Anti-DDoS

Getting Started

Issue 02

Date 2024-11-26

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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 Using CNAD Basic for Free

If you have purchased Huawei Cloud EIPs, you can use CNAD Basic for free.

CNAD Basic offers EIPs Layer 4 protection against DDoS attacks and real-time alarm notifications, enhancing bandwidth utilization and ensuring the stable operation of user services.

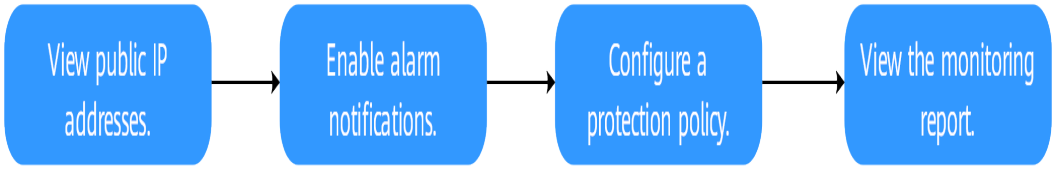
CNAD Basic monitors the service traffic from the Internet to elastic public IP addresses (EIPs) to detect attack traffic in real time. It then scrubs attack traffic based on user-configured defense policies without interrupting services. It also generates monitoring reports that provide visibility into the network traffic security.

CNAD Basic automatically activates protection for **EIPs on Huawei Cloud**. You can simply configure alarm notifications and protection policies to access the protection features of CNAD Basic.

Procedure

This section describes how to quickly configure CNAD Basic protection for an EIP. **Figure 1-1** shows the process.

Figure 1-1 Procedure



Step	Description
Prerequisites	Register a Huawei ID, enable Huawei Cloud, grant CNAD Basic permissions, and prepare protected objects.
Step 1: Viewing the EIP Status	Check whether the protected objects are synchronized to the CNAD Basic console and whether the default protection is enabled.

Step	Description
Step 2: Enabling Alarm Notifications	Set traffic scrubbing alarm notifications for protected objects.
Step 3: Configuring a DDoS Protection Policy	Configure traffic scrubbing policies for protected objects.
Step 4: Viewing a Monitoring Report	View the protection status and traffic details of protected objects.

Prerequisites

1. Before using CNAD Basic, register a Huawei ID and enable Huawei Cloud. For details, see **Registering a Huawei ID and Enabling Huawei Cloud Services** and **Real-Name Authentication**.

   If you have enabled Huawei Cloud and completed real-name authentication, skip this step.
2. Ensure that the account has been assigned related permissions. For details, see **Creating a User Group and Assigning the Anti-DDoS Access Permission**.
3. Create an ECS and bind an EIP to it. For details, see section **Purchasing an ECS**.

   NOTE

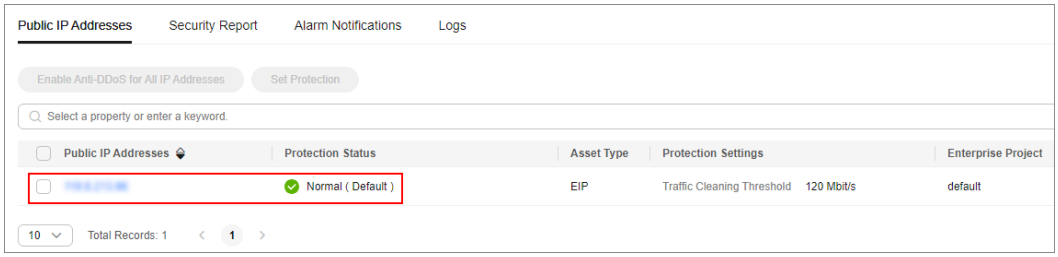
   If you have an ECS that meets the requirements, you do not need to create one again.

Step 1: Viewing the EIP Status

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

Step 2 On the **Public IP Addresses** tab, ensure that the EIP prepared in **Prerequisites** has been synchronized to CNAD Basic and the default protection has been enabled for it.

