AhnLab CLOUD PLUS

AhnLab XTG VM

강력한 보안, 유연한 확장! 클라우드에 최적화된 차세대 방화벽

AhnLab XTG VM은 클라우드 환경에서
비즈니스 자산을 안전하게 보호하는 클라우드 차세대 방화벽입니다.

제품 개요

클라우드로의 전환이 빠르게 이뤄진 가운데, 클라우드를 향한 위협도 날로 증가하고 있습니다. 클라우드 상에서 조직의 비즈니스 자산을 안전하게 보호하고 보안 위협을 최소화 하기 위해서는 네트워크 일선에서 위협을 탐지해 차단하는 클라우드 최적화 차세대 방화벽이 필요합니다.

AhnLab XTG VM은 탁월한 성능과 안정성을 인정받은 차세대 방화벽 AhnLab XTG의 모든 기능을 계승한 동시에 클라우드 환경에 최적화된 유연성과 확장성을 갖춘 클라우드 차세대 방화벽입니다.

클라우드 환경에 최적화된 **차세대 방화벽**	최신 위협을 효과적으로 방어하는 **고도화된 보안 기능**
고객의 요구사항에 부합하는 **CSP 별 환경 최적화**	오랜 노하우가 축적된 **편리한 사용자 인터페이스**

도입 효과

클라우드 환경에서는 견고한 보안 뿐만 아니라 유연성과 관리 편의성 역시 필수 요소입니다. AhnLab XTG VM 사용자들은 ▲강력한 보안 ▲쉽고 안정적인 배포 ▲편리한 운영까지 클라우드 방화벽에 요구되는 핵심 역량들을 바탕으로 안전한 클라우드 환경을 조성할 수 있습니다.

강력한 보안

- 방화벽, ZTNA, 디도스 방어, 안티 멀웨어, VPN을 통합한 보안 역량 확보
- VPN 서비스로 외부에서 인증 기반 안전하고 편리한 접속 관리
- AhnLab XTG와 동일한 수준의 차세대 방화벽 기능 활용

쉽고 안정적인 배포

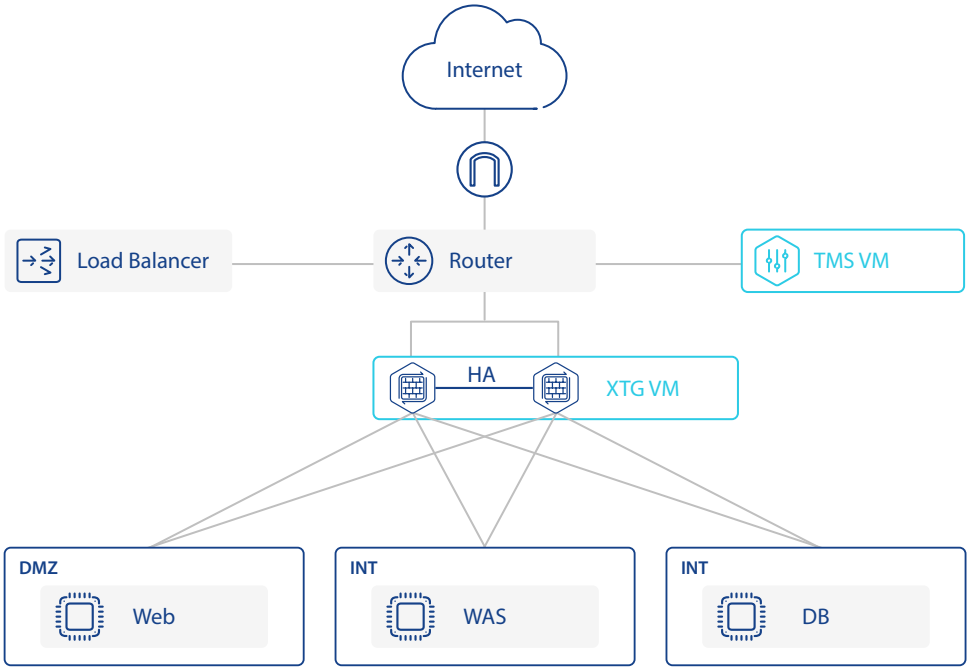
- CSP 마켓플레이스에서 서비스 신청 시 간단한 절차로 이용 가능
- 이중화 구성을 지원하여 장애로부터 네트워크 안정성 확보
- 외부-내부 혹은 내부 간 통신에 대해 디테일한 보안 구성

