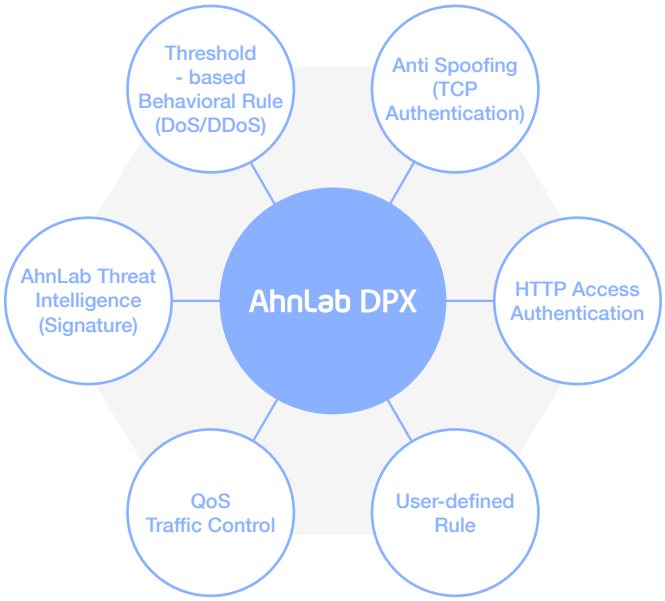
AhnLab DPX

High Performance DDoS Mitigation Solution

AhnLab DPX protects customers from DDoS attacks with the specialized technology, experience, and expertise.

Overview

DDoS remains to be one of the oldest, yet the most frequent cyber-attack. Especially because of its ease of accessibility, DDoS has evolved into various forms, making it difficult to block with a single detection method. AhnLab DPX is a is the industry-leading DDoS mitigation solution specialized in addressing DDoS attacks. Built on our dedicated DDoS mitigation technology, AhnLab DPX delivers advanced traffic analysis and multiple detection techniques.

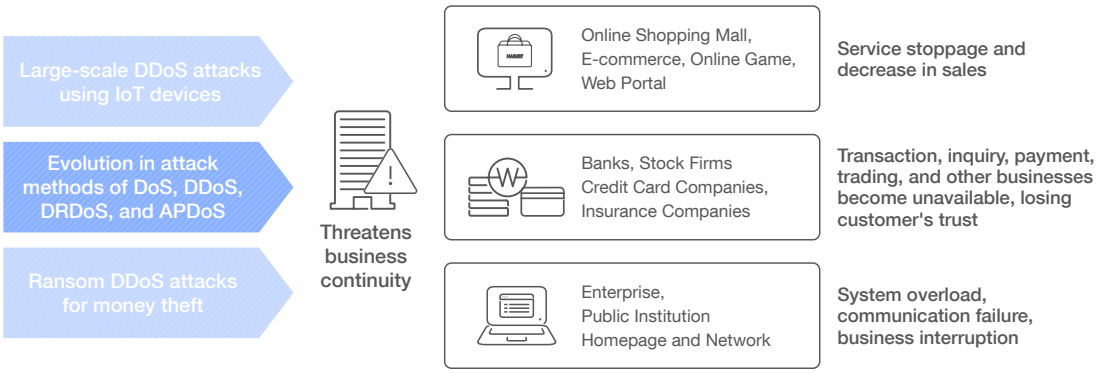


Advantages

Analyzes L2–L7 layer information, packet headers and payloads for precise threat detection	Supports multi-tenancy based on a maximum of 1000 zones
Full stack DDoS mitigation that covers next-gen protocols (QUIC) and supports scrubbing center integration	Granular response to DDoS traffic with over 60 behavioral rules
Unmatched packet processing with DPDK (Data Plane Development Kit)	High-performance traffic sensor generating 40 types of logs per protection target and transmitting them to each log server.

