1.

SIC reset is needed after upgrade from 4.1.2 R60 to 4.1.3 R60

CR # Q01540529
Last Updated: 04/30/2007
Affected Releases: 4.1.x
Current Status: No fix planned

When upgrade from 4.1.2 R60 to 4.1.x R60, its required to re-establish the trust with the Check Point SmartCenter server (or in other terms, reset SIC operation needs to be performed).

This is a design limitation in the way Check Point daemons are installed on the Firewall and it always require a reset SIC after upgrade.

A feature limitation document on this issue is written. Please contact Nortel technical support for a copy of this document.

No special character support for login password

CR # Q01460968
Last Updated: 04/30/2007
Affected Releases: 4.1.x
Current Status: Open

Configuring special characters like "$" for login password is not supported. The password settings are only restricted to support alpha-numeric characters only.

CLI command to enable/disable TCP sequence verification

CR # Q01587914
Last Updated: 04/30/2007
Affected Releases: 4.1.x
Fixed in Release: 4.1.4

Current Status: Closed

With TCP Sequence verification configuration enabled on the SFD, once the session is established on the Firewall and the information is sent to the accelerator, the sequence verification would be handled by the accelerator device directly.

However, enabling the TCP sequence verification adds an extra 24 bytes of header information to the frame. This exceeds the maximum frame size supported by the underlying switch ports. Hence the traffic coming on non-jumbo capable ports (ports 1-8 on 6600 SFA and ports 1-24 on 6400 SFA) would be dropped.

A new CLI command "/maint/debug/tcpseq/" is added which can enable/disable TCP sequence verification.

Please note that enabling/disabling TCP sequence verification from the CLI requires a similar configuration on the Check Point SmartDefense settings.

Backup accelerator processing nonIP multicast packets when IDSLB is enabled

CR # Q01456570
Last Updated: 04/30/2007
Affected Releases: 4.1.x
Fixed in Release: 4.1.4
Current Status: Closed

When IDSLB was enabled and non-IP multicast packets are received by the Firewall, the backup accelerator was treating the packets as unkown and flooding the packets causing a network loop. Examples for non-IP multicast traffic are Cisco's CDP & HSRP.

A validation has been added in the switch code which doesn't process unknown traffic when its acting as 'backup'.

ASF6614 4.1.3/R60 - CheckPoint VPN is failing following HA failover

CR # Q01469207
Last Updated: 03/20/2007
Affected Releases: 4.1.x
Fixed in Release: 4.1.4
Current Status: Closed

In a typical cluster topology consisting of a single SFA and multiple SFD's, when the fail-over happens, the

sessions are not re-bound properly to the available SFD. Though the CR mentions the VPN traffic, this CR is applicable for regular firewall traffic as well.

This issue was happening as the SFA will re-bound the sessions only when the accelerator status is master alone.

A fix is added in the accelerator code which handles the session re-bounding in standalone case as well.

Websense UFP filtering stops due to lack of ports

CR # Q01539020
Last Updated: 04/30/2007
Affected Releases: 4.1.x
Fixed in Release: 4.1.4
Current Status: Closed

When a new cluster is created, the local port range used for maintaining session information on the Firewall members is calculated based on the assumption that the max. no. of members in a cluster can be 255.

Hence the local port range available for each Firewall member is limited. With Websense, multiple connections are opened and the local port range can exhaust very quickly.

In 4.1.4, the local port range is divided among the cluster members based on the total count of cluster members currently configured.

Issues Updated on 12/14/2006

Firewall Director locks up after several hours because of memory leak

CR # Q01415915
Last Updated: 09/14/2007
Affected Releases: 4.1.x
Current Status: Open

SFD locks up requiring a reboot to recover because of memory leak. After booting the director, it will lock up after a few hours. This happens on 4.1.2.0_R60. This is a CP issue. This occurs when the sync is enabled in a standalone setup. The case as mentioned can happen when there is no second director.

This issue is reproducible and is currently under investigation by checkpoint.

Large Packets are getting dropped incorrectly

CR # Q01496816
Last Updated: 03/20/2007
Affected Releases: 4.1.x
Current Status: Closed. No fix planned

In 4.1.x, we have a new feature called TCP Sequence Verification, which appends additional state information to TCP packets. Since the 6600 hardware supports larger size packets only on uplink ports 9 to 12, as per the hardware architecture the best practice is to connect the SFD to SFA in ports 9-12. To support large size packets on copper ports (1-8), the TCP Sequence Verification should be disabled. You may also refer to CR Q01587914 for more information on this.

