DDoS Mitigation

User Guide

Issue 09

Date 2021-04-29



HUAWEI

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 CNAD Basic (Anti-DDoS) User Guide....1
1.1 Setting a Default Protection Policy for Newly Purchased Public IP Addresses....1
1.2 Viewing a Public IP Address....5
1.3 Enabling Alarm Notification....7
1.4 Configuring an Anti-DDoS Protection Policy....9
1.5 Viewing a Monitoring Report....13
1.6 Viewing an Interception Report....15
1.7 Audit....17
1.7.1 Anti-DDoS Operations That Can Be Recorded by CTS....17
1.7.2 Viewing CTS Traces....17
1.8 Permission Management....18
1.8.1 Creating a User Group and Assigning the Anti-DDoS Access Permission....18
2 Permissions Management....20
2.1 Creating a User and Granting the CNAD Pro Access Permission....20
2.2 CNAD Pro Custom Policies....21
2.3 CNAD Pro Permissions and Actions....22
3 Advanced Anti-DDoS User Guide....27
3.1 Enabling the AAD Service....27
3.1.1 Purchasing AAD Instances....27
3.1.2 Line Packages....31
3.1.3 Upgrading Specifications....35
3.2 Connecting a Website Service to AAD....36
3.3 Connecting a Non-website Service to AAD....46
3.4 Configuring a Forwarding Rule....52
3.5 Configuring a Protection Policy....55
3.5.1 Configuring a Blacklist and a Whitelist....55
3.5.2 Configuring Traffic Control....57
3.5.3 Configuring CC Attack Protection Rules....59
3.6 Adding a CNAME Record....65
3.7 Viewing Protection Details....69
3.8 Enabling Alarm Notification....72
3.9 Managing an Instance....74

 Copyright © Huawei Technologies Co., Ltd.

3.9.1 Viewing AAD Instance Information....74
3.9.2 Changing the Name of an AAD Instance....75
3.9.3 Changing the Elastic Protection Bandwidth....76
3.10 Managing a Forwarding Rule....77
3.10.1 Viewing Information About a Forwarding Rule....77
3.10.2 Changing an Origin Server IP Address....79
3.10.3 Deleting a Forwarding Rule....79
3.10.4 Exporting a Forwarding Rule....80
3.11 Managing a Domain Name....81
3.11.1 Viewing Information About a Domain Name....81
3.11.2 Enabling Basic Web Protection and CC Attack Protection....83
3.11.3 Updating a Certificate....84
3.11.4 Modifying Resolution Lines for High-Defense IP Addresses of a Domain Name....88
3.11.5 Modifying Domain Name Configuration....89
3.11.6 Deleting a Domain Name....90
3.12 Viewing a Back-to-Origin IP Address Range....91
3.13 Viewing a Protection Report....92
3.14 Permissions Management....94
3.14.1 Creating a User and Granting the AAD Access Permission....94

 Copyright © Huawei Technologies Co., Ltd.

1 CNAD Basic (Anti-DDoS) User Guide

1.1 Setting a Default Protection Policy for Newly Purchased Public IP Addresses

In the **Set Default Protection Policy** dialog box, you can select **Manual** for **Protection Settings** and set the default protection policy. The new public IP addresses you purchase from HUAWEI CLOUD will be protected against DDoS attacks based on your configured default protection policy

If you want to disable the default protection policy, you can select **Default** for **Protection Settings** in the **Set Default Protection Policy** dialog box.

If you do not set a default protection policy for the newly purchased public IP addresses, the **Protection Settings** in **Default** mode apply to the IP addresses. The value of **Traffic Cleaning Threshold** is **120 Mbps** and **CC Defense** is disabled if you select **Default** for **Protection Settings** in the **Set Default Protection Policy** dialog box.

Prerequisites

You have obtained an account and its password for logging in to the management console.

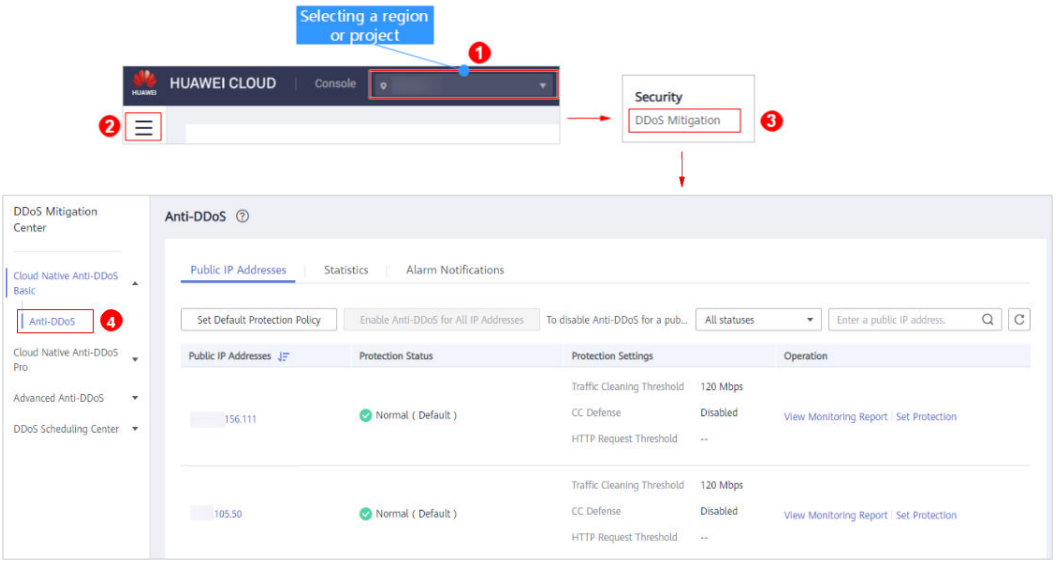
Manually Setting a Default Protection Policy

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

Step 2 Go to the Anti-DDoS console.

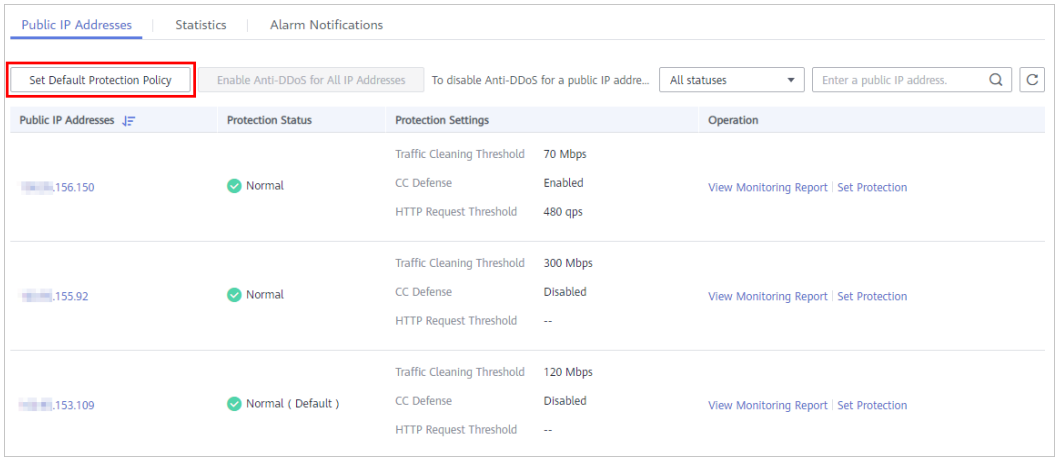
 Copyright © Huawei Technologies Co., Ltd.

Figure 1-1 Anti-DDoS console



Step 3 Select the **Public IP Addresses** tab and click **Set Default Protection Policy**.

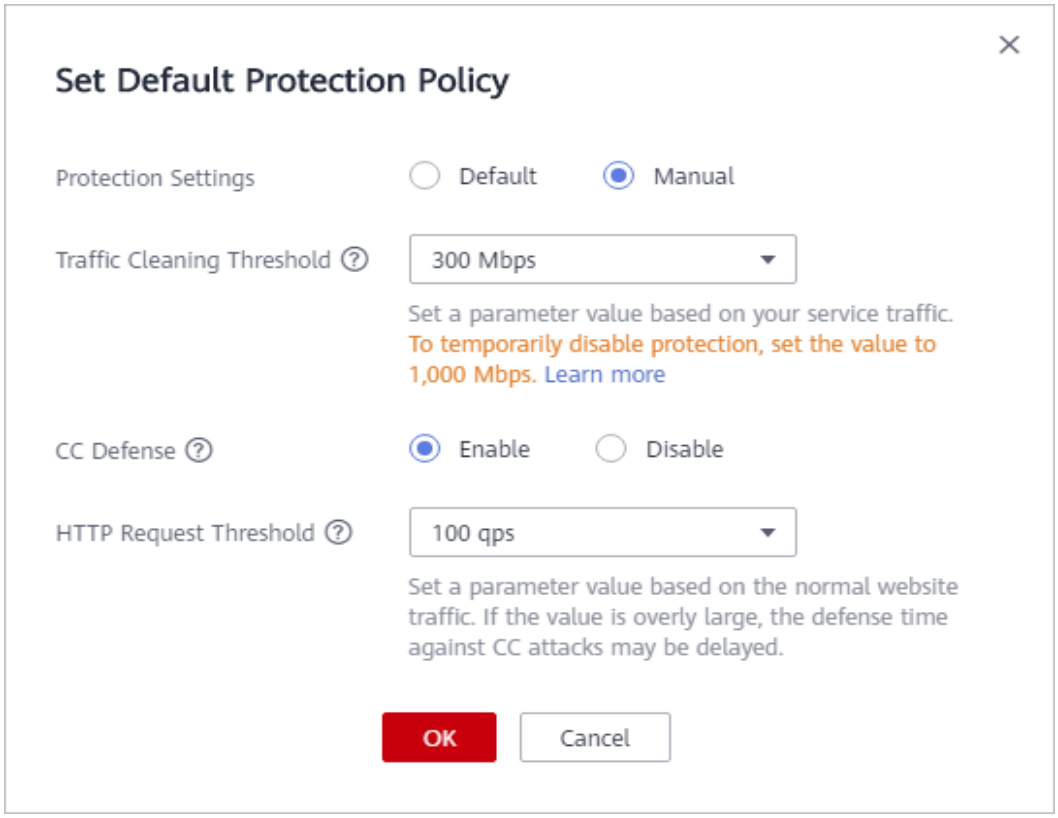
Figure 1-2 Setting a default protection policy for newly purchased public IP addresses



Step 4 In the displayed dialog box, select **Manual** for **Protection Settings**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-3 Manually configuring the default protection policy



Step 5 Configure **Traffic Cleaning Threshold** and **CC Defense**.

Table 1-1 Parameter description

Parameter	Description
Traffic Cleaning Threshold	Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the threshold. You can set the traffic cleaning threshold based on your service traffic. Set the threshold to a value closest to the purchased bandwidth but not greater than the purchased bandwidth. **NOTE** If service traffic triggers scrubbing, only attack traffic is intercepted. If service traffic does not trigger scrubbing, no traffic is intercepted. Set this parameter based on the actual service access traffic.
CC Defense	• **Disable**: disables the defense. • **Enable**: enables the defense. **NOTE** CC defense is available only for clients that carry web services and support the full HTTP protocol stack. CC defense works in redirection or redirection+verification code mode. If your client does not support the full HTTP protocol stack, you are advised to disable CC defense.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
HTTP Request Threshold	This parameter is required only when **CC Defense** is set to **Enable**. This parameter is used to defend against a large number of malicious requests targeting websites. Defense against CC attacks, which aim to exhaust server resources by sending specially crafted GET or POST requests, is triggered when the HTTP request rate on a site reaches the selected value. In EIP protection, the maximum recommended value is **5000**. In ELB protection, the value can be larger. Set this parameter to the maximum number of HTTP requests that can be processed by the deployed service. Anti-DDoS will automatically scrub traffic if detecting that the total number of requests exceeds the configured HTTP request threshold. If the value is too large, CC defense will not be triggered promptly.

Step 6 Click **OK**.

After you set the default protection policy, the newly purchased public IP addresses are protected based on the configured policy. For details about how to adjust a configured protection policy, see **Configuring an Anti-DDoS Protection Policy**.

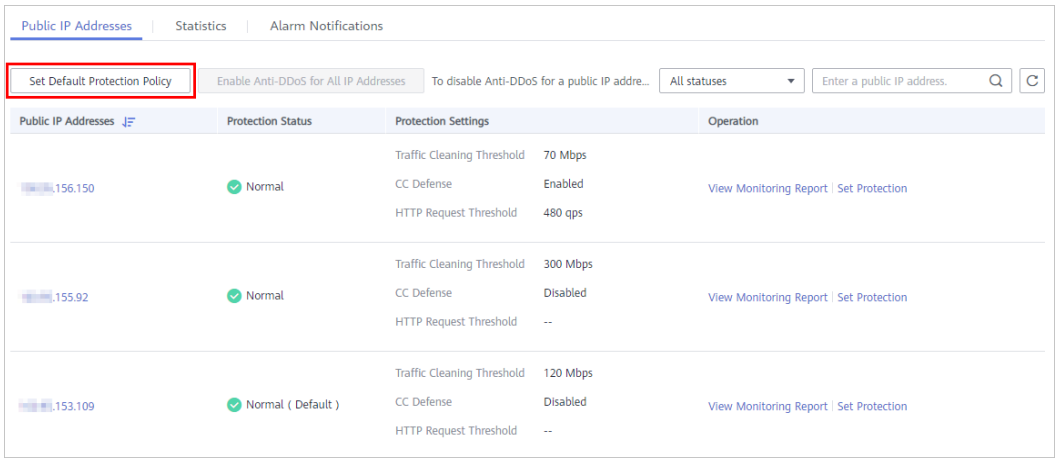
----End

Disabling the Default Protection Policy Manually Configured for Newly Purchased IP Addresses

If you do not want the manually configured protection policy to apply to the new public IP addresses, you can disable it. Then, the **Protection Settings** in **Default** mode apply to the new IP addresses.

Step 1 Select the **Public IP Addresses** tab and click **Set Default Protection Policy**.

Figure 1-4 Setting a default protection policy for newly purchased public IP addresses

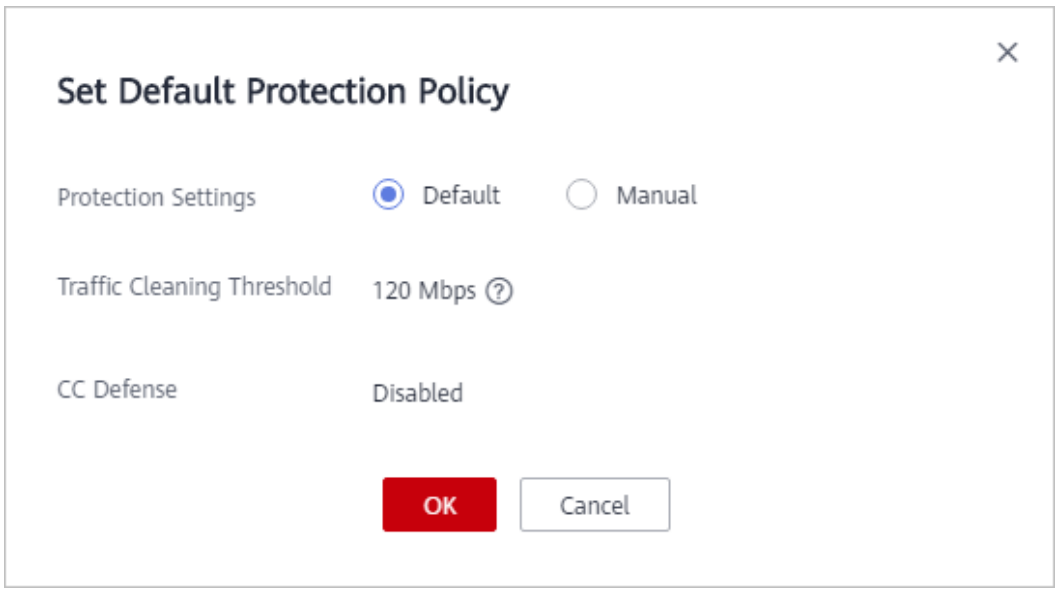


 Copyright © Huawei Technologies Co., Ltd.

Step 2 Select **Default** for **Protection Settings** in the **Set Default Protection Policy** dialog box.

The value of **Traffic Cleaning Threshold** is **120 Mbps** and **CC Defense** is disabled.

Figure 1-5 Disabling the default protection policy manually configured for newly purchased IP addresses



Step 3 Click **OK**.

The **Protection Settings** in **Default** mode will apply to the new public IP addresses.

----End

1.2 Viewing a Public IP Address

Scenarios

This topic describes how to view a public IP address.

NOTICE

- After you purchase a public IP address, Anti-DDoS automatically enables the protection by default, and protects your public IP address against DDoS attacks.
- You are not allowed to disable Anti-DDoS after it has been enabled.

Prerequisites

- You have obtained a username and password for logging in to the management console.
- You have purchased at least one public IP address.

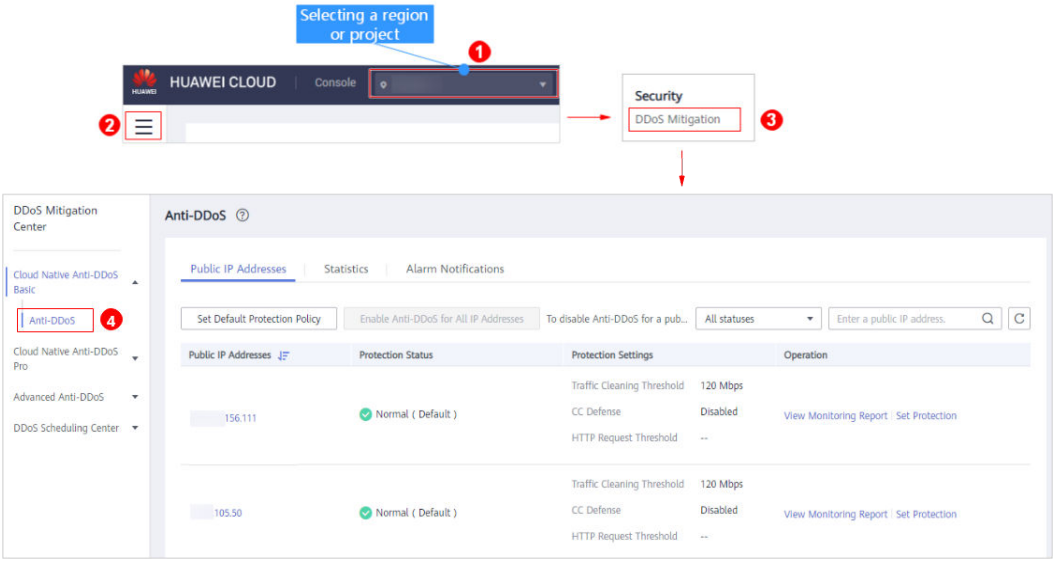
Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the management console.

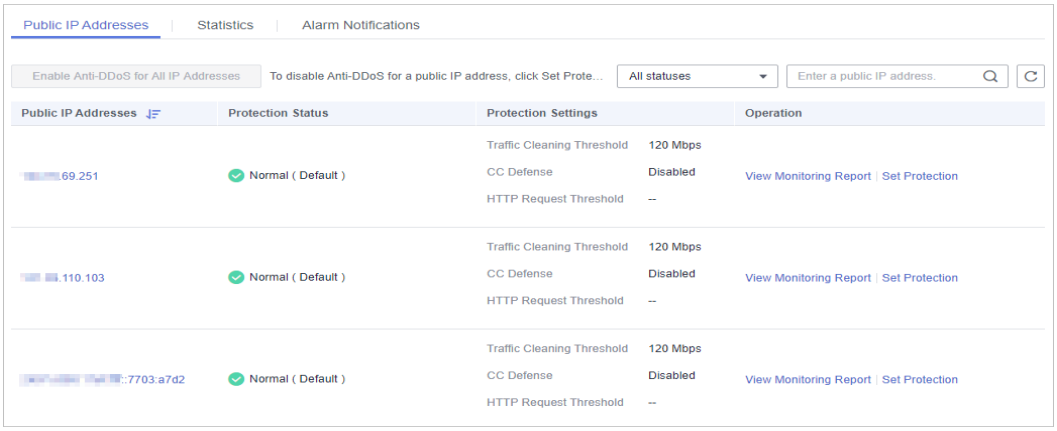
Step 2 Go to the Anti-DDoS console.

Figure 1-6 Anti-DDoS console



Step 3 On the **Public IP Addresses** tab, view all protected public IP addresses. Table 1-2 describes the parameters.

Figure 1-7 Viewing a public IP address



 Copyright © Huawei Technologies Co., Ltd.

NOTE

- Anti-DDoS provides protection for servers using IPv4 and IPv6 protocols against DDoS attacks.
- Click **Enable Anti-DDoS for All IP Addresses** to enable the protection for all unprotected IP addresses in the current region.
- After the default Anti-DDoS protection settings are enabled, traffic is scrubbed when its volume reaches 120 Mbit/s. You can modify Anti-DDoS protection settings according to **Configuring an Anti-DDoS Protection Policy**.
- 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.
- The **All statuses** drop-down box enables you to specify a status so that only public IP addresses of the selected status are displayed.
- Enter a public IP address or a keyword of a public IP address in the search box and click or to search for the desired public IP address.

Table 1-2 Parameter description

Parameter	Description
Public IP Address	Public IP address protected by Anti-DDoS **NOTE** If Anti-DDoS is enabled for a public IP address, you can click the IP address to go to its **Monitoring Report** page.
Protection Status	Protection status of a public IP address. The values are: • **Normal** • **Configuring** • **Disabled** • **Cleaning** • **Black hole**

----End

1.3 Enabling Alarm Notification

Scenarios

The alarm notification function sends you alarm notifications (by SMS or email) if a DDoS attack is detected. If you do not enable this function, you have to log in to the management console to view alarms.

Prerequisites

- You have obtained a username and password for logging in to the management console.

Copyright © Huawei Technologies Co., Ltd.

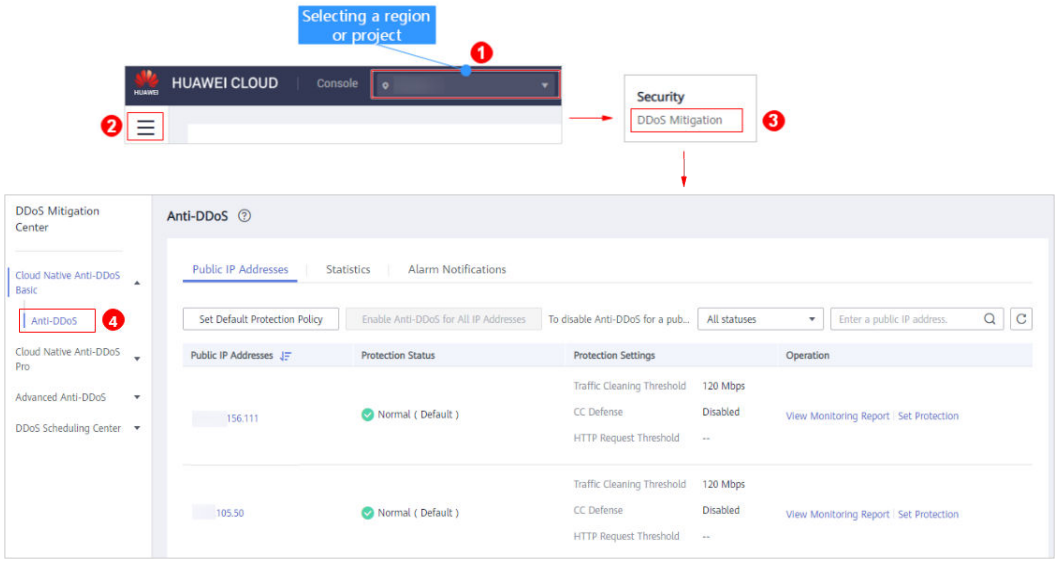
- You have purchased at least one public IP address.

Procedure

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

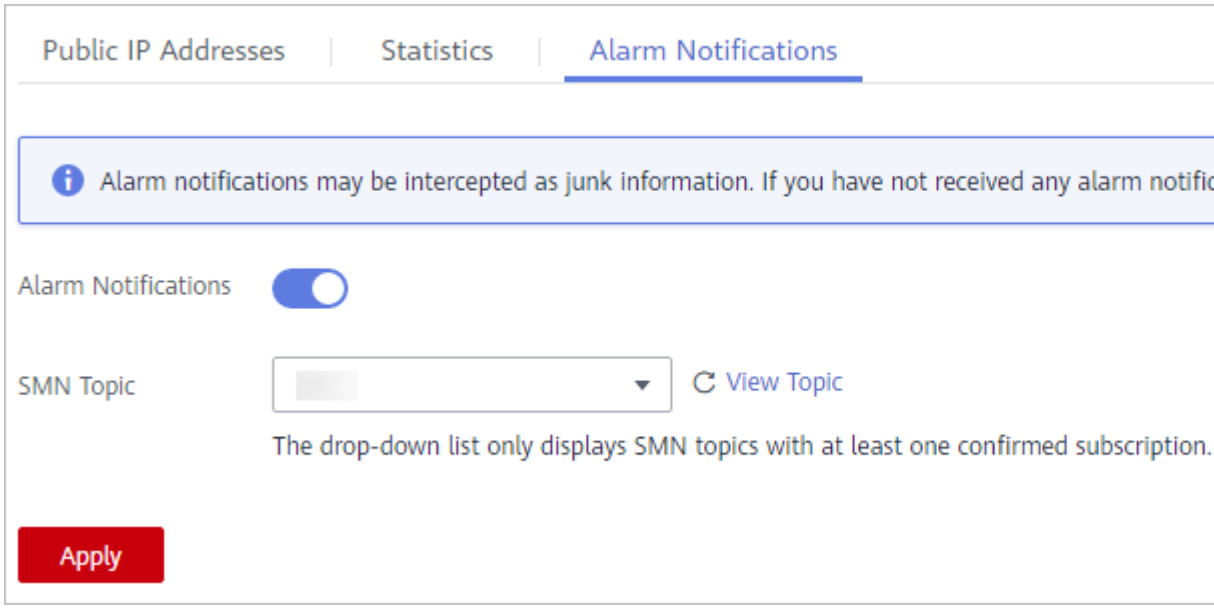
Step 2 Go to the Anti-DDoS console.

Figure 1-8 Anti-DDoS console



Step 3 On the **Anti-DDoS** page, click the **Alarm Notifications** tab and configure the alarm notification. For details about the parameter settings, see **Figure 1-9**.

Figure 1-9 Configuring alarm notifications



 Copyright © Huawei Technologies Co., Ltd.

Table 1-3 Configuring alarm notifications

Parameter	Description	Example Value
Alarm Notifications	Indicates whether the alarm notification function is enabled. There are two values: • : enabled • : disabled If the function is in the disabled state, click  to set it to .	
SMN Topic	You can select an existing topic or click **View Topic** to create a topic. For more about SMN topics, see **Simple Message Notification User Guide**.	N/A

Step 4 Click **Apply** to enable alarm notification.

----End

1.4 Configuring an Anti-DDoS Protection Policy

Scenarios

You can adjust your Anti-DDoS protection policy after Anti-DDoS is enabled.

Prerequisites

You have obtained a username and password for logging in to the management console.

