AhnLab

# Central Network Security Management for All Organizations

## AhnLab TMS 2000B, 10000B and 20000B


### Highlights

**Network threat management system for central** management of policies and threat analysis and response of our network security solutions

**Providing two modules (Threat Manager and Policy Manager)** for effective threat and policy management

**Equipped with a big data processing engine to quickly process large volumes of logs** received from integrated solutions and supporting convenient search features

**Performing scenario-based correlation analysis and threshold-based analysis** by incorporating various events ingested from integrated solutions

**Supporting various use cases** based on the integration with AhnLab AIPS

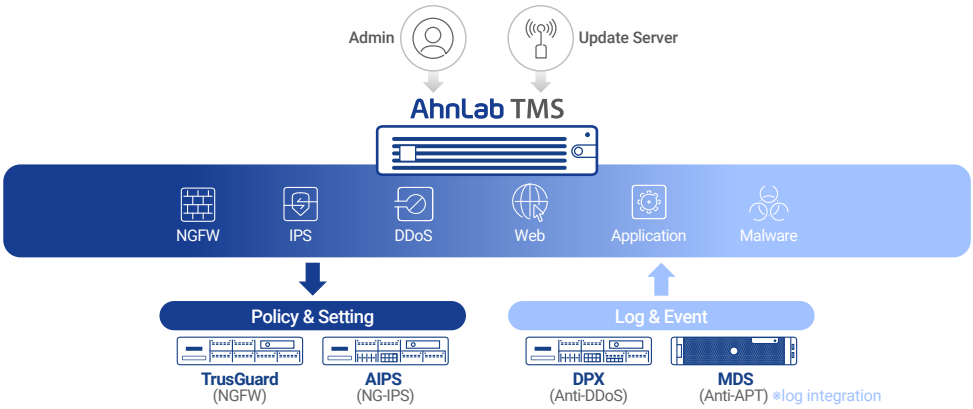
## Stay Resilient with Unified Network Security

We designed three models (2000B, 10000B and 20000B) of AhnLab TMS, to centrally manage our network security solutions and address the security requirements of various organizations across multiple industries. AhnLab TMS enhances operational efficiency of network security and helps customers stay resilient against modern network attacks through unified policy management for integrated solutions, large-scale event collection and management, and in-depth threat analysis and response by leveraging next-generation analysis technologies.

# Use Case

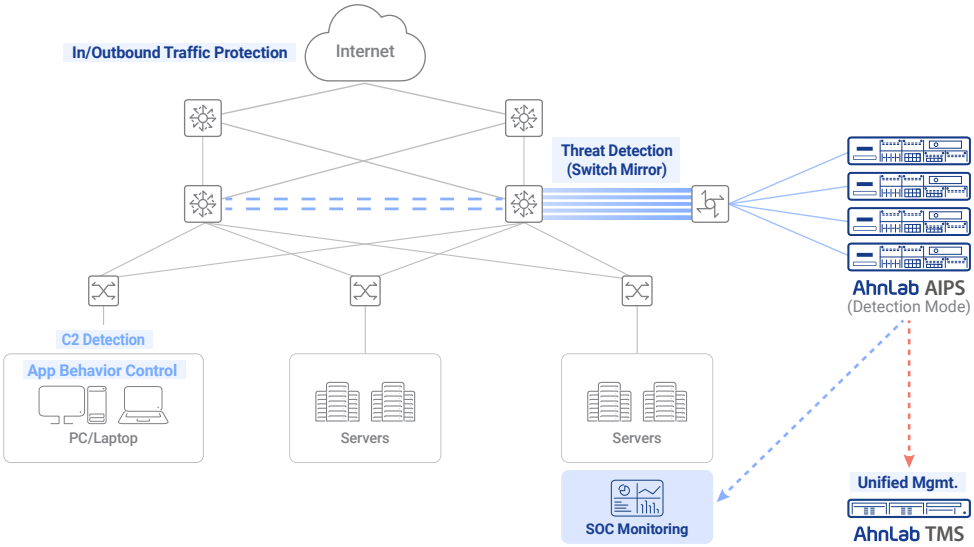
## Unified Network Security

- AhnLab TMS delivers unified management for our next-generation firewall, IPS, DDoS mitigation solution, and sandbox (APT response) solution.
- AhnLab TMS empowers customers with central policy and event management as well as in-depth threat analysis for integrated solutions.
- The threat management system creates a dynamic architecture that comprehensively analyze and respond to modern cyber threats difficult to defend against with a point solution.



