# NSFOCUS

# 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 20 years of experience protecting the world's largest banks, telecommunications, gaming, and SMBs. 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.
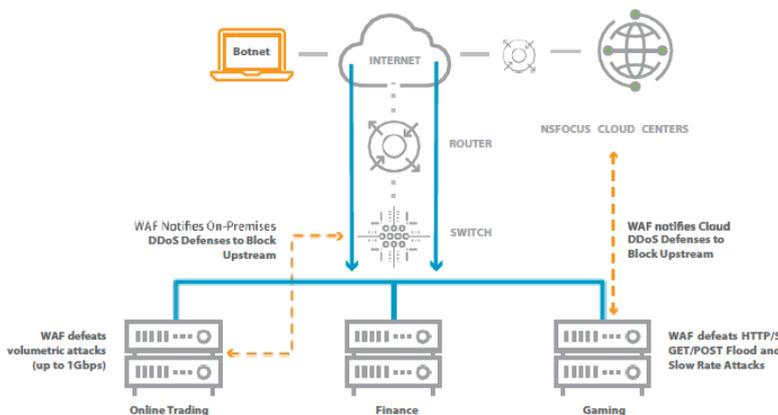


### KEY BENEFITS

**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 identify unknown threats and minimize false positive and false negative

**API security**
API security detection and protection against API abuse

**Patches for code vulnerabilities.**
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-prems & cloud DDoS solutions for ensuring performance during the largest DDoS attacks

**Dynamic Bot Attack Protection**
Detect and block malicious bots from automatically scanning and attacking websites

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

## 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 Anti-DDoS System, the WAF delivers high quality application layer security for organizations of any size.

## 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
» Cross Site Request Forgery (CSRF)
» Cross-site Scripting (XSS)
» Command & SQL Injection
» Remote File Inclusion Protection
» Malicious Scanning
» Botnet Protection
» XML Attack Protection
» Cookie Signing and Encryption
» URL Access Control
» Web Scraping Protection
» File Upload and Download Control

» LDAP Injection Protection
» Server-Side Includes (SSI) Injection Protection
» xPath Injection Protection
» Path Traversal Protection
» Webshell Protection
» Anti-Leeching/Anti-Phishing
» Response control
» Outbound Data Theft Protection to secure personal privacy information such as credit card, social security number, and ID
» Buffer Overflow Protection
» Data Loss Protection

### Web Server and Network Security
» Web server cloaking
» Server extension security
» Network-layer ACLs
» ARP spoofing protection
» Real-time server status monitoring to ensure server availability

» 802.1Q support
» Cookie Poisoning Protection
» VLAN decode
» Protection in Trunk
» Protection in Port-channels

### DDoS Protection
» TCP Flood (SYN Flood/ACK Flood)
» HTTP/S GET/POST Flood (Up to 1 Gbps)
» Low-and-Slow Attacks

» Brute Force Protection
» Integration with external Anti-DDoS products
» Integration with cloud based Anti-DDoS products

### Security Services
» Content Filtering
» Sensitive Information Filtering
» IP Reputation
» Geo IP location
» Virtual patching
» Customized policies and rules

» Risk level policies
» Client IP-address tracking
» Exception control
» Base64 decode
» False positive analysis and automatic/manual adjustment

### Supported Web Protocols
» HTTP/HTTPS
» XML/SOAP
» WebSocket

» HSTS
» IPv4/IPv6 full stack (IPv4, IPv6 or hybrid)

### Application Delivery
» HTTPS/SSL Offloading
» HTTP Compression to compress textual content transferred from web servers to browsers.
» Layer 7 Server Load balancing

» Catching
» Web Page Defacement Protection
» Page prefetch
» Offline Server Takeover

## High Availability Configuration

» Active/Active
» Active/Passive
» VRRP
» Internal "Software" bypass to pass traffic without inspection (HW appliance)
» Fail-open hardware bypass NIC interfaces
» Emergency Mode based on thresholds of new connections, use of CPU and use of memory

## Management and Reporting

» Secure web-based GUI
» SSH-based CLI access network management
» SNMP
» Syslog-based logging
» REST API
» Built-in test tools
» Packet capture
» Real-time dashboard

