

DDoS Mitigation

User Guide

Issue 05
Date 2024-03-19



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

1 CNAD Basic (Anti-DDoS) User Guide.....	1
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 Configuring LTS for Anti-DDoS Logging.....	10
1.7 Adding a Tag.....	14
1.8 Viewing Monitoring Reports.....	15
1.9 Viewing Interception Reports.....	17
1.10 Audit.....	18
1.10.1 Anti-DDoS Operations That Can Be Recorded by CTS.....	18
1.10.2 Viewing CTS Traces.....	19
1.11 Permission Management.....	20
1.11.1 Creating a User Group and Assigning the Anti-DDoS Access Permission.....	20
1.11.2 Anti-DDoS Custom Policies.....	21
1.11.3 Anti-DDoS Permissions and Actions.....	22
2 CNAD Advanced Operation Guide.....	25
2.1 Usage Overview.....	25
2.2 Purchasing a CNAD Instance.....	26
2.3 Adding a Protection Policy.....	29
2.3.1 Configuring the Scrubbing Threshold.....	29
2.3.2 Watermarking.....	31
2.3.2.1 Configuring Watermark Protection.....	31
2.3.2.2 Watermark Configuration Guide.....	33
2.3.2.2.1 Working Principles.....	33
2.3.2.2.2 Development Example.....	33
2.3.3 Configuring an ACL.....	35
2.3.4 Configuring Port Blocking.....	38
2.3.5 Configuring Protocol Blocking.....	40
2.3.6 Configuring Fingerprint Filtering.....	42
2.3.7 Configuring Connection Protection.....	45
2.3.8 Configuring Geo-Blocking.....	47

2.4 Adding a Protected Object.....	48
2.5 Setting Alarm Notifications.....	50
2.6 Managing Protection Logs.....	51
2.6.1 Viewing Statistics Reports.....	51
2.7 Managing Instances.....	53
2.7.1 Viewing Information About an Instance.....	53
2.7.2 Configuring Instance Tags.....	54
2.8 Managing Protected Objects.....	55
2.8.1 Viewing Details about a Protected Object	55
2.8.2 Selecting a Protection Policy for a Protected Object.....	57
2.8.3 Deleting a Protected Object.....	58
2.9 Permissions Management.....	59
2.9.1 Creating a User and Granting the CNAD Pro Access Permission.....	59
2.9.2 CNAD Pro Custom Policies.....	61
2.9.3 CNAD Pro Permissions and Actions.....	61
2.10 Monitoring.....	66
2.10.1 Setting Event Alarm Notifications.....	66
2.10.2 Configuring Monitoring Alarm Rules.....	69
2.10.3 Viewing Monitoring Metrics.....	75
2.10.4 Metrics.....	75
2.11 Audit.....	77
2.11.1 DDoS Mitigation Operations Recorded By CTS.....	77
2.11.2 Viewing CTS Traces.....	78
3 Advanced Anti-DDoS User Guide.....	80
3.1 Usage Overview.....	80
3.2 Purchasing an AAD Instance.....	81
3.2.1 Purchasing AAD Instances.....	81
3.2.2 Purchasing an AAD Instance (International Edition).....	85
3.3 Connecting Services to AAD.....	88
3.3.1 Connecting Domain Name Website Services to Advanced Anti-DDoS.....	88
3.3.1.1 Website Service Access Process.....	88
3.3.1.2 Step 1: Configuring a Protected Domain Name (Website Services).....	89
3.3.1.3 Step 2: Adding the Back-to-Source IP Address Range to the Whitelist.....	99
3.3.1.4 Step 3: Locally Verifying the Website Service Configuration.....	101
3.3.1.5 Step 4: Modifying DNS Resolution.....	102
3.4 Configuring a Protection Policy.....	103
3.4.1 Configuring a Blacklist and a Whitelist.....	104
3.4.2 Configuring Protocol Blocking.....	106
3.4.3 Configuring Geo-Blocking.....	107
3.4.4 Configuring CC Attack Protection Rules.....	108
3.4.4.1 Configuring Frequency Control Rules.....	108
3.4.5 Enabling Basic Web Protection and CC Attack Protection.....	114

3.5 Enabling Alarm Notifications.....	115
3.6 Managing Instances.....	116
3.6.1 Viewing Information About an Instance.....	116
3.6.2 Upgrading Instance Specifications.....	118
3.6.3 Changing the Elastic Protection Bandwidth.....	119
3.6.4 Enabling Auto-renewal.....	120
3.6.5 Configuring Instance Tags.....	121
3.7 Managing Domain Names.....	122
3.7.1 Viewing Information About a Domain Name.....	123
3.7.2 Updating a Certificate.....	124
3.7.3 Modifying Resolution Lines for High-Defense IP Addresses of a Domain Name.....	126
3.7.4 Modifying Domain Name Configuration.....	128
3.7.5 Deleting a Domain Name.....	129
3.7.6 Configuring Field Forwarding.....	130
3.7.7 Modify TLS Configuration.....	131
3.8 Managing Protection Logs.....	133
3.8.1 Viewing Protection Details.....	133
3.9 Permissions Management.....	137
3.9.1 Creating a User and Granting the AAD Access Permission.....	137
3.9.2 Creating an AAD Custom Policy.....	138
3.9.3 AAD Permissions and Actions.....	139
3.10 Monitoring.....	141
3.10.1 Setting Event Alarm Notifications.....	141
3.10.2 Configuring Monitoring Alarm Rules.....	143
3.10.3 Viewing Monitoring Metrics.....	150
3.10.4 AAD Monitoring Metrics.....	150
3.11 Auditing.....	153
3.11.1 AAD Operations Supported by CTS.....	153
3.11.2 Viewing CTS Traces.....	153
4 Anti-DDoS Scheduling Center Protection Management.....	155
4.1 Purchasing Anti-DDoS Scheduling Center Protection.....	155
4.2 Configuring Tiered Scheduling Policies.....	157
4.3 Enabling Tiered Scheduling Alarm Notifications.....	160
4.4 Configuring CDN Scheduling Rules.....	161
A Change History.....	164

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 Setting a Protection Policy .
Enabling alarm notifications	After the alarm notification function is enabled, you will receive an alarm if a DDoS attack is detected. For details, see Enabling Alarm Notifications .
Setting event alarm notifications	Cloud Eye enables event monitoring for protected EIPs and generates alarms for scrubbing, blocking, and unblocking events. For details, see Setting Event Alarm Notifications .
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 Viewing Monitoring Reports .
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 Viewing Interception Reports .

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

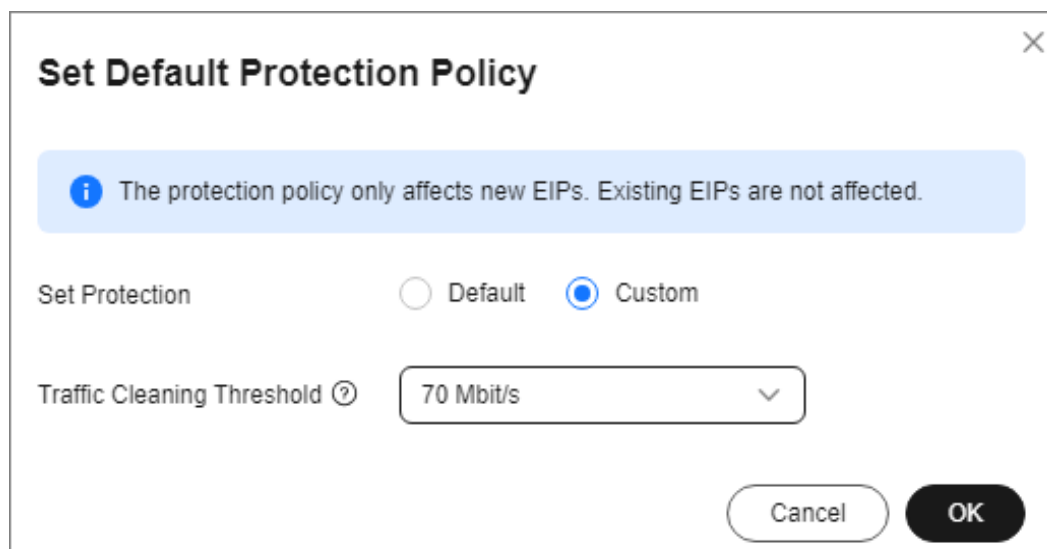
Step 1 Log in to the management console.

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



Set Default Protection Policy ✕

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

Set Protection Default Custom

Traffic Cleaning Threshold ? ▼

Cancel OK

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>NOTE</p> <ul style="list-style-type: none">• If service traffic triggers scrubbing, only attack traffic is intercepted. If service traffic does not trigger scrubbing, no traffic is intercepted.• Set this parameter based on the actual service access traffic.

Step 5 Click **OK**.


 **NOTE**

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

----End

Manually Setting a Protection Policy

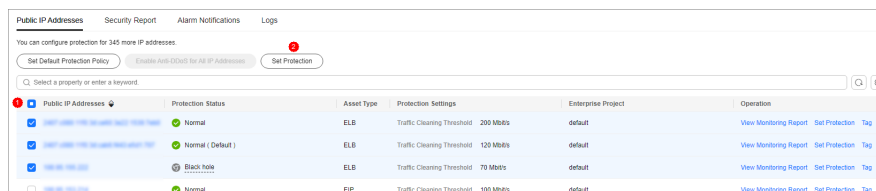
Step 1 Log in to the management console.

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.

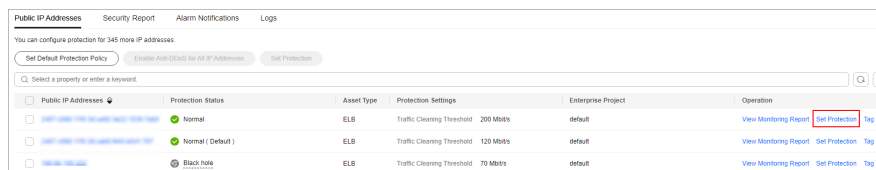
Step 3 On the **Public IP Addresses** tab page, select a setting method based on the site requirements.

- 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.

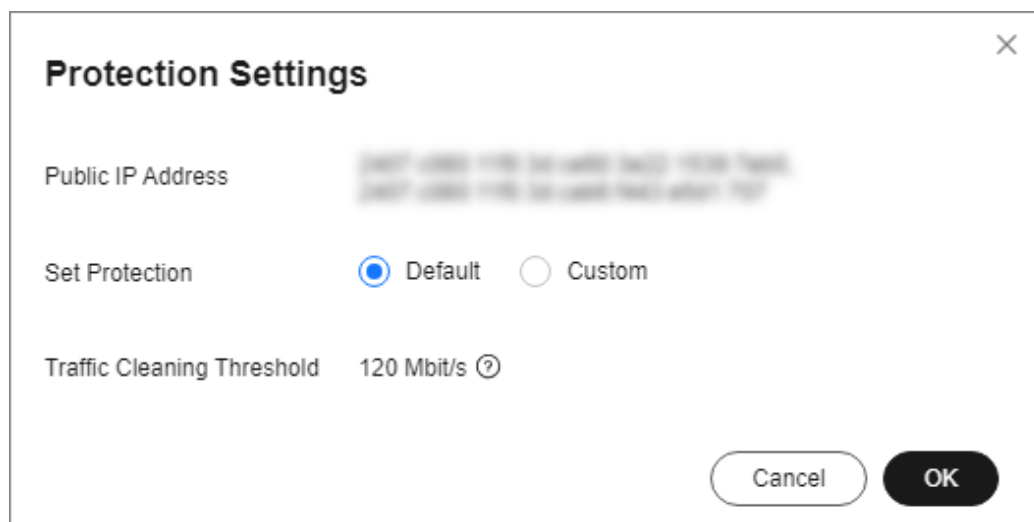
Figure 1-2 Configuring protection policies in batches



- 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 120 Mbit/s. You can manually set more protection levels.</p> <p>NOTE</p> <ul style="list-style-type: none">• If service traffic triggers scrubbing, only attack traffic is intercepted. If service traffic does not trigger scrubbing, no traffic is intercepted.• Set this parameter based on the actual service access traffic. You are advised to set a value closest to, but not exceeding, the purchased bandwidth.

Step 5 Then, click **OK**.

----End

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


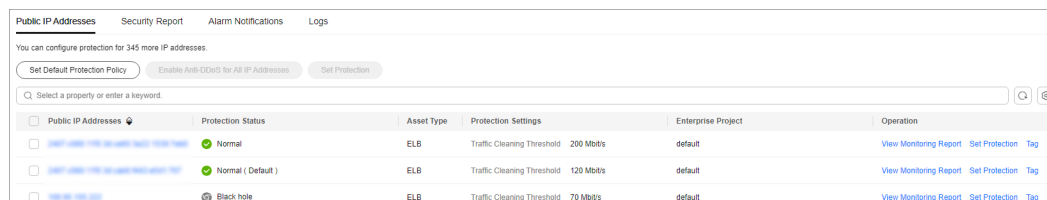
- Step 1** Log in to the management console.
- Step 2** Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS** page is displayed.
- Step 3** On the **Public IP Addresses** tab, view all protected 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"/> 192.168.1.100	Normal	ELB	Traffic Cleaning Threshold: 200 Mbit/s	default	View Monitoring Report Set Protection Tag
<input type="checkbox"/> 192.168.1.101	Normal (Default)	ELB	Traffic Cleaning Threshold: 120 Mbit/s	default	View Monitoring Report Set Protection Tag
<input type="checkbox"/> 192.168.1.102	Black hole	ELB	Traffic Cleaning Threshold: 70 Mbit/s	default	View Monitoring Report Set Protection Tag

NOTE



- Anti-DDoS provides protection for servers using IPv4 and IPv6 protocols against DDoS attacks.
- Click **Enable Anti-DDoS for All IP Addresses** to enable the protection for all unprotected IP addresses in the current region.
- After the default Anti-DDoS protection settings are enabled, traffic is scrubbed when its volume reaches 120 Mbit/s. You can modify Anti-DDoS protection settings according to [Setting a 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 NOTE If Anti-DDoS is enabled for a public IP address, you can click the IP address to go to its Monitoring Report page.
Protection Status	Protection status of a public IP address. The values are: <ul style="list-style-type: none">• Normal• Configuring• Disabled• Cleaning• Black hole
Asset Type	<ul style="list-style-type: none">• EIP• ELB• NetInterFace• Virtual Private Network (VPN)• NAT Gateway• VIP: HA virtual IP address.• Cloud Container Instance (CCI)• SubEni
Protection Settings	Traffic scrubbing threshold of the current public IP address.
Enterprise Project	Enterprise project to which the current public IP address belongs.

----End

1.4 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.


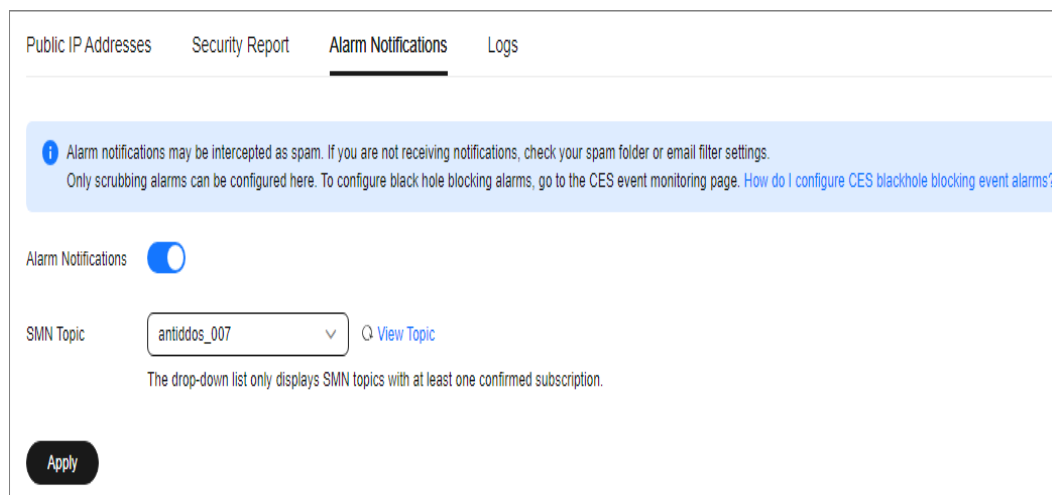


- Step 2** Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS** page is displayed.
- Step 3** On the **Anti-DDoS** page, click the **Alarm Notifications** tab and configure the alarm notification. 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"> : enabled : disabled
SMN Topic	You can select an existing topic or click View Topic to create a topic. For more information about SMN topics, see Simple Message Notification User Guide .

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

----End

1.5 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**.

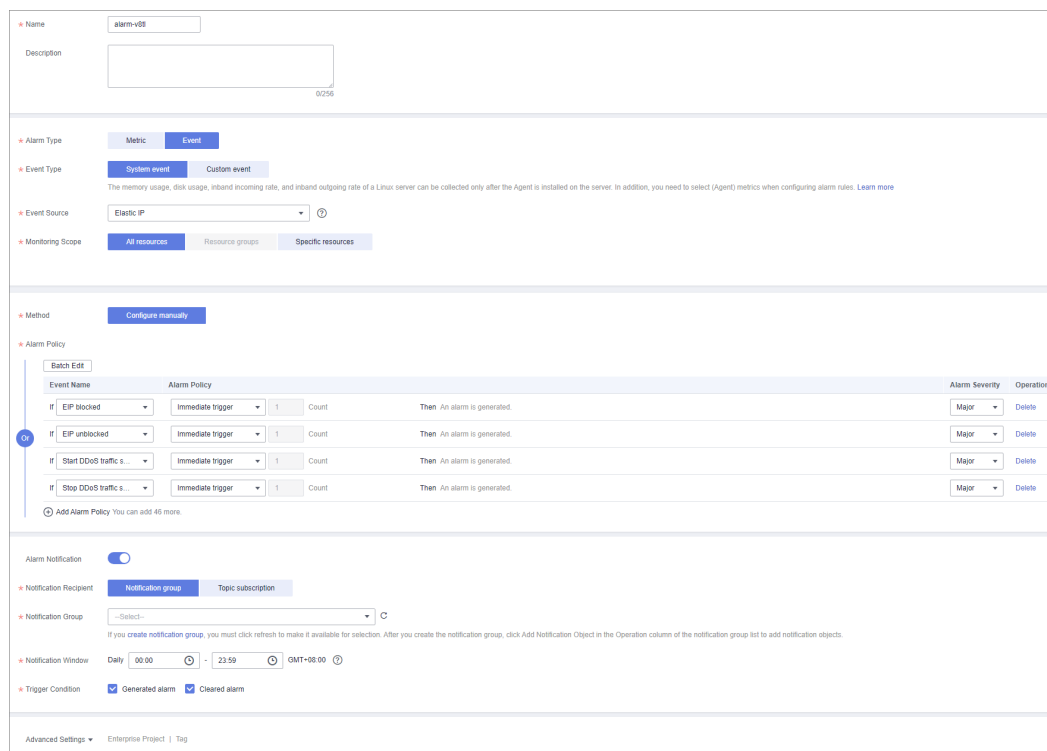
Step 4 Select a monitoring method based on the site requirements.

- 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



Name: alarm-v88

Description:

Alarm Type: Metric | **Event**

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

Event Source: Elastic IP

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

Method: **Configure manually**

Alarm Policy

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:

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

Notification Group: -Select-

Notification Window: Daily 00:00 - 23:59 GMT+08:00

Trigger Condition: Generated alarm Cleared alarm

Advanced Settings: Enterprise Project | Tag

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 Event .
Event Type	Choose System Event .
Event Source	Choose Elastic IP .
Monitoring Scope	Specifies the resource scope to which the alarm rule applies. Set this parameter as required.
Method	The default option is Configure manually .
Alarm Policy	You are advised to select EIP blocked, EIP unblocked, Start Anti-DDoS traffic scrubbing, and Stop Anti-DDoS traffic scrubbing . When the traffic is greater than 10,000 kbit/s, the system sends an alarm notification when scrubbing starts and when scrubbing ends. When the traffic is less than 10,000 kbit/s, no alarm notification is sent.
Notification Recipient	Select Notification group or Topic subscription .
Notification Group	Select the required notification group.
Notification Object	Select the required topic subscription.
Notification Window	Set this parameter as required.
Trigger Condition	Choose Generated alarm and Cleared alarm .

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 Notification group or Topic subscription as required.
Notification Group	This parameter takes effect when Notification Recipient is set to Notification group . Set this parameter based on the site requirements.
Notification Object	This parameter is valid only when Notification Recipient is set to Topic Subscription . 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 Configuring LTS for Anti-DDoS Logging

Scenario


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

Prerequisites

You have enabled LTS.

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 **Configure Logs** tab, enable LTS (), and select a log group and log stream. [Table 1-8](#) describes the parameters.

Figure 1-8 Configuring logs

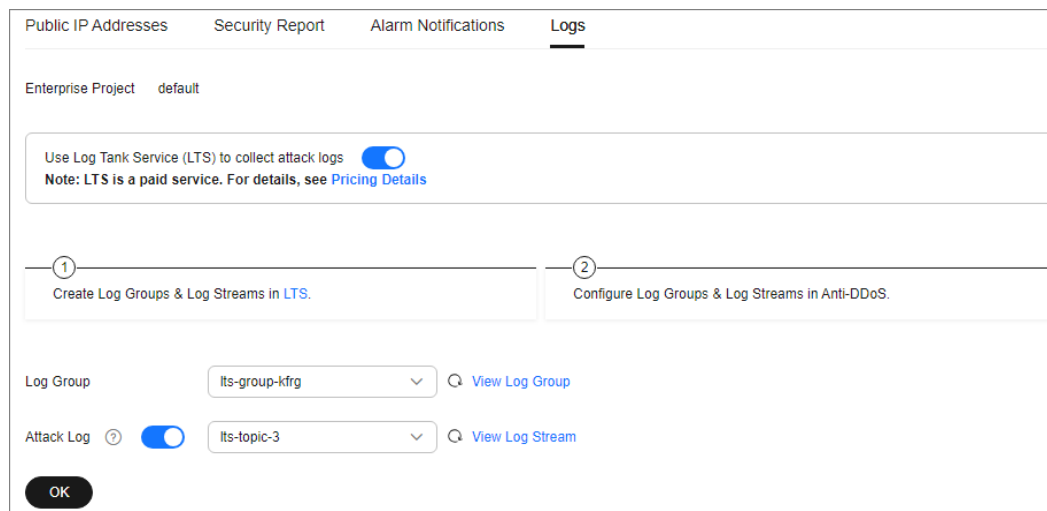


Table 1-8 Log configuration

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

Step 4 Click **OK**.

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

----End

Log Fields in LTS

The following table describes the log fields.

Table 1-9 Log field description

Field	Description
logType	Log type. The default value is ip_attack_sum , indicating attack logs.
deviceType	Type of the device that reports logs. The default value is CLEAN , indicating the scrubbing device.

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

Table 1-10 Attack type description

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

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

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

1.7 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


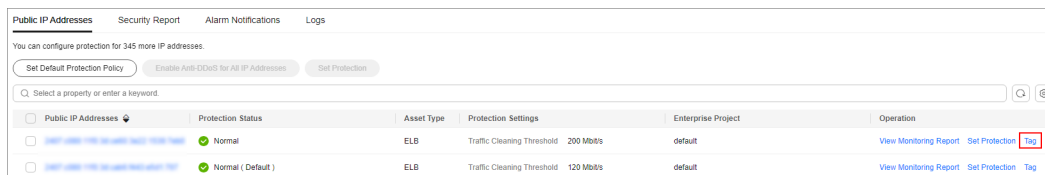
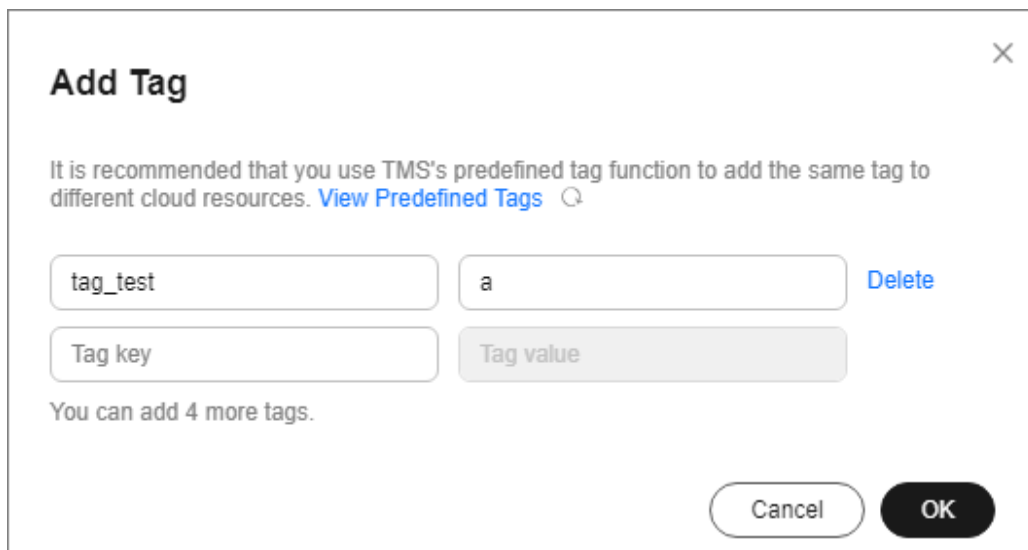
- Step 1** [Log in to the management console.](#)
- Step 2** Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.
- Step 3** Click the **Public IP Addresses** tab.
- Step 4** Locate the row that contains the public IP address for which you want to set a tag, click **Tag**.

Figure 1-9 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 1-10 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


1.8 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.

