

# Anti-DDoS Service

## User Guide

**Issue** 01  
**Date** 2024-03-21



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

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

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

## **Huawei Cloud Computing Technologies Co., Ltd.**

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

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

---

# Contents

---

<b>1 CNAD Basic (Anti-DDoS) User Guide.....</b>	<b>1</b>
1.1 Usage Overview.....	1
1.2 Setting a Protection Policy.....	2
1.3 Viewing a Public IP Address.....	5
1.4 Enabling Alarm Notifications.....	6
1.5 Setting Event Alarm Notifications.....	7
1.6 Adding a Tag.....	10
1.7 Viewing Monitoring Reports.....	11
1.8 Viewing Interception Reports.....	13
1.9 Audit.....	14
1.9.1 Anti-DDoS Operations That Can Be Recorded by CTS.....	14
1.9.2 Viewing CTS Traces.....	15
1.10 Permission Management.....	16
1.10.1 Creating a User Group and Assigning the Anti-DDoS Access Permission.....	16
1.10.2 Anti-DDoS Custom Policies.....	17
1.10.3 Anti-DDoS Permissions and Actions.....	17
1.10.4 Permission Dependency of the Anti-DDoS Console.....	19
<b>2 CNAD Advanced Operation Guide.....</b>	<b>21</b>
2.1 Usage Overview.....	21
2.2 Purchasing a CNAD Instance.....	22
2.3 Adding a Protection Policy.....	25
2.3.1 Configuring the Scrubbing Threshold.....	25
2.3.2 Watermarking.....	27
2.3.2.1 Configuring Watermark Protection.....	27
2.3.2.2 Watermark Configuration Guide.....	29
2.3.2.2.1 Working Principles.....	29
2.3.2.2.2 Development Example.....	29
2.3.3 Configuring an ACL.....	31
2.3.4 Configuring Port Blocking.....	34
2.3.5 Configuring Protocol Blocking.....	36
2.3.6 Configuring Fingerprint Filtering.....	37
2.3.7 Configuring Connection Protection.....	40
2.3.8 Configuring Geo-Blocking.....	42

2.4 Adding a Protected Object.....	43
2.5 Setting Alarm Notifications.....	45
2.6 Managing Protection Logs.....	46
2.6.1 Viewing Statistics Reports.....	46
2.7 Managing Instances.....	48
2.7.1 Viewing Information About an Instance.....	48
2.7.2 Configuring Instance Tags.....	49
2.8 Managing Protected Objects.....	50
2.8.1 Viewing Details about a Protected Object.....	50
2.8.2 Selecting a Protection Policy for a Protected Object.....	52
2.8.3 Deleting a Protected Object.....	53
2.9 Permissions Management.....	54
2.9.1 Creating a User and Granting the CNAD Pro Access Permission.....	54
2.9.2 CNAD Pro Custom Policies.....	56
2.9.3 CNAD Pro Permissions and Actions.....	56
2.9.4 Permission Dependency of the CNAD Console.....	61
2.10 Monitoring.....	62
2.10.1 Setting Event Alarm Notifications.....	62
2.10.2 Configuring Monitoring Alarm Rules.....	65
2.10.3 Viewing Monitoring Metrics.....	71
2.10.4 Metrics.....	71
2.11 Audit.....	73
2.11.1 DDoS Mitigation Operations Recorded By CTS.....	73
2.11.2 Viewing CTS Traces.....	74

# 1 CNAD Basic (Anti-DDoS) User Guide

## 1.1 Usage Overview

[Usage Overview](#) provides an overview of Cloud Native Anti-DDoS Basic Edition.

**Table 1-1** Anti-DDoS usage overview

Step	Description
Setting a protection policy	Set a traffic scrubbing threshold for public IP addresses. For details, see <a href="#">Setting a Protection Policy</a> .
Enabling alarm notifications	After the alarm notification function is enabled, you will receive an alarm if a DDoS attack is detected. For details, see <a href="#">Enabling Alarm Notifications</a> .
Setting event alarm notifications	Cloud Eye enables event monitoring for protected EIPs and generates alarms for scrubbing, blocking, and unblocking events. For details, see <a href="#">Setting Event Alarm Notifications</a> .
Viewing a monitoring report	View the monitoring report of an EIP, covering the current protection status, protection settings, and the traffic and anomalies within the last 24 hours. For details, see <a href="#">Viewing Monitoring Reports</a> .
Viewing an interception report	This topic describes how to view the protection statistics, including the traffic cleaning frequency, cleaned traffic amount, weekly top 10 attacked public IP addresses, and total number of intercepted attacks of all public IP addresses of a user. For details, see <a href="#">Viewing Interception Reports</a> .

## 1.2 Setting a Protection Policy


Anti-DDoS automatically enables defense against DDoS attacks for public IP addresses on Huawei Cloud (Huawei Cloud EIPs).

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

- Use the default protection policy.  
The default protection policy is an initial policy and takes effect for all newly purchased EIPs. The default **traffic scrubbing threshold** is 120 Mbit/s and can be modified.
- Manually set a protection policy.  
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.

### Manually Setting a Default Protection Policy

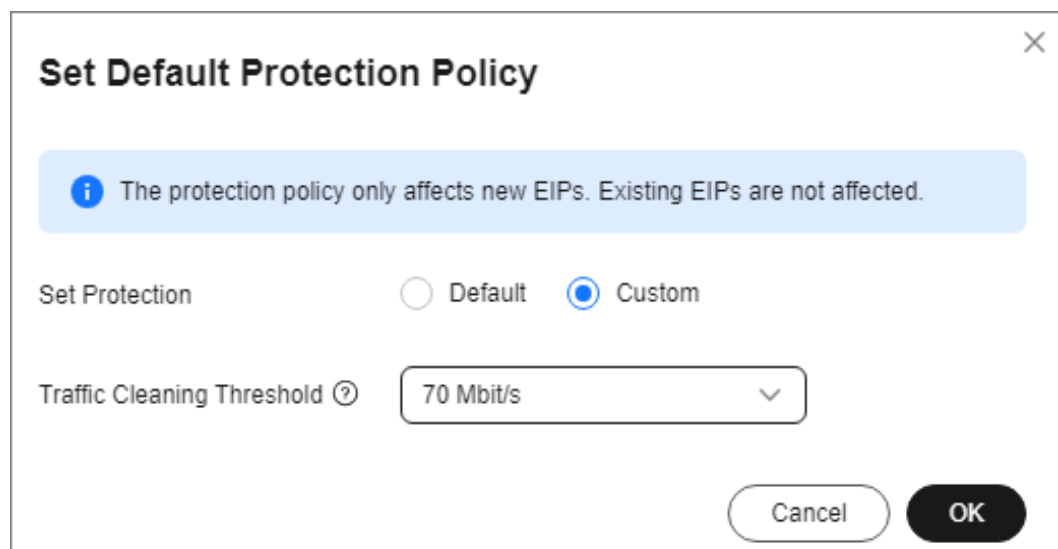
**Step 1** Log in to the management console.

**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 1-1](#).

**Figure 1-1** Manually configuring the default protection policy



**Table 1-2** Parameter description

Parameter	Description
Traffic Cleaning Threshold	<p>Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the threshold.</p> <p>You can set the traffic cleaning threshold based on your service traffic. Set the threshold to a value closest to the purchased bandwidth but not greater than the purchased bandwidth.</p> <p>The default protection rate is 120 Mbit/s. You can manually set more protection levels.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• If service traffic triggers scrubbing, only attack traffic is intercepted. If service traffic does not trigger scrubbing, no traffic is intercepted.</li> <li>• Set this parameter based on the actual service access traffic.</li> </ul>

**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

## Manually Setting a Protection Policy

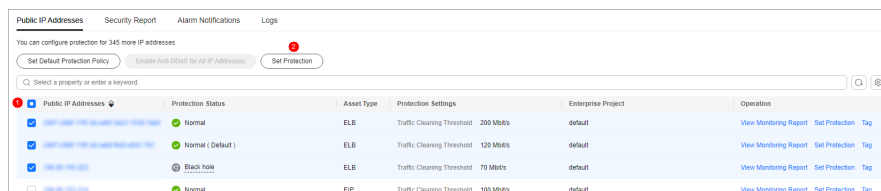
**Step 1** Log in to the management console.

**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** page is displayed.

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

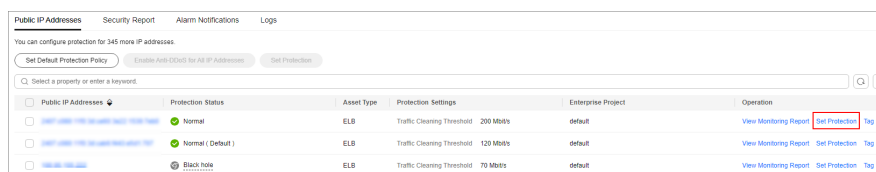
- To configure protection policies for multiple public IP addresses, select multiple public IP addresses and choose **Set Protection** in the upper part of the page.

**Figure 1-2** Configuring protection policies in batches



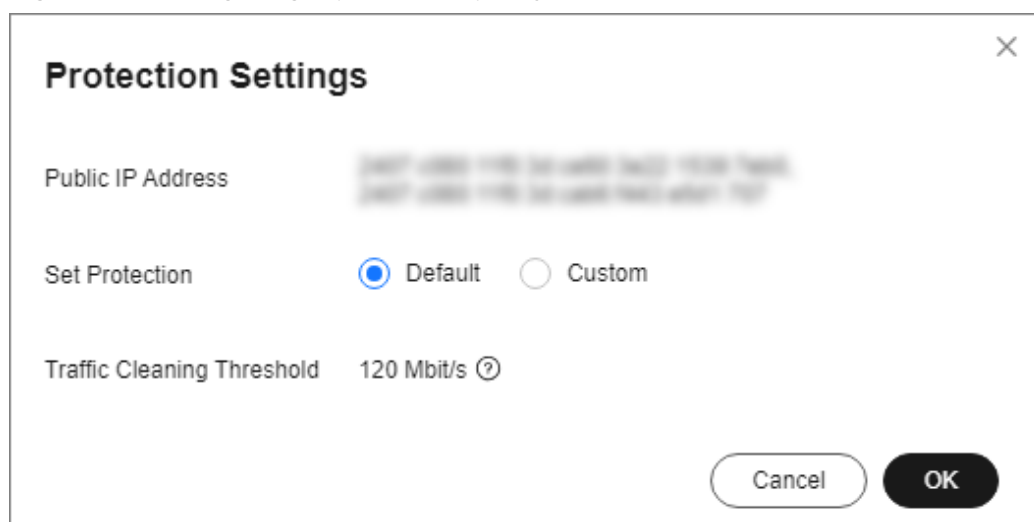
- To configure a protection policy for a single public IP address, in the row containing the desired public IP address, choose **Set Protection**.

**Figure 1-3** Configuring a protection policy for a public IP address



**Step 4** Set the **traffic scrubbing threshold** based on the site requirements, as shown in [Figure 1-4](#).

**Figure 1-4** Configuring a protection policy



**Table 1-3** Parameters for configuring a protection policy

Parameter	Description
Traffic Cleaning Threshold	<p>Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the threshold.</p> <p>You can set the traffic cleaning threshold based on your service traffic. Set the threshold to a value closest to the purchased bandwidth but not greater than the purchased bandwidth.</p> <p>The default protection rate is <b>120 Mbit/s</b>. You can manually set more protection levels.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>If service traffic triggers scrubbing, only attack traffic is intercepted. If service traffic does not trigger scrubbing, no traffic is intercepted.</li> <li>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.</li> </ul>

**Step 5** Then, click **OK**.

----End



## 1.3 Viewing a Public IP Address


### Scenarios

This topic describes how to view a public IP address.

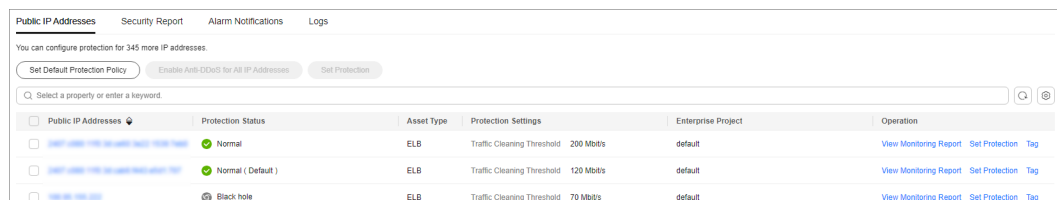
#### NOTICE

- After you purchase a public IP address, Anti-DDoS automatically enables the protection by default, and protects your public IP address against DDoS attacks.
- You are not allowed to disable Anti-DDoS after it has been enabled.

### Procedure



- 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, view all protected public IP addresses. [Table 1-4](#) describes the parameters.

**Figure 1-5** Viewing a public IP address



Public IP Addresses	Protection Status	Asset Type	Protection Settings	Enterprise Project	Operation
<input type="checkbox"/> <a href="#">192.168.1.1</a>	Normal	ELB	Traffic Cleaning Threshold: 200 Mbit/s	default	<a href="#">View Monitoring Report</a> <a href="#">Set Protection</a> <a href="#">Tag</a>
<input type="checkbox"/> <a href="#">192.168.1.2</a>	Normal (Default)	ELB	Traffic Cleaning Threshold: 120 Mbit/s	default	<a href="#">View Monitoring Report</a> <a href="#">Set Protection</a> <a href="#">Tag</a>
<input type="checkbox"/> <a href="#">192.168.1.3</a>	Black hole	ELB	Traffic Cleaning Threshold: 70 Mbit/s	default	<a href="#">View Monitoring Report</a> <a href="#">Set Protection</a> <a href="#">Tag</a>

#### 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 Protection Policy](#).
- 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.
- Enter a public IP address or a keyword of a public IP address in the search box and click  or  to search for the desired public IP address.

