

**Anti-DDoS Service**

# Getting Started with Common Practices

**Issue**            03  
**Date**             2025-01-03



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. 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

---

<b>1 Using CNAD Basic for Free.....</b>	<b>1</b>
<b>2 Quick Access to CNAD - Unlimited Protection Basic Edition.....</b>	<b>6</b>
<b>3 Quick Access to CNAD - Unlimited Protection Advanced Edition.....</b>	<b>13</b>
<b>4 Quick access to Cloud Native Anti-DDoS 2.0.....</b>	<b>21</b>
<b>5 Getting Started with Common Practices.....</b>	<b>29</b>

# 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.

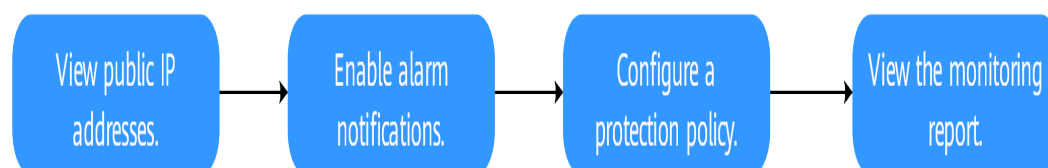
CNAD Basic monitors the service traffic from the Internet to elastic public IP addresses (EIPs) to detect attack traffic in real time. It then scrubs attack traffic based on user-configured defense policies without interrupting services. It also generates monitoring reports that provide visibility into 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
<b>Prerequisites</b>	Register a Huawei ID, enable Huawei Cloud, grant CNAD Basic permissions, and prepare protected objects.
<b>Step 1: Viewing the EIP Status</b>	Check whether the protected objects are synchronized to the CNAD Basic console and whether the default protection is enabled.

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


## Prerequisites

- 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.
- Ensure that the account has been assigned related permissions. For details, see [Creating a User Group and Assigning the Anti-DDoS Access Permission](#).
- Create an ECS and bind an EIP to it. For details, see section [Purchasing an ECS](#).

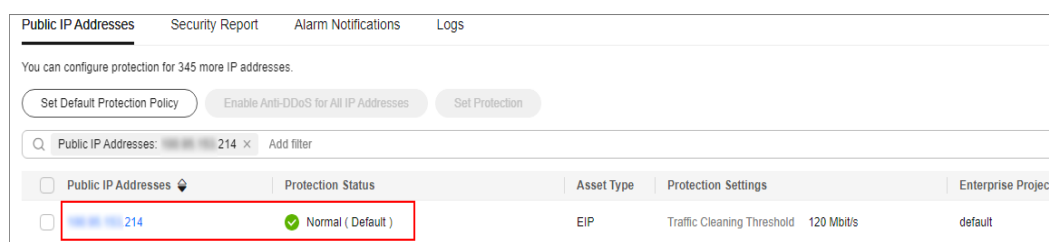
### NOTE



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 Service**. 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



Public IP Addresses	Protection Status	Asset Type	Protection Settings	Enterprise Project
 214	 Normal ( Default )	EIP	Traffic Cleaning Threshold 120 Mbit/s	default

----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** Configuring alarm notifications

**Setting**

Scrubbed Traffic Alarm Threshold ?  Kbit/s

SMN Alarm Notifications

SMN Topic  [View Topic](#)

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

**Apply**

**Table 1-1** Parameter description

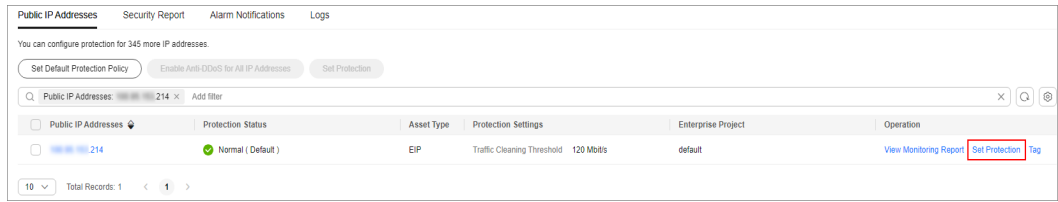
Parameter	Example Value	Description
Scrubbed Traffic Alarm Threshold	<b>1000Kbps</b>	When the volume of scrubbed traffic reaches the threshold, an alarm notification is sent. Set the threshold as required.
Alarm Notifications	<input checked="" type="checkbox"/>	Set the alarm switch to <input checked="" type="checkbox"/> 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 <b>View Topic</b> to create a topic. For details about how to create a topic, see <a href="#">Creating a Topic</a> .

----End

## Step 3: Configuring a DDoS Protection Policy

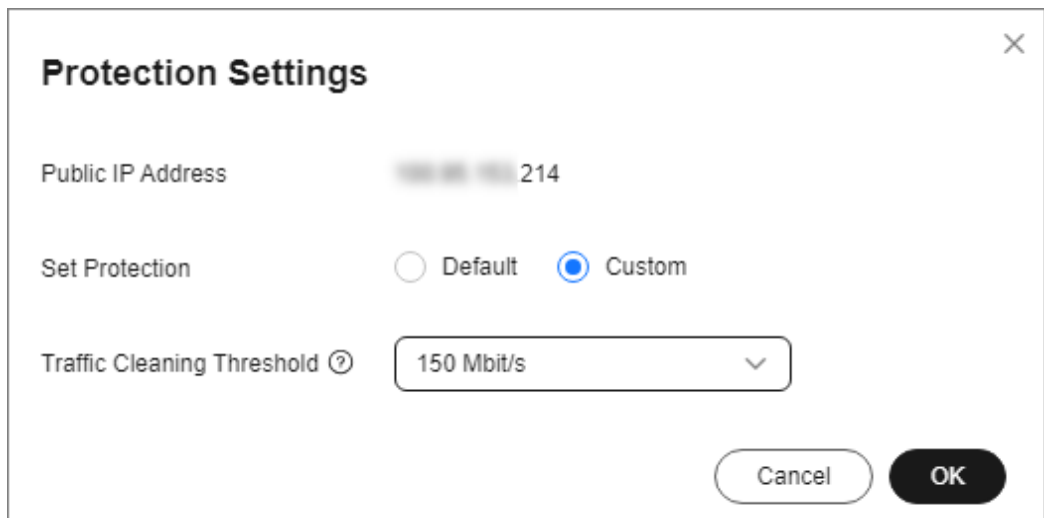
**Step 1** Click the **Public IP Addresses** tab, locate the row that contains the target public IP address, and click **Set Protection**.

