

Anti-DDoS

FAQs

Issue 06
Date 2021-10-09



Copyright © Huawei Technologies Co., Ltd. 2022. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks 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 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 About Anti-DDoS	1
1.1 What Is Anti-DDoS?	1
1.2 What Are a SYN Flood Attack and an ACK Flood Attack?	1
1.3 What Is a CC Attack?	1
1.4 What Is a Slow HTTP Attack?	2
1.5 What Are a UDP Attack and a TCP Attack?	2
1.6 What Is the Million-level IP Address Blacklist Database?	2
1.7 How Will Anti-DDoS Be Triggered to Scrub Traffic?	2
1.8 Does Anti-DDoS Traffic Cleaning Affect Normal Services?	3
1.9 How Does Anti-DDoS Scrub Traffic?	3
1.10 What Are the Restrictions of Anti-DDoS?	3
1.11 What Is the Protection Capacity of Anti-DDoS?	3
1.12 What Data Can Be Provided by Anti-DDoS?	3
1.13 In Which Regions Is Anti-DDoS Available?	4
1.14 What Is the Maximum Protection Capacity Provided by HUAWEI CLOUD Anti-DDoS for Free?	4
1.15 Which Services Can Use Anti-DDoS?	4
1.16 Can Anti-DDoS Be Used Across Clouds?	4
1.17 How to Determine Whether an Attack Occurs?	4
2 About Basic Functions	5
2.1 What Are Regions and AZs?	5
2.2 What Is the HTTP Request Threshold Set for Anti-DDoS Protection?	6
2.3 What Would Happen When I Am Under a DDoS Attack Exceeding 500 Mbit/s?	7
2.4 Which Types of Attacks Does Anti-DDoS Mitigate?	7
2.5 What Should I Do If My Service Is Frequently Attacked?	7
2.6 What Is the Difference Between ELB Protection and ECS Protection?	7
2.7 Why Is the Number of Times of Cleaning Different from the Number of Attacks for the Same Public IP Address?	7
2.8 Is Anti-DDoS Enabled by Default?	8
2.9 Does Anti-DDoS Protect a Region or a Single IP Address?	8
2.10 Do I Need to Clear the Resources of Anti-DDoS When I Delete an Account?	8
2.11 How Do I View the Traffic Cleaning Frequency?	8
2.12 How Can I View Anti-DDoS Protection Statistics?	8
2.13 How Can I View Public IP Address Monitoring Data in Anti-DDoS?	9

2.14 How Can I View an Interception Report?.....	9
2.15 Can I Disable Anti-DDoS Completely?.....	9
2.16 How Do I Check Whether the Inbound Traffics Are Routed Through Anti-DDoS Devices?.....	9
3 About Threshold and Black Hole.....	11
3.1 How Does the Traffic Cleaning Threshold Take Effect in Anti-DDoS?.....	11
3.2 What Is the Black Hole Policy of HUAWEI CLOUD?.....	11
3.3 How Do I Set the Anti-DDoS Traffic Cleaning Threshold?.....	12
3.4 How Can I Adjust the Block Threshold?.....	12
3.5 What Can I Do If an IP Address Is Blocked?.....	12
4 About Alarm notification.....	14
4.1 Will I Be Promptly Notified When an Attack Is Detected?.....	14
4.2 What Should I Do If I Receive an Alarm Notification?.....	14
4.3 How Do I Disable the Alarm Notification?.....	14
A Change History.....	17

1 About Anti-DDoS

1.1 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. In addition, 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 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.

1.2 What Are a SYN Flood Attack and an ACK Flood Attack?

A SYN flood attack is a typical denial of service (DoS) attack. Utilizing the loop hole in the Transmission Control Protocol (TCP), the attacker sends a huge number of forged TCP connection requests to the target to exhaust its resources (fully loaded CPU or insufficient memory). Consequently, the target fails to respond to normal connection requests.

An ACK flood attack works in a similar mechanism as a SYN flood attack.

An ACK flood attack is when an attacker attempts to overload a server with TCP ACK packets. Like other DDoS attacks, the goal of an ACK flood is to deny service to other users by slowing down or crashing the target using junk data. The targeted server has to process each ACK packet received, which uses so much computing power that it is unable to serve legitimate users.

