>BUSINESS MADE **SIMPLE**

N⊘RTEL

Nortel Security Solutions
Product Readme

Nortel Switched Firewall 5100
Series 2.3.x - Readme

Document Date: 11 December, 2007
Document Version: 1.8

Table of Contents

Change Log

Version	What	When	Who
1.0.0	Initial draft – Consolidated README file for all 2.3.x releases	05/22/05	Ranganath P S
1.0.1	Added Q01106902-01 to the list of known issues	07/13/05	Ranganath P S
1.1.0	Added Section-4 and updated other sections for 2.3.3 release	10/26/05	Ranganath P S
1.2.0	Added Section-5 and updated other sections for 2.3.4 release	03/31/06	Navaneetha J
1.3.0	Added Section-6 and updated other sections for 2.3.4.1 release	08/02/06	Ranganath P S
1.4.0	Added Section-8 and updated other sections for 2.3.5 release	10/15/06	Gopi Krishna B
1.5.0	Added Section-9 and updated other sections for 2.3.5.1 release	12/14/06	Samuel Praveen
1.6.0	Added Section-10 and updated other sections for 2.3.6 release	04/30/07	Samuel Praveen
1.7.0	ReadMe for 2.3.7 Release	09/14/2007	Samuel Praveen
1.8.0	ReadMe for 2.3.8 Release	12/11/2007	Samuel Praveen

1 INTRODUCTION

This is the consolidated readme for all NSF-5100 2.3.x releases. The document is organized in different sections as follows.

Section-2 lists the status of all known issues found in 2.3.x releases. It also shows the release where the issue was found, the current status of the issue, and the status of the issue in each of the 2.3.x software releases. Sub sections under each release's sections describe the procedure to upgrade the old software to a 2.3.x release.

Appendix-A provides a more detailed explanation and workaround (if available) for all the known issues found/fixed in the 2.3.x releases.

2 STATUS OF KNOWN ISSUES AND LIMITATIONS

All the known issues found in 2.3.x releases are summarized in Table 1. 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 CR# is not available for an item, then search for the issue title in the Appendix for the specific update. The known issues without the CR# are listed at the beginning of each sub-section with the specific update date.
On viewing this document, click on a description item to jump to the detailed explanation 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, ☑ denotes the issue is fixed in the particular build and N/A means the issue is not applicable for that particular build.

Table 1   Current status of all issues found in NSF (5100)-2.3.x releases.

CR #	Description of Issues and Limitations	Last Updated	Current Status	2.3.1	2.3.3	2.3.4	2.3.4.1	2.3.5	2.3.5.1	2.3.6	2.3.7	2.3.8
Q01493358	ENHANCEMENT REQUEST FOR TRAP OF CLUSTER MEMBER DOWN	11/30/2007	Closed			☒	☒	☒	☒	☒	☒	☑
Q01287603	NSF: KEVLAR 2.2.7 - VRRP UNSTABLE WHEN NO VLAN CONFIGURED	11/30/2007	Closed	☒	☒	☑						
Q01196335	USER AUTHENTICATION DOESN'T WORK WITH L3 BRIDGE	11/30/2007	No Fix Planned		☒	☒	☒	☒	☒	☒	☒	☒
Q01196436	SECURID DOESN'T WORK WITH L3 BRIDGE	11/30/2007	No Fix Planned		☒	☒	☒	☒	☒	☒	☒	☒
Q01790177	GETOS IN CP R65 SMART DASHBOARD IDENTIFIES SECURE PLATFORM AS THE OS AND NOT LINUX	11/30/2007	No Fix Planned							☒	☒	☒
Q00778697	WEBUI OF KEVLAR WITH EMC: BBI STILL HAS THE OPTION TO RESET SIC	12/11/2007	Closed	☒	☒	☒	☒	☒	☒	☒	☒	☑
Q01740559	ON 2.3.5.1 R62 UNSUPPORTED SOFTWARE BUILD IS DISPLAYED AFTER ADMIN LOGIN	12/07/2007	Closed					☒	☒	☑		
Q01638568	IP ADDRESS OF MIP AND HOST MISSING IN /CFG/DUMP	08/31/2007	Closed					☒	☒	☒	☑	
Q01520987	BACKUP/CLONE FEATURE OVER DIFFERENT H/W PLATFORM	08/31/2007	Closed		☒	☒	☒	☒	☒	☒	☑	
Q01673027	NO VRRP FAILOVER WHEN VRRP ADVERTISEMENT RECEIVED HAS VRID SAME AS ON THE FIREWALL	08/31/2007	Closed							☒	☑	
Q01643825	OSPF FAILOVER NOT OCCURRING PROPERLY	08/31/2007	Closed					☒	☒	☒	☑	
Q01684913	AUTO BACK-UP FEATURE ON NSF PRODUCTS	08/31/2007	Closed		☒	☒	☒	☒	☒	☒	☑	
Q01303830	SSI RESTART CAUSES SNMP RESTART	08/31/2007	Closed	☒	☒	☒	☒	☑				
Q01687079	DEFAULT GATEWAY IS VALIDATED AGAINST SSI SUBNET	11/30/2007	Closed							☒	☒	☑

CR #	Description of Issues and Limitations	Last Updated	Current Status	2.3.1	2.3.3	2.3.4	2.3.4.1	2.3.5	2.3.5.1	2.3.6	2.3.7	2.3.8
	MASK AND NOT THE INTERFACE MASK											
Q01722998	SSH SECURID AND CP SECURID DOESN'T WORK SIMULTANEOUSLY	11/30/2007	Closed							❌	❌	✅
Q01725521	LIMITATION NOTE FOR SNMP TRAPSRCIP	11/30/2007	Closed							❌	❌	✅
Q01722991	CP SECURID DISABLE / ENABLE NOT WORKING PROPERLY	09/07/2007	Open							❌	❌	❌
Q01526730	ISD BOOT DELETE NOT WORKING PROPERLY FROM BBI	11/30/2007	Closed					❌	❌	❌	❌	✅
Q01742413	BACKUP/CLONE FAILS FOR DIFFERENT CP VERSIONS	11/30/2007	No Fix Planned							❌	❌	❌
Q01744444	UNABLE TO CONFIGURE GRE TUNNEL THROUGH OSPF - APPLY FAILS	09/13/2007	Open Workaround available								❌	❌
Q01619281	FAILED TO LOAD THE VPN ACCELERATOR CARD MODULE AFTER UPGRADE FROM 2.3.X_R55 TO 2.3.6_R65	04/23/2007	Open Workaround available	N/A	N/A	N/A	N/A	N/A	N/A	❌	❌	❌
Q01637091	CHECKPOINT EXPRESS GATEWAY IS NOT WORKING PROPERLY IN R65	08/31/2007	Closed	N/A	N/A	N/A	N/A	N/A	N/A	❌	✅	
Q01493746	2.3.5 VRRP BACKUP FIREWALL USING VIRTUAL MAC ADDRESS	03/29/2007	Closed	N/A	N/A	❌	❌	❌	❌	✅		
Q01409969	INCONSISTENT LINK DOWN SYSLOG MESSAGES IN VRRP CONFIGURATION	03/29/2007	Closed	❌	❌	❌	❌	❌	❌	✅		
Q01586553	DEFAULT GATEWAY MISSING AFTER FAILOVER ON VLAN TAGGED PORT	03/29/2007	Closed	N/A	N/A	N/A	N/A	❌	❌	✅		
Q01246421	SNMP TRAP SOURCE IP INCORRECT WITH CERTAIN TYPE OF CONFIG	03/29/2007	Closed	❌	❌	❌	❌	❌	❌	✅		
Q01156694	SYSTEM SHOWS ZERO VALUE FOR ALL HARDWARE SENSOR INFOMATION UNDER STRESS TEST	03/29/2007	Closed	❌	❌	❌	❌	❌	❌	✅		
Q01530693	NOT ABLE TO INSTALL ISO IMAGE ON 5100 NE MODELS WITH 160 GB HDD	03/29/2007	Closed	❌	❌	❌	❌	❌	❌	✅		
Q01588691	CHECK POINT SYNCHRONIZATION STATUS IS SHOWN AS "HA MODULE NOT STARTED" AFTER UPGRADING TO 2.3.6	08/31/2007	Closed	N/A	N/A	N/A	N/A	❌	❌	❌	✅	
Q01355224	SYSLOG SRCIP DOES NOT WORK, DEPENDS ON CONFIGURATION	03/29/2007	Closed	❌	❌	❌	❌	❌	❌	✅		
Q01347061	NSF 5111(V2.3.3.0) NIC LEDS STATUS DIFFERENT FROM THE HW GUIDE	03/29/2007	Closed	❌	❌	❌	❌	❌	❌	✅		
Q01573879	CPSYN NOT UP WHEN UPGRADED FROM 2.3.5 R60 TO 2.3.5.13 R65 WITH CP SECID ENABLED	08/31/2007	Closed	N/A	N/A	N/A	N/A	❌	❌	❌	✅	
Q01464653	EVENTIA REPORTER DOES NOT GENERATE REPORTS PROPERLY	12/06/2006	Open	N/A	N/A	N/A	N/A	❌	❌	❌	❌	❌

Nortel Switched Firewall 5100 series, Version 2.3.x

CR #	Description of Issues and Limitations	Last Updated	Current Status	2.3.1	2.3.3	2.3.4	2.3.4.1	2.3.5	2.3.5.1	2.3.6	2.3.7	2.3.8
Q01511853	EVENTIA REPORTER IS GIVING PROBLEM, WHEN CONFIGURED IN DISTRIBUTED MODE	08/31/2007	No Fix Planned	N/A	N/A	N/A	N/A	N/A	☒	☒	☒	☒
Q01451030	STATIC RT MISSING IN UPGRADED BOX IF A SMART CLIENT IS ADDED IN A NON EMC SETUP	08/31/2007	Closed	N/A	N/A	N/A	N/A	☒	☒	☒	☑	
Q01469502	CHECKPOINT ALERTS RECEIVED WHEN ISDS STRESSED WITH HIDE NATED CONNECTIONS	08/31/2007	No Fix Planned	N/A	N/A	N/A	N/A	☒	☒	☒	☒	☒
Q01475323	TRAFFIC DOES NOT CONTINUE AFTER A FAILOVER IN AA MODE	08/31/2007	No Fix Planned	N/A	N/A	N/A	N/A	☒	☒	☒	☒	☒
Q01451297	HOST IP'S ARE CONFIGURED AS SYSLOG SERVERS	08/31/2007	Closed	N/A	N/A	N/A	N/A	☒	☒	☒	☑	
Q01371193	NTP SYNCHRONIZATION ERRORS IN ASF5109 VER2.3.1	10/05/2006	Closed	☒	N/A	N/A	N/A	☑	☑	☑		
Q01457794	SYSLOG SERVER NOT GETTING UPDATED AFTER UPGRADED TO 2.3.4.18_R61	08/31/2007	No Fix Planned	N/A	N/A	N/A	N/A	☒	☒	☒	☒	☒
Q01460850	L2 FIREWALL NOT WORKING IN R55	08/31/2007	No Fix Planned	N/A	N/A	N/A	N/A	☒	☒	N/A	N/A	N/A
Q01464594	CP R61, AFTER CONFIGURING/ENABLING QOS ON INTERFACE GETTING THE WARNING MESSAGE	15/10/2006	Open	N/A	N/A	N/A	N/A	☒	☒	☒	☒	☒
Q01394047	2.3.4.0: UNABLE TO SEND SYSLOG AND SNMP TRAP	03/29/2007	Closed	N/A	N/A	N/A	N/A	☒	☒	☑		
Q01403593	EVENTIA REPORTER CLI IS MISSING	09/11/2006	Closed	N/A	N/A	N/A	☒	☑	☑	☑		
Q01333862	ESL: KEVLAR OSPF SPF INTERVAL TIMER CAN BE SET AS 0	08/22/2006	Closed	☒	☒	☒	☒	☑	☑	☑		
Q01330359	COULDN'T GET THE INTERFACE STATUS PAGE FROM BBI AFTER UPGRADING TO 2.3.4.0_R60	08/31/2007	Closed	N/A	N/A	☒	☒	☑				
Q01319328	SNMP TRAP SOURCE IP IS NOT CORRECT WHEN TRAP SOURCE IP SET TO MIP	08/31/2007	Closed	☒	☒	☒	☒	☑				
Q01328134	ER DOES NOT WORK AFTER BOOT DELETING THE BOX IN EMC MODE.	09/11/2006	Closed	N/A	N/A	☒	☒	☑	☑	☑		
Q01333945	WEB [UI] - "PRODUCT TYPE" IS SHOWN WITH INCORRECT HARDWARE TYPE FOR MIX PLATFORM	09/13/2006	Closed	☒	☒	☒	☒	☑	☑	☑		
Q01316824	WEB SERVICE IS STILL RUNNING WHEN DISABLING IT BY "CFG/SYS/ADMIN/WEB/HTTP/DIS"	08/22/2006	Closed	☒	☒	☒	☒	☑	☑	☑		
Q01233372	FAIL-OVER DOESN'T WORK WITH USER AUTHENTICATION ON VRRP H/A	08/31/2007	Closed	N/A	☒	☒	☒	☑				
Q01235159	THE CP SYNC IS DOWN WITH 68 INTERFACES IN HA MODE AFTER REBOOTING THE SYSTEM	10/26/05	Open	N/A	☒	☒	☒	☒	☒	☒	☒	☒
Q01210529	CP FAILS TO GET TOPOLOGY FROM L3-BRIDGE WITH VLANID IN HA	10/26/05	Open Workaround available	N/A	☒	☒	☒	☒	☒	☒	☒	☒
Q01157972	[BBI] TICKER SHOWS INCORRECT	10/26/05	Open									☒

