Huawei HiSecEngine AntiDDoS12000-F Series Products

Superb Performance, Millisecond-Level Response, Precise Protection, and Intelligent Driving

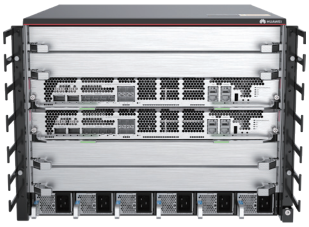
With the rapid development of the Internet, tactics that hackers use to carry out attacks are evolving and competition within many industries is also growing more vicious. Against this backdrop, DDoS attacks are dramatically rising in intensity, frequency, and complexity, presenting many new challenges, including the following:

- Intensified attacks are increasing the defense costs.
- Fast flooding of heavy-traffic attacks is challenging the response speed of the defense system.
- A diverse range of services and complex attacks are making traditional defense technologies outdated.

To tackle these new challenges, Huawei unveiled the HiSecEngine AntiDDoS12000-F series products featuring:

- Per-packet detection capability for all traffic and over 60 traffic models, allowing for effective response to DDoS attacks within milliseconds.
- Network Processor (NP)-boosted defense acceleration, efficiently blocking network-layer attacks.
- 7-layer intelligent filtering capability, multi-dimensional behavior analysis, and machine learning, accurately identifying various complex Challenge Collapsar (CC) attacks.
- Unique defense engine that allows online upgrade, rapidly guarding against 0-day DDoS attacks.
- Automatic policy tuning, implementing automatic driving during defense.

Product Appearances



AntiDDoS12004-F

AntiDDoS12008-F

Highlights

- **Superb performance:** NP-boosted defense acceleration powered by collaborative processing with CPU, efficiently blocking network-layer attacks with low costs.
- **Millisecond-level response:** Per-packet detection capability for all traffic, over 60 traffic models, and millisecond-level response to attacks, causing no impact to services.
- **Precise protection:** 7-layer intelligent filtering capability + multi-dimensional machine learning to filter attacks at Layer 3/4/7; unique defense engine that allows online upgrade, fast blocking 0-day DDoS attacks; three-layer defense architecture, responding to carpet-bombing attacks in seconds.
- **Intelligent driving:** Policy templates that combine extensive expert experience, and defense effect evaluation + automatic policy tuning, implementing automatic driving during defense.

Solution Overview

Defense against network-layer DDoS attacks

- With carrier-class hardware architecture as well as NP-boosted defense acceleration powered by collaborative processing with CPU, the AntiDDoS12000-F can defend against heavy traffic.
- By capitalizing on full traffic collection and per-packet detection capabilities, as well as over 60 traffic models, the AntiDDoS12000-F can respond to attacks within milliseconds and block network-layer attacks rapidly, ensuring the availability of network links.

Defense against application-layer DDoS attacks

- Based on multi-dimensional behavior analysis and machine learning, the AntiDDoS12000-F is able to accurately defend against HTTP/HTTPS CC attacks as well as encryption attacks without decryption, delivering higher performance.

- This product series offers all-round protection against session-layer and application-layer attacks, safeguarding mission-critical service systems such as websites, APPs, APIs, and DNS.

Value-added services

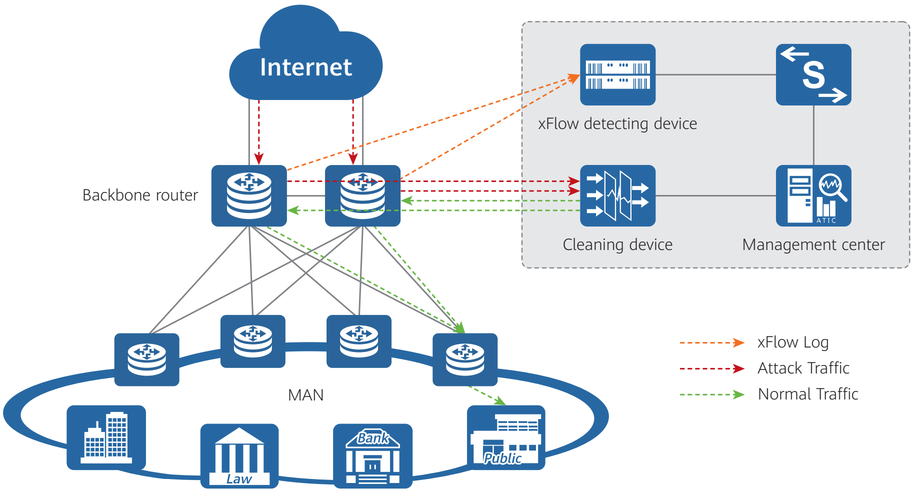
- Differentiated protection and report management based on tenant services and the protection bandwidth.
- Open APIs and syslogs for easy integration with third-party operation platforms to deliver defense policies and display reports.

