DDoS Mitigation

FAQs

Issue 06

Date 2021-04-27



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2021. 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 Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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.

Contents

1 General FAQs..... 1
1.1 What Are Regions and AZs?..... 1
1.2 What Is the Black Hole Policy of HUAWEI CLOUD?..... 2
1.3 What are the Relationships Between DDoS Mitigation and the Anti-DDoS, CNAD Pro, and AAD Services?..... 5
1.4 What Are the Differences Between Anti-DDoS and Advanced Anti-DDoS?..... 5
1.5 What Are a SYN Flood Attack and an ACK Flood Attack?..... 6
1.6 What Is a CC Attack?..... 6
1.7 What Is a Slow HTTP Attack?..... 6
1.8 What Are a UDP Attack and a TCP Attack?..... 7
1.9 What Are the Differences Between DDoS Attacks and Challenge Collapsar Attacks?..... 7
1.10 What Is the Maximum Protection Capacity Provided by HUAWEI CLOUD Anti-DDoS for Free?..... 9
1.11 What Can I Do If an IP Address Is Blocked?..... 9
2 CNAD Basic (Anti-DDoS) FAQs..... 11
2.1 About Anti-DDoS..... 11
2.1.1 What Is the Million-level IP Address Blacklist Database?..... 11
2.1.2 How Will Anti-DDoS Be Triggered to Scrub Traffic?..... 11
2.1.3 Does Anti-DDoS Traffic Cleaning Affect Normal Services?..... 11
2.1.4 How Does Anti-DDoS Scrub Traffic?..... 11
2.1.5 What Are the Restrictions of Anti-DDoS?..... 12
2.1.6 What Is the Protection Capacity of Anti-DDoS?..... 12
2.1.7 What Data Can Be Provided by Anti-DDoS?..... 12
2.1.8 Which Regions Does Anti-DDoS Support?..... 12
2.1.9 Which Services Can Use Anti-DDoS?..... 12
2.1.10 Can Anti-DDoS Be Used Across Clouds?..... 12
2.1.11 How to Determine Whether an Attack Occurs?..... 13
2.2 About Basic Functions..... 13
2.2.1 What Is the HTTP Request Threshold Set for Anti-DDoS Protection?..... 13
2.2.2 What Would Happen When I Am Under a DDoS Attack Exceeding 5 Gbit/s?..... 13
2.2.3 Which Types of Attacks Does Anti-DDoS Mitigate?..... 13
2.2.4 What Should I Do If My Service Is Frequently Attacked?..... 13
2.2.5 What Is the Difference Between ELB Protection and ECS Protection?..... 14

 Copyright © Huawei Technologies Co., Ltd.

2.2.6 Why Is the Number of Times of Cleaning Different from the Number of Attacks for the Same Public IP Address? 14
2.2.7 Is Anti-DDoS Enabled by Default? 14
2.2.8 Does Anti-DDoS Protect a Region or a Single IP Address? 14
2.2.9 How Do I Temporarily Disable Anti-DDoS? 14
2.2.10 Do I Need to Clear the Resources of Anti-DDoS When I Delete an Account? 16
2.2.11 How Do I View the Traffic Cleaning Frequency? 16
2.2.12 How Can I View Anti-DDoS Protection Statistics? 16
2.2.13 How Can I View Public IP Address Monitoring Data in Anti-DDoS? 17
2.2.14 How Can I View the Change History of Anti-DDoS? 17
2.2.15 How Can I View an Interception Report? 17
2.2.16 How Do I Select an AZ in Anti-DDoS? 17
2.2.17 Can I Disable Anti-DDoS Completely? 17
2.2.18 How Do I Check Whether the Inbound Traffics Are Routed Through Anti-DDoS Devices? 17
2.3 About Threshold and Black Hole 18
2.3.1 How Does the Traffic Cleaning Threshold Take Effect in Anti-DDoS? 18
2.3.2 How Do I Set the Anti-DDoS Traffic Cleaning Threshold? 19
2.3.3 How Can I Adjust the Block Threshold? 19
2.3.4 Do I Need to Manually Enable the Free-of-Charge 5 Gbit/s DDoS Protection Provided by Anti-DDoS? 19
2.4 About Alarm notification 19
2.4.1 Will I Be Promptly Notified When an Attack Is Detected? 19
2.4.2 What Should I Do If I Receive an Alarm Notification? 19
2.4.3 How Do I Disable the Alarm Notification? 20
2.5 About Service Faults 22
2.5.1 Why Is the Traffic Volume of a Public IP Address is Low? 22
2.5.2 Why Is the Access from the Internet Abnormal? 22
2.5.3 Traffic Scrubbed Unexpectedly Without Traffic Fluctuations Reported 23
2.5.4 What Should I Do If Access to a Client Is Denied Due to DDoS Attacks? 23
2.5.5 How Do I Query the Protection Information About a Public IP Address That Is Under DDoS Attacks? 23
2.5.6 Is Traffic Cleaning Triggered Even If No Attack Occurs? 23
3 Product 24
3.1 What Is Unlimited Protection? 24
3.2 Can CNAD Pro Protect Non-HUAWEI CLOUD and On-Premises IP Addresses? 24
4 AAD FAQs 25
4.1 Function Specifications 25
4.1.1 What Forwarding Protocols Does AAD Support? 25
4.1.2 What Carrier Lines Does AAD Support? 28
4.1.3 What Basic and Elastic Protection Bandwidths Does Each Carrier Line Support? 28
4.1.4 Can I Change My Protection Bandwidths? 29
4.1.5 Can an AAD Origin Server Use a CDN CNAME? 29

 Copyright © Huawei Technologies Co., Ltd.

4.1.6 How Many Ports and Protected Domain Names Can an AAD Instance Provide? Is the Quota Expansion Supported? 29
4.1.7 What Is the Maximum Protection Capability When I Purchase 10 Gbit/s as the Basic Protection Bandwidth and 20 Gbit/s as the Elastic Protection Bandwidth? 29
4.1.8 Does AAD Use a Public IP Address to Switch Traffic Back to Origin Servers? 29
4.1.9 What Is the Maximum Number of Domain Names AAD Can Protect? 30
4.1.10 How Much Additional Latency Will Be Incurred When AAD Is Deployed? 30
4.1.11 Is There a Limit to the Number of Concurrent Requests? 30
4.1.12 How Do I Disable Advanced Anti-DDoS? 30
4.2 Access Configuration 30
4.2.1 Can I Connect My Service System to AAD If It Is Not Running on HUAWEI CLOUD? 30
4.2.2 How Do I Connect Website Services to AAD? 30
4.2.3 How Do I Connect Non-Website Services to AAD? 30
4.2.4 How Do I Check Whether a Protected Domain Name Is Correctly Configured After I Connect It to AAD? 31
4.2.5 What Can I Do When Message "Invalid request" Is Displayed When I Upload an HTTPS/WebSockets Certificate? 32
4.2.6 How Do I Convert a Non-PEM Certificate into a PEM One? 32
4.2.7 How Do I Enable Both AAD and WAF? 32
4.2.8 Can an Unrecorded Domain Name Be Protected by AAD (Chinese Mainland)? 33
4.2.9 How Do I Connect My Service System to AAD? 33
4.2.10 How Is CNAME-based Access Implemented? 33
4.2.11 How Does AAD Distribute Traffic When There Are Multiple Origin Servers? 34
4.2.12 How Do I Check Whether a Back-to-Origin IP Address Has Been Whitelisted on My Origin Server? 34
4.2.13 How Do I Change the Exposed IP Address of an Origin Server? 36
4.2.14 How Do I Query the Back-to-Origin IP Address Range? 38
4.2.15 How Do I Delete AAD Instances? 40
4.2.16 Can I Migrate Enterprise Project Resources After Adding the Protected Domain Name? 40
4.2.17 Can I Build My Own Anti-DDoS System Using HUAWEI CLOUD ECSs? 40
4.2.18 How Do the AAD Blacklist and Whitelist Protect Customer's Servers? 40
4.2.19 What Can I Do If the System Displays a Message Indicating that the Domain Name to Be Added Shares the High-Defense IP Address and Port with Another Domain Name But the Domain Names Have Different Origin Server Types When I Connect Website Services to AAD? 40
4.2.20 Does the Back-to-Origin IP Address Target the Origin Server IP Address or Domain Name After AAD Is Configured for Website Services? 43
4.2.21 Can I Configure the Same Port in Forwarding Rules? 44
4.2.22 Do I Need to Configure Forwarding Rules for All Lines of an AAD Instance? 44
4.3 Faults 44
4.3.1 What Should I Do When Encountering an Access Freezing, Delay, or Failure? 44
4.3.2 Why Is Error 504 Displayed When I Access a Website After AAD Is Configured? 47
4.3.3 How Do I Identify the Type of Attacks? 47
4.3.4 What Should I Do If Error 500, 502, or 504 Is Reported When I Access My Website After I Enable Basic Web Protection for My Domain Name? 48
4.3.5 What Does Duplicate forwarding rule Mean? 51

 Copyright © Huawei Technologies Co., Ltd.

4.3.6 What Can I Do If I Failed to Configure a Forwarding Rule?....51
4.3.7 What Can I Do If My UDP Traffic Is Blocked?....51
4.3.8 Why Is a Domain Name Error Reported When I Add a WAF CNAME for Interworking Between AAD and WAF?....51
4.3.9 How Do I Unblock the Access That Has Been Automatically Blocked Due to the Threshold-Overtopped Attack Traffic?....51
4.3.10 What Can I Do If the Access Status of a Protected Domain Name Remains Abnormal After the IP Address of the Origin Server Has Been Changed?....52
4.4 Product....53
4.4.1 Can a Third-Party Server or an On-Premises Server Use HUAWEI CLOUD Advanced Anti-DDoS?....53
4.4.2 What Is a Protected IP Address?....53
4.4.3 Does AAD Support Weighted Back-to-Origin?....53
4.4.4 Can AAD Obtain Real IP Addresses from a Windows Origin Server?....54
4.4.5 Can AAD Be Used Across Regions?....54
4.4.6 Can Multiple Accounts Share Same AAD Instances?....54
4.4.7 What Is a CNAME Record?....54
4.4.8 What is BGP?....54
4.4.9 What Is the Origin Server Port of AAD?....55
4.4.10 What Is the Origin Server IP Address?....55
4.4.11 What Is the Website IP Address Protected by AAD?....55
4.4.12 What Is Service Bandwidth?....55
4.4.13 How Do I Access AAD?....55
4.4.14 What Is an AAD Instance?....56
4.4.15 What Is a Forwarding Protocol?....56
4.4.16 Are Services Interrupted When They Are Being Connected to AAD?....56
4.4.17 Can I Use AAD If My Service Severs Are Deployed Outside Chinese Mainland?....56
4.4.18 Can AAD Provide Protection for Domain Names?....56
4.4.19 Can a Domain Name Be Bound to Multiple AAD Instances?....56
4.4.20 Why Does the High-Defense IP Address Actually Receive Access Requests from a Client After AAD Is Deployed?....56
4.4.21 Why Does the Attack Traffic Volume Increase After AAD Is Deployed?....57
4.4.22 Will the Origin Server Be Exposed When the Attack Traffic Volume Increases After AAD Is Deployed?....57
4.4.23 How Does AAD Protect the Origin Server IP Address?....57
4.4.24 What Information Can I Obtain in the CC Attack Protection Statistics?....57
4.4.25 How Do I Obtain the AAD Sales License?....57
4.4.26 Does AAD Support Two-Way SSL Authentication?....57
4.4.27 Can I Modify or Delete the Certificates Uploaded to AAD?....57
4.4.28 Does AAD Support Wildcard Domain Names?....58
4.4.29 What Will Happen If My Service Traffic Exceeds the Configured Service Bandwidth?....58
4.4.30 Does Advanced Anti-DDoS Implement Load Balancing?....58
4.4.31 Is Advanced Anti-DDoS Software or Hardware?....59
4.5 Fees....59
4.5.1 Is the AAD Service Free of Charge?....59

 Copyright © Huawei Technologies Co., Ltd.

4.5.2 How Is AAD Billed? 59
4.5.3 What Is the Impact on AAD If Your Account Balance Is in Arrears? 61
4.5.4 Why Does My Payment Status Not Update After I Make a Payment? 61
4.5.5 Will I Be Charged If I Buy an Elastic Protection Bandwidth and My Elastic IP Address Is Not Attacked for the Whole Month? 61
4.5.6 What Happens If the Attack Traffic Exceeds the Elastic Protection Bandwidth? 61
4.5.7 Can I Adjust My Elastic Protection Bandwidth From 100 Gbit/s to 200 Gbit/s When I Find 100 Gbit/s Is Insufficient? 61
4.5.8 What Is the Charge If My IP Address Is Attacked Many Times a Day? 62
4.5.9 How Will I Be Charged If I Have Purchased the CTCC & CUCC & CMCC Line and Both My CTCC, CUCC, and CMCC IP Addresses Are Attacked? 62
4.5.10 How Do I Stop Elastic Protection to Avoid Being Charged for the Elastic Protection Bandwidth? 62
4.5.11 How Can I Renew the AAD service? 62
4.5.12 How Can I Unsubscribe from the AAD Service? 63
4.5.13 How Should I Automatically Renew AAD? 63
4.5.14 Will an Expired AAD Instance Incur Fees? 64
4.5.15 What Can I Do When I Receive an Arrears Notification? 65
4.5.16 What Is the Peak Attack Traffic in AAD Pricing? 65
4.5.17 Can the Original Configuration Data Be Saved After I Unsubscribe from an AAD Instance? 65

 Copyright © Huawei Technologies Co., Ltd.

1 General FAQs

1.1 What Are Regions and AZs?

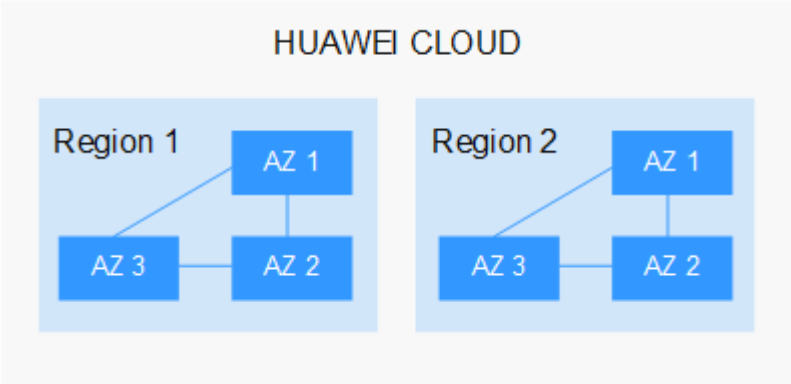
Concepts

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided from the dimensions of geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

Figure 1-1 shows the relationship between the regions and AZs.

Figure 1-1 Region and AZ



 Copyright © Huawei Technologies Co., Ltd.

HUAWEI CLOUD provides services in many regions around the world. You can select a region and AZ as needed.

Selecting a Region

When selecting a region, consider the following factors:

- Location

  You are advised to select a region close to you or your target users. This reduces network latency and improves access rate. However, Chinese mainland regions provide basically the same infrastructure, BGP network quality, as well as operations and configurations on resources. Therefore, if you or your target users are in the Chinese mainland, you do not need to consider the network latency differences when selecting a region.

  - If you or your target users are in the Asia Pacific region, except the Chinese mainland, select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If you or your target users are in Africa, select the **AF-Johannesburg** region.
  - If you or your target users are in Europe, select the **EU-Paris** region.

- Resource price

  Resource prices may vary in different regions. For details, see **Product Pricing Details**.

Selecting an AZ

When determining whether to deploy resources in the same AZ, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs in the same region.
- For low network latency, deploy resources in the same AZ.

Regions and Endpoints

Before using an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

1.2 What Is the Black Hole Policy of HUAWEI CLOUD?

To protect the usability of HUAWEI CLOUD services in general, if a cloud server is subject to a large enough attack, a black hole will be triggered to block all accesses from the Internet for a certain period of time.

What Is a Black Hole?

A black hole refers to a situation where access to a cloud server is blocked by HUAWEI CLOUD because attack traffic targeting a cloud server exceeds a certain threshold.

 Copyright © Huawei Technologies Co., Ltd.

Why Is the Blackhole Policy Required?

DDoS attacks will interrupt user services and cause adverse impacts on the AAD data center. Defense against DDoS attacks is costly on bandwidth consumption.

Bandwidth is purchased by HUAWEI CLOUD from carriers, and those carriers bill for bandwidth even if it was part of DDoS attack. HUAWEI CLOUD provides Cloud Native Anti-DDoS Basic (Anti-DDoS) for free to protect your resources against DDoS attacks below a certain threshold, but if an attack exceeds a certain size, we will route the traffic to a black hole.

How Do I Deactivate a Black Hole?

When the access to a cloud server is blocked by HUAWEI CLOUD because attack traffic targeting a cloud server exceeds a certain threshold, follow the instructions described in **Table 1-1** to handle it.

Table 1-1 Black hole deactivation methods

Anti-DDoS Edition	Deactivation Policy	Deactivation Method
Cloud Native Anti-DDoS Basic (Anti-DDoS) **NOTE** Cloud Native Anti-DDoS Basic (CNAD Basic) is enabled by default.	• The system automatically deactivates the black hole 24 hours after the access to a cloud server is blocked. • If the system detects that the attack has not stopped, and attack traffic is still exceeding the configured threshold, the access will be blocked again.	You need to wait until the system deactivates it automatically.

Copyright © Huawei Technologies Co., Ltd.

Anti-DDoS Edition	Deactivation Policy	Deactivation Method
Cloud Native Anti-DDoS Pro	The system automatically deactivates the black hole 24 hours after the access to a cloud server is blocked.	When an IP address is blocked due to a triggered black hole, you can manually unblock the IP address. • The first time you unblock an IP address in a day must be more than 30 minutes after it has been blocked. **NOTICE** In the same day, the second time you unblock the IP address must be 60 minutes after it has been unblocked for the first time, and the third time you unblock the IP address must be 120 minutes after it has been unblocked. • A maximum of three attempts are allowed for each user to unblock an IP address in a day. • CNAD Pro automatically adjusts the allowed IP unblocking attempts and the interval based on risk control.
Advanced Anti-DDoS	The system automatically deactivates the black hole 30 minutes, by default, after the black hole has been triggered. The duration of persistent black hole depends on the times of the black hole triggered and amount of peak attack traffic of the day, and it can be a maximum of 24 hours. If you need to unblock access before a black hole becomes ineffective, contact Huawei technical support.	You can upgrade the elastic protection bandwidth to deactivate the black hole.

 Copyright © Huawei Technologies Co., Ltd.

How Can I Increase the Black Hole Threshold?

You can increase the black hole threshold using the following methods:

- Enable Cloud Native Anti-DDoS Pro (CNAD Pro) to obtain the unlimited protection capability without changing the service IP address.
- Connect your services to AAD to obtain the Tbit/s protection capability. The malicious attacks targeting the origin servers can be diverted to the high-defense IP address for scrubbing to ensure the stable running of mission-critical workloads.

1.3 What are the Relationships Between DDoS Mitigation and the Anti-DDoS, CNAD Pro, and AAD Services?

Anti-DDoS is free while CNAD Pro and AAD are paid services that you need to purchase.

1.4 What Are the Differences Between Anti-DDoS and Advanced Anti-DDoS?

Anti-DDoS defends against most common DDoS attacks at no additional charge, whereas Advanced Anti-DDoS (AAD) provides expanded protection and expert support with subscription fees. For details, see **Table 1-2**.

