DATASHEET

WAF

Web Application Firewall

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 on-premise and cloud WAF uses next generation technologies to provide comprehensive app 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 nut just web applications, but their underlying infrastructure, plug-ins, protocols, and more.

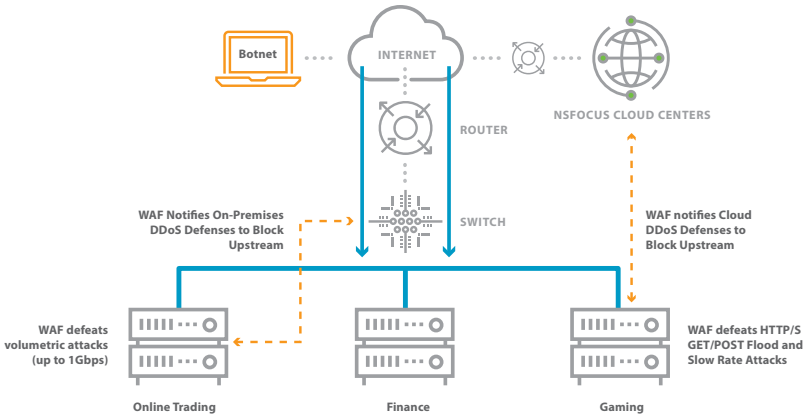
ADVANCED, INNOVATIVE TECHNOLOGY

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 social media companies. The WAF uses **Intelligent Detection**™ advanced machine learning technology (patent pending) 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 ADS 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.



WEB SECURITY MADE SMART AND SIMPLE

The NSFOCUS WAF is the ideal solution for safeguarding your critical web infrastructure whether on-prem or in the cloud. With Intelligent Detection, Smart Patch, Threat Intelligence and ADS anti-DDoS integration, the WAF delivers high quality application layer security for organizations of any size.

BENEFITS

Eliminate costly data breaches

Reduce false positives to ensure business continuity

Simplify PCI compliance efforts

KEY FEATURES

Comprehensive Protection
Full application layer transparent and reverse proxy for complete out-of-the-box OWASP Top Ten Protection

Best-in-Class HTTPS Performance
Transaction optimized appliances provide high HTTPS performance

Multi-Layered Hybrid Security
Integrates with NSFOCUS on-prem & cloud DDoS solutions for ensuring performance during the largest DDoS attacks

Closed Loop Vulnerability Mitigation
Integrates with NSFOCUS WVSS web scanner for fastest time for 0-day vulnerability mitigation by automatically creating virtual patching policies for most found vulnerabilities

SOFTWARE SPECIFICATIONS

Security Analysis

- Intelligent Detection™ next-gen advanced machine learning for lower false positive/negative rates identifying web attacks
- Automated False Positive Behavioral Analysis
- Positive behavior-based protection model with enhanced dynamic profile learning and whitelist security
- Negative signature-based model

Application Attack Prevention

- OWASP Top 10 including Cross-site Scripting (XSS), Cross Site Request Forgery (CSRF), Command & SQL Injection, API protection, Remote File Inclusion (RFI), Web Page Defacement, Malicious Scanning, and Botnet Protection

Virtual Machine & Cloud Support

- VMware, KVM
- AliCloud, AWS, Microsoft Azure (China), Softbank (Japan)

Web Server and Network Security

- Web server and app plug-in vulnerability modules, Layer 4 ACL and ARP spoofing protection

Anti-DDoS

- TCP flood, HTTP/S GET/POST floods (up to 1Gbps)

Certification

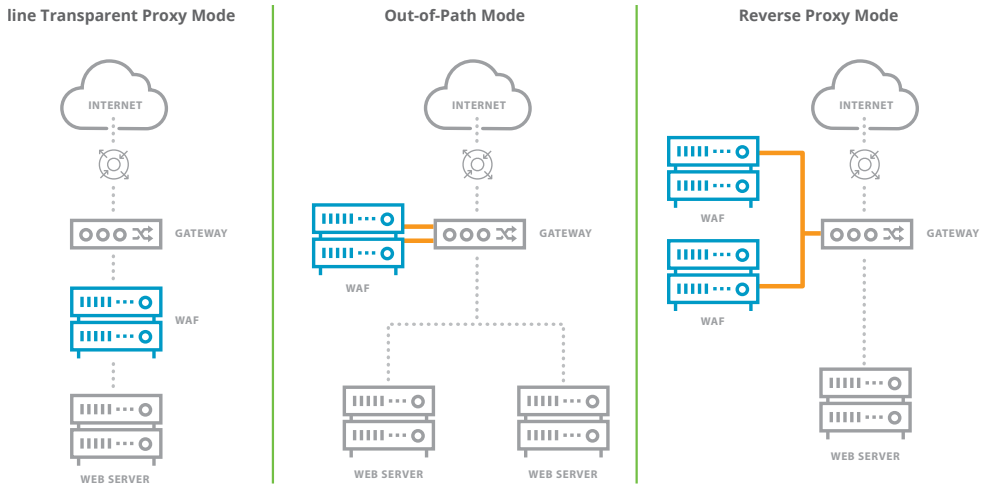
- Compliance reporting and support for PCI DSS 3.2
- ICSA certified
- Veracode VL4 certified

High Availability Configuration

- Active/active; active/passive; VRRP
- Internal "software" bypass to pass traffic without inspection (HW appliance)
- Fail-open hardware bypass NIC interfaces

DEPLOYMENT OPTIONS

Shown here are the most popular deployment options, with no changes to applications or networks



PERFORMANCE – CLOUD/VIRTUAL WAF

Hardware	WAF (C)V1000	WAF (C)V600	WAF (C)V300	WAF (C)V100
Application Layer Throughput	1 Gbps	500 Mbps	100 Mbps	50 Mbps
HTTP Transactions/sec (TPS)	25,000 TPS	10,000 TPS	2,000 TPS	1,000 TPS
HTTPS Transactions/sec (TPS)	3,000 TPS	2,000 TPS	2,000 TPS	1,000 TPS

PERFORMANCE – HARDWARE

Hardware	WAF 2020	WAF 1600	WAF 1000	WAF 600
Application Layer Throughput	6 Gbps	3 Gbps	1 Gbps	500 Mbps
HTTP Transactions/sec (TPS)	110,000 TPS	55,000 TPS	25,000 TPS	10,000 TPS
HTTPS Transactions/sec (TPS)	35,000 TPS	9,000 TPS	9,000 TPS	2,000 TPS