Anti-DDoS Service

FAQs

Issue 08

Date 2025-08-20

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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.

Contents

1 General FAQs

1.1 What Are Regions and AZs?

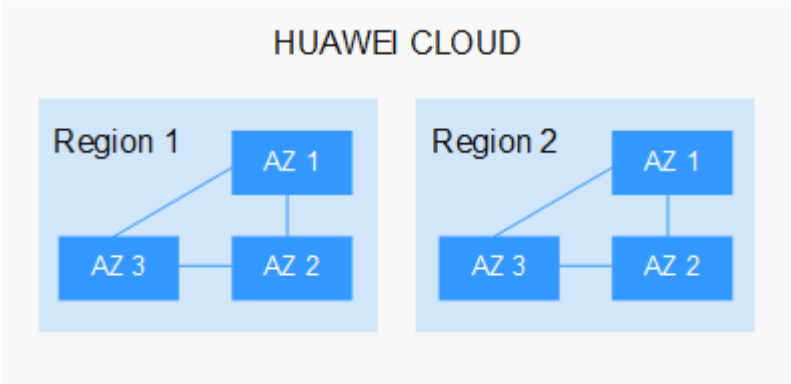
Concepts

A region or an availability zone (AZ) identifies the location of a data center. You can create resources in a specific region or an 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 1-1 shows the relationship between the regions and AZs.

Figure 1-1 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.

  - If you or your users are in the Asia Pacific region and outside the Chinese mainland, select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If you or your users are in Africa, select the **AF-Johannesburg** region.
  - If you or your users are in Latin America, select the **LA-Santiago** 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**.

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 Blackhole?

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 blackhole.

How Do I Deactivate a Blackhole?

After a blackhole is executed, Huawei Cloud continuously monitors the DDoS attack status. After the attack ends, Huawei Cloud automatically removes the blackhole from the ECS and restores Internet access.

When a server (ECS) enters is put in the blackhole, 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 blackhole is automatically removed after the traffic enters the blackhole for 24 hours. • 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.
Cloud Native Anti-DDoS Pro	• The blackhole is automatically removed after the traffic enters the blackhole for 24 hours. • 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.

Anti-DDoS Edition	Deactivation Policy	Deactivation Method
Advanced Anti-DDoS	The default blackhole duration is 30 minutes.	You need to wait until the system deactivates it automatically.

1.3 What are the Relationships Between ADS and Anti-DDoS Traffic Cleaning, CNAD Pro, and AAD?

Huawei Cloud provides multiple security solutions to defend against DDoS attacks. You can select an appropriate one based on your service requirements. Huawei Cloud Anti-DDoS Service provides three sub-services: Cloud Native Anti-DDoS Basic, Cloud Native Anti-DDoS Advanced, and Advanced Anti-DDoS.

Cloud Native Anti-DDoS Basic is free while Cloud Native Anti-DDoS Advanced and Advanced Anti-DDoS are paid services.

The application scenarios and DDoS protection capabilities of the three sub-services are shown in **Table 1-2**.

Table 1-2 Anti-DDoS service editions

Edition	Description	Application Scenario	DDoS Protection Capability
Cloud Native Anti-DDoS Basic	Cloud Native Anti-DDoS Basic monitors the service traffic from the Internet to public IP addresses and detects attack traffic in real time. It then scrubs attack traffic based on user-configured defense policies without interrupting services. It also generates monitoring reports that provide visibility into the security of network traffic.	You can use this service to protect your Huawei Cloud EIPs (IPv4 and IPv6) against the DDoS attacks if you have only basic security requirements.	Cloud Native Anti-DDoS Basic provides 500 Mbit/s DDoS attack defense for users free of charge.

Edition	Description	Application Scenario	DDoS Protection Capability
Cloud Native Anti-DDoS Advanced	Cloud Native Anti-DDoS Advanced is developed to improve the anti-DDoS capabilities of cloud services such as ECS, ELB, WAF, and EIP. Cloud Native Anti-DDoS Advanced takes effect for IP addresses on Huawei Cloud. You do not need to change the IP addresses. With few clicks on the console, you can enjoy always-on DDoS mitigation.	Cloud Native Anti-DDoS Advanced is used to protect your Huawei Cloud services (with public IP addresses assigned to) from DDoS attacks, meeting your requirements for immense protection capability and high network quality. Cloud Native Anti-DDoS Advanced can be used for the following scenarios: • Occasional DDoS attacks **NOTE** If you require Tbps-level cloud native protection, you are advised to select Cloud Native Anti-DDoS Advanced - Unlimited Protection Advanced Edition. • Huawei Cloud services with public IP addresses assigned for external communication **NOTICE** The CNAD Unlimited Protection Advanced edition must use EIPs in the dedicated resource pool of the Cloud Native Anti-DDoS Advanced unlimited protection editions. • Services with high bandwidth requirements and high Queries per Second (QPS), such as online video and live streaming • IPv6 protection • A large number of public IP addresses on Huawei Cloud. A large number of ports, domain names,	• Cloud Native Anti-DDoS Advanced - Unlimited Protection Basic Edition Shared protection for not less than 20 Gbit/s of traffic • Cloud Native Anti-DDoS Advanced - Unlimited Protection Advanced Edition Unlimited protection, with up to 1 Tbit/s protection capability. Dedicated EIPs and service bandwidth are billed separately.

Edition	Description	Application Scenario	DDoS Protection Capability
		and IP addresses need to be protected from DDoS attacks. **NOTICE** CNAD Advanced can work with only cloud WAF. For details, see **Using WAF, ELB, and CNAD Advanced to Improve Website Service Security**.	
Advanced Anti-DDoS	Advanced Anti-DDoS works as a proxy and uses Advanced Anti-DDoS IP addresses to forward requests to origin servers. All public network traffic is diverted to the high-defense IP address so that the origin server is hidden from the public. This protects origin servers from DDoS attacks.	Huawei Cloud, non-Huawei Cloud, and IDC hosts can be protected. Advanced Anti-DDoS applies to the following scenarios: Services are frequently attacked by DDoS attacks. Continuous protection is required to ensure service continuity. **NOTICE** • Advanced Anti-DDoS does not support domain names that have no ICP licenses. To use Advanced Anti-DDoS to protect website services, ensure that the website domain name has an ICP license. • The quality of network access from users in the Chinese mainland to users outside the Chinese mainland cannot be guaranteed.	One high-defense IP address is able to defend against 1 Tbit/s network-, and application-layer DDoS attacks. The Advanced Anti-DDoS service offers more than 15 Tbit/s of defense capability. • 15 Tbit/s of defense capability is the overall defense capability of the Advanced Anti-DDoS equipment room. • 1 Tbit/s of defense capability refers to the maximum protection capability of a single high-defense IP address.

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 1-3**.

Table 1-3 Differences between Anti-DDoS and Advanced Anti-DDoS

Item	Anti-DDoS	Advanced Anti-DDoS
Cost	Free	Charged
Protection capability	A maximum of 500 Mbit/s protection	A maximum of 1 Tbit/s protection
Protected objects	HUAWEI CLOUD resources only	HUAWEI CLOUD, non-HUAWEI CLOUD, and on-premises resources
Protection policy	• Fixed protection policies • Globally applied policies	• Diverse protection policies • Basic 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 Slow HTTP Attack?

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

An attacker establishes a connection with a large content length from the client to the server, then sends packets to the server at a slow rate (e.g., one byte every one to ten seconds), maintaining the connection.

If the attacker continues to create such connections, the server's available connections are gradually consumed, causing the server to reject normal user requests.

1.7 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.

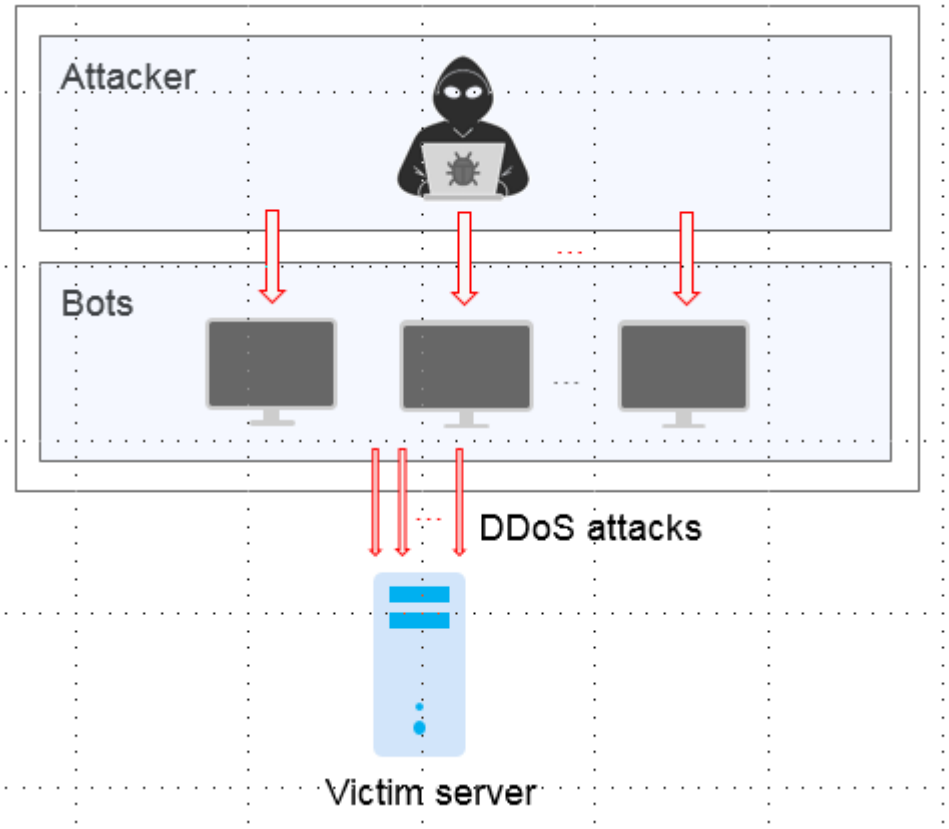
1.8 What Are the Differences Between DDoS Attacks and Challenge Collapsar Attacks?

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.

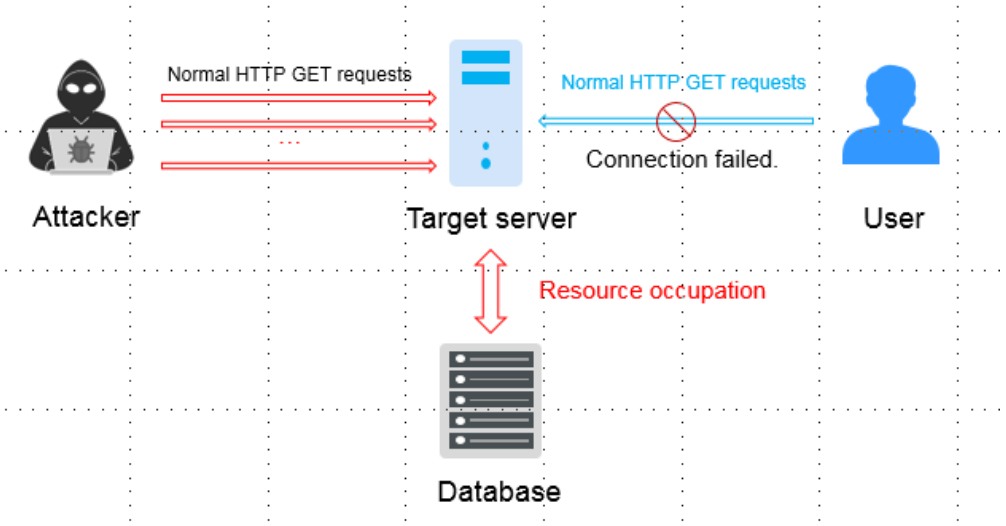
Figure 1-2 DDoS attack



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 1-3 CC attack



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.

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

Possible Causes

Huawei Cloud provides free basic CNAD service for common users. The protection capability depends on the available network bandwidth in the region where the asset is located. The protection capability in China is 2 Gbit/s to 5 Gbit/s, and that in regions outside China is 500 Mbit/s to 5 Gbit/s. A blackhole will be triggered to block accesses from the Internet within a time range when a cloud server is under volumetric traffic attacks.

CAUTION

- If the bandwidth (Bit/s) of normal service traffic is greater than the blackhole threshold, you need to increase the asset bandwidth in a timely manner. Otherwise, normal service traffic may be identified as abnormal traffic, causing the asset to be blackholed and service access to be interrupted.
- If your asset is under a DDoS attack, the attack traffic will also trigger a blackhole, interrupting service access. To ensure that your valuable assets have the maximum blackhole threshold within the available bandwidth of the Huawei Cloud network during a DDoS attack, purchase the Anti-DDoS service.

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 1-4** to handle that.

Table 1-4 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 blackhole is automatically removed after the traffic enters the blackhole for 24 hours. • 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.
Cloud Native Anti-DDoS Pro	• The blackhole is automatically removed after the traffic enters the blackhole for 24 hours. • 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.
Advanced Anti-DDoS	The default blackhole duration is 30 minutes.	You need to wait until the system deactivates it automatically.

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 accessed through 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.

