

# DDoS Mitigation

## Best Practices

**Issue** 05  
**Date** 2025-01-27



**Copyright © Huawei Technologies Co., Ltd. 2025. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI 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.

# Security Declaration

## Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

---

# Contents

---

<b>1 Overview.....</b>	<b>1</b>
<b>2 Best Practices of Cloud Native Anti-DDoS (CNAD) Basic.....</b>	<b>2</b>
2.1 Accessing a Black-holed Server Through ECS.....	2
<b>3 Best Practices of Cloud Native Anti-DDoS (CNAD) Advanced.....</b>	<b>5</b>
3.1 Using ELB and CNAD Advanced to Improve the DDoS Protection Capabilities of ECSs.....	5
3.2 Using WAF, ELB, and CNAD Advanced to Improve Website Service Security.....	8
<b>4 Best Practices of Advanced Anti-DDoS.....</b>	<b>11</b>
4.1 Using AAD to Identify Attack Types.....	11
4.2 Using the TOA Module to Obtain the Actual Source IP Addresses of Requests.....	12
4.3 Using WAF and AAD to Protect Domain Names.....	14
4.4 Using CDN and AAD to Protect Dynamic and Static Resources.....	21
4.5 Migrating Website Services Between Two AAD Instances.....	24
<b>5 Using the Scheduling Center to Implement Tiered Traffic Scheduling.....</b>	<b>27</b>

# 1 Overview

This document describes best practices for working with Anti-DDoS Service and provides operational guidelines that you can follow when using this service.

**Table 1-1** Best practices

Component	Reference
Post-attack handling	<a href="#">Accessing a Black-holed Server Through ECS</a>
	<a href="#">Using AAD to Identify Attack Types</a>
	<a href="#">Migrating Website Services Between Two AAD Instances</a>
Origin server IP addresses	<a href="#">Using the TOA Module to Obtain the Actual Source IP Addresses of Requests</a>
Improving protection capabilities	<a href="#">Using the Scheduling Center to Implement Tiered Traffic Scheduling.</a>
Joint protection	<a href="#">Using ELB and CNAD Advanced to Improve the DDoS Protection Capabilities of ECSs</a>
	<a href="#">Using WAF, ELB, and CNAD Advanced to Improve Website Service Security</a>
	<a href="#">Using WAF and AAD to Protect Domain Names</a>
	<a href="#">Using CDN and AAD to Protect Dynamic and Static Resources</a>

# 2 Best Practices of Cloud Native Anti-DDoS (CNAD) Basic

## 2.1 Accessing a Black-holed Server Through ECS

### Application Scenarios

When your server is under a traffic flooding attack, a black hole will be triggered to block all accesses from the Internet. You can connect to a black-holed server through an Elastic Cloud Server (ECS).

Once you have connected your ECS to a server in the black hole state, you can transfer files to the server and can make whatever configuration changes are necessary.

### Limitations and Constraints


Ensure the ECS can be accessed and in the same region as the black-holed server.

### Resource and Cost Planning

Resource	Description	Quantity	Cost
ECS	Used to connect to the black-holed server.	1	For details about ECS billing modes and standards, see <a href="#">ECS Billing Description</a> .

### Procedure

**Step 1** [Log in to the management console](#).

**Step 2** Click  in the upper left corner of the management console and select a region or project.

**Step 3** Click  and choose **Computing > Elastic Cloud Server**.

**Step 4** Log in to the ECS that can be accessed and in the same region as the server which a black hole has been triggered for.

Select a login method and log in to the ECS.

- For details about how to log in to a Windows ECS, see [Windows ECS Login Overview](#).
- For details about how to log in to a Linux ECS, see [Linux ECS Login Overview](#).

**Step 5** [Table 2-1](#) describes how to connect to a server which a black hole has been triggered for.

**Table 2-1** Server connection

ECS OS	Black-holed Server OS	Connection Method
Windows	Windows	Use MSTSC to log in to the server which a black hole has been triggered for. <ol style="list-style-type: none"><li>1. Search for <b>mstsc</b> in the ECS and click it to open the <b>Remote Desktop Connection</b> dialog box.</li><li>2. Click <b>Show Options</b> in the displayed dialog box.</li><li>3. Enter the EIP and username (<b>Administrator</b> by default) of the server which a black hole has been triggered for.</li><li>4. Click <b>OK</b> and enter the login password as prompted to log in to the server.</li></ol>
	Linux	Use a remote login tool, such as PuTTY or Xshell, to log in to the server.
Linux	Windows	<ol style="list-style-type: none"><li>1. Install a remote connection tool, such as <b>rdesktop</b>.</li><li>2. Run the following command to log in to the server which a black hole has been triggered for. <b>rdesktop -u Username -p Password -g Resolution EIP bound to the server which a black hole has been triggered for</b></li></ol>

ECS OS	Black-holed Server OS	Connection Method
	Linux	Run the following command to log in to the server which a black hole has been triggered for. <i>ssh EIP bound to the server which a black hole has been triggered for</i>

----End



# 3 Best Practices of Cloud Native Anti-DDoS (CNAD) Advanced

---

## 3.1 Using ELB and CNAD Advanced to Improve the DDoS Protection Capabilities of ECSs

### Application Scenarios

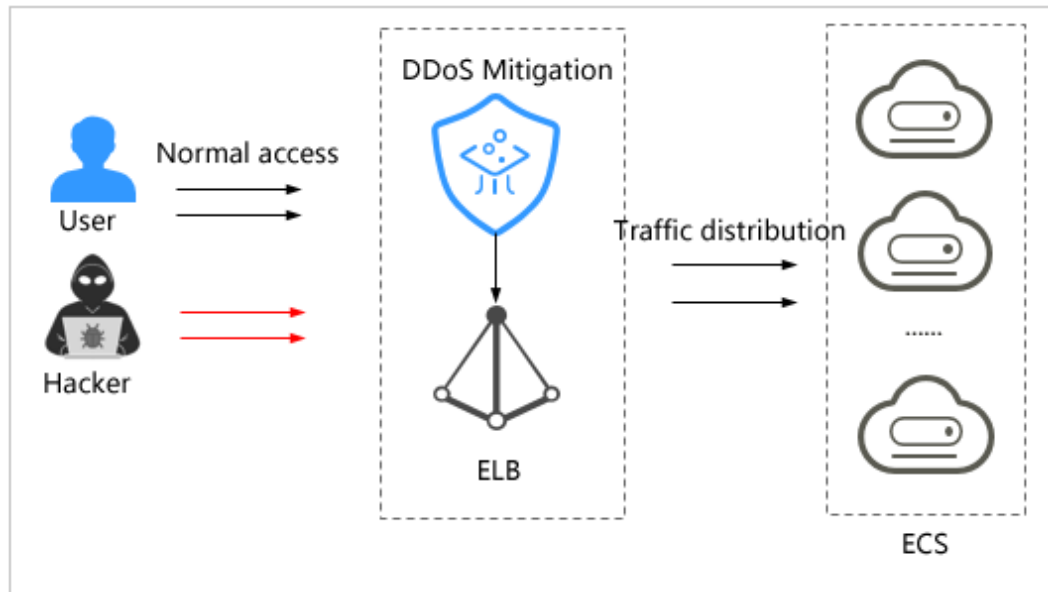
CNAD Advanced enhances the DDoS protection capabilities of cloud services, such as Elastic Cloud Server (ECS) and Elastic Load Balance (ELB), ensuring service security.

