



Alteon Switched Firewall (ASF) System, Version 3.5.x

Readme

Version 3.19
14 Dec, 2006

Nortel Networks, Inc.

Table of Contents

1	Introduction.....	1
2	Status of Known Issues and Limitations.....	2
3	Software Upgrade	12
4	Alteon Switched Firewall (ASF) System, Version 3.5.1.0g (10/16/2003).....	12
4.1	New Hardware Platform	12
4.2	Supported Check Point Releases	12
4.3	Configuration of the Gateway Cluster Object	12
4.4	Supported Features.....	12
4.4.1	DHCP Relay Support.....	12
4.4.2	Sync Device Configuration.....	13
4.4.3	IDS Load Balancing.....	14
4.5	Bugs Fixed Since 3.2.1.0b	14
5	Alteon Switched Firewall (ASF) System, Version 3.5.1.4a (11/04/2003)	15
5.1	Supported Hardware Platforms.....	15
5.2	Supported Check Point Releases:	15
5.3	Bugs Fixed Since 3.5.1.0g Release.....	15
6	Alteon Switched Firewall (ASF) System, Version 3.5.1.10 (12/07/2003).....	16
6.1	Supported Hardware Platforms.....	16
6.2	Supported Check Point Releases	16
6.3	Bugs Fixed Since 3.5.1.4a Release	16
7	Alteon Switched Firewall (ASF) System, Version 3.5.2 (03/04/2004)	17
7.1	Supported Hardware Platforms.....	17
7.2	Supported Check Point Releases	17
7.3	Supported Features.....	17
7.3.1	Check Point VPN Support with NG AI (R54).....	17
7.3.2	Check Point SmartView Monitor Support.....	17
7.3.3	Check Point Express License Support for FP-3.....	17
7.3.4	Audit Log Support	18
7.3.5	Backup/Restore of Directors.....	18
7.3.6	Remote SSH Login to Linux Shell	18
7.3.7	Mix-n-Match Directors in the Cluster.....	18
7.3.8	Change In Proxy ARP Implementation	18
7.3.9	Localnet Command Removed.....	19
7.4	Bugs Fixed Since 3.5.1.10 Release.....	19
8	Alteon Switched Firewall (ASF) System, Version 3.5.2.1 (03/22/2004).....	20
8.1	ASF 3.5.2.1 Replaces ASF 3.5.2	20
8.2	Bugs Fixed Since 3.5.2 Release.....	20
9	Alteon Switched Firewall (ASF) System, Version 3.5.3 (06/07/2004)	21
9.1	Supported Hardware Platforms.....	21
9.2	Supported Check Point Releases	21
9.3	Configuration of the Gateway Cluster Object	21
9.4	Supported Features.....	21
9.4.1	NAAP VLAN ID Configuration.....	21

- 9.5 Bugs Fixed Since 3.5.2.1 Release..... 23
- 10 Alteon Switched Firewall (ASF) System, Version 3.5.4 (11/01/2004) 24
 - 10.1 Supported Hardware Platforms..... 24
 - 10.2 Supported Check Point Releases 24
 - 10.3 Supported Features..... 24
 - 10.3.1 CLI to Set sysname for Directors..... 24
 - 10.3.2 Automatic Check Point Upgrade 24
 - 10.3.3 Upgrade from CD-ROM..... 25
 - 10.3.4 Configurable AIM Connection Table Size 25
 - 10.3.5 MIB files can be downloaded from the WebUI..... 25
 - 10.4 Bugs Fixed Since 3.5.3 Release..... 25
- 11 Alteon Switched Firewall (ASF) System, Version 3.5.5 (9/15/2005) 26
 - 11.1 Supported Hardware Platforms..... 26
 - 11.2 Supported Check Point Releases 26
 - 11.3 Supported Features..... 26
 - 11.3.1 Usability Improvement 26
 - 11.3.2 MP Flow Control 28
 - 11.4 Bugs Fixed Since 3.5.4 Release..... 28
- 12 Alteon Switched Firewall (ASF) System, Version 3.5.6 (11/23/2005) 29
 - 12.1 Supported Hardware Platforms..... 29
 - 12.2 Supported Check Point Releases 29
 - 12.3 Configuration of the Gateway Cluster Object for R60 30
 - 12.4 Bugs Fixed Since 3.5.5 Release..... 30
- 13 Alteon Switched Firewall (ASF) System, Version 3.5.6.2 (07/07/2006) 30
 - 13.1 Supported Hardware Platforms..... 30
 - 13.2 Supported Check Point Releases 31
 - 13.3 Bugs Fixed Since 3.5.6 Release..... 31
- 14 Alteon Switched Firewall (ASF) System, Version 3.5.7 (07/20/2006) 32
 - 14.1 Supported Hardware Platforms..... 32
 - 14.2 Supported Check Point Releases 32
 - 14.3 Configuration of the Gateway Cluster Object for R60 33
 - 14.4 Bugs Fixed Since 3.5.6 Release..... 33
- 15 Alteon Switched Firewall (ASF) System, Version 3.5.7.4 (12/14/2006) 34
 - 15.1 Supported Hardware Platforms..... 34
 - 15.2 Supported Check Point Releases 34
 - 15.3 Bugs Fixed Since 3.5.7 Release..... 35
- 16 Appendix-A: List of Known Issues 35

Change Log

Version	What	When	Who
1.0	Initial draft – Consolidated readme files for all 3.5.x releases (3.5.1.0g, 3.5.1.4a, and 3.5.1.10d). Also added Section-7 for 3.5.2 release.	03/04/2004	Satya Pradhan Rajesh Vijayakumar
2.0	Added Linux kernel mremap vulnerability	03/18/2004	Satya Pradhan
2.1	Added Section-8 for ASF 3.5.2.1 release. Added Q00858866 to list of known issues.	03/22/2004	Rajesh Vijayakumar
2.2	Added Q00879931 to list of known issues Added Q00878406 to list of known issues Added 040312-80021 to list of issues fixed in 3.5.1.0g Updated Section 3: Upgrading to ASF 3.5.x	04/02/2004	Rajesh Vijayakumar
2.3	Added Q00733964 to list of known issues	04/20/2004	Rajesh Vijayakumar
2.4	Added Q00901409 to list of known issues	05/07/2004	Rajesh Vijayakumar
2.5	Added Q00909049 to list of known issues	05/18/2004	Rajesh Vijayakumar
2.6	Added Section-9 for ASF 3.5.3 release and updated other sections for ASF 3.5.3 release.	06/07/2004	Satya Pradhan
2.7	Added Q00939253, Q00895609-01 and Q00939269 to the list of known issues. The first two issues are fixed in 3.5.3. Also added an item for change in LED behavior in the back switch to the list of known issues.	07/01/2004	Satya Pradhan
2.8	Clarified that the fix for Q00879931 is available only in 3.5.3-FP4 (R54) release. Updated Q00901409 to mention that this issue affects all accelerators (not just ASF 6400). Also, added Q00951131-01, Q00919674-01, Q00955134-01, and Q00957226.	08/10/2004	Satya Pradhan
2.9	Added Q00966728 to list of known issues.	08/18/2004	Satya Pradhan
2.10	Added Q00973930 to list of known issues.	08/31/2004	Satya Pradhan
2.11	Added Q00991305 and Q00964274 to list of known issues.	09/31/2004	Satya Pradhan
3.0	Added Section-10 for ASF 3.5.4 release and updated other sections (particularly Section 3 on upgrade) for ASF 3.5.4 release.	10/25/2004	Satya Pradhan
3.1	Added Q01001073 to list of known issues.	11/02/2004	Satya Pradhan
3.2	Added Q00914964, Q00921499 and Q01028626 to the list of known issues.	11/16/2004	Satya Pradhan

3.3	Added some comments to the details for Q00914964 and Q00921499.	12/14/2004	Satya Pradhan
3.4	Changed the status of Q00737761 to “Fixed.”	01/17/2005	Satya Pradhan
3.5	Added Q00862911-01 and Q01081888-01 to the list of known issues.	02/18/2005	Satya Pradhan
3.6	Added Q01076608 to the list of known issues.	03/18/2005	Satya Pradhan
3.7	Added Q01106902-01 to the list of known issues.	04/12/2005	Satya Pradhan
3.8	Added Section 4 and Appendix B for the release of HFA 415 (FP4) and HFA 13 (R55).	04/29/2005	Satya Pradhan
3.9	Updated Section 4 and Appendix B for the release of HFA 14 (R55).	05/31/2005	Satya Pradhan
3.10	Added Section 12 for 3.5.5 release.	09/15/2005	Satya Pradhan
3.11	Updated section 4 for HFA 16 (R55) release. Also, added Section 13 for 3.5.6 release.	11/23/2005	Satya Pradhan
3.12	Added Q01187253 to the list of known issues. Removed the section on HFA releases for 3.5.x. We have a separate release note for HFA releases.	12/12/2005	Satya Pradhan
3.13	Added R61 contents	07/07/2006	Ganesh Lakshmanan
3.14	Added 3.5.7 contents	07/20/2006	Santhosh Balasubramanian
3.15	Changed the status of Q00694532 to “Fixed”	07/27/2006	Santhosh Balasubramanian
3.16	Added Q01338744 to the list of known issues and marked the status to “Fixed”	08/03/2006	Santhosh Balasubramanian
3.17	Updated the fix details of Q01106902-01	08/21/2006	Santhosh Balasubramanian
3.18	Added ‘special character admin password’ to the list of known issues	08/25/2006	Ashok P
3.19	Added section 15 for 3.5.7.4 release	12/14/2006	Samuel Praveen

1 INTRODUCTION

This is the consolidated readme for all ASF 3.5.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 3.5.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 3.5.x software release. The next section (Section-3) describes the procedure to upgrade the old software to a 3.5.x release.

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

2 STATUS OF KNOWN ISSUES AND LIMITATIONS

All the known issues found and/or fixed in 3.5.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 that 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-3.5.x releases.

CR #	Description of Issues and Limitations	Last Updated	Current Status	Status in Different Releases											
				3.5.1.0g		3.5.1.10d	3.5.2	3.5.2.1	3.5.3	3.5.4	3.5.5	3.5.6	3.5.6.2	3.5.7	3.5.7.4
Q01311541	PARP IP address issue	7/20/2006	Fixed												
Q01379352	DST 2007 daylight saving issue	7/20/2006	Fixed												
Q01339316	Redistributes a non-existent default route into OSPF	7/20/2006	Fixed												
Q01142033	/info/det does NOT display the correct state of acc	7/20/2006	Fixed												
Q01242647-01	WEBUI: Not able to upload package using WEBUI	7/20/2006	Fixed												
Q01266907	SSI Restarting	7/20/2006	Fixed												
Q01106902-01	Health Check Daemon and Config Daemon may not work	7/20/2006	Fixed												

CR #	Description of Issues and Limitations	Last Updated	Current Status	Status in Different Releases												
				3.5.1.0g		3.5.1.10d	3.5.2	3.5.2.1	3.5.3	3.5.4	3.5.5	3.5.6	3.5.6.2	3.5.7	3.5.7.4	
	properly after 248 days of uptime															
Q01338744	mond log file is not getting rotated when we run the system more than 10 days	8/03/2006	Fixed										✗	✗	✓	
Q01380368	R61: Firewall template did not start even after pushing policy	7/20/2006	Fixed											✗	✓	
Q01187253	Reset SIC does not work from BBI	7/20/2006	Open										✗	✗	✗	✗
Q01258039	RIPv2 doesn't work in R60	11/23/2005	Open										✗	✗	✗	
Q01296152-01	CLI: /maint/debug/fw/version in R61 has problem	7/20/2006	Fixed											✗	✓	
Q01245413	/opt/tng/bin/lb is not giving the expected output	7/20/2006	Fixed											✗	✓	
Q01152681	VPN problem in R60	11/23/2005	Work Around Available										✓			
Q01139113	Problem with SFA ARP responses	11/23/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓		
Q01061608	Confusing output of /info/acc	11/23/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓			
Q01125484	Error in MIB File	11/23/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓			
Q01187353	"/info/clu" shows "Firewall Synchronization Status: Error"	7/20/2006	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	
Q01190579	Changing timezone on the director causes Director to lose contact with the Accelerator	9/15/2005	Open	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q01199949	Adding VLAN I/F causes impact	9/15/2005	Open	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

CR #	Description of Issues and Limitations	Last Updated	Current Status	Status in Different Releases												
				3.5.1.0g		3.5.1.10d	3.5.2	3.5.2.1	3.5.3	3.5.4	3.5.5	3.5.6	3.5.6.2	3.5.7	3.5.7.4	
	on existing VLAN traffic															
Q01208947	Adding interface or changing IP address of interface may cause SFA failover	9/15/2005	Open	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q01023162	TCPdump or tethereal displays inbound traffic twice	9/15/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✓				
Q01081888-01	SP ARP Table Corruption after Port Move	9/15/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✓				
Q01028405	ASF Port Stats via CLI	9/15/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✓				
Q01147448	VRRP Buffer allocation failure causing 100% MP CPU	9/15/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✓				
Q01099841	Kernel Warning Message displayed on 3.5.x	9/15/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✓				
Q01065271	MP CPU reaches 100% if default route learned though OSPF	9/15/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✓				
Q00999034	MP Flow Control	9/15/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✓				
Q01035151-01	Trunk ports may cause L2 loop after Accelerator reboot	9/15/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✓				
Q00983584	Need a description field in stactic routes	9/15/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✓				
Q01048329	Incorrect MAC addresses shown in display	9/15/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✓				
Q00951131-01	Firewall Director Join will Fail if '\$' is in the Admin Password	9/15/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✓				
Q00976886	ASF replies to proxyARP even after NAT/proxyARP configuration is deleted	9/15/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✓				