1.3 What Is a CC Attack?

In a challenge collapser (CC) attack, the attacker uses a proxy server to generate and send disguised requests to the target host. In addition, the attacker controls other hosts in the Internet and makes them send large numbers of data packets

to the target server to exhaust its resources. In the end, the target server stops responding to requests. As you know, when many users access a web page, the page opens slowly. So in a CC attack, the attacker simulates a scenario where a large number of users (a thread represents a user) are accessing pages all the time. Because the accessed pages all require a lot of data operations (consuming many CPU resources), the CPU usage is kept at the 100% level for a long time until normal access requests are blocked.

You can use the CC defense function to control the HTTP request rate.

1.4 What Is a Slow HTTP Attack?

Slow HTTP attacks are a variation of CC attacks. Here is how slow HTTP attacks work:

The attacker establishes a connection to the target server which allows HTTP access. Then the attacker specifies a large content length and sends packets in an extremely low rate, such as one byte per one to ten seconds. The connection is maintained this way. If the attacker keeps establishing such connections, available connections on the target server are slowly consumed and the server will stop responding to valid requests.

1.5 What Are a UDP Attack and a TCP Attack?

Exploiting the interaction characteristics of UDP and TCP, attackers use botnets to send large numbers of various TCP connection packets or UDP packets to exhaust the bandwidth resources of target servers. As a result, the servers become slow in processing capability and fail to work properly.

1.6 What Is the Million-level IP Address Blacklist Database?

The million-level IP address blacklist database refers to the database of millions of malicious IP addresses collected by experts in the past years. When users' services are attacked by these IP addresses, Anti-DDoS responds to those attacks first to defend your servers in a timely manner.

1.7 How Will Anti-DDoS Be Triggered to Scrub Traffic?

Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the traffic cleaning threshold.

- When the service traffic reaches this threshold, Anti-DDoS intercepts only attack traffic.
- If the service traffic does not reach the threshold, Anti-DDoS will not intercept the traffic, regardless of whether it is attack traffic.

You can adjust the traffic cleaning threshold based on the actual service bandwidth. For details, see [Configuring an Anti-DDoS Protection Policy](#).

1.8 Does Anti-DDoS Traffic Cleaning Affect Normal Services?

Anti-DDoS traffic cleaning exerts no adverse impacts on normal traffic.

1.9 How Does Anti-DDoS Scrub Traffic?

Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the traffic cleaning threshold.

You can [view an interception report](#) on protection statistics, including the traffic cleaning frequency, cleaned traffic amount, weekly top 10 attacked public IP addresses, and total number of intercepted attacks of all public IP addresses of a user.

1.10 What Are the Restrictions of Anti-DDoS?

Anti-DDoS provides a 500 Mbit/s mitigation capacity against DDoS attacks.

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.

1.11 What Is the Protection Capacity of Anti-DDoS?

Anti-DDoS provides a maximum of 500 Mbit/s protection capacity free of charge (depending on the available bandwidth of HUAWEI CLOUD). 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.

1.12 What Data Can Be Provided by Anti-DDoS?

- You can [view the monitoring report](#) of a public IP address, including the current protection status, protection settings, and the traffic and anomalies within the last 24 hours.
- You can [view an interception report](#) on protection statistics, including the traffic cleaning frequency, cleaned traffic amount, weekly top 10 attacked ECSs, load balancers, or BMSs, and total number of intercepted attacks of all public IP addresses of a user.
- You can [enable alarm notification](#) for Anti-DDoS so that you can receive notifications in a timely manner if a public IP address is attacked. If you do not enable this function, you have to log in to the management console to view alarms.

1.13 In Which Regions Is Anti-DDoS Available?

Currently, Anti-DDoS only provides protection for services deployed on HUAWEI CLOUD.

HUAWEI CLOUD supports the following regions: CN-Hong Kong, AP-Bangkok, AF-Johannesburg, AP-Singapore, LA-Santiago, LA-Mexico City¹, and LA-Sao Paulo¹.

