NORTEL NETWORKS™

How the world shares ideas.

Alteon Switched Firewall (ASF) System, Version 4.0.x Readme

Version 2.9
01 February, 2006

Nortel Networks, Inc.

Table of Contents

Change Log

Version	What	When	Who
1.0	Initial draft – Readme for 4.0.1 release	05/25/2004	Rajesh Vijayakumar
1.1	Final Readme for 4.0.l release	06/04/2004	Rajesh Vijayakumar
1.2	Added Q00921793 to list of known issues	06/07/2004	Rajesh Vijayakumar
1.3	Added Q00951131, Q00919674, and Q00955134 to the list of known issues.	08/11/2004	Satya Pradhan
1.4	Added Q00966728-01 to the list of known issues.	08/18/2004	Satya Pradhan
2.0	Added Section-5 and updated other sections for ASF 4.0.2.0a release.	10/25/2004	Satya Pradhan
2.1	Added Q00900430 to the list of known issues.	11/16/2004	Satya Pradhan
2.2	Added Q01035151 to the list of known issues.	12/10/2004	Satya Pradhan
2.3	Added Q01081888 to the list of known issues.	2/18/2005	Satya Pradhan
2.4	Changed “4.x” in the name of this document to “4.0.x”. Added Section-6 and updated other sections for ASF 4.0.3.0 release.	4/15/2005	Satya Pradhan
2.5	Added Section 4 and Appendix B for the release of HFA 14 (R55). Numbering of other sections is also changed accordingly.	5/31/2005	Satya Pradhan
2.6	Added Q01149312 to the list of known issues.	8/8/2005	Satya Pradhan
2.7	Added 4.0.4 release	12/21/2005	Ganesh Lakshmanan
2.8	Added few customer CRs fixed in 4.0.4 release.	1/10/2006	Ganesh Lakshmanan
2.9	Added 6616 and 6416 as supported hardware for 4.0.3 and 4.0.4 releases.	2/1/2006	Satya Pradhan

1 INTRODUCTION

This is the consolidated readme for all ASF 4.x releases. The objective of a single readme is to help the reader find and track the status and history of an issue more easily. In order to meet this objective, the document is organized in different sections as follows.

Section-2 contains a table that lists the status of all known issues found in 4.x releases. It shows the release where the issue was found, the current status of the issue, and the status of the issue in each 4.x software release. The next section (Section-3) describes the procedure to upgrade the old software to a 4.x release.

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

Note: This readme documents all ASF 4.0.x releases. Therefore, the name of this readme has been changed. “Version 4.x” in the document name is now “Version 4.0.x.”

2 STATUS OF KNOWN ISSUES AND LIMITATIONS

All the known issues found and/or fixed in 4.x releases are summarized in the following table. The details of the issues are described in Appendix-A. Each row in the table corresponds to a known issue. A detailed explanation of the issue can be found by looking at the CR # (if available) in the Appendix. If CR# is not available for an item, then search for the issue title in the Appendix for the specific update date. The known issues without the CR# are listed at the beginning of each sub-section for the specific update date. If viewing this document on your computer, you can click on a description item to jump to the full description in Appendix A.

The current status and the status of the issue in different releases are also presented in the table. In the table, ☒ means the particular build is affected ☑ means the issue is fixed in the particular build, ☑ means a patch is available for the problem, and ☒ means no fix is planned for the particular issue.

Table 1 Current status of all issues found in ASF-4.x releases.

CR #	Description of Issues and Limitations	Last Updated	Current Status	Status in Different Releases			
				4.0.1	4.0.2.0a	4.0.3	4.0.4
Q01154281	ASF MLT - problems with links/active ports - 8630GBR/6600 - auto ON	1/10/2006	Fixed	☒	☒	☒	☑
Q01194820	GARP Problem	1/10/2006	Fixed	☒	☒	☒	☑
Q00862550	Sync network problems after backup and restore	1/10/2006	Fixed	☒	☒	☒	☑
Q01213472	SFA 6600 and OPTera 5000 autoneg issue	1/10/2006	Fixed	☒	☒	☒	☑
Q01152681	VPN PROBLEM IN R60	12/21/2005	Open				☒
Q01149312	/maint/tsdump/exdump command times out	12/21/2005	Fixed			☒	☑
Q01106902-01	Health Check Daemon and Config Daemon may not work properly after 248 days of uptime	12/21/2005	Fixed	☒	☒	☒	☑
Q01169359	Problem with SFA detection after config changes related to default NAAP ports	12/21/2005	Fixed			☒	☑

CR #	Description of Issues and Limitations	Last Updated	Current Status	Status in Different Releases			
				4.0.1	4.0.2.0a	4.0.3	4.0.4
Q01169238	Cold Start traps because of more frequent restart of snmpd	12/21/2005	Fixed	☒	☒	☒	☑
Q00991305	Accelerator generates incorrect ARP entry	4/15/2005	Fixed	☒	☒	☑	☑
Q00951131	Join will fail if there is a '$' in the admin password	4/15/2005	Fixed	☒	☒	☑	☑
Q01072979	Error running some maint and stat commands	4/15/2005	Fixed	☒	☒	☑	☑
Q00976886-01	ASF replies ProxyARP even after NAT/ProxyARP configuration is deleted	4/15/2005	Fixed	☒	☒	☑	☑
Q01043291-01	VRRP issue may cause FDB timeout	4/15/2005	Fixed	☒	☒	☑	☑
Q01081888	SP ARP Table Corruption after Port Move	4/15/2005	Fixed	☒	☒	☑	☑
Q01035151	Trunk ports may cause L2 loop after Accelerator reboot	4/15/2005	Fixed	☒	☒	☑	☑
Q00939253	Connections may be deleted after TCP Start Timeout	4/15/2005	Fixed	☒	☑		
Q01088596	snmpdm Daemon Exits during SNMP Walk	4/15/2005	Open	☒	☒	☒	☒
Q01115296	Multiple Upgrade may require manual reboot	4/15/2005	Open	☒	☒	☒	☒
Q00900430	Hash algorithm for selecting trunk port does not maintain session persistency for accelerated connections	11/16/2004	Fixed	☒	☑		
Q00964274-01	MP CPU uses becomes high if default gateway is learned through dynamic routing	10/25/2004	Fixed	☒	☑		
Q00966728-01	High CPU usage when ELA Logging is enabled	10/25/2004	Fixed	☒	☑		
Q00955134	Check Point ASN-1 Vulnerability	10/25/2004	Fixed	☒	☑		
Q00921793	"fwaccel templates" Command Prints IP Addresses in Reverse Order	10/25/2004	Fixed	☒	☑		
Q00907069	Jumbo Frames Is Not Supported	10/25/2004	Fixed	☒	☑		

CR #	Description of Issues and Limitations	Last Updated	Current Status	Status in Different Releases			
				4.0.1	4.0.2.0a	4.0.3	4.0.4
Q00919661	Director Freezes Under Heavy Fragmented Traffic	10/25/2004	Fixed	☒	☑		
Q00870946	Changing Director Type Deletes Installed Policy	10/25/2004	No Fix Planned	☒	☒	☒	☒
Q00845830	Large SNMP Bulk GETs May Fail	10/25/2004	No Fix Planned	☒	☒	☒	☒
Q00857915	ASF Does Not Generate asfAcceleratorUp and asfAcceleratorDown Traps	10/25/2004	Fixed	☒	☑		
Q00737761	Sync Through VNIC Problem	10/25/2004	Fixed	☒	☑		
Q00901409	Firewall Directors Keep Losing Contact With Each Other	10/25/2004	Fixed	☑	☑		
Q00946307	Can't ping remote GRE tunnel end-point from non-MIP SFD	10/25/2004	No Fix Planned	☒	☒	☒	☒
Q00969461	SFD may reboot automatically after restoring configuration	10/25/2004	Open	☒	☒	☒	☒
Q00951990	GRE tunnel collision errors cause OSPF neighbor up and down	10/25/2004	Open	☒	☒	☒	☒
Q00694532-01	SFD may experience Accel-off under stress with NAT and Check Point synchronization	10/25/2004	Open	☒	☒	☒	☒
Q00983354	Disabling an interface does not bring back static route to the accelerator	10/25/2004	Open	☒	☒	☒	☒
Q00924515	OSPF logs may consume large disk space	10/25/2004	Open	☒	☒	☒	☒
Q00889975	Firewall license will disappear after reboot if “cplic put” command is used to add the license	10/25/2004	Open	☒	☒	☒	☒
Q00957186	Establishing trust may fail after resetting SIC	10/25/2004	Open	☒	☒	☒	☒
Q00919674	Firewall Accelerator Boots up Incorrectly if IAP Auto-Negotiation is Disabled	08/11/2004	No Fix Planned	☒	☒	☒	☒
Q00914964	Activating SYN Attack Protection Causes High CPU Usage	06/04/2004	Open	☒	☒	☒	☒
Q00921499-01	Enabling ISN Spoofing Causes High CPU Usage	06/04/2004	Open	☒	☒	☒	☒