» PCI-DSS compliance reporting
» Centralized logging and reporting
» Custom templates
» Central management for multiple NSFOCUS devices
» Session tracking and forensics
» Geo IP analytics and blocking
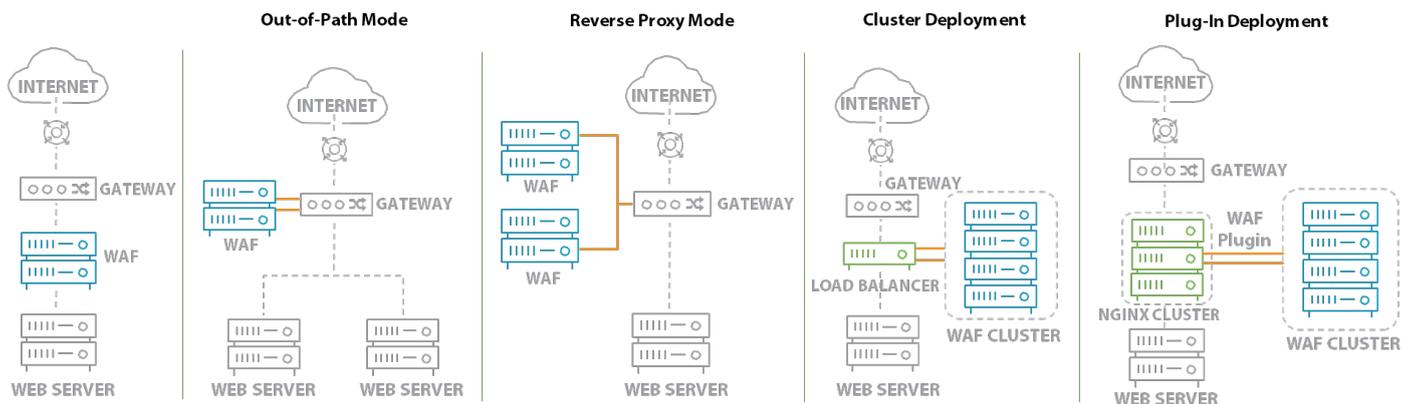
## Virtual Machine & Cloud Support

» VMware, KVM
» AWS, Microsoft Azure (China), AliCloud, HUAWEI, ZTE, Wo Cloud, Softbank (Japan), OpenStack

## Certification

» Veracode VL4 Certified

## DEPLOYMENT OPTIONS

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



Out-of-Path Mode     Reverse Proxy Mode     Cluster Deployment     Plug-In Deployment

