DDoS Mitigation

User Guide

Issue	08
Date	2025-02-07

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 CNAD Basic (Anti-DDoS) User Guide

1.1 Anti-DDoS Overview

Figure 1-1 shows the process of adding an EIP to Anti-DDoS for protection.

Figure 1-1 Process of using Anti-DDoS

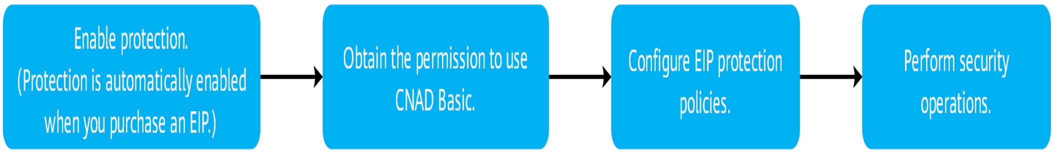

Enable protection.
(Protection is automatically enabled when you purchase an EIP.)
Obtain the permission to use CNAD Basic.
Configure EIP protection policies.
Perform security operations.

Table 1-1 Procedures

No.	Procedure	Description
1	Enabling Anti-DDoS	Anti-DDoS is free of charge. It is automatically enabled when you purchase an EIP.
2	**Using IAM to grant Anti-DDoS permissions**	Use Identity and Access Management (IAM) to grant fine-grained Anti-DDoS service permissions to users.
3	**Configuring an EIP protection policy**	You can set a traffic scrubbing threshold for the protected EIP. When service traffic exceeds the traffic scrubbing threshold, Anti-DDoS scrubs the traffic to mitigate DDoS attacks.

No.	Procedure	Description
4	Performing common security operations	- **Setting DDoS Alarm Notifications**: After the alarm notification function is enabled, you will receive an alarm if a DDoS attack is detected. - **Enabling DDoS Alarm Notifications**: After event monitoring is enabled on Cloud Eye, alarms are triggered when events such as scrubbing, blocking, or unblocking occur. - **Adding a Tag to an EIP**: You can use tags to classify cloud resources for easy management. - **Viewing an EIP Monitoring Report**: You can view the monitoring details of a specified public IP address, including the protection status, protection parameters, traffic in the last 24 hours, and abnormal events. - **Viewing an Interception Report**: You can view the protection statistics of all public IP addresses of a user, including the number of scrubbing times, scrubbed traffic, and top 10 attacked IP addresses. - **Querying Audit Logs**: You can view historical Anti-DDoS operation records on CTS.

NOTE

CNAD Basic does not support attack alarm notification and protection policy customization for public IP addresses of the GEIP and GA types.

1.2 Using IAM to Grant Anti-DDoS Permissions

1.2.1 Creating a User Group and Assigning the Anti-DDoS Access Permission

If you want to implement refined permission management for your Anti-DDoS service,you can use **Identity and Access Management (IAM)**. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to Anti-DDoS resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust another Huawei Cloud account or cloud service to perform professional and efficient O&M to your Anti-DDoS resources.

If your Huawei Cloud account does not need individual IAM users for permissions management, skip this chapter.

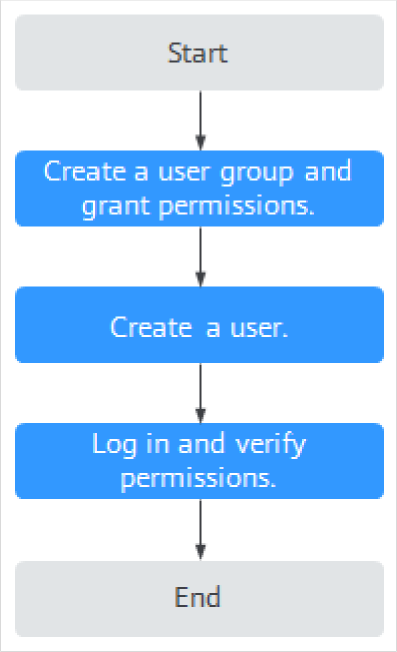
This section describes the procedure for granting permissions (see **Figure 1-2**).

Prerequisites

Before assigning permissions to a user group, you should learn about the Anti-DDoS permissions that can be added to the user group, and select the permissions based on the site requirements. For details about the permissions, see **Anti-DDoS Permissions**. For the system policies of other services, see **Permissions Policies**.

Process

Figure 1-2 Process for granting permissions


Start
Create a user group and grant permissions.
Create a user.
Log in and verify permissions.
End

1. **Create a user group and assign permissions**.

   Create a user group on the IAM console, and assign the **Anti-DDoS Administrator** policy to the group.

2. **Create a user and add it to a user group**.

   Create a user on the IAM console,and add the user to the group created in **1**.

3. **Log in** and verify permissions.

   Log in to the management console using the user created, and verify that the user only has read permissions for AAD.

   In **Service List** on the management console, select any other services. If a message indicating that the permission is insufficient is displayed, the **Anti-DDoS Administrator** permission takes effect.

1.2.2 Anti-DDoS Custom Policies

Custom policies can be created to supplement the system-defined policies of Anti-DDoS. For details about the actions supported by custom policies, see **Anti-DDoS Permissions and Actions**.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see **Creating a Custom Policy**. The following section contains examples of common Anti-DDoS custom policies.

Anti-DDoS Custom Policy Examples

- Example 1: Authorizing a user to query the default Anti-DDoS policy

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "anti-ddos:defaultDefensePolicy:get"
                                                        ]
                }
        ]
}
```

1.2.3 Anti-DDoS Permissions and Actions

This section describes fine-grained permissions management for Anti-DDoS. If your account does not need individual IAM users, then you may skip over this section.

By default, new IAM users do not have any permissions. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added. Users inherit permissions from the groups and can perform operations on cloud services as allowed by the permissions.

You can grant users permissions by using **roles** and **policies**. Roles are provided by IAM to define service-based permissions depending on user's job responsibilities. IAM uses policies to perform fine-grained authorization. A policy defines permissions required to perform operations on specific cloud resources under certain conditions.

Supported Actions

Anti-DDoS provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control.

- Permissions: Statements in a policy that allow or deny certain operations
- Actions: Added to a custom policy to control permissions for specific operations

Permission	Action	Dependency
Querying default protection policy of Anti-DDoS	anti-ddos:defaultDefensePolicy:get	-

Permission	Action	Dependency
Configuring default Anti-DDoS protection policies	anti-ddos:defaultDefensePolicy:create	-
Deleting the default Anti-DDoS policies	anti-ddos:defaultDefensePolicy:delete	-
Querying Anti-DDoS specifications	anti-ddos:optionalDefensePolicy:list	-
Querying configured Anti-DDoS policies	anti-ddos:ip:getDefensePolicy	vpc:publicIps:list
Updating Anti-DDoS policies	anti-ddos:ip:updateDefensePolicy	-
Enabling Anti-DDoS	anti-ddos:ip:enableDefensePolicy	-
Querying weekly defense statistics	anti-ddos:ip:getWeeklyReport	-
Querying the traffic of a specified EIP	anti-ddos:ip:getDailyTrafficReport	-
Querying events of a specified EIP	anti-ddos:ip:getDailyEventReport	-
Querying the defense status of a specified EIP	anti-ddos:ip:getDefenseStatus	-
Querying the list of defense statuses of EIPs	anti-ddos:ip:listDefenseStatuses	-
Querying Anti-DDoS tasks	anti-ddos:task:list	-
Querying alarm configuration	anti-ddos:alertConfig:get	smn:topic:list
Updating alarm configuration	anti-ddos:alertConfig:update	-
Querying LTS configurations	anti-ddos:logConfig:get	-

Permission	Action	Dependency
Updating LTS configurations	anti-ddos:logConfig:update	-
Querying quotas	anti-ddos:quota:list	-
Querying resource tags	anti-ddos:ip:listTagsForResource	-
Batch creating tags	anti-ddos:ip:tagResource	-
Batch deleting tags	anti-ddos:ip:untagResource	-

1.2.4 Permission Dependency of the Anti-DDoS Console

When using Anti-DDoS, you may need to view resources of or use other cloud services. So you need to obtain required permissions for dependent services so that you can view resources or use Anti-DDoS functions on the Anti-DDoS console. To that end, make sure you have the Anti-DDoS Administrator assigned first. For details, see **Creating a User Group and Assigning the Anti-DDoS Access Permission**.

Dependency Policy Configuration

If an IAM user needs to view or use related functions on the console, ensure that the **Anti-DDoS Administrator policy** has been assigned to the user group to which the user belongs. Then, add roles or policies of dependent services based on the following **Table 1-2**.

Table 1-2 Anti-DDoS console dependency policies and roles

Console Function	Dependent Service	Role or Policy
Enabling alarm notifications	Simple Message Notification (SMN)	The **SMN ReadOnlyAccess** system policy is required to obtain SMN topic groups.
Adding a tag to an Anti-DDoS instance	Tag Management Service (TMS)	Tag keys can be created only after the **TMS FullAccess** system policy is added.

1.3 Setting a Traffic Scrubbing Threshold to Intercept Attack Traffic

Anti-DDoS automatically enables defense against DDoS attacks for EIPs on Huawei Cloud.

You can configure an Anti-DDoS defense policy in either of the following ways:

- Use the default protection policy.

  The initial system policy serves as the default protection policy and applies to all newly purchased EIPs. It does not impact the traffic scrubbing threshold of existing EIPs. The default **traffic scrubbing threshold** is 120 Mbit/s and can be modified.
- Set a protection policy for a specified EIP.

  You can manually set protection policies for your public IP addresses in batches or one by one. The default protection policy will no longer be used for public IP addresses for which protection policies have been manually configured.

NOTICE

If the selected threshold does not align with the workloads, some attacks may not be properly defended against, or service traffic may be inaccurately scrubbed. Choose a value closest to the purchased bandwidth but not exceeding it.

Manually Setting a Default Protection Policy

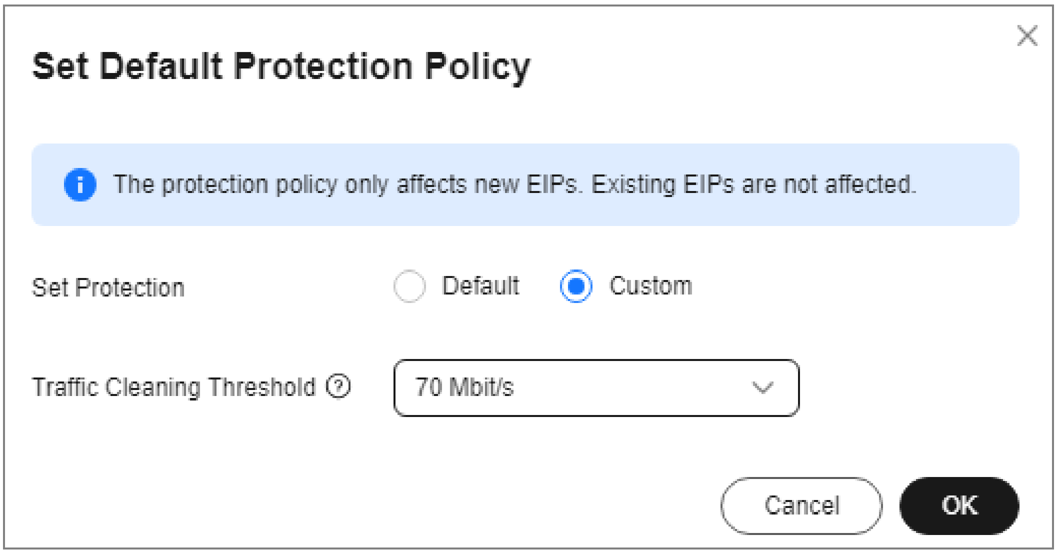
Step 1 Log in to the management console.

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

Step 3 Select the **Public IP Addresses** tab and click **Set Default Protection Policy**.

Step 4 Set the **traffic cleaning threshold** based on the site requirements, as shown in **Figure 1-3**.

Figure 1-3 Manually configuring the default protection policy



Set Default Protection Policy

The protection policy only affects new EIPs. Existing EIPs are not affected.

Set Protection ○ Default ● Custom

Traffic Cleaning Threshold: 70 Mbit/s

Table 1-3 Parameter description

Parameter	Description
Traffic Cleaning Threshold	Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the threshold. The default protection rate is 120 Mbit/s. You can manually set more protection levels. **NOTE** ● If service traffic triggers scrubbing, only attack traffic is intercepted. If service traffic does not trigger scrubbing, no traffic is intercepted. ● Set this parameter based on the actual service access traffic.

Step 5 Click **OK**.

NOTE

After you set the default protection policy, the newly purchased public IP addresses are protected based on the configured policy.

----End

Setting a Protection Policy for a Specified EIP

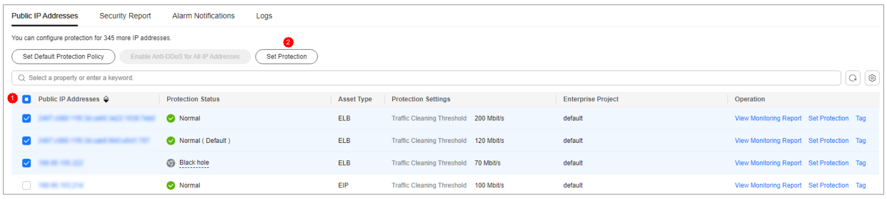
Step 1 Log in to the management console.

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

Step 3 On the **Public IP Addresses** tab page, select a setting method based on the site requirements.

- To configure protection policies for multiple public IP addresses, select multiple public IP addresses and choose **Set Protection** in the upper part of the page.

Figure 1-4 Configuring protection policies in batches

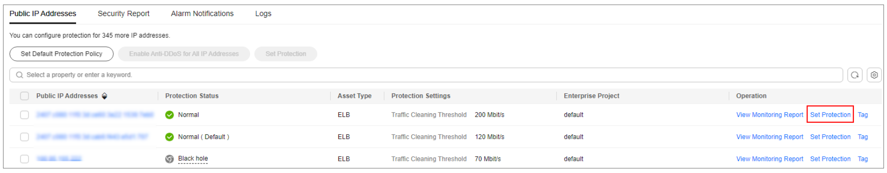

Public IP Addresses
Security Report
Alarm Notifications
Logs
Set Default Protection Policy
Enable Anti-DDoS for All IP Addresses
2
Set Protection
Select a property or enter a keyword.
1

You can configure protection for 345 more IP addresses.

	Public IP Addresses	Protection Status	Asset Type	Protection Settings		Enterprise Project	Operation
☑	[redacted]	Normal	ELB	Traffic Cleaning Threshold	200 Mbit/s	default	View Monitoring Report Set Protection Tag
☑	[redacted]	Normal (Default)	ELB	Traffic Cleaning Threshold	120 Mbit/s	default	View Monitoring Report Set Protection Tag
☑	[redacted]	Black hole	ELB	Traffic Cleaning Threshold	70 Mbit/s	default	View Monitoring Report Set Protection Tag
□	[redacted]	Normal	EIP	Traffic Cleaning Threshold	100 Mbit/s	default	View Monitoring Report Set Protection Tag

- To configure a protection policy for a single public IP address, in the row containing the desired public IP address, choose **Set Protection**.

Figure 1-5 Configuring a protection policy for a public IP address

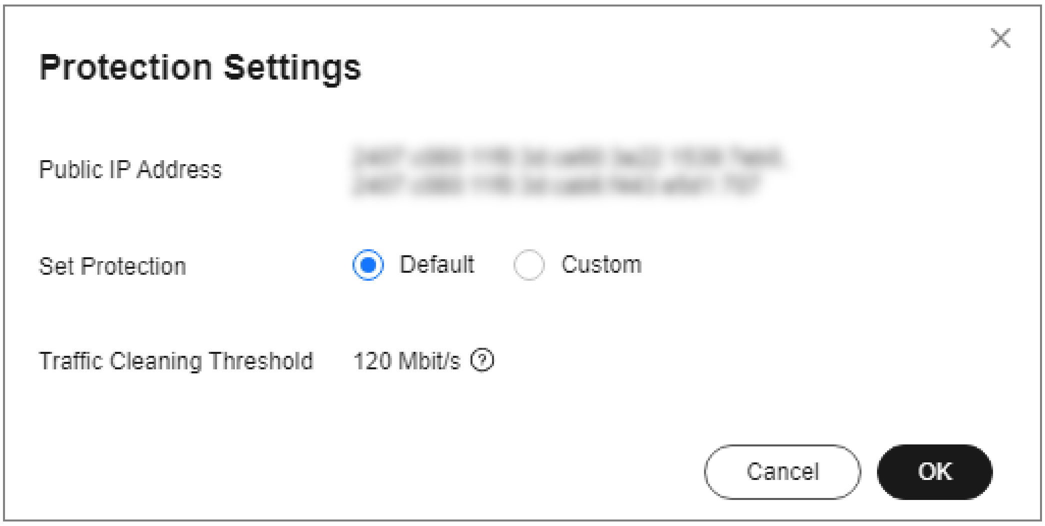

Public IP Addresses
Security Report
Alarm Notifications
Logs
Set Default Protection Policy
Enable Anti-DDoS for All IP Addresses
Set Protection
Select a property or enter a keyword.

You can configure protection for 345 more IP addresses.

□	Public IP Addresses	Protection Status	Asset Type	Protection Settings		Enterprise Project	Operation
□	[redacted]	Normal	ELB	Traffic Cleaning Threshold	200 Mbit/s	default	View Monitoring Report Set Protection Tag
□	[redacted]	Normal (Default)	ELB	Traffic Cleaning Threshold	120 Mbit/s	default	View Monitoring Report Set Protection Tag
□	[redacted]	Black hole	ELB	Traffic Cleaning Threshold	70 Mbit/s	default	View Monitoring Report Set Protection Tag

Step 4 Set the **Traffic Cleaning Threshold** based on the site requirements.

Figure 1-6 Configuring a protection policy



Protection Settings

Public IP Address [redacted]

Set Protection ● Default ○ Custom

Traffic Cleaning Threshold 120 Mbit/s

Table 1-4 Parameters for configuring a protection policy

Parameter	Description
Traffic Cleaning Threshold	Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the threshold. The default protection rate is **120 Mbit/s**. You can manually set more protection levels. **NOTE** ● If service traffic triggers scrubbing, only attack traffic is intercepted. If service traffic does not trigger scrubbing, no traffic is intercepted. ● Set this parameter based on the actual service access traffic. You are advised to set a value closest to, but not exceeding, the purchased bandwidth.

Step 5 Then, click **OK**.

----End

Viewing the EIP Protection Status

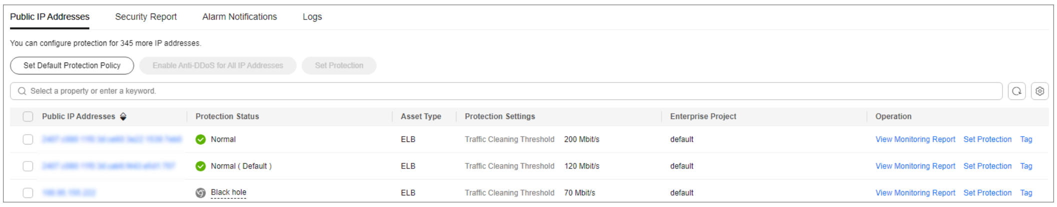
After setting a traffic scrubbing threshold for an EIP, you can view the EIP status and protection information.

Step 1 Log in to the management console.

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

Step 3 Click the **Public IP Addresses** tab to view the public IP addresses.

Figure 1-7 Viewing a public IP address



Public IP Addresses
Security Report
Alarm Notifications
Logs
Set Default Protection Policy
Enable Anti-DDoS for All IP Addresses
Set Protection
Select a property or enter a keyword.

You can configure protection for 345 more IP addresses.

Public IP Addresses	Protection Status	Asset Type	Protection Settings	Enterprise Project	Operation
[redacted]	✓ Normal	ELB	Traffic Cleaning Threshold 200 Mbit/s	default	View Monitoring Report Set Protection Tag
[redacted]	✓ Normal (Default)	ELB	Traffic Cleaning Threshold 120 Mbit/s	default	View Monitoring Report Set Protection Tag
[redacted]	Black hole	ELB	Traffic Cleaning Threshold 70 Mbit/s	default	View Monitoring Report Set Protection Tag

NOTE

- Anti-DDoS provides protection for servers using IPv4 and IPv6 protocols against DDoS attacks.
- Click **Enable Anti-DDoS for All IP Addresses** to enable the protection for all unprotected IP addresses in the current region.
- After the default Anti-DDoS protection settings are enabled, traffic is scrubbed when its volume reaches 120 Mbit/s. You can modify Anti-DDoS protection settings according to **Setting a Traffic Scrubbing Threshold to Intercept Attack Traffic**.
- Anti-DDoS provides a 500 Mbit/s mitigation capacity against DDoS attacks. Traffic that exceeds 500 Mbit/s from the attacked public IP addresses will be routed to the black hole and the legitimate traffic will be discarded. To protect your server from volumetric attacks exceeding 500 Mbit/s, purchase HUAWEI CLOUD Advanced Anti-DDoS (AAD) for enhanced protection.
- The **All statuses** drop-down box enables you to specify a status so that only public IP addresses of the selected status are displayed.

Table 1-5 Parameter description

Parameter	Description
Public IP Address	Public IP address protected by Anti-DDoS **NOTE** If Anti-DDoS is enabled for a public IP address, you can click the IP address to go to its **Monitoring Report** page.
Protection Status	Protection status of a public IP address. The values are: ● **Normal** ● **Configuring** ● **Disabled** ● **Cleaning** ● **Black hole**
Asset Type	Type of a protected object. ● EIP ● ELB ● NetInterFace ● Virtual Private Network (VPN) ● NAT Gateway ● VIP: HA virtual IP address. ● Cloud Container Instance (CCI) ● SubEni
Protection Settings	Traffic scrubbing threshold of the current public IP address.
Enterprise Project	Enterprise project to which the current public IP address belongs.

----End

1.4 Setting DDoS Alarm Notifications

If alarm notifications are enabled, alarm notifications will be sent to you (by SMS or email) if a DDoS attack is detected. If you do not enable this function, you have to log in to the management console to view alarms.

Prerequisites

You have created a message notification topic. For details, see **Simple Message Notification User Guide**.

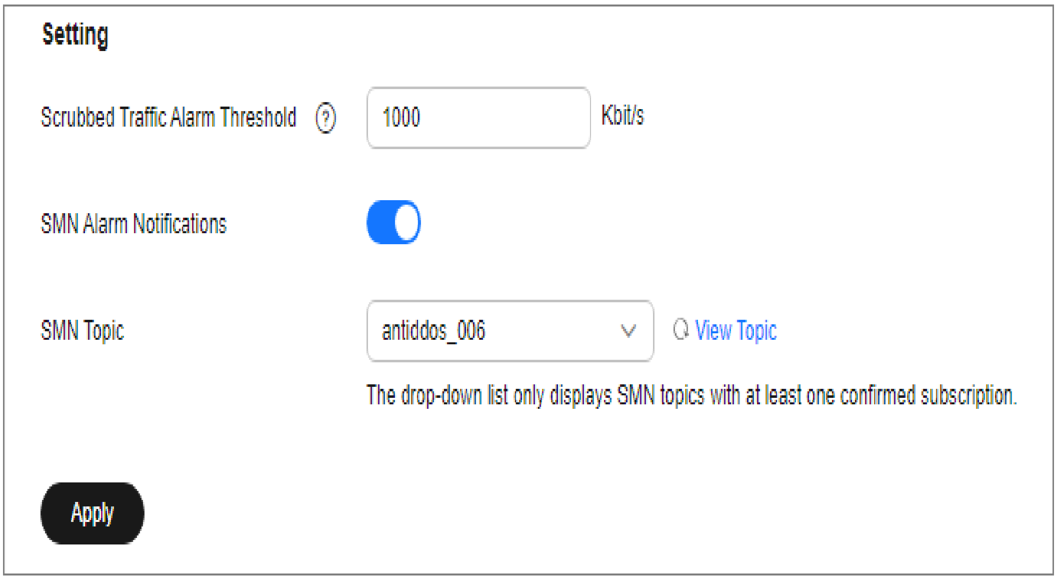
Enabling Alarm Notifications

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

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

Step 3 On the **Anti-DDoS** page, click the **Alarm Notifications** tab and configure the alarm notification. For details about the parameter settings, see **Table 1-6**.

Figure 1-8 Configuring alarm notifications



Setting

Scrubbed Traffic Alarm Threshold: 1000 Kbit/s

SMN Alarm Notifications: ●

SMN Topic: antiddos_006

The drop-down list only displays SMN topics with at least one confirmed subscription.

Table 1-6 Configuring alarm notifications

Parameter	Description
Scrubbed Traffic Alarm Threshold	When the volume of scrubbed traffic reaches the threshold, an alarm notification is sent. Set the threshold as required.

Parameter	Description
Alarm Notifications	Indicates whether the alarm notification function is enabled. There are two values: ● : enabled ● : disabled
SMN Topic	You can select an existing topic or click **View Topic** to create a topic. For more information about SMN topics, see **Simple Message Notification User Guide**.

Step 4 Click **Apply** to enable alarm notification.

----End

1.5 Enabling DDoS Alarm Notifications

Cloud Eye enables event monitoring for protected EIPs. When events like scrubbing, blocking, or unblocking occur, an alarm is triggered, ensuring you are promptly informed about the protection status.

After the event alarm notification function is enabled, you can view event details on the **Event Monitoring** page of the Cloud Eye console when an event occurs.

Enabling Event Alarm Notifications

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

Step 2 Click in the upper left corner of the displayed page to select a region.

Step 3 Hover your mouse over ☰ in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

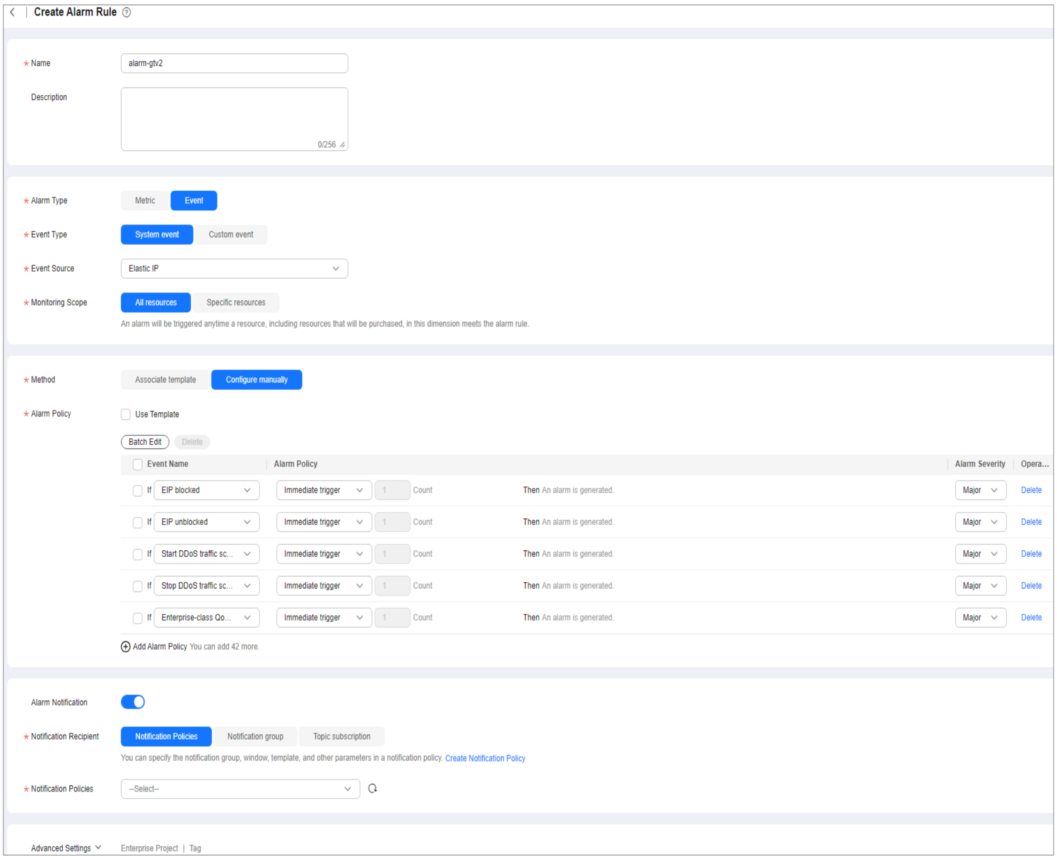
Step 4 Select a monitoring method based on the site requirements.

- Method 1: In the navigation tree on the left, choose **Event Monitoring**. The **Event Monitoring** page is displayed.
- Method 2: In the navigation pane on the left, choose **Alarms** > **Alarm Rules**. The **Alarm Rules** page is displayed.

Step 5 In the upper right corner of the page, click **Create Alarm Rule**. The **Create Alarm Rule** page is displayed.

Step 6 Set alarm parameters by referring to **Table 1-7**.

Figure 1-9 Alarm parameters



Create Alarm Rule

* Name: alarm-gtv2

Description: 0/256

* Alarm Type: Metric | **Event**

* Event Type: **System event** | Custom event

* Event Source: Elastic IP

* Monitoring Scope: **All resources** | Specific resources

An alarm will be triggered anytime a resource, including resources that will be purchased, in this dimension meets the alarm rule.

* Method: Associate template | **Configure manually**

* Alarm Policy: □ Use Template

Batch Edit | Delete

□ Event Name	Alarm Policy				Alarm Severity	Opera...
□ If EIP blocked	Immediate trigger	1	Count	Then An alarm is generated.	Major	Delete
□ If EIP unblocked	Immediate trigger	1	Count	Then An alarm is generated.	Major	Delete
□ If Start DDoS traffic sc...	Immediate trigger	1	Count	Then An alarm is generated.	Major	Delete
□ If Stop DDoS traffic sc...	Immediate trigger	1	Count	Then An alarm is generated.	Major	Delete
□ If Enterprise-class Qo...	Immediate trigger	1	Count	Then An alarm is generated.	Major	Delete

Add Alarm Policy You can add 42 more.

Alarm Notification: ●

* Notification Recipient: **Notification Policies** | Notification group | Topic subscription

You can specify the notification group, window, template, and other parameters in a notification policy. Create Notification Policy

* Notification Policies: --Select--

Advanced Settings: Enterprise Project | Tag

Table 1-7 Parameters for configuring a protection policy

Parameter	Description
Name	Name of the rule. The system generates a random name and you can modify it.
Description	Description about the rule.
Alarm Type	Select **Event**.
Event Type	Choose **System Event**.
Event Source	Choose **Elastic IP**.
Monitoring Scope	Specifies the resource scope to which the alarm rule applies. Set this parameter as required.
Method	The default option is **Configure manually**.

Parameter	Description
Alarm Policy	You are advised to select **EIP blocked**, **EIP unblocked**, **Start Anti-DDoS traffic scrubbing**, and **Stop Anti-DDoS traffic scrubbing**. When the traffic is greater than 10,000 kbit/s, the system sends an alarm notification when scrubbing starts and when scrubbing ends. When the traffic is less than 10,000 kbit/s, no alarm notification is sent.
Notification Recipient	Set it to the actual recipient. **NOTE** Alarm messages are sent by Simple Message Notification (SMN), which may incur a small amount of fees.

Step 7 Click **Create**. In the dialog box that is displayed, click **OK**. The alarm notification is created successfully.

----End

1.6 Enabling Logging

After you authorize Anti-DDoS to access Log Tank Service (LTS), you can use the Anti-DDoS logs recorded by LTS for quick and efficient real-time analysis, device O&M management, and analysis of service trends.

Prerequisites

You have created an LTS log group and a log stream. For details, see **Managing Log Groups** and **Managing Log Streams**.

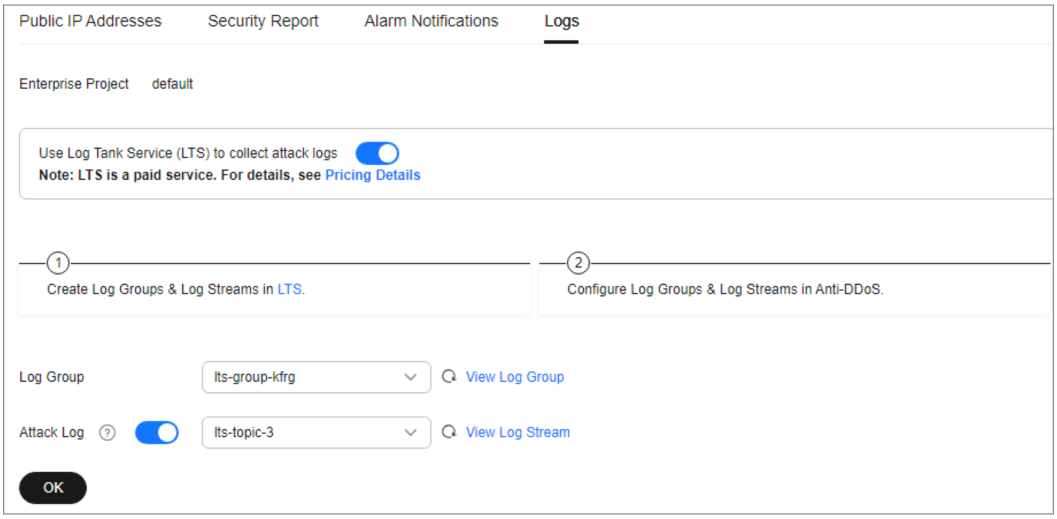
Enabling LTS

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

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

Step 3 Click the **Configure Logs** tab, enable LTS (●), and select a log group and log stream. **Table 1-8** describes the parameters.

Figure 1-10 Configuring logs



Enterprise Project default

Use Log Tank Service (LTS) to collect attack logs

Note: LTS is a paid service. For details, see Pricing Details

1
Create Log Groups & Log Streams in LTS.
2
Configure Log Groups & Log Streams in Anti-DDoS.

Log Group lts-group-kfrg

Attack Log lts-topic-3

Table 1-8 Log configuration

Parameter	Description
Log Group	Select a log group or click **View Log Group** to go to the LTS console and create a log group.
Attack Log	Select a log stream or click **View Log Stream** to go to the LTS console and create a log stream. Attack logs record alarm information about each attack, including the attack type and protected IP address.

Step 4 Click **OK**.

You can view Anti-DDoS protection event logs on the LTS console.

----End

Log Fields in LTS

The following table describes the log fields.

Table 1-9 Log field description

Field	Description
logType	Log type. The default value is **ip_attack_sum**, indicating attack logs.
deviceType	Type of the device that reports logs. The default value is **CLEAN**, indicating the scrubbing device.
inKbps	Inbound traffic, in kbit/s.
maxPps	Peak incoming traffic, in pps.

Field	Description
dropPps	Average number of discarded packets, in pps.
maxAttackInBps	Indicates the incoming traffic at the peak time of attack traffic, in bit/s.
currentConn	Current connections
zoneIP	Protected IP address.
logTime	Time when a log is generated.
attackType	Attack type. For details about the corresponding attack types, see **Table 1-10**.
inPps	Inbound traffic, in pps.
maxKbps	Peak inbound traffic, in kbit/s.
dropKbps	Average discarded traffic, in kbit/s.
startTime	Time when the attack starts.
endTime	End time of the attack. If this parameter is left blank, the attack has not ended yet.
maxAttackInConn	Number of connections at the peak time of attack traffic.
newConn	New connections.

Table 1-10 Attack type description

Value	Attack Type
0-9	User-defined attack type
10	SYN flood attack
11	Ack flood attack
12	SynAck flood attack
13	Fin/Rst flood attack
14	Concurrent connections exceed the threshold.
15	New connections exceed the threshold.
16	TCP fragment attack
17	TCP fragment bandwidth limit attack
18	TCP bandwidth limit attack
19	UDP flood attack

Value	Attack Type
20	UDP fragment attack
21	UDP fragment bandwidth limit attack
22	UDP bandwidth limit attack
23	ICMP bandwidth limit attack
24	Other bandwidth limit attack
25	Traffic limiting attack
26	HTTPS flood attack
27	HTTP flood attack
28	Reserved
29	DNS query flood attack
30	DNS reply flood attack
31	SIP flood attack
32	Blacklist dropping
33	Abnormal HTTP URL behavior
34	TCP fragment abnormal dropping traffic attack
35	TCP abnormal dropping traffic attack
36	UDP fragment abnormal dropping traffic attack
37	UDP abnormal dropping traffic attack
38	ICMP abnormal attack
39	Other abnormal attacks
40	Connection flood attack
41	Domain name hijacking attack
42	DNS poisoning packet attack
43	DNS reflection attack
44	Oversize DNS packet attack
45	Abnormal rate of DNS source requests
46	Abnormal rate of DNS source replies
47	Abnormal rate of DNS domain name requests
48	Abnormal rate of DNS domain name replies
49	DNS request packet TTL anomaly

Value	Attack Type
50	DNS packet format anomaly
51	DNS cache matching and dropping attack
52	Port scan attacks
53	Abnormal TCP packet flag bit
54	BGP attack
55	UDP association defense anomaly
56	DNS NO such Name
57	Other fingerprint attacks
58	Zone traffic limit attack
59	HTTP slow attacks
60	Malware prevention
61	Domain name blocking
62	Filtering
63	Web attack packet capture
64	SIP source rate limiting

1.7 Adding a Tag to an EIP

A tag consists of a tag key and a tag value and is used to identify cloud resources. You can use tags to classify cloud resources by dimension, such as usage, owner, or environment. Anti-DDoS allows you to configure tags for protected public IP addresses to better manage them.

Adding a Tag to an EIP

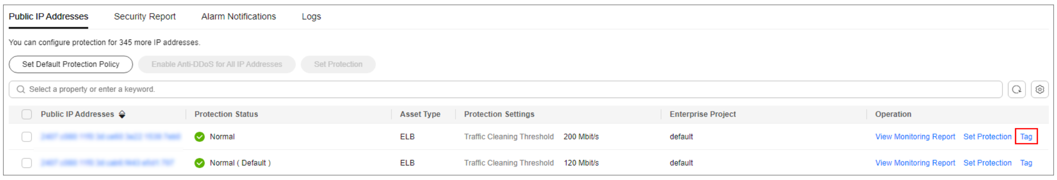
Step 1 Log in to the management console.

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

Step 3 Click the **Public IP Addresses** tab.

Step 4 Locate the row that contains the public IP address for which you want to set a tag, click **Tag**.

Figure 1-11 Adding a tag to an EIP


Public IP Addresses
Security Report
Alarm Notifications
Logs
Set Default Protection Policy
Enable Anti-DDoS for All IP Addresses
Set Protection
Select a property or enter a keyword.

You can configure protection for 345 more IP addresses.

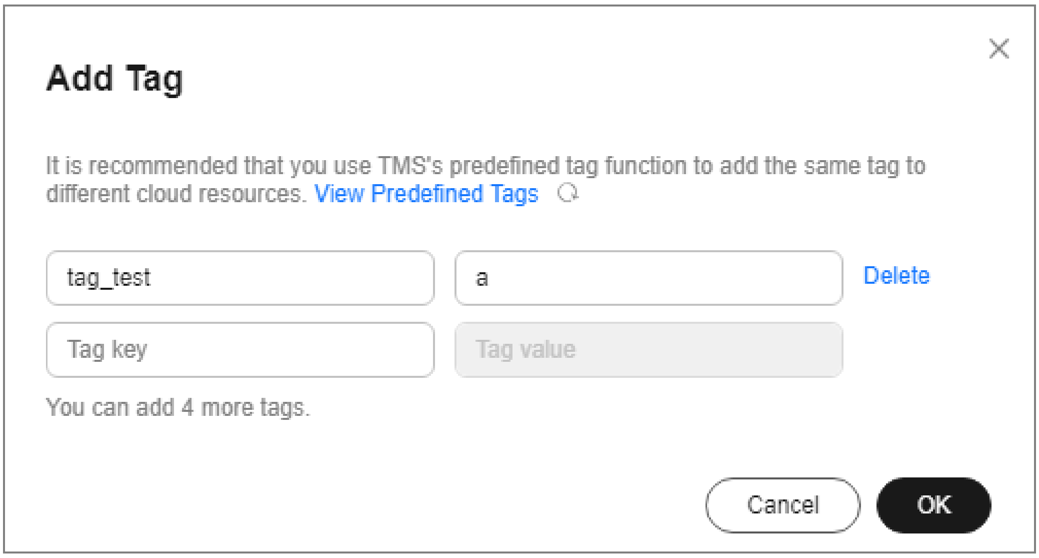
Public IP Addresses	Protection Status	Asset Type	Protection Settings	Enterprise Project	Operation
[redacted]	Normal	ELB	Traffic Cleaning Threshold 200 Mbit/s	default	View Monitoring Report Set Protection Tag
[redacted]	Normal (Default)	ELB	Traffic Cleaning Threshold 120 Mbit/s	default	View Monitoring Report Set Protection Tag

Step 5 On the tag adding page, click **Add Tag** to add a tag.

Step 6 Select the **Tag key** and **Tag value**. There are two ways to add a tag:

- Manually enter a tag key and tag value.
- Select an existing tag.

Figure 1-12 Adding a tag



Add Tag

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View Predefined Tags

tag_test	a	Delete
Tag key	Tag value	

You can add 4 more tags.

NOTE

If your organization has configured a tag policy for the service, you need to add tags to resources based on the tag policy. Otherwise, the tagging operation might fail. For more information about the tag policy, contact your organization administrator.

Step 7 Click **OK**.

----End

1.8 Viewing an EIP Monitoring Report

On the Anti-DDoS console, you can view the monitoring details of a specified EIP. This includes the current protection status, protection settings, and traffic and abnormal events within the last 24 hours.

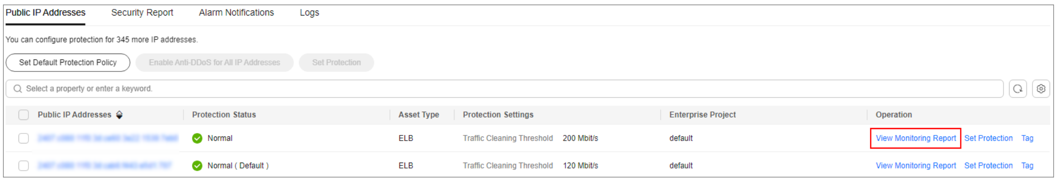
Viewing a monitoring report

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

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

Step 3 Click the **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 1-13 Viewing a monitoring report



Public IP Addresses
Security Report
Alarm Notifications
Logs

You can configure protection for 345 more IP addresses.

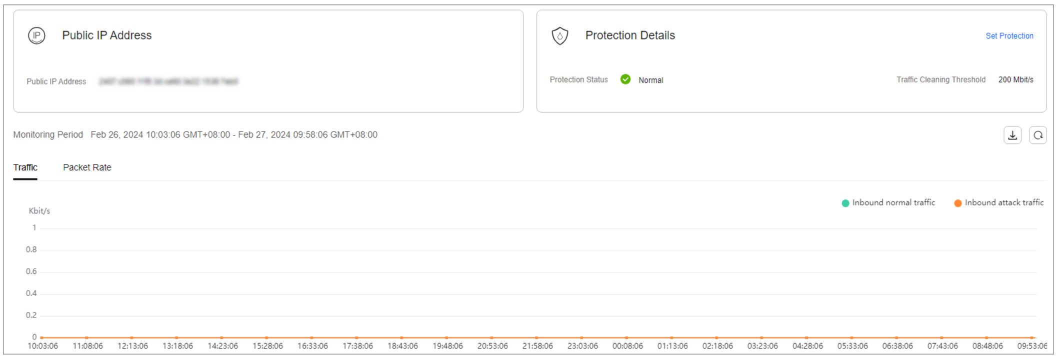
Set Default Protection Policy
Enable Anti-DDoS for All IP Addresses
Set Protection
Select a property or enter a keyword.

□	Public IP Addresses	Protection Status	Asset Type	Protection Settings	Enterprise Project	Operation
□	[redacted]	✓ Normal	ELB	Traffic Cleaning Threshold 200 Mbit/s	default	View Monitoring Report Set Protection Tag
□	[redacted]	✓ Normal (Default)	ELB	Traffic Cleaning Threshold 120 Mbit/s	default	View Monitoring Report Set Protection Tag

Step 4 On the **Monitoring Report** page, view monitoring details about the public IP address.

- You can view information such as the current defense status, current defense configurations, traffic within 24 hours, and abnormalities within 24 hours.
- A 24-hour defense traffic chart is generated from data points taken in five-minute intervals. It includes the following information:
  - **Traffic** displays the traffic status of the selected ECS, including the incoming attack traffic and normal traffic.
  - **Packet Rate** displays the packet rate of the selected ECS, including the attack packet rate and normal incoming packet rate.
- The attack event list within one day records DDoS attacks on the ECS within one day, including cleaning events and black hole events.

Figure 1-14 Viewing a traffic monitoring report



Public IP Address

Public IP Address [redacted]

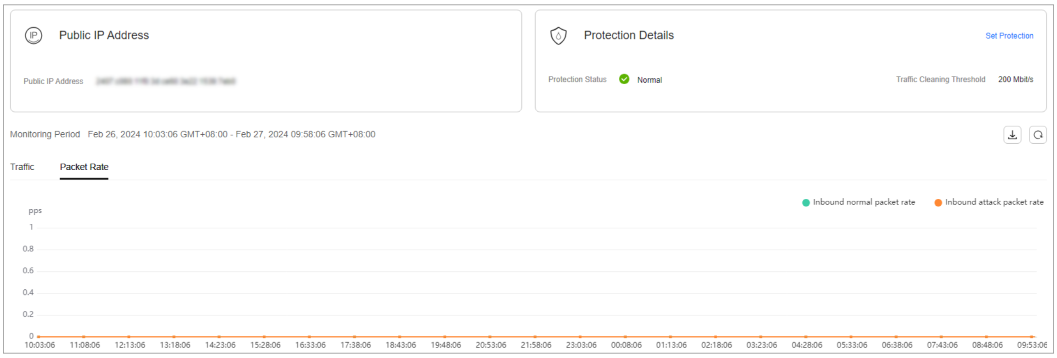
Protection Details

Protection Status ✓ Normal

Traffic Cleaning Threshold 200 Mbit/s

Monitoring Period Feb 26, 2024 10:03:06 GMT+08:00 - Feb 27, 2024 09:58:06 GMT+08:00

Figure 1-15 Viewing the packet rate



Public IP Address

Public IP Address [redacted]

Protection Details

Set Protection

Protection Status ✓ Normal

Traffic Cleaning Threshold 200 Mbit/s

Monitoring Period Feb 26, 2024 10:03:06 GMT+08:00 - Feb 27, 2024 09:58:06 GMT+08:00

Traffic Packet Rate

NOTE

Click ⤓ to download monitoring reports to view monitoring details about the public IP address.

----End

1.9 Viewing an Interception Report

The Anti-DDoS console produces weekly interception reports. These reports provide EIP protection statistics, including the number of scrubbing times, scrubbed traffic volume, the top 10 attacked public IP addresses, and the total number of intercepted attacks.

Viewing an Interception Report

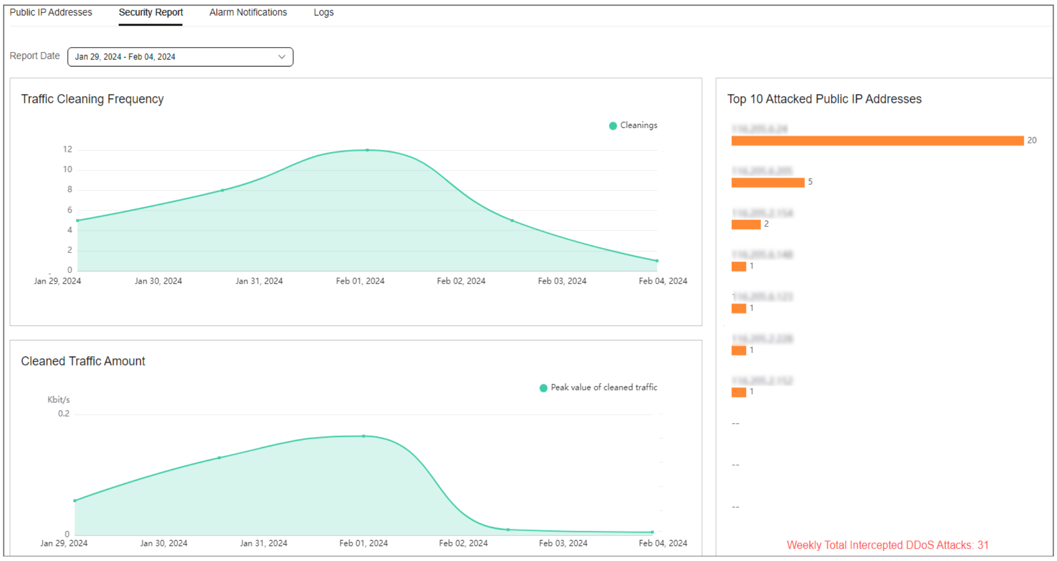
Step 1 Log in to the management console.

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

Step 3 Click the **Statistics** tab to view the protection statistics about all public IP addresses.

You can view the weekly security report generated on a specific date. Currently, statistics, including the number of cleaning times, cleaned traffic, weekly top 10 most frequently attacked public IP addresses, and total number of intercepted attacks over the past four weeks can be queried.

Figure 1-16 Viewing an interception report



Report Date Jan 29, 2024 - Feb 04, 2024

Weekly Total Intercepted DDoS Attacks: 31

NOTE

Click ⤓ to download interception reports to view defense statistics of a time range.

----End

1.10 Querying Audit Logs

1.10.1 Anti-DDoS Operations That Can Be Recorded by CTS

Cloud Trace Service (CTS) provides you with a history of Anti-DDoS operations. After enabling CTS, you can view all generated traces to query, audit, and review performed Anti-DDoS operations. For details, see the *Cloud Trace Service User Guide*.

Table 1-11 lists the Anti-DDoS operations that can be recorded by CTS.

Table 1-11 Anti-DDoS operations that can be recorded by CTS

Operation	Trace Name
Modifying Anti-DDoS service configurations	UPDATE_ANTIDDOS
Setting LTS full log configurations	UPDATE_LTS_CONFIG
Adding or editing TMS resource tags in batches	UPDATE_RESOURCE_TAGS
Deleting TMS resource tags in batches	DELETE_RESOURCE_TAGS
Updating the alarm notification configuration of a tenant	UPDATE_ALERT_CONFIG

Operation	Trace Name
Changing the default traffic scrubbing threshold of Anti-DDoS	UPDATE_DEFAULT_CONFIG
Deleting the default traffic scrubbing threshold of Anti-DDoS	DELETE_DEFAULT_CONFIG
Querying the task list	QUERY_TASK_LIST
Querying alarm configuration details	QUERY_ALERT_CONFIG
Querying the protection configuration of an IP address	QUERY_IP_DEFENSE_POLICY
Querying the Anti-DDoS configuration list	QUERY_DEFENSE_POLICY_LIST
Querying the protection status of an IP address	QUERY_IP_DEFENSE_STATUS
Querying the protection status of IP addresses in batches	QUERY_IP_LIST_DEFENSE_STATUS
Querying daily traffic details of an IP address	QUERY_IP_DAILY_TRAFFIC_REPORT
Exporting daily traffic details of an IP address	EXPORT_IP_DAILY_TRAFFIC_REPORT
Querying the daily abnormal event list of an IP address	QUERY_IP_DAILY_EVENT_REPORT
Querying weekly defense statistics of an IP address	QUERY_IP_WEEKLY_REPORT
Exporting weekly defense statistics of an IP address	EXPORT_IP_WEEKLY_REPORT
Querying the configuration status	QUERY_CONFIG_STATUS
Querying credit information	QUERY_CREDIT_INFO
Querying the default traffic scrubbing threshold	QUERY_DEFAULT_CONFIG
Querying quotas	QUERY_QUOTA
Querying all log configurations	QUERY_LOG_CONFIG
Querying a resource instance	QUERY_TMS_RESOURCE_INSTANCE
Querying the number of resource instances	QUERY_TMS_RESOURCE_COUNT
Querying the resource tags of an IP address	QUERY_IP_RESOURCE_TAG
Querying the resource tag list	QUERY_RESOURCE_TAG_LIST

1.10.2 Viewing Logs on CTS

After you enable CTS, the system starts recording operations performed to Anti-DDoS resources. Operation records generated during the last seven days can be viewed on the CTS console.

You can view historical Anti-DDoS operation records on the CTS console.

Prerequisites

You have enabled CTS. For details, see **Enabling CTS**.

Viewing Anti-DDoS Audit Logs

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

Step 2 Click ☰ on the left of the page and choose **Cloud Trace Service** under **Management & Deployment**.

Step 3 Choose **Trace List** in the navigation pane on the left.

Step 4 Select **Trace Source** from the drop-down list, enter **Anti-DDoS**, and press **Enter**.

Step 5 Click a trace name in the query result to view the event details.

You can use the advanced search function to combine one or more filter criteria in the filter box.

- Enter **Trace Name**, **Resource Name**, **Resource ID**, and **Trace ID**.
  - **Resource Name**: If the cloud resource involved in the trace does not have a name or the corresponding API operation does not involve resource names, this field is left empty.
  - **Resource ID**: If the resource does not have a resource ID or the resource fails to be created, this field is left empty.
- **Trace Source** and **Resource Type**: Select the corresponding cloud service name or resource type from the drop-down list.
- **Operator**: Select one or more operators from the drop-down list.
- Trace Status: The value can be **normal**, **warning**, or **incident**. You can select only one of them.
  - **normal**: indicates that the operation is successful.
  - **warning**: indicates that the operation failed.
  - **incident**: indicates a situation that is more serious than an operation failure, for example, other faults are caused.
- Time range: You can query traces generated in the last hour, day, or week, or customize traces generated in any time period of the last week.

----End

2 CNAD Advanced (CNAD) Operation Guide

2.1 CNAD Overview

The following figure shows the process of connecting an EIP to CNAD for protection.

Figure 2-1 Connecting an EIP to CNAD

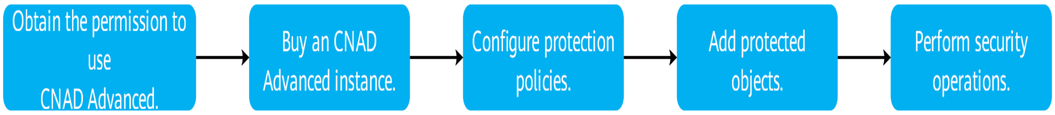

Obtain the permission to use CNAD Advanced.
Buy an CNAD Advanced instance.
Configure protection policies.
Add protected objects.
Perform security operations.

Table 2-1 Procedures

No.	Procedure	Description
1	**Using IAM to Grant CNAD Permissions**	Use Identity and Access Management (IAM) to grant fine-grained CNAD service permissions to users.
2	**Purchasing a CNAD Instance**	Purchase a CNAD instance based on service requirements.
3	**Adding a Protection Policy**	Configure protection policies based on your service requirements. CNAD provides a wide range of protection policies.
4	**Adding a Protected Object**	Add the EIP to be protected to the CNAD instance.

No.	Procedure	Description
5	Performing common security operations	- **Enabling Alarm Notifications for DDoS Attacks**: After the alarm notification function is enabled, you will receive alarm notifications if your EIP is under a DDoS attack. - **Enabling Logging**: With LTS, you can perform real-time decision analysis, device O&M management, and service trend analysis in a timely and efficient manner. - **Viewing Statistics Reports**: You can view access and attack statistics within a specified time range. - **Managing Instances**: You can perform common instance management operations, such as enabling renewal, upgrading specifications, and configuring tags. - **Managing Protected Objects**: You can view information about protected objects and remove protected objects. - **Viewing Monitoring Metrics**: You can enable event and metric monitoring for protected EIPs on Cloud Eye. - **Querying Audit Logs**: You can view historical operation records of CNAD on CTS.

2.2 Using IAM to Grant CNAD Permissions

2.2.1 Creating a User and Granting the CNAD Access Permission

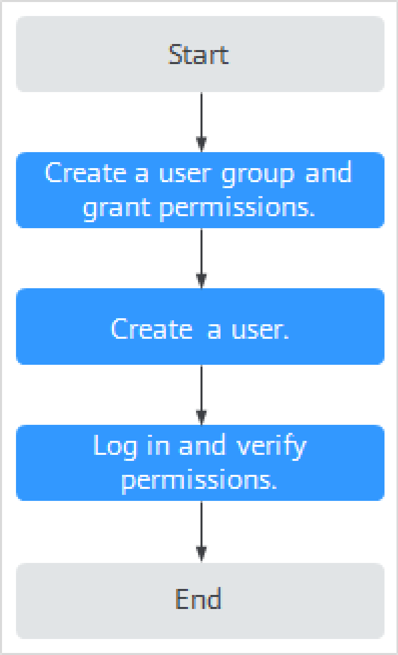
You can use **Identity and Access Management (IAM)** for refined permissions control for CNAD resources. To be specific, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing CNAD resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust a Huawei Cloud account or cloud service to perform professional and efficient O&M to your CNAD resources.

If your Huawei Cloud account does not require individual IAM users, skip this section.

Process

Figure 2-2 Process for granting permissions


Start
Create a user group and grant permissions.
Create a user.
Log in and verify permissions.
End

1. **Create a user group and assign permissions to it.**

   Create a user group on the IAM console, and grant the **CNAD FullAccess** permission to the group.

2. **Create an IAM user and add the user to the group.**

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify permissions.

   Log in to the management console using the created user, and verify the user's permissions.

   Hover over ☰ in the upper left corner, select any other services (for example, there is only the **CNAD FullAccess** policy). If a message indicating that the permission is insufficient is displayed, the **CNAD FullAccess** permission has taken effect.

2.2.2 CNAD Pro Custom Policies

Custom policies can be created to supplement the system-defined policies of CNAD Pro. For details about the actions supported by custom policies, see **CNAD Pro Permissions and Actions**.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. You do not need to have knowledge of the policy syntax.
- JSON: Create a policy in JSON format or edit the JSON strings of an existing policy.

For details, see **Creating a Custom Policy**. The following section contains examples of common CNAD Pro custom policies.

Example of Custom CNAD Pro Policies

- Example 1: Allowing users to query the protected IP address list

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "cnad:protectedIpDropList:list"
                                                        ]
                }
        ]
}
```

- Example 2: Denying deleting an IP address blacklist or whitelist rule

  A deny policy must be used together with other policies. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  The following method can be used if you need to assign permissions of the **CNAD FullAccess** policy to a user but you want to prevent the user from deleting namespaces (cnad:blackWhiteIpList:delete). Create a custom policy for denying namespace deletion, and attach both policies to the group to which the user belongs. Then, the user can perform all operations on CNAD Pro except deleting namespaces. The following is an example policy for denying deleting an IP address blacklist or whitelist rule.

