MONITORAPP

APPLICATION INSIGHT SVA

Intelligent SSL Visibility Appliance | AiSVA

AISVA : Application Insight SSL Visibility Appliance

It is a visibility appliance that prevents security blind spots by providing visibility and reducing the load caused by the encryption traffic processing of network security systems by acting as a proxy of encryption and decryption for SSL/TLS communication.

Why Do You Need an SVA?

Encrypted traffic and Cybersecurity threats

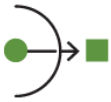
- Encrypted traffic surged due to the increased popularity of SSL/TLS such as HTTPS,
  SMTPS, POP3S, FTPS, etc.
  - 20% increase in encrypted traffic every year
- Increasing security threats hidden in encrypted traffic
  - 80% of APT attacks use encrypted traffic
- Encrypted traffic cannot be detected or security solutions are overloaded due to constantly increasing traffic
  - HTTP/2 and TLS 1.3 usage increased

Network configuration and operation

- Increasing security threats hidden in encrypted traffic
- Securing visibility of in-line security solutions such as NG F/W, DLP, IPS, and WAF
- Securing visibility of out-of-path configuration security solutions such as IDS and log collection server
- Solve the difficulties caused by the advancement of encryption traffic technology
  - RSA type Cipher-Suite usage rate decreased and DH type usage rate increased
  - Popularization of Cipher-Suite with a high level of encryption strength
  - Encrypted SNI issues, etc.

High-Performance

Full Transparent Proxy



NAT and Async Traffic

Linked system health check

PKP Management

Application type identification

Key Benefits of AISVA

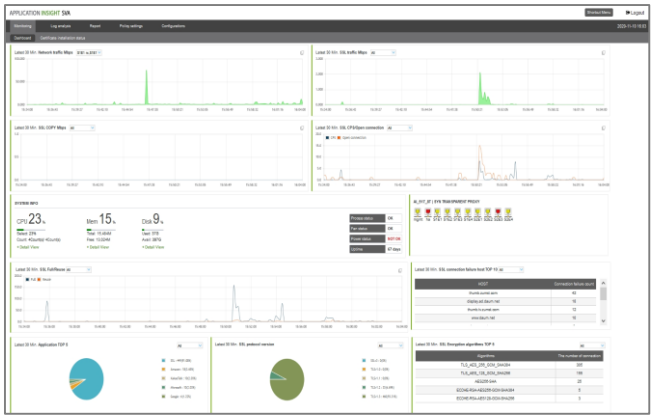
Integrated visibility

- Provides Full Transparent Proxy mode that does not affect the existing network
  - Configuration for internal server protection
    : visibility of inbound traffic
  - Configuration for internal user protection
    : Visibility of out-bound traffic
  - Copy decrypted traffic and transmit it to security solutions
- Supports SSL3.0, TLS 1.0, TLS1.1, TLS1.2, TLS1.3 and automatically identifies encrypted traffic
- Supports various encryption algorithms such as RSA, DH, DHE
- Classifies application types of encrypted traffic such as Office365, IOS, Google APP, etc.
- Automatic detection of invalid certificates
- Supports ALPN(Application-Layer Protocol Negotiation)
- Supports NAT(Network Address Translation) network environment
- Supports for asynchronous traffic network environment

Easy management and operation

- Intuitive integrated dashboard such as traffic, decryption success/failure, negotiation protocol version, Cipher-Suite statistics status, etc.
- Automatic bypass when a problem occurs in the security system linkage section
- Decrypted data body logging
- Display of the reason for negotiation failure for a session that failed to decrypt
- Distribution and management of certificates for outbound
  - Identify the certificate installation client and redirect the installation page
  - Automatic update of certificate installation status through NAC
- Certificate management for inbound
  - Supports Multi-domain Certificate and various file extensions
  - Automatic synchronization of the Cipher-Suite list with the server to be decrypted
  - Certificate expiration notification and automatic bypass setting on the expiration
- Online update of PKP(Public Key Pinning) list

AISVA Administration GUI



1) System Monitoring
> Real-time system status, traffic processing, and status monitoring

2) Log Analysis
> Easy log inquiry through various search conditions
> Logging of body and application type for decrypted data

3) Policy Setting
> Intuitive policy setting by classifying outbound and inbound menus

4) Statistics and Reporting
> Statistics and reports on various contents such as traffic, decryption performance, bypass session, full handshake, and reuse rate

Key Features of AISVA

1) Optimize network compatibility
> Full-transparent proxy : no need to change the existing network configuration
> Completely maintains the TCP session information to seamlessly interwork with various heterogeneous security solutions

2) Active Zone
> Provides visibility to inline security solutions such as NG F/W, DLP, IPS, and WAF
> Active: Proxy operation in SSL/TLS session to perform encryption/decryption processing

3) Passive Zone
> Provides visibility to out-of-path security solutions such as URL Filtering, IDS, and log collection server
> Passive: A method of copying the decrypted traffic in the active zone and delivering it to the security solution

4) Support Standard SSL/TLS traffic
> SSL3.0, TLS1.0, TLS1.1, TLS1.2, TLS1.3

5) Supports various encryption algorithms
> RSA, DHE, EDH, Camellia
> AES, DES, SEED, 3DES, RC4
> MD5, SHA-1, SHA-2

6) Network Application content identification
> Identifies the encrypted traffic's application type, such as, Office 365, Google APP, Amazon, MSN, etc.

