Anti-DDoS
Quick Start

Copyright Notice

Trademark Notice

Tencent Cloud

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Quick Start
- Anti-DDoS Pro Package
- Anti-DDoS Advanced IP
  - Website Business Integration
  - Non-Website Business Integration
  - Anti-DDoS Advanced (Global Enterprise Edition)

Quick Start
Anti-DDoS Pro Package

Last updated: 2025-03-19 21:34:15

Anti-DDoS Pro provides higher DDoS protection capabilities for Tencent Cloud public IP addresses, supporting the protection of products and services such as CVM, CLB, NAT, WAF, etc. Anti-DDoS Pro is easy to connect, requiring no changes to business IP addresses, allowing for quick completion of protection configuration.

Prerequisites

Before binding a protected IP, you need to successfully purchase Anti-DDoS Pro (Standard Edition) or Anti-DDoS Pro (Lite Edition).

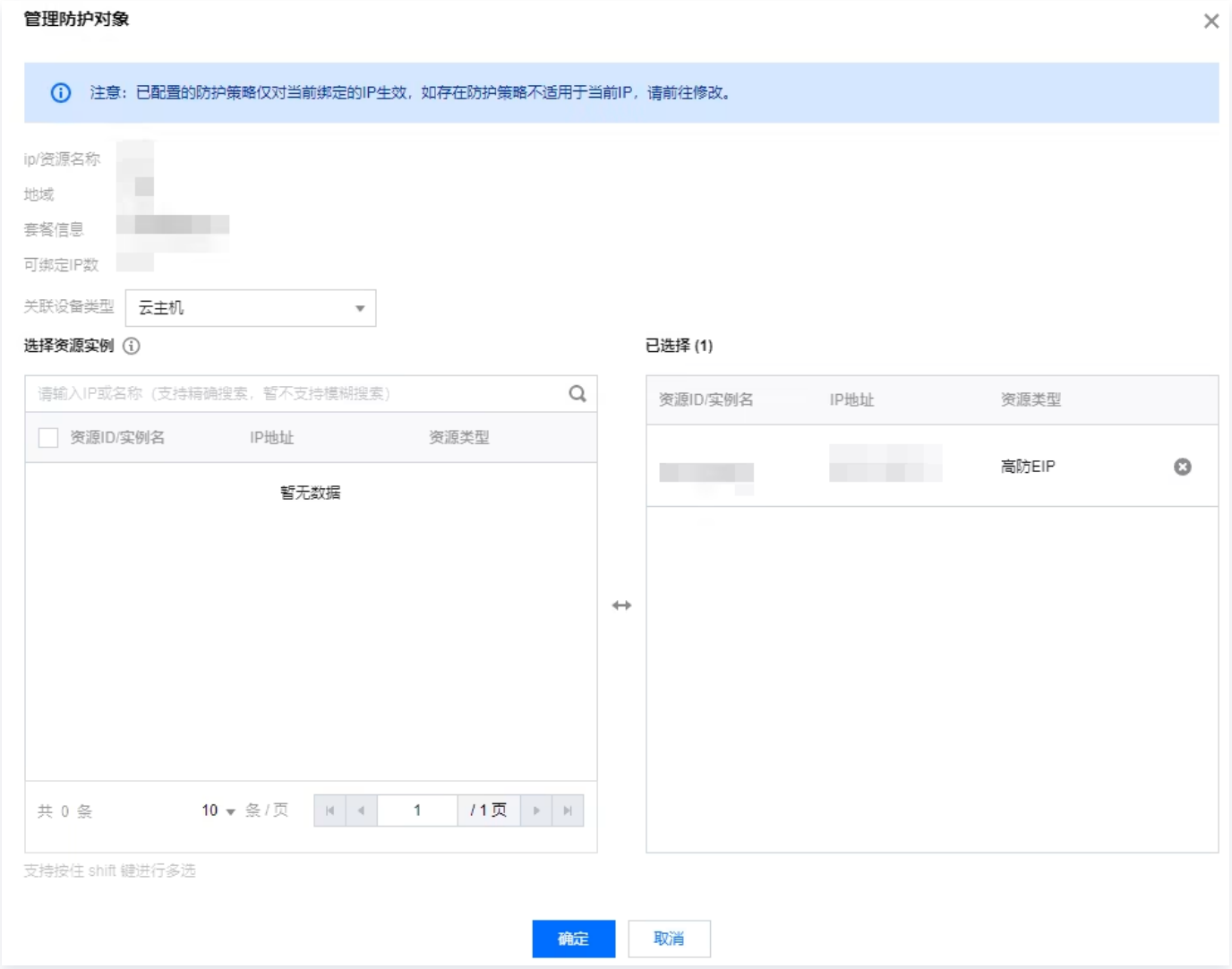
Operation Steps

1. Log in to the Anti-DDoS (New Version) console, and click **Anti-DDoS instances** in the left sidebar.
2. On the Anti-DDoS instances page, select the target instance and click **manage protection object** in the operation column.

3. In the manage protection object window, select "Associated Device Type" and "Resource Instance" according to actual protection needs.

> **Note:**
> Anti-DDoS Pro supports managed IP, which is currently available for use in the allowlist. If a user uses Tencent Cloud's managed IP and needs to connect to Anti-DDoS Pro, please call 4009100100 ext. 1 (Monday to Friday, 9:00 am – 6:00 pm) for consultation, or submit a ticket to apply for use.

- Associated device types: Supports Cloud Host, Cloud Load Balancer, Web Application Firewall, and other public cloud resources with a public IP address.
- Select resource instances: Multi-option selection is allowed. The number of "selected resource instances" must not exceed the number of IP addresses that can be bound.



