Case Study

AhnLab

대규모 공격에도 안정적인 서비스 운영 L사의 DDoS 방어 체계 구축 사례

업종
공공기관

규모
직원 수
100-1000명

도입제품
AhnLab DPX
AhnLab TMS

최근 공공기관을 대상으로 한 DDoS 공격이 고도화되고 있으며, 공격 방식 또한 다양해지고 있다. 이러한 상황에서 공공기관 L사 역시 지속적으로 발생하는 DDoS 공격에 대응하면서도 정상 서비스의 안정성을 유지할 수 있는 보호 체계가 필요했다. 특히 대규모 공격 트래픽을 처리할 수 있는 방어 구조와 함께, 여러 장비와 정책을 효율적으로 운영할 수 있는 관리 환경을 함께 고려해야 했다.

이에 L사는 AhnLab DPX를 활용해 다양하게 운영하는 서비스망을 기반으로 DDoS 공격에 대한 대응력을 강화하고, 정상 서비스의 안정성을 유지할 수 있는 보호 체계를 구축했다.

Key Results

- 서비스망 분리로 정상 트래픽 영향 최소화
- AhnLab DPX 병렬 구성으로 대규모 공격 대응 기반 확보
- AhnLab TMS 기반 통합 관리로 운영 효율성 향상

주요 과제 (Key Challenges)

L사의 핵심 과제는 DDoS 공격 대응력을 높이는 동시에, 운영 관리 효율성을 확보하고 정상 트래픽과 서비스 운영에 미치는 영향을 최소화하는 데 있었다.

1. 서비스 특성에 맞는 방어 체계

L사는 서로 다른 특성을 가진 여러 서비스망을 운영하며 고객에게 서비스를 제공한다. 이 때 각 서비스의 특성을 고려하지 않고 동일한 방어 정책을 적용하면 정상 트래픽까지 영향을 받을 수 있다.

이에 L사는 보호 자원의 특성에 맞는 방어 정책을 적용할 수 있도록 서비스망을 분리하고, 유형별 방어 기준을 세분화해 정상 트래픽에 미치는 영향을 최소화하는 구조를 마련해야 했다.

2. 대규모 DDoS 공격 트래픽 처리 구조

DDoS 공격 규모가 커질수록 단일 장비에 부하가 집중될 위험이 커진다. 안정적인 방어를 위해서는 충분한 처리 대역폭과 장비 장애 상황까지 고려한 구성이 필요했다. L사는 각 서비스망에 다수의 DDoS 방어 장비를 병렬로 구성해 공격 트래픽이 급증하는 상황에서도 보호 자원을 안정적으로 운영할 수 있는 환경을 마련해야 했다.

하지만 서비스 망이 분리되고, 각 망에 여러 대의 장비가 구성되면서 정책과 로그를 개별적으로 관리하는 데 한계가 발생할 수 있었다. 이에 L사는 여러 망에 구성된 장비를 하나의 체계에서 관리하고, 정책과 로그를 일관되게 운영할 수 있는 통합 관리 환경이 필요했다.

구축 방안 (Solutions)

L사는 기존 네트워크 중심 보안 모델에서 벗어나 가시성 확보, 행위 기반 제어, 안정성 유지 세가지 축을 중심으로 네트워크 보안 구조를 재설계했다.

1. 서비스 유형 기반 망 분리

L사는 보호 대상 자원의 특성에 맞게 서비스망을 분리했다. 또한 목적지 기반 라우팅을 통해 트래픽이 해당 망으로 전달되도록 구성하고, 각 유형에 맞는 DDoS 방어 정책을 적용할 수 있도록 했다.

2. AhnLab DPX 병렬 구성

L사는 각 서비스망에 AhnLab DPX를 병렬로 배치했다. 이를 통해 각 망에서 대규모 트래픽을 분산 처리할 수 있도록 하고, 일부 장비에 장애가 발생해도 다른 장비가 서비스 트래픽을 이어받을 수 있는 구조를 마련했다.

