

# DPX17000-A10-H

## Overview

**DoS: Denial of Service**

**DDoS: Distributed Denial of Service**

DoS (Denial of Service) leverage various service requests to exhaust victims' system resources, causing the victim to deny service to its customers. DDoS (Distributed Denial of Service) grows rapidly with the rise of botnet, featuring with simple attack methods, great influence and difficulties in trace. Botnet consists of thousands of hijacked computers and provides bandwidth and hosts for DDoS attacks, it will forms a large attack scale and a significant amount of network flows, causing great harm to victims.

With the continuous improvement and development of DDoS attack technology, service providers like ISP, ICP, IDC and etc face increasing security and operation challenges. In order to ensure normal network and service operation, service providers must inspect and clean flows before DDoS attacks influence key services and applications. Meanwhile, service providers can make probe and cleaning of DDoS attack flows as a kind of value-added service and get better user satisfaction.

Traditional DDoS defense methods use devices based on network layer inspection like firewall, router and etc. But most DDoS attacks adopt with standard protocols during attack, traditional defense methods cannot correctly identify and protect. Meanwhile, firewall and router are not designed for DDoS attack defense. Therefore, it will suffer significant performance degradation and cannot work properly once this feature enables.

To solve these technical problems, DPtech releases professional Anti-DDoS Series products against DDoS attacks, which include anomalous flows inspection(Probe), anomalous flows cleaning (Guard) and anomalous flows cleaning service management platform.

DPtech Anti-DDoS Series are dedicated, appliance-based solutions deployed on hardware platforms. Leveraging industry-leading technologies such as Parallel Flow Filtering and Intelligent Flow Probing, these solutions can detect a wide range of DDoS threats in real time. They enable rapid filtering of malicious traffic, effectively protecting critical infrastructure such as WAN links, Internet Data Centers (IDCs), and other core network assets against large-scale DDoS attacks.

## Hardware Introduction

### ■ Host



DPX17000-A10-H

## Specifications

Hardware Specifications	DPX17000-A10-H
Product Form	Chassis
Max Hardware Accelerated 10GE SFP+ Slots	64
Hardware Accelerated 100GE QSFP28 / 40GE QSFP+ Slots	24
MCU Slots	2
Management Port	2
USB Ports	2
Console Port	1
Power Supply Slots	4
Fan Slots	4
In-built DDR4 Memory	256GB
Controller NVMe SSD for OS, Configuration and Log event storage	1.92TB
W×D×H	440mm*800mm*264mm
Form Factor	6RU
Weight (kg)	31.5KG
High Availability Configurations	Active-Active, Active-Passive, Clustering
<b>Power</b>	
Power Supply	AC 100 to 240 V (50/60 Hz), DC -40 to -60 V
Max Power Consumption	3200W
Redundant Power Supplies	N+1 or N+N or N+M, Hot swappable
<b>Environment</b>	
Operating Temperature	-10-60°C
Storage Temperature	-45-75°C
Humidity	15-95% non-condensing
Operating Altitude	Up to 3,000m
<b>System Performance</b>	<b>DPX17000-A10-H</b>
Max L4 Throughput	600Gbps
Max Compression Throughput	480Gbps

Hardware Specifications	DPX17000-A10-H
Max Concurrent Connections	200,000,000
Max L4 Connections per Second	10,000,000
NetFlow	20,000(400G-1T)
Max SSL TPS for RSA (2K keys)	800,000
Max ECC TPS (EC-P256)	600,000
Max SSL throughput (bulk encryption)	300Gbps
Compliance	
FCC 47 CFR Part 15, Subpart B, Class B, CE, ROHS EN 55032:2015/A11:2020 EN 55035:2017/A11:2020 EN IEC 61000-3-2:2019+A1:2021 EN 61000-3-3:2013+A1:2019+A2:2021 EN IEC 62368-1:2020+A11:2020	

## Feature Overview

### Carrier-class Products

Built upon a high-performance architecture platform independently developed by DPtech, it offers a maximum detection efficiency of 100W flows/s and a maximum T-class protection performance as a single device. Instant response within a second helps cut off abnormal traffic immediately

### Operation-level Management Platform

Using a self-service management platform, operators is capable of providing Safety protection value-added services for customers with anti-DDoS attack needs (such as Internet cafes, hotels, governments, shopping malls, etc.). After purchasing the services, tenants can open a dedicated account and log onto the DDoS Traffic Cleaning System for further processing based on their demands. Functions available include conducting attack traffic query, initiate/stop traffic cleaning, viewing cleaning reports and cleaning history, and bill query.

