Anti-DDoS Service

FAQs

Issue 03

Date 2024-11-29

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 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 the attack traffic on the cloud server exceeds the threshold, a black hole will be triggered to block all accesses from the Internet for a certain period of time.

What Is a Black Hole?

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

Why Is the Blackhole Policy Required?

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

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

How Do I Deactivate a Black Hole?

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

Table 1-1 Black hole deactivation methods

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

1.3 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.

1.4 What Is a CC Attack?

In a challenge collapsar (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.

1.5 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.

1.6 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.

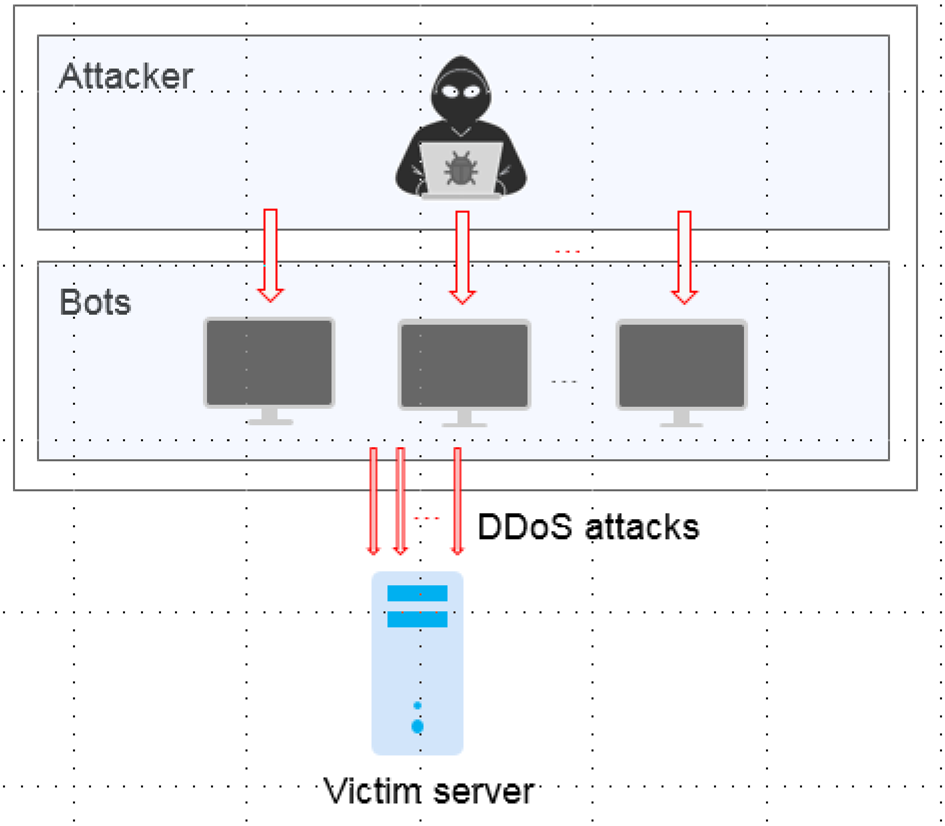
1.7 What Are the Differences Between DDoS Attacks and Challenge Collapsar Attacks?

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.

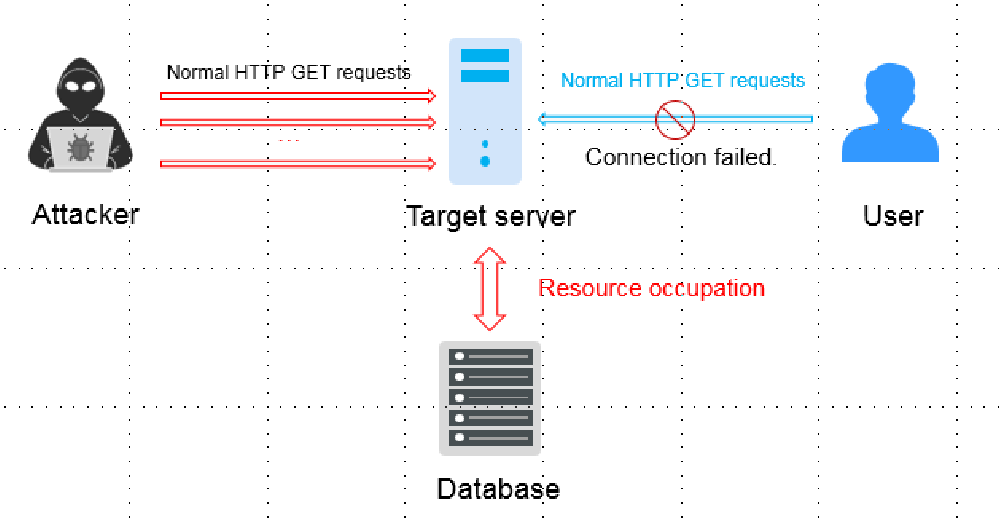
Figure 1-1 DDoS attack



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



1.8 Does Anti-DDoS Provide SDKs and APIs?

Currently, only Cloud Native Anti-DDoS Basic supports SDK access.

2 CNAD Basic (Anti-DDoS) FAQs

2.1 About Anti-DDoS

2.1.1 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

2.1.2 Does Anti-DDoS Traffic Scrubbing 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.

2.1.3 What Are the Restrictions of Using 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.

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.

2.3 About Threshold and Black Hole

2.3.1 How Does the Traffic Scrubbing 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 Anti-DDoS traffic scrubbing threshold is **120 Mbps**. You can adjust the threshold based on your service bandwidth. For details, see **Setting a Protection Policy**.

2.3.2 How Do I Set the Anti-DDoS Traffic Scrubbing 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 traffic scrubbing threshold based on your service bandwidth. For details, see **Setting a Protection Policy**.

- 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.

2.4 About Alarm Notification

2.4.1 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 .

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

An alarm notification does not necessarily means 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 .

2.4.3 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 management 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.

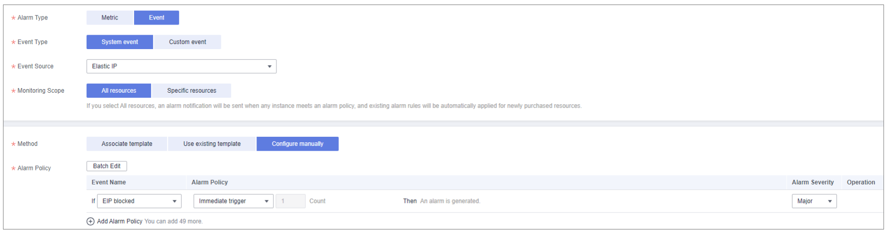
Step 3 In the navigation tree on the left, choose **Event Monitoring**. The **Event Monitoring** page is displayed.

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**
- **Method**: Select **Configure manually**.
- **Alarm Policy**: Select **EIP Blocked** and select the **Alarm Severity**.
- **Notification Method**: Select a notification method.

Figure 2-1 Parameters of the EIP blocking alarms



* Alarm Type: Event

* Event Type: System event

* Event Source: Elastic IP

* Monitoring Scope: All resources

If you select All resources, an alarm notification will be sent when any instance meets an alarm policy, and existing alarm rules will be automatically applied for newly purchased resources.

* Method: Configure manually

* Alarm Policy

Event Name	Alarm Policy				Alarm Severity	Operation
If EIP blocked	Immediate trigger	1	Count	Then An alarm is generated.	Major	

Add Alarm Policy You can add 49 more.

Step 6 Click **Create**.

----End

2.5 About Service Faults

2.5.1 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.

2.5.2 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.

2.5.3 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.

2.5.4 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".