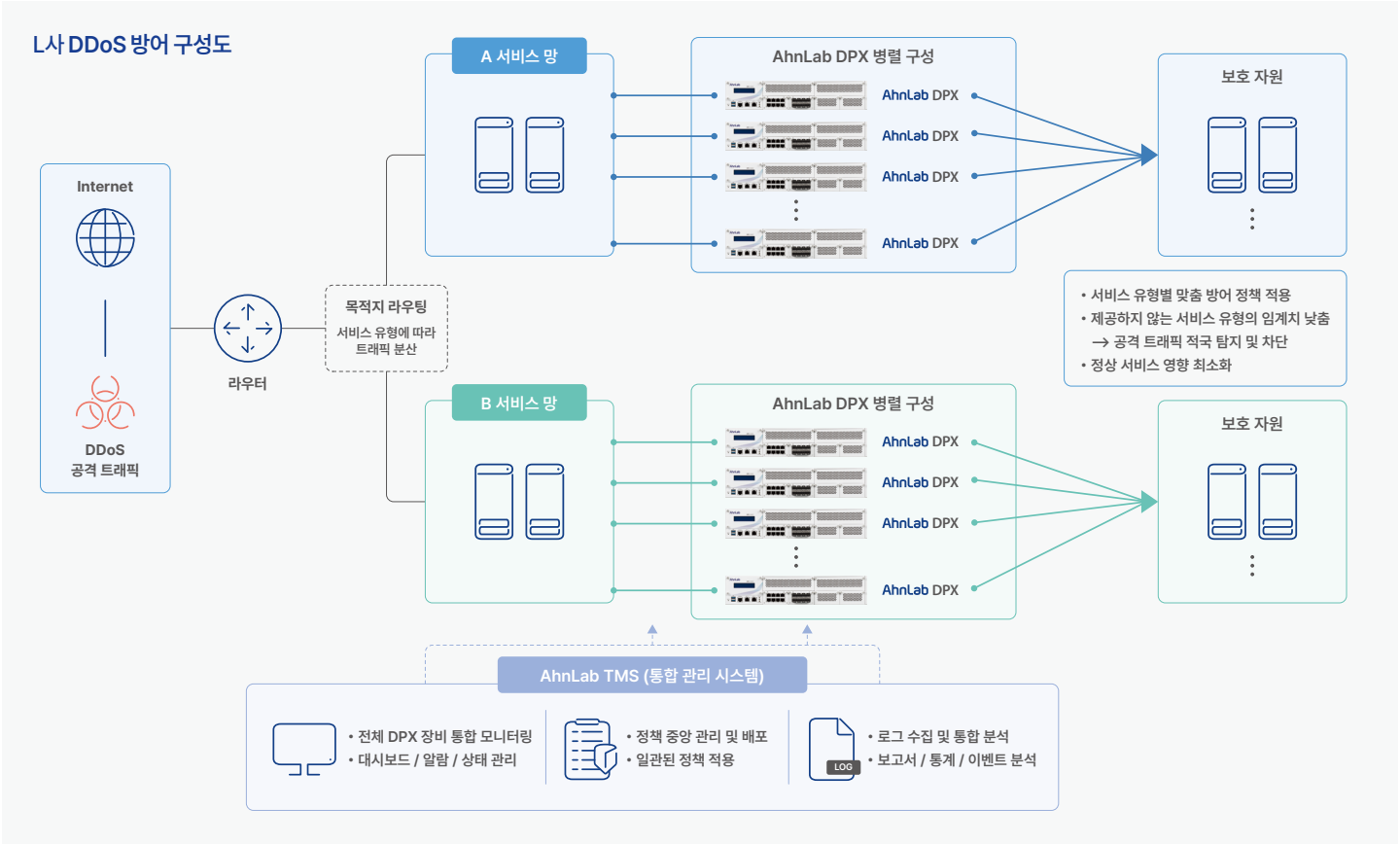
3. AhnLab TMS 기반 통합 관리

L사는 AhnLab TMS를 활용해 다수의 AhnLab DPX 장비를 통합 관리했다. 장비별 정책과 로그를 중앙에서 관리해 개별 장비 관리 부담을 줄이고, 분리된 서비스망의 DPX 장비를 하나의 관리 체계에서 일관되게 운영할 수 있게 됐다.

