Intelligent SSL Visibility Appliance

APPLICATION **INSIGHT SVA**

MONITORAPP

Contents

1. SSL 보안의 필요성

SSL Visibility Appliance,

HTTPS, SMTPS, POP3S, FTPS 등 SSL/TLS 트래픽의 일반화로,
암호화 트래픽은 급증하는데 반해 기존 네트워크 보안장비들은 SSL 트래픽 탐지가 불가하거나 지속적으로 증가하는 암호화 트래픽을 감당하기 어려운 상황 입니다.

SVA 솔루션은 이로 인해 발생되는 보안 위협 문제점 제거 목적으로,
SSL/TLS 트래픽에 대한 암복호화 역할을 대행 하여, 네트워크 보안 시스템을 비롯 IDS, 로그 수집 서버와 같은 보안 솔루션에 가시성을 제공하는 SSL/TLS 트래픽 암복호화 전용 솔루션 입니다.

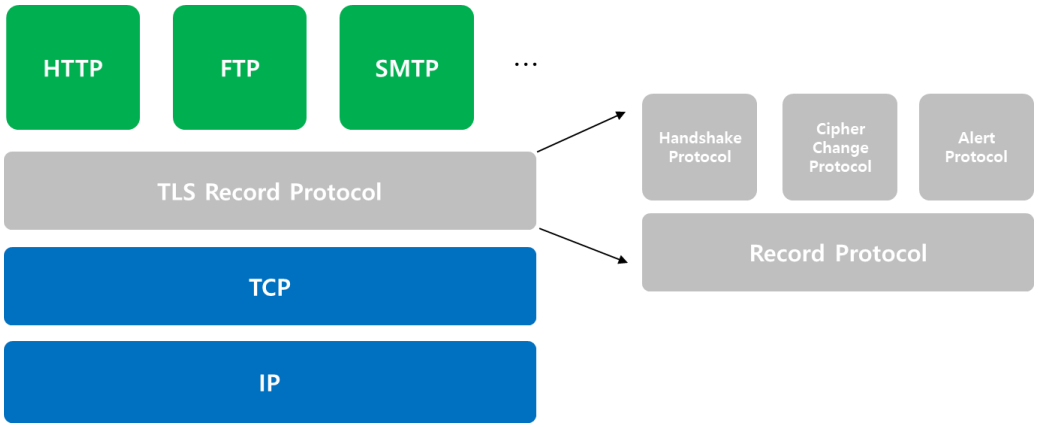
SSL/TLS

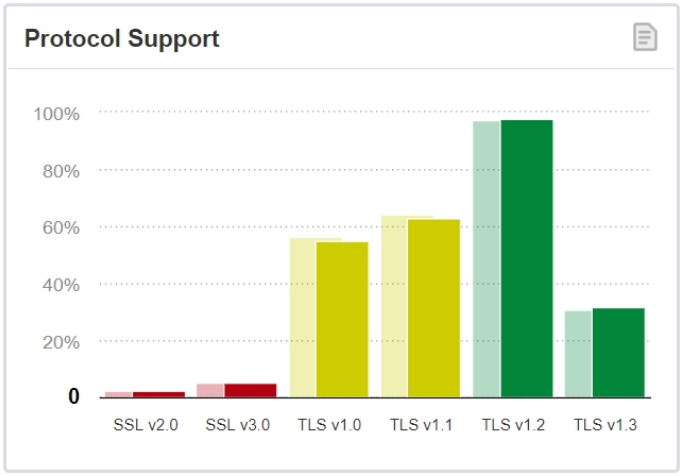
■ SSL (Secure Socket Layer)

- 웹 서버와 브라우저 간의 안전한 통신을 위해 개발 (Netscape , 1993)
- 세션계층에서 적용되며, 어플리케이션 데이터의 안전성 보장
- SSL 2.0 deprecated(`11, RFC 6176) , SSL 3.0 deprecated(`15, RFC 7568)

■ TLS (Transport Layer Security)

- SSL 3.0 이 표준화된 이후 IETF에서 TLS 프로토콜 표준화 (1996, SSLv3.1)
- SSL 3.0 기반(계승) 업그레이드 프로토콜
- TLS 1.3까지 발표 (RFC 8446, 2018.08)





- SSL Labs

SSL/TLS

■ 전송 계층(Transport Layer)의 암호화

- TCP/IP 네트워크를 사용하는 통신에 적용
- 전송계층 종단간 보안과 데이터 무결성 확보
- 전송계층의 암호화 방식이므로, HTTP 외 FTP, SMTP 등 다양한 응용계층 프로토콜에서 사용

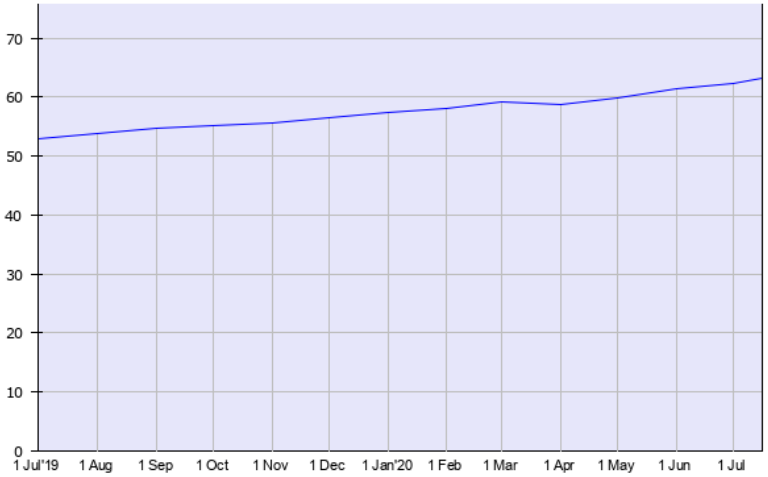
프로토콜	Well-Known Port	Description
HTTPS	443/TCP	HTTP over TLS/SSL
NNTPS	563/TCP	NNTP over SSL
LDAPS	636/TCP	LDAP over SSL
FTPS-DATA	989/TCP	FTP over SSL
TELNETS	992/TCP	Telnet over SSL
IMAPS	993/TCP	IMAP over SSL
IRCS	994/TCP	IRC over SSL
SMTPS	465,587/TCP	SMTP over TLS/SSL
POP3S	995/TCP	POP-3 over SSL
SUUCP	4031/TCP	UUCP over SSL
AMQPS	5671/TCP	AMQP protocol over TLS/SSL
SYSLOG-TLS	6514/TCP	Syslog over TLS
SIP-TLS	5061/TCP	SIP over TLS

암호화 트래픽의 지속적인 증가

■ 암호화 트래픽 사용률 현황

- 전체 네트워크 트래픽의 25~35% 차지
- `20 HTTPS 트래픽은 80% 예상
- HTTP/2 사용률 증가

Default protocol https is used by 63.1% (2020. 07)



Usage of Default protocol https for websites, 16 Jul 2020, W3Techs.com

- w3techs.com

■ APT 공격에 암호화 트래픽 사용량 증가

- APT 공격의 약 80%가 암호화 트래픽 사용

■ 보안 장비의 약 20% 만이 완전한 복호화 수행

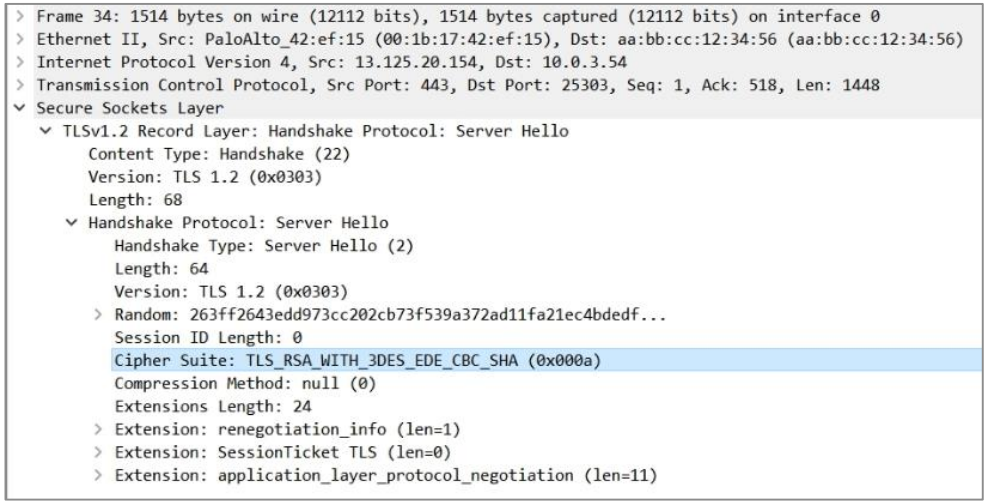
- 암호화 강도 High 레벨의 Cipher-Suite 대중화로 보안시스템 성능 저하
- ECC 타입 인증서 도입 증가
- TLS 1.3 사용률 증가
- Out-bound 보안 솔루션의 경우 복호화 불가

Changes in https (TLS 1.3 – RFC8446)

■ 데이터센터 내 암호화 트래픽 가시성 확보의 한계

- Static RSA and Diffie-Hellman cipher suites have been removed; all public-key based key exchange mechanisms now provide forward secrecy.

