AntiDDoS1000 Series

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

AntiDDoS1000 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 the online services of small and medium-sized enterprises, governments, financial organizations, and ICP service providers, Huawei anti-DDoS solution accurately defends against various traffic and application-layer attacks, especially CC attacks, connection attacks, low-rate attacks, and SSL DoS/DDoS attacks. This fully ensures network security and service continuity.

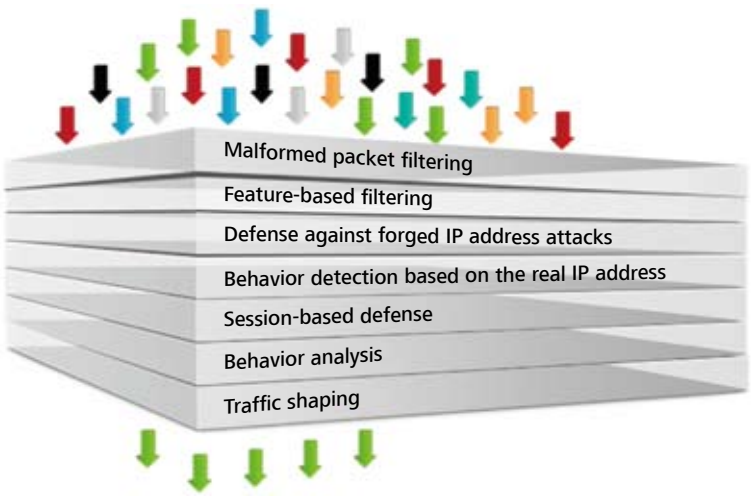
Highlights

Efficient and speedy: 5 Gbit/s defense performance and response within seconds

- High-performance multi-core CPU as well as dedicated anti-DDoS operating system, providing 5 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: "V-ISA" reputation technical to defend against hundreds of attacks

- "V-ISA" reputation technical 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.



Easy-to-use: easy management and enriched reports

- User/Service-centered management design, supporting the self-learning of the service traffic model and the automatic policy generation, and resulting in easy management.
- Enriched reports display attack status in multiple perspectives, such as the service traffic, attack statistics, and attack trend analysis, providing a visibility into services and threats.
- Self-extraction of attack fingerprints, implementing emergency defense and effectively defending against zero-day attacks.

Specifications

Model	AntiDDoS1520	AntiDDoS1550	AntiDDoS1500-D
Flood attack defense performance	3 Mpps	3 Mpps	3 Mpps
Detecting/Cleaning performance	2 Gbit/s	5 Gbit/s	5 Gbit/s (detecting)
Defense start latency	≤ 2 seconds	≤ 2 seconds	≤ 2 seconds
Fixed interface	4 × GE (RJ45)+4 × GE (combo)		
Expansion slot	2 × FIC	2 × FIC	2 × FIC
Expansion interface card	2 × 10GE (SFP+) and 2 × 10GE (SFP+)+8GE (RJ45) 8 × 1GE (SF) and 8 × 1GE (RJ45)		
Bypass card	4×1GE (RJ45) Dual-link LC/UPC multi-mode optical interface Dual-link LC/UPC single-mode optical interface		
Dimensions (H × W × D)	43.6 × 442 × 560	43.6 × 442 × 560	43.6 × 442 × 560
Maximum power consumption	150 W	150 W	150 W
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		

Copyright © Huawei Technologies Co., Ltd. 2013. All rights reserved.

General Disclaimer

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

HUAWEI TECHNOLOGIES CO., LTD.

Huawei Industrial Base
Bantian Longgang
Shenzhen 518129, P.R. China
Tel: +86-755-28780808

Version No.: M3-035027-20130914-C-2.0

www.huawei.com