CR #	Description of Issues and Limitations	Last Updated	Current Status	2.3.1	2.3.3	2.3.4	2.3.4.1	2.3.5	2.3.5.1	2.3.6	2.3.7	2.3.8
	INFORMATION ABOUT THROUGHPUT		Workaround available	N/A	✗	✗	✗	✗	✗	✗	✗	
Q01203464	L3-BRIDGE: OSPF WORK ON A DISABLED VRRP INTERFACE	08/31/2007	Closed	N/A	✗	✗	✗	✗	✗	✗	✓	
Q01191170	HIDE-NAT NOT WORKING PROPERLY IN VRRP AA SETUP	08/31/2007	Closed	N/A	✗	✗	✗	✓				
Q01188039	QOS POLICY NOT GETTING DOWNLOADED AFTER THE UPGRADE	08/31/2007	Closed	N/A	✗	✗	✗	✗	✗	✓		
Q01198129	MAINT/BACKUP/LOCAL COMMAND FAILS IN STAND-ALONE MODE	03/29/2006	Closed	N/A	✗	✓	✓	✓	✓	✓		
Q01184682	SECURID DOESN'T WORK WITH HIDE-NAT IN HA MODE	04/12/2006	Closed	N/A	✗	✓	✓	✓	✓	✓		
Q01188074	SESSION FAILOVER NOT WORKING WITH SYNC PORT IN VLAN	08/31/2007	Closed	N/A	✗	✗	✗	✓				
Q01194543	THE POLICY IS NOT DOWNLOADED TO THE FIREWALL AFTER UPGRADING FROM R55 TO R60	10/26/05	Open Workaround available	N/A	✗	✗	✗	N/A	N/A	N/A	N/A	N/A
Q01163068	SYSTEM COULDN'T CLEAR THE OSPF ROUTES WITH 200 ROUTES	09/19/2006	Closed	N/A	✗	✓	✓	✓	✓	✓		
Q01155340	RESTRICTION VIA HOSTS.ALLOW FILE DOESN'T WORK FOR SMARTPORTAL	08/31/2007	Closed	N/A	✗	✗	✗	✓				
Q01181504	SERVICES DHCP_REQ… AND DHRP_REQ… NEED TO BE EDITED TO ACCEPT DHCP TRAFFIC	07/31/2006	Closed	N/A	N/A	✓	✓	✓	✓	✓		
Q01215993	VPN S2S WITH STANDALONE SYSTEMS: NEED SOME WORK AROUND STEPS	08/31/2007	Closed	N/A	✗	✗	✗	✓				
Q01201687	PARTITION HDA3 OF ISD IS REACH 99% AFTER DOING UPGRADING	08/31/2007	No Fix Planned	N/A	✗	✗	✗					
Q01176213	STATIC ROUTES ARE NOT DELTED AFTER /BOOT/DELETE	07/13/05	Closed	✗	✓	✓	✓	✓	✓	✓		
Q01106902-01	HEALTH CHECK DAEMON AND CONFIG DAEMON MAY NOT WORK PROPERLY AFTER 248 DAYS OF UPTIME	07/13/05	Closed	✗	✓	✓	✓	✓	✓	✓		
Q01052791	ENABLE OSPF REDISTRIBUTION WILL MAKE THE GRE TUNNEL UP/DOWN CONTINUOUSLY	08/31/07	Closed	N/A	N/A	N/A	N/A	✓				
Q01054089	FWMON DOESN'T WORK FOR THE FILTER OPTION "NET"	08/31/07	No Fix Planned	N/A	N/A	✗	✗	✗	✗	✗	✗	✗
Q01052205	BBI: RESETING SIC OPERATION FROM WEB BROWSER REACHES TIMEOUT	08/31/07	No Fix Planned	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q01059503, Q01048974, Q01048977	TSDUMP DOESN'T WORK AFTER BREAKING BY CTL+C	05/22/05	Closed	✗	✓	✓	✓	✓	✓	✓		
Q01040018	DYNAMIC NAT IS FAILED ON LAYER 3 BRIDGE	05/22/05	Closed	N/A	N/A	✓	✓	✓	✓	✓		
Q01048980	BBI: ALL KEVLAR CONFIGURATION IS DETROYED	05/22/05	Open Workaround	✗	✗	✗	✗	✗	✗	✗	✗	✗

CR #	Description of Issues and Limitations	Last Updated	Current Status	2.3.1	2.3.3	2.3.4	2.3.4.1	2.3.5	2.3.5.1	2.3.6	2.3.7	2.3.8
	WHEN IMPORTING EMPTY FILE		available									
	HOST/USB-OHCI.C: FOUND OHCI DEVICE WITH NO IRQ ASSIGNED. CHECK BIOS SETTINGS!	05/22/05	Closed	☒	☑	☑	☑	☑	☑	☑		
Q01137943	CHECKPOINT DAEMON IS NOT STARTED AFTER HOST DELETE ACTION IN CLUSTER	05/22/05	Closed	☒	☑	☑	☑	☑	☑	☑		
Q01070889	THE AUTONEGOTIATION'S FEATURE ON PORT HAVE PROBLEM WHEN DISABLED	05/22/05	Closed	☒	☒	☒	☒	☑	☑	☑		
	PCI BUS SPEED IS SET TO 66MHZ, REGARDRLESS OF WHICH CARDS ARE INSTALLED, ON THE 5124-NE1 MODELS	05/22/05	Open	☒	☒	☒	☒	☒	☒	☒	☒	
Q01046976-01	OSPF: ONE ISD COULD NOT SEE OTHER AS NEIGHBOUR AND CPU HIT INTO 100%	05/22/05	Closed	☒	☑	☑	☑	☑	☑	☑		
Q01114346	KEVLAR 2.3 BETA - SOMETIMES KEVLAR OPERATING IN PROMISCUOUS MODE	08/31/07	No Fix Planned	☒	☒	☒	☒					

3 UPGRADING TO NSF 2.3.X

Upgrade to 2.3.x is supported from 2.2.7 or later versions.

2.3.x requires 250 MBytes free space on the /isd partition. To check the available free space, login as root, run "df –H /isd" and look under the "Avail" column. If you do not have enough free space, you will get an error saying "Failed to unpack software …" when you try to download the .pkg file.

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

To upgrade, first download the appropriate 2.3.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".

Upgrading can be done from the BBI as well.

The summary of the main steps for upgrading to NSF 2.3.x is given below.

Pre upgrade checks:

New validations have been added for some CLI commands. If these parameters are not configured properly, upgrade to 2.3.8 will fail due to the new validation checks. Please refer to the CR# Q01475332 for all the new validations.

Upgrade procedure in cluster mode:

➢ Get the NSF5100_2.3.8.0_Rxx.pkg file and copy it to an ftp server or in a CD
➢ Download the new upgrade image via ftp/CDROM using /boot/software/download or /boot/software/cdrom command from the CLI. This should be done only in one Director
➢ After the download is complete, check the current versions of the software and you will see that the version you downloaded has a status 'unpacked'
➢ Check if any access list entries are configured on the Firewall. If access lists are configured for networks other than the SSI network, add a new access list entry for SSI network (it's mandatory for NSF 2.3.8.0 upgrade process to have entries for the SSI network as well)
➢ Activate the new (unpacked) version software by running the following command in the CLI: /boot/software/activate
➢ At this time, both firewalls will be rebooted twice to make the post upgrade changes effective.
➢ Wait for a minute or two for the firewalls to initialize all system components
➢ Check the firewall status by executing /info/sum command from the CLI and make sure you see both firewalls as 'up'
➢ Check the CP sync status. This should show both the iSDs as 'active'

Note: It takes a longer time for 2.3.x version to come up. This is due to the new Check Point packages included in this version. Check the Appendix-B for the approximate boot up time it takes on each hardware model.

Upgrade procedure in standalone mode:

➢ Get the NSF5100_2.3.8.0_Rxx.pkg file and copy it to an ftp server or in a CD
➢ Download the new upgrade image via ftp/CDROM using /boot/software/download or /boot/software/cdrom command from the CLI
➢ Once the download is complete, check the current versions of the software and you will see that the version you downloaded has a status 'unpacked'
➢ Activate the new (unpacked) version software by running the following command in the CLI: /boot/software/activate
➢ At this time, both firewalls will be rebooted twice to make the post upgrade changes effective
➢ Wait for a minute or two for the firewall to initialize all system components
➢ Check the firewall status by executing /info/sum command from the CLI and make sure you are seeing the firewall status as 'up'

4 NORTEL FIREWALL SYSTEM 5100, VERSION 2.3.1 (05/22/05)

4.1 Supported Hardware

NSF 2.3.1 supports NSF 5106, 5109, 5111-NE1, 5114 & 5114-NE1 hardware platforms.

4.2 Supported Check Point Releases

NSF 2.3.1 supports
- Check Point NG with Application Intelligence (R55) Build 541 With HFA-12
(This build contains special fixes, which enables Check Point Firewall to work properly with Linux kernel version 2.4.20)

4.3 Notes on Newly Supported Features

The following features, which are not supported in 2.2.7.x R54 releases, are supported in this 2.3.1 R55 release.

