

Anti-DDoS Service

FAQ

Issue 01
Date 2023-07-18



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. 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 General FAQs.....	1
1.1 What Are Regions and AZs?.....	1
1.2 What Is the Black Hole Policy of HUAWEI CLOUD?.....	2
1.3 What are the Relationships Between DDoS Mitigation and the Anti-DDoS, CNAD Pro, and AAD Services?.....	4
1.4 What Are the Differences Between Anti-DDoS and Advanced Anti-DDoS?.....	4
1.5 What Are a SYN Flood Attack and an ACK Flood Attack?.....	5
1.6 What Is a CC Attack?.....	5
1.7 What Is a Slow HTTP Attack?.....	6
1.8 What Are a UDP Attack and a TCP Attack?.....	6
1.9 What Are the Differences Between DDoS Attacks and Challenge Collapsar Attacks?.....	6
1.10 Does Anti-DDoS Support the Transparent Access Mode?.....	8
2 CNAD Basic (Anti-DDoS) FAQs.....	9
2.1 About Anti-DDoS.....	9
2.1.1 What Is the Million-level IP Address Blacklist Database?.....	9
2.1.2 How Will Anti-DDoS Be Triggered to Scrub Traffic?.....	9
2.1.3 Does Anti-DDoS Traffic Cleaning Affect Normal Services?.....	9
2.1.4 How Does Anti-DDoS Scrub Traffic?.....	9
2.2 About Basic Functions.....	10
2.2.1 Which Types of Attacks Does Anti-DDoS Mitigate?.....	10
2.2.2 What Is the Difference Between ELB Protection and ECS Protection?.....	10
2.2.3 Why Is the Number of Times of Cleaning Different from the Number of Attacks for the Same Public IP Address?.....	10
2.2.4 How Do I Temporarily Disable Anti-DDoS?.....	10
2.3 About Alarm notification.....	12
2.3.1 Will I Be Promptly Notified When an Attack Is Detected?.....	12
2.3.2 What Should I Do If I Receive an Alarm Notification?.....	12
2.3.3 How Do I Enable Anti-DDoS Blocking Notifications?.....	12
2.4 About Service Faults.....	13
2.4.1 Why Is the Traffic Volume of a Public IP Address is Low?.....	13
2.4.2 Why Is the Access from the Internet Abnormal?.....	13
2.4.3 Traffic Scrubbed Unexpectedly Without Traffic Fluctuations Reported.....	13
2.4.4 What Should I Do If Access to a Client Is Denied Due to DDoS Attacks?.....	14

2.4.5 How Do I Query the Protection Information About a Public IP Address That Is Under DDoS Attacks?	14
2.4.6 Is Traffic Cleaning Triggered Even If No Attack Occurs?	14

1 General FAQs

1.1 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.

Selecting a Region

If you or your users are in Europe, select the **EU-Dublin** region.

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.

1.2 What Is the Black Hole Policy of HUAWEI CLOUD?

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

Huawei Cloud CNAD Basic (Anti-DDoS) provides 2 Gbit/s of defense against DDoS attacks for common users for free. Anti-DDoS can provide up to 5 Gbit/s of defense capability (depending on the available bandwidth 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 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 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 1-1](#) to handle that.

Table 1-1 Black hole deactivation methods

Edition	Deactivation Policy	Deactivation Method
CNAD Basic (Anti-DDoS) NOTE Cloud Native Anti-DDoS Basic (CNAD Basic) 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. 	<ul style="list-style-type: none"> You need to wait until the system deactivates it automatically.
CNAD Advanced	The system automatically deactivates the black hole 24 hours after the access to a cloud server is blocked.	
AAD	Contact Huawei Cloud technical support to deactivate the blackhole quickly. You are advised to increase the elastic bandwidth to avoid being black-holed again.	You can upgrade the elastic protection bandwidth to deactivate the blackhole.

Self-Service Unblocking Rules

 **NOTE**

If you have purchased Anti-DDoS (Native Advanced Anti-DDoS Protection or Advanced Anti-DDoS), you will be rewarded with three self-service blackhole-deactivation quotas for free every month. If the quotas are not used up in the current month, they will be cleared at the end of the month.

