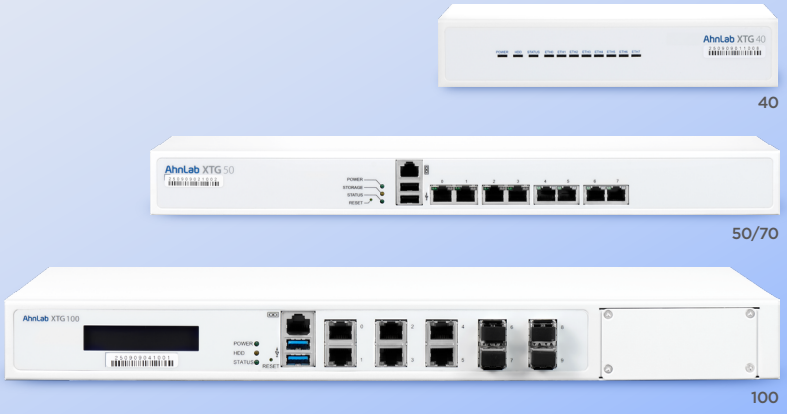
AhnLab

NGFW Lineup for Small Businesses

AhnLab XTG 40, 50, 70 and 100



Highlights

High-end NGFW delivering full-scale performance with mega-volume traffic processing for large enterprises and data centers

Creating a secure and flexible VPN network access environment for remote access through simultaneous support of IPSec VPN and SSL VPN

Providing a virtual system that achieves the benefit of configuring up to 10 appliances with a single machine

Implementing consolidated endpoint-network security through the integration with our native endpoint security solutions

Delivering ZTNA-based secure and powerful access control

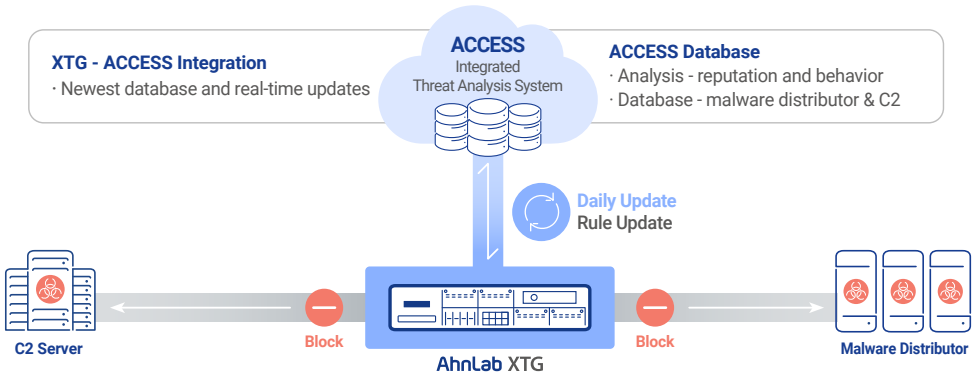
Simple and Efficient NGFW

We designed four models (40, 50, 70 and 100) of AhnLab XTG, the next-generation firewall (NGFW), to address the security requirements of small businesses. AhnLab XTG not only offers NGFW and VPN capabilities but also provides extended network security features such as ZTNA, SD-WAN, IPS, application control, URL filtering, C2 detection and prevention, anti-spam, DDoS mitigation, and DLP to protect customers' businesse

