Anti-DDoS

User Guide

Issue	09
Date	2021-10-09

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Contents

1 Setting a Default Protection Policy for Newly Purchased Public IP Addresses

In the **Set Default Protection Policy** dialog box, you can select **Manual** for **Protection Settings** and set the default protection policy. The new public IP addresses you purchase from HUAWEI CLOUD will be protected against DDoS attacks based on your configured default protection policy

If you want to disable the default protection policy, you can select **Default** for **Protection Settings** in the **Set Default Protection Policy** dialog box.

If you do not set a default protection policy for the newly purchased public IP addresses, the **Protection Settings** in **Default** mode apply to the IP addresses. The value of **Traffic Cleaning Threshold** is **120 Mbps** and **CC Defense** is disabled if you select **Default** for **Protection Settings** in the **Set Default Protection Policy** dialog box.

Prerequisites

You have obtained an account and its password for logging in to the management console.

Manually Setting a Default Protection Policy

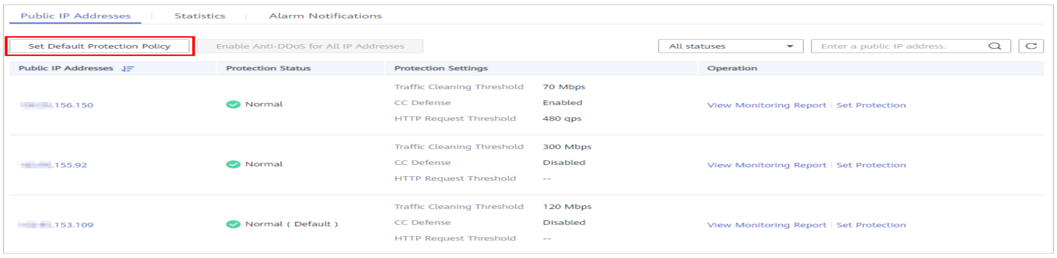
Step 1 Log in to the management console.

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 **Security & Compliance** > **Anti-DDoS**.

Step 4 Select the **Public IP Addresses** tab and click **Set Default Protection Policy**.

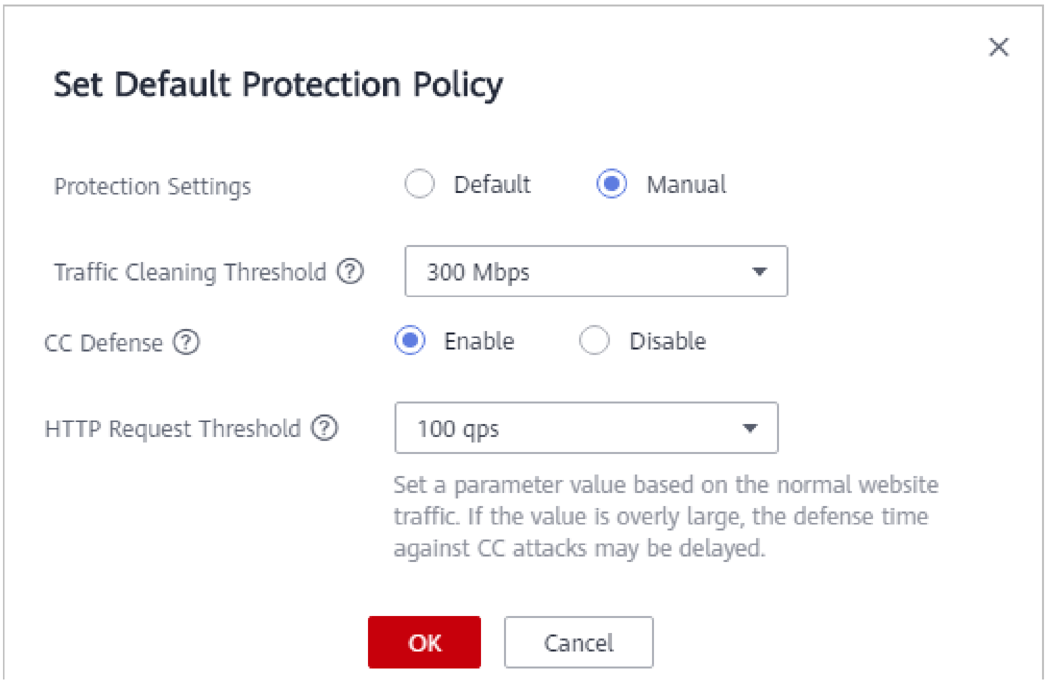
Figure 1-1 Setting a default protection policy for newly purchased public IP addresses


Public IP Addresses
Statistics
Alarm Notifications
Set Default Protection Policy
Enable Anti-DDoS for All IP Addresses
All statuses
Enter a public IP address.

