Huawei HiSecEngine AntiDDoS12000 Series Products

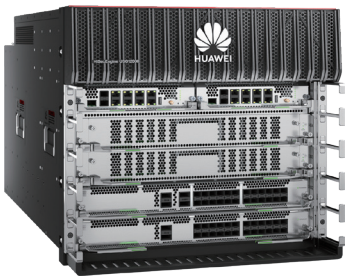
While the whole world is enjoying substantial benefits brought by the growing use of IPv6 and 5G networks, this also gives rise to the ramp-up of DDoS attacks. Attacks are emerging as services and initiated from dedicated platforms, facilitating the sharing of botnets. Against this backdrop, DDoS attacks are upgraded to a high level that feature heavier traffic, higher frequency, and greater complexity. In recent years, DDoS attacks have developed new characteristics:

- **Constant terabit-level attacks:** Attacks are increasing in both frequency and bandwidth consumption. The peak attack size reached up to 1.7 T/bits in 2018.
- **Diversified attacks:** Complex attacks, such as combined SYN flood attacks, fast flood attacks, pulse wave attacks, and hit and run attacks, occur frequently.
- **Impersonated attacks:** Attacks from real sources simulate access behaviors of authorized users, featuring a slow speed.

To effectively cope with DDoS attacks in the new era, Huawei rolls out the HiSecEngine AntiDDoS12000 series products. Equipped with a distributed hardware platform, the HiSecEngine AntiDDoS12000 products provide industry-leading security protection performance and expansion capabilities. A single HiSecEngine AntiDDoS12000 delivers up to 2.4 Tbit/s defense capability, effectively defending against heavy-traffic DDoS attacks. It can respond to complex DDoS attacks, such as combined SYN flood attacks, fast flood attacks, pulse wave attacks, and hit and run attacks, within seconds or even milliseconds, blocking such attacks in a timely manner. With full traffic collection and L3/L4/L7 per-packet analysis capabilities, the product can defend against over 100 types of attacks, providing the most accurate and comprehensive attack detection.

HUAWEI

Product Appearances



AntiDDoS12004

AntiDDoS12008

Highlights

- **Ultra-high performance:** Built on the industry-leading hardware architecture, a single HiSecEngine AntiDDoS12000 delivers a 2.4 Tbit/s DDoS attack protection capability, which is the highest in the industry.
- **Ultra-fast response:** The product can effectively respond to new types of DDoS attacks within seconds or even milliseconds, which is the fastest in the industry.
- **Accurate defense:** With full traffic collection and per-packet analysis capabilities, the product provides accurate defense against hundreds types of DDoS attacks.

Solution Benefits

Defense against high-volume DDoS attacks

- Using a distributed hardware platform, the product provides industry-leading service processing capabilities and scalability. A single HiSecEngine AntiDDoS12000 delivers a 2.4 Tbit/s DDoS attack defense capability.
- It can respond to attacks within milliseconds, quickly blocking DDoS attacks.

All-round DDoS attack protection

- 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 provides multiple defense methods, such as source authentication, behavior analysis, and rate limiting, to effectively and accurately defend against multiple attacks from real sources.
- The product can defend against over 100 types of attacks, effectively protecting web, DNS, DHCP, VoIP, and other key service systems.

IPv4/IPv6 dual-stack DDoS protection

- Supports IPv4/IPv6 dual-stack DDoS attack defense, eliminating the need for switching between protocols.

- Supports IPv4/IPv6 defense policy configuration and displays traffic statistics in reports.

Associated DDoS protection between the local device and the cloud

- On-premises devices are always online, protecting customers' services.
- When a link is congested, the on-premises device can automatically send signals to the cloud to start the cloud cleaning service, protecting links on customer networks.
- By interworking with more than 10 cleaning centers around the world, the product delivers over 2 Tbit/s cloud cleaning capabilities and responds to attacks within minutes.

