Solution Brief

Symantec
A Division of Broadcom

Web Application Firewall for Web Environments

Overview

Web-based solutions are being implemented for nearly every aspect of business operations, and increasingly for trusted environments with mission-critical business applications. 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, and full authentication and putting new demands on web infrastructure—both on-premises and in the cloud. To secure and accelerate web applications, whether with their own apps hosted in environments like Amazon Web Services (AWS) or cloud applications from vendors like Oracle, Microsoft, SAP and others, organizations turn to Symantec® Web Application Firewall (WAF)—deployed either on-premises or as a virtual solution in AWS.

Why Symantec for WAF Deployments?

Symantec WAF combines robust security, high-performance content delivery, and operational simplicity on a secure proxy architecture—allowing organizations to secure and accelerate their web applications to end-users, customers, employees, and vendors.

Application Protection: The WAF offering includes advanced next-generation protection engines designed to target the OWASP Top 10 vulnerability concerns. Protection is provided through advanced signature-less engines. Administrators can set policy taking advantage of protection that includes content nature detection engines for protection around code injection, HTML injection, directory traversal, command injection, JSON validation, SQL injection, and cross-site scripting. In addition, signature-based engines can be used for blocking known attack patterns.

Protects Web Servers: The WAF securely isolates general-purpose servers from direct access, acting as an intermediary between web applications and the external clients who attempt to access them. The WAF 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, the WAF integrates with the Symantec Content Analysis System and offers a choice of three leading anti-malware engines, plus static code analysis, sandbox brokering, and integration. To ensure confidentiality, the WAF can be configured to encrypt communications between users and web applications using Secure Sockets Layer (SSL)/Transport Layer Security (TLS).

Accelerates Web Content: The WAF is based on 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 to 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 physical or virtual appliance that combines proxy software and hardware, the WAF is easy to install, configure, and maintain on-premises or virtually in AWS. Symantec Management Center provides an easy to use graphical interface to define and implement policy rules. 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.

Geo-IP: The WAF includes Geo-IP capability. Geo-IP enables administrators to set policy based on the geographic location of the end-user accessing the enterprise website. It allows country-specific locations to be used in policy for regulatory, corporate, or compliance needs—or for help with troubleshooting policy. Geo-IP allows customers to identify the country location of a specific client IP of traffic coming to the WAF. The Geo-IP database is automatically updated through the Symantec Global Intelligence Network (GIN) to reflect changes in locations of the IP addresses.

The WAF enables organizations to do the following:

- Accelerate delivery of web applications and content through 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 and secure 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 the WAF 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, such as web e-mail, intranet, and extranets by acting as an SSL/TLS termination/origination point. The WAF provides both server and client side certificate support, with web services encryption and decryption, and digital signature verification. Key management and failover handling is also provided. In addition, the WAF can also act as an IPv6 web gateway providing IPv6-to-IPv4 and IPv4-to-IPv6 proxy gateway capabilities. New media NOCs are migrating to IPv6 and the WAF provides the ability to serve both IPv6 and IPv4 audiences.
- Support deployments on-premises and in the cloud, with on-premises physical or virtual appliances, and virtual deployments in Amazon Web Services (AWS).
- Deploy a reverse proxy solution, transparently or non- transparently, using the WAF. The WAF provides an open relay server protection policy as well as compression support in HTTP to improve the web user experience. The WAF 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 WAF 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 WAF 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. The WAF has access to over 500 header request and response variables and leverages 40-plus triggers for advanced policy controls. For example, user policy can be enforced requiring certain browsers and/or browser software versions.
- Support load balancing for distribution of traffic to multiple web server farms and clustering of WAF appliances for high availability. Enhanced load balancing is also available with a number of partner-based solutions.
- Enable logging per policy rule and exceptions. This is very useful when detecting unknown user agents and numeric hosts on a trusted network environment. 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 allow-listing policy control. The WAF also supports custom logging with field selection, custom text, and formats within its graphical policy manager for point-and-click selection of custom logs.
- Control 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, two way URL rewriting plus method level controls for HTTP, HTTPS, and FTP. The WAF 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, SAML, and Kerberos Constrained Delegation).

- Cache user credentials within its system. Depending on the security needs of the company and the trusted 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. Content Analysis System integrates with the WAF 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. Content Analysis System supports three leading anti-malware engines (Kaspersky, McAfee, and Sophos) and analyzes files up to 5 GB in size and 99 layers of compression. Content Analysis System can even detect masquerading files within compressed archives with Kaspersky or Sophos anti-malware engines. In addition, Content Analysis System supports static code analysis, allow listing, and sandbox integration and brokering.
- Deliver high-performance streaming media to thousands of simultaneous users with streaming proxies. The WAF 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 one-to-many benefit to the WAF including RTMP and HTML objects (including Flash). Users expect a rich media experience and the WAF can offload rich media content servers to scale server farms and provide an improved user experience.
- Gain visibility using Symantec Management Center and Symantec Reporter to aggregate log files from multiple WAF devices for visibility and trending of WAF utilization, threat detection from the advanced nature content threat detection, as well as the traditional detection engines and the Content Analysis System, user/group profile analysis, denied access attempts, and more. Management Center provides role-based access via Active Directory integration and custom dashboards when integrated with Reporter.
- Offload webserver traffic, reducing infrastructure costs while providing control, protection, and performance.

WAF appliances are easily configured and tuned for the workload of high traffic websites. IT administrators can use the WAF 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 the WAF to implement a scalable and secured web portal by front-ending web applications such as corporate web email (for Outlook Web Access, Lotus Domino, SharePoint, and so on) and web-based business applications (Siebel, Oracle, SAP, and so on).

For added security, the WAF can originate and terminate SSL/TLS-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 of a particular kiosk or workstation from accessing a previous user's account, the WAF can be configured to erase cached authentication cookies. For added protection, the WAF can be configured to automatically time out after a specified period of inactivity, enabling administrators to strengthen secure access from public networks. Symantec WAF is the leading proxy appliance for securing and accelerating web applications in trusted and untrusted environments. The WAF 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

- Advanced next-generation protection engines target all security risks including the OWASP Top 10 vulnerability concerns. Protection is provided through advanced signature-less engines. Examples of available security include protection around code injection, HTML injection, directory traversal, command injection, JSON validation, SQL injection, and cross-site scripting. In addition, signature-based engines can be used for blocking known attack patterns.

- Securely isolates general-purpose servers from direct access.
- Built on SGOS, a secure object-based operating system specifically designed to handle web content. The WAF is built on the ProxySG platform, which 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.

Accelerates Web Content

- Optimized TCP stack rapidly serves large amounts of static and dynamic web content.
- Intelligent cache allows 60 to 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-assisted SSL/TLS 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.
- Intuitive graphical interface simplifies policy rule creation and management.
- Comprehensive logging and reporting provide visibility into web usage patterns and security issues.
- Offloads IT web infrastructure, while adding control, protection, and performance to existing applications.
- Deployable as on-premises or virtual appliances, and with virtual appliances in Amazon Web Services (AWS)

Summary

For web environments, the WAF provides a full-protection reverse proxy solution rich in authentication options, SSL/TLS 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 reverse proxy benefit, available on-premises or in AWS.

As SSL/TLS growth continues due to remote access with mobile workers, the WAF scales out SSL performance to offload web server infrastructure. The WAF within a DMZ using a secure proprietary OS provides a safer footprint and keeps web origin servers safely protected inside a network and out of harm's way. Web-based business applications, collaboration solutions, web-based email, online training, and live media all benefit from a Symantec WAF.

WAF-Web-Environments-SB100 January 7, 2022