APPLICATION INSIGHT WAF

Specification Sheet

< APPLICATION INSIGHT WAF Specification Sheet >

	Technical Full Details
Detailed Function	**[Functions]** - Support HTTP/2 (same security functions and detection log of HTTP/1.1) - Support HTTPS TLS 1.3 - support domain based QoS function (Bandwidth limit) setting function for securing Web service availability - Support web acceleration and displaying cached data information/status with web caching function - Support Server Load balancing (Hash, Round-robin, Latency, Least connection) - Support the SSL Offload feature for the WEB server's SSL traffic reduction - Support Asynchronous traffic in the multi-segment configuration for multiple networks - Support HA (Active-Standby) function with VRRP - Support SSL Termination function to substitute for the server not available SSL service **[Security]** - Real-time response to various web attack threats (Black Client IP, C&C IP, Malicious code insertion or etc.) with Cyber Threat Intelligence Platform interworking - Support Unknown attack detection function with Machine-Learning interworking - Support web attack detection code in web socket traffic - Support the malicious code(Exploit Kit, Redirection, js obfuscation, etc.) analyzing for server's malware stopover/exploitation misusage detection - Service(URL) Access control based on authorized user account

	- Real-time decoding function to detect multiple encoded traffics as URL, HEX, Unicode, BASE64 or etc. - Support the profiling feature regarding HTTP request parameter type function and auto policy applying - Support the profiling feature regarding HTTP request parameter type function and auto policy applying - Support policy configuration and logging function based on real client IP (X-Forwarded-For, True-Client-IP, etc.) or selected header(IP) which connects through a proxy server - Support server IP detection function which connects through a proxy server and proxy server IP auto update which is external-facing - Support the cloaking feature of DBMS message in webserver's response page - Support detection function when the embedded type file (exist the other file inside of it) is uploaded/downloaded with personal information - Support the security function and configuration with IPv6 traffic same as IPv4 - Support the notice page for advice to use high-level protocol if the client uses disabled SSL version - Support the hidden field's parameter control detection - OWASP Top 10 detection feature - Support the HTTP based DoS attack(HTTP Flood, Flowloris, RUDY, Hash DoS, Range DoS, session over) protection feature - Support the CAPTCHA to verify the normal users or computer bot - Support the Honey Pot TRAP, JS Injection feature which is able to detect the computer bot program (the crawler, scrapper or etc.) - Support abnormal request violated by HTTP detection function - Support the malicious file upload detection function (extension control, contents mismatch detection function and etc.) - Support access control function of uploading or uploaded web shell file

- Support the login fraud attempt detection function based on results(attempt/success/fail) except the normal login page accessing

- Support target policy configuration (select the necessary policy in a supported list) and auto-detection function to block the client who performs repetitive attacks efficiently

- Send response page without source code annotation to the client from the web server

[Operation]

- Provide REST API for interworking 3rd party solution regarding web firewall operation and policy configuration

- Support the various trouble shooting(TCPDUMP, Debug log, System recovery mode, etc.) user interface

- Support the real-time monitoring of the protected web server's service quality (reply code, reply speed, duration or etc.)

- Automatic SSL protocol and algorithm synchronization function when the certification and personal key of HTTPS server are uploaded to protected web server

- Self-test function to determine the manually inputted request/response data

- Pattern searching function based on CVE vulnerability code

- Notice the HTTPS certificate expiry with Email or popup notice

- Enable / Disable feature provided by each policy's patterns

- Support the Client IP, exception client IP, apply URL and exception URL configuration for each policy

- Dashboard for each domain and HTTP/HTTPS traffic control(Mbps, CPS, TPS and, etc.) information are provided

- Support the SSL version and encrypt algorithm (Cipher) setup for both different sessions (Client/Server)

- Support policy and manager setup for each domain

	- Support the URL detection function with Webserver’s IP/Port regardless of domain registration - Support continuous system operation during the automatic or manual pattern update - Support continuous system operation during the old policy collective recovery - Support the block page configuration feature for each policy - Support the policy synchronous with grouped systems - Support encrypted communication (SSH, HTTPS) for the remote connection - Support permission setup and access control IP function for the administrator - Support manual format setting of detection log, audit log and system log for variable EMS interworking - Support web-based GUI management console page without additional program installation or Active-X - Support the variable statistics report item, auto report creation and email sending function - Support the SNMP GET and SNMP TRAP function - One-click URL exception registration of detected URL function is provided in the detection log view - One-click whitelist/blacklist registration of client IP function is provided in the detection log view - Auto email sending function if the traffic exceeded the limit of the configured domain’s HTTP, HTTPS or all traffics - Support Pivot Chart function as user defined model to Detection Log