APPLICATION INSIGHT SWG

Intelligent Secure Web Gateway | **AISWG**

MONITORAPP

Application Security Leader

AISWG (Application Insight Secure Web Gateway) : Staff's URL Access Filtering Solution

AISWG is an On-Premise secure web gateway product that analyzes Web protocols (HTTP/HTTPS) and controls access to non-business & malicious website with URL category filtering to build a secure web environment for company staff and maximize business efficiency.

AISWG controls users' non-business and malicious Web access.

- Real-time update of non-business and malicious URL categories by working on with MONITORAPP's cloud-based threat intelligence (AICC)
  - Blocking various unknown attacks through behavior-based collecting system in advance
  - Provides 57 non-business categories and 9 malicious categories for URL filtering and each category can be on/off and updated by admin.
- Controls Bypass access and Network Application such as P2P, Messenger
- Supports network-based DLP (Data Loss Prevention) to prevent leakage of main assets and information
- Support NAT / DHCP environment with user authentication

AISWG has excellent performance.

- **Transparent Proxy System** (Patent No. 10-0898371)
  - Maximizes bulk traffic analysis performance and high-speed packet analysis with load balancing algorithm
  - Its Full Transparent Proxy type does not affect network configuration.
- Non-stop service with Fail-open (Bypass) function
- Fully controls request/response Web traffic with DPI (Deep Packet Inspection)
- **HTTPS traffic analysis with SSL traffic encryption/decryption technology**
  Auto-deployment of SSL certificate, Auto-learning the website unavailable on SSL communication, Auto-blocking the invalid SSL certificate

Why AISWG ?

Increased Security Threats via Web

- More than 80% of recent security incidents happen on the Web
  - Security threats hidden in SSL traffic
  - Increased APT attacks targeting countries or enterpises
  - Malware infected by just online AD banner click
  - Most companies access to the domain providing known malicious file or web services
- Reduced work efficiency and productivity by non-business website access
- Diversified threat targets such as P2P and SNS

AISWG 's Benefits

- Build information protection system following IT Compliance
- Protect internal users against various threats by blocking malicious site access or C&C server communication in advance
- Prevent internal users from leaking sensitive or confidential information with network DLP
- Manage internal traffic and improve business efficiency by controlling internal user's access to Internet and Network Application
- Supports SSL traffic handling, so organization can reduce the budget needed to build extra SSL solution

Key Freatures of AISWG

Malicious / Non-business Website Access Control

- Analyzes request traffic to block malicious & non-business URL access
  - URL Filtering Categories : Consist of 57 non-business and 9 malicious categories for URL filtering and hold about 100 million URLs
- Analyzes response traffic to block malware intrusion
- Blocks C&C center and Botnet traffic
- Controls commercial Web mail service by function
- Controls non-standard web traffic and non-HTTP / HTTPS traffic
- Controls Network Application such as P2P, messenger, web hard
- Blocks Proxy and Bypass access program
- Network DLP for attachments by analyzing keyword and regular expression

Equipment Management

- It's installed as Transparent Gateway at once , and does not affect existing network
- HA (High Availibility) configuration mode : Active-Standby, Active-Active
- Supports NAT / DHCP environment through user authentication
- Multi-user group management logically separate by each organization
- Self- Decrypting / Encrypting SSL traffic
  - Derives the SSL certificate distribution page for easy deployment
- Comprehensive information with real-time dashboard
- Provides various logs such as Detection / SSL connection / Audit log

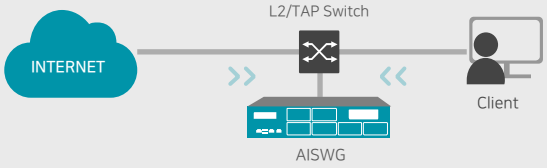
Network Configuration Modes of AISWG

Inline Mode (Full Transparent Proxy)

- In-line configuration in the Bridge type on the network path
- Transparent Proxy Mode
- Bypass in case of failure
- Support Multi-Segment

Out-of-path Mode (Forward Proxy)

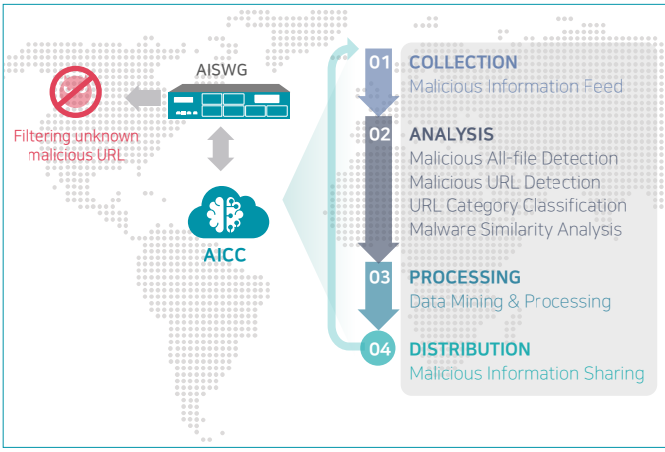
- Broad protection for distributed Clients
- PAC (Proxy Auto-Confg) and browser settings (WEB protocol only)
- Bypass in case of failure (Auto-unlock the browser Proxy setting)



Out-of-path Mode (Mirroring)

- Configuration using Mirroring function of TAP or L2 Switch
- No impact on existing network
- Inspection based on copied traffic

