RELEASE NOTES:

Alteon Firewall 5100 Series™

Release 2.2.2

Part Number: 213456-G, June 2003

NORTEL NETWORKS™

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

Release Notes

These release notes provide the latest information regarding the Alteon Firewall 5100 Series (models ASF 5105, ASF 5109, ASF 5112, and ASF 5114) for Release 2.2.2. This supplement modifies information found in the complete documentation. Please keep this information with your Nortel Networks product manuals.

Late-Breaking News and Support

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. In particular, the readme.txt file collocated with the software may contain valuable information that was not available at the time these release notes were published. To access the Web site:

- Point your browser to: http://www.nortelnetworks.com/cs.
- 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.
- Once you have signed in, go to the Software page for the Alteon Firewall by selecting:

  Alteon ▸ Alteon Switched Firewall System (Software).
- Click on "Software Type" in the list header to sort the Software page by type. Alteon Firewall software is type "AF."
- Follow the "Software Download Procedure" on page 20 to download the present software release, patch release software (if it exists) and readme.txt file.

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.

Documentation

These *Release Notes* (Part No. 213456-G) are posted along with the *Alteon Firewall 5100 Series Installation and User's Guide* (Part No. 213455-F) at the Nortel Customer Support Web site. Navigate to the site according to the instructions under "Late-Breaking News and Support" on page 3, log in, and select:

Alteon ▸ Alteon Switched Firewall System (Documentation)

Then select the document you are interested in and open it. You must have Adobe Acrobat Reader running on your system to open the guide in your browser. (Adobe Acrobat Reader is available for free at www.adobe.com.) Once you have opened the document in your browser, you can save it to your system by pressing the micro floppy disk icon on the Acrobat Reader menu bar (below your browser tool bars).

CheckPoint Product Name Changes

For FP-3 and later feature packs, Check Point changed the names of some of their products that are referenced in the Alteon Firewall 5100 system. These names have been changed, where applicable, in the Alteon Firewall 5100 Series Installation and User's Guide, the Command Line Interface (CLI) and the Browser-Based Interface (BBI). A table of name changes is provided here:

Table 1 Check Point Product Name Changes for FP-3 and later

Current Name	Name Prior to NG FP-3
SmartDashboard	Policy Editor
SmartView Tracker	Log Manager or Log Viewer
SmartView Status	Status Manager or System Status
SmartView Monitor	Real-Time Monitor or Traffic Monitor
Smart Center Server	Management Server
SMART Clients	Management Clients
SmartUpdate (see note below)	SecureUpdate

NOTE – SmartUpdate/SecureUpdate is not supported by the Alteon Firewall for installing patches. You must use the Alteon Firewall software releases.

New Features for Release 2.2.2

CheckPoint has released FireWall-1 NG *Application Intelligence*, a feature pack upgrade that succeeds FireWall-1 NG FP-3. Alteon Firewall Release 2.2.2 is an upgrade of Release 2.2.1 (also referenced as Release 2.2) that supports the Application Intelligence feature pack.

NOTE – Release 2.2.2 does not support FP-3. The latest version of the Alteon Firewall 5100 Series software that supports FP-3 is Release 2.2.1.

Application Intelligence has functions that allow the CheckPoint FireWall-1 NG system to detect intrusions at the application layer. For more information, go to www.checkpoint.com and view CheckPoint's Application Intelligence literature.

No new features for the Alteon Firewall 5100 series were added for Release 2.2.2. The *Alteon Firewall 5100 Series Installation and User's Guide* (Part No. 213455-F), which was updated for Release 2.2.1, applies to Release 2.2.2 as well.

Below are listed the features that are new for Release 2.2.2 (reprinted from the Release Notes for Release 2.2.1).

ASF 5114

Support for the model ASF 5114 has been added to the Alteon Firewall 5100 Series. The ASF 5114 has two Gigabit copper Ethernet ports and a dual-port multimode Gigabit fiber Network Interface Card (NIC).

