WAF for Enterprises

Mission Critical Applications Need More than a Firewall and IPS for Complete Security

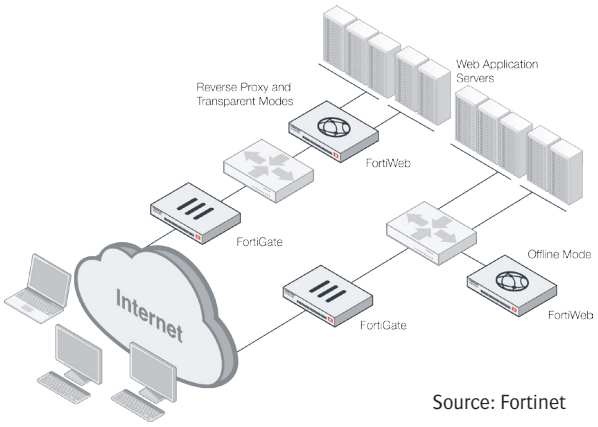
Introduction

In today's ever-changing threat landscape, enterprises must have the latest in firewall and intrusion protection to defend their networks, applications and users from sophisticated and dynamic attacks. However, even the most advanced firewalls and IPS systems can do only so much when it comes to protecting against attacks that target weaknesses in your web-based applications. Firewalls and IPS systems rely on signatures to detect application attacks like Cross Site Scripting and SQL Injection. This method can be highly reliable against previously discovered threats, however it cannot detect zero-day application attacks.

Application Protection Beyond Compliance

Although Payment Card Industry Data Security Standards (PCI DSS) compliance is the primary reason most organizations deploy Web Application Firewalls (WAFs), many who don't need to comply with PCI standards are now realizing that web applications can be the easiest point of entry for data breaches. Externally facing web applications are vulnerable to attacks such as Cross Site Scripting, SQL injection, and layer 7 Denial of Service (DoS). Internal web applications can be even easier to compromise if an attacker is able to gain access behind the firewall. Many enterprises mistakenly think they're protected by their perimeter network defenses and don't think applications behind them are at risk.

Typical FortiWeb Deployment Options



Source: Fortinet

Custom code is usually the weakest link as development teams have the impossible task of staying on top of every new attack type. However, even commercial code is vulnerable as many organizations don't have the resources to apply patches and security fixes as soon as they're made available. Even if every patch is applied and there's an army of developers to address code vulnerabilities, zero day attacks can leave systems defenseless.

FortiWeb Web Application Firewalls: Complete Application Protection

Only Fortinet offers high-performance enterprise-grade WAFs with throughputs up to 20 Gbps that include ASIC-based SSL offloading, layer 7 load balancing, antivirus, and application vulnerability scanning for complete web-application protection and compliance.

FortiWeb uses an optimized multi-layered approach to detecting application threats that cover the OWASP Top 10 and many other threats, plus it can detect zero day web-application attacks.

Multiple Layers of Protection:

- IP Reputation to scan for botnets and other malicious sources.
- DoS detection and prevention.
- HTTP RFC validation and compliance.
- FortiWeb WAF Security Signatures to detect known attack types.
- Antivirus and Antimalware protection.
- Automatic Behavioral detection to screen for unknown attacks.
- Correlation of attack mechanisms to detect sophisticated threats.

Included Vulnerability Scanning and Third-party Virtual Patching

Only FortiWeb includes a web application vulnerability scanner in every appliance at no extra cost to help meet PCI DSS compliance or to perform security audits of applications. FortiWeb's vulnerability scanning dives deep into all application elements and provides in-depth results of potential weaknesses in applications. FortiWeb also provides integration with third-party vulnerability scanners to provide dynamic virtual patches to security issues in enterprise application environments. Vulnerabilities found by the scanner are quickly and automatically turned into security rules by FortiWeb to protect the application until developers can address them in the application code.

