AhnLab DPX

국내 최초, 국내 1위 100G 디도스 대응 솔루션

디도스 방어 기술, 경험, 전문성의 결합
대한민국 네트워크를 디도스 공격으로 부터 보호합니다.

제품 개요

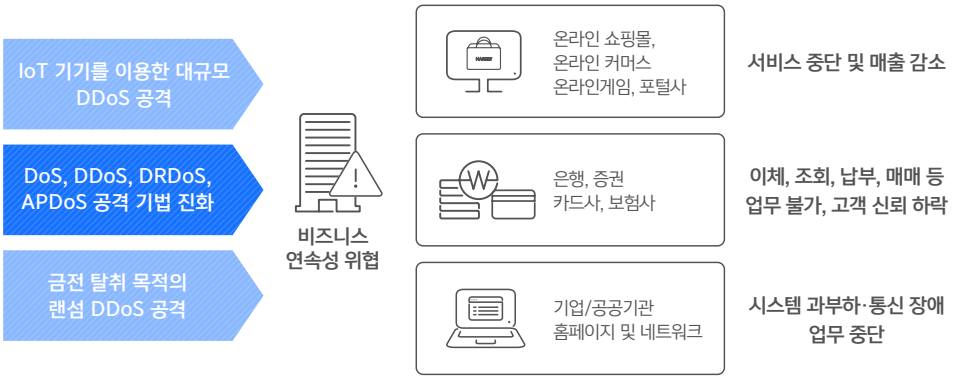
AhnLab DPX(DDoS Prevention eXpress)는 디도스 공격 대응을 위한 솔루션입니다. 2010년 최초 출시한 AhnLab TrusGuard DPX v1.0를 토대로 2021년 AhnLab DPX v2.0을 출시하였습니다. 안랩의 디도스 대응 전문 기술과 노하우를 바탕으로 국내 최초 100G 환경에서 디도스 공격 대응을 시작합니다.
디도스는 가장 오래됐지만, 아직도 가장 빈번한 공격입니다. 역사가 깊은 만큼 쉽게 공격을 수행할 수 있으며, 방법도 많습니다. 이러한 디도스 공격 대응을 위해서 여러가지 대응 기법이 필요합니다. AhnLab DPX는 다음과 같은 디도스 대응 기능을 제공합니다.

특장점

40G, 100G NIC을 지원하는 **국내 최초 제품**	IP Pool, Profile 정책 구조보다 편리한 **최대 300개 Zone 기반의 멀티테넌시 지원**
최신 인텔 서버 플랫폼 사용 **고성능 DPX 20000B 모델 신규 출시**	60개 이상의 행위규칙 기반 **디도스 트래픽 핀셋 대응**
DPDK(Data Plane Development Kit)기반의 **압도적인 고성능 패킷처리**	40가지의 로그 생성, 보호 대상별 로그 전송 **고성능 트래픽 센서 역할**

디도스 공격 고도화

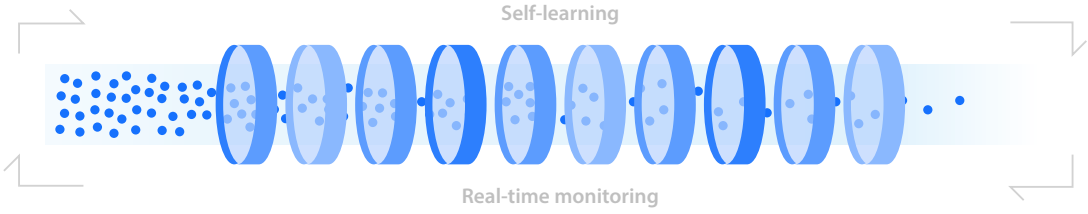
일상화, 고도화된 디도스 공격을 대응하기 위한 전문 솔루션이 반드시 필요합니다.



디도스 대응 12단계 필터

디도스 공격은 다음 12단계 필터로 대응, 완화(Mitigation) 합니다.

1. 국가 기반 차단	2. 정책 예외/접근 차단	3. 시스템 격리	4. 프로토콜 이상	5. TCP/DNS 인증	6. HTTP 접속 인증
· 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	· HTTP 공격 탐지 · HTTP (302, Javascript)



7. Segment Protection	8. 비인증 IP 차단	9. Stateful 검사	10. 행위 규칙	11. 시그니처	12. QoS
· 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 대역폭 제한

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: 위협 대응 편의 기능

- 경보 알림(Email,SMS)
- 패킷 캡처 / 패킷 자동 수집 & 전송 / SNMP

멀티테넌시: 보호 대상별 최적화된 정책

- 보호대상 별 Zone 설정 (최대 300개)
- Zone별 정책, 관리자 제공 / Zone별 로그 전송 / Zone별 최적 트래픽 학습(셀프런)

다양한 로그: 탐지 및 대응 정책 강화

- 40종류 로그 생성 – 보호 대상별 트래픽 현황 파악
- 공격 탐지 정보, 공격 보고서 / 다수 로그 서버 연동 가능 / SIEM, SOAR 연동

디도스 완벽 대응

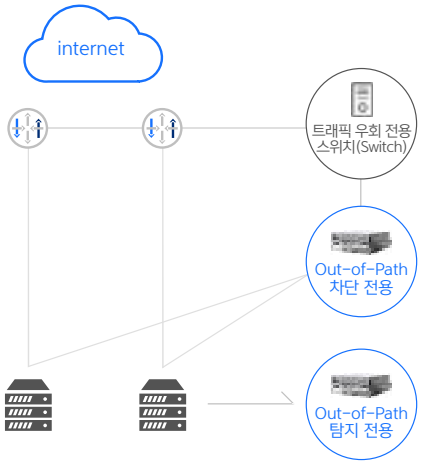
다양한 디도스 공격, AhnLab DPX로 방어할 수 있습니다. AhnLab MDS(APT), AhnLab TMS, AhnLab SOAR와 같이 사용하면 향상된 디도스 대응이 가능합니다.

