Understanding SSL

Regardless of where you access the Internet from, the connection between your Web browser and any other point can be routed through dozens of independent systems. Through snooping, spoofing, and other forms of Internet eavesdropping, unauthorized people can steal credit card numbers, PIN numbers, personal data, and other confidential information.

![Figure 1 – Non-Secure Transmission Request vs. Secure SSL Transmission Request](image)

The Secure Sockets Layer (SSL) protocol was developed to transfer information privately and securely across the Internet. SSL is layered beneath application protocols such as HTTP, SMTP, and FTP and above the connection protocol TCP/IP. It is used by the HTTPS access method. Figure 1 illustrates the difference between a non-secure HTTP request and a secure SSL request.

Transport Layer Security (TLS) is the successor of Secure Sockets Layer (SSL); they are both cryptographic protocols that provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging, and other data transfers. There are slight differences between SSL and TLS, but the protocol remains substantially the same.

Who Uses SSL?

SSL is the de facto standard for encrypted and authenticated communications between clients and servers on the Internet. Virtually all online purchases and browser-based monetary transactions that occur on the Internet are secured by SSL. However, SSL is not just limited to securing e-commerce transactions; the following are a few other examples of SSL use:

- Financial institutions implement SSL to secure the transmission of PIN numbers and other confidential account information.
- Insurance companies implement SSL to secure transmission of confidential policy information.
- Organizations who have established Business-to-Business (B2B) extranets implement SSL to secure transactions between the company and its partners, suppliers, and customers.
- Private organizations implement SSL in their intranets to confidentially transfer information to and from employees.
- Email providers implement SSL to secure webmail for users.
How It Works

When a client and server communicate, SSL ensures that the connection is private and secure by providing authentication, encryption, and integrity checks. Authentication confirms that the server, and optionally the client, is who they say they are. Encryption through a key-exchange then creates a secure “tunnel” between the two that prevents any unauthorized system from reading the data. Integrity checks guarantee that any unauthorized system cannot modify the encrypted stream without being detected.

SSL-enabled clients (such as a Mozilla™ or Microsoft Internet Explorer™ web browser) and SSL-enabled servers (such as Apache or Microsoft IIS™) confirm each other’s identities using digital certificates. Digital certificates are issued by trusted third parties called Certificate Authorities (CAs) and provide information about an individual’s claimed identity, as well as their public key. Public keys are a component of public-key cryptographic systems. The sender of a message uses a public key to encrypt data. The recipient of the message can only decrypt the data with the corresponding private key. Public keys are known to everybody; private keys are secret and only known to the owner of the certificate. By validating the CA digital signature on the certificates, both parties can ensure that an imposter has not intercepted the transmission and provided a false public key for which they have the correct private key. SSL uses both public-key and symmetric key encryption. Symmetric key encryption is much faster than public-key encryption, but public-key encryption provides better authentication techniques. So SSL uses public key cryptography for authentication and for exchanging the symmetric keys that are used later for bulk data encryption.

The secure tunnel that SSL creates is an encrypted connection that ensures that all information sent between an SSL-enabled client and an SSL-enabled server remains private. SSL also provides a mechanism for detecting if someone has altered the data in transit. This is done with the help of message integrity checks. These message integrity checks ensure that the connection is reliable. If, at any point during a transmission, SSL detects that a connection is not secure, it terminates the connection and the client and server establish a new secure connection.

SSL Transactions

The SSL transaction has two phases: the SSL Handshake (the key exchange) and the SSL data transfer. These phases work together to secure an SSL transaction.

![Figure 2 - SSL Transaction](image-url)
Figure 2 illustrates an SSL transaction:

1. The handshake begins when a client connects to an SSL-enabled server, requests a secure connection, and presents a list of supported ciphers and versions.

2. From this list, the server picks the strongest cipher and hash function that it also supports and notifies the client of the decision. Additionally, the server sends back its identification in the form of a digital certificate. The certificate usually contains the server name, the trusted certificate authority (CA), and the server’s public encryption key. The server may require client authentication via a signed certificate as well (required for some on-line banking operations); however, many organizations choose not to widely deploy client-side certificates due to the overhead involved in managing a public key infrastructure (PKI).

3. The client verifies that the certificate is valid and that a Certificate Authority (CA) listed in the client’s list of trusted CAs issued it. These CA certificates are typically locally configured.

4. If it determines that the certificate is valid, the client generates a master secret, encrypts it with the server’s public key, and sends the result to the server. When the server receives the master secret, it decrypts it with its private key. Only the server can decrypt it using its private key.

5. The client and server then convert the master secret to a set of symmetric keys called a keyring or the session keys. These symmetric keys are common keys that the server and browser can use to encrypt and decrypt data. This is the one fact that makes the keys hidden from third parties, since only the server and the client have access to the private keys.

