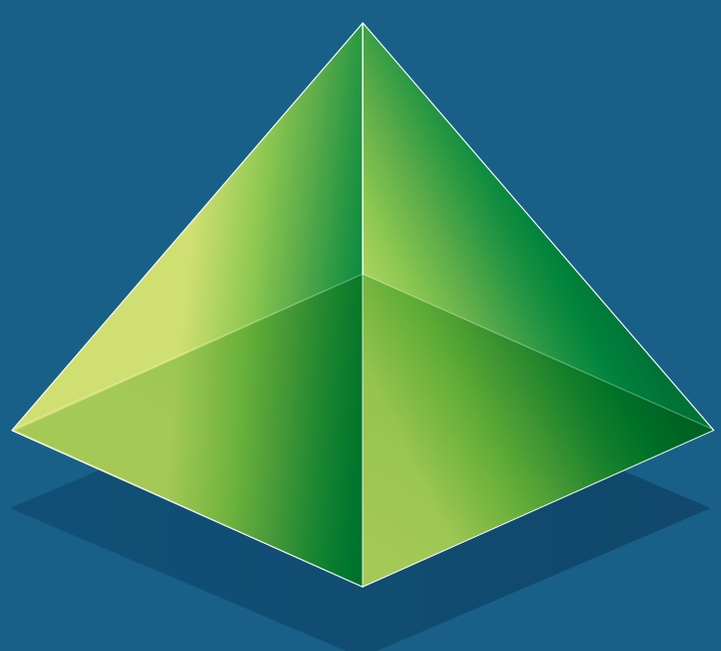
Prism SSL VA

암호화 트래픽 관리의 시작,
모든 트래픽에 대한 가시성을 확보하는
복호화 솔루션



SOOSAN INT

ePrism SSL VA

금융

IBK기업은행
수호천사 동양생명
KDB산업은행
한국은행
MIRAE ASSET 미래에셋생명
Sh BANK
예가람저축은행 Yegaram Savings Bank
산업은행계열 KDB생명
Heungkuk 흥국화재
SBI 저축은행

공공 / 교육

책임운영기관 국가정보자원관리원
KLID 한국지역정보개발원 Korea Local Information Research & Development Institute
국세청 National Tax Service
통일부
해양수산부
국토교통부
KGC인삼공사
캠코 한국자산관리공사
Incheon Airport
한국전력
경상북도교육청 Gyeongsangbuk-do Office of Education
VERITAS LUX MEA
KMU 국민대학교 KOOKMIN UNIVERSITY
LH 한국토지주택공사
SSiS 사회보장정보원 SOCIAL SECURITY INFORMATION SERVICE

