DDoS Mitigation

Best Practices

Issue	01
Date	2021-06-11



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 Identifying the Attack Type..... 1
2 Obtaining the Source IP Address of a Client.....3
3 Enabling Both AAD and WAF on HUAWEI CLOUD..... 6
4 Enabling Both AAD and CDN on HUAWEI CLOUD..... 14

 Copyright © Huawei Technologies Co., Ltd.

1 Identifying the Attack Type

DDoS attacks are launched towards services over layer 4 protocols. You can view the attack protection result on the **DDoS Attack Protection** tab on the AAD dashboard. CC attacks are launched towards website services over layer 7 protocols. You can view the attack protection result on the **CC Attack Protection** tab on the AAD dashboard.

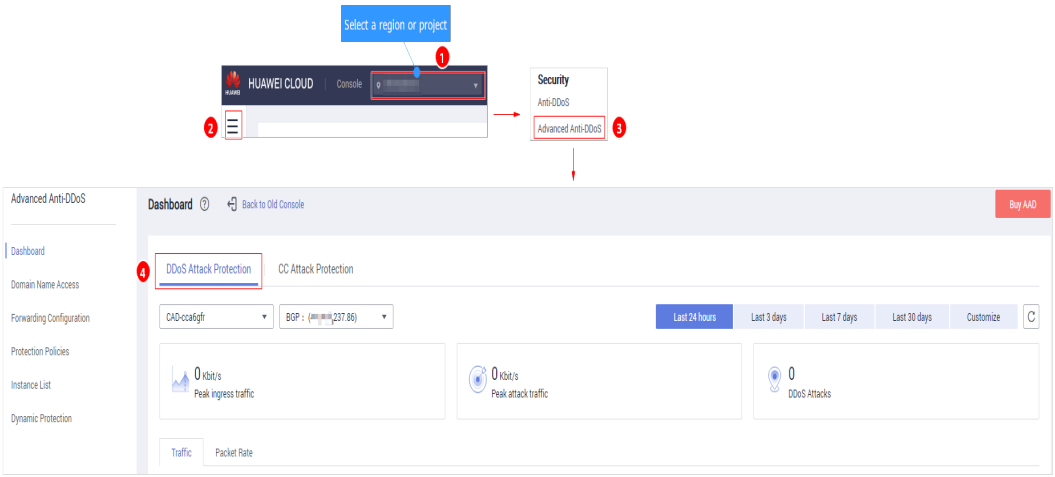
Procedure

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

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

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

Figure 1-1 DDoS attack protection entry



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

 Copyright © Huawei Technologies Co., Ltd.

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

----End

 Copyright © Huawei Technologies Co., Ltd.

2 Obtaining the Source IP Address of a Client

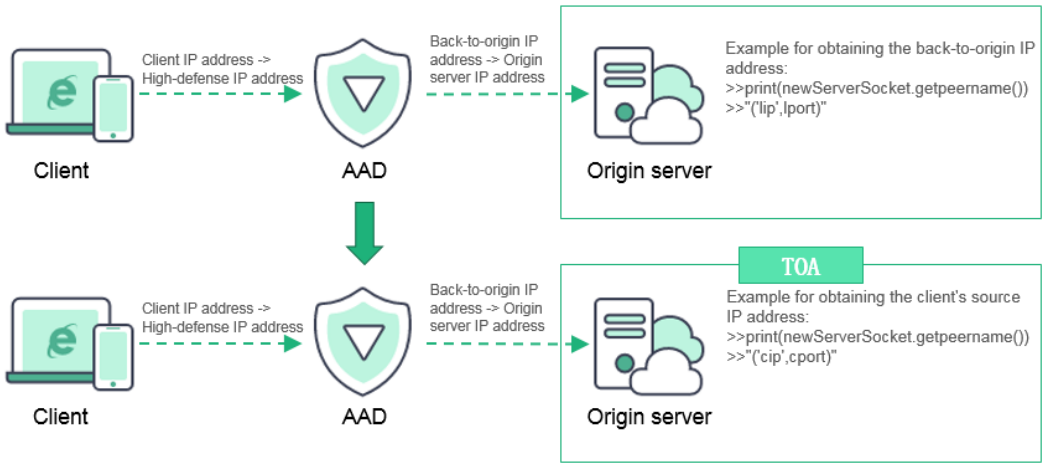
Scenarios

The real source IP address of a client is hidden from the origin server after the traffic is forwarded by the high-defense IP address. This topic describes how to obtain the real source IP address through the TOA module provided by Huawei AAD.

