Entobil Soft.

NetFreezer Platform

실시간 전체 패킷 수집, 추출, 분석 및 관리 플랫폼

NetFreezer

Real-Time Traffic Analysis
- 1G/10G급 트래픽 양방향 패킷 수집, 저장 및 분석
- Connection, Protocol, IP, Port 상세 분석
- Top N, Bottom M 통계분석

Suspicion Monitoring
- 악성코드 발생 트래픽
- 내부 정보유출 정황
- 기타 유해 트래픽

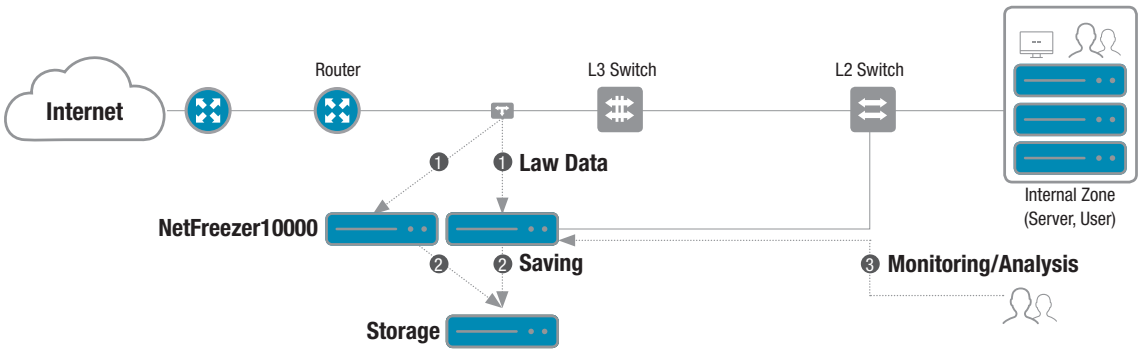
Logging & Analysis
- 전체 트래픽 전송 로그 저장
- 전체 패킷 단기저장
- 의심 패킷 단기 및 장기 저장
- HTTP, FTP, SMTP 등 프로토콜별 저장

NetFreezer 플랫폼 구성

NetFreezer 수집 시스템
- 패킷 수집, 추출, 관리 및 분석
- 저장 성능 7Gbps 보장 (최대 10Gbps 처리)
- Monitoring : 10GbE, Mgmt:1GbE
- 최대 20TB의 추출 결과 저장 공간 지원
- GUI

