AhnLab TrusGuard DPX

실망 40G 성능의 국내 시장점유율 1위 DDoS 대응 솔루션

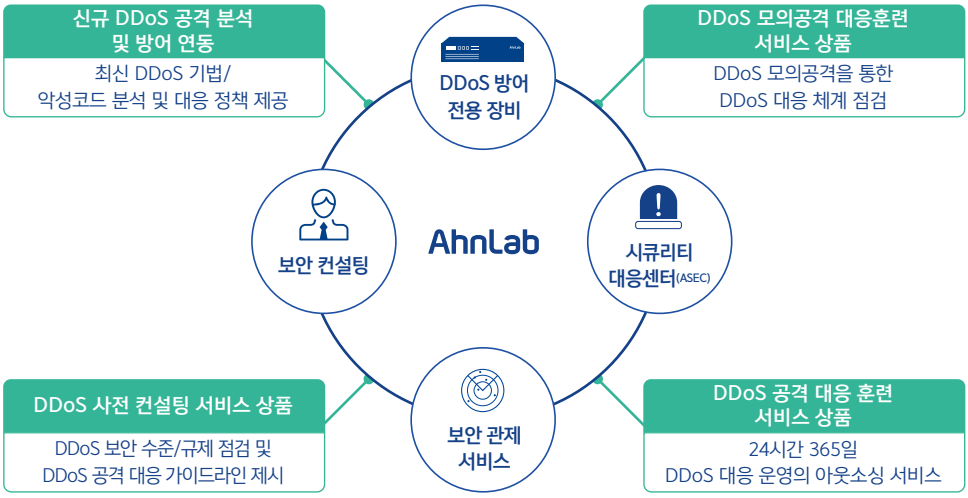
DDoS 방어 기술, 인프라, 경험, 전문가의 결합
DDoS 공격 방어를 위한 종합 프로세스 제공

강력한 방어 | 다단계 필터 | 고성능 | 자가 학습

제품 개요

AhnLab TrusGuard DPX(DDoS Prevention eXpress)는 고도화, 지능화되고 있는 DDoS 공격 방어를 위한 "방어 성능 최대 40G, 다양한 DDoS 완화/대응/차단 기능(임계치 기반 행위규칙, 프로토콜 인증, 시그니처 등), 기술 지원 프로세스"를 제공하는 국내 최고의 DDoS 대응 솔루션 입니다.
안랩 TrusGuard DPX는 진화하는 DDoS 공격으로부터 기업의 비즈니스 환경을 보호합니다.

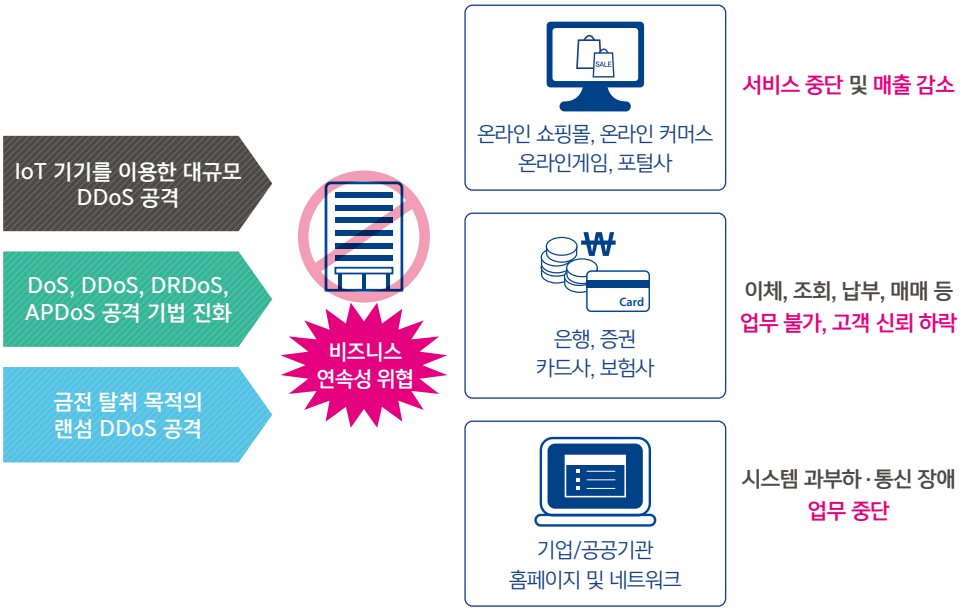
- **국내 DDoS 솔루션 시장점유율 전체 1위(2017년 보고서 기준)**
  (출처: "South Korea Distributed Denial of Service(DDoS) Solution Market, Forecast to 2021", Frost & Sullivan, 2017-08)
- **서비스 가용성(Availability) 장애에 따른 매출 감소, 서비스 중단 및 평판 하락 방지**
- **자동 방어 대응을 통해 인력 투입 부담 최소화**
  - 임계치 기반 행위규칙과 TCP/HTTP/DNS 인증 기법을 포함한 10단계 필터 기반 자동 방어 설정으로 운영 리소스 절감
- **신종 DDoS 공격에 대한 신속한 대응 가능**
  - 신종 공격 발견 시, 즉각적인 대응 규칙 업데이트
- **모의 DDoS 공격 대응 훈련을 통한 기업의 DDoS 방어 능력 측정**
  (DDoS 공격 모의 대응 훈련 서비스 별매)
- **24시간 x 365일 관제 서비스를 통한 실시간 모니터링**
  ('TrusGuard DPX + 보안관제 서비스' 이용 고객에 한 함)
- **기업 내부의 좀비 PC 탐지 및 제거, 내부로부터의 DDoS 공격 발생 방지**
  ('TrusGuard DPX + AhnLab MDS' 사용 고객에 한 함)