Table 1-2 Differences between Anti-DDoS and Advanced Anti-DDoS

Item	Anti-DDoS	Advanced Anti-DDoS
Cost	Free	Charged
Protection capability	Provides a 2 Gbit/s DDoS mitigation capability, and its maximum mitigation capability can reach 5 Gbit/s.	A maximum of 1 Tbit/s protection capacity
Protected objects	HUAWEI CLOUD resources only	HUAWEI CLOUD, non-HUAWEI CLOUD, and on-premises resources
Protection policy	• Fixed protection policies • Basic CC attack defense • Globally applied policies	• Diverse protection policies • Professional CC attack defense • Customized policies
Key event assurance	None	Expert support (for VIP customers)

Copyright © Huawei Technologies Co., Ltd.

Item	Anti-DDoS	Advanced Anti-DDoS
Detailed reports	Provides an overview report.	Provides a detailed report.
Technical support	24/7 online customer service	24/7 expert support service

1.5 What Are a SYN Flood Attack and an ACK Flood Attack?

A SYN flood attack is a typical denial of service (DoS) attack. Utilizing the loop hole in the Transmission Control Protocol (TCP), the attacker sends a huge number of forged TCP connection requests to the target to exhaust its resources (fully loaded CPU or insufficient memory). Consequently, the target fails to respond to normal connection requests.

An ACK flood attack works in a similar mechanism as a SYN flood attack.

An ACK flood attack is when an attacker attempts to overload a server with TCP ACK packets. Like other DDoS attacks, the goal of an ACK flood is to deny service to other users by slowing down or crashing the target using junk data. The targeted server has to process each ACK packet received, which uses so much computing power that it is unable to serve legitimate users.

1.6 What Is a CC Attack?

In a challenge collapsar (CC) attack, the attacker uses a proxy server to generate and send disguised requests to the target host. In addition, the attacker controls other hosts in the Internet and makes them send large numbers of data packets to the target server to exhaust its resources. In the end, the target server stops responding to requests. As you know, when many users access a web page, the page opens slowly. So in a CC attack, the attacker simulates a scenario where a large number of users (a thread represents a user) are accessing pages all the time. Because the accessed pages all require a lot of data operations (consuming many CPU resources), the CPU usage is kept at the 100% level for a long time until normal access requests are blocked.

You can use the CC defense function to control the HTTP request rate.

1.7 What Is a Slow HTTP Attack?

Slow HTTP attacks are a variation of CC attacks. Here is how slow HTTP attacks work:

The attacker establishes a connection to the target server which allows HTTP access. Then the attacker specifies a large content length and sends packets in an extremely low rate, such as one byte per one to ten seconds. The connection is maintained this way. If the attacker keeps establishing such connections, available

 Copyright © Huawei Technologies Co., Ltd.

connections on the target server are slowly consumed and the server will stop responding to valid requests.

1.8 What Are a UDP Attack and a TCP Attack?

Exploiting the interaction characteristics of UDP and TCP, attackers use botnets to send large numbers of various TCP connection packets or UDP packets to exhaust the bandwidth resources of target servers. As a result, the servers become slow in processing capability and fail to work properly.

1.9 What Are the Differences Between DDoS Attacks and Challenge Collapsar Attacks?

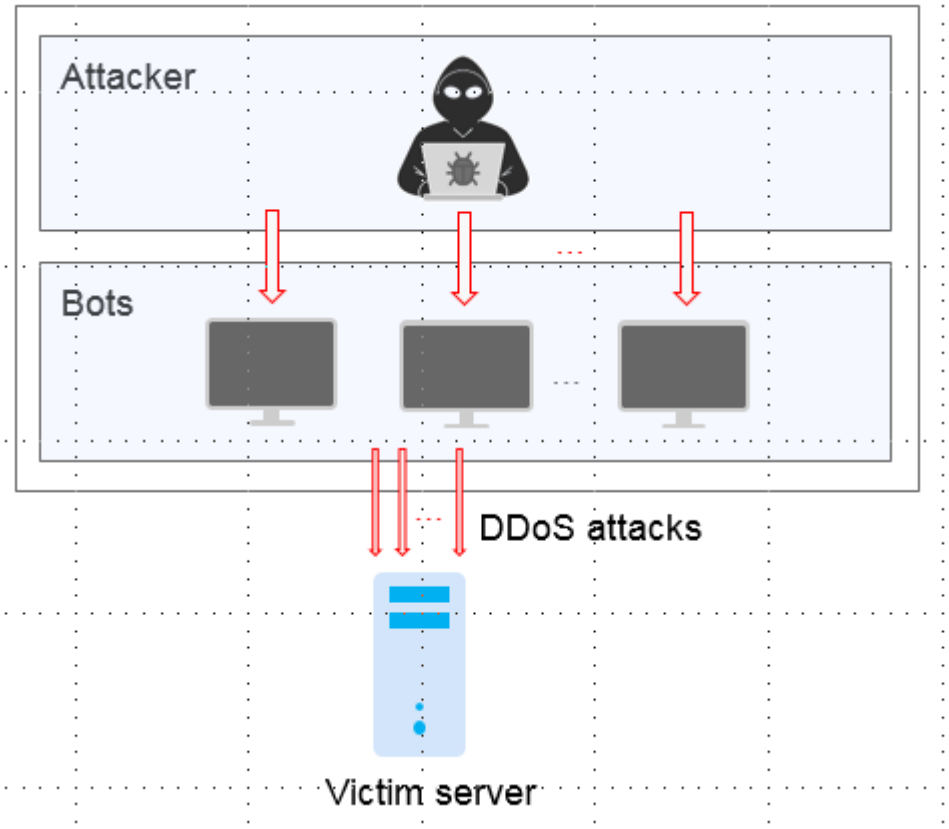
Challenge Collapsar (CC) attack is a type of Distributed Denial of Service (DDoS) attack.

DDoS Attack

DDoS attacks are distributed and coordinated large-scale DoS attacks. Multiple attackers in different locations launch attacks to one or more targets at the same time, or an attacker controls multiple compromised computers in different locations and uses these computers to attack the victim at the same time. The DDoS attack process consists of target confirmation, botnet establishment, attack launching.

 Copyright © Huawei Technologies Co., Ltd.

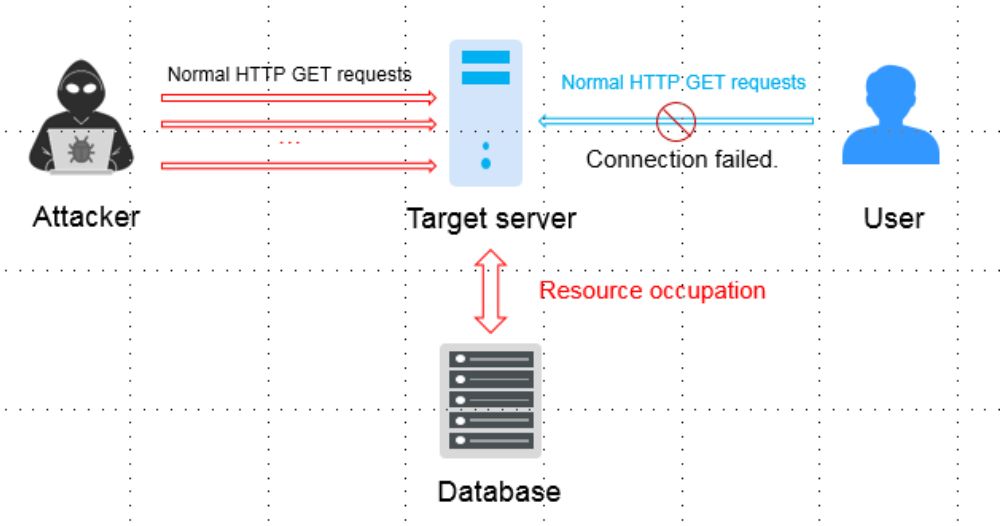
Figure 1-2 DDoS attack



CC Attack

A Challenge Collapsar (CC) attack is an attack that standard HTTP requests are sent to a targeted web server frequently. The attacker controls some servers to keep sending a large number of data packets to the target server, causing resource exhaustion and breakdown of the server.

Figure 1-3 CC attack



 Copyright © Huawei Technologies Co., Ltd.

1.10 What Is the Maximum Protection Capacity Provided by HUAWEI CLOUD Anti-DDoS for Free?

HUAWEI CLOUD Anti-DDoS provides a 2 Gbit/s DDoS mitigation capacity for free, and its maximum mitigation capacity can reach 5 Gbit/s.

1.11 What Can I Do If an IP Address Is Blocked?

Possible Causes

Anti-DDoS provides a 2 Gbit/s DDoS mitigation capacity for free, and its maximum mitigation capacity can reach 5 Gbit/s (depending on the available bandwidth of HUAWEI CLOUD). HUAWEI CLOUD Anti-DDoS will trigger a black hole to block access from the Internet within a time period when detecting an ECS is under volumetric flood attacks.

Solution

For details about how to deactivate a black hole, see **Table 1-3**.

Table 1-3 Black hole deactivation methods

Anti-DDoS Edition	Deactivation Policy	Deactivation Method
Cloud Native Anti-DDoS Basic (Anti-DDoS) **NOTE** Cloud Native Anti-DDoS Basic (CNAD Basic) is enabled by default.	• The system automatically deactivates the black hole 24 hours after the access to a cloud server is blocked. • If the system detects that the attack has not stopped, and attack traffic is still exceeding the configured threshold, the access will be blocked again.	You need to wait until the system deactivates it automatically.

Copyright © Huawei Technologies Co., Ltd.

Anti-DDoS Edition	Deactivation Policy	Deactivation Method
Cloud Native Anti-DDoS Pro	The system automatically deactivates the black hole 24 hours after the access to a cloud server is blocked.	When an IP address is blocked due to a triggered black hole, you can manually unblock the IP address. • The first time you unblock an IP address in a day must be more than 30 minutes after it has been blocked. **NOTICE** In the same day, the second time you unblock the IP address must be 60 minutes after it has been unblocked for the first time, and the third time you unblock the IP address must be 120 minutes after it has been unblocked. • A maximum of three attempts are allowed for each user to unblock an IP address in a day. • CNAD Pro automatically adjusts the allowed IP unblocking attempts and the interval based on risk control.
Advanced Anti-DDoS	The system automatically deactivates the black hole 30 minutes, by default, after the black hole has been triggered. The duration of persistent black hole depends on the times of the black hole triggered and amount of peak attack traffic of the day, and it can be a maximum of 24 hours. If you need to unblock access before a black hole becomes ineffective, contact Huawei technical support.	You can upgrade the elastic protection bandwidth to deactivate the black hole.

 Copyright © Huawei Technologies Co., Ltd.

2 CNAD Basic (Anti-DDoS) FAQs

2.1 About Anti-DDoS

2.1.1 What Is the Million-level IP Address Blacklist Database?

The million-level IP address blacklist database refers to the database of millions of malicious IP addresses collected by experts in the past years. When users' services are attacked by these IP addresses, Anti-DDoS responds to those attacks first to defend your servers in a timely manner.

2.1.2 How Will Anti-DDoS Be Triggered to Scrub Traffic?

Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the traffic cleaning threshold.

- When the service traffic reaches this threshold, Anti-DDoS intercepts only attack traffic.
- If the service traffic does not reach the threshold, Anti-DDoS will not intercept the traffic, regardless of whether it is attack traffic.

You can adjust the traffic cleaning threshold based on the actual service bandwidth. For details, see section "Configuring an Anti-DDoS Protection Policy".

2.1.3 Does Anti-DDoS Traffic Cleaning Affect Normal Services?

Anti-DDoS traffic cleaning exerts no adverse impacts on normal traffic.

If you are worried that normal traffic may be discarded mistakenly, you can set the traffic cleaning threshold to 1000 Mbit/s, a value so large that your EIPs get almost no protection from Anti-DDoS.

2.1.4 How Does Anti-DDoS Scrub Traffic?

Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the traffic cleaning threshold.

You can view an interception report on protection statistics, including the traffic cleaning frequency, cleaned traffic amount, weekly top 10 attacked public IP

 Copyright © Huawei Technologies Co., Ltd.

addresses, and total number of intercepted attacks of all public IP addresses of a user.

2.1.5 What Are the Restrictions of Anti-DDoS?

Anti-DDoS provides a 2 Gbit/s DDoS mitigation capacity for free, and its maximum mitigation capacity can reach 5 Gbit/s.

Traffic that exceeds 5 Gbit/s from the attacked public IP address will be routed to the black hole and the legitimate traffic will be discarded. Therefore if you may suffer from volumetric attacks exceeding 5 Gbit/s, it is a better choice to purchase HUAWEI CLOUD Advanced Anti-DDoS (AAD) for enhanced protection.

2.1.6 What Is the Protection Capacity of Anti-DDoS?

Anti-DDoS provides a 2 Gbit/s DDoS mitigation capacity for free, and its maximum mitigation capacity can reach 5 Gbit/s (depending on the available bandwidth of HUAWEI CLOUD). For applications threatened by attack traffic larger than 5 Gbit/s, it is a better choice to purchase the Advanced Anti-DDoS service on HUAWEI CLOUD to expand protection capacity.

2.1.7 What Data Can Be Provided by Anti-DDoS?

- You can **view the monitoring report** of a public IP address, including the current protection status, protection settings, and the traffic and anomalies within the last 24 hours.
- You can **view the interception report** on protection statistics, including the traffic cleaning frequency, cleaned traffic amount, weekly top 10 attacked ECSs, load balancers, or BMSs, and total number of intercepted attacks of all public IP addresses of a user.
- You can **enable alarm notification** for Anti-DDoS so that you can receive notifications in a timely manner if a public IP address is attacked. If you do not enable this function, you have to log in to the management console to view alarms.

2.1.8 Which Regions Does Anti-DDoS Support?

Currently, Anti-DDoS only provides protection for services deployed on HUAWEI CLOUD.

HUAWEI CLOUD supports the following regions: CN North-Beijing1, CN North-Beijing3, CN North-Beijing4, CN North-Beijing2, CN North-Ulanqab201, CN North-Ulanqab2, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, and CN Southwest-Guiyang1.

2.1.9 Which Services Can Use Anti-DDoS?

Anti-DDoS provides the traffic cleaning function for public IP addresses purchased by users.

2.1.10 Can Anti-DDoS Be Used Across Clouds?

Anti-DDoS currently supports protection only for services deployed on HUAWEI CLOUD.

Copyright © Huawei Technologies Co., Ltd.

2.1.11 How to Determine Whether an Attack Occurs?

- You can log in to the HUAWEI CLOUD console to **view the monitoring report** of a public IP address, including the current protection status, protection settings, and the traffic and anomalies within the last 24 hours.
- You can log in to the HUAWEI CLOUD console to **view an interception report** on protection statistics, including the traffic cleaning frequency, cleaned traffic amount, weekly top 10 attacked ECSs, load balancers, or BMSs, and total number of intercepted attacks of all public IP addresses of a user.

2.2 About Basic Functions

2.2.1 What Is the HTTP Request Threshold Set for Anti-DDoS Protection?

The HTTP request threshold refers to the number of HTTP requests that can be processed by the deployed service per second on average. It is calculated based on the total number of requests. Anti-DDoS will automatically scrub traffic if detecting that the total number of requests exceeds the configured HTTP request threshold.

2.2.2 What Would Happen When I Am Under a DDoS Attack Exceeding 5 Gbit/s?

Anti-DDoS provides a 2 Gbit/s DDoS mitigation capacity for free, and its maximum mitigation capacity can reach 5 Gbit/s (depending on the available bandwidth of HUAWEI CLOUD). The attacked public IP address will be routed to a black hole when the attack traffic exceeds 5 Gbit/s, and the normal access traffic will be discarded. It is a better choice to purchase HUAWEI CLOUD Advanced Anti-DDoS for enhanced protection.

2.2.3 Which Types of Attacks Does Anti-DDoS Mitigate?

Anti-DDoS helps users mitigate the following attacks:

- Web server attacks

  Include SYN flood, HTTP flood, Challenge Collapsar (CC), and low-rate attacks
- Game attacks

  Include UDP flood, SYN flood, TCP-based, and fragmentation attacks
- HTTPS server attacks

  Include SSL DoS and DDoS attacks
- DNS server attacks

  Include attacks exploiting DNS protocol stack vulnerabilities, DNS reflection attacks, DNS flood attacks, and DNS cache miss attacks

2.2.4 What Should I Do If My Service Is Frequently Attacked?

When your services are frequently under DDoS attacks, the public IP address is prone to be routed to a black hole, damaging service continuity. Therefore, it is

 Copyright © Huawei Technologies Co., Ltd.

recommended that you purchase Advanced Anti-DDoS to expand protection capability.

2.2.5 What Is the Difference Between ELB Protection and ECS Protection?

An EIP can be bound to a load balancer or ECS. Anti-DDoS protects EIP against DDoS attacks. There is no difference between ELB and ECS protection.

2.2.6 Why Is the Number of Times of Cleaning Different from the Number of Attacks for the Same Public IP Address?

Cleaning is triggered automatically when an attack is detected on a public IP address. The cleaning lasts for a while. (Only attack traffic is cleaned, and users' services will not be affected.) If, during the cleaning, another attack is detected on the same public IP address, the attack will be cleaned together with the previous attack. Consequently, the number of attacks increases by one while the number of times of cleaning does not.

2.2.7 Is Anti-DDoS Enabled by Default?

Yes. It is enabled by default and uses the default protection policy. To modify this setting, see section "Configuring an Anti-DDoS Protection Policy".

NOTE

Once enabled, Anti-DDoS cannot be disabled. To temporarily disable Anti-DDoS, see **How Do I Temporarily Disable Anti-DDoS?**

2.2.8 Does Anti-DDoS Protect a Region or a Single IP Address?

A single IP address.

2.2.9 How Do I Temporarily Disable Anti-DDoS?

You can set the traffic cleaning threshold to 1000 Mbit/s, a value so large that your EIP gets almost no protection from DDoS attacks.

NOTE

This value is suitable for temporary disabling of protection for commissioning or other special purposes. You are advised not to use it for a long time.

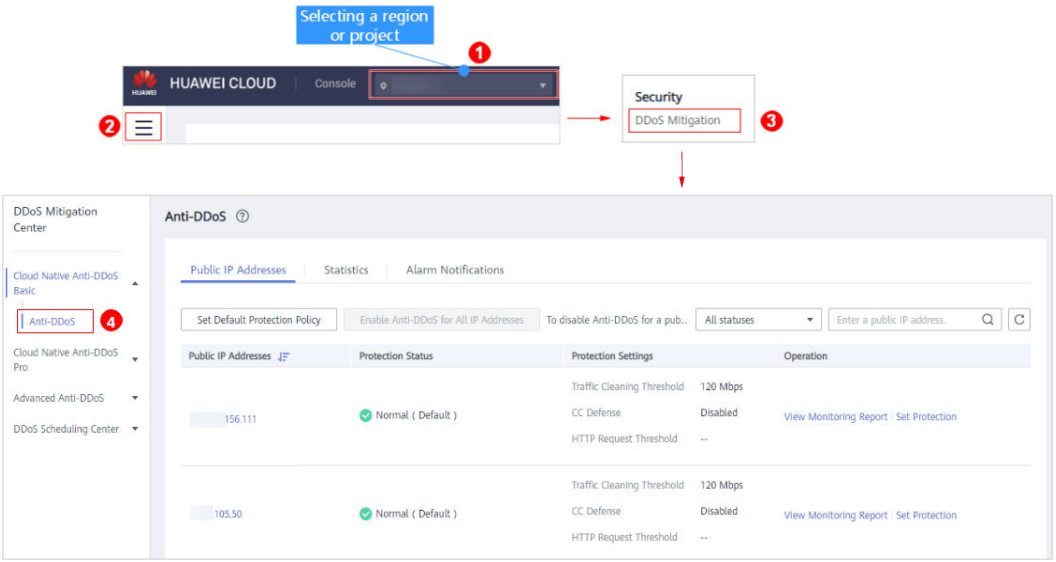
Procedure

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

Step 2 Go to the Anti-DDoS console.