Typical Scenarios

MAN Protection

The surge in heavy-traffic DDoS attacks is squeezing the significant bandwidth of carrier networks, causing growing complaints from enterprises. In addition, frequent DDoS attacks targeting DNS is threatening the availability of network infrastructure. Against this backdrop, it has become a necessity to deploy DDoS mitigation systems on carrier networks to protect the availability of network channels and infrastructure.

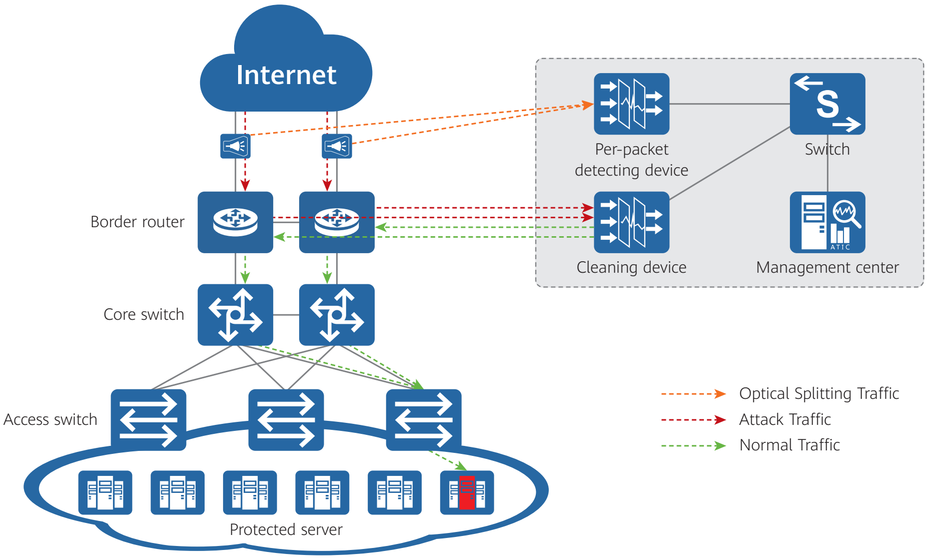
As shown in the figure, the xFlow detecting device collects and analyzes the xFlow logs generated by the routers in real time to detect DDoS attacks on the protected network. Once a DDoS attack is detected, the detecting device reports an alarm to the management center, triggering the cleaning device to advertise a traffic-diversion route to divert the attack traffic. The traffic is then diverted to the cleaning device for filtering. Finally, the cleaned traffic is sent back to the original network after processing.



Data Center Protection

The vicious competition in the industry has turned data centers the worst affected area by DDoS attacks. The services of the attacked IP addresses become unavailable in the event of a DDoS attack, and in severe cases, the availability of the data center network infrastructure may be threatened. Therefore, defense against DDoS on the network border becomes the very first and necessary barrier for data centers.

As shown in the figure, the AntiDDoS device is deployed at the network border in off-path mode and sends the traffic of the protected network to the detecting device through 1:1 optical splitting or mirroring for per-packet detection in real time. Once a DDoS attack is detected, the detecting device reports an alarm to the management center, triggering the cleaning device to advertise a traffic-diversion route to divert the attack traffic. The traffic is then diverted to the cleaning device for filtering. Finally, the cleaned traffic is sent back to the original network after processing. This solution causes no single-point failure, and only the attack traffic needs to be diverted to the cleaning device, ensuring the highest reliability.



Value-added Operation

The management center supports tenant-level anti-DDoS service operations. The system configures defense policies and displays reports based on Zones, which correspond to particular tenants, so that ISPs can provide differentiated anti-DDoS services based on tenant service types and the protection bandwidth. The management center can interconnect with third-party operation platforms through RESTful APIs to implement defense policies, or through multi-dimensional syslogs to display attack logs and defense effect reports.