- ➢ Check Point User Authority
- ➢ Check Point ISP Redundancy
- ➢ SSI bypass
- ➢ SSI management on VLAN
- ➢ L2/L3 bridging
- ➢ GRE tunneling
- ➢ OSPF in HA/AA mode
- ➢ BOOTP/DHCP Relay
- ➢ Radius Authentication
- ➢ UPS Support
- ➢ USB storage support
- ➢ Patch rpm install from CLI
- ➢ Hardware monitoring support
- ➢ Extended logging

4.4 Feature Limitations

4.4.1 OSPF: Limitations with OSPF & GRE

In the current NSF 2.3.1_R55 version, the following OSPF & GRE features are not supported:
- ➢ Virtual Link
- ➢ Stub Area
- ➢ NSSA Area
- ➢ Route map
- ➢ Summarizing Route
- ➢ Host Route
- ➢ Multiple MD5 key per one OSPF interface
- ➢ Default gateway and OSPF default route are not supported together
- ➢ Disable area 0, or make it become inactive
- ➢ Elect DR will not occur when iSD is not in initialization state
- ➢ Support GRE and OSPF on the same interface
- ➢ OSPF connected interface redistribution

4.4.2   L2/L3 - Limitations with L2/L3 Bridge interfaces

In the current NSF 2.3.1_R55 release, the following features are not supported on the L2/L3 interfaces:

➢ QoS cannot be set on the L2/L3 bridge interfaces
➢ User authentication for the traffic between the L2/L3 interfaces doesn't work.

4.5 Upgrading to NSF-5100 2.3.1

Follow the following steps while upgrading to 2.3.1.

In Cluster mode:
➢ Get the NSF5100_2.3.1_R55.pkg file and copy it to an ftp server or in a CD
➢ Download the new upgrade image via ftp/CDROM using */boot/software/download* or */boot/software/cdrom* command from the CLI
➢ Once the download is complete, check the current versions of the software and you will see that the version you downloaded has a status '*unpacked*'
➢ Disable the Check Point sync by executing the CLI command (*/cfg/fw/sync/dis/apply*)
➢ Wait for 2-3 minutes, as Check Point applications take some time to re-initialize
➢ Check the firewalls status by executing */info/clu* command from the CLI and make sure you see both firewalls as 'up'
➢ Check if any access list entries are configured on the Firewall. If access lists are configured for networks other than the SSI network, add a new access list entry for SSI network (*it's mandatory for NSF 2.3.x upgrade process to have entries for the SSI network as well*)
➢ Activate the new (unpacked) version software by running the following command in the CLI: */boot/software/activate 2.3.1*
➢ At this time, both firewalls will be rebooted
➢ Wait for a minute or two for the firewalls to initialize all system components
➢ Enable the Check Point sync by executing the CLI command (*/cfg/fw/sync/ena*)
➢ Both the firewalls will now reboot for updating the Check Point configuration
➢ After both the firewalls have come up wait for a 2-3 minutes, then check the firewall status by executing /info/sum command from the CLI and make sure you see both firewalls as 'up'

In Standalone mode:
Upgrade procedure for NSF 2.3.1 in standalone mode is same as given in   Section 3.

5   NORTEL FIREWALL SYSTEM 5100, VERSION 2.3.3 (10/26/05)

5.1 Supported Hardware

NSF 2.3.3 supports NSF 5106, 5109, 5111-NE1, 5114 & 5114-NE1 hardware platforms.

5.2 Supported Check Point Releases

NSF 2.3.3 supports
• Check Point VPN-1™ & Firewall-1® NGX (R60) Build 458 with Hotfix 014 – build 009.

5.3 Notes on Newly Supported Features

The following features, which are not supported in 2.3.1.x R55 releases, are supported in this 2.3.3 R60 release.

- ➢ Check Point Smart Portal
- ➢ System Monitoring support from CLI
- ➢ Web Ticker
- ➢ Configuration support for SecurID feature from CLI/BBI

5.4 Feature Limitations

All the limitations listed in 2.3.1 release section are not supported in 2.3.3 release as well.

6 NORTEL FIREWALL SYSTEM 5100, VERSION 2.3.4 (03/29/06)

6.1 Supported Hardware

NSF 2.3.4 supports NSF 5106, 5109, 5111-NE1, 5114 & 5114-NE1 hardware platforms.

6.2 Supported Check Point Releases

NSF 2.3.4 supports

- Check Point VPN-1(TM) & FireWall-1 (R) NG with Application Intelligence (R55) HFA_17, Hotfix 670 – Build 005
- Check Point VPN-1(TM) & FireWall-1 (R) NGX (R60) – Build 458 with Hotfix 014 – Build 009

6.3 Notes on Newly Supported Features

NSF5100 Series Firewalls release 2.3.4 with Check Point R60 supports Check Point Eventia Reporter as one of its main features.

Eventia Reporter support is provided only when the NSF firewalls are configured in EMC (SmartCenter Server) mode.

Eventia Reporter can be configured via the CLI/BBI. NSF supports both 'Local' & 'Distributed' modes of Eventia Reporter. The Preferred and default option is set to 'distributed' as per the Check Point user guide.

6.4 Feature Limitations

All the limitations listed in 2.3.3 release section are not supported in 2.3.4 release as well.

7 NORTEL FIREWALL SYSTEM 5100, VERSION 2.3.4.1 (08/02/06)

7.1 Supported Hardware

NSF 2.3.4.1 supports NSF 5106, 5109, 5111-NE1, 5114 & 5114-NE1 hardware platforms.

7.2 Supported Check Point Releases

NSF 2.3.4.1 supports

- Check Point VPN-1(TM) & FireWall-1 (R) NGX (R61) – Build 207

7.3 Feature Limitations

NSF5100 Series Firewalls release 2.3.4.1 does not support Check Point Eventia Reporter. Hence for users who're upgrading from 2.3.4.0_R60 with Eventia Reporter enabled, the feature will not work. For more information on the limitation, please refer to CR # Q01403593.

8 NORTEL FIREWALL SYSTEM 5100, VERSION 2.3.5 (09/19/06)

8.1 Supported Hardware

NSF 2.3.5 supports NSF 5106, 5109, 5111-NE1, 5114 & 5114-NE1 hardware platforms.

8.2 Supported Check Point Releases

NSF 2.3.5 supports

- Check Point VPN-1(TM) & FireWall-1(R) NG with Application Intelligence (R55) HFA_18, Hotfix 771 - Build 011
- Check Point VPN-1(TM) & FireWall-1(R) NGX (R60) HFA_04, Hotfix 604 - Build 028
- Check Point VPN-1(TM) & FireWall-1(R) NGX (R61) - Build 207

8.3 Notes on Newly Supported Features

- SSIbyPass Enhancement:

While configuring an NSF Firewall in a standalone or in cluster mode, we have to configure first, a management IP address and an MIP address to the Firewall(s). This management interface is used to communicate between the cluster members and also for electing the MIP owner.
For creating a cluster, we need to allow flow of traffic between the cluster members. By default, the Check Point FW module's behavior is to drop any traffic. Hence, users are required to create a separate rule to allow traffic within the management network.

To avoid this, a new feature called "SSI bypass" is introduced from 2.3.1 release onwards. With this feature, any communication between the cluster members and any traffic within the management

network directed towards the cluster members will not be controlled by Check Point rules. A new set of Linux iptables rules has been added to limit the access in the management network.

Hence the users need not add any specific rule to allow traffic within the management network.

A new CLI command is provided to enable/disable this SSI bypass feature at run time.

CLI Command output to enable/disable SSIbypass:

```
[Maintenance Menu]
    backup    - Backup system configuration
    fw        - Firewall Maintenance Menu
    tsdump    - Tech Support Dump Menu
    chkcfg    - Check applied configuration
    cplog     - Check Point Logs
    emc       - EMC Server's admin password change
    logdetail - Obtain extensive detail about the log/error code dumped
    ospf      - OSPF Debug Menu
    snmp      - Snmp Menu
    ssibypass - SSIbypass Menu

>> Maintenance#

>> Maintenance# ssibypass/

---------------------------------------------------------------
[SSIbypass Menu]
    ena       - Enable SSIbypass
    dis       - Disable SSIbypass

>> SSIbypass Feature#

>> SSIbypass Feature# cur

SSIbypass Feature:
  Enable SSIbypass = y
```

8.4 Feature Limitations

All the limitations listed in 2.3.4 release section are not supported in 2.3.5 release as well.

9 NORTEL FIREWALL SYSTEM 5100, VERSION 2.3.5.1 (12/06/06)

9.1 Supported Hardware

NSF 2.3.5.1 supports NSF 5106, 5109, 5111-NE1, 5114 & 5114-NE1 hardware platforms.

9.2 Supported Check Point Releases

NSF 2.3.5.1 supports

- Check Point VPN-1(TM) & FireWall-1 (R) NGX (R62) – Build 120

9.3 Feature Limitations

All the limitations listed in 2.3.5 release section are not supported in 2.3.5.1 release as well.

10 NORTEL FIREWALL SYSTEM 5100, VERSION 2.3.6 (04/30/07)

10.1 Notes on Newly Supported Features

➢ SecurID authentication for login to the Firewall via SSH

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

From 2.3.6 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 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 could be logged in.

➢ Checkpoint R65
Release 2.3.6 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.

10.2 Feature Limitations

- Upgrade from any 2.3.x R55 version to 2.3.6_R65 is not supported. Please refer to CR # Q01619281 for more details
- Configuring the Firewall in 'Check Point Express Gateway' or 'Check Point Express Gateway and SmartCenter Server' are not supported in 2.3.6_R65
- All the limitations listed in 2.3.5.1 release section are not supported in 2.3.6 release as well
- Eventia reporter is not supported in CP R65 version

- L2-L3 firewall functionality is not supported in CP R65 version. Please refer CR# Q01523984 notes for more information

11 NORTEL SWITCHED FIREWALL 5100, 2.3.7 (09/14/2007)

11.1 Notes on Newly Supported Features

11.1.1 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 2.3.7 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). Later if the user wants to restore this configuration, it can be done with the 'clone' command. Note that the user needs to do '/boot/delete' before doing the 'clone'. The configuration file name that will be stored in the remote host would be of 'filename_isd ip_ddmmyyyy' format. For example if the file name is 'test' then the final file name will be 'test_10.10.1.1_16Jul2007'.

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.

11.1.2 Cloning between different Hardwares

Nortel has introduced three new hardware types (5111-NE1, 5114-NE1, 5124-NE1) as compatible hardware types for their older counterparts (5109,5114 and 5124 respectively). So it is now possible to replace the above mentioned older hardware types with the compatible new counterparts. However the hardware dependency in the clone feature prevents the user from cloning the original setup to the new hardware.

To overcome this problem, the clone feature has been modified to support cloning from compatible hardware types. With the modifications, the new hardware types can be cloned from their older counterparts. However the reverse is not possible , as the new hardware types support some extra features.
> Ex. 1. 5111-NE1 supports the bridge feature whereas its counterpart 5109 doesn't.
>> 2. Only NE Kestrel boxes (5111-NE1, 5114-NE1, 5124 NE1) support setting gig speed with auto-off, for the copper gig ports.

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

Previously, the Broadcom 'BCM5822' provided the VPN acceleration in the 5124. Broadcom discontinued the manufacturing of this card recently and replaced it with a new model. The Broadcom 'BCM5823' has replaced the BCM5822 for new models of 5124.

The new card has slight modifications to the driver software and uses CPacc4 drivers. These drivers have been added to version 2.3.7 of the software such that 2.3.7 supports both the older and new versions of the VPN accelerator card.

11.1.4 Supported SecurID feature in WEBUI

In 2.3.6, SecurID support was offered only through CLI. From 2.3.7 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

11.1.5 Support for Check Point Express & SmartCenter Server modes in R65

Configuring the NSF5100 firewall mode in 'Check Point Express Gateway' or 'Check Point Express Gateway and SmartCenter server' is supported in 2.3.7 release. For more information please refer to CR   Q01637091

11.2 The following customer CR's are fixed in this Release

- Backup/Clone feature over different H/W platform (Q01520987)
- No VRRP failover when VRRP advertisement received has VRID same as on the firewall (Q01673027)
- Auto back-up feature on NSF products (Q01684913)

12 NORTEL SWITCHED FIREWALL 5100, 2.3.8 (12/11/2007)

12.1 Supported Hardware Platforms and Supported Checkpoint Releases

Please refer to the 2.3.8 Release notes available in the Nortel site

12.2 Notes on Newly Supported Features

12.2.1 SecurID Enhancement

This section covers the design change in the Checkpoint SecurID configuration for NSF5100 firewalls, allowing both Checkpoint SecurID and SSH SecurID to be configured simultaneously.

