Anti-DDoS Service

Getting Started with Common Practices

Issue   01
Date   2023-09-11

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?

- 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

> **NOTE**
>
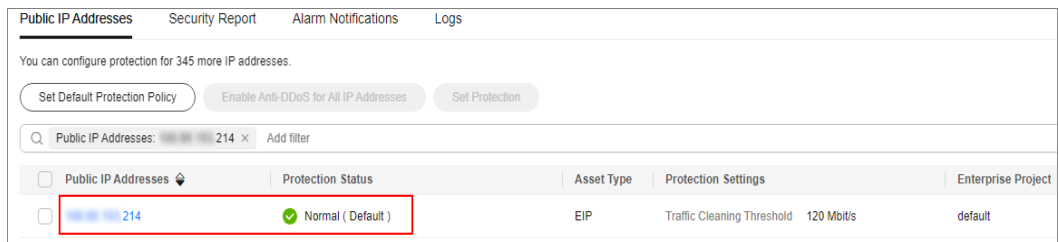> After you purchase an EIP, Anti-DDoS automatically enables default protection to protect the EIP.

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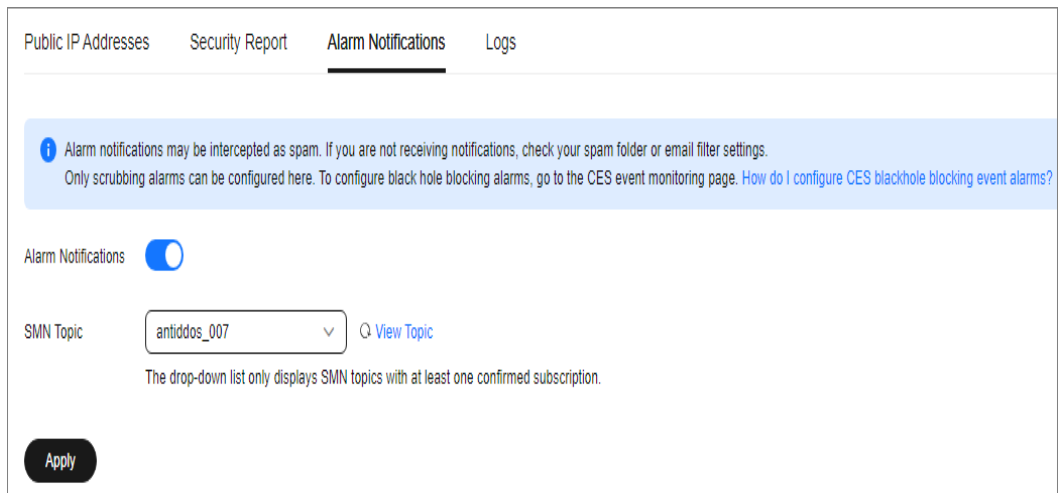
> **NOTE**
>
> The alarm notification function sends you alarm notifications (by SMS or email) if a DDoS attack is detected.

----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 Protection settings

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

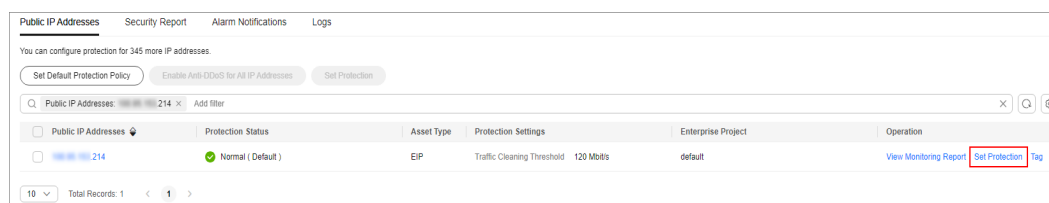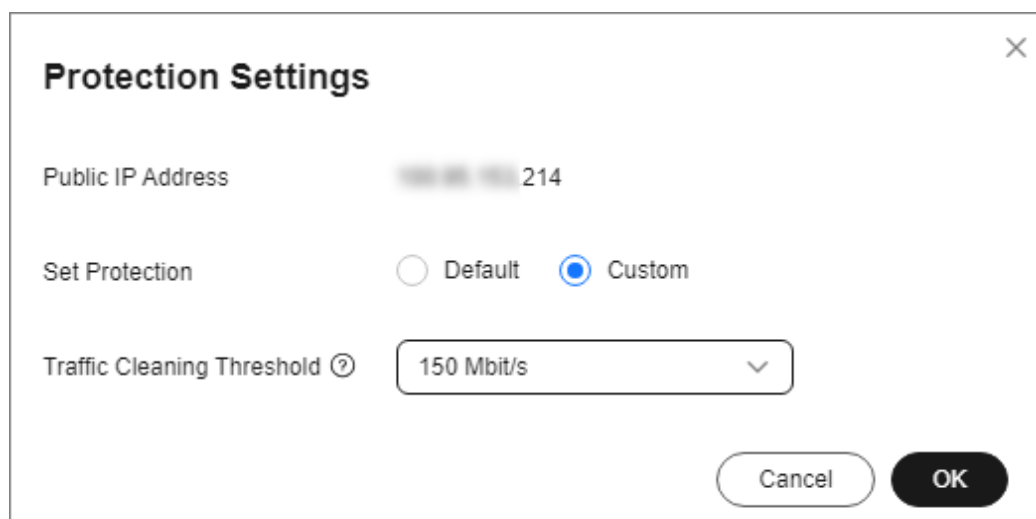**Figure 1-4** Modifying protection settings

