SSL Acceleration: A Technology Primer

SONICWALL

Overview

Secure transactions are a necessity with e-commerce and sensitive corporate intranets and extranets. The Secure Sockets Layer (SSL) protocol is the widely used means for transmitting data securely over TCP/IP networks. SSL protection, however, comes at a high cost on the performance of Web servers because of its CPU-demanding authentication schemes and encryption/decryption of data.

This SSL overhead can result in the undesirable consequences of lost connections, lost productivity, and lost sales. Whether it's a Web-enabled application like Oracle, PeopleSoft, or Siebel, a Web site delivering secure content, or an e-commerce site, the impact of the SSL burden can have a direct impact on the bottom line. According to Zona Research, users are willing to wait 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. Of those users who leave a site because of a bad experience, 42% never go back (Forrester Research).

Many secure Web sites began to employ SSL accelerators to boost their performance. These early SSL accelerators were limited solutions that lacked flexibility and scalability. Today's next generation of SSL accelerators, also known as SSL offloaders, are complete, robust solutions that deliver reliable, scalable, and cost-effective handling of SSL traffic for enterprises, data centers, co-location and Web hosting facilities, and application service providers (ASPs).

This paper explains the basics of the SSL protocol, how SSL impacts Web site performance, and how today's SSL acceleration technology can dramatically boost the performance of secure Web sites.

SSL in the Real World

SSL is widely deployed to support a wide range of secure transactions, and it promises to play an even more important role as more and more services are made available online. Today, SSL is used as the secure basis for:

- Access to mission-critical applications such as Oracle, PeopleSoft, and Siebel from any web browser
- Storefront sites for taking orders and processing credit card transactions
- Financial sites for banking, stock trading, and bill payment services
- Healthcare providers for sharing confidential medical information

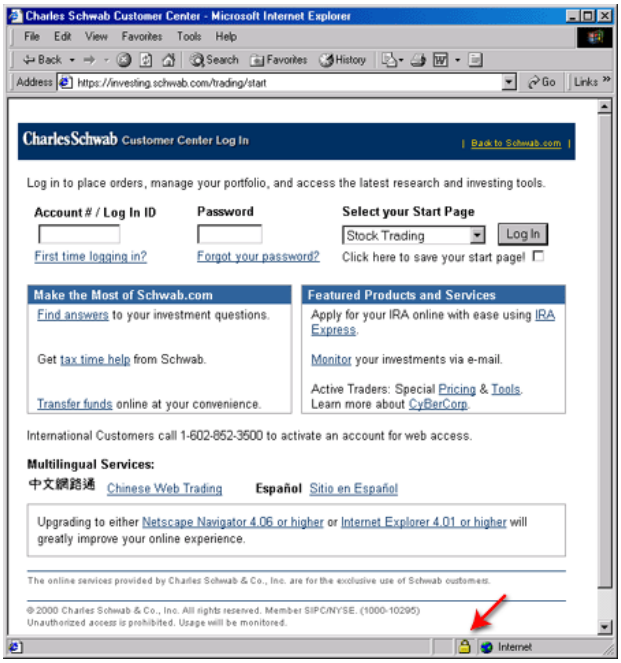
- Insurance companies for providing online access to agents and customers
- Business-to-business e-commerce service providers
- Government services requiring confidentiality of data including tax, Social Security, military, and health information
- Travel sites for making reservations and online ticketing
- Intranets for protecting confidential information within organizations
- Extranets for secure access to company resources by partners, vendors and key customers

What is SSL?

The connection between a Web browser and any point on the Internet is routed through dozens of independent systems without any protection of confidential information. Neither the user nor the Web server has any control over the path their data takes, nor can they control who examines the data along the route. To protect confidential information on the Internet or any TCP/IP network, SSL incorporates the following elements to establish secure transactions:

- **Site Authentication**. Ensures the identity of the site you are doing business with on the other end of the connection. Likewise, Web sites need to verify the identity of their users.
- **Data Confidentiality**. Ensures the data is not accessible by a third party. To eliminate eavesdropping of sensitive data as it passes through the Internet, the data must be encrypted to make it unreadable except for the sender and receiver.
- **Message Integrity**. Ensures the data is not altered and it is the exact representation of the information originally sent.