## HARDWARE SPECIFICATIONS

| | | WAF 300 | WAF 600 | WAF 800 |
|---|---|---|---|---|
| **Ethernet Interface** | Gigabit Ethernet Ports | 4 * GE RJ45 bypass port | 4 * GE RJ45 bypass port | 4 * GE RJ45 bypass port |
| | Expansion Slot | 1 | 1 | 1 |
| | Optional Network Interface Modules for Extension Slot | 4 * GE SFP interface<br>4 * GE multi-mode SFP interface<br>4 * GE RJ45 bypass port | 4 * GE SFP interface<br>4 * GE multi-mode SFP interface<br>4 * GE RJ45 bypass port | 4 * GE SFP interface<br>4 * GE multi-mode SFP interface 4 * GE RJ45 bypass port<br>2 * 10 GE SFP + interface |
| **Management Interface** | Management Port | 1 * RJ45 | 1 * RJ45 | 1 * RJ45 |
| | Serial Port | 1 * RJ45 | 1 * RJ45 | 1 * RJ45 |
| | USB Interface | 2 | 2 | 2 |
| **Memory** | Memory | 8G | 8G | 8G |
| **Storage** | Hard Disk | 1T, SATA | 1T, SATA | 1T, SATA |
| **Performance** | Network-layer Throughput (RFC 2544) | 2000 Mbps | 2400 Mbps | 2800 Mbps |
| | Latency (RFC 2544) | <150 μs | <150 μs | <150 μs |
| | HTTP Throughput | 200 Mbps | 400 Mbps | 800 Mbps |
| | HTTP Transactions Per Second | 10,000 TPS | 15,000 TPS | 20,000 TPS |
| | HTTP Connections Per Second | 3,000 CPS | 5,000 CPS | 8,000 CPS |
| | Max. Number of Concurrent Connections | 80,000 | 110,000 | 150,000 |
| | HTTPS Transaction Per Second (1KB) | 4,000 TPS | 6,000 TPS | 8,500 TPS |
| **Physical** | Form Factor | 1U | 1U | 1U |
| | Dimensions (in) (W x H x D)" | 17.0x1.7x15.4 | 17.0x1.7x15.4 | 17.0x1.7x15.4 |
| | Weight | 5.2kg/11lbs | 5.2kg/11lbs | 5.2kg/11lbs |
| | Power Supply | Redundant power supplies | Redundant power supplies | Redundant power supplies |
| | AC Input (Amps) | 2A | 2A | 2A |
| | Voltage | 100-240V 50-60 Hz | 100-240V 50-60 Hz | 100-240V 50-60 Hz |
| | Mean Time Between Failure (MTBF) | Over 100,000 hours | Over 100,000 hours | Over 100,000 hours |
| | Heat Output (BTU/Hr) | 222 | 222 | 222 |
| | Operating Temperature | 0°C-40°C (32°F-104°F) | 0°C-40°C (32°F-104°F) | 0°C-40°C (32°F-104°F) |
| | Storage Temperature | -20°C-70°C (-4°F-158°F) | -20°C-70°C (-4°F-158°F) | -20°C-70°C (-4°F-158°F) |
| | Operational Relative Humidity | 5% - 95% (non-condensing) | 5% - 95% (non-condensing) | 5% - 95% (non-condensing) |

| | | WAF 1000 | WAF 1600 | WAF 4000 | WAF 6000 |
|---|---|---|---|---|---|
| **Ethernet Interface** | Gigabit Ethernet Ports | 6-port GE RJ45 interface card (bypass); 4-port GE SFP interface card (Transceiver not included) | – | – | – |
| | Expansion Slot | 2 | 4 | 4 | 4 |
| | Optional Network Interface Modules for Extension Slot | 8 * 10/100/1000M RJ45 coppers and 4-path built-in bypass<br><br>4 * GE multi-mode SFP interface<br><br>2 * 10GE SFP+ (bypass/non-bypass) | 4 * GE SFP (bypass/non-bypass)<br>8 * GE SFP (non-bypass)<br>2 * 10GE SFP+ (bypass/non-bypass)<br>4 * 10GE SFP+ (bypass/non-bypass)<br>4 * 10/100/1000M RJ45 copper with bypass.<br>8 * 10/100/1000M RJ45 copper with bypass. | 4 * GE SFP (bypass/non-bypass)<br>2 * 10GE SFP+ (bypass/non-bypass)<br>4 * 10GE SFP+ (bypass/non-bypass)<br>4 * 10/100/1000M RJ45 copper with bypass.<br>8 * 10/100/1000M RJ45 copper with bypass. | 4 * GE SFP (bypass/non-bypass)<br>2 * 10GE SFP+ (bypass/non-bypass)<br>4 * 10GE SFP+ (bypass/non-bypass)<br>4 * 10/100/1000M RJ45 copper with bypass.<br>8 * 10/100/1000M RJ45 copper with bypass. |
| **Management Interface** | Management Port | 2 * GE | 2 * GE | 2 * GE | 2 * GE |
| | Serial Port | 1 * RJ45 | 1 * RJ45 | 1 * RJ45 | 1 * RJ45 |
| | USB Interface | 2 | 2 | 2 | 2 |
| **Memory** | Memory | 16G | 8G | 32G | 128G |
| **Storage** | Hard Disk | 1T, SATA | 1T, SATA, up to 4T, SATA | 1T, SATA, up to 4T, SATA | 1T, SATA, up to 4T, SATA |
| **Performance** | Network-layer Throughput (RFC 2544) | 4 Gbps | 6 Gbps | 8 Gbps | 20 Gbps |
| | Latency (RFC 2544) | <60 μs | <50 μs | <50 μs | <20 μs |
| | HTTP Throughput | 1 Gbps | 3 Gbps | 6 Gbps | 10 Gbps<br>18Gbps (Transparent mode only) |
| | HTTP Transactions Per Second | 30,000 TPS | 55,000 TPS | 110,000 TPS | 450,000 TPS<br>500,000 TPS (Transparent mode only) |
| | HTTP Connections Per Second | 10,000 CPS | 20,000 CPS | 38,000 CPS | 110,000 CPS<br>250,000 CPS (Transparent mode only) |
| | Max. Number of Concurrent Connections | 500,000 | 175,000 | 1,100,000 | 4,000,000 |
| | HTTPS Transaction Per Second (1KB) | 15,500 TPS | 15,500 TPS | 20,000 TPS | 68,000 TPS |
| **Physical** | Form Factor | 2U | 2U | 2U | 2U |
| | Dimensions (in) (W x H x D)" | 17.0 x 3.5 x 22.6 | 17.0 x 3.5 x 22.6 | 17.0 x 3.5 x 22.6 | 24.6 x 3.5 x 17.4 |
| | Weight | 12.7kg/27.9lbs | 16kg/35.2lbs | 16kg/35.2lbs | 16.5kg/36.3lbs |
| | Power Supply | Redundant power supplies | Redundant power supplies | Redundant power supplies | Redundant power supplies |
| | AC Input (Amps) | 8-5A | 4.5-2A | 8-5A | 7-3A |
| | Voltage | 100-240V<br>50-60 Hz | 100-240V<br>50-60 Hz | 100-240V<br>50-60 Hz | 100-240V<br>50-60 Hz |
| | Mean Time Between Failure (MTBF) | Over 100,000 hours | Over 100,000 hours | Over 100,000 hours | Over 100,000 hours |
| | Heat Output (BTU/Hr) | 1194 | 1365 | 1365 | 1706 |
| | Operating Temperature | 0°C-40°C (32°F-104°F) | 0°C-40°C (32°F-104°F) | 0°C-40°C (32°F-104°F) | 0°C-40°C (32°F-104°F) |

