Anti-DDoS

Service Overview

Issue	08
Date	2021-08-06

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei 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.

Contents

1 What Is Anti-DDoS?

The Anti-DDoS service protects public IP addresses against Layer 4 to Layer 7 distributed denial of service (DDoS) attacks and sends alarms immediately when detecting an attack. Anti-DDoS improves the bandwidth utilization and ensures the stable running of user services.

Anti-DDoS 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 service running. It also generates monitoring reports that provide visibility into the network traffic security.

2 Concepts

2.1 Black Hole Policy

A black hole will be triggered to block accesses from the Internet within a time range when a cloud server is under volumetric traffic attacks.

What Is a Black Hole?

A black hole refers to a situation where access to a cloud server is blocked by HUAWEI CLOUD because the attack traffic targeting the cloud server exceeds the configured black hole threshold. 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 traffic still persists and exceeds the threshold, the access will be blocked again.

The black hole service is purchased from the carrier, who has restrictions on the time and frequency of its deactivation. Therefore, the black hole cannot be manually deactivated. You need to wait until the system automatically deactivates it.

Why Is the Black Hole Policy Used?

DDoS attack mitigation is costly, especially in the bandwidth fees. Bandwidth is purchased by HUAWEI CLOUD from carriers. Carriers do not take the cleaned part out when charging HUAWEI CLOUD for bandwidth fees. HUAWEI CLOUD provides as much free defense as possible. However, when the attack traffic exceeds the threshold, it will route traffic to a black hole. To ensure service continuity, it is a better choice to purchase Advanced Anti-DDoS to expand protection capabilities.

2.2 Scrubbing Principle and Black Hole Threshold

HUAWEI CLOUD Anti-DDoS mitigates DDoS attacks and is enabled by default.

Scrubbing Principle

Anti-DDoS monitors service traffic in real time. Once an attack is detected, it diverts service traffic to the HUAWEI CLOUD Anti-DDoS scrubbing system, which identifies the traffic from that IP address, discards the attack traffic, and forwards legitimate traffic to the target IP address.

Black Hole Threshold

The black hole threshold refers to the basic attack mitigation capacity provided by HUAWEI CLOUD. When the scale of attack exceeds the threshold, HUAWEI CLOUD executes a black hole policy to block the IP address.

Anti-DDoS provides a 500 Mbit/s mitigation capacity against DDoS attacks free of charge. For applications threatened by attack traffic larger than 500 Mbit/s, it is a better choice to purchase the Advanced Anti-DDoS service on HUAWEI CLOUD to expand protection capacity.

2.3 Differences Between Anti-DDoS and Advanced Anti-DDoS

Anti-DDoS defends against most common DDoS attacks at no additional charge, whereas Advanced Anti-DDoS (AAD) provides expanded protection and expert support with subscription fees. For details, see **Table 2-1**.

Table 2-1 Differences between Anti-DDoS and Advanced Anti-DDoS

Item	Anti-DDoS	AAD
Charging	Free of charge	Charged
Protection capacity	A maximum of 500 Mbit/s protection capacity	A maximum of 1 Tbit/s protection capacity
Protected object	HUAWEI CLOUD resources only	On- and off-premises
Protection policy	● Fixed protection policies ● Globally applied policies	● Diverse protection policies ● Professional CC attack defense ● Customized policies
Key event assurance	None	Expert support (for VIP customers)
Detailed reports	Provides an overview report.	Provides a detailed report.
Technical support	24/7 online customer service	24/7 expert support service

2.4 Common DDoS Attacks

DoS attacks are also called flood attacks. They are intended 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 2-2** lists common DDoS attacks.

