FORTINET

MACHINE LEARNING PUSHES FORTIWEB TO THE HEAD OF THE WAF CLASS

EXECUTIVE SUMMARY

As businesses rely increasingly on web applications and the threat landscape evolves and becomes more difficult to combat, web application firewalls (WAFs) have taken center stage in enterprise security architectures. But not every WAF offers security organizations the capabilities and scale needed. This is where FortiWeb distinguishes itself from the rest of the pack.

FortiWeb is a highly scalable and robust WAF solution that meets the security and operational requirements security organizations need. In particular, FortiWeb excels when it comes to using artificial intelligence (AI)-based machine learning to address zero-day attacks and known vulnerabilities. At the same time, this enables it to virtually eliminate false positives that plague other WAF solutions. It also seamlessly integrates into the Fortinet Security Fabric, enabling bi-directional threat intelligence sharing, including with FortiSandbox, and automation of security workflows and processes.

FORTIWEB EXCELS IN WAF FUNDAMENTALS

When it comes to the building blocks of web application security, FortiWeb WAFs stand out from the rest of the pack. In 2017, Gartner named Fortinet a “Challenger” in the WAF Magic Quadrant,[1] and NSS Labs described FortiWeb as a “market leader” and assigned it a “Recommended” rating.[2] Let’s recount some of the key reasons FortiWeb has received such recognition:

1. SIGNATURE-DETECTION ENGINE

Every stand-alone WAF offers a signature-detection engine, but the signature feed that FortiWeb WAFs use is unique. It is updated frequently and automatically with data from FortiGuard Labs, Fortinet’s world-class threat intelligence service. Moreover, FortiWeb WAFs can incorporate threat intelligence information from other devices plugged into the Fortinet Security Fabric, including FortiGate firewalls and certain third-party services.

2. ANALYZING THE SOURCE

At the same time, FortiWeb’s IP-reputation capabilities monitor the source of web application traffic. Specifically, FortiWeb compares a packet’s originating IP address against both a blacklist and whitelist that receive ongoing updates from FortiGuard Labs and other Security Fabric-enabled devices. FortiWeb also uses device fingerprinting to identify traffic sources and update the originator’s reputation risk score dynamically based on device behavior.

3. PROTOCOL VALIDATION

Protocol validation is another area where FortiWeb excels. Using protocol validation, FortiWeb confirms that all web application traffic conforms to HTTP RFC standards. This enables it to stop attacks that attempt to exploit weaknesses in web protocols.

KEY FEATURES OF FORTIWEB

- Sophisticated, dual-layer approach to machine learning, based on true artificial intelligence, that achieves optimal threat-detection accuracy while minimizing false positives
- Signature-detection engine that draws on FortiGuard Labs’ threat intelligence service and other devices in the Fortinet Security Fabric
- Dynamic IP-reputation checks using threat intelligence and FortiWeb device fingerprinting
- Award-winning antivirus engine
- Integration into Fortinet Security Fabric, facilitating deep sandboxing analysis of threat alerts
- Streamlined, integrated management for reduced administration and improved compliance

SOLUTION BRIEF

4. ANTIVIRUS ENGINE

Antivirus capabilities are a core requisite of a WAF. In the case of FortiWeb, it uses FortiGuard Labs' award-winning antivirus engine to scan traffic for any threat that might infect servers or other network devices.[3]

5. SCALABILITY AND PERFORMANCE

FortiWeb offers the fastest protected WAF throughput on the market.[4] In fact, FortiWeb's protected throughput can scale to 20 Gbps, double the advertised protected throughput of the next-fastest WAF. This best-in-class speed gives FortiWeb the scalability to address the ever-increasing volumes of web traffic.

6. SECURITY INTEGRATION

Other WAF solutions reside in silos and fail to integrate with the broader security architecture. This creates inefficiencies and inhibits their effectiveness, as they simply cannot keep pace with the advanced threat landscape that includes multi-vector and polymorphic attacks.

However, FortiWeb seamlessly integrates with the Fortinet Security Fabric. This reduces the time security and network teams spend compiling and interpreting manual security logs and other information. It also makes intrusion detection and prevention real-time. For example, when FortiWeb identifies a suspicious file attachment, it forwards it to FortiSandbox for closer inspection. Integration with leading third-party vulnerability scanners enables FortiWeb to provide dynamic virtual patches to security issues in application environments.

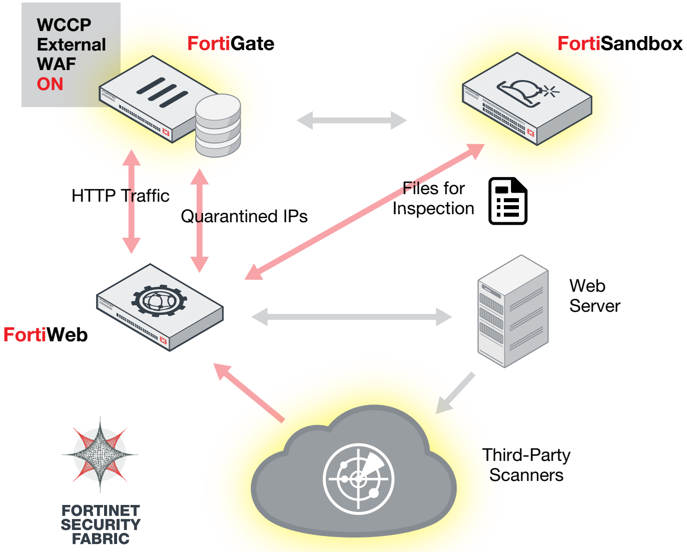

FIGURE 1: INTEGRATION WITH OTHER FORTINET SECURITY FABRIC ELEMENTS, INCLUDING FORTIGATE AND FORTISANDBOX, DELIVERS APPLICATION PROTECTION AND EXTENDS VULNERABILITY SCANNING WITH LEADING THIRD-PARTY PROVIDERS.