편리한 운영

- VPC 내 Router와 Load Balancer를 통한 이중화 구성
- 다양한 인스턴스와 스토리지 사용 가능
- Rest API와 Syslog를 지원해 관리 툴과의 연동 운영

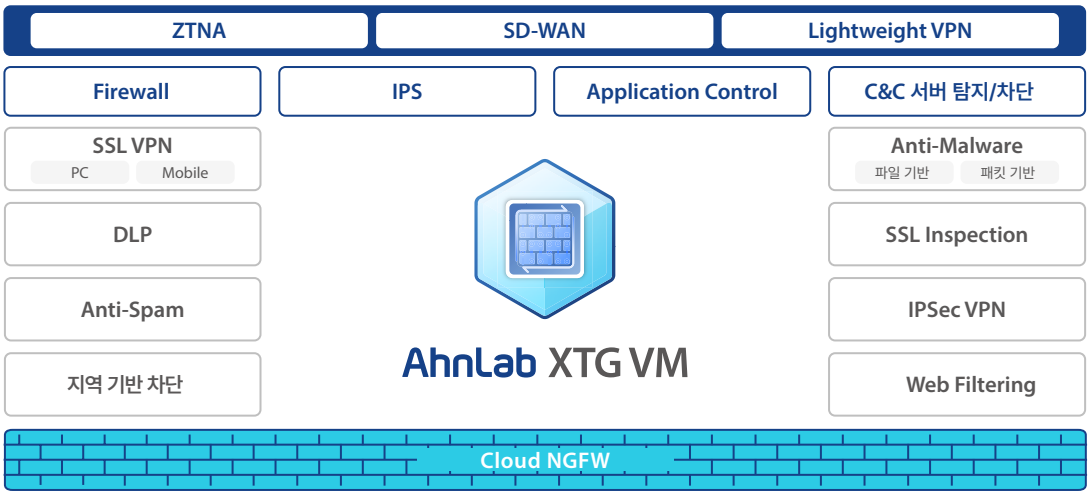
제품 구성도

AhnLab XTG VM은 분리된 대역을 보안 정책에 따라 영역 별로 관리하고, 외부와 내부 및 영역 간 접근 제어를 지원합니다. AhnLab XTG VM 이미지를 통한 인스턴스 생성 및 단일 구성과 Router/Load Balancer를 통한 이중화 구성을 함께 제공합니다. 또한, 장애 복구(failover)를 위해 세션 정책을 동기화하고, 단일 가상 어플라이언스에서 라이선스에 따라 방화벽, IPS, VPN을 통합 운영할 수 있습니다.



기능 소개

AhnLab XTG VM은 ▲방화벽 ▲ZTNA ▲IPS ▲VPN ▲콘텐츠 필터링 ▲웹 필터링 ▲애플리케이션 제어 ▲DLP ▲SSL Inspection 등 안랩의 차세대 방화벽 AhnLab XTG의 모든 기능을 클라우드 환경에 맞게 최적화했습니다.



차별화된 방화벽 기능

- 국내 및 글로벌 애플리케이션 심층 방어
- 다양한 VPN을 통한 안전한 네트워크 접속
- C&C 서버 접속 탐지 및 차단
- 암호화된 트래픽 탐지

독보적인 위협 탐지 · 차단 기술

- 보안 위협 탐지에 특화된 다계층 멀티 엔진
- 보안 인텔리전스 기반 차별화된 위협 탐지
- 최신 위협 대응 위한 실시간 위협 정보 반영
- 제로데이 및 알려지지 않은 위협 대응