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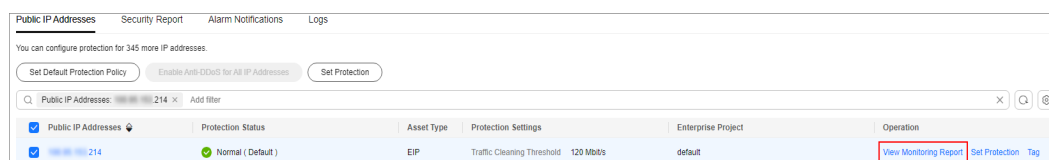
You can view the protection status, traffic details, and attack events of a public IP address within the last 24 hours.

Figure 1-6 Monitoring details

----End

2 Quick Access to CNAD - Unlimited Protection Basic Edition

Cloud Native Anti-DDoS Advanced (CNAD) provides higher DDoS protection capability for cloud services on Huawei Cloud such as Elastic Cloud Server (ECS), Elastic Load Balance (ELB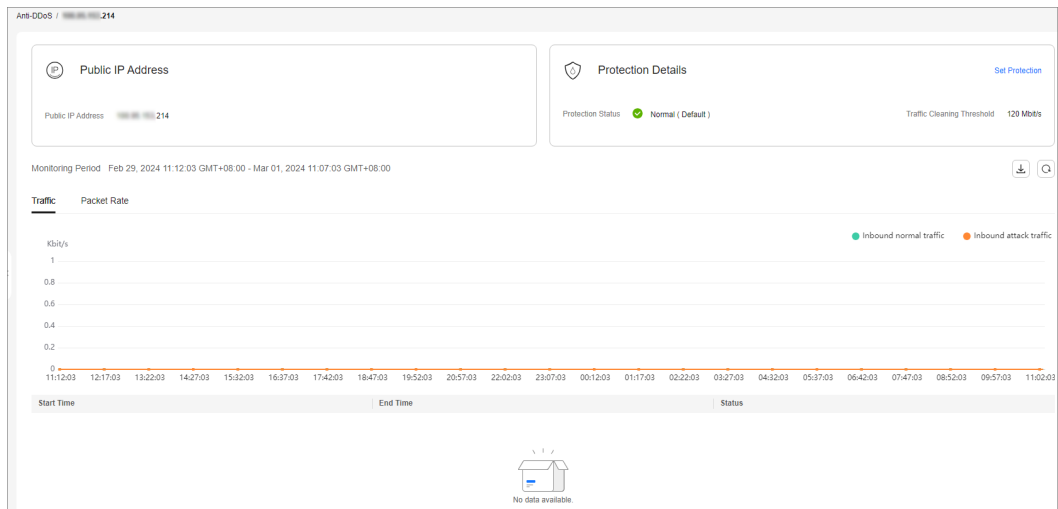), Web Application Firewall (WAF), and Elastic IP (EIP). CNAD defends against the DDoS attacks targeting the IP addresses on Huawei Cloud and it provides higher protection capabilities for cloud services. With few clicks on the console, you can enjoy always-on DDoS mitigation on Huawei Cloud.