CR #	Description of Issues and Limitations	Last Updated	Current Status	Status in Different Releases												
				3.5.1.0g		3.5.1.10d	3.5.2	3.5.2.1	3.5.3	3.5.4	3.5.5	3.5.6	3.5.6.2	3.5.7	3.5.7.4	
Q01000256	VRRP priority is configurable via WebUI	9/15/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✓				
Q01076608	Long TCP Sessions may Timeout if the SFA Uptime is more than 194 days	9/15/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✓				
Q01028626	Traffic may be affected while applying configuration	9/15/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✗	✓				
Q00862911-01	Multicast Traffic Causes Looping in Trunk Group	02/18/2005	Fixed			✗	✗	✗	✗	✗	✗	✓				
Q00737761	Sync Through VNIC Problem	01/17/2005	Fixed	✗	✗	✗	✗	✗	✗	✗	✓					
Q01001073	Fragments do not pass through ASF with 5300 accelerators	11/02/2004	Fixed	✗	✗	✗	✗	✗	✗	✗	✓					
Q00991305	ARP entry corruption that may cause connectivity problem	10/25/2004	Fixed	✗	✗	✗	✗	✗	✗	✗	✓					
Q00964274	MP CPU uses becomes high if default gateway is learned through dynamic routing	10/25/2004	Fixed	✗	✗	✗	✗	✗	✗	✗	✓					
Q00966728	High CPU usage when ELA Logging is enabled	10/25/2004	Fixed	✗	✗	✗	✗	✗	✗	✗	✓					
Q00955134-01	Check Point ASN-1 Vulnerability	10/25/2004	Fixed							✗	✓					
Q00957226	Upgrade does not update fwkern.conf file	10/25/2004	Fixed							✗	✓					
Q00914617	/isd partition may get full after multiple upgrades from 3.0.x to 3.5.3	10/25/2004	Patch Available							✓	✓					
Q00886219	The CLI shows Accelerator type 6400 as a supported Accelerator	10/25/2004	Fixed							✗	✓					
Q00921793-	“fwaccel templates” Command	10/25/2004	Fixed							✗	✓					

CR #	Description of Issues and Limitations	Last Updated	Current Status	Status in Different Releases												
				3.5.1.0g		3.5.1.10d	3.5.2	3.5.2.1	3.5.3	3.5.4	3.5.5	3.5.6	3.5.6.2	3.5.7	3.5.7.4	
01	Prints IP Addresses in Reverse Order															
Q00922413	Accelerator Instability Caused by FIFO	10/25/2004	Fixed							✗	✓					
Q00969461	SFD may reboot automatically after restoring configuration	10/25/2004	Open				✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q00694532	SFD may experience Accel-off under stress with NAT and Check Point synchronization	07/27/2006	Fixed				✗	✗	✗	✗	✗	✓				
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				✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q00972348	Could configure SFD host name with special character ("")	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				✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q00973930	If auto-neg is enabled, synch may not work with different SFD hardware in ASF cluster	08/31/2004	No Fix Planned				✗	✗	✗	✗	✗	✗				
Q00919674-01	Firewall Accelerator Boots up Incorrectly if IAP Auto-Negotiation is Disabled	08/10/2004	No Fix Planned	✗	✗	✗	✗	✗	✗	✗	✗	✗				
Q00879931	Long TCP Sessions are Timed out	08/10/2004	Fixed	✗	✗	✗	✗	✗	✗	✓						

CR #	Description of Issues and Limitations	Last Updated	Current Status	Status in Different Releases											
				3.5.1.0g		3.5.1.10d	3.5.2	3.5.2.1	3.5.3	3.5.4	3.5.5	3.5.6	3.5.6.2	3.5.7	3.5.7.4
	Even if not Idle														
Q00901409	Firewall Directors Keep Losing Contact With Each Other	08/10/2004	Fixed	✗	✗	✗	✗	✗	✓						
Q00939253	Connections may be deleted after TCP Start Timeout	07/01/2004	Fixed	✗	✗	✗	✗	✗	✓						
	Backup Accelerator LED Blinks Like Active Accelerator	07/01/2004	Fixed						✓						
Q00895609-01	snmpagentd May Take 99% of the CPU	07/01/2004	Fixed	✗	✗	✗	✗	✗	✓						
Q00939269	fw Daemon may Take More Than 95% CPU After Reboot	07/01/2004	Open	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q00880890	Open-SSL vulnerability (CAN-2004-0079)	06/07/2004	Fixed	✗	✗	✗	✗	✗	✓						
Q00881896	Check Point H323 vulnerability	06/07/2004	Fixed	✗	✗	✗	✗	✗	✓						
Q00864792	Director panics when handling fragmented IGMP packets	06/07/2004	Fixed	✗	✗	✗	✗	✗	✓						
Q00804868	OSPF has to be restarted after changing OSPF configuration	06/07/2004	Fixed	✗	✗	✗	✗	✗	✓						
Q00900430	Hash algorithm for selecting trunk port does not maintain session persistency for accelerated connections	06/07/2004	Fixed	✗	✗	✗	✗	✗	✓						
Q00914964	Activating SYN Attack Protection Causes High CPU Usage	06/07/2004	Open	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q00921499-01	Enabling ISN Spoofing Causes High CPU Usage	06/07/2004	Open	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q00914964	TCP sessions are not accelerated when SYN defender is enabled	12/14/2004	Fixed				✗	✗	✗	✓					
Q00921499	TCP sessions are not accelerated when ISN spoofing is enabled	12/14/2004	Fixed				✗	✗	✗	✓					

CR #	Description of Issues and Limitations	Last Updated	Current Status	Status in Different Releases												
				3.5.1.0g		3.5.1.10d	3.5.2	3.5.2.1	3.5.3	3.5.4	3.5.5	3.5.6	3.5.6.2	3.5.7	3.5.7.4	
Q00915973	SFD may loose contact with switch after upgrade	06/07/2004	Open							✗	✗	✗	✗	✗	✗	✗
Q00916164	ASF 3.5.3 does not support different AD3 hardware in the same cluster	06/07/2004	Open							✗	✗	✗	✗	✗	✗	✗
Q00914969-01	FP4 (R54) smart dashboard will crash if SFD internal network is a subnet of data network	06/07/2004	Open							✗	✗	✗	✗	✗	✗	
Q00855084	“fwaccel templates” Command Times Out	06/07/2004	Fixed	✗	✗	✗	✗	✗	✗	✓						
Q00878406	Remote SSH User Cannot Login After Upgrade	06/07/2004	Fixed					✗	✗	✓						
Q00866909	Linux Kernel do_mremap() Vulnerability	06/07/2004	Fixed				✗	✗	✗	✓						
Q00834278	TCP and UDP Fragments Not Being NAT'ed Correctly with R54	06/07/2004	Fixed	✗	✗	✗	✗	✗	✗	✓						
Q00726119	'cfgd' Freezes When Trying to Change AIM State	06/07/2004	Fixed	✗	✗	✗	✗	✗	✗	✓						
Q00748462	Active FTP Fails With Hide NAT	06/07/2004	Fixed	✗	✗	✗	✗	✗	✗	✓						
Q00909049	5014-x305 Firewall Director Does Not Recognize Dual Fiber Card	05/18/2004	Fixed	✗	✗	✗	✗	✓								
Q00733964	Firewall Director Panics While Rebooting	04/02/2004	Fixed	✗	✗	✗	✗	✓								
Q00858866	Accelerator Panic in Fw_proc_data_tunnel() Routine	03/22/2004	Fixed				✗	✓								
	HTTP Security Server Vulnerability	03/04/2004	Patch Available	✓	✓	✓	✓	✓	✓	✓	✓					
	Multiple Failure Scenarios	03/04/2004	Fixed	✗	✗	✗	✗	✓								
	Port Mirroring No Longer	03/04/2004	No Fix	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗			

CR #	Description of Issues and Limitations	Last Updated	Current Status	Status in Different Releases												
				3.5.1.0g		3.5.1.10d	3.5.2	3.5.2.1	3.5.3	3.5.4	3.5.5	3.5.6	3.5.6.2	3.5.7	3.5.7.4	
	Supported with 5x00 Accelerators		Planned													
Q00849018	Validation Error After Upgrade	03/04/2004	Open	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q00849035	Proxy ARP for SFD Subnet Not Supported	03/04/2004	Fixed	✗	✗	✗	✓									
Q00822122	Proxy IPs Not Accessible After Disabling High Availability	03/04/2004	Open				✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q00829630	Cannot Delete Host From Cluster	03/04/2004	Open				✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q00781453	'/info/clu' Reports CPU Usage as 0%	03/04/2004	Fixed	✗	✗	✗	✓									
Q00768627-01	Static Routes Don't Disappear Even When Interface Goes Down	03/04/2004	Fixed	✗	✗	✗	✓									
Q00784707	Filter Based on Broadcast or Multicast Address Does Not Work	03/04/2004	Fixed	✗	✗	✗	✓									
Q00746960	Supernetted Routes May Cause 100% MP CPU Usage	03/04/2004	Fixed	✗	✗	✗	✓									
Q00746099	Stateful Session Fail Over Problem	03/04/2004	Fixed	✗	✗	✗	✓									
Q00851121	Join Fails if ASF Cluster Already Contains 2 or More Directors	03/04/2004	Fixed	✗	✗	✗	✓									
Q00842221	When Firewall is Started, Director May Run Out of Memory	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	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q00786623	Email Archive Does not Include '/var/tmp/tngsys.log'	12/07/2003	Open	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q00717195	With OSPF, Area 0 Cannot be	12/07/2003	Open	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

CR #	Description of Issues and Limitations	Last Updated	Current Status	Status in Different Releases											
				3.5.1.0g		3.5.1.10d	3.5.2	3.5.2.1	3.5.3	3.5.4	3.5.5	3.5.6	3.5.6.2	3.5.7	3.5.7.4
	Disabled														
Q00722198	Accelerator Stats Show Discards on the Outbound	12/07/2003	Open	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q00784709	'/maint/debug/ac1/btinfo' Not Supported with 5x00 Accelerators	12/07/2003	Open			✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q00803000	'Accelerator Session Table Overflow' Message in Syslog	12/07/2003	Fixed		✗	✓									
Q00783207	Acceleration Not Restarted Even Though '/cfg/fw/accel' is Set	12/07/2003	Fixed	✗	✗	✓									
	IDSLB Not Supported on 5x00 Accelerators	11/04/2003	No Fix Planned		✗	✗	✗	✗	✗	✗	✗	✗			
	Port Mirroring Limitation on 5x00 Accelerators	11/04/2003	No Fix Planned		✗	✗	✗	✗	✗	✗	✗	✗			
Q00780070	Director Can Upgrade Only Directly Connected Accelerator's Firmware	11/04/2003	No Fix Planned		✗	✗	✗	✗	✗	✗	✗	✗			
Q00743287	VLAN 4092 is Reserved	11/04/2003	Fixed	✗	✓										
Q00771385	ELA Logging Feature Does Not Work	11/04/2003	Fixed	✗	✓										
	VRRP MAC Feature is Not Available	10/16/2003	No Fix Planned	✗	✗	✗	✗	✗	✗	✗	✗	✗			
	Dynamic Routing Issues	10/16/2003	Open	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	OSPF and Accelerator / MIP Firewall Director fail over	10/16/2003	Open	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q00742985	Maximum Number of Interfaces Supported is 250	10/16/2003	Open	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q00741429	Auto-Join Failure	10/16/2003	Open	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Q00748787	Check Point Sync Stops Working	10/16/2003	Open	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

CR #	Description of Issues and Limitations	Last Updated	Current Status	Status in Different Releases											
				3.5.1.0g		3.5.1.10d	3.5.2	3.5.2.1	3.5.3	3.5.4	3.5.5	3.5.6	3.5.6.2	3.5.7	3.5.7.4
	After Changing Sync Device														
Q00764267	HTTP Worm Catcher and Concurrent Connections	10/16/2003	No Fix Planned	☒	☒	☒	☒	☒	☒	☒					
Q00747993	Missing '/var/tmp/tngsys.log' File	10/16/2003	Open	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Q00733543	'Packet Out of State' Message under Stress	10/16/2003	Open	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Q00683652	Policy Installation Fails with Error "TCP connectivity failure"	10/16/2003	Open	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Q00724862	Firewall Director Takes More Than 10 Minutes to Recover	10/16/2003	Open	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Q00734318	Auto Negotiation Off with FE Links	10/16/2003	Open	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Q00617850	Interface and Static Route in the Same Subnet	10/16/2003	Open	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

3 SOFTWARE UPGRADE

Upgrading to 3.5.7.4_R62 from previous versions is not supported. Only clean ISO installation is supported

4 ALTEON SWITCHED FIREWALL (ASF) SYSTEM, VERSION 3.5.1.0G (10/16/2003)

4.1 New Hardware Platform

ASF 3.5.1.0g introduces a new Director ASF 5014 and new Accelerator ASF 6400. The new Accelerator and Director can be paired only with each other and the combination is called ASF 6414. The 6400 Accelerator has 24 FE ports and 4 gig ports and supports 1 million concurrent connections. ASF 6414 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 3.5.1.0g is supported only on ASF 5014 Director. It should not be installed on the existing hardware platforms like ASF 5010 and 5008. Nortel will soon be releasing a 3.5.1.x build that will support all existing platforms.

4.2 Supported Check Point Releases

ASF 3.5.1.0g supports Check Point NG with Application Intelligence Build 315.

4.3 Configuration of the Gateway Cluster Object

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

4.4 Supported Features

The following new features are supported in this release.

4.4.1 DHCP Relay Support

Since the DHCP request is an IP broadcast, it has the limitation that the DHCP server should be on the same LAN segment as the client. A DHCP relay agent overcomes this limitation by converting the broadcast DHCP request into a unicast packet and sending it to the server on a different LAN segment. When the DHCP Relay Agent gets the response, it forwards the response to the client.

ASF 3.2.1.0b has a built-in DHCP Relay Agent. It can be configured using the `"/cfg/net/dhcprl"` command.

If you enable DHCP relay on the ASF, please be sure to add rules to your policy allowing the following traffic:

- DHCP request from clients to ASF
- DHCP reply from ASF to clients
- DHCP request from ASF to DHCP servers
- DHCP reply from DHCP servers to ASF

Please define your own DHCP request and reply services in SmartDashboard instead of using the built-in 'dhcp-req-localmodule' and 'dhcp-rep-localmodule' services. These built-in services are not intended for DHCP relay.

