SOLUTION OVERVIEW

F5 Managed Rules for AWS Web Application Firewall

Spend less time writing firewall rules and more time building applications with F5 managed rules for AWS WAF. Get started fast and protect your web applications or APIs against common threats–without the need for in-house security expertise.

KEY BENEFITS

Plug & Play
No security expertise needed—simply attach F5 WAF rules to your AWS Web App Firewall (WAF) or Application Load Balancer (ALB) to bolster your security posture.

Fast, Simple Deployment
Attach F5 WAF rules to your AWS WAF in a matter of minutes by following three simple deployment steps.

Extensive Protection
Augment your AWS WAF with a selection of four unique rulesets, each offering protection against specific application threats.

Continuous Updates
Rulesets are monitored, maintained, and updated by F5 security experts to ensure protection against evolving threats.

Pay As You Go
Add and remove rulesets as needed—no commitments or contracts; you simply pay for the rules you use on an hourly basis.

The Need for Enhanced Security in the Cloud

A recent report established that a staggering 52% of all data breaches were traced back to attacks on web applications[1], making these targeted attacks the single biggest cause of data breaches. When coupled with rapidly accelerating digital transformation efforts built around cloud-first and cloud-only strategies, the need for application protection in the cloud is clearer now than ever before.

However, not all applications are created equal. Different applications have different security requirements based on a number of factors, including business purpose, deployment location, sensitivity of user data, and regulatory requirements. For certain applications, the advanced functionality and protection offered by enterprise-grade web application firewalls such as F5® Advanced Web Application Firewall™ may not be required—at least not initially—and a cloud-native firewall like AWS Web Application Firewall (WAF) may be sufficient.

Thanks to its simple deployment, ease of use, and relatively inexpensive pricing model, thousands of organizations have taken this stance and deployed the AWS WAF to help protect their apps. To combat the growing complexity and sophistication of application layer threats, however, security teams now have the opportunity to strengthen their security posture through the AWS WAF support for managed rulesets.

F5 Managed Rules for AWS WAF

F5 Managed Rules for AWS WAF offer an additional layer of protection against a range of malicious threats and are easily applied to your AWS WAF instances. From bot and API protection, to defense against web exploits and common app vulnerabilities, these rulesets go above and beyond the AWS WAF protection to help keep your apps and data secure.

Protection provided by each of the four F5 rulesets includes:

- Bot Protection Ruleset—Analyzes all incoming requests and blocks any malicious bot activities including DDoS tools, vulnerability scanners, web scraper, and forum spam tools.
- OWASP Top 10 Web Exploits Protection Ruleset—Mitigates attacks that seek to exploit vulnerabilities contained in the OWASP Top 10, including cross-site scripting (XSS) attacks, injection attacks, and many more.

52% OF ALL DATA BREACHES WERE TRACED BACK TO ATTACKS ON WEB APPLICATIONS[1]

- API Attack Protection Ruleset—Secures against API-level attacks, as well as XML external entity attacks and server-side request forgery (SSRF), and offers support for both XML and JSON payloads and common web API frameworks.
- Common Vulnerabilities & Exposures (CVE) Protection Ruleset—Defends against high-profile CVEs that can be found in popular systems such as Apache, Java, MySQL, WordPress, and many more.

