



## FEATURES

- **Hardware offload for compute-intensive encryption, secure key exchange, and certificate validation**
- **A cluster of SSL Accelerators can process up to 150,000 SSL sessions per second on a single Content Switch**
- **Centralized, advanced key and certificate management saves administrative costs and maintenance hassles**
- **Automatic import of keys generated by Apache, Stronghold, OpenSSL, IIS 4.0, Weblogic and PKCS12**
- **The SSL Accelerator is available on two hardware platforms:**
  - the iSD-310, processing up to 600 SSL transactions per second per unit for high-volume SSL traffic*
  - the iSD-100, processing up to 400 SSL transactions per second per unit for low to medium volume SSL traffic*
- **Processes SSL transactions 5 to 250 times faster than an HTTPS server**
- **Scalable up to 255 hot swappable SSL Accelerators per Content Switch for performance and redundancy**
- **Supports multiple virtual SSL servers in active-standby mode for resilient SSL services**

## The Alteon iSD SSL Accelerator, V2.0

The Alteon integrated Service Director (iSD) is an innovative service delivery platform designed to provide a variety of value-added traffic management applications that further extend the performance, scalability and flexibility of advanced Content Switching infrastructures. The Nortel Networks' Alteon iSD SSL Accelerator intelligently accelerates secure business transactions by offloading Secure Sockets Layer (SSL) processing from local servers without imposing delays on other traffic in the same data path. The SSL Accelerator also simplifies the way to deploy and maintain a Public Key Infrastructure (PKI), enabling business critical electronic transactions. Purpose-built to perform processing tasks with long duty-cycles that would otherwise bog down network performance, the SSL Accelerator seamlessly integrates with Alteon Content Switches to offer the best of Content Switching and IP appliance technologies.

### Secure Transaction Performance Means Revenue

Today's most successful companies are using the Web to communicate with their customers, suppliers and partners because of the open and ubiquitous nature of Internet. But the very openness of the Web makes security a concern. Secure Socket Layer (SSL), combined with Public Key Infrastructure (PKI), can provide a standard means of securing transactions, but each has possible drawbacks to your site's performance and resources. SSL transactions can be so compute-intensive that they slow your site to crawl as Web servers are forced to handle key exchanges and bulk encryption. And PKI can take a toll in administration. Nortel's Alteon iSD SSL Accelerator has been specifically designed and enhanced to work with Nortel's industry-leading Alteon Content Switch, to create a total solution that allows you to ensure security for you and your customers and manage key administration centrally, all without losing the site performance that is truly critical to your success. So you can enjoy the performance you need with the strong security your customers demand at a much lower cost than adding more servers, all in a highly scalable solution that is easy to integrate.

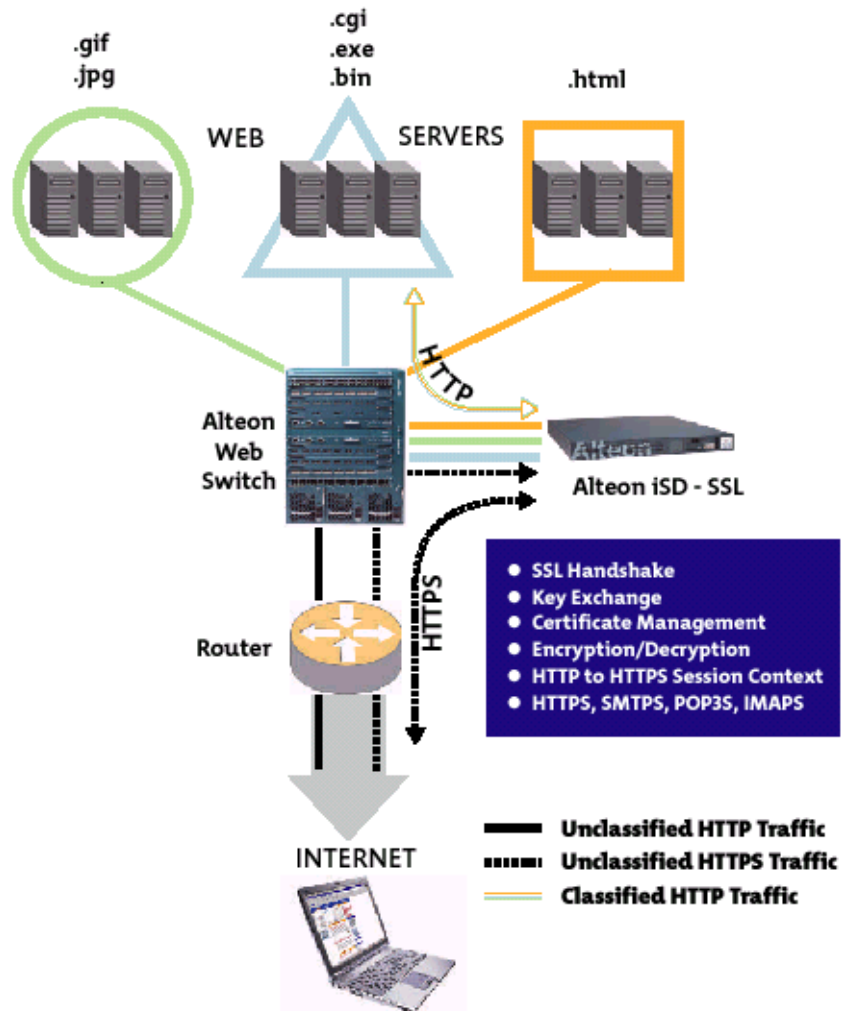
### Optimize Your Investment in Your Web Servers