### Full Protection against Various DDoS Attacks

The innovative detection engine performs in-depth detection of and defense against traffic DDoS and application DDoS, taking effective precautions against mainstream DDoS attacks. Attackers send similar headers and payloads to ensure the effectiveness of attacks. To this end, fingerprinting helps cutting off a majority of popular attacks and makes necessary adjustments to signature policies to avoid new types of attacks in the network

### Two-way Protection and Near-Source Cleaning

Traditional traffic cleaning of DDoS attacks is aimed at fixed targets, focusing on cleaning inbound abnormal traffic. As the attack target of outbound DDoS attacks is uncertain, near-source cleaning is enabled to implement global cleaning, rather than protection based on specified IP addresses. In this way, two-way protection and defense of DDOS attacks is realized.

### Abnormal Traffic is Traceable

Apart from detection and cleaning of DDoS attacks, users need to perform in-depth analysis on the attack packets. Integrating a set of tools for packet traceability and automatic attack analysis, the Abnormal Traffic Cleaning System from DPtech supports analysis on packets captured before and after attacks as well as cleaned and dropped packets. Based on captured files, it is possible to trace the source IP of attacks and extract packet signatures, allowing administrators to establish security policies for targeted protection.

### Flexible Deployment in Complex Networks

A wide array of network features are supported to enable deployment in complex network environments such as BGP and MPLS VPN. In the Bypass mode, traffic traction is realized through using the BGP technology, and

traffic re-injection can be achieved by using technologies such as policy-go-together, VLAN, GRE and MPLS.

### Multi-Tenancy and Network Segmentation

Support multi-tenancy with full isolation at the device level to securely separate tenant traffic.

Support scalability up to 150 tenant/contexts through additional blade or module insertion as needed.

Support VRF-like functionality for traffic and routing domain separation.

### Traffic Model Self-learning

Fully redundant hardware architecture DPX17000 Series supports master control board 1+1 redundancy, switching board N+1 redundancy, fan module N+M redundancy, power supply module N+1 or N+N or N+M redundancy. It supports uninterrupted restart, hot fixes, separated data/control/monitoring planes and other technologies, ensuring 99.999% carrier-grade reliability. It supports BFD, OAM and other fast fault detection technologies, and provides a series of device-level and network-level fault detection methods.

### Centralized Management

DPX17000 product support the linkage with DPtech UMC, which fully integrates functional components such as log collectors, databases, log analysis, auditing, reporting, etc. It can achieve comprehensive network traffic analysis of the entire network, automatically associate security events, help administrators understand the overall network situation in real time, identify potential security risks, and ensure network security.

### Product Architecture

DPX17000 Series Supports localization programming, dual-controller architecture, template configuration, the management port supports joining a VRF (Virtual Routing and Forwarding) for routing isolation.

## Feature List

Item	Description
<b>Flexible Deployment</b>	Support Bypass and Online Deployments
<b>Hardware Platform</b>	Support high-performance, highly scalability, purpose-built appliance designed next-generation hardware platform for DDoS protection. Support integrated functionalities for Layer 3-Layer 4 DDoS Protection and DNS DDoS Protection. Support modular system architecture to enable future expansion and scalability. Support dual system controllers/engines for control plane level redundancy and high availability.
<b>Automation &amp; Programmability</b>	Support programmability for automation, native integration, and orchestration. Support RESTful APIs for automated onboarding and configuration of Layer 2-3 network objects such as Routes, VLANs, Dynamic routing configurations etc.
<b>Configuration Management</b>	Support template/script-driven configurations to simplify complex deployment scenarios, accelerate onboarding of applications and reduce the risk of misconfiguration.
<b>Routing Protocols</b>	Support routing protocols include RIP, OSPF, ISIS, BGP and MPLS.
<b>Network Features</b>	Support dynamic and static BGP traffic traction. Supported re-injection methods include policy-go-together, MPLS VPN, GRE VPN and layer-2 transparent transmission mode.
<b>Detection Methods</b>	Available detection methods include NetFlow/NetStream/SFlow protocol-based detection (DFI) Deep Packet Inspection (DPI)
<b>Protection against Malformed Attacks</b>	Capable of preventing malformed packet attacks, especially those against protocol vulnerabilities, such as Land, Smurf, Fraggle, Tear Drop, and Winnuke.

