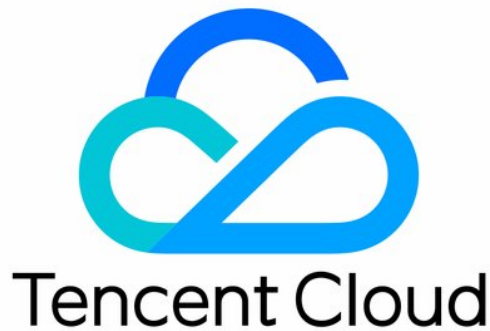


# Anti-DDoS

## Getting Started

### Product Documentation



## Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

## Trademark Notice

 Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

## Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

---

# Contents

## Getting Started

- Anti-DDoS Pro

- Anti-DDoS Advanced

  - Website Business Connection

  - Non-Website Business Connection

  - Anti-DDoS Advanced (Global Enterprise)

# Getting Started

## Anti-DDoS Pro

Last updated : 2024-07-01 11:20:28

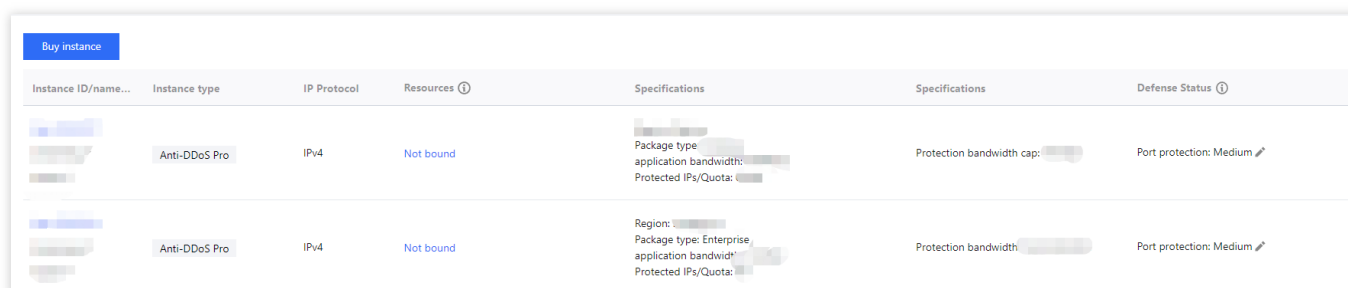
Anti-DDoS Pro provides Tencent Cloud public IPs with higher anti-DDoS capability. It supports Tencent Cloud services such as CVM, CLB, NAT, and WAF. It is easy to connect and requires no IP changes.

## Prerequisite

You need to purchase an [Anti-DDoS Pro \(Standard\) instance](#) first before you can bind it to the IP address you want to protect.

## Directions

1. Log in to the new [Anti-DDoS console](#) and click **Anti-DDoS Instances** on the left sidebar.
2. On the **Anti-DDoS Instances** page, select a target Anti-DDoS Pro instance and click **Protected Resource** in the **Operation** column.



The screenshot shows a table with columns: Instance ID/name..., Instance type, IP Protocol, Resources, Specifications, Specifications, and Defense Status. Two rows are visible, both for Anti-DDoS Pro instances with IPv4 protocol and 'Not bound' resources. The first row shows 'Port protection: Medium' and 'Protection bandwidth cap:'. The second row shows 'Region:', 'Package type: Enterprise', 'application bandwidth:', and 'Protected IPs/Quota:'.

Instance ID/name...	Instance type	IP Protocol	Resources	Specifications	Specifications	Defense Status
[blurred]	Anti-DDoS Pro	IPv4	Not bound	Package type: [blurred] application bandwidth: [blurred] Protected IPs/Quota: [blurred]	Protection bandwidth cap: [blurred]	Port protection: Medium
[blurred]	Anti-DDoS Pro	IPv4	Not bound	Region: [blurred] Package type: Enterprise application bandwidth: [blurred] Protected IPs/Quota: [blurred]	Protection bandwidth: [blurred]	Port protection: Medium

3. In the **Protected Resource** window, select a device type and a resource instance as needed.

### Note:

Anti-DDoS Pro supports Tencent Cloud managed IPs, which is currently available for beta users. If you want to use this feature, please call 4009100100 ext. 1 (Monday–Friday, 9:00–18:00) or [submit a ticket](#).

**Device type:** Support public cloud resources (such as CVM, CLB, and WAF) with public IPs.

**Select instance:** You can select one or more instances. The maximum instances selected cannot exceed the number of bound IPs.

**Protected Resource**

**i** Note: Configured protection policy only works to the currently bound IP. If the protection policy is not applicable to

IP/Resource name

Region

Plan information

Max bound IPs

Device type

**Select instance** **i**

**Selected (0)**

Please enter IP or name (exact search is supported, fuzzy search is not supported)

<input type="checkbox"/>	Resource ID/Name	IP address	Resource type
No data yet			

Total items: 0    10 / page      1 / 1 page

Resource ID/Name	IP address
------------------	------------

You can make multiple selection by holding down the Shift key

4. Click **OK**.

**Note:** After you have connected to the service, you can customize your protection settings on the **Configurations** page. For more information, see [Protection Configuration](#).



# Anti-DDoS Advanced

## Website Business Connection

Last updated : 2024-07-01 11:20:28

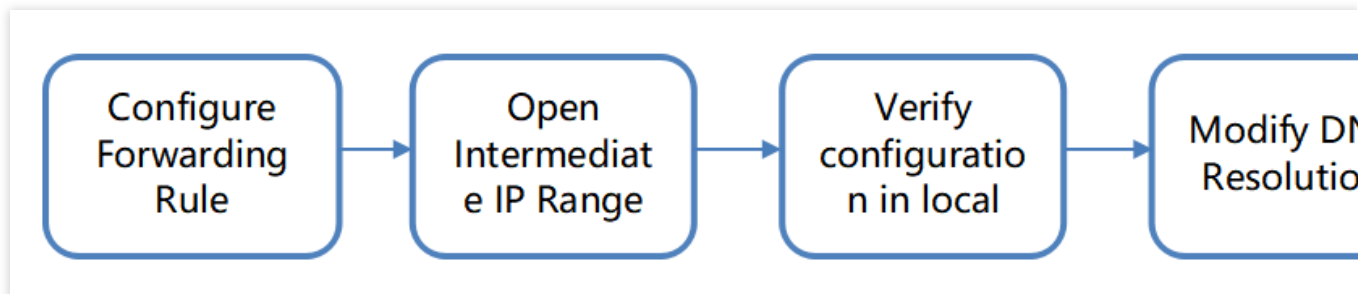
This document describes how to connect a website business to an Anti-DDoS Advanced instance and verify the forwarding configuration.

### Prerequisite

To add a forwarding rule, you need to purchase an [Anti-DDoS Advanced \(Chinese Mainland\)](#) or [Anti-DDoS Advanced \(Global\)](#) instance.