CLI modifications for NSF5100 series firewalls:

A new set of CLI commands are added for selecting address mode and configuring the respective interface index instead of configuring IP address.

>> Main# /cfg/fw/securid/

```
---------------------------------------------------------------
[SecurID Configuration Menu]
     local         - Import SecurID config file from a floppy/usb
     remote        - Import SecurID config file from a remote server
     addrmode   - Set SecurID interface address mode
     ifindex        - Set SecurID interface index
```

/cfg/fw/securid/addrmode - This command is used to select either VRRP IP or Real IP to connect to the RSA ACE server.

Note: User should select the 'addrmode' before configuring 'ifindex'.

/cfg/fw/securid/ifindex - This command is used to configure the interface index number for connecting the ACE server.

Note: Make sure that ACE server is reachable through the configured interface index.

Configuration:

This section covers the configuration details about the new CLI menus added. For detailed configuration on the ACE server, refer to RSA ACE server documentation.

High-Availability mode:

1) If the user selects VRRP IP under 'addrmode' then,
     a)"Hide cluster members outgoing traffic behind cluster's IP address" option on the smart
        dashboard should be checked.
     b) One agent host pointing to the VRRP IP of the cluster should be configured on the
        ACE server.
2) If the user selects Real IP under 'addrmode' then,
     a)"Hide cluster members outgoing traffic behind cluster's IP address" option on the smart
        dashboard should be unchecked.

b) Two agent hosts, each one pointing to one cluster member should be configured on the
ACE server.

Active-Active mode:

1) If the user selects VRRP IP under 'addrmode' then,
    a)"Hide cluster members outgoing traffic behind cluster's IP address" option on the smart
       dashboard should be checked.
    b) Two agent hosts, each one pointing to the VRRP IP's of the cluster should be
       configured on the ACE server.
2) If the user selects Real IP under 'addrmode' then,
    a)"Hide cluster members outgoing traffic behind cluster's IP address" option on the smart
       dashboard should be unchecked.
    b) Two agent hosts, each one pointing to one cluster member should be configured on the
       ACE server.

Both Checkpoint SecurID and SSH SecurID can be configured simultaneously when the user selects
Real IP under 'addrmode' CLI menu.

12.3 The following customer CR's are fixed in this Release

- Enhancement Request for Trap of cluster member down (Q01493358)

- Default gateway is validated against ssi subnet mask and not the interface mask (Q01687079)

- SSH SecurID and CP SecurID doesn't work simultaneously (Q01722998)

- WEBUI of Kevlar with EMC: BBI still has the GUI to reset SIC (Q00778697)

13 APPENDIX-A: LIST OF KNOWN ISSUES

This Appendix provides detailed explanation on all the issues found in 2.3.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 12/11/2007

ENHANCEMENT REQUEST FOR TRAP OF CLUSTER MEMBER DOWN

CR # Q01493358
Last Updated: 11/30/2007
Affected Releases: 2.3.4
Current Status: Closed

In VRRP configuration, NSF does not send SNMP trap when non-MIP host port link is down.

This is fixed in 2.3.8 by modifying the health check daemon code, which sends trap when the SSI connectivity is lost.

NSF: KEVLAR 2.2.7 - VRRP UNSTABLE WHEN NO VLAN CONFIGURED

CR # Q01287603
Last Updated: 11/30/2007
Affected Releases: 2.2.7
Current Status: Closed

If there are multiple interfaces configured on multiple VLANs and if one of the VLANs are not configured on the connected layer-2 device thereby causing no vrrp advertisements to be seen on that interface, the fail-over triggers even if the advertisements are seen on other interfaces. So the vrrp flips and then becomes master again as it sees advertisements on other connected interfaces. This causes a loop.

This is fixed in 2.3.4 by adding a time variable which gets updated whenever a vrrp advertisement is received. During fail-over this timer will be checked and if it is less than the vrrp timeout, failover does not happen.

USER AUTHENTICATION DOESN'T WORK WITH L3 BRIDGE

CR # Q01196335
Last Updated: 11/30/2007
Affected Releases: 2.3.3
Current Status: No Fix Planned

After configuring the ports in the bridge mode, user authentication does not work.
Since the 'user authentication' is a Check Point feature, it may not work on L3 bridge support.

This is a limitation when L3 bridge mode is configured in NSF5100

SECURID DOESN'T WORK WITH L3 BRIDGE

CR # Q01196436
Last Updated: 11/30/2007
Affected Releases: 2.3.3

Current Status: No Fix Planned

After configuring the ports in the bridge mode, SecurID authentication does not work.

This is a limitation when L3 bridge mode is configured in NSF5100

GETOS IN CP R65 SMART DASHBOARD IDENTIFIES SECURE PLATFORM AS THE OS AND NOT LINUX

CR # Q01790177
Last Updated: 11/30/2007
Affected Releases: 2.3.6
Current Status: No Fix Planned

The OS of the R65 release is identified as Secure Platform when initializing SIC and when doing GetOS in Smart Dashboard.

Since GetOS fetches Secure Platform as the OS, the user has to manually change it to Linux and push the policy.

WEBUI OF KEVLAR WITH EMC: BBI STILL HAS THE OPTION TO RESET SIC

CR # Q00778697
Last Updated: 12/11/2007
Affected Releases: 2.2.x
Current Status: Closed

In WEBUI of Kevlar 2.2.3.5 with EMC, under the firewall → settings page there is an option to reset SIC for the iSD, which should be removed.

This is fixed in 2.3.8.

ON 2.3.5.1 R62 UNSUPPORTED SOFTWARE BUILD IS DISPLAYED AFTER ADMIN LOGIN

CR # Q01740559
Last Updated: 11/30/2007
Affected Releases: 2.3.5
Current Status: Closed

After upgrading to 2.3.5.1_R62, the following message is seen saying that this is an internal use only build after logging into firewall using admin.

"login: admin

Password:
Nortel Firewall
Unsupported Software build on Thu Nov 16 14:25:25 PST 2006
Nortel, Inc. Internal Use Only.

Hardware platform: NSF-5109
Software version: 2.3.5.1_R62"

This is nothing but an additional warning message being added which will be displayed for any release version that does not end with .0. This is to distinguish between the FCS builds or any internal/private builds that is given to the customer.

However, with some patch releases that do not end with .0 as the release version, this warning pops up.

Please ignore this warning for any pre-2.3.6.0 FCS builds as its corrected in 2.3.6.0 and above releases.

Issues Updated on 09/14/2007

IP ADDRESS OF MIP AND HOST MISSING IN /CFG/DUMP

CR # Q01638568
Last Updated: 08/31/2007
Affected Releases: 2.3.5
Current Status: Closed

Running the command '/cfg/dump' won't show the host IP and MIP because the latest code does not support changing the host IP & MIP. So commands like /cfg/sys/cluster/host #/ip and /cfg/sys/cluster/MIP were removed . Hence /cfg/dump won't show them. There were instances when some issues were reported while changing the Host IP & MIP So those commands were removed.

Alternatively, the command '/info/net/if' has been modified to display the Host IP and MIP along with the interface information.

BACKUP/CLONE FEATURE OVER DIFFERENT H/W PLATFORM

CR # Q01520987
Last Updated: 08/31/2007
Affected Releases: 2.3.3
Current Status: Closed

In earlier software releases, backup/clone feature had a dependency over hardware type. So it was not possible to backup from an IBM box and perform clone on a Network Engine box.

This is addressed in 2.3.7 and the clone process for the following listed patterns (from IBM models to Network Engine counterparts) are supported now.

 From NSF-5109 to NSF-5111-NE1
 From NSF-5114 to NSF-5114-NE1
 From NSF-5124 to NSF-5124-NE1

Please refer to the 'Cloning between different hardwares' section for more information.

NO VRRP FAILOVER WHEN VRRP ADVERTISEMENT RECEIVED HAS VRID SAME AS ON THE FIREWALL

CR # Q01673027
Last Updated: 08/31/2007
Affected Releases: 2.3.6
Current Status: Closed

If NSF5100 receives an external VRRP advertisement with a VRID equal to a VRRP interface on another interface, then VRRP failover does not occur.

Whenever a VRRP advertisement is received, a time variable gets updated. This timer value is compared against the VRRP timeout value to initiate a VRRP failover. So if the timer value is less than the VRRP timeout value, failover does not happen.

In this particular CR scenario, a bogus advertisement from an external device is seen and the timer value is updated. So whenever VRRP doesn't detect any advertisement from the peer cluster member, it starts a fail-over. But since the timer is already updated after the last received bogus advertisement, it assumes that advertisement is seen on other interface and hence the fail-over does not happen.

This is fixed in 2.3.7 based on packet validation.

OSPF FAILOVER NOT OCCURING PROPERLY

CR # Q01643825
Last Updated: 08/31/2007
Affected Releases: 2.3.5
Current Status: Closed

In an Active-Active NSF5100 setup connected to redundant ISP routers with OSPF enabled, one of the NSF routers drops all packets when its highest priority ISP router goes down. The reason NSF could not forward packets is because it loses its default route although the OSPF neighbor status is correct. Since the "Extended Cluster Anti-Spoofing" option was enabled on the Smart Dashboard, firewall was dropping the packets due to TTL check, causing the above problem.

To avoid such TTL drops, "Extended Cluster Anti-Spoofing" in case of Active-Active configurations with dynamic routing should always be disabled.

AUTO BACK-UP FEATURE ON NSF PRODUCTS

CR # Q01684913
Last Updated: 08/31/2007
Affected Releases: 2.3.6
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 11.1.1)

SSI RESTART CAUSES SNMP RESTART

CR # Q01303830
Last Updated: 08/31/2007
Affected Releases: 2.3.1
Current Status: Closed

SNMP registers with SSI daemon for handling events & alarms. The SSI daemon is getting restarted and this causes SNMP to restart. Since SNMP restarts, cold-start traps are being observed on each director intermittently.

This has been fixed in the new SSI patch, where SNMP daemon is separated preventing it from getting restarted whenever connection to SSI is lost.

DEFAULT GATEWAY IS VALIDATED AGAINST SSI SUBNET MASK AND NOT THE INTERFACE MASK

CR # Q01687079
Last Updated: 11/30/2007
Affected Releases: 2.3.6
Current Status: Closed

The firewall config daemon is using the SSI subnet mask instead of the interface subnet mask to validate whether the gateway address is valid or not. This causes the cfgd to not configure the gateway in the linux kernel.

This is fixed in 2.3.8 by removing the SSI validation and adding the validation to the regular cfgd validation function

SSH SECURID AND CP SECURID DOESN'T WORK SIMULTANEOUSLY

CR # Q01722998
Last Updated: 11/30/2007
Affected Releases: 2.3.6
Current Status: Closed

If both the features, SSH SecurID and CP SecurID are enabled at the same time, it leads to some compatibility problem.

After the fix in 2.3.8, both the SSH SecurID and CP SecurID can be configured simultaneously.

Please refer to the SecurID Enhancement section for more information.

