Release Notes

Alteon Switched Firewall™ Bridge Mode

Release 3.1.2

Part Number: 216202-A, February 2004

NORTEL NETWORKS™

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

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 3.1.2 Bridging Firewall, ASF 5408, ASF 5610, ASF 5710, Firewall OS, Firewall Director, ASF 5008, ASF 5010, 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.

Check Point and SmartCenter are trademarks of Check Point Software Technologies Ltd. FireWall-1 and VPN-1 are registered trademarks of Check Point Software Technologies Ltd. Any other trademarks appearing in this manual are owned by their respective companies.

Originated in the USA.

Export

This product, software and related technology is subject to U.S. export control and may be subject to export or import regulations in other countries. Purchaser must strictly comply with all such laws and regulations. A license to export or reexport may be required by the U.S. Department of Commerce.

Licensing

This product includes software developed by Check Point Software Technologies (http://www.checkpoint.com). This product also contains software developed by other parties.

For more information, see Appendix D, "Software Licenses," in the *ASF 3.1 Bridging Firewall Installation and User's Guide* (part number 212535-E).

Common Criteria Certified Software

The ASF product has received Common Criteria Certification at assurance level EAL-4. The certified version of ASF software is 2.0.3.0.

Regulatory Compliance

International regulatory statements of conformity

This is to certify that the Nortel Networks 8000 Series chassis and components installed within the chassis were evaluated to the international regulatory standards for electromagnetic compliance (EMC) and safety and were found to have met the requirements for the following international standards:

- EMC - Electromagnetic Emissions – CISPR 22, Class A
- EMC - Electromagnetic Immunity – CISPR 24
- Electrical Safety – IEC 60950, with CB member national deviations

Further, the equipment has been certified as compliant with the national standards as detailed below.

National electromagnetic compliance (EMC) statements of compliance

FCC statement (USA only)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission (FCC) rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to take whatever measures may be necessary to correct the interference at their own expense.

ICES statement (Canada only)

Canadian Department of Communications Radio Interference Regulations

This digital apparatus does not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

CE marking statement (Europe only)

EN 55 022 statements

This is to certify that the Nortel Networks equipment are shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC. Conformity is declared by the application of EN 55 022 Class A (CISPR 22).

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case, the user may be required to take appropriate measures.

Achtung: Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Attention: Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilisateur de prendre les mesures spécifiques appropriées.

EN 55 024 statement

This is to certify that the Nortel Networks equipment is shielded against the susceptibility to radio interference in accordance with the application of Council Directive 89/336/EEC. Conformity is declared by the application of EN 55 024 (CISPR 24).

EC Declaration of Conformity

This product conforms to the provisions of the R&TTE Directive 1999/5/EC.

VCCI statement (Japan/Nippon only)

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI) for information technology equipment. If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

　この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

BSMI statement (Taiwan only)

This is a Class A product based on the standard of the Bureau of Standards, Metrology and Inspection (BSMI) CNS 13438, Class A.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者 會被要求採取某些適當的對策。

MIC notice (Republic of Korea only)

This device has been approved for use in Business applications only per the Class A requirements of the Republic of Korea Ministry of Information and Communications (MIC). This device may not be sold for use in a non-business application. Reference Regulatory label on the base of the equipment for specific Korean approval information.

National Safety Statements of Compliance

CE marking statement (Europe only)

EN 60 950 statement

This is to certify that the Nortel Networks equipment are in compliance with the requirements of EN 60 950 in accordance with the Low Voltage Directive. Additional national differences for all European Union countries have been evaluated for compliance. Some components installed within the 8000 Series chassis may use a nickel-metal hydride (NiMH) and/or lithium-ion battery. The NiMH and lithium-ion batteries are long-life batteries, and it is very possible that you will never need to replace them. However, should you need to replace them, refer to the individual component manual for directions on replacement and disposal of the battery.

Lithium Battery Cautions

Caution—This product contains a lithium battery. Batteries are not customer replaceable parts. They may explode if mishandled. Do not dispose of the battery in fire. Do not disassemble or recharge.

(Norge) ADVARSEL—Litiumbatteri - Eksplosjonsfare. Ved utskifting benyttes kun batteri som anbefalt av apparatfabrikanten. Brukt batteri returneres apparatleverandøren.

(Sverige) VARNING—Explosionsfara vid felaktigt batteribyte. Använd samma batterityp eller en ekvivalent typ som rekommenderas av apparattillverkaren. Kassera använt batteri enligt fabrikantens instruktion.