AICC for Threat Intelligence



- Collect, analyze and respond in real time to emerging threats worldwide
- **Virtual Patching**
  Rapid and accurate automatic threat analysis and determining whether malicious to collect unknown new / variant attack information and generate pattern about it and distribute real-time patch
- Process :
  Collecting > Analyzing > Processing > Distributing Threat Information
- **Threat Similarity Profiling**
  - Classify the features of the collected threats and group and learn through deep learning
  - In case of unknown threat such as zero-day vulnerability, measure similar groups and analyze and respond quickly

AISWG 's Core Technology

- Inline Mode : Full transparent Proxy
- Out-of-path Mode : Forward Proxy, Mirroring
- Multi-Segment, Bonding

Various Network Configuration Mode 01

- Control Web service by user
- Block non-business and malicious URL access
- Detect malware hidden in response traffic
- Prevent data leakage via the network

02 Detailed Packet inspection

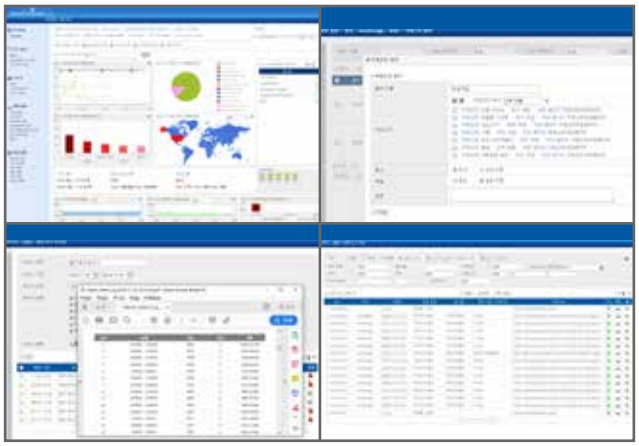
Proxy Gateway 03

- Transparent Proxy system (Patent No. 10-0898371)
- Self- Decrypting / Encrypting SSL traffic

04 Threat Intelligence

- Various categories (57+9) and DB (100 million URLs)
- Real-time update via cloud type threat intelligence (AICC)
- Detailed basis for malicious URL detection

AISWG Administrator GUI



1) Monitoring and System Status
> Real-time checking system status and traffic change
> Real-time monitoring of Web service usage status by user

2) Log Analysis
> View and manage via various search options of logs that violate policy

3) Policy Setting
> User centered profile type policy setting
> Exception URL, Harmful URL / Category / Web filter

4) Statistics and Reporting
> Report on traffic status and various attack detection information such as IP, URL, user, category

Key Features of AISWG

1) Various network configuration mode
> Inline Mode : Transparent Proxy
> Out-of-path Mode : Forward Proxy, Mirroring
> Multi-Segment, Bonding

2) AICC (APPLICATION INSIGHT Cloud Center)
> Real-time threat information update through working on with AICC (its Threat Intelligence)

3) User Authentication
> Full policy setting by user even in NAT / DHCP environment with its user authentication

4) Multi-user group management
> Logically completely separated by organization, easy to set independent policy by organization

5) Encrypting / Decrypting SSL traffic
> Eliminate security threats hidden in SSL traffic using its SSL encryption / decryption, without independently

6) Network DLP
> Masking sensitive information in all traffic leaked via the web such as text, attachment

7) Control C&C server, Botnet traffic
> Block internal users' access to C&C server or Botnet (including reverse session)

8) Malware Inflow Detection
> Analyze web response traffic to detect Drive By Download, malicious script, Exploit Kit

9) Category Filter
> Accessible website control by user through 57 categories (stock, shopping, portal, etc.)

10) Malicious URL Access Control
> Block access to anonymous service, exploited site, phishing / fraud site, and malicious software

11) Bypass Connection Control
> Control access through programs such as Anonymizing VPN Services and Tor Exit Nodes for security bypass

12) Network Application Contol
> In addition to web traffic, control applications such as P2P, messenger, web hard, and cloud.

13) Commercial Webmail Service Control
> Control by detailed option (reading, writing, attachment size / extension, specific keyword, etc.) of commercial web mail service

AISWG Model & Specification (Optional Interface)

AISWG-200- Y17	AISWG-500- Y17	AISWG-1000- Y17	AISWG-2000- Y17	AISWG-4000_Y17
				
> UTP 1G x 6 > UTP 1G x 4 x 1 or Fiber 1G x 4 x 1 > SSL Acceleration Card	> Redundant Power Supply > UTP 1G x 6 > UTP 1G x 4 x 2 or Fiber 1G x 4 x 2 > SSL Acceleration Card	> Redundant Power Supply > UTP 1G x 2 and UTP 1G x 4 x 1 or Fiber 1G x 4 x 1 or 10G x 2 x 1 > UTP 1G x 4 x 1 or Fiber 1G x 4 x 3 or 10G x 2 x 3 > SSL Acceleration Card	> Redundant Power Supply > UTP 1G x 2 and UTP 1G x 4 or Fiber 1G x 4 or Fiber 10G x 2 > UTP 1G x4 x 7 or Fiber 1G x 4 x 7 or 10G x 2 x 7 > SSL Acceleration Card	> Redundant Power Supply > UTP 1G x 2 and UTP 1G x 4 or Fiber 1G x 4 or Fiber 10G x 2 > UTP 1G x4 x 7 or Fiber 1G x 4 x 7 or 10G x 2 x 7 > SSL Acceleration Card

MONITORAPP
APPLICATION SECURITY LEADER

MONITORAPP Co., Ltd.
www.monitorapp.com
Email | sales@monitorapp.com

Copyright 2019 MONITORAPP Co.,Ltd. All rights reserved.
S/N : #G1001110