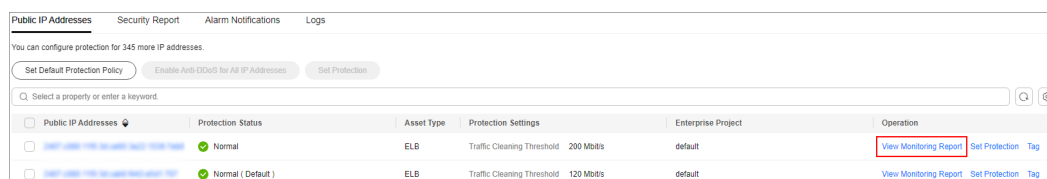
Procedure

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 1-11 Viewing a monitoring report



Public IP Addresses	Protection Status	Asset Type	Protection Settings	Enterprise Project	Operation
<input type="checkbox"/> 100.100.100.100	Normal	ELB	Traffic Cleaning Threshold 200 Mbit/s	default	View Monitoring Report Set Protection Tag
<input type="checkbox"/> 100.100.100.100	Normal (Default)	ELB	Traffic Cleaning Threshold 120 Mbit/s	default	View Monitoring Report Set Protection Tag

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

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

Figure 1-12 Viewing a traffic monitoring report

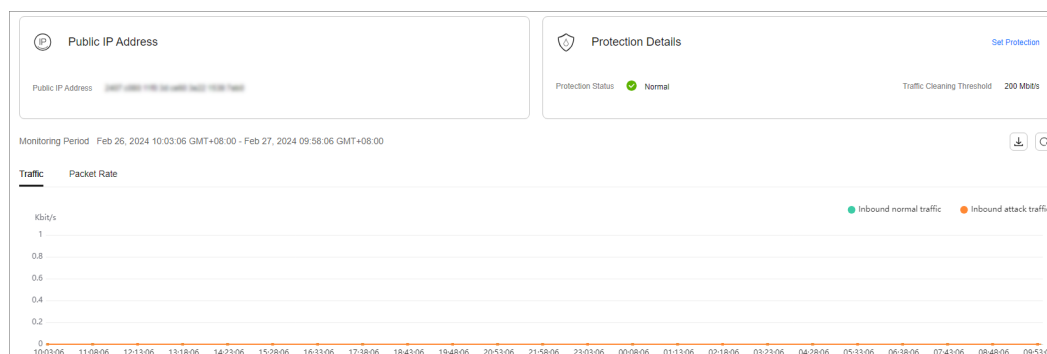
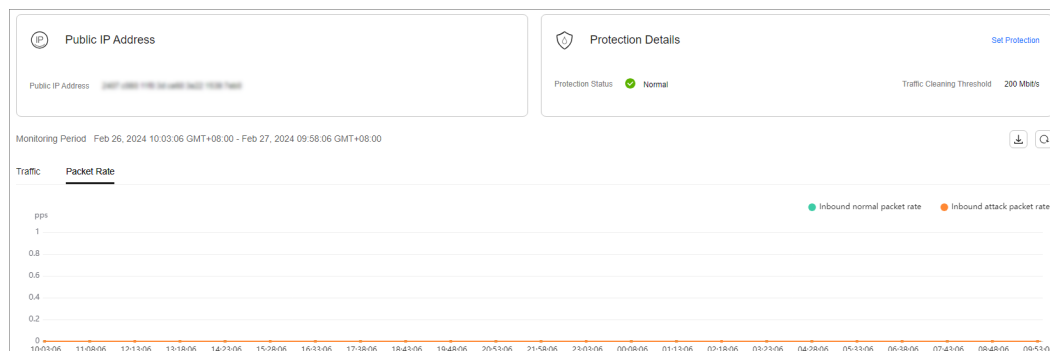







Figure 1-13 Viewing a packet rate monitoring report**NOTE**

- 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

1.9 Viewing Interception Reports

Scenarios

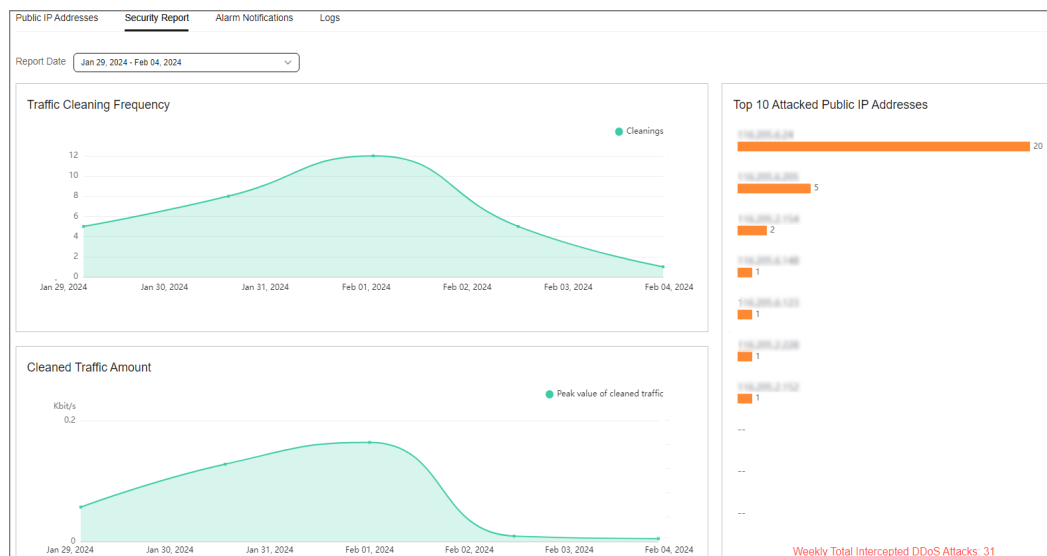
This section describes how to view the protection statistics, including the traffic cleaning frequency, cleaned traffic amount, weekly top 10 attacked public IP addresses, and total number of intercepted attacks of all public IP addresses of a user.

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 1-14 Viewing an interception report



 **NOTE**

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

-----End

1.10 Audit

1.10.1 Anti-DDoS Operations That Can Be Recorded by CTS

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

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

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

Operation	Trace Name
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

1.10.2 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

1.11 Permission Management

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

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

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

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

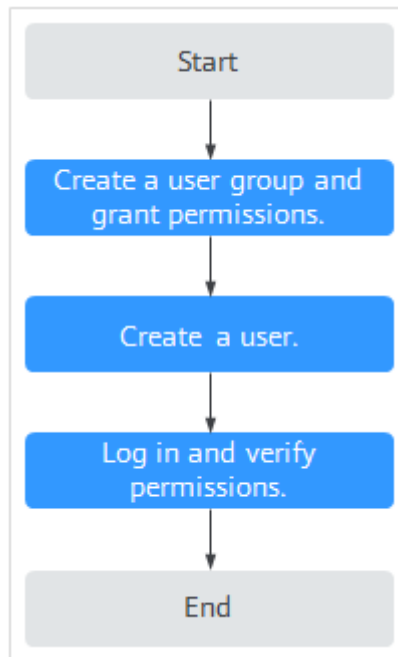
This section describes the procedure for granting permissions (see [Figure 1-15](#)).

Prerequisites

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

Process

Figure 1-15 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** policy to the group.