CR #	Description of Issues and Limitations	Last Updated	Current Status	Status in Different Releases			
				4.0.1	4.0.2.0a	4.0.3	4.0.4
Q00914969	Smart Dashboard Crashes After Getting Topology	06/04/2004	Open	☒	☒	☒	☒
Q00860008	Default Gateway And Default Route Not Supported Together	06/04/2004	Open	☒	☒	☒	☒
Q00883420	Adjacent OSPF Devices Should Define Only One MD5 Key For OSPF	06/04/2004	No Fix Planned	☒	☒	☒	☒
Q00893753	Firewall Director Panics While Rebooting	06/04/2004	Open	☒	☒	☒	☒
Q00883573	Director May Freeze Under Sustained Stress	06/01/2004	Open	☒	☒	☒	☒
Q00860630	WebUI Commands to Find Sessions on Accelerator Fails	06/01/2004	Open	☒	☒	☒	☒
Q00887958	ASF Does Not Generate asfExtraAcceleratorDetected Trap	06/01/2004	Open	☒	☒	☒	☒
Q00822122	Proxy IPs Not Accessible After Disabling High Availability	03/04/2004	Open	☒	☒	☒	☒
Q00882761	Cannot Delete Host From Cluster	03/04/2004	Open	☒	☒	☒	☒
Q00742217	‘State Synchronization of This Machine is at Risk’ Message	12/07/2003	Open	☒	☒	☒	☒
Q00743399	Local Licenses Installed via SmartUpdate Disappear	12/07/2003	Open	☒	☒	☒	☒
Q00717195	With OSPF, Area 0 Cannot be Disabled	12/07/2003	Open	☒	☒	☒	☒
	Dynamic Routing Issues	10/16/2003	Open	☒	☒	☒	☒
	OSPF and Accelerator / MIP Firewall Director fail over	10/16/2003	Open	☒	☒	☒	☒
Q00748787	Check Point Sync Stops Working After Changing Sync Device	10/16/2003	Open	☒	☒	☒	☒
Q00764267	HTTP Worm Catcher and Concurrent Connections	10/16/2003	No Fix Planned	☒	☒	☒	☒

3 SOFTWARE UPGRADE

The SFD hard disk partition used during upgrade has been increased in 4.0.2.0a release to take care of the increased size of the software image. The partition sizes in earlier releases are smaller and may cause difficulty (particularly for multiple upgrades) during upgrade process. Therefore, it is recommended to do a clean install using bootable CD-ROM of ASF 4.0.2.0a or 4.0.3.0 image. If the clean install is not possible, then the following procedure could be used for the upgrade.

The size of the upgrade package for ASF 4.0.2.0a-R55, 4.0.3.0-R55, 4.0.4.0 R55/R60 is quite large and will not fit into the partition available in ASF 4.0.1 and earlier ASF releases for 6400 and 6600 Accelerator. Therefore, CLI based upgrade from ASF 4.0.1 and earlier version to ASF 4.0.2.0a-R55 is not supported. If you are upgrading to 4.0.2.0a-R55/4.0.3.0-R55/4.0.4.0 R55-R60 version, it is recommended to do a clean install. In the setup where service down time is a critical issue, the in-service upgrade procedure can be used that requires very minimal down time.

The software upgrade through CLI is supported only for ASF 4.0.2.0a-FP4, ASF 4.0.3.0-R55 and ASF 4.0.4.0 R55-R60. The upgrade process consists of the followings: pre-upgrade preparation; downloading the upgrade package; activating the new software; and post-upgrade verification. The details of these steps are presented below.

The summary of the main steps for upgrading to ASF 4.0.4.0 is given in Table 2.

Table 2 Upgrading to ASF 4.0.4.0

From	To	Upgrade Steps
4.0.1-x 3.5.x-x	4.0.4.0-FP4 (HFA-417)	• Do the pre-upgrade preparation. Clean up each SFD in the cluster using UpgradePrep.sh script*. • Use "/boot/software/download" to download FP4 upgrade package (ASF_Director_4.0.4.0_FP4.pkg). This should be done only in one SFD. • Activate 4.0.4.0 image using "/boot/software/activate". This should be done only in one SFD. • Please wait until SFDs reboot and all upgrade process is complete. • Get topology in the Check Point management station and push the policy. • Do the post-upgrade verification.
4.0.1-x 3.5.x-x	4.0.4.0-R55 (HFA-16) Or R60	• Do a clean install using iso image.
4.0.2.0a	4.0.4.0-FP4 (HFA 417) or R55 (HFA 16) Or	• Use "/boot/software/download" to download FP4 or R55 or NGX upgrade package (ASF_Director_4.0.4.0_FP4.pkg or ASF_Director_4.0.4.0_R55.pkg or ASF_Director_4.0.4.0_R60.pkg). This should be done only in one SFD. • Activate 4.0.4.0 image using "/boot/software/activate". This should be done only in one SFD.

	R60	• Please wait until SFDs reboot and all upgrade process is complete. • Get topology in the Check Point management station and push the policy. • Do the post-upgrade verification.
4.0.3.0	4.0.4.0-FP4 (HFA 417) or R55 (HFA 16) Or R60	• Use "/boot/software/download" to download FP4 or R55 or NGX upgrade package (ASF_Director_4.0.4.0_FP4.pkg or ASF_Director_4.0.4.0_R55.pkg or ASF_Director_4.0.4.0_R60.pkg). This should be done only in one SFD. • Activate 4.0.4.0 image using "/boot/software/activate". This should be done only in one SFD. • Please wait until SFDs reboot and all upgrade process is complete. • Get topology in the Check Point management station and push the policy. • Do the post-upgrade verification.

* The clean up script (UpgradePrep.sh) is available under "/alteon/Alteon Switched Firewall System/ ASF Accelerated Firewall Software" at the Nortel support web site (http://www.nortelnetworks.com/support/).

3.1 Pre-Upgrade Preparation

Backup configuration

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

Clean up /isd partition

If you are upgrading from 3.5.x, the disk usage for the /isd partition may become high (> 80%) during the upgrade process. This is more likely to happen if you have done multiple upgrades. The disk usage problem can be resolved by doing a clean install of 4.0.4.0. If it is not possible to do a clean install, the work around is to clean up the /isd partition by deleting the files that are not required. This should be done in each Director in the ASF cluster by running a script (UpgradePrep.sh) before upgrade. The compressed version (UpgradePrep.tgz) of this script is available under "/alteon/Alteon Switched Firewall System/ASF Accelerated Firewall Software" at the Nortel support web site (http://www.nortelnetworks.com/support/). The procedure to clean up the /isd partition is given below.

1. Copy the clean up script (UpgradePrep.tgz) to a floppy disk.
2. Insert the floppy into the SFD
3. Login to the Director as 'root'.
4. Run "mount /mnt/floppy"
5. Run "cd /var/tmp"
6. Run "cp /mnt/floppy/UpgradePrep.tgz ./UpgradePrep.tgz"
7. Run "tar –xzvf UpgradePrep.tgz"
8. Run "./UpgradePrep.sh cleanall"
9. Run "umount /mnt/floppy" and remove the floppy disk from the SFD
10. Repeat steps 2-9 on each Director in the cluster.

3.2 Downloading the upgrade Package

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

Starting from ASF 4.0.3.0, a new CLI has been added to download the upgrade package from a CD-ROM using "/boot/software/cdrom." Since the ASF installation CD contains the upgrade files (i.e. pkg files), it can be used to import the pkg file to the SFD. User can also burn his/her own CD containing the pkg file. Note that upgrade process requires that file extension to be .pkg. The CD-ROM is automatically ejected at the end of the operation.

Note: Since the CLI for downloading the package from CD-ROM is not available in builds before ASF 4.0.2.0a, this method can ONLY be used during upgrade from ASF 4.0.2.0a.

This step should be done only in one SFD.

3.3 Activating the new software

Once the upgrade package is downloaded, "/boot/software/cur" can be used to display all the software versions in the SFD. The version that was just imported will have the status "unpacked." The new version (4.0.4.0) can now be activated using "/boot/software/activate". This should be done only in one SFD.

