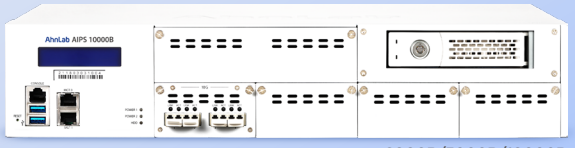
AhnLab

Next-Gen IPS Lineup for All Organizations

AhnLab AIPS 2000B, 5000B, 10000B and 20000



2000B/5000B/10000B

20000

Highlights

The next-gen IPS that detects and blocks the latest threats according to the requirements of various organizations

Precise detection and prevention of high-volume traffic by incorporating high-performance hardware and acceleration technology

Providing up to 128 logically separated “Security Zone” in a single appliance to **ensure resource efficiency**

Detecting traffic and applications across L2-L7 based on the latest signatures and behavior detection

Supporting advanced use cases by integrating with AhnLab TMS

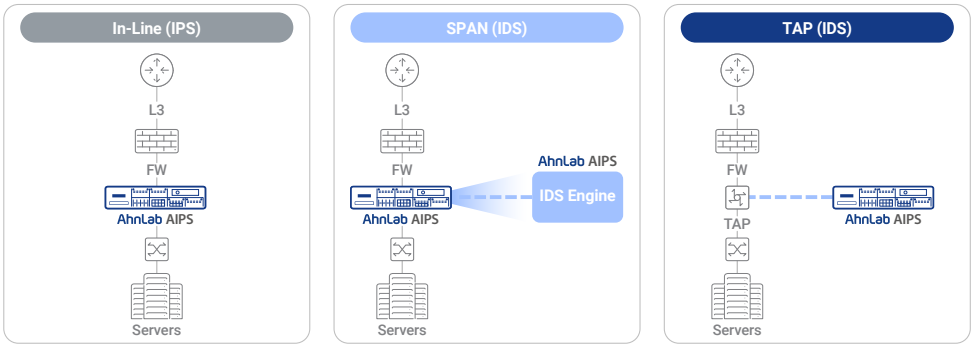
Next-Gen IPS Preventing Novel Threats

We designed four models (2000B, 5000B, 10000B and 20000) of AhnLab AIPS, the next-generation IPS, to address the security requirements of various organizations across multiple industries. AhnLab AIPS, powered by high-performance hardware and engines, precisely detects, analyzes, and blocks various types of network attacks, malware, and vulnerabilities (network, OS, web, applications, etc.) across L2-L7. Through this, it safely protects the customer's business environment from evolving network attacks.