Use Case

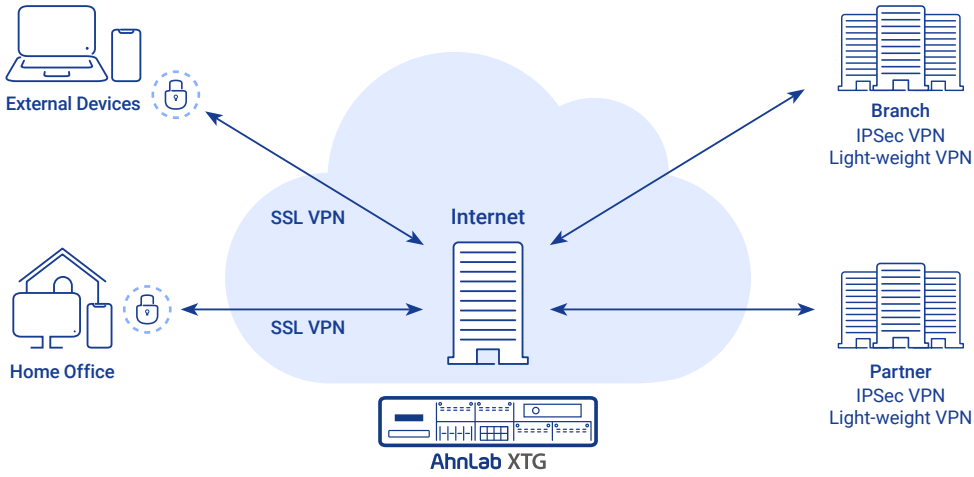
Next-generation Firewall

- AhnLab XTG precisely allows or prevents inbound and outbound traffic by assessing various attributes such as user, device, IP, and URL.
- It blocks high-risk IPs or websites in real-time and controls IP and port access to internal assets to prevent damage from cyber-attacks, including ransomware.
- It protects businesses from cyber threats by detecting and blocking connections to C2 servers by leveraging our C2 blacklist database and threat analysis system.



VPN – Remote Access

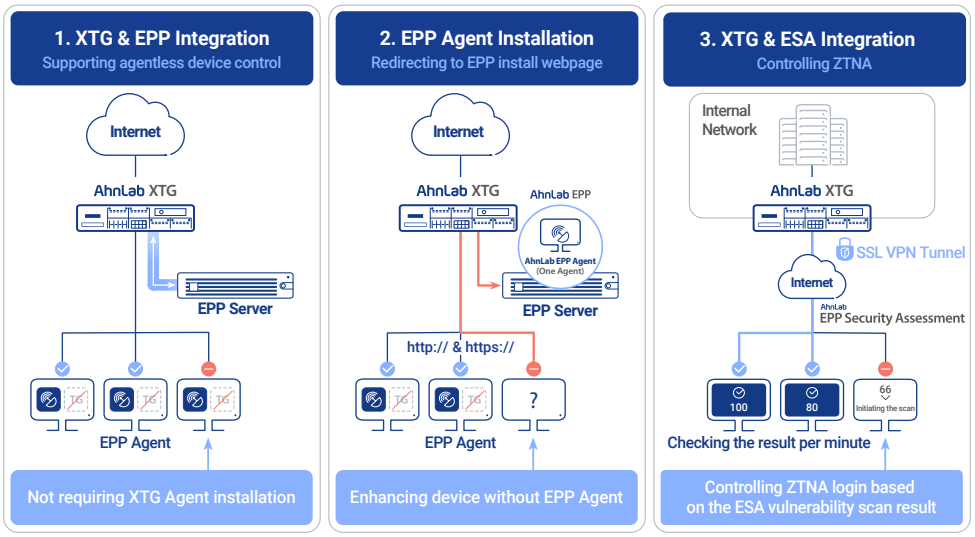
- AhnLab XTG delivers IPSec VPN, SSL VPN and light-weight VPN to enhance security for remote access and HQ-branch network connections.
- It supports various operating systems, including Windows, Mac, Linux, Android, and iOS.
- It also offers mobile-dedicated SSL VPN.
- The NGFW maximizes VPN stability and availability by leveraging cutting-edge technologies such as high availability (HA) configurations and multi-line load balancing.



EPP Integration

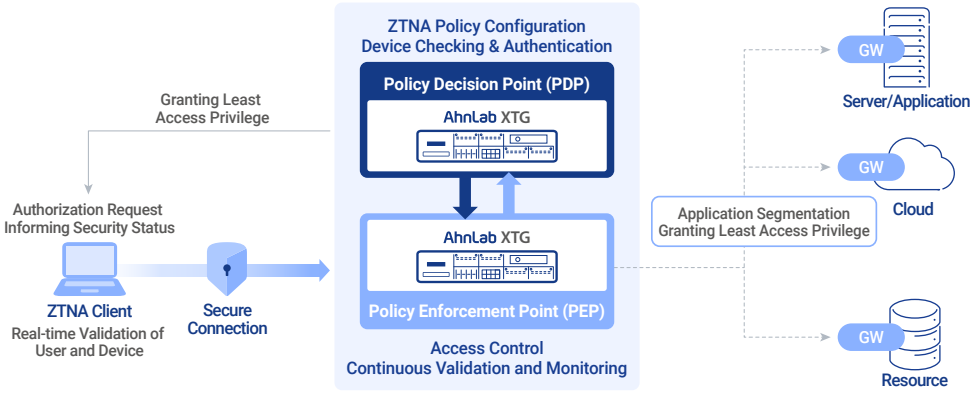
AhnLab XTG integrates with AhnLab EPP to allow network access only for secure devices.

