

RELEASE NOTES:



Alteon Switched FirewallTM **Version 1.0.42 for SFA-AD3 & iSD308-SFD**

Part Number: 213028, Revision A, January 2002

NORTEL
NETWORKSTM

50 Great Oaks Boulevard
San Jose, California 95119

408-360-5500 Main

408-360-5501 Fax

www.nortelnetworks.com

 **Alteon WebSystems**
Intelligent WebworkingSM

Copyright 2002 Nortel Networks, Inc., 50 Great Oaks Boulevard, San Jose, California 95119, USA. All rights reserved. Part Number: 213028, Revision A.

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of Nortel Networks, Inc. Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement or the implied warranties of merchantability or fitness for a particular purpose.

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.

Alteon Switched Firewall, iSD308-SFD, iSD310-SFD, Firewall Director, Firewall OS, Alteon SFA-AD3, Alteon SFA-184, Firewall Accelerator, and Accelerator OS are trademarks of Nortel Networks, Inc. in the United States and certain other countries. FireWall-1 NG is a registered trademark of Check Point Software Technologies. Any other trademarks appearing in this manual are owned by their respective companies.



Release Notes

Thank you for purchasing the Alteon Switched Firewall (ASF) with software version 1.0.42 for the Alteon SFA-AD3 Firewall Accelerator and iSD308-SFD Firewall Director.

These release notes provide the latest information regarding your Alteon Switched Firewall and contain important modifications to the complete documentation. Please keep this document with your Nortel Networks product manuals.

Documentation on CD-ROM

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

NOTE – The manual documents version 1.0.41 of this product for the Alteon SFA-184 and iSD310-SFD. Version 1.0.42 for the Alteon SFA-AD3 and iSD308-SFD 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 Adobe Systems Incorporated (<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.

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, Revision 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.

Web access: <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.

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.

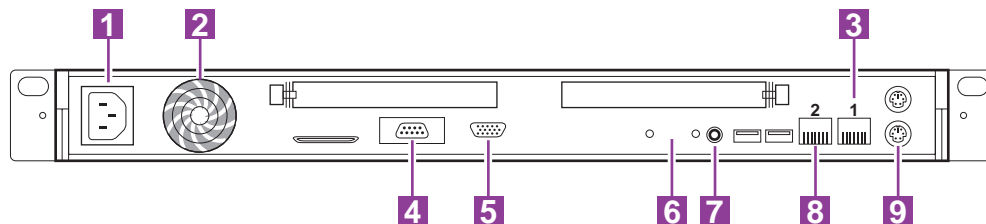


Figure 1 Rear Panel of the Firewall Director



- 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 1 iSD308-SFD Front Panel LEDs

LED	Description
	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.

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

10. Items not presently supported:

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

The Alteon SFA-AD3 Firewall Accelerator

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

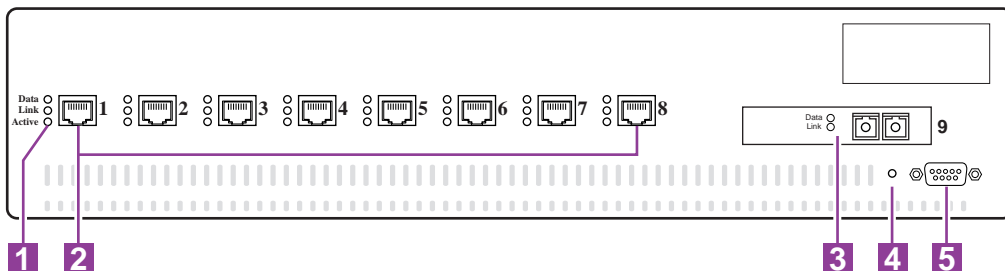


Figure 2 Front Panel of the Firewall Accelerator

1. Port LED indicators

Table 2 describes the lights and conditions represented by the state of the Port LEDs.

Table 2 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 has been disabled by software.