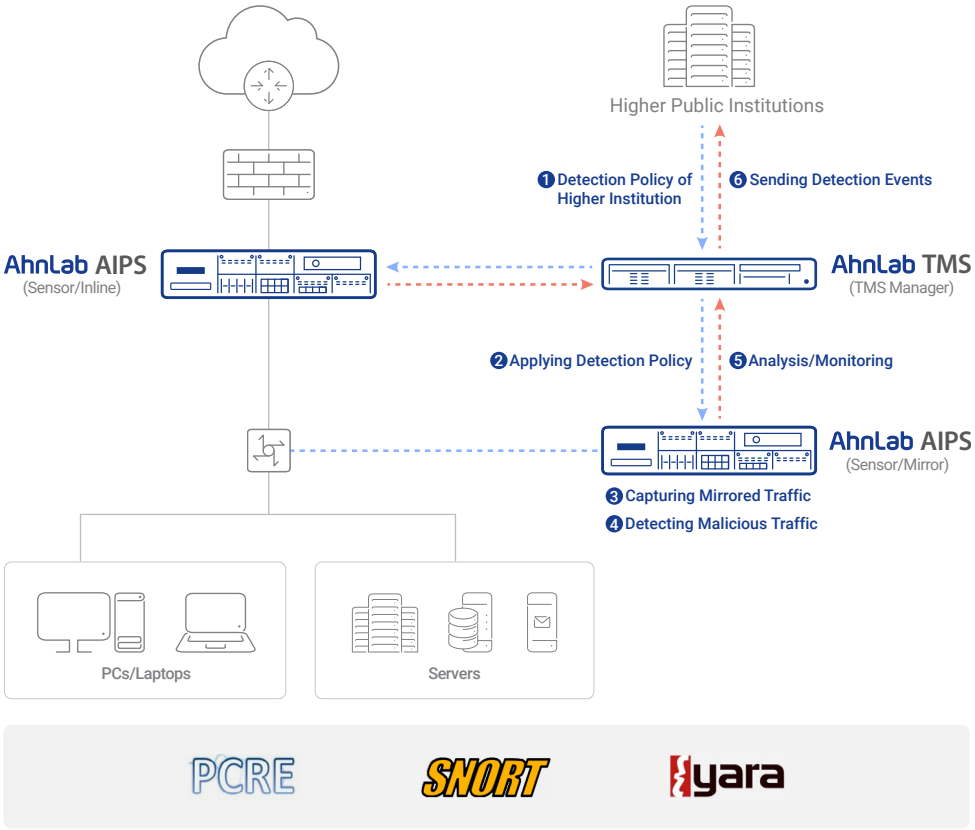

## IDS Management for Data Centers

- AhnLab AIPS, the next-generation IPS, 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.
- The next-generation IPS integrates with AhnLab TMS to centralize the policy and appliance management, enhancing monitoring efficiency in the SOC.



