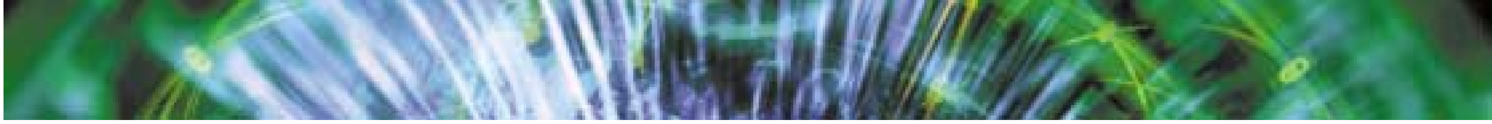
INCREASE THE POWER OF SSL WITH nCIPHER



CREATING A SECURE ONLINE SERVICE

OPTIMIZE WEB SERVER SECURITY

In the world of e-business, where an organization's reputation and its users' loyalty can be shattered in an instant, the powerful session-level security delivered by SSL (Secure Sockets Layer) has emerged as the de facto standard for delivering a secure online service. Internet users routinely look for the closed padlock or unbroken key symbol to appear at the bottom of the browser window as a sign of security and a connection they can trust.

As the use of SSL has increased, so has the need for organizations to optimize their Web infrastructure to efficiently handle the heavy processing demands of SSL — while simultaneously protecting the security of their online services in order to minimize risk, create confidence and build loyalty. Establish trust, and you've unlocked a user's willingness to share private information, transact online and adopt new services in the future.

nCipher's line of nForce™ secure e-commerce accelerators helps companies do just that — speed and protect a secure online service by providing powerful SSL acceleration and flexible, secure key management capabilities.

ENHANCE PERFORMANCE

THE NEED FOR SPEED — SSL ACCELERATION

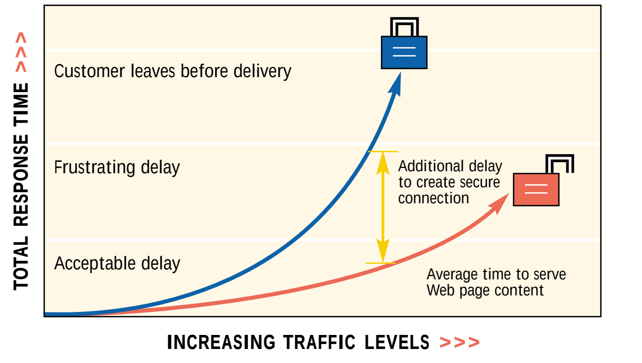
Internet users don’t want to wait for anything. In fact, most won’t wait more than a few seconds to access an online service. How much SSL traffic can your service handle without making users wait?

Unfortunately, Web servers are simply not designed to efficiently handle the heavy processing associated with executing the public key operations required by SSL. Simultaneous SSL sessions can saturate even the fastest of servers, dramatically impacting performance and causing users to wait in “virtual lines” for service.

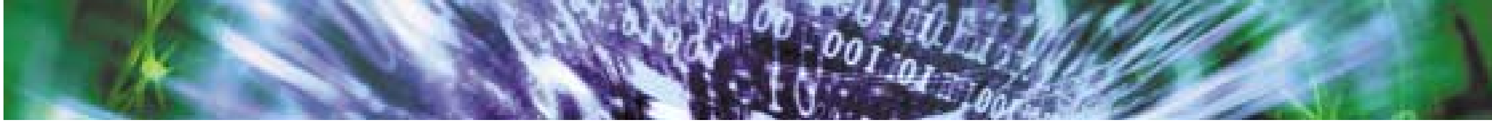
However, by offloading SSL processing from the server to an nCipher acceleration module, you can dramatically increase server processing capacity. nCipher’s powerful acceleration co-processors free the server’s CPU to respond to more customer requests.

Performance

THE CONSEQUENCES OF SUCCESS – E-QUEUES



For example, by adding a single nCipher nForce to a server, you can achieve sustained throughput of up to 400 new SSL connections per second while an unaided server might typically sustain less than 20 new SSL connections per second. In the most demanding applications, additional modules can be added to the same server for even greater throughput.



