

# **End-to-End Secure Connections Over The Internet**

**A Resource Guide for Internet Security Managers**

## ***Introduction***

The importance of maintaining the security of Internet transactions and ensuring the integrity of sensitive information is readily apparent in today's business world. Security is critical to e-commerce as well as within the corporate intranets and extranets used to connect businesses with their partners. Firewalls serve to secure the perimeter, but they cannot protect against security breaches from within. Disgruntled employees, physical location visitors, and contractors can circumvent access control measures to intercept or tamper with transmitted and stored data. Providing methods of securing data during transmission has meant relying on secure web servers to process all security-related data, dramatically reducing their performance and forcing clients to wait for transaction requests to be filled.

## ***Secure Sockets Layer (SSL) Basics***

Several security-related protocols are in use on the Internet, including Secure Electronic Transaction (SET), Secure Hypertext Transfer Protocol (SHTTP), and Secure Sockets Layer (SSL). The protocols most relevant to e-commerce are SSL and SET, with SSL being used predominantly. SSL isn't a single, standalone protocol. Instead, it consists of a set of standardized routines for verification of entities and encryption and decryption of data. Two pieces of information are critical for SSL: keys and certificates.

Keys, public and private, are ciphers used to encrypt and decrypt data. Though public keys are given away quite freely, private keys are never shared. The device responsible for SSL encryption and decryption keeps the private key and shares the public key with clients requesting a secure connection. Sharing public keys may sound like a potential breach of security; however, the two types of keys complement each other. Data encrypted with the public key can only be decrypted with the private key. SSL also employs a client-created session key, used only for a single secure transaction session.

Clients rely on the entity's certificate to prove the entity's identification. Certificate Authorities (CAs) such as Thawte and VeriSign are non-interested parties that issue certificates in response to entity requests. Each certificate acts as a digital identification card, containing several pieces of data:

- The entity's name
- The name of the CA that issued the certificate
- The certificate's expiration date
- The entity's public key

## ***The Burden of SSL***

The data encryption and decryption routines aren't simple substitution codes, but consist of high-level mathematical functions. The majority of web servers are not designed to perform these calculations as well as provide normal page retrieval services. And even the fastest server and OS combinations are adversely affected by SSL slowdown. SSL content may be delivered up to 50 times slower than typical HTTP content. In some cases, up to 90% of the CPU capacity is used for page retrieval for a single SSL connection. A typical web server may slow from approximately 750 connections per second while delivering non-secure services to only 13 connections per second for SSL-enabled).

Providing secure services not only impairs the performance of a web server, it contributes to increased downtime and reduces the server's life span. Overworked processors are notoriously unstable. This instability leads to crashes, which are a catastrophe when servers of any kind are involved, especially those responsible for secure data processing.

As the strength of ciphers increases in response to increased security concerns, the performance hit worsens. Ciphers vary in strength with the strongest being reserved for domestic use. While the 40-bit ciphers most commonly used in the recent past have been considered secure, 128-bit ciphers used today are much safer and are becoming standard as security requirements increase. The stronger the cipher, the more intensive the mathematical calculations needed to use it.

This decrease in performance has a terribly detrimental effect on customer satisfaction. A Zona Research study indicates that users are willing to wait only about eight seconds for a page to load. After 8 seconds, customers go somewhere else. And they think twice about coming back to the same site. According to Forrester Research, 42% of people who leave a site because of a bad experience will never go back. As web page loading times continue to increase during an intensive SSL processing session, customers have even less patience. During the 1999 holiday season, up to 88% of online buyers left e-commerce sites before the transactions were completed, according to The Industry Standard.

## ***Increasing Performance of Secure Servers***

To solve these SSL-related problems some way must be found increase SSL transaction performance. The most effective solution is to transfer the job of processing the SSL routines from the web server to a specially designed device to do the job quickly and efficiently. SSL accelerators and offloaders were created to fill this niche.

Accelerators take some of the SSL processing burden from overworked web servers by performing the initial encryption/decryption routines. With an accelerator in place, performance of web servers increases significantly but does not approach the performance of processing non-secure transactions. SSL accelerators are available as network devices, PCI cards, and via USB/SCSI dongles. However, accelerators don't solve the burden problem completely. They perform only some of the SSL routines: a secure web server is still required. This means an accelerator cannot be placed in front of a load balancer to enable URL- and cookie-based load balancing schemes.

Data flow with an accelerator in place differs slightly from the flow of an SSL transaction involving a secure server.

A much better solution is to use an SSL offloader to remove SSL routines from the web server. A secure server is not required because the server is no longer required to perform any SSL processing procedures. In this case, the offloader is the first point of contact with the client, as shown in Figure 5.

Now the web server is free to provide secure requests at the same high speeds as non-secure requests are supplied. Client applications and, more importantly, prospective customers do not notice any slowdown in processing or page loading. In addition, key and certificate management is streamlined tremendously. Keys and certificates are loaded only once—directly and securely into the offloader. Individual applications no longer need to be manually configured with each piece of SSL information. Because there is no reliance upon a secure web server, an offloading network device can be placed in front of a load balancer to enable cookie-based and URL-parsing load balancing schemes.

Using an offloading appliance still leaves the same security hole as with network device-based accelerators: the data is not secure from the device to the server. The ultimate solution, providing both fast and efficient SSL processing and a high level of security, is the installation of a PCI-card offloader directly into the server. Two major benefits of this strategy, to systems administrators are:

- Server performance for secure connections is boosted to that of non-secure levels
- Transactions are secured from the client all the way to the server

## **Conclusion**

Security requirements will only increase, and systems administrators will be hard-pressed to provide efficient and reliable secure services to users. PCI-based SSL offloading devices are a superior tool that can be brought into service to help ensure speedy and secure connections.

## **SonicWALL SSL Offloading Products**

SonicWALL designs and manufactures the SSL offloading products listed below.

### **SonicWALL SSL-IA**

SonicWALL SSL-IA enables eCommerce sites to transact secure business and deliver sensitive information quickly, confidentially and without errors. The SonicWALL SSL-IA performs all key management and encryption for the Internet user's session, offloading this heavy burden from web servers. The result is tremendous performance boost for busy eCommerce sites.

- Enables eCommerce sites to perform secure transactions quickly and confidentially
- Boosts performance of secure web sites up to 50 times
- Offloads the management and encryption of all sensitive information
- US retail \$4,995

### **SonicWALL SSL-PCI**

The SonicWALL SSL-PCI is a secure transaction processor in the form factor of a PCI card. When installed in any server in a web site cluster, the SonicWALL SSL-PCI is the only product that creates a secure connection all the way from the server to the customer's browser.

- Provides end-to-end security, from client browser to secure server
- Replaces the Ethernet NIC in a server with Secure Sockets Layer (SSL) processor
- Offloads the management and encryption of all sensitive information
- US retail \$2,995

### **SonicWALL, Inc.**

348 East 4500 South  
Salt Lake City, Utah 84107  
(801) 743-2200 (phone)  
(801) 743-2201 (fax)  
[www.sonicwall.com](http://www.sonicwall.com)