**Table 1-4** Parameter description

Parameter	Description
Public IP Address	Public IP address protected by Anti-DDoS <b>NOTE</b> If Anti-DDoS is enabled for a public IP address, you can click the IP address to go to its <b>Monitoring Report</b> page.
Protection Status	Protection status of a public IP address. The values are: <ul style="list-style-type: none"><li>• <b>Normal</b></li><li>• <b>Configuring</b></li><li>• <b>Disabled</b></li><li>• <b>Cleaning</b></li><li>• <b>Black hole</b></li></ul>
Asset Type	<ul style="list-style-type: none"><li>• EIP</li><li>• ELB</li><li>• NetInterFace</li><li>• Virtual Private Network (VPN)</li><li>• NAT Gateway</li><li>• VIP: HA virtual IP address.</li><li>• Cloud Container Instance (CCI)</li><li>• SubEni</li></ul>
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 Enabling Alarm Notifications

### Scenarios


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

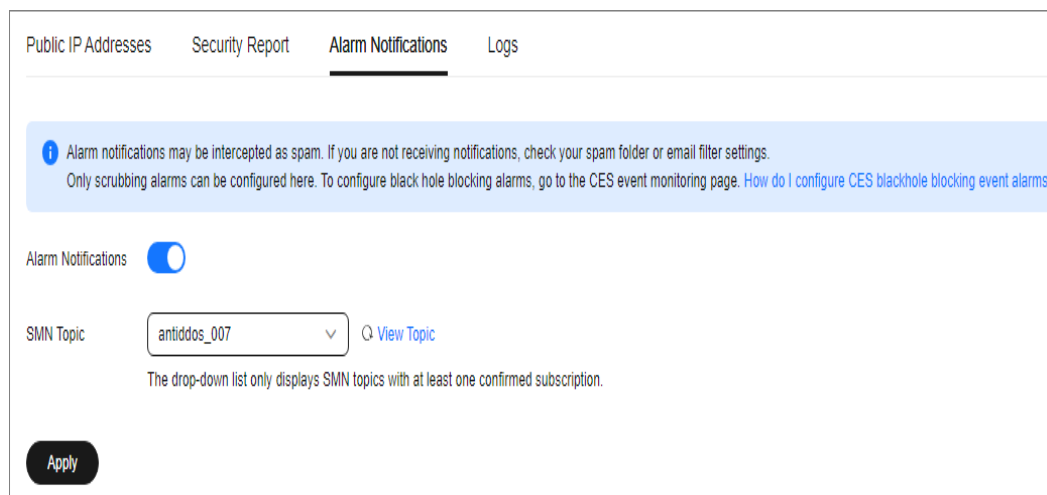
You have purchased at least one public IP address.

### Procedure



**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 [Figure 1-6](#).

**Figure 1-6** Configuring alarm notifications



**Table 1-5** Configuring alarm notifications

Parameter	Description
Alarm Notifications	Indicates whether the alarm notification function is enabled. There are two values: <ul style="list-style-type: none"> <li> : enabled</li> <li> : disabled</li> </ul>
SMN Topic	You can select an existing topic or click <b>View Topic</b> to create a topic. For more information about SMN topics, see <a href="#">Simple Message Notification User Guide</a> .

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

----End



## 1.5 Setting Event Alarm Notifications

### Scenarios

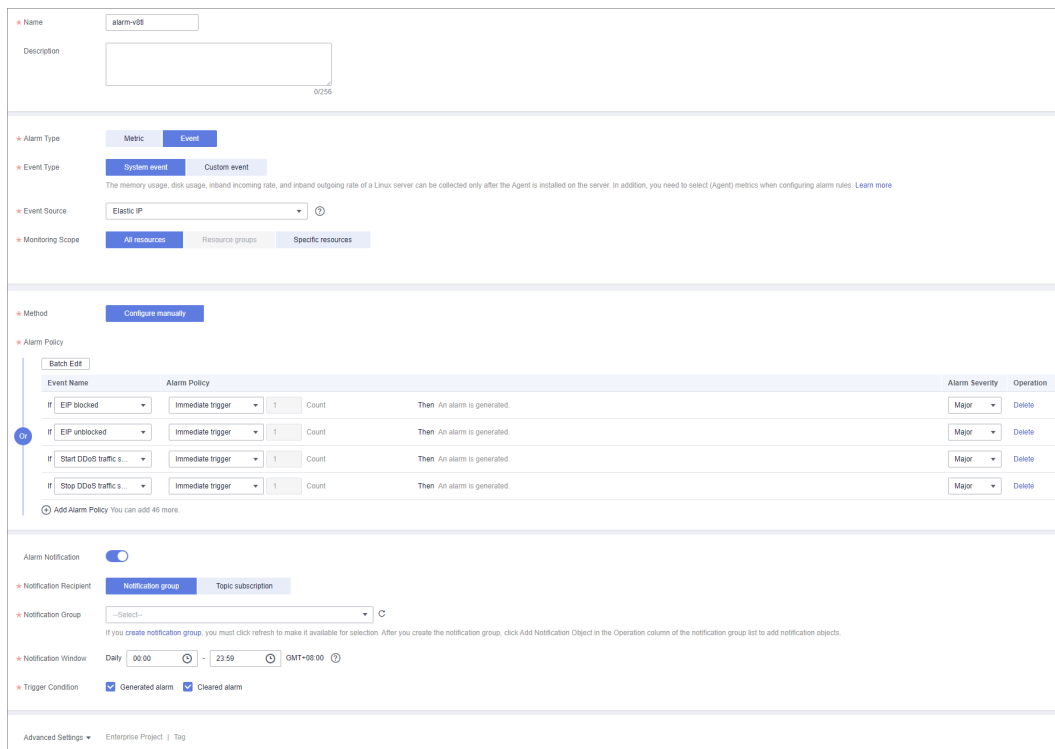
Cloud Eye enables event monitoring for protected EIPs and generates alarms for scrubbing, blocking, and unblocking events. This helps you learn about the protection status of Anti-DDoS in a timely manner.

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.

## Procedure

- 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 1-6](#).

**Figure 1-7** Alarm parameters



The screenshot displays the 'Create Alarm Rule' configuration page. Key sections include:

- Name:** alarm-v88
- Description:** (Empty text area)
- Alarm Type:** Metric (selected), Event
- Event Type:** System event (selected), Custom event
- Event Source:** Elastic IP
- Monitoring Scope:** All resources (selected), Resource group, Specific resources
- Method:** Configure manually
- Alarm Policy:** A table defining the conditions for the alarm.
 

Event Name	Alarm Policy	Count	Then	Alarm Severity	Operation
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 s...	Immediate trigger	1	Count	Then An alarm is generated.	Major   Delete
If Stop DDoS traffic s...	Immediate trigger	1	Count	Then An alarm is generated.	Major   Delete
- Alarm Notification:** Enabled (toggle)
- Notification Recipient:** Notification group (selected), Topic subscription
- Notification Group:** --Select--
- Notification Window:** Daily, 00:00 - 23:59 GMT+08:00
- Trigger Condition:** Generated alarm (checked), Cleared alarm (checked)

**Table 1-6** 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 <b>Event</b> .
Event Type	Choose <b>System Event</b> .
Event Source	Choose <b>Elastic IP</b> .
Monitoring Scope	Specifies the resource scope to which the alarm rule applies. Set this parameter as required.
Method	The default option is <b>Configure manually</b> .
Alarm Policy	You are advised to select <b>EIP blocked</b> , <b>EIP unblocked</b> , <b>Start Anti-DDoS traffic scrubbing</b> , and <b>Stop Anti-DDoS traffic scrubbing</b> .
Notification Recipient	Select <b>Notification group</b> or <b>Topic subscription</b> .
Notification Group	Select the required notification group.
Notification Object	Select the required topic subscription.
Notification Window	Set this parameter as required.
Trigger Condition	Choose <b>Generated alarm</b> and <b>Cleared alarm</b> .

**Step 7** Determine whether to send a notification based on the site requirements.

 **NOTE**

Alarm messages are sent by Simple Message Notification (SMN), which may incur a small amount of fees.

**Table 1-7** Notification Parameters

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 Recipient	You can select a <b>Notification group</b> or <b>Topic subscription</b> as required.
Notification Group	This parameter takes effect when <b>Notification Recipient</b> is set to <b>Notification group</b> . Set this parameter based on the site requirements.
Notification Object	This parameter is valid only when <b>Notification Recipient</b> is set to <b>Topic Subscription</b> . Set this parameter based on the site requirements.
Notification Window	Cloud Eye sends notifications only within the notification window specified in the alarm rule.
Trigger Condition	Set this parameter as required.

**Step 8** Click **Create**. In the dialog box that is displayed, click **OK**. The alarm notification is created successfully.


----End

## 1.6 Adding a Tag

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.

### Procedure

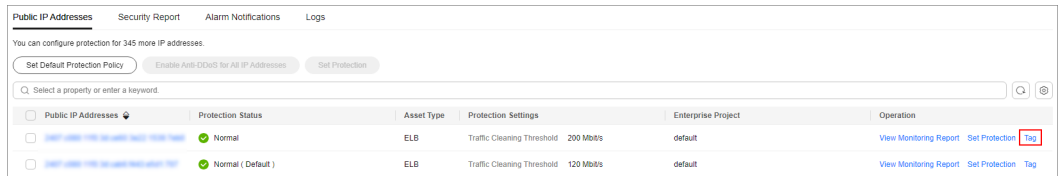
**Step 1** Log in to the management console.

**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 1-8** Adding a tag to an Anti-DDoS instance

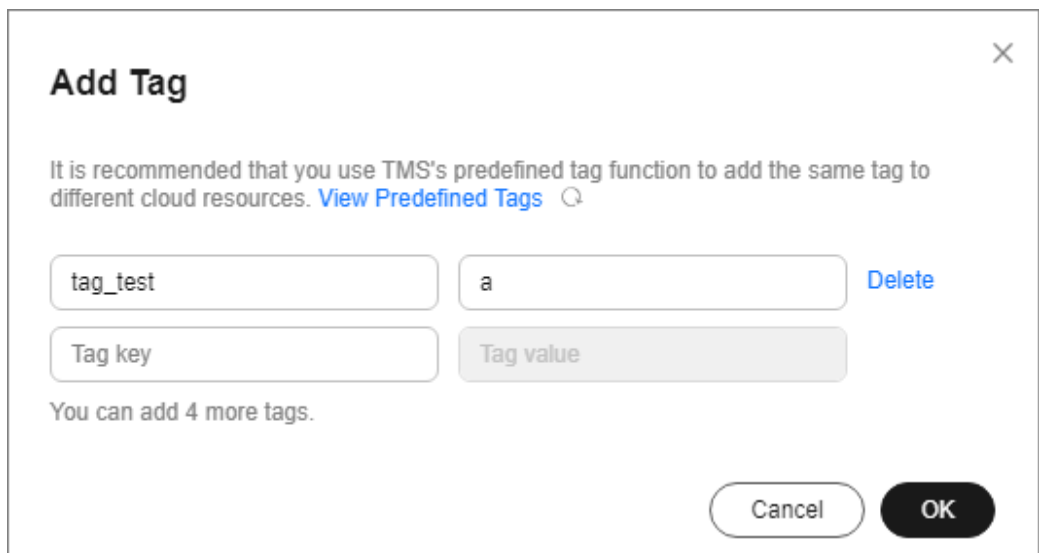


**Step 5** On the tag adding page, click **Add Tag** to add a tag.

**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 1-9** Adding a tag



**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


## 1.7 Viewing Monitoring Reports

### Scenarios

This section describes how to view the monitoring report of a public IP address. This report includes the protection status, protection settings, and the last 24 hours' traffic and anomalies.