Public IP Addresses	Protection Status	Protection Settings		Operation
[redacted].156.150	Normal	Traffic Cleaning Threshold CC Defense HTTP Request Threshold	70 Mbps Enabled 480 qps	View Monitoring Report | Set Protection
[redacted].155.92	Normal	Traffic Cleaning Threshold CC Defense HTTP Request Threshold	300 Mbps Disabled --	View Monitoring Report | Set Protection
[redacted].153.109	Normal (Default)	Traffic Cleaning Threshold CC Defense HTTP Request Threshold	120 Mbps Disabled --	View Monitoring Report | Set Protection

Step 5 In the displayed dialog box, select **Manual** for **Protection Settings**.

Figure 1-2 Manually configuring the default protection policy



Set Default Protection Policy

Protection Settings ○ Default ● Manual

Traffic Cleaning Threshold ⓘ 300 Mbps

CC Defense ⓘ ● Enable ○ Disable

HTTP Request Threshold ⓘ 100 qps

Set a parameter value based on the normal website traffic. If the value is overly large, the defense time against CC attacks may be delayed.

Step 6 Configure **Traffic Cleaning Threshold** and **CC Defense**.

Table 1-1 Parameter description

Parameter	Description
Traffic Cleaning Threshold	Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the threshold. You can set the traffic cleaning threshold based on based on your expected traffic volume. Set the threshold to a value closest to the purchased bandwidth but not greater than the purchased bandwidth. **NOTE** If service traffic triggers scrubbing, only attack traffic is intercepted. If service traffic does not trigger scrubbing, no traffic is intercepted. Set this parameter based on the actual service access traffic.

Parameter	Description
CC Defense	● **Disable**: disables the defense. ● **Enable**: enables the defense. **NOTE** CC defense is available only for clients that carry web services and support the full HTTP protocol stack. CC defense works in redirection or redirection+verification code mode. If your client does not support the full HTTP protocol stack, you are advised to disable CC defense.
HTTP Request Threshold	This parameter is required only when **CC Defense** is set to **Enable**. This parameter is used to defend against a large number of malicious requests targeting websites. Defense against CC attacks, which aim to exhaust server resources by sending specially crafted GET or POST requests, is triggered when the HTTP request rate on a site reaches the selected value. In EIP protection, the maximum recommended value is **5000**. In ELB protection, the value can be larger. Set this parameter to the maximum number of HTTP requests that can be processed by the deployed service. Anti-DDoS will automatically scrub traffic if detecting that the total number of requests exceeds the configured HTTP request threshold. If the value is too large, CC defense will not be triggered promptly.

Step 7 Click **OK**.

After you set the default protection policy, the newly purchased public IP addresses are protected based on the configured policy. For details about how to adjust a configured protection policy, see **Configuring an Anti-DDoS Protection Policy**.

----End

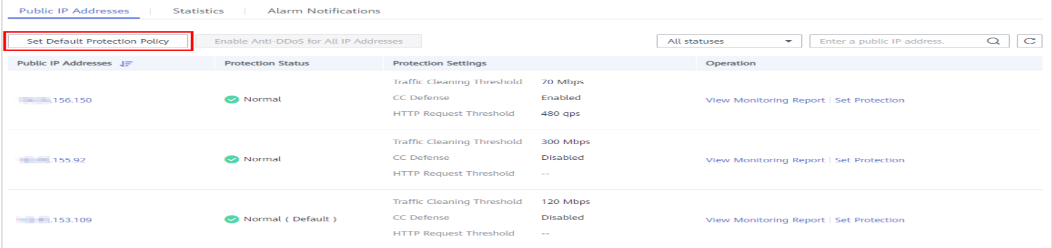
Disabling the Default Protection Policy Manually Configured for Newly Purchased IP Addresses

If you do not want the manually configured protection policy to apply to the new public IP addresses, you can disable it. Then, the **Protection Settings** in **Default** mode apply to the new IP addresses.

Step 1 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Anti-DDoS**.

Step 2 Select the **Public IP Addresses** tab and click **Set Default Protection Policy**.

Figure 1-3 Setting a default protection policy for newly purchased public IP addresses