4. After completing the selection, click **Confirm**.

> **Note:**
> After the connection is completed, if personalized protection is required, you can configure it on the Protection Configuration page. For details, please refer to the Protection Configuration document.

Anti-DDoS Advanced IP Website Business Integration

Last updated: 2026-03-11 17:46:43

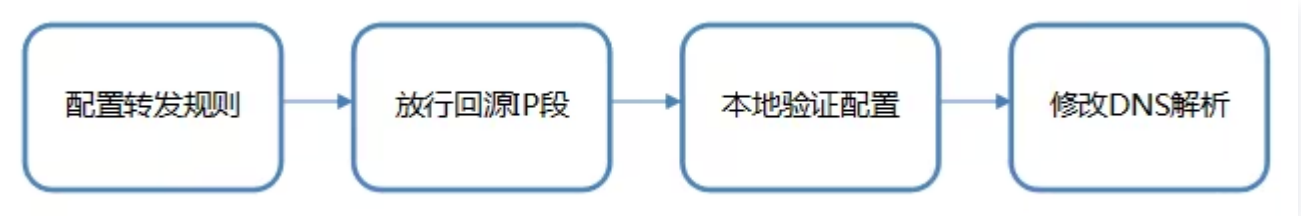
This document introduces the detailed operation steps for website business users to integrate their business into Anti-DDoS Advanced IP instances and verify the forwarding configuration.

> **Note:**
> The operation steps for website business integration and non-website business integration are the same. The difference lies in the local verification configuration.

Prerequisites

- Before adding a forwarding rule, you need to successfully purchase an Anti-DDoS Advanced instance in Mainland China or an Anti-DDoS Advanced instance outside Mainland China.
- Before modifying the DNS information of your business domain, you need to successfully purchase a DNS product, such as Tencent Cloud's DNSPod.

Operating Procedures



Operation Steps

Configure Forwarding Rules

1. Log in to the Anti-DDoS (New Version) Console, and in the left directory, click **Business Access** > **Domain Access**.
2. On the domain access page, click **Start Access**.

3. On the domain business access page, select the associated instance ID, and click **Next: Protocol Port**.

> **Note:**
> Support multi-option, and synchronize multiple instances for integration.

4. Select the forwarding protocol and cert, enter the business domain, and click **Next: Origin-Pull Method**.

5. Select the origin-pull method, enter the origin server IP+Port or origin server domain name, and click **Next: Modify DNS Resolution**.