LIMITATION NOTE FOR SNMP TRAPSRCIP

CR # Q01725521
Last Updated: 11/30/2007
Affected Releases: 2.3.6
Current Status: Closed

While configuring the SNMP traps (with '/cfg/sys/adm/snmp/adv/trapsrcip/' CLI) and syslog messages source IP (with '/cfg/sys/log/srcip' CLI), if 'unique' option is selected, then the source IP of the traps/syslog messages should be firewall IP address instead of the cluster IP. But, if the 'Hide Cluster Member's outgoing traffic behind the Cluster's IP Address' option is enabled in 'cluster properties -> 3rd Party Configuration' on the Smart Dashboard, then the traps/syslog messages are sent with the cluster IP instead of source IP. Unselect this option to send the traps/syslog messages with firewall IP as the source IP because when 'Hide outgoing traffic behind cluster member's ip address' option is selected, any packet originating from the iSD will have the cluster IP as the source IP and it'll over write any settings for trapsrcip or syslog srcip.

This is a limitation. Please refer to the CR Q01725521 for more info.

CP SECURID DISABLE / ENABLE NOT WORKING PROPERLY

CR # Q01722991
Last Updated: 09/07/2007
Affected Releases: 2.3.6
Current Status: Open

When we configure CP SecurID in the NSF, for the first time the Authentication through RSA Server is done successfully. But if we remove all the configurations related to CP SecurID from the CLI (for example, disabling and enabling again) and re-configure the same, the authentication is not happening properly.

ISD BOOT DELETE NOT WORKING PROPERLY FROM BBI

CR # Q01526730
Last Updated: 11/30/2007
Affected Releases: 2.3.5
Current Status: Closed

In a HA setup after disabling 'ha' and 'sync', changes are applied successfully after one isd is deleted using the directors tab in the BBI. But when the changes are applied after deleting the second isd, the following error message is displayed,

"internal exception, validation failed: can't read /network/hosts/2/networks/1/ports".

In 2.3.8, the 'isd del' option at the 'Operation / Directors' tab has been removed.

BACKUP/CLONE FAILS FOR DIFFERENT CP VERSIONS

CR # Q01742413
Last Updated: 11/30/2007
Affected Releases: 2.3.6
Current Status: No Fix Planned

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)

UNABLE TO CONFIGURE GRE TUNNEL THROUGH OSPF - APPLY FAILS

CR # Q01744444
Last Updated: 09/13/2007
Affected Releases: 2.3.7
Current Status: Open (Workaround available)

When you create a GRE tunnel with index other than the existing interface ID's, configuration is not successful. There seems to be a problem with the mapping of GRE tunnel ID.

As a workaround, configure GRE tunnel ID as one of the existing Interface ID's.

Issues Updated on 04/23/2007

FAILED TO LOAD THE VPN ACCELERATOR CARD MODULE AFTER UPGRADE FROM 2.3.X_R55 TO 2.3.6_R65

CR # Q01619281
Last Updated: 04/23/2007

Affected Releases: 2.3.6
Current Status: Open

Environment:
NSF5100 Firewall, build 2.3.6_R65

Checkpoint module 'CPacc3' for the VPN Accelerator card model # BCM5822 is not installed when we do upgrade from R55 to 2.3.6.0 R65 version in 5124 Firewalls. Hence the upgrade from any R55 based software version to 2.3.6_R65 on 5124 platform is not supported.

As a work around, users have to first upgrade from R55 to an R60 and then upgrade to 2.3.6_R65.

CHECKPOINT EXPRESS GATEWAY IS NOT WORKING PROPERLY IN R65

CR # Q01637091
Last Updated: 08/31/2007
Affected Releases: 2.3.6
Current Status: Closed

Environment:
NSF5100 Firewall, build 2.3.6_R65

With 2.3.6_R65 image, 'Checkpoint Express gateway' and 'Checkpoint Express gateway with SmartCenter server' are not configured properly when option 3 or 4 are selected while doing initial 'new' configuration.

This issue is fixed in 2.3.7

2.3.5 VRRP BACKUP FIREWALL USING VIRTUAL MAC ADDRESS

CR # Q01493746
Last Updated: 04/23/2007
Affected Releases: 2.3.4, 2.3.5
Fixed in Release: 2.3.6
Current Status: Closed

Environment:
NSF5100 Firewall, build 2.3.5_R6x

After VRRP failover, the VRRP backup firewall was transmitting packets with the source MAC address set to the VRRP virtual MAC address, and not its real MAC address.
This issue was happening due to the failure in resetting the backup firewall's MAC address to real MAC address. The issue was seen more under stress conditions.

In 2.3.6, a fix is added which brings down the interface and then resets the MAC address.

INCONSISTENT LINK DOWN SYSLOG MESSAGES IN VRRP CONFIGURATION

CR # Q01409969
Last Updated: 04/23/2007
Affected Releases: 2.3.4
Fixed in Release: 2.3.6
Current Status: Closed

Environment:
NSF5100 Firewall, build 2.3.4_R60

There are five issues involved in this CR. They are,

    a.   Sync up/down message does not appear
    b.   Port number does not appear, driver name appear
    c.   The message of link up/down is not consistent, i.e., only "100 Mbps Full-Duplex" appears
    d.   Eth1 down of VRRP Master causes eth0 up message though it's maintained up
    e.   Fail-over happens and MIP becomes Master, then eth0 and eth1 up messages appears

For the first three issues (a, b & c), the syslog messages are corrected to provide meaningful messages to the user.

The last two points (d, e) are working as per the design. Whenever VRRP fail-over occurs, all the interfaces MAC addresses have to be reset. For this, all the VRRP enabled interfaces are brought down and up again. Hence the user sees the link status change messages for all VRRP enabled interfaces.

DEFAULT GATEWAY MISSING AFTER FAILOVER ON VLAN TAGGED PORT

CR # Q01586553
Last Updated: 04/23/2007
Affected Releases: 2.3.5
Fixed in Release: 2.3.6
Current Status: Closed

Environment:
NSF5100 Firewall, build 2.3.5_R55 and 2.3.5_R60

In the in Active-Standby mode, whenever the master Firewall is halted, the default gateway is not seen on the new master.
This issue was seen when vlan tagging is enabled on the external interface. As all the interfaces are brought down and made up again after a fail-over, the default gateway is deleted but not re-configured. Deleting and adding the default gateway again after a fail-over shows the correct value.

This is fixed in 2.3.6. After a fail-over, an additional default gateway configuration function call has been added which will re-configure the default gateway.

SNMP TRAP SOURCE IP INCORRECT WITH CERTAIN TYPE OF CONFIG

CR # Q01246421
Last Updated: 04/23/2007
Affected Releases: 2.3.1
Fixed in Release: 2.3.6
Current Status: Closed

Environment:
NSF5100 Firewall, build 2.3.1_R60

SNMP trap source IP is incorrect with certain type of configuration.
When the trap source IP is set to 'Auto', the packets were sent with host IP of the firewall, when the trap source IP is set to 'MIP', the packets were sent with VRRP IP and when the trap source IP is set to 'Unique', the packets were sent with interface IP address.

This is fixed in 2.3.6. Check Point daemon which controls all the traffic that's coming in/out of firewall, automatically configures the source IP irrespective of trap source IP configuration.
As the Check Point daemon has the highest priority, any settings on the 'setsrcip' module had no effect on the behavior. Modified the code to give highest priority to the 'setsrcip' module, which then corrected the trap messages behavior.

SYSTEM SHOWS ZERO VALUE FOR ALL HARDWARE SENSOR INFOMATION UNDER STRESS TEST

CR # Q01156694
Last Updated: 04/23/2007
Affected Releases: 2.3.2
Fixed in Release: 2.3.6
Current Status: Closed

Environment:
NSF5100 Firewall, build 2.3.2.2_R60

During the stress testing, it had been observed that the hardware sensor information shows incorrect information. The sensor values for all CPU, Board Temperature, and System Fan of the master ISD were '0'. Even after stopping the stress test the values were still '0'.

The problem was related to the sensor chip driver, which automatically gets unloaded under heavy stress. Hence all the sensor values were reset to '0'.

In 2.3.6, an additional check has been added which checks if the driver is unloaded. If yes, it won't reset the sensor values to '0', but will try to re-load the driver for a predefined no. of times. By then the driver gets loaded properly and the sensor values will reflect the correct status.

NOT ABLE TO INSTALL ISO IMAGE ON 5100 NE MODELS WITH 160 GB HDD

CR # Q01530693
Last Updated: 04/23/2007
Affected Releases: 2.3.5
Fixed in Release: 2.3.6
Current Status: Closed

Environment:
NSF5100 Firewall, build 2.3.5_R60

Installation fails when installing NSF5100 iso image on NE models with 160 GB HDD. The latest NSF5100 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 run 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-2.3.6 release and would like to upgrade to 2.3.6, then this issue is not applicable. That will happen 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 NSF5100 series firewall Release notes version 2.3.6.

Fore more information, please refer to the NSF5100 series firewalls customer support bulletin ID: 2007007923, Rev 1.

CHECK POINT SYNCHRONIZATION STATUS IS SHOWN AS "HA MODULE NOT STARTED" AFTER UPGRADING TO 2.3.6

CR # Q01588691
Last Updated: 08/31/2007
Affected Releases: 2.3.6
Current Status: Closed

Environment:
NSF5100 Firewall, build 2.3.6_R60

After upgrading from 2.3.x_R60 to 2.3.6_R60, the Check Point's synchronization status is shown incorrectly. Running 'cphaprob stat' command from the root mode shows the status as "HA module not started".

This issue is fixed in 2.3.7 and 'cphaprob stat' shows proper output when it is executed from root prompt. Please refer to the CR notes for more info.

SYSLOG SRCIP DOES NOT WORK, DEPENDS ON CONFIGURATION

CR # Q01355224
Last Updated: 04/23/2007
Affected Releases: 2.3.4
Fixed in Release: 2.3.6
Current Status: Closed. Working as per design

Environment:
NSF5100 Firewall, build 2.3.4_R55 and 2.3.4_R60

After changing /cfg/sys/log/srcip to auto|unique|mip, syslog packet had same source ip which is the interface address that the syslog packet has been sent from.

This issue is similar to CR # Q01246421, and is fixed in 2.3.6.

NSF 5111(V2.3.3.0) NIC LEDS STATUS DIFFERENT FROM THE HW GUIDE

CR # Q01347061
Last Updated: 04/23/2007
Affected Releases: 2.3.x
Current Status: Closed

Environment:
NSF5100 Firewall, build 2.3.3_R60

The observed behavior of Gig Ports NIC LED status is different from the explanation on the user manual (Nortel Switched Firewall 5100 Series Release 2.3.3 Hardware Installation Guide). The correct LED status is observed and the user guide will be modified accordingly in the next release to reflect the changes. For more information please refer to the CR notes.

CPSYN NOT UP WHEN UPGRADED FROM 2.3.5 R60 TO 2.3.5.13 R65 WITH CP SECID ENABLED

CR # Q01573879
Last Updated: 08/31/2007
Affected Releases: 2.3.6
Current Status: Closed

Environment:
NSF5100 Firewall, build 2.3.6_R60

After upgrading from 2.3.5.R60 to 2.3.6_R65, running the Check Point sync status command 'cphaprob stat' from the root prompt is showing the status as "HA module not started" on one cluster member and on the other, the status is shown as 'active'.

This issue is seen when we upgrade from 2.3.5_R60 to 2.3.6_R65 with SecurID configuration enabled on the Check Point.

