信安世纪 Infosec

NetWAF Application Security Firewall

DATASHEET

NetWAF Series application security firewall provides enterprise-grade Web Application Firewall (WAF) and Distributed Denial of Service (DDoS) mitigation solutions, helping protect the critical services of the enterprise data center against the OWASP Top 10 Web attacks, information leakage, Denial of Service (DoS) attacks, DDoS attacks and other security threats.

Infosec NetWAF Series providing comprehensive detection and defense against attacks and threats for business-critical applications. Combined the negative and positive WAF models together, Infosec NetWAF Series can not only detect and block latest known attacks and security vulnerabilities, but also effectively prevent “Zero-day” attacks. NetWAF Series provide granular attack defense control, support automatic learning and dynamic refreshing of defense profiles, and enhance the attack detection accuracy through client source verification mechanisms.

Highlights And Benefits

- As Next-generation Web Application Firewall, NetWAF Series provide multi-layer security defense for business-critical servers and applications.
- Combined the negative and positive WAF models together, NetWAF Series can not only detect and block latest known attacks and security vulnerabilities, but also effectively prevent “Zero-day” attacks.
- NetWAF Series have integrated a sophisticated attack signature library, which can prevent a wide range of attacks, such as SQL injection, PHP injection, XSS, command execution, network crawler/scanner, CSRF, leech, Webshell, sensitive data leakage, Highlightsand Advantages session hijacking and protocol violation.
- NetWAF Series provide Layer 3 to Layer 7 defense for Web servers, including enterprise-grade DDoS mitigation, advanced network access control, whitelist and blacklist, HTTP protocol compliance checks, cookie tampering defense, brute force defense, anti-leech, anti-crawling/scanning, and packet anomaly checks.
- NetWAF Series support customized attack signatures and flexible deployment modes/defense models, meeting the requirements of various complicated Web applications.
- NetWAF Series provide a configuration wizard to help quickly build the defense profile based on application characteristics, which reduces the configuration complexity and provisions accurate defense capability.
- NetWAF Series provide positive WAF to automatically learn the normal traffic to form positive whitelist and refresh the WAF profile dynamically.
- NetWAF Series provide the traffic baseline learning function to dynamically refresh the rule and option settings of automatic DDoS profiles based on learning results, which simplifies the configuration and enhances the defense accuracy.
- NetWAF Series support Data Leak Protection (DLP) rules, which can prevent the user’s private or sensitive information, such as identity information, mobile phone number, email address, credit card number, from being exposed.
- NetWAF Series support the virtual patching function, which can convert the scanning results of thirdparty Web vulnerability scanner (IBM AppScan) into executable security policies (called “Virtual Patch”) and thus reduces the risks caused by vulnerabilities to customers.
- NetWAF Series support the Web Anti-defacement (WAD) feature to detect the defacement attacks against Web pages in realtime and recover the normal pages when defacement occurs, which protects the customer’s public image.
- NetWAF Series provide abundant events logs to help replay attacks and conduct auditing, and support exporting of event logs for external analysis.
- NetWAF Series provide granular and intuitive graphic monitoring function, which enables the monitoring of the system status, attacks, traffic and packet drops.

- NetWAF Series provide monitoring reports, advanced service security reports and PCI DSS compliance reports, and support periodic report generation and report customization.
- NetWAF Series provide role-based administrative privilege control, support external authentication and authorization, and provide administrator audit logs.
- NetWAF Series support the software and hardware bypass function, which can help avoid service interruption (such as software or hardware fault) caused by a failure of a single NetWAF device.
- NetWAF Series provide industry-leading ECC performance and RSA 2048/4096-bit SSL performance.
- NetWAF Series provide comprehensive IPv6 support, helping solving the problem of IPv4 address exhaustion and promoting the migration to IPv6 adoption.
- NetWAF Series support XML-RPC and eCloud™ RESTful API, which allow them to integrate Cloud management systems and third-party monitoring and management platforms seamlessly.
- NetWAF Series employ 64-bit SpeedCore™ multi-core processing architecture, providing industry-leading performance, and support seamless integration with hardware and virtual appliances.
- NetWAFSeries allow up to 32 hardware or virtual appliance to operate as a N+1 cluster, which provides industry-leading high availability and scalability.
- NetWAF Series use space-efficient, redundant-power hardware appliances that consume 10-35% less power versus alternative solutions.
- NetWAF Series provide easy-to-use CLI and intuitive WebUI for ease of use and configuration.