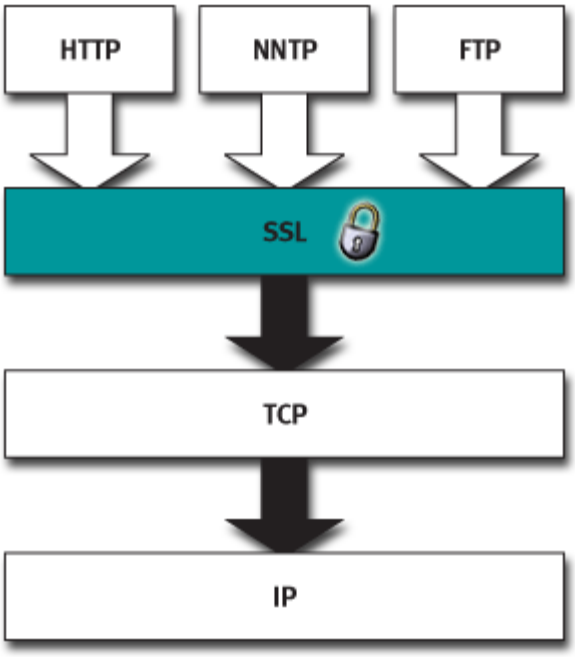
With SSL enabled, Web sites can safely provide confidentiality, authentication and message integrity to its Web users. The SSL is integrated into every browser and every Web server, allowing any user to interact with any Web site in a secure manner. When a Web browser is using an SSL connection to a server, a pad lock icon appears on the status bar of the browser window and the standard “http” entry in the URL address changes to “https.” An SSL HTTPS session uses TCP port 443 instead of TCP port 80 used for unsecured HTTP sessions.



Inside the SSL Protocol

Originally developed by Netscape, the Secure Sockets Layer (SSL) protocol is now universally accepted on the World Wide Web for authenticating and encrypting communication between client and servers. The Internet Engineering Task Force (IETF) has taken responsibility for the SSL standard and changed its name to Transport Layer Security (TLS). Despite the name change, TLS is just a new version of SSL. TLS version 1.0 is the equivalent of SSL version 3.1. SSL is the more widely used term.

SSL was designed as a separate protocol for security to enable it to support multiple applications. The SSL protocol runs above TCP/IP and below higher-level application protocols like HTTP (HyperText Transport Protocol), IMAP (Internet Messaging Access Protocol) and FTP (File Transport Protocol). While SSL can be used to support secure transactions for a variety of Internet applications, SSL is used primarily for Web-based transactions.



SSL isn't a single, standalone protocol but instead consists of a set of standardized routines that perform the following security tasks:

- **SSL Server Authentication**. Enables a user's Web browser to confirm a server's identity. SSL-enabled browsers use standard techniques of public-key cryptography to check that a server's certificate and public ID are valid and have been issued by a certificate authority listed in the client's list of trusted CAs.
- **SSL Client Authentication**. Allows a server to confirm a user's identity. Using the same techniques as those used for server authentication, SSL-enabled server software can check that a client's certificate and public ID are valid and have been issues by a certificate authority (CA) listed in the server's list of trusted CAs.
- **Encrypted Connection**. Requires all information sent between a client and a server to be encrypted to provide a high degree of confidentiality to protect both parties of any private transaction. All data sent over an encrypted SSL connection is also protected with a mechanism for detecting tampering called a hash algorithm to ensure the data has not been altered in transit.

SSL Cryptography

Integral to the SSL protocol is its use of cryptographic algorithms, commonly referred to as ciphers. A cipher is a mathematical function

used to perform the encryption and decryption, which is the process of scrambling information so it's unintelligible to anyone but the intended recipient.

