Anti-DDoS Service

Service Overview

Issue	03
Date	2024-11-26

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Understanding DDoS Attacks

1.1 What Is a DDoS Attack?

DoS attacks are also called flood attacks. They intend to exhaust the network or system resources on the target computer, causing service interruption or suspension. Consequently, legitimate users fail to access network services. A DDoS attack involves multiple compromised computers controlled by an attacker flooding the targeted server with superfluous requests. **Table 1-1** describes the common DDoS attacks.

Table 1-1 Common DDoS attacks

Attack Type	Description	Example
Network layer attack	Occupies the network bandwidth with volumetric traffic, causing your service to be unable to respond to legitimate access requests.	NTP flood attack
Transport layer DDoS attack	Occupies the connection resources of the server, resulting in denial of services.	SYN flood, ACK flood, and ICMP flood attacks.
Session layer attack	Occupies SSL session resources of the server, resulting in denial of services.	SSL slow connection attack

Attack Type	Description	Example
Application layer attack	Occupies the application processing resources of the server and consumes its processing performance, resulting in denial of services.	HTTP GET flood attack and HTTP POST flood attack

1.2 Black Hole Policy

To protect the usability of Huawei Cloud services in general, if the attack traffic on the cloud server exceeds the threshold, a black hole will be triggered to block all accesses from the Internet for a certain period of time.

What Is a Black Hole?

A black hole refers to a situation where access to a cloud server is blocked by Huawei Cloud because attack traffic targeting a cloud server exceeds a certain threshold.

Why Is the Blackhole Policy Required?

DDoS attacks will interrupt user services and cause adverse impacts on the AAD data center. Defense against DDoS attacks is costly on bandwidth consumption.

Bandwidth is purchased by HUAWEI CLOUD from carriers, and those carriers bill for bandwidth even if it was part of DDoS attack. Huawei Cloud provides Cloud Native Anti-DDoS Basic (Anti-DDoS) for free to protect your resources against DDoS attacks below a certain threshold, but if an attack exceeds a certain size, we will route the traffic to a black hole.

How Do I Deactivate a Black Hole?

When a server (ECS) enters is put in the black hole, you handle it by referring to **Table 1-2**.

Table 1-2 Black hole deactivation methods

Anti-DDoS Edition	Deactivation Policy	Deactivation Method
Cloud Native Anti-DDoS Basic (Anti-DDoS) **NOTE** Anti-DDoS is enabled by default.	• The system automatically deactivates the black hole 24 hours after the access to a cloud server is blocked. • If the system detects that the attack has not stopped, and attack traffic is still exceeding the configured threshold, the access will be blocked again.	You need to wait until the system deactivates it automatically.

Black Hole Threshold

The black hole threshold refers to the basic attack mitigation capability provided by Huawei Cloud. When the scale of attack exceeds the threshold, Huawei Cloud executes a black hole policy to block the attacked IP address.

Scrubbing Principles

The system detects attack traffic in real time. Once detecting an attack on a cloud host, the system diverts the service traffic from the original network path to the Huawei Cloud DDoS scrubbing system. The Huawei Cloud DDoS scrubbing system identifies the traffic of the attacking IP address, discards attack traffic, and forwards normal traffic to the target IP address to mitigate the damage to the server.

Self-Service Unblocking Rules

- There is a minimum block duration after which you can unblock a blocked IP address. The minimum block duration for the first time you unblock an IP address in a day is 30 minutes. Minimum block duration = $2^{(n-1)}$ x 30 minutes (*n* indicates the number of times you want to unblock the same IP address)

  For example, a 30-minute block duration is required for the first time you unblock an IP address, a 60-minute block duration for the second time, and a 120-minute block duration for the third time.
- For the same protected IP address, if it is blocked again less than 30 minutes after it is unblocked, you can unblock it 2^n x 30 minutes later (*n* indicates the number of times you are unblocking it).

  For example, if the IP address has been unblocked once at 10:20, and is blocked again at 10:40, the interval between the two time points is less than

30 minutes. This is the second time you unblock the IP address on the day. The IP address cannot be unblocked until the 120-minute block duration expires at 12: 40 (2x2x30 minutes after 10:40).

