AhnLab TrusGuard DPX

20G 실망 성능의 지능형 DDoS 대응 솔루션

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

강력한 방어 | 다단계 필터 | 고성능 | 자가 학습

제품개요

AhnLab TrusGuard DPX(DDoS Prevention eXpress)는 고도화, 지능화되고 있는 DDoS 공격 방어를 위해 실망 트래픽 20G의 탁월한 성능과 종합 대응 프로세스까지 제공하는 **지능형 DDoS 공격 방어 전용 제품**입니다. 안랩은 TrusGuard DPX를 통해 진화하는 DDoS 공격으로부터 기업의 비즈니스 환경을 보호합니다.

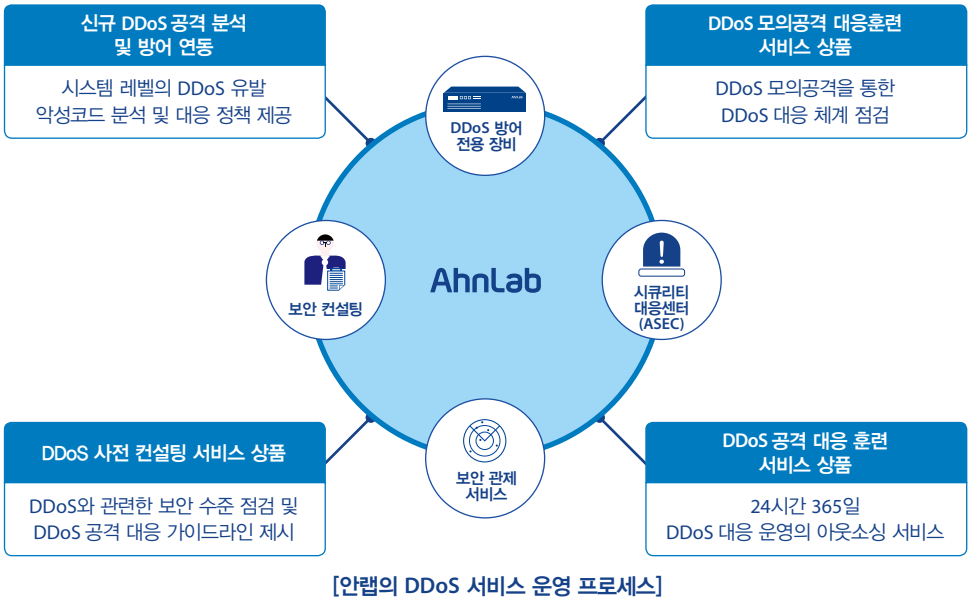
- **서비스 장애에 따른 매출감소, 업무 중단 및 평판 하락 방지**
- **자동 대응을 통한 인적 리소스 부담 최소화**
  - 다양한 필터와 자가 학습(Self-Learning)을 통한 자동 방어 설정 기능으로 운영 리소스 절감
  ※ 자동 방어 및 자동 우회 기능 미제공 시, 공격이 진행 되는 동안 관리자가 수동으로 설정을 지속적으로 변경 해야만 합니다.
- **신종 DDoS 공격에 대한 신속한 대응 가능**
  - 신종 공격 발견 시, 즉각적인 대응 필터 적용
  ※ 안랩은 지속적으로 신종 악성코드를 모니터링 및 분석하고 있으며,
  이를 통해 2009년 7·7 DDoS 대란, 2011년 3·4 DDoS 공격 당시 그 진가를 유감없이 발휘한 바 있습니다.
- **모의 DDoS 공격 대응 훈련을 통한 기업의 DDoS 방어 능력 측정**
  (DPX 구매 시 DDoS 공격 대응 모의훈련 1회 무상 제공)
- **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 동시 운용 시)