Use Case

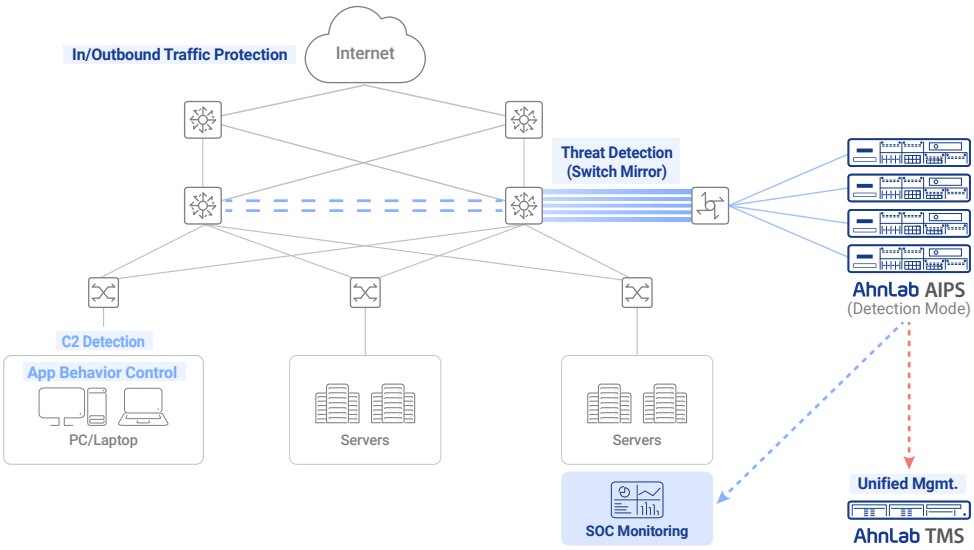
Next-Gen IPS and IDS

- AhnLab AIPS, located at the network perimeter, defends against network attacks and vulnerability exploitations attempted from outside and prevents C2 connections from inside.
- It offers next-gen IPS and IDS capabilities, allowing solution deployment tailored to various customer requirements.
- Customers can utilize IPS features through inline deployment and apply SPAN and TAP methods if they need IDS capabilities.



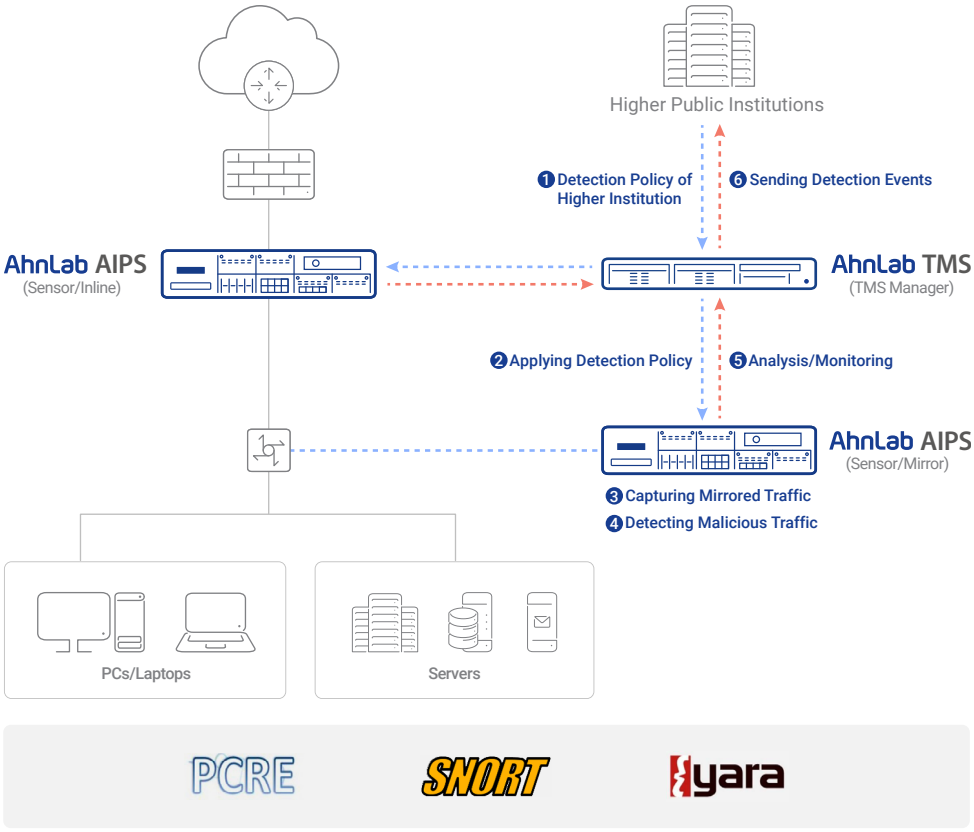
IDS for Data Centers

- Considering the characteristics of data centers where system availability is crucial, AhnLab AIPS provides traffic control and threat detection for inbound and outbound traffic of internal infrastructure.
- In the detection mode, AhnLab AIPS detects inbound traffic and network threats and C2 connections heading outside by mirroring the traffic through “Switch Mirror” to ensure system availability.
- It integrates with the central management solution “AhnLab TMS” to centralize the policy and appliance management, enhancing monitoring efficiency in the SOC.



