Huawei AntiDDoS1600 DDoS Protection System

Precise Protection, Second-level Response, In-line Deployment, Layered Defense

As the Internet and IoT thrive, the Distributed Denial of Service (DDoS) attacks are developing new characteristics:

- Attacks increase in frequency and traffic volume.
- An era of reflection attacks emerges, and reflection amplification attacks, such as NTP, SSDP, and DNS attacks are devouring limited enterprise and data center bandwidths.
- IoT devices could be exploited to construct Botnets for initiating large-scale attacks.
- Targets of DDoS attacks spread from large enterprises to various industries.
- Attacks become more diversified, with volumetric and application attacks mixed to circumvent defense at a single layer.

In response to these challenges, Huawei rolls out the AntiDDoS1600 DDoS protection system, which employs the big data analytics technology and supports modeling for 60+ types of network traffic to offer second-level attack response and comprehensive defense against 100+ types of attacks. The AntiDDoS1600 can be deployed on a user network in in-line mode to defend against volumetric and application attacks in real time. When attack traffic exceeds the bandwidth or defense capability of a local scrubbing device, the AntiDDoS1600 associates with the AntiDDoS device of the upstream carrier or ISP to defend against flood attacks and guarantee service continuity.

Product Appearances

AntiDDoS1650

AntiDDoS1680

Solution Function

Defense against high-volume DDoS attacks

- Multi-core distributed architecture and big data based intelligent protection engine.
- Second-level attack response to rapidly block attack traffic.

Defense against application-layer DDoS attacks

- Collection of all traffic, Layer 3~7 per-packet analysis, and modeling for 60+ types of network traffic to provide the most precise and comprehensive attack detection.
- All-round reputation system of local session behavior reputation, location reputation, and Botnet IP reputation to precisely defend against application-layer DDoS attacks launched from Botnets, reducing false positives and improving user experiences.
- Comprehensive defense against 100+ types of attacks to protect key service systems, such as Web, DNS, DHCP, and VoIP.

In-line protection

- Transparent access and simple deployment to defend against DDoS attacks in real time.
- Bypass expansion cards for high availability.

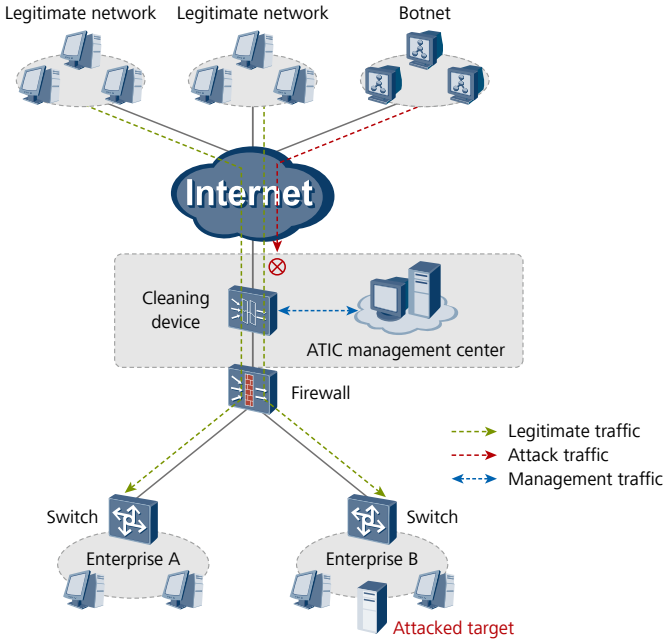
Layered Anti-DDoS

- Deployed at enterprise and data center borders to protect user services.
- Associated with AntiDDoS devices of upstream carriers or ISPs to defend against flood attacks when the attack traffic exceeds access bandwidths or processing capabilities of on-premise devices.