> **Note:**
> - Backup Origin Server: When the origin server forwarding encounters an exception, it will automatically switch to forward to the backup origin server.
> - Only supports standard protocol ports `(http:80, https:443)`.
> - Supports wildcard domain names.

6. Click **Complete** to finish the access rule.

> **Note:**
> After the integration is completed, if you need personalized protection, you can customize it on the Protection Configuration page. For details, see Protection Configuration documentation.

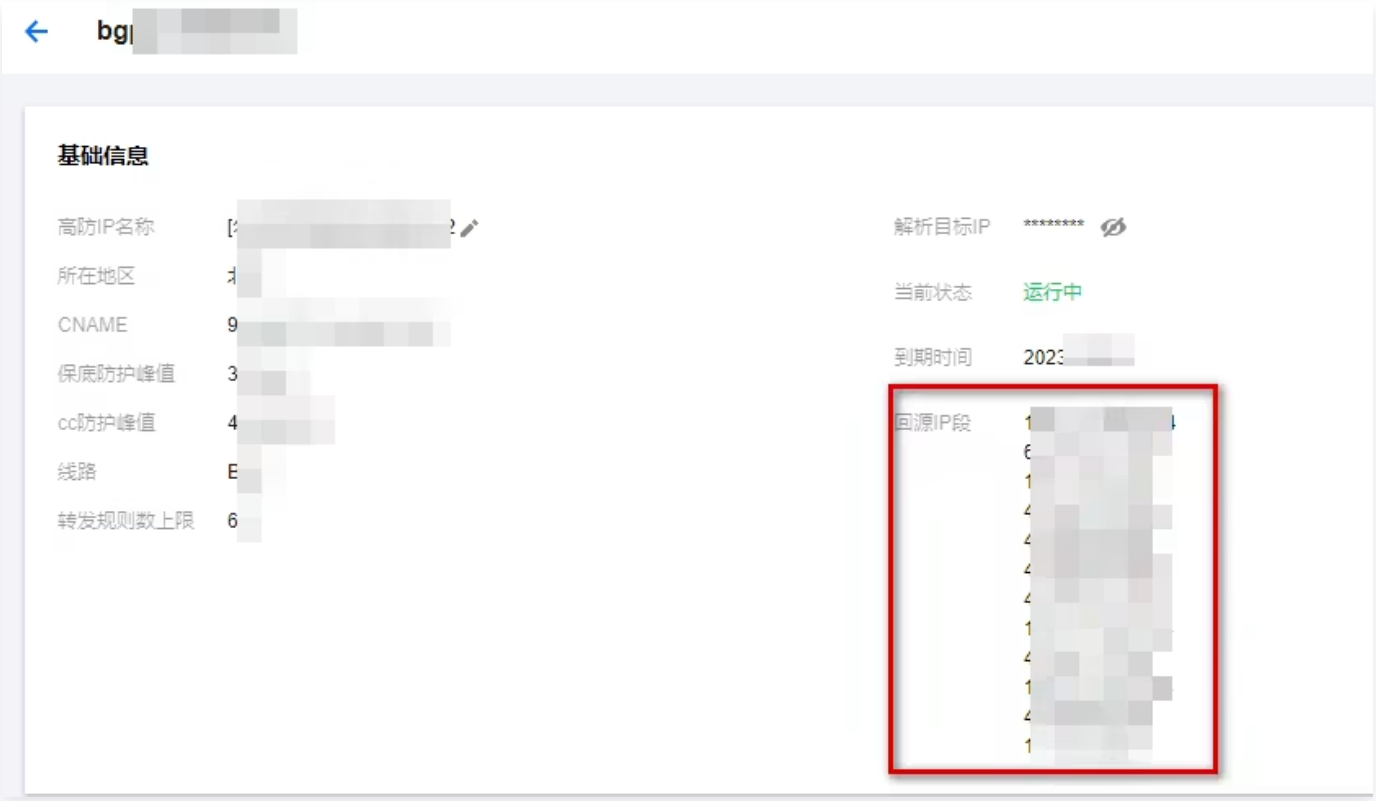
Allow Originating IP Range

To avoid the origin server intercepting the Anti-DDoS Advanced IP's origin-pull IP address and affecting the business, it is recommended to set an allowlist policy on the origin server's firewall, Web Application Firewall (WAF), IPS intrusion prevention system, traffic management and other hardware devices. Turn off the protection function of the host firewall on the origin

