RELEASE NOTES:

Alteon Switched Firewall™
Version 1.0.43

Part Number: 213028-B, April 2002

NORTEL
NETWORKS™

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

Alteon Web Systems
Intelligent Webworking™

Release Notes

Thank you for purchasing the Alteon Switched Firewall (ASF) with software version 1.0.43. These release notes provide the latest information regarding your ASF and contain the following important modifications to the complete documentation:

- About the documentation (page 4)
  - Product manuals are located on CD-ROM
  - Printed manuals can be obtained through your sales representative
  - The System Information document extends to the Alteon SFA-AD3 and iSD308-SFD
  - Late breaking information is available at the Nortel Networks Web site

- Upgrading the ASF Software
  - Upgrade the Check Point management station with Feature Pack-1 (page 5)
  - Upgrade the Alteon iSD-SFD (page 5)
  - Upgrade the Alteon SFA (page 7)

- Changes for Version 1.0.43
  - The initial setup procedure has been simplified (page 9)
  - The setting for synchronization device name has been removed (page 9)
  - TFTP is available only when a single Alteon iSD-SFD is installed (page 9)
  - The BBI includes a new Proxy ARP form (page 10)
  - SNMP has been upgraded to enhance security (page 10)
  - The synchronization configuration process has been changed (page 11)

- The Alteon iSD308-SFD and Alteon SFA-AD3
  - Physical characteristics differ slightly from manual (page 13)
  - Installation requirements and cable connections are slightly different (page 16)
  - Settings for unavailable gigabit ports are disregarded in the CLI and BBI (page 18)
  - Expanding the cluster with additional equipment is slightly different (page 19)

Please keep this document with your Nortel Networks product manuals.

About the Product Documentation

Documentation CD-ROM

The *Alteon Switched Firewall Installation and User's Guide* (part number 212535-A) is supplied on a CD-ROM included with this product.

NOTE – The manual documents version 1.0.41 of this product. Version 1.0.43 behaves exactly like version 1.0.41 with a few important exceptions as discussed in these release notes.

The manual is a PDF file which can be read and printed using the free Acrobat Reader software available from the Adobe Systems Incorporated Web site:

http://www.adobe.com

To access the manual, open the "212535a.pdf" file on the *Alteon Switched Firewall Documentation* CD-ROM. When the manual opens, you can navigate through the book by selecting the pre-defined bookmarks on the right side of the window, and by scrolling through the pages.

Obtaining Printed Documentation

To obtain a manual in hardcopy format, contact your Nortel Networks sales representative and order part number 212535.

System Information

The *Alteon Switched Firewall System Information* document (part number 212537-A) included with this product describes the Alteon SFA-184 and iSD310-SFD. This information also applies to the Alteon SFA-AD3 and iSD308-SFD.

Late-Breaking News and Support

Check the Nortel Networks Web site for current product information:

http://www.nortelnetworks.com

This Web site includes software updates, release notes, and white papers. The Web site also includes access to Nortel Networks customer support for accounts under warranty or that are covered by a maintenance contract.

AlteonWebSystems

Upgrading the ASF Software

NOTE – Because the ASF version 1.0.43 upgrade requires Check Point NG Feature Pack-1 (FP-1), the upgrade procedure is different from that stated in the manual. Please read the following upgrade instructions carefully.

Part 1: Upgrade the Management Station with FP-1

Before you upgrade the ASF software, you must first upgrade your Check Point management station with Check Point NG Feature Pack-1 (FP-1) software.

FP-1 is a feature-rich addition to the initial release of the Check Point Next Generation Firewall-1 software. The FP-1 upgrade is available from Check Point Software Technologies Ltd. to customers who meet Check Point's support eligibility requirements.

For FP-1 feature information, eligibility requirements, software download, and installation instructions, see the Check Point Web site: http://www.checkpoint.com

NOTE – If you do not upgrade your Check Point management station with FP-1, the ASF will be unable to re-establish trust or obtain firewall policies once ASF version 1.0.43 is installed.