Under stress condition, After rebooting the ISD's, sync is in "error state"

CR # Q01509522
Last Updated: 12/11/2006
Affected Releases: 4.1.x
Current Status: Open

Under stress condition, after rebooting the ISD's, sync is in "error state". After pushing the policy from CP, sync state is changing into working state. Mainly the problem is occurring while rebooting the MIP holding ISDs. This problem happens for the 5016-NE1 with 6600 switch, 5010- dell ISD with 5600 switch hardwares under the stress condition.

Issues Updated on 09/08/2006

IDSLB: Not able to set IDSLB group as 0 (to disable monitoring) on a particular VLAN

CR # Q01448475
Last Updated: 09/07/2006
Affected Releases: 4.1.x
Current Status: Closed

The IDSLB configuration on the VLAN for which the IDSgroup is configured as ‘0’ or ‘none’ is not getting pushed to switch as ISD treats that Monitoring is not enabled on particular VLAN, but this has to be informed to switch as well. This is fixed now.

IDSLB: IDS load balancing on NSF High Availability setup causes network loop

CR # Q01435035
Last Updated: 09/07/2006
Affected Releases: 4.1.x
Current Status: Closed

The Backup switch processed the ARP packets coming from Master switch received via IAP and sent out, causing a loop and ARP flooding. Now, switch VRRP state is checked before processing ARP packet and hence network loop is avoided from backup switch.

Issues Updated on 08/28/2006

HEALTH CHECK DAEMON AND CONFIG DAEMON MAY NOT WORK PROPERLY AFTER 248 DAYS OF UPTIME

CR# Q01106902-03
Last Updated: 08/28/2006
Affected Releases: 4.1.x
Current Status: Closed

The time variable used for health check daemon (hcd) and config daemon (cfgd) wraps around in 248.5 days. Current processing of this variable does not take care of the wrapping and could cause problems where "/info/clu" will show old date, cfgd will not configure accelerator when the SFA is rebooted, hcd will not send health check packets, naapd will not detect the other peers.

When you run "/info/clu," if the "Health Report as of ..." field shows an old time and does not get updated, this may indicate that the problem has occurred. To verify, please login as root and run "uptime" to see if the system has been up for more than 248 days. After 248.5 days, ::times() wraparound causes general havoc for the system.

For earlier releases, the work around for this problem is only to reboot the SFDs well ahead of 248 days. The issue has now been fixed in 3.5.7 release. The jiffies wrap around case is now taken care and the system runs normally even after 248.5 days.

NSF/BBI or Web UI based port configuration is causing BBI problems

CR # Q01418950
Last Updated: 08/28/2006
Affected Releases: 4.1.x
Current Status: Closed

To update on port configuration page on BBI cause httpd to hang.
Now we have the fix in HFA_018 and hence the issue would be no longer seen.

Web Server did not work when adding new port or new filter

CR # Q01334782
Last Updated: 08/28/2006
Affected Releases: 4.1.x
Current Status: Closed

To update on port configuration page on BBI cause httpd to hang.
Now we have the fix in HFA_018 and hence the issue would be no longer seen.

WEBUI TICKER: Not able to view history while running ticker for more than 10 days

CR # Q01373575
Last Updated: 08/28/2006
Affected Release: 4.1.x
Current Status: Closed

If the user runs NSF ticker for more than 10 days, the history cannot be viewed. This issue has been fixed now.

WEBUI ticker: Throughput In and Out shown in Ebps when we do fail over

CR#Q01329143
Last Updated: 08/28/2006
Affected Release: 4.1.x
Current Status: Closed

With NSF ticker, once the fail over is initiated, the Throughput graphs display traffic in Ebps.
The issue has been fixed. Now the throughput comes down to zero at the fail over instance.

Issues Updated on 08/28/2006

SSI RESTARTING

CR# Q01266907
Last Updated: 08/28/2006

Affected Releases: 4.1.x
Current Status: Closed

The SSI service restarts intermittently and causes daemons such as clicbd, cfgd, hc to disconnect from SSI and reconnect again. The impact is when user is logged-in to CLI/BBI and restart takes place, the user CLI/BBI is terminated and user needs to connect again. The issue is fixed now.

ISDLB: Switch reboots when we use /cfg/slb/isdfw/isd_no command in GOD mode.

