Precise, Full-Scale, and Reliable Service Protection
Huawei Next Generation Anti-DDoS Solution

Highlights

- T-bit defense performance and response within seconds
- Multiple fingerprint technologies, which defend against mobile DDoS attacks
- Defense against 100+ DDoS attacks, which secures service availability
- Customized, value-added operation management

Overview

During the era of mobile Internet and Big Data, DDoS attacks become increasingly complex.

- The peak attack traffic keeps growing. In 2013, the peak DDoS attack traffic exceeds 300 Gbit/s.
- An increasing number of application-layer DDoS attacks occur in data center service systems.
- The number of mobile service-specific DDoS attacks that come from mobile terminals increases rapidly.
- Data centers are attack targets, and hackers can easily use a data center to launch attacks to external service systems.

Traditional Anti-DDoS solutions in the industry cannot adapt to these changes. Huawei Next Generation (NG) Anti-DDoS Solution performs abstract modeling and reputation system construction on network traffic from over 60 dimensions by leveraging Big Data analytics technologies. Compared to traditional Anti-DDoS mechanisms in the industry, the Huawei NG Anti-DDoS Solution provides more precise and comprehensive DDoS attack defense.

Functionalities

Anti-Large-DDoS: Heavy Traffic DDoS Attack Defense

- Multi-core, distributed hardware architecture and *Big Data-based Intelligent Defense Engine*[1] provide T-bit defense performance.
- Instant attack response within seconds protects link availability.

Anti-App-DDoS: Application DDoS Attack Defense

- Performs all traffic collection and 3-7-layer packet-by-packet analysis, create traffics models from over 60 dimensions, and provides the most precise and comprehensive attack detection.
- Fine-grained reputation system consisting of local session behavior-based reputation, service access behavior-based reputation, geographical location-based reputation, and botnet cloud-based reputation precisely guards against various lightweight, slow application-layer DDoS attacks launched by botnets.
- Full-scale defense against over 100 attacks guarantees continuous operations of key service systems that encompass enterprise web applications and DNS, DHCP, and VoIP services.

Anti-Mobile-DDoS: Mobile DDoS Attack Defense

- Dynamic, real-time upgrade of 20,000 fingerprints and filtering of traffic by a mobile botnet database effectively defend DDoS attacks launched by botnets and mobile terminals and guarantees authorized access to mobile gateways.
- Protects availability of mobile data service systems such as mobile payment, mobile store, mobile social networking, and mobile game.

Anti-Outbound-DDoS: Inbound-to-Outbound DDoS Attack Defense

- Blocks the global most active zombie, Trojan horse, and worm controlling traffic.
- Blocks C&C DNS request traffic.
- Prevents DDoS attacks at the source.

Managed-Anti-DDoS: Managed DDoS Attack Defense Service

- Provides Zone (VIP)/service-based automatic and manual defense policies and complete defense methods.
- VIP/service-based independent statistics reports and email sending simplify defense management.
- Increases VIP' service stickiness by providing Portal-based self-service functions for VIP.
- Supports large-scale operations, for example, 10,000 VIPs/services, and protects 10,000 IP addresses of each VIP/service simultaneously.

[1] Big Data-based Intelligent Defense Engine is Huawei's proprietary security protection engine that leverages Big Data analytics technologies. This engine first performs one-time intelligent dual-stack resolution and in-depth analysis of Layers 3 through 7. Then the engine carries out a correlation analysis and mode matching from multiple dimensions to ensure precise and timely analysis.

Attack Defense Functions (IPv4/IPv6 Supported)

Protocol abuse attack defense

Defense against IP spoofing, LAND, Fraggle, Smurf, Winnuke, Ping of Death, Tear Drop, IP Option, IP Fragment Control Packet, TCP Error Flag check, Large ICMP Control Packet, ICMP Redirect Control Packet, and ICMP unreachable control packet attacks

Scanning and sniffing attack defense

Defense against Port Scanning, IP Scanning, Tracert Control Packet, IP Option, IP Timestamp, and IP Routing Record attacks