Typical Scenarios

Scenario 1: Enterprise Network Defense

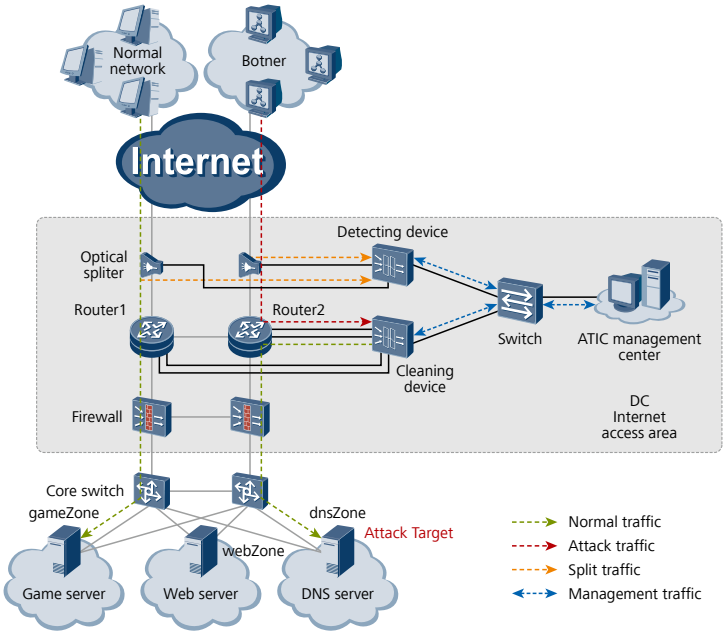
With the development of internet technologies, enterprise networks are prone to extensive threats. In addition to defending against attacks from Internet, enterprise networks require smooth service operating.



On the network shown in above figure, the cleaning device is deployed at the ingress of the enterprise network in in-line mode to protect incoming and outgoing traffic. When anomalies occur, the cleaning device enables attack defense immediately. Meanwhile, the cleaning device can be configured with Bypass card to enhance solution reliability.

Scenario 2: Data Center Security Protection

An Internet Data Center (IDC) is a part of basic network resources. It provides large-scale, high-quality, secure, and reliable data transmission services and high-speed access services for Internet content providers, enterprises, media, and each types of websites. The IDC provides DNS servers, Web servers, game servers, and other services. In recent years, more and more Internet-initiated DDoS attacks target IDCs. As a result, important servers are attacked; data center link bandwidth is occupied; videos and games are compromised by application-layer attacks.



On the network shown in above figure, a cleaning device is attached to the core router1 and router2 to detect and clean the traffic destined for the Zone. The traffic must be diverted to the cleaning device using BGP in real time. After traffic is cleaned, normal traffic is injected back to the original link through PBR and finally forwarded to the Zone.

Specifications

DDoS Defense Specifications

Defense against protocol abuse attacks Defense against Land, Fraggle, Smurf, WinNuke, Ping of Death, Teardrop, and TCP error flag attacks	Web application protection Defense against HTTP GET flood, HTTP POST flood, HTTP slow header, HTTP slow post, HTTPS flood, SSL DoS/DDoS, WordPress reflection amplification, RUDY, and LOIC attacks; packet validity check
Defense against scanning and sniffing attacks Defense against address and port scanning attacks, and attacks using Tracert packets and IP options, such as IP source route, timestamp, and record route	DNS application protection Defense against DNS query flood, DNS reply flood, and DNS cache poisoning attacks; source limit
Defense against network-type attacks Defense against SYN flood, SYN-ACK 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 Defense against SIP flood/SIP methods flood attacks, including Register, Deregistration, Authentication, and Call flood attacks; source limit
Defense against UDP-based reflection amplification attacks Defense against NTP, DNS, SSDP, Chargen, TFTP, SNMP, NetBIOS, QOTD, Quake Network Protocol, Portmapper, Microsoft SQL Resolution Service, RIPv1, and Steam Protocol reflection amplification attacks	Filter IP, TCP, UDP, ICMP, DNS, SIP, and HTTP packet filters Location-based filtering Traffic block or limit based on the source IP address location
Attack signature database RUDY, slowhttptest, slowloris, LOIC, AnonCannon, RefRef, ApacheKill, and ApacheBench attack signature databases; automatic weekly update of these signature databases	IP reputation Tracking of most active 5 million zombies and automatic daily update of the IP reputation database to rapidly block attacks; local access IP reputation learning to create dynamic IP reputation based on local service sessions, rapidly forward service access traffic, and enhance user experience