Product Function Description

Next-generation Web Application Firewall

As applications have increasingly moved to the Web, the servers that host critical business applications have become targets of malicious attacks, tampering and other security incidents that can compromise intellectual property, customer information and other sensitive business data, which cause huge economic and reputation damages.

Infosec'sNetWAF Series application security firewalls protect against the most widespread attack mechanisms while providing active incident response to halt hackers in their tracks, with post-incident analysis and diagnosis to provide guidance for strengthening servers against future attacks.

NetWAF Series adopt an architecture that combines the positive and negative WAF models to allow them provide defense for Web applications at the same time. The negative WAF model defends against the latest known Web attacks by upgrading Infosec Signature Library from time to time to support the signatures of latest attacks. The positive WAF model learns the characteristics of normal traffic and dynamically refreshes the defense profile, thus halting various kinds of complicated and unknown Web attacks effectively.

Infosec's NetWAF Series support the virtual patching function, which can convert the scanning results of third-party Web vulnerability scanner (IBM AppScan) into executable security policies (called "Virtual Patch") and thus reduces the risks caused by vulnerabilities to customers.

Enterprise-grade DDoS Mitigation

NetWAF Series can mitigate Layer 3 to Layer 7 DDoS attacks in the OSI network model. They can automatically generate defense rules suitable for customers' existing network by learning their traffic baseline, and support multiple source verification mechanisms such as CAPTCHA, session tracking, anti-scraping and various attack sources and legitimate sources to achieve fast response and accurate defense against BOT. The Layer 3 to Layer 7 DDoS attacks mitigated by NetWAF Series include but not limited to:

- HTTP GET Flood attack
- HTTP POST Flood attack
- HTTP Slowloris attack
- HTTP Slow Post attack
- HTTP ChallengeCollapsar (CC) attack
- HTTP Packet Anomaly attacks
- SSL Handshake attack
- SSL Renegotiation attack
- SSL Packet Anomaly attacks
- DNS Query Flood attack
- DNS Reply Flood attack
- DNS NXDomain Flood attack
- DNS Cache Poisoning attack
- DNS Packet Anomaly attacks
- TCP SYN Flood attack
- TCP SYN-ACK Flood attack
- TCPACK Flood attack
- TCP FIN/RST Flood attack
- TCP Connection Exhaustion attack
- TCP Fragment Flood attack
- TCP Slow Connection attack
- TCP Abnormal Connection attack
- UDP Flood attack
- UDP Fragment Flood attack
- TCMP Flood attack
- Smurf, Ping of Death, LAND, IP Spoofing, Teardrop, Fraggle, Winnuke, Tracert and other malformed single-packet attacks

Flexible Deployment Options

NetWAF Series provide flexible deployment options to meet various customer network situations. NetWAF Series support the following deployment modes:

• Bridge transparent mode: NetWAF connects the network transparently on layer 2. The administrator does not need to change any configuration of the network. Besides, this mode supports the Bypass function, but does not support HTTPS application defense.

• Bridge proxy mode: NetWAF connects the network transparently on layer 2. The administrator needs to modify the network's NAT/Route configurations or DNS resource records to direct the application traffic to the virtual service IP to make sure that the application traffic passes through the NetWAF appliance physically.

• Routing transparent mode: NetWAF connects the network on layer 3. The administrator needs to draw the requests and responses ofthe application traffic to the Uplink and Downlink interfaces respectively.

• Routing proxy mode: NetWAF connects the network transparently on layer 3. The administrator needs to modify the network's NAT/Route configuration or DNS resource records to draw the application traffic to the virtual service IP.

• Out-of-path TAP mode: The NetWAF appliance is deployed out of the traffic path. The administrator needs to configure a port mirroring policy on the switch that NetWAF connects to copy the traffic to the NetWAF appliance for detection. This mode only detects attacks but does not block attacks. In addition, it does not support HTTPS application defense.