Currently, only public IP addresses in North China, East China, and South China can be unblocked by you.

- 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 = $2^{(n-1)} \times 30$ 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 $2^n \times 30$ 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.

-
- ADS automatically adjusts the allowed IP unblocking attempts and the interval based on the risk control.

How Can I Increase the Black Hole Threshold?

You can increase the black hole threshold using the following methods:

- Enable Cloud Native Anti-DDoS Pro (CNAD Pro) to obtain the unlimited protection capability without changing the service IP address.
- Connect your services to AAD to obtain the Tbit/s protection capability. The malicious attacks targeting the origin servers can be diverted to the high-defense IP address for scrubbing to ensure the stable running of mission-critical workloads.

1.3 What are the Relationships Between DDoS Mitigation and the Anti-DDoS, CNAD Pro, and AAD Services?

Anti-DDoS is free while CNAD Advanced and AAD are paid services.

1.4 What Are the 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 1-2](#).

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

Item	Anti-DDoS	Advanced Anti-DDoS
Cost	Free	Charged
Protection capability		A maximum of 1 Tbit/s protection capacity
Protected objects	HUAWEI CLOUD resources only	HUAWEI CLOUD, non-HUAWEI CLOUD, and on-premises resources
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

1.5 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.

1.6 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.

1.7 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.

1.8 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.

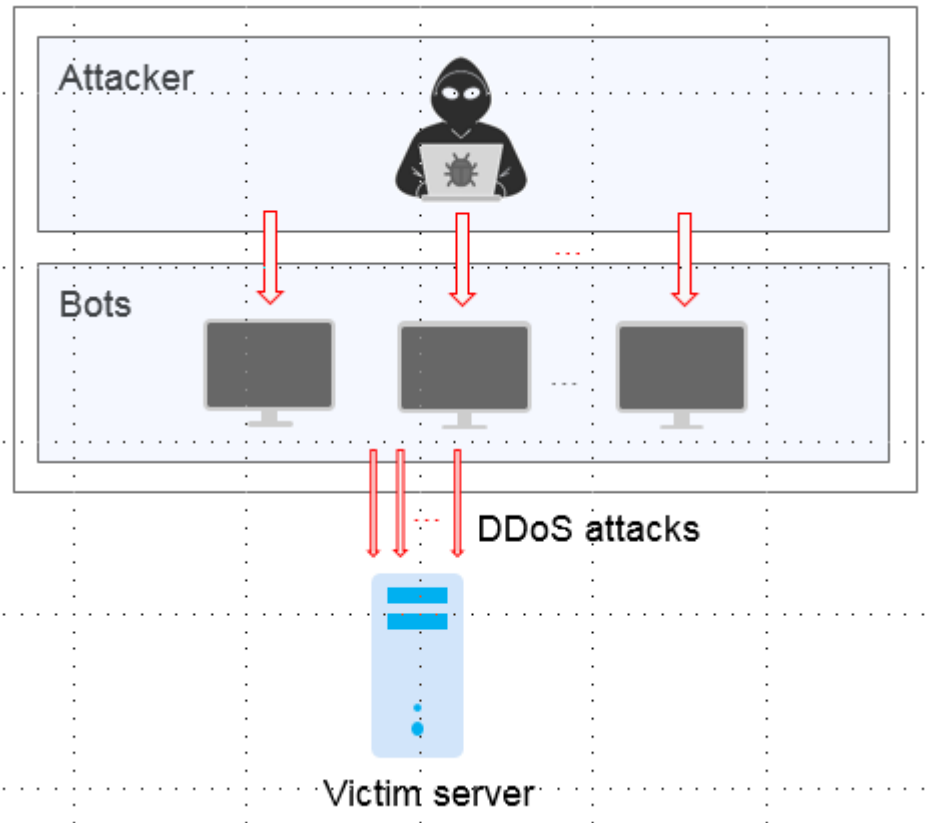
1.9 What Are the Differences Between DDoS Attacks and Challenge Collapsar Attacks?