**Figure 1-4** Protection settings



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

**Figure 1-5** Modifying protection settings



**Table 1-2** Parameter description

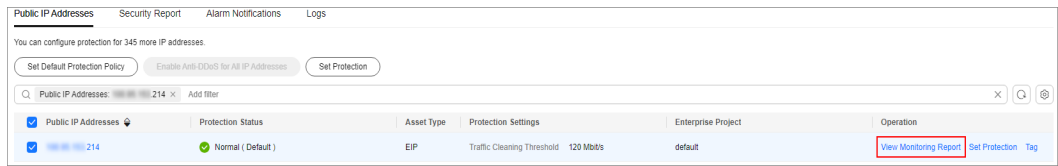
Parameter	Example Value	Description
Set Protection	<b>Custom</b>	The default protection level is 120 Mbit/s, but you can manually adjust to higher levels if needed.
Traffic Cleaning Threshold	<b>150Mbps</b>	You are advised to set a value closest to, but not exceeding, the purchased bandwidth. CNAD Basic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

----End

## Step 4: Viewing a Monitoring Report

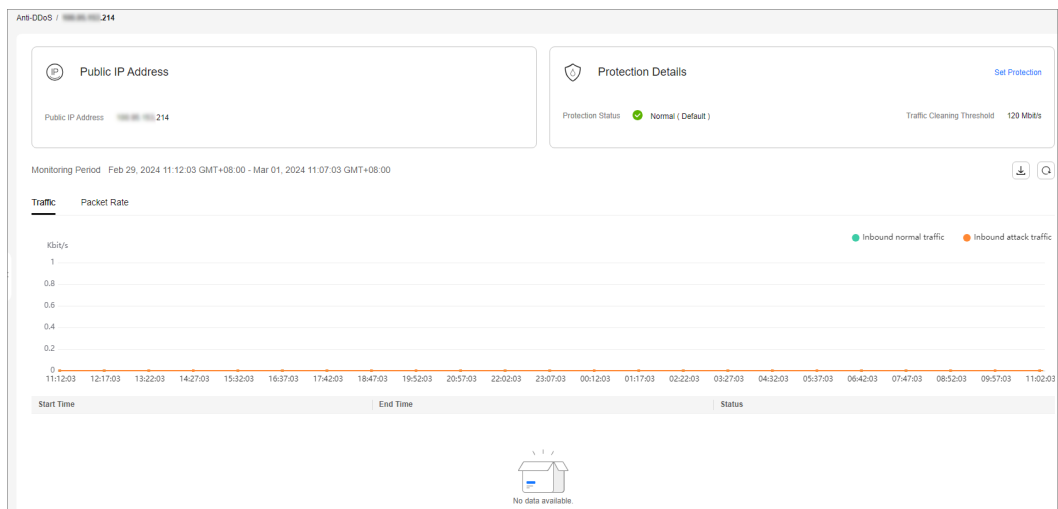
**Step 1** Click the **Public IP Addresses** tab, locate the row that contains the target public IP address, and click **View Monitoring Report**.

**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 [Setting Event Alarm Notifications](#).
- If you want to enable attack logging for a protected EIP for subsequent analysis and O&M, you can enable LTS. For details, see [Configuring LTS for Anti-DDoS Logging](#).



# 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 Unlimited Protection Basic Edition defends against the DDoS attacks targeting the **dynamic BGP EIPs 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.

This section uses an EIP in CN North-Beijing4 (Chinese mainland) as an example to describe how to purchase and use the Unlimited Protection Basic Edition.

## Procedure

This section describes how to quickly purchase Unlimited Protection Basic Edition and enable protection. The process is shown in [Figure 2-1](#).

**Figure 2-1** Procedure



Step	Description
<b>Prerequisites</b>	Register a Huawei ID, enable Huawei Cloud, top up the account, grant CNAD Advanced permissions, and prepare protected objects.
<b>Step 1: Purchasing an Unlimited Protection Basic Edition Instance</b>	Purchase Unlimited Protection Basic Edition in the specified region.

Step	Description
<a href="#">Step 2: Creating a Protection Policy</a>	Create and configure protection policies for protected objects.
<a href="#">Step 3: Adding a Protected Object</a>	Add protected objects to the Unlimited Protection Basic Edition instance.

## Prerequisites


1. Before using Unlimited Protection Basic Edition, 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. Make sure your account has enough funds to avoid issues when purchasing Unlimited Protection Basic Edition.
3. Ensure that the account has been assigned related permissions. For details, see [Creating a User and Granting the CNAD Access Permission](#).
4. In the CN North-Beijing4 region, 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: 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 DDoS Mitigation**.

**Step 4** Set the purchase parameters as required, click **Buy Now**, and complete the payment as prompted.

**Table 2-1** Parameter description

Parameter	Example Value	Description
Instance Type	<b>Cloud Native Anti-DDoS</b>	Type of the instance to be purchased.
Billing Mode	<b>Yearly/Monthly</b>	You are charged based on the subscription period. This means that you have to pay for a certain period of time in advance. Unlimited Protection Basic Edition supports only the yearly/monthly billing mode.

Parameter	Example Value	Description
Region	<b>Chinese Mainland</b>	<ul style="list-style-type: none"><li>● <b>Chinese Mainland:</b> applies to scenarios where service servers are deployed in Chinese mainland (cross-region deployment is supported). Only dynamic BGP EIPs are supported.</li><li>● <b>Other:</b> applies to scenarios where the service server is deployed in the Asia Pacific region (Hong Kong is supported currently). Only premium BGP EIPs are supported.</li></ul>
Protection Level	<b>Unlimited Protection Basic Edition:</b>	Edition to be purchased.
Resource Location	<b>CN North-Beijing4</b>	Region where the protected cloud resources are located. Cross-region protection is not supported.
Protected IP Addresses	<b>50</b>	The number of protected IP addresses refers to the number of EIPs that can be protected by each CNAD Advanced instance. You are advised to evaluate the number of protected IP addresses based on the number of EIPs of your cloud resources.
Service Bandwidth	<b>100Mbps</b>	The service bandwidth indicates clean service bandwidth forwarded to the origin server from the AAD scrubbing center. It is recommended that the service bandwidth be greater than or equal to the egress bandwidth of the origin server. Otherwise, packet loss may occur or services may be affected.
Instance Name	<b>CNAD-test</b>	Name of the purchased instance, which is user-defined.
Enterprise Project	-	This parameter is displayed only when you use an enterprise account for purchase. Select a value based on the site requirements.
Required Duration	-	Select the required duration based on the site requirements.
Quantity	-	Select the quantity based on the site requirements.

