

Anti-DDoS

FAQs

Issue 01
Date 2024-05-10



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. 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 Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI 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 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?.....	4
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.....	7
2.1 What Is the HTTP Request Threshold Set for Anti-DDoS Protection?.....	7
2.2 What Would Happen When I Am Under a DDoS Attack Exceeding ?.....	7
2.3 Which Types of Attacks Does Anti-DDoS Mitigate?.....	7
2.4 What Should I Do If My Service Is Frequently Attacked?.....	8
2.5 What Is the Difference Between ELB Protection and ECS Protection?.....	8
2.6 Why Is the Number of Times of Cleaning Different from the Number of Attacks for the Same Public IP Address?.....	8
2.7 Is Anti-DDoS Enabled by Default?.....	8
2.8 Does Anti-DDoS Protect a Region or a Single IP Address?.....	8
2.9 Do I Need to Clear the Resources of Anti-DDoS When I Delete an Account?.....	8
2.10 How Do I View the Traffic Cleaning Frequency?.....	9
2.11 How Can I View Anti-DDoS Protection Statistics?.....	9
2.12 How Can I View Public IP Address Monitoring Data in Anti-DDoS?.....	9
2.13 How Can I View an Interception Report?.....	9

2.14 Can I Disable Anti-DDoS Completely?.....	9
2.15 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.

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 traffic detection includes the following detection items. Different traffic scrubbing thresholds correspond to different detection thresholds.

When traffic surpasses a detection threshold, Anti-DDoS triggers traffic scrubbing.

- Abnormal TCP sessions
- SYN Flood
- ACK Flood
- TCP fragment attacks
- FIN\RST Flood
- UDP Flood

- Fingerprint defense
- UDP fragment attacks
- Abnormal UDP packets
- ICMP
- Other Flood
- DNS Query Flood
- DNS Reply Flood

1.8 Does Anti-DDoS Traffic Cleaning Affect Normal Services?

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

To prevent normal traffic from being blocked, you can set the traffic scrubbing threshold to a value higher than the service bandwidth.

1.9 How Does Anti-DDoS Scrub Traffic?

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

You can view an interception report on protection statistics, including the traffic scrubbing frequency, clean 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 defends against all DDoS attacks, such as CC, SYN flood, and UDP flood, and 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 the 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.

Anti-DDoS is available in EU-Dublin.

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

Anti-DDoS defends against all DDoS attacks, such as CC, SYN flood, and UDP flood, and 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.

1.15 Which Services Can Use Anti-DDoS?

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

1.16 Can Anti-DDoS Be Used Across Clouds?

Anti-DDoS cannot be used by multiple accounts. Currently, Anti-DDoS only protects services deployed on Huawei Cloud.


1.17 How to Determine Whether an Attack Occurs?

To check whether a public IP address is attacked, perform the following operations:

- For details about how to query attack traffic information and anomaly events within 24 hours, see [Method 1: Viewing Monitoring Reports](#).
- For details about how to query information about public IP addresses attacked within one month, see [Method 2: Viewing the Security Report](#).

Method 1: Viewing Monitoring Reports

Step 1 Log in to the management console.

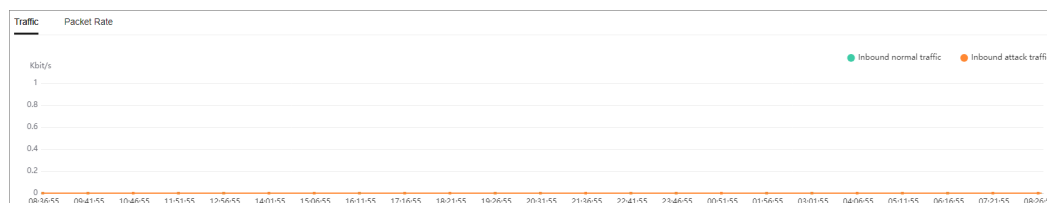
Step 2 Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS** page is displayed.

Step 3 Click the **Public IP Addresses** tab, locate the row that contains the IP address of which you want to view its monitoring report, and click **View Monitoring Report**.

Step 4 Check whether there are attack traffic and anomaly events.

- On the **Traffic** tab page, check whether there is attack traffic displayed in the corresponding time range. If there is, the public IP address is attacked.
- Check whether there are abnormal events in the event list at the bottom. If there are abnormal events, the public IP address is attacked.