클라우드 환경 최적화

- VPC 내 Router / LB를 통한 이중화 구성
- 다양한 인스턴스와 스토리지 사용

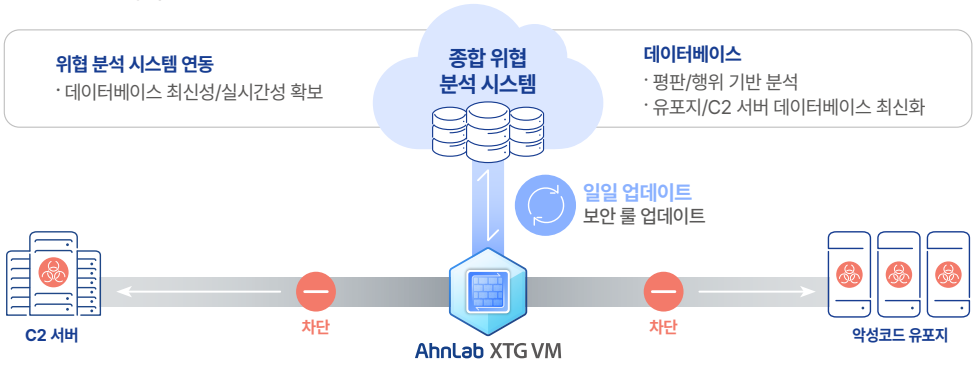
오랜 노하우가 축적된 사용자 인터페이스

- 위젯 방식의 대시보드로 유연한 패널 구성
- 연관 분석 기능을 활용한 통계 트래킹
- 한 곳에서 모든 트래픽 로그 정보 확인
- Custom 리포트로 맞춤형 보고서 생성

주요 기능

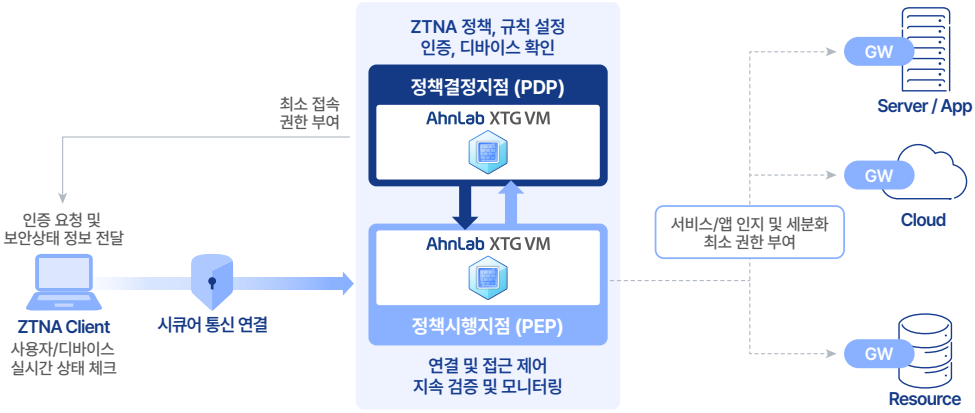
차세대 방화벽

인바운드 및 아웃바운드 트래픽을 사용자, 디바이스, IP, URL 등 다양한 속성에 따라 정교하게 허용 또는 차단합니다. 보안 관점에서 위험도가 높은 IP나 웹사이트를 실시간으로 차단하고, 외부에서 내부 중요 자산으로의 IP, 포트(Port) 접근을 제어해 랜섬웨어 등 악성코드 감염을 예방합니다. 자체 보유한 위협 분석 시스템과 C2 블랙리스트 데이터베이스를 기반으로 C2 서버 접속을 탐지 및 차단해 사이버 위협으로부터 비즈니스 환경을 보호합니다.



