AhnLab AI PLUS

AhnLab DPX

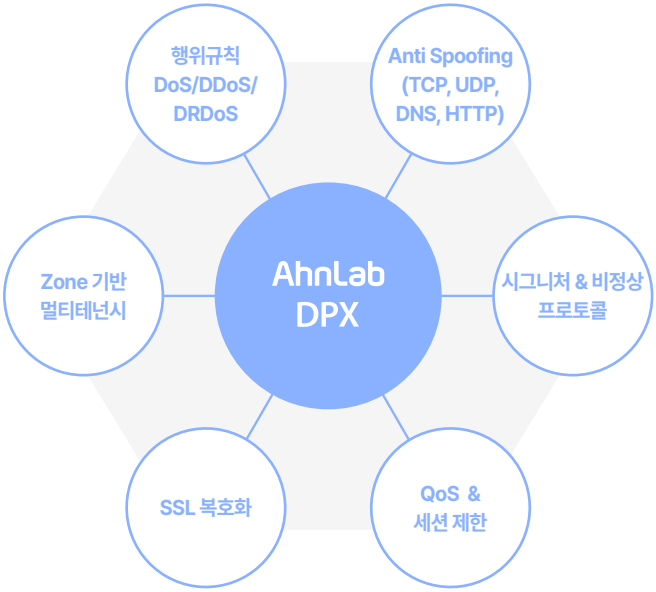
AI 기술을 활용한 지능형 디도스 대응

축적된 디도스 방어 기술과 운영 노하우에 AI 기술을 더해, 변화하는 공격에
효과적으로 대응합니다. 정밀한 트래픽 분석과 다양한 탐지·차단 기술로
디도스 공격을 신속하게 식별하고 안정적인 네트워크 환경을 보호합니다.

제품 개요

AhnLab DPX는 국내 최초로 100G NIC를 탑재한 고성능 디도스 대응 솔루션으로 고성능 패킷 처리와 정밀한 트래픽 분석, 다양한 탐지·차단 기술을 기반으로 AI 기술을 활용해 변화하는 디도스 위협에 효과적으로 대응하고 안정적인 네트워크 환경을 보호합니다.

디도스 공격은 가장 오래된 사이버 위협 중 하나이지만 여전히 빈번하게 발생하며, 공격 방식 또한 지속적으로 진화하고 있습니다. 최근에는 AI 기술이 사이버 공격의 자동화와 고도화에 활용되면서 공격 속도와 형태가 더욱 다양해지고 있어, 정상 트래픽과 공격 트래픽을 정확하게 구분하고 공격 패턴을 신속하게 식별하는 것이 더욱 중요해지고 있습니다. AhnLab DPX는 안랩이 축적해 온 디도스 대응 기술과 운영 노하우를 바탕으로 트래픽 특성과 변화 패턴을 학습하고 분석해 이상 징후를 빠르게 식별하며, AI 기술을 활용해 고도화되는 디도스 위협에 정밀하게 대응합니다.

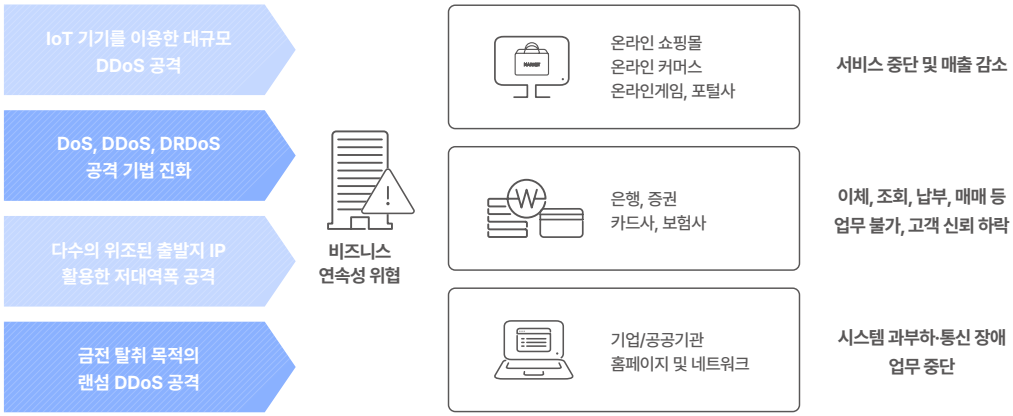


특장점

10G/40G/100G NIC 장착 Inline/Out-of-Path 구축	최대 1,000개 Zone(보호대상) 기반 멀티테넌시 지원
QUIC, HTTPS 프로토콜 대응 SSL Inspection & HTTP 분석 지원	70개 이상 다양한 프로토콜 특징 기반 행위규칙 임계치 대응
DPDK(Data Plane Development Kit)기반 압도적인 고성능 패킷처리	40가지의 로그 생성, 보호 대상별 로그 전송으로 운영 고도화