To modify the DNS information of your business domain name, you need to purchase a DNS service, such as Tencent Cloud **DNSPod**.

### Process




### Directions

#### Configuring forwarding rules

1. Log in to the new [Anti-DDoS console](#), and click **Business Access** > **Access via domain name** on the left sidebar.
2. On the **Access via domain name** tab, click **Start access**.

**Application Accessing**

IP access    Access via ports    **Access via domain names**    IP access ⓘ



**Access via Domain Name**

If your business is a website business, you can add forwarding rules through the Anti-DDoS Pro domain name business access method to effectively defend against DDoS and CC attacks for the website business. According to the rules you configure, the business traffic will first be cleaned by Anti-DDoS Pro, and then back to the target origin server, you can delete or edit existing rules. [View details](#)

Accessed business

**188**

---

Last access: 2023-08-21 20:14:41

Access

**53**

Start Access

Batch import

Batch export

Batch delete

3. On the **Access via Domain Name** page, select an associated instance ID and click **Next: Set Protocol Port**.

**Note:**

You can select multiple instances.


**Access via Domain Name**

**1** Select Instance >

2 Protocol port >


3 Set Forwarding


4 Modify DNS resolution



User

CNAME address/A record





Edge Defender

Forwarding port

---

Forwarding

---

Anti-DDoS Advanced

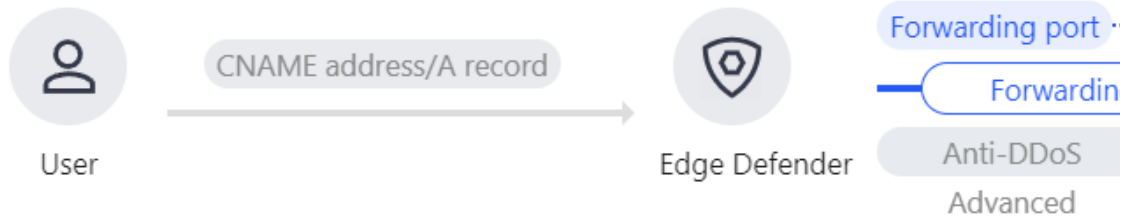
\* Associated Instance

4. Select a forwarding protocol and certificate, specify a domain name, and then click **Next: Set Forwarding Method**.



### Access via Domain Name

- ✓ **Select Instance** >
- 2 **Protocol port** >
- 3 **Set Forwarding**
- 4 **Modify DNS resolution**



\* Forwarding protocol  http

https

\* Application domain name

Recommended to enable protection configuration  CC Protection + CC AI Protection ⓘ

5. Select a forwarding method, specify a real server IP and port or a real server domain name, and then click **Next: Modify DNS Resolution**.

## Access via Domain Name

- Select Instance** > 
  **Protocol port** > 
  **3 Set Forwarding Method** > 
  **4 Modify DNS resolution**



\* Set Forwarding Method

**Forwarding via IP**

Forwarding via domain name

Clean traffic can be forwarded back to the real server by the IP or domain name.

\* Real Server IP & Port

Real server IP

Origin port

Enter the real server (eg: 1.1.1.1)

Eg: 80

**+ Add**

Please enter the combination of real server IP and port. Up to 16 entries.

### Note:

An alternate real server is used when the forwarding to the real server fails.

Only the standard protocol ports `80 (HTTP)` and `443 (HTTPS)` are supported.

Wildcard domain names are supported.

6. Click **Complete**.

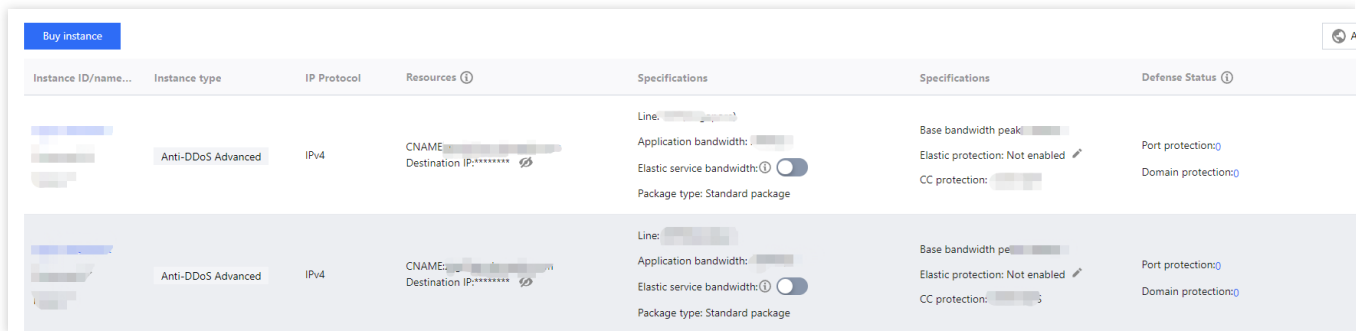
### Note:

After you have connected to the service, you can customize your protection settings on the **Configurations** page. For more information, see [Protection Configuration](#).