The hardware and performance features are stated below:

Characteristic	ASF 5114
Network Interface Ports	Two 10/100/1000 Mbps copper Gigabit Ethernet ports Two 1000-SX multimode fiber Gigabit Ethernet Ports
Processor Speed	2.4 GHz
RAM	1 GB
Chassis	1U, 19-inch rack-mount
Throughput	1,600 Mbps
Concurrent Sessions	500,000
New Connections Per Second	5,500

Proxy ARP

Proxy ARP has been implemented at the CLI and on the BBI. With the addition of this capability, it is no longer necessary to setup Proxy ARP for the cluster using OS level commands as in previous releases of the Alteon Firewall software. For command and status information see "New CLI and BBI Commands" on page 6.

Open Shortest Path First (OSPF)

Support for the OSPF routing protocol has been added to the Alteon Firewall software. This implementation conforms to the OSPF version 2 specifications detailed in Internet RFC 1583. An entire chapter on OSPF has been added to the *Alteon Firewall 5100 Series Installation and User's Guide*. Included are an overview of the OSPF concepts, specific details on the OSPF implementation, and topological examples accompanied by configuration samples. For command and status information see "New CLI and BBI Commands" on page 6.

New CLI and BBI Commands

NOTE – For complete descriptions, see the *Alteon Firewall 5100 Series Installation and User's Guide*.

Proxy ARP

CLI commands for Proxy ARP

`/cfg/net/parp` opens the Proxy ARP Menu.

```
[Proxy Arp Menu]
      list        - Proxy ARP List Menu
      enable      - Set Proxy ARP enable/disable
      cur         - Display current settings
```

`/cfg/net/parp/list` opens the Proxy ARP List Menu:

```
[Proxy ARP List Menu]
      list        - List all values
      del         - Delete a value by number
      add         - Add a new value
```

Once you have enabled Proxy ARP for the cluster and have added IP address(es) to the Proxy ARP list, you must open the Check Point SmartDashboard and add Network Address Translation (NAT) rules and security policies to allow the cluster to proxy ARP for specified IP addresses. For more information, see the Proxy Arp Menu and Proxy Arp List Menu descriptions in the *Alteon Firewall 5100 Series Installation and User's Guide*.

BBI Commands for Proxy ARP

The same Proxy ARP status and configuration controls that are accessible at the CLI are also accessible from the BBI by selecting:

Network ▸ Routes ▸ Proxy ARP

OSPF

CLI commands for OSPF

Commands for configuring OSPF and accessing OSPF status information are accessible from the OSPF menus below. For detailed information on using options presented here, start at the OSPF Menu description in the *Alteon Firewall 5100 Series Installation and User's Guide*. For an overview of OSPF and topological examples see Chapter 9, "Open Shortest Path First."

`/cfg/net/adv/route/ospf` opens the OSPF Menu:

```
[OSPF Menu]
      aindex      - OSPF Area (index) Menu
      if          - OSPF Interface Menu
      redist      - Route Redistribute Menu
      rtrid       - Set OSPF router ID
      spf         - Set time interval between two SPF calculations
      ena         - Enable OSPF
      dis         - Disable OSPF
      cur         - Display current settings
```

`/cfg/net/adv/route/ospf/aindex` <*area index #*> opens the OSPF Area Index Menu:

```
[OSPF Area Index 1 Menu]
      id          - Set area ID
      type        - Set area type
      ena         - Enable area
      dis         - Disable area
      del         - Remove OSPF Area Index
      cur         - Display current settings
```

`/cfg/net/adv/route/ospf/if` <*if#*> opens the OSPF Interface # Menu:

```
[OSPF Interface 1 Menu]
      aindex     - Set area index
      prio       - Set interface router priority
      cost       - Set interface cost
      hello      - Set hello interval in seconds
      dead       - Set dead interval in seconds
      trans      - Set transmit delay in seconds
      retra      - Set retransmit delay in seconds
      auth       - Set authentication type
      key        - Set password authentication key
      md5key     - Set MD5 authentication key
      ena        - Enable interface
      dis        - Disable interface
      cur        - Display current settings
```