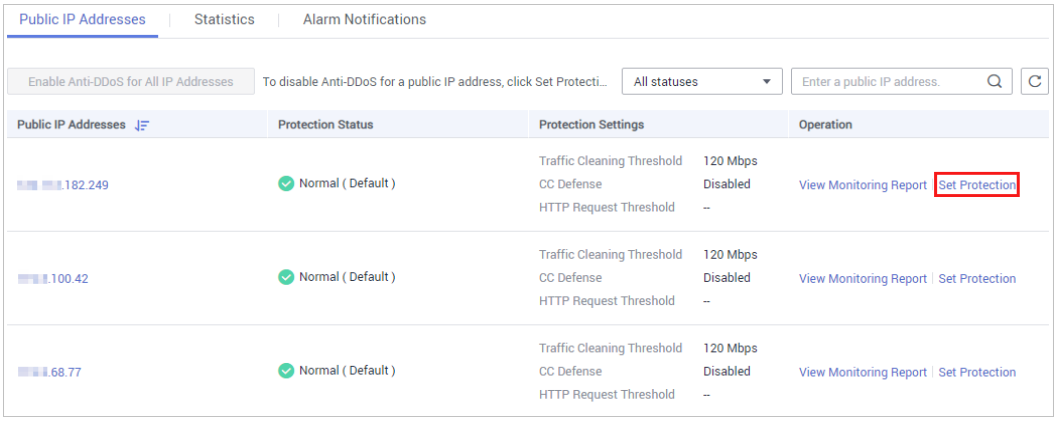
 Copyright © Huawei Technologies Co., Ltd.

Figure 2-1 Anti-DDoS console



Step 3 Click the **Public IP Addresses** tab, locate the row that contains the IP address for which you want to set protection, and click **Set Protection** in the **Operation** column.

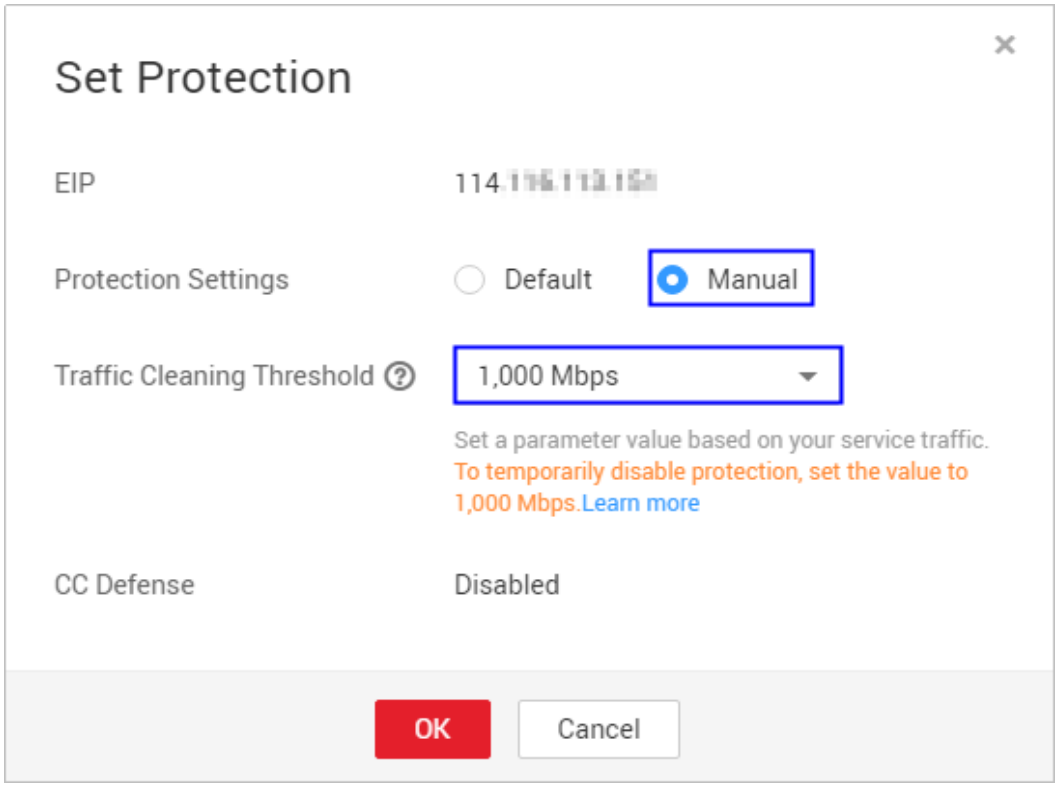
Figure 2-2 Protection settings



Step 4 In the dialog box that is displayed, set **Protection Settings** to **Manual** and **Traffic Cleaning Threshold** to **1,000 Mbps**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-3 Protection settings



Step 5 Click **OK**.

----End

2.2.10 Do I Need to Clear the Resources of Anti-DDoS When I Delete an Account?

No. Anti-DDoS is free of charge.

- Anti-DDoS does not consume your resources.
- Anti-DDoS is enabled by default at no additional charge. Therefore you do not need to clear the resources when deleting the account.
- Anti-DDoS is automatically enabled when you purchase a public IP address without incurring any fee.

2.2.11 How Do I View the Traffic Cleaning Frequency?

You can **view an interception report** on protection statistics, including the traffic cleaning frequency, cleaned traffic amount, weekly top 10 attacked public IP addresses, and total number of intercepted attacks of all public IP addresses of a user.

2.2.12 How Can I View Anti-DDoS Protection Statistics?

You can **view an interception report** on protection statistics, including the traffic cleaning frequency, cleaned traffic amount, weekly top 10 attacked public IP addresses, and total number of intercepted attacks of all public IP addresses of a user.

Copyright © Huawei Technologies Co., Ltd.

2.2.13 How Can I View Public IP Address Monitoring Data in Anti-DDoS?

You can **view the monitoring report** of a public IP address, including the current protection status, protection settings, and the traffic and anomalies within the last 24 hours.

2.2.14 How Can I View the Change History of Anti-DDoS?

You can use the Cloud Trace Service (CTS) to view operations performed on Anti-DDoS, including enabling and disabling Anti-DDoS protection and adjusting Anti-DDoS security settings. For details, see **Viewing CTS Traces**.

2.2.15 How Can I View an Interception Report?

You can **view an interception report** on protection statistics, including the traffic cleaning frequency, cleaned traffic amount, weekly top 10 attacked public IP addresses, and total number of intercepted attacks of all public IP addresses of a user.

2.2.16 How Do I Select an AZ in Anti-DDoS?

Anti-DDoS has no requirement on AZs.

2.2.17 Can I Disable Anti-DDoS Completely?

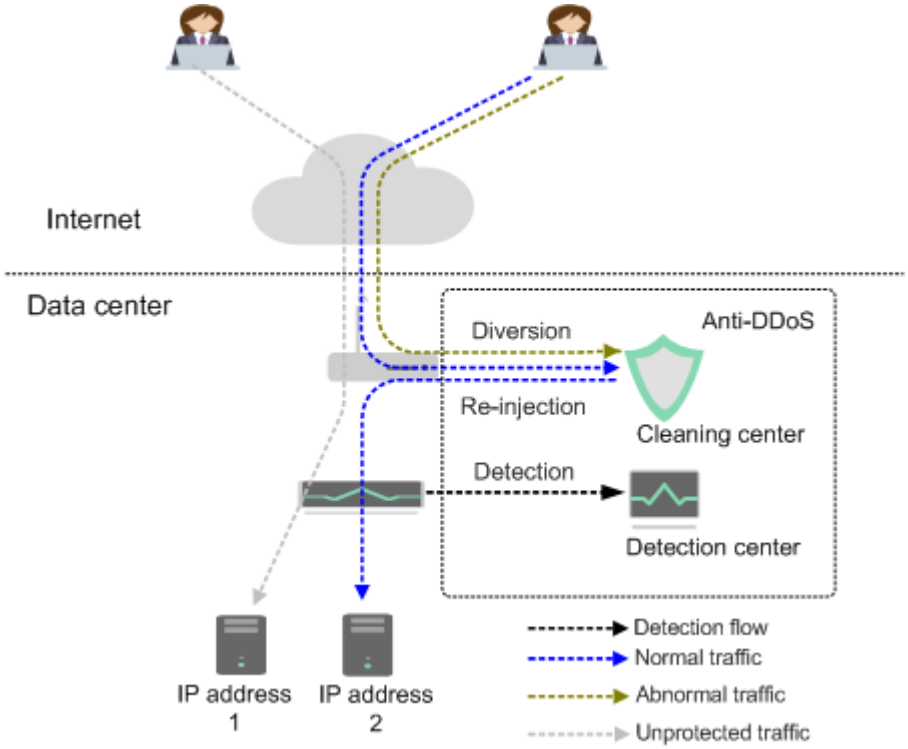
No.

2.2.18 How Do I Check Whether the Inbound Traffics Are Routed Through Anti-DDoS Devices?

Anti-DDoS provides anti-DDoS only for HUAWEI CLOUD EIPs. Anti-DDoS devices are deployed at the egresses of data centers.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-4 Network topology



Anti-DDoS only enables protection for inbound traffics from external network.

- If you access the EIP from an external network, the inbound traffics are routed through the public network routes. You can check whether the traffics are forwarded from the public network routes on the VM bound to the EIP. If yes, the access traffics are routed through Anti-DDoS devices.

  If inbound traffics are routed through Anti-DDoS devices, the following information is displayed when the EIP is threatened by DDoS attacks:

  – Traffic cleaning records exist on the Anti-DDoS console.
  – An alarm notification is sent by SMS or Email.
- If you access the EIP from the intranet, the inbound traffics are not routed through public network routes. As a result, the traffics are not routed through Anti-DDoS devices.

  For example, if you apply for two EIPs in two different regions of HUAWEI CLOUD, the access traffics between the two EIPs will not be routed through Anti-DDoS.

2.3 About Threshold and Black Hole

2.3.1 How Does the Traffic Cleaning Threshold Take Effect in Anti-DDoS?

Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the traffic cleaning threshold. It will discard attack traffic and permit normal service traffic.

 Copyright © Huawei Technologies Co., Ltd.

The default cleaning threshold of Anti-DDoS is 120 Mbit/s. You can adjust the threshold based on the actual service bandwidth. For details, see **Configuring an Anti-DDoS Protection Policy**.

2.3.2 How Do I Set the Anti-DDoS Traffic Cleaning Threshold?

After you purchase a public IP address, Anti-DDoS automatically enables protection. The default traffic cleaning threshold is **120 Mbps**.

The default cleaning threshold of Anti-DDoS is 120 Mbit/s. You can adjust the threshold based on the actual service bandwidth. For details, see **Configuring an Anti-DDoS Protection Policy**.

- The cleaning threshold for each attack type is automatically generated based on your settings and the service traffic.
- When the service traffic hits the traffic cleaning threshold, Anti-DDoS automatically scrubs attack traffic instead of blocking the service.

2.3.3 How Can I Adjust the Block Threshold?

Anti-DDoS provides a 2 Gbit/s DDoS mitigation capacity for free, and its maximum mitigation capacity can reach 5 Gbit/s (depending on the available bandwidth of HUAWEI CLOUD). Traffic that exceeds 5 Gbit/s will be routed to a black hole. For applications threatened by attack traffic larger than 5 Gbit/s, it is a better choice to purchase the Advanced Anti-DDoS service on HUAWEI CLOUD to expand protection capacity.

2.3.4 Do I Need to Manually Enable the Free-of-Charge 5 Gbit/s DDoS Protection Provided by Anti-DDoS?

CNAD Basic (Anti-DDoS) provides a 2 Gbit/s DDoS mitigation capability for free, and its maximum mitigation capability can reach 5 Gbit/s. It is enabled automatically by default for your purchased public IP address. For applications threatened by attack traffic larger than 5 Gbit/s, it is a better choice to purchase the Advanced Anti-DDoS service on HUAWEI CLOUD to expand protection capacity.

2.4 About Alarm notification

2.4.1 Will I Be Promptly Notified When an Attack Is Detected?

Yes, if you enable alarm notification.

On the console, click the **Alarm Notifications** tab to enable the alarm notification function, which enables you to receive alarms (by SMS or email) if a DDoS attack is detected. For details, see section "Enabling Alarm Notification".

2.4.2 What Should I Do If I Receive an Alarm Notification?

It is normal if you receive an alarm notification. After the alarm notification function is enabled for your Anti-DDoS service, you will receive SMS messages or emails when the public IP address is under DDoS attacks.

 Copyright © Huawei Technologies Co., Ltd.

You can log in to the management console to view the protection status of of an EIP. If you do not want the traffic to be scrubbed, increase the traffic cleaning threshold. For details, see section "Configuring an Anti-DDoS Protection Policy".

2.4.3 How Do I Disable the Alarm Notification?

The alarm notification of Anti-DDoS is sent by the Simple Message Notification (SMN) service.

If you do not need to receive alarm notifications from SMN, you can disable or modify the alarm notification settings on the Anti-DDoS console.

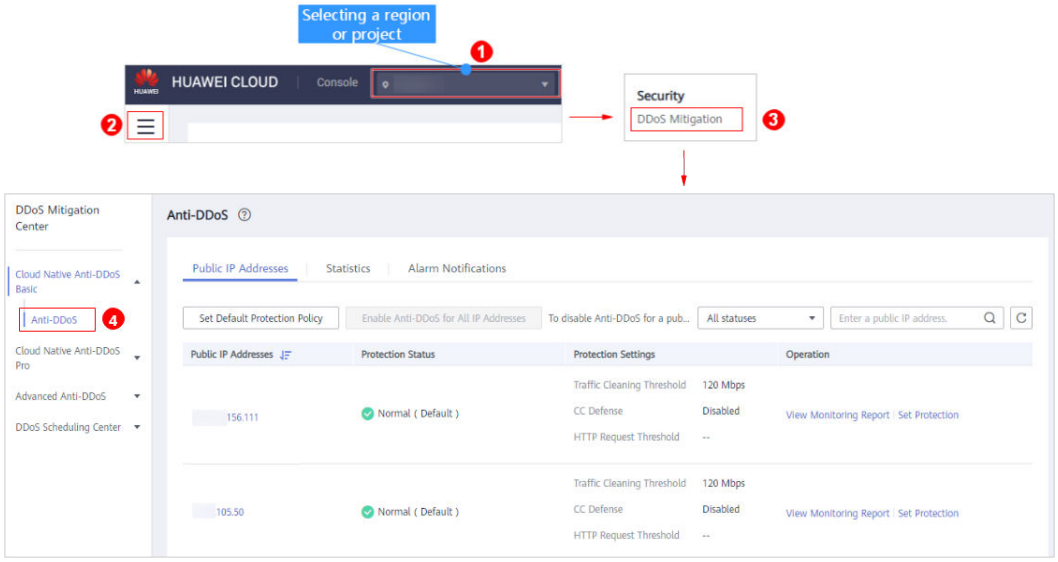
Disabling Alarm Notifications

If you do not need to receive alarm notifications, you can disable the alarm notification function on the **Alarm Notifications** tab page of the Anti-DDoS console. After alarm notification is disabled, you will not receive alarm information.

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

Step 2 Go to the Anti-DDoS console.

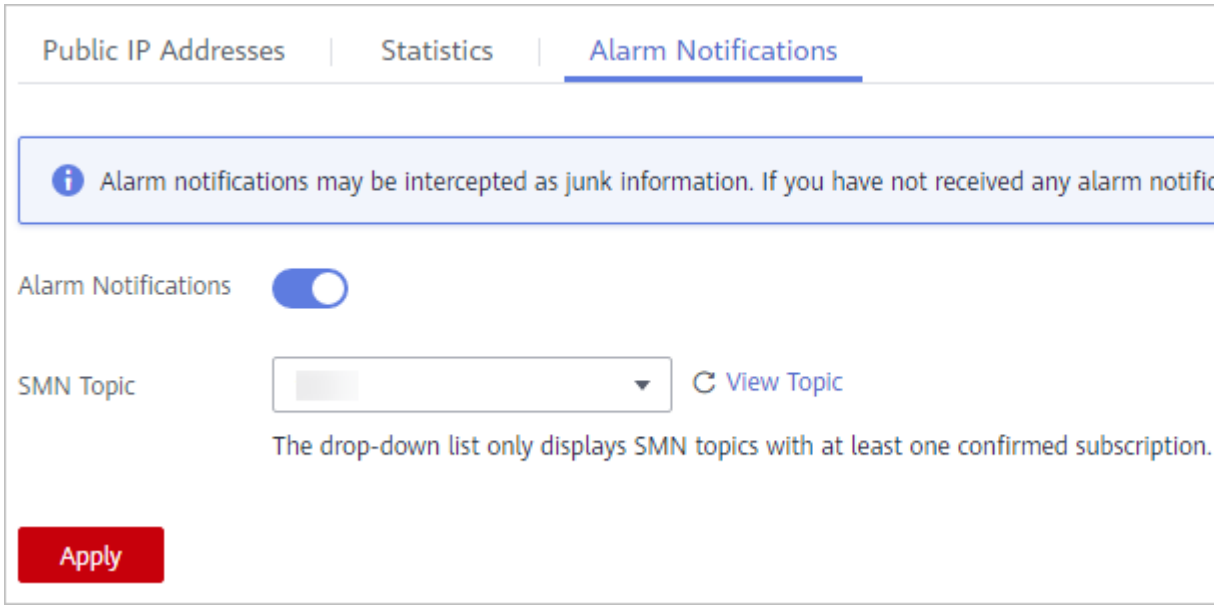
Figure 2-5 Anti-DDoS console



Step 3 Click the **Alarm Notifications** tab and click  to disable the alarm notification function.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-6 Configuring alarm notifications



----End

Deleting the Subscription

If the subscription endpoint (mobile number or email address) that receives alarm notifications changes, you need to delete the subscription. For example, you need to delete an alarm notification recipient if the recipient resigns.

The alarm notification topic is **antiddos-warning** and the subscription endpoint is **test@example.com**.

Prerequisites

You have obtained the SMN administrator permission.

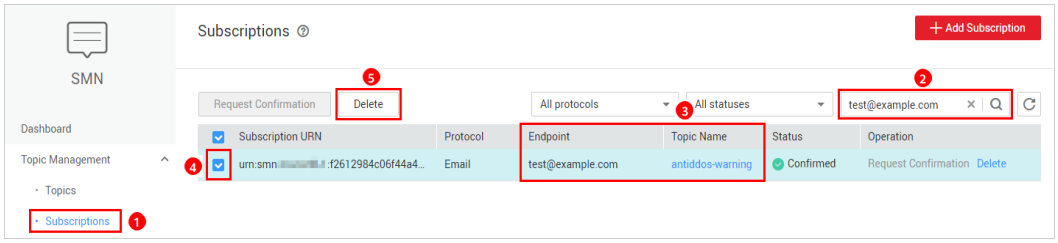
Procedure

Step 1 Log in to the management console.

Step 2 In the upper left corner, click ☰ and choose **Application** > **Simple Message Notification**.

Step 3 On the displayed page, choose **Topic Management** > **Subscriptions** in the navigation pane on the left. Enter the endpoint (mobile number or email address) in the search box.

Figure 2-7 Searching for the target subscription endpoint



 Copyright © Huawei Technologies Co., Ltd.

Step 4 Check whether the subscription endpoint receives the alarm notifications sent from SMN for Anti-DDoS.

Step 5 Click **Delete** in the **Operation** column.

NOTE

After a subscription is deleted, the endpoint no longer receives alarm notifications for Anti-DDoS. Exercise caution when performing this operation.

----End

Follow-up Operations

Add a Subscription

After you delete the subscription for the resigned recipient from SMN, you can add a subscription for the succeeding personnel. For details about how to add a subscription, see **Adding a Subscription** and **Requesting Subscription Confirmation**.