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Deny",
                        "Action": [
                                "cnad:blackWhiteIpList:delete"
                        ]
                },
        ]
}
```

2.2.3 CNAD Pro Permissions and Actions

This section describes how to use IAM for fine-grained CNAD permissions management. If your Huawei Cloud account does not need individual IAM users, skip this section.

By default, new IAM users do not have any permissions. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added. Users inherit permissions from the groups and can perform operations on cloud services as allowed by the permissions.

You can grant users permissions by using **roles** and **policies**. Roles are a type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. IAM uses policies to perform fine-grained authorization. A policy defines permissions required to perform operations on specific cloud resources under certain conditions.

Supported Actions

CNAD Pro provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control.

- Permissions: Statements in a policy that allow or deny certain operations
- Actions: Added to a custom policy to control permissions for specific operations

Permission	Action	Dependency
Querying Quotas	cnad:quota:get	-
Querying Details About a Protection Policy	cnad:policy:get	-
Querying Statistics	cnad:countReport:get	-
Querying the Asset Security Status	cnad:securityStatusReport:get	-
Querying Weekly Security Statistics	cnad:weekStatisticsReport:get	-
Configuring an Alarm Notification	cnad:alarmConfig:create	To grant the alarm notification permission to users, you must also grant the **cnad:alarmConfig:create** permission and the **SMN Administrator** permission configured for the **CN-Hong Kong** region to the users.
Deleting an Alarm Notification	cnad:alarmConfig:delete	To grant the alarm notification permission to users, you must also grant the **cnad:alarmConfig:delete** permission and the **SMN Administrator** permission configured for the **CN-Hong Kong** region to the users.

Permission	Action	Dependency
Querying Alarm Notifications	cnad:alarmConfig:get	To grant the alarm notification permission to users, you must also grant the **cnad:alarmConfig:get** permission and the **SMN Administrator** permission configured for the **CN-Hong Kong** region to the users.
Upgrading an Instance	cnad:package:put	-
Binding an IP Address to Be Protected to an Instance	cnad:protectedIp:create	To grant a user the permission for binding objects to a CNAD Pro instance, you need to grant both the **cnad:protectedIp:create** permission and the **vpc:publicIps:list** permission configured for the region to which the instance belongs. For example, a user purchases a CNAD Pro instance that is located in **CN-Hong Kong**. To grant a user the permission for binding objects to a CNAD Pro instance, you need to grant both the **cnad:protectedIp:create** permission, and the **vpc:publicIps:list** permission configured for **CN-Hong Kong** so that the user can only perform operations on the protected objects in **CN-Hong Kong**.
Creating a Protection Policy	cnad:policy:create	-
Updating a Protection Policy	cnad:policy:put	-
Deleting a Protection Policy	cnad:policy:delete	-

Permission	Action	Dependency
Binding a Protection Policy to a Protected IP Address	cnad:bindPolicy:create	-
Removing a Protection Policy from a Protected IP Address	cnad:unbindPolicy:create	-
Adding a Blacklist or Whitelist Rule	cnad:blackWhiteIpList:create	-
Deleting a Blacklist or Whitelist Rule	cnad:blackWhiteIpList:delete	-
Updating the Tag of a Protected IP Address	cnad:ipTag:put	-
Querying the Cleaning Scope	cnad:cleanScaleDropList:list	-
Querying Instances	cnad:packageDropList:list	-
Querying Protection Policies	cnad:policyDropList:list	-
Querying the List of Protected IP Addresses	cnad:protectedIpDropList:list	-
Querying Details of an Instance	cnad:package:list	-
Querying Details About a Protection Policy	cnad:policy:list	-
Querying the List of Protected IP Addresses	cnad:protectedIp:list	-
Querying Total Traffic Data	cnad:trafficTotalReport:list	-
Querying Attack Traffic	cnad:trafficAttackReport:list	-
Queries the Total Number of Data Packets	cnad:packetTotalReport:list	-
Querying the Number of Attack Packets	cnad:packetAttackReport:list	-
Querying DDoS Mitigation Trend	cnad:cleanCountReport:list	-
Querying the Peak Traffic Scrubbed	cnad:cleanKbpsReport:list	-

Permission	Action	Dependency
Querying the Distribution of Attack Types	cnad:attackTypeReport:list	-
Querying Attack Events	cnad:attackReport:list	-
Querying Top 10 Attacked IP Addresses	cnad:attackTop:list	-
Creating an Instance	cnad:package:create	To grant a user the permission for purchasing CNAD Pro, you need to grant the **cnad:package:create** permission to the user and the following BSS permissions configured for all regions: ● bss:order:update Order Operation ● bss:contract:update Contract Modification ● bss:balance:view Account Querying ● bss:order:pay Payment

2.2.4 Permission Dependency of the CNAD Console

When using CNAD, you may need to view resources of or use other cloud services. So you need to obtain required permissions for dependent services so that you can use the dependent services or view their resources. To that end, make sure you have the **CNAD FullAccess** or **CNAD ReadOnlyAccess** assigned first. For details, see **Creating a User and Granting the CNAD Access Permission**.

Dependency Policy Configuration

If an IAM user needs to view or use related functions on the console, ensure that the **CNAD FullAccess** or **CNAD ReadOnlyAccess** has been assigned to the user group to which the user belongs. Then, add roles or policies of dependent services based on the following **Table 2-2**.

Table 2-2 AAD console dependency policies and roles

Console Function	Dependent Service	Roles or Policy
Enabling LTS	Log Tank Service (LTS)	The LTS ReadOnlyAccess system policy is required to select log group and log stream names created in LTS.
Enabling alarm notifications	Simple Message Notification (SMN)	The SMN ReadOnlyAccess system policy is required to obtain SMN topic groups.
Configuring instance tags	Tag Management Service (TMS)	Tag keys can be created only after the **TMS FullAccess** system policy is added.
Purchase an instance	Enterprise Project Management Service (EPS)	You can select an enterprise project when purchasing an instance only after adding the **EPS ReadOnlyAccess** system policy.

2.3 Purchasing a CNAD Instance

To enable CNAD protection, you need to purchase a CNAD instance.

For details about the functions and specifications of each CNAD edition, see **Table 2-3**. Purchase an edition based on service requirements.

Table 2-3 CNAD editions and specifications

Item	Unlimited Protection Basic Edition	Unlimited Protection Advanced Edition	CNAD 2.0
Billing Mode	Yearly/Monthly	Yearly/Monthly	- The instance is billed on a yearly/monthly basis. - Service bandwidth can be billed on a yearly/ monthly or pay-per-use basis.

Item	Unlimited Protection Basic Edition	Unlimited Protection Advanced Edition	CNAD 2.0
Protected Object	Huawei Cloud EIP	Anti-DDoS Service dedicated EIPs	● Chinese mainland: Dynamic BGP EIPs and Anti-DDoS Service dedicated EIPs ● Outside the Chinese mainland: Premium BGP EIPs and Anti-DDoS Service dedicated EIPs
Region	Single-region protection	Single-region protection	● Chinese mainland: Cross-region protection is supported. ● Outside the Chinese mainland: Only Hong Kong and Singapore are supported.
Protocol	IPv4 and IPv6	IPv4	IPv4 and IPv6
Number of Objects	50-500	50-500	50-1000
Service Bandwidth	100Mbps-20Gbps	100Mbps-20Gbps	100Mbps-20Gbps
Protection Capability	Shared unlimited protection, no less than 20 Gbit/s, up to hundreds of Gbit/s.	Shared unlimited protection for up to 1 Tbit/s of traffic	● Chinese mainland: Shared unlimited protection, no less than 20 Gbit/s. ● Outside the Chinese mainland: carrier-based cross-border protection.

NOTE

- When using an Anti-DDoS Service dedicated EIP, extreme scenarios such as network fluctuations may result in traffic being redirected to a standby equipment room with lower protection capabilities, thereby reducing overall protection.
- After adding a premium BGP EIP to CNAD 2.0, it can defend against attacks originating from China but not those from outside China. The black hole threshold for a premium BGP EIP is low; when the number of attacks from outside China exceeds this threshold, the premium BGP EIP will be blocked. To defend against attacks from outside China, purchase an Anti-DDoS Service dedicated EIP and use it with CNAD 2.0.

Prerequisites

- The account must have the permissions of the **CNAD FullAccess** and **BSS Administrator** roles.
- You have applied for using the corresponding service edition.

NOTE

Go to the **Buy AAD** page, set **Instance Type** to **Cloud Native Anti-DDoS Advanced**, and select the specifications.

Purchasing a CNAD Instance

You can purchase instances of different editions based on service requirements.

Purchasing CNAD 2.0

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

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

Step 3 In the upper right corner of the page, click **Buy DDoS Mitigation**.

Step 4 Set **Instance Type** to **Cloud Native Anti-DDoS**.

Step 5 Select a region where the resources to be protected are located.

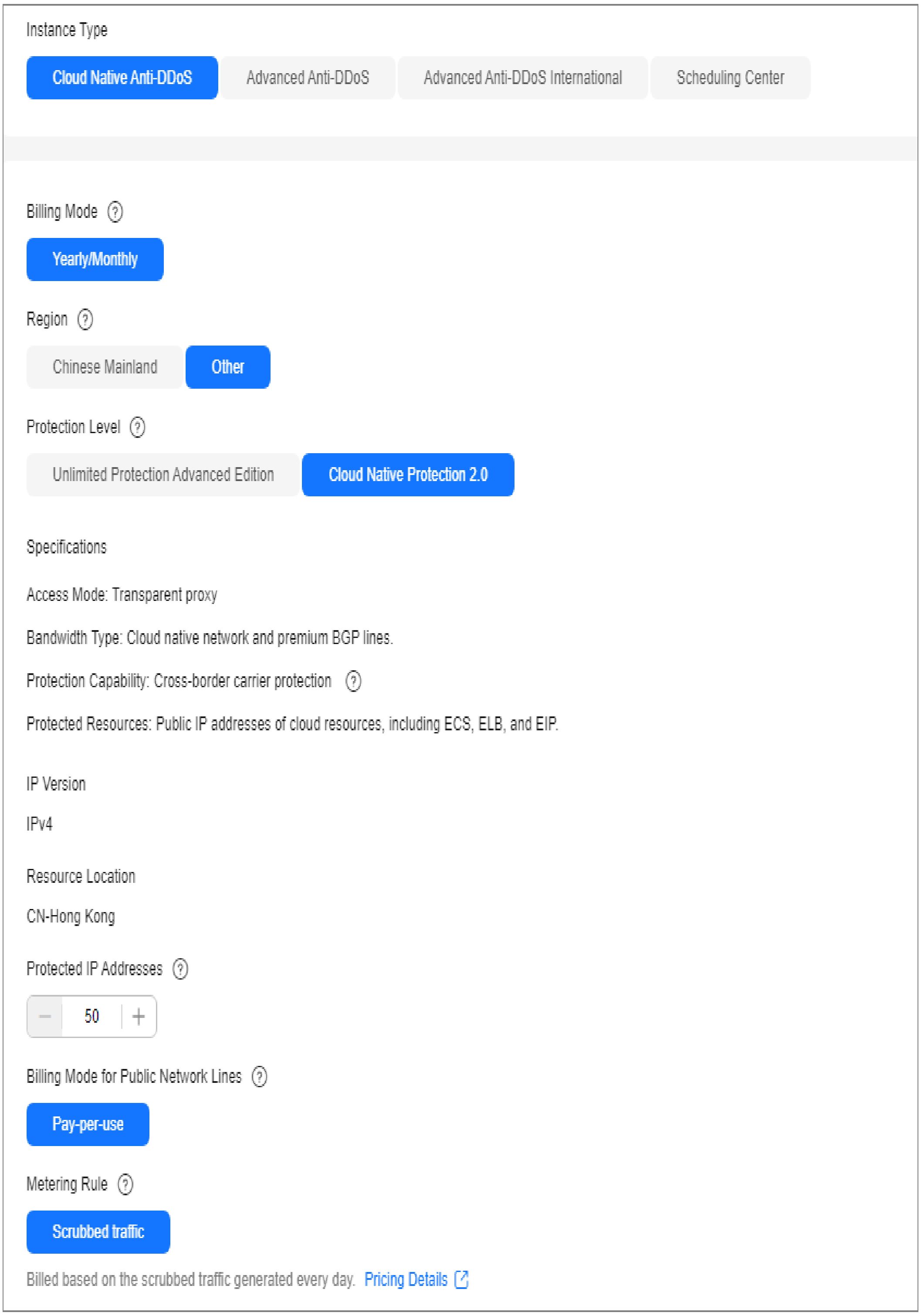
CAUTION

Cloud Native Anti-DDoS 2.0 outside the Chinese mainland can only protect premium BGP IP addresses 49.0.236.0/22, 49.0.234.0/23, and 49.0.233.0/24.

Step 6 For **Protection Level**, select **Cloud Native Anti-DDoS 2.0**.

Step 7 Set the specifications parameters by referring to **Table 2-4**.

Figure 2-3 Cloud Native Anti-DDoS 2.0



Instance Type

Cloud Native Anti-DDoS
Advanced Anti-DDoS
Advanced Anti-DDoS International
Scheduling Center

Billing Mode

Region

Protection Level

Unlimited Protection Advanced Edition
Cloud Native Protection 2.0

Specifications

Access Mode: Transparent proxy

Bandwidth Type: Cloud native network and premium BGP lines.

Protection Capability: Cross-border carrier protection

Protected Resources: Public IP addresses of cloud resources, including ECS, ELB, and EIP.

IP Version

IPv4

Resource Location

CN-Hong Kong

Protected IP Addresses

50

Billing Mode for Public Network Lines

Metering Rule

Billed based on the scrubbed traffic generated every day. Pricing Details

Table 2-4 Parameter description

Parameter	Description
Protected IP Addresses	The value ranges from 50 to 1000, and the number of protected IP addresses must be a multiple of 50.

Parameter	Description
Billing Mode for Public Network Lines	Select one based on site requirements. ● Yearly/Monthly: Your subscription fee is billed according to the selected payment cycle, requiring prepayment for the chosen duration. This mode is supported only in the Chinese mainland. ● Pay-per-use: Charges are incurred daily based on the volume of clean traffic.
Service Bandwidth	This parameter is displayed only when you select **Yearly/ Monthly** for **Billing Mode for Public Network Lines**.
Metering Rule	This parameter is displayed only when you select **Pay-Per-Use** for **Billing Mode for Public Network Lines**. Clean traffic refers to normal service traffic that is not polluted by attacks, excluding attack traffic.

Step 8 Set **Instance Name**, **Required Duration**, and **Quantity**. In the lower right corner of the page, click **Next**.

NOTE

The **Auto-renew** option enables the system to renew your service by the purchased period when the service is about to expire.

Step 9 On the confirmation page, confirm your order and click **Submit Order**.

Step 10 On the **Pay** page, click **Pay**.

After the payment is successful, the newly bought instance will be displayed on the instance list. After the instance status becomes **Normal**, the instance is created.

Step 11 (Optional) Purchase dedicated EIPs in the required region by referring to **Assigning an EIP**.

NOTE

- Compared with common EIPs, Anti-DDoS Service dedicated EIPs offer enhanced defense against attacks at the Anti-DDoS scrubbing center, along with Terabit-level bandwidth and robust protection capabilities.
- To apply for an Anti-DDoS Service dedicated EIP, perform the following steps:
- The following lines are for reference only. The actual lines are listed on the console.

Table 2-5 Network lines for dedicated EIPs

Region	Line
CN South-Guangzhou	5_ddosalways1bgp
CN North-Beijing2	5_DDoSAlways1bgp
CN North-Beijing4	5_DDoSAlways1bgp

Region	Line
CN East-Shanghai1	5_ddosalways1bgp
CN East-Shanghai2	5_DDoSAlways1bgp
AP-Bangkok	5_thddosbgp
LA-Sao Paulo1	5_brzddosbgp
LA-Santiago	5_DDoSAlways1bgp
AF-Johannesburg	5_saddosbgp
CN-Hong Kong	5_DDoSAlways2bgp
AP-Singapore	5_DDoSAlways1bgp

----End

Purchasing Unlimited Protection Basic Edition

Step 1 Log in to the management console.

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

Step 3 In the upper right corner of the page, click **Buy DDoS Mitigation**.

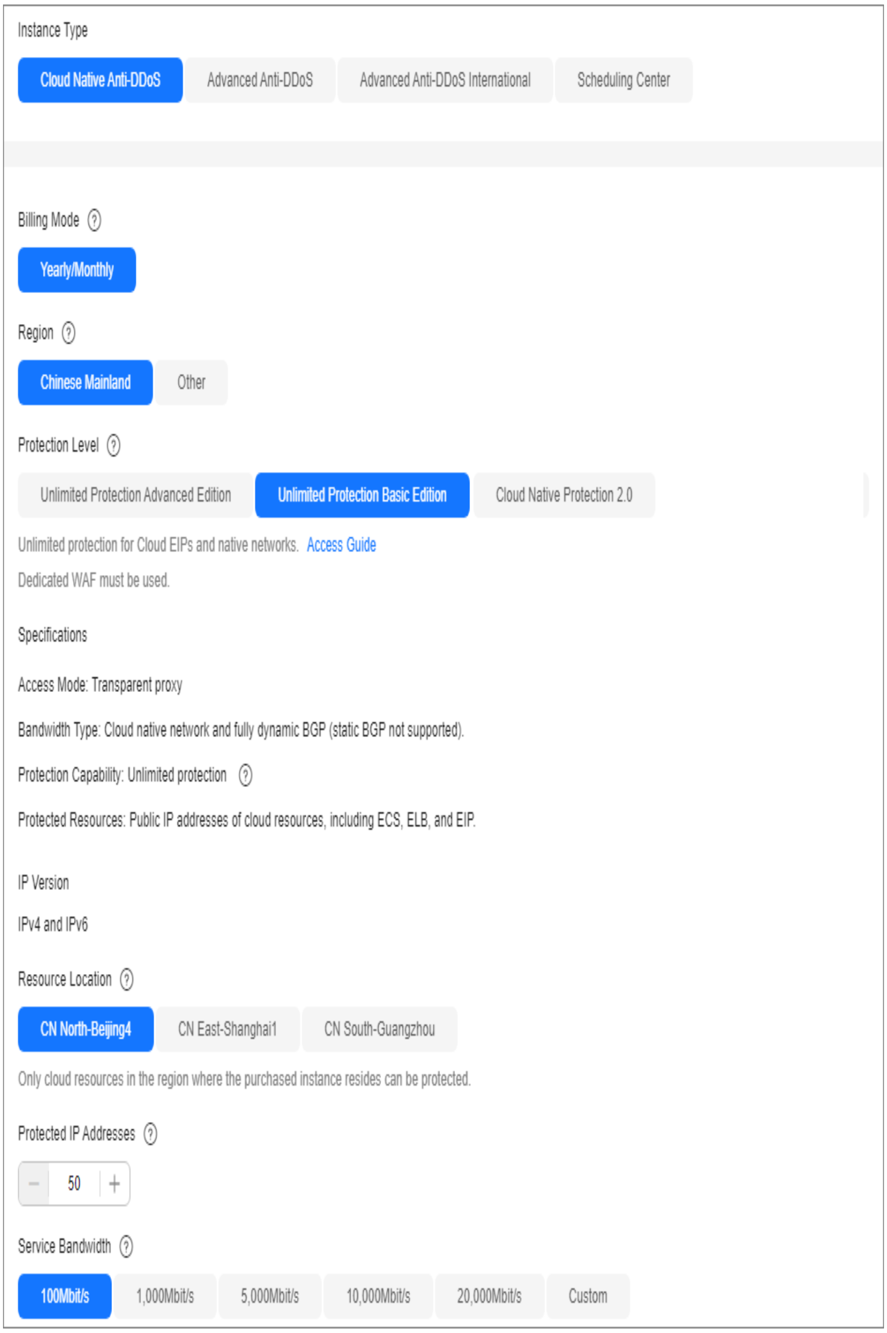
Step 4 Set **Instance Type** to **Cloud Native Anti-DDoS**.

Step 5 **Region**: Select **Chinese Mainland**.

Step 6 Set **Protection Level** to **Unlimited Protection Basic Edition**.

Step 7 Set the specifications parameters, as shown in **Figure 2-4**. **Table 2-6** describes the parameters.

Figure 2-4 Setting Unlimited Protection Basic edition specifications



Instance Type

[✓ Cloud Native Anti-DDoS] Advanced Anti-DDoS Advanced Anti-DDoS International Scheduling Center

Billing Mode

[✓ Yearly/Monthly]

Region

[✓ Chinese Mainland] Other

Protection Level

Unlimited Protection Advanced Edition [✓ Unlimited Protection Basic Edition] Cloud Native Protection 2.0

Unlimited protection for Cloud EIPs and native networks. Access Guide

Dedicated WAF must be used.

Specifications

Access Mode: Transparent proxy

Bandwidth Type: Cloud native network and fully dynamic BGP (static BGP not supported).

Protection Capability: Unlimited protection

Protected Resources: Public IP addresses of cloud resources, including ECS, ELB, and EIP.

IP Version

IPv4 and IPv6

Resource Location

[✓ CN North-Beijing4] CN East-Shanghai1 CN South-Guangzhou

Only cloud resources in the region where the purchased instance resides can be protected.

Protected IP Addresses

− 50 +

Service Bandwidth

[✓ 100Mbit/s] 1,000Mbit/s 5,000Mbit/s 10,000Mbit/s 20,000Mbit/s Custom

Table 2-6 Parameters of Unlimited Protection Basic Edition

Parameter	Description
Region	Unlimited Protection Basic Edition is available only in the Chinese mainland.

Parameter	Description
Resource Location	Select the region where the protected resources are located. **NOTICE** CNAD instances can only protect cloud resources in the same region. Cross-region protection is not supported. For example, a CNAD instance in CN East-Shanghai1 can protect only cloud resources in CN East-Shanghai1.
Protected IP Addresses	A maximum of 50 IP addresses can be protected by default. Every five IP addresses can be added each time, and a maximum of 500 IP addresses can be added.
Service Bandwidth	The service bandwidth indicates clean service bandwidth forwarded to the origin server from the AAD scrubbing center.

Step 8 Set **Instance Name**, **Required Duration**, and **Quantity**. In the lower right corner of the page, click **Next**.

NOTE

The **Auto-renew** option enables the system to renew your service by the purchased period when the service is about to expire.

Step 9 On the confirmation page, confirm your order and click **Submit Order**.

Step 10 On the **Pay** page, click **Pay**.

After the payment is successful, the newly bought instance will be displayed on the instance list. After the instance status becomes **Normal**, the instance is created.

----End

Purchasing Unlimited Protection Advanced Edition

NOTE

Before purchasing the advanced edition, you should know that the Unlimited Protection Advanced edition can protect only exclusive EIPs.

Step 1 Log in to the management console.

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

Step 3 In the upper right corner of the page, click **Buy DDoS Mitigation**.

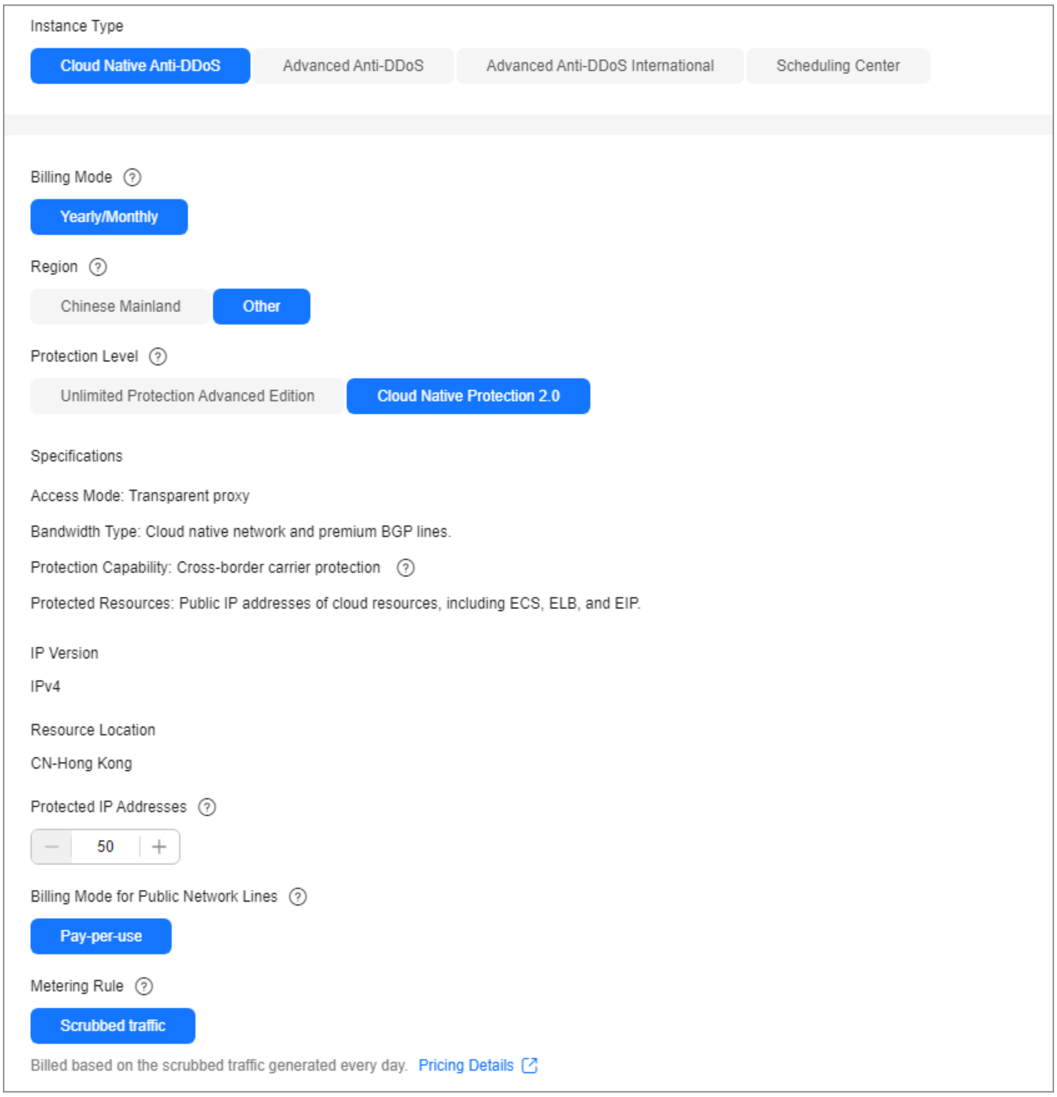
Step 4 Set **Instance Type** to **Cloud Native Anti-DDoS**.

Step 5 Select a region where the resources to be protected are located.

Step 6 Select **Unlimited Protection Advanced Edition** for **Protection Level**.

Step 7 Set the specifications parameters. **Table 2-7** describes related parameters.

Figure 2-5 Setting specifications of the Unlimited Protection Advanced edition



Instance Type

Cloud Native Anti-DDoS
Advanced Anti-DDoS
Advanced Anti-DDoS International
Scheduling Center

Billing Mode: Yearly/Monthly

Region

Protection Level

Unlimited Protection Advanced Edition
Cloud Native Protection 2.0

Specifications

Access Mode: Transparent proxy

Bandwidth Type: Cloud native network and premium BGP lines.

Protection Capability: Cross-border carrier protection

Protected Resources: Public IP addresses of cloud resources, including ECS, ELB, and EIP.

IP Version

IPv4

Resource Location

CN-Hong Kong

Protected IP Addresses: 50

Billing Mode for Public Network Lines: Pay-per-use

Metering Rule: Scrubbed traffic

Billed based on the scrubbed traffic generated every day. Pricing Details

Table 2-7 Parameters of Unlimited Protection Advanced Edition

Parameter	Description
Region	● Chinese Mainland: applies to scenarios where service servers are deployed in Chinese mainland. Only dynamic BGP EIPs are supported. ● Outside the Chinese mainland: applies to scenarios where the service server is deployed in the Asia Pacific region. Only premium BGP EIPs are supported.

Parameter	Description
Resource Location	Select the region where the protected resources are located. **NOTICE** CNAD instances can only protect cloud resources in the same region. Cross-region protection is not supported. For example, a CNAD instance in CN East-Shanghai1 can protect only cloud resources in CN East-Shanghai1.
Protected IP Addresses	A maximum of 50 IP addresses can be protected by default. Every five IP addresses can be added each time, and a maximum of 500 IP addresses can be added.
Service Bandwidth	The service bandwidth indicates clean service bandwidth forwarded to the origin server from the AAD scrubbing center. Value range: 100 Mbit/s to 40,000 Mbit/s

Step 8 Set **Instance Name**, **Required Duration**, and **Quantity**. In the lower right corner of the page, click **Next**.

NOTE

The **Auto-renew** option enables the system to renew your service by the purchased period when the service is about to expire.

Step 9 On the confirmation page, confirm your order and click **Submit Order**.

Step 10 On the **Pay** page, click **Pay**.

After the payment is successful, the newly bought instance will be displayed on the instance list. After the instance status becomes **Normal**, the instance is created.

Step 11 Purchase dedicated EIPs in the required region by referring to **Assigning an EIP**.

Table 2-8 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
AP-Bangkok	5_thddosbgp
LA-Sao Paulo1	5_brzddosbgp
LA-Santiago	5_DDoSAlways1bgp

Region	Line
AF-Johannesburg	5_saddosbgp
CN-Hong Kong	5_DDoSAlways2bgp
AP-Singapore	5_DDoSAlways1bgp

NOTE

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

----End

2.4 Adding a Protection Policy

2.4.1 Protection Policy Overview

CNAD provides various protection policies. After purchasing an instance, you can select an appropriate protection policy based on service requirements. For details, see **Table 2-9**.

NOTICE

If the protection policy is incorrectly configured, attacks may fail to be defended against or traffic may be incorrectly scrubbed. Exercise caution when performing this operation.

Table 2-9 Protection policies

Protection Policy	Section	Description
Basic protection	**Configuring a Basic Protection Policy to Intercept Attack Traffic**	Configure a basic protection policy for protected objects. If the DDoS attack bandwidth for an IP address surpasses the configured scrubbing threshold, CNAD is activated to scrub the attack traffic, ensuring service availability.
IP address blacklist or whitelist	**Blocking or Permitting Traffic From Specified IP Addresses Using a Blacklist and Whitelist**	You can configure an access control list to control access to your IP addresses.

Protection Policy	Section	Description
Fingerprint filtering	**Setting a Traffic Handling Policy Based on Fingerprint Features**	You can configure fingerprint filtering protection rules to match the content at a specified location within a data packet. Based on the matching result, you can set actions such as discarding, allowing, or rate limiting.
Port blocking	**Blocking Traffic to a Specified Port**	If a destination port is unnecessary for access, you can set up a port blocking policy to block traffic from reaching the port, thereby minimizing DDoS attack risks.
Protocol-based access block	**Blocking Traffic of a Specified Protocol**	You can block source traffic destined for the protected objects by protocol type. UDP, TCP, and ICMP protocols can be blocked.
Watermarking	**Using Watermarks to Defend Against CC Attacks**	CNAD supports the sharing of watermark algorithms and keys with the service end. All packets sent by the client are embedded with watermarks, which can effectively defend against layer-4 CC attacks.
Advanced protection	**Using Advanced Protection Policies to Restrict Abnormal Connections**	If an origin server IP address frequently sends a high volume of abnormal connection packets within a short period, you can set up an advanced protection policy to blacklist the origin server IP address for a certain period. Access from it can be restored once the blacklist period ends.
Geo-blocking	**Blocking Traffic From Specified Locations**	CNAD can block traffic from specified geographic regions. Once the policy is in effect, access traffic from the designated region will be discarded.

2.4.2 Configuring a Basic Protection Policy to Intercept Attack Traffic

After your service is connected to CNAD, you can set basic protection policies for the protected objects. If the DDoS bandwidth on an IP address exceeds the configured threshold, CNAD is triggered to scrub attack traffic to ensure service availability.

NOTICE

If the selected threshold does not align with the workloads, some attacks may not be properly defended against, or service traffic may be inaccurately scrubbed. Choose a value closest to the purchased bandwidth but not exceeding it.

Limitations and Constraints

If you have a custom policy, you cannot change the traffic scrubbing threshold. To change the traffic scrubbing threshold, **submit a service ticket** to Huawei technical support.

Enabling Basic Protection

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

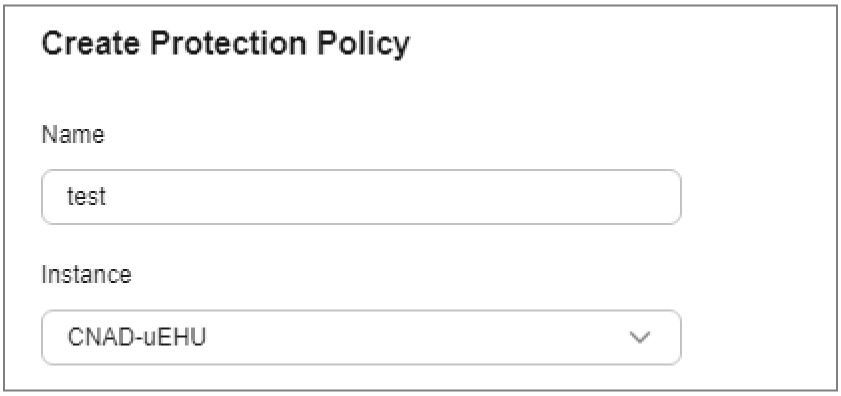
Step 2 Select a region in the upper part of the page, click ☰ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

Step 3 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced > Protection Policies**. The **Protection Policies** page is displayed.

Step 4 Click **Create Protection Policy**.

Step 5 In the displayed dialog box, set the policy name, select an instance, and click **OK**.

Figure 2-6 Creating a policy



Create Protection Policy

Name

test

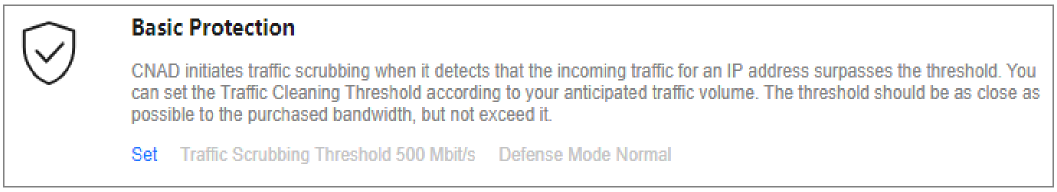
Instance

CNAD-uEHU

Step 6 In the row containing the target policy, click **Set Protection Policy** in the **Operation** column.

Step 7 In the **Basic Protection** area, click **Set**.

Figure 2-7 Basic protection



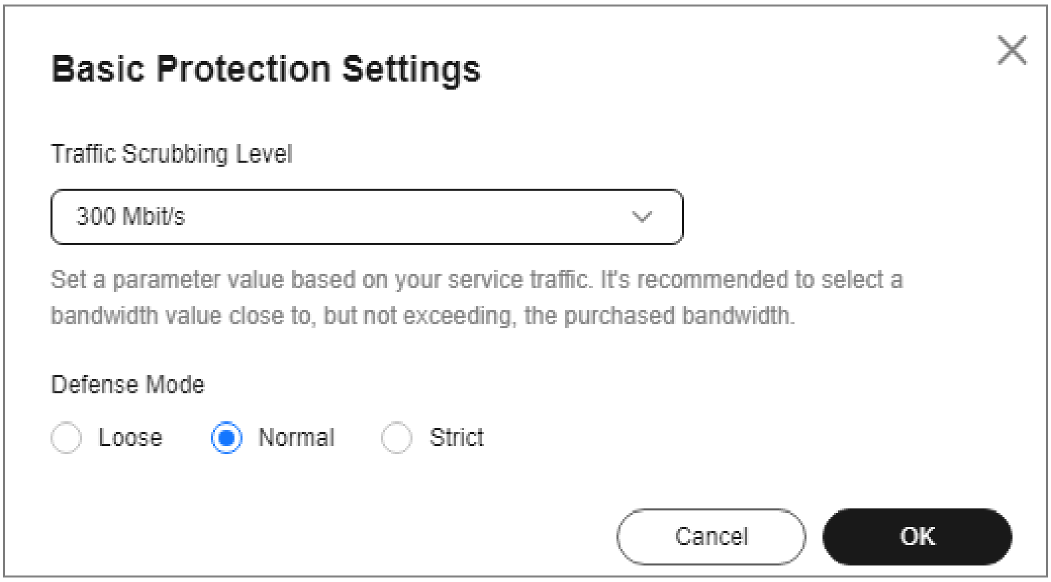
Basic Protection

CNAD initiates traffic scrubbing when it detects that the incoming traffic for an IP address surpasses the threshold. You can set the Traffic Cleaning Threshold according to your anticipated traffic volume. The threshold should be as close as possible to the purchased bandwidth, but not exceed it.

Set Traffic Scrubbing Threshold 500 Mbit/s Defense Mode Normal

Step 8 In the **Basic Protection Settings** dialog box that is displayed, set the traffic scrubbing threshold.

Figure 2-8 Basic protection settings



Basic Protection Settings

Traffic Scrubbing Level

300 Mbit/s

Set a parameter value based on your service traffic. It's recommended to select a bandwidth value close to, but not exceeding, the purchased bandwidth.

Defense Mode

○ Loose ● Normal ○ Strict

Table 2-10 Parameter description

Parameter	Description
Traffic Scrubbing Level	If the DDoS bandwidth on an IP address exceeds the configured scrubbing level, CNAD is triggered to scrub attack traffic. You are advised to set a value closest to, but not exceeding, the purchased bandwidth. **NOTE** The traffic scrubbing threshold should be selected based on the service bandwidth and is unrelated to protection policies. If the threshold is set significantly lower than the actual service bandwidth, false alarms may be generated. Conversely, if the threshold is set much higher than the actual service bandwidth, some attacks might not be effectively defended against. Therefore, it is recommended to choose a value as close as possible to the actual service bandwidth but not exceeding the purchased bandwidth.
Defense Mode	If the traffic reaches the specified scrubbing level, traffic scrubbing is triggered. ● Loose: Scrubbing is triggered when the traffic reaches three times the scrubbing level. This mode is recommended to mitigate the impact on services when traffic is incorrectly scrubbed. ● Normal: Scrubbing is triggered when the traffic reaches twice the scrubbing level. This mode is recommended for the default protection policy. ● Strict: Scrubbing is triggered when the traffic reaches the scrubbing level. This mode is recommended to enhance defense after there have been escaped attacks.

Step 9 Click **OK**. The basic protection policy configuration is completed.

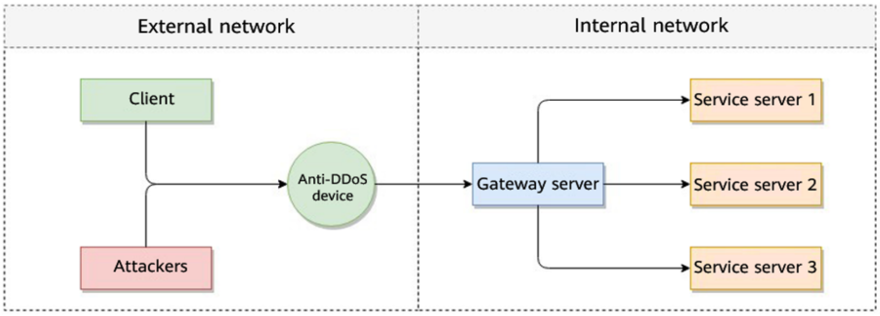
----End

2.4.3 Using Watermarks to Defend Against CC Attacks

CNAD supports the sharing of watermark algorithms and keys with the service end. All packets sent by the client are embedded with watermarks, which can effectively defend against layer-4 CC attacks.

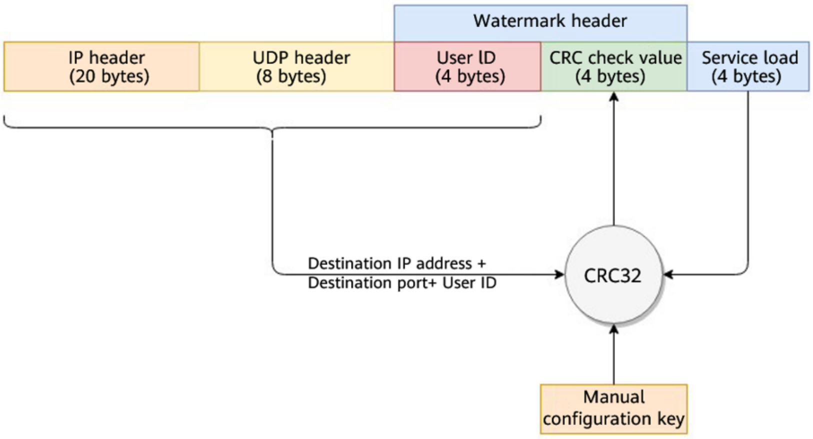
There are generally two modes of defending against UDP floods: dynamic fingerprint learning and UDP traffic limiting. The former may mistakenly learn normal service payloads as attack fingerprints, leading to false positives. The latter may block both normal and attack traffic, affecting your service.

Figure 2-9 Device protection principles



As shown in **Figure 2-10**, the Huawei cloud solution adds watermark header information to UDP packets to identify normal service packets. After receiving a UDP packet, the offline Anti-DDoS service device checks whether the UDP watermark is correct to efficiently and accurately permit normal service packets and block attack packets.

Figure 2-10 Watermarking solution



The client and Anti-DDoS device need to use the same information structure and calculation rule. The calculation rule refers to the hash factor and hash algorithm for calculating the watermark value. In this solution, the hash factor uses: the destination IP address, destination port, user identifier, and the watermark keyword; and the hash algorithm uses the CRC32.

Limitations and Constraints

- This function needs to be developed on the client. To use this function, **submit a service ticket**.
- Up to two keys can be configured for a watermark.

Enabling Watermark Protection

You can set a watermark protection policy on the console and configure watermarks on the client.

Setting the Watermark Protection Policy

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

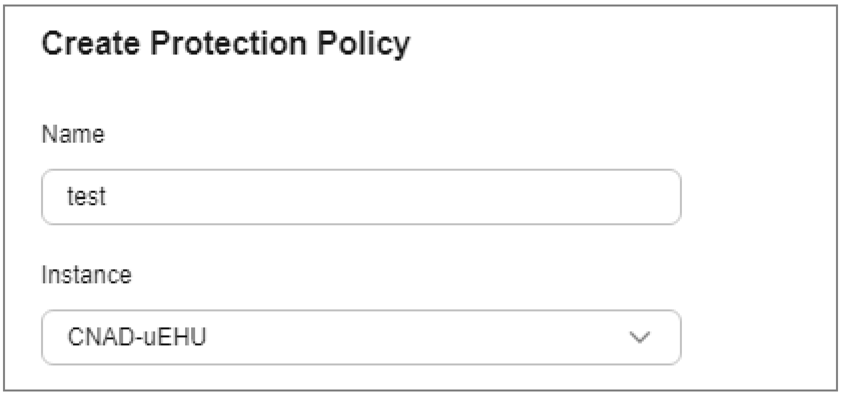
Step 2 Select a region in the upper part of the page, click ☰ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

Step 3 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced** > **Protection Policies**. The **Protection Policies** page is displayed.

Step 4 Click **Create Protection Policy**.

Step 5 In the displayed dialog box, set the policy name, select an instance, and click **OK**.

Figure 2-11 Creating a policy



Create Protection Policy

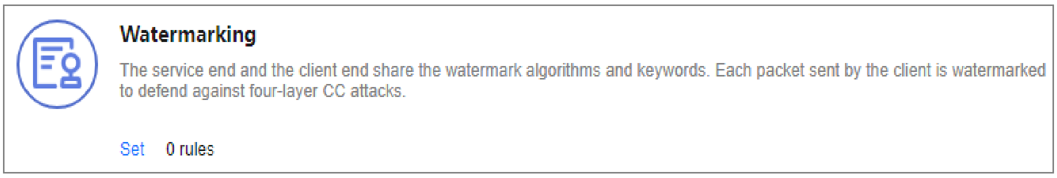
Name: test

Instance: CNAD-uEHU

Step 6 In the row containing the target policy, click **Set Protection Policy** in the **Operation** column.

Step 7 In the **Watermark** configuration area, click **Set**.

Figure 2-12 Watermarking



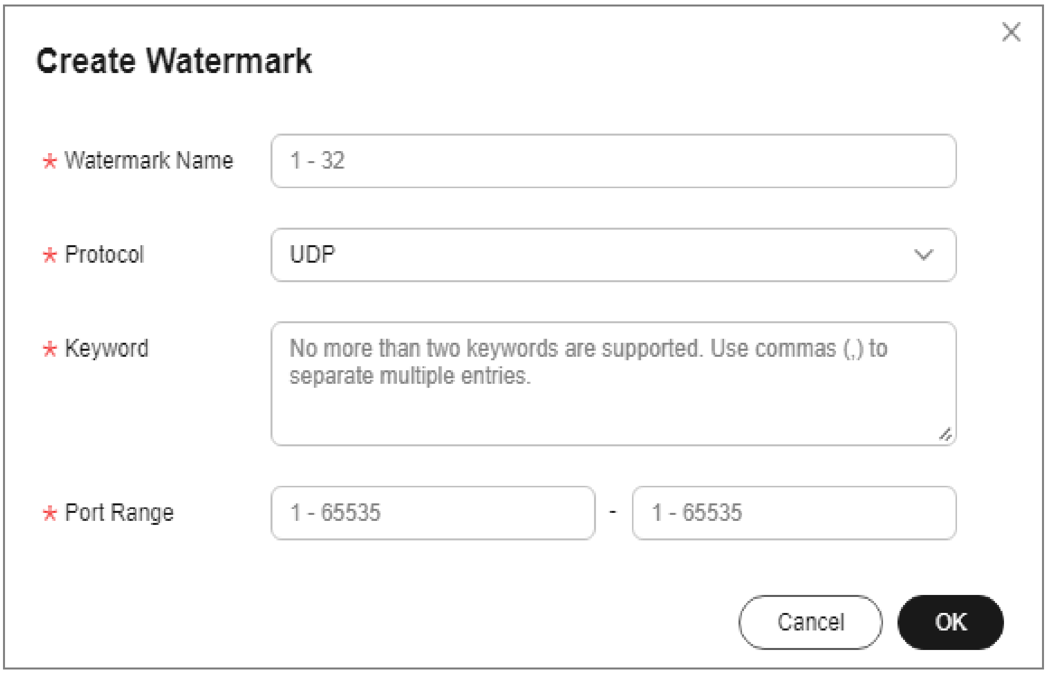
Watermarking

The service end and the client end share the watermark algorithms and keywords. Each packet sent by the client is watermarked to defend against four-layer CC attacks.

Step 8 On the displayed **Watermark Configuration** page, click **Create**.

Step 9 In the **Create Watermark** dialog box, set watermark parameters.

Figure 2-13 Create Watermark



Create Watermark

* Watermark Name: 1 - 32

* Protocol: UDP

* Keyword: No more than two keywords are supported. Use commas (,) to separate multiple entries.

* Port Range: 1 - 65535 - 1 - 65535

Table 2-11 Watermark parameters

Parameter	Description
Watermark Name	Watermark name
Protocol	Currently, only **UDP** is supported.
Key	Keyword. Up to two keywords are supported.
Port Range	The supported port number ranges from 1 to 65535.

Step 10 Click **OK**.

----End

Configuring Watermarks on the Client

This section uses the C language as an example to describe how to calculate and add UDP watermarks on the client. Developers can adjust the code based on the development platform.

Step 1 Initialize the CRC table:

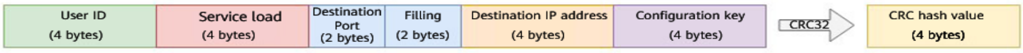
```
unsigned int g_szCRCTable[256];
void CRC32TableInit(void)
{
    unsigned int c;
    int n, k;
    for (n = 0; n < 256; n++) {
        c = (unsigned int)n;
        for (k = 0; k < 8; k++) {
            if (c & 1) {
                c = 0xedb88320 ^ (c >> 1);
            }
            else {
                c = c >> 1;
            }
        }
        g_szCRCTable[n] = c;
    }
}
```

Step 2 Interface for calculating the CRC hash value. The first parameter **crc** is set to **0** by default.

```
unsigned int CRC32Hash(unsigned int crc, unsigned char* buf, int len)
{
    unsigned int c = crc ^ 0xFFFFFFFF;
    int n;
    for (n = 0; n < len; n++) {
        c = g_szCRCTable[(c ^ buf[n]) & 0xFF] ^ (c >> 8);
    }
    return c ^ 0xFFFFFFFF;
}
```

Step 3 Example Code for Calculating the Watermark Value of a Packet **Figure 2-14** shows the watermark structure for compute

Figure 2-14 Watermark structure for compute



- The watermark data structure is defined as follows:

CAUTION

– The byte order needs to use the network byte order.

– If the service payload is less than four bytes, you can use 0s to fill it up.

```
typedef struct {
unsigned int userId; /*User ID*/
unsigned int payload; /*Service payload*/
unsigned short destPort; /*Service destination port*/
unsigned short rsv; /*Reserved field, 2-byte filling*/
unsigned int destIp; /*Service destination IP address*/
unsigned int key; /*Watermark keyword*/
} UdpWatermarkInfo;
```

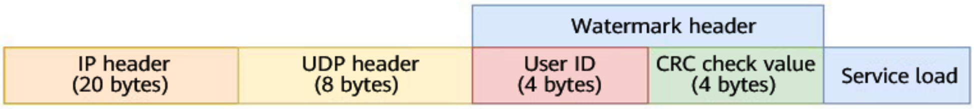
- The CPU hardware acceleration interface can be used to calculate the CRC hash value to improve the processing performance.

```
unsigned int UdpFloodWatermarkHashGet(unsigned int userId, unsigned int payload, unsigned short destPort, unsigned int destIp, unsigned int key)
{
    UdpWatermarkInfo stWaterInfo;