## National Network Security Architecture

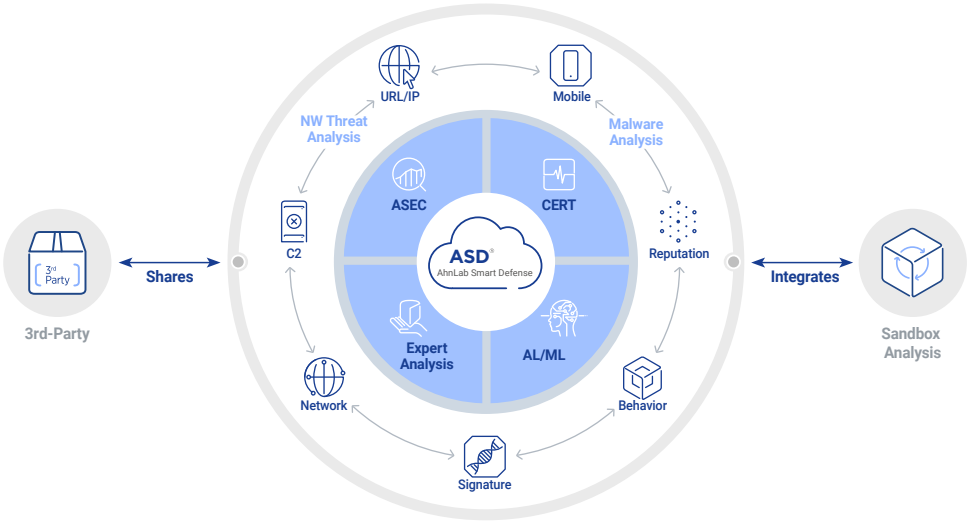
- AhnLab TMS and AhnLab AIPS support the security requirements of public institutions.
- Higher institutions can apply PCRE and Snort policies for network threat detection and YARA policies for malware detection to subordinate institutions' AhnLab AIPS through their AhnLab TMS.
- Subordinate institutions 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

## Intelligence-Driven Unified Network Security

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.




AhnLab TMS incorporates specialized technology and infrastructure for threat detection, analysis, and response, reflecting the latest signatures, vulnerabilities, reputation, and C2 information. In addition, the integration with our threat intelligence platform, AhnLab TIP, enables AhnLab TMS to precisely identify major vulnerabilities and cyber threat-related information. Customers can check details about vulnerabilities found in commercial software, affected product, and countermeasures, allowing them to proactively defend against the latest network threats.

# Key Features

## Two Modules

AhnLab TMS provides two modules, Threat Manager and Policy Manager, to help customers efficiently manage threats and security policies. Threat Manager is responsible for collecting logs, managing events, and performing integrated analysis for NGFW and IPS, offering custom dashboards and reports. Policy Manager supports the integrated or individual policy configuration and management for NGFW and IPS.

## Unified Threat Analysis

AhnLab TMS delivers integrated analysis of various events collected through connected appliances. Firstly, it provides automated analysis to detect and alert abnormal behaviors based on patterns learned from cyber threats, ranging from malicious traffic to malware. In addition, it offers scenario-based correlation analysis and threshold-based analysis by contextualizing multiple events. AhnLab TMS also provides a flexible interface that allows customers to quickly respond to imminent threats backed by comprehensive threat analysis.

## Unified Log Management

AhnLab TMS applies a big data engine to promptly collect and efficiently manage large-scale events. It supports integrated search and management of heterogeneous logs, regardless of appliance or log type. Also, it delivers maximal convenience for event and statistics lookup via flexible drill-down and correlation analysis to help customers better understand a current security status.

## Unified Policy Management

AhnLab TMS supports integrated or individual policy configuration and management, as well as status monitoring for our network security solutions. It enhances the operational efficiency by allowing policy management for each solution, common policy settings for multiple solutions, and integrated search for unused objects and policies. Additionally, it ensures network-wide resilience by enabling policy backup and restoration in case of unexpected failures.

## User-Centered Monitoring

AhnLab TMS offers user-centered monitoring and reporting features to deliver comprehensive visibility. Administrators can search for threat events and create custom rules for continuous statistics and analysis. Furthermore, the created rules can be added to custom dashboards for real-time monitoring and generating custom reports for reporting purposes.