1.11 Does Anti-DDoS Service Provide SDKs?

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

1.12 How Do I Migrate Instance Resources in an Enterprise Project?

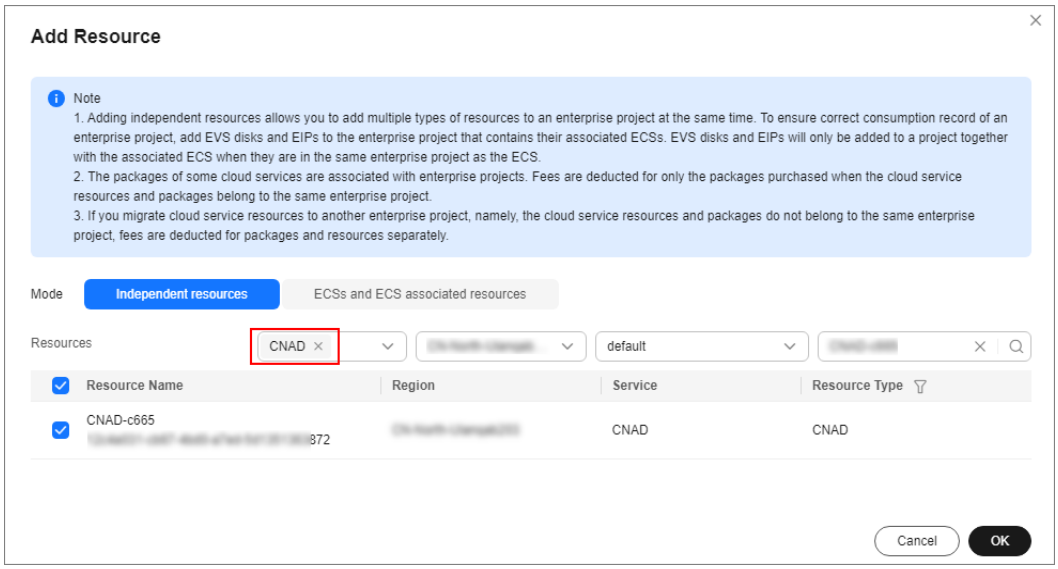
For details about how to migrate CNAD or AAD instance resources in enterprise projects, see **Adding Resources to an Enterprise Project**.

- To migrate CNAD resources, set **Resource** to **CNAD**.
- To migrate AAD resources, set **Resource** to **AAD**.

NOTE

AAD instances bound to domain names cannot be migrated. Unbind the domain names before migration.

Figure 1-4 Adding resources to an enterprise project



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 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.

2.1.4 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 scrubbing 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.

2.1.5 Can CNAD Basic Be Used Across Clouds or By Multiple Accounts?

CNAD Basic cannot be used by multiple accounts.

Currently, CNAD Basic only provides protection for services deployed on Huawei Cloud.

2.1.6 How to Determine Whether an Attack Occurs?

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

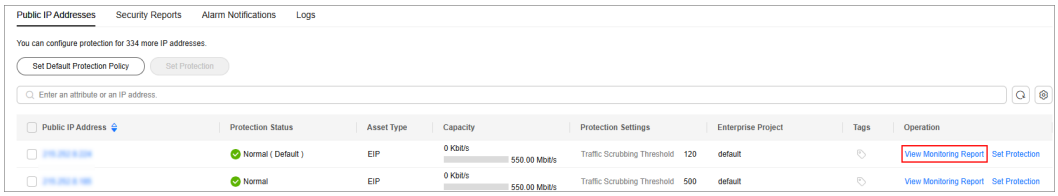
- For details about how to query attack traffic information and anomaly events within 24 hours, see **Method 1: Viewing Monitoring Reports**.
- For details about how to query information about public IP addresses attacked within one month, see **Method 2: Viewing the Security Report**.

Method 1: Viewing Monitoring Reports

Step 1 **Log in to the AAD console**.

Step 2 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**.

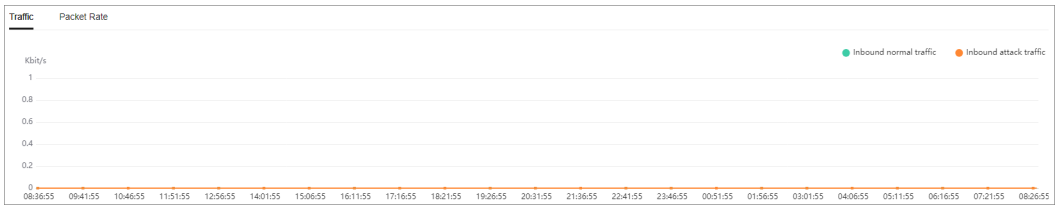
Figure 2-1 Viewing a monitoring report



Step 3 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 2-2 Monitoring reports



----End

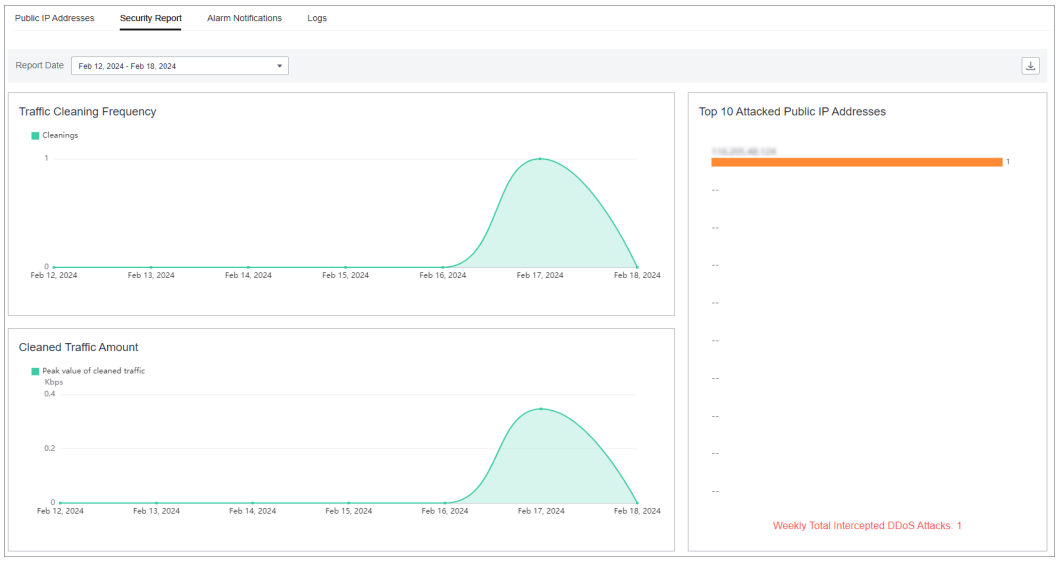
Method 2: Viewing the Security Report

Step 1 **Log in to the AAD console**.

Step 2 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 2-3 Security report



----End

2.2 About Basic Functions

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

For details about Anti-DDoS, CNAD, and AAD, see **Anti-DDoS service**.

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.

2.2.2 Which Types of Attacks Does Anti-DDoS Mitigate?

Anti-DDoS helps users mitigate the following attacks:

- Web server attacks

  SYN flood attacks
- Game attacks

  Including User Datagram Protocol (UDP) flood, SYN flood, Transmission Control Protocol (TCP), and fragment attacks

2.2.3 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 CNAD Advanced or AAD to expand protection capability.

CNAD Advanced is available for EIPs on Huawei Cloud. For details about how to purchase a CNAD Advanced instance, see **Purchasing a CNAD Instance**.

AAD can protect domain names or IP addresses. For details about how to purchase an AAD instance, see **Purchasing an AAD Instance**.

2.2.4 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.

2.2.5 Is CNAD Basic Enabled by Default?

Yes. CNAD Basic is enabled by default and uses the default protection policy.

For details about how to modify settings, see **Setting a Protection Policy**.

NOTE

Once enabled, Anti-DDoS cannot be disabled.

2.2.6 Does CNAD Basic Protect a Region or IP Addresses?

IP addresses.

CNAD Basic provides network- and application-layer DDoS attack defense for Huawei Cloud Elastic IPs (EIPs) for free. The protected objects are Huawei Cloud EIPs and are irrelevant to regions.

For more information about CNAD Basic, see **What Is Cloud Native Anti-DDoS Basic?**

2.2.7 Do I Need to Release Anti-DDoS Resources 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.

2.2.8 How Do I View the Traffic Scrubbing 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.

2.2.9 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.

2.2.10 How Can I View the Monitoring Data of a Public IP Address 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.

2.2.11 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.

2.2.12 Can I Disable Anti-DDoS Completely?

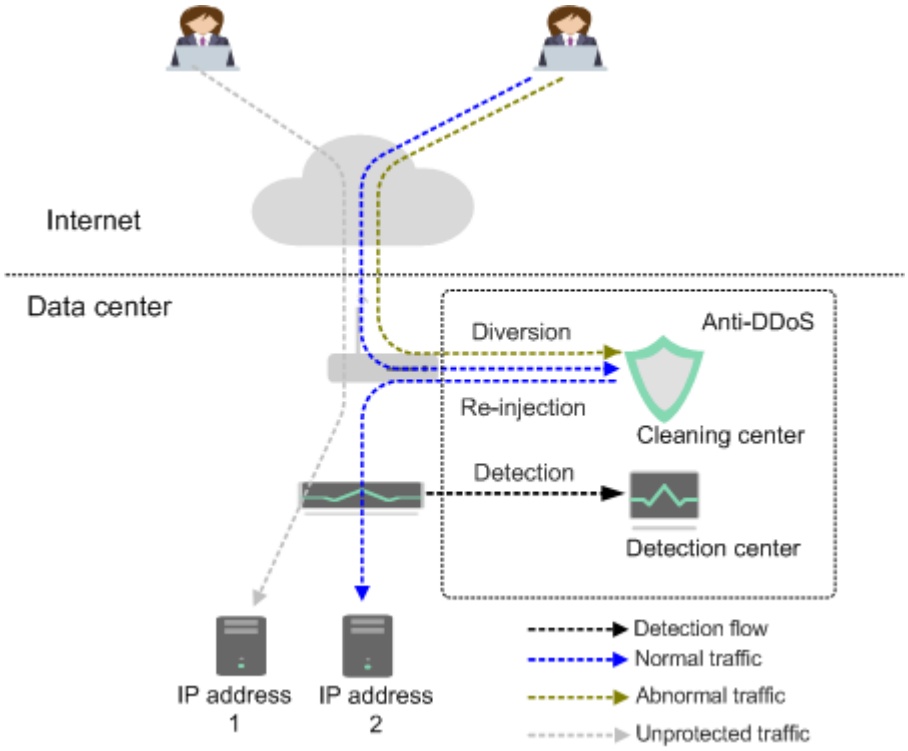
No.

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

2.2.13 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 2-4 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. On the VM of the EIP, you can check whether traffic is routed from the public network. If so, the inbound traffic is filtered 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.

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 scrubbing 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**.

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 threshold based on the actual service bandwidth. For details, see **Configuring an Anti-DDoS 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.

2.3.3 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.

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 **Enabling Alarm Notifications**.

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 **Configuring an Anti-DDoS Protection Policy**.

2.4.3 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.

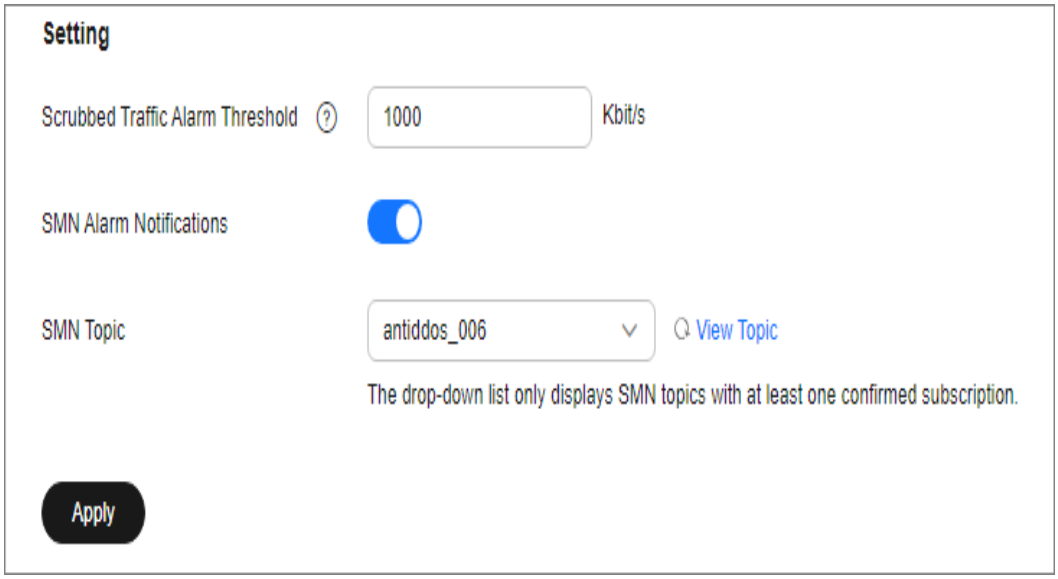
Disabling Alarm Notifications

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 AAD console**.

Step 2 Click the **Alarm Notifications** tab and click  to disable the alarm notification function.

Figure 2-5 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.

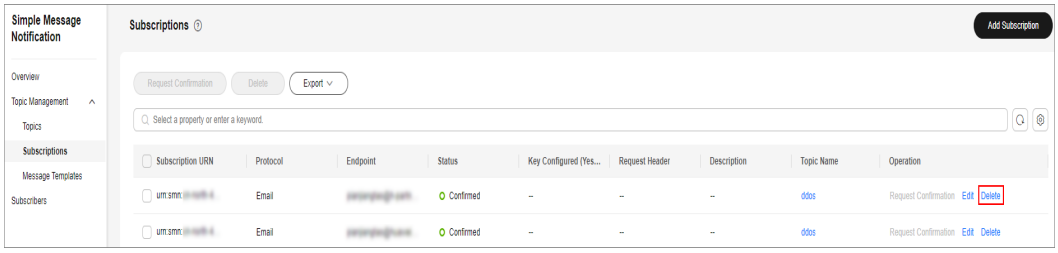
Procedure

Step 1 **Log in to the SMN console.**

Step 2 In the navigation pane on the left, choose **Topic Management** > **Subscriptions**.