## Allowing forwarding IP ranges

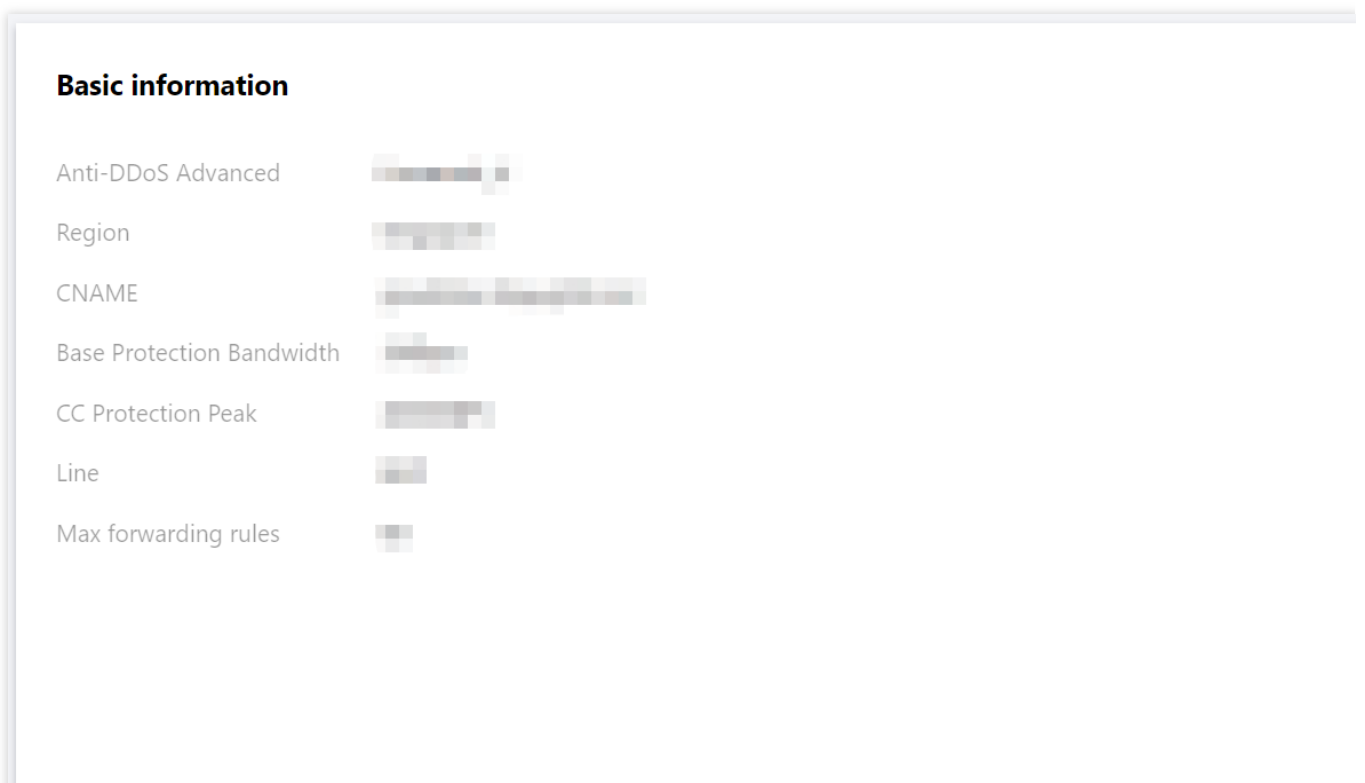
Allow the Anti-DDoS's forwarding IP in the firewall rules of the origin server or disable the firewall to , so that the forwarding IP will not be affected by the security policies of the real server.

1. Log in to the new [Anti-DDoS console](#) and click **Anti-DDoS instances** on the left sidebar.
2. On the **Anti-DDoS instances** page, select a target instance and click the **instance ID**.



Instance ID/name...	Instance type	IP Protocol	Resources	Specifications	Specifications	Defense Status
[Redacted]	Anti-DDoS Advanced	IPv4	CNAME: [Redacted] Destination IP: [Redacted]	Line: [Redacted] Application bandwidth: [Redacted] Elastic service bandwidth: [Redacted] Package type: Standard package	Base bandwidth peak: [Redacted] Elastic protection: Not enabled CC protection: [Redacted]	Port protection: [Redacted] Domain protection: [Redacted]
[Redacted]	Anti-DDoS Advanced	IPv4	CNAME: [Redacted] Destination IP: [Redacted]	Line: [Redacted] Application bandwidth: [Redacted] Elastic service bandwidth: [Redacted] Package type: Standard package	Base bandwidth pe: [Redacted] Elastic protection: Not enabled CC protection: [Redacted]	Port protection: [Redacted] Domain protection: [Redacted]

3. On the **Basic information** page, you will see the forwarding IP ranges.



Basic information	
Anti-DDoS Advanced	[Redacted]
Region	[Redacted]
CNAME	[Redacted]
Base Protection Bandwidth	[Redacted]
CC Protection Peak	[Redacted]
Line	[Redacted]
Max forwarding rules	[Redacted]

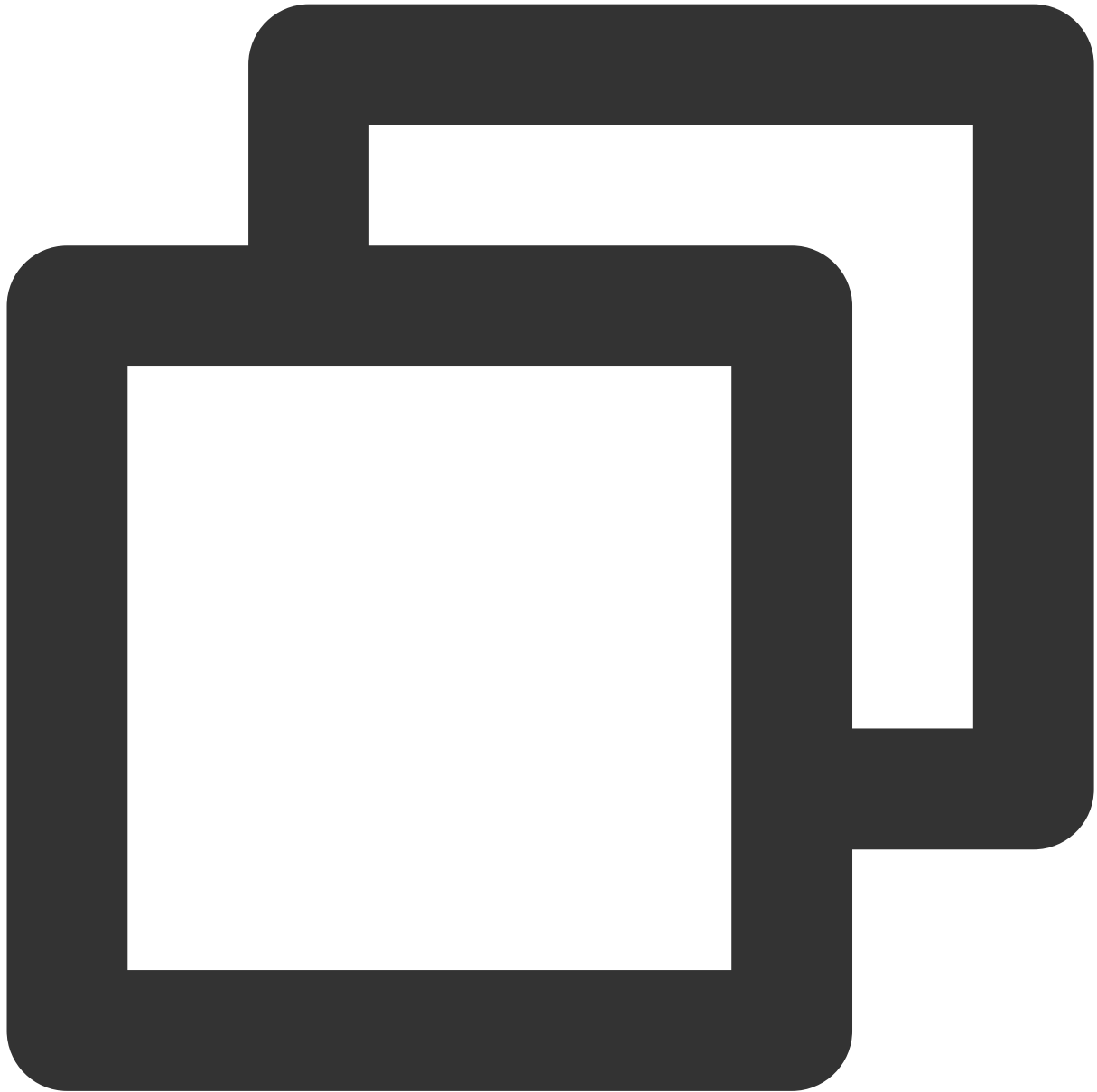
## Verifying configuration locally

After the forwarding configuration is completed, the Anti-DDoS Advanced IP will forward packets from the relevant port to the corresponding real server port according to the forwarding rules.