The SSL protocol supports the use of a variety of different ciphers for such operations as authenticating the server and client to each other, transmitting certificates, and establishing session keys. Clients and servers can support different cipher suites, or sets of ciphers, depending on factors such as the version of SSL they support, company policies regarding acceptable encryption strength, and government restrictions on export of SSL-enabled software.

Keys

An essential element of cryptography is the use of secret codes, called keys, which are shared only by the communicating parties. Cryptography uses keys that enable users at each end of the connection to lock and unlock encrypted data. These keys are unique identifiers made up of data strings that vary in length depending on the cipher method used. An important quality that determines the effectiveness of a cipher is the size of the secret key. The larger the key, the more difficult it is to break the code.

Cryptographic techniques fall into two classifications, depending on the types of keys they use: secret key cryptography and public key cryptography. With secret key cryptography, both parties know the same key and both keep the key secret from everyone else, which is why this type of keys are known as symmetric encryption. Encryption algorithms based on secret key techniques are mathematical transformations on the data to be encrypted combined with the secret key itself.

Most of the problems with secret key cryptography are caused by the keys themselves in their distribution between the two parties. Public key cryptography or asymmetric cryptography eliminates the key distribution problem. With public key cryptography, each of the two parties use separate keys: one for encryption and a different one for decryption. The critical aspect of public key cryptography is that only one of these two keys needs to be kept secret. The other key, the public key does not need to be kept secret at all.

Public-Key Infrastructure (PKI) is the leading means by which public keys can be managed on a secure basis for use by widely distributed users. Public-key cryptography based on Public-Key Infrastructure (PKI) requires the use of digital certificates and certificate authorities.

Digital Certificates

A certificate or digital certificate is an electronic document used to identify an individual, a server, a company, or some other entity and to associate that identity with a public key. Acting like a driver's license or a passport,

a certificate provides a generally recognized proof of a person's identity. Public-key cryptography based on PKI uses certificates to address the problem of impersonation.

Certificates are issued by certificate authorities (CAs), which are trusted third parties, such a VeriSign, that issue certificates in response to entity requests. CAs can be either independent third parties or organizations running their own certificate-issuing server software. Each certificate acts as a digital identification card. The certificate issued by the CA binds a particular public key to the name of the entity the certificate identifies. Certificates help prevent the use of fake public keys for impersonation. Only the public key certified by the certificate will work with the corresponding private key possessed by the entity identified by the certificate.

SSL Acceleration

SSL acceleration uses optimized devices built to handle the CPU-intensive requirements of SSL transactions. SSL accelerators dramatically boost the performance of SSL transactions up to 50 times faster than servers alone. SSL acceleration technology has evolved with changes in Web site persistence methods and the rise large, multi-server Web sites utilizing load-balancing solutions to efficiently route traffic across all Web servers.

SSL Acceleration and Web Site Persistence

In the early days of SSL transactions, static IP addresses provided the basis for Web site persistence. Persistence, commonly referred to as stickiness, is a requirement of stateful applications. An example of persistence is the online shopping cart, where information is unique to a client session, necessitating that the client connect to the same Web server for the life of the session. SSL plays a critical role in the process of securing these persistent connections.

When the wide spread deployment of proxy servers caused source IP addresses to change frequently for users through the life of the session, it impacted the way Web sites could maintain persistence for SSL transactions, and in turn impacted the way sites could balance their data traffic among servers. SSL transactions could no longer be handled using IP-based load balancing for Web sites. Multi-server Web sites utilizing IP-based load balancing solutions needed new switching solutions and new SSL acceleration technologies to utilize the higher-layer persistence methods, such as URLs, file extensions, headers, and especially cookies. A cookie is a block of data that a Web server stores on a client system. When a user returns to the Web site, the browser sends a copy of the cookie back to the server to identify the user, instruct the server to send customized Web pages, submit account information, and provide other

information. This ushered in the next generation of load balancing solutions called content switches.