Secured by FortiGuard

Fortinet's Award-winning FortiGuard Labs is the backbone for many of FortiWeb's layers in its approach to application security. Offered as 3 separate options, FortiGuard services can be subscribed to as needed to protect web applications. FortiWeb IP Reputation service protects from known attack sources like botnets, spammers, anonymous proxies, and sources known to be infected with malicious software. FortiWeb Security Service is designed just for FortiWeb that includes items such as application layer signatures, malicious robots, suspicious URL patterns and web vulnerability scanner updates. Finally, FortiWeb offers FortiGuard's top-rated antivirus engine that scans all file uploads for threats that can infect servers or other network elements.

Deep Integration for Advanced Threat Protection

FortiWeb is one of many Fortinet products that provides integration with our FortiSandbox advanced threat detection platform. FortiWeb can be configured with FortiSandbox to share threat information and block threats as they're discovered in the sandboxing environment. Attachments sent to web servers can be sent to FortiSandbox for analysis and quarantined until they're proven safe. If they're not, the files are flagged for inspection or removal.

Easy to Deploy and Manage

Unlike many other WAF solutions, FortiWeb has been designed to provide maximum flexibility and ease of use. FortiWeb is offered in hardware and virtual versions, including on-demand licensing available through Amazon Web Services. It supports multiple deployment configurations including Reverse Proxy, Inline Transparent, True Transparent Proxy, and Offline Sniffing modes. Out-of-the-box, FortiWeb is preconfigured to protect applications from common application threats where it can be deployed quickly and its auto learning mode can protect most environments after less than an hour of traffic monitoring. Using its intuitive GUI, FortiWeb easily can be configured, managed, and used to generate detailed application attack reports.

Source: Fortinet

From the Gartner Files:

Web Application Firewalls Are Worth the Investment for Enterprises

Firewalls and intrusion prevention systems don't provide sufficient protections for most public-facing websites or internal business-critical and custom Web applications. Here, we explain how Web application firewalls help security leaders to better protect Web applications in their organizations.

Key Findings

- Web application firewalls (WAFs) are different from next-generation firewalls (NGFWs) and intrusion prevention systems (IPSs). WAFs protect, at a granular level, the enterprise's custom Web applications against Web attacks.
- Even when NGFWs and IPSs are deployed, the WAF is most often the only technology that inspects encrypted and unencrypted inbound Web traffic.
- Understanding how much work your staff will undertake is a critical decision factor in whether you employ a WAF and how. Avoiding false alerts ("false positives"), in particular, requires specific attention.
- Enterprises tend to focus their WAF efforts on compliance or protecting public-facing custom Web applications, but often neglect equally important internal applications.

Recommendations

Security leaders should:

- Strive for more than PCI compliance. Assess the need for Web application firewalls, based on the business impact of each Web application — public-facing, partner-facing or internal — rather than protecting public-facing Web applications only.
- Evaluate and deploy WAF technology, in combination with alternative security safeguards, such as application security testing and secure coding practices.
- Evaluate which deployment use cases are acceptable for your organization, and understand the specific challenges for each.
- Invest enough time in training security staff, conducting initial configuration tuning during the learning period and performing integration with other network security technologies. Then, continuously monitor and update the WAF configuration to gain the benefits from the technology.

What You Need to Know

WAFs are deployed on or in front of Web servers, and include protection techniques dedicated to the granular protection of specific Web applications. WAFs combine negative (protecting against known attacks) and positive (enforcing legitimate traffic only) security models to detect and protect against Web attacks and reduce the risk of false positives.

Security professionals sometimes confuse WAFs with NGFWs, or estimate that WAFs do not bring enough value to justify the cost when compared with IPSs. Organizations already equipped with best-of-breed firewalls and IPSs might view WAFs as an exponential investment for incremental benefits. However, IPS protections against Web vulnerabilities are too general; often limited to known vulnerabilities from off-the-shelf third-party libraries and frameworks. These protections are also mostly disabled by default. Corporate websites and Web applications carrying business-critical operations, such as for payroll, e-banking transactions and e-commerce orders, often include a combination of custom code, with self-inflicted vulnerabilities and third-party components. CIOs can't decide to leave critical Web servers untouched for fear of false alerts or service interruptions, because the complex Web languages (HTML5, JavaScript) give attackers attractive targets.