(Danmark) ADVARSEL! Litiumbatteri - Eksplosionsfare ved fejlagtig håndtering. Udskiftning må kun ske med batteri af samme fabrikat og type. Levér det brugte batteri tilbage til leverandøren.

(Suomi) VAROITUS—Paristo voi räjähtää, jos se on virheellisesti asennettu. Vaihda paristo ainoastaan laitevalmistajan suosittelemaan tyyppiin. Hävitä käytetty paristo valmistajan ohjeiden mukaisesti.

Safety Information

Caution—Nortel Networks products are designed to work with single-phase power systems having a grounded neutral conductor. To reduce the risk of electric shock, do not plug Nortel Networks products into any other type of power system. Contact your facilities manager or a qualified electrician if you are not sure what type of power is supplied to your building.

Caution—Not all power cords have the same ratings. Household extension cords do not have overload protection and are not meant for use with computer systems. Do not use household extension cords with your Nortel Networks product.

Caution—Your Nortel Networks product is shipped with a grounding type (three-wire) power cord. To reduce the risk of electric shock, always plug the cord into a grounded power outlet.

NOM statement (Mexico only)

The following information is provided on the devices described in this document in compliance with the safety requirements of the Norma Oficial Méxicana (NOM):

Exporter:Nortel Networks, Inc.
4655 Great America Parkway
Santa Clara CA 95054 USA

Importer:Nortel Networks de México, S.A. de C.V.
Avenida Insurgentes Sur #1605
Piso 30, Oficina
Col. San Jose Insurgentes
Deleg-Benito Juarez
México D.F. 03900

Tel:52 5 480 2100

Fax: 52 5 480 2199

Input:100 to 240 VAC, 50 to 60 Hz, 9 A max. per power supply
single supply, or + one redundant supply configurations

Información NOM (unicamente para México)

La información siguiente se proporciona en el dispositivo o en los dispositivos descritos en este documento, en cumplimiento con los requisitos de la Norma Oficial Méxicana (NOM):

Exportador: Nortel Networks, Inc.
4655 Great America Parkway
Santa Clara, CA 95054 USA

Importador: Nortel Networks de México, S.A. de C.V.
Avenida Insurgentes Sur #1605
Piso 30, Oficina
Col. San Jose Insurgentes
Deleg-Benito Juarez
México D.F. 03900

Tel: 52 5 480 2100

Fax:52 5 480 2199

Embarcar a:100 to 240 V CA, 50 to 60 Hz, 9 A max. por fuente de poder
una fuente o una + configuraciones de una fuente redundante

Release Notes

These release notes provide the latest information regarding your Alteon Switched Firewall (ASF) release 3.1.2. ASF 3.1.2 is a bridging or layer 2 firewall. A bridging firewall functions as a bridge whereas a layer 3 firewall functions as a router. This firewall is also called a transparent or stealth firewall because it is effectively invisible on the network.

This document is a supplement to the *ASF 3.1 Bridging Firewall Installation and User's Guide* (part number 212535-F). Refer to the this document for additional technical questions regarding the product architecture and features.

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.

Release 3.1.2 Changes

The following topics are discussed in these Release Notes:

- Software Support on this page
- New Director Support on this page
- “Mixing Director Types” on page 13
- “Support for Newer Versions of OpenSSH and OpenSSL” on page 13
- “Check Point Anti-spoofing Support” on page 14
- “Layer 2 Filter Menu” on page 19
- “ASF Combinations” on page 20

Software Support

ASF 3.1.2 Bridging Firewall is supported on

- Check Point™ FireWall-1® NG software with Feature Pack 3 (FP3) Hotfix Accumulator, number 315 (HFA_315)
- Check Point Express™

This version of ASF software is supported on Linux 2.4 kernel.

ASF 3.1.2 can be upgraded from ASF 3.1.1.x only.

New Director Support

ASF 3.1.2 is supported on Director 5014. This section describes the Firewall Director 5014 as shown in Table 1 and in Figure 1.

Table 1 Firewall Director 5014 Hardware Features

Firewall Director 5014	Features
Port capacity	■ Two Fiber Gig with LC connector ■ Two 10/100/1000 BaseT Copper Gigabit Ethernet Ports
RAM	1 GB
Hard disk capacity	40 GB
Dimension/Chassis	1U, 20-inch rack-mount
Power supply	Single

.

