Huawei HiSecEngine AntiDDoS1900 Series Products

Precise Protection, Flexible Deployment, and Efficient Cleaning

With the development of the Internet and IoT, DDoS attacks are also evolving, presenting new challenges:

- There are more frequent attacks and heavier attack traffic.
- Reflection attacks, such as NTP, SSDP, and DNS reflection amplification, are consuming limited enterprise and data center bandwidth.
- IoT devices may be exploited to construct botnets to launch large-scale attacks.
- DDoS attacks are targeting various industries, beside large enterprises.
- Attack types are diversified. Traffic attacks and application-layer attacks are combined to make single-layer defense fail.

To tackle these challenges, the AntiDDoS1900 series is launched by Huawei, which uses big data analysis to abstract and model more than 60 types of network traffic, being able to respond to attacks within seconds and defend against over 100 types of attacks. The AntiDDoS1900 series can be deployed on user networks in in-path or off-path mode to defend against traffic attacks and application-layer attacks in real time. It implements multi-dimensional behavior analysis based on attack sources to effectively defend against complex CC attacks.

Product Appearances

Huawei HiSecEngine AntiDDoS1905

HUAWEI

Product Functions

Traffic-based Anti-DDoS

- With the multi-core distributed hardware architecture, the product is equipped with the big data-based intelligent protection engine.
- The product can respond to attacks within seconds and rapidly block attack traffic.

Defense Against Application-Layer DDoS Attacks

- With full traffic collection and per-packet analysis at Layers 3, 4, and 7, the product can build models for more than 60 types of network traffic, providing the most accurate and comprehensive detection of attacks.
- With all-round reputation systems, including local session behavior, geographical location, and botnet IP reputation systems, the product can accurately defend against application-layer DDoS attacks launched from botnets, reducing false positives and improving user experience.
- The product can defend against over 100 types of attacks, effectively protecting web, DNS, DHCP, VoIP, and other key service systems.
- The product can implement multi-dimensional behavior analysis based on attack sources to effectively defend against CC attacks.

Flexible Deployment

- The product supports transparent access, simple deployment, and real-time defense against DDoS attack traffic.
- The product supports bypass cards to implement high reliability.
- The product supports in-path deployment, off-path traffic diversion and injection, and flexible deployment, meeting the requirements of various scenarios.

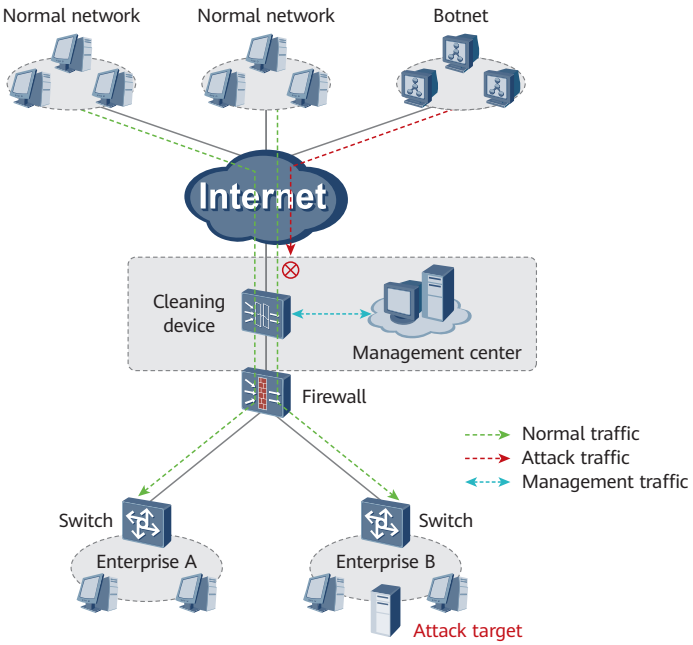
Efficient DDoS Mitigation

- The 1U high device supports the cleaning capability of up to 50 Gbit/s.
- Flexible license options are available for various types of services.

