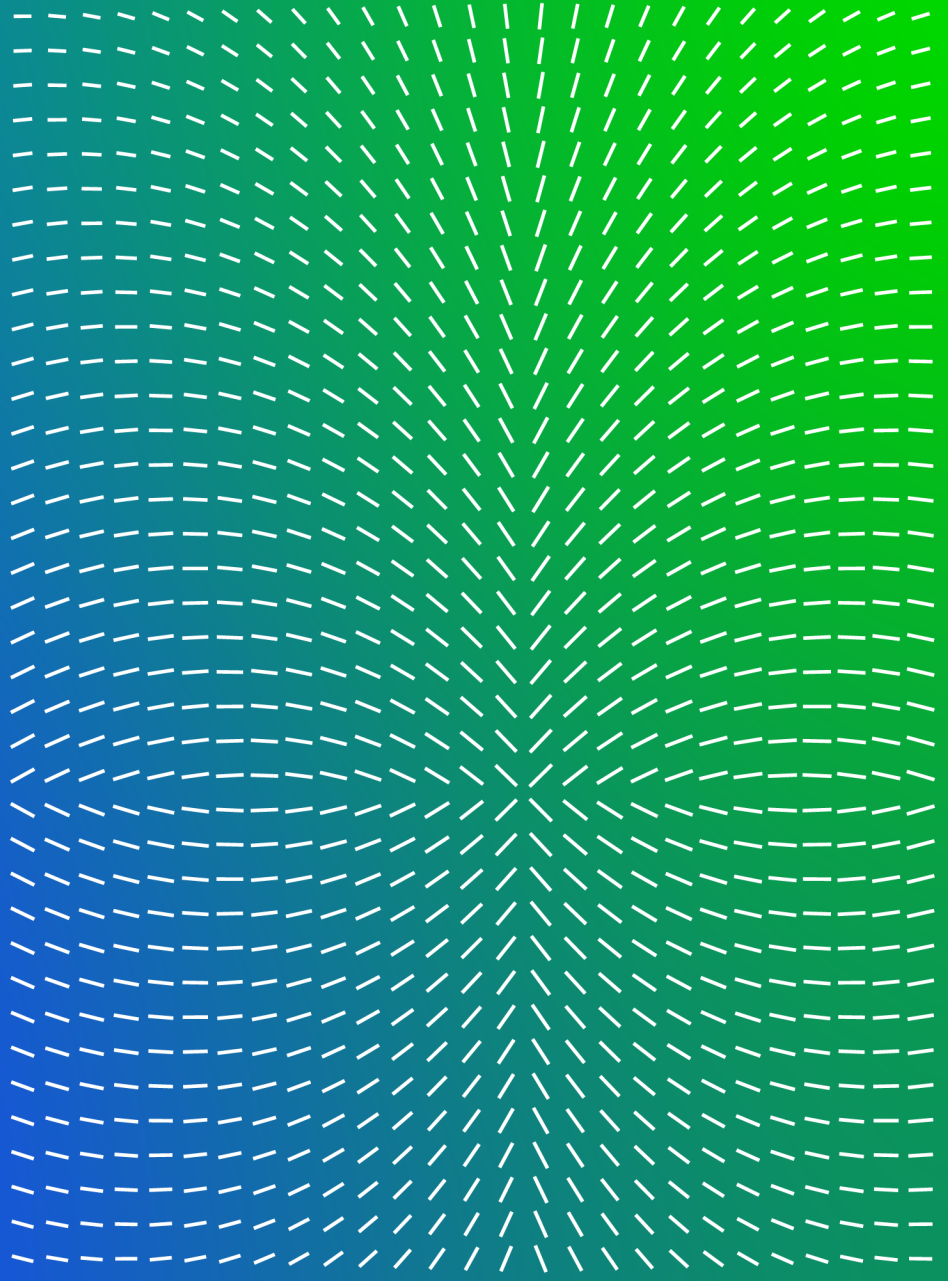
Trellix

Advanced Attack의 방어를 위한 Intelligent IPS

㈜ 초록에스티

Sept 2022

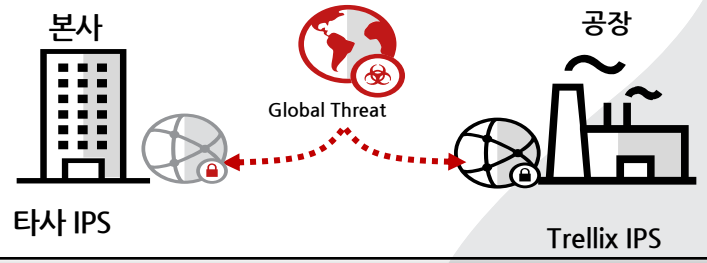


Case#1. 고객사 A의 최적화 룰 업데이트를 통한 탐지율 향상

고객사 요구사항

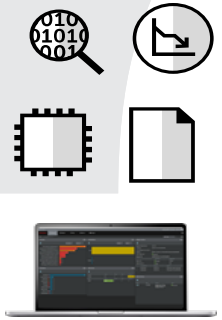
고객사 A의 기 구축된 IPS 환경

- **고객사A**는 본사와 공장에 다른 벤더의 IPS(침입탐지시스템)을 제품을 이용하여 구축됨



고객사 A의 IPS 환경분석

- 구축된 타벤더 IPS의 탐지율 미흡
- IPS H/W Resource와 시그니쳐 패턴의 최적화 부족
- IPS 관제의 편리성 부족



Case#1. A 고객사 최적화 룰 업데이트를 통한 탐지율 향상

Trellix의 IPS/IDS 플랫폼을 통한 구축

- NS-Series로 본사/공장 장비교체를 통한 성능확보

- **Trellix의 다중화된 탐지엔진을 통한 탐지율 향상과 위협에 대한 대응 강화**
  - 다양한 Intelligence의 제공을 통해 진화된 공격에 대응환경 제공
  - 최적화된 시그니쳐 세트(26,700개의 Rule)를 적용한 H/W 성능 제공

- 3세대 H/W 플래폼으로 NGIPS기능 제공
- 3Gbps의 Throughput

- GUI기반 실용적 인터페이스 제공

- 구축 후 고객사A는 장비 단일화를 통한 운영의 용이성과 성능에 대한 문제 해결을 통해 탐지와 위협에 대한 개선된 보안관련 기반구축이 이루어짐

Case#2. B 고객사 네트워크 환경에 대한 지원

고객사 요구사항

고객사B IPS/IDS 필요기능

- 백본의 이중화에 따른 Full Mesh type의인프라 네트워크를 지원하는 Active- Active 구성에서 정상동작 하는 IPS 플랫폼을 요구함