National Network Security Architecture

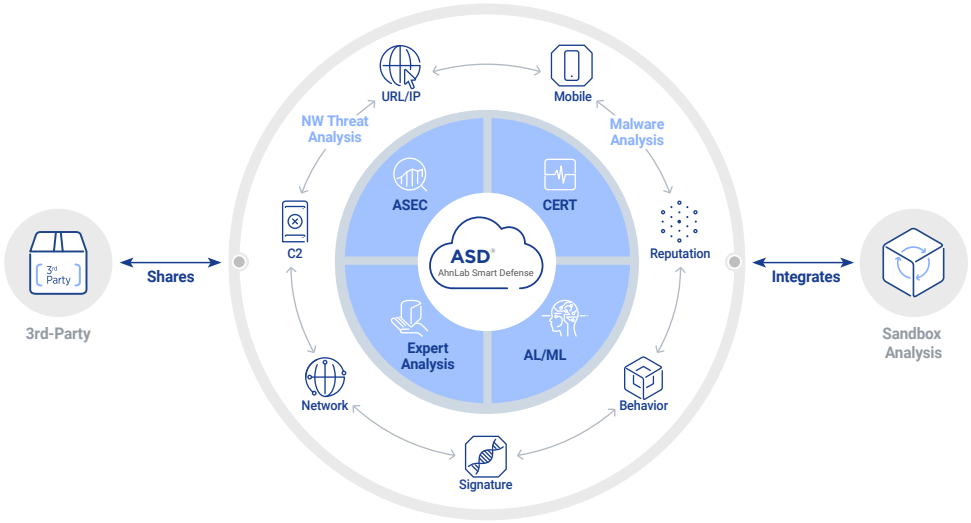
- AhnLab AIPS integrates with AhnLab TMS to support the security requirements of public institutions.
- Higher institutions can apply PCRE and Snort policies for network threat detection and YARA policies for malware detection to subordinate institutions' AhnLab AIPS through their AhnLab TMS.
- Subordinate institutions detect network threats according to the detection rules of the higher institution and report events via AhnLab TMS.
- This establishes a robust network threat detection and blocking system encompassing national institutions.



Backend Infrastructure

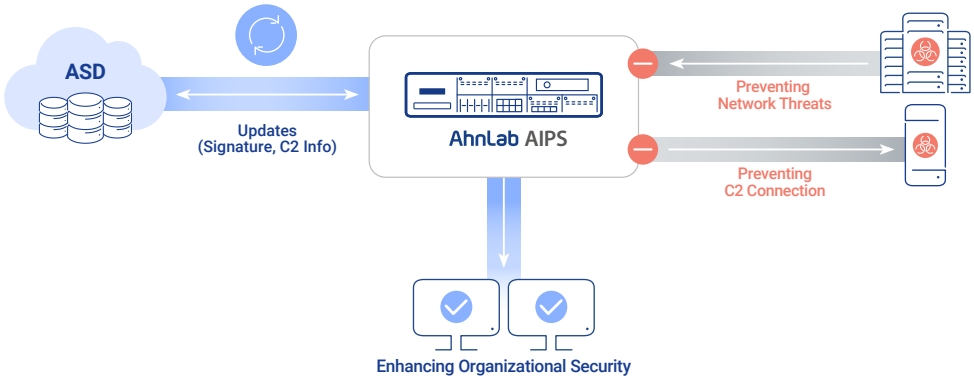
Technology

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 AIPS

Such sophisticated technology and infrastructure for threat detection, analysis, and response are also applied to AhnLab AIPS. Powered by our own infrastructure, AhnLab AIPS leverages the latest signatures, vulnerabilities, reputation, and C2 information to detect and block the latest network threats ahead of time.



Key Features

Signatures

AhnLab AIPS delivers exceptional network threat detection and blocking capabilities with our native high-performance engine and over 11,000 signatures optimized for modern network environments. Our signatures are the foundation of network intrusion prevention and are regularly and continuously updated to ensure superior network security.

