



Product Brief

Nortel Switched Firewall 6000 Series

Accelerated VPN-Firewall

High-performance stateful firewall appliance for perimeter deployment

- Dual component switch-based appliance for high-capacity, accelerated and low-latency performance leveraging Check Point secure XL technology
- Deployed to protect data centers, service provider and enterprise networks
- Secured by Check Point VPN-1 Power technology
- Site-to-site and client-to-site IPsec VPN connectivity
- Key element in the Nortel Layered Defense architecture
- Hitless Upgrade capability for improved resiliency and availability
- Protection of IT assets from a growing number of sophisticated attacks
- Layer 2 and Layer 3 deployment flexibility
- Firewall Clustering with Single System Image for pay-as-you-grow scalability and central management

High level of security for critical applications

- Integrated security pack for Advanced Denial of Service protection
- Protocol-based rate limiting
- IDS server load balancing
- Gateway persistency — extremely useful in multiple ISP links environment
- Integrated with Nortel Threat Protection System to prevent real-time threats and attacks
- Deep Packet Inspection with Check Point SmartDefense for extra protection from sophisticated hacks and attacks
- Multimedia and security for VoIP, SIP, Windows Media and RealVideo
- Support for Nortel VoIP portfolio (e.g., Multimedia Communication Server 5100 and Communication Server 1000)

Nortel Switched Firewall 6000 Series

Network threats and attacks are on the rise. Organizations are using the network to gain a competitive advantage. Convergence of network resources drives cost savings and productivity while improving customer engagement. However, an unprotected or poorly protected network is not a competitive advantage. The network must be protected by the best security firewall available.

The Nortel Switched Firewall, based on Check Point Software, a leader in firewall technology, is a key component in Nortel's Layered Defense.

The 6000 Series is ideal for deployment in large enterprise environments, and is certified under the Check Point Open Platform for Security (OPSEC) criteria and enhances the VPN-1/Firewall-1 deployment with unique services and capabilities.

Switched Firewall — defined

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

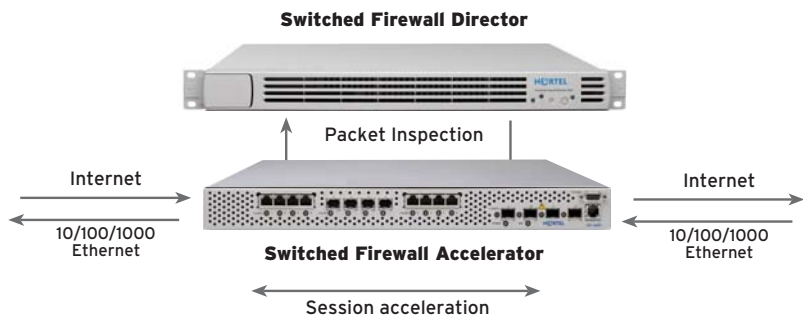


Figure 1. Nortel Switched Firewall System 6616

Ideal for VoIP, SIP and multimedia:

- High performance: 5 to 7 Gbps
- 20,000 to 100,000 connections per second
- 99.999% availability with in-service upgrades
- Accelerated NAT and application intelligence

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.



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 easy management and troubleshooting
- > Protection from application-level attacks via Check Point SmartDefense functionality
- > Availability for both site-to-site and client-to-site IPsec VPN with Check Point VPN-1 technology
- > Stateful Policy Inspection — Inspecting all traffic and comparing it to defined security rules
- > Policy Enforcement and Data Forwarding — Forwarding or blocking traffic based on the rules and signatures
- > Intelligent security with high performance
 - Throughput of up to 7 Gbps
 - Connections per second of 20,000 to 100,000
 - Concurrent connections of 2,000,000

Nortel Switched Firewalls are also available in non-accelerated forms. These include 5111, 5114 and 5124. Please see the Nortel Switched Firewall 5100 Series product brief for more information.