2.5 About Service Faults

2.5.1 Why Is the Traffic Volume of a Public IP Address is Low?

Troubleshooting:

1. Anti-DDoS provides a 2 Gbit/s DDoS mitigation capacity for free, and its maximum mitigation capacity can reach 5 Gbit/s (depending on the available bandwidth of HUAWEI CLOUD). Traffic that exceeds 5 Gbit/s will be routed to a black hole. For applications threatened by attack traffic larger than 5 Gbit/s, it is a better choice to purchase the Advanced Anti-DDoS service on HUAWEI CLOUD to expand protection capacity.
2. Check the HTTP request threshold. If the actual HTTP request threshold is greater than or equal to the configured value, Anti-DDoS triggers CC defense to analyze and check each request, which affects responses to normal requests.

If the fault persists, contact HUAWEI CLOUD security technical experts.

2.5.2 Why Is the Access from the Internet Abnormal?

HUAWEI CLOUD Anti-DDoS will trigger a black hole to block access from the Internet within a time period when detecting an ECS is under volumetric flood attacks.

Anti-DDoS provides a 2 Gbit/s DDoS mitigation capacity for free, and its maximum mitigation capacity can reach 5 Gbit/s (depending on the available bandwidth of HUAWEI CLOUD). Traffic that exceeds 5 Gbit/s will be routed to a black hole. For applications threatened by attack traffic larger than 5 Gbit/s, it is a better choice to purchase the Advanced Anti-DDoS service on HUAWEI CLOUD to expand protection capacity.

 Copyright © Huawei Technologies Co., Ltd.

2.5.3 Traffic Scrubbed Unexpectedly Without Traffic Fluctuations Reported

Troubleshooting:

1. Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the traffic cleaning threshold. If you do not want the traffic to be scrubbed, increase the traffic cleaning threshold. For details, see section "Configuring an Anti-DDoS Protection Policy".
2. After the alarm notification function is enabled for your Anti-DDoS service, you will receive SMS messages or emails when the public IP address is under DDoS attacks. It is normal if you receive an alarm notification.

2.5.4 What Should I Do If Access to a Client Is Denied Due to DDoS Attacks?

You can use the view the anomalies of a single public IP address within the last 24 hours in the monitoring report, or view the protection statistics of all public IP addresses, such as the Top 10 attacked public IP addresses in the interception report, to determine whether the access to a client is blocked due to the black hole triggered when your services are under DDoS attacks.

The system automatically deactivates the black hole 24 hours after the access to a cloud server was blocked due to the triggered black hole.

2.5.5 How Do I Query the Protection Information About a Public IP Address That Is Under DDoS Attacks?

You can view the monitoring report of a public IP address, including the current protection status, protection settings, and the traffic and anomalies within the last 24 hours.

2.5.6 Is Traffic Cleaning Triggered Even If No Attack Occurs?

Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the traffic cleaning threshold. If you do not want the traffic to be scrubbed, increase the traffic cleaning threshold. For details, see section "Configuring an Anti-DDoS Protection Policy".

 Copyright © Huawei Technologies Co., Ltd.

3 Product

3.1 What Is Unlimited Protection?

HUAWEI CLOUD provides as high DDoS mitigation capability as possible based on the network and resource capabilities in the current region. The protection capability provided grows with the improvement of HUAWEI CLOUD's network capabilities.

3.2 Can CNAD Pro Protect Non-HUAWEI CLOUD and On-Premises IP Addresses?

CNAD Pro provides DDoS protection capability only for cloud services on HUAWEI CLOUD such as ECS, ELB, WAF, and EIP. To protect your non-HUAWEI CLOUD and on-premises resources, purchase AAD.

 Copyright © Huawei Technologies Co., Ltd.

4 AAD FAQs

4.1 Function Specifications

4.1.1 What Forwarding Protocols Does AAD Support?

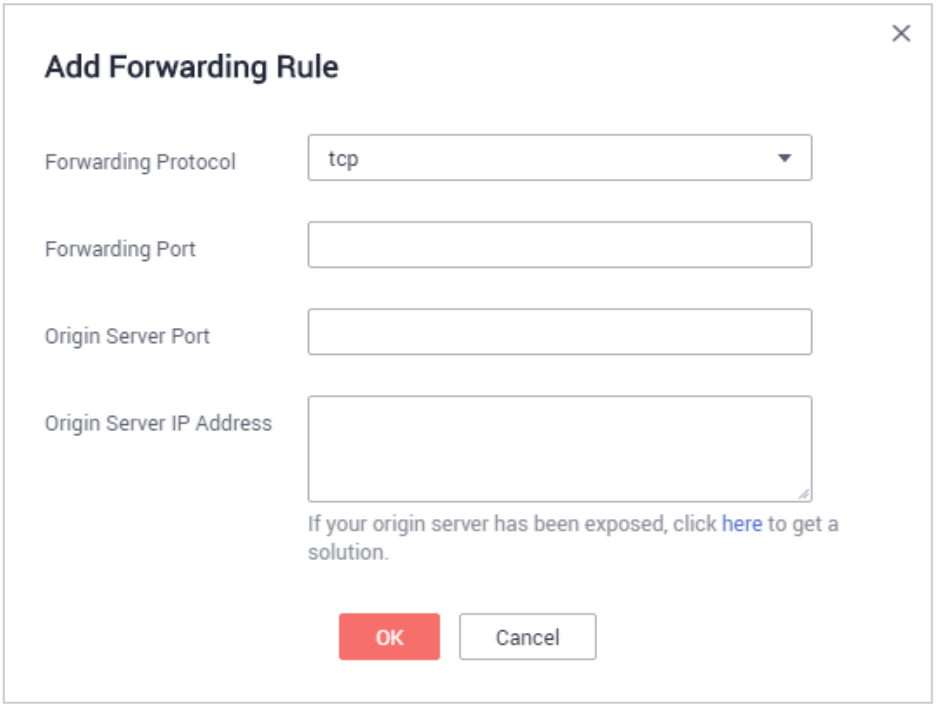
HUAWEI CLOUD supports layer 4 protocols (TCP and UDP) and layer 7 protocols (HTTP/WebSocket and HTTPS/WebSockets).

How to Configure TCP and UDP Forwarding Protocols?

In the navigation pane on the left of the **Security Console**, choose **Advanced Anti-DDoS** > **Forwarding Configuration**. On the **Forwarding Configuration** page, click **Add** to add a TCP or UDP forwarding rule.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-1 Adding a forwarding rule



How to Configure HTTP/WebSocket and HTTPS/WebSockets Forwarding Protocols?

In the navigation pane on the left of the **Security Console**, choose **Advanced Anti-DDoS** > **Domain Name Access**. On the **Domain Name Access** page, click **Add Domain Name** to configure an HTTP/WebSocket or HTTPS/WebSockets forwarding protocol.

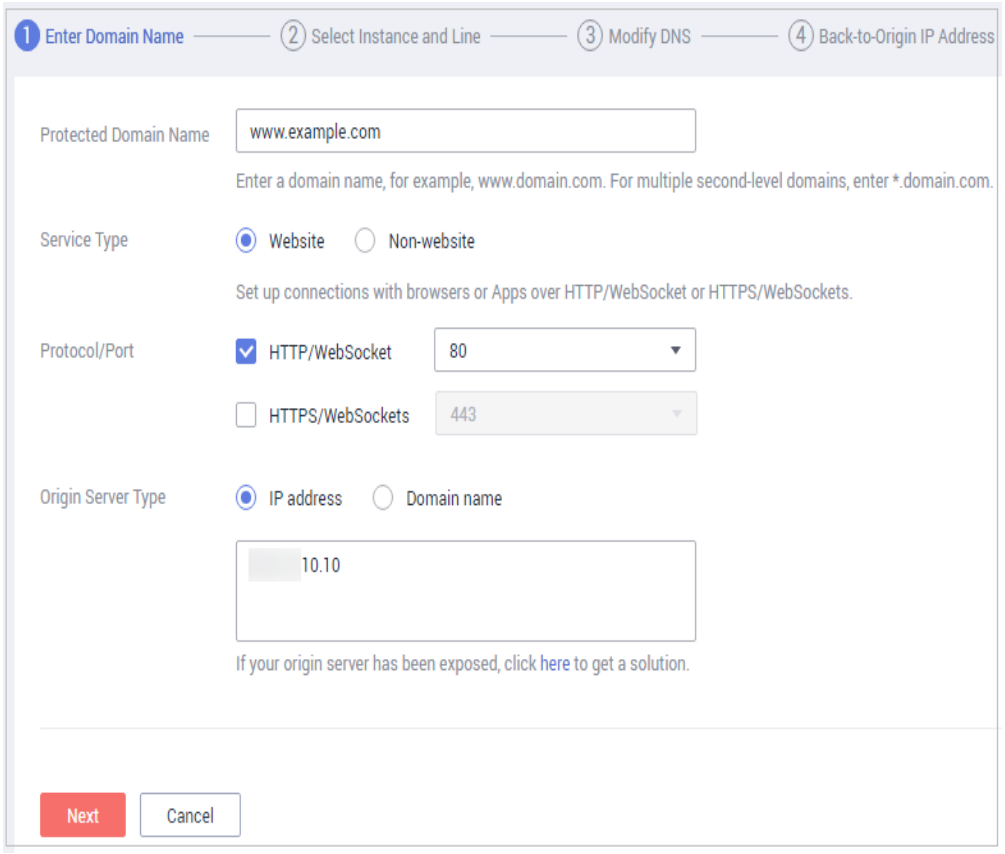
- **For an HTTP/WebSocket protocol:**

  Set **Service Type** to **Website** and **Protocol/Port** to **HTTP/WebSocket**.

  Available HTTP/WebSocket ports are **80**, **81**, **82**, **83**, **84**, **8080**, and **8081**.

 Copyright © Huawei Technologies Co., Ltd.

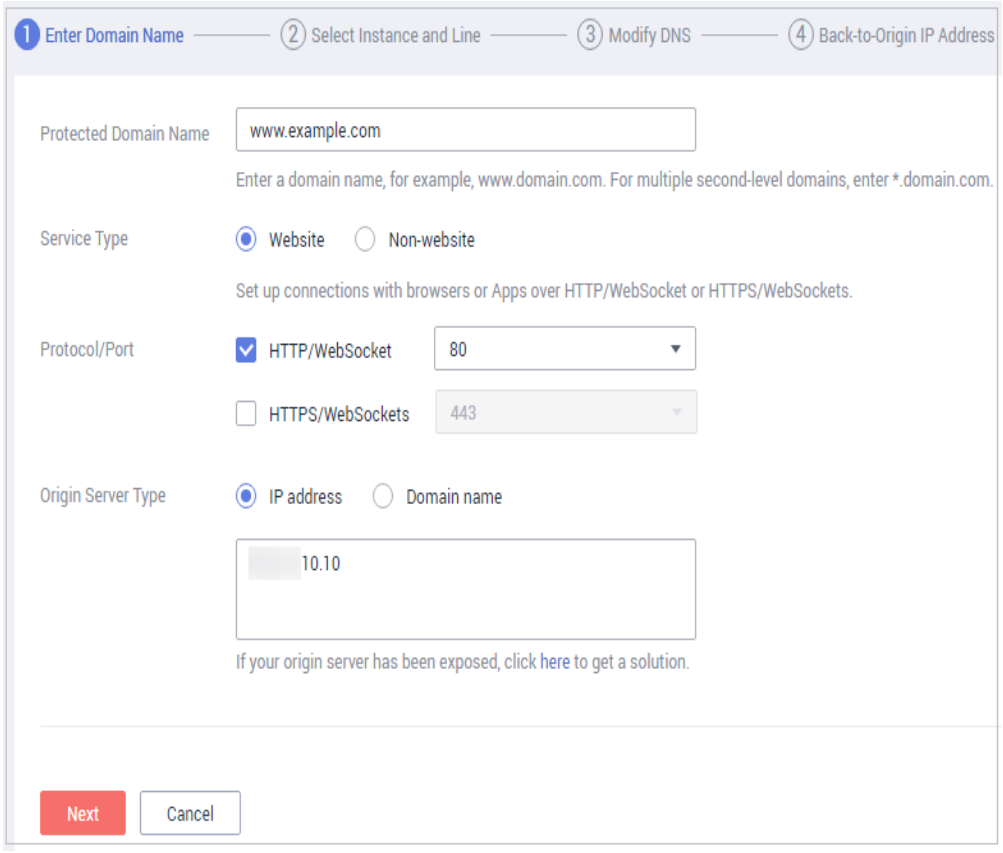
Figure 4-2 Entering domain name information for a website service



- **For an HTTPS/WebSockets protocol:**
  Set **Service Type** to **Website** and **Protocol/Port** to **HTTPS/WebSockets**. Available HTTPS/WebSockets ports are **443**, **7443**, and **8443**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-3 Entering domain name information for a website service



4.1.2 What Carrier Lines Does AAD Support?

Currently, AAD offers three line packages:

- CTCC & CUCC & CMCC
- CTCC & CUCC & BGP
- BGP

4.1.3 What Basic and Elastic Protection Bandwidths Does Each Carrier Line Support?

- **CTCC & CUCC & CMCC**:
  - Basic protection bandwidth: 10 Gbit/s to 600 Gbit/s
  - Elastic protection bandwidth: 10 Gbit/s to 600 Gbit/s
- **CTCC & CUCC & BGP**:
  - Basic protection bandwidth: 10 Gbit/s to 30 Gbit/s
  - Elastic protection bandwidth: 10 Gbit/s to 600 Gbit/s
- BGP
  - Basic protection bandwidth: 10 Gbit/s to 20 Gbit/s
  - Elastic protection bandwidth: 10 Gbit/s to 200 Gbit/s

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The maximum protection bandwidth for one IP address is 600 Gbit/s in the CTCC line, 600 Gbit/s in the CUCC line, 100 Gbit/s in the CMCC line, and 200 Gbit/s in the BGP line.
- In the **CTCC & CUCC & BGP** line, the maximum protection bandwidth for BGP is 200 Gbit/s.

4.1.4 Can I Change My Protection Bandwidths?

- AAD allows you to upgrade the basic protection bandwidth.
- AAD allows you to modify the elastic protection bandwidth for a maximum of three times a day. The modification takes effect immediately.

4.1.5 Can an AAD Origin Server Use a CDN CNAME?

No. Currently, AAD supports only HUAWEI CLOUD WAF CNAME records.

4.1.6 How Many Ports and Protected Domain Names Can an AAD Instance Provide? Is the Quota Expansion Supported?

You can buy a maximum of five AAD instances by default. Each AAD instance provides 50 protected domain names and 50 ports for free. A maximum of 200 protected domain names and 200 ports are supported. If the quota is insufficient, **submit a service ticket** to apply for a quota increase.

For details about AAD specifications, see **AAD specifications**.

4.1.7 What Is the Maximum Protection Capability When I Purchase 10 Gbit/s as the Basic Protection Bandwidth and 20 Gbit/s as the Elastic Protection Bandwidth?

Your maximum protection capability is 20 Gbit/s. The maximum protection capability is the elastic protection bandwidth. Do not mistake the elastic protection bandwidth as an increment over the basic protection bandwidth. If you purchase the same value for your basic and elastic protection bandwidths, the elastic protection capability will not take effect.

For example, if you purchase 50 Gbit/s for both the basic and elastic protection bandwidths, the maximum protection capability is 50 Gbit/s and the elastic protection will not take effect.

4.1.8 Does AAD Use a Public IP Address to Switch Traffic Back to Origin Servers?

Yes. AAD uses public IP addresses as the back-to-origin IP addresses to switch scrubbed traffic back to the origin servers over the public network.

 Copyright © Huawei Technologies Co., Ltd.

4.1.9 What Is the Maximum Number of Domain Names AAD Can Protect?

By default, one AAD instance can protect 50 domain names for free. You can pay to increase this quota and a maximum of 200 domain names are available. If you want to purchase more than 200 domain names, purchase another AAD instance.

4.1.10 How Much Additional Latency Will Be Incurred When AAD Is Deployed?

After AAD is deployed, the average latency is increased by 30 ms.

4.1.11 Is There a Limit to the Number of Concurrent Requests?

The number of concurrent requests that can be processed by a system indicates the load capacity of the system. A website needs to process concurrent requests sent from users.

AAD does not limit the number of concurrent requests. AAD supports multiple forwarding protocols such as TCP, UDP, HTTP, HTTPS, Websocket, and Websockets. AAD does not limit the number of TCP and HTTP connections.

4.1.12 How Do I Disable Advanced Anti-DDoS?

Advanced Anti-DDoS cannot be directly disabled on the console. If you do not want to use AAD anymore, delete the domain names added to AAD for protection first and unsubscribe from AAD.

4.2 Access Configuration

4.2.1 Can I Connect My Service System to AAD If It Is Not Running on HUAWEI CLOUD?

Yes, as long as its IP address is accessible on the Internet.

4.2.2 How Do I Connect Website Services to AAD?

You can use the Canonical Name (CNAME)-based access to connect your website service to AAD so that access traffic will be directed to the high-defense IP address. All public network traffic is diverted to the high-defense IP address, and therefore user services on the origin servers are protected against DDoS attacks.

For details about how to connect website services to AAD, see **Connecting a Website Service to AAD**.

4.2.3 How Do I Connect Non-Website Services to AAD?

Non-website services include Apps and PC client services. After a non-website service is connected to AAD, the service IP address of the non-web service is

 Copyright © Huawei Technologies Co., Ltd.

changed to the high-defense IP address. All public network traffic is diverted to the high-defense IP address, and therefore user services on the origin servers are protected against DDoS attacks. For such services, you can configure CNAME records in DNS or directly configure high-defense IP addresses on clients to use AAD.

For details about how to connect non-website services to AAD, see **Connecting a Non-website Service to AAD**.

4.2.4 How Do I Check Whether a Protected Domain Name Is Correctly Configured After I Connect It to AAD?

Step 1 Log in to the management console.

Step 2 **How Do I Connect My Service System to AAD?** describes how to add domain names to be protected to AAD.

Step 3 Choose **Security** > **Advanced Anti-DDoS** > **Domain Name Configuration** and copy the **CNAME** value of the domain name to be tested.

Step 4 Ping the **CNAME** value and record the corresponding IP address (for example, 192.168.0.1).

Step 5 Modify the local **hosts** file. This section uses Windows as an example. Go to the **C:\Windows\System32\drivers\etc** directory and open the **hosts** file. Add a record to the file, as shown in the following figure:

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      [redacted]                    # source server
#      [redacted]                    # x client host

# localhost name resolution is handled within DNS itself.
#   [redacted]       localhost
#   ::1              localhost

192.168.0.1    www.test.com
```

Step 6 Clear the browser cache and enter the domain name in the address box to check whether you can access the domain name properly.

----End

 Copyright © Huawei Technologies Co., Ltd.

4.2.5 What Can I Do When Message "Invalid request" Is Displayed When I Upload an HTTPS/WebSockets Certificate?

The causes and solutions for that message are as follows:

- The certificate name is too long.

  Solution: Change the certificate file name to one shorter than 10 characters.
- The certificate file name contains special characters.

  Solution: Use only letters and digits to name the certificate.
- The certificate content does not meet requirements.

  Solution: Delete information that does not meet the requirements of the certificate and private key input formats as described in FAQ "How Do I Convert a Non-PEM Certificate into a PEM One", for example, delete information in front of **---BEGIN CERTIFICATE---**.

4.2.6 How Do I Convert a Non-PEM Certificate into a PEM One?

- **Converting a .cer or .crt certificate into a .pem one**

  Change the name extension of the certificate file.

  For example, change **certificate.cer** to **certificate.pem**.
- **Converting a .pfx certificate into a .pem one**

  Use OpenSSL to convert the certificate.

