MONITORAPP

APPLICATION INSIGHT SVA

Intelligent SSL Visibility Appliance | AiSVA

AISVA : Application Insight SSL Visibility Appliance

SSL/TLS 통신에 대한 암복호화를 대행 함으로서 네트워크 보안 시스템들의 암호화 트래픽 처리에 따른 부하를 감소 시키고 가시성을 제공하여 보안 사각지대를 방지하는 가시성 어플라이언스 입니다.

Why Do You Need an SVA?

암호화 트래픽과 보안 위협

> HTTPS, SMTPS, POP3S, FTPS 등 SSL/TLS 의 일반화로 암호화 트래픽 급증

- 매년 20% 수준의 암호화 트래픽 증가 추세

> 암호화 트래픽 속에 숨겨진 보안 위협 증가

- APT 공격의 80%는 암호화 트래픽을 활용

> 암호화 트래픽 탐지가 불가하거나 지속적으로 증가하는 트래픽으로 인해 보안 솔루션들의 부하 발생

- HTTP/2 및 TLS 1.3 사용률 증가

네트워크 구성 및 운영

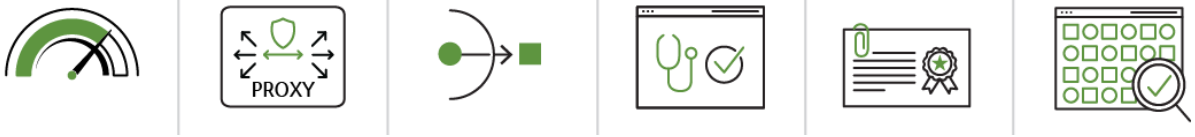
> 일원화 된 암호화 트래픽 관리 및구성

> NG F/W, DLP, IPS, WAF 등 In-line 구성 보안 솔루션의 가시성 확보

> IDS, 로그수집서버 등 Out-of-path 구성 보안 솔루션의 가시성 확보

> 암호화 트래픽 기술 발전으로 인한 애로사항 해소

- RSA 타입의 Cipher-Suite 사용률 감소 및 DH 타입 사용률 증가
- 암호화 강도 High 레벨의 Cipher-Suite 대중화
- Encrypted SNI 이슈 등



High-Performance | Full Transparent Proxy | NAT and Async Traffic | Linked system health check | PKP Management | Application type identification

Key Benefits of AISVA

완전한 가시성 확보

> 기존 네트워크에 영향 없는 Full Transparent Proxy 모드 제공

- 내부 서버 보호를 위한 구성 (In-bound 트래픽에 대한 가시성)
- 내부 사용자 보호를 위한 구성 (Out-bound 트래픽에 대한 가시성)
- 복호화 된 트래픽을 복사 하여 보안 솔루션들로 전송