Figure 2-2 Setting Unlimited Protection Basic edition specifications

The screenshot displays the configuration interface for the Unlimited Protection Basic Edition. The 'Instance Type' section includes 'Cloud Native Anti-DDoS', 'Advanced Anti-DDoS', 'Advanced Anti-DDoS International', and 'Scheduling Center'. The 'Billing Mode' is set to 'Yearly/Monthly'. The 'Region' is 'Chinese Mainland'. The 'Protection Level' is 'Unlimited Protection Basic Edition'. The 'Specifications' section includes 'Access Mode: Transparent proxy', 'Bandwidth Type: Cloud native network and fully dynamic BGP (static BGP not supported)', 'Protection Capability: Unlimited protection', and 'Protected Resources: Public IP addresses of cloud resources, including ECS, ELB, and EIP'. The 'IP Version' is 'IPv4 and IPv6'. The 'Resource Location' is 'CN North-Beijing4'. The 'Protected IP Addresses' is set to 50. The 'Service Bandwidth' is '100Mbit/s'. The 'Instance Name' is 'CNAD-bdef'. The 'Required Duration' is '3 months'. The 'Auto-renew' checkbox is unchecked. The 'Quantity' is 1.

Instance Type

Cloud Native Anti-DDoS Advanced Anti-DDoS Advanced Anti-DDoS International Scheduling Center

Billing Mode ?

Yearly/Monthly

Region ?

Chinese Mainland Other

Protection Level ?

Unlimited Protection Advanced Edition Unlimited Protection Basic Edition Cloud Native Protection 2.0

Unlimited protection for Cloud EIPs and native networks. [Access Guide](#)

Dedicated WAF must be used.

Specifications

Access Mode: Transparent proxy

Bandwidth Type: Cloud native network and fully dynamic BGP (static BGP not supported).

Protection Capability: Unlimited protection ?

Protected Resources: Public IP addresses of cloud resources, including ECS, ELB, and EIP.

IP Version

IPv4 and IPv6

Resource Location ?

CN North-Beijing4 CN East-Shanghai1 CN South-Guangzhou

Only cloud resources in the region where the purchased instance resides can be protected.

Protected IP Addresses ?

50

Service Bandwidth ?

100Mbit/s 1,000Mbit/s 5,000Mbit/s 10,000Mbit/s 20,000Mbit/s Custom

Instance Name

CNAD-bdef

If you create multiple instances at a time, the system will automatically add a suffix to each instance name, for example, CNAD-0001.

Required Duration

3 months 6 months 1 year

Auto-renew ?

Quantity

1

----End

## Step 2: Creating a Protection Policy

### NOTE

CNAD Advanced supports many types of protection policies. The following uses the cleaning policy as an example.

**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** Click **Create Protection Policy** to create a policy.

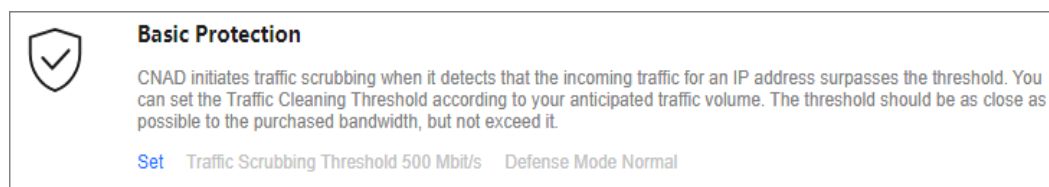
**Table 2-2** Parameter description

Parameter	Example Value	Description
Name	<b>Policy01</b>	Name of the protection policy, which is user-defined.
Instance	Select the instance purchased in <a href="#">Step 4</a> .	Target instance to which the protection policy is associated to.

**Step 3** In the row containing the created policy, click **Configure Policy**. The **Policy Content** page is displayed.

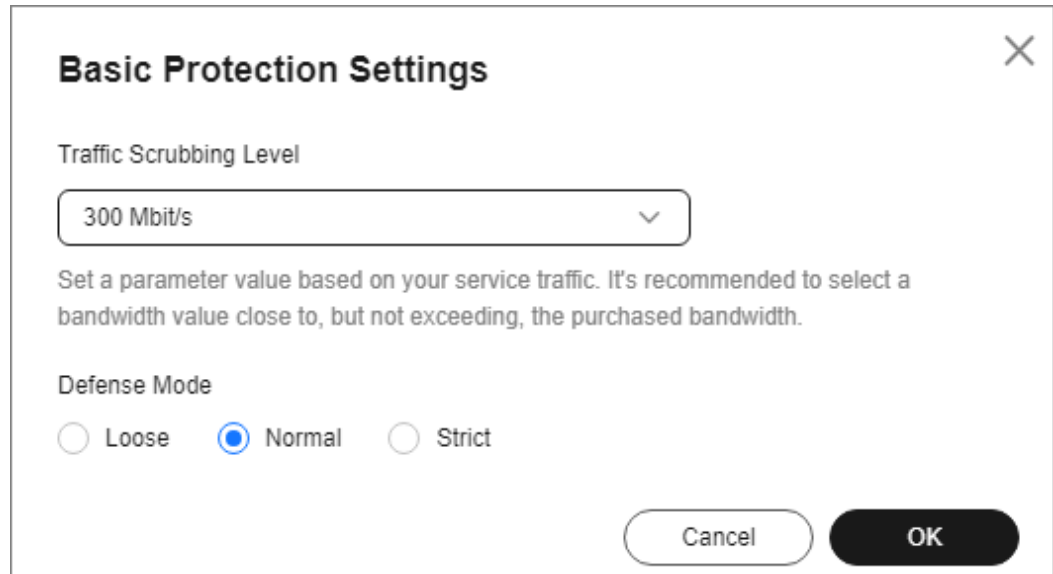
**Step 4** Under **Basic Protection**, click **Set**.

**Figure 2-3** Basic protection



**Step 5** In the **Basic Protection Settings** dialog box that is displayed, set the **Traffic Scrubbing Level** and **Defense Mode**.