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

This is the step where the software is upgraded to the new version. If the upgrade fails for some reason, the ASF will go back to the old version and you may not be able to login as 'admin'. To recover from this situation, please do the following

1. Login to the Director as 'root'
2. Run "make-part-rw /isd on" to make the /isd partition read-write
3. Run "cd /isd/opt"
4. Run "rm tng"
5. Run "ln -s ../tng-3.0.* tng"
6. Run "reboot" to reboot the Director
7. Repeat 1-6 on each Director

The Directors may reboot twice but after that you will be able to login as 'admin'. At this point, the system will run without any problem with the older version. You may now attempt to activate 4.0.4.0 again. If the second attempt fails (which will not happen in most cases), it is recommended to do a clean install of 4.0.4.0.

After successful software upgrade, the following steps must be done

- Get topology information in the Check Point management station and
- Push the policy to the ASF cluster.

3.4 Post-Upgrade Verification

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

- Login as root and run “os-version”. You will get the output “1.4.1.3_tng.4.0.4.0_FP4”, “1.4.1.3_tng.4.0.4.0_R55” and “1.4.1.3_tng.4.0.4.0_R60” for FP4, R55 and R60, respectively.
- Login as admin and check “/info/cluster” CLI to make sure that all the directors in the cluster are working fine.

4 HFA RELEASES FOR ASF

HFAs released by Check Point may need additional hotfixes to run with ASF software. Check Point does not release these hotfixes in their web site. Therefore, the HFAs released by Check Point should not be directly installed on ASF. To allow customers to upgrade to the latest HFA without waiting for the next ASF release, Nortel releases special HFA packages for ASF. These packages include Check Point HFA and ASF specific hotfixes. This section lists the HFA packages that are released by Nortel to run with specific ASF releases.

Note: Please contact Nortel support to get the HFA package you need. The HFA files from Check Point site **should not** be installed on ASF.

4.1 Released HFAs

The HFAs certified by Nortel including the installation procedure are presented in the sections below. The following table summarizes all the certified HFAs.

Table 3 List of HFAs released by Nortel.

HFA Number	CP Version	Released for ASF Version	HFA Package	Release Date
HFA 14	R55	ASF 4.0.3 – R55	ASF_4_0_R55_HFA14.tgz	5/31/2005
HFA17	R55	ASF 4.0.3 - R55	ASF_R55_HFA17.tgz	12/20/2005

4.2 HFA Installation Procedure

Follow the steps given below to install the HFA package in the ASF cluster.

(1) Login as root to a director (SFD)
(2) ftp or copy the HFA package <package.tgz> (Table 3) to "/var"
(3) run "cd /var" to change current directory to /var
(4) run "tar –xzvf <package>" to extract all required files
(5) run "./install_hfa.sh" to install the HFA. The system will automatically reboot to activate the new HFA.
(6) Wait until the current SFD is operational and acceleration is on. Use "cat /proc/aim/cur" at the root prompt to check for the acceleration status.
(7) Repeat steps-1 to 6 on each SFD in the cluster.

4.3 Status of Known Issues and Limitations in HFA

All the known issues found in different HFAs are summarized in the following table. The details of the issues are described in Appendix-B. Each row in the table corresponds to a known issue. A detailed explanation of the issue can be found by looking for the issue under the HFA subsection in Appendix-B.

If viewing this document on your computer, you can click on a description item to jump to the full description in Appendix B.

Table 4 Current status of all issues found in HFA releases.

HFA Number	CR #	Description of Issues and Limitations	Last Updated	Current Status

Note: No issue has been found in the HFAs released on ASF.

5 ALTEON SWITCHED FIREWALL, VERSION 4.0.1 (06/01/2004)

5.1 New Hardware Platform

ASF 4.0.1 introduces a new accelerator ASF 6600. The new accelerator can be paired only with the 5014 director and the combination is called ASF 6614. The 6600 accelerator has 4 copper gig ports, 4 fiber gig ports and 4 copper/fiber gig ports for a total of 12 gig ports. ASF 6614 supports up to 500,000 concurrent connections with Check Point Sync enabled and up to 1 million concurrent connections with Sync disabled (and at least 2 Directors in the cluster).

ASF 4.0.1 is supported only on ASF 6614 platform. The 4.0.2 release will add support for 64xx platforms also. The 5x00 series accelerators will not be supported on 4.0.

5.2 Supported Check Point Releases

ASF 4.0.1 supports Check Point NG with Application Intelligence R54 with HFA-410.

5.3 Configuration of the Gateway Cluster Object

Check Point SmartDashboard in NG AI has a new tab called "3rd Party Configuration" in the gateway cluster properties. When you define a gateway cluster for the ASF, make sure you go to the "3rd Party Configuration" tab and configure it as follows:

Cluster Operation Mode: Load Sharing (mandatory)
3rd Party Solution: OPSEC (mandatory)
Support non-sticky connections: Yes (mandatory)
Hide Cluster Members' outgoing traffic behind Cluster's IP Address: No
Forward Cluster's incoming traffic to Cluster Members' IP Address: No

5.4 Supported Features

The following new features are supported in this release.

5.4.1 Route Table Size Increased to 8K

ASF 4.0.1 has an increased route table size of 8K. The route table is shared by the static routes, dynamic routes, multicast routes (used internally) and the default routes for each configured interface.

5.4.2 NAAP VLAN ID Configuration

ASF 4.0.1 allows user to configure NAAP VLAN ID (CR# Q00881922). Any number between 2 and 4094 (except 4092) can be used for NAAP VLAN ID.

The following steps need to be done for changing NAAP VLAN ID.

- Disconnect all the directors in the cluster from the accelerators.
- Re-image the directors with ASF 4.0.1 iso image, login as admin and change the NAAP VLAN ID using the *naap* menu. This needs to be done in all the directors in the ASF cluster before running any other CLI command (e.g. *new*). The setup menu with *naap* CLI is given below.

```
--------------------------------------------------------
[Setup Menu]
    join      - Join an existing ASF cluster
    new       - Create a new ASF installation
    restore   - Restore this SFD from a backup taken earlier
    offline   - Configure this SFD for offline, switchless maintenance
    boot      - Boot Menu
    naap      - Set NAAP VLAN id
    exit      - Exit
--------------------------------------------------------
```

- Login to the accelerator as ‘admin’. Reboot the accelerator with factory default configuration using “/boot/conf fact/reset”.
- Change the NAAP VLAN ID in all the accelerators using the following commands.

```
# /cfg/vlan <VLAN ID>/ena/add <NAAP ports>
# /cfg/sys/naap/vlan <VLAN ID>
# apply
# save
# /boot/reset
```

- Connect the directors with the accelerators and continue with the setup procedure.

5.4.3 New CLI Commands to Manage Accelerator

The "/maint/debug/ac1/back" and "/maint/debug/ac2/back" CLI commands will force accelerator-1 and accelerator-2 respectively to become the backup. Please use “/maint/debug/ac1/vrrp” to confirm the new VRRP state. Please keep in mind that the accelerator forced to become the backup will remain as backup only if its VRRP priority is less tan or equal to that of the other accelerator.

The “/maint/debug/ac1/reboot” and “/maint/debug/ac2/reboot” CLI commands will reboot accelerator-1 and accelerator-2 respectively.

6 ALTEON SWITCHED FIREWALL, VERSION 4.0.2.0A (11/01/2004)

6.1 Supported Hardware Platforms

ASF 4.0.2.0a supports the following hardware platforms:

- ASF 6414 (6400 Accelerator + 5014 Director)
- ASF 6614 (6600 Accelerator + 5014 Director)

6.2 Supported Check Point Releases

ASF 4.0.2.0a supports the following Check Point builds.

- Check Point NG with Application Intelligence (R54) with HFA-412
- Check Point NG with Application Intelligence (R55) with HFA-08

6.3 Supported Features

The following new features are available in ASF 4.0.2.0a release.

6.3.1 Route Table Size

The supported route table sizes are 8K and 4K for 6600 Accelerator and 6400 Accelerator, respectively. The route table is shared by the static routes, dynamic routes, multicast routes (used internally) and the default routes for each configured interface.

6.3.2 CLI to set sysname for Directors

A new CLI has been added that allows you to give a user friendly name to each director: “/cfg/sys/clu/host <n>/<name>” where <n> is the host number and <name> is the host name you want to give to host n. When you login as “admin”, the name of that director will be displayed as part of the banner. This allows you to easily identify the director as the right one.

6.3.3 Automatic Check Point Upgrade

The upgrade procedure before 4.0.2.0a releases was a two step process that required separate steps for upgrading Nortel software and Check Point software. This procedure has been simplified in ASF 4.0.2.0a where the upgrade is done only in one step. The pkg file provided with 4.0.2.0a version includes the upgrade packages for both Nortel and Check Point software. The new upgrade procedure automatically updates the Check Point software to the same version as a clean install from the CD. It is no longer required to run “/cfg/fw/software/*” or install RPMs using “/boot/software/patch/install” for upgrading Check Point software. Please refer to Section 3 for a detailed upgrade procedure.