You can deploy ELB and connect its public IP address to CNAD Advanced to significantly improve defense against various types of DDoS attacks.

### Architecture

When your website services are deployed on HUAWEI CLOUD ECSs, you can configure the combination of CNAD Advanced and ELB for your services. Deploy ELB on the origin server of your ECS, and add the EIP address of the ELB to the CNAD instance to improve the anti-DDoS capability of the ECS.

**Figure 3-1** Using CNAD Advanced in combination with ELB



## Advantages

Compared to enabling CNAD Advanced for ECSs, combining CNAD Advanced and Elastic Load Balance (ELB) allows for the discarding of traffic from unlisted protocols and ports. This enhances defense against various DDoS attacks (including reflection attacks like SSDP, NTP, and Memcached, as well as UDP flood and SYN flood attacks), significantly improving the DDoS protection capability of ECSs and ensuring the security and reliability of user services.

## Limitations and Constraints

ELB must be deployed in regions where CNAD Advanced instances can be purchased, for example, CN North-Beijing4.

## Resource and Cost Planning

Resource	Description	Quantity	Cost
ELB	Distributes access traffic to backend ECSs to mitigate single point of failures (SPOFs) caused by DDoS attacks.	1	For details, see <a href="#">Billing Overview</a> .
CNAD Advanced	Public IP addresses used to connect to the ELB for DDoS attack defense.	1	For details about CNAD Advanced billing modes and standards, see <a href="#">Billing Overview</a> .

## Procedure

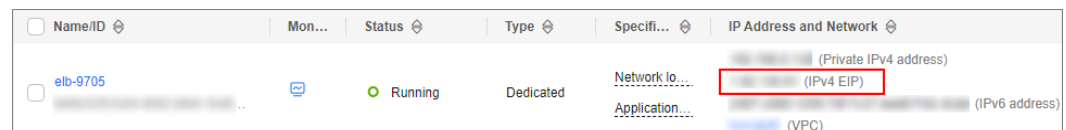
**Step 1** Create a load balancer. For details, see [Creating a Shared Load Balancer](#).

**Table 3-1** Parameter description

Parameter	Description
Region	Select the region where the ECS is located.
EIP	Select <b>Automatically assign</b> .
Line	Select <b>Dynamic BGP</b> .

**Step 2** Obtain the public IP address of the created load balancer, as shown in [Figure 3-2](#).

**Figure 3-2** Public IP address of the ELB instance

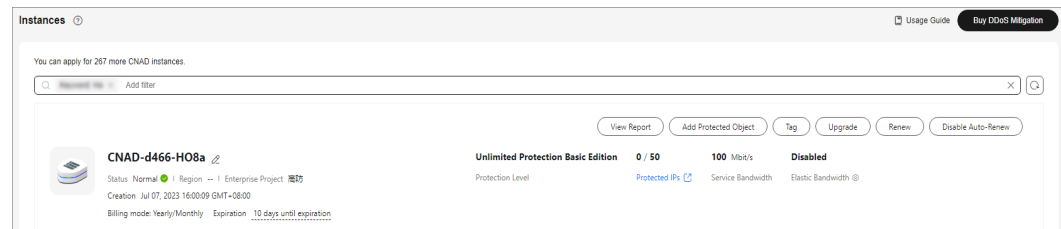


Name/ID	Mon...	Status	Type	Specifi...	IP Address and Network
elb-9705		Running	Dedicated	Network Jo...	(Private IPv4 address) (IPV4 EIP) (IPV6 address) (VPC)

**Step 3** [Buy a CNAD Advanced instance](#) in the same region as the ECS.

**Step 4** In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced > Instances**. The **Instances** page is displayed.

**Figure 3-3** Instance list



**Step 5** In the upper right corner of the target instance box, click **Add Protected Object**.

**Step 6** In the **Add Protected Object** dialog box that is displayed, select the elastic IP address of the load balancer obtained in [Step 2](#) and click **OK**.

After adding protected objects, you can configure protection policies for them. Cloud Native Anti-DDoS Advanced provides unlimited protection against DDoS attacks for ECSs. When a DDoS attack occurs, traffic scrubbing is automatically triggered.

For details about how to configure a protection policy, see [Adding a Protection Policy](#).

----End

## 3.2 Using WAF, ELB, and CNAD Advanced to Improve Website Service Security

### Application Scenarios

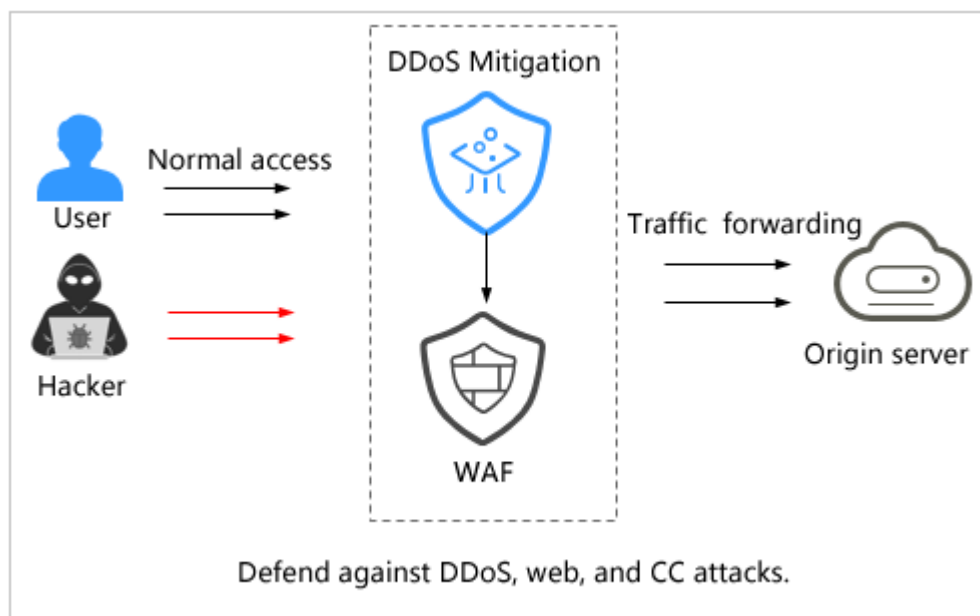
Huawei Cloud Web Application Firewall (WAF) detects HTTP and HTTPS requests to identify and block attacks such as SQL injection, cross-site scripting (XSS), web shells, file inclusion, sensitive file access, third-party vulnerability exploits, CC attacks, malicious crawlers, and cross-site request forgery (CSRF), ensuring web service security and stability.

