능동적이고 자동화된 대응·완화·차단 체계 구축 필수

AI/ML 기반 지능형 방어 체계 구현 … 실시간으로 DDoS 공격 패턴 감지·차단

홍정표 넷스카우트코리아 상무
JeongPyo.Hong@netscout.com

DDoS 공격은 기업과 주요 서비스를 마비시키는 심각한 위협이 됐다. 전통적인 방식의 DDoS 방어 방식은 진화하는 공격 패턴에 효과적인 대응과 완화에 한계를 보이고 있다. AI 및 머신러닝(ML) 기술을 활용한 DDoS 방어 솔루션을 심층 분석하고 복잡해지고 정교해지는 새로운 패턴의 DDoS 공격에 대한 효과적인 방어 전략을 살핀다. 〈편집자〉

디지털 전환의 가속화와 더불어 인공지능(AI)의 발전은 사이버 공격에 대한 위협이 새로운 국면으로 접어들었음을 의미한다. 특히 DDoS 공격은 그 규모와 복잡성이 날로 증가하고 있으며, 기업과 주요 서비스를 마비시키는 심각한 위협으로 자리를 잡았다.

전통적인 방식의 DDoS 방어는 급변하고 진화하는 공격 패턴에 효과적인 대응과 완화에 한계를 보이고 있다. AI 및 머신러닝(ML) 기술을 활용한 DDoS 방어 솔루션의 작동 원리를 심층 분석하고 점점 더 복잡해지고, 정교해지는 새로운 패턴의 DDoS 공격에 효과적인 방어 전략을 살핀다.

변화하는 DDoS 공격

기존의 DDoS 공격은 대량의 트래픽을 활용한 방법이 주를 이뤄왔다. 흔히 말하는 플러딩(Flooding), 증폭(Amplification), 반사(Reflection) 등의 공격 수행을 통해 서비스 접속을 차단하거나 단일 서비스를 공격해 타격을 주는 형태가 많았다.

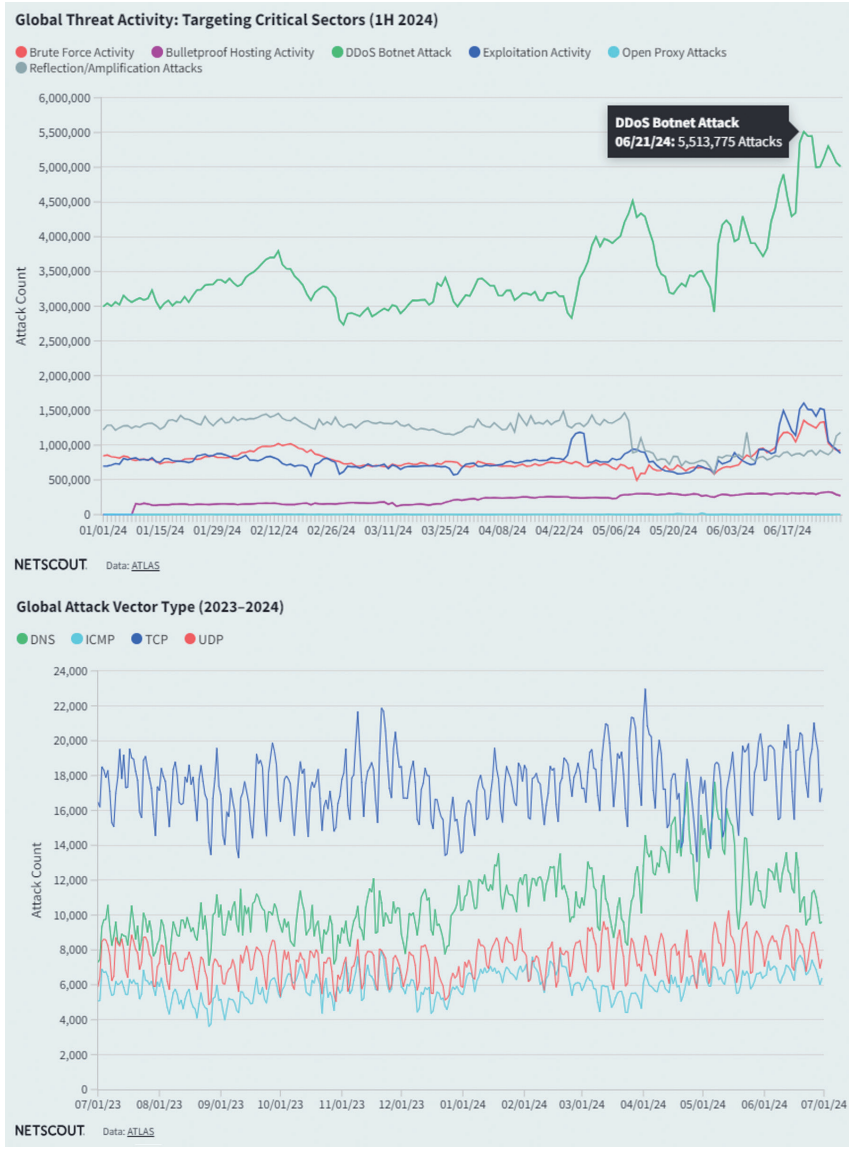
그러나 최근의 DDoS 공격은 그 양상이 다양하게 변화하며 진화하고 있다. 동적 DDoS 공격(D2DoS, Dynamic DDoS)이 증가하고 있으며, 특히 AI 봇넷의 발전은 DDoS 공격을 방어하는 입장에서는 재앙과도 같은 무차별 공격을 당하고 있다.