| | Storage Temperature | -20°C-70°C (-4°F-158°F) | -20°C-70°C (-4°F-158°F) | -20°C-70°C (-4°F-158°F) | -20°C-70°C (-4°F-158°F) |
|---|---|---|---|---|---|
| | Operational Relative Humidity | 5%-95% (non-condensing) | 5%-95% (non-condensing) | 5%-95% (non-condensing) | 5%-95% (non-condensing) |

## VM SPECIFICATIONS

| | (C)V1000 | (C)V500 | (C)V200 | (C)V100 | (C)V50 |
|---|---|---|---|---|---|
| **HTTP Throughput** | 1 Gbps | 500 Mbps | 200 Mbps | 100 Mbps | 50 Mbps |
| **Hypervisor** | QEMU-KVM 1.2.8 VMware vSphere ESXi 5.0/5.5/6.0 | | | | |
| **Minimal Environment Requirements** | | | | | |
| **CPU Cores** | 8 | 8 | 4 | 4 | 4 |
| **Memory (Min.)** | 32G | 16G | 8G | 4G | 4G |
| **Storage (Min.)** | 100G | 100G | 100G | 100G | 100G |
| **Performance** | | | | | |
| **HTTP Transactions Per Second (TPS)** | 75,000 TPS | 75,000 TPS | 50,000 TPS | 50,000 TPS | 50,000 TPS |
| **Connections Per Second (CPS)** | 26,000 CPS | 26,000 CPS | 20,000 CPS | 20,000 CPS | 20,000 CPS |
| **Max. Number of Concurrent Connections** | 1,000,000 | 500,000 | 250,000 | 100,000 | 100,000 |
| **HTTPs Transactions Per Second (TPS)** | 26,000 TPS | 26,000 TPS | 18,000 TPS | 18,000 TPS | 18,000 TPS |

*The performance data is obtained when using Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz.*