Part 2: Upgrade the Firewall Director Software

1. **Make sure that all Firewall Directors in the cluster are operational.**

2. **Download the ASF 1.0.43 upgrade package into the Firewall Director.**

   Follow the instructions starting on page 248 of the manual, or as summarized here:

   ■ Connect to the any active Firewall Director using the console and log in as the administrator. Telnet and SSH cannot be used to install the upgrade.

   ■ To load the upgrade package, use the following command:

      `/boot/software/ftp`

   Follow the screen prompts to begin loading the upgrade.

3. **When the upgrade is loaded, activate the new version.**

   Use the following command:

      `/boot/software/activate`

   When the command is issued, the new software will be unpacked and each Firewall Director in the cluster will automatically reboot. This process may take a few minutes.

4. **Log in again and verify that the upgrade package is marked as "permanent."**

Use the following command to display the status of the upgrade package:

    /boot/software/cur

NOTE – The newly installed upgrade package will be marked as "current" for approximately one minute before becoming "permanent." Repeat this verification step as necessary until the upgrade is marked as permanent.

---

5. **If applicable, disconnect any version 1.0.41 synchronization cables.**

If upgrading from version 1.0.41, disconnect any cables from the Alteon iSD310-SFD synchronization port (network port 1). Later, these will be reconnected using the network port 2 as the new synchronization port.

6. **Activate the FP-1 upgrade on the Firewall Director.**

The FP-1 upgrade is included as part of the ASF version 1.0.43 software. You are not required to download of any additional software images. Instead, use the following new command to initiate activation of the included FP-1 upgrade:

    /cfg/fw/software/upgrade

NOTE – After you activate the upgrade (Step 3), the Firewall Director re-initializes with the new menus system. If you log in (Step 4) before the initialization is complete, the old menu system may still be displayed and the upgrade command may not appear on the expected menu. If this occurs, allow a few moments for the Firewall Director to comple initialization. When ready, the "system successfully re-initialized" message is displayed. Log out and log back in again for the new menu system.

After entering the upgrade command, you will be prompted to supply a new one-time password that will be used to re-establish trust after the upgrade. The supplied password will be used on each Firewall Director. Once the password is entered, the system will begin installing FP-1 on each active Firewall Director in your cluster.

During the installation process, you will see the following message on the console:

```
SYSTEM INFO: iSD is being reinitiated.
```

This warning is normal. You will also see log messages stating that cfgd has been stopped and then restarted. After about three minutes, the following message should appear:

```
SYSTEM INFO: iSD has successfully been reinitiated.
Ok.
```

Alteon*Web*Systems

The installation is complete when the CLI prompt returns. At this point, if the firewall was up and running prior to the upgrade, it should have automatically restarted. No reboot is required.

7. **If applicable, reconnect any synchronization cables to iSD-SFD network port 2.**

If upgrading from version 1.0.41, please note that the synchronization network now uses network port 2 instead of network port 1. If using synchronization, reconnect the cables that were disconnected in Step 5 to network port 2.

8. **On the Check Point management station, update the firewall objects to version NG FP-1.**

9. **Re-establish trust between the Check Point management station.**

10. **Push the firewall policies to the ASF cluster.**

This is required since the firewall policies on the ASF are reset after the initial activation of the FP-1 upgrade.

Part 3: Upgrade the Firewall Accelerator Software

Each Firewall Accelerator in the cluster must be manually upgraded to use the version 1.0.43 software. To upgrade the Firewall Accelerator software, the following is required:

- A computer running ASCII terminal emulation software.

- A standard serial cable with a male DB9 connector (included with the Firewall Director). See page 46 of the manual for cable specifications.

- A binary upgrade image for the Firewall Accelerator.