  - 고객사의 인프라환경에서 정상적인 Traffic의 모니터링을 통한 탐지와 대응이 이루어짐

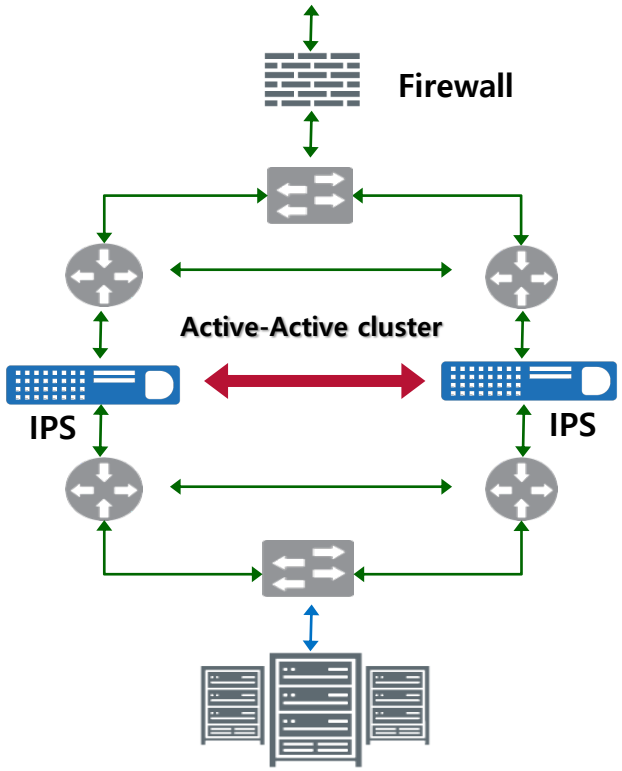
타벤더 IPS/IDS의 문제점

- 타사 IPS 장비는 트래픽의 Inbound와 Outbound의 경로가 다를 경우, 비정상 트래픽으로 인지되어 트래픽이 차단됨

Case#2. B 고객사에 적용할 Trellix의 보유기술

Trellix의 Solution을 통한 요구사항의 반영

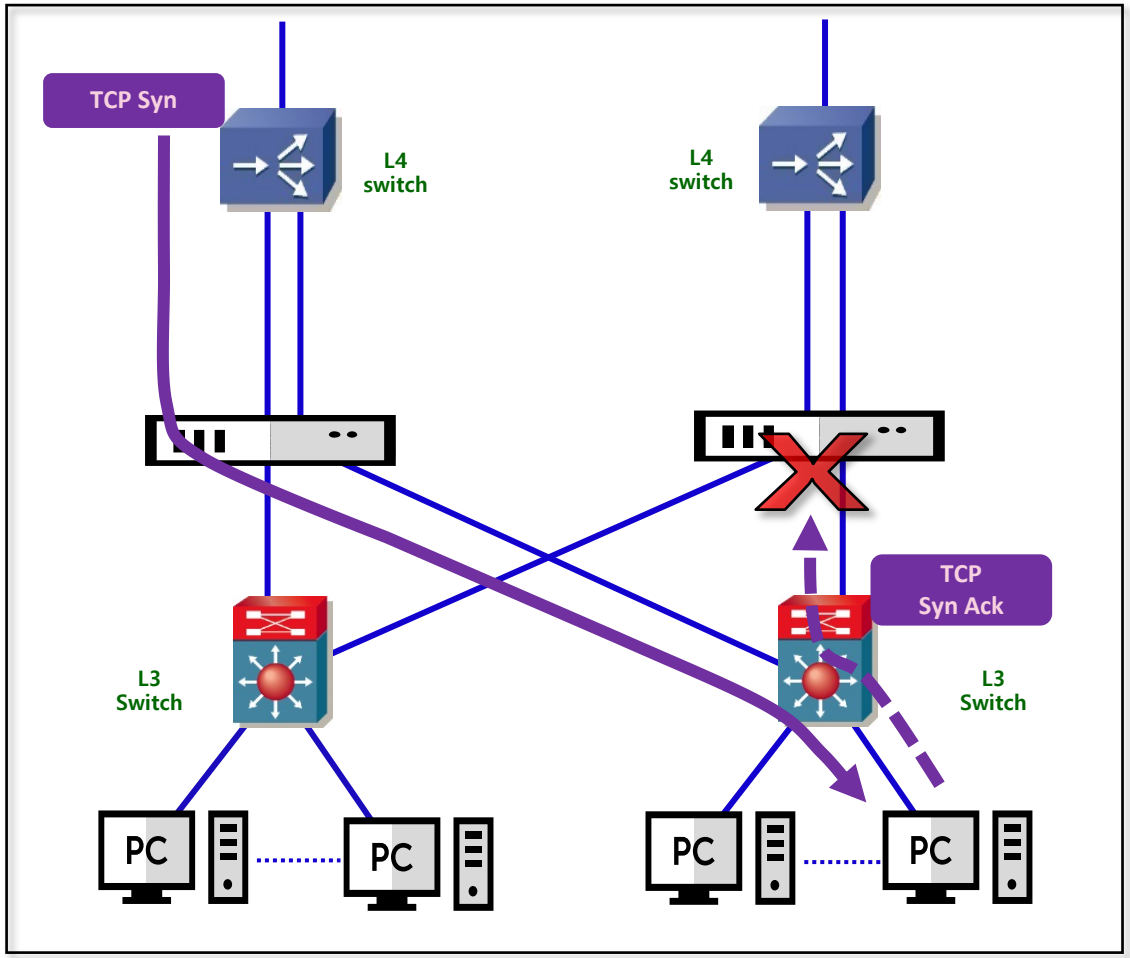
- **Trellix장비는 IPS간의 연결을 통해 Health Check와 Full Stateful Analysis를 통한 트래픽 정보 공유를 통하여 고객사 환경에 구성함**