To ensure the stability of your business, a local test is recommended. The verification methods are as follows:

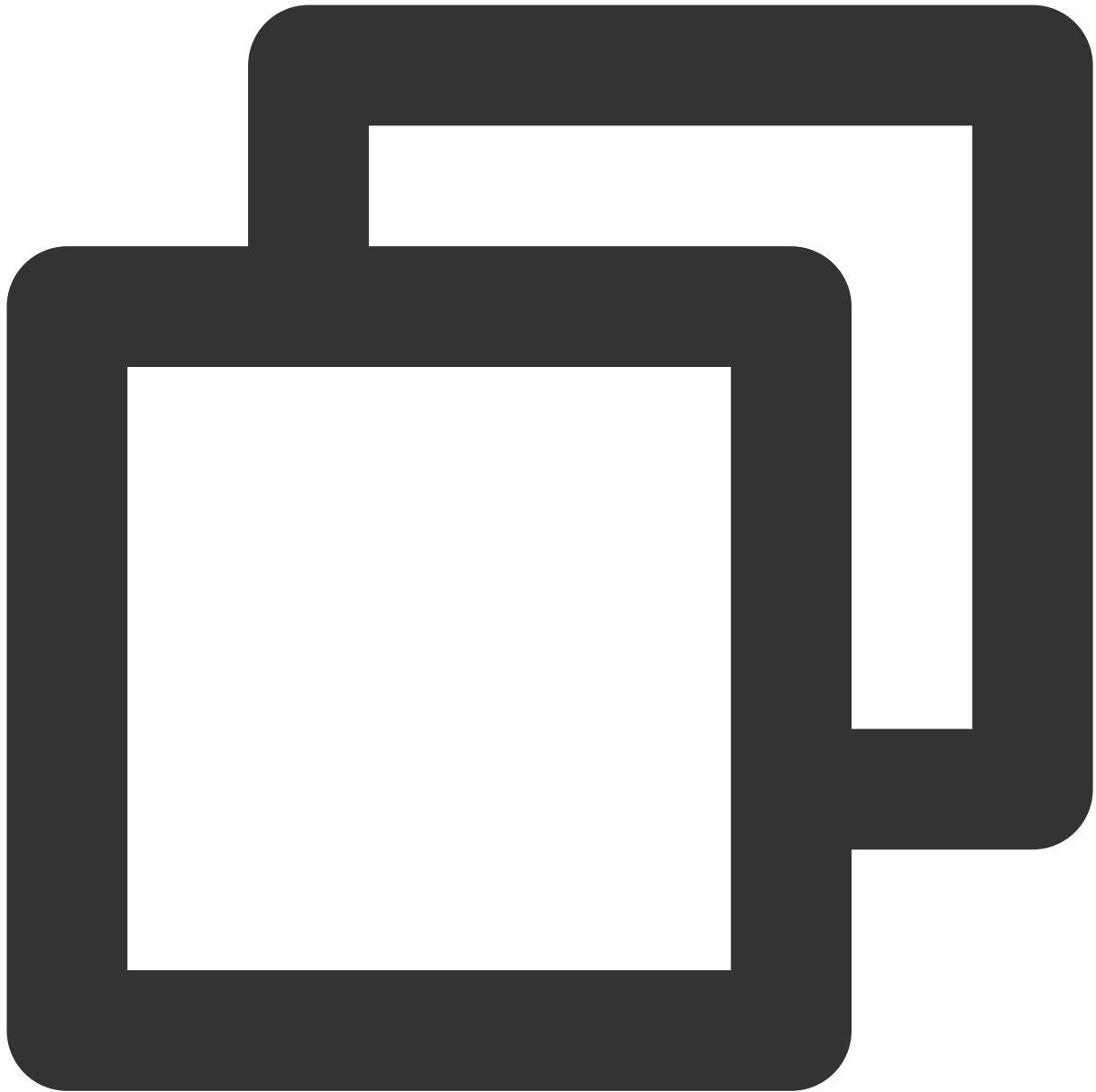
1. Edit the local `hosts` file to direct local requests to the protected site to your Anti-DDoS Advanced instance. The following uses Windows OS as an example to describe how to configure the local `hosts` file:

Open the `hosts` file in `C:\\Windows\\System32\\drivers\\etc` and add the following content at the end of the file:



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

2. For example, if the Anti-DDoS Advanced IP is `10.1.1.1` and the domain name is `www.qq.com`, add:



```
10.1.1.1 www.qq.com
```

Save the `hosts` file and ping the protected domain name on the local computer. If the resolved IP address is the Anti-DDoS Advanced IPs bound in the `hosts` file, the local `hosts` configuration has taken effect.

**Note:**

If the resolved IP is still the real server IP, try running `ipconfig/flushdns` in the Windows Command Prompt to refresh the local DNS cache.

3. After confirming the protective IP bound in the `hosts` file has taken effect, check whether the domain name can be accessed. If it can be accessed properly, the configuration has taken effect.

**Note:**

If the verification still fails with the correct method, log in to the Anti-DDoS Advanced console and check the configuration. If the problem persists, please [submit a ticket](#).

**Modifying DNS resolution**

To modify DNS resolution, see [Configuring Smart Scheduling](#).

**Note:**

The DNS resolution address should be changed to the CNAME address provided, which will be updated from time to time. (Non-BGP resources are not supported).

# Non-Website Business Connection

Last updated : 2024-07-01 11:20:28

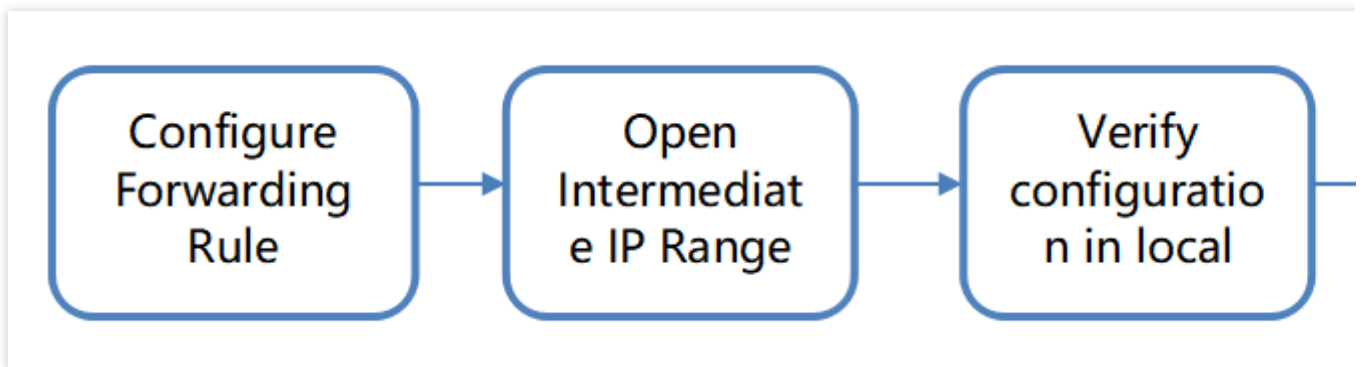
This document describes how to connect a non-website business to an Anti-DDoS Advanced instance and verify the forwarding configuration.

