

Anti-DDoS

User Guide

Issue 04
Date 2024-12-02



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 Usage Overview.....	1
2 Setting a Protection Policy.....	2
3 Viewing a Public IP Address.....	6
4 Enabling Alarm Notifications.....	8
5 Setting Event Alarm Notifications.....	10
6 Configuring LTS for Anti-DDoS Logging.....	14
7 Viewing Monitoring Reports.....	19
8 Viewing Interception Reports.....	21
9 Audit.....	23
9.1 Anti-DDoS Operations That Can Be Recorded by CTS.....	23
9.2 Viewing CTS Traces.....	23
10 Permission Management.....	25
10.1 Creating a User Group and Assigning the Anti-DDoS Access Permission.....	25
10.2 Anti-DDoS Custom Policies.....	26
10.3 Anti-DDoS Permissions and Actions.....	27
10.4 Permission Dependency of the Anti-DDoS Console.....	29

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 .
Configuring Anti-DDoS logs on LTS	With Anti-DDoS logs recorded on LTS, users can perform real-time decision analysis, device O&M management, and service trend analysis in a timely and efficient manner. For details, see Configuring LTS for Anti-DDoS Logging .
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 .

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.

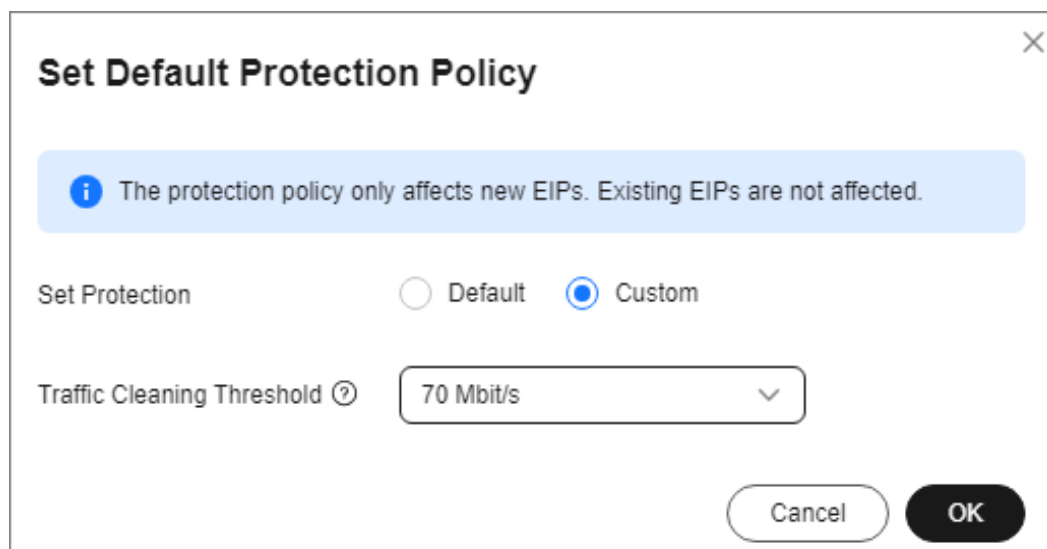
Manually Setting a Default Protection Policy

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 2-1](#).

Figure 2-1 Manually configuring the default protection policy**Table 2-1** 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

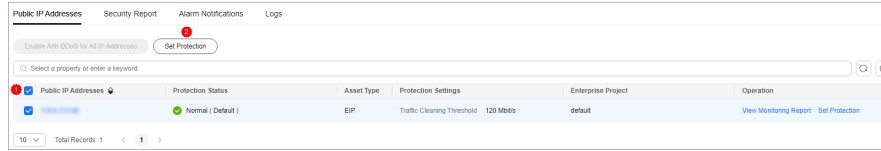
Step 1 [Log in to the management console.](#)

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

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

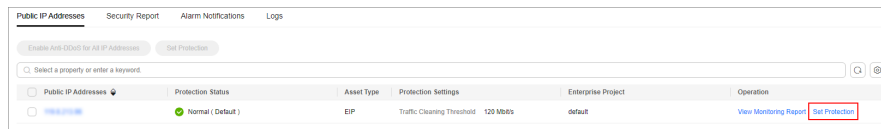
- To configure protection policies for multiple public IP addresses, select multiple public IP addresses and choose **Set Protection** in the upper part of the page.

