
# SSL ACCELERATION

## DEPLOYMENT STRATEGIES FOR ENTERPRISE SECURITY

nCIPHER™

# *Introduction*
# OPTIMIZING SSL DEPLOYMENT

*On-demand business breaks down the traditional network perimeter, creating interconnected systems between customers, suppliers and partners. Organizations need a secure, proven and straightforward technology to protect data as it moves between them. As a result, Secure Sockets Layer (SSL) has emerged as the technology of choice for internet, intranet and extranet communications.*

*nCipher's SSL acceleration solutions speed SSL processing to free up server capacity, reducing the requirement for additional servers and software licences, lowering overall security infrastructure costs*

The use of SSL has evolved from simple browser-oriented security for Internet transactions to the de facto transport security, securing corporate communications in the form of SSL VPNs and server-to-server connections between front-office and back-office applications. The increasing demand for secure messaging and for more frequent access to sensitive resources requires higher performance and an enhanced level of security.

Performing SSL purely in software is inefficient and insecure, competing for the same valuable server resources that provide business services. Hence effective SSL deployments require dedicated hardware that offloads all the SSL processing from the host system. In addition to significant performance benefits, the deployment of a dedicated SSL sub-system can be used to isolate valuable cryptographic keys from the vulnerable software layer.

nCipher's SSL acceleration solutions speed SSL processing to free up server capacity, reducing the requirement for additional servers and software licences, lowering overall security infrastructure costs. Because these solutions handle 100% of the SSL processing, they provide a straightforward route to strong transport-layer security, even for enterprise applications that do not natively support SSL.

Increased performance can be combined with FIPS 140-2-validated key management to provide the highest level of information assurance, reducing risk and promoting compliance with regulatory requirements.

### SSL secures productivity

Achieving secure, boundary-less information flow across and between organisations is emerging as a compelling business driver. The promise of lower costs, flexible working and reduced time-to-market is forcing IT security professionals to re-examine their traditional reliance on perimeter controls and to examine a more data-centric approach. As organizations expand their use of encryption from external Internet transactions to the sensitive data sent across their intranets and extranets, SSL becomes the core building block for protecting data in transit.

*A comprehensive approach to deploying an SSL infrastructure must go beyond performance alone to encompass advanced protection and secure management of the digital keys that underlie its fundamental security*

## SSL Applications

- **Web servers**
  Web servers are the main interface for the majority of transactions over the internet. When that interface is encrypted via SSL, customers are protected against interception, impersonation and eavesdropping. SSL acceleration technology allows Web servers to handle thousands of simultaneous customers and hardware key management protects Web site identity and data confidentiality.
- **Application servers**
  Web-enabled applications lie at the heart of today's extended enterprise, whether financial, manufacturing, logistics or human resource systems. These applications rely on SSL to create a secure channel for communication, whether over the intranet or extranet. SSL acceleration ensures that processing bottlenecks are eliminated.
- **Edge servers/load balancers**
  Server farms are a common way of handling large scale deployments. The edge server/load balancer is used to handle processing at the front end of a server farm including SSL traffic. Because these edge servers and load balancers can become a serious bottleneck, it is important to ensure maximum performance.
- **Distributed computing**
  Information is rarely processed on a single server. Increasingly, this information is distributed across multiple servers, potentially spanning the globe, each with interrelated data. It is vital that information passing between these database servers is secured but encryption must not be allowed to degrade the performance.
- **Single sign-on**
  These authentication gateways for intranets and B2B systems support SSL communication from clients as well as encryption to back-end application servers. Using SSL Acceleration hardware, data processing can be increased and the authentication server identity protected.
- **SSL VPNs**
  SSL VPNs can act as the front-end to a host of applications and services. Using SSL to create a secure tunnel allows users to access enterprise services including Web content and email.
- **Web email access**
  Many companies have implemented Web-based email systems, such as Microsoft Exchange Outlook Web Access, to allow their users the ability to access their mail remotely and require SSL to be enabled to provide enhanced security.
- **Legacy applications**
  Adding SSL to commercial legacy applications can present significant problems. Many of these applications will not include a native SSL stack. Even if SSL applications are developed in-house, the original development team may no longer be in place.



*Armed with your SSL private key, an intruder can destroy the authenticity and privacy of your secure service*

*Tamper-resistant hardware security modules create a protective subsystem within your server. These cryptographic modules provide a key management architecture that helps to ensure the secrecy and integrity of the cryptographic keys*

### Balancing security and performance

Unfortunately, Web and application servers are simply not designed to efficiently handle the heavy processing associated with executing the cryptographic operations required by SSL.

Two distinct cryptographic processes impact the performance of these servers:

- At the start of every SSL session there are public key cryptographic operations associated with the SSL handshake process to establish the session itself. This cryptographic load is expensive, slowing the servers down and significantly impacting the overall performance of the service they are providing.
- The establishment of each SSL session creates a secure virtual 'pipe' over which confidential information can be exchanged. To achieve this, the payload is encrypted; again, this process consume valuable host processor resource slowing the system down.