- The EPP integration implements device control without installing the XTG agent.
- AhnLab XTG guides users to install the EPP agent (HTTP/HTTPS).
- ZTNA login is controlled based on the security assessment score of AhnLab ESA.



ZTNA

The ZTNA of AhnLab XTG thoroughly verifies the identity of all users and devices inside and outside the network to ensure minimum privilege access.

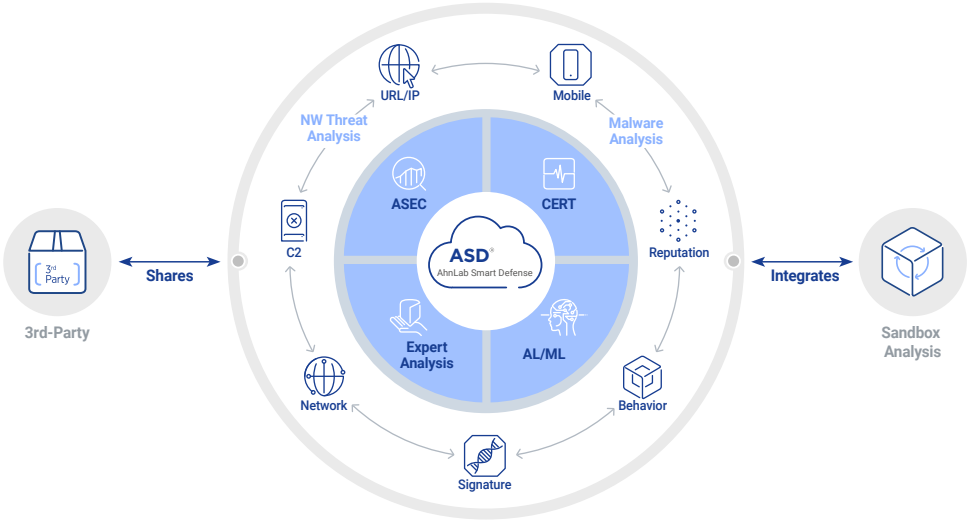


External User Access Control	Branch Office Access Control
Controlling access to internal resources of external devices by verifying user identity and device status (SSL VPN)	Performing access control by verifying the identity and device of branch office users connecting to the HQs via IPSec tunneling
Internal Network Access Control	**Web Access Control**
Controlling access from the internal network to corporate resources by verifying users and devices	Controlling web access by creating an encrypted channel based on HTTPS in an agentless environment