  ```
  # Certificate extraction command
  openssl pkcs12 -in certificate.pfx -nokeys -out cert.pem
  # Private key extraction command
  openssl pkcs12 -in certificate.pfx -nocerts -out key.pem -nodes
  ```
- **Converting a .p7b certificate into a .pem one**

  Use OpenSSL to convert the certificate.

  a. Run the following command to convert the certificate:

  ```
  openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer
  ```

  b. Obtain the certificate content in **outcertificat.cer**.

  c. Save the content in .pem format.
- **Converting a .der certificate into a .pem one**

  Use OpenSSL to convert the certificate.

  ```
  # Certificate extraction command
  openssl x509 -inform der -in certificate.cer -out certificate.pem
  # Private key extraction command
  openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem
  ```

4.2.7 How Do I Enable Both AAD and WAF?

Perform the following operations to enable both AAD and WAF:

1. Obtain the CNAME value of the domain name on the WAF management console.
2. Configure the WAF CNAME in AAD.
3. Modify DNS configuration.

 Copyright © Huawei Technologies Co., Ltd.

For details about how to enable both AAD and WAF, see **Enabling Both AAD and WAF on HUAWEI CLOUD**.

After the configuration is complete, traffic is processed by AAD first and then forwarded to WAF, thereby achieving collaborative protection.



4.2.8 Can an Unrecorded Domain Name Be Protected by AAD (Chinese Mainland)?

AAD (Chinese Mainland) is recommended if your server is deployed in the Chinese Mainland. You must obtain an ICP license before using AAD (Chinese Mainland) to protection your domain names.

For details about how to purchase an AAD instance, see **Purchasing an AAD Instance**.

4.2.9 How Do I Connect My Service System to AAD?

- If your system provides services through a domain name, you need to modify the DNS configuration to resolve the domain name to the CNAME record provided by HUAWEI CLOUD.
- If your system provides services through an IP address, change the IP address to a high-defense IP address.

4.2.10 How Is CNAME-based Access Implemented?

What is a CNAME record?

A Canonical Name (CNAME) record is a type of DNS record that maps an alias name to a true or canonical domain name. A DNS A record maps a domain name to an IP address, whereas a CNAME record maps a domain name to another domain name (alias of that domain name). For example, CNAME ccd01c25c8535fa4.huaweisafedns.com is configured for domain name www.abc.com. When a user accesses www.abc.com, the DNS protocol automatically obtains its CNAME alias ccd01c25c8535fa4.huaweisafedns.com and uses the alias to obtain the real IP address.

What are the advantages of CNAME-based access?

- Easy to Use

  You only need to modify the resolution configuration with the DNS service provider (for example, DNS on HUAWEI CLOUD).

  The CNAME records generated in multiple lines for the same domain name are the same. You only need to configure one CNAME resolution record. Then AAD automatically configures the CNAME record for multiple high-defense IP addresses used by the domain name. When the high-defense IP address is changed, AAD updates CNAME mapping automatically, without requiring any manual DNS configuration modification.

 Copyright © Huawei Technologies Co., Ltd.

- Excellent access performance

  If multiple lines are configured for a domain name, AAD can schedule access traffic based on the traffic source and select the optimal line to ensure the best access performance.

- High reliability

  You can select multiple lines for one domain name. If the high-defense IP address of a line encounters an exception, AAD automatically switches CNAME resolution to other available lines, ensuring service continuity.

How is a carrier line resolved during CNAME resolution on HUAWEI CLOUD?

- **CTCC & CUCC & CMCC**: The CTCC line is resolved to the CTCC high-defense IP address, the CUCC line to the CUCC high-defense IP address, the CMCC line to the CMCC high-defense IP address, and other carriers to the CTCC high-defense IP address.
- **CTCC & CUCC & BGP**: The CTCC line is resolved to the CTCC high-defense IP address, the CUCC line to the CUCC high-defense IP address, and other carriers to the BGP high-defense IP address.
- **BGP**: All lines are resolved to the high-defense IP address provided for the BGP line.

What will I configure for CNAME-based access further if I have configured line-based resolution?

Generally, the CNAME resolution for one default line is required to replace line-based resolution. HUAWEI CLOUD will complete the resolution automatically.

The CNAME records provided by HUAWEI CLOUD are capable of line-based resolution. Based on the lines you purchased, HUAWEI CLOUD will perform line-based resolution automatically.

4.2.11 How Does AAD Distribute Traffic When There Are Multiple Origin Servers?

AAD distributes traffic evenly to origin servers in polling mode.

4.2.12 How Do I Check Whether a Back-to-Origin IP Address Has Been Whitelisted on My Origin Server?

Check servers and security devices to ensure that they have whitelisted the back-to-origin IP addresses and will not limit or block access traffic. For example:

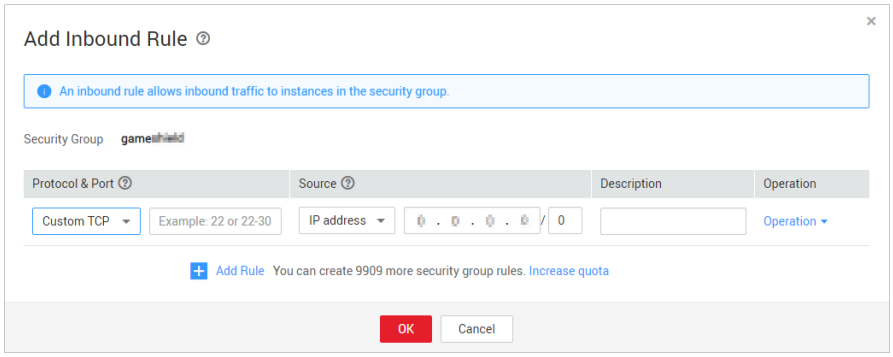
- If your origin servers are HUAWEI CLOUD servers, configure ACLs and security groups to permit the back-to-origin IP addresses.
  a. Log in to the management console.
  b. Click  in the upper left corner to select a region and a project.
  c. Click **Service List**. Under **Network**, click **Virtual Private Cloud**.
  d. Add a security group rule to allow access from the back-to-origin IP address.
     i. In the navigation pane on the left, choose **Access Control** > **Security Groups**.

 Copyright © Huawei Technologies Co., Ltd.

ii. On the **Security Group** page, locate the target security group and click **Manage Rule** in the **Operation** column to switch to the page for managing inbound and outbound rules.

iii. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.

Click **+** to add more inbound rules.



Parameter	Description
Protocol & Port	Specifies the protocol and port for which a security group rule takes effect.
Source	Select **IP address** and enter the back-to-origin IP address.

iv. Click **OK**.

e. Add an ACL rule to allow access from the back-to-origin IP address.

i. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.

ii. Locate the target network ACL on the **Network ACLs** page, and click the network ACL name to switch to the details page.

iii. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.

You can click **+** to add more inbound rules.

Parameter	Description
Action	Select **Permit**.
Protocol	Specifies the protocol supported by the network ACL. This parameter is mandatory. You can select a value from the drop-down list. The value can be **TCP**, **UDP**, **ICMP**, or **ANY**. If **ICMP** or **ANY** is selected, you do not need to specify port information.
Source	Set this parameter to the back-to-origin IP address.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Source Port Range	Specifies the source port number or port number range. The value ranges from 0 to 65535. To specify a range, enter two port numbers connected by a hyphen (-). The range cannot start with 0, for example, **1-100**. This parameter is mandatory if you set **Protocol** to **TCP** or **UDP**.
Destination	Specifies the destination IP address to which the traffic is permitted. The default value is **0.0.0.0/0**, indicating that traffic can be sent to all IP addresses. For example: xxx.xxx.xxx.xxx/32 (an IP address) xxx.xxx.xxx.0/24 (a subnet) 0.0.0.0/0 (any IP address)
Destination Port Range	Specifies the destination port number or port number range. The value ranges from 0 to 65535. To specify a range, enter two port numbers connected by a hyphen (-). The range cannot start with 0, for example, **1-100**. This parameter is mandatory if you set **Protocol** to **TCP** or **UDP**.

iv. Click **OK**.

- If your origin servers already have their own security policies, ensure that they have taken effect. Some custom security policies may take effect only after a restart.

4.2.13 How Do I Change the Exposed IP Address of an Origin Server?

Scenarios

If the origin server is still under attacks even after AAD is configured, change the IP address of the origin server because it has been exposed.

This topic uses the EIP of an ECS as an example to describe how to change the origin server IP address.

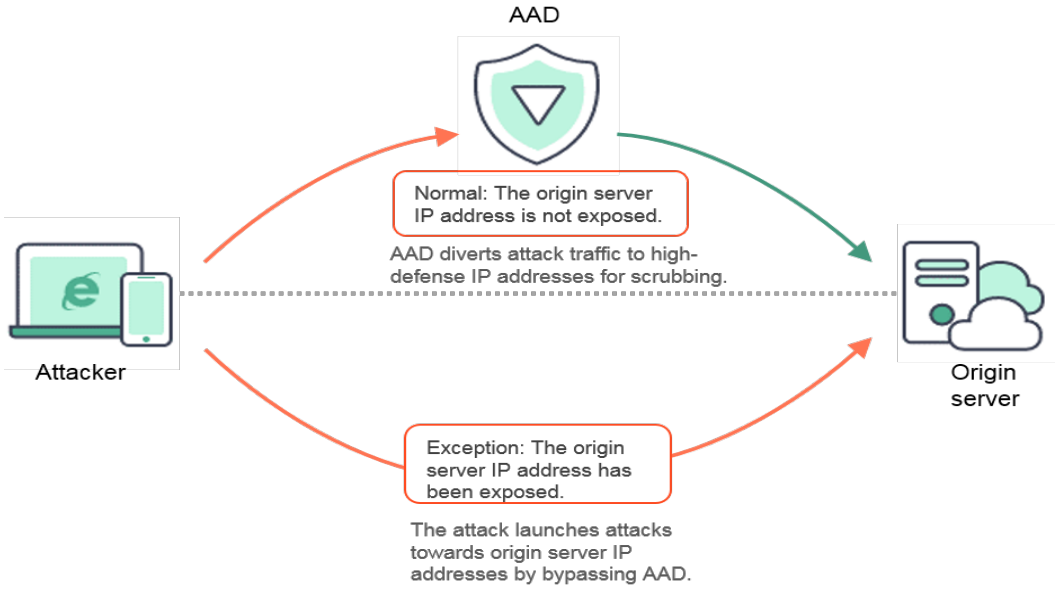
Typical causes

- If the IP address of an origin server has been attacked by hackers before the AAD service is configured, the origin server IP address has been exposed to attackers.

 Copyright © Huawei Technologies Co., Ltd.

- Some attackers may record the IP addresses used by exposed origin servers. Even after AAD is configured, the attackers will bypass AAD and directly launch attacks towards the known IP addresses. In this case, it is best practice to change the IP addresses of the origin servers.

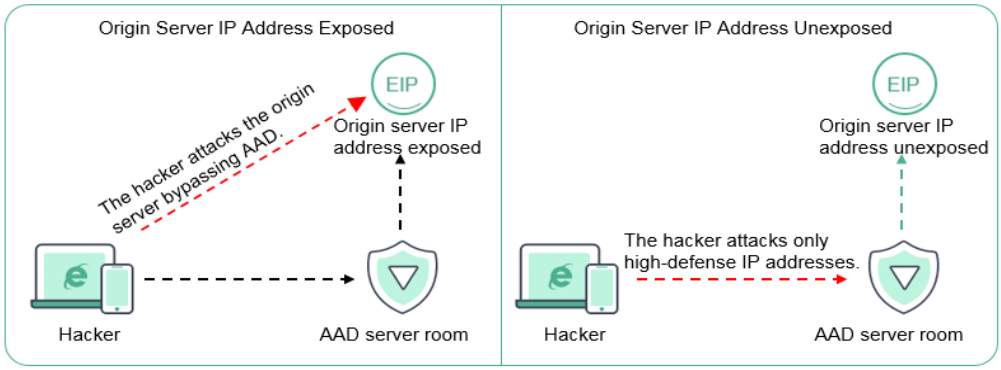
Figure 4-4 Typical causes



Solution

An ECS is used as an example. If the EIP of the ECS is exposed, you can reassign an unexposed EIP to the ECS to change the IP address of the origin server.

Figure 4-5 Mechanism



Procedure

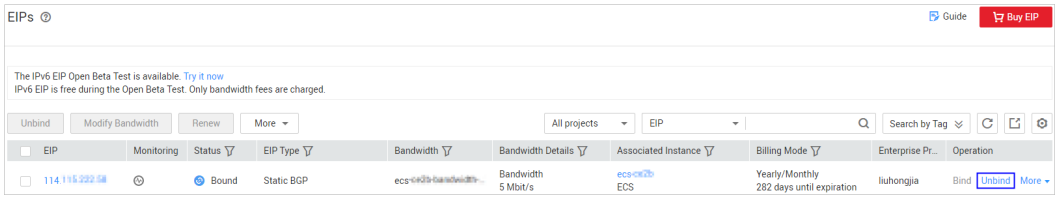
Step 1 Log in to the management console.

Step 2 Under **Network**, choose **Virtual Private Cloud**. The **Network Console** is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Step 3 In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **EIPs**. The **EIPs** page is displayed.

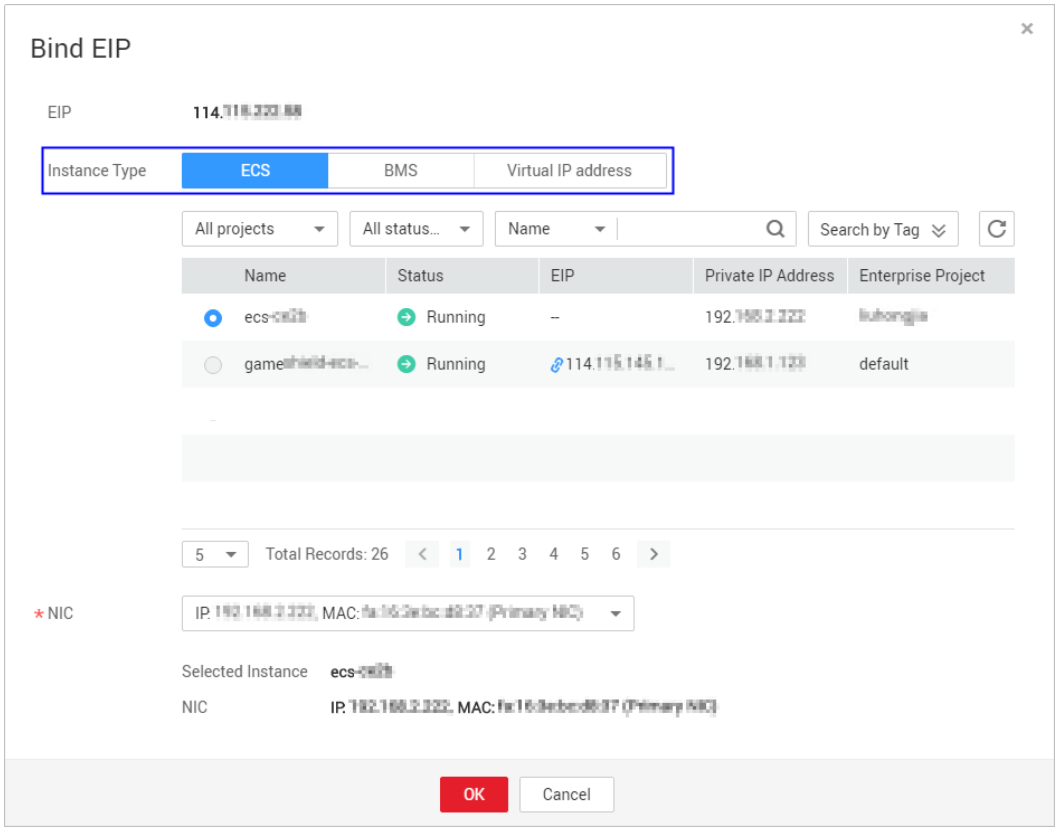
Step 4 Locate the row containing the target EIP and click **Unbind** in the **Operation** column.



Step 5 Click **OK**.

Step 6 Assign another IP address for the ECS. Locate the row containing the target EIP and click **Bind** in the **Operation** column.

Step 7 Select the desired instance.



Step 8 Click **OK**.

----End

4.2.14 How Do I Query the Back-to-Origin IP Address Range?

If a firewall has been configured for your origin server, add the back-to-origin IP address range to the whitelist of the firewall (or another protective software) of the origin server.

 Copyright © Huawei Technologies Co., Ltd.

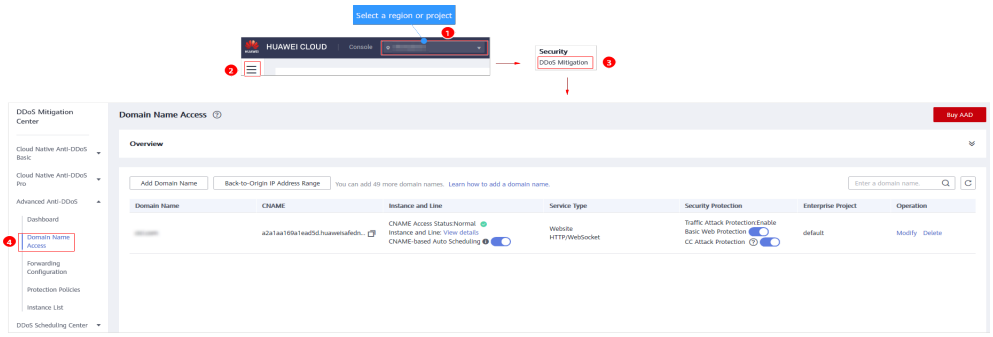
This topic describes how to query the back-to-origin IP address range and whitelist them on the firewall or another protective software on the origin server.

Procedure

Step 1 Log in to the management console.

Step 2 Follow the procedure shown in the following figure to enter the **Domain Name Access** page.

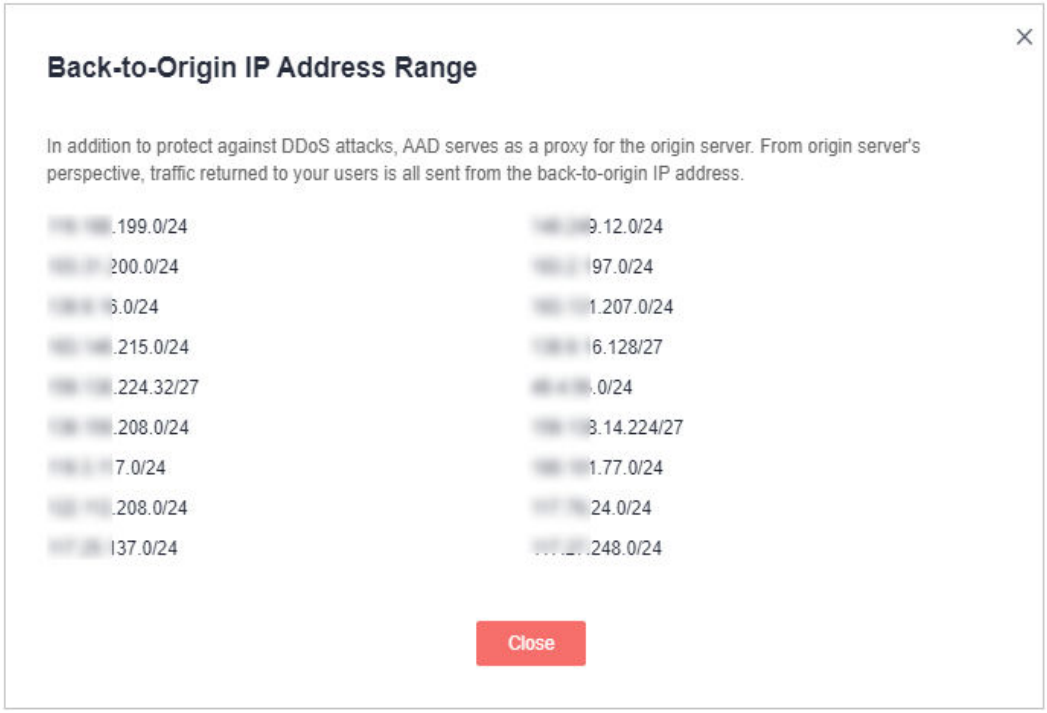
Figure 4-6 Domain Name Access page



Step 3 On the displayed page, click **Back-to-Origin IP Address Range**.

Step 4 In the displayed **Back-to-Origin IP Address Range** dialog box, view the back-to-origin IP address range and then whitelist the IP addresses to the firewall or other protective software on the origin server.

Figure 4-7 Back-to-Origin IP Address Range



----End

 Copyright © Huawei Technologies Co., Ltd.

4.2.15 How Do I Delete AAD Instances?

You can **submit a service ticket** and contact Huawei technical support to delete AAD instances.

4.2.16 Can I Migrate Enterprise Project Resources After Adding the Protected Domain Name?

AAD supports multi-project management, allowing enterprises to manage their AAD resources by project and migrate project resources. However, you cannot change the enterprise project of an AAD instance for which a domain name is added for protection. You can perform the following operations:

4.2.17 Can I Build My Own Anti-DDoS System Using HUAWEI CLOUD ECSs?

Yes, you can. You can set up an anti-DDoS system on your own for your business using ECSs of HUAWEI CLOUD. However, HUAWEI CLOUD will block or freeze traffic when detecting frequent flood attacks, which may interrupt your normal service running. Therefore, you are advised to purchase the AAD service to defend against attacks while ensuring your service continuity.

4.2.18 How Do the AAD Blacklist and Whitelist Protect Customer's Servers?

You can configure the blacklist and whitelist for AAD instances. Blacklisted IP addresses will be blocked, and whitelisted IP addresses will be allowed through. For details, see **Configuring a Blacklist and a Whitelist**. If you need to protect the origin servers, contact HUAWEI CLOUD security technical experts.

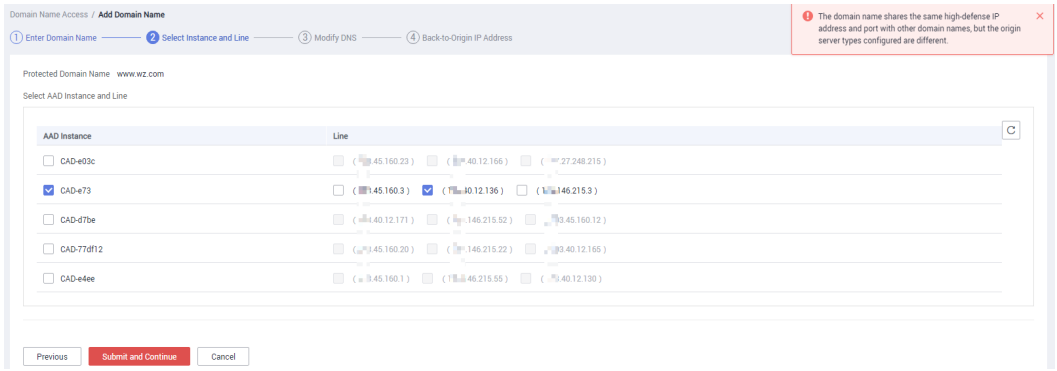
4.2.19 What Can I Do If the System Displays a Message Indicating that the Domain Name to Be Added Shares the High-Defense IP Address and Port with Another Domain Name But the Domain Names Have Different Origin Server Types When I Connect Website Services to AAD?

Symptom

Domain names cannot be added when website services are connected to AAD. A message, indicating the domain name to be added shares the same high-defense IP address and port with other domain names, while the origin server types configured are different, is displayed.

Copyright © Huawei Technologies Co., Ltd.

Figure 4-8 Domain name that failed to be added



Possible Causes

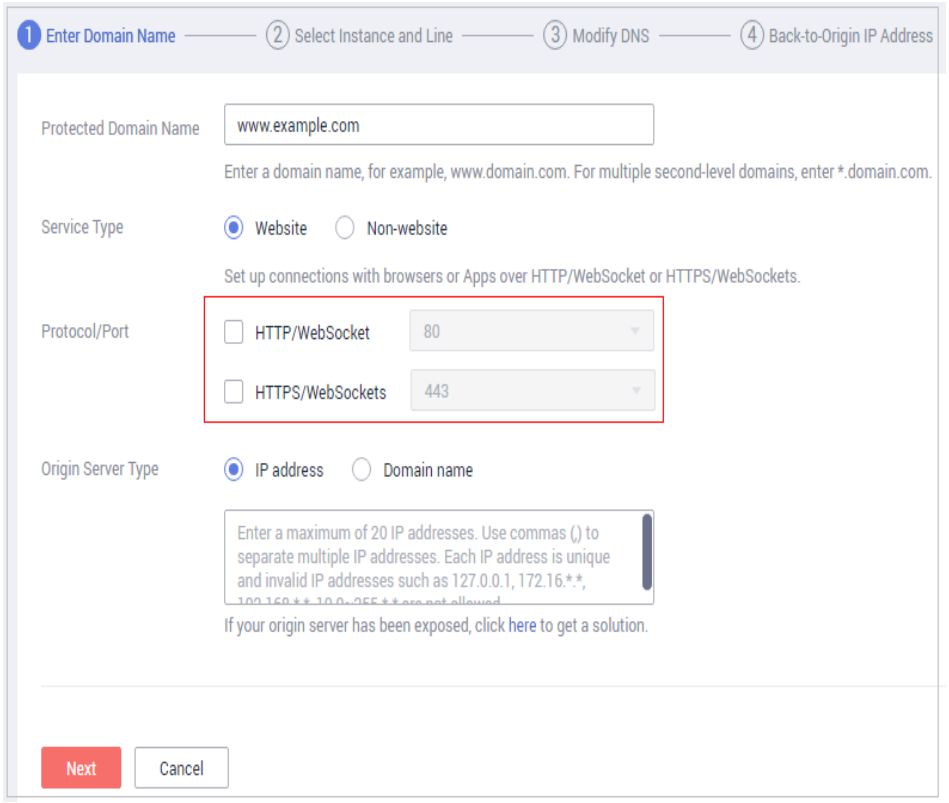
The domain name to be added shares the same high-defense IP address and protocol/port with other domain names that have been added when the origin server types configured are different.

Solution

Solution 1: Reselect the protocol/port for the domain name to be added. Ensure that the domain name to be added does not use the same protocol/port with domain names that have been added.

1. Click **Previous** in Figure 4-8 to switch back to the **Enter Domain Name** page, and reset **Protocol/Port**.

Figure 4-9 Resetting **Protocol/Port**



 Copyright © Huawei Technologies Co., Ltd.

2. Click **Next**. On the displayed page, select an instance and line and click **Submit and Continue**.

   Follow the instructions described in **Connecting a Website Service to AAD** to finish the follow-up operations.

