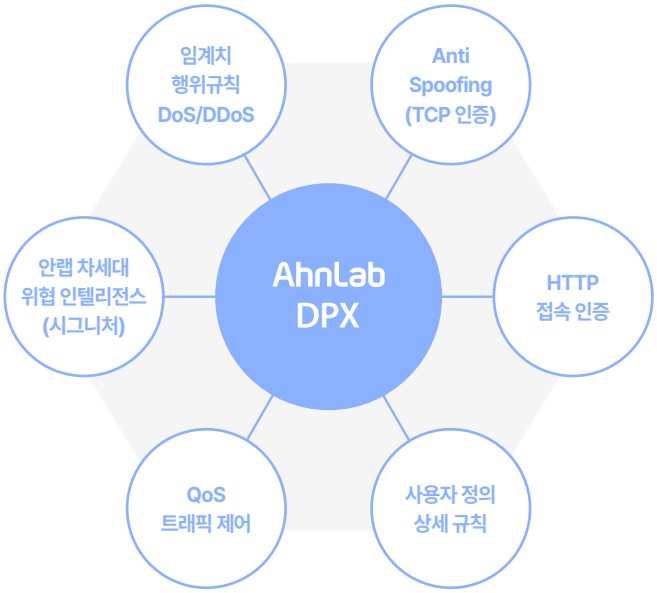
AhnLab DPX

국내 최초, 국내 1위 고성능 디도스 대응 솔루션

디도스 방어 기술, 경험, 전문성의 결합으로
고객 환경을 지키는 가장 견고한 차단선으로
네트워크를 디도스 공격으로 부터 보호합니다.

제품 개요

AhnLab DPX(DDoS Prevention eXpress)는 디도스 공격 대응을 위한 통합 보안 솔루션입니다. 2010년 출시한 이래로 기술적 진보를 통해 명실상부한 국내 1위로 자리잡았으며 국내 디도스 대응 시장을 선도하고 있습니다.
디도스 공격은 가장 오래된 사이버 위협 중의 하나이지만, 여전히 가장 빈번하게 발생하며 위협적인 공격입니다. 특히, 접근이 쉬운 만큼 다양한 형태로 진화하고 있어 단일 탐지 방식만으로는 완벽한 대응이 어렵습니다. 안랩의 축적된 디도스 대응 기술력과 운영 노하우를 기반으로 발전을 거듭한 AhnLab DPX는 고성능 차단 엔진, 정밀한 트래픽 분석, 다양한 탐지 방식을 통해 위협에 대응합니다.

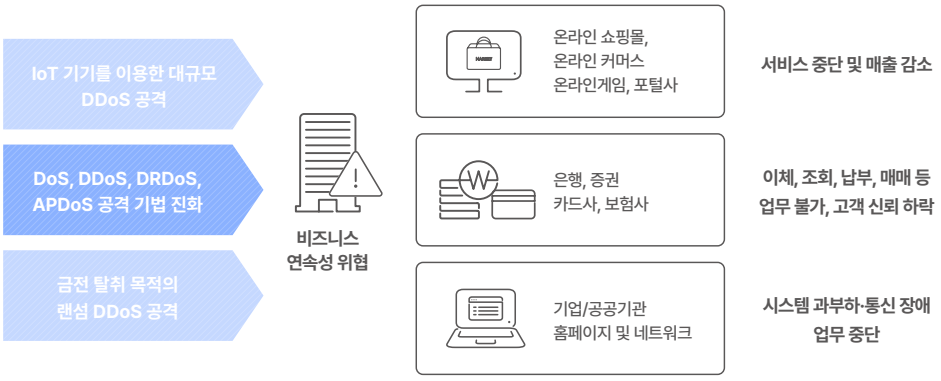


특장점

위협만 정확/정밀하게 탐지가 가능하도록 L2~L7 계층 정보와 패킷의 헤더 뿐만 아니라 페이로드까지 분석	단일장비로 수십개의 테넌시와 서비스 라인을 분리 보호할 수 있는 최대 1,000개 Zone 기반의 멀티테넌시 지원
국내 최초 차세대 프로토콜(QUIC) 대응 및 스크러빙까지 포괄하는 올스택 DDoS 공격 완화 솔루션	60개 이상의 행위규칙 기반 디도스 트래픽 핀셋 대응
DPDK(Data Plane Development Kit)기반의 압도적인 고성능 패킷처리	40가지의 로그 생성, 보호 대상별 로그 전송으로 운영 고도화

