AhnLab NETWORK PLUS

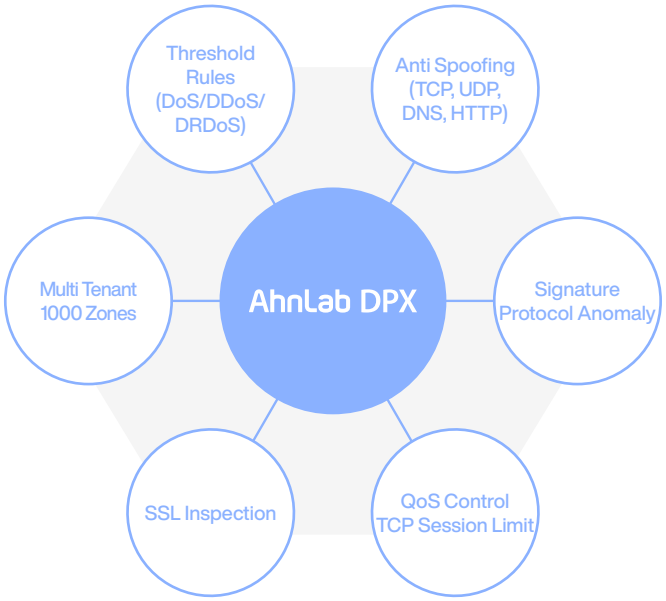
AhnLab DPX

High Performance DDoS Mitigation Solution

AhnLab DPX protects customers from DDoS attacks through specialized technology, proven experience, and deep expertise.

Overview

DDoS remains one of the oldest and most frequent types of cyberattack. Because DDoS attacks are relatively easy to launch, DDoS has evolved into various forms, making them difficult to block with a single detection method. AhnLab DPX is an industry-leading DDoS mitigation solution designed to address DDoS attacks. Built on our dedicated DDoS mitigation technology, AhnLab DPX delivers advanced traffic analysis and multiple detection techniques.



Advantages

Supports 10G/40G/100G NIC Inline/Out-of-Path Deployment	Supports multi-tenancy based on a maximum of 1000 zones
Supports QUIC and HTTPS Protocol Supports SSL Inspection and HTTP Analysis	Granular response to DDoS traffic with over 70 Threshold 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.

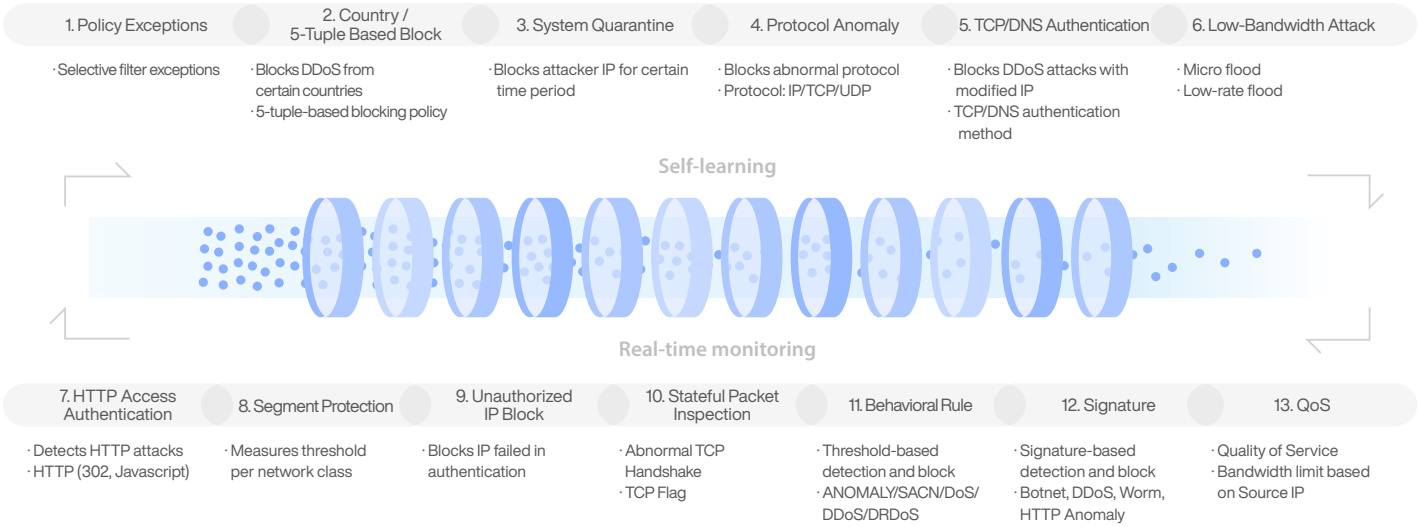
- Large-scale DDoS attacks using IoT devices
- Evolution in attack methods of DoS, DDoS, DRDoS
- Low-bandwidth attack using multiple spoofed source IPs
- Ransom DDoS attacks for money theft