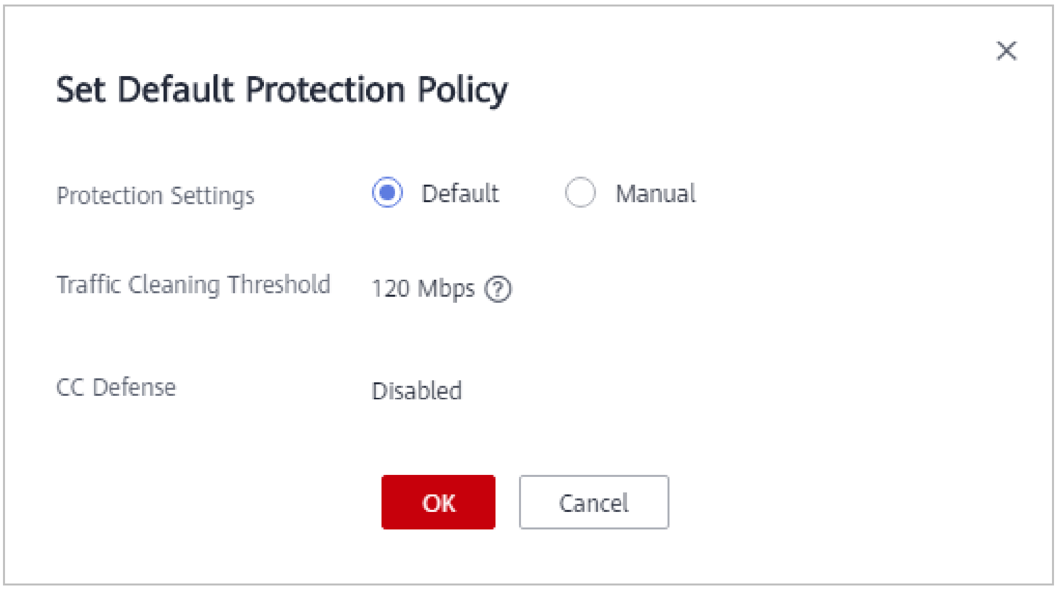
Public IP Addresses | Statistics | Alarm Notifications
Set Default Protection Policy
Enable Anti-DDoS for All IP Addresses
All statuses
Enter a public IP address.

Public IP Addresses	Protection Status	Protection Settings		Operation
[redacted].156.150	Normal	Traffic Cleaning Threshold CC Defense HTTP Request Threshold	70 Mbps Enabled 480 qps	View Monitoring Report | Set Protection
[redacted].155.92	Normal	Traffic Cleaning Threshold CC Defense HTTP Request Threshold	300 Mbps Disabled --	View Monitoring Report | Set Protection
[redacted].153.109	Normal (Default)	Traffic Cleaning Threshold CC Defense HTTP Request Threshold	120 Mbps Disabled --	View Monitoring Report | Set Protection

Step 3 Select **Default** for **Protection Settings** in the **Set Default Protection Policy** dialog box.

The value of **Traffic Cleaning Threshold** is **120 Mbps** and **CC Defense** is disabled.

Figure 1-4 Disabling the default protection policy manually configured for newly purchased IP addresses



Set Default Protection Policy

Protection Settings ● Default ○ Manual

Traffic Cleaning Threshold 120 Mbps

CC Defense Disabled

Step 4 Click **OK**.

The **Protection Settings** in **Default** mode will apply to the new public IP addresses.

----End

2 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.

Prerequisites

- You have obtained a username and password for logging in to the management console.
- You have purchased at least one public IP address.

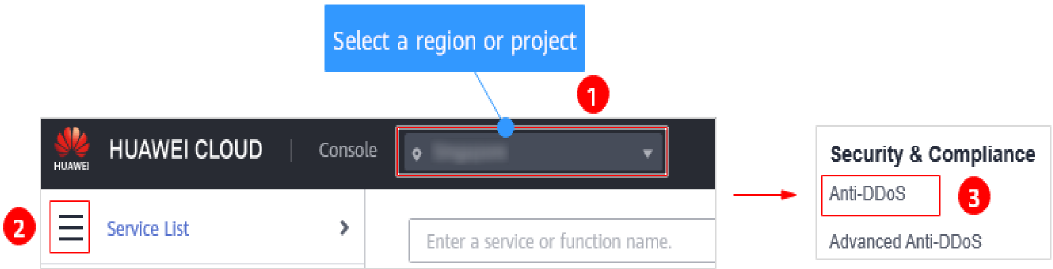
Procedure

Step 1 Log in to the management console.

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

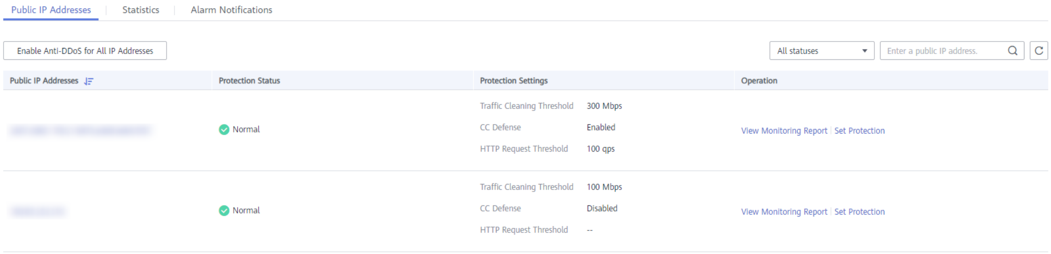
Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Anti-DDoS**.

Figure 2-1 Anti-DDoS



Step 4 On the **Public IP Addresses** tab, view all protected public IP addresses. **Table 2-1** describes the parameters.

Figure 2-2 Viewing a public IP address


Public IP Addresses
Statistics
Alarm Notifications
Enable Anti-DDoS for All IP Addresses
All statuses
Enter a public IP address.