Web servers were designed to serve content; not to process SSL sessions. Whether PC-based or Unix-based servers are used, performance drops dramatically when the burden of processing SSL web traffic, including terminating sessions, handling verification, and performing bulk encryption, is added. Transactions are slowed, and revenue can be lost due to those performance issues. Even worse, it is impossible to provide content-intelligent switching or to ensure persistence when traffic is encrypted. Some providers have tried to solve the problem by implementing in-line SSL Accelerators, but deployment in the data path only serves to move the bottleneck from the Web servers to the incoming data path itself.

Nortel's Alteon iSD SSL Accelerator has a better way to process SSL traffic. When SSL traffic comes in to the Alteon Content Switch, it is transparently offloaded to an SSL Accelerator, which terminates each client HTTP-S session, performs hardware-assisted security verification with the client and establishes a HTTP session to the chosen Web server. On the return path, the SSL Accelerator encrypts the server response according to

- Content intelligent-Switching services for secure SSL sessions
- HTTP application level knowledge which enables functions like header add/remove and redirection
- Maintains session context between HTTP and HTTP-S
- Processes SMTP-S, POP3-S and IMAP-S secure messaging protocols
- Shopping-cart persistence without server reconfiguration or waste of VIP addresses
- SSH secure management protocol and SNMP support
- Supports SSL v2.0, SSL v3.0 and TLS v1.0
- Easy import of keys generated by Netscape Server via a conversion utility
- 10/100 Mbps copper or 1,000 Mbps fiber link from SSL Accelerator to Content Switch
- Attach to Content Switch directly or across a local broadcast domain
- Rack-mountable 1U high unit

the negotiated encryption rules and forwards it to the requesting client using the established, secure HTTP-S session. One or more SSL Accelerator units, coupled to a single Alteon Content Switch, can process from 400 to over 150,000 SSL transactions per second, which is equivalent to up to 15 to several hundred HTTP-S servers processing the same traffic.



And, because the SSL Accelerator is out of the data path, non-encrypted traffic speeds through the network without slowdown. Not only does this configuration assist with performance, but it is also intrinsically scalable. Additional SSL Accelerators can be added with no change to your infrastructure, and up to 255 SSL Accelerator units can be transparently load balanced by an Alteon Content Switch to form a super-fast, scalable, modular and fault-tolerant SSL front-end for traffic-intensive Internet, Intranet and Extranet websites. The SSL Accelerator frees up server resources for application processing, optimizes installed server investment and saves potential new server acquisition costs as well as valuable labor time.

## **The Alteon iSD SSL Accelerator Also Enables PKI!**

The Nortel Networks' Alteon iSD SSL Accelerator has advanced key and certificate management capabilities, such as encrypted private keys management, multiple certificate generation and support, cipher selection, and both client and server authentication and revocation. It enables easy deployment of Public Key Infrastructure (PKI) by centralizing the main security administration tasks, instead of duplicating them over several servers. Those management capabilities reduce both the human factor and the software license cost of using a PKI. Moreover, PKI management on a hardware platform is a lot more secure. It is far more difficult to break into a purpose-built appliance than to hack a server running an OS with well-known back doors to steal certificates or encryption keys. The SSL Accelerator can also handle secure email protocols like SMTP-S, POP3-S and IMAP-S enabling use of secure messaging applications in internal, external or in Application Service Provider modes. These advanced key and certificate management capabilities, combined with a unique usability, makes the SSL Accelerator the ideal solution to implement PKI.