Step 3 Locate the target subscription and click **Delete** in the **Operation** column.

Figure 2-6 Deleting the Subscription



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**.

2.4.4 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 Cloud Eye console.**

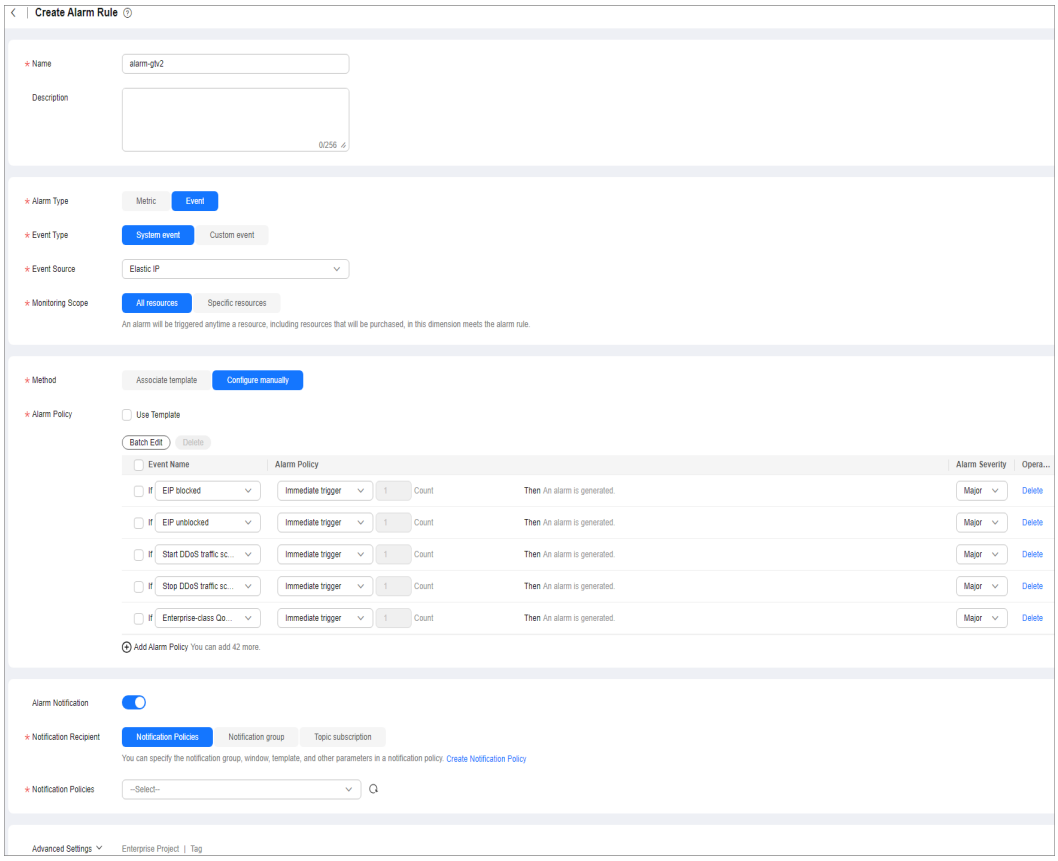
Step 2 In the navigation tree on the left, choose **Event Monitoring**. The **Event Monitoring** page is displayed.

Step 3 Click **Create Alarm Rule** in the upper right corner. The **Create Alarm Rule** page is displayed.

Step 4 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 2-7 Alarm parameters



Step 5 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".

3 CNAD Advanced FAQs

3.1 Function Consulting

3.1.1 What Is Unlimited Protection?

CNAD Unlimited Protection provides as high DDoS mitigation bandwidth as possible based on the network and resources in the current region. The protection capability provided grows with the improvement of Huawei Cloud's network capabilities.

Currently, two editions are available: CNAD Unlimited Protection Basic Edition and CNAD Unlimited Protection Advanced Edition.

3.1.2 Can CNAD Advanced Protect Non-Huawei Cloud and On-Premises IP Addresses?

CNAD Advanced protects Huawei Cloud resources that use public IP addresses, such as ECSs, ELBs, WAFs, and EIPs, while cannot protect non-Huawei Cloud and on-premises resources.

3.1.3 Does CNAD Advanced Protect IPv6 Addresses?

Yes, CNAD Advanced protects Huawei Cloud public IP addresses (IPv6 and IPv4).

3.1.4 What Do I Do If an IP Address Protected by CNAD Advanced Is Blocked?

You can use the self-service unblocking function to unblock the blocked IP addresses.

3.1.5 What Are the Protection Objects of CNAD Advanced?

CNAD Advanced protects Huawei Cloud resources, such as ECS, ELB, WAF, and EIP, by public IP addresses.

3.1.6 How Many Layers of Attacks Can CNAD Advanced Defend Against?

CNAD Advanced can defend against Layer 3 and Layer 4 traffic attacks. To defend against Layer 7 traffic attacks, you need to configure the joint protection with the dedicated WAF.

3.1.7 How Long Does It Take to Switch Traffic from CNAD Advanced Back to AAD?

It takes about 5 to 10 minutes to switch traffic from CNAD Advanced Back to AAD.

The required time depends on how long that the DNS domain name and the local recursive DNS can take effect. During the switch, the traffic may exist in both the CNAD Advanced IP address and AAD IP address.

3.1.8 Can CNAD Advanced Be Used Across Regions?

In CNAD Advanced, only Cloud Native Anti-DDoS 2.0 supports cross-region protection.

3.1.9 What Is A Dedicated EIP?

A dedicated EIP is an IP address dedicated to the Anti-DDoS Service. While common EIPs are protected against attacks within the local equipment room of Huawei Cloud, dedicated EIPs are protected at the Anti-DDoS scrubbing center, enjoying Terabit-level bandwidth and robust protection capabilities.

Once a dedicated EIP is associated with an ECS, it can be added to Unlimited Protection Advanced Edition and Cloud Native Anti-DDoS 2.0 for enhanced security. To purchase an Anti-DDoS Service dedicated EIP, perform the following steps:

Procedure

Step 1 **Log in to the EIP console.**

Step 2 Purchase dedicated EIPs in the required region by referring to **Assigning an EIP**.

Table 3-1 Network lines for dedicated EIPs

Region	Line
CN South-Guangzhou	5_ddosalways1bgp
CN North-Beijing2	5_DDoSAlways1bgp
CN North-Beijing4	5_DDoSAlways1bgp
CN East-Shanghai1	5_ddosalways1bgp
CN East-Shanghai2	5_DDoSAlways1bgp
CN-Hong Kong	5_DDoSAlways2bgp

Region	Line
AP-Singapore	5_DDoSAlways1bgp

NOTE

The preceding line names are for reference only. The actual line names are displayed on the console.

----End

3.1.10 Does CNAD Advanced Support Bypass?

CNAD Advanced does not support bypass.

If the service is abnormal, traffic is scheduled through different routes for disaster recovery, which does not affect normal services.

3.1.11 What Should I Do If the Protection Capability of CNAD Deteriorates After the Service Bandwidth Exceeds the Threshold?

The timing for crossing the service bandwidth threshold of CNAD is as follows:

When the average service bandwidth per minute of all IP addresses in the protection package is greater than the purchased service bandwidth plus the purchased elastic service bandwidth, the system starts to record the threshold-crossing duration.

If the service bandwidth exceeds the threshold for **36 hours**, the protection capability deteriorates. For details, see **Table 3-2**.

Table 3-2 Service bandwidth exceeding the threshold

Type	CNAD 1.0		CNAD 2.0	
Edition	**Unlimited Protection Basic Edition**	**Unlimited Protection Advanced Edition**	**Enterprise edition**	**SME edition**
Description	If the service bandwidth exceeds the limit, the protection capability drops and ranges from 10 Gbit/s to 20 Gbit/s.	If the service bandwidth exceeds the limit, the protection capability drops and ranges from 10 Gbit/s to 20 Gbit/s.	• Chinese mainland: If the service bandwidth exceeds the limit, the protection capability drops and ranges from 10 Gbit/s to 20 Gbit/s. • Outside the Chinese mainland: If the service bandwidth exceeds the limit, the protection capability drops to 5 Gbit/s.	Chinese mainland: If the service bandwidth exceeds the limit, the protection capability drops and ranges from 10 Gbit/s to 20 Gbit/s.

You can use the following methods to restore the protection capability:

- Wait until next month for the protection capability to automatically recover.
- Upgrade the service bandwidth of the instance. For details, see **Modifying Specifications of an Instance**.
- Enable elastic service bandwidth. For details, see **Modifying Specifications of an Instance**.

3.2 Billing

3.2.1 How Will I Be Charged for Using CNAD?

Pricing

For price details, see **Product Pricing Details**.

Billing Mode

CNAD advanced service is billed based on the edition and specifications you select. For details, see **Billing Items**.

3.2.2 Will I Be Charged for Using the Bandwidth of CNAD Advanced?

There are two editions of CNAD Advanced: CNAD Unlimited Protection Basic and CNAD Unlimited Protection Advanced.

Service bandwidth charges apply to all three editions.

AAD diverts attacking traffic to high-defense IP addresses, which incurs extra service bandwidth fees through the Internet. CNAD Unlimited Protection Basic and CNAD Unlimited Protection Advanced can directly forward the traffic within Huawei Cloud, and no extra service bandwidth fee is generated over the Internet.

3.2.3 How Do I Unsubscribe From CNAD Advanced?

CNAD Advanced paid monthly/yearly cannot be unsubscribed unconditionally. If your conditions meet the unsubscription criteria, you can contact the customer service to apply for unsubscription.

Unsubscription Criteria

If you find that CNAD Advanced does not suit your businesses, you can contact the customer service personnel to unsubscribe from CNAD Advanced.

CNAD Advanced instances in use cannot be unsubscribed. The CNAD Advanced background can detect whether the service has been put to use. If it is used, it cannot be unsubscribed.

3.2.4 How Is Elastic Bandwidth Charged?

Billing Rules

The elastic bandwidth fees in different scenarios are described as follows:

- Actual service bandwidth ≤ Service bandwidth: No elastic service bandwidth fee is generated.
- Service bandwidth < Actual service bandwidth < Elastic bandwidth: Elastic bandwidth fees will be generated.
- Actual service bandwidth ≥ Elastic service bandwidth: Elastic service bandwidth fees will be generated.

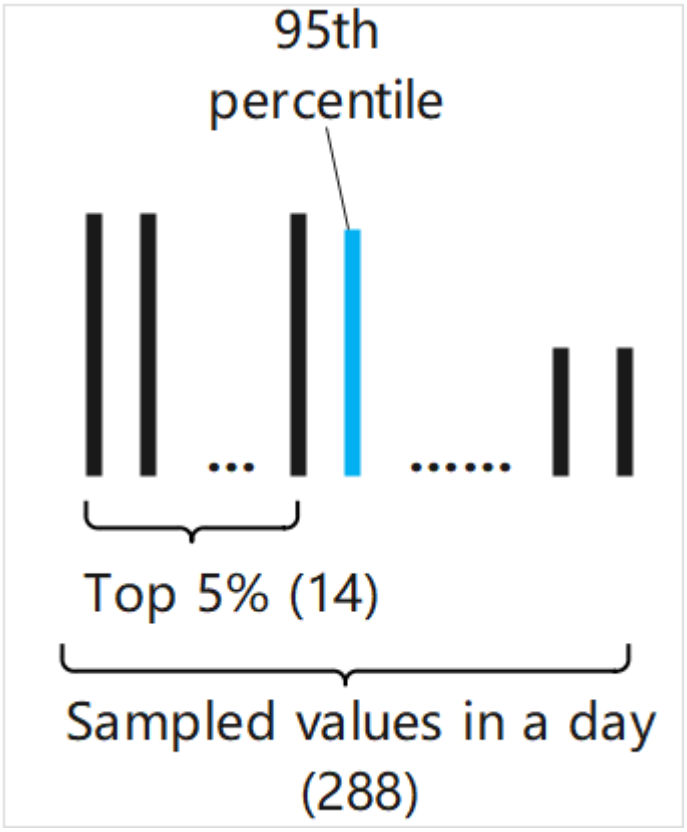
Billing Principles

Elastic bandwidth can be billed in two modes: daily 95th percentile billing and monthly 95th percentile billing.

- Daily 95th percentile billing

  The bandwidth is sampled every 5 minutes on a calendar day. The sampling vertices are sorted in descending order of peak values, the maximum value of 5% is removed, and the maximum value among the remaining values is used as the charged bandwidth. **Figure 3-1** describes how to calculate the daily 95th percentile billing bandwidth.