Public IP Addresses	Protection Status	Protection Settings		Operation
[redacted]	✓ Normal	Traffic Cleaning Threshold CC Defense HTTP Request Threshold	300 Mbps Enabled 100 qps	View Monitoring Report | Set Protection
[redacted]	✓ Normal	Traffic Cleaning Threshold CC Defense HTTP Request Threshold	100 Mbps Disabled --	View Monitoring Report | Set Protection

NOTE

- 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 **Configuring an Anti-DDoS 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 address will be routed to the black hole and the legitimate traffic will be discarded. Therefore if you may suffer from volumetric attacks exceeding 500 Mbit/s, it is a better choice to 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 2-1 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: ● **Normal** ● **Configuring** ● **Disabled** ● **Cleaning** ● **Black hole**

----End

3 Enabling Alarm Notification

Scenarios

When alarm notification is enabled in Anti-DDoS, you will receive alarm messages through the endpoint you have configured, such as SMS or email, if your IP address is DDoS attacked. If you do not enable this function, you have to log in to the management console to view alarms.

Prerequisites

- You have obtained a username and password for logging in to the management console.
- You have purchased at least one public IP address.

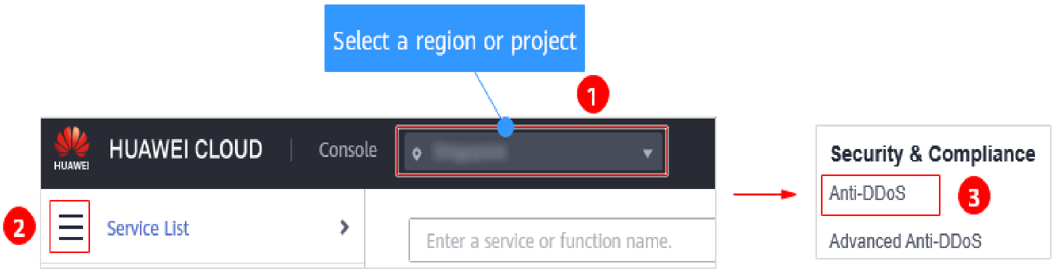
Procedure

Step 1 Log in to the management console.

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

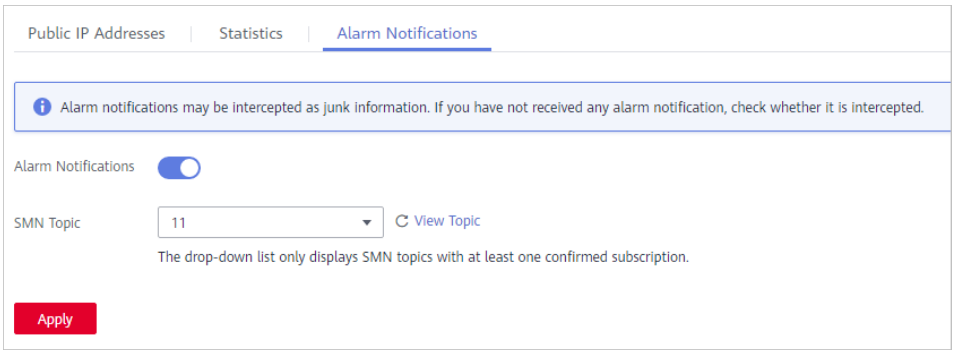
Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Anti-DDoS**.

Figure 3-1 Anti-DDoS



Step 4 On the **Anti-DDoS** page, click the **Alarm Notifications** tab and configure the alarm notification. For details about the parameter settings, see **Table 3-1**.

Figure 3-2 Configuring alarm notifications



Alarm notifications may be intercepted as junk information. If you have not received any alarm notification, check whether it is intercepted.

Alarm Notifications ◉

SMN Topic 11 View Topic

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

Table 3-1 Configuring alarm notifications

Parameter	Description	Example Value
Alarm Notifications	Indicates whether the alarm notification function is enabled. There are two values: - ◉: enabled - ○: disabled If the function is in the disabled state, click ○ to set it to ◉.	◉
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**.	N/A

Step 5 Click **Apply** to enable alarm notification.

----End

4 Configuring an Anti-DDoS Protection Policy

Scenarios

You can adjust your Anti-DDoS protection policy after Anti-DDoS is enabled.

Prerequisites

You have obtained a username and password for logging in to the management console.

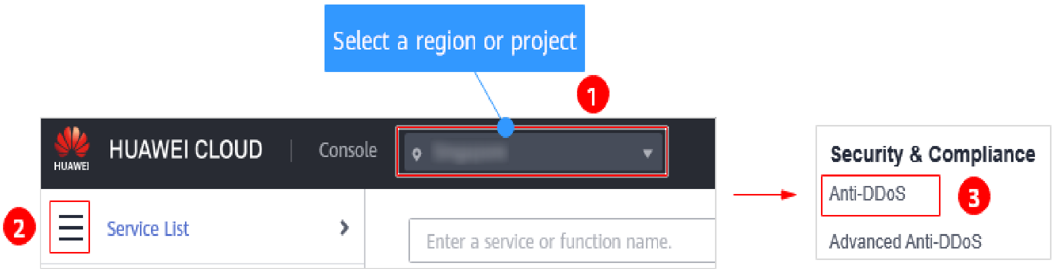
Procedure

Step 1 Log in to the management console.