Security leaders should consider investing in WAFs, application security testing and secure coding tools if their organization owns public websites, makes internal Web applications available to partners and clients, or has business-critical internal Web applications. Organizations that receive the greatest benefits from WAFs will go beyond compliance. They will spend enough time to select the right WAF deployment scenario, train operational staff, tune the different protections and monitor the infrastructure closely.

Analysis

In the early 2000s, most enterprises were not using WAFs to protect their Web servers and applications. Firewalls were the best practice, and intrusion detection and prevention were still maturing. The relatively low complexity of the Web applications was not a sufficient driver to justify an additional investment, and attackers were not yet backed by well-funded organizations.

Since then, Web applications have become more complex, relying on languages and scripts such as HTML5, Java, JavaScript, and PHP for rich interface application (RIA),extensive frameworks and complex third-party libraries. False positives and performance hits arising from protections that relied on traffic-pattern matching became a real issue. IPS vendors elected to disable most of the Web application protection signatures by default to mitigate these issues. Type A organizations realized the need for a new approach to Web application security, and have added WAFs to their security portfolios.

In 2008, the PCI Security Standards Council (PCI SSC) released the PCI Data Security Standard (PCI DSS) 1.2 with an updated requirement 6.6, which allowed WAFs as a viable alternative to Web application vulnerability assessments.[1] The PCI requirement has given additional momentum to the WAF market, helping it expand beyond niche use cases, especially in financial and banking organizations.

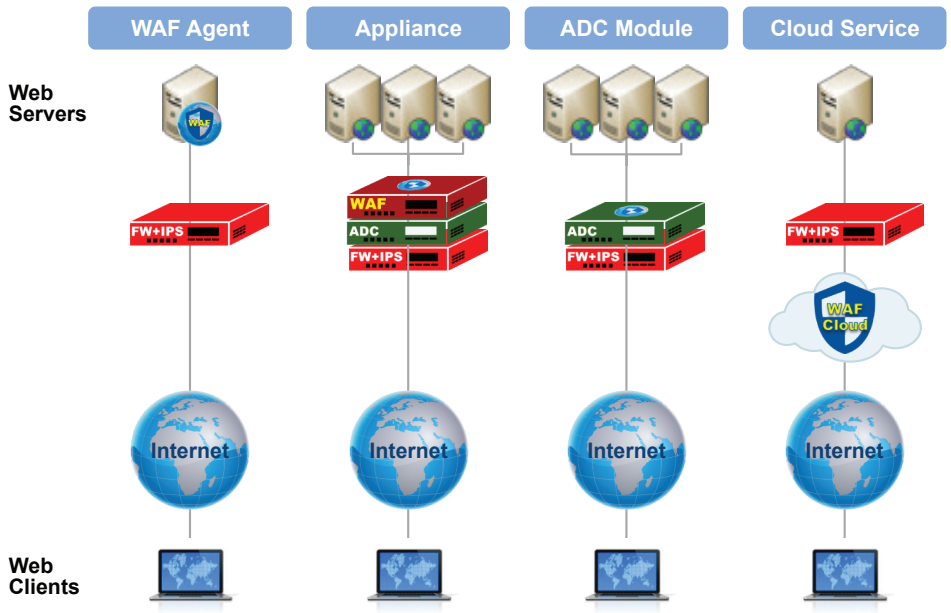
Unfortunately, many enterprises and WAF vendors use the low PCI compliance standard as the goal and do not seek more than a successful audit. Good Web application security requires more than a checkbox approach. Most WAFs can provide the PCI check mark but, as history often reminds us, compliance is not automatically equivalent with good security. Competitive evaluations for WAF technologies are still complicated and require a lengthy proof of concept, because similar feature names mask significant discrepancies in security depth. Once in production, WAFs continue to demand close monitoring to deliver high value.

