Nortel Switched Firewall 5100 Series
Release 2.3.1
Release Notes

part number: 213456-R, June 2005

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

4655 Great America Parkway, Santa Clara, California, 95054, USA. Part Number: 213456-R.

Regulatory Compliance

International regulatory statements of conformity

This is to certify that the Nortel Networks 5100 Series is 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 the Nortel Switched Firewall 5100 Series for Release 2.3.1. This supplement 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 (**Switched Firewall 5100 series**)

  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 2.3.1 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 2.3.1 User's Guide and Command Reference* (213455-K)
- *Nortel Switched Firewall 5100 Series Hardware Installation Guide* (216382-C)
- *Nortel Switched Firewall 2.3.1 Browser-Based Interface Users Guide* (216383-C)

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 5100 Series 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 2.3.1 since the last major release:

Software Support

Nortel Switched Firewall 2.3.1 supports Check Point® FireWall-1® NG with the following Application Intelligence software:

Table 1 Check Point version and corresponding NSF software images

NG Version	Hot Fix Accumulator	NSF Software Images
R55	HFA-12	NSF5100_2.3.1.0_R55.img/.iso/.pkg

For more information on the software features, see *Nortel Switched Firewall 2.3.1 User's Guide and Command Reference* (213455-K).

Hardware Support

Nortel Switched Firewall 2.3.1 software is supported on the following hardware systems:

- **New systems:** NSF 5111-NE1, 5114-NE1, and 5124-NE1
- **Existing systems:** NSF 5106, 5109, 5114, and 5124

The platforms differ with respect to hardware features and performance. But in all other operational aspects (software, certification, system management, logging, and monitoring) the platforms are the same.

For more information on the hardware features, see *Nortel Switched Firewall* 5100 Series *Hardware Installation Guide* (216382-C).

VPN Support

Nortel Switched Firewall 2.3.1 software is supported on the NSF 5124 and NSF 5124-NE1 hardware systems. For more information on the hardware and software features, see the *VPN Addendum for the Nortel Switched Firewall 2.3.1 User's Guide and Command Reference* (320752-A).

DHCP, Routing, and Bridging

- Supports either Layer 2 or Layer 3 firewall modes or both.
- Supports OSPF in a high availability configuration.

  NSF 2.3.1 supports both active-standby and active-active configurations.
- Supports OSPF across a GRE Tunnel.
- Supports BOOTP or DHCP relay agent.

  NSF 2.3.1 supports up to a maximum of 8 DHCP servers in high availability environments: active-standby and active-active configurations.

Reliability and Redundancy

- Radius Authentication and Auditing

  Radius Authentication is supported for managing user logins. NSF 2.3.1 supports
  - fallback to local authentication when the Radius server is not available.
  - auditing from the remote Radius Audit Servers.
  - Radius authentication in a standalone or cluster configuration.
  - multiple Radius servers can be configured for redundancy.
- Manages power supply by supporting APC Uninterruptible Power Supply (UPS) models

  UPS is supported through USB, Ethernet, 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 Check Point ISP Redundancy feature

  ISP Redundancy guarantees reliable Internet connectivity by allowing a single or clustered Switched Firewall to connect to the Internet through redundant Internet Service Provider (ISP) links.
- VRRP enhancements
  - Supports failover time to less than 1 second
  - SSI MIP does not migrate on failover
  - Supports the “preferred master” configuration
  - Access SSI management through VRRP interface

- Supports high availability in an OSPF network
- Access the firewall (Telnet or BBI) using the VRRP interface IP address

- Supports secure file transfer through SCP/SFTP

  SCP/SFTP uses a username and password for authentication.

- Collect log information from the root login using the `tsdump` command if the CLI commands are not accessible.

Management

- Supports Check Point User Authority feature

  The UserAuthority feature provides centralized management of user authentication and authorization.

- Supports SSI management traffic on VLAN

  NSF2.3.1 allows you to configure the SSI network on a VLAN, so you can share the management port for other interfaces.

- Supports SSI management traffic to bypass Check Point rules

  This bypass implementation prevents Check Point from blocking SSI traffic, so you do not have to create a separate policy on the Check Point management station to allow SSI traffic.

- Provides a hardware sensor module

  The sensor module is responsible for generating alarm events and SNMP traps when hardware parameters, such as the fan rpm values or temperature reach critical levels.

- Supports a user-friendly name for your firewall

Usability Enhancements

- Extended logging

  Description of syslog error messages is available immediately through the CLI (/maint/logdetail) and the BBI. The error messages displayed at the console have log IDs. A detailed description of these messages and possible work around can be found by entering the log IDs.