CNAD Advanced provides layer-4 DDoS attack defense for website services connected to WAF (cloud mode - ELB access). It offers dual protection through CNAD Advanced and cloud WAF (ELB access), defending against layer-4 DDoS attacks, layer-7 web attacks, and CC attacks, significantly enhancing the security and stability of website services.

### Architecture

With a CNAD Advanced and a cloud WAF instance in place, the WAF engine inspects all incoming traffic. It filters out malicious activities such as DDoS, web, and CC attacks, ensuring that only legitimate traffic reaches your origin server.

Figure 3-4 CNAD Advanced collaborates with WAF





### Limitations and Constraints

Only website services that have been connected to cloud WAF (ELB access) are supported. For details, see [Connecting Your Website to WAF \(Cloud Mode - Load Balancer Access\)](#).

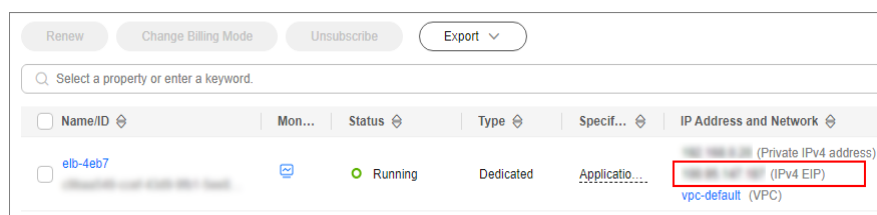
## Resource and Cost Planning


Resource	Description	Quantity	Cost
Cloud WAF (ELB access)	Connected to websites for defense against web and CC attacks.	1	For details about WAF billing modes and standards, see <a href="#">WAF Billing Overview</a> .
CNAD Advanced	Protects website services connected to WAF against DDoS attacks.	1	For details about CNAD Advanced billing modes and standards, see <a href="#">Billing Overview</a> .

## Procedure

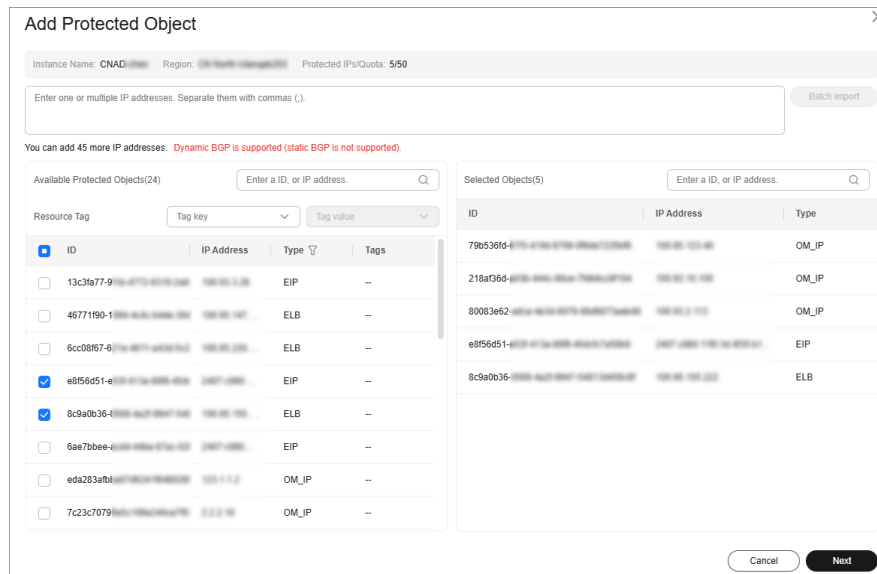
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner of the page and choose **Elastic Load Balance** under **Network** to go to the ELB console.
- Step 4** Locate the row that contains the load balancer bound to the WAF instance, and obtain the EIP of the load balancer.

**Figure 3-5** Copying the EIP



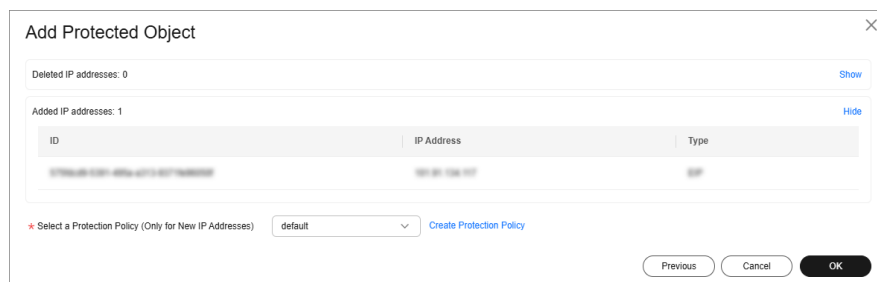
- Step 5** [Buy a CNAD Advanced instance](#) in the region where the EIP bound to the load balancer resides.
- Step 6** Click  in the upper left corner of the page and choose **Security & Compliance** > **DDoS Mitigation**.
- Step 7** In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced** > **Instances**. The **Instances** page is displayed.
- Step 8** In the upper right corner of the target instance box, click **Add Protected Object**.
- Step 9** Search for the EIP of the load balancer in [Step 4](#), set it as a protected object, and click **Next**.

**Figure 3-6** Adding a protected object



**Step 10** Select a protection policy for the added IP address and click **OK**.

**Figure 3-7** Policy



After adding a protected object, you can configure a protection policy for it. For details, see [Adding a Protection Policy](#).

----End

# 4 Best Practices of Advanced Anti-DDoS

## 4.1 Using AAD to Identify Attack Types

### Application Scenarios

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.


### Resource and Cost Planning

Resource	Description	Quantity	Cost
AAD	Defends against DDoS attacks.	1	For details about AAD billing modes and standards, see <a href="#">Billing Overview</a> .

### 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** Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS Service Center** page is displayed.