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

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

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

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

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

1.11.2 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"
      ]
    }
  ]
}
```

1.11.3 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	-

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

Permission	Action	Dependency
Batch creating tags	anti-ddos:ip:tagResource	-
Batch deleting tags	anti-ddos:ip:untagResource	-

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 Purchasing a CNAD Instance .
Configuring protection policies	CNAD provides a wide range of protection rules. You can configure protection policies based on your service requirements. For details, see Adding a Protection Policy .
Adding a protected object	You can add public IP addresses on Huawei Cloud as protected objects to enable CNAD for them. For details, see Adding a Protected Object .
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 Setting Alarm Notifications .
Viewing statistics report	You can view the access and attack statistics of last three days. For details, see Viewing Statistics Reports .
Managing instances	Perform common instance management operations, such as enabling renewal, upgrading specifications, and configuring labels. For details, see Managing Instances .

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 Setting Event Alarm Notifications .

2.2 Purchasing a CNAD Instance

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

CNAD has two editions: CNAD Unlimited Protection Basic and CNAD Unlimited Protection Advanced. You can choose an edition based on your service requirements. For details about the specifications of each edition, see [Functions](#).

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

The screenshot displays the configuration interface for a DDoS mitigation instance. The 'Instance Type' is set to 'Native DDoS protection'. The 'Billing Mode' is 'Yearly/Monthly'. The 'Protection Level' is 'Unlimited Protection Basic Edition', with a note that it provides unlimited protection for Cloud EIPs and native networks, and that exclusive WAF must be used. The 'Specifications' section lists: Access Mode: Transparent proxy; Bandwidth Type: Cloud native network and fully dynamic BGP (static BGP not supported); Protection Capability: Unlimited protection; and Protected Resources: Public IP addresses of cloud resources, including ECS, ELB, and EIP. The 'IP Version' is set to 'IPv4 and IPv6'. The 'Resource Location' is 'CN North-Beijing4'. The 'Protected IP Addresses' are set to 50. The 'Service Bandwidth' is set to 100 Mbit/s.

Table 2-2 Specifications of the Unlimited Protection Basic edition

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

Step 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.

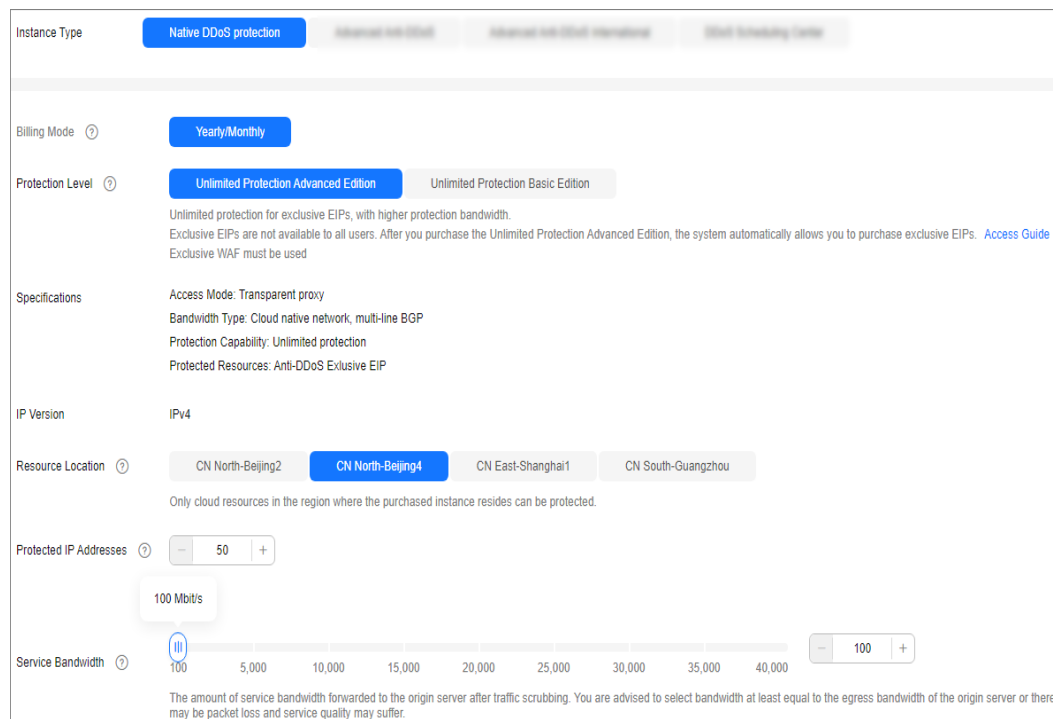
Step 3 In the upper right corner of the page, click **Buy CNAD Pro**.

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. The settings are as follows:

- Instance Type:** Native DDoS protection (selected)
- Billing Mode:** Yearly/Monthly (selected)
- Protection Level:** Unlimited Protection Advanced Edition (selected). Description: Unlimited protection for exclusive EIPs, with higher protection bandwidth. Exclusive EIPs are not available to all users. After you purchase the Unlimited Protection Advanced Edition, the system automatically allows you to purchase exclusive EIPs. Access Guide. Exclusive WAF must be used.
- 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 (selected). Note: Only cloud resources in the region where the purchased instance resides can be protected.
- Protected IP Addresses:** 50 (value in input field)
- Service Bandwidth:** 100 Mbit/s (value in input field). Scale: 100, 5,000, 10,000, 15,000, 20,000, 25,000, 30,000, 35,000, 40,000. Note: The amount of service bandwidth forwarded to the origin server after traffic scrubbing. You are advised to select bandwidth at least equal to the egress bandwidth of the origin server or there may be packet loss and service quality may suffer.

Table 2-3 Specifications of the Unlimited Protection Advanced edition

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

Step 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](#).


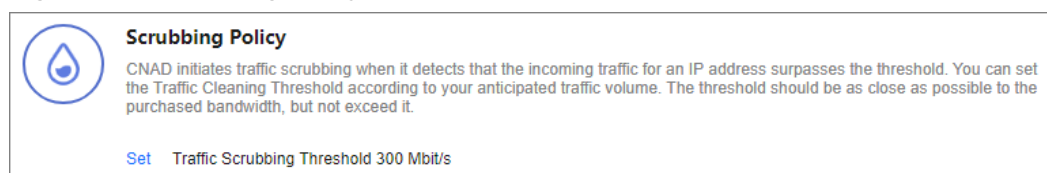
- Step 2** Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.
- Step 3** In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced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



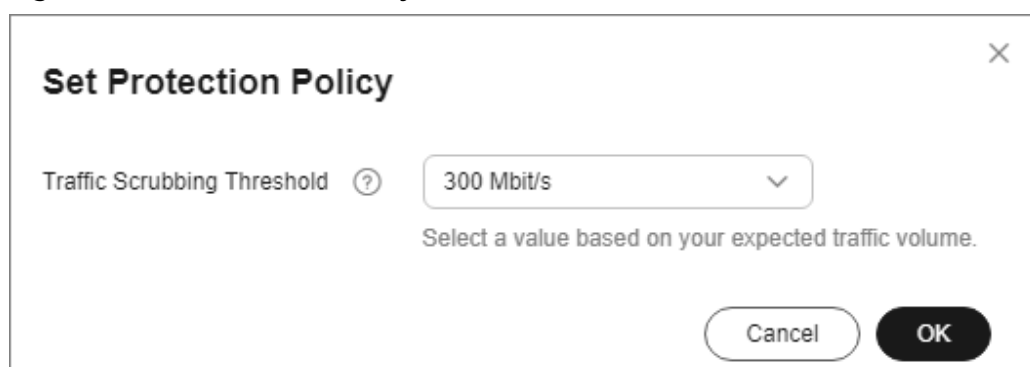
- Step 6** In the row containing the target policy, click **Set Protection Policy** in the **Operation** column.
- Step 7** In the **Scrubbing Policy** area, click **Set**.

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



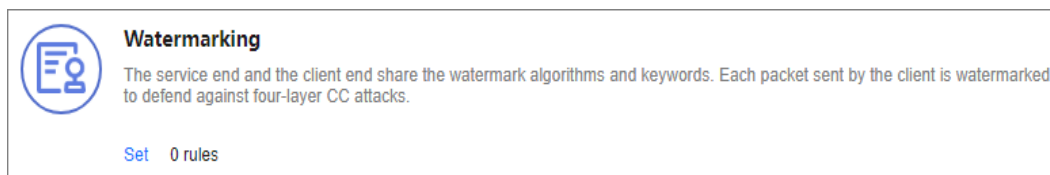
Create Protection Policy ✕

Name

Instance

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

Step 7 In the **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

Create Watermark [Close]

* Watermark Name: 1 - 32

* Protocol: UDP

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

* Port Range: 1 - 65535 - 1 - 65535

Cancel OK

Table 2-4 Watermark parameters

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

Step 10 Click **OK**.

NOTE

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

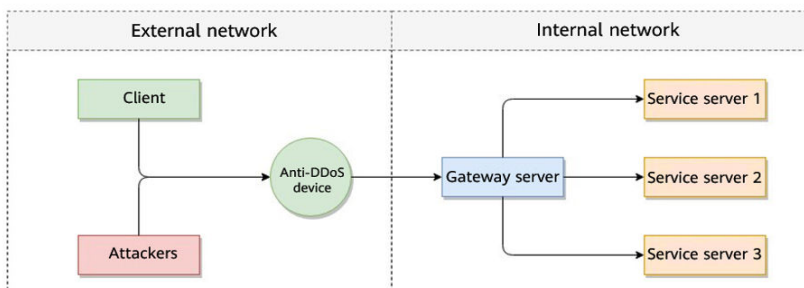
----End

2.3.2.2 Watermark Configuration Guide

2.3.2.2.1 Working Principles

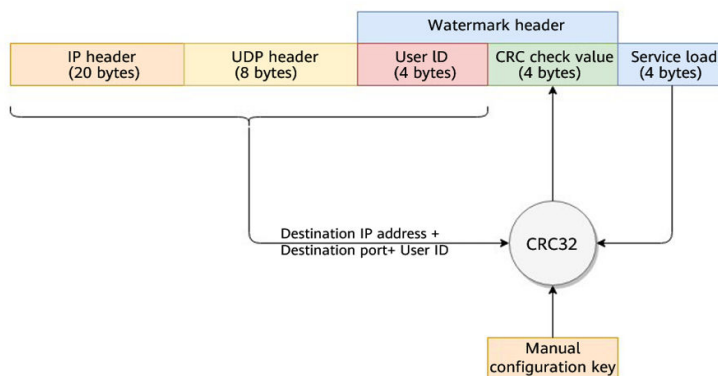
There are generally two modes of defending against UDP floods: dynamic fingerprint learning and UDP traffic limiting. The former may mistakenly learn normal service payloads as attack fingerprints, leading to false positives. The latter may block both normal and attack traffic, affecting your service.

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

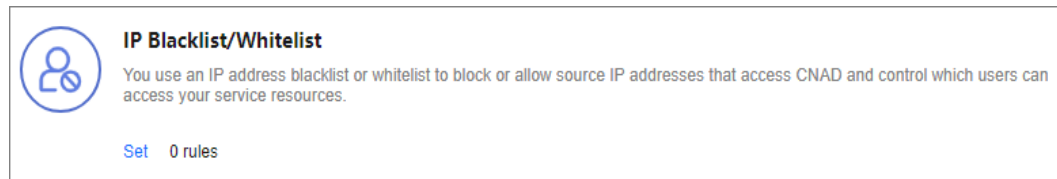


The screenshot shows a dialog box titled "Create Protection Policy". It has a close button (X) in the top right corner. The dialog contains two input fields: "Name" with the value "test" and "Instance" with a dropdown menu showing "CNAD-9cb4". At the bottom right, there are two buttons: "Cancel" and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

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

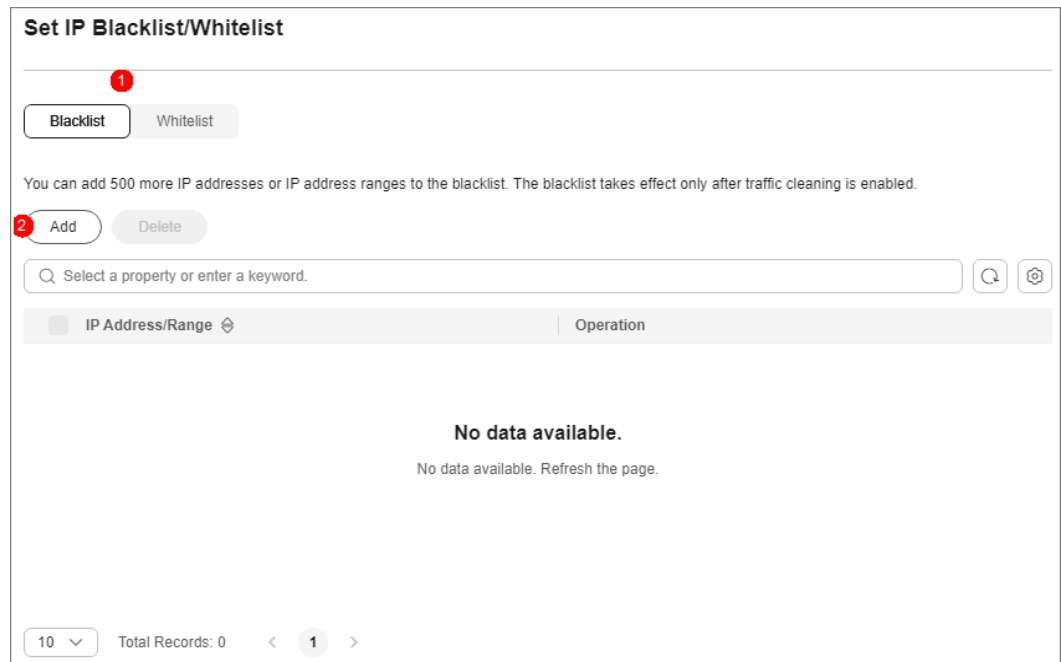
Step 7 In the **IP Blacklist/Whitelist** area, click **Set**.

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

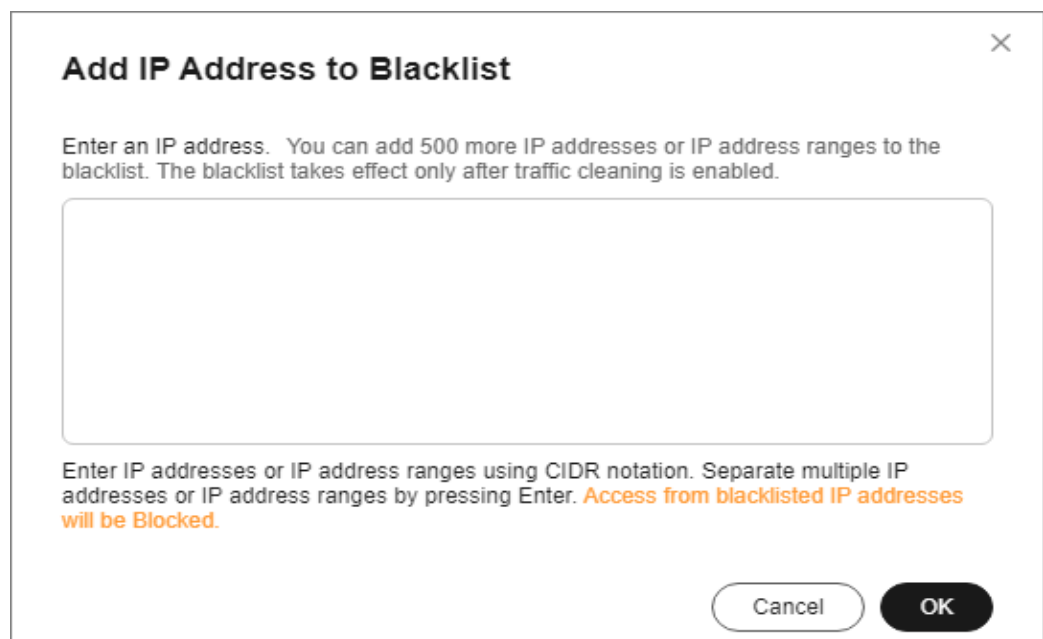


Figure 2-17 Adding whitelist IP addresses

Add IP Address to Whitelist

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

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

Cancel OK

----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



Create Protection Policy

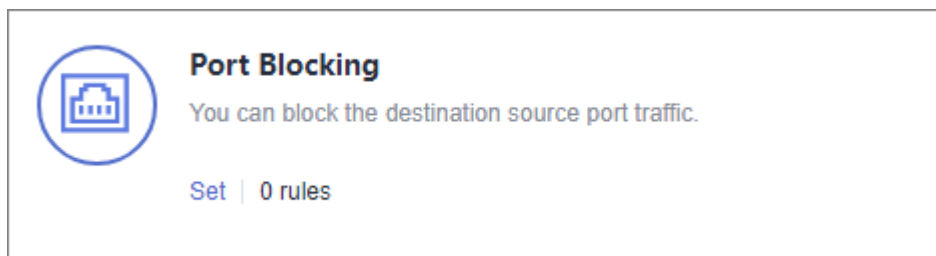
Name

Instance

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

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

Figure 2-19 Port blocking configuration box



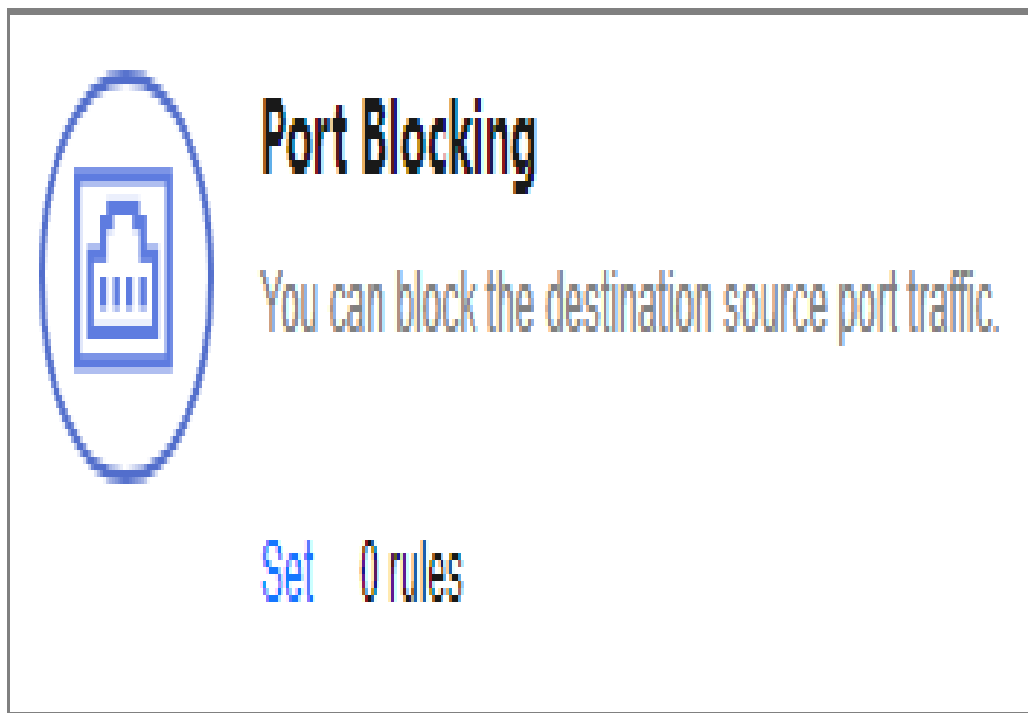
Port Blocking

You can block the destination source port traffic.

[Set](#) | 0 rules

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

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

Figure 2-20 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
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



Create Protection Policy

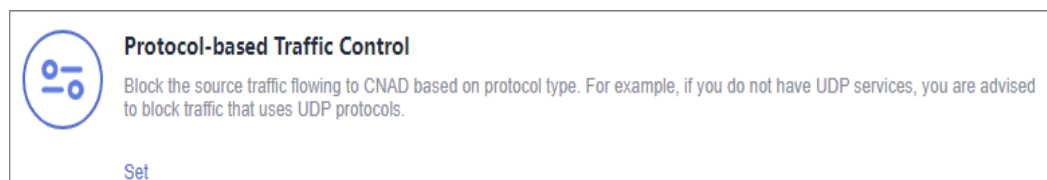
Name


Instance

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

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

Figure 2-22 Protocol-based Traffic Control

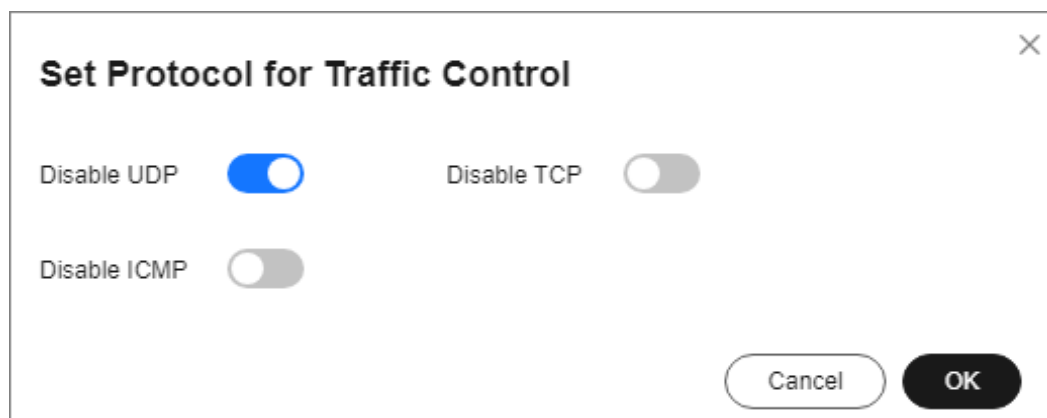




 **Protocol-based Traffic Control**

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

[Set](#)

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



Create Protection Policy [X]


Name

Instance

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



 **Fingerprint Filtering**

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

[Set](#) 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

Create Fingerprint [X]

* Fingerprint name: 1 - 32

* Protocol: UDP

Start Source Port - End Source Port: 1 - 65535 - 1 - 65535

Destination Source Port - End Destination Port: 1 - 65535 - 1 - 65535

* Action ⓘ: Discarded

* Test Load ⓘ: 2 - 128 * Offset: 0 - 1500 Check Depth ⓘ: 1 - 1500 [⊕]

Cancel OK

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 Discard or Allow .
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](#).

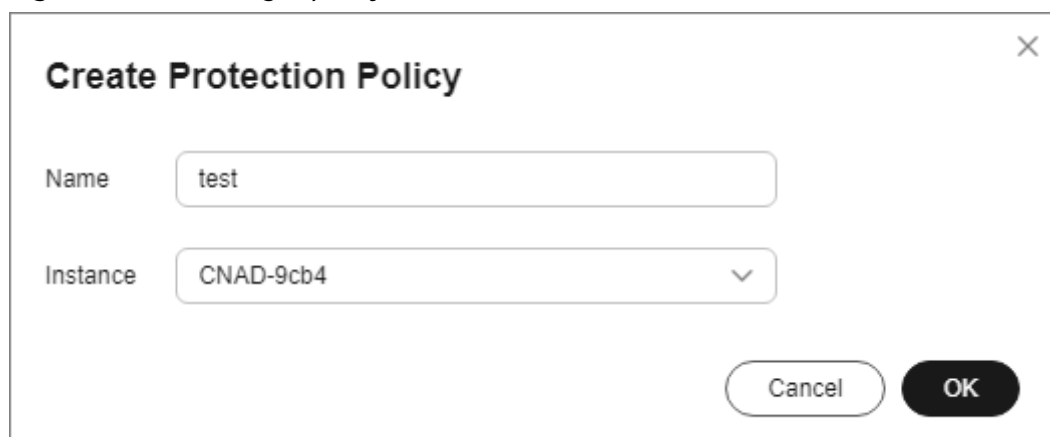
Step 2 Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

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 ×

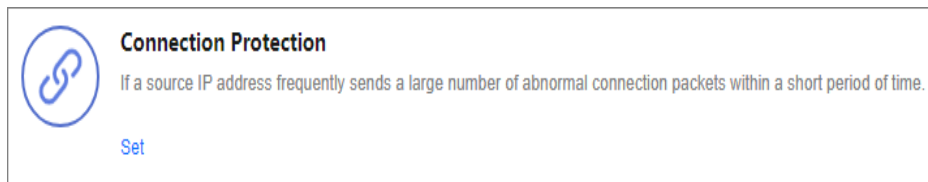
Name

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

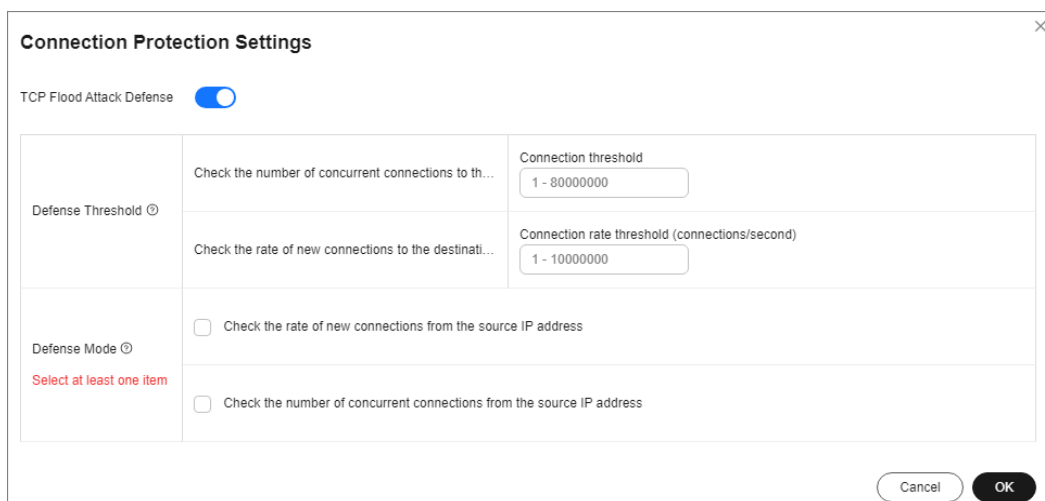


Table 2-7 Parameter description

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 Threshold , 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 Threshold , 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 Check Cycle exceeds Threshold , 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 Threshold , 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



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 **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.

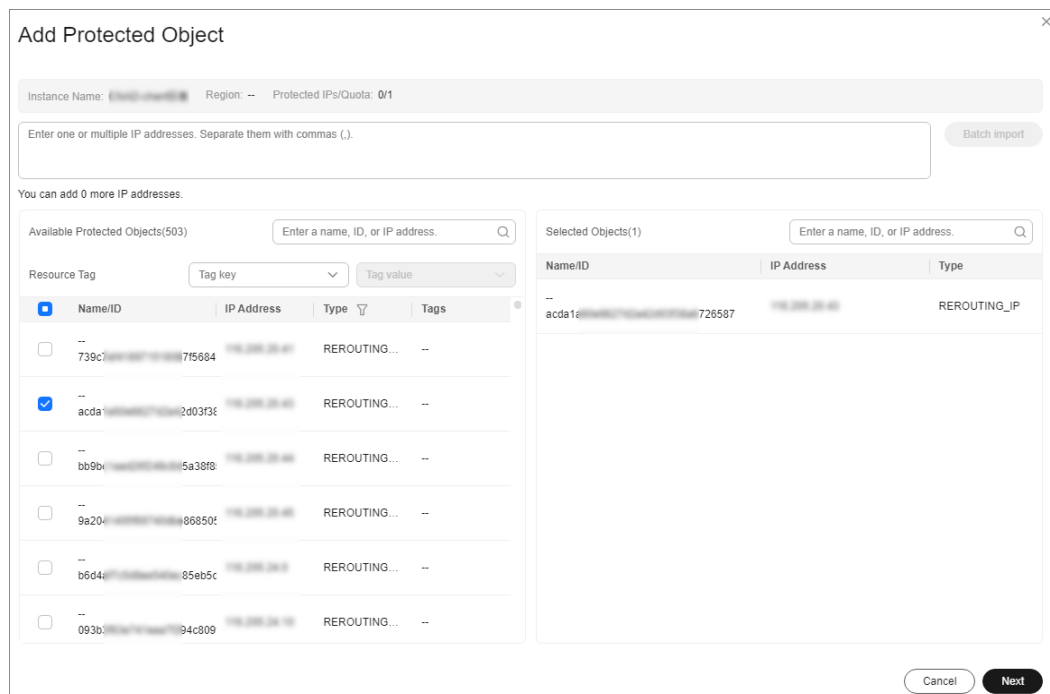
Step 2 Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

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

Dialog box titled "Add Protected Object" with a close button (X) in the top right corner.

Deleted IP addresses: 0 [Show](#)

Added IP addresses: 1 [Hide](#)

Name/ID	IP Address	Type
...
b56...	2290	REROUTING_IP

* Select a Protection Policy (Only for New IP Addresses) [Create Protection Policy](#)

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


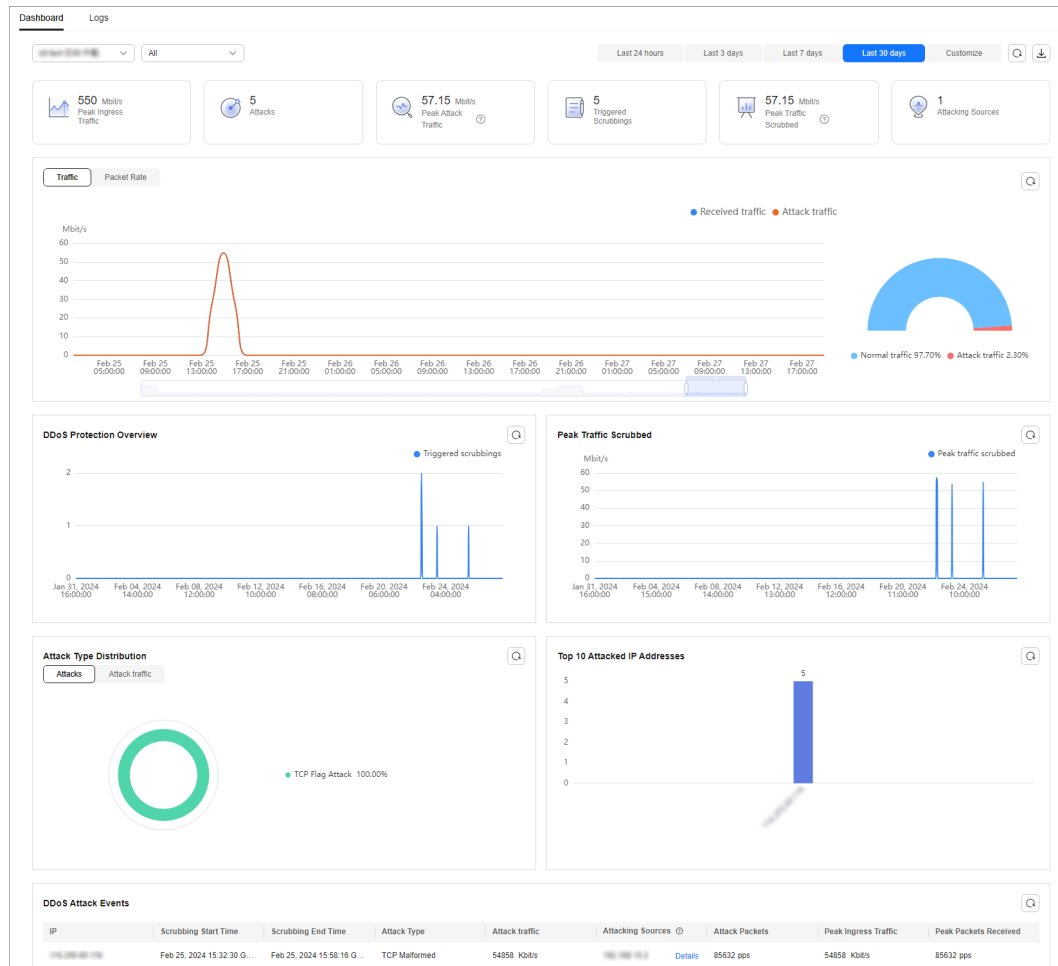
- Step 1** [Log in to the management console.](#)
- Step 2** Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.
- Step 3** In the navigation pane on the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

Figure 2-36 Dashboard

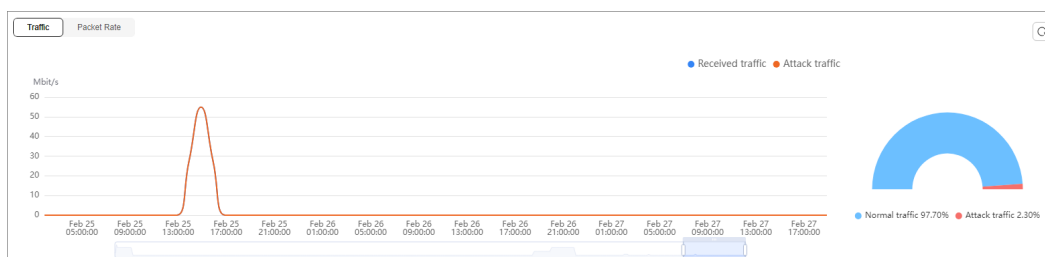



NOTE

- 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.

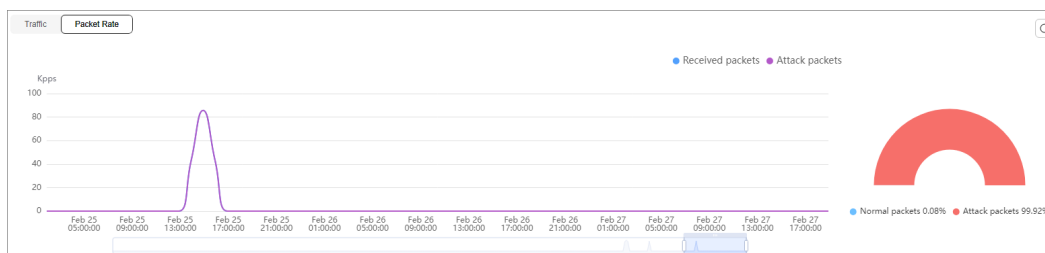
Figure 2-37 Traffic




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

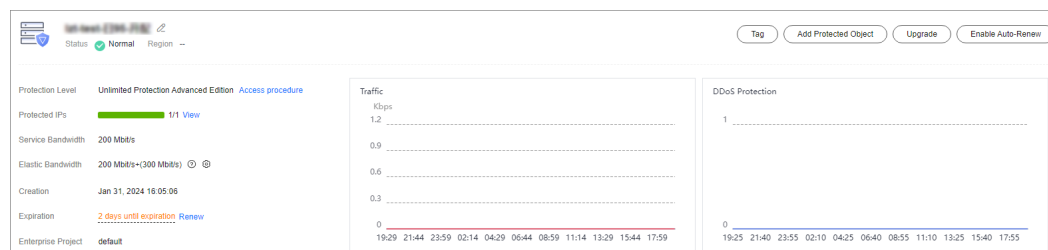
Step 1 [Log in to the management console.](#)

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.

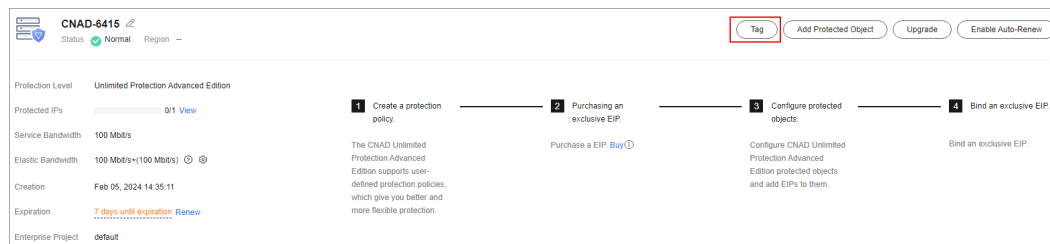
Procedure

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.

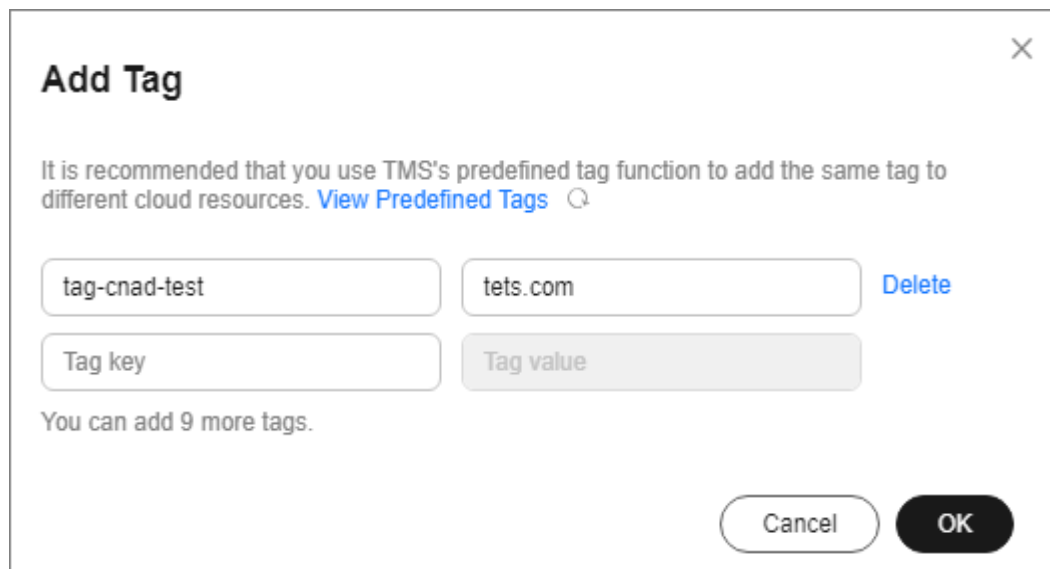
Step 4 In the row containing the target instance, click **Set Tag**.

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.

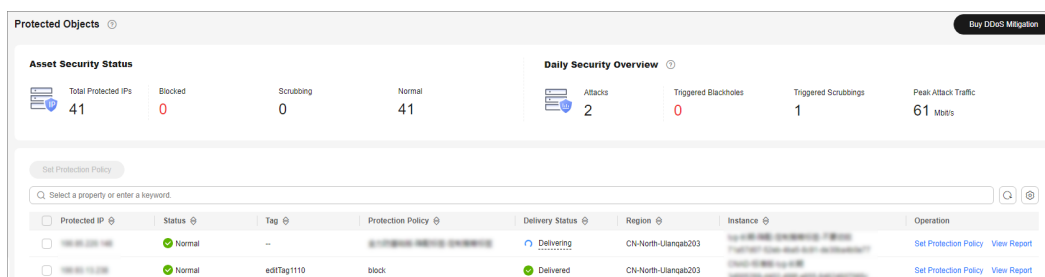
Procedure

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"> Normal Delivering
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"> You can click View Report to go to the Dashboard tab and view protection data. If no protection policy has been configured for a protected IP address, you can click Set Protection Policy to select a protection policy for the IP address.

----End

2.8.2 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.

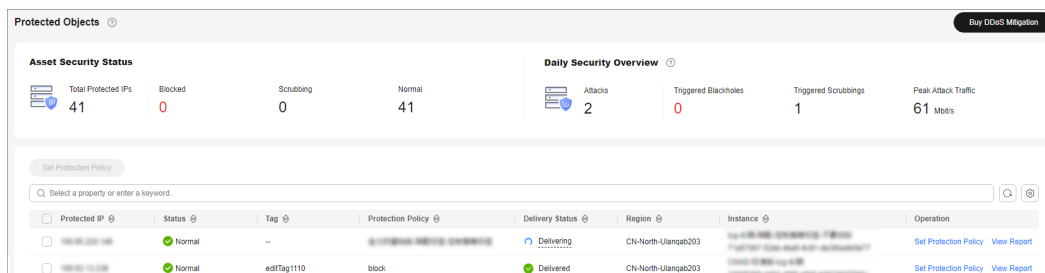
Procedure

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.

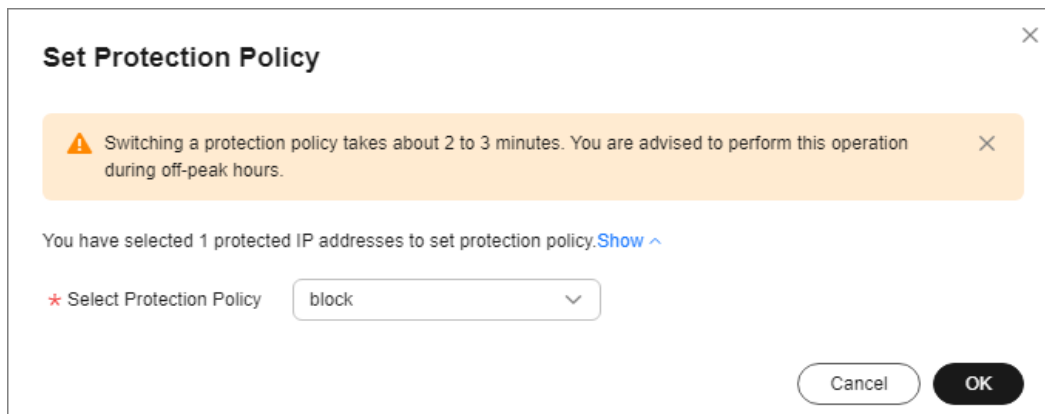
Figure 2-43 Protected objects



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

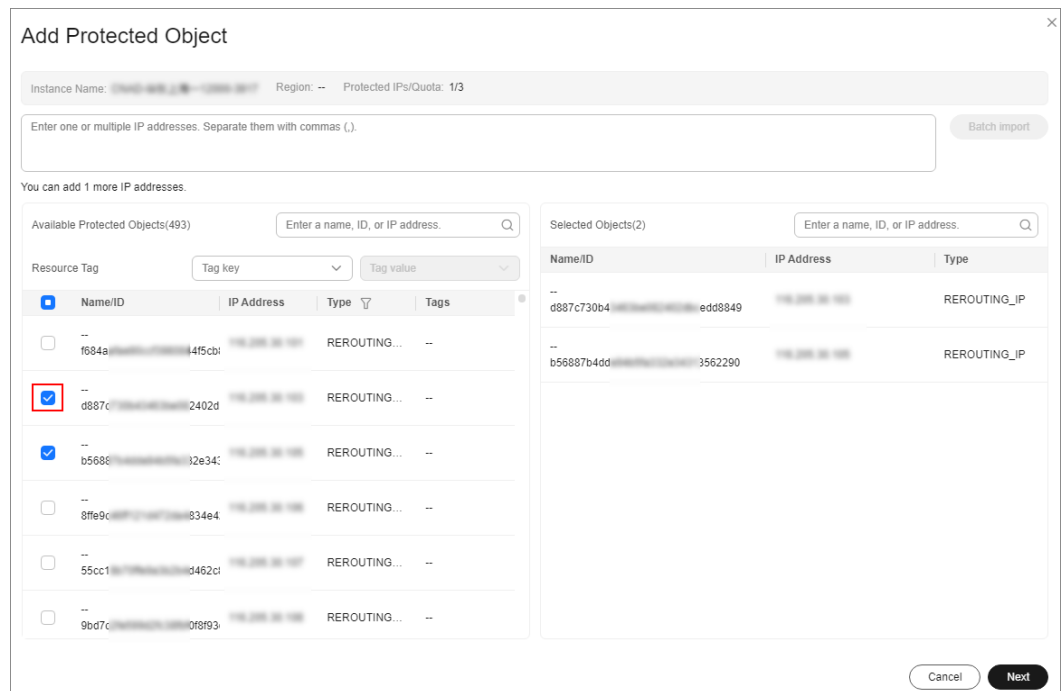
Step 1 [Log in to the management console](#).

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.

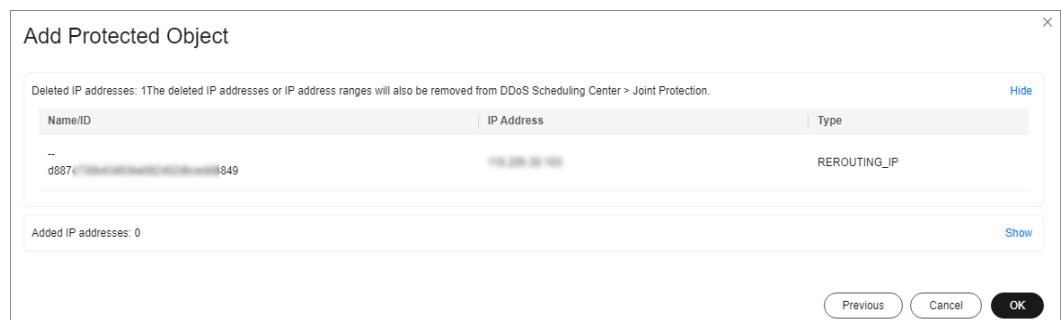
Step 3 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced > Instances**. The **Instances** page is displayed.

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

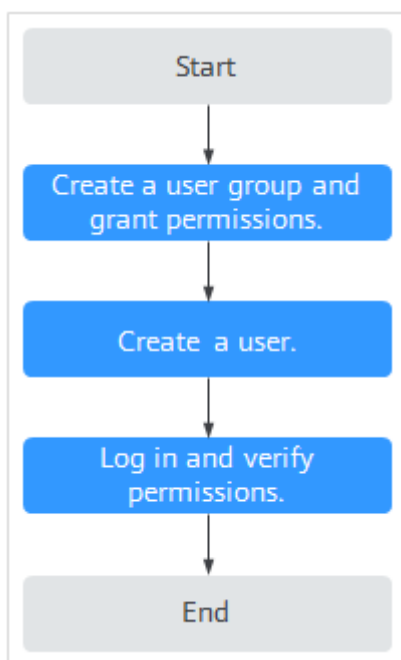
You can use **Identity and Access Management (IAM)** for refined permissions control for CNAD Pro resources. To be specific, you can:

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


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

Process

Figure 2-47 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 permissions management. If your Huawei Cloud account does not need individual IAM users, skip this section.

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

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

Supported Actions

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

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

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

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

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 cnad:protectedIp:create permission and the vpc:publicIps:list 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 CN-Hong Kong. To grant a user the permission for binding objects to a CNAD Pro instance, you need to grant both the cnad:protectedIp:create permission, and the vpc:publicIps:list permission configured for CN-Hong Kong so that the user can only perform operations on the protected objects in CN-Hong Kong.</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	To grant a user the permission for purchasing CNAD Pro, you need to grant the cnad:package:create permission to the user and the following BSS permissions configured for all regions: <ul style="list-style-type: none">• bss:order:update Order Operation• bss:contract:update Contract Modification• bss:balance:view Account Querying• bss:order:pay Payment

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 2-9](#).

Figure 2-48 Alarm parameters

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

- Name:** alarm-v01
- Description:** (Empty text area)
- Alarm Type:** Metric / **Event**
- Event Type:** System event / Custom event
- Event Source:** Elastic IP
- Monitoring Scope:** All Resources / Resource groups / Specific resources
- Method:** Configure manually
- Alarm Policy:** A table with columns: Event Name, Alarm Policy, Alarm Severity, Operation. It contains four rows for 'EIP blocked', 'EIP unblocked', 'Start DDoS traffic', and 'Stop DDoS traffic', all with 'Immediate trigger' and 'Count' metrics.
- Alarm Notification:** Enabled (toggle)
- Notification Recipient:** Notification group / Topic subscription
- Notification Group:** --Select--
- Notification Window:** Daily 00:00 - 23:59 GMT+08:00
- Trigger Condition:** Generated alarm, Cleared alarm

Table 2-9 Parameters for configuring a protection policy

Parameter	Description
Name	Name of the rule. The system generates a random name and you can modify it.
Description	Description about the rule.
Alarm Type	Select Event .
Event Type	Choose System Event .
Event Source	Choose Elastic IP .

Parameter	Description
Monitoring Scope	Specifies the resource scope to which the alarm rule applies. Set this parameter as required.
Method	The default option is Configure manually .
Alarm Policy	You are advised to select EIP blocked, EIP unblocked, Start Anti-DDoS traffic scrubbing, and Stop Anti-DDoS traffic scrubbing . When the traffic is greater than 10,000 kbit/s, the system sends an alarm notification when scrubbing starts and when scrubbing ends. When the traffic is less than 10,000 kbit/s, no alarm notification is sent.
Notification Recipient	Select Notification group or Topic subscription .
Notification Group	Select the required notification group.
Notification Object	Select the required topic subscription.
Notification Window	Set this parameter as required.
Trigger Condition	Choose Generated alarm and Cleared alarm .