공격하는 중간에 공격 유형의 변경은 물론 정상 트래픽과 공격 트래픽을 섞어 감지가 어려운 공격(Direct Path Attack), IP 단위 공격이 아닌 CIDR(IP Block) 단위 공격(Carpet Bombing), AI 봇넷과 클라우드 활용을 통한 방대한 공격 소스(Highly Distributed Source Attack)의 작은 트래픽 단위 공격, 구글 DNS 등 글로벌 DNS를 활용한 정상 DNS 요청을 가장한 공격(DNS Water Torture) 등 기존의 대용량 트래픽 공격과 함께 동적으로 변화하는 다양한 공격이 계속되고 있다.

AI/ML 기반 방어선 구축으로 진화하는 DDoS 공격 차단

앞서 언급한 다양한 DDoS 공격에 대응과 완화를 위해 필요한 것은 기존 임계치

〈그림 1〉 글로벌 DDoS 공격 리포트



운영자에게 보고할 수 있는 방안을 지원해야 한다.

DDoS 공격 시나리오 무력화

넷스카우트의 DDoS 공격 방어 솔루션이 제공하는 AI/ML 기반의 방어 체계는 다양한 DDoS 공격 시나리오의 무력화를 위한 최전선의 방어 체계를 구성한다.

데이터 기반의 실시간 트래픽 분석, AI 기반의 위협 인텔리전스를 통한 지능형 DDoS 공격 방어 구성은 미처 차단하지 못한 사이버 보안 위협, 경험하지 못했던 보안 위협, 정상 트래픽을 가장한 공격, 무차별 애플리케이션 공격 등 기존 DDoS 공격 방어 체계를 초월한 다양한 방어 정책과 프로세스를 수립하고, 수행해야 한다.

뿐만 아니라 DDoS 공격 방어를 위한 정책, 설정 권고 등을 자동으로 제공해 동적으로 변화하는 공격에 대한 지속적인 차단 정책을 유지해야 한다.

이러한 자동화 프로세스는 AI/ML 기반의 지속적인 분석, 감지, 알림, 정책 권고를 반복적으로 수행하고 방어 전략을 발전시켜 서비스 운영에 문제 없이 동적 DDoS 공격 시나리오를 무력화한다.

기반의 방어에서 벗어나고, 단순 시그니처 방어 방식의 한계를 극복해야 한다. 실시간으로 DDoS 공격 패턴을 감지하고 차단하는 것에 초점을 맞춰야 하며, 결국 AI/ML 기반 지능형 방어 체계 구축을 통해 능동적이고 자동화된 대응, 완화, 차단 체계가 필요하다.