`/cfg/net/adv/route/ospf/redist` opens the Route Redistribution Menu:

```
[Route Redistribution Menu]
      connected  - Connected Route Redistribution Menu
      static     - Static Route Redistribution Menu
      defaultgw  - Default Gateway Redistribution Menu
      cur        - Display current settings
```

`/info/net/route/ospf` opens the OSPF Router Information Menu:

```
[OSPF Router Information Menu]
      routes     - Display routes learned from OSPF
      lsa        - Display OSPF LSA information
      neigh      - Display OSPF neighbor information
      if         - Display OSPF interface information
      fib        - Display OSPF router FIB
      ospf       - Show OSPF configuration
```

BBI Commands for OSPF

The same OSPF status and configuration controls that are accessible from the CLI are also accessible from the BBI by selecting:

Network ▸ Routes ▸ OSPF

Other New Commands

The menus and commands below have added to Alteon Firewall software for this release. For more information, you can find their descriptions in Chapter 6, “Command Reference,” of the *Alteon Firewall 5100 Series Installation and User’s Guide.*

- `/info/summary` displays the operational status for iSD hosts in the cluster.

  You can find the same information in the BBI by selecting:

  Monitor ▸ Hosts

- `/info/host` opens the Info_host Menu:

```
[info_host Menu]
      status      - Show runtime information
      link        - Show physical ports link status
      ether       - Show ethernet stats
      syslog      - Show syslog entries
```

  You can find status and syslog information in the BBI by selecting:

  Monitor ▸ Hosts and Monitor ▸ Syslog

- `/info/net` opens the Info_net Menu:

```
[info_net Menu]
      if          - Show interface details
      route       - Show route configuration
      vrrp        - Show vrrp details
```

  You can find the same information in the BBI by selecting:

  Network ▸ Interfaces, Network ▸ Routes, or Network ▸ VRRP

- `/maint` opens an upgraded Maintenance Menu:

```
[Maintenance Menu]
      diag        - Diagnostic Tools Menu
      tsdump      - Tech Support Dump Menu
      ospf        - OSPF Debug Menu
```

  - `diag` opens the (unchanged) Firewall Maintenance Menu.

- `tsdump` opens the Tech Support Menu:

```
[Tech Support Menu]
      dump        - Create a tech support dump
      exdump      - Create a tech support dump including logs
      ftp         - FTP tech support dump to an FTP server
      floppy      - Copy Tech Support Dump to Floppy
      cur         - Current Tech Support Information
```

- `ospf` opens the OSPF Debug Menu:

```
[OSPF Debug Menu]
      events      - Set log OSPF generic events
      ism         - Set log OSPF ISM events
      lsa         - Set log OSPF LSA events
      nsm         - Set log OSPF NSM events
      packets     - Set log OSPF packets
      msgs        - View last 100 debug messages
      cur         - Display current settings
```

- `/cfg/misc` opens the Miscellaneous Settings Menu:

```
[Miscellaneous Settings Menu]
      warn        - Set Enable Warnings When Apply Configuration
      cur         - Display current settings
```

The `warn` command turns warning messages on or off. When enabled (default), whenever the global `apply` command is issued, applicable warning messages are displayed if problems are found in the pending configuration changes. Warnings will not cause the apply command to fail, but can be helpful for managing configuration issues.

You can display and control in the BBI by selecting:

Cluster ▸ Miscellaneous

Clarifications

Check Point High Availability and VRRP

Check Point High Availability (CPHA) and Alteon Firewall VRRP are separate implementations of the same feature. CPHA requires a license and supports both load-balancing and failover. Alteon Firewall VRRP does not require a license and only supports failover.

To run Alteon Firewall VRRP, it is not necessary to configure CPHA on the Check Point Management station. To run CPHA, an Alteon Firewall VRRP configuration is required.

OpenSSL

This release includes OpenSSL 0.9.6.g with buffer overflow patches.