    stWaterInfo.destIp   = destIp;
    stWaterInfo.destPort = destPort;
    stWaterInfo.userId   = userId;
    stWaterInfo.payload  = payload;
    stWaterInfo.key      = key;
    stWaterInfo.rsv      = 0;
    return CRC32Hash(0, (UCHAR *)&stWaterInfo, sizeof(stWaterInfo));
}
```

Step 4 The packet is filled with the calculated CRC hash value according to the structure in **Figure 2-15** and then sent out.

Figure 2-15 Filling UDP Watermarks



----End

2.4.4 Blocking or Permitting Traffic From Specified IP Addresses Using a Blacklist and Whitelist

You can configure an access control list to control access to your IP addresses.

Limitations and Constraints

A maximum of 200 IP addresses can be added to the access control list for each policy.

Adding an IP Address to the Blacklist or Whitelist

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

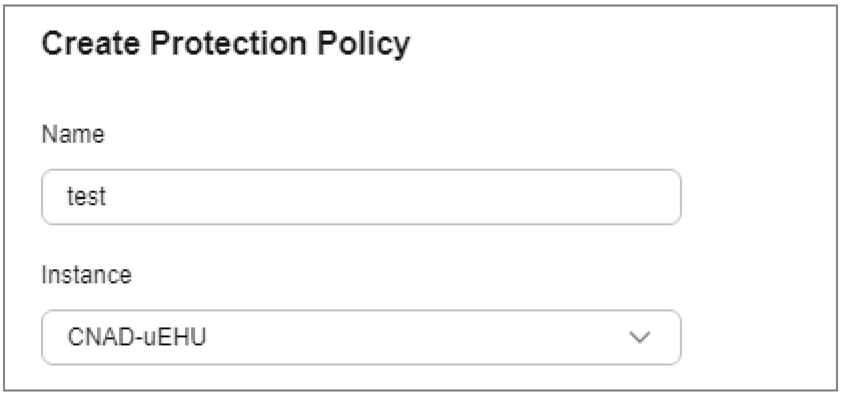
Step 2 Select a region in the upper part of the page, click ☰ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

Step 3 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced** > **Protection Policies**. The **Protection Policies** page is displayed.

Step 4 Click **Create Protection Policy**.

Step 5 In the displayed dialog box, set the policy name, select an instance, and click **OK**.

Figure 2-16 Creating a policy



Create Protection Policy

Name

test

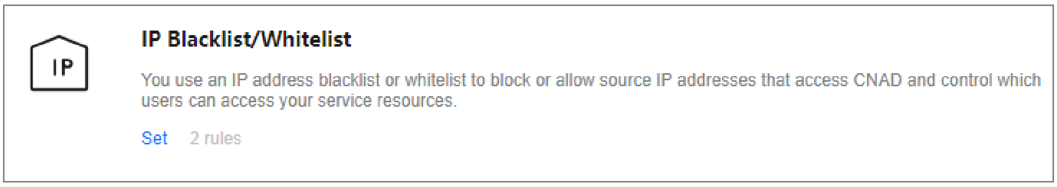
Instance

CNAD-uEHU

Step 6 In the row containing the target policy, click **Set Protection Policy** in the **Operation** column.

Step 7 In the **IP Blacklist/Whitelist** area, click **Set**.

Figure 2-17 IP Blacklist/Whitelist

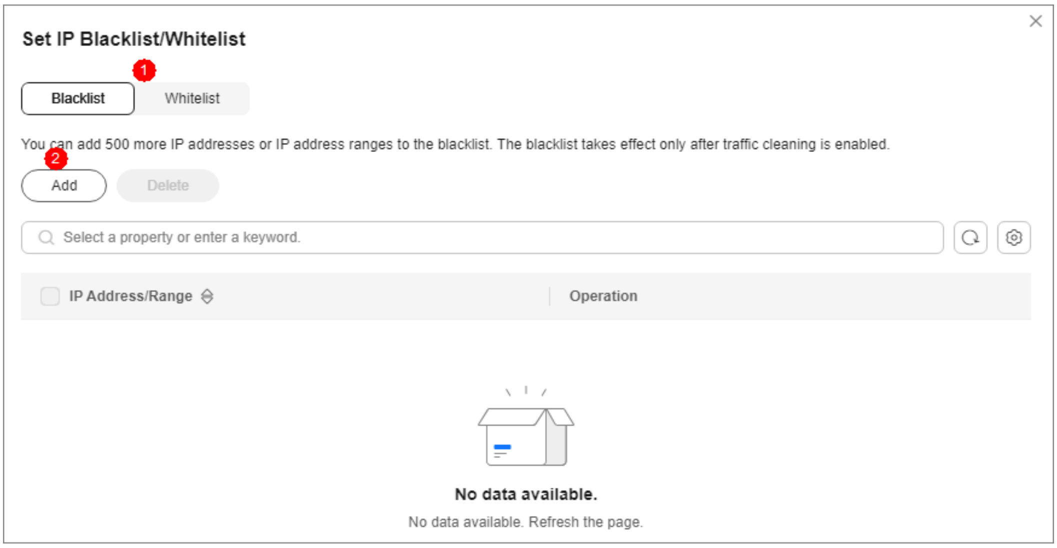


IP Blacklist/Whitelist

You use an IP address blacklist or whitelist to block or allow source IP addresses that access CNAD and control which users can access your service resources.

Step 8 On the displayed **Set IP Blacklist/Whitelist** page, choose **Blacklist** or **Whitelist** and click **Add**.

Figure 2-18 Add IP Address



Set IP Blacklist/Whitelist

You can add 500 more IP addresses or IP address ranges to the blacklist. The blacklist takes effect only after traffic cleaning is enabled.

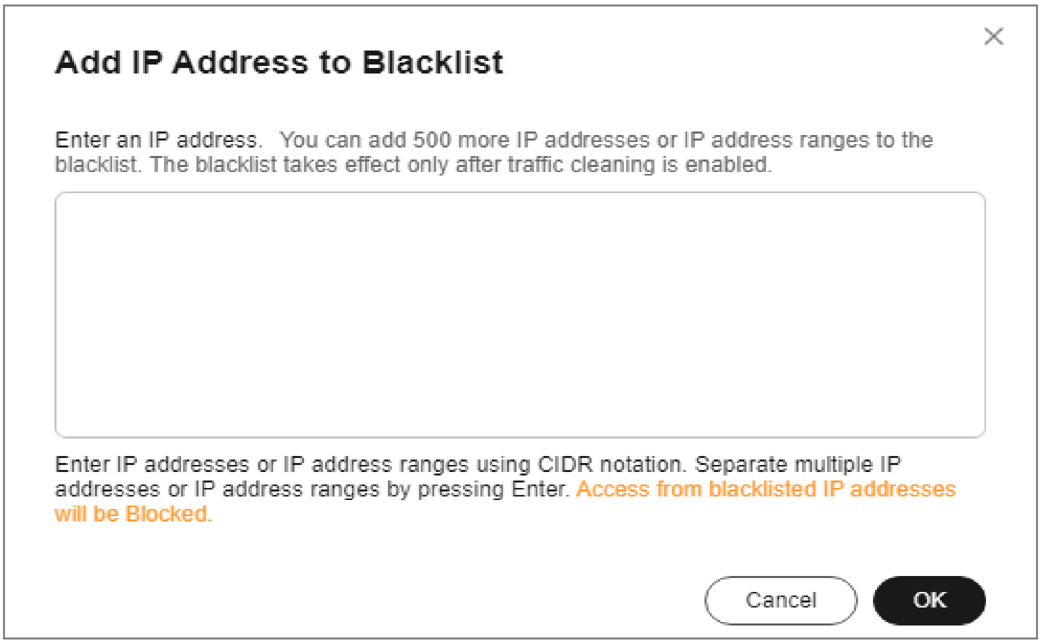
IP Address/Range	Operation

No data available.

No data available. Refresh the page.

Step 9 Enter the IP addresses or IP address ranges, and click **OK**.

Figure 2-19 Adding blacklist IP addresses

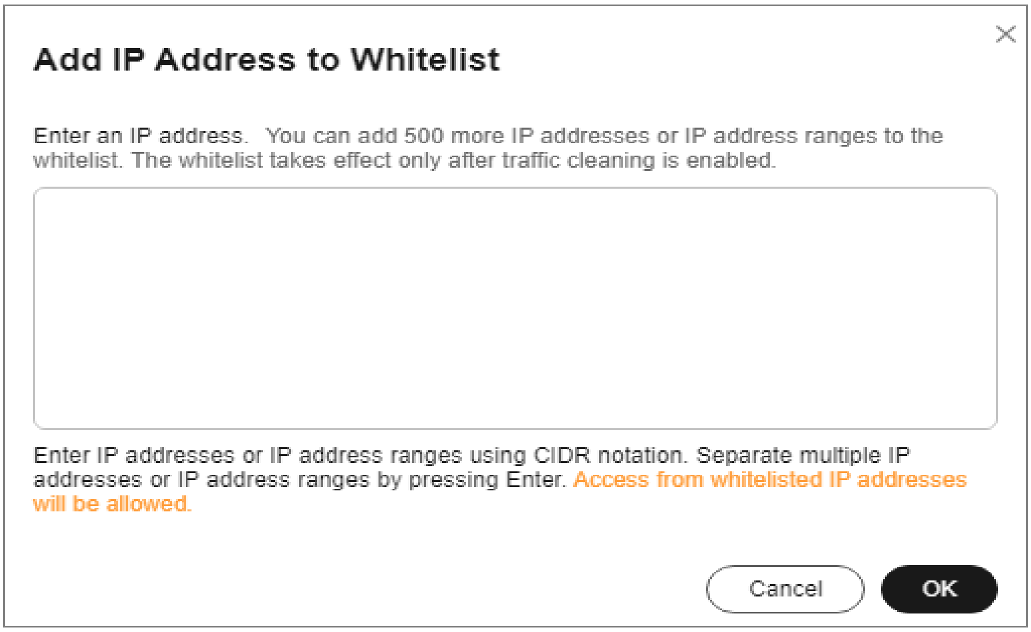


Add IP Address to Blacklist

Enter an IP address. You can add 500 more IP addresses or IP address ranges to the blacklist. The blacklist takes effect only after traffic cleaning is enabled.

Enter IP addresses or IP address ranges using CIDR notation. Separate multiple IP addresses or IP address ranges by pressing Enter. Access from blacklisted IP addresses will be Blocked.

Figure 2-20 Adding whitelist IP addresses



Add IP Address to Whitelist

Enter an IP address. You can add 500 more IP addresses or IP address ranges to the whitelist. The whitelist takes effect only after traffic cleaning is enabled.

Enter IP addresses or IP address ranges using CIDR notation. Separate multiple IP addresses or IP address ranges by pressing Enter. Access from whitelisted IP addresses will be allowed.

----End

Related Operations

- On the blacklist tab, click **Delete** in the **Operation** column of a target IP address or select IP addresses to be deleted in batches, and click **Delete** above the list. Access from the deleted IP addresses will not be blocked.
- On the whitelist tab, click **Delete** in the **Operation** column of a target IP address or select IP addresses to be deleted in batches, and click **Delete** above the list. Access from the deleted IP addresses will not be directly allowed.

2.4.5 Blocking Traffic to a Specified Port

If a destination port is unnecessary for access, you can set up a port blocking policy to block traffic from reaching the port, thereby minimizing DDoS attack risks.

Enabling Port Blocking

Step 1 Log in to the management console.

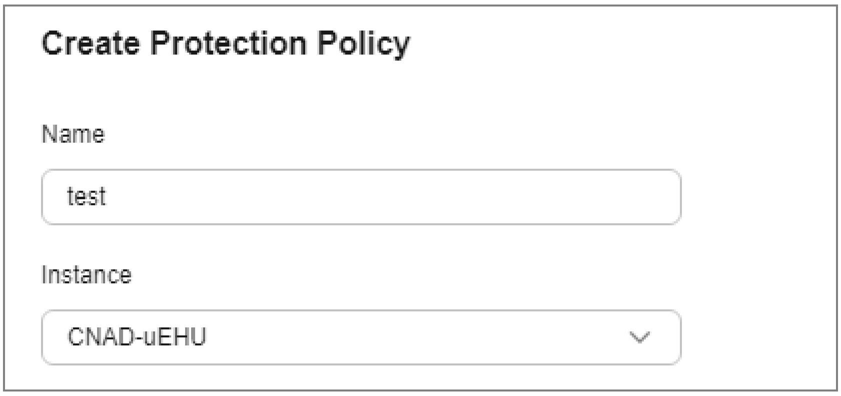
Step 2 Select a region in the upper part of the page, click ☰ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

Step 3 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced** > **Protection Policies**. The **Protection Policies** page is displayed.

Step 4 Click **Create Protection Policy**.

Step 5 In the displayed dialog box, set the policy name, select an instance, and click **OK**.

Figure 2-21 Creating a policy



Create Protection Policy

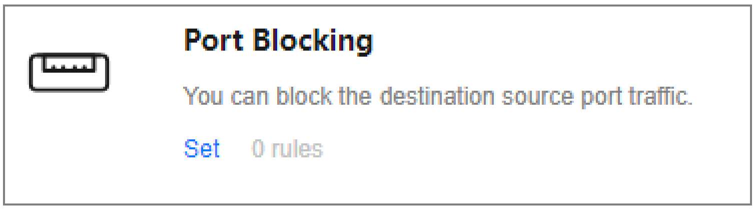
Name: test

Instance: CNAD-uEHU

Step 6 In the row containing the target policy, click **Set Protection Policy** in the **Operation** column.

Step 7 In the **Port Blocking** configuration area, click **Set**.

Figure 2-22 Port blocking configuration box



Port Blocking

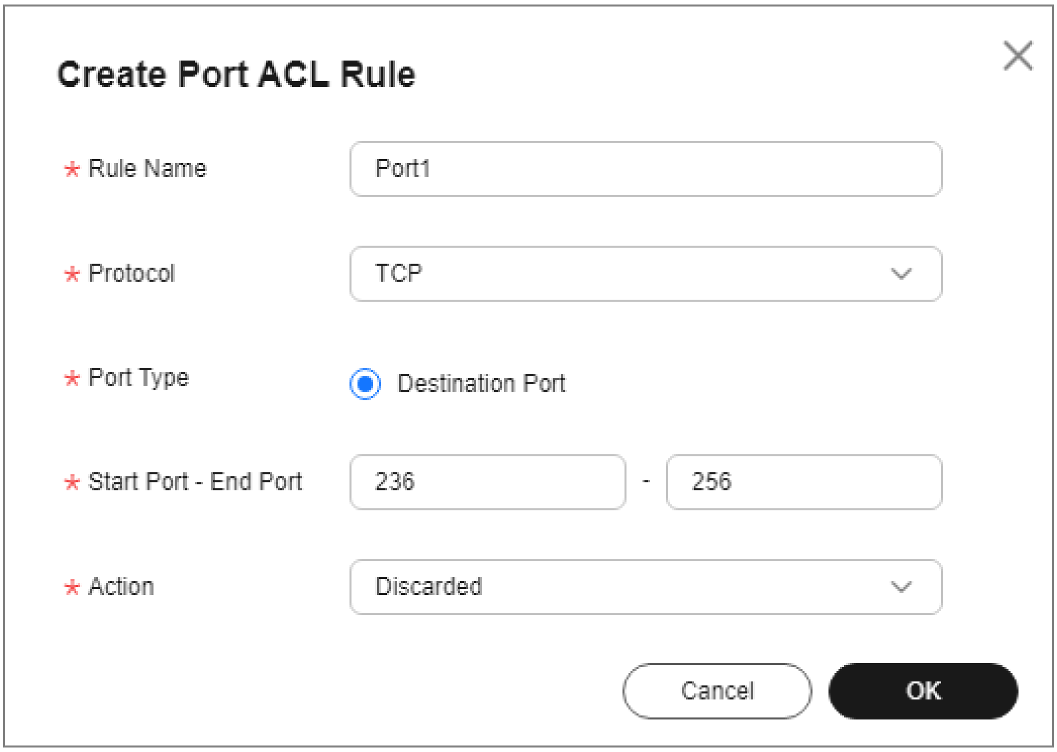
You can block the destination source port traffic.

Set 0 rules

Step 8 In the **Port Blocking** dialog box, click **Create Port ACL Rule**.

Step 9 In the dialog box that is displayed, set the port ACL.

Figure 2-23 Creating a port ACL rule



Create Port ACL Rule

* Rule Name: Port1

* Protocol: TCP

* Port Type: ● Destination Port

* Start Port - End Port: 236 - 256

* Action: Discarded

Table 2-12 Port ACL parameters

Parameter	Description
Rule Name	Enter a rule name.
Protocol	Protocol of the port to be blocked TCP and UDP are supported.
Port Type	Only **Destination Port** is supported.
Start Port-End Port	Set the range of ports to be blocked.
Action	Protection action after the port is blocked **Discard**: Discard traffic destined for the port.

Step 10 Click **OK**.

----End

Follow-up Procedure

- Locate the row that contains the target port and click **Delete** in the **Operation** column to delete the port blocking rule.
- Locate the row that contains the target port and click **Edit** in the **Operation** column to edit the port blocking rule.

2.4.6 Blocking Traffic of a Specified Protocol

After protocol blocking is enabled, the system limits the rate of traffic destined for Anti-DDoS Service objects based on the protocol type. This feature supports protocols such as UDP, TCP, and ICMP.

For details about the rate limit thresholds for different protocols, see **Table 2-13**.

Table 2-13 Rate Limit (pps)

Protocol Type	Rate Limit (pps)
UDP	10Mbps
TCP	10Mbps
ICMP	100pps
Other (other protocols)	10Mbps

Enabling Protocol Blocking

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

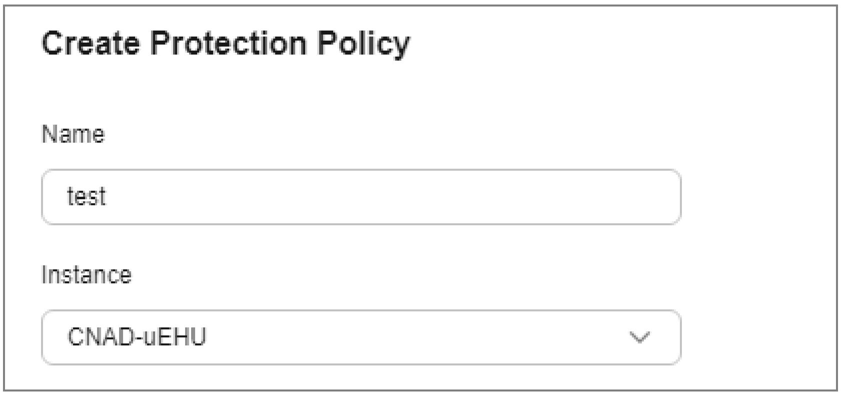
Step 2 Select a region in the upper part of the page, click ☰ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

Step 3 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced > Protection Policies**. The **Protection Policies** page is displayed.

Step 4 Click **Create Protection Policy**.

Step 5 In the displayed dialog box, set the policy name, select an instance, and click **OK**.

Figure 2-24 Creating a policy



Create Protection Policy

Name

test

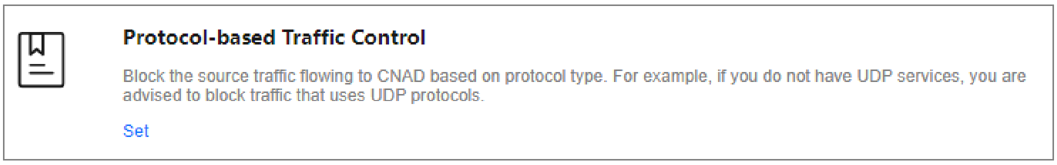
Instance

CNAD-uEHU

Step 6 In the row containing the target policy, click **Set Protection Policy** in the **Operation** column.

Step 7 In the **Protocol-based Traffic Control** area, click **Set**.

Figure 2-25 Protocol-based Traffic Control

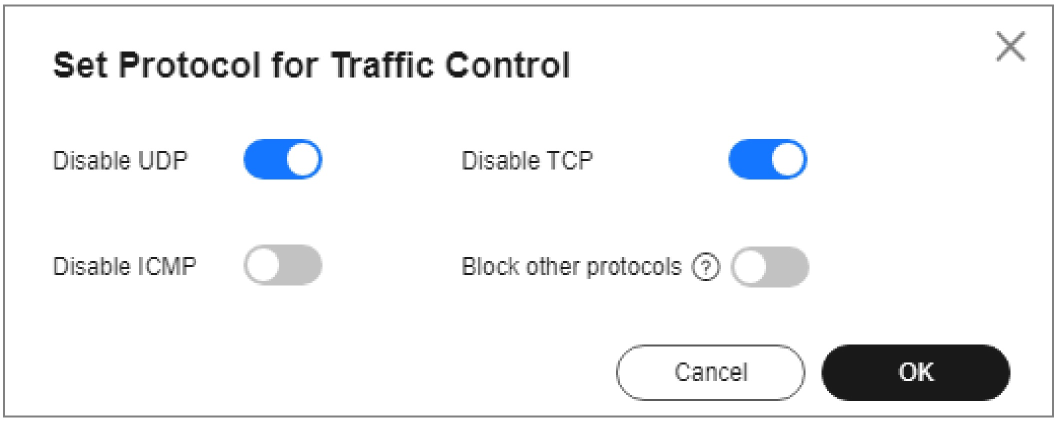


Protocol-based Traffic Control

Block the source traffic flowing to CNAD based on protocol type. For example, if you do not have UDP services, you are advised to block traffic that uses UDP protocols.

Step 8 In the displayed **Set Protocol for Traffic Control** dialog box, enable or disable traffic control, and click **OK**.

Figure 2-26 Setting protocol blocking



Set Protocol for Traffic Control

Disable UDP: ●

Disable TCP: ●

Disable ICMP: ○

Block other protocols: ○

- ● indicates that traffic of the protocol type is blocked.
- ○ indicates that traffic of the protocol type is allowed.

----End

2.4.7 Setting a Traffic Handling Policy Based on Fingerprint Features

You can configure a fingerprint filtering rule to match the content of a specified location in a data packet.

You can set actions for matched traffic, such as discarding, allowing, and rate limiting.

Enabling Fingerprint Filtering

Step 1 Log in to the management console.

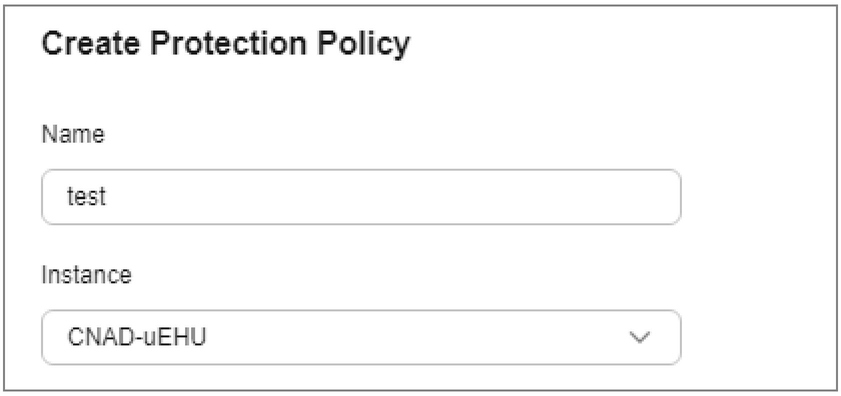
Step 2 Select a region in the upper part of the page, click ☰ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

Step 3 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced > Protection Policies**. The **Protection Policies** page is displayed.

Step 4 Click **Create Protection Policy**.

Step 5 In the displayed dialog box, set the policy name, select an instance, and click **OK**.

Figure 2-27 Creating a policy



Create Protection Policy

Name

test

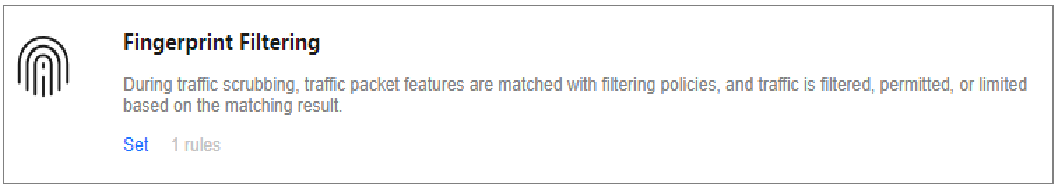
Instance

CNAD-uEHU

Step 6 In the row containing the target policy, click **Set Protection Policy** in the **Operation** column.

Step 7 In the **Fingerprint Filtering** configuration area, click **Set**.

Figure 2-28 Fingerprint filtering configuration box



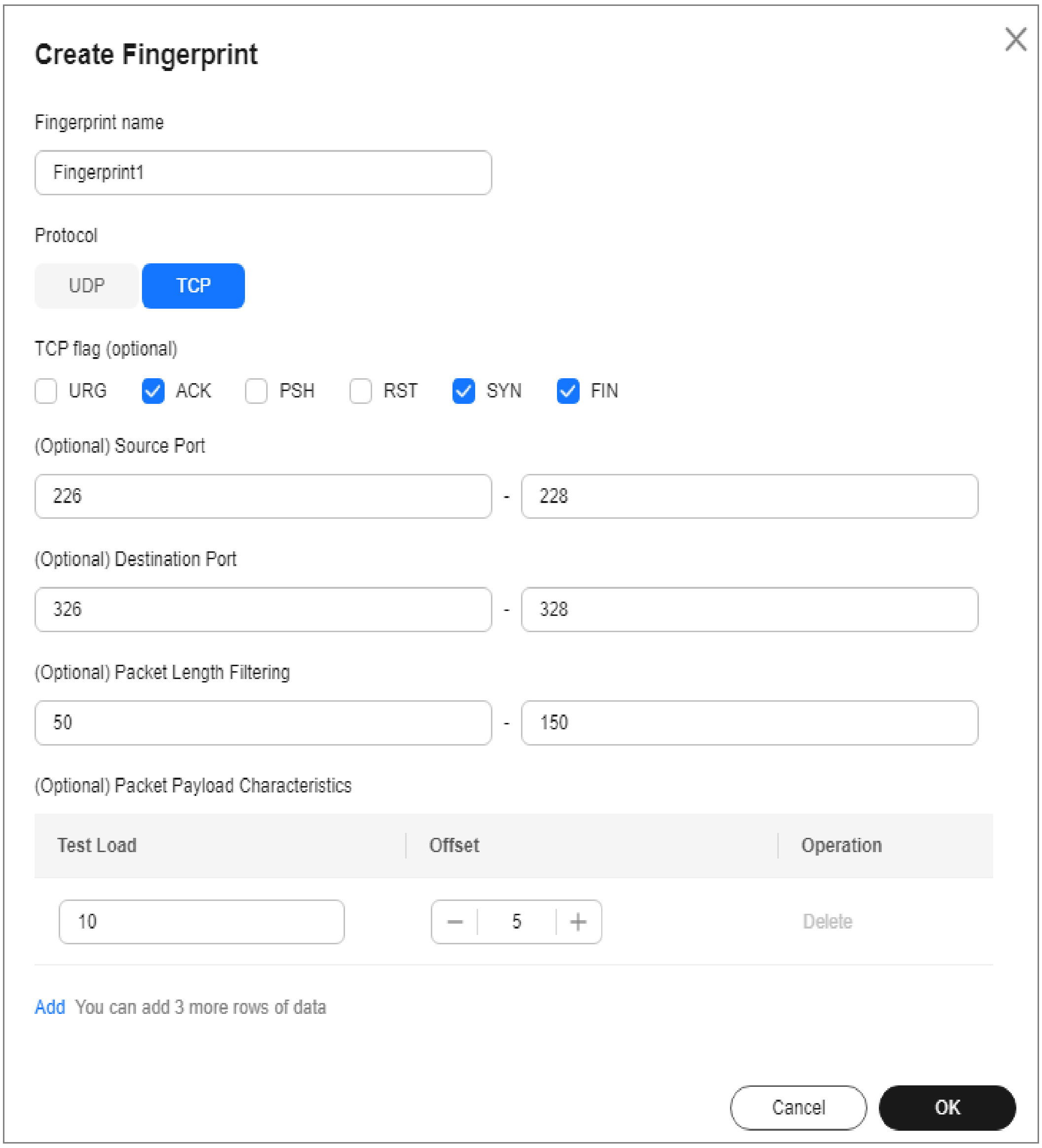
Fingerprint Filtering

During traffic scrubbing, traffic packet features are matched with filtering policies, and traffic is filtered, permitted, or limited based on the matching result.

Step 8 In the displayed **Fingerprint Filtering Settings** dialog box, click **Create Fingerprint**.

Step 9 In the displayed dialog box, set fingerprint parameters.

Figure 2-29 Creating a fingerprint



Create Fingerprint

Fingerprint name: Fingerprint1

Protocol: UDP [✓ TCP]

TCP flag (optional): □ URG ☑ ACK □ PSH □ RST ☑ SYN ☑ FIN

(Optional) Source Port: 226 - 228

(Optional) Destination Port: 326 - 328

(Optional) Packet Length Filtering: 50 - 150

(Optional) Packet Payload Characteristics

Test Load	Offset	Operation
10	5	Delete

Add You can add 3 more rows of data

Table 2-14 Fingerprint parameters

Parameter	Description
Fingerprint Name	Enter the fingerprint rule name.
Protocol	Set the fingerprint protocol. The value can be **UDP** or **TCP**.
Source Port	Range of the fingerprint source port.
Destination Port	Range of the fingerprint destination port.
Packet Length Filtering	Length of the traffic packet to be filtered out.

Parameter	Description
Packet Payload Characteristics	● **Test Load**: Set the hexadecimal value of the detection payload. ● **Offset**: Set the offset of the fingerprint. For instance, if the test load is **1234afee** and the offset is **20**, and the content from the 21st to 32nd bytes of the data area matches **1234afee**, the packet is considered to match the fingerprint.
Action	Set the response action for matched traffic. ● **Allow**: Allow traffic through. ● **Discard**: Discard traffic. ● **Rate limiting (source)**: Requests from a specific source are limited. For example, if traffic from an IP address (or user) exceeds the rate limit you configured in this rule, CNAD will limit the traffic rate. ● **Allow & whitelist**: Allow the traffic and add the fingerprint feature to the whitelist. ● **Discard & blacklist**: Discard the traffic and add the fingerprint feature to the blacklist. ● **Rate Limit**: Limits the traffic access rate.

Step 10 Click **OK**.

----End

Follow-up Procedure

- Locate the row that contains the target port and click **Delete** in the **Operation** column to delete the fingerprint filtering rule.
- Locate the row that contains the target port, click **Edit** in the **Operation** column to modify the fingerprint filtering rule.

2.4.8 Using Advanced Protection Policies to Restrict Abnormal Connections

If an origin server IP address frequently sends a high volume of abnormal connection packets within a short period, you can set up an advanced protection policy to blacklist the origin server IP address for a certain period. Access from it can be restored once the blacklist period ends.

Limitations and Constraints

The advanced protection function is still in the open beta test (OBT) phase. This function is supported only by Unlimited Protection Advanced Edition instances in some regions. You can **submit a service ticket** to enable this function.

Enabling Advanced Protection

Step 1 Log in to the management console.

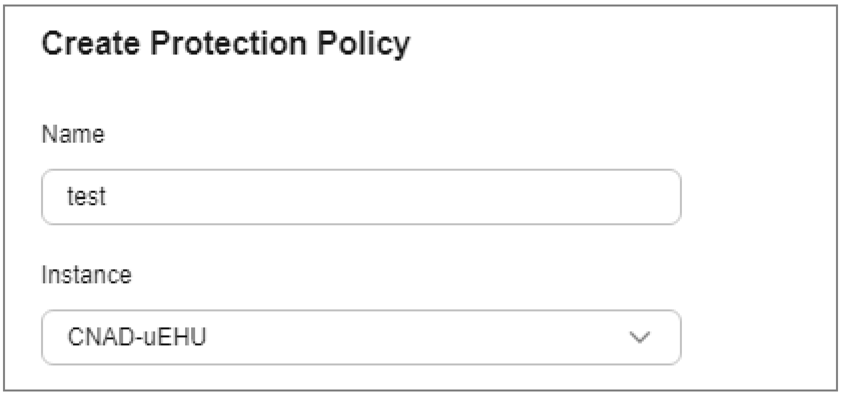
Step 2 Select a region in the upper part of the page, click ☰ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

Step 3 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced > Protection Policies**. The **Protection Policies** page is displayed.

Step 4 Click **Create Protection Policy**.

Step 5 In the displayed dialog box, set the policy name, select an instance, and click **OK**.

Figure 2-30 Creating a policy



Create Protection Policy

Name

test

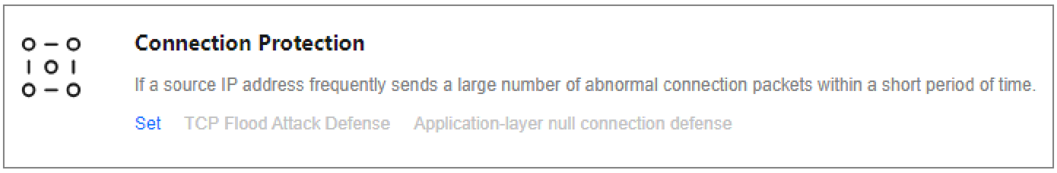
Instance

CNAD-uEHU

Step 6 In the row containing the target policy, click **Set Protection Policy** in the **Operation** column.

Step 7 In the **Connection Protection** area, click **Set**.

Figure 2-31 Advanced protection



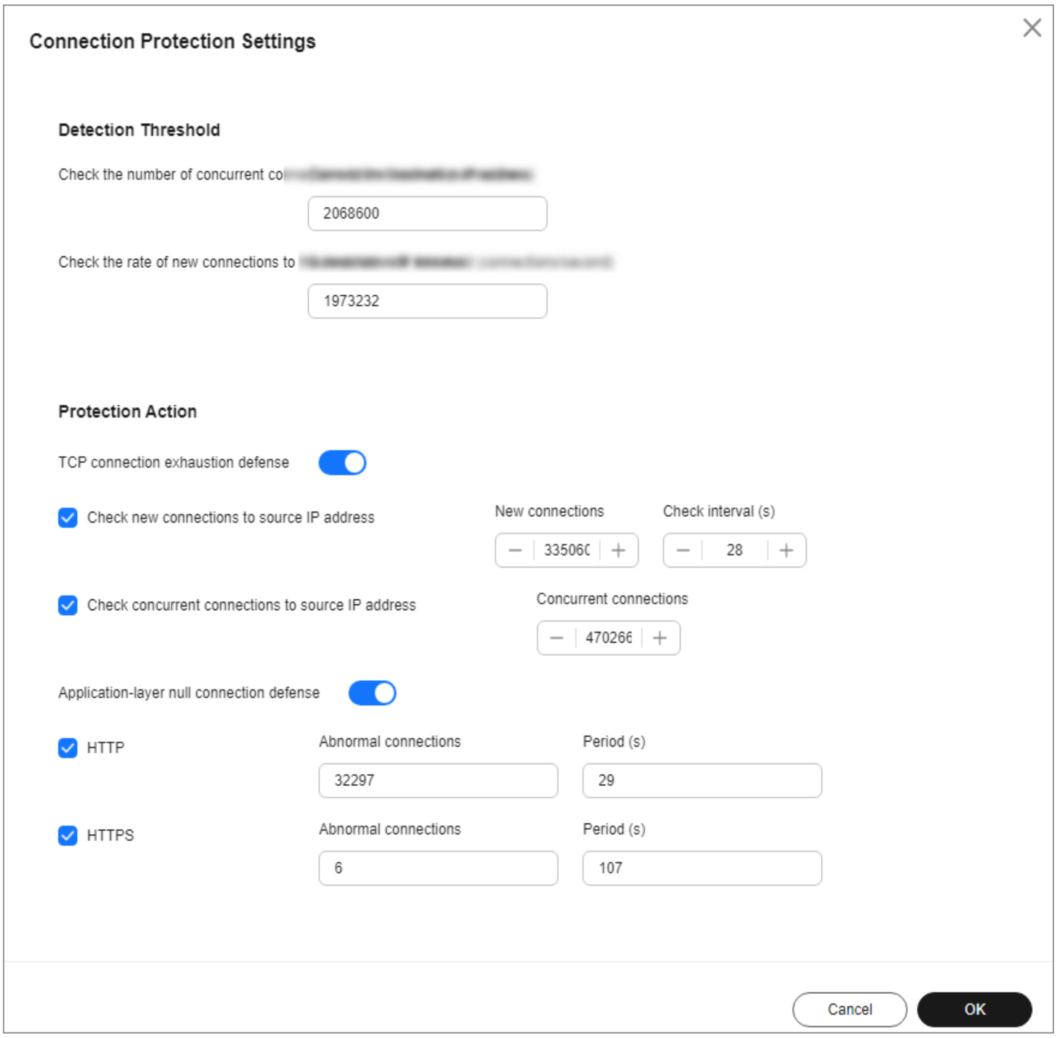
Connection Protection

If a source IP address frequently sends a large number of abnormal connection packets within a short period of time.

Set TCP Flood Attack Defense Application-layer null connection defense

Step 8 Set protection parameters as required.

Figure 2-32 Connection protection settings



Connection Protection Settings

Detection Threshold

Check the number of concurrent co[redacted]

2068600

Check the rate of new connections to [redacted]

1973232

Protection Action

TCP connection exhaustion defense ●

☑ Check new connections to source IP address — New connections: 33506(— Check interval (s): 28

☑ Check concurrent connections to source IP address — Concurrent connections: 47026€

Application-layer null connection defense ●

☑ HTTP — Abnormal connections: 32297 — Period (s): 29

☑ HTTPS — Abnormal connections: 6 — Period (s): 107

Table 2-15 Parameter description

Type	Parameter	Description
Detection Threshold	Check the number of concurrent connections to the destination IP address.	When the number of the concurrent TCP connections of a destination IP address exceeds **Threshold**, defense against connection flood attacks is started. After the defense is started, the source IP address starts to be checked.
	Check the rate of new connections to the destination IP address.	When the number of the new TCP connections per second of a destination IP address exceeds the **Detection Threshold**, defense against connection flood attacks is started. After the defense is started, the source IP address starts to be checked.

Type	Parameter	Description
Protection Action	TCP connection exhaustion defense	After **TCP connection exhaustion defense** is enabled, the following parameters can be set: ● **Check new connections to source IP address**: The system checks for new connections to the source IP address at regular intervals. If the number of new connections exceeds the specified threshold within the specified interval, the origin server's IP address is blocked until the block period ends. ● **Check concurrent connections to source IP address**: If the number of concurrent TCP connections from an IP address exceeds the specified threshold, the IP address is temporarily blocked. Access resumes once the block period ends.
	Application-layer null connection defense	After **Application-layer null connection defense** is enabled, you can set the following parameters: ● **HTTP**: The system monitors HTTP connections for each source IP address. If the number of connections exceeds the specified threshold, the system blocks access from that IP address by adding it to the blacklist. Access is automatically restored when the block period ends. ● **HTTPS**: The system monitors HTTPS connections for each source IP address. If the number of connections exceeds the specified threshold, the system blocks access from that IP address by adding it to the blacklist. Access is automatically restored when the block period ends.

Step 9 Click **OK**.

----End

2.4.9 Blocking Traffic From Specified Locations

CNAD allows you to configure a policy to block traffic from outside China. After the policy takes effect, access traffic from outside China will be discarded.

The conditions for a policy to take effect vary according to product editions. For details, see **Table 2-16**.

Table 2-16 Geo-blocking policy effective conditions

Edition	Geo-Blocking Policy Effective Condition
Unlimited Protection Basic Edition	The policy takes effect once it is enabled and an attack is detected.
Unlimited Protection Advanced Edition	The policy takes effect after being enabled.
CNAD 2.0	● Dedicated EIPs: The policy takes effect after being enabled. ● Common EIPs: The policy takes effect once it is enabled and an attack is detected.

Limitations and Constraints

- This function is in the internal test phase and is available only to some users. If you want to use it, **submit a service ticket**.
- Currently, only **Locations outside China** can be blocked.

Geo-Blocking

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

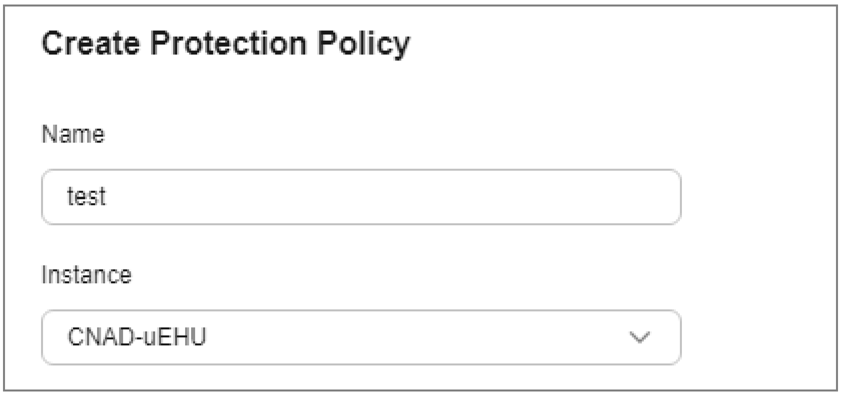
Step 2 Select a region in the upper part of the page, click ☰ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

Step 3 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced > Protection Policies**. The **Protection Policies** page is displayed.

Step 4 Click **Create Protection Policy**.

Step 5 In the displayed dialog box, set the policy name, select an instance, and click **OK**.

Figure 2-33 Creating a policy



Create Protection Policy

Name

test

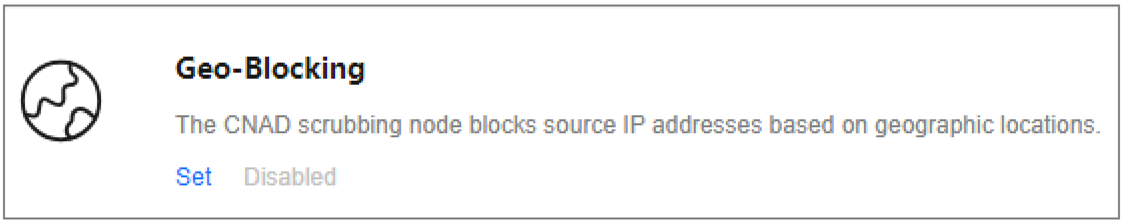
Instance

CNAD-uEHU

Step 6 In the row containing the target policy, click **Set Protection Policy** in the **Operation** column.

Step 7 In the **Geo-Blocking** configuration area, click **Set**.

Figure 2-34 Geo-blocking settings

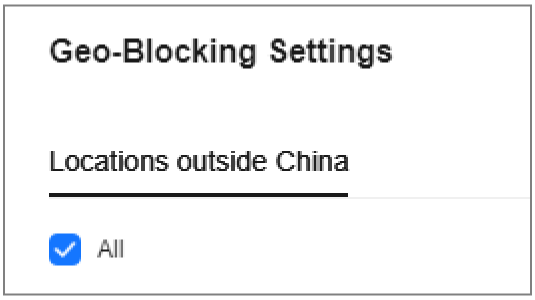


Geo-Blocking

The CNAD scrubbing node blocks source IP addresses based on geographic locations.

Step 8 In the dialog box that is displayed, select the locations to be blocked.

Figure 2-35 Select blocked locations



Geo-Blocking Settings

☑ All

Step 9 Click **OK**. The geo-blocking setting is complete.

----End

2.5 Adding a Protected Object

After enabling CNAD, you need to add public IP addresses on Huawei Cloud as protected objects to enable protection for these public IP addresses.

Limitations and Constraints

- The added protected objects (such as ECS, ELB, WAF, and EIP) must be in the same region as the region of the purchased CNAD instance.
- Unlimited Protection Advanced Edition can protect only dedicated EIPs. Cloud Native Anti-DDoS 2.0 can protect both common and dedicated EIPs.
- Cloud Native Anti-DDoS 2.0 outside the Chinese mainland can only protect premium BGP IP addresses 49.0.236.0/22, 49.0.234.0/23, and 49.0.233.0/24.

Prerequisites

A protection policy has been created. For details, see **Adding a Protection Policy**.

Adding Protected Objects to an Instance

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

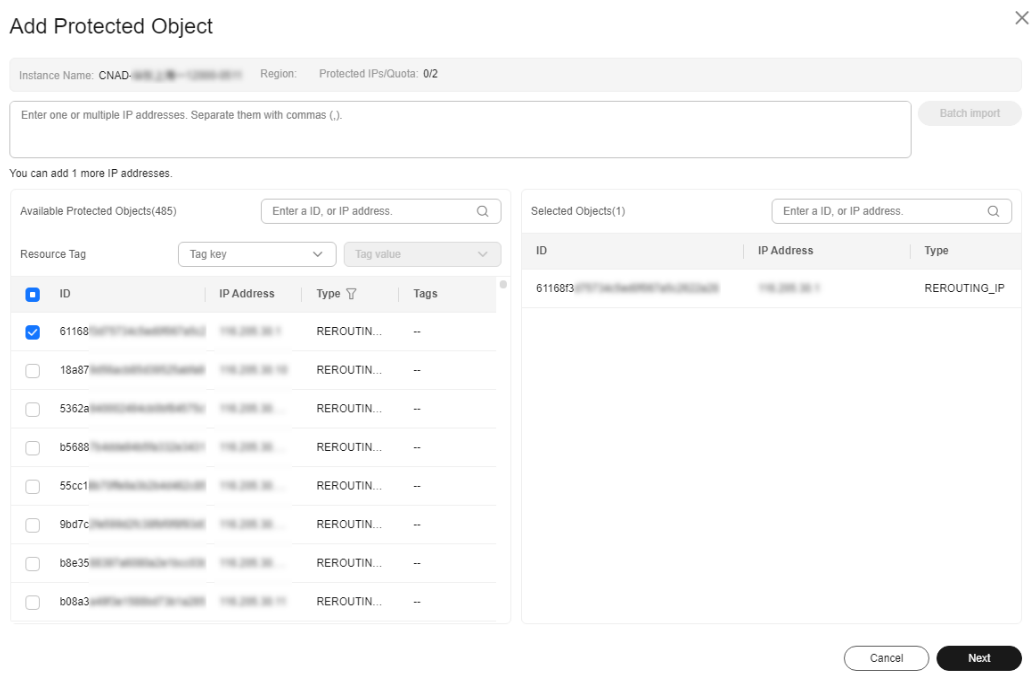
Step 2 Select a region in the upper part of the page, click ☰ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

Step 3 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced > Instances**. The **Instances** page is displayed.

Step 4 In the target instance, click **Set Protected Objects**.

Step 5 In the **Add Protected Object** dialog box that is displayed, select the IP addresses you want to protect and click **Next**.

Figure 2-36 Adding a protected object



Add Protected Object

Instance Name: CNAD-[redacted] Region: Protected IPs/Quota: 0/2

Enter one or multiple IP addresses. Separate them with commas (,).

Batch import

You can add 1 more IP addresses.

Available Protected Objects(485)

Enter a ID, or IP address.

Resource Tag: Tag key, Tag value

■	ID	IP Address	Type	Tags
☑	61168[redacted]	[redacted]	REROUTIN...	--
□	18a87[redacted]	[redacted]	REROUTIN...	--
□	5362a[redacted]	[redacted]	REROUTIN...	--
□	b5688[redacted]	[redacted]	REROUTIN...	--
□	55cc1[redacted]	[redacted]	REROUTIN...	--
□	9bd7c[redacted]	[redacted]	REROUTIN...	--
□	b8e35[redacted]	[redacted]	REROUTIN...	--
□	b08a3[redacted]	[redacted]	REROUTIN...	--

Selected Objects(1)

Enter a ID, or IP address.

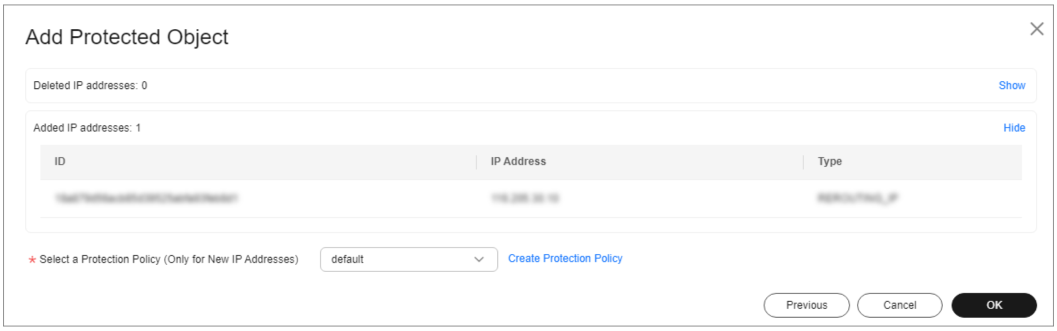
ID	IP Address	Type
61168f3[redacted]	[redacted]	REROUTING_IP

NOTE

- **Available Protected Objects** are the IP addresses available to be added.
- Batch import of protected IP addresses is supported.

Step 6 Confirm the settings of the protected objects, select an IP protection policy, and click **OK**.

Figure 2-37 Confirming protected object settings



Add Protected Object

Deleted IP addresses: 0 Show

Added IP addresses: 1 Hide

ID	IP Address	Type
[redacted]	[redacted]	[redacted]

* Select a Protection Policy (Only for New IP Addresses): default

NOTE

For details about how to set protection policies, see **Adding a Protection Policy**.

----End

Related Operations

- **Viewing protected objects**: In the instance box, click **View** next to **Protected IPs** to view the protected objects of the current instance.
- **Deleting protected objects**: Deselect the protected objects to be deleted on the protected objects settings page.
- **Configuring a tag**: In the **Tag** column of the row containing the target object, click ✎. Enter the tag name and click **OK**.

2.6 Enabling Alarm Notifications for DDoS Attacks

After you enable alarm notifications, a notification message will be sent to you (through the method you have configured) when an IP address is under DDoS attacks.

Limitations and Constraints

Notification topics are available only in CN North-Beijing4 and CN-Hong Kong.

Prerequisites

Before enabling alarm notification, **create a topic** and **add a subscription to the topic** in SMN.

NOTE

You will be billed for using the Simple Message Notification (SMN) service. For billing details, see **Product Pricing Details**.

Enabling Alarm Notifications

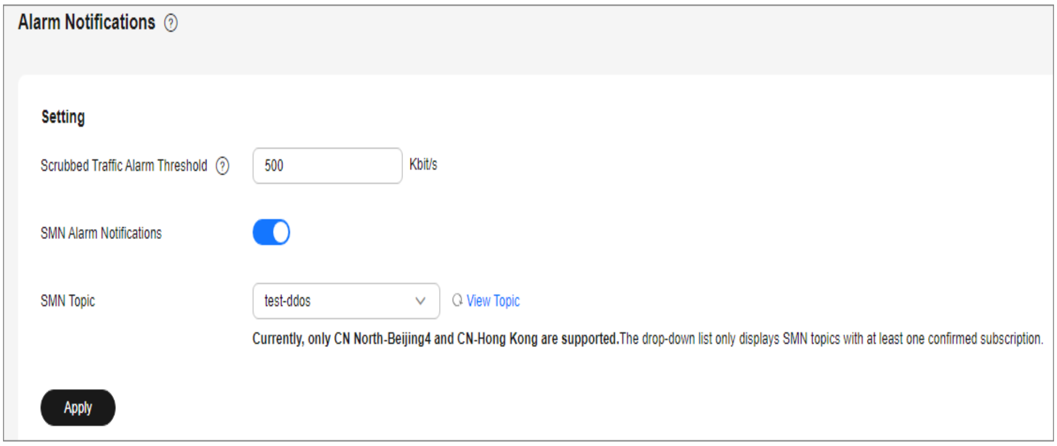
Step 1 **Log in to the management console**.

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

Step 3 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced** > **Alarm Notifications**. The **Alarm Notifications** page is displayed.

Step 4 On the **Alarm Notifications** page, configure alarm notifications. **Table 2-17** describes related parameters.

Figure 2-38 Configuring alarm notifications



Alarm Notifications

Setting

Scrubbed Traffic Alarm Threshold: 500 Kbit/s

SMN Alarm Notifications: enabled

SMN Topic: test-ddos

View Topic

Currently, only CN North-Beijing4 and CN-Hong Kong are supported.The drop-down list only displays SMN topics with at least one confirmed subscription.

Apply

Table 2-17 Configuring alarm notifications

Parameter	Description
Scrubbed Traffic Alarm Threshold	When the volume of scrubbed traffic reaches the threshold, an alarm notification is sent. Set the threshold as required.
Alarm Notifications	Indicates whether the alarm notification function is enabled. There are two values: - : enabled - : disabled
SMN Topic	You can select an existing topic or click **View Topic** to create a topic. For more information about SMN topics, see **Simple Message Notification User Guide**.

Step 5 Click **Apply**.

----End

Related Operations

To disable alarm notifications, set the button in **Figure 2-38** to .

2.7 Enabling Logging

After you authorize CNAD to access Log Tank Service (LTS), you can use the Anti-DDoS logs recorded by LTS for quick and efficient real-time analysis, device O&M management, and analysis of service trends.

Prerequisites

LTS has been enabled. For details, see **Managing Log Groups** and **Managing Log Streams**.

Enabling LTS

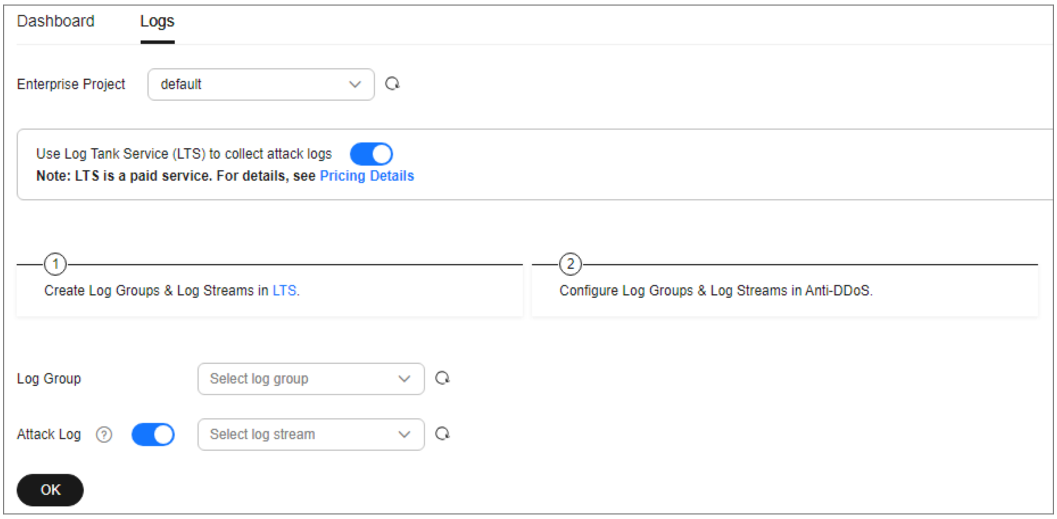
Step 1 **Log in to the management console**.

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

Step 3 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced** > **Dashboard**. The **Data Reports** page is displayed.

Step 4 Click the **Logs** tab, toggle on , and select the log group and log stream. **Figure 2-39** describes related parameters.

Figure 2-39 Configuring logs



Dashboard Logs

Enterprise Project: default

Use Log Tank Service (LTS) to collect attack logs

Note: LTS is a paid service. For details, see Pricing Details

1 Create Log Groups & Log Streams in LTS.

2 Configure Log Groups & Log Streams in Anti-DDoS.

Log Group: Select log group

Attack Log: Select log stream

OK

Table 2-18 Log parameters

Parameter	Description
Enterprise Project	Select an enterprise project.
Log Group	Select a log group or click **View Log Group** to go to the LTS console and create a log group.
Attack Log	After this option is enabled, you can set: Select a log stream or click **View Log Stream** to go to the LTS console and create a log stream. An attack log includes information about event type, protective action, and attack source IP address of each attack.

Step 5 Click **OK**.

You can view protection logs of CNAD on the LTS console.

----End

Log Fields in LTS

This section describes the fields of CNAD logs.

Table 2-19 Key fields

Field	Description
currentConn	Current Connections
maxInPps	Peak rate of incoming packets, in pps.
newConn	New connections
deviceType	Type of the device that reports logs. The default value is **CLEAN**, indicating the scrubbing device.
attackTypes	Attack type. For details, see **Table 2-20**.
zoneIP	Protected IP address.
logType	Log type. The default value is **ip_attack_sum**, indicating attack logs.
maxDropPps	Peak rate of attack packets, in pps.
maxInKbps	Peak inbound traffic, in kbit/s.
startTime	Time when the attack starts
endTime	End time of the attack. If this parameter is left blank, the attack has not ended yet.
maxDropKbps	Peak attack traffic, in **kbps**.
attackStatus	Attack status. ● ATTACK: being attacked ● NORMAL: normal

Table 2-20 Attack type description

Value	Attack Type
0-9	User-defined attack type
10	SYN flood attack
11	Ack flood attack
12	SynAck flood attack

Value	Attack Type
13	Fin/Rst flood attack
14	Concurrent connections exceed the threshold.
15	New connections exceed the threshold.
16	TCP fragment attack
17	TCP fragment bandwidth limit attack
18	TCP bandwidth limit attack
19	UDP flood attack
20	UDP fragment attack
21	UDP fragment bandwidth limit attack
22	UDP bandwidth limit attack
23	ICMP bandwidth limit attack
24	Other bandwidth limit attack
25	Traffic limiting attack
26	HTTPS flood attack
27	HTTP flood attack
28	Reserved
29	DNS query flood attack
30	DNS reply flood attack
31	SIP flood attack
32	Blacklist dropping
33	Abnormal HTTP URL behavior
34	TCP fragment abnormal dropping traffic attack
35	TCP abnormal dropping traffic attack
36	UDP fragment abnormal dropping traffic attack
37	UDP abnormal dropping traffic attack
38	ICMP abnormal attack
39	Other abnormal attacks
40	Connection flood attack
41	Domain name hijacking attack
42	DNS poisoning packet attack

Value	Attack Type
43	DNS reflection attack
44	Oversize DNS packet attack
45	Abnormal rate of DNS source requests
46	Abnormal rate of DNS source replies
47	Abnormal rate of DNS domain name requests
48	Abnormal rate of DNS domain name replies
49	DNS request packet TTL anomaly
50	DNS packet format anomaly
51	DNS cache matching and dropping attack
52	Port scan attacks
53	Abnormal TCP packet flag bit
54	BGP attack
55	UDP association defense anomaly
56	DNS NO such Name
57	Other fingerprint attacks
58	Zone traffic limit attack
59	HTTP slow attacks
60	Malware prevention
61	Domain name blocking
62	Filtering
63	Web attack packet capture
64	SIP source rate limiting

2.8 Viewing Statistics Reports

CNAD shows normal traffic and attack traffic in two dimensions: traffic and packet rate. You can view the normal traffic and attack traffic to know your network security situation.

On the **Dashboard** tab, you can view the attack sources, received traffic, attack traffic, DDoS protection overview, peak traffic scrubbed, attack type distribution, and top 10 attacked IP addresses.

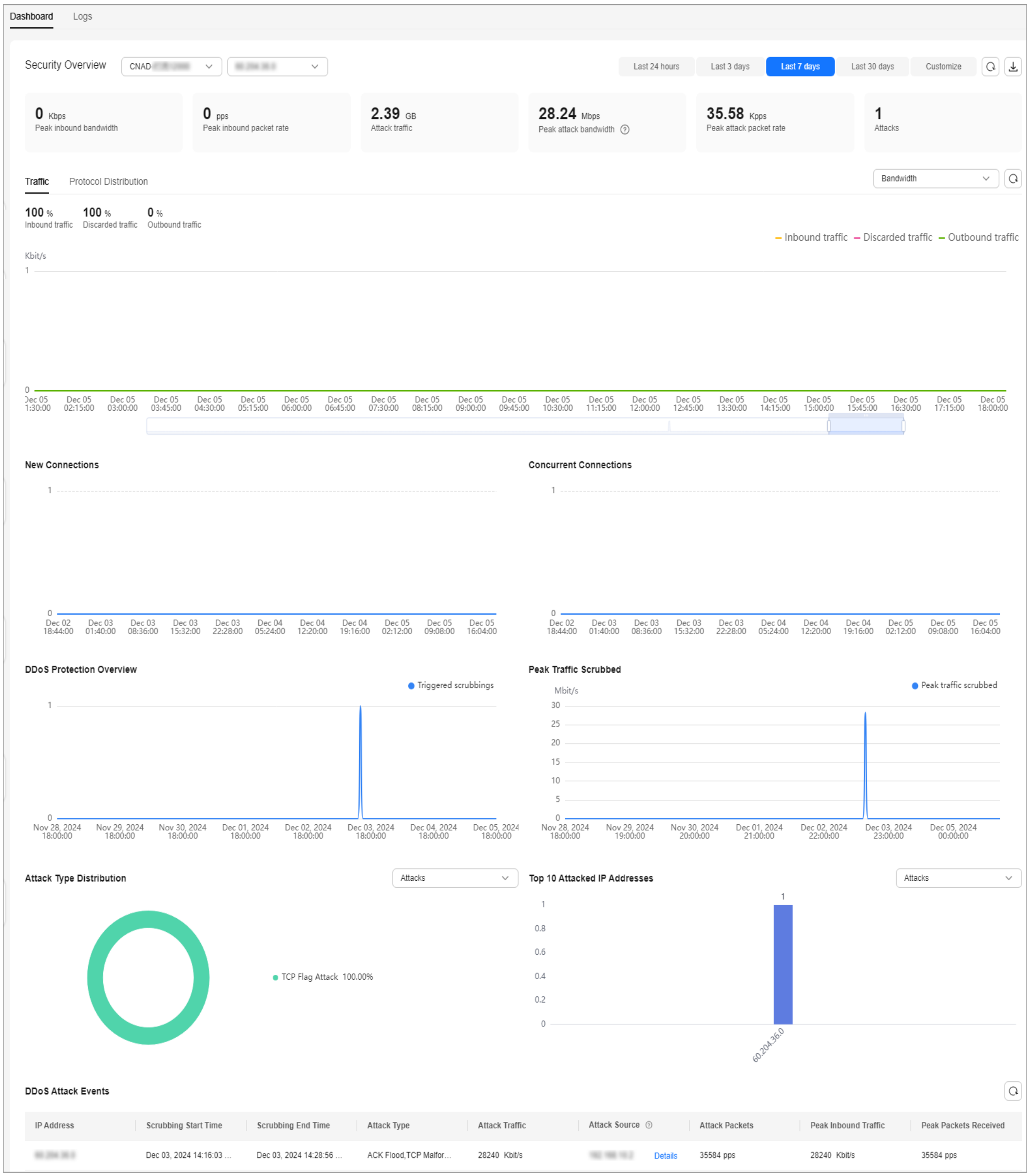
Viewing the CNAD Report

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced** > **Dashboard**. The **Data Reports** page is displayed.

Figure 2-40 Dashboard



0 Kbps
Peak inbound bandwidth

0 pps
Peak inbound packet rate

2.39 GB
Attack traffic

28.24 Mbps
Peak attack bandwidth

35.58 Kpps
Peak attack packet rate

1
Attacks

100 % Inbound traffic
100 % Discarded traffic
0 % Outbound traffic

DDoS Attack Events

IP Address	Scrubbing Start Time	Scrubbing End Time	Attack Type	Attack Traffic	Attack Source	Attack Packets	Peak Inbound Traffic	Peak Packets Received
[redacted]	Dec 03, 2024 14:16:03 ...	Dec 03, 2024 14:28:56 ...	ACK Flood,TCP Malfor...	28240 Kbit/s	[redacted] Details	35584 pps	28240 Kbit/s	35584 pps

Table 2-21 Parameter description

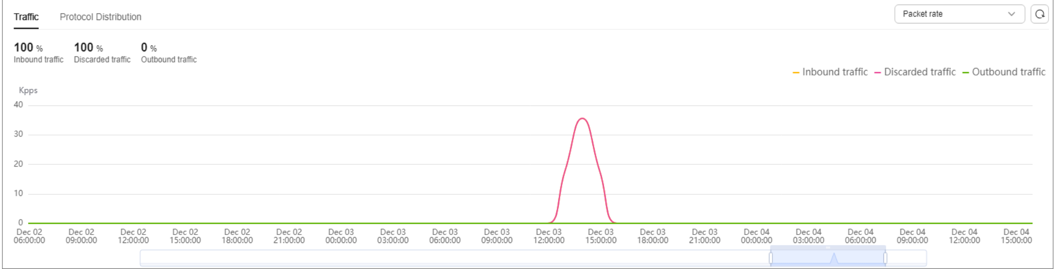
Parameter	Description
Peak Inbound Bandwidth	Maximum traffic accessing the specified IP address of a specified instance per second
Peak Packets Received	Maximum number of incoming packets per second
Peak Attack Bandwidth	Maximum traffic attacking the specified IP address of a specified instance per second The attack traffic refers to the attack traffic that triggers security events.
Peak Attack Packet Rate	Maximum number of incoming attack packets per second
Attacks	Number of DDoS attacks launched on the specified IP address of a specified instance
Traffic Trend	Proportions and distribution trends of inbound traffic, outbound traffic, and discarded traffic.
Protocol Distribution	Proportions and distribution trend of protocols such as TCP, UDP, and ICMP in traffic.
Concurrent Connections	Number of concurrent connections.
New Connections	Number of new connections.
DDoS Protection Overview	Trend of scrubbing times.
Peak Traffic Scrubbed	Trend of peak scrubbed traffic.
Attack Type Distribution	Types of attack events. Views attack traffic by **Attacks** or **Attack Traffic**.
Top 10 Attacked IP Addresses	Top 10 IP addresses that are most frequently attacked. You can view statistics by **Attacks** or **Bandwidth**.
DDoS Attack Events	DDoS attack events Click **Details** next to the attack source IP address to view the complete attack source IP address list.

NOTE

- Click **Details** next to the attack source IP address to view the complete attack source IP address list.
- For ongoing attack events, you can click **View Dynamic Blacklist** to view the blacklisted IP addresses that are in attack.
- The attack sources of ongoing attacks may not be displayed.
- Some attack events contain only some attack types. Their attack sources are not displayed.
- Attack sources are sampled randomly. Not all attack source information is displayed.

Step 4 Click the **Traffic** tab to view the traffic data.

Figure 2-41 Traffic Trend



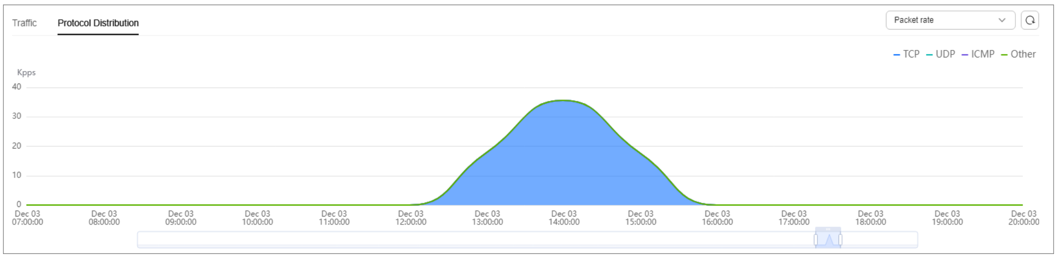
100 % Inbound traffic

100 % Discarded traffic

0 % Outbound traffic

Step 5 Click the **Protocol Distribution** tab to view the protocol distribution information.

Figure 2-42 Protocol distribution



----End

Related Operations

Downloading a report: Click ⤓ in the upper right corner of the page to download the data report to the local host.

2.9 Managing Instances

2.9.1 Viewing Information About an Instance

To verify that your instances are running normally after enabling CNAD, check their status in the instance list.

Viewing CNAD Instance Information

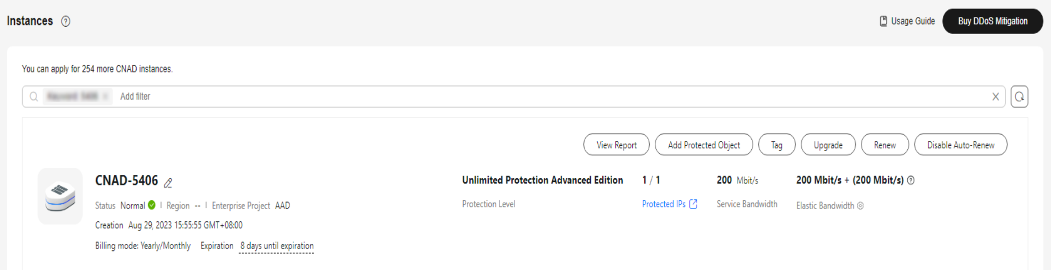
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced > Instances**. The **Instances** page is displayed.

Step 4 View the instance information.

Figure 2-43 Instances



You can apply for 254 more CNAD instances.

[redacted]

CNAD-5406

Status Normal | Region -- | Enterprise Project AAD

Creation Aug 29, 2023 15:55:55 GMT+08:00

Billing mode: Yearly/Monthly Expiration 8 days until expiration

Unlimited Protection Advanced Edition — Protection Level

1 / 1 — Protected IPs

200 Mbit/s — Service Bandwidth

200 Mbit/s + (200 Mbit/s) — Elastic Bandwidth

----End

2.9.2 Configuring Instance Tags

A tag consists of a tag key and a tag value and is used to identify cloud resources. You can use tags to classify cloud resources by dimension, such as usage, owner, or environment. Tags allow you to better manage CNAD instances.

Add a tag for the instance.

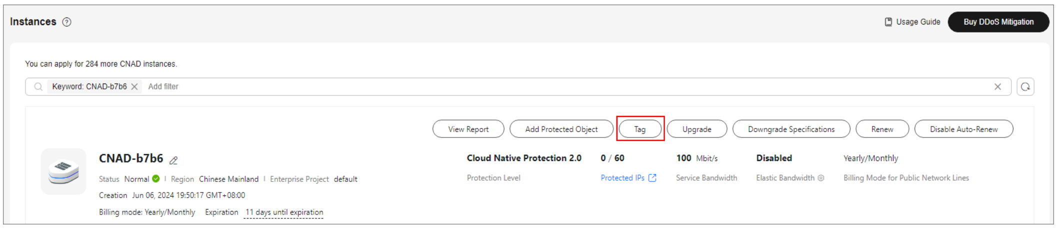
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced** > **Instances**. The **Instances** page is displayed.

Step 4 In the row containing the target instance, click **Set Tag**.

Figure 2-44 Set a tag for a CNAD instance



You can apply for 284 more CNAD instances.

Keyword: CNAD-b7b6

CNAD-b7b6

Status Normal | Region Chinese Mainland | Enterprise Project default

Creation Jun 06, 2024 19:50:17 GMT+08:00

Billing mode: Yearly/Monthly Expiration 11 days until expiration

Cloud Native Protection 2.0 — Protection Level

0 / 60 — Protected IPs

100 Mbit/s — Service Bandwidth

Disabled — Elastic Bandwidth

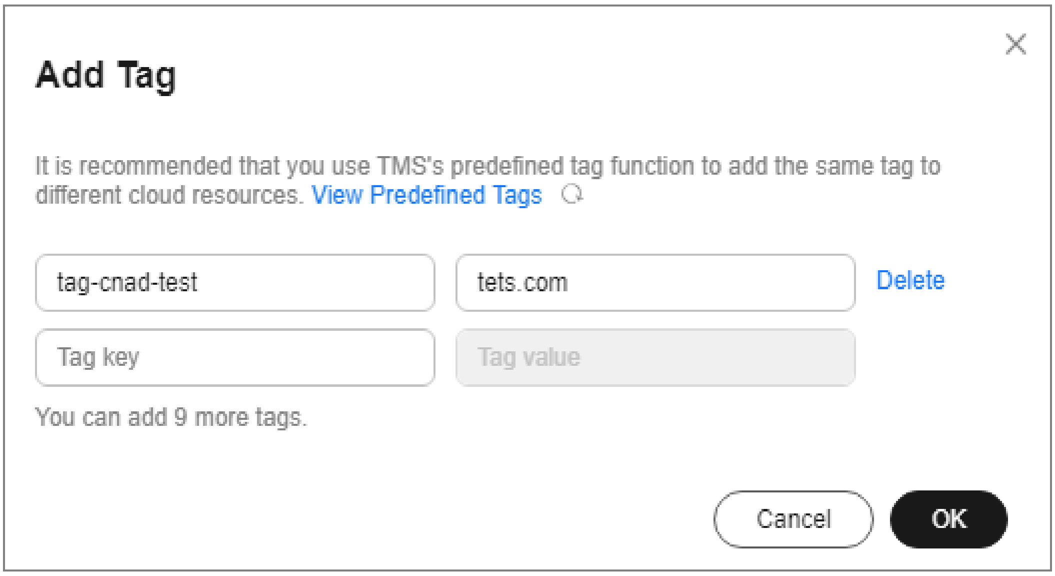
Yearly/Monthly — Billing Mode for Public Network Lines

Step 5 On the tag adding page, click **Add Tag** to add a tag.

Step 6 Select the **tag key** and **tag value**. There are two ways to add a tag:

- Manually enter a tag key and tag value.
- Select an existing tag.

Figure 2-45 Adding a tag



Add Tag

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View Predefined Tags

tag-cnad-test	tets.com	Delete
Tag key	Tag value	

You can add 9 more tags.

NOTE

If your organization has configured a tag policy for the service, you need to add tags to resources based on the tag policy. Otherwise, the tagging operation might fail. For more information about the tag policy, contact your organization administrator.

Step 7 Click **OK**.

----End

2.10 Managing Protected Objects

2.10.1 Viewing Details about a Protected Object

After adding protected objects, you can regularly monitor their protection status and attack statistics. This allows you to adjust the protection policy promptly to enhance service security.

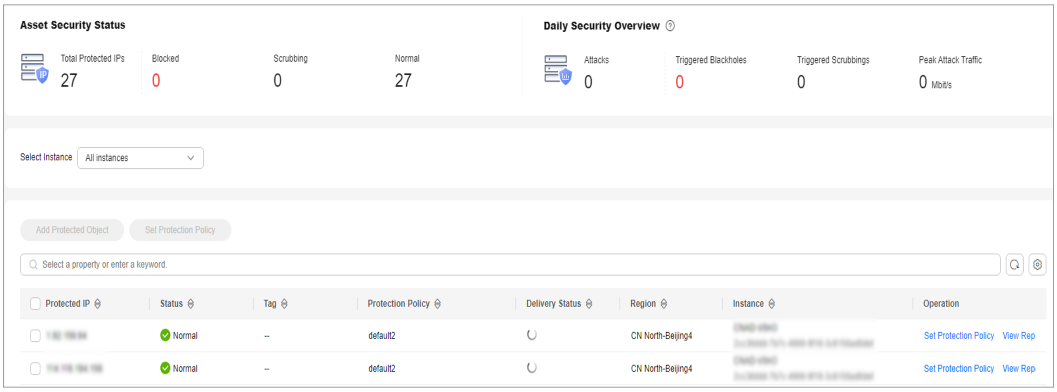
Checking a Protected Object

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

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

Step 3 In the navigation tree on the left, choose **Cloud Native Anti-DDoS Advanced > Protected Objects**. The **Protected Objects** page is displayed.

Figure 2-46 Protected objects



Asset Security Status

Total Protected IPs 27 | Blocked 0 | Scrubbing 0 | Normal 27

Daily Security Overview

Attacks 0 | Triggered Blackholes 0 | Triggered Scrubbings 0 | Peak Attack Traffic 0 Mbit/s

Select Instance: All instances

Protected IP	Status	Tag	Protection Policy	Delivery Status	Region	Instance	Operation
[redacted]	Normal	--	default2		CN North-Beijing4	[redacted]	Set Protection Policy View Rep
[redacted]	Normal	--	default2		CN North-Beijing4	[redacted]	Set Protection Policy View Rep

Step 4 View the information described in **Table 2-22** about the target protected object.

Table 2-22 Information about a protected object

Parameter	Description
Protected IP	IP address protected by CNAD
Tag	Tag of a protected IP address
Status	Status of a protected IP address ● **Normal** ● **Cleaning**
Protection Policy	Protection policy for a protected IP address
Delivery Status	Delivery status of the protection policy. ● **Delivering** ● **Delivered**
Region	Region of a protected IP address
Instance	Instance that a protected IP address belongs to
Operation	● You can click **View Report** to go to the **Dashboard** tab and view protection data. ● If no protection policy has been configured for a protected IP address, you can click **Set Protection Policy** to select a protection policy for the IP address.

----End

2.10.2 Selecting a Protection Policy for a Protected Object

You need to select a protection policy for a protected object so that it can be protected by CNAD from DDoS attacks.

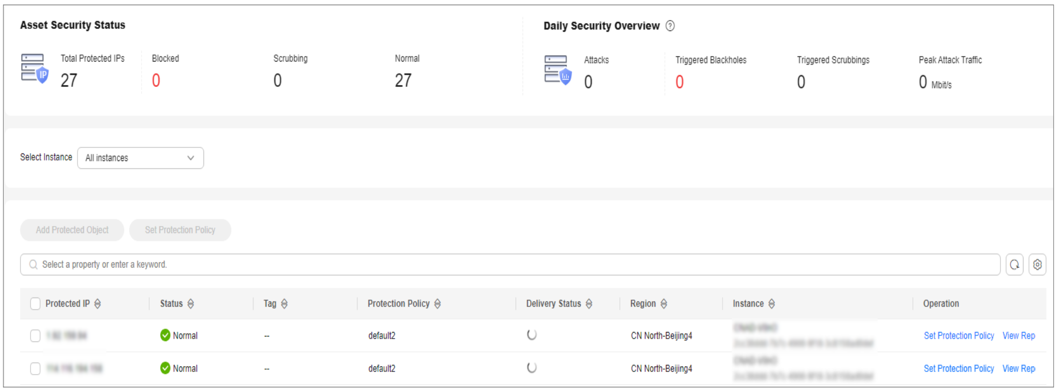
Configuring a Protection Policy

Step 1 Log in to the management console.

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

Step 3 In the navigation tree on the left, choose **Cloud Native Anti-DDoS Advanced** > **Protected Objects**. The **Protected Objects** page is displayed.

Figure 2-47 Protected objects



Asset Security Status

Total Protected IPs	Blocked	Scrubbing	Normal
27	0	0	27

Daily Security Overview

Attacks	Triggered Blackholes	Triggered Scrubbings	Peak Attack Traffic
0	0	0	0 Mbit/s

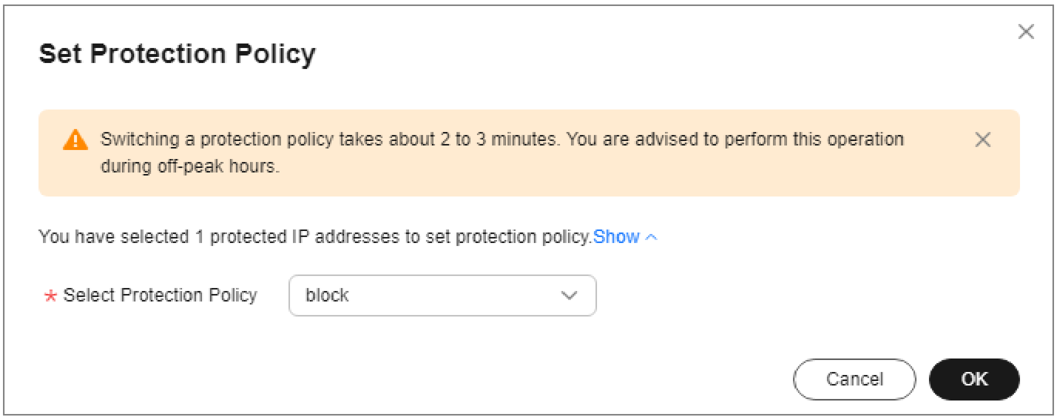
Select Instance: All instances

Protected IP	Status	Tag	Protection Policy	Delivery Status	Region	Instance	Operation
[redacted]	Normal	--	default2		CN North-Beijing4	[redacted]	Set Protection Policy View Rep
[redacted]	Normal	--	default2		CN North-Beijing4	[redacted]	Set Protection Policy View Rep

Step 4 In the row containing the target protected object, click **Set Protection Policy** in the **Operation** column.

Step 5 In the dialog box that is displayed, select a protection policy and click **OK**.

Figure 2-48 Set Protection Policy



Set Protection Policy

Switching a protection policy takes about 2 to 3 minutes. You are advised to perform this operation during off-peak hours.

You have selected 1 protected IP addresses to set protection policy. Show

* Select Protection Policy: block

NOTE

You can click **Show** to view details about the protected IP addresses.

----End

Batch Configuring Protection Policies

Select protected objects for which you want to set a protection policy. In the upper left corner of the list, click **Set Protection Policy**. Select a protection policy as prompted and click **OK**.

NOTE

Batch setting can be used only for multiple protected objects in the same instance.

2.10.3 Removing a Protected Object from CNAD Advanced

If a protected object no longer needs CNAD Advanced protection, you can remove it from the CNAD Advanced instance.

If an EIP is removed from a CNAD Advanced instance, it will be **automatically protected by CNAD Basic**.

The dedicated EIP bound to **CNAD Advanced - Unlimited Protection Advanced Edition** cannot be accessed from the Internet after being removed. Exercise caution when removing a protected object.

NOTICE

Once protected objects are removed, they will no longer have DDoS protection, introducing potential security risks to your resources. Proceed with caution when performing this operation.

Deleting a Protected Object

Step 1 Log in to the management console.

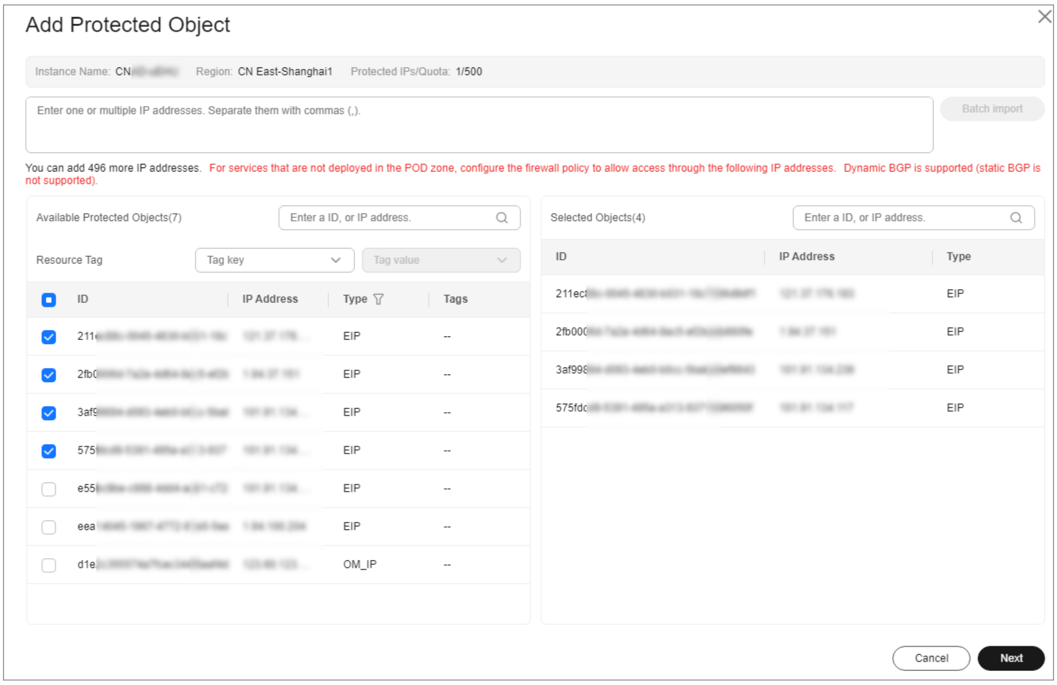
Step 2 Select a region in the upper part of the page, click ☰ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

Step 3 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced > Instances**. The **Instances** page is displayed.

Step 4 Find the instance from which you want to remove the protected object and click **Add Protected Object**.

Step 5 In the dialog box that is displayed, deselect the object to be removed and click **Next**.

Figure 2-49 Deleting a protected object



Add Protected Object

Instance Name: CN[redacted] Region: CN East-Shanghai1 Protected IPs/Quota: 1/500

Enter one or multiple IP addresses. Separate them with commas (,).

You can add 496 more IP addresses. For services that are not deployed in the POD zone, configure the firewall policy to allow access through the following IP addresses. Dynamic BGP is supported (static BGP is not supported).

Available Protected Objects(7)

Enter a ID, or IP address.

Resource Tag: Tag key, Tag value

■	ID	IP Address	Type	Tags
☑	211[redacted]	[redacted]	EIP	--
☑	2fb0[redacted]	[redacted]	EIP	--
☑	3af9[redacted]	[redacted]	EIP	--
☑	575[redacted]	[redacted]	EIP	--
□	e55[redacted]	[redacted]	EIP	--
□	eea[redacted]	[redacted]	EIP	--
□	d1e[redacted]	[redacted]	OM_IP	--

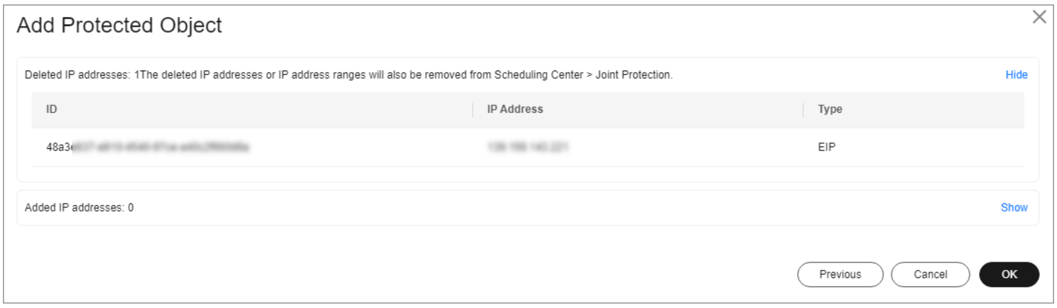
Selected Objects(4)

Enter a ID, or IP address.

ID	IP Address	Type
211ec[redacted]	[redacted]	EIP
2fb000[redacted]	[redacted]	EIP
3af998[redacted]	[redacted]	EIP
575fdc[redacted]	[redacted]	EIP

Step 6 Confirm the object to be removed and click **OK**.

Figure 2-50 Confirming the removal of a protected object



Add Protected Object

Deleted IP addresses: 1The deleted IP addresses or IP address ranges will also be removed from Scheduling Center > Joint Protection.

ID	IP Address	Type
48a3[redacted]	[redacted]	EIP

Added IP addresses: 0

----End

2.11 Viewing Monitoring Metrics

2.11.1 CNAD Monitoring Metrics

Description

This topic describes metrics reported by CNAD to Cloud Eye as well as their namespaces. You can use Cloud Eye to query the metrics of the monitored objects and alarms generated for CNAD.

Namespaces

SYS.DDOS

NOTE

A namespace is an abstract collection of resources and objects. Multiple namespaces can be created in a single cluster with the data isolated from each other. This enables namespaces to share the same cluster services without affecting each other.

Metrics

Table 2-23 Monitoring metrics supported by CAND Advanced

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
ip_drop_rate	Discarding traffic	Traffic discarding bandwidth of an IP address	≥0kb/s	CNAD	60s
instance_drop_rate	Discarding traffic	Traffic discarding bandwidth of an instance	≥0kb/s	CNAD	60s
ip_back_to_source_rate	Retrieval bandwidth	Retrieval traffic bandwidth of an IP address	≥0kb/s	CNAD	60s
instance_back_to_source_rate	Retrieval bandwidth	Retrieval traffic bandwidth of an instance	≥0kb/s	CNAD	60s
ip_internet_in_rate	Inbound traffic	Inbound traffic bandwidth of an IP address	≥0kb/s	CNAD	60s
instance_internet_in_rate	Inbound traffic	Inbound traffic bandwidth of an instance	≥0kb/s	CNAD	60s
ip_new_connection	New connections	Number of new connections of an IP address	≥0count/s	CNAD	60s
instance_new_connection	New connections	Number of new connections of an instance	≥0count/s	CNAD	60s

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
ip_concurrent_connection	Concurrent connections	Number of concurrent connections of an IP address	≥0count/s	CNAD	60s
instance_concurrent_connection	Concurrent connections	Number of concurrent connections of an instance	≥0count/s	CNAD	60s

Dimension

Key	Value
package	Protection package
package_ip	Protection package - protected IP addresses

2.11.2 Viewing Monitoring Metrics

On the management console, you can view CNAD metrics to learn about the protection status in a timely manner and set protection policies based on the metrics.

Prerequisites

You have configured alarm rules on the Cloud Eye console. For more details, see **Configuring Monitoring Alarm Rules**.

Viewing Monitoring Metrics

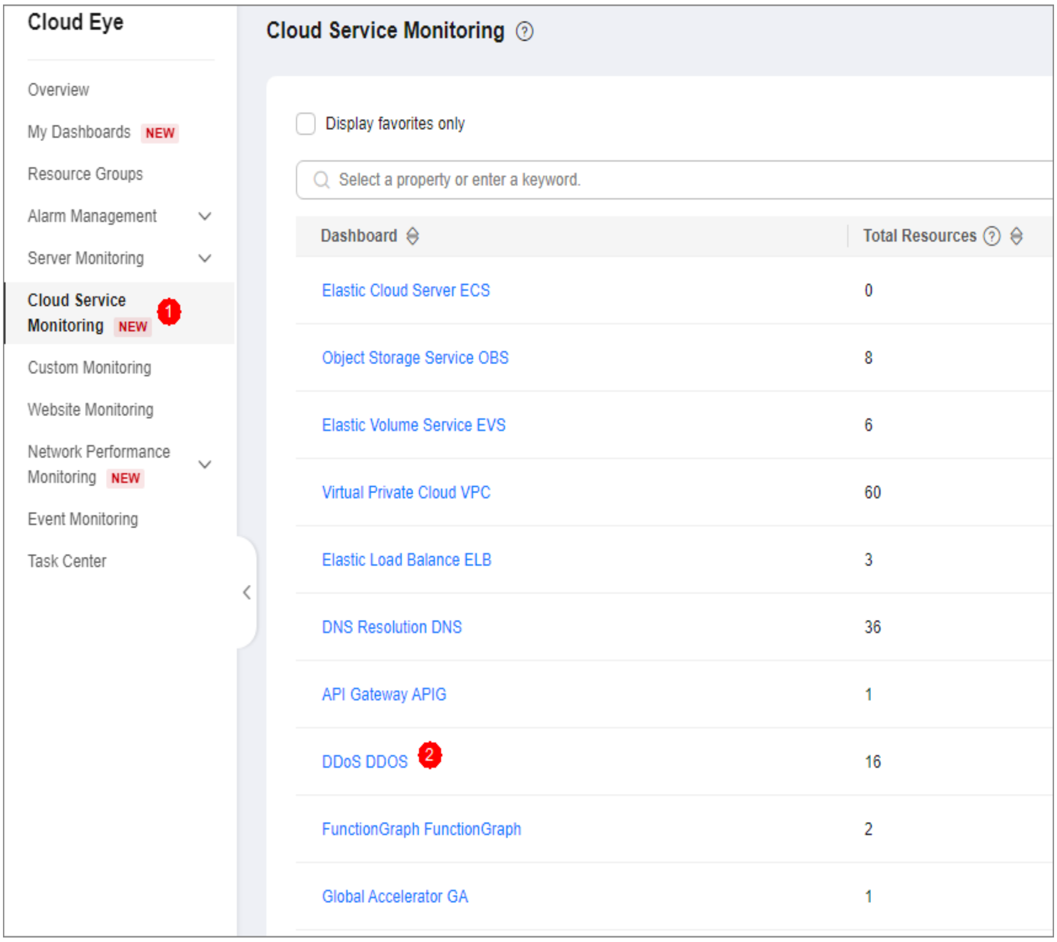
Step 1 **Log in to the management console**.

Step 2 Click 📍 in the upper left corner of the displayed page to select a region.

Step 3 Hover your mouse over ☰ in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

Step 4 Choose **Cloud Service Monitoring** > **Anti-DDoS Service**.

Figure 2-51 Selecting a service



Dashboard	Total Resources
Elastic Cloud Server ECS	0
Object Storage Service OBS	8
Elastic Volume Service EVS	6
Virtual Private Cloud VPC	60
Elastic Load Balance ELB	3
DNS Resolution DNS	36
API Gateway APIG	1
DDoS DDOS	16
FunctionGraph FunctionGraph	2
Global Accelerator GA	1

Step 5 On the **Cloud Service Monitoring Details** page, choose **Anti-DDoS Service** > **Protection Package**.

Step 6 Locate the row that contains the target object and click **View Metric** to view the metric details of the object.

----End

2.11.3 Configuring Monitoring Alarm Rules

You can set alarm rules to customize the monitored objects and notification policies, and set parameters such as the alarm rule name, monitored object, metric, threshold, monitoring scope, and whether to send notifications. This helps you learn the CNAD protection status in a timely manner.

For details about how to set monitoring alarms for multiple instances or protected IP addresses, see **Setting Monitoring Alarm Rules in Batches**. For details about how to set monitoring alarms for a specified instance or protected IP address, see **Setting Monitoring Alarm Rules for a Specified Resource**.

If you need to customize more metrics, you can report them to Cloud Eye through API requests. For details, see **Adding Monitoring Data** and **CNAD Monitoring Metrics**.

Setting Monitoring Alarm Rules in Batches

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

Step 2 Click 📍 in the upper left corner of the displayed page to select a region.

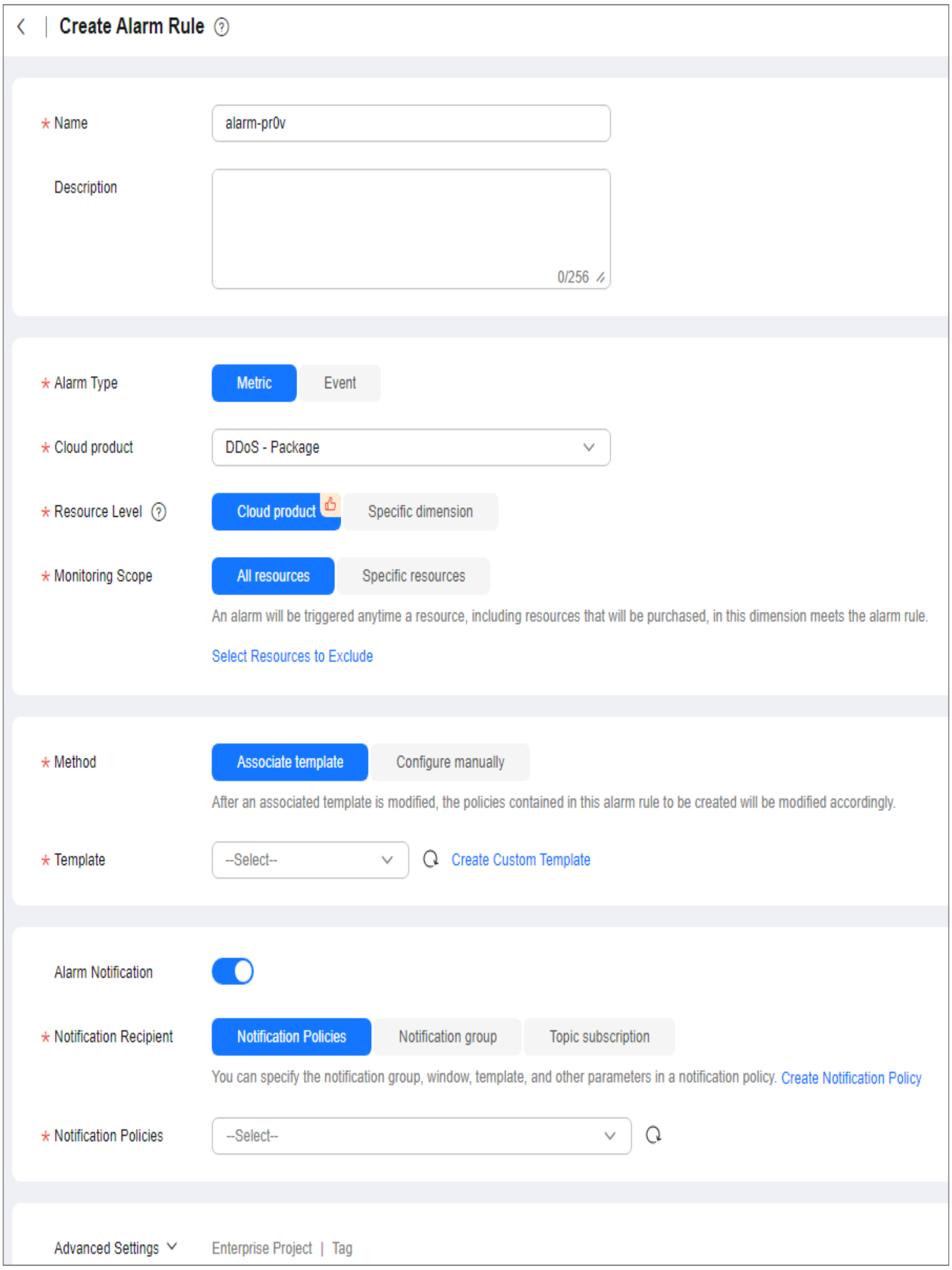
Step 3 Hover your mouse over ☰ in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.

Step 5 In the upper right corner of the page, click **Create Alarm Rule**.

Step 6 Enter the alarm rule information by referring to **Table 2-24**.

Figure 2-52 Configuring Monitoring Alarm Rules



Create Alarm Rule

* Name: alarm-pr0v

Description: 0/256

* Alarm Type: Metric | Event

* Cloud product: DDoS - Package

* Resource Level: Cloud product | Specific dimension

* Monitoring Scope: All resources | Specific resources

An alarm will be triggered anytime a resource, including resources that will be purchased, in this dimension meets the alarm rule.

Select Resources to Exclude

* Method: Associate template | Configure manually

After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.

* Template: --Select-- Create Custom Template

Alarm Notification

* Notification Recipient: Notification Policies | Notification group | Topic subscription

You can specify the notification group, window, template, and other parameters in a notification policy. Create Notification Policy

* Notification Policies: --Select--

Advanced Settings: Enterprise Project | Tag

Table 2-24 Alarm rule parameters

Parameter	Description
Name	Name of the rule. The system generates a random name and you can modify it.
Description	Description about the rule.

Parameter	Description
Alarm Type	Alarm type
Cloud Service	Select **DDoS-Package** from the drop-down list box.
Resource Level	Select the resource dimension to be monitored.
Monitoring Scope	Scope where the alarm rule applies to. You can select **All resources**, **Resource groups** or **Specific resources**.
Method	You can select **Associate Template** or **Customize**. For details about how to create a custom template, see **Creating a Custom Template**. **NOTE** After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.
Template	Select a template.
Alarm Notification	Whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message.
Notification Recipient	Object to which the alarm notification is sent. Select an object based on the site requirements.

Step 7 Click **Create**. In the displayed dialog box, click **OK**.

----End

Setting Monitoring Alarm Rules for a Specified Resource

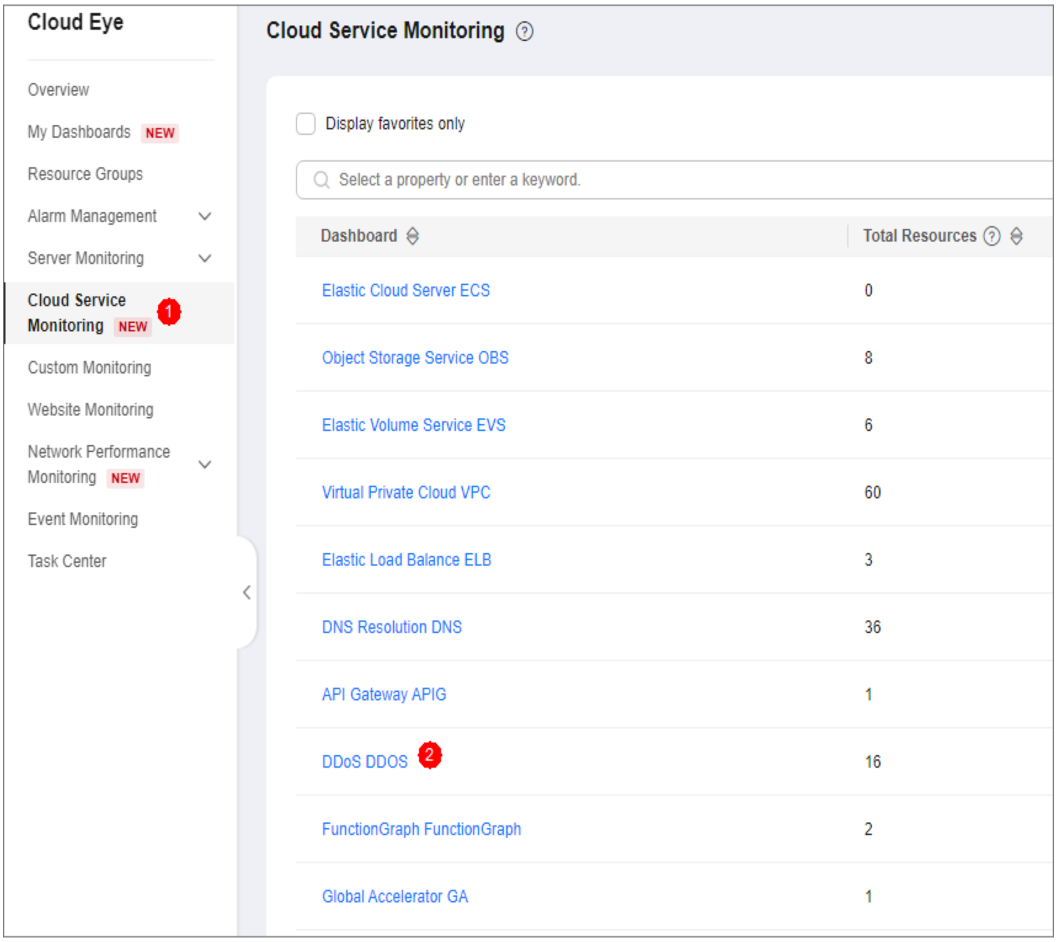
Step 1 **Log in to the management console**.

Step 2 Click 📍 in the upper left corner of the displayed page to select a region.

Step 3 Hover your mouse over ☰ in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

Step 4 Choose **Cloud Service Monitoring** > **Anti-DDoS Service**.

Figure 2-53 Selecting a service



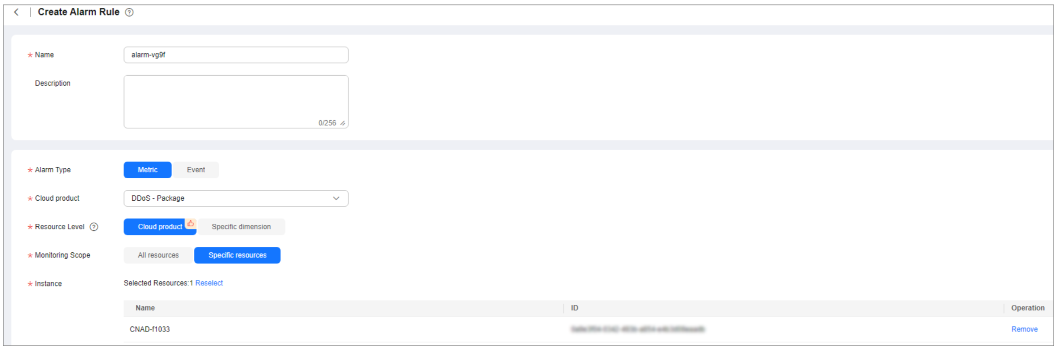
Dashboard	Total Resources
Elastic Cloud Server ECS	0
Object Storage Service OBS	8
Elastic Volume Service EVS	6
Virtual Private Cloud VPC	60
Elastic Load Balance ELB	3
DNS Resolution DNS	36
API Gateway APIG	1
DDoS DDOS	16
FunctionGraph FunctionGraph	2
Global Accelerator GA	1

Step 5 On the **Cloud Service Monitoring Details** page, choose **Anti-DDoS Service** > **Protection Package**.

Step 6 Locate the row that contains the object to be monitored, and click **Create Alarm Rule**.

Step 7 Enter the alarm rule information by referring to **Table 2-25**.

Figure 2-54 Configuring monitoring alarm rules



* Name: alarm-vg9f

Description: 0/256

* Alarm Type: Metric

* Cloud product: DDoS - Package

* Resource Level: Cloud product

* Monitoring Scope: Specific resources

* Instance: Selected Resources:1 Reselect

Name	ID	Operation
CNAD-f1033	[redacted]	Remove

Table 2-25 Alarm rule parameters

Parameter	Description
Name	Name of the rule. The system generates a random name and you can modify it.
Description	Description about the rule.
Alert Type	Retain the default value.
Resource Type	Retain the default value.
Dimension	Retain the default value.
Monitoring Scope	Retain the default value.
Monitored objects	Retain the default value.
Method	You can select **Associate Template** or **Customize**. For details about how to create a custom template, see **Creating a Custom Template**. **NOTE** After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.
Template	Select a template.
Alarm Notification	Whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message.
Notification Type	Select a notification method as required.

Step 8 Click **Create**. In the displayed dialog box, click **OK**.

----End

2.11.4 Setting Event Alarm Notifications

Cloud Eye enables event monitoring for protected EIPs and generates alarms for scrubbing, blocking, and unblocking events. This helps you learn about the protection status of CNAD in a timely manner.

After the event alarm notification function is enabled, you can view event details on the **Event Monitoring** page of the Cloud Eye console when an event occurs.

NOTE

If you enable **Alarm Notifications**, Simple Message Notification (SMN) will be used and related fees will be incurred.

Enabling Event Alarm Notifications

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

Step 2 Click 📍 in the upper left corner of the displayed page to select a region.

Step 3 Hover your mouse over ☰ in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

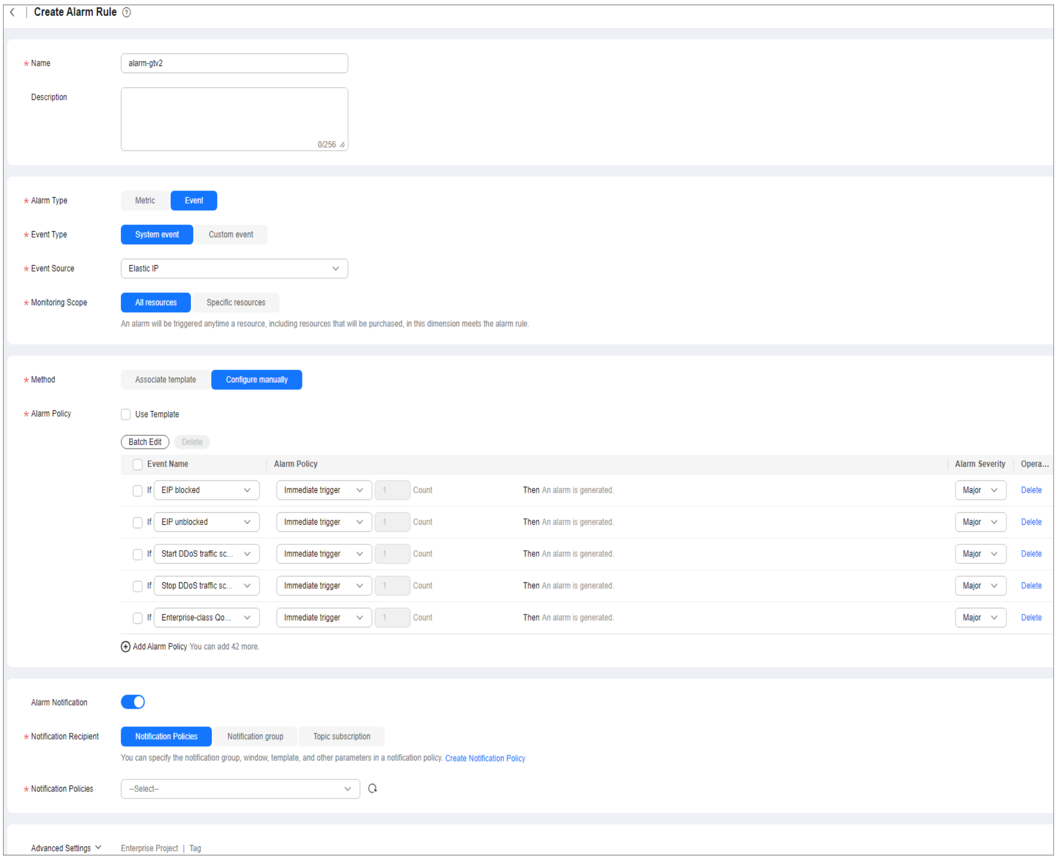
Step 4 Select a monitoring method based on the site requirements.

- Method 1: In the navigation tree on the left, choose **Event Monitoring**. The **Event Monitoring** page is displayed.
- Method 2: In the navigation pane on the left, choose **Alarms** > **Alarm Rules**. The **Alarm Rules** page is displayed.

Step 5 In the upper right corner of the page, click **Create Alarm Rule**. The **Create Alarm Rule** page is displayed.

Step 6 Set alarm parameters by referring to **Table 2-26**.

Figure 2-55 Alarm parameters



Create Alarm Rule

* Name: alarm-gtv2

Description: 0/256

* Alarm Type: Metric | **Event**

* Event Type: **System event** | Custom event

* Event Source: Elastic IP

* Monitoring Scope: **All resources** | Specific resources

An alarm will be triggered anytime a resource, including resources that will be purchased, in this dimension meets the alarm rule.

* Method: Associate template | **Configure manually**

* Alarm Policy: □ Use Template

Batch Edit | Delete

□ Event Name	Alarm Policy				Alarm Severity	Opera...
□ If EIP blocked	Immediate trigger	1	Count	Then An alarm is generated.	Major	Delete
□ If EIP unblocked	Immediate trigger	1	Count	Then An alarm is generated.	Major	Delete
□ If Start DDoS traffic sc...	Immediate trigger	1	Count	Then An alarm is generated.	Major	Delete
□ If Stop DDoS traffic sc...	Immediate trigger	1	Count	Then An alarm is generated.	Major	Delete
□ If Enterprise-class Qo...	Immediate trigger	1	Count	Then An alarm is generated.	Major	Delete

Add Alarm Policy You can add 42 more.

Alarm Notification: ●

* Notification Recipient: **Notification Policies** | Notification group | Topic subscription

You can specify the notification group, window, template, and other parameters in a notification policy. Create Notification Policy

* Notification Policies: --Select--

Advanced Settings: Enterprise Project | Tag

Table 2-26 Parameters for configuring a protection policy

Parameter	Description
Name	Name of the rule. The system generates a random name and you can modify it.

Parameter	Description
Description	Description about the rule.
Alarm Type	Select **Event**.
Event Type	Choose **System Event**.
Event Source	Choose **Elastic IP**.
Monitoring Scope	Specifies the resource scope to which the alarm rule applies. Set this parameter as required.
Method	The default option is **Configure manually**.
Alarm Policy	You are advised to select **EIP blocked**, **EIP unblocked**, **Start Anti-DDoS traffic scrubbing**, and **Stop Anti-DDoS traffic scrubbing**. When the traffic is greater than 10,000 kbit/s, the system sends an alarm notification when scrubbing starts and when scrubbing ends. When the traffic is less than 10,000 kbit/s, no alarm notification is sent.
Notification Recipient	Set it to the actual recipient. **NOTE** Alarm messages are sent by Simple Message Notification (SMN), which may incur a small amount of fees.

Step 7 Click **Create**. In the dialog box that is displayed, click **OK**. The alarm notification is created successfully.

----End

2.12 Querying Audit Logs

2.12.1 CNAD Advanced Operations That Can Be Recorded by CTS

CTS provides records of DDoS Mitigation operations. With CTS, you can query, audit, and backtrack these operations. For details, see **Cloud Trace Service User Guide**.

Table 2-27 lists DDoS Mitigation operations recorded by CTS.

Table 2-27 DDoS Mitigation operations recorded by CTS

Operation	Trace Name
Updating alarm notification configuration	updateAlarmConfig
Deleting alarm notification configuration	deleteAlarmConfig
Creating a protection package	createPackage
Updating a protection package	updatePackage
Binding an IP address to a protection package	bindIpToPackage
Unbinding an IP address from a protection package	unbindIpToPackage
Deleting a protection package	DeletePackage
Creating a policy	createPolicy
Updating a policy	updatePolicy
Binding an IP address to a policy	bindIpToPolicy
Unbinding an IP address from a policy	unbindIpToPolicy
Configuring the blacklist or whitelist	addblackWhiteIpList
Removing a blacklisted or whitelisted item	deleteblackWhiteIpList
Deleting a policy	deletePolicy
Configuring log groups and log streams	updateLogConfig
Disabling log groups and streams	deleteLogConfig
Updating the tag for a protected IP address	updateTagForIp
Setting the connection protection policy	updateConnectionProtection

Operation	Trace Name
Adding a blocked port	addPortBlock
Updating blocked ports	updatePortBlock
Remove a blocked port	deletePortBlock
Adding a fingerprint filter	createFingerprint
Updating fingerprint filters	updateFingerprint
Deleting a fingerprint filter	deleteFingerprint
Adding an IP address to the blacklist or whitelist	addBlackWhiteIpList
Deleting an IP address to the blacklist or whitelist	deleteBlackWhiteIpList
Adding a watermark	createWatermark
Modifying a watermark	updateWatermark
Deleting a watermark	deleteWatermark

2.12.2 Viewing CTS Traces

After you enable CTS, the system starts recording operations on Anti-DDoS Service. You can view the operation records of the last 7 days on the CTS console.

Prerequisites

You have enabled CTS. For details, see **Enabling CTS**.

Viewing CNAD Advanced Audit Logs

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

Step 2 Click ☰ on the left of the page and choose **Cloud Trace Service** under **Management & Deployment**.

Step 3 Choose **Trace List** in the navigation pane on the left.

Step 4 Select **Trace Source** from the drop-down list, enter **CNAD**, and press **Enter**.

Step 5 Click a trace name in the query result to view the event details.

You can use the advanced search function to combine one or more filter criteria in the filter box.

- Enter **Trace Name**, **Resource Name**, **Resource ID**, and **Trace ID**.
  - **Resource Name**: If the cloud resource involved in the trace does not have a name or the corresponding API operation does not involve resource names, this field is left empty.
  - **Resource ID**: If the resource does not have a resource ID or the resource fails to be created, this field is left empty.
- **Trace Source** and **Resource Type**: Select the corresponding cloud service name or resource type from the drop-down list.
- **Operator**: Select one or more operators from the drop-down list.
- Trace Status: The value can be **normal**, **warning**, or **incident**. You can select only one of them.
  - **normal**: indicates that the operation is successful.
  - **warning**: indicates that the operation failed.
  - **incident**: indicates a situation that is more serious than an operation failure, for example, other faults are caused.
- Time range: You can query traces generated in the last hour, day, or week, or customize traces generated in any time period of the last week.

----End

3 Advanced Anti-DDoS User Guide

3.1 AAD Overview

You can purchase an AAD instance and connect your services to the instance. The widely covering defense rules provided by AAD will protect your services from massive DDoS attacks.

Figure 3-1 shows the process of connecting services to AAD.

Figure 3-1 Connecting services to AAD

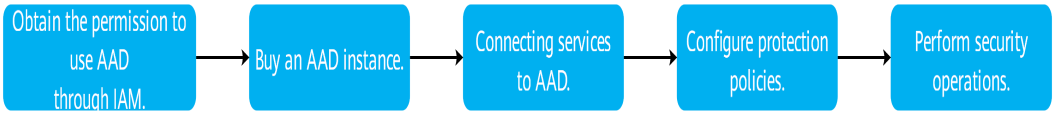

Obtain the permission to use AAD through IAM.
Buy an AAD instance.
Connecting services to AAD.
Configure protection policies.
Perform security operations.

Table 3-1 Procedures

No.	Procedure	Description
1	**Using IAM to Grant AAD Permissions**	Use Identity and Access Management (IAM) to grant fine-grained AAD permissions to users.
2	**Purchasing an AAD Instance**	Purchase an AAD instance based on service requirements.
3	**Connecting Services to AAD**	Connect the domain name or IP address to AAD.
4	**Configuring a Protection Policy**	AAD provides abundant and comprehensive protection rules. You can configure protection policies based on your service requirements.

No.	Procedure	Description
5	Performing common security operations	- **Enabling Alarm Notifications for DDoS Attacks**: After the alarm notification function is enabled, you will receive alarm notifications upon DDoS attacks. - **Enabling Logging**: With LTS, you can perform real-time decision analysis, device O&M management, and service trend analysis in a timely and efficient manner. - **Viewing Statistics**: You can view the DDoS attack defense report and CC attack defense report to learn about the network security status of your service. - **Managing Instances**: You can view AAD instance information and modify instance specifications and configurations. - **Managing Domain Names**: You can view the domain name information, modify the resolution line, and configure the domain name. - **Certificate Management**: You can view certificate information, and update or delete certificates. - **Managing Forwarding Rules**: You can view forwarding rules, modify origin server IP addresses, and export forwarding rules. - **Viewing Monitoring Metrics**: You can view AAD metrics through Cloud Eye to learn about the AAD protection status and adjust protection policies in a timely manner. - **Querying Audit Logs**: You can view historical operation records of AAD on CTS.

3.2 Using IAM to Grant AAD Permissions

3.2.1 Creating a User and Granting the AAD Access Permission

You can use **Identity and Access Management (IAM)** to implement refined permission control for AAD resources. To be specific, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to AAD resources.
- Grant only the permissions required for users to perform a task.
- Entrust a Huawei Cloud account or cloud service to perform professional and efficient O&M to your AAD resources.

If your Huawei Cloud account does not require individual IAM users, skip this section.

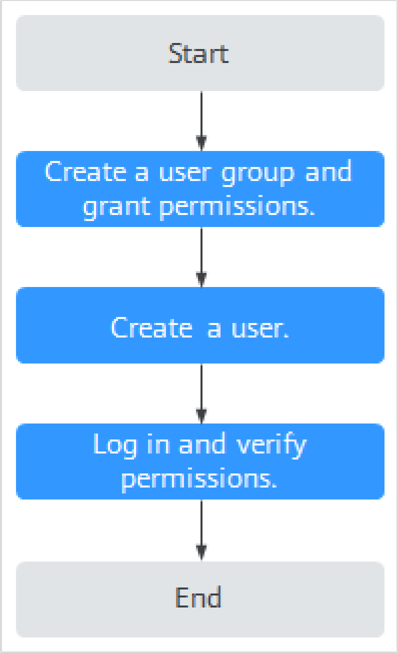
This section describes the procedure for granting permissions (see **Figure 3-2**).

Prerequisites

Learn about the permissions supported by AAD and choose policies or roles according to your requirements.

Process

Figure 3-2 Process for granting permissions


Start
Create a user group and grant permissions.
Create a user.
Log in and verify permissions.
End

1. **Create a user group and assign permissions** to it.

   Create a user group on the IAM console, and assign the **AAD FullAccess** permission to the group.

2. **Create an IAM user**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify the user's permissions.

   Log in to the management console as the created user, and verify the user's permissions.

   Click ☰ and select any other services (for example, the policy contains only the **AAD FullAccess** permission). If a message indicating that the permission is insufficient is displayed, the **AAD FullAccess** permission takes effect.

3.2.2 Creating an AAD Custom Policy

Custom policies can be created to supplement the system-defined policies of AAD. For details about the actions supported by custom policies, see **AAD Permissions and Actions**.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see **Creating a Custom Policy**. This section contains examples of typical AAD custom policies.

Example of Custom AAD Policies

- Example 1: Authorizing a user to query a protection policy.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aad:policy:get"
                                ]
        }
    ]
}
```

