

# Overview of SSL Acceleration Implementations

By Chad W. Engelgau and Sanjeet Singh

**Increases in SSL-based traffic hinder the performance of today's Web server infrastructure. Web-enabling corporate applications and the need for higher security exacerbate this problem. This article examines the various SSL implementations available today and analyzes how a centralized SSL acceleration infrastructure can increase the capacity of a system to accommodate SSL traffic.**

Secure Web environments are no longer limited to e-commerce implementations; more and more enterprise applications require Web server security. The Secure Sockets Layer (SSL) protocol is the de facto standard to secure Internet and intranet transactions as well as communications between users and applications. In fact, SSL is the primary means of securing Transmission Control Protocol/Internet Protocol (TCP/IP) traffic regardless of the network topology.

Increasing SSL traffic minimally affects overall network performance, but processing the SSL traffic can adversely affect server performance, which slows the performance and response times of Web sites and Web-based applications.

Today's increasingly SSL-dependent computing environments require more than just faster processors; they require products that off-load encryption and decryption processing from the servers while maintaining data transfer security. The appropriate SSL implementation will also increase server performance, decrease certificate management, and address the need for persistence in the communication process.

## Corporate uses of SSL

SSL ensures more than secure credit card transactions over the Internet. Many organizations use

SSL to provide secure communication between users and applications. This security is the basis for corporate applications such as the following:

**Enterprise intranet applications.** Companies around the world are deploying enterprise resource planning (ERP), customer relationship management (CRM), and personnel management systems on the Internet. Many companies also use their intranets to exchange these and other types of confidential information. Because the data transmitted from these applications must remain secure, encryption is a requirement.

**Business-to-business (B2B) solutions.** The increasing speed of business demands direct and automated communication with partners and suppliers. Extranet-based communications (tying together two business partners' networks) and B2B applications that focus on supply chain management, purchasing, or billing require secure communication channels. These systems and applications rely on the guarantee that the information each company shares is safe and retrieved only by the intended party.

**Human resources and benefits sites.** Providing employees with secure, Web-based access to their personal data has become the norm for most companies. Human resources policies, employee data, payroll information and records, and health

---

The appropriate SSL implementation will increase server performance, decrease certificate management, and address the need for persistence in the communication process.

---

insurance information have all become Web-based to better respond to employee needs and to reduce the cost of delivering information. Employees also can access financial data such as 401Ks, stock portfolios, options accounts, and securities information online. In most of these applications, employees connect to a secure server farm, via a local intranet or the World Wide Web, and then access or download information specific to their accounts.

## The basics of SSL

The Internet communications protocols IP and TCP, in particular, make the Internet possible by facilitating the cooperation of a large number of computers. Because the original design of the Internet did not include security, third parties can easily observe or modify communication over Internet protocols such as TCP. This security problem motivates the need for a protocol that meets the following criteria:

- ▶ **Authentication.** Each communicating partner should be able to verify that the other is who it claims to be and not an impostor.
- ▶ **Privacy.** A third party should not be able to eavesdrop on a private communication.
- ▶ **Integrity.** The protocol should automatically or easily detect any tampering with the transmission.
- ▶ **Non-repudiation.** A sender should not be able to claim that it did not send what the receiver got.

SSL meets these criteria. Developed by Netscape, SSL initially had numerous security problems, but these issues were corrected with the release of SSL Version 3 (SSLv3). SSLv3 is now the most popular and widely used Internet security protocol for the World Wide Web. Although the Internet Engineering Task Force (IETF) released Transport Layer Security (TLS) in January 1999, it has yet to become as popular as SSLv3.

## Mechanics of SSL

SSL is a public key cryptography system. The keys are numbers that always occur in pairs: a public key well known by outside parties and a private key known only by the key owner. Either key can be used to encrypt information, which the other key then decrypts. When a sender uses the recipient's public key to encrypt a transmission, only the receiver can decrypt it; this process ensures privacy. When a sender uses its private key to encrypt a transmission, the recipient uses the sender's public key to decrypt the message. Only

Software-based SSL is more suitable for servers that manage low volumes of SSL traffic such as departmental, workgroup, or non-e-commerce commercial Web servers.

the sender's public key will result in a meaningful message; this process ensures authenticity.

An SSL session begins with a key exchange called the SSL handshake. In this exchange, the client and server authenticate each other using their respective key pairs and then establish a secure channel of communication. Although this secure channel could be used for the entire duration of the communication, it is not because the calculations involved are extremely processor-intensive.