Item	Description
<b>Flood-Based Attacks</b>	Layer 2 / Layer 3 Floods: ARP Flood, ICMP Flood, IGMP Flood, IP Fragment Flood Layer 4 Floods: UDP Flood, TCP SYN Flood, TCP RST Flood, TCP ACK Flood Advanced Floods: Christmas Tree Flood Attack, Single Endpoint Flood, Smurf Attack, Ping of Death Reflection/Amplification Floods: NTP Flood, DNS Reflection Flood, SSDP Amplification
<b>Malformed Packet and Protocol Anomaly Attacks</b>	LAND Attack, Large ICMP Frame, Bad ICMP/IGMP Frame, IP Unknown Protocol Bad IP TTL Value, Bad UDP Checksum, Bad TCP Checksum, Bad TCP Flags, TCP Window Size Abuse TCP Half Open Connection, Overlapping Fragment Attack, Invalid Header Length Single Endpoint Sweep, Port Scanning Detection, Protocol Tunneling Detection
<b>Protocol Abuse and IP Stack Exploits</b>	Protocol abuse, Bad IP Version, IP Error Checksum, IP Option Illegal Length, IP Header Length Inconsistency, IP Fragment Overlap / Overrun, Bad IPv6 Version, Bad IPv6 Hop Count, Bad IPv6 Address, IPv6 Extension Header Abuse, Unknown or Reserved Protocol Numbers, Abnormal Packet Reassembly Behavior
<b>DNS-Based Attacks</b>	DNS AAAA Query Flood, DNS Malformed Packets, DNS NXDOMAIN Query Flood DNS Response Flood, NS Record Oversize, ANY Query Flood Slow DNS Attack, DNS Tunneling Detection, DNS Water Torture Attack Recursive Query Exploits, DNS Amplification with Spoofed Source
<b>Attack Traceback</b>	Integrating a set of tools for packet traceability, it supports analysis on packets captured before and after attacks as well as cleaned and dropped packets. Based on captured files, it is possible to trace the source IP of attacks and extract packet signatures before sending them to cleaning devices for filtering.
<b>System Monitoring</b>	Monitor device performance, traffic information in interfaces, CPU and memory utilization, as well as online status. Support online troubleshooting and traffic analysis tools, enabling users to capture snapshots or on-device packet data and upload configurations to the DPtech's web-based diagnostic platform for health and vulnerability assessment. Support role-based access control (RBAC) to configure and manage user privileges and permissions with granularity.
<b>Logs and Reports</b>	An independent log server is provided, on which regular automatic backups can be performed. With its built-in hundreds of reports, functions such as graphic inquiry, audit, statistics and retrieval of various network behavior logs on the intranet are enabled to facilitate the management in understanding and controlling the network.
<b>Device Management</b>	A user friendly graphical management interface, which supports Web GUI, SSH and serial console, web service APIs. Centralized management through UMC network management is also made possible. Support multi-user permission isolation and is scalable to at least 30 administrator users and allow administrators to add and modify signatures.
<b>Protection from DNS-based DDoS and Flooding Attacks</b>	<p><b>DNS Security and Protection</b></p> Support Domain Name System (DNS) security features, including protection against DNS-based DDoS and related threats. Support DNS Flood Protection, including detection of statistical anomalies in DNS traffic and mitigation using the following mechanisms: <ul style="list-style-type: none"> <li>✧ DNS query rate limiting</li> <li>✧ Protection against DNS domain attacks</li> <li>✧ DNS TCP active authentication mechanism</li> <li>✧ DNS pattern matching using regular expressions</li> <li>✧ Protection from DNS cache poisoning</li> </ul> <p><b>Network-wide Threat Mitigation</b></p> Support IPv6 compliance across DNS and network defense features. Support connection rate limiting per source IP and dynamic blacklisting of IPs violating