Threatens business continuity

Online Shopping Mall E-commerce, Online Game Web Portal	Service stoppage and decrease in sales
Banks, Stock Firms Credit Card Companies, Insurance Companies	Transaction, inquiry, payment, trading, and other businesses become unavailable, losing customer's trust
Enterprise, Public Institution Homepage and Network	System overload, communication failure, business interruption

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, 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

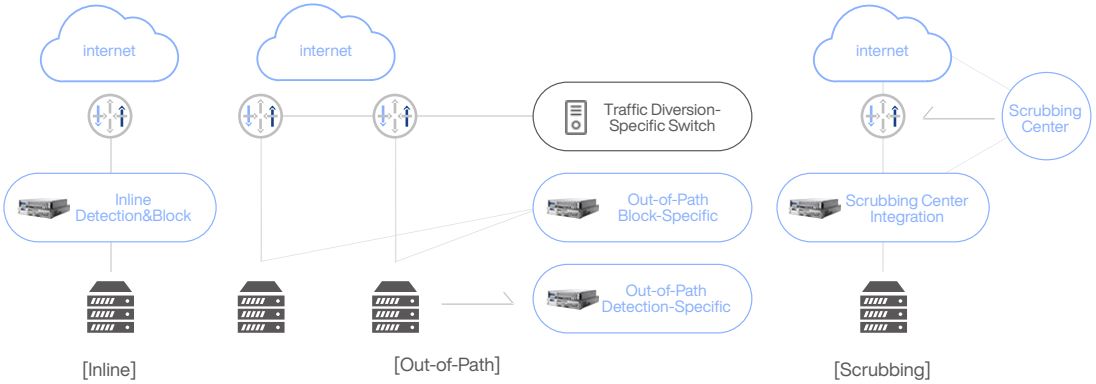
AhnLab DPX can prevent various types of DDoS attacks. Customers can experience an advanced response capabilities by interoperating the solution with AhnLab MDS(APT), AhnLab TMS(Threat Management), and AhnLab Sefinity AIR(SOAR).

Category	Attack Type	Description	Response Feature
Attack Method	DoS	An attack from a single client toward a single server(1:1)	· DoS Threshold Rule · ACL 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 Threshold Rule · Anti-Spoofing(TCP, HTTP) · System Quarantine · QoS Control
	DRDoS	· A UDP Attack using a reflector · Reported new cases of attacks with alternate protocols and ports	· DRDoS Threshold Rule
Volumetric DDoS	TCP Flooding	· Attacks with mixing TCP components · SYN, ACK, XMAS(ALL), NULL(Nothing), etc.	· Threshold Rule(TCP) · Anti-Spoofing(TCP) · 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.	· Threshold Rule(UDP) · Anti-Spoofing(UDP, DNS) · Segment Protection
	HTTP Flooding	· An attack using HTTP request · Different types of attack per HTTP Method(i.e., GET, POST)	· Threshold Rule(HTTP, HTTPS) · Anti-Spoofing(HTTP) · Protocol Anomaly
	Fragmentation Flooding	· An attack through fragmented IP packets · Induces load via packet recombination · Used as a method to bypass solution policy	· Threshold Rule(Fragmentation) · Signature
	DNS Flooding	· NXDOMAIN attack that drains DNS server resources	· Anti-Spoofing(DNS)
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, UDP, HTTP) · TCP Session Limit · Protocol Anomaly · Signature
	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	· Threshold Rule(Anomaly) · Protocol Anomaly · Signature