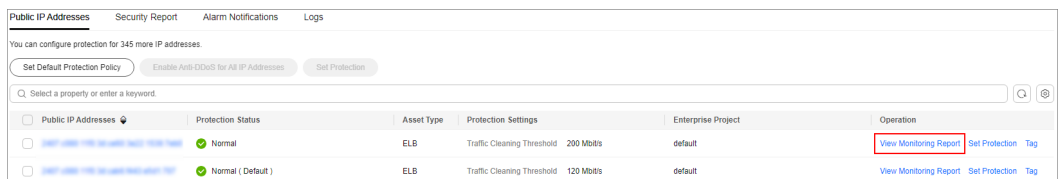
## Procedure

**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 1-10** Viewing a monitoring report

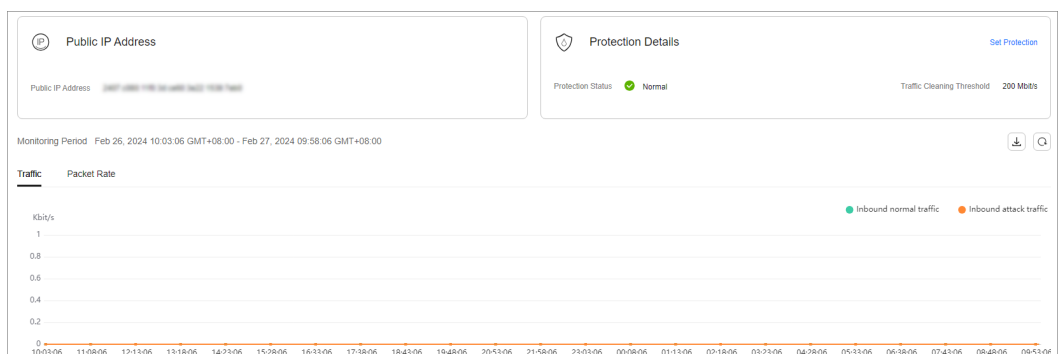


Public IP Addresses	Protection Status	Asset Type	Protection Settings	Enterprise Project	Operation
<a href="#">192.168.1.1</a>	Normal	ELB	Traffic Cleaning Threshold 200 Mbit/s	default	<a href="#">View Monitoring Report</a> <a href="#">Set Protection</a> <a href="#">Tag</a>
<a href="#">192.168.1.2</a>	Normal (Default)	ELB	Traffic Cleaning Threshold 120 Mbit/s	default	<a href="#">View Monitoring Report</a> <a href="#">Set Protection</a> <a href="#">Tag</a>

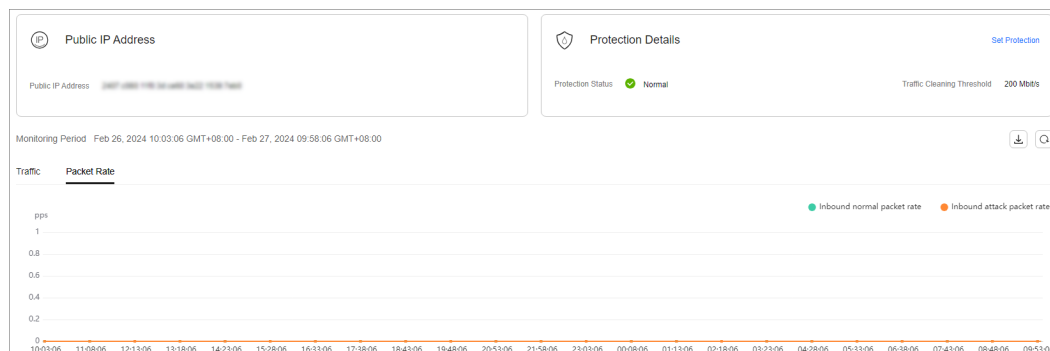
**Step 4** On the **Monitoring Report** page, view monitoring details about the public IP address.






- 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 1-11** Viewing a traffic monitoring report





**Figure 1-12** Viewing a packet rate monitoring report**NOTE**

- Click  to download monitoring reports to view monitoring details about the public IP address.
- On the traffic monitoring report page, click  **Inbound attack traffic** or  **Inbound normal traffic** to view details about the **Inbound attack traffic** or **Inbound normal traffic**.
- On the packet rate monitoring report page, click  **Inbound attack packet rate** or  **Inbound normal packet rate** to view details about the **Inbound attack packet rate** and **Inbound normal packet rate**.


----End

## 1.8 Viewing Interception Reports

### Scenarios

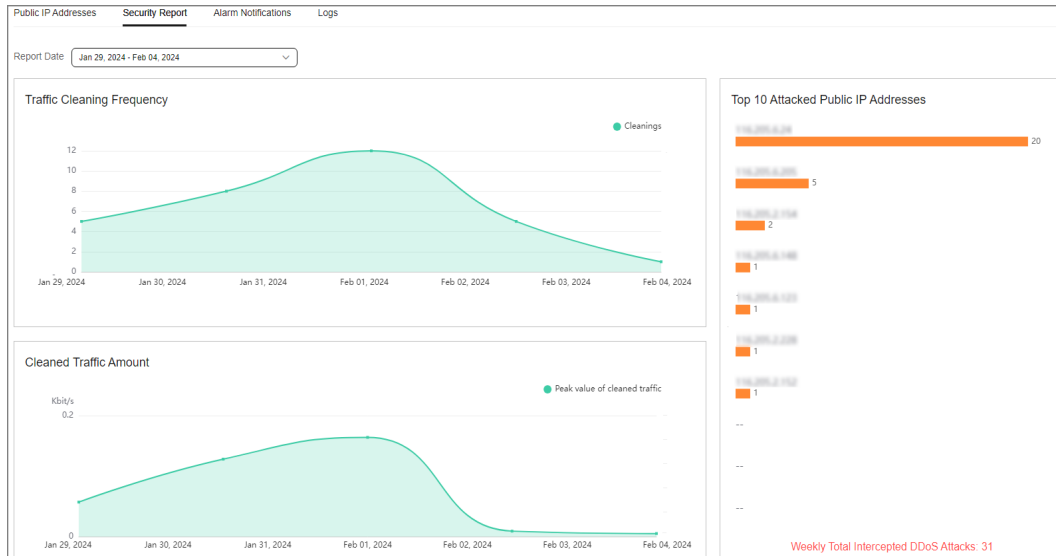
This section describes how to view the protection statistics, including the traffic cleaning frequency, cleaned traffic amount, weekly top 10 attacked public IP addresses, and total number of intercepted attacks of all public IP addresses of a user.

### Procedure


- 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 1-13** Viewing an interception report



**NOTE**

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

----End

## 1.9 Audit

### 1.9.1 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 1-8** lists the Anti-DDoS operations that can be recorded by CTS.

**Table 1-8** Anti-DDoS operations that can be recorded by CTS

Operation	Trace Name
Enabling Anti-DDoS	OPEN_ANTIDDOS
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


Operation	Trace Name
Updating the alarm notification configuration of a tenant	UPDATE_ALERT_CONFIG
Changing the default traffic scrubbing threshold of Anti-DDoS	UPDATE_DEFAULT_CONFIG
Deleting the default traffic scrubbing threshold of Anti-DDoS	DELETE_DEFAULT_CONFIG

## 1.9.2 Viewing CTS Traces

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.

### Procedure

**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

## 1.10 Permission Management

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

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

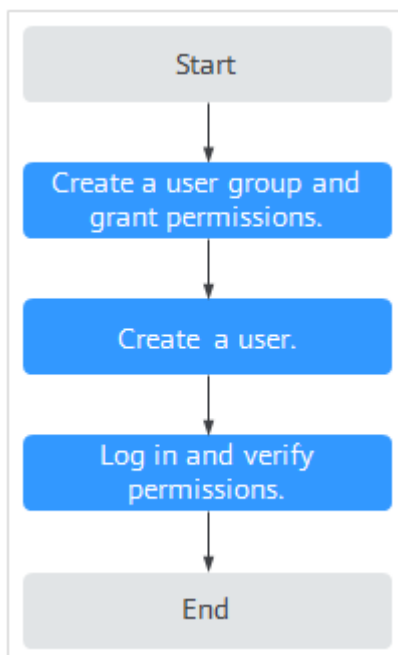
- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to Anti-DDoS resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust a HUAWEI CLOUD account or cloud service to perform professional and efficient O&M to your 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 1-14](#)).

#### Process

**Figure 1-14** Process for granting permissions



1. [Create a user group and assign permissions.](#)

Create a user group on the IAM console and assign the Anti-DDoS administrator permission to it.

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

Create a user on the IAM console and add the user to the user 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 Huawei Cloud console, select any other services. If a message indicating that the permission is insufficient is displayed, the **Anti-DDoS Administrator** permission takes effect.