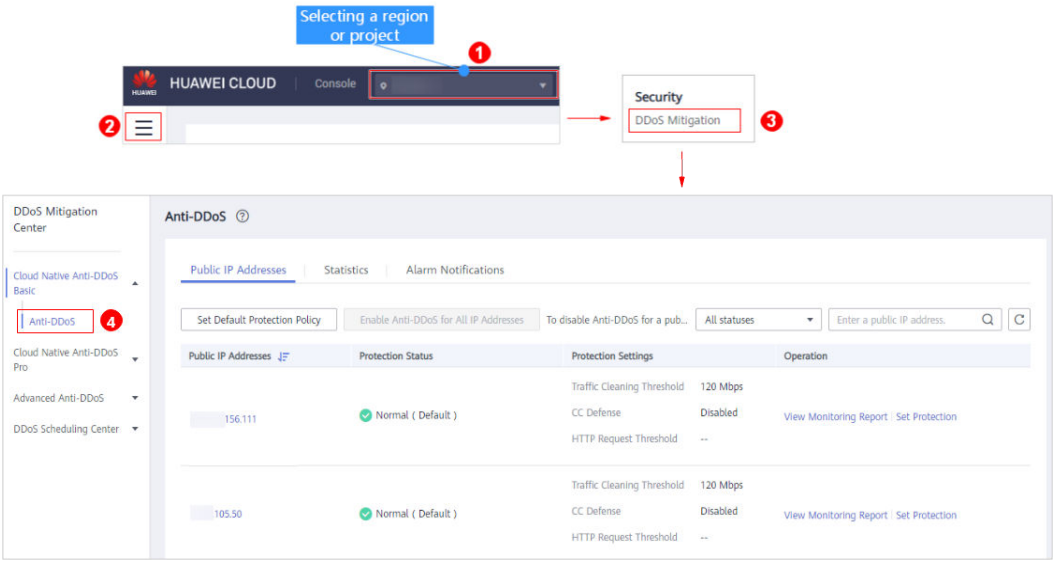
Procedure

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

Step 2 Go to the Anti-DDoS console.

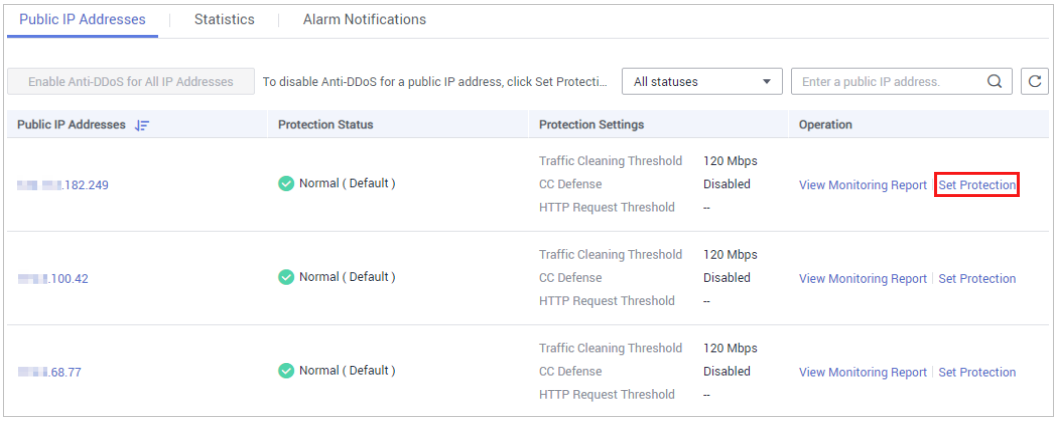
 Copyright © Huawei Technologies Co., Ltd.

Figure 1-10 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 1-11 Protection settings



Step 4 In the **Set Protection** dialog box, modify desired parameters. **Figure 1-12** describes the parameters.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-12 Configuring a protection policy

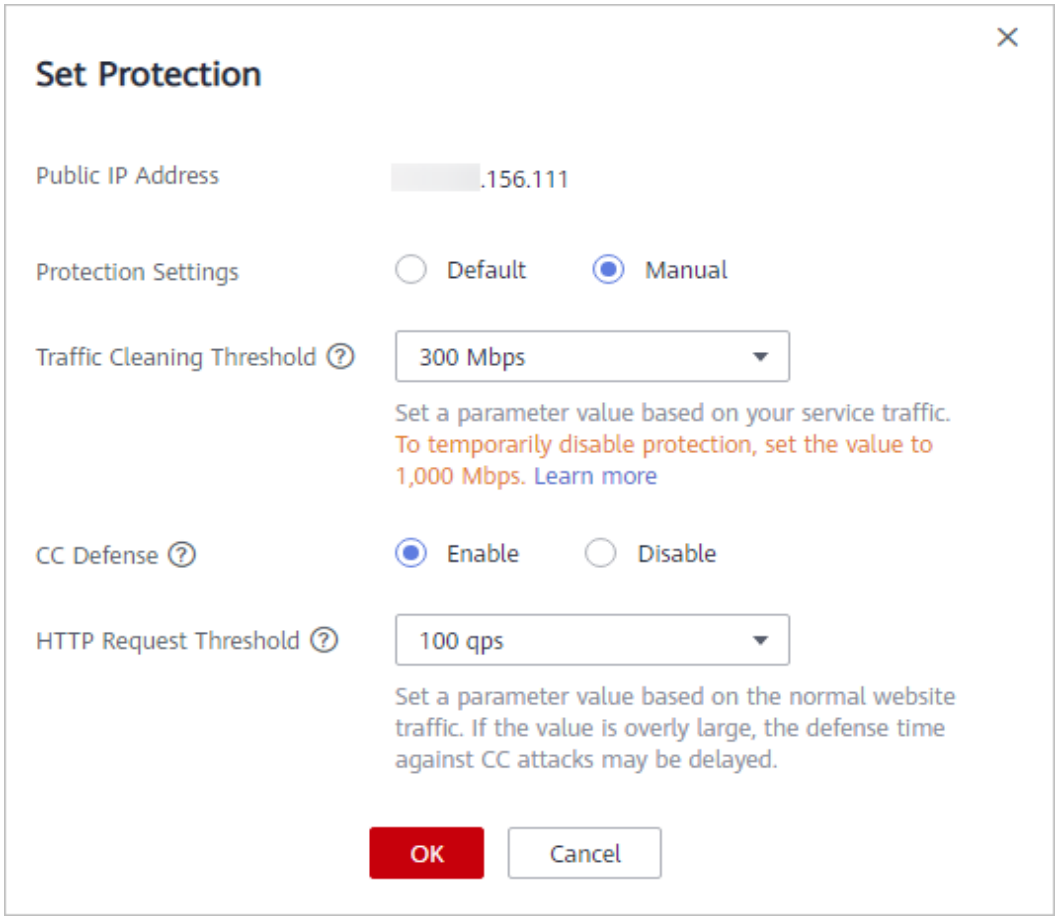


Table 1-4 Parameter description

Parameter	Description
Protection Settings	• **Default**: In this mode, **Traffic Cleaning Threshold** is fixed at **120 Mbps**. When the service UDP traffic is greater than 120 Mbps or the TCP traffic is greater than 35,000 pps, traffic scrubbing is triggered and Anti-DDoS will automatically intercept the attack traffic. • **Manual**: In this mode, you can set the value of **Traffic Cleaning Threshold** based on your service needs and enable **CC Defense**. **NOTE** • Mbps = Mbit/s (short for 1,000,000 bit/s). It is a unit of transmission rate and refers to the number of bits transmitted per second. • PPS, short for Packets Per Second, is a measure of throughput for network devices. It means the number of packets sent per second.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Traffic Cleaning Threshold	Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the threshold. • When **Protection Settings** is set to **Default**, the value of **Traffic Cleaning Threshold** is **120 Mbps** by default. • When **Protection Settings** is set to **Manual**, the value of **Traffic Cleaning Threshold** can be set based on your service needs. You are advised to set the threshold to a value closest to the purchased bandwidth but not greater than the purchased bandwidth. **NOTE** If service traffic triggers scrubbing, only attack traffic is intercepted. If service traffic does not trigger scrubbing, no traffic is intercepted. Set this parameter based on the actual service access traffic. You are advised to set a value closest to, but not exceeding, the purchased bandwidth.
CC Defense	• **Disable**: disables the defense. • **Enable**: enables the defense. **NOTE** Challenge Collapsar (CC) defense is available only for clients supporting the full HTTP protocol stack because CC defense works in redirection or redirection+verification code mode. If your client does not support the full HTTP protocol stack, you are advised to disable CC defense.
HTTP Request Threshold	This parameter is required only when **CC Defense** is set to **Enable**. The unit is qps (short for queries per second). QPS is a common measure of the amount of search traffic an information retrieval system, such as a search engine or a database, receives during one second. This parameter is used to defend against a large number of malicious requests targeting websites. Defense against CC attacks, which aim to exhaust server resources by sending specially crafted GET or POST requests, is triggered when the HTTP request rate on a site reaches the selected value. In the EIP address protection, the maximum recommended value is **5000**. In ELB protection, the value can be larger. You are advised to set this parameter to the maximum number of HTTP requests that can be processed by the deployed service. Anti-DDoS will automatically scrub traffic if detecting that the total number of requests exceeds the configured HTTP request threshold. If the value is too large, CC defense will not be triggered promptly. • If the actual HTTP request rate is smaller than the configured value, the deployed service is able to process all HTTP requests, and Anti-DDoS does not need to be involved. • If the actual HTTP request rate 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.

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Click **OK** to save the settings.

----End

1.5 Viewing a Monitoring Report

Scenarios

This section describes how to view the monitoring report of a public IP address. This report includes the protection status, protection settings, and the last 24 hours' traffic and anomalies.

Prerequisites

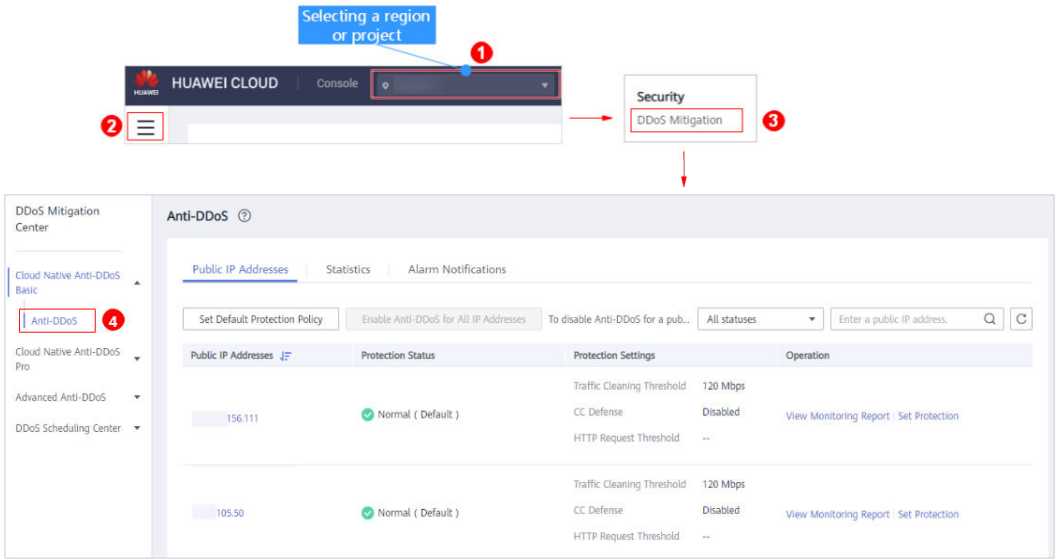
You have obtained a username and password for logging in to the management console.

Procedure

Step 1 Log in to the management console.

Step 2 Go to the Anti-DDoS console.

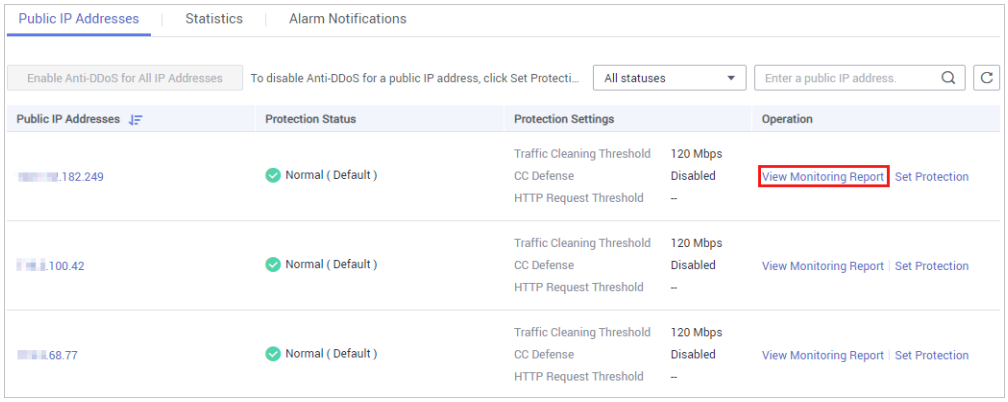
Figure 1-13 Anti-DDoS console



Step 3 Click the **Public IP Addresses** tab, locate the row that contains the IP address of which you want to view its monitoring report, and click **View Monitoring Report**.

Copyright © Huawei Technologies Co., Ltd.

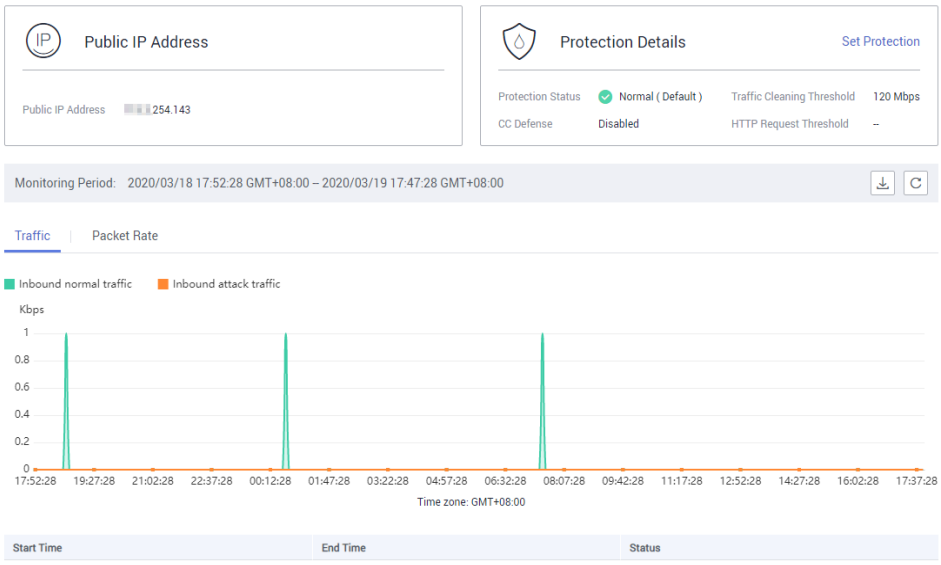
Figure 1-14 Viewing a monitoring report



Step 4 On the **Monitoring Report** page, view monitoring details about the public IP address.

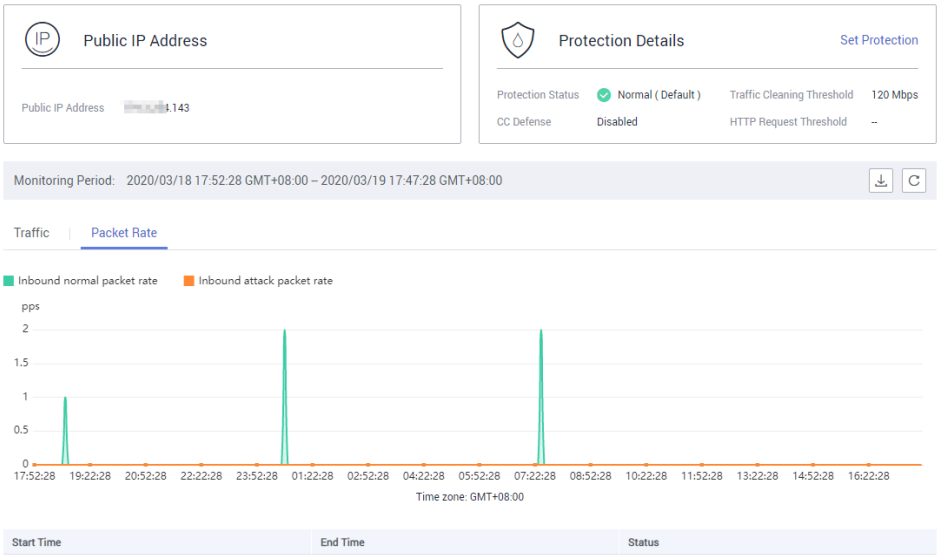
- You can view information such as the current defense status, current defense configurations, traffic within 24 hours, and abnormalities within 24 hours.
- A 24-hour defense traffic chart is generated from data points taken in five-minute intervals. It includes the following information:
  - **Traffic** displays the traffic status of the selected ECS, including the incoming attack traffic and normal traffic.
  - **Packet Rate** displays the packet rate of the selected ECS, including the attack packet rate and normal incoming packet rate.
- The attack event list within one day records DDoS attacks on the ECS within one day, including cleaning events and black hole events.

Figure 1-15 Viewing a traffic monitoring report



 Copyright © Huawei Technologies Co., Ltd.

Figure 1-16 Viewing a packet rate monitoring report



NOTE

- Click to download monitoring reports to view monitoring details about the public IP address.
- On the traffic monitoring report page, click Inbound attack traffic or Inbound normal traffic to view details about the **Inbound attack traffic** or **Inbound normal traffic.**
- On the packet rate monitoring report page, click Inbound attack packet rate or Inbound normal packet rate to view details about the **Inbound attack packet rate** and **Inbound normal packet rate**.

----End

1.6 Viewing an Interception Report

Scenarios

This section describes how to view the 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.

Prerequisites

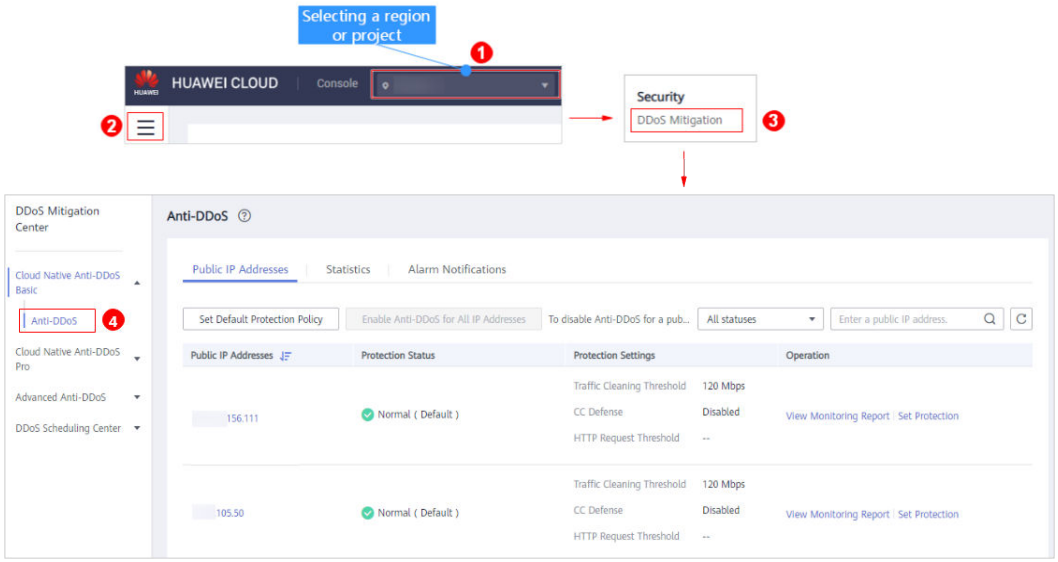
You have obtained a username and password for logging in to the management console.

Procedure

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

Step 2 Go to the Anti-DDoS console.

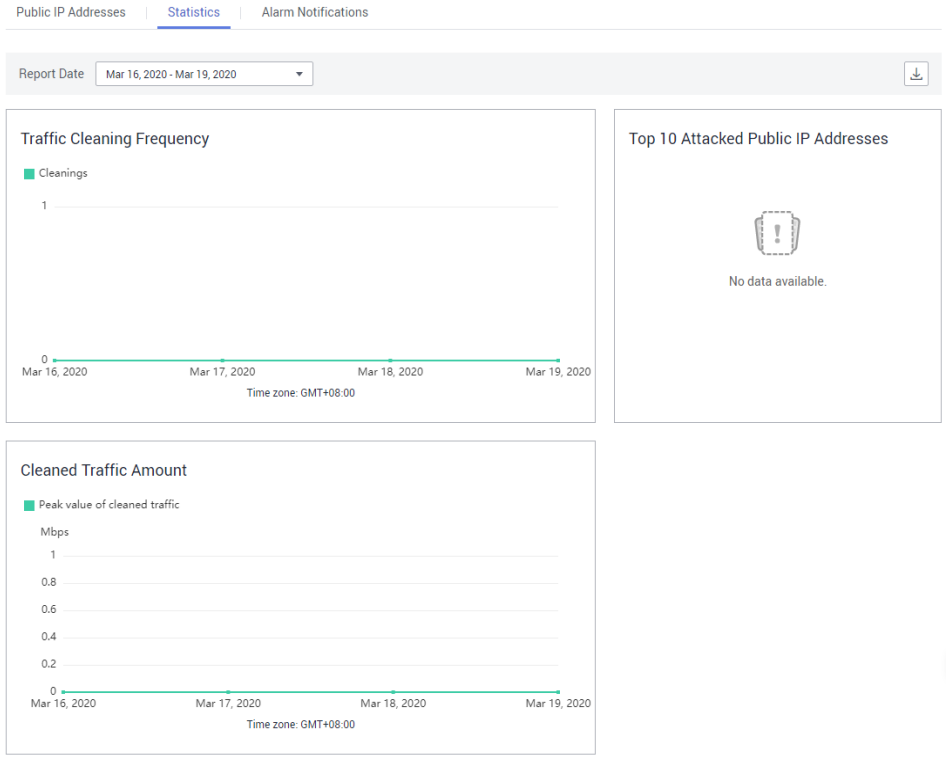
Figure 1-17 Anti-DDoS console



Step 3 Click the **Statistics** tab to view the protection statistics about all public IP addresses.

You can view the weekly security report generated on a specific date. Currently, statistics, including the number of cleaning times, cleaned traffic, weekly top 10 most frequently attacked public IP addresses, and total number of intercepted attacks over the past four weeks can be queried.

Figure 1-18 Viewing an interception report



 Copyright © Huawei Technologies Co., Ltd.

NOTE

Click to download interception reports to view defense statistics of a time range.

----End

1.7 Audit

1.7.1 Anti-DDoS Operations That Can Be Recorded by CTS

Cloud Trace Service (CTS) provides you with a history of Anti-DDoS operations. After enabling CTS, you can view all generated traces to query, audit, and review performed Anti-DDoS operations. For details, see the *Cloud Trace Service User Guide*.

Table 1-5 lists the Anti-DDoS operations that can be recorded by CTS.

Table 1-5 Anti-DDoS operations that can be recorded by CTS

Operation	Trace Name
Enabling Anti-DDoS	openAntiddos
Disabling Anti-DDoS	deleteAntiddos
Adjusting Anti-DDoS security settings	updateAntiddos

1.7.2 Viewing CTS Traces

After you enable CTS, the system starts recording operations performed to Anti-DDoS resources. Operation records generated during the last seven days can be viewed on the CTS console.

Viewing CTS Traces Generated for Operations Performed to Anti-DDoS Resources

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

Step 2 Click on the left of the page and choose **Cloud Trace Service** under **Management & Deployment**. The CTS console is displayed.

Step 3 Choose **Trace List** in the navigation pane on the left.

Step 4 On the displayed page, you can query traces by setting the filtering criteria. The following four filters are available:

- **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**

  Select the desired filter criterion from the drop-down list.

  – Set **Trace Type** to **Management**.

Copyright © Huawei Technologies Co., Ltd.

  - Set **Trace Source** to **Anti-DDoS**.
  - When you select **Trace name** for **Search By**, you also need to select a specific trace name. When you select **Resource ID** for **Search By**, you also need to select or enter a specific resource ID. When you select **Resource name** for **Search By**, you also need to select or enter a specific resource name.
- **Operator**: Select a specific operator (a user rather than tenant).
- **Trace Status**: Available options include **All trace statuses**, **normal**, **warning**, and **incident**. You can only select one of them.
- **Time Range**: In the upper right corner of the page, you can query traces in the last one hour, last one day, last one week, or within a customized period.

Step 5 Click **Query**.

Step 6 Click ⌄ on the left of the record to be queried to extend its details.

Step 7 Locate a trace and click **View Trace** in the **Operation** column.

----End

1.8 Permission Management

1.8.1 Creating a User Group and Assigning the Anti-DDoS Access Permission

This chapter describes IAM's fine-grained permissions management for your Anti-DDoS. With **IAM**, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to Anti-DDoS resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust a HUAWEI CLOUD account or cloud service to perform professional and efficient O&M to your Anti-DDoS resources.

If your HUAWEI CLOUD account does not need individual IAM users for permissions management, skip this chapter.

This section describes the procedure for granting permissions (see **Figure 1-19**).

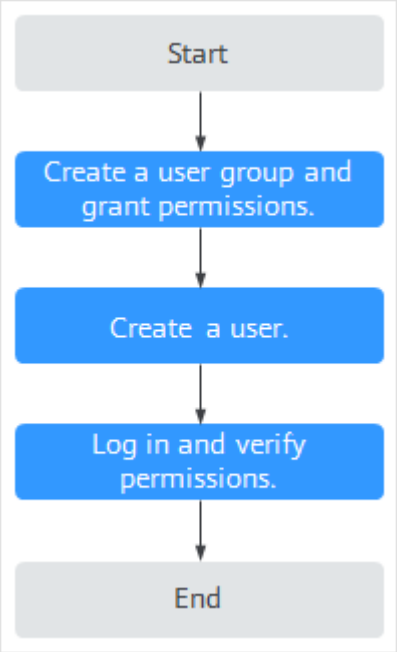
Prerequisites

Before assigning permissions to a user group, you should learn about the Anti-DDoS permissions that can be added to the user group, and select the permissions based on the site requirements. For details about the permissions, see **Anti-DDoS Permissions**. For the system policies of other services, check IAM permissions policies..

 Copyright © Huawei Technologies Co., Ltd.

Process

Figure 1-19 Process for granting permissions



1. **Creating a User Group and Assigning Permissions**.

   Create a user group on the IAM console and assign the Anti-DDoS administrator permission to it.

2. **Creating an IAM User**.

   Create a user on the IAM console and add the user to the user group created in **1**.

3. **Log in** and verify the permission.

   Log in to the management console by using the user created in **2**, and verify that the user only has read permissions for AAD.

   In **Service List** on the HUAWEI CLOUD console, select any other services. If a message indicating that the permission is insufficient is displayed, the Anti-DDoS administrator permission takes effect.

Copyright © Huawei Technologies Co., Ltd.

2 Permissions Management

2.1 Creating a User and Granting the CNAD Pro Access Permission

You can use **Identity and Access Management (IAM)** to implement refined permission control for CNAD Pro resources. To be specific, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing CNAD Pro resources.
- Grant only the permissions required for users to perform a task.
- Entrust a HUAWEI CLOUD account or cloud service to perform professional and efficient O&M to your CNAD Pro resources.

If your HUAWEI CLOUD account does not require individual IAM users, skip this section.

This section describes the procedure for granting permissions (see **Figure 2-1**).

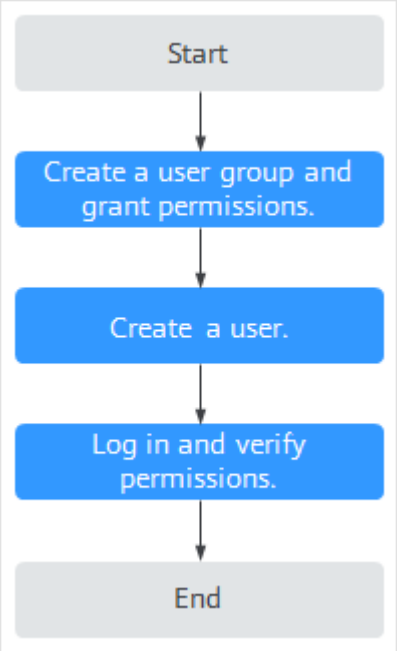
Prerequisites

Before assigning permissions to a user group, you should learn about the CNAD Pro permissions that can be added to the user group, and select the permissions based on the site requirements. For details about the permissions, see **Permissions Management**. For the permissions of other services, see section "Permissions Management".

