Anti-DDoS

Getting Started

Issue	01
Date	2024-05-11

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 How Do I Use Anti-DDoS?..... 1
2 Getting Started with Common Practices..... 5

1 How Do I Use Anti-DDoS?

- Cloud Native Anti-DDoS Basic (CNAD Basic) protects public IP addresses from Layer 4 to Layer 7 distributed denial of service (DDoS) attacks and reports alarms immediately when an attack is detected. In addition, CNAD Basic improves the bandwidth utilization to further safeguard user services.
- CNAD Basic monitors the service traffic from the Internet to elastic public IP addresses (EIPs) to detect attack traffic in real time. It then scrubs attack traffic based on user-configured defense policies without interrupting services. It also generates monitoring reports that provide visibility into the network traffic security.
- This document provides a quick start guide for CNAD Basic, covering how to view public IP addresses, enable alarm notification, configure service policies, and view monitoring and interception reports.

Step 1: Prepare the Environment

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 **Compute** > **Elastic Cloud Server (ECS)**.

Step 3 Create an ECS and bind an EIP to it. For details, see section **Purchasing an ECS**.

NOTE

- An EIP must be bound to the ECS so that the ECS can access the Internet.
- If you have an ECS, you can reuse it without the need to create one again.

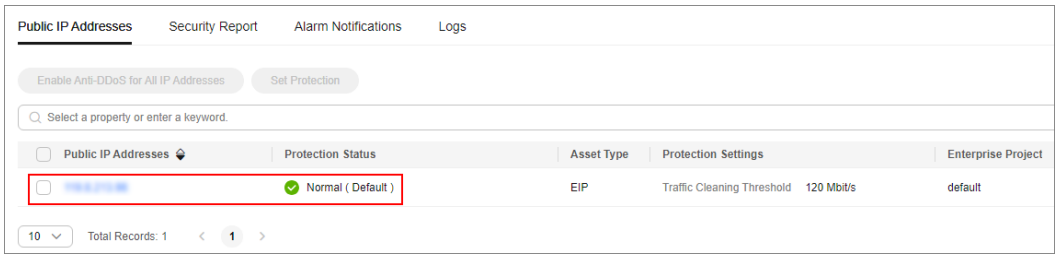
----End

Step 2: View EIPs

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

Step 2 On the **Public IP Addresses** tab page, check whether default protection has been enabled for the public IP address prepared in **Step 1: Prepare the Environment**.

Figure 1-1 Viewing public IP address



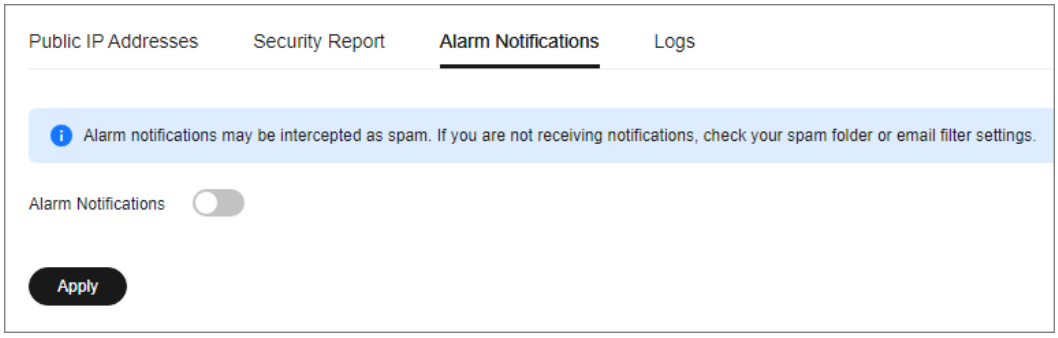
----End

Step 3: Enabling Alarm Notifications

Step 1 Click the **Alarm Notifications** tab.

Step 2 Enable the alarm notification function, set the notification topic, and click **Apply**.

Figure 1-2 Setting alarm notifications



NOTE

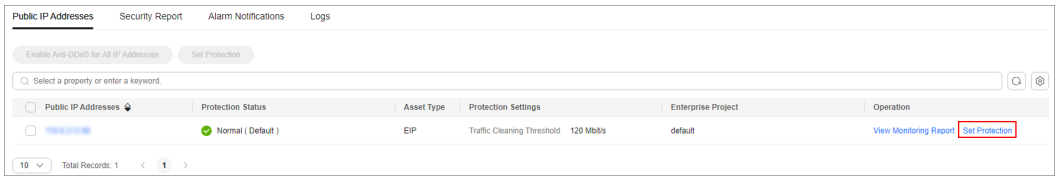
The alarm notification function sends you alarm notifications (by SMS or email) if a DDoS attack is detected.

