NORTEL NETWORKS™

How the world shares ideas.

NSF-5100 2.3.x

Readme

Version 1.4
15th October 2006

Nortel Networks, Inc.

Table of Contents

1 Introduction....1
2 Status of Known Issues and Limitations....2
3 Upgrading to NSF 2.3.x....4
4 Nortel Firewall System 5100, Version 2.3.1 (05/22/05)....6
4.1 Supported Hardware....6
4.2 Supported Check Point Releases....6
4.3 Notes on Newly Supported Features....6
4.4 Feature Limitations....6
4.4.1 OSPF: Limitations with OSPF & GRE....6
4.4.2 L2/L3 - Limitations with L2/L3 Bridge interfaces....7
4.5 Upgrading to NSF-5100 2.3.1....7
5 Nortel Firewall System 5100, Version 2.3.3 (10/26/05)....8
5.1 Supported Hardware....8
5.2 Supported Check Point Releases....8
5.3 Notes on Newly Supported Features....8
5.4 Feature Limitations....8
6 Nortel Firewall System 5100, Version 2.3.4 (03/29/06)....8
6.1 Supported Hardware....8
6.2 Supported Check Point Releases....8
6.3 Notes on Newly Supported Features....8
6.4 Feature Limitations....9
7 Nortel Firewall System 5100, Version 2.3.4.1 (08/02/06)....9
7.1 Supported Hardware....9
7.2 Supported Check Point Releases....9
7.3 Feature Limitations....9
8 Nortel Firewall System 5100, Version 2.3.5 (09/19/06)....9
8.1 Supported Hardware....9
8.2 Supported Check Point Releases....9
8.3 Notes on Newly Supported Features....9
8.4 Feature Limitations....11
9 Appendix-A: List of Known Issues....11
10 Appendix–B: Upgrade Time....32

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 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 2.3.x software release. 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 for the specific update date.

If 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 and ☑ means the issue is fixed the 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
Q01451030	STATIC RT MISSING IN UPGRADED BOX IF A SMART CLIENT IS ADDED IN A NON EMC SETUP	09/14/2006	Open Workaround available	N/A	N/A	N/A	N/A	☒
Q01453019	CPHAPROB STAT SHOWING "HA MODULE NOT STARTED" AFTER UPGRADE TO 2.3.4.17 R61	09/15/2006	Open Workaround available	N/A	N/A	N/A	N/A	☒
Q01469502	CHECKPOINT ALERTS RECEIVED WHEN ISDS STRESSED WITH HIDE NATED CONNECTIONS	10/14/2006	Open Workaround available	N/A	N/A	N/A	N/A	☒
Q01475323	TRAFFIC DOES NOT CONTINUE AFTER A FAILOVER IN AA MODE	10/15/2006	Open Workaround available	N/A	N/A	N/A	N/A	☒
Q01451297	HOST IP'S ARE CONFIGURED AS SYSLOG SERVERS	09/22/2006	Open Workaround available	N/A	N/A	N/A	N/A	☒
Q01371193	NTP SYNCHRONIZATION ERRORS IN ASF5109 VER2.3.1	10/05/2006	Ready To Verify	☒	N/A	N/A	N/A	☑
Q01457794	SYSLOG SERVER NOT GETTING UPDATED AFTER UPGRADED TO 2.3.4.18_R61	09/26/2006	Open Workaround available	N/A	N/A	N/A	N/A	☒
Q01460850	L2 FIREWALL NOT WORKING IN R55	10/05/2006	Open Workaround available	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	09/26/2006	Open Workaround available	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	03/17/2006	Open	N/A	N/A	☒	☒	☒
Q01319328	SNMP TRAP SOURCE IP IS NOT CORRECT	02/03/2006	Open	☒	☒	☒		N/A

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
	WHEN TRAP SOURCE IP SET TO MIP						☒	
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	10/26/05	Open	N/A	☒	☒	☒	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 INFORMATION ABOUT THROUGHPUT	10/26/05	Open Workaround available	N/A	☒	☒	☒	☒
Q01203464	L3-BRIDGE: OSPF WORK ON A DISABLED VRRP INTERFACE	10/26/05	Open Workaround available	N/A	☒	☒	☒	☒
Q01191170	HIDE-NAT NOT WORKING PROPERLY IN VRRP AA SETUP	10/06/05	Open Workaround available	N/A	☒	☒	☒	☒
Q01188039	QOS POLICY NOT GETTING DOWNLOADED AFTER THE UPGRADE	10/26/05	Open Workaround available	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	10/26/05	Open Workaround Available	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
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	10/26/05	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	10/26/05	Open Workaround available	N/A	☒	☒	☒	☒
Q01201687	PARTITION HDA3 OF ISD IS REACH 99% AFTER DOING UPGRADING	10/26/05	Closed Upgrade Procedures redefined	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	☒	☑	☑	☑	☑