1.14 What Is the Maximum Protection Capacity Provided by HUAWEI CLOUD Anti-DDoS for Free?

HUAWEI CLOUD Anti-DDoS provides a maximum of 500 Mbit/s protection capacity for free.

1.15 Which Services Can Use Anti-DDoS?

Anti-DDoS provides the traffic cleaning function for public IP addresses purchased by users.

1.16 Can Anti-DDoS Be Used Across Clouds?

Anti-DDoS currently supports protection only for services deployed on HUAWEI CLOUD.

1.17 How to Determine Whether an Attack Occurs?

- You can log in to the HUAWEI CLOUD console to [view the monitoring report](#) of a public IP address, including the current protection status, protection settings, and the traffic and anomalies within the last 24 hours.
- You can log in to the HUAWEI CLOUD console to [view an interception report](#) on protection statistics, including the traffic cleaning frequency, cleaned traffic amount, weekly top 10 attacked ECSs, load balancers, or BMSs, and total number of intercepted attacks of all public IP addresses of a user.

2 About Basic Functions

2.1 What Are Regions and AZs?

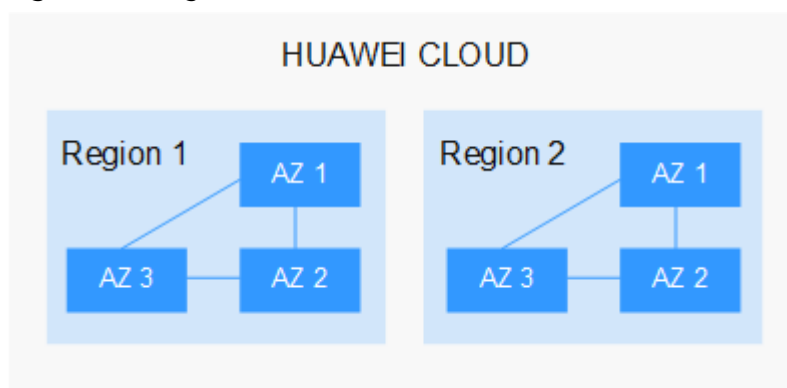
Concepts

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided from the dimensions of geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

Figure 2-1 shows the relationship between the regions and AZs.

Figure 2-1 Region and AZ



HUAWEI CLOUD provides services in many regions around the world. You can select a region and AZ as needed.

Selecting a Region

When selecting a region, consider the following factors:

- Location
You are advised to select a region close to you or your target users. This reduces network latency and improves access rate. However, Chinese mainland regions provide basically the same infrastructure, BGP network quality, as well as operations and configurations on resources. Therefore, if you or your target users are in the Chinese mainland, you do not need to consider the network latency differences when selecting a region.
 - If you or your target users are in the Asia Pacific region, except the Chinese mainland, select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
 - If you or your target users are in Africa, select the **AF-Johannesburg** region.
 - If you or your target users are in Europe, select the **EU-Paris** region.
- Resource price
Resource prices may vary in different regions. For details, see [Product Pricing Details](#).

Selecting an AZ

When determining whether to deploy resources in the same AZ, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs in the same region.
- For low network latency, deploy resources in the same AZ.

Regions and Endpoints

Before using an API to call resources, specify its region and endpoint. For more details, see [Regions and Endpoints](#).

2.2 What Is the HTTP Request Threshold Set for Anti-DDoS Protection?

The HTTP request threshold refers to the number of HTTP requests that can be processed by the deployed service per second on average. It is calculated based on the total number of requests. Anti-DDoS will automatically scrub traffic if detecting that the total number of requests exceeds the configured HTTP request threshold.

2.3 What Would Happen When I Am Under a DDoS Attack Exceeding 500 Mbit/s?

Anti-DDoS provides a maximum of 500 Mbit/s protection capacity free of charge (depending on the available bandwidth of HUAWEI CLOUD). The attacked public IP address will be routed to a black hole when the attack traffic exceeds 500 Mbit/s, and the normal access traffic will be discarded. It is a better choice to purchase HUAWEI CLOUD Advanced Anti-DDoS for enhanced protection.