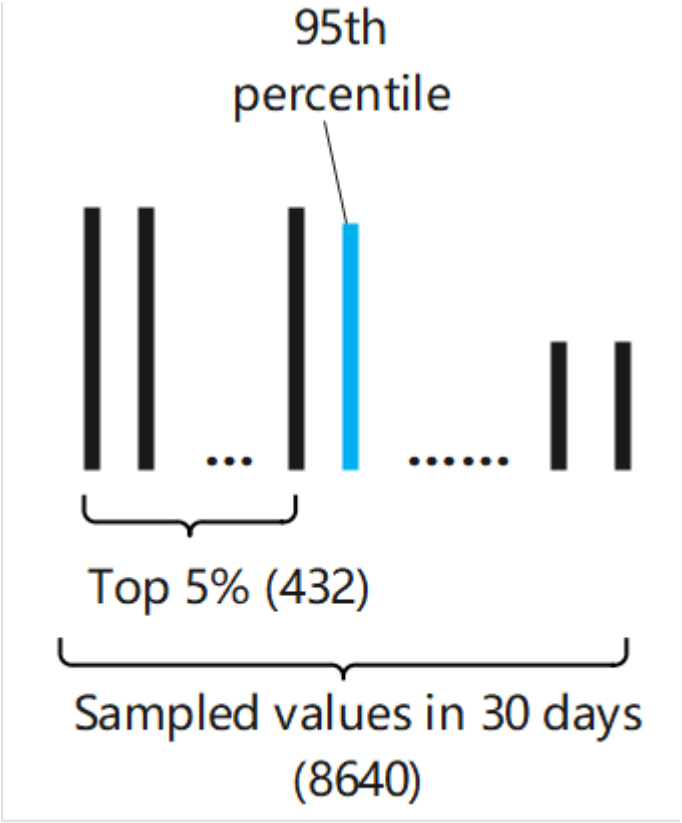
Figure 3-1 Daily 95th percentile billing



- Monthly 95th percentile billing

  The bandwidth is sampled every 5 minutes in a calendar month. The sampling vertices are sorted in descending order of the peak value, the maximum value of 5% is removed, and the maximum value among the remaining values is used as the charged bandwidth. **Figure 3-2** shows how to calculate the monthly 95th percentile bandwidth for 30 days.

Figure 3-2 Monthly 95th percentile billing



4 AAD FAQs

4.1 Function Specifications

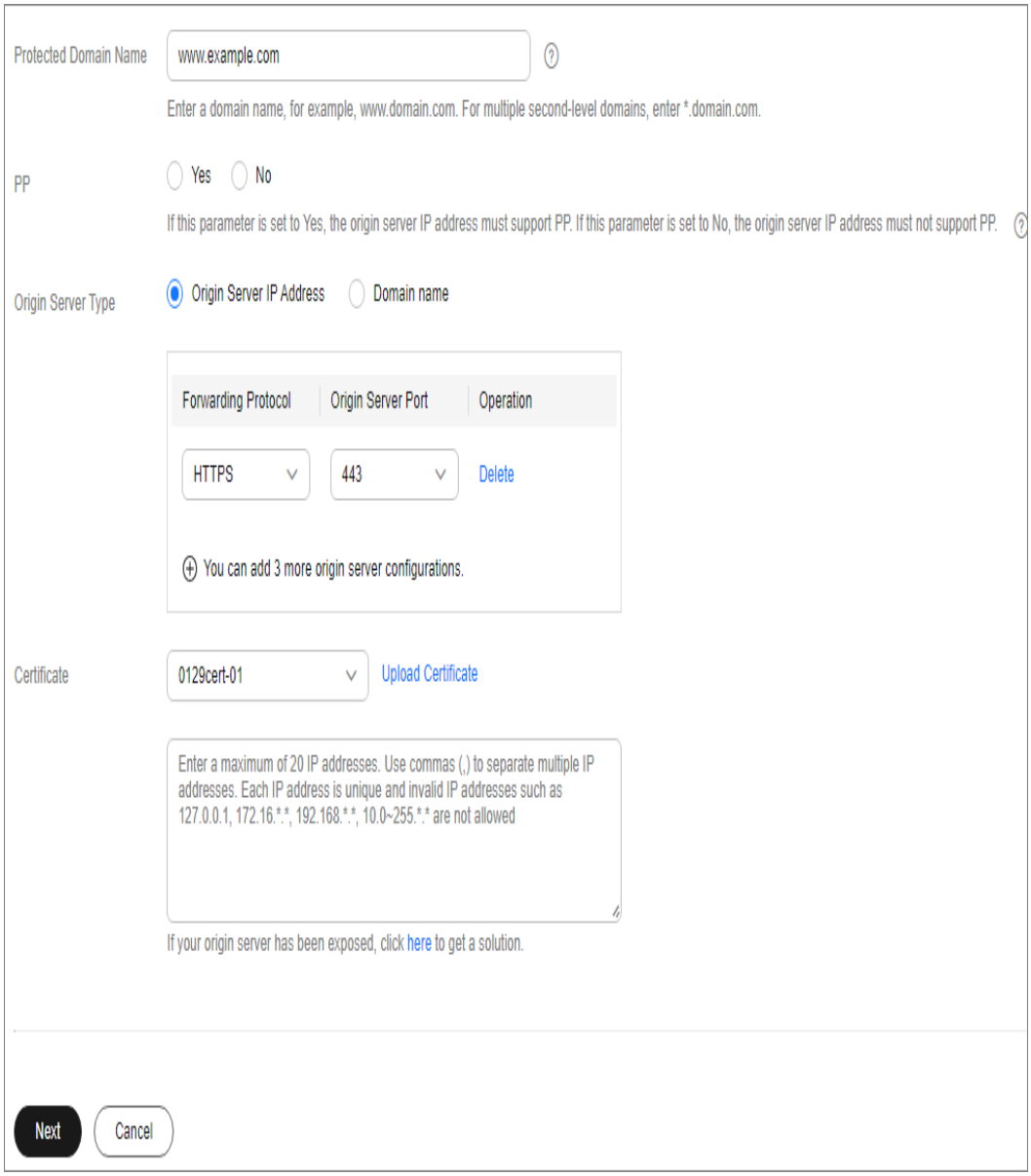
4.1.1 What Service Ports Does AAD Support?

Context

If your domain name needs to be connected to AAD and **Origin Server Type** is set to **IP Address**, you need to configure **Forwarding Protocol** and **Origin Server Port**.

- **Forwarding Protocol**: The protocol used by AAD to forward requests from clients (such as browsers).
- **Server Port**: The service port over which AAD forwards client requests to the service port of the origin server.

Figure 4-1 Configuring the origin server port



Service Ports Supported by AAD

- Four-layer protection

  The port range supported by AAD four-layer protection is **80-65535**.
- Seven-layer protection

Table 4-1 Ports supported by AAD seven-layer protection

Forwarding Protocol	Origin Server Port
HTTP	80, 81, 82, 83, 84, 85, 88, 133, 134, 140, 141, 144, 151, 881, 1135, 1139, 7000, 7001, 8006, 8078, 8080, 8087, 8088, 8089, 8090, 8093, 8097, 8100, 8182, 8200, 8813, 8814, 8888, 9000, 9001, 9002, 9003, 18080, 19101, 19501, 21028, 40010
HTTPS	443, 882, 1818, 4006, 4430, 4443, 5443, 6443, 7443, 8033, 8081, 8082, 8083, 8443, 8445, 8553, 8663, 8750, 8804, 8805, 9443, 9999, 13080, 14443, 18443, 18980, 20000, 28443, 30001, 30003, 30004, 30005

4.1.2 What Forwarding Protocols Does AAD Support?

Huawei Cloud supports the following forwarding protocols:

- Four-layer protocol: TCP and UDP
- Seven-layer protocol: HTTP/WebSocket and HTTPS/WebSockets

How to Configure HTTP/WebSocket and HTTPS/WebSockets Forwarding Protocols

On the **Anti-DDoS Service Center** page, choose **Advanced Anti-DDoS** > **Domain Name Access**. On the **Domain Name Access** page, click **Add Domain Name** to configure an HTTP/WebSocket or HTTPS/WebSockets forwarding protocol.

4.1.3 Can I Change My Protection Bandwidths?

- AAD allows you to upgrade the basic protection bandwidth.
- AAD allows you to modify the elastic protection bandwidth for a maximum of three times a day. The modification takes effect immediately.

4.1.4 Can an AAD Origin Server Use a CDN CNAME?

No. Currently, AAD supports only HUAWEI CLOUD WAF CNAME records.

4.1.5 What Is the Maximum Protection Capability When I Purchase 10 Gbit/s as the Basic Protection Bandwidth and 20 Gbit/s as the Elastic Protection Bandwidth?

Your maximum protection capability is 20 Gbit/s. The maximum protection capability is the elastic protection bandwidth. Do not mistake the elastic protection bandwidth as an increment over the basic protection bandwidth. If you purchase the same value for your basic and elastic protection bandwidths, the elastic protection capability will not take effect.

For example, if you purchase 50 Gbit/s for both the basic and elastic protection bandwidths, the maximum protection capability is 50 Gbit/s and the elastic protection will not take effect.

4.1.6 Does AAD Use a Public IP Address to Switch Traffic Back to Origin Servers?

Yes. AAD uses public IP addresses as the back-to-origin IP addresses to switch scrubbed traffic back to the origin servers over the public network.

4.1.7 What Is the Maximum Number of Domain Names AAD Can Protect?

By default, one AAD instance can protect 50 domain names for free. You can pay to increase this quota and a maximum of 200 domain names are available. If you want to purchase more than 200 domain names, purchase another AAD instance.

NOTICE

The number of domain names includes the total number of top-level domain names (for example, example.com), single domain names/subdomain names (for example, www.example.com), and wildcard domain names (for example, *.example.com). Each AAD instance can protect 50 single domain names or wildcard domain names, or protect one top-level domain name and 49 subdomain names or wildcard domain names related to the top-level domain name.

4.1.8 How Much Additional Latency Will Be Incurred When AAD Is Deployed?

After AAD is deployed, the average latency is increased by 30 ms. The actual service latency varies according to service conditions.

4.1.9 Is There a Limit to the Number of Concurrent Requests?

The number of concurrent requests that can be processed by a system indicates the load capacity of the system. A website needs to process concurrent requests sent from users.

AAD does not limit the number of concurrent requests. AAD supports multiple forwarding protocols such as TCP, UDP, HTTP, HTTPS, Websocket, and Websockets. AAD does not limit the number of TCP and HTTP connections.

4.1.10 How Do I Disable Advanced Anti-DDoS?

Advanced Anti-DDoS cannot be directly disabled on the console. If you do not want to use AAD anymore, remove the protected domain names configured in AAD, and then unsubscribe from AAD.

4.1.11 How Many Origin Server IP Addresses and Ports Does AAD Support?

In the domain name access scenario, AAD supports any number of origin server IP addresses. You can add a maximum of 20 origin server IP addresses at a time.

In the IP access scenario, each AAD instance outside the Chinese mainland provides protection for five source site ports for free. You can add up to 200 domain names at an additional cost.

4.1.12 Can an AAD Instance Support Both Website and IP Address Access?

For security purposes, an instance supports only one access type. If you have multiple service types, purchase instances of different access types.

4.2 Access Configuration

4.2.1 Can I Connect My Service System to AAD If It Is Not Running on HUAWEI CLOUD?

Yes, as long as its IP address is accessible on the Internet.

4.2.2 How Do I Check Whether a Protected Domain Name Is Correctly Configured After I Connect It to AAD?

Step 1 Log in to the management console.

Step 2 **How Do I Connect My Service System to AAD?** describes how to add domain names to be protected to AAD.

Step 3 Copy the **CNAME** value of the domain name to be tested.

Step 4 Ping the **CNAME** value and record the corresponding IP address (for example, 192.168.0.1).

Step 5 Modify the local **hosts** file. This section uses Windows as an example. Go to the **C:\Windows\System32\drivers\etc** directory and open the **hosts** file. Add a record to the file, as shown in the following figure:


```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      [redacted]      [redacted]          # source server
#      [redacted]      [redacted]          # x client host

# localhost name resolution is handled within DNS itself.
#   [redacted]       localhost
#   ::1              localhost

192.168.0.1    www.test.com
```

Step 6 Clear the browser cache and enter the domain name in the address box to check whether you can access the domain name properly.

----End

4.2.3 What Can I Do When Message "Invalid request" Is Displayed When I Upload an HTTPS/WebSockets Certificate?

The causes and solutions for that message are as follows:

- The certificate name is too long.

  Solution: Change the certificate file name to one shorter than 10 characters.
- The certificate file name contains special characters.

  Solution: Use only letters and digits to name the certificate.
- The certificate content does not meet requirements.

  Solution: Delete information that does not meet the requirements of the certificate and private key input formats as described in FAQ **How Do I Convert a Non-PEM Certificate into a PEM One**, for example, delete information in front of **---BEGIN CERTIFICATE---**.

4.2.4 How Do I Convert a Non-PEM Certificate into a PEM One?

- **Converting a .cer or .crt certificate into a .pem one**

  Change the name extension of the certificate file.

  For example, change **certificate.cer** to **certificate.pem**.
- **Converting a .pfx certificate into a .pem one**

  Use OpenSSL to convert the certificate.


```
# Certificate extraction command
openssl pkcs12 -in certificate.pfx -nokeys -out cert.pem
# Private key extraction command
openssl pkcs12 -in certificate.pfx -nocerts -out key.pem -nodes
```

- **Converting a .p7b certificate into a .pem one**

  Use OpenSSL to convert the certificate.

  a. Run the following command to convert the certificate:
  ```
  openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer
  ```
  b. Obtain the certificate content in **outcertificat.cer**.
  c. Save the content in .pem format.

