Nortel Switched Firewall 4.1.1

Release Notes

part number: 217017-C, July 2005

4655 Great America Parkway
Santa Clara, CA 95054
Phone 1-800-4Nortel
http://www.nortel.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.

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 Nortel Switched Firewall, version 4.1.1 and higher. This document modifies information found in the complete documentation. Please keep this information with your Nortel Networks product manuals.

The following topics are addressed in these Release Notes:

Late-Breaking News and Support

Before you put your system into commission, please check the Nortel Networks Technical Support Web site for the latest software and documentation on the Switched Standalone Firewall. Be sure to review the Readme file on the Software Detail Information page, which has the list of open Change Requests (CR) and closed CRs for this release. To access the Web site:

- Point your browser to: http://www.nortel.com/cs. The Technical Support page will open.
- Select the **Browse product support** tab.

  ① Select from **Product Families** (**Alteon / Alteon Switched Firewall System**)

  ② choose a product (**ASF Accelerated Switched Firewall**)

  ③ and get the content (**Software**)

  Then click on **Go**.
- Click on a software title and enter the registered user name and password previously assigned to you by Nortel Networks Technical Support. This opens the Software Detail Information page.

  If you are not a registered user, please click on the **Register** link on the left-hand column of the Nortel Networks Technical Support Web site, and complete the registration process.

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

- You must authenticate at the Check Point Web site to obtain the Firewall software. Instructions are provided on the Software Detail Information page to help you access and navigate the Check Point Web site.

  For Check Point Release Notes, go to http://www.checkpoint.com/techsupport/installation/ng/release_notes.html

  For Check Point User Documentation, go to http://www.checkpoint.com/support/technical/documents/index.html
- A Readme file for Release 4.1.1 is kept on the Software Detail Information page. Just click on the **ReadMe** link to download the file to your workstation.

Documentation

The following manuals are supplied on a CD-ROM that ships with new products:

- *Nortel Switched Firewall* 4.1.1 *User's Guide and Command Reference* (217014-B)
- *Nortel Switched Firewall Hardware Installation Guide* (217016-B)
- *Nortel Switched Firewall* 4.1.1 *Browser-Based Interface Users Guide* (217015-B)

The manuals are PDF files that can be read and printed using the free Acrobat Reader software available from Adobe Systems Incorporated (http://www.adobe.com).

To access a manual, open the `welcome.pdf` file on the *Nortel Switched Firewall 4.1.1 Documentation* CD-ROM and select a title. When the manual opens, you can navigate through it by selecting the bookmarks on the left side of the window or by scrolling through the pages.

You can also download the manuals from the Nortel Networks Technical Support Web site. To access the site, follow the procedure in "Late-Breaking News and Support" on page 8 but select **Documentation** instead of **Software**. The Documentation page opens sorted by date. Click on a title to open it in your browser.

To reduce clutter on the Documentation page, click on the **Rls** header. This will sort the page by Release and omit any document that doesn't have a Release version.

New Features

The following features have been added to the Nortel Switched Firewall release 4.1.1 since the last major release:

Software Support

Nortel Switched Firewall 4.1.1 supports Check Point™ FireWall-1® NG with

- Application Intelligence R55 and Hotfix Accumulator 512 (HFA_512) software
- Application Intelligence R54 and Hotfix Accumulator 414 (HFA_414) software

Hardware Support

Nortel Switched Firewall 4.1.1 supports two new Firewall Directors, 5016-NE1 and 5026-NE1. As a result, four additional Nortel Switched Firewall systems are supported: NSF 6616, 6416, 6626, and 6426.

Table 1 lists all the supported hardware platforms with the different Firewall Accelerator and Firewall Director systems.

Table 1 Firewall Systems

NSF	Firewall Accelerator	Firewall Director
6616	6600	5016-NE1
6416	6400	5016-NE1
6614	6600	5014
6414	6400	5014
6626	6600	5026-NE1
6426	6400	5026-NE1
6624	6600	5024
6424	6400	5024

For more details on the supported hardware, see the Nortel Switched Firewall 4.1.1 *Hardware Installation Guide* (217016-B).