# Feature Snapshot

| Category | Subcategory | Description |
|---|---|---|
| Threat Manager | Threat Management | · Identifying and managing collected events |
| | Relay | · Relaying policies and logs between institutions |
| | Network Monitoring | · Threat monitoring for each network domain |
| | Account Monitoring | · Real-time monitoring for each user account |
| Policy Manager | Individual and Collective Policy Management | · Individual and collective policy management of integrated solutions |
| | Copying Policy | · Providing a policy copy feature between appliances for efficient policy configuration |
| | Central Policy and Configuration Management | · Individual or collective management of policies and configurations |
| | Export/Import | · Supporting export and import features for unified management of policies and objects |
| | Unused Policy Lookup | · Looking up an unused policy of firewall |
| | Unused Object Lookup | · Checking unused and unreferred firewall objects<br>· Delivering information for optimal object configuration |
| | Unused Policy Management | · Visualizing the hit count of each firewall policy for managing unused policy |
| | Scheduled Execution | · Running scripts to schedule real-time and periodic execution of the solution |
| | Disaster Recovery | · Supporting transition to disaster recovery (DR) mode for solutions with DR settings |
| | Rollback | · Supporting the rollback of recent policies and configurations |
| | History Comparison | · Supporting the change history comparison for recent policies and configurations |
| Log Management | Unified Log Provision | · Providing integrated logs of heterogenous appliances, allowing for batch search of various events |
| | Advanced Search | · Supporting logical queries (And/Not/Or/Wild Card) for searching under various conditions |
| | Operational Log Provision | · Providing system operation logs to check the status of solution |

| Category | Subcategory | Description |
|---|---|---|
| Statistics/Analysis | Event Statistics | · Providing top and trend statistics for events |
| | User-Defined Statistics | · Delivering custom top and trend statistics for flexible analysis under various conditions |
| | User-Defined Event Analysis | · Enabling threshold-based custom event analysis |
| | Auto-Prevention of Source IP | · Auto-prevention of source IPs for rapid threat response |
| | Threat Detection Alert | · Sending alerts via pop-up, email, sound, and SMS upon threat detection |
| | Statistics Report | · Generating reports based on statistical rules<br>· Flexible report generation for various statistics |
| | Correlation Statistics | · Creating top and trend statistics for additional correlation analysis |
| Monitoring | Default and User-Defined Dashboard | · Providing default and user-defined dashboards for traffic, threats, and DDoS monitoring |
| | Account-Dedicated Dashboard | · Offering account-dedicated custom dashboards to support convenient monitoring for different users |
| | Drill-Down | · Providing flexible drill-down to log and statistics from the dashboard for additional analysis |
| | Resource Monitoring | · Real-time monitoring of appliance resources (CPU, memory, disk) and key statuses (HA, session, bps/pps) |
| Report | User-Defined Report | · Providing user-defined statistical reports to suit user reporting purposes |
| | Periodic Report | · Generating daily, weekly and monthly reports |
| System | Privilege Management | · Granting three level privileges (read, edit, all) per users |
| | Access Control | · Setting access times, lock times, allowed login failure attempts, password change intervals, and account locking for effective admin access control |
| | Remote Restart | · Remotely restarting the solution |
| | Remote Update | · Remotely updating the firmware of the solution |
| | Data Restoration | · Restoring the backup data of the solution |
| | Signature Update in Air-Gapped Network | · Manually updating signatures and databases in an air-gapped network |