Solution 2: Select another line for the domain name to be added. Ensure that the domain name to be added does not use the same line as domain names that have been added.

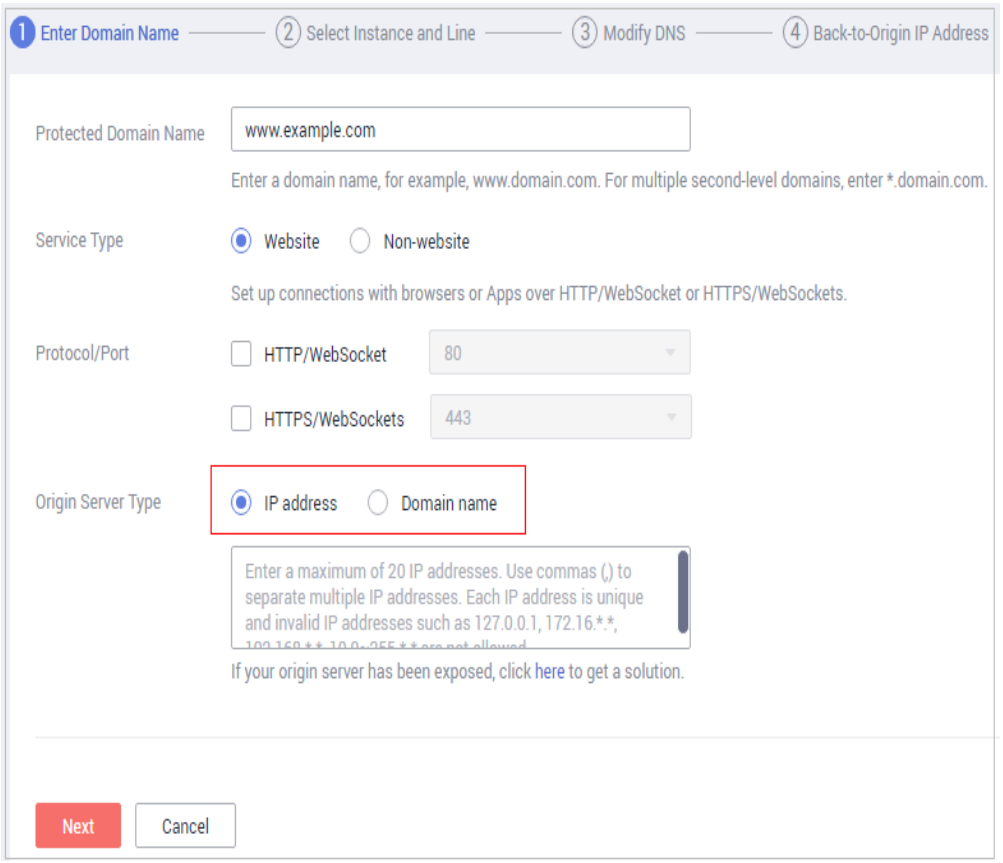
1. Select another line for the domain name to be added in **Figure 4-8**.
2. Click **Submit and Continue**.

   Follow the instructions described in **Connecting a Website Service to AAD** to finish the follow-up operations.

Solution 3: Reset Origin Server Type for the domain name to be added. Ensure that the origin server type of the domain name to be added is the same as that of other domain names that have been added.

1. Click **Previous** in **Figure 4-8**. On the displayed page, reset **Origin Server Type** and ensure the value of this parameter configured for the domain name to be added is the same as that of other domain names that have been added.

   Figure 4-10 Setting the origin server type



2. Click **Next**. On the displayed page, select an instance and line and click **Submit and Continue**.

Copyright © Huawei Technologies Co., Ltd.

Follow the instructions described in **Connecting a Website Service to AAD** to finish the follow-up operations.

4.2.20 Does the Back-to-Origin IP Address Target the Origin Server IP Address or Domain Name After AAD Is Configured for Website Services?

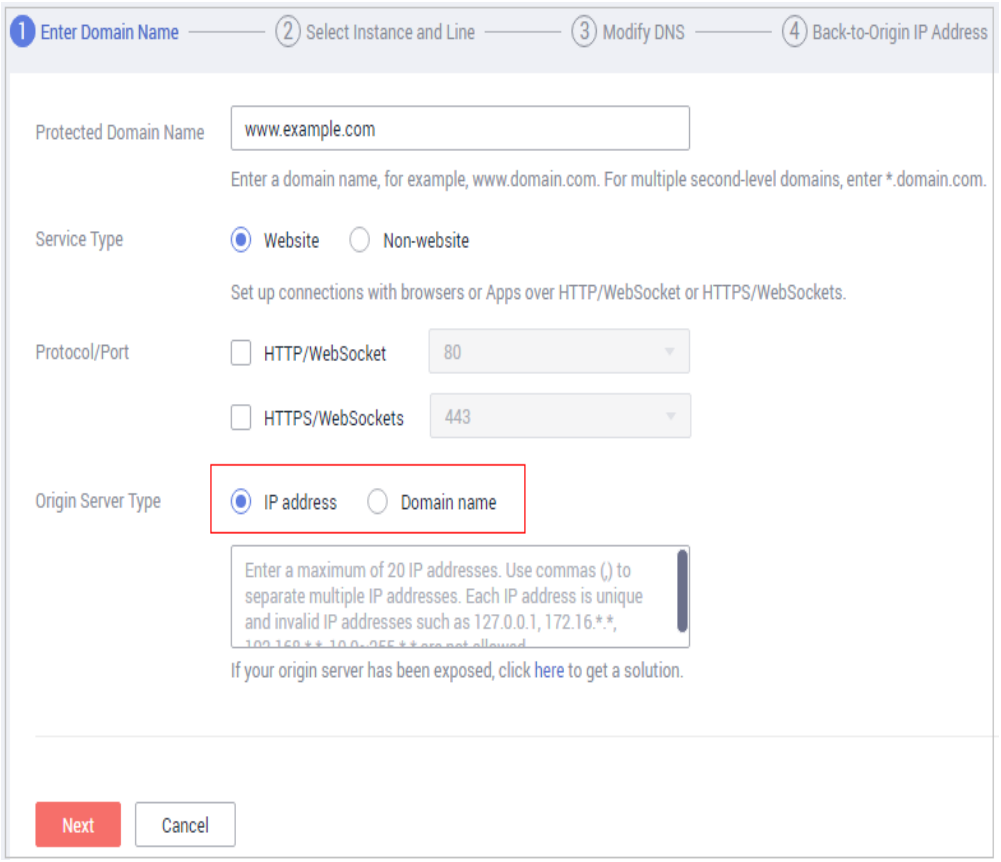
You can select **IP address** or **Domain name** for **Origin Server Type** when you configure the domain name for website services. The back-to-end IP address targets the origin server IP address or domain name based on the origin server type:

- If you select **IP address** for **Origin Server Type**, the target is the origin server IP address.
- If you select **Domain name** for **Origin Server Type**, the target is the origin server domain name.

NOTICE

If you set **Origin Server Type** to **Domain name**, ensure you have purchased the Web Application Firewall (WAF) service because only HUAWEI CLOUD WAF CNAME is supported. You need to enter a WAF CNAME address in the text box. For details, see **Buying WAF**.

Figure 4-11 Setting the origin server type



 Copyright © Huawei Technologies Co., Ltd.

4.2.21 Can I Configure the Same Port in Forwarding Rules?

The forwarding protocol and forwarding port in each forwarding rule must be unique. The forwarding port and the port that is configured in adding a domain name can be the same.

4.2.22 Do I Need to Configure Forwarding Rules for All Lines of an AAD Instance?

You need to configure forwarding rules for all lines of an AAD instance when configuring a forwarding rule for the instance.

4.3 Faults

4.3.1 What Should I Do When Encountering an Access Freezing, Delay, or Failure?

Symptom

Access from a client to the high-defense IP address is frozen, has long delays, or loses packets.

Troubleshooting

- **Cross-network access**

  AAD supports CTCC, CUCC, CMCC, and BGP lines. Access delays and packet loss may occur if cross-network resolution is configured on DNS or cross-network back-to-origin is configured for origin server IP addresses on AAD.

  Solution:

  - On the DNS console: Check DNS configuration.

    This fault will not occur if you use the CNAME resolution provided by HUAWEI CLOUD. If you are using A record resolution, configure high-defense IP addresses based on the carrier of the line transmitting the access traffic. If your traffic is transmitted over the BGP line, retain the default high-defense IP address configuration. HUAWEI CLOUD is not responsible for the packet loss or delays caused by improper DNS configuration.
  - On the AAD console: Check the origin server IP address.

    If the origin server uses a specific carrier line, packet loss and delays exist inevitably during cross-network access, and HUAWEI CLOUD is not responsible for the packet loss and delays.

    If the origin server uses lines of multiple carriers, add origin server IP addresses accordingly based on the high-defense IP addresses of the carrier lines, for example, associate a CTCC high-defense IP address with a CTCC origin server IP address. HUAWEI CLOUD is not responsible for the packet loss or delays caused by improper back-to-origin line configuration.

 Copyright © Huawei Technologies Co., Ltd.

- **Backend server exceptions**

  Troubleshoot the fault based on the origin server type configured for the high-defense IP address.

  - **The origin server is a load balancer.**

    To resolve the problem, perform the following steps:

    i. Run TCPing using the IP address and port number of the load balancer to locate the fault.

    ii. Check the load balancer status (such as number of connections and backend servers).

    iii. Check whether blacklists, whitelists, or other access control policies have been configured for the load balancer and ensure that the back-to-origin IP address range is allowed through.

    iv. Check backend servers and networks of the load balancer for any IP address blocking policies on firewalls.

  - **The origin server is a cloud server.**

    To resolve the problem, perform the following steps:

    i. Run TCPing using the IP address and port number of the cloud server to locate the fault.

    ii. Check whether the server has encountered exceptions, such as black holes, scrubbing incidents, high CPU usage, slow database requests, and outbound bandwidth exhaustion.

    iii. Check whether blacklists, whitelists, or other access control policies have been configured for the cloud server and ensure that the back-to-origin IP address range is allowed through.

    iv. Check the cloud server or networks for security software or IP address blocking policies that block the back-to-origin IP addresses.

- **Whether high-defense IP addresses have scrubbing incidents**

  - **High-defense IP addresses have experienced scrubbing incidents.**

    To resolve the problem, perform the following steps:

    i. Run TCPing to check for and record delays and packet loss on attacked ports.

    ii. Run TCPing to check for and record delays and packet loss on non-attacked ports.

    Locate the fault by checking the records against the following table.

 Copyright © Huawei Technologies Co., Ltd.

Table 4-1 Results

Delay and Packet Loss on Attacked Ports	Delay and Packet Loss on Non-attacked Ports	Cause Analysis
Yes	No	The scrubbing policy is executed properly on attack traffic. Check the backend server status and identify the server's attack defense capability. If the attack defense capability is weak, you need to enforce a powerful defense policy.
Yes	Yes	Normal traffic is scrubbed by the scrubbing policy. You can submit a service ticket for background troubleshooting.
No	No	The fault is not caused by the scrubbing policy.
No	Yes	Generally, this situation does not exist.

In the first two cases, you are advised to **submit a service ticket**. To enforce a more powerful defense policy, you need to provide details about your server's attack defense performance, including:

- Normal user access
- Service interaction processes
- Application service capabilities

– **High-defense IP addresses have not experienced scrubbing incidents.**

The fault is not caused by attacks.

- **High-defense IP addresses are blocked by black holes.**

  The high-defense IP address is blocked by a black hole if the attack traffic towards this IP address exceeds the configured elastic protection bandwidth. You can check whether packet loss is caused by a black hole.

 Copyright © Huawei Technologies Co., Ltd.

If so, you are advised to purchase a large elastic protection bandwidth and adjust your service systems to make them capable of switching traffic to another line when a black hole is triggered.

4.3.2 Why Is Error 504 Displayed When I Access a Website After AAD Is Configured?

Symptom

When a user visits a website with AAD configured, error code 504 is displayed after a long period of wait time.

Possible Causes

It takes a long period of time for the website to process some POST requests, and the time required exceeds the connection timeout threshold of AAD. As a result, AAD proactively drops the connection.

- The default TCP connection timeout is 900s.
- The default HTTP/WebSocket or HTTPS/WebSockets connection timeout is 120s.

Solution

It is recommended that you deploy a heartbeat mechanism to process time-consuming tasks at the application layer. This mechanism helps keep connections alive during the wait time.

For occasional time-consuming requests, you can send them directly to cloud servers by bypassing AAD.

4.3.3 How Do I Identify the Type of Attacks?

You can view the traffic report on the **Dashboard** page of AAD to identify whether the attacks are CC attacks or DDoS attacks.

Procedure

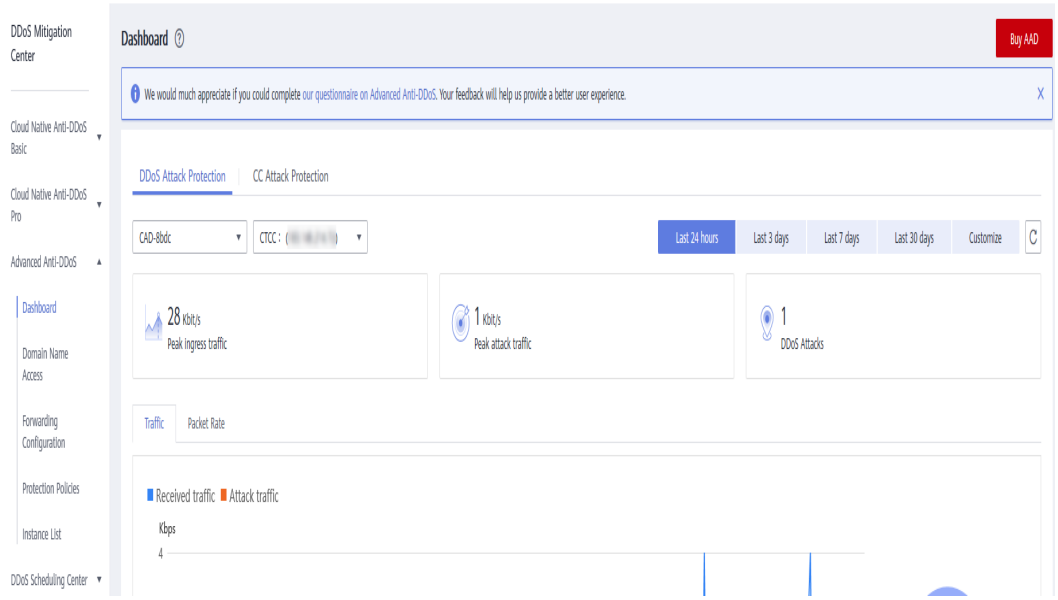
If both CC and DDoS attacks are launched, you can use the following methods to quickly identify the attack type:

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

Step 2 Follow the procedure in the following figure to enter the **Advanced Anti-DDoS** console page. In the navigation pane on the left, choose **Dashboard** and then select the **DDoS Attack Protection** tab.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-12 DDoS attack protection entry



Step 3 View the traffic reports respectively on the **DDoS Attack Protection** and **CC Attack Protection** pages and determine the attack types accordingly.

Attack Type	DDoS Attack Protection Report	CC Attack Protection Report
DDoS Attack	• The report indicates attack traffic fluctuations. • Traffic scrubbing has been triggered.	• There is no associated traffic fluctuation in the report.
CC Attacks	• The report indicates attack traffic fluctuations. • Traffic scrubbing has been triggered.	• There are associated traffic fluctuations in the report.

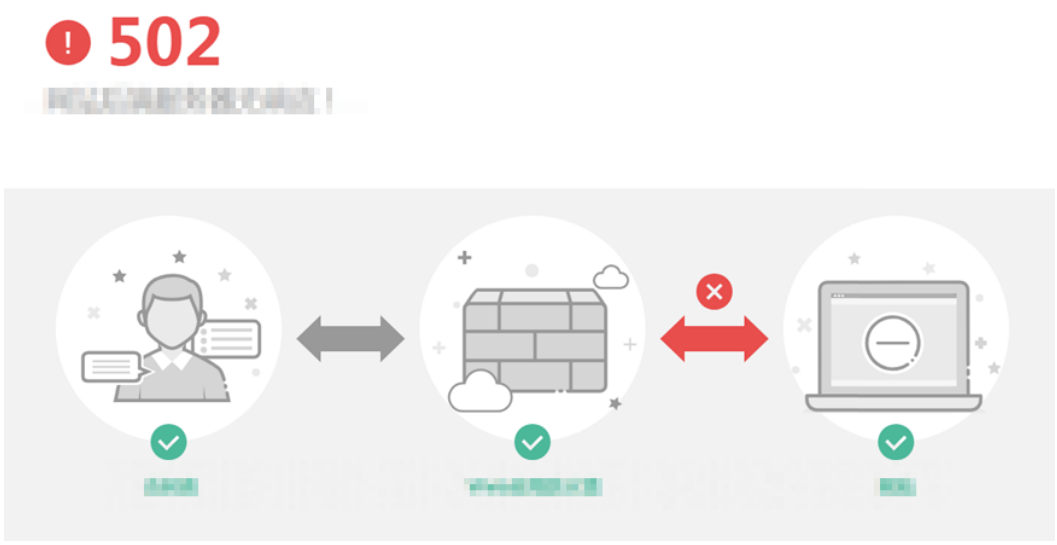
----End

4.3.4 What Should I Do If Error 500, 502, or 504 Is Reported When I Access My Website After I Enable Basic Web Protection for My Domain Name?

Errors 500, 502, or 504 may be displayed when you access your website after enabling basic web protection for it. The error page may also display connection failure with WAF and your website, as shown in **Figure 4-13**.

Copyright © Huawei Technologies Co., Ltd.

Figure 4-13 Error 502



There are many possible causes, such as firewall interception, incorrect origin server configuration, insecure HTTPS/WebSockets versions, and back-end server performance problems.

The following are the possible causes and solutions:

- Interception by the firewall, security protection software installed on the back-end server, or the rate limiting policy

  Symptom: Error 502 is reported at high possibility a while after basic web protection is enabled for a domain name.

  Solution: Add the proxy IP address range to the whitelist of the firewall (hardware or software), security protection software, or rate limiting module.

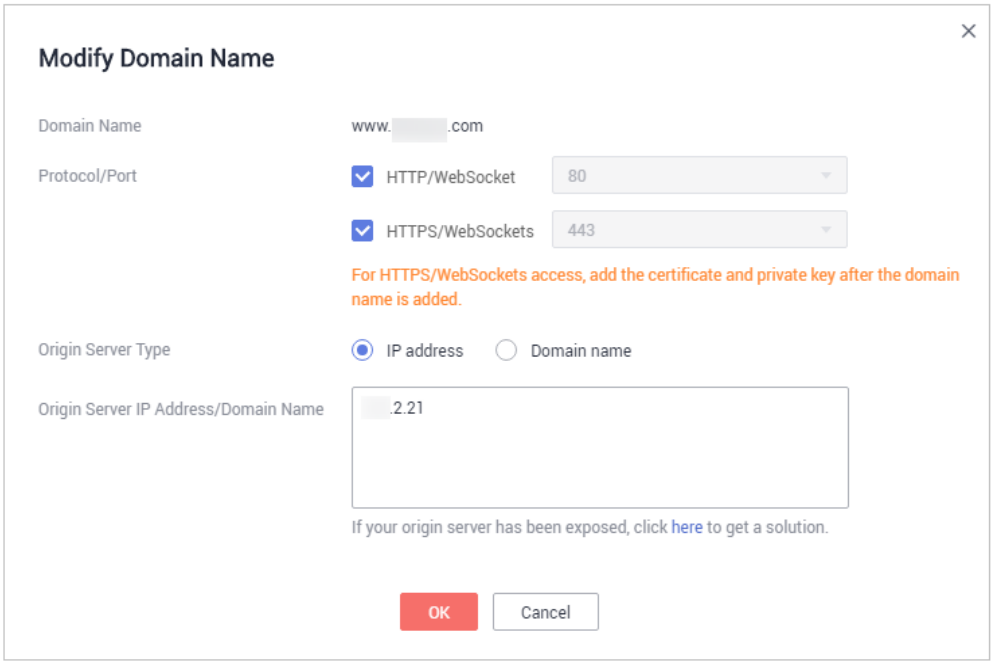
- Incorrect origin server configuration

  Symptom: After basic web protection is enabled for your domain name, you access your website but error 502 or 500 is reported at high possibility (when multiple back-end servers are configured).

  Solution: Locate the corresponding domain name record in the domain name configuration list, click **Edit Domain Name** to check whether the protocol, IP address, and port number used by the origin server are correct.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-14 Modifying domain name configurations



As shown in **Figure 4-14**, you can try to visit http://xx.xx.xx.108:80 and https://xx.xx.xx.108:443 to check whether the back-end service port is enabled.

- Insecure HTTPS/WebSockets versions

  Symptom: After basic web protection is enabled, you access your website and error 502 is reported at high possibility for HTTPS/WebSockets services. However, if you visit by IP address, you can access your website.

  Solution: An earlier SSL version has serious security risks. WAF supports TLS1.2 and later. If such error is displayed because an early version of SSL is used by your server, upgrade your SSL version.

  You can try to visit **https://www.ssllabs.com/ssltest/index.html** to check the SSL version.

  - If the OS of your web server is earlier than Windows Server 2008, the SSL protocol does not support TLS1.2 and later. In this case, you need to upgrade the server OS to Windows Server 2008 or later (or a new version of Linux) and enable TLS1.2 in services such as IIS.
  - If your web server does not run Windows, check whether the SSL protocol is TLS1.2 or later.

- Poor back-end server performance

  Symptom: After basic web protection is enabled, your service works properly. However, when the number of access requests increases, error 502 or 504 increases as well. If you directly access your web server, there is also possibility that the error is returned.

  Solution:

  - Optimize the server configuration, including TCP network parameters and **Ulimit** parameters.
  - Increase the number of back-end ECSs to support increasing requests. AAD supports multiple back-end servers.

 Copyright © Huawei Technologies Co., Ltd.

4.3.5 What Does Duplicate forwarding rule Mean?

You can add multiple forwarding rules to one high-defense IP address. However, the forwarding protocol and port of each rule must be unique. When the parameter is set to the same value for different forwarding rules of the same high-defense IP address, **Duplicate forwarding rule** is displayed.

4.3.6 What Can I Do If I Failed to Configure a Forwarding Rule?

Troubleshooting:

- It takes 2-3 minutes for the forwarding rule configuration to take effect. If the forwarding rule is in the **Processing** state, you can refresh the page later.
- After you add a forwarding rule, the AAD service will check the connectivity of your origin server IP address and port and check for any conflicts with existing forwarding rules. If the configuration fails, check whether the origin server is running properly or whether a forwarding rule has already been configured.