Multi-stage Security Handling

• Before a security incident occurs, Web vulnerabilities scanners are used to scan the applications and scanning results can be quickly converted to executable security policies (called "Virtual Patch"), thus reducing the risks caused by vulnerabilities to customers.

• During a security incident, the NetWAF Series enforce the defense profiles to detect and block attacks in real time and record detailed audit logs, including suspicious request data and all related interaction data.

• After a security incident, administrators can analyze logs and statistics to tune the defense profiles so as to enhance the defense accuracy and efficiency.

Sophisticated Signature Library

NetWAF Series have integrated the Attack Signature Library (ASL) regularly released by Infosec Security Center (ASC). This library includes the predefined signatures of latest known Web attacks, including but not limited to SQL injection, PHP injection, XSS, Crawlers/Scanners, CSRF, leech, Webshell, sensitive data leakage, session hijacking and protocol violations. ASC updates and releases the ASL regularly to add the signatures of new attacks or vulnerabilities, and updates scanner/crawler types, malicious URLs and Webshell characteristics. NetWAF Series support manual and automatic update of the ASL.

NetWAF Series allow administrators to build a signature rule set based on the application characteristics such as application type, platform type, database type, and programing language, which suites their applications best and provides highest defense accuracy and performance.

In addition, NetWAF Series support custom attack signatures and integration of third-party commercial attack signatures.

SSL Offload

NetWAF Series provide hardware SSL or software based SSL offload capability, which migrates the computingintensive SSL encryption and decryption workload to the NetWAF appliances, thus reducing the workload of backend servers and enhancing server performance.

With SSL offload capability, NetWAF Series can perform deep inspection on the HTTP packets, which makes attacks employing encryption methods nowhere to hide.

Comprehensive Server Protection

NetWAF Series provide comprehensive server protection for servers:

- NetWAF Series support advanced ACL, which enables traffic control for specified defense objects based on Layer 3 to Layer 7 traffic characteristics.
- NetWAF Series support the HTTP filter function, which can filter HTTP packets based on HTTP protocol characteristics (such as request method, header, URL, Cookie) and perform deep protocol compliance or security compliance checks against customer Web applications, clock error response.
- NetWAF Series provide advanced defense options, such as HTTP Via header masking, response header removal, cookie security settings, Cookie tampering defense, session hijacking defense, error page customization, and URL detection and monitoring.
- NetWAF Series support protection of all versions of HTTP including HTTP 0.9/ 1.0/ 1.1/ 2.0. It also provides protection for FTP and SMTP.

Web Anti-Defacement

NetWAF Series provide the Web Anti-defacement (WAD) feature, which can monitor the protected Web page files in real time and cache page contents. When detecting Web page defacement, the NetWAF Series will automatically restore the tampered Web pages returned by Websites to normal pages, thus protecting public image.

Automatic Learning and Dynamic Profiling

NetWAF Series provide the positive WAF feature, which can generate positive whitelists based on the characteristics of normal traffic. Administrators can configure the appliances to automatically generate positive whitelists at the specified interval or when the number of incremental learning log count reaches the specified threshold.

NetWAF Series provide the traffic baseline learning function. After it is enabled, the appliances automatically learn the traffic baseline of defense objects, and support dynamic refreshing the automatic DDoS profiles based on learning results. This not only reduces the manual intervention but enhances the defense accuracy.

Application Security Visibility

- Providing rich event logs to facilitate the replay and audit of attacks.
- Providing WAF attack logs, WAF audit logs, HTTP access logs. DDoS warning logs, DDoS attack logs and HTTP filter logs
- Supporting admin audit logs to facilitate the auditing against administrators.
- Supporting exporting security event logs.
- Providing granular and intuitive graphic monitoring.
- Displaying system status such as CPU usage, RAM usage, disk usage and throughput.
- Displaying attack statistics, covering severity distribution, attack type, attack sources, attack source regions and so on.
- Displaying service traffic statistics, including detailed statistics for the traffic of different protocols.
- Displaying packet drop statistics includingthe drop reason statistics.
- Displaying service access statistics, includingthe TopN accessed URLs, client IPs and so on.
- Supporting custom monitoring pages by adding desired monitoring graphs.
- Supporting exporting monitoring graphs manually and generating monitoring report periodically.
- Supporting generating one-time or periodic advanced reports.
- Supporting system status reports, application security status report, PCI DSS compliance reports and so on.