## Prerequisite

To add a forwarding rule, you need to purchase an [Anti-DDoS Advanced \(Chinese Mainland\)](#) or [Anti-DDoS Advanced \(Global\)](#) instance.

To modify the DNS information of your business domain name, you need to purchase a DNS service, such as Tencent Cloud **DNSPod**.

## Process




## Directions

### Configuring forwarding rules

1. Log in to the new [Anti-DDoS console](#), and click **Business Access > Access via domain name** on the left sidebar.
2. On the **Access via domain name** tab, click **Start access**.

**Application Accessing**

IP access   Access via ports   **Access via domain names**   IP access ⓘ



### Access via Domain Name

If your business is a website business, you can add forwarding rules through the Anti-DDoS Pro domain name business access method to effectively defend against DDoS and CC attacks for the website business. According to the rules you configure, the business traffic will first be cleaned by Anti-DDoS Pro, and then back to the target origin server, you can delete or edit existing rules. [View details](#)

Accessed business	Accessible applica
188	5370

Last access: 2023-08-21 20:14:41

**Start Access**   Batch import   Batch export   Batch delete

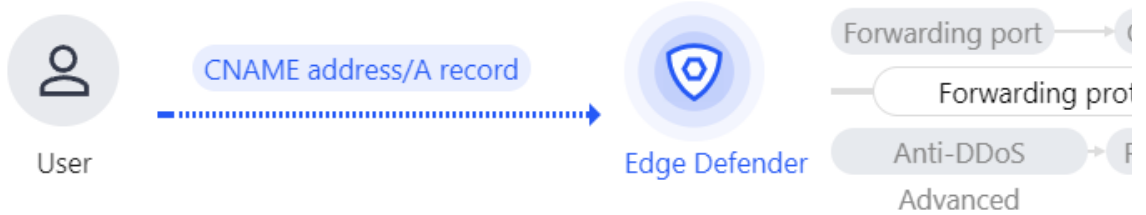
3. On the **Access via Domain Name** page, select an associated instance ID and click **Next: Set Protocol Port**.

**Note:**

You can select multiple instances.

### Access via Domain Name

- 1 Select Instance** >
- 2 Protocol port >
- 3 Set Forwarding Method
- 4 Modify DNS resolution



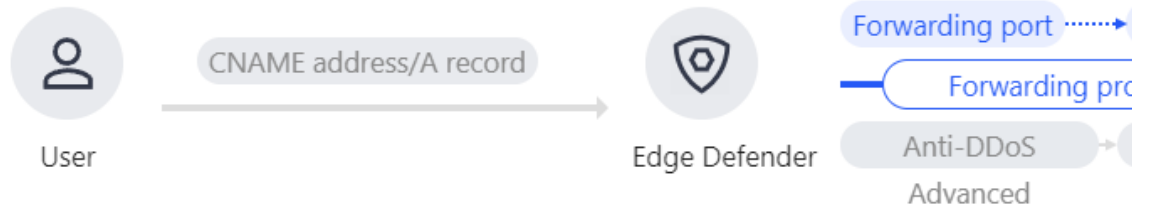
\* Associated Instance   Search IP, name or Anti-DDoS resource ▼

4. Select a forwarding protocol and certificate, specify a domain name, and then click **Next: Set Forwarding Method**.



## Access via Domain Name

- ✓ Select Instance >
- 2 Protocol port >
- 3 Set Forwarding
- 4 Modify DNS resolution



\* Forwarding protocol

http

https

\* Application domain name

The domain name cannot exceed

Recommended to enable protection configuration

CC Protection + CC AI Protection ⓘ

5. Select a forwarding method, specify a real server IP and port or a real server domain name, and then click **Next: Modify DNS Resolution**.

### Access via Domain Name

✓ Select Instance > ✓ Protocol port > 3 Set Forwarding  
4 Modify DNS resolution

\* Set Forwarding Method:  Forwarding via IP  Forwarding via domain name  
 Clean traffic can be forwarded back to the real server by the IP or domain name.

\* Real Server IP & Port

Real server IP	Origin port	
<input type="text" value="Enter the real server (eg: 1.1.1.1)"/>	<input type="text" value="Eg: 80"/>	<input type="button" value="Delete"/>
<input type="button" value="+ Add"/>		

Please enter the combination of real server IP and port. Up to 16 entries are supported.

**Note:**

An alternate real server is used when the forwarding to the real server fails.

Only the standard protocol ports 80 (HTTP) and 443 (HTTPS) are supported.

Wildcard domain names are supported.

6. Click **Complete**.

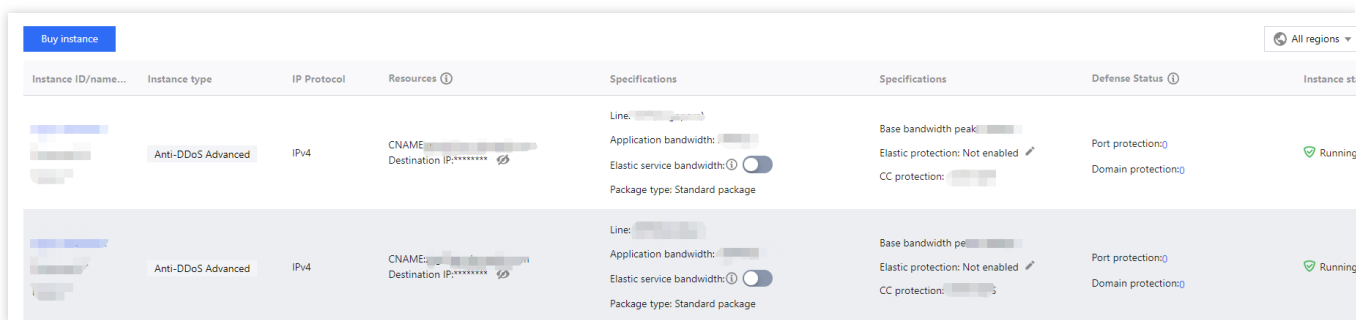
**Note:**

After you have connected to the service, you can customize your protection settings on the **Configurations** page. For more information, see [Protection Configuration](#).