4.3.7 What Can I Do If My UDP Traffic Is Blocked?

If UDP traffic control is enabled for a line, UDP traffic on this line will be blocked. Therefore, ensure that UDP traffic control for the line is disabled. For details, see **Traffic Control**.

4.3.8 Why Is a Domain Name Error Reported When I Add a WAF CNAME for Interworking Between AAD and WAF?

The WAF CNAME is automatically generated during the configuration of the WAF policy. For details about how to add the CNAME, see **Enabling Both AAD and WAF on HUAWEI CLOUD**. If the fault persists, contact HUAWEI CLOUD security technical experts.

4.3.9 How Do I Unblock the Access That Has Been Automatically Blocked Due to the Threshold-Overtopped Attack Traffic?

The access that has been blocked by the carriers will be automatically unblocked in 24 hours.

The black hole lasts 30 minutes by default. However, depending on the number of black holes triggered and peak attack traffic of the day, it may last up to 24 hours.

If you need to unblock access before a black hole becomes ineffective, contact Huawei technical support.

Copyright © Huawei Technologies Co., Ltd.

4.3.10 What Can I Do If the Access Status of a Protected Domain Name Remains Abnormal After the IP Address of the Origin Server Has Been Changed?

Symptoms

After a website service is connected to AAD and the origin server IP address of the protected domain name is changed on the **Domain Name Access** page, the domain name fails to be connected to AAD.

Possible Cause

- The high-defense IP address cannot be accessed.
- The forwarding rule is incorrectly configured
- The origin server IP address has not been added to the whitelist

  If the origin server IP address is not added to the whitelist, AAD may regard the access from the origin server IP address as attack traffic and block it when there are a large number of visits to the domain name.
- The origin server configuration is incorrect. For example, the network jitters or the performance of the origin server is poor.

Suggestion

Step 1 Use a client to access the high-defense IP address and check whether the access is successful.

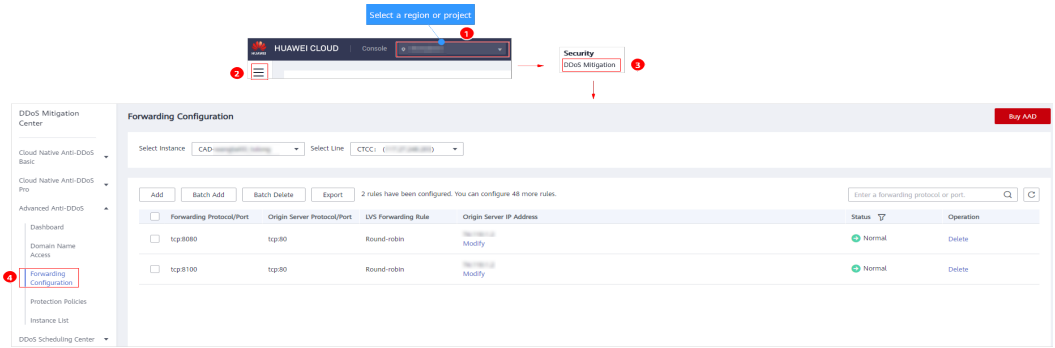
- If yes, go to **Step 2**.
- If no, rectify the fault by referring to **What Should I Do When Encountering an Access Freezing, Delay, or Failure?**.
  - If the domain name is successfully connected, no further action is required.
  - If the domain name still fails to be connected, go to **Step 2**.

NOTE

You can go to the instance list page and view the line information to obtain the high-defense IP address. For details, see **Viewing AAD Instance Information**.

Step 2 Switch to the **Forwarding Configuration** page and check whether the forwarding rule is correctly configured.

Figure 4-15 Forwarding configuration entry



 Copyright © Huawei Technologies Co., Ltd.

- If yes, go to **Step 3**.
- If no, reconfigure the forwarding rule.
  - If the domain name is successfully connected, no further action is required.
  - If the domain name still fails to be connected, go to **Step 3**.

Step 3 Check whether the origin server IP address is added to the whitelist.

- If yes, go to **Step 4**.
- If no, add the origin server IP address to the whitelist.
  - If the domain name is successfully connected, no further action is required.
  - If the domain name still fails to be connected, go to**Step 4**.

Step 4 Check the origin server configuration and contact your website administrator to rectify the fault.

----End

4.4 Product

4.4.1 Can a Third-Party Server or an On-Premises Server Use HUAWEI CLOUD Advanced Anti-DDoS?

Yes. Advanced Anti-DDoS can defend against attacks targeting HUAWEI CLOUD, non-HUAWEI CLOUD, and IDC hosts. For on-premises services, ensure that the IP addresses of the origin servers (users' service systems) can be accessed from the public network.

For details about AAD specifications, see **AAD specifications**.

4.4.2 What Is a Protected IP Address?

The IP address of an origin server is the IP address to be protected. It is a public IP address.

A high-defense IP address is the IP address used by the AAD service to provide protection.

The AAD service uses the high-defense IP address to proxy services for origin servers. All public network traffic is diverted to the high-defense IP address, and therefore user services on the origin servers are protected against DDoS attacks.

4.4.3 Does AAD Support Weighted Back-to-Origin?

No, weighted back-to-origin is not supported currently. AAD switches traffic back to origin servers based on the polling mechanism. You can direct traffic to the public IP address used by ELB and then switch it back to origin servers from ELB based on weight.

 Copyright © Huawei Technologies Co., Ltd.

4.4.4 Can AAD Obtain Real IP Addresses from a Windows Origin Server?

AAD can only obtain the real IP address from the Linux origin server. For details about how to obtain the real IP address from the Linux origin server, see **Obtaining the Source IP Address of a Client**.

4.4.5 Can AAD Be Used Across Regions?

Advanced Anti-DDoS is a global service that is not region-specific. Therefore, it can be used across regions.

4.4.6 Can Multiple Accounts Share Same AAD Instances?

Multiple HUAWEI CLOUD accounts or multiple IAM accounts can share same AAD instances.

- Shared by multiple HUAWEI CLOUD accounts

  For example, you have registered two accounts (**domain1** and **domain2**) on HUAWEI CLOUD. If you delegate the permissions of **domain1** to **domain2**, **domain2** can use the AAD instances of **domain1**.

  For details about agency management, see **Creating an Agency**.
- Shared by multiple IAM accounts

  For example, you have registered an account (**domain1**) on HUAWEI CLOUD, and created two IAM accounts (**sub-user1a** and **sub-user1b**) on IAM using **domain1**. If you have authorized AAD permissions to **sub-user1b**, **sub-user1b** can use the AAD instances of **sub-user1a**.

  For details about AAD permission management, see **Creating a User and Granting the AAD Access Permission**.

4.4.7 What Is a CNAME Record?

A Canonical Name (CNAME) record is a type of DNS record that maps an alias name to a true or canonical domain name. A DNS A record maps a domain name to an IP address, whereas a CNAME record maps a domain name to another domain name (alias of that domain name). For example, the alias of **www.abc.com** is **ccd01c25c8535fa4.huaweisafedns.com**. When a user accesses **www.abc.com**, DNS obtains its alias **ccd01c25c8535fa4.huaweisafedns.com** and uses the alias to obtain the real IP address. The resolution is automatically completed by DNS.

4.4.8 What is BGP?

Border Gateway Protocol (BGP) is an inter-AS routing protocol. It was designed based on the experience gained from EGP, and is the only protocol that can run a network as large as the Internet and process many connections between unrelated routing domains. When purchasing Advanced Anti-DDoS, you can select BGP lines.

The BGP line is able to connect networks of different carriers smoothly, preventing the cross-network transmission problems.

This line package addresses the requirements for accessing the networks of CTCC, CUCC and other carriers (such as CMCC, CERNET, China Mobile Tietong, and Great

 Copyright © Huawei Technologies Co., Ltd.

Wall Broadband Network) and for defending against flooding attacks smaller than 200 Gbit/s. The maximum basic protection bandwidth is 20 Gbit/s, and the maximum elastic protection bandwidth is 200 Gbit/s.

4.4.9 What Is the Origin Server Port of AAD?

It is a port used by the origin server to provide services for external systems.

4.4.10 What Is the Origin Server IP Address?

It is the public IP address used by origin servers to provide services for external systems.

4.4.11 What Is the Website IP Address Protected by AAD?

The IP address used by AAD to provide protection is the high-defense IP address. The public IP address used by the origin server, namely, the origin server IP address, is protected by the AAD service. The high-defense IP address is used to provide services in place of the origin server IP address. The AAD service uses the high-defense IP address to proxy services for origin servers. All public network traffic is diverted to the high-defense IP address, and therefore user services on the origin servers are protected against DDoS attacks.

4.4.12 What Is Service Bandwidth?

The service bandwidth indicates clean service bandwidth forwarded to the origin server from the AAD scrubbing center. 100 Mbit/s service bandwidth is provided for each instance free of charge. You can pay for a quota increase. A maximum of 2 Gbit/s is supported. Packet losses may occur when the traffic exceeds the service bandwidth.

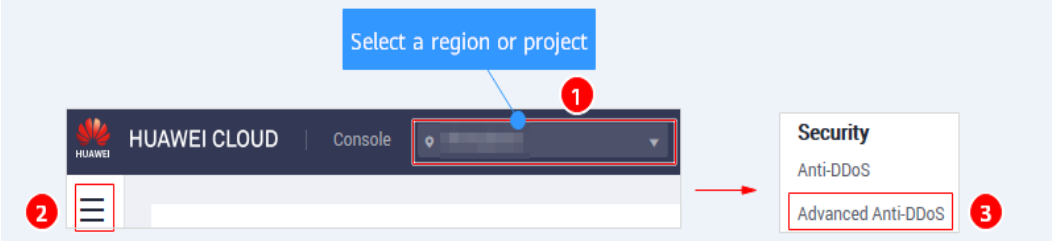
4.4.13 How Do I Access AAD?

You can use the management console to access AAD. If you have registered an account for logging in to the public cloud, perform the following operations to access AAD:

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

Step 2 Follow the procedure in the following figure to enter the **Advanced Anti-DDoS** console page.

Figure 4-16 AAD entry



----End

Copyright © Huawei Technologies Co., Ltd.

4.4.14 What Is an AAD Instance?

An AAD instance is one or multiple independently running Advanced Anti-DDoS services. Before using Advanced Anti-DDoS, you must purchase Advanced Anti-DDoS instances.

For details about how to purchase an AAD instance, see **Purchasing AAD Instances**.

4.4.15 What Is a Forwarding Protocol?

A forwarding protocol used by user's server to provide services for external systems can be Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

4.4.16 Are Services Interrupted When They Are Being Connected to AAD?

When services are connected to AAD, the DNS resolution needs to be changed and the service domain name is resolved to high defense IP address. To avoid the service interruption, you are advised to keep the origin server running till all domain names are resolved to the high-defense IP address. Then, you can bring the origin server offline.

4.4.17 Can I Use AAD If My Service Severs Are Deployed Outside Chinese Mainland?

AAD (Chinese Mainland) only provides protection for servers deployed in Chinese mainland. If your server is deployed outside the Chinese mainland, AAD (International) is recommended.

For details about how to purchase an AAD instance, see **Purchasing AAD Instances**.

4.4.18 Can AAD Provide Protection for Domain Names?

After domain names are added, you can configure protection policies for the domain names. For details about how to configure protection policies for protected domain names, see **Configuring Web Attack Protection**.

4.4.19 Can a Domain Name Be Bound to Multiple AAD Instances?

If an AAD instance to which a domain name has been bound is in use, the domain name cannot be bound to other AAD instances due to domain name conflict. Resolve the domain name to the origin server and unbind it from the AAD instance. Then, you can bind the domain name to other AAD instances.

4.4.20 Why Does the High-Defense IP Address Actually Receive Access Requests from a Client After AAD Is Deployed?

After you purchase the AAD service, the domain name of a web service is resolved into a high-defense IP address, and the service IP address of a non-web service is

 Copyright © Huawei Technologies Co., Ltd.

changed to a high-defense IP address. In this case, all access traffic is filtered by the high-defense IP address.

The high-defense IP address receives access requests from a client in place of origin server IP address, that is, the high-defense IP address is accessed by the client.

4.4.21 Why Does the Attack Traffic Volume Increase After AAD Is Deployed?

Some attackers may record the IP addresses used by exposed origin servers. Even after AAD is configured, the attackers will bypass AAD and directly launch attacks towards the known IP addresses. In this case, it is best practice to change the IP addresses of the origin servers.

4.4.22 Will the Origin Server Be Exposed When the Attack Traffic Volume Increases After AAD Is Deployed?

No. After you purchase the AAD service, the domain name of a web service is resolved into a high-defense IP address, and the service IP address of a non-web service is changed to a high-defense IP address. All public network traffic is diverted to the high-defense IP address, and therefore services on the origin servers are protected against DDoS attacks

4.4.23 How Does AAD Protect the Origin Server IP Address?

The AAD service uses the high-defense IP address to proxy services for origin servers. All public network traffic is diverted to the high-defense IP address, and therefore user services on the origin servers are protected against DDoS attacks.

4.4.24 What Information Can I Obtain in the CC Attack Protection Statistics?

You can obtain the information about the number of attacks and requests in the CC attack protection statistics. For details about how to view the CC attack protection statistics, see **Viewing CC Attack Protection Details**.

4.4.25 How Do I Obtain the AAD Sales License?

HUAWEI CLOUD provides sales licenses of Advanced Anti-DDoS. You can contact your customer manager or **submit a service ticket** to apply for a sales license.

4.4.26 Does AAD Support Two-Way SSL Authentication?

No.

4.4.27 Can I Modify or Delete the Certificates Uploaded to AAD?

For website services connected to AAD, if **Protocol/Port** is set to **HTTPS/WebSockets** and **Origin Server Type** is set to **IP address**, you need to upload a certificate.

 Copyright © Huawei Technologies Co., Ltd.

After the certificate is uploaded to AAD, you can go to the **Domain Name Access** page. Locate the row that contains the target domain name and click **Update** in the **Service Type** column.

The certificates uploaded to AAD cannot be deleted.