6.3.4 Upgrade from CD-ROM

A new CLI (/boot/software/cdrom) has been added that will allow the user to get the upgrade pkg file from the CD-ROM instead of having to ftp it. The system will search the CD-ROM for "*.pkg". If only one file is found, it is imported automatically. If multiple files are found, the list of files is displayed and user is prompted to enter the path. If no files are found, user is prompted to enter the path. The full path should be entered in both these cases. It can be any file on the CD-ROM or the hard disk. After the operation has completed, "/boot/software/cur" will display the version that was just imported with the status "unpacked." User can activate the new version as usual. Since the ASF installation CD contains the pkg file also, it can be used to import the pkg file. User can also burn his/her own CD containing the pkg file. Note that upgrade process requires that file extension to be .pkg. The CD-ROM is automatically ejected at the end of the operation. Please refer to Section 3 for detailed steps for the upgrade procedure.

6.3.5 Configurable AIM Connection Table Size

Starting with 4.0.2.0a, a CLI (/cfg/fw/sxl/conns) is provided to override the default maximum value of the AIM connection table size. The minimum allowed table size is 40,000. The maximum allowed number depends on the accelerator type. It is not recommended to change the maximum size of the AIM table. The default value is sufficient for most networks. If you are changing the connection table size, please use "/maint/debug/aim/acp/tbl" CLI command on each director to make sure that the size of all the tables are below their maximum limit.

6.3.6 MIB files can be downloaded from the WebUI

For user convenience, the MIB files are available in SFD. There are 3 MIB files available for download: Base OID, alteon-isd & alteon-asf. These MIB files can be downloaded from the WebUI (Administration/SNMP/MIBs).

6.3.7 GRE support in ASF

ASF 4.0.2.0a release supports GRE tunnel. One of the SFD in the ASF cluster can terminate the GRE tunnel. Packets originating from the SFD (e.g. OSPF packets) and external packets from other networks can be sent through the GRE tunnel. Since GRE tunnels terminate on the SFD, all the packets that are sent through the tunnel are forwarded to the SFD (i.e. the packets in GRE tunnel are not accelerated). Therefore, it is recommended not to send large amount of data through the GRE tunnel.

6.4 Bugs Fixed Since 4.0.1 Release

- MP CPU uses becomes high if default gateway is learned through dynamic routing (CR# Q00964274-01)
- High CPU usage when ELA Logging is enabled (Q00966728-01)

- Check Point ASN-1 Vulnerability (Q00955134)
- "fwaccel templates" Command Prints IP Addresses in Reverse Order (Q00921793)
- Jumbo Frames Is Not Supported (Q00907069)
- ASF Does Not Generate asfAcceleratorUp and asfAcceleratorDown Traps (Q00857915)
- Sync Through VNIC Problem (Q00737761)
- Director Freezes Under Heavy Fragmented Traffic (CR# Q00919661)

7 ALTEON SWITCHED FIREWALL, VERSION 4.0.3.0 (04/15/2005)

7.1 Supported Hardware Platforms

ASF 4.0.3.0 supports the following hardware platforms:

- ASF 6414 (6400 Accelerator + 5014 Director)
- ASF 6614 (6600 Accelerator + 5014 Director)
- ASF 6416 (6400 Accelerator + 5016 Director)
- ASF 6616 (6600 Accelerator + 5016 Director)

7.2 Supported Check Point Releases

ASF 4.0.3.0 supports the following Check Point builds:

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

The following Check Point applications are supported by ASF 4.0.3.0:

- Firewall (on-box):
  - SmartDefense, Load Sharing, NAT, Authentication, Content Security, Securing Voice over IP (VOIP)
- SmartView Monitor (on-box and off-box)
- SmartCenter Server (off-box)
- SmartDashboard (off-box)
- SmartView Tracker (off-box)
- SmartView Status (off-box)
- Provider-1 (off-box)

Note: In this Release Note, “on-box” refers to “on the Switched Firewall Director (SFD)” and “off-box” means the application can run outside the SFD.

7.3 Supported Features

The following new features are available in ASF 4.0.3.0 release.

7.3.1 Usability Improvement

Release 4.0.3.0 implements several usability enhancements. New CLI commands are added to use/enable these enhancements. These are:

- Configure an additional interface on SFD for external users
- View port properties and ASF capability
- Download Secure-ID configuration
- Simplify packet capture using the fw monitor command
- View traffic information

CONFIGURE AN ADDITIONAL INTERFACE ON SFD FOR EXTERNAL USERS

- A Command Line Interface (CLI) is added to create an interface in the SFD for external users. Use this new interface to connect to the Check Point management station and the Browser Based Interface (BBI) before configuring ASF interfaces.

VIEW PORT PROPERTIES AND ASF CAPABILITY

- Release 4.0.3.0 introduces new CLI commands to show port properties (/info/net/sfdports) and ASF capability (/info/capability).

DOWNLOAD SECURE-ID CONFIGURATION

- Release 4.0.3.0 introduces a command to download Secure-ID configuration (/cfg/apps/securid/).

SIMPLIFY PACKET CAPTURE USING THE FW MONITOR COMMAND

- The current fw monitor command has complex syntax. Release 4.0.3.0 adds a new CLI command (/info/fwmon) to simplify the packet capture using fw monitor. The CLI provides an easy and quick way to capture packets. For packet capture with advanced filters, Nortel recommends using the fw monitor command from the root prompt.

VIEW TRAFFIC INFORMATION

- A new command shows traffic information (/info/traffic) from the CLI.

7.3.2 SFA link teardown during failover

In many deployments, it is required to do failover of connected devices when SFAs failover. With the new feature, the ASF software takes down link states on the Ethernet ports connected to the next hop routers/switches when an SFA fails over to the standby SFA. This allows the connected routers/switches to sense this ASF failover and failover themselves to their backup components, which are connected to the now active SFA. This behavior can be turned on a per port basis using "/cfg/net/port <n>/bounce" CLI.

7.4 Bugs Fixed Since 4.0.3.0 Release

- Accelerators cause L2 bridge after power cycle (Q01035151)
- Accelerator generates incorrect ARP entry (Q00991305)
- Join will fail if there is a "$" in the admin password (Q00951131)
- Incorrect entry in SP ARP table (Q01081888)
- Error running some maint and stat commands (Q01072979)
- ASF replies ProxyARP even after NAT/ProxyARP configuration is deleted (Q00976886-01)
- VRRP issue may cause FDB timeout (Q01043291-01)

8 ALTEON SWITCHED FIREWALL, VERSION 4.0.4.0 (12/21/2005)

8.1 Supported Hardware Platforms

ASF 4.0.4.0 supports the following hardware platforms:

- ASF 6414 (6400 Accelerator + 5014 Director)
- ASF 6614 (6600 Accelerator + 5014 Director)
- ASF 6416 (6400 Accelerator + 5016 Director)
- ASF 6616 (6600 Accelerator + 5016 Director)

8.2 Supported Check Point Releases

ASF 4.0.4.0 supports the following Check Point builds:

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

The following Check Point applications are supported by ASF 4.0.4.0:

- Firewall (on-box):
  - SmartDefense, Load Sharing, NAT, Authentication, Content Security, Securing Voice over IP (VOIP)
- SmartView Monitor (on-box and off-box)
- SmartCenter Server (off-box)
- SmartDashboard (off-box)
- SmartView Tracker (off-box)
- SmartView Status (off-box)
- Provider-1 (off-box)

Note: In this Release Note, “on-box” refers to “on the Switched Firewall Director (SFD)” and “off-box” means the application can run outside the SFD.

8.3 Supported Features

The following new feature is available in ASF 4.0.4.0 release.

8.3.1 USB support

USB support has been added and a script is provided to mount and unmount USB device from the Director. The CLI/BBI does not support USB device for transferring files. The device needs to be mounted from root using the script /opt/tng/bin/usbmount and unmount by /opt/tng/bin/usbumount.

