

Web Application Firewall (WAF)

NEXT GEN TECH TO STOP NEXT GEN ATTACKS

OVERVIEW

Attacks on web applications and servers are more complex and frequent than ever. Organizations continue to suffer costly data breaches using WAFs that still rely on signatures and pattern matching as their primary defenses; technologies that are easily evaded. And moving applications to the cloud does not make them any safer.

The NSFOCUS WAF uses next generation technologies to provide comprehensive application layer security, eliminating these problems and completely protecting your critical web applications. With full out-of-the-box protection against the OWASP Top Ten, the WAF is specifically engineered to protect not just web applications, but their underlying infrastructure, plug-ins, protocols, and more.

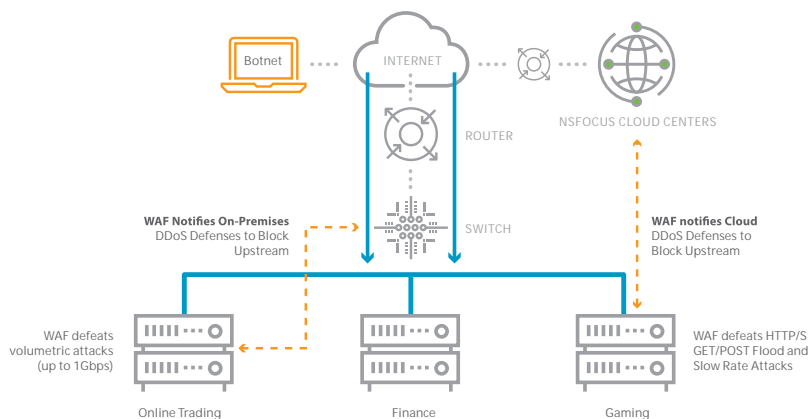
ADVANCED, INNOVATIVE TECHNOLOGY

The NSFOCUS WAF technology is powered by an internationally-recognized research lab and developed with over 10 years of experience protecting the world's largest banks, telecommunications, gaming, and 4. 7. The WAF uses Intelligent Detection™ advanced machine learning technology that is far superior for identifying web attacks and minimizing false positives/negatives than traditional positive and negative security models to deliver next-gen real-time web security.

SQLi	False Negative (based on 7442 payloads)	False Positive (based on 1458625 payloads)
Intelligent Detection	0.026874%	0.000745%
Signature-based Detection	0.604676%	0.342720%

COMPREHENSIVE, MULTI-LAYER SECURITY

The WAF serves as an essential part of a multi-layer security strategy by providing advanced inspection and specialized security for the web application layer. It also includes up to 1 Gbps of DDoS protection from volumetric layer 7 attacks, including TCP flood and HTTP/S GET/POST floods. When deployed together with higher capacity NSFOCUS on-premises or cloud Anti-DDoS Defenses, the WAF can direct traffic flows in real time to the ADS to keep your servers running under the most extreme DDoS attacks.



KEY BENEFITS

Eliminate costly data breaches

Reduce false positives to ensure business continuity

Simplify PCI compliance efforts

KEY FEATURES

Semantic analysis engine
 Semantic analysis and contextual logic-based attack detection identifies unknown threats and minimizes false positive and false negative

API security

API security detection and protection against API abuse

Patches for code vuln.

Integration with the 3rd-party code audit products and capability of providing patches for source code vulnerabilities

Hybrid management and solution

Open API configuration; on-premises and cloud management through centralized management platform; Integration with NSFOCUS on-prem & cloud DDoS solutions for ensuring performance during the largest DDoS attacks

Closed Loop vulnerability mitigation

Integration with NSFOCUS web scanner (WVSS) for fastest time for 0-day vulnerability mitigation by automatically creating virtual patching policies for most found vulnerabilities