Known Issues

Check Point FireWall-1 NG Application Intelligence Issues

- All Check Point licenses and firewall policies are bound to the Alteon Firewall's host IP address. Changing the host IP may lead the Alteon Firewall to fail. To prevent this, reconfigure Check Point licenses and firewall policies for the new host IP address.
- If you have the Application Intelligence management station on Win NT, right-clicking on a "User" object in the SmartDashboard may cause the SmartDashboard to freeze. If this happens, kill the SmartDashboard and re-launch it. To edit the user object, use the menu item "Manage | Users and Administrators..."
- The Application Intelligence feature pack loads the default filter first and then the initial filter. It is normal to see a default filter for a while.
- Check Point FireWall-1 NG Application Intelligence is part of the Alteon Firewall 2.2.2 code release. You can review the latest Check Point features at the Check Point Web site:
  - Point your browser to http://www.checkpoint.com/techsupport/installation/ng/release_notes.html.
  - Then select NG with Application Intelligence Suite Release Notes.pdf.

You must first sign in using the username and password that were assigned to you by Check Point. To obtain a username and password, go to: http://www.checkpoint.com/techsupport/contacts.html and follow the instructions provided there.

- For upgraded documentation go to: http://www.checkpoint.com/support/technical/documents/index.html (username and password are required).

CLI Issues

- After configuring the Alteon Firewall for the first time, reboot the unit using the `/boot/reboot` command.
- When logging into the CLI while the Alteon Firewall is processing heavy traffic, the CLI may display the message, "`iSD initialized`." You may safely ignore this message.
- In indexed list items such as static routes, NTP servers, only one item can be deleted at a time. After you delete the first item, all remaining items in the list are renumbered.
- When swapping port configurations (i.e. between the host IP and interface IP) an error will occur stating an invalid configuration (CR Q00511648). In that case, disable the interfaces, apply the new configuration, re-enable the interfaces, and apply the final configuration.
- To check the version of Check Point running on the Firewall, login as root and run the `fw ver` command or launch the BBI and select Monitor ▸ About.
- When changing the date on the Firewall, it is highly recommended that the unit be rebooted (CR Q00527847).
- Changes to the host IP address and network mask do not show up in the `diff` command (CR Q00522847).
- Under high traffic load, logging into the CLI may be slow. In that case, try BBI access, which will be comparatively faster (CR Q00572082).

Browser-Based Interface (BBI) Issues

- When using Check Point User Authentication and the BBI, the user may not be able to access the page on the first attempt. If so, simply refresh the browser.
- When generating a private key, it will be lost upon logout. Use the CLI to generate the private key (CR Q00540734).
- Changing the management port from the BBI causes SSI to go out of sync (CR Q00622507).
- The Alteon Firewall may not automatically start after a fresh install (CR Q00662056).

  Workaround: Reboot.

SmartCenter Server Issues

- `/boot/delete` is not supported when the SmartCenter Server is installed on the iSD host (CR Q00563930).

  This means you can not remove the Check Point SmartCenter Server from the Firewall using the `/boot/delete` command. To uninstall the Check Point SmartCenter Server from the Firewall, you must re-install the entire Firewall OS software package from the Alteon Firewall 5100 series Software CD. For more information, see "Installing a New Image From CD-ROM" in the Alteon Firewall 5100 Series Installation and User's Guide.

Gigabit Port Issues

- Even if VLAN tagging is not enabled, the copper gigabit Ethernet ports will accept and respond to VLAN tagged packets (CR Q00585995).
- If a copper gigabit port is connected to fast Ethernet port the link light on the appliance will not light up. The `/info/host/link` command will show the actual status of the port (CR Q00585993).

Rebooting Issues

The Alteon Firewall must be rebooted under the following scenarios:

- after enabling HA
- after performing `/boot/delete`
- after performing `/cfg/gtcfg` (CR Q00594626)
- after changing VLAN tagging options
- after changing the time by more than a minute

Secure Internal Communication (SIC) Issues

- When the SIC is reset, the existing firewall policy may be reset to the default, which denies all filters (CR Q00494416). In that case, a new policy must be pushed from the SMART Client. The default policy can be unloaded using the CLI command:

  `/maint/diag/fw/unldplcy`

  Then the policy can be pushed.