2.4 Which Types of Attacks Does Anti-DDoS Mitigate?

Anti-DDoS helps users mitigate the following attacks:

- Web server attacks
Include SYN flood, HTTP flood, Challenge Collapsar (CC), 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
- DNS server attacks
Include attacks exploiting DNS protocol stack vulnerabilities, DNS reflection attacks, DNS flood attacks, and DNS cache miss attacks

2.5 What Should I Do If My Service Is Frequently Attacked?

When your services are frequently under DDoS attacks, the public IP address is prone to be routed to a black hole, damaging service continuity. Therefore, it is recommended that you purchase Advanced Anti-DDoS to expand protection capability.

2.6 What Is the Difference Between ELB Protection and ECS Protection?

An EIP can be bound to a load balancer or ECS. Anti-DDoS protects EIP against DDoS attacks. There is no difference between ELB and ECS protection.

2.7 Why Is the Number of Times of Cleaning Different from the Number of Attacks for the Same Public IP Address?

Cleaning is triggered automatically when an attack is detected on a public IP address. The cleaning lasts for a while. (Only attack traffic is cleaned, and users'

services will not be affected.) If, during the cleaning, another attack is detected on the same public IP address, the attack will be cleaned together with the previous attack. Consequently, the number of attacks increases by one while the number of times of cleaning does not.

2.8 Is Anti-DDoS Enabled by Default?

Yes. It is enabled by default and uses the default protection policy. To modify this setting, see [Configuring an Anti-DDoS Protection Policy](#).

NOTE

Once enabled, Anti-DDoS cannot be disabled.

2.9 Does Anti-DDoS Protect a Region or a Single IP Address?

A single IP address.

2.10 Do I Need to Clear the Resources of Anti-DDoS When I Delete an Account?

No. Anti-DDoS is free of charge.

- Anti-DDoS does not consume your resources.
- Anti-DDoS is enabled by default at no additional charge. Therefore you do not need to clear the resources when deleting the account.
- Anti-DDoS is automatically enabled when you purchase a public IP address without incurring any fee.

2.11 How Do I View the Traffic Cleaning Frequency?

You can [view an interception report](#) on protection statistics, including the traffic cleaning frequency, cleaned traffic amount, weekly top 10 attacked public IP addresses, and total number of intercepted attacks of all public IP addresses of a user.

2.12 How Can I View Anti-DDoS Protection Statistics?

You can [view an interception report](#) on protection statistics, including the traffic cleaning frequency, cleaned traffic amount, weekly top 10 attacked public IP addresses, and total number of intercepted attacks of all public IP addresses of a user.

2.13 How Can I View Public IP Address Monitoring Data in Anti-DDoS?

You can [view the monitoring report](#) of a public IP address, including the current protection status, protection settings, and the traffic and anomalies within the last 24 hours.

2.14 How Can I View an Interception Report?

You can [view an interception report](#) on protection statistics, including the traffic cleaning frequency, cleaned traffic amount, weekly top 10 attacked public IP addresses, and total number of intercepted attacks of all public IP addresses of a user.

