

Huawei AntiDDoS8000 DDoS Protection System

Terabit-level Capacity, Second-level Response, Precise Protection, Value-added Operation

As the Internet and IoT thrive, DDoS attacks are developing new characteristics:

- Attacks increase in frequency and traffic volume, and the peak attack traffic is up to 600 Gbps in 2015.
- Reflection amplification attacks spread across the world, congesting links.
- Low-rate application-layer attacks target precisely at service systems like e-finance or gaming.

Reflection amplification and low-rate application-layer attacks are gaining momentum, and layered defense becomes the first choice in anti-DDoS. Huawei AntiDDoS8000 employs big data analysis to conduct modeling for 60+ types of traffic, offering Terabit-level protection, second-level response, and comprehensive defense against 100+ types of attacks. It works with Huawei cloud cleaning center to deliver layered cleaning, providing full-fledged protection that covers network link bandwidths and online services.

Product Appearances



AntiDDoS8030



AntiDDoS8080



AntiDDoS8160



Solution Function

Defense against high-volume DDoS attacks

- Multi-core distributed architecture and big data-based intelligent protection engine to offer Terabit-level protection performance.
- 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 experience.
- Comprehensive defense against 100+ types of attacks to protect key service systems, such as Web, DNS, DHCP, and VoIP.

Anti-DDoS operation

- Tenant-specific automatic and manual defense policies for comprehensive protection.
- Tenant-specific report statistics and report sending via email to simplify management.
- Differentiated operation for 100,000 tenants.

Dual-stack (IPv4/IPv6) DDoS attack defense

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

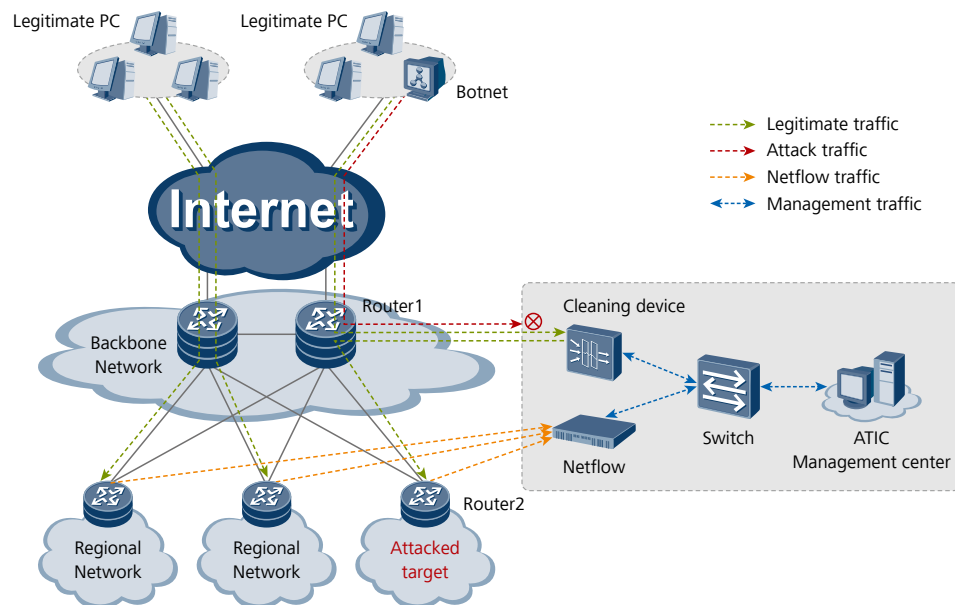
On-premise + Cloud layered anti-DDoS

- The on-premise device is online in real time to protect user services.
- When a link is congested, the on-premise device can automatically send cloud signals to start cloud cleaning and protect user links.
- 2Tbps+ cloud mitigation capacity. 10+ cloud scrubbing center with global scheduling. Minute-level defense response.

Typical Scenarios

Scenario 1: MAN Attack Defense

A metropolitan area network (MAN) provides a platform on which comprehensive services of a city are transmitted. MANs often apply to large and medium-sized cities. The MANs provide common and public network architecture and allow data, voice, images, and videos to be effectively transmitted at high speeds, meeting changeable Internet application requirements.

