DPtech Anti-DDoS System

Overview

Common types of DDoS attack, one of the most popular attacks by hackers, include traffic DDoS attacks and application DDoS attacks, featuring low costs, easy implementation, difficulty in behavior detection and extensive outreach. The Anti-DDoS System from DPtech is a professional protection tool against DDoS attacks, consisting of the following: Probe3000 for abnormal traffic detection, Guard3000 for abnormal traffic cleaning, and a management platform of abnormal traffic cleaning. By detecting all sorts of DDoS attacks in the network and timely and quickly filtering attack traffic, it provides a maximum of T-class anti-DDoS capabilities. In addition, the DPtech Anti-DDoS System provides users with security visualization services to help them intuitively understand their network security status and eliminate potential risks in a timely manner.

Product Features

- **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 playloads 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.

- **Traffic Model Self-learning**

  Fully redundant hardware architecture DPX17000 Series supports master control board 1+1 redundancy, switching board N+1 redundancy, fan module 1+1 redundancy, power supply module 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.

Product Series


Guard3000-GA


Guard3000-GE-X


Guard3000-TS-A


Guard3000-TM-X


Guard3000-TA-X


Probe3000-GE


Probe3000-TS


Guard3000-Blade-S


Guard3000-Blade-A


Guard3000-Blade-EI


Guard3000-Blade-EI


Probe3000-Blade-AI

Function Descriptions

Product Model	Function Descriptions
Flexible Deployment	Support Bypass and Online Deployments

Routing Protocols	Supported routing protocols include RIP, OSPF, ISIS, BGP and MPLS.
Network Features	It supports dynamic and static BGP traffic traction.Supported re-injection methods include policy-go-together, MPLS VPN, GRE VPN and layer-2 transparent transmission mode.
Detection Methods	Available detection methods include NetFlow/NetStream/SFlow protocol-based detection (DFI)Deep Packet Inspection (DPI)
Basic Protection	It supports multiple methods for anti-DDoS attacks, including SYN/ACK Flood, ICMP Flood, UDP Flood, DNS Query Flood, Http Flood, Https Flood, CC, Connections Flood and other common DDoS attack methods under the IPv4/IPv6 dual stack protocol.
Protection against Malformed Attacks	It is capable of preventing malformed packet attacks, especially those against protocol vulnerabilities, such as Land, Smurf, Fraggle, Tear Drop, and Winnuke.
attack traceback	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.
System Monitoring	It can monitor device performance, traffic information in interfaces, CPU and memory utilization, as well as online status.
Logs and Reports	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.
Device Management	A user friendly graphical management interface, which supports Web GUI, SSH and serial console. Centralized management through UMC network management is also made possible.
Interactions with Third-party Devices	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.

* These specifications apply only to DPtech products available on the international market.

Hangzhou DPtech Technologies Co., Ltd.
Address：6th Floor, Zhongcai Building, No. 68 Tonghe Road, Binjiang District, Hangzhou City, Zhejiang Province
Postcode：310051
Official Website：www.dptech.com
Service Hotline：400-6100-598