This research covers the major features of WAF technology, explains the deployment options and provides selection guidelines. It will help security leaders responsible for Web application security projects to better understand the benefits and challenges of WAF implementation.

Technology Description

Web application firewalls protect Web servers and hosted Web applications against attacks at the application layer and nonvolumetric attacks at the network layer. It can be deployed as an endpoint

FIGURE 1 Web Application Firewall Deployment Options for On-Premises Web Applications



Source: Gartner (February 2014)

agent on the Web server, a software or hardware network appliance, a software module hosted on an application delivery controller (ADC; see "Magic Quadrant for Application Delivery Controllers"), a virtual appliance or a cloud service (see Figure 1). Most of the time, WAFs are in-line, acting as a reverse proxy, but other deployments are available, such as transparent proxy, network bridge or out-of-band.

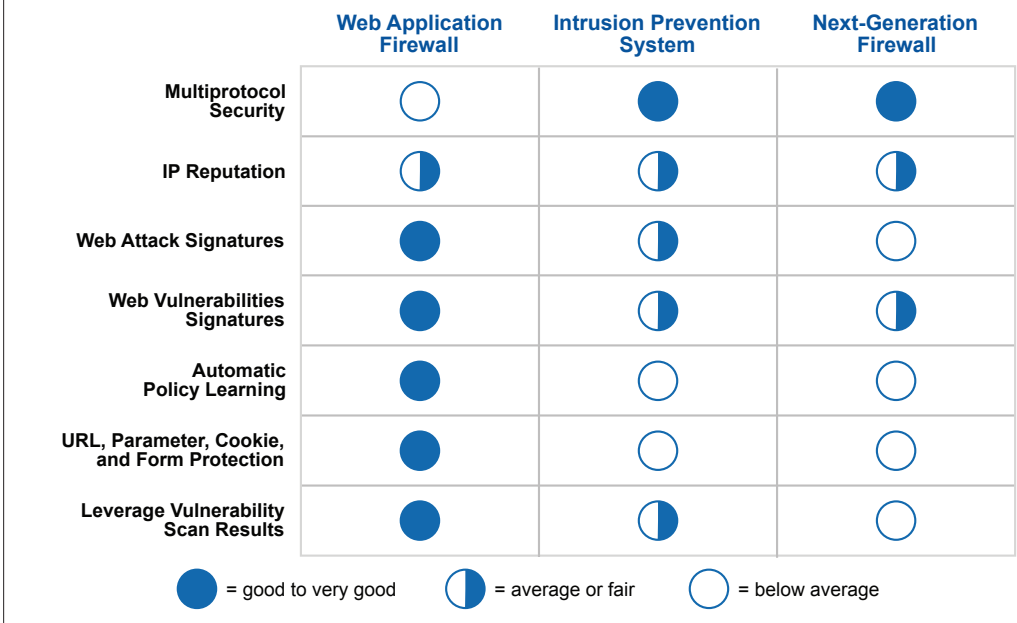
Web Attacks Command More Than Signatures

Threats against Web applications are well-documented. The Open Web Application Security Project (OWASP) Top Ten, CWE/SANS Top 25 Most Dangerous Software Errors and Web Application Security Consortium (WASC) Threat Classification v2.0 and Cross Reference View can help raise awareness of the threat landscape, providing elements to justify the need for technology dedicated to Web application security. However, security staff often fail to explain how WAFs can provide deeper, more-granular Web application safeguards than NGFWs and IPSs. Figure 2 highlights feature differences between NGFWs, IPSs and WAFs when it comes to Web application security.