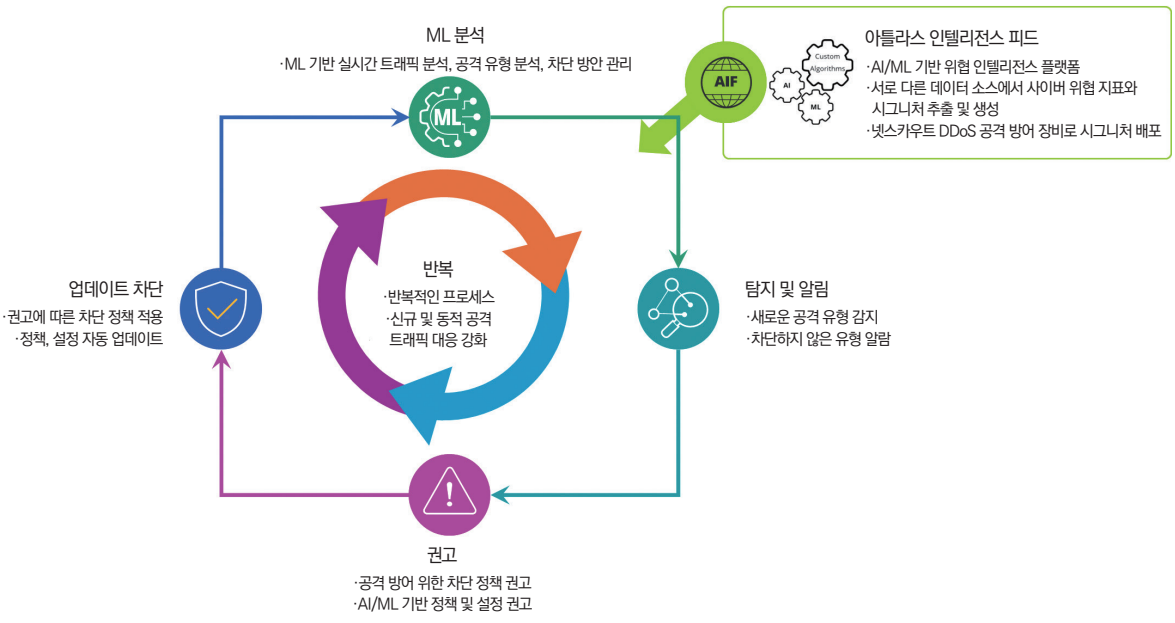
AI/ML 기반의 방어선은 실시간 대응과 분석 체계, 데이터 처리와 지능형 플랫폼 등 다양한 구성 요소를 갖춰야 한다. 덧붙여 경험하지 못한 공격에 대한 방어와 정상 트래픽에 숨겨져 공격을 감행하는 트래픽 유형까지 확인하는 방안을 보유하고