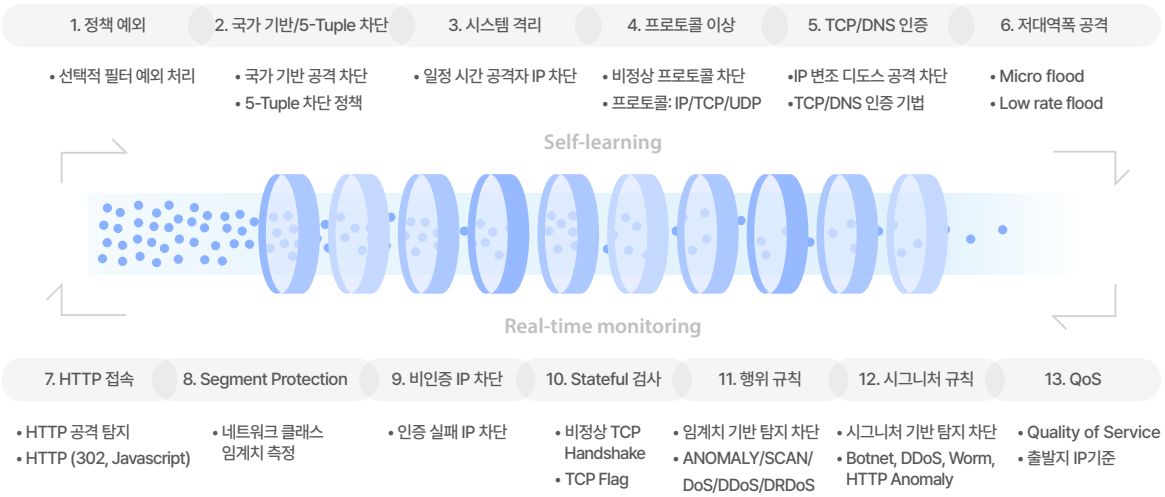
디도스 공격 고도화

일상화, 고도화된 디도스 공격을 대응하기 위한 전문 솔루션이 반드시 필요합니다.



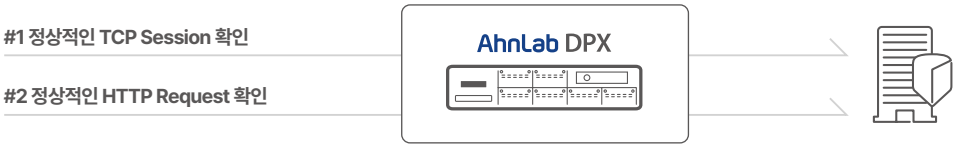
디도스 대응 13단계 필터

13단계 계층형 필터링으로 다양한 DDoS 위협을 전략적으로 완화(Mitigation) 합니다.



인증

트래픽 유발 대상이 사람인지 봇(Bot)인지 식별하는 인증 기능, 안랩이 가장 자신 있습니다.
디도스 공격을 수행하는 Bot 탐지, 차단이 가능합니다.



편의 기능

AhnLab DPX는 다음과 같은 편의 기능을 제공합니다.

위협 대응 편의 기능: 실효성 높은 실시간 대응력과 운영 편의성 제공

- CPU, 메모리, 디스크, 트래픽 등 이상징후를 감지해 경보 알림(Email, SMS, SNMP)
- 패킷 캡처 / 패킷 자동 수집 및 외부 전송 / SNMP 지원

멀티테넌시: 하나의 장비로 다수 환경을 완벽 분리해 비용은 줄이고 보안은 강화

- 보호대상별 Zone 지정 및 별도 정책 설정
- Zone 별 정책/관리자 제공, 로그 전송 및 최적 트래픽 학습(셀프런)
  ※ 라인업별 지원 ZONE 개수 다름

다양한 로그 및 대응 정책으로 완성하는 보안 인텔리전스

- 공격유형, 시간대, 출발지/목적지 등 다양한 요소를 포괄하는 40종의 상세로그 제공
- 공격 탐지 정보, 공격 보고서 / 다수 로그 서버 연동 가능 / SIEM, SOAR 연동