The AI-based machine-learning capabilities of FortiGuard Labs relies on **tens of thousands of known attacks** for behavioral analysis.

FortiWeb can scale to **20 Gbps protected throughput.** This is twice the advertised protected throughput of the next-fastest WAF.

FORTIWEB LEADS WAF MARKET WITH BEHAVIOR-DETECTION CAPABILITIES

Many WAF vendors offer application-learning-based behavioral threat detection, which is extremely basic.[5] These solutions compare web application traffic against observed patterns and alert every deviation from these norms. This approach, as a result, requires human investigation of every user or device behavior that the WAF has not specifically observed previously. This requires an inordinate amount of staff resources, which is a real challenge in an environment where security leaders already struggle to fill security openings due to a security skills shortage and are constrained due to budget limitations.[6] This can stretch already overburdened staff while heightening risk.

In this case, identifying all the true threats coming into protected web applications, while minimizing false positives, requires true AI-based machine learning. This is something available only in FortiWeb.

FortiWeb takes a multi-layer approach to behavior-detection technology. The first machine-learning layer builds a profile and mathematical model for each parameter in the protected web application. It monitors variations in each parameter, using data in multiple dimensions to rate the probability that a variation represents an anomaly.

Whenever a variation reaches a predetermined threshold on this probability scale, FortiWeb sends it to a second machine-learning layer to determine if it is a threat. The anomaly is compared against continuously updated threat models developed and curated by FortiGuard Labs. These models are based on analyses of tens of thousands of known attacks. They include syntax-based detection to identify SQL injection attacks, as well as machine-learning code specifically designed to recognize exploits in cross-site scripting, operating system injection, and more. And as the FortiGuard Labs team identifies new attacks, they automatically push threat-model changes to FortiWeb in real time.

This dual-layer approach minimizes false positives by ensuring that only true attacks are blocked rather than every single anomaly, as is the case with application-learning-based WAFs.

STREAMLINED MANAGEMENT AND REPORTING

FortiWeb also minimizes management requirements. While Akamai customers complain about a "longer-than-expected learning curve" and Barracuda Networks customers fret about its lack of alert aggregation,[7] FortiWeb requires virtually no resources to deploy and fine-tune. The Fortinet approach to WAF management is "set and forget."

This ease of use is enhanced by FortiWeb's advanced graphical analysis and reporting. Security managers can visualize and easily drill down into key elements of FortiWeb, such as server or IP configurations, attack and traffic logs, attack maps, and user activity. This means staff can achieve, at a glance, a much deeper understanding of threats to the organization's web applications and expend far fewer resources to reach those insights.

In addition, as a key element of the Fortinet Security Fabric, FortiWeb can integrate into a unified, organization-wide security management dashboard via FortiSIEM or FortiAnalyzer. This consolidated, real-time tracking and reporting model, which extends across every security area, enables security leaders to demonstrate compliance with industry and security standards—everything from the National Institute of Standards and Technology (NIST) 800 standards, to ISO 27001, to the Payment Card Industry Data Security Standard (PCI DSS).

FortiWeb can reduce total cost of ownership (TCO) per protected connection **by as much as 30%.**[8]

Identifying all the true threats coming into protected web applications, while minimizing false positives, **requires true AI-based machine learning.**

FortiWeb uses application-learning-based behavioral threat detection, which enables it to minimize false positives by **ensuring that only true attacks are blocked** rather than every single anomaly.

SUMMARY

By taking a comprehensive, correlated, multi-layer approach to web application security, FortiWeb protects web-based applications from all of the top 10 security risks as identified by the Open Web Application Security Project (OWASP).[9] In addition, compared with other WAFs, FortiWeb virtually eliminates false positives and achieves accuracy in the detection of both known and unknown exploits targeting web applications.

Plus, as traffic skyrockets and the volume, velocity, and sophistication of threats evolve and increase, FortiWeb, which delivers the fastest WAF-protected throughput on the market, provides a WAF solution that can easily scale and expand to meet these new challenges.

Its use of AI-based machine learning for behavioral threat detection, along with its integration with the Security Fabric, differentiates FortiWeb from all other competitive WAF solutions on the market. This enables security leaders to concurrently improve security efficiencies and effectiveness.

References:

[1] Jeremy D'Hoinne, Adam Hils, and Claudio Neiva, "Magic Quadrant for Web Application Firewalls," Gartner, August 7, 2017.

[2] "Web Application Firewall Group Test," NSS Labs, April 11, 2017.

[3] "AV-Comparatives Awards," accessed May 25, 2018.

[4] Based on published data contained in Fortinet and competitive data sheets.

[5] Jeremy D'Hoinne, Adam Hils, and Claudio Neiva, "Magic Quadrant for Web Application Firewalls," Gartner, August 7, 2017.

[6] Jon Oltsik, "Research suggests cybersecurity skills shortage is getting worse," CSO Online, January 11, 2018.

[7] Jeremy D'Hoinne, Adam Hils, and Claudio Neiva, "Magic Quadrant for Web Application Firewalls," Gartner, August 7, 2017.

[8] Based on Fortinet internal research.

[9] "OWASP Top 10 – 2017: The Ten Most Critical Web Application Security Risks," The OWASP Foundation, accessed May 25, 2018.

FORTINET®

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990