APPLICATION INSIGHT WAF-VE

Specification Sheet

< WAF Product Specification Sheet>

Division	Technical specifications
Functions	**[[Configuration]** - Automatic list and policy management for Auto Scale In/Out of WAF solution - Traffic routing according to Auto Scale In/Out of the protected web server - East-West (internal) / North-South (external) traffic handling - HA (Active-Standby) configuration without changing service IP between fail-over and fail-back - Network interface bonding - Transmit decrypted HTTPS traffic to 3rd party solution - HTTP/2 protocol support (providing the same security function and detection log as HTTP/1.1) - HTTPS TLS 1.3 support - Bandwidth Limit for each domain for web service availability - Web acceleration/content compression and caching information/status display - Web server load balancing (Hash, Round-robin, Latency, Least connection, Weighted Round Robin, Weighted Least Connections) - SSL Offload Configuration to Reduce Web Server SSL Traffic Load - SSL traffic proxy support for non-HTTPS web servers - URL Rewrite function for request and response data **[WEB Security]** - Support IPv6 traffic - Bot identification and detection

	- HTTP-based DoS attacks (HTTP Flood, Slowloris, RUDY, Slowread, Hash DoS, Range DoS, etc.) defense - Real-time response to various web attack threats (Black Client IP, C&C IP, etc.) through the cyber threat intelligence platform linkage - Unknown attack identification through machine learning linkage - Detect attacks embedded in Web Socket traffic - Detects malicious code (Exploit Kit, redirect, js obfuscation, etc.) inserted in the body of the web server response page - Restrict access to only authorized users for the specified service (URL) - URL Encryption function to prevent external exposure of the specified URL path - Real-time decoding and detection of double (or multiple) encoded traffic for bypass purposes such as URL, HEX, Unicode, Base64, etc. - Detect attacks embedded in headers other than HTTP body (User-Agent, Origin, Cookie, etc.) - Profiling by URL parameter (length/attribute) and automatic policy reflection - Header identification and policy reflection of X-Forwarded-For, True-Client-IP, etc. - Add X-custom-header when forwarding traffic to web server - Automatic update of public proxy server list and restriction of proxy IP access - Cloaking DBMS error messages in web server response page - Detection of abnormal requests that violate HTTP protocol format - Webshell upload detection and Restricting access to already uploaded webshell - Remove comment text in web server response page - Manually restricting input parameter ranges or dynamically identifying tampered parameters for parameter tampering detection. - Operating security rules based on session IDs for improved accuracy of parameter tampering detection policies.

	- Create security rules with parameter names and User-Agent conditions in addition to the login URL for efficient Bruteforce defense. - Device identification and security policy application with Fingerpint or session ID instead of IP to improve bruteforce defense policy accuracy. - Bruteforce defense rules are created based on the number of login attempts from the same device or client during the threshold period of time (up to 2 hours). - Provides leaked credentials DB update function and credential stuffing defense security function based on DB. **[API Security]** - Complete parsing of JSON, XML, and YAML formats and signature-based detection such as SQLi and CSRF - Blocked by API security rules, block page in JSON format is sent - Supports Open API SPEC upload and OAS URL link for API-Endpoint management - JWT(JSON Web Token) integrity verification through authentication server redirection or decryption - JWT(JSON Web Token) Claim and data comparison inspection to detect API request data tempering by unauthorized users - Detect unapproved methods and response codes for each API-Endpoint - Permit/Deny rules based on IP and Geo Location for each API-Endpoint - maximum request length limit rules for each API-Endpoint - force timeout and rate limit rules for each API-Endpoint - rules for specifying required headers for each API-Endpoint - file upload extension limit rules for each API-Endpoint

	[Operation and convenience] - REST API provided - Separately provided dedicated web UI for troubleshooting - Real-time monitoring of service response code, response speed, and availability rate of the web server to be protected - Synchronizes certificates, protocols and algorithms with web servers to be protected by HTTPS - Provides a self-test page to verify whether an attack is detected and the establishment policy - Response pattern search function for each CVE vulnerability code - Advance notification before HTTPS certificate expiration (warning popup, E-mail) - Provides independent dashboard by domain and integrated dashboard for all web services - Independent policy setting and administrator designation for each domain - Provides non-stop service during signature update - Provides non-stop service during policy backup or recovery - Differential setting of blocking pages for each security rule - Real-time policy synchronization between grouping systems - Provides encrypted management channel(HTTPS, SSH) - Authority and access IP setting for each administrator - Support customization for SIEM and ESM logs format - Regular automatic report generation and e-mail sending - Support SNMP GET and SNMP TRAP - Provides one-click handling function in detection log - Provides notification function when web traffic exceeds the threshold