- Export the Check Point log files from the CLI and the BBI.

- Allows you to specify a user friendly name for the firewall from the CLI and the BBI. This name is displayed when you login.

- Support for cloning configurations through the CLI.

- Provides an easy and quick way to capture packets through the CLI using the new CLI commands, /info/fwmon and /info/ethereal.
- Display firewall capacity with the `/info/capacity` command.

  This command lists the ports supported, firewall memory, maximum connections, VLAN interface, routes supported, and disk capacity.
- New improved Browser-Based Interface (HTTP and HTTPS) offers easy configuration of network settings and displays dynamic status of the firewall. In addition, the configuration wizards provides step-by-step instructions to configure interfaces, bridge mode, Check Point Firewall, routes/gateways, DHCP, and OSPF.

  For more information, see the *NSF 2.3.1 Browser-Based Interface (BBI) Quick Access Guide* (216383-C).

Simplified Upgrade Procedure

NSF 2.3.1 supports a simplified upgrade process and you do not have to stop the traffic in the firewall. For step-by-step instructions, see "Upgrading to NSF 2.3.1 Software" on page 14.

Check Point Applications Supported

Nortel Switched Firewall 2.3.1 supports the following Check Point applications. To support these applications on the Nortel Switched Firewall 5100 Series hardware systems, you must configure NSF 2.3.1 and Check Point software:

- FireWall-1®
- ISP Redundancy
- User Authority®
- VPN-1®
- SmartDefense™
- NAT
- Authentication
- Content Security
- ClusterXL®
- Policy Server
- Floodgate-1®

- Management Tools
  - SmartView Monitor™
  - SmartCenter™ Server

  The following management tools do not need any configuration within the NSF 2.3.1 software; these tools are configured outside of the NSF 2.3.1 software:
  - SmartDashboard™
  - SmartView Tracker™
  - SmartView Status™

Upgrading to NSF 2.3.1 Software

To upgrade the software on your Nortel Switched Firewall, you must perform the following tasks:

1. **Backup of the Nortel Switched Firewall configuration.**

   You can use the backup to restore the configuration (clone) in case you have problems during upgrade. To back up, use the command

   - `/cfg/sys/backup` if you are running NSF 2.2.7.0
   - `/maint/backup` if you are running NSF 2.3.1

   For more information on backing up your configuration, see the *Nortel Switched Firewall 2.3.1 User's Guide and Command Reference* (213455-K).

2. **Download the new software upgrade package or install image.**

   Obtain the NSF5100_2.3.1.0_R55.pkg file and copy it to an FTP/TFTP/SCP/SFTP server or to a CDROM. The server must allow anonymous login.

   NOTE – Make certain that your FTP/TFTP/SCP/SFTP server is on a secure, trusted network. One way to ensure FTP security is to implement the server on the SmartCenter Server workstation.

3. **"Loading the New Software" on page 15**
4. **"Activating the Software" on page 17**

Loading the New Software

To install a minor or major release upgrade on your Nortel Switched Firewall, you need the following:

- Access to the CLI through the local console terminal or through a remote Telnet or SSH connection (using the Firewall host IP address).
- Verify that you have a rule on the Check Point management system that allows you to ping the FTP/TFTP/SCP/SFTP server and connect to it.
- The host name or IP address of the FTP/TFTP/SCP/SFTP server. If you choose to specify the host name, please note that the DNS parameters must be configured. For more information, see the "DNS Servers Menu" section in the Command Reference of the *Nortel Switched Firewall* 2.3.1 *User's Guide and Command Reference* (213455-K).

Access can be accomplished through the local serial port, or remote Telnet or SSH (Secure Shell) connection. Note, however, that Telnet and SSH connections are disabled by default, and if desired, must be manually configured after you have set up the firewall. For more information about enabling Telnet and SSH connections, see Chapter 10, "The Command Line Interface," in the *Nortel Switched Firewall 2.3.1 User's Guide and Command Reference* (213455-K).

