Web Application Firewall for Untrusted Web Environments

ProxySG Web Application Firewall

Web-based solutions are being implemented for nearly every aspect of business operations, and these are increasingly under attack within public web access or untrusted environments. As a result, growing security concerns, sluggish performance, and increasing complexity are straining existing web server infrastructures. Web servers are also increasingly the primary source for malware delivery networks, hosting malware and putting users, resources and reputations at risk. Growing privacy concerns are increasing SSL usage, user identification or full authentication and putting new demands on web infrastructure. To secure and accelerate public web applications in untrusted environments, organizations turn to Blue Coat for web application firewall (WAF) protection.

Why ProxySG for Web Application Firewall Deployments?

ProxySG™ proxy appliances combine robust security, high performance content delivery, and operational simplicity, allowing organizations to secure and accelerate their public web applications to trusted users and the public.

Protects Web Servers – ProxySG securely isolates general-purpose servers from direct access, acting as an intermediary between web applications and the external clients who attempt to access them. ProxySG can provide comprehensive web server protection including: Payment Card Industry (PCI) compliance, SQL Structured Query Language (SQL) injection protection, Cross Site Scripting (XSS) protection and Cross Site Request Forgery (CSRF) protection. In addition, ProxySG provides robust authentication and policy support and can either challenge users or transparently check authentication credentials using an organization's existing security framework. For high-performance, low-latency web threat protection of all uploaded content to web servers, ProxySG integrates with ProxyAV™ and offers a choice of five leading anti-malware engines. Integration with Data Loss Protection (DLP) solutions enables both content aware fingerprinting and data loss detection of confidential, proprietary or customer information. To ensure confidentiality, ProxySG can be configured to encrypt communications between users and web applications using Secure Sockets Layer (SSL).

Accelerates Web Content – At the heart of the ProxySG solution is SGOS, a secure, object based operating system specifically designed to handle web content and rich media. SGOS combines patented proxy caching technology with an optimized TCP stack for efficient web content acceleration. SGOS's intelligent use of its integrated cache allows 60-90% of an application's web objects to be cached and served directly to users, further enhancing site performance and scalability, and simultaneously offloading web servers. Rich media support includes stream splitting and video on demand caching, plus bandwidth controls on all proxy services. In addition, SSL services provide hardware-accelerated key negotiation, encryption, and decryption support.

Simplifies Operations – An integrated, optimized appliance that combines proxy software and hardware, ProxySG is easy to install, configure, and maintain. The Visual Policy Manager (VPM) provides an intuitive, graphical interface to define and manage a wide range of policy rules. The Content Policy Language (CPL) enables advanced policy controls for application attack protection. Comprehensive logging and reporting provide

detailed accounting information, giving administrators the visibility necessary to assess web usage patterns and track security issues, plus meet regulations and policy compliance.

ProxySG Web Application Firewall enables organizations to:

- Accelerate delivery of web applications and content through a proxy architecture with integrated caching, stream splitting, bandwidth controls, threat analysis of inbound and outbound web content, and a flexible policy language with unmatched user authentication options.

- Protect web infrastructure by isolating origin servers from direct Internet access and scaling web farms by off-loading user authentication, SSL tunnels and web content optimization. Plus ProxySG health checks for HTTP, HTTPS, TCP, ICAP and ICMP to monitor web content servers and proxy related devices to alert administrators. This includes strict HTTP/HTML protocol validation from the server and client. Alerts are provided via Email, syslog and SNMP.

- Secure user access to web applications by acting as an SSL termination / origination point. This enables ProxySG as an SSL termination point with re-encryption to web servers, or a man-in-the-middle (MITM) configuration. ProxySG provides both server and client side certificate support, with web services encryption & decryption and digital signature verification. Key management and fail over handling is also provided.

- Deploy a reverse proxy solution, transparently or non-transparently as a web application firewall. The ProxySG Web Application Firewall provides an open relay server protection policy. ProxySG is also an IPv6 proxy gateway providing IPv6 to IPv4, and IPv4 to IPv6 support. New media NOCs are migrating to IPv6 and ProxySG provides the ability to serve both IPv6 and IPv4 public audiences.