To install the upgrade image, perform the following steps:

1. **Gracefully halt and shut down each iSD308-SFD Firewall Director in the cluster.**

The Firewall Directors must each be shut down before any Firewall Accelerators can be upgraded. To halt each Firewall Director in turn, connect to its console, log in as the administrator, and issue the following command:

```
/boot/halt
```

After confirming the command, the Firewall Director to which you are connected will halt. When the halt is complete, turn off the Firewall Director.

Repeat this step for each active Firewall Director in the cluster.

2. **Connect a terminal directly to the Firewall Accelerator console port.**

   Set the communications parameters as shown in the table below:

   Table 1 Console Configuration Parameters

Parameter	Value
Baud Rate	9600
Data Bits	8
Parity	None
Stop Bits	1
Flow control	None

3. **Turn off the Firewall Accelerator and then turn it back on.**

4. **Press <Shift-F> while the Firewall Accelerator is attempting to boot (while the "AceSwitch BootMon..." message is displayed).**

5. **Reconfigure your terminal to use a baud rate of 57600.**

6. **Transfer the binary upgrade image from the terminal to the Firewall Accelerator using Xmodem protocol.**

   For example, if using Hyperterminal, select the Transfer | Send File command and select Xmodem or 1K-Xmodem (faster) as the protocol.

7. **When the transfer is complete, return your terminal to a baud rate of 9600.**

8. **Turn off the Firewall Accelerator and then turn it back on.**

9. **If using a high-availability configuration, repeat this process on the redundant Firewall Accelerator.**

10. **Sequentially turn on each Firewall Director that was halted at the start of this procedure.**

   NOTE – After turning on any Firewall Director in the cluster, allow it to initialize for about one minute before turning on the next.

Alteon *Web* Systems

Changes for Version 1.0.43

Initial Setup

In the initial setup of the Firewall Director, you are no longer prompted to specify the Ethernet device used for connecting to the Firewall Accelerator. With this simplification, step 2 on page 53 of the manual no longer applies. All other steps for the Firewall Director setup as described in Chapter 3 remain in effect.

Menu System

Synchronization for Stateful Failover

The Synchronization Configuration Menu has been simplified to remove the obsolete `dev` option. The network device name is now determined automatically. The full command path of the deleted option is as follows:

`/cfg/fw/sync/dev`	(Page 157)

Using TFTP

TFTP is available only when a single Firewall Director is used. Transferring software or configuration files to or from a TFTP server will fail if more than one Firewall Director is present.

When using the following TFTP commands, temporarily detach all but one Firewall Director:

`/cfg/ptcfg`	(Page 99)
`/cfg/gtcfg`	(Page 99)
`/boot/software/tftp`	(Page 169. Or use FTP instead)
`/maint/dumplogs`	(Page 170)
`/maint/dumpstat`	(Page 170)

Browser-Based Interface (BBI)

Firewall / Synchronization Form

The Firewall / Synchronization form has been simplified to remove the Device Name field discussed on page 215 of the manual. The network device name is now determined automatically.

Proxy ARP Form

A Network / Proxy ARP form has been added to the BBI. This form is used to configure IP addresses that the cluster should respond to on behalf of Network Address Translation (NAT) features configured in the Check Point FireWall-1 NG software.

More information on this form can be found by clicking on the global help button in the BBI.

SNMP Security Enhancements

The ASF version 1.0.43 upgrade includes enhanced SNMP Research International software release 15.3.1.7.

In this upgrade, the SNMP Research Master Agent binds to port 161, though GET requests are discarded. This provides an extra measure of security (beyond the restricted SNMP functionality and existing protections of the firewall and the access list).

This security enhancement comes in response to CERT® advisory CA-2002-03, released on February 12, 2002. The advisory noted potential vulnerabilities with SNMP software products from SNMP Research International, some of which were used in the ASF.

For more information about CERT advisories, check their Web site at http://www.cert.org.