- **Converting a .der certificate into a .pem one**

  Use OpenSSL to convert the certificate.
  ```
  # Certificate extraction command
  openssl x509 -inform der -in certificate.der -out certificate.pem
  # Private key extraction command
  openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem
  ```

4.2.5 How Do I Enable Both AAD and WAF?

Perform the following operations to enable both AAD and WAF:

1. Obtain the CNAME value of the domain name on the WAF management console.
2. Configure the WAF CNAME in AAD.
3. Modify DNS configuration.

After the configuration is complete, traffic is processed by AAD first and then forwarded to WAF, thereby achieving collaborative protection.

4.2.6 How Do I Connect My Service System to AAD?

- If your system provides services through a domain name, you need to modify the DNS configuration to resolve the domain name to the CNAME record provided by HUAWEI CLOUD.
- If your system provides services through an IP address, change the IP address to a high-defense IP address.

4.2.7 How Is CNAME-based Access Implemented?

What is a CNAME record?

A Canonical Name (CNAME) record is a type of DNS record that maps an alias name to a true or canonical domain name. A DNS A record maps a domain name to an IP address, whereas a CNAME record maps a domain name to another domain name (alias of that domain name). For example, CNAME ccd01c25c8535fa4.huaweisafedns.com is configured for domain name www.abc.com. When a user accesses www.abc.com, the DNS protocol

automatically obtains its CNAME alias ccd01c25c8535fa4.huaweisafedns.com and uses the alias to obtain the real IP address.

What are the advantages of CNAME-based access?

- Easy to Use

  You only need to modify the resolution configuration with the DNS service provider (for example, DNS on HUAWEI CLOUD).

  The CNAME records generated in multiple lines for the same domain name are the same. You only need to configure one CNAME resolution record. Then AAD automatically configures the CNAME record for multiple high-defense IP addresses used by the domain name. When the high-defense IP address is changed, AAD updates CNAME mapping automatically, without requiring any manual DNS configuration modification.
- Excellent access performance

  If multiple lines are configured for a domain name, AAD can schedule access traffic based on the traffic source and select the optimal line to ensure the best access performance.
- High reliability

  You can select multiple lines for one domain name. If the high-defense IP address of a line encounters an exception, AAD automatically switches CNAME resolution to other available lines, ensuring service continuity.

What will I configure for CNAME-based access further if I have configured line-based resolution?

Generally, the CNAME resolution for one default line is required to replace line-based resolution. HUAWEI CLOUD will complete the resolution automatically.

The CNAME records provided by HUAWEI CLOUD are capable of line-based resolution. Based on the lines you purchased, HUAWEI CLOUD will perform line-based resolution automatically.

4.2.8 How Does AAD Distribute Traffic When There Are Multiple Origin Servers?

AAD distributes traffic evenly to origin servers in polling mode.

4.2.9 How Do I Check Whether a Back-to-Origin IP Address Has Been Whitelisted on My Origin Server?

Check servers and security devices to ensure that they have whitelisted the back-to-origin IP addresses and will not limit or block access traffic. For example:

- If your origin servers are Huawei Cloud servers, configure ACLs and security groups to permit the back-to-origin IP addresses.
  a. Log in to the management console.
  b. Click  in the upper left corner of the page and choose **Networking** > **Virtual Private Cloud**.
  c. Add a security group rule to allow traffic to the back-to-origin IP address. For details, see **Adding a Security Group Rule**.

d. Add a network ACL rule to allow access from the back-to-origin IP address. For details, see **Creating a Network ACL**.

- If your origin servers already have their own security policies, ensure that they have taken effect. Some custom security policies may take effect only after a restart.

4.2.10 How Do I Change the Exposed IP Address of an Origin Server?

Scenarios

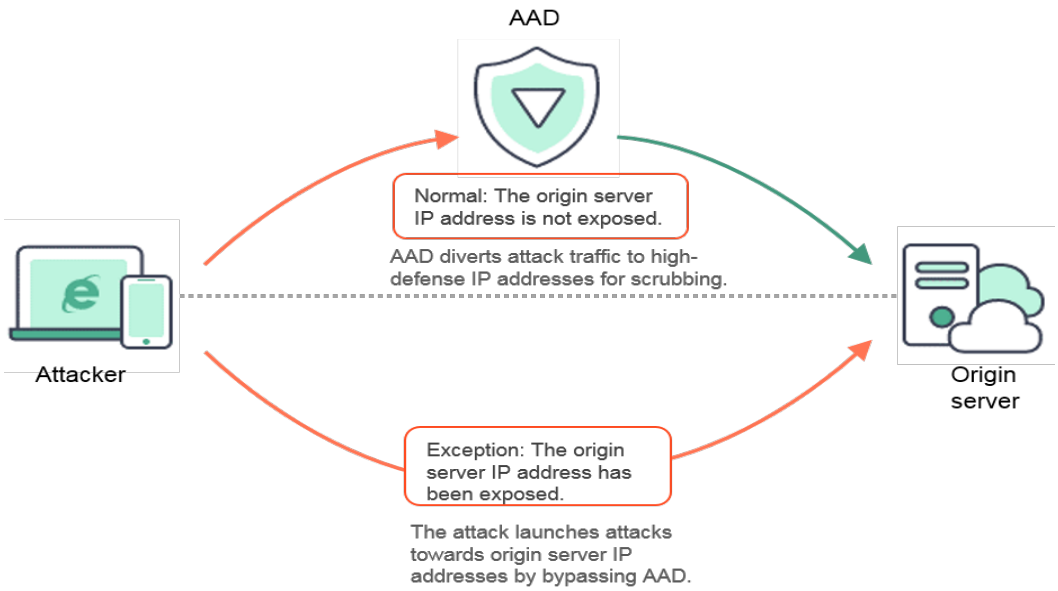
If the origin server is still under attacks even after AAD is configured, change the IP address of the origin server because it has been exposed.

This topic uses the EIP of an ECS as an example to describe how to change the origin server IP address.

Typical causes

- If the IP address of an origin server has been attacked by hackers before the AAD service is configured, the origin server IP address has been exposed to attackers.
- Some attackers may record the IP addresses used by exposed origin servers. Even after AAD is configured, the attackers will bypass AAD and directly launch attacks towards the known IP addresses. In this case, it is best practice to change the IP addresses of the origin servers.

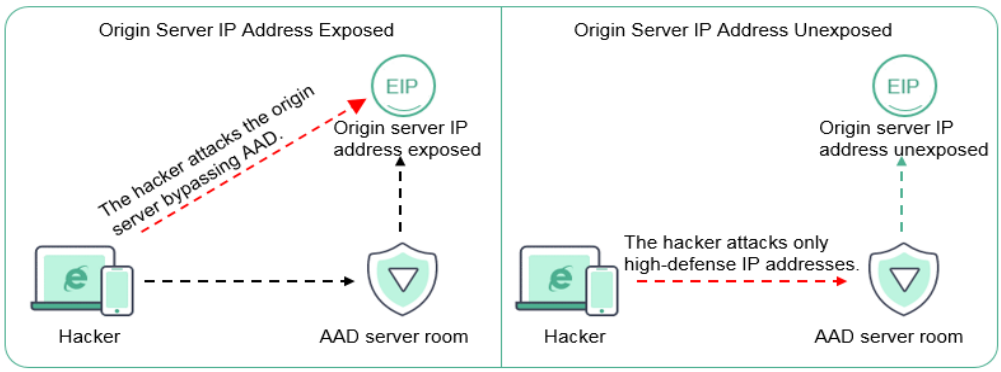
Figure 4-2 Typical causes



Solution

An ECS is used as an example. If the EIP of the ECS is exposed, you can reassign an unexposed EIP to the ECS to change the IP address of the origin server.

Figure 4-3 Mechanism



Procedure

Step 1 **Log in to the EIP console.**

Step 2 Locate the row containing the target EIP and click **Unbind** in the **Operation** column.

Step 3 Click **OK**.

Step 4 Assign another IP address for the ECS. Locate the row containing the target EIP and click **Bind** in the **Operation** column.

Step 5 Select the desired instance.

Step 6 Click **OK**.

----End

4.2.11 How Do I Query the Back-to-Origin IP Address Range?

If a firewall has been configured for your origin server, add the back-to-origin IP address range to the whitelist of the firewall (or another protective software) of the origin server.

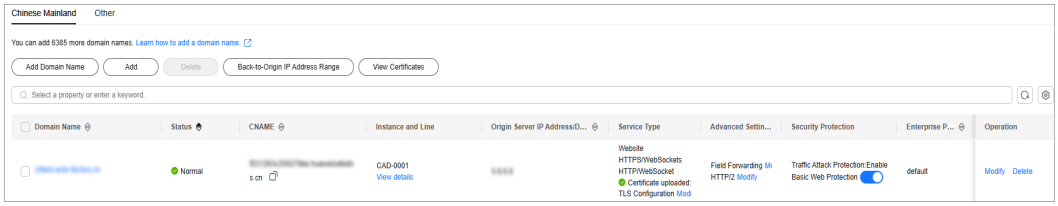
This topic describes how to query the back-to-origin IP address range and whitelist them on the firewall or another protective software on the origin server.

Procedure

Step 1 **Log in to the AAD console**.

Step 2 In the navigation pane on the left, choose **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.

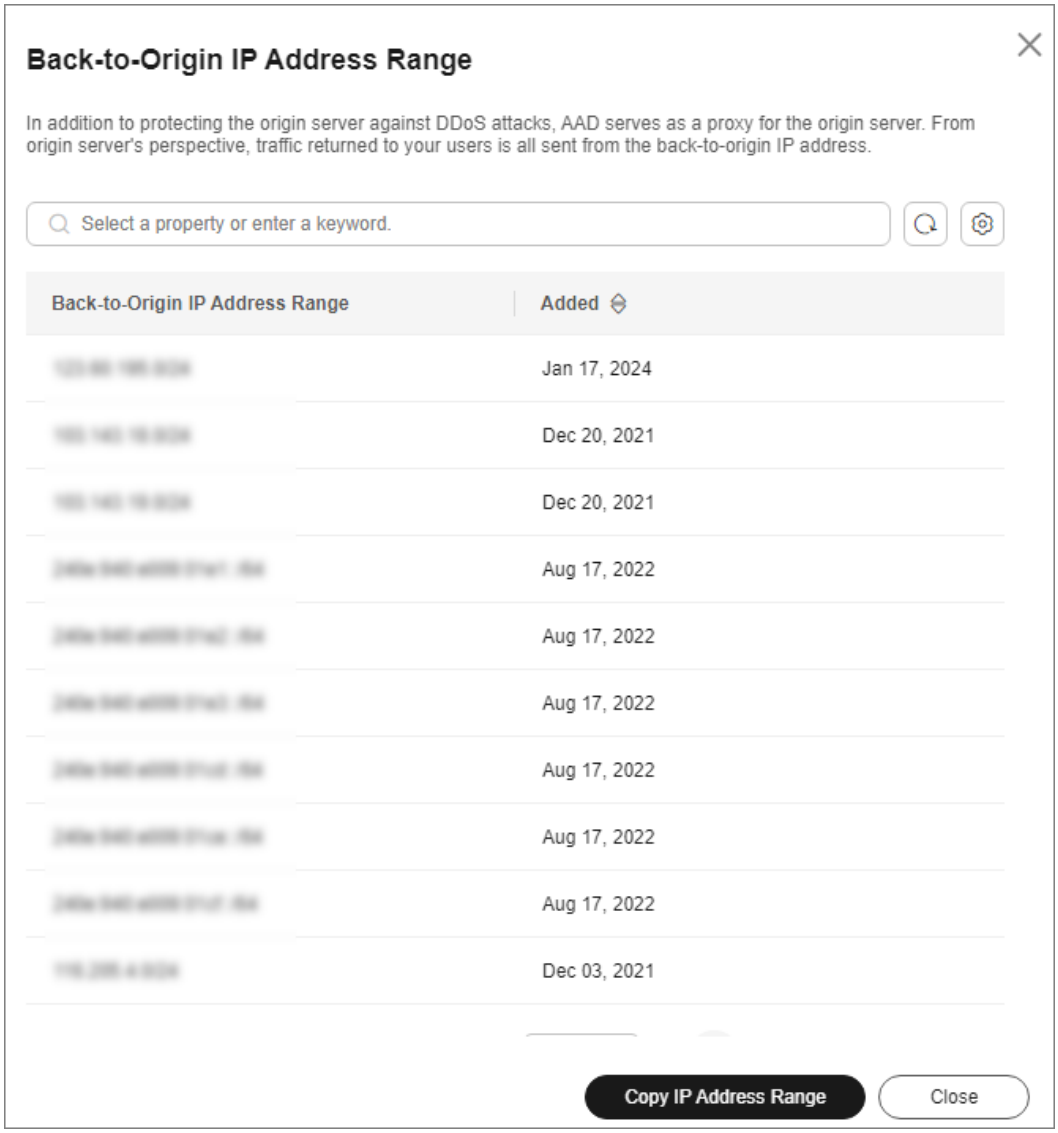
Figure 4-4 Domain name access



Step 3 On the displayed page, click **Back-to-Origin IP Address Range**.

Step 4 In the **Back-to-Origin IP Address Segment** dialog box, view information about the back-to-origin IP address segment.

Figure 4-5 Viewing the back-to-origin IP address range



Step 5 Add the back-to-origin IP address to the whitelist of the firewall or security software on the origin server.