High Availability

NetWAF Series provide multiple high availability options through which the application on-line time can be maximized and ensures the high availability of application services.

- The Clustering function provides fast fail-over for the two or multiple NetWAF appliances deployed in routing mode. The NetWAF appliances can work in active-standby or active-active mode. NetWAF Series Datasheet
- In a network environment deployed with redundancy solution, the administrator can use the external HA solution to provide traffic high availability fortheNetWAF appliance deployed in Bridge transparent or proxy mode.
- Software and hardware bypass functions can avoid traffic interruption caused by failure (such as software and hardware failures) fortheNetWAF appliance deployed in Bridge transparent mode.
- If the NetWAF appliance is deployed in out-of-path TAP mode, the appliance failure will not lead to service interruption.

Management and Integration

NetWAF Series are easy to deploy, providing intuitive Web User Interface and easy-to-operate command line interface for configuration management. With the admin tools, network administrators can view the status of system parameters, enable services and implement configuration automation by employing the XML-RPC technology. By employing extensible API interface, administrators can integrate the system management with the 3rd-party monitoring and management system.

To meet the deployment and management requirements of application security in the cloud, Infosec's eCloud RESTful API provides a script-level interface for cloud management systems to manage and monitor Infosec devices and assist in interactions between cloud operating systems and virtual machines running Infosec DDoS mitigation.

Physical and Virtual Appliances

Dedicated NetWAF Series appliances leverage a multicore architecture, SSDs, software or hardware SSL and compression, energy-efficient components and 10 GigE or 40 GigE to create solutions purpose-built for scalable application security. Whether running on Infosec's AVX Series Network Functions Platform, or on common hypervisors, vNetWAF virtual appliances are ideal for organizations seeking to benefit from the flexibility of virtual environments, offer infrastructure services and new elastic business models or evaluate Infosec application security firewall with minimal risk and upfront cost.

Product Function List

APPLICATION SECURITY

WAF

- OWASP Top 10, API Security including SOAP, XML and JSON, WASC Classification.
- Signature-based defense, preventing SQL injection, XSS, network crawlers, CSRF attacks, leech, Webshell, local/remote file inclusion, command injection, sensitive data leakage, and so on, and supporting one-click signature exclusion.
- Identity card information, phone number, email address, bankcard number DLP rules and content filter
- CSRF defense, anti-leech, anti-crawling/scanning,unauthorized navigation, predefined resource location.
- Positive WAF Security Model and negative security model.
- Automatic traffic learning, automatic generation of positive whitelists, defense against “Zero-day” attacks, learning the traffic pattern of only trusted sources

Application DDoS Mitigation

- HTTP GET Flood, HTTP POST flood, HTTP Slowloris attack, HTTP Slow POST attack, HTTP CC attack, HTTP Packet Anomaly attacks,SMTP and FTP protection
- SSL Handshake attack, SSL Renegotiation attack, SSL Packet Anomaly attacks
- DNS Query Flood, DNS Reply Flood, DNS NXDomain Flood, DNS Cache Poisoning, DNS Packet Anomaly attacks
- Client source authentication , behaviour analysis including IOT and bot threat
- Application traffic baseline learning, dynamic refreshing of defense profiles

API Protection

- Positive AI Asset security protection and API profile learning
- API Authentication & Authorization includes Basic, JWT, Digest, API ID, and OAuth2
- API Rate Limit control includes address or user based control
- API Circuit Breaker

Advanced Defense Options

- HTTP filter, HTTP Via header masking, removal of HTTP response headers containing backend server information
- Cookie tampering defense, session hijacking defense, brute force defense, buffer overflow,backdoor
- Web anti-defacement , client fingerprinting, Web parameter protection, credential encryption
- Inserting http only and secure attributes into HTTP response cookies
- URL detection and URL monitoring
- Error page customization and DNS domain statistics
- Real source IP detection, forceful browsing, data encoding
- Antivirus for file upload scanning
- ICAP support
- Http2 support
- Bot protection
- GeoIP protection
- Dynamic Web Page Obfuscation - selectively applies code obfuscation to HTTP requests and responses