TrusGuard DPX 2000A


TrusGuard DPX 6000


TrusGuard DPX 10000

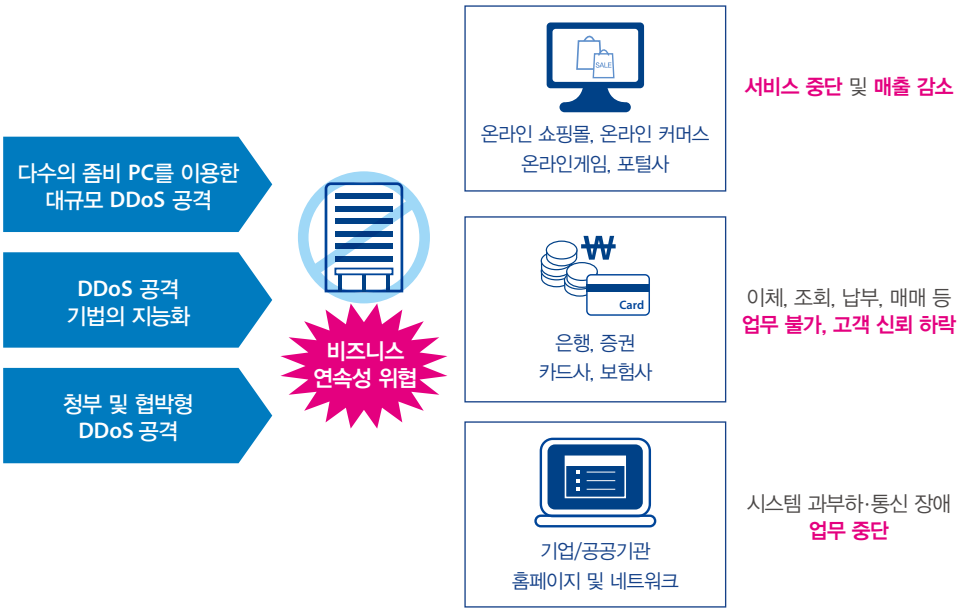

TrusGuard DPX 10000A



[안랩의 DDoS 서비스 운영 프로세스]

DDoS 공격의 고도화

DDoS(Distributed Denial of Service, 분산서비스거부) 공격은 대량의 네트워크 패킷을 전송하여 네트워크 장비의 운용을 마비시키는(Service Down) 것과, 네트워크 프로토콜의 취약점이나 가용성이 낮은 웹 서버나 DB 서버를 타깃으로 한 소량의 패킷 전송 형태로 DDoS 공격의 패턴을 숨기는 지능적 공격이 상시적으로 발생 하고 있습니다. 또한, 네트워크 환경과 다양한 장비의 통신기능 탑재등의 발전으로 수십만대의 좀비 PC나 좀비 장비가 증가하여 가용규모 이상의 패킷 전송의 공격이 더욱 증가하고 있습니다.



주요 DDoS 공격 방어 유형

TrusGuard DPX는 각 네트워크 환경에 따라 트래픽 유형별 정책을 세분화하여 자동 학습을 할 수 있습니다. 특히, 네트워크 환경 변화 및 기존의 보안 시스템을 우회하는 최신 DDoS 공격에 대해서도 지능적인 방어가 가능합니다.

- **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

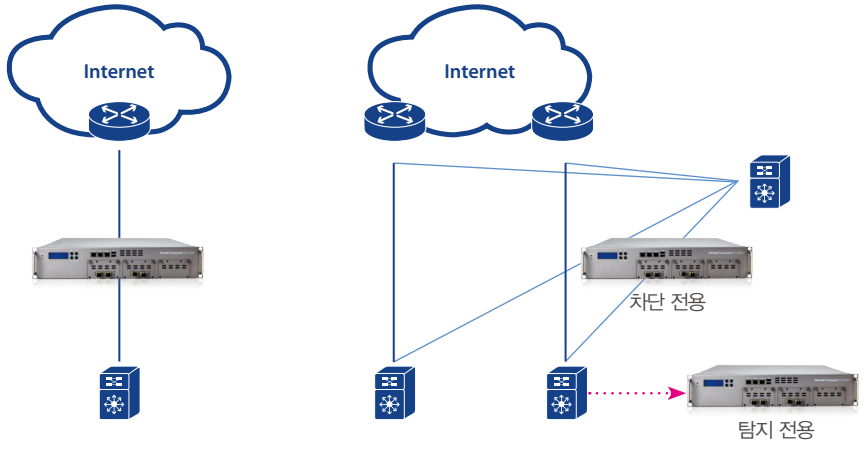
- **HTTP 기반 DDoS 공격 방어**
  - HTTP Get Flooding, HTTP Null Page Flooding, HTTP CC Attack, HTTP Redirect 우회 Flooding, SQL Query 기반 HTTP 공격 등

- **신종 DDoS 공격 방어**
  - RUDY, Slowloris, DNS Amplification, DNS Spoofing 공격 등

특장점

TrusGuard DPX는 고도의 공격에 대한 강력한 방어를 제공하는 DDoS 공격 방어 전용 장비로 다단계 필터 구조와 정밀한 자동 학습 정책을 이용하여 오탐을 최소화 하였습니다.

고도의 공격에 대한 강력한 방어	• 기존 솔루션에서 탐지하지 못하는 임계치 이하의 소규모 정밀 타격형 신종 HTTP 공격에 대해서도 강력한 방어 가능
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	• 최대 20Gbps와 30Mpps의 처리 성능
유연한 구성 방식	• 인라인(In-line) 구성 방식 및 아웃오브패스(Out-of-Path) 구성 방식을 제공해 다양한 네트워크 환경에 유연하게 적용 가능
혁신적인 분산 관리	• 한 대의 장비에서 최대 128개의 논리적인 네트워크에 대한 분산 관리 • 최대 128개의 존(Zone) 설정 : 존 별로 각각의 DDoS 공격 대응 정책 및 예외처리 설정 가능
안랩의 기술과 노하우 (인증 및 특허)	• CC 인증 : EAL 4 획득 • '분산서비스거부 공격 차단 장치 및 방법' 국제 특허 획득 • 자체 DDoS 방어 엔진 국제 특허 출원 중