CR # Q01104528
Last Updated: 08/28/2006
Affected Releases: 4.1.x
Current Status: Closed

If /cfg/slb/isdfw/isd_no command was run without giving the isd number, it used to make switches reboot. Old build had this issue. Fix is already checked in. Not present in latest 4.1 build.

mond.log file is not getting rotated when we run the system more than 10 days

CR # Q01338744
Last Updated: 08/28/2006
Affected Releases: 4.1.x
Current Status: Fixed

mond.log file was not rotating when system is left running for more than 10 days which was harmful for hard disk memory

New HFAs are missing for R55 & R60

CR # Q01410552
Last Updated: 08/28/2006
Affected Releases: 4.1.x
Current Status: Closed

New HFAs, HFA-18 & HFA-03, were missing for R55 and R60 respectively. The issue has been resolved.

Unable to add Proxy ARP

CR #Q01311541-01
Last Updated: 08/28/2006
Affected Releases: 4.1.x
Current Status: Closed

User was unable to set PARP IP addresses like x.0.0.x or x.0.x.x or x.x.0.x which are valid IP format. Now user can add such type of IPs as Proxy ARP IPs.

oper group permissions

CR # Q00910450-01
Last Updated: 08/28/2006
Affected Releases: 4.1.x
Current Status: Closed

oper group had permissions to load and unload policies i.e. they could access /maint/diag/ldplcy & /maint/diag/unldplcy.

Validation should give error/warning msg when we delete the 10.10.1.0 from accesslist

CR # Q01317877
Last Updated: 08/28/2006
Affected Releases: 4.1.x
Current Status: Closed

Validation was not showing any error if any network/host was added to the access list in absence of sfd subnet but apply was showing the error. However empty list is allowed. Now the fix gives error if SFD subnet (10.10.1.0) or any of its subsuming nets (10.0.0.0 or 10.10.0.0) is missing and any other net/host is added to access list

SFD always get panic when installing R60 HFA-03 with kdb mode on

CR# Q01340625
Last Updated: 08/28/2006
Affected Release: 4.1.3
Current Status: Closed

This problem arises when we upgrade HFA-03 package manually on SFD for checkpoint R60. Now our forthcoming build has HFA-03 as inbuilt. So there is no need to separately install.

SFD always get panic when installing new HFA version with kdb mode on

CR# Q01340625-01
Last Updated: 08/28/2006
Affected Release: 4.1.3
Current Status: Open

This problem arises when we upgrade HFA package manually on SFD. With the kdb mode on, the SFD is getting panic when new HFA versions are installed.

HFA is not getting upgraded during software from 4.1.1.0_R55 to 4.1.2_R55

CR# Q01338725
Last Updated: 08/28/2006
Affected Release: 4.1.3
Current Status: Closed

HFA is not getting upgraded, after upgradation of the same checkpoint version. The reason behind is, cfgd restores the backup configuration after the upgrade, which overrides the latest upgraded hfa with old one. Now while upgrading process we took the backup of "/var/opt" directory before restoring the backup configuration. The backup of "/var/opt" directory contains latest upgraded hfa and it can be restored after it restored the backup checkpoint configuration.

JOIN fails when we try to add a member with 16-bit mask

CR# Q01338741
Last Updated: 08/28/2006
Affected Releases: 4.1.x
Current Status: Closed

A new cli is added to receive net mask as part of join.

Not able to bring up copper gig port when we disable auto negotiation in 6600

CR# Q01095463
Last Updated: 08/28/2006
Affected Releases: 4.1.x
Current Status: Closed

Added validation code for ports 9-12 in 6600

NSF 6600 / 4.1.1 / RSA sdconf.rec file is deleted from /var/ace after reboot

CR# Q01408009
Last Updated: 08/28/2006
Affected Releases: 4.1.x

Current Status: Closed

The secureid file "sdconf.rec" is deleted from the /var/ace directory. This happens when the SFD hardware is "NE". In this case the file could not be properly imported since the floppy drive is not available. As a fix we now allow the file to imported locally via, floppy, USB and also remotely via ftp, ssh, tftp and scp. Validation handles the configuration of these file transfer modes based on the hardware.

SFD cannot detect SFA after disabling jumbo frame and enabling trunking

CR# Q01161524
Last Updated: 08/28/2006
Affected Releases: 4.1.3
Current Status: Closed

The communication between SFD and SFA is lost when we try to enable a disabled non-gig port, which was part of Jumbo vlan then. The cfgd is not able to apply the switch configuration as the jumbo configurations are sent last to SFA.

The default Jumbo configuration is sent to the SFA ahead of port/vlan configuration to resolve this.

Command /opt/tng/bin/lb is not giving the expected output

CR #Q01245413-01
Last Updated: 08/28/2006
Affected Releases: 4.1.x
Current Status: Fixed

There was a problem in the lb script which was wrongly reading /info/naap/dump output at switch end.