Figure 1-2 Viewing public IP address



----End

Step 2: Enabling Alarm Notifications

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

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

Figure 1-3 Setting alarm notifications

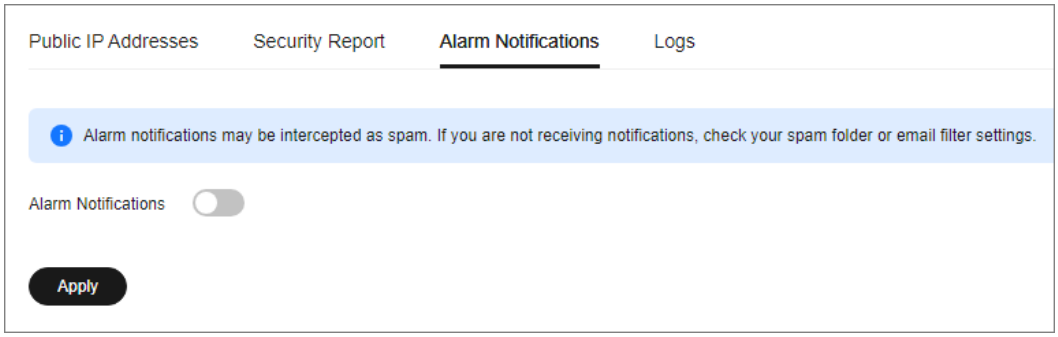


Table 1-1 Parameter description

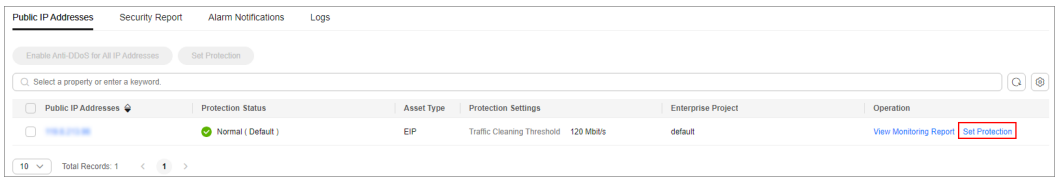
Parameter	Example Value	Description
Scrubbed Traffic Alarm Threshold	**1000Kbps**	When the volume of scrubbed traffic reaches the threshold, an alarm notification is sent. Set the threshold as required.
Alarm Notifications		Set the alarm switch to  to enable the alarm function. You will receive notifications (by SMS or email) if a DDoS attack is detected on your EIP.
SMN Topic	-	You can select an existing topic or click **View Topic** to create a topic. For details about how to create a topic, see **Creating a Topic**.

