



›THIS IS THE WAY

›THIS IS NORTEL™

## Product Brief

### 8660 Service Delivery Module for the Nortel Ethernet Routing Switch 8600

**Flexible services module integrated into the high-availability 8600 supporting Check Point Firewall-1 today and cooperating in the complete campus security solution**

The 8660 Service Delivery Module (SDM) is a device that hosts network applications and is installed into the spare slot of a Nortel Ethernet Routing Switch 8600 (formerly known as Passport\* 8600) chassis.

Up to four SDMs can be installed into a 10-slot chassis, up to two into the 6-slot version, and a single SDM is supported in the 3-slot chassis. An SDM can be ordered with either one, two or four application processors pre-installed, and it is possible to field-replace and field-

upgrade these application processors. The hardware is a combination of the base board module and PrPMC sub-modules (each with a Hard Disk), and functionally these are referred to as “Integrated Services Directors” (iSDs).

The first phase of the SDM’s development has seen the porting of stateful firewall functionality from the Nortel Switched Firewall (formerly known as Alteon\* Switched Firewall) portfolio; hence, the current use for an SDM is as an enterprise-class firewall running Check

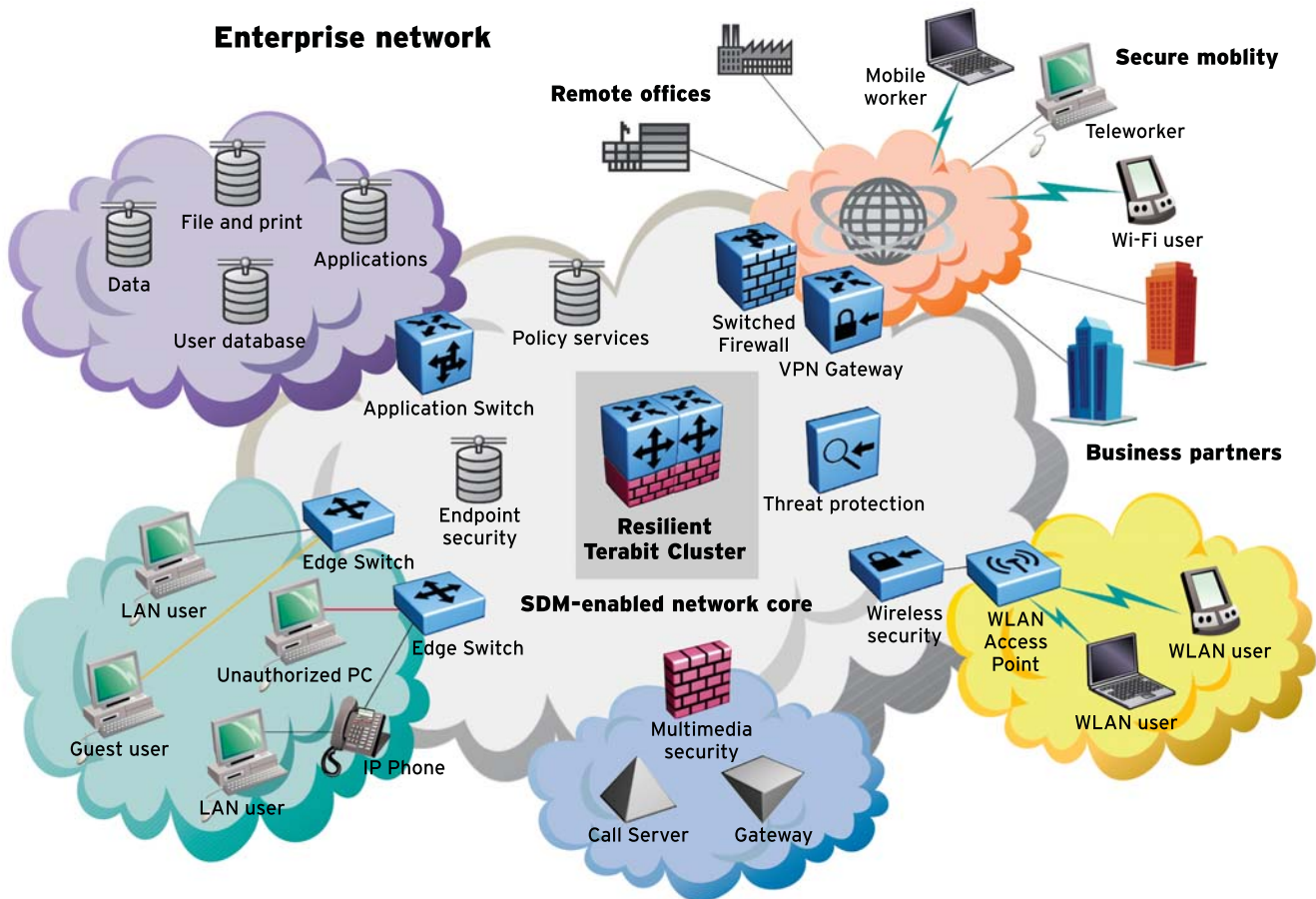


**8660 Service Delivery Module**

Point’s Firewall-1 NG software. The SDM also supports the Nortel enhancements such as Single System Image (SSI); which means that as additional capacity is added to an existing SDM implementation (as additional PrPMC processors are installed), the new iSDs can be configured with virtually zero effort.

The SDM complements the other service modules currently available for the Ethernet Routing Switch 8600; the Web Switch Module (WSM) and the 8661 SSL Acceleration Module (SAM). The strategic advantage that the SDM offers is its flexibility — the breadth of applications and services it can be developed to support; whereas these other modules are task-specific. The SDM can theoretically be enhanced and developed to support any network application.





### Key benefits of the 8660 Service Delivery Module:

- > Highly-available stateful firewall solution
- > Integrated into the 8600 Resilient Terabit Cluster design
- > Running Check Point's Firewall-1 NG for leading features
- > Leveraging OPSEC to integrate Nortel's Threat Protection System
- > Scalable performance to allow cost-effective security solutions
- > Flexible design approach with future-proofed architecture

### New class of product

The first-release functionality — stateful firewall — means that the SDM can be positioned into designs where the need for a security solution that is tightly integrated with the core network is paramount.