- Provide compression support in HTTP to improve the web user experience. The ProxySG can compress or decompress content on the appliance and cache the response in various forms. For example, you can fetch the content in the uncompressed form, and deliver it to client in compressed form. If the content is cacheable, both compressed and uncompressed forms are stored on the ProxySG for future use. The supported compression formats are Gzip and deflate. Similarly, you can fetch compressed content from the origin web server if it provides compressed content, and decompress it on the ProxySG if the client is not capable of handling compressed content.

- Implement granular access policies based on users, groups, time of day, location, network address, user agent, and other attributes to meet unique business requirements. ProxySG has access to over 500 header request and response variables and leverages 40-plus triggers for advanced policy controls. ProxySG and filter, strip or replace content in web requests and responses via its policy controls.

- Log per policy rule and exceptions. This is very useful when detecting unknown user agents and numeric hosts in untrusted network environments. The use of the “negate” option in policy creation allows logging on a policy rule when the element is not part of the approved list for the trusted environment. As a WAF, this provides an allow policy control, in addition to the block policy control available. ProxySG’s flexible policy configuration allows either a positive security model (block everything implicitly with an allow list) or negative security model (allow everything with a block list) and a customized mixes of these two policy models. ProxySG also supports custom logging with field selection, custom text and formats within its graphical policy manager for point and click selection of custom logs.

- Provide control of file types, file extensions, true file type checks for masquerading files, the ability to strip and replace active content (Java, Visual Basic, ActiveX), restrict uploads of information, specify user agent types and versions to control client software, header inspection, rewrites and suppression, plus method level controls for HTTP, HTTPS, and FTP. ProxySG provides policy flexibility to header elements beyond typical "regex" processing for improved performance, plus full URL parsing when required.

- Authenticate clients using existing security framework, including Active Directory (NTLM, Kerberos, LDAP, SSO), eDirectory (LDAP, SSO), tokens (SecurID, Safeword), authentication schemes (Oracle COREid, CA Siteminder, x.509 certificates, local password files), credential support (NTLM, Basic, HTTPS Basic, HTML Form, HTTPS HTML Form, Explicit Proxy Auth Pop-up Form), mapping users to traffic (IP addresses, Cookies, Check with Domain Server (SSO)), and supported authentication protocols (LDAP, RADIUS, XML Interface, Sequence of Authentication Realms, Assign failed users to Guest).

- Cache user credentials within its system. Depending on the security needs of the company and the untrusted environment, credential cache can be set to store the credentials for any set period of time or flush immediately after use.

- Safeguard web infrastructure from malware, worms, and Trojans with real-time anti-malware analysis of all uploaded or downloaded content. ProxyAV integrates with ProxySG via ICAP+ or S-ICAP and leverages a dual intelligent cache design to optimize content analysis for threats. Cacheable objects are analyzed once, served and then cached for subsequent user requests. Any updates to the anti-malware analysis engine signals a new threat analysis cycle for cached objects based on user demand, the object cache is never flushed. Non-cacheable objects are fingerprinted if clean, served and then if seen again with the same fingerprint, they are served directly to users for a faster web experience. Any update to the anti-malware engine refreshes the non-cacheable fingerprint cache. ProxyAV supports five leading anti-malware engines (Kaspersky, McAfee, Sophos, Panda and Trend Micro) and analyzes files up to 2GB in size and 99 layers of compression. ProxyAV can even detect masquerading files within compressed archives with Kaspersky or Sophos anti-malware engines.

- Integrate Data Loss Protection (DLP) for compliance to stop information leakage with content aware fingerprinting of confidential information, or via keywords, lexicons, regular expressions, patterns with checksums, file meta data, or statistical analysis. Boolean logic also allows the combination of the methods noted for compliance and regulations that continue to increase to protect consumers and their privacy rights.

- Enable advanced policy controls to protect against SQL Injections, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF). ProxySG also provides complete isolation of SSL certificates, protection from buffer overflow attacks, protocol compliance checks, and DoS protection.

- Provide the ability with WebPulse to identify any malware download or call-home malicious traffic from web servers protected by ProxySG as a web application firewall. Collaborative inputs from over 75M users enable Blue Coat labs to track malware delivery networks (MDNs) and block any participation if web servers are maliciously active or providing hosting for malware delivery infrastructure. While ProxyAV reviews inbound and outbound content for specific threats, WebPulse looks at web correlations, traffic patterns, delivery methods within MDNs. While every defense provided protects web servers, the extra insurance is tracking MDNs and when and if a web server is participating.