Instead, one party generates a temporary session key to share secretly with the other party over the secure link, which is then terminated. The rest of the transmission is encrypted using the secret, temporary session key. Although encrypting with a session key is less CPU intensive than using a public key pair, it can still degrade server performance if a large amount of data is transferred.

## Authentication of communicators using digital certificates

In the initial key exchange, the server and client authenticate one another by presenting a digital certificate that has been signed by a mutually trusted party known as a certificate authority (CA). Digital certificates prevent impostors from using their own public key pair while claiming someone else's name. The CA signs the server's public key and binds the key and identity together. Each Web server using SSL needs a separate digital certificate, which must be purchased from a public CA such as VeriSign, CyberTrust, or Thawte.

## Various approaches to SSL

Web servers can process SSL transactions with the help of software, accelerator adapters, or acceleration appliances. The following sections will examine each type of SSL implementation—how it works and its best environment.

## Software-based SSL implementation

In a software-based SSL implementation, the server processor handles the initial key exchange as well as the subsequent bulk encryption in a single session (see Figure 1). These intense computational processes tax server performance and can reduce capacity by tens to hundreds of transactions per second.

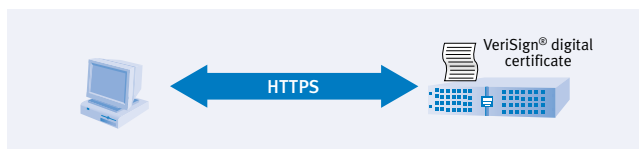


Figure 1. Traffic flow between server and client in a software-based SSL configuration

Because of this effect on Web server performance, software-based SSL is more suitable for servers that manage low volumes of SSL traffic such as departmental, workgroup, or non-e-commerce commercial Web servers.

Web server administrators can maximize server performance in software-based SSL implementations by limiting the number of SSL sessions or by adding servers. Multiple Web servers, however, can hinder persistence—the ability to keep a client connected to the same server throughout the SSL session. Furthermore, requiring a Web server to perform SSL computation reduces its capacity to perform its primary function of serving Web content.

### Server-based SSL accelerator adapters

Installing an SSL accelerator adapter, such as the Broadcom® CryptoNetX™, on a server alleviates the workload of the primary processors, freeing those processors to serve Web pages or to run applications (see Figure 2). Each accelerator card can handle hundreds of transactions per second (TPS), and most commercially available Web servers support off-loading SSL encryption and decryption to these adapters.

On average, most Web servers can manage between 2,000 and 3,000 unencrypted transactions per second. Without an accelerator card, a few hundred SSL transactions per second can stress even a dual-processor Web server, reducing the amount of overall traffic it can serve. By introducing multiple SSL accelerator cards, the number of encrypted SSL transactions can be easily increased to about 1200 TPS of encrypted traffic while maintaining the overall request range capable for the server. Improvements in accelerator technology are expected to further increase this rate in the near future.

Multiple servers are needed if requests exceed the 2,000 to 3,000 TPS threshold. When running multiple Web servers for a single site, administrators must load balance the servers to achieve scalability and fault tolerance.

One limiting consequence of using SSL accelerator adapters in a load-balancing implementation is that session persistence is not guaranteed. Normally, when a Web server farm or cluster of Web applications run behind a Layer 4 switch, the load balancer examines the request headers for cookies so that it can route the request to the server that issued the cookie. When the server handles the SSL processing, the load balancer cannot see the cookies and the request may be sent to the wrong server, breaking the session persistence.

Until recently, this problem was overcome by basing persistence on SSL session IDs. But new security features in recent releases of Microsoft® Internet Explorer cause the browser to renegotiate

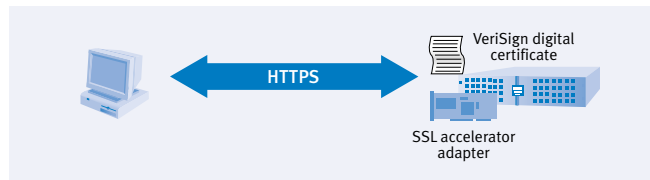


Figure 2. Traffic flow between server and client in an SSL accelerator adapter configuration

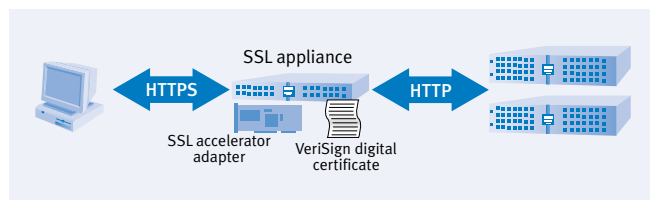


Figure 3. Traffic flow between servers and client in an SSL acceleration appliance configuration

the SSL ID and encryption keys with the back-end server, thus breaking persistence.

