AntiDDoS8000 Series

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

AntiDDoS8000 series

Overview

With the IT and network evolution, the Distributed Denial of Service (DDoS) attack has already broken away from original hacker behaviors. Instead, it forms an integral dark industry chain with overwhelming damages.

At present, a single DDoS attack consumes more than 100 Gbit/s bandwidth, ten times of that in 2007. DDoS attacks have increased by 20 times and over 30,000,000 zombie hosts flood the network. Moreover, attack tools become intelligent and attack behaviors become hidden and emulational. Especially, those attacks upon IDC applications are rampant, disabling the current defense measures of customers.

Designed for carriers, large enterprises, data centers, and large ICP service providers (including Web portals, game service providers, online videos, DNS service providers, and CDN services), Huawei anti-DDoS solution enhances the defense against application-layer attacks and the attacks in IPv6-IPv4 composite networking. This fully ensures network security and service continuity.

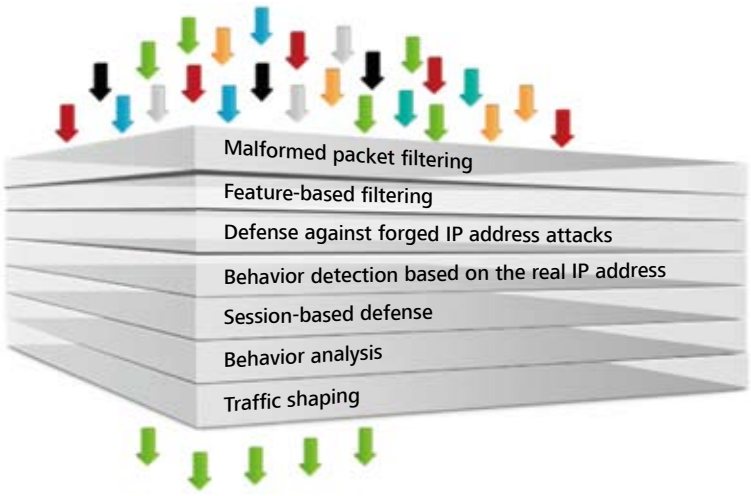
Highlights

Efficient and speedy: 200 Gbit/s defense performance and response within seconds

- Distributed architecture as well as a maximum of 10 times scalability, providing 200 Gbit/s performance.
- Self-learning of the service model and per-packet detect technology. Once a traffic or packet anomaly is found, the defense policy is automatically triggered. The defense latency is within two seconds.

Accurate and comprehensive: defense against hundreds of attacks and IPv6 defense

- Particular seven-layer filtering technology to defend against over 100 DDoS attacks, with the industry-leading defense types.
- Defense against over 200 zombies, Trojan horses, and worms, protecting users from hackers.
- IPv4/IPv6, as the first to support IPv6 attack defense.
- Terminal identification technology, accurately identifying illegitimate clients and ensuring zero false positive.



Value-added operation: protection for tens of thousands of leasers and diverse self-services

- Self-configuration of defense policies and generation of independent security reports, providing visibility into defense effects.
- Self-extraction of attack fingerprints, implementing emergency defense and effectively defending against zero-day attacks.

Specifications

Model	AntiDDoS8030	AntiDDoS8080	AntiDDoS8160
Flood attack defense performance	30 Mpps (15Mpps/SPU)	75 Mpps (15Mpps/SPU)	150 Mpps (15Mpps/SPU)
Detecting/Cleaning performance	40 Gbit/s (20 Gbit/s per SPU)	100 Gbit/s (20 Gbit/s per SPU)	200 Gbit/s (20 Gbit/s per SPU)
Defense start latency	≤ 2 seconds	≤ 2 seconds	≤ 2 seconds
Expansion slot	3	8	16
Expansion slot	1 × 10GE (XFP), 2 × 10GE (XFP), and 1 × 10G POS (XFP) 12 × 1GE (SFP) and 20 × 1GE (SFP)		
Dimensions (H × W × D)	175 × 442 × 650 (DC) 220 × 442 × 650 (AC)	620 × 442 × 650 (DC) 709 × 442 × 650 (AC)	1420 × 442 × 650 (DC) 1598 × 442 × 650 (AC)
Maximum power consumption	1330 W (DC) 1368 W (AC)	3038 W (DC) 3231 W (AC)	5824 W (DC) 6195 W (AC)
IPv4 defense types			
Anomaly filtering	Blacklist, HTTP field-based filtering, TCP/UDP/Other protocol load feature-based filtering		
Protocol vulnerability defense	Defense against IP spoofing, LAND, Fraggle, Smurf, WinNuke, Ping of Death, Tear Drop, IP Option, IP fragment control packet, TCP label validity check, large ICMP control packet, ICMP redirect control packet, and ICMP unreachable control packet attacks		
Transport-layer attack defense	Defense against SYN flood, ACK flood, SYN-ACK flood, FIN/RST flood, TCP fragment flood, UDP flood, UDP fragment flood, and ICMP flood attacks		
Scanning and sniffing attack defense	Defense against port scanning, address scanning, Tracert control packet, IP Option, IP timestamp, and IP routing record attacks		
DNS attack defense	Defense against forged source DNS query flood attacks, real source DNS query flood attacks, DNS reply flood attacks, DNS cache poisoning attacks, DNS protocol vulnerability attacks, and fast flux botnet		
Web attack defense	Defense against HTTP get/post flood attacks, CC attacks, HTTP slow header/post attacks, HTTPS flood attacks, SSL DoS/DDoS attacks, TCP connection attacks, Sockstress attacks, TCP retransmission attacks, and TCP null connection attacks		
VoIP attack defense	Defense against SIP flood attacks		
Zombie/Trojan horse/Worm attack defense	Defense against over 200 zombies, Trojan horses, and worms, such as LOIC, HOIC, Slowloris, Pyloris, HttpDosTool, Slowhttptest, and Thc-ssl-dos		
IPv6 defense types			
IPv6 defense types	Defense against ICMP fragment attacks, blacklist, HTTP field-based filtering, TCP/UDP/Other protocol load feature-based filtering, SYN flood attacks, ACK flood attacks, SYN-ACK flood attacks, FIN/RST flood attacks, TCP fragment flood attacks, UDP flood attacks, UDP fragment flood attacks, ICMP flood attacks, forged source DNS query flood attacks, real source DNS query flood attacks, DNS reply flood attacks, DNS cache poisoning attacks, DNS protocol vulnerability attacks, fast flux botnet, HTTP get/post flood attacks, CC attacks, HTTP slow header/post flood attacks, HTTPS flood attacks, SSL DoS/DDoS attacks, TCP connection attacks, Sockstress attacks, TCP retransmission attacks, TCP null connection attacks, and SIP flood attacks		
IPv4/IPv6 dual-stack attack defense	Supported		