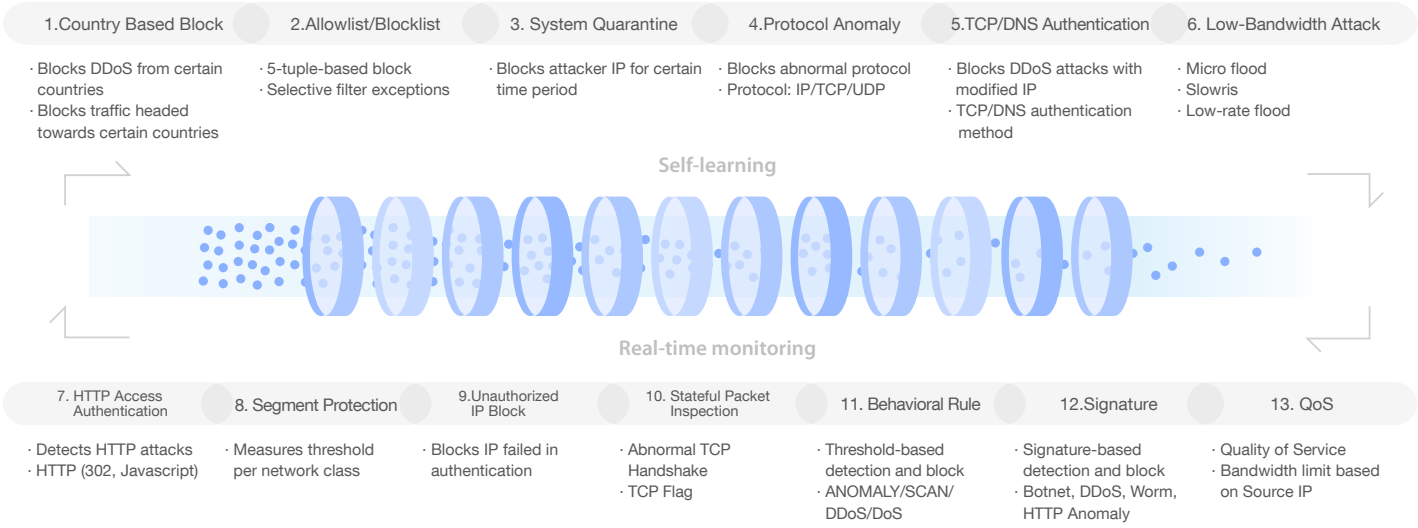
Advanced DDoS Attacks

A specialized security solution is required to mitigate prevalent and advanced DDoS attacks.



13-Layered Filtering

AhnLab DPX mitigates and responds to DDoS attacks with 13-layered filters.



Authentication

AhnLab guarantees the best authentication feature to identify whether the subject causing traffic is human or bot. We are capable of detecting and blocking the majority of automated DDoS attack bots.

Features for User Convenience

AhnLab DPX provides the following features for user convenience.

Threat Response: Convenient Features for Threat Response
- Alerts anomalies in CPU, memory, disk, and traffic (Email, SMS, SNMP)
- Packet capture & Packet auto collection and transmission & SNMP

Multi-Tenancy: Environment Separation with a Single Device
- Zone settings per protection target
- Policy & admin, log transmission and optimized traffic learning (self-learn) per Zone

* Number of supported zones differs by models

Intelligence Based on Diverse Logs and Response Policies
- Triages logs into 40 different types - identifying traffic status per protection target
- Detection information and report & Integration with multiple log servers, SIEM and SOAR