- After a SIC reset in a cluster configuration, `/maint/diag/fw/unldplcy` must be performed on each Firewall (CR Q00585706).

- When performing SIC reset in a cluster, the warning message can be safely ignored (CR Q00585705).

VRRP Issues

- ASF 5105: Sometimes loads the default filter after `/cfg/fw/sync` ena/dis (CR Q00622591).
- ASF 5105: Join command does not work after `/boot/delete` of redundant Firewall. (CR Q00630170).

  Workaround: `/maint/diag/fw/unldplcy` followed by `/maint/diag/fw/ldplcy` which disrupts traffic.
- ASF 5105: VRRP will stop working if two VRRP ports and the management station are on the same L2 switch (CR Q00628167).

  Workaround: Put the management station on a different network from the VRRP network.
- ASF 5105: Interface links toggle up/down during failover (CR Q00624314).

  Workaround: This was only seen once and can not be reproduced.
- There are problems changing the IP address of the backup master from the active master (CR Q00626424).
- Changing ip1 or ip2 address in a High Availability setup does not get updated immediately (CR Q00633915).

  Workaround: Disable and enable the interface (see `/cfg/net/if #`).
- Moving from High Availability setup to a non-High Availability setup fails to configure the IP address properly (CR Q00633865).

  Workaround: Disable and enable the interface (see `/cfg/net/if #`) or reboot.
- Deleting Firewall #2 from a VRRP configuration does not show up in status query (CR Q00630904).
- You must add a rule to allow multicast advertisement messages between redundant Alteon Firewalls configured for VRRP.
- The master should have an operational firewall (valid license, policy for cluster traffic) at the time of joining the second member.

- Both masters should be connected to the same device.

NOTE – Using two linked hubs (one connected to each master) is not recommended because a link failure between the hubs can cause both Firewalls to become active.

- During VRRP configuration, if the default filter (deny all) is installed, unload the firewall rules using `/maint/diag/fw/unldplcy`.
- After using the join command to add a second member to the cluster, the firewall may take up to five minutes to restart.
- In heavy traffic conditions, VRRP advertisements may not reach the backup host. It is recommended to modify the VRRP advertisement interval, the `garp` delay, and `garp` broadcast interval to suit your traffic load.
- The advertisement interval (`adint`) range that is given at the CLI is 3-3600 seconds. In fact, the CLI will accept and apply a value as low as 1, but 3 is the lowest recommended value.
- The backup waits (adint value * 3) seconds before ARPing the virtual IP for 4 seconds. If there is no response, it backs up the failed master.
- Upon applying any new configuration in which the network interfaces, VRRP, VLAN tagging or port information has changed, the VRRP master/backup status will change (CR Q00581671).
- When a user tries to get authenticated by the firewall manually using the VIP, the connection will be rejected. The workaround is to add VIP to topology and push a policy (CR Q00589638).
- Do not enable sync while traffic is running (CR Q00577976).
- When enabling or disabling a default gateway in a cluster, the CLI appears to hang for a minute or two (CR Q00573511).
- Both cluster members can become MIP (Management IP Address) owner if they can't communicate on the host port (e.g. unplugging links on the host port). If configuration changes were made during the time appliances were partitioned, then after connectivity is re-established, only changes made to elected MIP owner will be kept as active configuration (CR Q00593966).
- VRRP clusters only support two members even though extra members are able to join the cluster (CR Q00594629).
- For Radius authentication support in high availability configurations, you should not configure Virtual Interface Address in the Radius server. Instead configure both the interface addresses of the appliance in the Radius server (CR Q00576341).

- It is recommended to use the `/cfg/sys/cluster/host #/delete` command to delete the appliance from the cluster. If the `/boot/delete` command is used instead, then appliance will be re-initialized but host, Check Point Sync, and VRRP information will still stay in cluster configuration (CR Q00594882 and Q00594876).
- If user authentication is enabled, ftp throughput can decrease after a VRRP failover (CR Q00589609).