Accelerated performance

The Nortel Switched Firewall System 6416 consists of a Switched Firewall Accelerator (SFA) 6400 and a Switched Firewall Director (SFD) 5016. The Nortel Switched Firewall System 6616 uses a Switched Firewall Accelerator 6600 with a 5016. 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 6416 and 7.0 Gbps for the 6616. This high capacity and low latency performance, made possible through Check Point Secure XL technology, 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 type of performance is critical in any real-time services deployment such as VoIP, SIP or multimedia. Since traditional implementations would require expensive extra resources

to deal with the expected peak traffic loads, this feature distinguishes the Nortel Switched Firewall from all server-based platforms.

- Ideal for VoIP, SIP and multimedia:
- > High performance: 5 to 7 Gbps
 - > 20,000 to 100,000 connections per second
 - > 99.999 percent availability with in-service upgrades
 - > Accelerated NAT and application intelligence

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.

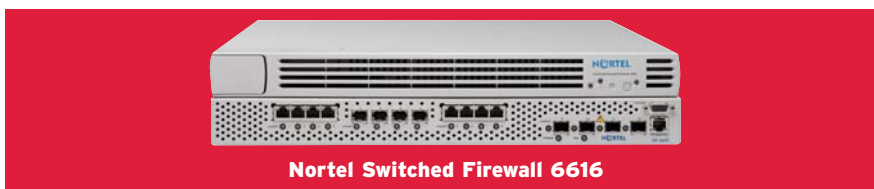
Key applications — Nortel Switched Firewall System 6416 and 6616

Threat Protection

Nortel's Threat Protection System uses intrusion detection and real-time threat intelligence to analyze and detect network threats. An intelligent, automatic update to Nortel Switched Firewall blocks threats before they harm the network.

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.

Hitless Upgrade

The Switched Firewall 6000 Series supports hitless upgrade, which keeps the network traffic flowing with minimal disruption in service during the upgrade process. If the upgrade process is interrupted, hitless upgrade allows for graceful rollback to the previous version without affecting traffic.

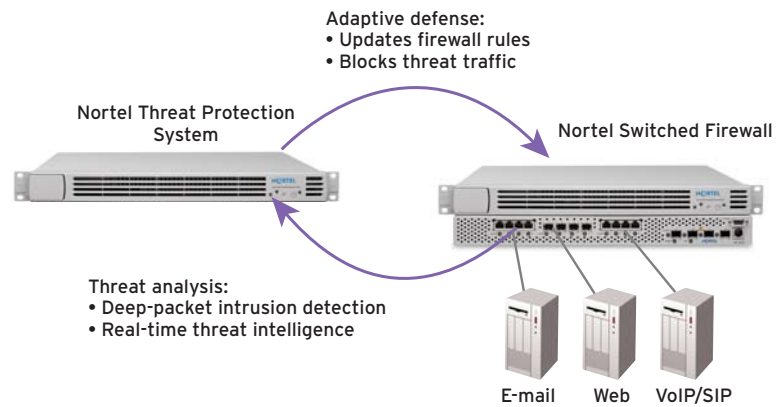
Device Load Balancing

Up to six Switched Firewall Directors can be load balanced and health checked 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 6416 and 6616 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, banks, schools, universities and hospitals.

Figure 2. Threat Protection System model



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.

Layer 2/Layer 3 mode deployment

The Switched Firewall 6000 Series supports flexible deployment in both Layer 2 and Layer 3 mode. Customers easily deploy the 6000 Series into existing topologies in Layer 2 mode. No address or routing changes are required. Network segments can then be migrated port-by-port to Layer 3 mode if desired.

Gateway Persistency

Gateway persistency is another very useful feature in the Switched Firewall 6000 Series. In a multiple ISP links scenario, gateway persistency ensures that the requests and responses for a particular connection always traverse the same gateway that is forwarding the packets.

Solution benefits

Low total cost of ownership

Network traffic is growing. Organizational dependence on communication and interaction means that security solutions must be cost-effective and able to grow to meet future demand. The Nortel Switched Firewall System 6416 and 6616 can both be scaled to meet this growth.