Table 2-2 Common DDoS attacks

Attack Type	Description	Example
Network layer attack	Occupies the network bandwidth with volumetric traffic, causing your service unable to respond to legitimate access requests.	NTP flood attack
Transport layer DDoS attack	Occupies the connection resources of the server, causing denial of services.	SYN flood attack and ACK flood attack
Session layer attack	Occupies SSL session resources of the server, causing denial of services.	SSL slow connection attack
Application layer attack	Occupies the application processing resources of the server and consumes its processing performance, causing denial of services.	HTTP GET flood attack and HTTP POST flood attack

3 Functions

The Anti-DDoS service protects public IP addresses against layer-4 to layer-7 distributed denial of service (DDoS) attacks and sends alarms immediately when detecting an attack. In addition, Anti-DDoS improves the bandwidth utilization to further safeguard user services.

Anti-DDoS monitors the service traffic from the Internet to public IP addresses to detect attack traffic in real time. It then scrubs attack traffic based on user-configured defense policies without interrupting service running. It also generates monitoring reports that provide visibility into the security of network traffic.

Anti-DDoS helps users mitigate the following attacks:

- Web server attacks

  Include SYN flood, HTTP flood, and low-rate attacks
- Game attacks

  Include UDP flood, SYN flood, TCP-based, and fragmentation attacks
- HTTPS server attacks

  Include SSL DoS and DDoS attacks

Anti-DDoS also provides the following functions:

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

4 Advantages

Anti-DDoS mitigates DDoS attacks for HUAWEI CLOUD users. It delivers the following advantages.

- Premium protection

  Monitors DDoS attacks in real time, discards attack traffic, and forwards legitimate traffic to the destination IP address.

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

- Complete and accurate

  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 equipment, Anti-DDoS checks each packet and responds to any attack immediately without causing service delays.

- Enabled automatically

  This service is automatically enabled after you purchase an EIP. No expensive scrubbing device or installation is required.

- Free of charge

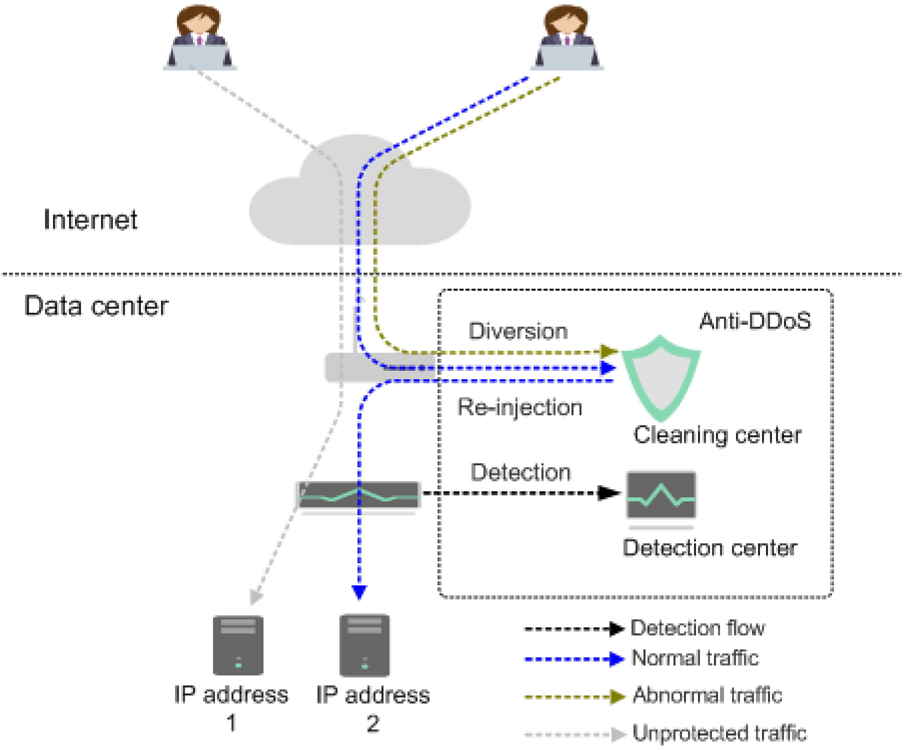
  This service is free of charge. Users can use the service without purchasing resources.