----End

Step 4: Configuring a DDoS Protection Policy

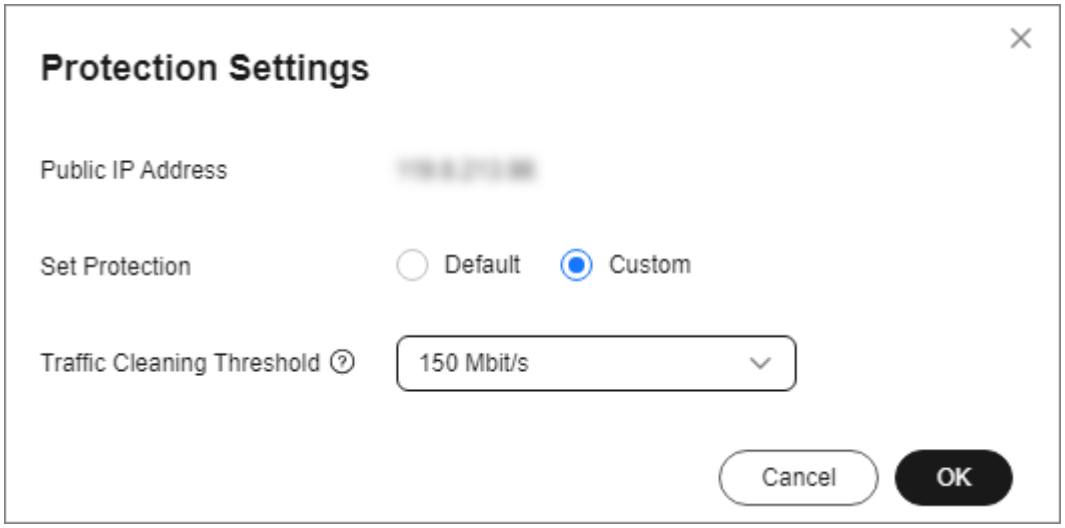
Step 1 Click the **Public IP Addresses** tab, locate the row that contains the target public IP address, and click **Set Protection**.

Figure 1-3 Set Protection



Step 2 Modify the protection settings as required and click **OK**.

Figure 1-4 Modifying protection settings



NOTE

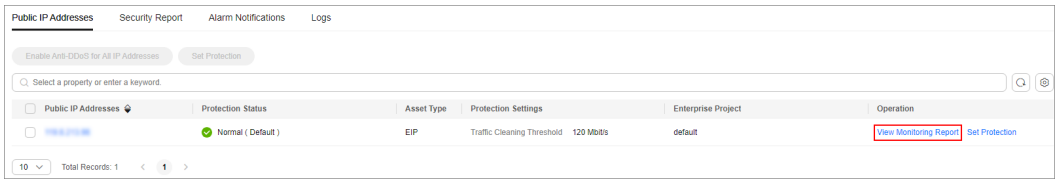
Configure the traffic cleaning threshold based on the actual service access traffic. You are advised to set a value closest to, but not exceeding, the purchased bandwidth.

----End

Step 5: Viewing a Monitoring Report

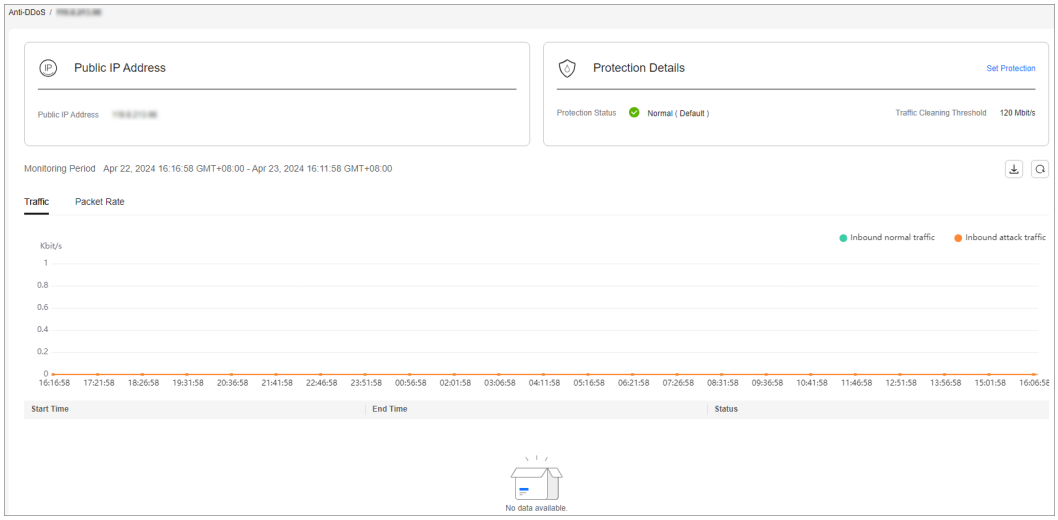
Step 1 Click the **Public IP Addresses** tab, locate the row that contains the target public IP address, and click **View Monitoring Report**.

Figure 1-5 Viewing a monitoring report



You can view the protection status, traffic details, and attack events of a public IP address within the last 24 hours.

Figure 1-6 Monitoring details



----End

2 Getting Started with Common Practices

This section describes Anti-DDoS protection practices.

Table 2-1 DDoS protection

Version	Practice		Description
Anti-DDoS	Routine maintenance	**Configuring Alarm Notifications**	Enable alarm notification for DDoS attacks.
		Connecting to a Server Routed to a Black Hole	Use an ECS to remotely access the server that has been blackholed.