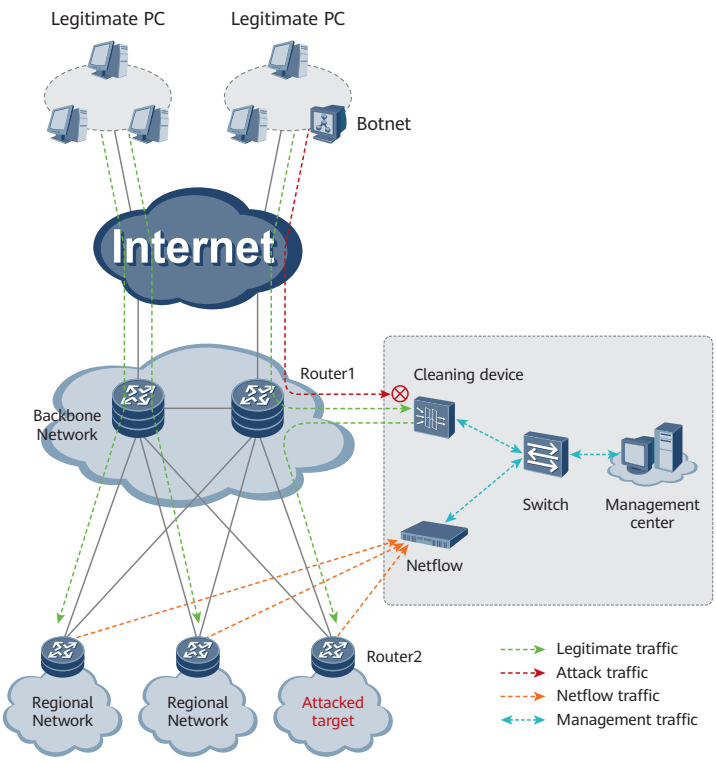
Value-added operations

- Tenant-specific automatic and manual defense policies for comprehensive protection
- Tenant-specific report statistics collection and reports sending via email, simplifying management
- Self-service portal for tenants, enhancing tenant loyalty
- Differentiated operations at a scale of 100,000 tenants

Typical Scenarios

MAN Protection

A metropolitan area network (MAN) provides a platform on which comprehensive services of a city are transmitted. Typically applying to large and medium-sized cities, a MAN provides a common and public network architecture and allows data, voice, images, and videos to be effectively transmitted at high speeds, meeting ever-changing requirements of Internet applications.

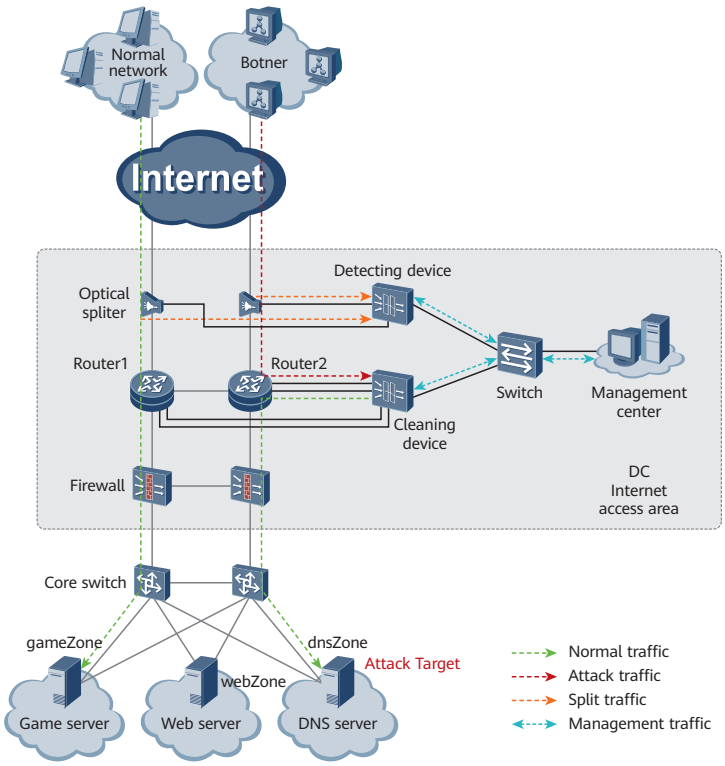


As shown in the figure, the NetFlow device collects NetFlow logs of routers in real time and determines whether there are anomalies in network traffic. When detecting a traffic anomaly, the

NetFlow device instructs the cleaning device to start cleaning. The cleaning device is attached to the core router Router1 in bypass mode 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. Only one interface of the cleaning device is directly connected to Router1. Traffic is diverted through the main interface and injected through the sub-interface. Traffic can be injected through other interfaces if there are sufficient interfaces.

Data Center Protection and Operations

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 bypass mode to detect and clean the traffic destined for the Zone. Downstream traffic destined for the Zone is diverted to the cleaning device in real time for detection and cleaning through BGP diversion. 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.

The SecoManager supports secure operations. The SecoManager allows administrators to configure defense policies based on tenants' service characteristics. When an attack occurs, the SecoManager automatically enables defense and sends alarms to administrators by mail. Tenants can log in to the portal to query attack and defense information. IDC carriers can design business models based on tenants, implementing value-added services.