5 Application Scenarios

Anti-DDoS provides anti-DDoS only for HUAWEI CLOUD public IP addresses.

Anti-DDoS devices are deployed at egresses of data centers. **Figure 5-1** shows the network topology.

Figure 5-1 Network topology



The detection center detects network access traffic according to user-configured security policies. If an attack is detected, traffic is diverted to cleaning devices for real-time defense. Abnormal traffic is cleaned, and legitimate traffic is forwarded.

Anti-DDoS provides a 500 Mbit/s mitigation capacity against DDoS attacks for free. Traffic that exceeds 500 Mbit/s from the attacked public IP address will be routed to the black hole and the legitimate traffic will be discarded. Therefore if you may suffer from volumetric attacks exceeding 500 Mbit/s, it is a better choice to purchase HUAWEI CLOUD Advanced Anti-DDoS (AAD) for enhanced protection.

6 Pricing Details

Anti-DDoS provides a maximum of 500 Mbit/s DDoS protection capacity for free. For applications threatened by attack traffic larger than 500 Mbit/s, it is a better choice to purchase the Advanced Anti-DDoS service on HUAWEI CLOUD to expand protection capacity.

7 Accessing and Using Anti-DDoS

7.1 How to Access Anti-DDoS

The public cloud provides a web-based service management platform. You can access Anti-DDoS using HTTPS-compliant APIs or the management console.

- Management console

  If you have registered with HUAWEI CLOUD, you can log in to the management console directly. In the upper left corner of the console, click 📍 and select your region and project. Choose **Security & Compliance** > **Anti-DDoS** to access the Anti-DDoS service.

- HTTPS-compliant APIs

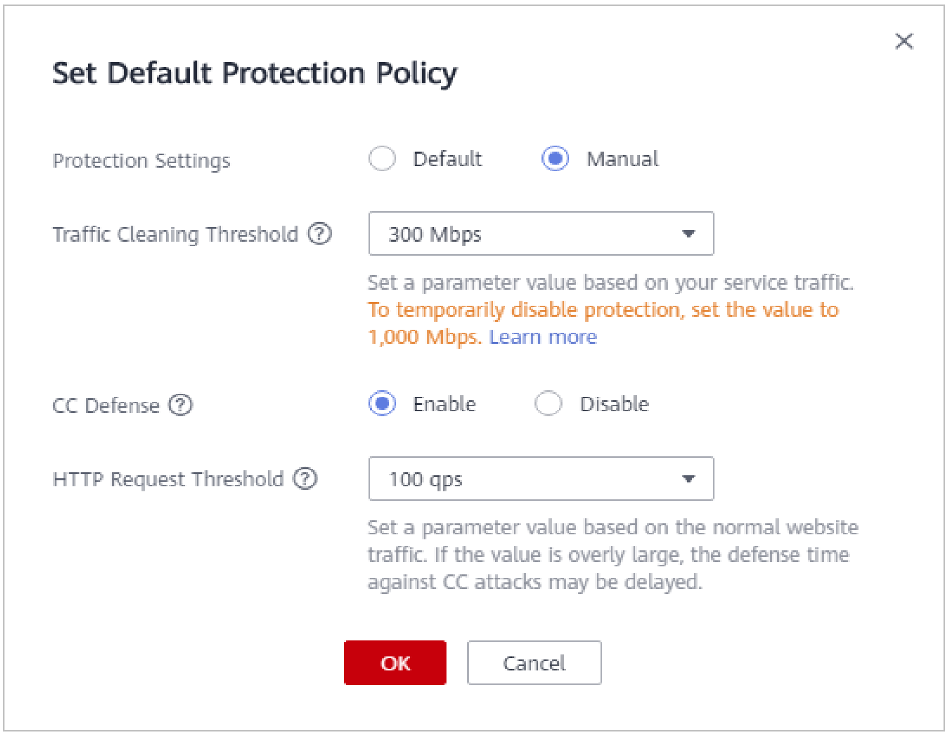
  You can access Anti-DDoS using APIs. For details, see the *Anti-DDoS API Reference*.