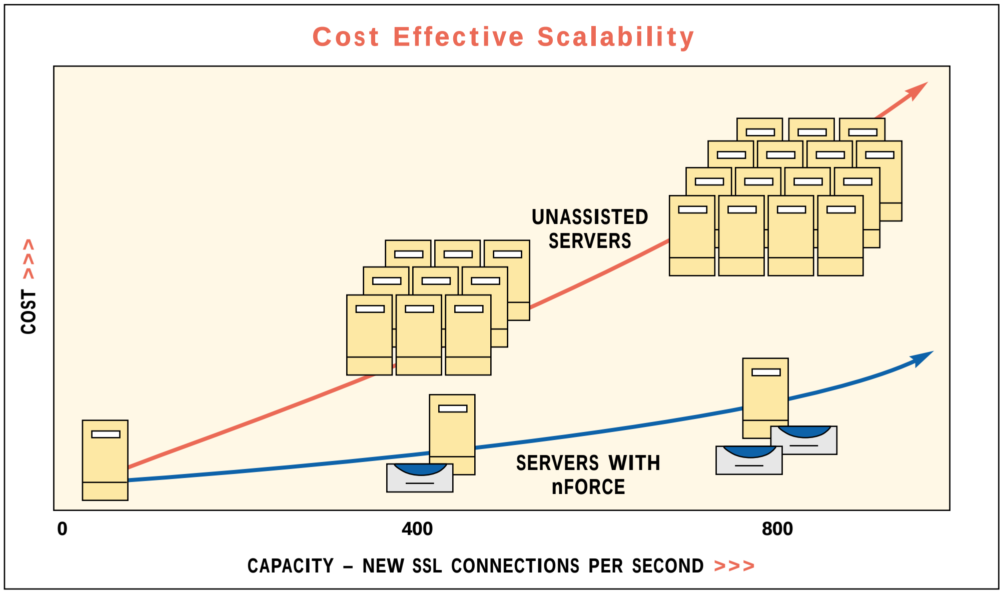
ENSURE SCALABILITY

> You’re an online retailer *and it’s the holiday season. A new advertising campaign launches, highlighting 25% off the hottest toy of the season. Your site is flooded with eager buyers...*

> You’re a financial institution *offering a wide range of investment options. The stock market takes an unexpected downturn, sending a flood of customers to your site to check their portfolios...*

HOW WILL YOUR BUSINESS HANDLE A SUDDEN BURST OF SSL SESSIONS?

Whatever your business, architecting the right capacity for your service’s infrastructure is critical to your ability to maintain customer loyalty. Even under light or predictable traffic conditions, your ability to process new SSL connections is likely to be a system bottleneck just waiting to happen. Simply adding more secure Web pages or experiencing a sudden surge in SSL traffic can leave most organizations facing a serious server performance problem.



Adding servers isn’t the most effective approach to scaling capacity and managing growth: additional servers can be incredibly expensive, provide limited SSL processing capacity and require significant administrative resources.

nCipher SSL accelerators provide an affordable, highly scalable solution that increases your capacity without taxing already overburdened IT staff. Simply install the number of modules required to meet your current capacity needs and add more as your user base and traffic volumes increase — at a fraction of the cost of adding new server hardware with equivalent speed. With built-in automatic load balancing across multiple accelerators and fail over protection, nCipher acceleration modules work together to protect your service from SSL bottlenecks and keep it running at maximum capacity.

INCREASE SECURITY

ADVANCED SSL SECURITY — A CRITICAL COMPONENT IN BUILDING TRUST

As use of your secure online service increases and user confidence builds, the need to protect the continuity and integrity of your service and preserve your users' trust becomes paramount. A comprehensive approach to your secure Web server infrastructure looks beyond performance alone to encompass advanced protection and secure management of the digital keys that underlie your trusted infrastructure.

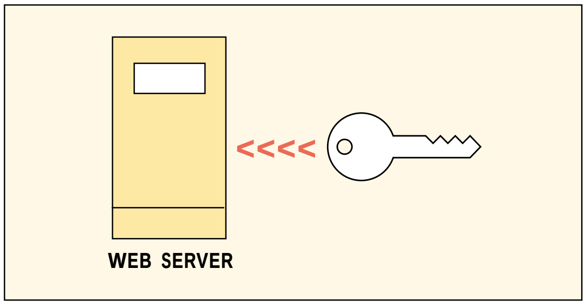
The Web server's digital certificate private key is the primary means of proving a Web site's authenticity and is the cryptographic secret used to create encrypted sessions to each browser. However, while the powerful encryption provided by SSL enables secure communications, SSL can do nothing to protect the private key itself, which if stored in a software environment — and exposed in server memory — leaving it subject to compromise.