## **Content-intelligent Switching for Secured Web Sessions**

Since the SSL Accelerator renders encrypted sessions visible to the Content Switch, Alteon's Web OS content-intelligent services, which involve the inspection and parsing of HTTP headers, cookies and Uniform Resource Locators (URLs), can now be applied to secure Web traffic. This enables website operators to distribute secure Web sessions to specific Web servers based on user attributes such as geography, language, the user's browser device, or priority; as well as by the content type requested. With the SSL Accelerator and Content Switch, Hosters and Application Service Providers can now offer value-added, content-intelligent bandwidth metering and QoS services to their eCommerce and Enterprise customers.

## **Hassle-Free Shopping-Cart Persistence**

It can sometimes be difficult to ensure session-level persistence, even with unencrypted traffic, due to the use of mega-and micro-proxies which can change the end user's IP address. Ensuring persistence is vitally important with applications such as eShopping carts and secure Web forms, where ease of use often ties directly to revenue. The Alteon Content Switch solves this problem by parsing deeply into the packet to look for Layer 7 attributes such as cookies. This methodology cannot be easily implemented when handling secure traffic, however, since the cookie is encrypted when the session goes from HTTP to HTTP-S. Some implementations try to solve this problem by using the SSL Session ID, but the browser itself can change this ID during a session. The combination of the SSL Accelerator and the Content Switch solves this problem by enabling the Content Switch to utilize the decrypted cookie to guarantee necessary persistence.

## **Non-Intrusive Integration**

Unlike traditional IP appliances that must be located directly in the data path or cryptographic cards embedded in the web servers, the SSL Accelerator is non-intrusive to existing network topologies. Attached directly or across a local broadcast domain to a Content Switch, the Alteon iSD appears to the Content Switch as another transparent server, allowing all Web OS traffic management services, including load balancing, filtering, network address translation, policy redirection, automatic fail-over, and intelligent scriptable server health-checks, to be configured for one or a group of SSL Accelerators. The SSL traffic can then be processed by intelligent traffic management capabilities and the clear non-encrypted traffic is directly passed to the servers without being delayed by yet another layer of data analysis.

## Product Specifications

### ISD-310 SSL Accelerator

Part #	Product
700231	iSD-310 SSL-FE Accelerator, 10/100BASE-TX
700232	iSD-310 SSL-GE Accelerator, 1000BASE-SX

#### **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

#### **Security Algorithms Supported**

RC2, RC4, DES, 3DES, MD5, SHA1

#### **Dimensions**

Width: 17.61 inches (44.73 cm)

Depth: 24.00 inches (60.96 cm)

Height: 1.7 inches (4.32 cm)

Weight: 22lbs (9.9 kg)

(Standard 19" EIA 1U rack mountable)

#### **Environmental**

##### Operating

- Temperature 10 to 35° C

- Humidity 8% to 80% (non-condensing)

##### Power

- Power supply: 100-240 VAC@ 60-50 Hz, 3.6-1.8 A

- Power consumption: 240

#### **MTBF**

- >50,000 hours

#### **Certifications**

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

- Safety: UL 1950, CSA 950, CE Mark EN60950, IEC60950

### ISD-100 SSL Accelerator

Part #	Product
700203	iSD-100 SSL –F2A Accelerator, 1000BASE-SX
700204	iSD-100 SSL –C1A Accelerator, 10/100BASE-TX

#### **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

#### **Security Algorithms Supported**

RC2, RC4, DES, 3DES, MD5, SHA1

#### **Dimensions**

Width: 17.00 inches (43.2 cm)

Depth: 18.00 inches (45.7 cm)

Height: 1.6 inches (4 cm)

Weight: 9 lbs (4.1 kg)

(Standard 19" EIA 1U rack mountable)

**Environmental**

Operating

- Temperature 0 to 50° C
- Humidity 5% to 85% @ 40° C (non-condensing)

Power

- Auto-ranging supply: 90-265 VAC@ 47-65 Hz
  - Power consumption: 250W-AC +5V/25A, +12V/10, -12V/0.5A, -5V/0.5A

**MTBF**

- >50,000 hours

**Certifications**

Emissions: US – FCC 47 CFR Part 15; Canada – ICES-003;

Europe – CISPR22; CE Mark to EN55022/EN50082

- Safety: UL 1950, CSA C22.2 No. 950, CE Mark EN60950, IEC950
-

