Anti-DDoS Service

Getting Started with Common Practices

 Issue
 01

 Date
 2023-09-11





HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. 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

NUAWEI 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 Quick Access to CNAD - Unlimited Protection Basic Edition	. 5
3 Quick Access to CNAD - Unlimited Protection Advanced Edition	. 8
4 Getting Started with Common Practices1	11

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

Public IP Addresses	Security Report	Alarm Notifications	Logs				
You can configure protection	n for 345 more IP addres	ses.					
Set Default Protection P	olicy Enable Ant	i-DDoS for All IP Addresses	Set Protection				
Q Public IP Addresses	214 × A	dd filter					
Public IP Address	ses 🍦	Protection Status		Asset Type	Protection Settings		Enterprise Project
214		📀 Normal (Default)		EIP	Traffic Cleaning Threshold	120 Mbit/s	default

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

Public IP Addresses	Security Report	Alarm Notifications	Logs
i Alarm notificatio Only scrubbing	ns may be intercepted as span alarms can be configured here.	n. If you are not receiving no To configure black hole blo	otifications, check your spam folder or email filter settings. cking alarms, go to the CES event monitoring page. How do I configure CES blackhole blocking event alarms'
Alarm Notifications			
SMN Topic	antiddos_007	✓ Q View Topic	
1	'he drop-down list only displays	SMN topics with at least o	ne confirmed subscription.
Apply			

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

Public IP Addresses	Security Report Alarm Notifications Logs								
You can configure protection	You can configure protection for 345 mole IP addresses.								
Set Default Protection P	licy Enable Anti-DDoS for All IP Addresses Set Protection								
Q Public IP Addresses:	214 × Add filter				× Q (\$				
Public IP Address	Protection Status	Asset Type	Protection Settings	Enterprise Project	Operation				
.214	📀 Normal (Default)	EIP	Traffic Cleaning Threshold 120 Mbit/s	default	View Monitoring Report Set Protection Tag				
10 V Total Records	10 v Total Records: 1 < 1 >								

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

Figure 1-4 Modifying protection settings

Protection Settings		×
Public IP Address	214	
Set Protection	O Default 💿 Custom	
Traffic Cleaning Threshold ⑦	150 Mbit/s V	
	Cancel	

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

Public IP Addresses Security Rep	port Alarm Notifications Logs								
You can configure protection for 345 more IP	You can configure protection for 345 more IP addresses.								
Set Default Protection Policy En	able Anti-DDoS for All IP Addresses Set Prote	ection							
Q Public IP Addresses:	× Add filter				× Q 0				
Public IP Addresses 🖨	Protection Status	Asset Type	Protection Settings	Enterprise Project	Operation				
214	Normal (Default)	EIP	Traffic Cleaning Threshold 120 Mbit/s	default	View Monitoring Report Set Protection Tag				

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

Ami-DDoS / 214										
Public IP Address	C Protection Details Set Protection									
Public IP Address 214	Protection Status 🥥 Normal (Default) Traffic Cleaning Threshold 128 Mobils									
Monitoring Period Feb 29, 2024 11:12:03 GMT+08:00 - Mar 01, 2024 11:07:03 GMT+08:00	Montoring Period Feb 29, 2024 11:12 03 GMT+06 00 - Mar 01, 2024 11:07 03 GMT+06 00									
Kbi/s	Inbound normal traffic									
0.5										
0.4										
1111203 12:1709 13:22:03 14:27:03 15:32:03 16:37:03 17:42:09 18:47:03 19:52:03 20:57:03 22:02:03 2 Start Time End Time	380709 00.12.09 01.17.09 02.22.09 0327.09 04.32.09 05.37.09 06.42.09 07.47.09 08.52.09 09.57.09 11.02.02 Status									
No dati	1 / zvenilatio									

----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.

Instance Type	Native DDoS protection
Billing Mode 🕜	Yearly/Monthly
Protection Level (?)	Unlimited Protection Advanced Edition Unlimited Protection Basic Edition
	Unlimited protection for Cloud EIPs and native networks. Access Guide Exclusive 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 ③ 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 CN Southwest-Guiyang1
	Only cloud resources in the region where the purchased instance resides can be protected.
Protected IP Addresses ⑦	- 50 +
	100 Mbit/s

Figure 2-1 Setting Unlimited 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

- Protected IPs/Quota: 0/1			
them with commas (,).			Batch import
Enter a name, ID, or IP address.	Q Selected Obj	Enter a name, IE), or IP address. Q
✓ Tag value	Name/ID	IP Address	Туре
ddress Type 🍸 Tag	s acda1a	726587	REROUTING_IP
REROUTING			
	them with commas (.).	them with commas (.).	them with commas (.). Enter a name, ID, or IP address. Tag value ddress Type Ty Tags REROUTING REROUTING.

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.

Instance Type	Native DDoS protection
Billing Mode 🕜	Yearly/Monthly
Protection Level ⑦	Unlimited Protection Advanced Edition Unlimited Protection Basic Edition
	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 Exclusive 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 Exlusive 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 +
	100 Mbit/s
Service Bandwidth 🧿	(II) 100 5,000 10,000 15,000 20,000 25,000 30,000 35,000 40,000 - 100 +
	The amount of service handwidth forwarded to the origin server after traffic scrubbing. You are advised to select bandwidth at least equal to the egress handwidth of the origin server or there may be packet loss and service quality may suffer.

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



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

Instance	Name:	Region:	Protected IPs/Q	uota: 0/1					
Enter or	ie or multiple IP addr	esses. Separate them	with commas (,)	l.					Batch import
ou can a	dd 0 more IP address	Ges.							
Availabl	e Protected Objects(503)	Enter a name	ID, or IP add	iress.	Q	Selected Objects(1)	Enter a name, ID,	or IP address. Q
Resourc	ce Tag	Tag key	~	Tag value			Name/ID	IP Address	Туре
٥	Name/ID	IP Addres	ss Type	7	Tags	0	 acda1: 726587	110,200,20-40	REROUTING_IP
	 739ci	715684	RER	DUTING					
	 acda	2d03f38	RER	DUTING					
	 bb9bi	5a3818	RER	DUTING					
	 9a204	868505	RER	DUTING					
	 b6d4;	85eb5c	RER	DUTING					
	 093b:	94c809	RER	DUTING					

----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.

Version	Pract	ice	Description
Anti-DDoS	Rout ine	Configuring Alarm Notifications	Enable alarm notification for DDoS attacks.
	mai nten ance	Connecting to a Server Routed to a Black Hole	Use an ECS to remotely access the server that has been blackholed.
	Prot ecti on upgr ade	Enhancing Anti- DDoS Service Capabilities	Purchase an AAD edition of higher specifications.

Table 4-1 DDoS protection