Anti-DDoS Solution

- ZTW attacks
- Application-layer attacks
- Heavy traffic attacks
- Malformed packet attacks
- Protected service system
- Leaser self-service system

Overview

With the IT and Internet 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 DC applications are rampant, disabling the current defense measures of customers.

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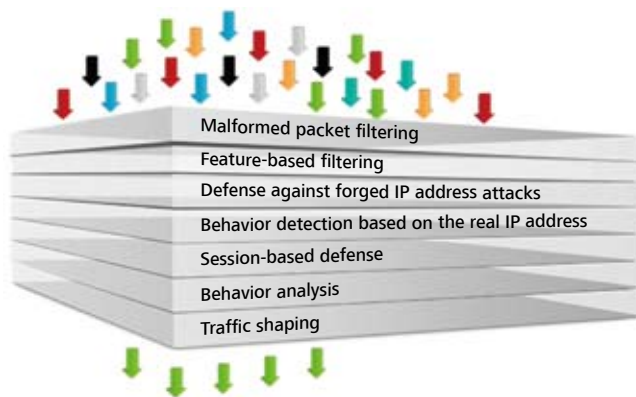

AntiDDoS1000 series | AntiDDoS8000 series

Highlights

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

- High-performance multi-core CPU, providing anti-DDoS products covering 2G to 200G 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.

Precise 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, precisely identifying illegitimate clients and ensuring zero false positive.

- Malformed packet filtering
- Feature-based filtering
- Defense against forged IP address attacks
- Behavior detection based on the real IP address
- Session-based defense
- Behavior analysis
- Traffic shaping

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

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

HUAWEI ENTERPRISE A BETTER WAY

Specifications

	AntiDDoS1000 Series			AntiDDoS8000 Series		
Model	AntiDDoS1520	AntiDDoS1550	AntiDDoS1500-D	AntiDDoS8030	AntiDDoS8080	AntiDDoS8160
Flood defense performance	3 Mpps	3 Mpps	3 Mpps	30 Mpps (15 Mpps per SPU)	75 Mpps (15 Mpps per SPU)	150 Mpps (15 Mpps per SPU)
Detecting/Cleaning performance	2 Gbit/s	5 Gbit/s	5 Gbit/s (detecting)	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	≤ 2 seconds	≤ 2 seconds	≤ 2 seconds
Fixed interface	4 × GE (RJ45)+4 × GE (combo)			None		
Expansion slot	2 × FIC	2 × FIC	2 × FIC	3	8	16
Expansion interface card	2 × 10 GE (SFP+) 2 × 10 GE (SFP+)+8 GE (RJ45) 8 × 1 GE (SFP) 8 × 1 GE (RJ45)			1 × 10 GE (XFP) 2 × 10 GE (XFP) 1 × 10 GE POS (XFP) 12 × 1 GE (SFP) 20 × 1 GE (SFP)		
Bypass card	4 × 1 GE (RJ45) Dual-link LC/UPC multi-mode optical interface Dual-link LC/UPC single-mode optical interface			None		
Dimensions (H × W × D)	43.6 × 442 × 560	43.6 × 442 × 560	43.6 × 442 × 560	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	150 W	150 W	150 W	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						
IPv4 defense types	Defense against ICMP fragment attacks, blacklist, HTTP field-based filtering, TCP/UDP/Other prorocol 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					