

APPLICATION *i*NSIGHT SWG

Intelligent Secure Web Gateway | *ai*swg



AISWG : Application Insight Secure Web Gateway

AISWG protects internal users from various web-based threats using complete web protocol analysis and network application control fitted for your business needs.

AISWG eliminates security blind spots and decreases the workload of other security appliances through SSL/TLS decryption.

Why Do You Need a Web Gateway?

For business efficiency

- > Access to non-work-related sites can decrease productivity.
- > Provide visibility into internal user's internet activities and control access
- > Prevent data leaks by internal users
- > Secure blind spots created by unauthorized network path
- > Follow the IT compliance for an information protection system

To protect against threats and encrypted traffic

- > Rise in usage of HTTPS, SMTPS, POP3S, FTPS has increased the popularity of SSL/TLS encryption
 - 20% increase (yearly) in encrypted traffic usage
- > More and more cyber threats are being hidden in the encrypted traffic
 - 80% of APT attacks are delivered in encrypted traffic
 - A malware infection can happen just by an AD banner click
 - Companies unknowingly access malicious files and web services
- > Increased usage of HTTP/2 and TLS 1.3



Real-time
URL Filtering



Application
Filtering



Anti-malware



WEB DLP



Bandwidth
Optimization



Comprehensive
Reporting

Key Benefits of AISWG

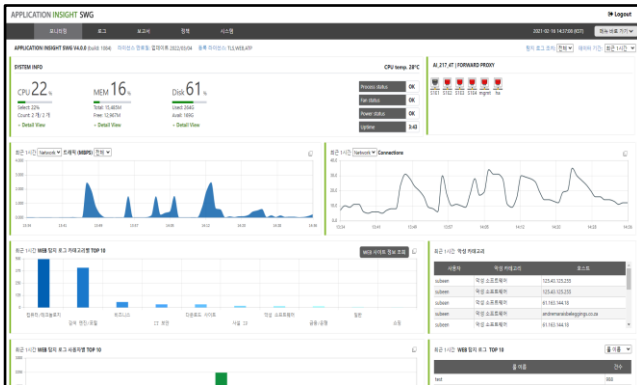
Secure web control and visibility

- > Analyze request traffic to block malicious & non-work-related URL access
 - Provide over 70 URL filtering categories for easy policy management
- > Analyze response traffic to block malware intrusion
- > Malware analysis, detection, and block via AV, static, dynamic, and reverse engineering.
- > Controls popular webmail services by function
- > Block proxy and VPN programs trying to bypass the SWG
- > Over 1,100 network application (social media, messenger, game, Office 365, Google Apps) detection and filtering
- > WEB DLP with attachment control by keyword and regular expression
- > YouTube filtering by content
- > Web caching and QoS for web service quality improvement

Convenient Appliance Management and operating

- > No need to reconfigure the existing network with the full transparent proxy mode
- > SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3 support and encrypted traffic auto-recognition
 - Supports various encryption algorithms such as RSA, DH, DHE, etc.
- > Supports ALPN (Application-Layer Protocol Negotiation)
- > Supports NAT (Network Address Translation) configuration
- > Supports asynchronous network traffic configuration
- > Certificate distribution and management
 - Distinguish clients with certificates installed. If not installed, direct them to the installation page
 - Automatic certificate installation management using NAC
- > Regularly updated PKP (Public Key Pinning) list