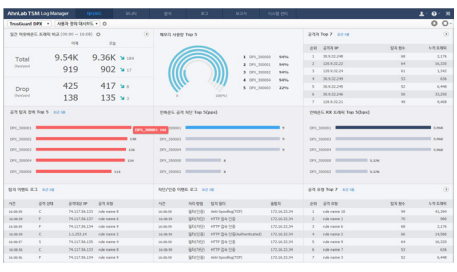


[인라인 방식] [아웃오브패스 방식]

[TrusGuard DPX 인라인과 아웃오브패스 구성 방식 동시 지원]

주요 UI

▲ 필터 현황 모니터



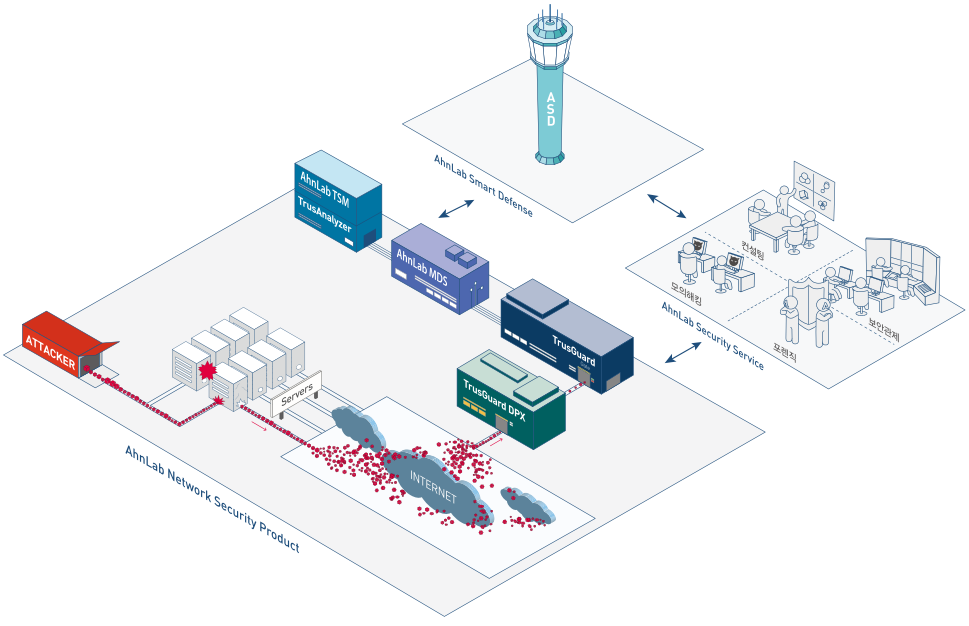
▲ 공격탐지현황 대시 보드

제품 사양

		TrusGuard DPX 2000A	TrusGuard DPX 6000	TrusGuard DPX 10000	TrusGuard DPX 10000A
기본 제공 성능 (bps)		1Gbps	3Gbps	10Gbps (+10Gbps)	10Gbps (+10Gbps)
CPU		멀티 코어	멀티 코어	매니 코어	매니 코어
Memory		8GB, DDR3	8GB, DDR3	16GB, DDR3	32GB, DDR4
Flash Disk		4GB	2GB	2GB	8GB
OS		AhnLab 자체 OS			
콘솔		1 (RJ-45)			
Inter-face	10/100/1000 Base-T (Copper) Port (Bypass)	4	옵션	-	-
	1G Base-X (Fiber - SFP) Port (Bypass)	4	4	-	옵션
	10G Base-X Port (Bypass)	-	옵션	4	4
옵션모듈		-	(Default +) 2 Port * 1GF Bypass Or (Default +) 4 Port * Copper Bypass Or (Default –) 2 Port * 10GF Bypass Or (Default –) 4 Port * 10GF Bypass	(Default +) 4 Port * 10GF Bypass	(Default +) 4 Port * 1GF Bypass Or (Default +) 4 Port * 10GF Bypass
전원		Redundant, 300W	Redundant, 500W	Redundant, 500W	Redundant, 550W
CC 인증		EAL4			

TrusGuard DPX만의 경쟁력

안랩은 글로벌 통합 보안 기업으로서 다양한 네트워크 보안 제품의 라인업을 구축하고 있습니다. DDoS 방어 장비인 TrusGuard DPX와 더불어 고성능 방화벽인 TrusGuard, APT 대응 솔루션인 AhnLab MDS로 청정 네트워크를 구현합니다. 또한 TrusGuard DPX는 DDoS에 특화된 사전 컨설팅, DDoS 공격 모의 대응 훈련, 보안 관제 등 다양한 서비스와 결합한 차별화된 프로세스를 제공합니다.



AhnLab
경기도 성남시 분당구 판교역로 220 (우)463-400
홈페이지: http://www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901