Backend Infrastructure

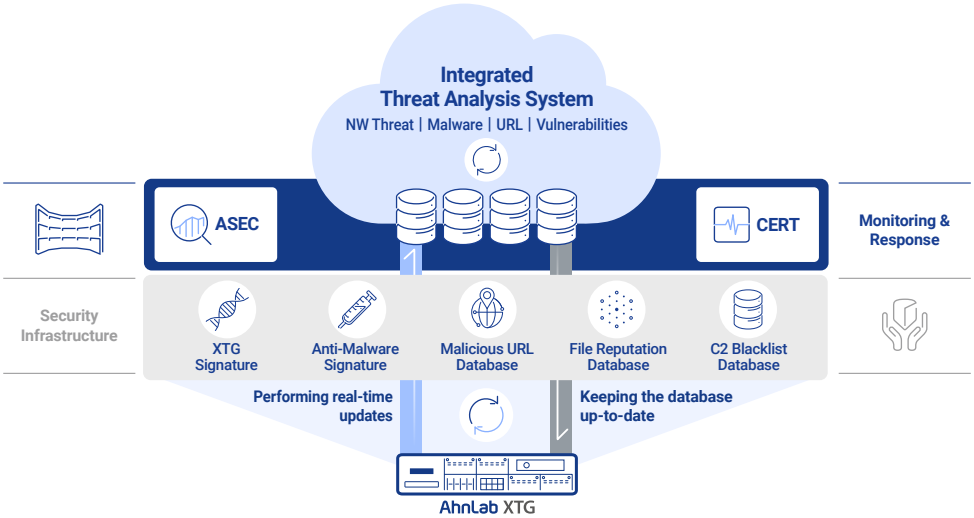
Technology

There is the cloud-based engine “AhnLab Smart Defense (ASD)” at the core of our products and services, which reflects our decades of accumulated technology and knowledge. The ASD engine implements multi-dimensional detection and response to novel cyber threats by performing the full-scale analysis into data across URL/IP, C2, mobile, network, behavior, signature, and reputation. Also, it incorporates AI and machine learning technologies, along with the expertise of threat analysis professionals, to fuel our products and services to enhance overall threat detection, analysis, and response capabilities.



How It Enhances AhnLab XTG

AhnLab XTG is also reinforced by the specialized technology and infrastructure regarding threat detection, analysis, and response. The NGFW leverages the infrastructure to apply the latest signatures, vulnerabilities, reputation, and C2 information, ensuring customers are protected from the latest network attacks.



Key Features

NGFW

AhnLab XTG delivers multiple features to keep up with the nature of a next-generation firewall, which protects internal networks from external cyber threats. In detail, customers can create user/device-based policies and choose whether to block, allow, or deny them. AhnLab XTG also provides cloud objects and country-based objects for explicit policy control and performs SSL VPN user access control using user objects. Customers can validate the created policies in various ways and filter duplicate objects or policies. In addition, HA configuration is available even without an L4 switch. Policy and session synchronization also ensure service continuity without interruption in case of appliance failure.

IPSec VPN

The IPSec VPN of AhnLab XTG supports the IPSec standard protocol and offers various encryption and hash algorithms. It provides a stable VPN powered by high-end HA technology and supports redundancy configurations for headquarters and branch offices. It also prevents the spread of malware through VPN tunnels by integrating with the IPS solution. Furthermore, it supports the multi-line load balancing for as many interfaces as available, efficiently distributing traffic and expanding bandwidth to maximize VPN availability. AhnLab XTG also provides a dynamic access feature, allowing the dynamic creation of IPSec VPN tunnels between hubs and spokes without changing hub settings. Then, it ensures management convenience by dynamically creating communication tunnels between spokes.

SSL VPN

The SSL VPN of AhnLab XTG, based on the SSL standard protocol, supports the gateway-to-client network connection in full tunnel mode. The NGFW integrates with standardized third-party authentication servers to enable various user verification methods across ID/PW, certificate-based two-factor authentication, and FIDO authentication. The SSL VPN supports various client OS across Windows, Mac, and Linux, and provides access control for SSL VPN users and decrypted SSL VPN traffic. Its active/active configuration ensures service continuity without VPN reconnection, even when the devices experience failure.

Light-weight VPN

AhnLab XTG's light-weight VPN, powered by the WireGuard protocol, supports gateway-to-gateway configuration and offers faster and more efficient connections compared to existing VPNs. It enhances security with the latest encryption algorithms while ensuring fast speeds and resource efficiency thanks to its lightweight protocol architecture. Its simple setup allows easy VPN deployment with just key pairs, and it quickly reconnects even when the network setting changes, ensuring stable access. The light-weight VPN operates smoothly in firewall and NAT environments using UDP-based transmission technologies. Enterprises can design efficient remote access environments by leveraging the high-performance VPN with simple configurations.

SD-WAN

AhnLab XTG provides SD-WAN (Software-Defined WAN) feature that optimizes the network by incorporating intelligent traffic control and security. The NGFW monitors network quality in real-time to automatically transmit packets over the highest quality lines and selects the optimal path for each application to maximize performance. It combines encrypted tunneling and firewall features to ensure robust security and stable data transmission. As SD-WAN supports both cloud and on-premises environments, enterprises can enjoy the benefit of flexible network configurations.

