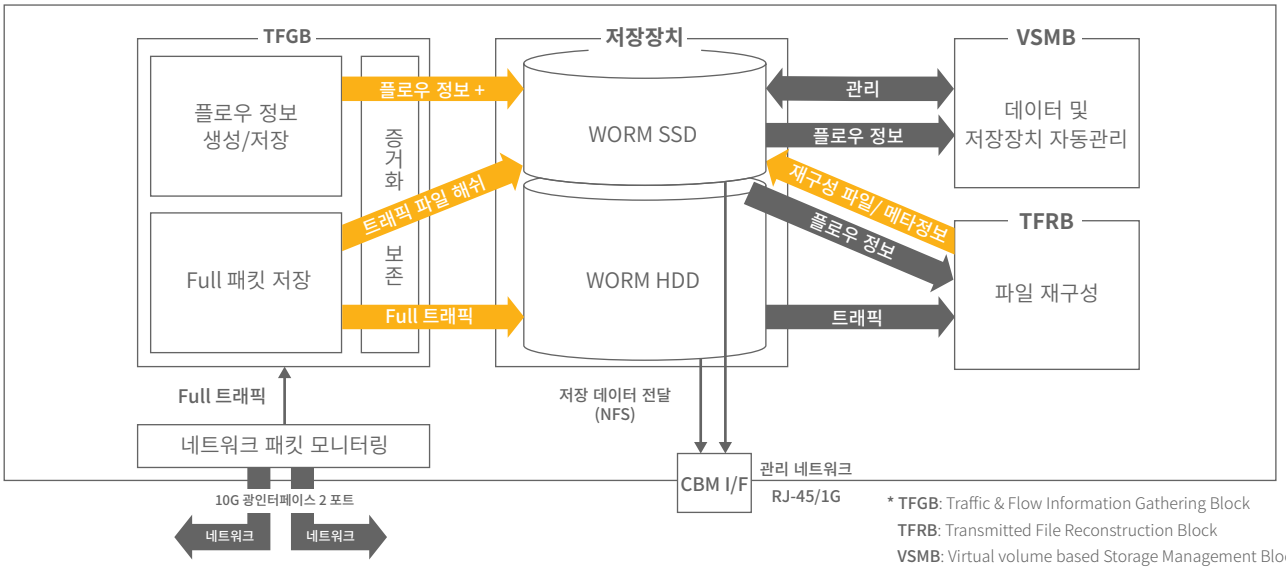
zPR-1000
고속 패킷 저장 장치

최근 사이버 침해사고는 기 설치된 보안 장비를 우회하는 방법 등으로 네트워크를 통하여 침투, 정보 유출, 공격 지시 등이 이루어지고 있습니다. 이때 원인 분석을 위한 증거 데이터 부재로 인하여 대응의 적기를 놓치고 있습니다. 이와 같은 문제점을 해결하기 위해서는 공격 정보 분석의 기본 데이터에 해당하는 네트워크 트래픽을 장기간 수집, 보존하는 기술이 필요합니다. zPR-1000은 네트워크를 통과하는 모든 정보를 저장, 인덱싱함으로써 신속하고 정확한 네트워크 포렌식 인프라를 제공합니다.

시스템 구조



* **TFGB**: Traffic & Flow Information Gathering Block
TFRB: Transmitted File Reconstruction Block
VSMB: Virtual volume based Storage Management Block
WORM: Write Once Read Many

네트워크 트래픽 전수 저장

zPR-1000은 10기가급 네트워크 트래픽을 96TB 스토리지에 실시간으로 무손실 전수, 저장함으로써 사이버 침해사고 발생 시 신속한 침해사고 대응을 위한 원인 분석 지원과 법적 증거 확보를 위한 네트워크 포렌식 인프라를 제공합니다. 이는 블랙박스, CCTV처럼 사이버상에서 언제든지 발생할 수 있는 침해사고의 근본적인 원인을 분석할 수 있으며 방화벽, 내부정보시스템, IDS/IPS, SIEM 등과 같은 기 설치된 네트워크 보안 장비의 기능과 성능을 보완합니다.