- TLS1.3 부터 RSA 키 교환 타입 Cipher-Suite 미 지원 (DH 키 교환 타입 Cipher-Suite만 사용)
- IDS, 로그수집서버와 같이 Sniffing 타입의 보안시스템은 암호화 트래픽 복호화 불가

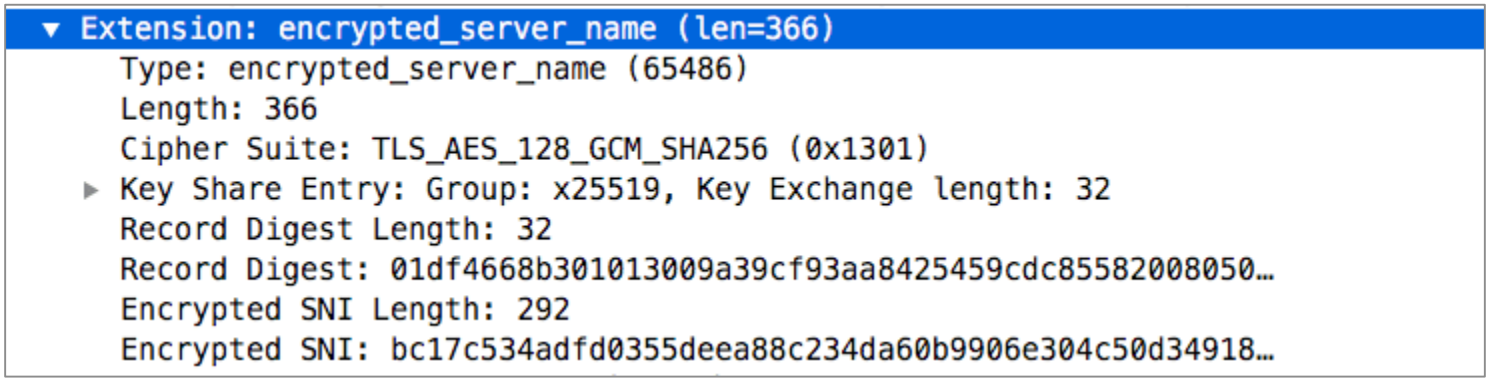


Changes in https (Encrypted SNI for TLS 1.3 - draft-ietf-tls-esni-06)

■ 데이터센터 내 암호화 트래픽 가시성 확보의 한계

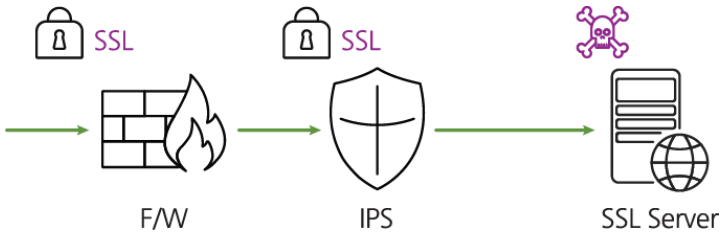
- ECHO works by encrypting the entire ClientHello, including the SNI and any additional extensions such as ALPN. This requires that each provider publish a public key and metadata which is used for Client Hello encryption for all the domains for which it serves directly or indirectly (via Split Mode).

- SSL Handshake 과정 내 SNI(도메인 정보) 필드 암호화
- 도메인 정보 확인 불가에 따라 기존 보안 장비들의 SNI 필드에 의거한 보안 정책 무효화



기존 보안시스템의 한계

■ 도입 이전

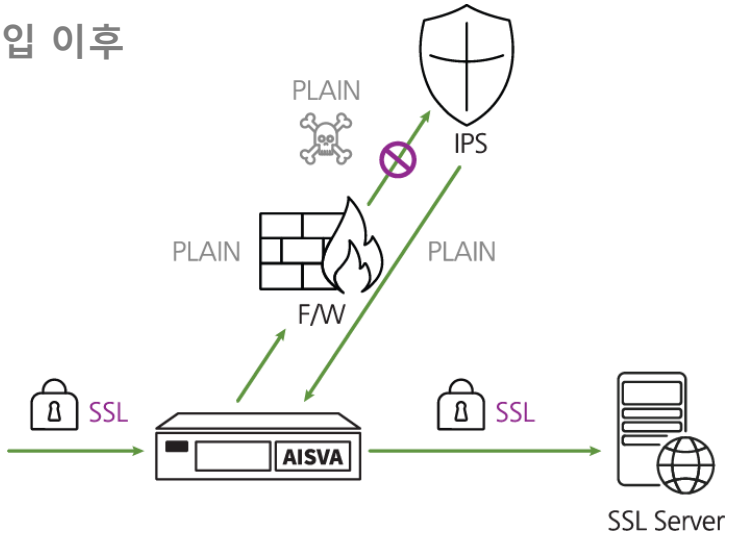


① 암호화 트래픽 복호화 미 수행
- 복호화 기능 부재, 시스템 과부하 등

② 암호화 트래픽은 기존 보안시스템 구간통과

③ 침해 사고 발생

■ 도입 이후



① AISVA가 암호화 트래픽 복호화 수행

② 복호화 평문 트래픽을 보안시스템 구간으로 전송

③ 보안 정책 통과된 평문 트래픽은 AISVA가 수신

④ AISVA가 재 암호화 하여 서버 전송

2. APPLICATION INSIGHT SVA
소개 및 특장점

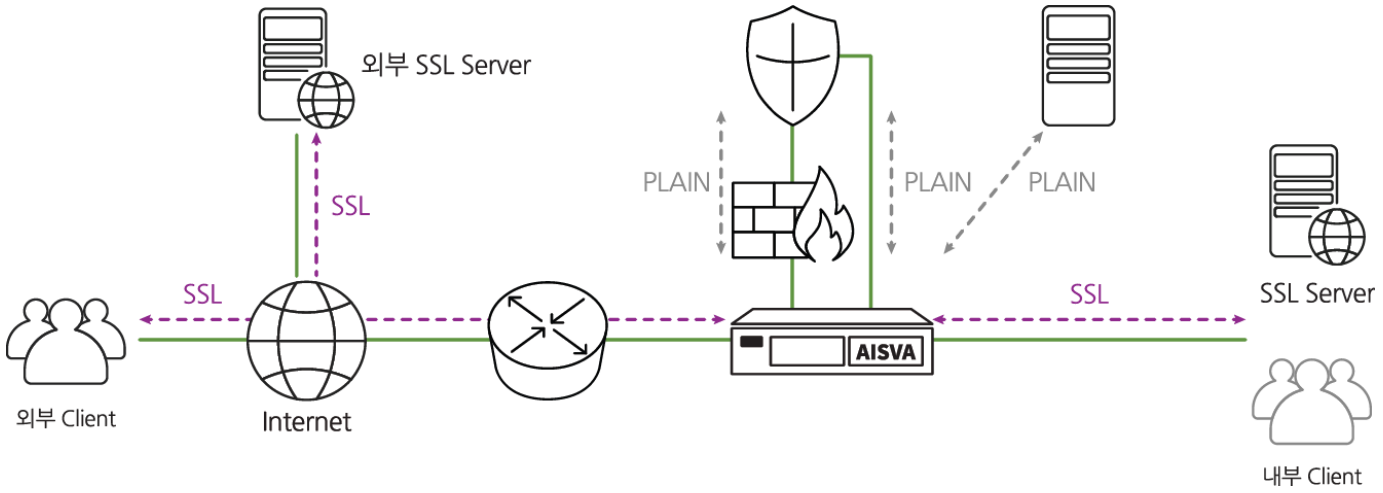
Proxy base Full Transparent 모드

■ 별도의 IP 부여 없이 Stealth-mode로 운영

- 기존 네트워크 구성 환경 변화 및 영향도 없음

■ Inbound / Outbound 양방향 트래픽 처리

- In-bound : 외부에서 내부 SSL Server로 유입 되는 트래픽 (서비스 구간 DMZ/IDC 보안 강화)
- Out-bound : 내부에서 외부 SSL Server로 유출 되는 트래픽 (내부 사용자 구간 보안 강화)