An initial system with one Switched Firewall Director supports 20,000 session connection requests per second. As 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 2,000,000 total concurrent connections.

Managing a Switched Firewall System is easy. A Single System Image (SSI) 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 re-use their existing license to easily move their firewall onto any Nortel Switched Firewall System.

Support for Multi-Link Trunking

To achieve resiliency in a data center environment, the Nortel Switched Firewall can be integrated with the core routers Ethernet Routing Switch 8600 using Multi-Link Trunking (MLT). By incorporating resiliency into the network core, user access points can remain connected to the network even in the event of a failure.

Enhanced VoIP and multimedia support

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 imple-

mentations 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. In addition, the Nortel Switched Firewall has been successfully tested with Nortel's widely deployed multimedia devices (e.g., Multimedia Communication Server 5100 and Communication Server 1000).

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 and provides 99.999 percent application and service availability. This eliminates single

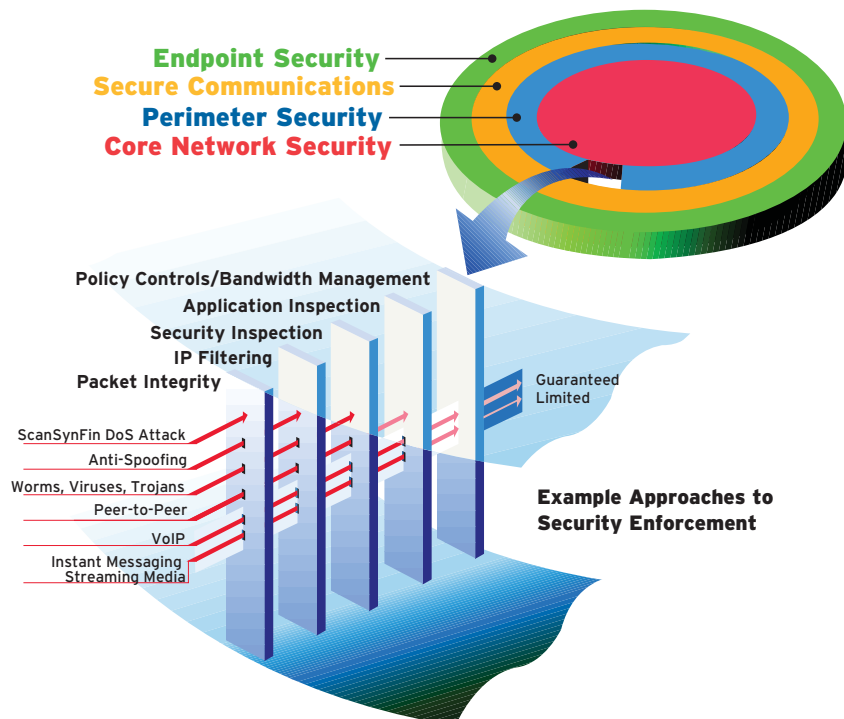
points of failure in the network. The High-Availability configuration uses two Switched Firewall Accelerators and supports in-service upgrades so that the firewall system never needs to be taken out of service. With Plug and Play (PnP) deployment and expansion with a Single System Image, the Nortel Switched Firewall is easy to manage and maintain.

Total threat protection

The Nortel Switched Firewall is a key component of the Nortel Layered Defense Architecture. It provides the highest level of security, combined with high performance and low latency, as demanded by today's leading enterprise and carrier customers. The Nortel Switched Firewall is an important pillar in the complete Nortel security solution that includes the Nortel Application Switch, Nortel Secure Network Access Switch and Nortel Threat Protection System. When combined, the comprehensive solution provides total threat protection.

Figure 3. Nortel's Layered Defense Architecture

The Nortel Layered Defense Architecture ensures that there are no single points of security failure in the network. By building security into every new product and solution, a layered defense approach will protect your network from threats both outside and within the network. The **Nortel Switched Firewall** operates at the Perimeter and Secure Communications Layers.