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

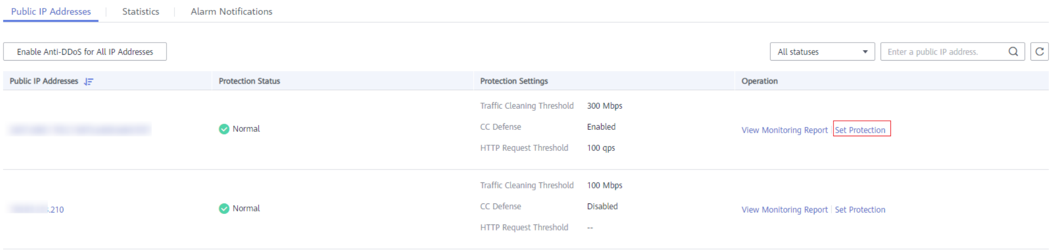
Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Anti-DDoS**.

Figure 4-1 Anti-DDoS



Step 4 Click the **Public IP Addresses** tab, locate the row that contains the IP address for which you want to set protection, and click **Set Protection** in the **Operation** column.

Figure 4-2 Protection settings

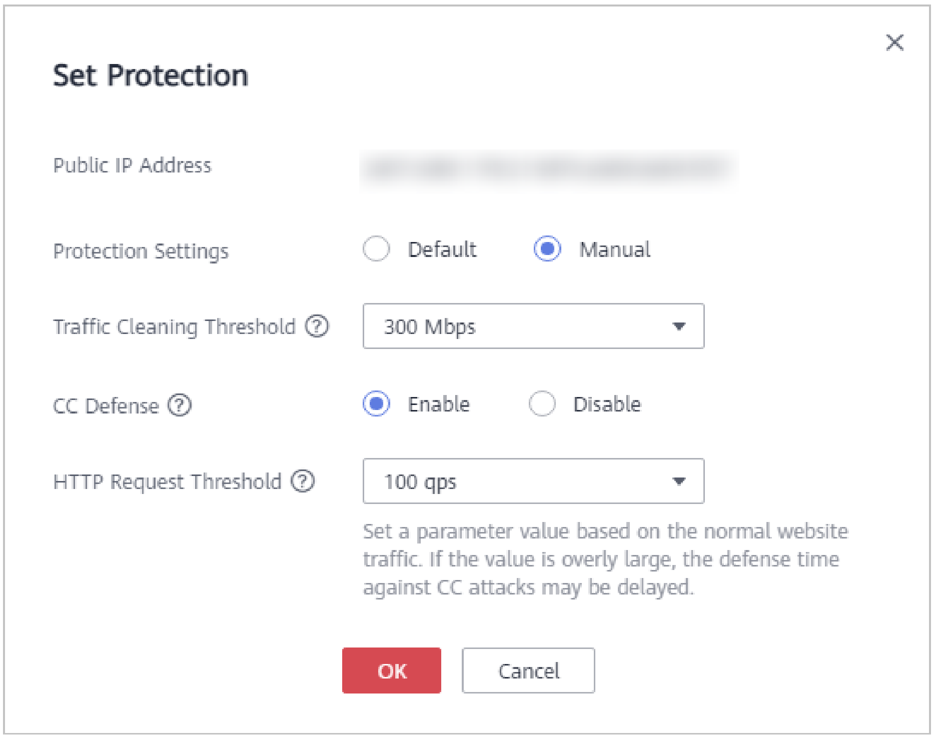


Public IP Addresses
Statistics
Alarm Notifications
Enable Anti-DDoS for All IP Addresses
All statuses
Enter a public IP address.

Public IP Addresses	Protection Status	Protection Settings	Operation
[redacted]	Normal	Traffic Cleaning Threshold 300 Mbps CC Defense Enabled HTTP Request Threshold 100 qps	View Monitoring Report | Set Protection
[redacted].210	Normal	Traffic Cleaning Threshold 100 Mbps CC Defense Disabled HTTP Request Threshold --	View Monitoring Report | Set Protection

Step 5 In the **Set Protection** dialog box, modify desired parameters. **Table 4-1** describes the parameters.

Figure 4-3 Protection settings



Set Protection

Public IP Address [redacted]

Protection Settings ○ Default ● Manual

Traffic Cleaning Threshold 300 Mbps

CC Defense ● Enable ○ Disable

HTTP Request Threshold 100 qps

Set a parameter value based on the normal website traffic. If the value is overly large, the defense time against CC attacks may be delayed.