A final challenge that administrators face with this type of SSL environment is certificate management. Every server in the cluster must have a unique digital certificate. Initial purchase, deployment, and maintenance of these multiple certificates can increase the total cost of ownership (TCO) of the SSL implementation.

### SSL acceleration appliances

An SSL appliance is a separate, stand-alone device with an embedded SSL accelerator card that decrypts encrypted traffic and sends the unencrypted message to the back-end servers. On the return path, the appliance encrypts the message sent by the back-end server and forwards it to the client (see Figure 3).

The back-end server is now free to serve data or run applications. It does not need to keep track of any SSL connections, which dramatically increases its performance. Scalability is another advantage of the SSL appliance. Administrators can group multiple appliances together to offer a larger number of SSL transactions that might not be possible by any other means.

To be truly effective in an application or Web server environment, an SSL appliance must run in conjunction with a load balancer that balances multiple back-end servers. But deploying a separate load balancer and SSL acceleration appliance can drive up TCO and may prevent the load balancer from supporting session persistence.

SSL acceleration appliances are most commonly implemented in a small site where a single back-end server with an SSL appliance is

Installing an SSL accelerator adapter on a server alleviates the workload of the primary processors.

sufficient. An environment that requires a large number of connections may use multiple SSL appliances to handle thousands of new SSL connections per second.

### Load balancer with SSL acceleration: PowerApp.BIG-IP

Developed in conjunction with F5 Networks, the Dell® PowerApp.BIG-IP is a traffic management appliance that supports SSL off-loading to an optional SSL accelerator card. PowerApp.BIG-IP provides not only IP-layer load balancing, but also application-layer load balancing. It can examine the HTTP header and make a load-balancing decision based on rules written by the administrator to achieve the highest level of SSL load balancing.

#### Load-balancing capabilities of PowerApp.BIG-IP

To provide more flexibility to environments that require simple IP or Layer 4 load balancing, PowerApp.BIG-IP can perform the following types of load balancing:

- ▶▶ **Round robin.** Servers receive connections in turn
- ▶▶ **Ratio.** Servers receive traffic based on a user-defined ratio
- ▶▶ **Dynamic ratio.** Servers receive traffic according to ratios determined by server statistics that PowerApp.BIG-IP gathers
- ▶▶ **Priority.** Back-end servers belong to different priority groups; when the number of highest priority servers drops below a user-defined number, the next priority level servers start receiving traffic
- ▶▶ **Least connections.** Servers with the least connections receive traffic
- ▶▶ **Fastest.** Servers with the fastest response time receive the most traffic
- ▶▶ **Observed.** Servers are ranked by the connections they can handle and their response times; the highest ranking ones receive the most traffic
- ▶▶ **Predictive.** Similar to observed load balancing, but improving servers get more traffic

In addition to IP load balancing, PowerApp.BIG-IP can intelligently monitor back-end servers so that failed servers will be taken from the load-balanced array and users will not experience service interruption.

PowerApp.BIG-IP also can perform Extended Content Verification (ECV) on the back-end servers by periodically fetching and checking the content of a static page on a Web server. This monitoring method not only removes failed servers, it also

---

Administrators can group multiple SSL appliances together to offer a larger number of SSL transactions that might not be possible by any other means.

---

removes servers with content that has been changed by hackers.

Extended Application Verification (EAV), another feature of the PowerApp.BIG-IP, goes a step beyond ECV by checking the dynamic content returned by the server. For example, scripts executed to check an e-commerce shopping cart can verify the back-end server application response and the database call. If a node returns a wrong result, PowerApp.BIG-IP removes it from service so that end users do not see it.

To prevent a PowerApp.BIG-IP from being the single point of failure in a network, administrators should configure two PowerApp.BIG-IP appliances in a redundant pair. If the active system fails, the redundant system takes over in milliseconds with a serial-based failover between the units. Since mirroring occurs at the session state between the active and redundant pairs, transition appears seamless and uninterrupted to the end users.

#### SSL capabilities of PowerApp.BIG-IP

For a site that requires users to return to the same server at a later visit, PowerApp.BIG-IP offers many methods of persistence (even to transparent devices) based on the source IP addresses, HTTP cookies, or SSL session IDs for an encrypted site.