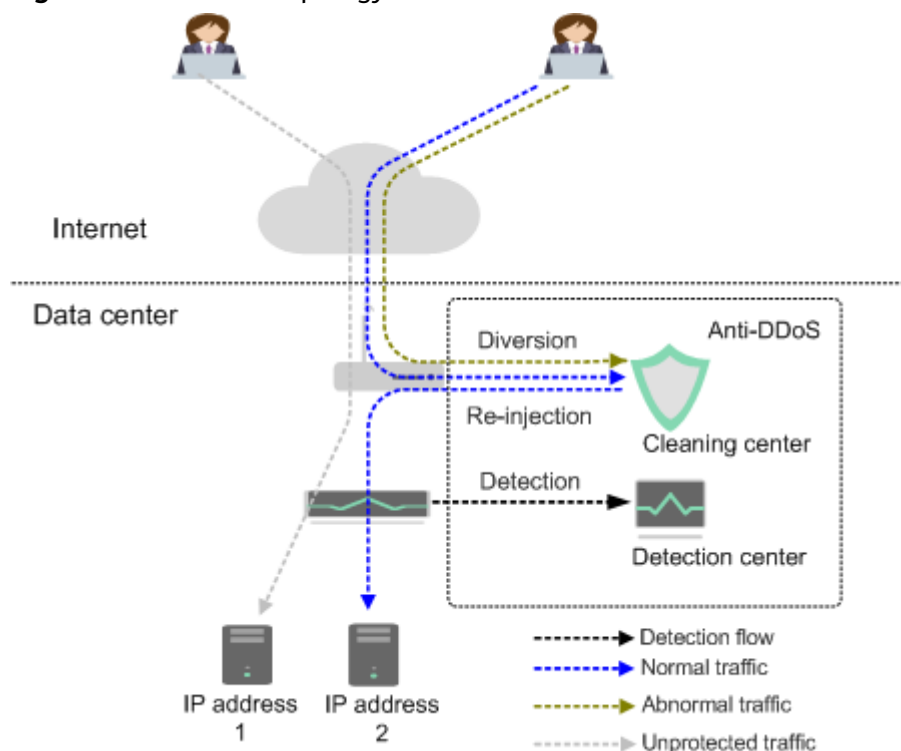
2.15 Can I Disable Anti-DDoS Completely?

No.

2.16 How Do I Check Whether the Inbound Traffics Are Routed Through Anti-DDoS Devices?

Anti-DDoS provides anti-DDoS only for HUAWEI CLOUD EIPs. Anti-DDoS devices are deployed at the egresses of data centers.

Figure 2-2 Network topology



Anti-DDoS only enables protection for inbound traffics from external network.

- If you access the EIP from an external network, the inbound traffics are routed through the public network routes. You can check whether the traffics are forwarded from the public network routes on the VM bound to the EIP. If yes, the access traffics are routed through Anti-DDoS devices.

If inbound traffics are routed through Anti-DDoS devices, the following information is displayed when the EIP is threatened by DDoS attacks:

- Traffic cleaning records exist on the Anti-DDoS console.
- An alarm notification is sent by SMS or Email.
- If you access the EIP from the intranet, the inbound traffics are not routed through public network routes. As a result, the traffics are not routed through Anti-DDoS devices.

For example, if you apply for two EIPs in two different regions of HUAWEI CLOUD, the access traffics between the two EIPs will not be routed through Anti-DDoS.

3 About Threshold and Black Hole

3.1 How Does the Traffic Cleaning Threshold Take Effect in Anti-DDoS?

Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the traffic cleaning threshold. It will discard attack traffic and permit normal service traffic.

The default cleaning threshold of Anti-DDoS is 120 Mbit/s. You can adjust the threshold based on the actual service bandwidth. For details, see [Configuring an Anti-DDoS Protection Policy](#).

3.2 What Is the Black Hole Policy of HUAWEI CLOUD?

What is a black hole?

A black hole refers to a situation where access to a cloud server is blocked by HUAWEI CLOUD Anti-DDoS because the traffic targeting the cloud server exceeds the configured black hole threshold.

Why is a black hole required for HUAWEI CLOUD Anti-DDoS?

DDoS attacks impose adverse impacts on users' services and HUAWEI CLOUD. Defense against DDoS attacks is costly on bandwidth consumption.

The bandwidth is purchased by HUAWEI CLOUD from carriers, but carriers will not take the attack traffic out when calculating the total bandwidth fees.

Therefore, the access to a cloud server is blocked by HUAWEI CLOUD Anti-DDoS when the traffic targeting the cloud server exceeds the configured black hole threshold.

What is the black hole rule?

A black hole will be triggered when the traffic targeting the cloud server exceeds the configured black hole threshold.

The black hole lasts 24 hours by default. If the system detects that the traffic still persists and exceeds the threshold, the access will be blocked again.

3.3 How Do I Set the Anti-DDoS Traffic Cleaning Threshold?

After you purchase a public IP address, Anti-DDoS automatically enables protection. The default traffic cleaning threshold is **120 Mbps**.