실시간 트래픽 분석·공격 유형 탐지·정책 수립 편의성

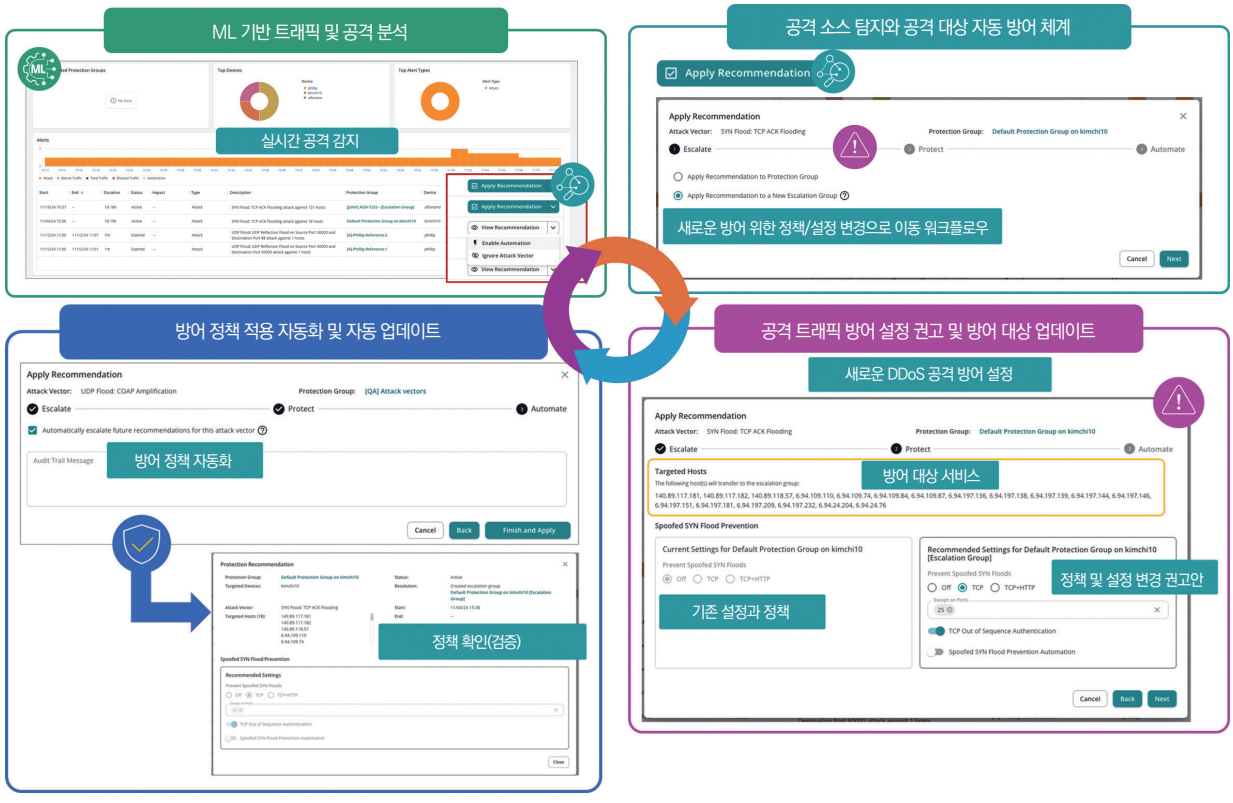
넷스카우트의 DDoS 공격 방어 전략은 사용자 편의성을 위한 자동화 프로세스가 핵심이다.

DDoS 공격에 대비해 전문가는 물론 초보자도 실수 없이 효율적으로 정책을 수립 및 수행하고, 쉽고 빠르지만 정교하고 오탐 없는 방어 체계를 효율적인 사용자 인터페이스 및 사용자 경험(UI/UX)으로 제공한다.