6. This concludes the handshake and begins the secured connection allowing the bulk data transfer, which is encrypted and decrypted with the keys until the connection closes. If any one of the above steps fails, the SSL handshake fails, and the connection is not created.

Though the authentication and encryption process may seem rather involved, it happens in less than a second. Generally, the user does not even know it is taking place. However, the user is able to tell when the secure tunnel has been established since most SSL-enabled web browsers display a small closed lock at the bottom (or top) of their screen when the connection is secure. Users can also identify secure web sites by looking at the web site address; a secure web site’s address begins with https rather than the usual http.

SSL Crypto Algorithms

SSL supports a variety of different cryptographic algorithms, or ciphers, that it uses for authentication, transmission of certificates, and establishing session keys. SSL-enabled devices can be configured to support different sets of ciphers, called cipher suites. If an SSL-enabled client and an SSL-enabled server support multiple cipher suites, the client and server negotiate which cipher suites they use to provide the strongest possible security supported by both parties.

A cipher suite specifies and controls the various cryptographic algorithms used during the SSL handshake and the data transfer phases. Specifically, a cipher suite provides the following:

- **Key exchange algorithm:** The asymmetric key algorithm used to exchange the symmetric key. RSA and Diffie Hellman are common examples.

- **Public key algorithm:** The asymmetric key algorithm used for authentication. This decides the type of certificates used. RSA and DSA are common examples.

- **Bulk encryption algorithm:** The symmetric algorithm used for encrypting data. RC4, AES, and Triple-DES are common examples.

- **Message digest algorithm:** The algorithm used to perform integrity checks. MD5 and SHA-1 are common examples.
For instance the cipher suite "RSA-RC4-MD5" means that RSA certificates are used for both authentication and key exchange, while RC4 is used as the bulk encryption cipher, and MD5 is used for digest computation.

SSL and the OSI Model
The SSL protocol is a security protocol that sits on top of TCP at the transport layer. In the OSI model, application layer protocols such as HTTP or IMAP, handle user application tasks such as displaying web pages or running email servers. Session layer protocols establish and maintain communications channels. Transport layer protocols such as TCP and UDP, handle the flow of data between two hosts. Network layer protocols such as IP and ICMP provide hop-by-hop handling of data packets across the network.

SSL operates independently and transparently of other protocols so it works with any application layer and any transport layer protocol. This allows clients and servers to establish secure SSL connections without requiring knowledge of the other party’s code.

Figure 3 illustrates how SSL functions in the OSI model:
An application layer protocol hands unencrypted data to the session/transport layer, SSL encrypts the data and hands it down through the layers. When the server receives the data at the other end, it passes it up through the layers to the session layer where SSL decrypts it and hands it off to the application layer. Since the client and the server have gone through the key negotiation handshake, the symmetric key used by SSL is the same at both ends.

The Cost of Encryption
While SSL solves the problem of securely transferring private data, it introduces another problem: HTTPS traffic poses a major security risk to enterprises.
As illustrated in Figure 4, because SSL (Secure Sockets Layer) content is encrypted, it can’t be intercepted by normal means. Users can bring in various malware including viruses, access forbidden sites, and leak confidential business information over an HTTPS connection, which uses port 443. Because IT organizations have no visibility into SSL sessions, they are blind to any potential security threats sent over HTTPS. In addition to the security threat, encrypted traffic makes it difficult for IT to assess bandwidth usage and apply intelligent content control policies to ensure maximum user productivity.

Additionally, key signing and certificate verification is extremely CPU-intensive. Many security-sensitive websites that have implemented SSL experience bottlenecks created by the managing and processing of SSL sessions. The end result is that SSL degrades web server performance considerably and web transactions are slowed to a crawl. Because of the performance degradation caused by SSL, many organizations cannot, because of budgetary or infrastructure limitations, implement SSL. Or they implement it in a very limited capacity by applying SSL only to sensitive data or transactions.

The Blue Coat Systems SSL Traffic Solutions

The Blue Coat ProxySG solves a number of SSL related issues. Depending on your needs, you can use the ProxySG as an SSL forward proxy for securing outbound traffic, an SSL proxy for wide area network (WAN) optimization, or an HTTPS reverse proxy for web server acceleration.