Use the following procedure to load the software to your Switched Firewall:

1. **Log in into the firewall using the** `admin` **account and check the current version of the software as shown below.**

```
>> Main# /boot/software
------------------------------------------------------------
[Software Management Menu]
      cur         - Display current software status
      activate    - Select software version to run
      download    - Download a new software package via TFTP/FTP
      del         - Remove downloaded (unpacked) releases
>> Software Management# cur
Version              Name            Status
-------              ----            ------
2.2.7.0              tdo             permanent
```

2. **FTP or TFTP download: If you downloaded the upgrade image to the FTP/TFTP/SCP/SFTP server, do the following (only anonymous FTP is supported):**

```
>> Main# /boot/software/download                (FTP download)
Select tftp/ftp/scp/sftp [tftp]: ftp
Enter hostname or IP address of server: 172.17.124.46
Enter filename on server: NSF5100_2.3.1.0_R55.pkg
Received 53212760 bytes in 27.2 seconds
Unpacking...
ok
>> Software Management#
```

3. **CD-ROM download: If you downloaded the upgrade image to a CD-ROM, do the following:**

```
>> Main# /boot/software/cdrom                   (CD-ROM download)
Insert the installation CD-ROM.
press Enter when ready.
Found /mnt/cdrom/isd/images/NSF5100_2.3.1.0_R55.pkg
Software package imported successfully.
>> Software Management#
```

4. **After the download is complete, check the current versions of the software and make sure the version you downloaded has a status *unpacked*.**

```
>> Main# /boot/software/cur
Version              Name            Status
-------              ----            ------
2.3.1.0_R55          tdo             unpacked
2.2.7                tdo             permanent
```

The downloaded software upgrade package is indicated with the status `unpacked`. The software versions can be marked with one out of four possible status values. The meaning of each of these status values is as follows:

- **unpacked** means that the software upgrade package has been downloaded and automatically decompressed.
- **current** means that a software version marked as *old* or *unpacked* has been activated. As soon as the system has performed the necessary health checks, the *current* status changes to *permanent*.
- **permanent** means that the software is operational and will survive a reboot of the system.

- **old** means that the software version was permanent but is not currently operational.

  NSF 2.3.1 does not support downgrade from 2.3.1 to previous releases. You cannot "switch back" to the **old** version of the software.

Once the upgrade is loaded, the software must be activated as described in the following section.

Activating the Software

The Nortel Switched Firewall can hold up to two versions of the same major software release simultaneously (for example, version 2.2.7 and version 2.3.1). To view the current software status, use the `/boot/software/cur` command. When a new version of the software is downloaded to the Nortel Switched Firewall, the software package is decompressed automatically and marked as *unpacked*. After you *activate* the unpacked software version (which causes the Nortel Switched Firewall to reboot), the software version is marked as *permanent*. The software version previously marked as *permanent* will then be marked as *old*.

Refer to the one of the following two sections to upgrade your software:

- Standalone Upgrade
- "Cluster Upgrade" on page 18

Standalone Upgrade

When you have downloaded the software upgrade package, you can inspect its status and activate it using the following command:

1. **Inspect the status of the software package:**

```
>> Main# /boot/software/cur
```

2. **Activate the new (unpacked) software package:**

```
>> Main# /boot/software/activate 2.3.1.0_R55
Confirm action 'activate'? [y/n]: y
Activate ok, relogin
Restarting system.

login:
```

3. **Wait for the firewall to reboot.**

   As a result of running the `activate` command, the system reboots and you have to re-log in after the reboot. The reason for this is the CLI menus may be upgraded. Wait until the login prompt appears again, which may take up to two minutes while the system reboots.

4. **Wait for a 1-2 minutes for the firewall to initialize all system components.**

5. **After the firewall comes up, wait for a 2-3 minutes, then check the firewall status by running the /info/clu command to make sure the firewall is up.**

6. **Log in again and check the software status again:**

```
>> Main# /boot/software/cur
Version              Name            Status
-------              ----            ------
2.3.1.0_R55          tdo             permanent
2.2.7                tdo             old
```

   In this example, version 2.3.1 is now operational and will survive a reboot of the system, while the software version previously indicated as *permanent* is now marked as *old*.

7. **(Optional) From the Management Server, change the version of the Check Point™ Gateway Object.**

8. **If you are using centralized Check Point licenses, re-attach the licenses using SmartUpdate.**

9. **Push the Policy to the firewall.**

Cluster Upgrade

After you have downloaded the software upgrade package, you can inspect its status and activate it using the following commands:

1. **Determine which firewall holds the MIP (the firewall with the * in the MIP column).**

```
>> Main# /info/summary
IP addr          type    MIP Local cpu(%) mem(%)   op
10.10.1.193      master  *     *     26      42      up
10.10.1.194      master              26      42      up
```

2. **Log in into one of the firewalls with the MIP using the `admin` account.**

3. **Disable Check Point synchronization:**

```
>> Main# /cfg/fw/sync/dis
>> Main# apply
```