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 2-10 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 Notification group or Topic subscription as required.
Notification Group	This parameter takes effect when Notification Recipient is set to Notification group . Set this parameter based on the site requirements.

Parameter	Description
Notification Object	This parameter is valid only when Notification Recipient is set to Topic Subscription . 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 2-11](#).

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.
- Alarm Type:** Two tabs, 'Metric' (selected) and 'Event'.
- Resource Type:** A dropdown menu set to 'DDoS'.
- Dimension:** A dropdown menu set to 'Package'.
- Monitoring Scope:** Two tabs, 'All resources' (selected) and 'Specific resources'.
- Method:** Three tabs: 'Associate template' (selected), 'Use existing template', and 'Configure manually'.
- Template:** A dropdown menu set to '--Select--' with a 'Create Custom Template' link.
- Alarm Notification:** A toggle switch that is turned on.
- Notification Recipient:** Two tabs: 'Notification group' (selected) and 'Topic subscription'.
- 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 2-11 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 DDoS from the drop-down list box.
Dimension	Select the resource dimension to be monitored. <ul style="list-style-type: none"> Package: instance dimension Protected IP Address: IP address dimension
Monitoring Scope	Scope where the alarm rule applies to. You can select All resources , Resource groups or Specific resources .

Parameter	Description
Method	You can select Associate template , Use existing template , or Configure manually . For details about how to create a custom template, see Creating a Custom Template . NOTE After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.
Template	Select a template.
Alarm Notification	Whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message.
Notification Recipient	Specifies the receiving method of the alarm notification. You can select Notification group or Topic subscription . <ul style="list-style-type: none">Account contact is the mobile phone number and email address provided for registration.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 Creating a Topic and Adding Subscriptions.
Notification Group (Valid when Notification Recipient is set to Notification group)	Select the group to be notified.
Topic subscription (Valid when Notification Recipient is set to Topic subscription)	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 Generated alarm when an alarm is generated or Cleared alarm 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



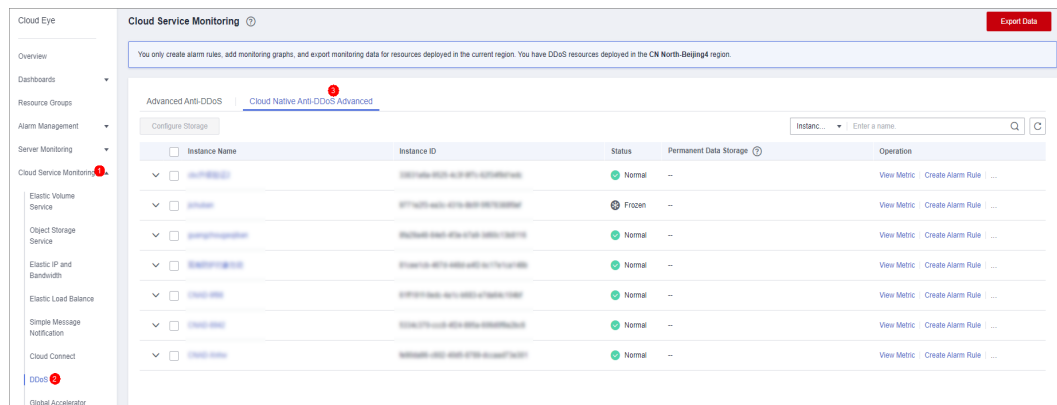
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the displayed page to select a region.
- Step 3** Hover your mouse over  in the upper left corner of the page and choose **Management & Governance > Cloud Eye**.
- Step 4** Choose **Cloud Service Monitoring > DDoS**. 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 2-12](#).

Figure 2-51 Configuring monitoring alarm rules

The screenshot shows a configuration page for monitoring alarm rules. The fields are as follows:

- Name: alarm-p0ta
- Description: (empty text box, 0/256 characters)
- Alarm Type: Metric
- Resource Type: DDoS
- Dimension: Package
- Monitoring Scope: Specific resources
- Monitored Objects: jichuban
- Method: Associate template (selected), Use existing template, Configure manually
- Template: --Select-- (dropdown), Create Custom Template
- Alarm Notification: (checked)
- Notification Recipient: Notification group (selected), Topic subscription
- Notification Group: --Select-- (dropdown)
- Notification Window: Daily, 00:00 - 23:59 GMT+08:00
- Trigger Condition: (checked) Generated alarm, (checked) Cleared alarm

Advanced Settings | Enterprise Project | Tag

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.
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 Associate template , Use existing template , or Configure manually . For details about how to create a custom template, see Creating a Custom Template . NOTE After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.
Template	Select a template.
Alarm Notification	Whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message.
Notification Type	Specifies the receiving method of the alarm notification. You can select Notification group or Topic subscription . <ul style="list-style-type: none">Account contact is the mobile phone number and email address provided for registration.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 Creating a Topic and Adding Subscriptions.
Notification Group (Valid when Notification Recipient is set to Notification group)	Select the group to be notified.
Topic subscription (Valid when Notification Recipient is set to Topic subscription)	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 Generated alarm when an alarm is generated or Cleared alarm 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 2-13 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 2-14 lists DDoS Mitigation operations recorded by CTS.

Table 2-14 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

3 Advanced Anti-DDoS User Guide

3.1 Usage Overview

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

[Usage Overview](#) shows the usage overview of AAD.

Table 3-1 Usage Overview

Step	Description
Connecting services to AAD	For details, see Connecting Domain Name Website Services to Advanced Anti-DDoS .
Configuring protection policies	AAD provides abundant and comprehensive protection rules. You can configure protection policies based on your service requirements. For details, see Configuring a Protection Policy .
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 Enabling Alarm Notifications .
Managing instances	View instance information, upgrade protection bandwidth and service bandwidth, and modify elastic protection bandwidth. For details, see Managing Instances .
Managing domain names	View domain name information, update certificates, modify resolution lines, change origin server IP addresses, and modify domain name service configurations. For details, see Managing Domain Names .
Monitoring	You can set alarms based on monitoring metrics, black hole, scheduling events, and attack events to learn about the protection status of AAD in a timely manner. For details, see Monitoring .

Step	Description
Auditing	AAD related operations are recorded for later query, audit, and backtrack operations. For details, see Auditing .

3.2 Purchasing an AAD Instance

3.2.1 Purchasing AAD Instances

Before using AAD protection, you must purchase AAD instances.

NOTICE

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

Prerequisite

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


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

Constraints

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

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 upper right corner of the page, click **Buy CNAD Pro**.
- Step 4** On the **Buy AAD** page, set **Instance Type** to **Advanced Anti-DDoS**.
- Step 5** Set instance specifications, as shown in **Figure 3-1**. **Table 3-2** describe related parameters.

Figure 3-1 Setting the parameters required for purchasing an AAD instance

The screenshot shows the configuration interface for an Advanced Anti-DDoS (AAD) instance. The 'Instance Type' is set to 'Advanced Anti-DDoS'. Under 'Access Type', 'Website' is selected. The 'Region' is 'Chinese Mainland' and the 'Line' is 'BGP'. For 'Service Access Point', 'North China 1' is selected. 'IP Type' is set to 'IPv4'. The 'Basic Protection Bandwidth' is configured with a grid of options ranging from 10 Gbit/s to 1000 Gbit/s. The 'Elastic Protection Bandwidth' also has a grid of options from 10 Gbit/s to 1000 Gbit/s. The 'Service Bandwidth' is set to 100 Mbit/s using a slider. The 'Protected Domain Names' are set to 50. A note at the bottom indicates that 50 domain names are provided by default.

Table 3-2 Parameters for purchasing an AAD instance

Parameter	Description
Access Type	Website: Huawei Cloud uses intelligent algorithms to select the optimal access point for you and does not provide fixed high-defense IP addresses. This type is recommended for users using "Domain Name Access".
Region	Chinese mainland: applies to scenarios where service servers are deployed in Chinese Mainland. If service servers are deployed in other regions, you are advised to purchase the AAD international edition.
Line	Chinese mainland: Only BGP is supported.

Parameter	Description
Service Access Point	<p>The following access points are available in Chinese Mainland. Select an access point based on your service location.</p> <ul style="list-style-type: none">• North China 1: China Mobile, China Telecom, China Unicom, Beijing Education Network, Dr. Peng, Hebei Broadcast & Television, and Chongqing Broadcast & Television are supported.• CN East 2: China Mobile, China Telecom, and China Unicom are supported.
IP Type	<ul style="list-style-type: none">• IPv4: To protect an IPv4 origin server, you need to select IPv4.• IPv6: To protect an IPv6 origin server, you need to select IPv6.
Basic Protection Bandwidth	<p>The basic protection bandwidth is purchased by customers. If the peak attack traffic is less than or equal to the basic protection bandwidth, customers do not need to pay extra fees.</p> <p>To achieve enhanced protection, use the Elastic Protection Bandwidth parameter.</p>
Elastic Protection Bandwidth	<p>If you set this parameter to a value larger than the basic protection bandwidth, additional charges ensue when attack traffic exceeding the basic protection bandwidth is scrubbed.</p> <p>You can modify the elastic protection bandwidth as needed after you have purchased an AAD instance.</p> <p>NOTE</p> <p>The elastic protection bandwidth must be greater than or equal to the basic protection bandwidth. If the two are set to the same value, the elastic protection bandwidth function does not take effect.</p>
Protected Domain Names	<p>(This parameter is available only when Access Type is set to Website.) By default, 50 domain names are supported. You can pay for more domain names. A maximum of 200 domain names are supported.</p>

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

Step 6 Set **Required Duration** and **Quantity**, as shown in [Figure 3-2](#). [Table 3-3](#) describes the parameters.

Figure 3-2 Setting **Required Duration** and **Quantity**

The screenshot shows the configuration interface for an AAD instance. It includes the following fields and options:

- Instance Name:** A text input field containing "CAD-7620". A tooltip indicates: "If you create multiple instances at a time, the system will automatically add a suffix to each instance name, for example, CAD-0001."
- Enterprise Project:** A dropdown menu set to "default".
- Required Duration:** A series of buttons for 1, 2, 3, 4, 5, 6, 7, 8, 9 months, and 1 year. The "1" button is selected.
- Auto-renew:** An unchecked checkbox with a tooltip.
- Quantity:** A numeric input field set to "1". A tooltip states: "You can purchase a maximum of 20 instances at a time. You can create 4 more instances. To apply for a higher quota, submit a service ticket."

Table 3-3 Parameter description

Parameter	Description	Example Value
Instance Name	<p>Enter a name for the AAD instance you are purchasing.</p> <ul style="list-style-type: none"> The name can contain a maximum of 32 characters. The name can contain only letters, digits, underscores (_), and hyphens (-). 	CAD-0001

Parameter	Description	Example Value
Enterprise Project	This option is only available when you are logged in using an enterprise account, or when you have enabled enterprise projects. To learn more, see Enabling the Enterprise Center . You can use enterprise projects to more efficiently manage cloud resources and project members. NOTE <ul style="list-style-type: none">default: indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are listed in the default enterprise project.The default option is available in the Enterprise Project drop-down list when you purchase AAD with a registered Huawei Cloud account.	N/A
Required Duration	Set this parameter as required.	N/A
Quantity	Select the number of instances to be purchased. By default, each user can purchase a maximum of five instances.	1

NOTE

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

Step 7 Click **Next**.

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

Step 9 Pay for the order on the payment page.

----End

3.2.2 Purchasing an AAD Instance (International Edition)

Before using AAD protection, you must purchase AAD instances.

NOTICE

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

Prerequisites

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


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

Specifications Restrictions

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

Procedure

Step 1 [Log in to the management console](#).

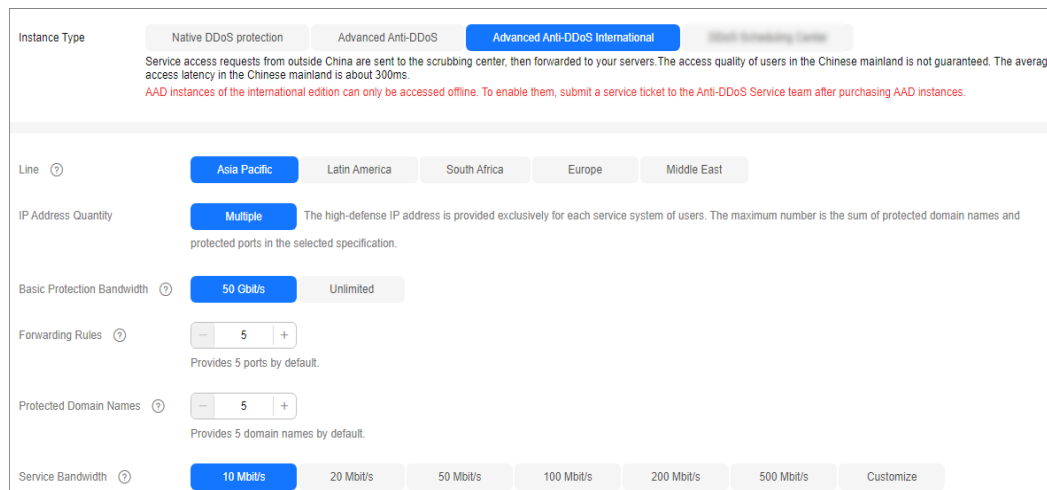
Step 2 Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

Step 3 In the upper right corner of the page, click **Buy CNAD Pro**.

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

Step 5 Set the specifications of the AAD instance, as shown in [Figure 3-3](#). [Table 3-4](#) describes the parameters.

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



The screenshot shows the configuration interface for purchasing an Advanced Anti-DDoS International instance. At the top, the 'Instance Type' is set to 'Advanced Anti-DDoS International'. Below this, there is a warning: 'Service access requests from outside China are sent to the scrubbing center, then forwarded to your servers. The access quality of users in the Chinese mainland is not guaranteed. The average access latency in the Chinese mainland is about 300ms. AAD instances of the international edition can only be accessed offline. To enable them, submit a service ticket to the Anti-DDoS Service team after purchasing AAD instances.'

The configuration options are as follows:

- Line**: Asia Pacific (selected), Latin America, South Africa, Europe, Middle East.
- IP Address Quantity**: Multiple (selected). Note: The high-defense IP address is provided exclusively for each service system of users. The maximum number is the sum of protected domain names and protected ports in the selected specification.
- Basic Protection Bandwidth**: 50 Gbit/s (selected), Unlimited.
- Forwarding Rules**: 5 (selected). Note: Provides 5 ports by default.
- Protected Domain Names**: 5 (selected). Note: Provides 5 domain names by default.
- Service Bandwidth**: 10 Mbit/s (selected), 20 Mbit/s, 50 Mbit/s, 100 Mbit/s, 200 Mbit/s, 500 Mbit/s, Customize.

Table 3-4 Parameters for purchasing an AAD instance

Parameter	Description
Line	Asia Pacific, Latin America, South Africa, Europe, and Middle East.
IP Address Quantity	The default value is Multiple . AAD provides exclusive high-defense IP addresses (used to provide services in place of the origin server IP address) for each of customer's service systems. The maximum number is the sum of protected domain names and protected ports in the selected specification.
Basic Protection Bandwidth	50 Gbit/s : provides a maximum of 50 Gbit/s protection capacity. Unlimited : provides unlimited DDoS protection capacity.
Forwarding Rules	By default, five IP addresses are provided. A maximum of 50 IP addresses can be selected.
Protected Domain Names	By default, five IP addresses are provided. A maximum of 50 IP addresses can be selected.