ZTNA

AhnLab XTG's ZTNA (Zero Trust Network Access) ensures secure network access based on the fundamental principles of zero trust: continuous validation and least access privilege. It continuously verifies the identity and security status of users and devices, allowing only authenticated users to access applications and network resources. Customers can apply granular security policies at the application level, enabling safer remote access. Its ZTNA SWG allows remote access configurations via web browsers when it is challenging to set up the tunnel. Ultimately, the ZTNA provides robust and flexible access control, raising the overall security level of enterprises.

IPS

AhnLab XTG delivers IPS features that detect and block malicious traffic based on signatures and behavior rules. It offers over 10,000 signatures for vulnerability exploitation to counter cyber-attacks, weaponizing vulnerabilities in networks, operating systems, and applications. Also, it supports automated daily updates of signature patterns to promptly respond to the latest and zero-day attacks. This enables customers to effectively detect and block network intrusions that exploit protocol and application vulnerabilities.

Application Control

AhnLab XTG provides an application control feature that analyzes and controls various application traffic within the network. This allows real-time analysis, blocking, allowing, and detailed behavior control for thousands of known and unknown applications. Customers can create and manage custom rules to suit their network environments. Its application mapping feature can be used to more easily control specific traffic and enhance organizational cybersecurity posture.

DLP

AhnLab XTG leverages the DLP engine to prevent the leakage of critical information, such as personal data and internal documents, by performing attachment classification and dynamic content analysis; this protects customers from internal asset leakage and ensures company-wide content visibility.

DDoS Mitigation

AhnLab XTG, powered by our native engine, safeguards customers from DoS and DDoS attacks with abnormal traffic or excessive service requests. It leverages TCP and HTTP authentications to identify DDoS traffic and effectively blocks abnormal traffic of DDoS attacks using the IP spoofing technique.

Virtual System

The virtual system enables customers to create independent virtual instances that can be managed separately within the physical appliance. Customers can manage each virtual system's policies and objects and harness all AhnLab XTG's features in a maximum of ten virtual instances.

Anti-Malware

AhnLab XTG is empowered with an outstanding malware filtering feature backed by a globally proven anti-malware engine. Leveraging our native stream-based anti-malware engine, customers can promptly check for malware in emails, websites, and FTP-transferred files.

Anti-Spam

Powered by a globally certified anti-spam engine, AhnLab XTG prevents unknown malware transmitted via email (SMTP/POP3). Customers can set conditions and methods for detecting spam emails in SMTP/POP3 traffic and manage sender IPs and email addresses leveraging the anti-spam feature. It also delivers keyword filtering to detect whether specific keywords are included in the email subject or body.

Device Control

The integration with AhnLab EPP allows AhnLab XTG to communicate with the EPP server and check the security status of multiple endpoint devices in real-time. The aggregated data helps AhnLab XTG gain more granular control over devices when integrated with the AhnLab EPP Security Assessment (ESA) agent. Ultimately, the NGFW can dictate the network connection of endpoint devices by assessing multiple factors, including their OS versions, security patch status, and vulnerability inspection results.

Feature Snapshot

Category	Subcategory	Description
Network	Interface	· Bridge, aggregation, VLAN, VXLAN and VRF
	Operation Mode	· Router and bridge mode
	Routing Protocol	· Static, dynamic and multicast protocols · Routing simulator
	DHCP	· Client, server and relay
	SD-WAN	· Application and service path optimization · Network quality monitoring, load balancing, etc.
NGFW	High Availability (HA)	· Active/standby and active/active
	Synchronization	· Admin settings, log settings and policies · Synchronizing user and FQDN IP information with other XTG appliances
	Object	· Cloud synchronization · Providing country-based objects for firewall policy configurations
	QoS	· Guaranteeing minimum and limiting maximum bandwidth per policy
	Blacklist	· Managing IPv4/IPv6 prevention · Inspecting protocols of L3, L4 and above · Supporting tools to check for duplicate IPs within access prevented files
	Whitelist	· Supporting policy exception for IPv4/IPv6
	Duplicate Object Inspection	· Inspecting and duplicate and referred policies · Checking duplicates of selected policies
	Policy Inspection	· Filtering duplicate policies · Inspecting validity of virtual packet policies
	NAT	· Static, dynamic and policy-based NAT
	User Authentication	· Integrating with standardized third-party authentication servers(RADIUS, LDAP, AD, TACACS+, MS-SQL, etc.)
	Policy Setting	· IP/MAC, user and device setting & control
	ZTNA	· Access control for applications and resources based on users and devices · Supporting agent and agentless ZTNA
	Virtual Packet Search	· Supporting virtual packet simulator for NGFW policies
IPSec VPN	Configuration	· Hub, spoke and mesh
	Dynamic Access (DA)	· Dynamic creation of IPSec VPN tunnels between hubs and spokes without changing hub settings · Dynamic tunnel creation for communication between spokes
	Algorithm	· Supporting various encryption and hash algorithms
	HA	· Redundant VPN configuration for HQ (active/standby, active/active)
	Load Balancing	· Multi-line load balancing for various internet connection types
	Failover	· DPD testing and DR center connection
SSL VPN	OS	· Windows, Mac, Linux, Android, iOS, etc.
	User Authentication	· Integrating with standardized third-party authentication servers (RADIUS, LDAP, AD, DBMS, OTP, Oracle, FIDO, SMS, etc.)
	Algorithm	· Supporting various encryption algorithms (AES, SEED, ARIA, LEA, HIGHT, etc.)
	EPP Integration	· Ensuring endpoint device security before and after making VPN connection
	HA	· Active/standby and active/active
	Supporting Devices	· Endpoint devices including mobile (cell phone/tablet) and embedded devices (router)