Blue Coat appliances use patented technology to detect, inspect, optimize, and accelerate all web traffic and SSL/TLS based applications. Unlike other solutions, administrators have the flexibility to choose the optimization and acceleration techniques for their enterprise depending on their security policies. Blue Coat appliances use patented software techniques and hardware acceleration to optimize encryption algorithms and reduce SSL/TLS handshakes over the WAN. This significantly improves user experience, improves overall productivity, and increases performance of servers in the data center. In addition, administrators can reduce latency and improve bandwidth by securely reducing and limiting redundant patterns of traffic, anywhere from the byte/packet level up to the application level, or even both when configured. Security policies and acceleration and optimization techniques can be granularly applied (or not applied) based on users or departments, source or destination, application or content, or all of the above. Figure 5 shows Blue Coat SSL Proxy-Based Solutions.
An SSL “forward” proxy sits between users on a corporate LAN and their access to the Internet/Web, protecting the client. It is used for applying security and performance features such as authentication, malware prevention, URL filtering, data loss prevention, and caching. The ProxySG can be used as an SSL forward proxy to tunnel or intercept HTTPS traffic. Deployed in this way, it usually sits at the Internet “gateway”, or where the organization’s network meets their Internet feed(s).

The Blue Coat ProxySG can also be used for WAN optimization to accelerate “inside-out” (users inside the organization accessing external/outside sites) SSL traffic from internal websites as well as external websites when used in an application delivery network (ADN) deployment across a WAN link, while providing complete visibility for security policies. Deployed in this way, a branch/remote office ProxySG intercepts and securely communicates with an upstream ProxySG deployed as a WAN optimization concentrator/gateway.

An HTTPS “reverse” proxy sits on the edge of a corporate network and accepts requests from users on the WWW coming into a corporate website. It is typically used to offload SSL processing from the server to the proxy, cache server content, and optionally provide threat detection, and data loss prevention checks. In a content delivery network (CDN) it can also be used for bandwidth management and server acceleration deployed in the middle of the network – away from the server but not necessarily at the branch or network edge. Communications between the HTTPS reverse proxy and the server might or might not use SSL.

To help alleviate the threat that encrypted HTTPS traffic can pose and the strain SSL places on general-purpose web servers, Blue Coat ProxySGs have integrated full SSL capabilities. When a client sets up a new SSL session through ProxySG to a server, the SSL proxy performs validation checks on the server’s certificate. Once validated, this SSL session can be reused multiple times by that same client and server for some period of time. During this time, the proxy continues to perform checks on the certificate present in the cached server-side SSL session. Every time a new connection is made, the ProxySG continues to check dates on the certificate to see if it has expired. No SSL data is stored nor are SSL keys at risk. Administrators can invoke the object cache for SSL traffic, if the acceleration benefits and security profile makes sense; the object caches have almost zero administration time since they self-tune as traffic passes.
Blue Coat ProxySGs are the industry’s only solutions designed specifically for securing, accelerating and scaling SSL traffic to internal as well as external sites over your LAN and WAN. Three solutions are discussed:

- **Secured and Accelerated Outbound SSL Traffic – Forward Proxy**
- **WAN Optimization – MACH5 SSL Proxy**
- **Web Server Acceleration – HTTPS Reverse Proxy**

**Secured and Accelerated Outbound SSL Traffic – Forward Proxy**

Many organizations today have a need to protect their users and their corporate assets. An SSL forward proxy can help an organization protect their end-users from downloading and installing threats from the Internet, as well as help protect corporate assets by preventing confidential and proprietary information from making its way to the Internet [data loss prevention]. Figure 6, below, illustrates the Blue Coat ProxySG SSL forward proxy solution.

The SSL proxy can intercept HTTPS traffic allowing organizations to apply various security policies to prevent malware infection and still allow access to secured, external SSL sites. The SSL Forward proxy can do the following operations while tunneling HTTPS traffic:

- Validate server certificates, including CA checking and revocation checks using Certificate Revocation Lists (CRLs).
- Check and optionally enforce various SSL parameters such as cipher and version.
- Log useful information about the HTTPS connection.
- URL filter based on the server certificate hostname.

*Figure 6 – Blue Coat ProxySG Forward SSL Solution*
When the SSL forward proxy is used to intercept HTTPS traffic, it can also:

- Optionally cache HTTPS content.
- Apply HTTP-based authentication mechanisms.
- Initiate ICAP actions for DLP (data loss prevention) checks or malware detection, never exposing data to a live network. (Secure-ICAP is recommended for content analysis between locations).
- URL filter based on the full URL and even obscured URLs, plus deep content inspection for translation services, image and cached search engine content searches, and proxy avoidance.
- Apply granular policies such as validating apparent data type, magic byte, container mismatch, mime type, or filename extension.

Blue Coat ProxySG’s SSL forward proxy intercept functionality terminates SSL traffic. It can exert policy control at the initiation of the SSL session (i.e., on client connect, and on server response) and throughout the session – because there are two separate connections: one between the client and the proxy, and another between the proxy and the server – see Figure 7, below. This enables all of the proxy controls, but also some SSL-specific controls.

First, Blue Coat ProxySG can make gateway trust decisions – meaning that organizations can decide whether or not they accept secure connections from servers with a questionable certificate (i.e., the certificate is out of date, or issued by an untrusted party, or doesn’t match the server name), instead of trusting their users to make that determination. This has tremendous anti-phishing benefits – most of the servers used in phishing and pharming attacks depend on users blithely clicking “yes” to certificate warnings. Also proxy avoidance toolkits can be blocked by requiring valid server certificates.

