

Huawei HiSecEngine AntiDDoS12000 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- A diverse range of services and complex attacks are making traditional defense technologies outdated.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 series products featuring:

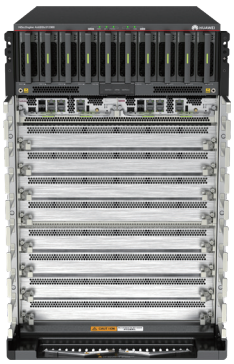
- Per-packet detection capability for all traffic and over 60 traffic models, allowing for effective response to DDoS attacks within milliseconds.
- Network Processor (NP)-boosted defense acceleration and up to 2.4 Tbps defense for each standalone device, efficiently blocking network-layer attacks.
- 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.

HUAWEI

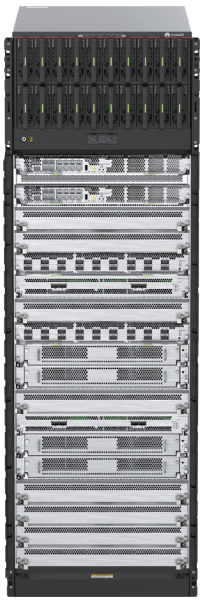
Product Appearances



AntiDDoS12004



AntiDDoS12008



AntiDDoS12016

Highlights

- **Superb performance:** NP-boosted defense acceleration powered by collaborative processing with CPU, ensuring up to 2.4 Tbps defense for each standalone device.
- **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 can achieve up to 2.4 Tbps defense.
- By capitalizing on full traffic collection and per-packet detection capabilities, as well as over 60 traffic models, the AntiDDoS12000 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 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

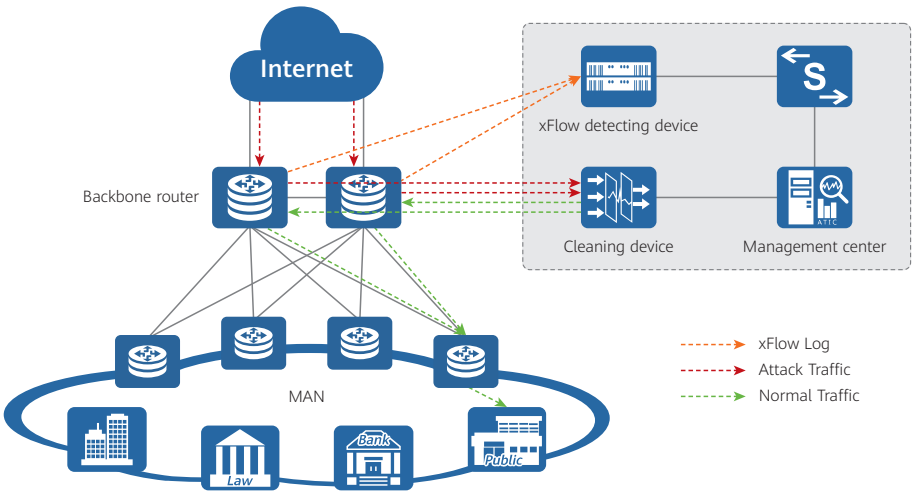
- Differentiated protection and report management based on tenant services and the protection bandwidth.
- Open APIs and syslogs for easy integration with third-party operation platforms to deliver defense policies and display reports.

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.

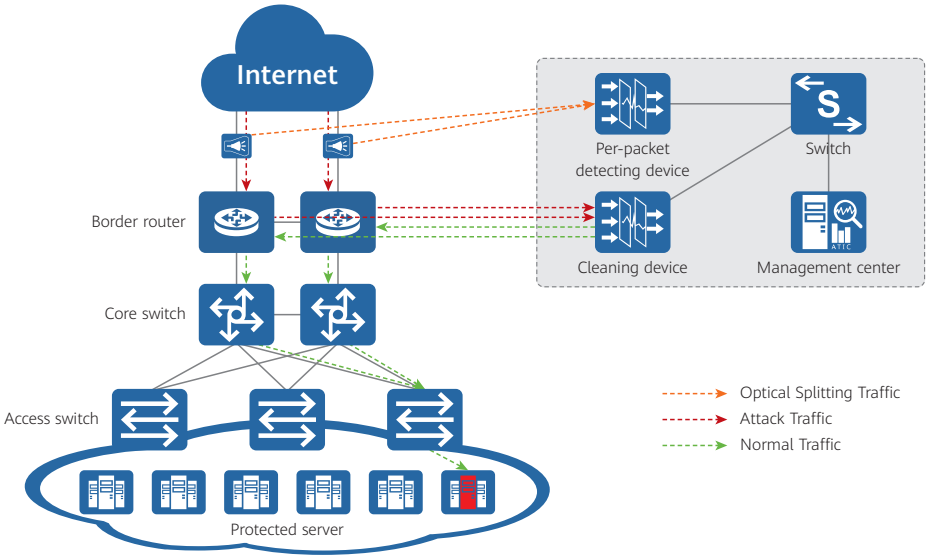
As shown in the figure, the xFlow detecting device collects and analyzes the xFlow logs generated by the routers in real time to detect DDoS attacks on the protected network. Once a DDoS attack is detected, the detecting device reports an alarm to the management center, triggering the cleaning device 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.