8.4 Configuration of the Gateway Cluster Object for R60

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

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

8.5 Bugs Fixed Since 4.0.3.0 Release

- /maint/tsdump/exdump command times out (Q01149312)
- Health Check daemon and config daemon may not work properly after 248 days of uptime (Q01106902-01**)**
- Problem with SFA detection after config changes related to default NAAP ports (Q01169359)
- COLD START TRAPS BECAUSE OF MORE FREQUENT RESTART OF SNMPD (Q01169238)
- ASF MLT - problems with links/active ports - 8630GBR/6600 - auto ON (Q01154281)
- GARP Problem (Q01194820)
- Sync network problems after backup and restore (Q00862550)
- SFA 6600 and OPTera 5000 autoneg issue (Q01213472)

9 APPENDIX-A: LIST OF KNOWN ISSUES

This Appendix provides detailed explanation on all the issues found and/or fixed in 4.0.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 01/10/2006

ASF MLT - PROBLEMS WITH LINKS/ACTIVE PORTS - 8630GBR/6600 - AUTO ON

CR# Q01154281
Last Updated: 01/10/2006
Affected Releases: 4.0.x
Current Status: Fixed in 4.0.4

The Gig link LED connected to Passport (8630GBR) is UP for ports on the SFA but port is not getting used on the accelerator and the link status was shown as disabled.

GARP PROBLEM

CR# Q01194820
Last Updated: 01/10/2006
Affected Releases: 4.0.x
Current Status: Fixed in 4.0.4

When GARP packet was received by master accelerator, the arp cache was not updated with new MAC address. The fix clears arp/route cache when GARP is received.

SYNC NETWORK PROBLEMS AFTER BACKUP AND RESTORE

CR# Q00862550
Last Updated: 01/10/2006
Affected Releases: 4.0.x
Current Status: Fixed 4.0.4

The CheckPoint sync service was not started automatically after restore. The backup process did not include the configuration file which caused the issue.

SFA 6600 AND OPTERA 5000 AUTONEG ISSUE

CR# Q01213472
Last Updated: 01/10/2006
Affected Releases: 4.0.x
Current Status: Fixed 4.0.4

When one of the gig accelerator ports was connected to OPTera 5000 and the cable is unplugged and plugged back, the accelerator does not bring up the link and the negotiation between accelerator and OM5K GFSRM was broken.

Issues Updated on 12/21/2005

VPN PROBLEM IN R60

CR# Q01152681
Last Updated: 12/21/2005
Affected Releases: 4.0.4-R60
Current Status: Work around available
Both site-to-site and client-to-site VPN will not work in 4.0.4-R60 with the default management station settings. The work around to resolve this problem is described below.

1. Configure the VPN gateway object in the Check Point SmartDashboard and save the configuration. Close the management station if it is opened.
2. Open a dos window.
3. Type "cd \program files\checkpoint\smartconsole\r60\program". If you have installed Check Point management software in a different location, you should cd to appropriate directory.
4. Type in "guidbedit" and connect to management station.
5. Hit "ctrl F" (for find) and type "reroute" in the "Find What" box
6. Click on the "Find Next" button
7. It should take you to the "reroute_encryted_packets" in the "Field Name" column
8. Change the "Value" to false.
9. Hit “F3" and it should find the next instance of "reroute_encryted_packets"
10. Change its "Value" to false.
11. click on "File" and click on "Save All"
12. Close the guidbedit window and start it again and double check the values of "reroute_encryted_packets" are set to false.
13. Close the guidbedit window after verifying the values.
14. Start the management station and push the policy to the FW.

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

/MAINT/TSDUMP/EXDUMP COMMAND TIMES OUT

CR# Q01149312
Last Updated: 12/21/2005
Affected Releases: 4.0.3.0
Current Status: Fixed

In ASF 4.0.3.0 release, running tsdmp command leaves the directors in a hung state whereby the user will not be able to issue any CLI commands. However, traffic flowing through the firewall is not impacted. This happens because the script that collects the log files when invoking the tsdmp command is missing in ASF 4.0.3.0 release. The issue has been fixed in 4.0.4.0.

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

CR# Q01106902-01
Last Updated: 12/21/2005
Affected Releases: 4.0.x
Current Status: Fixed

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

When you run “/info/clu,” if the “Health Report as of ...” field shows an old time and does not get updated, this may indicate that the problem has occurred. To verify, please login as root and run “uptime” to see if the system has been up for more than 248 days. The issue has been fixed in 4.0.4.0.

PROBLEM WITH SFA DETECTION AFTER CONFIG CHANGES RELATED TO DEFAULT NAAP PORTS

CR# Q01169359
Last Updated: 12/21/2005
Affected Releases: 4.0.3.0
Current Status: Fixed

In ASF 4.0.3.0 release, when the default NAAP port is used as non-naap port or disabled, the director may not be able to apply configuration on the accelerator after the accelerator reboots. The issue has been fixed in 4.0.4.0.

COLD START TRAPS BECAUSE OF MORE FREQUENT RESTART OF SNMPD

CR# Q01169238

Last Updated: 12/21/2005
Affected Releases: 4.0.x
Current Status: Fixed

In ASF 4.0.x releases, SNMP daemon restarts when SSI process restarts. The issue has been fixed in 4.0.4.0 by keeping SNMP independent of SSI process.

Issues Updated on 4/15/2005

ACCELERATOR GENERATES INCORRECT ARP ENTRY

CR# Q00991305
Last Updated: 4/15/2005
Affected Releases: 4.0.1 and 4.0.2.0a
Current Status: Fixed in 4.0.3.0

An error in ARP response processing in SFA could corrupt ARP entries in 6000 series accelerators. This could affect packet forwarding because of the incorrect ARP table. The problem has been fixed in 4.0.3.0.

JOIN WILL FAIL IF THERE IS A '$' IN THE ADMIN PASSWORD

CR# Q00951131
Last Updated: 4/15/2005
Affected Releases: 4.0.1 and 4.0.2.0a
Current Status: Fixed in 4.0.3.0

The ‘$’ in the admin password string has been handled correctly and the problem has been fixed in fixed in 4.0.3.0.

ERROR RUNNING SOME MAINT AND STAT COMMANDS

CR# Q01072979
Last Updated: 4/15/2005
Affected Releases: 4.0.1 and 4.0.2.0a
Current Status: Fixed in 4.0.3.0

Some maint and stat commands do not work in ASF 4.0.1 and 4.0.2 releases. These commands are:

```
/stat/slb/port <n>/maint
/stats/port <n>/maint
/stat/port <n>/cpu
/maint/debug/ac <n>/prtstat
```

These errors have been fixed in ASF 4.0.3.0

ASF REPLIES PROXYARP EVEN AFTER NAT/PROXYARP CONFIGURATION IS DELETED

CR# Q00976886-01
Last Updated: 4/15/2005
Affected Releases: 4.0.1 and 4.0.2.0a
Current Status: Fixed in 4.0.3.0

When the configuration for StaticNAT and ProxyARP are deleted, the corresponding entries in the backup switch are not removed. This could cause SFA to send GARP and respond to ARP request for the deleted NATed addresses after SFA fail-over (i.e. when the backup SFA becomes active). The issue has been fixed by updating the backup accelerator for ARP processing.

VRRP ISSUE MAY CAUSE FDB TIMEOUT

CR# Q01043291-01
Last Updated: 4/15/2005
Affected Releases: 4.0.1 and 4.0.2.0a
Current Status: Fixed in 4.0.3.0

If some L2 device is connected to an ASF in HA configuration, the VRRP processing logic in ASF may cause timeout of the FDB entry in the L2 device. Therefore, the L2 device may start flooding all the packets in the VLAN connecting the ASF. This issue does not cause any connectivity problem and has been fixed in 4.0.3.0 by an optimal VRRP processing logic.

CONNECTIONS MAY BE DELETED AFTER TCP START TIMEOUT

CR# Q00939253
Last Updated: 4/15/2005
Affected Releases: 3.5.1.0g, 3.5.1.10d, 3.5.2.1, and 4.0.1
Current Status: Fixed in 4.0.2.0a

This happens because of a particular sequence of SecureXL API calls that creates a situation where SYN and SYN-ACK packets are sent to the SFD and the ACK packet is accelerated by the SFA. In this case, the firewall does not see the ACK packet and thinks that the connection is not completely established. Therefore, the firewall deletes the connection after TCP_start_timeout period. The problem has been fixed so that the ACK packet is not accelerated

SP ARP TABLE CORRUPTION AFTER PORT MOVE

CR# Q01081888
Last Updated: 4/15/2005
Affected Releases: 4.0.1 and 4.0.2.0a
Current Status: Fixed in 4.0.3.0

When an ARP entry is modified after a port move due to MAC address change, the ARP entry in the SPs may not get updated correctly. This may cause connectivity problem to the IP addresses involved. If this problem happens, clear the ARP tables by running "/maint/arp/clear" in the SFA CLI. SFA will learn the correct MAC address and forward the traffic correctly. If the problem persists after this change, the work around is to reset the SFAs in the cluster.