Second, the ProxySG’s SSL forward proxy can apply full proxy functionality to HTTPS traffic and manage traffic tunneling through SSL (typically rogue applications like Skype, peer-to-peer, or IM) differently – deciding whether or not to pass that traffic – which has significant benefits for security groups trying to manage vulnerability-prone consumer applications.
Perhaps surprisingly, remote application performance actually improves as a result of the acceleration techniques of compression, caching, and HTTP optimizations integrated with the SSL interception techniques, if activated (by default caching is not enabled for SSL traffic inspection). Correctly sized, Blue Coat ProxySG handles any size network, and accelerates overall session performance.

**Preventing Encrypted Malware Example**

As part of forward proxy, the ProxySG with ProxyAV can prevent malware in encrypted sessions. Before the existence of an SSL forward proxy, HTTPS sessions could transfer malicious content directly to a user’s desktop with no visibility available to the network or systems administrator.

Figure 8 shows ProxySG + ProxyAV in forward proxy mode. The ProxySG can terminate the session containing encrypted data coming into the enterprise. At that point, data can be converted to "cleartext" and automatically inspected by the ProxySG to determine compliance with corporate policy. Decisions on how to handle the data can be based on ProxySG’s advanced session control policies that enable IT to set granular policies on which SSL sessions are intercepted, allowing organizations to adhere to corporate or governmental rules on data privacy. ProxyAV can use a variety of proactive detection engines, including Sophos, Panda, McAfee, and Kaspersky, to stop malware, spyware, and viruses. Any potentially malicious traffic is automatically thwarted at that point, preventing any security breaches in the enterprise. Valid traffic is safely passed on to the Web browser to complete the session.

ProxySG + ProxyAV in forward proxy mode enable organizations to protect the enterprise and its users by allowing IT to:

- Gain visibility and control over SSL-encrypted traffic.
- Control or stop rogue applications (e.g., IM, P2P) that use SSL (and universally open Port 443) to subvert enterprise controls and security measures.
- Analyze SSL-encrypted traffic for malware, viruses, worms, and Trojans, and stop them at the gateway.
- Halt secured phishing and pharming attacks that use SSL to hide from IT controls or to increase the appearance of authenticity.
- Scan all web traffic (in the clear and encrypted) for threats, using best-of-breed proactive detection and scanning engines.
- Control downloads, installers, and attachments with allow or deny blended policies based on reputation, source, destination, users, group, time of day, or service.
**Securing Outsourced Applications Example**

More and more critical services are being provided by partners, often over the Internet and secured by SSL. Be it order entry, fulfillment, human resources, or sales management, organizations are dependant on fast and reliable access to these outsourced applications. Until recently, however, that critical traffic was opaque to IT management because it was tunneled through SSL. The SSL forward proxy allows the organization to make sure no malware gets through from even trusted sources, like outsourced sites, and provides an audit/tracking mechanism for these outsourced applications.

The ProxySG can be used to secure communications with known outsourced applications, such as Salesforce.com, or services such as hosted email providers. The flexibility of the SSL forward proxy functionality allows you to control – or not control – based on a variety of criteria (e.g., user, application, source, etc.), so you can:

- Pass-through SSL traffic untouched,
- Make some initial judgments about where the traffic is coming from and going to, then pass it through, Or
- Fully proxy control of the SSL connection.

These three options are represented in the three diagrams in Figure 9.

![Figure 9](image.png)

*Figure 9 – Blue Coat enables IT organizations to apply varying levels of SSL proxy management, from simply passing through traffic to full proxy enabling policy-based SSL control.*

In the latter two of the above scenarios, organizations can also warn end-users what is going on; for example, a splash page that lets users know that some monitoring is going on, and reminds them of the acceptable use policy. This flexibility extends to caching, logging, and administrative functions as well. Using the Blue Coat ProxySG SSL forward proxy capabilities, organizations can be selective about what they cache – perhaps only caching certain elements that do not contain sensitive data (for example, GIFs and JPEGs). Similarly, logging can be equally selective, and organizations can send the encrypted...
and signed logs off to a secure server to ensure audit-ability. Without these robust policy features, combined with automatic website categorization with URL and content filtering, organizations would struggle to comply with both their internal privacy policy and the myriad regulations globally for handling sensitive information.