4.1.1 drops packets that arrive out of order

CR # Q01231858
Last Updated: 08/28/2006
Affected Releases: 4.1.x
Current Status: Open

When packets arrive out of order, the switch was found to drop those. This created issues with browsing certain websites.

Workaround 1: Disabling acceleration will allow traffic to pass.

Workaround 2: Disable TCP Sequence Verification on the NSF.
This can be done as follows:

Login as root
a. Go to 'vi /opt/tng/conf/config'
b. Uncomment the second line (remove the # at the beginning)
#Disable AIM from registering TCP SEQ VERIFICATION capability
#NO_TCP_SEQ_VERIFICATION=1
c. This must be done on each SFD and reboot the cluster.

Hard disk space (/config) usage goes more than 70% after the upgrade

CR # Q01351923
Last Updated: 08/28/2006
Affected Releases: 4.1.x
Current Status: Closed

/config partition on the iSD was almost filled up to 70 % with R61 upgrade. Now the partition size has been increased to 2GB to accommodate more files.

CLI : Request to have an info cmd to view the CPU usage over a period of time

CR # Q01329192
Last Updated: 08/28/2006
Affected Releases: 4.1.x
Current Status: Fixed

The /info/clu command now displays the average CPU usage over a period of 5 minutes. This is updated every 30 seconds. This also solves the issue of unncessary alarms caused due to CPU usage exceeding the limit.

ASF continuously deleting and adding default route sent by Cisco

CR # Q01445437
Last Updated: 03/20/2007
Affected Releases: 4.1.x
Current Status: Closed

When default routes are learnt via dynamic routing protocols, the ASF continuously adds and removes these routes. This also leads to excessive log messages filling up the /var directory to even 100%.. This is fixed now

oper user is able to change the password of admin user

CR # Q01427432
Last Updated: 03/20/2007

Affected Releases: 4.1.x
Current Status: Closed

Through the oper login, the user must not be able to change the password of admin user. Presently the oper user is able to change the admin user password. It denies the user to login further with the old admin password. This is fixed now and Oper user can be able to change its own password and admin password cannot be changed by Oper user

Hard disk usage calculation is wrong when we connect usb stick to the ISD

CR # Q01435023
Last Updated: 03/20/2007
Affected Releases: 4.1.x
Current Status: Closed

After mounting a usb (using usbmount command from root), the hard disk usage is shown very high from CLI. If the usb stick is 85% full, we display harddisk usage as 85, which is wrong. The problem happens only for usb. For CD there is no such wrong calculation. This is fixed now

Upgrade: Switch panic while doing hitless Upgrade from 4.1.2.0 to 4.1.3.0

CR # Q01435081
Last Updated: 08/28/2006
Affected Releases: 4.1.x
Current Status: Open

When doing a hitless upgrade from 4.1.2 to 4.1.3, the master gets upgraded successfully. While decommissioning, the back up current master switch gets a panic.

Non MIP ISD remains in passing state after the upgradation to 4.1.3_R61

CR # Q01438644
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: Closed

After downloading and activating the 4.1.3_R61 package, and pushing the policy from CP, the status of non-MIP SFD in /info/clu is seen to remain in passing state itself.

The latest code was tested and the non-MIP SFD remained in ‘accelerating’ status.

IDSLB: disable or enable IDS globally, there is a failover triggered always

CR # Q01448478
Last Updated: 08/28/2006
Affected Releases: 4.1.x
Current Status: Open

Whenever we disable or enable IDS globally, there is a failover triggered. Even when we disable and enable a group, failover is seen to occur.

/cfg/acc/det and /info/det are not showing active accelerators

CR # Q01437950
Last Updated: 09/07/2007
Affected Releases: 4.1.x
Current Status: Open

info/net/if, /info/net/port shows all the interfaces and port details and /info/clu shows firewall status as accelerating but /info/det and /cfg/acc/det shows no active accelerators are found. This was seen in both standalone and HA set up

ASF6414 - Clearing accelerator stats from the director

CR # Q01444801
Last Updated: 03/20/2007
Affected Releases: 4.1.x
Current Status: Closed

When two ASF6414 form a cluster, user is unable to clear statistics of any of the accelerators.

There are two issues.
1. ASF doesn't clear statistics value if you use "clear" CLI command on the director.
2. If there are two accelerators, accelerator2 doesn't respond to "prtstat" CLI command.