2. Port 1 through Port 8 network ports

The 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

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

Installation

Physical installation 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:

- Alteon SFA-AD3 Firewall Accelerators and iSD308-SFD Firewall Directors require version 1.0.42 software. These devices cannot use software version 1.0.41 or below.
- High capacity Alteon SFA-184 Firewall Accelerators and iSD310-SFD Firewall Directors require version 1.0.41 software. These devices cannot use software version 1.0.42 and 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:

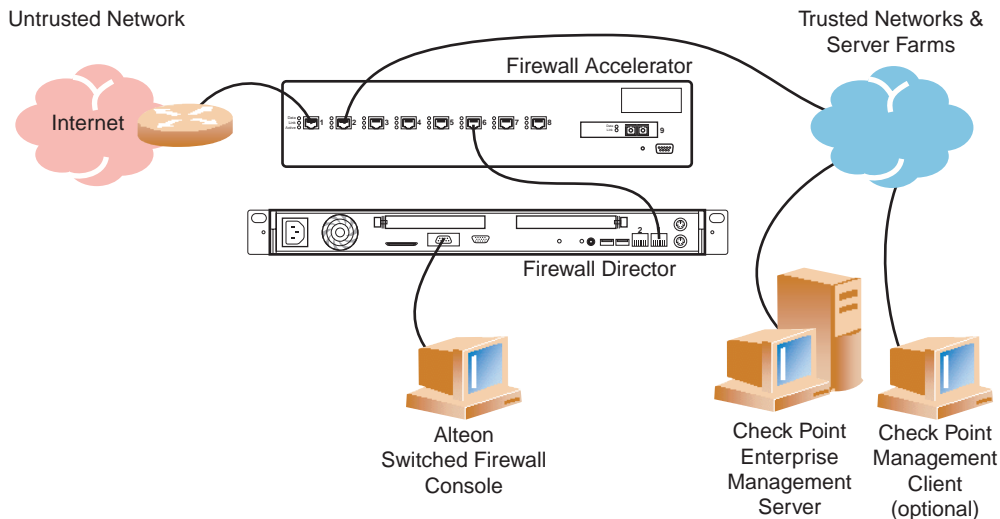


Figure 3 Basic Alteon Switched Firewall Network

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

- Ports 1 through 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 through 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.

Initial Setup

Initial setup of the Firewall Director is identical to that described in Chapter 3 of the manual, except that you are no longer prompted to specify the Ethernet device used for connecting to the Firewall Accelerator. Initial setup step 2 on page 53 of the manual no longer applies.

Menu System

Disregarded Port Settings

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:

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

- Disregarded for 1000Mbps port 9:

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

Synchronization for Stateful Failover

The configuration of Firewall Director synchronization has been simplified. It is no longer necessary to specify the network device name. The following command has been removed:

<code>/cfg/fw/sync/dev</code>	(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:

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

Browser-Based Interface

Network / Ports Forms

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

Firewall / Synchronization Form

The configuration of Firewall Director synchronization has been simplified. It is no longer necessary to specify the network device name. The Device Name field as discussed on page 215 of the manual has been removed.

Proxy ARP Form

A new form has been added to the Browser-Based Interface (BBI). The Proxy ARP form, located under the Network tab, 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.

Adding a Second Firewall Accelerator

The procedure for adding a second 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 with version 1.0.42 software 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 1000Mbps 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 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 with version 1.0.42 software 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 through 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.

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.

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
```

Upgrading the Firewall Accelerator Software

The following section replaces information found on page 272 of the manual.

To upgrade the Firewall Accelerator software when necessary, 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 Alteon SFA-AD3 Firewall Accelerator.

To install the upgrade image, perform the following steps:

1. Connect a terminal directly to the Firewall Accelerator console port.

Set the communications parameters as shown in the table below:

Table 3 Console Configuration Parameters

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

2. Turn off the Firewall Accelerator and then turn it back on.
3. Press <Shift-F> while the Firewall Accelerator is attempting to boot (while the “AceSwitch BootMon...” message is displayed).
4. Reconfigure your terminal to use a baud rate of 57600.
5. 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.

6. When the transfer is complete, return your terminal to a baud rate of 9600.
7. Turn off the Firewall Accelerator and then turn it back on.