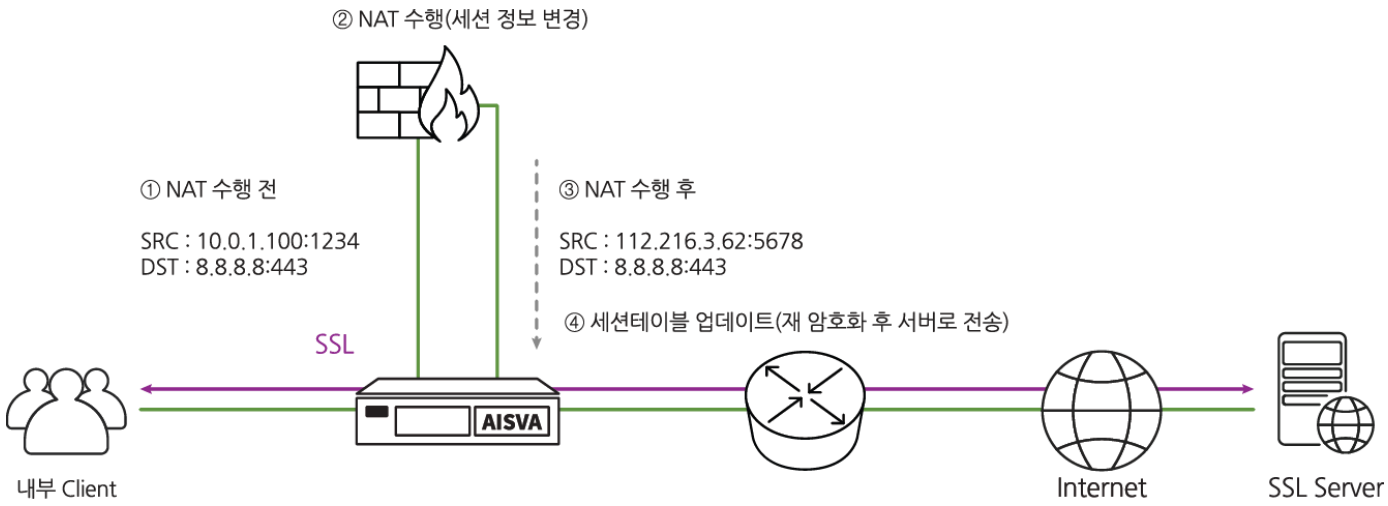
다양한 네트워크 구성 지원

■ NAT(Network Address Translation) 환경 지원

- Active Inline 구간에 NAT 와 같이 세션정보가 변경되는 보안장비 구성 및 연동

■ 비동기 트래픽 환경 지원

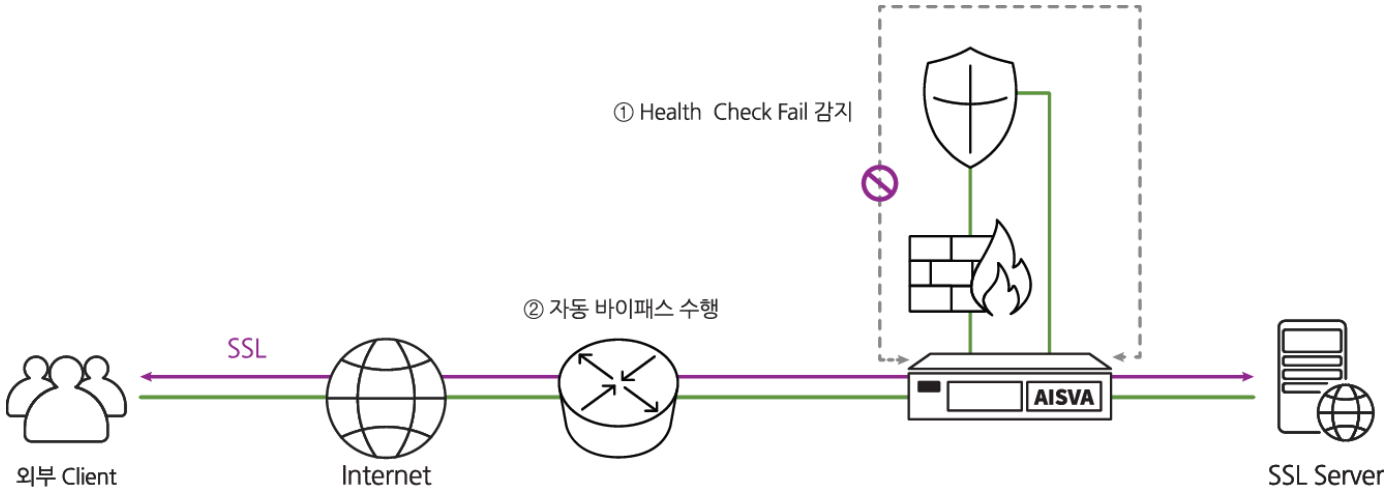
- 단일 장비 멀티 세그먼트 구성에서 발생하는 비동기 트래픽 처리
- 이중화 구성에서 발생하는 비동기 트래픽 처리 (세션 포워딩)



보안시스템 연동 구간 Health Check

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

- ICMP 또는 IPX 트래픽을 이용한 Active 구간 Health Check
- Health Check Fail 시 Active 구간 트래픽 바이패스 수행



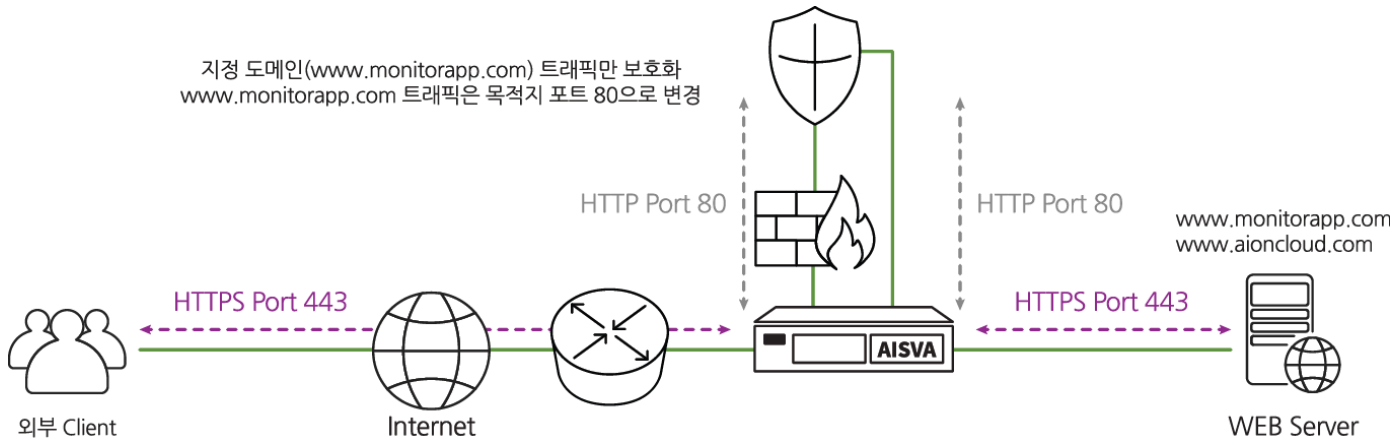
목적지 포트 변경 및 지정 도메인만 복호화

■ 목적지 포트 변경 기능

- 투명한 세션처리를 위한 5-Tuple(Src IP, Dst IP, Src Port, Dst Port, Transport Type) 유지
- 서비스 포트 기반으로 프로토콜을 인식하는 보안 시스템을 위해 목적지 Port 변경(Port Conversion) 설정

■ 지정 도메인에 대한 선별적 암복호화

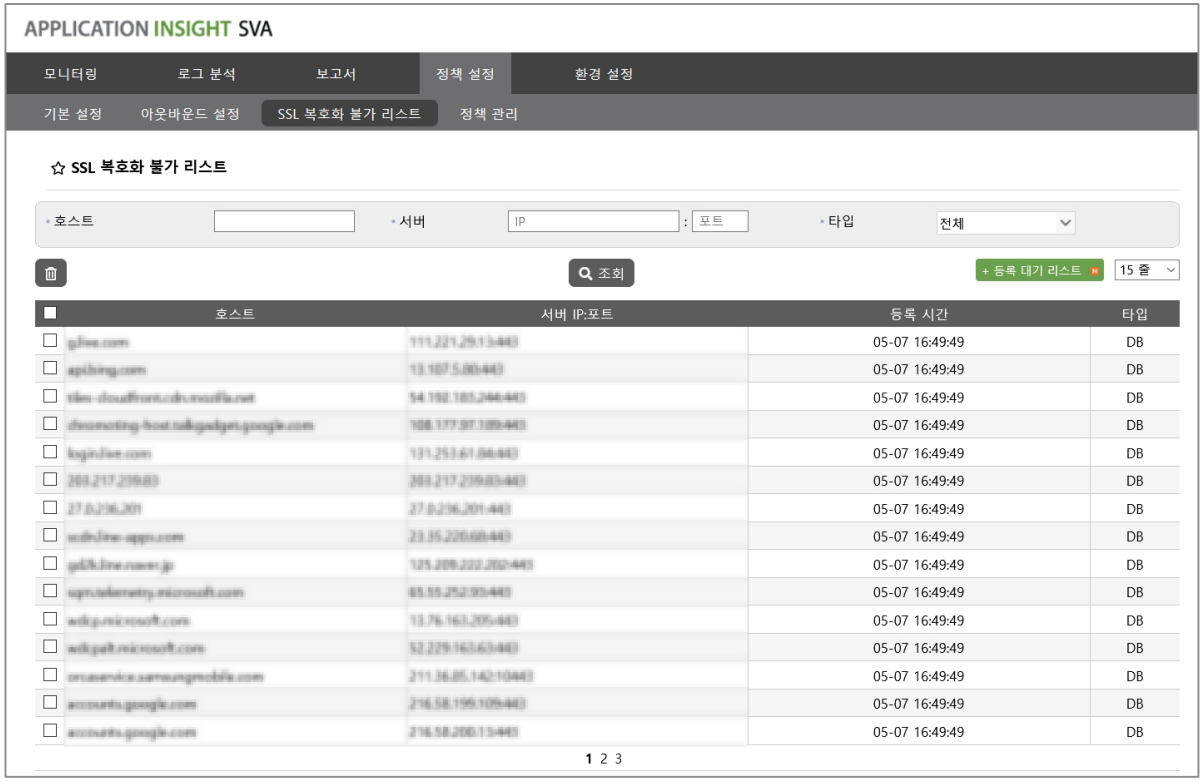
- 동일 서버(IP:PORT)에서 여러 개의 웹 서비스(Virtual Host)를 제공하는 경우 특정 도메인만 지정하여 복호화 수행