Network-layer attack defense

Defense against SYN Flood, ACK Flood, SYN-ACK Flood, FIN/RST Flood, TCP Fragment Flood, UDP Flood, UDP Fragment Flood, NTP Flood, ICMP Flood, TCP Connection Flood, Sockstress, TCP Retransmission, and TCP Null Connection attacks

Zombie, Trojan horse, worm, and tools traffic blocking:

Blocking of controlling traffic of active zombies, Trojan horses, worms, and tools, such as LOIC, HOIC, Slowloris, Pyloris, HttpDosTool, Slowhttptest, Thc-ssl-dos, YoyoDDOS, IMDDOS, Puppet, Storm, fengyun, AladinDDoS, And so on

C&C DNS request traffic blocking

Web attack defense

Defense against HTTP Get Flood, HTTP Post Flood, HTTP Head Flood, HTTP Slow Header Flood, HTTP Slow Post Flood, HTTPS Flood, and SSL DoS/DDoS attacks

DNS attack defense

Defense against DNS Query Flood attacks from real or spoofed source IP addresses, DNS Reply Flood attacks, DNS Cache Poisoning attacks, DNS Protocol Vulnerability Exploits, and DNS Reflection attacks

SIP attack defense

Defense against SIP Methods Flood attacks

DHCP attack defense

Defense against DHCP Flood attacks

Mobile attack defense

Defense DDoS attacks launched by mobile botnets, for example, AnDOSid/WebLOIC/Android.DDoS.1.origin

Feature-based filtering

Blacklist, HTTP/DNS/SIP/DHCP field-based filtering, and IP/TCP/UDP/ICMP/other protocol field-based and load feature-based filtering

IP reputation database[1]

12 data centers across the globe process 12 billion query analysis requests on a daily basis and tracks the global most active 5 million zombie hosts with a daily update.

Management and reports

Supports account management and rights allocation; supports 10,000 defense objects; supports import of defense policies in batches; supports device performance monitoring; supports source tracking through packet capture and fingerprint extraction; supports SMS/Voice/Email alarming; supports log dumping; supports network traffic model learning, supports multidimensional reports including attack traffic analysis, attack event analysis, and attack trend analysis; supports download of reports in multiple formats such as HTML, PDF, Excel, and CSV; supports report push through emails; and supports Portal-based operations.

Networking and Traffic Diversion Policies

Deployment Modes:

Supports inline and offline deployment.

Traffic Diversion Policies:

Supports manual traffic diversion and multiple automatic traffic diversion modes such as policy-based routing and BGP routing.

Interface and Hardware Parameters

		AntiDDoS8030 (4 U Height)	AntiDDoS8080 (14 U Height)	AntiDDoS8160 (32 U Height)
Max Performance		40Gbps/80Gbps[2]	100Gbps/480Gbps[3]	200Gbps/960Gbps[3]
Max Performance/Slot		20Gbps	20Gbps	20Gbps
		80Gbps[2]	160Gbps[3]	160Gbps[3]
Expansion slot		3	8	16
Interface Card Type	LPUF-21 interface card	12 x 1GE (RJ45)/12 x 1GE (SFP)/1 x 10GE (XFP)/4 x 10GE (XFP)/1 x 10GE POS (XFP)		
	LPUF-40 interface card	20 x 1GE (SFP)/2 x 10GE (XFP)/4 x 10GE (XFP)		
	LPUF-101 interface card	24 x GE (SPF)/4 x 10GE (SPF+)/5 x 10GE (SPF+)/1 x 40GE (CPF)/1 x 100GE (CPF)		
Reliability		Supports dual MPUs and achieves a five-nine carrier-grade reliability (99.999%).		
Power Supply Type		Supports both DC and AC power supply.		

[1] .IP reputation database Function will be ready in 2014Q4

[2] .AntiDDoS8030 with SPUC max performance can get 80Gbps, and SPUC will be ready in 2014Q4

[3] .AntiDDoS8080/8160 with SPUD max performance can get 480Gbp/960Gbps and SPUD will be ready in 2014Q4

THIS DOCUMENT IS FOR INFORMATION PURPOSE ONLY, AND DOES NOT CONSTITUTE ANY KIND OF WARRANTIES.