[안랩의 DDoS 서비스 운영 프로세스]

DDoS 공격의 고도화

DDoS 공격은 정상 패킷을 대량 전송하여 네트워크의 운용을 마비시키는 형태와, 프로토콜/서버/애플리케이션의 취약점이나 낮은 가용성을 공략하기 위한 소량의 비정상 패킷을 전송하는 형태로 상시 발생하고 있습니다. 또한, 네트워크 환경의 변화(5G 모바일 네트워크, 10G 기가 인터넷 상용화), IoT 기기와 같은 장비의 통신 기능 탑재로 인한 DDoS 공격이 가능한 좀비 Client가 보편화되어 더욱 빈번하게 DDoS 공격이 발생하고 있습니다.



주요 DDoS 공격 방어 유형

TrusGuard DPX는 네트워크 환경을 Zone이라는 가상화된 공간으로 구분하며, Zone의 환경에 따라 프로토콜을 기반으로 한 트래픽 자동 학습을 수행합니다. 학습된 데이터를 기반으로 DDoS 공격에 대응하거나, 인증 기법을 활용하여 최신 DDoS 공격을 자동으로 방어합니다. 그 밖의 신종 공격 Tool이나 비정상 패킷에 대하여 시그니처 기반 차단을 수행합니다.

실시간 트래픽 유효성 검증 및 트래픽 유형별 자동 학습 기반의 DDoS 공격 방어

네트워크에서 애플리케이션(HTTP)까지 종합적인 DDoS 공격 대응

출발지 IP(Source IP) 기반의 DDoS 공격 방어
- TCP 플러딩(Flooding): SYN, SYN-ACK, ACK, Fin, PSH, RST, URG, XMAS 등
- 기타 플러딩: UDP, ICMP, IP, Fragments, DNS Query
- 변조(Spoof)된 출발지 IP 기반의 DDoS 공격 방어

TCP Session 기반 공격 방어
- TCP Multi-Connection, TCP Established Attack, 저대역폭 TCP Session Flooding

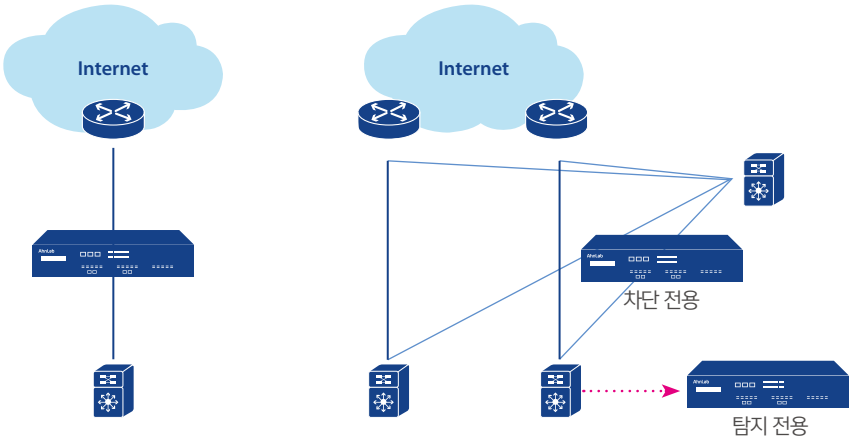
HTTP 기반 DDoS 공격 방어
- HTTP Get Flooding, HTTP Null Page Flooding, HTTP CC Attack, HTTP Redirect 우회 Flooding, SQL Query 기반 HTTP 공격 등

신종 DDoS 공격 방어
- RUDY, Slowloris, DNS Amplification, DNS Spoofing 공격 등
- IPv6 공격 탐지/ 방어

특장점

TrusGuard DPX는 DDoS공격을 탐지/대응/완화/차단하기 위한 전용 장비로, 다단계 방어와 실망 성능을 보장하는 인증기능을 제공합니다. 이를 통해 오탐을 최소화 하면서도 서비스 가용성을 보장할 수 있습니다.