PKP(Public Key Pinning) 대응

■ 인증서 Pinning 서비스 대응

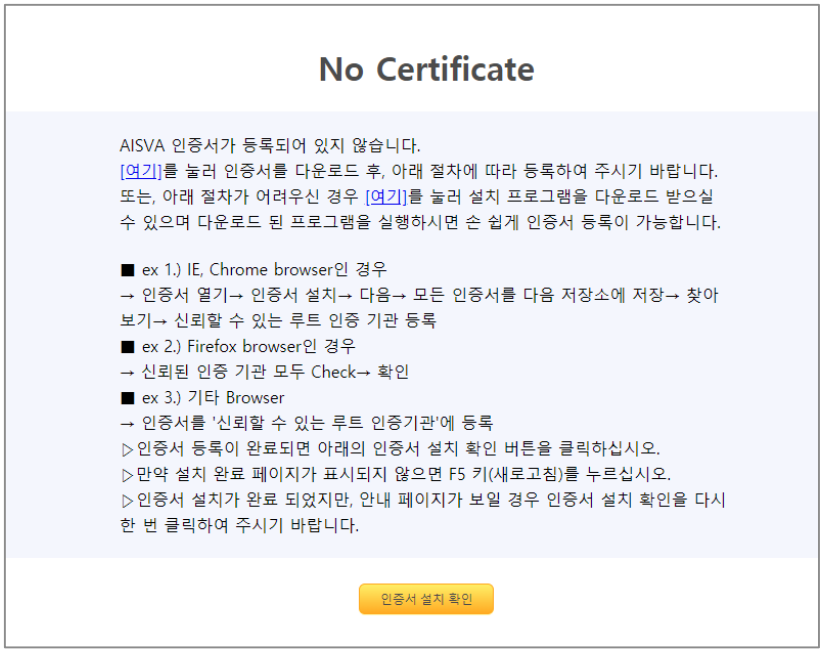
- 클라이언트가 협상을 통해 다운로드 받은 인증서가 실제 서버의 인증서와의 동일 여부 검증 (EX: 카카오톡, 윈도우 업데이트 등)
- Certification Pining 에 따른 SSL 통신 불가 세션에 대한 자동 학습 및 관리
- 시스템 자체 학습 외 PKP 리스트 온라인 DB 업데이트 제공

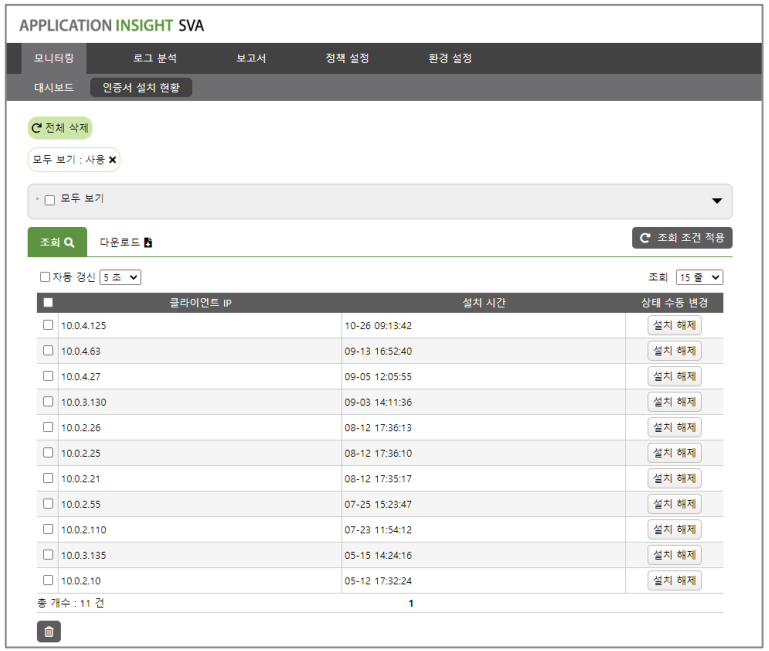


손쉬운 인증서 배포 및 현황 관리

■ SSL 인증서 설치를 위한 인증서 배포페이지 리 다이렉트

- 인증서 미 설치 클라이언트는 인터넷 접속 시, 설치 가이드라인이 기재된 페이지로 강제 리 다이렉트
- PMS 나 NAC을 통한 인증서 설치 시, 인증서 미 설치 클라이언트는 설치 시점까지 지속 바이패스 시키는 옵션 제공





Invalid SSL 인증서 검출

■ SSL 협상에 사용되는 인증서가 Invalid 인증서인 경우 해당 세션 차단

- Invalid 인증서는 주로 악용된 웹 사이트에서 빈번하게 발생
- 사설 인증서, 유효 기간 만료, 웹 사이트 주소와 발급된 인증서 주소 미 일치, 인가되지 않은 CA 등 다양한 유형의 Invalid 인증서 검출

유연하고 손 쉬운 HTTPS 트래픽 관리

■ HTTPS 설정 및 관리로 인한 장애 포인트 최소화

- TLS 1.3 지원
- 멀티도메인 인증서 지원
- 다양한 확장자 지원(인증서 변환 과정 불 필요)에 따른 간편한 인증서 등록
- 실제 웹 서버 활성화 Cipher-Suite 목록과 동기화(자동 설정)
- 인증서 만료 사전 알림 및 인증서 만료 시 자동 바이패스 기능

APPLICATION INSIGHT SVA Line-UP

Specification	AISVA-200_Y20	AISVA-500_Y20	AISVA-1000_Y20	AISVA-2000_Y20	AISVA-4000_Y20	AISVA-8000_Y20
Appearance						
RAM	8GB (최대 128GB)	16GB (최대 128GB)	32GB (최대 2TB)	32GB (최대 2TB)	64GB (최대 2TB)	64GB (최대 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	8 Slot - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port	8 Slot - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port	8 Slot - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port	8 Slot - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port
CPS	10,000	16,000	29,000	47,000	55,000	94,000
TPS	45,000	72,000	145,000	225,000	280,000	489,000
Throughput	2G	2G	6.7G	10.3G	13.3G	20G
CC	100,000	200,000	400,000	400,000	840,000	842,000

- Slot에 NIC 모듈을 선택/조합하여 장착할 수 있으며, SSL 가속카드를 옵션으로 장착 가능 합니다.
- 본 제품의 사양은 성능향상을 위하여 예고 없이 변경될 수 있습니다.
- 성능 수치는 계측기 프로파일 및 환경에 따라 차등적 일 수 있습니다. 계측 환경은 APPLIANCE SHEET 정보를 참고하시기 바랍니다.

3. APPLICATION INSIGHT SVA
주요 기능

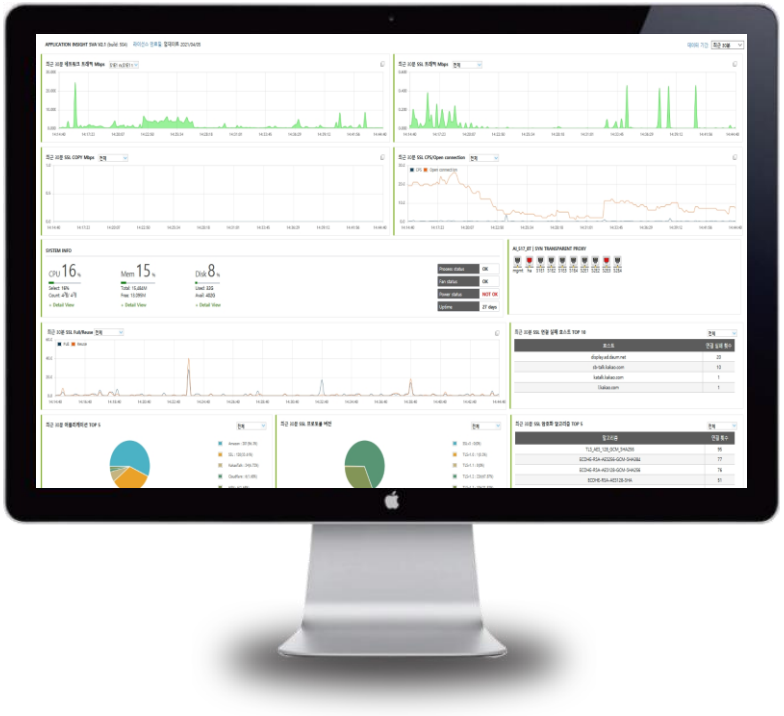
APPLICATION INSIGHT SVA 주요 정책 (요약)