If we consider the typical enterprise network, there's a clearly understood role for the traditional firewall that undertakes perimeter defense, carefully interfacing the enterprise network with the Internet and providing protection against external threats. However, there's also an evolving role for a stateful firewall providing protection within the core of the network, against internal threats and to establish clearly enforced intra-network boundaries. This might be to securely partition the different VLANs that make up an end-user access control solution, or to more strictly control inter-departmental or inter-company zones.

Some of these architectural requirements will come from an internal need to build specific layers of control within the network core, moving away from the traditional concept of “once in, everything's open” computing. Additionally, there are emerging regulatory requirements that require specific business functions and information to be limited to a clearly-identified set of users, and a credible enforcement and audit solution must be demonstrated.

This is the sweet-spot for an SDM providing stateful firewall services — it sits at the very heart of the network core, rather than at the edge of the network. Therefore, it is easily integrated into the existing VLAN design and provides a solution with scalable performance so that today's niche requirements can be effectively supported, even though these might grow in the future.

One of the major benefits that the SDM currently provides is of course the integration into the 8600 from the perspectives of network placement and traffic flow, high availability, and integrated management. The SDM has further advantages in that it will be the platform onto which additional current applications are ported and future ones are developed — giving a single SDM the capability to be running multiple network applications, both independently and simultaneously.

### Solution overview

Enterprises have embraced Wireless LAN and other mobility techniques as a means of improving personal productivity and overall business advantage and competitiveness. These new network options have highlighted certain security concerns, and coincide with an emerging trend for controlling network access beyond simply relying upon PC/server operating system security.

Techniques such as 802.1X and other third-party policy-based solutions aim to establish an environment that could be described as “guilty until proven innocent”, meaning that network access will be restricted until the user (and/or their device) proves themselves against some defined corporate security policy.

These access control solutions typically aim to create multiple Virtual LANs (VLANs) with different communication limitations and possibilities. One way to visualize this secure access control solution is to have a series of “colored” VLANs.