- Example 2: Denying deleting an IP address blacklist or whitelist rule.

  A deny policy must be used together with other policies. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  The following method can be used if you need to assign permissions of the **AAD FullAccess** policy to a user but you want to prevent the user from deleting namespaces (aad:whiteBlackIpRule:delete). Create a custom policy for denying namespace deletion, and attach both policies to the group to which the user belongs. Then, the user can perform all operations on AAD except deleting namespaces. The following is an example policy for denying deleting an IP address blacklist or whitelist rule.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "aad:whiteBlackIpRule:delete"
            ]
        },
    ]
}
```

3.2.3 AAD Permissions and Actions

This section describes how to use IAM for fine-grained AAD permissions management. If your Huawei Cloud account does not need individual IAM users, skip this section.

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

You can grant users permissions by using **rules** and **policies**. Roles are a type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. IAM uses policies to perform fine-grained authorization. A policy defines permissions required to perform operations on specific cloud resources under certain conditions.

Supported Actions

AAD provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control.

- Permissions: Statements in a policy that allow or deny certain operations.
- Actions: Specific operations that are allowed or denied.

Permission	Action
Obtain instance details.	aad:instance:get
Query the instance list.	aad:instance:list
Create an instance.	aad:instance:create
Modify an instance.	aad:instance:put
Query the certificate list.	aad:certificate:list
Upload a certificate.	aad:certificate:create
Delete a certificate.	aad:certificate:delete
Obtain domain name details.	aad:domain:get
Obtain the domain name list.	aad:domain:list
Add a domain name.	aad:domain:create
Edit a domain name.	aad:domain:put
Delete a domain name.	aad:domain:delete
Query a protection policy.	aad:policy:get
List domain names with an enabled protection policy.	aad:policy:list
Create a protection policy.	aad:policy:create
Update a protection policy.	aad:policy:put
Delete a protection policy.	aad:policy:delete
Create a blacklist or whitelist rule.	aad:whiteBlackIpRule:create
Delete a blacklist or whitelist rule.	aad:whiteBlackIpRule:delete
Query the blacklist and whitelist rule list.	aad:whiteBlackIpRule:list

Permission	Action
Query quotas.	aad:quotas:get
Query a forwarding rule.	aad:forwardingRule:get
Export forwarding rules.	aad:forwardingRule:list
Add a forwarding rule.	aad:forwardingRule:create
Modify a forwarding rule.	aad:forwardingRule:put
Delete a forwarding rule.	aad:forwardingRule:delete
View a statistics report.	aad:dashboard:get
Query alarm notifications.	aad:alarmConfig:get
Create an alarm notification.	aad:alarmConfig:create

3.2.4 Permission Dependency of the AAD Console

When using AAD, you may need to view resources of or use other cloud services. So you need to obtain required permissions for dependent services so that you can view resources or use AAD functions on AAD Console. To that end, make sure you have the **AAD FullAccess** or **AAD ReadOnlyAccess** assigned first. For details, see **Creating a User and Granting the AAD Access Permission**.

Dependency Policy Configuration

To grant an IAM user the permissions to view or use resources of other cloud services on the AAD console, you must first grant the CAD Administrator, AAD FullAccess, or AAD ReadOnlyAccess policy to the user group to which the user belongs and then grant the dependency policies listed in the table below to the user. The dependency policies in **Table 3-2** will allow the IAM user to access resources of other cloud services.

Table 3-2 AAD console dependency policies and roles

Console Function	Dependent Service	Roles or Policy
Adding a domain name.	Cloud Certificate Manager (CCM)	If the origin server uses the HTTPS forwarding protocol, pulling certificates requires the **SCM ReadOnlyAccess** permission.
Configuring AAD logs	Log Tank Service (LTS)	The LTS ReadOnlyAccess system policy is required to select log group and log stream names created in LTS.

Console Function	Dependent Service	Roles or Policy
Enabling alarm notifications	Simple Message Notification (SMN)	The **SMN ReadOnlyAccess** system policy is required to obtain SMN topic groups.
Configuring instance tags	Tag Management Service (TMS)	Tag keys can be created only after the **TMS FullAccess** system policy is added.
Purchasing an AAD instance	Enterprise Project Management Service (EPS)	You can select an enterprise project when purchasing an instance only after adding the **EPS ReadOnlyAccess** system policy.

3.3 Purchasing an AAD Instance

3.3.1 Purchasing AAD Instances

AAD offers continuous protection to maintain service continuity during frequent DDoS attacks, particularly those with high traffic.

After purchasing the service, you need to perform only simple operations to gain robust protection capabilities. This service is suitable for servers deployed in the Chinese mainland and Asia Pacific regions.

NOTICE

- After you purchase an AAD instance, refunds are not supported.
- If an AAD instance has expired for more than 30 calendar days, AAD will stop forwarding service traffic and the instance will become invalid. If you do not need to use AAD anymore, switch your service traffic from AAD to the origin server 30 calendar days before the expiration date.

Limitations and Constraints

- Each user can purchase a maximum of five instances by default. If the quota is insufficient, **submit a service ticket** to apply for a higher quota.
- If your service servers are located in Chinese Mainland, you are advised to purchase AAD. You have obtained an ICP license for your domain names to be protected by AAD.
- If your service servers are located outside Chinese mainland, you are advised to purchase AAD (International Edition).

Prerequisites

The account must have the permissions of the **CAD Administrator** and **BSS Administrator** roles.

Setting the parameters required for purchasing an AAD instance

Step 1 Log in to the management console.

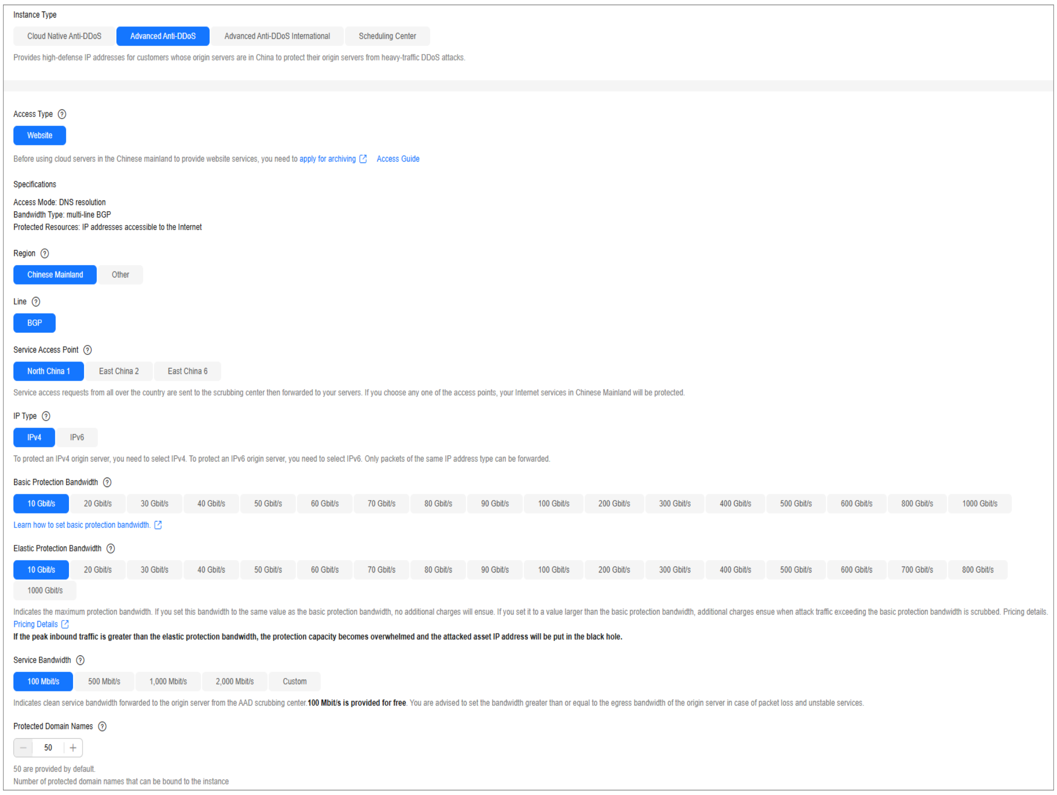
Step 2 Select a region in the upper part of the page, click ☰ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

Step 3 In the upper right corner of the page, click **Buy DDoS Mitigation**.

Step 4 On the **Buy AAD** page, set **Instance Type** to **Advanced Anti-DDoS**.

Step 5 Set instance specifications, as shown in **Figure 3-3**. **Table 3-3** describe related parameters.

Figure 3-3 Setting the parameters required for purchasing an AAD instance



Instance Type: Advanced Anti-DDoS

Provides high-defense IP addresses for customers whose origin servers are in China to protect their origin servers from heavy-traffic DDoS attacks.

Access Type: Website

Before using cloud servers in the Chinese mainland to provide website services, you need to apply for archiving Access Guide

Specifications

Access Mode: DNS resolution
Bandwidth Type: multi-line BGP
Protected Resources: IP addresses accessible to the Internet

Region: Chinese Mainland

Line: BGP

Service Access Point: North China 1

Service access requests from all over the country are sent to the scrubbing center then forwarded to your servers. If you choose any one of the access points, your Internet services in Chinese Mainland will be protected.

IP Type: IPv4

To protect an IPv4 origin server, you need to select IPv4. To protect an IPv6 origin server, you need to select IPv6. Only packets of the same IP address type can be forwarded.

Basic Protection Bandwidth: 10 Gbit/s

Learn how to set basic protection bandwidth.

Elastic Protection Bandwidth: 10 Gbit/s

Indicates the maximum protection bandwidth. If you set this bandwidth to the same value as the basic protection bandwidth, no additional charges will ensue. If you set it to a value larger than the basic protection bandwidth, additional charges ensue when attack traffic exceeding the basic protection bandwidth is scrubbed. Pricing details.
Pricing Details
If the peak inbound traffic is greater than the elastic protection bandwidth, the protection capacity becomes overwhelmed and the attacked asset IP address will be put in the black hole.

Service Bandwidth: 100 Mbit/s

Indicates clean service bandwidth forwarded to the origin server from the AAD scrubbing center.**100 Mbit/s is provided for free**. You are advised to set the bandwidth greater than or equal to the egress bandwidth of the origin server in case of packet loss and unstable services.

Protected Domain Names: 50

50 are provided by default.
Number of protected domain names that can be bound to the instance

Table 3-3 Parameters for purchasing an AAD instance

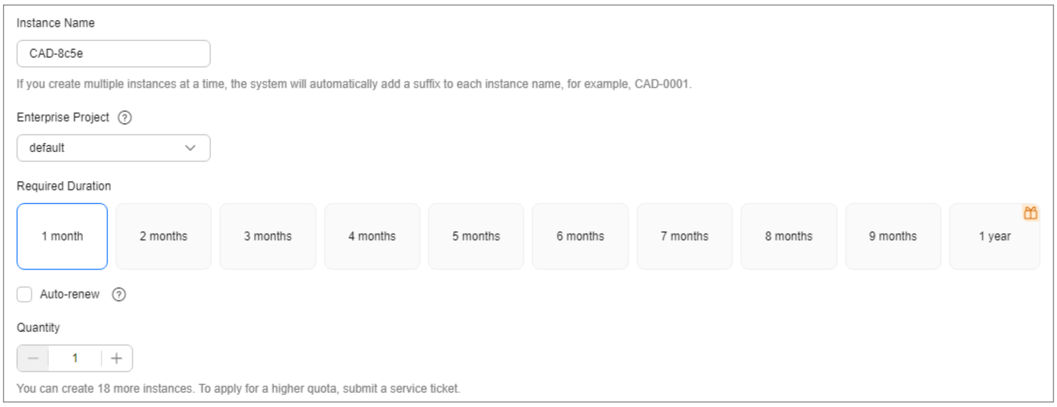
Parameter	Description
Access Type	● Website: Huawei Cloud uses intelligent algorithms to select the optimal access point for you and does not provide fixed high-defense IP addresses. This type is recommended for users using "Domain Name Access". ● IP Address: provides only IP port protection and fixed high-defense IP addresses.
Region	● Chinese mainland: applies to scenarios where service servers are deployed in Chinese Mainland. ● Outside the Chinese mainland: applies to scenarios where service servers are deployed in Asia Pacific (Hong Kong and Singapore are supported currently). If service servers are deployed in other regions, you are advised to purchase the AAD international edition.
Line	● Chinese mainland: Only **BGP** is supported. ● Outside the Chinese mainland: Only AnyCast is supported.
Service Access Point	The following access points are available in Chinese Mainland. Select an access point based on your service location. ● North China 1: China Mobile, China Telecom, China Unicom, Beijing Education Network, Dr. Peng, Hebei Broadcast & Television, and Chongqing Broadcast & Television are supported. ● CN East 2: China Mobile, China Telecom, and China Unicom are supported. ● CN East 6: China Mobile, China Telecom, and China Unicom are supported. Only Asia Pacific is supported outside the Chinese mainland. This line applies to servers located in Asia Pacific (currently, Hong Kong and Singapore are supported).
IP Type	● IPv4: To protect an IPv4 origin server, you need to select IPv4. ● IPv6: To protect an IPv6 origin server, you need to select IPv6. Only IPv4 addresses can be protected outside the Chinese mainland.

Parameter	Description
Protection package	This parameter is available only in areas outside the Chinese mainland. ● Basic protection: provides advanced protection twice a month for services with low DDoS attack risks. ● Unlimited protection: provides advanced protection for unlimited times, which is suitable for defending against services with high DDoS attack risks.
Basic Protection Bandwidth	The basic protection bandwidth is purchased by customers. If the peak attack traffic is less than or equal to the basic protection bandwidth, customers do not need to pay extra fees. To achieve enhanced protection, use the **Elastic Protection Bandwidth** parameter.
Elastic Protection Bandwidth	If you set this parameter to a value larger than the basic protection bandwidth, additional charges ensue when attack traffic exceeding the basic protection bandwidth is scrubbed. You can modify the elastic protection bandwidth as needed after you have purchased an AAD instance. **NOTE** The elastic protection bandwidth must be greater than or equal to the basic protection bandwidth. If the two are set to the same value, the elastic protection bandwidth function does not take effect.
Protected Domain Names	This parameter is available only when **Access Type** is set to **Website**. By default, 50 ports are provided. You can pay for more. A maximum of 200 ports are supported.
Forwarding Rules	This parameter is available only when the access type is **IP Access**. ● Chinese mainland: 50 are provided by default. You can pay for more rules. A maximum of 500 rules are supported. ● Outside the Chinese mainland: 5 are by default. You can pay for more rules. A maximum of 200 rules are supported.

Parameter	Description
Service Bandwidth	Specifies the service bandwidth for the AAD instance to forward scrubbed traffic to origin servers. The value ranges from **100 Mbit/s** to **5000 Mbit/s**. Collect statistics on the peak inbound and outbound traffic of all services to be connected to the AAD instance. The service bandwidth must be greater than both the peak inbound and outbound traffic. **CAUTION** If the service bandwidth of your instance is lower than peak inbound or outbound traffic, packet loss may occur and your services may be affected. In this case, upgrade the service bandwidth in a timely manner. For details about upgrading specifications, see **Upgrading Instance Specifications**. Assume that you have two services (service A and service B) to access AAD. The peak traffic of service A does not exceed 50 Mbit/s, and the peak traffic of service B does not exceed 70 Mbit/s. The total traffic does not exceed 120 Mbit/s. In this case, you only need to ensure that the maximum service bandwidth of the purchased instance is greater than 120 Mbit/s.

Step 6 Set **Required Duration** and **Quantity**, as shown in **Figure 3-4**. **Table 3-4** describes the parameters.

Figure 3-4 Setting **Required Duration** and **Quantity**



Instance Name: CAD-8c5e

If you create multiple instances at a time, the system will automatically add a suffix to each instance name, for example, CAD-0001.

Enterprise Project: default

Required Duration: 1 month

□ Auto-renew

Quantity: 1

You can create 18 more instances. To apply for a higher quota, submit a service ticket.

Table 3-4 Parameter description

Parameter	Description	Example Value
Instance Name	Enter a name for the AAD instance you are purchasing. ● The name can contain a maximum of 32 characters. ● The name can contain only letters, digits, underscores (_), and hyphens (-).	CAD-0001
Enterprise Project	This option is only available when you are logged in using an enterprise account, or when you have enabled enterprise projects. To learn more, see **Enabling the Enterprise Center**. You can use enterprise projects to more efficiently manage cloud resources and project members. **NOTE** ● **default**: indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are listed in the default enterprise project. ● The **default** option is available in the **Enterprise Project** drop-down list when you purchase AAD with a registered Huawei Cloud account.	N/A
Required Duration	Set this parameter as required.	N/A
Quantity	Select the number of instances to be purchased. By default, each user can purchase a maximum of five instances.	1

NOTE

The **Auto-renew** option is optional. If you tick **Auto-renew**, the system will automatically renew the AAD instance before it expires.

Step 7 Click **Next**.

Step 8 On the **Details** page, select the agreement and click **Submit Order**.

NOTE

For regions outside the Chinese mainland, the payment can be made only after the order is approved.

Step 9 Pay for the order on the payment page.

----End

3.3.2 Purchasing an AAD Instance (International Edition)

If your servers frequently experience DDoS attacks, particularly those with high traffic, the AAD International Edition can offer you with continuous protection to maintain service continuity.

After purchasing the service, you need only to perform simple operations to access gain protection capabilities. This service is suitable for servers deployed outside the Chinese mainland.

NOTICE

- After you purchase an AAD instance, refunds are not supported.
- If an AAD instance has expired for more than 30 calendar days, AAD will stop forwarding service traffic and the instance will become invalid. If you do not need to use AAD anymore, switch your service traffic from AAD to the origin server 30 calendar days before the expiration date.

Limitations and Constraints

- Each user can purchase a maximum of five instances by default. If the quota is insufficient, **submit a service ticket** to apply for a higher quota.
- If your service servers are located in Chinese Mainland, you are advised to purchase AAD. You have obtained an ICP license for your domain names to be protected by AAD.
- If your service servers are located outside Chinese mainland, you are advised to purchase AAD (International Edition).
- Currently, you can only purchase and renew AAD International Edition instances and manage domain name access via the console. Configuration of protection policies or alarm notifications is not available.

Prerequisites

The account must have the permissions of the **CAD Administrator** and **BSS Administrator** roles.

Purchasing an AAD Instance (International Edition)

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

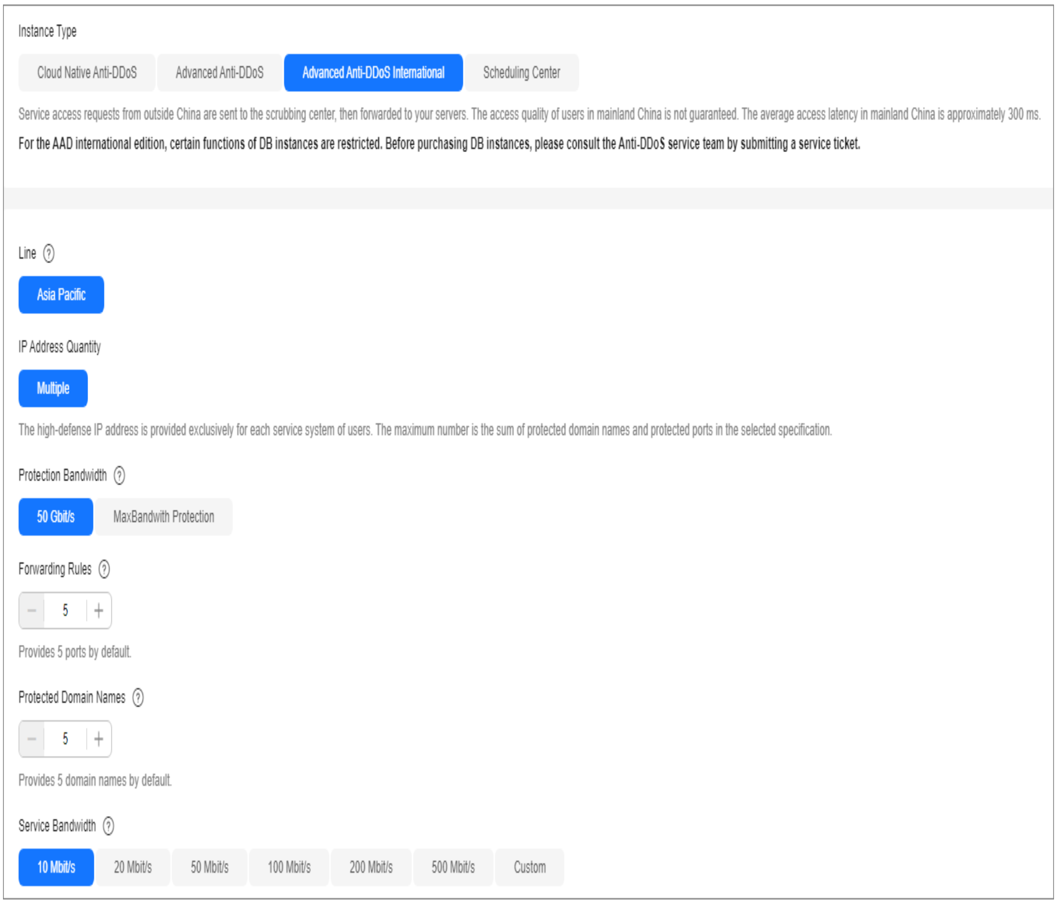
Step 2 Select a region in the upper part of the page, click ☰ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

Step 3 In the upper right corner of the page, click **Buy DDoS Mitigation**.

Step 4 On the **Buy AAD** page, set **Instance Type** to **Advanced Anti-DDoS International**.

Step 5 Set the specifications of the AAD instance, as shown in **Figure 3-5**. **Table 3-5** describes the parameters.

Figure 3-5 Purchasing an AAD instance (international edition)



Instance Type: Advanced Anti-DDoS International

Service access requests from outside China are sent to the scrubbing center, then forwarded to your servers. The access quality of users in mainland China is not guaranteed. The average access latency in mainland China is approximately 300 ms.

For the AAD international edition, certain functions of DB instances are restricted. Before purchasing DB instances, please consult the Anti-DDoS service team by submitting a service ticket.

Line: Asia Pacific

IP Address Quantity: Multiple

The high-defense IP address is provided exclusively for each service system of users. The maximum number is the sum of protected domain names and protected ports in the selected specification.

Protection Bandwidth: 50 Gbit/s

Forwarding Rules: 5

Provides 5 ports by default.

Protected Domain Names: 5

Provides 5 domain names by default.

Service Bandwidth: 10 Mbit/s

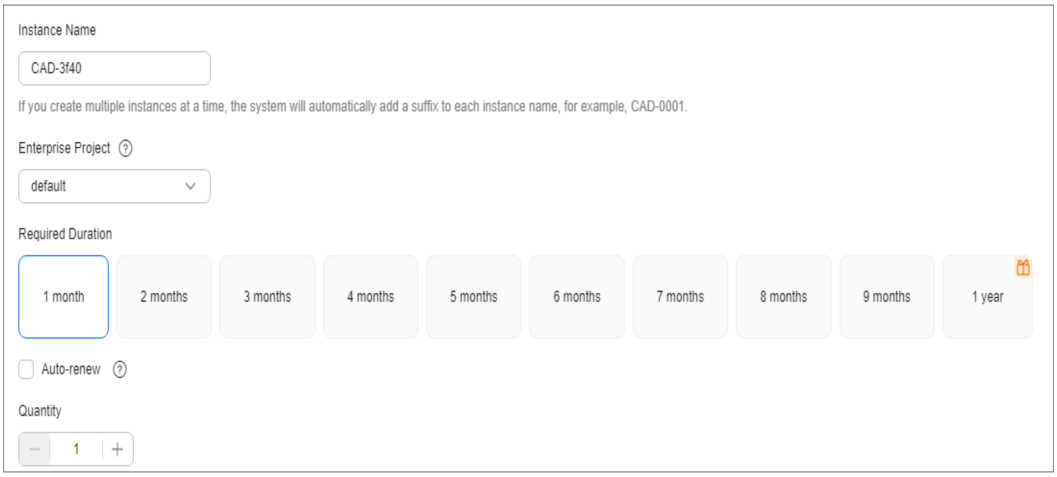
Table 3-5 Parameters for purchasing an AAD instance

Parameter	Description
Line	Currently, **Asia Pacific** is supported.
IP Address Quantity	The default value is **Multiple**. AAD provides exclusive high-defense IP addresses (used to provide services in place of the origin server IP address) for each of customer's service systems. The maximum number is the sum of protected domain names and protected ports in the selected specification.
Protection Bandwidth	**50 Gbit/s**: provides a maximum of 50 Gbit/s protection capacity. Unlimited Protection: An AAD cluster uses all available resources for full protection. However, if the attack exceeds the available protection capability of the cluster, black holes may still be triggered.
Forwarding Rules	By default, five IP addresses are provided. A maximum of 50 IP addresses can be selected.
Protected Domain Names	By default, five IP addresses are provided. A maximum of 50 IP addresses can be selected.

Parameter	Description
Service Bandwidth	Service bandwidth specifies the maximum bandwidth used by AAD scrubbing center to forward the scrubbed traffic to the origin server. ● The service bandwidth ranges from 10 Mbit/s to 5000 Mbit/s. ● 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.

Step 6 Set **Required Duration** and **Quantity**, as shown in **Figure 3-6**. **Table 3-6** describes the parameters.

Figure 3-6 Setting **Required Duration** and **Quantity**



Instance Name

CAD-3f40

If you create multiple instances at a time, the system will automatically add a suffix to each instance name, for example, CAD-0001.

Enterprise Project ?

default

Required Duration

□ Auto-renew ?

Quantity

− 1 +

Table 3-6 Parameter description

Parameter	Description	Example Value
Instance Name	Enter a name for the AAD instance you are purchasing. ● The name must be 32 or fewer characters in length. ● The name can contain only letters, digits, underscores (_), and hyphens (-).	CAD-0001

Parameter	Description	Example Value
Enterprise Project	This option is only available when you are logged in using an enterprise account, or when you have enabled enterprise projects. To learn more, see **Enabling Enterprise Center**. You can use enterprise projects to more efficiently manage cloud resources and project members. **NOTE** ● **default**: indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are listed in the default enterprise project. ● The **default** option is available in the **Enterprise Project** drop-down list when you purchase AAD with a registered Huawei Cloud account.	-
Required Duration	Select a period from three months to one year.	3
Quantity	Select the number of instances to be purchased. By default, each user can purchase a maximum of five instances.	1

NOTE

The **Auto-renew** option is optional. If you tick **Auto-renew**, the system will automatically renew the AAD instance before it expires.

Step 7 Click **Next**.

Step 8 After the order is approved, go to the **Details** page and click **Submit Order**.

Step 9 Pay for the order on the payment page.

----End

3.4 Connecting Services to AAD

3.4.1 Overview

AAD supports domain name and IP address access. The differences between the two access modes are as follows:

Table 3-7 AAD access modes

Access Mode	Applicable Scenario	Major Differences
Domain name access	If your services use domain names licensed by ICMP, you can connect the domain names to AAD.	Huawei Cloud uses algorithms to select the optimal access point for you and does not provide fixed high-defense IP addresses. If you use this mode, you are advised to purchase an instance that uses domain name access.
IP access	If your services use IP addresses rather than domain names, you can configure forwarding rules to connect your services to AAD.	AAD provides IP port protection and fixed high-defense IP addresses. This type is recommended for users using "Layer 4 Forwarding Rules".

NOTICE

Incorrect configurations during service access may cause protection failures or service interruptions. Exercise caution when performing this operation.

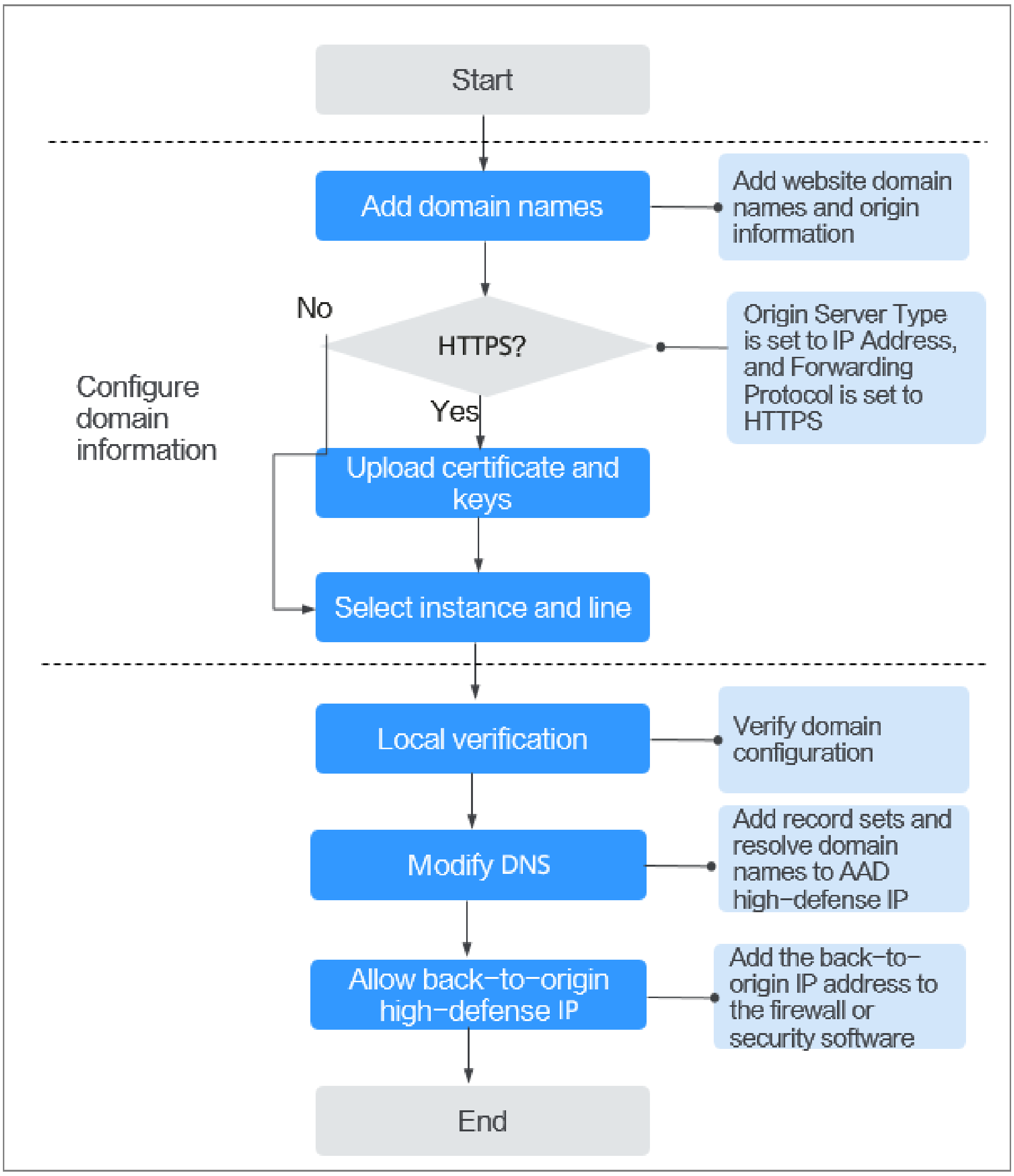
3.4.2 Connecting Domain Name-based Website Services to AAD

If your services are provided via a domain name licensed by ICMP, you can connect the domain name to AAD to safeguard against heavy-traffic DDoS attacks.

Process of Connecting Website Services to AAD

Figure 3-7 shows the process of connecting website services to AAD.

Figure 3-7 Process of connecting website services to AAD


Start
Add domain names
Add website domain names and origin information
No
HTTPS?
Origin Server Type is set to IP Address, and Forwarding Protocol is set to HTTPS
Yes
Configure domain information
Upload certificate and keys
Select instance and line
Local verification
Verify domain configuration
Modify DNS
Add record sets and resolve domain names to AAD high-defense IP
Allow back-to-origin high-defense IP
Add the back-to-origin IP address to the firewall or security software
End

Limitations and Constraints

- If the server protocol is HTTPS, you need to upload a certificate. Currently, AAD supports only certificates in PEM format.
- A CNAME record is generated based on the domain name. For the same domain name, the CNAME records are the same.
- If the origin server domain name is a CNAME, only a CNAME of Huawei Cloud WAF is supported.
- You can select multiple lines (high-defense IP addresses) for a domain name. When selecting multiple high-defense IP addresses, ensure that the number of forwarding rules, the forwarding protocol, forwarding port, and service type configured for each AAD IP address are the same.

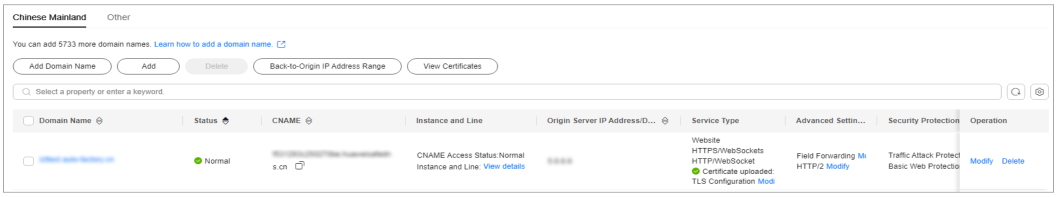
Step 1. Adding a Domain Name

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-8 Domain name access



Chinese Mainland | Other

You can add 5733 more domain names. Learn how to add a domain name.

Add Domain Name | Add | Delete | Back-to-Origin IP Address Range | View Certificates

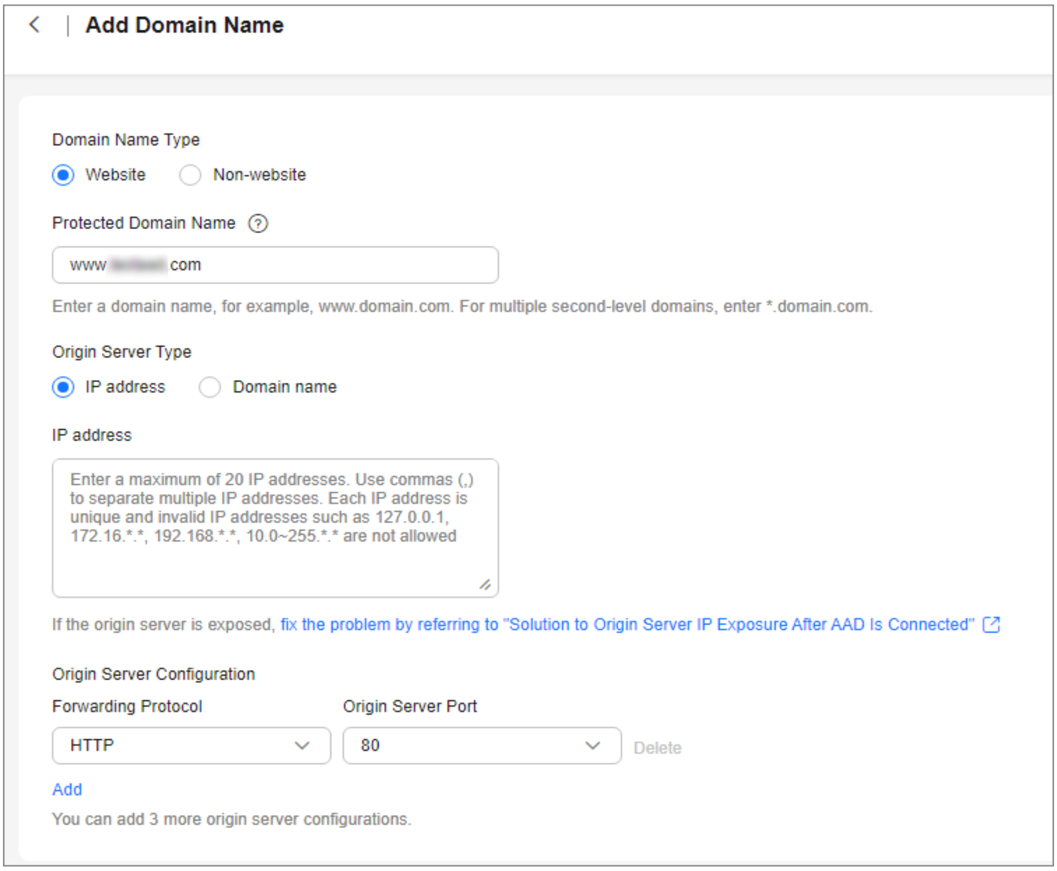
Select a property or enter a keyword.

Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/D...	Service Type	Advanced Settin...	Security Protection	Operation
[redacted]	Normal	[redacted] s.cn	CNAME Access Status:Normal Instance and Line: View details	[redacted]	Website HTTPS/WebSockets HTTP/WebSocket Certificate uploaded: TLS Configuration Modi	Field Forwarding Mo HTTP/2 Modify	Traffic Attack Protect Basic Web Protectio	Modify Delete

Step 4 On the displayed page, click **Add Domain Name**.

Step 5 On the **Add Domain Name** page, configure domain name information, as shown in Figure 3-9. Table 3-8 describes the parameters.

Figure 3-9 Configuring a website domain name



Add Domain Name

Domain Name Type

● Website ○ Non-website

Protected Domain Name

www[redacted]com

Enter a domain name, for example, www.domain.com. For multiple second-level domains, enter *.domain.com.

Origin Server Type

● IP address ○ Domain name

IP address

Enter a maximum of 20 IP addresses. Use commas (,) to separate multiple IP addresses. Each IP address is unique and invalid IP addresses such as 127.0.0.1, 172.16.*.*, 192.168.*.*, 10.0~255.*.* are not allowed

If the origin server is exposed, fix the problem by referring to "Solution to Origin Server IP Exposure After AAD Is Connected"

Origin Server Configuration

Forwarding Protocol: HTTP

Origin Server Port: 80

Delete

Add

You can add 3 more origin server configurations.

Table 3-8 Domain name parameters

Parameter	Description	Example Value
Protected Domain Name	Enter the domain name of the service to protect. ● Single domain name: Enter a single domain name, for example, www.example.com. ● Wildcard domain name – If the server IP address of each subdomain name is the same, enter a wildcard domain name. For example, if the subdomain names ***a.example.com***, ***b.example.com***, and ***c.example.com*** have the same server IP address, you can directly add the wildcard domain name ****.example.com*** to AAD for protection. – If the server IP addresses of subdomain names are different, add subdomain names one by one.	Single domain name: **www.example.com** Wildcard domain name: ***.example.com**

Parameter	Description	Example Value
Origin Server Type	Type of the origin server. ● **IP address**: Public IP address of the origin server. Enter a maximum of 20 IP addresses and separate them using commas (,). ● **Domain name** Currently, only Huawei Cloud WAF CNAMEs are supported. ● **Forwarding Protocol** Protocol used by AAD to forward requests from clients (such as browsers) The options are **HTTP** and **HTTPS**. ● **Origin Server Port** Port used by AAD to forward client requests to the server **NOTICE** ● If the protected domain name to be added shares the high-defense IP address and protocol or port with another domain name, the values for the **Origin Server Type** of these domain names must be the same. – If **Origin Server Type** is of the other domain name is set to **IP address**, ensure the web protection is enabled for that domain name. For details about how to enable the web protection, see **Enabling Basic Web Protection**. – If **Origin Server Type** of the other domain name is set to **Domain name**, ensure that the two domain names are connected to the same WAF region. – Do not alter or remove the CNAME details of the first origin server on WAF. Should changes be necessary, first remove the related domain name details in AAD, then proceed with modifications or deletions in the WAF settings. ● If **Origin Server Type** is set to **Domain name**, ensure that the domain name has been allowed to use a proxy. Otherwise, the service may be unavailable after being connected to AAD. ● If you connect your service to AAD using a WAF CNAME but no longer need WAF protection, delete the service domain name from AAD first.	Origin server IP address: *XXX.XXX*.1.1 Forwarding Protocol: HTTP **Origin Server Port**: **80**
Certificate Name	If **Origin Server Type** is set to **IP Address** and **Forwarding Protocol** is set to **HTTPS**, you need to upload a certificate. For details about how to upload a certificate, see **Step 6**.	-

Step 6 (Optional) Upload a certificate.

If **Origin Server Type** is set to **IP Address** and **Forwarding Protocol** is set to **HTTPS**, you need to import a certificate.

You can select an existing certificate from the drop-down list or upload a certificate.

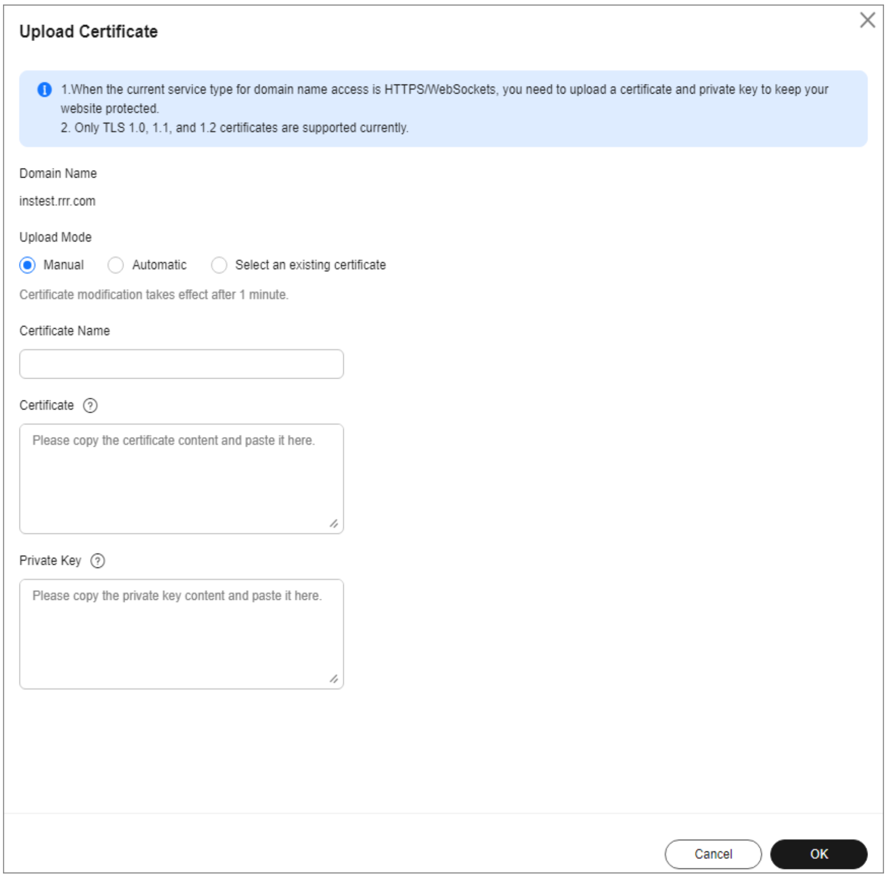
To upload a certificate, perform the following steps:

1. Click **Upload Certificate**. In the displayed **Upload Certificate** dialog box, select a certificate upload mode.
   - **Manual**: Enter the certificate name and paste the certificate and private key text content, as shown in **Figure 3-10**. **Table 3-9** describes the parameters.
   - **Automatic**: Select an issued certificate.

NOTICE

The certificate name contains a maximum of 10 characters and cannot contain special characters.

Figure 3-10 Uploading a certificate



Upload Certificate

1.When the current service type for domain name access is HTTPS/WebSockets, you need to upload a certificate and private key to keep your website protected.
2. Only TLS 1.0, 1.1, and 1.2 certificates are supported currently.

Domain Name
instest.rrr.com

Upload Mode
● Manual ○ Automatic ○ Select an existing certificate
Certificate modification takes effect after 1 minute.

Certificate Name

Certificate
Please copy the certificate content and paste it here.

Private Key
Please copy the private key content and paste it here.

NOTE

- Currently, only TLS 1.0, TLS 1.1, and TLS 1.2 certificates can be uploaded.
- Currently, only .pem certificates are supported.
- Each certificate name of a user must be unique.

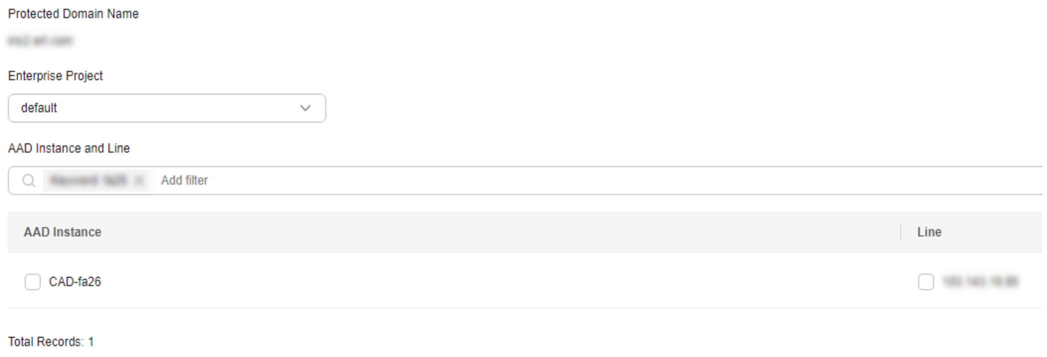
Table 3-9 Parameter description

Parameter	Description
Certificate	– The certificate must be in the following format: -----BEGIN CERTIFICATE----- MIIDljCCAv+gAwIBAgIJAMD2jG2tYGQ6MA0GCSqGSIb3DQEBBQUAMIGPMQswCQYD VQQGEwJDSDELMAkGA1UECBMCWkoxCzAJBgNVBAcTAkhaMQ8wDQYDVQQKEwZodWF3 ZWkxDzANBgNVBAsTBmh1YXdlaTEPMA0GA1UEAxMGaHVhd2VpMQ8wDQYDVQQpEwZz ZXJ2ZXIxIjAgBgkqhkiG9w0BCQEWE3p3YW5nd2VpZGtkQDE2My5jb20wHhcNMTUw MzE4MDMzNjU5WhcNMjUwMzE1MDMzNjU5WjCBjzELMAkGA1UEBhMCQ0gxCzAJBgNV BAgTAlpKMQswCQYDVQQHEwJIWjEPMA0GA1UEChMGaHVhda2VpMQ8wDQY...... -----END CERTIFICATE----- – Method for you to copy your certificate: ■ For a .pem certificate: Use a text editor to open the certificate file and copy the content here. ■ For other certificates: Convert your certificate to a .pem one. Then open it with a text editor and copy its content.
Private Key	The private key must be in the following format: -----BEGIN RSA PRIVATE KEY----- MIIDljCCAv+gAwIBAgIJAMD2jG2tYGQ6MA0GCSqGSIb3DQEBBQUAMIGPMQswCQYDVQQG EwJDSDELMAkGA1UECBMCWkoxCzAJBgNVBAcTAkhaMQ8wDQYDVQQKEwZodWF3ZWkxDzAN BgNVBAsTBmh1YXdlaTEPMA0GA1UEAxMGaHVhd2VpMQ8wDQYDVQQpEwZzZXJ2ZXIxIjAg BgkqhkiG9w0BCQEWE3poYW5nd2VpZGtkQDE2My5jb20wHhcNMTUwMzE4MDMzNjU5WhcN MjUwMzE1MDMzNjU5WjCBjzELMAkGA1UEBhMCQ0gxCzAJBgNVBAgTAlpKMQswCQYDVQQH EwJIWjEPMA0GA1UEChMGaHVhd2VpMQ8wDQYDVQQLEwZ -----END RSA PRIVATE KEY----- – Method for you to copy your private key: ■ For a .pem certificate: Use a text editor to open the certificate file and copy the content here. ■ For other certificates: Convert your certificate to a .pem one. Then open it with a text editor and copy its content.

2. Click **OK**.

Step 7 Click **Next** and select an AAD instance and line, as shown in **Figure 3-11**.

Figure 3-11 Selecting an AAD instance and line



Protected Domain Name

[redacted]

Enterprise Project

default

AAD Instance and Line

[redacted] Add filter

AAD Instance	Line
☐ CAD-fa26	☐ [redacted]

Total Records: 1

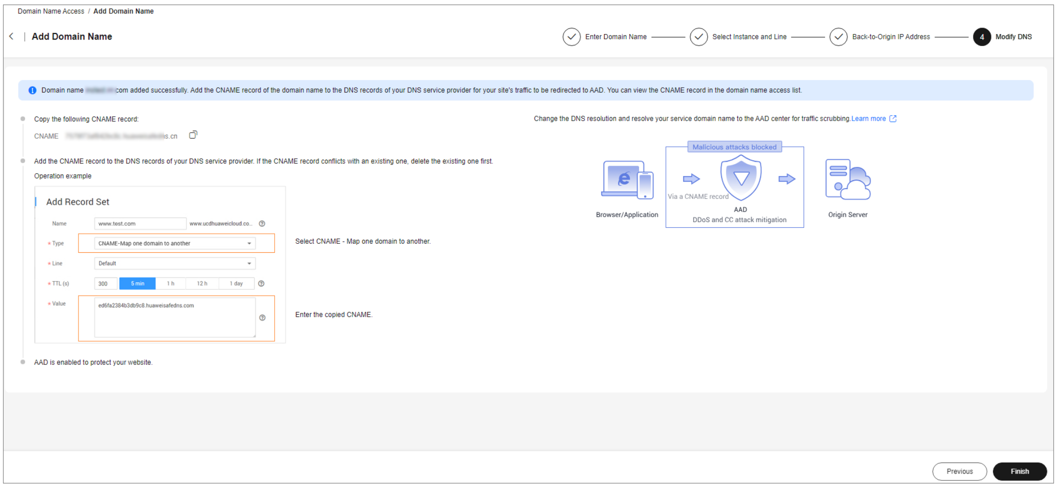
NOTICE

- You can select multiple lines (AAD IP addresses) for a domain name. When selecting multiple AAD IP addresses, ensure that the number of forwarding rules, the forwarding protocol, forwarding port, and service type configured for each AAD IP address are the same.

Step 8 Click **Submit and Continue**. A dialog box is displayed, as shown in **Figure 3-12**.

You are advised to click **Next** to skip this step. You can configure DNS later according to **Step 4: Modifying DNS Resolution**.

Figure 3-12 Modifying DNS



Domain Name Access / **Add Domain Name**

Add Domain Name

✓ Enter Domain Name — ✓ Select Instance and Line — ✓ Back-to-Origin IP Address — 4 Modify DNS

Domain name [redacted]com added successfully. Add the CNAME record of the domain name to the DNS records of your DNS service provider for your site's traffic to be redirected to AAD. You can view the CNAME record in the domain name access list.

- Copy the following CNAME record:

  CNAME [redacted]s.cn

- Add the CNAME record to the DNS records of your DNS service provider. If the CNAME record conflicts with an existing one, delete the existing one first.

  Operation example

  Add Record Set

Name	www.test.com www.ucdhuaweicloud.co...	
* Type	CNAME-Map one domain to another	Select CNAME - Map one domain to another.
* Line	Default	
* TTL (s)	300 [5 min] 1 h 12 h 1 day	
* Value	ed6fa2384b3db9c8.huaweisafedns.com	Enter the copied CNAME.

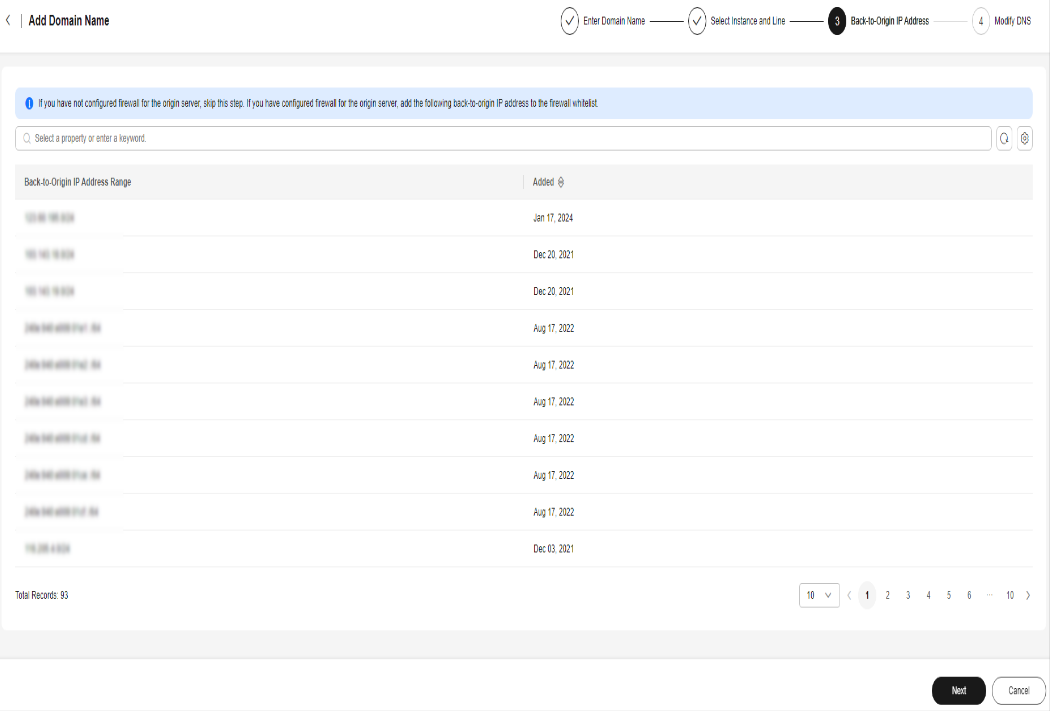
- AAD is enabled to protect your website.

Change the DNS resolution and resolve your service domain name to the AAD center for traffic scrubbing. Learn more

Step 9 Click **Finish** to complete the configuration.

After the domain name is configured, the **Domain Name Access** is automatically displayed. You can view the added domain name in the domain name list.

Figure 3-13 Back-to-origin IP address



If you have not configured firewall for the origin server, skip this step. If you have configured firewall for the origin server, add the following back-to-origin IP address to the firewall whitelist.

Select a property or enter a keyword.

Back-to-Origin IP Address Range	Added
[redacted]	Jan 17, 2024
[redacted]	Dec 20, 2021
[redacted]	Dec 20, 2021
[redacted]	Aug 17, 2022
[redacted]	Aug 17, 2022
[redacted]	Aug 17, 2022
[redacted]	Aug 17, 2022
[redacted]	Aug 17, 2022
[redacted]	Aug 17, 2022
[redacted]	Dec 03, 2021

Total Records: 93

If a firewall has been configured or security software has been installed on the origin server, add the back-to-origin IP address to the firewall or security software, so as to ensure that the back-to-origin IP address is not affected by the security policies set on the origin server. For details, see **Step 2: Adding the Back-to-Origin IP Address Range to the Whitelist**.

NOTICE

AAD replaces customers' real IP addresses and diverts access traffic to the back-to-origin IP addresses.

- If AAD is not used, access traffic is sent directly from the source IP addresses of clients towards origin servers. From the view of origin servers, the requests originate from scattered clients and each source IP address sends only a few access requests.
- After AAD is enabled, access traffic will be forwarded to the back-to-origin IP addresses. From the view of origin servers, the requests originate from these back-to-origin IP addresses. These IP addresses are fixed and limited in quantity, and each carries more requests than the source IP address. Therefore, they may be mistakenly regarded as the sources that launch attacks. In this case, other anti-DDoS security policies working on the origin servers may block or limit the requests from the back-to-origin IP addresses. For example, error 502 is reported if the access request is blocked by mistake.

----End

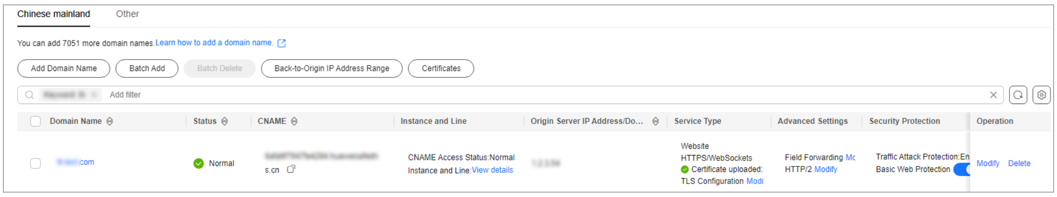
Step 2: Adding the Back-to-Origin IP Address Range to the Whitelist

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-14 Domain name access



Chinese mainland | Other

You can add 7051 more domain names. Learn how to add a domain name.

Add Domain Name | Batch Add | Batch Delete | Back-to-Origin IP Address Range | Certificates

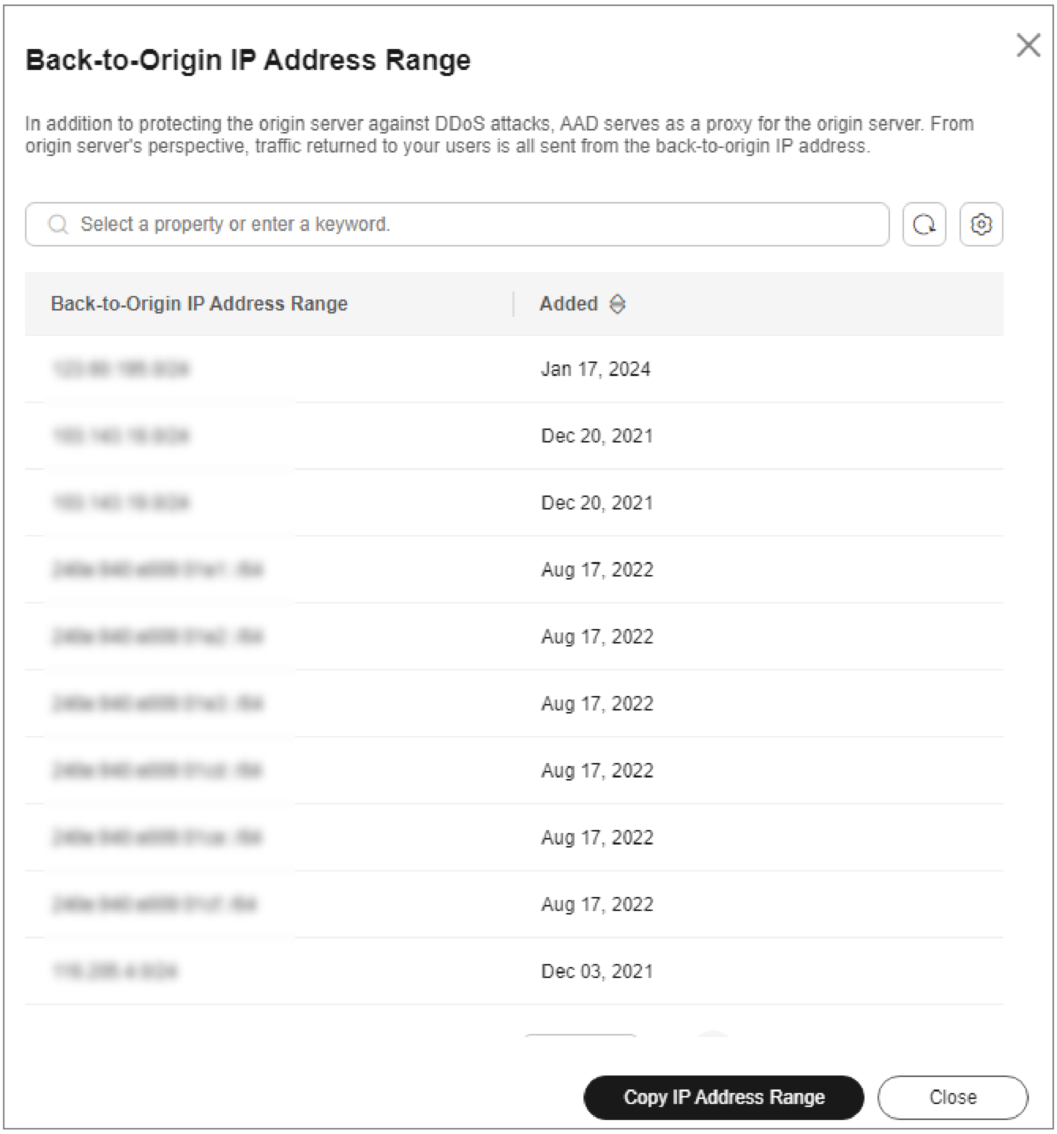
[redacted] Add filter

□	Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Operation
□	[redacted]com	Normal	[redacted] s.cn	CNAME Access Status:Normal Instance and Line:View details	[redacted]	Website HTTPS/WebSockets Certificate uploaded: TLS Configuration Modi	Field Forwarding Mc HTTP/2 Modify	Traffic Attack Protection:En Basic Web Protection	Modify Delete

Step 4 On the displayed page, click **Back-to-Origin IP Address Range**.

Step 5 In the **Back-to-Origin IP Address Segment** dialog box, view information about the back-to-origin IP address segment.

Figure 3-15 Viewing the back-to-origin IP address range



Back-to-Origin IP Address Range

In addition to protecting the origin server against DDoS attacks, AAD serves as a proxy for the origin server. From origin server's perspective, traffic returned to your users is all sent from the back-to-origin IP address.

Select a property or enter a keyword.

Back-to-Origin IP Address Range	Added
[redacted]	Jan 17, 2024
[redacted]	Dec 20, 2021
[redacted]	Dec 20, 2021
[redacted]	Aug 17, 2022
[redacted]	Aug 17, 2022
[redacted]	Aug 17, 2022
[redacted]	Aug 17, 2022
[redacted]	Aug 17, 2022
[redacted]	Aug 17, 2022
[redacted]	Dec 03, 2021

Step 6 Add the back-to-origin IP address to the whitelist of the firewall or security software on the origin server.

----End

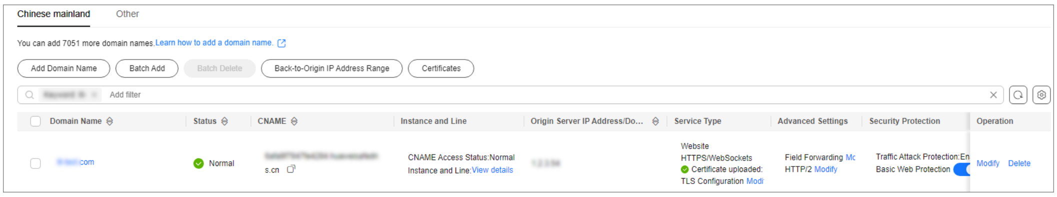
Step 3: Verifying the Domain Name Access Status

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-16 Domain name access



Chinese mainland | Other

You can add 7051 more domain names. Learn how to add a domain name.

Add Domain Name | Batch Add | Batch Delete | Back-to-Origin IP Address Range | Certificates

[redacted] Add filter

□	Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Operation
□	[redacted]com	✓ Normal	[redacted] s.cn	CNAME Access Status:Normal Instance and Line:View details	[redacted]	Website HTTPS/WebSockets ✓ Certificate uploaded: TLS Configuration Modi	Field Forwarding Mc HTTP/2 Modify	Traffic Attack Protection:En Basic Web Protection	Modify Delete

Step 4 In the **CNAME** column of the target domain name, click ⧉ to copy the CNAME value of the domain name.

Step 5 Enable Telnet and run the following command to check the connectivity between the origin server and AAD:

telnet *Origin_server_IP_address* **80**

Take the **port 80** as an example.

- If the connection setup is successful, you can Telnet to the public IP address from your local network environment.
- If the connection setup fails, change your test network environment and try again. Some enterprises may have internal network constraints that cause the failure of the verification. For example, you can connect to the personal hotspot of your phone to verify the connectivity.

Step 6 Run the following command to check whether the configuration for connecting the domain name to AAD is correct:

telnet *the_CNAME_value_copied_in_**Step 4*** **80**

- If you can telnet the domain name, the configuration is correct.
- If you fail to telnet the domain name, check whether the domain name parameters are correctly configured.

NOTE

For details about how to verify whether WAF basic protection is enabled, see **Testing WAF**.

----End

Step 4: Modifying DNS Resolution

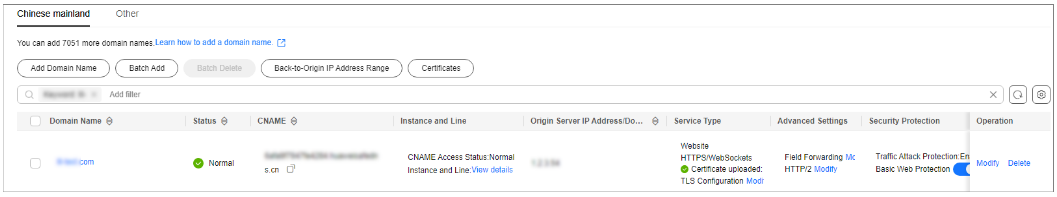
After obtaining the CNAME value of the protected domain name, add the value to the DNS record set.

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

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-17 Domain name access



Chinese mainland | Other

You can add 7051 more domain names. Learn how to add a domain name.

Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Operation
[redacted]com	Normal	[redacted]s.cn	CNAME Access Status:Normal Instance and Line:View details	[redacted]	Website HTTPS/WebSockets Certificate uploaded: TLS Configuration Modi	Field Forwarding Mc HTTP/2 Modify	Traffic Attack Protection:En Basic Web Protection	Modify Delete

Step 4 In the **CNAME** column of the target domain name, click ⧉ to copy the CNAME value of the domain name.

Step 5 Click ☰ in the upper left corner of the page and choose **Networking** > **Domain Name Service**.

Step 6 For details, see section **Adding a CNAME Record Set**.

----End

3.4.3 Connecting Non-Domain Name Services to AAD

If your service does not have a domain name and provides services only through a public IP address, you can configure forwarding rules to connect your service to Advanced Anti-DDoS (AAD). After forwarding rules are configured, a high-defense IP address automatically forwards traffic to the origin server IP address. In this way, the origin server is hidden from heavy-traffic DDoS attacks.

Limitations and Constraints

- An origin server IP address can be added to multiple forwarding rules.
- The forwarding protocol and forwarding port in each forwarding rule must be unique.
- During batch configuration of forwarding rules, only **.txt** files can be imported. The number of forwarding rules in the file cannot exceed the quota limit. Within the quota limit, a maximum of 200 rules can be imported at a time.

Connecting IP-based Services to AAD

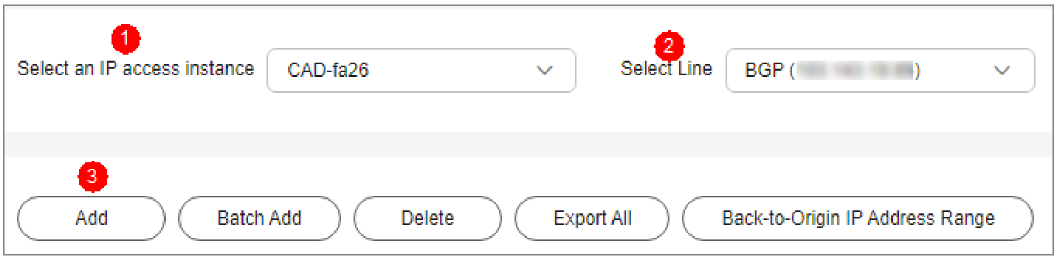
Step 1 **Log in to the management console**.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Forwarding Configuration**.

Step 4 Select the instance and line for which you want to add a forwarding rule, and click **Add**.

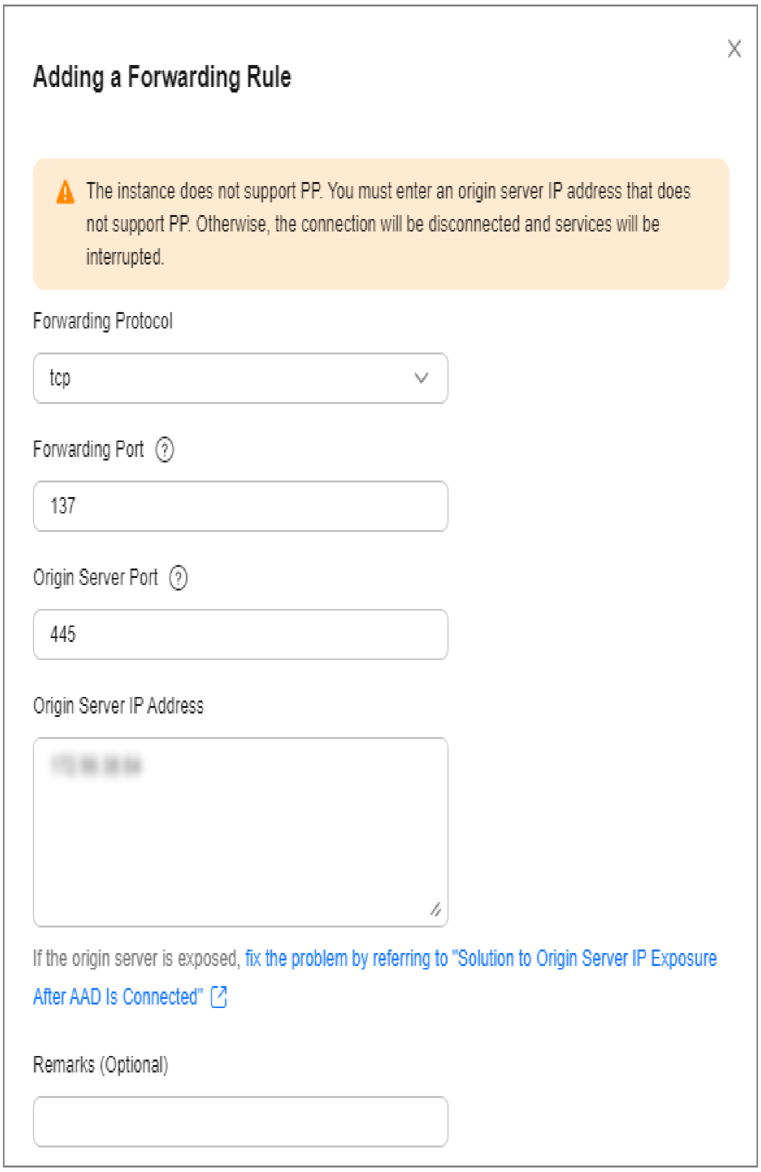
Figure 3-18 Selecting an instance and line



Select an IP access instance: CAD-fa26

Select Line: BGP ([redacted])

Step 5 Enter the forwarding information based on the site requirements.



Adding a Forwarding Rule

The instance does not support PP. You must enter an origin server IP address that does not support PP. Otherwise, the connection will be disconnected and services will be interrupted.

Forwarding Protocol: tcp

Forwarding Port: 137

Origin Server Port: 445

Origin Server IP Address: [redacted]

If the origin server is exposed, fix the problem by referring to "Solution to Origin Server IP Exposure After AAD Is Connected"

Remarks (Optional)

Table 3-10 Parameter description

Parameter	Description
Forwarding Protocol	Specifies the protocol used to forward user service workload. ● **tcp**: TCP is a connection-oriented protocol that provides reliable delivery of a stream of bytes at the transport layer. ● **udp**: UDP is a connectionless protocol that provides simple transaction-oriented delivery of messages at the transport layer.
Forwarding Port	Specifies the port used to forward user service workload.
Origin Server Port	Specifies the port used by the origin server.
Origin Server IP Address	Specifies the public IP address used by the origin server. ● After configuring the rules, change the domain names based on your services. AAD will automatically forward traffic to your origin server IP addresses. ● You can add a maximum of 20 origin server IP addresses. Separate them with commas (,). ● Enter a valid public IP address.

⚠ CAUTION

Some carriers will block the following ports for security reasons. It is recommended that you do not use the following ports.

- TCP: 42, 135, 137-139, 444, 445, 593, 1025, 1068, 1434, 3127-3130, 3332, 4444, 4789, 4790, 5554, 5800, 5900, 6669, 9996.
- UDP: 135-139, 445, 593, 1026-1028, 1068, 1433, 1434, 4444, 4789, 4790, 5554, 9996, 17185.

Step 6 Confirm the information and click **OK**.

----End

Related Operations

- If a forwarding rule is not needed, see **Delete a Forwarding Rule**.
- To back up a forwarding rule or quickly modify its configuration information, go to **Export Forwarding Rules**.

3.4.4 Protection Suggestions After AAD Is Connected

After connecting services to AAD, ensuring access security is crucial as it impacts the origin server's security and service continuity.

The following content provides some specific suggestions for protecting the origin server and enhancing service availability.

Protection Suggestions

You can take the following measures to reduce the risk of DDoS attacks and improve the security of origin servers. **Table 3-11** and **Table 3-12** describe the main methods.

Figure 3-19 Service architecture

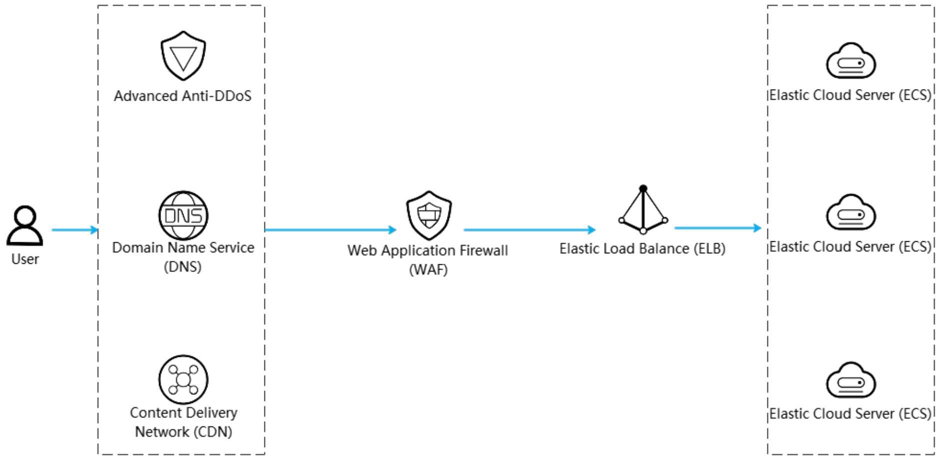

User
Advanced Anti-DDoS
Domain Name Service (DNS)
Content Delivery Network (CDN)
Web Application Firewall (WAF)
Elastic Load Balance (ELB)
Elastic Cloud Server (ECS)
Elastic Cloud Server (ECS)
Elastic Cloud Server (ECS)

Table 3-11 Optimizing security configurations

Hardening Operation	Description
Configuring a security group	Adding an ECS to a security group can effectively reduce irrelevant access requests and reduce attack risks. For details, see **Adding an ECS to a Security Group**.
Using VPCs	You can use virtual private clouds (VPCs) to isolate ECSs, effectively defending against intranet attacks. For details, see **Creating a VPC**.
Enabling AS	With auto scaling (AS), ECSs can be automatically added during an attack, enhancing processing performance and reducing the impact of attacks. For details, see **What Is Auto Scaling?**
Enhancing service monitoring	You can set DDoS alarm rules to customize the monitored objects and notification policies, so that you can learn about the AAD protection status in a timely manner. For details, see **Configuring Monitoring Alarm Rules**.
Enabling CDN scheduling	The DDoS scheduling center facilitates both AAD and CDN scheduling. During regular service access, traffic is directed to the nearest CDN node for acceleration. When an attack occurs, traffic is rerouted to AAD for scrubbing, mitigating DDoS attacks and ensuring service stability. For details, see **Configuring CDN Scheduling Rules**.

Hardening Operation	Description
Enabling WAF	Connect website applications to WAF for collaborative protection with AAD. The traffic is forwarded to WAF after passing through AAD. For details, see **AAD and WAF Interworking** .
Enable HSS	Host Security Service (HSS) monitors host risks in real time and prevents unauthorized intrusions, reducing major security risks. For details, see **Accessing HSS**.
Optimizing DNS resolution	Hosting services to multiple DNS service providers and optimizing DNS resolution policies can effectively mitigate traffic attacks. For details about how to connect your services to the Huawei Cloud DNS service, see **Add an A Record Set for the Domain Name**.

Table 3-12 Hardening the origin server

Scenario	Service Flow	Hardening Description
Services are deployed on Huawei Cloud ECSs.	AAD → Huawei Cloud ECS	Configure **security group rules** to allow all back-to-origin IP addresses of AAD to access the ECS. For details about how to view the DDoS back-to-origin IP address range, see **Step 2: Adding the Back-to-Origin IP Address Range to the Whitelist**.
	AAD → Huawei Cloud ELB → Huawei Cloud ECS	Set access control policies on the ELB console. For details, see **Access Control**.
	AAD → Huawei Cloud WAF → Huawei Cloud ECS	Configure an access control policy on the origin server to allow only the access from the WAF back-to-source IP address range. For details, see **Configuring Security Group Rules**. For details about how to view the back-to-source IP address range of WAF, see **How Do I Whitelist Back-to-Source IP Addresses of Cloud WAF?**

Scenario	Service Flow	Hardening Description
Services are deployed on servers outside Huawei Cloud.	AAD → Origin server outside Huawei Cloud	In the origin server's security software, configure a protection policy to allow only access from IP addresses in the AAD back-to-origin IP address range while denying access from all other IP addresses. For details about how to view the DDoS back-to-origin IP address range, see **Step 2: Adding the Back-to-Origin IP Address Range to the Whitelist**.

3.5 Configuring a Protection Policy

3.5.1 Protection Policy Overview

AAD provides various protection policies. After purchasing an instance, you can select an appropriate protection policy based on service requirements. For details, see **Table 3-13**.

NOTICE

If the protection policy is incorrectly configured, attacks may fail to be defended against or traffic may be incorrectly scrubbed. Exercise caution when performing this operation.

Table 3-13 Protection policies

Protection Scenario	Protection Policy	Section	Description
Basic attack protection	Basic web protection	**Enabling Basic Web Protection**	Once this function is enabled, you can use the layer-7 CC attack protection capabilities provided by AAD. Additionally, if you need to add multiple domain names whose origin server type is IP address to AAD, ensure that this function is also enabled.

Protection Scenario	Protection Policy	Section	Description
DDoS attack protection	Blacklist and whitelist	**Blocking or Allowing Traffic From Specified IP Addresses Using a Blacklist and Whitelist**	Configure an IP address blacklist or whitelist to block or allow source IP addresses that access AAD, thereby controlling which users can access your service resources.
	Protocol-based access block	**Blocking Traffic of a Specified Protocol**	You can use the traffic control rules to allow or block UDP traffic or Traffic Outside Chinese Mainland that accesses your AAD instances.
	Geo-blocking	**Blocking Traffic From Specified Locations**	AAD can block traffic from specified geographic regions. Once the policy is in effect, access traffic from the designated region will be discarded.
Web CC protection	Intelligent CC	**Using Intelligent CC Policies to Defend Against CC Attacks**	Automated defense against CC attacks with security rules generated by WAF. If you enable intelligent access control, it takes 10 to 15 minutes for WAF to learn how much traffic your website can handle and generate a rule for you.
	Frequency control rules	**Mitigating CC Attacks Using Frequency Control Policies**	You can establish a frequency control rule to restrict the access frequency of a single IP address, cookie, or referer to the source end of the protected website, thereby effectively mitigating CC attacks.

3.5.2 Enabling Basic Web Protection

Once a domain name is connected to AAD, you can enable basic web protection for the corresponding origin server IP address. With basic web protection enabled, you can then use the layer-7 CC attack protection capabilities provided by AAD.

NOTICE

Enabling or disabling basic web protection may interrupt services. Exercise caution when performing this operation.

Limitations and Constraints

Basic web protection takes effect only for forwarding rules whose service type is **Website** and origin server type is **Origin Server IP Address**.

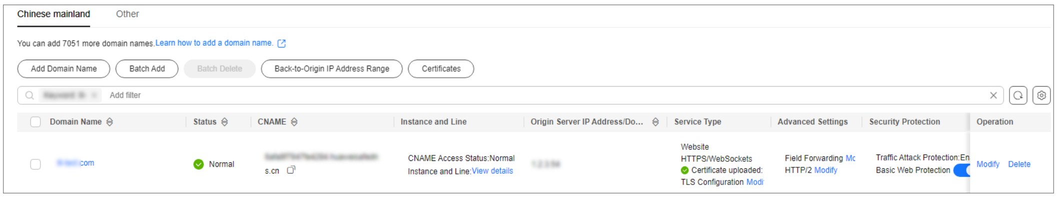
Enabling Basic Web Protection

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-20 Domain name access



Chinese mainland | Other

You can add 7051 more domain names. Learn how to add a domain name.

Add Domain Name | Batch Add | Batch Delete | Back-to-Origin IP Address Range | Certificates

[redacted] Add filter

Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Operation
[redacted]com	Normal	[redacted]s.cn	CNAME Access Status:Normal Instance and Line:View details	[redacted]	Website HTTPS/WebSockets Certificate uploaded: TLS Configuration Modi	Field Forwarding Mc HTTP/2 Modify	Traffic Attack Protection:En Basic Web Protection	Modify Delete

Step 4 Set the status of **Basic Web Protection** to ⬤ to enable basic web protection.

NOTE

Traffic Attack Protection is enabled by default.

----End

3.5.3 Blocking Traffic From Specified Locations

AAD can block traffic from specified geographic regions. Once the policy is in effect, access traffic from the designated region will be discarded.

Limitations and Constraints

AAD allows or blocks traffic outside Chinese Mainland in one-click mode, but cannot block country or region-specific traffic.

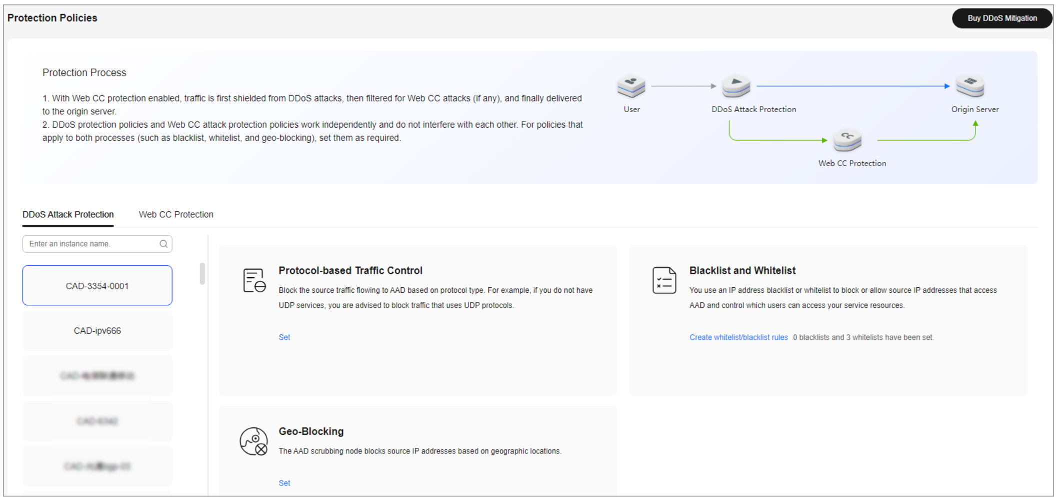
Geo-Blocking

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Protection Policies**. The **Protection Policies** page is displayed.

Figure 3-21 Advanced Anti-DDoS protection policies



Protection Process

1. With Web CC protection enabled, traffic is first shielded from DDoS attacks, then filtered for Web CC attacks (if any), and finally delivered to the origin server.
2. DDoS protection policies and Web CC attack protection policies work independently and do not interfere with each other. For policies that apply to both processes (such as blacklist, whitelist, and geo-blocking), set them as required.

Protocol-based Traffic Control

Block the source traffic flowing to AAD based on protocol type. For example, if you do not have UDP services, you are advised to block traffic that uses UDP protocols.

Set

Blacklist and Whitelist

You use an IP address blacklist or whitelist to block or allow source IP addresses that access AAD and control which users can access your service resources.

Create whitelist/blacklist rules 0 blacklists and 3 whitelists have been set.

Geo-Blocking

The AAD scrubbing node blocks source IP addresses based on geographic locations.

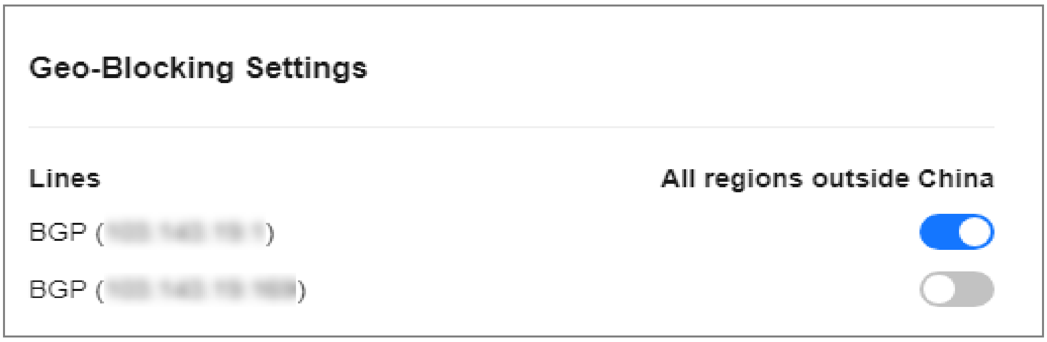
Set

Step 4 Select the instance for which geo-blocking needs to be configured.

Step 5 In the **Geo-Blocking** configuration area, click **Set**.

Step 6 In the displayed dialog box, select a route and select the areas you want to block.

Figure 3-22 Geo-blocking settings



Geo-Blocking Settings

Lines	All regions outside China
BGP ([redacted])	● on
BGP ([redacted])	○ off

Step 7 Click **OK**. The geo-blocking setting is complete.

----End

3.5.4 Blocking Traffic of a Specified Protocol

AAD offers a one-click mode to block traffic based on protocol type. If there is no UDP service, you are advised to disable the UDP protocol.

Once the UDP protocol blocking is enabled, the rate of UDP access traffic will be restricted if it exceeds 2 Mbit/s.

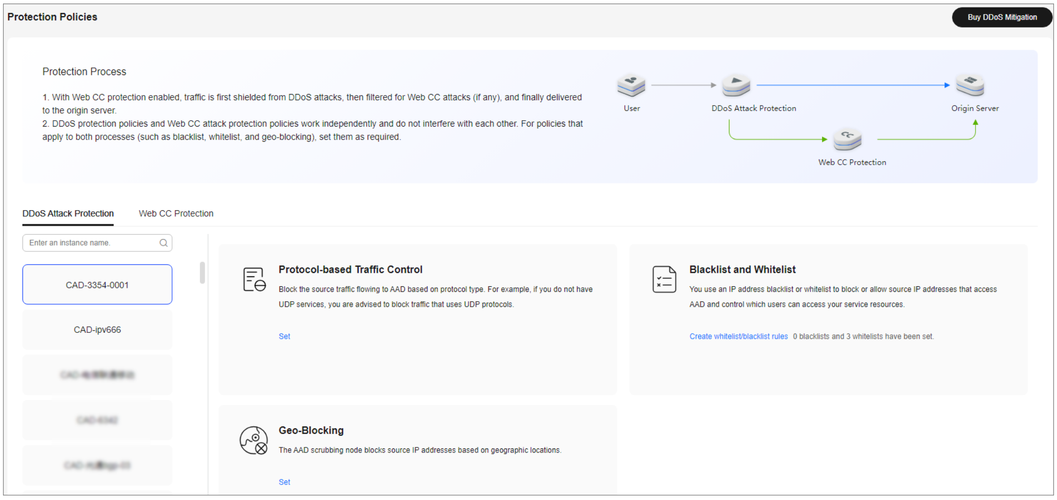
Enabling Protocol Blocking

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Protection Policies**. The **Protection Policies** page is displayed.

Figure 3-23 Advanced Anti-DDoS protection policies



Protection Process

1. With Web CC protection enabled, traffic is first shielded from DDoS attacks, then filtered for Web CC attacks (if any), and finally delivered to the origin server.
2. DDoS protection policies and Web CC attack protection policies work independently and do not interfere with each other. For policies that apply to both processes (such as blacklist, whitelist, and geo-blocking), set them as required.

Protocol-based Traffic Control

Block the source traffic flowing to AAD based on protocol type. For example, if you do not have UDP services, you are advised to block traffic that uses UDP protocols.

Blacklist and Whitelist

You use an IP address blacklist or whitelist to block or allow source IP addresses that access AAD and control which users can access your service resources.

0 blacklists and 3 whitelists have been set.

Geo-Blocking

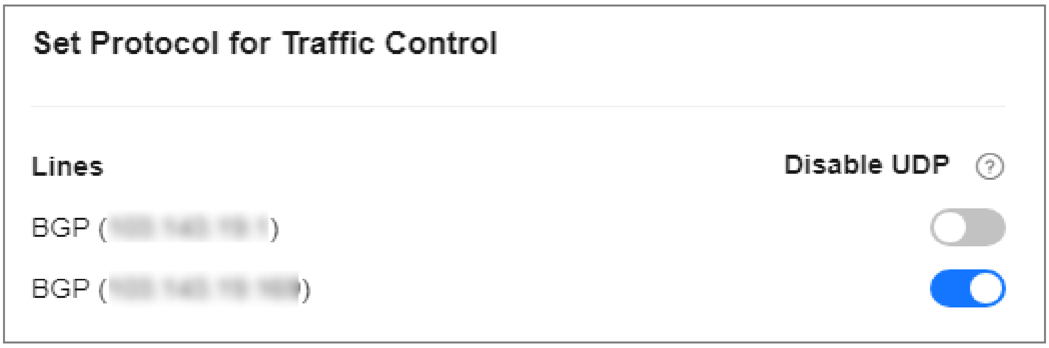
The AAD scrubbing node blocks source IP addresses based on geographic locations.

Step 4 Select the instance for which you want to configure protocol blocking.

Step 5 In the **Protocol-based Traffic Control configuration** area, click **Set**.

Step 6 In the dialog box that is displayed, select a route and set the switch to ● to disable the protocol.

