# 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- A diverse range of services and complex attacks are making traditional defense technologies outdated.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.
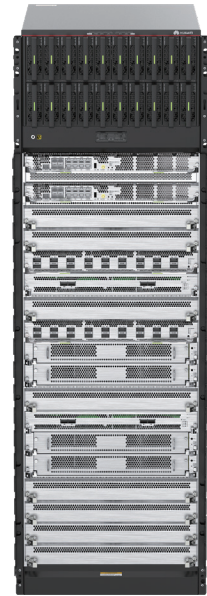- Automatic policy tuning, implementing automatic driving during defense.

HUAWEI

## Product Appearances
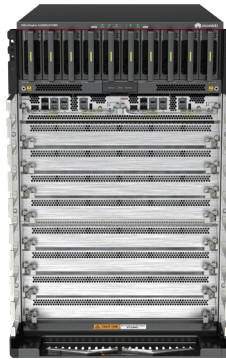
AntiDDoS12004          AntiDDoS12008          AntiDDoS12016

## 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.
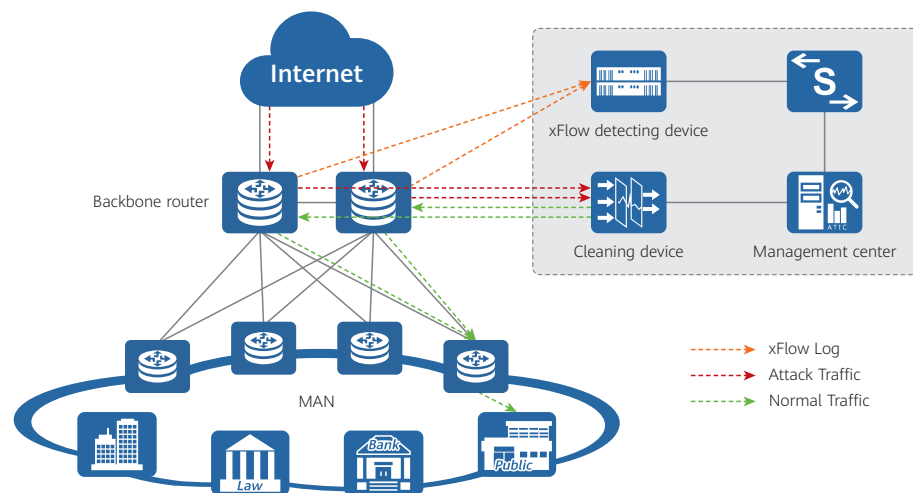


## Data Center Protection

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.
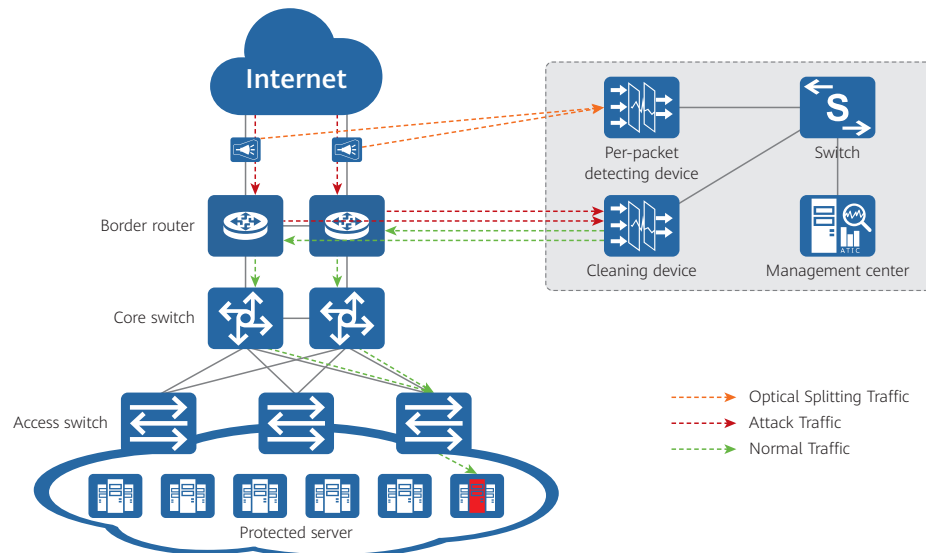


## Value-added Operation

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.