If a private key is discovered, for example through a modern key finding attack, the security of the whole system is at risk. Armed with your private key, an intruder can damage the authenticity and privacy of your secure service. When private keys are compromised, organizations are in danger of "spoofing" attacks, where a stolen key is used to impersonate your legitimate Web site, or "eavesdropping" attacks, where a stolen key is used to hack into an online transaction or unscramble earlier transactions. These types of crimes can go undetected, placing both user and online service at risk, never knowing a security breach has occurred.

Organizations that don't properly protect their keys by managing them in a dedicated tamper-resistant hardware environment are putting their customer relationships at tremendous risk. By providing a highly secure facility for the management and protection of private keys, nForce can help protect your keys from compromise while still providing the powerful SSL acceleration capabilities needed to alleviate processing bottlenecks.

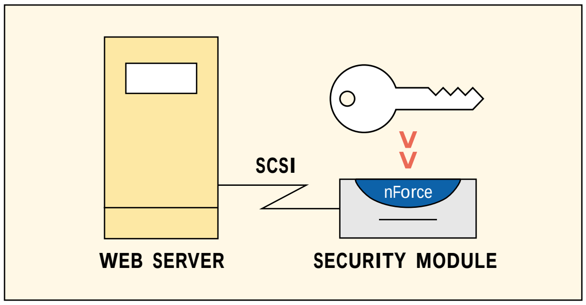
Key Stored in Software on Web Server

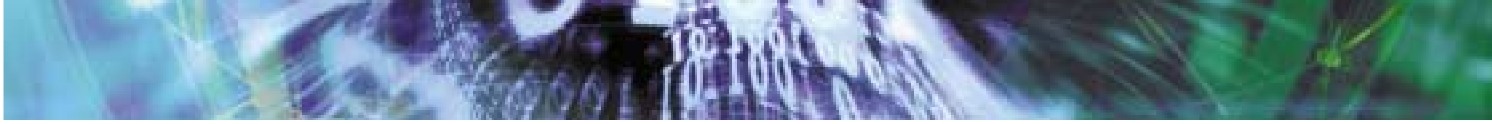
VULNERABLE TO A KEY FINDING ATTACK



Encrypted Key Stored in Hardware

SECURE AND PROTECTED FROM A KEY FINDING ATTACK



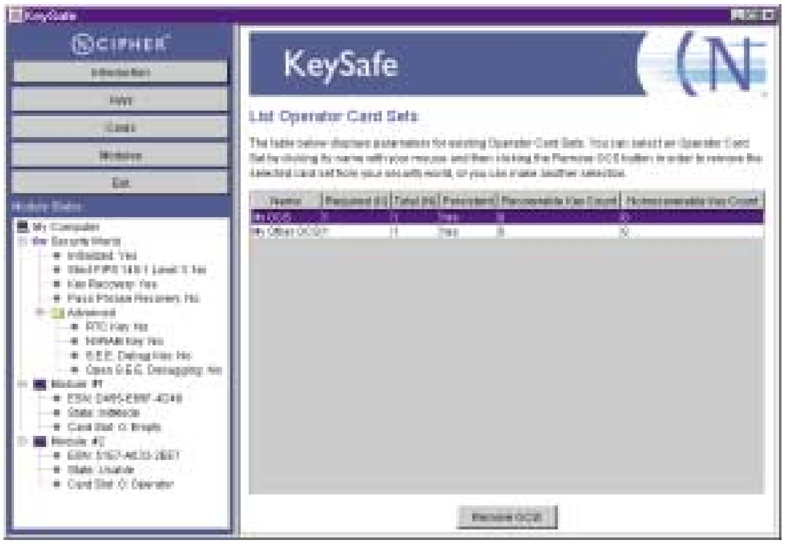


IMPLEMENT MANAGEABILITY

A FLEXIBLE FRAMEWORK FOR EFFECTIVE KEY MANAGEMENT

As a secure online service grows and the number of users increase, securely managing the multitude of keys associated with that service across an enterprise presents a tremendous challenge. How effectively an organization can manage the lifecycle of those keys will ultimately determine how secure the online service will be.

nCipher's nForce security modules combine flexible key management functionality with a highly secure hardware environment making it easy to manipulate and organize keys on a specific device or across a distributed environment of many dispersed devices. nCipher's approach to secure key management is built on a framework known as an nCipher Security World that is independent of the network architecture and supports any number of physical devices and keys. Once you define and initialize an nCipher Security World, you'll be able to define security policies, implement disaster recovery mechanisms and create failover practices. The use of smart cards to authenticate administrators and then grant access rights to manage a security world provides a highly flexible means of defining and sharing responsibilities between individuals within the organization.