----End

4.2.12 Can I Build My Own Anti-DDoS System Using HUAWEI CLOUD ECSs?

Yes, you can. You can set up an anti-DDoS system on your own for your business using ECSs of HUAWEI CLOUD. However, Huawei Cloud will block or freeze traffic when detecting frequent flood attacks, which may interrupt your normal service running. Therefore, you are advised to purchase the AAD service to defend against attacks while ensuring your service continuity.

4.2.13 How Do the AAD Blacklist and Whitelist Protect Customer's Servers?

You can configure the blacklist and whitelist for AAD instances. Blacklisted IP addresses will be blocked, and whitelisted IP addresses will be allowed through. For details, see "Configuring a Blacklist and a Whitelist". If you need to protect the origin servers, contact Huawei Cloud security technical experts.

4.2.14 Do I Still Need to Configure the Blacklist and Whitelist in WAF Protection Policies After Configuring Them in DDoS Protection Policies?

The whitelist configured in DDoS protection policies is automatically synchronized to WAF protection policies. You do not need to configure a whitelist again in web protection policies.

After a blacklist is configured in DDoS protection policies, the anti-DDoS device automatically blocks service traffic. You do not need to configure a blacklist again in WAF protection policies. If a domain name is bound to multiple instances, you need to configure a blacklist on each of these instances.

4.2.15 How Do I Use a Domain Name to Access Both IPv4 and IPv6 Services?

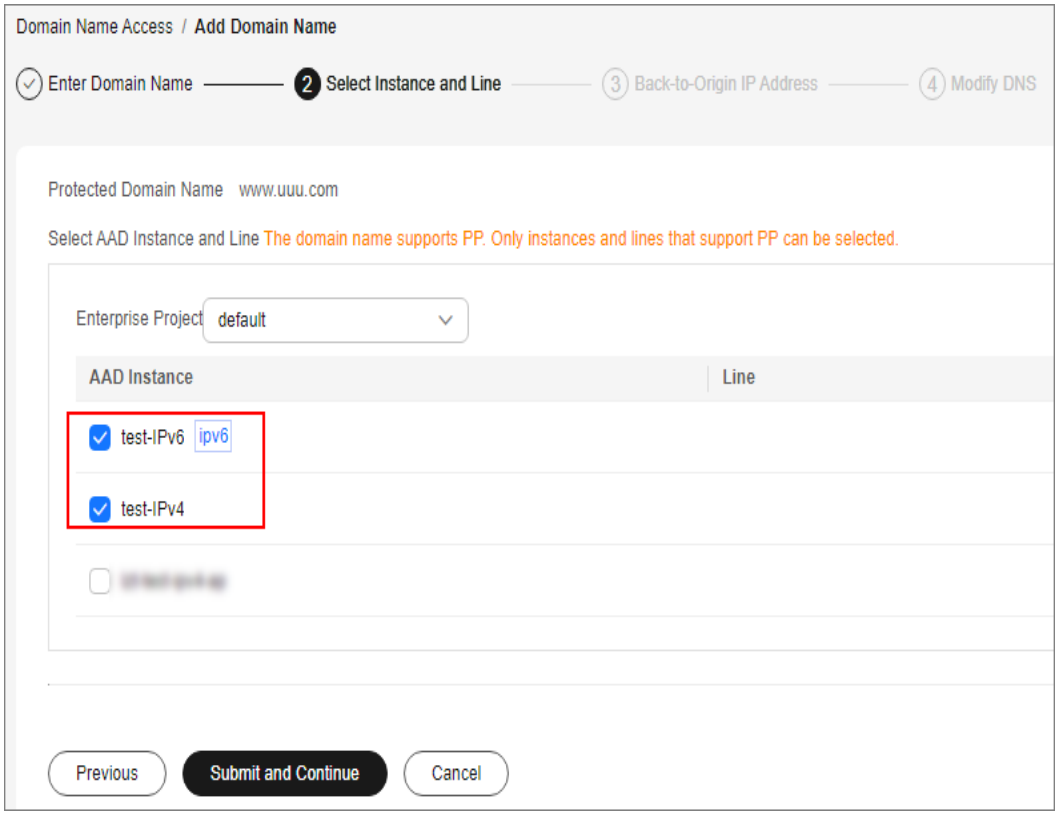
The AAD Chinese edition allows to use a domain name to access both IPv4 and IPv6 services. The procedure is as follows:

Step 1 Purchase an IPv4 instance and an IPv6 instance by referring to **Buying an AAD Instance**.

Step 2 Connect the domain name to AAD by referring to **Configuring a Protected Domain Name**. When selecting an instance line, select both the purchased IPv4 and IPv6 instances.

- **Origin Server Type**: Select **Domain Name**.
- **Select Instance and Line**: Select both the IPv4 and IPv6 instances.

Figure 4-6 Selecting instances and lines



----End

4.2.16 What Should I Do If I Receive a Message Stating That the Domain Name Already Exists When Trying to Connect?

Rectify the fault based on the displayed information.

- **The domain name already exists.** If you encounter a message that the domain name already exists, it typically means that the domain has been previously connected by you or another account you own. To resolve this, locate the domain name or its instance under any old accounts, remove it, and attempt to reconnect. If it is not the case, submit a service ticket to contact R&D engineers for troubleshooting.
- **The domain name already exists or is used by another user.** If you have not previously connected the domain name but still receive an error, it may indicate a conflict with another user's domain. This issue commonly arises when a level-2 domain name identical to yours is already in use. The ownership of a level-2 domain is exclusive to a single tenant by default. If you can prove the ownership of the level-2 domain, submit a service ticket to the backend to add it to the whitelist.

4.3 Faults

4.3.1 What Should I Do When Encountering an Access Freezing, Delay, or Failure?

Symptom

Access from a client to the high-defense IP address is frozen, has long delays, or loses packets.

Troubleshooting

- **Cross-network access**

  AAD supports CTCC, CUCC, CMCC, and BGP lines. Access delays and packet loss may occur if cross-network resolution is configured on DNS or cross-network back-to-origin is configured for origin server IP addresses on AAD.

  Solution:

  - On the DNS console: Check DNS configuration.

    This fault will not occur if you use the CNAME resolution provided by HUAWEI CLOUD. If you are using A record resolution, configure high-defense IP addresses based on the carrier of the line transmitting the access traffic. If your traffic is transmitted over the BGP line, retain the default high-defense IP address configuration. Huawei Cloud is not responsible for the packet loss or delays caused by improper DNS configuration.
  - On the AAD console: Check the origin server IP address.

    If the origin server uses a specific carrier line, packet loss and delays exist inevitably during cross-network access, and HUAWEI CLOUD is not responsible for the packet loss and delays.

    If the origin server uses lines of multiple carriers, add origin server IP addresses accordingly based on the high-defense IP addresses of the carrier lines, for example, associate a CTCC high-defense IP address with a CTCC origin server IP address. Huawei Cloud is not responsible for the packet loss or delays caused by improper back-to-origin line configuration.

- **Backend server exceptions**

  Troubleshoot the fault based on the origin server type configured for the high-defense IP address.

  - **The origin server is a load balancer.**

    To resolve the problem, perform the following steps:

    i. Run TCPing using the IP address and port number of the load balancer to locate the fault.

    ii. Check the load balancer status (such as number of connections and backend servers).

    iii. Check whether blacklists, whitelists, or other access control policies have been configured for the load balancer and ensure that the back-to-origin IP address range is allowed through.

    iv. Check backend servers and networks of the load balancer for any IP address blocking policies on firewalls.

- **The origin server is a cloud server.**

  To resolve the problem, perform the following steps:

  i. Run TCPing using the IP address and port number of the cloud server to locate the fault.

  ii. Check whether the server has encountered exceptions, such as black holes, scrubbing incidents, high CPU usage, slow database requests, and outbound bandwidth exhaustion.

  iii. Check whether blacklists, whitelists, or other access control policies have been configured for the cloud server and ensure that the back-to-origin IP address range is allowed through.

  iv. Check the cloud server or networks for security software or IP address blocking policies that block the back-to-origin IP addresses.

- **Whether high-defense IP addresses have scrubbing incidents**
  - **High-defense IP addresses have experienced scrubbing incidents.**

    To resolve the problem, perform the following steps:

    i. Run TCPing to check for and record delays and packet loss on attacked ports.

    ii. Run TCPing to check for and record delays and packet loss on non-attacked ports.

    Locate the fault by checking the records against the following table.

Table 4-2 Results

Delay and Packet Loss on Attacked Ports	Delay and Packet Loss on Non-attacked Ports	Cause Analysis
Yes	No	The scrubbing policy is executed properly on attack traffic. Check the backend server status and identify the server's attack defense capability. If the attack defense capability is weak, you need to enforce a powerful defense policy.
Yes	Yes	Normal traffic is scrubbed by the scrubbing policy. You can submit a service ticket for background troubleshooting.

Delay and Packet Loss on Attacked Ports	Delay and Packet Loss on Non-attacked Ports	Cause Analysis
No	No	The fault is not caused by the scrubbing policy.
No	Yes	Generally, this situation does not exist.

In the first two cases, you are advised to **submit a service ticket**. To enforce a more powerful defense policy, you need to provide details about your server's attack defense performance, including:

- Normal user access
- Service interaction processes
- Application service capabilities

– **High-defense IP addresses have not experienced scrubbing incidents.**

The fault is not caused by attacks.

- **High-defense IP addresses are blocked by black holes.**

  The high-defense IP address is blocked by a black hole if the attack traffic towards this IP address exceeds the configured elastic protection bandwidth. You can check whether packet loss is caused by a black hole.

  If so, you are advised to purchase a large elastic protection bandwidth and adjust your service systems to make them capable of switching traffic to another line when a black hole is triggered.

4.3.2 Why Is Error 504 Displayed When I Access a Website After AAD Is Configured?

Symptom

When a user visits a website with AAD configured, error code 504 is displayed after a long period of wait time.

Possible Causes

It takes a long period of time for the website to process some POST requests, and the time required exceeds the connection timeout threshold of AAD. As a result, AAD proactively drops the connection.

- The default TCP connection timeout is 900s.
- The default HTTP/WebSocket or HTTPS/WebSockets connection timeout is 120s.

Solution

It is recommended that you deploy a heartbeat mechanism to process time-consuming tasks at the application layer. This mechanism helps keep connections alive during the wait time.

For occasional time-consuming requests, you can send them directly to cloud servers by bypassing AAD.

4.3.3 How Do I Identify the Type of Attacks?

You can view the traffic report on the **Dashboard** page of AAD to identify whether the attacks are CC attacks or DDoS attacks.

Procedure

If both CC and DDoS attacks are launched, you can use the following methods to quickly identify the attack type:

Step 1 **Log in to the AAD console**.

Step 2 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Dashboard**.

Step 3 View the traffic reports respectively on the **DDoS Attack Protection** and **CC Attack Protection** pages and determine the attack types accordingly.

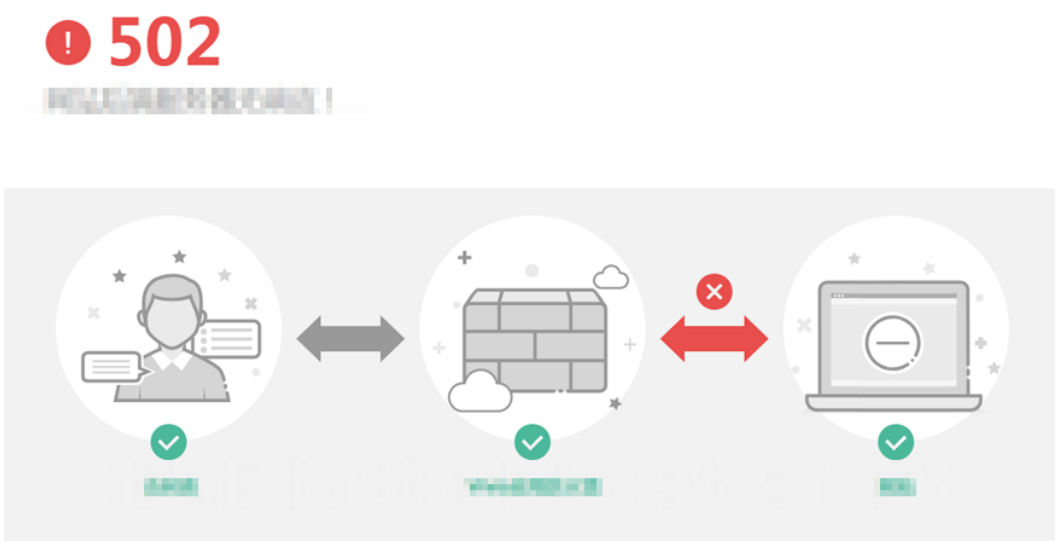
Attack Type	DDoS Attack Protection Report	CC Attack Protection Report
DDoS Attack	• The report indicates attack traffic fluctuations. • Traffic scrubbing has been triggered.	• There is no associated traffic fluctuation in the report.
CC Attacks	• The report indicates attack traffic fluctuations. • Traffic scrubbing has been triggered.	• There are associated traffic fluctuations in the report.

----End

4.3.4 What Should I Do If Error 500, 502, or 504 Is Reported When I Access My Website After I Enable Basic Web Protection for My Domain Name?

Errors 500, 502, or 504 may be displayed when you access your website after enabling basic web protection for it. The error page may also display connection failure with WAF and your website, as shown in **Figure 4-7**.

Figure 4-7 Error 502



There are many possible causes, such as firewall interception, incorrect origin server configuration, insecure HTTPS/WebSockets versions, and back-end server performance problems.