Complete DDoS Response

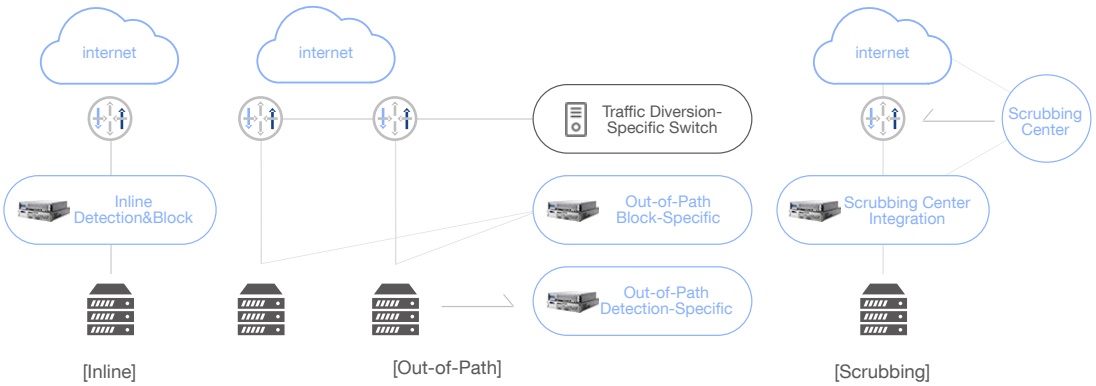
AhnLab DPX can prevent various types of DDoS attacks. Customers can experience an advanced response capabilities by interoperating the solution with AhnLab MDS(APT), AhnLab TMS(Threat Management), and AhnLab Sefinity AIR(SOAR).

Category	Attack Type	Description	Response Feature
Attack Method	DoS	An attack from a single client toward a single server (1:1)	· DoS behavioral rule · ACL-based blocklist · Thresholds-based behavior rule · Access control (TCP/UDP/ICMP)
	DDoS	· A simultaneous attack using bot and infecting multiple PCs with malware · An attack from multiple clients toward a single server (N:1)	· DDoS Behavioral Rule · Anti-Spoofing (TCP Authentication) · HTTP Access Authentication · System Quarantine / QoS
	DRDoS	· A UDP Attack using a reflector · Reported new cases of attacks with alternate protocols and ports	·DRDoS behavioral rule · ACL-based blocklist · DRDoS amplifier detection
Volumetric DDoS	TCP Flooding	· Attacks with mixing TCP components · SYN, ACK, XMAS (ALL), NULL (Nothing), etc.	· Behavioral rule (TCP) · Anti-Spoofing (TCP authentication) · Stateful packet inspection
	UDP Flooding	· An attack using characteristics of UDP. · Can be combined with DRDoS · Based on connectionless/unreliable characteristics of UDP protocol · Memcached, SNMP, CHARGEN, DNS, NTP, etc.	· Behavioral rule (UDP) · Segment protection · DNS authentication
	HTTP Flooding	· An attack using HTTP request · Different types of attack per HTTP Method (i.e., GET, POST)	· Behavioral rule (HTTP) · HTTP access authentication
	Fragmentation Flooding	· An attack through fragmented IP packets · Induces load via packet recombination · Used as a method to bypass solution policy	· Behavioral rule (Fragmentation) · Signature
	DNS Flooding	· NXDOMAIN attack that drains DNS server resources	· Anti-spoofing (NXDomain authentication)
Low-Volume DDoS	Low-Volume Precise Strike	· Low-volume attack to bypass solution policy · Occupying server resource without terminating session & induces depletion (i.e.: Exhaustion attack)	· Anti-spoofing (TCP authentication) · HTTP access authentication · Signature and protocol anomaly
	Abnormal Protocol	· An abnormal protocol attack violating protocol rules · Usually detected/responded in a form of vulnerability · Caused by wrong settings or low application version i.e.: Ping of Death, Slowloris, Slowread, LAND, Rudy, Smurf	· Behavioral rule (Anomaly) · Anti-spoofing (TCP authentication) · HTTP access authentication · Signature and protocol anomaly

Deployment & Configuration

AhnLab DDoS supports various deployment methods based on the network structure.

- Inline: Easly to setup and strong in real-time prevention
- Out-of-Path: Separates detection and prevention for threat mitigation in large-scale environments
- Scrubbing: Increase visibility by integrating with cloud scrubbing centers for excess traffic



Category	Inline	Out-of-Path
# of Devices Required	1 (Detection & Response)	2 (Detector: Detection, Guard: Block)
Deployment Difficulty	Real time protection and easy to implement	Minimal bottlenecks and network impact
DDoS Response Speed	Very Fast	Fast
Client	Public Institution, Finance, School	ISP, Portal, IDC