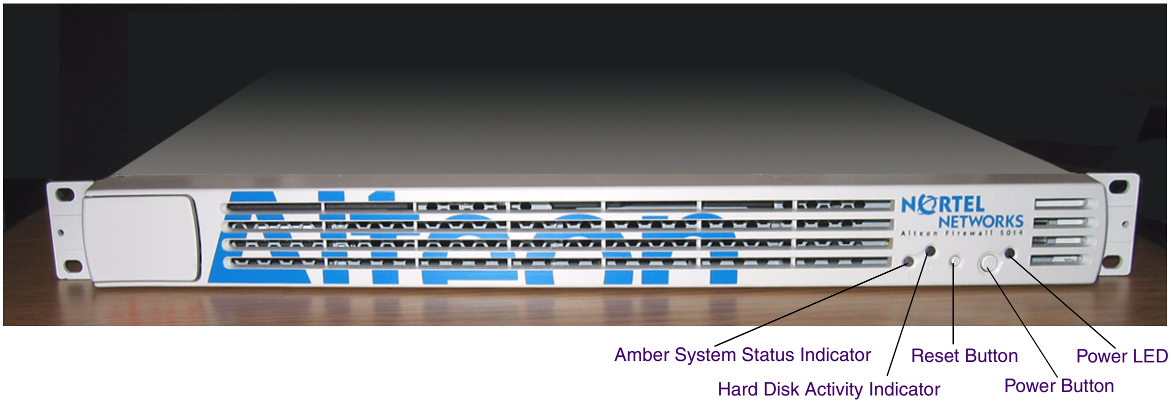


Figure 1 Front Panel of the Firewall Director 5014 with the Bezel

Table 2 describes the front panel LEDs shown in Figure 1.

Table 2 Firewall Director 5014 Front Panel LEDs

LED	Description
Amber system status indicator !	The amber system status indicator lights up when the system needs attention due to a problem. LED is normally off. If the system detects a problem with any of the system voltages, temperature sensors, or fans, this LED blinks amber.When the system is reset, the LED is off. When the system is running, this LED displays solid green. If the system hangs, the LED flashes.
Hard-disk drive activity indicator ⛁	This LED blinks when activity is detected on the hard-disk drive.
System power indicator ⏻	This LED is green when the power supply is turned on.

The front panel LEDs are duplicated on the back-panel.

Removing and Installing the Bezel

To remove the bezel off the Firewall Director 5014, open the flap (See ➋ in Figure 2) and slide the bezel to the right. Then, pull the bezel off the faceplate.

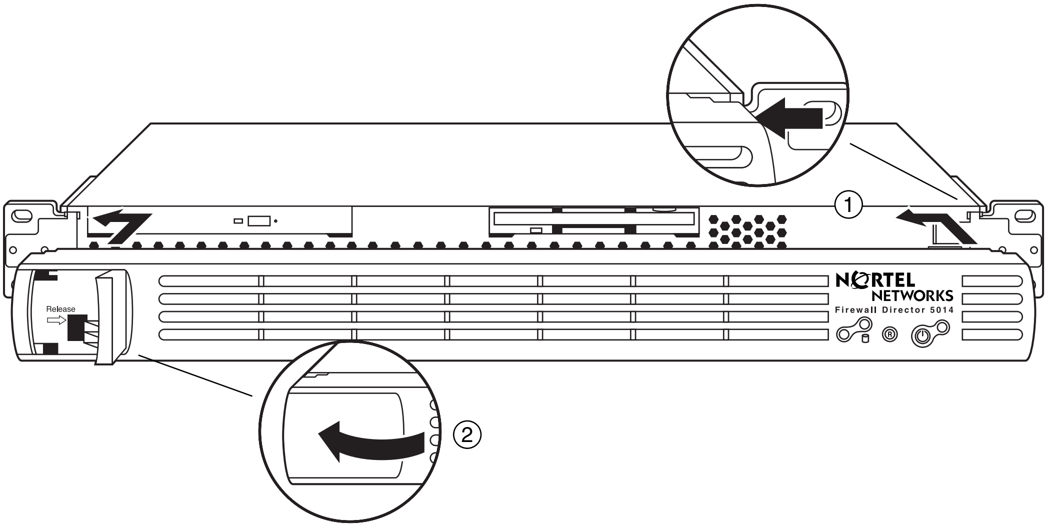


Figure 2 Installing the Bezel on the Firewall Director 5014

To install the bezel, slide the bezel on the face plate as shown in Figure 2 and follow the steps below:

1. **Lift the flap that is located at the left end of the bezel.**
2. **Slide the bezel on the face plate from right to left, until the edge of the bezel aligns with the edge of the face plate lengthwise. (See ➀ in Figure 2.)**
3. **Keep sliding all the way over until you hear a click, which means the bezel has locked on to the face plate.**
4. **Shut the flap. (See ➋ in Figure 2.)**

Front Panel Without the Bezel

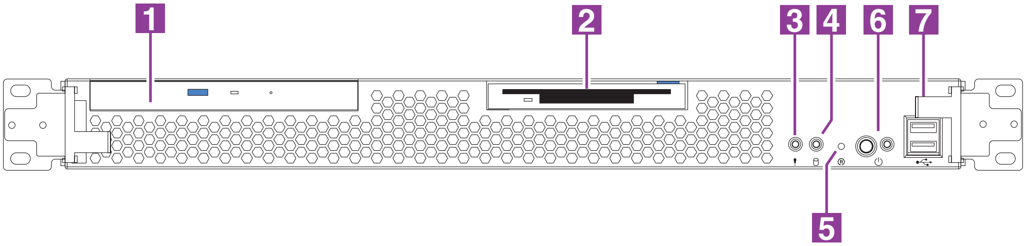


Figure 3 Front Panel of Firewall Director 5014 with Bezel Removed

1. **CD-ROM drive**
2. **Floppy diskette drive**
3. **System error LED (amber)**
4. **Hard disk activity LED (green)**
5. **Reset button**
6. **Power button (left) and power LED (green)**
7. **Universal Serial Bus (USB) connectors (not supported)**

Rear Panel

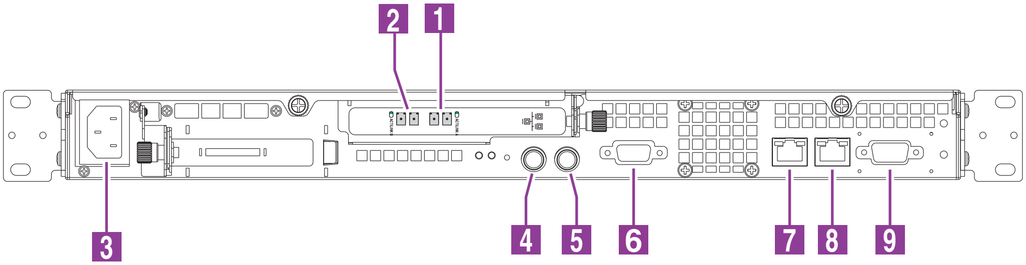


Figure 4 Rear Panel of the Firewall Director 5014

1. **Gigabit Port 1 with LC connector: 1000Base-SX Multimode Fiber Ethernet**

   Use this port to connect to the Accelerator.

2. **Gigabit Port 2 with LC connector: 1000Base-SX Multimode Fiber Ethernet**

   (See *ASF 3.1 Bridging Firewall Installation and User's Guide* for ports 1-2 LED status conditions.)

3. **AC Receptacle**

4. **Keyboard Connector (not supported)**

5. **Mouse Connector (not supported)**

6. **Video Connector (not supported)**

7. **Port 1: 10/100/1000Base-T copper Ethernet port**

   Use this port to connect to the management server.

8. **Port 2: 10/100/1000Base-T copper Ethernet port**

   Use this port for Check Point synchronization.

   (See *ASF 3.1 Bridging Firewall Installation and User's Guide* for ports 1 and 2 LED status conditions.)

9. **Serial Connector (DTE) for system configuration and diagnostics (console connection)**

   Refer to the *ASF 3.1 Bridging Firewall Installation and User's Guide* to install and mount the Director.

Mixing Director Types

ASF 3.1.2 does not support different models of the Director in the same cluster. For example, you cannot mix Directors 5010 and 5014 in the same cluster.

Support for Newer Versions of OpenSSH and OpenSSL

ASF 3.1.2 includes newer versions of OpenSSL and OpenSSH with fixes for the following vulnerabilities:

- Buffer management vulnerability (CERT® Advisory CA-2003-24 Buffer Management Vulnerability in OpenSSH)
- Multiple vulnerabilities in SSL/TLS Implementations (CERT® Advisory CA-2003-26 Multiple Vulnerabilities in SSL/TLS Implementations)

Check Point Anti-spoofing Support

ASF 3.1.2 supports Check Point anti-spoofing. To support this feature you must manually enter the enforcement ports for every Director and define the IP addresses behind the interface.