**Step 3** In the navigation pane on the left, choose **Advanced Anti-DDoS > Dashboard**. The **Dashboard** page is displayed.

**Step 4** Click the **DDoS Attack Protection** tab.

**Step 5** View the traffic reports respectively on the **DDoS Attack Protection** and **CC Attack Protection** pages and determine the attack types accordingly.

Attack Type	DDoS Attack Protection Report	CC Attack Protection Report
DDoS attacks	<ul style="list-style-type: none"><li>• The report indicates attack traffic fluctuations.</li><li>• Traffic scrubbing has been triggered.</li></ul>	<ul style="list-style-type: none"><li>• There is no associated traffic fluctuation in the report.</li></ul>
CC attacks	<ul style="list-style-type: none"><li>• The report indicates attack traffic fluctuations.</li><li>• Traffic scrubbing has been triggered.</li></ul>	<ul style="list-style-type: none"><li>• There are associated traffic fluctuations in the report.</li></ul>

----End

## 4.2 Using the TOA Module to Obtain the Actual Source IP Addresses of Requests

### Application Scenarios

After a service is connected to AAD, the actual source IP address of the traffic forwarded by AAD is concealed once it reaches the server. The source IP address of the customer's service origin server becomes the back-to-origin IP address of AAD. The true source IP address can be retrieved from the **tcp option** field in the TCP packet. IPv6 source IP addresses can be obtained.

During service application development, it is necessary to obtain the client's real IP address. Taking the voting system as an example, the real IP addresses of clients used for casting votes needs to be obtained to ensure that each client casts only one vote.

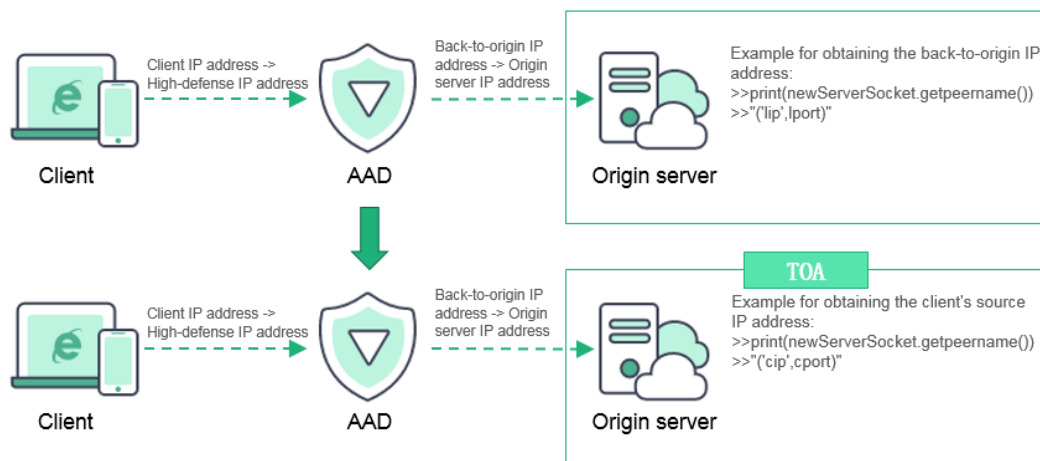
This topic describes how to use the TOA module provided by AAD to obtain the real source IP address.

### Architecture

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 high-defense IP address and from the back-to-origin 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 4-1 Mechanism



- 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.

## Limitations and Constraints

If the origin server runs one of the following Linux OSs, you can use the TOA module provided by AAD to obtain the real source IP address of the traffic forwarded by AAD.

- CentOS 6.5 (corresponding to the Linux kernel version 2.6.X)
- CentOS 7 (corresponding to the Linux kernel version 3.10.X)
- toa\_common (TOA of common version, which is applicable to OSs whose Linux kernel version is 3.0 or later, such as Ubuntu 14/16 and SUSE 11/42)
- toa\_linux-2.6.32-220.23.1.el6.x86\_64.rs (corresponding to linux-2.6.32-220.23.1.el6.x86\_64.rs)

### NOTICE

- In the "AAD+web origin server" scenario, if basic web protection is disabled on AAD, you need to install TOA on the origin server to obtain the real source IP address.
- If basic web protection is enabled for AAD or Huawei Cloud WAF is configured as the origin server, you do not need to install TOA to obtain the real source IP address. You can obtain the real source IP address from the Layer 7 request headers such as **xff** and **x-real**. Only the real IPv4 access source can be obtained. Obtain the Layer 7 HTTP real source IP addresses by referring to [Obtaining the Real Client IP Addresses](#).
- If the origin server runs other operating systems (such as Ubuntu and SUSE), follow the instructions described in [Configuring the TOA Plug-in](#) to customize and install the TOA plug-in to obtain the real source IP address.

## Procedure

- Step 1** Compile and install the TOA module by referring to [the open-source code of TOA](#).

 **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.

- Step 2** Verify the module.

You can obtain the real source IP address by referring to [Configuring the TOA Plug-in](#) or the following example code.

```
>>print(newServerSocket.getpeername())  
>>"('cip',cport)"
```

----End

## 4.3 Using WAF and AAD to Protect Domain Names

### Application Scenarios

Huawei Cloud Web Application Firewall (WAF) detects HTTP and HTTPS requests to identify and block attacks such as SQL injection, cross-site scripting (XSS), web shells, file inclusion, sensitive file access, third-party vulnerability exploits, CC attacks, malicious crawlers, and cross-site request forgery (CSRF), ensuring web service security and stability.

AAD ensures the continuity of domain names and protects services against heavy-traffic DDoS attacks.

WAF and AAD together can defend against web application attacks and traffic attacks, greatly enhancing the security and stability of domain names.

This practice is based on the scenario where a domain name is connected to WAF. It explains how to enable website traffic to pass through both AAD and WAF, thereby improving the comprehensive protection capability of your website.

 **NOTE**

For details about how to connect a domain name to WAF, see [Connecting Your Website to WAF](#).

### Architecture

After AD with WAF interworking is enabled, traffic is routed through AAD before being directed to WAF, enabling a coordinated defense mechanism.

**Figure 4-2** AAD and WAF interworking



 **CAUTION**

When protecting multiple domain names under AAD with the same instance and port, and using WAF CNAME as the origin server, it is important to note that if the origin server IP addresses for these CNAMEs differ and all WAF CNAMEs are bypassed, then all domain names linked to that particular high-defense IP address and port will become inaccessible.

## Limitations and Constraints




- Joint protection with AAD and WAF is only for domain names. When configuring the joint protection with AAD and WAF, you need to configure these two domain names separately.
- For a high-defense IP address and port, you can configure only one type of origin server. Once an origin server domain name is set, configuring an additional origin server IP address is not possible.