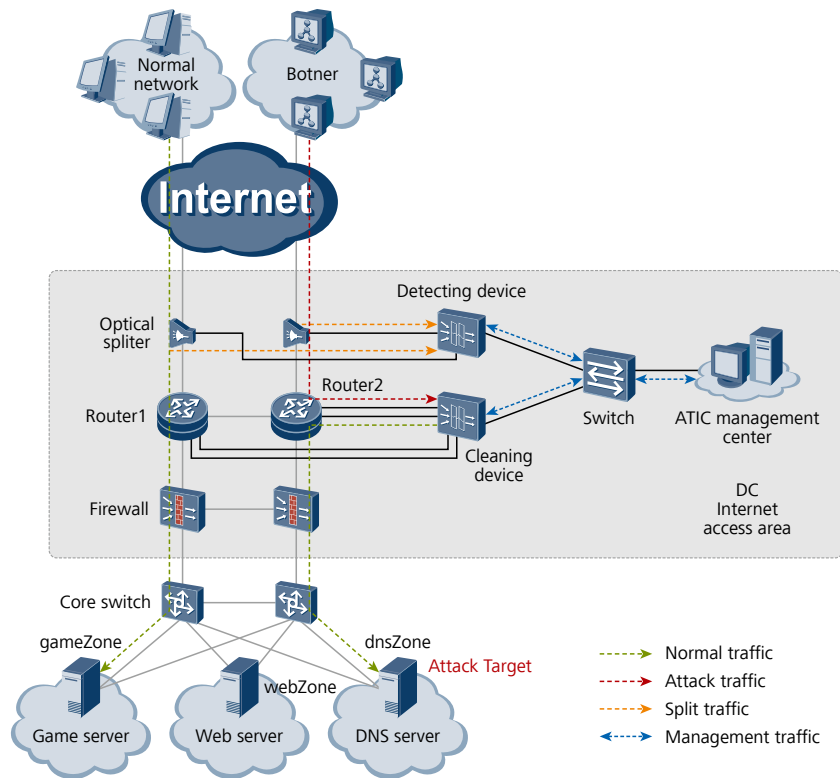


On the network shown in above figure, a netflow detection device collects the logs from routers in real time to determine whether the traffic in the network is abnormal. When traffic is abnormal, cleaning device is notified to start the cleaning. The cleaning device is attached to the core router Router1 to clean traffic destined for the Zone. After cleaning traffic, the cleaning device injects normal traffic back to the original link in MPLS LSP injection mode. Router2 then forwards the traffic to the Zone.

The cleaning device is directly connected to Router1 only through one interface. Traffic is diverted to the cleaning device through the main interface, while injected back through a sub-interface. The traffic can also be injected back through another interface if there are enough interfaces.

Scenario 2: Data Center Protection and Managed Security Service

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.

ATIC management center supports managed security service. ATIC management center can be configured with customized defense policies based on the tenant's service features. When attack happened, ATIC management center can initiate automatic protection and send alarm information by email or other methods. Data center operators can design business models based on tenants and expand business revenue.

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

| | |
|---|--|
| <p>Defense against scanning and sniffing attacks</p> <p>Defense against address and port scanning attacks, and attacks using Tracert packets and IP options, such as IP source route, timestamp, and record route</p> | <p>DNS application protection</p> <p>Defense against DNS query flood, DNS reply flood, and DNS cache poisoning attacks; source limit</p> |
| <p>Defense against network-type attacks</p> <p>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</p> | <p>SIP application protection</p> <p>Defense against SIP flood/SIP methods flood attacks, including Register, Deregistration, Authentication, and Call flood attacks; source limit</p> |
| <p>Defense against UDP-based reflection amplification attacks</p> <p>Defense against NTP, DNS, SSDP, Chargen, TFTP, SNMP, NetBIOS, QOTD, Quake Network Protocol, Portmapper, Microsoft SQL Resolution Service, RIPv1, and Steam</p> <p>Protocol reflection amplification attacks</p> | <p>Filter</p> <p>IP, TCP, UDP, ICMP, DNS, SIP, and HTTP packet filters</p> <p>Location-based filtering</p> <p>Traffic block or limit based on the source IP address location</p> |
| <p>Attack signature database</p> <p>RUDY, slowhttptest, slowloris, LOIC, AnonCannon, RefRef, ApacheKill, and ApacheBench attack signature databases; automatic weekly update of these signature databases</p> | <p>IP reputation</p> <p>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</p> |

Management and Report

| | |
|---|--|
| <p>Management functions</p> <p>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</p> | <p>Report functions</p> <p>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</p> |
|---|--|

Traffic Diversion and Injection

| | |
|--|---|
| <p>Traffic diversion</p> <p>Supports manual, and PBR or BGP based automatic traffic diversion</p> | <p>Traffic injection</p> <p>Supports static route injection, MPLS VPN injection, MPLS LSP injection, GRE tunnel injection, Layer 2 injection, PBR based injection, etc</p> |
|--|---|