Step 1: Purchasing an Unlimited Protection Basic Edition Instance

Step 1 **Log in to the management console**.

Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS** page is displayed.
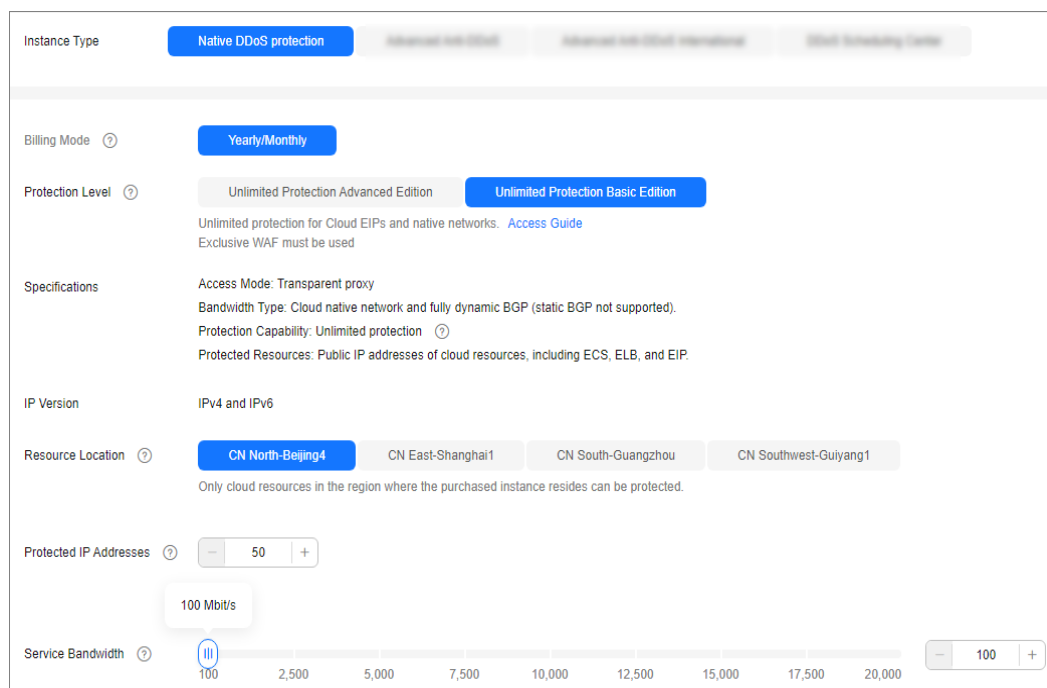
Step 3 In the upper right corner of the page, click **Buy CNAD Pro**.

Step 4 Set **instance Type** to **Native DDoS Protection**.

Step 5 Set **Protection Level** to **Unlimited Protection Basic Edition**.

Step 6 Set the purchase parameters as required, click **Buy Now**, and complete the payment as prompted.

Figure 2-1 Setting Unlimied Protection Basic edition specifications

----End

Step 2: Creating a Protection Policy

Step 1 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced > Protection Policies**. The **Protection Policies** page is displayed.

Step 2 Configure a protection policy by referring to section **Adding a Protection Policy**.