Category	Subcategory	Description
Light-weight VPN	HA	· Redundant VPN configuration for HQ (active/standby, active/active)
	Configuration	· Gateway-to-Gateway
	Prevention List	· The central appliance has the prevention list of branch office appliances
Virtual System	Virtualization	· Logical virtualization of appliance via MAC VLAN configuration
	HA	· Supporting high availability configurations for virtual systems
	Communication	· Supporting communication between virtual systems via the Veth interface
	Management	· Managing private cloud, SDN and NFV via virtual systems
IPS	Signature	· Supporting over 10,000 signatures with regular update to patterns
	Detection & Prevention	· Anomaly, vulnerability and malware detection & prevention
	Signature Management	· Managing user-defined and PCRE (snort rule) patterns
DDoS Mitigation	Prevention	· Preventing various DDoS attacks – UDP, ICMP and TCP flooding & TCP Spoofing & HTTP vulnerability exploitation
Application Control	Support Range	· Threat detection and prevention for over 3,000 known and unknown applications
	Control	· Controlling user access/login, detailed functions and unknown applications
C2 Detection/Prevention	Detection	· Cloud-based C2 connection · Inflow of unknown/suspicious files and potentially unwanted programs (PUPs)
	Prevention	· Blocking C2 connection based on the blacklist database
Anti-Malware	Engine	· Supporting the native engine
	Detection/Prevention	· High-speed malware detection and prevention powered by stream-based AV engine
	Signature Updates	· Updating signatures at least twice a day
	Malware Scan	· Thorough malware scan for various protocols (HTTP/SMTP/POP3/FTP, etc.) and files
Anti-Spam	Engine	· Powered by globally-certified anti-spam engine
	Filter	· Filtering based on real-time blacklist (RBL) and user-defined keyword
	Prevention	· When receiving more than a certain amount of emails during a specific period or receiving email from a particular sender
DLP	Control	· Controlling file/content per type and transmission of internal asset
	Detection/Prevention	· Personal information and keywords (pattern-based)
Threat Detection Filter	Database	· Native malware distribution source database and global URL categorization database
Product Integration	Native Integration	· V3, EPP, MDS, AIPS, DPX, ASTx, ESA, TMS, AIPS, etc.
Others	SSL Inspection	· Inspecting encrypted traffic
	Monitoring/Log	· Log storage: HDD
		· Dashboard: Widgets and correlation analysis
		· Content: Centrally displaying traffic logs and delivering custom reports
	Prevention	· GeoIP: Geolocation-based prevention (country or continent)
	Management	· Privilege: Multi-layered admin privileges
		· Access: Web (HTTPS)
		· Integration: Open API