Table 4-1 Parameter description

Parameter	Description
Protection Settings	● **Default**: In this mode, **Traffic Cleaning Threshold** is fixed at **120 Mbps**. When the service UDP traffic is greater than 120 Mbps or the TCP traffic is greater than 35,000 pps, traffic scrubbing is triggered and Anti-DDoS will automatically intercept the attack traffic. ● **Manual**: In this mode, you can set the value of **Traffic Cleaning Threshold** based on your service needs and enable **CC Defense**. **NOTE** ● Mbps = Mbit/s (short for 1,000,000 bit/s). It is a unit of transmission rate and refers to the number of bits transmitted per second. ● PPS, short for Packets Per Second, is a measure of throughput for network devices. It means the number of packets sent per second.
Traffic Cleaning Threshold	Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the threshold. ● When **Protection Settings** is set to **Default**, the value of **Traffic Cleaning Threshold** is **120 Mbps** by default. ● When **Protection Settings** is set to **Manual**, the value of **Traffic Cleaning Threshold** can be set based on your service needs. You are advised to set the threshold to a value closest to the purchased bandwidth but not greater than the purchased bandwidth. **NOTE** If service traffic triggers scrubbing, only attack traffic is intercepted. If service traffic does not trigger scrubbing, no traffic is intercepted. Set this parameter based on the actual service access traffic. You are advised to set a value closest to, but not exceeding, the purchased bandwidth.
CC Defense	● **Disable**: disables the defense. ● **Enable**: enables the defense. **NOTE** Challenge Collapsar (CC) defense is available only for clients supporting the full HTTP protocol stack because CC defense works in redirection or redirection+verification code mode. If your client does not support the full HTTP protocol stack, you are advised to disable CC defense.

Parameter	Description
HTTP Request Threshold	This parameter is required only when **CC Defense** is set to **Enable**. The unit is qps (short for queries per second). QPS is a common measure of the amount of search traffic an information retrieval system, such as a search engine or a database, receives during one second. This parameter is used to defend against a large number of malicious requests targeting websites. Defense against CC attacks, which aim to exhaust server resources by sending specially crafted GET or POST requests, is triggered when the HTTP request rate on a site reaches the selected value. In the EIP address protection, the maximum recommended value is **5000**. In ELB protection, the value can be larger. You are advised to set this parameter to the maximum number of HTTP requests that can be processed by the deployed service. Anti-DDoS will automatically scrub traffic if detecting that the total number of requests exceeds the configured HTTP request threshold. If the value is too large, CC defense will not be triggered promptly. ● If the actual HTTP request rate is smaller than the configured value, the deployed service is able to process all HTTP requests, and Anti-DDoS does not need to be involved. ● If the actual HTTP request rate is greater than or equal to the configured value, Anti-DDoS triggers CC defense to analyze and check each request, which affects responses to normal requests.

Step 6 Click **OK** to save the settings.

----End

5 Viewing a Monitoring Report

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.

Prerequisites

You have obtained a username and password for logging in to the management console.

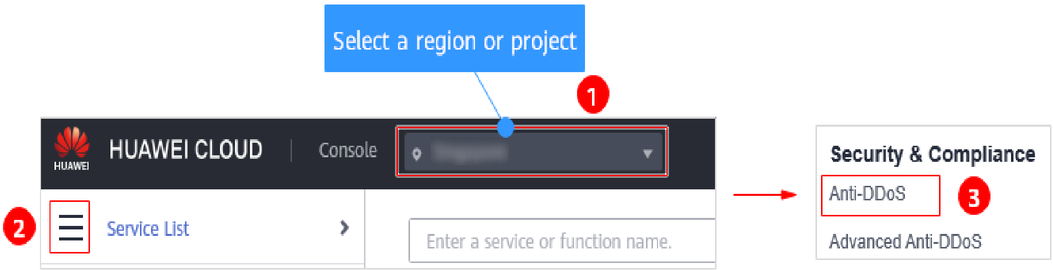
Procedure

Step 1 Log in to the management console.

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

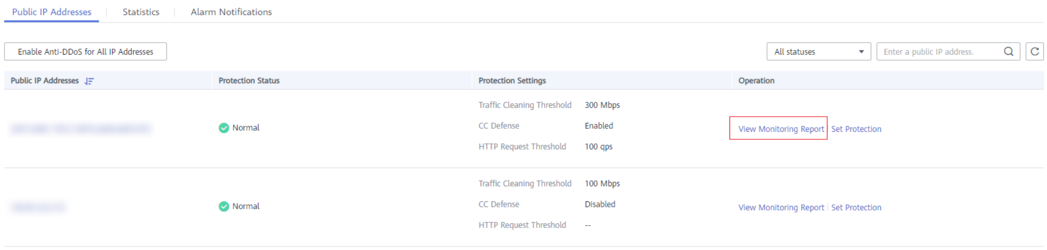
Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Anti-DDoS**.