Application ACL

- HTTP ACL, DNS ACL, URL whitelists , Rate limit based on URL,IP,URI etc.
- Static blacklist, static whitelist, dynamic blacklist, dynamic whitelist, GeoIP-based access control

SSL Acceleration	• Hardware SSL acceleration • RSA/ECC/SM2 certification, SSLv3/TLSv1/TLSv1.1/TLSv1.2,TLSv1.3 and custom cipher suites • Client certificate authentication • SSL session reuse and timeout control • Server Name Indication (SNI)
	NETWORK SECURITY
Network DDoS Mitigation	• TCP SYN Flood, TCP SYN-ACK Flood, TCPACK Flood, TCP FIN/RST Flood, TCP Connection Flood, TCP Fragment Flood, TCP Slow Connection, TCP Abnormal Connection • UDP Flood, UDP Fragment Flood • ICMP Flood • Traffic baseline learning, dynamic refreshing of defense profiles • Client source authentication • IP reputation
Common DoS Attacks and Malformed Single Packet Attacks	• Smurf, LAND, Fraggle, IP Spoofing, Ping of Death, Teardrop, WinNuke, Tracert • TCP packet with abnormal flag, large UDP packet, ICMP redirect packet, ICMP unreachable packet, large ICMP packet, IP packet with routing record option, IP packet with source routing option, IP packet with Timestamp option
Network ACL	• TCP ACL, UDPACL, ICMPACL • Static blacklist, static whitelist, dynamic blacklist, dynamic whitelist, GeoIP-based access control
	APPLICATION SECURITY VISIBILITY
Event Logs	• WAF attack logs, WAF audit logs, HTTP access logs, HTTP violation logs, HTTP filter logs • DDoS warning logs, DDoS attack logs • Log aggregation, security event alert via Email/SNMP
Graphic Monitoring •	• Global attack statistics, security group attack statistics, security service attack statistics • Global traffic statistics, traffic statistics of defense objects • Global packet drop statistics, packet drop statistics of defense objects • CPU usage, memory usage, throughput, disk usage • Custom monitoring graphs
Report	System status monitoring reports, advanced service security status reports, PCI DSS compliance reports • Report customization, periodic reports
	APPLICATION AVAILABILITY
Networking and Deployment	• Link Aggregation, VLAN, MNET, JUMBO Frame • Bridge mode, Routing mode, TAP mode • Static route, RIP/OSPF/BGP dynamic route, policy route, ICAP Integration
High Availability	• Clustering among up to 32 nodes, Active/Active or Active/Standby working mode • Configuration synchronization, VRRP • Hardware bypass, software bypass
IPv6	• Full IPv6 support, IPv4 and IPv6 dual stack support • IPv6-ready gold certified

MANAGEMENT

System

- Centralized management
- Supporting secure CLI, WebUI and SSH remote management as well as XML-RPC remote management interfaces, facilitating the integration with third-party management and monitoring platforms
- Supporting SNMPv2, SNMPv3 and private MIB file
- Syslog (based on UDP orTCP)
- User management, admin authentication and authorization (Active Directory, LDAP,RADIUS and TACACS+ role-based privilege management, admin audit logs
- Supporting system alert via Email and SNMP
- Supporting multiple configuration files and configuration synchronization between nodes
- On-line troubleshooting and real-time monitoring, debug, tcp -dump