- Deliver high-performance streaming media to thousands of simultaneous users with streaming proxies. ProxySG supports stream splitting to reduce the load on rich media servers using RTMP, RTSP or MMS,

plus HTMLv5. Caching of video on demand provides a 1:Many benefit to ProxySG including RTMP and HTML objects including Flash. Today, users expect a rich media experience and ProxySG can off-load rich media content servers to scale server farms and provide an improved user experience.

- Gain visibility by using Blue Coat Reporter to provide the ability to aggregate log files from multiple ProxySG devices for visibility and trending of Web Application Firewall utilization, threat detection from ProxyAV, user/group profile analysis, streaming and video usage, plus denied access attempts and custom logging. Reporter provides roles-based access via Active Directory inheritance, custom dashboards and reports per reporting user, and the ability to schedule and deliver both standard and custom reports on a regular basis.

- Offload webserver traffic, reducing infrastructure costs while providing control, protection, and performance.

ProxySG appliances as Web Application Firewalls enable IT administrators to efficiently scale their web farms to address flash or peak periods of traffic, leveraging advanced features, such as content acceleration, compression, protection against Denial-of-Service attacks, and optional stream splitting and caching. Administrators can also use ProxySG to implement a scalable and secured web portal by front-ending web applications.

For added security, ProxySG can originate and terminate SSL-encrypted sessions between web applications and users. This allows organizations to secure actions such as authentication and message review on both sides of the data stream.

To prevent subsequent users to a particular kiosk or workstation from accessing a previous user's account, ProxySG can be configured to erase cached authentication cookies. For added protection, the ProxySG Web Application Firewall can be configured to automatically time out after a specified period of inactivity, enabling administrators to strengthen secure access from public networks. Blue Coat ProxySG is the leading proxy appliance for securing and accelerating web applications. ProxySG Web Application Firewall integrates robust web server protection and accelerated web content delivery in a scalable, centralized proxy architecture that simplifies operations while significantly enhancing network performance.

Key Features and Benefits:

Protects Web Servers

- Securely isolates general-purpose servers from direct access.

- Built on SGOS, a secure object-based operating system specifically designed to handle web content. ProxySG is FIPS 140-2 certified, plus Common Criteria EAL2 certified (3 major SGOS versions).

- Controls user access with robust authentication and policy rules.

- Intelligent OS distinguishes between valid and malicious connections to service legitimate users while resisting DoS attacks.

- Allows inline scanning of content, with integrated anti-malware, DLP and malicious web traffic defenses.

Accelerates Web Content

- Optimized TCP stack rapidly serves large amounts of static and dynamic web content.
- Intelligent cache allows 60-90% of an application's web objects to be cached and served directly to users.
- HTTP compression reduces required bandwidth, conserves CPU resources, and delivers previously compressed pages faster.
- Hardware-accelerated SSL processing of key negotiations.
- Streaming proxies provide stream splitting and caching of video on demand to deliver high-performance streams to thousands of simultaneous users.

Simplifies Operations

- "Set and forget" proxy appliance is easy to deploy and manage.
- Integrated appliance eliminates need to install applications or OS patches.
- Scalable solution reduces number of web servers required.
- ProxySG can be clustered and configured for high-availability with load balancers.
- Intuitive graphical interface simplifies policy rule creation and management.
- Comprehensive logging and reporting provide visibility into web usage patterns and security issues.
- Offloads IT infrastructure, reducing infrastructure costs while providing control, protection, and performance.

Summary

For untrusted web environments, ProxySG Web Application Firewall is rich in authentication options, SSL off-loading, and both object caching and rich media optimization to scale web applications. As users move to tablets and smart phones with access from unknown networks, or their everyday desktop within a company office location, they expect a fast web experience, no delays, available web content and rich media on demand. While virtualization enables new data center economics and scale, the ability to optimize and scale out both traditional web server farms, or virtualized ones, remains a Web Application Firewall benefit for public facing web services.

As SSL growth continues for compliance and privacy concerns, ProxySG scales out SSL performance to off-load web server infrastructure. ProxySG Web Application Firewall uses a secure proprietary OS that provides a safer footprint and keeps web origin servers safely protected inside a network and out of harm's way. Integrated AV, DLP and malicious web traffic analysis, plus advanced policy controls to block application and browser attacks make ProxySG a unique and valued Web Application Firewall solution.