Item	Description
	<p>thresholds.</p> <p>Support both inbound and outbound threat protection mechanisms.</p> <p>Support static and dynamic IP whitelisting and blacklisting, including automatic detection, dynamic blacklisting and blocking of offending sources.</p> <p><b>Logging and Visibility</b></p> <p>Support SIEM integration via Syslog, with high-speed logging to enable visibility into real-time security status events, incident tracking, logging and reporting.</p>
<b>Interactions with Third- party Devices</b>	<p>Work with traffic detection devices from DPtech or any third party to receive information on detection devices, and initiate routing traction and re-injection by the traffic cleaning device.</p>
<b>High Availability</b>	<p>Support Redundant heartbeat interfaces</p> <p>Support both Active-Active and Active-Passive modes, enabling seamless takeover in case of device failure when deployed in dual configuration.</p> <p>Support transparent failover between devices, including session mirroring, connection mirroring, and heartbeat monitoring.</p> <p>Support generation of logs for audit and compliance purposes during HA operations.</p> <p>Support Standalone session synchronization</p> <p>Support HA reserved management interface</p> <p>Support Active-Standby HA clustering for uninterrupted service continuity.</p> <p>Support failover deployment and configuration synchronization between HA systems to ensure that any configuration updates are automatically synchronized across all HA systems.</p> <p>Implement redundant components to allow configuration, maintenance, and backup procedures without service interruption.</p> <p>Support device failure detection and link failure detection for rapid recovery and fault tolerance.</p>
<b>Security Features</b>	<p>Support L3 Routed deployment mode</p> <p>Support security policy configuration without affecting network traffic.</p> <p>Support creating dynamic signatures;</p> <p>Support DDOS security policy building feature</p> <p>Support automatic creation of dynamic signatures to enable faster and more accurate identification and blocking of evasive threats.</p> <p>Support automatic DDoS security policy generation through time-based learning, utilizing detection methods such as traffic flow analysis, traffic threshold profiling, and DDoS signature recognition.</p> <p>Learning is performed over a configurable time period without impacting network traffic, ensuring non-intrusive behavior during policy building.</p> <p>Support at least 100 DDoS attack vectors/signatures and comprehensive L3-L4 metrics to provide in-depth, real-time visibility of DDoS attacks, enabling more effective protection and response.</p> <p>Support advanced detection mechanism.</p> <p>Support differentiating and isolating potentially malicious traffic from legitimate traffic.</p> <p>Support identifying DDoS flood/scanning attack threats at L3-L4 based on Packet Per Second.</p> <p>Support protection against SSL/TLS protocol attacks and application-layer low-and-slow attacks.</p> <p>Support fully automatic DDoS threshold mode protection as settings for DoS signature to adjust typical DoS vector levels over time, and automatically adjust the detection sensitivity and rate limiting for each vector to ensure adaptive and accurate mitigation.</p> <p>Support configurable DDoS defense thresholds based on Packets Per Second (PPS) and Requests Per Second (RPS) to enable accurate detection and mitigation of volumetric</p>