Figure 2-2 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 2-3 Configuring a protection policy for a public IP address



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

Figure 2-4 Configuring a protection policy

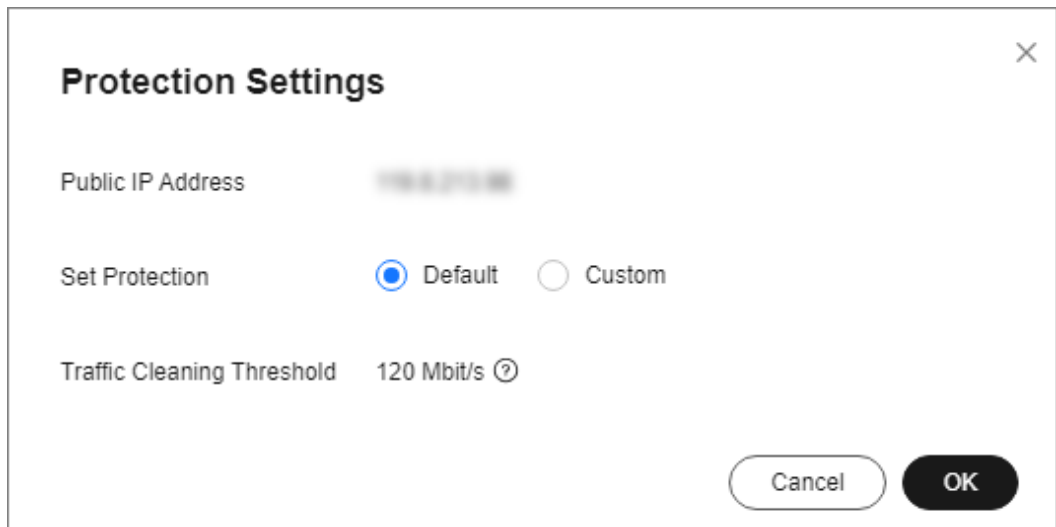


Table 2-2 Parameters for configuring a protection policy

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**

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.

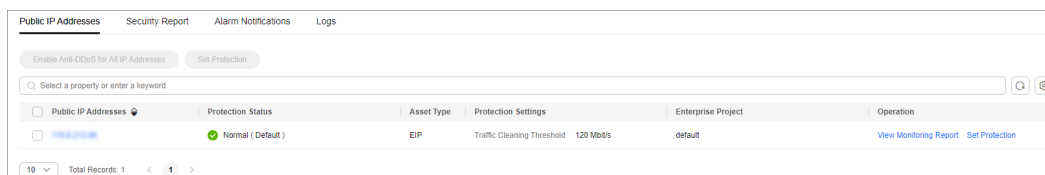
Procedure

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

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

Step 3 On the **Public IP Addresses** tab, view all protected public IP addresses. [Table 3-1](#) describes the parameters.

Figure 3-1 Viewing a public IP address



Public IP Addresses	Security Report	Alarm Notifications	Logs		
Enable Anti-DDoS for All IP Addresses Set Protection					
Select a property or enter a keyword.					
Public IP Addresses	Protection Status	Asset Type	Protection Settings	Enterprise Project	Operation
<input type="checkbox"/>	● Normal (Default)	EIP	Traffic Cleaning Threshold: 120 Mbits	default	View Monitoring Report Set Protection
10	Total Records: 1	< 1 >			

 **NOTE**

- Anti-DDoS provides protection for servers using IPv4 and IPv6 protocols against DDoS attacks.
- 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](#).
- Select a protection status from the search box. Only public IP addresses of that status are displayed on the **Public IP Addresses** page.