## Resource and Cost Planning

Resource	Description	Quantity	Cost
Web Application Firewall (WAF)	Connected to websites for defense against web and CC attacks.	1	For details about WAF billing modes and standards, see <a href="#">WAF Billing Overview</a> .
AAD	Protects domain names connected to WAF against DDoS attacks.	1	For details about AAD billing modes and standards, see <a href="#">Billing Overview</a> .

## Procedure

**Step 1** Obtain the WAF CNAME value.

1. Log in to the management console.
2. Click  in the upper left corner of the management console and select a region or project.
3. Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
4. In the navigation pane, choose **Website Settings**.
5. On the **Domains** page, click the target domain name whose CNAME value you want to obtain.
6. In the **Basic Information** area, click  under **Use Layer-7 Proxy**.

**Figure 4-3** Basic information

**Basic Information**

Website Name --

Website Remarks --

CNAME (New)

CNAME (Old)

**Client Protocol**

Client Protocol

HTTP

Use Layer-7 Proxy

No

**NOTE**

If you are using Huawei Cloud AAD before connecting the domain name to WAF, set **IP Tag** to **\$remote\_addr** in the **Traffic Identifier** area on the **Basic Information** page to obtain the actual IP address of the client. For details, see [Configuring a Traffic Identifier for a Known Attack Source](#).

7. On the displayed page, set **Use Layer 7 Proxy** to **Yes** and click **OK**.
8. On the **Basic Information** page, copy the CNAME.

**Figure 4-4** Copying the CNAME value

**Basic Information**

Website Name --

CNAME (New)

Client Protocol

Client Protocol

HTTP

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

**NOTE**

After interworking with WAF is configured, no certificate needs to be uploaded for website services.

1. Click in the upper left corner of the page and choose **Security & Compliance > DDoS Mitigation**.
2. Choose **AAD > Domain Name Access**. The **Domain Name Access** configuration page is displayed.
3. Select **Chinese mainland** or **Other**.
4. Click **Add Domain**.

5. Enter the domain name information and click **Next**.

**Figure 4-5** Configuring website domain

**Table 4-1** 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.

Parameter	Description
Origin Server Type	<ul style="list-style-type: none"><li>– Set this parameter to <b>Domain name</b>.</li><li>– Enter the forwarding protocol and origin server port of the origin server domain name.</li><li>– Enter the copied WAF CNAME.</li></ul>
Server Configuration	Enter the forwarding protocol and port used by the origin server.

6. On the **Select Instance and Line** page, select the required instances and high-defense IP addresses and click **Submit and Continue**.

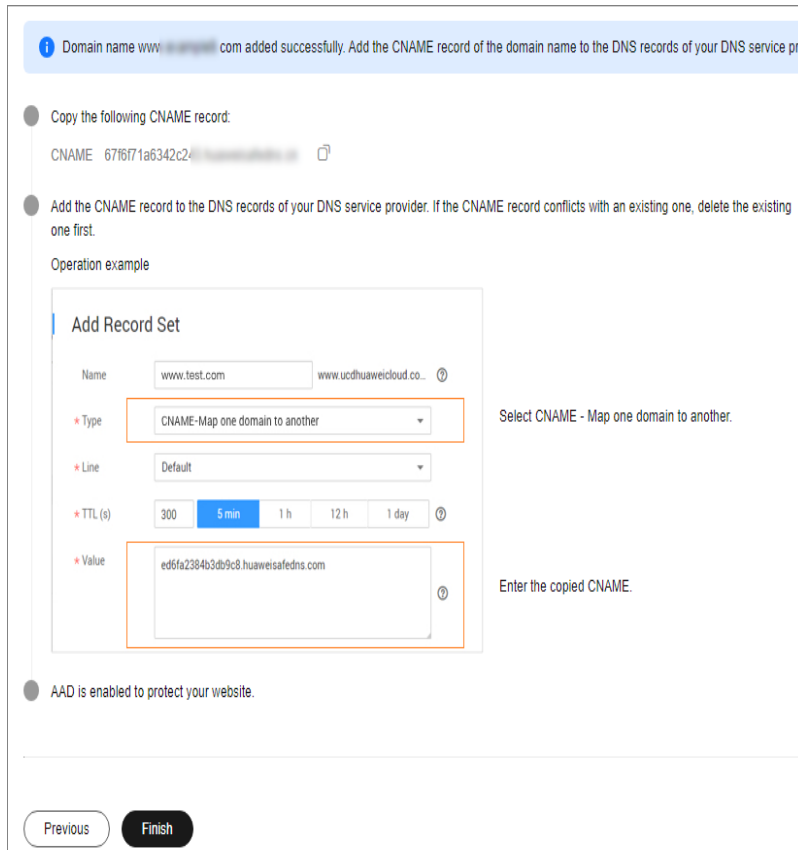
**Figure 4-6** Selecting an instance and a line

The screenshot shows a web interface for selecting an instance and a line. At the top, there is a 'Protected Domain Name' field with the value 'www.123.com'. Below it is an 'Enterprise Project' dropdown menu set to 'default'. The main section is titled 'AAD Instance and Line' and contains a search bar with the placeholder text 'Select a property or enter a keyword'. Below the search bar is a table with two columns: 'AAD Instance' and 'Line'. The table has several rows, with the first row selected. The first row has a checked checkbox in the 'AAD Instance' column and the value 'CIDR-6524' in the 'Line' column. The other rows have unchecked checkboxes. At the bottom right of the page, there are three buttons: 'Previous', 'Submit and Continue', and 'Cancel'.


**Step 3** Click **Next**.

**Step 4** On the **Modify DNS Resolution** page, copy the CNAME of the AAD and click **Finish**.

Figure 4-7 Copying AAD CNAME



**Step 5** 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. Click **Public Zones**.
3. Locate the row that contains the target domain name, and choose **Manage Record Set**.
4. Click **Add Record Set** to add a CNAME record set.

**Figure 4-8** Adding a record set

✕

[Redacted].com

**Add Record Set** [Add Record Sets for Email Domain](#)

Type

CNAME – Map one domain to another ▼

Name

Example: www [Redacted].com

Line ?

Default ▼

TTL (s) ?

300

Value ?

www.[Redacted].com

✓ Advanced Settings (Optional)

Alias: NoWeight: 1Tag: --Description: --

CancelOK



**Table 4-2** Key parameters

Parameter	Description
Name	Set this parameter to the domain name configured in AAD.
Record Type	Select <b>CNAME - Map one domain to another</b> .
Line	Select <b>Default</b> .
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.
DNS record	Enter the copied AAD CNAME.