The default cleaning threshold of Anti-DDoS is 120 Mbit/s. You can adjust the threshold based on the actual service bandwidth. For details, see [Configuring an Anti-DDoS Protection Policy](#).

- The cleaning threshold for each attack type is automatically generated based on your settings and the service traffic.
- When the service traffic hits the traffic cleaning threshold, Anti-DDoS automatically scrubs attack traffic instead of blocking the service.

3.4 How Can I Adjust the Block Threshold?

Anti-DDoS provides a maximum of 500 Mbit/s protection capacity free of charge (depending on the available bandwidth of HUAWEI CLOUD). Traffic that exceeds 500 Mbit/s will be routed to a black hole. 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.

3.5 What Can I Do If an IP Address Is Blocked?

Possible Causes

Anti-DDoS provides a maximum of 500 Mbit/s protection capacity free of charge (depending on the available bandwidth of HUAWEI CLOUD). HUAWEI CLOUD Anti-DDoS will trigger a black hole to block access from the Internet within a time period when detecting an ECS is under volumetric flood attacks.

Solution

You can use either of the following methods to unblock the IP address:

- The system automatically deactivates the black hole 24 hours after the IP address was blocked.
If the system detects that the attack traffic still persists and exceeds the threshold, the IP address will be blocked again.
- Advanced Anti-DDoS (AAD) is recommended because it automatically deactivates the black hole 30 minutes, by default, after the black hole has been triggered. The duration of persistent black hole depends on the times of the black hole triggered and volume of peak attack traffic of the day, and it can be a maximum of 24 hours. If you need to permit access before a black hole becomes ineffective, upgrade Anti-DDoS to AAD and contact Huawei technical support.

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 3-1](#).

Table 3-1 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	<ul style="list-style-type: none">• Fixed protection policies• Basic CC attack defense• Globally applied policies	<ul style="list-style-type: none">• 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

4 About Alarm notification

4.1 Will I Be Promptly Notified When an Attack Is Detected?

Yes, if you enable alarm notification.

On the console, click the **Alarm Notifications** tab to enable the alarm notification function, which enables you to receive alarms through the endpoint you have configured if a DDoS attack is detected. For details, see [Enabling Alarm Notification](#).

4.2 What Should I Do If I Receive an Alarm Notification?

It is normal if you receive an alarm notification. After the alarm notification function is enabled for your Anti-DDoS service, you will receive notifications through the endpoint you have configured when the public IP address is under DDoS attacks.

You can log in to the management console to [view the protection status of a public IP address](#).

4.3 How Do I Disable the Alarm Notification?

The alarm notification of Anti-DDoS is sent by the Simple Message Notification (SMN) service.

If you do not need to receive alarm notifications from SMN, you can disable or modify the alarm notification settings on the Anti-DDoS console.

Disabling Alarm Notifications

If you do not need to receive alarm notifications, you can disable the alarm notification function on the **Alarm Notifications** tab page of the Anti-DDoS

console. After alarm notification is disabled, you will not receive alarm information.

Step 1 Log in to the management console.


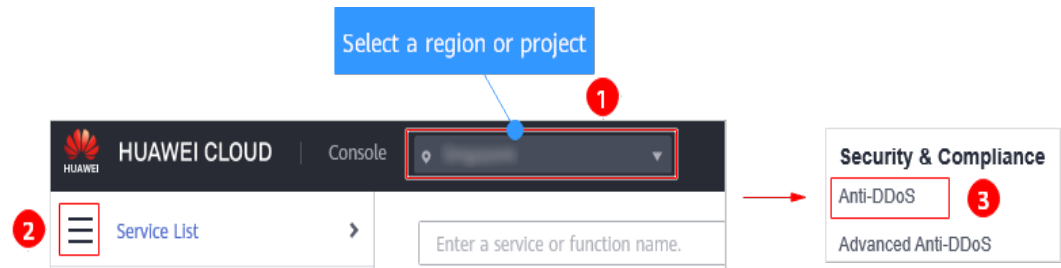
Step 2 Click  in the upper left corner of the page and choose **Security & Compliance > Anti-DDoS**.

