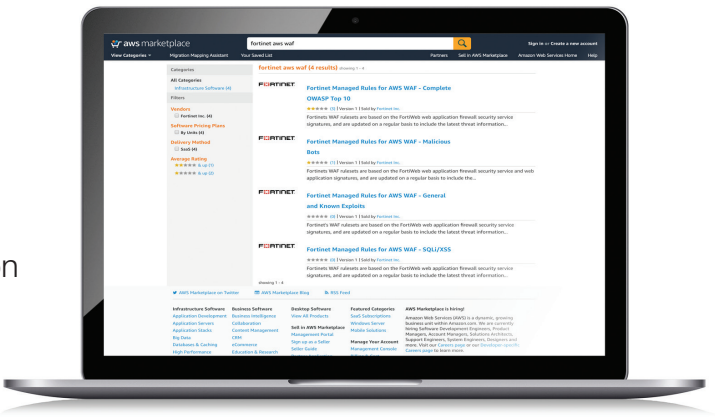
Managed Rules for AWS WAF

Advanced supplemental protection for AWS WAF subscribers

Fortinet's WAF rulesets are additional security signatures that can be used to enhance the protections included in the base AWS WAF product. 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 options to choose from starting with our entry-level SQL injection and cross-site scripting rules to the complete OWASP Top 10 package.

SQLi/XSS Rule Group

The SQLi/XSS Ruleset 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 ruleset 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 Ruleset 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 Ruleset combines Fortinet's other AWS WAF rulesets into one comprehensive package for the best web application protection offered by Fortinet to help protect against the OWASP Top 10 web application threats. Included are the SQLi/XSS, General and Known Exploits, and Malicious Bots rulesets.

Highlights

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

HIGHLIGHTS

API Gateway Rule Group

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

Easy to Deploy and Manage

Fortinet's rule groups for AWS are exclusively available via the 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 URIs 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 through the 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 – SQLi/XSS

Fortinet Managed Rules for AWS WAF – General and Known Exploits

Fortinet Managed Rules for AWS WAF – Malicious Bots

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
8 Temasek Boulevard
#12-01 Suntec Tower Three
Singapore 038988
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990

FST-PROD-DS-AWSWAF

AWS-WAF-DAT-R1-201811