



Huawei AntiDDoS8000 DDoS Protection System

Terabit capacity, attack response within seconds, precise protection, and value-added operation

Solution Highlights

- Terabit-level DDoS protection: 1.92 Tbit/s performance and attack response within seconds
- Precise DDoS protection: 60+ traffic models and defense against 100+ types of DDoS attacks
- Value-added operation: 100,000 tenants, differentiated operations, and a self-service portal for tenants

Solution Overview

As the Internet and IoT continue to evolve, DDoS attacks are developing new characteristics:

- Attacks are increasing both in terms of frequency and traffic volume, with peak attack traffic up to 1.35 Tbit/s in 2018.
- Reflection and amplification attacks are now widespread, causing network congestion around the world.
- Low-rate application-layer attacks are targeting service systems such as e-finance or gaming systems.
- SSL-encrypted attacks are on the rise but increasingly difficult to detect.

Reflection and amplification attacks and low-rate application-layer attacks are increasingly common these days, and a layered security approach is now being implemented to combat the trend. Huawei AntiDDoS8000 uses Big Data analytics to create 60+ traffic models, featuring DDoS protection with terabit capacity, response to attacks within seconds, and defense against 100+ types of attacks. The device works with Huawei's cloud cleaning center to deliver layered cleaning, providing fully fledged protection that covers link bandwidth and online services.

Solution Benefits

Defense against high volumes of DDoS attacks

- Multi-core distributed architecture and Big Data-based intelligent protection engine, helping to offer terabit-level protection
- Attacks are responded to within seconds

Defense against application-layer DDoS attacks

- Traffic is collected for per-packet analysis at L3, L4, and L7, and 60+ types of network traffic are modeled, providing the most precise and comprehensive detection of attacks
- All-round reputation systems, including local session behavior, location, and botnet IP reputation systems, defend accurately against application-layer DDoS attacks launched from botnets, reducing false positives and improving user experience
- Defense against 100+ types of attacks helps protect mission-critical service systems, such as web, DNS, VoIP, and gaming systems

Anti-DDoS operations

- Tenant-specific automatic and manual defense policies for comprehensive protection
- Tenant-specific report statistics and sending of reports via email to simplify management
- Self-service portal for tenants to help increase their loyalty
- Differentiated operations at a scale of 100,000 tenants

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

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

Layered anti-DDoS on the premises and in the cloud

- The on-premises device protects user services in real time.
- When a link is congested, the on-premises device can automatically send signals to the cloud to start cloud cleaning.
- 10+ cleaning centers around the world provide 2T+ cloud cleaning capacity and respond to attacks within minutes.



AntiDDoS8030



AntiDDoS8080



AntiDDoS8160

Huawei AntiDDoS8000 DDoS Protection System

Terabit capacity, attack response within seconds, precise protection, and value-added operation

DDoS Protection

Defense against the following protocol anomaly attacks: Land, Fraggle, Smurf, WinNuke, Ping of Death, Teardrop, and TCP error flag attacks	DNS application protection against the following attacks: - DNS query flood, DNS reply flood, and DNS spoofing - Source rate limiting and domain name rate limiting
Defense against the following network attacks: SYN 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	SIP application protection against the following attacks: SIP flood and SIP method flood attacks, including register flood, deregistration flood, authentication flood, and call flood attacks Source rate limiting
Defense against the following UDP-based reflection and amplification attacks: NTP, DNS, SSDP, Chargen, TFTP, SNMP, NetBIOS, QOTD, Quake Network Protocol, Portmapper, Microsoft SQL Resolution Service, RIPv1, and Steam Protocol reflection and amplification attacks	Filters: IP, TCP, UDP, ICMP, DNS, SIP, and HTTP packet filters
Attack signature databases: RUDY, slowhttptest, slowloris, LOIC, AnonCannon, RefRef, ApacheKill, and ApacheBench attack signature databases, which are updated automatically each week	Location-based filtering: Traffic is blocked or limited based on the location of the source IP address.
Web application protection against the following attacks: - HTTP Get flood, HTTP Post flood, HTTP slow header, HTTP slow post, HTTPS flood, SSL (renegotiation) DoS/DDoS, WordPress amplification, RUDY, and LOIC attacks - Packet validity check	IP reputation: - Most active zombies are tracked, and the IP reputation database is updated automatically on a daily basis to block attacks fast. - Local reputation records are automatically learned. - The learning of local access IP reputations creates dynamic IP reputation records based on local service sessions, helping to forward service access traffic quickly and enhance user experience.

Management and Report

Management functions: - Account management and permission allocation - Defense policy configuration and reports based on Zones (tenants), at a scale of up to 100,000 Zones - Device performance monitoring - Source tracing and fingerprint extraction by capturing packets - Email, short message, and audio alarms - Log dumping - Dynamic baseline learning - Policy interworking and log interworking APIs	Report functions: - Traffic comparison 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 trends - DNS resolution success ratio - Top N traffic statistics for the application layer (by source IP address, HTTP URI, HTTP HOST, and domain name) - Downloading of reports in HTML, PDF, or Excel format - Report pushing via email - Generation of daily, weekly, monthly, and yearly reports - Self-service portal for tenants - Creation, deletion, updating, and viewing of Zones, and addition and deletion of protected IP addresses - Creation and deletion of traffic diversion policies - Creation and deletion of blackhole routes - Traffic and attack logs for each IP address - Sending of logs in syslog format
--	---

Traffic Diversion and Injection Functions

Traffic diversion: Manual traffic diversion and automatic PBR- or BGP-based traffic diversion	Traffic injection: Static route, MPLS VPN, MPLS LSP, GRE tunnel, Layer 2, and PBR-based injection
---	---

Hardware Parameters

Model	AntiDDoS8030	AntiDDoS8080	AntiDDoS8160
Expansion slot	3	8	16
Expansion interface board	FW-LPUF-120, with two sub-slots	FW-LPUF-120, with two sub-slots FW-LPUF-240, with two sub-slots	FW-LPUF-120, with two sub-slots FW-LPUF-240, with two sub-slots
Expansion card	24 × GE (SFP) 5 × 10 GE (SFP+) 6 × 10 GE (SFP+) 12 × 10 GE (SFP+) 1 × 40 GE (CFP) 1 × 100 GE (CFP) 3 × 40 GE (QSPF+)		
Dimensions (W × D × H)	DC: 442mm × 650mm × 175mm (4U) AC: 442mm × 650mm × 220mm (5U)	442mm × 650mm × 620mm (14U)	1420mm × 442mm × 650mm (32U)
Weight	DC: 15 kg (empty) or 30.7 kg (fully configured) AC: 25 kg (empty) or 40.7 kg (fully configured)	43.2 kg (empty) or 112.9 kg (fully configured)	94.4 kg (empty) or 233.9 kg (fully configured)
Power supply mode	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 supply redundancy	DC: Two hot swappable power supplies AC: Two hot swappable power supplies	DC: 4 hot swappable PEM modules AC: 4 PEM modules + 1 external AC-DC convertor	DC: 8 hot swappable PEM modules AC: 8 PEM modules + 2 external AC-DC convertors
Temperature	Working environment: 0°C to 45°C (long-term), -5°C to 50°C (short-term) Storage: -40°C to 70°C		
Relative humidity (RH)	Working environment: 5% RH to 85% RH, non-condensing (long-term), 5% RH to 95% RH, non-condensing (short-term) Storage: 0% RH to 95% RH		
Security certifications	Electromagnetic compatibility (EMC) CB, RoHS, FCC, MET, C-Tick, and VCCI		

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.

Copyright©2018 Huawei Technologies Co., Ltd. All rights reserved.