SSL Acceleration and Content Switches

Content switches were the next evolutionary step for Web site load balancing. Content switches offer an intelligent form of load balancing by working at higher network layers. By providing such powerful inspection and switching capabilities at higher network layers, content-switches introduced the much-needed ability to switch data based on URL information, file extensions, headers, cookies, etc. Of particular importance was the cookie-switching capability, because this allowed content-switches to provide stickiness with a reliable mechanism. No matter how many times the client IP address might change during a session, the cookie would always be returned, and could always be used for persistence.

The big weakness of content switching was the handling SSL transactions. Sessions encrypted with SSL prohibited the content switch from inspecting data packet to enable smart switching for Web sites based on application layer information. This ushered in the next generation of content-switch friendly SSL acceleration technology.

Evolution of SSL Accelerators

SSL accelerators were originally introduced to solve the problem of high CPU utilization incurred by the SSL handshake. While these SSL accelerators dramatically reduced CPU utilization for individual server, they proved to be limited in flexibility and scalability and didn't perform the bulk encryption and decryption of SSL data.

The next generation of SSL accelerators, also known as SSL offloaders, took cryptographic computational assistance one step further by handling not only the public-key cryptographic functions but also the bulk data encryption and decryption, offering even greater performance benefits. These devices provide a complete SSL offloading solution with increased security over server-based solutions.

The only drawback with early versions of SSL offloaders was their deployment required an inline configuration where all the Internet data traffic, SSL and non-SSL, passed through the SSL offloader before going to content switch and then on to the Web servers. This created a bottleneck for data traffic and introduced a single point of failure for Web sites. In response to this problem, vendors included fail-over, fail- through, and spill- through designs, allowing for redundant active/passive configurations or chained (aggregated) installations. These modifications addressed some of the problems, but didn't truly solve them because the attempts were inefficient, still obtrusive, and still limited in their scalability.

SonicWALL SSL Offloaders

SonicWALL SSL Offloaders takes on the job of processing SSL transactions, freeing up valuable Web server resources at a fraction of the cost of additional web servers. SonicWALL's content-switch friendly SSL offloading innovation eliminates the bottlenecks of placing the SonicWALL SSL Offloader in front of all Internet data traffic. This technology allows the SonicWALL SSL Offloader to integrate with the content switch, enabling the switch to make intelligent decisions on unencrypted data.

The content switch redirects all port 443 (HTTPS) requests to the SonicWALL SSL Offloader, which handles the SSL handshake, decrypts the data, and then sends the clear text to the content switch. The content switch then routes the clear text to the Web servers. Upon the return of the data, the clear text is encrypted and sent back to the client.

SonicWALL's One-Port Offloader technology offers flexible configuration with the content switch by allowing a single port to be used for both ingress and egress traffic with no performance degradation. This allows for greater port utilization for content switches where per port costs run high.

The simple, drop-in deployment of SonicWALL SSL Offloaders allows Web sites to quickly add capacity reserve to handle surprise peak demand. And because SonicWALL SSL Offloaders are self-contained and interoperate seamlessly with traffic managers and servers, no updating or reinstallation of specialized cryptography hooks are required for servers, content switches or routers.

SonicWALL SSL Offloader Features and Benefits

SonicWALL SSL Offloaders deliver industry-leading price/performance for the enterprise, data centers and service providers. They offer cost-effective solutions for boosting Web site performance without adding expensive servers. SonicWALL SSL Offloaders also work seamlessly with Cisco, and other vendor content switches to deliver a comprehensive, content-switch friendly SSL offloading solution.