7) PKP list management
> Provide an online update of the application and domain list that cannot be decrypted by Public Key Pinning

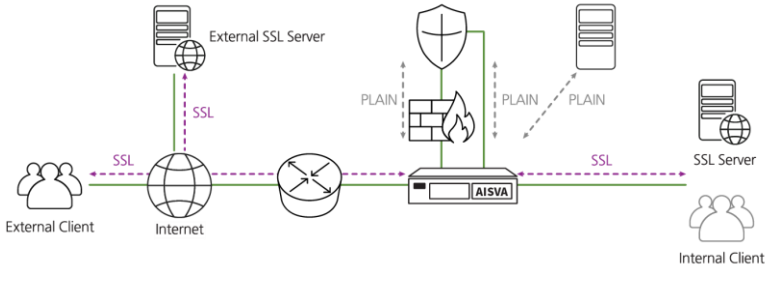
8) Health check for active zone
> Active zone abnormality detection and bypass through health check

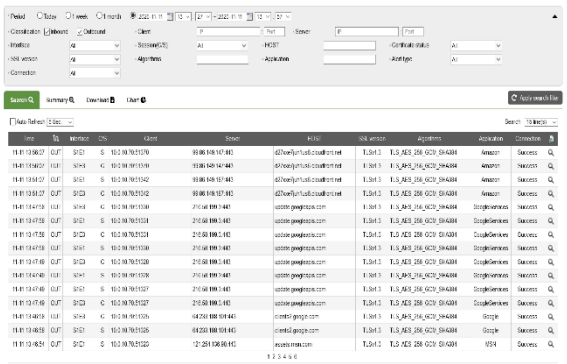
9) NAT environment support
> Session identification and encryption/decryption even if NAT (Network Address Translation) occurs in the active zone

10) Various operation convenience
> Real-time integrated dashboard
> Provision of contents essential for the operation
- Logging with Payload for decryption session
- Logging of failed sessions and reason
- Logging of bypass sessions and reason
- Certificate install client statistics/search

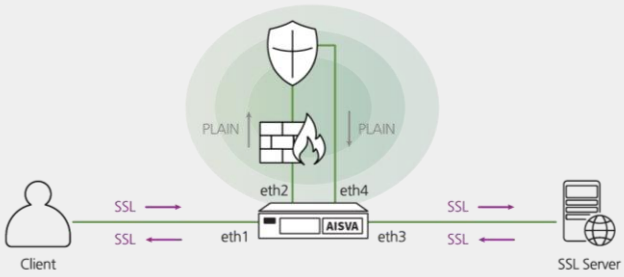
> Easy policy setting
- Automatic identification of encrypted traffic
- One-click exception handling
- Automatic policy backup and recovery
- Real-time policy synchronization between multiple systems

Standard Reference



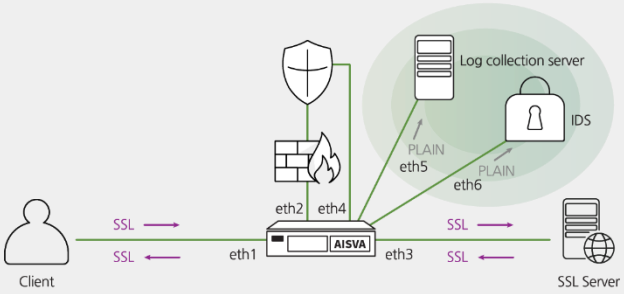


AISVA Network deployment



Active – Interworking with inline security system

- Deployed inline and no network configuration changes required
- S/W bypass and H/W bypass in case of failure
- Support Multi-segment and asynchronous traffic processing
- Decrypts encrypted traffic and transmits origin traffic to the link
- Re-encrypt the received decryption traffic and transmit it to the destination



Passive - Interworking with out of path security system

- Copy the traffic decrypted in the active zone and transmit it to the interlocking system
- Expansion of interworking target solution according to the number of physical NIC ports

AISVA Models & Specifications

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

Specification	AISVA-200_Y20	AISVA-500_Y20	AISVA-1000_Y20	AISVA-2000_Y20	AISVA-4000_Y20	AISVA-8000_Y20
Appearance						
RAM	8GB (Max 128GB)	16GB (Max 128GB)	32GB (Max 2TB)	32GB (Max 2TB)	64GB (Max 2TB)	64GB (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
CPS	> 10,000	> 20,000	> 35,000	> 50,000	> 65,000	> 80,000
TPS	> 40,000	> 70,000	> 150,000	> 200,000	> 250,000	> 350,000
Throughput	> 1G	> 2G	> 5G	> 6.5G	> 8G	> 10G

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

S/N : #F100101011