Defense Functions

Attack Protections	
Malformed packet • LAND • Fraggle • Smurf • Winnuke • Ping of Death • Tear Drop, Targa3, Jolt2, Nestea • TCP Error Flag • Malformed IPv6 Extend Header • IPv6 Extend Header Order Check • IPv6 Extend Headers Check	Scanning and sniffing attacks • Address Scanning • Port Scanning • Tracert Control Packet • IP Source Routing Option • IP Timestamp Option • IP Route Record Option

Network-layer flood attacks

- SYN Flood
- SYN-ACK Flood
- ACK Flood
- FIN/RST Flood
- TCP Fragment Flood
- TCP Malformed
- Steam Flood
- UDP Malformed
- UDP Flood
- UDP Fragment Flood
- IP Flood
- NDP Flood
- ICMP Flood
- ICMP Fragment Flood
- Other Flood
- IP Fragment Flood

TCP state exhaustion attacks

- Real Source SYN Flood
- TCP Connection Exhaustion
- Sockstress
- TCP Null Connection
- Real Source ACK Flood
- Network-layer CC
- Slow Network-layer CC

Website, APP, and API application-layer attacks

- HTTP Flood: Includes HTTP GET Flood, HTTP POST Flood, HTTP HEAD Flood, etc.
- LOIC
- HOIC
- XOIC
- HULK
- XerXes
- HTTP Slow Header (Slowloris, Pylori, HTTPDoSTool, Slowhttptest)
- HTTP Slow Post(RUDY, R-U-Dead-Yet)
- HTTP Slow Read
- HTTP Multi-Methods
- HTTP Pipelining Attack
- HTTP Range Amplification
- HTTP Null Connection
- HTTPS Flood
- TLS Encrypted Attack
- SSL Renegotiation
- THC-SSL Attack
- Incomplete TLS Session
- TLS NULL Connetion
- Slow HTTP CC
- Slow HTTPS CC
- QUIC Flood
- HTTP/2 Multiplexing Attack
- HTTP/2 Rapid Reset Attack

Reflection attacks

- TCP Reflection: Includes SYN-ACK reflection and mixed TCP reflection consisting of SYN-ACK, ACK, RST-ACK, and RST.
- UDP Reflection: DNS, SSDP, NTP, CLDAP, Memcached, WSD, mDNS, NetBIOS, RIPv1, Portmapper, SNMP, SQL RS, Chargen, L2TP, Microsoft SQL Resolution Service, etc

SIP application-layer attacks

- SIP Flood
- SIP Methods Flood
- Register Flood
- Deregistration Flood
- Authentication Flood
- Call Flood

DNS application-layer attacks

- DNS Query Flood
- DNS NXDomain Flood
- DNS Malformed
- DNS Reply Flood

Complex attacks

- Fast Flooding
- Carpet-Bombing Attack
- Pulse-Wave Attack
- IPv4/IPv6 Dual-stack

Defense Actions

- Packet blocking
- Source authentication
- Blacklist
- Whitelist
- Connections limit (new connection, concurrent connection)
- Rate limit (SrcIP/DstIP, bps/pps)
- BGP flowspec
- Black hole
- Packet capture
- Cloud mitigation

