Release Notes

Alteon Switched Firewall™

Release 3.5.3

Part Number: 215041-K, June 2004

NORTEL NETWORKS™

4655 Great America Parkway
Santa Clara, CA 95054
Phone 1-800-4Nortel
www.nortelnetworks.com

Export

This product, software and related technology is subject to U.S. export control and may be subject to export or import regulations in other countries. Purchaser must strictly comply with all such laws and regulations. A license to export or reexport may be required by the U.S. Department of Commerce.

Licensing

This product includes software developed by Check Point Software Technologies (http://www.checkpoint.com). This product also contains software developed by other parties.

For more information, see Appendix D, "Software Licenses," in the ASF 3.5.1 User's Guide and Command Reference.

Common Criteria Certified Software

For more details, see Appendix E, "Common Criteria Certified Software" in the ASF 3.5.1 User's Guide and Command Reference.

Regulatory Compliance

International regulatory statements of conformity

This is to certify that the Nortel Networks 8000 Series chassis and components installed within the chassis were evaluated to the international regulatory standards for electromagnetic compliance (EMC) and safety and were found to have met the requirements for the following international standards:

- EMC - Electromagnetic Emissions – CISPR 22, Class A
- EMC - Electromagnetic Immunity – CISPR 24
- Electrical Safety – IEC 60950, with CB member national deviations

Further, the equipment has been certified as compliant with the national standards as detailed below.

National electromagnetic compliance (EMC) statements of compliance

FCC statement (USA only)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission (FCC) rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to take whatever measures may be necessary to correct the interference at their own expense.

ICES statement (Canada only)

Canadian Department of Communications Radio Interference Regulations

This digital apparatus does not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

CE marking statement (Europe only)

EN 55 022 statements

This is to certify that the Nortel Networks equipment are shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC. Conformity is declared by the application of EN 55 022 Class A (CISPR 22).

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case, the user may be required to take appropriate measures.

Achtung: Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Attention: Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilisateur de prendre les mesures spécifiques appropriées.

EN 55 024 statement

This is to certify that the Nortel Networks equipment is shielded against the susceptibility to radio interference in accordance with the application of Council Directive 89/336/EEC. Conformity is declared by the application of EN 55 024 (CISPR 24).

EC Declaration of Conformity

This product conforms to the provisions of the R&TTE Directive 1999/5/EC.

VCCI statement (Japan/Nippon only)

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI) for information technology equipment. If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

BSMI statement (Taiwan only)

This is a Class A product based on the standard of the Bureau of Standards, Metrology and Inspection (BSMI) CNS 13438, Class A.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

MIC notice (Republic of Korea only)

This device has been approved for use in Business applications only per the Class A requirements of the Republic of Korea Ministry of Information and Communications (MIC). This device may not be sold for use in a non-business application. Reference Regulatory label on the base of the equipment for specific Korean approval information.

National Safety Statements of Compliance

CE marking statement (Europe only)

EN 60 950 statement

This is to certify that the Nortel Networks equipment are in compliance with the requirements of EN 60 950 in accordance with the Low Voltage Directive. Additional national differences for all European Union countries have been evaluated for compliance. Some components installed within the 8000 Series chassis may use a nickel-metal hydride (NiMH) and/or lithium-ion battery. The NiMH and lithium-ion batteries are long-life batteries, and it is very possible that you will never need to replace them. However, should you need to replace them, refer to the individual component manual for directions on replacement and disposal of the battery.

Lithium Battery Cautions

Caution—This product contains a lithium battery. Batteries are not customer replaceable parts. They may explode if mishandled. Do not dispose of the battery in fire. Do not disassemble or recharge.

(Norge) ADVARSEL—Litiumbatteri - Eksplosjonsfare. Ved utskifting benyttes kun batteri som anbefalt av apparatfabrikanten. Brukt batteri returneres apparatleverandøren.

(Sverige) VARNING—Explosionsfara vid felaktigt batteribyte. Använd samma batterityp eller en ekvivalent typ som rekommenderas av apparattillverkaren. Kassera använt batteri enligt fabrikantens instruktion.

(Danmark) ADVARSEL! Litiumbatteri - Eksplosionsfare ved fejlagtig håndtering. Udskiftning må kun ske med batteri af samme fabrikat og type. Levér det brugte batteri tilbage til leverandøren.

