Advanced SSL Traffic Visibility Appliance

Prism SSL VA

네트워크 트래픽의 SSL/TLS 암호화에 따른 전용 처리 장비의 필요성

- SSL/TLS 기반 암호화 트래픽은 보안을 이유로 필수 기술로 권장/사용 되고 있지만, 기존 네트워크 보안 장비가 암호화 트래픽을 분석하지 못하는 치명적 부작용 발생 (악성코드 유포, 내부자료 유출)
- 악성코드/랜섬웨어는 C&C (Command and Control)서버와 암호화 통신을 하고 있어 이에 대한 대책 필요
- 다양한 기법의 비 표준 암호화 통신을 해독할 수 있는 복호화 전용 장비 필요

7 Models

SSL	100Mbps
Total	500Mbps

~

SSL	10Gbps
Total	20Gbps

CONTACT US
www.roiworks.info
sales@roiworks.info

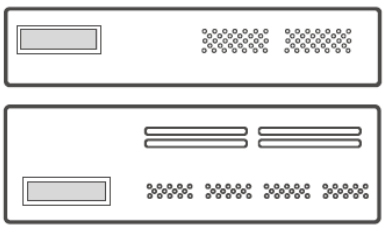
SOOSAN INT

Delivering Innovative Security Solutions and Services

Advanced SSL Traffic Visibility Appliance

ePrism SSL VA

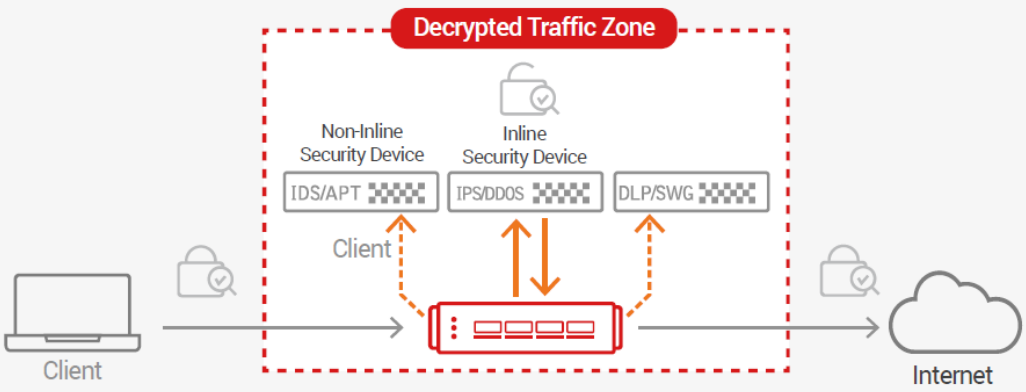
- SSL/TLS 복호화 전용 장비
- SSL 전용 H/W 및 자사 특허 기반 네트워크의 지연 없는 고성능
- 기존 보유 보안 장비와 연동 가능 (DLP, SWG, IPS, APT 등)
- 인증서 자동 배포로 편리성 확보
- 복호화 영역인 DTZ 제공 (Decrypted Traffic Zone)



ePrism SSL VA 란?

ePrism SSL VA는 단일 장비로서 네트워크 망에 설치된 기존의 보안 장비를 그대로 운영하며 암호화로 인한 다양한 보안 위협을 해결할 수 있는 수산아이앤티의 SSL/TLS 트래픽 분석/차단 전용 장비로 복호화 영역인 DTZ(Decrypted Traffic Zone)를 제공합니다.
ePrism SSL VA는 기존에 존재하는 네트워크 보안 장비의 변화 없이 설치 연동이 가능하며 성능에 따른 다양한 모델을 제공합니다. 또한 검증된 바이패스 카드를 탑재하여 안정된 성능과 SSL 가속 카드를 지원함으로써 빠른 SSL 처리 성능을 보장합니다.
특히 TST방식의(TCP Session Transparency) 복호화 엔진을 탑재하여 네트워크 전송에 영향을 주지 않으면서 모든 포트를 투명하게 감시하고 SSL 트래픽만을 선별적으로 복호화 할 뿐만 아니라 L7 분석을 통해 불가능했던 암호화된 SSL 트래픽을 포함한 전체 트래픽에 대해 세션별 분석 기능을 제공하는 암호화 시대의 새로운 필수 네트워크 장비입니다.