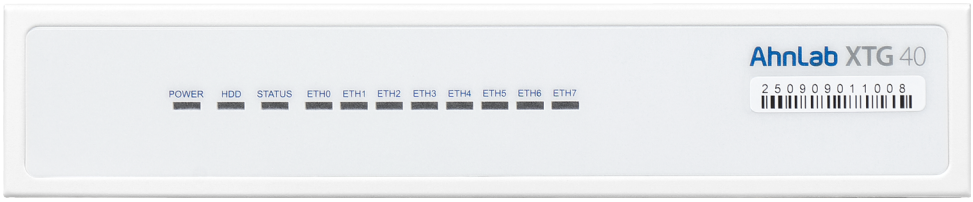
System Performance & Hardware Specification

Category	40	50	70	100
Certification				
IPv6 Certificate	IPv6 Ready Logo Phase-2 (Router)			
Electromagnetic Wave Certificate	KC			
Physical				
Processor	2 Core/1.8Ghz	4 Core/1.3Ghz	4 Core/2.4Ghz	8 Core/2.4Ghz
Memory	32GB	64GB	64GB	256GB
System Storage	eMMC 9.6GB	eMMC 9.6GB	eMMC 9.6GB	M.2 SSD 512GB
Log Storage	-	-	-	HDD 2TB
Form Factor	Desktop	19" Rack Mount/1U	19" Rack Mount/1U	19" Rack Mount/1U
Dimension (WxHxD mm)	220x44x194.5	438x44x194	438x44x194	430x44x340
Power (External Power Supply)	40W Single	65W Single	65W Single	100W Single
Operating Temperature	0~40°C			
Storage Temperature	-20~70°C			
Interface				
Slot	-	-	-	1
10/100/1000 Base-T	8	8	8	6 (Max 10)
1G Base-X	-	-	-	4 (Max 8)
Bypass	○			
System Performance				
Max Concurrent Sessions (CC)	1,000,000	1,500,000	2,000,000	3,500,000
Connection Per Second (CPS)	35,000	50,000	50,000	200,000
Firewall Throughput (UDP)	4G	6G	8G	12G
Firewall Throughput (UDP 64B)	1G	1.5G	2G	3.5G
IPS Throughput (Max)	-	1.5G	2.5G	5G
VPN Throughput	1G	1.2G	1.4G	2.5G
VPN Tunnels	2,500	5,000	5,000	20,000
Simultaneously Accessible Devices (ZTNA)	50	100	100	100
Simultaneously Accessible Sessions (SSL VPN)	500	1,000	1,000	1,000