# System Performance & Hardware Specification

| Category | 2000B | 10000B | 20000B |
|---|---|---|---|
| **Certification** | | | |
| **CC Certificate** | EAL4 | | |
| **Electromagnetic Wave Certificate** | KC | | |
| **Physical** | | | |
| **Processor** | 4 Core/3.6Ghz | 10 Core/2.4Ghz | 10 Core*2/2.4Ghz |
| **Memory** | 16GB/32GB (Optional) | 32GB/64GB (Optional) | 64GB/128GB (Optional) |
| **System Storage** | SSD 500GB | SSD 500GB | SSD 500GB |
| **Log Storage** | SATA3 1TB | SATA3 3TB | SATA3 3TB |
| | 1 Slot (1 Backup Slot)<br>Type: 1TB/2TB/4TB | 4 Slot<br>Type: 1TB/2TB/4TB/8TB/12TB | 8 Slot<br>Type: 1TB/2TB/4TB/8TB/12TB |
| **Dimension (WxHxD mm)** | 437x503x43 | 437x507x43 | 437x647x89 |
| **Power (External Power Supply)** | 500W Single | 800W Redundant | 800W Redundant |
| **Power Consumption (W)** | 500W | 800W | 800W |
| **Operating Temperature** | 5~35 ℃ | 5~35 ℃ | 5~35 ℃ |
| **Storage Temperature** | -40℃ ~ 70℃ | -40℃ ~ 70℃ | -40℃ ~ 70℃ |
| **Heat (BTU/h)(Max)** | 1,700 | 2,700 | 2,700 |
| **Interface** | | | |
| **10/100/1000 Base-T** | 4 | 2 | 2 (Max 4) |
| **1G Base-X** | - | - | 0 (Max 2) |
| **10G Base-X** | - | - | 0 (Max 2) |

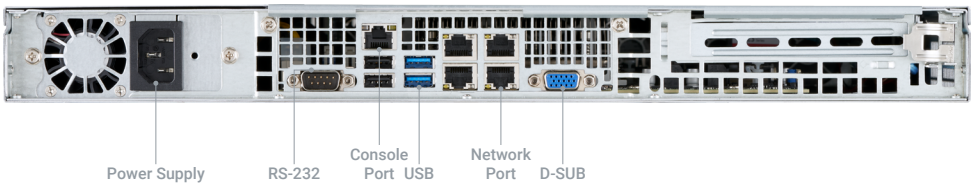
# Interface

## 2000B

### Front Panel


| # | Category | Description |
|---|---|---|
| 1 | Status LED | The LED displays the status of appliance. |
| 2 | Lock Key | Users can lock or unlock the appliance. |
| 3 | Bezel Unlock Button | This is the button for unlocking the bezel. |

### Back Panel



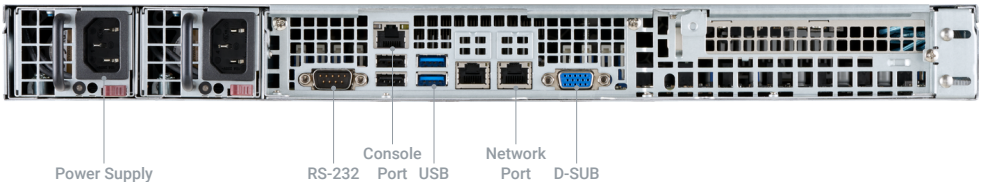

| # | Category | Description |
|---|---|---|
| 1 | Power Supply | Connecting the power to the appliance. |
| 2 | RS-232 | This is a port for a serial communication. |
| 3 | Console Port | The port is disabled. It connects the appliance to the admin's computer via a serial cable. The admin can use CLI commands after connected. |
| 4 | USB | This is the port for USB connection. |
| 5 | Network Port | This is a port for network connection of the appliance. |
| 6 | D-SUB | This is a D-SUB cable that transmits analog signals. |

# 10000B

## Front Panel


| # | Category | Description |
|---|---|---|
| 1 | Status LED | The LED displays the status of appliance. |
| 2 | Lock Key | Users can lock or unlock the appliance. |
| 3 | Bezel Unlock Button | This is the button for unlocking the bezel. |