For example, you could have a “red” VLAN as the default level of network access, limiting yet-to-be-authorized users to the minimum required in order to test and confirm authorization; i.e., DHCP, DNS, Domain Controllers, Policy Servers, etc. Assuming that the user is authorized and any environmental

checking of their device is successful, then this user is automatically moved into their normal VLAN, which provides them with generic network access.

In between these two levels would be one or more “yellow” VLANs, providing restricted zones that might be used for guest users that are restricted to Internet access, or perhaps a remediation zone that allows authorized users to update their security applications to an acceptable level.

Where the SDM fits into this solution is the ability to easily and directly integrate into the existing VLAN scheme that radiates from the core of the network. The SDM can now provide highly-secure stateful firewall control of the interconnection between these various VLANs, further enhancing and strengthening the entire solution. Add in the need to provide a heightened level of control over Wireless LAN connections, and the SDM is now able to perform a key role in the protection against internal threats.

Another advantage of the SDM is the fact that it’s running Check Point’s Firewall-1 NG software. Apart from the

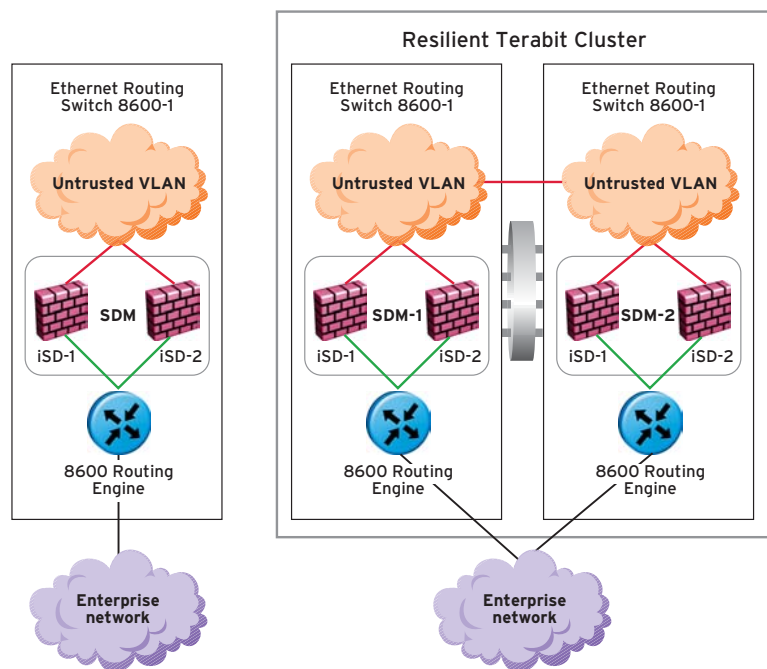
obvious brand recognition of this industry-leading product, there is a compelling technological advantage when used in combination with another Nortel product — the Threat Protection System. The recently-released Threat Protection System (TPS) supports the OPSEC interface and leverages this to proactively feed configuration updates to the SDM Firewall if any traffic matches the signature of a known attack.

Today the TPS is a standalone offering although it is one of the network applications under development for porting onto the SDM. This could provide a combined solution supporting both stateful firewall and intrusion detection and prevention applications.

### High availability: more than just redundancy

The SDM is unique in the way that it’s been integrated into the Ethernet Routing Switch 8600, itself the leader in highly-available core switching solutions for enterprise networks.

The SDM features multiple layers of device and process redundancy that, when combined with the Resilient Terabit



Cluster design architecture, translate into genuine high availability. A single SDM can be configured with one iSD backing up another. Multiple SDMs within the same 8600 chassis can also provide hardware-level redundancy to each other, and multiple SDMs installed into multiple 8600s within a cluster provide a true high-availability solution.

These various configurations combine to provide protection for software processes, hardware and traffic connectivity, clearly demonstrating the tangible benefits of an integrated high-availability solution.

### Best-in-class firewalling

The SDM has a clear advantage in that it's running the industry-leading stateful firewall solution from Check Point Software Technologies.