 Copyright © Huawei Technologies Co., Ltd.

Process

Figure 2-1 Process for granting permissions



1. **Creating a User Group and Assigning Permissions**

   Create a user group on the IAM console, and grant the **CNAD FullAccess** permission to the group.
2. **Creating an IAM User**

   Create a user on the IAM console and add the user to the group created in **1**.
3. **Log in** and verify the permission.

   Log in to the management console by using the user created in **2**, and verify that the user only has read permissions for AAD.

   In **Service List** on the HUAWEI CLOUD console, select any other services (for example, there is only the **CNAD FullAccess** policy). If a message indicating that the permission is insufficient is displayed, the **CNAD FullAccess** permission takes effect.

2.2 CNAD Pro Custom Policies

Custom policies can be created to supplement the system-defined policies of CNAD Pro. For details about the actions supported by custom policies, see **CNAD Pro Permissions and Actions**.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see **Creating a Custom Policy**. The following section contains examples of common CNAD Pro custom policies.

 Copyright © Huawei Technologies Co., Ltd.

Example of a user-defined CNAD Pro policy

- Example 1: Allowing users to query the protected IP address list

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cnad:protectedIpDropList:list"
                                ]
        }
    ]
}
```

- Example 2: Denying deleting an IP address blacklist or whitelist rule

  A deny policy must be used together with other policies. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  The following method can be used if you need to assign permissions of the **CNAD FullAccess** policy to a user but you want to prevent the user from deleting namespaces (cnad:blackWhiteIpList:delete). Create a custom policy for denying namespace deletion, and attach both policies to the group to which the user belongs. Then, the user can perform all operations on CNAD Pro except deleting namespaces. The following is an example policy for denying deleting an IP address blacklist or whitelist rule.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "cnad:blackWhiteIpList:delete"
            ]
        },
    ]
}
```

2.3 CNAD Pro Permissions and Actions

This section describes how to use IAM for fine-grained CNAD Pro permissions management. If your HUAWEI CLOUD account does not need individual IAM users, skip this section.

By default, new IAM users do not have any permissions. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added. Users inherit permissions from the groups and can perform operations on cloud services as allowed by the permissions.

You can grant users permissions by using **roles** and **policies**. Roles are a type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. IAM uses policies to perform fine-grained authorization. A policy defines permissions required to perform operations on specific cloud resources under certain conditions.

Copyright © Huawei Technologies Co., Ltd.

Supported Actions

CNAD Pro provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control.

- Permissions: Statements in a policy that allow or deny certain operations
- Actions: Added to a custom policy to control permissions for specific operations

Permission	Action	Dependency
Querying Quotas	cnad:quota:get	-
Querying Details About a Protection Policy	cnad:policy:get	-
Viewing Protection Statistics	cnad:countReport:get	-
Querying the Asset Security Status	cnad:securityStatusReport:get	-
Querying Weekly Security Statistics	cnad:weekStatisticsReport:get	-
Configuring an Alarm Notification	cnad:alarmConfig:create	To grant the alarm notification permission to users, you must also grant the **cnad:alarmConfig:create** permission and the **SMN Administrator** permission configured for the CN North-Beijing4 region to the users.
Deleting an Alarm Notification	cnad:alarmConfig:delete	To grant the alarm notification permission to users, you must also grant the **cnad:alarmConfig:delete** permission and the **SMN Administrator** permission configured for the CN North-Beijing4 region to the users.

Copyright © Huawei Technologies Co., Ltd.

Permission	Action	Dependency
Querying Alarm Notifications	cnad:alarmConfig:get	To grant the alarm notification permission to users, you must also grant the **cnad:alarmConfig:get** permission and the **SMN Administrator** permission configured for the CN North-Beijing4 region to the users.
Upgrading an Instance	cnad:package:put	-
Binding an IP Address to Be Protected to an Instance	cnad:protectedIp:create	To grant a user the permission for binding objects to a CNAD Pro instance, you need to grant both the **cnad:protectedIp:create** permission and the **vpc:publicIps:list** permission configured for the region to which the instance belongs. For example, a user purchases CNAD Pro instance that is located in CN North-Beijing4. To grant a user the permission for binding objects to a CNAD Pro instance, you need to grant both the **cnad:protectedIp:create** permission and the **vpc:publicIps:list** permission configured for CN North-Beijing4 so that the user can only perform operations on the protected objects in CN North-Beijing4.
Creating a Protection Policy	cnad:policy:create	-
Updating a Protection Policy	cnad:policy:put	-
Deleting a Protection Policy	cnad:policy:delete	-

Copyright © Huawei Technologies Co., Ltd.

Permission	Action	Dependency
Binding a Protection Policy to a Protected IP Address	cnad:bindPolicy:create	-
Removing a Protection Policy from a Protected IP Address	cnad:unbindPolicy:create	-
Adding a Blacklist or Whitelist Rule	cnad:blackWhiteIpList:create	-
Deleting a Blacklist or Whitelist Rule	cnad:blackWhiteIpList:delete	-
Updating the Tag of a Protected IP Address	cnad:ipTag:put	-
Querying the Cleaning Scope	cnad:cleanScaleDropList:list	-
Querying Instances	cnad:packageDropList:list	-
Querying Protection Policies	cnad:policyDropList:list	-
Querying the List of Protected IP Addresses	cnad:protectedIpDrop-List:list	-
Querying Details of an Instance	cnad:package:list	-
Querying Details About a Protection Policy	cnad:policy:list	-
Querying the List of Protected IP Addresses	cnad:protectedIp:list	-
Querying Total Traffic Data	cnad:trafficTotalReport:list	-
Querying Attack Traffic	cnad:trafficAttackRe-port:list	-
Queries the Total Number of Data Packets	cnad:packetTotalReport:list	-
Querying the Number of Attack Packets	cnad:packetAttackReport:list	-
Querying DDoS Mitigation Trend	cnad:cleanCountReport:list	-
Querying the Peak Traffic Scrubbed	cnad:cleanKbpsReport:list	-

Copyright © Huawei Technologies Co., Ltd.

Permission	Action	Dependency
Querying the Distribution of Attack Types	cnad:attackTypeReport:list	-
Querying Attack Events	cnad:attackReport:list	-
Querying Top 10 Attacked IP Addresses	cnad:attackTop:list	-
Creating an Instance	cnad:package:create	To grant a user the permission for purchasing CNAD Pro, you need to grant the **cnad:package:create** permission to the user and the following BSS permissions configured for all regions: • bss:order:update Order Operation • bss:contract:update Contract Modification • bss:balance:view Account Querying • bss:order:pay Payment

Copyright © Huawei Technologies Co., Ltd.

3 Advanced Anti-DDoS User Guide

3.1 Enabling the AAD Service

3.1.1 Purchasing AAD Instances

Scenarios

Before using Advanced Anti-DDoS (AAD), you must purchase AAD instances.

NOTE

Each user can purchase a maximum of five instances by default. If the quota is insufficient, **submit a service ticket** to apply for a higher quota.

Precautions

- Ensure that the account used for purchasing AAD instances 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.
- After an AAD instance is purchased, the instance specifications cannot be modified.

Prerequisites

- AAD (Chinese Mainland) is recommended if your server is deployed in the Chinese Mainland. You have obtained an ICP license first before protecting your domain names.
- If your server is outside the Chinese Mainland, AAD (International) is recommended.

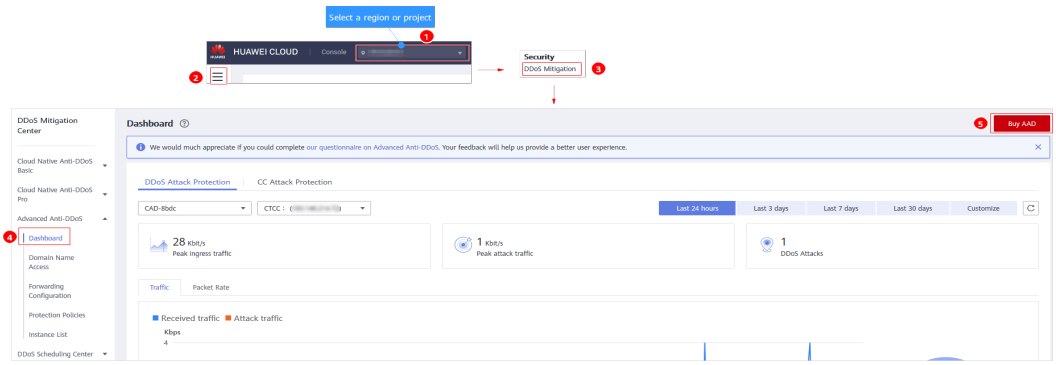
 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the management console.

Step 2 Figure 3-1 shows how to enter the AAD console page.

Figure 3-1 Entering the AAD console page

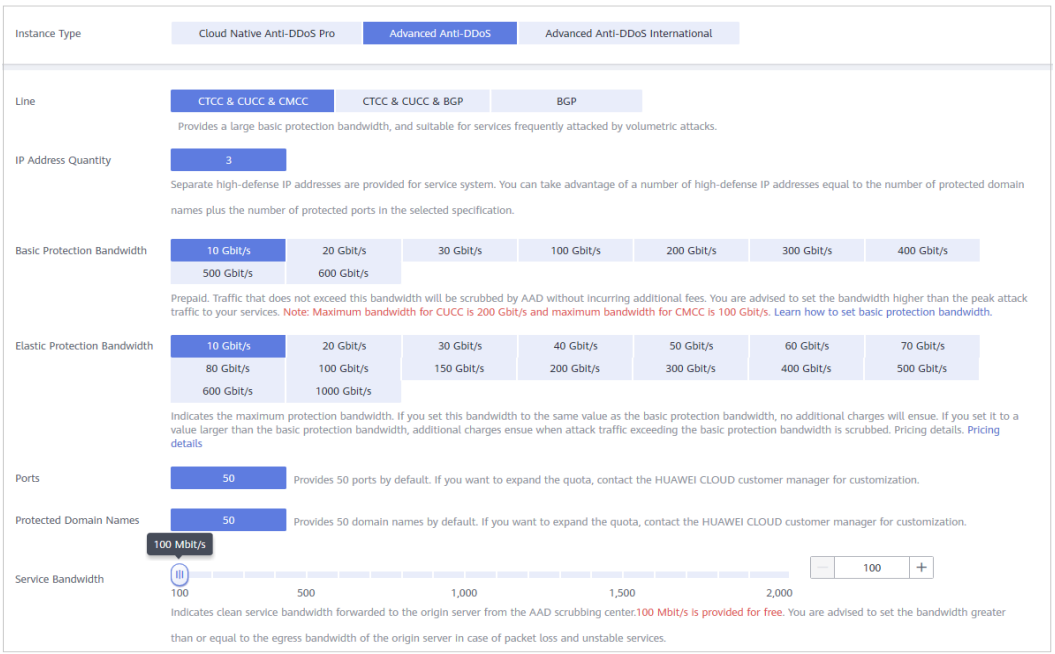


NOTE

Figure 3-1 describes how to enter the AAD console for customers who buy AAD for the first time. When you purchase Advanced Anti-DDoS for the first time, click **Buy Now**.

Step 3 On the displayed **Buy AAD** page, set required parameters shown in Figure 3-2. Table 3-1 describes the parameters to be configured.

Figure 3-2 Setting required parameters



 Copyright © Huawei Technologies Co., Ltd.

Table 3-1 Parameter description

Parameter	Description	Example Value
Line	Lines **CTCC & CUCC & CMCC**, **CTCC & CUCC & BGP**, and **BGP** are supported.	**CTCC & CUCC & CMCC**:
IP Address Quantity	Specifies the number of high-defense IP addresses automatically assigned to the line. The high-defense IP address is provided exclusively for each of your service system. **NOTE** The IP addresses are the ones assigned by AAD and used for providing services for customers in place of the origin server IP address.	3
Basic Protection Bandwidth	Value range: ● **CTCC & CUCC & CMCC**: **10 Gbit/s** to **600 Gbit/s** ● **CTCC & CUCC & BGP**: **10 Gbit/s** to **30 Gbit/s** ● **BGP**: **10 Gbit/s** and **20 Gbit/s** Traffic that does not exceed this bandwidth will be scrubbed by AAD without incurring additional fees. To achieve enhanced protection, use the **Elastic Protection Bandwidth** parameter.	10 Gbit/s

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Elastic Protection Bandwidth	Value range: • **CTCC & CUCC & CMCC**: **10 Gbit/s** to **600 Gbit/s** • **CTCC & CUCC & BGP**: **10 Gbit/s** to **600 Gbit/s** • **BGP**: **10 Gbit/s** to **200 Gbit/s** If you set this parameter to a value larger than the basic protection bandwidth, additional charges ensue when attack traffic exceeding the basic protection bandwidth is scrubbed. If the attack traffic exceeds the elastic protection bandwidth, the high-defense IP address will be blocked by a black hole and cannot provide services. You can modify the elastic protection bandwidth as needed after you have purchased an AAD instance. **NOTE** • The elastic protection bandwidth must be greater than or equal to the basic protection bandwidth. If the two are set to the same value, the elastic protection bandwidth function does not take effect. • **Line Packages** describes the elastic protection bandwidth ranges in different scenarios.	10 Gbit/s
Ports	Specifies the number of ports an AAD instance can protect. 50 ports can be protected for free by default. You can **submit a service ticket** to apply for a quota increase.	50
Protected Domain Names	Specifies the number of domain names an AAD instance can protect. 50 domain names can be protected for free by default. You can **submit a service ticket** to apply for a quota increase.	50
Service Bandwidth	Specifies the service bandwidth for the AAD instance to forward scrubbed traffic to origin servers. The value ranges from **100 Mbit/s** to **2000 Mbit/s**.	100

Step 4 Set **Required Duration** and **Quantity**, as shown in **Figure 3-3**. **Table 3-2** describes the parameters.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-3 Setting **Required Duration** and **Quantity**

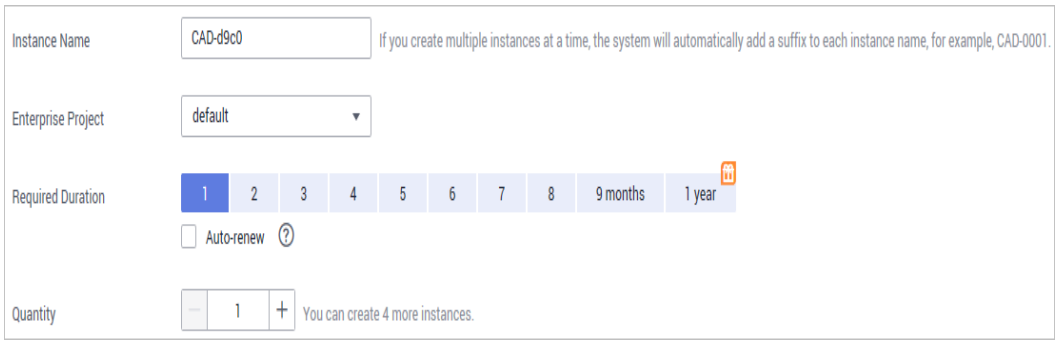


Table 3-2 Parameter description

Parameter	Description	Example Value
Instance Name	Enter a name for the AAD instance you are purchasing. • The name can contain a maximum of 32 characters. • The name can contain only letters, digits, underscores (_), and hyphens (-).	CAD-0001
Enterprise Project	This parameter can only be set by enterprise project users.	N/A
Required Duration	Select a value from one month to one year.	1
Quantity	Select the number of instances to be purchased. By default, each user can purchase a maximum of five instances.	1

NOTE

The **Auto-renew** option is optional. If you tick **Auto-renew**, the system will automatically renew the AAD instance before it expires.

Step 5 Click **Next**.

Step 6 On the **Confirm** page, confirm your order and click **Submit Order**.

Step 7 On the **Pay** page, click **Pay** to pay for the order.

Step 8 When **Order submitted successfully** is displayed, choose **Service List** > **Security** > **Advanced Anti-DDoS**. The instance list is displayed.

----End

3.1.2 Line Packages

Currently, AAD offers three line packages:

 Copyright © Huawei Technologies Co., Ltd.

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

NOTE

These line packages apply only to AAD instances that will protect your servers deployed in the Chinese Mainland. If your servers are deployed outside the Chinese Mainland, visit the international website.

NOTICE

Ensure that the account used for purchasing lines 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.

Line Specifications and Application Scenarios

Line	Basic Protection Bandwidth	Elastic Protection Bandwidth	Application Scenario
CTCC & CUCC & CMCC:	10 Gbit/s to 600 Gbit/s	A maximum of 600 Gbit/s for CTCC, 600 Gbit/s for CUCC, and 100 Gbit/s for CMCC	This line package applies to service systems that have a large user group and have connections to the networks of all three carriers. It protects services against volumetric flooding attacks.
CTCC & CUCC & BGP:	10 Gbit/s to 30 Gbit/s	A maximum of 600 Gbit/s for CTCC, 200 Gbit/s for CUCC, and 200 Gbit/s for BGP (The maximum bandwidth for BGP is dynamically adjusted based on the real-time network traffic, sometimes lower than 200 Gbit/s.)	This line package applies to service systems that have a large user group and have connections to the networks of the three carriers, China Education and Research Network (CERNET), and China Mobile Tietong. It comprises both better user experience of the BGP line and protection against volumetric flooding attacks.

 Copyright © Huawei Technologies Co., Ltd.

Line	Basic Protection Bandwidth	Elastic Protection Bandwidth	Application Scenario
BGP	10 Gbit/s to 20 Gbit/s	A maximum of 200 Gbit/s (The maximum bandwidth is dynamically adjusted based on the real-time network traffic, sometimes lower than 200 Gbit/s.)	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 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.

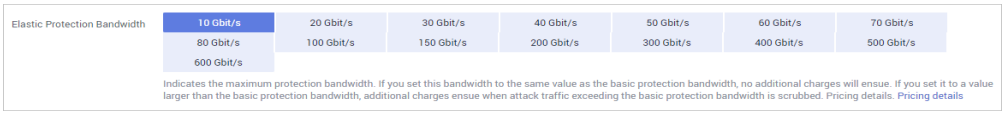
Elastic Protection Bandwidth

The elastic protection bandwidth is set to a value greater than or equal to the basic protection bandwidth.

If you set this bandwidth to the same value as the basic protection bandwidth, no additional charges will ensue. If you set it to a value larger than the basic protection bandwidth, the maximum protection capability is determined by the elastic protection bandwidth you set. Additional charges ensue when attack traffic exceeding the basic protection bandwidth is scrubbed. For details about the charging, see **Product Pricing Details**.

- You can set the elastic protection bandwidth when you purchase the AAD instance on the **Buy AAD** page.

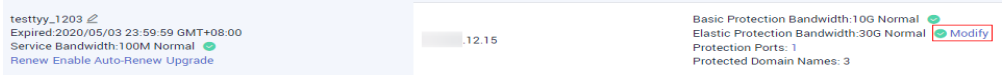
  Figure 3-4 Setting **Elastic Protection Bandwidth**

- You can click **Modify** to adjust the elastic protection bandwidth based on the actual requirements on the console, as shown in **Figure 3-5**. If you set this bandwidth to the same value as the basic protection bandwidth, no additional charges will ensue. If you set it to a value larger than the basic protection bandwidth, additional charges ensue when attack traffic exceeding the basic protection bandwidth is scrubbed. For details about the pricing details, see **Product Pricing Details**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-5 Modifying the elastic protection bandwidth



CTCC & CUCC & CMCC:

You will obtain three high-defense IP addresses respectively for the CTCC, CUCC, and CMCC lines. CTCC offers a maximum of 600 Gbit/s elastic protection, CUCC 600 Gbit/s, and CMCC 100 Gbit/s.

NOTICE

- You need to obtain an ICP license first before protecting your website domain names using the CTCC, CUCC, and CMCC lines.
- If a user visits the website over the network of another carrier other than CTCC, CUCC, and CMCC, packet loss or delay may occur due to cross-network data transmission. To avoid this problem, you are advised to use the BGP line.

CTCC & CUCC & BGP:

You will obtain three high-defense IP addresses respectively for the CTCC, CUCC, and BGP lines. Each line has a basic protection bandwidth of 20 Gbit/s. The two high-defense IP addresses of CTCC and CUCC have a maximum elastic protection capability of 600 Gbit/s and 200 Gbit/s respectively. The BGP line also supports elastic protection. Its maximum elastic protection bandwidth is dynamically adjusted from 20 Gbit/s to 200 Gbit/s depending on real-time network traffic.

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

You are advised to configure the same forwarding rules for the three IP addresses to achieve optimal protection capability and access experience.

NOTICE

You need to obtain an ICP license first before protecting your website domain names using the CTCC, CUCC, and BGP lines.

BGP

You will obtain a high-defense IP address for the BGP line. You can set the basic protection bandwidth for 10 Gbit/s or 20 Gbit/s. This line is recommended for defending against attacks less than 200 Gbit/s. If the DDoS attack traffic exceeds the basic protection bandwidth, the high-defense IP address will be blocked by a black hole.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

You need to obtain an ICP license first before protecting your website domain names using the BGP line.

3.1.3 Upgrading Specifications

Scenarios

This topic describes how to modify the basic protection bandwidth, elastic protection bandwidth, and service bandwidth for an AAD instance.

NOTE

- The basic protection bandwidth and service bandwidth can be increased only.
- The lines cannot be changed during the upgrade.
- Expired instances do not support specifications upgrades.
- Frozen instances do not support specifications upgrades.

Prerequisites

You have obtained a username and its password for logging in to the management console.

NOTICE

Ensure that the account used for upgrading the specifications of AAD instances 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.

Fees Description

Modifying specifications will lead to fee changes. For details, see **Pricing of a Changed Specification**.

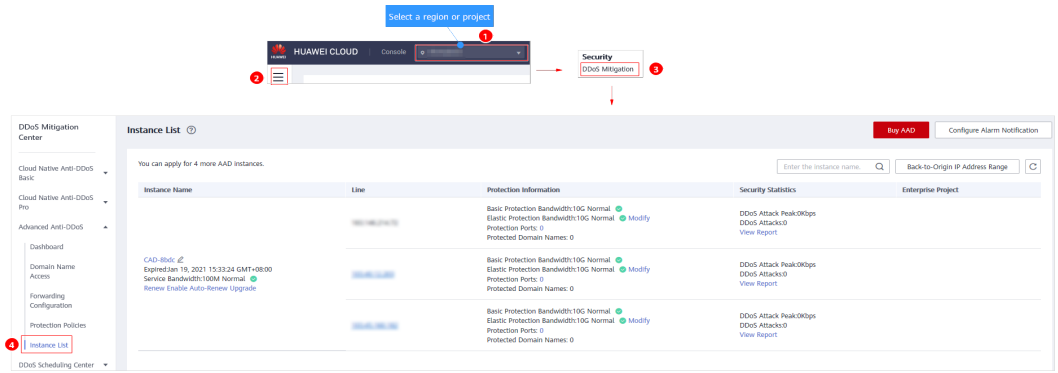
Procedure

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

Step 2 Choose **Advanced Anti-DDoS** > **Instance List** in the left navigation pane.

 Copyright © Huawei Technologies Co., Ltd.

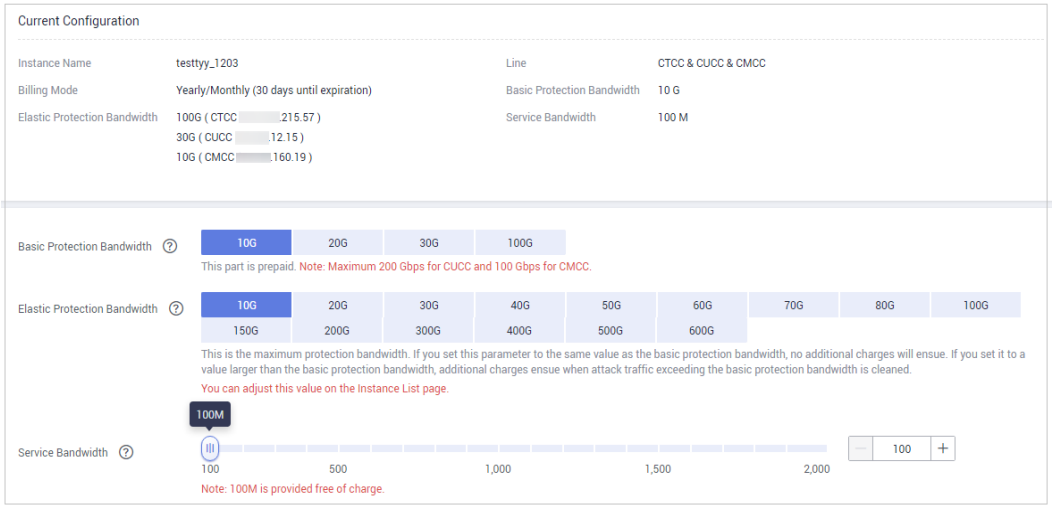
Figure 3-6 Switching to instance list page



Step 3 On the displayed page, locate the target instance and click **Upgrade**.

Step 4 On the displayed page, configure **Basic Protection Bandwidth**, **Elastic Protection Bandwidth**, and **Service Bandwidth**.

Figure 3-7 Upgrading specifications



Step 5 After you click **Submit**, the system will determine whether the configuration has changed. If the configuration does not change, the system displays a failure message indicating that selected specifications are the same as original specifications. If the configuration has changed, the **Details** page is displayed.

Step 6 Click **Submit Order**. When the payment is successful, the **Order submitted successfully** page is displayed.

----End

3.2 Connecting a Website Service to AAD

Scenarios

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. A CNAME record is a type of DNS record that maps an alias name to a true or canonical domain name.

 Copyright © Huawei Technologies Co., Ltd.

Each AAD instance can protect a maximum of 50 domain names. Domain names that need to be protected cannot be added in batches.

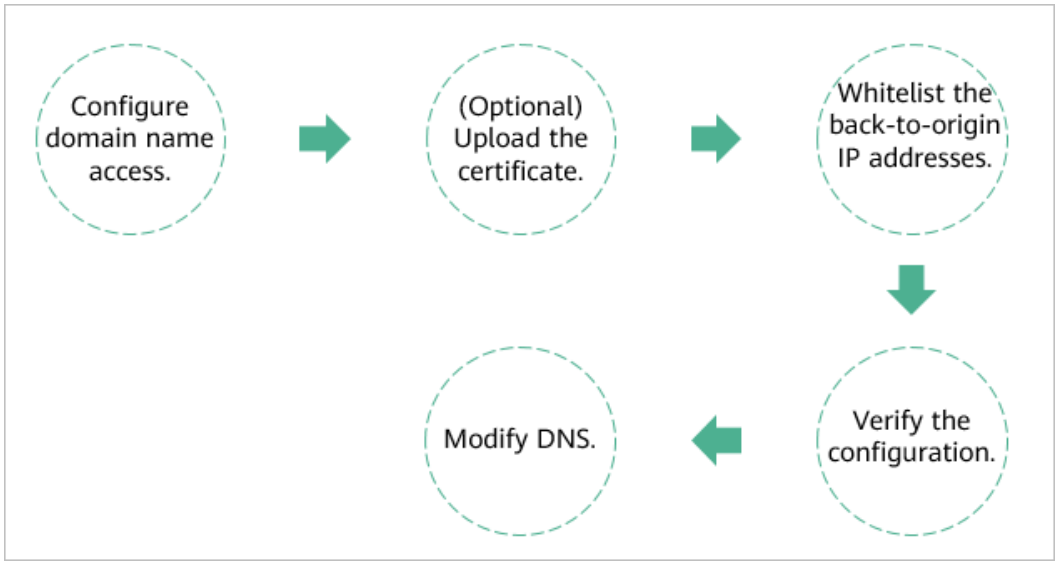
Prerequisites

- You have obtained the username and password for logging in to the management console.
- You have purchased an AAD instance.

