SOLUTION BRIEF

Managed Rules for AWS WAF

Advanced Supplemental Protection for Amazon Web Services (AWS) Web Application Firewall (WAF) Subscribers

Fortinet Managed Rules for AWS WAF are additional security signatures that can be used to enhance the protection of web applications running on Amazon Web Services (AWS). They are based on the FortiWeb web application firewall security service signatures, and are updated on a regular basis to include the latest threat information from the award-winning FortiGuard Labs.

There are multiple rule group options to choose from, starting with our entry-level SQL Injection (SQLi) and Cross-Site Scripting (XSS) rules to the Complete OWASP Top 10 package.

SQLi/XSS Rule Group

The SQLi/XSS Rule Group provides protection from the two primary web application attack types identified in the OWASP Top 10: SQL injection and cross-site scripting.

General and Known Exploits Rule Group

The General and Known Exploits Rule Group detects common and advanced OWASP Top 10 threats, including numerous injection attacks, Remote File Inclusion (RFI), Local File Inclusion (LFI), HTTP response splitting, database disclosure vulnerabilities, and other Common Vulnerabilities and Exposures (CVEs).

Malicious Bots Rule Group

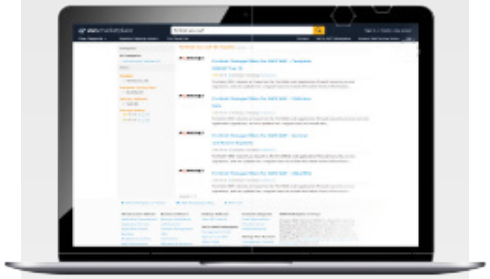
The Malicious Bots Rule Group analyzes requests and blocks known content scrapers, spiders looking for vulnerabilities, and other unwanted automated clients that OWASP has identified as risks to web applications.

Complete OWASP Top 10 Rule Group

The Complete OWASP Top 10 Rule Group combines Fortinet's other AWS WAF rulesets into one comprehensive package to help protect against the OWASP Top 10 web application threats. Included are the SQLi/XSS, General and Known Exploits, and Malicious Bots Rule Groups.

API Gateway Rule Group

The API Gateway Rule Goup defends against threats that target the AWS API Gateway and by extension your back-end applications. Unlike traditional application threats, APIs require specialized rules to help defend against the OWASP Top 10 application threats. Included in this ruleset are all the protections that Fortinet offers in the OWASP Top 10 Rule Group, however, they have been modified for the AWS API Gateway.



AWS WAF Overview

AWS WAF is a service available natively on AWS that helps you protect web applications from common web exploits. With this service, you can control web application traffic by implementing customizable security rules—all done in a matter of minutes. Users who want help managing and updating security rules can opt to leverage Fortinet Managed Rules for AWS WAF to bolster web application security.

Fortinet Managed Rules for AWS WAF Highlights

- Add-on to AWS WAF
- Additional layers of protection
- Updated automatically
- Little to no user intervention required

Highlights

Easy to Deploy and Manage

Fortinet's rule groups for AWS are exclusively available in AWS Marketplace. Once you subscribe to the rule group, you simply configure it through the AWS WAF console to take actions based on application requests that match or don't match the items in the rule group.

Via the AWS WAF console, you can view the attack logs to see which URL and source IPs have triggered rule group violations and what actions have been taken against the requests. Additional insights are available, including client information, rule ID, request line, and headers.

Secured by FortiGuard

Fortinet's award-winning FortiGuard Labs is the backbone for the Fortinet rule group signatures. As long as you're an active rule group subscriber, you automatically have the latest protections and updates without having to do anything further.

Order Information

Fortinet's AWS WAF Partner Rule Groups are available exclusively in AWS Marketplace.

Please visit the links below for more information on each rule group:

- Fortinet Managed Rules for AWS WAF – Complete OWASP Top 10
- Fortinet Managed Rules for AWS WAF – API Gateway
- Fortinet Managed Rules for AWS WAF – SQLi/XSS
- Fortinet Managed Rules for AWS WAF – General and Known Exploits
- Fortinet Managed Rules for AWS WAF – Malicious Bots

FORTINET | aws

www.fortinet.com

March 23, 2022 8:30 AM
1540412-A-0-EN