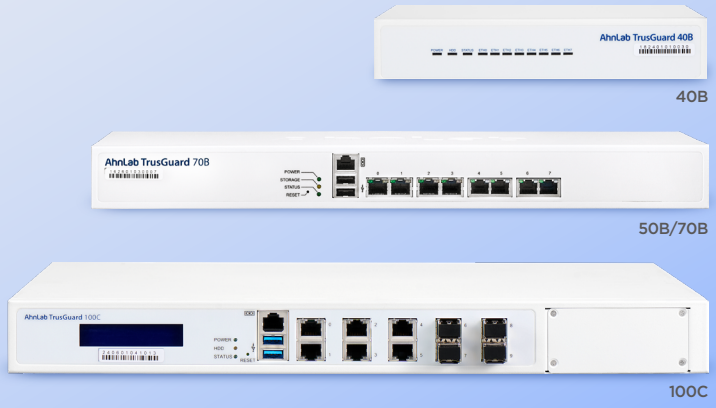
AhnLab

NGFW Lineup for Small Businesses

AhnLab TrusGuard 40B, 50B, 70B and 100C



Highlights

High-performance NGFW with strong traffic processing capabilities optimized for small businesses

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 powerful network segmentation in air-gapped environments, including IT-OT

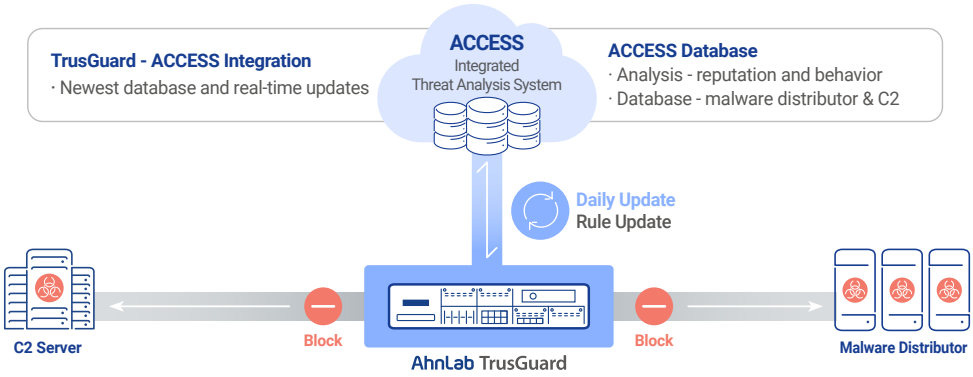
Simple and Efficient NGFW

We designed four models (40B, 50B, 70B, and 100C) of AhnLab TrusGuard, the next-generation firewall (NGFW), to address the security requirements of small businesses. AhnLab TrusGuard, recognized for its technology, performance, and stability by thousands of customers, not only offers NGFW and VPN capabilities but also provides next-generation network security features such as IPS, application control, URL filtering, C2 detection and prevention, anti-spam, DDoS mitigation, and DLP to protect customers' businesses.

Use Case

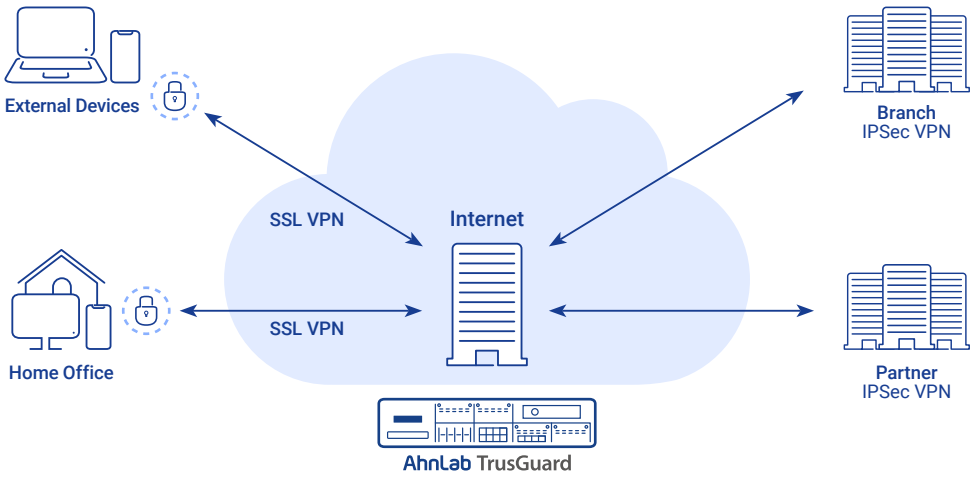
NGFW

- AhnLab TrusGuard 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.