Mechanism

Generally, AAD changes the source IP address and destination IP address of the traffic passing through (respectively from the client's source IP address into the back-to-origin IP address and from the high-defense IP address into the origin server IP address). The source IP address visible to the user on the origin server is the back-to-origin IP address.

Figure 2-1 Mechanism



 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The high-defense IP address is provided by HUAWEI CLOUD to replace the IP address of the origin server to ensure its stability and reliability.
- From the perspective of an origin server, all traffic originates from the back-to-origin IP address.
- The origin server IP address is the public IP address used to provide services.

Prerequisites

The TOA module provided by Huawei AAD supports the following Linux OSs:

- OSs with kernel version 2.6 (such as CentOS 6.5)
- OSs with kernel version 3.10 (such as CentOS 7)
- For details, see **TOA open-source code** provided by Huawei AAD.
- If the origin server runs another OS (such as Ubuntu and SUSE), you can customize TOA according to **Configuring the TOA Plug-in** in the *Elastic Load Balance User Guide*.

  If the TOA version of the OS cannot be determined, **submit a service ticket**.

Procedure

The TOA module used by AAD has been optimized based on the open-source TOA. It can be directly compiled and installed on a Linux CentOS server. (Customizations are required for other Linux OSs.)

Step 1 Obtain the TOA module.

Huawei AAD has offered the **TOA open-source code**.

NOTE

- The AAD TOA plug-in is installed to obtain the real source IP address over the layer-4 protocol (TCP).
- If you also use the WAF service, the real source IP address must be obtained over the layer-7 protocol (HTTP). For details, see **How Do I Obtain the Real IP Address of a Web Visitor After WAF Is Enabled?**.

Step 2 Compile the TOA module.

```
 >> make   #Enter the target directory containing gcc, depending on the server version.
>> rmmod toa   #Uninstall TOA of the earlier version.
>> insmod toa.ko   #Mount the compiled TOA.
>> lsmod | grep toa   #Check whether the operation is successful.
```

NOTE

When the kernel module is mounted, you can obtain the real source IP address easily without modifying the existing server processes or interrupting existing services.

----End

- After TOA is installed in a Linux OS, the OS does not automatically load TOA during the restart by default. If you need to reload TOA during the OS restart, see the subsequent descriptions of the TOA open-source code.
- If you cannot obtain the real source IP address, contact Huawei technical support.

 Copyright © Huawei Technologies Co., Ltd.

Verification

Verify that you can obtain the real source IP address by using a common function or the above mentioned code.

 Copyright © Huawei Technologies Co., Ltd.

3 Enabling Both AAD and WAF on HUAWEI CLOUD

Scenarios

This topic describes how to configure DNS resolution to implement interworking between AAD and WAF.

Prerequisites

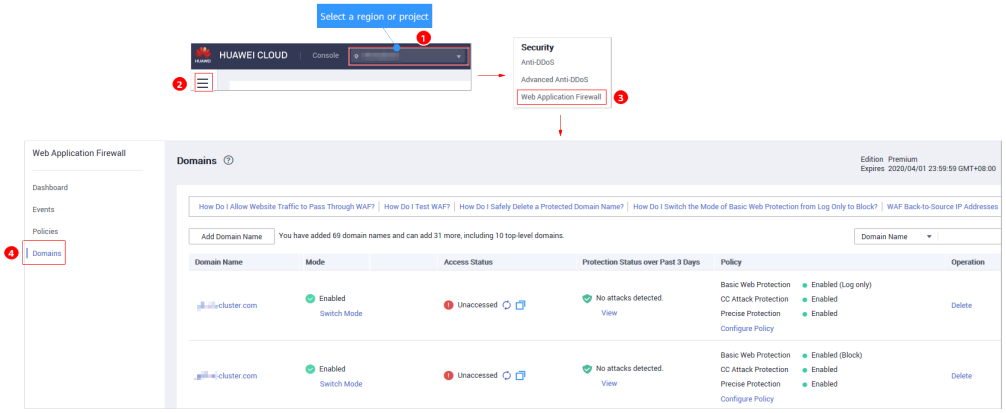
- You have purchased an AAD instance.
- You have purchased WAF and properly configured the protected domain names.