Challenge Collapsar (CC) attack is a type of Distributed Denial of Service (DDoS) attack.

DDoS Attack

DDoS attacks are distributed and coordinated large-scale DoS attacks. Multiple attackers in different locations launch attacks to one or more targets at the same time, or an attacker controls multiple compromised computers in different locations and uses these computers to attack the victim at the same time. The DDoS attack process consists of target confirmation, botnet establishment, attack launching.

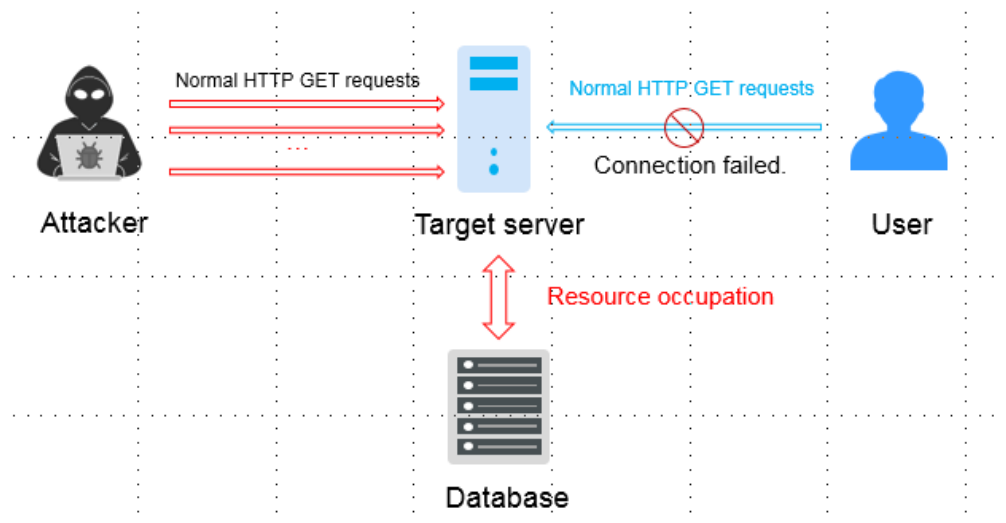
Figure 1-1 DDoS attack



CC Attack

A Challenge Collapsar (CC) attack is an attack that standard HTTP requests are sent to a targeted web server frequently. The attacker controls some servers to keep sending a large number of data packets to the target server, causing resource exhaustion and breakdown of the server.

Figure 1-2 CC attack



1.10 Does Anti-DDoS Support the Transparent Access Mode?

The CNAD Basic and CNAD Advanced support the transparent access mode. They can be used to defend your Huawei Cloud public IP addresses against DDoS attacks, with no need to modify domain name resolution or set origin server protection.

AAD works in proxy mode and needs to be connected using domain names or IP addresses. After AAD is connected, the malicious attacks targeting the origin servers can be diverted to the high-defense IP address for scrubbing to ensure that mission-critical workloads run stably.

2 CNAD Basic (Anti-DDoS) FAQs

2.1 About Anti-DDoS

2.1.1 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.

2.1.2 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 section "Configuring an Anti-DDoS Protection Policy".

2.1.3 Does Anti-DDoS Traffic Cleaning Affect Normal Services?

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

If you are worried that normal traffic may be discarded mistakenly, you can set the traffic cleaning threshold to 1000 Mbit/s, a value so large that your EIPs get almost no protection from Anti-DDoS.

2.1.4 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.

2.2 About Basic Functions

2.2.1 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

2.2.2 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.

2.2.3 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.

2.2.4 How Do I Temporarily Disable Anti-DDoS?

You can set the traffic cleaning threshold to 1000 Mbit/s, a value so large that your EIP gets almost no protection from DDoS attacks.

NOTE

This value is suitable for temporary disabling of protection for commissioning or other special purposes. You are advised not to use it for a long time.

Procedure

Step 1 Log in to the management console.

Step 2 Go to the Anti-DDoS console.