Figure 1-1 Monitoring reports



----End

Method 2: Viewing the Security Report

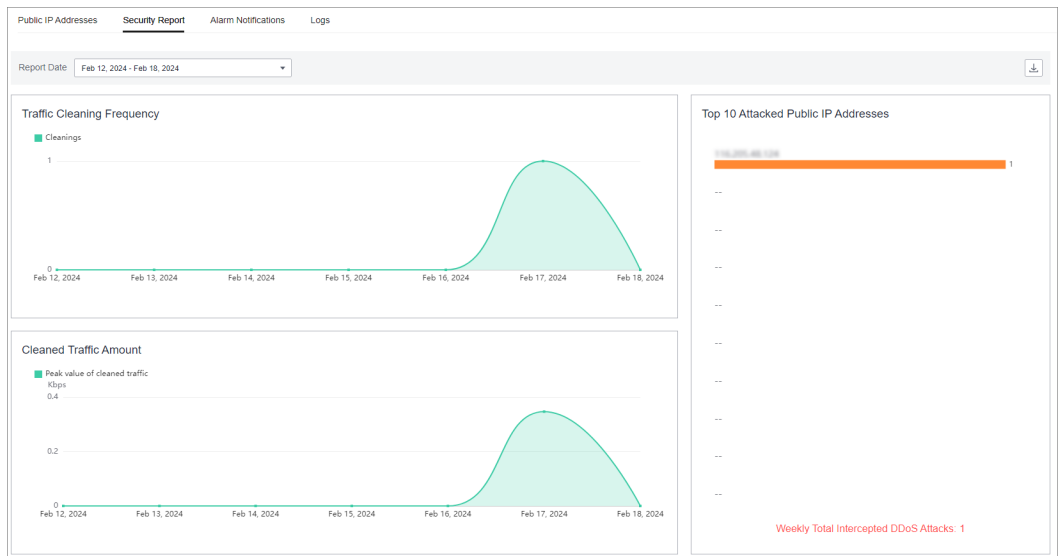
Step 1 Log in to the management console.

Step 2 Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS** page is displayed.

Step 3 Click the **Security Report** tab, select a time range, and check whether the queried public IP address is in **Top 10 Attacked Public IP Addresses**.

If the public IP address is in **Top 10 Attacked Public IP Addresses**, the public IP address is attacked.

Figure 1-2 Security report



----End

2 About Basic Functions

2.1 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.

2.2 What Would Happen When I Am Under a DDoS Attack Exceeding ?

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.

2.3 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

2.4 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.

2.5 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.

2.6 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.

2.7 Is Anti-DDoS Enabled by Default?

Yes. Yes. It is enabled by default and uses the default protection policy. To modify this setting, see .

NOTE

Once enabled, Anti-DDoS cannot be disabled.

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

Single IP address.

2.9 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. You do not need to release the resources when deleting the account.
- Anti-DDoS is automatically enabled when you purchase a public IP address without incurring any fee.

2.10 How Do I View the Traffic Cleaning Frequency?

You can view an interception report on protection statistics, including the traffic scrubbing frequency, clean traffic amount, weekly top 10 attacked public IP addresses, and total number of intercepted attacks of all public IP addresses of a user.

2.11 How Can I View Anti-DDoS Protection Statistics?

You can view an interception report on protection statistics, including the traffic scrubbing frequency, clean 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 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.

2.13 How Can I View an Interception Report?

You can view an interception report on protection statistics, including the traffic scrubbing frequency, clean traffic amount, weekly top 10 attacked public IP addresses, and total number of intercepted attacks of all public IP addresses of a user.

2.14 Can I Disable Anti-DDoS Completely?

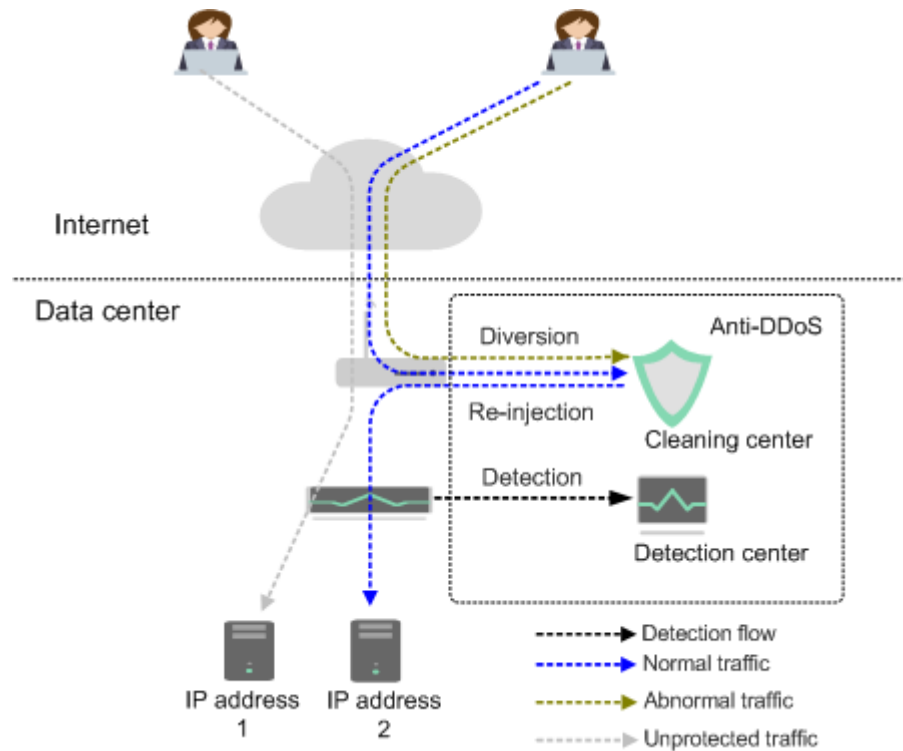
No.