For defining the DHCP Request service, please use the following parameters:

- Name: dhcp-request
- Comment: DHCP Request for ASF DHCP Relay
- Port: 67
- Advanced
 - Source Port: 68
 - Protocol Type: None
 - Accept Replies: No
 - Match for Any: No
 - Synchronize on Cluster: No

For defining the DHCP Reply service, please use the following parameters:

- Name: dhcp-reply
- Comment: DHCP Reply for ASF DHCP Relay
- Port: 68
- Advanced
 - Source Port: 67
 - Protocol Type: None
 - Accept Replies: No
 - Match for Any: No
 - Synchronize on Cluster: No

You can add these new service definitions in SmartDashboard using "Manage | Services | New | UDP" menu.

4.4.2 Sync Device Configuration

ASF 3.2.1.0b allows you to select which NIC to use as the sync device. For example, on the 5010 Firewall Director, you can choose either one on the FE ports for sync. Please use the `"/cfg/fw/sync/dev"` CLI to select the sync device. You also have the option to disable auto negotiation for the sync device and set the speed and duplex manually. These settings are also under the `"/cfg/fw/sync"` command.

4.4.3 *IDS Load Balancing*

The IDS load balancing feature allows you to connect your IDS servers directly to the Accelerator and have the Accelerator load balance them. IDS load balancing is available only with the 6400 Accelerator. Multiple VLANs can be monitored by the same IDS group. In this case, traffic to the IDS servers will be tagged and the IDS server should be capable of handling this. Some IDS servers transmit RST packets to block suspicious activity. This is not supported in the current implementation. Some IDS servers are capable of using Check Point's OPSEC interface to dynamically change the policy in order to block an intruder. This will work with ASF only if the IDS server has a separate NIC card other than the sensor to talk to ASF.

4.5 Bugs Fixed Since 3.2.1.0b

- Added SNMP traps for session table overflow and Accelerator CPU usage
- Accelerator link events are not SNMP trapped (Q00658709-01, 030424-28268)
- SNMP Traps not generated when Sync port fails (Q00658712-01, 030424-28272)
- Replacing defective Director requires Accelerator reboot (Q00628746)
- Set link speed and duplex for sync device (Q006587016)
- WebUI to display which is the master Accelerator (Q00658719, 030424-28277)
- For 10/100 port with auto negotiation off, the port does not start forwarding traffic until you bounce the link (Q00665533)
- Incorrect CPU usage reported under '/info/clu' (Q00740251)
- Configuring MD5 key for OSPF gives "Unexpected error" message (040312-80021)

5 ALTEON SWITCHED FIREWALL (ASF) SYSTEM, VERSION 3.5.1.4A (11/04/2003)

5.1 Supported Hardware Platforms

ASF 3.5.1.4a supports the following ASF platforms:

ASF 5308 (5300 Accelerator + 5008 Director)

ASF 5408 (5400 Accelerator + 5008 Director)

ASF 5610 (5600 Accelerator + 5010 Director)

ASF 5710 (5700 Accelerator + 5010 Director)

For ASF 6414 platform, please use the 3.5.1.0g version of software.

ASF 3.5.1.4a replaces the 3.2.1.0b release. If you are running 3.2.1.0b, it is strongly recommended that you upgrade to 3.5.1.4a. The 3.2.1.0b release has a memory leak bug that will force you to reboot the Directors every 3-4 months.

5.2 Supported Check Point Releases:

ASF 3.5.1.0g supports Check Point NG with Application Intelligence Build 315.

5.3 Bugs Fixed Since 3.5.1.0g Release

ELA Logging Feature Does Not Work (Q00771385)

User Allowed to Configure Reserved VLAN 4092 (Q00743287)

SNMP Agent Gets Statistics From Backup Instead of Master Accelerator (Q00665610)

cfgd Goes Into Tight Loop on Startup (Q00784060) (031015-17793)

6 ALTEON SWITCHED FIREWALL (ASF) SYSTEM, VERSION 3.5.1.10 (12/07/2003)

6.1 Supported Hardware Platforms

ASF 3.5.1.10 supports the following hardware platforms:

- ASF 5309 (5300 Accelerator + 5009 Director) (new)
- ASF 5409 (5400 Accelerator + 5009 Director) (new)
- ASF 5614 (5600 Accelerator + 5014 Director) (new)
- ASF 5714 (5700 Accelerator + 5014 Director) (new)
- ASF 5308 (5300 Accelerator + 5008 Director)
- ASF 5408 (5400 Accelerator + 5008 Director)
- ASF 5610 (5600 Accelerator + 5010 Director)
- ASF 5710 (5700 Accelerator + 5010 Director)
- ASF 6414 (6400 Accelerator + 5014 Director)

6.2 Supported Check Point Releases

ASF 3.5.1.10 supports Check Point NG with Application Intelligence Build 315.

6.3 Bugs Fixed Since 3.5.1.4a Release

- CERT Advisory CA-2003-24 Buffer Management Vulnerability in OpenSSH
- CERT Advisory CA-2003-26 Multiple Vulnerabilities in SSL/TLS Implementations
- Acceleration Not Restarted Even Though '/cfg/fw/accel' is Set (Q00783207)
- '/info/det' Says 'Contains a stale configuration and needs reconfiguration' (Q00792569)
- '/info/clu' reports 'Inet server is not running' (Q00794612)
- 'cfgd' Dies When DHCP Relay is Enabled (Q00796605)
- 'Accelerator Session Table Overflow' Message in Syslog (Q00803000)

7 ALTEON SWITCHED FIREWALL (ASF) SYSTEM, VERSION 3.5.2 (03/04/2004)

Note: Please use ASF 3.5.2.1 instead of ASF 3.5.2. If you have already installed ASF 3.5.2, please upgrade to ASF 3.5.2.1. ASF 3.5.2.1 fixes a critical issue (Q00858866) in ASF 3.5.2.

7.1 Supported Hardware Platforms

ASF 3.5.2 supports the new 5024 Director for customers who want to use the VPN capabilities of the ASF. 5024 is similar to the 5014 platform except that it contains a VPN Accelerator card for enhanced VPN throughput.

All other platforms supported by 3.5.1.10 are also supported by 3.5.2.

7.2 Supported Check Point Releases

ASF 3.5.2 supports the following Check Point builds.

- Check Point Feature Pack 3 with HFA-318

- Check Point NG with Application Intelligence Build 315 (R54)

7.3 Supported Features

7.3.1 *Check Point VPN Support with NG AI (R54)*

ASF 3.5.2 fully supports the VPN capabilities of Check Point NG AI (R54). Both site-to-site and client-to-site VPN is supported. For client-to-site VPN, you can use either SecureClient or SecuRemote clients. The 5024 Director also provides hardware based acceleration for VPN traffic.

Please refer to the VPN Addendum for important information on setting up VPN with ASF 3.5.2.

VPN is not supported with the FP3 version of 3.5.2.

7.3.2 *Check Point SmartView Monitor Support*

SmartView Monitor support was limited in earlier releases of ASF because the Directors did not include the back-end component. Starting with 3.5.2, ASF will fully support Check Point SmartView Monitor. If you are already running an older version of ASF with FP-3 and you upgrade to 3.5.2 FP-3, you will not get SmartView Monitor. In this case, please perform a clean install from the CD.

7.3.3 *Check Point Express License Support for FP-3*

The new Check Point Express license requires a patch for it to work with FP-3. This patch is already installed on 3.5.2 FP-3. However, if you upgrade from an older version of ASF running FP-3 to 3.5.2 FP-3, you will have to install this patch manually. The Check Point Express patch is available from Check Point. Please contact Nortel support for instructions on installing the patch.

7.3.4 Audit Log Support

ASF 3.5.2 has the capability to generate detailed audit logs for all actions performed by users in the CLI or BBI. You can configure a list of RADIUS servers, and ASF will send the audit log to the first available RADIUS server. A local copy of the audit logs is also maintained in the “/var/log/audit.log” file on the Director. The audit log settings can be configured using the “/cfg/sys/adm/audit” submenu in the CLI.

7.3.5 Backup/Restore of Directors

The backup/restore mechanism on ASF 3.5.2 allows the user to backup the state of a Director and restores it later to the same state from the backup file that was created. The restore operation will restore the configuration in the registry as well as the Check Point SIC and policy.

The backup created is for a particular Director, not the entire cluster.

The restore option is available only in the Setup Menu, not in the Config Menu.

If you delete a Director from the cluster, restoring it will not make it part of the cluster again. So be sure to disconnect the Director from the cluster before doing a “/boot/delete”.

7.3.6 Remote SSH Login to Linux Shell

ASF 3.5.2 can be configured to allow remote users to login to the Linux shell instead of the CLI. This is useful for remote troubleshooting. This feature should be used with extreme caution because of the security implications. Remote users can login to Linux shell only over SSH and only using public key/private key authentication. Authentication based on username/password is not supported. The keys have to be in OpenSSH v2 RSA or DSA format. These users are managed from the “/cfg/sys/users/adv” command.

7.3.7 Mix-n-Match Directors in the Cluster

The restriction that the cluster has to be made up of exactly the same model of Directors is removed starting with ASF 3.5.2. Now you can have the following combinations in a cluster.

ASF 5014-x305 and ASF 5010-1650 Directors can be part of the same cluster

ASF 5009-x305 and ASF 5008-1650 Directors can be part of the same cluster

To facilitate this, the sync device configuration command has moved from “/cfg/fw/sync” to “/cfg/fw/sync/host <n>”.

While mixing different directors in the same cluster, the Check Point synchronization may not work if link states for the synch port are not negotiated correctly (CR# Q00973930). If you encounter any problem with synch, check the link status for the synch ports using “ethtool <dev>”, where <dev> is the name of the synch device (e.g. eth2), command at the root prompt and make sure that the link states are same in all cluster members. If they are not same, disable auto-neg for the synch ports and configure the same values for port parameters in all cluster members.

7.3.8 Change In Proxy ARP Implementation

ASF 3.5.2 uses the VRRP MAC address for the configured proxy IP addresses. Earlier, the physical MAC address of the master Accelerator was used. When the master Accelerator failed

over, the MAC address that was associated with the proxy IP would change. The new master would send out GARP messages to the connected devices to update their ARP tables with the new MAC address. However, some devices do not respond to these GARP messages and as a result, they would continue to use the old MAC address until the ARP entry is timed out. This problem is eliminated by the new implementation. When used in non-HA configuration, ASF will use the physical MAC address of the Accelerator for the proxy IP addresses.

7.3.9 Localnet Command Removed

Since SP Route Lookup was introduced in 3.0.3.0d, the recommended setting was to keep localnets disabled. Starting with 3.5.2, the “/cfg/net/adv/local” command has been removed to prevent customers from accidentally enabling localnets.

If you currently have localnets configured, these settings will be lost after you upgrade to 3.5.2 or later.

7.4 Bugs Fixed Since 3.5.1.10 Release

Static routes don't disappear even when interface goes down (Q00768627-01)

Allow RST packets from IDS server to go through when IDS LB is used.

Multicast packets other than VRRP are not being bridged between ports in the same VLAN (Q00767567)

Patch for Linux do_brk() Vulnerability (http://isec.pl/vulnerabilities/isec-0012-do_brk.txt)

Patch for mmap() Local Privilege Escalation Vulnerability (<http://isec.pl/vulnerabilities/isec-0013-mmap.txt>)

“/info/clu” reports CPU Usage as 0% (Q00781453)

Filter Based on Broadcast or Multicast Address Does Not Work (Q00784707)

Proxy ARP for SFD Subnet Not Supported (Q00849035)

Supernetted Routes May Cause 100% MP CPU Usage (Q00746960)

Stateful Session Fail Over Problem (Q00746099)

8 ALTEON SWITCHED FIREWALL (ASF) SYSTEM, VERSION 3.5.2.1 (03/22/2004)

8.1 ASF 3.5.2.1 Replaces ASF 3.5.2

A critical issue was discovered with ASF 3.5.2 after it was released. This caused the Accelerator to panic under certain traffic conditions. The 3.5.2.1 patch release fixes this issue. If you have already installed 3.5.2, please upgrade to 3.5.2.1 as soon as possible.

8.2 Bugs Fixed Since 3.5.2 Release

Q00858866: Accelerator Panic in Fw_proc_data_tunnel() Routine

9 ALTEON SWITCHED FIREWALL (ASF) SYSTEM, VERSION 3.5.3 (06/07/2004)

9.1 Supported Hardware Platforms

ASF 3.5.3 supports the following hardware platforms:

- ASF 5714 (5700 Accelerator + 5014 Director)
- ASF 5710 (5700 Accelerator + 5010 Director)
- ASF 5614 (5600 Accelerator + 5014 Director)
- ASF 5610 (5600 Accelerator + 5010 Director)
- ASF 5409 (5400 Accelerator + 5009 Director)
- ASF 5408 (5400 Accelerator + 5008 Director)
- ASF 5309 (5300 Accelerator + 5009 Director)
- ASF 5308 (5300 Accelerator + 5008 Director)

Note: 6400 Accelerator is not supported by ASF 3.5.3 release. The upcoming ASF 4.0.2 version should be used for installations with 6400 Accelerator.

9.2 Supported Check Point Releases

ASF 3.5.3 supports the following Check Point builds.

- Check Point Feature Pack 3 with HFA-325
- Check Point NG with Application Intelligence (R54) with HFA-410

9.3 Configuration of the Gateway Cluster Object

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

9.4 Supported Features

9.4.1 NAAP VLAN ID Configuration

ASF 3.5.3 allows user to configure NAAP VLAN ID (CR# Q00881922). Any number between 2 and 4094 (except 4092) can be used for NAAP VLAN ID.

This change can be done using CLI in a new ASF installation. If an ASF is upgraded from an older version to ASF 3.5.3, the SFA side change can be done using CLI and the SFD side change has to be done by modifying the config file (/opt/tng/conf/config). The detail procedure to change NAAP VLAN ID is given below.

Changing NAAP VLAN ID in new ASF installation

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

Disconnect all the SFDs in the cluster from the SFAs.