Specifications

DDoS Mitigation Functions

Defense against malformed-packet attacks

Defense against LAND, Fraggle, Smurf, WinNuke, Ping of Death, Teardrop, and TCP error flag attacks

Defense against scanning and sniffing attacks

Defense against port scan and IP sweep attacks, and attacks using Tracert packets and IP options, such as IP source route, IP timestamp, and IP route record options

Defense against network-layer flood 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 Malformed flood, UDP Fragment flood, IP flood, ICMP Fragment flood, ICMP food, Other flood, carpet-bombing flood, and pulse-wave attacks

Defense against session-layer attacks

Defense against common session-layer attacks, such as real-source SYN flood, real-source ACK flood, TCP connection exhaustion, sockstress, and TCP null connection attacks

Defense against UDP reflection attacks

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

Dynamic generation of filtering rules to defend against new UDP amplification attacks

Defense against TCP reflection attacks

Static filtering rules that are created based on network-layer characteristics

TCP reflection attack filtering rules that are dynamically generated

Defense against application-layer attacks for protecting websites, APPs, and APIs/Defense against HTTP CC attacks

Defense against high-frequency application-layer attacks (HTTP and HTTP CC attacks) based on behavior analysis

Defense against low-frequency application-layer attacks (HTTP and HTTP CC attacks) based on machine learning

Defense against slow-rate HTTP attacks based on behavior analysis, including HTTP slow header, HTTP slow post, RUDY, LOIC, HTTP multi-methods, HTTP Range request amplification, and HTTP null connection attacks

Defense against encrypted application-layer attacks for protecting websites, APPs, and APIs/Defense against HTTPS CC/TLS encrypted attacks/Defense against QUIC Flood

Defense against high-frequency HTTPS/TLS encrypted attacks

Defense against slow-rate incomplete TLS session and null connection attacks

Defense against QUIC Flood

Defense against application-layer attacks (DNS)

Defense against DNS malformed flood, DNS query flood, NXDomain flood, DNS reply flood, and DNS cache poisoning attacks

Source-based rate limiting and domain name–based rate limiting

Defense against application-layer attacks (SIP)

Defense against SIP flood/SIP methods flood attacks, including Register, Deregistration, Authentication, and Call flood attacks

Source-based rate limiting

User-defined filtering rules

User-defined filtering rules for local software and hardware, as well as BGP FlowSpec rules for remote filtering. The fields can be customized, including source/destination IP address, packet length, IP protocol, IP payload, source/destination port, TCP flag bit, TCP payload, UDP payload, ICMP payload, DNS domain name, HTTP URI, HTTP field user-agent, as well as caller and callee in the SIP protocol.

Geographical location filtering

The blocking policy can be customized. For countries outside china, blocking policies can be customized based on country. In China, blocking policies can be customized based on province.

Dual-stack defense

IPv4/IPv6 dual-stack defense against DDoS attacks

Automatic tuning of defense policies

Attack traffic snapshot, defense effect evaluation, and automatic tuning of defense policies

Automatic attack evidence collection

Synchronization of policy templates from the cloud

Baseline learning

Support for dynamic traffic baseline learning and intelligent noise reduction to avoid baseline pollution. The learning period is configurable.

Packet capture-based evidence collection

Automatic packet capture based on attack events and user-defined ACLs

Online parsing and analysis, source tracing, and local analysis after downloading for captured packets

Management and Report Functions

Management functions

- Unified policy management, performance monitoring, and alarm management for multiple AntiDDoS devices
- Rights- and domain-based user permission management
- Notification of attack events by message, audio, and email
- Log audit and storage by third-party platforms after forwarding

Report functions

- Multi-dimensional traffic statistics analysis, including traffic comparison, top N traffic, and protocol type distribution
- Multi-dimensional attack event analysis, including attack details, top N attacks, and top N attack events
- Multi-dimensional attack situation analysis, including attack type distribution, peak traffic distribution, and duration distribution
- Report display of carpet-bombing attack defense
- Report display of attack sources
- Report data export

Value-added operation

- Zone customization and configuration of customized protection address segments and protection bandwidth
- Customized defense policies
- Customized reports
- Tenant-based portal

Third-party platform interconnection

- Log and report interconnection based on syslogs
- Defense policy interconnection based on RESTful APIs

Deployment Mode and Traffic Diversion and Injection

Deployment mode

- In-path deployment and off-path deployment (static traffic diversion, per-packet detection + dynamic traffic diversion, and xFlow detection + dynamic traffic diversion)

Traffic diversion and injection

- Traffic diversion: supports static traffic diversion based on PBR and BGP and dynamic traffic diversion based on BGP.
- Traffic injection: supports multiple injection modes, such as Layer 2 injection, static route injection, PBR-based injection, GRE tunnel injection, SRv6 injection, and MPLS LSP/VPN injection.