Table 3-1 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

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 the **region** in the upper part of the page, click  in the upper left corner of the page, and choose **Security > Anti-DDoS**. The **Anti-DDoS** page is displayed.
- Step 3** On the **Anti-DDoS** page, click the **Alarm Notifications** tab and configure the alarm notification. For details about the parameter settings, see [Table 4-1](#).

Figure 4-1 Configuring alarm notifications

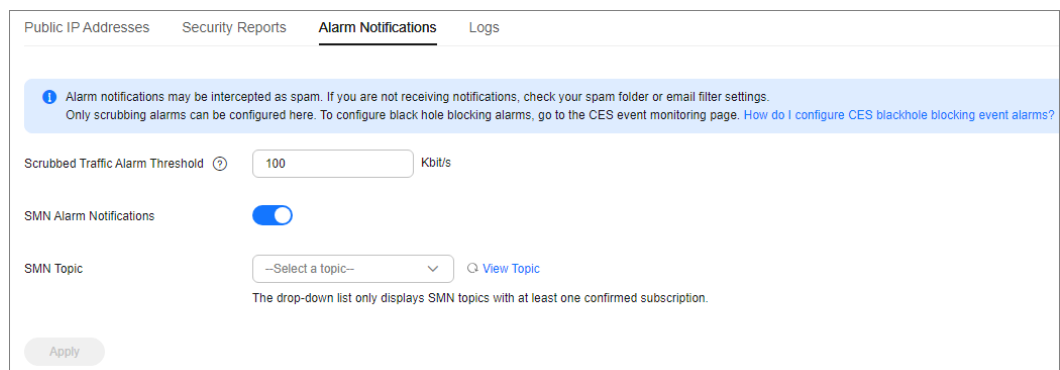




Table 4-1 Configuring alarm notifications

Parameter	Description
Scrubbed Traffic Alarm Threshold	When the volume of scrubbed traffic reaches the threshold, an alarm notification is sent. Set the threshold as required.
Alarm Notifications	Indicates whether the alarm notification function is enabled. There are two values: <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

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 5-1](#).

Figure 5-1 Alarm parameters

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

- Name:** alarm-c3a5
- Description:** (Empty text area)
- Alarm Type:** Event (selected)
- Event Type:** System event (selected)
- Event Source:** Elastic IP
- Monitoring Scope:** All resources
- Method:** Configure manually
- Alarm Policy Table:**

Event Name	Trigger Mode	Alarm Policy	Alarm Severity	Operation
Delete EIP	Immediate tr...	5 minutes - Occurrences >= 1 Count One day	Major	Delete
EIP blocked	Immediate tr...	5 minutes - Occurrences >= 1 Count One day	Major	Delete
EIP unblocked	Immediate tr...	5 minutes - Occurrences >= 1 Count One day	Major	Delete
Start DDoS traffic scrub...	Immediate tr...	5 minutes - Occurrences >= 1 Count One day	Major	Delete
Stop DDoS traffic scrub...	Immediate tr...	5 minutes - Occurrences >= 1 Count One day	Major	Delete
Enterprise-class OoS b...	Immediate tr...	5 minutes - Occurrences >= 1 Count One day	Major	Delete
- Alarm Notification:** Enabled
- Notification Object:** Account contact
- Notification Window:** Daily, 00:00 - 23:59
- Trigger Condition:** Generated alarm (checked)

Table 5-1 Parameters for configuring a protection policy

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

Parameter	Description
Alarm Policy	You are advised to select EIP blocked, EIP unblocked, Start Anti-DDoS traffic scrubbing, and Stop Anti-DDoS traffic scrubbing. When the traffic is greater than 10,000 kbit/s, the system sends an alarm notification when scrubbing starts and when scrubbing ends. When the traffic is less than 10,000 kbit/s, no alarm notification is sent.
Notification Recipient	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 5-2 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.