Defense Countermeasures

- Black Lists
- White Lists
- IP Reputation
- Geo-IP Block/Limit
- Anti-spoofing
- SYN First-packet-drop
- SYN Challenge Authentication
- TCP Ratio Check
- ACK First-packet-drop
- ACK Session Detection
- ACK Behavior Analysis
- FIN/RST Session Detection
- TCP Malformed Packet Check
- Concurrent Connections Limit
- Connection Rate Limit
- TCP Abnormal Connections Detection
- TCP Rate Limit
- TCP Fragment Rate Limit
- UDP Malformed Packet Check
- UDP Payload Check
- UDP Payload Fingerprint Leaning
- UDP Watermark Check
- UDP Rate Limit
- UDP Fragment Rate Limit
- ICMP Rate Limit
- Other Rate Limit
- TCP Reflection Filtering Rules
- UDP Reflection Filtering Rules
- IP Pattern Matching
- TCP Pattern Matching
- UDP Pattern Matching
- HTTP URI Fingerprint
- HTTP Challenge Authentication(302-redirect, JavaScript, Cookie, CAPTCHA)
- HTTP Behavior Analysis
- HTTPS Challenge Authentication
- HTTP Pattern Matching
- TLS Fingerprints
- DNS Malformed Packet Check
- DNS Challenge Authentication
- DNS Passive Authentication
- DNS Request Rate Limit
- DNS Reply Rate Limit
- SIP Challenge Authentication
- SIP Rate Limit
- Dynamic Hardware Filtering Rules
- TCP Network Segment Rate Limit
- UDP Network Segment Rate Limit
- ICMP Network Segment Rate Limit
- Other Network Segment Rate Limit
- User-defined Zone Filtering Rule
- User-defined Hardware Filtering Rule
- BGP FlowSpec Rule
- Dynamic BGP FlowSpec
- Blackhole Route

User-defined Filtering Rules

- Zone Filtering Rule
- Hardware Filtering Rule
- BGP Flowspec rules
- ICMP Payload
- DNS Domain
- DNS QR

• Src/Dst IP • Packet Length • IP Protocol • IP Payload • Source/Destination Port • TCP-Flag • IP-ID • TCP-Flag • TCP Option • TCP Payload • UDP Payload	• DNS Type • HTTP Opcode • HTTP Cookie • HTTP HOST • HTTP URI • HTTP Referer • HTTP User-Agent • SIP Caller • SIP Callee
0-day DDoS Defense	
• Agile release of the defense engine, without service interruption during upgrade	
Threat Information	
• IP reputaion • Geo-IP	• Online upgrade
Deployment Mode	
• In-path deployment in transparent mode • Off-path deployment (static traffic diversion) • Off-path deployment (per-packet detection + dynamic traffic diversion) • Off-path deployment (xFlow detection + dynamic traffic diversion) • PBR-based traffic diversion • BGP-based static traffic diversion	• BGP-based dynamic traffic diversion • Layer-2 injection • Static route injection • PBR injection • GRE tunnel injection • SRv6 injection • MPLS LSP injection • MPLS VPN injection
Reliability	
• Link-Group • BFD (Bidirectional Forwarding Detection)	• NQA (Network Quality Analysis) • LACP (Link Aggregation Control Protocol)

SecoManager

Management	
• Unified management of multiple AntiDDoS devices • Device performance monitoring • User-defined real-time monitoring • Alarm management • Right- and domain-based management • Account policy	• Local authentication supports two-factor authentication. • Remote authentication supports LDAP and RADIUS. • Alarm notified by SMS, audio, and email • Log audit
Report	
• Traffic comparison • Top N traffic statistics • Traffic distribution by protocol type • TCP connection statistics • Traffic distribution by regions	• Attack event details • Top N attack events • Attack type distribution • Attack traffic trend • Distribution of dynamic blacklists by regions

Intelligent Defense	
• Scenario-based expert strategy template • Attack traffic and defense effect snapshot • Defense effect evaluation	• Automatic optimization of defense policies • Automatic attack packet capture • Online synchronization of policy templates
Packet Capture	
• Automatic packet capture based on attack event • Packet capture by user-defined ACL • Source tracing via packet capture files	• Downloading packet capture files • Online parsing and analysis of packet capture files
Baseline Learning	
• Dynamic traffic baseline learning	• User-defined learning cycle
• AI denoising	
Multi-tenant Management	
• User-defined zone, configuration ofprotected IP address and protection bandwidth • Tenant defense policy • Policy self-service and report self-service portal	• Tenant reports, and daily reports, weekly reports, monthly reports, and annual reports can be generated periodically and automatically pushed by emails.
Third-party Platform Integration	
• Syslog for log and report integration	• RESTful API for defense policy integration
Reliability	
• Remote disaster recovery deployment	• Cluster deployment

Interface and Hardware Specifications

Model	AntiDDoS12004	AntiDDoS12008	AntiDDoS12016
Interfaces			
Number of MPU slots	2		
Number of extended slots	4	8	16
LPU	• 24-port 10GBase-SFP+ + 2-port 40G/100GBase-QSFP28 • 48-port 10GBase-SFP+	• 24-port 10GBase-SFP+ + 2-port 40G/100GBase-QSFP28 • 48-port 10GBase-SFP+ • 4-port 400GBase-QSFP • 12-port 40G/100GBase-QSFP28 + 24-port 10GBase-SFP+ (Only four ports are provided by default. If needed, you can purchase 100G interface expansion RTUs for capacity expansion. Only a maximum of two 100GE ports can be added.)	• 24-port 10GBase-SFP+ + 2-port 40G/100GBase-QSFP28 • 48-port 10GBase-SFP+ • 4-port 400GBase-QSFP • 12-port 40G/100GBase-QSFP28 + 24-port 10GBase-SFP+ (Only four ports are provided by default. If needed, you can purchase 100G interface expansion RTUs for capacity expansion. Only a maximum of two 100GE ports can be added.)