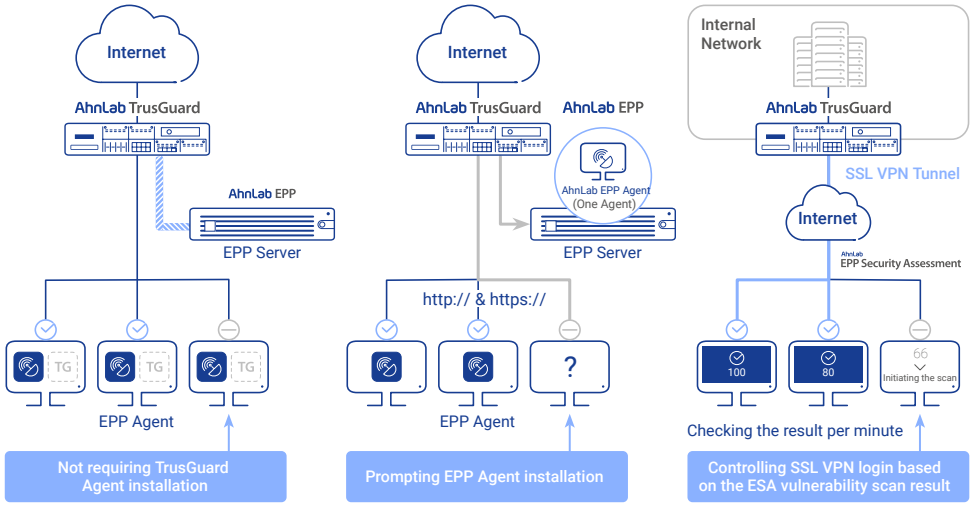
VPN – Remote Access

- AhnLab TrusGuard delivers both IPSec VPN and SSL 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.



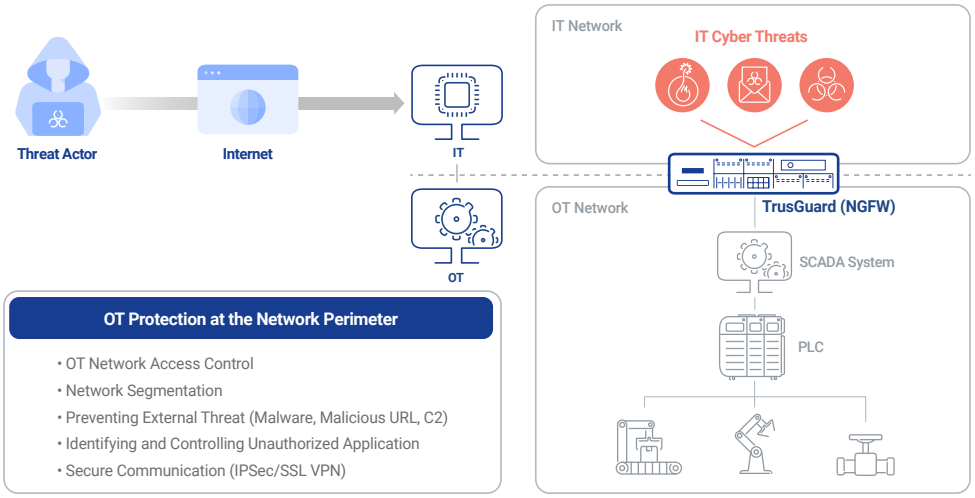
EPP Integration

- AhnLab TrusGuard integrates with AhnLab EPP to allow VPN access only for secure devices.
- The EPP integration implements device control without installing the TrusGuard agent.
- AhnLab TrusGuard guides users to install the EPP agent (HTTP/HTTPS).
- SSL VPN login is controlled based on the security assessment score of AhnLab ESA.