Web Protection

AhnLab AIPS detects and blocks various web-based attacks, such as web vulnerability exploitations and flooding attacks, backed by its web protection capabilities. We pursue three approaches to web protection: URL categorization, user-defined URL, and malicious website prevention. To detect vulnerability exploitations using the HTTP protocol, AhnLab AIPS provides pre-defined and user-defined web protection rules, allowing customers to set policies tailored to their environments.

Behavior Detection

AhnLab AIPS utilizes thresholds to detect and block various malicious behaviors, such as port scans and protocol vulnerability-based DDoS attacks. Upon packet reception, it matches rules by protocol and identifies an attack that exceeds thresholds of detection frequency, attack duration, etc. Also, AhnLab AIPS offers traffic self-learning to help customers optimize threshold rules.

QoS

AhnLab AIPS ensures network stability through dynamic flooding and static flooding features. It applies threshold-based prevention policies to set bandwidth and control traffic when traffic exceeds the threshold. The product provides logs of attacks blocked, allowing customers to identify when and how the attack occurred and develop strategies to prevent similar attacks.

Security Zone

AhnLab AIPS can maximize operational efficiency by creating multiple security zones that logically divide a single appliance. Customers can configure up to 128 security zones by segment, VLAN, or IP address. Security policies operate per security zones, allowing customers to combine and set rules to detect and block attacks for each security zone. According to the configured rules, AhnLab AIPS can detect and block abnormal traffic, DDoS attacks, and network intrusions exploiting protocol and application vulnerabilities.

Application Control

AhnLab AIPS precisely controls over 1,600 applications to block cyber attacks and prevent the leakage of critical business data. It manages access by application and can control detailed actions within applications.

Overload Rule Management

AhnLab AIPS identifies rules that may affect product performance and allows customers to identify and manage the causes of overload. The product conducts a comprehensive pattern inspection to assess the overload. Then, based on protocol and port evaluation, performance impact is classified into five levels, from very high to very low. AhnLab AIPS performs an automatic rule optimization by considering the impact on performance.

Feature Snapshot

Category	Subcategory	Description
Signature	Signature Database	· Providing more than 11,000 signatures
	User-defined Signature	· Managing up to 20,000 signatures
Security Zone	Policy Setting and Monitoring	· Creating up to 128 security zones · Individual policy settings · Statistics and log monitoring
Detection Rule	Snort	· Maximal support of Snort options · Supporting Snort-based user-defined signatures
	PCRE	· Supporting various PCRE pattern matching
	YARA	· Providing YARA-based detection rules · Supporting up to 1,000 user-defined rules
Detection & Prevention	Web Protection	· Providing web protection rules · Registering up to 2,000 user-defined rules
	Abnormal Protocol	· Detecting and preventing traffic with protocol vulnerabilities (TCP, UDP, ICMP, etc.)
	Behavior	· Detecting and preventing malicious behaviors such as port and IP scan, protocol vulnerability spoofing and DDoS attacks
	C2 Connection	· Supporting up to 100,000 C2 blacklists (ASD)
	Threshold	· Registering up to 2,000 QoS policies
	X-Forwarded-for	· Extracting the actual IP from headers
URL Filter	Category-based URL Filter	· Detection and prevention of websites by categorizing URLs: general websites (27), malicious websites (31), malware source (8)
IP and Mac Address Control	Dynamic IP Quarantine	· 5 tuple-based IP control · Isolating up to one million IPs
	Blacklist	· Registering up to 200,000 IP blacklists
SSL Inspection	SSL-Encrypted Traffic Detection	· Decrypting SSL-encrypted traffic for inspection · Registering up to 1,000 addresses
	Exception Rule	· Allowlist for not performing SSL inspection · Registering up to 1,000 rules
Policy Optimization	Traffic Self-Learn	· Traffic learning based on certain behavior rules and web protection (flooding) over a certain period · Providing the threshold guideline
	Overload Rule Management	· Analyzing and optimizing the rules affecting product performance · Rule example: short detection pattern, no pattern, etc.
Application	Application Control	· Providing access control of more than 1,600 applications · Controlling detailed behaviors