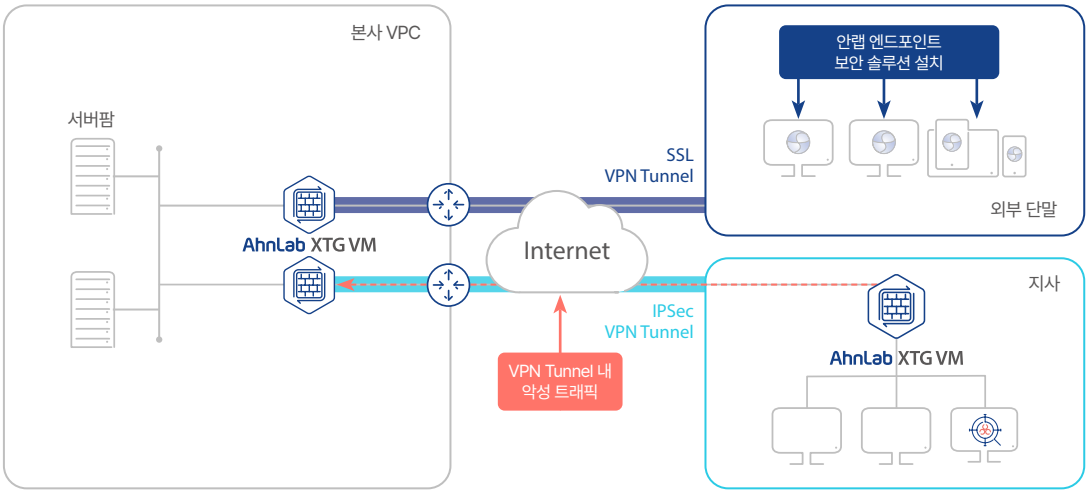
ZTNA 접근 제어

AhnLab XTG VM의 ZTNA는 네트워크 내부와 외부를 불문하고 모든 사용자와 디바이스의 신원을 철저히 검증하여 최소 권한 접근을 보장합니다.



VPN

AhnLab XTG VM은 IPSec, SSL, lightweight VPN 기능을 동시에 지원해 언제, 어디서나 안전한 네트워크 접 속을 구현합니다. 또한 IPS 및 애플리케이션 제어를 기반으로 VPN 터널을 통한 악성코드 확산을 강력하게 통제합니다.



여러 VPN을 동시 지원하는 유연한 구조	VPN-IPS 연동으로 지사 감염과 악성코드 내부 확산 탐지 및 방어	지점/지사 VPC 보안 강화를 통한 강력한 통합 보안

안랩 보안 인프라

차세대 방화벽

안랩은 위협 분석과 침해 대응을 통해 30여 년간 축적한 방대한 보안 데이터를 기반으로 AI 보안 플랫폼 AhnLab AI PLUS를 운영하고 있습니다. 차별화된 보안 데이터를 학습한 안랩의 AI는 위협 탐지와 대응 역량을 고도화하고, 보안 운영의 생산성 혁신을 지원합니다.

라인업

제품 사양

구분	XTG VM04	XTG VM08	XTG VM16	XTG VM32
vCPU (Min/Recommend)	2 / 4	2 / 8	2 / 16	2 / 32
Memory (Min/Max/Recommend)	5 / 8 / 8GB	9 / 16 / 16GB	17 / 32 / 32GB	33 / 256 / 64GB
Fixed Storage	8GB			
Additional Storage (Min/Max)	16GB / 4TB			
FW Throughput (HTTP)	TBD	TBD	TBD	TBD
IPS Throughput (HTTP)	TBD	TBD	TBD	TBD
IPSec VPN Throughput (HTTP)	TBD	TBD	TBD	TBD
CC (Concurrent Session)	2,500,000	8,000,000	10,000,000	30,000,000
IPSec VPN Tunnel	2,500	40,000	40,000	50,000
SSL VPN Client	500	3,000	5,000	10,000
ZTNA Devices	50	1,000	2,500	5,000

※ 성능 수치는 세부 환경 및 시스템 구성에 따라 달라질 수 있습니다.
※ 사용 환경에 맞는 라인업 및 CSP별 인스턴스 사양 등은 별도의 기술 상담을 통해서 가이드 받으실 수 있습니다.

패키지(번들)

구분	기능
BASIC	Firewall, C2 detection & prevention, application control, NAC, SD-WAN, Lightweight VPN, SSL VPN (10 users)
VPN	Basic bundle, IPSec VPN, SSL VPN (인스턴스 별 Max)
ALL	VPN Bundle, IPS, anti-virus, threat detection filter, anti-spam, anti-malsite, URL category filter, virtual system, ZTNA, DLP, application firewall

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

AhnLab