server and any other security software (such as Safe Dog, etc.) or set an allowlist policy to ensure that the Anti-DDoS Advanced IP's origin-pull IP address is not affected by the security policy of the origin server.

1. Log in to the Anti-DDoS (New Version) Console, and in the left sidebar, click **Anti-DDoS Instances**.
2. On the Anti-DDoS Instances page, select the target instance, and click **Instance ID** in the operating column.

3. On the basic information page, view the origin-pull IP range.



Validate Local Configuration

After the forwarding configuration is completed, the high-protection IP of the Anti-DDoS Advanced IP instance will forward the messages of related ports to the corresponding ports of the origin server according to the forwarding rules.
To ensure the maximum stability of the business, it is recommended to conduct a local test before fully switching the business. The specific verification method is as follows:

1. Modify the local hosts file so that requests for the protected site go through the anti-DDoS locally. Below is an example for configuring the local hosts file on Windows OS.
   Open the hosts file in `C:\Windows\System32\drivers\etc` path on the local computer, and add the following content at the end of the file:

```
<High-defense IP address> <Domain name of the protected website>
```

2. For example, if the high-protection IP is 10.1.1.1 and the domain name is `www.qqq.com`, then add:

```
10.1.1.1 www.qqq.com
```

   Save the hosts file. Run the ping command on the local computer for the protected domain name. When the resolved IP address is the Anti-DDoS Advanced IP address bound in the hosts file, it means that the local hosts file takes effect.

> **Note:**
> If the resolved IP address is still the origin server address, you can try running `ipconfig /flushdns` command in Windows Command Prompt to refresh the local DNS cache.

3. After confirming that the hosts binding has taken effect, verify it using the domain name. If it can be accessed normally, it means the configuration has taken effect.

> **Note:**
> If the correct method shows verification failure, please log in to the Anti-DDoS Advanced console to check whether the configuration is correct. After excluding configuration errors and incorrect verification methods, if the problem still exists, please submit a ticket to contact us for assistance.

Modify DNS Resolution

If you need to modify DNS resolution, please refer to Configure Intelligent Scheduling document for DNS resolution modification operations.

> **Note:**
> The high-defense resource will provide a CNAME. Please modify the DNS resolution address to this CNAME high-defense resource. The CNAME resolution destination high-defense IP will be changed periodically. (Not involving triple-network resources).

Non-Website Business Integration

Last updated: 2026-03-11 17:47:56

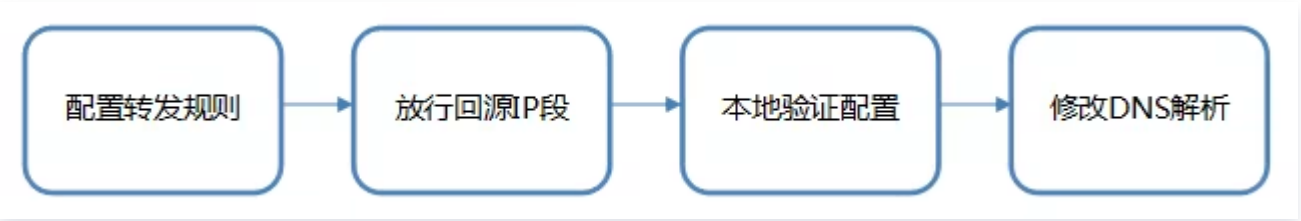
This document describes how non-website business users can connect their services to an Anti-DDoS Advanced instance and verify the forwarding configuration.