서비스 유형별 방어 정책

- 행위 규칙 제외 임계치 하향
- Anti-Spoofing
- HTTP 접속 인증
- 비인증 IP 차단 필터
- 기타 서비스 특성에 맞는 DDoS 방어 정책

L사 DDoS 방어 구성도



도입 효과(Business Outcomes)

L사는 서비스 유형별 방어 구조와 통합 관리 체계를 구축해 DDoS 공격 대응력, 서비스 안정성, 운영 효율성을 함께 높일 수 있었다.

1. 서비스 유형별 방어 정책 적용

망분리를 통해 L사는 각 서비스 특성에 맞는 방어 정책을 적용할 수 있게 됐다. 특히 보호 자원에서 제공하지 않는 서비스 유형에 대해서는 행위 규칙의 임계치를 낮춰 공격 트래픽을 보다 적극적으로 탐지하고 차단할 수 있었다. 이를 통해 정상 트래픽에 미치는 영향을 줄이면서도 DDoS 대응 효과를 높일 수 있었다.

2. 대규모 DDoS 공격 대응력 강화

AhnLab DPX 병렬 구성으로 공격 트래픽이 급증하는 상황에서도 특정 장비에 부하가 집중되는 위험을 줄일 수 있었다. 또한 일부 장비에 장애가 발생하더라도 서비스 트래픽이 다른 장비를 통해 처리될 수 있어, 대규모 공격 상황에서도 서비스 안정성과 연속성을 높일 수 있었다.

3. 통합 관리를 통한 운영 효율성 확보

AhnLab TMS를 통해 여러 망에 구성된 AhnLab DPX 장비를 통합 관리함으로써 운영 부담을 줄일 수 있었다. 운영자는 개별 장비별로 정책과 로그를 확인하는 대신, 하나의 관리 체계에서 전체 방어 환경을 일관되게 운영할 수 있게 됐다.

DDoS 공격 대응은 공격 트래픽을 차단하는 것만으로 완성되지 않는다. 방어 기능이 동작하더라도 정상 트래픽에 영향을 주거나 운영 관리가 복잡해지면, 실제 서비스 안정성은 흔들릴 수 있다. L사는 AhnLab DPX를 기반으로 보호 자원의 서비스 특성에 맞는 방어 체계를 구성하고, AhnLab TMS를 통해 분리된 망과 다수 장비를 통합 관리할 수 있는 환경을 마련했다. 이를 통해 대규모 DDoS 공격에 대응하면서도 정상 서비스 영향을 최소화하고, 보다 안정적인 서비스 운영 기반을 확보했다.

이번 사례는 DDoS 방어 체계를 설계할 때 공격 대응력, 서비스 안정성, 운영 효율성을 함께 고려해야 한다는 점을 보여준다. 특히 서비스 유형에 맞는 방어 구조와 통합 관리 체계를 함께 갖추는 것이 고도화되는 DDoS 공격에 대응하기 위한 중요한 기준이 될 수 있다.

기존 환경 대비 개선 효과

Before	After
일괄 방어 정책	서비스 유형별 망 분리
정상 트래픽 영향 우려	임계치 및 방어 정책 최적화
장비별 개별 관리	TMS 기반 통합 관리

AhnLab DPX는 국내 최초 100G NIC을 지원하는 디도스 공격 대응 솔루션 입니다. 글로벌 최고 수준의기능, 성능으로 국가와 고객의 네트워크를 안전하게 보호합니다.
디도스 공격은 가장 오래된 사이버 위협으로, 여전히 가장 빈번하게 발생하는 공격입니다. 정상 트래픽과 공격 트래픽의 경계가 모호하며, 적은 네트워크 지연 발생 만으로 고객 불편을 야기합니다. 또한 AI 기법이 사이버 공격에 활용되면서 공격의 빈도가 증가하고 방식도 다양해지고 있어 이에 대한 대응 체계 구축이 중요해지고 있습니다. 안랩의 기술과 노하우를 기반으로 발전을 거듭하는 AhnLab DPX는 고성능 패킷 처리, 정밀한 트래픽 분석, 다양한 탐지 기법을 통해 디도스 공격에 대응합니다