Firewalls and IPSs provide signatures, mostly against SQL injection (SQLi) or cross-site scripting (XSS), but do not include more advanced features that WAF technologies can offer, such as:

- **Contextualized Web traffic inspection**: WAFs embed dedicated inspection engines for Web protocols and languages, to perform traffic decoding and normalization before applying in-context security inspection. This improves the effectiveness of Web attack and Web vulnerabilities signatures.
- **Automatic policy learning**: The WAF security engine listens to HTTP requests/answers for configured Web domains, creates a map of URLs and different parameters, then suggests appropriate whitelisting enforcements (often called positive security models).
- **"Virtual patching"**: The name is an overstatement. The WAF can leverage data from dynamic application security testing (DAST) tools to suggest or automatically enable additional controls/signatures to protect against the detected threats. The level of value provided highly depends on the quality of the vulnerability assessment tool.
- **Anti-automation**: This distinguishes real humans from automated clients that would interact with a Web application.

FIGURE 2 Main Differences Between WAF, IPS and NGFW



IP = Internet Protocol
Source: Gartner (February 2014)

- **Business logic defense**: WAFs monitor user sessions to detect attacks that exploit business transactions in order to perform malicious activities that disrupt a normal business practice.

- **Anti-DDoS**: WAFs might include protection against application-targeted distributed denial of service (DDoS), but can't mitigate volumetric attacks. Vendors with a cloud offer often try to upsell their anti-DDoS solutions to their clients using WAFs.

These features are not the only differences between WAFs and other network security technologies. IPS appliances can operate out-of-band, on a copy of the traffic — or in-line, in bridge mode. While a few WAF technologies support these two deployment modes, most of them use the more intrusive reverse or transparent proxy modes. Acting as a proxy allows additional operations:

- **Secure Sockets Layer (SSL)/Transport Layer Security (TLS) decryption/offloading**: Reverse or transparent proxy modes allow decryption of TLS traffic when using cipher suites that enable forward secrecy2 (Ephemeral Diffie-Hellman [DHE] and Elliptic Curve Diffie-Hellman [ECDH]). For other ciphers, WAFs might offer the ability to decrypt a copy of the encrypted traffic, when deployed in in-line bridge mode, or out-of-band.

- **Web content modification**: WAFs modify the responses sent by Web applications with techniques such as cookie signing, URL encryption, custom error page, and code injection in Web pages (for example, to prevent cross-site request forgery [CSRF]).

- **Authentication services**: WAFs can provide single sign-on for existing Web applications, or act as an authentication broker for legacy applications that don't have any authentication in place.

The ability for WAFs to decrypt SSL traffic makes a big difference when compared to NGWFs and IPSs. In 2013, Gartner conducted an industry survey of network security vendors and enterprises to find out how organizations are tackling the challenge of traffic decryption (see "Security Leaders Must Address Threats From Rising SSL Traffic"). The survey revealed that less than 20% of organizations with a firewall, an IPS or a unified threat management (UTM) appliance can decrypt inbound or outbound SSL traffic. However, more than 90% of organizations with a public website and a WAF can decrypt inbound Web traffic.

WAF technology might provide many other features, including ad hoc reports for PCI audit, multiprotocol inspections to cover other services provided by Web applications (such as FTP), Web service security, or remote user/host fingerprinting.

Technology Definition

A Web application firewall is a shielding safeguard intended to protect applications accessed via HTTP and HTTPS against exploitation. WAFs focus primarily on Web server protection at Layer 7 — the application layer — which includes classes of "self-inflicted" vulnerabilities in configured commercial applications, or in custom-developed code that makes Web applications subject to attacks. WAFs may also include safeguards against attacks at other layers.

Uses

Enterprises primarily use WAFs to protect public Web applications, as well as custom and internal applications such as payroll, Web mail or extranet. On rare occasions, organizations also use WAFs to protect their on-premises internal applications, such as intranet, since these applications are some of the easiest targets for attackers looking for a lateral move after an initial infection. WAF projects can be driven by compliance issues or initiated to improve the security of business-critical Web applications. At times, organizations leverage other infrastructure projects to include WAFs in an ADC deployment or within a DDoS mitigation project.