Routing and bridging

- Supports pure Layer 2 and Layer 3 Firewall
- Supports multicast Protocol Independent Multicast-Sparse Mode (PIM-SM)
- Supports Open Shortest Path First (OSPF) route maps

  OSPF route maps are used to control the redistribution of routes between OSPF and any other protocols such as, RIP, static, OSPF, and connected. The globally configured route maps is used to implement routing policies.

Reliability and Redundancy

- Gateway Persistency

  In a multiple ISP links scenario, gateway persistency ensures that the requests and responses for a given connection always traverse the same gateway that is forwarding the packets.

- Manages power supply by supporting APC Uniterruptible Power Supply (UPS) models

  UPS is supported through USB and SNMP.

- Supports USB storage stick

  The USB port can be used to store all uploads such as tsdump, backup, configuration, and Check Point logs.

- Supports RADIUS Authentication in both standalone and high availability configurations

  Multiple RADIUS servers can be configured for redundancy.

- Supports secure file transfer through SCP/SFTP

  SCP/SFTP uses a username and password for authentication.

- Firewall Accelerator link teardown during failover

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

Usability Enhancements

- Out-of-band management port

  The out-of-band management port allows you to automatically use the BBI to configure the firewall. You start the BBI using the management port interface and configure the firewall. Basically, you don't need to configure the CLI to start using the BBI if you configure the out-of-band management port.

- Extended logging

  Detailed information on errors is available immediately both at the CLI and on the BBI.

- Configuration wizards

  To simplify configurations, wizards are provided in the new improved Browser-Based Interface (BBI). These wizards will help you setup the firewall, add VLANs and interfaces, configure routes, gateways, GRE Tunnel, DHCP Relay, OSPF, RIP, PIM, remote access, ELA log daemon, and set up high availability.

  For more information, see the NSF 4.1.1 *Browser-Based Interface Users Guide* (215710-B).

- New CLI commands

  - Viewing traffic information

    The new command /info/traffic displays traffic information.

  - Viewing port properties and NSF capability

    The `/info/net/sfdports` command displays port properties. The `/info/capability` command displays capabilities of the firewall, such as maximum interfaces, number of ports, VLANS, default gateways, trunks, filters, connections and so on.

  - Downloading Secure-ID configuration

    The `/cfg/apps/securid` command allows you to download Secure-ID configuration.

Security

Nortel Switched Firewall 4.1.1 allows for deep packet inspection, and as a result:

- Protects the firewall from DoS attacks
- Manages the maximum number of ARP, ICMP, TCP, and UDP packets per second sent to the Firewall Accelerator.
- Protects against UDP blasts
- Blocks client IP addresses
- Rate limits TCP, UDP, and ICMP sessions
- Deny TCP or UDP traffic based on pattern matching

Load balancing Firewall Directors

Firewall Director load balancing allows you to set different weights for each Firewall Director present in a cluster. Apart from doing load balancing based on IP hash and IP port hash, the load is evenly distributed depending upon the Firewall Director weight.

Upgrade

Hitless Upgrade is supported in a high availability environment which keeps the network traffic flowing with minimal disruption in service during the upgrade process. In case of failure, the hitless upgrade allows for graceful rollback to previous version without affecting traffic.

NSF 4.1.1 allows you to load the new image from a CD-ROM or the USB port.

Troubleshooting

- Tracing NSF packets

  The packet capture command, `asfcapture` allows you to trace a packet as it passes through different devices and modules on the Nortel Switched Firewall. In previous releases, you had to use several packet capture commands (`ethereal`, `tcpdump`, and `debug`) separately to capture and trace the packets at different locations in the kernel. The `asfcapture` command is available from `root` login only.

- Simplifying packet capture using the `fw monitor` command

  The /info/fwmon command 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.

- Capturing packets using the `ethereal` command

  The `ethereal` packet capture tool allows you to capture packets on the Firewall Director and display the output to the CLI or save it to a TFTP (FTP/SFTP) server or the USB port.

Check Point Applications Supported

Nortel Switched Firewall 4.1.1 supports the following Check Point applications. To support these applications on the Nortel Switched Firewall hardware systems, you must configure NSF 4.1.1 and the Check Point software:

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

  The following management tools do not need any configuration within the NSF 4.1.1 software; these tools are configured outside of the NSF 4.1.1 software:
  - SmartDashboard™
  - SmartView Tracker™
  - SmartView Status™