Parameter	Description
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

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 the **region** in the upper part of the page, click  in the upper left corner of the page, and choose **Security** > **Anti-DDoS**. The **Anti-DDoS** page is displayed.


Step 3 Click the **Configure Logs** tab, enable LTS () , and select a log group and log stream. [Table 6-1](#) describes the parameters.

Figure 6-1 Configuring logs

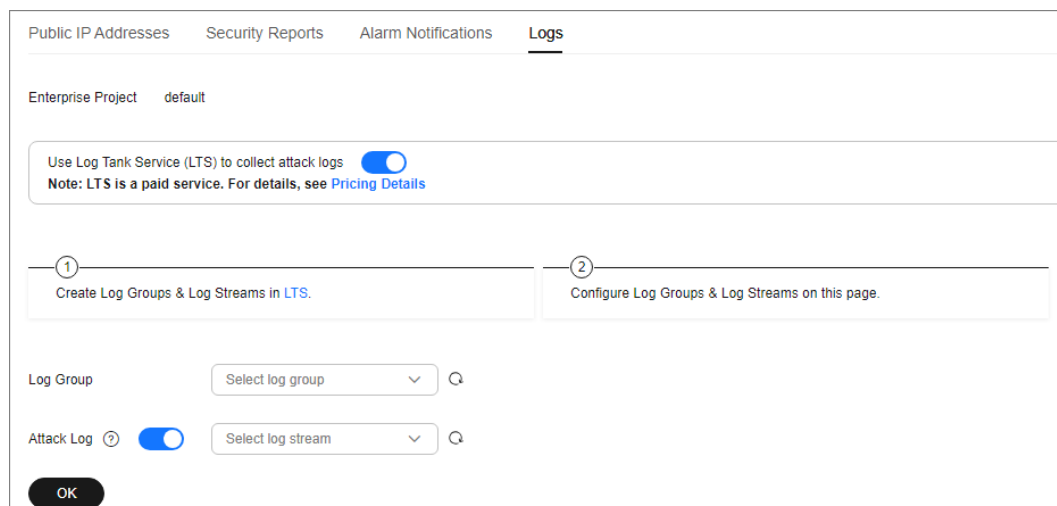


Table 6-1 Log configuration

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 6-2 Log field description

Field	Description
logType	Log type. The default value is ip_attack_sum , indicating attack logs.
deviceType	Type of the device that reports logs. The default value is CLEAN , indicating the scrubbing device.
inKbps	Inbound traffic, in kbit/s.
maxPps	Peak incoming traffic, in pps.
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 6-3 .
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.

Field	Description
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 6-3 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
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

Value	Attack Type
31	SIP flood attack
32	Blacklist dropping
33	Abnormal HTTP URL behavior
34	TCP fragment abnormal dropping traffic attack
35	TCP abnormal dropping traffic attack
36	UDP fragment abnormal dropping traffic attack
37	UDP abnormal dropping traffic attack
38	ICMP abnormal attack
39	Other abnormal attacks
40	Connection flood attack
41	Domain name hijacking attack
42	DNS poisoning packet attack
43	DNS reflection attack
44	Oversize DNS packet attack
45	Abnormal rate of DNS source requests
46	Abnormal rate of DNS source replies
47	Abnormal rate of DNS domain name requests
48	Abnormal rate of DNS domain name replies
49	DNS request packet TTL anomaly
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

Value	Attack Type
61	Domain name blocking
62	Filtering
63	Web attack packet capture
64	SIP source rate limiting