Procedure

Figure 3-8 shows the procedure for accessing website services.

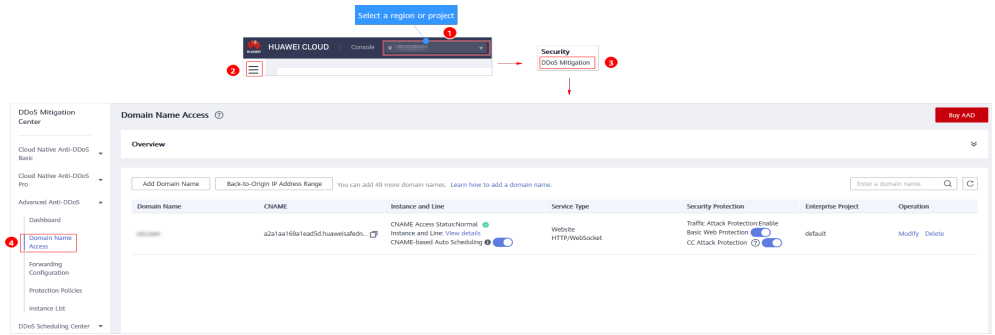
Figure 3-8 Procedure for accessing website services



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 3-9 Domain Name Access page



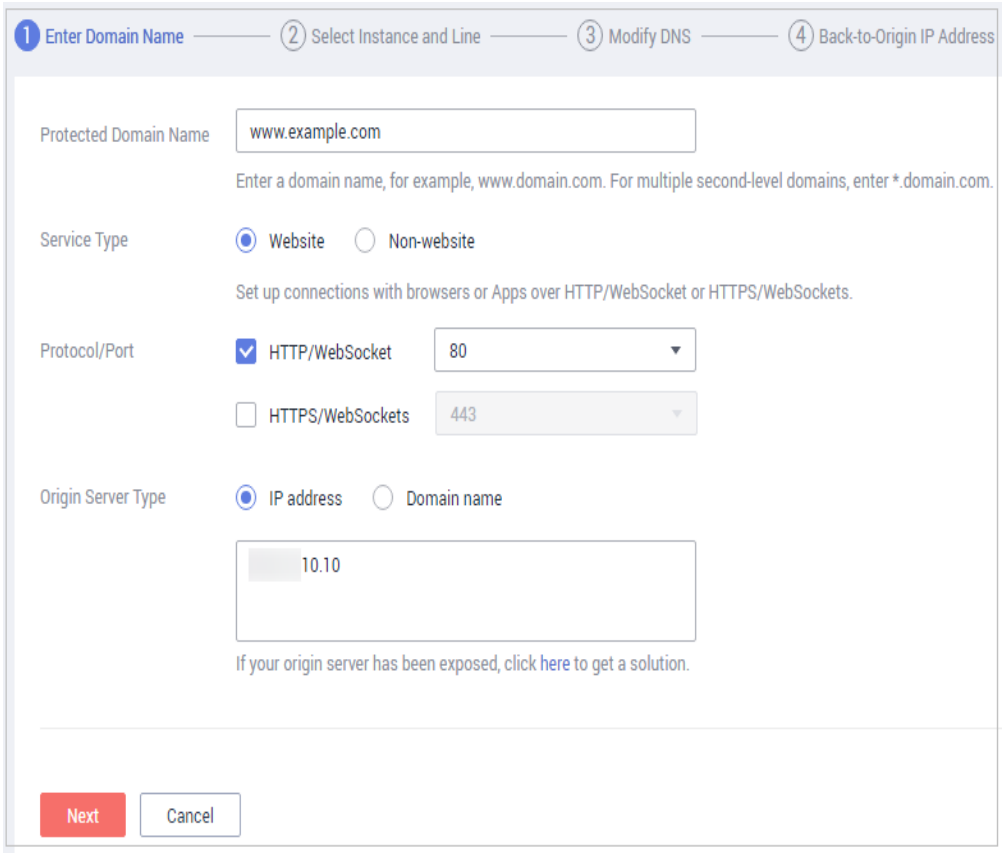
Step 3 On the displayed page, click **Add Domain Name**.

Step 4 Configure domain name access.

 Copyright © Huawei Technologies Co., Ltd.

1. Set required parameters on the displayed page. **Table 3-3** describes the parameters. Click **Next** after the parameters are all configured.

Figure 3-10 Entering domain name information for a website service



NOTE

If you log in to the management console using an enterprise project account, you can choose **Enterprise** > **Project Management** in the upper right corner. On the displayed page, choose **Project Management** in the navigation pane on the left, and select the target project.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-3 Parameter description

Parameter	Description	Example Value
Protected Domain Name	Enter the domain name of the service to protect. – Single domain name: Enter a single domain name, for example, www.example.com. – Wildcard domain name ▪ If the server IP address of each subdomain name is the same, enter 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 the server IP addresses of subdomain names are different, add subdomain names one by one.	Single domain name: **www.example.com** Wildcard domain name: ***.example.com**
Service Type	Select **Website**.	Website
Protocol/ Port	Select a port based on your needs. – Available HTTP/WebSocket ports are **80**, **81**, **82**, **83**, **84**, **8006**, **8078**, **8080**, **8081**, **8087**, **8097**, **19101**, **19501**, **21028**, **40009**, and **40010**. – Available HTTPS/WebSocket ports are **443**, **4006**, **4443**, **5443**, **6443**, **7443**, **8443**, **9443**, **14443**, **20000**, **28443**, **30001**, **30002**, **30003**, **30004**, and **30005**. **NOTE** In one line, website services and non-network services cannot use the same port number.	80

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Origin Server Type	Origin server type of the protected domain name to be added. The value of this parameter can be: – IP address IP address of a real server. A maximum of 20 IP addresses can be entered. Use commas (,) to separate the IP addresses. – Domain name Currently, only HUAWEI CLOUD WAF CNAME is supported. **NOTICE** – If the protected domain name to be added shares the high-defense IP address and protocol or port with a domain name, the values of **Origin Server Type** for the domain names must be same. ■ If **Origin Server Type** is set to **IP address** for a domain name, ensure the web protection is enabled for the domain name. For details about how to enable the web protection, see **Step 4.7**. ■ If **Origin Server Type** is set to **Domain name** for a domain name, ensure that the domain name and the protected domain name to be added are connected to the same WAF. – If **Origin Server Type** is set to **Domain name**, ensure that the domain name has been allowed to use a proxy. Otherwise, the service may be unavailable after being connected to AAD. – If you connect your service to AAD using a WAF CNAME but no longer need WAF protection, delete the service domain name from AAD first.	IP address

2. (Optional) Upload a certificate.

   If you have selected **HTTPS/WebSockets** and set **Origin Server Type** to **IP address**, perform the following steps to upload or update a certificate:

   You can select an existing certificate from the drop-down list or upload a certificate. To upload a certificate, perform the following steps:

   a. Click **Upload Certificate**.

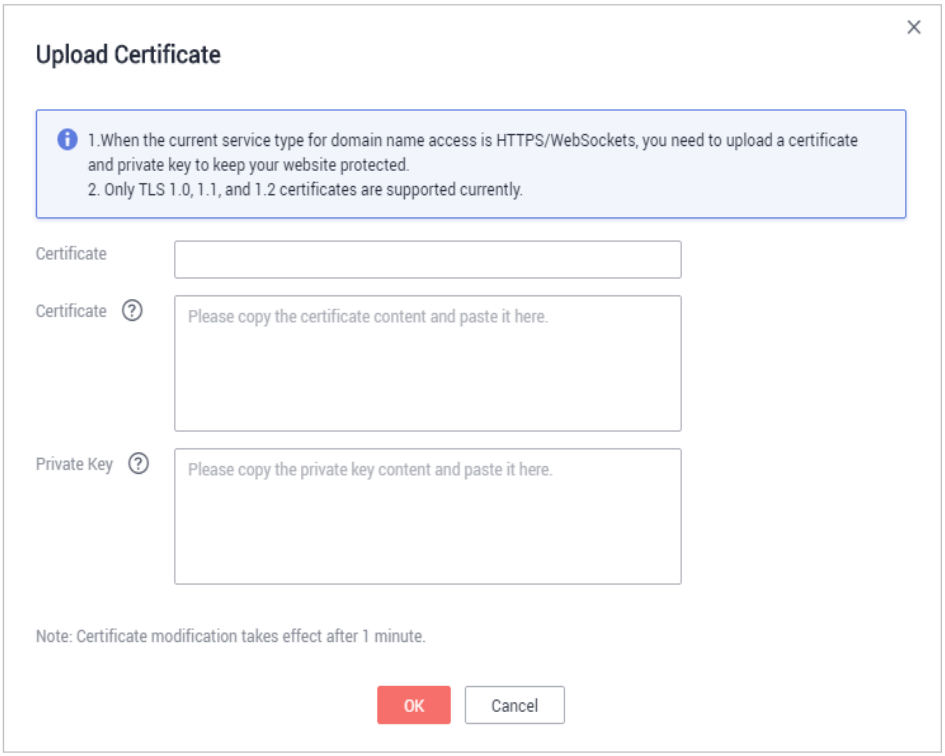
   b. In the displayed **Upload Certificate** dialog box, enter the domain name, certificate content, and private key. **Table 3-4** describes the required parameters.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

The certificate name contains a maximum of 10 characters and cannot contain special characters.

Figure 3-11 Uploading a certificate



NOTE

- Currently, only TLS 1.0, TLS 1.1, and TLS 1.2 certificates can be uploaded.
- You can select an existing certificate.
- Each certificate name of a user must be unique.
- You can select an existing certificate through fuzzy search.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-4 Parameter description

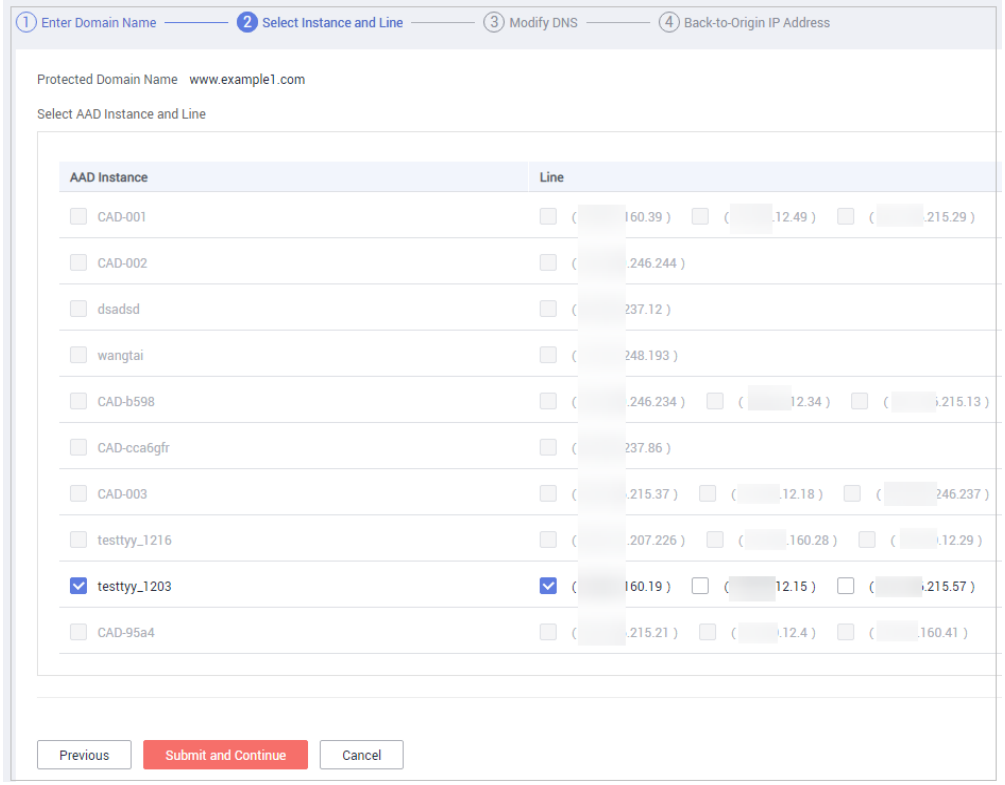
Parameter	Description
Certificate	■ The certificate must be in the following format: -----BEGIN CERTIFICATE----- MIIDljCCAv+gAwIBAgIJAMD2jG2tYGQ6MA0GCSqGSIb3DQEBBQUAMIGPMQswCQYD VQQGEwJDSDELMAkGA1UECBMCWkoxCzAJBgNVBAcTAkhaMQ8wDQYDVQQKEwZodWF3 ZWkxDzANBgNVBAsTBmh1YXdlaTEPMA0GA1UEAxMGaHVhd2VpMQ8wDQYDVQQpEwZz ZXJ2ZXIxIjAgBgkqhkiG9w0BCQEWE3p3YW5nd2VpZGtkQDE2My5jb20wHhcNMTUw MzE4MDMzNjU5WhcNMjUwMzE1MDMzNjU5WjCBjzELMAkGA1UEBhMCQ0gxCzAJBgNV BAgTAlpKMQswCQYDVQQHEwJIWjEPMA0GA1UEChMGaHVhda2VpMQ8wDQY..... -----END CERTIFICATE----- ■ Method for you to copy your certificate: ○ For a .pem certificate: Use a text editor to open the certificate file and copy the content here. ○ For other certificates: Convert your certificate to a .pem one. Then open it with a text editor and copy its content. **NOTE** For details about how to convert a certificate, see **How Do I Convert a Non-PEM Certificate into a PEM One?**.
Private Key	The private key must be in the following format: -----BEGIN RSA PRIVATE KEY----- MIIDljCCAv+gAwIBAgIJAMD2jG2tYGQ6MA0GCSqGSIb3DQEBBQUAMIGPMQswCQYDVQQG EwJDSDELMAkGA1UECBMCWkoxCzAJBgNVBAcTAkhaMQ8wDQYDVQQKEwZodWF3ZWkxDzAN BgNVBAsTBmh1YXdlaTEPMA0GA1UEAxMGaHVhd2VpMQ8wDQYDVQQpEwZzZXJ2ZXIxIjAg BgkqhkiG9w0BCQEWE3poYW5nd2VpZGtkQDE2My5jb20wHhcNMTUwMzE4MDMzNjU5WhcN MjUwMzE1MDMzNjU5WjCBjzELMAkGA1UEBhMCQ0gxCzAJBgNVBAgTAlpKMQswCQYDVQQH EwJIWjEPMA0GA1UEChMGaHVhd2VpMQ8wDQYDVQQLEwZ -----END RSA PRIVATE KEY----- ■ Method for you to copy your private key: ○ For a .pem file: Use a text editor to open the private key file and copy the content here. ○ For other certificates: Convert your certificate to a .pem one. Then open it with a text editor and copy its content. **NOTE** For details about how to convert a certificate, see **How Do I Convert a Non-PEM Certificate into a PEM One?**.

c. Click **OK**.

3. Select required AAD instances and lines and click **Submit and Continue**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-12 Select Instance and Line

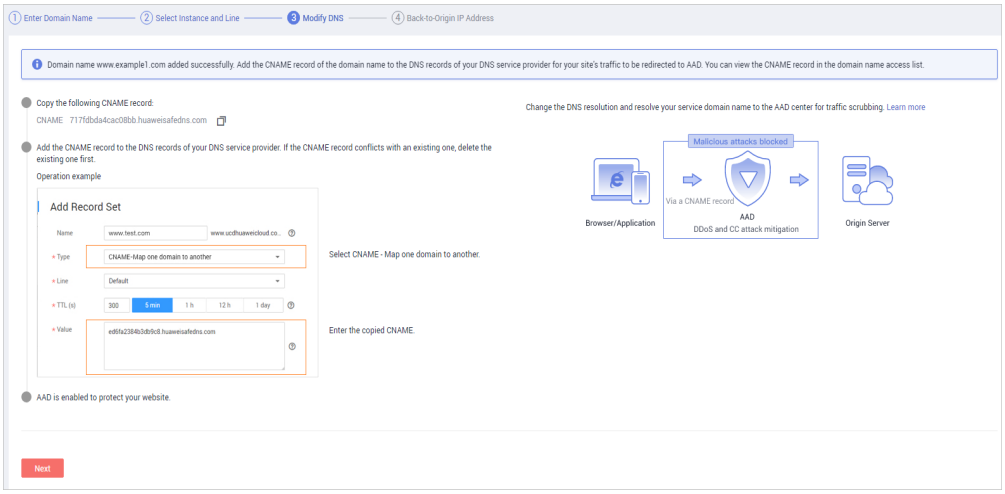


NOTE

- You can select multiple lines (with high-defense IP addresses) for a domain name. However, the IP addresses must have the same number of forwarding rules, the same forwarding protocols, ports, and the same service type.
- HUAWEI CLOUD provides multiple carrier lines for each instance to avoid cross-carrier access from your users. You are advised to select a complete set of lines, which includes all carriers, when selecting lines for your instance.

4. Copy the displayed CNAME record of the domain name and add the CNAME to DNS. Then click **Next**.

Figure 3-13 Modifying DNS

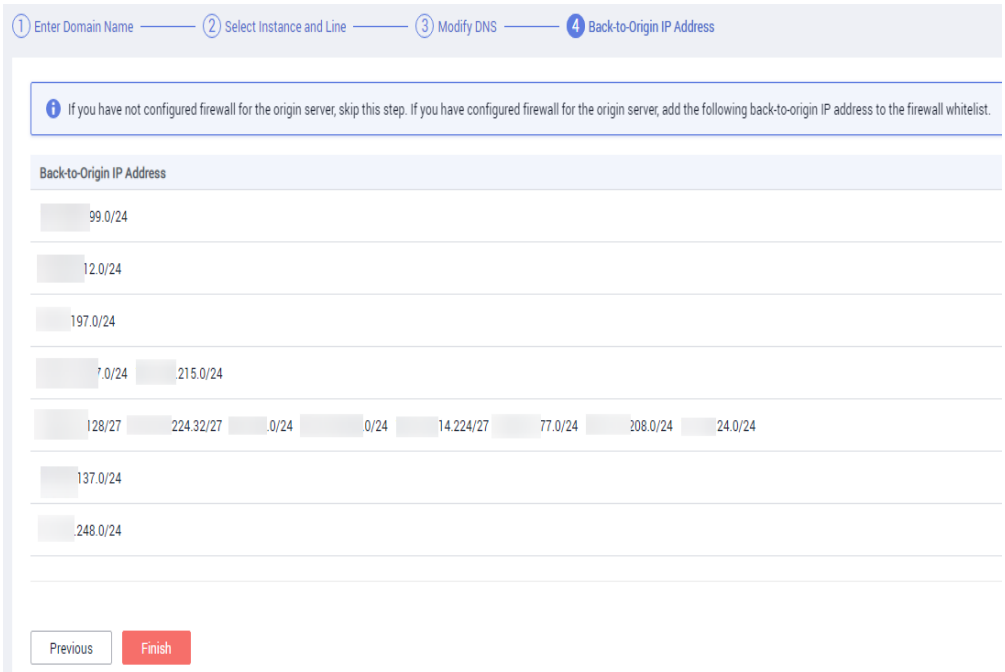


 Copyright © Huawei Technologies Co., Ltd.

For details about modifying DNS configuration, see **Adding a CNAME Record**.

5. Add the back-to-origin IP addresses to the firewall whitelist.

Figure 3-14 Adding the back-to-origin IP addresses to the firewall whitelist



- If no firewall has been configured for the origin server, click **Finish**.
- If a firewall has been configured for the origin server, whitelist the back-to-origin IP addresses on the firewall, ACL, or any other security software of your origin servers to prevent the access traffic from being blocked or limited by the security policies. Click **Finish**.

The **Domain Name Access** page is displayed. The newly added domain name is displayed in the list.

NOTE

AAD executes Full Network Address Translation (Full-NAT) and diverts access traffic to the back-to-origin IP addresses.

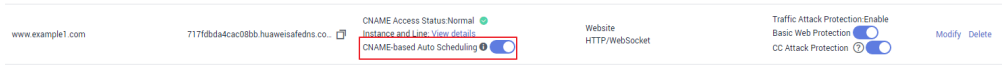
- If AAD is not used, access traffic is sent directly from the source IP addresses of clients towards origin servers. From the view of origin servers, the requests originate from scattered clients and each source IP address sends only a few access requests.
- After AAD is enabled, access traffic will be forwarded to the back-to-origin IP addresses. From the view of origin servers, the requests originate from these back-to-origin IP addresses. These IP addresses are fixed and limited in quantity, and each carries more requests than the source IP address. Therefore, they may be mistakenly regarded as the sources that launch attacks. In this case, other Anti-DDoS security policies working on the origin servers may block or limit the requests from the back-to-origin IP addresses. For example, error 502 is reported if the access request is blocked by mistake.

6. (Optional) Enable CNAME-based auto scheduling.

   CNAME-based auto schedule distributes incoming traffic based on its originating carrier. It can divert traffic to other lines if a line is blocked by a black hole.

 Copyright © Huawei Technologies Co., Ltd.

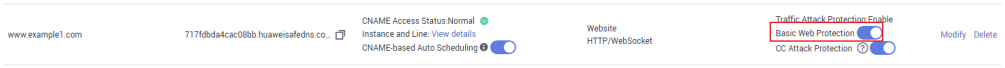
Figure 3-15 Enabling CNAME-based automatic scheduling



7. (Optional) If you set **Origin Server Type** to **IP address**, locate the row containing the target domain name and enable **Basic Web Protection** in the **Security Protection** column, as shown in **Figure 3-16**.

   AAD provides you with layer-7 protection only after you enable basic web protection.

Figure 3-16 Enabling basic web protection



Step 5 Verify the configuration.

After the configuration takes effect, AAD is expected to forward the packets sent to the high-defense IP address or AAD CNAME to the origin servers. To ensure service stability, you can use the following steps to verify the configuration:

- **Assumed CNAME:**
  - CNAME: 5dc728e1769ad666.huaweisafedns.com
- **Procedure:**
  a. Use **Telnet www.huaweicloud.com 80** to verify the network connectivity.
     - If the connection setup is successful, you can Telnet to the public IP address from your local network environment.
     - If the connection setup fails, change your test network environment and try again. Some enterprises may have internal network constraints and fail the verification. For example, you can connect to the personal hotspot of your phone to verify the connectivity.

  b. After verifying the network connectivity, you can Telnet to the AAD CNAME over port 80.
     - If the Telnet command is executed successfully, the configuration has taken effect.
     - If the command execution fails, check whether the required steps have been completed.
     - If the fault persists, contact technical support.

Step 6 Modify DNS.

For details, see **Adding a CNAME Record**.

The DNS configuration takes effect after a period of time. In this period, you can test the domain name resolution using some online test tools such as 17ce and China Webmaster.

----End

 Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

- If you do not want a domain name to be resolved to a high-defense IP address, locate the row containing the domain name on the **Domain Name Access** page and click **View details** in the **Instance and Line** column. On the page that is displayed, click  for the target high-defense IP address to set **DNS Resolution** to .
- If you do not want to protect a domain name, locate the row containing the domain name on the **Domain Name Access** page and click **Delete** in the **Operation** column.

3.3 Connecting a Non-website Service to AAD

Scenarios

Non-website services include Apps and PC client services. For such services, you can configure CNAME records in DNS or directly configure high-defense IP addresses on clients to use AAD.

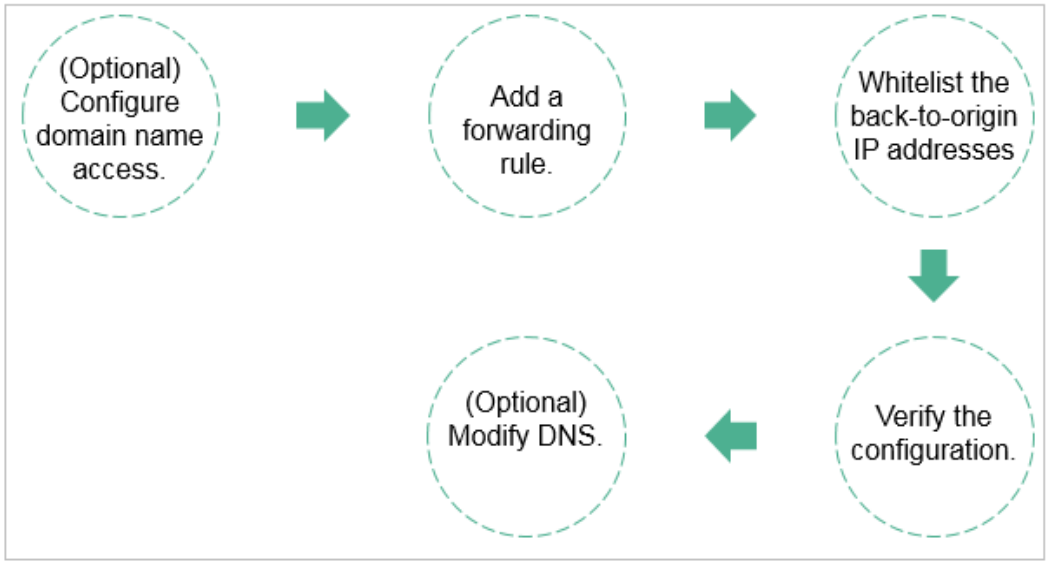
Prerequisites

- You have obtained an account and its password to log in to the management console.
- You have purchased an AAD instance.

Procedure

Figure 3-17 shows the procedure for accessing non-website services.

Figure 3-17 Procedure for accessing non-website services



Step 1 Log in to the management console.

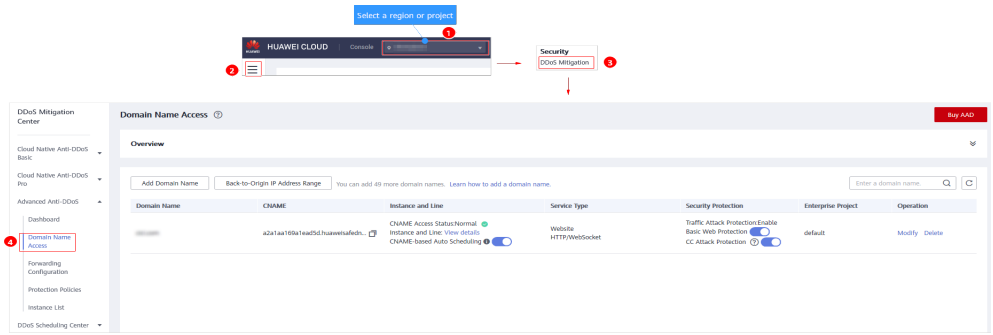
 Copyright © Huawei Technologies Co., Ltd.

Step 2 (Optional) Configure domain name access.

Perform this step if intelligent resolution lines will be provided for domain names.

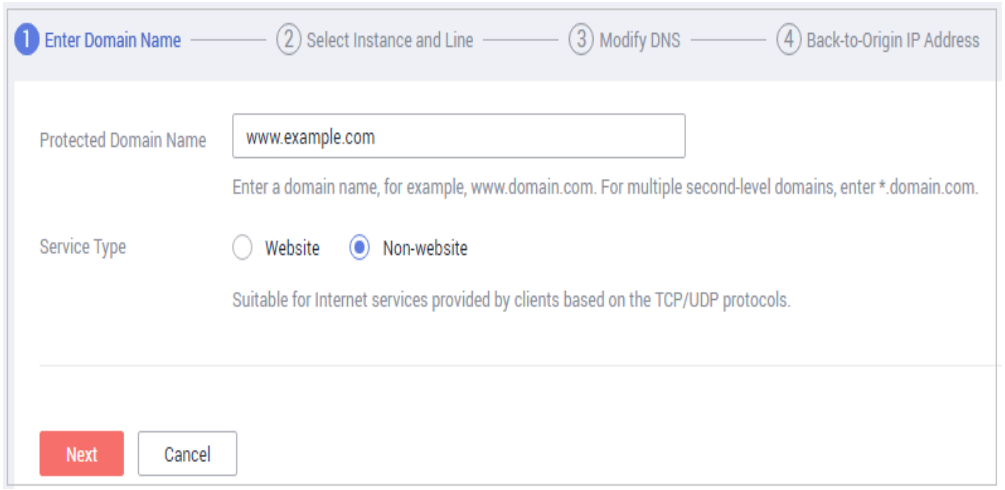
1. **Log in to the management console.**
2. Follow the procedure in the following figure to enter the **Domain Name Access** page.