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
Q01052791	ENABLE OSPF REDISTRIBUTION WILL MAKE THE GRE TUNNEL UP/DOWN CONTINUOUSLY	05/22/05	Open	N/A	N/A	N/A	N/A	N/A
Q01054089	FWMON DOESN'T WORK FOR THE FILTER OPTION "NET"	05/22/05	Open Workaround available	N/A	N/A	☒	☒	☒
Q01052205	BBI: RESETING SIC OPERATION FROM WEB BROWSER REACHES TIMEOUT	05/22/05	Open Workaround available	☒	☒	☒	☒	☒
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 WHEN IMPORTING EMPTY FILE	05/22/05	Open Workaround 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	05/22/05	Open	☒	☒	☒	☒	☒

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 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*".

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. Note that upgrading to NSF5100_2.3.5.0_R61.pkg from BBI is not supported as this package size too large. It can be done only from CLI. Refer CR# Q01451248 for more info.

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 2.3.5 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_2.3.5.0_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 2.3.5.0 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 are seeing both firewalls as '**up**'
- Check the CP sync status, and if the status is shown as 'HA module not started', disable and enable the synch. Refer to CR # Q01453019 for more details.

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_2.3.5.0_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
- 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*'
- 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
- 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*'
- 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 are seeing 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 y*)
- Both the firewalls will now reboot for updating the Check Point configuration
- After both the firewalls 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 are seeing 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

- **SSlbyPass Enhancement:**

While configuring an NSF Firewall in a standalone or in cluster mode, we first configure a management IP address and an MIP address to the Firewall(s). This management interface is used for communication 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 were 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 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

<u>**Issues Updated on 09/19/2006**</u>

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

CR # Q01451030
Last updated: 09/14/2006
Affected Releases: 2.3.5
Current Status: Open
<u>Environment:</u>
- NSF5100 firewall, build 2.3.5.

Before upgrading to 2.3.5, if any smart clients are configured in a cluster setup, static routes are missing after upgrading to NSF 2.3.5.
Work around is make sure to delete all the smart clients added in a cluster setup before upgrading to 2.3.5

9.1.1.2 CPHAPROB STAT SHOWING "HA MODULE NOT STARTED" AFTER UPGRADE TO 2.3.5 R61

CR # Q01453019
Last updated: 09/15/2006
Affected Releases: 2.3.5
Current Status: Open

<u>Environment:</u>
- NSF5100 firewall, build 2.3.5

In a cluster setup with sync is enabled, when we upgrade to 2.3.5, ‘cphaprob stat’ shows “HA

module not started" message.
As a work around, after upgrade disable and enable the sync, then 'cphaprob stat' shows the correct output.

9.1.1.3 CHECKPOINT ALERTS RECEIVED WHEN ISDS STRESSED WITH HIDE NATED CONNECTIONS

CR # Q01469502
Last updated: 10/14/2006
Affected Releases: 2.3.5 R55
Current Status: Open

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.

9.1.1.4 TRAFFIC DOES NOT CONTINUE AFTER A FAILOVER IN AA MODE

CR # Q01475323
Last updated: 10/15/2006
Affected Releases: 2.3.5 R60
Current Status: Open

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

9.1.1.5 HOST IP'S ARE CONFIGURED AS SYSLOG SERVERS

CR # Q01451297
Last updated: 09/22/2006
Affected Releases: 2.3.5
Current Status: Open

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

9.1.1.6 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.

9.1.1.7 SYSLOG SERVER NOT GETTING UPDATED AFTER UPGRADED TO 2.3.4.18_R61

CR # Q01457794
Last updated: 09/ 26/2006
Affected Releases: 2.3.5
Current Status: Open

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.

9.1.1.8 L2 FIREWALL NOT WORKING IN 2.3.5.0 R55

CR # Q01460850
Last updated: 10/14/2006
Affected Releases: 2.3.5
Current Status: Open

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.

9.1.1.9 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.

9.1.1.102.3.4.0: UNABLE TO SEND SYSLOG AND SNMP TRAP

CR # Q01394047
Last updated: 09/26/2006
Affected Releases: 2.3.5
Current Status: Open

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. However, the syslog messages are not corrected. For now, it’s suggested to look at the SNMP traps for detecting any change in the CPU load levels. The syslog message would be fixed in the next releases. For more information, please refer to the CR # Q01394047.

Issues Updated on 03/31/2006

9.1.1.11EVENTIA 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.

9.1.1.12ESL: 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 cause spf to run continuously.

Its suggested 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.