Figure 3-24 Disabling a protocol



Set Protocol for Traffic Control

Lines	Disable UDP
BGP ([redacted])	○
BGP ([redacted])	●

----End

3.5.5 Blocking or Allowing Traffic From Specified IP Addresses Using a Blacklist and Whitelist

You can configure an IP address blacklist or whitelist to block or allow access requests from specified IP addresses.

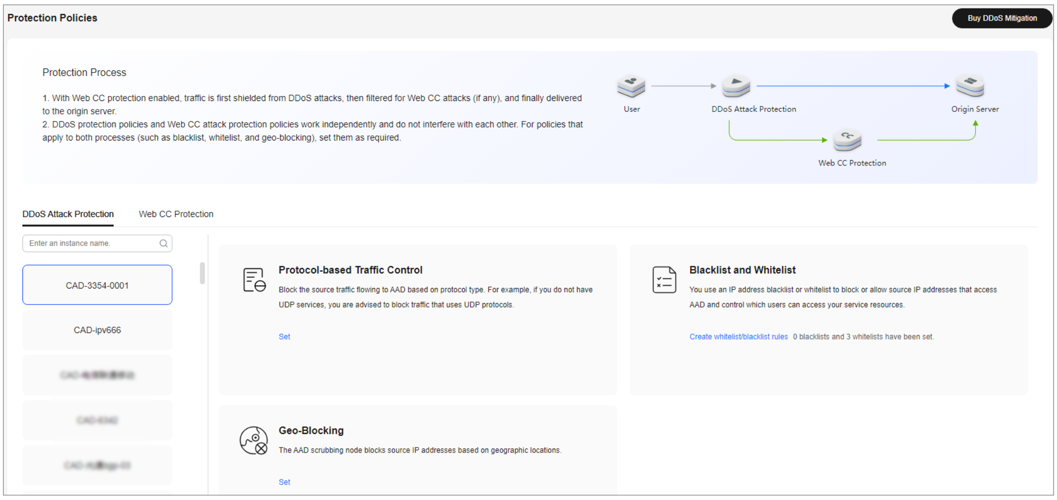
Configuring a Blacklist and a Whitelist

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Protection Policies**. The **Protection Policies** page is displayed.

Figure 3-25 Advanced Anti-DDoS protection policies



Protection Policies

Buy DDoS Mitigation

Protection Process

1. With Web CC protection enabled, traffic is first shielded from DDoS attacks, then filtered for Web CC attacks (if any), and finally delivered to the origin server.
2. DDoS protection policies and Web CC attack protection policies work independently and do not interfere with each other. For policies that apply to both processes (such as blacklist, whitelist, and geo-blocking), set them as required.

DDoS Attack Protection | Web CC Protection

Enter an instance name.

CAD-3354-0001

CAD-ipv666

[redacted]

[redacted]

[redacted]

Protocol-based Traffic Control

Block the source traffic flowing to AAD based on protocol type. For example, if you do not have UDP services, you are advised to block traffic that uses UDP protocols.

Set

Blacklist and Whitelist

You use an IP address blacklist or whitelist to block or allow source IP addresses that access AAD and control which users can access your service resources.

Create whitelist/blacklist rules 0 blacklists and 3 whitelists have been set.

Geo-Blocking

The AAD scrubbing node blocks source IP addresses based on geographic locations.

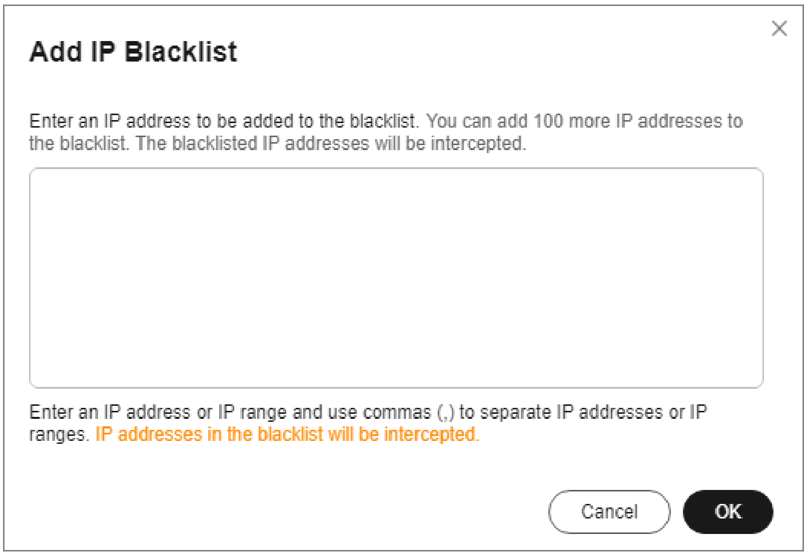
Set

Step 4 Select the instance for which you want to configure a blacklist or whitelist.

Step 5 Configure a blacklist and a whitelist.

- Configuring a Blacklist
  a. In the **Blacklist and Whitelist** configuration area, click **Create whitelist/ blacklist rules**.
  b. Select the **IP Blacklist** tab and click **Add**.
  c. In the displayed dialog box, enter the IP addresses or IP ranges to be blocked.

Figure 3-26 Adding blacklisted IP addresses



Add IP Blacklist

Enter an IP address to be added to the blacklist. You can add 100 more IP addresses to the blacklist. The blacklisted IP addresses will be intercepted.

Enter an IP address or IP range and use commas (,) to separate IP addresses or IP ranges. IP addresses in the blacklist will be intercepted.

NOTE

A maximum of 100 IP addresses can be added to the blacklist of an instance, and IP addresses in the blacklist will be blocked.

d. Click **OK**.

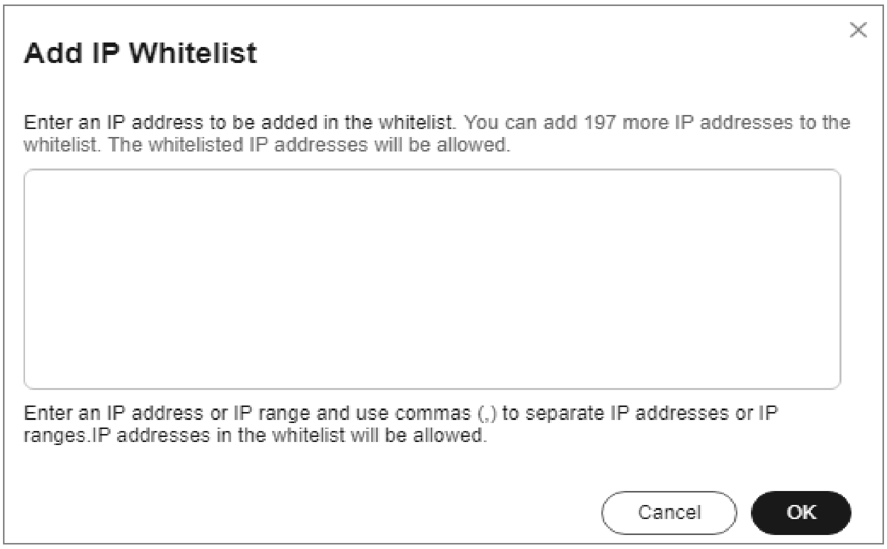
   On the **IP Blacklist** page, click **Delete** in the **Operation** column or select the blacklisted IP addresses to be deleted and click **Delete** to delete IP addresses in batch. Deleted IP addresses will not be blocked.

- Configuring an IP whitelist

  a. Select the **IP Whitelist** tab and click **Add**.

  b. In the displayed dialog box, enter the IP addresses or IP ranges to be permitted.

Figure 3-27 Adding whitelisted IP addresses



Add IP Whitelist

Enter an IP address to be added in the whitelist. You can add 197 more IP addresses to the whitelist. The whitelisted IP addresses will be allowed.

Enter an IP address or IP range and use commas (,) to separate IP addresses or IP ranges.IP addresses in the whitelist will be allowed.

NOTE

- IP addresses/ranges should be separated by commas (,) and must be unique. The number of IP addresses/ranges cannot exceed the remaining quota.
- The mask length of an IPv4 address must be at least 16 bits, and for an IPv6 address, it must be at least 64 bits. Only one subnet segment can be configured at a time.

  c. Click **OK**.

     On the **IP Whitelist** page, click **Delete** in the **Operation** column or select the whitelisted IP addresses to be deleted and click **Delete** to delete IP addresses in batch. After an IP address is deleted from the whitelist, the device will not directly permit traffic from this IP address.

----End

3.5.6 Mitigating CC Attacks Using Frequency Control Policies

You can set frequency control rules to limit the access frequency of a single IP address, cookie, or referer to the origin server of a protected website. You can also enable policy-based, domain name, and URL rate limiting to detect and block malicious traffic.

Prerequisites

Basic Web Protection has been enabled for website services. For details, see **Enabling Basic Web Protection**.

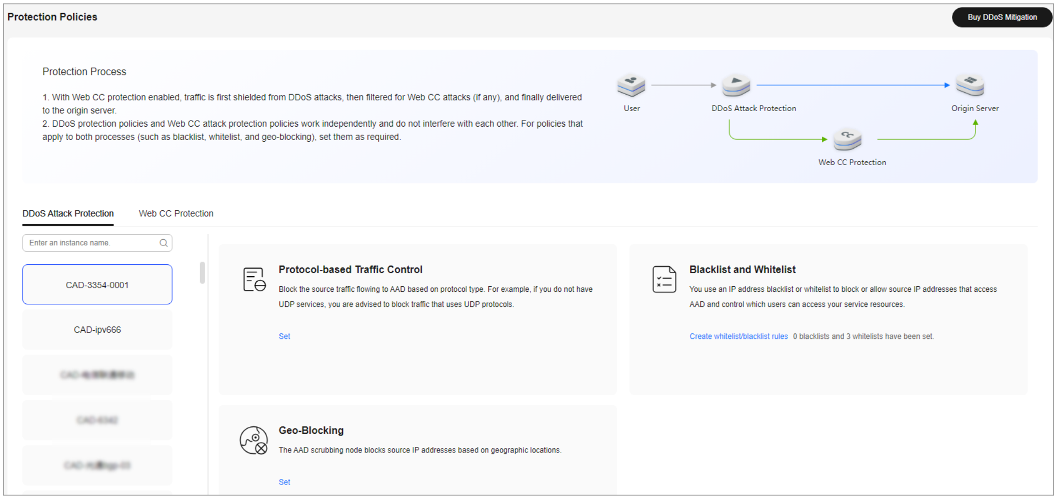
Enabling a Frequency Control Policy

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

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Protection Policies**. The **Protection Policies** page is displayed.

Figure 3-28 Advanced Anti-DDoS protection policies



Protection Policies

Protection Process

1. With Web CC protection enabled, traffic is first shielded from DDoS attacks, then filtered for Web CC attacks (if any), and finally delivered to the origin server.
2. DDoS protection policies and Web CC attack protection policies work independently and do not interfere with each other. For policies that apply to both processes (such as blacklist, whitelist, and geo-blocking), set them as required.

Enter an instance name.

CAD-3354-0001

CAD-ipv666

[redacted]

[redacted]

[redacted]

Protocol-based Traffic Control

Block the source traffic flowing to AAD based on protocol type. For example, if you do not have UDP services, you are advised to block traffic that uses UDP protocols.

Set

Blacklist and Whitelist

You use an IP address blacklist or whitelist to block or allow source IP addresses that access AAD and control which users can access your service resources.

Create whitelist/blacklist rules 0 blacklists and 3 whitelists have been set.

Geo-Blocking

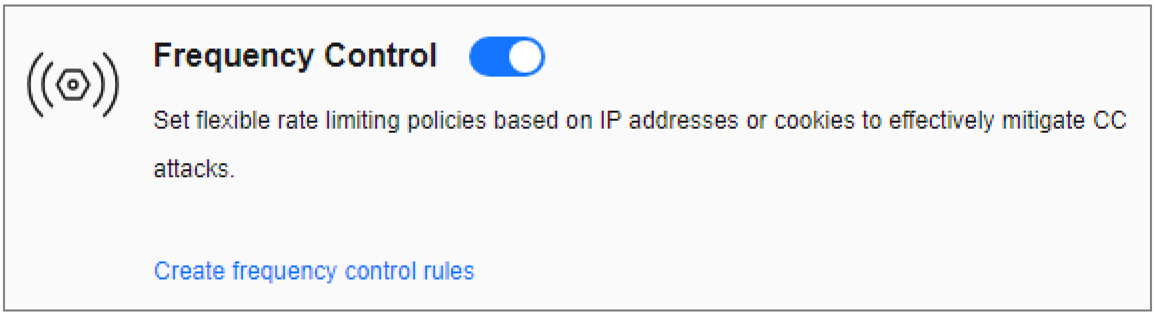
The AAD scrubbing node blocks source IP addresses based on geographic locations.

Set

Step 4 Click the **Web Attack Protection** tab.

Step 5 After selecting the region and objects, click **Create frequency control rules**.

Figure 3-29 Frequency control rules



Frequency Control

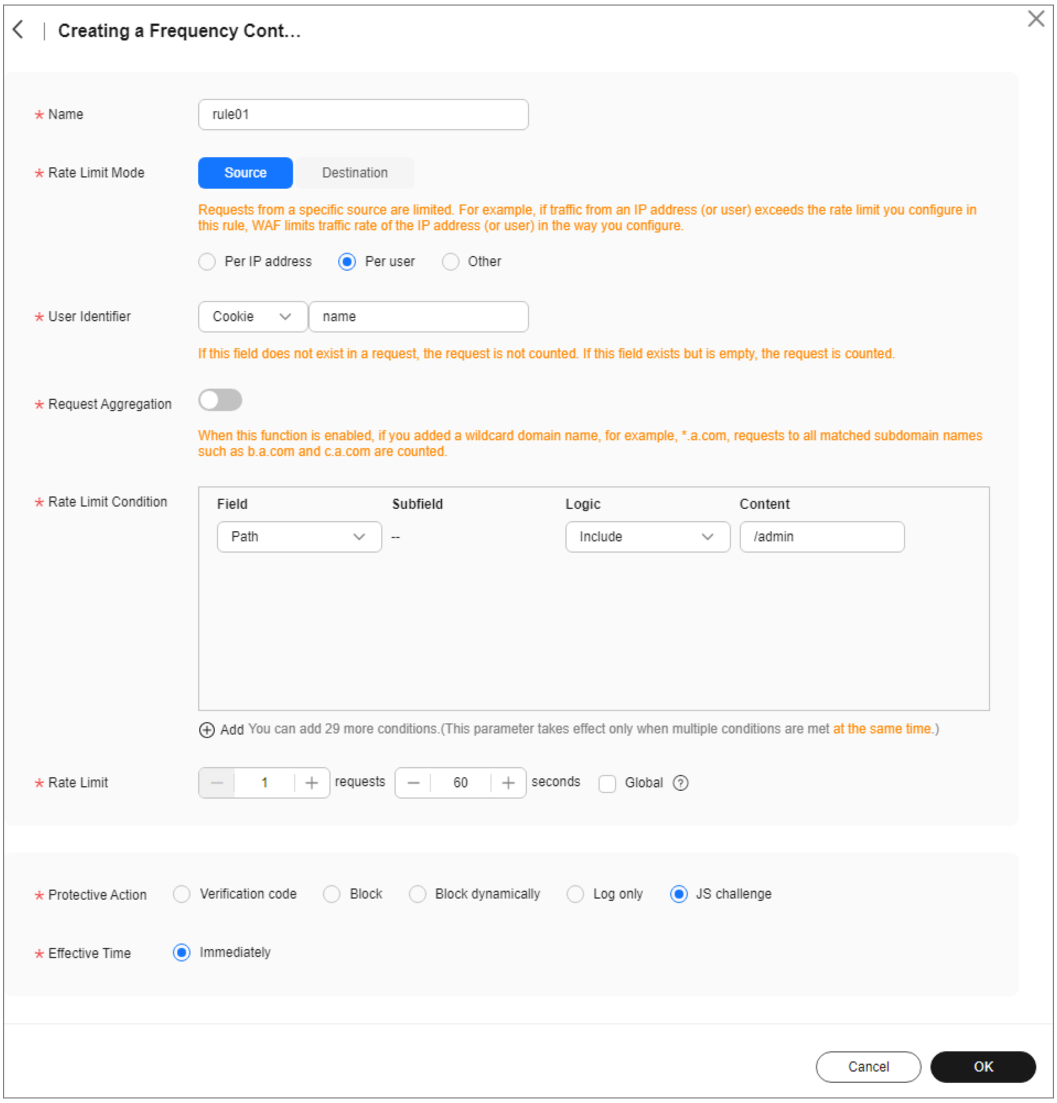
Set flexible rate limiting policies based on IP addresses or cookies to effectively mitigate CC attacks.

Create frequency control rules

Step 6 Click **Create frequency control rules**.

Step 7 Configure the frequency control rule, as shown in **Figure 3-30**.

Figure 3-30 Creating a frequency control rule



* Name: rule01

* Rate Limit Mode: **Source** | Destination

Requests from a specific source are limited. For example, if traffic from an IP address (or user) exceeds the rate limit you configure in this rule, WAF limits traffic rate of the IP address (or user) in the way you configure.

○ Per IP address ● Per user ○ Other

* User Identifier: Cookie | name

If this field does not exist in a request, the request is not counted. If this field exists but is empty, the request is counted.

* Request Aggregation

When this function is enabled, if you added a wildcard domain name, for example, *.a.com, requests to all matched subdomain names such as b.a.com and c.a.com are counted.

* Rate Limit Condition

Field	Subfield	Logic	Content
Path	--	Include	/admin

⊕ Add You can add 29 more conditions.(This parameter takes effect only when multiple conditions are met at the same time.)

* Rate Limit: 1 requests 60 seconds □ Global

* Protective Action: ○ Verification code ○ Block ○ Block dynamically ○ Log only ● JS challenge

* Effective Time: ● Immediately

Table 3-14 Parameter description

Parameter	Description
Name	Name of the rule

Parameter	Description
Rate Limit Mode	● **Source**: Requests from a specific source are limited. For example, if traffic from an IP address (or user) exceeds the rate limit you configure in this rule, WAF limits traffic rate of the IP address (or user) in the way you configure. – **Per IP address**: A web visitor is identified by the IP address. – **Per user**: A website visitor is identified by the key value of **Cookie** or **Header**. – **Other**: A web visitor is identified by the **Referer** field (user-defined request source). **NOTE** If you set **Rate Limit Mode** to **Other**, set **Content** of **Referer** to a complete URL containing the domain name. The **Content** field supports prefix match and exact match only, but cannot contain two or more consecutive slashes, for example, **///admin**. If you enter **///admin**, the engine will convert it to **/admin**. For example, if you do not want visitors to access www.test.com, set **Referer** to **http://www.test.com**. ● **Destination**: Requests to a specific destination are limited. – **By rule**: If this rule is used by multiple domain names, requests for all these domain names are counted for this rule no matter what IP addresses these requests originate from. If you have added a wildcard domain name to WAF, requests for all domain names matched the wildcard domain name are counted for triggering this rule no matter what IP addresses these requests originate from. – **By domain name**: Requests for each domain name are counted separately. If the number exceeds the threshold you configure, the protective action is triggered no matter what IP addresses these requests originate from. – **By URL**: Requests for each URL are counted separately. If the number exceeds the threshold you configure, the protective action is triggered no matter what IP addresses these requests originate from.
Request Aggregation	This parameter is not required when you select **Destination** and **By rule** for **Rate Limit Mode**. This function is disabled by default. Keep this function enabled so that requests to all domain names that match a protected wildcard domain are counted for triggering this rule. For example, if you added ***.a.com**, requests to all matched domain names such as **b.a.com** and **c.a.com** are counted.

Parameter	Description
User Identifier	This parameter is mandatory when you select **Source** and **Per user** for **Rate Limit Mode**. ● **Cookie**: A cookie field name. You need to configure an attribute variable name in the cookie that can uniquely identify a web visitor based on your website requirements. This field does not support regular expressions. Only complete matches are supported. For example, if a website uses the **name** field in the cookie to uniquely identify a web visitor, enter **name**. ● **Header**: Set the user-defined HTTP header you want to protect. You need to configure the HTTP header that can identify web visitors based on your website requirements.
Trigger	Click **Add** to add conditions. At least one condition is required, but up to 30 conditions are allowed. If you add more than one condition, the rule will only take effect if all of the conditions are met. ● **Field**: Set this parameter based on the site requirements. ● **Subfield**: Configure this field only when **IPv4**, **IPv6**, **Cookie**, **Header**, or **Params** is selected for **Field**. ● **Logic**: Select the required logic from the drop-down list box. ● **Content**: Enter or select the content that matches the condition.
Rate Limit	The number of requests allowed from a website visitor in the rate limit period. If the number of requests exceeds the rate limit, the system takes the action you configure for **Protective Action**. **Global**: Requests to one or more nodes will be aggregated according to the rate limit mode you select. By default, requests to each node are counted. If you enable this option, the system will count requests to all nodes for triggering this rule. To enable user-based rate limiting, select **Per user** or **Other** (Referer) instead of **Per IP address** for **Rate Limit Mode**. IP address-based rate limiting cannot restrict the access rate of a specific user. However, with user-based rate limiting, requests may be forwarded to one or more nodes. Select **Global** to count requests to all nodes.

Parameter	Description
Protective Action	The action that WAF will take if the number of requests exceeds **Rate Limit** you configured. The options are as follows: ● **Verification code**: WAF allows requests that trigger the rule as long as your website visitors complete the required verification. ● **Block**: WAF blocks requests that trigger the rule. ● **Block dynamically**: WAF blocks requests that trigger the rule based on **Allowable Frequency**, which you configure after the first rate limit period is over. ● **Log only**: WAF only logs requests that trigger the rule. ● **JS Challenge**: AAD returns a piece of JavaScript code that can be automatically executed by a normal browser to the client. If the client properly executes the JavaScript code, AAD allows all requests from the client within a period of time (30 minutes by default). During this period, no verification is required. If the client fails to execute the code, AAD blocks the requests.
Lock Verification	This parameter is mandatory if **Protective Action** is set to **Verification code**. If a visitor fails verification code authentication, verification is required for all access requests within the specified period.
Allowable Frequency	This parameter can be set if you select **Block dynamically** for **Protective Action**. WAF blocks requests that trigger the rule based on **Rate Limit** first. Then, in the following rate limit period, WAF blocks requests that trigger the rule based on **Allowable Frequency** you configure. The **Allowable Frequency** must be less than or equal to the **Rate Limit**.
Notification Window	The default option is **Immediately**.
Block Duration	Period of time for which to block the item when you set **Protective Action** to **Block**.
Block Page	The page displayed if the request limit has been reached. This parameter is configured only when **Protective Action** is set to **Block**. ● If you select **Default settings**, the default block page is displayed. ● If you select **Customize**, customize a page to be displayed.
Block Page Type	If you select **Custom** for **Block Page**, select a type of the block page among options **application/json**, **text/html**, and **text/xml**.

Parameter	Description
Page Content	Specifies the content to be displayed on the page you will customize.

Step 8 Click **OK**.

----End

Follow-up Operations

- Enable frequency control protection: On the **Web Attack Protection** page, set **Frequency Control** to .
- Disable frequency control protection: On the **Web Attack Protection** page, set **Frequency Control** to .

3.5.7 Using Intelligent CC Policies to Defend Against CC Attacks

If you enable intelligent CC attack protection, AAD uses built-in AI-powered models to analyze traffic to your website, identify CC attacks and abnormal features in HTTP requests on the origin server, and generate specific precise protection and access control rules for your website. In this way, AAD can then automatically protect your website from CC attacks.

Limitations and Constraints

This function is in the internal test phase and is available only to some users. If you want to use it, **submit a service ticket**.

Prerequisites

Basic Web Protection has been enabled for website services. For details, see **Enabling Basic Web Protection**.

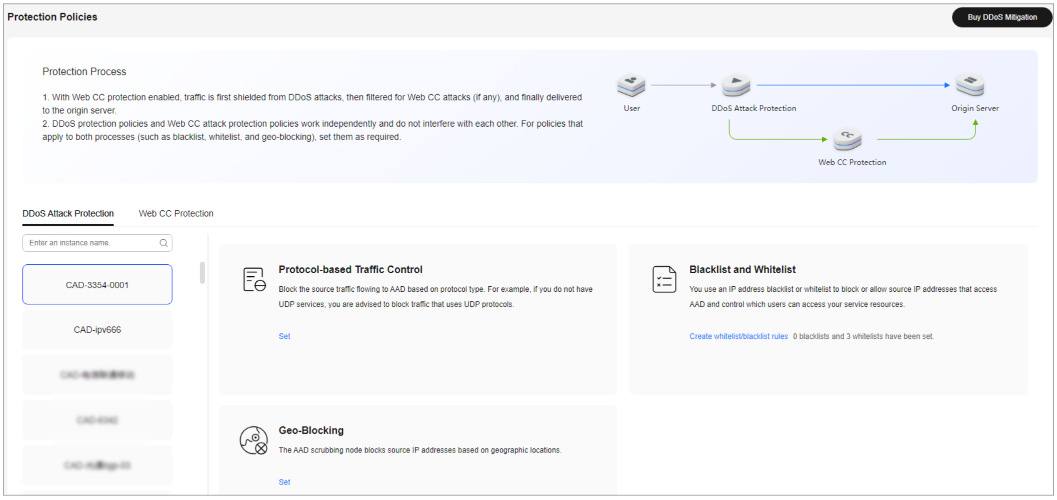
Enabling Intelligent CC

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

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Protection Policies**. The **Protection Policies** page is displayed.

Figure 3-31 Advanced Anti-DDoS protection policies



Protection Policies

Buy DDoS Mitigation

Protection Process

1. With Web CC protection enabled, traffic is first shielded from DDoS attacks, then filtered for Web CC attacks (if any), and finally delivered to the origin server.
2. DDoS protection policies and Web CC attack protection policies work independently and do not interfere with each other. For policies that apply to both processes (such as blacklist, whitelist, and geo-blocking), set them as required.

DDoS Attack Protection | Web CC Protection

Enter an instance name.

CAD-3354-0001

CAD-ipv666

[redacted]

[redacted]

[redacted]

Protocol-based Traffic Control

Block the source traffic flowing to AAD based on protocol type. For example, if you do not have UDP services, you are advised to block traffic that uses UDP protocols.

Set

Blacklist and Whitelist

You use an IP address blacklist or whitelist to block or allow source IP addresses that access AAD and control which users can access your service resources.

Create whitelist/blacklist rules 0 blacklists and 3 whitelists have been set.

Geo-Blocking

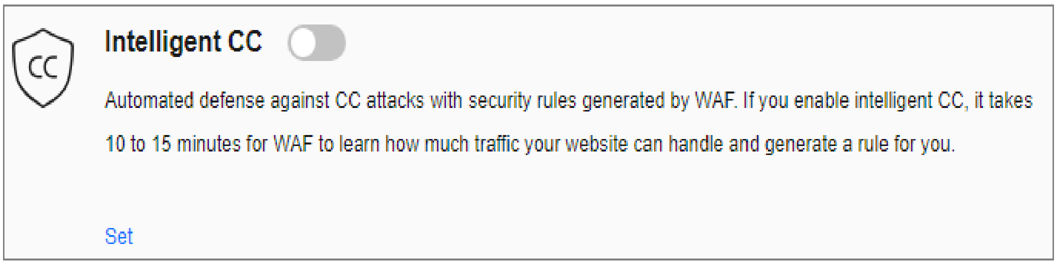
The AAD scrubbing node blocks source IP addresses based on geographic locations.

Set

Step 4 Click the **Web CC Protection** tab.

Step 5 After selecting the region and object to be protected, click **Set** under **Intelligent CC**.

Figure 3-32 Intelligent CC



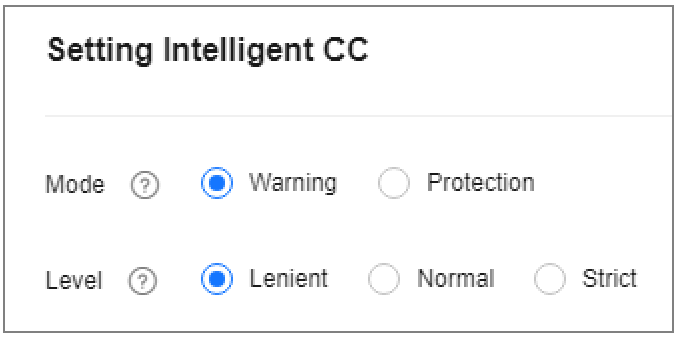
Intelligent CC

Automated defense against CC attacks with security rules generated by WAF. If you enable intelligent CC, it takes 10 to 15 minutes for WAF to learn how much traffic your website can handle and generate a rule for you.

Set

Step 6 Set the protection policy as required, as shown in **Table 3-15**.

Figure 3-33 Setting Intelligent CC



Setting Intelligent CC

Mode ● Warning ○ Protection

Level ● Lenient ○ Normal ○ Strict

Table 3-15 Parameter description

Parameter	Description
Schema	● **Warning**: Records log but does not block malicious requests. ● **Protection**: Block malicious requests and records logs.

Parameter	Description
Severity	● **Lenient**: Only known malicious attacks are blocked. This mode is suitable for large-scale websites and ensures that normal requests are not mistakenly blocked. ● **Normal**: Ideal for scenarios with stable request volumes and redundant server processing performance. When detecting malicious attacks, with intelligent protection enabled, the impact on normal services is little. In this case, you are advised to use this level. ● **Strict**: Suitable for scenarios where website performance is poor and protection needs to be stringent. However, some legitimate requests may be mistakenly blocked.

Step 7 On the **Web CC Protection** page, set **Intelligent CC** to to enable protection.

----End

3.6 Enabling Alarm Notifications for DDoS Attacks

After you enable the alarm notification, a notification message will be sent to you through the method you have configured when:

- An IP address is under the DDoS attacks.
- Additional fees are incurred for traffic exceeding the basic protection bandwidth.

If you want to monitor service metrics in detail, you are advised to use Cloud Eye to set alarm rules and alarm notifications. For details, see **Viewing Monitoring Metrics**.

Prerequisites

- The Simple Message Notification (SMN) service is a paid service. For details about the price, see **SMN Product Pricing Details**.
- Before enabling alarm notifications, you are advised to create a message topic in the SMN service as an administrator. For details, see .

Enabling Alarm Notifications

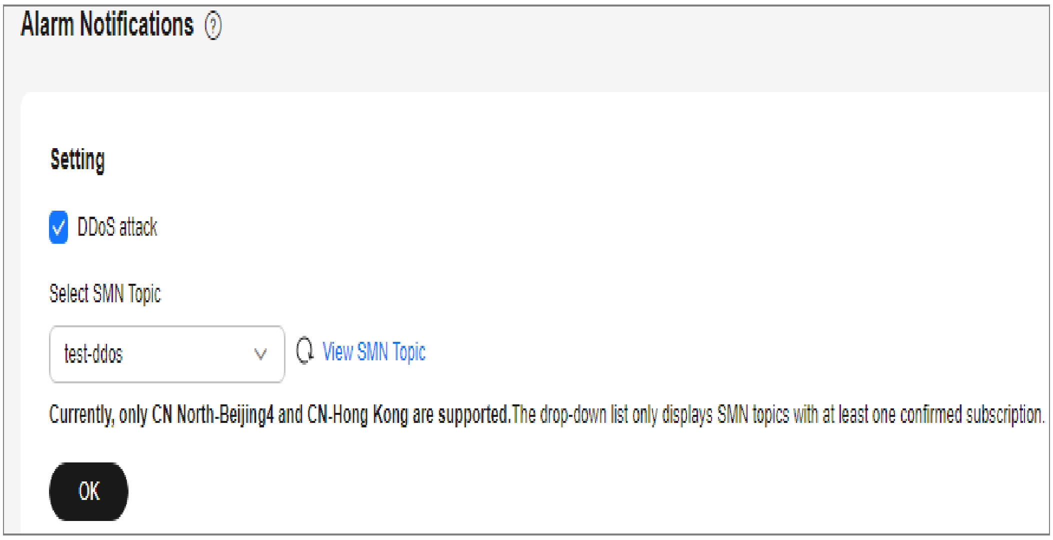
Step 1 **Log in to the management console**.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS > Alarm Notifications**. The **Alarm Notifications** page is displayed.

Step 4 On the **Alarm Notifications** page, select **DDoS attack**.

Figure 3-34 Configure Alarm Notification



Alarm Notifications

Setting

☑ DDoS attack

Select SMN Topic

test-ddos

Currently, only CN North-Beijing4 and CN-Hong Kong are supported.The drop-down list only displays SMN topics with at least one confirmed subscription.

Select an existing topic from the drop-down list or click **View SMN Topic** and create an SMN topic on the displayed page for configuring the terminals for receiving alarm notifications.

NOTE

Notification topics are available only in CN North-Beijing4 and CN-Hong Kong.

Perform the following steps to create a topic:

1. Create a topic by referring to **Creating a Topic**.
2. You can add one or more subscriptions to a topic by configuring the phone number, email address, function, platform application endpoint, DMS endpoint, or HTTP/HTTPS endpoint for receiving alarm notifications. For details, see **Adding a Subscription**.
3. Confirm the subscription. After the subscription is added, confirm the subscription.

For details about topics and subscriptions, see *Simple Message Notification User Guide*.

Step 5 Click **OK**.

NOTE

To disable the alarm notification function, deselect **DDoS attack** in **Figure 3-34** and click **OK**.

----End

3.7 Enabling Logging

After you authorize AAD to access Log Tank Service (LTS), you can use the AAD logs recorded by LTS for quick and efficient real-time analysis, device O&M management, and analysis of service trends.

Prerequisites

LTS has been enabled. For details, see **Managing Log Groups** and **Managing Log Streams**.

Enabling AAD Logging

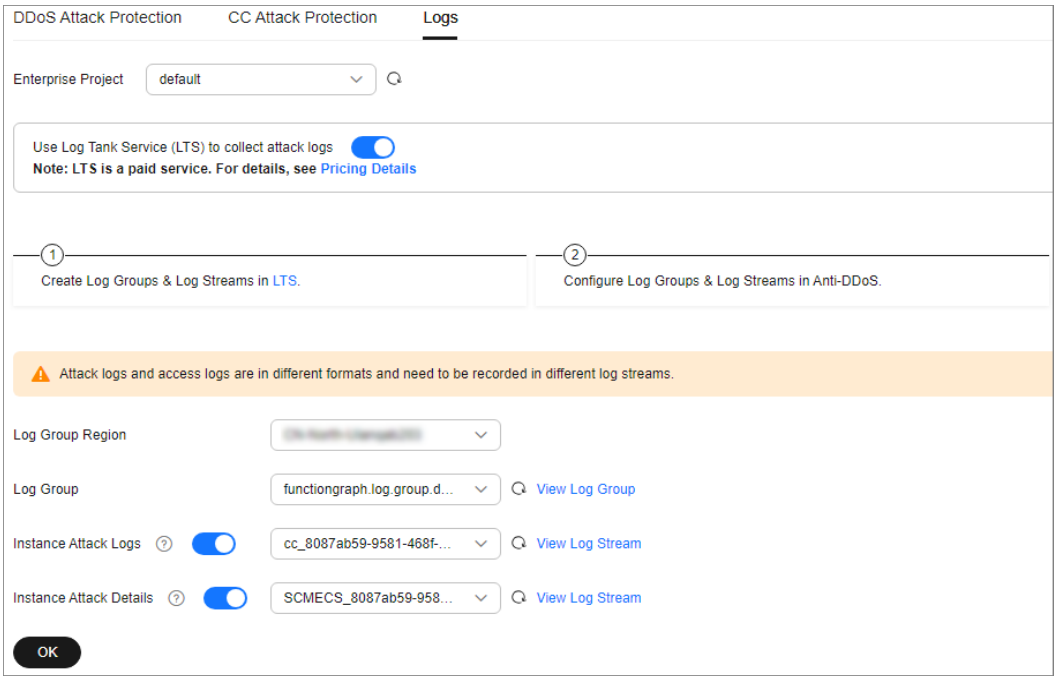
Step 1 **Log in to the management console**.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Dashboard**. The **Dashboard** page is displayed.

Step 4 Click **Logs**, enable full logs, and configure log groups and log streams. For details about related parameters, see **Figure 3-35**.

Figure 3-35 Configuring AAD logs



Enterprise Project: default

Use Log Tank Service (LTS) to collect attack logs
Note: LTS is a paid service. For details, see Pricing Details

1 Create Log Groups & Log Streams in LTS.

2 Configure Log Groups & Log Streams in Anti-DDoS.

Attack logs and access logs are in different formats and need to be recorded in different log streams.

Log Group Region: [redacted]

Log Group: functiongraph.log.group.d... View Log Group

Instance Attack Logs: cc_8087ab59-9581-468f-... View Log Stream

Instance Attack Details: SCMECS_8087ab59-958... View Log Stream

Table 3-16 AAD log parameters

Parameter	Description
Enterprise Project	Select an enterprise project.
Log Group Region	Select the region to which the log group belongs.

Parameter	Description
Log Group	Select a log group or click **View Log Group** to go to the LTS console and create a log group.
Instance Attack Logs	Select a log stream or click **View Log Stream** to go to the LTS console and create a log stream. An attack log includes information about event type, protective action, and attack source IP address of each attack. For details about the log fields, see **Table 3-17**.
Instance Attack Details	Select a log stream or click **View Log Stream** to go to the LTS console and create a log stream. Instance attack details include the attack start time, end time, attack status, and attack type. For details about the fields, see **Table 3-18**.

Step 5 Click **OK**.

You can view protection logs on the LTS console.

----End

Log Fields in LTS

This section describes the fields of AAD logs.

Table 3-17 Fields in an instance attack log

Field	Description
ip	Attacked IP address
ip_id	ID of the attacked IP address
attack_type	Attack type
attack_protocol	This field is not used currently. The default value is 0.
attack_start_time	Time the attack starts, which is a timestamp accurate to millisecond.
attack_status	Attack status. ● **ATTACK**: The attack is ongoing. ● **NORMAL**: The attack ends.
drop_kbits	The minute-level maximum attack traffic, in **bits**.
attack_pkts	The minute-level maximum number of attack packets

Field	Description
duration_elapse	Duration of an ended security event, in **seconds**.
end_time	Time the attack ends, which is a timestamp accurate to millisecond. For an on-going security event, the value of this field is **0**.
max_drop_kbps	Peak attack traffic, in **Kbit/s**.
max_drop_pps	Peak attack packets, in **pps**.

Table 3-18 Description of fields in the instance attack details

Field	Description
attackStatus	Attack status
attackType	Attack status ● **ATTACK**: The attack is ongoing. ● **NORMAL**: The attack ends.
attackTypeDescCn	Attack type, in Chinese.
attackTypeDescEn	Attack type, in English.
attackUnit	Attack unit
attacker	Attack source
attackerKbps	Peak attack traffic, in **kbps**.
attackerPps	Peak attack traffic, in **pps**.
direction	Log direction ● **inbound** ● **outbound**
dropKbits	Total volume of discarded traffic, in **kbps**.
dropPackets	Total number of discarded packets.
duration	Attack duration, in **seconds**.
handleTime	Time when the log is processed.
logTime	Log time
logType	Log type
maxDropKbps	Peak value of discarded IP traffic, in **kbps**.
maxDropPps	Peak value of discarded IP traffic, in **pps**.
port	Port number

Field	Description
startTimeAlert	Start time of an exception
timeScale	Time identifier (identifier for minute-level processing time or hour-level processing time).
valid	Indicates whether logs are successfully parsed.
writeTime	Persistence time
zoneIP	Protected IP
startTimeAttack	Time when the attack starts
startTimeKey	ID of an attack starting at a certain time

3.8 Viewing Statistics

After your services are connected to AAD, you can view the DDoS and CC attack protection reports to learn about the network security status of your services.

On the **Dashboard** page, you can view the following protection details:

- DDoS Attack Protection

  You can view the security overview, traffic trend, protocol distribution, number of connections, attack distribution, security events, and blackhole events in a specified time range.

- CC Attack Protection

  You can view the number of requests, number of attacks, bandwidth, attack distribution, attack sources, and attack events in a specified period.

Viewing DDoS Attack Protection Statistics

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

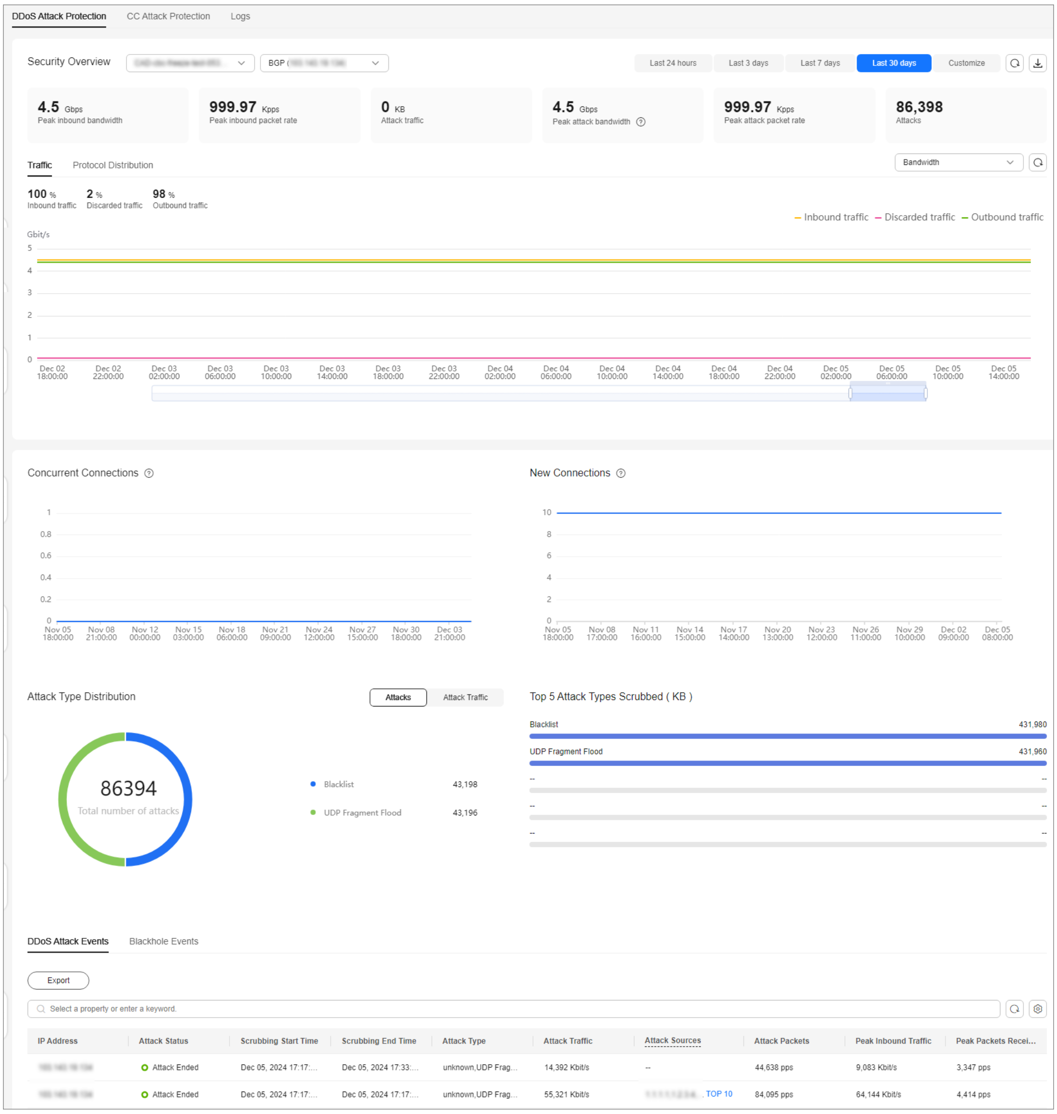
Step 2 Select a region in the upper part of the page, click ☰ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS > Dashboard**. The **Dashboard** page is displayed.

Step 4 Click the **DDoS Attack Protection** tab.

Step 5 Select an instance, line, and time range (last 24 hours, last 3 days, last 7 days, last 30 days, or a custom period). **Table 3-19** describes the related parameters.

Figure 3-36 DDoS attack protection



DDoS Attack Protection | CC Attack Protection | Logs

Security Overview [redacted] BGP ([redacted])

Last 24 hours | Last 3 days | Last 7 days | **Last 30 days** | Customize

4.5 Gbps Peak inbound bandwidth

999.97 Kpps Peak inbound packet rate

0 KB Attack traffic

4.5 Gbps Peak attack bandwidth

999.97 Kpps Peak attack packet rate

86,398 Attacks

Traffic | Protocol Distribution — Bandwidth

100 % Inbound traffic

2 % Discarded traffic

98 % Outbound traffic

Attack Type Distribution — Attacks | Attack Traffic

86394 Total number of attacks

Blacklist	43,198
UDP Fragment Flood	43,196

Top 5 Attack Types Scrubbed (KB)

Blacklist	431,980
UDP Fragment Flood	431,960
--	--
--	--
--	--

DDoS Attack Events | Blackhole Events

Export

Select a property or enter a keyword.

IP Address	Attack Status	Scrubbing Start Time	Scrubbing End Time	Attack Type	Attack Traffic	Attack Sources	Attack Packets	Peak Inbound Traffic	Peak Packets Recei...
[redacted]	Attack Ended	Dec 05, 2024 17:17:...	Dec 05, 2024 17:33:...	unknown,UDP Frag...	14,392 Kbit/s	--	44,638 pps	9,083 Kbit/s	3,347 pps
[redacted]	Attack Ended	Dec 05, 2024 17:17:...	Dec 05, 2024 17:17:...	unknown,UDP Frag...	55,321 Kbit/s	[redacted] TOP 10	84,095 pps	64,144 Kbit/s	4,414 pps

Table 3-19 Parameter description

Parameter	Description
Peak inbound bandwidth	Maximum traffic accessing the specified IP address of a specified instance per second
Peak inbound packet rate	Maximum number of incoming packets per second
Peak attack bandwidth	Maximum traffic attacking the specified IP address of a specified instance per second The attack traffic refers to the attack traffic that triggers security events.

Parameter	Description
Peak attack packet rate	Maximum number of incoming attack packets per second
Attacks	Number of DDoS attacks launched on the specified IP address of a specified instance
Traffic	Proportions and distribution trends of inbound traffic, outbound traffic, and discarded traffic.
Protocol distribution	Proportions and distribution trend of protocols such as TCP, UDP, and ICMP in traffic.
Concurrent connections	Number of concurrent connections.
New connections	Number of new connections.
Attack type distribution	Types of attack events ● You can click **Attacks** to see the type, count, and percentage of an attack. ● You can click **Attack traffic** then click any colored section in the displayed circle to see the type, traffic, and traffic percentage of an attack.
Top 5 attack types scrubbed (Kbit/s)	Top 5 attack types that have been scrubbed

Parameter	Description
DDoS attack events	Details about DDoS attacks ● Click **Details** next to the attack source IP address to view the complete attack source IP address list. ● Click **View Dynamic Blacklist** to view the blacklisted IP addresses that are in attack. ● Click **Export** to export the security event report. **NOTE** Note the following points about the attack source field in the DDoS attack event report: ● The attack sources of ongoing attacks may not be displayed. ● Some attack events contain only some attack types. Their attack sources are not displayed. ● Attack sources are sampled randomly. Not all attack source information is displayed.
Blackhole events	Blocked IP address, blocking status, blocking start time, and blocking end time. Click **Export** to export the blackhole event report.

NOTE

In the traffic or packet chart on the **DDoS Attack Protection** page, the display granularity varies according to the query interval. The details are as follows:

- Query time < 20 minutes: The display granularity is 1 minute.
- 20 minutes < Query time < 40 minutes: The display granularity is 2 minutes.
- 40 minutes < Query time < 60 minutes: The display granularity is 3 minutes.
- 1 hour < Query time ≤ 6 hours: The display granularity is 5 minutes.
- 6 hours < Query time ≤ 24 hours: The display granularity is 10 minutes.
- 1 day < Query time ≤ 7 days: The display granularity is 30 minutes.
- 7 days < Query time ≤ 15 days: The display granularity is 1 hour.
- 15 days < Query time ≤ 30 days: The display granularity is 14 hours.

----End

Viewing CC Attack Protection Statistics

Step 1 Log in to the management console.

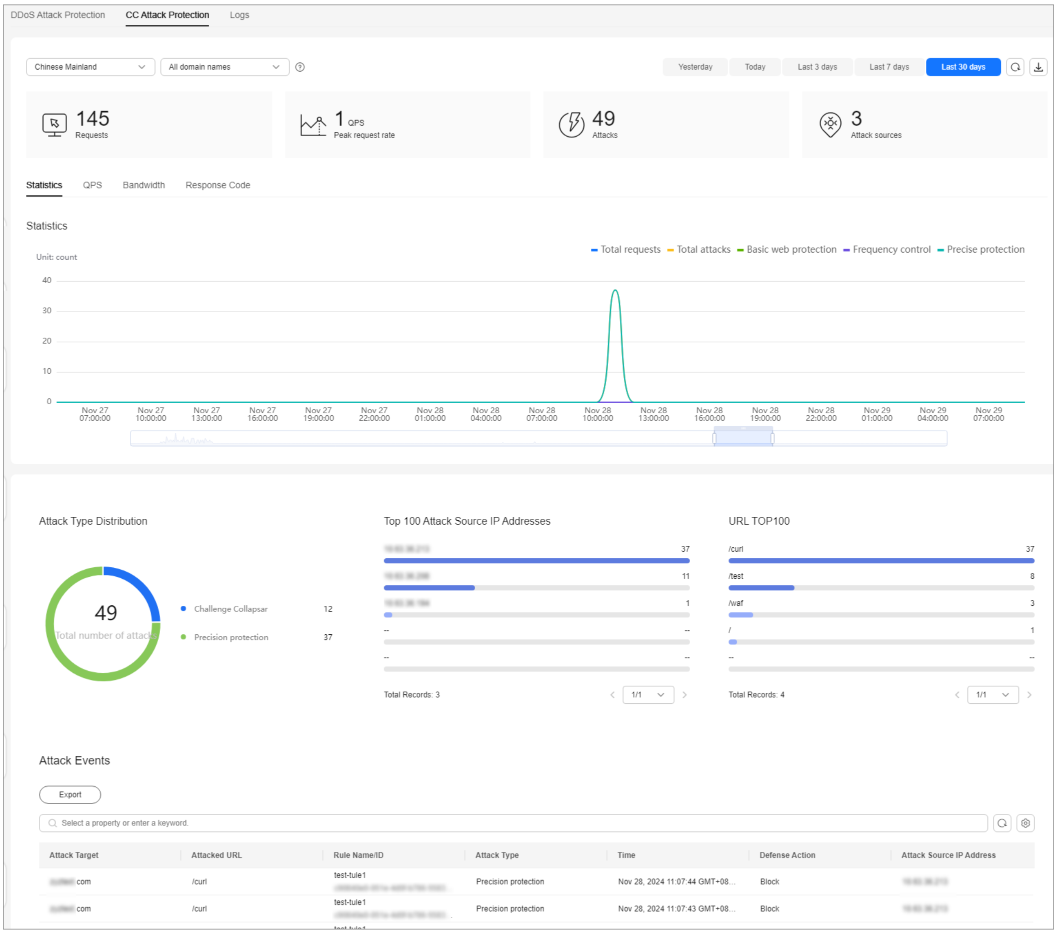
Step 2 Select a region in the upper part of the page, click ☰ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS > Dashboard**. The **Dashboard** page is displayed.

Step 4 Click the **CC Attack Protection** tab.

Step 5 Select a domain name and time range. For details about related parameters, see **Table 3-20**.

Figure 3-37 CC Attack Protection



Top 100 Attack Source IP Addresses

[redacted]	37
[redacted]	11
[redacted]	1
--	--
--	--

Total Records: 3 1/1

URL TOP100

/curl	37
/test	8
/waf	3
/	1
--	--

Total Records: 4 1/1

Attack Target	Attacked URL	Rule Name/ID	Attack Type	Time	Defense Action	Attack Source IP Address
[redacted] com	/curl	test-tule1 [redacted]	Precision protection	Nov 28, 2024 11:07:44 GMT+08...	Block	[redacted]
[redacted] com	/curl	test-tule1 [redacted]	Precision protection	Nov 28, 2024 11:07:43 GMT+08...	Block	[redacted]

Table 3-20 Parameter description

Parameter	Description
Requests	Total number of requests to a specified domain name If you select **All domain names**, the total number of requests to all domain names with WAF enabled is collected.

Parameter	Description
Peak request rate	Maximum number of requests to a specified domain name per second If you select **All domain names**, the maximum number of requests to all domain names with WAF enabled is collected per second.
Attacks	Number of attacks towards a specified domain name
Attack sources	Number of sources that attack a specified domain name
Statistics	Displays the request trend chart over time, detailing the total number of requests, total number of attacks, and the number of different types of attacks.
QPS	Queries Per Second (QPS) indicates the number of requests per second. For example, an HTTP GET request is also called a query. Average: average number of requests per second to a domain name. Peak value: maximum number of requests per second to a domain name.
Bandwidth	**Average**: average value of the outbound bandwidth and the inbound bandwidth. **Peak**: peak value of the outbound bandwidth and the inbound bandwidth.
Response code	● **AAD Response**: indicates the response code returned by AAD to the client and the number of responses. ● **Origin Server Response**: indicates the response code returned by the origin server to AAD and the number of responses.

Parameter	Description
Attack type distribution	Numbers and proportions of different attacks. ● You can click any colored area in the attack distribution circle under **Attack Type Distribution** to view the type, count, and proportion of an attack. ● To stop displaying information about a specific type of attacks, click the legend with the same color to the right of the circle.
Top 100 attack source IP addresses	Top 100 attack source IP addresses.
URL TOP 100	Top 100 attacked URLs.
Attack events	For details about attack event parameters, see **Table 3-21**. Click **Export** to export the attack event report.

Table 3-21 Attack event parameters

Parameter	Description
Target	Specifies an attacked domain name.
Attacked URL	Specifies the URL of the protected domain name, for example, **/4b87ef**.
Attack Type	Indicates the type of the attack, for example, **frequency control**.
Time	Time when the attack occurred.
Protective Action	Protective actions. ● **Block** ● **Log only** ● **Verification code**
Source IP	Indicates the IP address of the attacker.

----End

3.9 Managing Instances

3.9.1 Viewing Information About an Instance

To verify that your instances are running normally after enabling AAD, check their status in the instance list.

Viewing AAD Instance Information

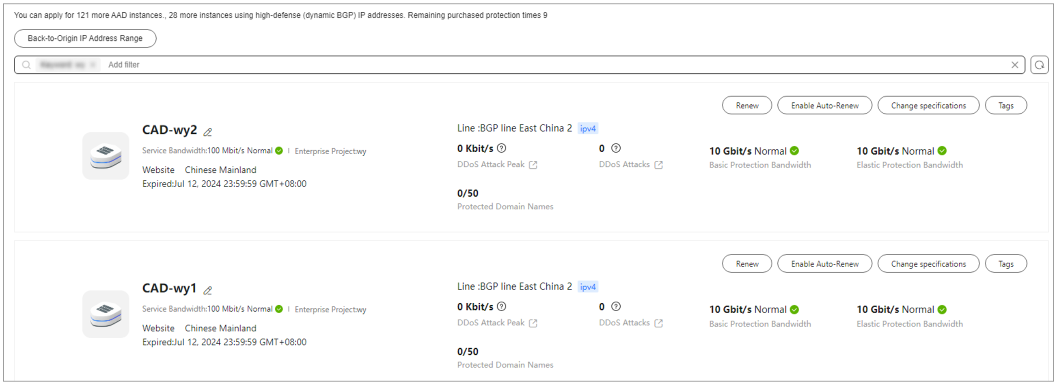
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS > Instance List**. The **Instance List** page is displayed.

Step 4 On the displayed page, view the details about an instance. Table 3-22 describes the parameters.

Figure 3-38 Instances



You can apply for 121 more AAD instances., 28 more instances using high-defense (dynamic BGP) IP addresses. Remaining purchased protection times 9

CAD-wy2
Service Bandwidth:100 Mbit/s Normal | Enterprise Project:wy
Website Chinese Mainland
Expired:Jul 12, 2024 23:59:59 GMT+08:00

Line :BGP line East China 2 ipv4
0 Kbit/s DDoS Attack Peak
0 DDoS Attacks
10 Gbit/s Normal Basic Protection Bandwidth
10 Gbit/s Normal Elastic Protection Bandwidth
0/50 Protected Domain Names

CAD-wy1
Service Bandwidth:100 Mbit/s Normal | Enterprise Project:wy
Website Chinese Mainland
Expired:Jul 12, 2024 23:59:59 GMT+08:00

Line :BGP line East China 2 ipv4
0 Kbit/s DDoS Attack Peak
0 DDoS Attacks
10 Gbit/s Normal Basic Protection Bandwidth
10 Gbit/s Normal Elastic Protection Bandwidth
0/50 Protected Domain Names

Table 3-22 Parameter description

Parameter	Description
Instance Name	Name of an AAD instance. You can click ✎ on the right to change the name.
Service Bandwidth	Service bandwidth and status of the instance.
Enterprise Project	Enterprise project that the instance belongs to.
Access Type	Type of the protected object that accesses to the instance.
Region	Region protected by the instance.
Line	line resources, including service access points, and IP types.
Peak Attack Peak	Peak DDoS attack traffic on the current day.
DDoS Attacks	Number of DDoS attacks on the current day.

Parameter	Description
Instance Specifications.	Basic protection bandwidth, elastic protection bandwidth, and number of protected domain names.

----End

3.9.2 Upgrading Instance Specifications

If your services evolve and you require higher instance specifications after purchasing an instance, you can upgrade these specifications.

Fees Description

Modifying specifications will lead to fee changes. For details, see **Pricing of a Changed Specification**.

Limitations and Constraints

- If a customer purchases a non-BGP triple-line instance (not for sale currently), the specifications cannot be upgraded. To change the elastic bandwidth, **submit a work order** for technical support.
- The lines cannot be changed during the upgrade.
- Expired instances do not support specifications upgrades.
- Frozen instances do not support specifications upgrades.

Upgrading the Specifications of an AAD Instance

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

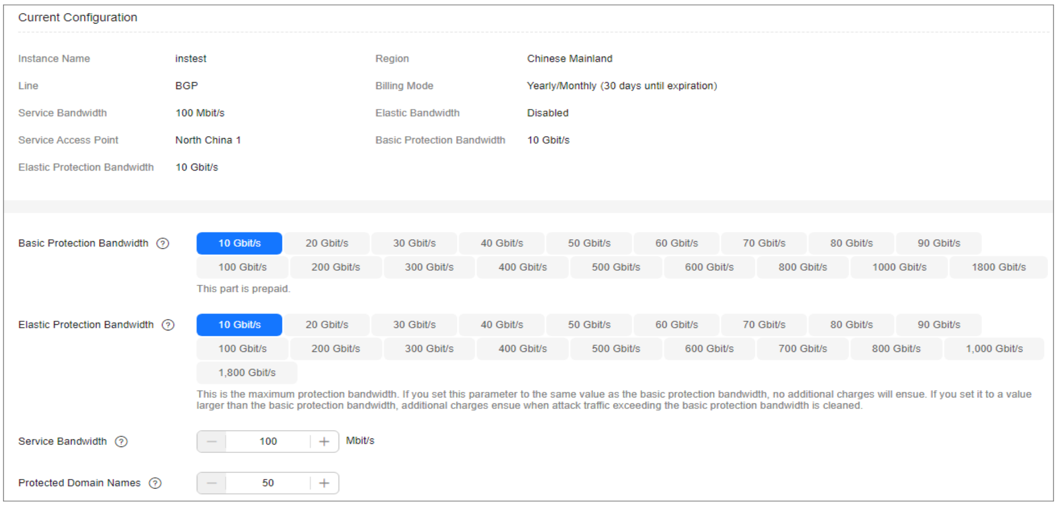
Step 2 Select a region in the upper part of the page, click ☰ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS** page is displayed.

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS > Instance List**. The **Instance List** page is displayed.

Step 4 On the displayed page, locate the target instance and click **Change Specifications**.

Step 5 On the **Modify AAD Specifications** page, adjust the instance specifications.

Figure 3-39 Specifications of a domain-based instance



Current Configuration

Instance Name	instest	Region	Chinese Mainland
Line	BGP	Billing Mode	Yearly/Monthly (30 days until expiration)
Service Bandwidth	100 Mbit/s	Elastic Bandwidth	Disabled
Service Access Point	North China 1	Basic Protection Bandwidth	10 Gbit/s
Elastic Protection Bandwidth	10 Gbit/s		

Basic Protection Bandwidth ⓘ: [✓ 10 Gbit/s] 20 Gbit/s 30 Gbit/s 40 Gbit/s 50 Gbit/s 60 Gbit/s 70 Gbit/s 80 Gbit/s 90 Gbit/s 100 Gbit/s 200 Gbit/s 300 Gbit/s 400 Gbit/s 500 Gbit/s 600 Gbit/s 800 Gbit/s 1000 Gbit/s 1800 Gbit/s

This part is prepaid.

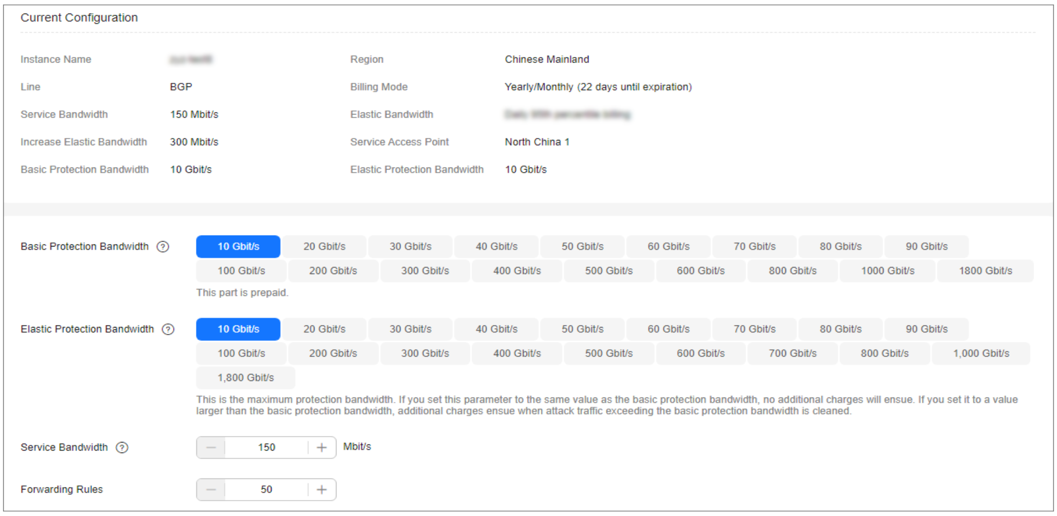
Elastic Protection Bandwidth ⓘ: [✓ 10 Gbit/s] 20 Gbit/s 30 Gbit/s 40 Gbit/s 50 Gbit/s 60 Gbit/s 70 Gbit/s 80 Gbit/s 90 Gbit/s 100 Gbit/s 200 Gbit/s 300 Gbit/s 400 Gbit/s 500 Gbit/s 600 Gbit/s 700 Gbit/s 800 Gbit/s 1,000 Gbit/s 1,800 Gbit/s

This is the maximum protection bandwidth. If you set this parameter to the same value as the basic protection bandwidth, no additional charges will ensue. If you set it to a value larger than the basic protection bandwidth, additional charges ensue when attack traffic exceeding the basic protection bandwidth is cleaned.

Service Bandwidth ⓘ: − 100 + Mbit/s

Protected Domain Names ⓘ: − 50 +

Figure 3-40 Specifications of a IP-based instance



Current Configuration

Instance Name	[redacted]	Region	Chinese Mainland
Line	BGP	Billing Mode	Yearly/Monthly (22 days until expiration)
Service Bandwidth	150 Mbit/s	Elastic Bandwidth	[redacted]
Increase Elastic Bandwidth	300 Mbit/s	Service Access Point	North China 1
Basic Protection Bandwidth	10 Gbit/s	Elastic Protection Bandwidth	10 Gbit/s

Basic Protection Bandwidth ⓘ: [✓ 10 Gbit/s] 20 Gbit/s 30 Gbit/s 40 Gbit/s 50 Gbit/s 60 Gbit/s 70 Gbit/s 80 Gbit/s 90 Gbit/s 100 Gbit/s 200 Gbit/s 300 Gbit/s 400 Gbit/s 500 Gbit/s 600 Gbit/s 800 Gbit/s 1000 Gbit/s 1800 Gbit/s

This part is prepaid.

Elastic Protection Bandwidth ⓘ: [✓ 10 Gbit/s] 20 Gbit/s 30 Gbit/s 40 Gbit/s 50 Gbit/s 60 Gbit/s 70 Gbit/s 80 Gbit/s 90 Gbit/s 100 Gbit/s 200 Gbit/s 300 Gbit/s 400 Gbit/s 500 Gbit/s 600 Gbit/s 700 Gbit/s 800 Gbit/s 1,000 Gbit/s 1,800 Gbit/s

This is the maximum protection bandwidth. If you set this parameter to the same value as the basic protection bandwidth, no additional charges will ensue. If you set it to a value larger than the basic protection bandwidth, additional charges ensue when attack traffic exceeding the basic protection bandwidth is cleaned.

Service Bandwidth ⓘ: − 150 + Mbit/s

Forwarding Rules: − 50 +

Table 3-23 Parameter description

Parameter	Description
Basic Protection Bandwidth	The basic protection bandwidth is purchased by customers. If the peak attack traffic is less than or equal to the basic protection bandwidth, customers do not need to pay extra fees.
Elastic Protection Bandwidth	Elastic protection bandwidth is the maximum available defense bandwidth. The elastic protection bandwidth is not a part that is added on top of the basic protection bandwidth. If the elastic protection bandwidth is the same as the basic protection bandwidth, the elastic bandwidth will not work.

Parameter	Description
Service Bandwidth	The service bandwidth indicates clean service bandwidth forwarded to the origin server from the AAD scrubbing center. Each instance includes 100 Mbit/s of service bandwidth at no charge. If the AAD equipment room is outside of Huawei Cloud, it is recommended that the purchased AAD service bandwidth be equal to or greater than the egress bandwidth of the origin server.
Protected Domain Names	This parameter is available only for domain-based instances.
Forwarding Rules	This parameter is available only for IP-based instances.

Step 6 After you click **Submit**, the system will determine whether the configuration has changed. If the configuration does not change, the system displays a failure message indicating that selected specifications are the same as original specifications. If the configuration has changed, the **Details** page is displayed.

Step 7 Click **Submit Order**. When the payment is successful, the **Order submitted successfully** page is displayed.

----End

3.9.3 Enabling Auto-renewal

If you have enabled auto-renewal when purchasing an AAD instance, When the service period expires, the system automatically renews the instance for another period. You can enable auto-renewal based on your service requirements.

NOTE

If auto-renewal is enabled for a resource, you can manually renew the resource at any time. After the manual renewal is successful, the auto-renewal is still valid, and the system deducts the fee seven days before the manually renewed resource expires. For details about auto-renewal, see **Renewal Rules**.

Prerequisites

Ensure that the account for which auto-renewal is to be enabled has the permissions of both the **AAD FullAccess** and **BSS Administrator** roles.

Enabling Auto-renewal

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

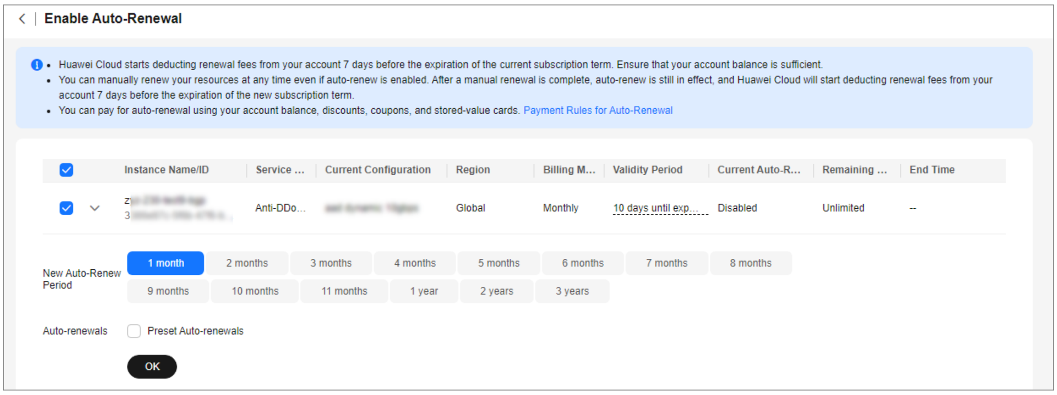
Step 2 Select a region in the upper part of the page, click ☰ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Instance List**. The **Instance List** page is displayed.

Step 4 In the row containing the desired instance, click **Enable Auto-Renewal**. The **Enable Auto-Renewal** page is displayed.

Step 5 Select a renewal period and specify the auto-renewal times.

Figure 3-41 Enabling auto-renewal



Enable Auto-Renewal

- Huawei Cloud starts deducting renewal fees from your account 7 days before the expiration of the current subscription term. Ensure that your account balance is sufficient.
- You can manually renew your resources at any time even if auto-renew is enabled. After a manual renewal is complete, auto-renew is still in effect, and Huawei Cloud will start deducting renewal fees from your account 7 days before the expiration of the new subscription term.
- You can pay for auto-renewal using your account balance, discounts, coupons, and stored-value cards. Payment Rules for Auto-Renewal

☑	Instance Name/ID	Service ...	Current Configuration	Region	Billing M...	Validity Period	Current Auto-R...	Remaining ...	End Time
☑	z[redacted] 3[redacted]	Anti-DDo...	[redacted]	Global	Monthly	10 days until exp...	Disabled	Unlimited	--

New Auto-Renew Period: 1 month | 2 months | 3 months | 4 months | 5 months | 6 months | 7 months | 8 months | 9 months | 10 months | 11 months | 1 year | 2 years | 3 years

Auto-renewals: □ Preset Auto-renewals

Step 6 Click **OK** and enable auto-renewal as prompted.

----End

3.9.4 Configuring Instance Tags

A tag consists of a tag key and a tag value and is used to identify cloud resources. You can use tags to classify cloud resources by dimension, such as usage, owner, or environment. Tags allow you to better manage AAD instances.

Configuring Tags for an AAD Instance

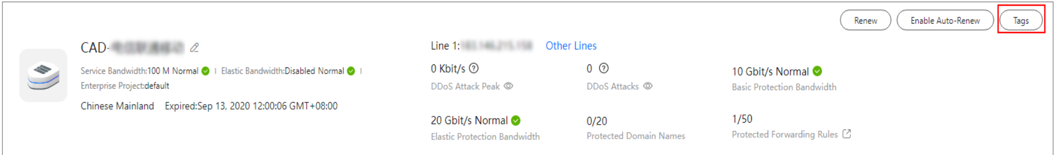
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Instance List**. The **Instance List** page is displayed.

Step 4 Locate the row that contains the target AAD instance and click **Tags**.

Figure 3-42 Configuring tags for an AAD instance



CAD-[redacted]

Service Bandwidth:100 M Normal | Elastic Bandwidth:Disabled Normal | Enterprise Project:default

Chinese Mainland Expired:Sep 13, 2020 12:00:06 GMT+08:00

Line 1:[redacted] Other Lines

0 Kbit/s DDoS Attack Peak

0 DDoS Attacks

10 Gbit/s Normal Basic Protection Bandwidth

20 Gbit/s Normal Elastic Protection Bandwidth

0/20 Protected Domain Names

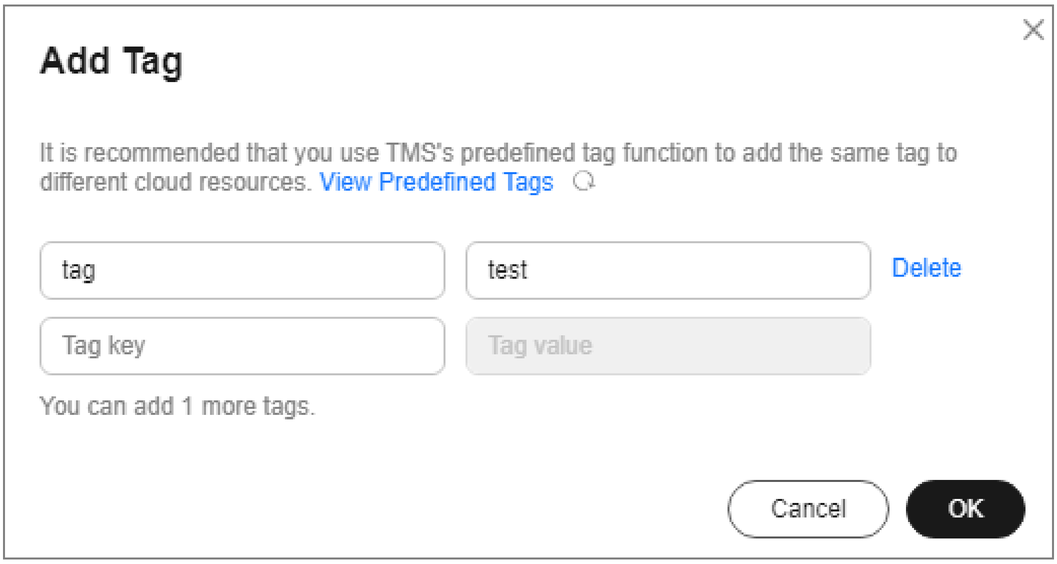
1/50 Protected Forwarding Rules

Step 5 On the tag adding page, click **Add Tag** to add a tag.

Step 6 Select the **Tag key** and **Tag value**. There are two ways to add a tag:

- Manually enter a tag key and tag value.
- Select an existing tag.

Figure 3-43 Adding a tag



Add Tag

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View Predefined Tags

tag | test

Tag key | Tag value

You can add 1 more tags.

NOTE

If your organization has configured a tag policy for the service, you need to add tags to resources based on the tag policy. Otherwise, the tagging operation might fail. For more information about the tag policy, contact your organization administrator.

Step 7 Click **OK**.

----End

3.10 Managing Domain Names

3.10.1 Viewing Information About a Domain Name

After a domain name is connected to AAD, you can view information about the domain name in the domain name list to ensure that its protection status is normal.

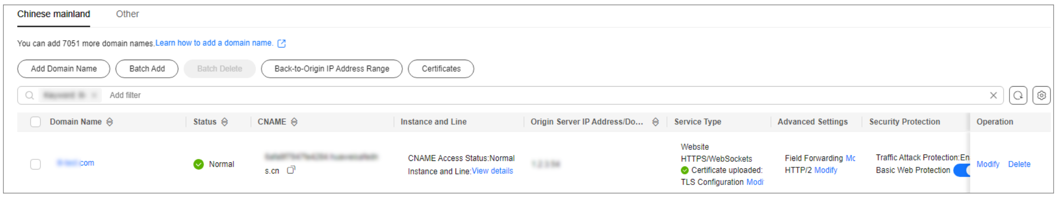
Viewing Information About a Domain Name

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-44 Domain name access



You can add 7051 more domain names. Learn how to add a domain name.

Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Operation
[redacted]com	Normal	[redacted] s.cn	CNAME Access Status:Normal Instance and Line:View details	[redacted]	Website HTTPS/WebSockets Certificate uploaded: TLS Configuration Modi	Field Forwarding Mc HTTP/2 Modify	Traffic Attack Protection:En Basic Web Protection	Modify Delete

Step 4 View information about the domain name.

Table 3-24 Parameter description

Parameter	Description
Domain Name	Protected domain name. You can click a domain name to view its Web CC protection details.
CNAME	- CNAME record obtained for the domain name after a CNAME resolution - Click ❐ to copy the CNAME record.
Instance and Line	- CNAME-based access status of the domain name - Click **View details** to view details about the line of the domain name. - Enable **CNAME-based Auto Scheduling** so that DNS resolution will automatically schedule the traffic if the high-defense IP address is blocked by a black hole.
Origin Server IP Address/Domain name	IP address or domain name of the origin server.
Service Type	- Service type of the domain name - Locate the row that contains **HTTPS/WebSockets** certificate, click **Update** in the **Service Type** column to update the certificate. For details, see **Updating a Certificate**.
Security Protection	Status of traffic attack protection, basic web protection, and CC attack protection - For a website service whose **Origin Server Type** is set to **IP address**, you can enable basic web protection and CC attack protection for your domain name. - For a website service whose **Origin Server Type** is set to **Domain name**, you do not need to enable basic web protection and CC attack protection for your domain name. - For a non-website service, only traffic attack defense is provided and enabled by default.
Enterprise Project	Enterprise project that the instance belongs to.

----End

3.10.2 Modifying Resolution Lines for High-Defense IP Addresses of a Domain Name

After your service is connected to AAD, you can change the high-defense IP resolution line to change the resolution line of the corresponding domain name.

NOTICE

Modifying the resolution line of a high-defense IP address may cause protection failure or service interruption. Exercise caution when performing this operation.

Limitations and Constraints

The change takes effect in about five minutes.

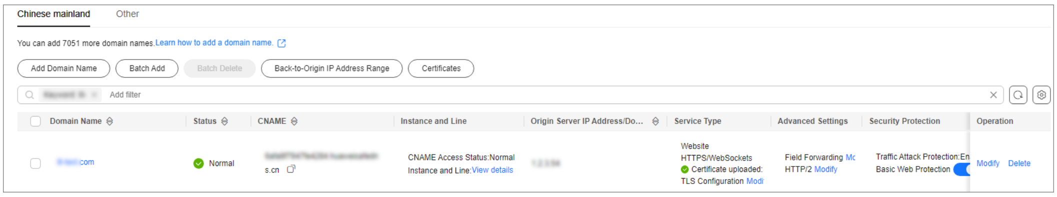
Changing the Resolution Line for a Domain Name

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-45 Domain name access



You can add 7051 more domain names. Learn how to add a domain name.

Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Operation
[redacted]com	Normal	[redacted] s.cn	CNAME Access Status:Normal Instance and Line:View details	[redacted]	Website HTTPS/WebSockets Certificate uploaded: TLS Configuration Modi	Field Forwarding Mc HTTP/2 Modify	Traffic Attack Protection:En Basic Web Protection	Modify Delete

Step 4 In the row containing the desired domain name, click **View details** in the **Instance and Line** column.

Step 5 Modify the resolution lines for the domain name.

- Disable DNS resolution for a high-defense IP address of the domain name.

  On the line details page, change **Line Resolution** to ○ for the line to be disabled to disable domain name resolution for the high-defense IP address of the AAD instance and line. After you disable DNS resolution, you can still use the A record for the high-defense IP address.

- Add a resolution line for the domain name.

  a. On the line details page, click **Add Instance Line**.

b. In the **Add Instance Line** dialog box, select instances and lines and click **OK**.

c. Set **Line Resolution Switch** to ● to enable DNS resolution for the high-defense IP addresses.

- Delete a resolution line for the domain name.

   a. Close the line to be deleted.

   b. Locate the row that contains the disabled line, and click **Delete Line**.

   c. Click **OK**.

- Export all rules.

   On the line details page, click **Export All** to export all forwarding rules of the domain name.

----End

3.10.3 Modifying Domain Name Configuration

After a domain name is connected to AAD, if the origin server information changes, you can modify the origin server information in the domain name list.

NOTICE

Modifying the origin server IP address may cause protection failure or service interruption. Exercise caution when performing this operation.

Limitations and Constraints

- If this protected domain name will share a high-defense IP address and port with another domain name, ensure that they have the same **Origin Server Type** value.
- To change the **Origin Server Type** value from **IP address** to **Domain name**, ensure that **Basic Web Protection** is disabled for the domain name.

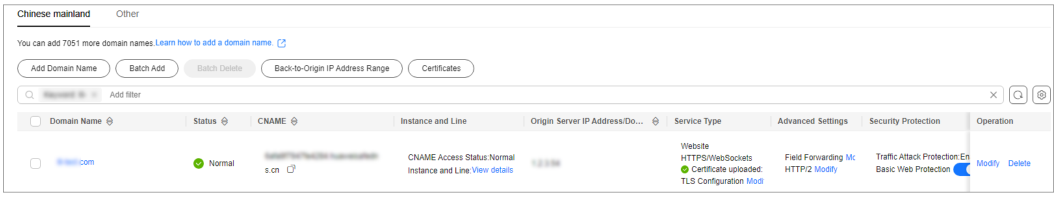
Modifying Domain Name Configuration

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-46 Domain name access



You can add 7051 more domain names. Learn how to add a domain name.

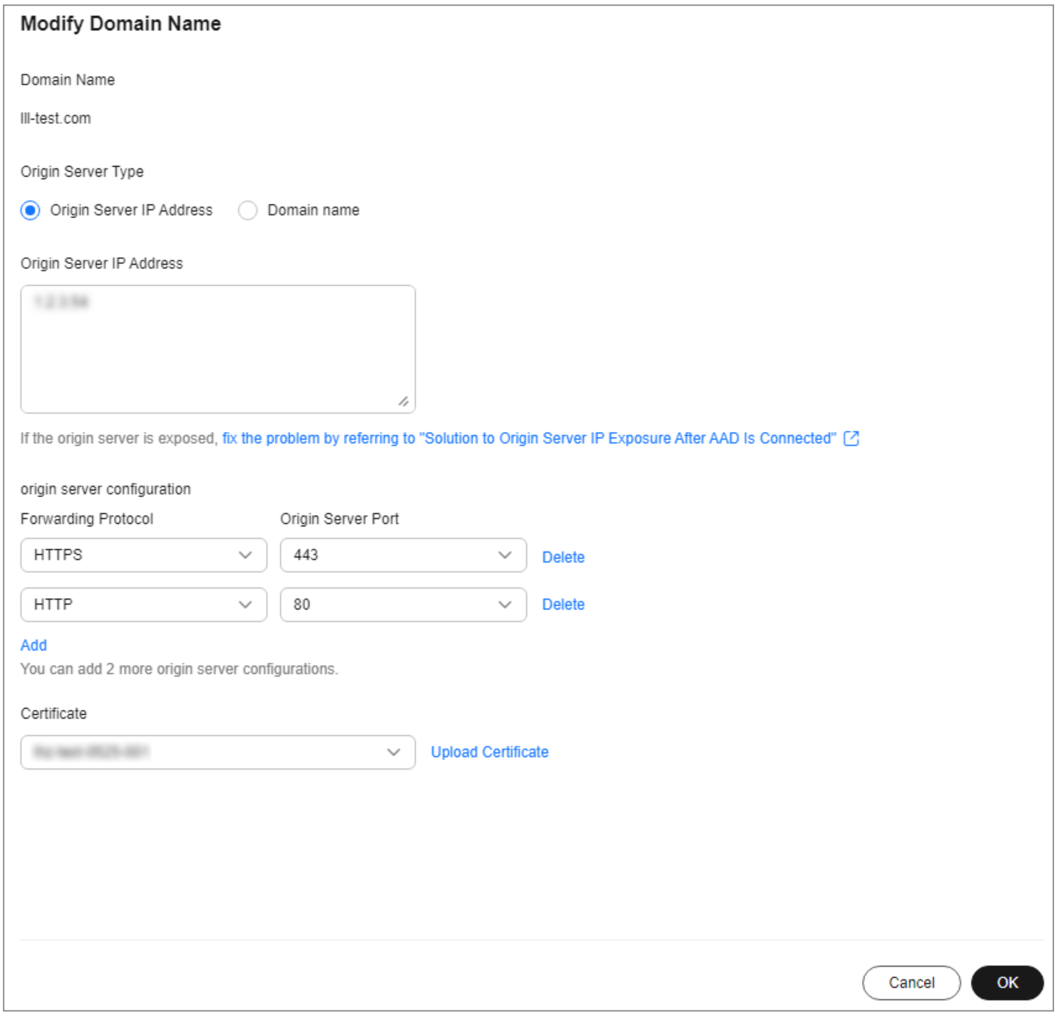
[redacted]

☐	Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Operation
☐	[redacted].com	✓ Normal	[redacted]s.cn	CNAME Access Status:Normal Instance and Line:View details	[redacted]	Website HTTPS/WebSockets ✓ Certificate uploaded: TLS Configuration Modi	Field Forwarding Mc HTTP/2 Modify	Traffic Attack Protection:En Basic Web Protection	Modify Delete

Step 4 In the row containing the desired domain name, click **Modify** in the **Operation** column.

Step 5 In the **Modify Domain Name** dialog box that is displayed, modify the domain name configurations.

Figure 3-47 Modifying the domain name configuration



Modify Domain Name

Domain Name

lll-test.com

Origin Server Type

● Origin Server IP Address ○ Domain name

Origin Server IP Address

If the origin server is exposed, fix the problem by referring to "Solution to Origin Server IP Exposure After AAD Is Connected"

origin server configuration

Forwarding Protocol	Origin Server Port	
HTTPS	443	Delete
HTTP	80	Delete

Add

You can add 2 more origin server configurations.

Certificate

Upload Certificate

Step 6 Click **OK**.

----End

3.10.4 Modify TLS Configuration

Once a domain name is connected to AAD, you can adjust the minimum TLS version and the encryption algorithm that matches the HTTPS certificate in the domain name list.

NOTE

Access is denied for requests from TLS versions older than the minimum TLS version.

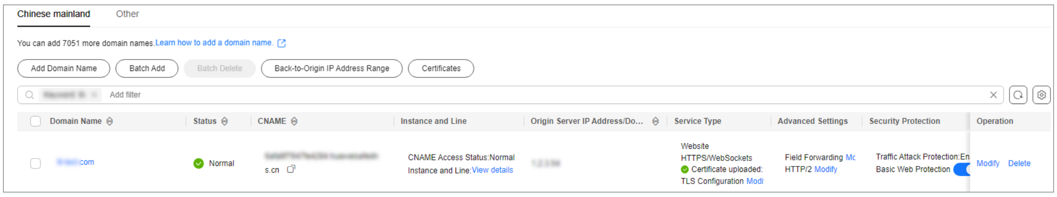
Modify TLS Configuration

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-48 Domain name access



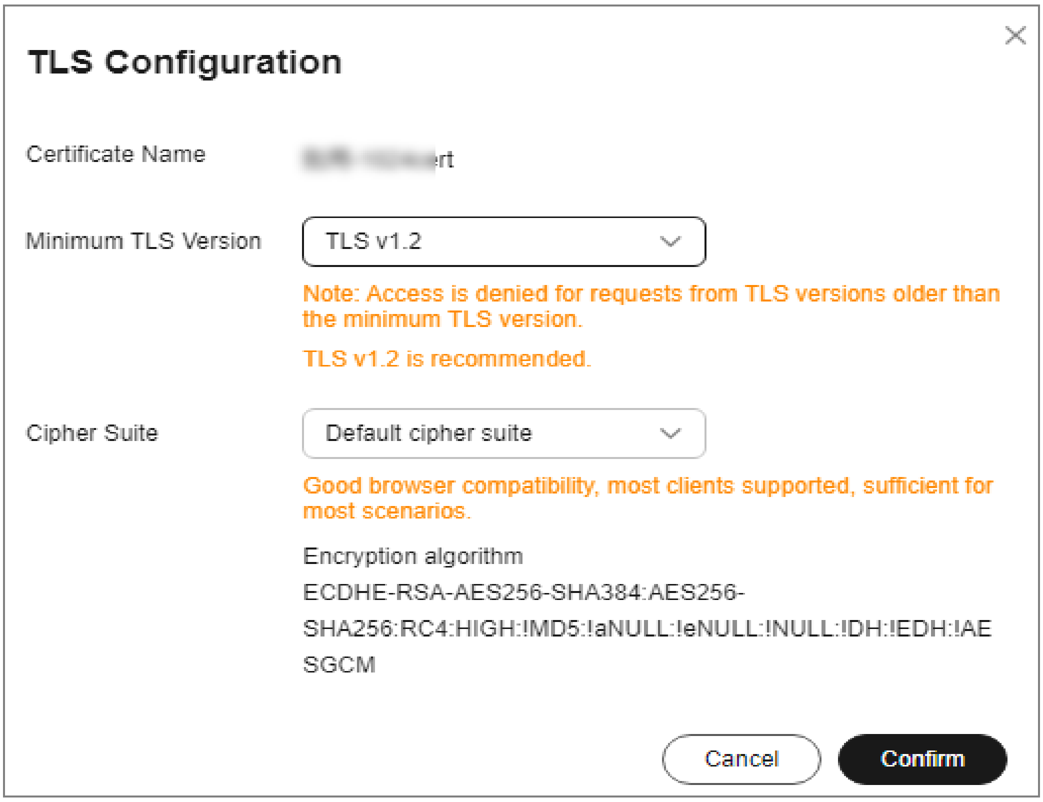
You can add 7051 more domain names. Learn how to add a domain name.

Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Operation
[illegible]com	Normal	[illegible]s.cn	CNAME Access Status:Normal Instance and Line:View details	[illegible]	Website HTTPS/WebSockets Certificate uploaded: TLS Configuration Modi	Field Forwarding Mc HTTP/2 Modify	Traffic Attack Protection:En Basic Web Protection	Modify Delete

Step 4 Click **Edit** next to **TLS Configuration** of the target domain name.

Step 5 After selecting the TLS version and cipher suite, click **Confirm**.

Figure 3-49 Forwarding rule fields



TLS Configuration

Certificate Name: [illegible]rt

Minimum TLS Version: TLS v1.2

Note: Access is denied for requests from TLS versions older than the minimum TLS version.

TLS v1.2 is recommended.

Cipher Suite: Default cipher suite

Good browser compatibility, most clients supported, sufficient for most scenarios.

Encryption algorithm
ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM

----End

3.10.5 Setting the HTTP2 Protocol

If your domain name supports HTTP/2, you can enable HTTP/2 protection on the **Domain Name Access** page.

Limitations and Constraints

- HTTP2 can be set only for domain names whose forwarding protocol is HTTPS and with basic web protection enabled.
- HTTP/2 takes effect only when the TLS version of the client is not later than TLS 1.2.

Prerequisites

Basic web protection has been enabled for the connected domain name. For details, see **Enabling Basic Web Protection**.

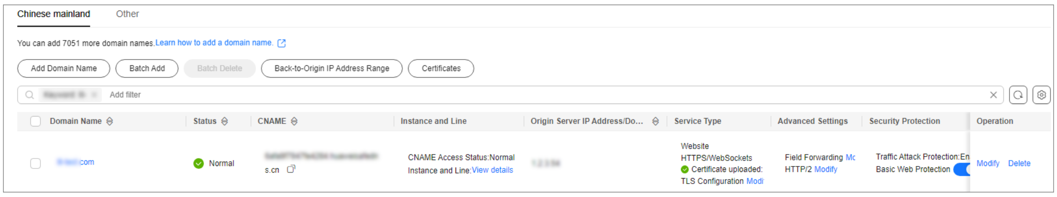
Enabling the HTTP/2 Protocol

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

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-50 Domain name access



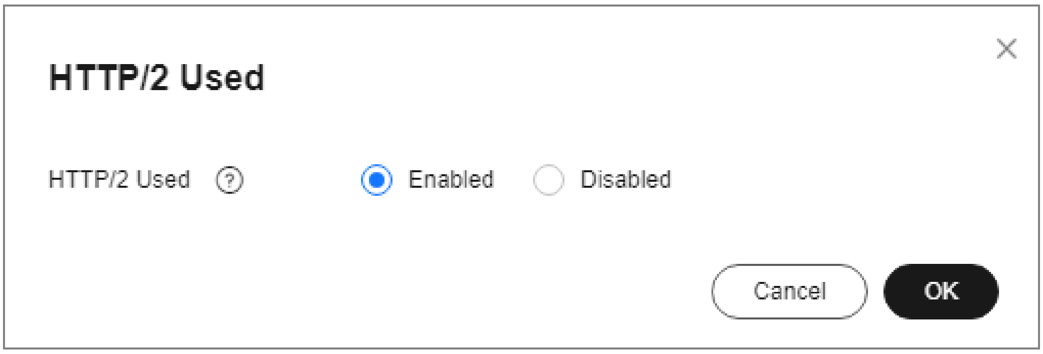
You can add 7051 more domain names. Learn how to add a domain name.

☐	Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Operation
☐	[redacted]com	✓ Normal	[redacted] s.cn	CNAME Access Status:Normal Instance and Line:View details	[redacted]	Website HTTPS/WebSockets ✓ Certificate uploaded: TLS Configuration Modi	Field Forwarding Mc HTTP/2 Modify	Traffic Attack Protection:En Basic Web Protection	Modify Delete

Step 4 Click **Edit** after the **HTTP2 Protocol** of the target domain name.

Step 5 Set HTTP2 based on the site requirements.

Figure 3-51 HTTP2 protocol



HTTP/2 Used

HTTP/2 Used ⓘ ● Enabled ○ Disabled

Step 6 Click **OK**.

----End

3.10.6 Configuring Field Forwarding

AAD lets you configure field forwarding for domain names to add fields to the header and send it to the origin server.

You can add header fields to the back-to-origin requests to identify those that pass through AAD for service statistics analysis.

Limitations and Constraints

- You can configure up to eight key/value pairs.
- Note that the key value of a custom header field cannot be the same as any native Nginx fields.
- The value can be set to a custom string or a variable starting with $. Variables starting with $support only the following fields:

```
$time_local
$request_id
$connection_requests
$tenant_id
$project_id
$remote_addr
$remote_port
$scheme
$request_method
$http_host
$origin_uri
$request_length
$ssl_server_name
$ssl_protocol
$ssl_curves
$ssl_session_reused
```

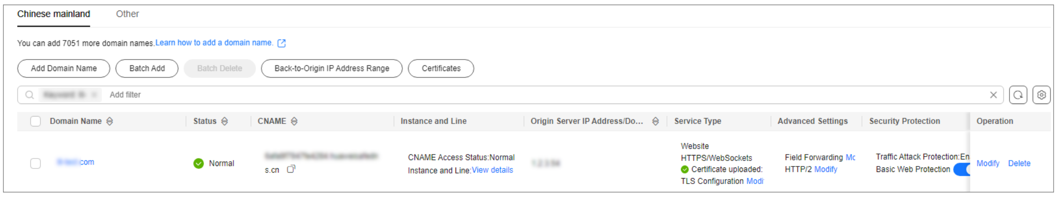
Configuring Field Forwarding

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-52 Domain name access



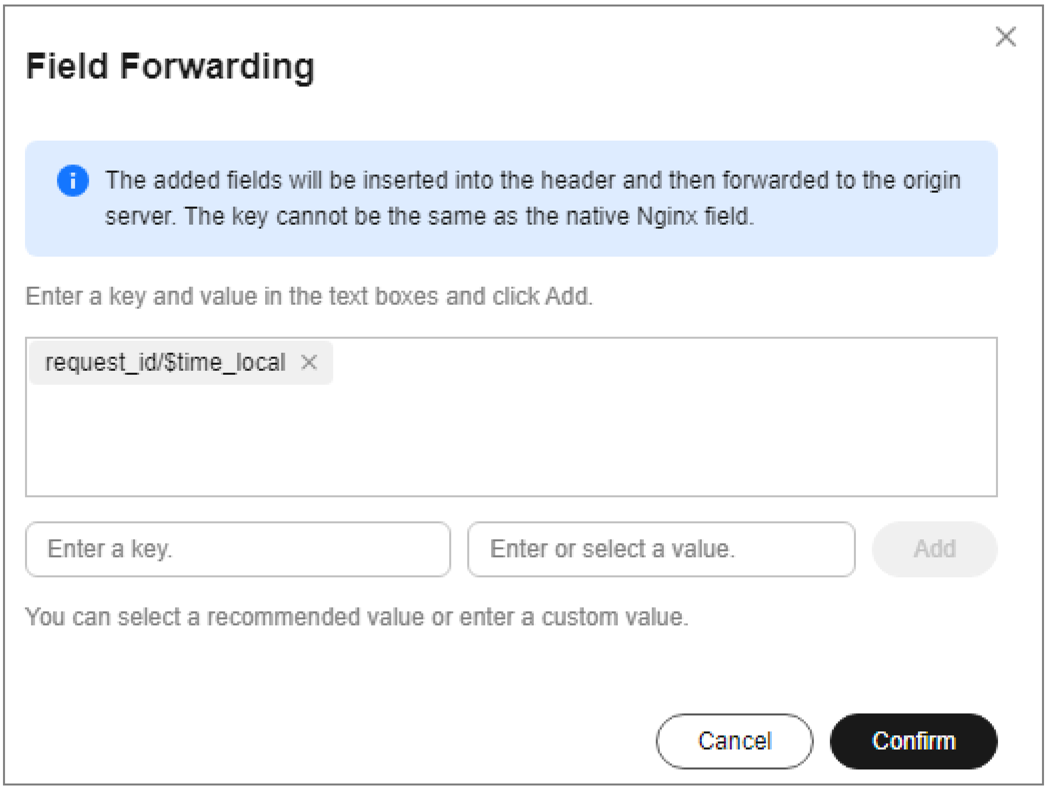
You can add 7051 more domain names. Learn how to add a domain name.

□	Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Operation
□	[redacted]com	Normal	[redacted] s.cn	CNAME Access Status:Normal Instance and Line:View details	[redacted]	Website HTTPS/WebSockets Certificate uploaded: TLS Configuration Modi	Field Forwarding Mc HTTP/2 Modify	Traffic Attack Protection:En Basic Web Protection	Modify Delete

Step 4 In the **Advanced Setting** column of the row containing the target domain name, click **Modify**.

Step 5 Enter the Key/Value value and click **Add**.

Figure 3-53 Forwarding rule fields



Field Forwarding

The added fields will be inserted into the header and then forwarded to the origin server. The key cannot be the same as the native Nginx field.

Enter a key and value in the text boxes and click Add.

request_id/$time_local ×

Enter a key. | Enter or select a value.

You can select a recommended value or enter a custom value.

Step 6 Click **OK**.

----End

3.10.7 Adding Domain Names in Batches

If multiple domain names need to be connected to AAD, you can add them in batches using XML files.

Adding Domain Names to AAD in Batches

Step 1 Prepare the **.xml** domain name file based on the following example.