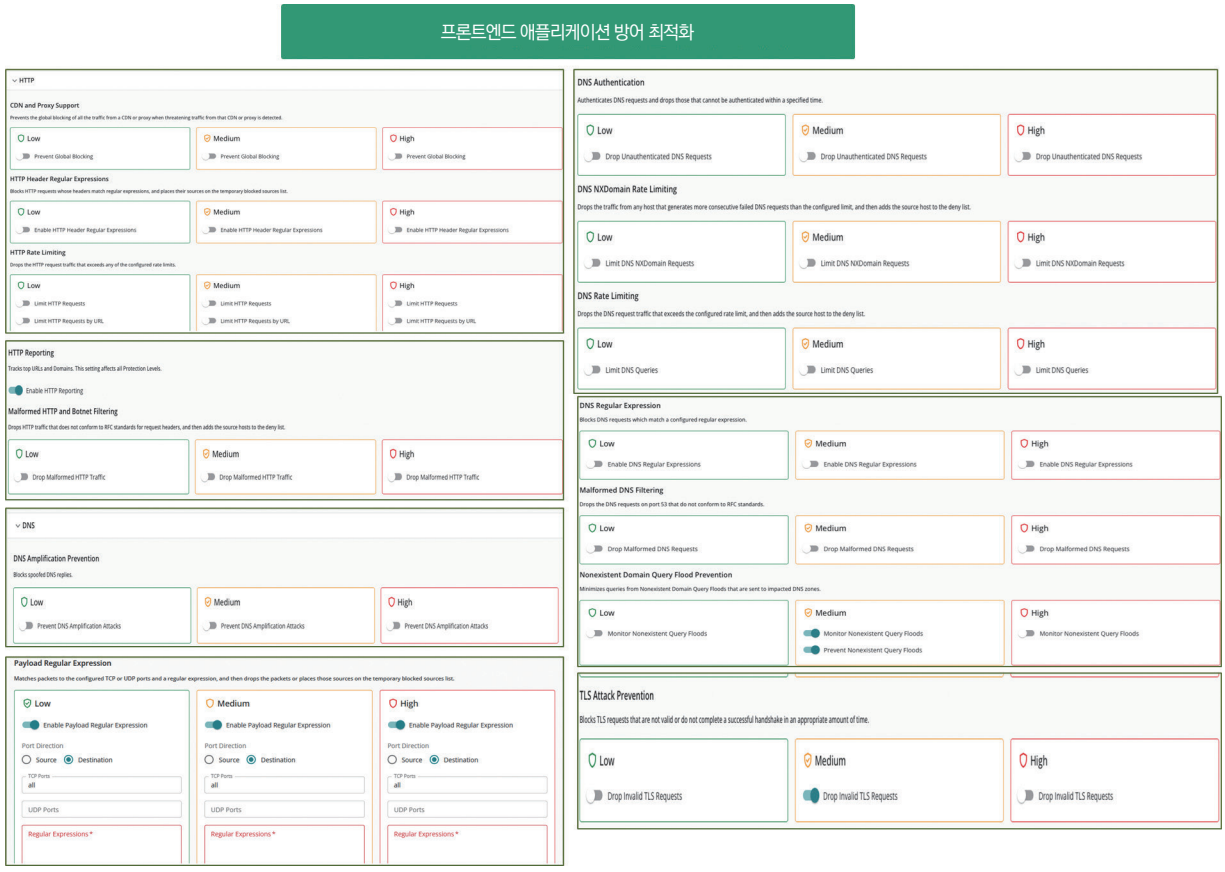
〈그림 2〉 AI/ML 기반 적응형 DDoS 공격 방어 프로세스



〈그림 3〉 UI/UX 기반 AI/ML 방어 프로세스 자동화



〈그림 4〉 애플리케이션 이해하는 방어 체계와 손쉬운 방어 정책 템플릿 적용



애플리케이션 이해하는 방어 체계 구성과 정책 수립

애플리케이션에 직접적인 타격을 가하고 있는 봇넷을 활용한 무차별 공격이 빠르게 증가하고 있다. 따라서 공격을 방어하는 입장에서는 공격의 특성과 보호 대상의 정교한 정책 설정이 무엇보다 필요하다.

가장 최전방에 노출되는 HTTP 및 HTTPS, 서비스 접근의 필수 애플리케이션인 DNS에 대한 공격 차단만 잘 활용해도 실제 사용자와 고객에 대한 서비스 안정성을 매우 높일 수 있다. 애플리케이션을 이해하는 DDoS 공격 방어 솔루션은 DDoS 공격을 넘어선 사이버 위협 방어 체계이자 내부 서비스 인프라 보호를 위한 필수 구성 요소다.

기존 방어 체계 넘어선 새로운 DDoS 공격 위협 완화

DDoS 공격 방어는 변화하고 진화하는 공격 트래픽을 이해하고, 경험하지 못한 공격에 대비해야 하며, HTTPS 등의 암호화 트래픽에 대한 사이버 위협 대응 방안을 수립해야 한다. 이를 통해 조직과 기업이 운영하는 애플리케이션을 보호하고, 나아가 실 사용자에게 원활한 서비스 제공을 위한 가장 최전방의 공격수이자 수비수가 돼야 한다.

이제 DDoS 공격 방어 솔루션은 ML을 기반으로 지속적으로 공격을 분석하고, 가시성 기반의 통찰력 있는 보안 위협 관리와 AI 방어 체계를 구성해야 한다. 또한 운영자의 빠른 판단을 보장하는 명확한 프로세스 기반의 자동화를 제공하고, 손쉽게 운영할 수 있는 데이터 기반의 가시성도 보장해야 한다.

넷스카우트는 유기적인 프로세스와 복잡한 애플리케이션 및 트래픽의 손쉬운 운영 체계, ML 기반의 신뢰성이 높은 정책 자동화, 그리고 분석과 운영의 전 과정을 쉽게 확인할 수 있는 가시성 기반의 DDoS 방어 솔루션을 공급하고 있다.