NSF 4.1.2_R60 SNMP queries, not returned

CR # Q01434591
Last Updated: 08/31/2007

Affected Releases: 4.1.x
Current Status: Closed

SNMP queries are returned with wrong IP setting because /cfg/sys/snmp/adv/trapsrcip is not working. SNMP traps and queries responses have a source IP of the interface. The configuration of /cfg/sys/snmp/adv/trapsrcip does not have any affect on the source IP. This was found to be a CP issue, which was fixed in the latest CP versions and HFA's and the fix is already a part of 4.1.5 now.

Radius user accounts on NSF

CR # Q01437363
Last Updated: 08/28/2006
Affected Releases: 4.1.x
Current Status: Open

Unable to use a RADIUS server as central database for cli logins. Customer is still required to create the user accounts manually on the firewalls. Managing the creation and deletion of users from the RADIUS server is not possible presently.

Issues Updated on 03/22/2006

PRIMARY PORT FAILING TO COPPER BACKUP FLIPS CLUSTER.

CR# Q01218241
Last Updated: 03/22/2006
Affected Releases: 4.1.1
Current Status: Closed

When the primary physical link of a port failed (fibre), the backup physical link (copper) was activated but a VRRP failover on the accelerator was triggered. By allowing enough time for port failure, vrrp failover was avoided.

SNMPD PROCESS KEEPS RESTARTING.

CR# Q01229738
Last Updated: 03/22/2006
Affected Releases: 4.1.1
Current Status: Closed

When the SSI process went down, SNMP went down and health check restarted snmpd process. The fix made the snmp daemon independent of SSI and does not go down when SSI internally restarts. The snmp

daemon service is restarted once in every week.

NTP SERVER ACCESS IS NOT RESTRICTED TO SFD SUBNET.

CR# Q01208951
Last Updated: 03/22/2006
Affected Releases: 4.1.2
Current Status: Closed

NTP server access was not restricted to SFD subnet. Technically, NTP server runs on MIP and other SFDs and accelerators access NTP server. Since iptables rule was missing, any host with access to MIP could talk to NTP and get details such as OS info, time etc. The fix was to make NTP accessible within SFD subnets and configured NTP servers.

NSF 4.1.1 REPLACING A SFA SHOWS 3 SFA'S IN /INFO/DET.

CR# Q01234723
Last Updated: 03/22/2006
Affected Releases: 4.1.2
Current Status: Closed

After replacing an accelerator, 3 SFA'a are displayed under CLI command `/info/det`. The fix was to display only detected/reachable accelerators.

UNNECESSARY/CONFUSING LOG MESSAGE RELATED TO SFD STATUS IN SINGLE SFD SETUP

CR# Q01248760
Last Updated: 03/22/2006
Affected Releases: 4.1.2
Current Status: Closed

When there is only one SFD-Accelerator (standalone) in the setup, the process which was invoked as part of determining isolation case from the cluster reported misleading information which was not appropriate for standalone setup. The fix was to check for type of cluster before writing log messages.

ACCELERATOR IS 1 HOUR AHEAD OF DIRECTORS

CR# Q01279395
Last Updated: 08/31/2007
Affected Releases: 4.1.x
Current Status: No Fix Planned

When the SFD date changes to Apr 02 2006 01:59:00 (time zone: North America), the SFD time changes to 3AM (PST) after one minute but the accelerator still shows 2AM PST.

L2 VLAN DOES NOT WORK PROPERLY

CR# Q01326194
Last Updated: 08/31/2007
Affected Releases: 4.1.2 R60, 4.1.2.1 R61
Current Status: Closed

When a vlan is configured with two ports and L2FW is enabled for the vlan, CheckPoint NGX drops traffic in the vlan. This is fixed now and the traffic passes between the two stations in the same vlan

/CFG/SYS NOT AVAILABLE TO CHANGE NAAP VLAN ID ON ACCELERATOR

CR# Q01252655
Last Updated: 03/22/2006
Affected Releases: 4.1.1
Current Status: Closed

User is unable to set NAAP VLAN id in accelerator on NSF 4.1.1 since the `/cfg/sys` menu is not available in the accelerator when logged in as 'admin' user. The issue is fixed and now user can change default NAAP vlan. The `/cfg/vlan` menu is hidden in 'admin' mode since user should not accidentally change vlans in the accelerator.