Reimage the SFDs with ASF 3.5.3 iso image, login as admin and change the NAAP VLAN ID using the *naap* menu. This needs to be done in all the SFDs 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

```

Load the binary SFA image in all the Accelerators in the ASF cluster.

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 SFDs with the SFAs and continue with the setup procedure.

Changing NAAP VLAN ID in ASF installation upgraded to 3.5.3

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

Upgrade the firewall cluster to ASF 3.5.3 and make the system operational without changing the NAAP VLAN ID.

Disconnect all the SFDs in the cluster from the SFAs.

Configure NAAP VLAN ID in all SFDs using the following steps.

- Edit the config (/opt/tng/conf/config) file using *vi* editor in Linux and change the line “#NAAP_VLAN_ID=<number>” to “NAAP_VLAN_ID=<number>”, where, “<number>” with the NAAP VLAN ID. If the config file does not have this line, then add a new line “NAAP_VLAN_ID=<number>” at the end of the file.
- Save the config file.
- Reboot the SFD.

All the SFAs should now have 3.5.3 image. Reboot all the SFAs in factory default configuration.

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 SFDs with the SFAs. The ASF cluster should become operational without user intervention.

9.5 Bugs Fixed Since 3.5.2.1 Release

Long TCP sessions are timed out even if not idle (Q00879931)

Active FTP fails with hide NAT (Q00748462)

TCP and UDP Fragments not being NAT'ed correctly with R54 (Q00834278).

“fwaccel templates” command times out (Q00855084).

Remote SSH User Cannot Login After Upgrade (Q00878406).

'cfgd' Freezes When Trying to Change AIM State (Q00726119).

Linux kernel do_mremap() vulnerability, CAN-2004-0077 (Q00866909).

Open-SSL vulnerability, CAN-2004-0079 (Q00880890).

Check Point H323 vulnerability (Q00881896).

Director panics when handling fragmented IGMP packets (Q00864792).

OSPF has to be restarted after changing OSPF configuration (Q00804868).

Hash algorithm for selecting trunk port does not maintain session persistency for accelerated connections (Q00900430).

Connections may be deleted after TCP Start Timeout (Q00939253).

10 ALTEON SWITCHED FIREWALL (ASF) SYSTEM, VERSION 3.5.4 (11/01/2004)

10.1 Supported Hardware Platforms

ASF 3.5.4 supports the following hardware platforms:

- ASF 5714 (5700 Accelerator + 5014 Director)
- ASF 5710 (5700 Accelerator + 5010 Director)
- ASF 5614 (5600 Accelerator + 5014 Director)
- ASF 5610 (5600 Accelerator + 5010 Director)
- ASF 5409 (5400 Accelerator + 5009 Director)
- ASF 5408 (5400 Accelerator + 5008 Director)
- ASF 5309 (5300 Accelerator + 5009 Director)
- ASF 5308 (5300 Accelerator + 5008 Director)

Note: 6400 and 6600 Accelerators are not supported by ASF 3.5.4 release. ASF 4.0.2 version should be used for installations with 6400 and 6600 Accelerators.

10.2 Supported Check Point Releases

ASF 3.5.4 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

10.3 Supported Features

The following new features are available in ASF 3.5.4 release.

10.3.1 *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.

10.3.2 *Automatic Check Point Upgrade*

The upgrade procedure up to ASF 3.5.3 release was a two step process that required separate steps for upgrading Nortel software and Check Point software. This procedure has been simplified in ASF 3.5.4 where the upgrade is done only in one step. The pkg file provided with 3.5.4 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.

10.3.3 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 her/his 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.

10.3.4 Configurable AIM Connection Table Size

Starting with 3.5.4, 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.

10.3.5 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).

10.4 Bugs Fixed Since 3.5.3 Release

- ARP entry corruption that may cause connectivity problem (CR# Q00991305)
- MP CPU uses becomes high if default gateway is learned through dynamic routing (CR# Q00964274)
- High CPU usage when ELA Logging is enabled (CR# Q00966728)
- Check Point ASN-1 Vulnerability (CR# Q00955134-01)
- Upgrade does not update fwkern.conf file (CR# Q00957226)
- The CLI shows Accelerator type 6400 as a supported Accelerator (CR# Q00886219)
- “fwaccel templates” Command Prints IP Addresses in Reverse Order (CR# Q00921793-01)

Accelerator Instability Caused by FIFO (CR# Q00922413)

ASF Trap asfAcceleratorFailover is not generated when a SFA is brought down (Q00937334)

ASF: Using the web GUI, command (diagnostics -> /info/route/dump) times out (Q00922178-01)

"error in application" shows up if login into SFD after idle for hours (Q00959082)

Sync Through VNIC Problem (Q00737761)

11 ALTEON SWITCHED FIREWALL (ASF) SYSTEM, VERSION 3.5.5 (9/15/2005)

11.1 Supported Hardware Platforms

ASF 3.5.5 supports the following hardware platforms:

ASF 5714 (5700 Accelerator + 5014 Director)

ASF 5710 (5700 Accelerator + 5010 Director)

ASF 5614 (5600 Accelerator + 5014 Director)

ASF 5610 (5600 Accelerator + 5010 Director)

ASF 5409 (5400 Accelerator + 5009 Director)

ASF 5408 (5400 Accelerator + 5008 Director)

ASF 5309 (5300 Accelerator + 5009 Director)

ASF 5308 (5300 Accelerator + 5008 Director)

Note: 6400 and 6600 Accelerators are not supported by ASF 3.5.5 release. ASF 4.0.3 or NSF 4.1.1 versions should be used for installations with 6400 and 6600 Accelerators.

11.2 Supported Check Point Releases

ASF 3.5.4 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

11.3 Supported Features

The following new features are available in ASF 3.5.5 release.

11.3.1 Usability Improvement

Release 3.5.5 implements several usability enhancements. WebUI enhancements and new CLI commands are added to use/enable these enhancements. These are:

Configuration Wizard in WebUI

Detailed explanation of log messages

- 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

WEBUI ENHANCEMENTS

The WebUI has a new tab for easy configuration. The “Wizards” tab has a number of wizards which walk the user through various configuration tasks.

DETAILED EXPLANATION OF LOG MESSAGES

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

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. While executing “new”, the CLI will prompt for this configuration. 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/secuid/).

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.

11.3.2 MP Flow Control

Management processor rate limiting feature protects the MP on the accelerator by limiting the number of packets forwarded to it.

11.4 Bugs Fixed Since 3.5.4 Release

- TCPdump or tethereal displays inbound traffic twice (Q01023162)
- MP and SP table corruption in 3.5.x (Q01081888-01)
- ASF Port Stats via CLI (Q01028405)
- VRRP Buffer allocation failure causing 100% MP CPU (Q01147448)
- Kernel Warning Message displayed on 3.5.x (Q01099841)
- MP CPU reaches 100% if default route learned though OSPF (Q01065271)
- MP Flow Control (Q00999034)
- Trunk ports may cause L2 loop after Accelerator reboot (Q01035151-01)
- Need a description field in static routes (Q00983584)
- Incorrect MAC addresses shown in display (Q01048329)
- Firewall Director Join will Fail if '\$' is in the Admin Password (Q00951131-01)
- ASF replies to proxyARP even after NAT/proxyARP configuration is deleted (Q00976886)
- VRRP priority is configurable via WebUI (Q01000256)
- Long TCP Sessions may Timeout if the SFA Uptime is more than 194 days (Q01076608)
- Traffic may be affected while applying configuration (Q01028626)

12 ALTEON SWITCHED FIREWALL (ASF) SYSTEM, VERSION 3.5.6 (11/23/2005)

12.1 Supported Hardware Platforms

ASF 3.5.6 supports the following hardware platforms:

- ASF 5714 (5700 Accelerator + 5014 Director)
- ASF 5710 (5700 Accelerator + 5010 Director)
- ASF 5614 (5600 Accelerator + 5014 Director)
- ASF 5610 (5600 Accelerator + 5010 Director)
- ASF 5409 (5400 Accelerator + 5009 Director)
- ASF 5408 (5400 Accelerator + 5008 Director)
- ASF 5309 (5300 Accelerator + 5009 Director)
- ASF 5308 (5300 Accelerator + 5008 Director)

Note: 6400 and 6600 Accelerators are not supported by ASF 3.5.6 release. ASF 4.0.3 or NSF 4.1.1 versions should be used for installations with 6400 and 6600 Accelerators.

12.2 Supported Check Point Releases

ASF 3.5.4 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-16
- Check Point NGX (R60)

The following Check Point applications are supported. To support these applications on the Nortel Switched Firewall hardware, you must configure NSF 3.5.6 and the Check Point software (SmartDashBoard).

- Firewall-1®
- VPN-1®
- SmartDefense™
- NAT
- Authentication
- Content Security
- Policy Server
- Management Tools
- SmartView Monitor™
- SmartCenter™ Server

The following Check Point management/monitoring tools don't need any configuration within the NSF 3.5.6 software; these tools are configured outside of the 4.1.1 software:

- SmartDashBoard™
- SmartView Tracker™
- SmartView Status™

12.3 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.

12.4 Bugs Fixed Since 3.5.5 Release

- Problem with SFA ARP responses (Q01139113)

- ASF/confusing output of /info/acc (Q01061608)

- Error in MIB File (Q01125484)

13 ALTEON SWITCHED FIREWALL (ASF) SYSTEM, VERSION 3.5.6.2 (07/07/2006)

13.1 Supported Hardware Platforms

ASF 3.5.6.2 supports the following hardware platforms:

- ASF 5714 (5700 Accelerator + 5014 Director)

- ASF 5710 (5700 Accelerator + 5010 Director)

- ASF 5614 (5600 Accelerator + 5014 Director)

- ASF 5610 (5600 Accelerator + 5010 Director)

- ASF 5409 (5400 Accelerator + 5009 Director)

ASF 5408 (5400 Accelerator + 5008 Director)
ASF 5309 (5300 Accelerator + 5009 Director)
ASF 5308 (5300 Accelerator + 5008 Director)

Note: 6400 and 6600 Accelerators are not supported by ASF 3.5.6 release. ASF 4.0.3 or NSF 4.1.1 versions should be used for installations with 6400 and 6600 Accelerators.

13.2 Supported Check Point Releases

ASF 3.5.6.2 supports the following Check Point builds.

Check Point NGX (R61)

The following Check Point applications are supported. To support these applications on the Nortel Switched Firewall hardware, you must configure NSF 3.5.6.2 and the Check Point software (SmartDashBoard).

Firewall-1®
VPN-1®
SmartDefense™
NAT
Authentication
Content Security
Policy Server
Management Tools
SmartView Monitor™
SmartCenter™ Server

The following Check Point management/monitoring tools don't need any configuration within the NSF 3.5.6.2 software; these tools are configured outside of the 4.1.1 software:

SmartDashBoard™
SmartView Tracker™
SmartView Status™

13.3 Bugs Fixed Since 3.5.6 Release

No bug fixes added

14 ALTEON SWITCHED FIREWALL (ASF) SYSTEM, VERSION 3.5.7 (07/20/2006)

14.1 Supported Hardware Platforms

ASF 3.5.7 supports the following hardware platforms:

- ASF 5714 (5700 Accelerator + 5014 Director)
- ASF 5710 (5700 Accelerator + 5010 Director)
- ASF 5614 (5600 Accelerator + 5014 Director)
- ASF 5610 (5600 Accelerator + 5010 Director)
- ASF 5409 (5400 Accelerator + 5009 Director)
- ASF 5408 (5400 Accelerator + 5008 Director)
- ASF 5309 (5300 Accelerator + 5009 Director)
- ASF 5308 (5300 Accelerator + 5008 Director)

Note: 6400 and 6600 Accelerators are not supported by ASF 3.5.7 release. ASF 4.0.x or NSF 4.1.x versions should be used for installations with 6400 and 6600 Accelerators.

14.2 Supported Check Point Releases

ASF 3.5.7 supports the following Check Point builds.

- Check Point NG with Application Intelligence (R55) with HFA-18
- Check Point NGX (R60) with HFA-03
- Check Point NGX (R61)

The following Check Point applications are supported. To support these applications on the Nortel Switched Firewall hardware, you must configure NSF 3.5.7 and the Check Point software (SmartDashboard).

- Firewall-1®
- VPN-1®
- SmartDefense™
- NAT
- Authentication
- Content Security
- Policy Server
- Management Tools
- SmartView Monitor™
- SmartCenter™ Server

The following Check Point management/monitoring tools don't need any configuration within the NSF 3.5.7 software; these tools are configured outside of the 4.1.1 software:

- SmartDashboard™
- SmartView Tracker™
- SmartView Status™

14.3 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.

14.4 Bugs Fixed Since 3.5.6 Release

PARP IP address issue (Q01311541)

DST 2007 daylight saving issue (Q01379352)

Under /info/clu Firewall Synchronization Status shows Error though sync was UP. (Q01187353)

Redistributes a non-existent default route into OSPF (Q01339316)

/info/det does NOT display the correct state of acc (Q01142033)

WEBUI: Not able to upload package using WEBUI (Q01242647-01)

SSI Restarting (Q01266907)

R61:FW Templates did not start even after pushing policy(Q01380368)

fix for 248.5 Days Issue (Q01106902-01)

CLI: /maint/debug/fw/version in R61 has problem (Q01296152-01)

/opt/tng/bin/lb is not giving the expected output (Q01245413)

mond log file is not getting rotated when we run the system more than 10 days (Q01338744)

15 ALTEON SWITCHED FIREWALL (ASF) SYSTEM, VERSION 3.5.7.4 (12/14/2006)

15.1 Supported Hardware Platforms

ASF 3.5.7.4 supports the following hardware platforms:

- ASF 5714 (5700 Accelerator + 5014 Director)
- ASF 5710 (5700 Accelerator + 5010 Director)
- ASF 5614 (5600 Accelerator + 5014 Director)
- ASF 5610 (5600 Accelerator + 5010 Director)
- ASF 5409 (5400 Accelerator + 5009 Director)
- ASF 5408 (5400 Accelerator + 5008 Director)
- ASF 5309 (5300 Accelerator + 5009 Director)
- ASF 5308 (5300 Accelerator + 5008 Director)

Note: 6400 and 6600 Accelerators are not supported by ASF 3.5.7.4 release. ASF 4.0.3 or NSF 4.1.1 versions should be used for installations with 6400 and 6600 Accelerators.