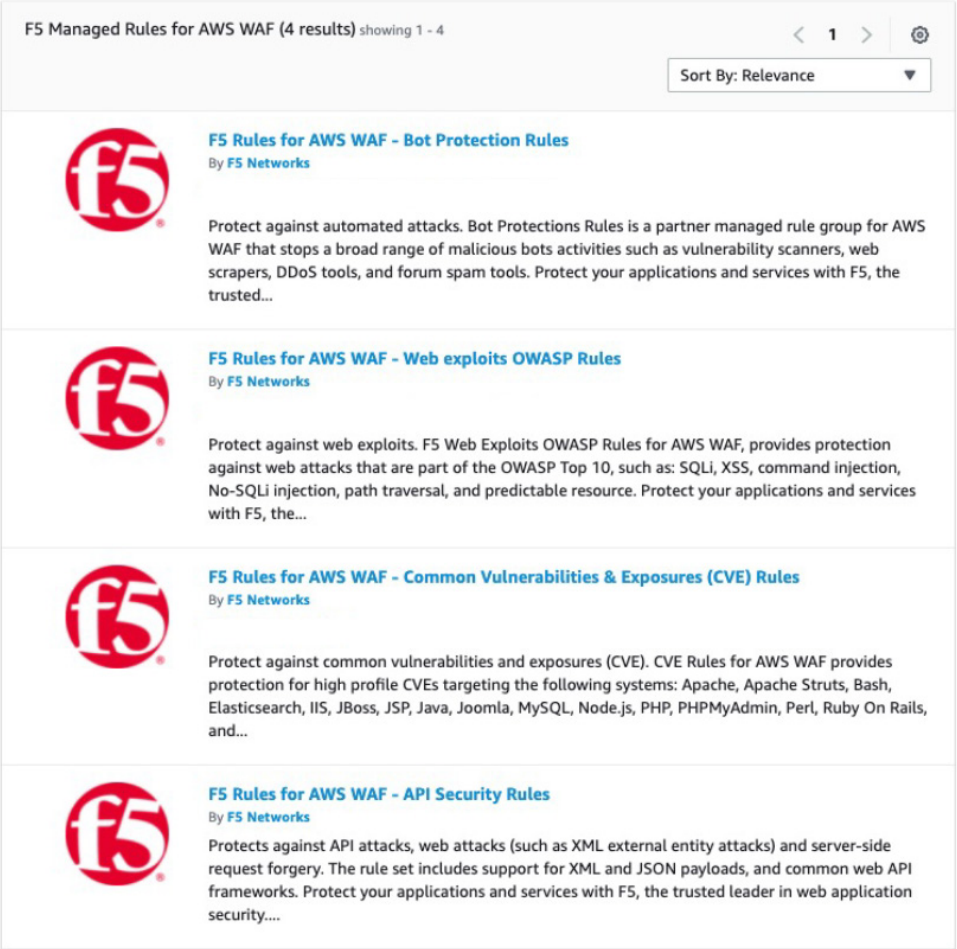

Figure 1: F5's Managed Rules for AWS WAF listings in AWS Marketplace.

Each ruleset is written, managed, and regularly updated by F5 security specialists to ensure your apps are protected against evolving threats—without the need for any intervention on your part. Whether they're applied to new or existing AWS WAF instances, F5 rulesets can be attached in minutes with just a few clicks of your AWS WAF console. Additionally, all F5 rulesets are licensed on a pay-as-you-go basis, so you'll only pay for what you use, with no contracts or commitments.

ADDITIONAL RESOURCES

Deployment Guide

AskF5 – Overview of F5 Rulesets for AWS WAF

The AWS WAF Managed Rules You Need to Deploy Now (Blog)

Deploying F5 Managed Rules for the AWS WAF

F5 Managed Rules for AWS WAF can be quickly and easily applied to new or existing AWS WAF instances in a matter of minutes. To do so, simply follow the steps below:

1. Identify the F5 ruleset(s) you wish to attach to your AWS WAF and navigate to its listing in AWS Marketplace. Links to each of the four managed rules are included below:
   - F5 Rules for AWS WAF - Common Vulnerabilities and Exposures (CVE)
   - F5 Rules for AWS WAF - Web exploits OWASP Rules
   - F5 Rules for AWS WAF - Bot Protection Rules
   - F5 Rules for AWS WAF - API Security Rules
2. Subscribe to the desired managed rules via the AWS Marketplace listing.
3. Associate the rules with your AWS WAF web ACL via the AWS WAF console.

Detailed, step-by-step deployment guidance can be found in AWS Marketplace, or you can watch this deployment demonstration video from one of F5's security solution engineers to see how you can easily attach F5 managed rules to an AWS WAF.

F5 MANAGED RULES FOR AWS WAF CAN BE QUICKLY AND EASILY APPLIED TO NEW OR EXISTING AWS WAF INSTANCES IN A MATTER OF MINUTES.

Should you have any questions or need assistance with any aspect of the F5 Managed Rules for AWS WAF, simply head over to the F5 technical community site, DevCentral, to sign in and ask a question. One of the F5 technical experts will get back to you within two working days in the event a member of our outstanding user community doesn't answer your query first.

To learn more, reach out to your F5 representative or F5 sales.

[1] The Verizon 2021 Data Breach Investigation Report (DBIR), found at https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/