Figure 5-1 Anti-DDoS



Step 4 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 5-2 Viewing a monitoring report



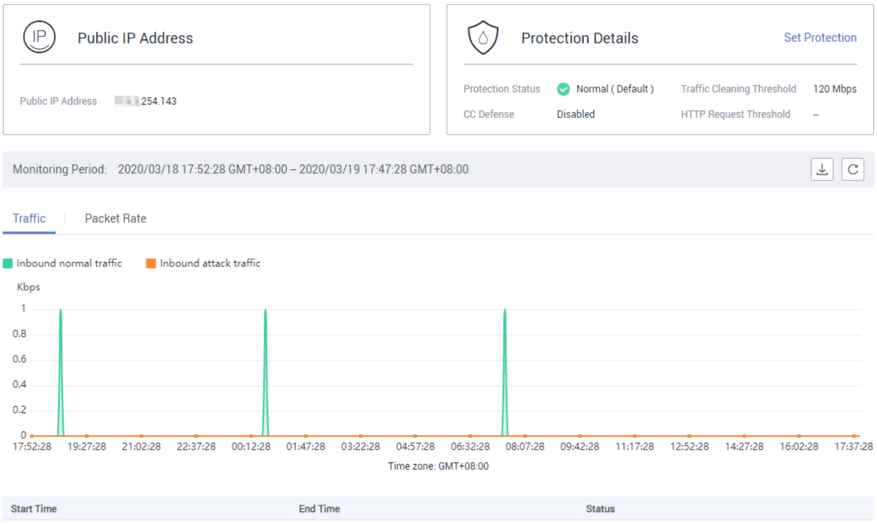
Public IP Addresses
Statistics
Alarm Notifications
Enable Anti-DDoS for All IP Addresses
All statuses
Enter a public IP address.

Public IP Addresses	Protection Status	Protection Settings	Operation
[redacted]	Normal	Traffic Cleaning Threshold 300 Mbps CC Defense Enabled HTTP Request Threshold 100 qps	View Monitoring Report | Set Protection
[redacted]	Normal	Traffic Cleaning Threshold 100 Mbps CC Defense Disabled HTTP Request Threshold --	View Monitoring Report | Set Protection

Step 5 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 5-3 Viewing a traffic monitoring report



Public IP Address

Public IP Address [redacted]254.143

Protection Details — Set Protection

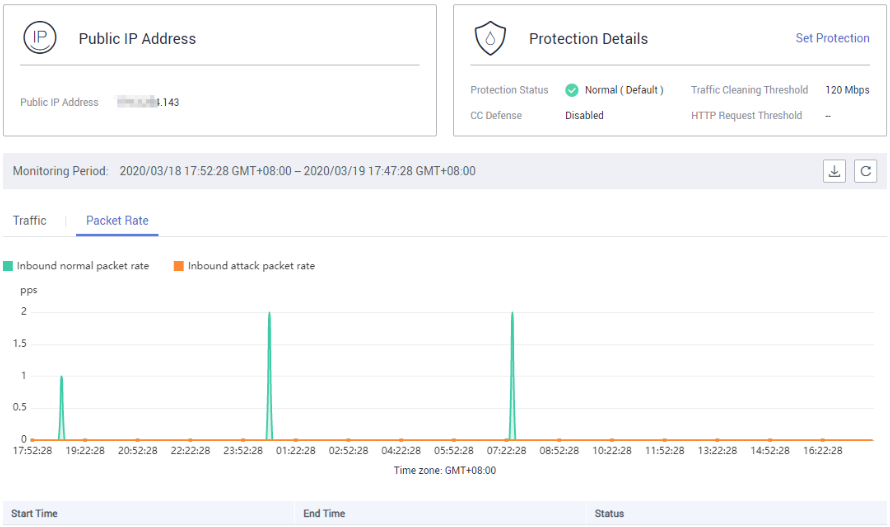
Protection Status: Normal (Default) — Traffic Cleaning Threshold: 120 Mbps

CC Defense: Disabled — HTTP Request Threshold: --

Monitoring Period: 2020/03/18 17:52:28 GMT+08:00 – 2020/03/19 17:47:28 GMT+08:00

Start Time	End Time	Status

Figure 5-4 Viewing a packet rate monitoring report



Public IP Address

Public IP Address [redacted].143

Protection Details

Set Protection

Protection Status ✓ Normal (Default)

Traffic Cleaning Threshold 120 Mbps

CC Defense Disabled

HTTP Request Threshold --

Monitoring Period: 2020/03/18 17:52:28 GMT+08:00 – 2020/03/19 17:47:28 GMT+08:00

Traffic | Packet Rate

Start Time	End Time	Status

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

6 Viewing an Interception Report

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.

Prerequisites

You have obtained a username and password for logging in to the management console.