[ePrism SSL VA 구성도]



Key Benefits

SSL 트래픽의 완벽한 Visibility로 첨단 위협 대응

- DPI(Deep packet Inspection)기반 엔진. 모든 SSL/TLS, 모든 포트 복호화
- 5-Tuple 유지를 통한 Full Transparency 확보
- TST기술 기반 세션 투명성 유지 & SSL 전용 H/W칩을 통한 고성능 확보 (10G, 20,000 CPS)
- HTTPS, SMTPS, XMPP, POP3S, IMAPS, FTPS, STARTTLS 등 SSL/TLS기반 프로토콜의 Visibility 제공

DTZ(Decrypted Traffic Zone) 구성 지원

- 사용 중인 기존의 보안 장비를 Chain으로 구성하여 별도의 복호화 구간 설정 가능
- 중앙 집중적 복호화를 통해 여러 보안 장비에 복호화 트래픽을 한번에 제공
- One Source – Multi Use를 통한 운영 비용 절감
- DTZ 내부 장비의 장애를 감지하여 바이패스 가능

우회 접속 프로그램 분석 및 차단

- 우회 프로그램 분석 및 차단
- 지원 범위: Openvpn, Tor, UltraSurf, Zenmate, QUIC 등

기존 설치된 보안 제품의 변화/변동/조작 없음

- IPS, IDS, SWG, APT 등 기존 제품의 변경없이 연동 가능 (첨단 위협 대응)
- Active 및 Passive 포트 동시 지원 (Active-inline, Passive-inline)
- Message Pass Through 기능을 통해 연동 보안 장비의 모든 차단 메시지를 그대로 클라이언트에게 전송

다양한 Deployment option 제공

- Active-Active, Active-Standby지원 (전환 속도 0.1초 미만)
- LLCF(자동 링크 단절)기능 제공
- 클러스터 GUI (1 Management Console - Multi engine)를 통한 통합 관리 가능

설치 및 사용 편의성 강화

- 복호화 수행을 위한 Client의 인증서 자동 설치 페이지 유도 기능 제공
- 직관적이고 간단한 GUI 제공을 통한 사용자 중심의 메뉴 구성 (한글/영문)
- 편리한 사용을 위한 Web 도움말 기능 제공

트래픽 상세 분석 및 로그 검색, 다양한 보고서 제공

- 암호화 트래픽을 포함한 전체 트래픽 상세 분석 및 실시간 검색 가능
- SSL 트래픽 보고서, 전체 트래픽 보고서를 PDF, Excel 형태로 제공

Advanced SSL Traffic Visibility Appliance

Prism SSL VA

Line Up & Specifications

	SPA-500	SPA-1000	SPA-1100	SPA-2000	SPA-2100	SPA-3000	SPA-3100
성능							
총 처리량	500 Mbps	1.2 Gbps	1.2 Gbps	10 Gbps	15 Gbps	20 Gbps	20 Gbps
SSL 인터셉트 처리량	100 Mbps	300 Mbps	600 Mbps	2 Gbps	4 Gbps	6 Gbps	10 Gbps
새로운 핸드 셰이크 SSL 세션 수 (CPS)	700/sec	1,500/sec	2,500/sec	4,500/sec	6,000/sec	8,000/sec	21,000/sec
동시 처리 SSL 플로우 수	25,000	50,000	100,000	220,000	350,000	500,000	800,000
SSL 가시성							
세션 제어 매핑	지원	지원	지원	지원	지원	지원	지원
트래픽 분석/모니터링	지원	지원	지원	지원	지원	지원	지원
다차원적 분석 및 리포트 (카테고리별 / 사용자별 / 시간대별)	지원	지원	지원	지원	지원	지원	지원
인증서 배포 툴	지원	지원	지원	지원	지원	지원	지원
필터링 (*SSL/비SSL)							
DB기반 악성코드 차단/우회접속 제어	지원	지원	지원	지원	지원	지원	지원
기타							
네트워크 인터페이스 구성	Fixed 8 X 1Gbps Copper (2페어 바이패스 포함)			4Port 1G/10G Fiber Bypass (SR) 1개 및 4Port 1G/10G Fiber NIC 1개 (고객사 환경에 따라 변경 가능)			
동작모드	하드웨어 바이패스가 가능한 인라인 모드						
SSL 관리 투명성	Certification Resign으로 TCP 세션 투명성 제공 (5-Tuple) 유지						
암호화 프로토콜	TLS1.0, TLS 1.1, TLS 1.2, SSL v3						
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						

Main References

MBC 한국전력공사 KB손해보험 woongjin NH농협생명

Roiworks Always New

㈜로이워스
서울시 구로구 디지털로 288 대륭포스트타워 1차 207호(르호봇 구로비즈니스센터)
TEL : 070-8002-1828 | E-mail : sales@roiworks.info | www.roiworks.info