Release Notes:

Alteon Firewall 5100 Series™

Release 2.0

Part Number: 213456-D, February 2003

NORTEL NETWORKS™

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

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.

Release Notes

These release notes provide the latest information regarding your Alteon Firewall 5100 series (model ASF 5105, ASF 5109, or ASF 5112), version 2.0 and higher. This supplement modifies information found in the complete documentation. Please keep this information with your Nortel Networks product manuals.

Documentation on CD-ROM

The *Alteon Firewall 5100 Series Installation and User's Guide* (part number 213455-D) is supplied on a CD-ROM included with this product. The manual is a PDF file that can be read and printed using the free Acrobat Reader software available from Adobe Systems Incorporated (http://www.adobe.com).

To access the manual, open the "`welcome.pdf`" file on the *Alteon Firewall 5100 series Documentation* CD-ROM. When the manual opens, you can navigate through the book by selecting the bookmarks on the right side of the window, and by scrolling through the pages.

NOTE – To obtain a manual in hardcopy, read the flyer that ships with the Documentation CD.

Late-Breaking News and Support

Check the Nortel Networks Web site for the product information on the Alteon Firewall and other products.

Web access: http://www.nortelnetworks.com

This Web site provides access to software updates, release notes, readme files that accompany the code release (and which may contain important release information that was not included in the release notes), technical bulletins, and white papers. The Web site also provides access to Nortel Networks customer support for accounts under warranty or that are covered by a maintenance contract.

New Features for Release 2.0

ASF 5109

The model ASF 5109 has been added to the Alteon Firewall 5100 Series. The ASF 5109 has two more Fast Ethernet ports than the ASF 5105 or the ASF 5112 that you may use for any purpose (for additional DMZ support, for instance).

The hardware and performance features are stated below:

Characteristic	ASF 5109
Network Interface Ports	Two 10/100/1000 Base-T copper Gigabit Ethernet ports Four 10/100 Base-T Fast Ethernet Ports
Processor Speed	2.4 GHz
RAM	512 MB
Chassis	1U, 19-inch rack-mount
Throughput	1000 Mbps
Concurrent Sessions	250,000
New Connections Per Second	5,500

Virtual Router Redundancy Protocol (VRRP)

VRRP was implemented on the Alteon Firewall to allow for high-availability failover when a redundant Alteon Firewall host is present in a cluster (see Alteon Firewall Clustering). The VRRP Interface Menu (for configuring the *virtual router*) and the VRRP Settings Menu (for enabling high-availability failover and configuring VRRP features) were added to the CLI (see "New CLI Commands" on page 5 for command descriptions).

Alteon Firewall Clustering

Release 2.0 supports clustering of Alteon Firewalls for failover (but not for Firewall load-balancing). Only two Alteon Firewalls may be in a cluster. To form the cluster, you must use the `join` command (which is supported for release 2.0) during initial configuration of the second Alteon Firewall. The Management Interface IP address (MIP) identifies the cluster, so the MIP must be the same for both units. For high-availability failover configuration, see Virtual Router Redundancy Protocol (VRRP).

Stateful Failover

Stateful failover of open sessions during a failover event is supported in release 2.0. See a description of the applicable CLI commands in "Synchronization" on page 6. See "Configure State Synchronization using the Check Point Policy Editor" on page 235, in the *Alteon Firewall Installation and User's Guide* for a representative configuration.

VLAN Tags

The Alteon Firewall will now forward VLAN tagged packets to devices on Alteon Firewall interfaces with matching VLAN IDs. The `/cfg/net/if` <if number>`/vlanid` command was added to the CLI to allow you to enter a VLAN ID for that interface (see "New CLI Commands" on page 5 for command descriptions). VLAN tagging is also configurable at the BBI. See "VLAN Tags" on page 236, in the *Alteon Firewall Installation and User's Guide* for a representative configuration.

New CLI Commands

New commands for release 2.0. For complete descriptions, see the Alteon Firewall User's Guide for release 2.0 (part number 213455-D).

VLAN Tagging

The VLAN tagging feature allows Alteon Firewalls to forward tagged packets to the appropriate VLANs.

`/cfg/net/if` ***<if number>*****`/vlanid`** ***<ID number (0-4094)>*** allows you to set the VLAN ID for the specified interface.