List Operator Card Sets

KeySafe

COMPLETE LIFE-CYCLE KEY MANAGEMENT

KeySafe™ provides a convenient and easy to use graphical interface for the key management capabilities of nForce products. KeySafe allows organizations to securely create, store, import, back-up, restore or remove private keys for a variety of applications.

nCIPHER SECURE E-COMMERCE ACCELERATION

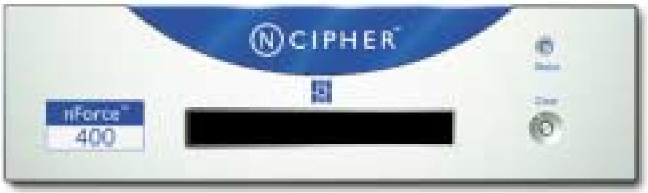
CHOOSING THE RIGHT nCIPHER SOLUTION FOR YOUR BUSINESS

Explore the chart below to determine which nCipher solution is right for your business.

		Security Requirements	
		MODEST	ENHANCED
Site Traffic	PREDICTABLE & LIGHT	**Standard Software** If your SSL traffic levels are light and your service requires only a modest level of security, then standard server platforms should meet your needs today. However, planning and anticipating your future security and scalability needs is essential.	**nForce & KeySafe** If delivering a high-level of security is critical to the success of your online service, a hardware based security infrastructure is essential. Until your traffic levels grow, nCipher's nForce 150 combined with KeySafe is the right solution for you.
	DYNAMIC OR HEAVY	**nFast** If performance is your greatest challenge and security is not a serious consideration, then nCipher's nFast™ acceleration modules can provide a cost-effective solution for increasing your server's processing capacity.	**nForce & KeySafe** If delivering a high level of security in a highly scalable environment is critical to the success of your online service, the combination of nForce 300 or 400 with KeySafe provides the SSL processing acceleration and security assurance you need to deliver a trustworthy, reliable service.

Partnering for Interoperability

nCipher is committed to provide support for all common SSL based applications to reduce support costs and shorten time to market. To achieve this, nCipher partners with leading Web server and application platform vendors to deliver certified interoperability and establish performance metrics. Visit our Web site www.ncipher.com for a complete list of nCipher partners.



nForce

SECURE E-COMMERCE ACCELERATOR

nFast

E-COMMERCE ACCELERATOR

nCipher is a leading developer of hardware and software Internet security products that help global e-businesses maximize information security, system scalability and transaction processing performance in electronic commerce and public key infrastructure applications.

Many of the world's leading organizations requiring the highest level of online security — from Microsoft to Barclays Bank to the U.S. Navy — use nCipher products to protect their information assets and global networks from external and internal security risks. nCipher's products are particularly well suited to organizations seeking to manage risk, boost system performance or innovate new online services , such as financial institutions, e-retailers and online service providers (ISP/ASPs).

Visit nCipher at **www.ncipher.com**

NCIPHER™

CORPORATE HEADQUARTERS

Europe, Middle East & Africa
nCipher Corporation Ltd.
Jupiter House
Station Road
Cambridge, CB1 2JD
United Kingdom
Tel: +44 (0) 1223 723600
Fax: +44 (0) 1223 723601
E-mail: sales@ncipher.com

The Americas & Asia Pacific
nCipher Inc.
500 Unicorn Park Drive
Woburn, MA 01801
United States
Tel: 1 800 NCIPHER (1 800 624 7437)
or +1 781 994 4000
Fax: +1 781 994 4001
E-mail: ussales@ncipher.com

Every effort has been made to ensure the information included in this data sheet is true and correct at the time of going to press. However, the products described herein are subject to continuous development and improvement, and the right is reserved to change their specifications at any time.