NetFreezer 저장 장치
- Storage (Option): DAS 방식, 최대 240TB 지원

이중화 구성
- 듀얼 포트 Tap으로 동시 저장

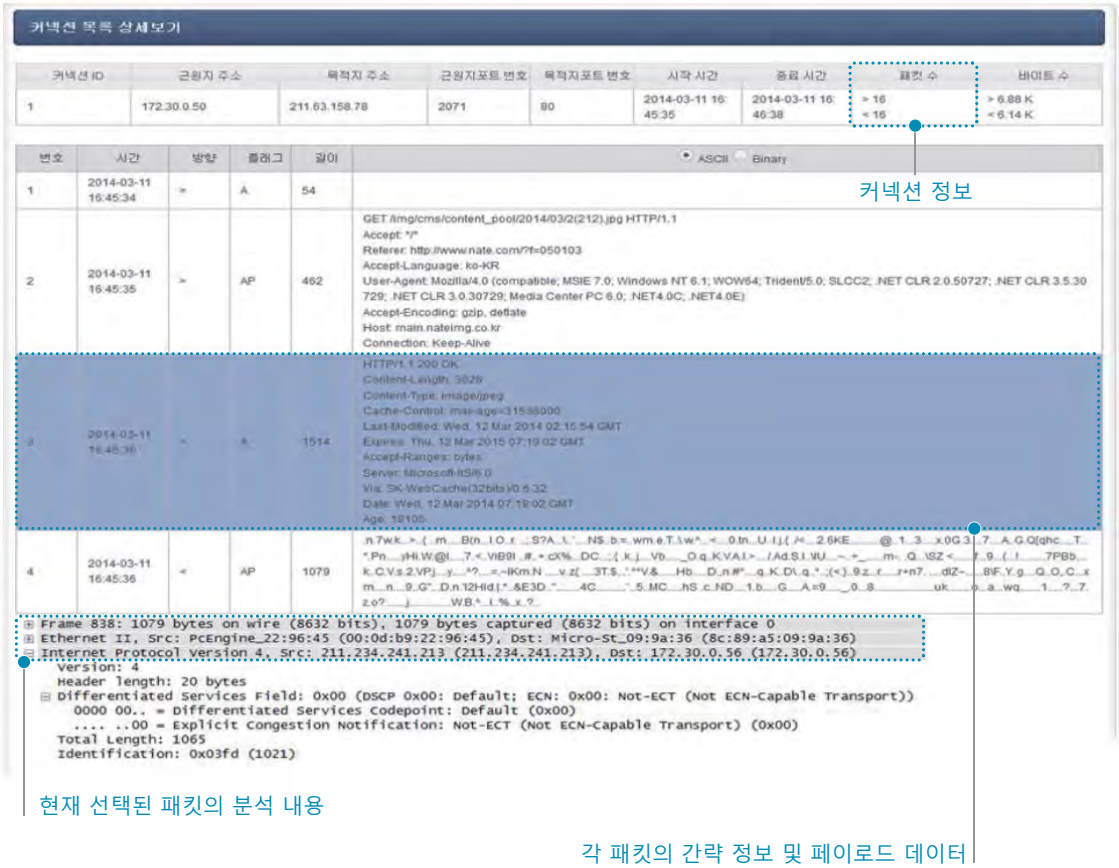


- 추출 결과 저장 공간 : NetFreezer에 추출 결과 파일을 저장하기 위해 할당된 공간, 20TB
- 전체 패킷 저장 공간 : NetFreezer Storage에 패킷을 저장하기 위해 할당된 공간, 192TB

실시간 패킷 분석 절차

단계	기능	설명
1단계	저장	· 전체 패킷 저장 공간[180TB]에 실시간 저장
2단계	1차 추출	· 다양한 검색 조건을 이용한 패킷 추출 · 추출 결과는 '추출 결과 저장 공간' (20TB)에 자동 보관 · 검색 조건: 기간, IP 주소, 포트 번호, 프로토콜, 최대 추출 파일 사이즈 · 추출 결과는 수십 MB ~ 수 GB 파일 사이즈 예상
3단계	커넥션 검색	· 1차 추출된 결과를 커넥션 단위로 조회 · 특정 시그너쳐를 포함한 커넥션 검색 기능을 이용하여 상세 분석 대상 커넥션 선택 · 시그너쳐 : PCRE 정규식, ASCII 문자열, 헥사 문자열 등
4단계	커넥션 분석	· 선택된 커넥션의 패킷을 상세하게 분석 · 페이로드 데이터를 ASCII 혹은 바이너리 형태로 표시 · Wireshark의 분석 기능 대응
5단계	pcap 파일 추출	· 상세한 커넥션 검색을 통해 선택된 커넥션만 pcap 파일로 추출해 저장 · 추출 결과는 수십KB ~ 수십MB 파일 사이즈 예상
6단계	PC로 다운로드 및 분석	· 저장된 pcap 파일을 다운로드 후 Wireshark 등을 통해 패킷 단위 분석

저장 패킷 추출 및 분석 화면



도입 및 기대 효과

· 실시간 전체 패킷 저장, 추출, 분석 및 모니터링 가능
· 보안 및 침해 사고 발생 시, 정밀한 세부 분석을 통한 빠른 사후 대처 가능
· 3rd 보안 솔루션 연계로 지능적이고 능동적인 대응 (APT 솔루션 등)

상세 스펙

구성 옵션	NetFreezer 수집 장치
CPU	Single Intel Xeon 60 Core 3.50GHz 25MB
RAM	96GB
HDD	4TB 7.2K RPM SATA HDD 3.5" * 8
Management Port	100/1000M Ethernet * 4
Capture Port	10GbE SFP+ * 4
RAID 컨트롤러	내부 컨트롤러 외부 컨트롤러 (6Gbps SAS * 2)
전원 공급 장치	듀얼, 핫플러그, 예비 전원 공급 장치 750W
Dim (WxDxH mm)	482.6 * 756.92 * 86.36
폼 팩터	Rack Type (2U size)
작동 온도	10℃~35℃
구성 옵션	**NetFreezer 저장 장치**
디스크	4TB 7.2K RPM SATA HDD 3.5” *60
디스크 확장	최대 4TB 3.5" * 180
RAID Controller Module	Two Hot-swappable Modules
모듈 인터페이스	SAS IN Port * 8
Management port	100/1000M Ethernet * 1
Dim (WxDxH mm)	482.6 * 825.5 * 177.8
폼 팩터	Rack Type (4U Size)
작동 온도	10℃~35℃