AhnLab TrusGuard IPX

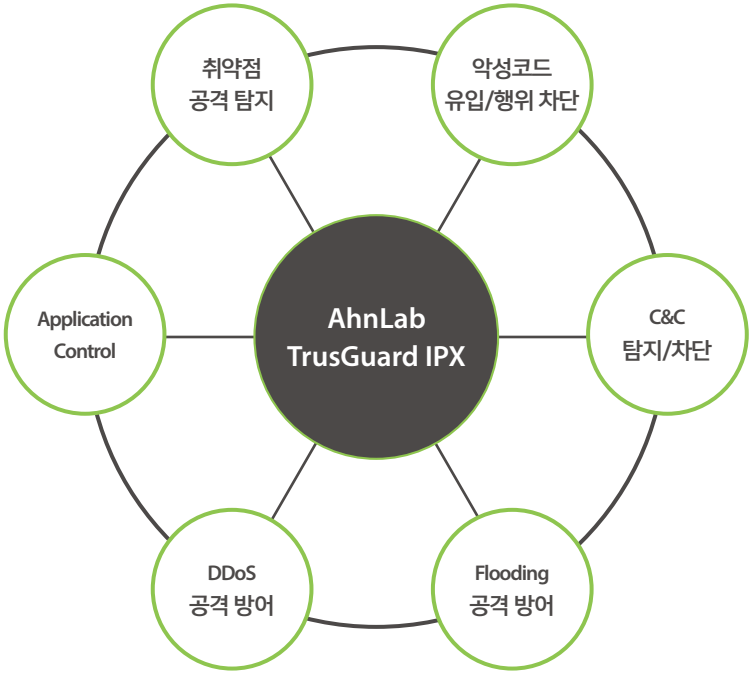
차세대 IPS의 새로운 이름, TrusGuard IPX

TrusGuard IPX는 안랩의 강력한 보안 위협 대응 기술력과 광범위한 인프라가 응집된 강력한 차세대 네트워크 침입방지 솔루션(IPS)입니다.

탐지 대응 모니터링 성능

제품 개요

TrusGuard IPX(Intrusion Prevention eXpress)는 최근 주요 공격의 경로로 이용되고 있는 네트워크 취약점은 물론 애플리케이션/웹 취약점, 그 외 다양한 유형의 네트워크 기반 공격 및 악성코드 공격을 차단해 기업의 비즈니스 환경을 안전하게 보호합니다.



차세대 위협 대응

TrusGuard IPX는 안랩의 분석 기술과 자체 제작한 룰을 기반으로 다양한 유형의 최신 네트워크 기반 공격 및 악성코드 침입을 차단합니다.

- VRS 취약성 분석
- BotNet 관리 시스템
- WebMon 시스템
- DDoS 모니터링 시스템
- 침해로그 분석 시스템

- 네트워크 취약점 공격 방어
- 웹/애플리케이션 취약점 공격 방어
- OS/시스템 취약점 공격 방어
- 악성코드 공격 및 유포지 차단

특장점

국내외 네트워크 침입방지 솔루션(Intrusion Prevention System, IPS) 장비 중 최대 수준인 6,000여 개의 최신성과 정확성을 겸비한 네트워크 공격 대응 시그니처를 보유하고 있는 TrusGuard IPX는 최신 보안 위협 환경에 최적화된 네트워크 탐지 범위를 제공합니다.

다양한 공격 탐지 기법 적용

- 시그니처 기반 공격 탐지
- 행위(Behavior) 기반 공격 탐지
- 존(Zone)별 상이한 룰(rule) 적용

최대 규모의 정확한 최신 시그니처

- 일일(daily) 정기 업데이트
- 6,000여 개의 시그니처 기본 제공

각종 취약점 공격 방어

- 웹 취약점 공격(OWASP) 방어
- 네트워크 취약점 공격 방어
- OS/애플리케이션 취약점 공격 방어

악성코드 공격 방어

- C&C 탐지/차단
- Bot/ BotNet
- 웜, 트로이목마
- 다운로더/ 스파이웨어 등

제로데이 공격 방어

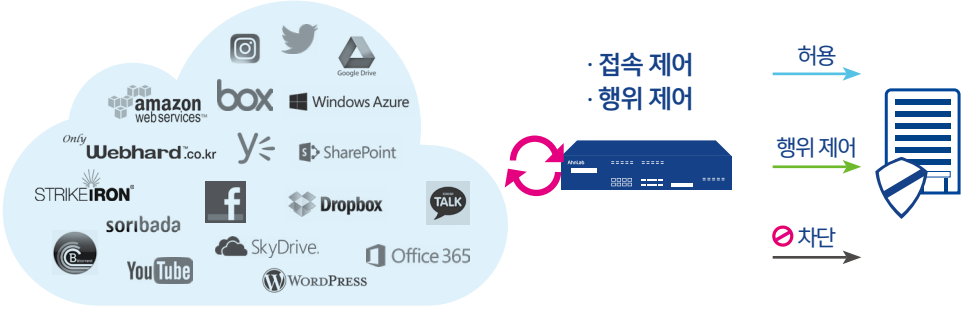
- 독자적인 보안 체계 ACCESS 기반 대응
- 공격 명령 악성코드 다운로드 차단
- Microsoft MAPP 파트너십