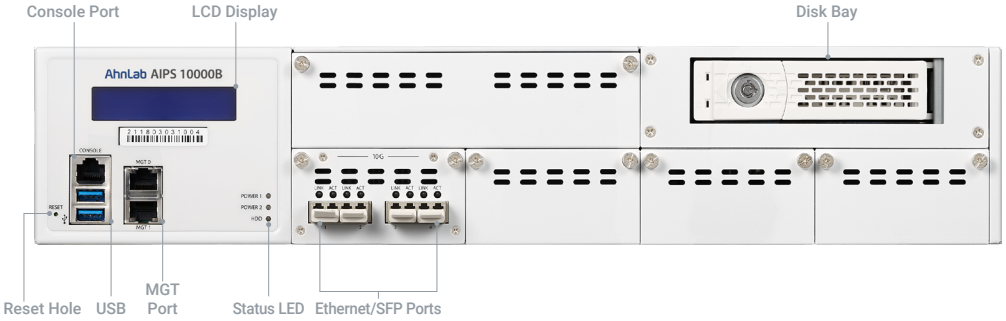
System Performance & Hardware Specification

Category	2000B	5000B	10000B	20000
Certification				
CC Certificate	EAL4 (IPS Protection Profile)			
GS Certificate	○			
IPv6 Certificate	IPv6 Ready Logo TTA Verified	IPv6 Ready Logo TTA Verified	IPv6 Ready Logo TTA Verified	Pv6 Ready Logo
Electromagnetic Wave Certificate	FCC/KCC			
Physical				
Processor	8 Core/3.5Ghz	10 Core*2/2.4Ghz	16 Core*2/2.9Ghz	24 Core*2/3.0Ghz
Memory	64GB	128GB	128GB	384GB
System Storage	SSD 64GB	SSD 64GB	SSD 64GB	SSD 64GB
Log Storage	HDD 2TB	HDD 2TB	HDD 2TB	SSD 1.92TB
Form Factor	19" Rack Mount/2U			
Dimension (WxHxD mm)	438x88x571			
Power (External Power Supply)	550W Redundant	550W Redundant	900W Redundant	900W Redundant
Power Consumption (W)	234.6W	241.8W	405.6W	534.8W
Operating Temperature	0~40°C	0~40°C	0~40°C	0~40°C
Storage Temperature	-20~70 ℃	-20~70 ℃	-20~70 ℃	-20~70 ℃
Heat (BTU/h)(Max)	800.45	825.02	1383.9	1824.73
Interface				
Slot	4	6	6	8
10/100/1000 Base-T	8 (Max 32)	8 (Max 48)	8 (Max 48)	0 (Max 48)
1G Base-X	2 (Max 16)	4 (Max 48)	0 (Max 48)	0 (Max 48)
10G Base-X	0 (Max 2)	0 (Max 24)	4 (Max 24)	0 (Max 24)
40G Base-X	-	-	0 (Max 6)	0 (Max 6)
100G Base-X	-	-	-	2 (Max 4)
Onboard 10GF	-	-	-	4 (HA-dedicated)
Bypass	○			
Performance				
IPS Throughput (UDP)	20G	80G	120G	200G
Max Concurrent Sessions (CC)	10,000,000	15,000,000	20,000,000	30,000,000
CPS	500,000	1,000,000	1,200,000	2,000,000