NOTICE

If you have unblocked any other IP address within 30 minutes, you cannot unblock the IP address even if the preceding conditions are met.

- Anti-DDoS Service automatically adjusts the allowed IP unblocking attempts and the interval based on the risk control.

2 Understanding Anti-DDoS Service

2.1 What Is Cloud Native Anti-DDoS Basic

What Is Cloud Native Anti-DDoS Basic

Cloud Native Anti-DDoS Basic (CNAD Basic) defends public IP addresses (ECSs and ELBs) on Huawei Cloud against Distributed Denial of Service (DDoS) attacks, such as flood attacks and resource consumption attacks, at the network- and application-layer. It also provides real-time alarms for attack interception, effectively improving your bandwidth utilization and ensuring service stability and reliability.

NOTE

CNAD Basic does not support attack alarm notification and protection policy customization for public IP addresses of the GEIP and GA types.

Features

CNAD Basic monitors the service traffic from the Internet to public IP addresses and detects attack traffic in real time. It then scrubs attack traffic based on user-configured defense policies without interrupting services. It also generates monitoring reports that provide visibility into the network traffic security.

CNAD Basic helps users mitigate the following attacks:

- Web server attacks

  SYN flood attacks
- Game attacks

  Including User Datagram Protocol (UDP) flood, SYN flood, Transmission Control Protocol (TCP), and fragment attacks

CNAD Basic also:

- Monitors the security status of a single public IP address and offers a monitoring report, covering the current protection status, protection settings, and the traffic and anomalies within the last 24 hours.

- Provides attack reports on all protected public IP addresses, covering the traffic cleaning frequency, cleaned traffic amount, the top 10 attacked public IP addresses, and the number of blocked attacks.

2.2 Advantages

CNAD Basic mitigates DDoS attacks against workloads on Huawei Cloud. With CNAD Basic, you can enjoy:

- Premium protection

  Detects DDoS attacks in real time, discards attack traffic, and forwards legitimate traffic to destination IP addresses.

  Provides high-quality bandwidth to ensure service continuity and stability as well as user access speed.
- Complete and accurate protection

  A constantly updated database (carrying millions of blacklisted IP addresses) coupled with a 7-layer, smart cleaning mechanism ensures accurate traffic cleaning.
- Instantaneous response

  With industry-leading technology and powerful scrubbing devices, CNAD Basic checks each packet and responds to any attack immediately without causing service delays.
- Enabled automatically

  This service is automatically enabled when you purchase an EIP. No expensive scrubbing device or time-consuming installation is required.
- Free of charge

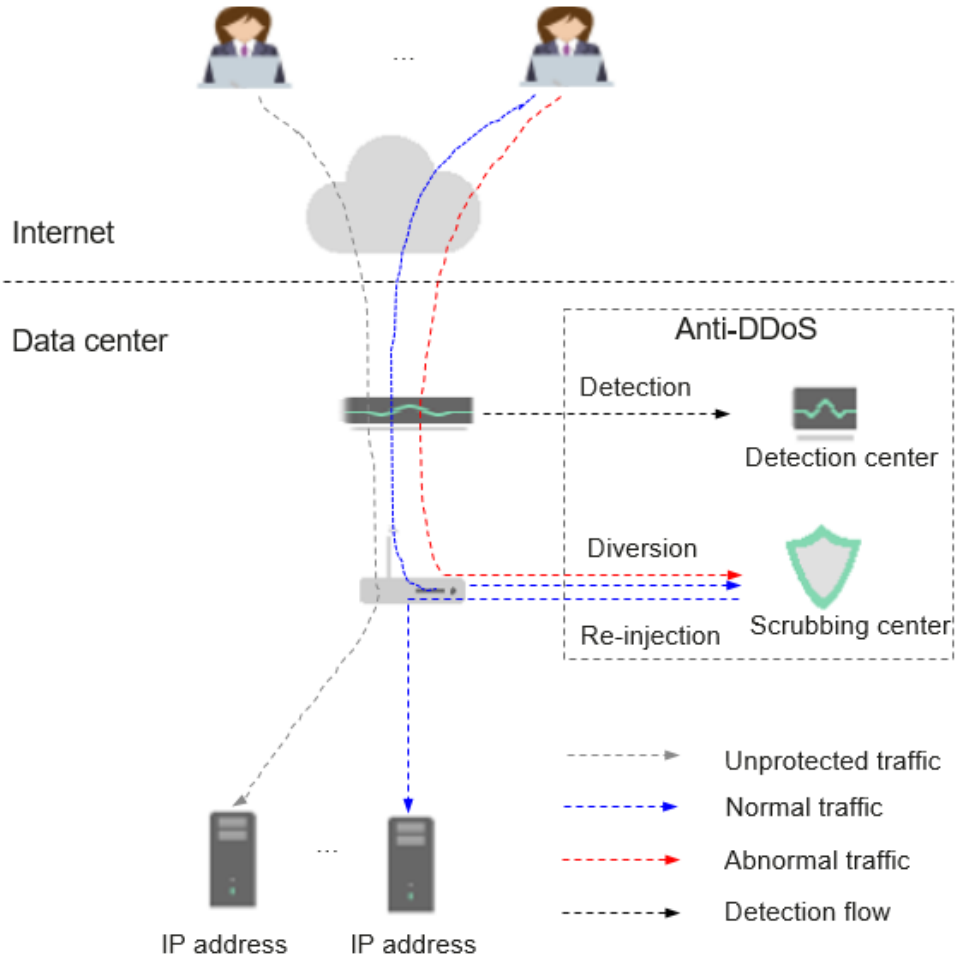
  This service is free. You can use the service without purchasing any additional resources.