----End

Step 3: Adding a Protected Objects

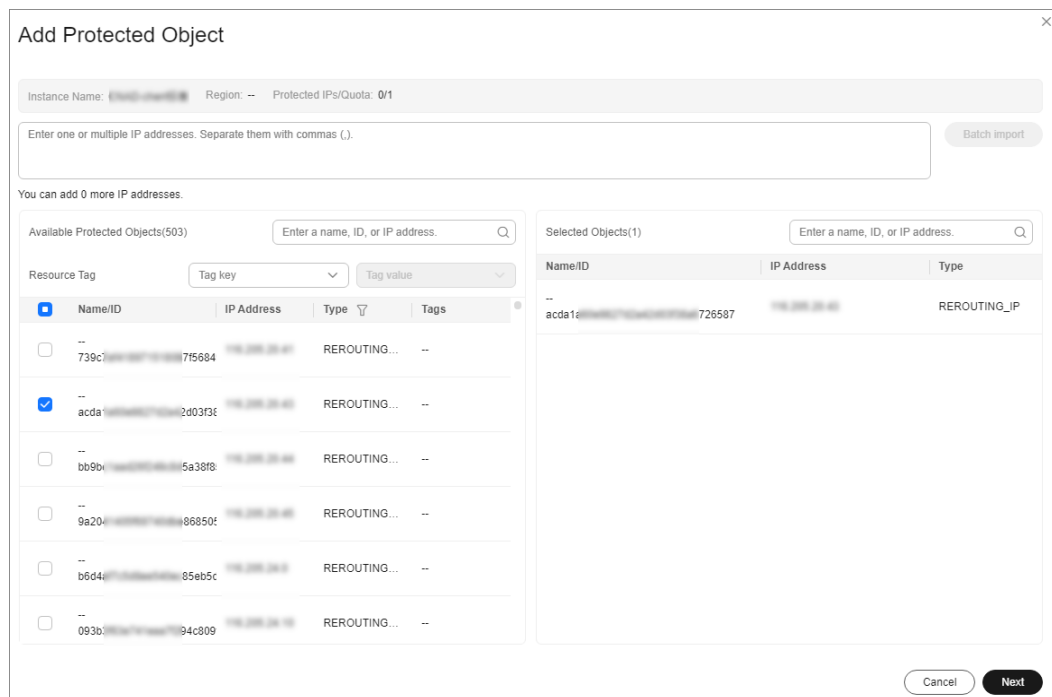**Step 1** In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced > Instances**. The **Instances** page is displayed.

Step 2 In the upper right corner of the target instance box, click **Add Protected Object**.

Step 3 Add the IP address to be protected as a protected object by referring to **Adding a Protected Object**.'

Figure 2-2 Adding a protected object

NOTE

The added protected objects (such as ECS, ELB, WAF, and EIP) are in the same region as the region of the purchased CNAD instance.

----End

3 Quick Access to CNAD - Unlimited Protection Advanced Edition

Cloud Native Anti-DDoS Advanced (CNAD) provides higher DDoS protection capability for cloud services on Huawei Cloud such as Elastic Cloud Server (ECS), Elastic Load Balance (ELB), Web Application Firewall (WAF), and Elastic IP (EIP). CNAD defends against the DDoS attacks targeting the IP addresses on Huawei Cloud and it provides higher protection capabilities for cloud services. With few clicks on the console, you can enjoy always-on DDoS mitigation on Huawei Cloud.

Step 1: Purchasing an Unlimited Protection Advanced Edition Instance

Step 1 **Log in to the management console**.

Step 2 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 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 purchase parameters as required, click **Buy Now**, and complete the payment as prompted.

Figure 3-1 Setting specifications of the Unlimited Protection Advanced edition
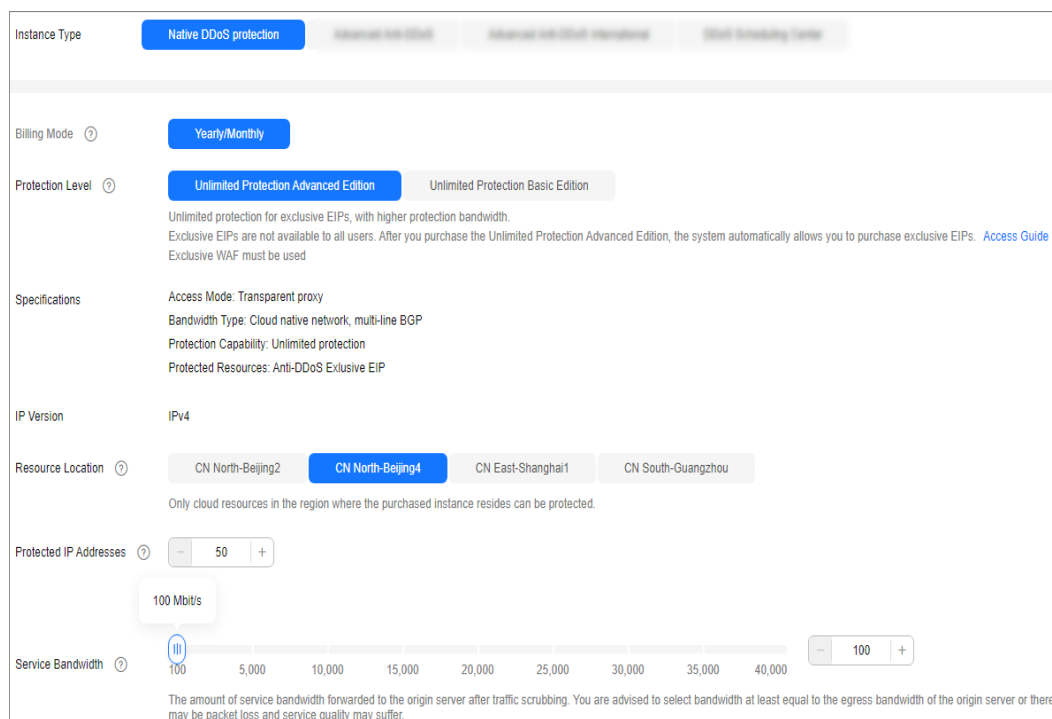
----End