7 Viewing Monitoring Reports

Scenarios

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

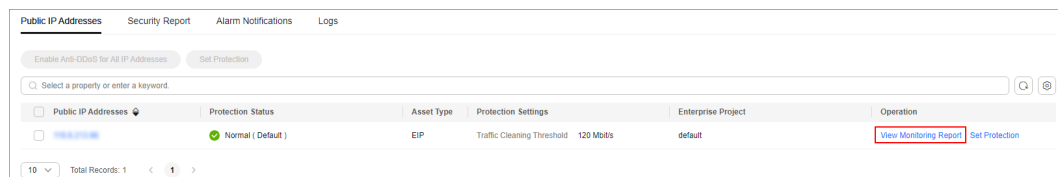
Procedure

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

Step 2 Select the **region** in the upper part of the page, click  in the upper left corner of the page, and choose **Security > Anti-DDoS**. 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 7-1 Viewing a monitoring report



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 7-2 Viewing a traffic monitoring report

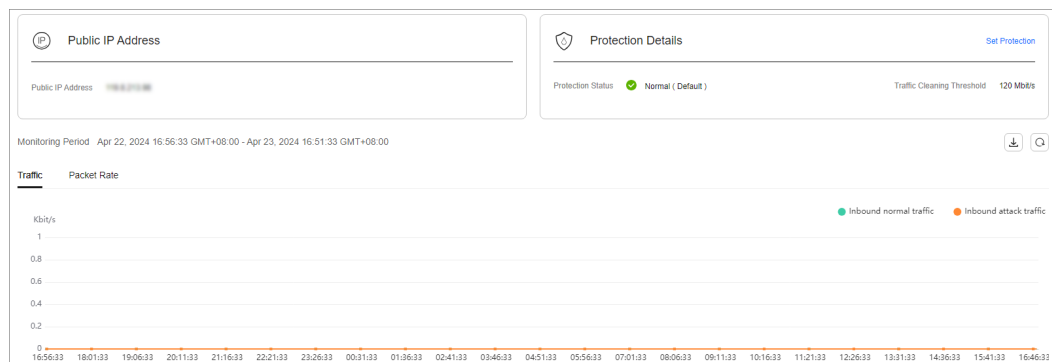
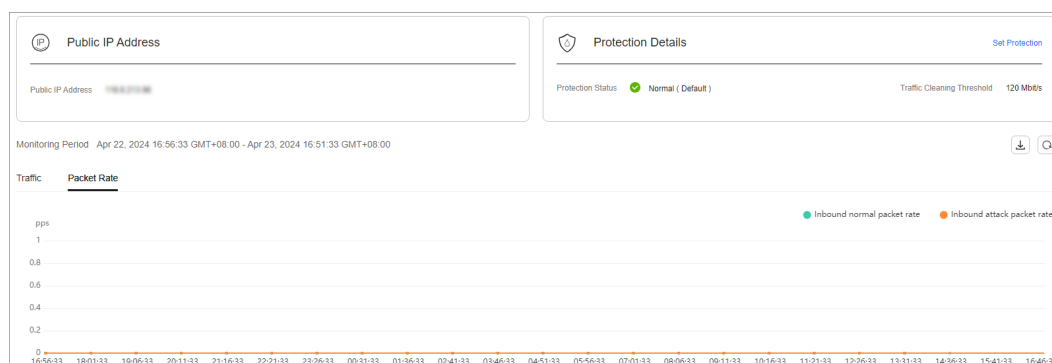