VLAN Tag Issues

- IP address change does not update for non-MIP holding iSD host on a vlan tagged interface (CR Q00628247).

  Workaround: Reboot the Firewall.

OSPF Issues

- Deleted interfaces are still being advertised by OSPF (CR Q00655920).

  Workaround: Issue the following command from the root login: `service zebra restart`.
- When enabling OSPF authentication, the authentication key should not have spaces, although the CLI will allow the operation (CR Q00673729).

General Issues

- You can configure licenses using the CLI or BBI. You can also install licenses from the Check Point Management station using Check Point Central Licensing. However, licenses installed through the Check Point Management station will not be displayed at the CLI or BBI.
- Firewall licenses that were not added using the `/cfg/pnp/add` command may be deleted after an upgrade or reboot. The workaround is to manage licenses only using `/cfg/pnp` menu.
- Evaluation licenses must be entered using the Check Point SmartUpdate (CR Q00660409).
- `/boot/delete` is the correct command for changing the host IP address of any Alteon Firewall if the new IP address is not in the same subnet as the old IP address. For instance if the current host IP address is 10.10.1.1 and the new IP address is 47.80.18.5, `/boot/delete` must be performed. Changing 10.10.1.1 to 10.10.1.5 can be done from `/cfg/sys/cluster/host x/ip` (this applies in the single box case also).

- Nortel Networks recommends using Gigabit Ethernet ports (ASF 5109 and ASF 5112) for data traffic.
- There may be a time difference reported in healthcheck for each node. The local host will have latest healthreport.
- When there are problems pushing a policy to the cluster, push the policy to each individual firewall, then the cluster itself.
- When there is a warning for disk usage in syslog, free space must be created in the log partition.
- STP should be disabled on switch ports that are connected to the firewall.
- Logs are not generated when using Check Point's User Authentication with a location restriction (CR Q00514088).
- The command `/info/host/ethernet` displays the statistics for untagged ports. Statistics for tagged ports are not supported in this release, only partial statistics for tagged ports will be +displayed with this command (CR Q00592928).
- The SNMP trap asfAcceleratorAddedTrap-0.5 can be safely ignored (CR Q00594875).
- The host port and subnet of the appliance is restricted for cluster and Check Point Sync communication (CR Q00593812).
- The user may safely ignore duplicate error messages when an invalid configuration is applied (CR Q00580877).
- Sometimes the message:

  ```
  fwlddist_adjust buf: record too big for sync messages
  ```

  or

  ```
  Checking 386/387 coupling...OK, FPU using exception 16
  ```

  will appear in the logs (CR Q00494127/Q00530029). These are harmless errors that can be ignored safely.
- Sometimes `enabling/disabling SSH/telnet` does not seem to take effect. The workaround is to disable/enable it, apply, then enable/disable, and apply (CR Q00608258).
- The Alteon Firewall cannot synchronize time with an NTP server that is not part of the cluster (CR Q00596627).
- When using `/cfg/gtcfg` with a configuration with ELA enabled, you must pull the certificate (`/cfg/sys/log/ela/pull`) and push the policy again (CR Q00608447).
- During re-imaging, error messages such as “lilo, locating tarballs, modprob” are displayed at the local terminal (CR Q00631869).

  Workaround: Ignore error messages. They are for system level debugging and are harmless.

Upgrading Software

The Alteon Firewall provides a variety of ways to upgrade your software. Before you begin downloading software, consider the following information.

Alteon Firewall Upgrade Matrix

- Upgrading Release 1.x to Release 2.x using a ftp/tftp server is not supported on any platform (see "Upgrading from Release 1.1.2 or 1.1.3" on page 19 for an upgrade workaround).
- Upgrading Release 2.1.x is supported on all platforms.

Alteon Firewall Software Upgrade/Reinstall Options

There are three image versions of Alteon Firewall software; .iso, .img, and .pkg:

- The .iso image is for creating the Alteon Firewall software CD. You must download the .iso image to a server that your CD-ROM burner has access to.
- Both the .img image and the .pkg image are installed from an ftp or tftp server using the /boot/software/download command. The .img image overwrites the current software version, while the.pkg image installs it in parallel with the existing version. You can activate .pkg image at your convenience using the `/boot/software/activate` command.