Benefits and Risks

WAF technology leverages the knowledge gained on Web applications via careful monitoring of the applications' behavior to implement tightened security controls. When correctly implemented and tuned, WAFs are the technology of choice to enhance the security of existing Web applications. However, when organizations don't invest enough energy in their WAF deployment, they often face disappointing results.

Risks:

- False positives are the most important risk when deploying WAFs. Fear of false positives affects many WAF implementations and can lead to the displacement of the technology.

- Automatic policy learning can fail in various ways. If using a WAF as a permanent monitoring tool is not the objective, this might be an important issue. Organizations with fast-changing Web applications sometimes never progress beyond the learning period, due to a fear of false positives. Security leaders should also anticipate business-specific use cases, like B2B commerce with a peak period at the end of every quarter, or e-commerce sites with annual events such as the holiday season at the end of the year.

- WAF inner vulnerabilities are more critical than for other network security technologies. When acting in reverse or transparent proxy mode, the WAF itself might be a target for attackers.

- WAFs don't protect against volumetric DDoS attacks, which can bring down public websites and Web applications allowing remote access.

Technology Alternatives

When compliance dictates the WAF implementation project, application security testing (AST) coupled with software development best practices often compete with the WAF budget (see "Magic Quadrant for Application Security Testing," "Interaction Between Security Scanners and Monitors Strengthens Application Protection" and "Application Security Detection and Protection Must Interact and Share Knowledge").

Organizations should put effort into secure development practices through development staff training and static code analysis and scanning, and they should consider the use of specific sanitization libraries (see the OWASP Developer Guide). However, Web applications rely heavily on third-party modules or libraries, so the detection of vulnerabilities can fall out of the direct control of Web application development teams. Upgrading these components might not be possible in a timely manner, and network-based compensatory controls might remain necessary. Using penetration testing applications can complement a secure development approach to provide a better assessment of the risks for Web applications.

NGFWs and IPSs include signature sets for Web application protection. Enterprises might see them as a price-attractive solution compared with a dedicated WAF. As discussed earlier in the document, these technologies only offer a subset of the many protections techniques available with a WAF. Moreover, Web security signatures are disabled in most default configurations, which means the workload is transferred to the network security staff. Fine-tuning the configuration per Web domain might also be difficult, with technologies not optimized to be sufficiently granular.

Open-source, free Web application firewalls like the ubiquitous ModSecurity or the more recent IronBee often compete against commercial offers. Even when a commercial set of signatures is available, organizations should carefully assess what the true gains will be, since these solutions are likely to require much more configuration work and rely on signatures, which is the technology most prone to false alerts.

Other vendors, such as Shape Security or Juniper Networks, with its WebApp Secure offering, focus on a few innovative techniques to protect Web applications. On-server security applications (such as runtime application self-protection [RASP]) are also available.

Selection Guidelines

Organizations willing to perform a competitive assessment of WAF vendors might face unexpected difficulties. PCI compliance and the availability of various ad hoc threat lists shape many RFPs. Too often, the comparison shrinks to a list of features, which lacks the necessary depth to uncover true differences between WAF vendors.

The WAF market landscape includes many different categories of vendors: large and small WAF pure players, more general network security vendors, ADC vendors, and cloud service providers. A number of the vendors are also relative newcomers to the WAF market, and are in the middle of an ambitious road map for Web application security. Organizations should understand the characteristics of each vendor to determine whether the vendor meets the organization's needs.

WAF Deployment Scenario Drives the Selection Process

Enterprises should first evaluate which deployments options are acceptable for them. Each deployment scenario brings its own challenges (see Table 1), and many WAF vendors provide only the reverse proxy mode.