----End

Step 3: 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 1-4 Set Protection



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

Figure 1-5 Modifying protection settings

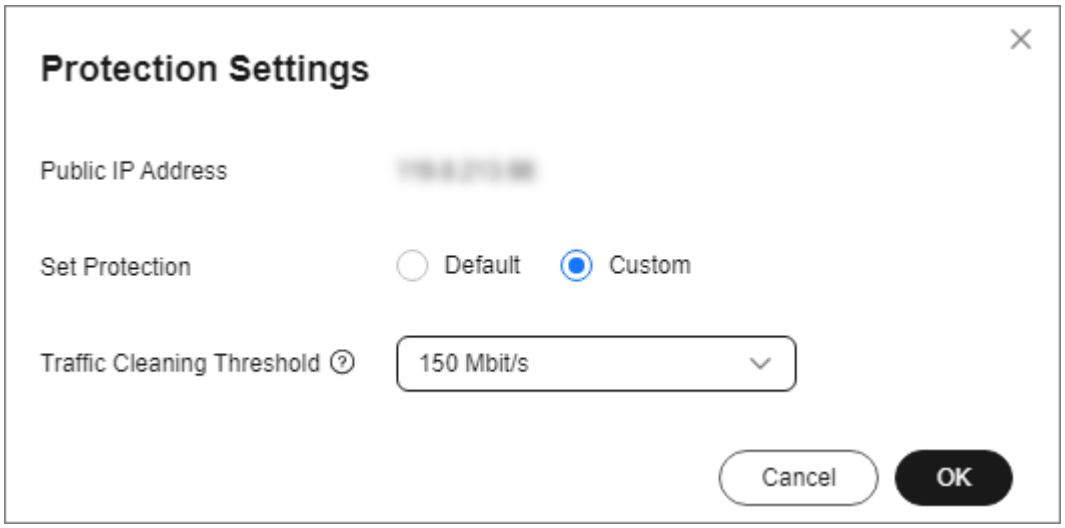


Table 1-2 Parameter description

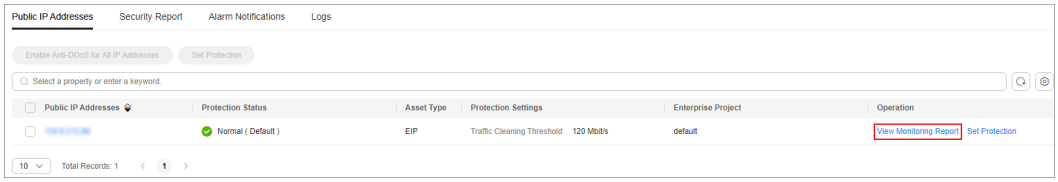
Parameter	Example Value	Description
Set Protection	**Custom**	The default protection level is 120 Mbit/s, but you can manually adjust to higher levels if needed.
Traffic Cleaning Threshold	**150Mbit/s**	You are advised to set a value closest to, but not exceeding, the purchased bandwidth. CNAD Basic scrubs traffic when detecting that the inbound traffic of an IP address exceeds the threshold.

----End

Step 4: Viewing a Monitoring Report

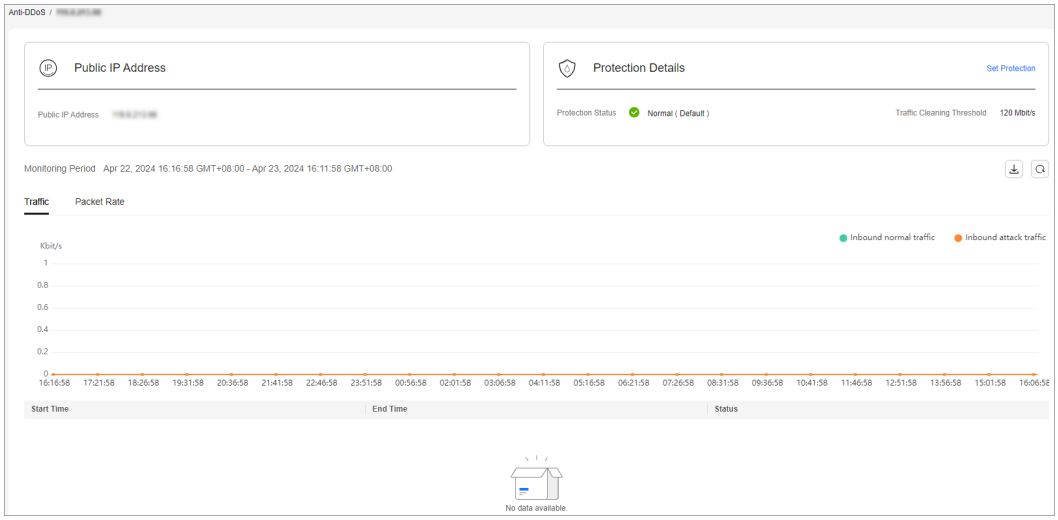
Step 1 Click the **Public IP Addresses** tab, locate the row that contains the target public IP address, and click **View Monitoring Report**.

Figure 1-6 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 1-7 Monitoring details



----End

Related Information

- Event monitoring can be enabled for a protected EIP, which triggers an alarm when events like scrubbing, blocking, or unblocking occur. For details, see .
- If you want to enable attack logging for a protected EIP for subsequent analysis and O&M, you can enable LTS. For details, see .

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.

