# APPLICATION INSIGHT WAF

# Specification Sheet

# < Web Application Firewall Specification Sheet >

## Technical specifications

**[Performance]**

HTTP

// Please enter the values by referring to the APPLIANCE SHEET of the model you are proposing.

- 1K CPS HTTP xxxxx processing

- 1K TPS HTTP xxxxx processing

- 32K TPS HTTP x.xG processing

HTTPS

// Please enter the values by referring to the APPLIANCE SHEET of the model you are proposing.

- 1K CPS HTTPS(TLS1.2, AES256-SHA256, certification 2048bit) xxxxx processing

- 1K TPS HTTPS(TLS1.2, AES256-SHA 256, certification 2048bit) xxxxx processing

- 32K TPS HTTPS(TLS1.2, AES256-SHA 256, certification 2048bit) x.xG processing

**[Installation]**

- Hardware-Integrated Appliance Product

- Support for Hardware Bypass Functionality to Ensure Continuity During Hardware Fault Conditions

- Support for Software Bypass Functionality to Ensure Service Continuity During Software Fault Conditions

- Support for Hardware-Based SSL/TLS Acceleration Card Installation to Enhance Performance

- Support for Deployment via Transparent Proxy Architecture Without Modifying Existing Network Configuration

- Support for GWLB-Integrated Virtual Inline Proxy Deployment with Various Encapsulation Protocols (GRE, VXLAN, GENEVE, etc.)

- Support for One-Armed Mode Deployment Providing Equivalent Web Security to In-Line Configuration in Out-of-Path Architecture

- Support for Sniffing (In-Line) and Mirroring (Out-of-Path) Mode Deployment for HTTPS Decryption and Web Security Policy Enforcement

- Support for High Availability (HA) Configuration with Active-Standby Redundancy

- Support for Asynchronous Traffic Handling in Redundant or Multi-Segment Network Configurations

- Support for Network Interface Redundancy via Link Aggregation (Bonding Configuration)

- Support for SSL Offload Configuration: Encrypted Communication with Clients and Plaintext Communication with Servers

- Support for SSL Termination Configuration: Encrypted Communication Proxy for Web Servers Without HTTPS Capability

- Support for Passive Decrypted Traffic Mirroring Across More Than Eight Ports

- Support for Traffic Mirroring Configuration Using VXLAN Protocol in Reverse Proxy Architecture

- Support for Domain-Based Bandwidth Limitation Settings to Maintain Web Service Availability (QoS, Bandwidth Control)

- Support for Web Acceleration via Caching Functionality and Dedicated UI for Cache Status Monitoring

- Support for Various Server Load Balancing Algorithms for Registered Web Servers in Reverse Proxy Architecture (Hash, Round-Robin, Latency, Least Connection, Weighted Round Robin, Weighted Least Connections, etc.)

**[Web Security]**

- Support for Official Web Vulnerability Mitigation Patterns Including OWASP Top 10

- Support for Detection of Abnormal Encoding: Real-Time Decoding and Security Enforcement Against Repeated or Mixed Encoding Used for Evasion

- Support for HSTS (HTTP Strict Transport Security) Configuration to Enforce HTTPS Connections in Web Browsers

- Support for HTTP Header Inspection to Detect Attacks Embedded in Headers (e.g., User-Agent, Origin, Cookie, etc.)

- Support for Real Client IP Identification via HTTP Headers (e.g., X-Forwarded-For, True-Client-IP) When Traffic Passes Through a Proxy, with Security Policy Enforcement

- Support for Preventing Information Leakage in Server-Sent Events (SSE) Communication by Detecting Personal Data Embedded in Response Streams (e.g., Chatbot Responses)

- Support for WebSocket-Based Attack Detection: Identifying Web Attacks Embedded in WebSocket Communication and Detecting DoS Attacks Based on Frame Count Analysis

- Support for Detection of Web Server Abuse via Malicious Code Embedded in HTTP Responses (e.g., Exploit Kits, Redirects, JavaScript Obfuscation)

- Support for User Authentication to Restrict Access to Specific Web Page Paths Based on Individual Account Verification

- Support for URL Obfuscation via Encryption to Prevent Exposure of Specific Web Page Paths

- Support for Web Traffic Profiling and Automatic Learning: Signature Generation Based on Parameter-Type Profiling of HTTP Requests to Detect Unknown Threats

- Support for Custom Header Injection in Reverse Proxy: Adding Specified Headers to Indicate WAF Traversal When Forwarding Traffic to the Next Node (e.g., Load Balancer or Web Server)