(Suomi) VAROITUS—Paristo voi räjähtää, jos se on virheellisesti asennettu. Vaihda paristo ainoastaan laitevalmistajan suosittelemaan tyyppiin. Hävitä käytetty paristo valmistajan ohjeiden mukaisesti.

Safety Information

Caution—Nortel Networks products are designed to work with single-phase power systems having a grounded neutral conductor. To reduce the risk of electric shock, do not plug Nortel Networks products into any other type of power system. Contact your facilities manager or a qualified electrician if you are not sure what type of power is supplied to your building.

Caution—Not all power cords have the same ratings. Household extension cords do not have overload protection and are not meant for use with computer systems. Do not use household extension cords with your Nortel Networks product.

Caution—Your Nortel Networks product is shipped with a grounding type (three-wire) power cord. To reduce the risk of electric shock, always plug the cord into a grounded power outlet.

NOM statement (Mexico only)

The following information is provided on the devices described in this document in compliance with the safety requirements of the Norma Oficial Méxicana (NOM):

Exporter:Nortel Networks, Inc.
4655 Great America Parkway
Santa Clara CA 95054 USA

Importer:Nortel Networks de México, S.A. de C.V.
Avenida Insurgentes Sur #1605
Piso 30, Oficina
Col. San Jose Insurgentes
Deleg-Benito Juarez
México D.F. 03900

Tel:52 5 480 2100

Fax: 52 5 480 2199

Input:100 to 240 VAC, 50 to 60 Hz, 9 A max. per power supply
single supply, or + one redundant supply configurations

Información NOM (unicamente para México)

La información siguiente se proporciona en el dispositivo o en los dispositivos descritos en este documento, en cumplimiento con los requisitos de la Norma Oficial Méxicana (NOM):

Exportador: Nortel Networks, Inc.
4655 Great America Parkway
Santa Clara, CA 95054 USA

Importador: Nortel Networks de México, S.A. de C.V.
Avenida Insurgentes Sur #1605
Piso 30, Oficina
Col. San Jose Insurgentes
Deleg-Benito Juarez
México D.F. 03900

Tel: 52 5 480 2100

Fax:52 5 480 2199

Embarcar a:100 to 240 V CA, 50 to 60 Hz, 9 A max. por fuente de poder
una fuente o una + configuraciones de una fuente redundante

Release Notes

These release notes provide the latest information regarding your Alteon Switched Firewall software version 3.5.3 and higher.

Documentation on CD ROM

This document is a supplement to the complete ASF 3.5.1 documentation suite. Please keep this document with your product manuals. For additional technical questions regarding the product architecture and features, refer to the following ASF 3.5.1 product documentation:

- *Alteon Switched Firewall 3.5.1 User's Guide and Command Reference* (part number 215709-A)
- *Alteon Switched Firewall Hardware Installation Guide* (part number 215712-A)
- *Alteon Switched Firewall 3.5.1 Browser-Based Interface Quick Access Guide* (part number 215710-A)

These documents are available on the Web. The manuals are PDF files which can be read and printed using the free Acrobat Reader software available from Adobe Systems Incorporated (http://www.adobe.com). To obtain a manual in hardcopy format, contact your Nortel Networks sales representative and order the part numbers.

Late-Breaking News

Before you put your system into commission, please check the Nortel Networks Customer Support Web site for the latest software and documentation on the Alteon Firewall. Be sure to review the readme.txt file collocated with the software, which has the list of open Change Requests (CRs) and closed CRs for this release. To access the Web site:

- Point your browser to http://www.nortelnetworks.com/documentation.
- Go to the Software page for the Alteon Firewall by selecting:

  Alteon/ASF Accelerated Firewall (Software)
- Click on “Date” in the list header to sort the Software page by date (ascending or descending).
- Double click on a title and enter the registered user name and password previously assigned to you by Nortel Networks Customer Support.

  If you are not a registered user at Nortel Networks, please click on the **Register** button on the left-hand column of the Nortel Networks Customer Support Web site, and follow the 5-step registration process.

NOTE – The Nortel Networks Customer Support Web site also provides access to Nortel Networks customer support for accounts under warranty or accounts that are covered by a maintenance contract.

