MONITORAPP

APPLICATION INSIGHT WAF

Intelligent Web Application Firewall | AiWAF

AIWAF : Application Insight Web Application Firewall

It is a web application firewall appliance that inspects the traffic flowing to the web server and protects the server from various web attacks.

Why Do You Need a WAF?

Threats to open web servers

> The web is always open for services, so it is exposed to the threat of hackers

> With the development of information and communication devices and technologies, access through the web takes place anytime, anywhere

> With existing network security solutions such as IDS and IPS, security for the web is insufficient

> In the event of a security incident, it causes a negative impact on the company's reputation

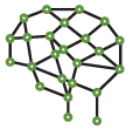
Strengthened IT compliance

> Today's IT compliance is a mandate, not a choice for survival and competition

> Failure to comply may result in economic loss, loss of awareness and loss of business opportunities

> Representative IT compliance

- GDPR (General Data Protection Regulation)
- HIPPA (Health Insurance Portability and Accountability Act)
- PCI-DSS (Payment Card Industry Data Security Standard), etc.



Machine Learning

Threat Intelligence

Web socket and API

WEB DLP

Bot

HTTP/2

Key Benefits of AIWAF

Complete web server security

> Comprehensive web attack detection through request and response data parsing

- Request-based attacks such as SQL/LDAP Injection, XSS, CSRF, Web Shell, Overflow, etc.
- Response-based attacks such as Directory Listing, Error page and comment clocking, etc.

> Detect Unknown Attacks through Machine Learning & Threat Intelligence

> Decode double & multi-encoded traffic

> Prevention of leakage of major server information and personal information

> Analyze and detect traffic accessed by using Script, Bot, etc.

> Malware detection and APT response through web server response page analysis

> Support Full HTTP/2 connection and same security features as HTTP/1.1

Easy management and operation

> Full-transparent proxy mode that does not affect the existing network

> HA (high availability) : active-standby, active-active

> Integrated dashboard for all or specific website status

> Differential policy setting and administrator designation for each website

> Logging request/response data in detection log and highlighting detection grounds

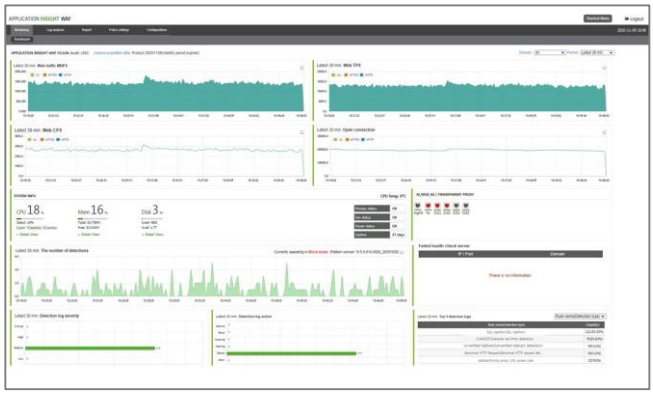
> Customizing monitoring contents such as ESM and SNMP

> Web cache and QoS to improve web service quality

> Server Health check and Traffic Load Balancing

> Transmit decrypted HTTPS traffic to 3rd party solution

AIWAF Administration GUI



1) System Monitoring
> Real-time system status and detection, traffic status monitoring
> Provides an integrated dashboard for all or specific websites

2) Log analysis
> Easy log inquiry through various search conditions
> Logging request/response body in detection log and highlighting detection grounds

3) Policy Setting
> Independent differential policy setting for each domain
> IP/URL application for each individual policy and pattern

Key Features of AIWAF

1) Various network configuration mode
> In-line: Full Transparent Proxy
> Out-of-path: Reverse proxy, Mirroring

2) Passive Mirror
> Transmit decrypted HTTPS traffic with 3rd party security solution

3) Threat intelligence Platform
> Real-time threat information update by AICC
> Client via Proxy, Black Client, C&C Traffic

4) Machine Learning
> Determine attack traffic and presenting predicted probability for each policy

5) Adaptive Profiling
> Profile database construction for normal request and response data by self-learning engine

6) Full HTTP/2 Support
> Complete HTTP/2 connection and parsing
> Provides the same security features as HTTP/1.1

7) ATP attack defense
> Detect destination/distribution abuse by malicious code
> Malware detection through response data body analysis

8) Security optimization
> Detailed control of each individual security rule and pattern
> Self-test function for established security policy

9) Traffic optimization
> Web Server Load balancing
> QoS(Bandwidth Limit) setting for each domain
> URL Rewrite (Request/Response)

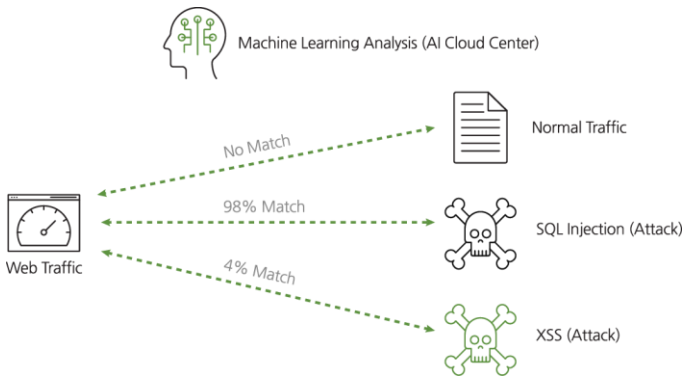
10) Web acceleration
> Reduce traffic and response time through web caching