```
<DomainList>
  <DomainConfig>
    <Domain>example.domain.com</Domain>
    <InstanceConfig>
      <InstanceList>CAD-159</InstanceList>
    </InstanceConfig>
    <RealServerConfig>
      <ServerPortList>80,443</ServerPortList>
      <ServerList>xx.xx.xx.xx</ServerList>
    </RealServerConfig>
    <CertificateConfig>
      <Certificate>certificateName</Certificate>
    </CertificateConfig>
  </DomainConfig>
  <DomainConfig>
    <Domain>demo.domain.com</Domain>
    <InstanceConfig>
      <InstanceList>CAD-169,CAD-179</InstanceList>
    </InstanceConfig>
    <RealServerConfig>
      <ServerPortList>80,443</ServerPortList>
      <ServerList>learn.domain.com</ServerList>
    </RealServerConfig>
  </DomainConfig>
</DomainList>
```

Table 3-25 Parameter description

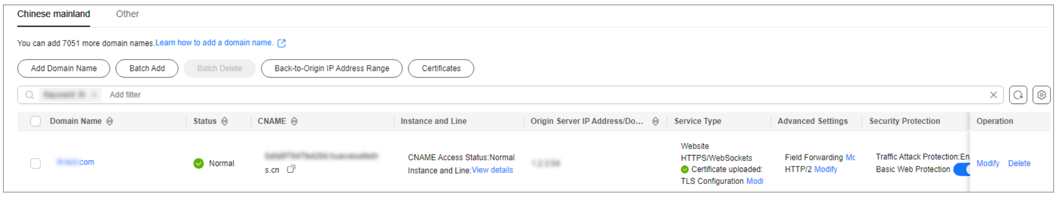
Parameter	Description
<Domain>***example.domain.com***</Domain>	***example.domain.com*** indicates the name of the domain to be added. Only one domain name can be set for this field.
<InstanceList>***CAD-159***</InstanceList>	***CAD-159*** indicates the ID of the AAD instance. Use commas (,) to separate multiple instances.
<Certificate>***certificateName***</Certificate>	***certificateName*** indicates the certificate used by the HTTPS port. If there is no HTTPS port, this parameter can be ignored.
<RealServerConfig><ServerPortList>***80,443***</ServerPortList><ServerList>***xx.xx.xx.xx***</ServerList></RealServerConfig>	Origin server details ● ***80,443*** indicates the port number of the origin server. Use commas (,) to separate multiple port numbers. ● ***xx.xx.xx.xx*** indicates the origin server address. Use commas (,) to separate multiple addresses. ● Both origin server IP addresses and origin server domain names are supported, but they cannot be used at the same time.

Step 2 Log in to the management console.

Step 3 Select a region in the upper part of the page, click ☰ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

Step 4 In the navigation pane on the left, choose **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-54 Domain name access



Chinese mainland | Other

You can add 7051 more domain names. Learn how to add a domain name.

Add Domain Name | Batch Add | Batch Delete | Back-to-Origin IP Address Range | Certificates

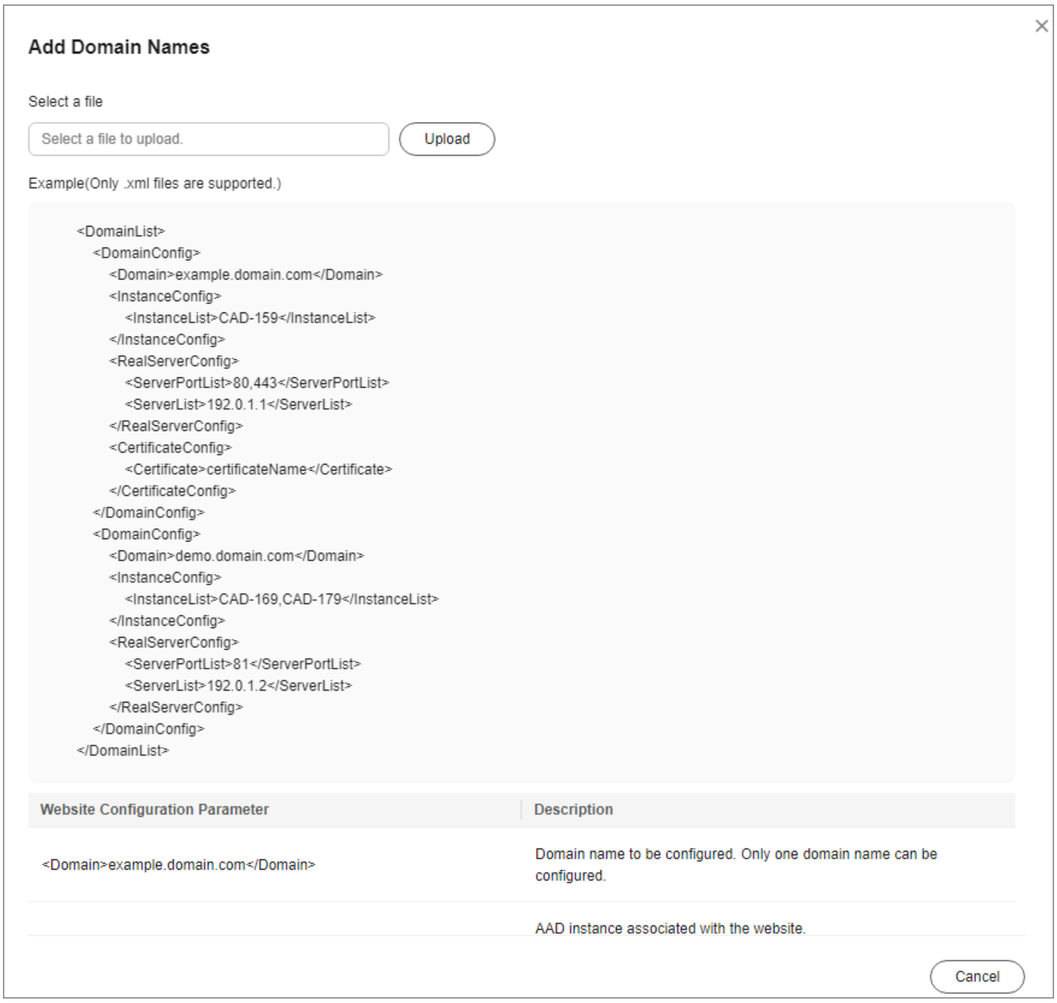
[redacted] Add filter

□	Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Operation
□	[redacted]com	Normal	[redacted] s.cn	CNAME Access Status:Normal Instance and Line:View details	[redacted]	Website HTTPS/WebSockets Certificate uploaded: TLS Configuration Modi	Field Forwarding Mc HTTP/2 Modify	Traffic Attack Protection:En Basic Web Protection	Modify Delete

Step 5 Click **Batch Add**.

Step 6 Click **Upload** file and select the local **.xml** domain name file.

Figure 3-55 Uploading the domain name file



Add Domain Names

Select a file

Example(Only .xml files are supported.)

```
<DomainList>
  <DomainConfig>
    <Domain>example.domain.com</Domain>
    <InstanceConfig>
      <InstanceList>CAD-159</InstanceList>
    </InstanceConfig>
    <RealServerConfig>
      <ServerPortList>80,443</ServerPortList>
      <ServerList>192.0.1.1</ServerList>
    </RealServerConfig>
    <CertificateConfig>
      <Certificate>certificateName</Certificate>
    </CertificateConfig>
  </DomainConfig>
  <DomainConfig>
    <Domain>demo.domain.com</Domain>
    <InstanceConfig>
      <InstanceList>CAD-169,CAD-179</InstanceList>
    </InstanceConfig>
    <RealServerConfig>
      <ServerPortList>81</ServerPortList>
      <ServerList>192.0.1.2</ServerList>
    </RealServerConfig>
  </DomainConfig>
</DomainList>
```

Website Configuration Parameter	Description
<Domain>example.domain.com</Domain>	Domain name to be configured. Only one domain name can be configured.
	AAD instance associated with the website.

Step 7 Click **Close**.

----End

3.10.8 Deleting Domain Names

If your services change and you no longer need to protect a domain name, you can delete the domain name on the **Domain Name Access** page.

NOTICE

Before deleting a domain name, you need to ensure that the DNS domain name provider has changed the CNAME record to the real IP address. Otherwise, deleting the domain name will cause service interruption or unavailability.

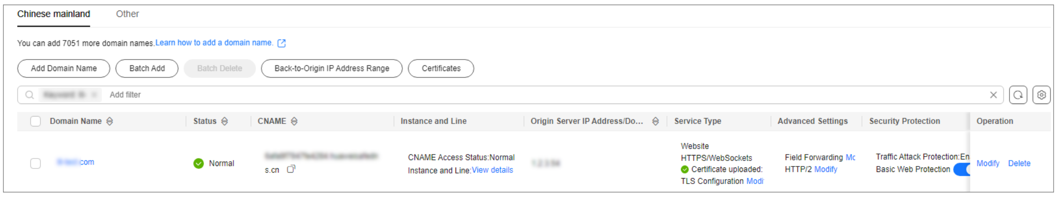
Deleting Domain Names

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-56 Domain name access



You can add 7051 more domain names.Learn how to add a domain name.

[redacted]

	Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Operation
□	[redacted]com	Normal	[redacted] s.cn	CNAME Access Status:Normal Instance and Line:View details	[redacted]	Website HTTPS/WebSockets Certificate uploaded: TLS Configuration Modi	Field Forwarding Mc HTTP/2 Modify	Traffic Attack Protection:En Basic Web Protection	Modify Delete

Step 4 Select a deletion mode.

- **Deleting a single domain name**: In the **Operation** column of the row containing the domain name to be deleted, click **Delete**.
- **Deleting domain names in batches**: Select the domain names to be deleted and click **Batch Delete**.

Step 5 Click **OK**.

----End

3.11 Certificate Management

3.11.1 Updating a Certificate

If the purchased certificate is about to expire, you are advised to purchase a new certificate before the expiration date and update the certificate associated with the domain name in AAD.

To update the certificate associated with a domain name, you can associate a new certificate with the domain name in AAD.

NOTICE

- The certificate takes effect 1 minute after it is updated. Therefore, update certificates in off-peak hours.
- Certificate expiration has a great impact on the origin server. You are advised to update the certificate before it expires.
- Each domain name must be associated with a certificate. A wildcard domain name can only be used for a wildcard domain certificate. If you have not purchased a wildcard domain certificate and have only a single-domain certificate, you can only add domain names one by one in AAD.

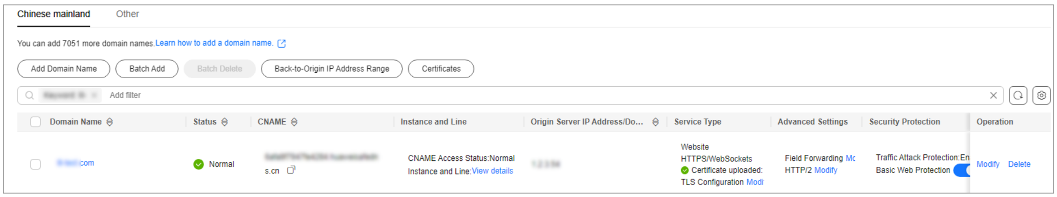
Updating a Certificate

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-57 Domain name access



You can add 7051 more domain names.Learn how to add a domain name.

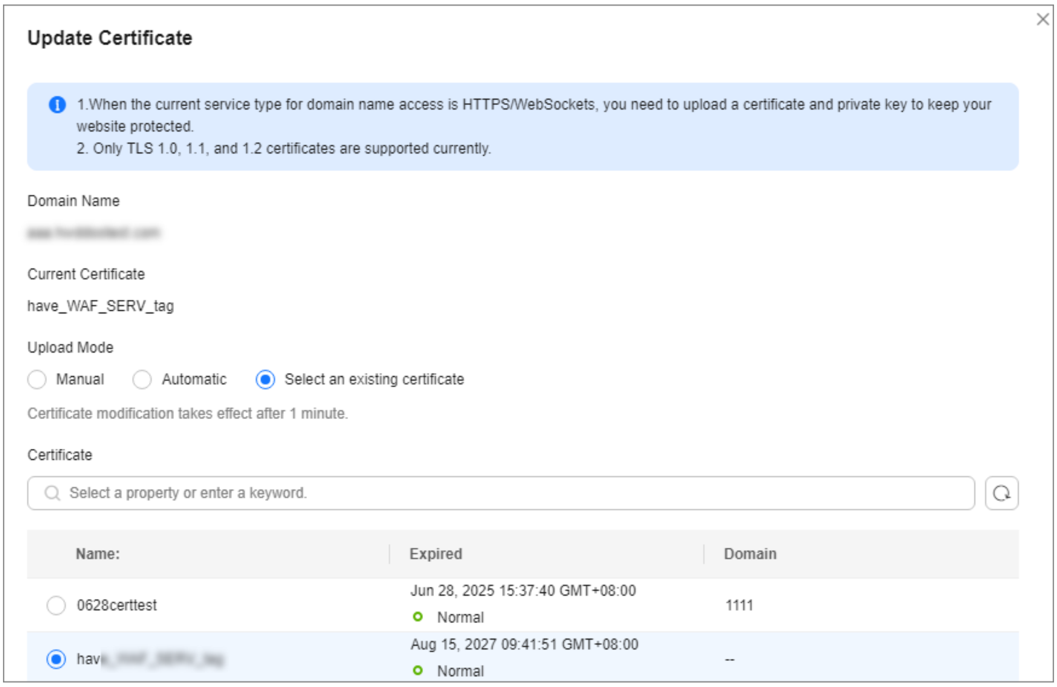
Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Operation
[redacted]com	Normal	[redacted] s.cn	CNAME Access Status:Normal Instance and Line:View details	[redacted]	Website HTTPS/WebSockets Certificate uploaded: TLS Configuration Modi	Field Forwarding Mc HTTP/2 Modify	Traffic Attack Protection:En Basic Web Protection	Modify Delete

Step 4 Locate the row that contains the target domain name, and click **Update** in the **Service Type** column.

Step 5 In the displayed **Update Certificate** dialog box, upload a new certificate or select an existing certificate.

- **Manual**: Enter the certificate name and paste the certificate and private key text. Currently, only PEM certificates are supported. For details about how to convert non-PEM certificates, see Table 3-26.
- **Automatic**: Select an issued certificate.
- **Select an existing certificate**: Select the certificate that is in use.

Figure 3-58 Replacing a certificate



Update Certificate

1.When the current service type for domain name access is HTTPS/WebSockets, you need to upload a certificate and private key to keep your website protected.
2. Only TLS 1.0, 1.1, and 1.2 certificates are supported currently.

Domain Name

[redacted]

Current Certificate

have_WAF_SERV_tag

Upload Mode

○ Manual ○ Automatic ● Select an existing certificate

Certificate modification takes effect after 1 minute.

Certificate

	Name:	Expired	Domain
○	0628certtest	Jun 28, 2025 15:37:40 GMT+08:00 Normal	1111
●	hav[redacted]	Aug 15, 2027 09:41:51 GMT+08:00 Normal	--

Table 3-26 Certificate format conversion commands

Format	Conversion Method
CER/CRT	Rename the **cert.crt** certificate file to **cert.pem**.
PFX	Use OpenSSL to convert the certificate. Obtain a private key. For example, run the following command to convert **cert.pfx** into **cert.key**: **openssl pkcs12 -in cert.pfx -nocerts -out cert.key -nodes** Obtain a certificate. For example, run the following command to convert **cert.pfx** into **cert.pem**: **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**
P7B	Use OpenSSL to convert the certificate. 1. Run the following command to convert the certificate: **openssl pkcs7 -print_certs -in incertificat.p7b -out cert.cer** 2. Obtain the certificate content in **cert.cer**. 3. Save the content in .pem format.
DER	Use OpenSSL to convert the certificate. 1. Obtain a private key. For example, run the following command to convert **privatekey.der** into **privatekey.pem**: **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** 2. Obtain a certificate. For example, run the following command to convert **cert.cer** into **cert.pem**: **openssl x509 -inform der -in cert.cer -out cert.pem**

NOTE

Before running the openssl command in Windows, ensure that the **OpenSSL** tool has been installed.

Step 6 Click **OK**.

----End

3.11.2 Viewing a Certificate

Once a certificate is bound to a domain name, periodically check the certificate information on the certificate management page and update it as needed to prevent service access failures after the certificate expires.

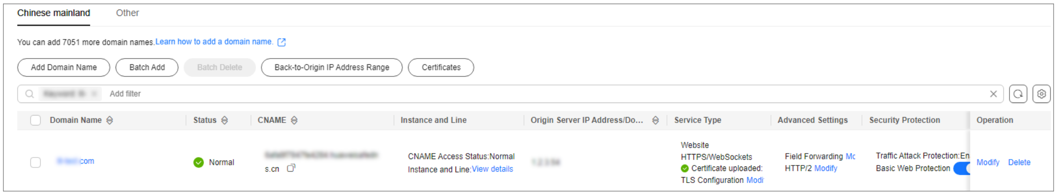
Checking Certificate Details

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

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-59 Domain name access

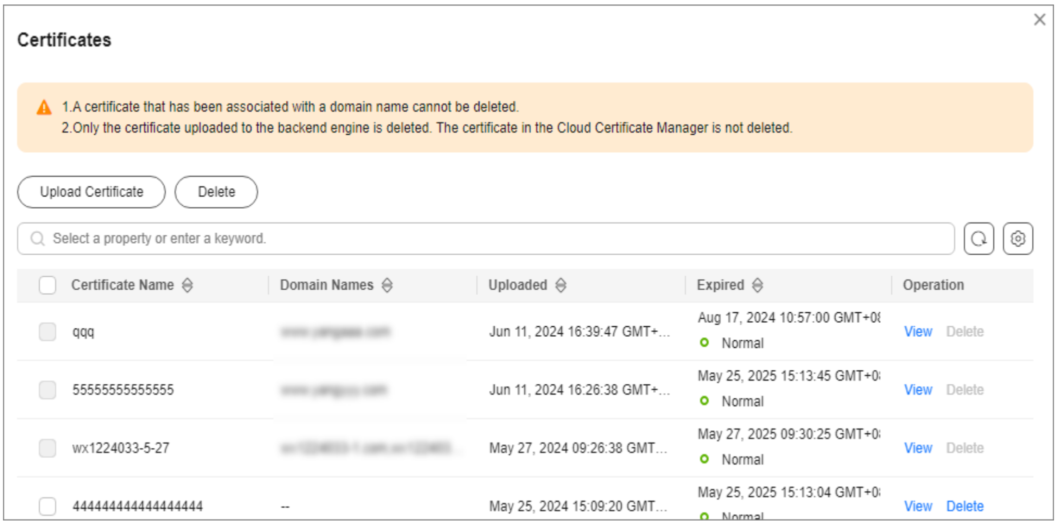


You can add 7051 more domain names. Learn how to add a domain name.

Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Operation
[redacted]com	Normal	[redacted] s.cn	CNAME Access Status:Normal Instance and Line:View details	[redacted]	Website HTTPS/WebSockets Certificate uploaded: TLS Configuration Modi	Field Forwarding Mc HTTP/2 Modify	Traffic Attack Protection:En Basic Web Protection	Modify Delete

Step 4 Choose **Certificates** to view the certificate information.

Figure 3-60 Viewing the certificate



1.A certificate that has been associated with a domain name cannot be deleted.
2.Only the certificate uploaded to the backend engine is deleted. The certificate in the Cloud Certificate Manager is not deleted.

Certificate Name	Domain Names	Uploaded	Expired	Operation
qqq	[redacted]	Jun 11, 2024 16:39:47 GMT+...	Aug 17, 2024 10:57:00 GMT+0 Normal	View Delete
55555555555555	[redacted]	Jun 11, 2024 16:26:38 GMT+...	May 25, 2025 15:13:45 GMT+0 Normal	View Delete
wx1224033-5-27	[redacted]	May 27, 2024 09:26:38 GMT...	May 27, 2025 09:30:25 GMT+0 Normal	View Delete
4444444444444444	--	May 25, 2024 15:09:20 GMT...	May 25, 2025 15:13:04 GMT+0 Normal	View Delete

Table 3-27 Parameter description

Parameter	Description
Certificate Name	Certificate name.
Domain Name	Domain name associated with the certificate.
Uploaded	Time when the certificate is uploaded.
Expired	Time when the certificate expires.

NOTE

Locate the row that contains the target certificate, and click **View** to view the certificate information.

----End

3.11.3 Uploading a Certificate

If the origin server type is IP address and the forwarding protocol is HTTPS, you need to bind a certificate to the protected domain name. Before binding a certificate, you can upload the required certificate on the certificate management page.

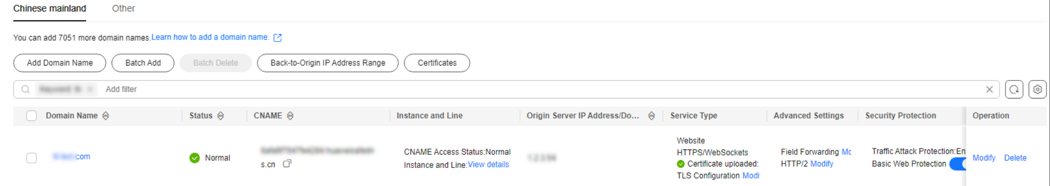
Uploading a Certificate

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-61 Domain name access



Chinese mainland   Other

You can add 7051 more domain names. Learn how to add a domain name.

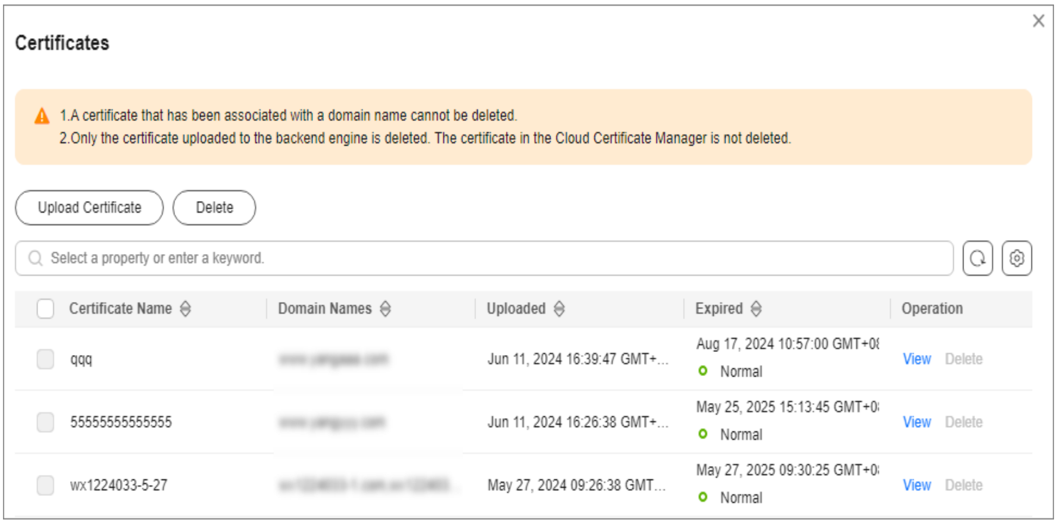
Add Domain Name | Batch Add | Batch Delete | Back-to-Origin IP Address Range | Certificates

[redacted] Add filter

☐	Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Operation
☐	[redacted]com	✓ Normal	[redacted] s.cn	CNAME Access Status:Normal Instance and Line:View details	[redacted]	Website HTTPS/WebSockets ✓ Certificate uploaded: TLS Configuration Modi	Field Forwarding Mc HTTP/2 Modify	Traffic Attack Protection:En Basic Web Protection	Modify Delete

Step 4 Choose **Certificates**. The certificate list is displayed.

Figure 3-62 Viewing the certificate



Certificates

1.A certificate that has been associated with a domain name cannot be deleted.
2.Only the certificate uploaded to the backend engine is deleted. The certificate in the Cloud Certificate Manager is not deleted.

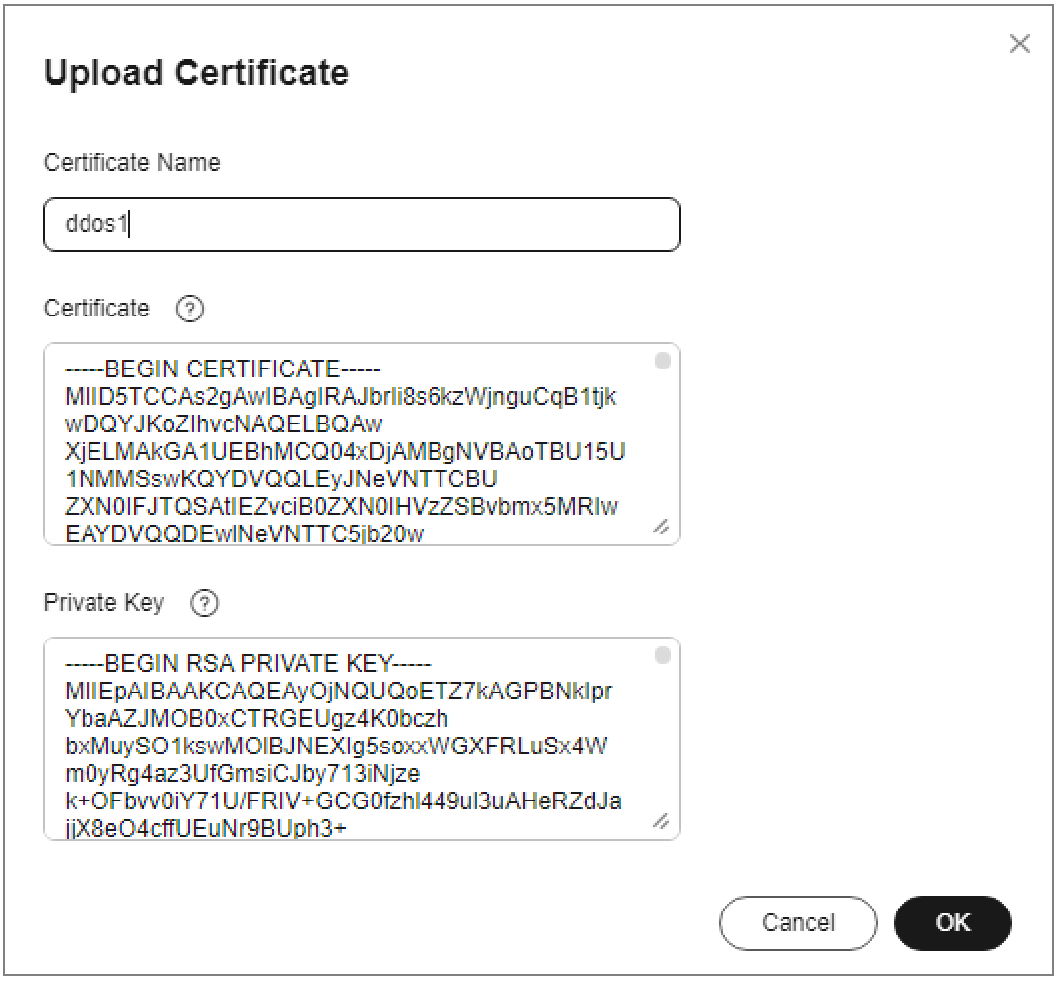
Upload Certificate | Delete

Select a property or enter a keyword.

☐	Certificate Name	Domain Names	Uploaded	Expired	Operation
☐	qqq	[redacted]	Jun 11, 2024 16:39:47 GMT+...	Aug 17, 2024 10:57:00 GMT+0 Normal	View Delete
☐	55555555555555	[redacted]	Jun 11, 2024 16:26:38 GMT+...	May 25, 2025 15:13:45 GMT+0 Normal	View Delete
☐	wx1224033-5-27	[redacted]	May 27, 2024 09:26:38 GMT...	May 27, 2025 09:30:25 GMT+0 Normal	View Delete

Step 5 Click **Upload Certificate**.

Step 6 Enter the certificate name and paste the certificate and private key text content. Currently, only PEM certificates are supported. For details about how to convert non-PEM certificates to PEM certificates, see **Table 3-28**.



Certificate Name: ddos1

Certificate

```
-----BEGIN CERTIFICATE-----
MIID5TCCAs2gAwIBAgIRAJbrli8s6kzWjnguCqB1tjk
wDQYJKoZIhvcNAQELBQAw
XjELMAkGA1UEBhMCQ04xDjAMBgNVBAoTBU15U
1NMMSswKQYDVQQLEyJNeVNTTCBU
ZXN0IFJTQSAtIEZvciB0ZXN0IHVzZSBvbmx5MRIw
EAYDVQQDEwlNeVNTTC5jb20w
```

Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAyOjNQUQoETZ7kAGPBNklpr
YbaAZJMOB0xCTRGEUgz4K0bczh
bxMuySO1kswMOlBJNEXIg5soxxWGXFRLuSx4W
m0yRg4az3UfGmsiCJby713iNjze
k+OFbvv0iY71U/FRIV+GCG0fzhl449ul3uAHeRZdJa
jjX8eO4cffUEuNr9BUph3+
```

Figure 3-63 Uploading a certificate

Table 3-28 Certificate format conversion commands

Format	Conversion Method
CER/CRT	Rename the **cert.crt** certificate file to **cert.pem**.
PFX	Use OpenSSL to convert the certificate. Obtain a private key. For example, run the following command to convert **cert.pfx** into **cert.key**: **openssl pkcs12 -in cert.pfx -nocerts -out cert.key -nodes** Obtain a certificate. For example, run the following command to convert **cert.pfx** into **cert.pem**: **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**

Format	Conversion Method
P7B	Use OpenSSL to convert the certificate. 1. Run the following command to convert the certificate: **openssl pkcs7 -print_certs -in incertificat.p7b -out cert.cer** 2. Obtain the certificate content in **cert.cer**. 3. Save the content in .pem format.
DER	Use OpenSSL to convert the certificate. 1. Obtain a private key. For example, run the following command to convert **privatekey.der** into **privatekey.pem**: **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** 2. Obtain a certificate. For example, run the following command to convert **cert.cer** into **cert.pem**: **openssl x509 -inform der -in cert.cer -out cert.pem**

NOTE

Before running the openssl command in Windows, ensure that the **OpenSSL** tool has been installed.

