The percentage of traffic on an enterprise network that is encrypted in SSL continues to grow as increasingly more application developers use SSL to protect sensitive information. Most of the applications that use SSL are Web (or browser-based) applications – such as online banking, Web mail and CRM applications, but there are also other applications – such as Instant Messaging – that use SSL to encrypt their traffic. For approved business applications, SSL provides clear value for data protection.

Because it hides the traffic from view, SSL has also quickly become one of the most popular ways to mask malicious code such as Trojans, viruses and other exploits. Hackers know that most perimeter security products cannot examine SSL encrypted traffic so they use it to sneak malware past the perimeter and into the corporate network. IT departments cannot turn off SSL (i.e., block port 443 on the firewall) because too many business-critical applications use it, but at the same time they cannot afford to let hackers freely infiltrate their networks.

Additionally, SSL privacy can be used by employees or other authorized users to leak sensitive information, such as personnel records, credit card numbers or proprietary information and intellectual property. For example, an encrypted email that contains sensitive corporate financial information would pass by most data leak prevention solutions without being detected. Whether intentional or not, information loss over SSL represents a significant risk for organizations.

Blue Coat’s ProxySG Provides SSL Visibility and Control

By providing SSL visibility and control, Blue Coat offers a complete data leakage solution with its ProxySG family of secure proxy appliances. As opposed to point solutions which offer a limited set of protocol support and risk coverage, the Blue Coat ProxySG solution protects against a wide range of risks, regardless of whether the traffic is encrypted. Blue Coat’s market leading ProxySG appliance is deployed inside the corporate firewall – in the session path between the internal user and external application – and acts as a secure intermediary between the remote Web server and the user’s Web browser. In this type of deployment, the ProxySG will automatically set up a trusted SSL session on behalf of the browser and perform the necessary steps for authentication.

Just as important, the ProxySG can terminate the session containing encrypted data coming into the enterprise. At that point, data can be converted to “clear text” 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, which enable IT to set granular policies on which SSL sessions are intercepted, allowing organizations to adhere to corporate or governmental rules on data privacy. 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.

Blue Coat’s ProxySG allows organizations to:

- Eliminate IT’s SSL blind spot – gain visibility and control over SSL-encrypted traffic.
- Stop rogue applications (e.g., IM, P2P) that use SSL to subvert enterprise controls and security measures.
- Scan SSL-encrypted traffic for viruses, worms, and Trojans, and stop them at the gateway.
- Prevent spyware from installing or communicating over SSL.
- Halt secured phishing and pharming attacks that use SSL to hide from IT controls or to increase the appearance of authenticity.
- Accelerate approved and safe SSL-encrypted traffic.
- Take a granular approach to proxying SSL for applications of different trust levels and privacy concerns – pass through, check/verify then pass through, or proxy with full visibility and control.
- Display splash screens reminding users of acceptable use, and warn them that monitoring extends to SSL.
- Stop information leakage over SSL links through scanning of encrypted traffic for sensitive information.

Blue Coat’s SSL proxy functionality provides unprecedented visibility and control of all SSL traffic – both internal and external. Not only is security enhanced, but the user experience is improved. The Blue Coat solution actually improves overall session performance up to 1,000% by leveraging the ProxySG’s MACH5 acceleration technologies (caching, compression, bandwidth prioritization policies).

All ProxySG appliances are powered by a purpose-built operating system, and can be centrally managed as part of an enterprise-wide solution deployment.
Blue Coat SSL Proxy Solution Summary

Deployed at tens of thousands of organizations worldwide, ProxySG appliances empower the enterprise with centrally-managed proxy control points for policy, protection and performance across distributed environments.

Control Encrypted Web Traffic – define and apply fine-grained controls for users, Web content, applications and services – regardless of encryption, including access, application-aware bandwidth allocation, time, content or quota limitations and antivirus / malware scanning.

Protect Against Encrypted Web Threats & Information Leaks – defend users from threats, including viruses/worms and spyware that use encrypted tunnels on trusted partner portals, accidental uploads, Webmail or valid/spoofed Websites and block users from leaking confidential information over encrypted links.

Accelerate Encrypted Web Applications – apply a variety of compression and caching techniques to accelerate authorized access to both third-party hosted and internally hosted SSL-encrypted Web applications.

Protects the Enterprise and its Users

- With SSL Proxy, ProxySG + ProxyAV can scan all Web traffic (in the clear and encrypted) for threats, using best-of-breed scanning engines.
- Using the spyware policy in concert with SSL Proxy, ProxySG can stop spyware installation and communications – even when it’s encrypted.
- ProxySG can unmask and block encrypted phishing and pharming attacks.
- Prevent users from leaking confidential information over encrypted links – such as employees sending company data over encrypted personal Webmail accounts – by scanning traffic for personal or other sensitive information.

Controls Users and Applications

Who, What, Where, When, and How

ProxySG governs all of the key attributes of user/application interaction – knowing who the individual user is, what kind of application is being used, where the application is, when (time and priority) the application is being used, and how the interaction is being conducted (browser versions, servers, protocols, etc.). With SSL proxy, this control is extended to encrypted traffic.

Gateway Trust Decisions

ProxySG can manage certificate policy at the gateway – if a server certificate is expired or untrusted, administrators can deny the connection – rather than have end-users figure it out on their own.

Best-of-Breed URL filtering

With SSL Proxy, ProxySG’s broad URL filtering support extends to SSL-encrypted traffic – and can use certificate names in addition to hostnames for filtering input.

Stop Rogue Applications

With SSL Proxy, ProxySG can handle HTTPS with one set of controls, while handling non-HTTP SSL traffic differently (e.g., block it).

Accelerates Applications

Fine-grained, intelligent acceleration techniques (caching, compression) accelerate applications while mitigating privacy concerns.

SSL hardware acceleration (800 key negotiations per second) is available on most models.