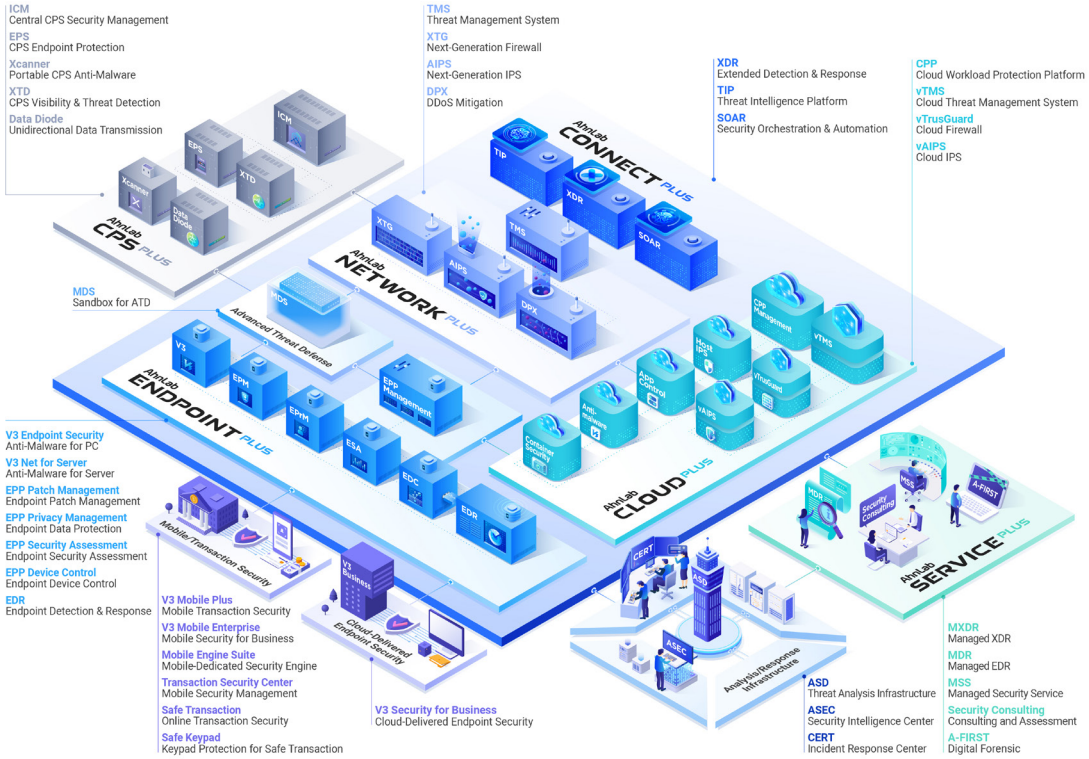
Specifications

		AhnLab DPX 5000C	AhnLab DPX 10000C	AhnLab DPX 20000C
CPU		8Core	16Core x 2	32Core x 2
Memory		128GB	256GB	512GB
HDD		SSD 2TB (1.92TB)	SSD 2TB (1.92TB)	SSD 2TB (1.92TB)
NIC	1GC	(Max 32) Mgmt not included	(Max 64) Mgmt not included	(Max 64) Mgmt not included
	1GF	(Max 8)	(Max 16)	(Max 16)
	10GF	(Max 8)	(Max 16)	(Max 16)
	40GF	–	0 (Max 4)	0 (Max 4)
	100GF	–	–	0 (Max 4)
Power		550W, Redundant	1300W, Redundant	1300W, Redundant
Korean CC Certification		EAL4 (DDoS Response Equipment Security Requirement V3.0)		

* Performance may vary by environment and system configuration.

AhnLab

AhnLab is a global unified security vendor with variety of solutions and a professional services. AhnLab DPX also interoperates with AhnLab TMS (Threat Management) and AhnLab SOAR (SOAR), AhnLab TIP (Threat Intelligence) and customers can also enjoy the benefits of specialized professional services.



AhnLab, Inc.
220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13493, South Korea
www.ahnlab.com/en | global.sales@ahnlab.com

AhnLab