**NOTICE**

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

----End

## 4.4 Using CDN and AAD to Protect Dynamic and Static Resources

### Application Scenarios

If your business (such as videos and e-commerce platforms) has a large number of images or videos displayed to users, and you want these resources to be quickly accessed,

consider using the "AAD + CDN" solution from Huawei Cloud. This solution ensures rapid resource retrieval and enhances network capabilities for service systems, such as user login and payment processing, ensuring the stable operation of the platform.

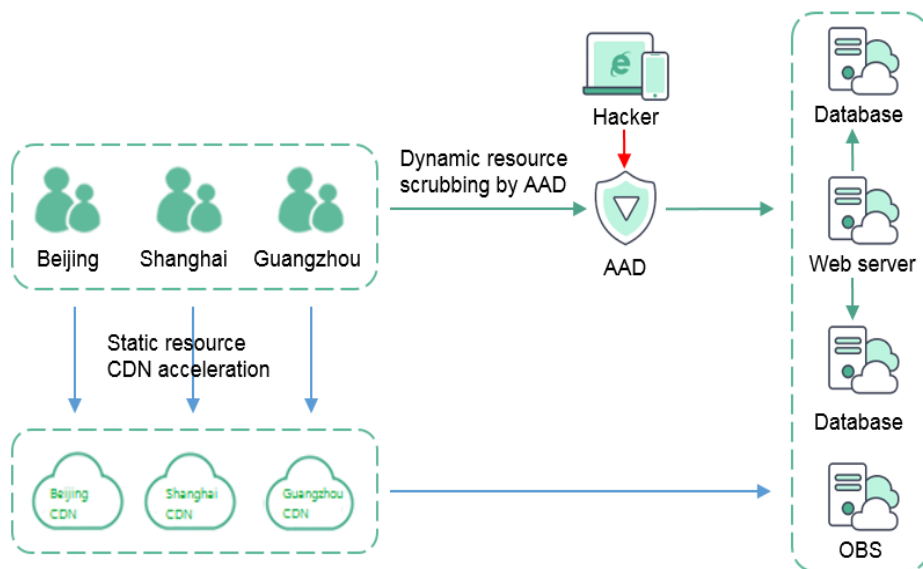
### Architecture

When users' video and e-commerce service systems can distinguish dynamic and static resources by domain name, the AAD+CDN interworking solution is recommended. For details about dynamic and static resources, see [Figure 4-9](#).

- 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 stable running of the login function.

**Figure 4-9** Mechanism of the "AAD + CDN" joint solution



**Table 4-3** Solution description

Type	Description	Example	Solution
Dynamic resource	A service that the server needs to interact with the database before responding to a user request	<ul style="list-style-type: none"> <li>• Payment</li> <li>• Login</li> </ul>	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.

Type	Description	Example	Solution
Static resource	A fixed resource that can be obtained from the Object Storage Service (OBS)	<ul style="list-style-type: none"><li>Image</li><li>Video</li></ul>	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.

## Limitations and Constraints

This solution is not suitable for the platforms that do not distinguish between dynamic and static resources and apply the same set of domain names to the resources.

## Resource and Cost Planning

Resource	Description	Quantity	Cost
CDN	Used to accelerate static resources.	1	For details about CDN billing modes and standards, see <a href="#">Billing Items</a> .
AAD	Protects dynamic resources.	1	For details about AAD billing modes and standards, see <a href="#">Billing Items</a> .

## Procedure

- Step 1** Connect static resources to CDN by referring to [Adding a Domain Name](#).
- Step 2** Connect dynamic resources to AAD by referring to [Connecting Domain Name Website Services to Advanced Anti-DDoS](#).

----End

## 4.5 Migrating Website Services Between Two AAD Instances

### Application Scenarios

Once a website service is connected to AAD, you can switch its origin server IP address or origin server domain name to another AAD instance for protection by changing the corresponding high-defense IP resolution line.

#### NOTICE

The modified resolution lines take effect in about five minutes. To ensure normal service access, you are advised to perform this operation during off-peak hours.

### Resource and Cost Planning

Resource	Description	Quantity	Cost
AAD instance	Protects origin server domain names or IP addresses.	2	For details about AAD billing modes and standards, see <a href="#">Billing Items</a> .

### Procedure


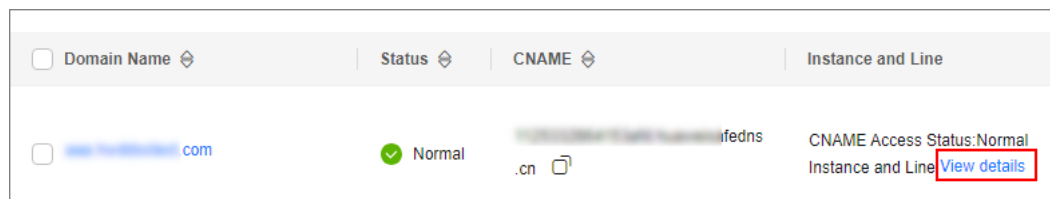
- Step 1** Log in to the management console.
- Step 2** Select a region in the upper part of the page, click  in the upper left corner of the page, and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS** page is displayed.
- Step 3** In the navigation pane on the left, choose **Advanced Anti-DDoS > Domain Name Access**.
- Step 4** Locate the target domain name, and click **View Details** in the **Instance and Line** column.

Figure 4-10 Viewing task details



Domain Name	Status	CNAME	Instance and Line
<input type="checkbox"/> <a href="#">[redacted].com</a>	<input checked="" type="checkbox"/> Normal	<a href="#">[redacted].cn</a>	CNAME Access Status: Normal Instance and Line: <a href="#">View details</a>