15.2 Supported Check Point Releases

ASF 3.5.7.4 supports the following Check Point builds.

Check Point NGX (R62)

The following Check Point applications are supported. To support these applications on the Nortel Switched Firewall hardware, you must configure NSF 3.5.7.4 and the Check Point software (SmartDashBoard).

- Firewall-1®
- VPN-1®
- SmartDefense™
- NAT
- Authentication
- Content Security
- Policy Server
- Management Tools
- SmartView Monitor™
- SmartCenter™ Server

The following Check Point management/monitoring tools don't need any configuration within the NSF 3.5.7.4 software; these tools are configured outside of the 4.1.1 software:

- SmartDashBoard™
- SmartView Tracker™
- SmartView Status™

15.3 Bugs Fixed Since 3.5.7 Release

No bug fixes added

16 APPENDIX-A: LIST OF KNOWN ISSUES

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

Issues Updated on 08/25/2006

SPECIAL CHARACTERS IN ADMIN PASSWORD

Last Updated: 08/25/2006

Affected Releases: 3.5.x

The admin passwords can't contain special characters, as the current SSI version does not allow join of new members with such characters in the password string.

Issues Updated on 08/03/2006

MOND.LOG FILE IS NOT GETTING ROTATED WHEN WE RUN THE SYSTEM MORE THAN 10 DAYS

CR # Q01338744

Last Updated: 08/03/2006

Affected Releases: 3.5.x

Current Status: Closed

mond.log file was not rotating when system was left running for more than 10 days. The fix rotates log files periodically.

Issues Updated on 07/20/2006

R61: FIREWALL TEMPLATE DID NOT START EVEN AFTER PUSHING POLICY

CR# Q01380368
Last Updated: 07/20/2006
Affected Releases: 3.5.6.2-R61
Current Status: Closed

Firewall template is always disabled even after pushing policy and it is never enabled.

RESET SIC DOES NOT WORK FROM BBI

CR# Q01187253
Last Updated: 07/20/2006
Affected Releases: 3.5.6-R60, 3.5.7
Current Status: Open

Resetting SIC from BBI does not work for 3.5.6 R60 release. If you need to reset the SIC, please use CLI to do this.

Issues Updated on 07/20/2006

PARP IP ADDRESS ISSUE

CR # Q01311541
Last updated : 07/20/2006
Affected Release : 3.5.6
Current Status: Closed

If any IP addresses like x.0.0.x or x.0.x.x or x.x.0.x were set as PARP IP, it was giving error. But these addresses should be valid. Now any valid value can be set after the fixing it.

Issues Updated on 07/20/2006

DST 2007 DAYLIGHT SAVING ISSUE

CR # Q01379352
Last updated : 6/20/2006
Affected Release : 3.5.6
Current Status : Closed

Daylight Saving Time begins for most of the United States at 2:00 a.m. on the first Sunday of April. Time reverts to standard time at 2:00 a.m. on the last Sunday of October. In the U.S., each time zone switches at a different time.

On August 8, 2005, President George W. Bush signed the Energy Policy Act of 2005. This Act changed the time change dates for Daylight Saving Time in the U.S. Beginning in 2007, DST will begin on the second Sunday of March and end the first Sunday of November. Now the build is having this new settings.

Issues Updated on 07/20/2006

"/INFO/CLU" SHOWS "FIREWALL SYNCHRONIZATION STATUS: ERROR" THOUGH SYNC WAS UP

CR#Q01187353
Last updated: 6/20/2006
Affected Release : 3.5.x
Current Status : Closed

When sync device was configured as "eth2", and the management IP address was configured, the health check for sync connectivity failed.

The validation for the sync device checks if valid management IP address is already configured and generates error if present. The error message displays the list of available sync devices.

Issues Updated on 07/20/2006

REDISTRIBUTES A NON-EXISTENT DEFAULT ROUTE INTO OSPF

CR#Q01339316
Last updated : 6/20/2006
Affected Release : 3.5.x
Current Status : Closed

Default route was redistributed and into OSPF though default gateway was not configured on NSF. The cfgd had mapped the redistribute command in CLI to "default-originate always" instead of "default-originate". This has been fixed. Now we redistribute a default route only when the gateway is configured and is reachable.

Issues Updated on 07/20/2006

/INFO/DET DOES NOT DISPLAY THE CORRECT STATE OF ACC

CR#Q01142033
Last updated : 07/20/2006
Affected Release : 3.5.x
Current Status : Closed

The accelerator which lost contact with the cluster was still displayed as part of the /info/det. The fix was to display only the accelerators, which were in contact with the cluster.

Issues Updated on 07/20/2006

SSI RESTARTING

CR#Q01266907
Last updated : 07/20/2006
Affected Release: 3.5.x
Current Status: Closed

The beam process crashed intermittently due to callback timeouts. The fix is to avoid internal restarts when the timeout happens. The SSI restart was the root cause for sudden SNMP agent restarts and CLI console freeze.

Issues Updated on 07/20/2006

WEBUI: NOT ABLE TO UPLOAD PACKAGE USING WEBUI

CR#Q01242647-01
Last Updated : 07/20/2006
Affected Release: 3.5.7
Current Status: Closed

The upload max size in PHP was set to 100 Mb. So web-ui was not allowed the user to upload more than 100 mb files. The upload file size in webui changed from 100 mb to 160 mb. Now we can upload any file in BBI which is less than 160mb in size.

Issues Updated on 07/20/2006

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

CR# Q01106902-01
Last Updated: 07/20/2006
Affected Releases: 3.5.x
Current Status: Fixed in 3.5.7

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

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

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

Issues Updated on 07/20/2006

/OPT/TNG/BIN/LB IS NOT GIVING THE EXPECTED OUTPUT

CR# Q01245413
Last Updated: 07/20/2006

Affected Release: 3.5.x
Current Status: Closed

The lb script is performing the load-balancing between the ISDs. There was a problem in the lb script which was wrongly reading /info/naap/dump output at switch end. Now its reading correctly.

Issues Updated on 07/20/2006

CLI : /MAINT/DEBUG/FW/VERSION IN R61 HAS PROBLEM

CR # Q01296152-01
Last updated : 7/20/2006
Affected Release : 3.5.x
Current Status: Closed

cli command /maint/debug/fw/ver could not execute and display the hfa ver command.

Issues Updated on 11/23/2005

RIPv2 DOESN'T WORK IN R60

CR# Q01258039
Last Updated: 11/23/2005
Affected Releases: 3.5.6-R60, 3.5.7-R61
Current Status: Open

RIP v2 is supported in 3.5.6 FP4 and R55. It is NOT supported in R60. We are currently working with Check Point to resolve this issue.

VPN PROBLEM IN R60

CR# Q01152681
Last Updated: 11/23/2005
Affected Releases: 3.5.6-R60
Current Status: Work around available

Both site-to-site and client-to-site VPN will not work in 3.5.6-R60 with the default management station. 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.
2. Close the management station if it is opened.
3. Open a dos window.
4. 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.
5. Type in "guidbedit" and connect to management station.
6. Hit "ctrl F" (for find) and type "reroute" in the "Find What" box

7. Click on the "Find Next" button
8. It should take you to the "reroute_encrypted_packets" in the "Field Name" column
9. Change the "Value" to false.
10. Hit "F3" and it should find the next instance of "reroute_encrypted_packets"
11. Change its "Value" to false.
12. click on "File" and click on "Save All"
13. Close the guidbedit window and start it again and double check the values of "reroute_encrypted_packets" are set to false.
14. Close the guidbedit window after verifying the values.
15. 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).

PROBLEM WITH SFA ARP RESPONSES

CR# Q01139113
 Last Updated: 11/23/2005
 Affected Releases: 3.5.x
 Current Status: Fixed

There could be problem with SFA ARP response if proxy ARP is configured for ASF VRRP addresses. To avoid this problem, validation is now enforced not to allow user to enter Proxy ARP for VRRP addresses.

CONFUSING OUTPUT OF /INFO/ACC

CR# Q01061608
 Last Updated: 11/23/2005
 Affected Releases: 3.5.x
 Current Status: Fixed in 3.5.6

In the ASF releases before 3.5.6, the output of /info/acc was more confusing and had redundant information. Now, /info/acc has clear and direct output and it is more understandable.

ERROR IN MIB FILE

CR# Q01125484
 Last Updated: 11/23/2005
 Affected Releases: 3.5.x
 Current Status: Fixed

In ASF 3.5.5 and earlier releases, SNMP MIB file had duplicate entry which causes confusion during MIP walk. This issue has been fixed by removing the duplicate entries in alteon_asf.mib file.

Issues Updated on 9/15/2005

“/INFO/CLU” SHOWS “FIREWALL SYNCHRONIZATION STATUS: ERROR”

CR# Q01187353

Last Updated: 9/15/2005

Affected Releases: 3.5.x

Current Status: Open

Sometimes the output of “/info/clu” may show “Firewall Synchronization Status: Error” even when Check Point synchronization is working. This is only a display issue. When you see this error, use “fw ctl pstat” and “cphaprob stat” at the root prompt of all SFDs in the cluster to verify that the synchronization is working. You may also want to check connectivity by pinging the synch interface IP address of the other SFDs in the cluster. If everything is OK, the error message can be ignored without any problem.

CHANGING TIMEZONE ON THE DIRECTOR CAUSES DIRECTOR TO LOSE CONTACT WITH THE ACCELERATOR

CR# Q01190579

Last Updated: 9/15/2005

Affected Releases: 3.5.x

Current Status: Open

Changing time zones multiple times on the director may cause the director lose contact with the accelerators. The work around for the problem is to reboot the complete cluster after changing the time zone.

ADDING VLAN I/F CAUSES IMPACT ON EXISTING VLAN TRAFFIC

CR# Q01199949

Last Updated: 9/15/2005

Affected Releases: 3.5.x

Current Status: Open

Adding VLAN and/or interfaces may cause traffic disruption for up to 20 seconds. The system comes back to normal behavior after 20 secs time period. Variables related to VLANs, interfaces and ports may be initialized during this change and may result in traffic disruption for a short period of time. It is recommended to change any configuration during a maintenance window so that the impact is minimized.

ADDING INTERFACE OR CHANGING IP ADDRESS OF INTERFACE MAY CAUSE SFA FAILOVER

CR# Q01208947

Last Updated: 9/15/2005
Affected Releases: 3.5.x
Current Status: Open

Adding an interface or changing IP address of an existing interface may causes accelerator failover. This has no impact on the system performance.

TCPDUMP OR TETHEREAL DISPLAYS INBOUND TRAFFIC TWICE

CR# Q01023162
Last Updated: 9/15/2005
Affected Releases: 3.5.x
Current Status: Fixed in 3.5.5

TCPdump/tethereal, when run from the root console of an SFD running 3.5 code, displays incoming packets twice. There is no functionality impact because of this. It is just an display anomaly, which has been fixed in 3.5.5.

SP ARP TABLE CORRUPTION AFTER PORT MOVE

CR# Q01081888-01
Last Updated: 9/15/2005
Affected Releases: 3.5.x
Current Status: Fixed in 3.5.5

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.

ASF PORT STATS VIA CLI

CR# Q01028405
Last Updated: 9/15/2005
Affected Releases: None (this is a feature request)
Current Status: Available in 3.5.5

The requested port stats are available under “/maint/debug/ac1/prtstat <port>” and “/maint/debug/ac2/prtstat <port>.”

VRRP BUFFER ALLOCATION FAILURE CAUSING 100% MP CPU

CR# Q01147448
Last Updated: 9/15/2005

Affected Releases: 3.5.x
 Current Status: Fixed in 3.5.5

Under certain incoming VRRP traffic rate, the VRRP buffer may get full and cause MP CPU usage to reach 100%. This is a timing issue that happens when the number of incoming packets is more than the rate at which MP buffers are freed. It is dependent on a particular traffic rate (not on high traffic). The issue has been fixed in ASF 3.5.5.

KERNEL WARNING MESSAGE DISPLAYED ON 3.5.X

CR# Q01099841
 Last Updated: 9/15/2005
 Affected Releases: 3.5.x
 Current Status: Fixed in 3.5.5

Under specific traffic condition, ASF releases up to 3.5.4 could display the following message
 [aim_app::pkt_time_tunl_in_accel](Couldn't find connection! ...
 This message did not cause any traffic disruption. The condition that was creating this error message without any real problem has been fixed in 3.5.5. Please keep in mind that this message could appear under genuine error conditions.

MP CPU REACHES 100% IF DEFAULT ROUTE LEARNED THROUGH OSPF

CR# Q01065271
 Last Updated: 9/15/2005
 Affected Releases: 3.5.x
 Current Status: Fixed in 3.5.5

If default route is learned through OSPF, the MP CPU in the accelerator will reach 100% under moderate traffic condition. The work around is not to learn the default route through OSPF. The issue has been fixed in 3.5.5 release.

MP FLOW CONTROL

CR# Q00999034
 Last Updated: 9/15/2005
 Affected Releases: None (this is a feature request)
 Current Status: Available in 3.5.5

Management processor rate limiting protects the MP on the accelerator by limiting the number of packets forwarded to it. This can be configured using “/cfg/acc/mprlimit” menu in the CLI or “Config | Cluster | Accelerator(s) | General” page in the WebUI.

TRUNK PORTS MAY CAUSE L2 LOOP AFTER ACCELERATOR REBOOT

CR# Q01035151-01

Last Updated: 9/15/2005
 Affected Releases: 3.5.x
 Current Status: Fixed in 3.5.5

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 3.5.5 release.

NEED A DESCRIPTION FIELD IN STACTIC ROUTES

CR# Q00983584
 Last Updated: 9/15/2005
 Affected Releases: 3.5.x
 Current Status: Fixed in 3.5.5

A comment field has been added to the CLI menu for static route. Users can add a description for the static route in this field.