Procedure

Step 1 Obtain the WAF CNAME value.

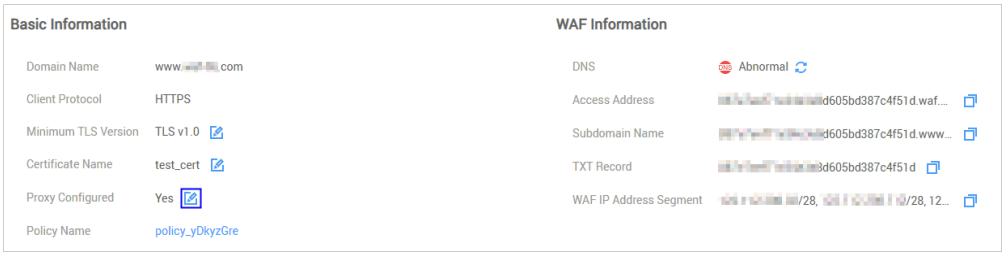
1. **Log in to the management console.**
2. Follow the procedure in the following figure to enter the **Domains** page.

   Figure 3-1 Domain configuration entry



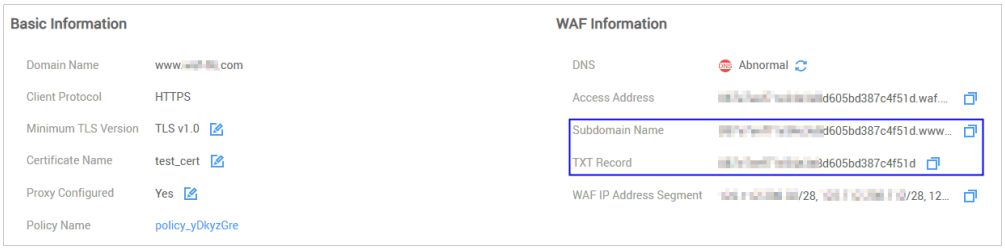
3. On the **Domains** page, click the target domain name in the **Domain Name** column.
4. In the **Basic Information** area, click for **Proxy Configured**.

 Copyright © Huawei Technologies Co., Ltd.



5. In the **Proxy Configured** dialog box, set **Proxy Configured** to **Yes** and click **OK**.
6. In the **Basic Information** area, copy the access address, subdomain name, and TXT record.

Figure 3-2 WAF information



7. Click ☰ in the upper left corner of the page and choose **Network** > **Domain Name Service**. The **Domain Name Service** management console is displayed.
8. Add a record set.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-3 Adding a TXT record set