Balancing User Performance and User Privacy

Using an SSL proxy to manage encrypted traffic can remove a significant network blind spot. Yet by inspecting the traffic, the explicit trust model of SSL comes into question; SSL is, after all, deployed to ensure that the traffic is private during transit. Certain situations require more care and consideration. For example, employees may be allowed to connect to secure web brokerages to manage their corporate compensation plans, or to health insurance sites to schedule confidential doctors visits. Partners and other invited guests connecting back to their own offices may access confidential materials under the expectation of secrecy. Depending on your jurisdiction, respecting the privacy of such communication may be more than a policy – it may be the law. Therefore, when deploying an SSL proxy organizations have three options with respect to balancing optimization needs and privacy requirements:

- **Do not decrypt and proxy SSL-tunneled traffic.** This is a short term solution that bypasses any regulatory or perception issues associated with intercepting SSL connections. Generally, however, this is only an option when SSL traffic is minimal or can be otherwise restricted, optimization of other protocols frees up sufficient bandwidth on the WAN, and latency of existing SSL applications is not a concern. This solution offers no protection.

- **Proxy selected SSL connections, respecting user confidentiality where appropriate.** The choice to intercept could be based either on a white list of known business applications that require acceleration, or an exclude list of known private sites that users are allowed to browse without the proxy opening their communication. For highly regulated organizations that need to testify to the flow of information for compliance purposes, this type of partial proxy deployment allows them the flexibility to inspect and audit traffic selectively.

- **Open, inspect and accelerate all SSL traffic.** Clearly, this would allow the proxy maximum control over bandwidth and unauthorized communication. Implicitly, it also facilitates and encourages additional use of SSL by removing network performance considerations, aiding compliance objectives. Though ideal from an application performance and bandwidth management perspective, any full SSL proxy must be able to notify users and log their consent to a use policy. That requires the use of a pop-up or splash screen to collect the consent, inline authentication to know who is consenting, logging functions to aggregate it, and a reporting mechanism to produce audit-proof documentation.

WAN Optimization – MACH 5 SSL Proxy

In the WAN optimization scenario Blue Coat ProxySG offers many of the same benefits to the organization as the SSL forward proxy example. Blue Coat ProxySG appliances with MACH 5 technology can seamlessly open all SSL applications, regardless of whether they are internal or external. This allows you to deliver the same performance and great user experience you can provide through WAN optimization to your most important traffic as well. All five MACH5 technologies (bandwidth management, object caching, byte caching, protocol optimization, and compression) can be used with SSL applications, without the need to break security best-practices by removing private keys from your servers. Just as importantly, Blue Coat user management tools, including alerts and coaching pages, user authentication, and centralized reporting, allow you not only to be selective in the SSL you intercept, but also to produce auditable logs of user consent. Figure 10 illustrates the Blue Coat ProxySG SSL WAN Optimization solution.
Blue Coat ProxySG appliances at the branch provide performance relief for backhauled Internet applications, even if they are SSL-encrypted. With caching, compression, and protocol optimizations, Blue Coat MACH5 technology dramatically reduces user wait times caused by long round trips to and from the organization’s web gateway while cutting bandwidth use by 80% or more. Using bandwidth management, the organization can prioritize their SSL outbound traffic to optimize certain critical sites and guarantee a minimum quality of service. Reducing rogue applications alone can result in significant bandwidth gains, but more granular controls allow for sophisticated management techniques – for example changing application priorities at month’s end, or making room for backups on crowded multi-protocol label switching (MPLS) links at night.

Putting ProxySG appliances at branch offices has additional benefits; by the time outsourced application data reaches the secured Internet gateway, it is already optimized and compressed to minimize network load on that pipe as well. Adding ProxySG appliances to the branch with ProxySG appliances at the gateway enables IT to have complete, policy-based control over application delivery and security – even over applications and networks they don’t own.

By selectively opening SSL tunnels, the user’s expectation of privacy can be maintained while known-good or known-bad applications can be silently accelerated or dropped, respectively. All without requiring that server certificates leave the safety of the datacenter or sending insecure session requests to downstream appliances. The flexibility of Blue Coat’s WAN optimization technology allows for unmatched sophistication in meeting quality of service mandates for internal applications. Natively supporting not only HTTPS but also CIFS, MAPI and most streaming media, the ProxySG is well equipped for the protocols that clog intra-company WANs.

Combining SSL session awareness, including facts about the source certificate such as who signed it, when it expires, and the organization that issued it, with AAA (authentication, authorization, accounting) and PKI (public key infrastructure) integration uniquely allows the Blue Coat solution to fully accelerate and control SSL traffic without breaking the SSL trust model.
Securing and Optimizing WAN Traffic Example

A Blue Coat ProxySG used for SSL WAN optimization acts as the SSL proxy allowing branch office workers secure access that can be inspected and optimized to internal web servers and external websites as well, providing the same benefits discussed in the SSL forward proxy example. See Figure 11, below.

The ProxySG can hold both client and server keys for its internal clients. This allows SSL sessions to be carried out twice: once between the client and proxy server, and again between the proxy server and the secure server. In that way, the ProxySG can to listen in on the conversation without having the private keys of external servers.