Follow the step-by-step procedure to configure Check Point anti-spoofing support on ASF:

1. **Launch the SmartDashboard software from the Check Point management console.**

2. **Select Network and create Network objects for networks that are reachable from every "internal" port.**

   This would include the network the port is on. See the sample configuration on "Configuration Example" on page 17.

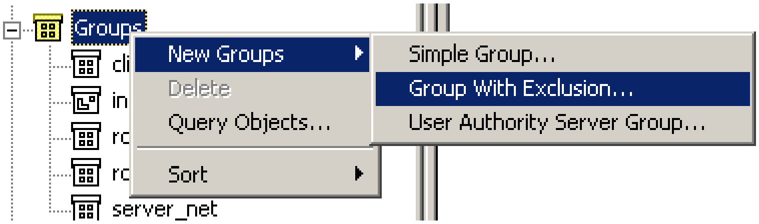
3. **Select Node and create a Host/Node object for every system that would be on the external side of the Firewall.**

4. **For each internal port, combine all networks reachable from it into a Simple Group object, by clicking on Groups >New Groups >Simple Group.**

   See the sample configuration on "Configuration Example" on page 17.

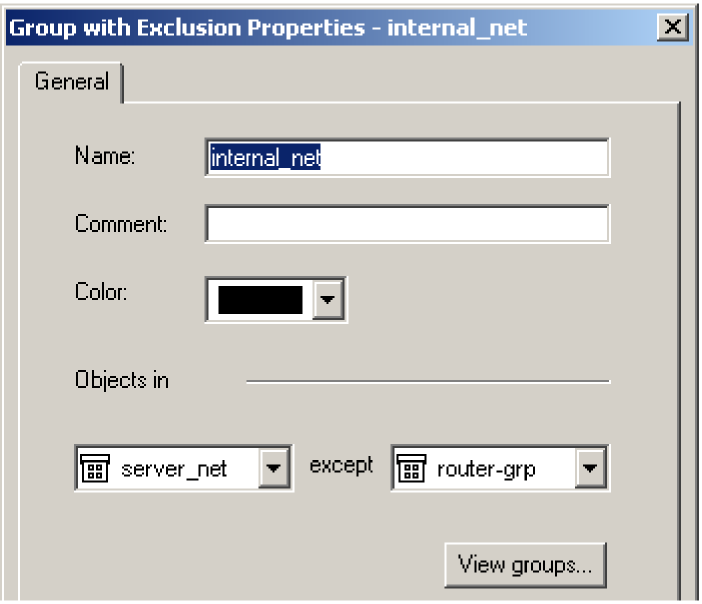
5. **Combine the Host/Node objects into a Simple Group object. Click Groups >New Groups >Simple Group.**

6. **Create a Group with Exclusion object. Click Groups >New Groups >Group With Exclusion.**



See the sample configuration in Figure 6 on page 18.

For each Simple Group object with networks, create a Group with Exclusion object. The “Objects in Group” is the group of networks and the “except” group is the group of hosts on the external side, as shown below.



Group with Exclusion Properties - internal_net

Name: internal_net

Comment:

Color:

Objects in

server_net except router-grp

7. **From the Check Point Main menu, open the Topology tab for the cluster Director. Click Check Point > L2 cluster > SFD.**

   The initial topology is empty (unlike the individual Directors, where the management and sync interfaces are visible).

8. **Click Get Topology.**

   Get Topology gets the sync and management networks.

9. **Click Add and manually add the enforcement interfaces.**

   An arbitrary IP address and a network mask 255.255.255.255 are required. These addresses are not used, but they must be unique for each Director and they should not exist on the network, because packets from these addresses are refused.

   The Interface Name option must correspond to the name `ifconfig` displays in the CLI menu. If the default VLAN is used and a port is not trunked, the interface name is “p” followed by the port number. If a VLAN is explicitly defined, a “-” followed by the VLAN Id is appended. For trunked ports, the list of ports contained in that trunk is used (for example, p12-10 is a trunk of ports 1 and 2 on VLAN 10).

Note – Do not click "Get Topology" after you manually add the enforcement interfaces. This will delete the newly added enforcement interfaces.

