AhnLab DPX

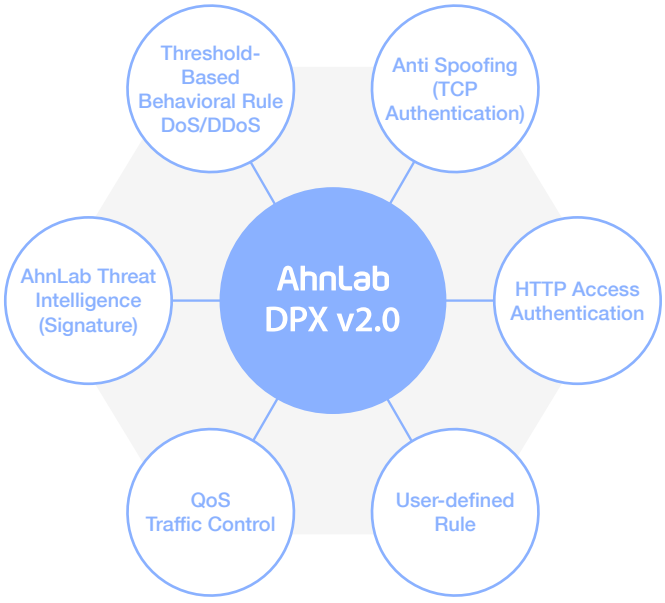
The Best 100G DDoS Mitigation Solution

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

Overview

AhnLab DPX(DDoS Prevention eXpress) is a solution specialized in mitigating DDoS attacks. Released in 2021, AhnLab DPX v2.0 was built on the foundation of AhnLab TrusGuard DPX v1.0 which was first released in 2010. AhnLab's cutting-edge anti-DDoS technology and expertise allow DPX to mitigate DDoS attacks in a 100G environment.

DDoS remains to be one of the oldest and the most frequent cyber-attack. With its long history, DDoS is capable of effortless attacks of various methods. To mitigate these DDoS attacks, a wide variety of response methods is required. AhnLab DPX provides the following DDoS response features.

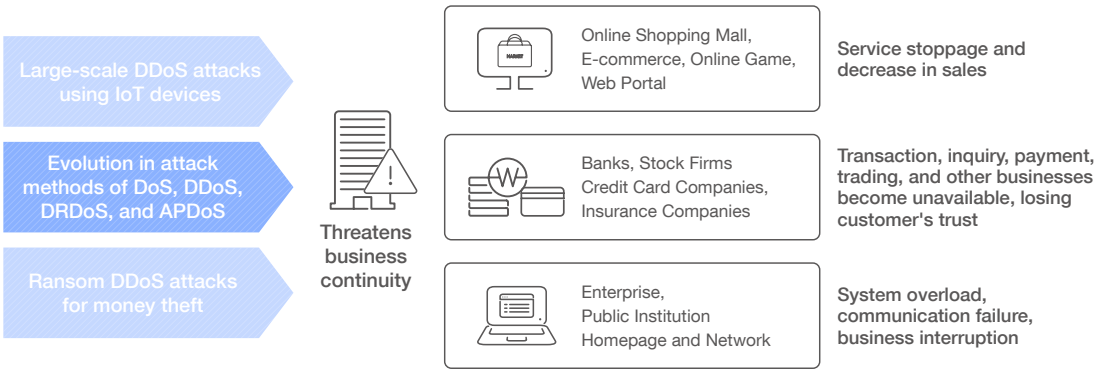


Advantages

Supports 40G and 100G NIC	Supports multi-tenancy based on a maximum of 500 Zones
Newly released high-performance DPX 20000B model with the latest Intel server platform	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.