## 1.10.2 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"
      ]
    }
  ]
}
```

## 1.10.3 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 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

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	-
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	-
Disabling Anti-DDoS	anti-ddos:ip:disableDefensePolicy	-
Querying weekly defense statistics	anti-ddos:ip:getWeeklyReport	-
Querying the traffic of a specified EIP	anti-ddos:ip:getDailyTrafficReport	-

Permission	Action	Dependency
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	-
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	-

## 1.10.4 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 1-9](#).

**Table 1-9** Anti-DDoS console dependency policies and roles

Console Function	Dependent Service	Role or Policy
Configuring Anti-DDoS logs on LTS	Log Tank Service (LTS)	The <b>LTS ReadOnlyAccess</b> system policy is required to select log group and log stream names created in LTS.
Enabling alarm notifications	Simple Message Notification (SMN)	The <b>SMN ReadOnlyAccess</b> 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 <b>TMS FullAccess</b> system policy is added.



# 2 CNAD Advanced Operation Guide

## 2.1 Usage Overview

After you enable a CNAD instance and bind Huawei Cloud public IP addresses to it, you can use the CNAD anti-DDoS capabilities to protect your cloud services.

[Table 2-1](#) shows the usage overview of CNAD.

**Table 2-1** CNAD usage overview

Step	Description
Purchasing a CNAD instance	For details, see <a href="#">Purchasing a CNAD Instance</a> .
Configuring protection policies	CNAD provides a wide range of protection rules. You can configure protection policies based on your service requirements. For details, see <a href="#">Adding a Protection Policy</a> .
Adding a protected object	You can add public IP addresses on Huawei Cloud as protected objects to enable CNAD for them. For details, see <a href="#">Adding a Protected Object</a> .
Enabling alarm notifications	After the alarm notification is enabled, you will receive alarm notifications if your IP address is under a DDoS attack. For details, see <a href="#">Setting Alarm Notifications</a> .
Viewing statistics report	You can view the access and attack statistics of last three days. For details, see <a href="#">Viewing Statistics Reports</a> .
Managing instances	Perform common instance management operations, such as enabling renewal, upgrading specifications, and configuring labels. For details, see <a href="#">Managing Instances</a> .

Step	Description
Setting event alarm notifications	Cloud Eye enables event monitoring for protected EIPs and generates alarms for scrubbing, blocking, and unblocking events. For details, see <a href="#">Setting Event Alarm Notifications</a> .

## 2.2 Purchasing a CNAD Instance

To enable CNAD protection, you need to purchase CNAD instances. CNAD takes effect immediately after you purchase it.

### Prerequisites

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.


### Specifications Restrictions

The Unlimited Protection Advanced edition can protect only exclusive EIPs. You can [submit a work order](#) to the Anti-DDoS Service team to obtain the permission to purchase exclusive EIPs.

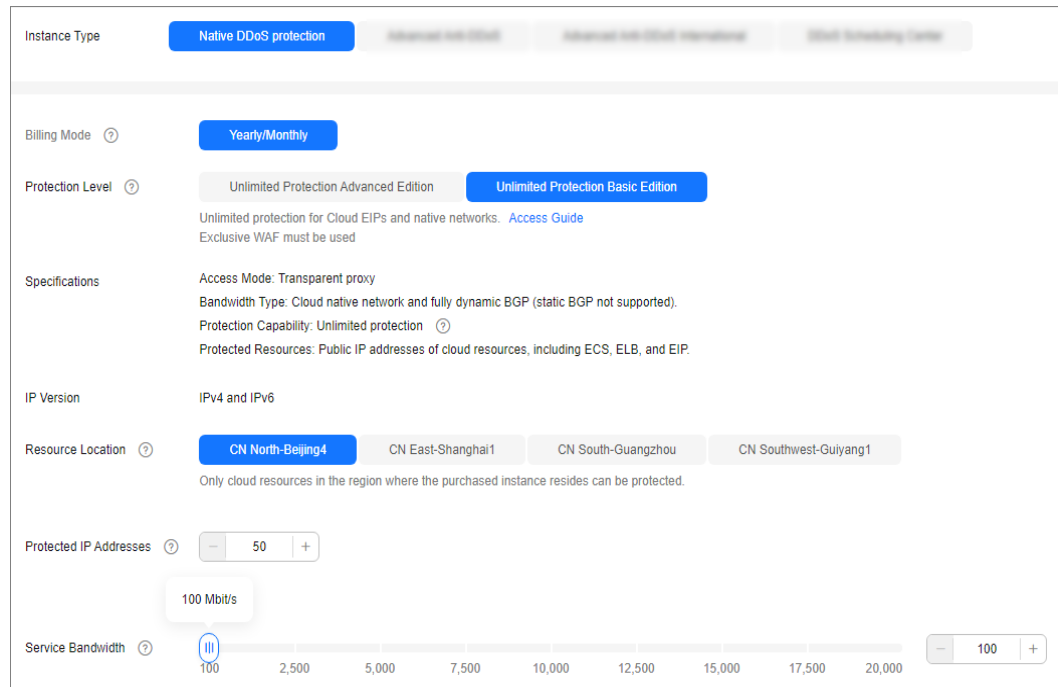
### Constraints

Ensure that the account used for purchasing CNAD instances has both the **CNAD FullAccess** and **BSS Administrator** roles or has the **Tenant Administrator** role.

### 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 CNAD Pro**.
- Step 4** Set **instance Type** to **Native DDoS Protection**.
- Step 5** Set **Protection Level** to **Unlimited Protection Basic Edition**.
- Step 6** Set the specifications parameters, as shown in [Figure 2-1](#). [Table 2-2](#) describes the parameters.

**Figure 2-1** Setting Unlimited Protection Basic edition specifications



**Table 2-2** Specifications of the Unlimited Protection Basic edition

Parameter	Description
Resource Location	Select the region where the protected resources are located. <b>NOTICE</b> 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 7** Set **Instance Name**, **Required Duration**, and **Quantity**. In the lower right corner of the page, click **Next**.

- **Required Duration:** You can select 3 months, 6 months, or 1 year.
- **Quantity:** Select the number of instances you want to purchase.

**NOTE**

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

**Step 8** On the confirmation page, confirm your order and click **Submit Order**.

**Step 9** 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 CNAD Pro**.

**Step 4** Set **instance Type** to **Native DDoS Protection**.

**Step 5** Select **Unlimited Protection Advanced Edition** for **Protection Level**.

**Step 6** Set the specifications parameters. [Table 2-3](#) describes related parameters.

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

The screenshot displays the configuration interface for the Unlimited Protection Advanced Edition. Key settings include:

- Instance Type:** Native DDoS protection
- Billing Mode:** Yearly/Monthly
- Protection Level:** Unlimited Protection Advanced Edition
- Specifications:**
  - Access Mode: Transparent proxy
  - Bandwidth Type: Cloud native network, multi-line BGP
  - Protection Capability: Unlimited protection
  - Protected Resources: Anti-DDoS Exclusive EIP
- IP Version:** IPv4
- Resource Location:** CN North-Beijing4
- Protected IP Addresses:** 50
- Service Bandwidth:** 100 Mbit/s

**Table 2-3** Specifications of the Unlimited Protection Advanced edition

Parameter	Description
Resource Location	Select the region where the protected resources are located. <b>NOTICE</b> 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 7** Set **Instance Name**, **Required Duration**, and **Quantity**. In the lower right corner of the page, click **Next**.

- **Required Duration:** You can select 3 months, 6 months, or 1 year.
- **Quantity:** Select the number of instances you want to purchase.

 **NOTE**

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

**Step 8** On the confirmation page, confirm your order and click **Submit Order**.

**Step 9** 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


## 2.3 Adding a Protection Policy

### 2.3.1 Configuring the Scrubbing Threshold

If the DDoS bandwidth on an IP address exceeds the configured threshold, CNAD is triggered to scrub attack traffic to ensure service availability.

#### Procedure

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

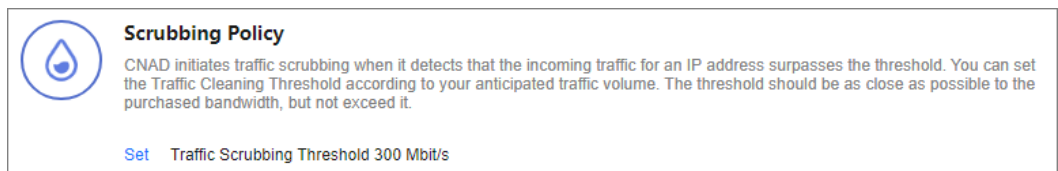
- Step 2** Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.
- Step 3** In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced > 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 2-3** Creating a policy



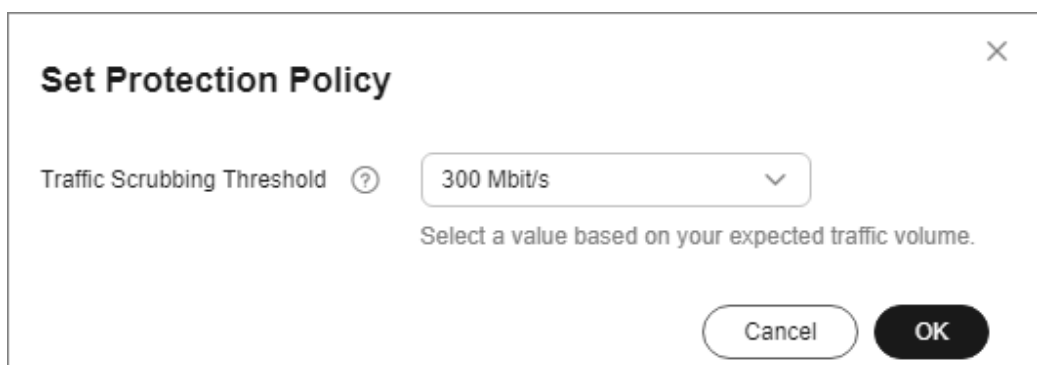
- Step 6** In the row containing the target policy, click **Set Protection Policy** in the **Operation** column.
- Step 7** In the **Scrubbing Policy** area, click **Set**.

**Figure 2-4** Scrubbing Policy



- Step 8** In the **Set Protection Policy** dialog box that is displayed, set the traffic scrubbing threshold, as shown in [Figure 2-5](#).

**Figure 2-5** Set Protection Policy



**Step 9** Click **OK**.

----End

## 2.3.2 Watermarking

### 2.3.2.1 Configuring Watermark Protection


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.

#### Constraints

Up to two keys can be configured for a watermark.

#### Procedure

**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

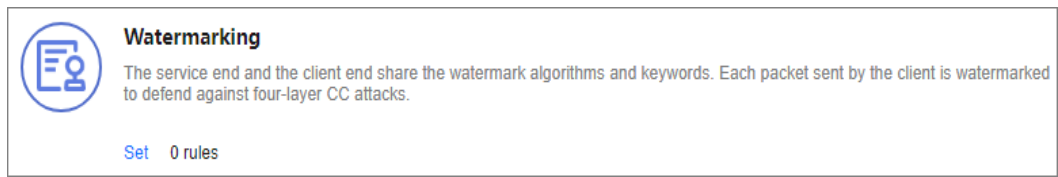


The screenshot shows a dialog box titled "Create Protection Policy". It has a close button (X) in the top right corner. The dialog contains two input fields: "Name" with the value "test" and "Instance" with a dropdown menu showing "CNAD-9cb4". At the bottom right, there are two buttons: "Cancel" and "OK".

**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**.

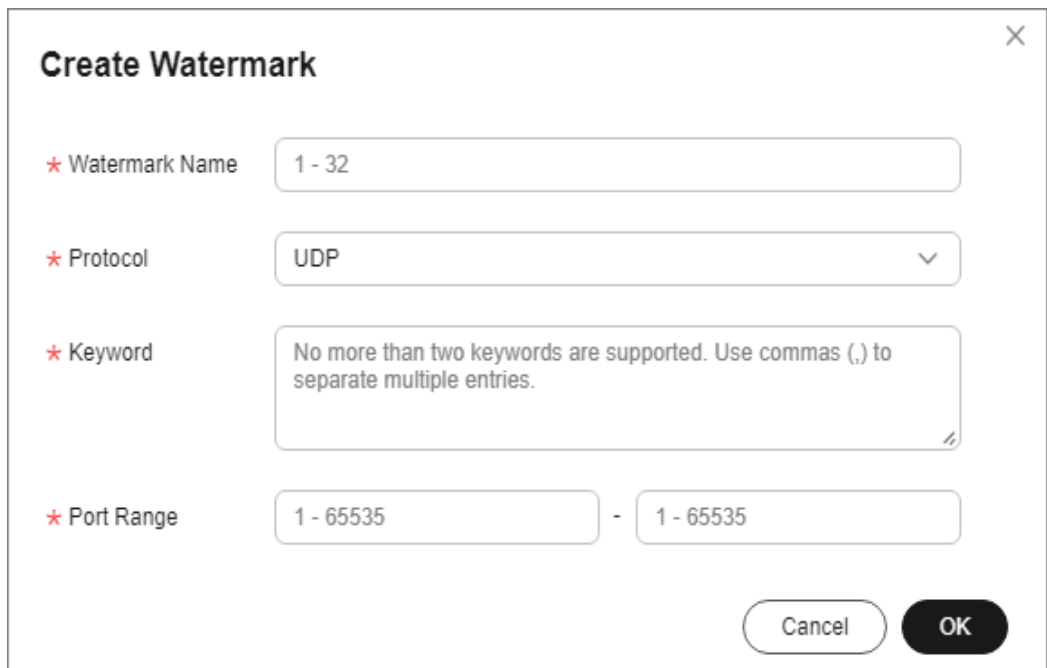
**Figure 2-7** Watermarking



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

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

**Figure 2-8** Create Watermark



**Table 2-4** Watermark parameters

Parameter	Description
Watermark Name	Watermark name
Protocol	Currently, only <b>UDP</b> 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**.

**NOTE**

For details about how to configure watermarks, see section [Watermark Configuration Guide](#).

----End

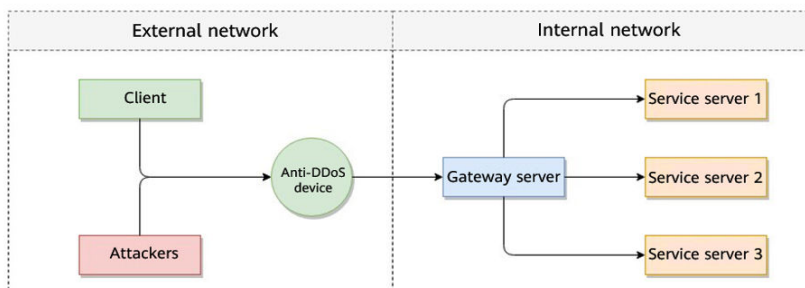


## 2.3.2.2 Watermark Configuration Guide

### 2.3.2.2.1 Working Principles

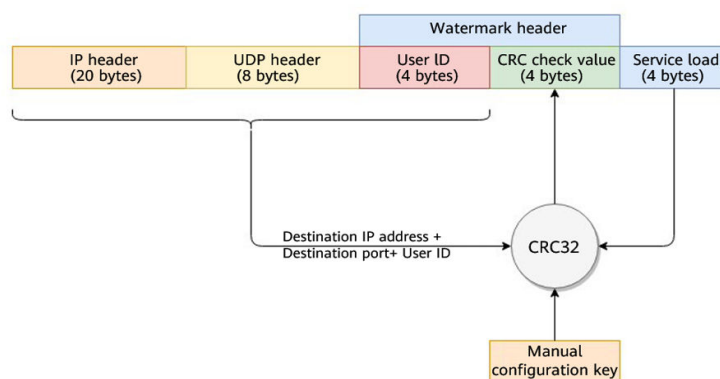
There are generally two modes of defending against UDP floods: dynamic fingerprint learning and UDP traffic limiting. The former may mistakenly learn normal service payloads as attack fingerprints, leading to false positives. The latter may block both normal and attack traffic, affecting your service.

**Figure 2-9** Device protection principles



As shown in [Figure 2-10](#), the Huawei cloud solution adds watermark header information to UDP packets to distinguish normal service packets from attack packets. The offline Anti-DDoS device verifies the UDP watermark and allows only the normal service packets to pass through, while blocking the 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.

### 2.3.2.2.2 Development Example

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.

## Example Code for Calculating the CRC Hash Value

**CAUTION**

The CRC algorithm in this section uses CRC-32-IEEE 802.3.

- 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;
    }
}
```

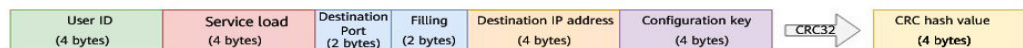
- Interface for calculating the CRC hash value. The first parameter **crc** is set to **0** by default.

```
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;
}
```

## Example Code for Calculating the Watermark Value of a Packet

Figure 2-11 shows the watermark structure for compute

Figure 2-11 Watermark structure for compute



- The watermark data structure is defined as follows:

```
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;
```