Synchronizing Firewall Directors

The following section replaces material found on pages 242 through 244 of the manual. The procedure has been modified to make configuration easier.

NOTE – Version 1.0.43 synchronization uses Alteon iSD-SFD network port 2 instead of network port 1 as used with version 1.0.41.

Firewall Directors can be synchronized to provide stateful failover of sessions. With synchronization, if a Firewall Director fails, its open sessions will be transparently reassigned to a healthy Firewall Director.

To achieve stateful failover, synchronization must be configured both on the Alteon Switched Firewall and on the Check Point management server.

1. **Make sure Alteon Switched Firewall synchronization is off.**

   Log in to the Alteon Switched Firewall cluster MIP address using an administrator account and enter the following commands:

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

2. **Define a network for use with synchronization traffic.**

   A unique network address should be used for synchronization traffic. This should be the same network address specified in the Synchronization tab of the cluster properties. For example:

   ```
   >> Sync Configuration# net 192.168.2.0
   >> Sync Configuration# mask 255.255.255.0
   ```

3. **Apply the changes:**

   ```
   >> Sync Configuration# apply
   ```

4. **From the Check Point Policy Editor, update the firewall interface information.**

   Start the Policy Editor application on your management client station. From within the Policy Editor, select a Firewall Director in the cluster and edit its properties. Select the Topology tab in the Properties window and click on the Get Interfaces button.

   Verify that the list of detected interfaces includes eth1 with an IP address on the synchronization network defined in Step 2. In keeping with our example network from the manual, the interface should have an address in the 192.168.2.0/24 network.

   Repeat this step for each Firewall Director in the cluster.

5. **From the Policy Editor, enable Check Point firewall synchronization.**

Select the Gateway Cluster in the Network Objects tree on the left side of the Policy Editor window. If necessary, click on the minus (-) icon in front of the Gateway Cluster to reveal its objects.

Check for a gateway cluster object representing the Alteon Switched Firewall. This object should have been created when a new Firewall Director was initially added to the existing cluster. If no object exists, see steps 8 through 10 on pages 238 and 239 of the manual.

Right click on the gateway cluster object and select Edit from the pop-up menu. When the properties dialog appears, select the Synchronization tab and check the "Use State Synchronization" box.

Next, click on the Add button to add a synchronization network and enter the following information:

- Network Name: Enter your choice of network name to represent the synchronized network.

- IP Address: Enter the base network IP address which will be used for synchronization. This should be the same address specified in Step 2.

- Net Mask: Enter the network mask for synchronization network. The network IP Address and Net Mask combination should provide as many unique IP addresses as there are Firewall Directors within the cluster. Use the same mask specified in Step 2.

Click OK to add the configured synchronization network.

6. **From the Policy Editor, re-install the security policies on the firewall cluster.**

7. **Connect all Firewall Director SyncNet ports together.**

Connect synchronization port 2 on both Firewall Directors. If connecting the ports directly together, use a crossover network cable. If connecting the ports through a hub or layer-2 switch, use a straight-through network cable.

If there are more than two Firewall Directors in the cluster, connect all of them together through a hub or layer-2 switch using straight-through network cables. In such a case, synchronization port 2 of all the Firewall Directors should be connected to the hub or layer-2 switch.

8. **Enable Alteon Switched Firewall synchronization.**

Log in to the Alteon Switched Firewall cluster MIP address using an administrator account and enter the following commands:

```
>> # /cfg/fw/sync/ena
>> Sync Configuration# apply
```

Alteon *Web*Systems

The Alteon iSD308-SFD and Alteon SFA-AD3

The following material applies only to the Alteon iSD308-SFD and Alteon SFA-AD3. Disregard this information if using the Alteon iSD310-SFD and Alteon SFA-184.

Physical Characteristics

The physical features of the Alteon iSD308-SFD and Alteon SFA-AD3 differ slightly from the Alteon iSD310-SFD and Alteon SFA-184 described in the manual. This is chiefly due to the removal of the SC fiber-optic ports as shown in the following sections.