SonicWALL's high-performance SSL Offloaderss deliver these features and benefits:

- **Performance**. Dedicated high-performance SSL offloading eliminates the need for costly multiple-server deployment and maintenance. SonicWALL SSL Offloaders deliver increased performance and security for Web sites and commercial applications like Oracle, PeopleSoft, Siebel, SAP, WebLogic, iPlanet, etc.
- **Offloads All SSL Processing**. Transparently offloads all encryption, decryption and secure processes using a powerful

embedded processor, freeing Web servers to perform essential tasks and guaranteeing end-to-end security from server to browser

- **Strong ROI**. SonicWALL SSL Offloaders offer industry-leading price/performance for offloading SSL transactions at a fraction of the cost of deploying HTTPS servers. At significant savings over competing SSL accelerators, SonicWALL SSL Offloaders are a cost-effective way to dramatically boost the performance of your secure Web site and applications while providing complete security.
- **Simple Deployment**. Offers a variety of deployments to operate independently or in concert with a vast array of core and edge network components, meeting the needs of your existing production network with little downtime or installation headaches. Ease of installation and little or no maintenance reduces administration time, overhead, and costs.
- **Content Switch Friendly**. Integrates seamlessly with Layer 4 load balancers and Layer 5-7 content switches to manage SSL traffic and maximize Web site efficiency, enabling comprehensive secure content networking and guaranteeing a swift and persistent customer experience.
- **Reliable**. A solid-state architecture with no critical moving parts and redundant power supplies ensures maximum reliability and eliminates potential failures common to PC-based SSL appliances. Multiple SonicWALL SSL Offloaders can be combined to create highly available SSL transaction processing and redundancy to keep your secure Web site and applications up and running.
- **Flexible Management**. Can be configured and managed using several management interfaces including serial-based CLI, Telnet, Web-based GUI, and HTTPS and TelnetS encryption for secure communications.
- **Back-End Encryption**. Initiate SSL sessions to an SSL termination point on another device, delivering end-to-end security while still allowing the content switch to make intelligent routing decisions.
- **SSL Aggregation**. End-to-end security for all SSL transactions at a fraction of the overhead normally associated with establishing multiple connections, guaranteeing no clear text for highly secure environments.
- **Secure URL Rewrite**. SonicWALL's unique Secure URL Rewrite feature dynamically eliminates potential data exposure and risks common to most Web-enabled applications, with no additional coding or changes to the application.

- **Certificate and Key Management**. Centralized management of up to 4,095 keys and certificates, with better security of certificates over server-based management options.
- **Client Certificate Support**. Enforce client certificates during the SSL handshake for mutual authentication. The certificate information can then be forwarded back to the secure server via multiple methods.
- **Advanced Authentication Support**. Supports most authentication platforms with customizable back-end authentication capabilities using extensive HTTP header definitions.
- **Ciphers and Random Number Generation**. Only the SonicWALL SSL-RX uses dedicated hardware to accelerate not only RSA operations, but all cryptographic functions including symmetric ciphers, message digests, and random number generation.

SonicWALL SSL Offloaders

SonicWALL's high-performance SSL Offloaders dramatically increase the performance and security of Web-enabled applications and Web sites, enabling comprehensive secure content networking and guaranteeing a swift and persistent customer experience.

SonicWALL's family of SSL Offloaders increases the performance and security of Web sites and applications at a fraction of the cost of HTTPS server, transparently integrating with load balancers and content switches to deliver a comprehensive, secure content networking solution.

SonicWALL SSL-R Offloader

- Up to 200 RSA operations per second and 5,000 concurrent connections
- Seamless integration with load balancers and content switches
- Redundant power supplies for mission-critical processing
- Stores up to 255 keys and certificates

The SonicWALL SSL-R Offloader is an affordable 1U rack mount, 2-port SSL offloading solution that supports up to 200 peak RSA operations per second and up to 5,000 concurrent connections. Seamless integration with Layer 4 load balancers and Layer 5-7content switches ensures persistence for secure content networking environments, enhancing site performance and content location flexibility.

SonicWALL SSL-R3 Offloader

- Up to 600 RSA operations per second and 15,000 concurrent connections

- Seamless integration with load balancers and content switches
- Redundant power supplies for mission-critical processing
- Stores up to 765 keys and certificates

The SonicWALL SSL-R3 is a 6-port, high-performance 1U rack-mount SSL offloading solution that supports up to 600 RSA operations per second and 15,000 concurrent connections. Seamless integration with Layer 4 load balancers and Layer 5-7 content switches ensures persistence for secure content networking environments, enhancing site performance and content location flexibility.