TRUNK PORTS MAY CAUSE L2 LOOP AFTER ACCELERATOR REBOOT

CR# Q01035151
Last Updated: 4/15/2005
Affected Releases: 4.0.1 and 4.0.2.0a
Current Status: Fixed in 4.0.3.0

If trunk is configured, ASF may cause L2 loop after accelerator reboot. This problem is caused by the partial configuration saved in the accelerator. The loop will exist until the director pushes the configuration to the accelerator. The work around is not to save any configuration in the accelerator. The following steps should be done to implement the work around for this problem.

1. login to the director as root.
2. edit "/opt/tng/conf/config" using vi.
3. find the line "#DONT_SAVE_TO_SWITCH=1" and change it to "DONT_SAVE_TO_SWITCH=1" (remove the comment from this line).
4. save the file.
5. repeat steps 1-4 on each director in the cluster.
6. login to each accelerator as admin and run "/boot/conf fact". This will make sure that the accelerator boots up with factory default configuration.
7. reboot the accelerators.

The above changes make sure that the director does not save configuration in the accelerator so the accelerator always boots up in factory default. After boot up, the accelerator gets the entire configuration from the director.

After this work around, the configuration is not saved and, therefore, the accelerators always boot up with the default NAAP ports. If you have configured non-default NAAP ports as NAAP, then the work around may cause other problems. Therefore, if you are using this work around, you should use only default NAAP ports for the SFD subnet. The problem has been fixed in ASF 4.0.3.0 release.

SNMPDM DAEMON EXITS DURING SNMP WALK

CR# Q01088596
Last Updated: 4/15/2005
Affected Releases: 4.0.x
Current Status: Open

For some specific configuration when MIB-II element groups are accessed for "ip" followed by "interfaces", the snmpdm may exit abnormally. The work around is not to access the "ip" section of the MIB-II. Instead, use the items within the Nortel/Alteon-specific MIBs. They contain the SNMP details most relevant to ASF.

MULTIPLE UPGRADE MAY REQUIRE MANUAL REBOOT

CR# Q01115296
Last Updated: 4/15/2005
Affected Releases: 4.0.3.0
Current Status: Open

If you are upgrading to 4.0.3.0 for a system that has already been upgraded once from an earlier build, and if you have large number of static routes (> 1000) and OSPF routes (> 400), the upgrade process may not complete successfully for all directors in the cluster. Wait for 20 minutes for the upgrade process to complete. If the upgrade process does not reboot the system automatically, you need to reboot the SFDs manually to complete the upgrade. There should not be any other issue with these upgrades.

Issues Updated on 11/16/2004

HASH ALGORITHM FOR SELECTING TRUNK PORT DOES NOT MAINTAIN SESSION PERSISTENCY FOR ACCELERATED CONNECTIONS

CR# Q00900430
Last Updated: 11/16/2004
Affected Releases: 4.0.1
Current Status: Fixed in 4.0.2.0a

The hash algorithm for selecting trunk ports was not maintaining session persistency for accelerated sessions. That means the packets for the same session may be forwarded through different trunk ports. If other devices that are connected to the ASF through trunk ports do not handle this situation properly, there may be some packet drop for this session. The hash algorithm has been changed in ASF 4.0.2.0a release so that the session persistency is maintained for accelerated sessions.

Issues Updated on 10/25/2004

MP CPU USES BECOMES HIGH IF DEFAULT GATEWAY IS LEARNED THROUGH DYNAMIC ROUTING

CR# Q00964274-01

Last Updated: 10/25/2004
Affected Releases: 4.0.1
Current Status: Fixed in 4.0.2.0a

If you are using dynamic routing (OSPF, RIP) to learn default gateway, then all the packets that are routed to the default gateway will be routed by the MP in the accelerator. This may cause MP CPU usage to become high (100%) and packets may be dropped under this condition. The work around is to configure the default gateway on ASF and disable dynamic route redistribution on the connected device.

HIGH CPU USAGE WHEN ELA LOGGING IS ENABLED

CR# Q00966728-01
Last Updated: 10/25/2004
Affected Releases: 4.0.1
Current Status: Fixed in 4.0.2.0a

If ELA logging is enabled under "/cfg/sys/log/ela", but you have not yet pulled a SIC certificate from the Check Point management server using "/cfg/sys/log/ela/pull", the CPU usage of the director will go up to 100%. To fix the problem, either disable ELA logging temporarily or complete the ELA configuration by pulling the SIC certificate from the Check Point management server. Detailed instructions for configuring ELA logging are available in the ASF User Guide.

CHECK POINT ASN-1 VULNERABILITY

CR# Q00955134
Last Updated: 10/25/2004
Affected Releases: 4.0.1
Current Status: Fixed in 4.0.2.0a

Check Point has discovered a vulnerability (ASN-1) that affects ASF cluster if VPN is selected in the gateway cluster object in the Check Point management station. It does not affect ASF clusters if only firewall is selected in the cluster object. Details of this vulnerability can be found at http://www.checkpoint.com/techsupport/alerts/asn1.html

"FWACCEL TEMPLATES" COMMAND PRINTS IP ADDRESSES IN REVERSE ORDER

CR# Q00921793
Last Updated: 10/25/2004
Affected Releases: 4.0.1
Current Status: Fixed in 4.0.2.0a

The "fwaccel templates" command allows the user to see the template connections that have been offloaded. This command is accessible only when you login to the director as "root". In the output of this command, the IP addresses are printed backwards. For example, "192.168.1.1" will be printed as “1.1.168.192”. This is just a display issue and does not have any other effect on ASF operation.

JUMBO FRAMES IS NOT SUPPORTED

CR# Q00907069
Last Updated: 10/25/2004
Affected Releases: 4.0.1
Current Status: Fixed in 4.0.2.0a

This release of ASF does not support jumbo frames. Please do not enable jumbo frames from the CLI.

DIRECTOR FREEZES UNDER HEAVY FRAGMENTED TRAFFIC

CR# Q00919661
Last Updated: 10/25/2004
Affected Releases: 4.0.1
Current Status: Fixed in 4.0.2.0a

Under very high levels of fragmented traffic, the director may freeze and result in traffic disruption. This has been observed only in the lab with 700+ Mbps of 512 byte sized fragments. This scenario is unlikely in live deployments but may be simulated using traffic generators. Please reboot the director to recover.

CHANGING DIRECTOR TYPE DELETES INSTALLED POLICY

CR# Q00870946
Last Updated: 10/25/2004
Affected Releases: 4.0.1
Current Status: No Fix Planned

If you change the director type from ‘master’ to ‘slave’ or from ‘slave’ to ‘master’, that director will lose the installed Check Point policy and will go back to the ‘InitialPolicy’. When this happens, the director will stop processing traffic. This will not cause any traffic disruption as long as there are other directors in the cluster capable of handling the traffic. To recover from this situation, push policy again to the cluster from the Check Point SmartDashboard.

LARGE SNMP BULK GETS MAY FAIL

CR# Q00845830
Last Updated: 10/25/2004
Affected Releases: 4.0.1
Current Status: No Fix Planned

When doing Bulk GETs from the ASF using an SNMP tool, the total size of data requested in a single Bulk GET exceeds 1500 bytes, the operation will fail and the SNMP tool will not get any response back from ASF. This happens only if ‘/cfg/sys/adm/snmp/adv/trapsrcip’ is set to ‘mip’ or ‘unique’. The workaround is to set ‘/cfg/sys/adm/snmp/adv/trapsrcip’ to ‘auto’ (this is the default setting) or reduce the amount of date requested in a single Bulk GET operation.

ASF Does Not Generate asfAcceleratorUp and asfAcceleratorDown Traps

CR# Q00857915
Last Updated: 10/25/2004
Affected Releases: 4.0.1
Current Status: Fixed in 4.0.2.0a

ASF does not generate the ‘asfAcceleratorUp’ trap when an accelerator comes up. The ‘asfAcceleratorDown’ trap is also not generated when the accelerator goes down.

Sync Through VNIC Problem

CR# Q00737761
Last Updated: 10/25/2004
Affected Releases: 4.0.1
Current Status: Fixed in 4.0.2.0a

Sync through VNIC is not supported in builds up to 4.0.1. Please use any of the other available ports for sync. We are working with Check Point to resolve this and a patch will be made available as soon as possible.

Firewall Directors Keep Losing Contact With Each Other

CR# Q00901409
Last Updated: 10/25/2004
Affected Releases: 3.5.1.0g, 3.5.1.10d, 3.5.2.1 (these 3.5.x releases support 6400 accelerator)
Current Status: Fixed in 4.0.1

When you run “/info/clu” from the CLI, you may intermittently see message saying “No health report available...” for some Directors. You will also notice that the Directors will not be able to ping each other during this period. This issue affects all Accelerators (5600, 5700, 6400, etc) only if the MAC address of the Directors are very similar and differ only in the last byte.