Figure 3-18 Domain Name Access page



3. On the displayed page, click **Add Domain Name**.
4. Complete the necessary domain name information and click **Next**.

Figure 3-19 Entering domain name information for a non-website service



NOTE

If you log in to the management console using an enterprise project account, you can choose **Enterprise** > **Project Management** in the upper right corner. On the displayed page, choose **Project Management** in the navigation pane on the left, and select the target project.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-5 Parameter description

Parameter	Description
Protected Domain Name	Enter the domain name of the service to protect. – Single domain name: Enter a single domain name, for example, www.example.com. – Wildcard domain ▪ If the server IP address of each subdomain name is the same, enter a wildcard domain name to be protected. For example, if the subdomain names ***a.example.com***, ***b.example.com***, and ***c.example.com*** have the same server IP address, you can add the wildcard domain name ****.example.com*** to AAD to protect all three. ▪ If the server IP addresses of subdomain names are different, add subdomain names one by one.
Service Type	Select **Non-website**.

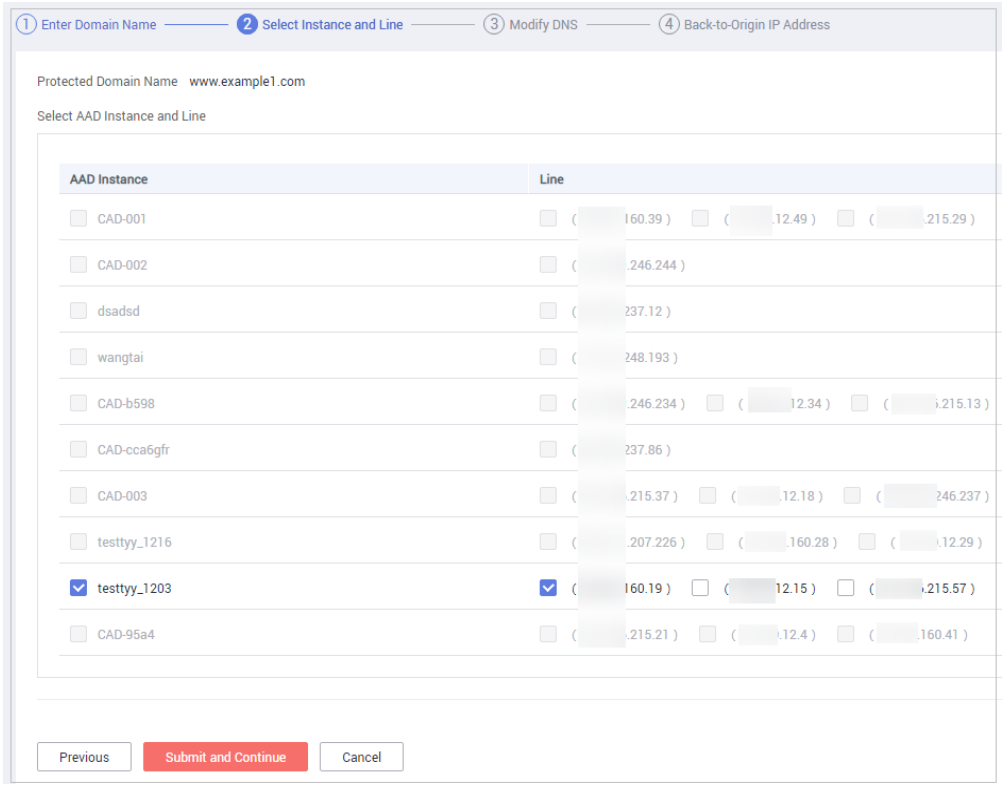
5. Select required AAD instances and lines and click **Submit and Continue**.

   You can select multiple lines (with high-defense IP addresses) for a domain name. However, the IP addresses must have the same number of forwarding rules, the same forwarding protocols, ports, and the same service type.

   HUAWEI CLOUD provides multiple carrier lines for each instance to avoid cross-carrier access from your users. You are advised to select a complete set of lines, which includes all carriers, when selecting lines for your instance.

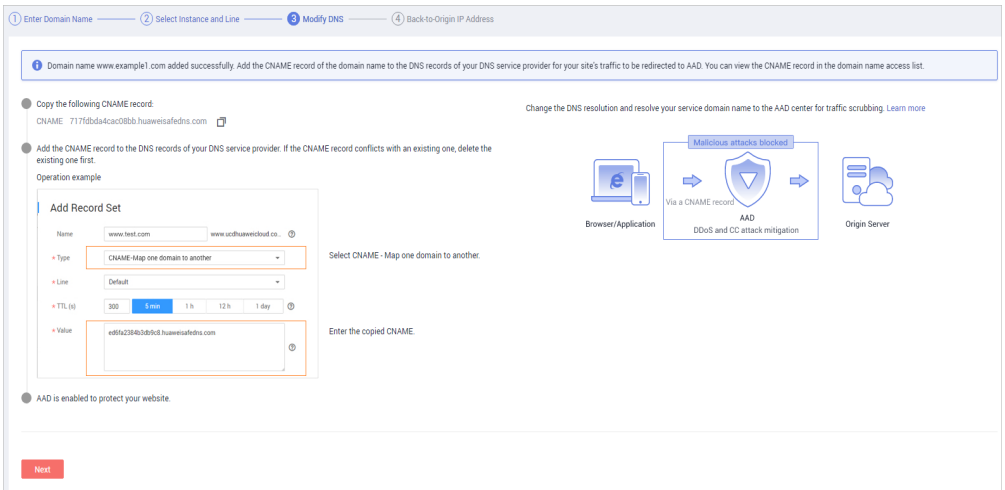
 Copyright © Huawei Technologies Co., Ltd.

Figure 3-20 Selecting an instance and a line



6. Copy the displayed CNAME record of the domain name and click **Next**.

Figure 3-21 Modifying DNS



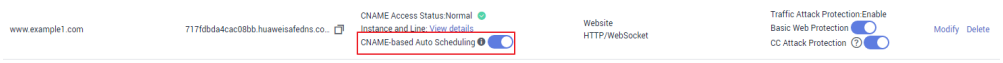
7. Whitelist the back-to-origin IP addresses.
   - If no firewall has been configured for the origin server, click **Finish**.
   - If a firewall has been configured for the origin server, add the back-to-origin IP address range to the whitelist of the firewall. Then click **Finish**.

   The **Domain Name Access** page is displayed. The newly added domain name is displayed in the list.
8. (Optional) Enable CNAME-based auto scheduling if you need to access the service using a domain name. CNAME-based auto schedule distributes

 Copyright © Huawei Technologies Co., Ltd.

incoming traffic based on its originating carrier. It can divert traffic to other lines if a line is blocked by a black hole.

Figure 3-22 Enabling CNAME-based automatic scheduling



Step 3 Add a forwarding rule.

For details, see **Configuring a Forwarding Rule**.

Step 4 Whitelist the back-to-origin IP addresses.

- Reason for whitelisting the IP addresses:

  AAD executes Full Network Address Translation (Full-NAT) and diverts access traffic to the back-to-origin IP addresses.

  - If AAD is not used, access traffic is sent directly from the source IP addresses of clients towards origin servers. From the view of origin servers, the requests originate from scattered clients and each source IP address sends only a few access requests.
  - After AAD is enabled, access traffic will be forwarded to the back-to-origin IP addresses. From the view of origin servers, the requests originate from these back-to-origin IP addresses. These IP addresses are fixed and limited in quantity, and each carries more requests than the source IP address. Therefore, they may be mistakenly regarded as the sources that launch attacks. In this case, other anti-DDoS security policies working on the origin servers may block or limit the requests from the back-to-origin IP addresses. For example, error 502 is reported if the access request is blocked by mistake.

- Procedure:

  a. View the back-to-origin IP address range. For details, see **Viewing a Back-to-Origin IP Address Range**.

  b. Whitelist the back-to-origin IP address range on the firewall, ACL, or any other security software on your origin servers to prevent the access traffic from being blocked or limited by the security policies.

Step 5 Verify the configuration.

After the configuration takes effect, AAD is expected to forward the packets sent to the high-defense IP address or AAD CNAME to the origin servers. To ensure service stability, you can use the following steps to verify the configuration:

- **Assumed parameter values:**
  - Lines: CTCC, CUCC, and CMCC
    - CTCC IP address: 1.1.1.1
    - CUCC IP address: 2.2.2.2
    - CMCC IP address: 3.3.3.3
  - CNAME: 5dc728e1769ad666.huaweisafedns.com
  - Forwarding port: 1234

 Copyright © Huawei Technologies Co., Ltd.

  - Protected domain name: www.test.com
  - Origin server IP address: 4.4.4.4
  - Origin server port: 1234
- **Procedure:**

  a. Use **Telnet www.huaweicloud.com 80** to verify the network connectivity.

     - If the connection setup is successful, you can Telnet to the public IP address from your local network environment.
     - If the connection setup fails, change your test network environment and try again. Some enterprises may have internal network constraints and fail the verification. For example, you can connect to the personal hotspot of your phone to verify the connectivity.

  b. After verifying the network connectivity, you can Telnet to the high-defense IP address of each carrier line and the AAD CNAME over port 1234.

     - If the Telnet command is executed successfully, the configuration has taken effect.
     - If the command execution fails, check whether the required steps have been completed.
     - If the fault persists, contact HUAWEI CLOUD technical support.

Step 6 (Optional) Modify DNS.

Perform this step if you need to access the service using a domain name.

- If you have configured domain name access and obtained the CNAME, perform **Adding a CNAME Record**.
- If you added a forwarding rule without configuring domain name access, perform **Adding an A Record**.

The DNS configuration takes effect after a period of time. In this period, you can test the domain name resolution using some online test tools such as 17ce and China Webmaster.

----End

Follow-up Procedure

- If you do not want a domain name to be resolved to a high-defense IP address, locate the row containing the domain name on the **Domain Name Access** page and click **View details** in the **Instance and Line** column. On the page that is displayed, click  for the target high-defense IP address to set **DNS Resolution** to .
- If you do not want to protect a domain name, locate the row containing the domain name on the **Domain Name Access** page and click **Delete** in the **Operation** column.

Copyright © Huawei Technologies Co., Ltd.

3.4 Configuring a Forwarding Rule

Scenarios

If your instance runs a non-website service, you need to configure forwarding rules for the instance.

By default, you can add a maximum of 50 forwarding rules to each instance. You can **submit a service ticket** to add more forwarding rules.

After configuring the rules, change the domain names based on your services. AAD will automatically forward traffic to your origin server IP addresses.

Prerequisites

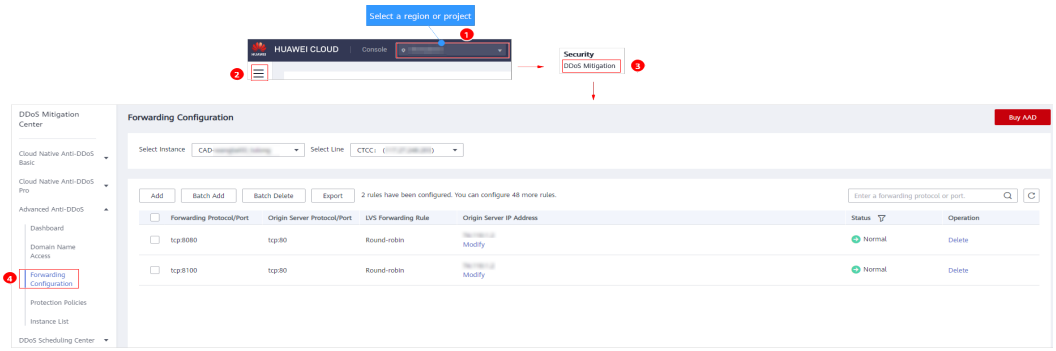
- You have obtained the username and password for logging in to the management console.
- You have purchased an AAD instance.

Procedure

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

Step 2 Follow the procedure in the following figure to enter the **Forwarding Configuration** page.

Figure 3-23 Forwarding configuration entry



Step 3 On the **Forwarding Configuration** page, add forwarding rules.

NOTE

- One origin server IP address can be added to multiple forwarding rules.
- The forwarding protocol and forwarding port in each forwarding rule must be unique.
- You can enter a forwarding protocol or port to search for specific rules in the search box in the upper right corner of the page.

- Add a single forwarding rule.
  a. Click **Add** on the **Forwarding Configuration** page.
  b. In the **Add Forwarding Rule** dialog box, configure forwarding rule information and click **OK**. **Table 3-6** describes the parameters.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-24 Adding a forwarding rule

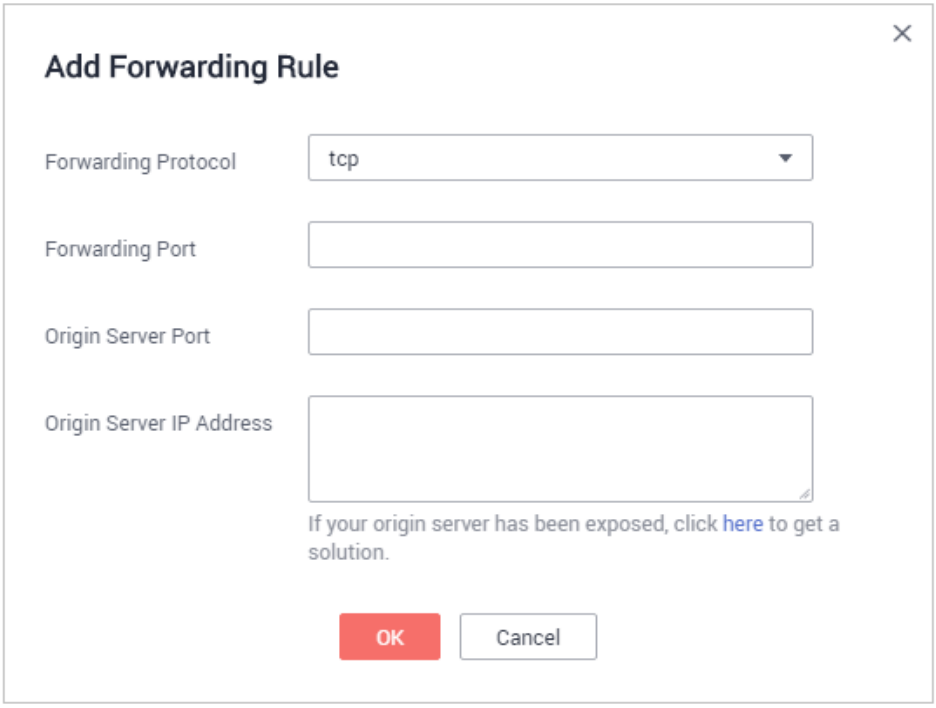


Table 3-6 Parameters for adding a forwarding rule

Parameter	Description
Forwarding Protocol	Specifies the protocol used to forward user service workload. ■ **tcp**: TCP is a connection-oriented protocol that provides reliable delivery of a stream of bytes at the transport layer. ■ **udp**: UDP is a connectionless protocol that provides simple transaction-oriented delivery of messages at the transport layer.
Forwarding Port	Specifies the ingress port used to forward user service workload. The value can be **1** to **65535**. ■ In one line, website services and non-network services cannot use the same port number.
Origin Server Port	Specifies the egress port used to forward user service workload. The value can be **1** to **65535**.

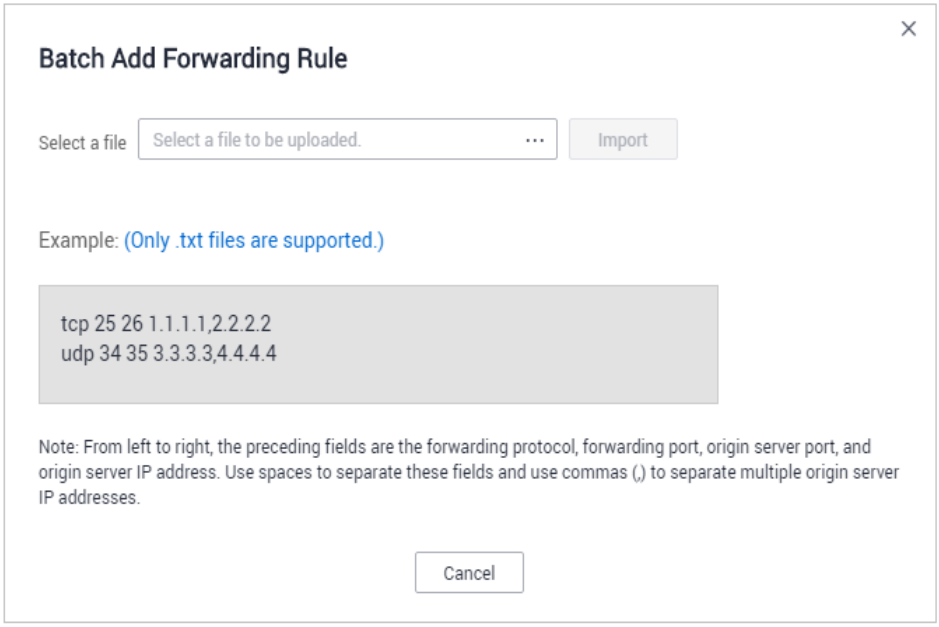
Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Origin Server IP Address	Specifies the public IP address used by the origin server. ■ After configuring the rules, change the domain names based on your services. AAD will automatically forward traffic to your origin server IP addresses. ■ You can add a maximum of 20 origin server IP addresses. Separate them with commas (,). ■ Enter a valid public IP address.

c. Click **OK**.

- Batch add forwarding rules.
  a. Click **Batch Add** on the **Forwarding Configuration** page.
  b. In the **Batch Add Forwarding Rule** dialog box, click ... to select a file and click **Import**.

Figure 3-25 Adding forwarding rules in batches



 Copyright © Huawei Technologies Co., Ltd.

NOTE

- Only a .txt file can be imported.
- In the imported file, fields from left to right are the forwarding protocol, forwarding port, origin server port, and origin server IP address, with spaces in between. Multiple origin server IP addresses are separated using commas (,).
- Each line accommodates only one forwarding rule. **Table 3-6** describes each field.
- The number of forwarding rules in the file cannot exceed the quota limit. Under the quota limit, you can import a maximum of 200 forwarding rules at a time.

----End

Follow-up Procedure

- To change the origin server IP address of a forwarding rule, see **Changing an Origin Server IP Address**.
- If a forwarding rule is not required, delete it by referring to **Deleting a Forwarding Rule**.
- To back up a forwarding rule or quickly modify its configuration information, go to **Exporting a Forwarding Rule**.

3.5 Configuring a Protection Policy

3.5.1 Configuring a Blacklist and a Whitelist

Scenarios

This section describes how to configure a blacklist and a whitelist for an AAD instance that has added a protected domain name.

Prerequisites

- You have obtained the username and password for logging in to the management console.
- You have purchased an AAD instance.

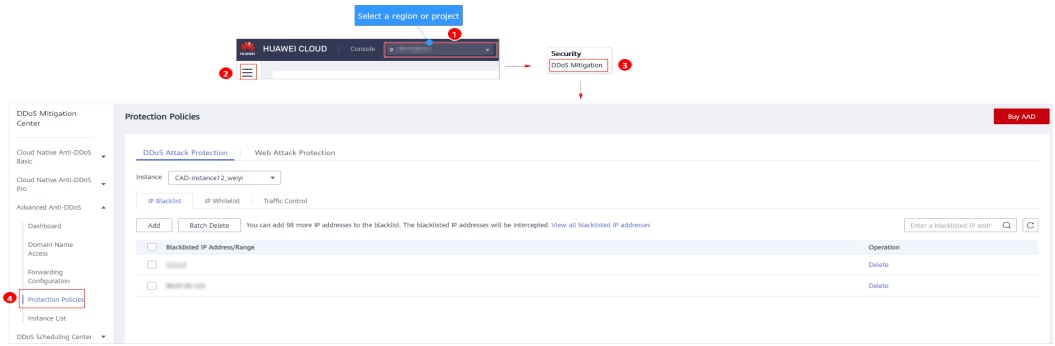
Procedure

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

Step 2 Follow the procedure in the following figure to enter the **Protection Policies** page.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-26 Entering the **Protection Policies** page

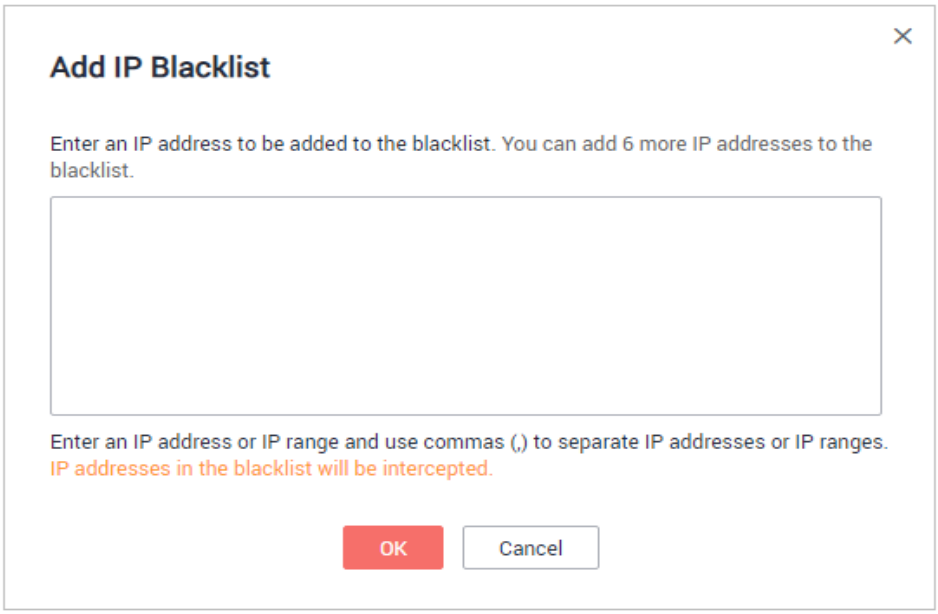


Step 3 In the drop-down list of **Instance**, select the instance for which you want to configure a blacklist or whitelist.

Step 4 Configure a blacklist and a whitelist.

- Configuring an IP blacklist
  a. Select the **IP Blacklist** tab and click **Add**.
  b. In the displayed dialog box, enter the IP addresses or IP ranges to be blocked.

  Figure 3-27 Adding blacklisted IP addresses

  NOTE

  A maximum of 100 IP addresses can be added to the blacklist of an instance, and IP addresses in the blacklist will be blocked.

  c. Click **OK**.

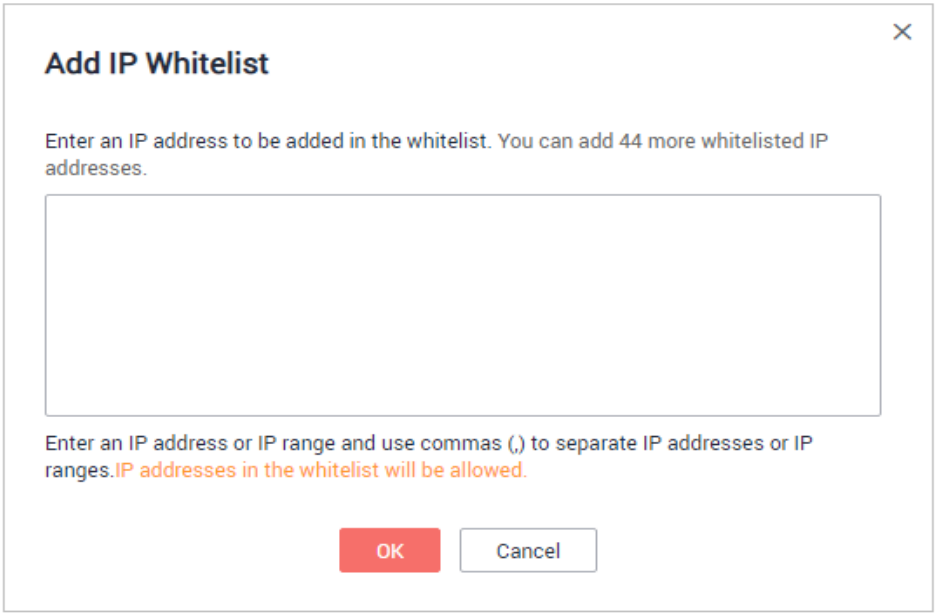
  On the **IP Blacklist** page, click **Delete** in the **Operation** column or select the blacklisted IP addresses to be deleted and click **Delete** to delete IP addresses in batch. Deleted IP addresses will not be blocked.
- Configuring an IP whitelist

 Copyright © Huawei Technologies Co., Ltd.

a. Select the **IP Whitelist** tab and click **Add**.

b. In the displayed dialog box, enter the IP addresses or IP ranges to be permitted.

Figure 3-28 Adding whitelisted IP addresses



NOTE

A maximum of 100 IP addresses can be added to the whitelist of an instance. IP addresses in the whitelist are permitted.

c. Click **OK**.

On the **IP Whitelist** page, click **Delete** in the **Operation** column or select the whitelisted IP addresses to be deleted and click **Delete** to delete IP addresses in batch. After an IP address is deleted from the whitelist, the device will not directly permit traffic from this IP address.

----End

3.5.2 Configuring Traffic Control

Scenarios

This section describes how to perform traffic control on AAD instance lines.

Prerequisites

- You have obtained the username and password for logging in to the management console.
- You have purchased an AAD instance.

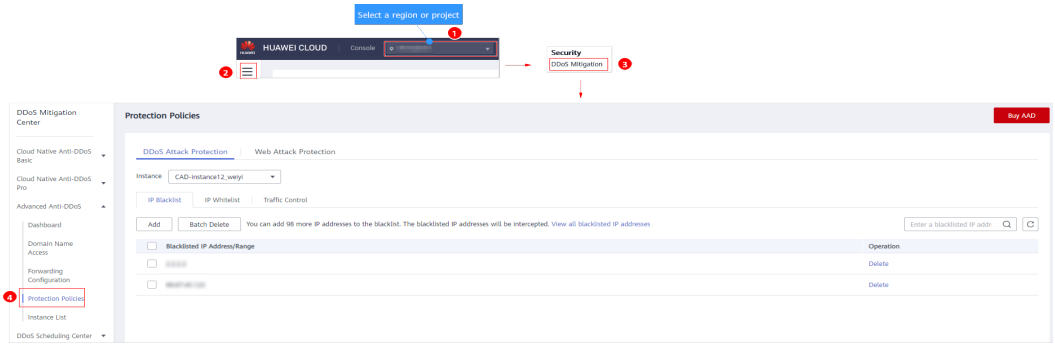
 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the management console.

Step 2 Follow the procedure in the following figure to enter the **Protection Policies** page.

Figure 3-29 Entering the **Protection Policies** page



Step 3 In drop-down list of **Instance**, select the instance for which you want to configure traffic control.

Step 4 Click the **Traffic Control** tab to view the status of **Traffic Control Outside Chinese Mainland** and **UDP Traffic Control**.

Figure 3-30 Traffic control

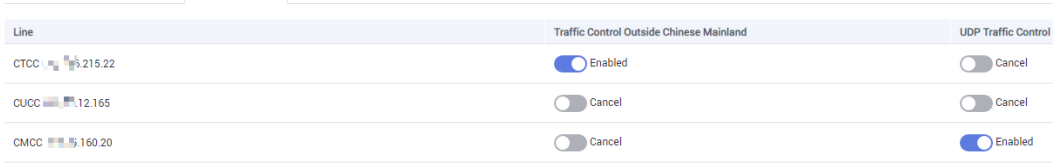


Table 3-7 Parameter description

Parameter	Description
Line	Line and IP address information about an instance
Traffic Control Outside Chinese Mainland	The default value is **disabled**. • If you set this parameter to , traffic outside Chinese mainland will be blocked. • If you set this parameter to , traffic outside Chinese mainland will not be blocked.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
UDP Traffic Control	The default value is **disabled**. • If you set this parameter to , UDP traffic will be blocked. • If you set this parameter to , UDP traffic will not be blocked.

