

RELEASE NOTES:



Alteon Switched Firewall™ Release 3.2.1

Part Number: 215041-D, August 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-D.

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, Alteon Switched Firewall, ASF 5308, ASF 5408, ASF 5610, ASF 5710, Firewall OS, Firewall Director, ASF 5008, ASF 5010, Accelerator OS, 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, version 3.2.1 and higher. This supplement modifies information found in the complete documentation. Please keep this information with your Nortel Networks product manuals.

Documentation

The *Alteon Switched Firewall Installation and User's Guide* (part number 212535-E) is available on the Web. 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-E.

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.

Release 3.2.1 Changes

Software Support

Alteon Switched Firewall version 3.2.1 fully supports Check Point FireWall-1 NG with Application Intelligence software.

ASF 3.2.1 Upgrade

Alteon Switched Firewall version 3.0.4 can be upgraded to ASF 3.2.1. However, ASF 3.1 cannot be upgraded to ASF 3.2.1, because ASF 3.1 is a layer 2 or Bridging Firewall.

Third Party Configuration

If you are using Check Point FireWall-1 NG with Application Intelligence software, a new tab called “3rd Party Configuration” exists in the Gateway Cluster properties window. Select Load Sharing for the Cluster operating mode and select OPSEC as the 3rd party solution. Uncheck the other 3 options in the Gateway Cluster properties window.

Configurable Sync Devices

This feature allows you to configure Sync devices for Check Point Sync interface such as the 2 onboard 10/100/1000 interfaces on the Firewall Directors. This capability also allows you to configure the speed, auto-negotiation features of the Sync device.

DHCP Relay

In the Dynamic Host Configuration Protocol (DHCP) environment, the Alteon Switched Firewall acts as a relay agent allowing hosts or clients on an IP network to obtain their configurations from a DHCP server, thereby reducing network administration. ASF implementation of the DHCP relay agent eliminates the need to have DHCP/BOOTP servers on every subnet reducing the number of DHCP servers deployed on the network and centralizing management.

For more information on the DHCP Relay implementation in Alteon Switched Firewall 3.2.1, see the following section, [DHCP Relay Support](#) in this document.

Check Point's Built-in DHCP Service

Do not use Check Point's built-in DHCP services. Check Point's built-in DHCP services available in the SmartDashboard utility under Manage > Services > DHCP (dhcp-req-localmodule and dhcp-rep-localmodule) are not intended for DHCP Relay requests. Define your own DHCP service to allow DHCP relay. For more information on configuring DHCP relay, see [Configuring for DHCP Relay Agent](#) in this document.

Product Name Change

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	185	5700
	184	5600
	AD4	5400
	AD3	5300
Firewall Directors	310	5010
	308	5008

DHCP Relay Support

In the DHCP environment, the Alteon Switched Firewall acts as a relay agent. DHCP is described in RFC 2131, and the DHCP relay agent supported on the Alteon Switched Firewall is described in RFC 1542. DHCP uses UDP as its transport protocol. The client sends messages to the server on port 67 and the server sends messages to the client on port 68.

DHCP defines the methods through which clients can be assigned an IP address for a finite lease period and allowing reassignment of the IP address to another client later. Additionally, DHCP provides the mechanism for a client to gather other IP configuration parameters it needs to operate in the TCP/IP network.

The DHCP relay feature (`/cfg/net/dhcpr1`) enables the Firewall to forward a client request for an IP address to DHCP servers with IP addresses that have been configured on the Alteon Switched Firewall.

When Alteon Switched Firewall receives a UDP broadcast on port 67 from a DHCP client requesting an IP address, the request is then forwarded as a UDP Unicast MAC layer message to DHCP servers whose IP addresses are configured on the Firewall. The servers respond with a UDP Unicast message back to the Firewall, with the default gateway and IP address for the client. The destination IP address in the server response represents the interface address on the Alteon Switched Firewall that received the client request. This interface address tells the Alteon Switched Firewall on which VLAN to send the server response to the client.

Configuring for DHCP Relay Agent

To enable the Alteon Switched Firewall to be the DHCP forwarder, you need to configure the DHCP server IP addresses on the Firewall. You must enable DHCP relay on the interface connected to the client subnet.

The following figure shows a basic DHCP network example:

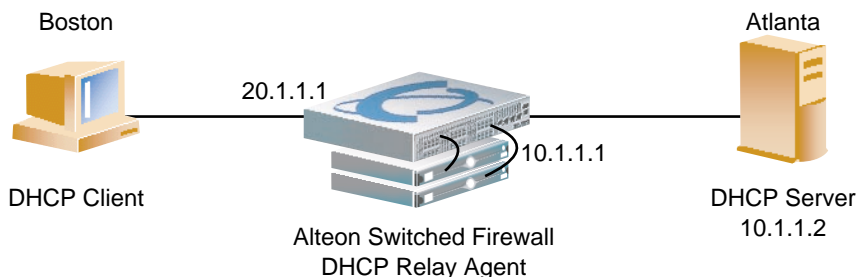


Figure 1 DHCP Relay Agent Configuration

The client request is forwarded to all DHCP servers configured on the Firewall. The use of two servers provide failover redundancy. However, no health checking is supported.

DHCP Relay functionality is assigned on a per interface basis. At least one server and one interface must be enabled for DHCP, otherwise the configuration will fail validation. Use the following commands to configure the Alteon Switched Firewall as a DHCP relay agent:

1. Enable DHCP Relay globally.

```
>> # /cfg/net/dhcpr1
>> DHCP Relay# ena
```

2. Configure DHCP requests to enter on this interface.

```
>> DHCP Relay# if 1  
>> DHCP Relay Interface 1# ena (Allow DHCP requests)
```

3. Configure DHCP server information.

```
>> # /cfg/net/dhcp1/server 1  
>> DHCP Server 1# addr 10.1.1.2 (Set IP address of 1st DHCP server)  
>> DHCP Server 1# ena (Enable the DHCP server)  
>> DHCP Server 1# ../server 2 (Set IP address of 2nd DHCP server)  
>> DHCP Server 2# addr 10.1.1.3 (Set IP address of 2nd DHCP server)  
>> DHCP Server 2# ena (Enable the DHCP server)
```

4. Display current configuration.

```
>> # /cfg/net/dhcp1/cur (Display current configuration)
```

5. Apply and save the changes.

```
>> DHCP Relay# apply
```