2.3 Application Scenarios

CNAD Basic protects public IP addresses on Huawei Cloud only from DDoS attacks.

CNAD Basic devices are deployed at egresses of data centers. **Figure 2-1** shows the network topology.

Figure 2-1 Network topology



The detection center monitors network access traffic based on security policies you configure. If an attack is detected, data is diverted to scrubbing devices for real-time defense. Abnormal traffic is cleaned, and normal traffic is forwarded.

Anti-DDoS provides 500 Mbit/s of mitigation capability against DDoS attacks for free. If access traffic to a public IP address exceeds the specified black hole threshold (500 Mbit/s for free Anti-DDoS), CNAD Basic redirects all traffic destined for the IP address to a black hole. This means legitimate traffic will be discarded. To get more DDoS mitigation capabilities, Huawei Cloud Advanced Anti-DDoS (AAD) is recommended.

3 Pricing Details

Anti-DDoS is free of charge.

It defends your Huawei Cloud IP resources, including ECSs and ELB load balancers, against network- and application-layer distributed denial of service (DDoS) attacks, such as flood attacks and resource consumption attacks. Anti-DDoS improves your bandwidth utilization, provides real-time alarms, and helps keep your workloads stable and reliable.

4 Related Services

Anti-DDoS can protect public IP addresses. Its relationships with other cloud services are as follows:

Table 4-1 Related Services

Service	Relationship with Other Cloud Services
Cloud Trace Service (CTS)	After you enable CTS, CTS records DDoS mitigation operations for later query, audit, and backtrack.
Simple Message Notification (SMN)	Simple Message Notification (SMN) provides the notification function. When alarm notification is enabled, you will receive alarm messages by SMS or email if your IP address is DDoS attacked.
Log Tank Service (LTS)	Attack logs are recorded in Log Tank Service (LTS), which enable real-time decision making and analysis, device O&M management, and service trend analysis.
Cloud Eye Service (CES)	Cloud Eye monitors metrics related to Anti-DDoS Service. You can learn about the protection status in a timely manner and set corresponding protection policies based on the metrics in Cloud Eye.
Identity and Access Management (IAM)	Identity and Access Management (IAM) provides the permission management function for Anti-DDoS Service. Only users with required permissions can use Anti-DDoS Service.
Enterprise Project Management (EPS)	You can create enterprise projects based on the enterprise organization structure. Then you can manage resources across different regions by enterprise project, grant different permissions to user groups, and add them to enterprise projects. Anti-DDoS Service can be interconnected with EPS. You can manage Anti-DDoS Service resources by enterprise project and grant different permissions to users.