The following are the possible causes and solutions:

- Interception by the firewall, security protection software installed on the back-end server, or the rate limiting policy

  Symptom: Error 502 is reported at high possibility a while after basic web protection is enabled for a domain name.

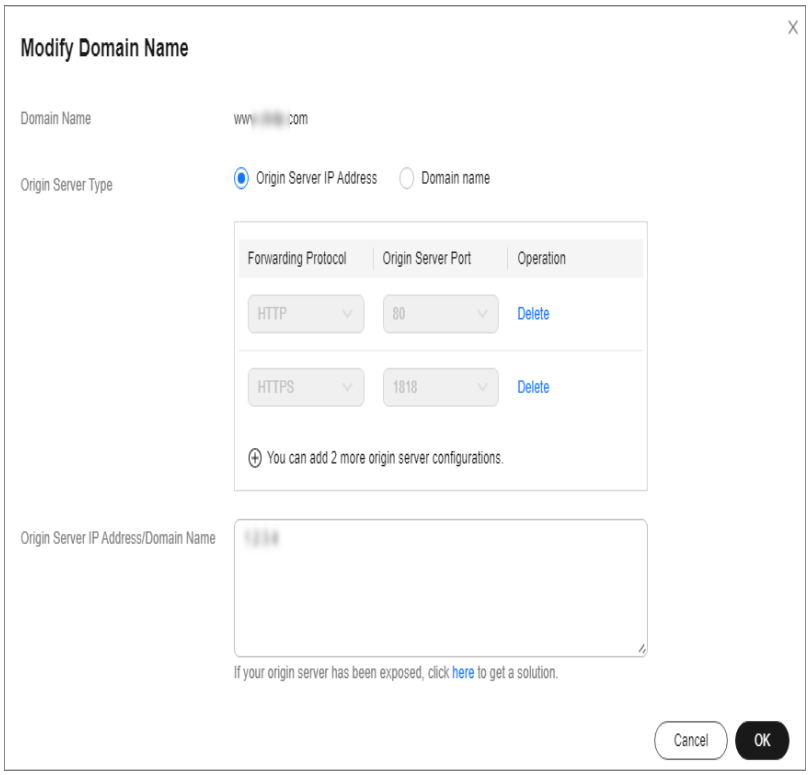
  Solution: Add the proxy IP address range to the whitelist of the firewall (hardware or software), security protection software, or rate limiting module.

- Incorrect origin server configuration

  Symptom: After basic web protection is enabled for your domain name, you access your website but error 502 or 500 is reported at high possibility (when multiple back-end servers are configured).

  Solution: Locate the target domain name in the domain name list, click **Edit** in the **Operation** column to check whether the forwarding protocol, IP address, and port number are correct.

Figure 4-8 Modifying the domain name configuration



As shown in **Figure 4-8**, you can try to visit http://xx.xx.xx.108:80 and https://xx.xx.xx.108:443 to check whether the back-end service port is enabled.

- Insecure HTTPS/WebSockets versions

  Symptom: After basic web protection is enabled, you access your website and error 502 is reported at high possibility for HTTPS/WebSockets services. However, if you visit by IP address, you can access your website.

  Solution: An earlier SSL version has serious security risks. WAF supports TLS1.2 and later. If such error is displayed because an early version of SSL is used by your server, upgrade your SSL version.

  You can try to visit **https://www.ssllabs.com/ssltest/index.html** to check the SSL version.

  - If the OS of your web server is earlier than Windows Server 2008, the SSL protocol does not support TLS1.2 and later. In this case, you need to upgrade the server OS to Windows Server 2008 or later (or a new version of Linux) and enable TLS1.2 in services such as IIS.
  - If your web server does not run Windows, check whether the SSL protocol is TLS1.2 or later.

- Poor back-end server performance

  Symptom: After basic web protection is enabled, your service works properly. However, when the number of access requests increases, error 502 or 504 increases as well. If you directly access your web server, there is also possibility that the error is returned.

  Solution:

  - Optimize the server configuration, including TCP network parameters and **Ulimit** parameters.

- Increase the number of back-end ECSs to support increasing requests. AAD supports multiple back-end servers.

4.3.5 What Can I Do If I Failed to Configure a Forwarding Rule?

Troubleshooting:

- It takes 2-3 minutes for the forwarding rule configuration to take effect. If the forwarding rule is in the **Processing** state, you can refresh the page later.
- After you add a forwarding rule, the AAD service will check the connectivity of your origin server IP address and port and check for any conflicts with existing forwarding rules. If the configuration fails, check whether the origin server is running properly or whether a forwarding rule has already been configured.

4.3.6 What Can I Do If My UDP Traffic Is Blocked?

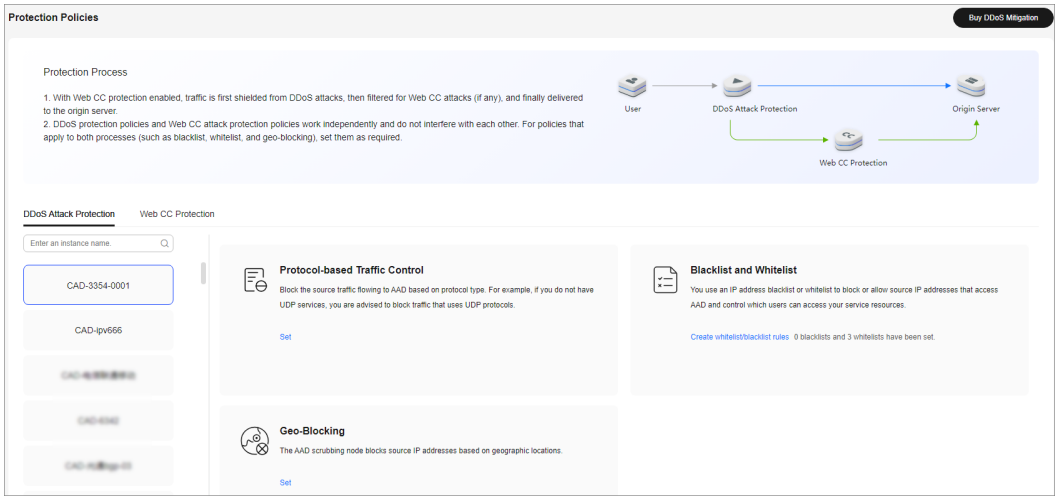
If UDP traffic control is enabled for a line, UDP traffic on this line will be blocked. Therefore, ensure that UDP traffic control for the line is disabled.

Procedure

Step 1 Log in to the AAD console.

Step 2 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Protection Policies**. The **Protection Policies** page is displayed.

Figure 4-9 Advanced Anti-DDoS protection policies



Step 3 Select the instance for which you want to configure protocol blocking.

Step 4 In the **Protocol-based Traffic Control configuration** area, click **Set**.

Step 5 In the dialog box that is displayed, select a route and set the switch to  to disable the protocol.

Figure 4-10 Disabling a protocol

----End

4.3.7 How Do I Unblock the Access That Has Been Automatically Blocked Due to the Threshold-Overtopped Attack Traffic?

The black hole lasts 30 minutes by default. However, this duration may vary based on the number of black holes triggered within the current day and the peak attack traffic.

If you need to unblock access before a black hole becomes ineffective, contact Huawei technical support.

4.3.8 Why Can't I Specify Certain Ports When Configuring the Forwarding Rule?

Symptoms

When I set the forwarding port and origin server port to specific ports, the configuration of the forwarding rule fails.

NOTE

Port range: 1 to 65535

Possible Causes

AAD regards the ports in **Table 4-3** as high-risk ports and cannot be used.

Table 4-3 High-risk ports

Protocol	Port
TCP	135, 136, 137, 138, 139, 445, 3333, 4444, 5554, 6000, 8090, 9995, 9996, 25000, 50050, 53413, 60000
UDP class	135, 137, 138, 139, 593, 901, 1027, 1028, 1068, 2745, 3127, 3128, 3333, 5800, 5900, 6000, 6129, 6667, 8090, 8998, 9996, 25000, 50050, 5341, 60000

Handling Suggestions

You are advised to change the port.

4.3.9 Error Message "Received fatal alert" Is Displayed After a Domain Name Is Bound to AAD

Symptoms

After a domain name is bound to AAD, the error **Received fatal alert: handshake_failure; nested exception is javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure** is reported. While it is normal before the binding operation.

Possible Causes

The callback platform client does not support SNI extension.

Solutions

The following suggestions are provided for clients that do not support SNI:

1. Upgrade your browser to the new version or use browsers that support SNI extension, such as Chrome and Firefox.
2. Upgrade the Java and OpenSSL versions of your client.
3. Upgrade the JDK version to 1.8, which supports TLSv1.2 and is backward compatible.
4. Third-party callbacks should use origin server IP addresses.

4.4 Product

4.4.1 What Is a Protected IP Address?

The IP address of an origin server is the IP address to be protected. It is a public IP address.

A high-defense IP address is the IP address used by the AAD service to provide protection.

The AAD service uses the high-defense IP address to proxy services for origin servers. All public network traffic is diverted to the high-defense IP address, and therefore user services on the origin servers are protected against DDoS attacks.

4.4.2 Does AAD Support Weighted Back-to-Origin?

No, weighted back-to-origin is not supported currently. AAD switches traffic back to origin servers based on the polling mechanism. You can direct traffic to the public IP address used by ELB and then switch it back to origin servers from ELB based on weight.

4.4.3 Can AAD Be Used Across Regions?

AAD is a global service that is not region-specific. Therefore, it can be used across regions. For multiple regions are protected by one AAD instance, the performance of the service system does not decrease.

4.4.4 Does AAD Support Migration of Resources in Enterprise Projects?

An AAD instance is exclusively associated with an enterprise project.

While AAD resources themselves are not directly tied to enterprise projects, you can migrate the enterprise project resources associated with AAD instances by referring to the **How Do I Migrate Instance Resources in an Enterprise Project?** guide for detailed steps.

An AAD instance with protected domain names cannot have its associated enterprise project changed.

4.4.5 What Is a CNAME Record?

A Canonical Name (CNAME) record is a type of DNS record that maps an alias name to a true or canonical domain name. A DNS A record maps a domain name to an IP address, whereas a CNAME record maps a domain name to another domain name (alias of that domain name). For example, the alias of **www.abc.com** is **ccd01c25c8535fa4.huaweisafedns.com**. When a user accesses **www.abc.com**, DNS obtains its alias **ccd01c25c8535fa4.huaweisafedns.com** and uses the alias to obtain the real IP address. The resolution is automatically completed by DNS.

4.4.6 What is BGP?

Border Gateway Protocol (BGP) is a routing protocol used between autonomous systems (ASs). BGP is the only protocol that can process many connections between unrelated routing domains.

4.4.7 What Is the Origin Server Port of AAD?

It is a port used by the origin server to provide services for external systems.

4.4.8 What Is the Origin Server IP Address?

It is the public IP address used by origin servers to provide services for external systems.

4.4.9 What Website IP Addresses Is Protected by AAD?

AAD provides protection using high-defense IP address. The public IP address used by the origin server, namely, the origin server IP address, is protected by AAD. The high-defense IP address is used to provide services in place of the origin server IP address. The AAD service uses the high-defense IP address to proxy services for origin servers. All public network traffic is diverted to the high-defense IP address, and therefore user services on the origin servers are protected against DDoS attacks.

4.4.10 What Is Service Bandwidth?

The service bandwidth indicates clean service bandwidth forwarded to the origin server from the AAD scrubbing center. Packet losses may occur when the traffic exceeds the service bandwidth.

4.4.11 What Is a Forwarding Protocol?

A forwarding protocol used by user's server to provide services for external systems can be Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

4.4.12 Are Services Interrupted When They Are Being Connected to AAD?

When services are connected to AAD, the DNS resolution needs to be changed and the service domain name is resolved to high defense IP address. To avoid the service interruption, you are advised to keep the origin server running till all domain names are resolved to the high-defense IP address. Then, you can bring the origin server offline.

4.4.13 Can a Domain Name Be Bound to Multiple AAD Instances?

If an AAD instance to which a domain name has been bound is in use, the domain name cannot be bound to other AAD instances due to domain name conflict. Resolve the domain name to the origin server and unbind it from the AAD instance. Then, you can bind the domain name to other AAD instances.

4.4.14 Why Does the High-Defense IP Address Actually Receive Access Requests from a Client After AAD Is Deployed?

After you purchase the AAD service, the domain name of a web service is resolved into a high-defense IP address, and the service IP address of a non-web service is changed to a high-defense IP address. In this case, all access traffic is filtered by the high-defense IP address.

The high-defense IP address receives access requests from a client in place of origin server IP address, that is, the high-defense IP address is accessed by the client.

4.4.15 Why Does the Attack Traffic Volume Increase After AAD Is Deployed?

Some attackers may record the IP addresses used by exposed origin servers. Even after AAD is configured, the attackers will bypass AAD and directly launch attacks towards the known IP addresses. In this case, it is best practice to change the IP addresses of the origin servers.

4.4.16 Will the Origin Server Be Exposed When the Attack Traffic Volume Increases After AAD Is Deployed?

No. After you purchase the AAD service, the domain name of a web service is resolved into a high-defense IP address, and the service IP address of a non-web service is changed to a high-defense IP address. All public network traffic is diverted to the high-defense IP address, and therefore services on the origin servers are protected against DDoS attacks

4.4.17 How Does AAD Protect Origin Server IP Addresses?

The AAD service uses the high-defense IP address to proxy services for origin servers. All public network traffic is diverted to the high-defense IP address, and therefore user services on the origin servers are protected against DDoS attacks.