7.2 How to Use Anti-DDoS

Description:

- Enable Anti-DDoS to defend IP addresses against DDoS attacks.
  - Anti-DDoS can automatically enable the protection
  - Before purchasing a public IP address, you can log in to the Anti-DDoS management console and click **Set Default Protection Policy** on the **Public IP Addresses** tab page to set the default protection policy for the new public IP address. After you purchase a public IP address, the default protection policy you have set will apply to the IP address.

Figure 7-1 Setting a default protection policy for newly purchased public IP addresses



Set Default Protection Policy

Protection Settings ○ Default ● Manual

Traffic Cleaning Threshold: 300 Mbps

Set a parameter value based on your service traffic. To temporarily disable protection, set the value to 1,000 Mbps. Learn more

CC Defense ● Enable ○ Disable

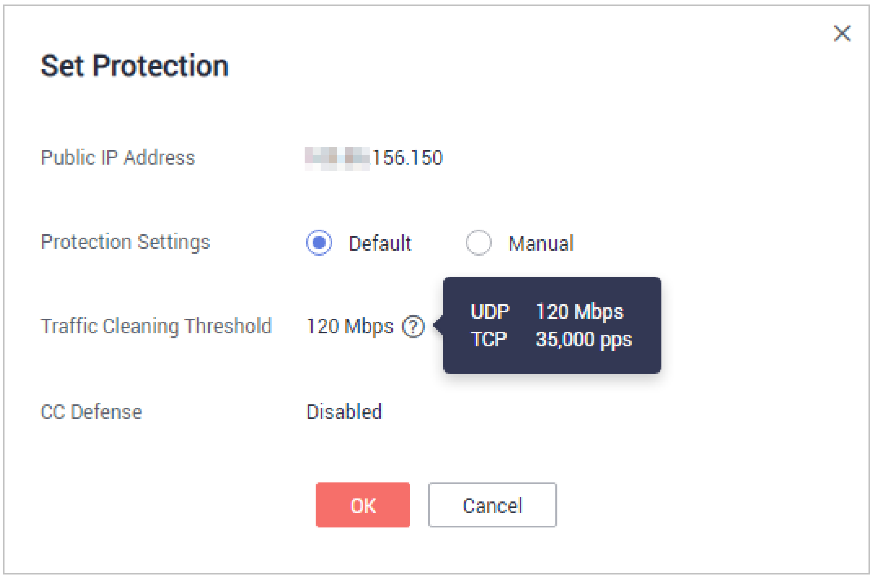
HTTP Request Threshold: 100 qps

Set a parameter value based on the normal website traffic. If the value is overly large, the defense time against CC attacks may be delayed.

– If you do not set a default protection policy for the newly purchased public IP addresses, the **Protection Settings** in **Default** mode apply to the IP addresses, as shown in **Figure 7-2**.

Default for **Protection Settings**: When the service User Datagram Protocol (UDP) traffic is greater than 120 Mbit/s or the Transmission Control Protocol (TCP) traffic is greater than 35,000 pps, traffic scrubbing is triggered and Anti-DDoS will automatically intercept the attack traffic.

Figure 7-2 Default protection settings



Set Protection

Public IP Address: [redacted]156.150

Protection Settings ● Default ○ Manual

Traffic Cleaning Threshold: 120 Mbps

UDP	120 Mbps
TCP	35,000 pps

CC Defense: Disabled

NOTE

- Mbps = Mbit/s (short for 1,000,000 bit/s). It is a unit of transmission rate and refers to the number of bits transmitted per second.
- PPS, short for Packets Per Second, is a measure of throughput for network devices. It means the number of packets sent per second.

– If you delete a public IP address, Anti-DDoS automatically disables the protection for the IP address, which is recorded in Cloud Trace Service (CTS).