```
>> Main# /cfg/ner/route/static 1
-----
[Static Route 1 Menu]
addr - Set destination host or network address
mask - Set destination subnet mask
gw - Set gateway IP address
comment - Set description for the static route
ena - Enable this static route
dis - Disable this static route
```

INCORRECT MAC ADDRESSES SHOWN IN DISPLAY

CR# Q01048329

Last Updated: 9/15/2005

Affected Releases: 3.5.x

Current Status: Fixed in 3.5.4

Because of this issue, the SFD assigns wrong MAC address to the switches in a HA environment. The MAC address of Accelerator-1 is assigned to Accelerator-2 and vice-versa. In this case, the system will not work after an accelerator. The issue has been fixed in ASF 3.5.4 release in 2004.

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

CR# Q00951131-01

Last Updated: 09/15/2005

Affected Releases: 3.5.x

Current Status: Fixed in 3.5.5

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

ASF REPLIES TO PROXYARP EVEN AFTER NAT/PROXYARP CONFIGURATION IS DELETED

CR# Q00976886

Last Updated: 9/15/2005

Affected Releases: 3.5.x

Current Status: Fixed in 3.5.5

If NAT/proxyARP configuration is deleted, ASF should not respond to the ARP request for the deleted address even after failover. The earlier implementation had some issue where the new active accelerator after fail-over was responding to P ARP for the deleted interface. This issue has been fixed in 3.5.5 release.

VRRP PRIORITY IS CONFIGURABLE VIA WEBUI

CR# Q01000256

Last Updated: 9/15/2005

Affected Releases: 3.5.x

Current Status: Fixed in 3.5.5

The CLI command for /cfg/net/if <x>/vrrp/prio was removed earlier. This was removed from WebUI in 3.5.5 release.

LONG TCP SESSIONS MAY TIMEOUT IF THE SFA UPTIME IS MORE THAN 194 DAYS

CR# Q01076608

Last Updated: 9/15/2005
 Affected Releases: 3.5.x
 Current Status: Fixed in 3.5.5

The variable used to keep SP time in SFA wraps around in 194 days. Because of some inconsistency in time processing, the TCP sessions may timeout if the SFA is up for more than 194 days. The problem has been fixed in 3.5.5 release. For earlier release, the work around is to reset all SFAs in the cluster (one at a time). This issue will not cause any other problem.

TRAFFIC MAY BE AFFECTED WHILE APPLYING CONFIGURATION

CR# Q01028626
 Last Updated: 9/15/2005
 Affected Releases: 3.5.x
 Current Status: Fixed in 3.5.5

While adding/deleting interfaces or VLANs in ASF, the active SFA may not send VRRP advertisements for several seconds. This may cause the backup SFA to become master temporarily and update the ARP entry in the connected devices by sending GARP. The end result is an incorrect ARP entry in the connected device and loss of connectivity. The connectivity is automatically restored when the ARP entry in the connected device expires.

This problem has been fixed in ASF 3.5.5 release. For earlier releases, one of the following approaches can be used to avoid the problem or immediately restore connectivity through ASF.

1. When problem happens, force the current master SFA to become the backup accelerator. The CLI command, “/maint/debug/<SFA>/back”, where <SFA> is either “ac1” or “ac2,” can be used. Please check the VRRP status (use “/maint/debug/<SFA>/vrrp”) of the SFA before making it backup.
2. Increase the VRRP advertisement interval from 1 to 5 seconds prior to modifying network configuration. The CLI command, “/cfg/net/adv/vrrp/adver” can be used to change the interval. Change this interval back to 1 second after applying the configuration.
3. When the problem happens after applying configuration change, delete appropriate ARP entries in the connected devices. At this time the device will ARP ASF and establish a correct ARP entry.

Issues Updated on 2/18/2005

MULTICAST TRAFFIC CAUSES LOOPING IN TRUNK GROUP

CR# Q00862911-01
 Last Updated: 2/18/2005
 Affected Releases: 3.5.1.10d, 3.5.2, 3.5.2.1 releases for 6000 series ASF
 Current Status: Fixed in 4.0.1

If trunk group is configured and the trunk is connected to an external L2 switch, the multicast packet from the L2 switch is being sent back (as if it is a unicast packet from another VLAN) on one of the trunk ports causing a L2 flood loop.

Issues Updated on 01/17/2005

SYNC THROUGH VNIC PROBLEM

CR# Q00737761

Last Updated: 01/17/2005

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2.1, 3.5.3

Current Status: Fixed in 3.5.4

Sync through VNIC is not supported in the above mentioned ASF releases. If you are using any of the affected releases, please upgrade to ASF 3.5.4. If an upgrade is not possible, please use a dedicated SFD port for Check Point state synchronization as an alternate solution. Please note that for better performance it is recommended (even for ASF 3.5.4 release) to use a dedicated SFD port for Check Point state synchronization.

Issues Updated on 12/14/2004

TCP SESSIONS ARE NOT ACCELERATED WHEN SYN DEFENDER IS ENABLED

CR# Q00914964

Last Updated: 12/14/2004

Affected Releases: 3.5.2, 3.5.2.1, 3.5.3

Current Status: Fixed in 3.5.4

When SYN defender is enabled, all the TCP connections are offloaded with F2F (Forward-to-Firewall) flag and, therefore, none of the TCP connections are accelerated. The problem has been fixed in 3.5.4 release.

Note: This fix does not address the high CPU usage problem because of other Smart Defense features. Please refer to Q00914964 and Q00921499-01 for high CPU related problem.

TCP SESSIONS ARE NOT ACCELERATED WHEN ISN SPOOFING IS ENABLED

CR# Q00921499

Last Updated: 12/14/2004

Affected Releases: 3.5.2, 3.5.2.1, 3.5.3

Current Status: Fixed in 3.5.4

When ISN spoofing is enabled, all the TCP connections are offloaded with F2F (Forward-to-Firewall) flag and, therefore, none of the TCP connections are accelerated. The problem has been fixed in 3.5.4 release.

Note: This fix does not address the high CPU usage problem because of other Smart Defense features. Please refer to Q00914964 and Q00921499-01 for high CPU related problem.

Issues Updated on 11/02/2004

FRAGMENTS DO NOT PASS THROUGH ASF WITH 5300 ACCELERATORS

CR# Q01001073

Last Updated: 11/02/2004

Affected Releases: 3.5.x

Current Status: Fixed in 3.5.4

All fragments are dropped by the SFD in an ASF with 5300 accelerators. The problem happens with fragments for all protocols. The issue has been fixed in ASF 3.5.4 release.

Issues Updated on 10/25/2004

ARP ENTRY CORRUPTION THAT MAY CAUSE CONNECTIVITY PROBLEM

CR# Q00991305

Last Updated: 10/25/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10, 3.5.2, 3.5.2.1 and 3.5.3

Current Status: Fixed in 3.5.4

Because of a possible race condition, the ARP entry in the accelerator may get corrupted after rebooting the accelerator. This results in an incorrect ARP entry where for a switch interface address with the MAC address pointing to the MIP ISD and NAAP VLAN (default value is 4094). Because of this, all the packets destined to the external IP address will be forwarded to the SFD and the connectivity with the external network will be lost. The ASF will continue to forward traffic to all other networks without any problem. In this case you will see a packet drop error message in /var/tmp/tngsys.log file that says “app_in_invalid - IP Packet should never come!!!” You should also see the external IP address in the packet drop message. If this problem happens, check the ARP table entry and delete the corrupted ARP entry by typing “/maint/arp/del <IP Addr>” in the SFA console. The problem should go away until the next reboot of the accelerator. The problem may reappear after the reboot. This issue has been fixed in 3.5.4 release.

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

CR# Q00964274

Last Updated: 10/25/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10, 3.5.2, 3.5.2.1 and 3.5.3

Current Status: Fixed in 3.5.4

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

Last Updated: 10/25/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10, 3.5.2, 3.5.2.1 and 3.5.3

Current Status: Fixed in 3.5.4

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# Q00955134-01

Last Updated: 10/25/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10, 3.5.2, 3.5.2.1 and 3.5.3

Current Status: Fixed in 3.5.4

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>

UPGRADE DOES NOT UPDATE FWKERN.CONF FILE

CR# Q00957226

Last Updated: 10/25/2004

Affected Releases: 3.5.3-FP4

Current Status: Fixed in 3.5.4

The fix for the long TCP sessions timeout problem (Q00879931) requires two configuration parameters (“cphwd_increase_expiration_tolerance=1” and “fw_force_refresh_on_expiration=1”) to be defined in \$FWDIR/modules/fwkernel.conf file.

In some upgrade process, these parameters may not be defined after the upgrade to ASF 3.5.3-FP4. Therefore, the long TCP sessions may fail after these upgrade. In this case, the work around is to manually define these two parameters in the fwkernel.conf file in each SFD. The following procedure may be used to update the fwkernel.conf file after the upgrade.

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

Upgrading to 3.5.4 will update these parameters correctly. However, if you are upgrading to 3.5.3, the above procedure should be used.

/ISD PARTITION MAY GET FULL AFTER MULTIPLE UPGRADES FROM 3.0.X TO 3.5.3

CR# Q00914617

Last Updated: 10/25/2004

Affected Releases: 3.5.3

Current Status: No fix planned

To accommodate larger images, the size of the /isd partition, where ASF images are stored, has been increased in 3.5.x releases. When an ASF with 3.0.x image is upgraded to 3.5.x version, the partition size does not change during the upgrade process. Therefore, the SFD has to store the bigger 3.5.x image in a smaller partition. If the SFD is again upgraded to 3.5.3 version, we have to keep two larger images (SFD keeps only last two images) in the smaller partition. Therefore, the disk usage may go up to 100% and some upgrade may even fail.

If an ASF installation requires multiple upgrades to 3.5.3 or 3.5.4, it is recommended to do a clean install. 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 can be done by a script provided for this purpose. The script can be run before an upgrade and also after a successful upgrade. Detailed procedure for the upgrade is presented in Section 3.

The size of the /isd partition has been increased in ASF 3.5.4. This change will fix the problem during future upgrades. However, this is not going to fix the problem while upgrading from builds prior to 3.5.4. In these cases, it is recommended to use the procedure outlined in Section 3.

THE CLI SHOWS ACCELERATOR TYPE 6400 AS A SUPPORTED ACCELERATOR

CR# Q00886219

Last Updated: 10/25/2004

Affected Releases: 3.5.3

Current Status: Fixed in 3.5.4

While running *new*, SFD CLI may show the Accelerator type 6400 as one of the supported Accelerators. ASF 3.5.3 does not support this Accelerator type. This additional Accelerator type does not cause any problem and can be safely ignored.

“FWACCEL TEMPLATES” COMMAND PRINTS IP ADDRESSES IN REVERSE ORDER

CR# Q00921793-01

Last Updated: 10/25/2004

Affected Releases: 3.5.3

Current Status: Fixed in 3.5.4

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 in reverse order. For example, “210.40.3.1” will be printed as “1.3.40.210”. This is just a display issue and does not have any other effect on ASF operation.

ACCELERATOR INSTABILITY CAUSED BY FIFO

CR# Q00922413

Last Updated: 10/25/2004

Affected Releases: 3.5.3

Current Status: Fixed in 3.5.4

In lab environment under certain traffic profile, accelerator instability caused by FIFO under run has been observed. If you encounter similar situation in your deployment please use fiber ports (if available) and upgrade to ASF 3.5.4.

SFD MAY REBOOT AUTOMATICALLY AFTER RESTORING CONFIGURATION

CR# Q00969461

Last Updated: 10/25/2004

Affected Releases: 3.5.2, 3.5.2.1, 3.5.3 and 3.5.4

Current Status: Work around available

While doing backup restore in an ASF cluster with Check Point synchronization, the SFD may keep rebooting after restore. 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.

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

CR# Q00694532

Last Updated: 07/27/2006

Affected Releases: 3.5.2, 3.5.2.1, 3.5.3 and 3.5.4

Current Status: Fixed

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 is used by Check Point synchronization mechanism. This causes loss of communication between the SFD and the SFA, and results in acceleration off.

The issue is fixed now. The flag `fw_block_new_sync_conns=0` in `fwkern.conf` file would automatically take care of this issue.

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

CR# Q00983354

Last Updated: 10/25/2004

Affected Releases: 3.5.2, 3.5.2.1, 3.5.3 and 3.5.4

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: 3.5.2, 3.5.2.1, 3.5.3 and 3.5.4

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. A character

COULD CONFIGURE SFD HOST NAME WITH SPECIAL CHARACTER (")

CR# Q00972348

Last Updated: 10/25/2004

Affected Releases: 3.5.4

Current Status: Open

In the current release, it is possible for the users to configure the host name with special character (") for SFD on 5308 platform via `/cfg/sys/cluster/host 1/name name#` and `'apply'` commands. It is recommended not to use this special character in the host name.

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: 3.5.2, 3.5.2.1, 3.5.3 and 3.5.4

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: 3.5.2, 3.5.2.1, 3.5.3 and 3.5.4

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 08/31/2004

IF AUTO-NEG IS ENABLED, SYNCH MAY NOT WORK WITH DIFFERENT SFD HARDWARE IN ASF CLUSTER

CR# Q00973930

Last Updated: 08/31/2004

Affected Releases: 3.5.2, 3.5.2.1, and 3.5.3

Current Status: No fix planned

Sometimes, the Check Point synchronization may not work if link states for the synch port are not negotiated correctly. This error condition is more probable when different director hardware is used in the same ASF cluster. If you encounter any problem with synch, check the link status for the synch ports using “ethtool <dev>”, where <dev> is the name of the synch device (e.g. eth2), command at the root prompt and make sure that the link states are same in all cluster members. If they are not same, disable auto-neg for the synch ports and configure the same values for port parameters in all cluster members.

Issues Updated on 08/10/2004

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

CR# Q00919674-01

Last Updated: 08/10/2004

Affected Releases: 3.5.x

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.

LONG TCP SESSIONS ARE TIMED OUT EVEN IF NOT IDLE

CR# Q00879931

Last Updated: 08/10/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2, 3.5.2.1

Current Status: Fixed in 3.5.3-FP4

Long TCP sessions like Telnet and SSH may get deleted from the firewall even when the session was not really idle. This normally happens when traffic in the session is very low.

The workaround is to increase the session timeout of the affected service to 24 hours. This can be done from Smart Dashboard by editing the advanced properties of that service. The fix for this problem is available in ASF 3.5.3-FP4 (R54) release. For FP3 installations, it is recommended to upgrade to FP4 code. If upgrade is not possible, the work around suggested above can be used to avoid the timeout.

FIREWALL DIRECTORS KEEP LOSING CONTACT WITH EACH OTHER

CR# Q00901409

Last Updated: 08/10/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2.1

Current Status: Fixed in 3.5.3

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`.

Issues Updated on 07/01/2004

CONNECTIONS MAY BE DELETED AFTER TCP START TIMEOUT

CR# Q00939253

Last Updated: 07/01/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2, 3.5.2.1

Current Status: Fixed in 3.5.3

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.

BACKUP ACCELERATOR LED BLINKS LIKE ACTIVE ACCELERATOR

Last Updated: 07/01/2004

Affected Releases: 3.5.3

Current Status: Closed

In earlier versions of SFA failover algorithm, the backup switch was receiving VRRP packets in the non-NAAP ports only after failure of the inter-accelerator link. Sometimes this may cause problem with VRRP failover. Therefore, the VRRP failover mechanism has been changed so that the backup switch will receive the VRRP packets at all times and will start processing them only after the failure of the inter-accelerator link. The result is a quicker and stable VRRP failover. With this new algorithm, the behavior of the LEDs in the backup switch is exactly same as that in the active switch. So, one need to check the switch CLI (/info/vrrp) or the SFD CLI (/info/det) to find out the active and backup SFA.

SNMPAGENTD MAY TAKE 99% OF THE CPU

CR# Q00895609-01

Last Updated: 07/01/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2, 3.5.2.1

Current Status: Fixed in 3.5.3

When SSI dies in the system, the SNMP agent will take up to 99% of the CPU utilization. The fix has been added to 3.5.3 release. For earlier releases, the work around is to reboot or restart the SNMP agent when problem occurs.

FW DAEMON MAY TAKE MORE THAN 95% CPU AFTER REBOOT

CR# Q00939269

Last Updated: 07/01/2004

Affected Releases: 3.5.3, 3.5.4-FP4

Current Status: Open

After reboot, fw daemon may take more than 95% CPU. The problem happens intermittently. Once the problem happens in an SFD, further reboot will not help. The work around is to run "cpstop" and "cpstart". We are currently working with Check Point to get a fix for this.

Issues Updated on 06/07/2004**ACTIVE FTP FAILS WITH HIDE NAT**

CR# Q00748462

Last Updated: 06/07/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2, 3.5.2.1

Current Status: Fixed

If you have multiple Firewall Directors in the cluster, active FTP may not work correctly if the FTP client is behind hide NAT. We are currently working with Check Point to resolve this issue. Passive FTP works correctly even with hide NAT.

TCP AND UDP FRAGMENTS NOT BEING NAT'ED CORRECTLY WITH R54

CR# Q00834278

Last Updated: 06/07/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2, 3.5.2.1

Current Status: Fixed

On ASF 3.5.2 R54, TCP and UDP fragments are not being NAT'ed correctly. A TCP or UDP packet for a NAT'ed session will pass through the firewall without being NAT'ed at all. If you have configured NAT and expect to see fragments, please use FP-3 instead of R54.

“FWACCEL TEMPLATES” COMMAND TIMES OUT

CR# Q00855084

Last Updated: 06/07/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2, 3.5.2.1

Current Status: Fixed

The Check Point command “fwaccel templates” used to view the offloaded template sessions may timeout without displaying any sessions. Please use the alternate command “cat /proc/aim/templates” to view the template sessions. Both these commands are available only to the ‘root’ user.

REMOTE SSH USER CANNOT LOGIN AFTER UPGRADE

CR# Q00878406

Last Updated: 06/07/2004

Affected Releases: 3.5.2.1

Current Status: Fixed

If you have configured remote SSH users, after upgrade, these users will no longer be able to login to the ASF. You will also see the following error message in the syslog:

```
ERROR: Error applying SSH User settings [Failed to add user ...]
```

To recover, please do the following.

1. Login to the CLI and delete all remote SSH users. Apply the change.
2. Login as root on each Director and run “rm -rf /config/users/*”
3. Login to the CLI and create the SSH users again.

'CFGD' FREEZES WHEN TRYING TO CHANGE AIM STATE

CR# Q00726119

Last Updated: 06/07/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2, 3.5.2.1

Current Status: Fixed

Under some circumstances, the 'cfgd' process may freeze when it tries to change the AIM state. When this happens, you will notice that any changes made from the CLI are not taking effect. To confirm that you are hitting this issue, login to the Director as 'root' and run 'tail /var/tmp/cfgd.log'. If the last line says 'Setting AIM state to AIM_FW_RUN' or 'Setting AIM state to AIM_FW_STOP', then please reboot the Director to recover.

LINUX KERNEL DO_MREMAP() VULNERABILITY

CR# Q00866909

Last Updated: 06/07/2004

Affected Releases: 3.5.2, 3.5.2.1

Current Status: Fixed

There were 2 mremap vulnerabilities published:

<http://isec.pl/vulnerabilities/isec-0013-mremap.txt>

<http://isec.pl/vulnerabilities/isec-0014-mremap-unmap.txt>

The first vulnerability is fixed in 3.5.2. The second vulnerability will be fixed in ASF-4.0.2 release. Tentative schedule for this release is Q3 2004. The severity of this vulnerability is "Medium".

The mremap system call (do_mremap) in Linux kernel 2.4 and 2.6 does not properly perform bounds checks, which could allow local users to cause a denial of service and possibly gain privileges by causing a remapping of a virtual memory area (VMA) to create a zero length VMA.

This vulnerability is not remotely exploitable (the potential attacker needs to be logged into the box) so the exploit could only be used by someone with a valid account or someone who was able to gain connection through another vulnerability. However at least two different attack vectors for the 2.4 kernel series have been identified and exploit code is available.

Impact on ASF

Alteon Switched Firewall (ASF) 3.0.x and below use 2.2 kernel. So, these releases are not impacted.

Other ASF releases before 3.5.2 don't allow any user to remotely access the Linux shell. Furthermore, the users configured in these releases have either the root access or the CLI access. The user having CLI access cannot execute anything out side the CLI and therefore cannot exploit this vulnerability. Therefore, these releases are also not affected.

The only release that is affected by this vulnerability is ASF-3.5.2.

Alteon Firewall 51xx uses the 2.4 kernel but doesn't allow remote login as root, so it is not vulnerable.

OPEN-SSL VULNERABILITY (CAN-2004-0079)

CR# Q00880890

Last Updated: 06/07/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2.1

Current Status: Fixed

All versions of OpenSSL from 0.9.6c to 0.9.6l inclusive and from 0.9.7a to 0.9.7c inclusive have vulnerability issue with null-pointer assignment during SSL handshake. Earlier ASF releases were using OpenSSL 0.9.6k and, therefore, are affected by this vulnerability. See http://www.openssl.org/news/secadv_20040317.txt for details. The patch for this vulnerability is included in ASF 3.5.3 release.

CHECK POINT H323 VULNERABILITY

CR# Q00881896

Last Updated: 06/07/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2.1

Current Status: Fixed

A recent NISCC advisory (<http://www.uniras.gov.uk/vuls/2004/006489/h323.htm>) reveals vulnerabilities in H.323 equipment including GateKeepers, endpoints (phones, softphones, video cameras, etc.), and firewalls that enforce H.323 security. Please see <http://www.checkpoint.com/techsupport/alerts/h323.html> for more details. The Check Point patch for this vulnerability has been included in ASF 3.5.3 release.

DIRECTOR PANICS WHEN HANDLING FRAGMENTED IGMP PACKETS

CR# Q00864792

Last Updated: 06/07/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2.1

Current Status: Fixed

Incorrect processing of fragmented IGMP packets was causing panic in the Director. The issue has been fixed in ASF 3.5.3 by properly handling the fragmented packets.

OSPF HAS TO BE RESTARTED AFTER CHANGING OSPF CONFIGURATION

CR# Q00804868

Last Updated: 06/07/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2.1

Current Status: Fixed

Changing area index on an interface does not correctly update routes. The work around is to restart ospfd for correct route update. Similarly, changing router id also requires reboot of ospfd. Whenever there is a change in the area index or router id, ASF 3.5.3 warns the user that ospfd has to be restarted for the changes to take effect. Then, the user needs to restart the ospfd.

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

CR# Q00900430

Last Updated: 06/07/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2, 3.5.2.1

Current Status: Fixed

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 3.5.3 release so that the session persistency is maintained for accelerated sessions.

ACTIVATING SYN ATTACK PROTECTION CAUSES HIGH CPU USAGE

CR# Q00914964

Last Updated: 06/07/2004

Affected Releases: 3.5.x

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: 06/07/2004

Affected Releases: 3.5.x

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.

SFD MAY LOOSE CONTACT WITH SWITCH AFTER UPGRADE

CR# Q00915973

Last Updated: 06/07/2004

Affected Releases: 3.5.3

Current Status: Open

After upgrading the SFD, sometimes the SFD may not be able to talk to the SFA. The cfgd log might show the error saying the SFD can't unjam itself. The work around for this issue is to reboot SFD after upgrade. It is recommended to reboot the SFD after all upgrade irrespective of whether the problem happens or not.

ASF 3.5.3 DOES NOT SUPPORT DIFFERENT AD3 HARDWARE IN THE SAME CLUSTER

CR# Q00916164

Last Updated: 06/07/2004

Affected Releases: 3.5.3

Current Status: Open

The AD4 tigon Accelerator can be converted to 5300 and used as AD3 hardware. ASF 3.5.3 does not support 5300 converted from AD4 and AD3 Accelerators in the same ASF cluster. It is recommended to use same AD3 hardware in an ASF cluster.

FP4 (R54) SMART DASHBOARD WILL CRASH IF SFD INTERNAL NETWORK IS A SUBNET OF DATA NETWORK

CR# Q00914969-01

Last Updated: 06/07/2004

Affected Releases: 3.5.3, 3.5.4

Current Status: Open

ASF supports SFD network to be a subnet of another network. In this case, the user needs to enable proxy ARP for the SFD subnet. However, if one gets this topology in the SmartDashboard and saves the information, the SmartDashboard may crash. The work around is to delete the *eth0* interface after getting the topology and before saving the information in the SmartDashboard.

Issues Updated on 05/18/2004**5014-X305 FIREWALL DIRECTOR DOES NOT RECOGNIZE DUAL FIBER CARD**

CR# Q00909049

Last Updated: 05/18/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d

Current Status: Fixed in 3.5.2

Intel recently updated the chipset in the dual port fiber card used in ASF 5014-x305 and ASF 5024-x305. This required an updated version of the driver also. The new driver has been included in ASF 3.5.2 and above. The Directors that are shipped with version 3.5.2 pre-installed may contain this new Intel card. If you reimage the box with an older version of ASF, the Director will fail to recognize the Intel card.

Before reimaging an ASF 3.5.2 Director with an older version, please check the following to see if the Intel card is compatible with older versions of ASF. Login to the Director as “root” and run “lspci | grep Intel”. If the output contains the string “Unknown device 107a”, it means the card will not work with older versions of ASF (3.5.1.10d and below)

Issues Updated on 04/20/2004

FIREWALL DIRECTOR PANICS WHILE REBOOTING

CR# Q00733964

Last Updated: 04/20/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d

Current Status: Fixed in 3.5.2

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

Issues Updated on 03/22/2004

ACCELERATOR PANIC IN FW_PROC_DATA_TUNNEL() ROUTINE

CR# Q00858866

Last Updated: 03/22/2004

Affected Releases: 3.5.2

Current Status: Fixed in 3.5.2.1

Under certain traffic conditions, the Accelerator may panic. If it is a high availability setup, there will not be traffic disruption but you may have to power cycle the Accelerator to bring it back up. This issue was discovered after 3.5.2 was released. Please upgrade to 3.5.2.1 to fix this issue.

Issues Updated on 03/04/2004

HTTP SECURITY SERVER VULNERABILITY

Last Updated: 03/04/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2

Current Status: Open. Please apply patch separately.

On Feb 04, 2004, Check Point announced a vulnerability in the HTTP Security Server and released a patch to fix it. For more details, please visit the following URL:
http://www.checkpoint.com/techsupport/alerts/security_server.html

This patch is not included in the ASF 3.5.2 release. If you are using HTTP Security Server, it is recommended that you install this patch. Detailed instructions for installing the patch on ASF can be found on the Nortel Support website.

If you are currently running a patched version of ASF and are upgrading to 3.5.2, you do not have to reapply the patch unless the Check Point version is also upgraded.

MULTIPLE FAILURE SCENARIOS

Last Updated: 03/04/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d

Current Status: Fixed in 3.5.2

Although simultaneous failure of multiple components may not be common in a live environment, such failures may be simulated in the lab by pulling out cables, turning off power etc. In these situations, please be aware of the following issues. If you are running RIP and you disconnect all Firewall Directors from the Accelerators and reconnect them after a couple of minutes, you may notice that one Director did not get all the RIP routes back into its routing table (Q00643774). If this happens please reboot that Director. If you disconnect all Firewall Directors except the MIP owner and then reconnect them back after about a minute, more than one Director may own the MIP simultaneously (Q00636612). To prevent this, wait at least one and a half minutes before plugging the Directors back. To recover, please reboot the duplicate MIP owner.

PORT MIRRORING NO LONGER SUPPORTED WITH 5X00 ACCELERATORS

Last Updated: 03/04/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2

Current Status: No fix planned

Port mirroring is no longer supported with 5x00 Accelerators. It is supported only on 6x00 Accelerators. If you enable port mirroring with 5x00 Accelerator, the Director will not be able to update the Accelerator configuration.

VALIDATION ERROR AFTER UPGRADE

CR# Q00849018

Last Updated: 03/04/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2

Current Status: Open

After upgrading to 3.5.2, you may get the following error message when you try to update some configuration in the CLI and apply it.

"Not all inter-Accelerator ports (0 and 0) are defined"

To correct this, please set the correct values of the inter-Accelerator port being used using '/cfg/acc/ac1/iap' and '/cfg/acc/ac2/iap' and apply again.

PROXY ARP FOR SFD SUBNET NOT SUPPORTED

CR# Q00849035

Last Updated: 03/04/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d

Current Status: Fixed in 3.5.2

Proxy ARP for SFD subnet (/cfg/net/adv/parp/sfd) is not working properly. Enabling this would cause the Directors to lose contact with each other and behave erratically. This will be fixed in an upcoming release.

PROXY IPS NOT ACCESSIBLE AFTER DISABLING HIGH AVAILABILITY

CR# Q00822122

Last Updated: 03/04/2004

Affected Releases: 3.5.2

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

CR# Q00829630

Last Updated: 03/04/2004

Affected Releases: 3.5.2

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.

'/INFO/CLU' REPORTS CPU USAGE AS 0%

CR# Q00781453

Last Updated: 03/04/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d

Current Status: Fixed in 3.5.2

On the 5009 and 5014 Directors, the '/info/clu' command incorrectly reports the CPU usage as 0%. To find the real CPU usage, login as 'root' and run 'top'. You will see a line similar to the following in the output:

CPU states: 0.1% user, 1.5% system, 0.0% nice, 98.2% idle

To exit out of 'top', press 'q' or Ctrl+C.

STATIC ROUTES DON'T DISAPPEAR EVEN WHEN INTERFACE GOES DOWN

CR# Q00768627-01

Last Updated: 03/04/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d

Current Status: Fixed in 3.5.2

With dynamic routes, when an interface goes down, all dynamic routes whose next hop is in that subnet are deleted. This causes the next best route to be used. With static routes, the route is deleted from the Director but not the Accelerator. This causes the ASF to try to forward traffic to a next hop router, even when the corresponding interface is down and the next hop router cannot be reached.

FILTER BASED ON BROADCAST OR MULTICAST ADDRESS DOES NOT WORK

CR# Q00784707

Last Updated: 03/04/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d

Current Status: Fixed in 3.5.2

If you try to filter based on broadcast or multicast address, it will not work. All such traffic will still be forwarded to the Director as if the filter did not exist. There is no workaround for this issue. It will be fixed in the 3.5.2 release.