Policy	Functions	Details
모니터링	네트워크 트래픽	네트워크 트래픽 및 암호화 트래픽에 대한 모니터링
	시스템 상태	시스템 리소스 및 인터페이스 상태 모니터링
로그	SSL 세션 로그 조회	인 바운드 / 아웃 바운드 암 복호화 수행 이력에 대한 로그 조회 및 저장
	바이패스 로그 조회	바이패스 설정에 따른 인 바운드 / 아웃 바운드 트래픽 바이패스 이력 로그 조회 및 저장
	감사 로그 조회	시스템 관리자의 시스템 설정 및 변경에 대한 운영 이력 로그 조회 및 저장
보고서	SSL 트래픽 보고서	네트워크 및 암호화 트래픽 운영 현황 보고서
정책	기본 설정	정책 동기화, 루트 인증서 관리, 인증서 만료 알림 등 시스템 운영을 위한 기본 설정
	복호화 대상 지정	인 바운드 서버 등록 및 관리, 아웃 바운드 복호화 대상 관리
	Passive Mirror	복호화 된 암호화 트래픽을 복사 및 전송하기 위한 Passive 포트 설정
	SSL 복호화 불가 리스트	암 복호화 불가(실패) 서버, 웹 사이트에 대한 학습 및 관리
	바이패스 관리	암 복호화 제외(바이패스) 대상 IP 또는 URL 설정 및 관리
환경설정	관리자 설정	시스템 관리자 설정(패스워드, 메뉴 별 권한, 접근 IP 등)
	시스템 설정	IP, 시간 동기화, 타임 존 등 설정

APPLICATION INSIGHT SVA 주요 정책

Monitoring

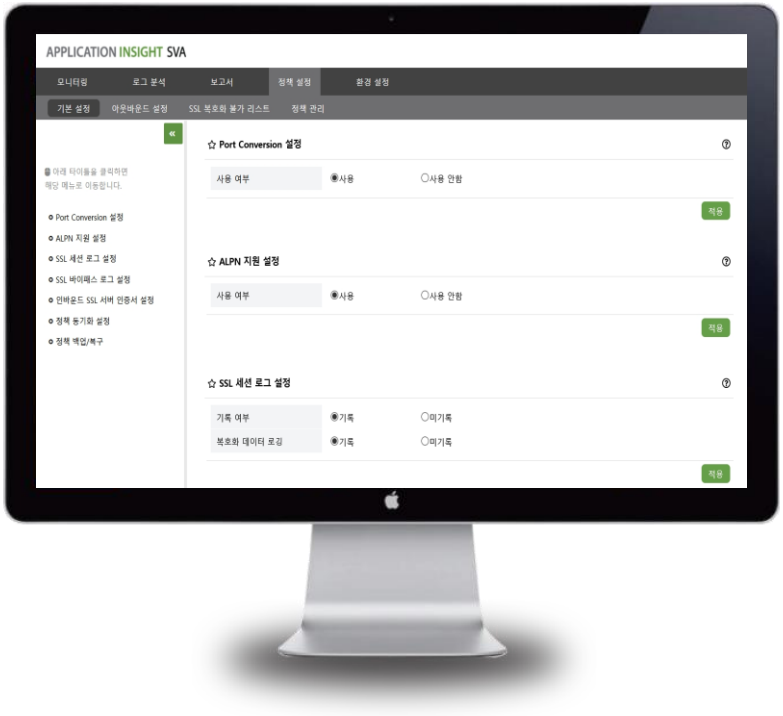
- 시스템, 트래픽, 복호화 현황에 대한 모니터링
  - 네트워크 트래픽
  - SSL 트래픽
  - SSL Copy 트래픽
  - CPS
  - Open Connection
  - Full Handshake / Reuse Session
  - 어플리케이션 유형 통계
  - 프로토콜 버전 통계
  - 암호화 알고리즘 통계
  - 연결 실패 호스트 목록
  - 시스템 리소스



APPLICATION INSIGHT SVA 주요 정책

Policy - Default

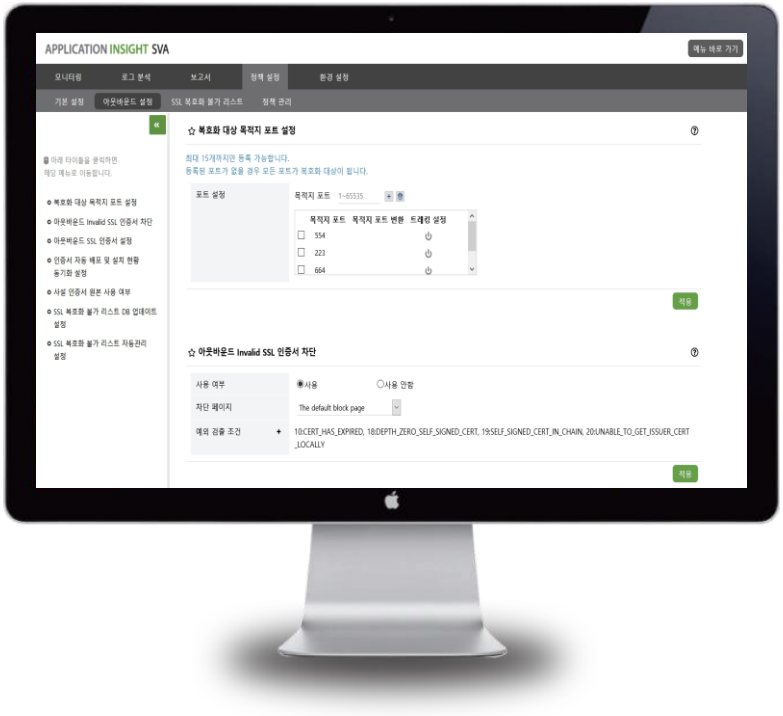
- Port Conversion 설정
  - 복호화 트래픽의 목적지 포트 변경 기능
- ALPN 지원 설정
  - ALPN 확장 헤더 유지 또는 삭제 설정
- SSL 세션 로그 설정 / SSL 바이패스 로그 설정
  - 세션 로그 / 바이패스 로그 로깅 여부 설정
- 인 바운드 SSL 서버 인증서 만료 설정
  - 인증서 만료 트래픽에 대한 자동 바이패스 설정
- 정책 동기화 설정
  - 정책 변경 시 실시간 동기화 대상 설정
- 정책 백업/복구
  - 정책 변경 시 자동 백업 대상 설정
  - 현재 정책 수동 백업 / 복원



APPLICATION INSIGHT SVA 주요 정책

Policy – Out bound

- 복호화 대상 목적지 포트 설정
  - 지정된 대상(포트)만 복호화 수행
  - 지정 시 트래픽 자동 선별 기능 Disable
- Invalid 인증서 차단
  - Expire, Revoke, Self Signed 등의 인증서 탐지
- SSL 인증서 설정
  - 협상에 사용될 Root 인증서 등록 및 관리
- 인증서 자동 배포 및 설치 현황
  - 인증서 배포 페이지 리 다이렉트 기능 설정
  - 인증서 배포 현황 모니터링
- 복호화 불가 리스트
  - 온라인 DB 업데이트 관리
  - 자체 학습 시 기준치 설정



APPLICATION INSIGHT SVA 주요 정책

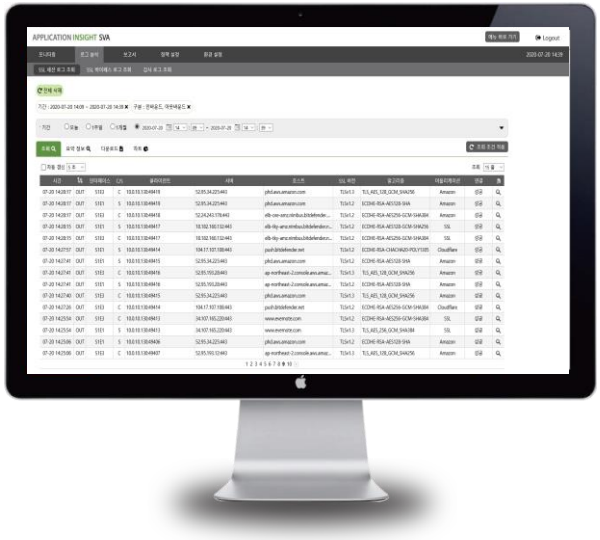
Policy – Operating

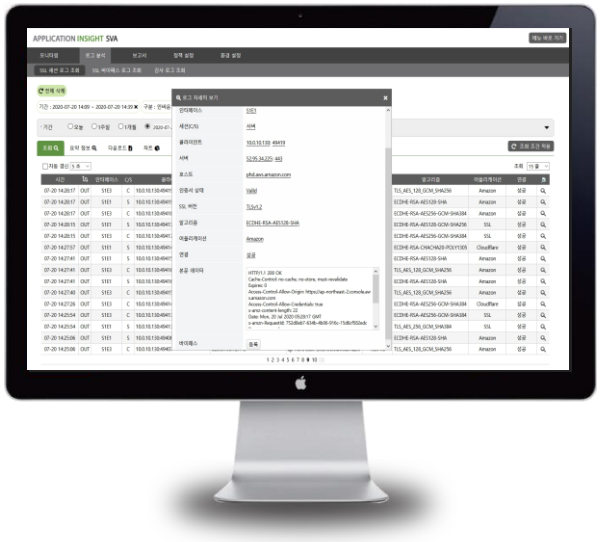
- 복호화 대상 지정
  - 인 바운드 SSL 서버 등록 및 관리
- 바이패스 관리
  - 인 바운드 IP 바이패스
  - 아웃 바운드 IP 바이패스
  - 아웃 바운드 URL 바이패스
- Passive Mirror
  - 복호화 트래픽에 대한 Passive 설정
  - 출발지/목적지 인터페이스, 목적지 포트, RX/TX