VPN SITE TO SITE DOESN'T WORK

CR# Q01284910
Last Updated: 08/31/2007
Affected Releases: 4.1.2 R60
Current Status: No Fix Planned

Both site-to-site and client-to-site VPN will not work in 4.0.4-R60 with the default management station settings. The work around to resolve this problem is described below:

1. Configure the VPN gateway object in the Check Point SmartDashboard and save the configuration. Close the management station if it is opened.
2. Open a dos window.
3. Type "`cd \program files\checkpoint\smartconsole\r60\program`". If you have installed Check Point management software in a different location, you should cd to appropriate

directory.
4. Type in "`guidbedit`" and connect to management station.
5. Hit "`Ctrl F`" (for find) and type "`reroute`" in the "Find What" box
6. Click on the "Find Next" button
7. It should take you to the "reroute_encryted_packets" in the "Field Name" column
8. Change the "Value" to false.
9. Hit "F3" and it should find the next instance of "reroute_encryted_packets"
10. Change its "Value" to false.
11. click on "File" and click on "Save All"
12. Close the guidbedit window and start it again and double check the values of "reroute_encryted_packets" are set to false.
13. Close the guidbedit window after verifying the values.
14. Start the management station and push the policy to the firewall.

In addition, if the encryption domain is NAT'ed and VPN community is used, it may be necessary to disable NAT inside the VPN community. The Disable NAT inside the VPN Community property checkbox can be toggled in the SmartDashboard (VPN Manager tab -> Community object properties -> Advanced VPN Properties tab). Disabling the reroute_encrypted_packets property for a NPV community also prevents Excluded Services within the VPN from working. The Excluded Services tab is also inside SmartDashboard (VPN Manager tab -> Community object properties).

BOGUS ERRORS ON PORTS 27 AND 28 OF THE ACCELERATOR

CR# Q01296879
Last Updated: 03/22/2006
Affected Releases: 4.1.x
Current Status: No Fix Planned

The error counters go up on ports 27 and 28 even when nothing is plugged into the ports. The error s only appears at the accelerator ports 27 & 28 and they appear only when both SFA and SFD reboot at the same time.

`/stats/port 27/clear` would clear this statistics.

NO VALIDATION CHECK TO PREVENT INVALID SUBNET MASK FOR IP ACL

CR# Q01149215
Last Updated: 03/22/2006
Affected Releases: 4.1.1
Current Status: Closed

While configuring IP ACL, 0.0.0.0 is not considered a valid subnet mask. However, there is no validation to prevent user from configuring 0.0.0.0 as a subnet mask for IP ACL entry. This invalid configuration will be rejected by the accelerator and you will see the following error under "`/info/det`".
IP subnet mask cannot be set to 0.0.0.0. The issue has been fixed now.

NSF /VAR/TMP/LOCAL_STATE FILE FILLING UP

CR# Q01335693
Last Updated: 03/22/2006
Affected Releases: 4.1.1
Current Status: Closed

When cfgd started, it created dynamic registry nodes in `/var/tmp/local_state` and the last node which was written disappeared. When cfgd tried to access it again, it caught an exception and exited. Health check restarted cfgd which triggered ACCEL OFF and ACCEL ON states on the accelerator.

The issue was the local_state file quickly filled up and the file was rotated. The rotation of the new file was the reason for exception and it was fixed.

Issues Updated on 08/23/2005

FTP SESSION FAILS WHEN TCP SEQUENCE VERIFICATION IS ENABLED

CR# Q01113493
Last Updated: 08/23/2005
Affected Releases: 4.1.1
Current Status: Closed

When TCP sequence verification is enabled in Check Point SmartDefense, the FIN packet of the FTP data session is incorrectly dropped with a Check Point log message indicating TCP sequence check failure. With some FTP clients, this will cause the FTP session to hang while the client waits indefinitely for the data connection to close.
The workaround is to turn off TCP sequence verification. Open SmartDashboard and from the SmartDefense tab, go to "Network Security | TCP" and uncheck "Sequence Verifier". Save the changes and push policy to NSF again.

Issues Updated on 07/25/2005

SYNC THRO VNIC IS NOT SUPPORTED WITH VPN

CR# Q01061470

Last Updated: 07/25/2005
Affected Releases: 4.1.x
Current Status: No Fix Planned

If VPN is selected in the cluster object properties of the NSF cluster object in Check Point SmartDashboard, you should not use "sync thro vnic" as this will cause VPN traffic to fail occasionally. Please use a dedicated port on the director for Check Point sync.

USING COPPER GBIC ON DUAL PORTS OF 6600

CR# Q01050555
Last Updated: 07/25/2005
Affected Releases: 4.1.x
Current Status: No Fix Planned

The 6600 accelerator has dual connecters for ports 3, 4, 5 and 6. You can use either copper of fiber GBICs for the GBIC slots. If you use copper GBICs, link negotiation happens between the accelerator and the GBIC causing the accelerator to consider that link as up as soon as the copper GBIC is inserted. If GBIC is configured as you preferred connector, the accelerator will switch over to the copper GBIC as soon as it is inserted even of there is no cable connected. To prevent this, you should set the GBIC port as the backup if you plan to use copper GBICs.