> SSL3.0, TLS 1.0, TLS1.1, TLS1.2, TLS1.3 지원 및 암호화 트래픽 자동 식별

> RSA, DH, DHE 등 다양한 암호화 알고리즘 지원

> 복호화 트래픽에 대한 Office365, IOS, Google APP등 어플리케이션 유형 구분

> Invalid 인증서 자동 검출

> ALPN(Application-Layer Protocol Negotiation) 지원

> NAT(Network Address Translation) 네트워크 구성 지원

> 비동기 트래픽 네트워크 구성 지원

간편한 관리 및 운영

> 트래픽, 복호화 성공/실패, 협상 프로토콜 버전, Cipher-Suite 통계 현황 등 직관적인 통합 대시보드

> 보안 시스템 연동 구간에 문제 발생시 자동 바이패스 수행 및 서비스 가용성 확보

> 복호화 데이터 본문 로깅

> 복호화 실패 세션들에 대한 협상 실패 근거 제시

> ESM, SNMP 등 모니터링 컨텐츠 커스터마이징

> Outbound 인증서 배포 및 관리

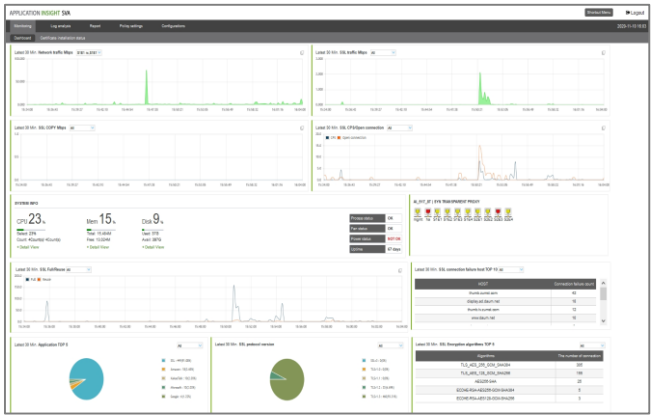
- 인증서 설치 클라이언트 식별 및 설치페이지 리 다이렉트
- NAC 연동을 통한 인증서 설치 현황 자동 업데이트

> Inbound 인증서 관리

- 멀티도메인 인증서 지원
- 다양한 확장자 지원
- 복호화 대상 서버와 Cipher-Suite 목록 자동 동기화
- 인증서 만료 사전 알림 및 인증서 만료 시 자동 바이패스 설정

> PKP(Public Key Pinning) 리스트 온라인 업데이트

AISVA Administration GUI



1) 시스템 모니터링
> 실시간 시스템 상태, 트래픽 처리 현황 모니터링

2) 로그 분석
> 다양한 검색 조건을 통한 상세 세션 로그 조회
> 복호화 데이터에 대한 본문 및 어플리케이션 유형 로깅

3) 정책 설정
> Outbound 및 Inbound 메뉴 구분으로 직관적인 정책설정

4) 통계 및 보고
> 트래픽, 복호화 수행, 바이패스 세션, Full Handshake 및 Reuse 비율 등
다양한 컨텐츠에 대한 통계 및 보고서

Key Features of AISVA

1) 네트워크 호환성 최적화
> Full Transparent Proxy 방식으로 기존 네트워크
구성 변경 불필요
> TCP 세션과 관련된 모든 형상을 유지하여 다양한
이기종 보안 솔루션과의 유기적인 연동

2) Active 구간
> NG F/W, DLP, IPS, WAF 등 인라인으로 구성된
보안 솔루션들에 대한 가시성 제공
> Active : 실제 SSL/TLS 세션에 개입하여 암복호화
처리를 대행하는 방식

3) Passive 구간
> URL Filtering, IDS, 로그수집서버 등 미러링으로
구성된 보안 솔루션들에 대한 가시성 제공
> Passive : Active 구간에서 복호화된 트래픽을
복사하여 보안 솔루션에 전달하는 방식

4) 표준 SSL/TLS 트래픽 처리
> SSL3.0, TLS1.0, TLS1.1, TLS1.2, TLS1.3

5) 다양한 알고리즘 지원
> RSA, DHE, EDH, Camellia
> AES, DES, SEED, 3DES, RC4
> MD5, SHA-1, SHA-2

6) Network Application 식별
> Office 365, Google APP, Amazon, MSN 등
암호화된 트래픽의 Application 유형 식별

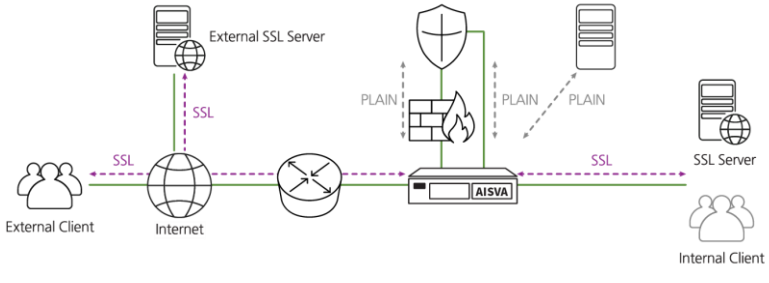
7) PKP 리스트 관리
> Public Key Pinning에 의한 복호화 불가
Application, Domain 리스트 온라인 업데이트 제공
> 관리 목록에 대한 커스터마이징 지원

