



>THIS IS THE WAY

>THIS IS NORTEL™

Product Brief

Nortel Switched Firewall 6000 Series

A layered defense combining the industry's best security firewall with the industry's best network switching and acceleration

> Nortel Switched Firewall with Firewall-1 from Check Point has both network-level and application-level protection.

For example, it guards against:

- > Denial of Service attacks
- > Oversized packets
- > SYN floods
- > Fragmentation attacks
- > Nimda
- > Code Red
- > Cross Site Scripting and other network- or application-based attacks

> FireWall-1 has the broadest application support in the industry. Its support for over 150 pre-defined applications helps to ensure that any Web services deployment can traverse the Switched Firewall without performance limitations.

Application examples include:

- > Microsoft CIFS
- > SMTP, FTP, HTTP, DNS and telnet traffic
- > SOAP/XML
- > Instant Messaging and Peer-to-Peer applications
- > Windows Media, RealVideo and Session Initiation Protocol (SIP)
- > H.323-based services, including Voice over IP (VoIP) and NetMeeting
- > Oracle SQL and ERP

Network threats and attacks are on the rise. Organizations are using the network to gain competitive advantage. Convergence of network resources drives cost savings and productivity while improving customer engagement. But, an unprotected or poorly protected network is not a competitive advantage.

The network should be protected by the best security firewall available. This is why Nortel has partnered with Check Point Software Technologies to create the Nortel Switched Firewall (formerly known as Alteon* Switched Firewall).

The Nortel Switched Firewall is ideal for deployment in large enterprise environments, and is certified under the Check Point Open Platform for Security (OPSEC) criteria and enhances the Firewall-1 deployment with unique services and capabilities:

- > Intelligent security with high performance
 - Throughput of 7 Gbps
 - Connections per second of 20,000 to 100,000
 - Concurrent sessions of 1,000,000



- › Plug-and-play deployment and expansion with a single-system-image that is easy to manage and maintain
- › Multi-layer packet inspection for extra protection from advanced hackers and attackers
- › Switch-based acceleration that off-loads CPU processing and minimizes impact on next-generation multi-media, SIP and VoIP services
- › Device load-balancing for advanced support of IDS or Nortel's Threat Protection System
- › Active-active configurations for high availability environments where 99.999 percent application and service availability is a must

Customers that have deployed Nortel Switched Firewall receive these benefits:

- › Support for SIP services with no performance impact
- › The combined security and networking expertise of Nortel and Check Point
- › The easy of transition and enhanced performance from a server-based to switch-based solution — no technical retraining required
- › Reduced operating costs with fewer firewalls and fewer licenses to manage with the same or better performance

Switched Firewall—defined

Any firewall has two basic functions:

- › *Policy Inspection*—Inspect all traffic and compare it to defined security rules

- › *Policy Enforcement and Data Forwarding*—Forward or block traffic based on the rules and signatures

In addition, today's firewalls must be application aware. This means that policy inspection occurs within the application data to help ensure that no attacks, viruses or worms are transported across the firewall.

The Nortel Switched Firewall 6000 series is a key component in Nortel's layered defense strategy. It separates the Policy Inspection function from the Policy Enforcement and Data Forwarding function. This results in a high-performance system that is optimized to support today's applications and services while protecting the network from today's threats. The benefits of this include:

- › Wire-speed packet forwarding for assured performance
- › Simplified network topology for easier management and troubleshooting
- › Rapid service restoration using common protocols
- › Protection from application-level attacks via Check Point Smart Defense functionality

Nortel Switched Firewalls are also available for stand-alone deployment. These include 5106, 5109 and 5114. Please see the Nortel Switched Firewall 5100 Series product brief for more information.

Accelerated performance

The Nortel Switched Firewall System 6414 consists of a Switched Firewall Accelerator (SFA) 6400 and a Switched Firewall Director (SFD) 5014. The Nortel Switched Firewall System 6614 uses a Switched Firewall Accelerator 6600 with a 5014. Initial packets in any session are sent by the SFA to the SFD for policy inspection. The SFD returns the packets to the SFA with instructions for handling subsequent packets. For most traffic, the SFA 6400 or 6600 performs deep-packet inspection that results in up to 90 percent of all packets being safely forwarded with hardware-based inspection as prescribed by the core firewall logic in the SFD. The resultant throughput is 5.0 Gbps for the 6414 and 7.0 Gbps for the 6614. This enables the system to use the core firewall resources to inspect and connect a much higher number of concurrent sessions and to deal with a higher number of connection requests per second. This kind of performance is critical in any Web services deployment that will undergo periods of heavy demand. Traditional implementations would require expensive extra resources to deal with the expected peak traffic loads.