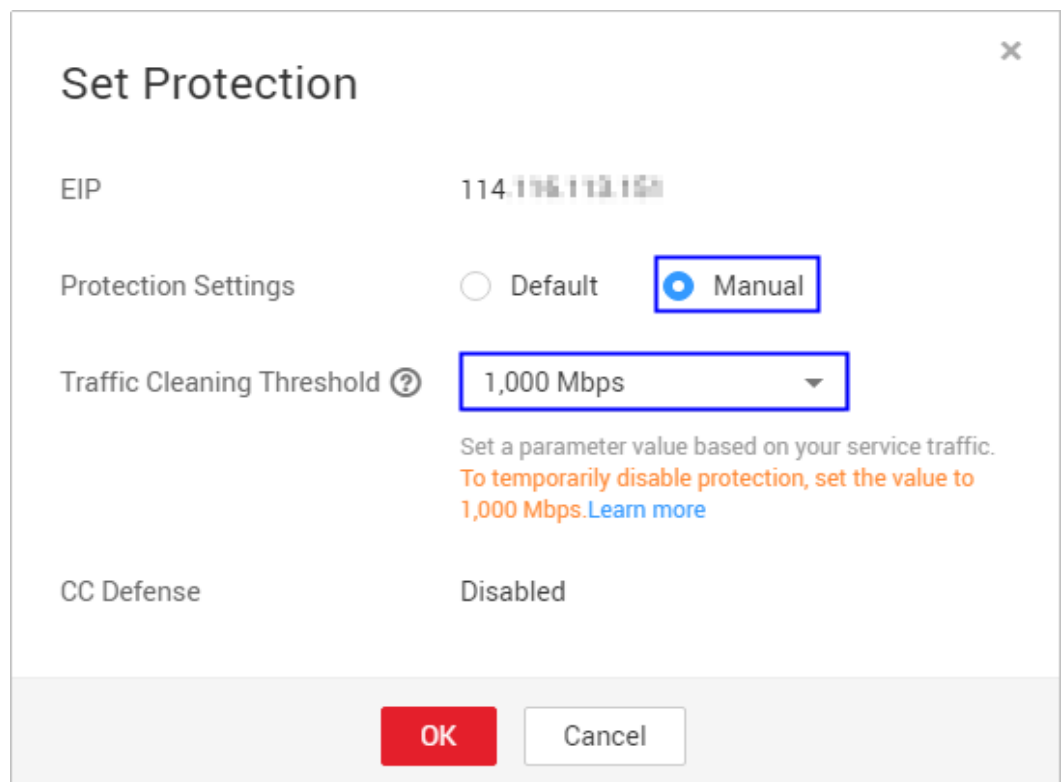
Figure 2-1 Anti-DDoS console



Step 3 Click the **Public IP Addresses** tab, locate the row that contains the IP address for which you want to set protection, and click **Set Protection** in the **Operation** column.

Step 4 In the dialog box that is displayed, set **Protection Settings** to **Manual** and **Traffic Cleaning Threshold** to **1,000 Mbps**.

Figure 2-2 Protection settings



Step 5 Click **OK**.

----End

2.3 About Alarm notification

2.3.1 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 section "Enabling Alarm Notification".

2.3.2 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 SMS messages or emails when the public IP address is under DDoS attacks.

You can log in to the management console to view the protection status of of an EIP. If you do not want the traffic to be scrubbed, increase the traffic cleaning threshold. For details, see section "Configuring an Anti-DDoS Protection Policy".

2.3.3 How Do I Enable Anti-DDoS Blocking Notifications?

Description

On the Anti-DDoS console, only the traffic scrubbing notifications can be enabled. To receive notifications about EIP blocking, perform the following steps.

Procedure


- Step 1** Log in to the Anti-DDoS console.
- Step 2** Select your region in the upper part of the page, click  in the upper left corner of the page, and choose **Management and Governance** > **Cloud Eye**. The **Overview** page is displayed.
- Step 3** In the navigation tree on the left, choose **Event Monitoring**. The **Event Monitoring** page is displayed.
- Step 4** Click **Create Alarm Rule** in the upper left corner. The **Create Alarm Rule** page is displayed.
- Step 5** Parameters for configuring the EIP blocking alarms
 - **Alarm Type:** Event
 - **Event Type:** System event
 - **Event Source:** Elastic IP
 - **Alarm Policy:** Select **EIP Blocked** and select the **Alarm Severity**.

