

RELEASE NOTES



Alteon Switched Firewall™ Release 3.5.2

Part Number: 215041-H, March 2004

NORTEL
NETWORKS™

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

Copyright © 2004 Nortel Networks, Inc., 4655 Great America Parkway, Santa Clara, California, 95054, USA. All rights reserved. Part Number: 215041-H.

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of Nortel Networks, Inc. Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement or the implied warranties of merchantability or fitness for a particular purpose.

U.S. Government End Users: This document is provided with a “commercial item” as defined by FAR 2.101 (Oct. 1995) and contains “commercial technical data” and “commercial software documentation” as those terms are used in FAR 12.211-12.212 (Oct. 1995). Government End Users are authorized to use this documentation only in accordance with those rights and restrictions set forth herein, consistent with FAR 12.211- 12.212 (Oct. 1995), DFARS 227.7202 (JUN 1995) and DFARS 252.227-7015 (Nov. 1995).

Nortel Networks, Inc. reserves the right to change any products described herein at any time, and without notice. Nortel Networks, Inc. assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Nortel Networks, Inc. The use and purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of Nortel Networks, Inc.

Alteon, Alteon WebSystems, Alteon Switched Firewall, Firewall OS, Firewall Director, ASF 5009, ASF 5010, ASF 5014, Accelerator OS, Firewall Accelerator, ASF 5400, ASF 5600, ASF 5700, and ASF 6400 are trademarks of Nortel Networks, Inc. in the United States and certain other countries.

Check Point, SecureXL, SmartView Monitor, and SmartCenter are trademarks of Check Point Software Technologies Ltd. FireWall-1 and VPN-1 are registered trademarks of Check Point Software Technologies Ltd. Any other trademarks appearing in this manual are owned by their respective companies.

Originated in the USA.

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 Mexicana (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 Mexicana (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 3.5.2 and higher.

This document is a supplement to the complete 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

Please check your software and documentation for any “Readme” document file. The readme file may contain important information regarding the product.

Release 3.5.2 Changes

Software Support

Alteon Switched Firewall version 3.5.2 supports Check Point™ FireWall-1® NG with Application Intelligence (R54) and Feature Pack 3 (FP3) Hotfix Accumulator, number 318 (HFA_318) 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 3.5.2

Firewall Accelerator Models	Firewall Director Models	ASF
6400	5014	6414
5700	5014	5714
5700	5010	5710
5600	5014	5614
5600	5010	5610
5400	5009 ^a	5409
5400	5008	5408
5300	5008	5308

a.The 5009 Director is supported with ASF 6400 if you are upgrading from the standalone ASF 5109 to the accelerated 6409.

ASF 6414, 5714, 5614, and 5409 are the only combinations that are available as product bundles on the price list.

Mix Director Types in a Cluster

ASF 3.5.2 supports different Director types in an ASF cluster. You cannot however, combine Directors 501x with 500x because of the difference in memory. For example, 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

This feature affects the Sync Configuration Menu (`cfg/fw/sync`) in the CLI. This menu used to be the same for all the cluster members. However, with this new feature, the `dev`, `autoneg`, `speed` and `mode` settings are now Director-specific, and other CLI items in the menu apply to all members in the cluster.

Audit Trail Support

ASF 3.5.2 supports a log mechanism that enables logging of all CLI actions performed by a user. This enhances your ability to pinpoint and respond to critical events, allows you to track admin user actions, and serves as a useful tool for debugging functions. The ASF Firewall keeps a log of the CLI commands and sends it to any configured syslog or RADIUS servers. To support audit trail, specify Radius server information using the CLI under `/cfg/sys/adm/audit`. For more information on the audit trail menu commands, see page 208 of the *Alteon Switched Firewall 3.5.1 User's Guide and Command Reference*.

SmartView Monitor Support

ASF 3.5.2 allows you to monitor your firewall performance in real time using Check Point SmartView Monitor™.