Application Control

- 글로벌한 애플리케이션 제어
- 세부 행위에 대한 선별 차단(로그인 등)
- 명확한 애플리케이션 카테고리 제공
- 애플리케이션별 도움말 제공

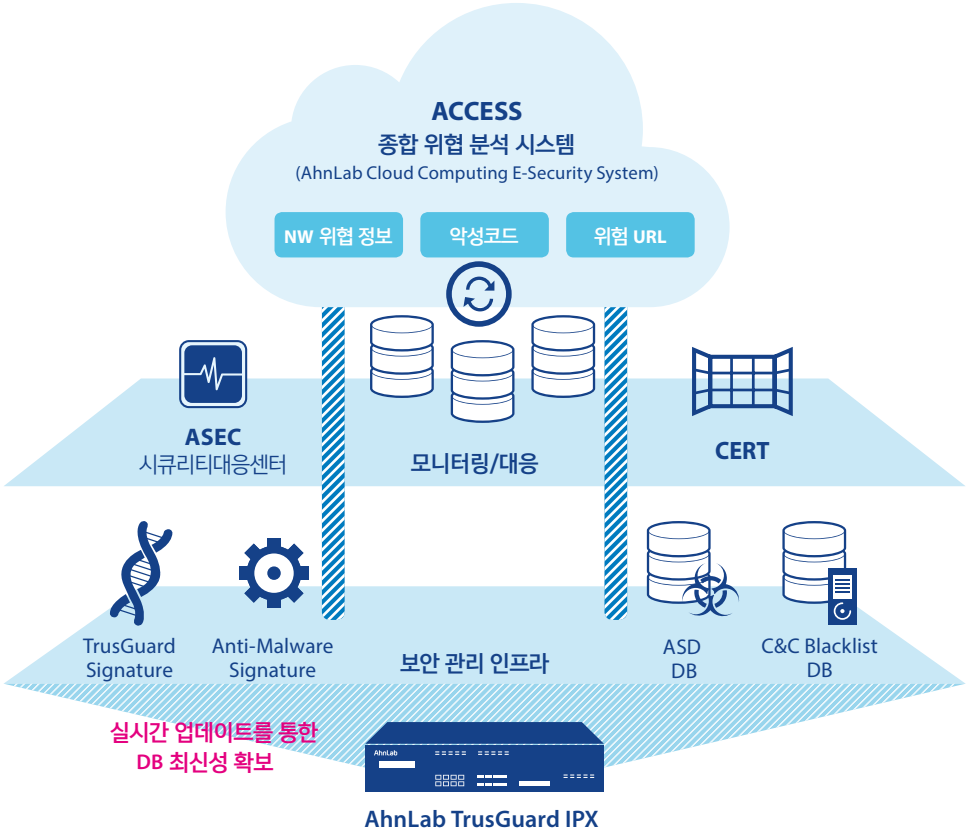
애플리케이션 컨트롤

TrusGuard IPX는 차세대 보안 기술인 애플리케이션 컨트롤(Application Control) 기능을 탑재해 P2P / 웹하드 / 메신저(Instant Messenger) / SNS 등 수 천 개의 글로벌 / 국내 애플리케이션에 대해 실시간 분석 및 차단·허용·행위 제어가 가능합니다. 특히 국내 환경에 특화된 주요 애플리케이션에 대한 독보적인 대응 능력을 제공합니다.