IT-OT Network Segmentation

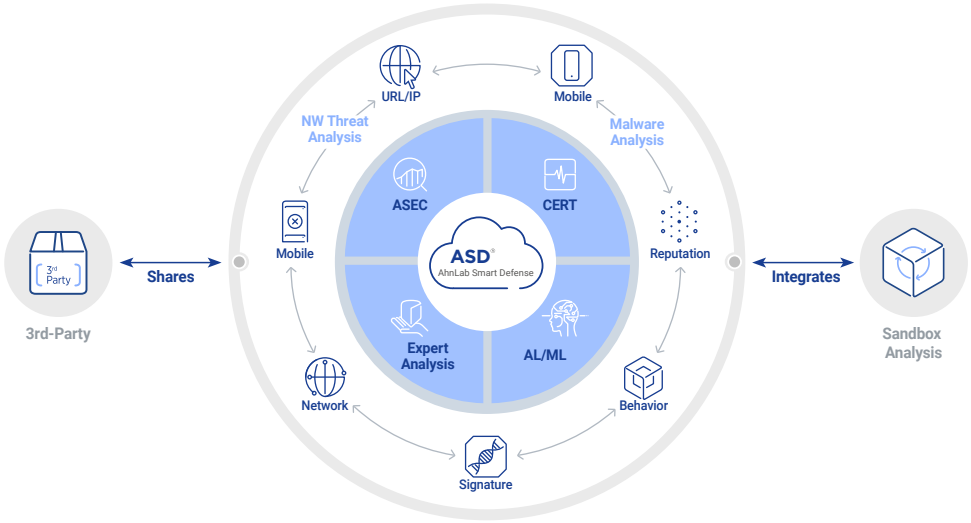
- AhnLab TrusGuard performs network segmentation and access control at the IT-OT perimeter to ensure networks are properly air-gapped.
- It blocks malicious URLs and C2 connections and supports IPSec/SSL VPN to enhance inter-network security.
- It provides OT-dedicated security capabilities by granularly controlling industrial protocols within the OT network.



Backend Infrastructure

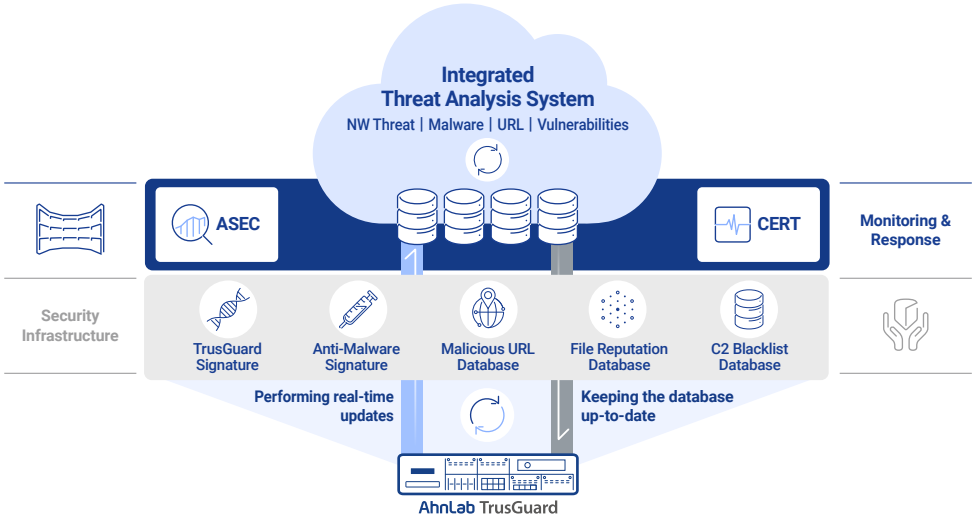
Technology

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 TrusGuard

AhnLab TrusGuard 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 TrusGuard delivers multiple features to keep up with the nature of a next-generation firewall, which is to protect internal networks from external cyber threats. In detail, customers can create user/device-based policies and choose whether to block, allow, or deny them. They 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 TrusGuard 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.

SSL VPN

The SSL VPN of AhnLab TrusGuard, 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. Its active/active configuration ensures service continuity without VPN reconnection, even when the devices experience failure. In addition, customers can enjoy the wide range of device options for SSL VPN connections as they can connect via mobile devices such as cell phones and tablets, as well as embedded devices.