다양한 디도스 공격 유형에 완벽 대응

다양한 디도스 공격, 하나의 해답- AhnLab DPX

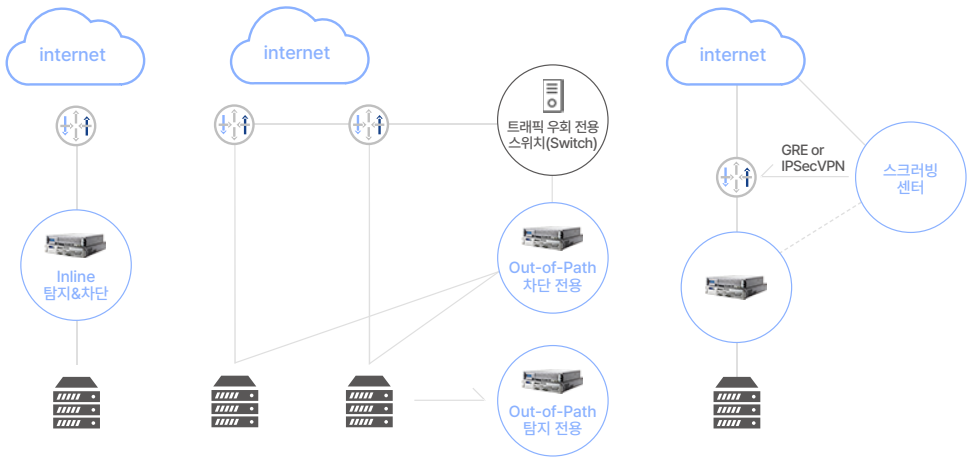
AhnLab DPX는 모든 유형의 DDoS 공격에 대해 선제적인 보안과 정밀한 방어 체계를 제공합니다.

분류	종류	설명	DPX 대응 기능
공격기법	DoS	단일 클라이언트가 단일 서버에 수행하는 공격(1:1)	DoS 행위 규칙 ACL 기반 접근 차단
	DDoS	다수의 PC를 악성코드로 감염, 봇(Bot)으로 동시 공격 다수 클라이언트가 단일 서버에 수행하는 공격 (N:1)	DDoS 행위 규칙 Anti-Spoofing(TCP, HTTP) 시스템 격리 QoS 제어
	DRDoS	반사체를 활용한 UDP 공격 프로토콜, 포트를 바꿔가며 신종 공격 발생	DRDoS 행위 규칙
대용량 디도스	TCP 플러딩	TCP의 구성 요소를 섞어서 공격 SYN, ACK, XMAS(ALL), NULL(Nothing) 등	행위 규칙(TCP) Anti-Spoofing(TCP) Stateful 검사
	UDP 플러딩	UDP의 특성을 활용한 공격, DRDoS와 결합 가능 비 연결성/비 신뢰성 UDP 프로트콜의 특성에 기반 Memcached, SNMP, CHARGEN, DNS, NTP 등	행위 규칙(UDP) Anti-Spoofing(UDP, DNS) Segment Protection
	HTTP 플러딩	HTTP 요청을 활용한 공격 HTTP Method별 공격이 존재(GET, POST 등)	행위 규칙(HTTP, HTTPS) Anti-Spoofing(HTTP) 프로토콜 이상
	Fragmentation 플러딩	단편화된 IP 패킷을 통한 공격 패킷 재조합에 따른 부하를 유도 솔루션 정책 우회를 위한 수단으로 사용	행위 규칙(Fragmentation) 시그니처
	DNS 플러딩	DNS 서버 리소스를 소모시키는 NXDomain 공격	Anti-Spoofing(DNS)
저용량 정밀 타격 디도스	저용량 정밀타격	저용량으로 공격하여 솔루션의 정책을 우회 세션을 종료하지 않고 서버 자원을 점유 & 고갈 유도 예: Exhaustion Attack	Anti-Spoofing(TCP, UDP, HTTP) TCP 세션 제한 프로토콜 이상 시그니처
	비정상 프로토콜	프로토콜의 규칙을 위반한 비정상 프로토콜 공격 취약점의 형태로 발견/대응되는 경우가 많음 잘못된 설정, 애플리케이션의 낮은 버전이 원인 예: Ping of Death, Slowloris, Slowread, LAND, Rudy, Smurf	행위 규칙(Anomaly) 프로토콜이상 시그니처

유연한 구축 방식

다양한 네트워크 환경에 최적화된 유연한 구축 방식 지원

AhnLab DPX는 네트워크 구조에 따라 인라인(Inline)과 아웃오브패스(Out-of-Path) 방식 모두 지원합니다. Inline은 구축이 간편하고 실시간 차단에 유리하며, Out-of-Path는 탐지와 차단을 분리함으로써 대규모 환경에서도 안전한 대응이 가능합니다. 또한 클라우드 스크러빙 센터와 연동해 트래픽이 초과했을 때 이상 트래픽을 스크러빙 센터로 우회시켜 서비스 지속성을 확보할 수 있습니다.