To ensure the security of the Huawei Cloud platform, protection policies must be enabled for all traffic entering Huawei Cloud.

2.15 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 2-1 Network topology



Anti-DDoS only protects inbound traffics from external network. Huawei Cloud traffic does not go through Anti-DDoS.

- 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 traffic is not routed through public network routes and 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 scrubbing threshold of Anti-DDoS is 120 Mbit/s. You can adjust the threshold based on the actual service bandwidth.

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 attack 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 attack 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 attack 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 attack 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 scrubbing threshold of Anti-DDoS is 120 Mbit/s.

You can adjust the threshold based on the actual service bandwidth.

- The scrubbing threshold for each attack type is automatically generated based on your settings and the service traffic.
- When the service traffic hits the traffic scrubbing 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). Anti-DDoS will trigger a black hole to block access from the Internet within a time period when detecting a cloud server is under volumetric flood attacks.

How Do I Deactivate a Black Hole?

When the access to a cloud server is blocked by Huawei Cloud because attack traffic targeting a cloud server exceeds a certain threshold, follow the instructions described in [Table 3-1](#) to handle that.

Table 3-1 Black hole deactivation methods

Edition	Deactivation Policy	Deactivation Method
Anti-DDoS NOTE Anti-DDoS is enabled by default.	<ul style="list-style-type: none">• 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.

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 (by SMS or email) if a DDoS attack is detected. For details, see .

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

An alarm notification does not necessarily mean that there is an attack. After the alarm notification function is enabled for your Anti-DDoS service, you will receive notifications through the endpoint you have configured (such as SMS or Email) when the public IP address is under DDoS attacks.

You can log in to the management console to view the protection status of an EIP. If you do not want the traffic to be scrubbed, increase the traffic scrubbing threshold. For details, see section .

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 no longer receive alarm notifications for Anti-DDoS.

Step 1 Log in to the management console.

Step 2 Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS** page is displayed.


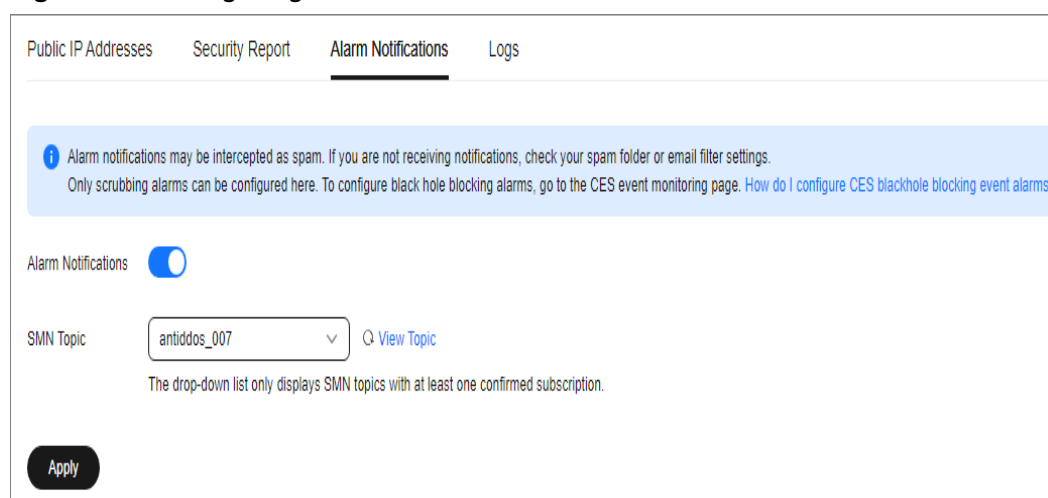
Step 3 Click the **Alarm Notifications** tab and click  to disable the alarm notification function.

Figure 4-1 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, hover your mouse over  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.

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,

A Change History

Date	Description
2022-09-30	This is the first official release.