----End

3.5.3 Configuring CC Attack Protection Rules

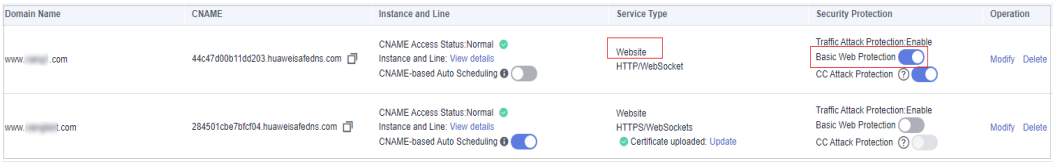
Scenarios

After website services are connected to AAD, you can configure Challenge Collapsar (CC) protection rules to restrict access to a specific URL on your website based on a unique IP address, cookie, or Referer field. AAD can accurately identify CC attacks and effectively mitigate CC attacks based on the protection rules you configured.

Prerequisites

Website services have been connected to AAD and **Basic Web Protection** has been enabled.

Figure 3-31 Basic Web Protection enabled for website services

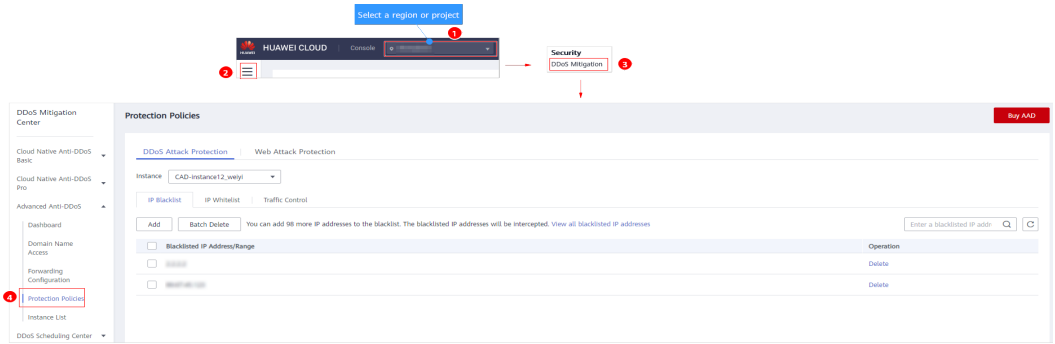


Procedure

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

Step 2 Follow the procedure in the following figure to enter the **Protection Policies** page.

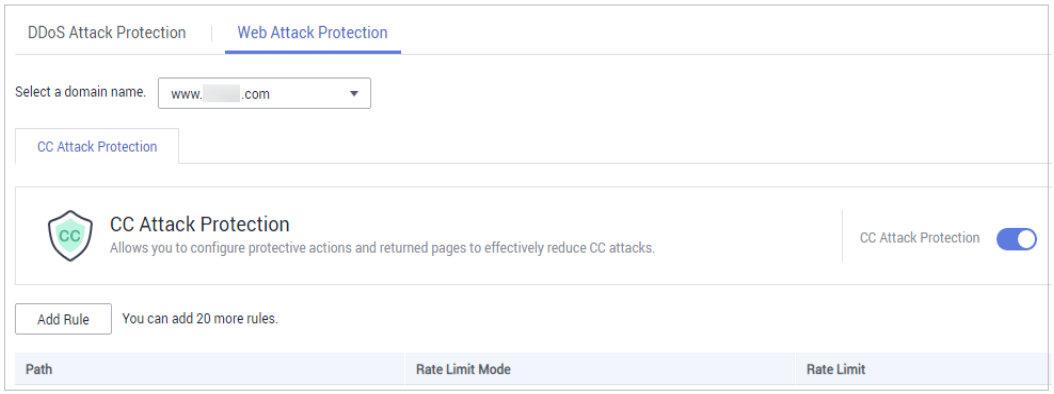
Figure 3-32 Entering the **Protection Policies** page



 Copyright © Huawei Technologies Co., Ltd.

Step 3 Click the **Web Attack Protection** tab and select the domain name for which you want to configure a protection policy from the **Select a domain name** drop-down list.

Figure 3-33 Web attack protection



Step 4 Set **CC Attack Protection** to  to enable the protection.

NOTE

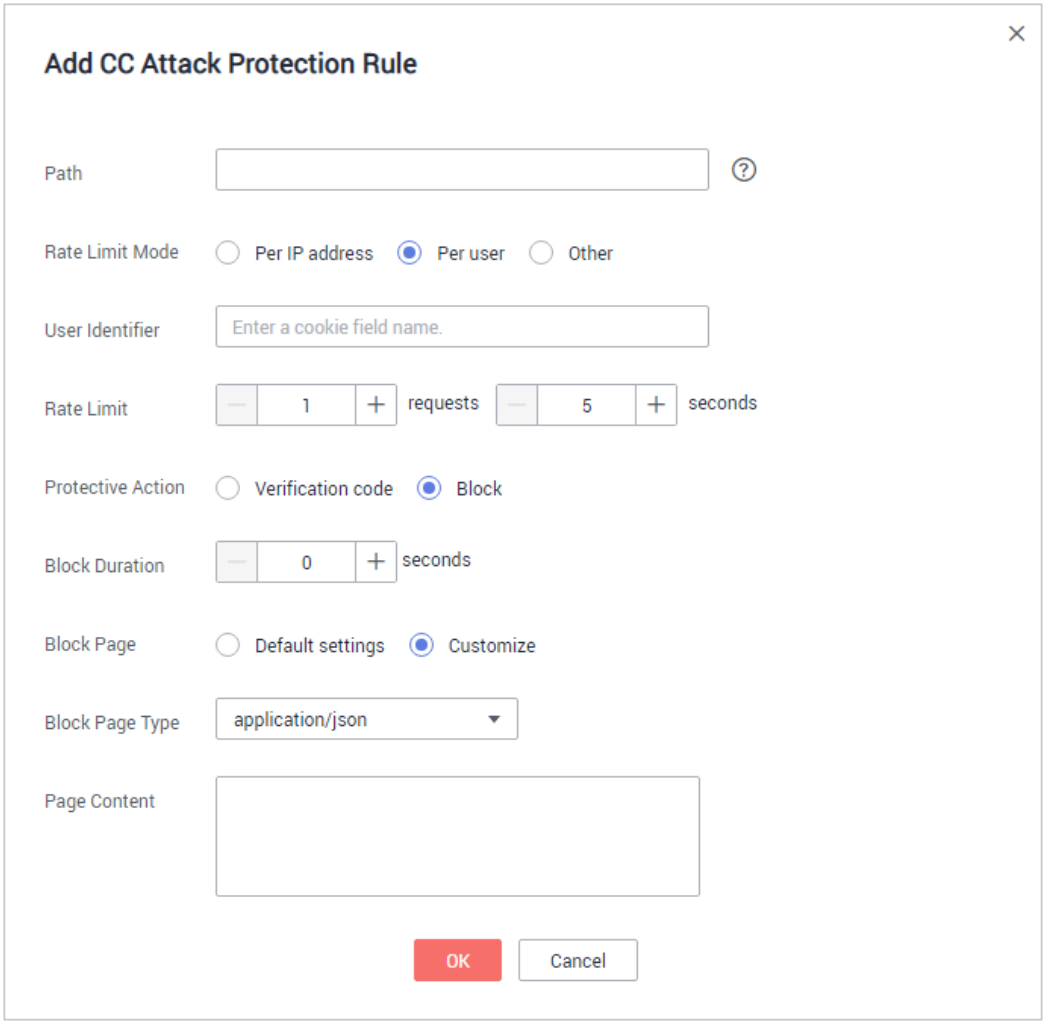
- Traffic Attack Protection is enabled by default.
- Before enabling **CC Attack Protection**, you need to enable **Basic Web Protection**.

Step 5 Click **Add Rule**.

Step 6 In the displayed dialog box, set required parameters. **Table 3-8** describes the parameters.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-34 Adding a CC attack protection rule



 Copyright © Huawei Technologies Co., Ltd.

Table 3-8 Parameters for adding a CC attack protection rule

Parameter	Description	Example Value
Path	Specifies the URL to be protected against CC attacks. The value does not contain a domain name. It supports the following matching rules: • Prefix match: Enter a value ending with an asterisk (*), and this value will be used as a prefix in the match. For example, if the path to be protected is **/admin/test.php** or **/adminabc**, you can set **Path** to **/admin***. • Exact match: Enter a value exactly the same as the path to be protected. For example, if the path to be protected is **/admin**, set **Path** to **/admin**. **NOTE** • The path does not support regular expressions. • The path cannot contain two or more consecutive slashes, for example, **///admin**. If you enter **///admin**, the WAF engine converts **///** to **/**.	/admin*

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Rate Limit Mode	• **Per IP address**: A web visitor is identified by the IP address. • **Per user**: A web visitor is identified by the cookie key value. • **Other**: A web visitor is identified by the **Referer** field (user-defined request source). **NOTE** If you set **Rate Limit Mode** to **Other**, enter a complete URL containing the domain name in the **Content** text box for the **referer** field. The **Content** field supports prefix match and exact match only, and cannot contain two or more consecutive slashes, for example, **/// admin**. If you enter **///admin**, the WAF engine converts it to **/admin**. For example, if **Path** is **/admin** and you do not want visitors to access the page from **www.test.com**, set **Content** to **http://www.test.com**.	Per user
User Identifier	Specifies an attribute variable in the cookie that uniquely identifies the web visitor. You need to set this parameter if **Rate Limit Mode** is **Per user**. This value supports only the exact match and does not support regular expressions. If you do not set the cookie key value, WAF will automatically assign one. For example, if a website uses the **name** field in the cookie to uniquely identify a web visitor, you can enter the **name** field for **User Identifier**.	name
Rate Limit	Specifies the number of requests allowed from a web visitor in the rate limiting period. Access from the visitor is denied once the limit is reached.	10 requests 60 seconds

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Protective Action	Specifies the action to be taken once the maximum number of requests is reached. Options are **Verification code** and **Block**. • **Verification code**: A verification code is displayed when the number of requests reaches the maximum limit within a specified period. Upon completing the verification, you are no longer restricted by the maximum number of requests allowed. • **Block**: Requests are blocked if the maximum number of requests is reached. **NOTE** If **Rate Limit Mode** is **Other**, **Protective Action** can only be **Block**.	Block
Block Duration	Specifies the period within which access is blocked. An error page is displayed in this period.	600 s
Block Page	Specifies the error page displayed when the maximum number of requests has been reached. This parameter is mandatory only when **Protective Action** is **Block**. Available options are **Default settings** and **Customize**. • If you select **Default settings**, the default block page is displayed. • If you select **Customize**, customize a page to be displayed.	Customize
Block Page Type	Specifies the type of the page you will customize. You can select **application/json**, **text/html**, or **text/xml**.	text/html

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Page Content	Specifies the content to be displayed on the page you will customize.	<html><body>Forbidden</body></html>

Step 7 Click **OK**. The CC attack protection rule is displayed in the CC rule list.

----End

3.6 Adding a CNAME Record

AAD supports A record-based access and CNAME-based access. CNAME-based access is recommended.

NOTICE

- When adding a CNAME record, you must delete the existing A records from the DNS record set. If they are not deleted, you will fail to add the new record because resolution conflicts may occur. Some DNS service providers support the change from A records into CNAME records, and this change does not affect domain name resolution.
- The DNS configuration may affect current service operating. Therefore, you are advised to configure DNS during off-peak hours.

CNAME-based access has the following advantages:

- Easy to use. You only need to modify the resolution configuration at a time during domain name resolution (for example, on HUAWEI CLOUD DNS).
- Automatic line switchover. If an AAD line encounters an exception, the CNAME resolution can be automatically switched to other properly working lines.
- Service continuity. In a three-line package service, if a line is attacked and blocked by a black hole, AAD automatically uses the other available lines to complete CNAME resolution, ensuring service availability.

Copyright © Huawei Technologies Co., Ltd.

The configuration mechanism is similar for each DNS service provider, with small differences in steps. This topic uses the Domain Name Service (DNS) on HUAWEI CLOUD as an example.

Adding a CNAME Record

If you have configured domain name access in **Connecting a Non-website Service to AAD**, you obtain a CNAME record from AAD. Add the CNAME record to DNS.

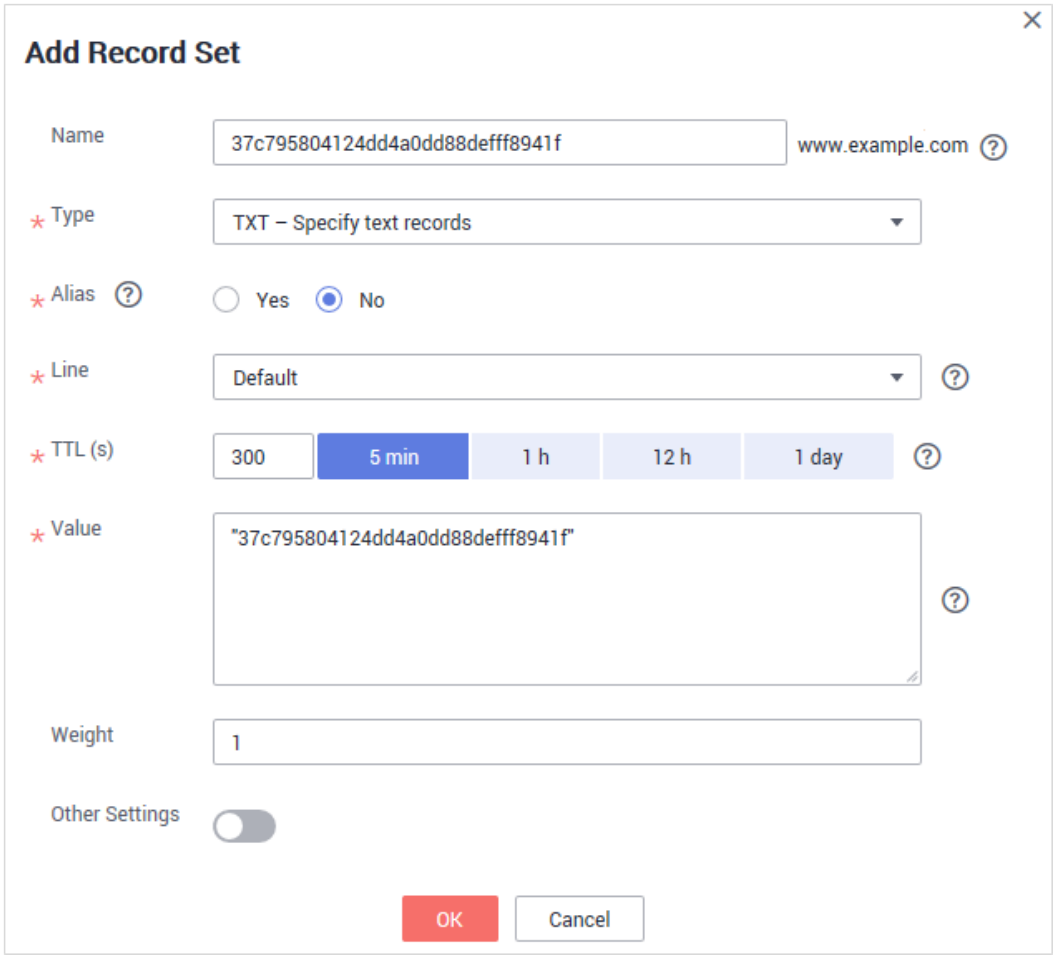
Step 1 Log in to the management console. Click **Service List**. Under **Network**, click **Domain Name Service**. The **DNS** console is displayed.

Step 2 In the navigation pane on the left, choose **DNS Resolution** > **Public Zones**. Then click the desired domain name in the list.

Step 3 Click **Add Record Set**.

Step 4 Add the CNAME record. For details, see **Table 3-9**.

Figure 3-35 Adding a record set



 Copyright © Huawei Technologies Co., Ltd.

Table 3-9 Parameters for adding a CNAME record

Parameter	Description
Name	Domain name alias (You do not need to manually add the suffix.)
Type	Record set type Select **CNAME – Map one domain to another**.
Alias	Whether to associate the record set with a cloud resource name Select **No**.
Line	Resolution line. The DNS server will return the IP address of the specified line based on the source of visitors. Select **Default**.
Value	Domain name mapped to the alias Enter the CNAME record obtained from AAD.

Step 5 Click **OK**.

----End

The DNS configuration takes effect after a period of time. In this period, you can test the domain name resolution using some online test tools such as 17ce and China Webmaster.

Adding an A Record

If you added a forwarding rule without configuring domain name access in **Connecting a Non-website Service to AAD**, add an A record to DNS.

The following steps use the China Telecom line package as an example.

Step 1 Log in to the management console. Click **Service List**. Under **Network**, click **Domain Name Service**. The **DNS** console is displayed.

Step 2 In the navigation pane on the left, choose **DNS Resolution** > **Public Zones**. Then click the desired domain name in the list.

Step 3 Click **Add Record Set**.

Step 4 Add an A record. For details, see **Table 3-10**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-36 Adding an A record set

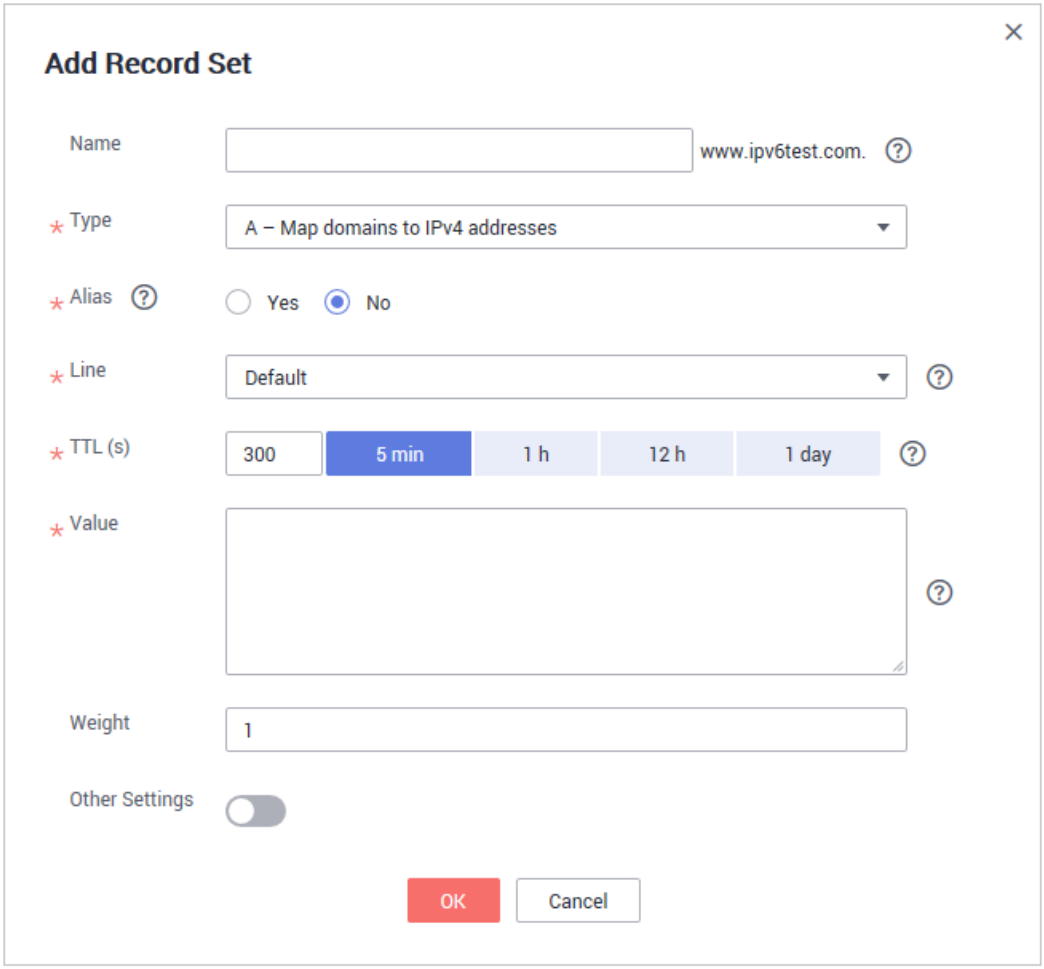


Table 3-10 Parameters for adding an A record - China Telecom

Parameter	Description
Name	Domain name (You do not need to manually add the suffix.)
Type	Record set type Select **A – Map domains to IPv4 addresses**.
Alias	Whether to associate the record set with a cloud resource name Select **No**.
Line	Resolution line. The DNS server will return the IP address of the specified line based on the source of visitors. Select **ISP** and **China Telecom**.
Value	IPv4 addresses mapped to the domain name Enter the high-defense IP address of the China Telecom line.

Copyright © Huawei Technologies Co., Ltd.

Step 5 Click **OK**.

----End

The DNS configuration takes effect after a period of time. In this period, you can test the domain name resolution using some online test tools such as 17ce and China Webmaster.

3.7 Viewing Protection Details

Scenarios

After your services are connected to AAD, you can view the DDoS and CC protection details of different lines in an AAD instance on the dashboard to learn about the current network security state.

On the **Dashboard** page, you can view the following protection details:

- DDoS Attack Protection

  The **Dashboard** page gives an overview of the peak ingress traffic, peak attack traffic, and number of DDoS attacks, and shows the attack type distribution, DDoS attack events, and top 5 attack types scrubbed on two tab pages **Traffic** and **Packet Rate**.

- CC Attack Protection

  The **Dashboard** page gives an overview of number of requests and attacks, attack type distribution, and top 5 attacked source IP addresses.

Precautions

- The protection details cannot be downloaded.
- On the **Dashboard** page, you can view the following protection details of the following time ranges:
  - DDoS Attack Protection

    You can select an AAD instance and a line to view the DDoS protection details of last 24 hours, last 3 days, last 7 days, last 30 days, or a custom period (maximum of last 90 days).
  - CC Attack Protection

    You can select a specific domain name or all domain names from the domain name drop-down list to view the CC protection details of yesterday, today, last 3 days, last 7 days, or last 30 days.

Prerequisites

- You have obtained the username and password for logging in to the management console.
- You have purchased an AAD instance.

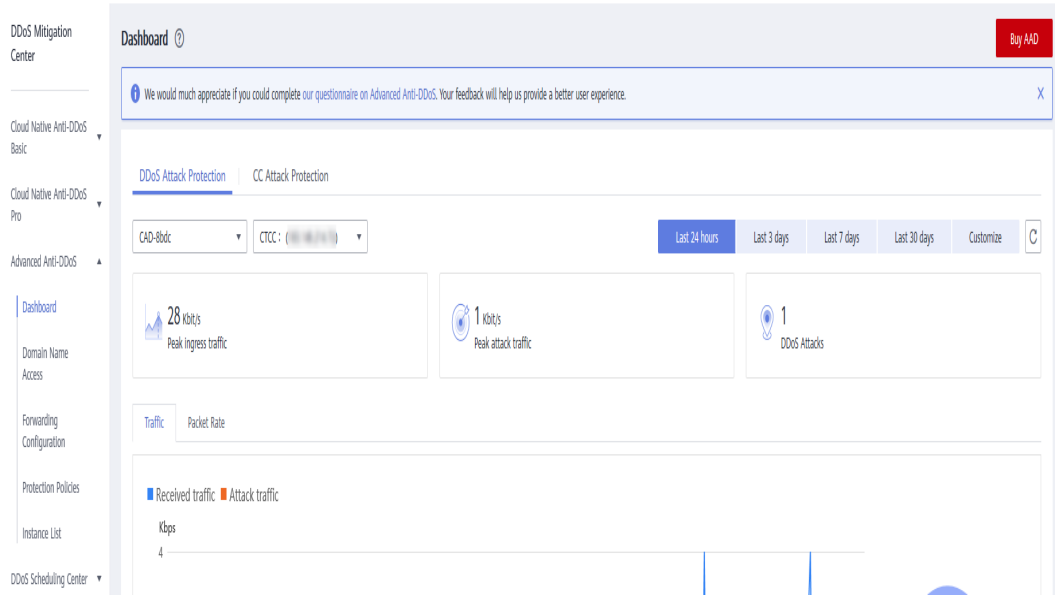
Viewing DDoS Attack Protection Details

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

 Copyright © Huawei Technologies Co., Ltd.

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.

Figure 3-37 DDoS attack protection entry



Step 3 Select an instance, line, and time range (last 24 hours, last 3 days, last 7 days, last 30 days, or a custom period). **Table 3-11** describes the related parameters.

Table 3-11 Parameter description

Parameter	Description
Peak ingress traffic	Maximum traffic accessing the specified IP address of a specified instance per second
Peak attack traffic	Maximum traffic attacking the specified IP address of a specified instance per second
DDoS Attacks	Number of DDoS attacks launched on the specified IP address of a specified instance
Traffic	Trend charts of received traffic and attack traffic
Packet Rate	Trend charts of received packets and attack packets

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Attack Type Distribution	Types of attack events • You can click any colored area in the attack distribution circle under **Attack Type Distribution** to view the type, count, and proportion of an attack. • To stop displaying information about a specific type of attacks, click the legend with the same color to the right of the circle.
Top 5 Attack Types Scrubbed (Kbit/s)	Top 5 attack types that have been scrubbed
DDoS Attack Events	Details about DDoS attacks

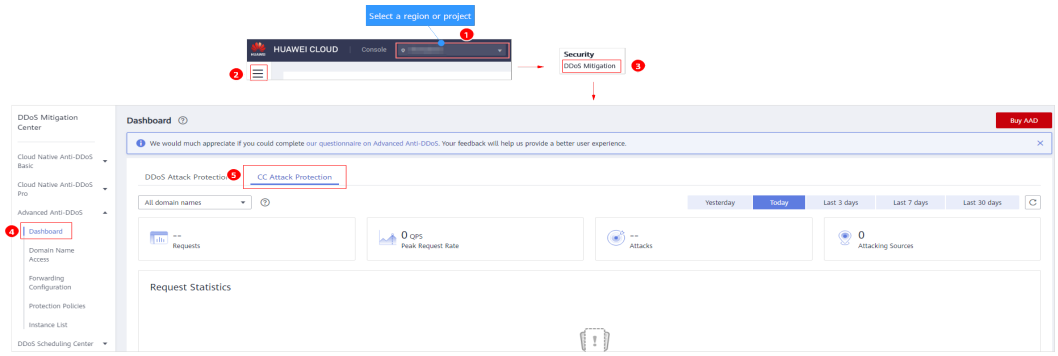
----End

Viewing CC Attack Protection Details

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 **CC Attack Protection** tab.

Figure 3-38 CC attack protection entry



Step 3 Select the target domain name from the **All domain names** drop-down list (select one domain name or retain all domain names).

In the upper right corner of the page, select a time range (yesterday, today, last 3 days, last 7 days, or last 30 days). **Table 3-12** describes the related parameters.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-12 Parameter description

Parameter	Description
Requests	Total number of requests to a specified domain name If you select **All domain names**, the total number of requests to all domain names with WAF enabled is collected.
Peak Request Rate	Maximum number of requests to a specified domain name per second If you select **All domain names**, the maximum number of requests to all domain names with WAF enabled is collected per second.
Attacks	Number of attacks towards a specified domain name
Attacking Sources	Number of sources that attack a specified domain name
Request Statistics	• Requests: trend chart for the access requests • Attacks: trend chart for attacks
Attack Type Distribution	Types of attack events • You can click any colored area in the attack distribution circle under **Attack Type Distribution** to view the type, count, and proportion of an attack. • To stop displaying information about a specific type of attacks, click the legend with the same color to the right of the circle.
Top 5 Attacking Source IP Addresses	Top 5 attacking source IP addresses and their cumulative number of attacks

----End

3.8 Enabling Alarm Notification

After you enable the alarm notification, a notification message will be sent to you through the method you have configured when:

- The IP address is under the DDoS attacks.
- The additional fees are incurred for the traffic exceeds the basic protection bandwidth threshold.