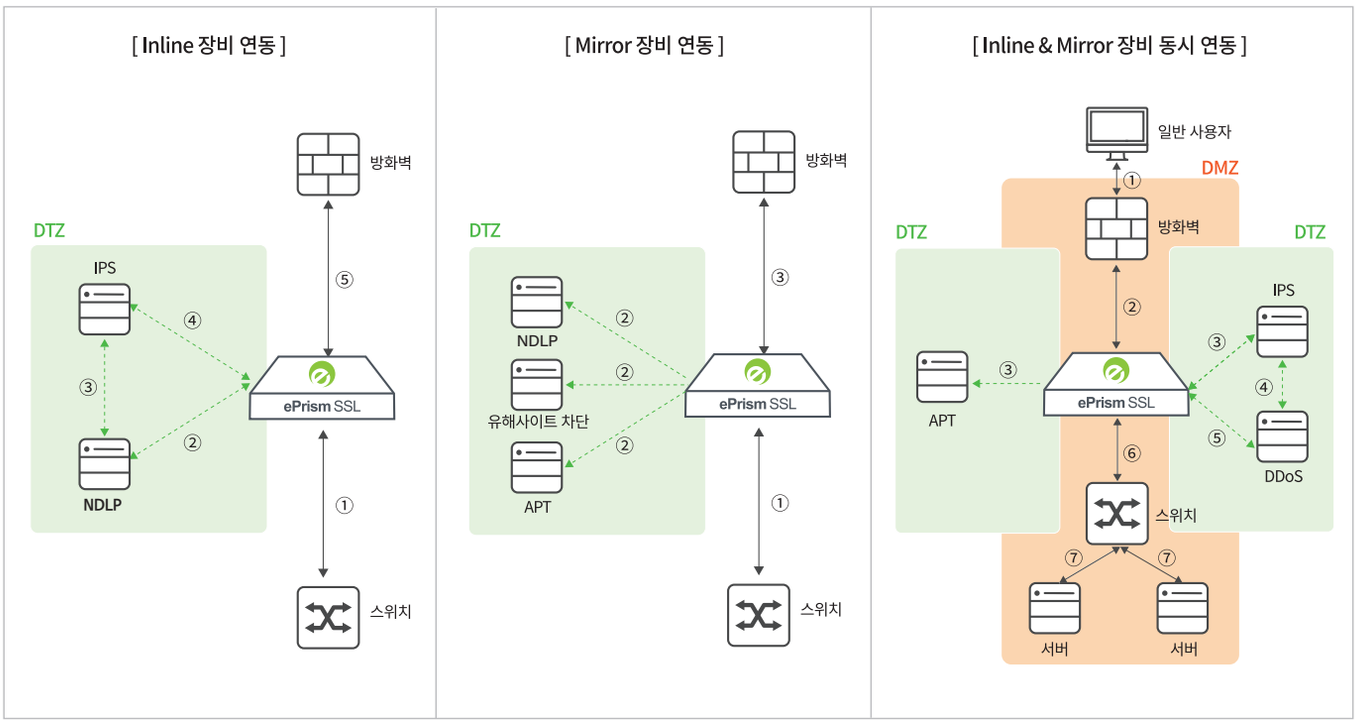
기업

HYUNDAI MOTOR GROUP
posco
SK 바이오랜드
KUMHO TIRE Better, All-Ways
ASIANA AIRLINES
MBC
woongjin 웅진에너지
ILJIN
국민건강보험 National Health Insurance Service
일산병원 Ilsan Hospital
Danal

SOOSAN INT
(주)수산아이앤티 서울시 강남구 밤고개로 5길 13 수산빌딩 | esales@soosan.co.kr | 02-541-0073
www.soosanint.com

제품 연동 방식

복호화 트래픽
일반 트래픽
①~⑦ 트래픽 흐름 (순방향, 역순)