Figure 4-1 Anti-DDoS




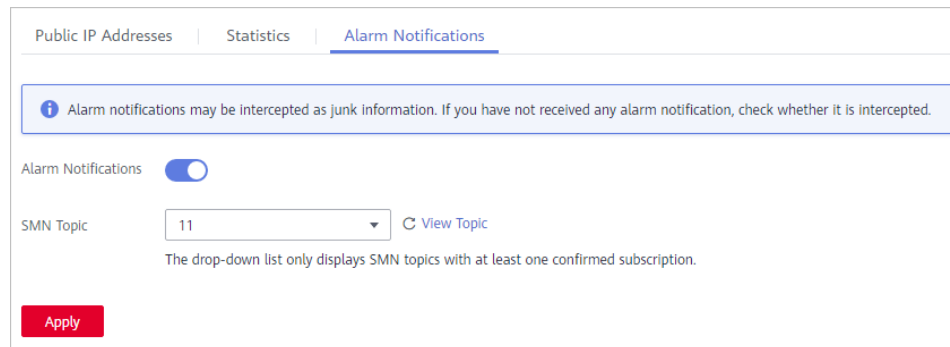
Step 3 Click the **Alarm Notifications** tab and click  to disable the alarm notification function.

Figure 4-2 Configuring alarm notifications



----End

Deleting the Subscription

If the subscription endpoint (mobile number or email address) that receives alarm notifications changes, you need to delete the subscription. For example, you need to delete an alarm notification recipient if the recipient resigns.

The alarm notification topic is **antiddos-warning** and the subscription endpoint is **test@example.com**.

Prerequisites

You have obtained the SMN administrator permission.

Procedure

Step 1 Log in to the management console.


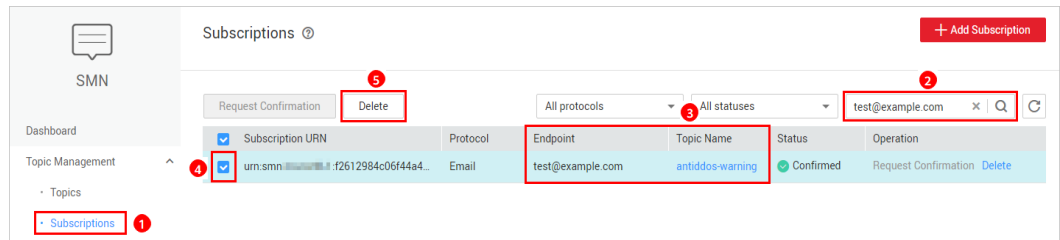
- Step 2** In the upper left corner, click  and choose **Application > Simple Message Notification**.
- Step 3** On the displayed page, choose **Topic Management > Subscriptions** in the navigation pane on the left. Enter the endpoint (mobile number or email address) in the search box.

Figure 4-3 Searching for the target subscription endpoint



- Step 4** Check whether the subscription endpoint receives the alarm notifications sent from SMN for Anti-DDoS.
- Step 5** Click **Delete** in the **Operation** column.

 **NOTE**

After a subscription is deleted, the endpoint no longer receives alarm notifications for Anti-DDoS. Exercise caution when performing this operation.

----End

Follow-up Operations

Add a Subscription

After you delete the subscription for the resigned recipient from SMN, you can add a subscription for the succeeding personnel. For details about how to add a subscription, see [Adding a Subscription](#) and [Requesting Subscription Confirmation](#).

A Change History

Released On	Description
2021-10-09	This issue is the sixth official release, which incorporates the following change: Deleted How Do I Temporarily Disable Anti-DDoS?
2021-08-06	This is the fifth official release. Modified the description of the entry on the management console.
2020-05-27	This is the fourth official release. Added How Do I Disable the Alarm Notification? .
2020-04-08	This is the third official release. Added the following FAQs: <ul style="list-style-type: none">• What Is the Black Hole Policy of HUAWEI CLOUD?• How Do I Disable the Alarm Notification?
2018-05-28	This is the second official release. Added the following FAQs: How Do I Temporarily Disable Anti-DDoS?
2017-12-31	This is the first official release.