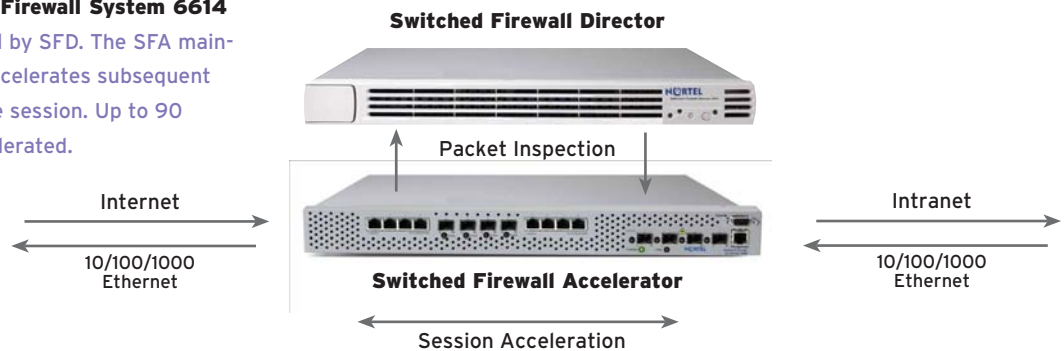
In addition, the Nortel Switched Firewall Accelerator 6400 and 6600 provide integrated Layer 2 through Layer 7 Content Filtering, Load Balancing, VLAN Tagging and Network Address Translation.

Nortel Switched Firewall System



Figure 2. Nortel Switched Firewall System 6614

Initial packets are inspected by SFD. The SFA maintains a session entry and accelerates subsequent packets from the same, safe session. Up to 90 percent of packets are accelerated.



Key applications—Nortel Switched Firewall System 6414 and 6614

Layer 2 through Layer 7 Content Filtering

The Switched Firewall System performs full inspection of any IP application header or payload. This information is used to apply firewall rules to the network data flows. This capability enables the switched firewall to block attacks and unauthorized traffic before there is any chance for performance degradation or network outage. Up to 224 filtering rules can be configured to allow or deny traffic based on application type, protocol type and IP source/destination addresses.

Device Load Balancing

Up to six Switched Firewall Directors can be load balanced with a single Switched Firewall Accelerator. Health checks are performed to ensure availability. In addition, Intrusion Detection Systems (IDSs) can be load balanced from the Switched Firewall System. Multiple systems may be run in parallel across multiple security zones or VLANs with the Switched Firewall System, ensuring that all sessions and all frames are sent to the same IDS system.

VLAN Tagging

With IEEE 802.1q support, each VLAN is supported as a separate firewall interface. Up to 242 individual

VLANs are supported. Unique security policies may be implemented and enforced for each VLAN. This makes the 6414 and 6614 ideal for deployment in multi-tenant or multi-department environments where unique security policies and inter-VLAN policy inspection are required. Examples include airports, government offices, malls, stadiums, schools, universities and hospitals.

Network Address Translation

The Nortel Switched Firewall System performs Network Address Translation (NAT) to preserve and hide organizational IP addresses. With this accelerated NAT function performed in the switch hardware, the core firewall system devotes its resources to session connections and complex security concerns — there is no performance or throughput degradation. Traditional firewalls often cause degradations in network performance and throughput when invoking NAT functions.

Solution benefits

Low total cost of ownership

Network traffic is growing. Organizational dependence on communication and interaction means that security solutions which are cost-effective and can grow to meet future demand must be deployed. The Nortel Switched Firewall System 6414 and 6614 can both grow to meet future demand.

An initial system with one Switched Firewall Director supports 20,000 session connection requests per second. As the network traffic increases, a second Director can be easily added with automatic configuration and no service disruption. Up to six Directors can be supported by a Switched Firewall Accelerator to provide up to 100,000 session connection requests per second, and 1,000,000 total concurrent sessions. Managing a Switched Firewall System is easy. A Single System Image controls all configuration data, including physical interfaces, VLANs, IP interfaces, routing protocols and administrative settings. This data is securely and automatically shared within the Switched Firewall cluster. In addition, the cluster is managed through a single IP address, making it easy to perform configuration changes, backup configuration data and update software for all units in the cluster.