> **Note:**
> The operation steps for non-website business access and website business access are the same. The difference lies in the local verification configuration.

Prerequisites

- Before adding a forwarding rule, you need to successfully purchase an Anti-DDoS Advanced instance in Mainland China or an Anti-DDoS Advanced instance outside Mainland China.
- Before modifying the DNS information of a business domain, you need to successfully purchase a DNS product, such as Tencent Cloud's DNSPod.

Operating Procedures



Operation Steps

Configure Forwarding Rules

1. Log in to the Anti-DDoS (New Version) Console, and click **Business Access** > **Domain Access** in the left directory.
2. On the domain access page, click **Start Access**.

3. On the domain business access page, select the associated instance ID, and click **Next: Protocol Port**.

> **Note:**
> Multiple selections are supported, allowing multiple instances to be connected simultaneously.

4. Select the forwarding protocol and certificate, fill in the business domain name, and click **Next: Origin-Pull Method**.

5. Select the origin-pull method, fill in the origin server IP+port or origin server domain name, and click **Next: Modifying DNS Resolution**.

> **Note:**
> - Backup origin server: When the origin server forwarding encounters an exception, it will automatically switch to forward to the backup origin server.
> - Supports wildcard domain names.

6. Click **Complete** to finish the access rule.

> **Note:**
> After the connection is completed, if personalized protection is required, you can configure it on the protection configuration page. For details, please refer to the Protection Configuration document.