AISWG Administration GUI

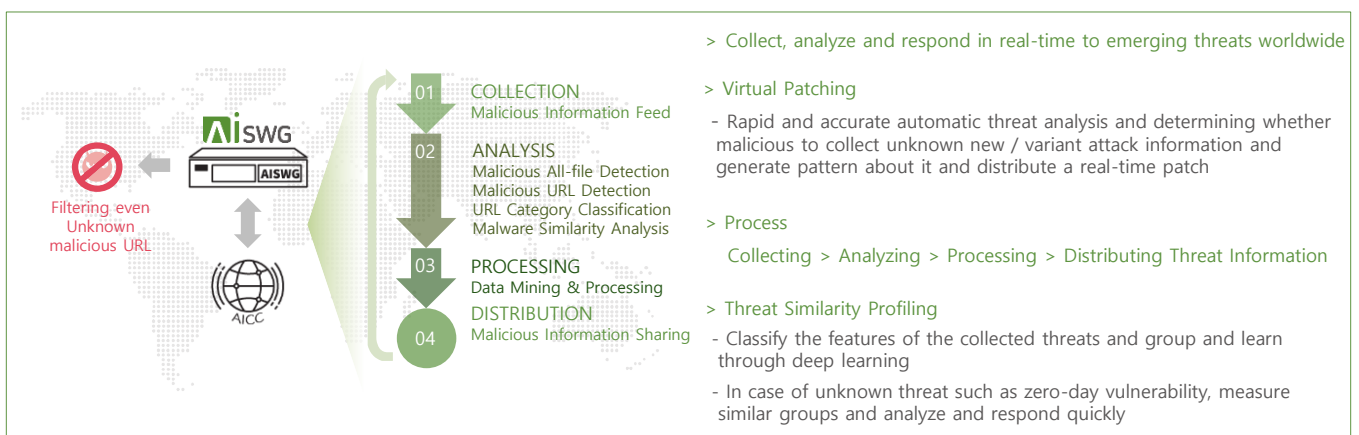


- 1) System Monitoring
 - > Real-time system status and traffic data
- 2) Log Analysis
 - > Detailed log with various search options
 - > Web access history by client
- 3) Policy Setting
 - > Granular policy setting by users or by group
- 4) Statistics and Reporting
 - > A detailed report with key variables such as traffic, IP, URL, users, categories, etc.

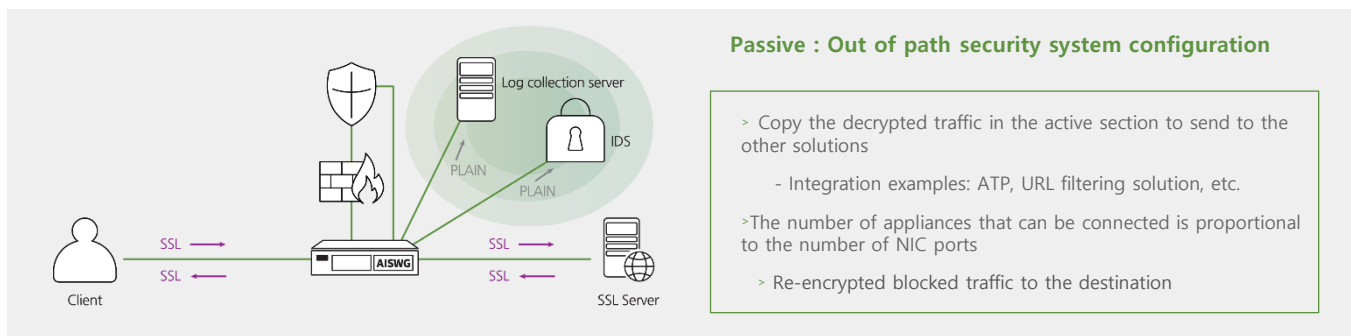
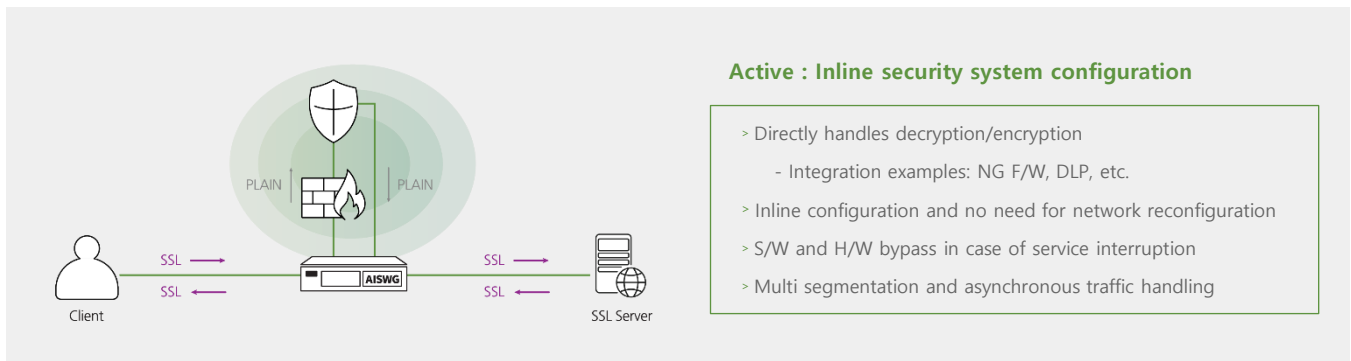
Key Features of AISWG