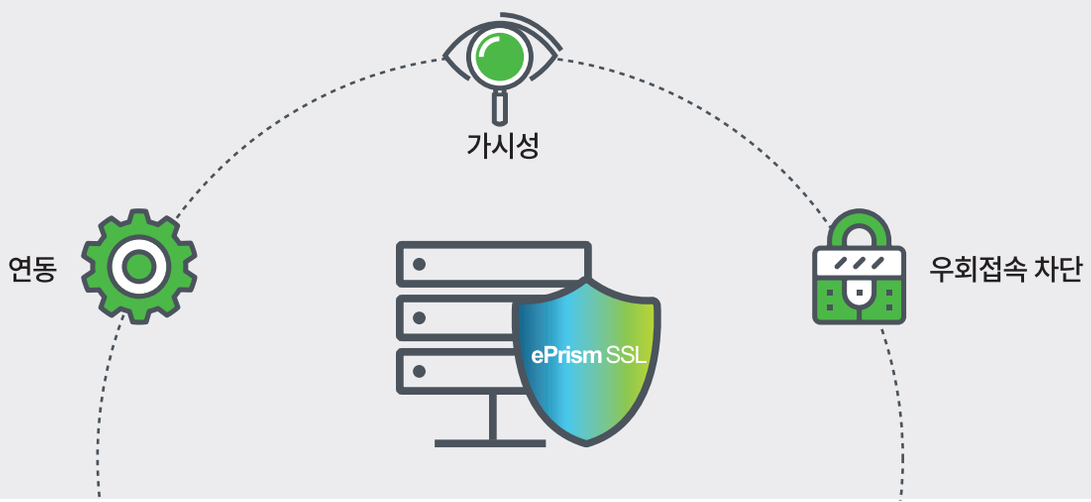


데이터 시트

	SPA-1000	SPA-1100	SPA-2000	SPA-2100	SPA-3000	SPA-3100
성능						
총 처리량	1.2 Gbps	1.2 Gbps	10 Gbps	15 Gbps	20 Gbps	20 Gbps
SSL 인터셉트 처리량	300 Mbps	600 Mbps	2 Gbps	4 Gbps	6 Gbps	10 Gbps
새로운 핸드 셰이크 SSL 세션 수 (CPS)	1,500/sec	2,500/sec	4,500/sec	6,000/sec	8,000/sec	21,000/sec
동시 처리 SSL 플로우 수	50,000	100,000	220,000	350,000	500,000	800,000
기타						
네트워크 인터페이스 구성	Fixed 8 X 1Gbps Copper (2페어 바이패스 포함)		기본 NIC 제공 없음 (고객사 네트워크 환경에 따라 NIC 추가)			
동작모드	하드웨어 바이패스가 가능한 인라인 모드					
SSL 관리 투명성	Certification Resign으로 TCP 세션 투명성 제공 (5-Tuple) 유지					
