

AhnLab XTG VM

Powerful and Scalable Cloud NGFW

AhnLab XTG VM is a cloud-native next-generation firewall designed to securely protect business assets in cloud environments.

Overview

As organizations rapidly accelerate their cloud migration, cyber threats targeting cloud environments continue to grow in scale and sophistication. To safeguard critical business assets and minimize security risks in the cloud, enterprises need a cloud-optimized next-generation firewall capable of detecting and blocking threats at the network perimeter in real time.

AhnLab XTG VM inherits the full capabilities of AhnLab XTG — a proven next-generation firewall recognized for its outstanding performance and reliability — while delivering the flexibility and scalability required for modern cloud environments.

Powerful and Scalable NGFW
Optimized for Cloud

Advanced Security Capabilities to
Defend Against Evolving Threats

Optimized for Various CSPs
Meeting Customer Requirements

Intuitive User Interface
Backed by Proven Expertise

Benefits

In cloud environments, strong security alone is not enough — flexibility and operational efficiency are equally critical. With AhnLab XTG VM, organizations can build a secure and resilient cloud infrastructure powered by the essential capabilities required for modern cloud firewalls: advanced features, simple and stable deployment, and streamlined operations.



Advanced Features

- Firewall, ZTNA, IPS, DDoS mitigation, anti-malware, VPN, etc.
- Secure remote access management with authentication-based VPN services
- Full functionality equivalent to our NGFW, AhnLab XTG



Simple and Stable Deployment

- Quick and easy deployment through CSP marketplaces
- High availability support for enhanced network resilience and business continuity
- Granular policy configurations for both north-south and east-west traffic

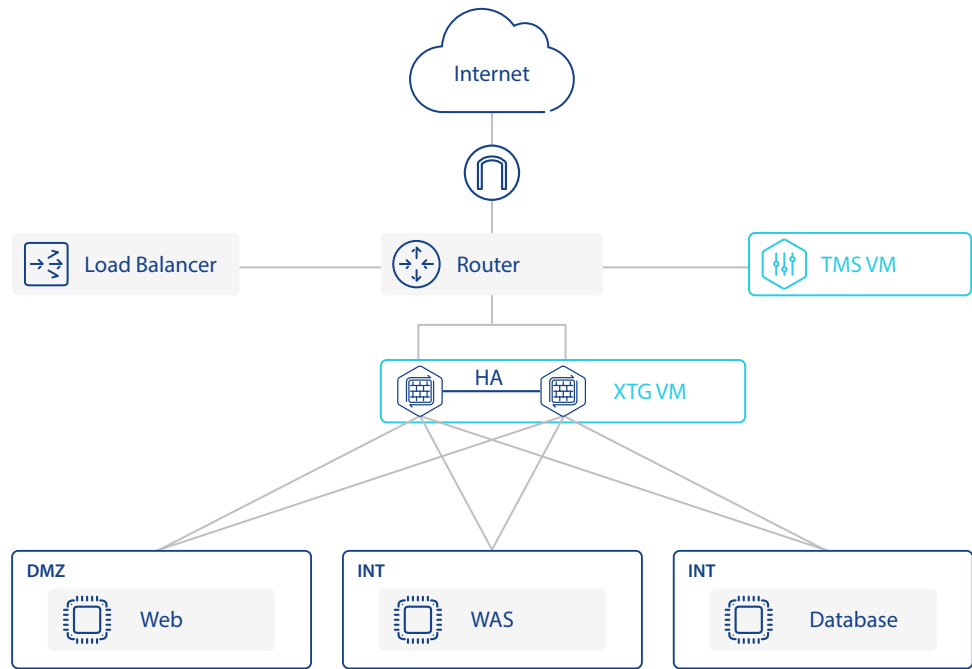


Streamlined Operations

- High availability architecture using routers and load balancers within VPCs
- Flexible support for various instance types and storage options
- Easy integration with management tools through REST API and Syslog