SUPERNETTED ROUTES MAY CAUSE 100% MP CPU USAGE

CR# Q00746960

Last Updated: 03/04/2004

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d

Current Status: Fixed in 3.5.2

If you define a supernetted route (e.g., route to a class B network address but with a class-A subnet such as 172.0.0.0/8), all packets in that subnet will be forwarded to the MP for routing causing the MP CPU usage to increase. When this happens, both the Accelerators may become masters, the Directors may lose contact with one or both Accelerators, and you will see traffic disruption. The workaround is to split the supernetted route into multiple regular routes.

STATEFUL SESSION FAIL OVER PROBLEM

CR# Q00746099

Last Updated: 03/04/2004
 Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d
 Current Status: Fixed in 3.5.2

When a Director fails, all of its sessions are automatically failed over to another Director in the cluster when Check Point sync is enabled. Sessions that are failed over in this manner are no longer accelerated. From end user's point of view, you may see an increased latency after a Director fail over. New sessions that are established after the fail over are fully accelerated.

JOIN FAILS IF ASF CLUSTER ALREADY CONTAINS 2 OR MORE DIRECTORS

CR# Q00851121
 Last Updated: 03/04/2004
 Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d
 Current Status: Fixed in 3.5.2

If there are two or more Directors in the cluster and you try to join a third Director, the join will fail. This will happen with auto-join as well as manual join. If you retry the join again with the same IP address, it will work. When you login again to retry the join, if you see the configuration menu instead of the setup menu, please run “/boot/delete” command, wait a couple of minutes and login as ‘admin’ again.

WHEN FIREWALL IS STARTED, DIRECTOR MAY RUN OUT OF MEMORY

CR# Q00842221
 Last Updated: 03/04/2004
 Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2
 Current Status: Open

When the firewall is started, either during boot up or by the user restarting the firewall, Check Point does a “full sync” where it tries to sync up all the sessions from other Directors in the cluster. Under heavy stress, the “full sync” operation will take up all of the available memory and the Director will freeze.

If you are running NG AI, Check Point has a mechanism to limit the amount of memory that can be used by “full sync”.

1. Login to the Director as root
2. Run “make-part-rw / on” to make the root partition read/write
3. Edit “\$FWDIR/modules/fwkernel.conf” file and add “fw_sync_max_saved_buf_mem=138” as the last line.
4. Save \$FWDIR/modules/fwkernel.conf
5. Run “make-part-rw / off” to make the root partition read-only
6. Repeat on each Director

Issues Updated on 12/07/2003

‘STATE SYNCHRONIZATION OF THIS MACHINE IS AT RISK’ MESSAGE

CR# Q00742217

Last Updated: 12/07/2003

Affected Releases: 3.5.1.0g FP-4, 3.5.1.4a FP-4, 3.5.1.10d FP-4, 3.5.2 FP-4

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: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2

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.

EMAIL ARCHIVE DOES NOT INCLUDE ‘/VAR/TMP/TNGSYS.LOG’

CR# Q00786623

Last Updated: 12/07/2003

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2

Current Status: Open

If you setup email archiving on log files using '/cfg/sys/log/archive', the 'tngsys.log' file will not be sent via email, although it will be rotated properly. 'tngsys.log' file contains system messages that are not of much interest to the end user but will help with debugging.

WITH OSPF, AREA 0 CANNOT BE DISABLED

CR# Q00717195

Last Updated: 12/07/2003

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2

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.

ACCELERATOR STATS SHOW DISCARDS ON THE OUTBOUND

CR# Q00722198
 Last Updated: 12/07/2003
 Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2
 Current Status: Open

With the 6400 Accelerator, if you login directly to the Accelerator CLI and run `!stats/port <n>/if` command, the outbound Discards counter will almost be the same as outbound unicast packets counter. The packet counter for discard displays an incorrect value and does not mean that the packets are actually dropped.

'/MAINT/DEBUG/AC1/BTINFO' NOT SUPPORTED WITH 5X00 ACCELERATORS

CR# Q00784709
 Last Updated: 12/07/2003
 Affected Releases: 3.5.1.10d, 3.5.2
 Current Status: Open

This is a new command on ASF that gives you brief information about the last Accelerator bootup including the time and reason for the reboot. However, this command currently works only with the ASF 6400 Accelerator and not on any of the 5x00 Accelerators.

'ACCELERATOR SESSION TABLE OVERFLOW' MESSAGE IN SYSLOG

CR# Q00803000
 Last Updated: 12/07/2003
 Affected Releases: 3.5.1.4a
 Current Status: Fixed in 3.5.1.10d

ASF has a feature called 'NAT caching' to optimize the NAT performance. When a NAT connection is closed, the session on the Accelerator is marked for deletion. Under heavy stress, the Accelerator gives higher priority to adding new sessions and lower priority to purging the sessions marked for deletion. If the stress is heavy enough that the session add rate is higher than the session delete rate, and this stress is maintained for an extended period of time, the Accelerator session table usage will slowly keep increasing until it runs out.

ACCELERATION NOT RESTARTED EVEN THOUGH '/CFG/FW/ACCEL' IS SET

CR# Q00783207
 Last Updated: 12/07/2003

Affected Releases: 3.5.1.0g, 3.5.1.4a
Current Status: Fixed in 3.5.1.10d

When running prolonged stress tests, the Director may transition to accel-off and stay in accel-off even though the command “/cfg/fw/accel” is set to automatically restart acceleration. To recover, login to the Director as 'root' and run the following command: "service naap2d restart"

Issues Updated on 11/04/2003

IDS/SLB NOT SUPPORTED ON 5x00 ACCELERATORS

Last Updated: 11/04/2003
Affected Releases: 3.5.1.4a, 3.5.1.10d, 3.5.2
Current Status: No fix planned

IDS Load Balancing is a new feature that was introduced in 3.5.1.0g. This feature works only with the new 6400 Accelerator and not on the 5x00 series of Accelerators. There are no plans to implement ISDLB on the 5x00 series.

PORT MIRRORING LIMITATION ON 5x00 ACCELERATORS

Last Updated: 11/04/2003
Affected Releases: 3.5.1.4a, 3.5.1.10d
Current Status: Port mirroring not supported with 5x00 on 3.5.2. No fix planned.

When doing port mirroring for inbound packets with the 5x00 series Accelerators for packets that are forwarded to the Director, you will see the NAAP encapsulated packet instead of the original packet on the mirrored port. This is an inherent limitation of the 5x00 platform. If you mirror only outbound traffic, you will not see this problem. Port mirroring works correctly for both inbound and outbound traffic with the 6400 Accelerator.

DIRECTOR CAN UPGRADE ONLY DIRECTLY CONNECTED ACCELERATOR'S FIRMWARE

CR# Q00780070
Last Updated: 11/04/2003
Affected Releases: 3.5.1.4a, 3.5.1.10d, 3.5.2
Current Status: No fix planned

ASF 3.5.x uses VLAN tagging for NAAP traffic. ASF 3.0.x and earlier do not support VLAN tagging of NAAP traffic. Because of this, a Director running 3.5.x can upgrade an Accelerator running 3.0.x or earlier only if they are directly connected. In a high availability (HA) setup, the Director cannot upgrade the Accelerator that is connected through the inter-Accelerator port. When upgrading an HA cluster from 3.0.x to 3.5.x, please make sure that there is at least one Director connected to each Accelerator. When doing a fresh install, it is recommended to install the binary image on the Accelerators rather than depending on the Director to upgrade the Accelerators.

VLAN 4092 IS RESERVED

CR# Q00743287

Last Updated: 11/04/2003

Affected Releases: 3.5.1.0g

Current Status: Fixed in 3.5.1.4a

VLAN 4092 should not be defined and used. This VLAN is used internally by the 6400 Accelerator. Currently ASF allows you to configure VLAN 4092 without any errors but all traffic in this VLAN will be dropped.

ELA LOGGING FEATURE DOES NOT WORK

CR# Q00771385

Last Updated: 11/04/2003

Affected Releases: 3.5.1.0g

Current Status: Fixed in 3.5.1.4a

The ELA Logging feature of ASF does not work with 3.5.1.0g.

Issues Updated on 10/16/2003

VRRP MAC FEATURE IS NOT AVAILABLE

Last Updated: 10/16/2003

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2

Current Status: No fix planned

The VRRP MAC feature introduced in ASF 3.0.1 has been temporarily removed from this release of ASF. This feature will no longer be supported.

DYNAMIC ROUTING ISSUES

Last Updated: 10/16/2003

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2

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: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2

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.

MAXIMUM NUMBER OF INTERFACES SUPPORTED IS 250

CR# Q00742985

Last Updated: 10/16/2003

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2

Current Status: Open

The maximum number of user-defined interfaces supported in this release is 250. Although ASF will allow you to configure up to 255 interfaces, please do not configure more than 250 interfaces.

AUTO-JOIN FAILURE

CR# Q00741429

Last Updated: 10/16/2003

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2

Current Status: Open

In some rare situations, auto join may fail. You will get the following error on the Firewall Director that is trying to join: 'Unable to contact system'. When this happens, please try to join manually using the same IP address, or reboot the Director that failed to auto join so that it will try the auto join again.

CHECK POINT SYNC STOPS WORKING AFTER CHANGING SYNC DEVICE

CR# Q00748787

Last Updated: 10/16/2003

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2
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: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2
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.

MISSING '/VAR/TMP/TNGSYS.LOG' FILE

CR# Q00747993
Last Updated: 10/16/2003
Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2
Current Status: Open

In order to make the messages in “/var/log/messages” less cluttered and easier to understand, most of the cryptic messages have been moved to a new file '/var/tmp/tngsys.log'. But if you do an upgrade to 3.5.1.0g from 3.0.x, this new file will be missing and all messages will still go into “/var/log/messages”. Please contact Nortel Support for a patch to fix this.

'PACKET OUT OF STATE' MESSAGE UNDER STRESS

CR# Q00733543
Last Updated: 10/16/2003
Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2
Current Status: Open

When running ASF with NG AI under stress, you may see drops in the SmartView Tracker with the message that packet with RST flag or ACK flag is out of state. Normally this does not affect the communication between hosts across the ASF because the packets that are dropped are part of the session teardown sequence.

POLICY INSTALLATION FAILS WITH ERROR "TCP CONNECTIVITY FAILURE"

CR# Q00683652

Last Updated: 10/16/2003

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2

Current Status: Open

Sometimes while installing policy on the ASF, you may get an error saying "TCP connectivity failure". When this happens, quit out of SmartDashboard and any other GUI clients you have open, run 'cpstop' followed by 'cpstart' on the management server, open SmartDashboard and try to install the policy again.

FIREWALL DIRECTOR TAKES MORE THAN 10 MINUTES TO RECOVER

CR# Q00724862

Last Updated: 10/16/2003

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2

Current Status: Open

If you have enabled RIP or OSPF on the ASF and there are a large number of dynamic routes (> 1000), if the MIP holder is unplugged from the cluster and plugged back in immediately, it will take approximately 10 minutes for the Director to recover and start processing traffic normally. During this period, any traffic being hashed to this Director will be dropped. If you get into this situation, please reboot the Director immediately to recover.

AUTO NEGOTIATION OFF WITH FE LINKS

CR# Q00734318

Last Updated: 10/16/2003

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2

Current Status: Open

When auto negotiation is turned off for the FE links, with some 3rd party equipment, you may not get a link light when the Accelerator boots up. When this happens, just unplug the cable from the Accelerator and plug it back in to get link. If link speed and duplex is being negotiated properly when auto negotiation is on, it is recommended that auto negotiation be enabled so that you don't have to manually bounce the link each time the Accelerator is rebooted.

INTERFACE AND STATIC ROUTE IN THE SAME SUBNET

CR# Q00617850

Last Updated: 10/16/2003

Affected Releases: 3.5.1.0g, 3.5.1.4a, 3.5.1.10d, 3.5.2

Current Status: Open

If you have an interface and a static route to the subnet of that interface, the expected behavior is that the ASF will use the connected route when the interface is up and the static route when the interface is down. But if you add the static route before you add the interface, ASF will incorrectly use the static route even if the interface is up. If this happens, please delete the static route add it again.