암호화 프로토콜	SSL v3, TLS1.0, TLS 1.1, TLS 1.2, TLS 1.3					
공개키 알고리즘	RSA, DHE, ECDHE					
대칭키 알고리즘	AES, AES-GCM, 3DES, SEED, ARIA, CAMELLIA, DES, RC4					
해쉬 알고리즘	MD5, SHA-1, SHA-2					
RSA 키	512 to 8192 bits					

ePrism SSL VA는 증가하는 SSL 트래픽 공격에 대한 가시성을
확보 & 연동할 수 있는 최적의 SSL 가시성 제품입니다.

TST 기반의 고성능 SSL 복호화 솔루션!



제품 개요

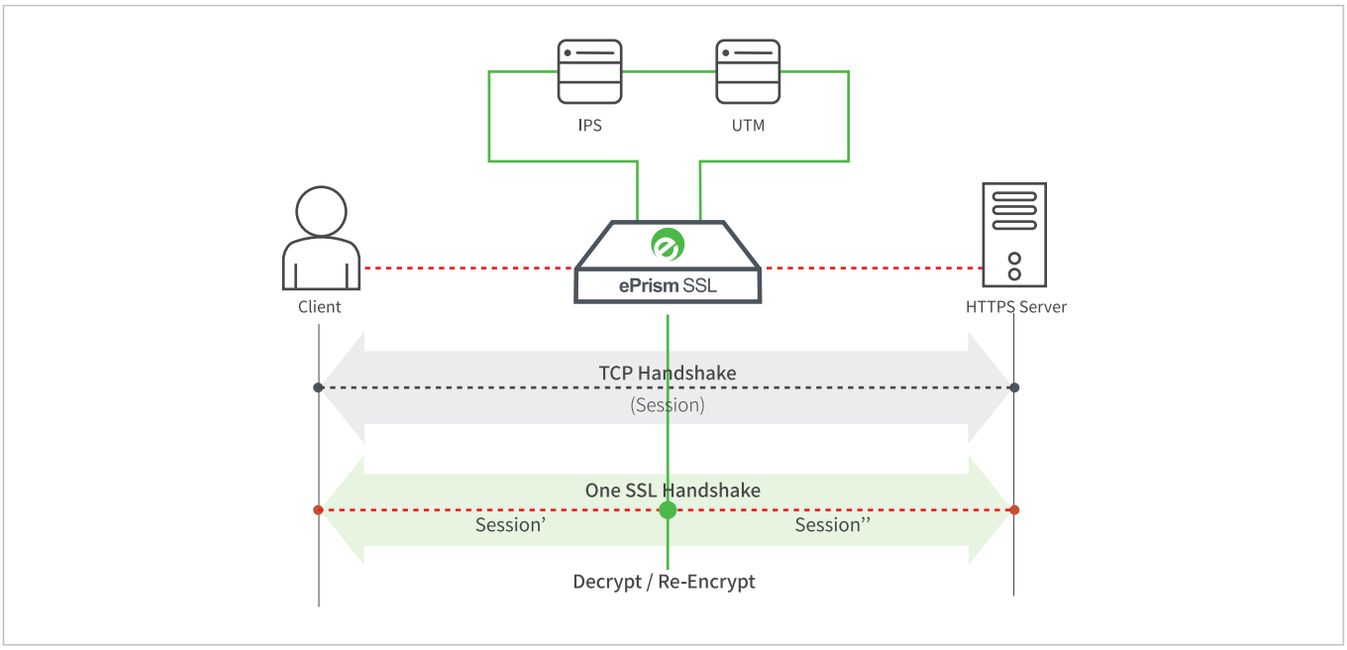
ePrism SSL VA는 SSL 트래픽이 증가하는 시대에 맞춰 IPS, IDS, DDoS, APT 등 기존보안 장비에서 대응하지 못하는 SSL 트래픽에 대한 가시성을 확보하고 기존 네트워크 환경 변경없이 연동/설치 가능한 제품입니다.
최대 10G SSL 트래픽 처리 모델까지 다양한 제품 라인업을 갖추어 고객사 네트워크 환경에 효율적으로 적용할 수 있으며 시장에서 기술력, 성능과 안정성을 인정받은 제품입니다.