**Figure 2-4** Basic protection settings



**Table 2-3** Parameter description

Parameter	Example Value	Description
Traffic Scrubbing Level	<b>300Mbps</b>	If the DDoS bandwidth on an IP address exceeds the configured scrubbing level, CNAD is triggered to scrub attack traffic. You are advised to set a value closest to, but not exceeding, the purchased bandwidth.
Defense Mode	<b>Normal</b>	If the traffic reaches the specified scrubbing level, traffic scrubbing is triggered. <ul style="list-style-type: none"> <li>• <b>Loose:</b> Scrubbing is triggered when the traffic reaches three times of the scrubbing level.</li> <li>• <b>Normal:</b> Scrubbing is triggered when the traffic reaches twice the scrubbing level.</li> <li>• <b>Strict:</b> Scrubbing is triggered when the traffic reaches the scrubbing level.</li> </ul>

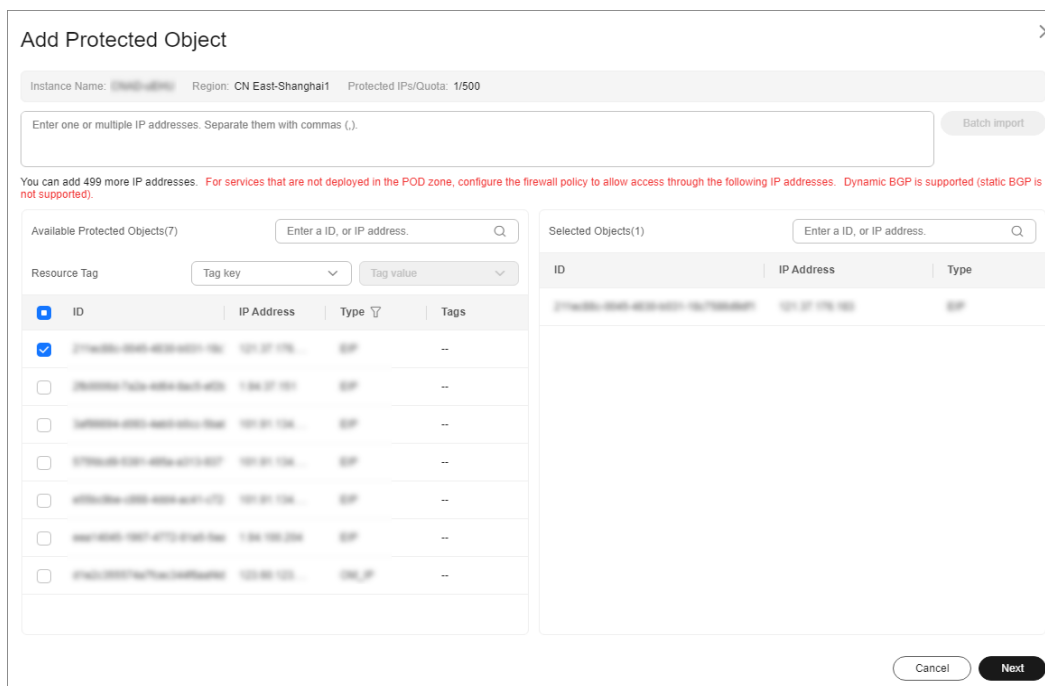
----End

### Step 3: 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 **Select Instance** drop-down box, select the instance purchased in [Step 4](#).
- Step 3** Click **Add Protected Object**. The **Add Protected Object** page appears.

**Step 4** Select the EIP obtained in [Prerequisites](#), and click **Next**.

**Figure 2-5** Adding a protected object



**Step 5** Click **OK**.

----End

## Related Information

- To obtain DDoS attack information in a timely manner, you can set alarm notifications. For details, see [Setting Alarm Notifications](#).
- You can view information such as the traffic trend and attack distribution on the CNAD Advanced console. For details, see [Viewing Statistics Reports](#).

# 3 Quick Access to CNAD - Unlimited Protection Advanced Edition

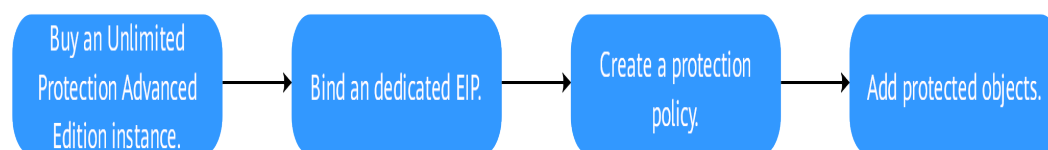
Cloud Native Anti-DDoS Advanced (CNAD) provides higher DDoS protection capability for cloud services on Huawei Cloud such as Elastic Cloud Server (ECS), Elastic Load Balance (ELB), Web Application Firewall (WAF), and Elastic IP (EIP). CNAD Advanced - Unlimited Protection Advanced Edition takes effect for the **Huawei Cloud Anti-DDoS dedicated EIPs**. After a simple configuration, the security features of CNAD Advanced - Unlimited Protection Advanced Edition are integrated into cloud services, enhancing their security and ensuring service protection and reliability.

This section uses CN North-Beijing4 (Chinese mainland) as an example to describe how to purchase and use the Unlimited Protection Advanced Edition.

## Procedure

This section describes how to quickly purchase Unlimited Protection Advanced Edition and enable protection. The process is shown in [Figure 3-1](#).

**Figure 3-1** Procedure



Step	Description
<b>Prerequisites</b>	Register a Huawei ID, enable Huawei Cloud, top up the account, grant CNAD Advanced permissions, and prepare an ECS.
<b>Step 1: Buying an Unlimited Protection Advanced Edition Instance</b>	Purchase Unlimited Protection Advanced Edition in the specified region.




Step	Description
<a href="#">Step 2: Purchasing a Dedicated EIP and Binding It to an ECS</a>	Purchase a dedicated EIP in the specified region and bind it to the prepared ECS.
<a href="#">Step 3: Creating a Protection Policy</a>	Create and configure protection policies for protected objects.
<a href="#">Step 4: Adding a Protected Object</a>	Add protected objects to the Unlimited Protection Advanced Edition instance.

## Prerequisites

- Before using Unlimited Protection Advanced Edition, 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.
- Make sure your account has enough funds to avoid issues when purchasing Unlimited Protection Advanced Edition.
- Ensure that the account has been assigned related permissions. For details, see [Creating a User and Granting the CNAD Access Permission](#).
- In the CN North-Beijing4 region, create an ECS. For details, see section [Purchasing an ECS](#).