Existing Check Point customers may reuse their existing license to easily move their firewall onto any Nortel Switched Firewall System.

Enhanced performance supporting productivity

Companies are deploying voice over IP (VoIP) and Session Initiation Protocol (SIP) services to enhance productivity. The added flexibility and mobility from these services means that VoIP and SIP traffic will need to traverse the firewall. This can present many problems.

Traditional firewalls may not support the complexity of signaling used by these services. Many existing firewall implementations add too much delay or jitter into the media path and adversely affect the voice or multimedia quality. The Nortel Switched Firewall System is optimized to support VoIP and SIP services. High packet throughput to minimize delay, VoIP and SIP application awareness and virtually jitter-free performance are fundamental to its design and function.

Carrier-class availability for assured customer connection

Network availability, reliable service and application performance are critical to any organization's IT strategy. Active-Active High Availability in the Switched Firewall System enables automatic failover to other Switched Firewall Directors in the security cluster. This eliminates single points of failure in the network.

The High-Availability configuration uses two Switched Firewall Accelerators and supports in-service upgrades so that the firewall system never needs to be taken out of service.



Nortel Switched Firewall product matrix

Model/feature	Standalone Firewalls for SME and Branch			Accelerated Firewall Systems for larger enterprise and data centers	
	5106	5109	5114	6414	6614
Throughput (Gbps)	0.350	1.2	1.6	5.0	7.0
Connections per sec ¹	3,600	10,000	10,000	20,000/Director	20,000/Director
Accelerated concurrent sessions	0	0	0	500,000	500,000
Total concurrent sessions	250,000	300,000	500,000	1,000,000	1,000,000
Layer 3 protocols	OSPF	OSPF	OSPF	OSPF, RIP 1 & 2	OSPF, RIP 1 & 2
Virtual Firewalls	No	No	Yes - 250	No	No
VLANs/IEEE 802.1q	Yes - up to 250	Yes - up to 250	Yes - up to 250	Yes - up to 242	Yes - up to 242
Health checks and load balancing	No	No	No	Yes	Yes
Multi-link trunking	No	No	No	Yes	Yes
Plug-and-play	No	No	No	Yes	Yes
Single system image upgrade	Yes	Yes	Yes	Yes	Yes
Expansion options	No	Via upgrade	Via upgrade	Yes	Yes
High availability	Yes	Yes	Yes	Yes	Yes
Ethernet TX ports: 10/100	2	4	0	24	0
Ethernet TX ports: 10/100/1000	2	2	2	0	8 ²
Ethernet Fiber ports	0	0	2 x 1000SX	4 x GBIC	8 x GBIC ²

Notes:

- Multiple Directors (up to 6) can be load balanced to achieve up to 100,000 connections per second in a cluster.
- Any 12 ports can be enabled at one time on the Switched Firewall Accelerator 6600.

Product specifications

Part numbers and description

- EB 1639114 - Switched Firewall System 6614, complete with Accelerator and Director
- EB 1639113 - Switched Firewall Accelerator 6600, to create a High Availability configuration
- EB 1639108 - Switched Firewall System 6414, complete with Accelerator and Director
- EB 1639067 - Switched Firewall Accelerator 6400, to create a High Availability configuration
- EB 1639069 - Switched Firewall Director 5014

Interfaces

Accelerator:

- 10/100/1000BASE-TX Port 10/100/1000 full or half-duplex (auto-negotiation) with RJ-45 UTP port
- 1000BASE-SX Port 1-port 1000BASE-SX SFP GBIC (Con. Type: LC)
- 1000BASE-LX Port 1-port 1000BASE-LX SFP GBIC (Con. Type: LC)
- RS-232C Console DB-9 serial connection, female DCE interface for out-of-band management

Director:

- 10BASE-T/100BASE-TX Port 10/100 full or half-duplex (auto-negotiation) with RJ-45 UTP port
- 1000BASE-SX Port Full-duplex Gigabit Ethernet with SC fiber connector
- RS-232C Console DB-9 serial connection, female DCE interface for out-of-band management