**Allowing forwarding IP ranges**

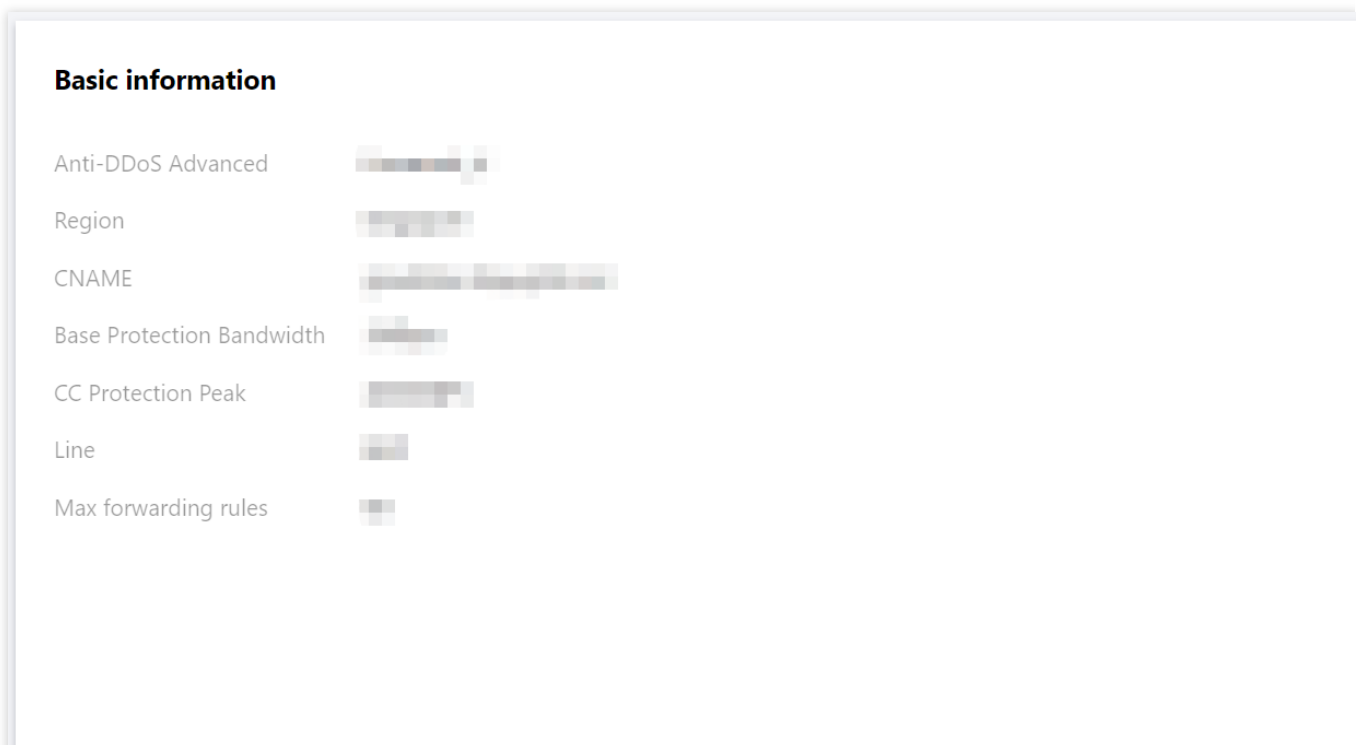
To prevent service unavailability from occurring when the real server blocks Anti-DDoS Advanced's forwarding IP, we recommend you configure allowlist policies for the real server infrastructure, including firewall, Web Application Firewall, intrusion prevention system (IPS), and traffic management, and disable the protection feature or set allowlist policies on the host firewall and other security software (such as safedog) of the real server, so that the forwarding IP will not be affected by the security policies of the real server.

1. Log in to the new [Anti-DDoS console](#) and click **Anti-DDoS instances** on the left sidebar.
2. On the **Anti-DDoS instances** page, select a target instance and click the **instance ID**.



Instance ID/name...	Instance type	IP Protocol	Resources	Specifications	Specifications	Defense Status	Instance st
[Redacted]	Anti-DDoS Advanced	IPv4	CNAME: [Redacted] Destination IP: [Redacted]	Line: [Redacted] Application bandwidth: [Redacted] Elastic service bandwidth: [Redacted] Package type: Standard package	Base bandwidth peak: [Redacted] Elastic protection: Not enabled CC protection: [Redacted]	Port protection: [Redacted] Domain protection: [Redacted]	Running
[Redacted]	Anti-DDoS Advanced	IPv4	CNAME: [Redacted] Destination IP: [Redacted]	Line: [Redacted] Application bandwidth: [Redacted] Elastic service bandwidth: [Redacted] Package type: Standard package	Base bandwidth peak: [Redacted] Elastic protection: Not enabled CC protection: [Redacted]	Port protection: [Redacted] Domain protection: [Redacted]	Running

3. On the **Basic information** page, you will see the forwarding IP ranges.



Basic information	
Anti-DDoS Advanced	[Redacted]
Region	[Redacted]
CNAME	[Redacted]
Base Protection Bandwidth	[Redacted]
CC Protection Peak	[Redacted]
Line	[Redacted]
Max forwarding rules	[Redacted]

## Verifying configuration locally

After the forwarding configuration is completed, the Anti-DDoS Advanced IP will forward packets from the relevant port to the corresponding real server port according to the forwarding rules. To ensure the stability of your business, a local test is recommended. The verification methods are as follows:

### For businesses accessed via IPs

For businesses accessed via IPs (such as games), run the `telnet` command to check whether the Anti-DDoS Advanced IP port is accessible. You can also enter the Anti-DDoS Advanced IP as the server IP in your local client (if available) to check whether the local client can access the Anti-DDoS Advanced IP.

For example, assume that the Anti-DDoS Advanced IP is `10.1.1.1` with the forwarding port `1234`, and the real server IP is `10.2.2.2` with the real server port `1234`. Run `telnet` on your local client to access `10.1.1.1:1234`. If the address can be accessed, the forwarding is successful.

### For businesses accessed via domain names

For businesses accessed via domain names, you can modify the local `hosts` file to verify whether the configuration has taken effect.