Interface and Hardware Specifications

Model	AntiDDoS12004-F	AntiDDoS12008-F
Interfaces		
Slots of main control unit	2	
Main control unit	Supports 1×100GE QSFP28/2×40GE QSFP+/4×25G SFP28/8×10G SFP+ ports	
Number of extended slots	4	8
LPU	2×40G/100GBase-QSFP28 + 12×100M/1G/10GBase-SFP+ 24×FE/1G/10GBase-SFP+	

Model	AntiDDoS12004-F	AntiDDoS12008-F
Defense Performance		
Maximum defense bandwidth	300 Gbps	600 Gbps
Maximum defense packet rate	200 Mpps	400 Mpps
Dimensions and Weight		
Dimensions (H×W×D)	352.8mm × 442mm × 515.5mm (8U)	575mm × 442mm × 515.5mm (13U)
Weight	31.3 kg (empty chassis)	48.94 kg (empty chassis)
Power Supply and Operating Environment		
Power supply	Rated input voltage: • DC: -48 V DC/-60 V DC/48 V DC • AC: 110 V AC/220 V AC, 50/60Hz • High-voltage DC: 240 V DC Maximum input voltage: • DC: -38.4 V DC to -72 V DC • AC: 90 V AC to 290 V AC, 45 Hz to 65 Hz • High-voltage DC: 190 V DC to 290 V DC	
Maximum power consumption	1560 W (full configuration)	2914 W (full configuration)
Power module redundancy	N+1	
Fan module redundancy	1+1 backup	
Airflow	Front-to-back airflow	
Long-term operating temperature	-5°C to 45°C (altitude: -60m to 1800m)	
Storage temperature	-40°C to 70°C	
Long-term relative operating humidity	5% to 95% RH, non-condensing	
Altitude for storage	< 5000m	

Ordering Information

Model	Description
Host	
ADS12004-F-AC-B01	ADS12004-F AC Basic Configuration (including assembly chassis, 2*SRUA HTM, 2*3000W AC Power, overseas)
ADS12004-F-DC-B01	ADS12004-F DC Basic Configuration (including assembly chassis, 2*SRUA HTM, 2*2200W DC Power, overseas)

Model	Description
ADS12008-F-AC-B01	ADS12008-F AC Basic Configuration (including assembly chassis, 2*SRUB HTM, 2*3000W AC Power, overseas)
ADS12008-F-DC-B01	ADS12008-F DC Basic Configuration (including assembly chassis, 2*SRUB HTM, 2*2200W DC Power, overseas)
Service Processing Unit	
SPUF-ADS-01	AntiDDoS12000-F Processing Board-01
SPUF-ADS-02	AntiDDoS12000-F Processing Board-02
SPUF-ADS-03	AntiDDoS12000-F Processing Board-03
Line Processing Unit	
LPUF-U-2CQ-12XS	2-port 40G/100GBase-QSFP28 and 12-port 100M/1G/10GBASE-X SFP+ interface card
LPUF-USG-24XS	24-port 100M/1G/10GBASE-X interface card(SFP+)
Management Software	
N1-AntiDDoS12000-F-Lic	N1-AntiDDoS12000 Foundation, Per Device
N1-AntiDDoS12000-F-SnS1Y	N1-AntiDDoS12000 Foundation, SnS, Per Device, 1 Year
LIC-ADS12000F-DET10G	Capability for Detecting (a multiple of 10G)(Applies to AntiDDoS12000F)
LIC-ADS12000F-CLN10G	Capability for Cleaning (a multiple of 10G)(Applies to AntiDDoS12000-F)

GENERAL DISCLAIMER

The information in this document may contain predictive statement including, without limitation, statements regarding the future financial and operating results, future product portfolios, new technologies, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.