Step 2: Purchasing an Exclusive EIP and Binding It to an Instance

Step 1 **Submit a service ticket** to contact the Anti-DDoS service team to obtain the permission to purchase exclusive EIPs.

Step 2 Purchase an exclusive EIP by referring to **Assigning an EIP**.

Step 3 Bind the exclusive EIP to the Unlimited Protection Advanced Edition instance. For details, see **Binding an EIP to an Instance**.

----End

Step 3: Creating a Protection Policy

Step 1 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced > Protection Policies**. The **Protection Policies** page is displayed.

Step 2 Configure a protection policy by referring to section **Adding a Protection Policy**.

----End

Step 4: Adding a Protected Object

Step 1 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced > Instances**. The **Instances** page is displayed.

Step 2 In the upper right corner of the target instance box, click **Add Protected Object**.

Step 3 Add the exclusive EIP as a protected object. For details, see section **Adding a Protected Object**.

Figure 3-2 Adding a protected object
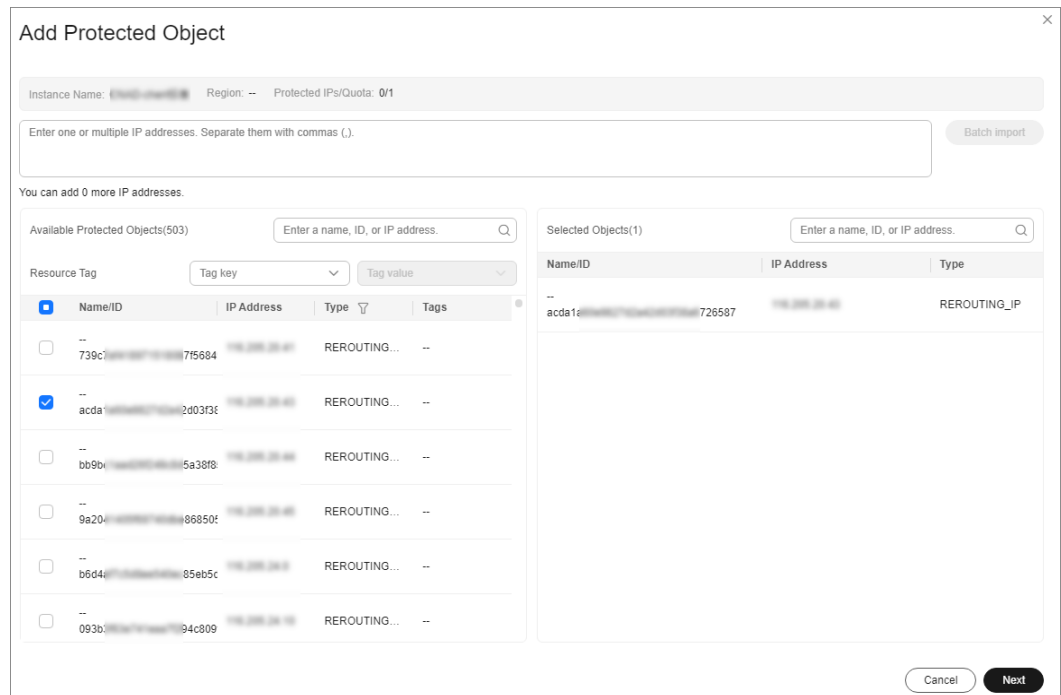
----End

4 Getting Started with Common Practices

After becoming a Huawei Cloud user, you can use Anti-DDoS for free. If you need better protection capabilities, you are advised to purchase editions with higher specifications.

This document describes the practices of using different editions of AAD.

Table 4-1 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.
	Protection upgrade	**Enhancing Anti-DDoS Service Capabilities**	Purchase an AAD edition of higher specifications.