The Alteon iSD308-SFD Firewall Director

The following section replaces information found on page 23 of the manual.
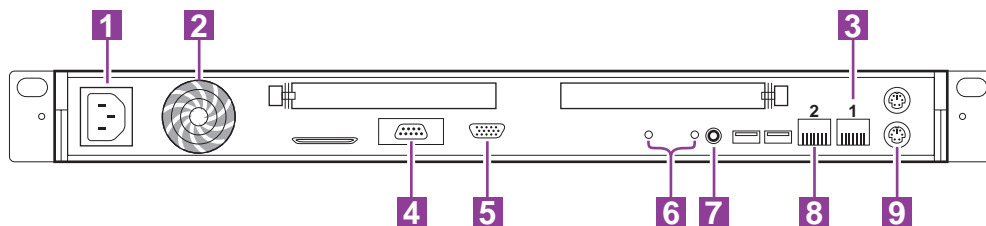
Figure 1 Rear Panel of the Alteon iSD308-SFD

1. **AC power receptacle**

2. **Fan exhaust**

3. **10/100 Mbps uplink connector (Port 1)**

    Dedicated connection to the Alteon SFA-AD3 Firewall Accelerator.

4. **Serial port**

    Connects a local console terminal for system configuration and diagnostics.

5. **Video connector**

    The video connector can be attached to a monitor. When used along with a keyboard attached to the keyboard connector, this provides a local console terminal for system configuration and diagnostics.

6. **Status LEDs**

   Table 2 iSD308-SFD Front Panel LEDs

LED	Description
⎯ᴧ⎯	System attention indicator When the system is reset, the LED is off. When the system is running, this LED displays solid green. If the system hangs or if the Chassis Identify function is selected, the LED flashes. There is a duplicate system attention indicator on the back-panel.
⏻	System power indicator This LED is green when the power supply is turned on. There is a duplicate system power status indicator on the back panel.

   These indicators are duplicated on the front panel.

7. **Power button**

   Controls the AC power input to the system's power supply.

8. **10/100 Mbps synchronization connector (Port 2)**

   Used for synchronizing sessions among multiple Firewall Directors. See "Synchronizing Firewall Directors" on page 11 for details.

9. **Keyboard connector (used along with the video connector)**

10. **Items not presently supported:**

   - SCSI connector
   - Universal Serial Bus (USB) connectors
   - Mouse connector

Alteon*Web*Systems

The Alteon SFA-AD3 Firewall Accelerator

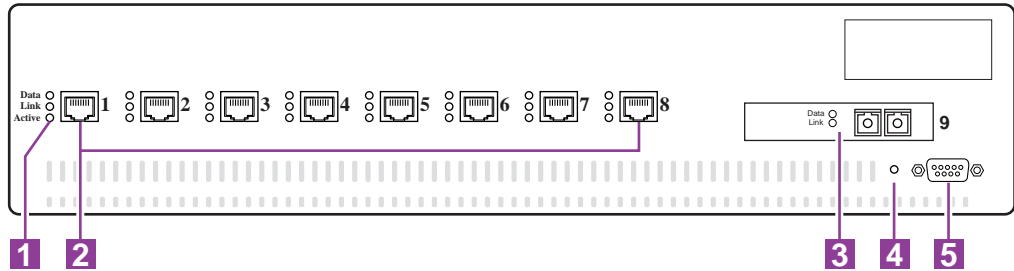The following section replaces information found on page 24 and 25 of the manual.

Figure 2 Front Panel of the Alteon SFA-AD3

1. **Port LED indicators**

Table 3 describes the lights and conditions represented by the state of the Port LEDs.

Table 3 Firewall Accelerator Port LEDs

LED	State	Description
Data	Blinking	Data detected on the port.
	Off	No data detected on the port.
Link	On	Good link.
	Off	No link; could be a result of a bad cable or bad connector.
	Blinking	Port has been disabled by software.
Active		Reserved for future functions. Currently, this LED lights when the port has a good link, or when it has been disabled by software.