- Support for Web Protocol Standardization: Detection and Blocking of Abnormal Requests That Violate Standard HTTP Protocols (e.g., RFC Specifications)

- Support for Malicious File Upload Prevention: Blocking Uploads of Web Shells and Files with Obfuscated or Suspicious Extensions

- Support for Malicious File Access Restriction: Detecting Access to Pre-Installed Web Shells or Malicious Files on Web Servers to Prevent Secondary Spread

- Support for HTTP & DBMS Error Exposure Prevention: Masking Error Messages to Conceal Attack Surfaces in Web Server Responses

- Support for Sensitive Information Detection and Response: Identifying and Responding to Personal Data Embedded in All Web Requests and Responses (HTTP Headers & Body, Attachments, Embedded Files) through Masking or Blocking

- Support for Multi-Dimensional Malicious Bot Detection: Behavior-Based Identification of Crawlers and Scrapers Using Honey Pot TRAP and JavaScript Injection Techniques

- Support for CAPTCHA Authentication to Mitigate Abnormal or Automated Access Attempts

- Support for HTTP-Based DoS Attack Mitigation: Detection and Prevention of HTTP Flooding, Slowloris, RUDY, Slowread, Hash DoS, Range DoS, and Excessive Session Generation

- Support for Automatic Black IP Management: Automatically Registering and Managing Client IPs That Repeatedly Attempt Attacks and Threaten Web Availability

- Support for Leaked Identity Information Management: Detecting Credential Stuffing Attacks Using a Leaked Credentials Database

- Support for Diverse Client Identification Methods in Brute Force Mitigation Policies: IP Address, Browser Fingerprint, Session Cookie, etc.

- Support for Diverse Detection Conditions in Brute Force Mitigation Policies: Authentication URL, Parameter Name, User-Agent, Threshold Time up to 2 Hours, and Login Behavior Patterns

- Support for Source Code Comment Exposure Prevention: Removing Comments from Web Responses to Prevent Leakage of Sensitive Information

- Support for GraphQL Vulnerability Mitigation: Detection Options Including Introspection Query Monitoring, Request Length Limitation, Batch Request Restriction, and Nested Query Depth Control

- Support for Parameter Tampering Detection: Input Validation Based on Regex or String Matching for Specified Parameters, with Server Response Verification per Client (Session Cookie, Header)

- Support for Integration with Proprietary Cyber Threat Intelligence Platform: Real-Time Detection and Response to Various Threats (e.g., Blacklisted Client IPs, C&C IPs), with Reputation Lookup for Malicious URLs and Files from Stored Log Data

**[API Security]**

- Support for Multiple API Specification Methods: Efficient API Endpoint Management via Direct Upload of OpenAPI Spec, OAS URL Integration, or Manual Input and Editing

- Support for Web Application Attack Detection via API Traffic: Full Syntax Parsing and Security Pattern Enforcement for JSON, XML, and YAML Payloads

- Support for Customizing API Block Messages: Predefining JSON-Formatted Block Pages Triggered by API Security Rules

- Support for API Authentication Control: Preventing Authentication Bypass by Verifying JWT (JSON Web Token) Integrity via Authentication Server Redirection or Direct Decryption Using Keys

- Support for API Authorization Control: Detecting Unauthorized Data Manipulation Attempts by Extracting and Validating JWT Claim-Based Permissions and Comparing Them with Actual Request Data

- Support for API Validation: Detecting and Controlling API Requests That Violate Predefined API Specifications

- Support for API Access Control Based on Client IP or Country-Specific IP per API Endpoint

- Support for Maximum Request Length Limitation per API Endpoint

- Support for Force Timeout and Rate Limit Configuration per API Endpoint

- Support for Mandatory Header Enforcement per API Endpoint

- Support for File Upload Extension Control and Tampering Detection per API Endpoint

**[Web Server Management]**

- Support for Multiple TLS Versions: SSL V3.0, TLS V1.0, TLS V1.1, TLS V1.2, TLS V1.3

- Support for HTTP/2: Full Security Feature Coverage for HTTPS Traffic over HTTP/2 Protocol

- Support for IPv6: Full Security Feature Coverage for HTTPS Traffic over IPv6 Networks

- Support for Multiple SSL Certificate Formats: cer, crt, pem, der, pfx, p12

- Support for SSL Certificate Expiration Alerts and Automatic Bypass Upon Expiry

- Support for Bulk SSL Certificate Replacement Across Web Servers Registered with the Same Certificate