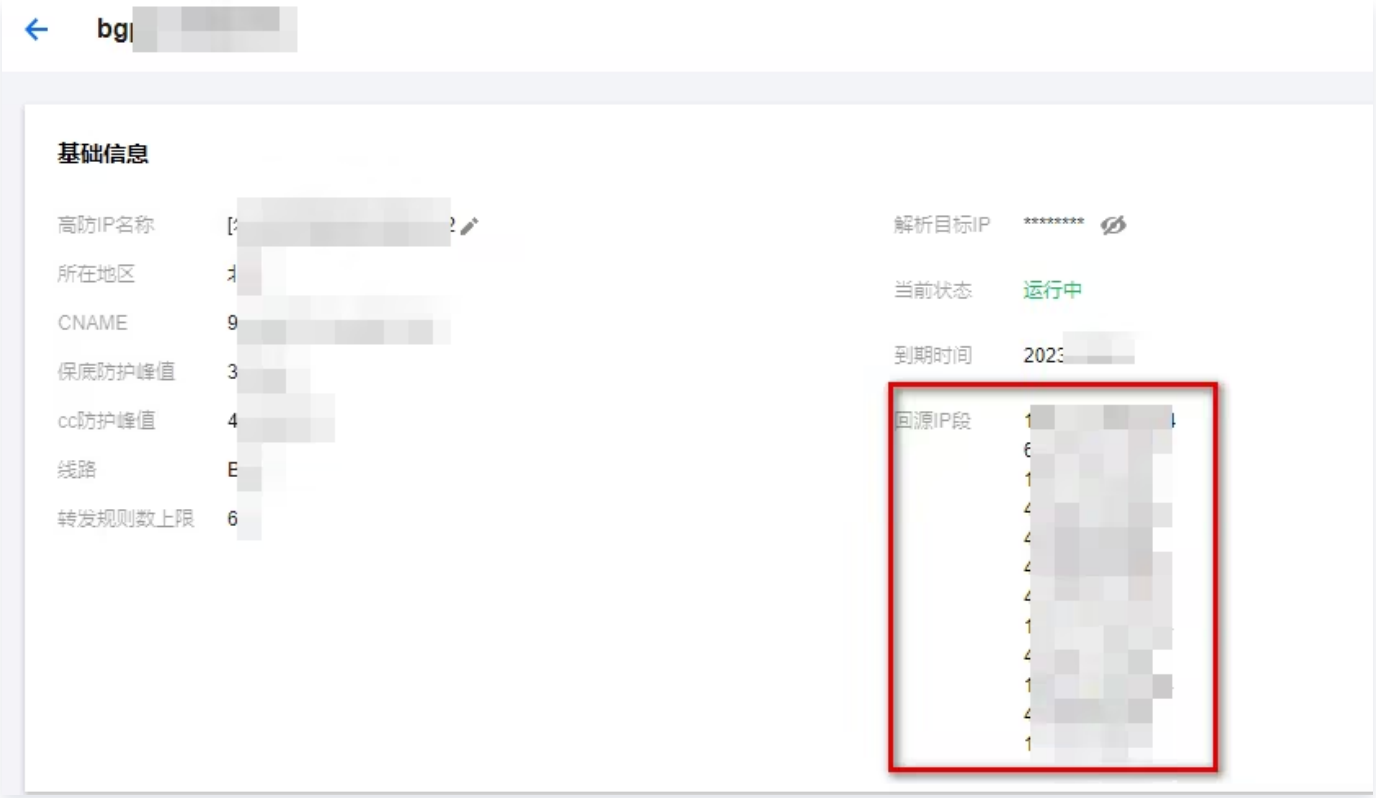
Release Origin-Pull IP Range

To avoid the origin server intercepting the origin-pull IP address of the Anti-DDoS Advanced and affecting the service, it is recommended to set an allowlist policy on the origin server's firewall, Web Application Firewall (WAF), IPS intrusion prevention system, traffic management,

and other hardware devices. Also, turn off the protection features of the host firewall and any other security software (such as Safe Dog, etc.) on the origin server or set an allowlist policy to ensure that the origin-pull IP of the high protection is not affected by the security policy of the origin server.

1. Log in to the Anti-DDoS (New Version) Console, and click **Anti-DDoS Instances** in the left sidebar.
2. On the Anti-DDoS Instances page, select the target instance, and click **Instance ID** in the operating column.

3. On the basic information page, view the origin-pull IP range.



Locally Validate Configuration

After the forwarding configuration is completed, the high-protection IP of the Anti-DDoS Advanced instance will forward the packets of the relevant ports to the corresponding ports of the origin server according to the forwarding rules. To ensure the maximum stability of the service, it is recommended to conduct local testing before fully switching the service. The specific verification methods are as follows:

- **Business accessed via IP**

  For services that interact directly through IP (such as gaming services), you can use the telnet command to access the high-protection IP port to check connectivity. If you can directly fill in the server IP on the local client, then fill in the high-protection IP for testing to see if the local client can connect normally.
  For example, if the high-protection IP is 10.1.1.1, the forwarding port is 1234, the origin server IP is 10.2.2.2, and the origin server port is 1234. Access 10.1.1.1:1234 locally through the telnet command. If the telnet command can connect, it means that the forwarding is successful.
- **Business accessed via domain name**

  For services that need to be accessed via domain name, you can verify whether the configuration is effective by modifying the local hosts file.

1. Modify the local hosts file so that local requests for the protected site go through the anti-DDoS. Below is an example for configuring the local hosts file on a Windows operating system.
   Open the hosts file in `C:\Windows\System32\drivers\etc` path on the local computer, and add the following content at the end of the file:

   ```
   <Anti-DDoS Advanced IP address> <Domain name of the protected website>
   ```

   For example, if the high-protection IP is 10.1.1.1 and the domain name is `www.qqq.com`, then add:

   ```
   10.1.1.1 www.qqq.com
   ```

Save the hosts file. Run the ping command on the local computer for the protected domain name. When the resolved IP address is the high-protection IP address bound in the hosts file, it means that the local hosts file is effective.

> **Note:**
> If the resolved IP address is still the origin server address, you can try running the `ipconfig /flushdns` command in Windows Command Prompt to refresh the local

DNS cache.

2. After confirming that the hosts binding has taken effect, verify it using the domain name. If it can be accessed normally, it means that the configuration has taken effect.

> **Note:**
> If the verification fails even when using the correct method, please log in to the Anti-DDoS Advanced console to check whether the configuration is correct. After excluding configuration errors and incorrect verification methods, if the problem persists, please submit a ticket to contact us for assistance.

