nFast Ultra™

NEXT GENERATION SSL ACCELERATOR

PRODUCT | DATA SHEET

The nFast Ultra SSL Accelerator is a high-performance PCI card that promotes enterprise-wide deployment of Secure Sockets Layer (SSL) security. The nFast Ultra is a complete solution: it provides all the functionality necessary to establish an SSL or TLS secure connection over an IP network, effectively removing the processing burden associated with SSL security in virtually any server environment.

EXTENDING SSL SECURITY

The SSL standard and its successor TLS have emerged as the benchmark for secure communications over IP networks. SSL provides both privacy and authentication in any situation where data may be compromised and, as a result, is used almost universally to protect e-commerce transactions and other web-based communications. Recently the use of SSL has expanded to secure corporate communications in the form of VPNs and server-to-server connections between front-office and back-office applications.

However, the use of SSL has traditionally come at a price. The intensive cryptographic processing and protocol handling required to establish SSL sessions can cripple a server by exhausting CPU horsepower, slowing down critical applications. This can result in acute server bottlenecks, particularly in the case of back-office or application servers where CPU capacity is already under pressure. Consequently, many security architects have faced a stark choice; to deploy SSL very sparingly, for example limiting its use to web-based services, or to deploy large numbers of expensive servers to handle the increased processor load.

100% SSL OFFLOAD

By offloading the entire SSL process from the CPU to a self-contained sub-system that replaces the existing network interface, the nFast Ultra enables organizations to expand deployment of SSL security. It removes the need for additional cryptographic acceleration and integrates with existing applications as easily as a standard network interface card. Also, by performing all SSL protocol handling, the nFast Ultra frees up 100% of the server's CPU capacity, maximizing the return from investment in expensive software server licenses. The nFast Ultra achieves best of breed performance, yet is completely transparent to legacy and new applications alike.

The nFast Ultra PCI card has been designed as a drop-in solution for virtually any server platform running Windows, Solaris or Linux. Because all of the SSL operations are terminated directly on the PCI card, there are no complicated integration steps or cryptographic APIs to support. All non-SSL traffic is passed transparently to the host. Prior to the availability of the nFast Ultra, the only way to achieve this level of transparency to the application was to deploy dedicated SSL terminating appliances outside the server.

MARKET-LEADING PERFORMANCE

A single nFast Ultra PCI card allows servers to achieve a sustained throughput of up to 10,000 SSL connections per second. This performance means that it is possible to handle even the highest peaks of internet traffic. The nFast Ultra enables the deployment of SSL across Web and internal application servers with confidence.

With the attention of IT security professionals shifting from perimeter to internal security, the nFast Ultra provides a way of expanding Internet-proven security techniques, such as SSL, to cover internal networks while, at the same time, providing future-proofing against unpredictable growth in network traffic.

nCIPHER™

FEATURE	BENEFIT
FULL OFFLOAD OF SSL PROCESSING	Transparent addition of SSL security to existing and new applications via a single, comprehensive solution
DEDICATED HARDWARE SOLUTION FOR SSL PROCESSING	By offloading all SSL processing from host, CPU performance is preserved to efficiently handle other critical server functions
HIGH PERFORMANCE CRYPTOGRAPHIC PROCESSING	Capable of supporting up to 10,000 new SSL/TLS connections per second and combined throughput of 600 Mbps
PLUG-AND-PLAY INTEROPERABILITY	Runs with any TCP-enabled application running on Windows, Solaris or Linux OS
INTEGRAL NETWORK INTERFACE ADAPTER	Operates as a full-duplex 10/100/1000 RJ-45 Ethernet network interface to facilitate easy installation with unencrypted traffic passing to the host server transparently

PRODUCT SPECIFICATIONS

OS Support

- Windows 2000
- Windows 2003
- Windows Server 2003
- Linux - Kernels 2.2 and 2.4 and a variety of Linux distributions including Redhat 7.0, 7.1, 7.2
- Solaris - Solaris 7, 8, 9

PCI Hardware Specification

- PCI Card 3.0 in x 8.0 in (76.2mm x 203.2mm)
- 10/100/1000 - BaseT Ethernet (RJ45)
- PCI v2.2 and PCI-X 1a Bus Connector upto 133 MHz
- Operating voltage +5 volts
- Typical power consumption: 17 watts
- Operating Temperature: 10-55 degrees centigrade with airflow (200 LFM recommended)

SSL/TLS Operation

- SSL 3.0, TLS 1.0
- Fully offloads SSL/TLS processing including handshaking, record handling and all cryptography
- Supports SSL V3.0, TLS V1.0 (RFC 2246)
- Stores up to 256 certificates

Cryptographic Algorithms

- RSA: 1024-bit, 2048-bit and 4096-bit, public and private key processing
- ARC4, DES, 3DES, and AES bulk cipher algorithms.

Performance

- Up to 10,000 RSA SSL handshakes per second (1024-bit RSA decryptions)
- 300 Megabit Full-duplex throughput

Gigabit Ethernet Network Port

- Full-duplex 10/100/1000 RJ-45 Ethernet network interface
- Handles IEEE 802.3 (RFC 1042) or DIX (RFC 894) frames
- Supports IEEE 802.3, 802.3u, 802.3x, 802.3z, and 802.3ac Ethernet specifications
- Supports MTUs up to 1500 bytes
- Pass-through of IEEE 802.1q VLAN tags

IP Layer Processing

- Processes IPv4 (RFC 791) datagrams
- Pass-through of IP header fields such as source/destination addresses and Type of Service (TOS)
- Calculates and verifies header checksums
- Supports limited ICMP messaging (RFC 792)
- Non-SSL traffic can be passed through unaltered to host or blocked

TCP Layer Processing

- Terminates TCP streams from clients and to servers (designated SSL/TLS connections)
- Supports standard TCP functions per RFCs 793, 813, and 1122
- Extracts/inserts SSL/TLS records
- Supports transparent pass-through of non-SSL/TLS traffic
- Segmentation and reassembly (including reordering)
- Performs TCP port translation (source and/or destination)
- Calculates/verifies pseudo-header checksums
- Fast Retransmit/Fast Recovery (RFC 2581)
- Round Trip Time Estimation (Karn's Algorithm)
- Slow Start (RFC 896)
- Window Scaling (RFC 1323)

Standards Certification

- FCC: CFRA47, Part 15, Subpart B, Class A
- CE: EN 55022 Class A
  EN 55024-1
  EN 60950

NCDS/NFASTULTRA/SEPT2004

nCipher Inc.
500 Unicorn Park Drive
Woburn, MA 01801 USA
Tel: +1 (781) 994 4000
E-mail: ussales@ncipher.com

nCipher Corporation Ltd.
Jupiter House, Station Rd.
Cambridge, CBI 2JD UK
Tel: +44 (0) 1223 723600
E-mail: int-sales@ncipher.com

nCipher Corporation Ltd.
15th Floor, Cerulean Tower,
26-1 Sakuragaoka-cho, Shibuya-ku,
Tokyo 150 8512 Japan
Tel: +81 3 5456 5484
E-mail: int-sales@ncipher.com

Visit our Web site at www.ncipher.com – today!

Redefining cryptographic security

nCIPHER™