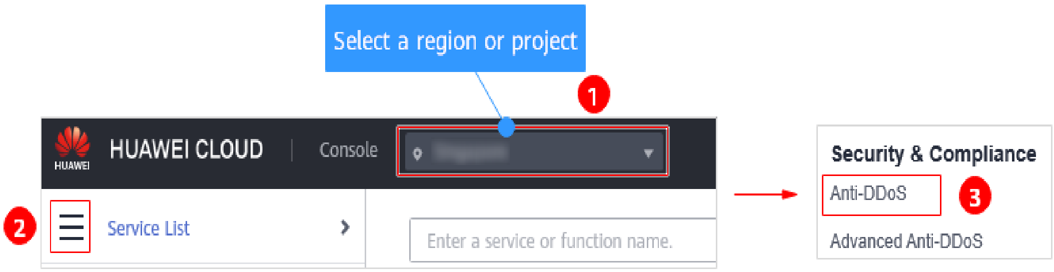
Procedure

Step 1 Log in to the management console.

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

Step 3 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Anti-DDoS**.

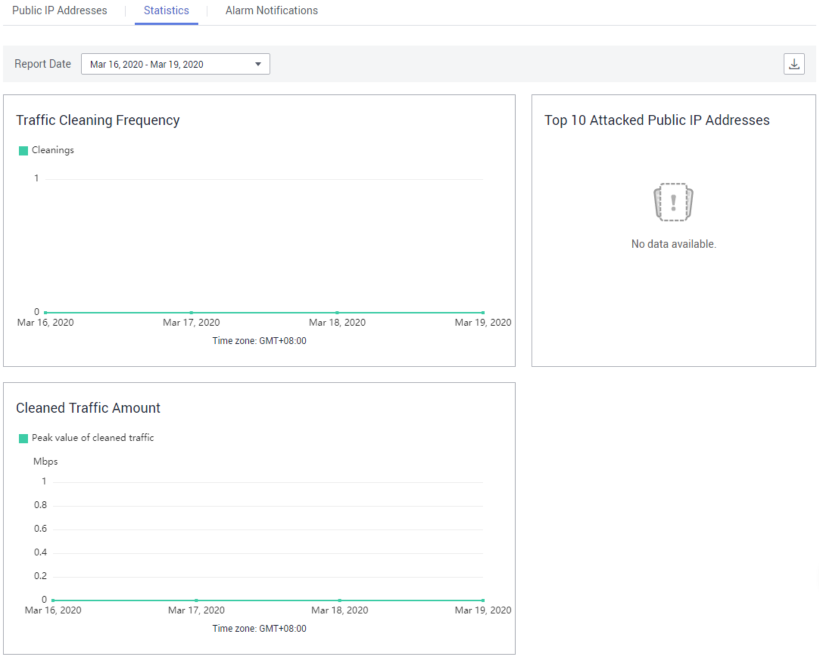
Figure 6-1 Anti-DDoS



Step 4 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 6-2 Viewing an interception report



NOTE

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

----End

7 Permission Management

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

This section describes IAM's fine-grained permissions management for your Anti-DDoS resources. 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 task.
- Entrust a HUAWEI CLOUD account or cloud service to perform professional and efficient O&M to your Anti-DDoS resources.

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

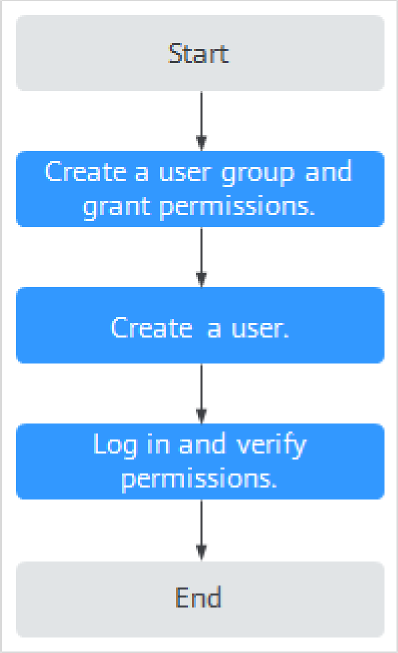
This section describes the procedure for granting permissions (see **Figure 7-1**).

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 **Permissions Management**.

Process

Figure 7-1 Process for granting permissions


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

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

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

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

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

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

   Log in to the management console by using the user created in **2**, and verify that the user only has read permissions for AAD.

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

A Change History

Released On	Description
2021-10-09	This issue is the ninth official release, which incorporates the following change: Updated some screenshots in **Configuring an Anti-DDoS Protection Policy**.
2021-08-06	This is the eighth official release. Modified the description of the entry on the management console.
2020-08-25	This is the seventh official release. Added **Setting a Default Protection Policy for Newly Purchased Public IP Addresses**.
2020-04-08	This is the sixth official release. Updated some screenshots.
2020-01-07	This is the fifth official release. Added parameter descriptions in section **Configuring an Anti-DDoS Protection Policy**.
2019-12-16	This is the fourth official release. Modified the domain name of HUAWEI CLOUD international website.
2019-11-21	This is the third official release. The figure titles are added to the figures, and documents' publish path IDs are fixed.
2018-01-19	This is the second official release. Optimized the alarm notification page in section **Enabling Alarm Notification**.
2017-12-31	This is the first official release.