10. **Click the Topology tab in the Interface Properties dialog box and select one of the following:**

    - External

      Select External if the port faces the outside world.

    - Internal

      Select Internal and Specific.

      Choose the correct Group with Exclusion to define the IP addresses reachable from this port.

    A check mark appears automatically for the "Perform Anti-Spoofing based on interface topology" option.

11. **Push the policy to activate the anti-spoofing definitions.**

Configuration Example

Figure 5 shows an sample topology of layer 2 firewall. Port 1, 2, and 3 on the ASF are connected to networks. Ports 1 and 2 are internal ports (connected to the internal side). Port 1 is connected to a gateway to networks 10.20.1.0 and 10.30.1.0. Port 2 is connected to a hub with hosts but no gateway on the subnet 10.10.1.0. Port 3 is connected to a router (10.10.1.1), which connects to the outside world.

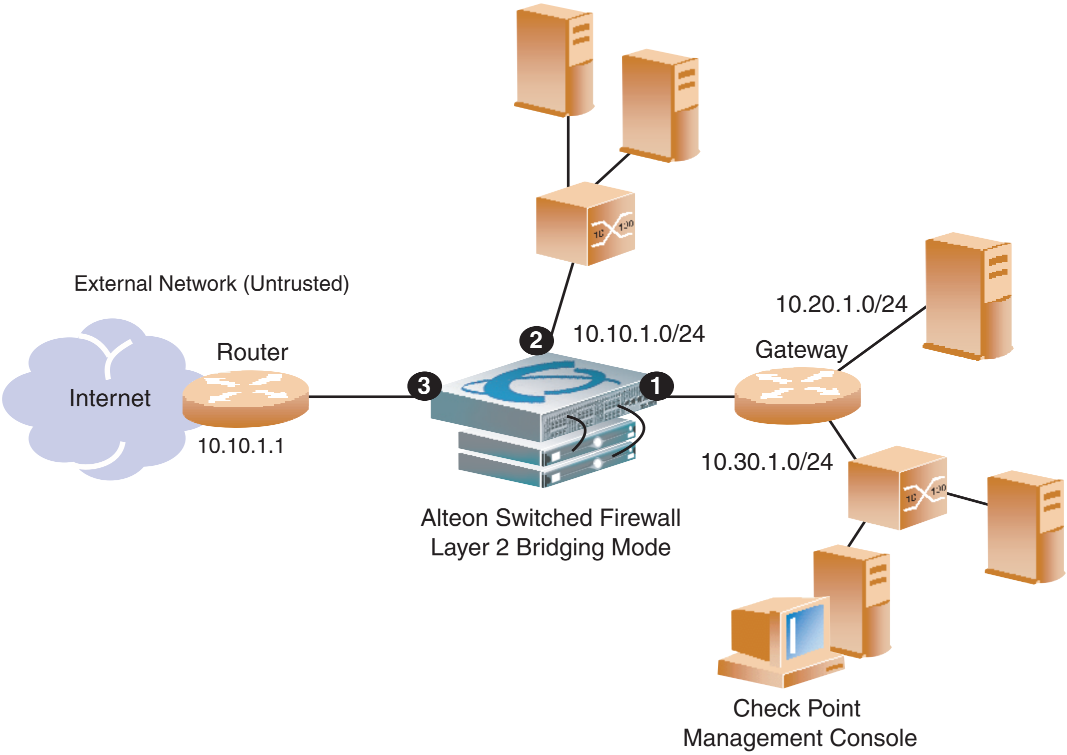


Figure 5 Check Point Anti-spoofing Configuration

1. **Create three network objects (one each for 10.10.1.0, 10.20.1.0, and 10.30.1.0).**

   You do not need to create a network object for port 3 (10.10.1.1), because it is an external port.

2. **Create a Host/Node object for IP address 10.10.1.1.**

3. **Create a Simple Group containing the three networks and a Simple Group for the Host/ Node object.**

Create three Simple Group objects: a Simple Group containing the three networks 10.10.1.0, 10.20.1.0 and 10.30.1.0, another Simple Group containing network 10.10.1.0 only, and a Simple Group containing 10.10.1.1 (the router group). Create two objects with exclusion by combining the network groups with the host/node (router) group as shown below.

