Huawei AntiDDoS8000 DDoS Protection System

Terabit-level Capacity, Second-level Response, Precise Protection, Value-added Operation

Solution Highlights

- Terabit-level anti-DDoS: 1.44 Tbps protection performance, second-level attack response.
- Precise anti-DDoS: 60+ traffic models, defense against 100+ types of DDoS attacks.
- Value-added operation: 100,000 tenants, differentiated operation.

Solution Overview

As the Internet and IoT thrive, DDoS attacks are developing new characteristics:

- Attacks increase in frequency and traffic volume, and the peak attack traffic is up to 600 Gbps in 2015.
- Reflection amplification attacks spread across the world, congesting links.
- Low-rate application-layer attacks target precisely at service systems like e-finance or gaming.

Reflection amplification and low-rate application-layer attacks are gaining momentum, and layered defense becomes the first choice in anti-DDoS. Huawei AntiDDoS8000 employs big data analysis to conduct modeling for 60+ types of traffic, offering Terabit-level protection, second-level response, and comprehensive defense against 100+ types of attacks. It works with Huawei cloud cleaning center to deliver layered cleaning, providing full-fledged protection that covers network link bandwidths and online services.

AntiDDoS8030

AntiDDoS8080

AntiDDoS8160

Solution Function

Defense against high-volume DDoS attacks

- Multi-core distributed architecture and big data-based intelligent protection engine to offer Terabit-level protection performance.
- Second-level attack response to rapidly block attack traffic.

Defense against application-layer DDoS attacks

- Collection of all traffic, Layer 3~7 per-packet analysis, and modeling for 60+ types of network traffic to provide the most precise and comprehensive attack detection.
- All-round reputation system of local session behavior reputation, location reputation, and Botnet IP reputation to precisely defend against application-layer DDoS attacks launched from Botnets, reducing false positives and improving user experiences.
- Comprehensive defense against 100+ types of attacks to protect key service systems, such as Web, DNS, DHCP, and VoIP.

Anti-DDoS operation

- Tenant-specific automatic and manual defense policies for comprehensive protection.
- Tenant-specific report statistics and report sending via email to simplify management.
- Differentiated operation for 100,000 tenants.

Dual-stack (IPv4/IPv6) DDoS attack defense

- Defense against dual-stack (IPv4/IPv6) DDoS attacks.

On-premise+Cloud layered anti-DDoS

- The on-premise device is online in real time to protect user services.
- When a link is congested, the on-premise device can automatically send cloud signals to start cloud cleaning and protect user links.
- 2Tbps+ cloud mitigation capacity. 10+ cloud scrubbing center with global scheduling. Minute-level defense response.

LEADING NEW ICT,
BUILDING A BETTER CONNECTED WORLD

HUAWEI

Huawei AntiDDoS8000 DDoS Protection System

Terabit-level Capacity, Second-level Response, Precise Protection, Value-added Operation

DDoS Defense Specifications

Defense against protocol abuse attacks

Defense against Land, Fraggle, Smurf, WinNuke, Ping of Death, Teardrop, and TCP error flag attacks

Defense against scanning and sniffing attacks

Defense against address and port scanning attacks, and attacks using Tracert packets and IP options, such as IP source route, timestamp, and record route

Defense against network-type attacks

Defense against SYN flood, SYN-ACK flood, ACK flood, FIN flood, RST flood, TCP fragment flood, UDP flood, UDP fragment flood, IP flood, ICMP flood, TCP connection flood, sockstress, TCP retransmission, and TCP empty connection attacks

Defense against UDP-based reflection amplification attacks

Defense against NTP, DNS, SSDP, Chargen, TFTP, SNMP, NetBIOS, QOTD, Quake Network Protocol, Portmapper, Microsoft SQL Resolution Service, RIPv1, and Steam Protocol reflection amplification attacks

Attack signature database

RUDY, slowhttptest, slowloris, LOIC, AnonCannon, RefRef, ApacheKill, and ApacheBench attack signature databases; automatic weekly update of these signature databases

Web application protection

Defense against HTTP GET flood, HTTP POST flood, HTTP slow header, HTTP slow post, HTTPS flood, SSL DoS/DDoS, WordPress reflection amplification, RUDY, and LOIC attacks; packet validity check

DNS application protection

Defense against DNS query flood, DNS reply flood, and DNS cache poisoning attacks; source limit