VRRP

Virtual Router Redundancy Protocol (VRRP) and the addition of a redundant Alteon Firewall to the cluster make it possible to configure an high-availability network that reduces the chance that a single point of failure can bring down the system.

`/cfg/net/if` ***<if number>*****`/vrrp`** accesses the VRRP Interface Menu. The options are:

- □ **`vrid`** ***<ID number*** **(*1-255*)>** for setting the unique ID for the *virtual router*
- □ **`ip1`** ***<IP address>*** for setting the IP address for the preferred master interface
- □ **`ip2`** ***<IP address>*** for setting the IP address for the backup interface

- □ **cur** for viewing the VRRP settings for the specified interface

/cfg/net/vrrp accesses the VRRP Settings Menu. The options are:

- □ **ha y|n** for enabling/disabling high-availability failover on the specified interface
- □ **master 1|2** for setting the preferred master (1 = iSD host 1, 2 = iSD host 2)
- □ **adint 3-3600** for setting the interval in seconds between multicast advertisement messages sent by the active Alteon Firewall to the backup Alteon Firewall
- □ **garp 1-600** for setting the Gratuitous ARP (garp) message delay, which determines how long the newly active Alteon Firewall waits (after a failover) before sending a gbcast messages to the end-hosts connected to the virtual router.
- □ **gbcast 2-100** for setting the interval between the interval between GARP messages that are sent by the active master to ensure that end-hosts on the virtual router interface have the correct MAC address/IP address mapping.
  The gratuitous broadcast (gbcast) value is multiplied by the `/cfg/net/vrrp/adint` value to determine the interval in seconds between GARP messages. For example, if your adint value is 10 and your gbcast value is 3, the interval between GARP messages will be 30 (10 x 3) seconds. The default gbcast value is 2.
- □ **cur** for viewing the VRRP settings

Synchronization

The synchronization feature provides for stateful failover to a redundant Alteon Firewall when the active Alteon Firewall fails.

/cfg/fw/sync accesses the Sync Configuration Menu. The options are:

- □ **ena** for enabling session state synchronization between redundant Alteon Firewalls
- □ **dis** for enabling session state synchronization between redundant Alteon Firewalls
- □ **cur** for viewing the synchronization settings

/maint/fw/sync tests the network link between redundant Alteon Firewalls. The link is the pathway for session state synchronization.

Join

The join command has been included in the 2.0 release for adding a second Alteon Firewall to the cluster (see "Alteon Firewall Clustering" on page 4). `Join` is only available from the Setup Menu which appears when you bring up an Alteon Firewall for first time.

BBI

The Browser Based Interface (BBI) and BBI help were updated to conform with the CLI changes.

Clarifications

Static NAT Setup

To set up static NAT for an internal host IP address so that the host has a valid external host IP address, login as root and set up *proxy arp* according to the example below (for this example 10.10.1.10 is the external host IP address and 01:02:03:04:05:06 is the MAC address):

```
make-part-rw / on
echo "arp -s 10.10.1.10 01:02:03:04:05:06 pub" >> /etc/rc.d/rc.local
echo "echo 1 > /proc/sys/net/ipv4/conf/all/proxy_arp" >> /etc/rc.d/rc.local
make-part-rw / off
arp -s 10.10.1.10 01:02:03:04:05:06 pub
echo 1 > /proc/sys/net/ipv4/conf/all/proxy_arp
```

Then, using the CLI or BBI, add a static route for the external host IP address using the internal host IP address (8.0.0.1 in this example) as the gateway. The CLI command is:

```
/cfg/sys/routes/add 10.10.1.10 255.255.255.255 8.0.0.1
```

Check Point EMC

Figure 3-1 in the *Alteon Firewall 5100 Series Installation and User's Guide* shows the Check Point EMC on a highly secure port/network that is separate from the management network. This is an acceptable configuration if you have an extra port. If you do not have an extra port (as would be the case if you had an optional DMZ LAN), the Check Point EMC should be on the management network.