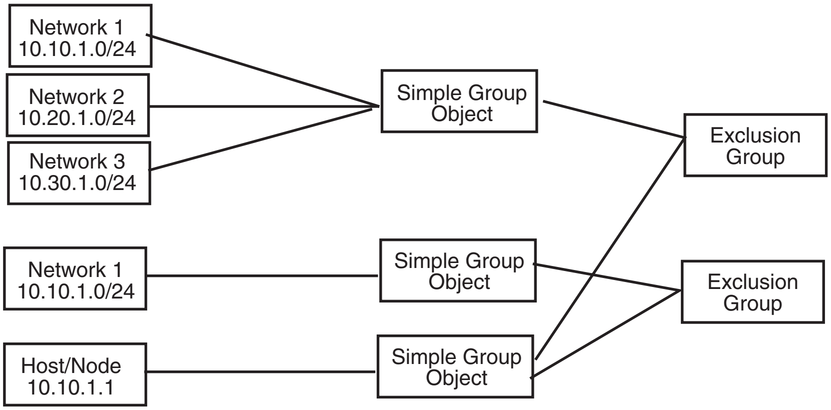


Figure 6 Creating Exclusion Groups

NOTE – If you are not concerned with spoofing on the internal side you could simply use the same group with exclusion for all internal ports and save creating one network group and one group with exclusion.

4. **Add the interfaces to the cluster Director.**

   Add the interfaces p1, p2, and p3 to the topology of the cluster Director, choosing the addresses 1.1.1.1, 1.1.1.2 and 1.1.1.3 respectively with the network mask 255.255.255.255. Make p1 and p2 interfaces internal with the specific Group with Exclusion and p3 external.

5. **Push the policy to activate the anti-spoofing definitions.**

Layer 2 Filter Menu

Configure a layer 2 filter to allow non-IP and non-ARP multicast traffic bypass the firewall. For example, you can configure a layer 2 filter to allow BPDU packets for spanning tree or a GVRP packets. By default, non-IP and non-ARP packets are dropped unless specified in this layer 2 filter.

The Layer 2 Filter menu is configured using the Command Line Interface (CLI) or the Browser-Based Interface (BBI). If you are using the CLI, the layer 2 filter command is configured at `/cfg/net/adv/l2filt` <#>. Each of the menu commands in the Layer 2 Filter menu is explained in the following section.

`/cfg/net/adv/l2filter` *<filter number>*

Layer 2 Filter Definition Menu

```
[Layer 2 Filter Definition 1 Menu]
     dmac        - Set Destination MAC
     ethtype     - Set Ether type
     ena         - Enable filter
     dis         - Disable filter
     del         - Remove Layer 2 Filter Definition
     cur         - Display current settings
```

The Layer 2 Filter menu allows you to specify non-IP and non ARP packets to bypass the firewall. ASF 3.1.2 software lets you define up to 4 layer 2 filters.

Table 3 Layer 2 Filter Menu (/cfg/net/adv/l2filter)

Command Syntax and Usage
`dmac any`|**`stp`**|**`bmga`**|**`gmrp`**|**`gvrp`**|*<destination MAC address>* This command sets the destination MAC address of non-IP and non-ARP packets to bypass the firewall. You can select either the built-in options (`stp`, `bmga`, `gmrp`, `gvrp`) or enter a *destination MAC address* (for example, 00:60:cf:40:56:00) for a specific packet type. The built-in options are translated to their respective destination MAC addresses. The default option `any` affects all packet types.
`ethtype any`|**`ether type`** *<in hexadecimal>* This command allows you to specify the ether type for non-IP and non-ARP packets to bypass the firewall. The ether type must be specified in hexadecimal, for example `1f02`. The default is `any`.

Table 3 Layer 2 Filter Menu (/cfg/net/adv/l2filter)

Command Syntax and Usage
`ena` This command enables this filter.
`dis` This command disables this filter.
`del` This command removes this filter from the cluster configuration.
`cur` This command displays current settings for all items in the Layer 2 Filter menu.

ASF Combinations

Typically, Firewall capacity refers to higher throughput, concurrent sessions, and sessions per second. Higher throughput and concurrent sessions are determined by the Firewall Accelerator model and sessions per second are determined by the Firewall Director model.

Use compatible ASF 3.1.2 Bridging Firewall components as shown in Table 4 to achieve the desired performance.

Table 4 Supported Combinations for ASF 3.1.2

ASF	Firewall Accelerator Models	Firewall Director Models
5714	5700	5014
5710	5700	5010
5614	5600	5014
5610	5600	5010

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.