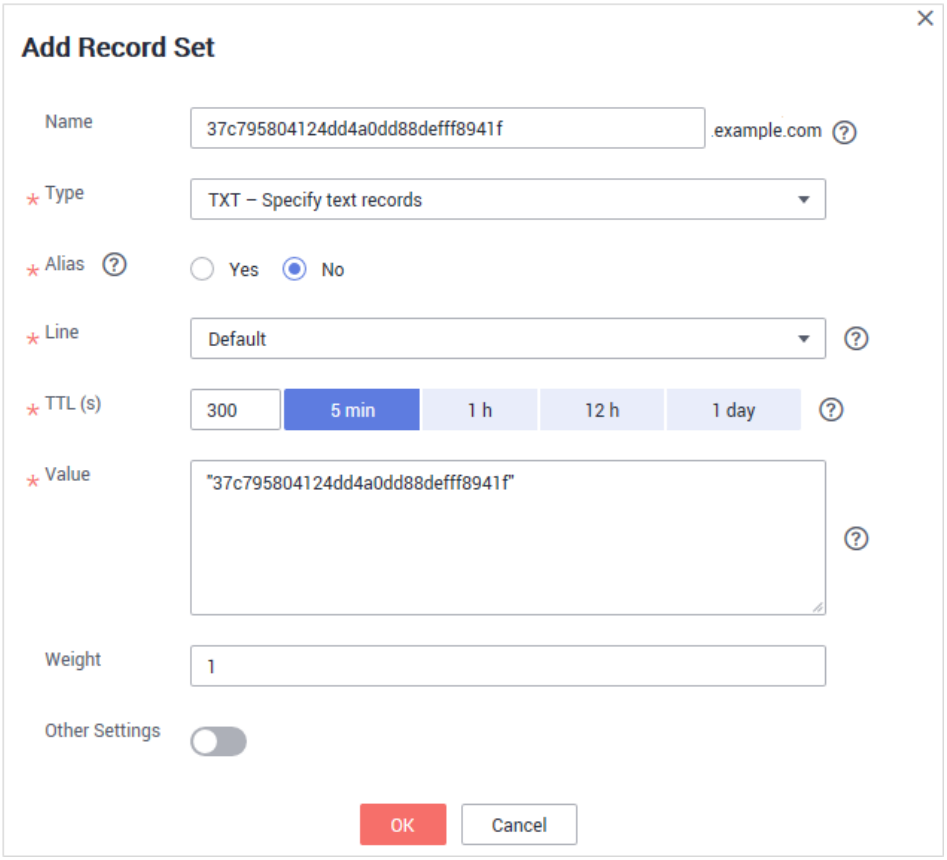


Table 3-1 Parameter description

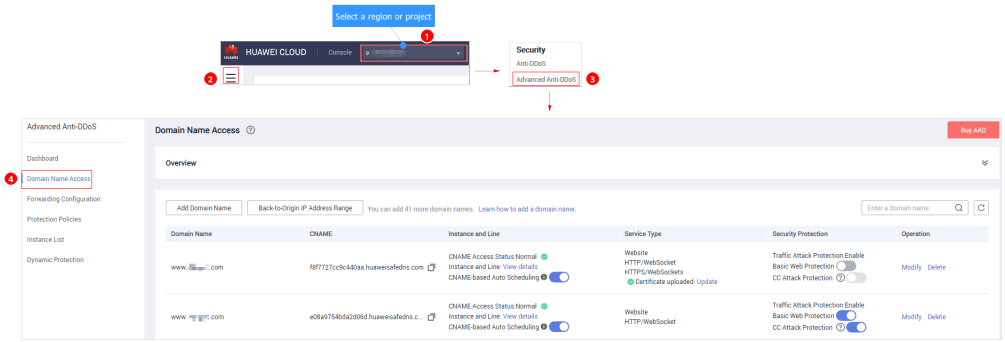
Parameter	Description
Name	Enter the subdomain name obtained in **Step 1.6**.
Type	Select **TXT – Specify text records**.
Line	Select **Default**.
TTL (s)	TTL is short for time-to-live, which specifies the cache period of resource records on a local DNS server. If your service address is frequently changed, set TTL to a smaller value.
Value	Enter the TXT record obtained in **Step 1.6**.

Step 2 Add the obtained WAF CNAME value to an AAD instance.

1. Follow the procedure in the following figure to enter the **Domain Name Access** page.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-4 Domain Name Access page