## Step 1: Buying 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 DDoS Mitigation**.

**Step 4** Set the purchase parameters as required, click **Buy Now**, and complete the payment as prompted.

**Table 3-1** Parameter description

Parameter	Example Value	Description
Instance Type	<b>Cloud Native Anti-DDoS</b>	Type of the instance to be purchased.

Parameter	Example Value	Description
Billing Mode	<b>Yearly/Monthly</b>	You are charged based on the subscription period. This means that you have to pay for a certain period of time in advance.  Unlimited Protection Advanced Edition supports only the yearly/monthly billing mode.
Region	<b>Chinese Mainland</b>	<ul style="list-style-type: none"> <li>• <b>Chinese Mainland:</b> applies to scenarios where service servers are deployed in Chinese mainland (cross-region deployment is supported). Only dynamic BGP EIPs are supported.</li> <li>• <b>Other:</b> applies to scenarios where the service server is deployed in the Asia Pacific region (Hong Kong is supported currently). Only premium BGP EIPs are supported.</li> </ul>
Protection Level	<b>Unlimited Protection Advanced Edition</b>	Edition to be purchased.
Resource Location	<b>CN North-Beijing4</b>	Region where the protected cloud resources are located. Cross-region protection is not supported.
Protected IP Addresses	<b>50</b>	The number of protected IP addresses refers to the number of EIPs that can be protected by each CNAD Advanced instance. You are advised to evaluate the number of protected IP addresses based on the number of EIPs of your cloud resources.
Service Bandwidth	<b>100Mbps</b>	The service bandwidth indicates clean service bandwidth forwarded to the origin server from the AAD scrubbing center. It is recommended that the service bandwidth be greater than or equal to the egress bandwidth of the origin server. Otherwise, packet loss may occur or services may be affected.
Instance Name	<b>CNAD-test</b>	Name of the purchased instance, which is user-defined.
Enterprise Project	-	This parameter is displayed only when you use an enterprise account for purchase. Select a value based on the site requirements.
Required Duration	-	Select the required duration based on the site requirements.

Parameter	Example Value	Description
Quantity	-	Select the quantity based on the site requirements.

Figure 3-2 Unlimited Protection Advanced Edition

Instance Type

**Cloud Native Anti-DDoS** Advanced Anti-DDoS Advanced Anti-DDoS International Scheduling Center

Billing Mode ⓘ

**Yearly/Monthly**

Region ⓘ

**Chinese Mainland** Other

Protection Level ⓘ

**Unlimited Protection Advanced Edition** Unlimited Protection Basic Edition Cloud Native Protection 2.0

Unlimited protection for exclusive EIPs, with higher protection bandwidth.  
Exclusive EIPs are not available to all users. After you purchase the Unlimited Protection Advanced Edition, the system automatically allows you to purchase exclusive EIPs. [Access Guide](#)  
Dedicated WAF must be used.

Specifications

Access Mode: Transparent proxy

Bandwidth Type: Cloud native network, multi-line BGP

Protection Capability: Unlimited protection

Protected Resources: Anti-DDoS Exclusive EIP

IP Version

IPv4

Resource Location ⓘ

CN North-Beijing2 **CN North-Beijing4** CN East-Shanghai1 CN South-Guangzhou

Only cloud resources in the region where the purchased instance resides can be protected.

Protected IP Addresses ⓘ

- 50 +

Service Bandwidth ⓘ

**100Mbit/s** 500Mbit/s 1,000Mbit/s 2,000Mbit/s 5,000Mbit/s 10,000Mbit/s Custom

This bandwidth is for the scrubbed traffic flow from the AAD equipment room to the origin server. To prevent potential packet loss and ensure uninterrupted service, it is advisable to set the service bandwidth no less than the origin server's egress bandwidth.

Instance Name

CNAD-d8c5

If you create multiple instances at a time, the system will automatically add a suffix to each instance name, for example, CNAD-0001.

Required Duration

**3 months** 6 months 1 year

Auto-renew ⓘ

Quantity

- 1 +

----End

## Step 2: Purchasing a Dedicated EIP and Binding It to an ECS

**Step 1** Purchase a dedicated EIP in the CN North-Beijing4 region by referring to [Assigning an EIP](#).

 **NOTE**

The EIP line in the CN North-Beijing4 region is **5\_DDoSAlways1bgp**. The actual line is displayed on the console.

**Step 2** Bind the purchased dedicated EIP to the ECS in [Prerequisites](#) by referring to [Binding an EIP to an Instance](#).

----End

## Step 3: Creating a Protection Policy

 **NOTE**

CNAD Advanced supports many types of protection policies. The following uses the cleaning policy as an example.

**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** Click **Create Protection Policy** to create a policy.

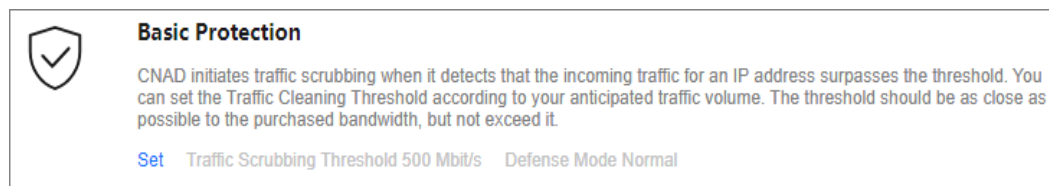
**Table 3-2** Parameter description

Parameter	Example Value	Description
Name	<b>Policy01</b>	Name of the protection policy, which is user-defined.
Instance	Select the instance purchased in <a href="#">Step 4</a> .	Target instance to which the protection policy is associated to.

**Step 3** In the row containing the created policy, click **Configure Policy**. The **Policy Content** page is displayed.

