

RELEASE NOTES:



Alteon Switched Firewall™ Bridge Mode

Release 3.1

Part Number: 215041-C, May 2003

NORTEL
NETWORKS™

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

Copyright © 2003 Nortel Networks, Inc., 4655 Great America Parkway, Santa Clara, California, 95054, USA. All rights reserved. Part Number: 215041-C.

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, Alteon WebSystems, ASF 3.1 Bridging Firewall, ASF 5308, ASF 5408, ASF 5610, ASF 5710, ASF 5722, Firewall OS, Firewall Director, ASF 5008, ASF 5010, ASF 5022, Bridge Mode, Firewall Accelerator, ASF 5300, ASF 5400, ASF 5600, and ASF 5700 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.

Originated in the USA.

Release Notes

These release notes provide the latest information regarding your Alteon Switched Firewall (ASF) release 3.1. ASF 3.1 is a bridging or layer 2 firewall. You cannot upgrade to ASF 3.1 from previous releases of the ASF software.

The ASF 3.1 Bridging Firewall is also called a transparent or stealth firewall because it is effectively invisible on the network. A Bridging Firewall functions as a bridge whereas a layer 3 firewall functions as a router. The same Check Point software used for layer 3 firewalls is running on the ASF 3.1 Bridging Firewall. Check Point management traffic and user traffic are kept separate.

Figure 1 illustrates the ASF 3.1 Bridging Firewall.

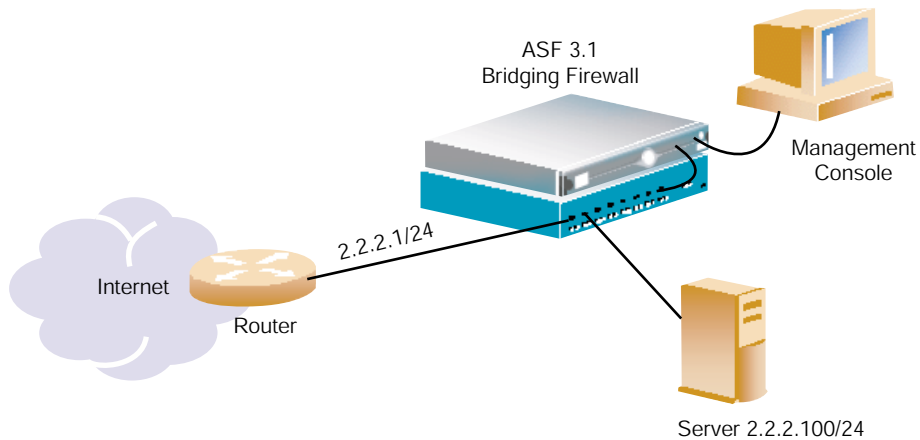


Figure 1 ASF 3.1 Bridging Firewall

ASF 3.1 Bridging Firewall

Software Support

ASF 3.1 Bridging Firewall supports Check Point FireWall-1 NG software with Feature Pack 3 (FP-3) Hotfix 2.

Hardware Support

ASF 3.1 Bridging Firewall software is supported on ASF 5710 and ASF 5610.

Features

Some of the ASF 3.1 Bridging Firewall features are listed below:

- Improves security
 - The Bridging Firewall is effectively invisible and does not have a publicly accessible IP address
- Deploys easily
 - Minimal configuration
 - No changes to existing topology
- Provides its own built-in anti-spoofing capability
 - By default, the management and SSI networks are blocked for traffic from enforcement ports. The command `/cfg/net/topo` associates IP addresses with ports. ASF 3.1 does not support Check Point's anti-spoofing feature.
- Filters data packets
- Bridges accepted data from one port to another
 - Data packets are not forwarded between VLANs
 - Uses same VLANs and network addresses on both sides of the firewall
- Access any Firewall Director locally or remotely via Telnet, Browser-based Interface (BBI), or SNMP.

Management Interface

The Management interface on Firewall Director FE 1 is implemented in ASF 3.1 with the following features:

- Used for communication between Checkpoint and Firewall Director
- Used for Web configuration, Telnet, FTP, SNMP etc.
- Shows up on Checkpoint topology
- Must be on a trusted network
- Cannot be reached through the Firewall Accelerator

The IP address associated with the management interface is different from the Management IP (MIP) which is used in the ASF internal network only. This management interface address is used to access the Firewall Director from any management console, such as Check Point management console, BBI, and Telnet.

ASF Internal Network

This network is configured in the initial setup of the Bridging Firewall. The internal Management IP (MIP) address is configured automatically when you specify the ASF internal subnet's network address. Typically, if the subnet is X.X.X.0/24, then the internal MIP address is X.X.X.1. The Firewall Accelerators are assigned X.X.X.2, X.X.X.3, and X.X.X.4. Additional Firewall Directors are assigned IP addresses of the type X.X.X.5, X.X.X.6 and so on.

If you are using the “join” command to manually add a new Firewall director to an existing cluster, then you must know the internal network IP address of the Firewall Director.

For more information, see the section “[Use Setup for Basic Configuration](#)” in Chapter 3, “Initial Setup” of the *Installation and User's Guide*.

Check Point Configuration

- Uncheck anti-spoofing in the topology section for the management and sync network when configuring Check Point software.
- The Reject policy is handled the same way as the Drop policy.
- VPN, NAT, SYN defender, and services that require proxy are not supported.

Product Name Changes

The ASF components have been renamed for integration into Nortel Networks' larger vision for network security products. Although the manual uses the new product names, the information still applies to the Alteon Firewall Accelerator ("SFA") and Firewall Director ("SFD") products you may currently use.

The following table clarifies how the documentation describes your older ASF products:

Table 1 ASF Product Names

Component	Old Name	New Name
Firewall Accelerators	SFA-185	ASF 5700
	SFA-184	ASF 5600
Firewall Directors	SFD-310	ASF 5010

Documentation

The *ASF 3.1 Bridging Firewall Installation and User's Guide* (part number 212535-F) is available on the Web at <http://www.nortelnetworks.com/documentation>. Click on the Alteon Switched Firewall documentation link to access the ASF 3.1 manual. 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>).

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

Late-Breaking News

Please check your software and documentation for any readme.txt file. The readme file may contain important information regarding the product. View the file in any standard text editor.