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 인증) HTTP 접속 인증 시스템 격리 QoS
	DRDoS	반사체를 활용한 UDP 공격 프로토콜, 포트를 바꿔가며 신종 공격 발생	행위 규칙 ACL 기반 접근 차단
	APDoS	APT 공격을 위한 수단으로서의 디도스 공격 디도스로 관리자 시선을 유도 후, APT 등 공격 다수 벡터를 활용한 디도스 공격을 지칭하기도 함	APT, 랜섬웨어 대응 솔루션 국내 1위 AhnLab MDS로 대응 가능합니다. ※2021년 차세대세계일류상품
	랜섬 디도스	금전적 보상을 위한 협박성 공격 협박을 위한 실력 과시용 디도스 공격을 동반	
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
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

솔루션 구성 및 구축 방식

AhnLab DPX는 2가지 구성으로 설치할 수 있습니다. Inline은 구축이 용이한 장점이 있고, Out-of-Path는 탐지와 차단을 분리해 DDoS를 대응할 수 있는 장점이 있습니다.

[Inline 구성 방식]



[Out-of-Path 구성 방식]

분류	Inline	Out-of-Path
필요 장비의 수	1대 (탐지 & 대응)	2대 (Detector: 탐지, Guard: 차단)
설치 난이도	낮음	높음
DDoS 대응 속도	매우 빠름	빠름
고객 분류	공공기관, 금융, 학교	ISP, Portal, IDC

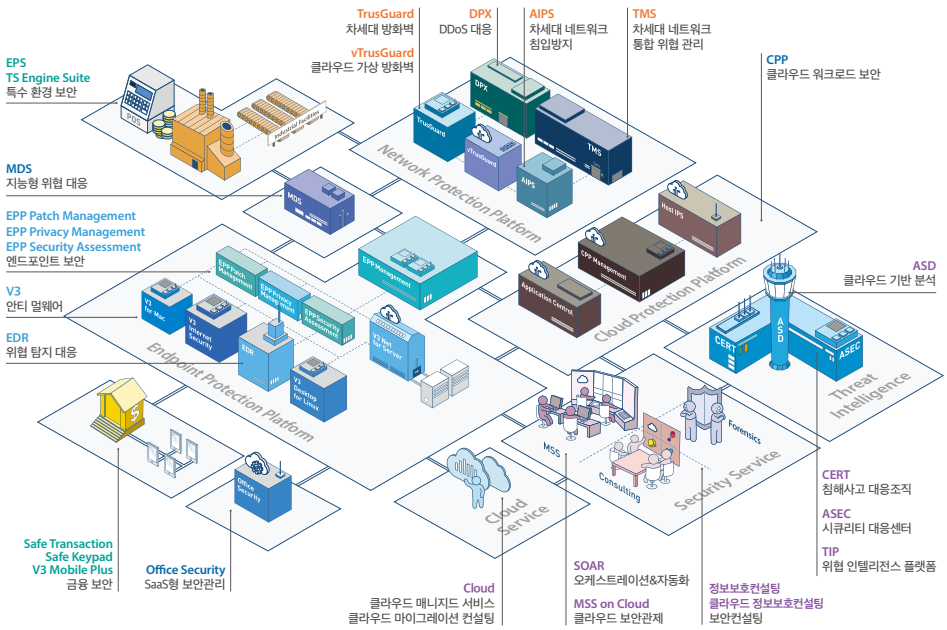
제품 사양

구분		AhnLab DPX 5000B	AhnLab DPX 10000B	AhnLab DPX 20000B
Throughput		10G	60G	150G
CPU		8Core	32Core	48Core
Memory		64GB	128GB	256GB
HDD		2TB	2TB	2TB
NIC	1GC	10 (최대 18, Mgmt 포함)	2 (최대 34, Mgmt 포함)	2 (최대 34, Mgmt 포함)
	1GF	2 (최대 8)	0 (최대 16)	0 (최대 16)
	10GF	0 (최대 8)	4 (최대 16)	12 (최대 20)
	40GF	-	0 (최대 4)	0 (최대 4)
	100GF	-	-	0 (최대 4)
Power		550W, Redundant	800~900W, Redundant	800~900W, Redundant
CC 인증		EAL4 (DDoS 대응장비 보안 요구사항 V1.0)		
GS 인증		1등급 (23년 4월)		

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

AhnLab

AhnLab은 글로벌 통합 보안 기업으로 다양한 솔루션과 전문 서비스 체계를 구축하고 있습니다. AhnLab DPX는 AhnLab TMS(네트워크 통합 보안), AhnLab SOAR(SOAR)와 연동 가능하며, 별도로 전문적인 보안 관제 서비스를 받으실 수 있습니다.



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

AhnLab