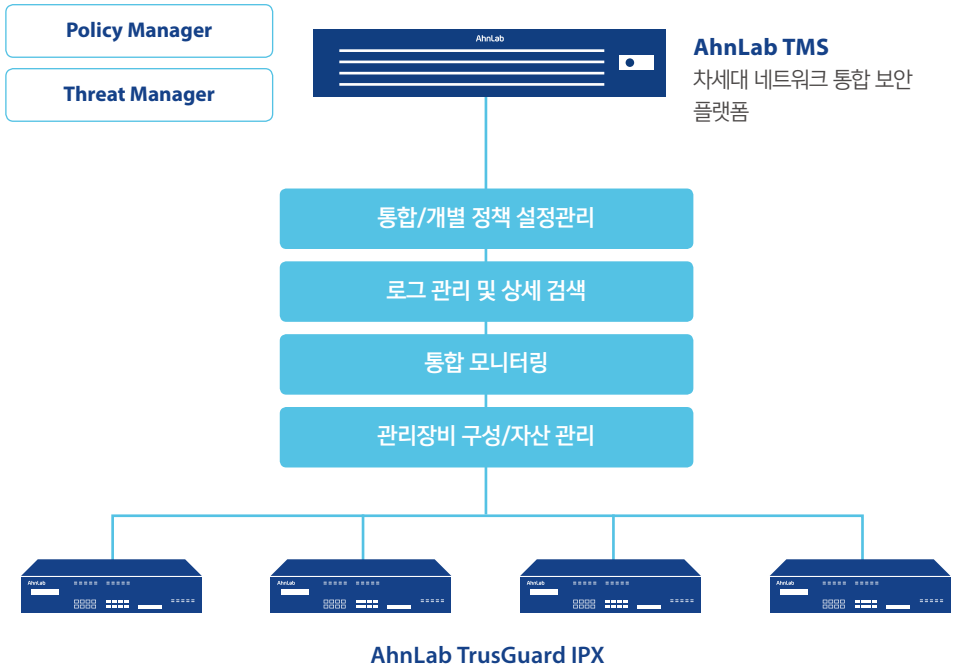
독보적인 위협 대응 체계

아시아 최고, 최대 규모의 보안 위협 대응 조직 및 인프라를 보유한 안랩은 클라우드 기반의 종합 위협 분석 시스템을 통해 급변하는 보안 위협에 대한 **실시간 모니터링 및 대응**을 제공합니다. 특히 국내 유일의 **자체 C&C 서버 블랙리스트 DB를 탑재**한 TrusGuard IPX는 고도의 네트워크 위협 차단을 요구하는 기업에 최적화된 네트워크 침입방지 솔루션입니다.



더 강력한 통합 관리

다수의 보안 장비에 대한 간편한 정책 설정 및 통합 모니터링 환경을 제공하는 **차세대 네트워크 통합 보안 플랫폼인 AhnLab TMS**와의 연동을 통해 **효율적이고 직관적인 모니터링 및 극대화된 관리 편의성**을 경험하실 수 있습니다.



주요 기능

Network
VLAN 인터페이스 지원
Port aggregation 지원
Multi-Line 지원
Static 라우팅
Dynamic 라우팅(RIP/ OSPF/ BGP)
IPv6 지원
Firewall
Stateful Inspection
정책 유효성 검증
블랙리스트(Blacklist) 기반 필터링
정책적용 예외
정책별 세션 제한
QoS(최대 제한/ 최소 보장)
카테고리 기반 URL 필터
IPS
Pre-defined Signature(6,000여 개)
User-defined Signature
네트워크 존(Zone) 별 상이한 IPS 정책 적용
다양한 대응 행동 지원
시그니처 일일(daily) 정기 업데이트
Infrastructure
클라우드 기반 보안 위협 수집/ 분석 시스템
MAPP Partnership
CDN 기반 안정적인 시그니처 업데이트
검증된 비상 대응체제/ 조직 보유
Application Control
글로벌 / 국내 애플리케이션 탐지 및 차단
애플리케이션별 세부 행위 제어
애플리케이션 도움말 제공

취약점 공격 차단
SQL Injection/ PHP Injection/ XSS 공격
IIS/ CGI 관련 취약점 공격
OS/ IE 취약점 공격
Shellcode/ Script 공격
네트워크 기반 공격 차단
각종 스캐닝(scanning) 공격
NetBios 공격
RPC 공격
DoS 공격
SSL Inspection
암호화된 트래픽 검사
악성코드 행위 제어
Worm/ Trojan/ Spyware
Downloader
Dropper
Mass mailer
악성코드 유포지/경유지 차단
Trojan 유포지/ 경유지
Spyware 유포지/ 경유지
Bot 유포지/ 경유지
C&C 탐지 / 차단
클라우드 기반 C&C(Command & Control) 서버 접속 탐지 및 차단
DDoS 공격 차단
TCP Flooding
UDP Flooding
ICMP Flooding
HTTP 취약점 공격
CC attack

제품 사양 (Specification)

구분		AhnLab TrusGuard IPX 2000A	AhnLab TrusGuard IPX 4000A	AhnLab TrusGuard IPX 10000A
최대성능		6G	10G	40G
CPU		6 Core	20 Core	20 Core
Memory		16GB	16GB	32GB
CF Memory		8GB	8GB	8GB
HDD		2TB	2TB	2TB
NIC	1GC	10 (최대 34)	10 (최대 50)	10 (최대 50)
	1GF	2 (최대 32)	4 (최대 48)	8 (최대 48)
	10GF	-	0 (최대 24)	4 (최대 24)
Power		550W Redundant	550W Redundant	550W Redundant

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