9.1.1.13COULDN'T GET THE INTERFACE STATUS PAGE FROM BBI AFTER UPGRADING TO 2.3.4.0_R60

CR # Q01330359
Last updated: 17/03/2006
Affected Releases: 2.3.4
Current Status: Open

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 we upgrade 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.

As a work around, when this problem is seen, the users are requested to close the existing WebUI session by closing the browser window and open a new WebUI session.

9.1.1.14SNMP TRAP SOURCE IP IS NOT CORRECT WHEN TRAP SOURCE IP SET TO MIP

CR # Q01319328
Last updated: 03/02/2006
Affected Releases: 2.3.1, 2.3.3, 2.3.4
Current Status: Open

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.

9.1.1.15ER 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.

9.1.1.16WEB [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

9.1.1.17WEB 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

9.1.1.18FAIL-OVER DOESN'T WORK WITH USER AUTHENTICATION ON VRRP H/A

CR # Q01233372
Last updated: 10/06/2005
Affected Releases: 2.3.3
Current Status: Open

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.

9.1.1.19THE 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.

9.1.1.20CP 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

Its been observed that when configured large number of L2-L3 bridge interfaces, the ‘get topology’ operation from the Check Point SmartDashboard sometimes fail 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 we configure the normal VRRP interfaces & bridge interfaces 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

9.1.1.21[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.

9.1.1.22L3-BRIDGE: OSPF WORK ON A DISABLED VRRP INTERFACE

CR # Q01203464
Last updated: 10/06/2005
Affected Releases: 2.3.3

Current Status: Open

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).

To avoid this scenario, the users are suggested to take care of these kinds of configuration and make sure that your bridge interface and other disabled VRRP interfaces are not on the same subnet. Also make sure to disable OSPF for the disabled interfaces.

9.1.1.23HIDE-NAT NOT WORKING PROPERLY IN VRRP AA SETUP

CR # Q01191170
Last updated: 10/06/2005
Affected Releases: 2.3.3
Current Status: Open

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).

9.1.1.24QOS POLICY NOT GETTING DOWNLOADED AFTER THE UPGRADE

CR # Q01188039

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

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”.

As a work around, run the following commands from the CLI:
/cfg/fw/dis
apply
/cfg/fw/ena

Alternately, users can also try restarting the Check Point services by running the following commands from the root prompt:
makeonall
cprestart

9.1.1.25MAINT/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.

9.1.1.26SECURID 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.

9.1.1.27SESSION FAILOVER NOT WORKING WITH SYNC PORT IN VLAN

CR # Q01188074
Last updated: 10/06/2005
Affected Releases: 2.3.3
Current Status: Open

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.

9.1.1.28THE 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.

9.1.1.29SYSTEM 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.

9.1.1.30RESTRICTION VIA HOSTS.ALLOW FILE DOESN’T WORK FOR SMARTPORTAL

CR # Q01155340
Last updated: 10/06/2005
Affected Releases: 2.3.3
Current Status: Open

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.

9.1.1.31SERVICES 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.

9.1.1.32VPN S2S WITH STANDALONE SYSTEMS: NEED SOME WORK AROUND STEPS

CR # Q01215993
Last updated: 10/06/2005
Affected Releases: 2.3.3
Current Status: Open

Environment:
- NSF5100 Firewall, build 2.3.3.0_R60

9.1.1.33PARTITION HDA3 OF ISD IS REACH 99% AFTER DOING UPGRADING

CR # Q01201687
Last updated: 10/06/2005
Affected Releases: 2.3.3
Current Status: Open

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

9.1.1.34STATIC 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.

9.1.1.35 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

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

CR# Q01052791
Last Updated: 05/22/2005
Affected Releases: 2.3.1
Current Status: Open

OSPF connected redistribution is not supported on GRE.

9.1.1.37FWMON DOESN'T WORK FOR THE FILTER OPTION "NET"

CR# Q01054089
Last Updated: 05/22/2005
Affected Releases: 2.3.1
Current Status: Open

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.

9.1.1.38BBI: RESETTING SIC OPERATION FROM WEB BROWSER REACHES TIMEOUT

CR# Q01052205
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:
- 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.

9.1.1.39TSDUMP 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.

9.1.1.40DYNAMIC 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.

9.1.1.41BBI: 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.

9.1.1.42HOST/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 IR
Q 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.

9.1.1.43CHECKPOINT 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 the concerned which outlines the limitation and also the workaround for the same.

9.1.1.44THE 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.

9.1.1.45PCI 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.

9.1.1.46OSPF: 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.

9.1.1.47KEVLAR 2.3 BETA - SOMETIMES KEVLAR OPERATING IN PROMISCUOUS MODE

CR # Q01114346
Last Updated: 05/22/2005
Affected Releases: 2.3.1
Current Status: Open

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.

10 Appendix–B: Upgrade Time

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