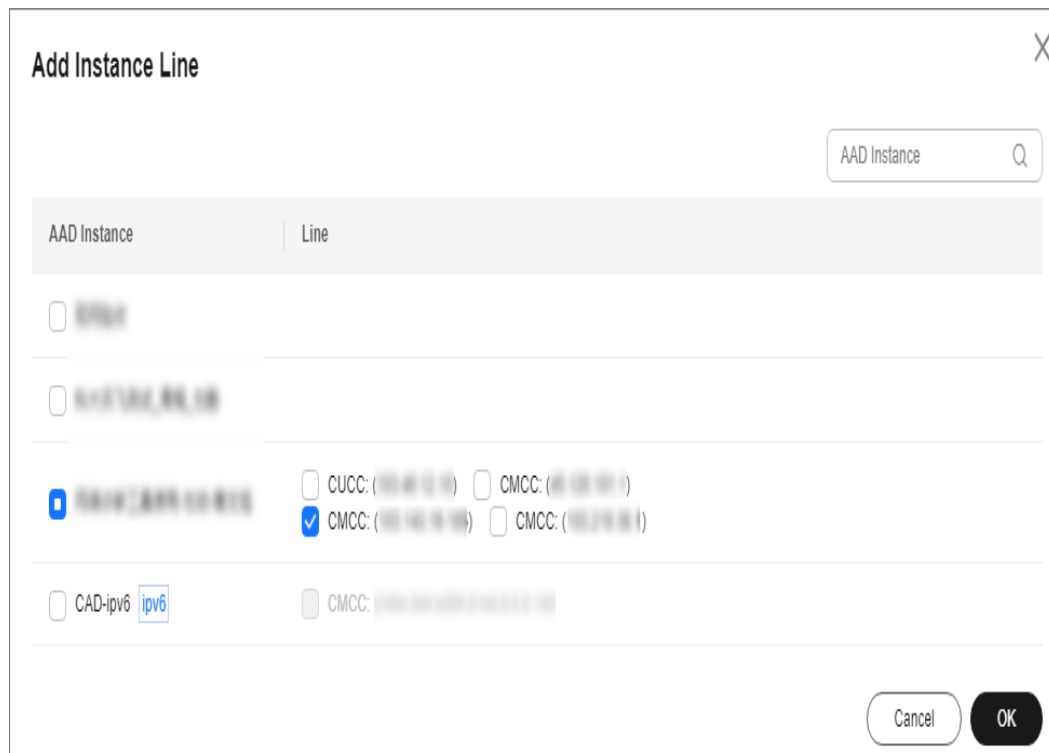
**Step 5** In the upper right corner of the instance line list, click **Add Instance Line**.

**Figure 4-11** Adding an instance line



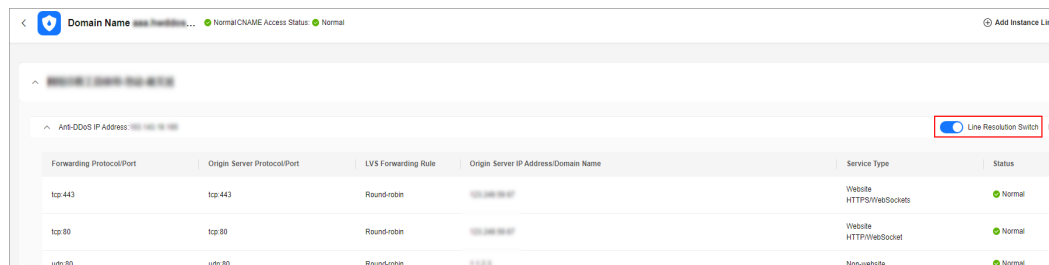
**Step 6** In the displayed dialog box, click **Add Instance Line**, and click **OK**.


**Figure 4-12** Adding a line



**Step 7** Set the **Line Resolution Switch** of the newly added line to .

**Figure 4-13** Line resolution



**Step 8** Set **Line Resolution Switch** of the old line to  to disable DNS resolution for the high-defense IP address of the old AAD instance and line.

**Step 9** Click **Delete Line**. In the displayed dialog box, click **OK** to delete the AAD instance and the high-defense IP address of the line.

 **CAUTION**

You are not advised to delete the line until 24 hours after disabling the domain name resolution function of the high-defense IP address in the old AAD instance and line.

---

----End

# 5 Using the Scheduling Center to Implement Tiered Traffic Scheduling.

## Application Scenarios

If you use both CNAD Unlimited Protection Basic Edition and AAD, you can configure tiered scheduling rules to schedule AAD to protect your cloud resources protected by the Unlimited Protection Basic Edition. This can significantly enhance the DDoS attack defense capability.

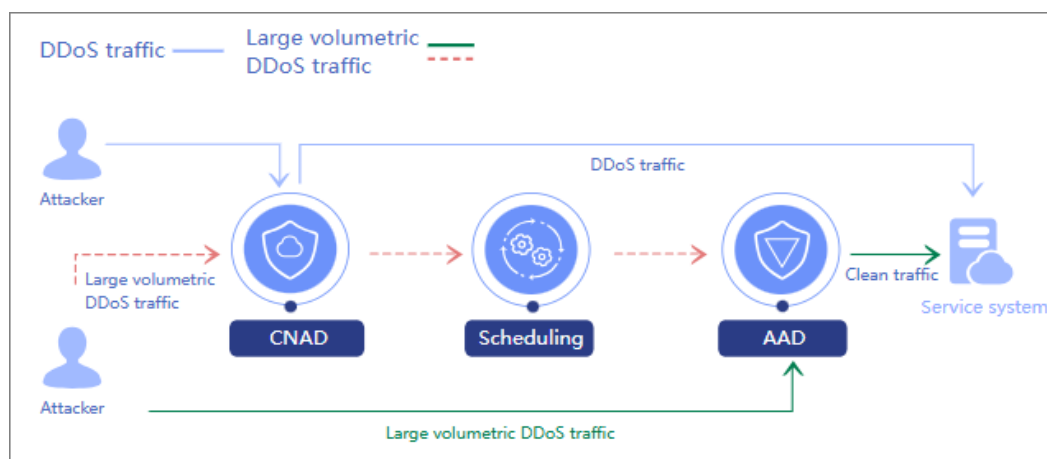
This section uses the domain name **www.example.com** of a website service as an example to describe how to use the scheduling center to implement tiered traffic scheduling.

## Architecture

**Figure 5-1** shows the working principle of tiered DDoS scheduling.

- CNAD Advanced offers comprehensive protection against DDoS attacks. If a DDoS attack is detected, traffic scrubbing will be automatically initiated.
- When a service is blocked due to heavy traffic attacks, AAD CNAMEs will be called to divert malicious attack traffic to AAD for scrubbing, ensuring that important services are not interrupted.

**Figure 5-1** Working principle of DDoS tiered scheduling



## Advantages

The Unlimited Protection Basic Edition defends against routine DDoS attacks without requiring the origin server IP address to be changed. Service traffic is directly transmitted to the origin server, so there is no extra latency.

When there are a large number of DDoS attacks, AAD is called to protect the cloud resources of the Unlimited Protection Basic Edition's protected objects. In this case, service traffic is forwarded by AAD.

## Limitations and Constraints


- The protected domain name (www.example.com) is deployed on Huawei Cloud in a region that supports CNAD Advanced instances (for example, CN North-Beijing4).
- The protected domain name (www.example.com) is not connected to WAF.