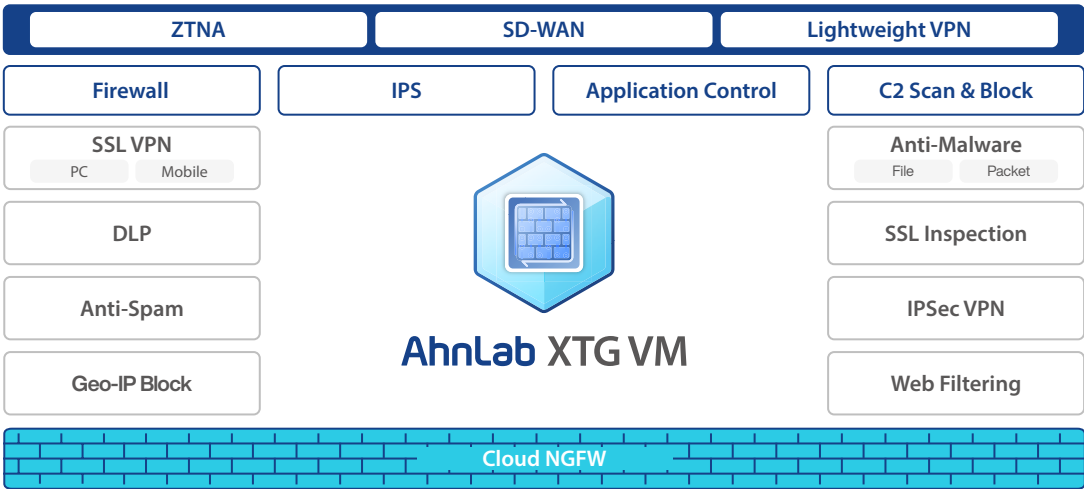
Architecture

AhnLab XTG VM enables customers to segment and manage network zones based on security policies while providing granular access control between external, internal, and inter-zone traffic. It supports both standalone deployment through AhnLab XTG VM instance creation and high-availability configurations using routers and load balancers. To ensure business continuity, AhnLab XTG VM synchronizes session policies for failover and allows integrated operation of firewall, IPS, and VPN within a single virtual appliance based on licensing options.



Feature Overview

AhnLab XTG VM brings the full power of our next-generation firewall capabilities to the cloud, optimized for modern cloud environments. Key features include: firewall, ZTNA, IPS, VPN, content and web filtering, application control, DLP, and SSL inspection.



Competitive NGFW Features

- Deep and granular application security
- Supporting various VPN for secure network access
- C2 detection and block
- Encrypted traffic detection

Next-Level Detection & Block

- Multi-layered engine for powerful detection
- Intel-driven threat detection
- Reflecting our real-time threat intelligence
- Addressing zero-day and unknown threats

Cloud-Optimized

- High-availability architecture with routers and load balancers within the VPC
- Flexible support for a wide range of instance types and storage options

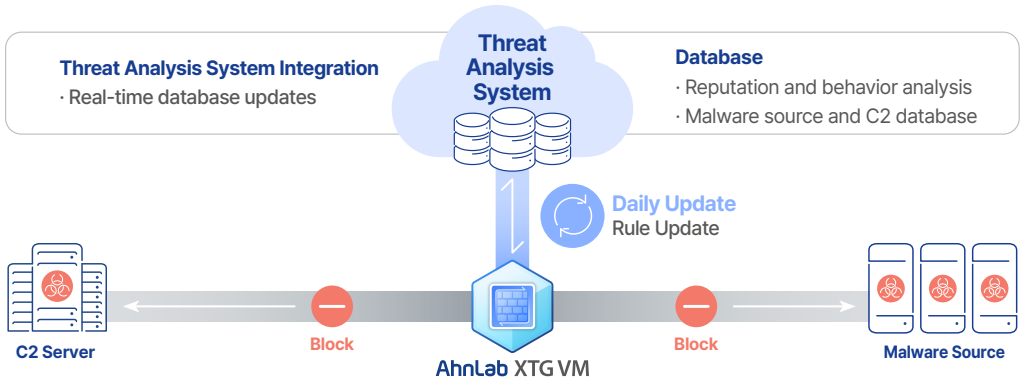
User-Friendly Interface

- Flexible widget-based dashboard
- Advanced analytics with correlation analysis
- Centralized visibility into all traffic logs
- Custom report generation