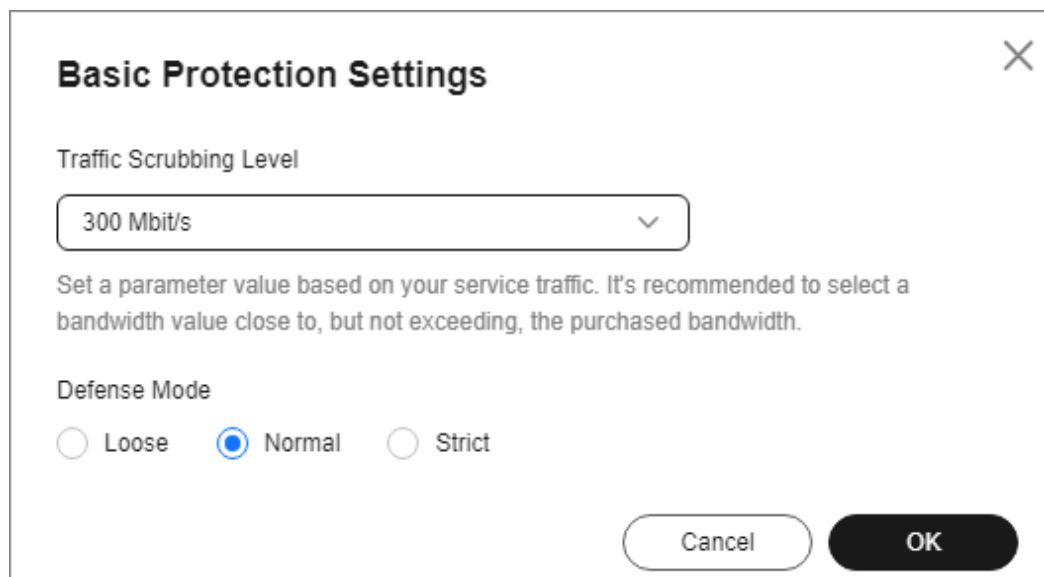
**Step 4** Under **Basic Protection**, click **Set**.

**Figure 3-3** Basic protection



**Step 5** In the **Basic Protection Settings** dialog box that is displayed, set the **Traffic Scrubbing Level** and **Defense Mode**.

**Figure 3-4** Basic protection settings



**Table 3-3** Parameter description

Parameter	Example Value	Description
Traffic Scrubbing Level	<b>300Mbps</b>	If the DDoS bandwidth on an IP address exceeds the configured scrubbing level, CNAD is triggered to scrub attack traffic. You are advised to set a value closest to, but not exceeding, the purchased bandwidth.
Defense Mode	<b>Normal</b>	If the traffic reaches the specified scrubbing level, traffic scrubbing is triggered. <ul style="list-style-type: none"> <li>• <b>Loose:</b> Scrubbing is triggered when the traffic reaches three times of the scrubbing level.</li> <li>• <b>Normal:</b> Scrubbing is triggered when the traffic reaches twice the scrubbing level.</li> <li>• <b>Strict:</b> Scrubbing is triggered when the traffic reaches the scrubbing level.</li> </ul>

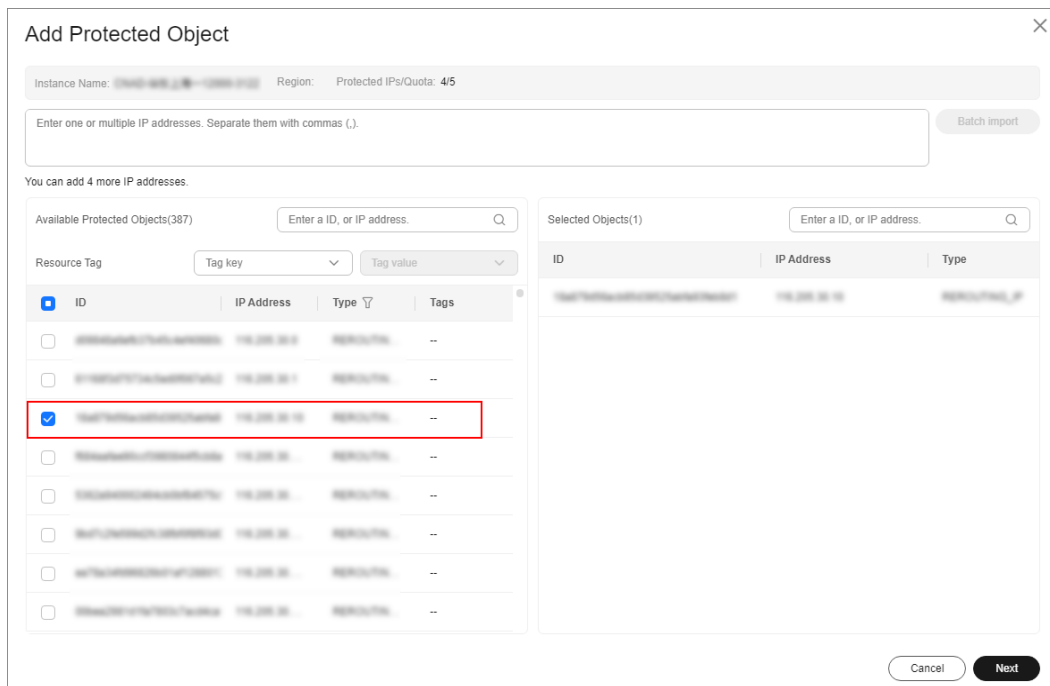
----End

## 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 **Select Instance** drop-down box, select the instance purchased in [Step 4](#).
- Step 3** Click **Add Protected Object**. The **Add Protected Object** page appears.

**Step 4** Select the dedicated EIP prepared in [Prerequisites](#) and click **Next**.

**Figure 3-5** Adding a protected object



**Step 5** Click **OK**.

----End

## Related Information

- To obtain DDoS attack information in a timely manner, you can set alarm notifications. For details, see [Setting Alarm Notifications](#).
- You can view information such as the traffic trend and attack distribution on the CNAD Advanced console. For details, see [Viewing Statistics Reports](#).

# 4 Quick access to Cloud Native Anti-DDoS 2.0

Cloud Native Anti-DDoS 2.0 (CNAD 2.0) 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 2.0 defends against the DDoS attacks targeting the Huawei Cloud EIPs and provides higher protection capabilities for cloud services. With few clicks on the console, you can enjoy always-on DDoS mitigation on Huawei Cloud.

**CNAD 2.0 supports both common EIPs and Anti-DDoS Service dedicated EIPs in the Chinese mainland, as well as premium BGP EIPs and Anti-DDoS Service dedicated EIPs outside the Chinese mainland.**

This section uses a common EIP in the Chinese mainland as an example to describe how to purchase and use CNAD 2.0.

## Procedure

This section describes how to quickly purchase CNAD 2.0 and enable protection. The process is shown in [Figure 4-1](#).

**Figure 4-1** Procedure



Step	Description
<b>Prerequisites</b>	Register a Huawei ID, enable Huawei Cloud, top up the account, grant CNAD Advanced permissions, and prepare protected objects.