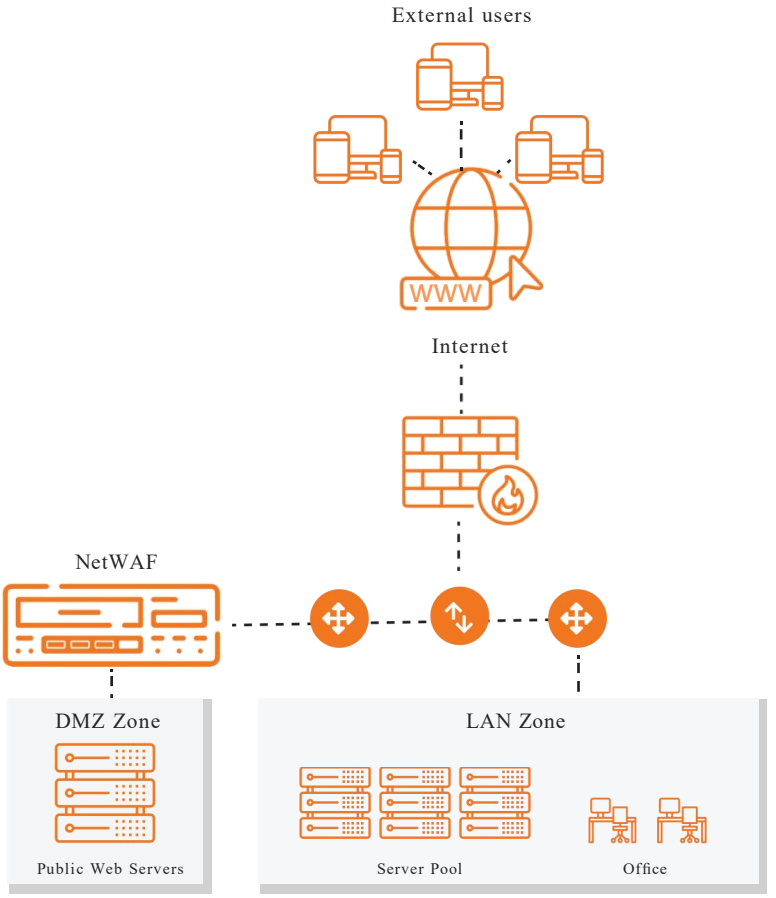
eCloud RESTful API

Providing interface for cloud management systems to control and monitor hardware and virtual NetWAF appliances

Assisting interaction between components such as virtual machines in CloudOSRemote management of NetWAF appliancesNotification of events on NetWAF appliances

NetWAF Application Security Defense Architecture

- Web Application Firewall
- Application DDoS Mitigation
- Network DDoS Mitigation
- Web Anti-defacement
- Advanced Access Control
- Automatic Learning
- Dynamic Profiling
- Application Visibility
- SSL Acceleration
- IPv6 Support
- N+1 Clustering



Product Specifications

• Standard o Optional	NetWAF2800	NetWAF5800	NetWAF6850	NetWAF7850
CPU	Intel	Intel	Intel	Intel
Max.L4 Throughput	10Gbps	20Gbps	70Gbps	100Gbps
Max.L7 Throughput	5Gbps	10Gbps	30Gbps	50Gbps
Max. SSL TPS (RSA 2K)	20K	20K	50K	80K
Max. ECC TPS (ECDSA P256)	15K	15K	25K	40K
Bypass card	No bypass card in standard configuration; optional			
1 GbE Copper	●	●	●	●
1 GbE Fiber	○	○	○	○
10 GbE Fiber	●	●	●	●
40 GbE Fiber				○
100 GbE Fiber				○
Power Supply (Hot Swappable)	NetWAF2800, 5800		Dual Power: AC(100V-240V、6.5A Max), DC(240V、4.5A Max)	
	NetWAF6850, 7850		Dual Power: AC(100V-240V、6.5A Max), DC(240V、4.5A Max)	
Maximum Power Supply Output（W)	450W		800W	
Dimensions(W × D × H)	547mm*435mm*44.5mm		549.9mm*435mm*88mm	
Environmental	Operating Temperature: 0 to 45° C; Humidity: 0% to 90%; Non-condensing			
Regulatory Compliance	GB 42250, ICES-003, EN 55024, CISPR 22, AS/NZS 3548, FCC, 47FR part 15 Class A, VCCI-A, CSA, C/US, CE, IEC60950-1, CSA 60950-1, EN 60950-1			
Safety	CCC, CSA, C/US, CE, IEC 60950-1, CSA 60950-1, EN 60950-1			
Support	Gold, Silver and Bronze Level Support Plan			
Warranty	1 Year Hardware, 90 Days Software			