SonicWALL SSL-R6 Offloader

- Up to 1,200 RSA operations per second and 30,000 concurrent connections
- Seamless integration with load balancers and content switches
- Redundant power supplies for mission-critical processing
- Stores up to 1,530 keys and certificates

The SonicWALL SSL-R6 is a 12-port, high-performance, 1U rack-mount SSL offloading solution that supports up to 1,200 RSA operations per second and 30,000 concurrent connections. Seamless integration with Layer 4 load balancers and Layer 5-7 content switches ensures persistence for secure content networking environments, enhancing site performance and content location flexibility.

SonicWALL SSL-RX Offloader

- Up to 4,400 RSA operations per second and 30,000 concurrent connections
- Seamless integration with load balancers and content switches
- Redundant power supplies for mission-critical processing
- Stores up to 4,095 keys and certificates

The SonicWALL SSL-RX Offloader is the industry's leading price/performance SSL offloading solution, a 1U rack-mount 2-port SSL offloader that supports up to 4,400 RSA operations per second and 30,000 concurrent connections. Seamless integration with Layer 4 load balancers and Layer 5-7 content switches ensures persistence for secure content networking environments, enhancing site performance and content location flexibility.

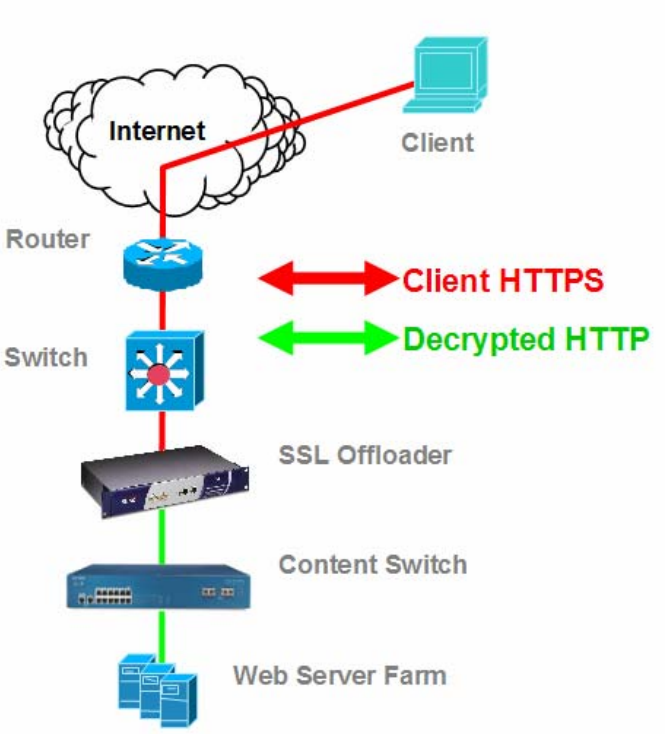
Deployment Strategies

SonicWALL SSL Offloaders can be deployed in many different Web site environments and configurations, dramatically boosting the performance of Web-enabled applications and servers. For Web caching servers or

appliances, which can't work with encrypted data, SonicWALL SSL Offloaders can be deployed to decrypt the SSL content before it hits caching server. Networks using content switches to deliver secure content are the most common solution today, and SonicWALL's Offloaders can be integrated seamlessly with content switches using three deployment strategies.