- 1) Various network configuration mode
 - > In-line: Full transparent proxy
 - > Out-of-path: Forward proxy, mirroring
- 2) Optimized network integration
 - > No need to reconfigure the existing network with the full transparent proxy mode
 - > Maintains the original form of the TCP session flawlessly link with other security solutions
- 3) Threat intelligence platform
 - > Real-time threat and category information update
 - > Machine learning-based URL and file analysis
- 4) Standard SSL/TLS traffic processing
 - > SSL3.0, TLS1.0, TLS1.1, TLS1.2, TLS1.3
- 5) Support various algorithms
 - > RSA, DHE, EDH, Camellia
 - > AES, DES, SEED, 3DES, RC4
 - > MD5, SHA-1, SHA-2
- 6) Full HTTP/2 Support
 - > Full HTTP/2 connections and parsing
 - > Provides the same security features as HTTP/1.1
- 7) Full access logging
 - > Web connection history on all the users
- 8) Category filter
 - > Easy website control setting with over 60 category filters (Stocks, shopping, gaming, social media, etc.)
- 9) Web DLP
 - > Prevent data leak through deep packet inspection
 - > Create rules with various conditions such as keywords, regular expressions, file extensions, and sizes
- 10) Webmail control
 - > Full webmail content logging (attachment included)
 - > Webmail control by features
 - Content: reading, writing, keywords, etc.
 - Attachment: extension, size, etc.
- 11) Blocking ATP attacks
 - > Block malicious URL access
 - > Filter C&C server and botnet traffic
 - > Analyze attached files and blocks malicious URL
 - > Analyze response payload to block malicious codes
 - > (Optional) Real-time file extraction and static/dynamic analysis from web traffic
- 12) Web acceleration
 - > Reduce traffic and response time through web caching
- 13) Network application Filtering
 - > Over 1,700 network applications (messenger, VPN, remote access, stocks, etc.) identification and filtering
- 14) PKP list management
 - > Secure service availability through a regularly update PKP list

AICC for Threat Intelligence



AISWG Network deployment



AISWG Models & Specifications

Specification	AISWG-200_Y20	AISWG-500_Y20	AISWG-1000_Y20	AISWG-2000_Y20	AISWG-4000_Y20	AISWG-8000_Y20
Appearance						
RAM	16GB (Max 128GB)	32GB (Max 128GB)	64GB (Max 2TB)	64GB (Max 2TB)	128GB (Max 2TB)	128GB (Max 2TB)
HDD	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
Network (Default)	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
Recommended users base on web traffic	> 100M > 200	> 500M > 1,000	> 1G > 5,000	> 1G > 10,000	> 1G > 20,000	> 1G > 40,000
Recommended web Traffic based on users	> 200M > 100	> 750M > 700	> 1G > 5,000	> 2G > 7,000	> 3G > 10,000	> 4G > 10,000
Recommended TLS traffic	> 100M	> 500M	> 1.5G	> 2.5G	> 4G	> 6G
Max WEB Throughput	> 1G	> 2G	> 5G	> 7G	> 10G	> 15G