## Back Panel



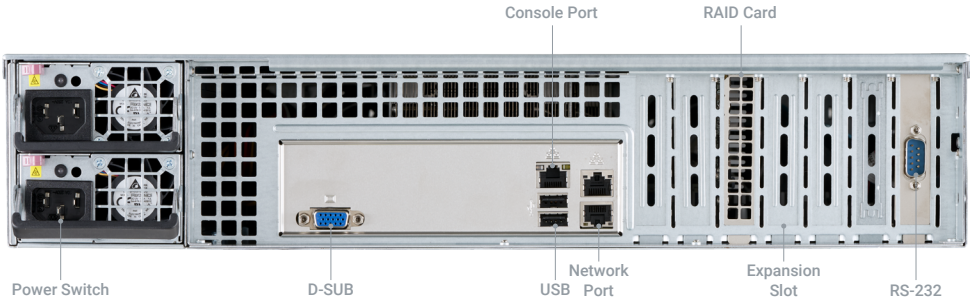

| # | Category | Description |
|---|---|---|
| 1 | Power Supply | Connecting the power to the appliance. |
| 2 | RS-232 | This is a port for a serial communication. |
| 3 | Console Port | The port is disabled. It connects the appliance to the admin's computer via a serial cable. The admin can use CLI commands after connected. |
| 4 | USB | This is the port for USB connection. |
| 5 | Network Port | This is a port for network connection of the appliance. |
| 6 | D-SUB | This is a D-SUB cable that transmits analog signals. |

# 20000B

## Front Panel


| # | Category | Description |
|---|---|---|
| 1 | Status LED | The LED displays the status of appliance. |
| 2 | Lock Key | Users can lock or unlock the appliance. |
| 3 | Bezel Unlock Button | This is the button for unlocking the bezel. |

## Back Panel




| # | Category | Description |
|---|---|---|
| 1 | Power Supply | Connecting the power to the appliance. |
| 2 | D-SUB | This is a D-SUB cable that transmits analog signals. |
| 3 | Console Port | The port is disabled. It connects the appliance to the admin's computer via a serial cable. The admin can use CLI commands after connected. |
| 4 | USB | This is the port for USB connection. |
| 5 | Network Port | This is a port for network connection of the appliance. |
| 7 | RAID Card | This is where users can mount the RAID card. |
| 8 | Expansion Slot | It expands network ports to enhance network connectivity. |
| 9 | RS-232 | This is a port for a serial communication. |

# Ordering Information

| Product | Description |
|---|---|
| **AhnLab TMS 2000B** | RJ45*1, 10/100/1000 Base-T*4, Single Power |
| **AhnLab TMS 10000B** | RJ45*1, 10/100/1000 Base-T*2, Redundant Power |
| **AhnLab TMS 20000B** | RJ45*1, 10/100/1000 Base-T*2, 10/100/1000 Base-T*2 (Option)<br>1GF*2 (Option) 10GF*2 (Option), Redundant Power |

| NIC Module | Description |
|---|---|
| **1G Copper 4 Port** | 1GbE Copper (RJ45) 4 Port LAN Module |
| **1G Copper 2 Port** | 1GbE Copper (RJ45) 2 Port LAN Module |
| **1G Fiber 2 Port** | 1GbE Fiber (SFP) 2 Port LAN Module |
| **10G Fiber 2 Port** | 10G Fiber (SFP+) 2 Port LAN Module |
| **Storage Type** | **Description** |
| **TMS 2000B HDD BASIC** | SATA3 1TB*1, 1 Slot (Option Type: 1TB/2TB/4TB)<br>*A separate backup slot can be used |
| **TMS 2000B SSD Option** | Option Type: 960GB/1.92TB |
| **TMS 10000B HDD BASIC** | SATA3 1TB*3, 4 Slots (Option Type: 1TB/2TB/4TB/8TB/12TB) |
| **TMS 10000B SSD Option** | Option Type: 960GB/1.92TB |
| **TMS 10000B RAID** | Default: Raid 5 (Option Type: 0, 1, 5, 6, 10, 50, 60) |
| **TMS 20000B HDD (Default)** | SATA3 1TB*3, 8 Slots (Option Type: 1TB/2TB/4TB/8TB/12TB) |
| **TMS 2000B SSD Option** | Option Type: 960GB/1.92TB |
| **TMS 20000B RAID** | Default: Raid 5 (Option Type : 0, 1, 5, 6, 10, 50, 60) |

※ Recommended to use a bypass NIC modules for network availability