C2 Detection & Prevention

AhnLab TrusGuard provides granular C2 detection and prevention backed by our C2 blacklist database. The C2 blacklist reflects behavior history over the past six months and guarantees high timeliness and reliability through daily updates. It analyzes C2 servers based on multiple factors, such as reputation and behavior. Then, it enables customers to make precise detection and prevention settings that consider the level of risk and range of spread.

IPS

AhnLab TrusGuard delivers IPS features that detects and blocks malicious traffic based on signatures and behavior rules; it offers over 7,000 signatures for vulnerability exploitations 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 TrusGuard 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 TrusGuard 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 ensures company-wide content visibility.

DDoS Mitigation

AhnLab TrusGuard, 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 feature of AhnLab TrusGuard 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 TrusGuard's features in a maximum of ten virtual instances.

Anti-Malware

AhnLab TrusGuard 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. A suspicious and undetermined file can be further analyzed using the sandbox solution integrated with the NGFW.

Anti-Spam

Powered by a globally certified anti-spam engine, AhnLab TrusGuard 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 TrusGuard to communicate with the EPP server and check the security status of multiple endpoint devices in real-time. The aggregated data helps AhnLab TrusGuard 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 and VLAN
	Operation Mode	· Router and bridge mode
	Routing Protocol	· Static, dynamic and multicast protocols
	DHCP	· Client, server and relay
NGFW	SSL Inspection	· Inspecting encrypted traffic
	Synchronization	· Admin settings, log settings and policies
	QoS	· Guaranteeing minimum and limiting maximum bandwidth per policy
	Blacklist	· Managing IPv4/IPv6 prevention · Inspecting protocols of L3, L4 and above
	Whitelist	· Supporting policy exception for IPv4/IPv6
	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, etc.)
	Policy Setting	· IP/MAC, user and device setting & control
IPSec VPN	Configuration	· Hub, spoke and mesh
	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, OTP, Oracle, FIDO, SMS, etc.)
	EPP Integration	· Ensuring endpoint device security before and after making VPN connection
	Supporting Devices	· Endpoint devices including mobile (cell phone/tablet) and embedded devices (router)
Virtual System	Virtualization	· Logical virtualization of appliance via MAC VLAN configuration
HA	NGFW	· Active/standby and active/active
	IPSec VPN	· Redundant VPN configuration for HQ (active/standby, active/active)
	SSL VPN	· Active/active
	Virtual System	· HA configuration for virtual systems
IPS	Signature	· Supporting over 7,000 signatures with regular update to patterns
	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, and detailed functions

Category	Subcategory	Description
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	· Our native engine
	Detection/Prevention	· High-speed malware detection and prevention powered by stream-based anti-malware engine
	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 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, etc
Others	Monitoring/Log	· Log storage: storing logs in embedded 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
		· Integration: Open API

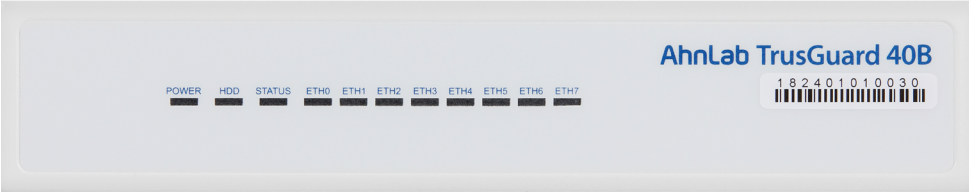
System Performance & Hardware Specification