 Copyright © Huawei Technologies Co., Ltd.

You will receive an alarm notification in the morning of the next day.

Precautions

- The Simple Message Notification (SMN) service is a paid service. For details about the price, see **SMN Product Pricing Details**.
- Before setting alarm notification, you are advised to create a message topic in the SMN service as an administrator. For details, see **Publishing a Message**.

Prerequisites

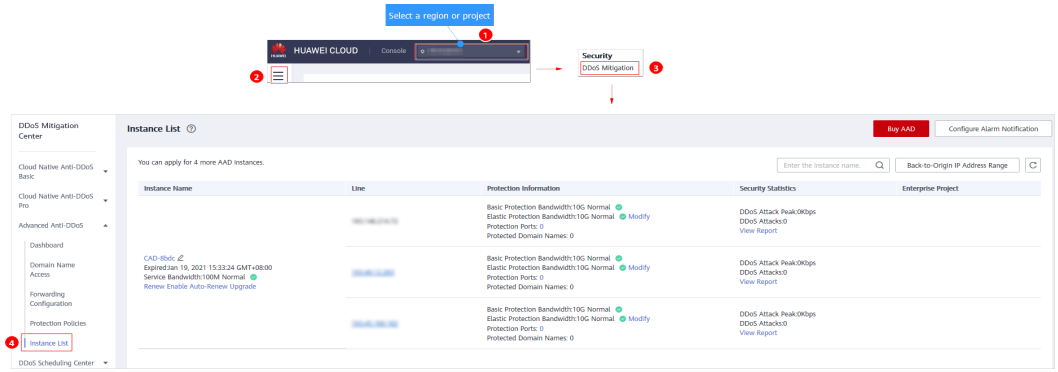
You have purchased an AAD instance.

Procedure

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

Step 2 Choose **Advanced Anti-DDoS** > **Instance List** in the left navigation pane.

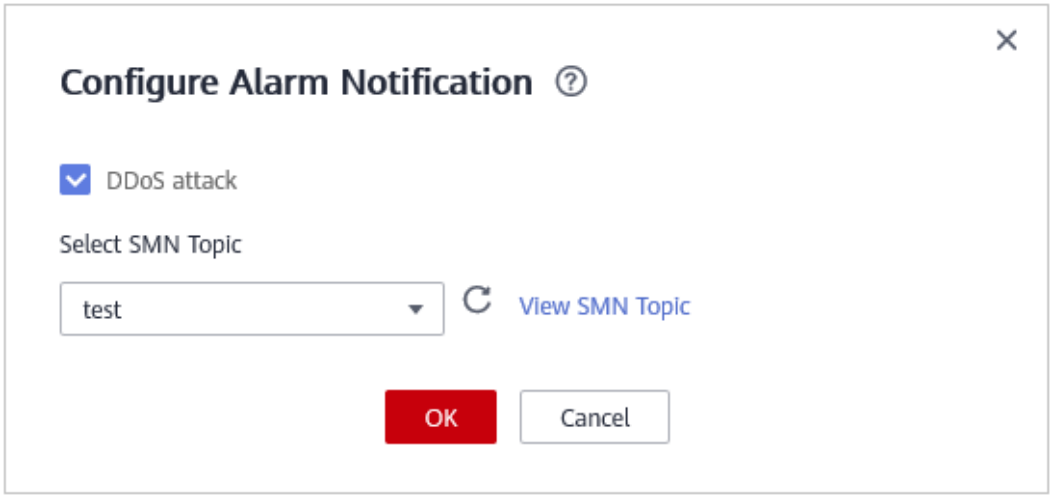
Figure 3-39 Switching to instance list page



Step 3 In the upper right corner of the instance list, click **Configure Alarm Notification**.

Step 4 In the displayed **Configure Alarm Notification** dialog box, select **DDoS attack**.

Figure 3-40 Configure Alarm Notification



 Copyright © Huawei Technologies Co., Ltd.

Select an existing topic from the drop-down list or click **View SMN Topic** and create an SMN topic on the displayed page for configuring the terminals for receiving alarm notifications.

Perform the following steps to create a topic:

1. Create a topic by referring to **Creating a Topic**.
2. You can add one or more subscriptions to a topic by configuring the phone number, email address, function, platform application endpoint, DMS endpoint, or HTTP/HTTPS endpoint for receiving alarm notifications. For details, see **Adding a Subscription**.
3. Confirm the subscription. After the subscription is added, confirm the subscription.

For details about topics and subscriptions, see *Simple Message Notification User Guide*.

Step 5 Click **OK**.

NOTE

To disable the alarm notification function, deselect **DDoS attack** in **Figure 3-40** and click **OK**.

----End

3.9 Managing an Instance

3.9.1 Viewing AAD Instance Information

Scenarios

This section describes how to view information about an Advanced Anti-DDoS instance.

Prerequisites

- You have obtained an account and its password to log in to the management console.
- You have purchased an AAD instance.

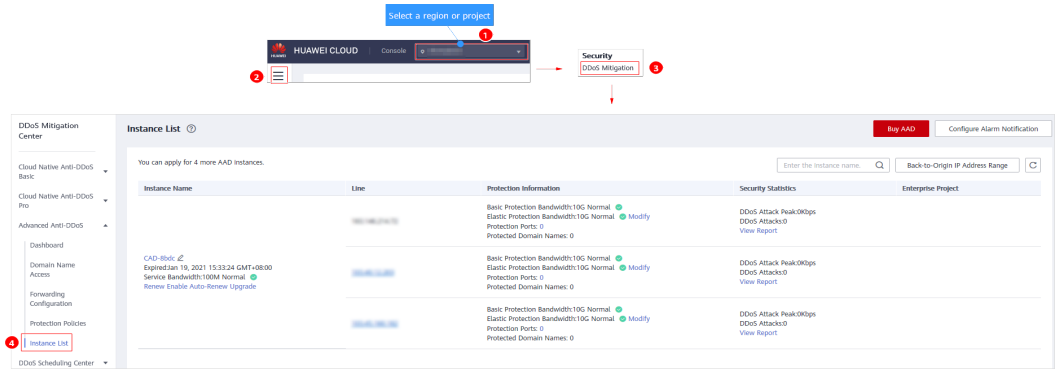
Procedure

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

Step 2 Choose **Advanced Anti-DDoS** > **Instance List** in the left navigation pane.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-41 Switching to instance list page



Step 3 On the displayed page, view the details about an instance. **Table 3-13** describes the parameters.

Table 3-13 Parameter description

Parameter	Description
Instance Name	• Name of an AAD instance. You can click on the right to change the name. • Time when the instance expires • **Recharge** button of the instance • Service bandwidth and protection bandwidth statuses of the instance
Line	Line and IP address information about an instance
Protection Information	Basic protection bandwidth, elastic protection bandwidth, number of protection ports, and number of protected domain names of the instance **NOTE** To change the elastic protection bandwidth, click **Edit**.
Security Statistics	Protection statistics about the instance, including: • Peak attack traffic • Number of attacks
Operation	• Click **View Report** to view the normal traffic and attack traffic. • Click **Configure** to configure forwarding rules for the instance.

----End

3.9.2 Changing the Name of an AAD Instance

Scenarios

This section describes how to change an AAD instance name.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

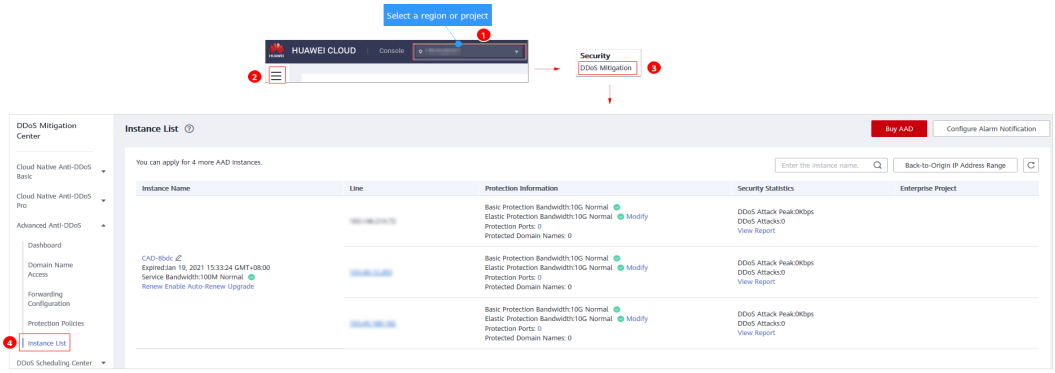
- You have obtained the username and password for logging in to the management console.
- You have purchased an AAD instance.

Procedure

Step 1 Log in to the management console.

Step 2 Choose **Advanced Anti-DDoS** > **Instance List** in the left navigation pane.

Figure 3-42 Switching to instance list page



Step 3 In the row containing the desired instance, click next to the instance name.

Step 4 Enter a new instance name in the text box and click .

----End

3.9.3 Changing the Elastic Protection Bandwidth

Scenarios

You can change the elastic protection bandwidth if it is insufficient.

This section describes how to change the elastic protection bandwidth for an AAD instance.

NOTICE

The elastic protection bandwidth of each instance can be changed for up to three times per day.

Prerequisites

- You have obtained a username and password for logging in to the management console.
- You have purchased an AAD instance.

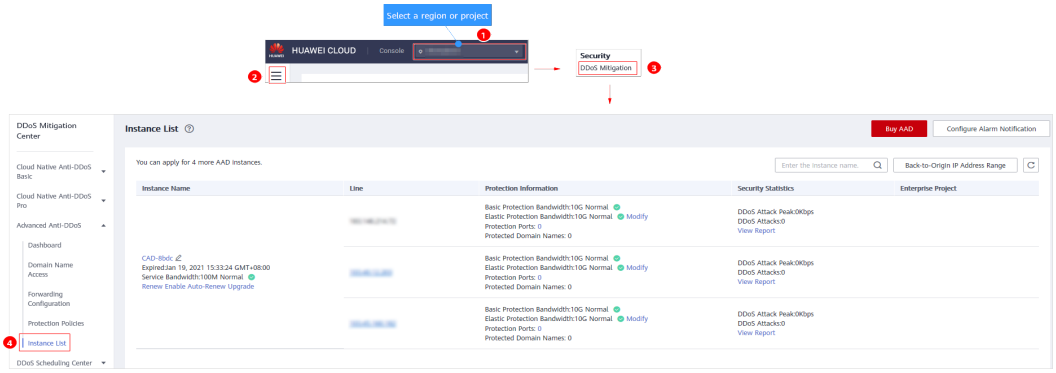
Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the management console.

Step 2 Choose **Advanced Anti-DDoS** > **Instance List** in the left navigation pane.

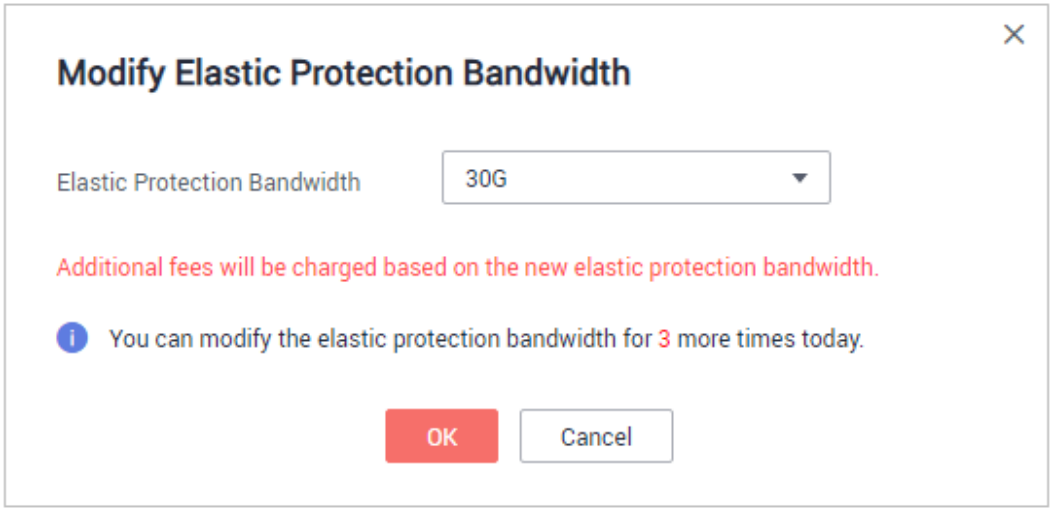
Figure 3-43 Switching to instance list page



Step 3 In the **Protection Information** column of the row containing the desired instance, click **Edit**.

Step 4 In the dialog box that is displayed, set a new bandwidth and click **OK**.

Figure 3-44 Dialog box for modifying elastic protection bandwidth



----End

3.10 Managing a Forwarding Rule

3.10.1 Viewing Information About a Forwarding Rule

Scenarios

This topic describes how to view information about a forwarding rule.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

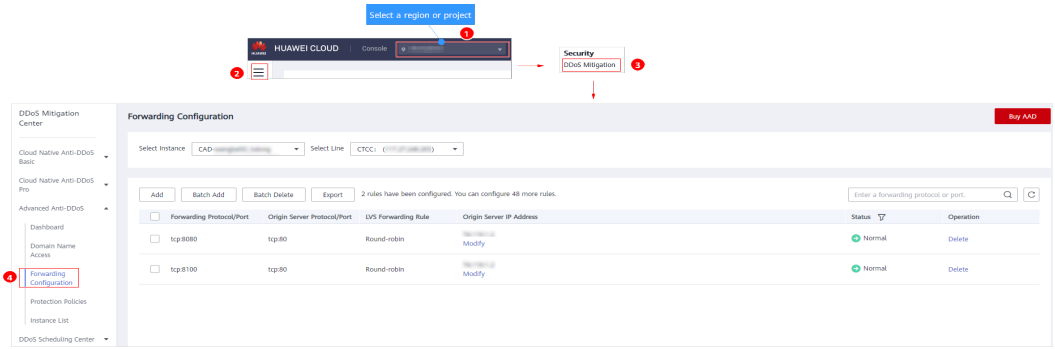
- You have obtained the username and password for logging in to the management console.
- You have configured forwarding rules for AAD instances.

Procedure

Step 1 Log in to the management console.

Step 2 Follow the procedure in the following figure to enter the **Forwarding Configuration** page.

Figure 3-45 Forwarding configuration entry



Step 3 View information about the desired forwarding rule.

Table 3-14 Parameter description

Parameter	Description
Forwarding Protocol/Port	Forwarding protocol and port for the rule
Origin Server Protocol/Port	Origin server protocol and port for the rule
LVS Forwarding Rule	Forwarding rule of the Linux Virtual Server (LVS)
Origin Server IP Address	Origin server IP address added to the rule Click **Modify** if you need to change the origin server IP address.
Status	• Running status of the forwarding rule
Operation	You can click **Delete** to delete the forwarding rule.

----End

 Copyright © Huawei Technologies Co., Ltd.

3.10.2 Changing an Origin Server IP Address

Scenarios

You can change the origin server IP address in the forwarding rule whenever necessary during defense.

Prerequisites

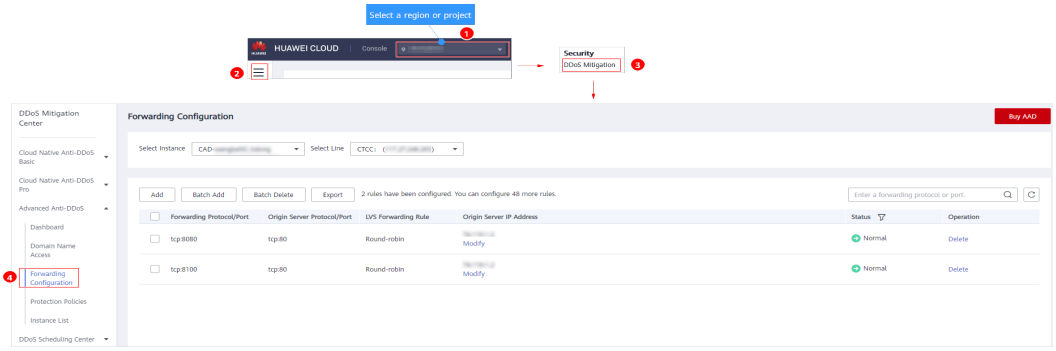
- You have obtained the username and password for logging in to the management console.
- You have configured forwarding rules for AAD instances.

Procedure

Step 1 Log in to the management console.

Step 2 Follow the procedure in the following figure to enter the **Forwarding Configuration** page.

Figure 3-46 Forwarding configuration entry



Step 3 Locate the row containing the target forwarding rule and click **Modify** in the **Origin Server IP Address** column.

Step 4 In the displayed **Modify Origin Server IP Address** dialog box, change the IP address of the origin server for the forwarding rule.

NOTICE

Enter a valid public IP address.

Step 5 Click **OK**.

----End

3.10.3 Deleting a Forwarding Rule

Scenarios

You can delete a specific forwarding rule if it is unnecessary.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

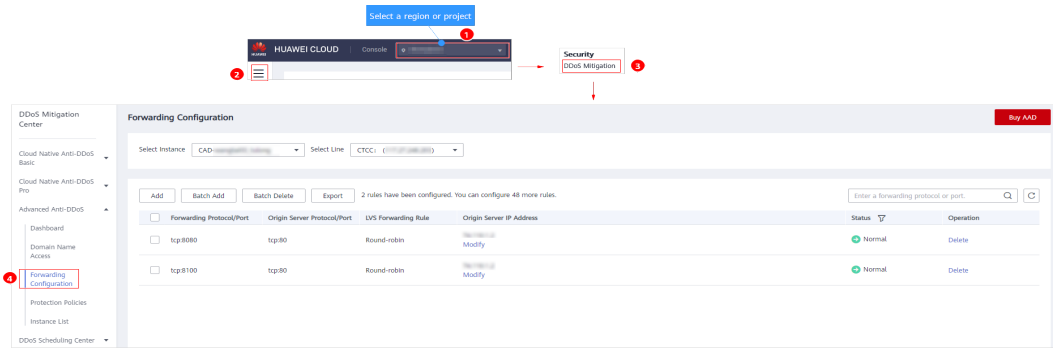
- You have obtained the username and password for logging in to the management console.
- You have configured forwarding rules for AAD instances.

Procedure

Step 1 Log in to the management console.

Step 2 Follow the procedure in the following figure to enter the **Forwarding Configuration** page.

Figure 3-47 Forwarding configuration entry



Step 3 Delete forwarding rules.

- Deleting one forwarding rule
  a. Locate the row containing the target forwarding rule and click **Delete** in the **Operation** column.
  b. Click **OK** in the displayed dialog box.
- Deleting multiple forwarding rules
  a. Select the target forwarding rules and click **Delete** above the forwarding rule list.

  NOTE

  You can batch delete a maximum of 50 forwarding rules at a time. (Up to 50 forwarding rules can be displayed per page.)

  b. Click **OK** in the displayed dialog box.

----End

3.10.4 Exporting a Forwarding Rule

Scenarios

- Back up all forwarding rules of an instance by exporting them.
- Using the exported file, modify forwarding rules quickly and batch add them to the console.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

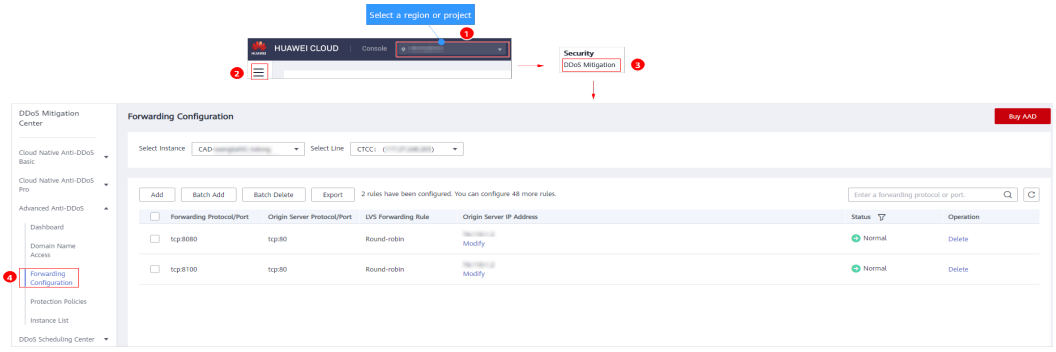
- You have obtained the username and password for logging in to the management console.
- You have configured forwarding rules for AAD instances.

Procedure

Step 1 Log in to the management console.

Step 2 Follow the procedure in the following figure to enter the **Forwarding Configuration** page.

Figure 3-48 Forwarding configuration entry



Step 3 Click **Export** to export all forwarding rules to the local computer.

Step 4 View the file of exported forwarding rules **rules.txt**.

----End

3.11 Managing a Domain Name

3.11.1 Viewing Information About a Domain Name

Scenarios

This topic describes how to view information about a domain name.

Prerequisites

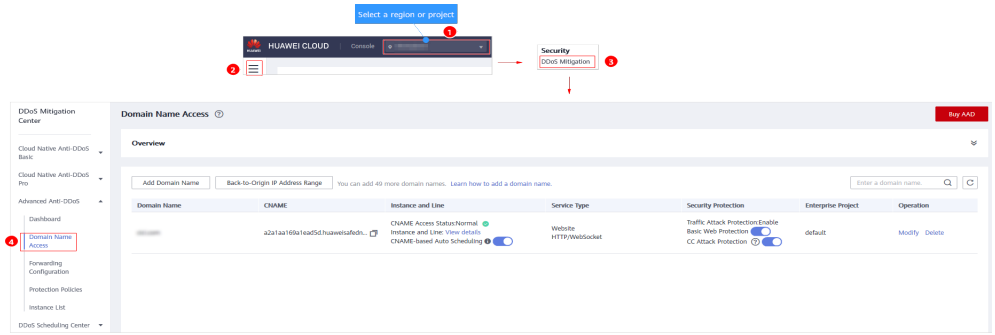
At least one domain name has been added for protection.

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 3-49 Domain Name Access page



Step 3 View information about the domain name.

Table 3-15 Parameter description

Parameter	Description
Domain Name	Protected domain name
CNAME	• CNAME record obtained for the domain name after a CNAME resolution • Click to copy the CNAME record.
Instance and Line	• CNAME-based access status of the domain name • Click **View details** to view details about the line of the domain name. • Enable **CNAME-based Auto Scheduling** so that DNS resolution will automatically schedule the traffic if the high-defense IP address is blocked by a black hole.
Service Type	• Service type of the domain name • Locate the row that contains **HTTPS/WebSockets** certificate, click **Update** in the **Service Type** column to update the certificate. For details, see **Updating a Certificate**.
Security Protection	Status of traffic attack protection, basic web protection, and CC attack protection • For a website service whose **Origin Server Type** is set to **IP address**, you can enable basic web protection and CC attack protection for your domain name. • For a website service whose **Origin Server Type** is set to **Domain name**, you do not need to enable basic web protection and CC attack protection for your domain name. • For a non-website service, only traffic attack defense is provided and enabled by default.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Operation	• You can click **Modify** to modify the domain name access configuration. • You can click **Delete** to delete a domain name.

----End

3.11.2 Enabling Basic Web Protection and CC Attack Protection

Scenarios

After adding a domain name, you can enable **Basic Web Protection** and **CC Attack Protection** for it. Basic web protection and CC attack protection are provided only for the forwarding rules whose **Service Type** is **Website** and **Origin Server Type** is **IP address**.

Prerequisites

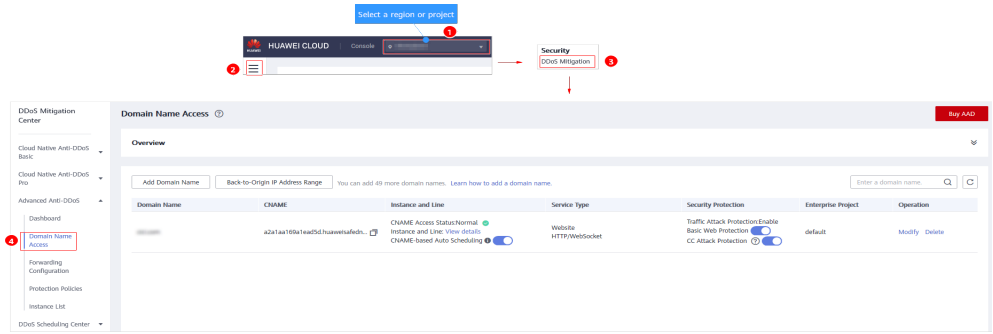
At least one domain name has been added for protection.

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 3-50 Domain Name Access page



Step 3 Set **CC Attack Protection** to  to enable the WAF protection and CC attack protection.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- Basic web protection and CC attack protection are provided only for the forwarding rules whose **Service Type** is **Website** and **Origin Server Type** is **IP address**.
- Traffic attack protection is enabled by default.
- Before enabling CC attack protection, you need to enable basic web protection.

----End

3.11.3 Updating a Certificate

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 (only TLS 1.0, TLS 1.1, and TLS 1.2 certificates are supported) to associate the certificate with the protected domain name.

- If the purchased certificate is about to expire, you are advised to purchase a new certificate before the expiration date and update the certificate associated with the domain name in AAD.
- To update the certificate associated with a domain name, you can associate a new certificate with the domain name in AAD.

NOTICE

- The certificate takes effect 1 minute after it is updated. Therefore, update certificates in off-peak hours.
- If a certificate expires, the origin server will be affected more severely than the host crash and website access failure. Therefore, you are advised to update the certificate before the certificate expires.
- Each domain name must be associated with a certificate. A wildcard domain name can only be used for a wildcard domain certificate. If you have not purchased a wildcard domain certificate and have only a single-domain certificate, you can only add domain names one by one in AAD.

Prerequisites

Website services have been connected to AAD.

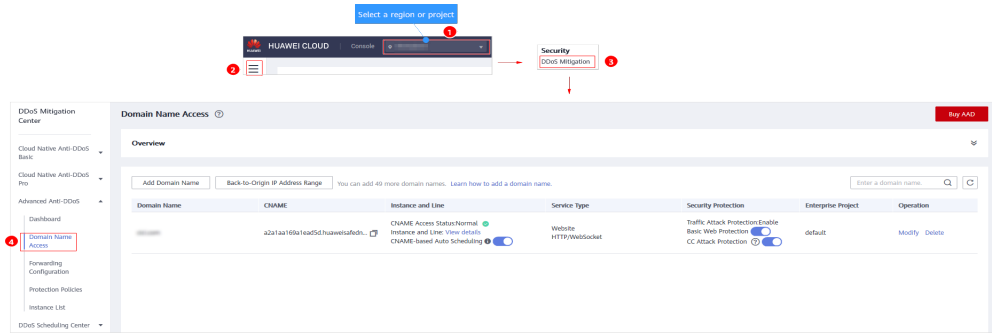
Procedure

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.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-51 Domain Name Access page



Step 3 Locate the row that contains the target domain name, and click **Update** in the **Service Type** column.

Step 4 In the displayed **Update Certificate** dialog box, upload a new certificate or select an existing certificate.