OpenSSL

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

Known Issues

Check Point FireWall-1 NG FP-3 Issues

- All Check Point licenses and firewall policies are tightly 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 FP-3 management station on Win NT, right-clicking on a "User" object in the Policy Editor will cause the Policy Editor to freeze. If this happens, kill the Policy Editor and re-launch it. To edit the user object, use the menu item "Manage | Users and Administrators..."
- FP3 loads default filter first and then initial filter. It is normal to see a default filter for a while.
- Automatic ARP is not supported by Check Point. Instead, you must configure ARP from the Linux command line (see "Static NAT Setup" on page 7). From the GUI, automatic ARP must also be disabled via Policy->Global Properties. On the left hand side of the new screen, click on NAT. Uncheck the box "Automatic ARP configuration". Also see Check Point FP3 Release notes page 64: Platform specific - Linux Automatic ARP is not supported (CR Q00592050).
- Other features and issues are documented in the Check Point FP-3 release notes. You can review them at the following URL: http://www.checkpoint.com/techsupport/installation/ng/release_notes.html. Then select the Next Generation Feature Pack 3 Suite Release Notes.pdf. You must first sign in using the username and password that were assigned to you by Check Point.

NOTE – Check Point has guidelines on this page to help you obtain a username and password if you do not already have them. Once you have signed in, download the release notes to your workstation.

CLI Issues

- After configuring the Alteon Firewall for the first time, reboot the unit using the `/boot/reboot` command.
- If a host name is not resolvable to an IP address, the CLI will hang for a few minutes before returning an error message.

- 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.
- 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

- The BBI does not support adding or removing users from groups. Create or modify users in the `/cfg/sys/user` menu in the CLI.
- 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).
- A SIC reset cannot be done from the BBI. Use `/cfg/fw/sic` instead (CR Q00606620).
- VRRP status cannot be checked from the BBI. Use `/info/vrrp` instead (CR Q00606661).

Enterprise Management Console (EMC) Management Server Issues

- Check Point EMC Management station can only be removed by installing a new image from CD-ROM. After initial installation, the Check Point EMC management station is not removable from the Firewall using the `/boot/delete` command. If you wish to uninstall the Check Point EMC management station from the Alteon Firewall 5100 series, reinstall 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.

- `boot/delete` is not supported on an EMC appliance (CR Q00563930).

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/link` command will show the actual status of the port (CR Q00585993).

Rebooting Issues

The appliance must be rebooted under the following scenarios:

- enabling HA
- performing `/boot/delete`
- performing `/cfg/gtcfg` (CR Q00594626).
- changing VLAN tagging options

Secure Internal Communication (SIC) Issues

- When the SIC is reset, the existing firewall policy may be reset to the default deny all filter (CR Q00494416). In that case, a new policy must be pushed from the GUI client. The default policy can be unloaded using the CLI command:

  ```
  /maint/fw/unldplcy
  ```

  Then the policy can be pushed.
- After a SIC reset in a cluster configuration, `/maint/fw/unldplcy` must be performed on each appliance (CR Q00585706).
- When performing SIC reset in a cluster, the warning message can be safely ignored (CR Q00585705).

VRRP Issues

- You must add an explicit 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.
- The preferred master and backup master should be connected to the same device.

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

- After using the join command to add a second member to the cluster, the firewall may take up to three minutes to restart.
- When the second appliance added to a cluster is to be the preferred master, the procedure is to add the second appliance as a backup, configure the cluster and firewall policies, and then change the preferred master option using the `/cfg/net/vrrp/master` command.
- 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 time it takes for VRRP to converge is determined by the number of interfaces. The formula for determining the amount of time is (CR Q00604684):

  Total time = <adint value> + 8 * <number of interfaces>
- 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 the VRRP process is started, IGMP membership reports are sent to multicast addresses 224.0.0.18 and 224.0.0.2. This does not affect VRRP operation (CR Q00588145).
- 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).
- In a cluster, CLI or BBI access may not be available from the MIP. The workaround is to use the IP address of the VRRP master (CR Q00588155).
- 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).

General Issues

- The Alteon Firewall allows users to configure licenses using the Command Line Interface (CLI) or Browser-Based Interface (BBI). The licenses can also be installed from the Management Server when using Check Point Central Licensing. Only the license installed using the Alteon Firewall CLI or BBI will be displayed in the info window BBI or CLI using the following command: `/cfg/pnp/list`. The license installed through the Check Point Management station will not be displayed by Alteon Firewall CLI or BBI.
- `boot/delete` is the correct method to change the host IP address of any appliance 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/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 command `/info/vrrp` displays the information for the physical ports based on index 0 (i.e. port 1 is displayed as eth0) (CR Q00588143).
- 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).