**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.
- 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));
}
    
```

### Filling UDP Watermarks

The packet is filled with the calculated CRC hash value according to the structure in [Figure 2-12](#) and then sent out.

**Figure 2-12** Filling UDP watermarks




### 2.3.3 Configuring an ACL

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

#### Constraints

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

#### Procedure

- 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 2-13** Creating a policy



The screenshot shows a dialog box titled "Create Protection Policy". It has a close button (X) in the top right corner. The dialog contains two input fields: "Name" with the value "test" and "Instance" with a dropdown menu showing "CNAD-9cb4". At the bottom right, there are two buttons: "Cancel" and "OK".

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

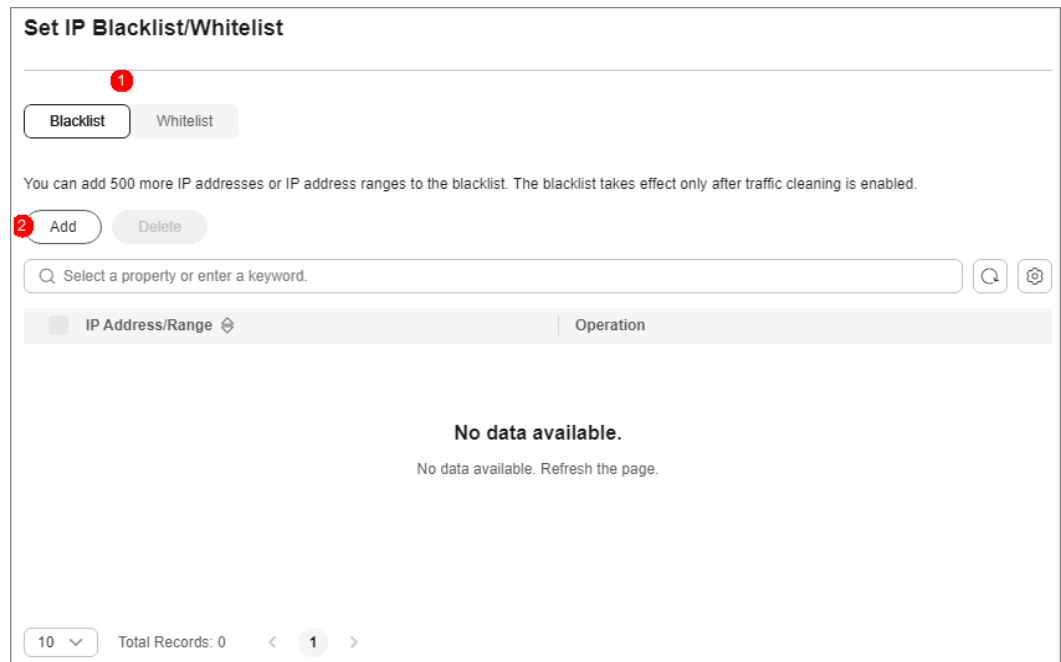
**Step 7** In the **IP Blacklist/Whitelist** area, click **Set**.

**Figure 2-14** IP Blacklist/Whitelist



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

**Figure 2-15** Add IP Address



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

**Figure 2-16** Adding blacklist IP addresses

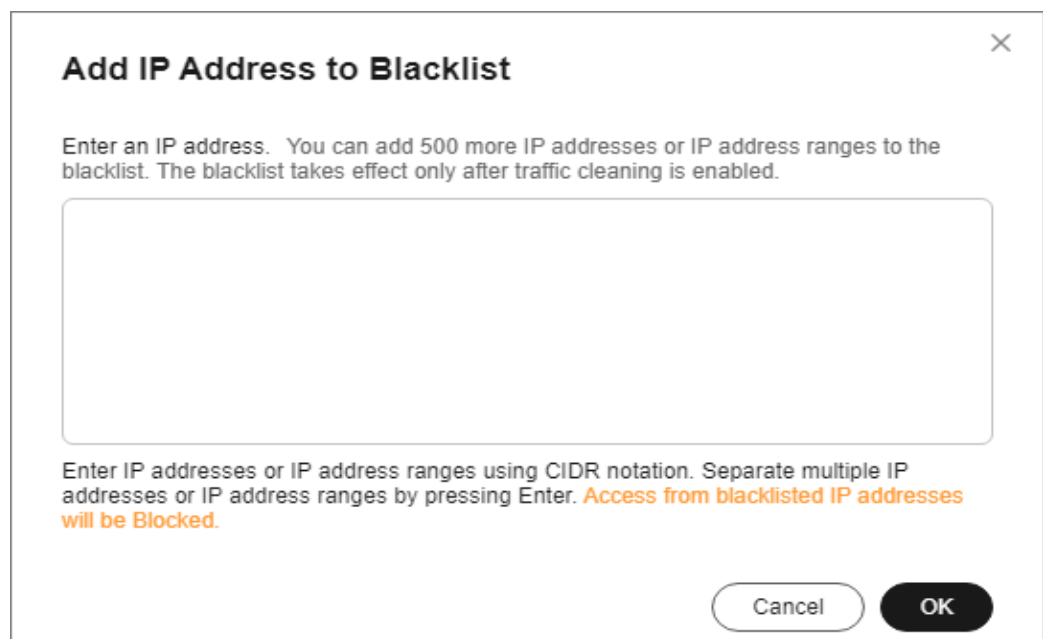
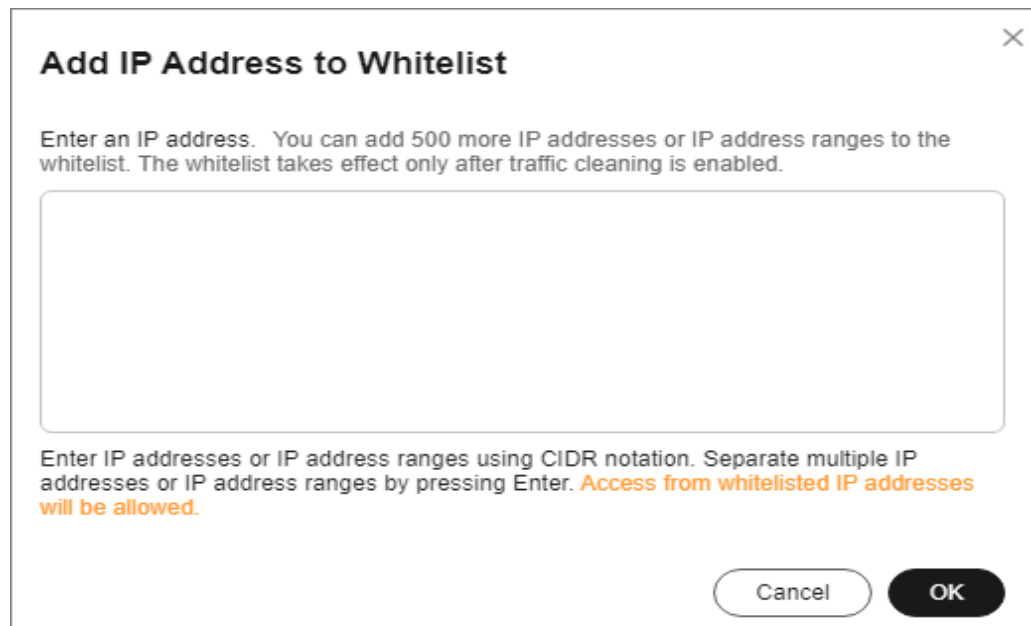


Figure 2-17 Adding whitelist IP addresses



----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.

## 2.3.4 Configuring Port Blocking

You can block the source traffic accessing CNAD based on port blocking rules.

### Procedure

- 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**.

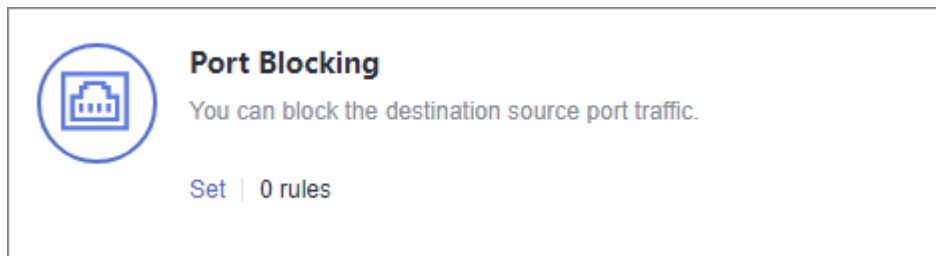
**Figure 2-18** Creating a policy



**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 2-19** Port blocking configuration box



**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 2-20** Creating a port ACL rule



**Table 2-5** 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	Type of the port to be blocked

Parameter	Description
Start Port-End Port	Set the range of ports to be blocked.
Action	Protection action after the port is blocked

**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.

## 2.3.5 Configuring Protocol Blocking

Traffic control is implemented for traffic targeting CNAD based on protocols. You can disable the UDP/TCP/ICMP protocol to block the traffic transmitted via the UDP/TCP/ICMP protocol.

### Procedure

**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

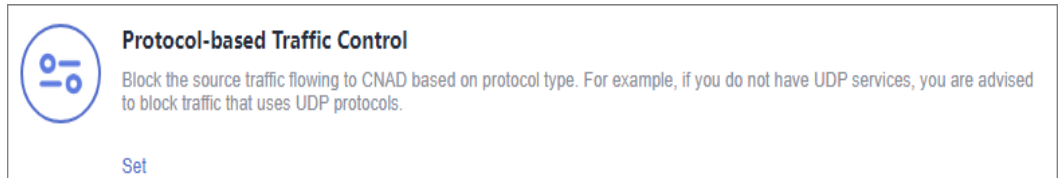




**Step 6** In the row containing the target policy, click **Set Protection Policy** in the **Operation** column.

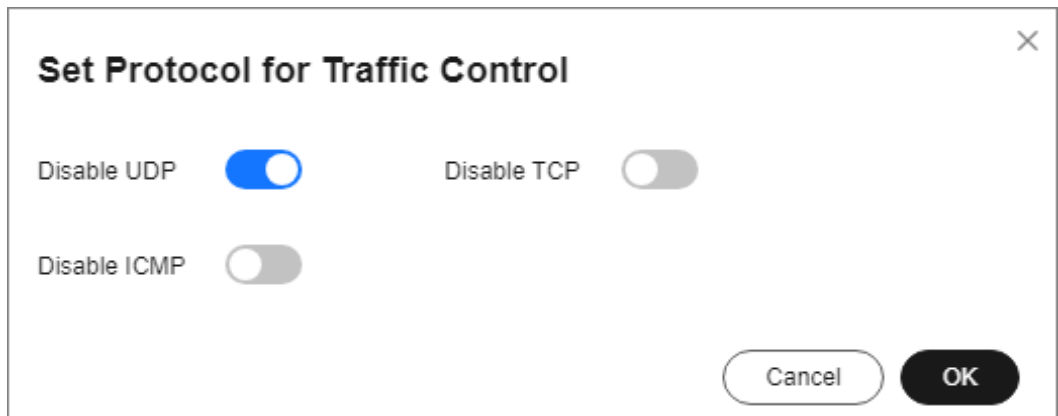
**Step 7** In the **Protocol-based Traffic Control** area, click **Set**.



**Figure 2-22** Protocol-based Traffic Control



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

**Figure 2-23** Setting protocol blocking



-  indicates that traffic blocking is enabled. UDP, TCP, and ICMP traffic is blocked.
-  indicates that traffic blocking is disabled.


----End

## 2.3.6 Configuring Fingerprint Filtering

You can configure fingerprint filtering rules to perform feature matching on the content at a specified location in a data packet and set discarding or rate limiting rules based on the matching result.

### Procedure

**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

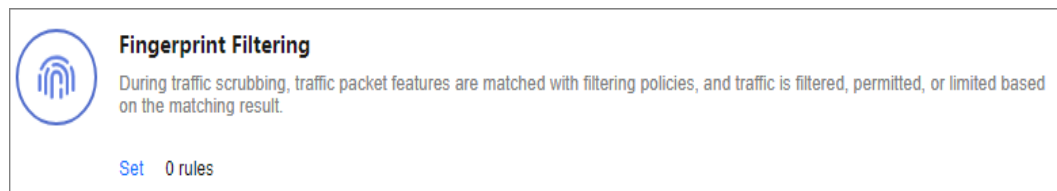


The screenshot shows a dialog box titled "Create Protection Policy". It has a close button (X) in the top right corner. The dialog contains two input fields: "Name" with the value "test" and "Instance" with a dropdown menu showing "CNAD-9cb4". At the bottom right, there are two buttons: "Cancel" and "OK".

**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 2-25** Fingerprint filtering configuration box



The screenshot shows a configuration box for "Fingerprint Filtering". It has a fingerprint icon on the left. The title is "Fingerprint Filtering". Below the title is a description: "During traffic scrubbing, traffic packet features are matched with filtering policies, and traffic is filtered, permitted, or limited based on the matching result." At the bottom, there is a "Set" button and the text "0 rules".

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

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

**Figure 2-26** Creating a fingerprint

**Table 2-6** Fingerprint parameters

Parameter	Description
Fingerprint Name	Enter the fingerprint rule name.
Protocol	Set the protocol of the fingerprint.
Start Source Port - End Source Port	Set the range of the fingerprint source ports.
Start Destination Port-End Destination Port	Set the range of the fingerprint destination ports.
Action	Set the action and rate limit after the fingerprint rule is matched. You can select <b>Discard</b> or <b>Allow</b> .
Test Load	Enter the hexadecimal value of the test load.
Offset	Set the offset of the fingerprint.
Check Depth	If, for example, the test load is "1234afee", the offset is 20, and the check depth is 8, then if there is data from the 21st byte to the 32nd byte that can be matched to "1234afee", the packet matches the fingerprint. $32 = 20 + 4$ (fingerprint length) + 8 (check depth)

**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.

## 2.3.7 Configuring Connection Protection


### NOTICE

The connection protection function is still in the open beta test (OBT) phase. This function is supported only by Unlimited Protection Advanced Edition instances in North China regions. You can [submit a service ticket](#) to enable this function.