Category	40B	50B	70B	100C
Certification				
CC Certificate	EAL4 (IPS Protection Profile & VPN Protection Profile)			
GS Certificate	○			
IPv6 Certificate	IPv6 Ready Logo Phase-2 (Router)	IPv6 Ready Logo Phase-2 (Router) IPv6 TTA Verified (Host)	IPv6 Ready Logo Phase-2 (Router) IPv6 TTA Verified (Host)	IPv6 Ready Logo Phase-2 (Router) IPv6 TTA Verified (Router)
Electromagnetic Wave Certificate	FCC/ KC			
Physical				
Processor	2 Core/1.6Ghz (1 each)	4 Core/1.6Ghz (1 each)	4 Core/2.2Ghz (1 each)	8 Core/2.4Ghz (1 each)
Memory	4GB	8GB	8GB	8GB
System Storage	eMMC 4GB			M.2 SSD 512GB
Log Storage	-	-	-	HDD 2TB
Form Factor	Desktop	19" Rack Mount/1U		
Dimension (WxHxD mm)	220x44x194.5	430x44x193	430x44x193	430x44x340
Power (External Power Supply)	40W Single Power	65W Single Power	65W Single Power	100W Single Power
Power Consumption (W)	17W	17.6W	20.4W	43.6W
Operating Temperature	0~40°C			
Storage Temperature	-20~70°C			
Heat (BTU/h)(Max)	58	60.05	69.6	117.37
Interface				
Slot	-	-	-	1
10/100/1000 Base-T	8	8	8	6 (Max 10)
1G Base-X	-	-	-	6 (Max 10)
Bypass	X	○		
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	5GB
VPN Throughput	1G	1.2G	1.4G	2.5G
VPN Tunnels	2,500	5,000	5,000	20,000
Simultaneous Access (SSL VPN)	-	500	1,000	1,000

Interface

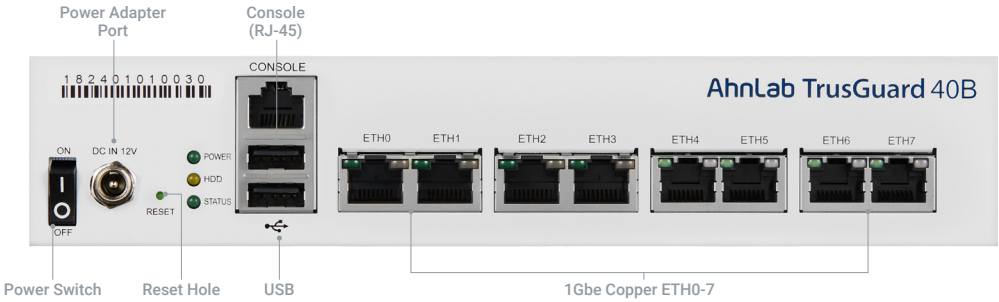
40B

Front Panel



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

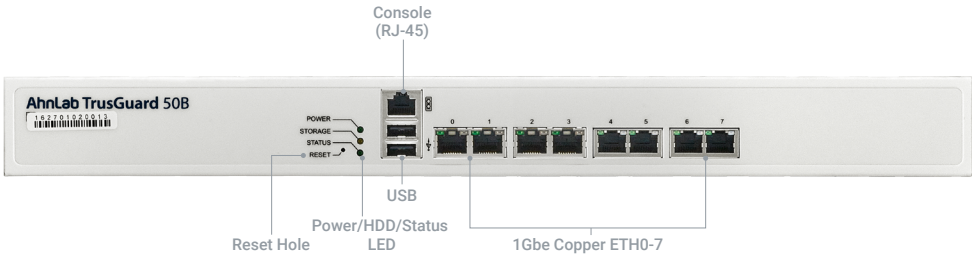
Back Panel



#	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.

50B/70B

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.

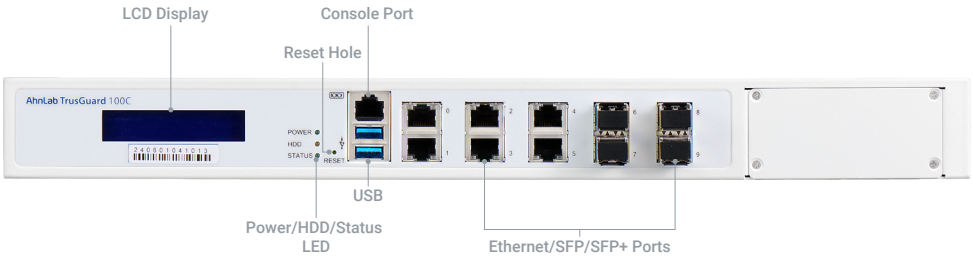
Back Panel



#	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.

100C

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	Displaying the status of power and HDD.
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 TrusGuard 40B	RJ45*8, Console*1
AhnLab TrusGuard 50B	RJ45*8, Console*1
AhnLab TrusGuard 70B	RJ45*8, Console*1
AhnLab TrusGuard 100C	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