2. Click **Add Domain Name**.
3. Enter the domain name information and click **Next**.

Figure 3-5 Entering domain name information for a website service

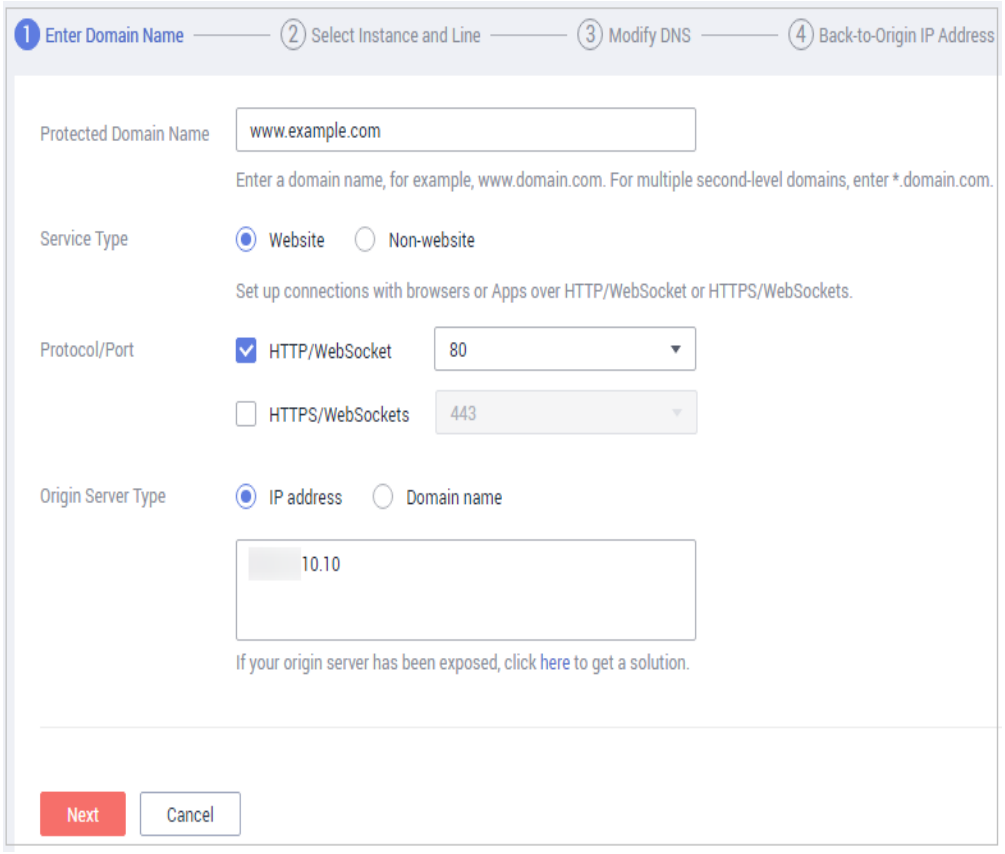


Table 3-2 Parameter description

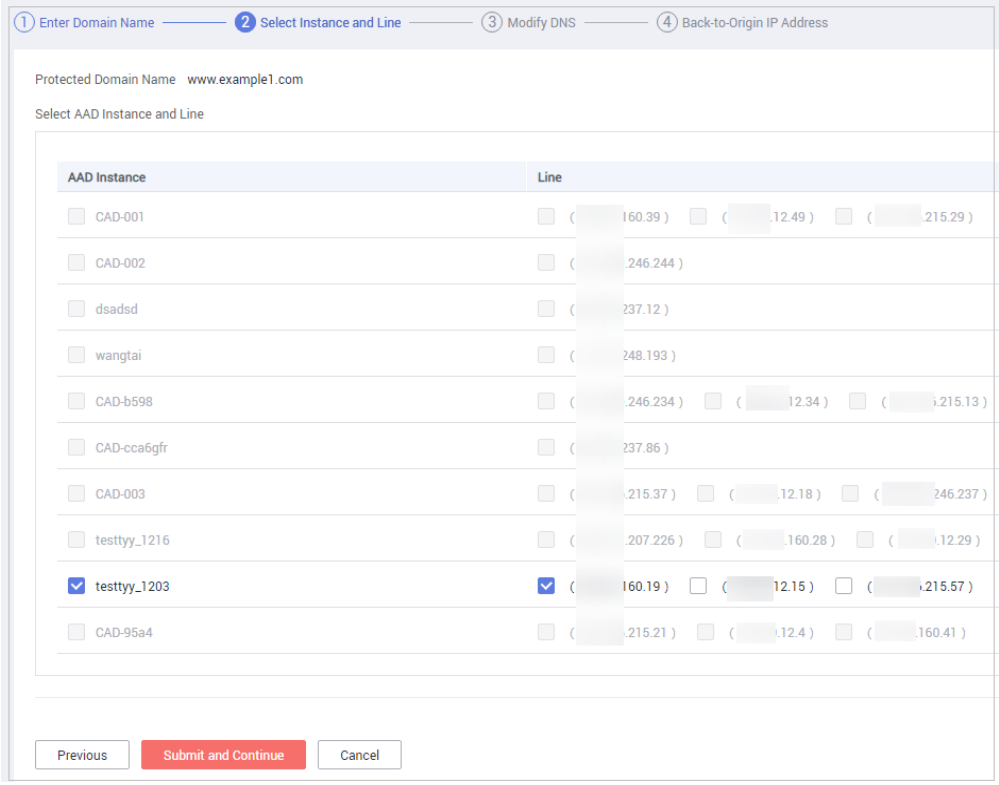
Parameter	Description
Protected Domain Name	Enter the domain name of the service to protect. Wildcard domain names are supported, for example, *.domain.com.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Origin Server Type	– Set this parameter to **Domain name**. – Enter the WAF CNAME obtained in **Step 1**.