If an origin server IP address frequently sends suspicious packets, you can configure connection protection to block the IP address. After the blocking period expires, the access from the IP address will be allowed.

## Procedure

**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** ×

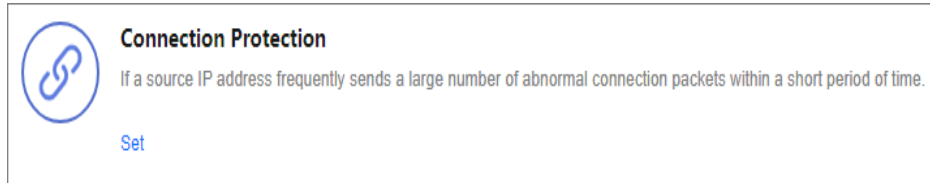
Name

Instance

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

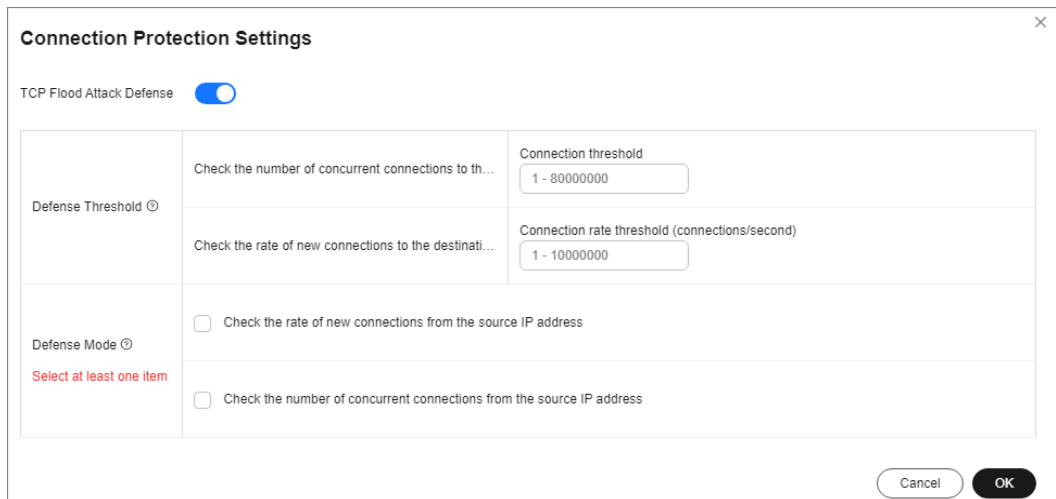
**Step 7** In the **Connection Protection** area, click **Set**.

**Figure 2-28** Connection Protection



**Step 8** Enable **TCP Flood Attack Defense** and set other parameters.

**Figure 2-29** Connection Protection Settings



**Table 2-7** Parameter description

Parameter	Description
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 <b>Threshold</b> , defense against connection flood attacks is started. After the defense is started, the source IP address starts to be checked. The value ranges from 1 to 80000000.
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 <b>Threshold</b> , defense against connection flood attacks is started. After the defense is started, the source IP address starts to be checked. The value ranges from 1 to 10000000.

Parameter	Description
Check the rate of new connections from the source IP address.	After defense against connection flood attacks is enabled, if the number of the TCP connections initiated by a source IP address within <b>Check Cycle</b> exceeds <b>Threshold</b> , the source IP address is regarded as the attack source and is reported to the ATIC management center. The values range from 1 to 60 (s) and 1 to 80000000, respectively.
Check the number of concurrent connections from the source IP address.	After defense against connection flood attacks is enabled, if the number of the concurrent TCP connections of a source IP address exceeds <b>Threshold</b> , the source IP address is regarded as the attack source and is reported to the ATIC management center. The value ranges from 1 to 80000000.

**Step 9** Click **OK**.


----End

## 2.3.8 Configuring Geo-Blocking

You can configure geo-blocking to prevent traffic from specific regions.

### Procedure

**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



**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 2-31** Geo-blocking settings



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

**Figure 2-32** Select blocked locations



**NOTE**

Currently, only **Locations outside China** can be blocked.

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

----End

## 2.4 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.


### Prerequisites

You have purchased a CNAD instance.

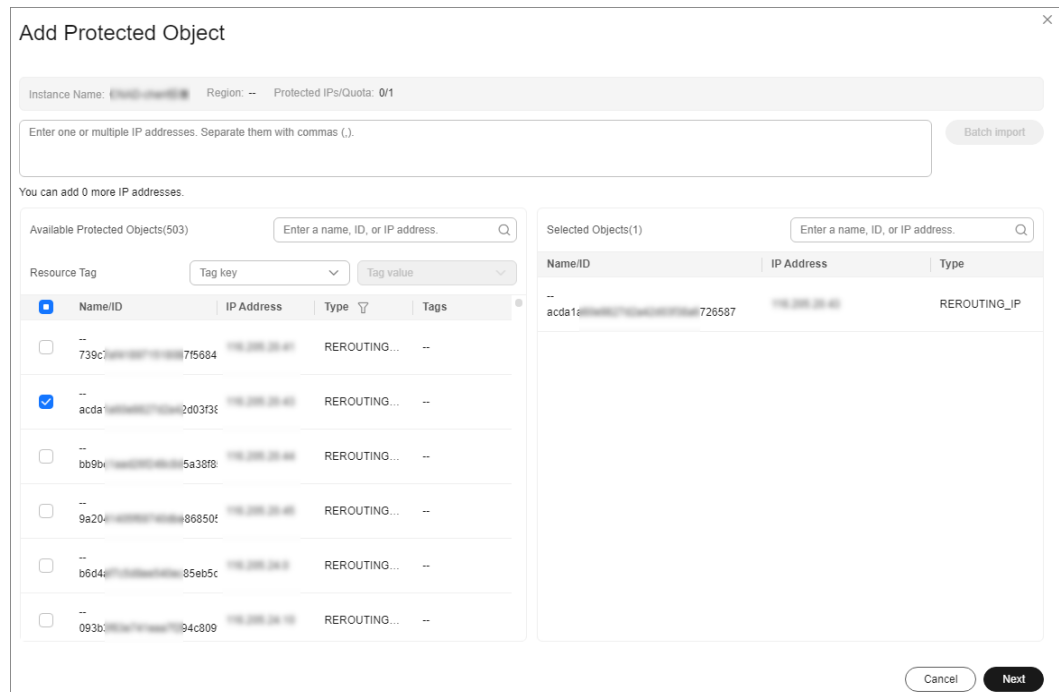
### Constraints

- The added protected objects (such as ECS, ELB, WAF, and EIP) are in the same region as the region of the purchased CNAD instance.
- The Unlimited Protection Advanced Edition can only protect exclusive EIPs. Exclusive EIPs can only be bound to instances of the Unlimited Protection Advanced Edition.

## Procedure

- 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 upper right corner of the target instance box, click **Add Protected Object**.
- Step 5** In the **Add Protected Object** dialog box that is displayed, select the IP addresses you want to protect and click **Next**.

**Figure 2-33** Adding a protected object



### 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 2-34** Confirming protected object settings

The screenshot shows a dialog box titled "Add Protected Object". At the top, it says "Deleted IP addresses: 0" with a "Show" link. Below that, it says "Added IP addresses: 1" with a "Hide" link. A table lists the added IP addresses:

Name/ID	IP Address	Type
b56	192.168.1.1	REROUTING_IP

At the bottom, there is a dropdown menu for "Select a Protection Policy (Only for New IP Addresses)" with "testNewPolicy\_llc1" selected, and a "Create Protection Policy" link. There are also "Previous", "Cancel", and "OK" buttons.

**NOTE**

For details about how to set protection policies, see [Adding a Protection Policy](#).

----End

## Related Operations

- In the instance box, click **View** next to **Protected IPs** to view the protected objects of the current instance.
- If an IP address does not need to be protected by CNAD, remove the IP address. For more details, see [Managing Protected Objects](#).
- **Configuring a tag:** In the **Tag** column of the row containing the target object, click . Enter the label name and click **OK**.

## 2.5 Setting Alarm Notifications

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.

### Prerequisites

You have purchased a CNAD instance.

### Constraints

- The Simple Message Notification (SMN) service is a paid service. For details about the price, see [SMN Product Pricing Details](#).
- Only notification topics in the same region as the CNAD Advanced instance can be displayed.

### Procedure

**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** Enable alarm notifications.

**Figure 2-35** Setting



Select an existing topic from the drop-down list, or click **View Topic** and create an SMN topic and configure an endpoint for receiving alarm notifications.

Perform the following steps to create a topic:


1. Create a topic by referring to [Creating a Topic](#).
2. Follow the instructions described in [Adding a Subscription](#) to configure an endpoint, such as mobile number or email address, to receive alarm notifications.

For details about topics and subscriptions, see *Simple Message Notification User Guide*.

**Step 5** Click **Apply**.

----End

