F5 Advanced WAF

Product overview

F5® Advanced Web Application Firewall™ provides malicious bot protection, application-layer encryption, API inspection, and behavior analytics to help defend against application attacks.

F5’s proactive bot defenses stop automated attacks and leverage a combination of challenge- and behavior-based techniques to identify and filter out bot traffic. By stopping bad bots, you can eliminate many of these opportunistic attacks.

Advanced WAF includes F5 DataSafe to help encrypt data and credentials at the application-layer—without having to update the application. This encrypts the data as it passes through the Advanced WAF solution.

Behavior analytics are a requirement for detecting blended attacks. Many layer 7 distributed denial-of-service (DDoS) attacks are stealthy and may go undetected by traditional signatures and reputation-based solutions. Advanced WAF automatically learns the application behavior, then combines the behavioral heuristics of traffic with the server stress to determine DDoS conditions. This process provides the most accurate detection without false positives. Dynamic signatures are then created and deployed on the fly for real-time protection.

Product features

Proactive bot protection
Proactively defend your applications against automated attacks by bot and other attack tools. This prevents layer 7 denial of service (DoS) attacks, web scraping, and brute-force attacks. Proactive bot defense helps identify and mitigate attacks before they cause damage to the site.

DataSafe
Protect sensitive information from interception by encrypting data while it’s still in the browser. DataSafe encrypts data at the application layer to protect against malware and keyloggers. This renders leaked credentials or data useless.

Behavioral DoS
Behavioral DoS provides automatic protection against DDoS attacks by analyzing traffic behavior using machine learning and data analysis. By continuously monitoring server health and load, anomalies (performance slowdowns or traffic spikes) can be accurately detected and mitigated as needed.

Flexible deployment
Available as a purpose-built appliance, a cloud-ready virtual appliance, or part of the F5 Silverline service.

Key benefits:

- Protect your web applications from vulnerabilities and web attacks
- Identify and mitigate automated attacks by bots and other attack tools before they cause damage
- Identify attacks using machine learning to detect and mitigate attacks with the highest level of accuracy
How it works

F5 Advanced WAF in AWS protects against bots, credential attacks, and app-layer DoS

Solution available in AWS Marketplace