- Support for Automatic SSL Certificate Renewal: Integrated with Certificate Lifecycle Management (CLM) for Pre-Expiration Update

- Support for Automatic Configuration of Protocols and Algorithms Aligned with Web Server Settings

- Support for Independent Configuration of Protocol Versions and Algorithms for Client-Side and Server-Side Connections

- Support for Block Page Response for Disallowed SSL/TLS Versions

- Support for Web Server Health Check: Real-Time Monitoring of Service Quality (Response Code, Latency, Availability) and Load Balancing Based on Health Check Results

- Support for URL Detection Using Only Web Server IP and Port Without Domain Registration

**[Operation and convenience]**

- Support for Seamless Service Availability During Pattern Updates and Policy Changes

- Support for Web-Based GUI Management Console Without Requiring Separate Program or ActiveX Installation

- Support for Custom Dashboard Configuration in Web Console

- Support for Encrypted Communication Protocols (SSH, HTTPS) for Remote Access

- Support for Two-Factor Authentication (2FA) Using One-Time Password (OTP) for Administrator Login

- Support for IP-Based Access Control for Web Console Login per Administrator Account

- Support for Granular Administrator Account Management Policies — Including Password Expiration and Inactivity-Based Account Lockout

- Support for Role-Based Access Control (RBAC) — Granular Menu-Level Permissions per Administrator Account

- Support for Multi-Tenant Operation by Domain Group — Dedicated Administrator Assignment and Segmented Web Console per Group (Policy Configuration and Monitoring Restricted to Authorized Domains)

- Support for Domain Group-Based Web Traffic Monitoring Dashboard Content

- Support for Domain-Based QoS Management — Configurable Traffic Thresholds per Domain or Domain Group with Automatic Alert Emails for Excessive Traffic

- Support for Customization of Statistical Report Items Across Multiple Categories

- Support for Automated Generation and Email Delivery of Traffic, System, and Report Data

- Support for Automatic Bypass Mode Activation and Tiered Bypass Transition Upon System Overload (Software Bypass → Hardware Bypass)

- Support for One-Click Exception Handling During Log Review — Including IP Whitelist, IP Blacklist, and URL Exception Registration

- Support for Configurable Bypass Conditions — Including IP, URL, and HTTP Header Information

- Support for Automatic Web Traffic Identification — Enables Bypass or Drop Actions for Non-Web Traffic Without Specifying TCP Port

- Support for Policy Import Function — Allows Loading of Predefined Policies During Web Server Registration or Domain Group Creation

- Support for Policy Testing Function — Enables Immediate Self-Test of Web Security Rules Using Custom Web Request and Response Data

- Support for Bulk Security Policy Lookup by IP, URL, HTTP Header, and CVE Vulnerability Code

- Support for Enabling or Disabling Built-In Detection Patterns per Security Policy

- Support for Security Policy-Based Configuration of Applied or Exception Targets — Including IP, URL, HTTP Header, and Group Settings

- Support for Customized Block Page Configuration per Security Policy

- Support for Mail Integration Types for Audit Log Delivery Upon System Anomalies — Including SMTP, SMTPS, and AWS SES

- Support for Telegram Messenger Integration for Audit Log Delivery Upon System Anomalies

- Support for Real-Time Monitoring of System Resources and Temperature with Threshold Alert Notifications

- Support for SNMP GET and SNMP TRAP Configuration for Versions v2 and v3

- Support for Operational Convenience via REST API-Based Open Web API

- Support for Direct Access to Technical Support Portal from Product Web Console

- Support for Offline Access to Product Manual and Version-Specific Release Notes from Web Console

- Support for User Interface-Based Troubleshooting Features Including TCPDUMP, Debugging, and Automated System Recovery

**[Log Management]**

- Support for Real-Time Logging and Query of Decrypted Plaintext Data (Request/Response)

- Support for Highlighting Detection Basis within Decrypted Plaintext Data in Logs for Enhanced Visibility

- Support for Masking Sensitive Information in All Types of Detection Logs

- Support for Real-Time Audit Logging and Query of System Operation History and Configuration Changes

- Support for Log Transmission and Customizable Format Settings for Integration with SIEM/SOAR Systems

- Support for Various Log Transmission Protocols (UDP, TCP, SSL, etc.) for Integration with SIEM/SOAR Systems

- Support for Pivot Chart Generation Based on Log Data — Customizable Pie and Bar Charts

- Support for Detailed Policy Configuration for Automated Log Management and Data Protection Compliance — Including Retention Period, Backup Path, and Deletion Conditions