- DPI 기반 HTTPS 복호화
- 세션 투명성 유지
- 다양한 3rd Party 연동
- DTZ 구성 지원 *DTZ:Decrypted Traffic Zone
- 우회 접속 프로그램 차단
- SSL 트래픽 상세분석 리포트 제공
- 인증서 설치 유도 및 배포 현황 관리
- TST 기반 고성능 세션처리 *TST:TCP Session Tranparency
- 다양한 설치 방식 지원 및 사용편의성 강화

제품 특장점

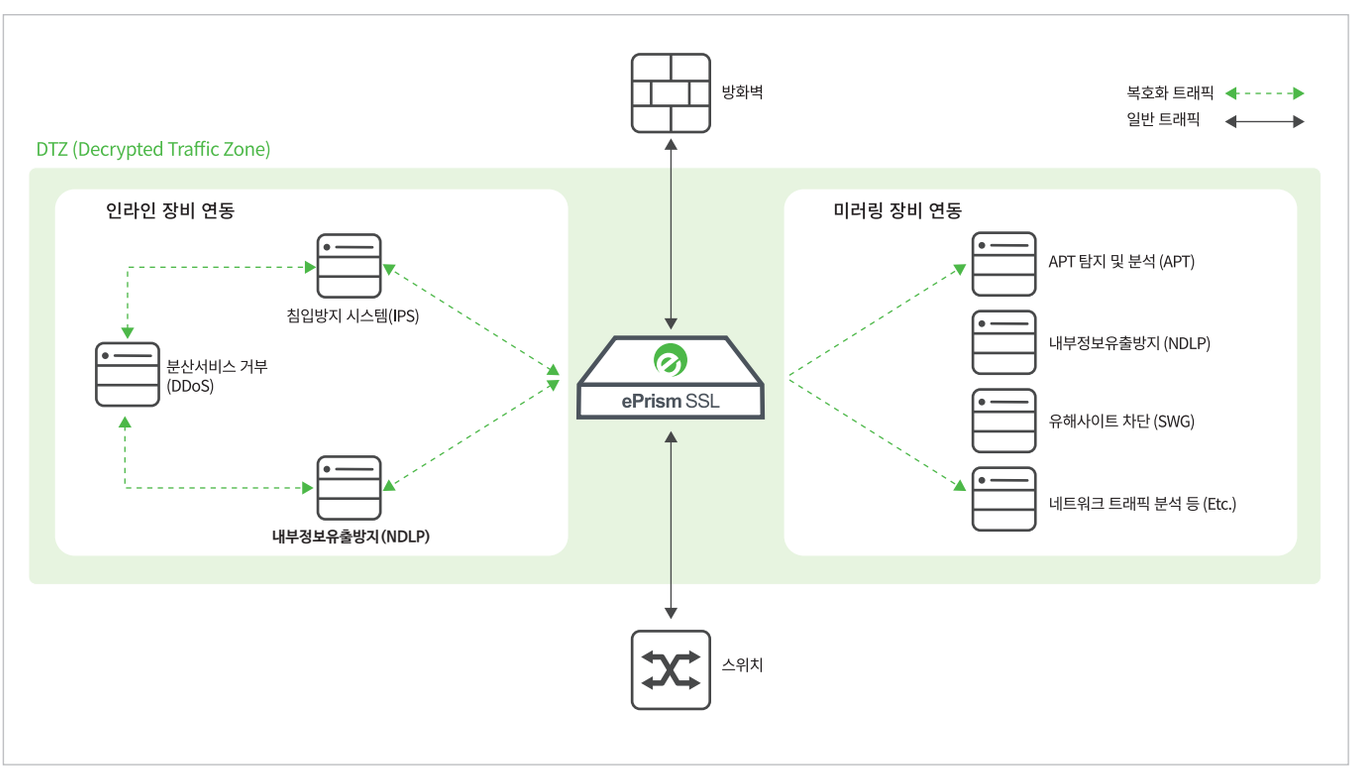
TST 기술

- DPI (Deep Packet Inspection) 기반 기술로 사용자와 서버가 세션이 맺어진 이후 특정 TLS/SSL Protocol 만을 선별적으로 분리하여 복호화 처리
- 네트워크 속도 저하 없이 비표준 TLS/SSL 트래픽에 대한 복호화 지원
- 세션의 투명성(5 Tuple : Source IP, Destination IP, Source Port, Destination Port, Protocol)을 유지



DTZ

- SSL 트래픽을 인식 못하는 보안/네트워크 장비에 복호화된 트래픽을 공급하여 암호화 트래픽을 분석할 수 있도록 지원
- In-Line 구성, Mirror 구성의 보안 장비를 동시 지원
- Forward / Reverse 형태 지원 및 양방향 TLS / SSL 트래픽을 분석, 전달



인증서 유도 및 관리

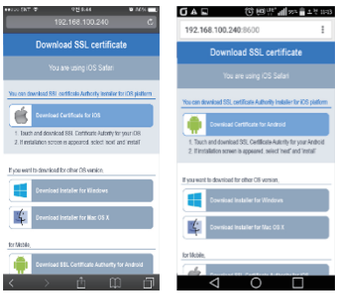
- 인증서 유도 페이지 지원 및 모니터링 화면을 제공하여 운영자 편의성 증대
- 다양한 OS(Mac OS, iOS, Android 포함)에 인증서 설치를 지원
- 내부 사용자에 대한 인증서 설치 / 배포 / 현황 관리

■ 자동 배포

사용자들에게 OS별 인증서 설치 화면으로 자동 유도 기능

[인증서 배포 화면]

(PC 버전)

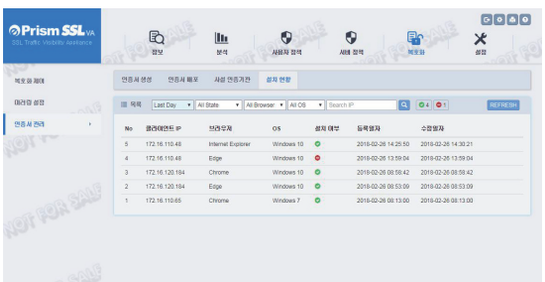


(모바일 버전)

■ 배포 현황 관리

내부 사용자에 대한 인증서 설치 현황 및 배포 현황 관리

[인증서 배포 현황 관리]



우회 접속 차단

- DPI 기반 패킷 분석을 통해 각종 우회경로 패턴 차단
- 주기적으로 프로토콜 업데이트를 통한 최신 패턴 DB 유지