디도스 공격 고도화

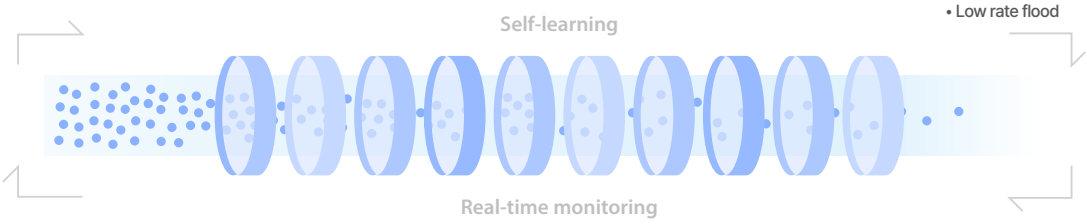
일상화, 고도화된 디도스 공격을 대응하기 위한 전문 솔루션이 반드시 필요합니다.



디도스 대응 13단계 필터

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

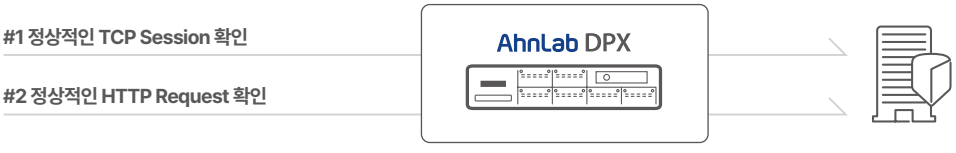
1. 국가 기반 차단	2. 정책 예외/접근 차단	3. 시스템 격리	4. 프로토콜 이상	5. TCP/DNS 인증	6. 저대역폭 공격
• 특정국 디도스 공격 차단 • 특정국 향하는 트래픽 차단	• 5tuple 기반으로 차단 • 선택적 필터 예외 처리	• 일정 시간 공격자 IP 차단	• 비정상 프로토콜 차단 • 프로토콜: IP/TCP/UDP	•IP 변조 디도스 공격 차단 •TCP/DNS 인증 기법	• Micro flood • Slowris • Low rate flood



7. HTTP 접속	8. Segment Protection	9. 비인증 IP 차단	10. Stateful 검사	11. 행위 규칙	12. 시그니처 규칙	13. QoS
• HTTP 공격 탐지 • HTTP (302, Javascript)	• 네트워크 클래스 별 임계치 측정	• 인증 실패 IP 차단	• 비정상 TCP Handshake • TCP Flag	• 임계치 기반 탐지 차단 • ANOMALY/SCAN/ DDoS/DoS	• 시그니처 기반 탐지 차단 • Botnet, DDoS, Worm, HTTP Anomaly	• Quality of Service • 출발지 IP기준

인증

트래픽을 유발하는 대상이 사람인지 봇(Bot)인지 식별하는 인증 기능, 안랩이 가장 자신 있습니다.
대부분의 자동화된 디도스 공격 Bot을 탐지, 차단할 수 있습니다.



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 별도 정책 및 Zone 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
  - 보호 대상별 트래픽 현황을 입체적으로 파악
- 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

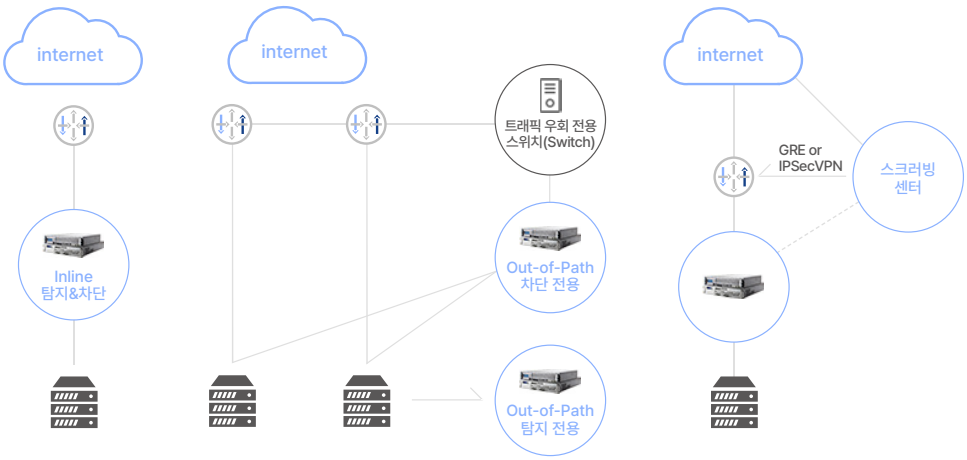
AhnLab DPX는 모든 유형의 DDoS 공격에 대해 선제적인 보안과 정밀한 방어 체계를 제공합니다.