Table 1. WAF Selection Questions for Different Deployment Use Cases

Use Case	Major Challenges	Subsequent Questions
Internet-Hosted (Cloud)	• Need for SSL decryption (secret key management) • Protection of internal Web applications • Incident response • Opt out	• How do the organization's compliance requirements affect its ability to delegate SSL decryption? • How will the organization handle incidents and false alerts (monitoring and response)? • What is an acceptable SLA for each level of incident? • How long does it take to opt out from the WAF provider?
Reverse or Transparent Proxy	• Performance • Tighter dependency with Web application due to "man in the middle" approach	• How can the WAF scale up and scale horizontally (cluster)? • How does the WAF integrate or partner with load balancers/ADCs? • What does the application team manage? What belongs to the security team?
In-line Bridge Mode	• SSL/TLS decryption with perfect forward secrecy • Limited ability to modify content	• What are the compensatory controls your organization can deploy to replace the features that require content modification? • Do (or will) the Web applications implement Diffie-Hellman cipher suites (forward secrecy)?
Out-of-band	• Restricted number of WAF vendors • Limited ability to block, and no ability at all to modify content • SSL/TLS decryption with perfect forward secrecy	• What are the acceptable compromises to keep this deployment scenario? What wouldn't be acceptable? • How will the organization handle incidents and false alerts (monitoring and response)? • Do (or will) the Web applications implement Diffie-Hellman cipher suites (forward secrecy)?

Source: Gartner (February 2014)

In large-scale deployments in which organization use ADCs, the integration of WAF features will benefit from available performance optimization features and shared traffic processing efforts.

Once the deployment scenario is chosen, security leaders should take special care of high-availability requirements, including cluster upgrade procedures and their impact on the production environment.

Enterprises Need to Compare WAFs Beyond Datasheet Check Marks

Differences between WAF technologies regarding price and performance may be easily recognized from the start, but discovering discrepancies in protection techniques requires further investigation. Because these differences exist (see Table 2 for examples), security leaders should not rely on vendor claims, but should use the proof of concept and request feedback from their peers to verify the efficiency of the different techniques in their own environment.

During WAF competitive assessment, security leaders should specifically question smaller WAF vendors and newcomers to the market about their reputation databases and their attack signatures databases. Be wary about miraculous generic approaches, especially for protections against XSS and SQLi. Even the most basic protections are tested against known tools like Metasploit, so it can be used as an exclusion criterion, but should not be considered as sufficient. In 2013, 650 XSS attacks and 150 SQLis have been added to the Common Vulnerabilities and Exposures (CVE) database.[3] Selecting a few known recent attacks and asking vendors about them will give security leaders a better sense of a vendor's coverage.

Organizations should also understand that some attacks, such as CSRF, are hard to catch, and that no turnkey preventive solution can guarantee a perfect protection.

Table 2. Analyzing Depth of WAF Protection

Threat	Minimal Protection	More-Advanced Techniques
Cross-Site Scripting (XSS) **SQL Injection (SQLi)**	• Pattern-matching signatures aimed at catching keywords	• Analyzing requests and responses • Multiple pass for traffic normalization covering various evasion techniques • Aggregated and contextual scoring to reduce false positives • Supplementary ad hoc signatures for known attacks • Enforcement using whitelisting rules
Automatic Policy Learning	• None (manual import of site map) *or* • One-time period without automatic ending	• Behavioral analysis automatically disables signatures that would trigger false positives • Automatic policy update when application changes • Predefined templates for well-known applications (Microsoft SharePoint, Microsoft Outlook Web Access, etc.)
"Virtual Patching"	• None or • Manual import of vulnerability scan result and/or • Limited number of supported scanners	• Automatic enforcement for critical vulnerability • Ability to launch a second test to confirm that a vulnerability is patched • Impact assessment of "virtual patch" deployment to help with the administrator's decision
Source: Gartner (February 2014)		