Step	Description
<a href="#">Step 1: Buying a Cloud Native Anti-DDoS 2.0 Instance</a>	Purchase CNAD 2.0 in a specified region.
<a href="#">Step 2: Creating a Protection Policy</a>	Create and configure protection policies for protected objects.
<a href="#">Step 3: Adding a Protected Object</a>	Add protected objects to the CNAD 2.0 instance.

## Prerequisites

- Before using Unlimited Protection Basic Edition, 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.
- Make sure that your account has sufficient balance, or you may fail to pay to your CNAD 2.0 orders.
- Ensure that the account has been assigned related permissions. For details, see [Creating a User and Granting the CNAD Access Permission](#).
- Create an ECS and bind an EIP to it. For details, see section [Purchasing an ECS](#).

## Step 1: Buying a Cloud Native Anti-DDoS 2.0 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 DDoS Mitigation**.

**Step 4** Set the purchase parameters as required, click **Buy Now**, and complete the payment as prompted.

**Table 4-1** Parameter description

Parameter	Example Value	Description
Instance Type	<b>Cloud Native Anti-DDoS</b>	Type of the instance to be purchased.
Billing Mode	<b>Yearly/Monthly</b>	You are charged based on the subscription period. This means that you have to pay for a certain period of time in advance. Currently, only the yearly/monthly billing mode is supported.

Parameter	Example Value	Description
Region	<b>Chinese Mainland</b>	<ul style="list-style-type: none"> <li>• <b>Chinese Mainland:</b> applies to scenarios where service servers are deployed in Chinese mainland (cross-region deployment is supported). Only dynamic BGP EIPs are supported.</li> <li>• <b>Other:</b> applies to scenarios where the service server is deployed in the Asia Pacific region (Hong Kong is supported currently). Only premium BGP EIPs are supported.</li> </ul>
Protection Level	<b>Cloud Native Anti-DDoS 2.0</b>	Edition to be purchased.
Protected IP Addresses	<b>50</b>	The number of protected IP addresses refers to the number of EIPs that can be protected by each CNAD Advanced instance. You are advised to evaluate the number of protected IP addresses based on the number of EIPs of your cloud resources.
Billing Mode for Public Network Lines	<b>Pay-per-use</b>	<ul style="list-style-type: none"> <li>• <b>Yearly/Monthly:</b> You need to pay for a certain period of time in advance and are charged based on the service bandwidth.</li> <li>• <b>Pay-per-use:</b> Charges are incurred daily based on the volume of scrubbed traffic.</li> </ul>
Metering Rule	<b>Scrubbed traffic</b>	Scrubbed traffic refers to normal service traffic that is not polluted by attacks, excluding attack traffic.
Service Bandwidth	<b>100Mbps</b>	<p>The service bandwidth indicates clean service bandwidth forwarded to the origin server from the AAD scrubbing center. It is recommended that the service bandwidth be greater than or equal to the egress bandwidth of the origin server. Otherwise, packet loss may occur or services may be affected.</p> <p>This parameter is displayed only when you select <b>Yearly/Monthly</b> for <b>Billing Mode for Public Network Lines</b>.</p>
Instance Name	<b>CNAD-test</b>	Name of the purchased instance, which is user-defined.
Enterprise Project	-	This parameter is displayed only when you use an enterprise account for purchase. Select a value based on the site requirements.
Required Duration	-	Select the required duration based on the site requirements.

Parameter	Example Value	Description
Quantity	-	Select the quantity based on the site requirements.

Figure 4-2 Cloud Native Anti-DDoS 2.0

Instance Type

Cloud Native Anti-DDoS Advanced Anti-DDoS Advanced Anti-DDoS International Scheduling Center

Billing Mode ?

Yearly/Monthly

Region ?

Chinese Mainland Other

Protection Level ?

Unlimited Protection Advanced Edition Unlimited Protection Basic Edition Cloud Native Protection 2.0

Specifications

Access Mode: Transparent proxy

Bandwidth Type: Cloud native network and fully dynamic BGP (static BGP not supported).

Protection Capability: Unlimited protection ?

Protected Resources: Public IP addresses of cloud resources, including ECS, ELB, and EIP.

IP Version

IPv4 and IPv6

Resource Location

Chinese mainland regions (including CN North-Beijing4, CN East-Shanghai1, and CN South-Guangzhou. Cross-region protection is supported.)

Protected IP Addresses ?

50

Billing Mode for Public Network Lines ?

Yearly/Monthly Pay-per-use

Metering Rule ?

Scrubbed traffic

Billed based on the scrubbed traffic generated every day. [Pricing Details](#)

Instance Name

CNAD-e26b

If you create multiple instances at a time, the system will automatically add a suffix to each instance name, for example, CNAD-0001.

Required Duration

1 month 3 months 6 months 1 year

Auto-renew ?

Quantity

1

----End

## Step 2: Creating a Protection Policy

### NOTE

CNAD Advanced supports many types of protection policies. The following uses the cleaning policy as an example.

**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** Click **Create Policy** to create a policy.

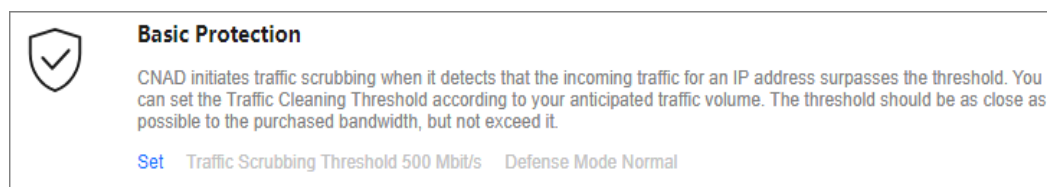
**Table 4-2** Parameter description

Parameter	Example Value	Description
Name	<b>Policy01</b>	Name of the protection policy, which is user-defined.
Instance	Select the instance purchased in <a href="#">Step 4</a> .	Target instance to which the protection policy is associated to.

**Step 3** In the row containing the created policy, click **Configure Policy**. The **Policy Content** page is displayed.