Model	AntiDDoS12004	AntiDDoS12008	AntiDDoS12016
Defense Performance			
Maximum defense bandwidth	400 Gbps	1.2 Tbps	2.4 Tbps
Maximum defense packet rate	300 Mpps	900 Mpps	1800 Mpps
New connection rate	DDoS defense enabled: 1 million/s per CPU		
Maximum number of concurrent connections	DDoS defense enabled: 35 million/CPU		
Dimensions and Weight			
Dimensions (H×W×D)	438mm × 442mm × 874mm (9.8U)	703mm × 442mm × 874mm (15.8U)	1436mm x 442mm x 1033mm (32.3U)
Weight	DC chassis: 82.8 kg (empty chassis) AC chassis: 77.8 kg (empty chassis)	DC chassis: 101.8 kg (empty chassis) AC chassis: 95.8 kg (empty chassis)	DC chassis: 233.6kg (empty chassis) AC chassis: 222.6kg (empty chassis)
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		
Maximum power consumption	4696 W	10917 W	21834 W
Power module redundancy	N+1		
Fan module redundancy	N+1		
Airflow	Front-to-back airflow		
Long-term operating temperature	0°C to 40°C		
Storage temperature	-40°C to 70°C		
Long-term relative operating humidity	5% to 85% RH, non-condensing		
Relative storage humidity	5% to 85% RH, non-condensing		

Ordering Information

Model	Description
Host	
ADS12004-AC-B05	AntiDDoS12004 AC Basic Configuration (include AC Chassis, 2*MPUD, 2*PM, Full Configuration FAN, HTM, overseas)

Model	Description
ADS12004-DC-B05	AntiDDoS12004 DC Basic Configuration (include DC Chassis, 2*MPUD, 2*PM, Full Configuration FAN, HTM, overseas)
ADS12008-AC-B05	AntiDDoS12008 AC Basic Configuration (include AC Chassis, 2*MPUD, 4*SFUA, 2*PM, Full Configuration FAN, HTM, overseas)
ADS12008-DC-B05	AntiDDoS12008 DC Basic Configuration (include DC Chassis, 2*MPUD, 4*SFUA, 2*PM, Full Configuration FAN, HTM, overseas)
ADS12016-AC-B01	AntiDDoS12016 AC Basic Configuration (include AC Chassis, 2*MPUB, 4*SFU16A, 4*PM, Full Configuration FAN)
ADS12016-DC-B01	AntiDDoS12016 DC Basic Configuration (include DC Chassis, 2*MPUB, 4*SFU16A, 5*PM, Full Configuration FAN, HTM, overseas)
Service Processing Unit	
SPUB-ADS-01	AntiDDoS12000 Service Processing Unit B-01
SPUB-ADS-02	AntiDDoS12000 Service Processing Unit B-02
SPCB-ADS-01	AntiDDoS12000 Protection Service Card B-01
SPCB-ADS-02	AntiDDoS12000 Protection Service Card B-02
Line Processing Unit	
LPUA-4DQ	4-Port 400GBase-QSFP-DD Interface Card
LPUA-12CQ	12-Port 100GBase-QSFP28+24-Port 10GBase-SFP+ Interface Card (Only four ports are provided by default. If needed, you can purchase 100G interface expansion RTUs for capacity expansion. Only a maximum of two 100GE ports can be added.)
LPUA-48XS	48 Port 10GBase -SFP+ Interface Card
LPUA-2CQ-24XS	24 Port 10GBase -SFP+ + 2 Port 100GBase-QSFP28 Interface Card
Management Software	
N1-AntiDDoS12000-F-Lic	N1-AntiDDoS12000 Foundation, Per Device
N1-AntiDDoS12000-F-SnS1Y	N1-AntiDDoS12000 Foundation, SnS, Per Device, 1 Year
LIC-ADS12000-DET	Capability for Detection (a multiple of 10G)
LIC-ADS12000-CLN	Capability for Cleaning (a multiple of 10G)
LIC-ADS12000-LPU-400G	1*400GE ADS Interface Card Expansion license (Applies to 4-port 400GE interface board)
LIC-ADS12000-LPU-100G	1*100GE ADS Interface Card Expansion license (Applies to 12-port 100GE interface board)

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.
Copyright © 2023 HUAWEI TECHNOLOGIES CO., LTD. All Rights Reserved.