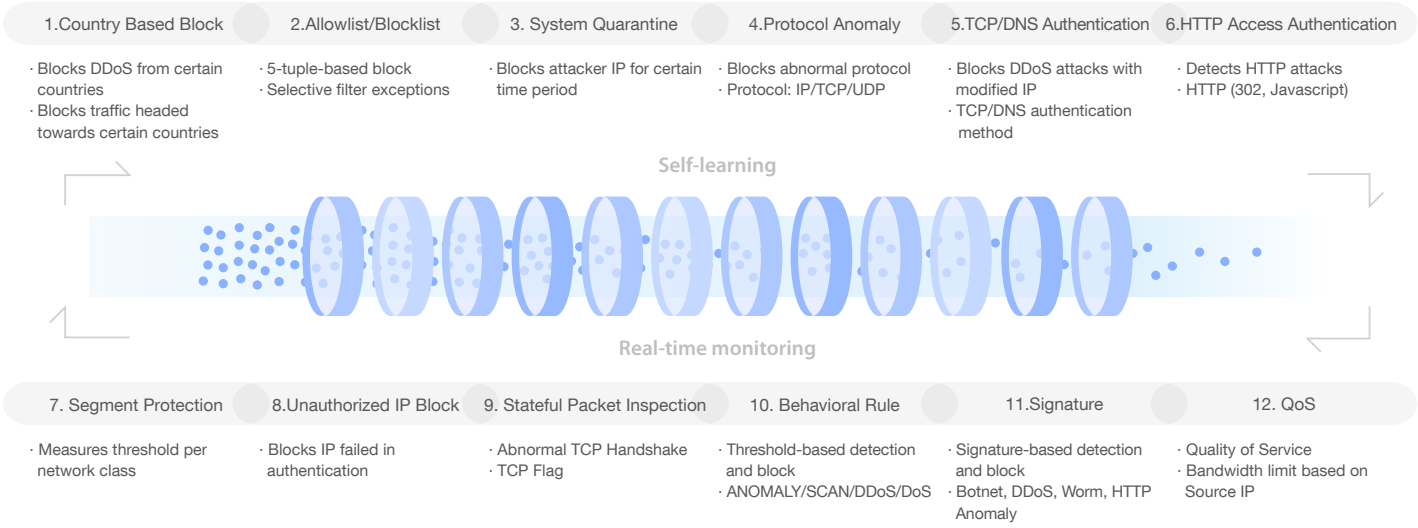
Advanced DDoS Attacks

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



12-Layered Filtering

AhnLab DPX mitigates and responds to DDoS attacks with 12-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
- Alert Notification (Email, SMS)
- Packet Capture / Auto Collection and Transmission of Packet / SNMP

Multi-Tenancy: Optimized Policy Per Protection Target
- Zone Settings per Protection Target
  - DPX 5000B - IPv4: 200, IPv6: 128
  - DPX 10000B - IPv4: 300, IPv6: 300
  - DPX 20000B - IPv4: 500, IPv6: 500
- Policy & admin, log transmission and optimized traffic learning (self-learn) per Zone

Various Logs: Enhanced Policy for Detection and Response
- Creates 40 Different Types of Logs - Identifies Traffic Status per Protection Target
- Detection Information and Report / Interoperation with Multiple Log Server, SIEM and SOAR

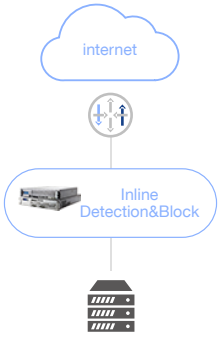
Complete Response to DDoS

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).

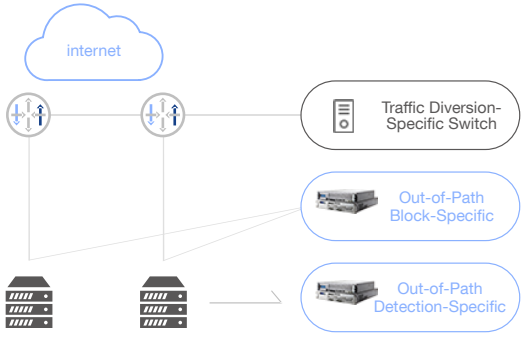
Category	Attack Type	Description	DPX Response Feature
Attack Method	DoS	An attack from a single client toward a single server (1:1)	· DoS Behavioral Rule · ACL-based Blocklist
	DDoS	· A simultaneous attack using bot and infecting multiple PCs with malware · An attack from multiple clients toward a single 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	· Behavioral Rule · ACL-based Blocklist
	APDoS	· A DDoS attack as a means for APT attack · Distracts admin with DDoS and attacks with APT · Also refers to DDoS attacks using multiple vectors	· AhnLab MDS: APT and ransomware solution nominated as 2021 Next-Gen World Class Product of Korea
	Ransom DDoS	· An extortion attack for monetary gain · Accompanies ostentatious DDoS attacks for threatening	
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
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 / 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 / Protocol Anomaly

Deployment & Configuration

AhnLab DPX can be deployed in two different methods. Inline allows easy deployment, and Out-of-Path allows response to DDoS by detecting and blocking separately.