2. **Port 1 through Port 8 network ports**

This RJ-45 jack is for connecting 10/100 Mbps Ethernet segments to the port. The ports are auto-negotiating and support half- or full-duplex operation.

3. **Port 9 is reserved for connecting redundant Firewall Accelerators**

This SC jack accepts fiber optic cable segments. It is used to interconnect two Firewall Accelerators in a high-availability configuration.

4. **Power LED**

This green LED lights to indicate that the device is on and receiving proper power.

5. **Serial port**

This female DB-9 serial connector is labeled "Console" for the console (DCE) connector. This port is used only for diagnostic and recovery functions.

Installation

Physical installation of the Alteon SFA-AD3 and iSD308-SFD is identical to that described in Chapter 2 of the manual, except as indicated in the following sections.

Requirements

The following information modifies the requirements found on page 32 of the manual:

■ High capacity Alteon SFA-184 Firewall Accelerators and iSD310-SFD Firewall Directors cannot be used in the same cluster as Alteon SFA-AD3 and iSD308-SFD devices.

Connecting Cables

The following section replaces information from page 40 and 41 of the manual.

Once the Alteon Switched Firewall equipment is physically mounted in a rack system, the required network cables can be attached. Although the precise topology depends on your specific network, the basic Alteon Switched Firewall network topology suggested for initial configuration is simple, as shown below:
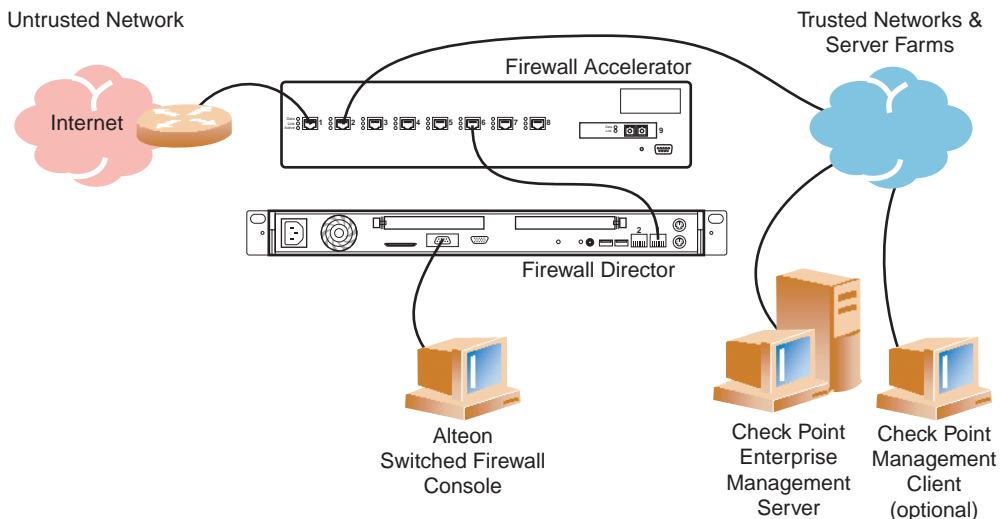

Figure 3 Basic Alteon Switched Firewall Network

By default, the various ports on the Firewall Accelerator are reserved for specific purposes:

■ Ports 1 though 5 are reserved for connecting trusted, untrusted and semi-trusted networks to the firewall. The RJ-45 connectors accept 10/100Base-T Ethernet segments.

■ Ports 6 though 8 are reserved for Firewall Director connections. The RJ-45 connectors accept 10/100Base-T Ethernet segments and are connected to iSD308-SFD Firewall Director uplink port 1.

   Port 6 through 8 can also be configured for use as regular network ports. See "Changing the Firewall Accelerator Ports" on page 245 of the manual for more information.