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

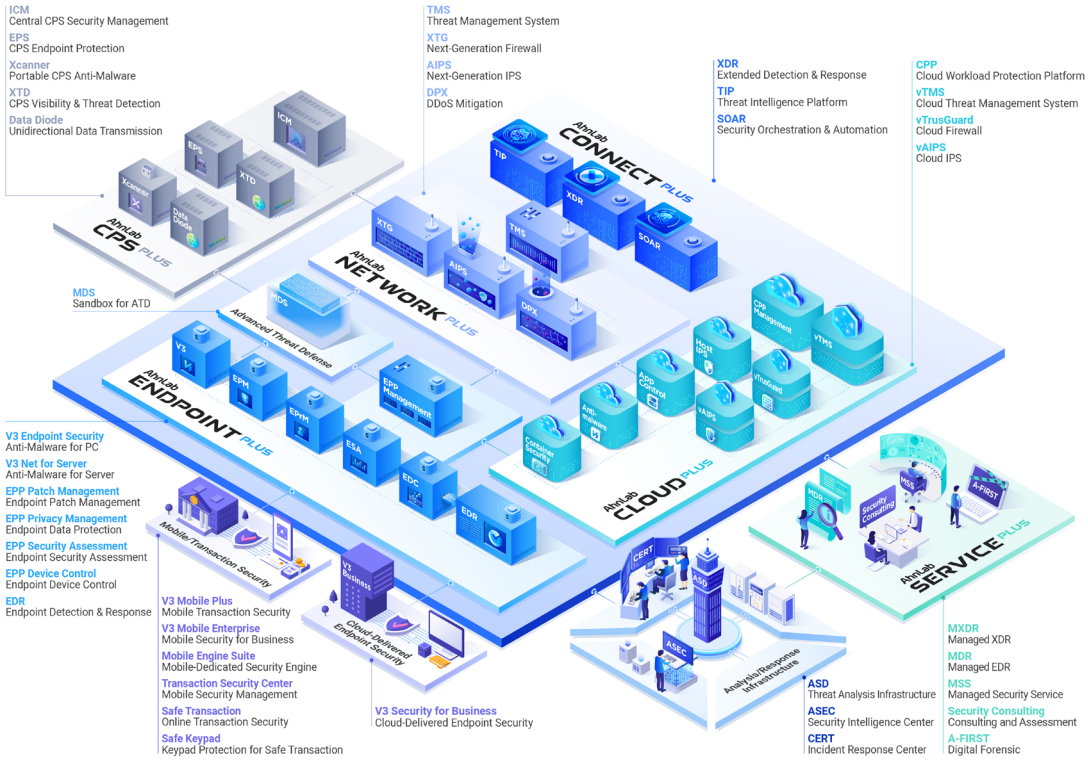
Specifications

		AhnLab DPX 5000C	AhnLab DPX 10000C	AhnLab DPX 20000C
CPU		8 Core	32 Core	64 Core
Memory		64GB/128GB	128GB/256GB	256GB/512GB
System Storage		SSD 512GB	SSD 512GB	SSD 512GB
Log storage		SSD 2TB	SSD 2TB	SSD 2TB
NIC	Slot	4	4	4
	1GC	8 (Max 32)	0 (Max 32)	0 (Max 32)
	1GF	2 (Max 16)	4 (Max 16)	8 (Max 16)
	10GF	0 (Max 4)	0 (Max 16)	0 (Max 16)
	40GF	–	0 (Max 4)	0 (Max 4)
	100GF	–	–	0 (Max 4)
Throughput (UDP/64byte)		10G	50G	100G
Throughput (UDP/MAX)		10G	80G	200G
Power		Redundant		

* 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 / global.sales@ahnlab.com

AhnLab