## Related Operations

To disable alarm notifications, set the button in [Figure 2-35](#) to .

## 2.6 Managing Protection Logs

### 2.6.1 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.

## Prerequisites

You have set a protection policy for a protected object.

## Procedure


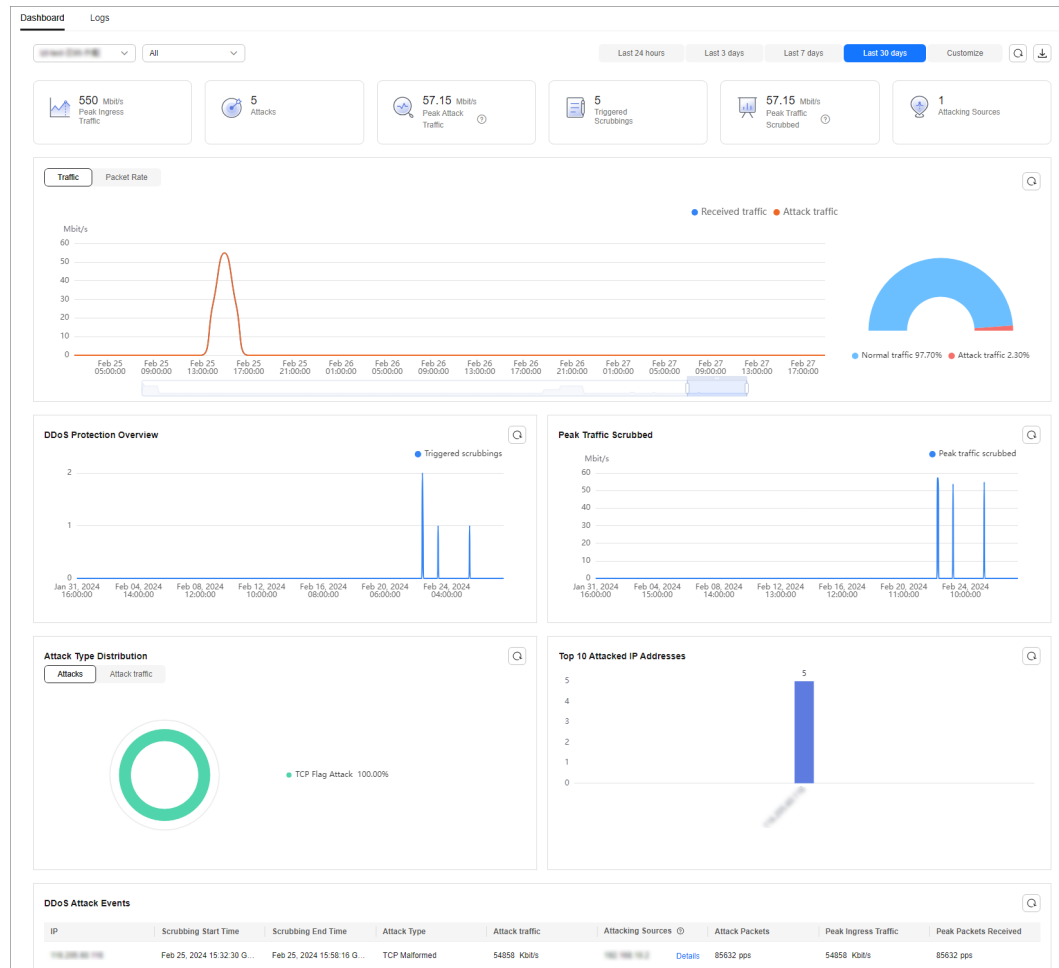
- Step 1** Log in to the management console.
- Step 2** Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.
- Step 3** In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced > Dashboard**. The **Dashboard** page is displayed.

Figure 2-36 Dashboard

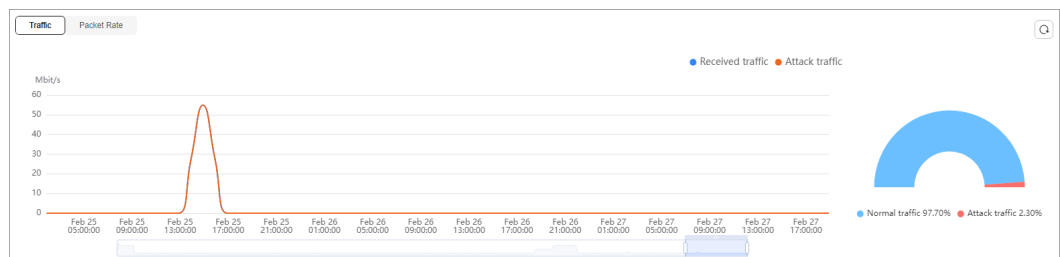



 NOTE

- 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.

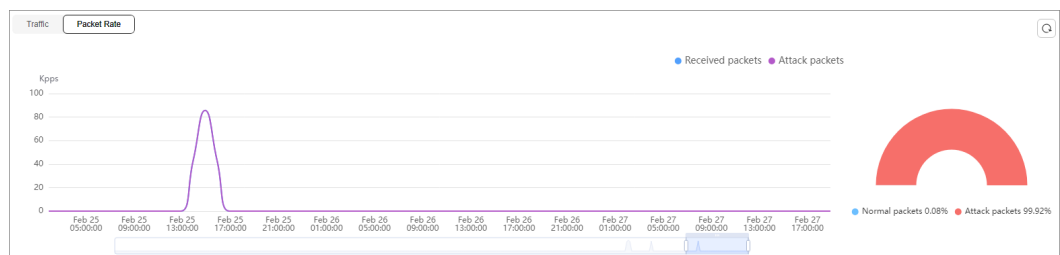
**Figure 2-37** Traffic




Click  in the upper right corner of the page to download protection logs.

**Step 5** Click the **Packet Rate** tab to view the packet rate data.

**Figure 2-38** Packet Rate



Click  in the upper right corner of the page to download protection logs.

----End

## 2.7 Managing Instances


### 2.7.1 Viewing Information About an Instance

After enabling CNAD, you can view instance information.

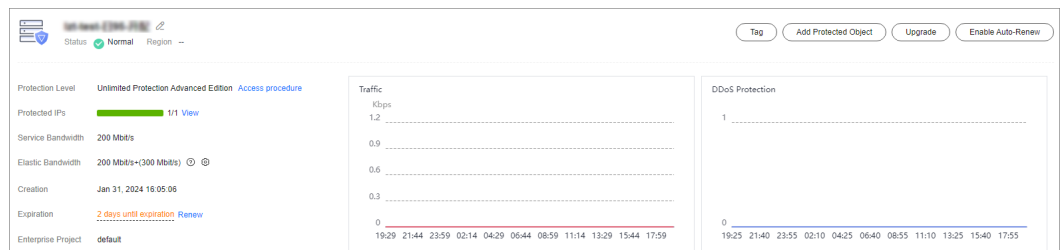
## Prerequisites

You have purchased a CNAD instance.

## Procedure

- 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 2-39** Instances




----End

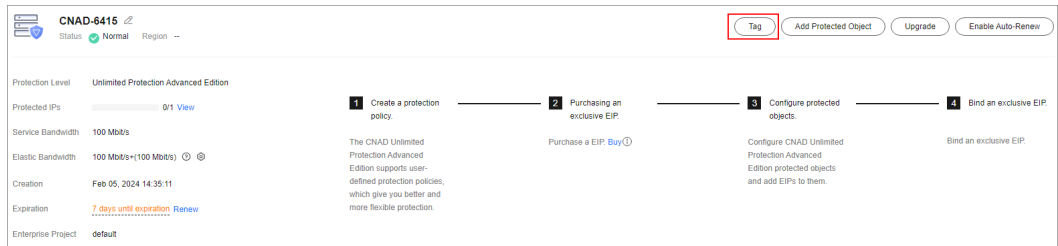
## 2.7.2 Configuring Instance Tags

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.

## Procedure

- 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 2-40** Set a tag for a CNAD instance

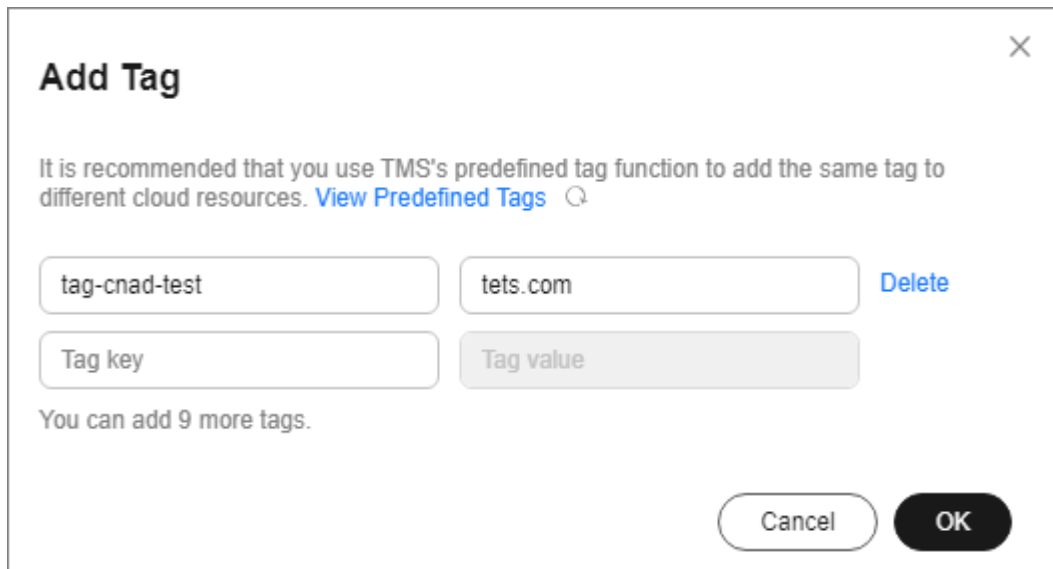


**Step 5** On the tag adding page, click **Add Tag** to add a tag.

**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 2-41** Adding a tag



**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

## 2.8 Managing Protected Objects


### 2.8.1 Viewing Details about a Protected Object

After adding a protected object, you can view its details.

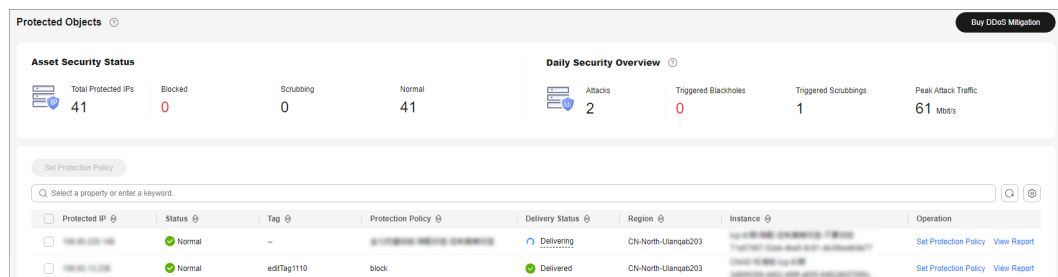
## Prerequisites

You have added a protected object.

## Procedure

- 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 2-42** Protected objects



- Step 4** View the information described in [Table 2-8](#) about the target protected object.

**Table 2-8** 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 <ul style="list-style-type: none"> <li>• Normal</li> <li>• Delivering</li> </ul>
Protection Policy	Protection policy for a protected IP address
Region	Region of a protected IP address
Instance	Instance that a protected IP address belongs to
Operation	<ul style="list-style-type: none"> <li>• You can click <b>View Report</b> to go to the <b>Dashboard</b> tab and view protection data.</li> <li>• If no protection policy has been configured for a protected IP address, you can click <b>Set Protection Policy</b> to select a protection policy for the IP address.</li> </ul>

----End

## 2.8.2 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.

### Prerequisites

- A protection policy has been created and configured.
- You have added a protected object.
- No protection policy has been set for the protected object.

### Procedure


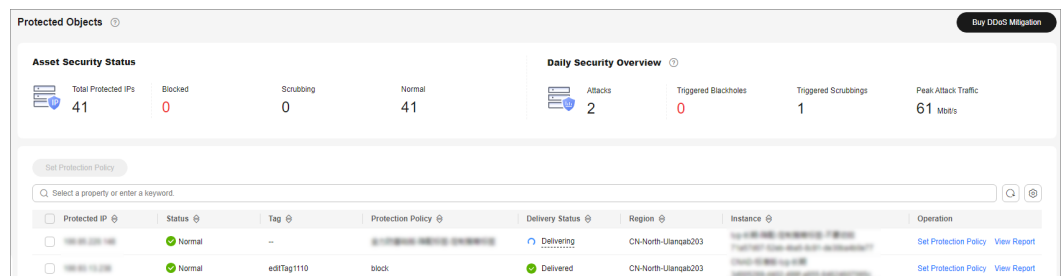
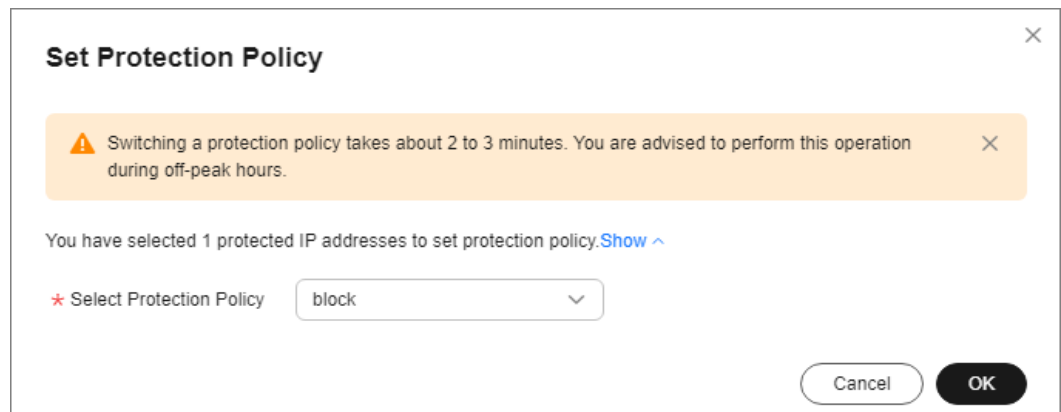
- Step 1** Log in to the management console.
- Step 2** Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.
- Step 3** In the navigation tree on the left, choose **Cloud Native Anti-DDoS Advanced > Protected Objects**. The **Protected Objects** page is displayed.

Figure 2-43 Protected objects



- 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 2-44 Set Protection Policy





 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.

## 2.8.3 Deleting a Protected Object

If a protected object does not require CNAD, you can delete the object.

---

**NOTICE**

If an EIP bound to a CNAD instance is removed, it will be automatically protected by Anti-DDoS, of which the protection capability is less than or equal to 5 Gbit/s.


After an exclusive EIP bound to a CNAD instance is removed, the EIP will be blacklisted and cannot be accessed from the Internet. Exercise caution when removing a protected object.

---

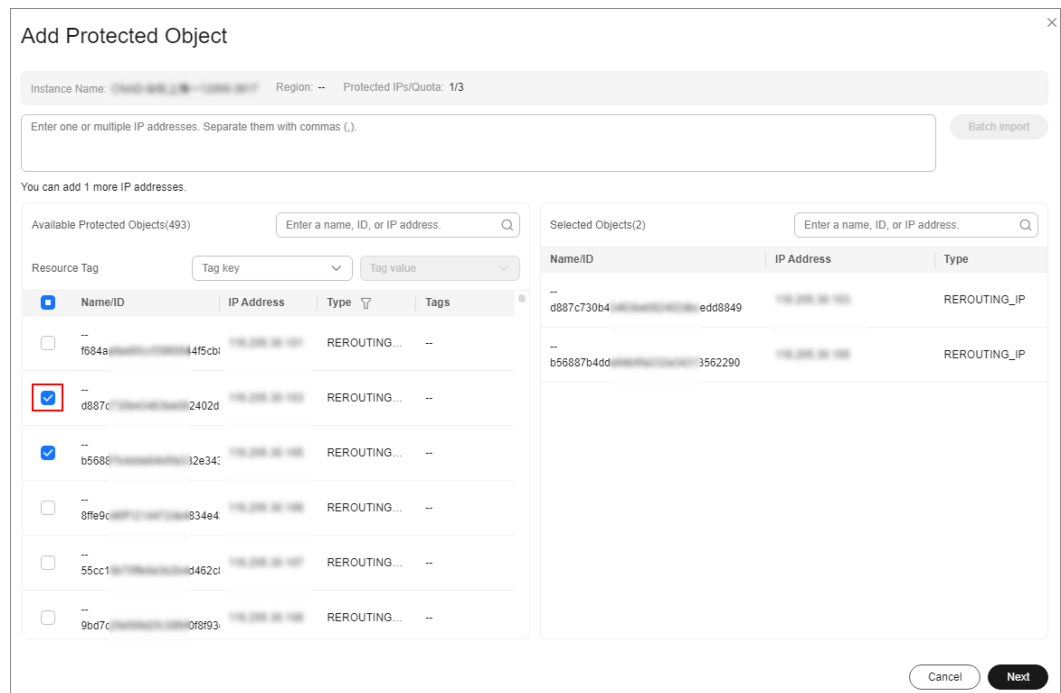
## Prerequisites

You have added a protected object.

## Procedure

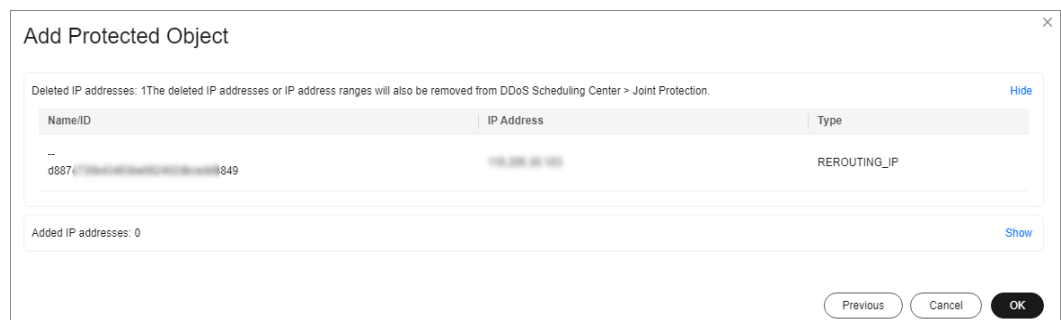
- Step 1** Log in to the management console.
- Step 2** Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.
- Step 3** In the navigation pane on the left, 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 2-45** Deleting a protected object



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

**Figure 2-46** Confirming the removal of a protected object



----End

## Batch Deleting Protected Objects

You can batch select objects you want to delete and click **Delete** above the object list.

## 2.9 Permissions Management

### 2.9.1 Creating a User and Granting the CNAD Pro Access Permission

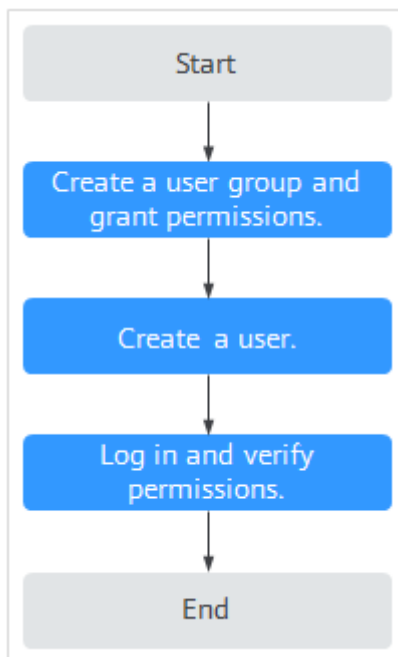
You can use Identity and Access Management (IAM) for refined permissions control for CNAD Pro resources. To be specific, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing CNAD Pro 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 Pro resources.


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

## Process

**Figure 2-47** Process for granting permissions



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.

## 2.9.2 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:blackWhitelplist: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:blackWhitelplist:delete"
      ]
    },
  ]
}
```