Key Features

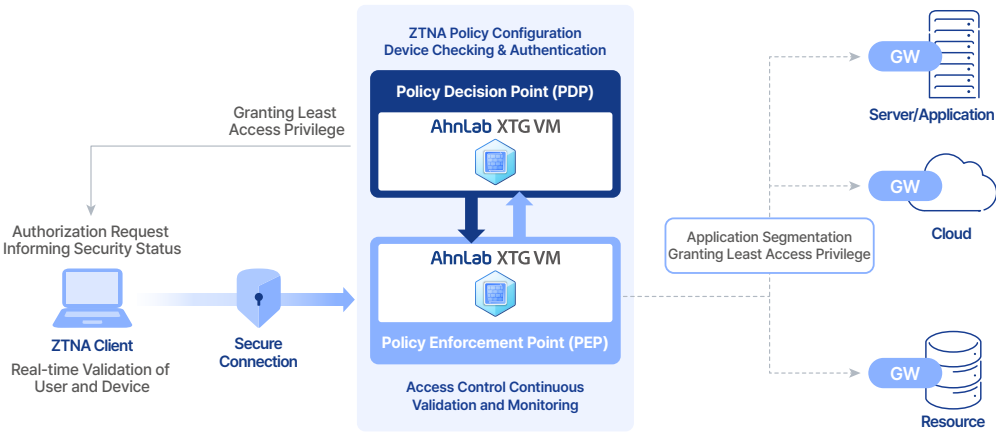
NGFW

AhnLab XTG VM delivers granular control over inbound and outbound traffic based on multiple attributes, including users, devices, IP addresses, and URLs. It also blocks high-risk IPs and malicious websites in real time while controlling IP and port access from external networks to critical internal assets to help prevent ransomware and other cyberattacks. Powered by our proprietary threat analysis system and C2 blacklist database, AhnLab XTG VM detects and blocks communications with C2 servers.



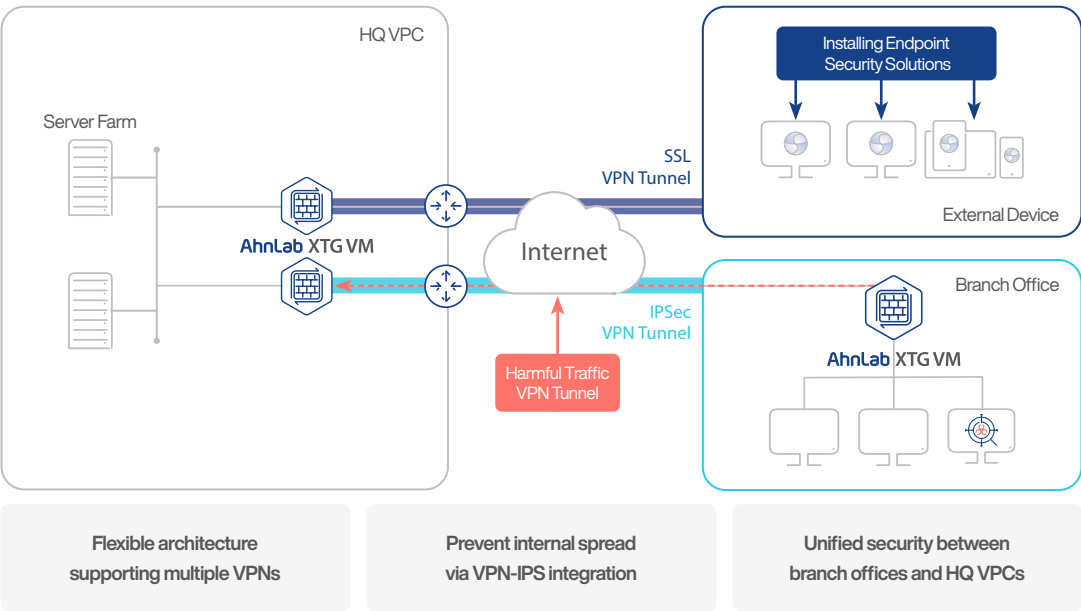
ZTNA

AhnLab XTG VM's ZTNA enforces strict identity verification for every user and device — both inside and outside the network — ensuring secure least-privilege access across the organization.



VPN

AhnLab XTG VM delivers IPSec, SSL, and lightweight VPNs to provide secure network access anytime, anywhere. In addition, IPS and application control features help prevent malware propagation through VPN tunnels, strengthening overall network security.



Our Infrastructure

Core Technology

Backed by over 30 years of cybersecurity expertise in threat analysis and incident response, we run the agentic AI security platform, AhnLab AI PLUS. Trained on our extensive and differentiated security data, the AI enhances threat detection and response capabilities while driving greater efficiency and productivity in security operations.



Line-up

Specifications

	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

* Performance may vary depending on the environment and system configuration.
* Guidance on lineups and CSP-specific instance specifications can be provided through technical consultation.

Package (Bundle)

	Features
BASIC	Firewall, C2 detection & prevention, application control, NAC, SD-WAN, Lightweight VPN, SSL VPN (10 users)
VPN	Basic bundle, IPSec VPN, SSL VPN (max capacity per instance)
ALL	VPN Bundle, IPS, anti-virus, threat detection filter, anti-spam, anti-malsite, URL category filter, virtual system, ZTNA, DLP, application firewall