11) Bot detection
> Malicious Bot used for Brute Force, Scraping, Denial of Inventory, Credential Stuffing, etc.
> Bot traffic identification through various mechanisms such as Java Script Injection and Human interaction

12) Multi-Layer Web Attack Defense
> Comprehensive defense against known web attacks such as OWASP TOP 10 attacks, Injection, XSS and HTTP Application DoS through various detection algorithms such as Signature, Threshold Limit, and Profiling

13) pattern update
> Monthly pattern update
> Real-time update and notification of emergency vulnerabilities

AICC for Machine Learning



Application Insight Cloud Center's Machine Leaning analysis of the request data is as follows: If it is determined to be an attack but is not detected by the current system, check that the policy or pattern is not used.

Analysis result : Maliciousness

Policy type	Attack
SQL injection	0.80129
Cross site script	0
CSRF detection	0
Command injection detection	0

Detection policy | Export to Excel

The test results were detected by the following policies and rules. (2020-11-09 17:49:03)

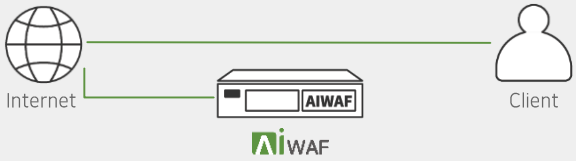
Detected domain: Default Detection policy: 2Count(s) Detection rule: 2Count(s)

Classification	Policy	Rule name
Vulnerability attack detection	SQL injection	1
Abnormal request/response	Character set limits detection	CHARSET

AIWAF Network deployment

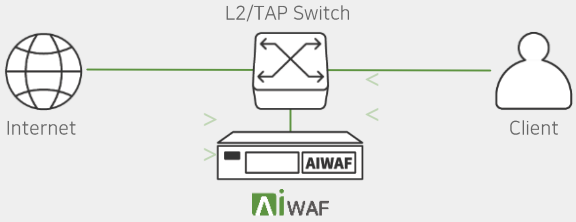
In-Line Mode (Full Transparent Proxy)

- In-line configuration in the bridge type on the network path
- Bypass in case of failure
- Support multi-segment and async traffic



Out-of-path Mode (Reverse Proxy)

- Broad protection for distributed servers
- Traffic flows into AIWAF through network route or DNS address change
- service continuity through HA configuration or DNS Failover



Out-of-path Mode (Mirroring)

- Configuration using the mirroring function of TAP or L2 Switch
- No impact on existing network
- Inspection based on copied traffic(Support Block)

AIWAF Models & Specifications

- It's written based on AIWAF APPLIANCE's standard workload, and actual performance can vary greatly depending on workload requirements.

Specification	AIWAF-100_Y20	AIWAF-200_Y20	AIWAF-500_Y20	AIWAF-1000_Y20	AIWAF-2000_Y20	AIWAF-4000_Y20	AIWAF-8000_Y20
Appearance							
RAM	4GB	8GB (Max 128GB)	16GB (Max 128GB)	32GB (Max 2TB)	32GB (Max 2TB)	64GB (Max 2TB)	64GB (Max 2TB)
HDD	500G	500G	500G	2TB	2TB	2TB	2TB
MGMT/HA	> Mgmt 1 UTP Port > HA 1 UTP Port	> Mgmt 1 UTP Port > HA 1 UTP Port	> Mgmt 1 UTP Port > HA 1 UTP Port	> Mgmt 1 UTP Port > HA 1 UTP Port	> Mgmt 1 UTP Port > HA 1 UTP Port	> Mgmt 1 UTP Port > HA 1 UTP Port	> Mgmt 1 UTP Port > HA 1 UTP Port
Network (Default)	1G UTP*2	1G UTP*4	1G UTP*4	-	-	-	-
Network (Option)	-	Slot 1 > 1G UTP 4Port > 1G Fiber 4Port > 10G Fiber 2Port	Slot 1 > 1G UTP 4Port > 1G Fiber 4Port > 10G Fiber 2Port	Slot 8 > 1G UTP 4Port > 1G Fiber 4Port > 10G Fiber 2Port	Slot 8 > 1G UTP 4Port > 1G Fiber 4Port > 10G Fiber 2Port	Slot 8 > 1G UTP 4Port > 1G Fiber 4Port > 10G Fiber 2Port	Slot 8 > 1G UTP 4Port > 1G Fiber 4Port > 10G Fiber 2Port
CPS HTTP / HTTPS	> 5,000 > 1,500	> 30,000 > 10,000	> 55,000 > 15,000	> 130,000 > 35,000	> 200,000 > 50,000	> 250,000 > 70,000	> 350,000 > 100,000
TPS HTTP / HTTPS	> 9,000 > 5,000	> 55,000 > 35,000	> 80,000 > 55,000	> 250,000 > 100,000	> 300,000 > 150,000	> 400,000 > 200,000	> 550,000 > 300,000
Throughput HTTP / HTTPS	> 400M > 200M	> 2G > 1G	> 4G > 2G	> 10G > 5G	> 14G > 8G	> 15G > 9G	> 16G > 10G

MONITORAPP, Inc.
EMAIL sales@monitorapp.com
www.monitorapp.com

S/N : #F100101011