Step 7 Click **OK**. The certificate is uploaded.

----End

3.11.4 Deleting a Certificate

If an uploaded AAD certificate is no longer required, you can delete it on the certificate management page.

Limitations and Constraints

A certificate that has been bound to a domain name cannot be deleted. Modify the certificate by referring to **Updating a Certificate**.

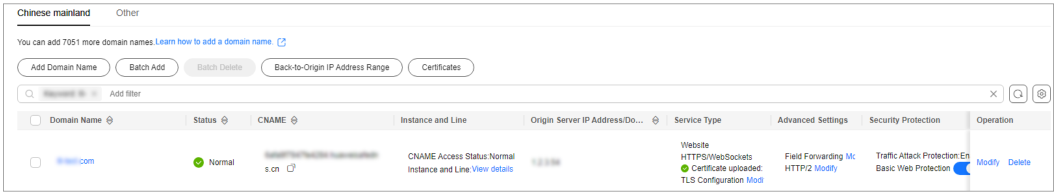
Deleting a Certificate

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

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-64 Domain name access

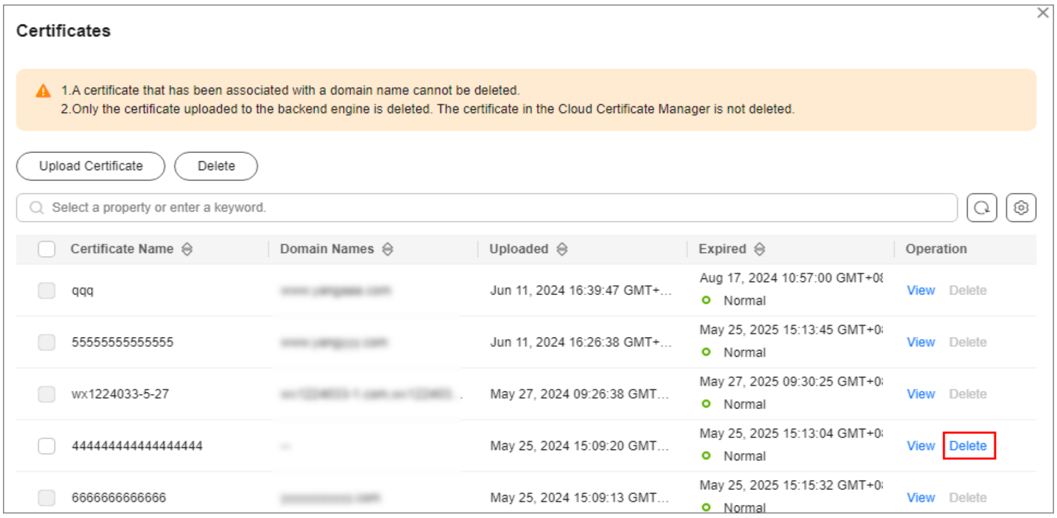


You can add 7051 more domain names. Learn how to add a domain name.

Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Operation
[redacted].com	Normal	[redacted]s.cn	CNAME Access Status:Normal Instance and Line:View details	[redacted]	Website HTTPS/WebSockets Certificate uploaded: TLS Configuration Modi	Field Forwarding Mc HTTP/2 Modify	Traffic Attack Protection:En Basic Web Protection	Modify Delete

Step 4 Choose **Certificates**. The certificate list is displayed.

Figure 3-65 Certificate list



Certificates

1.A certificate that has been associated with a domain name cannot be deleted.
2.Only the certificate uploaded to the backend engine is deleted. The certificate in the Cloud Certificate Manager is not deleted.

Certificate Name	Domain Names	Uploaded	Expired	Operation
qqq	[redacted]	Jun 11, 2024 16:39:47 GMT+...	Aug 17, 2024 10:57:00 GMT+08 Normal	View Delete
55555555555555	[redacted]	Jun 11, 2024 16:26:38 GMT+...	May 25, 2025 15:13:45 GMT+0: Normal	View Delete
wx1224033-5-27	[redacted]	May 27, 2024 09:26:38 GMT...	May 27, 2025 09:30:25 GMT+0: Normal	View Delete
444444444444444444	--	May 25, 2024 15:09:20 GMT...	May 25, 2025 15:13:04 GMT+0: Normal	View Delete
6666666666666	[redacted]	May 25, 2024 15:09:13 GMT...	May 25, 2025 15:15:32 GMT+0: Normal	View Delete

Step 5 In the row containing the target certificate, click **Delete**.

Step 6 In the dialog box that is displayed, click **OK**.

----End

3.12 Managing Forwarding Rules

After configuring forwarding rules, you can view their information, modify the origin server IP address, and export or delete them in batches.

NOTICE

Deleting or adding a forwarding rule or modifying an origin server IP address may interrupt services. Exercise caution when performing this operation.

View information about the desired forwarding rule.

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Forwarding Configuration**. The **Forwarding Configuration** page is displayed.

Step 4 View information about the desired forwarding rule.

Table 3-29 Forwarding rule parameters

Parameter	Description
Forwarding Protocol/Port	Specifies the forwarding protocol and port of the forwarding rule.
Status	Specifies the running status of the forwarding rule.
LVS Forwarding Rule	Specifies the Linux Virtual Server (LVS) forwarding mode.
Origin Server Region	Specifies the region of the origin server to which the forwarding rule is added.
Origin Server IP Address	Specifies the origin server IP address added to the forwarding rule. If you need to change the origin server IP address, click **Edit** to change it.
Weight	Specifies the weight of the forwarding rule.
Operation	You can click **Delete** to delete the forwarding rule.

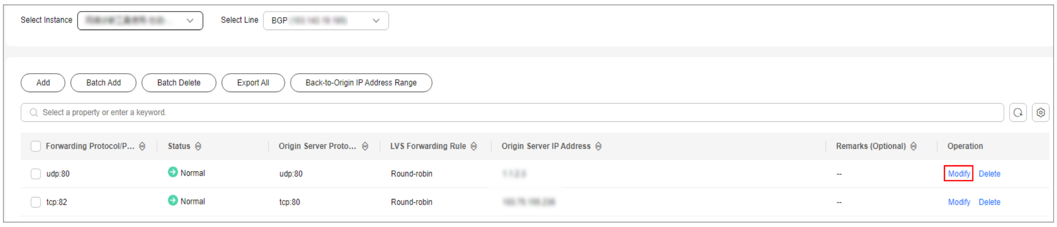
----End

Modifying the Origin Server IP Address

Step 1 Log in to the management console.

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

Step 3 Locate the row containing the target forwarding rule and click **Modify**.


Add
Batch Add
Batch Delete
Export All
Back-to-Origin IP Address Range
Select a property or enter a keyword.

Select Instance [redacted]
Select Line BGP [redacted]

Forwarding Protocol/P...	Status	Origin Server Proto...	LVS Forwarding Rule	Origin Server IP Address	Remarks (Optional)	Operation
udp:80	Normal	udp:80	Round-robin	[redacted]	--	Modify Delete
tcp:82	Normal	tcp:80	Round-robin	[redacted]	--	Modify Delete

Step 4 In the displayed **Modify Origin Server IP Address** dialog box, change the IP address of the origin server for the forwarding rule.

NOTICE

Enter a valid public IP address.

Step 5 Click **OK**.

----End

Export Forwarding Rules

After exporting forwarding rules, you can quickly modify their configuration in batches.

Step 1 Click **Export** to export all forwarding rules to the local computer.

Step 2 View the exported forwarding rule file **rules.txt**.

----End

Delete a Forwarding Rule

If a forwarding rule is no longer needed, you can delete it.

- Deleting a single forwarding rule:
  a. In the Operation column of the row containing the desired forwarding rule, click **Delete**.
  b. Click **OK**.
- Deleting forwarding rules in batches:
  a. Select the forwarding rules to be deleted and click **delete**.

     NOTE

     A maximum of 50 forwarding rules can be deleted at a time. (A maximum of 50 forwarding rules can be displayed on a single page on the console.)

  b. Click **OK**.

3.13 Viewing Monitoring Metrics

3.13.1 AAD Monitoring Metrics

Description

This topic describes metrics reported by AAD to Cloud Eye as well as their namespaces. You can use Cloud Eye to query the metrics of the monitored object and alarms generated for AAD.

Namespaces

SYS.DDOS

NOTE

A namespace is an abstract collection of resources and objects. Multiple namespaces can be created in a single cluster with the data isolated from each other. This enables namespaces to share the same cluster services without affecting each other.

Metrics

Table 3-30 AAD monitoring metrics

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
ip_drop_rate	Discarded traffic	Specifies the bandwidth for discarding traffic of high-defense IP addresses.	≥0kb/s	Advanced Anti-DDoS	5 minutes
instance_drop_rate	Discarded traffic	Specifies the discarded traffic bandwidth of an AAD instance.	≥0kb/s	Advanced Anti-DDoS	5 minutes
ip_back_to_source_rate	Retrieval bandwidth	Specifies the retrieval traffic bandwidth of the high-defense IP address.	≥0kb/s	Advanced Anti-DDoS	5 minutes
instance_back_to_source_rate	Retrieval bandwidth	Specifies the retrieval traffic bandwidth of AAD instances.	≥0kb/s	Advanced Anti-DDoS	5 minutes
ip_internet_in_rate	Inbound Traffic	Specifies the inbound traffic bandwidth of the high-defense IP address.	≥0kb/s	Advanced Anti-DDoS	5 minutes
instance_internet_in_rate	Inbound traffic	Specifies the inbound traffic bandwidth of an AAD instance	≥0kb/s	Advanced Anti-DDoS	5 minutes

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
ip_new_connection	New connections	Specifies the number of new connections to the high-defense IP address.	≥0count/s	Advanced Anti-DDoS	5 minutes
instance_new_connection	New Connections	Specifies the number of new connections of an AAD instance.	≥0count/s	Advanced Anti-DDoS	5 minutes
ip_concurrent_connection	Concurrent connections	Concurrent connections to the high-defense IP address.	≥0count/s	Advanced Anti-DDoS	5 minutes
instance_concurrent_connection	Concurrent connections	Concurrent connections to the AAD instance.	≥0count/s	Advanced Anti-DDoS	5 minutes
ip_service_bandwidth_usage	Service bandwidth usage	Service bandwidth usage of the high-defense IP address service.	≥0%	Advanced Anti-DDoS	5 minutes
instance_service_bandwidth_usage	Service bandwidth usage	Service bandwidth usage of an AAD instance.	≥0%	Advanced Anti-DDoS	5 minutes

Dimensions

Key	Value
zone_ip	Instance - Protected IP Address

Key	Value
instance_id	Instance ID

3.13.2 Viewing Monitoring Metrics

On the management console, you can view AAD metrics to learn about the protection status in a timely manner and set protection policies based on the metrics.

Prerequisite

You have configured alarm rules on the Cloud Eye console. For more details, see **Configuring Monitoring Alarm Rules**.

Viewing Monitoring Metrics

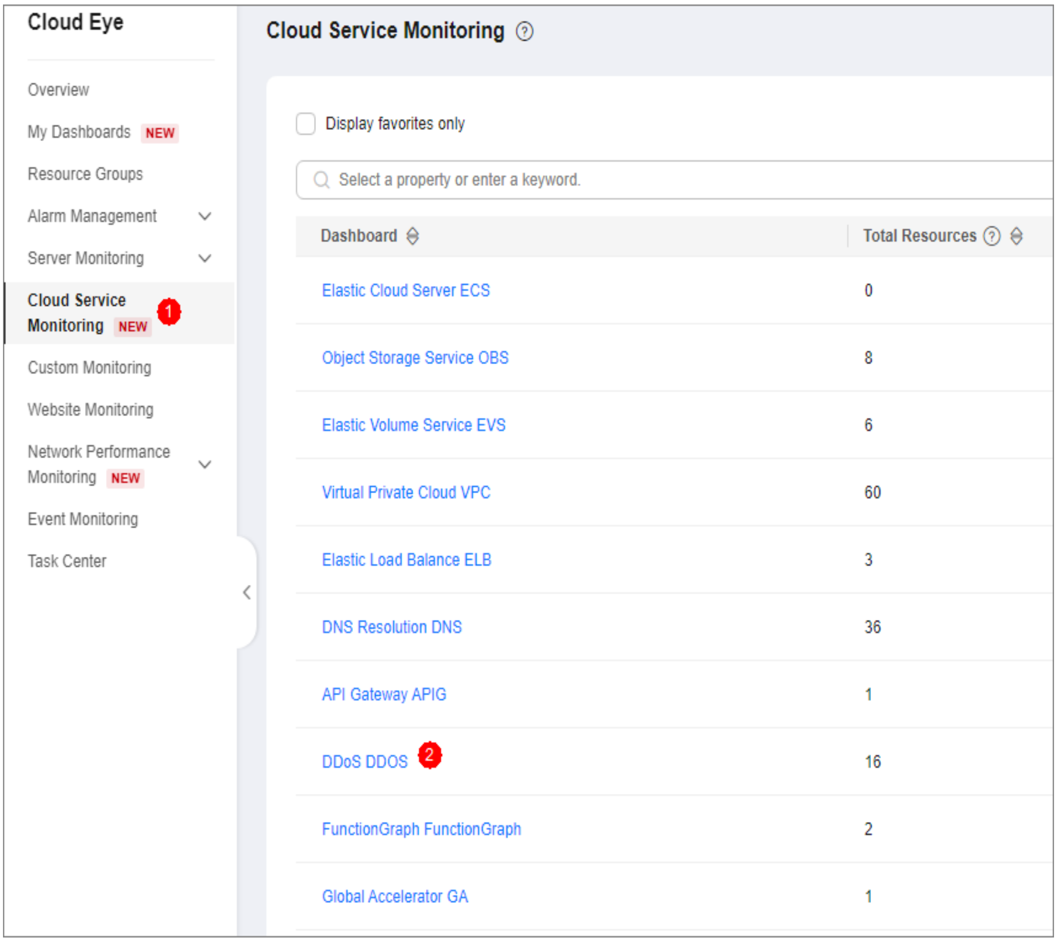
Step 1 **Log in to the management console**.

Step 2 Click 📍 in the upper left corner of the displayed page to select a region.

Step 3 Hover your mouse over ☰ in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Cloud Service Monitoring** > **Anti-DDoS Service**.

Figure 3-66 Selecting a service



□ Display favorites only

Select a property or enter a keyword.

Dashboard	Total Resources
Elastic Cloud Server ECS	0
Object Storage Service OBS	8
Elastic Volume Service EVS	6
Virtual Private Cloud VPC	60
Elastic Load Balance ELB	3
DNS Resolution DNS	36
API Gateway APIG	1
DDoS DDOS	16
FunctionGraph FunctionGraph	2
Global Accelerator GA	1

Step 5 On the **Cloud Service Monitoring Details** page, choose **Anti-DDoS Service** > **Instance ID**.

Step 6 Locate the row that contains the target object and click **View Metric** to view the metric details of the object.

----End

3.13.3 Configuring Monitoring Alarm Rules

You can set AAD alarm rules to customize the monitored objects and notification policies, and set parameters such as the alarm rule name, monitored object, metric, threshold, monitoring scope, and whether to send notifications. This helps you learn the AAD protection status in a timely manner.

For details about how to set monitoring alarms for multiple instances or protected IP addresses, see **Setting Monitoring Alarm Rules in Batches**. For details about how to set monitoring alarms for a specified instance or protected IP address, see **Setting Monitoring Alarm Rules for a Specified Resource**.

If you need to customize more metrics, you can report them to Cloud Eye through API requests. For details, see **Adding Monitoring Data** and **AAD Monitoring Metrics**.

Setting Monitoring Alarm Rules in Batches

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the displayed page to select a region.

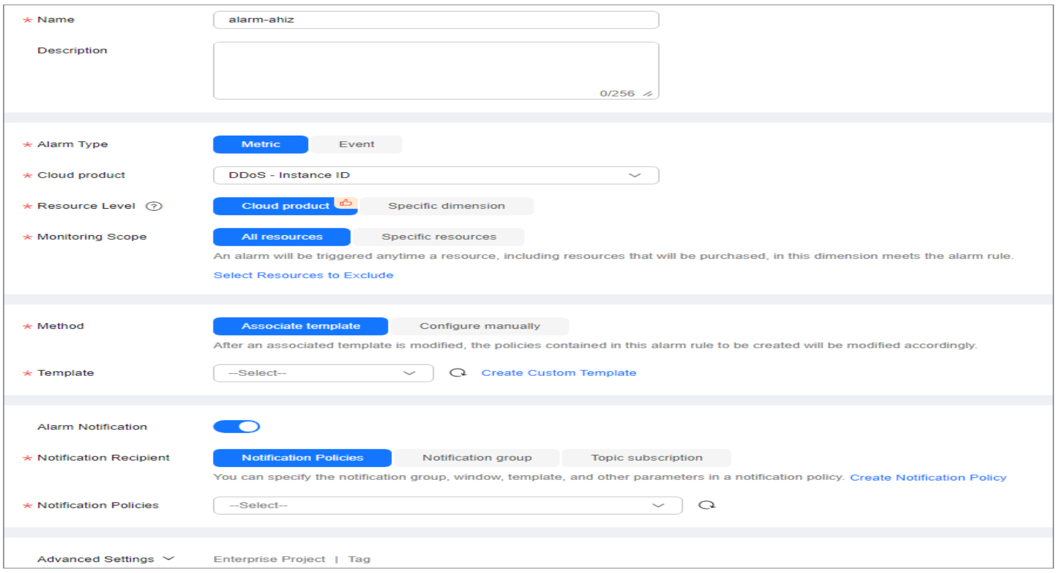
Step 3 Hover your mouse over ☰ in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.

Step 5 In the upper right corner of the page, click **Create Alarm Rule**.

Step 6 Enter the alarm rule information, as shown in **Configuring AAD alarm rules**. For details about how to enter the alarm rule information, see **Table 3-31**.

Figure 3-67 Configuring AAD alarm rules



* Name: alarm-ahiz

Description: 0/256

* Alarm Type: Metric

* Cloud product: DDoS - Instance ID

* Resource Level: Cloud product

* Monitoring Scope: All resources

An alarm will be triggered anytime a resource, including resources that will be purchased, in this dimension meets the alarm rule.

* Method: Associate template

After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.

* Template: --Select--

Alarm Notification: ●

* Notification Recipient: Notification Policies

You can specify the notification group, window, template, and other parameters in a notification policy.

* Notification Policies: --Select--

Advanced Settings: Enterprise Project | Tag

Table 3-31 AAD alarm rule parameters

Parameter	Description
Name	Name of the rule. The system generates a random name and you can modify it.
Description	Description about the rule.
Alarm Type	Alarm type
Cloud Service	Select **DDoS - Instance ID** from the drop-down list box.
Resource Level	Select the resource dimension to be monitored.
Monitoring Scope	Scope where the alarm rule applies to. You can select **All resources**, **Resource groups** or **Specific resources**.

Parameter	Description
Method	You can select **Associate template**, **Use existing template**, or **Configure manually**. For details about how to create a custom template, see **Creating a Custom Template**. **NOTE** After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.
Template	Select a template.
Alarm Notification	Whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/ HTTPS message.
Notification Recipient	Select a notification policy based on the site requirements.

Step 7 Click **Create**. In the displayed dialog box, click **OK**.

----End

Setting Monitoring Alarm Rules for a Specified Resource

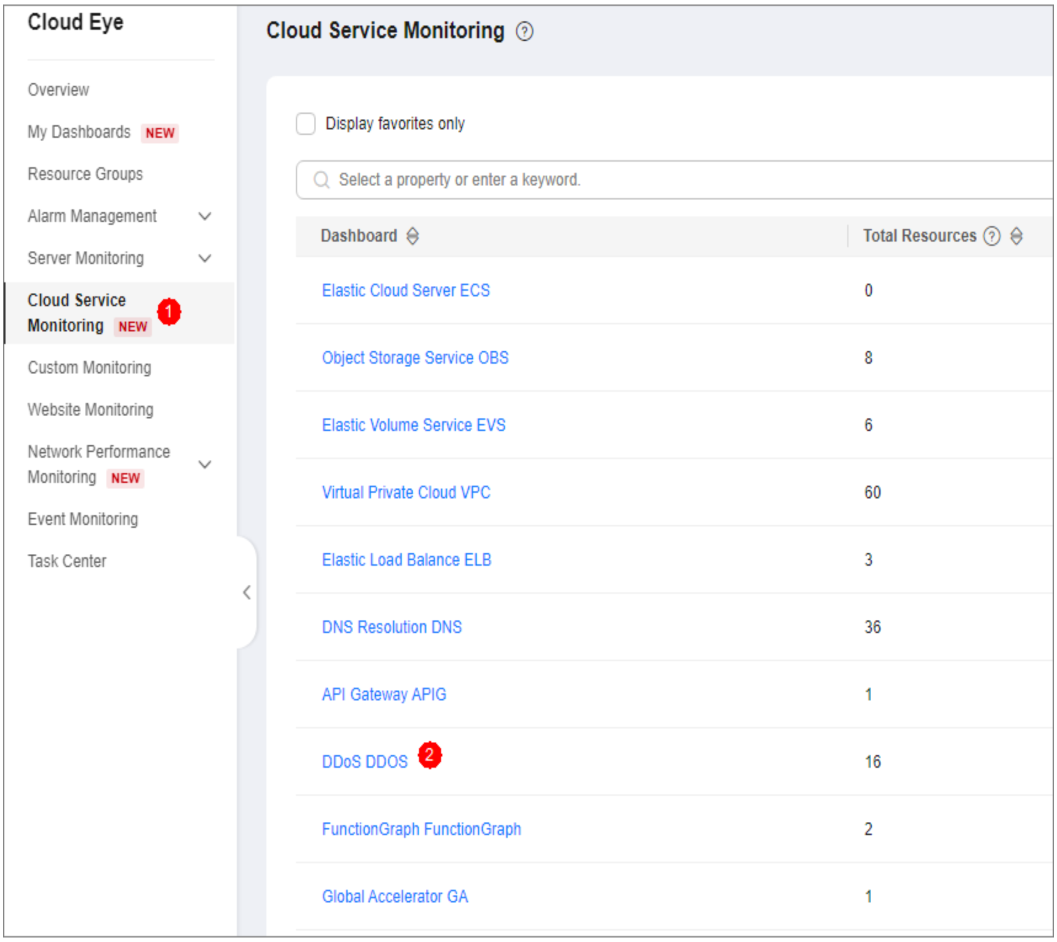
Step 1 **Log in to the management console**.

Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 Hover your mouse over ☰ in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Cloud Service Monitoring** > **Anti-DDoS Service**.

Figure 3-68 Selecting a service



☐ Display favorites only

Select a property or enter a keyword.

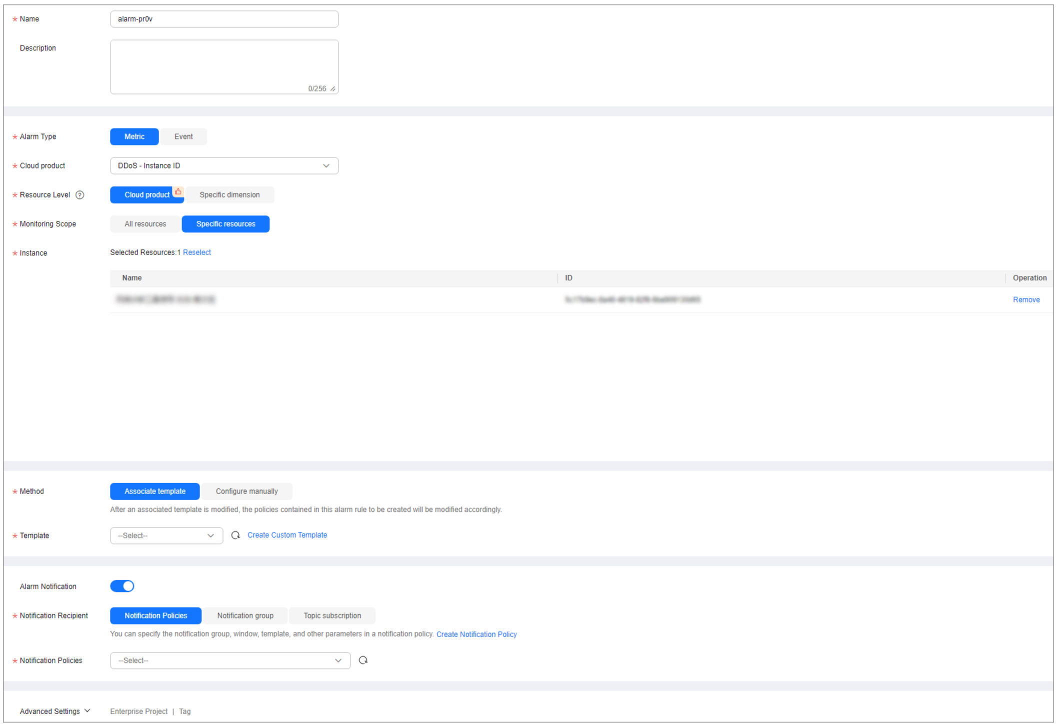
Dashboard	Total Resources
Elastic Cloud Server ECS	0
Object Storage Service OBS	8
Elastic Volume Service EVS	6
Virtual Private Cloud VPC	60
Elastic Load Balance ELB	3
DNS Resolution DNS	36
API Gateway APIG	1
DDoS DDOS	16
FunctionGraph FunctionGraph	2
Global Accelerator GA	1

Step 5 On the **Cloud Service Monitoring Details** page, choose **Anti-DDoS Service** > **Instance ID**.

Step 6 Locate the row that contains the object to be monitored, and click **Create Alarm Rule**.

Step 7 Enter the alarm rule information, as shown in **Configuring AAD alarm rules**. For details about how to enter the alarm rule information, see **Table 3-32**.

Figure 3-69 Configuring AAD alarm rules



* Name: alarm-pr0v

Description: 0/256

* Alarm Type: [✓ Metric] Event

* Cloud product: DDoS - Instance ID

* Resource Level: [✓ Cloud product] Specific dimension

* Monitoring Scope: All resources [✓ Specific resources]

* Instance: Selected Resources:1 Reselect

Name	ID	Operation
[redacted]	[redacted]	Remove

* Method: [✓ Associate template] Configure manually

After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.

* Template: --Select-- Create Custom Template

Alarm Notification: ●

* Notification Recipient: [✓ Notification Policies] Notification group Topic subscription

You can specify the notification group, window, template, and other parameters in a notification policy. Create Notification Policy

* Notification Policies: --Select--

Advanced Settings: Enterprise Project | Tag

Table 3-32 AAD alarm rule parameters

Parameter	Description
Workspace Name	Name of the rule. The system generates a random name and you can modify it.
Description	Description about the rule.
Alarm Type	Retain the default value.
Cloud Service	Retain the default value.
Resource Level	Retain the default value.
Monitoring Scope	Retain the default value.
Monitored Objects	Retain the default value.
Method	You can select **Associate template**, **Use existing template**, or **Configure manually**. For details about how to create a custom template, see **Creating a Custom Template**. **NOTE** After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.
Template	Select a template.

Parameter	Description
Alarm Notification	Whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message.
Notification Method	Select a notification mode as required.

Step 8 Click **Create**. In the displayed dialog box, click **OK**.

----End

3.13.4 Setting Event Alarm Notifications

Cloud Eye can monitor AAD events and generate alarms when events such as black hole, scheduling, and attacks occur. It helps you learn about the protection status of AAD in a timely manner.

After the event alarm notification function is enabled, you can view event details on the **Event Monitoring** page of the Cloud Eye console when an event occurs.

Limitations and Constraints

An event alarm notification is triggered only when the attack traffic exceeds 10 Mbit/s.

Configuring AAD Event Alarm Notifications

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

Step 2 Click 📍 in the upper left corner of the displayed page to select a region.

Step 3 Hover your mouse over ☰ in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

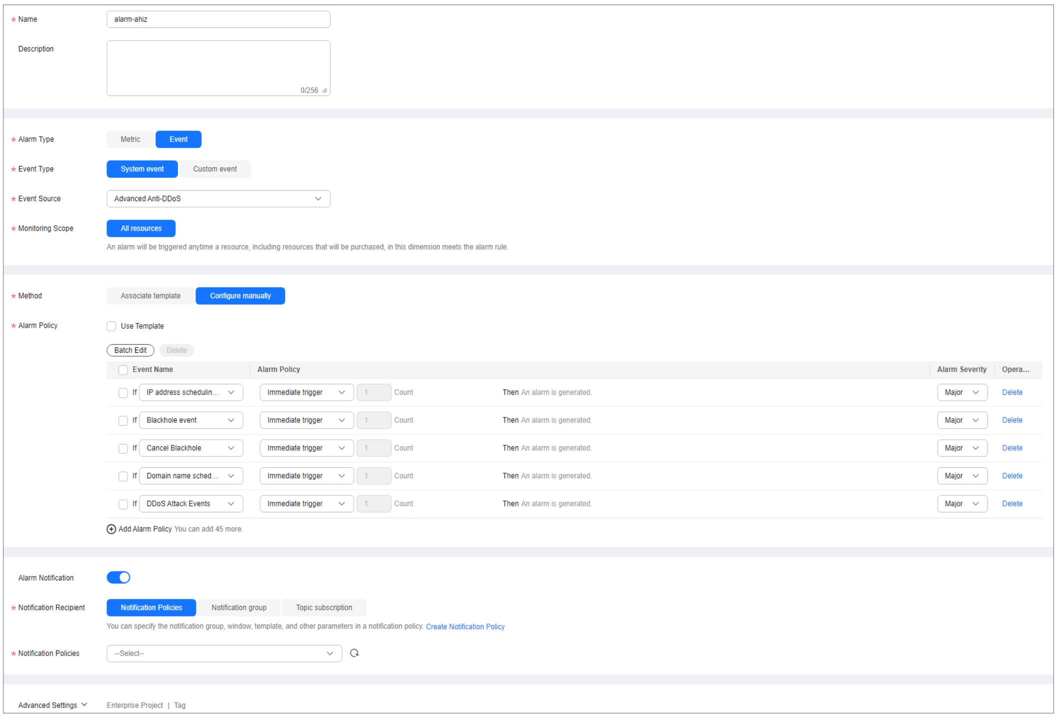
Step 4 Select a monitoring method based on the site requirements.

- Method 1: In the navigation tree on the left, choose **Event Monitoring**. The **Event Monitoring** page is displayed.
- Method 2: In the navigation pane on the left, choose **Alarms** > **Alarm Rules**. The **Alarm Rules** page is displayed.

Step 5 In the upper right corner of the page, click **Create Alarm Rule**. The **Create Alarm Rule** page is displayed.

Step 6 Set alarm parameters by referring to **Table 3-33**.

Figure 3-70 Alarm parameters



* Name: alarm-ahiz

Description: 0/256

* Alarm Type: Metric | **Event**

* Event Type: **System event** | Custom event

* Event Source: Advanced Anti-DDoS

* Monitoring Scope: **All resources**

An alarm will be triggered anytime a resource, including resources that will be purchased, in this dimension meets the alarm rule.

* Method: Associate template | **Configure manually**

* Alarm Policy: □ Use Template

Batch Edit | Delete

□ Event Name	Alarm Policy			Alarm Severity	Opera...
□ If IP address schedulin...	Immediate trigger	1 Count	Then An alarm is generated.	Major	Delete
□ If Blackhole event	Immediate trigger	1 Count	Then An alarm is generated.	Major	Delete
□ If Cancel Blackhole	Immediate trigger	1 Count	Then An alarm is generated.	Major	Delete
□ If Domain name sched...	Immediate trigger	1 Count	Then An alarm is generated.	Major	Delete
□ If DDoS Attack Events	Immediate trigger	1 Count	Then An alarm is generated.	Major	Delete

⊕ Add Alarm Policy You can add 45 more.

Alarm Notification: ●

* Notification Recipient: **Notification Policies** | Notification group | Topic subscription

You can specify the notification group, window, template, and other parameters in a notification policy. Create Notification Policy

* Notification Policies: --Select--

Advanced Settings: Enterprise Project | Tag

Table 3-33 Parameter description

Parameter	Description
Name	Name of the rule. The system generates a random name and you can modify it.
Description	Description about the rule.
Alarm Type	Select **Event**.
Event Type	Choose **System Event**.
Event Source	Choose **Advanced Anti-DDoS**.
Monitoring Scope	Select **All resources**.
Trigger Rule	The default option is **Configure manually**.
Event Name	You are advised to select **IP address scheduling event**, **Blackhole event**, **Cancel blackhole**, **Domain name scheduling event**, and **DDoS attack event**.

Parameter	Description
Notification Method	Select a notification method as required.

NOTE

Alarm messages are sent by Simple Message Notification (SMN), which may incur a small amount of fees.

Step 7 Click **Create**. In the dialog box that is displayed, click **OK**. The alarm notification is created successfully.

----End

3.14 Querying Audit Logs

3.14.1 AAD Operations Supported by CTS

CTS provides records of AAD operations. With CTS, you can query, audit, and backtrack these operations. For details, see **Cloud Trace Service User Guide**.

Table 3-34 lists Anti-DDoS Service operations recorded by CTS.

Table 3-34 AAD operations that can be recorded by CTS

Operation	Event Name
Uploading or modifying a certificate	domainCert
Deleting a certificate	delCertificate
Adding a domain name, connecting a domain name to AAD, and creating a domain name	domainDns
Importing domain names	importDomain
Modifying the domain name configuration	domainConfigEdit
Setting basic web protection and CC attack protection	domainSwitch
Deleting a domain name	deleteDomain
Enabling or disabling domain name line resolution	cnameSwitch

Operation	Event Name
Adding field forwarding, modifying TLS configuration, and modifying the HTTP/2 protocol.	setDomainWafConfig
Adding a forwarding rule	addProtocolRule
Importing and adding forwarding rules in batches	importProtocolRule
Deleting forwarding rules in batches	batchDelProtocolRule
Changing the back-to-origin IP address in the forwarding rule	modifyIpInRule
Enabling an instance	openInstance
Updating instance specifications	csbUpgrade
Deleting an instance	deleteInstance
Changing an instance name.	modifyInstanceName
Modifying the elastic bandwidth of an AAD instance	modifyElasticBandwidth
Setting the PP protocol switch for an instance	instancePpSwitch
Enabling an instance (using the console)	cadOpen
Enabling an instance (using CBC)	csbOpen
Upgrading specifications (using the console)	cadUpgrade
Modifying the LTS configuration of a user	updateLtsConfig
Deleting the current LTS configuration	deleteLtsConfig
Configuring the blacklist or whitelist	addBlackWhiteList
Removing a blacklisted or whitelisted item	delBlackWhiteList
Enabling cross-border traffic blocking	openForeignFlowBlock
Disabling cross-border traffic blocking	closeForeignFlowBlock
Enabling UDP traffic blocking	openUDPFlowBlock
Disabling UDP traffic blocking	closeUDPFlowBlock
Creating a frequency control rule	addCCPolicy
Updating a frequency control rule	setCCPolicy

Operation	Event Name
Deleting a frequency control rule	deleteCCPolicy
Configuring a web protection policy	updateWafPolicy
Modifying a CC attack protection rule	updateIntelligentCc
Creating a geo-blocking rule	addWafGeoIpRule
Deleting a geo-blocking rule	deleteWafGeoIpRule
Updating a geo-blocking rule	updateWafGeoIpRule
Creating a CC blacklist or whitelist rule	addWafWhiteIpRule
Deleting a CC blacklist or whitelist rule	deleteWafWhiteIpRule
Creating a precise protection rule	addWafCustomRule
Updating a precise protection rule	updateWafCustomRule
Deleting a precise protection rule	deleteWafCustomRule
Configuring alarms	setAlarmConfig
Batch adding or deleting tags	tmsResourceTagsAction
Enabling/Disabling CNAME automatic scheduling	cnameDispatchSwitch
Modifying an intelligent CC attack protection rule	updateIntellingentCc

3.14.2 Viewing CTS Traces

After you enable CTS, the system starts recording operations on Anti-DDoS Service. You can view the operation records of the last 7 days on the CTS console.

Prerequisites

You have enabled CTS. For details, see **Enabling CTS**.

Viewing AAD Audit Logs

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

Step 2 Click ☰ on the left of the page and choose **Cloud Trace Service** under **Management & Deployment**.

Step 3 Choose **Trace List** in the navigation pane on the left.

Step 4 Select **Trace Source** from the drop-down list, enter **AAD**, and press **Enter**.

Step 5 Click a trace name in the query result to view the event details.

You can use the advanced search function to combine one or more filter criteria in the filter box.

- Enter **Trace Name**, **Resource Name**, **Resource ID**, and **Trace ID**.
  - **Resource Name**: If the cloud resource involved in the trace does not have a name or the corresponding API operation does not involve resource names, this field is left empty.
  - **Resource ID**: If the resource does not have a resource ID or the resource fails to be created, this field is left empty.
- **Trace Source** and **Resource Type**: Select the corresponding cloud service name or resource type from the drop-down list.
- **Operator**: Select one or more operators from the drop-down list.
- Trace Status: The value can be **normal**, **warning**, or **incident**. You can select only one of them.
  - **normal**: indicates that the operation is successful.
  - **warning**: indicates that the operation failed.
  - **incident**: indicates a situation that is more serious than an operation failure, for example, other faults are caused.
- Time range: You can query traces generated in the last hour, day, or week, or customize traces generated in any time period of the last week.

----End

4 Scheduling Center Quotas

4.1 Purchasing Anti-DDoS Scheduling Center Protection

The scheduling center supports interconnection between CNAD and AAD. Under normal service access, traffic is routed to the CNAD (or CDN service). In the event of heavy attacks, traffic is redirected to the AAD service for scrubbing, ensuring that critical services remain uninterrupted.

Purchasing Scheduling Rules

Step 1 Log in to the management console.

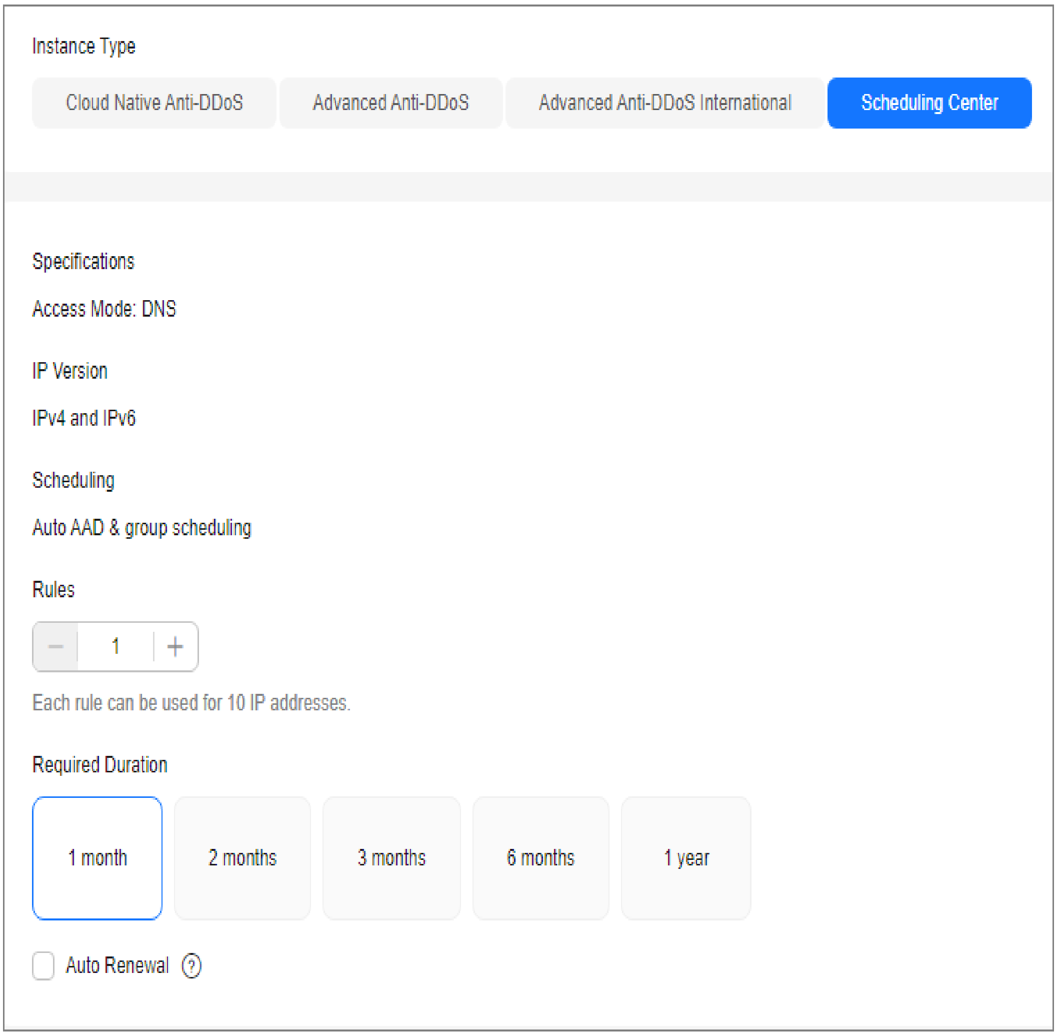
Step 2 Hover the mouse over the **Service List** icon, choose **Security & Compliance** > **Anti-DDoS**, and click **Advanced Anti-DDoS**.

Step 3 In the displayed **DDoS Migration Center** page, choose **DDoS Scheduling Center** > **Tiered Scheduling**.

Step 4 Click **Buy DDoS Mitigation** in the upper right corner of the page.

- **Instance Type**: Select **Scheduling Center**.
- **Rules**: Each rule can be used for 10 IP addresses. You can purchase multiple rules to schedule more IP addresses.
- **Required Duration**: Select a value based on the site requirements.
- **Auto Renewal**: Choose whether to automatically renew the subscription.

Figure 4-1 Purchasing scheduling rules



Instance Type

Specifications

Access Mode: DNS

IP Version

IPv4 and IPv6

Scheduling

Auto AAD & group scheduling

Rules

Each rule can be used for 10 IP addresses.

Required Duration

□ Auto Renewal ?

Step 5 Confirm the specifications and click **Submit Order** in the lower right corner to complete the payment.

----End

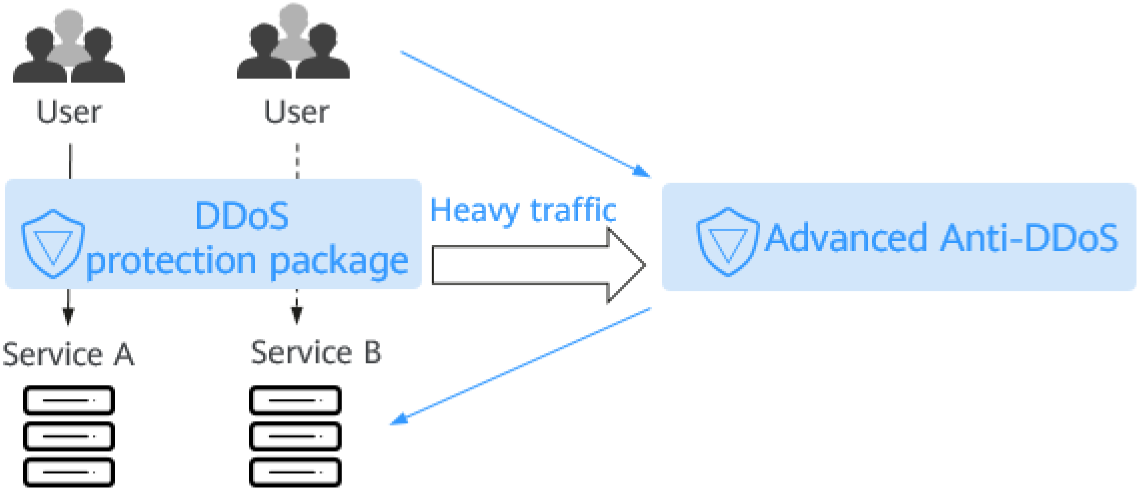
4.2 Configuring Tiered Scheduling Rules

If you have purchased a CNAD Unlimited Protection Basic instance, you can configure a tiered scheduling rule to automatically engage AAD protection for cloud resources protected by CNAD Unlimited Protection Basic.

Working Principles

Figure 4-2 shows how does CNAD Advanced automatically start AAD.

Figure 4-2 How auto AAD is started



Limitations and Constraints

- Auto AAD protects only the cloud resources protected by CNAD.
- You need to configure different origin server IP addresses for CNAD Advanced and AAD.
- Currently, the Anti-DDoS scheduling center does not support IPv6 addresses.

Configuring Tiered Scheduling Rules

Step 1 Log in to the management console.

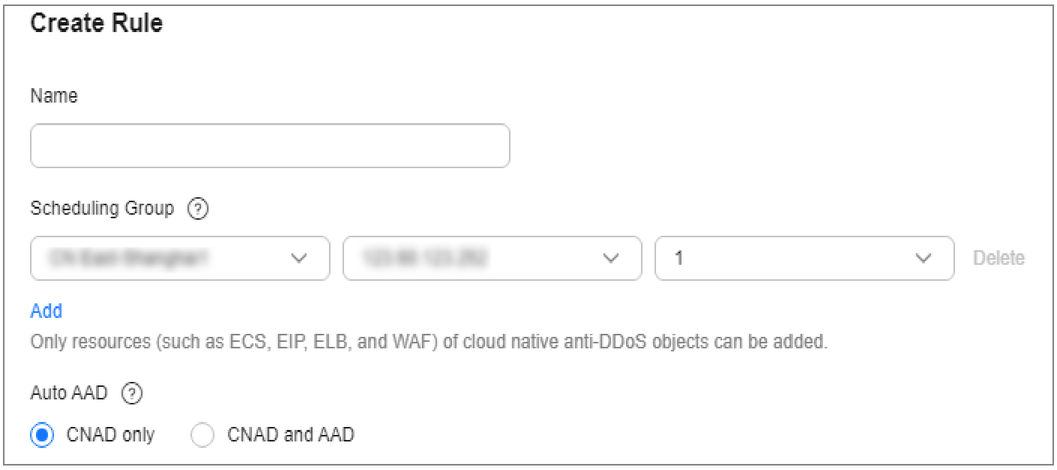
Step 2 Hover the mouse over the **Service List** icon, choose **Security & Compliance** > **Anti-DDoS**, and click **Advanced Anti-DDoS**.

Step 3 In the displayed **DDoS Migration Center** page, choose **DDoS Scheduling Center** > **Tiered Scheduling**.

Step 4 In the upper left corner of the tiered scheduling list, click **Create Rule**.

Step 5 In the dialog box that is displayed, set scheduling rule parameters. Parameters are listed in **Table 4-1**.

Figure 4-3 Creating a scheduling rule



Create Rule

Name

Scheduling Group ?

[redacted] [redacted] 1 Delete

Add

Only resources (such as ECS, EIP, ELB, and WAF) of cloud native anti-DDoS objects can be added.

Auto AAD ?

● CNAD only ○ CNAD and AAD

Table 4-1 Scheduling rule parameters

Parameter	Description
Name	Name of the scheduling rule. **NOTE** A maximum of 10 cloud resource IP addresses can be added to a rule. If you purchased *N* rules, a maximum of *N x 10* cloud resource IP addresses can be added.
Scheduling Group	Site, IP address, and scheduling group where the rule belongs to. IP address resolution starts from the group 1 and is performed by group. IP addresses in the same group will be resolved at the same time. Default group: 1 **NOTE** ● A blocked IP address in a group will be skipped. ● If all IP addresses in a group are blocked, the system will automatically start resolution for the next group. If no IP address in any group is available, the system starts AAD. ● Only resources (such as ECS, EIP, ELB, and WAF) of cloud native anti-DDoS objects can be added.
Auto AAD	● **CNAD only**: AAD will not be started to defend your servers against large volumetric DDoS traffic. ● **CNAD and AAD**: If you have purchased AAD, it will be started for large volumetric DDoS traffic. **CAUTION** The origin server IP address configured in AAD cannot be the same as the IP address in the tiered scheduling group. Otherwise, when the IP address in the tiered scheduling group is blocked, the back-to-origin IP address is also blocked and services cannot be recovered.

Step 6 Click **OK**.

----End

Related Operations

- To delete a rule, click **Delete** in the **Operation** column of the row containing the target scheduling rule.
- To view the details of a rule, click **View Details** in the **Operation** column of the row containing the target scheduling rule.
  - In the **Basic Information** area, click ✎ to modify the scheduling rule name and whether to enable joint scheduling.
  - Click **Add Resource**. In the displayed dialog box, you can modify, add, or delete the cloud resource IP address.
  - In the row containing the target resource, click **Delete** in the **Operation** column. You can also select the cloud resource to be deleted and click **Delete** in the upper left corner of the list to delete cloud resources in batches.

4.3 Enabling Tiered Scheduling Alarm Notifications

After you enable the alarm notification for the DDoS scheduling center, a notification message will be sent to you through the method you have configured when:

- An IP addresses in a tiered scheduling rule is blocked.
- An IP addresses in a tiered scheduling rule is unblocked.
- All IP addresses in a tiered scheduling rule are blocked.
- After all IP addresses in a tiered scheduling rule are blocked, one IP address is unblocked and can be scheduled.

Prerequisites

- Before enabling alarm notifications, you are advised to **create a topic** and **add a subscription** in **Simple Message Notification (SMN)**.
- The created topic needs to be confirmed by the subscriber. For details, see **Requesting Subscription Confirmation**.
- The DDoS tiered scheduling rule has been configured. For details, see **Configuring Tiered Scheduling Rules**.

Enabling Tiered Scheduling Alarm Notifications

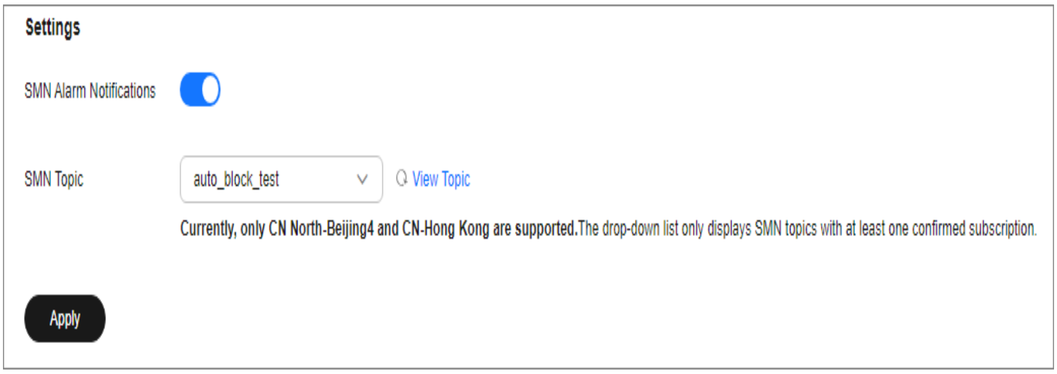
Step 1 **Log in to the management console**.

Step 2 Hover the mouse over the **Service List** icon, choose **Security & Compliance** > **Anti-DDoS**, and click **Advanced Anti-DDoS**. In the navigation pane on the left, choose **DDoS Scheduling Center** > **Alarm Notifications**.

Step 3 On the **Alarm Notifications** page, enable alarm notifications, that is, set **Alarm Notifications** to ●.

Step 4 Select a created topic from the **Notification Topic** drop-down list, as shown in **Figure 4-4**.

Figure 4-4 Configuring alarm notifications



Settings

SMN Alarm Notifications ●

SMN Topic: auto_block_test

Currently, only CN North-Beijing4 and CN-Hong Kong are supported.The drop-down list only displays SMN topics with at least one confirmed subscription.

NOTE

- Only topics whose subscription status is **Confirmed** can be displayed in the drop-down list box.
- Only topics in the same region as the DDoS scheduling center can be displayed in the drop-down list box.
- You will be billed for using the Simple Message Notification (SMN) service. For billing details, see **Product Pricing Details**.

Step 5 Click **Apply**.

----End

Related Operations

To disable alarm notifications, toggle off the **Alarm Notifications** function.

4.4 Configuring CDN Scheduling Rules

Huawei Cloud AAD and CDN are scheduled based on custom rules set at the scheduling center. Under normal conditions, traffic is directed to the closest CDN node for enhanced performance. In the event of an attack, the traffic is rerouted to AAD for scrubbing.

Prerequisites

- You have purchased and used CDN. For details, see **Enabling CDN**.
- You have purchased an AAD instance. For details, see **Purchasing an AAD Instance**.

Limitations and Constraints

You need to **submit a work order** to contact the Anti-DDoS Service team to obtain the CDN scheduling permission.

Enabling CDN Scheduling

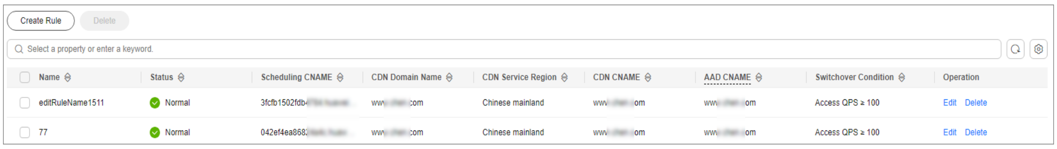
Step 1 **Log in to the management console**.

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

Step 3 In the navigation tree on the left, choose **DDoS Scheduling Center** > **CDN Scheduling**.

Step 4 On the **CDN Scheduling** page, click **Create Rule**.

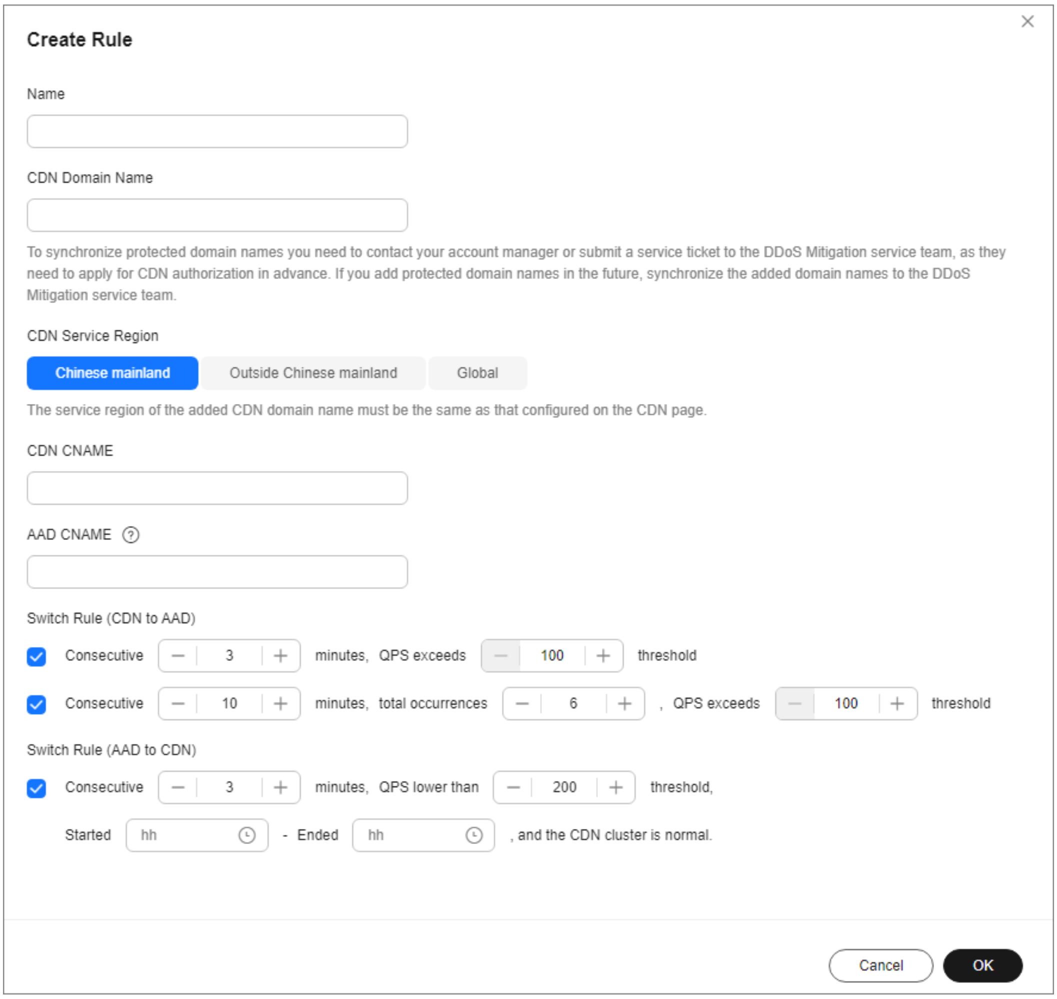
Figure 4-5 Creating a CDN scheduling rule



Name	Status	Scheduling CNAME	CDN Domain Name	CDN Service Region	CDN CNAME	AAD CNAME	Switchover Condition	Operation
editRuleName1511	Normal	3fcfb1502fdb4[redacted]	www[redacted]com	Chinese mainland	www[redacted]om	www[redacted]om	Access QPS ≥ 100	Edit Delete
77	Normal	042ef4ea868[redacted]	www[redacted]com	Chinese mainland	www[redacted]om	www[redacted]om	Access QPS ≥ 100	Edit Delete

Step 5 In the dialog box that is displayed, add the rule information. For details, see **Table 4-2**.

Figure 4-6 Rule details



Create Rule

Name

CDN Domain Name

To synchronize protected domain names you need to contact your account manager or submit a service ticket to the DDoS Mitigation service team, as they need to apply for CDN authorization in advance. If you add protected domain names in the future, synchronize the added domain names to the DDoS Mitigation service team.

CDN Service Region

Chinese mainland | Outside Chinese mainland | Global

The service region of the added CDN domain name must be the same as that configured on the CDN page.

CDN CNAME

AAD CNAME

Switch Rule (CDN to AAD)

☑ Consecutive 3 minutes, QPS exceeds 100 threshold

☑ Consecutive 10 minutes, total occurrences 6 , QPS exceeds 100 threshold

Switch Rule (AAD to CDN)

☑ Consecutive 3 minutes, QPS lower than 200 threshold,

Started hh - Ended hh , and the CDN cluster is normal.

Table 4-2 Rule details

Parameter	Description
Name	Enter the name of a user-defined CDN scheduling rule.
CDN Domain Name	Enter a CDN domain name. The domain name can contain only letters, digits, hyphens (-), and periods (.), and cannot exceed 64 characters.
CDN Service Scope	The region of the CDN domain name to be added must be the same as that configured on the CDN page. The supported service regions are **Chinese mainland**, **Outside Chinese mainland**, and **Global**.
CDN CNAME	Enter a CDN CNAME. The CDN CNAME can contain a maximum of 128 characters, including lowercase letters, digits, and periods (.).

Parameter	Description
AAD CNAME	Enter an AAD CNAME. The AAD CNAME can contain a maximum of 128 characters, including lowercase letters, digits, and periods (.).
Switch Rule (CND to AAD)	Set the rule for switching CDN to AAD based on the site requirements.
Switch Rule (AAD to CND)	Set the rule for switching back to the CDN based on the site requirements.

Step 6 Click **OK**.

----End

Related Operations

- Editing a rule: Locate the row that contains the target rule, click **Edit** in the **Operation** column. In the dialog box that is displayed, modify related parameters.
- Deleting a rule: Locate the row that contains the rule to be deleted, click **Delete** in the **Operation** column. In the dialog box that is displayed, click **OK**.