DATA SHEET

WEB APPLICATION FIREWALL (WAF)

PROTECT APPLICATIONS, CRITICAL DATA, RESOURCE UPTIME

OVERVIEW

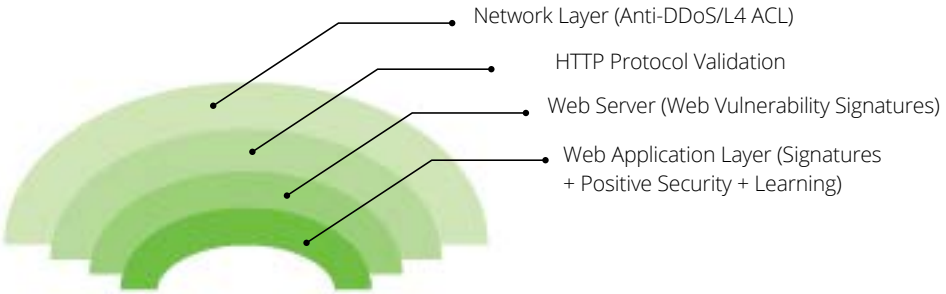
Attacks on web-based applications and servers are more complex and frequent than ever. Despite significant investment in perimeter security solutions, many organizations continue to experience costly data breaches and service disruptions. The NSFOCUS Web Application Firewall (WAF) provides comprehensive, application layer security to eliminate these problems and completely protect your critical servers and web applications. It provides full protection from the top 10 threats identified by the Open Web Application Security Project (OWASP), and has been specifically designed to protect web applications and their underlying infrastructure, including servers, plug-ins, protocols, network connectivity, and more.

ADVANCED, INNOVATIVE TECHNOLOGY

The NSFOCUS WAF includes technology 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 an innovative combination of positive and negative security models, as well as application profile learning, to deliver real-time application-layer security.

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 other volumetric and application layer attacks, including TCP flood and HTTP/S GET/POST floods. Additionally, if deployed in conjunction with a higher capacity NSFOCUS On-Premises Defenses, the WAF can direct flows in real-time to the ADS to keep your servers running under the most extreme conditions.



SIMPLE TO DEPLOY

WAF provides flexible deployment options with low overhead. One of the most common options is the drop-in transparent deployment without changes to existing applications or networks. Reverse proxy and out-of-path (traffic diversion and injection) options, which provide protection on demand, are available as well.

PERFORMANCE, QUALITY, VALUE

The NSFOCUS WAF is the ideal solution for safeguarding your critical servers, web applications and data. Available in a range of cost and performance optimized appliances, they are purpose-built to deliver high quality application layer security for organizations of any size.

NSFOCUS

BENEFITS

Eliminate costly data breaches

Ensure business continuity and website availability

Simplify PCI compliance efforts

KEY FEATURES

Comprehensive Protection
Full application layer protection, including protection from OWASP top 10 web security risks, zero-day exploits and more

Best-in-Class Performance
Performance optimized appliances provide real-time protection for any size organization

Multi-Layered Security
Hybrid DDoS and web application security for complete protection of your web-based assets

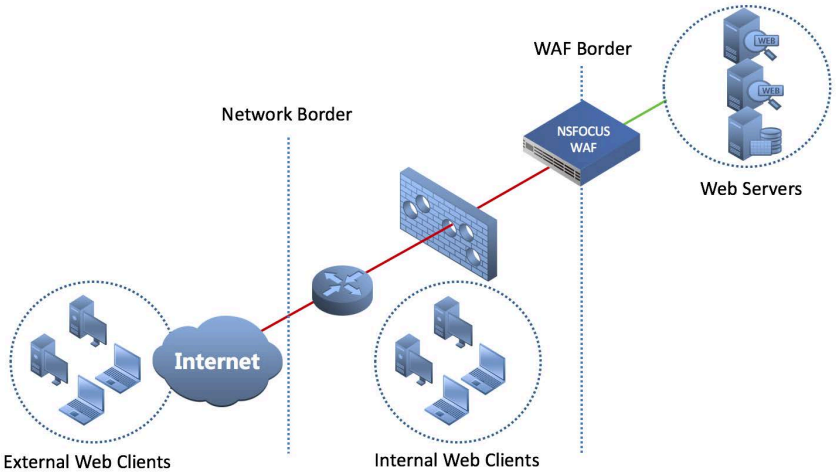
Collaborative Security Model
Integrates with NSFOCUS WVSS web scanner to automatically create "virtual" patching policies for most found vulnerabilities

SPECIFICATIONS - SOFTWARE

- **Security Models**
  - Negative, signature-based
  - Positive, with whitelist security and dynamic profile learning - Behavior-based protection
- **Application Attack Prevention**
  - OWASP Top 10, Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF), Injection, Remote File Inclusion (RFI), Illegal file upload and download restriction, Malicious Scanning, Webshell and Anti-Crawlers
- **Web Server and Network Security**
  - Web server and plug-in vulnerability signatures - Layer 4 ACL and ARP spoofing protection
- **Virtual Machine Support**
  VM and VMware ESX server
- **Anti-DDoS**
  - TCP flood (up to 1Gbps), HTTP/S GET/POST floods
- **Certification and PCI DSS Compliance**
  - Compliance reporting and support for PCI DSS 3.2
  - ICSA
  - Veracode VL4
- **High Availability Configuration**
  - Active/active; active/passive; VRRP
  - Internal "software" bypass to pass traffic without inspection
  - Hardware fail-open or integrated hardware bypass interfaces

DEPLOYMENT OPTIONS

Shown here is the most popular drop-in transparent deployment option, with no changes to applications or networks



SPECIFICATIONS - VIRTUAL WAF

Hardware	WAF V1000	WAF V600	WAF V300
Application Layer Throughput	1 Gbps	500Mbps	100Mbps
Txns per Second (TPS) Performance	25,000 TPS	10,000 TPS	2,000 TPS

SPECIFICATIONS - WAF APPLIANCE

Hardware	WAF 2000	WAF 1600	WAF 1000	WAF 600
Application Layer Throughput	6 Gbps	3 Gbps	1 Gbps	400 Mbps
Txns per Second (TPS) Performance	110,000 TPS	55,000 TPS	30,000 TPS	10,000 TPS
Interfaces	4 options slots (4 x 10/100/1000 BaseT, 4 x GE SX or 4 x GE LX Fiber)	4 options slots (4 x 10/100/1000 BaseT, 4 x GE SX or 4 x GE LX Fiber)	6 x 10/100/1000 BaseT (copper) One option slot	4 x 10/100/1000 BaseT (copper)
Management Interface	1 x 10/100/1000 BaseT (copper)	1 x 10/100/1000 BaseT (copper)	1 x 10/100/1000 BaseT (copper)	1 x 10/100/1000 BaseT (copper)
Dimensions (WxDxH)	22.6"x17"x3.5" 2 RU	22.6"x17"x3.5" 2 RU	22.6"x17"x3.5" 2 RU	17"x15.4"x1.7" 1 RU
Weight	24 lbs (11 kg)	24 lbs (11 kg)	28 lbs (12.6 kg)	11 lbs (5 kg)
Environmental	Operating: 32-104° F (0-40° C)	Operating: 32-104° F (0-40° C)	Operating: 32-104° F (0-40° C)	Operating: 32-104° F (0-40° C)
Power	Dual AC Power Supply 100~240 V (400W total)	Dual AC Power Supply 100~240 V (400W total)	Dual AC Power Supply 100~240 V (350W total)	Single AC Power Supply 100-240 V (60W)