You should check if you are affected by this issue.

1. Login to each Director as ‘root’ and run “ifconfig reth0”. The MAC address of the Director will be displayed in the first line of output.

   ```
   [root@localhost root]# ifconfig reth0
   ```

```
reth0     Link encap:Ethernet  HWaddr 00:04:23:9A:52:70
```

2. Compare the MAC addresses between the Directors. If the first 5 bytes are the same, then you will be affected by this issue. For example, if the first Director's MAC address is 00:04:23:9A:52:70 and the MAC address of the second Director is 00:04:23:9A:52:85, then you are affected.

If you are affected by this issue, it is recommended to upgrade to 3.5.3. If it is not possible to upgrade, the following workaround can be used to reconfigure the MAC address of one or more Directors so that the Directors in the cluster have different MAC addresses. This work around will work only for 5014 directors. For other directors, the only solution is to upgrade to 3.5.3 code. Furthermore, the work around will be lost during an upgrade process. So, the changes for the MAC address have to be done after each upgrade.

1. Choose the Director whose MAC address you want to change
2. Log in as root and run the following commands to make the file system read/write.
   a. `make-part-rw / on`
   b. `make-part-rw /isd on`
3. Edit "/etc/init.d/aim" using "vi" and find the line
   "`ifconfig $RNIC_NAME allmulti`"
4. Add the following line just below it
   "`ifconfig $RNIC_NAME hw ether 00:0e:de:ad:be:ef`"
5. Save the file and reboot the Director
6. After the Director boots back up, login as root, run "`ifconfig reth0`" and verify that the MAC address has been changed to 00:0e:de:ad:be:ef.

CAN'T PING REMOTE GRE TUNNEL END-POINT FROM NON-MIP SFD

CR# Q00946307
Last Updated: 10/25/2004
Affected Releases: 4.0.2.0a
Current Status: No Fix Planned

If GRE is configured in a HA configuration with two or more SFDs in the ASF cluster, you can not ping the remote tunnel end point IP from any of the non-MIP SFD. The work around is to ping from the MIP SFD. This does not affect any GRE functionality. Therefore, no fix is planned for this issue.

SFD MAY REBOOT AUTOMATICALLY AFTER RESTORING CONFIGURATION

CR# Q00969461
Last Updated: 10/25/2004
Affected Releases: 4.0.1 and 4.0.2.0a
Current Status: Work around available

While doing backup restore in an ASF cluster with Check Point synchronization, the SFD may automatically reboot within 3-4 minutes after coming up. This is caused by incorrect initialization of synchronization parameters. The solution is to disable sync (use “/cfg/fw/sync/dis” CLI command) after successfully restoring the configuration, then enable sync (use “/cfg/fw/sync/ena” CLI command) again. This will reboot all SFDs in the cluster.

GRE TUNNEL COLLISION ERRORS CAUSE OSPF NEIGHBOR UP AND DOWN

CR# Q00951990
Last Updated: 10/25/2004
Affected Releases: 4.0.2.0a
Current Status: Open

Enabling GRE tunnel and redistribution of connected routes in OSPF may cause OSPF neighbors go up and down. The work around is to disable redistribution of connected routes if GRE tunnel is configured in the ASF. This can be done using the “*/cfg/net/route/ospf/redist/connected/dis*” CLI menu. This feature is disabled by default.

SFD MAY EXPERIENCE ACCEL-OFF UNDER STRESS WITH NAT AND CHECK POINT SYNCHRONIZATION

CR# Q00694532-01
Last Updated: 10/25/2004
Affected Releases: 4.0.1 and 4.0.2.0a
Current Status: Open

If NAT and Check Point synchronization are configured in an ASF cluster, the SFDs may encounter acceleration off under high traffic. Lab tests have shown that this situation happens only when new connections are added at a rate more than 3000 conn/sec. This stress level is quite high for most networks. Under heavy stress a high percentage of the CPU us used by Check Point synchronization mechanism. This causes loss of communication between the SFD and the SFA, and results in acceleration off. The work around is to set a Firewall kernel parameter (fw_sync_block_new_conns=0) in $FWDIR/modules/fwkern.conf file. The procedure to change the parameter is given below.

1. Login as root into the SFD.
2. run “make-part-rw /isd on”
3. run “make-part-rw / on”
4. edit $FWDIR/modules/fwkern.conf file (use ‘vi’ editor in the SFD) and add the following lines (it is recommended to copy and paste these lines to avoid any typing error)

   ```
   fw_sync_block_new_conns=0
   ```

5. save the file with the changes
6. reboot the SFD
7. Continue step-1 to 6 for all SFDs in the cluster

DISABLING AN INTERFACE DOES NOT BRING BACK STATIC ROUTE TO THE ACCELERATOR

CR# Q00983354
Last Updated: 10/25/2004
Affected Releases: 4.0.1 and 4.0.2.0a
Current Status: Open

If a static route is configured for an IP contained in an interface subnet, then the packets will be forwarded based on the interface routing. There will not be any problem for this scenario. However, if the interface goes down for some reason, the static route will not be pushed to the accelerator. This will create connectivity problem to the specific IP for which a static route is configured. It is recommended not to have a static route contained in an interface subnet.

OSPF LOGS MAY CONSUME LARGE DISK SPACE

CR# Q00924515
Last Updated: 10/25/2004
Affected Releases: 4.0.1 and 4.0.2.0a
Current Status: Open

If the number of OSPF neighbors/routes on ASF is large, enabling all ospf/rip/zebra logging may consumes huge amount of disk space. It is recommended not to enable OSPF logging by default. It should be done only for debugging and during maintenance window.

FIREWALL LICENSE WILL DISAPPEAR AFTER REBOOT IF "CPLIC PUT" COMMAND IS USED TO ADD THE LICENSE

CR# Q00889975
Last Updated: 10/25/2004
Affected Releases: 4.0.1 and 4.0.2.0a
Current Status: Open

Any user with root access can a FW license in ASF using "cplic put" command at the root prompt. This license will disappear after rebooting the SFD. However, the license will remain permanent is it is installed using CLI/WebUI. Therefore, it is recommended to add licenses using CLI/WebUI.

ESTABLISHING TRUST MAY FAIL AFTER RESETTING SIC

CR# Q00957186
Last Updated: 10/25/2004
Affected Releases: 4.0.1 and 4.0.2.0a
Current Status: Open

If "/cfg/fw/accel" is set to "yes", then SFD will reload the default policy after SIC is reset by the user. This may prevent establishing new SIC from the Check Point management station and downloading new policy. It is recommended to set “/cfg/fw/accel” to “no” before resetting SIC and establishing trust. “/cfg/fw/accel” can be set back to “yes” after establishing SIC. If you forgot to set “/cfg/fw/accel” before resting SIC, you may do the followings before establishing trust:

- set “/cfg/fw/accel” to “no”
- run “fw unloadlocal” at the root prompt
- establish trust and push policy
- set “/cfg/fw/accel” back to “yes”

Issues Updated on 08/11/2004

FIREWALL DIRECTOR JOIN WILL FAIL IF '$' IS IN THE ADMIN PASSWORD

CR# Q00951131
Last Updated: 08/11/2004
Affected Releases: 4.0.1
Current Status: Open

The work around for this problem is to make sure that ‘$’ is not used in the admin password.

FIREWALL ACCELERATOR BOOTS UP INCORRECTLY IF IAP AUTO-NEGOTIATION IS DISABLED

CR# Q00919674
Last Updated: 08/11/2004
Affected Releases: 4.0.1
Current Status: No Fix Planned

Depending on the configuration, the ASF cluster may not function properly if auto-negotiation is disabled for any NAAP port including the inter-accelerator port (IAP). Therefore, it is recommended to keep the default values for link properties and keep the auto-neg enabled for all NAAP ports.

Issues Updated on 06/04/2004

ACTIVATING SYN ATTACK PROTECTION CAUSES HIGH CPU USAGE

CR# Q00914964
Last Updated: 06/04/2004
Affected Releases: 4.0.1
Current Status: Open

SYN Attack Protection is part of Smart Defense and is disabled by default. If this is enabled, all TCP packets will be non-accelerated. This will cause the CPU usage of the directors to increase drastically even under moderate traffic. It is recommended to leave SYN Attack Protection disabled.

Nortel is working with Check Point to resolve this issue as soon as possible.