Local Network Support Removed

ASF 3.5.2 does not support local network route cache (`/cfg/net/adv/local`). Any local network settings that are present in the registry before the upgrade will be ignored by the ASF 3.5.2 software.

Remote Login via SSH

ASF 3.5.2 allows remote users to login to troubleshoot or perform maintenance on the firewall.

This feature must be used cautiously, because it provides users with the ability to login remotely using SSH and access the Linux shell. Remote users with root password can use the the Linux utility, `su` and run “su root”.

The following defenses are built-in to ensure maximum security.

- To log in, the user has to authenticate using the public key/private key mechanism. DSA or RSA key pairs can be used but has to be in OpenSSH format version 2 format only. Password based authentication is not allowed.
- The IP address of the remote user must be part of the access list.
- The Check Point policy must allow the SSH connection between the remote user and the ASF.

The following new CLI items have been added to manage remote SSH users.

/cfg/sys/user/adv/user

SSH User Menu

```
[SSH User <user name> Menu]
  name      - Set Full name of User
  pubkey    - Set RSA/DSA Public Key for User
  ena       - Enable User Account
  dis       - Disable User Account
  del       - Remove SSH User
```

This menu allows you to manage remote SSH users.

Table 2 Remote SSH Users Menu (/cfg/sys/user/adv/user)

Command Syntax and Usage

name

This command sets the full name of the user.

pubkey

This command allows you to set the RSA or DSA public key for the user. The user will not be able to login until this value is set correctly and the SSH client is configured to use the corresponding private key for authentication. The RSA or DSA key has to be in OpenSSH v2 format only.

ena

This command enables the user account.

Table 2 Remote SSH Users Menu (`/cfg/sys/user/adv/user`)

Command Syntax and Usage

dis

This command disables the user account.

del

This command removes the user account.

Port Mirroring

ASF 3.5.2 does not support port mirroring (`/cfg/net/mirr`) on the 5000 series Firewall Accelerators. Port mirroring is supported on the Firewall Accelerator 6400.

Backup and Restore Firewall Configuration

ASF 3.5.2 allows you to backup the Director configuration and restore it later to the same state. The restore operation will restore the configuration in the registry as well as the Check Point SIC and policy.

The backup and restore feature is for a Director only and not the cluster. To backup an entire cluster, you must login to each Director and create backups separately. You cannot create a backup from one member of the cluster and use it to restore another member. A backup taken from a Director can be used only to restore that same Director or a replacement for that Director.

Creating a Backup

To create a backup of a Director, do the following using the Command Line Interface (CLI):

1. **Login as “admin” and run the command, `/maint/backup/backup`.**

You will be prompted to provide an FTP server.

2. **Provide the name of the FTP server to backup.**

The FTP server should allow anonymous login.

Restoring the Director

The restore process cannot fix a corrupt file system. If the Director becomes unusable because of a file system corruption, re-image the box before attempting to restore. The recommended way to restore is to re-image the Director and restore. However, you may restore the Director, by doing the following:

- 1. Copy the backup file to a CDROM.**

You can also restore from a local file on the hard disk, but by default, the restore process checks the CDROM for the backup file.

- 2. Disconnect the Director from the cluster if your Director is already part of a cluster.**

If you `/boot/delete` the Director while it is still connected to the cluster, it cannot be restored since the cluster will no longer consider that Director as part of the cluster.

- 3. Restore the Director to its factory default configuration with the command `/boot/delete`.**

This is mandatory as restore can be done only on a Director in factory default configuration.

- 4. Login as `admin` to see the Setup menu.**

- 5. Choose `restore` from the list of options.**

You will be prompted to insert the CDROM.

- 6. Insert the CDROM and press `<Enter>`.**

A list of all `.tar` files in the root directory of the CDROM is displayed.

- 7. Select the backup file.**

When prompted for the filename, either accept the default choice or enter your own. The file is copied to the hard drive and the CD ejected. It will take about 30 seconds for the restore to complete. When restore is complete, you will be logged out of the CLI.

- 8. Login again as `admin` and you will see the Configuration menu instead of the Setup menu.**