- If your system provides services through a domain name, you need to modify the DNS configuration to resolve the domain name to the CNAME record provided by HUAWEI CLOUD.
- If your system provides services through an IP address, change the IP address to a high-defense IP address.

4.4.18 Does AAD Support Two-Way SSL Authentication?

No.

4.4.19 Can I Modify or Delete the Certificates Uploaded to AAD?

For website services connected to AAD, if **Protocol/Port** is set to **HTTPS/WebSockets** and **Origin Server Type** is set to **IP address**, you need to upload a certificate.

After the certificate is uploaded to AAD, you can go to the **Domain Name Access** page. Locate the row that contains the target domain name and click **Update** in the **Service Type** column.

The certificates uploaded to AAD cannot be deleted.

4.4.20 What Will Happen If My Service Traffic Exceeds the Configured Service Bandwidth?

If your service traffic exceeds the configured service bandwidth of the purchased AAD instance, rate limiting is triggered, which may result in packet loss.

4.4.21 Is AAD Software or Hardware?

AAD, a software DDoS mitigation service, provides instantaneous protection once you connect your services to AAD. You can view DDoS attack protection details on its dashboard to learn about the network security state.

Compared with traditional hardware DDoS mitigation services, AAD has the following advantages:

- **Immense defense capability**

  One high-defense IP address is able to defend against 1000 Gbit/s network-, and application-layer DDoS attacks. The AAD service offers more than 15 Tbit/s defense capability.

- **High availability**

  Automated attack detection and adaptive defense policies support real-time protection. Service traffic is distributed in clusters, which features high performance, low latency, and high stability.

- **Flexible protection**

  You can buy both the basic bandwidth protection and elastic bandwidth protection of AAD for a higher protection capability. The protection bandwidth can be adjusted depending on your needs.

4.4.22 Does AAD Support IPv6 Protection?

AAD supports only some service access points using the IPv6 protocol. You can use CNAD Basic and CNAD Advanced to protect IPv6 addresses.

NOTE

When a network request passes through the AAD proxy, the IP address shown on the origin server is the AAD back-to-origin IP address. To retrieve the real source IP address, you can use the TOA protocol, which extracts it from the TCP option field in the packet. This method also allows you to obtain the real IPv6 access source.

However, if AAD basic web protection is enabled or the origin server is configured with Huawei Cloud WAF, the actual IPv6 access source cannot be retrieved.

4.4.23 Why Is the Traffic of AAD Inconsistent with That of ELB?

AAD collects statistics on the peak traffic of seconds within a period of time, in bit/s. ELB collects the average traffic within a period of time. Therefore, the ELB traffic statistics are smaller than the AAD traffic statistics.

Note that if the inbound traffic exceeds the DDoS service bandwidth, traffic limiting is triggered. It's essential to adjust the service bandwidth in accordance with the real-world service traffic.

You can view the AAD service bandwidth on the AAD Console.

4.5 Fees

4.5.1 How Is AAD Billed?

Pricing

To use AAD, you need to purchase AAD instances.

Billing Mode

AAD instances are charged by the service bandwidth, basic protection bandwidth, and elastic protection bandwidth you configure.

Table 4-4 Billing items

Billing Item	Billing Modes	Pricing details
Service Bandwidth	Prepaid by month or year	Service bandwidth for the AAD server room to forward scrubbed traffic to origin servers. **NOTE** If the AAD equipment room is outside Huawei Cloud, it is recommended that the service bandwidth be greater than or equal to the egress bandwidth of the origin servers.
Basic Protection Bandwidth	Prepaid by month or year	Basic bandwidth for defending against attacks. Traffic that does not exceed this bandwidth will be scrubbed by AAD without incurring additional fees.
Elastic Protection Bandwidth	Postpaid by day	Maximum available bandwidth for defending against attacks. For details about the price of the elastic protection bandwidth, see the **Product Pricing Details** tab in **Price Calculator**.
Elastic Bandwidth	A postpaid billing mode. You pay as you go and just pay for what you use.	95th percentile billing per month: The traffic peaks are measured every 5 minutes in a calendar month and then sorted in descending order. The top 5% of the peaks are discarded. The highest value of the rest is the billing bandwidth. For details about product prices, see **Pricing Details**.

Billing details for elastic protection bandwidth:

- Billing standard: It depends on the peak attack traffic on the day. If multiple attacks occur on a day, only the attack with the peak traffic counts.
- Postpaid: Elastic protection fees are generated based on the attack traffic peak. If there is no attack, no elastic protection fee is generated.
- Specifications adjustment: You can adjust the elastic protection bandwidth on the AAD console. Once adjusted, the new elastic protection bandwidth takes effect immediately.
- Free-to-use: If the elastic protection bandwidth is set to the same value as the basic protection bandwidth, you do not need to pay for elastic protection.

4.5.2 Why Does My Payment Status Not Update After I Make a Payment?

If you have not received any payment information after making a payment, and the payment status on the platform is not updated, the possible causes may be as follows:

- Check whether the recharge number is correct in the transaction record.
- The payment SMS message sent by the carrier is delayed. Contact the carrier or Huawei customer service to query the payment status.

4.5.3 Will I Be Charged If I Buy an Elastic Protection Bandwidth and My Elastic IP Address Is Not Attacked for the Whole Month?

If you have purchased elastic protection but no attack occurs for one month,

you are charged for the basic protection bandwidth only.

4.5.4 What Happens If the Attack Traffic Exceeds the Elastic Protection Bandwidth?

A black hole will be triggered, which means access traffic to the IP address will be blocked.

AAD supports dynamic adjustment of elastic protection bandwidth.

NOTICE

Adjusted bandwidth takes effect immediately. The charge depends on the peak attack traffic of the day.

4.5.5 Can I Adjust My Elastic Protection Bandwidth From 100 Gbit/s to 200 Gbit/s When I Find 100 Gbit/s Is Insufficient?

You can change the bandwidth to 200 Gbit/s.

AAD supports dynamic adjustment of elastic protection bandwidth.

NOTICE

Adjusted bandwidth takes effect immediately. The charge depends on the peak attack traffic of the day.

4.5.6 What Is the Charge If My IP Address Is Attacked Many Times a Day?

You will be charged only once based on the peak attack traffic of the day (0:00 to 23:00).

For example, if your IP address is attacked three times and the attack traffic is 50 Gbit/s, 100 Gbit/s, and 200 Gbit/s, you will be charged based on 200 Gbit/s.

4.5.7 How Do I Stop Elastic Protection to Avoid Being Charged for the Elastic Protection Bandwidth?

You can set the elastic protection bandwidth of the purchased AAD instance to be the same as the basic protection bandwidth.

If the traffic exceeds the basic protection bandwidth, no elastic protection bandwidth will be enabled for protection.

4.5.8 How Can I Renew the AAD Service?

You can renew an AAD instance on the AAD management console.

NOTICE

Ensure that the account used for renewing the AAD instance has both the CAD Administrator and BSS Administrator roles or has the Tenant Administrator role.

- **BSS Administrator**: has all permissions on account center, billing center, and resource center. It is a project-level role, which must be assigned in the same project.
- **Tenant Administrator**: has all permissions on all services except on IAM.

Step 1 Log in to the AAD console.

Step 2 In the navigation pane on the left, choose **Advanced Anti-DDoS > Instance List**. The **Instance List** page is displayed.

Step 3 Click **Renew** under the instance name.

Step 4 On the **Renew** page, select a renewal duration and click **Pay** to complete the payment.

----End

4.5.9 How Can I Unsubscribe from the AAD Service?

The AAD service does not support unconditional unsubscription.

If the unsubscription conditions are met, contact the customer service to apply for unsubscription

Unsubscription Conditions

If the service does not match your business requirements during your purchase or use, contact the customer service personnel to unsubscribe from the service. For

example, if your servers are deployed outside China but you have purchased the AAD service from the Chinese Mainland region, the AAD service cannot be used and in this case you can apply for service cancellation.

AAD instances in use cannot be unsubscribed.

The AAD background can detect whether the service has been put to use. If it has been used, it cannot be unsubscribed.

4.5.10 How Should I Automatically Renew AAD?

You can enable auto renewal for your AAD instance. The system automatically renews your service subscription according to the required duration specified in your previous purchase upon expiration of the service.

NOTICE

Ensure that the account for which the automatic renewal is to be enabled has both the CAD Administrator and BSS Administrator roles or has the Tenant Administrator role.

- **BSS Administrator**: has all permissions on account center, billing center, and resource center. It is a project-level role, which must be assigned in the same project.
- **Tenant Administrator**: has all permissions on all services except on IAM.

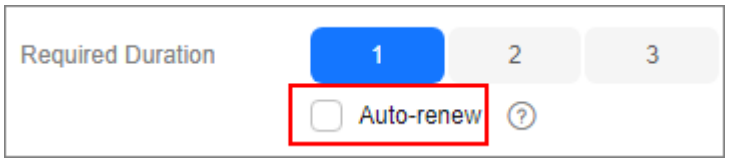
If you are currently purchasing AAD, you can enable the auto renewal function as follows:

1. When purchasing AAD, you can tick the **Auto-renew** option to configure automatic renewal.

   The procedure is as follows:

   Choose **Buy DDoS Mitigation** > **Required Duration** > **Auto-renew**.

   Figure 4-11 Required Duration

If you have purchased AAD, you can enable the auto renewal function as follows:

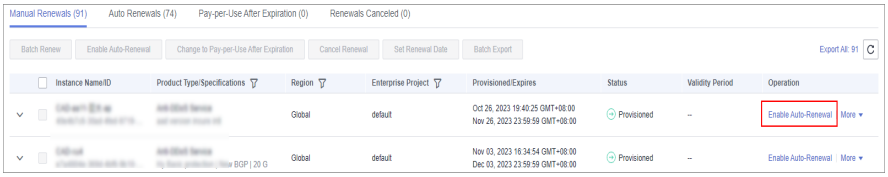
Go to the **Renewals** page, configure automatic renewal.

The procedure is as follows:

1. Log in to the management console and click **Fees** at the top right.

   The **Billing Center** page is displayed.
2. In the navigation pane on the left, choose **Orders** > **Renewals**.
3. Select the corresponding AAD instance for automatic renewal.

Figure 4-12 Auto-renew



4.5.11 Can the Original Configuration Data Be Saved After I Unsubscribe from an AAD Instance?

No. After you unsubscribe from an AAD instance, it will not keep your original configuration data. Therefore, you need to connect your services to the newly-purchased AAD instance.

For details about unsubscription, see **How Can I Unsubscribe from the AAD Service?**.

To connect a service to the AAD, perform the following steps:

- If your system provides services through a domain name, you need to modify the DNS configuration to resolve the domain name to the CNAME record provided by Huawei Cloud.
- If your system provides services through an IP address, change the IP address to a high-defense IP address.

4.5.12 How Is the Elastic Bandwidth Charged?

Billing Description

The elastic bandwidth of AAD instances is charged based on the peak traffic of DDoS attacks on the current day. The fees in different scenarios are described as follows:

- Peak DDoS attack traffic on the current day ≤ Basic protection bandwidth: No elastic protection bandwidth fee is generated.
- Basic protection bandwidth < Peak DDoS attack traffic on the current day < Elastic protection bandwidth: Elastic protection bandwidth fees will be generated.
- If the peak DDoS attack traffic on the current day is greater than or equal to the configured elastic protection bandwidth, you will be charged for the elastic protection bandwidth.

Billing Examples

- Basic protection bandwidth < Peak attack traffic < Elastic protection bandwidth: **Elastic protection bandwidth usage (billed) = Peak attack traffic on the current day – Basic protection bandwidth**
- Peak attack traffic ≥ Elastic protection bandwidth: **Elastic protection bandwidth usage (billed) = Elastic protection bandwidth – Basic protection bandwidth**

For example, for three AAD instances, each has a basic protection bandwidth of 20 Gbit/s and an elastic protection bandwidth of 100 Gbit/s. If the three instances are

under multiple DDoS attacks on the same day, the billing rules of the elastic protection bandwidth are as follows:

Table 4-5 Billing rules

Instance	Peak Attack Traffic	Generate Fee	Description
Instance A	20Gbps	No	The peak attack traffic does not exceed the basic protection bandwidth, no fee is generated.
Instance B	80Gbps	Yes	Billed protection bandwidth: 80 Gbit/s - 20 Gbit/s = 60 Gbit/s.
Instance C	120Gbps	Yes	120 Gbit/s is greater than the elastic protection bandwidth 100 Gbit/s. Billable protection bandwidth: 100 Gbit/s - 20 Gbit/s = 80 Gbit/s.

4.5.13 How Is the Elastic Service Bandwidth Charged?

Billing rules

The service bandwidth fees of AAD instances in different scenarios are described as follows:

- If the actually used service bandwidth is less than or equal to the service bandwidth, no elastic service bandwidth fee is generated.
- Service bandwidth < Actual service bandwidth < Elastic service bandwidth: Elastic service bandwidth fees will be generated.
- If the actually used service bandwidth is greater than or equal to the elastic service bandwidth, the elastic service bandwidth fee will be generated.

Billing Principles

- Monthly 95th percentile billing

  The bandwidth is sampled every 5 minutes in a calendar month. The sampling vertices are sorted in descending order of the peak value, the maximum value of 5% is removed, and the maximum value among the remaining values is used as the billable bandwidth. **Figure 4-13** shows how to calculate the monthly 95th percentile bandwidth for 30 days.

Figure 4-13 Monthly 95th percentile billing