Specifications

DDoS Protection 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	**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.
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	

Management and Report Functions

Management functions: Account management and permission allocation; defense policy configuration and displaying statistics in reports based on Zones (support of up to 100,000 Zones, namely, tenants); device performance monitoring; source tracing and fingerprint extraction through packet capturing; email, short message, and audio 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 source IP address; 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

Traffic Diversion and Injection Functions

Deployment mode In-path and off-path deployment	Traffic diversion and injection 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	AntiDDoS12004	AntiDDoS12008
Performance		
Defense Performance	Up to 600Gbps/300Mpps	Up to 2.4Tbps/600Mpps
New Sessions/Second	2,000,000/s per CPU	
Concurrent Session	80,000,000 per CPU	
Interfaces		
Number of MPU slots	2	
Number of extension slots	4	8

Model	AntiDDoS12004	AntiDDoS12008
LPU	24-port 10GBase LAN/WAN-SFP+ + 4-port 100GBase-QSFP 24-port 10GBase LAN/WAN-SFP+ + 2-port 100GBase-QSFP 48-port 10GBase LAN/WAN-SFP+	24-port 10GBase LAN/WAN-SFP+ + 4-port 100GBase-QSFP 24-port 10GBase LAN/WAN-SFP+ + 2-port 100GBase-QSFP 48-port 10GBase LAN/WAN-SFP+ 18-port 100GBase-QSFP
Dimensions and Weight		
Dimensions (H×W×D)	442mm × 874mm × 438mm (9.8U)	442mm × 874mm × 703mm (15.8U)
Weight	DC chassis: 81 kg (empty configuration) AC chassis: 76 kg (empty configuration)	DC chassis: 147.2 kg (empty configuration) AC chassis: 144.6 kg (empty configuration)
Power Supply and Operating Environment		
Power supply	Rated input voltage: • DC: -48 V/-60 V • AC: 220 V, 50 Hz/60 Hz • High-voltage DC: 240 V/380 V Maximum input voltage: • DC: -40 V to -72 V • AC: 176 V to 290 V, 45 Hz to 65 Hz • High-voltage DC: 188 V to 288 V/260 V to 400 V	
Power (entire system)	Maximum power consumption: 2226 W Typical power consumption: 1129 W Static power consumption: 771 W	Maximum power consumption: 8496 W Typical power consumption: 5007 W Static power consumption: 3278 W
Power module redundancy	N+1	
Operating temperature	0°C to 45°C (long term), -5°C to +50°C (short term)	
Storage temperature	-40°C to +70°C	
Relative operating humidity	5% to 85% RH, non-condensing (long term); 5% to 95% RH, non-condensing (short term)	
Storage relative humidity	0% to 95% RH	

Ordering Information

Model	Description
Main Equipment	
ADS12004-AC-B02	AntiDDoS12004 AC Basic Configuration(include AC Chassis, 2*MPU, 2*PM, Full Configuration FAN)

Model	Description
ADS12004-DC-B02	AntiDDoS12004 DC Basic Configuration(include DC Chassis, 2*MPU, 2*PM, Full Configuration FAN)
ADS12008-AC-B02	AntiDDoS12008 AC Basic Configuration(include AC Chassis, 2*MPU, 2*PM, Full Configuration FAN)
ADS12008-DC-B02	AntiDDoS12008 DC Basic Configuration(include DC Chassis, 2*MPU, 2*PM, Full Configuration FAN)
Service Processing Unit	
AntiDDoS12000-SPUB-ADS-01	AntiDDoS12000 Service Processing Unit 1
AntiDDoS12000-SPUB-ADS-02	AntiDDoS12000 Service Processing Unit 2
AntiDDoS12000-SPCB-ADS-01	AntiDDoS12000 Protection Service Card 1
AntiDDoS12000-SPCB-ADS-02	AntiDDoS12000 Protection Service Card 2
Line Processing Unit	
LPUA-18CQ	18 Port 100GBase-QSFP+ Interface Card
LPUA-48XS	48 Port 10GBase LAN/WAN-SFP+ Interface Card
LPUA-4CQ-24XS	24 Port 10GBase LAN/WAN-SFP+ + 4 Port 100GBase-QSFP+ Interface Card
LPUA-2CQ-24XS	24 Port 10GBase LAN/WAN-SFP+ + 2 Port 100GBase-QSFP+ Interface Card
Management Software	
AntiDDoS12000-F-Lic-N1	AntiDDoS12000 basic function package, per device
AntiDDoS12000-F-SnS1Y	AntiDDoS12000 Basic Function Package, 1-Year SnS, Per Device