Interface

2000B/5000B/10000B

Front Panel



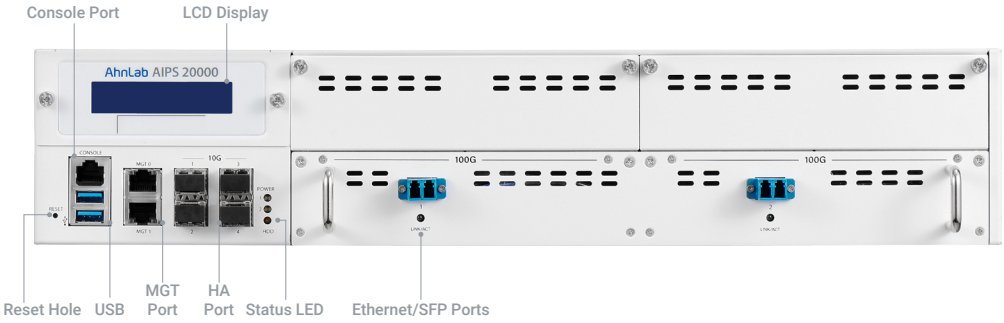
#	Category	Description
1	LCD Display	Displaying current appliance status on LCD display. When the appliance boots up, it updates and displays the status, including product name, copyright, and PSU.
2	Reset Hole	Press it with a pin to restart the appliance.
3	USB Port	The port is disabled.
4	Console Port	The port connects the appliance to the admin's computer via a serial cable. The admin can use CLI commands after connected.
5	MGT Port	The port enables connection to the web-based management console.
6	Status LED	Displaying the status of power and storage.
7	Ethernet/SFP Port	**Ethernet (RJ45) Port:** Admins can use CAT5, CAT 5e, or CAT 6 cables. It supports 10/100/1000Mbps connections. **SFP/SFP+ Port:** Supporting SFP type of gigabit connection.
8	Disk Bay	It is a rack that can hold storage (SSD/HDD) and it comes with a locking mechanism. AhnLab AIPS supports a disk bay that can hold two SSDs, which can be configured in RAID 0 or RAID 1.

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.

20000

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	Reset Hole	Displaying the status of power and storage.
3	USB Port	The port is disabled.
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	MGT Port	The port enables connection to the web-based management console.
6	HA Port	The port synchronizes status information for HA configuration between appliances
7	Status LED	The port enables connection to the web-based management console.
8	Ethernet/SFP Port	**Ethernet (RJ45) Port:** Admins can use CAT5, CAT 5e, or CAT 6 cables. It supports 10/100/1000Mbps connections. **SFP/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 AIPS 2000B	RJ45*8, SFP*2, MGT (RJ45)*2, Console*1, Interface Slots*4, Redundant Power
AhnLab AIPS 5000B	RJ45*8, SFP*4, MGT (RJ45)*2, Console*1, Interface Slots*6, Redundant Power
AhnLab AIPS 10000B	RJ45*8, SFP+*4, MGT (RJ45)*2, Console*1, Interface Slots*6, Redundant Power
AhnLab AIPS 20000	QSFP28*2, HA (SFP+)*4, MGT (RJ45)*2, Console*1, Interface Slots*8, Redundant Power

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
10G Fiber 4 Port	10G Fiber (SFP+) 4 Port LAN Module
10G Fiber 2 Port Bypass	10G Fiber (SFP+) 2 Port LAN Module with Bypass
10G Fiber 4 Port Bypass	10G Fiber (SFP+) 4 Port LAN Module with Bypass
40G Fiber 2 Port	40G Fiber (QSFP+) 2 Port LAN Module
40G Fiber 2 Port Bypass*	40G Fiber (QSFP+) 2 Port/2 Slot LAN Module with Bypass
100G Fiber 2 Port	100G Fiber (QSFP28) 2 Port/2 Slot LAN Module
100G Fiber 2 Port Bypass**	100G Fiber (QSFP28) 2 Port/4 Slot LAN Module with Bypass

※ Recommended to use a bypass NIC modules for network availability
* 40G NIC Modules can only be used in AhnLab AIPS 10000B/20000
** 100G NIC Modules can only be used in AhnLab AIPS 20000