Figure 2-3 Parameters of the EIP blocking alarms

The screenshot shows the configuration page for an alarm. Key elements include:

- Name:** alarm-100
- Description:** (empty)
- Alarm Type:** Metric, Event, Website (Event is selected)
- Event Type:** System event, Custom event (System event is selected)
- Event Source:** Elastic IP (highlighted with a red box)
- Monitoring Scope:** All resources, Specific resources (All resources is selected)
- Method:** Configure manually
- Alarm Policy:** A table with columns: Event Name, Alarm Policy, Count, Then, Alarm Severity, and Operation.

Event Name	Alarm Policy	Count	Then	Alarm Severity	Operation
if EIP bandwidth over	Immediate trigger	1	Count	Then An alarm is generated.	Major Delete
if Delete EIP	Immediate trigger	1	Count	Then An alarm is generated.	Major Delete
if EIP blocked	Immediate trigger	1	Count	Then An alarm is generated.	Major Delete
if Start DDoS traffic s	Immediate trigger	1	Count	Then An alarm is generated.	Major Delete

Step 6 Click **Create**.

----End

2.4 About Service Faults

2.4.1 Why Is the Traffic Volume of a Public IP Address is Low?

Troubleshooting:

1. Anti-DDoS provides a 2 Gbit/s DDoS mitigation capacity for free, and its maximum mitigation capacity can reach 5 Gbit/s (depending on the available bandwidth of HUAWEI CLOUD). Traffic that exceeds 5 Gbit/s will be routed to a black hole. For applications threatened by attack traffic larger than 5 Gbit/s, it is a better choice to purchase the Advanced Anti-DDoS service on HUAWEI CLOUD to expand protection capacity.
2. Check the HTTP request threshold. If the actual HTTP request threshold is greater than or equal to the configured value, Anti-DDoS triggers CC defense to analyze and check each request, which affects responses to normal requests.

If the fault persists, contact HUAWEI CLOUD security technical experts.

2.4.2 Why Is the Access from the Internet Abnormal?

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.

Anti-DDoS provides a 2 Gbit/s DDoS mitigation capacity for free, and its maximum mitigation capacity can reach 5 Gbit/s (depending on the available bandwidth of HUAWEI CLOUD). Traffic that exceeds 5 Gbit/s will be routed to a black hole. For applications threatened by attack traffic larger than 5 Gbit/s, it is a better choice to purchase the Advanced Anti-DDoS service on HUAWEI CLOUD to expand protection capacity.

2.4.3 Traffic Scrubbed Unexpectedly Without Traffic Fluctuations Reported

Troubleshooting:

1. Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the traffic cleaning threshold. If you do not want the traffic to be scrubbed, increase the traffic cleaning threshold. For details, see section "Configuring an Anti-DDoS Protection Policy".
2. After the alarm notification function is enabled for your Anti-DDoS service, you will receive SMS messages or emails when the public IP address is under DDoS attacks. It is normal if you receive an alarm notification.

2.4.4 What Should I Do If Access to a Client Is Denied Due to DDoS Attacks?

You can use the view the anomalies of a single public IP address within the last 24 hours in the monitoring report, or view the protection statistics of all public IP addresses, such as the Top 10 attacked public IP addresses in the interception report, to determine whether the access to a client is blocked due to the black hole triggered when your services are under DDoS attacks.

The system automatically deactivates the black hole 24 hours after the access to a cloud server was blocked due to the triggered black hole.

2.4.5 How Do I Query the Protection Information About a Public IP Address That Is Under DDoS Attacks?

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.

2.4.6 Is Traffic Cleaning Triggered Even If No Attack Occurs?

Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the traffic cleaning threshold. If you do not want the traffic to be scrubbed, increase the traffic cleaning threshold. For details, see section "Configuring an Anti-DDoS Protection Policy".