NOTE – For .iso and .img installations, all configuration parameters, logs, etc. are lost. Be sure to save your configuration to an ftp or tftp server using the `/cfg/ptcfg` command and restore it after reinstallation using the `/cfg/gtcfg` command.

NOTE – For complete installation instructions, see the readme.txt file that is collocated with the software (see "Software Download Procedure" on page 20 for Web-site navigation instructions).

Upgrading from Release 1.1.2 or 1.1.3

You must install an .iso image from a CD-ROM to upgrade from 1.x to 2.x. Follow the instructions below to download and install the image

Downloading Release 2.2.2

1. **Point your browser to Alteon Switched Firewall System Downloads page (see "Software Download Procedure" on page 20 for instructions).**
2. **Select the Alteon Firewall 2.2.x image file (.iso).**
3. **Copy the file to your ftp/tftp server.**

Installing Release 2.2.2

NOTE – Be sure to save your configuration to your ftp/tftp server before installing Release 2.2.2 (see the Firewall CLI commands /cfg/ptcfg and /cfg/gtcfg). Configuration parameters are lost when you install an ISO image.

---

1. **Put a blank CD in your CD-ROM burner, select the "File/Burn Image" option (or equivalent), and burn the Release 2.2.x image onto the blank CD.**
2. **Install the CD in the Alteon Firewall CD-ROM drive.**
3. **Reboot the Alteon Firewall.**
4. **Login as root (no password is necessary).**
5. **Issue the command: install-asf** <*model #*> (enter **asf5105** or **asf5109** or **asf5112** or **asf5114**, whichever matches your model #).

   Wait for the installation script to finish. If the Alteon Firewall does not reboot automatically, take the software CD out and reboot the system manually.
6. **Login as admin. The installation is complete.**
7. **Restore the configuration from the ftp/tftp server using the `/cfg/gtcfg` command.**

   This is required to apply the restored configuration.

Software Download Procedure

Downloading Alteon Firewall software includes a lengthy Web navigation process. Step 1 starts at the Nortel Networks Customer Support Web site (www.nortelnetworks.com/cs). Each associated Action takes you to the next Step/Web Page or Dialog Box in the procedure.

Note: You must have a username and password assigned by Check Point for Step 5 and beyond. If you do not, follow the links in the note on that Web page (Software Subscription Download Section) to obtain them.

Step	Web Page or Dialog Box	Action
1	Nortel Networks Customer Support	Select **Alteon**
2	Products By Product Family	Select **Alteon Switched Firewall System** (**Software**)
3	Alteon Switched Firewall Software	Sort By Type **AF** (Alteon Firewall) Select title of latest **AF** release
4	Software Detail Information	Select **www.Checkpoint.com**
5	Software Subscription Download Section	Enter username and password assigned by Check Point
6	Software Subscription Download Agreement	Select **Accept**
7	Downloads	Select product from drop-down box: **Nortel Alteon Switched Firewall** Then select **Go**
8	Downloads Nortel Alteon Switched Firewall	Select version from drop-down box: **NG for Alteon Firewall (5100 series)** Then select **Go**
9	Downloads Nortel Alteon Switched Firewall NG for Alteon Firewall (5100 series)	Select levels from the three drop-down boxes: Operating System: **Nortel OS** Encryption: **Any** SP Patch Level: **Application Intelligence - ASF 2.x.x.x** Then select **Go**
10	Downloads Nortel Alteon Switched Firewall NG for Alteon Firewall (5100 series) (Nortel OS Any Application Intelligence - ASF 2.x.x.x)	Select Download Option(s) CD Image (.iso) for burning a CD image Boot Image (.img) for reinstall via ftp/tftp Upgrade (.pkg) for upgrade via ftp/tftp
11	File Download Dialog Box	Select **Save**
12	Save As Dialog Box	Enter directory path, then select **Save**
13	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	