APPLICATION INSIGHT SVA 주요 정책

Session Log

- 암 복호화 수행 SSL/TLS 트래픽 정보 로깅
  - 시간
  - 트래픽 방향(IN / OUT)
  - 인터페이스
  - 클라이언트 IP:PORT
  - 서버 IP:PORT
  - 호스트
  - SSL 버전
  - 알고리즘
  - 어플리케이션 유형
  - 복호화 및 연결 결과(성공 / 실패)
  - 본문 데이터

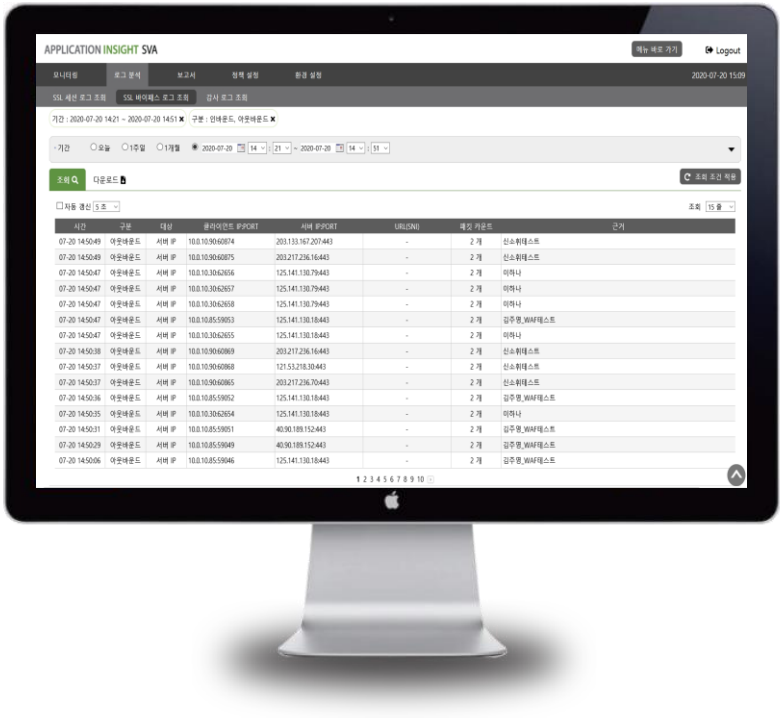




APPLICATION INSIGHT SVA 주요 정책

Bypass Log

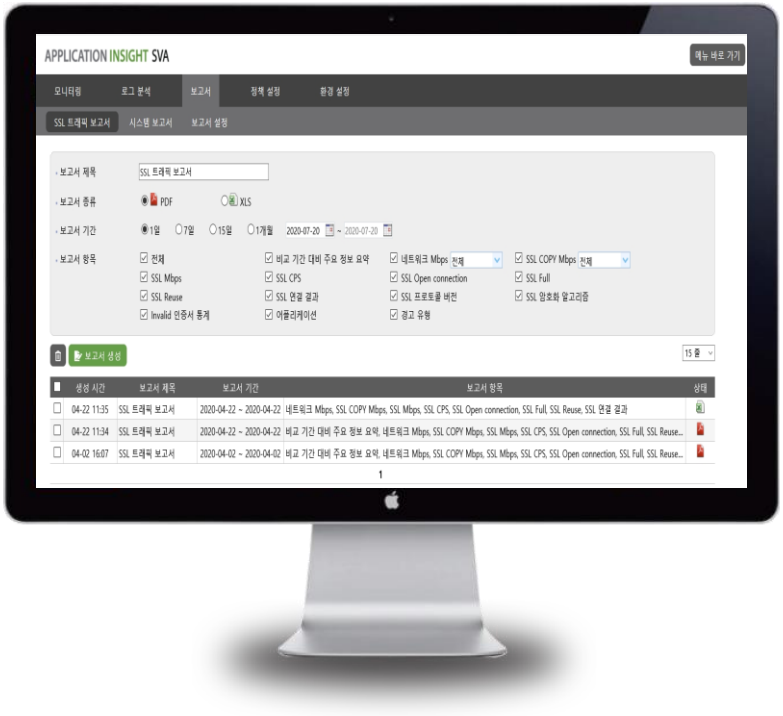
- 바이패스 수행 암호화 트래픽 정보 로깅
  - 시간
  - 트래픽 방향(IN / OUT)
  - 클라이언트 IP:PORT
  - 서버 IP:PORT
  - URL(SNI)
  - 근거



APPLICATION INSIGHT SVA 주요 정책

Report

- 보고서 생성 (PDF / XLS)
  - 비교 기간 대비 주요 요약 정보
  - 네트워크 트래픽
  - SSL/TLS 트래픽
  - CPS
  - Open Connection
  - Full Handshake / Reuse Session
  - 복호화 및 연결 결과(성공 / 실패)
  - 연결 실패 근거
  - 프로토콜 버전 통계
  - 알고리즘 통계
  - Invalid 인증서 통계
  - 어플리케이션 유형 통계

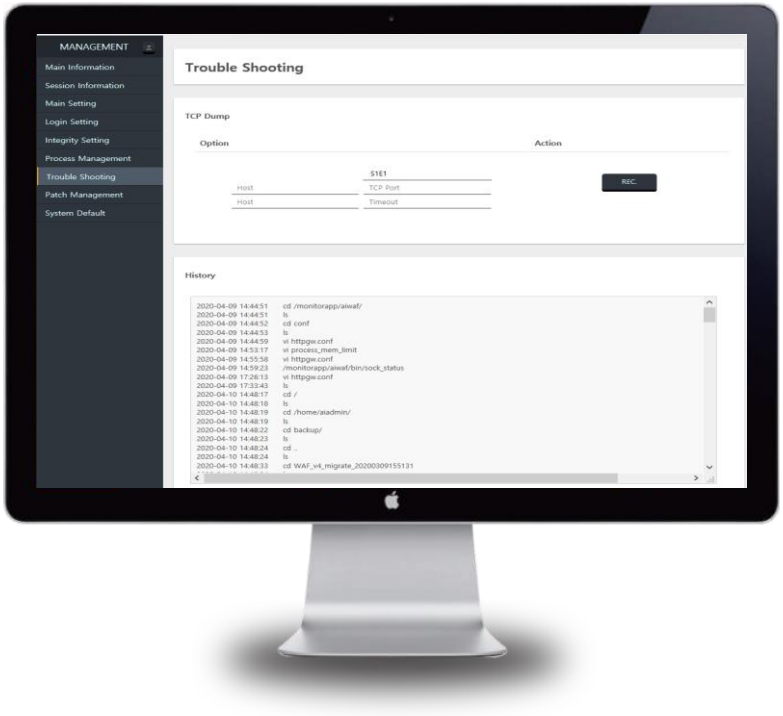


APPLICATION INSIGHT SVA 주요 정책

Trouble Shooting (AIMANAGER)

- 고급 관리자를 위한 제품 관리 및 트러블 슈팅 목적의 별도 인터페이스

  - 제품 패치
  - 제품 초기화
  - 긴급 복구 모드
  - 패스워드 초기화
  - Debug Log 수집
  - TCPDUMP 수집
  - 이슈 분석에 필요한 주요정보 자동 수집
  - 중요 설정 값 변경 및 조회