4. On the **Select Instance and Line** page, select the required instances and lines and click **Submit and Continue**.

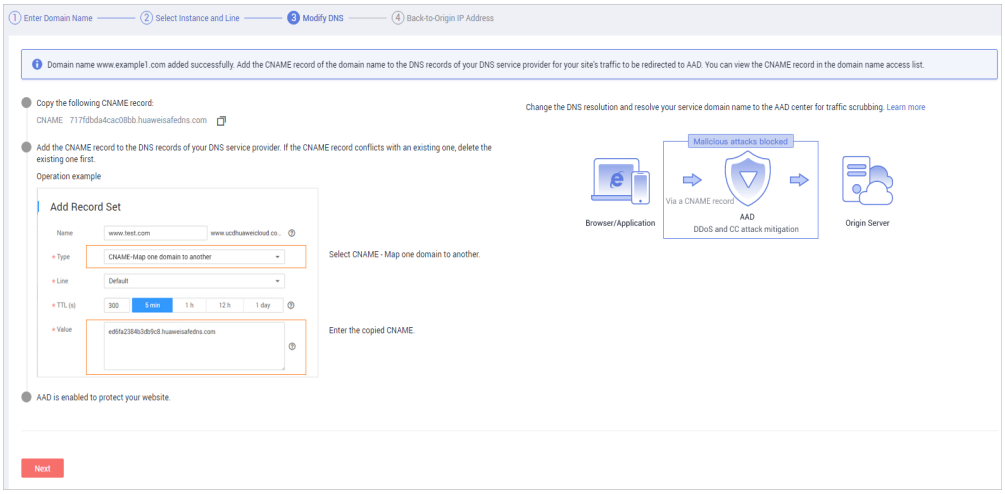
Figure 3-6 Select Instance and Line



5. On the **Modify DNS** page, copy the automatically generated AAD CNAME. Click **Next**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-7 Modifying DNS



NOTICE

- 1. After interworking with WAF is configured, no certificate needs to be uploaded for website services.
- 2. After interworking with WAF is configured, basic web protection and CC attack protection can be disabled.

Step 3 Modify DNS configuration.

1. Click ☰ in the upper left corner of the page and choose **Network** > **Domain Name Service**. The **Domain Name Service** management console is displayed.
2. Delete the record set whose **Type** is **A**.

NOTICE

Deleting the DNS A record set may adversely affect ongoing services. Therefore, you are advised to delete the record set during off-peak hours.

3. Click **Add Record Set** to add a record set. For details, see **Table 3-3**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-8 Adding a CNAME record set