Typical Scenarios

Scenario 1: Enterprise Network Protection

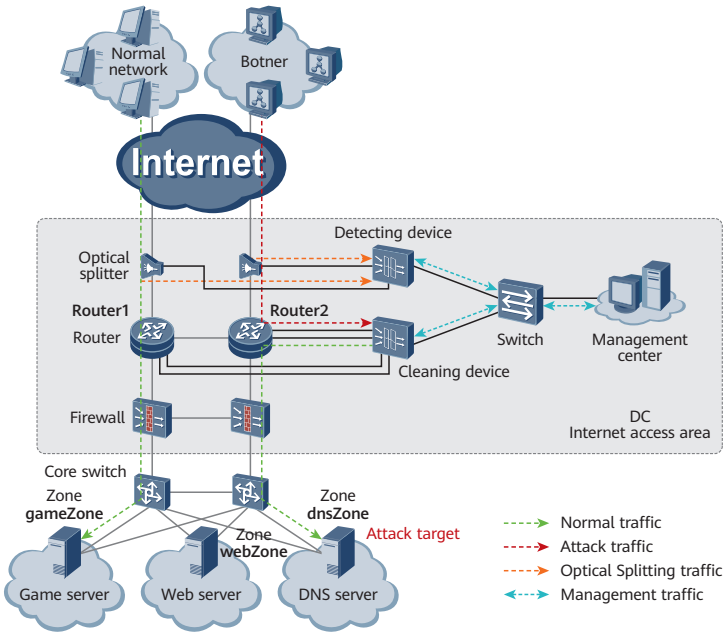
With the growth of the Internet, enterprise networks are facing more and more attacks. Enterprise networks must both defend against attacks from the Internet and ensure the continuity of service applications.



As shown in the figure, the cleaning device is deployed at the ingress of the enterprise network in in-path mode to protect incoming and outgoing traffic in real time. If an attack occurs, the cleaning device immediately starts defense. In addition, a bypass card can be equipped on the cleaning device to enhance reliability.

Scenario 2: Data Center Protection

Internet Data Centers (IDCs) are part of basic network resources. They provide large-scale, high-quality, secure, and reliable data transmission services and high-speed access services for Internet content providers (ICPs), enterprises, media agencies, and websites. The IDCs provide DNS servers, web servers, and online gaming services. In recent years, a growing number of DDoS attacks have been launched against IDCs from the Internet, compromising service-critical servers, exhausting IDC link bandwidth, and exposing video and online gaming services to application-layer attacks.



On the network shown in the figure, a cleaning device is attached to the core routers (Router1 and Router2) in off-path mode to detect and clean the traffic destined for the Zone. Downstream traffic destined for the Zone is diverted through BGP to the cleaning device in real time for detection and cleaning. After cleaning, normal traffic is injected back to the routers through policy-based routing (PBR). The routers then forward the normal traffic to the Zone.

Specifications List

DDoS Mitigation Functions

Defense against protocol abuse attacks Defense against LAND, Fraggle, Smurf, WinNuke, Ping of Death, Teardrop, and TCP Error Flag attacks	**HTTP application protection** Defense against high-frequency HTTP flood attacks Defense against HTTP Slow Header, HTTP Slow POST, RUDY, LOIC, HTTP Multi-Methods, HTTP Range amplification, and HTTP null connection attacks Defense against WordPress reflection attacks
Defense against scanning and sniffing attacks Defense against address sweep and port scan attacks, and attacks using Tracert packets and IP options, such as IP source routing, timestamp, and route record options	**HTTPS/TLS encryption application protection** Defense against high-frequency HTTPS/TLS encryption attacks Defense against slow TLS incomplete sessions and null connections
Defense against network-type attacks Defense against common network-layer flood attacks, such as SYN flood, SYN-ACK flood, ACK flood, FIN flood, RST flood, TCP Fragment flood, TCP Malformed flood, UDP flood, UDP Fragment flood, IP flood, and ICMP flood attacks Defense against common session-layer attacks, such as real source SYN, TCP connection flood, SockStress, TCP retransmission, and TCP null connection attacks	**DNS application protection** Defense against DNS Query flood, NXDomain flood, DNS Reply flood, and DNS cache poisoning attacks; source- and domain name-based rate limiting

UDP reflection attack filtering

Support for static rules for filtering common UDP reflection amplification attacks, such as NTP, DNS, SSDP, CLDAP, Memcached, Chargen, SNMP, and WSD reflection amplification

Support for dynamically generation of filtering rules to defend against new UDP amplification attacks

TCP reflection attack defense

Support for static filtering rules that are created based on network layer characteristics

Support for TCP reflection attack filtering rules that are dynamically generated

TCP replay attack defense

Support for static filtering rules that are created based on network layer characteristics

Support for TCP replay attack filtering rules that are dynamically generated

SIP application protection

Defense against SIP flood and SIP Methods flood attacks, including Register flood, Deregistration flood, Authentication flood, and Call flood attacks; source rate limiting

Intelligent behavior analysis

The intelligent analysis technology used to defend against slow attacks from real sources

Static software filtering rules

IP packet filter: filters traffic based on IP packet fields such as the source IP address, destination IP address, packet length, protocol, TTL, payload, and DF flag.