Interface

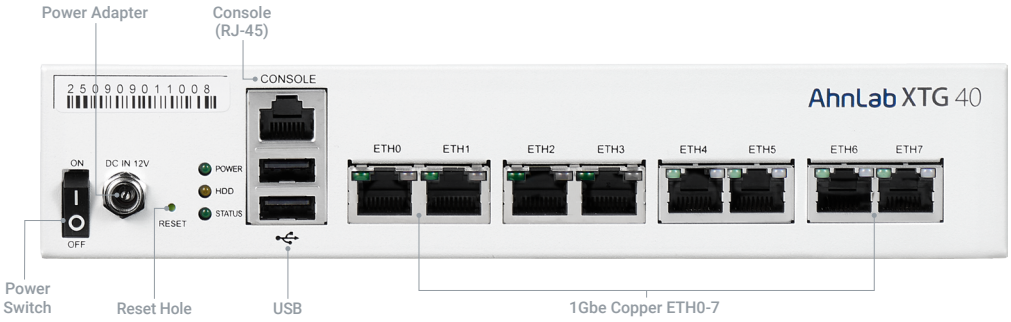
40

Front Panel



#	Category	Description
1	Status/Ethernet LED	Displaying the status of power, HDD, appliance, and ethernet port.

Back Panel

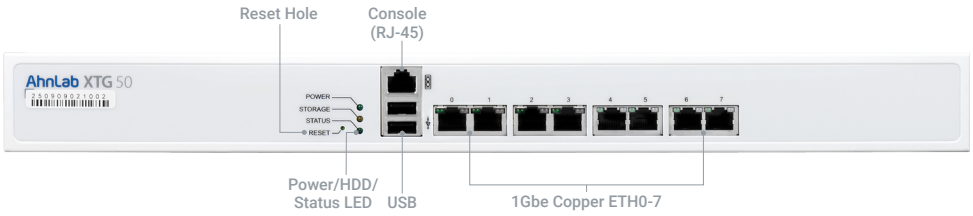


#	Category	Description
1	Power Switch	Press the power switch to run the appliance. If you press and hold the power switch of the operating machine, the power will be cut off, and the equipment will be forcibly shut down.
2	Power Adapter	Connecting the power to the appliance.
3	Reset Hole	Press it with a pin to restart the appliance.
4	Status LED	**POWER:** Displaying the power connection status of the appliance. **HDD:** Displaying the status of the appliance's flash memory. **STATUS:** Displaying the operating status of the appliance. It is off during booting and blinks at 1-second intervals when booting is complete.
5	Console Port	The port connects the appliance to the admin's computer via a serial cable. The admin can use CLI commands after connected.
6	USB Port	The port is disabled.
7	Ethernet Port	Admins can use CAT5, CAT 5e, or CAT 6 cables. It supports 10/100/1000Mbps connections.

Interface

50/70

Front Panel



#	Category	Description
1	Reset Hole	Press it with a pin to restart the appliance.
2	Status LED	Displaying the status of power and HDD.
3	Console Port	The port connects the appliance to the admin's computer via a serial cable. The admin can use CLI commands after connected.
4	USB Port	The port is disabled.
5	Ethernet Port	Admins can use CAT5, CAT 5e, or CAT 6 cables. It supports 10/100/1000Mbps connections.

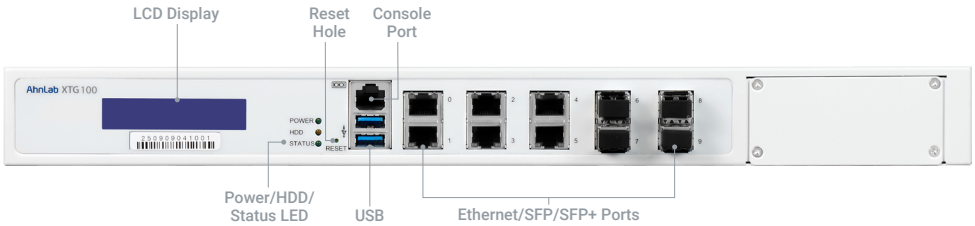
Back Panel

#	Category	Description
1	Power Switch	Press the power switch to run the appliance. If you press and hold the power switch of the operating machine, the power will be cut off, and the equipment will be forcibly shut down.
2	Power Supply	Connecting the power to the appliance.

Interface

100

Front Panel



#	Category	Description
1	LCD Display	Displaying current appliance status on LCD display. When the appliance boots up, it updates and displays the status, including product name, copyright, and PSU.
2	Status LED	Displaying the status of power and HDD.
3	Reset Hole	Press it with a pin to restart the appliance.
4	Console Port	The port connects the appliance to the admin's computer via a serial cable. The admin can use CLI commands after connected.
5	USB Port	The port is disabled.
6	Ethernet/SFP Port	**Ethernet (RJ45) Port:** Admins can use CAT5, CAT 5e, or CAT 6 cables. It supports 10/100/1000Mbps connections. **SFP Port:** Supporting SFP type of gigabit connection.

Back Panel

#	Category	Description
1	Power Switch	Press the power switch to run the appliance. If you press and hold the power switch of the operating machine, the power will be cut off, and the equipment will be forcibly shut down.
2	Power Supply	Connecting the power to the appliance.

Ordering Information

Product	Description
AhnLab XTG 40	RJ45*8, Console*1
AhnLab XTG 50	RJ45*8, Console*1
AhnLab XTG 70	RJ45*8, Console*1
AhnLab XTG 100	RJ45*6, 1G SFP*4, Console*1, Interface Slot*1

NIC Module	Description
1G Copper 8 Port	1GbE Copper (RJ45) 8 Port LAN Module with 2 Bypass Pairs
1G Fiber 4 Port	1GbE Fiber (SFP) 4 Port LAN Module
1G Fiber 8 Port	1GbE Fiber (SFP) 8 Port LAN Module
1G Fiber 2 Port Bypass	1GbE Fiber (SFP) 2 Port LAN Module with Bypass
1G Fiber 4 Port Bypass	1GbE Fiber (SFP) 4 Port LAN Module with Bypass

※ NIC Module can only be ordered if there is an interface slot available