Modify DNS Resolution

If you need to modify DNS resolution, please refer to the Configure Intelligent Scheduling document for modifying DNS resolution operations.

> **Note:**
> The high-defense resource will provide a CNAME. Please modify the DNS resolution address to this CNAME high-defense resource. The destination high-defense IP of the CNAME resolution will be changed periodically. (Not involving triple-play resources).

Anti-DDoS Advanced (Global Enterprise Edition)

Last updated: 2026-03-11 17:51:41

Anti-DDoS Advanced (Outside Chinese Mainland Enterprise Edition) is a paid product for users whose businesses are deployed in areas outside Chinese mainland on Tencent Cloud, aiming to improve DDoS protection capabilities outside Chinese mainland.

- Anti-DDoS Advanced (global enterprise) can be independently purchased and hold public network address resources.
- After Anti-DDoS Advanced (global enterprise) is bound to cloud resources, cloud resources can communicate with the public network through Anti-DDoS Advanced (global enterprise).

This article uses the association of Anti-DDoS Advanced (global enterprise) with cloud resources as an example to introduce the usage lifecycle of Anti-DDoS Advanced (global enterprise).

Background

The usage lifecycle of Anti-DDoS Advanced (global enterprise) includes purchasing Anti-DDoS Advanced (global enterprise), configuring protection rules for Anti-DDoS Advanced (global enterprise) instances, configuring business rules for Anti-DDoS Advanced (global enterprise), and the destruction of Anti-DDoS Advanced (global enterprise).

1. Proceed to purchase Anti-DDoS Advanced (global enterprise): Purchase Anti-DDoS Advanced (global enterprise) resources based on actual needs.
2. Anti-DDoS Advanced (global enterprise) instance Configure protection rules: Configure protection policies that fit the business.
3. Configure business rules for Anti-DDoS Advanced (global enterprise): Associate the Anti-DDoS Advanced (global enterprise) instance with the cloud resources that need protection.
4. Terminate Anti-DDoS Advanced (global enterprise): After disassociating Anti-DDoS Advanced (global enterprise) from cloud resources, you can associate it with other cloud resources. Disassociation may cause network issues for the corresponding cloud

resources, and Anti-DDoS Advanced (global enterprise) not bound to cloud resources will incur IP resource fees.

Operation Steps

Purchase DDoS High-Defense IP (Global Enterprise)

1. Log in to the Anti-DDoS Advanced (global enterprise) console.
2. Refer to the Purchase Guide above to purchase a package.
3. Click **Anti-DDoS instances** on the console to view the purchased Anti-DDoS Advanced (Global Enterprise Edition), which is currently unbound.

> **Note:**
> It is recommended that you bind cloud resources for the unbound Anti-DDoS Advanced (global enterprise) in a timely manner to save IP resource fees. The IP resource fee is billed by the hour and is accurate to the second. If it is less than one hour, the fee will be charged according to the proportion of idle time. Therefore, please bind the cloud resources in a timely manner. For detailed standards, see Billing Overview.