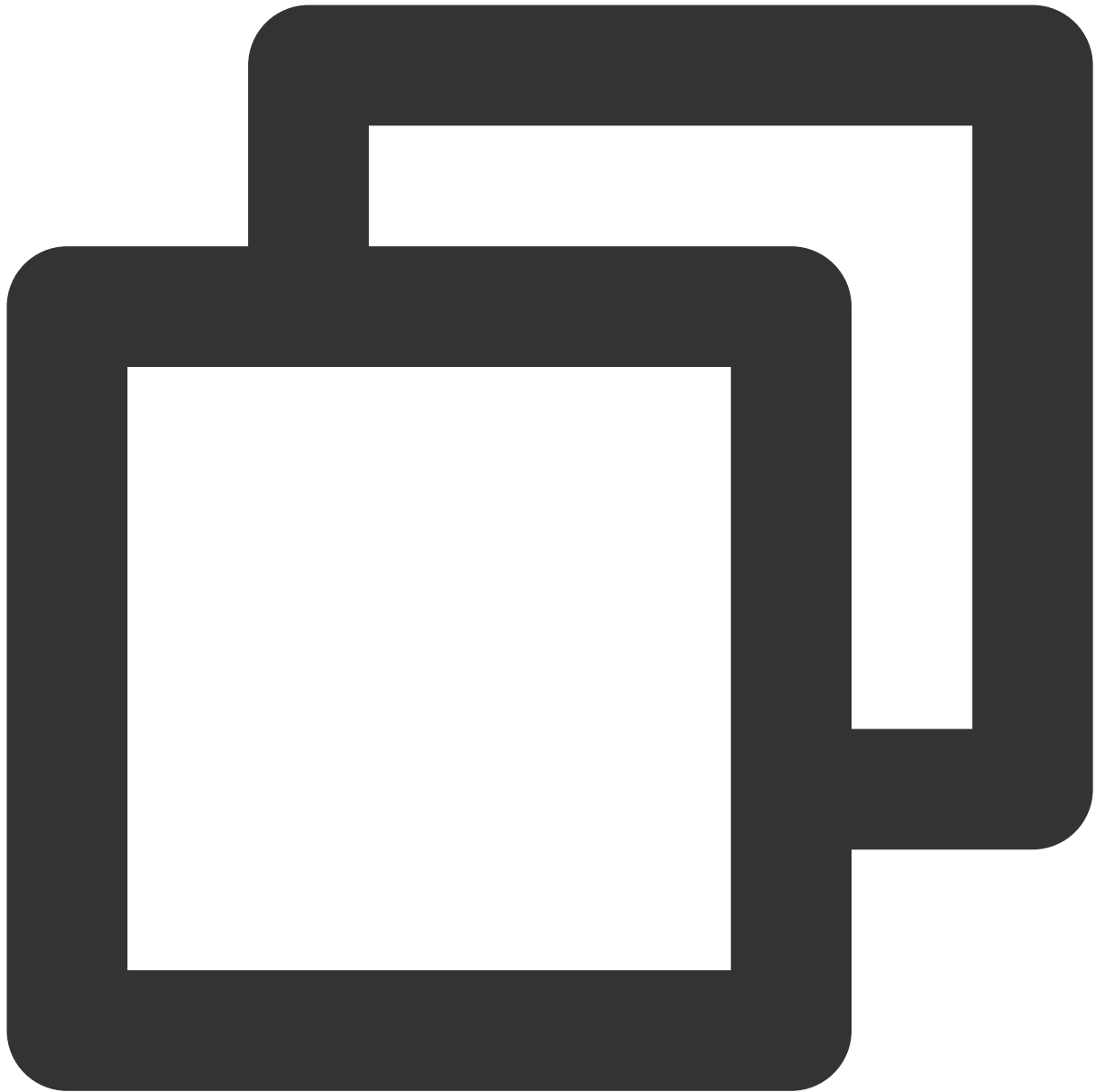
1. Edit the local `hosts` file to direct local requests to the protected site to your Anti-DDoS Advanced instance. The following uses Windows OS as an example to describe how to configure the local `hosts` file:

Open the `hosts` file in `C:\\Windows\\System32\\drivers\\etc` 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 Anti-DDoS Advanced IP is `10.1.1.1` and the domain name is `www.qq.com`, add:



```
10.1.1.1 www.qq.com
```

Save the `hosts` file and run the `ping` command on the local computer to ping the protected domain name. If the resolved IP address is the Anti-DDoS Advanced IP address bound in the `hosts` file, the local `hosts` configuration has taken effect.

**Note:**

If the resolved IP address is still the real server IP address, try running the `ipconfig/flushdns` command in the Windows command prompt to refresh the local DNS cache.

2. After confirming the Anti-DDoS Advanced IP bound in the `hosts` file has taken effect, check whether the domain name can be accessed. If it can be accessed properly, the configuration has taken effect.

**Note:**

If the verification still fails with the correct method, log in to the Anti-DDoS Advanced console and check whether the configuration is correct. If the problem persists after you fix all incorrect configuration items, please [submit a ticket](#) to us for assistance.

## Modifying DNS resolution

If you want to modify DNS resolution, see [Configuring Smart Scheduling](#) for instructions.

**Note:**

The DNS resolution address should be changed to the CNAME address provided, which will be updated from time to time. (Non-BGP resources are not supported).

# Anti-DDoS Advanced (Global Enterprise)

Last updated : 2024-07-01 11:20:28

Anti-DDoS Advanced (Global Enterprise) is a paid service for Tencent Cloud users with businesses deployed in regions outside the Chinese mainland.

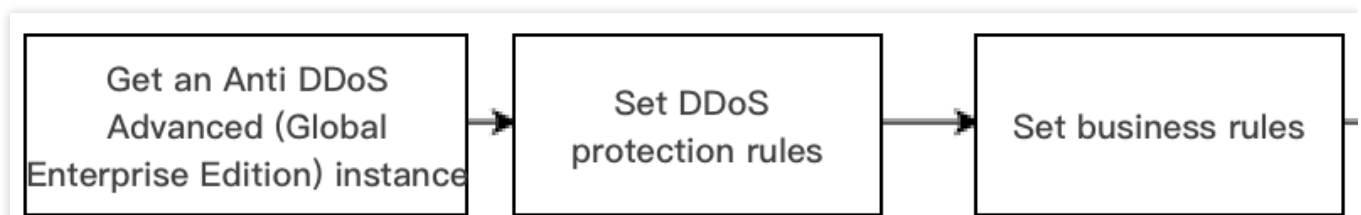
It allows you to purchase and hold public IP address resources separately.

After an Anti-DDoS Advanced (Global Enterprise) instance is bound to cloud resources, the cloud resources can communicate with the public network through it.

This document takes binding an instance to a cloud resource as an example to describe the lifecycle of an Anti-DDoS Advanced (Global Enterprise) instance.

## Background

The lifecycle of Anti-DDoS Advanced (Global Enterprise) includes purchasing an instance, configuring protection rules, configuring business rules for the instance, and terminating the instance.



1. [Purchasing an instance](#): Purchase an Anti-DDoS Advanced (Global Enterprise) instance according to your actual needs.
2. [Configuring protection rules](#): Configure protection policies that fit your business.
3. [Configuring business rules](#) : Associate the instance with the cloud resources to be protected.
4. [Terminating the instance](#): After disassociating the instance from cloud resources, you can associate it with other cloud resources. The disassociation operation may cause the network of the corresponding cloud resources to be disconnected, and instances that are not bound to cloud resources will incur idle resource fees.

