RELEASE NOTES:

Alteon Firewall 5100 Series™

Release 2.1

Part Number: 213456-E, March 2003

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

Release Notes

Release 2.1 (Web-only)

The Alteon Firewall 5100 Series 2.1 software will initially be a Web-only release. This means that the software and documentation are only available via the Nortel Networks Customer Support Web site. If you wish to upgrade your system to Release 2.1, follow this procedure:

- 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 4 to download the Release 2.1 software.

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.

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: **FP3 - ASF 2.x.x.x** Then select **Go**
10	Downloads Nortel Alteon Switched Firewall NG for Alteon Firewall (5100 series) (Nortel OS Any FP3 - ASF 2.x.x.x)	Select Download Option(s) CD Image (.iso) for burning a CD image Boot Image (.img) for reinstall via tftp Upgrade (.pkg) for upgrade via 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	

Alteon Firewall Upgrade Matrix

- Upgrading Release 1.x to Release 2.x using a tftp server is not supported on any platform.
- Upgrading Release 2.0.x to any future release will be supported on all platforms.

NOTE – To upgrade from Release 1.1.2 or Release 1.1.3 to the current release, see "Upgrading from Release 1.1.2 or 1.1.3" on page 18.

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.

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 /cfg/ptcfg and restore it after reinstallation using /cfg/gtcfg.

For complete installation instructions, see the Readme.txt file that is collocated with the software (see "Software Download Procedure" on page 4 for Web-site navigation instructions).

Documentation

The *Alteon Firewall 5100 Series Installation and User's Guide* is ordinarily supplied on a CD-ROM that ships with your system. Since this will initially be a Web-only release, a CD with 2.1 user documentation is not available. However, you can access the latest *Alteon Firewall 5100 Series Installation and User's Guide* by selecting:

Alteon ▸ Alteon Switched Firewall System (Documentation)

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.

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

New Features for Release 2.1

- The new features for Release 2.0 were exclusively addressed to the ASF 5109. For this release, the new features for Release 2.0 have been extended to the ASF 5105 and ASF 5112. See "New Features for Release 2.0" on page 7 for a description.
- For FP-3, 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 CLI and the BBI. A table of name changes is provided here:

Table 1 Check Point Product Name Changes for FP-3

Current NG FP-3 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.

- You can now configure SMART Client (also known as GUI client) access to the Alteon Firewall using the Browser Based Interface (BBI). In previous releases, access was configured exclusively at the CLI using the `/cfg/fw/client` menu.

NORTEL NETWORKS
213456-E, March 2003

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 8 for command descriptions).

Alteon Firewall Clustering

This release 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 this release) 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 this release. See a description of the applicable CLI commands in "Synchronization" on page 9. See "Configure State Synchronization using the SmartDashboard", 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 8 for command descriptions). VLAN tagging is also configurable at the BBI. See "VLAN Tags", in the *Alteon Firewall Installation and User's Guide* for a representative configuration.

New CLI Commands

New commands for this release

For complete descriptions, see the Alteon Firewall User's Guide for release (part number 213455-E). These same commands were available in release 2.0 for the ASF 5109

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 this release for adding a second Alteon Firewall to the cluster (see "Alteon Firewall Clustering" on page 7). `Join` is only available from the Setup Menu which appears when you bring up an Alteon Firewall for first time.

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
ln -s /etc/rc.d/rc.local /etc/rc3.d/S99local
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 SmartCenter Server

Figure 3-1 in the *Alteon Firewall 5100 Series Installation and User's Guide* shows the Check Point SmartCenter Server on a highly secure 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 Smart-Center Server 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 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 SmartDashboard (known in FP-2 as Policy Editor) will 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..."
- FP-3 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 10). 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 FP-3 Release notes page 64: Platform specific - Linux Automatic ARP is not supported (CR Q00592050).
- Check Point FireWall-1NG FP-3 is part of the Alteon Firewall 2.1.x 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 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. 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.
- 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

- BBI will not launch when you connect to the cluster MIP address (CR Q00628190).

  Workaround: Connect to the host IP address.
- 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).
- Changing the management port from the BBI causes SSI to go out of sync (CR Q00622507).

SmartCenter Server Issues

- `boot/delete` is not supported when the management 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 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/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

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/fw/unldplcy`

  Then the policy can be pushed.
- After a SIC reset in a cluster configuration, `/maint/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: Cannot change backup master IP address from the preferred master (CR Q00630277).
- 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/fw/unldplcy followed by /maint/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: Panics when you enter a *cpstop* command on the preferred master (CR Q00620702).
- 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 #).
- 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.
- 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).

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.

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.
- ASF 5105/5112: /Info/link shows autonegotiation is on when it is actually off (CR Q00626418).
- 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).
- 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 from Release 1.1.2 or 1.1.3

You must follow this procedure when upgrading your ASF 5105 or ASF 5112 to Release 2.1.

Downloading Release 2.1

1. **Point your browser to Alteon Switched Firewall System Downloads page (see "Software Download Procedure" on page 4 for instructions).**
2. **Select the Alteon Firewall 2.1.x image file (.iso).**
3. **Copy the file to your tftp server.**

Installing Release 2.1

NOTE – Be sure to save your configuration to your tftp server before installing Release 2.1 (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 and burn the Release 2.1.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 asf5105 or asf5112.**

   (The asf5105 applies to the ASF 5105 and the asf5112 applies to the ASF 5112.)

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

   This is required to apply the restored configuration.