After the fix in 2.3.7, the status of sync is 'active' and the securid is also enabled after upgrade

Issues Updated on 12/14/2006

EVENTIA REPORTER DOES NOT GENERATE REPORTS PROPERLY

CR # Q01464653
Last Updated: 12/07/2005
Affected Releases: 2.3.5.1
Current Status: Open

Environment:
-        NSF5100 Firewall, build 2.3.5.1_R62

There are few cases where eventia reporter does not generate reports properly. For more information please check the CR# Q01464653

EVENTIA REPORTER IS GIVING PROBLEM, WHEN CONFIGURED IN DISTRIBUTED MODE

CR # Q01511853
Last Updated: 08/31/2007
Affected Releases: 2.3.5.1
Current Status: No Fix Planned

Environment:
-        NSF5100 Firewall, build 2.3.5.1_R62

Eventia Reporter does not work properly, when configured in Distributed Mode. Eventia Reporter is supported only in Standalone mode, but not in Distributed mode.

Issues Updated on 09/19/2006

STATIC RT MISSING IN UPGRADED BOX IF A SMART CLIENT IS ADDED IN A NON EMC SETUP

CR # Q01451030
Last updated: 08/31/2007
Affected Releases: 2.3.5
Current Status: Closed
Environment:
- NSF5100 firewall, build 2.3.5.

Before upgrading to 2.3.5, if any smart clients are configured in a cluster setup, already configured static routes will be lost after upgrading to NSF 2.3.5. Before upgrading , the smart client's that are configured in the non-emc mode should be deleted in order to make the upgradation successful.

CHECKPOINT ALERTS RECEIVED WHEN ISDS STRESSED WITH HIDE NATED CONNECTIONS

CR # Q01469502
Last updated: 08/31/2007
Affected Releases: 2.3.5 R55
Current Status: No Fix Planned

Environment:
- NSF5100 firewall, build 2.3.5 R55

In a cluster setup with sync is enabled, hide NAT (behind GW & also IP) is configured. If HTTP Traffic passed at 2500 connections per second (around 47k connection), the CP management station showed alerts for unavailability of ports for doing Hide NAT

As a work around, reduce the TCP end time out from 20 seconds to 5 seconds. The TCP end timeout can be configured on the CP management station SmartDashboard ->Policy ->Global Properties->Stateful Inspection -> TCP end timeout.

TRAFFIC DOES NOT CONTINUE AFTER A FAILOVER IN AA MODE

CR # Q01475323
Last updated: 08/31/2007
Affected Releases: 2.3.5 R60
Current Status: No Fix Planned

Environment:
- NSF5100 firewall, build 2.3.5 R60

In a cluster setup with AA is configured and sync is enabled. If HTTP Traffic passed at 3500 connections per second, after failover traffic failed to continue.

As a workaround, reduce the TCP end time out from 20 seconds to 5 seconds. It can be done in CP management station from Smart dashboard ->Policy ->Global Properties->Stateful Inspection -> TCP end timeout

HOST IP'S ARE CONFIGURED AS SYSLOG SERVERS

CR # Q01451297
Last updated: 08/31/2007
Affected Releases: 2.3.5
Current Status: Closed

Environment:
- NSF5100 firewall, build 2.3.5

A new validation is added to throw error message when Host IPs are used for configuring syslog servers. Upgrading to 2.3.5 will cause trouble if the syslog servers are configured wrongly.
To resolve this issue make sure host ips are not configured as syslog servers before upgrading to 2.3.5

NTP SYNCHRONIZATION ERRORS IN ASF5109 VER2.3.1

CR # Q01371193
Last updated: 10/05/2006
Affected Releases: 2.3.5
Current Status: Ready To Verify

Environment:
- NSF5100 firewall, build 2.3.5

In a cluster setup, some times synchronization is lost continuously due to ntp drift. A new ntphealthcheck script has been provided in this release, which continuously monitors the NTP service for any drift. Whenever the drift occurs, this script would stop the ntp service, synchronize the hardware clock, synchronizes the time manually with the NTP server and then starts the NTP service. If the problem is still persists, please reboot the MIP iSD to fix this issue. Refer CR # Q01371193 for more info.

SYSLOG SERVER NOT GETTING UPDATED AFTER UPGRADED TO 2.3.4.18_R61

CR # Q01457794
Last updated: 08/31/2007
Affected Releases: 2.3.5
Current Status: No Fix Planned

Environment:
- NSF5100 firewall, build 2.3.5

In a cluster setup, when syslog servers are configured in 2.2.7.0 R55 and upgraded to 2.3.5.0 R61, configured syslog servers are missing after the upgrade. The same issue can be seen when we do upgrade from 2.2.7.0 R54 to 2.3.5.0 R55.
As a workaround, re-configure the syslog servers manually after upgrade.

L2 FIREWALL NOT WORKING IN 2.3.5.0 R55

CR # Q01460850
Last updated: 08/31/2007
Affected Releases: 2.3.5
Current Status: No Fix Planned

Environment:
- NSF5100 firewall, build 2.3.5 R55

In a cluster setup L2 firewall is not working with 2.3.5.0. R55.

As a workaround, remove/disable the option for 'drop out of state ICMP packets' options in SmartDashboard -> Policies -> Global Properties -> Stateful Inspection -> Out of state packets.

CP R61, AFTER CONFIGURING/ENABLING QOS ON INTERFACE GETTING THE WARNING MESSAGE

CR # Q01464594
Last updated: 15/10/2006
Affected Releases: 2.3.5
Current Status: Open

Environment:
- NSF5100 firewall, build 2.3.5 R61

While configuring Check Point QoS on NSF5100 2.3.5_R61 box, while configuring the cluster/host properties, some alert messages would be displayed on the SmartDashboard as "No activate interface defined for QOS". However, the QoS works fine even after the alert messages.

This issue has been reported to Check Point and for now, these messages can be ignored.

2.3.4.0: UNABLE TO SEND SYSLOG AND SNMP TRAP

CR # Q01394047
Last updated: 03/29/2007
Affected Releases: 2.3.5
Current Status: Closed

Environment:
- NSF5100 firewall, build 2.3.5

NSF5100 supports sending alarms & traps whenever the CPU load reaches above a particular threshold value. But the logic to detect the threshold is not correct, due to which no traps or alarms could be sent.

Corrected the logic, which now sends the SNMP traps correctly and proper syslog messages when the CPU usage is reached to the Maximum (100%).

Issues Updated on 03/31/2006

EVENTIA REPORTER CLI IS MISSING

CR # Q01403593
Last updated: 04/08/2006
Affected Releases: 2.3.4.1
Current Status: Open
Environment:
-        NSF5100 firewall, build 2.3.4.0_R60 in EMC mode

After upgrading to NSF 2.3.4.1, when we try to enable the Eventia Reporter feature through CLI, the CLI menu for Eventia is missing.

Eventia Reporter feature is not supported in NSF 2.3.4.1.

ESL: KEVLAR OSPF SPF INTERVAL TIMER CAN BE SET AS 0

CR # Q01333862
Last updated: 21/03/2006
Affected Releases: 2.3.1, 2.3.3, 2.3.4
Current Status: Open

Environment:
-        NSF5100 firewall, build 2.3.4.0_R60

OSPF spf interval timer can be set as 0, which can make spf to run continuously.

It suggests that the spf value should not be set 0, as this will result in the continuous execution of spf timer which will have adverse affect on the CPU load.

COULDN'T GET THE INTERFACE STATUS PAGE FROM BBI AFTER UPGRADING TO 2.3.4.0_R60

CR # Q01330359
Last updated: 08/31/2007
Affected Releases: 2.3.4
Current Status: Closed

Environment:
-        NSF5100 firewall, build 2.3.4.0_R60

Symptom:
- Configure HA cluster with 2.3.3.0_R60 version
- Configure 1000 static routes & 65 interfaces
- Upgrade to 2.3.4_R60 version

With the above configuration, after upgrading the cluster, the users could not get the interface status page from WebUI (*Config -> Network -> Status -> Interface*). After clicking on this tab, the other tabs were not working. While getting the interface status page from the WebUI, the CPU usage reached 100% and it took 5 minutes to come down.

This is already fixed in 2.3.5

SNMP TRAP SOURCE IP IS NOT CORRECT WHEN TRAP SOURCE IP SET TO MIP

CR # Q01319328
Last updated: 08/31/2007
Affected Releases: 2.3.1, 2.3.3, 2.3.4
Current Status: Closed

Environment:
- NSF5100 firewall, build 2.3.4.0_R60

Symptom:
- Configure HA cluster
- Enable SNMP (/cfg/sys/adm/snmp/ena)
- Set read access control (/cfg/sys/adm/snmp/access)
- Set trap event and alarm (/cfg/sys/adm/snmp/events y/alarm y)
- Enter trap host IP (Provide internal host IP. /cfg/sys/adm/snmp/host)
- Provide the community string (public)
- Provide the trap source ip (/cfg/sys/adm/snmp/adv/trapsrcip) as MIP
- Start SNMP agent in internal host machine
- Apply the changes

In the above configuration, plug out the VRRP master's cable to observe the trap for VRRP master change. Check the source IP in the SNMP agent. Source IP is kevlar internal interface IP instead of MIP.

This is closed since it is working as expected.

ER DOES NOT WORK AFTER BOOT DELETING THE BOX IN EMC MODE.

CR # Q01328134
Last updated: 03/14/2006
Affected Releases: 2.3.4

Current Status: Open

Environment:
- NSF5100 Firewall, build 2.3.4.0_R60

Configure the basic setup of Kevlar in EMC mode with 2.3.4.0_R60 and then enable Eventia Reporter in Distributed mode. Now issue /boot/delete and configure the box again with 'new' process. The current state of ER in CLI shows disabled. If Eventia Reporter is configured in Local mode Kevlar throws the error message: "disable the ER first and then enable it again to configure in Local mode".

Boot deleting the box does not uninstall/disable the ER, although the CLI shows it as disabled. "rpm -qa" still shows the CPrt_unify-R60-00 package installed. If the same mode is selected after boot delete, the box throws warning message for reboot though it does not happen.

As a workaround, the user is requested to first enable ER (in Distributed mode), then disable and then re-enable the ER.

WEB [UI] - "PRODUCT TYPE" IS SHOWN WITH INCORRECT HARDWARE TYPE FOR MIX PLATFORM

CR # Q01333945

Last updated: 03/21/2006
Affected Releases: 2.3.1, 2.3.3, 2.3.4
Current Status: Open

Environment:
NSF5114 firewall, build 2.3.4.0_R60

Setup HA/Sync system with build 2.3.4.0b_R60 on mix platform (5124-ne1 for iSD1 and 5124 for iSD2).

From BBI, go to "Administration->Monitor->Director(s)" tab, select an iSD and click on "Refresh" button:
- If the VRRP master is iSD1, the product type is shown "NSF-5124-NE1" for both iSD1 and iSD2
- If the VRRP master is iSD2, the product type is shown "NSF-5124" for both iSD1 and iSD2

WEB SERVICE IS STILL RUNNING WHEN DISABLING IT BY "CFG/SYS/ADMIN/WEB/HTTP/DIS"

CR # Q01316824
Last updated: 03/02/2006
Affected Releases: 2.3.1, 2.3.3, 2.3.4
Current Status: Open

Environment:
- NSF-5100 firewall build 2.3.4.0_R60

Even after disabling the web service (http) using the CLI command "cfg/sys/adm/web/http/dis", it would be still running. This can be viewed by command /info/clu or "ps –A | grep httpd" from root prompt.

Issues Updated on 09/28/05

FAIL-OVER DOESN'T WORK WITH USER AUTHENTICATION ON VRRP H/A

CR # Q01233372
Last updated: 08/31/2007
Affected Releases: 2.3.3
Current Status: Closed

Environment:
- NSF5100 Firewall, build 2.3.3.0_R60

Configure 'user authentication' for the traffic between the internal & external networks and install the necessary policies to allow the traffic between the internal & external hosts.

From the client, run an ftp operation to get a file from the external server (user is authenticated). While the file transfer is in progress, do a fail-over by unplugging the cable or by rebooting the VRRP Master, the file transfer stops and the ftp session is closed.