## Directions

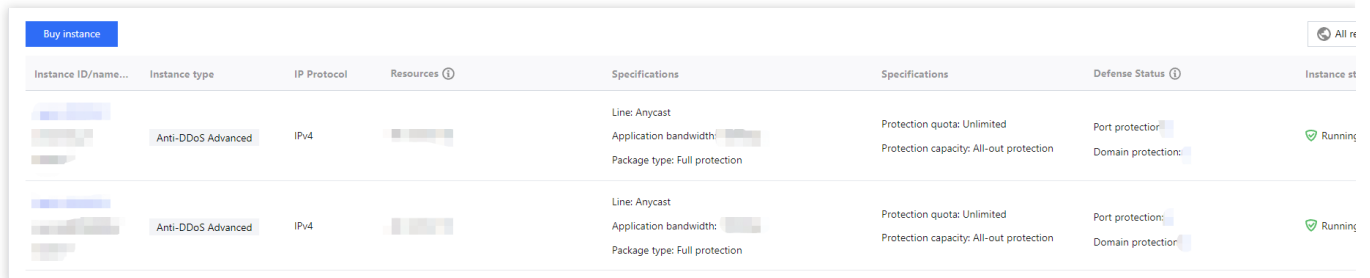
### Purchasing an instance

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise\)](#) console.
2. Purchase an instance as instructed in [Purchase Guide](#).
3. Click **Anti-DDoS instances** in the console to view the instance just purchased, which is in the **Not bound** status.



**Note:**

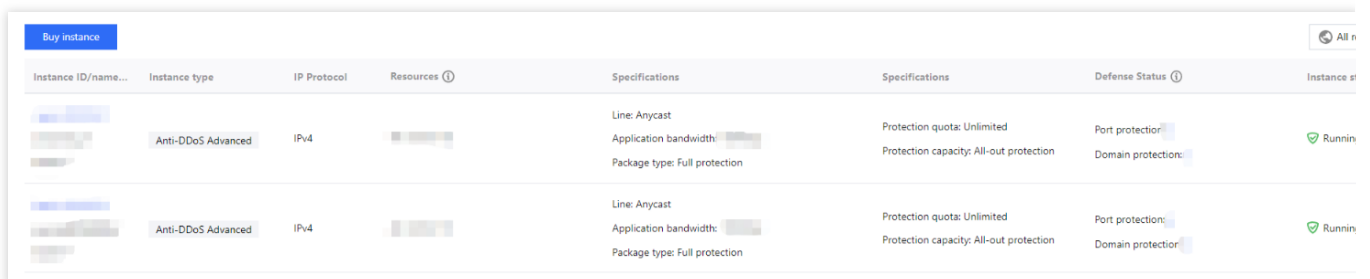
An Anti-DDoS Advanced (Global Enterprise) instance incurs an idle fee if it's not bound with cloud resource. The idle fee is calculated by second and billed per hour. Bind the instance with cloud resource in time to prevent unnecessary costs. For more information, see [Billing Overview](#).



Instance ID/name...	Instance type	IP Protocol	Resources	Specifications	Specifications	Defense Status	Instance st
[Redacted]	Anti-DDoS Advanced	IPv4	[Redacted]	Line: Anycast Application bandwidth: [Redacted] Package type: Full protection	Protection quota: Unlimited Protection capacity: All-out protection	Port protection: [Redacted] Domain protection: [Redacted]	Running
[Redacted]	Anti-DDoS Advanced	IPv4	[Redacted]	Line: Anycast Application bandwidth: [Redacted] Package type: Full protection	Protection quota: Unlimited Protection capacity: All-out protection	Port protection: [Redacted] Domain protection: [Redacted]	Running

**Configuring protection rules**

1. Log in to the new [Anti-DDoS console](#) and click **Anti-DDoS instances** on the left sidebar.
2. Select the target instance and click **Configurations**. For more information, see [Configuring Protection Rules](#).



Instance ID/name...	Instance type	IP Protocol	Resources	Specifications	Specifications	Defense Status	Instance st
[Redacted]	Anti-DDoS Advanced	IPv4	[Redacted]	Line: Anycast Application bandwidth: [Redacted] Package type: Full protection	Protection quota: Unlimited Protection capacity: All-out protection	Port protection: [Redacted] Domain protection: [Redacted]	Running
[Redacted]	Anti-DDoS Advanced	IPv4	[Redacted]	Line: Anycast Application bandwidth: [Redacted] Package type: Full protection	Protection quota: Unlimited Protection capacity: All-out protection	Port protection: [Redacted] Domain protection: [Redacted]	Running

**Associating with cloud resources**

1. Log in to the new [Anti-DDoS console](#) and click **Business Access > IP access**.
2. On the **IP access** page, click **Start Access**.
3. On the **IP access** page, select an Anti-DDoS Advanced (Global Enterprise) instance in the **Associate Anycast IP** field, select a cloud resource, and then click **OK**.

**Note:**

Cloud resources that are associated with a public IP or Anycast IP cannot be associated again.

### IP access

Associate Anycast IP

Instance type  Cloud Virtual Machine  Load balancer

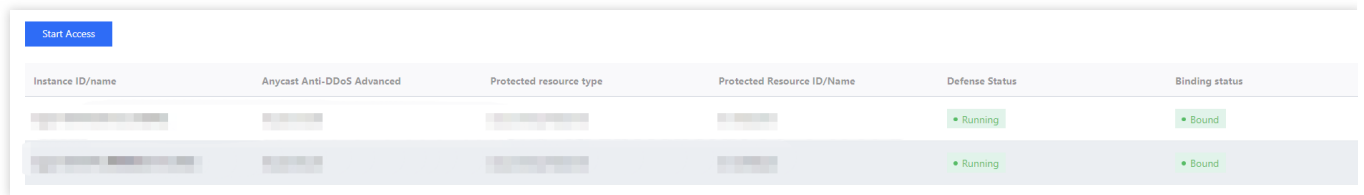
Enter the instance ID/IP

Instance ID/name	Availability zone	Private IP
No data yet		

Total items: 0 10 / page

### Disassociating with cloud resources

1. On the **IP access** page, select an instance and click **Delete** on the right.



The screenshot shows a table with the following columns: Instance ID/name, Anycast Anti-DDoS Advanced, Protected resource type, Protected Resource ID/Name, Defense Status, and Binding status. There are two rows of data, both showing a 'Running' defense status and a 'Bound' binding status.

Instance ID/name	Anycast Anti-DDoS Advanced	Protected resource type	Protected Resource ID/Name	Defense Status	Binding status
[Redacted]	[Redacted]	[Redacted]	[Redacted]	Running	Bound
[Redacted]	[Redacted]	[Redacted]	[Redacted]	Running	Bound

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

**Note:**

Note that the disassociation may disconnect your cloud resource from the network. After disassociation, you can associate the instance with other resources later.