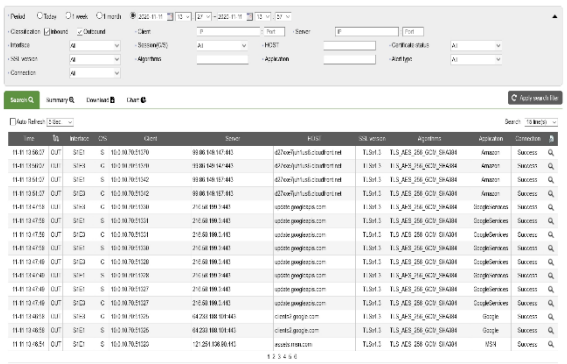
8) 구간 Health check
> Active 구간 내 Health check 트래픽을 발생하여
이상 여부 감지 및 이상 발생시 소프트웨어 바이패스 수행

9) NAT 환경 지원
> Active 구간 내 NAT(Network Address Translation) 솔루션이 배치되더라도 정상적인
세션 식별 및 암복호화 수행

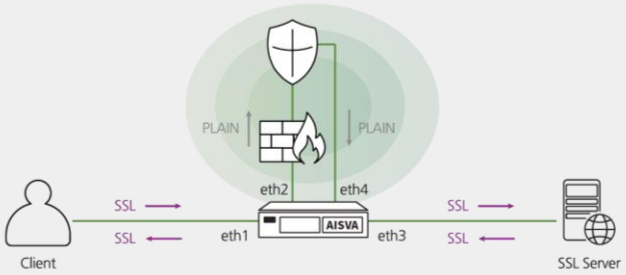
10) 다양한 운영 편의성
> 시스템 및 암호화 트래픽 처리 현황에 대한 실시간
통합 대시보드
> 운영에 필수적인 상세 컨텐츠 제공
- 복호화 세션에 대한 Payload 포함 로깅
- 복호화 실패 세션 로깅 및 근거 제시
- 바이패스 세션 로깅 및 근거 제시
- 인증서 설치 클라이언트 현황 조회
> 손쉬운 정책 설정
- 복호화 대상 트래픽 자동 식별
- One-click 예외 처리
- 정책 자동 백업 및 복구
- 다수 시스템 운영 시 실시간 정책동기화

Standard Reference



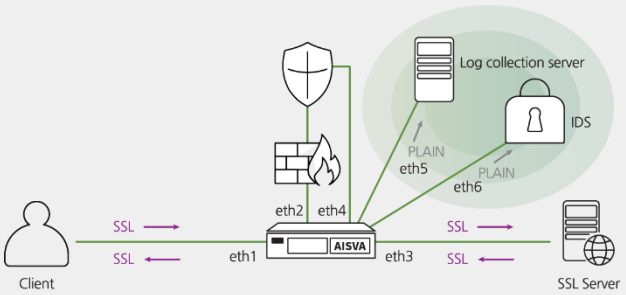


AISVA Network deployment



Active – Inline 구성 보안 시스템군 연동

> 인라인으로 배치되며 네트워크 구성 변경 불 필요
> 장애 발생시 S/W 바이패스 및 H/W 바이패스 수행
> 멀티 세그먼트 제공 및 비동기 트래픽 처리
> 암호화 트래픽 수신 시 복호화 하여 연동 구간으로 전송
> 수신된 복호화 트래픽을 재 암호화 하여 목적지로 전송



Passive – Out of path 구성 보안 시스템군 연동

> Active 구간에서 복호화 된 트래픽을 복사하여 연동 시스템으로 전송
> 보안 규칙에 의한 차단 트래픽 수신 시 재 암호화 하여 목적지로 전송
> 트래픽, 복호화 수행, 바이패스 세션, Full Handshake 및 Reuse 비율 등
다양한 컨텐츠에 대한 통계 및 보고서

AISVA Models & Specifications

- AISVA APPLIANCE의 표준 워크로드를 기반으로 작성 되었으며, 실제 성능은 워크로드 요구 사항에 따라 크게 달라질 수 있습니다.

Specification	AIWAF-200_Y20	AIWAF-500_Y20	AIWAF-1000_Y20	AIWAF-2000_Y20	AIWAF-4000_Y20	AIWAF-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
MONITORAPP CO., Ltd.
EMAIL sales@monitorapp.com
www.monitorapp.com

S/N : #F100101011