## 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 flood, 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 | Report functions |
|---|---|
| • Unified policy management, performance monitoring, and alarm management for multiple AntiDDoS devices<br>• Rights- and domain-based user permission management<br>• Notification of attack events by message, audio, and email<br>• Log audit and storage by third-party platforms after forwarding | • Multi-dimensional traffic statistics analysis, including traffic comparison, top N traffic, and protocol type distribution<br>• Multi-dimensional attack event analysis, including attack details, top N attacks, and top N attack events<br>• Multi-dimensional attack situation analysis, including attack type distribution, peak traffic distribution, and duration distribution<br>• Report display of carpet-bombing attack defense<br>• Report display of attack sources<br>• Report data export |
| **Value-added operation**<br>• Zone customization and configuration of customized protection address segments and protection bandwidth<br>• Customized defense policies<br>• Customized reports<br>• Tenant-based portal | **Third-party platform interconnection**<br>• Log and report interconnection based on syslogs<br>• Defense policy interconnection based on RESTful APIs |

## Deployment Mode and Traffic Diversion and Injection

| Deployment mode | Traffic diversion and injection |
|---|---|
| • In-path deployment and off-path deployment (static traffic diversion, per-packet detection + dynamic traffic diversion, and xFlow detection + dynamic traffic diversion) | • Traffic diversion: supports static traffic diversion based on PBR and BGP and dynamic traffic diversion based on BGP.<br>• 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 | AntiDDoS12008 | AntiDDoS12016 |
|---|---|---|---|
| **Interfaces** | | | |
| Number of MPU slots | 2 | | |
| Number of extended slots | 4 | 8 | 16 |

| Model | AntiDDoS12004 | AntiDDoS12008 | AntiDDoS12016 |
|---|---|---|---|
| LPU | • 24-port 10GBase-SFP+ + 2-port 40G/100GBase-QSFP28<br>• 48-port 10GBase-SFP+ | • 24-port 10GBase-SFP+ + 2-port 40G/100GBase-QSFP28<br>• 48-port 10GBase-SFP+<br>• 4-port 400GBase-QSFP<br>• 12-port 40G/100GBase-QSFP28 + 24-port 10GBase-SFP+<br>(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<br>• 48-port 10GBase-SFP+<br>• 4-port 400GBase-QSFP<br>• 12-port 40G/100GBase-QSFP28 + 24-port 10GBase-SFP+<br>(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.) |
| **Defense Performance** | | | |
| Maximum defense bandwidth | 400 Gbps | 1.2 Tbps | 2.4 Tbps |
| Maximum defense packet rate | 300 Mpps | 900 Mpps | 1800 Mpps |
| **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)<br>AC chassis: 77.8 kg (empty chassis) | DC chassis: 101.8 kg (empty chassis)<br>AC chassis: 95.8 kg (empty chassis) | DC chassis: 233.6kg (empty chassis)<br>AC chassis: 222.6kg (empty chassis) |
| **Power Supply and Operating Environment** | | | |
| Power supply | Rated input voltage:<br>• DC: -48 V/-60 V<br>• AC: 220 V, 50 Hz/60 Hz<br>• High-voltage DC: 240 V/380 V<br>Maximum input voltage:<br>• DC: -40 V to -72 V<br>• AC: 176 V to 290 V, 45 Hz to 65 Hz<br>• 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 | | |

| Model | AntiDDoS12004 | AntiDDoS12008 | AntiDDoS12016 |
|---|---|---|---|
| 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) |
| 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 |

| Model | Description |
|---|---|
| **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) |