The ProxySG can be used as described above, or simply to create a secure tunnel between sites across an insecure network. SSL doesn’t allow recursive encryption, so by using it this way you lose the transparency of the proxy and get multiple segments of secure connections, rather than a single secure end-to-end connection. The ProxySG has full SSL support as opposed to just SSL tunneling. It can therefore do client authentication and serve documents like a secure server, or request documents like an SSL-enabled client.

Figure 11 – Example WAN Optimization Deployment
When used in WAN optimization, the ProxySG is used similarly to a regular proxy, and works as follows:

1. The client makes a request for a service, which is intercepted on the network by the branch proxy.
2. If the request is allowed according to the proxy's policy, the proxy re-issues the request to the source server on the user's behalf.
3. Once the decision to encrypt is made and the SSL handshake begins, the proxy completes the handshake on the client side and the server side. There are then two separate tunnels, one on each end of the branch proxy, with the branch proxy in the middle bridging the connection. Ideally, this is transparent to both parties.
4. Additionally, the connection between the branch proxy and the server goes through another proxy (the concentrator proxy). The branch proxy and concentrator proxy co-operate to apply WAN optimization techniques to the SSL traffic for improving performance and response time. The connection between the branch and concentrator proxies is secure.

Since a full HTTPS Proxy runs at the branch, the object cache is co-located with the branch user; many other vendors deploy a cache located far from the user – in the data center – which means each user's request is forced to traverse the WAN link, contributing to network congestion.

**Web Server Acceleration – HTTPS Reverse Proxy**

Blue Coat Systems has designed the ProxySG series specifically to accelerate and scale high traffic websites. By adding SSL processing, the ProxySG offloads the origin server from the delivery of secure objects and the managing and processing of SSL sessions. As such, they offer several key capabilities not available in single-function SSL devices from other vendors:

- Not only manages and processes SSL sessions, but also caches and rapidly delivers the objects on a secure page without taxing server resources. Single-function devices only offload SSL processing; the web server must still perform object delivery.
- Establishes a secure channel from the appliance to the server for transferring customer-specific data. All other page objects are served directly from the appliance.
- Can be deployed within a content distribution network, removed from the server infrastructure and close to users. The ProxySG can serve content rapidly from the network edge, while passing encrypted data to the primary server farm over a secure SSL session.
- Is configured transparently in the network – not inline – eliminating reliability concerns and additional latencies.
- Optionally, ProxyAV can be deployed for malware detection when content is being uploaded to a web server. Outlook Web Access (OWA) for web-based email is a good example. Utilize ProxySG to reverse proxy the server to improve performance and provide SSL offloading, while using ProxyAV to detect malware in uploaded content.
- Optionally, DLP (data loss prevention) checks can be applied to web application server content being requested outbound to clients, utilizing authentication to assist in content controls per user or group.
Figure 12 illustrates the Blue Coat ProxySG Reverse HTTPS Solution.

Blue Coat ProxySG appliances can triple a website’s throughput and cut user response times by 50-80 percent while increasing the security and control of SSL transactions. This allows a website to serve more content and process more transactions through the existing server infrastructure, as well as keep better track of SSL connections and apply policy to intercepted HTTPS traffic. The ProxySG can negotiate 10-40 times more new SSL connections than a standard web server; supporting up to 7000 new SSL transactions per second, and up to 19,000 maximum existing connections. The ProxySG can process both HTTP (public) content and HTTPS (private) content and support several origin servers from multiple secure sites at one time.

Each origin server may have its own certificate loaded onto the appliance. Blue Coat ProxySGs ship with validation certificates from all major Certificate Authorities (CAs), which validate the origin server certificates. Customers can then add their own certificates for each original domain. Blue Coat appliances support all major CAs for origin server certificates.

Blue Coat ProxySG appliances also offer the ability to establish “back-end” SSL sessions with the origin server to support content distribution via global web server acceleration. In a back-end SSL session, the Blue Coat appliance encrypts the channel back to the origin server. The primary benefit to this is that organizations may deploy the Blue Coat ProxySG away from the origin server, which allows them to deploy secure data in a distributed manner. By establishing back-end SSL sessions, the Blue Coat ProxySG allows content distribution networks (CDNs) to support encrypted traffic. In such deployments back-end session reuse continues to lower the computational cost of SSL on the web server. In addition, by encrypting the channel between the Blue Coat ProxySG appliance and the origin server, an additional layer of security is achieved.
Web Server Acceleration Example

Figure 13 shows a typical configuration in a web server (content provider) application, in this case for www.example.com. Blue Coat ProxySG appliances front-end the example.com web server farm and offload the origin servers from both object delivery and SSL session processing. Object requests (for both HTTP and HTTPS) are directed to the ProxySG appliance through a Layer 4 switch. For cleartext HTTP requests, the appliance immediately delivers the objects stored in cache to the client. The appliance also retrieves objects not in cache from the origin server, caches them for future delivery, and delivers them to the client.