Web Application Security Is the "Heavenly Realm" for Evasion Techniques

The complexity of programming languages used in Web applications, and the extensive use of third-party source code and third-party byte/binary code in the form of libraries or frameworks, create perfect conditions for evasion techniques. A single vulnerability can be triggered in various ways, an SQLi can be distributed over several URL or form parameters, or the same string can be encoded in alternate ways. In addition, browsers might interpret the same content in a different way.[4]

Security leaders should request from WAF vendors additional elements regarding how their technology can prevent known evasion techniques and anticipate upcoming new variants.[5] Evaluation should only take into account specific examples of real attacks and discard marketing statements that are not backed up with evidence.

As a start, the WASC's Web Application Firewall Criteria (WAFEC), despite their publication in 2006, remain a good independent template to cover the basics of a WAF selection RFP, even if organizations must adapt each section to their specific needs.

Price Performance

WAF pricing models might vary based on the vendors and their deployment use cases. While most vendors offer the traditional initial purchase coupled with maintenance and subscriptions bundles, a few WAF vendors add additional limits, such as the number of Web applications, server IP addresses, or the CPU core for software appliances. Additional limits based on performance metrics, such as the number of transactions per second, might also apply. Cloud providers use subscription fees (monthly or yearly), occasionally coupled with performance-related restriction (page views).

Gartner recommends that clients ask WAF vendors for simple pricing models and require proposals with total cost of ownership for multiple years, including all the recurring subscriptions. Performance measurement can't be reliably assessed from vendor's collaterals, and should be confirmed during a proof of concept. Additional costs for SSL acceleration might significantly impact the total cost. Moreover, Gartner observes that many WAF deployments face unexpected short life cycles due to a lack of anticipation of growing application traffic. Organization should provision for growing Web and encrypted traffic based on trends observed in the past and knowledge of upcoming changes in their application offers.

Technology Providers

Sample WAF Vendors:

- A10 Networks
- AdNovum
- Akamai Technologies
- Anchiva
- Barracuda Networks
- Bee Ware
- BugSec
- Citrix
- CloudFlare
- DBAPPSecurity
- DenyAll
- Ergon Informatik
- F5 Networks
- Fortinet
- Igaware
- Imperva
- Nsfocus
- Penta Security
- Positive Technologies
- Qualys
- Radware
- Riverbed
- Sangfor
- Sucuri Security
- Trustwave
- United Security Providers
- Venustech

Sample Open-Source Projects:

- ModSecurity
- IronBee

Evidence

[1] "Payment Card Industry (PCI) Data Security Standard — Requirements and Security Assessment Procedures Version 1.2," October 2008; and "PCI Data Security Standards Council — Information Supplement: Application Reviews and Web Application Firewalls Clarified," October 2008.

[2] "SSL/TLS & Perfect Forward Secrecy," by Vincent Bernat, 2011.

[3] "Common Vulnerabilities and Exposures Details."

[4] "The InnerHTML Apocalypse: How mXSS Attacks Change Everything We Believed to Know So Far," by Mario Heiderich, Muenster University of Applied Sciences, 2013.

[5] "Protocol-Level Evasion of Web Application Firewalls," by Ivan RistiĐ, 25 July 2012.

Source: Gartner Research, G00258206, Jeremy D'Hoinne, Adam Hils, 12 December 2014

About Fortinet

Contact Us

Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and a market leader in unified threat management, next generation firewall and high performance datacenter firewall. Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2012 Fortune Global 100. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

A key differentiator, Fortinet's custom-built FortiASIC content and network processors enable our flagship FortiGate systems to detect and eliminate even complex, blended threats in real time without degrading network performance, while an extensive set of complementary management, analysis, database and endpoint protection solutions increases deployment flexibility, assists in compliance with industry and government regulations, and reduces the operational costs of security management.

US Headquarters
1090 Kifer Road
Sunnyvale, CA 94086
USA
Tel: +1-408-235-7700
Fax: +1-408-235-7737