Service Bandwidth	Service bandwidth specifies the maximum bandwidth used by AAD scrubbing center to forward the scrubbed traffic to the origin server. <ul style="list-style-type: none">• The service bandwidth ranges from 10 Mbit/s to 5000 Mbit/s.• If the AAD equipment room is outside Huawei Cloud, it is recommended that the service bandwidth be greater than or equal to the egress bandwidth of the origin servers.

Step 6 Set **Required Duration** and **Quantity**, as shown in [Figure 3-4](#). [Table 3-5](#) describes the parameters.

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

The screenshot shows the configuration interface for an AAD instance. It includes the following fields and options:

- Instance Name:** A text input field containing "CAD-c386". A note below it states: "If you create multiple instances at a time, the system will automatically add a suffix to each instance name, for example, CAD-0001."
- Enterprise Project:** A dropdown menu with "default" selected.
- Required Duration:** A row of buttons for selecting a duration: 1, 2, 3 (selected), 4, 5, 6, 7, 8, 9 months, and 1 year.
- Auto-renew:** A checkbox labeled "Auto-renew" which is currently unchecked.
- Quantity:** A numeric input field with a minus sign on the left, the number "1" in the center, and a plus sign on the right.

Table 3-5 Parameter description

Parameter	Description	Example Value
Instance Name	Enter a name for the AAD instance you are purchasing. <ul style="list-style-type: none">The name must be 32 or fewer characters in length.The name can contain only letters, digits, underscores (_), and hyphens (-).	CAD-0001
Required Duration	Select a value from one month to one year.	1
Quantity	Select the number of instances to be purchased. By default, each user can purchase a maximum of five instances.	1

 **NOTE**

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

Step 7 Click **Next**.

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

Step 9 Pay for the order on the payment page.

----End

3.3 Connecting Services to AAD

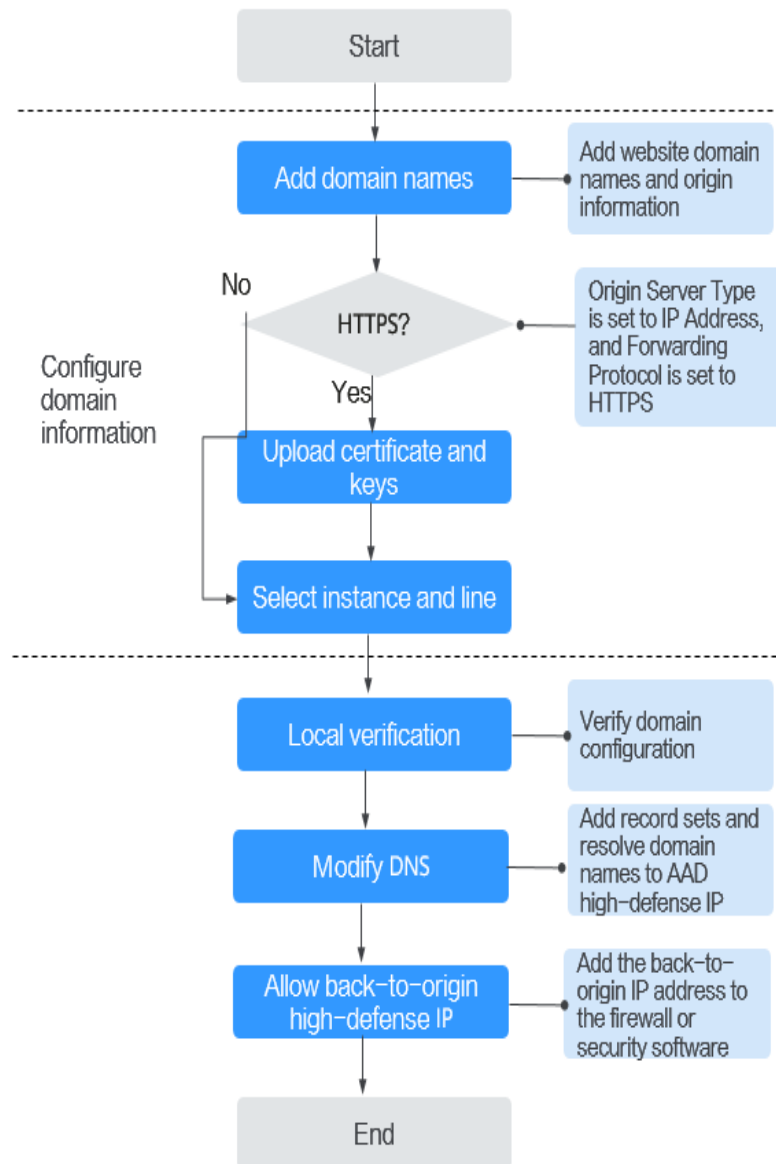
3.3.1 Connecting Domain Name Website Services to Advanced Anti-DDoS

3.3.1.1 Website Service Access Process

After purchasing AAD, you need to connect website services to AAD through CNAME resolution so that all public network traffic is diverted to the high-defense IP address and the origin server is not exposed.

Figure 3-5 shows the process of connecting website services to AAD.

Figure 3-5 Process of connecting website services to AAD



3.3.1.2 Step 1: Configuring a Protected Domain Name (Website Services)

For website services, after purchasing Advanced Anti-DDoS (AAD), you need to configure the protected domain names in the AAD instance so that the services can be connected to the high-defense IP address through CNAME resolution.

NOTE

If you have enabled the **Enterprise Project**, you can configure AAD instances and lines under the enterprise project.

Prerequisites

- You have purchased an AAD instance.

- The domain name of the website to be protected has been registered.

Specification Limitations


Each AAD instance can protect a maximum of 50 domain names. Domain names that need to be protected cannot be added in batches.

Constraints

- Currently, the **origin server domain name** can only be set to a CNAME of Huawei Cloud WAF.
- Currently, AAD only supports .pem certificates.
- A CNAME record is generated based on the domain name. For the same domain name, the CNAME records are the same.
- AAD supports the Web Socket protocol, which is enabled by default.
- You can select multiple lines (AAD IP addresses) for a domain name. When selecting multiple AAD IP addresses, ensure that the number of forwarding rules, the forwarding protocol, forwarding port, and service type configured for each AAD IP address are the same.

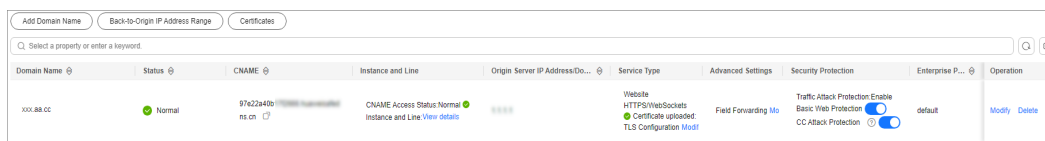
Procedure

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 **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-6 Domain name access



Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Enterprise P...	Operation
xxx.a8.cc	Normal	97622a40b... ns.cn	CNAME Access Status Normal Instance and Line View details		Website HTTPS/WebSockets Certificate updated TLS Configuration Modi	Field Forwarding Mo	Traffic Attack Protection Enable Basic Web Protection CC Attack Protection	default	Modify Delete

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

Step 5 On the **Add Domain Name** page, configure domain name information, as shown in [Figure 3-7](#). [Table 3-6](#) describes the parameters.

Figure 3-7 Configuring website domain

Protected Domain Name ?

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

Origin Server Type Origin Server IP Address Domain name

Forwarding Protocol	Origin Server Port	Operation
<input type="text" value="HTTP"/> ▾	<input type="text" value="80"/> ▾	Delete

+ You can add 1 more origin server configurations.

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

If your origin server has been exposed, click [here](#) to get a solution.

Table 3-6 Domain name parameters

Parameter	Description	Example Value
Protected Domain Name	<p>Enter the domain name of the service to protect.</p> <ul style="list-style-type: none">• Single domain name: Enter a single domain name, for example, <code>www.example.com</code>.• Wildcard domain name<ul style="list-style-type: none">- If the server IP address of each subdomain name is the same, enter a wildcard domain name. For example, if the subdomain names <i>a.example.com</i>, <i>b.example.com</i>, and <i>c.example.com</i> have the same server IP address, you can directly add the wildcard domain name <i>*.example.com</i> to AAD for protection.- If the server IP addresses of subdomain names are different, add subdomain names one by one.	<p>Single domain name: <code>www.example.com</code></p> <p>Wildcard domain name: <code>*.example.com</code></p>

Parameter	Description	Example Value
Origin Server Type	<p>Type of the origin server.</p> <ul style="list-style-type: none">● IP address: IP address of the origin server. Enter a maximum of 20 IP addresses and separate them using commas (,).● Domain name Currently, only Huawei Cloud WAF CNAMEs are supported.● Forwarding Protocol Protocol used by AAD to forward requests from clients (such as browsers) The options are HTTP and HTTPS.● Origin Server Port Port used by AAD to forward client requests to the server <p>NOTICE</p> <ul style="list-style-type: none">● If the protected domain name to be added shares the high-defense IP address and protocol or port with a domain name, the values of Origin Server Type for the domain names must be same.<ul style="list-style-type: none">– If Origin Server Type is set to IP address for a domain name, ensure the web protection is enabled for the domain name. For details about how to enable the web protection, see Enabling Basic Web Protection and CC Attack Protection.– If Origin Server Type is set to Domain name for a domain name, ensure that the domain name and the protected domain name to be added are connected to the same WAF.● If Origin Server Type is set to Domain name, ensure that the domain name has been allowed to use a proxy. Otherwise, the service may be unavailable after being connected to AAD.● If you connect your service to AAD using a WAF CNAME but no longer need WAF protection, delete the service domain name from AAD first.	<p>Origin server IP address: <i>XXX.XXX.1.1</i></p> <p>Forwarding Protocol: HTTP</p> <p>Origin Server Port: 80</p>
Certificate Name	<p>If Origin Server Type is set to IP Address and Forwarding Protocol is set to HTTPS, you need to upload a certificate. For details about how to upload a certificate, see Step 6.</p>	-

Step 6 (Optional) Upload a certificate.

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

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

To upload a certificate, perform the following steps:

1. Click **Upload Certificate**. In the displayed **Upload Certificate** dialog box, select a certificate upload mode.
 - **Manual**: Enter the certificate name and paste the certificate and private key text content, as shown in [Figure 3-8](#). [Table 3-7](#) describes the parameters.
 - **Automatic**: Select an issued certificate.

NOTICE

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

Figure 3-8 Uploading a certificate

Upload Certificate

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

Upload Mode Manual Automatic

Certificate

Certificate

Private Key

Note: Certificate modification takes effect after 1 minute.

Cancel OK

NOTE

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

Table 3-7 Parameter description

Parameter	Description
Certificate	<ul style="list-style-type: none"> - The certificate must be in the following format: <pre>-----BEGIN CERTIFICATE----- MIIDljCCAv+gAwIBAgIJAMD2jG2tYQG6MA0GCSqGSIb3DQEBBQUAMIGPMQswCQYD VQQGEwJDSDELMAkGA1UECBMCWkoxCzAJBgNVBACtAKhaMQ8wDQYDVQQKEwZodWF3 ZWkxZzANBgNVBAsTBmh1YXdlTEPMA0GA1UEAxMGaHVhd2VpMQ8wDQYDVQQPpEwZz ZXJ2ZXIxiAgBgkqhkiG9w0BCQEW3p3YW5nd2VpZGtKQDE2My5jb20wHhcNMTUw MzE4MDMzNjU5WhcNMjUwMzE1MDMzNjU5WjCBjzELMAkGA1UEBhMCQ0gxZAJBgNV BAGTAIpKMQswCQYDVQQHEwJlWjEPMA0GA1UEChMGaHVhd2VpMQ8wDQY..... -----END CERTIFICATE-----</pre> - Method for you to copy your certificate: <ul style="list-style-type: none"> ▪ For a .pem certificate: Use a text editor to open the certificate file and copy the content here. ▪ For other certificates: Convert your certificate to a .pem one. Then open it with a text editor and copy its content.
Private Key	<p>The private key must be in the following format:</p> <pre>-----BEGIN RSA PRIVATE KEY----- MIIDljCCAv+gAwIBAgIJAMD2jG2tYQG6MA0GCSqGSIb3DQEBBQUAMIGPMQswCQYDVQQG EwJDSDELMAkGA1UECBMCWkoxCzAJBgNVBACtAKhaMQ8wDQYDVQQKEwZodWF3ZWkxZzAN BgNVBAsTBmh1YXdlTEPMA0GA1UEAxMGaHVhd2VpMQ8wDQYDVQQPpEwZzZXJ2ZXIxiAg BgkqhkiG9w0BCQEW3p3YW5nd2VpZGtKQDE2My5jb20wHhcNMTUwMzE4MDMzNjU5WhcN MjUwMzE1MDMzNjU5WjCBjzELMAkGA1UEBhMCQ0gxZAJBgNVBAGTAIpKMQswCQYDVQQH EwJlWjEPMA0GA1UEChMGaHVhd2VpMQ8wDQYDVQQLEwZ -----END RSA PRIVATE KEY-----</pre> <ul style="list-style-type: none"> - Method for you to copy your private key: <ul style="list-style-type: none"> ▪ For a .pem file: Use a text editor to open the private key file and copy the content here. ▪ For other certificates: Convert your certificate to a .pem one. Then open it with a text editor and copy its content.

2. Click **OK**.

Step 7 Click **Next** and select an AAD instance and line, as shown in [Figure 3-9](#).

Figure 3-9 Selecting an AAD instance and line

Protected Domain Name: www.example.com

Select AAD Instance and Line This domain name supports IP. Only instances and lines that support IP can be selected.

Enterprise Project: default

AAD Instance	Line
<input checked="" type="checkbox"/> CAD-0001	
<input type="checkbox"/> CAD-c381	
<input type="checkbox"/> CAD-0002	
<input type="checkbox"/> CAD-0003	
<input type="checkbox"/> CAD-0004	
<input type="checkbox"/> CAD-0005	
<input type="checkbox"/> CAD-0006	
<input type="checkbox"/> CAD-0007	
<input type="checkbox"/> CAD-0008	
<input type="checkbox"/> CAD-0009	
<input type="checkbox"/> CAD-0010	

10 Total Records: 94 < 1 2 3 4 5 6 ... 10 >

Previous Submit and Continue Cancel

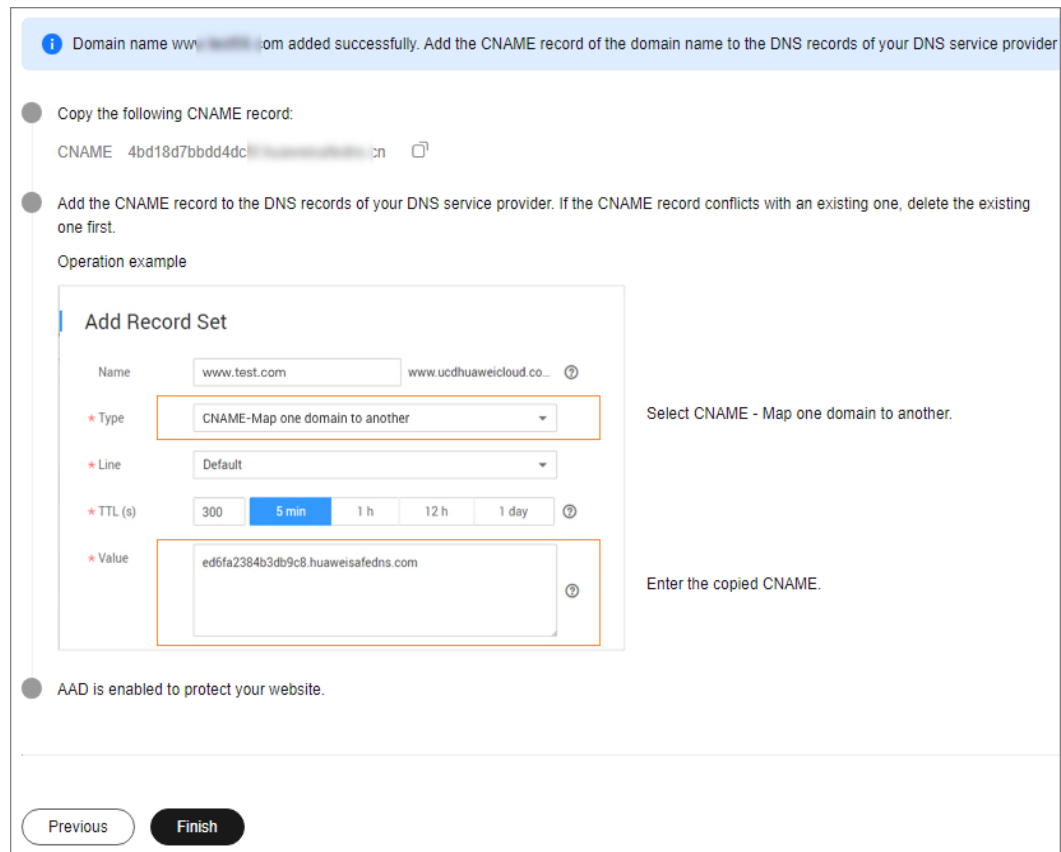
NOTICE

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

Step 8 Click **Submit and Continue**. A dialog box is displayed, as shown in [Figure 3-10](#).

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

Figure 3-10 Modifying DNS



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

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

Figure 3-11 Back-to-origin IP address

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

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

Back-to-Origin IP Address Range

10.0.0.0/24

10.0.0.1

10.0.0.0/24 10.0.0.1

10.0.0.1

10.0.0.0/24 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.6 10.0.0.7 10.0.0.8 10.0.0.9 10.0.0.10 10.0.0.11 10.0.0.12 10.0.0.13 10.0.0.14 10.0.0.15 10.0.0.16 10.0.0.17 10.0.0.18 10.0.0.19 10.0.0.20 10.0.0.21 10.0.0.22 10.0.0.23 10.0.0.24 10.0.0.25 10.0.0.26 10.0.0.27 10.0.0.28 10.0.0.29 10.0.0.30 10.0.0.31

Next

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

NOTICE

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



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

----End

Follow-up Procedure

After the domain name is configured, you are advised to locally verify that the domain name parameters are correctly configured. For details, see [Step 3: Locally Verifying the Website Service Configuration](#).

Related Operation

- If you do not want a domain name to be resolved to a high-defense IP address, locate the row containing the domain name on the **Domain Name Access** page and click **View details** in the **Instance and Line** column. On the page that is displayed, click  for the target high-defense IP address to set **DNS Resolution** to .
- If you do not want to protect a domain name, locate the row containing the domain name on the **Domain Name Access** page and click **Delete** in the **Operation** column.

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

A back-to-source IP address is used by AAD to proxy clients to request servers. AAD replaces all source IP addresses with back-to-source IP addresses to ensure the security, stability, and availability of origin servers.


If a firewall has been configured or security software has been installed on the origin server, whitelist the back-to-origin IP address for the firewall or security software. In this case, the back-to-origin IP address will not be blocked by the security policies set on the origin server.

Prerequisites

The domain name to be protected has been connected to AAD.

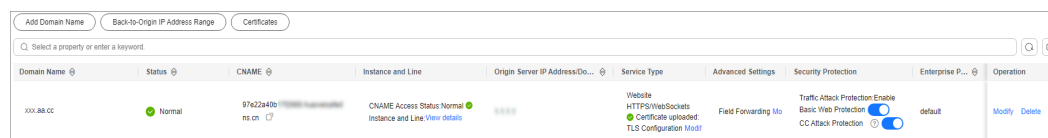
Procedure

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 **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-12 Domain name access



Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Enterprise P...	Operation
xxx.a8.cc	Normal	97e22a40b- ms.cn	CNAME Access Status Normal Instance and Line View details		Website HTTPS/WebSockets Certificate uploaded TLS Configuration Modf	Field Forwarding Mo	Traffic Attack Protection Enable Basic Web Protection CC Attack Protection	default	Modify Delete

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

Step 5 In the displayed **Back-to-Origin IP Address Range** dialog box, view the back-to-origin IP address range.

Figure 3-13 Viewing the back-to-origin IP address range



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

----End

3.3.1.4 Step 3: Locally Verifying the Website Service Configuration

After the configuration takes effect, AAD is expected to forward the packets sent to the high-defense IP address or AAD CNAME to the origin servers. To ensure service stability, you are advised to verify the configuration.


This section uses the Telnet tool as an example to describe how to locally verify the website service configuration.

Prerequisite

The domain name to be protected has been added to AAD.

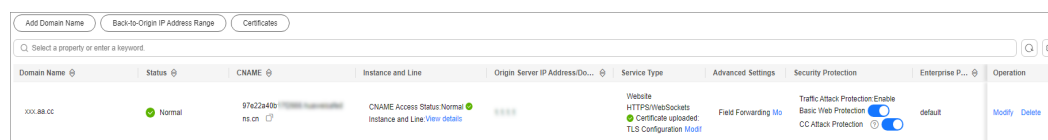
Procedure

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 **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-14 Domain name access



Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Enterprise P...	Operation
xxx.bb.cc	Normal	97a22a4b1ns.cn	CNAME Access Status Normal Instance and Line View details		Website HTTPS/WebSockets Certificate uploaded TLS Configuration Modi	Field Forwarding Mo	Traffic Attack Protector Enable Basic Web Protection <input checked="" type="checkbox"/> CC Attack Protection <input checked="" type="checkbox"/>	default	Modify Delete

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

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