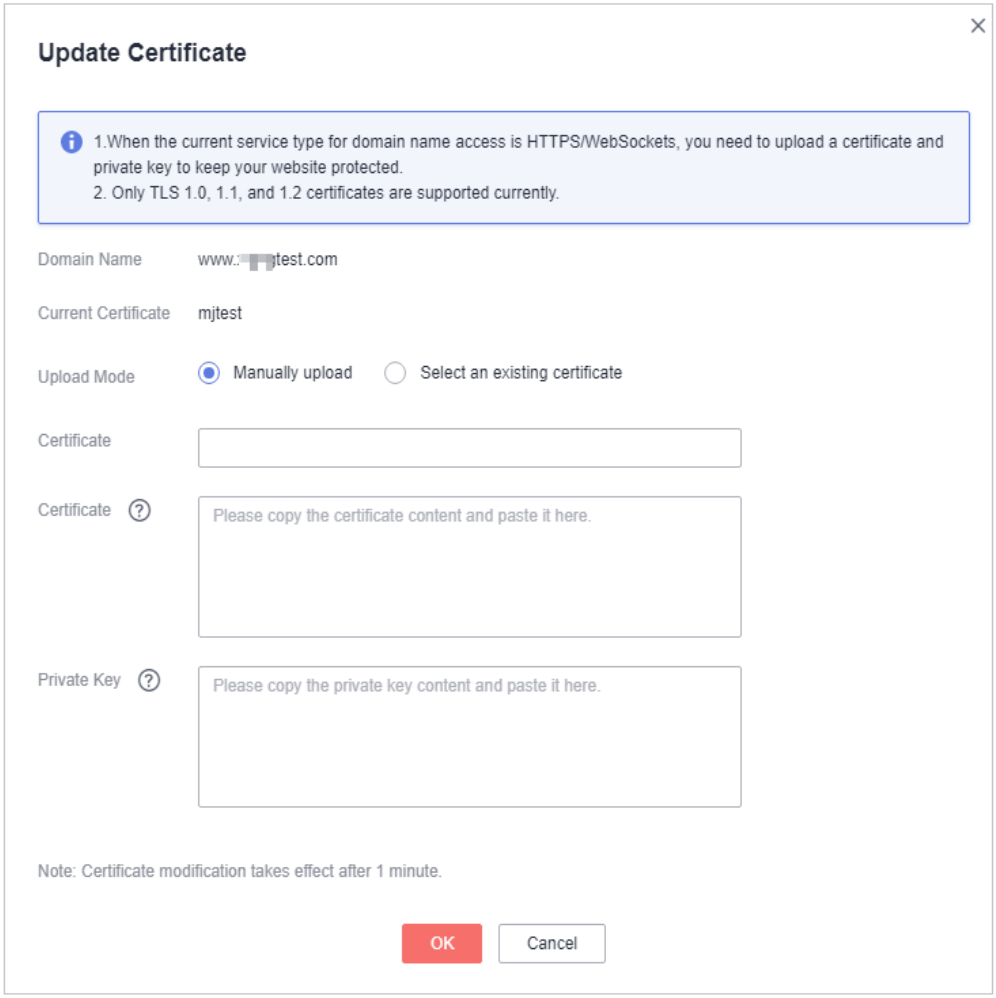
- If **Upload Mode** is set to **Manually upload**, enter the certificate name and paste the certificate content and private key to the target text box, as shown in **Figure 3-52**.

  NOTE

  AAD encrypts and saves the private key file to ensure its security.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-52 Manually uploading a certificate



Currently, AAD only supports PEM certificates. If the certificate is not in .pem format, before uploading it, convert it to .pem format by referring to **Table 3-16**.

Table 3-16 Certificate format conversion commands

Format	Conversion Method
CER/CRT	Rename the **cert.crt** certificate file to **cert.pem**.
PFX	Use OpenSSL to convert the certificate. Obtain a private key. For example, run the following command to convert **cert.pfx** into **cert.key**: **openssl pkcs12 -in cert.pfx -nocerts -out cert.key -nodes** Obtain a certificate. For example, run the following command to convert **cert.pfx** into **cert.pem**: **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**

Copyright © Huawei Technologies Co., Ltd.

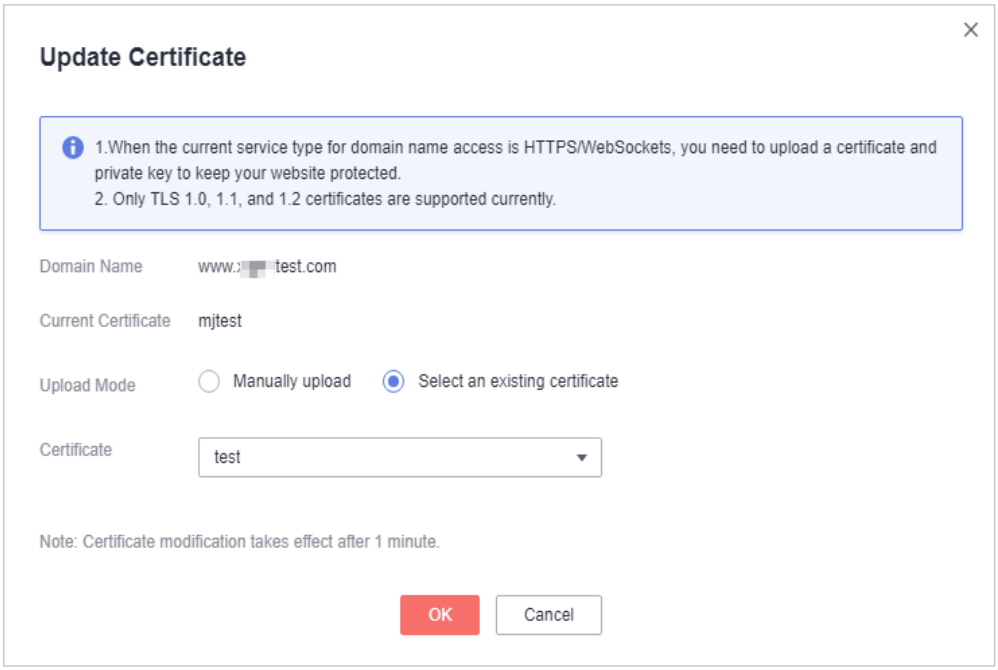
Format	Conversion Method
P7B	Use OpenSSL to convert the certificate. 1. Run the following command to convert the certificate: **openssl pkcs7 -print_certs -in incertificat.p7b -out cert.cer** 2. Obtain the certificate content in **cert.cer**. 3. Save the content in .pem format.
DER	Use OpenSSL to convert the certificate. 1. Obtain a private key. For example, run the following command to convert **privatekey.der** into **privatekey.pem**: **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** 2. Obtain a certificate. For example, run the following command to convert **cert.cer** into **cert.pem**: **openssl x509 -inform der -in cert.cer -out cert.pem**

NOTE

Before running the openssl command in Windows, ensure that the **openssl** tool has been installed.

- If **Upload Mode** is set to **Select an existing certificate**, select the uploaded certificate from the **Certificate** drop-down list.

Figure 3-53 Selecting an existing certificate



 Copyright © Huawei Technologies Co., Ltd.

Step 5 Click **OK**.

----End

3.11.4 Modifying Resolution Lines for High-Defense IP Addresses of a Domain Name

Scenarios

This topic describes how to:

- Disable DNS resolution for a high-defense IP address.
- Add a resolution line for a domain name.
- Delete a resolution line for a domain name.

Precautions

The modified resolutions lines take effect in about five minutes.

Prerequisites

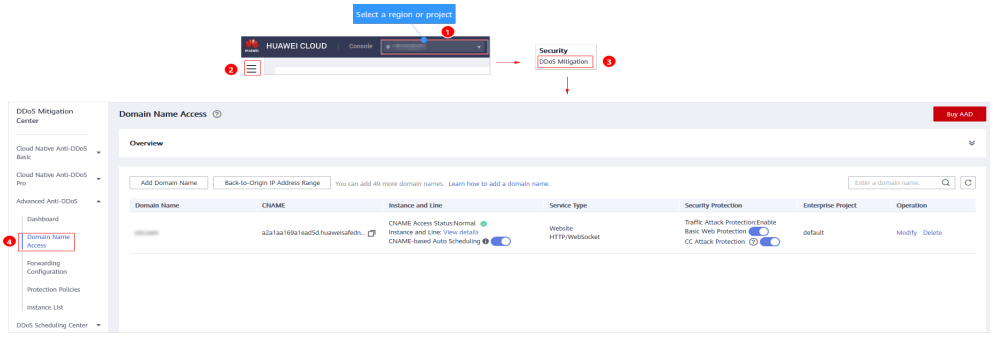
At least one domain name has been added for protection.

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 3-54 Domain Name Access page



Step 3 In the row containing the desired domain name, click **View details** in the **Instance and Line** column.

Step 4 Modify the resolution lines for the domain name.

- Disable DNS resolution for a high-defense IP address of the domain name.

  On the details page of the domain name, locate the target line and set **DNS Resolution** to  to disable DNS resolution for the high-defense IP address. After you disable DNS resolution, you can still use the A record for the high-defense IP address.

 Copyright © Huawei Technologies Co., Ltd.

- Add a resolution line for the domain name.
  a. On the details page of the domain name, click **Add Line**.
  b. In the **Add Line** dialog box, select new instances and lines and click **OK**.
  c. Set **DNS Resolution** to  to enable DNS resolution for the high-defense IP addresses.
- Delete a resolution line for the domain name.
  a. Disable DNS resolution for the high-defense IP address. For details, see **Disabling DNS Resolution**.
  b. Click **Delete Line**.
  c. Click **OK**.

----End

3.11.5 Modifying Domain Name Configuration

Scenarios

This topic describes how to modify the domain name configuration of a website service.

Prerequisites

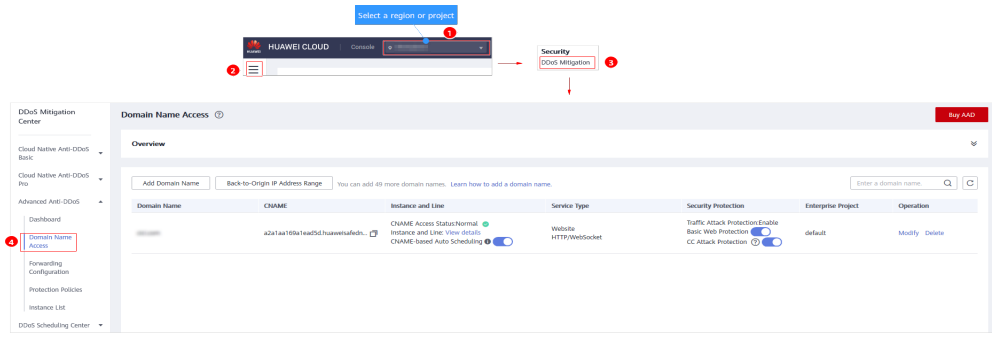
A website service domain name has been added.

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 3-55 Domain Name Access page



Step 3 In the row containing the desired domain name, click **Modify** in the **Operation** column.

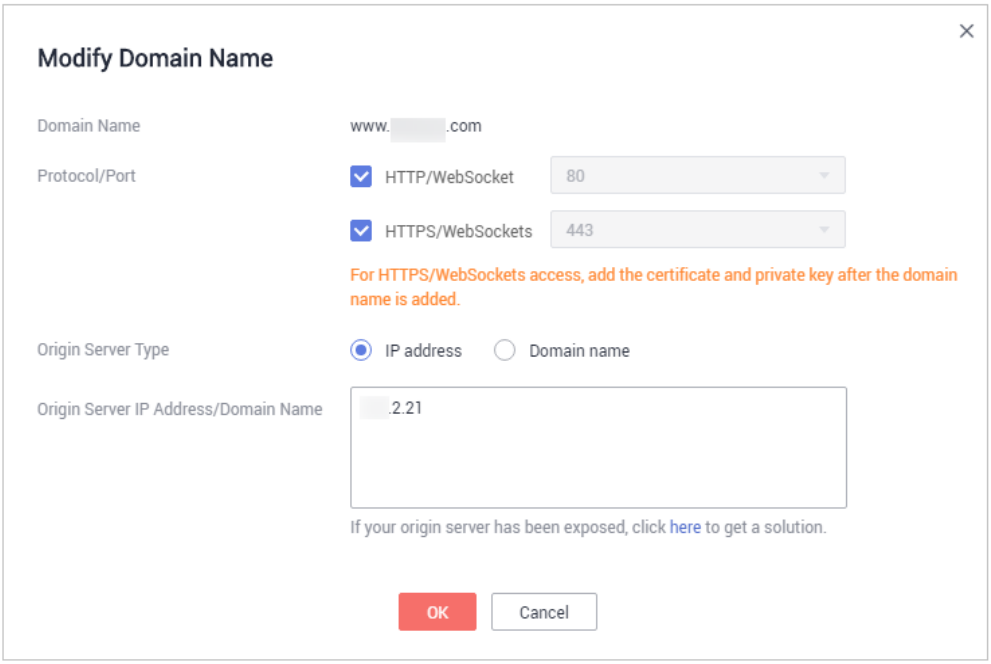
Step 4 In the **Modify Domain Name** dialog box that is displayed, modify the domain name configurations.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- If this protected domain name will share a high-defense IP address and port with another domain name, ensure that they have the same **Origin Server Type** value.
- To change the **Origin Server Type** value from **IP address** to **Domain name**, ensure that **Basic Web Protection** is disabled for the domain name.

Figure 3-56 Modifying domain name configurations



Step 5 Click **OK**.

----End

3.11.6 Deleting a Domain Name

Scenarios

You can delete domain names that you do not want to protect.

NOTICE

Before deleting a domain name, you need to ensure that the DNS domain name provider has changed the CNAME record to the real IP address. Otherwise, deleting the domain name will lead to service unavailability.

Prerequisites

At least one domain name has been added for protection.

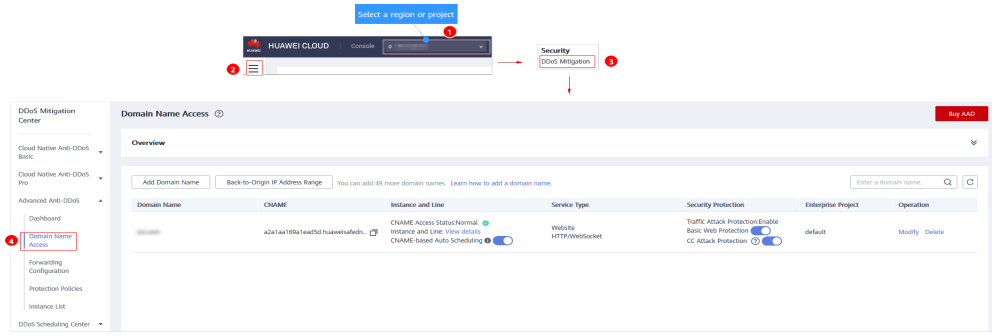
 Copyright © Huawei Technologies Co., Ltd.

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 3-57 Domain Name Access page



Step 3 Locate the row containing the target domain name and click **Delete** in the **Operation** column.

Step 4 Click **OK**.

----End

3.12 Viewing a Back-to-Origin IP Address Range

Scenarios

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.

This topic describes how to view a back-to-origin IP address range.

Prerequisites

- You have obtained the username and password for logging in to the management console.
- You have purchased an AAD instance.

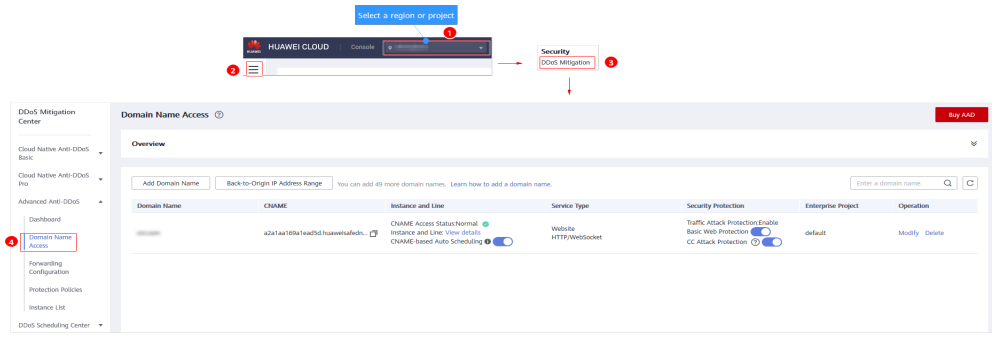
Procedure

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.

Copyright © Huawei Technologies Co., Ltd.

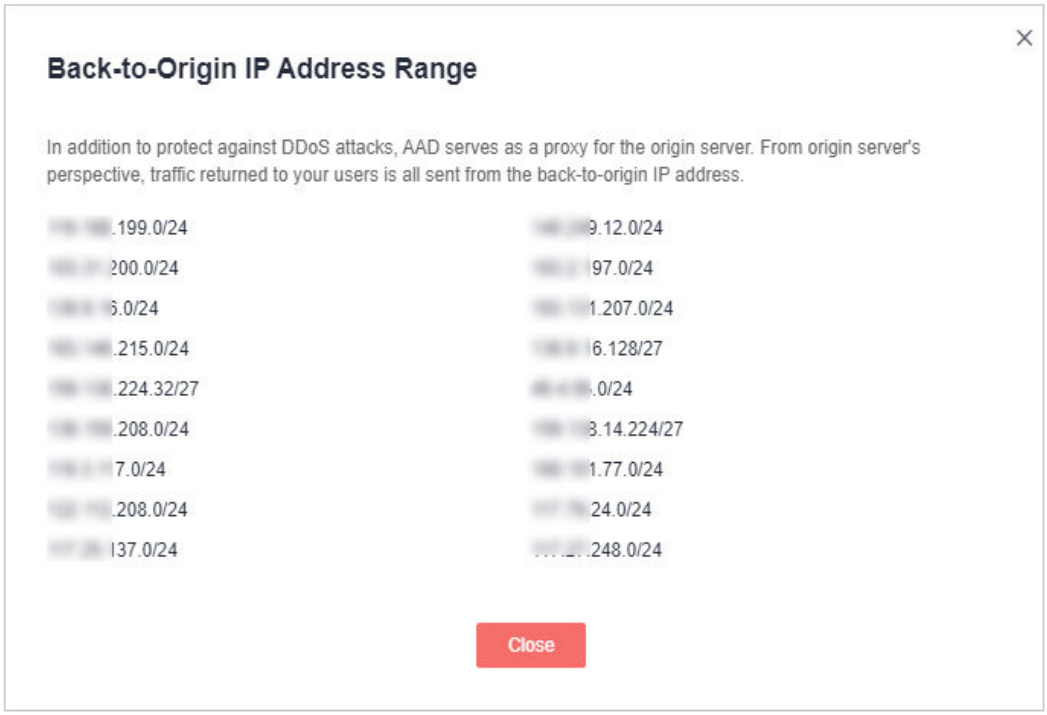
Figure 3-58 Domain Name Access page



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 3-59 Back-to-Origin IP Address Range



----End

3.13 Viewing a Protection Report

Scenarios

AAD shows normal traffic and attack traffic in two dimensions: byte and packet. You can view the normal traffic and attack traffic to know your network security situation.

This section describes how to view an AAD report.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

You can view the attack protection details (latest 90 days) of all AAD instances and all protected domain names on the AAD console.

Prerequisites

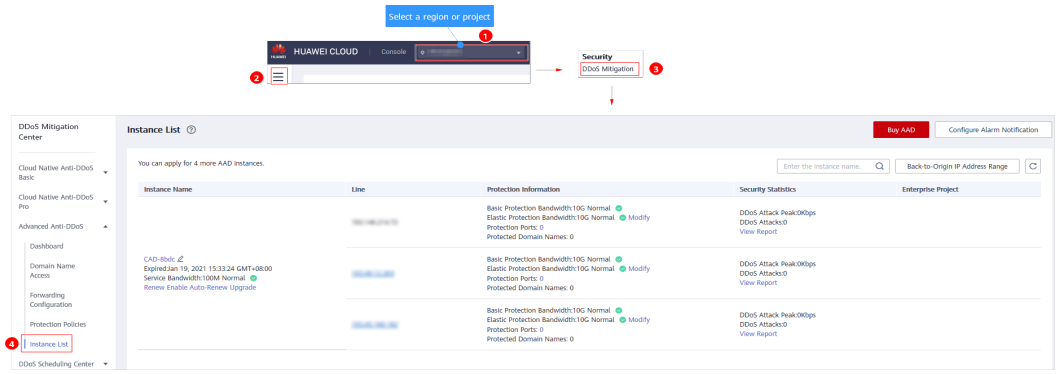
The services have been connected to AAD.

Procedure

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

Step 2 Choose **Advanced Anti-DDoS** > **Instance List** in the left navigation pane.

Figure 3-60 Switching to instance list page



Step 3 Select an instance and click **View Report** in the **Security Statistics** column.

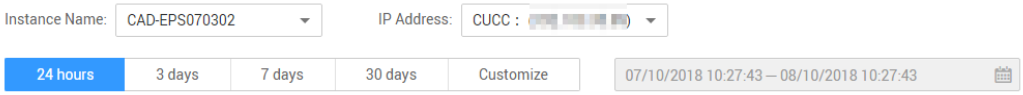
Step 4 Select the instance and IP address for which you want to view the protection report. Set the time range for the report, which includes the following options:

- **24 hours**: provides historical protection data of the last 24 hours. The minimum scale of the timeline is 10 seconds.
- **3 days**: provides historical protection data of the last 3 days. The minimum scale of the timeline is 5 minutes.
- **7 days**: provides historical protection data of the last 7 days. The minimum scale of the time axis is 1 hour.
- **30 days**: provides historical protection data of the last 30 days. The minimum scale of the time axis is 1 hour.
- Customize: Click , select the start date and time and end date and time, and click **OK**.

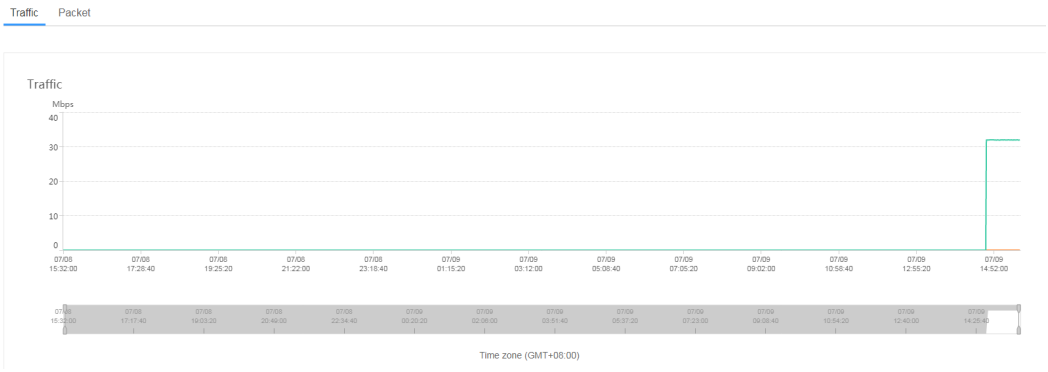
  You can query historical protection data of the last 90 days. The minimum scale of the timeline is determined based on the time range set and has the following options:

  – Time range ≤ 24 hours: The minimum scale is 10 seconds.
  – 24 hours < time range ≤ 3 days: The minimum scale is 5 minutes.
  – 3 days < time range ≤ 90 days: The minimum scale is 1 hour.

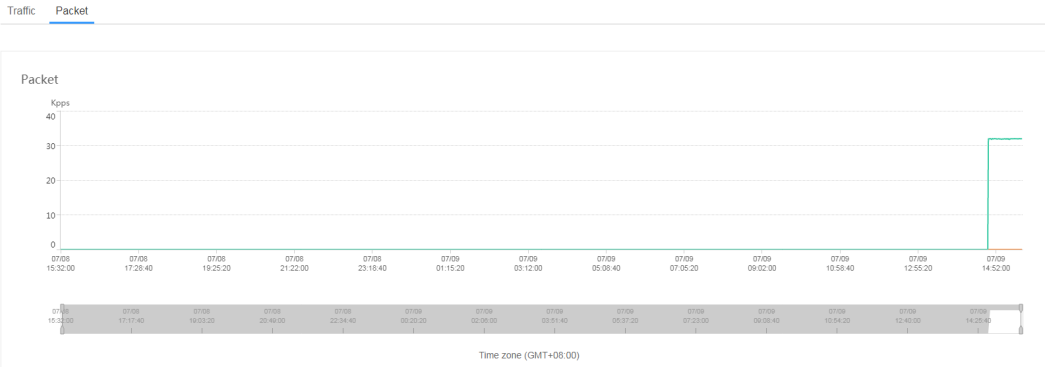
 Copyright © Huawei Technologies Co., Ltd.



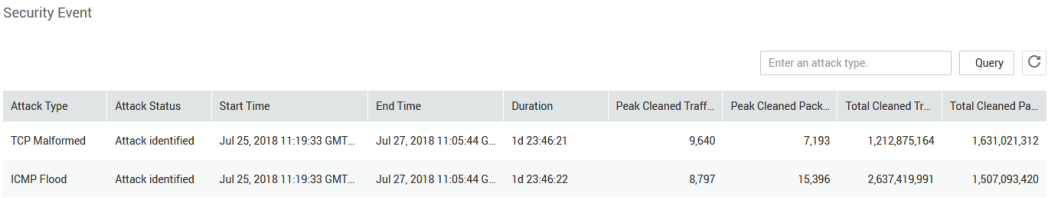
Step 5 Click the **Traffic** tab to view the traffic report.



Step 6 Click the **Packet** tab to view the packet report.



Step 7 View security events. Security event information can be queried by the attack type.



Attack Type	Attack Status	Start Time	End Time	Duration	Peak Cleaned Traff...	Peak Cleaned Pack...	Total Cleaned Tr...	Total Cleaned Pa...
TCP Malformed	Attack identified	Jul 25, 2018 11:19:33 GMT...	Jul 27, 2018 11:05:44 G...	1d 23:46:21	9,640	7,193	1,212,875,164	1,631,021,312
ICMP Flood	Attack identified	Jul 25, 2018 11:19:33 GMT...	Jul 27, 2018 11:05:44 G...	1d 23:46:22	8,797	15,396	2,637,419,991	1,507,093,420

----End

3.14 Permissions Management

3.14.1 Creating a User and Granting the AAD Access Permission

You can use **Identity and Access Management (IAM)** to implement refined permission control for AAD resources. To be specific, you can:

 Copyright © Huawei Technologies Co., Ltd.

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to AAD resources.
- Grant only the permissions required for users to perform a task.
- Entrust a HUAWEI CLOUD account or cloud service to perform professional and efficient O&M to your AAD resources.

If your HUAWEI CLOUD account does not require individual IAM users, skip this section.

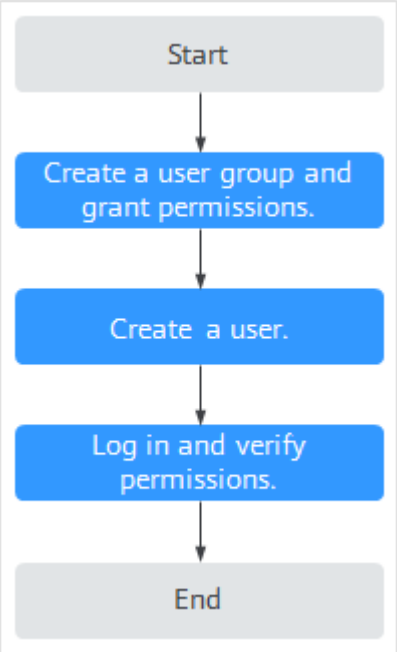
This section describes the procedure for granting permissions (see **Figure 3-61**).

Prerequisites

Before assigning permissions to a user group, you should learn about the AAD permissions that can be added to the user group, and select the permissions based on the site requirements. For details about the permissions, see **Permissions Management**. For the permissions of other services, see section "Permissions Management".

Process

Figure 3-61 Process for granting permissions



1. **Creating a User Group and Assigning Permissions**

   Create a user group on the IAM console, and grant the AAD administrator permissions (**CAD Administrator**) to the group.

2. **Creating an IAM User**

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify the permission.

 Copyright © Huawei Technologies Co., Ltd.

Log in to the management console by using the user created in 2, and verify that the user only has read permissions for AAD.

In **Service List** on the HUAWEI CLOUD console, select any other services (for example, there is only the **CAD Administrator** policy). If a message indicating that the permission is insufficient is displayed, the **CAD administrator** permission takes effect.

Copyright © Huawei Technologies Co., Ltd.