As per the Check Point design, the user authentication doesn't support a state-full fail-over. Due to this, after a fail-over, the open sessions will be closed. Hence, the users need to open a new session.

THE CP SYNC IS DOWN WITH 68 INTERFACES IN HA MODE AFTER REBOOTING THE SYSTEM

CR # Q01235159
Last updated: 10/06/2005
Affected Releases: 2.3.3
Current Status: Open

Environment:
- NSF5100 Firewall, build 2.3.3.0_R60

It's been observed that, when configuring 68 interfaces with Check Point Sync enabled, the system works fine initially. But after rebooting any one of the Firewalls, the CP Sync shows 'down'. The System works fine with less than 68 interfaces.

Contact the Nortel Technical support for more information & workaround on this problem.

CP FAILS TO GET TOPOLOGY FROM L3-BRIDGE WITH VLANID IN HA

CR # Q01210529

Last updated: 10/06/2005
Affected Releases: 2.3.3
Current Status: Open

Environment:
- NSF5100 Firewall, build 2.3.3.0_R60

It's been observed that when configured large number of L2-L3 bridge interfaces, the 'get topology' operation from the Check Point SmartDashboard sometimes failed with an error message displayed as "*Failed to connect to FW1 (IP address: '10.10.1.1'). Please make sure that Check Point services are running on FW1 and trust has been established*".

When the normal VRRP interfaces & bridge interfaces are configured in a way that they share the same ports with different VLAN ID's, the 'get topology' operation takes a long time (>10 minutes) to succeed or it sometimes returns with an error message as above.

As a work around, it's suggested to configure normal VRRP interfaces and bridge interfaces on different ports so that the above-mentioned scenarios can be avoided.

The scenario has also been seen when configuring large number of normal VRRP interfaces (>50) interfaces. The following table shows an approximate time taken for the 'get topology' operation when configuring large number of interfaces.

# of interfaces	Approx. time
50	10 minutes
70	30 minutes
>100	1 hour

[BBI] TICKER SHOWS INCORRECT INFORMATION ABOUT THROUGHPUT

CR # Q01157972
Last updated: 10/06/2005
Affected Releases: 2.3.3
Current Status: Open

Environment:
- NSF5100 Firewall, build 2.3.3.0_R60

After launching the Ticker application from the BBI, and keep it running for longer durations (ex: one day), the cluster information shows incorrect throughput information as fairly large negative numbers. This happens randomly and while running the ticker for long durations.

As a work around, users are suggested to close the Ticker page and re-launch the ticker application again.

L3-BRIDGE: OSPF WORK ON A DISABLED VRRP INTERFACE

CR # Q01203464
Last updated: 08/31/2007
Affected Releases: 2.3.3
Current Status: Closed

Environment:
- NSF5100 Firewall, build 2.3.3.0_R60

Configure basic VRRP HA setup with Sync enabled as the following:
- Port1 for Sync and Check Point management network
- Create a normal VRRP interface if # 2 on port 2
- Create a normal VRRP interface if # 3 on port 4
- Disable if # 3 and add a L3-bridge interface in the same subnet as if # 3
- Enable OSPF and enable OSPF for the disabled VRRP interface (if # 3)

Since OSPF is a network specific protocol and not interface specific, OSPF will start advertising the disabled interface network (if # 3) and both the Firewalls form adjacency between them via the bridge interface (since its on the same network as the disabled interface if # 3).

During zebra configuration, the system will check only whether the interface is enabled for OSPF. There is not any checking to see whether the actual physical interface is enabled.

This is fixed in 2.3.7

HIDE-NAT NOT WORKING PROPERLY IN VRRP AA SETUP

CR # Q01191170
Last updated: 08/31/2007
Affected Releases: 2.3.3
Current Status: Closed

Environment:
- NSF5100 Firewall, build 2.3.3.0_R60

Configure the basic VRRP AA setup
Configure the Hide NAT for internal network
Configure the internal and external hosts to your VRRP group1 IP's as Gateways

Start ping from internal to external host and observe the source IP of the packet in the external host. The ping request packets are sent with source IP as the IP address of the VRRP group2 whereas it should be the VRRP IP address of group1. Due to this mismatch, the first packet reply from external host for any connection is dropped at the Firewall citing the out of state (reply doesn't match the previous request).

As a work around, instead of using automatic Hide-NAT rules on the cluster, generate them in accordance with the router decision function; i.e., configure Hide-NAT for VRRP groups configured IP as a separate object in manual NAT rule base (hence two rule bases, one for each VRRP group).

QOS POLICY NOT GETTING DOWNLOADED AFTER THE UPGRADE

CR # Q01188039
Last updated: 08/31/2007
Affected Releases: 2.3.3
Current Status: Closed

Environment:
- NSF5100 Firewall, build 2.3.3.0_R60

Load 2.2.7.0_R54 image and configure the Firewall in SmartCenter Server mode (EMC), enable Floodgate and download all the necessary QoS policies, and then upgrade to 2.3.3 version using cdrom. After the upgrade is successful, and when the user tries to load the QoS policy, the policy installation fails with an error displaying "Error: Failed to receive interface list".

This is already fixed in 2.3.6

MAINT/BACKUP/LOCAL COMMAND FAILS IN STAND-ALONE MODE

CR # Q01198129
Last updated: 10/06/2005
Affected Releases: 2.3.3
Current Status: Open

Environment:
- NSF5100 Firewall, build 2.3.3.0_R60

It's been observed that /maint/backup/local command fails some times, especially after a reboot of the Firewall. The reason for this is, to handle the race condition (i.e., when multiple instances of backup/local command run at the same time); a locking mechanism has been introduced. And after a reboot, the command fails to delete the lock and hence the command fails. This scenario occurs randomly.

As a work around to this problem, check if */var/tmp/maint_backup.lock* file exists. If the file exists, delete this file and try again. If the problem persists, reboot the Firewall on which the /backup/local command is failing and it'll solve the problem.

SECURID DOESN'T WORK WITH HIDE-NAT IN HA MODE

CR # Q01184682
Last updated: 10/06/2005
Affected Releases: 2.3.3
Current Status: Open

Environment:

- NSF5100 Firewall, build 2.3.3.0_R60

- Setup a HA cluster with 2.3.3.0 build with the following configuration
  - *Interface 2 for Checkpoint management*
  - *Interface 3 for client network: 10.8.90.0*
  - *Interface 4 for server network: 200.200.200.0*
  - *ACE server: 200.200.200.11*
  - *Server: 200.200.200.10*
  - *Client: 10.8.90.205*

- Setup SecurID with User Authentication:
  - *Create a group Admin contains 2 users: user1 (SecurID user), user2 (Checkpoint password user).*
  - *Add a rule to allow service? Authenticated? action ?User Auth?, source?Admin@Any? And destination? Any?*
  - *Add a rule to allow securID traffic with source? ACE server, Cluster_HA? And destination? Any?*

- Enable Hide NAT on network 200.200.200.0 with behind gateway method and install policy

- From client ftp to server 200.200.200.10, verify with both of secured user and Checkpoint password user.

With the above configuration, the Client can ftp to Server after authenticating successfully with user2 (Check Point password user), but cannot authenticate with user1 (SecurID user) and SmartView Tracker shows dropped ftp packets with reason SecurID request failed.

To make SecurID work with Hide-NAT in HA, the users need to configure Hide NAT for network object and exclude real IP address.

SESSION FAILOVER NOT WORKING WITH SYNC PORT IN VLAN

CR # Q01188074
Last updated: 08/31/2007
Affected Releases: 2.3.3
Current Status: Closed

Environment:
- NSF5100 Firewall, build 2.3.3.0_R60

NSF 2.3.3 with R60 doesn't support configuring Sync port in a VLAN. Due to this, the session fail-over doesn't happen and */maint/fw/sync* command from the CLI shows the other host as down.

 It's suggested that the user to dedicate a port for Check Point Session Synchronization and do not configure the sync port in a VLAN.

THE POLICY IS NOT DOWNLOADED TO THE FIREWALL AFTER UPGRADING FROM R55 TO R60

CR # Q01194543

Last updated: 10/06/2005
Affected Releases: 2.3.3
Current Status: Open

Environment:
- NSF5100 Firewall, build 2.3.3.0_R60

Since 2.3.3 comes with Check Point R60, it has a certain upgrade procedure and the user needs to re-install the policies on the Firewall after upgrade.

Refer to the NSF5100 2.3.3 User Guide for the correct upgrade procedure.

SYSTEM COULDN'T CLEAR THE OSPF ROUTES WITH 200 ROUTES

CR # Q01163068
Last updated: 10/06/2005
Affected Releases: 2.3.3
Current Status: Open

Environment:
- NSF5100 Firewall, build 2.3.3.0_R60

Enable OSPF on the NSF Firewall and advertise 200 routes by using a traffic generator. Then stop the traffic and disconnect the link between the traffic generator and the Firewall and let the Firewall idle for about 30 minutes. Here, the all the dynamically learned routes should get deleted, and /info/net/route/ospf/routes doesn't show any routes. But from the Check Point Smart Dashboard, 'get interfaces with topology' operation still shows the networks reside behind the OSPF interface for each OSPF route learned from the traffic generator.

This issue has been forwarded to Check Point and the fix/updates on this are still awaited.

RESTRICTION VIA HOSTS.ALLOW FILE DOESN'T WORK FOR SMARTPORTAL

CR # Q01155340
Last updated: 08/31/2007
Affected Releases: 2.3.3
Current Status: Closed

Environment:
- NSF5100 Firewall, build 2.3.3.0_R60

The file to be used for limiting access to Smartportal service is, hosts.allow. The access limitation works fine with the hosts.allow file.

SERVICES DHCP_REQ… AND DHRP_REQ… NEED TO BE EDITED TO ACCEPT DHCP TRAFFIC

CR # Q01181504
Last updated: 10/06/2005
Affected Releases: 2.3.3
Current Status: Open

Environment:
- NSF5100 Firewall, build 2.3.3.0_R60

After adding a Firewall rule by selecting 'dhcp-rep-localmodule' and 'dhcp-req-localmodule' for allowing DHCP traffic between the internal & external networks, the clients cannot still receive the IP address from the DHCP servers. And the Check Point logs show that DHCP packets are being dropped.
To allow DHCP traffic pass through the internal & external networks, select the 'bootp' service as 'dhcp-rep-localmoudle' and dhcp-req-localmodule' are used for some other purposes.

VPN S2S WITH STANDALONE SYSTEMS: NEED SOME WORK AROUND STEPS

CR # Q01215993
Last updated: 08/31/2007
Affected Releases: 2.3.3
Current Status: Closed

Environment:
- NSF5100 Firewall, build 2.3.3.0_R60

PARTITION HDA3 OF ISD IS REACH 99% AFTER DOING UPGRADING

CR # Q01201687
Last updated: 08/31/2007
Affected Releases: 2.3.3
Current Status: No Fix Planned

Environment:
- NSF5100 Firewall, build 2.3.3.0_R60

When the user tries to upgrade from 2.2.3.x or 2.2.4.x to 2.2.7.0 later to 2.3.x version, the hda3 partition of iSD reaches 99% usage and the user gets an alert message on the console.

The reason for this is, in 2.2.x versions (prior to 2.2.7.0), the partition sizes were smaller for HDA3 partition, and our upgrade procedure requires that all the previous Check Point information be stored and install the new Check Point version on the same partition. Due to this, the partition usage goes higher.

But the partition sizes have been changed to handle these kinds of scenarios from 2.2.7.x version onwards. Hence whenever the user comes across this situation, it's suggested that they re-image the iSD with 2.2.7 or 2.3.1 through iso image and then upgrade to 2.3.3 version.