PROXY ARP ENTRIES ABOVE 1600 DOES NOT WORK

CR# Q01104775
Last Updated: 07/25/2005
Affected Releases: 4.1.1
Current Status: No Fix Planned

If you have more than 1600 proxy arp addresses defined, the system will not do proxy arp for entries above the first 1600.

"SOFTDOG DRIVER OPEN FAILURE" MESSAGE WHEN ACCELERATOR BOOTS UP

CR# Q01052781
Last Updated: 07/25/2005
Affected Releases: 4.1.1
Current Status: No Fix Planned

When the accelerator is booting up, you will see the above error message if you are connected to the serial console of the accelerator. The message is harmless and can be safely ignored.

PIMD RESTARTS WHEN IP ADDRESS ON PIM ENABLED INTERFACE IS CHANGED

CR# Q01094577
Last Updated: 07/25/2005
Affected Releases: 4.1.1
Current Status: No Fix Planned

If the IP address of a PIM enabled interface is changed, it will cause the pimd process to restart. This may cause disruption of multicast traffic for a few seconds.

CHANGES MADE TO ROUTEMAPS DO NOT TAKE EFFECT IMMEDIATELY

CR# Q01089358
Last Updated: 07/25/2005
Affected Releases: 4.1.1
Current Status: No Fix Planned

If more than one redistribution is enabled, changes made to routemaps do not take effect even after the changes are applied. As a workaround, please disable and enable OSPF redistributions when routemaps are updated.

ISSUES RELATED TO LARGE CONFIGURATIONS

CR# Q01142037
Last Updated: 07/25/2005
Affected Releases: 4.1.1
Current Status: No Fix Planned

If the NSF configuration is very large, the system will take a long time to apply the configuration or may fail to apply the configuration. Other symptoms include “accel off”, failing CLI commands under “`/info`” menu and high CPU usage on the director as it tries to apply the configuration. Examples of large configurations include 1500+ proxy arp addresses, 4000+ static routes and 2000+ filters.

INCORRECT UDP BLAST BEHAVIOR

CR# Q01117033
Last Updated: 07/25/2005
Affected Releases: 4.1.1
Current Status: No Fix Planned

The CLI allows user to specify multiple UDP ports and port ranges to be protected against UDP blast. However the system applies the UDP blast control to all ports that are between the lowest and highest user specified ports. For example, if you configure UDP blast protection for ports 1000 and 2000, all UDP ports between 1000 and 2000 also get UDP blast protection.

Under heavy stress, when traffic is more than 50% of gig line rate, the system is unable to enforce the configured UDP blast protection (Q01157980).

DIRECTOR RUNS OUT OF MEMORY DURING BOOTUP

CR# Q01157944
Last Updated: 03/22/2006
Affected Releases: 4.1.1
Current Status: No Fix Planned

If Check Point sync is enabled, the director tries to sync it's session table with that of the cluster members during bootup. However, if session rate is more than 4000 per second and all the sessions are being synched, the director will run out of memory trying to sync up its session table.
FW flags were added to fwkern.conf which limits memory usage for sync at startup.

DOS ATTACK TRAFFIC CAUSES HIGH MP CPU UTILIZATION ON ACCELERATOR

CR# Q01174716
Last Updated: 02/22/2006
Affected Releases: 4.1.1
Current Status: Closed

When DOS attack protection is enabled on a port, the accelerator will generate one syslog message per 128 attack packets dropped. However, if the number of attack packets is large enough, the amount of syslogs generated is enough to overwhelm the MP. Release 4.1.2 has CLI command which sets limit on logs generated per second.

ERROR MESSAGE FOR PMATCH STRING LONGER THAN 40 CHARACTERS IS NOT CLEAR

CR# Q01164785
Last Updated: 07/25/2005
Affected Releases: 4.1.1
Current Status: Closed

When configuring pattern matching string under "`/cfg/net/adv/filt <n>/adv/pmatch`" menu, there is a limit of 40 characters on the length of the pmatch string. If the length of the configured pmatch string is more than 40 characters, you will get the following error when you try to apply the configuration:

```
Update failed: Match String: Unable to set registry value: bad type of argument in
set operation
```

The validation checks for maximum string length and fixed in 4.1.2.