For SSL-encrypted HTTPS requests, the ProxySG appliance performs full SSL processing, from setting up the SSL session to encrypting all the outbound data. The Blue Coat appliance processes all the SSL requests, and the origin server is not burdened with this processing. Requests that the ProxySG does not cache, such as stock quotes, and bank account balances, are sent to the origin server for retrieval. The appliance retrieves this information and, without caching it, encrypts the data and sends it on to the requesting browser. The appliance can also implement policy on any intercepted traffic. Note that the channel between the Blue Coat ProxySG and the origin server can be configured for either SSL or cleartext traffic.
A Content Distribution Network (CDN) is defined as a network infrastructure where the content is stored in geographical locations, rather than in one central spot. When enterprise or content providers distribute their content throughout their global infrastructure, it is considered a dedicated CDN. Figure 14 shows a dedicated CDN for the site www.example.com. In this application, Blue Coat ProxySGs are used to front-end the www.example.com origin servers, and they are also located in geographical locations throughout the Internet, typically in various data centers. As requests come into the example.com web site, a Layer 4-Global Server Load Balancer (GSLB) automatically sends the browser requests to the appropriate Blue Coat secure proxy. For example, it directs requests from Los Angeles to the L.A. ProxySG; it sends requests from Europe to the London ProxySG, etc. The GSLB performs health checks on the proxies to ensure that requests are not sent to overloaded appliances. The primary benefit is end user (customer) response time and availability by getting data closer to them; additional benefits include bandwidth gain, origin server offload, surge protection, replicated content and reduced management requirements.

The SSL tunnel termination capabilities of the Blue Coat ProxySG allow the distributed content to be either cleartext objects, or SSL-encrypted objects. Before the Blue Coat ProxySG, CDNs could not be built to support the distribution of encrypted content.
How Secure is the ProxySG Itself?

The Blue Coat ProxySG has its own, patented, operating system known as SGOS (secure gateway operating system). SGOS is a proprietary, object-oriented operating system. As such, the fully proprietary "object store/cache" does not use a file system common to operating systems like Linux, UNIX, and Windows. Files are written in blocks, often non-contiguously, based on free-space availability. The ProxySG object cache is not an authoritative data store; there is no file editor, directories, or viewer available. In fact, no disk analysis tools exist outside of SGOS itself to reconstruct a full data file from the constituent data blocks. Creation of such a tool would require detailed knowledge of SGOS internal architecture and data structures. Further, when a disk from one ProxySG is inserted into another ProxySG, all reference information for data fragments is immediately overwritten and the files themselves effectively lost. In this way, the data security and privacy risks are minimal.

Secure portions of the ProxySG configuration (private keys, passwords, etc.) are stored with strong encryption so that drive theft will not compromise network security. These same portions of the configuration are intentionally excluded from all debugging and troubleshooting data for similar reasons.

The SGOS byte cache stores patterns that appear in data streams, within and between files. Though data is retained, it is never a full file and there is no retention of the original order of the sequence(s).

SGOS is both NIAP and ICSA certified. NIAP is a product security certification that is required by US government customers and tests the products for security vulnerabilities. ICSA certification is conducted by ICSA Labs. The goal for ICSA Labs certification is to enhance and improve security implementations of network and Internet computing, which improves commercial security and its use of appropriate security products, services, policies, techniques, and procedures. Certification enforces overall confidence in computing and drives enhanced security measures while at the same time decreasing the intrusion of security measures in everyday life. Certification also promotes user acceptance of increased security while improving the ease of use, and the invisible, automatic, and seamless integration of security technology in everyday computing.

Conclusion

SSL has become the universal standard for authenticating web sites to web browsers, and for encrypting communications between web browsers and web servers. However, SSL poses a security threat, is CPU-intensive, and degrades web server performance, so organizations have typically deployed SSL in a limited fashion. Delivering applications over long, skinny WAN pipelines is no easy feat, and the presence of impenetrable SSL tunnels has made it impossible to secure and accelerate a growing part of that traffic.

By integrating SSL processing with its appliances, Blue Coat Systems has eliminated the bottlenecks that served as barriers to widespread implementations of SSL. Companies can now apply SSL to more content without compromising network security or degrading the performance of their web sites. The Blue Coat ProxySG appliances can intercept and validate SSL traffic all while providing SSL processing and high speed caching, allowing the device to serve object requests, so the request does not need to return to the origin server for processing. Through offloading both SSL processing and object request from the origin servers, Blue Coat ProxySG increases throughput and cuts user response times for any secure web site. By tunneling and/or intercepting HTTPS traffic, Blue Coat ProxySG appliances provide the ability to apply policy to otherwise encrypted traffic.
IT can once again gain control over their WAN links, accelerating the good and denying the bad, regardless of SSL encryption. No matter how your users reach their critical applications, Blue Coat ProxySG can help: inbound to your own server farm, outbound to third-party service providers, SSL tunneled or in the clear; ProxySG accelerates and secures your business data. Blue Coat appliances do all of this in a way that acknowledges that the balance of performance, security, and privacy will be different for each organization, and empowers IT to translate written business policy into a deliverable quality of service pledge.