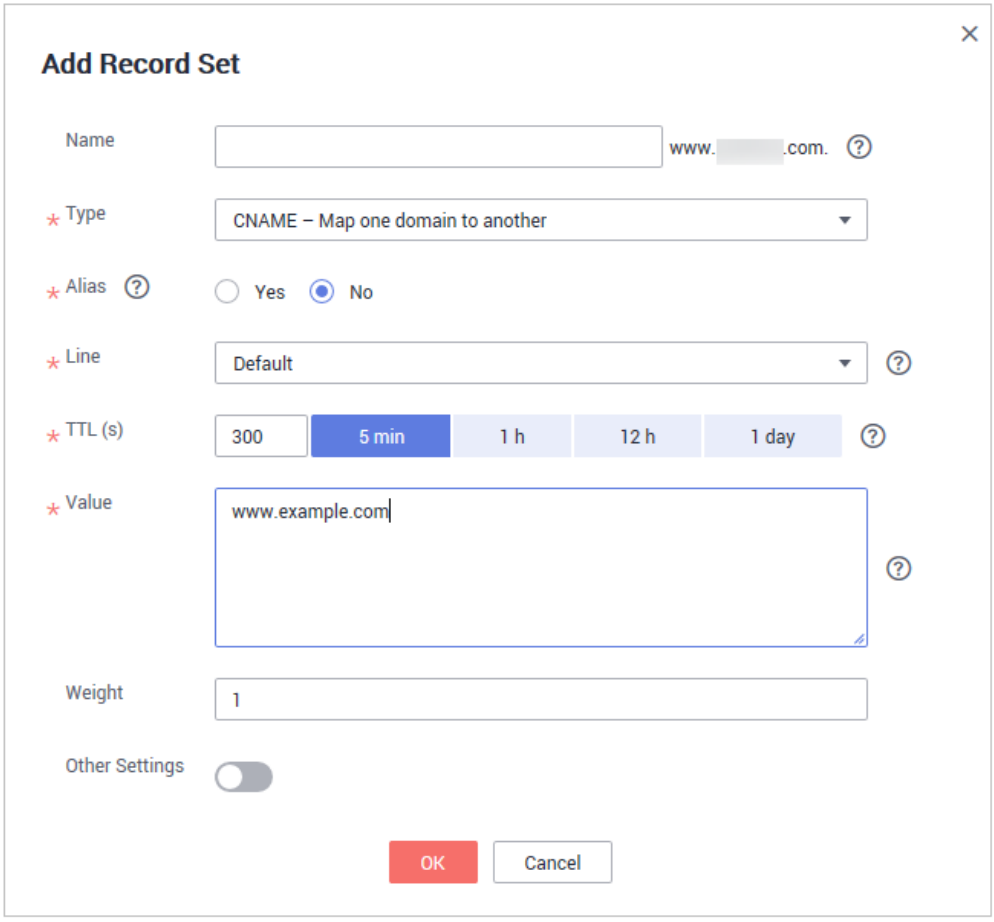


Table 3-3 Parameter description

Parameter	Description
Name	Set this parameter to the domain name configured in AAD.
Type	Select **CNAME – Map one domain to another**.
Line	Select **Default**.
TTL (s)	TTL is short for time-to-live, which specifies the cache period of resource records on a local DNS server. If your service address is frequently changed, set TTL to a smaller value.
Value	Enter the AAD CNAME obtained in **Step 2.5**.

Copyright © Huawei Technologies Co., Ltd.

NOTICE

DNS resolution takes a period of time. In most cases, domain names can be resolved within 5 minutes.

----End

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



 Copyright © Huawei Technologies Co., Ltd.

4 Enabling Both AAD and CDN on HUAWEI CLOUD

Scenarios

If you have plenty of resources, for example, images or videos on the video or e-commerce platform, to present to your customers and want them to be quickly acquired by the customers, you can use the AAD and CDN services. This service interworking implements quick access to the resources, ensures stable business running, and enhances network processing capabilities for deployed service systems, such as those for platform login and payment.

This topic describes how to configure interworking between AAD and CDN.

Mechanism

Your video and e-commerce service systems can distinguish dynamic and static resources by domain name.

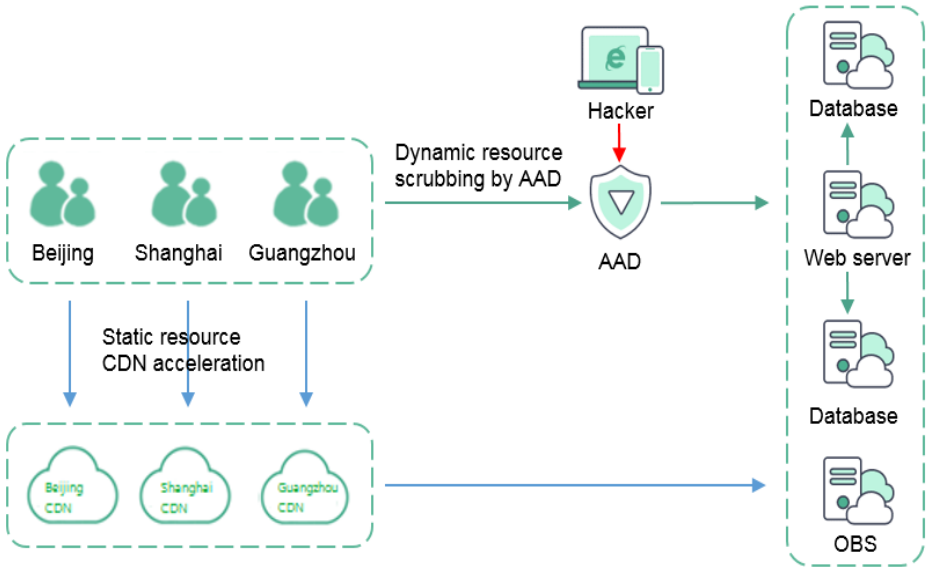
Table 4-1 Dynamic and static resources

Type	Description	Example	Solution
Dynamic resource	A service that the server needs to interact with the database before responding to a user request	• Payment • Login	The domain name of a dynamic resource is resolved into the AAD CNAME. AAD protects functional platforms, such as login and payment platforms, against DDoS attacks and ensures their stable running.