Product specifications

Part numbers and description

- EB1639174E5 - Switched Firewall System 6616, complete with Accelerator and Director
- EB1639113E5 - Switched Firewall Accelerator 6600, to upgrade an existing Director or to create a High Availability configuration
- EB1639173E5 - Switched Firewall System 6416, complete with Accelerator and Director
- EB1639067E5 - Switched Firewall Accelerator 6400, to upgrade an existing Director or to create a High Availability configuration
- EB1639130E5 - Switched Firewall Director 5016, 4 x 10/100/1000BASE-TX ports
- EB1639131E5 - Switched Firewall/VPN Director 5026, 4 x 10/100/1000BASE-TX ports and VPN Acceleration card

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/1000BASE-TX Port 10/100/1000 full or half-duplex (auto-negotiation) with RJ-45 UTP port
- 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
- 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)

Nortel Switched Firewall product matrix

Model/feature	5111	5114/5124 ¹	6416/6426 ¹	6616/6626 ¹
Deployment	Medium branch	Medium/ large branch	Larger enterprise carriers and data centers	
Throughput (Gbps)	1.2	1.6	5.0	7.0
Connections per sec ²	12,000	10,000	20,000/Director	20,000/Director
Accelerated concurrent sessions	0	0	750,000	750,000
Total concurrent sessions	300,000	500,000	2,000,000	2,000,000
Layer 3 protocols	OSPF	OSPF	OSPF, RIP 1 and 2	OSPF, RIP 1 and 2
VPN throughput 3DES ¹ (Mbps)	88	88/350	88/350 per Director	88/350 per Director
VPN concurrent tunnels	10,000	25,000	25,000	25,000
VLANs/IEEE 802.1q	Yes	Yes	Yes - up to 242	Yes - up to 242
Health checks and load balancing	Yes	Yes	Yes	Yes
Multi-link trunking	No	No	Yes	Yes
Plug-and-play	No	No	Yes	Yes
Single System Image upgrade	Yes	Yes	Yes	Yes
High availability	Yes	Yes	Yes	Yes
Hitless upgrade	No	No	Yes	Yes
IDS load balancing	No	No	Yes	Yes
Ethernet TX ports: 10/100	0	0	24	0
Ethernet TX ports: 10/100/1000	6	2	0	8 ³
Ethernet SX ports: 10/100/1000	0	2 x 1000SX	4 x GBIC	8 x GBIC ³

Notes:

1. NSF 5124 and 5026 have VPN Acceleration capability to improve encryption performance from 88 to 350 Mbps. Multiple (up to six) NSF 5026s may be clustered with 6400 or 6600 Switched Firewall Accelerators to create a high-performance VPN cluster with up to 2 Gbps of 3DES throughput.
2. Multiple Directors (up to six) can be load balanced to achieve up to 100,000 connections per second in an accelerated cluster.
3. Any 12 ports can be enabled at one time on the Switched Firewall Accelerator 6600.

Nortel is a recognized leader in delivering communications capabilities that make the promise of Business Made Simple a reality for our customers. Our next-generation technologies, for both service provider and enterprise networks, support multimedia and business-critical applications. Nortel's technologies are designed to help eliminate today's barriers to efficiency, speed and performance by simplifying networks and connecting people to the information they need, when they need it. Nortel does business in more than 150 countries around the world. For more information, visit Nortel on the Web at www.nortel.com. For the latest Nortel news, visit www.nortel.com/news.

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

Nortel, the Nortel logo, Nortel Business Made Simple, the Globemark and Alteon are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Copyright © 2007 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.

NN110161-110507

In the United States:

Nortel
35 Davis Drive
Research Triangle Park, NC 27709 USA

In Canada:

Nortel
195 The West Mall
Toronto, Ontario M9C 5K1 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
Phone: 00 800 8008 9009

In Asia:

Nortel
United Square
101 Thomson Road
Singapore 307591
Phone: (65) 6287 2877



BUSINESS MADE SIMPLE