Item	Description
	<p>and application-layer attacks.</p> <p>Support advanced detection mechanisms for monitoring application and network performance, protocol anomalies, and identifying application anomalies through behavior analysis of specific DDoS attacks. Provides protection capabilities including dynamic filtering, IP source tracking, dynamic signature generation, and in-depth policy control.</p> <p>Support automatic discovery and fingerprinting of new and unusual traffic patterns without human intervention, effectively distinguishing and isolating malicious traffic from legitimate flows. Mitigation signatures are automatically generated, deployed, and continuously analyzed to maintain DDoS protection effectiveness.</p> <p>Support detection and mitigation of unknown network-level DDoS attacks and network behavior-based DoS mitigation techniques to prevent zero-day DoS/DDoS flood attacks.</p> <p>Support comprehensive network-wide protection against DDoS and flooding attacks.</p> <p>Support automatic DDoS detection capabilities by continuously calculating dynamic rate limit thresholds based on real-time traffic analysis. When traffic volume reaches or exceeds these thresholds, system automatically initiates mitigation measures to effectively block or limit DDoS attack traffic, ensuring network stability and service availability without manual intervention.</p> <p>Support continuously adjusting, updating, and improving the accuracy of DDoS mitigation strategies during ongoing, evolving, or changing DDoS attacks.</p> <p>Support automatically detecting, logging, and restricting the rate of specific IP addresses based on custom criteria.</p> <p>Support minimizing security false positives by continuously tuning and updating DDoS mitigation policies in real time. It enables an automated DDoS protection cycle that dynamically refines detection precision and mitigation effectiveness as attacks continue/evolve/change.</p> <p>Support full inspection of Layer 3 and Layer 4 traffic to detect DDoS threats, including flood and sweep attacks based on source/destination IP, UDP, DNS, TCP (SYN, ACK, RST, FIN), and SIP protocols. Detection is performed using sub-second attack detection, protocol analysis, source tracking, network behavior analysis, and dynamic filtering prior to forwarding traffic to internal or external networks.</p> <p>Support using a SYN authentication mechanism to protect against any type of SYN flood attack.</p> <p>Support automatically discarding high-volume UDP, DNS queries, NXDOMAIN flood attacks, and malformed packets via protocol validation in the software, while effectively mitigating various DNS attacks with built-in DNS security capabilities.</p> <p>Support detecting statistical anomalies in DNS traffic and mitigating DNS floods using various mechanisms.</p> <p>Support profiling of web applications by automatically differentiating between good and bad traffic during the learning phase, ensuring that only good traffic is used to build the profile and bad traffic is excluded from learning.</p> <p>Support actions on attack detection including dropping requests/responses and blocking TCP sessions or IPs.</p> <p>Support SIEM integration via Syslog with high-speed logging for incident and status events visibility and logging&amp;reporting.</p> <p>Support Bad/DDoS Actor Detection for non-error, non-sweep/flood packets with automatic detection, logging, and rate-limiting of specific IP addresses identified as the likely source based on customizable criteria.</p> <p>Support SYN DDoS Protection using SYN authentication to defend against any form of SYN-based flood attacks.</p> <p>Support Comprehensive DNS Protection with protocol validation in software, including:</p> <ul style="list-style-type: none"> <li>◇ Auto-dropping of malformed/high-volume DNS query, UDP, NXDOMAIN packets.</li> </ul>

Item	Description
	<ul style="list-style-type: none"> <li>◇ Mitigation of Phantom Domain, NXDomain, Random Subdomain, Lock-Up Domain, Amplification, DNS Tunneling, Malformed Packet, and DNS Cache Poisoning attacks.</li> <li>◇ Detection of statistical anomalies in DNS traffic and mitigation through DNS query limits, domain-level protection, TCP active authentication, regular expressions, and DNS record type ACLs.</li> </ul> <p>Support Stateful inspection of all client-to-server and server-to-client traffic with threat mitigation based on security and application parameters before forwarding them on to the server.</p> <p>Support Automatic Thresholding of DoS vector-based traffic:</p> <ul style="list-style-type: none"> <li>◇ Dynamic connection limits and blacklisting per source IP exceeding thresholds.</li> <li>◇ Inbound and outbound threat protection.</li> </ul> <p>Support IP Whitelisting/Blacklisting, with dynamic blacklisting of offending sources.</p> <p>Support SSL Visibility for detection and mitigation at the network and session layers.</p> <p>Support integrated Geo-Location database with default IPv4 data coverage for accurate load balancing by continent, country, and state, based on available IP address data.</p> <p>Support IP Reputation Database with:</p> <ul style="list-style-type: none"> <li>◇ Periodic updates on IPs used for Anonymous Proxies, TOR, etc.</li> <li>◇ Integrated defense using the reputation list to get the insight and detail information about the most threatening IP addresses to block risky inbound/outbound connections.</li> </ul> <p>Support Signature Management, allowing administrators to add and modify attack detection signatures.</p> <p>Support Actionable Responses to detected attacks or unauthorized activity, including:</p> <ul style="list-style-type: none"> <li>◇ Dropping of requests and responses.</li> <li>◇ Blocking TCP sessions and IP addresses.</li> </ul> <p>Support mitigating parameter-related threats in servers and applications.</p> <p>Support GEO-Location database and regular updates of IP address reputation information.</p> <p>Support discarding requests and responses and blocking drawing operations (or other similar actions) when detecting attacks or any other unauthorized activities.</p> <p>Support analysis of performance and configuration for web applications.</p> <p>Support IPv4/IPv6 DNS Protection</p> <p>Supports detecting statistical anomalies in DNS traffic and mitigating them using various mechanisms.</p>