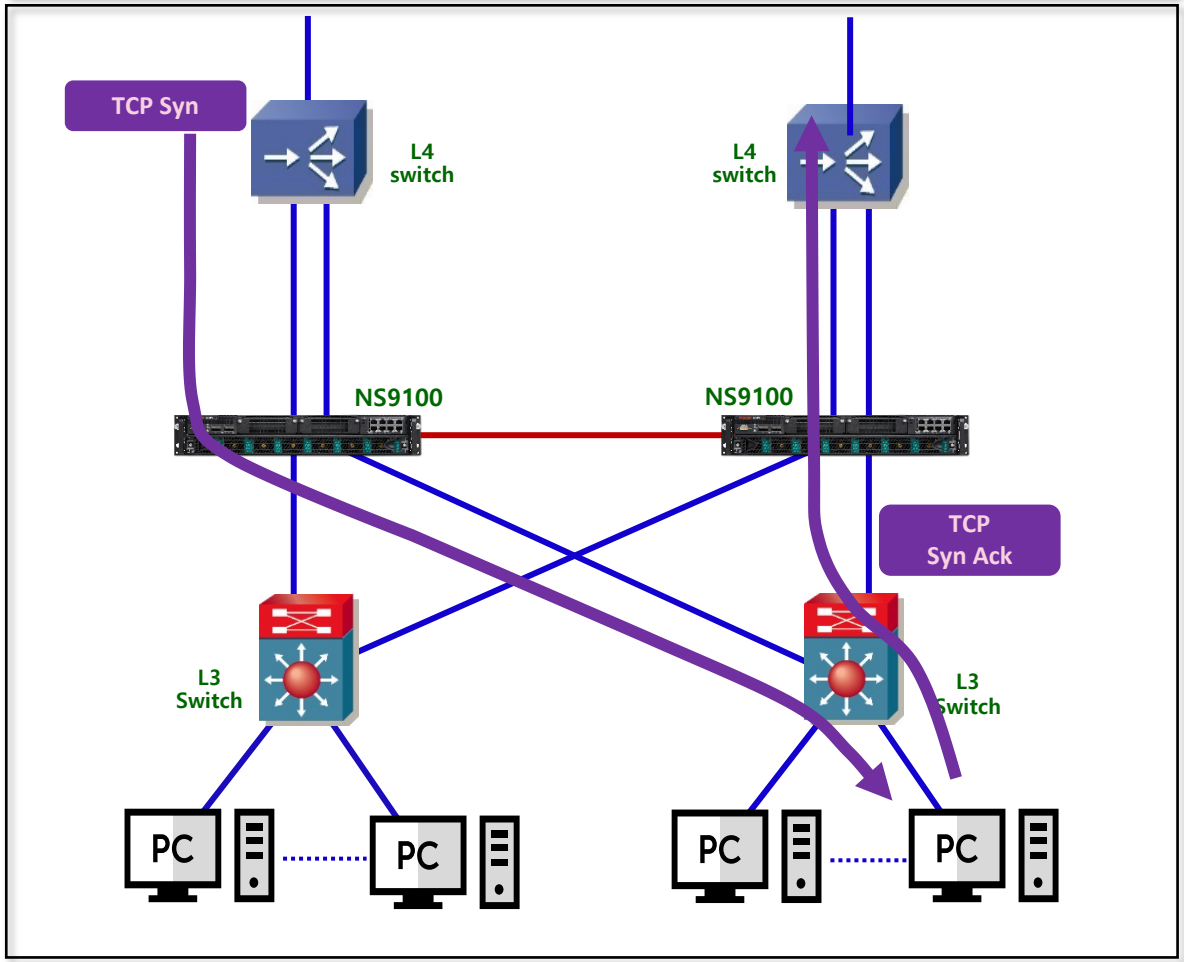
- **Active-Active**
- **Active-Passive**
- **Full stateful analysis**
- **Asymmetrical routes**

Case#2. B 고객사 Active-Active 환경에 대한 지원

타사의 장비로 구축시 트래픽 흐름



Trellix장비 구축시 트래픽 흐름

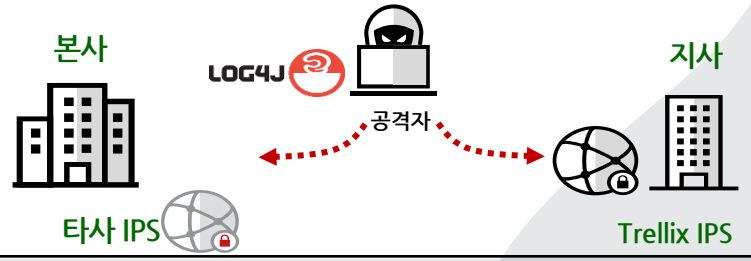


Case#3. C 고객사 글로벌 위협에 대한 빠른 대응

고객사 요구사항

긴급대응 Intelligence 제공의 지연

- **고객사 C**는 본사와 지사에 다른 벤더의 IPS (침입탐지시스템)를 이용하여 구축



타 벤더와의 비교

- 최초 Issue가 된 Log4j 취약점에 대한 시그니쳐 제공 지연
- **본사에선 해당 위협에 대한 Intelligence의 제공이 지연되어 탐지가 안되 실시간 위협대응에 미흡함이 발견됨**
- Trellix는 긴급 사용자 정의 시그니쳐의 제공을 통해 해당 취약성에 대한 대응 Intelligence가 신속이 제공됨