LIMIT ON NUMBER OF VIRTUAL NICS

CR# Q01138787
Last Updated: 07/25/2005
Affected Releases: 4.1.1
Current Status: No Fix Planned

NSF has a limit of 252 on the number of virtual NICs supported. Each L3 VLAN translates to one VNIC. Each port in an L2 VLAN translates to a VNIC. If your configuration results in more than 252 VNICs, all traffic coming to VNICs above 252 will be dropped.

CHANGING SUBNET ON RIP ENABLED INTERFACE REQUIRES RESTARTING RIP

CR# Q01159781
Last Updated: 07/25/2005
Affected Releases: 4.1.1
Current Status: No Fix Planned

If the subnet mask on a RIP enabled interface is changed, the RIP daemon will continue advertising the old subnet mask. Please login as root on the MIP director and run "`service ripd restart`" to restart the RIP daemon and force it to stop advertising the old subnet mask.

STATIC ROUTES ARE LOST AFTER IMPORTING CONFIGURATION

CR# Q01158579
Last Updated: 07/25/2005
Affected Releases: 4.1.1
Current Status: No Fix Planned

If you exported a configuration from 4.0.2 or earlier using "`/cfg/ptcfg`" and later imported it into 4.1.1 using "`/cfg/gtcfg`", the static routes will not be restored. This is because of the difference in the static route structure between the versions. To recover the static routes, login as root on the MIP director and run "`/opt/tng/bin/post-upgrade --routes –verbose`".

/INFO/SENSORS SHOW CPU AND BOARD TEMPERATURE TO BE NEGATIVE

CR# Q01133343
Last Updated: 08/31/2007
Affected Releases: 4.1.1
Current Status: No Fix Planned

"`/info/sensor`" CLI command displays the hardware monitoring information like CPU temperature, motherboard temperature, fan speeds etc. Sometimes, it may not be able to get the correct values and will

end up displaying “-1” for CPU and motherboard temperatures. You can recover from this situation by rebooting the director. If the problem recurs, please disable hardware monitoring by logging in as root and running the following commands.

```
make-part-rw / on
chkconfig sensord off
reboot
```

This issue is duplicate of CR Q01488250, which is fixed.

PIM: NSF DOES NOT SUPPORT FRAGMENTED PIM MESSAGES

CR# Q01150870
Last Updated: 07/25/2005
Affected Releases: 4.1.1
Current Status: No Fix Planned

When using PIM, fragmented “join” or “prune” messages are not supported. Fragmented bootstrap message (BSM) is also not supported (Q01150866) . Please ensure that these PIM control messages do not get fragmented.

VALIDATION ERROR ABOUT ACCESSLIST AFTER UPGRADE

CR# Q01157101
Last Updated: 08/31/2007
Affected Releases: 4.1.1
Current Status: Closed

If you upgrade from 4.0.x to 4.1.1, you will get the following validation error when you try to make some configuration change and apply.

```
Invalid setting for /cfg/sys/accesslist.
As an accesslist has been configured the MIP and
all hosts have to be part of the access list.
```

This is a new requirement in 4.1.1 that the NSF internal subnet has to be added to the access list. This is automatically done for you during clean install. In upgrade case, please add the NSF internal subnet to the access list to fix the above error.

After the fix in 4.1.3, SFD and MIP's ip are added to the access list.

“ASFCAPTURE” DOES NOT CAPTURE PACKETS SIMULTANEOUSLY ON ACCELERATOR AND DIRECTOR

CR# Q01160601
Last Updated: 03/22/2006
Affected Releases: 4.1.1
Current Status: Closed

The packet capture utility, “asfcapture”, captures packets only on the director even if the command line specifies both the director and accelerator as capture locations. The fix was to modify capture options from “sw” to “all” when accelerators and directors capture is enabled.

UNABLE TO CONFIGURE ACCELERATOR AFTER UPGRADE FROM 4.0.X

CR# Q01157140
Last Updated: 03/22/2006
Affected Releases: 4.1.x
Current Status: No Fix Planned

When upgrading from 4.0.x to 4.1.x, please make sure that the system was able to successfully configure the accelerators after upgrade is complete. You can do this by running “`/info/det`” and making sure the status of each accelerator says, “Accelerator is configured and unicast/igmp/pim routes are up-to-date”. If the accelerator was not configured, please login to the accelerator CLI as ‘admin’, set the accelerator to boot with factory default config using “`/boot/conf fact`” and reboot the accelerator using “`/boot/reset`”. This extra step is necessary because of changes in factory default configuration between 4.0.x and 4.1.x software.