Management and Report

Management functions	Report functions
Account management and permission allocation; defense policy configuration and report display based on Zones (up to 100,000 Zones, namely tenants); device performance monitoring; source tracing and fingerprint extraction through packet capture; email, short message, and audio alarms; log dumping; dynamic baseline learning	Comparison of traffic 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 trend; DNS resolution success ratio; application-layer top N traffic statistics (by source IP address, HTTP URI, HTTP HOST, and domain name); download of reports in HTML/ PDF/Excel format; report push via email; periodical generation of daily, weekly, monthly, and yearly reports; self-service portal for tenants

Deployment

Deployment mode	Traffic diversion and injection
In-line or out-of-path deployment	Traffic diversion: supports manual, and PBR or BGP based automatic traffic diversion. Traffic injection: supports static route injection, MPLS VPN injection, MPLS LSP injection, GRE tunnel injection, Layer 2 injection, PBR based injection, etc

Hardware Specifications

Model	AntiDDoS1650	AntiDDoS1680
Interfaces and performance		
Throughput	Up to 5Gbps	Up to 8Gbps
Mitigation rate	Up to 3Mpps	Up to 7Mpps
Latency	80 μs	80 μs
Standard interface	8×GE(RJ45)+4×GE(SFP)	16×GE(RJ45)+8×GE(SFP)+4×10GE(SFP)
Expansion slot	2×WSIC	5×WSIC
Expansion interfaces	8×GE(RJ45); 8×GE(RJ45)+2×10GE(SFP+); 8×GE(SFP); 4×GE(RJ45) Bypass card	
Deploy mode	in-line; Out-of-path(static defense); Out-of-patch(Dynamic defense)	
Function	Options for detecting or cleaning	

Model	AntiDDoS1650	AntiDDoS1680
External Bypass	Multi mode or single mode GE link; Multi mode or single mode 10GE link	
Dimensions		
Height × Width × Depth	44.4mm × 442mm × 421mm (1U)	130.5mm × 442mm × 470mm (3U)
Weight	Standard: 6 kg, Fully configured: 8.7 kg	Standard: 20 kg, Fully configured: 24 kg
Power and Environment		
Power supply	Rated input voltage: AC: 100 V to 240 V, 50 Hz/60 Hz Maximum input voltage range: AC: 90 V to 264 V, 47 Hz to 63 Hz Maximum input current: AC: 2.5 A	Rated input voltage: DC: -48V to -60V AC: 100 V to 240 V, 50 Hz/60 Hz Maximum input voltage range: DC: -48V to -60V AC: 90 V to 264 V, 47 Hz to 63 Hz Maximum input current: AC: 5 A
Power Consumption	170W	350W
Power redundancy	Single AC power module supply. Options for 2×AC power modules redundant, support hot-swap power supplies	AC: 1+1 power redundancy, hot-swappable DC: 1+1 power redundancy, hot-swappable
Operating temperature	0°C to 45°C (long-term), -5°C to 55°C (short term)	
Storage temperature	-40°C to 70°C	
Operating humidity	5% RH to 95% RH, non-condensing	
Storage humidity	5% RH to 95% RH, non-condensing	
Certifications		
Safety certifications	Electro Magnetic Compatibility (EMC) certification CB, CCC, CE-SDOC, ROHS, REACH&WEEE(EU), C-TICK, ETL, FCC&IC, VCCI, BSMI	

Order Information

Model	Description
Main Equipment	
AntiDDoS1650-AC	AntiDDoS1650 AC Host(8GE(RJ45)+4GE(SFP), 8GB Memory, 1 AC Power)
AntiDDoS1680-DC	AntiDDoS1680 DC Host(16GE(RJ45)+8GE(SFP)+4*10GE(SFP), 16GB Memory, 2 DC Power)

Model	Description
AntiDDoS1680-AC	AntiDDoS1680 AC Host(16GE(RJ45)+8GE(SFP)+4*10GE(SFP), 16GB Memory, 2 AC Power)
Business Module Group	
WSIC-8GE	8GE Electric Ports Interface Card
WSIC-4GEBYPASS	4GE Electric Ports Bypass Card
WSIC-8GEF	8GE Optical Ports Interface Card
WSIC-2XG8GE	2*10GE Optical Ports+8GE Electric Ports Interface Card
Management Software	
LIC-ADS-NOFA00	ATIC Basic Feature Summary