- Enable alarm notification, which sends notifications by SMS or email when an IP address is under a DDoS attack.
- Adjust the defense policy based on service needs during defense.
- View monitoring and interception reports after the defense is enabled to check network security situations.
- You are not allowed to disable Anti-DDoS after it has been enabled.

7.3 Related Services

CTS

Cloud Trace Service (CTS) provides you with a history of Anti-DDoS operations. After enabling CTS, you can view all generated traces to review and audit performed operations. For details, see **Cloud Trace Service User Guide**.

Table 7-1 Anti-DDoS operations that CTS supports

Operation	Trace Name
Enabling Anti-DDoS	openAntiddos
Disabling Anti-DDoS	deleteAntiddos
Adjusting Anti-DDoS security settings	updateAntiddos

IAM

Identity and Access Management (IAM) provides the permission management function for Anti-DDoS. Only users who have Anti-DDoS Administrator permissions can use Anti-DDoS. To obtain this permission, contact the users who have the Security Administrator permissions. For details, see **Identity and Access Management User Guide**.

SMN

The Simple Message Notification (SMN) service provides the notification function. When alarm notification is enabled in Anti-DDoS, you will receive alarm messages through the endpoint you have configured, such as SMS or email, if your IP address is DDoS attacked.

For details about SMN, see **Simple Message Notification User Guide**.

7.4 Permission Management

If you need to assign different permissions to employees in your enterprise to access your Anti-DDoS resources, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your HUAWEI CLOUD resources.

With IAM, you can use your HUAWEI CLOUD account to create IAM users for your employees, and assign permissions to the users to control their access to specific resource types. For example, some software developers in your enterprise need to use Anti-DDoS resources but must not delete them or perform any high-risk operations. To achieve this result, you can create IAM users for the software developers and grant them only the permissions required for using Anti-DDoS resources.

If your HUAWEI CLOUD account does not need individual IAM users for permissions management, skip this topic.

IAM can be used free of charge. You pay only for the resources in your account. For more information about IAM, see the **IAM Service Overview**.

Anti-DDoS Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups they belong to. After authorization, the user can perform specified operations on Anti-DDoS based on the permissions.

Anti-DDoS is a project-level service deployed in specific physical regions. Therefore, Anti-DDoS permissions are assigned to users in specific regions and only take effect for these regions. If you want the permissions to take effect for all regions, you need to assign the permissions to users in each region. When accessing Anti-DDoS, the users need to switch to a region where they have been authorized.

Table 7-2 lists all the system policies supported by Anti-DDoS. For example, some Anti-DDoS policies are dependent on the policies of other services. When assigning Anti-DDoS permissions to users, you need to also assign depending policies for the Anti-DDoS permissions to take effect.

Table 7-2 Anti-DDoS system policies

Policy Name	Description	Dependencies
Anti-DDoS Administrator	Administrator permissions for Anti-DDoS.	This role depends on the **Tenant Guest** role. **Tenant Guest**: a global role, which must be assigned in the Global project

- **IAM Service Overview**
- **Creating a User Group and Assigning the Anti-DDoS Access Permission**

A Change History

Released On	Description
2022-05-19	This issue is the ninth official release, which incorporates the following change: Removed the CC defense function.
2021-08-06	This is the eighth official release. Modified the description of the entry on the management console.
2020-05-27	This is the seventh official release. Added **Pricing Details**.
2020-01-07	This is the sixth official release. Added the description of the default protection in section **How to Use Anti-DDoS**.
2019-12-16	This is the fifth official release. Modified the domain name of HUAWEI CLOUD international website.
2019-12-04	This is the fourth official release. Optimized descriptions in section **Related Services**.
2019-11-21	This is the third official release. The figure titles are added to the figures, and documents' publish path IDs are fixed.
2018-05-28	This is the second official release. Added the procedure for viewing Anti-DDoS audit logs using CTS in section **Related Services**.
2017-12-31	This is the first official release.