```
telnet Origin_server_IP_address 80
```

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

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

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

```
telnet the_CNAME_value_copied_in_Step 4 80
```

- If you can telnet the domain name, the configuration is correct.

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

----End

 NOTE

For details about how to verify whether WAF basic protection is enabled, see [Testing WAF](#).

3.3.1.5 Step 4: Modifying DNS Resolution

After adding a domain name to AAD, you need to modify the DNS resolution to connect the domain name to AAD. All public network traffic is diverted to the high-defense IP address, and therefore your services on the origin servers are protected against DDoS attacks.

AAD supports A record-based access and CNAME-based access. The later is recommended. The CNAME-based access has the following advantages:

- Easy to use. You only need to modify the resolution configuration at a time during domain name resolution (for example, on Huawei Cloud DNS).
- Automatic line switchover. If an AAD line encounters an exception, the CNAME resolution can be automatically switched to other properly working lines.
- Service continuity. In a three-line package service, if a line is attacked and access is blocked, AAD automatically uses the other available lines to complete CNAME resolution, ensuring service availability.

This section uses Huawei Cloud DNS as an example to describe how to modify DNS record. The methods to modify DNS record on other platforms are similar.

Prerequisite

The domain name has been added to AAD.

Constraints

- When adding a CNAME record, you must delete the existing A records from the DNS record set. If they are not deleted, you will fail to add the new record because resolution conflicts may occur. Some DNS service providers allow you to change A records to CNAME records.
- The DNS configuration takes effect after a period of time. You can test the domain name resolution using some online test tools.


Impact on the System

The DNS configuration may affect current service operating. Therefore, you are advised to configure DNS during off-peak hours.

CNAME Access

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

Step 1 [Log in to the management console.](#)


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


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

Figure 3-15 Domain name access



Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Enterprise P...	Operation
xxx.a8.cc	Normal	97a22a4b0... ns.cn	CNAME Access Status Normal Instance and Line: View Details		Website HTTPS/WebSockets Certificate uploaded TLS Configuration Modif	Field Forwarding Mo	Traffic Attack Protection: Enable Basic Web Protection: default CC Attack Protection: <input checked="" type="checkbox"/>		Modify Delete

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

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

Step 6 For details, see section [Adding a CNAME Record Set](#).

----End


CAUTION


If you have configured the **hosts** file in [Step 3: Locally Verifying the Website Service Configuration](#) for the test, delete the configuration after this step. Otherwise, protection exceptions may occur.

A Record-based Access

The following steps use the China Telecom line package as an example.

Step 1 [Log in to the management console.](#)

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Networking > Domain Name Service**.

Step 4 Add and A record set. For details, see section [Adding an A Record Set](#).

----End

3.4 Configuring a Protection Policy


3.4.1 Configuring a Blacklist and a Whitelist

Scenarios

You can set whitelists and blocklists on your AAD instances to block or allow access requests from specified IP addresses.

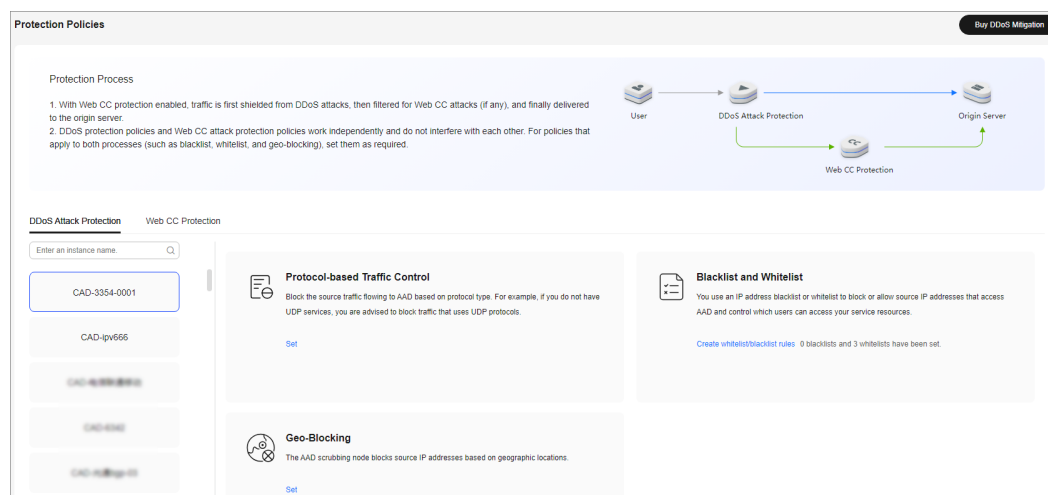
Procedure

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 **Advanced Anti-DDoS > Protection Policies**. The **Protection Policies** page is displayed.

Figure 3-16 Advanced Anti-DDoS protection policies



Step 4 Select the instance for which you want to configure a blacklist or whitelist.

Step 5 Configure a blacklist and a whitelist.

- Configuring a Blacklist
 - a. In the **Blacklist and Whitelist** configuration area, click **Create whitelist/blacklist rules**.
 - b. Select the **IP Blacklist** tab and click **Add**.
 - c. In the displayed dialog box, enter the IP addresses or IP ranges to be blocked.

Figure 3-17 Adding blacklisted IP addresses

Add IP Blacklist ×

Enter an IP address to be added to the blacklist. You can add 100 more IP addresses to the blacklist. The blacklisted IP addresses will be intercepted.

Enter an IP address or IP range and use commas (,) to separate IP addresses or IP ranges. IP addresses in the blacklist will be intercepted.

Cancel OK

NOTE

A maximum of 100 IP addresses can be added to the blacklist of an instance, and IP addresses in the blacklist will be blocked.

d. Click **OK**.

On the **IP Blacklist** page, click **Delete** in the **Operation** column or select the blacklisted IP addresses to be deleted and click **Delete** to delete IP addresses in batch. Deleted IP addresses will not be blocked.

• Configuring an IP whitelist

a. Select the **IP Whitelist** tab and click **Add**.

b. In the displayed dialog box, enter the IP addresses or IP ranges to be permitted.

Figure 3-18 Adding whitelisted IP addresses

Add IP Whitelist ×

Enter an IP address to be added in the whitelist. You can add 197 more IP addresses to the whitelist. The whitelisted IP addresses will be allowed.

Enter an IP address or IP range and use commas (,) to separate IP addresses or IP ranges. IP addresses in the whitelist will be allowed.

Cancel OK

NOTE

A maximum of 100 IP addresses can be added to the whitelist of an instance. IP addresses in the whitelist are permitted.

- c. Click **OK**.

On the **IP Whitelist** page, click **Delete** in the **Operation** column or select the whitelisted IP addresses to be deleted and click **Delete** to delete IP addresses in batch. After an IP address is deleted from the whitelist, the device will not directly permit traffic from this IP address.

----End


3.4.2 Configuring Protocol Blocking

You can use the traffic control rules to allow or block UDP traffic or Traffic Outside Chinese Mainland that accesses your AAD instances.

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

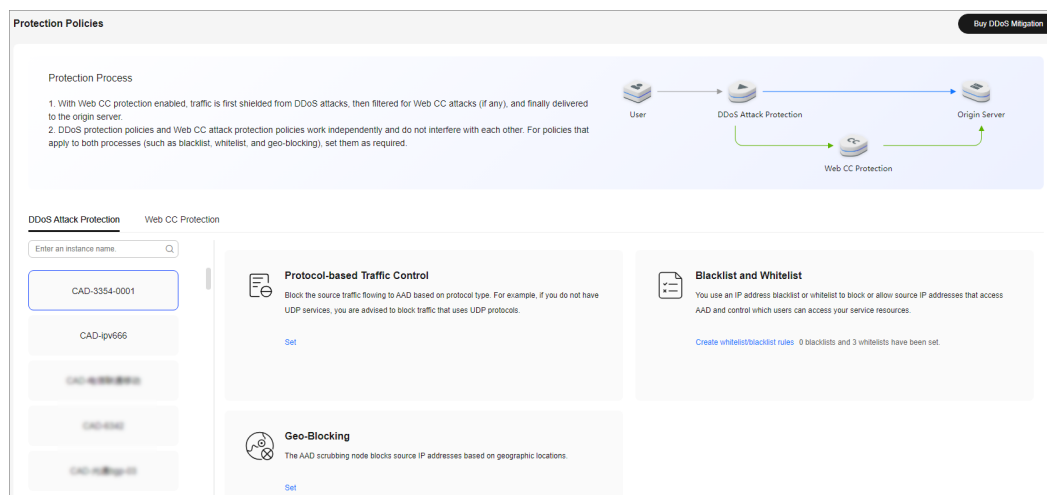
Procedure

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 **Advanced Anti-DDoS > Protection Policies**. The **Protection Policies** page is displayed.

Figure 3-19 Advanced Anti-DDoS protection policies



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

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


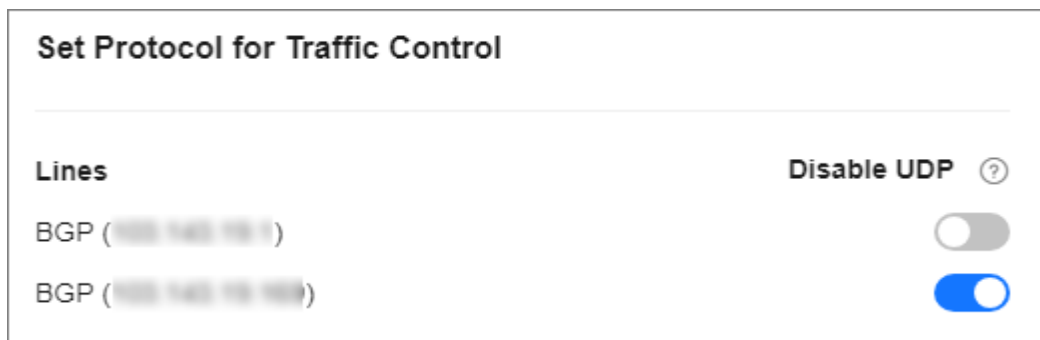
Step 6 In the dialog box that is displayed, select a route and set the switch to  to disable the protocol.

Figure 3-20 Disabling a protocol

----End

3.4.3 Configuring Geo-Blocking

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

Procedure


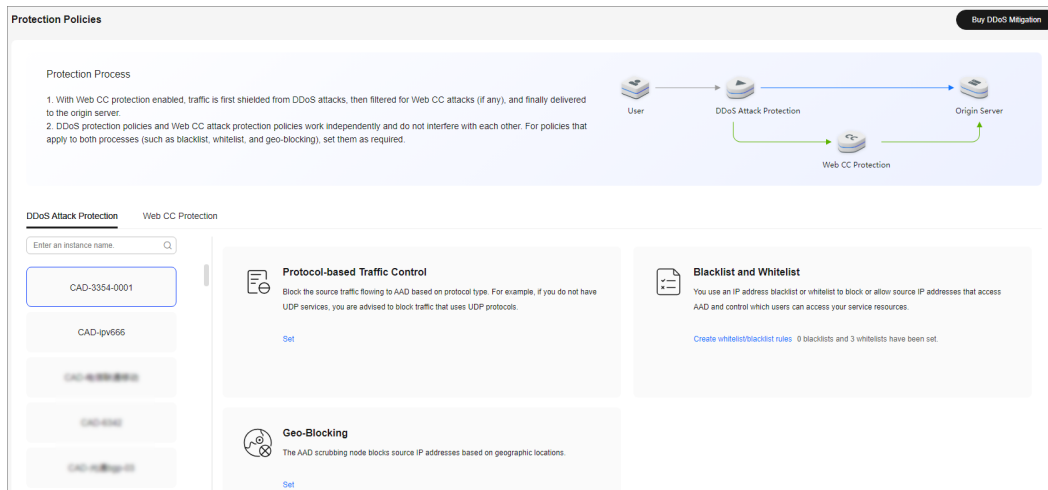
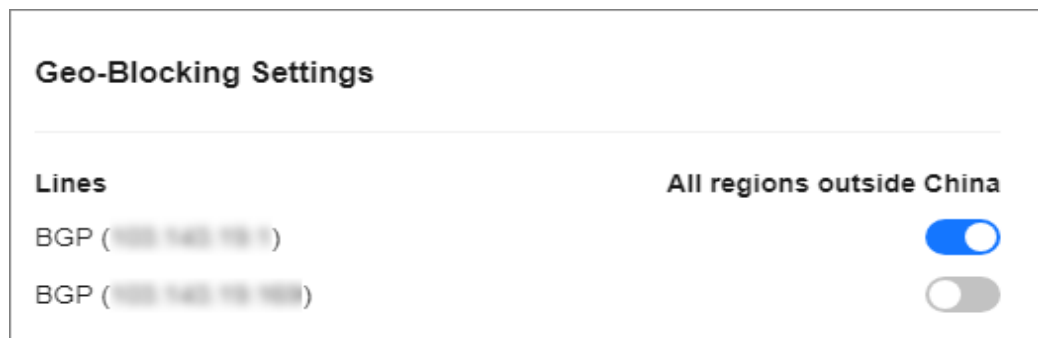
- Step 1** [Log in to the management console.](#)
- Step 2** Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.
- Step 3** In the navigation pane on the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

Figure 3-21 Advanced Anti-DDoS protection policies

- Step 4** Select the instance for which geo-blocking needs to be configured.
- Step 5** In the **Geo-Blocking** configuration area, click **Set**.
- Step 6** In the displayed dialog box, select a route and select the areas you want to block.

Figure 3-22 Geo-blocking settings

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

----End

3.4.4 Configuring CC Attack Protection Rules

3.4.4.1 Configuring Frequency Control Rules

Scenarios


You can set frequency control rules to limit the access frequency of a single IP address, cookie, or referer to the origin server of a protected website. You can also enable policy-based, domain name, and URL rate limiting to detect and block malicious traffic.

Prerequisites

Website services have been connected to AAD and **Basic Web Protection** has been enabled.

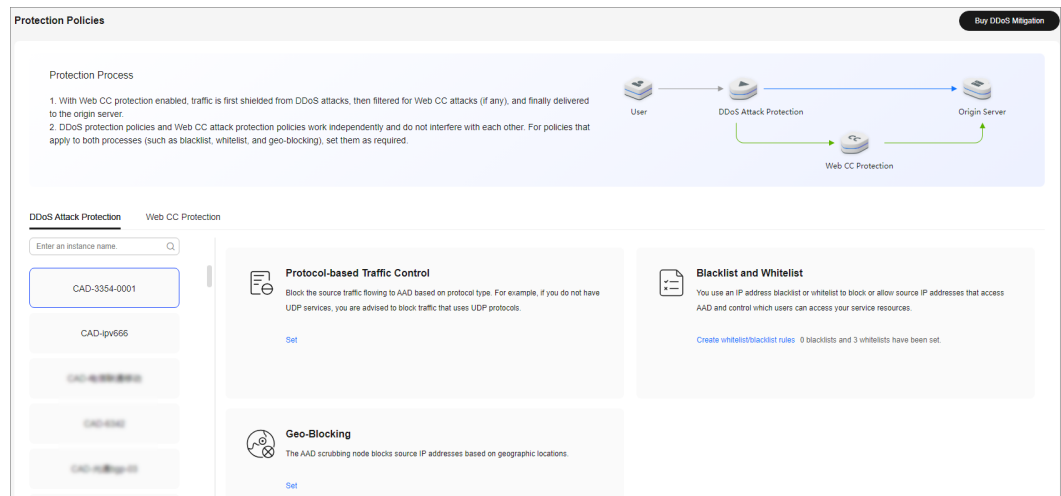
Procedure

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 Service Center** page is displayed.

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

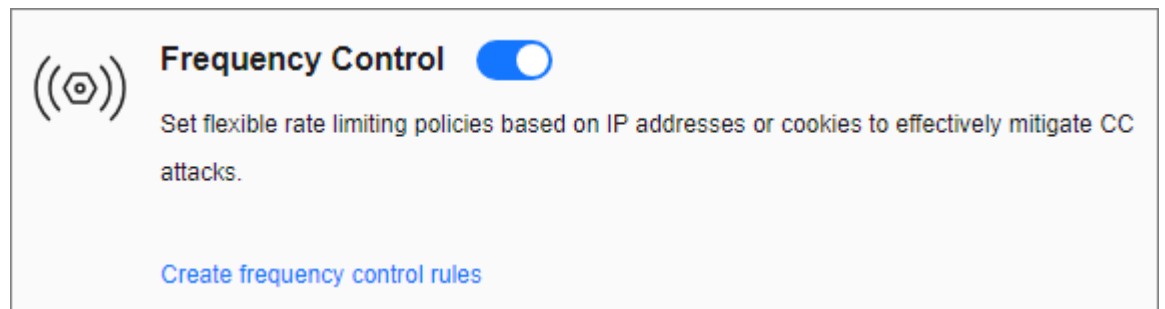
Figure 3-23 Advanced Anti-DDoS protection policies



Step 4 Click the **Web Attack Protection** tab.

Step 5 After selecting the region and objects, click **Create frequency control rules**.

Figure 3-24 Frequency control rules



Step 6 Click **Create frequency control rules**.

Step 7 Configure the frequency control rule, as shown in [Figure 3-25](#).

Figure 3-25 Creating a frequency control rule

Creating a Frequency Control Rule Configuration

- Name:** test01
- Rate Limit Mode:** Source (Selected), Destination
- Rate Limit Mode Description:** Requests from a specific source are limited. For example, if traffic from an IP address (or user) exceeds the rate limit you configure in this rule, WAF limits traffic rate of the IP address (or user) in the way you configure.
- Rate Limit Mode Options:** Per IP address, Per user (Selected), Other
- User Identifier:** Cookie (Selected), name
- User Identifier Description:** If this field does not exist in a request, the request is not counted. If this field exists but is empty, the request is counted.
- Request Aggregation:** Disabled
- Request Aggregation Description:** When this function is enabled, if you added a wildcard domain name, for example, *.a.com, requests to all matched subdomain names such as b.a.com and c.a.com are counted.
- Rate Limit Condition:**

Field	Subfield	Logic	Content
Path	--	Include	/admin
- Rate Limit Condition Description:** Add You can add 29 more conditions.(This parameter takes effect only when multiple conditions are met at the same time.)
- Rate Limit:** 1 requests, 60 seconds, Global (unchecked)
- Protective Action:** Verification code (Selected), Block, Block dynamically, Log only
- Lock Verification:** 0 seconds
- Effective Time:** Immediately (Selected)

Buttons: Cancel, OK

Table 3-8 Parameter description

Parameter	Description
Name	Name of the rule

Parameter	Description
Rate Limit Mode	<ul style="list-style-type: none">● Source: Requests from a specific source are limited. For example, if traffic from an IP address (or user) exceeds the rate limit you configure in this rule, WAF limits traffic rate of the IP address (or user) in the way you configure.<ul style="list-style-type: none">– Per IP address: A web visitor is identified by the IP address.– Per user: A website visitor is identified by the key value of Cookie or Header.– Other: A web visitor is identified by the Referer field (user-defined request source).<p>NOTE If you set Rate Limit Mode to Other, set Content of Referer to a complete URL containing the domain name. The Content field supports prefix match and exact match only, but cannot contain two or more consecutive slashes, for example, ///admin. If you enter ///admin, WAF will convert it to /admin. For example, if you do not want visitors to access www.test.com, set Referer to http://www.test.com.</p>● Destination: Requests to a specific destination are limited.<ul style="list-style-type: none">– By rule: If this rule is used by multiple domain names, requests for all these domain names are counted for this rule no matter what IP addresses these requests originate from. If you have added a wildcard domain name to WAF, requests for all domain names matched the wildcard domain name are counted for triggering this rule no matter what IP addresses these requests originate from.– By domain name: Requests for each domain name are counted separately. If the number exceeds the threshold you configure, the protective action is triggered no matter what IP addresses these requests originate from.– By URL: Requests for each URL are counted separately. If the number exceeds the threshold you configure, the protective action is triggered no matter what IP addresses these requests originate from.
Request Aggregation	<p>This parameter is not required when you select Destination and By rule for Rate Limit Mode.</p> <p>This function is disabled by default. Keep this function enabled so that requests to all domain names that match a protected wildcard domain are counted for triggering this rule. For example, if you added *.a.com, requests to all matched domain names such as b.a.com and c.a.com are counted.</p>



Parameter	Description
User Identifier	<p>This parameter is mandatory when you select Source and Per user for Rate Limit Mode.</p> <ul style="list-style-type: none">● Cookie: A cookie field name. You need to configure an attribute variable name in the cookie that can uniquely identify a web visitor based on your website requirements. This field does not support regular expressions. Only complete matches are supported. For example, if a website uses the name field in the cookie to uniquely identify a web visitor, enter name.● Header: Set the user-defined HTTP header you want to protect. You need to configure the HTTP header that can identify web visitors based on your website requirements.
Trigger	<p>Click Add to add conditions. At least one condition is required, but up to 30 conditions are allowed. If you add more than one condition, the rule will only take effect if all of the conditions are met.</p> <ul style="list-style-type: none">● Field: Set this parameter based on the site requirements.● Subfield: Configure this field only when IPv4, IPv6, Cookie, Header, or Params is selected for Field.● Logic: Select the required logic from the drop-down list box.● Content: Enter or select the content that matches the condition.
Rate Limit	<p>The number of requests allowed from a website visitor in the rate limit period. If the number of requests exceeds the rate limit, WAF takes the action you configure for Protective Action.</p> <p>All WAF instances: Requests to on one or more WAF instances will be counted together according to the rate limit mode you select. By default, requests to each WAF instance are counted. If you enable this, WAF will count requests to all your WAF instances for triggering this rule. To enable user-based rate limiting, Per user or Other (Referer must be configured) instead of Per IP address must be selected for Rate Limit Mode. This is because IP address-based rate limiting cannot limit the access rate of a specific user. However, in user-based rate limiting, requests may be forwarded to one or more WAF instances. Therefore, All WAF instances must be enabled for triggering the rule precisely.</p>

Parameter	Description
Protective Action	<p>The action that WAF will take if the number of requests exceeds Rate Limit you configured. The options are as follows:</p> <ul style="list-style-type: none">• Verification code: WAF allows requests that trigger the rule as long as your website visitors complete the required verification.• Block: WAF blocks requests that trigger the rule.• Block dynamically: WAF blocks requests that trigger the rule based on Allowable Frequency, which you configure after the first rate limit period is over.• Log only: WAF only logs requests that trigger the rule.
Lock Verification	<p>This parameter is mandatory if Protective Action is set to Verification code.</p> <p>If a visitor fails verification code authentication, verification is required for all access requests within the specified period.</p>
Allowable Frequency	<p>This parameter can be set if you select Block dynamically for Protective Action.</p> <p>WAF blocks requests that trigger the rule based on Rate Limit first. Then, in the following rate limit period, WAF blocks requests that trigger the rule based on Allowable Frequency you configure.</p> <p>The Allowable Frequency must be less than or equal to the Rate Limit.</p>
Notification Window	<p>The default option is Immediately.</p>
Block Duration	<p>Period of time for which to block the item when you set Protective Action to Block.</p>
Block Page	<p>The page displayed if the request limit has been reached. This parameter is configured only when Protective Action is set to Block.</p> <ul style="list-style-type: none">• If you select Default settings, the default block page is displayed.• If you select Customize, customize a page to be displayed.
Block Page Type	<p>If you select Custom for Block Page, select a type of the block page among options application/json, text/html, and text/xml.</p>
Page Content	<p>Specifies the content to be displayed on the page you will customize.</p>

Step 8 Click **OK**.

----**End**

Follow-up Operations

- Enable frequency control protection: On the **Web Attack Protection** page, set **Frequency Control** to .
- Disable frequency control protection: On the **Web Attack Protection** page, set **Frequency Control** to .

3.4.5 Enabling Basic Web Protection and CC Attack Protection

After a domain name is added, you can enable basic web protection and CC attack protection for your domain names.

Prerequisites


At least one domain name has been added for protection.

Constraints

- Basic web protection and CC attack protection take effect only for forwarding rules whose service type is **Website** and origin server type is **Origin Server IP Address**.
- Before enabling **CC Attack Protection**, you need to enable **Basic Web Protection**.

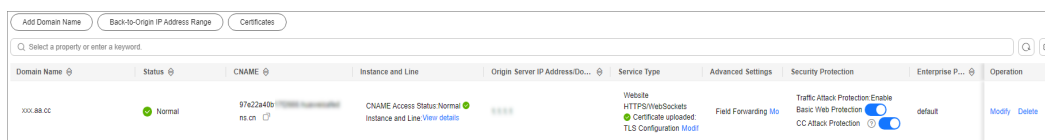
Procedure



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 **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-26 Domain name access



Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Enterprise P...	Operation
xxx.a8.cc	Normal	97622a40b1ns.cn	CNAME Access Status Normal Instance and Line View details		Website HTTPS/WebSockets Certificate updated TLS Configuration Modif	Field Forwarding Mo	Traffic Attack Protection Enable Basic Web Protection  default CC Attack Protection 	default	Modify Delete

Step 4 Set the status of **Basic Web Protection** and **CC Protection** to  to enable Basic Web Protection and CC Protection.

NOTE

Traffic Attack Protection is enabled by default.

----End

3.5 Enabling Alarm Notifications

After you enable the alarm notification, a notification message will be sent to you through the method you have configured when:

- An IP address is under the DDoS attacks.
- Additional fees are incurred for traffic exceeding the basic protection bandwidth.

If you want to monitor service metrics in detail, you are advised to use Cloud Eye to set alarm rules and alarm notifications. For details, see [Monitoring](#).

Precautions

- The Simple Message Notification (SMN) service is a paid service. For details about the price, see [SMN Product Pricing Details](#).
- Before enabling alarm notifications, you are advised to create a message topic in the SMN service as an administrator. For details, see .
- Only notification topics in the same region as the CNAD Advanced instance can be displayed.

Prerequisites

You have purchased an AAD instance.

Procedure

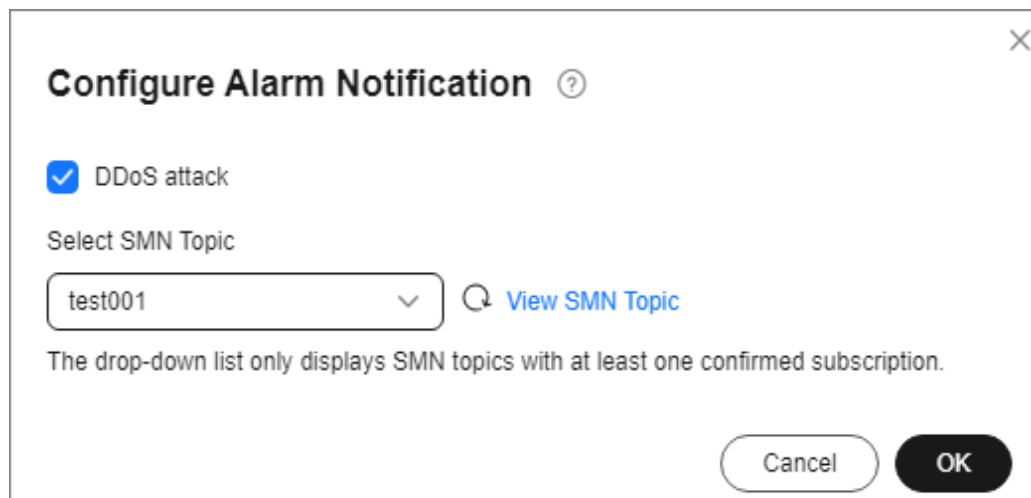
Step 1 [Log in to the management console](#).

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** page is displayed.

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

Step 4 In the upper right corner of the instance list, click **Configure Alarm Notification**.

Step 5 In the displayed **Configure Alarm Notification** dialog box, select **DDoS attack**.

Figure 3-27 Configure Alarm Notification

Select an existing topic from the drop-down list or click **View SMN Topic** and create an SMN topic on the displayed page for configuring the terminals for receiving alarm notifications.

Perform the following steps to create a topic:

1. Create a topic by referring to [Creating a Topic](#).
2. You can add one or more subscriptions to a topic by configuring the phone number, email address, function, platform application endpoint, DMS endpoint, or HTTP/HTTPS endpoint for receiving alarm notifications. For details, see [Adding a Subscription](#).
3. Confirm the subscription. After the subscription is added, confirm the subscription.

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

Step 6 Click **OK**.

 **NOTE**

To disable the alarm notification function, deselect **DDoS attack** in [Figure 3-27](#) and click **OK**.

----End

3.6 Managing Instances

3.6.1 Viewing Information About an Instance

Scenarios


This section describes how to view information about an Advanced Anti-DDoS instance.

Prerequisites

You have purchased an AAD 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** page is displayed.

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

Step 4 On the displayed page, view the details about an instance. [Table 3-9](#) describes the parameters.

Figure 3-28 Instances

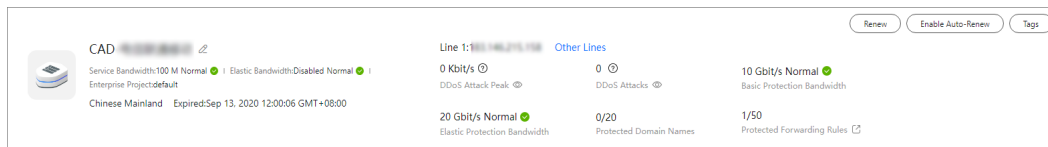



Table 3-9 Parameter description

Parameter	Description