[Inline]



[Out-of-Path]

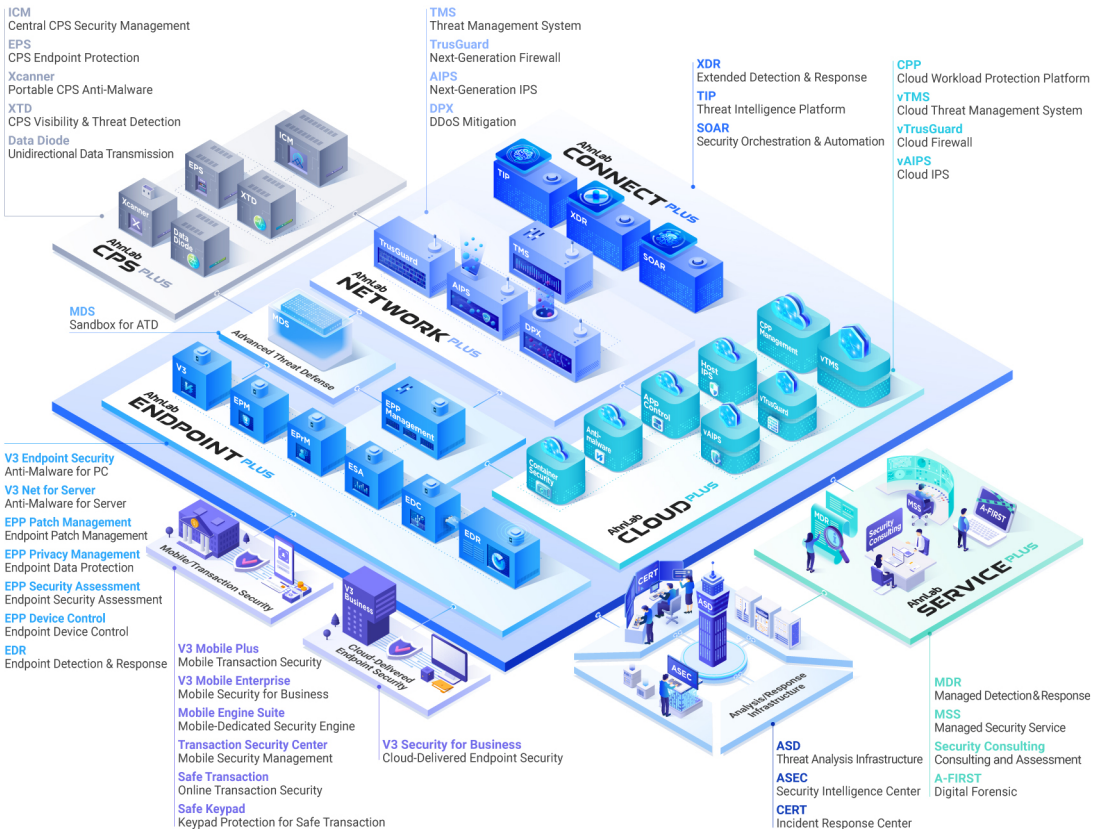
Category	Inline	Out-of-Path
# of Devices Required	1 (Detection & Response)	2 (Detector: Detection, Guard: Block)
Deployment Difficulty	Low	High
DDoS Response Speed	Very Fast	Fast
Client	Public Institution, Finance, School	ISP, Portal, IDC

Specifications

		AhnLab DPX 5000B	AhnLab DPX 10000B	AhnLab DPX 20000B
Throughput		10G	60G	200G
CPU		8Core	32Core	48Core
Memory		64GB	128GB	256GB
HDD		2TB	2TB	2TB
NIC	1GC	10 (Max 18, Including Mgmt)	2 (Max 34, Including Mgmt)	2 (Max 34, Including Mgmt)
	1GF	2 (Max 8)	0 (Max 16)	0 (Max 16)
	10GF	0 (Max 8)	4 (Max 16)	12 (Max 20)
	40GF	–	0 (Max 4)	0 (Max 4)
	100GF	–	–	0 (Max 4)
Power		550W, Redundant	800~900W, Redundant	800~900W, Redundant
Korean CC Certification		EAL4 (DDoS Response Equipment Security Requirement V1.0)		
HA		A-A/A-S HA support		
Installation		19 inches standard rack mounted		

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), 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