[Inline 구성 방식] [Out-of-Path 구성 방식] [스크러빙 구성 방식]

분류	Inline	Out-of-Path
필요 장비의 수	1대(탐지 & 대응)	2대(Detector: 탐지, Guard: 차단)
특징	실시간 차단, 설치 간편	장애 및 병목 최소화, 기존 네트워크 영향도 낮음
DDoS 대응 속도	매우 빠름	빠름
고객 분류	공공기관, 금융, 학교	ISP, Portal, IDC

제품 사양

구분		AhnLab DPX 5000C	AhnLab DPX 10000C	AhnLab DPX 20000C
CPU		8 Core	32 Core	64 Core
Memory		64GB/128GB	128GB/256GB	256GB/512GB
System Storage		SSD 512GB	SSD 512GB	SSD 512GB
Log storage		SSD 2TB	SSD 2TB	SSD 2TB
NIC	Slot	4	4	4
	1GC	8 (최대 32)	0 (최대 32)	0 (최대 32)
	1GF	2 (최대 16)	4 (최대 16)	8 (최대 16)
	10GF	0 (최대 4)	0 (최대 16)	0 (최대 16)
	40GF	–	0 (최대 4)	0 (최대 4)
	100GF	–	–	0 (최대 4)
Throughput (UDP/64byte)		16G	80G	150G
Throughput (UDP/MAX)		20G	160G	400G
Power		Redundant		
인증		CC인증, GS인증		

※ 성능 수치는 세부 환경 및 시스템 구성에 따라 달라질 수 있습니다.

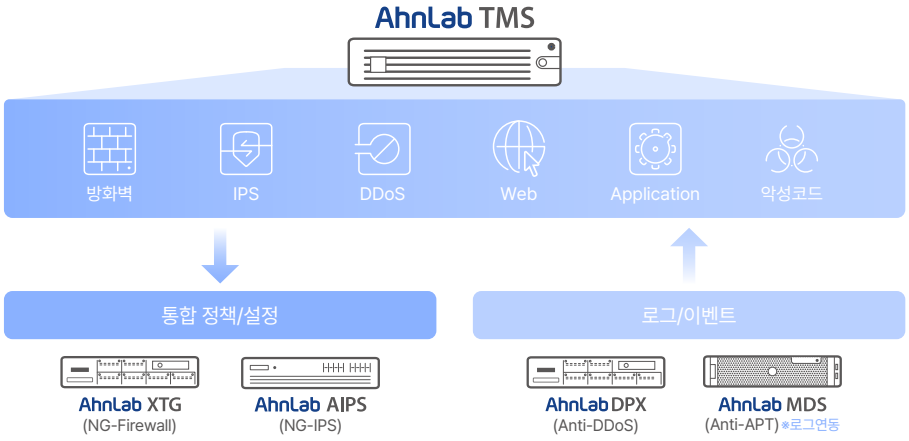
제품과 서비스의 근간을 이루는 기술력

안랩은 위협 분석과 침해 대응을 통해 30여 년간 축적한 방대한 보안 데이터를 기반으로 AI 보안 플랫폼 AhnLab AI PLUS를 운영하고 있습니다. 차별화된 보안 데이터를 학습한 안랩의 AI는 위협 탐지와 대응 역량을 고도화하고, 보안 운영의 생산성 혁신을 지원합니다.



AhnLab

AhnLab DPX는 안랩 네트워크 통합 관리 솔루션 AhnLab TMS와 연동해 향상된 위협 분석 및 대응 시너지를 발휘합니다. AhnLab TMS 연동 시, AhnLab DPX 장비 별 공격 현황 및 Zone 별 실시간 공격 현황과 통계를 한 눈에 확인할 수 있습니다. 또한, AhnLab DPX는 API 제공을 통해 SOAR와 TI 등의 솔루션과 연동이 가능합니다.



경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901
© 2026 AhnLab, Inc. All rights reserved.

AhnLab