4.4.28 Does AAD Support Wildcard Domain Names?

Yes. When connecting website or non-website services to AAD by adding the domain names to be protected, you can configure a single domain name or a wildcard domain name based on your service requirements.

- Single domain name

  Configure a single domain name to be protected. for example, www.example.com.

- Wildcard domain name

  You can configure a wildcard domain name to let AAD protect multiple sub-domains of the wildcard domain name.

  - If the server IP address of each sub-domain is the same, configure a wildcard domain name. For example, if the subdomain names ***a.example.com***, ***b.example.com***, and ***c.example.com*** have the same server IP address, you can directly add the wildcard domain name ****.example.com*** to AAD for protection.
  - If each subdomain points to different server IP addresses, add each subdomain as a single domain name one by one.

For details about how to connect a service to AAD, see **Connecting a Website Service to AAD** and **Connecting a Non-website Service to AAD**.

4.4.29 What Will Happen If My Service Traffic Exceeds the Configured Service Bandwidth?

!00 Mbit/s service bandwidth is provided for free in each AAD instance. You can buy an up to 2 Gbit/s service bandwidth. If your service traffic exceeds the configured service bandwidth of the purchased AAD instance, rate limiting is triggered, which may result in packet loss.

4.4.30 Does Advanced Anti-DDoS Implement Load Balancing?

Load balancing is achieved through access traffic distribution. It expands service capabilities of your applications and improves their availability by eliminating single points of failure (SPOFs). AAD does not implement load balancing. AAD offers high-defense IP addresses to provide services in place of the original server IP addresses for external systems. The malicious attacks targeting the origin servers can be diverted for scrubbing to ensure the stable running of mission-critical workloads.

For services requiring DDoS mitigation and load balancing, you can configure an elastic load balancer and connect the elastic IP address bound to the load balancer to AAD.

- For details about Elastic Load Balance, see **What Is Elastic Load Balance?**.

 Copyright © Huawei Technologies Co., Ltd.

- For details about how to connect your services to AAD, see **Connecting a Website Service to AAD**.

4.4.31 Is Advanced Anti-DDoS Software or Hardware?

AAD, a software DDoS mitigation service, provides instantaneous protection once you connect your services to AAD. You can view DDoS attack protection details on its dashboard to learn about the network security state.

Compared with the traditional hardware DDoS mitigation service, AAD has the following advantages:

- **Immense defense capability**

  One high-defense IP address is able to defend against 600 Gbit/s network-, and application-layer DDoS attacks. The AAD service offers more than 5 Tbit/s defense capability.
- **Highly available**

  Automated attack detection and adaptive defense policies support real-time protection. Service traffic is distributed in clusters, which features high performance, low latency, and high stability.
- **Flexible protection**

  You can buy both the basic bandwidth protection and elastic bandwidth protection of AAD for a higher protection capability. The protection bandwidth can be adjusted depending on your needs.

4.5 Fees

4.5.1 Is the AAD Service Free of Charge?

Advanced Anti-DDoS is a paid service and can be used only after you purchase Advanced Anti-DDoS instances. For more about the AAD pricing details, see **Pricing Details**.

4.5.2 How Is AAD Billed?

Pricing

To use AAD, you need to purchase AAD instances. For pricing details, see **Product Pricing Details**.

Billing Mode

AAD instances are charged by the service bandwidth, basic protection bandwidth, and elastic protection bandwidth you configure.

Copyright © Huawei Technologies Co., Ltd.

Table 4-2 Billing items

Billing Item	Billing Modes	Pricing details
Service Bandwidth	Prepaid by month or year	Service bandwidth for the AAD server room to forward scrubbed traffic to origin servers. **NOTE** If the AAD server room is outside HUAWEI CLOUD, it is recommended that the service bandwidth be greater than or equal to the egress bandwidth of the origin servers.
Basic Protection Bandwidth	Prepaid by month or year	Basic bandwidth for defending against attacks. Traffic that does not exceed this bandwidth will be scrubbed by AAD without incurring additional fees. **NOTE** The price of the basic protection bandwidth varies depending on the line package. For details, see **Product Pricing Details**.
Elastic Protection Bandwidth	Postpaid by day	Maximum available bandwidth for defending against attacks. Billable bandwidth equals to attack traffic peak on a day minus the purchased basic protection bandwidth. • If you set the elastic protection bandwidth to a value greater than the basic protection bandwidth, you will need to pay additional fees for scrubbing the attack traffic exceeding the basic protection bandwidth. • If the peak attack traffic exceeds the elastic protection bandwidth, you only need to pay for the selected elastic protection bandwidth. **NOTE** • If the peak attack traffic exceeds your selected elastic protection bandwidth, the high-defense IP address will be blocked by a black hole and cannot provide services for you. • High-defense IP addresses are charged separately. • The price varies depending on the line. For details, see **Product Pricing Details**.

Billing details for elastic protection bandwidth:

- Billing standard: It depends on the peak attack traffic on the day. If multiple attacks occur on a day, only the attack with the peak traffic counts.
- Postpaid: Elastic protection fees are generated based on the attack traffic peak. If there is no attack, no elastic protection fee is generated.
- Specifications adjustment: You can adjust the elastic protection bandwidth on the AAD console. Once adjusted, the new elastic protection bandwidth takes effect immediately.
- Free-to-use: If the elastic protection bandwidth is set to the same value as the basic protection bandwidth, you do not need to pay for elastic protection.

 Copyright © Huawei Technologies Co., Ltd.

4.5.3 What Is the Impact on AAD If Your Account Balance Is in Arrears?

Three days before the expiration of the AAD service, you will receive an SMS or email notifying you of the expiration and renewal.

Expiration

The AAD service will stop protection when your purchased AAD instances expire. Resolve the domain name bound to the AAD instance to the origin server.

Expiration Configuration

When a purchased instance is about to expire, you need to renew the subscription or top up the account within the retention period. If you do not renew the subscription or top up the account within this period, the data stored in the cloud service will be deleted and the cloud service resources will be released. For details, see **Grace Period and Retention Period**.

4.5.4 Why Does My Payment Status Not Update After I Make a Payment?

If you have not received any payment information after making a payment, and the payment status on the platform is not updated, the possible causes may be as follows:

- Check whether the recharge number is correct in the transaction record.
- The payment SMS message sent by the carrier is delayed. Contact the carrier or Huawei customer service to query the payment status.

4.5.5 Will I Be Charged If I Buy an Elastic Protection Bandwidth and My Elastic IP Address Is Not Attacked for the Whole Month?

Yes, you will be charged for the basic protection bandwidth only.

4.5.6 What Happens If the Attack Traffic Exceeds the Elastic Protection Bandwidth?

A black hole will be triggered, which means access traffic to the IP address will be blocked.

4.5.7 Can I Adjust My Elastic Protection Bandwidth From 100 Gbit/s to 200 Gbit/s When I Find 100 Gbit/s Is Insufficient?

Yes. AAD supports dynamic adjustment of elastic protection bandwidth.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

Adjusted bandwidth takes effect immediately. The charge depends on the peak attack traffic of the day.

4.5.8 What Is the Charge If My IP Address Is Attacked Many Times a Day?

You will be charged only once based on the peak attack traffic of the day (0:00 to 23:00). For example, if your IP address is attacked three times and the attack traffic is 50 Gbit/s, 100 Gbit/s, and 200 Gbit/s, you will be charged based on 200 Gbit/s.

4.5.9 How Will I Be Charged If I Have Purchased the CTCC & CUCC & CMCC Line and Both My CTCC, CUCC, and CMCC IP Addresses Are Attacked?

You will be charged by IP address instead of AAD instance. Therefore, you will be charged on the elastic protection bandwidths depending on the maximum attack traffic of the IP addresses.

4.5.10 How Do I Stop Elastic Protection to Avoid Being Charged for the Elastic Protection Bandwidth?

Set the elastic protection bandwidth to the same value as the basic protection bandwidth.

4.5.11 How Can I Renew the AAD service?

You can renew an AAD instance on the AAD management console.

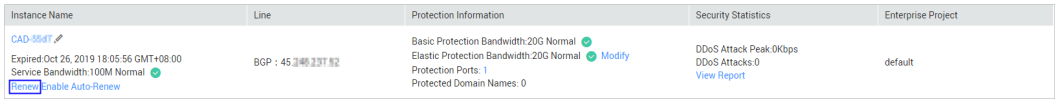
NOTICE

Ensure that the account used for renewing the AAD instance has both the CAD Administrator and BSS Administrator roles or has the Tenant Administrator role.

- **BSS Administrator**: has all permissions on account center, billing center, and resource center. It is a project-level role, which must be assigned in the same project.
- **Tenant Administrator**: has all permissions on all services except on IAM.

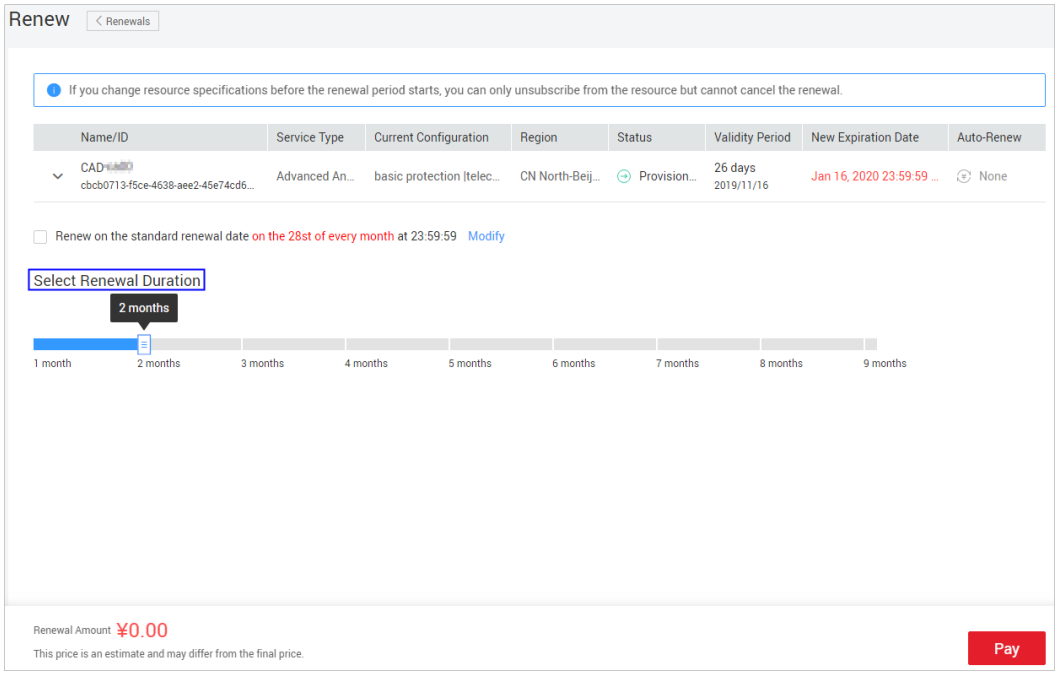
Step 1 Log in to the management console.

Step 2 Under **Security**, choose **Advanced Anti-DDoS**. The **Security Console** is displayed. In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Instance List**. On the **Instance List** page, click **Renew** in the **Instance Name** column.



 Copyright © Huawei Technologies Co., Ltd.

Step 3 On the **Renew** page, select a renewal duration and click **Pay** to complete the payment.



----End

4.5.12 How Can I Unsubscribe from the AAD Service?

The AAD service does not support unconditional unsubscription. If the unsubscription conditions are met, contact the customer service to apply for unsubscription

Unsubscription Conditions

If the service does not match your business requirements during your purchase or use, contact the customer service personnel to unsubscribe from the service. For example, if your servers are deployed outside China but you have purchased the AAD service from the Chinese Mainland region, the AAD service cannot be used and in this case you can apply for service cancellation.

An AAD instance that has been put to use does not allow cancellation.

4.5.13 How Should I Automatically Renew AAD?

You can enable auto renewal for your AAD instance. The system automatically renews your service subscription according to the required duration specified in your previous purchase upon expiration of the service.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

Ensure that the account for which the automatic renewal is to be enabled has both the CAD Administrator and BSS Administrator roles or has the Tenant Administrator role.

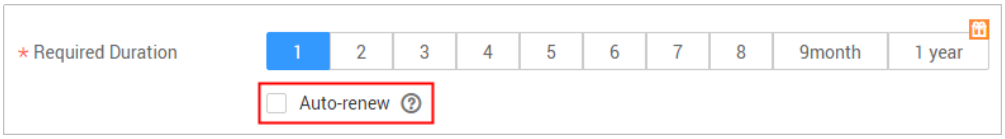
- **BSS Administrator**: has all permissions on account center, billing center, and resource center. It is a project-level role, which must be assigned in the same project.
- **Tenant Administrator**: has all permissions on all services except on IAM.

If you are currently purchasing AAD, you can enable the auto renewal function as follows:

1. When purchasing AAD, you can tick the **Auto-renew** option to configure automatic renewal.

   The procedure is as follows:

   Choose **Buy AAD** > **Required Duration** > **Auto-renew**.



If you have purchased AAD, you can enable the auto renewal function as follows:

1. Go to the **Renewals** page, configure automatic renewal.

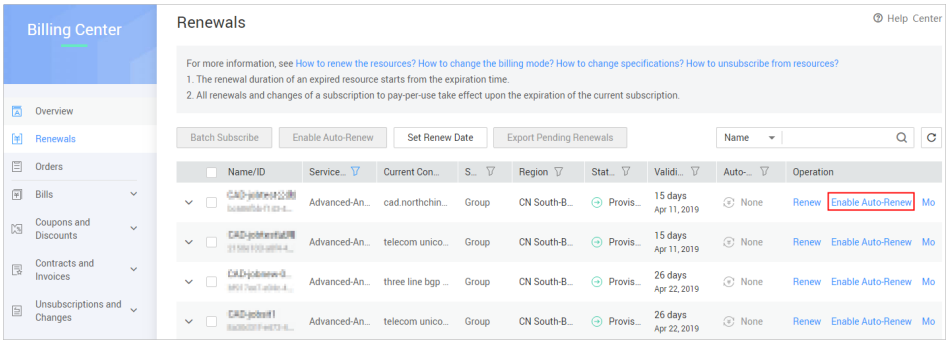
   The procedure is as follows:

   a. Log in to the management console and click **Fees** at the top right.

      The **Billing Center** page is displayed.

   b. In the navigation pane on the left, choose **Renewals**.

   c. Select the corresponding AAD instance for automatic renewal.



4.5.14 Will an Expired AAD Instance Incur Fees?

The auto-renew of AAD is disabled by default. If you do not manually enable it again, no extra fee will be generated.

For details about how to enable the auto-renew function, see **How Should I Automatically Renew AAD?**.

 Copyright © Huawei Technologies Co., Ltd.

4.5.15 What Can I Do When I Receive an Arrears Notification?

When the peak attack traffic of a DDoS attack has exceeded the basic protection bandwidth, fees are about to be charged on elastic protection bandwidth and you will receive SMS messages or emails in the next morning.

When receiving this notification and you do not want to be charged, you can set the elastic protection bandwidth to be the same as the basic protection bandwidth. This setting disables the elastic protection function but prevents possible postpaid fees.

NOTE

The notification function needs to be enabled manually. For details, see **Configuring Alarm Notification**.

4.5.16 What Is the Peak Attack Traffic in AAD Pricing?

Peak attack traffic refers to the peak traffic launched by attackers on AAD. For details about pricing rules, see **How Is AAD Billed?**.

4.5.17 Can the Original Configuration Data Be Saved After I Unsubscribe from an AAD Instance?

No. After you unsubscribe from an AAD instance, it will not keep your original configuration data. Therefore, you need to connect your services to the newly-purchased AAD instance.

- For details about unsubscription, see **How Can I Unsubscribe from the AAD Service?**.
- For details about how to connect services to AAD, see **How Do I Connect My Service System to AAD?**.

Copyright © Huawei Technologies Co., Ltd.