SSL Inline Configuration

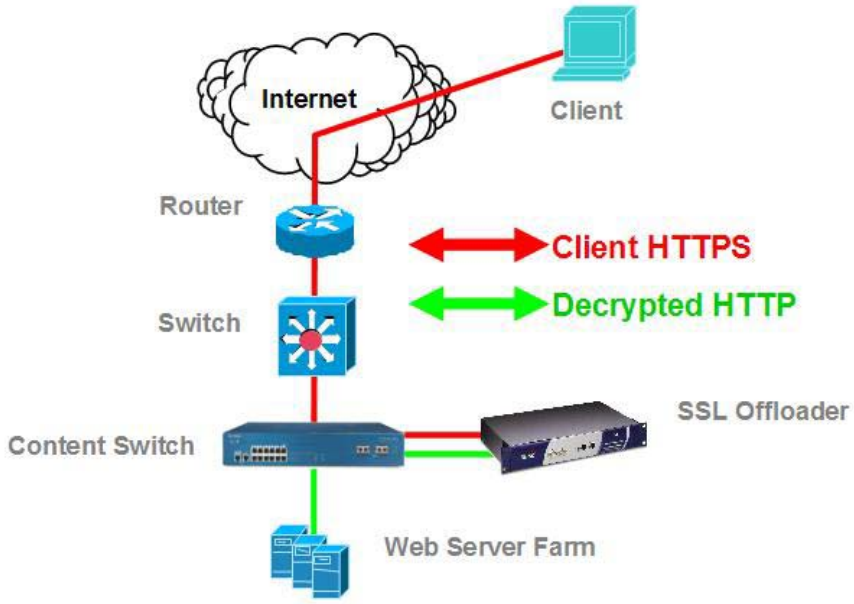
In an inline configuration, the content switch is front-ended with one or more SSL Offloaders, decrypting and encrypting all SSL traffic so the content switch can intelligently read the data. The SSL Offloaders will intercept all Port 443 traffic for those IP addresses configured on it, decrypt the data, and then forward it as clear traffic (Port 81) to the other content switch. The secondary switch will not have any Port 443 content rules defined since all traffic that terminates on it is decrypted.



SSL One Port Proxy Configuration

In a one port proxy configuration, the content switch is configured with both Layer 4 and Layer 5 rules, while the SonicWALL SSL Offloader

operates in non-transparent mode and behaves as a standard TCP/IP proxy. The client thinks it is talking to the device and sees both the device's IP address and MAC address, while the server sees the device connecting with the device's IP address and MAC address. Since the SonicWALL SSL Offloader is configured only at Layer 4, and the switch changes the destination IP address to the SSL offloader's IP address, the SSL offloader must use a technique other than IP address to ensure that the traffic is routed to the correct original server. This is accomplished by configuring multiple Destination IP/Destination Port pairs on the SonicWALL SSL Offloaders.



One-Armed SSL Offloading in Transparent Mode

In a one-armed transparent configuration the content switch treats the SonicWALL SSL Offloader as a cache device, enabling the transparent SSL offloader to use content rules on the switch. The content switch routes all Port 443 traffic to the SSL offloader. The IP stack on the SSL offloader terminates the TCP session and replies on behalf of the server. The source MAC address of the TCP/IP packets is the MAC addresses of the SSL offloader. This keeps the SSL session returning to the correct SSL offloader on the content switch. Once the SSL negotiation has been completed, the SSL offloader continues to handle the bulk decryption and encryption work. The SonicWALL SSL Offloader passes the clear text back to the content switch on Port 81. The clear text is then load balanced across the Web server farm using normal load balancing algorithms.

Because the SSL offloader has sent the client IP address (transparent mode) with it's own MAC address, the Web applications know the client IP address and the content switch is able to return responses to the correct SonicWALL SL Offloader for encryption back to the client.

Conclusion

Web sites delivering mission-critical applications, e-commerce services, or secure personalized information use Secure Sockets Layer (SSL) to secure transactions over the Internet. SSL acceleration enables secure Web sites to cost-effectively and dramatically boost secure Web site performance. SonicWALL's industry-leading SSL Offloaders deliver high performance, content-switch friendly solutions for the enterprise, data centers and service providers to ensure rapid response time for secure content.

To learn more on how SonicWALL SSL Offloaders can boost the performance and security of your Web servers at a fraction of the cost of deploying more HTTPS servers, call 1-888-557-6642 or visit us at www.sonicwall.com.