Hardware Specifications

| Model | AntiDDoS8030 | AntiDDoS8080 | AntiDDoS8160 |
|-----------------------------------|--|--|--|
| Interfaces and performance | | | |
| Throughput | Up to 120 Gbps | Up to 720 Gbps | Up to 1440 Gbps |
| Throughput/slot | Up to 80 Gbps | Up to 160 Gbps | Up to 160 Gbps |
| Mitigation rate/slot | Up to 60 Mpps | Up to 60 Mpps | Up to 60 Mpps |
| Latency | 80 μ s | 80 μ s | 80 μ s |
| Expansion slot | 3 | 8 | 16 |
| Expansion LPU | FW-LPUF-120, 2 sub-slots | FW-LPUF-120, 2 sub-slots FW-LPUF-240, 2 sub-slots | FW-LPUF-120, 2 sub-slots FW-LPUF-240, 2 sub-slots |
| Expansion interfaces | 24xGE (SFP); 5x10GE (SFP+); 6x10GE (SFP+); 12x10GE (SFP+); 1x40GE (CFP); 1x100GE (CFP) | | |
| Dimensions | | | |
| Height x Width x Depth | DC: 175mm x 442mm x 650mm (4U) AC: 220mm x 442mm x 650mm (5U) | 620mm x 442mm x 650mm (14U) | 1420mm x 442mm x 650mm (32U) |
| Weight | DC chassis: 15kg (empty), 30.7 kg (full) AC chassis: 25kg (empty), 40.7 kg (full) | 43.2 kg (empty), 112.9 kg (full) | 94.4 kg (empty), 233.9 kg (full) |
| Power and Environment | | | |
| Power supply | Rated input voltage: DC: -48 V AC: 175 V to 264 V; 50/60 Hz Maximum input voltage range: DC: -72 V to -38 V AC: 90 V to 264 V; 50/60 Hz | Rated input voltage: DC: -48 V AC: 175 V to 264 V; 50/60 Hz Maximum input voltage range: DC: -72 V to -38 V AC: 90 V to 264 V; 50/60 Hz | Rated input voltage: DC: -48 V AC: 175 V to 264 V; 50/60 Hz Maximum input voltage range: DC: -72 V to -38 V AC: 90 V to 264 V; 50/60 Hz |

| Model | AntiDDoS8030 | AntiDDoS8080 | AntiDDoS8160 |
|-----------------------|---|--|--|
| Power consumption | 1 × FW-LPUF-120 + 2 × ADS-SPUC-B + 2 × ADS-SPC-80-01: DC: 1066 W (avg), 1272 W (max) AC: 1185 W (avg), 1414 W (max) | 3 × FW-LPUF-240 + 5 × ADS-SPUD-B + 10 × ADS-SPC-80-01: DC: 4025 W (avg), 4823 W (max) AC: 4282 W (avg), 5132 W (max) | 6 × FW-LPUF-240 + 9 × ADS-SPUD-B + 18 × ADS-SPC-80-01: DC: 7387 W (avg), 8930 W (max) AC: 7858 W (avg), 9500 W (max) |
| Power redundancy | DC: Double hot-swappable power modules AC: Double hot-swappable power modules | DC: 4 hot-swappable PEM modules AC: 4 PEM modules+1 external AC power chassis | DC: 8 hot-swappable PEM modules AC: 8 PEM modules+2 external AC power chassis |
| Operating temperature | 0°C to 45°C (long-term), -5°C to 50°C (short-term) | | |
| Storage temperature | -40°C to 70°C | | |
| Operating humidity | 5% RH to 85% RH, non-condensing (long-term), 5% RH to 95% RH, non-condensing (short-term) | | |
| Storage humidity | 0% RH to 95% RH | | |
| Certifications | | | |
| Safety Certifications | Electro Magnetic Compatibility (EMC) certification CB, Rohs, FCC, MET, C-tick, and VCCI certification | | |

Order Information

| Model | Description |
|--------------------------------|---|
| Main Equipment | |
| ADS8030-BASE-DC-01 | AntiDDoS8030 DC Basic Configuration(include X3 DC Chassis, 2*MPU) |
| ADS8030-BASE-AC-01 | AntiDDoS8030 AC Basic Configuration(include X3 AC Chassis, 2*MPU) |
| ADS8080-BASE-DC-01 | AntiDDoS8080 200G DC Basic Configuration(include X8 DC Chassis, 2*SRU200A, 1*SFU200C) |
| ADS8160-BASE-DC-01 | AntiDDoS8160 200G DC Basic Configuration(include X16 DC Chassis, 2*MPU, 4*SFU200B) |
| Service Processing Card Module | |
| ADS-SPUC-B | AntiDDoS8030 Service Processing Unit(Base Board) |
| ADS-SPUD-B | AntiDDoS8080&AntiDDoS8160 Service Processing Unit(Base Board) |
| ADS-SPC-40-01 | DDoS Protection Service Card(with 1 CPU) |



| Model | Description |
|-----------------------------|--|
| ADS-SPC-80-01 | DDoS Protection Service Card(with 2 CPUs) |
| Line Processing Card Module | |
| FW-LPUF-120 | 120G Line Processing Unit |
| FW-LPUF-240 | 240G Line Processing Unit |
| FW-6X10G-SFP+ | 6*10GE SFP+ Daughter Card |
| FW-1X100G-CFP | 1*100GE CFP Daughter Card |
| FW-12X10G-SFP+ | 12*10GE SFP+ Daughter Card |
| E8KE-X-101-5X10GE-SFP+ | 5-Port 10GBase LAN/WAN-SFP+ Flexible Card A(P101, 1/2wide, Occupy two sub-slots) |
| E8KE-X-101-24XGE-SFP | 24-Port 100/1000Base-X-SFP Flexible Card(P101, 1/2wide, Occupy two sub-slots) |
| E8KE-X-101-1X40GE-CFP | 1-Port 40GBase LAN CFP Flexible Card(P101, 1/2wide, Occupy two sub-slots) |
| Management Software | |
| LIC-ADS-NOFA00 | ATIC Basic Feature Summary |

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©2017 Huawei Technologies Co., Ltd. All rights reserved.