 Copyright © Huawei Technologies Co., Ltd.

Type	Description	Example	Solution
Static resource	A fixed resource that can be obtained from the Object Storage Service (OBS)	• Image • Video	The domain name of a static resource is resolved into the CDN CNAME. CDN accelerates content delivery and enables customers to quickly obtain resources such as videos and images with better experience.

Figure 4-1 Mechanism



NOTE

This interworking solution is not suitable for the platforms that do not distinguish between dynamic and static resources and apply the same set of domain names for the resources. In this case, refer to **Alternative Solution** for substitution.

Procedure

For a static resource, for example, an image service whose domain name is image.abc.com, DNS will resolve image.abc.com into the CDN CNAME to accelerate the content delivery of the static resource.

For a dynamic resource, for example, a login service whose domain name is login.abc.com, DNS will resolve login.abc.com into the AAD CNAME to ensure the

 Copyright © Huawei Technologies Co., Ltd.

stable running of the login function. For details, see **Connecting a Website Service to AAD**.

Alternative Solution

This alternative solution applies to the service systems where dynamic and static resources are not separated. When services are suffering from heavy DDoS attacks, you can configure high-defense IP addresses to divert attack traffic for scrubbing, ensuring the stable and reliable running of services on origin servers. For details, see the *Advanced Anti-DDoS User Guide*. If no attack is launched, you can use CDN to accelerate content delivery and improve user experience.

Can I Configure Traffic to Be Forwarded from CDN to AAD or from AAD to CDN?

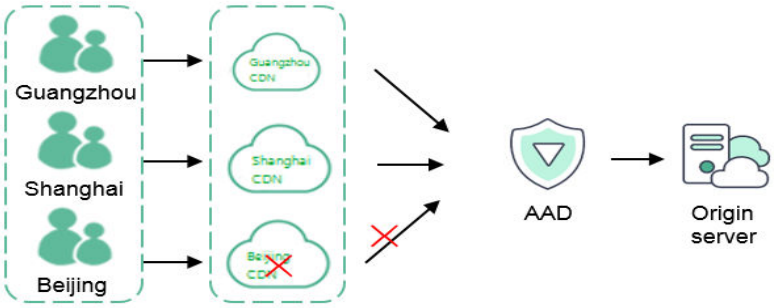
Neither of the forwarding sequences is allowed.

- Forwarding sequence 1: The AAD service is connected behind the CDN service. Traffic is processed by CDN first and then forwarded to AAD.

  Result: AAD protection becomes ineffective.

  Cause: The attack traffic reaches CDN first. CDN will process it before forwarding it to AAD. In this deployment, AAD does not scrub attack traffic in a timely manner.

  Figure 4-2 Mechanism



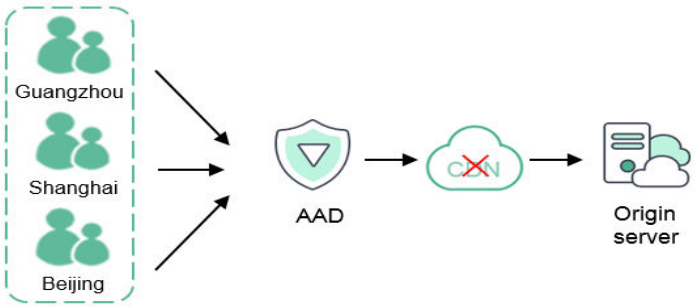
- Forwarding sequence 2: The CDN service is connected behind the AAD service. Traffic is processed by AAD first and then forwarded to CDN.

  Result: CDN acceleration function becomes ineffective.

  Cause: CDN delivers network content from origin servers to scattered CDN nodes and enables users to access their nearest CDN nodes, thereby accelerating content delivery. If the access requests are firstly directed to AAD, users cannot obtain desired content from the nearest CDN nodes.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-3 Mechanism



 Copyright © Huawei Technologies Co., Ltd.