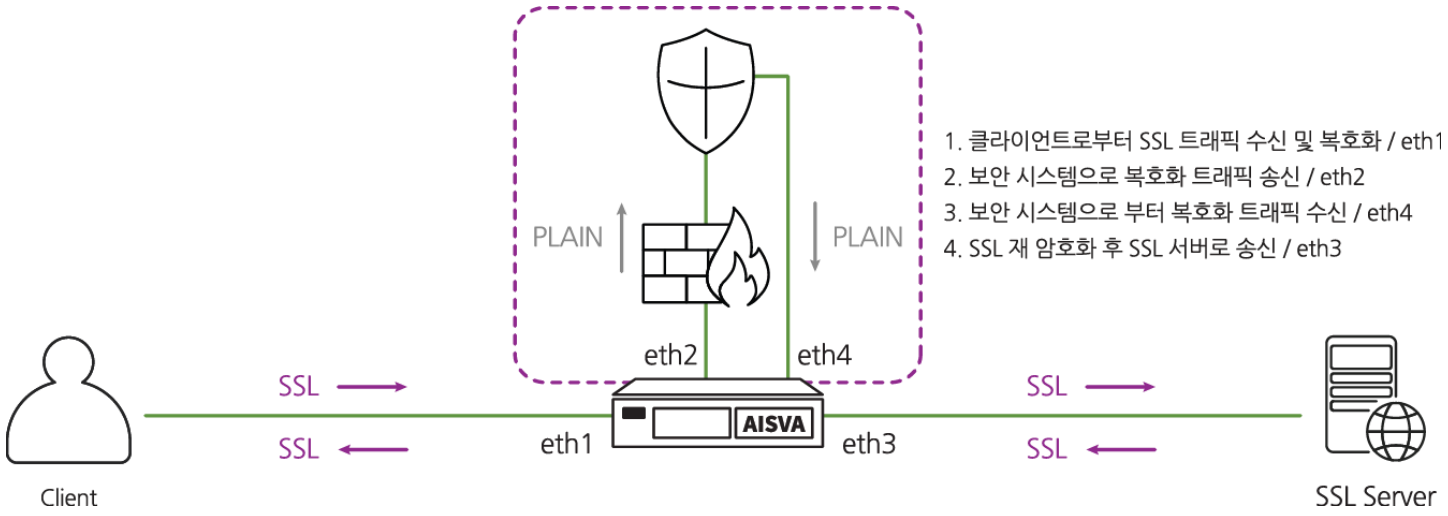


4. 구축 방안 및 사례

다양한 구성 방식

Deployment – Active

- 가장 범용적으로 사용되는 운영 모드
- 보안 시스템군을 Active 구간 내 인라인 배치 하여 복호화 트래픽을 송수신 하기 위한 구성

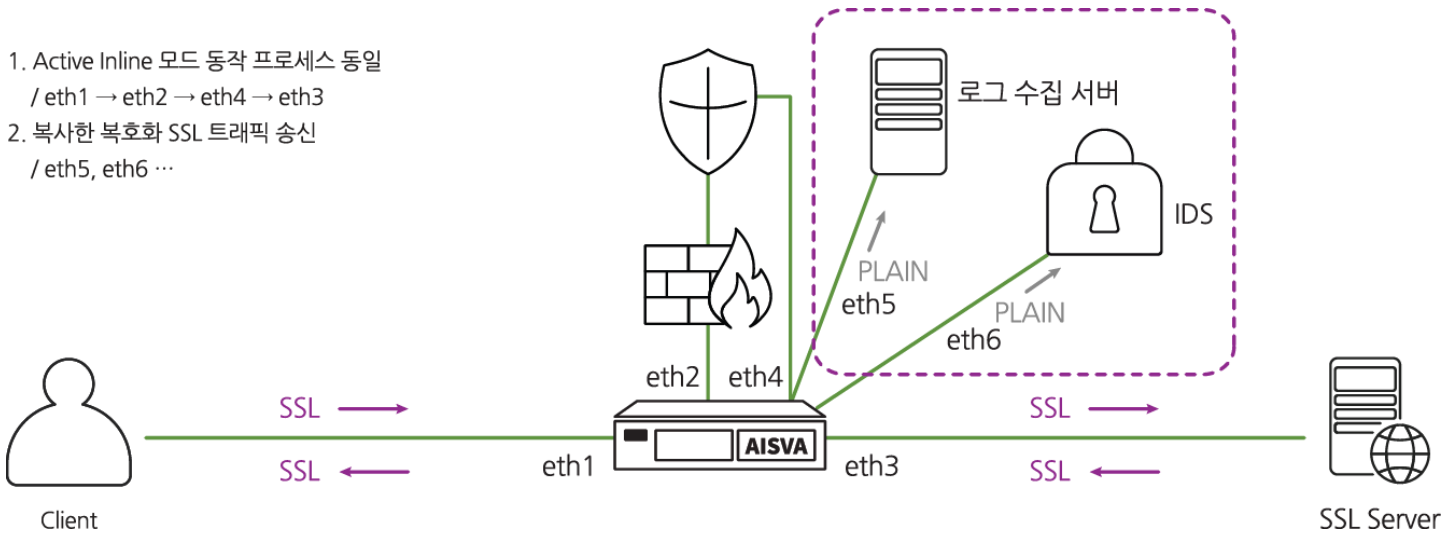


다양한 구성 방식

Deployment – Passive

- Out of Path로 구성된 보안 시스템에 복호화 된 트래픽을 전송하기 위한 모드(송신 전용)
- Active Inline 모드와 Passive Inline 모드 동시 사용 가능

1. Active Inline 모드 동작 프로세스 동일
   / eth1 → eth2 → eth4 → eth3
2. 복사한 복호화 SSL 트래픽 송신
   / eth5, eth6 …

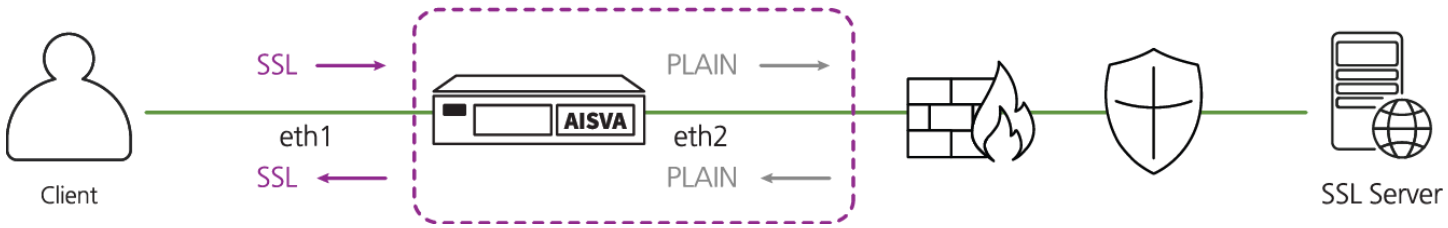


다양한 구성 방식

Deployment – SSL Offload

- 클라이언트 사이드는 SSL/TLS 통신하고 서버 사이드는 PLAIN으로 통신
- HTTP 요청에 대한 HTTPS Redirection 기능 제공 [선택 옵션]

1. Client에서 요청한 SSL 트래픽에 대한 복호화 수행 / eth1
2. 복호화 된 평문 트래픽 Server로 전송 / eth2
3. 수신된 평문 응답 트래픽 암호화 수행 / eth2
4. 암호화된 SSL 트래픽 Client로 전송 / eth1