Instance Name	<ul style="list-style-type: none"> Name of an AAD instance. You can click  on the right to change the name. Time when the instance expires Service bandwidth and protection bandwidth statuses of the instance Enterprise project to which the AAD instance belongs.
Service Bandwidth	Service bandwidth of the instance.
Elastic Bandwidth	Elastic service bandwidth of an instance.
Region	Region protected by the instance.
Line	Line and IP address information about an instance
Protection Information	Basic protection bandwidth, elastic protection bandwidth, number of protection ports, and number of protected domain names of the instance NOTE To change the elastic protection bandwidth, click Edit .
Security Statistics This Day	Protection statistics about the instance, including: <ul style="list-style-type: none"> Peak attack traffic Number of attacks

----End

3.6.2 Upgrading Instance Specifications

Scenarios

This section describes how to modify the basic protection bandwidth, elastic protection bandwidth, and service bandwidth for an AAD instance.

The number of protected domain names can be upgraded for website access instances, and the number of forwarding rules can be upgraded for IP access instances.

NOTE

- If a customer purchases a non-BGP triple-line instance (not for sale currently), the specifications cannot be upgraded. To change the elastic bandwidth, [submit a work order](#) for technical support.
- Only the service bandwidth and elastic protection bandwidth can be lowered.
- The lines cannot be changed during the upgrade.
- Expired instances do not support specifications upgrades.
- Frozen instances do not support specifications upgrades.

Prerequisites

You have the related permissions.

NOTICE

Ensure that the account used for upgrading the specifications of AAD instances has both the **CAD Administrator** and **BSS Administrator** roles or has the **Tenant Administrator** role.


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

Fees Description

Modifying specifications will lead to fee changes. For details, see [Pricing of a Changed Specification](#).

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** In the navigation pane on the left, choose **Advanced Anti-DDoS > Instance List**. The **Instance List** page is displayed.
- Step 4** On the displayed page, locate the target instance and click **Change Specifications**.
- Step 5** On the **Modify AAD Specifications** page, adjust the instance specifications.

Figure 3-29 Modifying specifications

The screenshot displays the 'Modify AAD Specifications' interface. At the top, a 'Current Configuration' table lists the following details:

Instance Name	CAD-hsk-test	Region	Chinese Mainland
Line	BGP	Billing Mode	Yearly/Monthly (26 days until expiration)
Service Bandwidth	100 Mbit/s	Elastic Bandwidth	Daily 95th percentile billing
Increase Elastic Bandwidth	100 Mbit/s	Basic Protection Bandwidth	10 Gbit/s
Elastic Protection Bandwidth	10 Gbit/s		

Below the table, several configuration options are shown with adjustable values:

- Basic Protection Bandwidth:** A dropdown menu with '10 Gbit/s' selected and '20 Gbit/s' as an alternative. A note below states 'This part is prepaid.'
- Elastic Protection Bandwidth:** A dropdown menu with '10 Gbit/s' selected and other options including 20 Gbit/s, 30 Gbit/s, 40 Gbit/s, 50 Gbit/s, 60 Gbit/s, 70 Gbit/s, 80 Gbit/s, 100 Gbit/s, 150 Gbit/s, and 200 Gbit/s.
- Service Bandwidth:** A numeric input field with '100' and 'Mbit/s'.
- Forwarding Rules:** A numeric input field with '50'.
- Protected Domain Names:** A numeric input field with '50'.

A note at the bottom of the Elastic Protection Bandwidth section reads: 'This is the maximum protection bandwidth. If you set this parameter to the same value as the basic protection bandwidth, no additional charges will ensue. If you set it to a value larger than the basic protection bandwidth, additional charges ensue when attack traffic exceeding the basic protection bandwidth is cleaned.'

- Step 6** After you click **Submit**, the system will determine whether the configuration has changed. If the configuration does not change, the system displays a failure message indicating that selected specifications are the same as original specifications. If the configuration has changed, the **Details** page is displayed.
- Step 7** Click **Submit Order**. When the payment is successful, the **Order submitted successfully** page is displayed.

----End

3.6.3 Changing the Elastic Protection Bandwidth

You can change the elastic protection bandwidth if it is insufficient.

This section describes how to change the elastic protection bandwidth for an AAD instance.

NOTE

- The adjustment of the elastic protection bandwidth does not involve prepayment.
- If a customer purchases a non-BGP triple-line instance (not for sale currently), the specifications cannot be upgraded. To change the elastic bandwidth, [submit a work order](#) for technical support.

Prerequisites

You have purchased an AAD instance.

Procedure


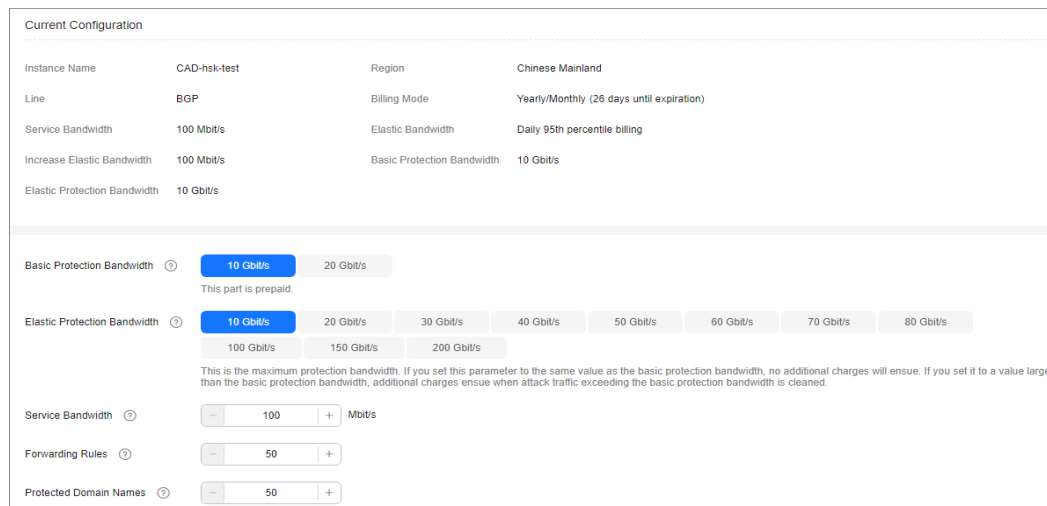
- Step 1** [Log in to the management console.](#)
- Step 2** Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS** page is displayed.
- Step 3** In the navigation pane on the left, choose **Advanced Anti-DDoS > Instance List**. The **Instance List** page is displayed.
- Step 4** On the displayed page, locate the target instance and click **Change Specifications**.
- Step 5** On the **Modify AAD Specifications** page, adjust the elastic protection bandwidth.

Figure 3-30 Modifying specifications



The screenshot displays the 'Modify AAD Specifications' interface. At the top, a 'Current Configuration' table lists instance details. Below this, several parameters are shown with adjustable values and buttons.

Current Configuration			
Instance Name	CAD-hsk-test	Region	Chinese Mainland
Line	BGP	Billing Mode	Yearly/Monthly (26 days until expiration)
Service Bandwidth	100 Mbit/s	Elastic Bandwidth	Daily 95th percentile billing
Increase Elastic Bandwidth	100 Mbit/s	Basic Protection Bandwidth	10 Gbit/s
Elastic Protection Bandwidth	10 Gbit/s		

Basic Protection Bandwidth	<input type="radio"/> 10 Gbit/s	<input type="radio"/> 20 Gbit/s						
This part is prepaid.								
Elastic Protection Bandwidth	<input type="radio"/> 10 Gbit/s	<input type="radio"/> 20 Gbit/s	<input type="radio"/> 30 Gbit/s	<input type="radio"/> 40 Gbit/s	<input type="radio"/> 50 Gbit/s	<input type="radio"/> 60 Gbit/s	<input type="radio"/> 70 Gbit/s	<input type="radio"/> 80 Gbit/s
	<input type="radio"/> 100 Gbit/s	<input type="radio"/> 150 Gbit/s	<input type="radio"/> 200 Gbit/s					
This is the maximum protection bandwidth. If you set this parameter to the same value as the basic protection bandwidth, no additional charges will ensue. If you set it to a value larger than the basic protection bandwidth, additional charges ensue when attack traffic exceeding the basic protection bandwidth is cleaned.								
Service Bandwidth	<input type="text" value="100"/>	Mbit/s						
Forwarding Rules	<input type="text" value="50"/>							
Protected Domain Names	<input type="text" value="50"/>							

- Step 6** After you click **Submit**, the system will determine whether the configuration has changed. If the configuration does not change, the system displays a failure message indicating that selected specifications are the same as original specifications. If the configuration has changed, the **Details** page is displayed.
- Step 7** Click **Submit Order**. When the payment is successful, the **Order submitted successfully** page is displayed.

----End

3.6.4 Enabling Auto-renewal

If you have enabled auto-renewal when purchasing an AAD instance, when the service period expires, the system automatically renews the instance for another period. You can enable auto-renewal based on your service requirements.

NOTE

If auto-renewal is enabled for a resource, you can manually renew the resource at any time. After the manual renewal is successful, the auto-renewal is still valid, and the system deducts the fee seven days before the manually renewed resource expires. For details about auto-renewal, see [Renewal Rules](#).

Prerequisites


You have purchased an AAD instance.

Constraints

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

Procedure

Step 1 [Log in to the management console.](#)

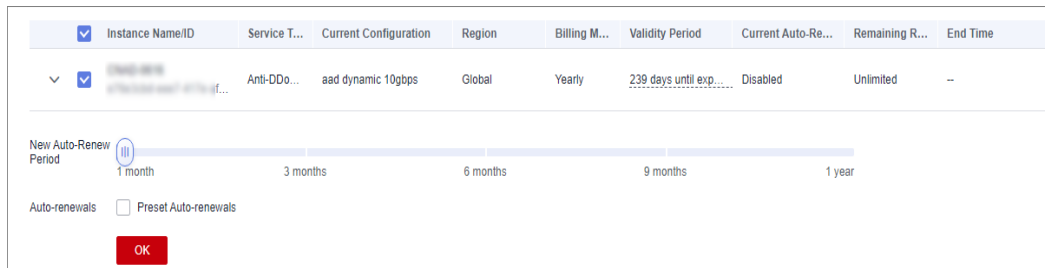
Step 2 Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

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

Step 4 In the row containing the desired instance, click **Enable Auto-Renewal**. The **Enable Auto-Renewal** page is displayed.

Step 5 On the **Enable Auto-Renewal** page, set **New Auto-Renew Period** and **Auto-renewals**.

Figure 3-31 Enabling auto-renewal



Step 6 Click **OK** and enable auto-renewal as prompted.


----End

3.6.5 Configuring Instance Tags

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

Procedure

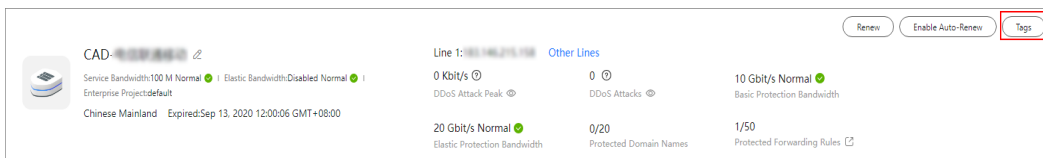
Step 1 [Log in to the management console.](#)

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 **Advanced Anti-DDoS > Instance List**. The **Instance List** page is displayed.

Step 4 Locate the row that contains the target AAD instance and click **Tags**.

Figure 3-32 Adding a tag for an AAD instance

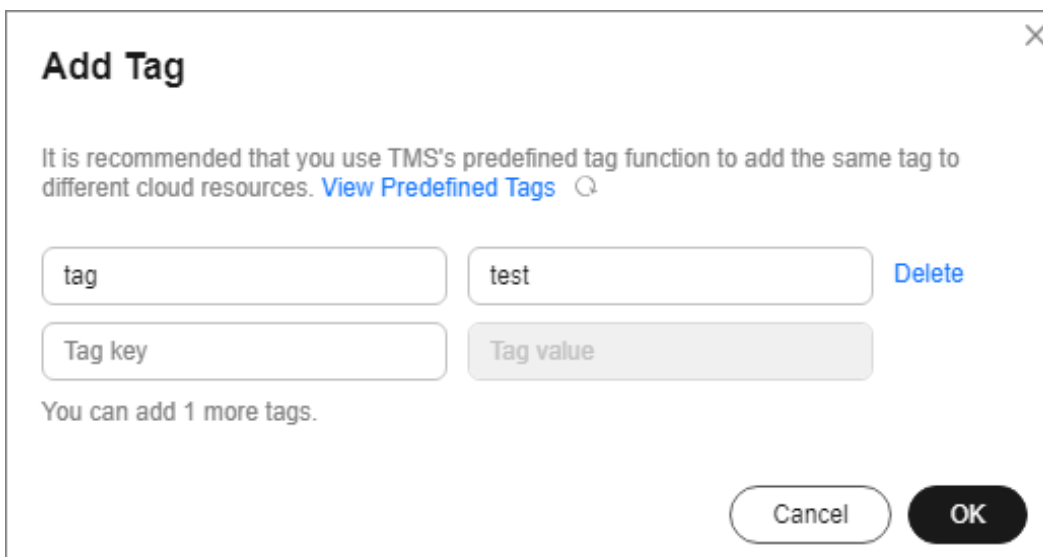


Step 5 On the tag adding page, click **Add Tag** to add a tag.

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 3-33 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

3.7 Managing Domain Names

3.7.1 Viewing Information About a Domain Name

Scenarios


This topic describes how to view information about a domain name.

Prerequisites

At least one domain name has been added for protection.

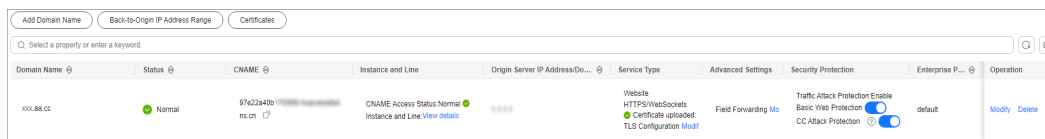
Procedure

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 **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-34 Domain name access



Step 4 View information about the domain name.

Table 3-10 Parameter description

Parameter	Description
Domain Name	Protected domain name
CNAME	<ul style="list-style-type: none">CNAME record obtained for the domain name after a CNAME resolutionClick  to copy the CNAME record.
Instance and Line	<ul style="list-style-type: none">CNAME-based access status of the domain nameClick View details to view details about the line of the domain name.Enable CNAME-based Auto Scheduling so that DNS resolution will automatically schedule the traffic if the high-defense IP address is blocked by a black hole.
Origin Server IP Address/Domain name	IP address or domain name of the origin server.

Parameter	Description
Service Type	<ul style="list-style-type: none">• Service type of the domain name• Locate the row that contains HTTPS/WebSockets certificate, click Update in the Service Type column to update the certificate. For details, see Updating a Certificate.
Security Protection	Status of traffic attack protection, basic web protection, and CC attack protection <ul style="list-style-type: none">• For a website service whose Origin Server Type is set to IP address, you can enable basic web protection and CC attack protection for your domain name.• For a website service whose Origin Server Type is set to Domain name, you do not need to enable basic web protection and CC attack protection for your domain name.• For a non-website service, only traffic attack defense is provided and enabled by default.
Enterprise Project	Enterprise project that the instance belongs to.

----End

3.7.2 Updating a Certificate

For website services connected to AAD, if **Protocol/Port** is set to **HTTPS/WebSockets** and **Origin Server Type** is set to **IP address**, you need to upload a certificate (only TLS 1.0, TLS 1.1, and TLS 1.2 certificates are supported) to associate the certificate with the protected domain name.

- If the purchased certificate is about to expire, you are advised to purchase a new certificate before the expiration date and update the certificate associated with the domain name in AAD.
- To update the certificate associated with a domain name, you can associate a new certificate with the domain name in AAD.

NOTICE


- The certificate takes effect 1 minute after it is updated. Therefore, update certificates in off-peak hours.
- If a certificate expires, the origin server will be affected more severely than the host crash and website access failure. Therefore, you are advised to update the certificate before the certificate expires.
- Each domain name must be associated with a certificate. A wildcard domain name can only be used for a wildcard domain certificate. If you have not purchased a wildcard domain certificate and have only a single-domain certificate, you can only add domain names one by one in AAD.

Prerequisites

Website services have been connected to AAD.

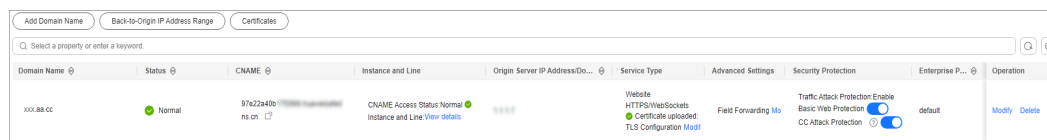
Procedure

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 **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-35 Domain name access



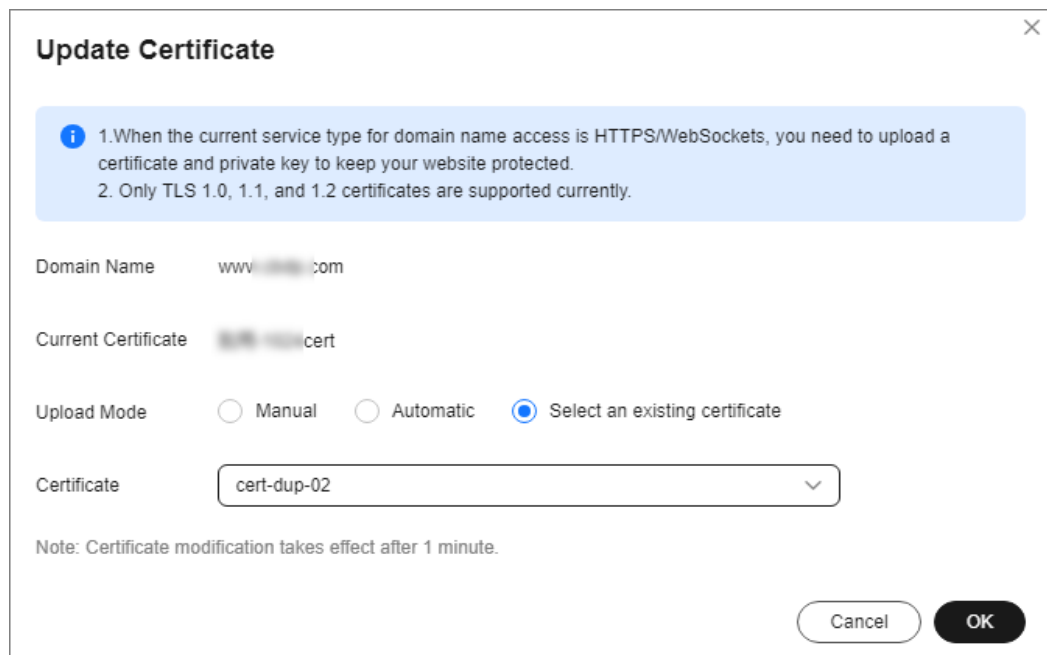
Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Enterprise P...	Operation
xxx.xx.cc	Normal	97a22a4b...ns.cn	CNAME Access Status Normal Instance and Line View details		Website HTTPS/WebSockets Certificate uploaded TLS Configuration Modify	Field Forwarding Mo	Traffic Attack Protector Enable Basic Web Protection <input checked="" type="checkbox"/> CC Attack Protection <input checked="" type="checkbox"/>	default	Modify Delete

Step 4 Locate the row that contains the target domain name, and click **Update** in the **Service Type** column.

Step 5 In the displayed **Update Certificate** dialog box, upload a new certificate or select an existing certificate.

- **Manual:** Enter the certificate name and paste the certificate and private key text. Currently, only PEM certificates are supported. For details about how to convert non-PEM certificates, see [Table 3-11](#).
- **Automatic:** Select an issued certificate.
- **Select an existing certificate:** Select the certificate that is in use.

Figure 3-36 Replacing a certificate



Update Certificate

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

Domain Name: www.com

Current Certificate:cert

Upload Mode: Manual Automatic Select an existing certificate

Certificate: cert-dup-02

Note: Certificate modification takes effect after 1 minute.

[Cancel](#) [OK](#)

Table 3-11 Certificate format conversion commands

Format	Conversion Method
CER/CRT	Rename the cert.crt certificate file to cert.pem .
PFX	Use OpenSSL to convert the certificate. Obtain a private key. For example, run the following command to convert cert.pfx into cert.key : openssl pkcs12 -in cert.pfx -nocerts -out cert.key -nodes Obtain a certificate. For example, run the following command to convert cert.pfx into cert.pem : openssl pkcs12 -in cert.pfx -nokeys -out cert.pem
P7B	Use OpenSSL to convert the certificate. 1. Run the following command to convert the certificate: openssl pkcs7 -print_certs -in incertificat.p7b -out cert.cer 2. Obtain the certificate content in cert.cer . 3. Save the content in .pem format.
DER	Use OpenSSL to convert the certificate. 1. Obtain a private key. For example, run the following command to convert privatekey.der into privatekey.pem : openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem 2. Obtain a certificate. For example, run the following command to convert cert.cer into cert.pem : openssl x509 -inform der -in cert.cer -out cert.pem

 **NOTE**

Before running the openssl command in Windows, ensure that the [OpenSSL](#) tool has been installed.

Step 6 Click **OK**.

----End

3.7.3 Modifying Resolution Lines for High-Defense IP Addresses of a Domain Name

Scenarios

This topic describes how to:

- Disable DNS resolution for a high-defense IP address.
- Add a resolution line for a domain name.
- Delete a resolution line for a domain name.

- Export all forwarding rules of a domain name.

Precautions


The modified resolutions lines take effect in about five minutes.

Prerequisites

At least one domain name has been added for protection.

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 **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.



Figure 3-37 Domain name access



Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Enterprise P...	Operation
xxx.ae.cc	Normal	97a22a40b... ns.cn	CNAME Access Status: Normal Instance and Line: View details		Website HTTPS/WebSockets Certificate uploaded TLS Configuration: Modify	Field Forwarding: Mo	Traffic Attack Protection: Enable Basic Web Protection: On CC Attack Protection: On	default	Modify Delete

Step 4 In the row containing the desired domain name, click **View details** in the **Instance and Line** column.

Step 5 Modify the resolution lines for the domain name.

- Disable DNS resolution for a high-defense IP address of the domain name.
On the details page of the domain name, locate the target line and set **DNS Resolution** to  to disable DNS resolution for the high-defense IP address. After you disable DNS resolution, you can still use the A record for the high-defense IP address.
- Add a resolution line for the domain name.
 - a. On the line details page, click **Add Instance Line**.
 - b. In the **Add Instance Line** dialog box, select instances and lines and click **OK**.
 - c. Set **Line Resolution Switch** to  to enable DNS resolution for the high-defense IP addresses.
- Delete a resolution line for the domain name.
 - a. Disable DNS resolution for the high-defense IP address. For details, see [Disabling DNS Resolution](#).
 - b. Click **Delete Line**.
 - c. Click **OK**.

- Export all rules.
On the line details page, click **Export All** to export all forwarding rules of the domain name.

----End

3.7.4 Modifying Domain Name Configuration

Scenarios

This topic describes how to modify the domain name configuration of a website service.

Prerequisites

A website service domain name has been added.

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 **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.

Figure 3-38 Domain name access



Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/Do...	Service Type	Advanced Settings	Security Protection	Enterprise P...	Operation
xxx.a8.cc	Normal	97e22a40b... ns on	CNAME Access Status Normal Instance and Line View details		Website HTTPS/WebSockets Certificate uploaded TLS Configuration Mod	Field Forwarding On	Traffic Attack Protection Enable Basic Web Protection On CC Attack Protection On	default	Modify Delete

- Step 4** In the row containing the desired domain name, click **Modify** in the **Operation** column.
- Step 5** In the **Modify Domain Name** dialog box that is displayed, modify the domain name configurations.

NOTE

- If this protected domain name will share a high-defense IP address and port with another domain name, ensure that they have the same **Origin Server Type** value.
- To change the **Origin Server Type** value from **IP address** to **Domain name**, ensure that **Basic Web Protection** is disabled for the domain name.

Figure 3-39 Modifying the domain name configuration

Modify Domain Name

Domain Name: www.***.com

Origin Server Type: Origin Server IP Address Domain name

Forwarding Protocol	Origin Server Port	Operation
HTTP	80	Delete
HTTPS	1818	Delete

+ You can add 2 more origin server configurations.

Origin Server IP Address/Domain Name: ****

If your origin server has been exposed, click [here](#) to get a solution.

Cancel OK

Step 6 Click **OK**.

----End

3.7.5 Deleting a Domain Name

Scenarios

You can delete domain names that you do not want to protect.

NOTICE

Before deleting a domain name, you need to ensure that the DNS domain name provider has changed the CNAME record to the real IP address. Otherwise, deleting the domain name will lead to service unavailability.

Prerequisites

At least one domain name has been added for protection.

Procedure

Step 1 [Log in to the management console](#).


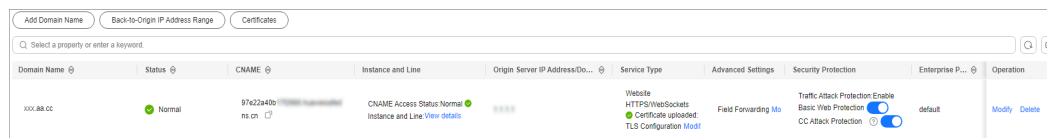
- Step 2** Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.
- Step 3** In the navigation pane on the left, choose **Advanced Anti-DDoS > Domain Name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

Figure 3-40 Domain name access

Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/DO...	Service Type	Advanced Settings	Security Protection	Enterprise P...	Operation
xxx.a8.cc	Normal	97622a4b...ms.cn	CNAME Access Status Normal Instance and Line: View Details		Website HTTPS/WebSockets Certificate uploaded TLS Configuration Modf	Field Forwarding Mo	Traffic Attack Protection Enable Basic Web Protection CC Attack Protection	default	Modify Delete

- Step 4** Locate the row containing the target domain name and click **Delete** in the **Operation** column.
- Step 5** Click **OK**.

----End

3.7.6 Configuring Field Forwarding

AAD lets you configure field forwarding for domain names to add fields to the header and send it to the origin server.

Prerequisites

The domain name has been added to AAD.

Constraints

- You can configure up to eight key/value pairs.
- Note that the key value of a custom header field cannot be the same as any native Nginx fields.
- The value can be set to a custom string or a variable starting with \$. Variables starting with \$support only the following fields:

```
$time_local  
$request_id  
$connection_requests  
$tenant_id  
$project_id  
$remote_addr  
$remote_port  
$scheme  
$request_method  
$http_host  
$origin_uri  
$request_length  
$ssl_server_name  
$ssl_protocol  
$ssl_curves  
$ssl_session_reused
```

Procedure

- Step 1** [Log in to the management console](#).


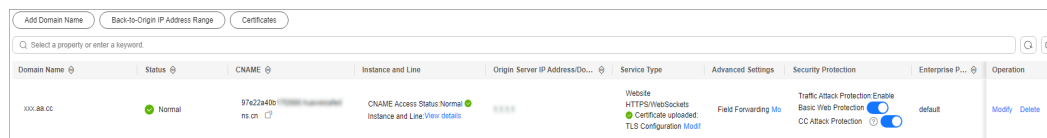
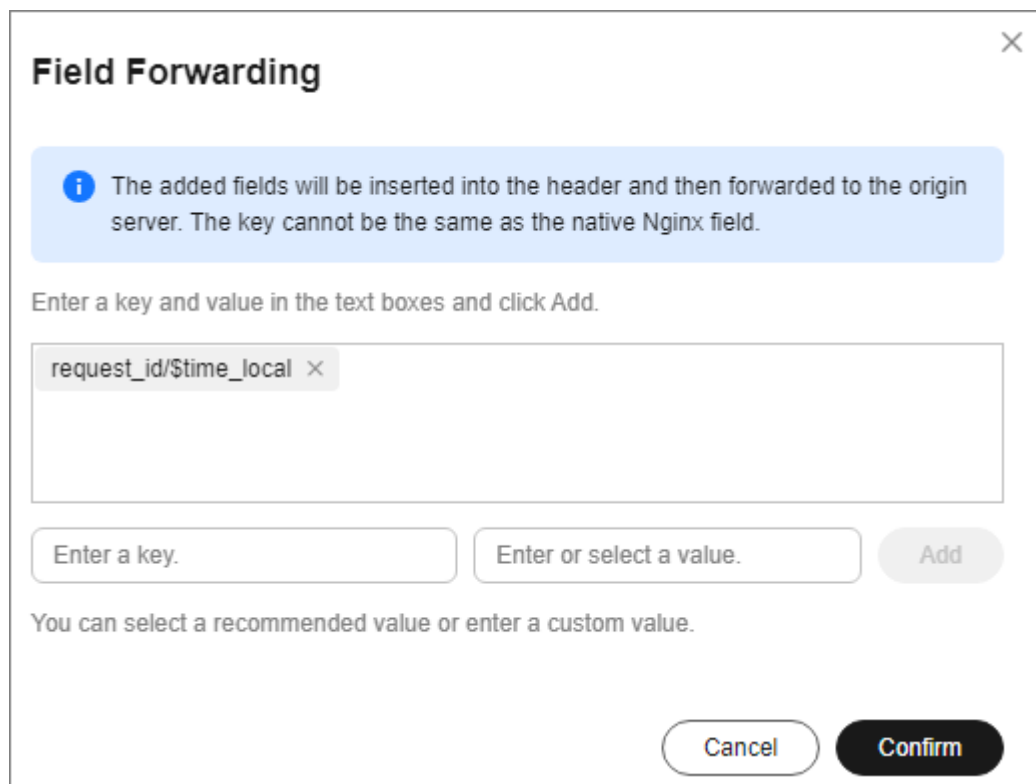
- Step 2** Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.
- Step 3** In the navigation pane on the left, choose **Advanced Anti-DDoS > Domain Name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

Figure 3-41 Domain name access

- Step 4** In the **Advanced Setting** column of the row containing the target domain name, click **Modify**.
- Step 5** Enter the Key/Value value and click **Add**.

Figure 3-42 Forwarding rule fields

- Step 6** Click **OK**.
- End

3.7.7 Modify TLS Configuration


AAD allows you to change the TLS version and cipher suite of the HTTPS certificate.

Prerequisites

Certificate uploaded:

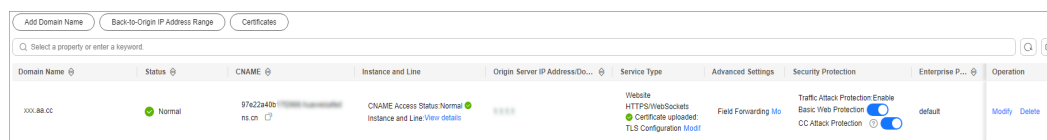
Procedure

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 **Advanced Anti-DDoS > Domain Name Access**. The **Domain Name Access** page is displayed.

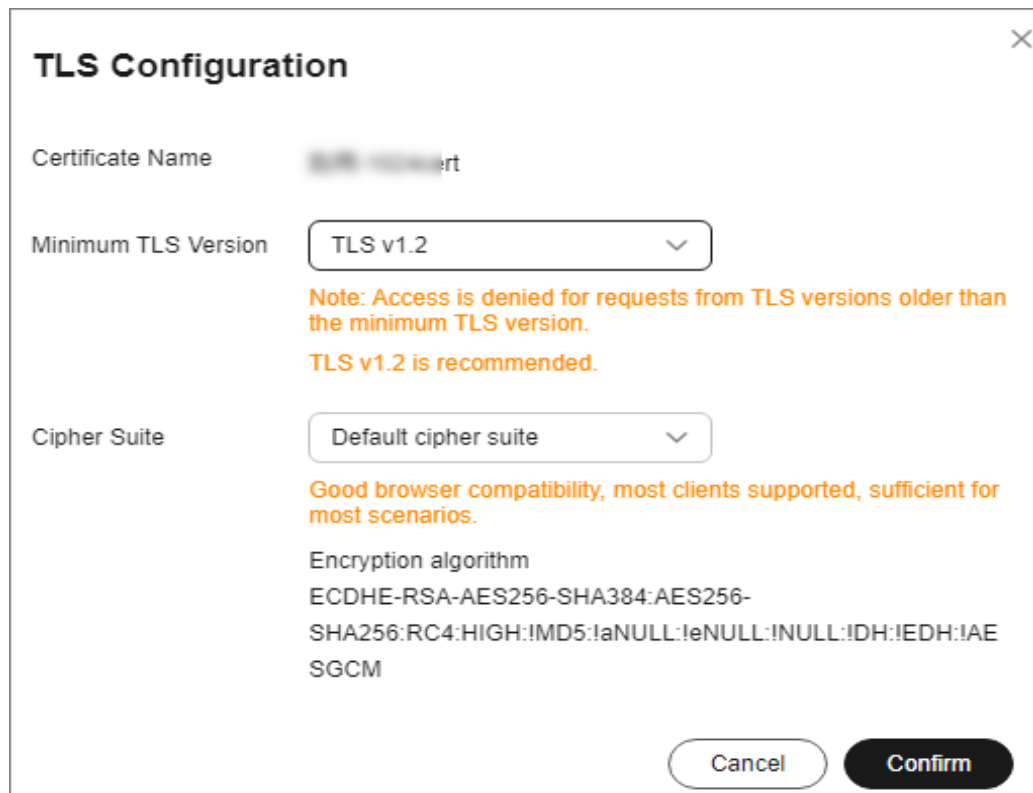
Figure 3-43 Domain name access



Step 4 Click **Edit** next to **TLS Configuration** of the target domain name.

Step 5 After selecting the TLS version and cipher suite, click **Confirm**.

Figure 3-44 Forwarding rule fields



----End

3.8 Managing Protection Logs

3.8.1 Viewing Protection Details

Scenarios

After your services are connected to AAD, you can view the DDoS and CC protection details of different lines in an AAD instance on the dashboard to learn about the current network security state.

On the **Dashboard** page, you can view the following protection details:

- **DDoS Attack Protection**
The **Dashboard** page gives an overview of the peak ingress traffic, peak attack traffic, and number of DDoS attacks, and shows the attack type distribution, DDoS attack events, and top 5 attack types scrubbed on two tab pages **Traffic** and **Packet Rate**.
- **CC Attack Protection**
The **Dashboard** page gives an overview of number of requests and attacks, attack type distribution, and top 5 attacked source IP addresses.

Precautions


- The protection details cannot be downloaded.
- On the **Dashboard** page, you can view the following protection details of the following time ranges:
 - **DDoS Attack Protection**
You can select an AAD instance and a line to view the DDoS protection details of last 24 hours, last 3 days, last 7 days, last 30 days, or a custom period (maximum of last 90 days).
 - **CC Attack Protection**
You can select a specific domain name or all domain names from the domain name drop-down list to view the CC protection details of yesterday, today, last 3 days, last 7 days, or last 30 days.

Prerequisites

You have purchased an AAD instance.

Viewing DDoS Attack Protection Details

Step 1 [Log in to the management console](#).

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

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

Step 4 Click the **DDoS Attack Protection** tab.

Step 5 Select an instance, line, and time range (last 24 hours, last 3 days, last 7 days, last 30 days, or a custom period). **Table 3-12** describes the related parameters.

Figure 3-45 DDoS attack protection

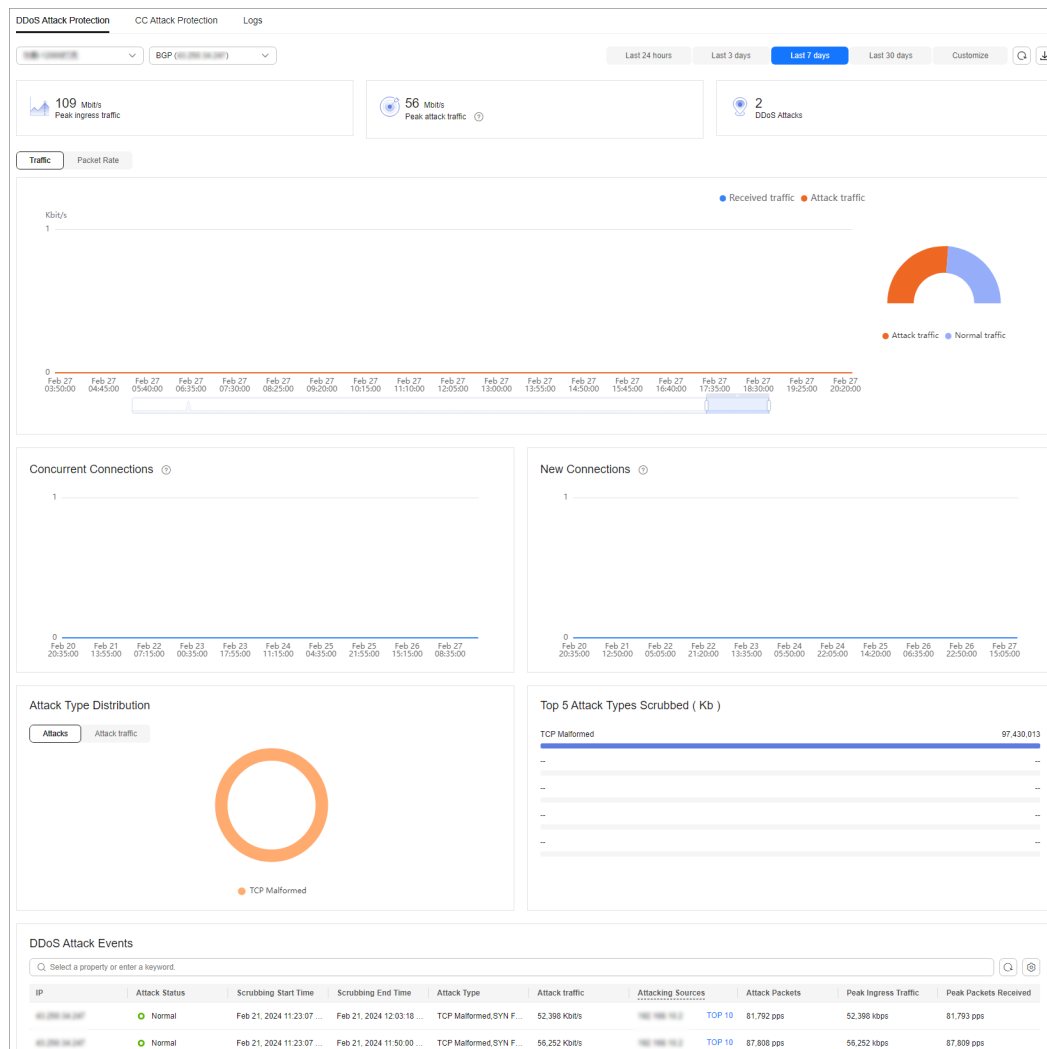


Table 3-12 Parameter description

Parameter	Description
Peak ingress traffic	Maximum traffic accessing the specified IP address of a specified instance per second
Peak attack traffic	Maximum traffic attacking the specified IP address of a specified instance per second
DDoS Attacks	Number of DDoS attacks launched on the specified IP address of a specified instance

Parameter	Description
Traffic	Trend charts of received traffic and attack traffic
Packet Rate	Trend charts of received packets and attack packets
Attack Type Distribution	Types of attack events <ul style="list-style-type: none">You can click Attacks then click any colored section in the displayed circle to see the type, count, and percentage of an attack.You can click Attack traffic then click any colored section in the displayed circle to see the type, traffic, and traffic percentage of an attack.
Top 5 Attack Types Scrubbed (Kbit/s)	Top 5 attack types that have been scrubbed
DDoS Attack Events	Details about DDoS attacks <ul style="list-style-type: none">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. <p>NOTE</p> <p>Note the following points about the attack source field in the DDoS attack event report:</p> <ul style="list-style-type: none">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.

 NOTE


In the traffic or packet chart on the **DDoS Attack Protection** page, the display granularity varies according to the query interval. The details are as follows:

- Query time < 20 minutes: The display granularity is 1 minute.
- 20 minutes < Query time < 40 minutes: The display granularity is 2 minutes.
- 40 minutes < Query time < 60 minutes: The display granularity is 3 minutes.
- 1 hour < Query time ≤ 6 hours: The display granularity is 5 minutes.
- 6 hours < Query time ≤ 24 hours: The display granularity is 10 minutes.
- 1 day < Query time ≤ 7 days: The display granularity is 30 minutes.
- 7 days < Query time ≤ 15 days: The display granularity is 1 hour.
- 15 days < Query time ≤ 30 days: The display granularity is 14 hours.

----End

Viewing CC Attack Protection Details

Step 1 [Log in to the management console.](#)

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

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

Step 4 Click the **CC Attack Protection** tab.

Step 5 Select a domain name and time range. For details about related parameters, see [Table 3-13](#).

Table 3-13 Parameter description

Parameter	Description
Requests	Total number of requests to a specified domain name If you select All domain names , the total number of requests to all domain names with WAF enabled is collected.
Peak Request Rate	Maximum number of requests to a specified domain name per second If you select All domain names , the maximum number of requests to all domain names with WAF enabled is collected per second.
Attacks	Number of attacks towards a specified domain name
Attacking Sources	Number of sources that attack a specified domain name

Parameter	Description
Request Statistics	<ul style="list-style-type: none">• Requests: trend chart for the access requests• Attacks: trend chart for attacks
Attack Type Distribution	Types of attack events <ul style="list-style-type: none">• You can click any colored area in the attack distribution circle under Attack Type Distribution to view the type, count, and proportion of an attack.• To stop displaying information about a specific type of attacks, click the legend with the same color to the right of the circle.
Top 5 Attacking Source IP Addresses	Top 5 attacking source IP addresses and their cumulative number of attacks

----End

3.9 Permissions Management

3.9.1 Creating a User and Granting the AAD Access Permission

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

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

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

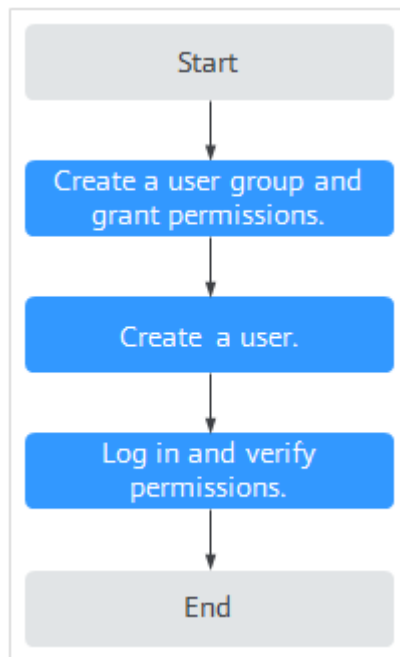
This section describes the procedure for granting permissions (see [Figure 3-46](#)).

Prerequisites


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

Process

Figure 3-46 Process for granting permissions



1. **Create a user group and assign permissions** to it.
Create a user group on the IAM console, and assign the **AAD FullAccess** permission to the group.
2. **Create an IAM user.**
Create a user on the IAM console and add the user to the group created in **1**.
3. **Log in** and verify the user's permissions.
Log in to the management console as the created user, and verify the user's permissions.

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

3.9.2 Creating an AAD Custom Policy

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

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

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

For details, see [Creating a Custom Policy](#). This section contains examples of typical AAD custom policies.

Example of Custom AAD Policies

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

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

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

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

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

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

3.9.3 AAD Permissions and Actions

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

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

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

Supported Actions

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

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

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

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

3.10 Monitoring

3.10.1 Setting Event Alarm Notifications

Scenarios

Cloud Eye can monitor AAD events and generate alarms when events such as black hole, scheduling, and attacks occur. It helps you learn about the protection status of AAD in a timely manner.

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

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 3-14](#).

Figure 3-47 Alarm parameters

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

- Name:** alarm-r2h
- Description:** (Empty text area)
- Alarm Type:** Event
- Event Type:** System event
- Event Source:** Advanced Anti-DDoS
- Monitoring Scope:** All Resources
- Method:** Configure manually
- Alarm Policy:** A table with 4 columns: Event Name, Alarm Policy, Alarm Severity, and Operation. It lists four conditions: Blackhole event, Cancel Blackhole, Domain name sche..., and DDoS Attack Events, all with an immediate trigger and a count of 1.
- Alarm Notification:** Enabled (toggle on)
- Notification Recipient:** Notification group
- Notification Group:** --Select--
- Notification Window:** Daily, 00:00 - 23:59 GMT+08:00
- Trigger Condition:** Generated alarm and Cleared alarm (both checked)

Table 3-14 Description

Parameter	Description
Name	Name of the rule. The system generates a random name and you can modify it.
Description	Description about the rule.
Alarm Type	Select Event .
Event Type	Choose System Event .
Event Source	Choose Advanced Anti-DDoS .
Monitoring Scope	Select All resources .
Method	The default option is Configure manually .
Event Name	You are advised to select Blackhole Event , Cancel Blackhole , Domain Name Scheduling Event , and DDoS Attack Event .

Parameter	Description
Trigger Mode	You can select Immediate trigger or Accumulative trigger based on the operation severity.
Alarm Severity	Alarm severity, which can be Critical , Major , Minor , or Informational .

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 3-15 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 Notification group or Topic subscription as required.
Notification Group	This parameter takes effect when Notification Recipient is set to Notification group . Set this parameter based on the site requirements.
Notification Object	This parameter is valid only when Notification Recipient is set to Topic Subscription . 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

3.10.2 Configuring Monitoring Alarm Rules

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

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

If you need to customize more metrics, you can report them to Cloud Eye through API requests. For details, see [Adding Monitoring Data](#) and [AAD Monitoring Metrics](#).

Prerequisite

Purchasing an AAD 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, as shown in [Configuring AAD alarm rules](#). For details about how to enter the alarm rule information, see [Table 3-16](#).

Figure 3-48 Configuring AAD alarm rules

The screenshot shows the configuration interface for an AAD alarm rule. It is divided into several sections:

- Name:** A text input field containing "alarm-tuum".
- Description:** A text area with a character count of "0/256".
- Alarm Type:** Two tabs, "Metric" (selected) and "Event".
- Resource Type:** A dropdown menu set to "DDoS".
- Dimension:** A dropdown menu set to "Instance ID".
- Monitoring Scope:** Two tabs, "All resources" (selected) and "Specific resources". A note below states: "If you select All resources, an alarm notification will be sent when any instance meets an alarm policy, and existing alarm rules will be automatically applied for newly purchased resources."
- Method:** Three tabs: "Associate template" (selected), "Use existing template", and "Configure manually". A note below states: "After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly."
- Template:** A dropdown menu set to "--Select--" with a "Create Custom Template" link.
- Alarm Notification:** A toggle switch that is turned on.
- Notification Recipient:** Two tabs, "Notification group" (selected) and "Topic subscription".
- Notification Group:** A dropdown menu set to "--Select--" with a refresh icon.

At the bottom, a note reads: "If you create notification group, you must click refresh to make it available for selection. After you create the notification group, click Add Notification Object in the Operation column of the notification group list to add notification objects."

Table 3-16 AAD alarm rule parameters

Parameter	Description
Name	Name of the rule. The system generates a random name and you can modify it.
Description	Description about the rule.
Alarm Type	Alarm type
Resource Type	Select DDoS from the drop-down list box.
Dimension	Select the resource dimension to be monitored. <ul style="list-style-type: none">● Instance ID: indicates the instance dimension.● Instance ID-Protected IP address: indicates the IP address dimension.
Monitoring Scope	Scope where the alarm rule applies to. You can select All resources , Resource groups or Specific resources .


Parameter	Description
Method	You can select Associate template , Use existing template , or Configure manually . For details about how to create a custom template, see Creating a Custom Template . NOTE After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.
Template	Select a template.
Alarm Notification	Whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message.
Notification Recipient	Specifies the receiving method of the alarm notification. You can select Notification group or Topic subscription . <ul style="list-style-type: none">Account contact is the mobile phone number and email address provided for registration.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 Creating a Topic and Adding Subscriptions.
Notification Group (Valid when Notification Recipient is set to Notification group)	Select the group to be notified.
Topic subscription (Valid when Notification Recipient is set to Topic subscription)	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 Generated alarm when an alarm is generated or Cleared alarm 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

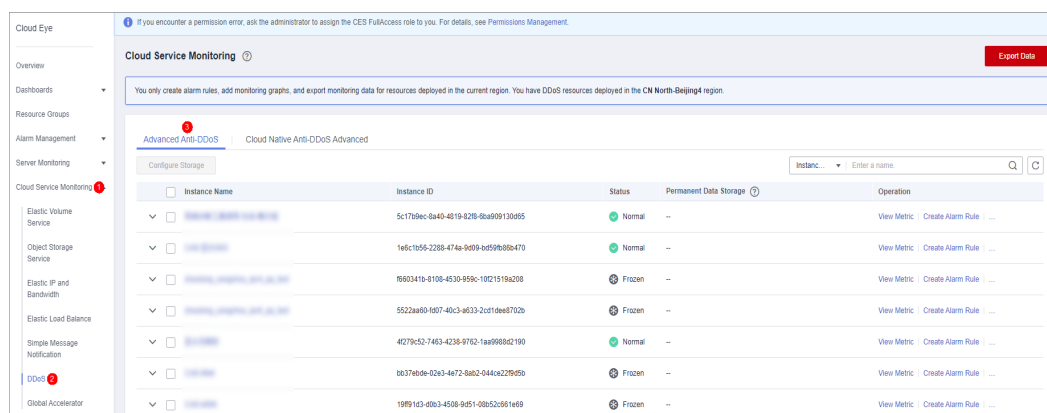
Step 1 [Log in to the management console](#).

Step 2 Click  in the upper left corner of the management console and select a region or project.

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

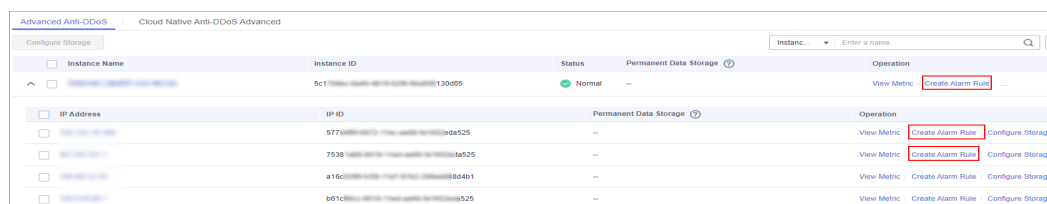
Step 4 In the navigation pane on the left, choose **Cloud Service Monitoring > DDoS**. The **Advanced Anti-DDoS** page is displayed.

Figure 3-49 AAD monitoring



Step 5 Locate the row that contains the object to be monitored, and click **Create Alarm Rule**.

Figure 3-50 Selecting the monitored object



Step 6 Enter the alarm rule information, as shown in [Configuring AAD alarm rules](#). For details about how to enter the alarm rule information, see [Table 3-17](#).

Figure 3-51 Configuring AAD alarm rules

* Name: alarm-p88r

Description: [Empty text box]

* Alarm Type: Metric

* Resource Type: DDoS

* Dimension: Instance ID - Protected IP address

* Monitoring Scope: Specific resources

* Monitored Objects: [Empty list]

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

* Template: -Select- [Create Custom Template]

Alarm Notification:

* Notification Recipient: Notification group | Topic subscription

* Notification Group: -Select- [Create]

If you create notification group, you must click refresh to make it available for selection. After you create the notification group, click Add Notification Object in the Operation column of the notification group list to add notification objects.

* Notification Window: Daily 00:00 - 23:59 GMT+08:00

* Trigger Condition: Generated alarm Cleared alarm

Advanced Settings | Enterprise Project | Tag

Table 3-17 AAD alarm rule parameters

Parameter	Description
Workspace Name	Name of the rule. The system generates a random name and you can modify it.
Description	Description about the rule.
Alarm Type	Retain the default value.
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 Associate template , Use existing template , or Configure manually . For details about how to create a custom template, see Creating a Custom Template . NOTE After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.
Template	Select a template.
Alarm Notification	Whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message.
Notification Recipient	Specifies the receiving method of the alarm notification. You can select Notification group or Topic subscription . <ul style="list-style-type: none">Account contact is the mobile phone number and email address provided for registration.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 Creating a Topic and Adding Subscriptions.
Notification Group (Valid when Notification Recipient is set to Notification group)	Select the group to be notified.
Topic subscription (Valid when Notification Recipient is set to Topic subscription)	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 Generated alarm when an alarm is generated or Cleared alarm when an alarm is triggered, or both.

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

----End



3.10.3 Viewing Monitoring Metrics

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

Prerequisite

You have configured alarm rules on the Cloud Eye console. For more details, see [Configuring Monitoring Alarm Rules](#).

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.

NOTE

In the upper right corner of the page, you can click **Select Metric** to modify the monitoring metrics.

----End

3.10.4 AAD Monitoring Metrics

Description

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

Namespaces

SYS.DDOS

NOTE

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

Metrics

Table 3-18 AAD monitoring metrics

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
ip_drop_rate	Discarded traffic	Specifies the bandwidth for discarding traffic of high-defense IP addresses.	≥0kb/s	Advanced Anti-DDoS	5 minutes
instance_drop_rate	Discarded traffic	Specifies the discarded traffic bandwidth of an AAD instance.	≥0kb/s	Advanced Anti-DDoS	5 minutes
ip_back_to_source_rate	Retrieval bandwidth	Specifies the retrieval traffic bandwidth of the high-defense IP address.	≥0kb/s	Advanced Anti-DDoS	5 minutes
instance_back_to_source_rate	Retrieval bandwidth	Specifies the retrieval traffic bandwidth of AAD instances.	≥0kb/s	Advanced Anti-DDoS	5 minutes
ip_internet_in_rate	Inbound Traffic	Specifies the inbound traffic bandwidth of the high-defense IP address.	≥0kb/s	Advanced Anti-DDoS	5 minutes
instance_internet_in_rate	Inbound traffic	Specifies the inbound traffic bandwidth of an AAD instance	≥0kb/s	Advanced Anti-DDoS	5 minutes

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
ip_new_connection	New connections	Specifies the number of new connections to the high-defense IP address.	≥0count/s	Advanced Anti-DDoS	5 minutes
instance_new_connection	New Connections	Specifies the number of new connections of an AAD instance.	≥0count/s	Advanced Anti-DDoS	5 minutes
ip_concurrent_connection	Concurrent connections	Concurrent connections to the high-defense IP address.	≥0count/s	Advanced Anti-DDoS	5 minutes
instance_concurrent_connection	Concurrent connections	Concurrent connections to the AAD instance.	≥0count/s	Advanced Anti-DDoS	5 minutes
ip_service_bandwidth_usage	Service bandwidth usage	Service bandwidth usage of the high-defense IP address service.	≥0%	Advanced Anti-DDoS	5 minutes
instance_service_bandwidth_usage	Service bandwidth usage	Service bandwidth usage of an AAD instance.	≥0%	Advanced Anti-DDoS	5 minutes

Dimensions

Key	Value
zone_ip	Instance - Protected IP Address

Key	Value
instance_id	Instance ID

3.11 Auditing

3.11.1 AAD Operations Supported by CTS

CTS provides records of AAD operations. With CTS, you can query, audit, and backtrack these operations. For details, see [Cloud Trace Service User Guide](#).

Table 3-19 lists Anti-DDoS Service operations recorded by CTS.

Table 3-19 AAD operations that can be recorded by CTS


Operation	Resource Type	Event Name
Adding a domain name	domainDns	domainDns
Deleting a domain name.	deleteDomain	deleteDomain
Purchase operations	cadOpen	cadOpen
Enabling/Disabling CNAME automatic scheduling	cnameDispatchSwitch	cnameDispatchSwitch
Uploading or modifying a certificate	domainCert	domainCert
Enabling/Disabling basic Web protection and CC protection	domainSwitch	domainSwitch
Editing a domain name.	domainConfigEdit	domainConfigEdit
Adding a forwarding rule	addProtocolRule	addProtocolRule
Adding forwarding rules in batches	importProtocolRule	importProtocolRule
Deleting forwarding rules in batches	batchDelProtocolRule	batchDelProtocolRule
Deleting a forwarding rule	deleteProtocolRule	deleteProtocolRule

3.11.2 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 **AAD**, and press **Enter**.

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

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

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

----End

4 Anti-DDoS Scheduling Center Protection Management

4.1 Purchasing Anti-DDoS Scheduling Center Protection

Before using the anti-DDoS scheduling center, you need to purchase scheduling rule quotas. After the purchase is successful, the anti-DDoS scheduling center starts working immediately. You need to configure a tiered scheduling policy.

Procedure

Purchasing Anti-DDoS Scheduling Center Protection

- Step 1** [Log in to the management console](#).
- Step 2** Hover the mouse over the **Service List** icon, choose **Security & Compliance > Anti-DDoS**, and click **Advanced Anti-DDoS**.
- Step 3** In the displayed **DDoS Migration Center** page, choose **DDoS Scheduling Center > Tiered Scheduling**.
- Step 4** Click **Buy DDoS Mitigation** in the upper right corner of the page.
 - **Rules:** Each rule can be used for 10 IP addresses. You can purchase multiple rules to schedule more IP addresses.
 - **Required Duration:** You can select one to **1 month, 2 months, 3 months, 6 months, or 1 year**.
 - **Auto-renew:** Enable or disable auto-renewal as needed.
- Step 5** Confirm the specifications and click **Submit Order** in the lower right corner to complete the payment.

----End

Upgrading Specifications

After purchasing anti-DDoS scheduling center protection, you can upgrade the specifications to purchase more rules.

- Step 1** [Log in to the management console.](#)
- Step 2** Hover the mouse over the **Service List** icon, choose **Security & Compliance > Anti-DDoS**, and click **Advanced Anti-DDoS**. In the displayed **DDoS Migration Center** page, choose **DDoS Scheduling Center > Tiered Scheduling**.
- Step 3** Click **Upgrade**, as shown in [Figure 4-1](#). On the **Upgrade** page, set the number of rules you need to purchase, as shown in [Figure 4-2](#).

Figure 4-1 Upgrading quotas

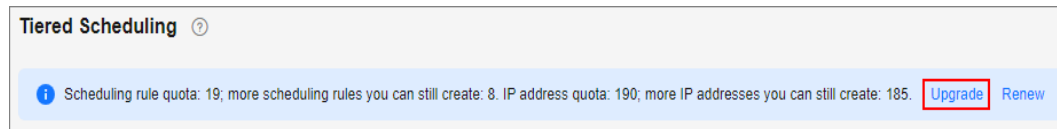
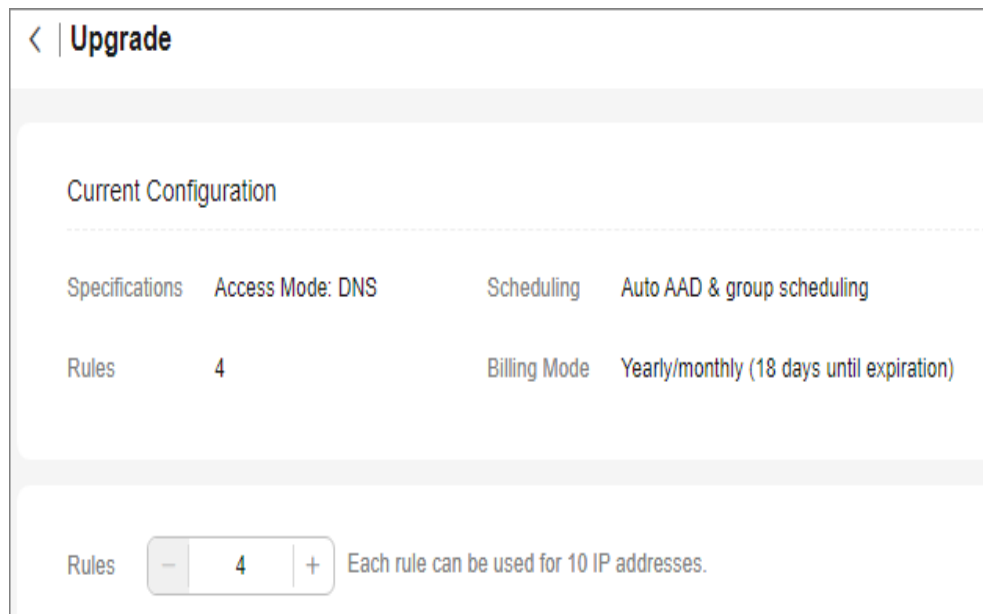


Figure 4-2 Purchasing rules



- Step 4** Click **Submit** in the lower right corner to complete the payment.

----End

Renewing

If your anti-DDoS scheduling center protection expires, you can renew it as required.

- Step 1** [Log in to the management console.](#)
- Step 2** Hover the mouse over the **Service List** icon, choose **Security & Compliance > Anti-DDoS**, and click **Advanced Anti-DDoS**. In the displayed **DDoS Migration Center** page, choose **DDoS Scheduling Center > Tiered Scheduling**.
- Step 3** Click **Renew**, as shown in [Figure 4-3](#). Set the renewal duration and determine whether to select **Renewal Date** as required, as shown in [Figure 4-4](#).

Figure 4-3 Renew

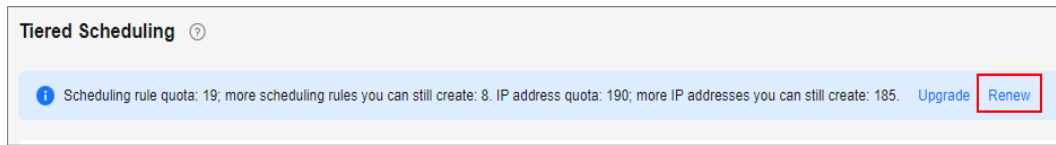
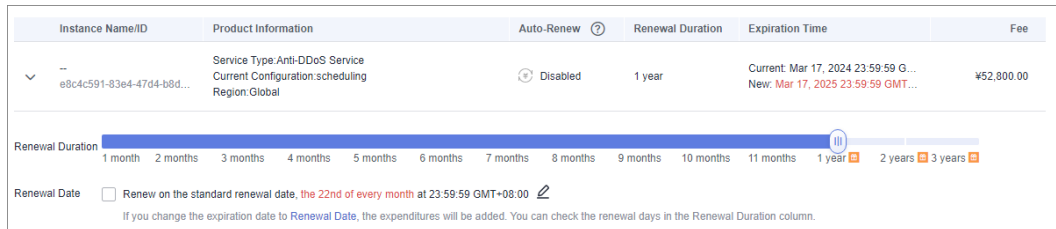


Figure 4-4 Purchasing specifications



NOTE

- If you change service specifications before the renewal period starts, you can unsubscribe from the service, but cannot cancel the renewal period.
- Renewed resources are not eligible of a 5-day unconditional unsubscription.

Step 4 Click **Submit** in the lower right corner to complete the payment.

----End

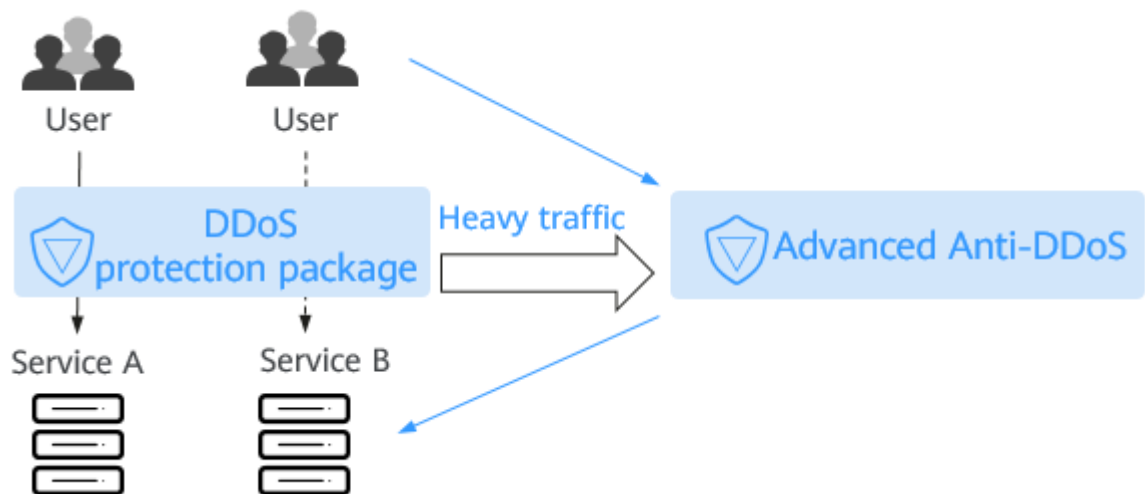
4.2 Configuring Tiered Scheduling Policies

If you enabled auto AAD when purchasing CNAD Unlimited Protection Basic, you can configure a tiered scheduling policy to automatically engage AAD for cloud resources protected by CNAD Unlimited Protection Basic.

Working Principles

Figure 4-5 shows how does CNAD Advanced automatically start AAD.

Figure 4-5 How auto AAD is started



Prerequisites

The protected object has been connected to AAD.

Constraints

- Auto AAD protects only the cloud resources protected by CNAD.
- You need to configure different origin server IP addresses for CNAD Advanced and AAD.
- Currently, the Anti-DDoS scheduling center does not support IPv6 addresses.

For details about how to configure the origin server IP address, see [Step 1: Configuring a Protected Domain Name \(Website Services\)](#).

Procedure

Step 1 [Log in to the management console](#).

Step 2 Hover the mouse over the **Service List** icon, choose **Security & Compliance > Anti-DDoS**, and click **Advanced Anti-DDoS**.

Step 3 In the displayed **DDoS Migration Center** page, choose **DDoS Scheduling Center > Tiered Scheduling**.

Step 4 In the upper left corner of the tiered scheduling list, click **Create Rule**.

Step 5 In the dialog box that is displayed, set scheduling rule parameters. Parameters are listed in [Table 4-1](#).

Figure 4-6 Creating a scheduling rule

Create Rule ✕

* Name

* Scheduling Group ? **Only resources (such as ECS, EIP, ELB, and WAF) of cloud native anti-DDoS objects can be added.**

CN-North-Ula... Group [Delete](#)

+ Add Resource

* Auto AAD ? CNAD only CNAD and AAD


Table 4-1 Scheduling rule parameters

Parameter	Description
Name	Name of the scheduling rule. NOTE A maximum of 10 cloud resource IP addresses can be added to a rule. If you purchased N rules, a maximum of $N \times 10$ cloud resource IP addresses can be added.
Scheduling Group	Site, IP address, and scheduling group where the rule belongs to. IP address resolution starts from the group 1 and is performed by group. IP addresses in the same group will be resolved at the same time. Default group: 1 NOTE <ul style="list-style-type: none">• A blocked IP address in a group will be skipped.• If all IP addresses in a group are blocked, the system will automatically start resolution for the next group. If no IP address in any group is available, the system starts AAD.• Only resources (such as ECS, EIP, ELB, and WAF) of cloud native anti-DDoS objects can be added.
Auto AAD	<ul style="list-style-type: none">• CNAD only: AAD will not be started to defend your servers against large volumetric DDoS traffic.• CNAD and AAD: If you have purchased AAD, it will be started for large volumetric DDoS traffic.

Step 6 Click **OK**.

----End

Related Operations

- To delete a rule, click **Delete** in the **Operation** column of the row containing the target scheduling rule.
- To view the details of a rule, click **View Details** in the **Operation** column of the row containing the target scheduling rule.
 - In the **Basic Information** area, click  to modify the scheduling rule name and whether to enable joint scheduling.
 - Click **Add Resource**. In the displayed dialog box, you can modify, add, or delete the cloud resource IP address.
 - In the row containing the target resource, click **Delete** in the **Operation** column. You can also select the cloud resource to be deleted and click **Delete** in the upper left corner of the list to delete cloud resources in batches.

4.3 Enabling Tiered Scheduling Alarm Notifications

After you enable the alarm notification for the DDoS scheduling center, a notification message will be sent to you through the method you have configured when:

- An IP addresses in a tiered scheduling rule is blocked.
- An IP addresses in a tiered scheduling rule is unblocked.
- All IP addresses in a tiered scheduling rule are blocked.
- After all IP addresses in a tiered scheduling rule are blocked, one IP address is unblocked and can be scheduled.

Prerequisites

- Before enabling alarm notifications, you are advised to [create a topic](#) and [add a subscription](#) in **Simple Message Notification (SMN)**.
- The created topic needs to be confirmed by the subscriber. For details, see [Requesting Subscription Confirmation](#).
- The Anti-DDoS tiered scheduling policy has been successfully configured.

Procedure


- Step 1** [Log in to the management console](#).
- Step 2** Hover the mouse over the **Service List** icon, choose **Security & Compliance > Anti-DDoS**, and click **Advanced Anti-DDoS**. In the navigation pane on the left, choose **DDoS Scheduling Center > Alarm Notifications**.
- Step 3** On the **Alarm Notifications** page, enable alarm notifications, that is, set **Alarm Notifications** to .
- Step 4** Select a created topic from the **Notification Topic** drop-down list, as shown in [Figure 4-7](#).

Figure 4-7 Configuring alarm notifications



NOTE

- Only topics whose subscription status is **Confirmed** can be displayed in the drop-down list box.
- Only topics in the same region as the DDoS scheduling center can be displayed in the drop-down list box.
- You will be billed for using the Simple Message Notification (SMN) service. For billing details, see [Product Pricing Details](#).

Step 5 Click **Apply**.

----End

Related Operations

To disable alarm notifications, toggle off the **Alarm Notifications** function.

4.4 Configuring CDN Scheduling Rules

After CDN scheduling is enabled, AAD can be automatically called to protect cloud resources.

Prerequisites


- You have purchased and used CDN.
- You have purchased AAD.

Constraints

You need to [submit a work order](#) to contact the Anti-DDoS Service team to obtain the CDN scheduling permission.

Procedure

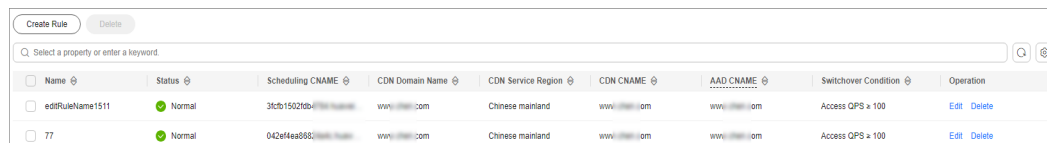
Step 1 [Log in to the management console](#).

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 **DDoS Scheduling Center > CDN Scheduling**.

Step 4 On the **CDN Scheduling** page, click **Create Rule**.

Figure 4-8 Creating a CDN scheduling rule



Name	Status	Scheduling CNAME	CDN Domain Name	CDN Service Region	CDN CNAME	AAD CNAME	Switchover Condition	Operation
editRuleName1511	Normal	3kcb15022db4	www.100.com	Chinese mainland	www.100.com	www.100.com	Access OPS > 100	Edit Delete
77	Normal	042ef4ea8682	www.100.com	Chinese mainland	www.100.com	www.100.com	Access OPS > 100	Edit Delete

Step 5 In the dialog box that is displayed, add the rule information. For details, see [Table 4-2](#).

Figure 4-9 Rule details

Create Rule

* Name

* CDN Domain Name
To synchronize protected domain names you need to contact your account manager or submit a service ticket to the DDoS Mitigation service team, as they need to apply for CDN authorization in advance. If you add protected domain names in the future, synchronize the added domain names to the DDoS Mitigation service team.

CDN Service Region: **Chinese mainland** | Outside Chinese mainland | Global
The service region of the added CDN domain name must be the same as that configured on the CDN page.

* CDN CNAME

* AAD CNAME

* Switchover Condition: Access QPS \geq

Table 4-2 Rule details

Parameter	Description
Name	Enter the name of a user-defined CDN scheduling rule.
CDN domain name	Enter a CDN domain name. The domain name can contain only letters, digits, hyphens (-), and periods (.), and cannot exceed 64 characters.
CDN service region	The region of the CDN domain name to be added must be the same as that configured on the CDN page. The supported service regions are Chinese mainland , Outside Chinese mainland , and Global .
CDN CNAME	Enter a CDN CNAME. The CDN CNAME can contain a maximum of 128 characters, including lowercase letters, digits, and periods (.).
AAD CNAME	Enter an AAD CNAME. The AAD CNAME can contain a maximum of 128 characters, including lowercase letters, digits, and periods (.).
Switchover condition	When the access QPS is greater than or equal to the configured value, scheduling is triggered. The value ranges from 100 to 10000.

Step 6 Click **OK**.

----End

Follow-up Operations

- Editing a rule: Locate the row that contains the target rule, click **Edit** in the **Operation** column. In the dialog box that is displayed, modify related parameters.
- Deleting a rule: Locate the row that contains the rule to be deleted, click **Delete** in the **Operation** column. In the dialog box that is displayed, click **OK**.

A Change History

Released On	Description
2024-02-29	<p>This issue is the fourth official release.</p> <ul style="list-style-type: none">• Added section Configuring Field Forwarding.• Added section Modify TLS Configuration.• Deleted section "Connecting Non-Domain Name Services to Advanced Anti-DDoS"• Deleted section "Managing Forwarding Rules".• Added the description of the dynamic blacklist in section Viewing Statistics Reports.• Added the description of the dynamic blacklist in section Viewing Protection Details.• Added protected IP address status parameters to the Viewing Details about a Protected Object .
2023-09-30	<p>This issue is the third official release.</p> <ul style="list-style-type: none">• Added section Usage Overview.• Added section Usage Overview.
2022-04-27	<p>This issue is the second official release.</p> <p>Updated the purchase parameters in Purchasing a CNAD Instance.</p>
2021-02-01	<p>This issue is the first official release.</p>