ENABLING ISN SPOOFING CAUSES HIGH CPU USAGE

CR# Q00921499-01
Last Updated: 06/04/2004
Affected Releases: 4.0.1
Current Status: Open

ISN Spoofing is part of Check Point SmartDefense settings and is disabled by default. . If this is enabled, all TCP packets will be non-accelerated. This will cause the CPU usage of the directors to increase drastically even under moderate traffic. It is recommended to leave ISN Spoofing disabled.

SMART DASHBOARD CRASHES AFTER GETTING TOPOLOGY

CR# Q00914969
Last Updated: 06/04/2004
Affected Releases: 4.0.1
Current Status: Open

If the ASF internal net is a subnet of one of the user defined interfaces (for example, is ASF internal net is 192.168.1.192/28 and interface is also defined with IP address 192.168.1.1/24), after doing “Get Topology” for the director, when you try to save it, Smart Dashboard may crash.

To workaround this issue, please delete the ‘eth0’ interface from the topology definition before saving.

DEFAULT GATEWAY AND DEFAULT ROUTE NOT SUPPORTED TOGETHER

CR# Q00860008
Last Updated: 06/04/2004
Affected Releases: 4.0.1
Current Status: Open

When using dynamic routing, you can either configure default gateways or let the ASF learn default routes from its RIP or OSPF peers. If you want ASF to learn the default route from RIP or OSPF, please do not configure any default gateways. When default gateway is configured, any learned default routes are ignored.

ADJACENT OSPF DEVICES SHOULD DEFINE ONLY ONE MD5 KEY FOR OSPF

CR# Q00883420
Last Updated: 06/04/2004
Affected Releases: 4.0.1
Current Status: No Fix Planned

When MD5 key authentication is used for OSPF interfaces, ASF supports only one MD5 key per interface. So the adjacent OSPF device should also have only one MD5 key defined for the OSPF interface that is connected to ASF. If multiple MD5 keys are defined, adjacency may never be formed.

FIREWALL DIRECTOR PANICS WHILE REBOOTING

CR# Q00893753
Last Updated: 06/04/2004
Affected Releases: 4.0.1
Current Status: Open

When the Director is rebooted, at the end of the shutdown process, you may see the director panic. This typically happens after a stress test. This panic may be safely ignored. The Director will reboot and come back up successfully.

Issues Updated on 06/01/2004

DIRECTOR MAY FREEZE UNDER SUSTAINED STRESS

CR# Q00883573
Last Updated: 06/01/2004
Affected Releases: 4.0.1
Current Status: Open

If you have four or more directors in the cluster, one or more directors may lock up under sustained stress. This happens if the traffic is more than 2000 sessions per second per director and the connection limit for the cluster is set to the maximum value of 500,000 in SmartDashboard.
To prevent this problem, please reduce the connection limit for the ASF cluster to 400,000 or less in the ‘Gateway Cluster’ object properties in SmartDashboard.

WEBUI COMMANDS TO FIND SESSIONS ON ACCELERATOR FAILS

CR# Q00860630
Last Updated: 06/01/2004
Affected Releases: 4.0.1
Current Status: Open

In the WebUI, under Diagnostics | Accelerators page, it allows the user to run ‘/info/slb/sess/port’ and ‘/info/slb/sess/find’ commands on the master accelerator. These commands currently do not work and user will always get empty results.

ASF DOES NOT GENERATE ASFEXTRAACCELERATORDETECTED TRAP

CR# Q00887958
Last Updated: 06/01/2004
Affected Releases: 4.0.1
Current Status: Open

ASF does not generate ‘asfExtraAcceleratorDetected’ trap even when it finde more than one accelerator in non high availability mode or more than 2 accelerators in high availability mode.

Issues Updated on 03/04/2004

PROXY IPS NOT ACCESSIBLE AFTER DISABLING HIGH AVAILABILITY

CR# Q00822122
Last Updated: 03/04/2004
Affected Releases: 4.0.1
Current Status: Open

If the ASF is currently configured in HA mode and you disable HA, the accelerator will stop responding to ARP requests for proxy IP address. Please reboot the accelerator to recover.

CANNOT DELETE HOST FROM CLUSTER WHEN SYNC IS ENABLED

CR# Q00882761
Last Updated: 03/04/2004
Affected Releases: 4.0.1
Current Status: Open

When you try to delete a director from the cluster, you get the following error message:

"System is currently busy doing a configuration synch. Please apply after some time."

The workaround is to disable Check Point sync (/cfg/fw/sync/dis) and then delete the director from the cluster. Please be sure to enable sync after the operation succeeds.

Issues Updated on 12/07/2003

‘STATE SYNCHRONIZATION OF THIS MACHINE IS AT RISK’ MESSAGE

CR# Q00742217
Last Updated: 12/07/2003
Affected Releases: 4.0.1
Current Status: Open

If you have Check Point Sync enabled and the firewall is not able to keep up with the amount of sync traffic being generated, you will get the above message in the Check Point SmartView Tracker. If you are using a switch or hub in your sync network, make sure it supports 100 Mbps speed and that it does negotiate to 100 Mbps full duplex. You could also reduce the amount of sync traffic by selectively disabling sync for short sessions like HTTP. To disable sync for a particular service, open Check Point SmartDashboard, go to 'Manage | Services | <service> | Advanced' and uncheck 'Synchronize connections on cluster'. Then install the policy on the ASF.

LOCAL LICENSES INSTALLED VIA SMARTUPDATE DISAPPEAR

CR# Q00743399
Last Updated: 12/07/2003
Affected Releases: 4.0.1
Current Status: Open

Check Point SmartUpdate allows you to install both central licenses as well as local license remotely. However, you should use SmartUpdate only to install central licenses. If you install a local license using SmartUpdate, it may be automatically deleted by the ASF later on. To install local licenses, always use '/cfg/pnp/add' CLI on the ASF.

WITH OSPF, AREA 0 CANNOT BE DISABLED

CR# Q00717195
Last Updated: 12/07/2003
Affected Releases: 4.0.1
Current Status: Open

When configuring OSPF, ASF will not allow the user to disable area 0 or make it inactive. There is currently no workaround for this.

Issues Updated on 10/16/2003

DYNAMIC ROUTING ISSUES

Last Updated: 10/16/2003
Affected Releases: 4.0.1
Current Status: Open

If virtual links are configured with OSPF, Accelerator fail over may cause the ospfd process to die. If this happens, login to the Director as root and restart the ospfd process using "service ospfd start" command. (Q00719480)

If virtual links are configured with OSPF and an interface is disabled, enabled or deleted, it may cause the ospfd process to die. If this happens, login to the Director as root and restart the ospfd process using "service ospfd start" command. (Q00725434)

With OSPF, if an area is defined as type NSSA, ASF tries to inject LSU type 4 routes into its neighbor in NSSA area. (Q00724996)

With OSPF, if an area is defined as type NSSA, ASF does not send default route to its neighbor in NSSA area. (Q00725585)

With OSPF configured, ASF does not send summary-range to its neighbor. (Q00733566)

OSPF AND ACCELERATOR / MIP FIREWALL DIRECTOR FAIL OVER

Last Updated: 10/16/2003
Affected Releases: 4.0.1
Current Status: Open

- Accelerator fail over without MIP Firewall Director fail over: No ospf neighbor adjacency is lost, however, 3-6 sec drop of packets will occur until the upstream/downstream routers arp tables re-learns "new" master VRRP MAC address.
- MIP ISD fail over [with / without Accelerator fail over]: This causes rebuild of neighbor adjacency (Q00611147) and hence upstream/downstream routers must relearn OSPF routes. To minimize downtime during this period, it is recommended to set the router dead-time interval to 120 seconds for routers connected to the ASF.

CHECK POINT SYNC STOPS WORKING AFTER CHANGING SYNC DEVICE

CR# Q00748787
Last Updated: 10/16/2003
Affected Releases: 4.0.1
Current Status: Open

If you change the Check Point sync device using the “/cfg/fw/sync/dev” command, please check the sync state using the “cphaprob stat” command from the root login. If any of the Directors report sync state as down, bounce the firewall using “cpstop; cpstart” command.

HTTP WORM CATCHER AND CONCURRENT CONNECTIONS

CR# Q00764267
Last Updated: 10/16/2003
Affected Releases: 4.0.1
Current Status: No fix planned

HTTP Worm Catcher is a new Smart Defense feature from Check Point. Enabling this feature causes a large amount of memory to be used when the number of concurrent connections is high. Worm Catcher is supported with up to 100,000 concurrent connections. If your traffic is above this limit, please keep Worm Catcher disabled.

10 APPENDIX-B: LIST OF KNOWN ISSUES IN HFA RELEASES

This Appendix provides detailed explanation on all the issues found and/or fixed in 3.5.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

HFA 14 – R55 (05/31/2005)

- No issue has been found in HFA 14