Release 3.5.3 Changes

Software Support

Alteon Switched Firewall version 3.5.3 is supported on the following Check Point™ software:

- Check Point FireWall-1® NG Application Intelligence (R54) with Hotfix Accumulator, number 410 (HFA_410) software
- Check Point FireWall-1 NG Feature Pack 3 (FP3) with Hotfix Accumulator, number 325 (HFA_325) software

Hardware Support

Typically, Firewall capacity refers to higher throughput, concurrent sessions, and sessions per second. Higher throughput and concurrent sessions are determined by the Firewall Accelerator model and sessions per second are determined by the Firewall Director model.

Use compatible Alteon Switched Firewall components as shown in Table 1 to achieve the desired performance.

Table 1 Supported Combinations for ASF 3.5.3

Firewall Accelerator Models	Firewall Director Models	ASF
5700	5014	5714
5700	5010	5710
5600	5014	5614
5600	5010	5610
5400	5009	5409
5400	5008	5408
5300	5008	5308

ASF 5714, 5614, and 5409 are the only combinations that are available as product bundles on the price list. ASF 3.5.3 software is not supported on Firewall Accelerator 6400.

Upgrading to ASF 3.5.3

The upgrade procedure requires you to prepare each Firewall Director in the cluster by running a clean-up script (UpgradePrep.sh). This script is available at the Nortel Support Web site (http://www.nortelnetworks.com/support) under Alteon >Alteon Switched Firewall System > ASF Accelerated Firewall Software.

Refer to the table below to upgrade to ASF 3.5.3 software from different versions of the ASF-software and Check Point Feature Packs.

Table 1 Upgrading to ASF 3.5.3 Software

From	To	Steps to Upgrade
ASF 3.5.3 with FP3	ASF 3.5.3 with R54 (HFA 410)	■ Prepare each Firewall Director in the cluster using UpgradePrep.sh script. ■ Use `/boot/software/patch/install` to get and install the latest R54 code (fp4patch-3.5.3-1.i386.rpm). This should be done on one Firewall Director only. ■ Reboot each Firewall Director in the cluster.
ASF 3.5.x with R54	ASF 3.5.3 with R54 (HFA 410)	■ Clean up each Firewall Director in the cluster using UpgradePrep.sh script. ■ Use `/boot/software/download` to download R54 upgrade package (ASF_Director_3.5.3.0_FP4.pkg). This should be done on one Firewall Director only. ■ Activate 3.5.3 image using `/boot/software/activate`. This should be done on one Firewall Director only. ■ Clean up each Firewall Director in the cluster using the UpgradePrep.sh script. ■ Use `/boot/software/patch/install` to get and install the latest HFA for R54 (hfa410patch-3.5.3-1.i386.rpm). This should be done on one Firewall Director only. ■ Reboot each Firewall Director in the cluster.

NORTEL NETWORKS
215041-K, June 2004

Table 1 Upgrading to ASF 3.5.3 Software

From	To	Steps to Upgrade
ASF 3.5.x with FP3 ASF 3.0.x with FP3 ASF 3.0.x with FP2	ASF 3.5.3 with R54 (HFA 410)	■ Clean up each Firewall Director in the cluster using UpgradePrep.sh script. ■ Use `/boot/software/download` to download the R54 upgrade package (ASF_Director_3.5.3.0_FP4.pkg). This should be done on one Firewall Director only. ■ Activate 3.5.3 image using `/boot/software/activate`. This should be done on one Firewall Director only. ■ Use `/cfg/fw/software/ngai` to activate R54 software. This should be done on one Firewall Director only. ■ Reboot each Firewall Director in the cluster.
ASF 3.5.x with FP3 ASF 3.0.x with FP3	ASF 3.5.3 with FP3 (HFA-325)	■ Clean up each Firewall Director in the cluster using UpgradePrep.sh script. ■ Use `/boot/software/download` to download FP3 upgrade package (ASF_Director_3.5.3.0_FP3.pkg). This should be done on one Firewall Director only. ■ Activate 3.5.3 image using `/boot/software/activate`. This should be done on one Firewall Director only. ■ Clean up each Firewall Director in the cluster using the UpgradePrep.sh script. ■ Use `/boot/software/patch/install` to get and install the latest HFA for FP3 (hfa325patch-3.5.3-1.i386.rpm). This should be done on one Firewall Director only. ■ Reboot each Firewall Director in the cluster.
ASF 3.0.x with FP2	ASF 3.5.3 with FP3 (HFA-325)	■ Clean up each Firewall Director in the cluster using UpgradePrep.sh script. ■ Use `/boot/software/download` to download FP3 upgrade package (ASF_Director_3.5.3.0_FP3.pkg). This should be done on one Firewall Director only. ■ Activate 3.5.3 image using `/boot/software/activate`. This should be done on one Firewall Director only. ■ Use `/cfg/fw/software/fp3` to activate FP3 software. This should be done on one Firewall Director only. ■ Reboot each Firewall Director in the cluster.