Issues Updated on 07/13/2005

STATIC ROUTES ARE NOT DELTED AFTER /BOOT/DELETE

CR # Q01176213
Last updated: 07/13/2005
Affected Releases: 2.3.1
Current Status: Fixed

Environment:
- NSF5100 Firewall, build 2.3.1.0_R55

To remove the configuration and set the Firewall to factory default settings, the users are provided with /boot/delete command. However, after doing a /boot/delete, the static routes that are configured on the system are not getting deleted.

The reason for this is, the zebra config file used to store the static routes information is not getting deleted during the teardown process.

To work around this problem, go to the root prompt and delete the /config/tdo/conf/zebra.conf file. This will cause the configuration to get erased.

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

CR# Q01106902-01
Last Updated: 07/13/2005

Affected Releases: 2.3.1.0
Current Status: Open

Environment:
a) In ASF-5100 2.3.1.0 Standalone/Cluster setup

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 wrapping and could cause problems where hcd will not send health check packets, proxy arp settings and default gateway settings will not be updated after VRRP fail-over etc.

To verify, please login as root and run "uptime" to see if the system has been up for more than 248 days.

The work around for this problem is to login as '*root*' and run the following commands in each firewall.

service hcd stop
service cfgd restart
service hcd start

Issues Updated on 05/22/2005

ENABLE OSPF REDISTRIBUTION WILL MAKE THE GRE TUNNEL UP/DOWN CONTINUOUSLY

CR# Q01052791
Last Updated: 08/31/2007
Affected Releases: 2.3.1
Current Status: Closed

OSPF connected redistribution is not supported on GRE.

WMON DOESN'T WORK FOR THE FILTER OPTION "NET"

CR# Q01054089
Last Updated: 08/31/2007
Affected Releases: 2.3.1
Current Status: No Fix Planned

Environment:
-        NSF5100 build 2.3.1_R55 in HA mode

Symptom:
-        Ping from internal network to external network.
-        Provide the command /info/fwmon
-        Select "net" in the filter option
-        Select a protocol number
-        Provide the source and destination net addresses.

Check Point's '*fw monitor*' command with *net* option doesn't work for local IP addresses.

BBI: RESETTING SIC OPERATION FROM WEB BROWSER REACHES TIMEOUT

CR# Q01052205
Last Updated: 08/31/2007
Affected Releases: 2.3.1
Current Status: No Fix Planned

Environment:
-        NSF5100 build 2.3.1_R55 in stand alone mode

Symptom:
-          Configure access list for allowing the user to connect to the iSD through BBI
-          Enable management support on the VRRP interface using */cfg/net/if #/mgmt y/apply*
-          Login to iSD through BBI using the VRRP IP address
-          Go to reset SIC page and reset the SIC connection

When the SIC is reset, Check Point reloads all the default policies and hence the user would not able to connect through the VRRP interface. Added a fix to stop loading the default policy when the SIC is reset. However, the user needs to re login to the BBI, since VRRP services are restarted whenever SIC is reset and the connection to the VRRP interface is lost.

TSDUMP DOESN'T WORK AFTER BREAKING BY CTL+C

CR# Q01059503, Q01048974, Q01048977
Last Updated: 05/22/2005
Affected Releases: 2.3.1
Current Status: Open

Environment:
-          NSF5100 build 2.3.1_R55 in HA mode

Symptom:
-          Run tsdump from CLI "/maint/tsdump/dump"
-          Press "CTL + C " to break the dump process

/maint/tsdump command tries to capture the firewall logs using '*fw log*' command and if the firewall logs are huge, the CLI command will be timed out and the user cannot complete the tsdump operation.
In another scenario, when executing */maint/tsdump* or */info/fwmon* or */info/ethereal* command and press a CTL+C, the commands would still be running in the background and hence the user would not be able to re-run these commands unless the background process completes.

As a work around, the user is requested to wait for the command execution complete or the timeout and then try other commands.

DYNAMIC NAT IS FAILED ON LAYER 3 BRIDGE

CR# Q01040018
Last Updated: 05/22/2005
Affected Releases: 2.3.1
Current Status: Open

Environment:
-          NSF5100 build 2.3.1_R55 in stand alone mode

Symptom:

-           Prepare iSD Layer3 Firewall environment
-           Do */info/clu* command to verify the iSD is up and running with the correct information
-           Configure an external interface *(/cfg/net/if #/addr1 <IP>/mask <mask>/port #/ena/apply)*
-           Configure the bridge as layer 2 configuration (*/cfg/net/br #/addr1 <IP>/mask <mask> ports/add #/add #/ena y/apply)*
-           Configure on CP Mgmt GUI:
-           Create new Check Point Gateway iSD1's IP address
-           Enable FW-1 by going to "General properties":
-           Check on Firewall-1 to enable FW-1:
-           Do "Communication -> Test SIC status" to get SIC connection for first cluster member.
-           Do "Topology -> Get Interface with Topology" to get the interface and topology.
-           Get version
-           From CPGUI Client, enable Hide NAT on network 10.8.90.0 with address 0.0.0.0
-           Add rule allow http traffic from network 10.8.90.0 to the external interface network and push policy to iSD1
-           Run "Ether peek" on Server and capture HTTP traffic
-           From the Client 10.8.90.205, browse Server's web page using the external interface ip address (*if #/addr1*)

The above configuration is not valid. Dynamic NAT is used to NAT traffic flowing from the hosts inside the internal network to the external network. But in the above configuration, the user tried to NAT the external network traffic.

This feature (Dynamic NAT on external interface) on L2 firewall is not supported in the current version of NSF5100.

BBI: ALL KEVLAR CONFIGURATION IS DESTROYED WHEN IMPORTING EMPTY FILE

CR# Q01048980
Last Updated: 05/22/2005
Affected Releases: 2.3.1
Current Status: Open

Environment:
-           NSF5100 build 2.3.1_R55 in stand alone mode

Symptom:
-           Enable BBI support for the iSD
-           Create an empty file
-           From the BBI, go to Operation -> Configuration -> import/export page
-           Try to import the empty file with secret key

As per the current implementation of export configuration, any invalid or unrecognized settings in the imported file will be ignored and if nothing valid is found in the configuration file, default configuration will be applied to all the parameters in the system.

It is not possible to add any validation checks for the export utility as in the next major platform release, the configuration file format will be changed and the validations will be handled then.

For the current version, users are requested to take caution while exporting a configuration file and see if it's a valid configuration file and only then export.

HOST/USB-OHCI.C: FOUND OHCI DEVICE WITH NO IRQ ASSIGNED. CHECK BIOS SETTINGS!

Last Updated: 05/22/2005
Affected Releases: 2.3.1
Current Status: Open

Environment:
- NSF5100 build 2.3.1_R55

Symptom:
After the initial startup of the 5109 with 2.3 installed, we saw the following on the console:
host/usb-ohci.c: found OHCI device with no IRQ assigned. Check BIOS settings!
<3>Feb 28 12:37:09 a192-168-240-65 host/usb-ohci.c: found OHCI device with no IRQ assigned. Check BIOS settings!

In the 2.3.x version, we have provided the support of USB storage and OHCI device is used for USB devices. The reason for this log message is, in some hardware models, it may be possible that the USB controller support is disabled in the BIOS. When the NSF boots up with 2.3.x version, it searches for USB controller support and if it's disabled, this log message appears on the console.

CHECKPOINT DAEMON IS NOT STARTED AFTER HOST DELETE ACTION IN CLUSTER

CR # Q01137943
Last Updated: 05/22/2005
Affected Releases: 2.3.1
Current Status: Open

Environment:
- NSF5100 build 2.3.1_R55

Symptom:
- Configure a HA setup with a fresh install of 2.3.1_R55 software
- Delete host1 from the cluster setup
- Reboot host1

The 2.3.1_R55 version has a software limitation in which, if a user wants to delete a particular host from a cluster and make the other host as a stand-alone system, a certain method has to be followed without which the remaining Firewall might not work properly.

To fix this issue, an engineering document would be provided to all concerned which outlines the limitation and also the workaround for the same.

THE AUTONEGOTIATION'S FEATURE ON PORT HAVE PROBLEM WHEN DISABLED

CR # Q01070889
Last Updated: 05/22/2005
Affected Releases: 2.3.1
Current Status: Open

Environment:
-        NSF5100 build 2.3.1_R55

Some times, when set the auto negotiation option to off and set the port speed of Copper Gig ports to 1000Mbps, the port link doesn't come up correctly. Also, even when autoneg option is set to 'off', /info/host/link command might display the autoneg as 'on'.

The current network driver used with the Linux 2.4.20 kernel has some known issues with which sometimes the link up/down status has some problem with some legacy cards, in particular with 82541/82547 cards.

As a workaround, the user can set the autoneg option back to 'on' and the link up/down status is detected correctly.

PCI BUS SPEED IS SET TO 66MHZ, REGARDRLESS OF WHICH CARDS ARE INSTALLED, ON THE 5124-NE1 MODELS

Affected Releases: 2.3.1
Current Status: Open

Environment:
-        NSF5124-NE1 build 2.3.1.0_R55

The PCI bus speed is supposed to operate at a maximum of 133MHz, depending on the quantity and capability of the option cards installed. However, the bus currently operates at 66MHz regardless of which cards are installed. In addition, the second internal PCI bus that the on-board gigabit ports reside on currently operates at 100MHz. Both bus speeds have the potential to affect the overall system performance.

Even though this issue might affect the system performance of 5124-NE1 models, the decrease in the performance is quite low when compared with 5124 models. This is because, the Firewall performance

is linked more with the CPU processor and RAM capacity. However, the bus speed might have a greater impact while processing the large packets, which should pass through the PCI bus.

OSPF: ONE ISD COULD NOT SEE OTHER AS NEIGHBOR AND CPU HIT INTO 100%

CR # Q01046976-01
Last Updated: 05/22/2005
Affected Releases: 2.3.1
Current Status: Open

Environment:
- NSF5100 build 2.3.1.0_R55

In a cluster environment, enable OSPF on both the Firewalls and pump OSPF traffic from a traffic generator sending dynamic routes. After running the stress for 2 days, the two Firewalls fail to form adjacency between them. Checking the logs on one of the Firewall says '*fw_log_drop: Packet proto=89 10.8.100.2:513 -> 224.0.0.5:52 dropped by fw_conn_post_inspect Reason: fwconn_init_links failed*'. CPU usage shows 100% on both the Firewalls.

This issue happens intermittently under heavy load and when CPU usage shows 100%. When increased the spf interval on the Firewall, this problem has been solved. Also check the memory usage and delete the Check Point logs if necessary.

KEVLAR 2.3 BETA - SOMETIMES KEVLAR OPERATING IN PROMISCUOUS MODE

CR # Q01114346
Last Updated: 08/31/2007
Affected Releases: 2.3.1
Current Status: No Fix Planned

Environment:
- NSF5100 Firewall, build 2.3.1.0_R55

When the SSI management port is enabled on a VLAN, and the same port is shared by another VRRP interface, the ports seem to run in promiscuous mode.

The reason for this is, whenever virtual mac is set for a vlan interface, the parent interface goes into promiscuous mode. This is part of the kernel implementation. The change is necessary as the mac of the vlan interface has been change and the parent will not receive the packets destined for the virtual mac unless it goes into promiscuous mode.

14 APPENDIX–B: UPGRADE TIME

The following table provides an approximate time it takes for the upgrade process to complete. The time calculations are based on 2.3.1 release.

Platform	Download time in minutes	Activate & Reboot in minutes	Total time in minutes
5106	5	10	15
5111-NE1/5109	2	5	7
5114-NE1/5114	2	5	7