## 2.9.3 CNAD Pro Permissions and Actions

This section describes how to use IAM for fine-grained CNAD Pro 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 <b>cnad:alarmConfig:create</b> permission and the <b>SMN Administrator</b> permission configured for the <b>CN-Hong Kong</b> region to the users.

Permission	Action	Dependency
Deleting an Alarm Notification	cnad:alarmConfig:delete	To grant the alarm notification permission to users, you must also grant the <b>cnad:alarmConfig:delete</b> permission and the <b>SMN Administrator</b> permission configured for the <b>CN-Hong Kong</b> region to the users.
Querying Alarm Notifications	cnad:alarmConfig:get	To grant the alarm notification permission to users, you must also grant the <b>cnad:alarmConfig:get</b> permission and the <b>SMN Administrator</b> permission configured for the <b>CN-Hong Kong</b> region to the users.
Upgrading an Instance	cnad:package:put	-

Permission	Action	Dependency
Binding an IP Address to Be Protected to an Instance	cnad:protectedIp:create	<p>To grant a user the permission for binding objects to a CNAD Pro instance, you need to grant both the <b>cnad:protectedIp:create</b> permission and the <b>vpc:publicIps:list</b> permission configured for the region to which the instance belongs.</p> <p>For example, a user purchases a CNAD Pro instance that is located in <b>CN-Hong Kong</b>. To grant a user the permission for binding objects to a CNAD Pro instance, you need to grant both the <b>cnad:protectedIp:create</b> permission, and the <b>vpc:publicIps:list</b> permission configured for <b>CN-Hong Kong</b> so that the user can only perform operations on the protected objects in <b>CN-Hong Kong</b>.</p>
Creating a Protection Policy	cnad:policy:create	-
Updating a Protection Policy	cnad:policy:put	-
Deleting a Protection Policy	cnad:policy:delete	-
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:blackWhitelPList:create	-
Deleting a Blacklist or Whitelist Rule	cnad:blackWhitelPList:delete	-

Permission	Action	Dependency
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	-
Querying the Distribution of Attack Types	cnad:attackTypeReport:list	-
Querying Attack Events	cnad:attackReport:list	-
Querying Top 10 Attacked IP Addresses	cnad:attackTop:list	-



Permission	Action	Dependency
Creating an Instance	cnad:package:create	<p>To grant a user the permission for purchasing CNAD Pro, you need to grant the <b>cnad:package:create</b> permission to the user and the following BSS permissions configured for all regions:</p> <ul style="list-style-type: none"> <li>• bss:order:update Order Operation</li> <li>• bss:contract:update Contract Modification</li> <li>• bss:balance:view Account Querying</li> <li>• bss:order:pay Payment</li> </ul>

## 2.9.4 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 Pro 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 2-9](#).

**Table 2-9** 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.

Console Function	Dependent Service	Roles or Policy
Configuring instance tags	Tag Management Service (TMS)	Tag keys can be created only after the <b>TMS FullAccess</b> 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 <b>EPS ReadOnlyAccess</b> system policy.

## 2.10 Monitoring

### 2.10.1 Setting Event Alarm Notifications

#### Scenarios

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.

#### Procedure



- 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 2-10](#).

Figure 2-48 Alarm parameters

The screenshot displays the configuration page for an alarm rule. Key sections include:

- Name:** A text input field containing 'alarm-v0t'.
- Description:** An empty text area.
- Alarm Type:** A toggle switch set to 'Event'.
- Event Type:** A dropdown menu set to 'System event'.
- Event Source:** A dropdown menu set to 'Elastic IP'.
- Monitoring Scope:** A dropdown menu set to 'All Resources'.
- Method:** A button labeled 'Configure manually'.
- Alarm Policy:** A table with columns for Event Name, Alarms Policy, Alarm Severity, and Operation. It lists four policies: 'EIP blocked', 'EIP unblocked', 'Start DDoS traffic scrubbing', and 'Stop DDoS traffic scrubbing', all with an 'Immediate trigger' and a count of '1'.
- Alarm Notification:** A toggle switch set to 'On'.
- Notification Recipient:** A dropdown menu set to 'Notification group'.
- Notification Group:** A dropdown menu set to '-Select-'.
- Notification Window:** A time range selector set to 'Daily' from '00:00' to '23:59' in 'GMT+08:00'.
- Trigger Condition:** Two checkboxes, 'Generated alarm' and 'Cleared alarm', both of which are checked.

Table 2-10 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 <b>Event</b> .
Event Type	Choose <b>System Event</b> .
Event Source	Choose <b>Elastic IP</b> .
Monitoring Scope	Specifies the resource scope to which the alarm rule applies. Set this parameter as required.
Method	The default option is <b>Configure manually</b> .
Alarm Policy	You are advised to select <b>EIP blocked</b> , <b>EIP unblocked</b> , <b>Start Anti-DDoS traffic scrubbing</b> , and <b>Stop Anti-DDoS traffic scrubbing</b> .
Notification Recipient	Select <b>Notification group</b> or <b>Topic subscription</b> .

Parameter	Description
Notification Group	Select the required notification group.
Notification Object	Select the required topic subscription.
Notification Window	Set this parameter as required.
Trigger Condition	Choose <b>Generated alarm</b> and <b>Cleared alarm</b> .

**Step 7** Determine whether to send a notification based on the site requirements.

 **NOTE**

Alarm messages are sent by Simple Message Notification (SMN), which may incur a small amount of fees.

**Table 2-11** Notification Parameters

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 Recipient	You can select a <b>Notification group</b> or <b>Topic subscription</b> as required.
Notification Group	This parameter takes effect when <b>Notification Recipient</b> is set to <b>Notification group</b> . Set this parameter based on the site requirements.
Notification Object	This parameter is valid only when <b>Notification Recipient</b> is set to <b>Topic Subscription</b> . Set this parameter based on the site requirements.
Notification Window	Cloud Eye sends notifications only within the notification window specified in the alarm rule.
Trigger Condition	Set this parameter as required.

**Step 8** Click **Create**. In the dialog box that is displayed, click **OK**. The alarm notification is created successfully.

----End

## 2.10.2 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 [Metrics](#).

### Prerequisites

Purchasing a CNAD instance

### 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 2-12](#).

**Figure 2-49** Configuring Monitoring Alarm Rules

The screenshot shows a configuration page for monitoring alarm rules. It is divided into several sections:

- Name:** A text input field containing 'alarm-xdrx'.
- Description:** A larger text input field, currently empty.
- Alarm Type:** Two radio buttons, 'Metric' (selected) and 'Event'.
- Resource Type:** A dropdown menu with 'DDoS' selected.
- Dimension:** A dropdown menu with 'Package' selected.
- Monitoring Scope:** Two radio buttons, 'All resources' (selected) and 'Specific resources'.
- Method:** Three radio buttons: 'Associate template' (selected), 'Use existing template', and 'Configure manually'.
- Template:** A dropdown menu with '--Select--' and a 'Create Custom Template' link.
- Alarm Notification:** A toggle switch that is turned on.
- Notification Recipient:** Two radio buttons, 'Notification group' (selected) and 'Topic subscription'.
- Notification Group:** A dropdown menu with '--Select--' and a refresh icon.
- Notification Window:** A time range selector set to 'Daily' from '00:00' to '23:59' in 'GMT+08:00'.
- Trigger Condition:** Two checkboxes, 'Generated alarm' (checked) and 'Cleared alarm' (checked).

**Table 2-12** 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
Resource Type	Select <b>DDoS</b> from the drop-down list box.
Dimension	Select the resource dimension to be monitored. <ul style="list-style-type: none"> <li>Package: instance dimension</li> <li>Protected IP Address: IP address dimension</li> </ul>
Monitoring Scope	Scope where the alarm rule applies to. You can select <b>All resources</b> , <b>Resource groups</b> or <b>Specific resources</b> .

Parameter	Description
Method	<p>You can select <b>Associate template</b>, <b>Use existing template</b>, or <b>Configure manually</b>.</p> <p>For details about how to create a custom template, see <a href="#">Creating a Custom Template</a>.</p> <p><b>NOTE</b> After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.</p>
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	<p>Specifies the receiving method of the alarm notification. You can select <b>Notification group</b> or <b>Topic subscription</b>.</p> <ul style="list-style-type: none"> <li>Account contact is the mobile phone number and email address provided for registration.</li> <li>A topic is used to publish messages and subscribe to notifications. If the required topic is unavailable, create one and add subscriptions to it on the SMN console. For details, see <a href="#">Creating a Topic</a> and <a href="#">Adding Subscriptions</a>.</li> </ul>
Notification Group (Valid when <b>Notification Recipient</b> is set to <b>Notification group</b> )	Select the group to be notified.
Topic subscription (Valid when <b>Notification Recipient</b> is set to <b>Topic subscription</b> )	Select a notification topic.
Notification Window	Cloud Eye sends notifications only within the notification window specified in the alarm rule.
Trigger Condition	Condition for triggering the alarm notification. Select <b>Generated alarm</b> when an alarm is generated or <b>Cleared alarm</b> when an alarm is triggered, or both.

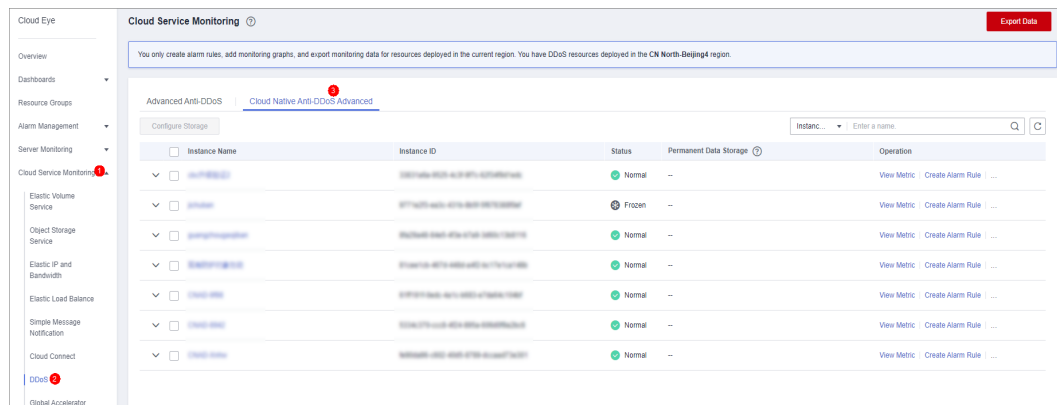
**Step 7** Click **Create**. In the displayed dialog box, click **OK**.

----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 > DDoS**. On the page that is displayed, click the **Cloud Native Anti-DDoS Advanced** tab.

**Figure 2-50** Cloud Native Anti-DDoS Advanced



- Step 5** Locate the row that contains the object to be monitored, and click **Create Alarm Rule**.
- Step 6** Enter the alarm rule information by referring to [Table 2-13](#).



**Figure 2-51** Configuring monitoring alarm rules

**Table 2-13** 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.

Parameter	Description
Method	You can select <b>Associate template</b> , <b>Use existing template</b> , or <b>Configure manually</b> . For details about how to create a custom template, see <a href="#">Creating a Custom Template</a> . <b>NOTE</b> 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	Specifies the receiving method of the alarm notification. You can select <b>Notification group</b> or <b>Topic subscription</b> . <ul style="list-style-type: none"> <li>Account contact is the mobile phone number and email address provided for registration.</li> <li>A topic is used to publish messages and subscribe to notifications. If the required topic is unavailable, create one and add subscriptions to it on the SMN console. For details, see <a href="#">Creating a Topic</a> and <a href="#">Adding Subscriptions</a>.</li> </ul>
Notification Group (Valid when <b>Notification Recipient</b> is set to <b>Notification group</b> )	Select the group to be notified.
Topic subscription (Valid when <b>Notification Recipient</b> is set to <b>Topic subscription</b> )	Select a notification topic.
Notification Window	Cloud Eye sends notifications only within the notification window specified in the alarm rule.
Trigger Condition	Condition for triggering the alarm notification. Select <b>Generated alarm</b> when an alarm is generated or <b>Cleared alarm</b> when an alarm is triggered, or both.

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

----End



## 2.10.3 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](#).

### Procedure

- 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**. The **Cloud Service Monitoring** page is displayed.
- Step 5** Locate the row that contains the target object and click **View Metric** to view the metric details of the object.

----End

## 2.10.4 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 2-14** 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 Audit

### 2.11.1 DDoS Mitigation Operations 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 2-15** lists DDoS Mitigation operations recorded by CTS.

**Table 2-15** DDoS Mitigation operations recorded by CTS

Operation	Resource Type	Trace Name
Updating alarm notification configuration	alarmConfig	updateAlarmConfig
Deleting alarm notification configuration	alarmConfig	deleteAlarmConfig


Operation	Resource Type	Trace Name
Creating a protection package	package	createPackage
Updating a protection package	package	updatePackage
Binding an IP address to a protection package	package	bindIpToPackage
Unbinding an IP address from a protection package	package	unbindIpToPackage
Deleting a protection package	package	DeletePackage
Creating a policy	policy	createPolicy
Updating a policy	policy	updatePolicy
Binding an IP address to a policy	policy	bindIpToPolicy
Unbinding an IP address from a policy	policy	unbindIpToPolicy
Configuring the blacklist or whitelist	policy	addblackWhitelplist
Removing a blacklisted or whitelisted item	policy	deleteblackWhitelplist
Deleting a policy	policy	deletePolicy
Configuring log groups and log streams	cnad	updateLogConfig
Disabling log groups and streams	cnad	deleteLogConfig
Updating the tag for a protected IP address	cnad	updateTagForIp

## 2.11.2 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.

### Procedure

**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