As organizations rollout SSL across their extended operations, they must avoid system bottlenecks where a sudden surge in SSL traffic can leave them facing serious performance problems. These bottlenecks can take many forms: from handling large numbers of concurrent user sessions on busy Web sites to encrypting large quantities of information over a smaller number of sessions, typically the case with SSL based VPN connections. Adding servers isn't the most effective approach to scaling capacity and managing growth; additional servers and associated software can be prohibitively expensive and require significant administrative resources.

### The need for advanced SSL security

A comprehensive approach to deploying an SSL infrastructure must go beyond performance alone to encompass advanced protection and secure management of the digital keys that underlie its fundamental security.

The server's SSL private key is the primary means of proving the server's identity and is the cryptographic secret used to create distinct encrypted sessions for each connection. However, if this private key is left exposed in server memory it becomes vulnerable to compromise. 'Key finding' attacks can put the security of the whole system at risk. Armed with your SSL private key, an intruder can destroy the authenticity and privacy of your secure service, impersonating a legitimate Web site, or hacking data as it crosses the wires, eavesdropping on secure traffic, stealing user's passwords, PINs or other valuable information

Tamper-resistant hardware security modules create a protective subsystem within your server. These cryptographic modules provide a key management architecture that helps to ensure the secrecy and integrity of the cryptographic keys. All cryptographic functions, which would otherwise be performed on the insecure server, take place inside the hardware module, providing defense-in-depth by ensuring that private keys are always protected from compromise.

# SSL offload


*The promise of lower costs, flexible working and reduced time-to-market is forcing IT security professionals to re-examine their traditional reliance on perimeter controls and to examine a more data-centric approach*

## Simplifying the roll-out of SSL

nCipher's range of SSL accelerators and offload cards can be used to enable the use of SSL with any networked application. These high-performance PCI cards provide SSL encryption and decryption functionality between remote clients and the local server, so that even non-SSL aware applications can communicate easily with clients over secure SSL channels.

The nFast and nForce Ultra cards provide all the functionality necessary to establish an SSL or TLS secure connection over an IP network. Both cards come equipped with an Ethernet interface and effectively replace the existing network interface of the host server. SSL-encrypted traffic arriving over the network is decrypted and passed to the host and traffic passing back to the network is encrypted whenever SSL protection is required. Non-SSL traffic passes through the card transparently. Both the nFast and nForce Ultra card have been optimized to provide market-leading performance, delivering up to 10,000 transactions per second (TPS) and throughput of 300Mb per second full duplex.

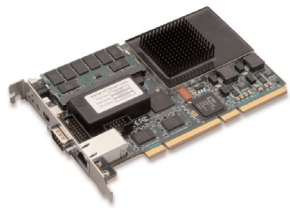
The nFast and nForce cards provide a subset of the functionality provided by the corresponding Ultra variants, providing acceleration for the initial, asymmetric, SSL handshake function. Although the cards require inherent SSL support within the application, they provide a valuable deployment alternative to a full offload card in situations where a network interface, other than Ethernet, is used.

| Feature | Benefit |
|---|---|
| SSL PERFORMANCE | Capable of supporting up to 10,000 new SSL/TLS connections per second |
| SYMMETRIC ACCELERATION | Capable of supporting symmetric SSL data throughput up to 300 Mb per second |
| SECURE KEY MANAGEMENT | nForce can be configured for dual control and split responsibility ensuring that there is no single point of compromise |
| FIPS 140-2 VALIDATION | Independently certified secure management and storage of SSL keys |
| FULL SSL OFFLOAD | By offloading all SSL processing from the host CPU performance is preserved for the business process in question |
| ETHERNET INTERFACE | The Ultra products come equipped with a Gigabit Ethernet interface providing in-line SSL processing prior to traffic reaching the host CPU |

# *The products*

*nFast* *nFast Ultra* *nForce* *nForce Ultra*



| | SSL performance | Symmetric acceleration | Secure Key Management | FIPS 140-2 validation | Full SSL offload | Ethernet interface |
|---|---|---|---|---|---|---|
| **nFast** | 300 | N/A | No | N/A | No | No |
| **nFast Ultra** | 10,000 | 300 Mbps | No | N/A | Yes | Yes |
| **nForce** | 1,600 | N/A | Yes | Level 2 | No | No |
| **nForce Ultra** | 10,000 | 300 Mbps | Yes | Level 3 | Yes | Yes |

## CORPORATE HEADQUARTERS

**Europe & International**
nCipher Corporation Ltd.
Jupiter House
Station Road
Cambridge, CB1 2JD
United Kingdom
Tel: +44 (0) 1223 723600
E-mail: int-sales@ncipher.com

**North America**
nCipher Inc.
92 Montvale Avenue, Suite 4500
Stoneham, MA 02180
USA
Tel: 800 NCIPHER (800 624 7437)
or +1 781 994 4000
E-mail: ussales@ncipher.com

**Asia Pacific**
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

nCIPHER™

Redefining cryptographic security

www.ncipher.com



NCBR/SSL/JULY2005