Firewall-1 provides protection against:

- > Denial of Service attacks
- > Oversized packets
- > SYN floods
- > Fragmentation attacks
- > Nimda and Code Red
- > Cross-site scripting
- > Other network- and application-based attacks

Firewall-1 is designed to ensure that critical business applications and Web services can operate effectively, including support for:

- > Microsoft CIFS
- > SMTP, FTP, HTTP, DNS and Telnet
- > SOAP/XML
- > Instant Messaging and Peer-to-Peer
- > Windows Media, Real Media and SIP
- > H.323-based services, including VoIP and NetMeeting
- > Oracle SQL and ERP

Therefore, it's possible to provide both optimum protection and business productivity. The OPSEC program and the "Secured by Check Point" tag identify products that meet Check Point's stringent security, usability and interoperability requirements, enabling customers to deploy products into their networks with complete confidence.

### Nortel options

The SDM is not intended to directly compete as a traditional perimeter firewall, and it's been developed to provide this specialized security service within the core of the network.

Some organizations have corporate policy which dictates that firewalls remain the preserve of the security group rather than the network group, and therefore a standalone product is needed to satisfy this demarcation.

In many ways, both the SDM and the Switched Firewall portfolio can fulfill the essential elements of the perimeter firewall and the core firewall roles.

However, the SDM has advantages in terms of flexibility and integration into the high-availability 8600 core, and today the Switched Firewalls have the advantage of greater scalability if ultimate performance is a key consideration.

While the SDM offers quite impressive performance levels today, there are opportunities for virtually unlimited performance. In the same way that Nortel has pioneered the concept of "accelerated" firewalling with the standalone products, we're working on a similar future capability with a combination of the SDM (acting as the "Director") and the new R-Series line cards (acting as line-rate "Accelerators").

### Competitive landscape

The SDM offers a highly competitive solution today for firewall services directly integrated into the high-availability network core — the Ethernet Routing Switch 8600.

Enhancing the SDM's competitiveness is of course our alliance with Check Point for the Firewall-1 NG software which is both the industry leader and universally-acknowledged as a best-in-class product. Together, Check Point and the Nortel optimizations — SSI and the integration into the 8600 — mean that the SDM is the leading solution in terms of features and functionality.

The SDM implementation brings some very unique differentiators to a Firewall-1 deployment; the 8600 provides enhanced LAN services such as QoS and EAP, together with high-availability and sub-second failover. Also unique is the 8600's Packet Capture capability, which allows network managers to flexibly target traffic with appliances such as intrusion detectors and sensors.

The competitive landscape is very limited; only Cisco can boast a similar offering — the Firewall Service Module (FWSM) which installs into the Catalyst 6500 Series Switches. And no other major vendor has anything approaching a network applications service module. None of the other established or commodity vendors operate in this value-added market.

The Cisco FWSM is somewhat similar to the SDM; it's a service module that integrates into a core switch, and although it boasts high firewall performance, it's hindered by the fact that it has to rely upon the PIX Firewall application: no support for OPSEC; no integration with third-party IDS/IPS; and multiple limitations in terms of granular application recognition and control.

The strategic limitation of the Cisco FWSM is that it's purely a firewall appliance, whereas the SDM is a multi-purpose application module with the future potential for supporting multiple network applications independently and simultaneously. As is normal practice, Cisco will position multiple devices to achieve the same result. For example, they also offer an Intrusion Detection Service Module and an IPSec VPN Service Module.

Nortel's philosophy is very different and this is why the SDM has been specifically designed to consolidate a number of functions onto a single device. Our approach saves the end-user money in

terms of hardware and precious slot usage on the core switch, and also minimizes network complexity, which improves application availability and service restoration.

### In conclusion

Today, the Service Delivery Module offers an intriguing alternative for firewalling services, integration into the high-availability and high-performance 8600 platform, and integration into the emerging secure access control solutions. The unique combination of high-availability, industry-leading stateful firewall feature capability, direct integration with Threat Protection System, future-proofed readiness for further security

enhancements, and scalable performance mean that the SDM is a compelling addition to the network architect's toolkit.

Importantly, the Service Delivery Module is an exciting development for Nortel's Ethernet Routing Switch portfolio as it offers a raft of new opportunities with further enhancements currently under development. It has the potential to be a key competitive differentiator and a strategically vital element as network applications consolidate and the network foundation devices play an increasingly important role in overall application security and reliability.