## Hardware Specifications

Hardware Specifications/Model	DPX17000-A10-H
Maximum Interfaces	Maximum 24*100GE/40GE + 64*10GE or 32*100GE/40GE
Maximum Power Consumption	3200W, redundant hot-swappable power supply
Management Interfaces	1 Console port, 2 MGT port, 2 USB port (on one MPU)
Power Supply	AC 100 to 240 V (50/60 Hz), DC -40 to -60 V
Height	6U
Dimension (W×D×H)	440 × 800 × 264 mm

## Hardware Order Information

Hardware Description	Model
Host	DPX17000-A10-H
MCU Unit	H10-MPU-G
Power Unit	PSU-AC800/ PSU-DC800
Service module	Guard3000-Blade-17E
Service module	Probe3000-Blade-HG2
100G Interface Unit(16*10GE(SFP+)+6*100GE(QSFP28)) * 100G QSFP28 Optical port also supports 40G QSFP+ SFP Module	H10-16XGS4CQ-G
Fan Unit	H10-FAN
NVMe SSD	SEC-SSD
Memory	DDR4 MEM

## Transceivers Order Information

Transceivers Description	Model
1000BASE-SX SFP Transceiver, Multi-Mode (850nm, 550m, LC)	SFP-G-SX-MM850
1000BASE-LX SFP Transceiver, Single Mode (1310nm, 10km, LC)	SFP-G-LX15-SM1310
1000BASE-LH40 SFP Transceiver, Single Mode (1310nm, 40km, LC)	SFP-G-LX40-SM1310
SFP+ 10-GigaBit Transceiver, Multi-mode,(850nm,0.3km,LC)	SFPP-SX-MM850
SFP+ 10-GigaBit Transceiver, Single Mode,(1310nm,10km,LC)	SFPP-LX10-SM1310
QSFP+ 40-GigaBit Transceiver, Multi-mode,(850nm,0.15km,MPO)	QSFP-SX-MM850
QSFP+ 40-GigaBit Transceiver, Single Mode,(1310nm,10km,MPO)	QSFP-LX10-SM1310-MPO
QSFP28 100-GigaBit Transceiver, Multi-mode ,(850nm,0.15km,MPO12)	QSFP28-SX-MM850
QSFP28 100-GigaBit Transceiver, Single Mode, (1310nm,10km,LC)	QSFP28-LX10-SM1310

### Contact Us

Hangzhou DPtech Technologies Co., Ltd.

<http://www.dptechnology.net>

6F, Zhongcai Tower, 68 Tonghe Rd, Binjiang District, Hangzhou 310051, Zhejiang Province, P.R.China

Tel: +86 0571 28280909

Fax: +86 0571 28280900

Technical Support Email: [support@dptechnology.net](mailto:support@dptechnology.net), Technical Support Hotline: 400-6100-598

Pre-sales Email: [market@dptechnology.net](mailto:market@dptechnology.net)

Copyright©2023 Hangzhou DPtech Technologies Co., Ltd. All rights reserved.

Statement: DPtech attempts to provide the accurate information for users, but they cannot take any responsibility for the technical error or print mistake, DPtech has all rights to modify the document without any notify or information.