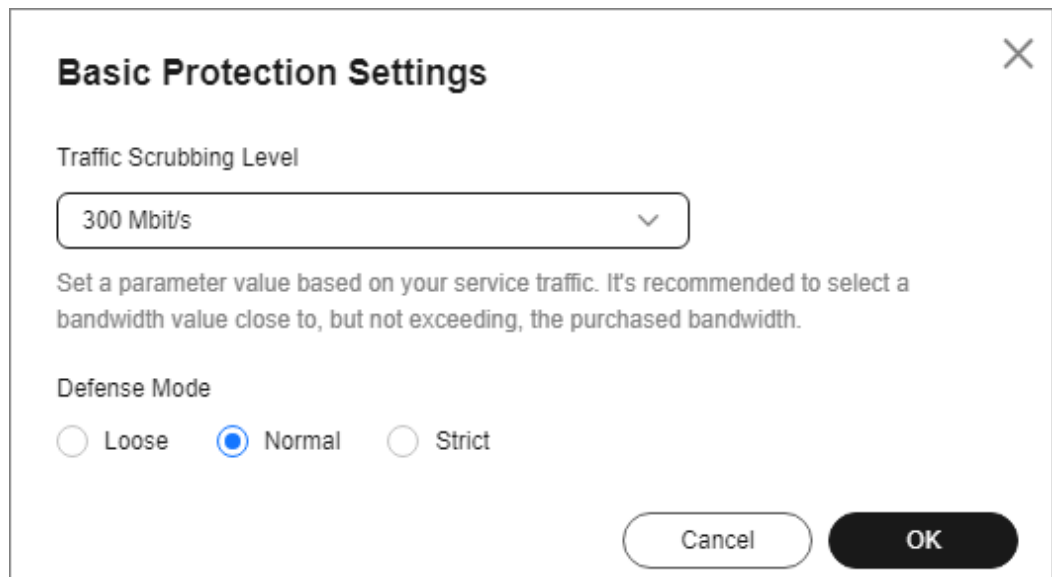
**Step 4** Under **Basic Protection**, click **Set**.

**Figure 4-3** Basic protection



**Step 5** In the **Basic Protection Settings** dialog box that is displayed, set the **Traffic Scrubbing Level** and **Defense Mode**.

**Figure 4-4** Basic protection settings



**Table 4-3** Parameter description

Parameter	Example Value	Description
Traffic Scrubbing Level	<b>300Mbps</b>	If the DDoS bandwidth on an IP address exceeds the configured scrubbing level, CNAD is triggered to scrub attack traffic. You are advised to set a value closest to, but not exceeding, the purchased bandwidth.
Defense Mode	<b>Normal</b>	If the traffic reaches the specified scrubbing level, traffic scrubbing is triggered. <ul style="list-style-type: none"> <li>• <b>Loose:</b> Scrubbing is triggered when the traffic reaches three times of the scrubbing level.</li> <li>• <b>Normal:</b> Scrubbing is triggered when the traffic reaches twice the scrubbing level.</li> <li>• <b>Strict:</b> Scrubbing is triggered when the traffic reaches the scrubbing level.</li> </ul>

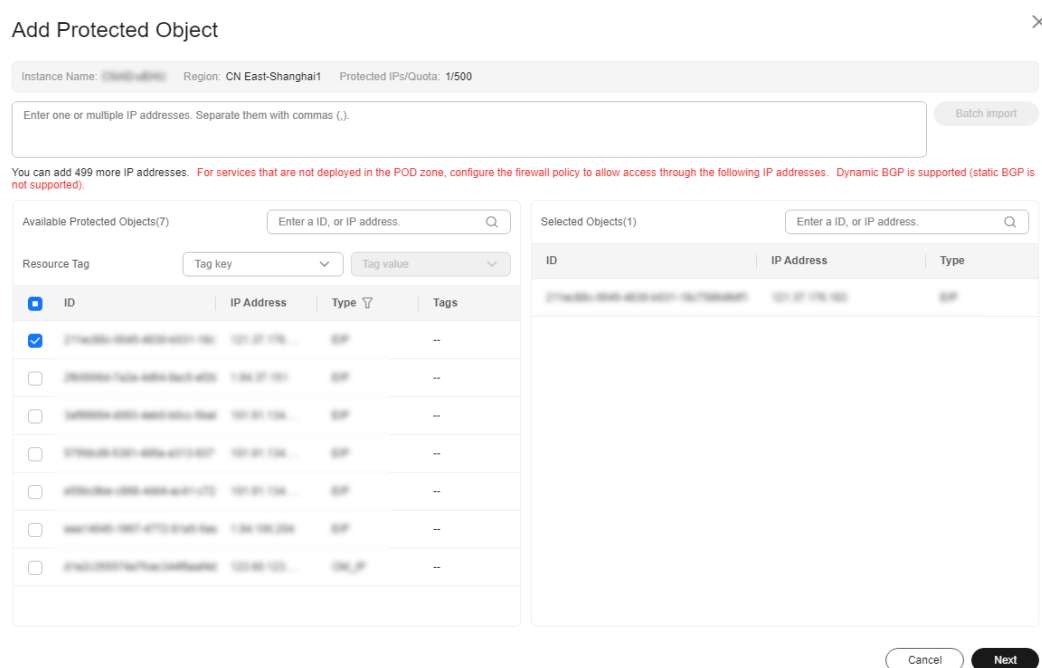
----End

### Step 3: 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 **Select Instance** drop-down box, select the instance purchased in [Step 4](#).
- Step 3** Click **Add Protected Object**. The **Add Protected Object** page appears.

**Step 4** Select the EIP prepared in [Prerequisites](#) and click **Next**.

**Figure 4-5** Adding a protected object



**Step 5** Click **OK**.

----End

## Related Information

- To obtain DDoS attack information in a timely manner, you can set alarm notifications. For details, see [Setting Alarm Notifications](#).
- You can view information such as the traffic trend and attack distribution on the CNAD Advanced console. For details, see [Viewing Statistics Reports](#).

# 5 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 5-1** DDoS protection

Version	Practice	Description
Anti-DDoS	Usage process	<a href="#">How Do I Use CNAD Basic?</a> Quickly use Anti-DDoS.
	Routine maintenance	<a href="#">Accessing a Black-holed Server Through ECS</a> Use an ECS to remotely access the server that has been blackholed.
CNAD	Joint protection	<a href="#">Using CNAD in Combination with ELB</a> You can use CNAD + ELB to protect your services deployed on Huawei Cloud ECSs against DDoS attacks.
Anti-DDoS scheduling center	Joint protection	<a href="#">Best Practices of Tiered DDoS Scheduling</a> If you enabled auto AAD when purchasing CNAD Unlimited Protection Basic, you can configure a tiered scheduling policy to automatically engage AAD for cloud resources protected by CNAD Unlimited Protection Basic.