## Technical specifications

**Table 1. 8660 Service Delivery Module technical specifications**

### Physical specifications

- > Occupies 1 standard slot in the 8600 chassis
- > Up to 4 x SDMs supported in the 10-slot chassis
- > Up to 2 x SDMs supported in the 6-slot chassis
- > Up to 1 x SDM supported in the 3-slot chassis

### Performance specifications

- > Throughput: 300 Mbps per iSD/up to 1.2 Gbps per SDM
- > Sessions: 250,000 per iSD/up to 1,000,000 per SDM
- > Connections per minute: 2,500 per iSD/up to 10,000 per SDM

### Supported standards, protocols and RFCs

- > Layer 1 and 2 support is as per the Nortel Ethernet Routing Switch
- > Layer 3 - 7 is equivalent to that provided by Check Point Firewall-1 as ported onto the Nortel Switched Firewall

### Mean Time Between Failure (MTBF)

- > 322,059 hours @ 25°C

### Electrical specifications

- > Input power consumption: 80W

### Environmental specifications

- > Operating temperature: 0° to 40°C (32° to 104°F)
- > Storage temperature: -25° to +70°C (-13° to 158°F)
- > Operating humidity: 85% maximum relative non-condensing humidity
- > Storage humidity: 95% maximum relative non-condensing humidity
- > Operating altitude: Up to 3,000m (10,000 ft.) above sea level
- > Storage altitude: Up to 3,000m (10,000 ft.) above sea level

### Software compatibility

- > Ethernet Routing Switch 8600 v3.7.6.0 and v4.1
- > Check Point Firewall-1 R55 HFA-08 Hot Fix 1

## Ordering information

**Table 2. Ordering information for the 8660 Service Delivery Module**

Order no:	Product description
DM1404104	8660 Service Delivery Module with 1 Firewall iSD Module for the Ethernet Routing Switch 8600
DM1404081	8660 Service Delivery Module with 2 Firewall iSD Modules for the Ethernet Routing Switch 8600
DM1404080	8660 Service Delivery Module with 4 Firewall iSD Modules for the Ethernet Routing Switch 8600
DM1411023	8660 Service Delivery Module Spare Disk Drive
DM1411024	8660 Service Delivery Module Spare PrPMC Module

## Maintenance services

**Table 3. Maintenance services available for the 8660 Service Delivery Module**

Order no:	Product description
GE53009**	Technical Support Services
GL53009**	Return & Replace Services
GF53009**	Managed Spares Services Pack - Next Business Day
GG53009**	Managed Spares Services Pack - Same Business Day
GH53009**	Managed Spares Services Pack - 4 Hour 7x24
GJ53009**	Managed On-Site with Spares Services Pack - Next Business Day
GK53009**	Managed On-Site with Spares Services Pack - Same Business Day
GN53009**	Managed On-Site with Spares Services Pack - 4 hour 7x24

Where "\*\*\*" is replaced with "08" for the DM1404104; "09" for the DM1404081; and "10" for the DM1404080

## Software licensing

**Table 4. Check Point Firewall-1 software licenses available for the 8660 Service Delivery Module**

Order no:	Product description
CPMP-VEPRO	Check Point Enterprise Pro Unlimited Users
CPVP-VCT	Check Point Enterprise Unlimited Users

The 8660 Service Delivery Module ships with Check Point software pre-loaded, and customers must then purchase the appropriate Check Point license. The type and cost of licenses may vary according to a number of variables, including the status of any site license and the number of users. Please contact an authorized Check Point Reseller for detailed pricing information.



Nortel is first-in-class to achieve IPv6 Ready Phase 2 Logo status with our Ethernet Routing Switch 8600: further proof of our commitment to sustainable networking!

For more information, visit: [www.nortel.com/ipv6](http://www.nortel.com/ipv6) or [www.ipv6ready.org](http://www.ipv6ready.org)



**TRC**  
TELECOM RESOURCE CORPORATION  
trcnetworks.com

Have A Question?  
Need More Info?  
Call Us: 1 877 390 1166

This is the Way. This is Nortel, Nortel, the Nortel logo, the Globemark, Alteon and Passport are trademarks of Nortel Networks. All other trademarks are the property of their owners. Copyright © 2005 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.