DDoS 공격 완벽 방어	· 기존 솔루션에서 탐지하지 못하는 임계치 이하의 소규모 정밀 타격형 신종 HTTP 공격에 대해서도 강력한 방어 가능 · IPv6 기반 DDoS 공격 대응 기능 지원
다단계 필터 구조	· 다단계 필터를 통해 다양한 유형의 DDoS 공격 탐지 및 방어 · 정상 패킷 · 세션 검증, TCP/HTTP/DNS 유효성 검증, 시그니처 기반 탐지 · 방어 등 10여 개 DDoS 공격 방어 필터 적용
오탐에 의한 장애 최소화	· TCP 세션 요청, HTTP 요청 및 DNS 요청의 정상 · 비정상을 정교하게 판단해 오탐에 의한 서비스 장애 방지
탁월한 성능	· 양방향 최대 40Gbps의 방어 성능
유연한 구성 방식	· 인라인(In-line) 구성 방식 및 아웃오브패스(Out-of-Path) 구성 방식을 제공해 다양한 네트워크 환경에 유연하게 적용 가능 · 국내 유일 OOP 환경에서의 CC인증 획득
혁신적인 분산 관리	· 최대 328개의 논리적인 네트워크에 대한 분산 관리 지원 (IPv4 200개, IPv6 128개) · 개별 존 정책 설정 및 존 관리자를 통한 개별 모니터링 가능
안랩의 기술과 노하우 (인증 및 특허)	· CC 인증 : EAL 4 획득 · “분산 서비스 거부 공격 차단 장치 및 방법” 국제 특허 획득 · “분산 서비스 거부 공격 방어방법 및 방어시스템” 특허 획득



[인라인 방식] [아웃오브패스 방식]

[TrusGuard DPX 인라인과 아웃오브패스 구성 방식 동시 지원]

주요 UI

▲ 필터 현황 모니터

▲ 공격탐지현황 대시 보드

제품 사양

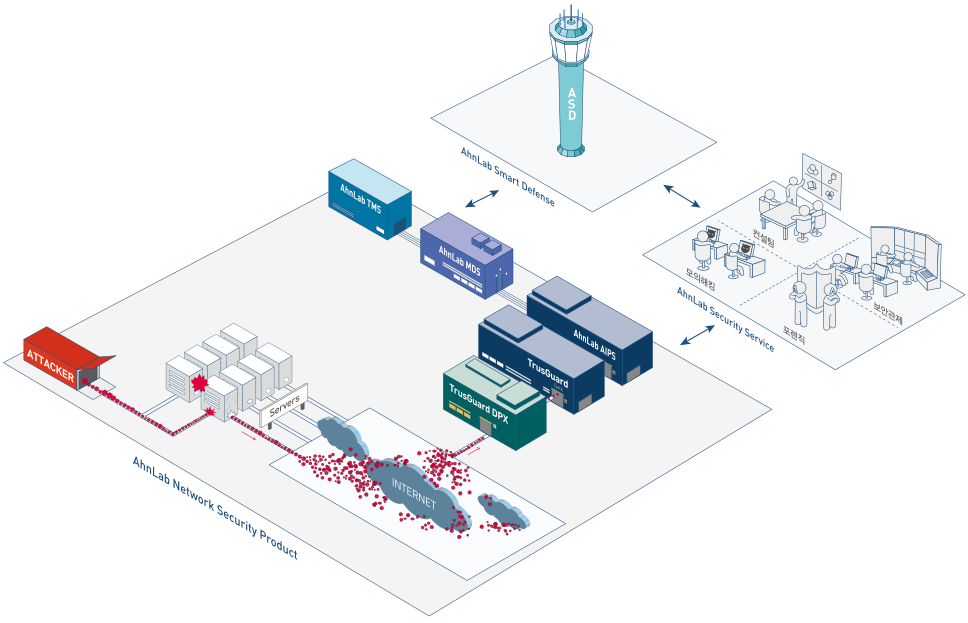
TrusGuard DPX 6000A

TrusGuard DPX 10000A

		TrusGuard DPX 6000A	TrusGuard DPX 10000A
Throughput (Max)		10G	40G
CPU		6 Core	28 Core
RAM		64GB	64GB
CFast		8GB	8GB
인터페이스 기본 (옵션)	1GC	10 (최대 34, Mgmt 포함)	2 (최대 34, Mgmt 포함)
	1GF	2 (최대 16)	0 (최대 16)
	10GF	0 (최대 16)	4 (최대 16)
Bypass		Support	Support
전원		550W Redundant	550W Redundant
CC 인증		EAL4	

TrusGuard DPX만의 경쟁력

TrusGuard DPX와 더불어 차세대 방화벽 TrusGuard, 차세대 네트워크 침입방지 솔루션 AhnLab AIPS, APT 대응 솔루션 AhnLab MDS로 청정 네트워크를 구현합니다. 또한 4개의 제품을 통합 관리 할 수 있는 솔루션 AhnLab TMS를 제공하여, 심층적인 위협 분석 및 효율적인 통합 정책 관리를 수행 할 수 있습니다.



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