## Resource and Cost Planning

Resource	Description	Quantity	Cost
CNAD Unlimited Protection Basic Edition	Defends against routine attacks. (Service traffic is directly transmitted to the origin server.)	1	For details about the billing modes and standards, see <a href="#">Billing Overview</a> .
AAD	Defends against massive attacks. (Service traffic is forwarded through AAD.)	1	

## Step 1: Purchasing and Configuring a CNAD Advanced Instance

**Step 1** [Log in to the management console](#).

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS** page is displayed.

**Step 3** In the upper right corner of the page, click **Buy DDoS Mitigation**.


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

- **Instance Type: Cloud Native Anti-DDoS**
- **Billing Mode: Yearly/Monthly**
- **Region: Chinese Mainland**
- **Protection Level: Unlimited Protection Basic Edition**
- Set other parameters as required.



- Step 5** Choose **Cloud Native Anti-DDoS Advanced > Instances**. The instance list page is displayed.
- Step 6** In the row containing the target instance, click **Add Protected Object**.
- Step 7** In the **Add Protected Object** dialog box that is displayed, select the origin server IP address of the protected domain name **www.example.com** and click **Next**.
- Step 8** Select a protection policy and click **OK**.
- End

## Step 2: Purchasing and Configuring an AAD Instance

- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Anti-DDoS Service**. The **Anti-DDoS** page is displayed.
- Step 3** In the upper right corner of the page, click **Buy DDoS Mitigation**.
- Step 4** Set the purchase parameters as required, click **Buy Now**, and complete the payment as prompted.
- **Instance Type: Advanced Anti-DDoS**
  - **Access Type: Website**
  - **Region: Chinese Mainland**
  - Set other parameters as required.
- Step 5** Choose **Advanced Anti-DDoS > Domain Name Access**. The domain name list page is displayed.
- Step 6** On the **Chinese Mainland** tab page, click **Add Domain Name**.
- Step 7** Enter the domain name information and click **Next**.
- **Protected Domain Name:** Enter the domain name to be protected, for example, **www.example.com**.
  - **Origin Server Type:** Select **IP address**.
  - **IP Address:** Enter the public IP address of the origin server.
  - **Forwarding Protocol:** Enter the forwarding protocol of the origin server.
  - **Origin Server Port:** Enter the port used by the origin server.

**Figure 5-2** Configuring a website domain

Protected Domain Name (?)

www.\*\*\*.com

Enter a domain name, for example, www.domain.com. For multiple second-level domains, enter \*.domain.com.

Origin Server Type

IP address  Domain name

IP address

Enter a maximum of 20 IP addresses. Use commas (,) to separate multiple IP addresses. Each IP address is unique and invalid IP addresses such as 127.0.0.1, 172.16.\*.\*, 192.168.\*.\*, 10.0~255.\*.\* are not allowed

If the origin server is exposed, [fix the problem by referring to "Solution to Origin Server IP Exposure After AAD Is Connected"](#)

Origin Server Configuration

Forwarding Protocol	Origin Server Port	
HTTP	80	Delete

[Add](#)

You can add 3 more origin server configurations.

**Step 8** Select an AAD instance and line, and click **Submit and Continue**.

**Figure 5-3** Selecting an AAD instance and line

Protected Domain Name

www.\*\*\*.com

Enterprise Project

default

AAD Instance and Line

Select a property or enter a keyword.

AAD Instance	Line
<input checked="" type="checkbox"/> CAD-0001	

**Step 9** Click **Next**, and then click **Finish**.

After the domain name is connected to AAD. Obtain the CNAME value of the AAD instance, as shown in **Figure 5-4**.

**Figure 5-4** Domain name connected to AAD

Domain Name	Status	CNAME	Instance and Line	Origin Server IP Address/D...
<a href="#">www.weisafedns.cn</a>	Normal	1531293c2501- s.cn	CNAME Access Status: Normal Instance and Line: <a href="#">View details</a>	

----End

### Step 3: Configuring Tiered Scheduling

**Step 1** [Log in to the management console.](#)

**Step 2** Hover the mouse over the **Service List** icon, choose **Security & Compliance > DDoS Mitigation**, and click **Advanced Anti-DDoS**.

**Step 3** In the displayed **DDoS Migration Center** page, choose **Scheduling Center > Tiered Protection**.

**Step 4** In the upper left corner of the tiered scheduling list, click **Create Rule**.

**Step 5** In the dialog box that is displayed, set the parameters of the scheduling rule.

- **Name:** Enter the scheduling rule name.
- **Scheduling Group:** Select the region, origin server IP, and group ID of the CNAD Advanced instance. A maximum of 10 IP addresses can be added.
- **Auto AAD:** Select **CNAD and AAD**.
- **AAD CNAME:** Enter the CNAME value of the AAD instance obtained from [Step 9](#).

**Figure 5-5** Creating a scheduling rule

#### Create Rule

Name

Scheduling Group ?  
   Delete

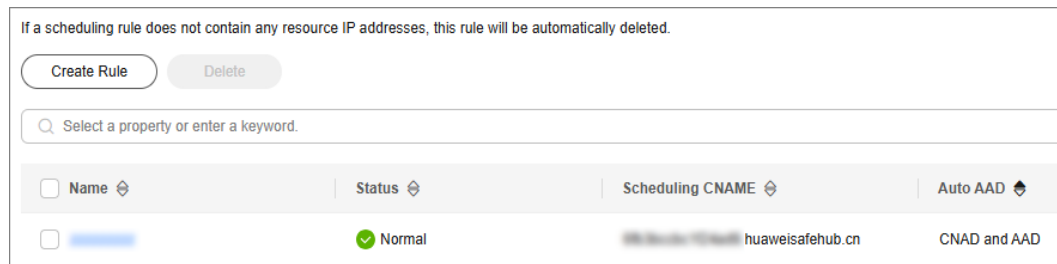
[Add](#)  
Only resources (such as ECS, EIP, ELB, and WAF) of cloud native anti-DDoS objects can be added.

Auto AAD ?  
 CNAD only  CNAD and AAD

AAD CNAME

**Step 6** Click **OK**

**Step 7** In the tiered scheduling rule list, obtain the scheduling CNAME.

**Figure 5-6** Scheduling CNAME

----End

## Step 4: Modifying DNS Resolution

**Step 1** [Log in to the management console](#).

**Step 2** In the service list, choose **Network > Domain Name Service**.

**Step 3** In the navigation pane, choose **Public Zones**.

**Step 4** In the row containing the target domain name (for example, www.example.com), click **Manage Record Set**.

**Step 5** Click **Add Record Set**.

- **Record Type:** Select **CNAME-Map one domain to another**.
- **Line:** **Default**
- **Value:** Scheduling CNAME value obtained from [Step 7](#).
- Set other parameters as required.

----End