4. **Wait for 2-3 minutes for Check Point applications to re-initialize.**

5. **Verify that both firewalls are up and running with the /info/clu or info/sum commands.**

6. **Check if an access list entries are configured on the firewalls.**

   If access lists are configured for networks other than the SSI network, add a new access list entry for SSI network (it is mandatory for NSF 2.3.1.x upgrade process to have entries for the SSI network).

```
>> Main# /cfg/sys/accesslist/add <network address_for_SSI network>
```

7. **Check the current version of the software.**

   Verify that the version you downloaded has a status of unpacked.

```
>> Main# /boot/software/cur
Version              Name            Status
-------              ----            ------
2.3.1.0_R55          tdo             unpacked
2.2.7                tdo             permanent
```

8. **Activate the new (unpacked) version software and do not disturb the system until it reboots:**

```
>> Main# /boot/software
>> Software Management# activate 2.3.1.0_R55
Confirm action 'activate'? [y/n]: y
Activate ok, relogin
Restarting system.
```

   Both the directors reboot. After two to three minutes, the status of the new software version changes from *unpacked* to *permanent*, and the older version changes from *permanent* to *old*:

```
>> Software Management# cur
Version            Name                    Status
-------            ----                    ------
2.3.1.0            tdo                     permanent
2.2.7              tdo                     old
```

9. **Wait for a 1-2 minutes for the firewalls to initialize all system components.**

10. **(Optional) From the Management Server, change the version of the Check Point Cluster Object.**

11. **If you are using centralized Check Point license, re-attach the licenses using Smart-Update.**

12. **Push the Policy to both the firewalls and make sure both firewalls are UP in the** `/info/summary` **menu.**

13. **Enable Check Point synchronization and verify operation.**

```
>> Main# /cfg/fw/sync/ena
Current value: n
Enabling sync may reboot all Firewall Hosts when you apply.
Are you sure (y|n)? y
>> Main# apply
```

14. **Both the firewalls reboot to update the Check Point configuration.**

15. **After both the firewalls come up, wait for a 2-3 minutes.**

    It takes a longer time for NSF 2.3.1 version to come up because of the various Check Point packages being installed.

16. **Verify that the firewalls are operational.**

    Use the `/info/clu` command to check the firewall status under the "CP FW" column. Both firewalls show the total running time in hours, minutes, and seconds (Xh:Ym:Zs).

17. **Verify VRRP status:**

    - High Availability (active-standby)

```
>> Main# /info/net/vrrp/status
Host 10.10.1.193
         VRRP Backup
Host 10.10.1.194
         VRRP Master
```

- Active-Active

```
>> Main# /info/net/vrrp/status
Host 10.10.1.193
>
> Group1  VRRP Master
>         20.20.20.1
>         30.30.30.1
> Group2  VRRP Backup
>         20.20.20.2
>         30.30.30.2
> Host 10.10.1.194

> Group2  VRRP Master
>         20.20.20.2
>         30.30.30.2
> Group1  VRRP Backup
>         20.20.20.1
>         30.30.30.1
```

18. **When the reboot is complete, log in as admin and verify that sync is working properly by entering `/maint/fw/sync` command.**

    Both firewalls should be active.

19. **Verify that data traffic is forwarding properly by watching the Check Point logs using SmartView Tracker on the Check Point SMART Client.**

    Table 2 shows the time it takes to complete an upgrade procedure.

Table 2 Upgrade Time in Minutes

Platform	Download time in minutes	Activate and Reboot time in minutes	Total time in minutes
5106	5	10	15
5111-NE1 and 5109	2	4	6
5114-NE1 and 5114	2	4	6
5124-NE1 and 5124	2	4	6

Reinstalling the NSF 2.3.1 Software

To reinstall software on the firewall, you must connect directly to the firewall serial port and log in as the `boot` or `root` user. When the reinstallation is performed, the new firewall is reset to its factory default configuration. All previous configuration data and software is erased, including old software image versions or upgrade packages.

There are two methods of reinstalling software on the firewall.

- Using the .iso image of the software

  Nortel Networks recommends this method which copies the .iso version of the software on a CD-ROM and boots from it. This reinstall removes the current configuration and reimages the firewall. This type of reinstall is done by logging in as root user.

- Using the .img image of the software

  This method installs the .img version of the software using TFTP or FTP. This reinstall overwrites the current configuration. This type of reinstall is done by logging in as boot or root user.

For more information on these two methods, see the *Nortel Switched Firewall 2.3.1 User's Guide and Command Reference* (213455-K).