Figure 7-3 Viewing the packet rate



 **NOTE**

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

----End


8 Viewing Interception Reports

Scenarios

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

Procedure

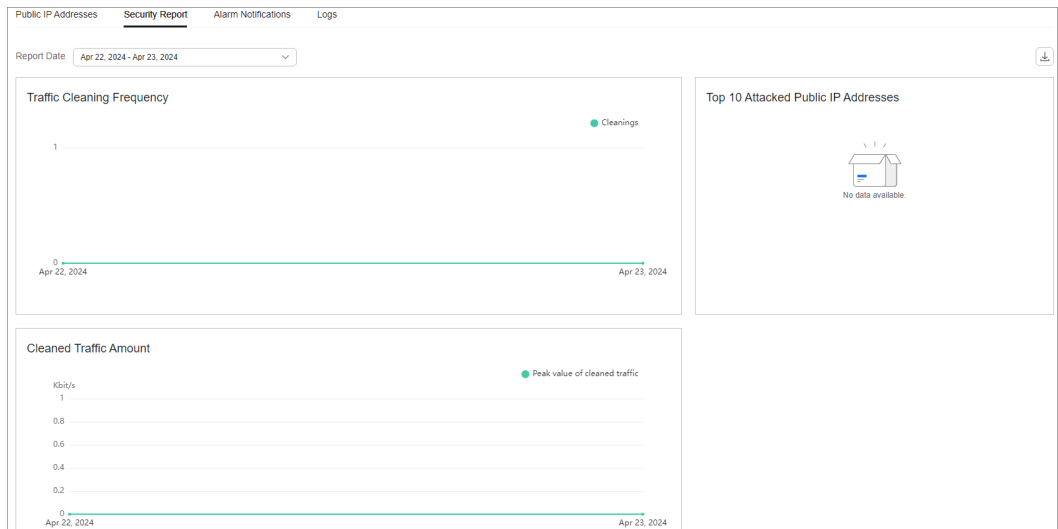
Step 1 [Log in to the management console.](#)

Step 2 Select the **region** in the upper part of the page, click  in the upper left corner of the page, and choose **Security > Anti-DDoS**. 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 8-1 Viewing an interception report



NOTE

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

----End

9 Audit

9.1 Anti-DDoS Operations That Can Be Recorded by CTS

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

Table 9-1 lists the Anti-DDoS operations that can be recorded by CTS.

Table 9-1 Anti-DDoS operations that can be recorded by CTS


Operation	Trace Name
Modifying Anti-DDoS service configurations	UPDATE_ANTIDDOS
Setting LTS full log configurations	UPDATE_LTS_CONFIG
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

9.2 Viewing CTS Traces

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

Procedure

Step 1 Log in to the management console.

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

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

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

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

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

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

----End

10 Permission Management

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

If you want to implement refined permission management for your Anti-DDoS service, With IAM, you can:

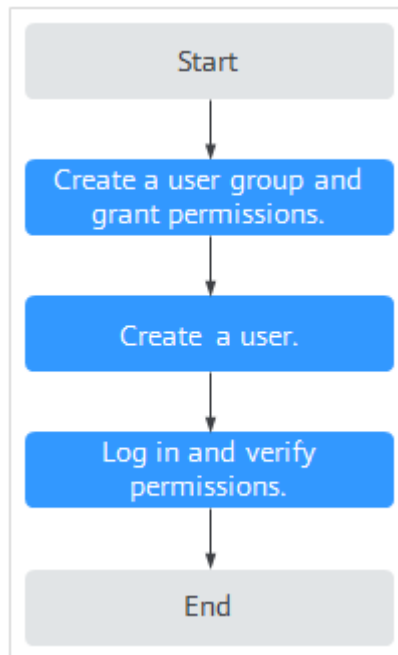
- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to Anti-DDoS resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust another Huawei Cloud account or cloud 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 10-1](#)).

Process

Figure 10-1 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.

10.2 Anti-DDoS Custom Policies

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

You can create custom policies using one of the following methods:

- 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"
      ]
    }
  ]
}

```

10.3 Anti-DDoS Permissions and Actions

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

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

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

Supported Actions

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

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

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

10.4 Permission Dependency of the Anti-DDoS Console

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

Dependency Policy Configuration

If an IAM user needs to view or use related functions on the console, ensure that the **Anti-DDoS Administrator policy** has been assigned to the user group to which the user belongs. Then, add roles or policies of dependent services based on the following [Table 10-1](#).

Table 10-1 Anti-DDoS console dependency policies and roles

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