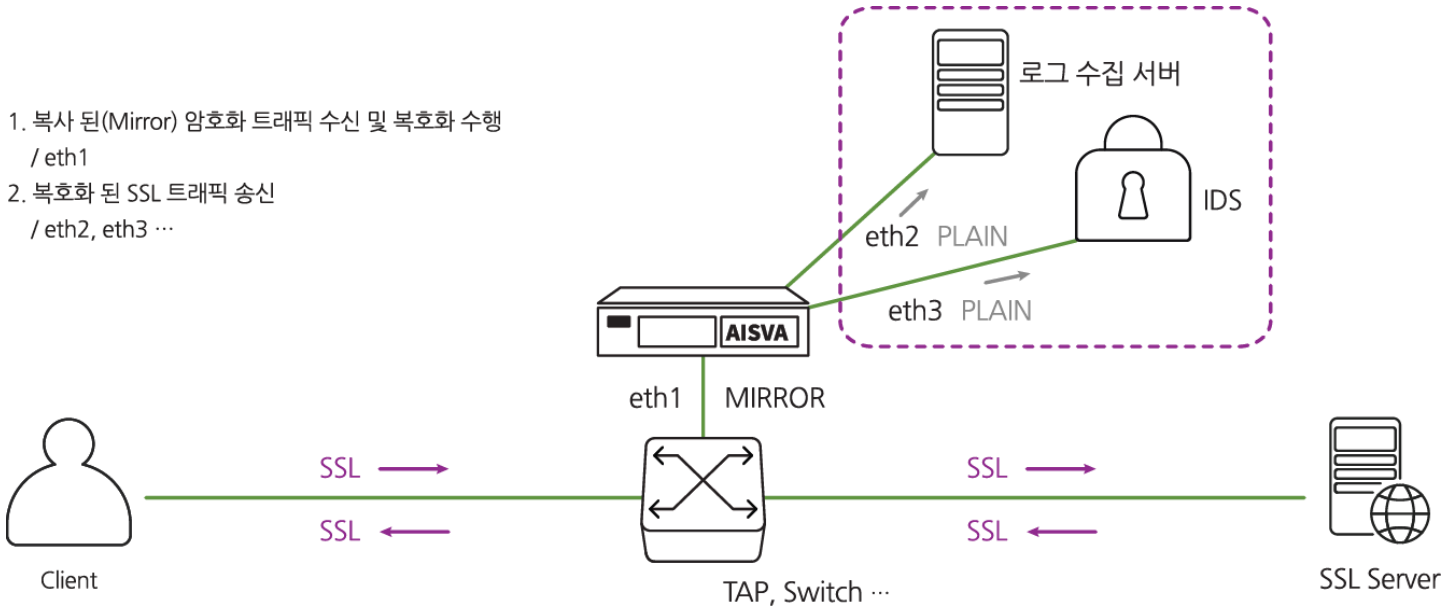


다양한 구성 방식

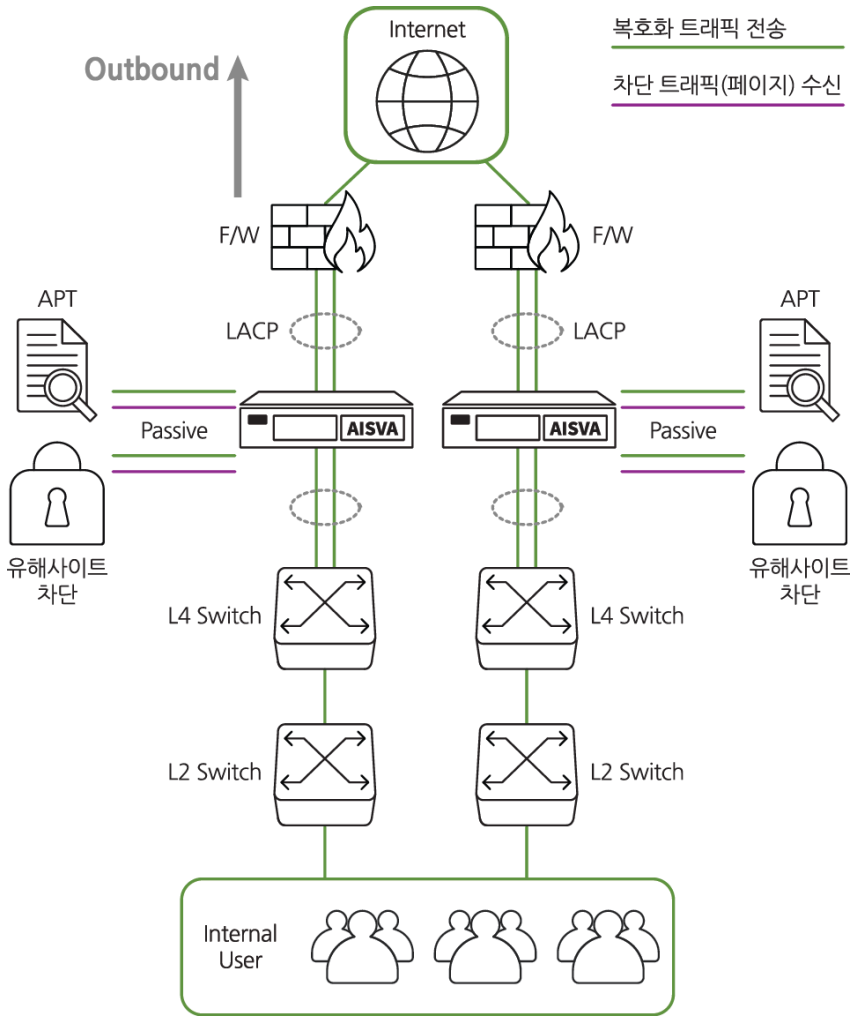
Deployment – Mirror

- Out of Path로 구성된 보안 시스템에 복호화 된 트래픽을 전송하기 위한 모드(송신 전용)
- 인라인 구성이 아닌 Mirror 방식으로 구성 되며, 복사(Mirror) 트래픽 수신 및 복호화 수행
  - RSA 타입 SSL 트래픽만 암복호화 지원

1. 복사 된(Mirror) 암호화 트래픽 수신 및 복호화 수행
   / eth1
2. 복호화 된 SSL 트래픽 송신
   / eth2, eth3 …



구축사례 (J 교육청)



Overview

- 대용량 암호화 트래픽 구간 및 LACP 환경 지원
  (네트워크 트래픽 10G 이상, 암호화 트래픽 5G 이상)
- APT 솔루션 및 유해사이트 차단 솔루션에 암호화 트래픽 가시성 제공

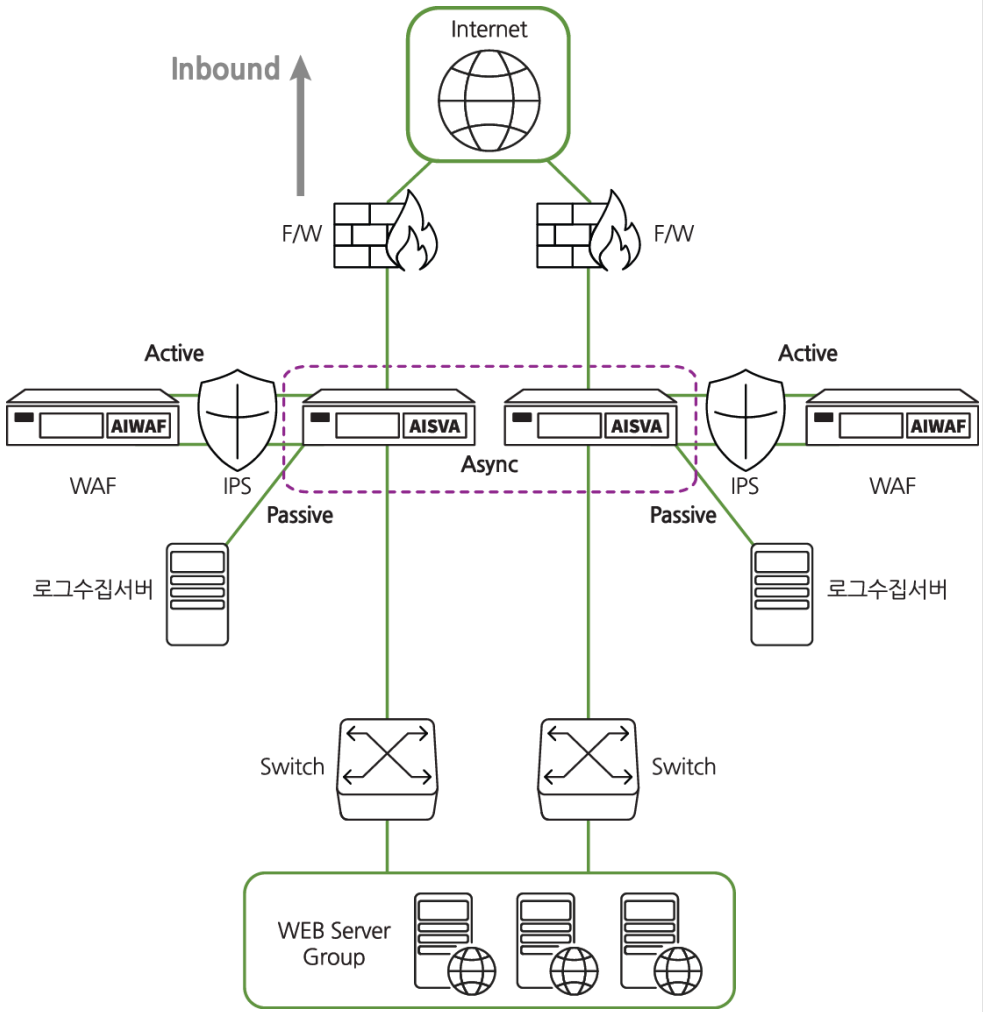
Deployment

- 각 보안 시스템 별 복호화 트래픽 전송용 인터페이스, 차단 트래픽(페이지) 수신 용 인터페이스 연결
- 인증서 자동 배포 페이지 Redirect 기능 활성화

Effectiveness

- 기존 네트워크 구성 변경 없이 사용자 인터넷 구간 내 대용량 암호화 트래픽 가시성 확보(구성 및 보안 시스템군 정책 변경 불필요)
- 내부 사용자에게 RST 패킷을 통한 단순 세션 차단방식에서 악성/비 업무 사이트 접속 시 차단페이지 제공을 통한 차단 근거 가시성 제공
- HTTPS 트래픽 외 SSL/TLS 암호화된 사용자 어플리케이션 유형(KakaoTalk, GoogleDocs, Skype 등) 모니터링

구축사례 (K 은행)



Overview

- 기존 네트워크 구성(비동기 트래픽 환경) 및 보안 정책 유지
- 웹 서비스 TLS1.3 도입에 따른 IPS, WAF, 로그 수집 서버에 암호화 트래픽 가시성 제공
- Inline 구성 시 시스템 Fault 발생 대비한 H/W 바이패스 지원

Deployment

- Inbound (Active - IPS, WAF / Passive – 로그수집서버)
- 비동기 트래픽 네트워크 환경 지원을 위한 AISVA 시스템간 Async 케이블 연결 및 세션포워딩 기능 활성화

Effectiveness

- 기존 네트워크 구성 변경 없이 IDC 내 암호화 트래픽 가시성 확보 (구성 및 보안 시스템군 정책 변경 불필요)
- 인증서 만료 사전 알림 및 만료 시 바이패스 기능을 통해, 다수의 관리 대상 서버(약 200여대)에서 인증서 만료로 인한 Risk 절감

THANK YOU

㈜모니터랩 | 주소 : 서울시 구로구 디지털로 27가길 27 아남빌딩 9층 08375 | Tel : 02-749-0799 | Fax : 02-749-0798 | Web : www.monitorapp.com
E-mail : sales@monitorapp.com | 사업자등록번호 : 214-87-66413 |