Configure Protection Rules

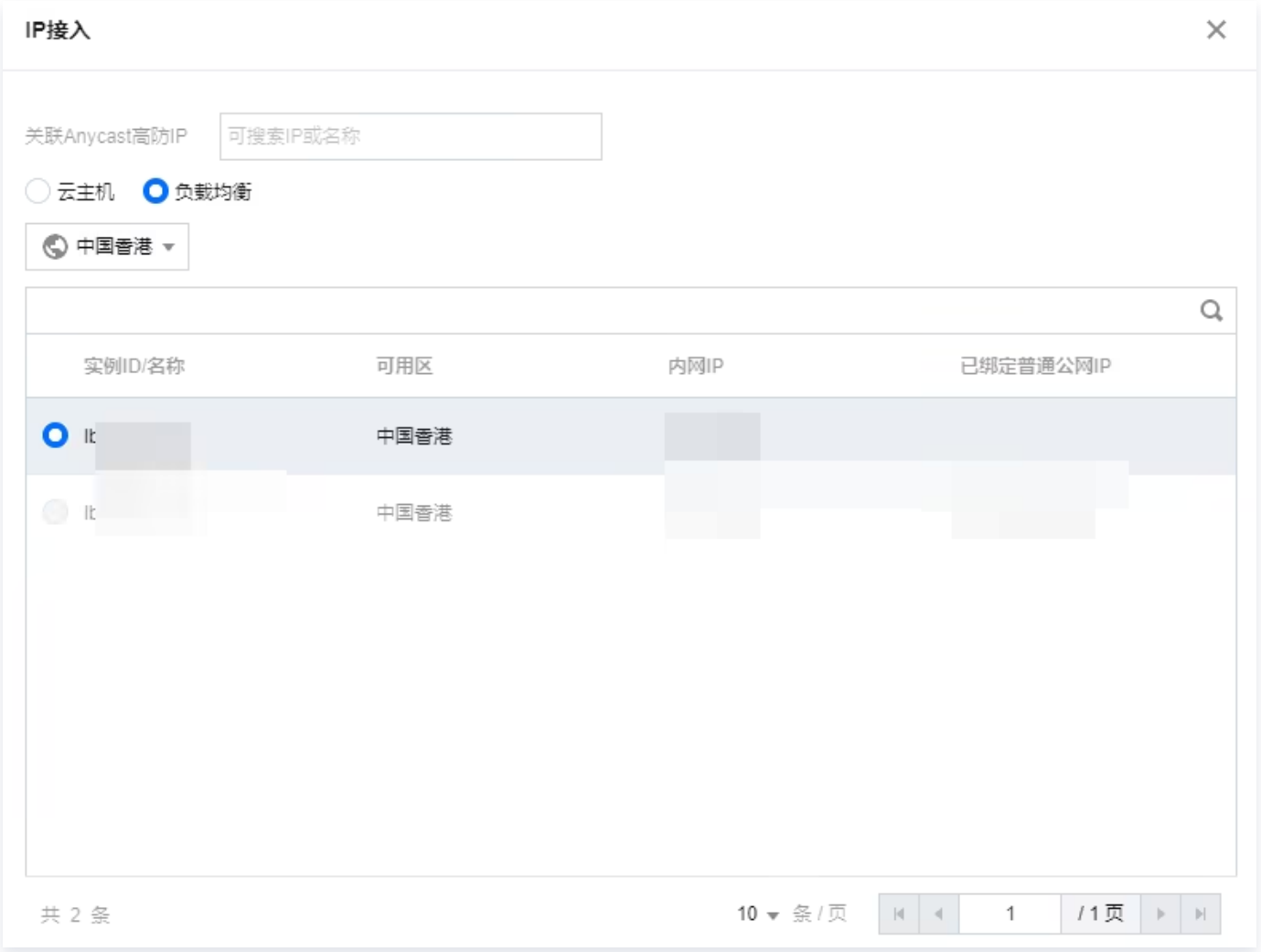
1. Log in to the Anti-DDoS (New Version) console, and in the left sidebar, click **Anti-DDoS instances**.
2. Select the corresponding Anti-DDoS Advanced (global enterprise) instance, click **Protection Configuration**, and refer to Configure Protection Rules for configuration methods.

Associate Cloud Resources

1. Log in to the Anti-DDoS (New Version) console, click **Business Access** > **IP Access**.

2. On the IP Access page, click **start access**.
3. On the IP Access page, select the Anti-DDoS Advanced (global enterprise) instance at "Associate Anycast High Defense IP", click **OK** to complete the binding with the cloud resource.

> **Note:**
> Resources that have been bound to a public IP or Anycast IP cannot be bound again.



Unlinking Cloud Resources

1. On the IP Access page, select the required instance, click **Delete** in the operation column.

2. In the Unbind pop-up window, click **OK** to disassociate.

> **Note:**
> Unbinding may cause your cloud resource network to be disconnected. Please proceed with caution. After it is unbound, you can bind the resource to other cloud resources.