Glossary

**Algorithm**
A formula or set of steps for solving a particular problem. To be an algorithm, a set of rules must be unambiguous and have a clear stopping point.

**Blue Coat ProxySG Appliance**
A system that services Web servers by offloading TCP/IP connections, responding to Web Client requests, replicating the Web content for availability and surge protection, and enhancing Web server performance. Also known as a Web accelerator or a reverse proxy server.

**Certificate Authorities**
A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be.

**Content Distribution Network (CDN)**
The physical network infrastructure of connecting global locations together which allows for Web content to be distributed to the edges of the entire network infrastructure.

**Cryptographic Algorithms**
A cryptographic system that uses two keys: a public key known to everyone, and a private or secret key known only to the recipient of the message. An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.

**Decrypt**
The process of decoding data that has been encrypted into a secret format. Decryption requires a secret key or password.

**Digital Certificate**
An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply. An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority.
Encrypt
The translation of data, a secret code. Encryption is the most effective way to achieve data security. Unencrypted data is called plain text, encrypted data is referred to as cipher text.

Global Server Load Balancer .GLSB.
Geographically front-ends server farms by balancing traffic requests to multiple servers using special load-balancing protocols that monitor the availability of individual servers and route requests to the most available server.

L4 Switch .L4. Switching
A device that delivers routing between disparate networks and clients at different layers of the OSI model. Layer 2 wire speed, layer 3 IP routing, and layer 4 policy access, and provides switching capabilities that provide resilience, performance enhancements, and ease of traffic management.

Hashing
Producing hash values for accessing data or for security. A hash value (or simply hash) is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value. Hashes play a role in security systems where they’re used to ensure that transmitted messages have not been tampered with. The sender generates a hash of the message, encrypts it, and sends it with the message itself. The recipient then decrypts both the message and the hash, produces another hash from the received message, and compares the two hashes. If they’re the same, there is a very high probability that the message was transmitted intact.

HTTP
Short for Hypertext Transfer Protocol, the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

HTTPS
By convention, Web pages that require an SSL connection start with https: instead of http.

ICMP
Short for Internet Control Message Protocol, an extension to the Internet Protocol (IP) defined by RFC 792. ICMP supports packets containing error, control, and informational messages.

IMAP
Short for Internet Message Access Protocol, a protocol for retrieving e-mail messages.

IP
Abbreviation of Internet Protocol, pronounced as two separate letters. IP specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transport Control Protocol (TCP) which establishes a virtual connection between a destination and a source.
ISP
Short for Internet Service Provider. A company that provides connection and services on the Internet, such as remote dial-in access, DSL connections and Web hosting services.

OSI
Short for Open System Interconnection, an ISO standard for worldwide communications that defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

PIN
Short for Personal Identification Number. Typically PINs are assigned by financial institutes to validate the identity of a person during a transaction.

RSA
A public-key encryption technology developed by RSA Data Security, Inc. The acronym stands for Rivest, Shamir, and Adelman, the inventors of the technique. The RSA algorithm is based on the fact that there is no efficient way to factor very large numbers. Deducing an RSA key, therefore, requires an extraordinary amount of computer processing power and time.

SSL
Short for Secure Sockets Layer, a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that’s transferred over the SSL connection.

SSL Handshake
SSL performs a negotiation between the two parties who are exchanging information, the negotiation process involves understanding the key pairs, the protocols, and the type of data request.

TCP
Abbreviation of Transmission Control Protocol, and pronounced as separate letters. TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

UDP
Short for User Datagram Protocol, a connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It’s used primarily for broadcasting messages over a network.

Web
A system of Internet servers that support specially formatted documents. The documents are formatted in with HTML (Hypertext Markup Language) that supports links to other documents, as well as graphics, audio, and video files.
Web Server Accelerators
A system that services Web servers by offloading TCP/IP connections, responding to Web Client requests, replicating the Web content for availability and surge protection, and enhancing Web server performance. Also known as a Web accelerator or a reverse proxy server.

Web Server
A computer that delivers (serves up) Web pages. Every Web server has an IP address and possibly a domain name. For example, if you enter the URL http://www.pcwebopedia.com/index.html in your browser, this sends a request to the server whose domain name is pcwebopedia.com. The server then fetches the page named index.html and sends it to your browser.