PowerApp.BIG-IP supports off-loading SSL termination to an SSL accelerator adapter—ideal for a network architecture that requires SSL termination in conjunction with load balancing. It also handles the decryption of incoming traffic from clients and can load balance the decrypted traffic to the back-end servers. The system then encrypts the traffic again when it is sent to the client. Figure 4 illustrates the traffic flow of this SSL configuration.

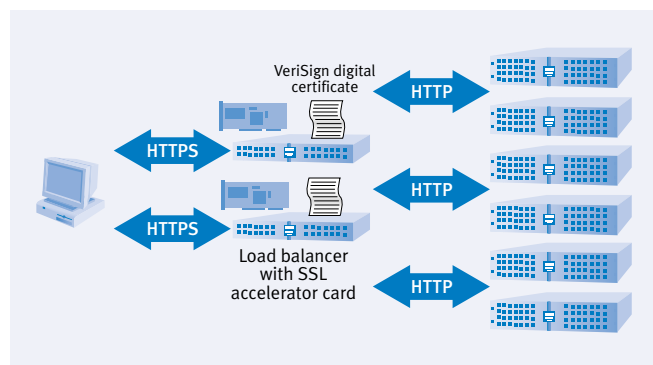


Figure 4. Traffic flow between servers and client in a PowerApp.BIG-IP SSL configuration

### Advantages of PowerApp.BIG-IP in SSL configuration

An SSL configuration using PowerApp.BIG-IP offers many advantages over configurations using software-based SSL, server-based SSL accelerator adapters, or other SSL acceleration appliances:

**Reduced TCO.** PowerApp.BIG-IP with SSL termination reduces TCO because each back-end server does not require a separate SSL card or a certificate. It requires only one certificate and one SSL accelerator card per PowerApp.BIG-IP.

**Increased server capacity.** Since the back-end servers do not need to process any encrypted data, they more effectively serve data or run applications, further reducing TCO.

**Centralized certificate management.** The overall management of certificates (deployment and updating) becomes much easier when only the PowerApp.BIG-IP has a certificate.


**Intelligent load balancing for encrypted Layer 7 traffic.** The SSL accelerator unlocks a powerful set of features in PowerApp.BIG-IP for SSL persistence management and intelligent Layer 7 load balancing of encrypted data. Since the PowerApp.BIG-IP has access to the decrypted data, the system can load balance based on either cookies or actual HTTP data.

**Internet Explorer browser security features.** As a security feature, Internet Explorer renegotiates the SSL session after a very short time-out. If the load balancer tries to determine server affinity using SSL session IDs, even short-lived applications can be mis-directed to the wrong back-end server. PowerApp.BIG-IP avoids this problem by supporting persistence based on other criteria such as IP addresses and cookies.

**End-to-end encryption.** Some critical applications require end-to-end encryption. PowerApp.BIG-IP can re-encrypt the traffic to the back-end servers and reduce the possibility of data loss. The intelligent SSL persistence features of PowerApp.BIG-IP are still available in this scenario.

Running in a redundant pair configuration, PowerApp.BIG-IP offers a highly available and a fault-tolerant solution. Large corporations and e-commerce sites can use PowerApp.BIG-IP to run critical Web-enabled applications or to leverage the persistence of Web sites and enhance SSL off-loading capabilities.

### Benefits of SSL acceleration

Depending on their organizations' SSL requirements, network and server administrators can use SSL accelerator adapters, stand-alone appliances, or load balancers with SSL acceleration adapters to move computationally intensive SSL processing off the Web servers. As a result, an organization can lower costs, increase server capacity and performance, and decrease certificate management while addressing persistence. 

**Chad W. Engelgau** (*chad\_engelgau@dell.com*) is an engineering manager in the Application/Software Development Group of the Dell Enterprise Systems Group. He leads the IP traffic management solutions team. Chad received his degree from Texas A&M University.

**Sanjeet Singh** (*sanjeet\_singh@dell.com*) is a software engineer advisor in the Application/Software Development Group of the Dell Enterprise Systems Group. He is currently working on solutions development with the PowerApp.BIG-IP. Sanjeet has a B.S. in Electrical Engineering and an M.S. in Computer Engineering from Purdue University.

### FOR MORE INFORMATION

McCulley, Gary. "Understanding SSL Accelerator Adapters in PowerEdge Servers." *Dell Power Solutions*, Issue 4, 2001