SIP application protection

Defense against SIP flood/SIP methods flood attacks, including Register, Deregistration, Authentication, and Call flood attacks; source limit

Filter

IP, TCP, UDP, ICMP, DNS, SIP, and HTTP packet filters

Location-based filtering

Traffic block or limit based on the source IP address location

IP reputation

Tracking of most active 5 million zombies and automatic daily update of the IP reputation database to rapidly block attacks; local access IP reputation learning to create dynamic IP reputation based on local service sessions, rapidly forward service access traffic, and enhance user experience

Management and Report

Management functions

Account management and permission allocation; defense policy configuration and report display based on Zones (up to 100,000 Zones, namely tenants); device performance monitoring; source tracing and fingerprint extraction through packet capture; email, short message, and audio alarms; log dumping; dynamic baseline learning

Report functions

Comparison of traffic before and after cleaning; top N traffic statistics; application-layer traffic comparison and distribution; protocol distribution; traffic statistics based on the source location; attack event details; top N attack events (by duration or number of packets); distribution of attacks by category; attack traffic trend; DNS resolution success ratio; application-layer top N traffic statistics (by source IP address, HTTP URI, HTTP HOST, and domain name); download of reports in HTML/PDF/Excel format; report push via email; periodical generation of daily, weekly, monthly, and yearly reports

Traffic Diversion and Injection

Traffic diversion

Supports manual, and PBR or BGP based automatic traffic diversion

Traffic injection

Supports static route injection, MPLS VPN injection, MPLS LSP injection, GRE tunnel injection, Layer 2 injection, PBR based injection, etc

Hardware Specifications

Model	AntiDDoS8030	AntiDDoS8080	AntiDDoS8160
Throughput	Up to 120 Gbps	Up to 720 Gbps	Up to 1440 Gbps
Throughput/slot	Up to 80 Gbps	Up to 160 Gbps	Up to 160 Gbps
Mitigation rate/slot	Up to 60 Mpps	Up to 60 Mpps	Up to 60 Mpps
Latency	80 μs	80 μs	80 μs
Expansion slot	3	8	16
Expansion LPU	FW-LPUF-120, 2 sub-slots	FW-LPUF-120, 2 sub-slots FW-LPUF-240, 2 sub-slots	FW-LPUF-120, 2 sub-slots FW-LPUF-240, 2 sub-slots
Expansion interfaces	24 × GE (SFP); 5 × 10GE (SFP+); 6 × 10GE (SFP+); 12 × 10GE (SFP+); 1 × 40GE (CFP); 1 × 100GE (CFP)		
Height × Width × Depth	DC: 175mm × 442mm × 650mm (4U) AC: 220mm × 442mm × 650mm (5U)	620mm × 442mm × 650mm (14U)	1420mm × 442mm × 650mm (32U)
Weight	DC chassis: 15kg (empty), 30.7 kg (full) AC chassis: 25kg (empty), 40.7 kg (full)	43.2 kg (empty), 112.9 kg (full)	94.4 kg (empty), 233.9 kg (full)
Power supply	DC: -72 V to -38 V AC: 90 V to 264 V; 50/60 Hz	DC: -72 V to -38 V AC: 90 V to 264 V; 50/60 Hz	DC: -72 V to -38 V AC: 90 V to 264 V; 50/60 Hz
Power redundancy	DC: Double hot-swappable power modules AC: Double hot-swappable power modules	DC: 4 hot-swappable PEM modules AC: 4 PEM modules+1 external AC power chassis	DC: 8 hot-swappable PEM modules AC: 8 PEM modules+2 external AC power chassises
Temperature	Operating: 0°C to 45°C (long-term), -5°C to 50°C (short-term); Storage: -40°C to 70°C		
Humidity	Operating: 5% RH to 85% RH, non-condensing (long-term), 5% RH to 95% RH, non-condensing (short-term); Storage: 0% RH to 95% RH		
Safety Certifications	Electro Magnetic Compatibility (EMC) certification; CB, Rohs, FCC, MET, C-tick, and VCCI certification		

About This Publication

This publication is for reference only and does not constitute any commitments or guarantees. All trademarks, pictures, logos, and brands mentioned in this document are the property of Huawei Technologies Co., Ltd. or a third party.

e.huawei.com