계층7 레벨 플로우 정보 수집 저장

zPR-1000은 원본 트래픽의 패킷 레벨 전수 저장과 동시에 두 호스트 간의 세션 연결에 해당하는 플로우를 추적, 관리하고 이들의 통계 정보, 해당 플로우의 응용 서비스 식별, 해당 플로우 내에 응용 파일 포함 여부를 실시간으로 판단하는 기능을 제공합니다. 이들 정보는 네트워크 포렌식에 필수적인 내부 전파 경로 추적을 위한 용도로 사용할 수 있습니다.

증거보존을 위한 데이터 무결성 보장

zPR-1000은 수집된 모든 네트워크 트래픽을 pcap 파일 형식으로 저장하며, 플로우 통계 정보에 해당 플로우에 속하는 패킷이 저장된 파일의 이름과 오프셋 정보 등을 기록하여 원본 패킷 데이터를 신속하게 검색합니다. 또한 저장되는 전수 데이터의 무결성 보장을 위해 해쉬값을 생성하여 지정된 디렉토리에 저장함으로써 해당 전수 데이터의 무결성 침해 여부를 확인할 수 있습니다. 또한 저장된 데이터의 무결성 확보, 보존 및 관리를 위하여 가상화 볼륨 기반의 스토리지 기술을 제공합니다.

시스템 사양

항목	구분	사양	비고
서버	운영체제	CentOS Linux 7.0 이상	
	프로세서	Intel CPU, 2Way 각 12Core	2 ea
	메모리	DDR4 128GB	8GB x 16
	스토리지	HDD 96TB / SSD 4TB	4TB x 24 / 4TB x 1
네트워크	Intel NIC	10GBASE-(SR)*2 또는 1000BASE-SX*2	1 ea
	관리 네트워크	10/100/1000BASE-T	2 port
시스템	외부형상	Rack-mountable Appliance	4U
주요기능	네트워크 트래픽 전수 저장, 계층7 레벨 플로우 정보 수집 저장, 증거보존을 위한 데이터 무결성 보장, 단방향플로우 메타정보, 수집트래픽 통계, 외부 시스템 연동정보, 송수신파일 메타정보		

응용 분야 및 용도

단방향 플로우 메타정보

특정 시스템 접속 연결 확인(의심 IP 선별)

- 특정 시스템에 접속한 적이 있는 시스템 확인
- 외부 IP 혹은 평소와 다른 IP라면 의심 IP로 선정 가능
- 피해 시스템으로부터 다음 단계분석 대상 선정

수집 트래픽 관련 통계 정보

플로우 정보 기반 이상트래픽 탐지 방안 적용

- 포트 스캔 등 이상트래픽 탐지 기술 적용 가능

2G급/10G급, 전수/선별 트래픽

원인 규명 및 책임 소재 파악을 위한 증거 확보

- 무결성이 보장되는 수집 트래픽 제시

외부 시스템 연동 정보

외부 침해 정보 제공 시스템과 연동을 통한 악성 IP 및 악성 파일 판별

- 의심 파일의 정확한 악성 여부 확인
- 외부 접속 의심 IP의 악성 여부 확인
- 사용자 시스템의 감염 여부 판단

송수신 파일 및 관련 메타정보

파일 내부 전파 경로 확인(의심 파일 선별)

- 악성 파일의 다운로드 경로 확인(웹, Email 등)
- 내부 중요 파일 유출경로 확인
- 악성파일 전파 목록 도출
- 최초 유포지 및 C&C 서버 도출
- 감염시스템 탐지

*본 문서에 기술된 기능은 별도의 고지없이 변경될 수도 있습니다.

ZENTILLION

㈜젠틸리언 | 대전광역시 유성구 테크노1로 75 한밭대학교 대덕산학융합캠퍼스 301호

www.zentillion.net | T: 042-933-0685 | F: 042-933-0687 | E-mail: marketing@zentillion.net