Case#3. C 고객사 글로벌 위협에 대한 빠른 대응

Trellix장비의 긴급 Intelligence 지원

최초 발견	2021.11.14	알리바바 클라우드 보안팀 Chen Zhaojun 발견
	2021.12.10	CVE-2021-44228로 등록
KISA 확인	2021.12.11~ 12.15	KISA는 보안공지를 통해 영향을 받는 버전 별로 해결할 수 있는 방법을 게시
	2021.12.11 21:53	
Trellix 대응	2021.12.11 21:53	Trellix 긴급 사용자 패턴 배포
	2021.12.14 08:30	Trellix 긴급 사용자 패턴 추가 배포
	2021.12.15 12:08	Trellix 정규 패턴 배포

Case#4. D 고객사의 SNORT환경에서 손쉬운 Migration 지원

고객사 요구사항

고객사D의 기 구축된 IDS 환경

- **고객사D**는 Linux기반의 Open Source기반의 IPS를 Snort Rule을 이용 IDS기반 구축
  - 약 30,000개의 Rule을 Customizing
  - CLI환경으로 운영

고객사D의 환경분석

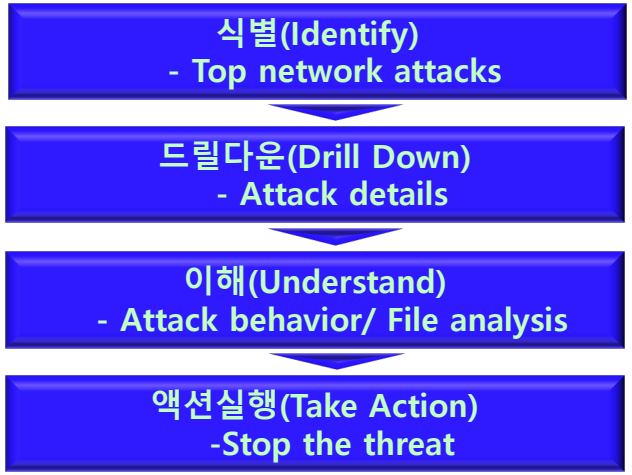
- Chaser방식의 관제운영으로 인한 과다한 Work-load 발생
  - 새로운 적용 시그니처의 제작과 반영의 work-load
  - 상황에 대한 전문가의 분석과 정책의 적용이 필요
  - Native Snort엔진의 저성능 문제

Case#4. D 고객사 Trellix IPS/IPS 플랫폼으로 이전 후 환경변화

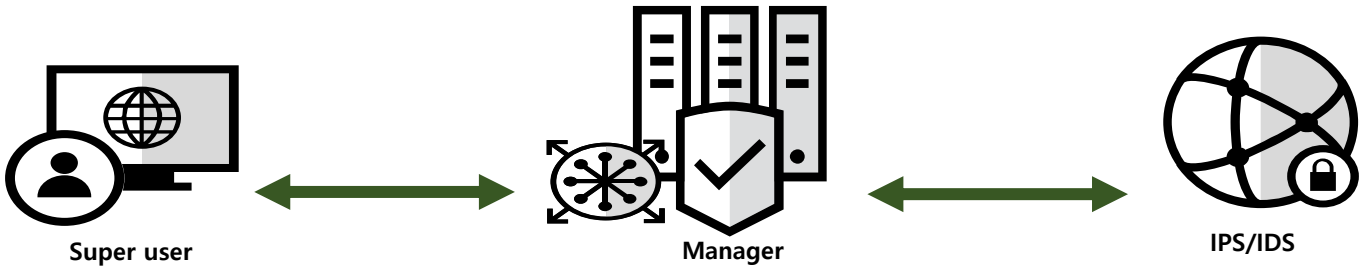
Trellix의 IPS/IDS 플랫폼의 구축

- UI기반 실용적 인터페이스 워크플로우 확보
- 인프라 규모와 성능에 맞는 NS-9500을 이용하여 구축
- 기존 SNORT 룰의 이용과 Trellix 축약 룰셋으로 도입

SURICATA *SURICATA엔진 적용을 통한 성능개선



- REST(Representational State Transfer) Protocol을 이용한 연동을 통한 정책 적용



Thank you