Dimensions

	<i>Accelerator:</i>	<i>Director:</i>
Height	1.75 inches (4.44 cm)	1.75 inches (4.44 cm)
Width	17.61 inches (44.0 cm)	16.69 inches (42.39 cm)
Depth	20 inches (50.8 cm)	16.53 inches (42.01 cm)
Weight	21 lbs (9.53 kg) (Standard 19" EIA 1U rack mountable)	19 lbs (8.6 kg) (Standard 19" EIA 1U rack mountable)

Technical specifications

- IP routing interfaces: 256
- VLANs: 242
- Default gateways: 4
- Trunk groups: 12

Network protocol and standards compatibility

- 10BASE-T/100BASE-TX/1000BASE-TX (IEEE 802.3-2000)
- 1000BASE-SX/LX (IEEE 802.3z)
- Logical link control (IEEE 802.2)
- Flow control (IEEE 802.3x)
- Link negotiation (IEEE 802.3z)
- Port Trunking (IEEE 802.3d)
- VLANs (IEEE 802.1Q): Frame tagging on all ports when LANs enabled
- IP (RFC 791)
- ICMP (RFC 792)
- ARP (RFC 826)
- RIP 1 (RFC 1058), RIP 2 (RFC 1723)
- OSPF with md5 authentication (RFC 2328)
- VRRP (RFC 2338)
- CIDR (RFC 1519)
- TFTP (RFC 783), FTP (RFC 959)
- Telnet (RFC 854)
- SSH v1/v2
- SSL/TLS (RFC 2246)
- DVMRP (RFC 1075)
- IGMP (RFC 2236)
- BootP/DHCP Relay (RFC 2131)
- SNMPv2c (RFCs 1901, 1905, 1906, 1907, 2578, 2579, 2580)
- SNMPv3 (RFCs 2570, 2571, 2572, 2573, 2574, 2575)

Power specifications

- Auto-ranging power supply: 00-240 VAC @ 3.5 Amps, 50-60 Hz
- Maximum power consumption: 250 Watts
- MTBF: >50,000 hours

Environmental specifications

- Operating temperature: 10° to 35° C (+45° to +100° F)
- Operating humidity: 8% to 80% (non-condensing)

Certifications

EMC: (Electromagnetic requirements)

- USA: FCC Part 15, Subpart B Class A
- Australia: AS/NZS CISPR 22:2002
- Canada: ICES-003
- Japan: VCCI Class A
- Europe: EN 300 386 v1.3.1 (2001-09)
- Taiwan: BSMI Registration Certificate
- Rest of World: CISPR 22 Class A

Emissions:

- US- FCC Class B
- Canada- DOC Class B
- Europe- CE Mark to EN55022/EN50082-1/ICE 801-2/ICE 801-3/ICE 801-4

Industry:

- EAL-4 (in progress)
- OPSEC
- ICSA

Safety

- IEC 60950 (International)
- National Deviation per CB Member Countries to IEC 60950
- UL 1950 (USA)
- CSA 22.2, No. 950 (Canada)
- EN 60950 (Europe)

In the United States:

Nortel
35 Davis Drive
Research Triangle Park, NC 27709 USA

In Canada:

Nortel
8200 Dixie Road, Suite 100
Brampton, Ontario L6T 5P6 Canada

In Caribbean and Latin America:

Nortel
1500 Concorde Terrace
Sunrise, FL 33323 USA

In Europe:

Nortel
Maidenhead Office Park, Westacott Way
Maidenhead Berkshire SL6 3QH UK

In Asia Pacific:

Nortel
Nortel Networks Centre
1 Innovation Drive
Macquarie University Research Park
Macquarie Park NSW 2109 Australia
Tel: +61 2 8870 5000

In Greater China:

Nortel
Sun Dong An Plaza, 138 Wang Fu Jing Street
Beijing 100006, China
Phone: (86) 10 6528 8877

Nortel is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Serving both service provider and enterprise customers, Nortel delivers innovative technology solutions encompassing end-to-end broadband, Voice over IP, multimedia services and applications, and wireless broadband designed to help people solve the world's greatest challenges. Nortel does business in more than 150 countries. For more information, visit Nortel on the Web at www.nortel.com.

For more information, contact your Nortel representative, or call 1-800-4 NORTEL or 1-800-466-7835 from anywhere in North America.

This is the Way. This is Nortel, Nortel, the Nortel logo, the Globemark, and Alteon are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Copyright © 2004 Nortel Networks. All rights reserved. Information in this document is subject to change without notice. Nortel assumes no responsibility for any errors that may appear in this document.