■ Port 9 is reserved for interconnecting redundant Firewall Accelerators.

Using the reserved ports, attach the Firewall Director uplink port 1 to the Firewall Accelerator using any of ports six through eight. Connect the trusted, untrusted and semi-trusted network feeds into any of ports one through five. See "Connector Specifications" on page 41 of the manual for connector and wiring specifications.

NOTE – Alteon SFA-AD3 Firewall Accelerators are compatible only with iSD308-SFD Firewall Directors. Do not use the Alteon SFA-AD3 or iSD308-SFD in the same cluster as the high-capacity Alteon SFA-184 and iSD310-SFD Alteon Switched Firewall devices.

Once network cabling is complete, power can be connected as described in "Connecting Power" on page 44 of the manual.

Disregarded Port Settings in the CLI

The Network Port Menu, accessed using the `/cfg/net/port` command, is used to configure physical ports on the Firewall Accelerator. Because the Alteon SFA-AD3 Firewall Accelerator does not have redundant network ports as described in the manual, the configuration settings for the following menu commands are ignored:

■ Disregarded for 10/100Mbps ports 1 through 8:

```
/cfg/net/port <number 1-8>/gig        (Pages 132 and 137)
/cfg/net/port <number 1-8>/pref       (Pages 132 and 245)
/cfg/net/port <number 1-8>/back       (Pages 132 and 245)
```

■ Disregarded for 1000Mbps port 9:

```
/cfg/net/port 9/fast                  (Pages 132, 135, and 136)
/cfg/net/port 9/pref                  (Pages 132 and 245)
/cfg/net/port 9/back                  (Pages 132 and 245)
```

Disregarded Network / Ports Form Settings in the BBI

The Network / Ports Forms are used to configure physical ports on the Firewall Accelerator. Because the Alteon SFA-AD3 Firewall Accelerator does not have redundant network ports as described in the manual, the configuration settings are ignored for the following fields discussed on pages 198 through 200 of the manual:

■ Disregarded for 10/100Mbps ports 1 through 8:

  □ Preferred Physical Connector

  □ Backup Physical Connector

  □ Gigabit Physical Connection Settings

■ Disregarded for 1000Mbps port 9:

  □ Preferred Physical Connector

  □ Backup Physical Connector

  □ Fast Physical Connection Settings

Alteon*Web*Systems

Adding a Second Firewall Accelerator

The procedure for adding a second Alteon SFA-AD3 Firewall Accelerator to the cluster is identical to that described in Chapter 8 of the manual, with the following exceptions.

Requirements

NOTE – An Alteon SFA-AD3 is compatible only with another identical Alteon SFA-AD3. You cannot use an Alteon SFA-AD3 and Alteon SFA-184 together in the same cluster.

Installing the New Firewall Accelerator

The procedure for installing a second Firewall Accelerator differs only in that port 9, the dedicated Inter-Accelerator Port (IAP), has only a 1000Mpbs fiber-optic SC connector. No redundant 10/100Mbps copper RJ-45 connector is available as described in step 4 on page 229 of the manual.

Adding Firewall Directors

The procedure for adding iSD308-SFD Firewall Directors to the cluster is identical to that described in Chapter 8 of the manual, with the following exceptions.

Requirements

NOTE – An iSD308-SFD Firewall Director is compatible only with an Alteon SFA-AD3 Firewall Accelerator. You cannot use an iSD308-SFD with a high-capacity Alteon SFA-184.

Installing the New Firewall Director

The procedure for installing additional Firewall Directors differs only in the port used to connect the new Firewall Director to the Firewall Accelerator. The following information replaces step 4 on page 233 of the manual.

Firewall Accelerator ports 6 though 8 are reserved for Firewall Director connections. Connect the Firewall Director uplink port 1 to an available port 6, 7, or 8 on any Alteon SFA-AD3 Firewall Accelerator.