분류	종류	설명	DPX 대응 기능
공격기법	DoS	단일 클라이언트가 단일 서버에 수행하는 공격 (1:1)	DoS 행위 규칙 ACL 기반 접근 차단 임계값 기반 행위 규칙 설정 TCP/UDP/ICMP 프로토콜별 접근제어
	DDoS	다수의 PC를 악성코드로 감염, 봇(Bot)으로 동시 공격 다수 클라이언트가 단일 서버에 수행하는 공격 (N:1)	DDoS 행위 규칙 Anti-Spoofing(TCP 인증) HTTP 접속 인증 시스템 격리 QoS 제어 및 우회 설정
	DRDoS	반사체를 활용한 UDP 공격 프로토콜, 포트를 바꿔가며 신종 공격 발생	행위 규칙 기반 DRDos 및 증폭 공격 탐지 ACL 기반 접근 차단 DRDoS Amplifier 공격 탐지
대용량 디도스	TCP 플러딩	TCP의 구성 요소를 섞어서 공격 SYN, ACK, XMAS(ALL), NULL(Nothing) 등	행위 규칙(TCP) Anti-Spoofing(TCP 인증) 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) Segment Protection DNS 인증
	HTTP 플러딩	HTTP 요청을 활용한 공격 HTTP Method별 공격이 존재(GET, POST 등)	행위 규칙(HTTP) HTTP 접속 인증
	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(NXDomain 인증)
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 인증) HTTP 접속 인증 시그니처 프로토콜 이상
	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) Anti-Spoofing(TCP 인증) HTTP 접속 인증 시그니처 프로토콜 이상

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. Inline 은 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

스크러빙 및 TI 연동

AhnLab DPX는 클라우드 스크러빙 센터와 유기적으로 연동되어 급격한 트래픽 증가 시 트래픽을 자동으로 스크러빙 센터로 우회하여 서비스 중단 없는 실시간 보호를 보장합니다. 또한, TI 연동을 통한 IP 평판조회 기능을 제공합니다.

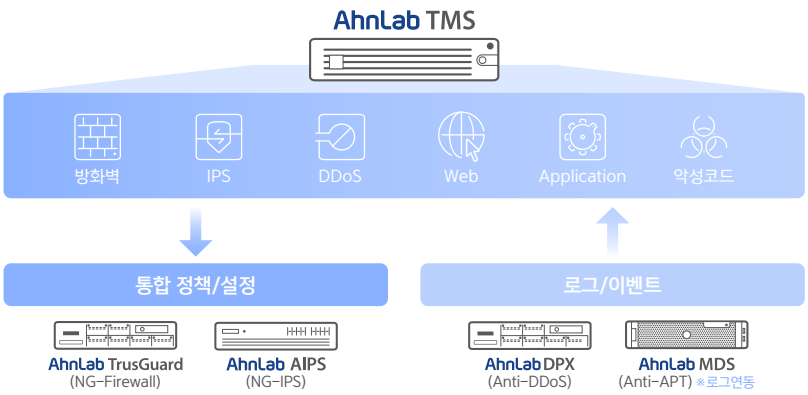
제품 사양

구분		AhnLab DPX 5000C	AhnLab DPX 10000C	AhnLab DPX 20000C
CPU		8Core	16Core x 2	32Core x 2
Memory		128GB	256GB	512GB
Log storage		SSD 2TB (1.92TB)	SSD 2TB (1.92TB)	SSD 2TB (1.92TB)
NIC	1GC	(최대32) Mgmt 별도	(최대 64) Mgmt 별도	(최대 64) Mgmt 별도
	1GF	(최대 8)	(최대 16)	(최대 16)
	10GF	(최대 8)	(최대 16)	(최대 16)
	40GF	–	(최대 4)	(최대 4)
	100GF	–	–	(최대 4)
Power		550W, Redundant	1300W, Redundant	1300W, Redundant
CC 인증		EAL4 (DDoS 대응장비 보안 요구사항 V3.0)		

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

AhnLab

AhnLab DPX는 안랩의 네트워크 위협 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 같은 자동화 솔루션과 연동이 가능합니다.



경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901

AhnLab