TCP packet filter: filters traffic based on TCP packet fields, such as the source IP address, destination IP address, packet length, source port, destination port, TCP flag, TTL, payload, and DF flag.

UDP packet filter: filters traffic based on UDP packet fields such as the source IP address, destination IP address, packet length, source port, destination port, TTL, payload, and DF flag.

ICMP packet filter: filters traffic based on ICMP packet fields, such as the source IP address, destination IP address, packet length, payload, and DF flag.

DNS packet filter: filters traffic based on DNS packet fields, such as the source IP address, destination IP address, packet length, source port, domain, type, QR, and DF flag.

HTTP packet filter: filters traffic based on HTTP packet fields such as the source IP address, destination IP address, packet length, source port, opcode, cookie, host, referer, URI, and User_Agant.

SIP packet filter: filters traffic based on SIP packet fields, such as the source IP address, destination IP address, packet length, source port, caller, and callee.

Hardware filtering rules can be created based on the source IP address, destination IP address, source port, destination port, protocol, TCP-Flag, packet length, and DF flag.

Management and Report Functions

Management functions

Account management and permission allocation; defense policy configuration and displaying statistics in reports based on Zones; device performance monitoring; source tracing and fingerprint extraction through packet capturing; short message, audio, and email alarms; log dumping; dynamic baseline learning

Report functions

Comparison of traffic before and after cleaning; top N traffic statistics; application-layer traffic comparison and distribution; protocol type distribution; traffic statistics based on the location of the source IP address; attack vent details; top N attack events (by duration or number of packets); distribution of attacks by category; attack traffic trend; DNS resolution success rate; application-layer top N traffic statistics (by source IP address, HTTP URI, HTTP host, and DNS domain name); download of reports in the HTML/PDF/Excel format; report push via email; periodic generation of daily, weekly, monthly, and yearly reports; self-service portal for tenants

Deployment Mode and Traffic Diversion and Injection

Deployment mode	Traffic diversion and injection
In-path and off-path deployment	Traffic diversion: supports manual and PBR/BGP-based automatic traffic diversion. Traffic injection: supports static route injection, GRE tunnel injection, Layer 2 injection, PBR-based injection, etc.

Interface and Hardware Specifications

Model	AntiDDoS1905
Performance	
Max Defense Throughput	50 Gbps
Max Defense Packet Rate	50 Mpps
New Sessions/Second	500,000/s
Concurrent Session	10,000,000
Interface	
Standard interfaces	8×GE Combo + 4×GE RJ45 + 4×GE SFP + 6×10GE SFP+
Deployment mode	In-path deployment; off-path deployment (static traffic diversion); off-path deployment (dynamic traffic diversion)
Function form	Cleaning or detection, which can be switched using commands
Bypass card	Supported
Dimensions and weight	
Dimensions (H×W×D)	43.6mm × 442mm × 420mm
Weight	9.3kg
Power supply and operating environment	
Power supply mode	Rated input voltage: AC: 100 V to 240 V, 50 Hz/60 Hz Maximum input voltage: AC: 90 V to 290 V, 47 Hz to 63 Hz
Power	242W
Power supply redundancy	AC: power modules in 1+1 redundancy mode
Operating temperature	0°C to 45°C (long term), -5°C to +55°C (short term)
Storage temperature	-40°C to +70°C
Relative operating humidity	5%RH-95%RH, non-condensing
Storage relative humidity	5%RH-95%RH, non-condensing

Model	AntiDDoS1905
Certification	
Security authentication	Electromagnetic compatibility (EMC) CB, CCC, CE-SDOC, ROHS, REACH&WEEE(EU), C-TICK, ETL, FCC&IC, VCCI, and BSMI

Purchase Information

Model	Description
Host	
AntiDDoS1905-AC	AntiDDoS1905 AC Host (8 × GE Combo + 4 × GE RJ45 + 10 × 10GE SFP+, Dual Power Modules)
Management center	
AntiDDoS1000-F-Lic-N1	AntiDDoS1000 basic function package, per device
AntiDDoS1000-F-SnS1Y-N1	AntiDDoS1000 Basic Function Package, 1-Year SnS, Per Device
License	
LIC-ADS1905-CLN10G	AntiDDoS1905 10G cleaning capability
LIC-ADS1905-DET10G	AntiDDoS1905 10G detection capability