Configuring VLAN ID for NAAP ports

ASF 3.5.3 allows you to modify the VLAN ID for the NAAP port from the default value of 4094. This is primarily used to support topologies where NAAP traffic flows through Passport switches. The VLAN ID for the NAAP port can be any number between 2 and 4094 (except 4092).

To modify the default VLAN ID for a NAAP port, use one of the following procedures depending on your installation type:

- New ASF 3.5.3 Installation
- Upgrading to ASF 3.5.3

New ASF 3.5.3 Installation

If your ASF 3.5.3 installation is new, then follow these steps to modify the NAAP VLAN ID.

1. **Disconnect all the Firewall Directors in the cluster.**
2. **Reimage the Firewall Directors with ASF 3.5.3 iso image.**
3. **Login as admin and change the NAAP VLAN ID using the naap menu.**

   This needs to be done on all the Firewall Directors in the ASF cluster before running any other CLI command (for example, new) as shown below:

```
login: admin
Password: admin (not displayed)

Welcome to the Alteon Switched Firewall initialization.
------------------------------------------------------------
[Setup Menu]
      join      - Join an existing SFD cluster
      new       - Initialize SFD as a new installation
      restore   - Restore this SFD from a backup taken earlier
      offline   - Initialize SFD for offline switchless maintenance
      boot      - Boot Menu
      naap      - Set NAAP VLAN id
      exit      - Exit

>> Setup#
```

4. **Load the binary Firewall Accelerator image on all the accelerators in the ASF cluster.**

5. **Change the NAAP VLAN ID on all the Firewall Accelerators using the following commands:**

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

6. **Connect the Firewall Directors to the Firewall Accelerators and continue with the Setup procedure.**

Upgrading to ASF 3.5.3

If you are upgrading to ASF 3.5.3 from an older version, then you must make CLI changes on the Firewall Accelerator and modify the configuration file (`/opt/tng/conf/config`) on the Firewall Director.

1. **Upgrade the Firewall cluster to ASF 3.5.3 as described in "Upgrading to ASF 3.5.3" on page 10.**

   Make the system operational without changing the NAAP VLAN ID. At the end of this step, the Accelerators are automatically upgraded to ASF 3.5.3.

2. **Disconnect all the Firewall Directors in the cluster from the Firewall Accelerators.**

3. **Configure NAAP VLAN ID on all Firewall Directors using the following steps:**

   - Edit the config file (`/opt/tng/conf/config`) using `vi` editor in Linux and modify the line

     #NAAP_VLAN_ID=<*number*> to NAAP_VLAN_ID=<*number*>

     where <*number*> is the NAAP VLAN ID.

     If the config file does not include the above line, then add the following line at the end of the file:

     NAAP_VLAN_ID=<number>

   - Save the config file.
   - Reboot the Firewall Director.

4. **Reboot all the Firewall Accelerators in factory default configuration.**

5. **Modify the NAAP VLAN ID on 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
```

6. **Connect the Firewall Directors to the Firewall Accelerators.**

   The ASF cluster should become operational without user intervention.

Long TCP Sessions Time out

Long TCP sessions like Telnet and SSH may get deleted from the firewall even if the sessions were not idle. Typically, this happens when traffic is very low in the session. To prevent the session from being timed out, increase the session time-out value of the affected service to 24 hours.

Active FTP with Hide NAT

If you have multiple Firewall Directors in the cluster and if the FTP client is behind hide NAT, ASF 3.5.3 allows active FTP to behave correctly.