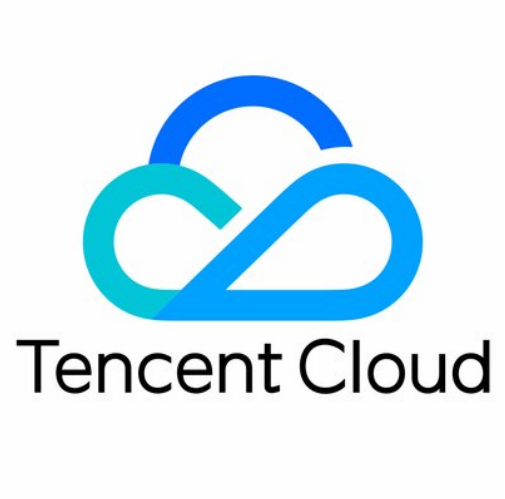
Anti-DDoS

Practical Tutorial

Product Documentation



Contents

Practical Tutorial
Remote Protection Scheme with Anti-DDoS Pro

Last updated：2024-07-01 11:38:27

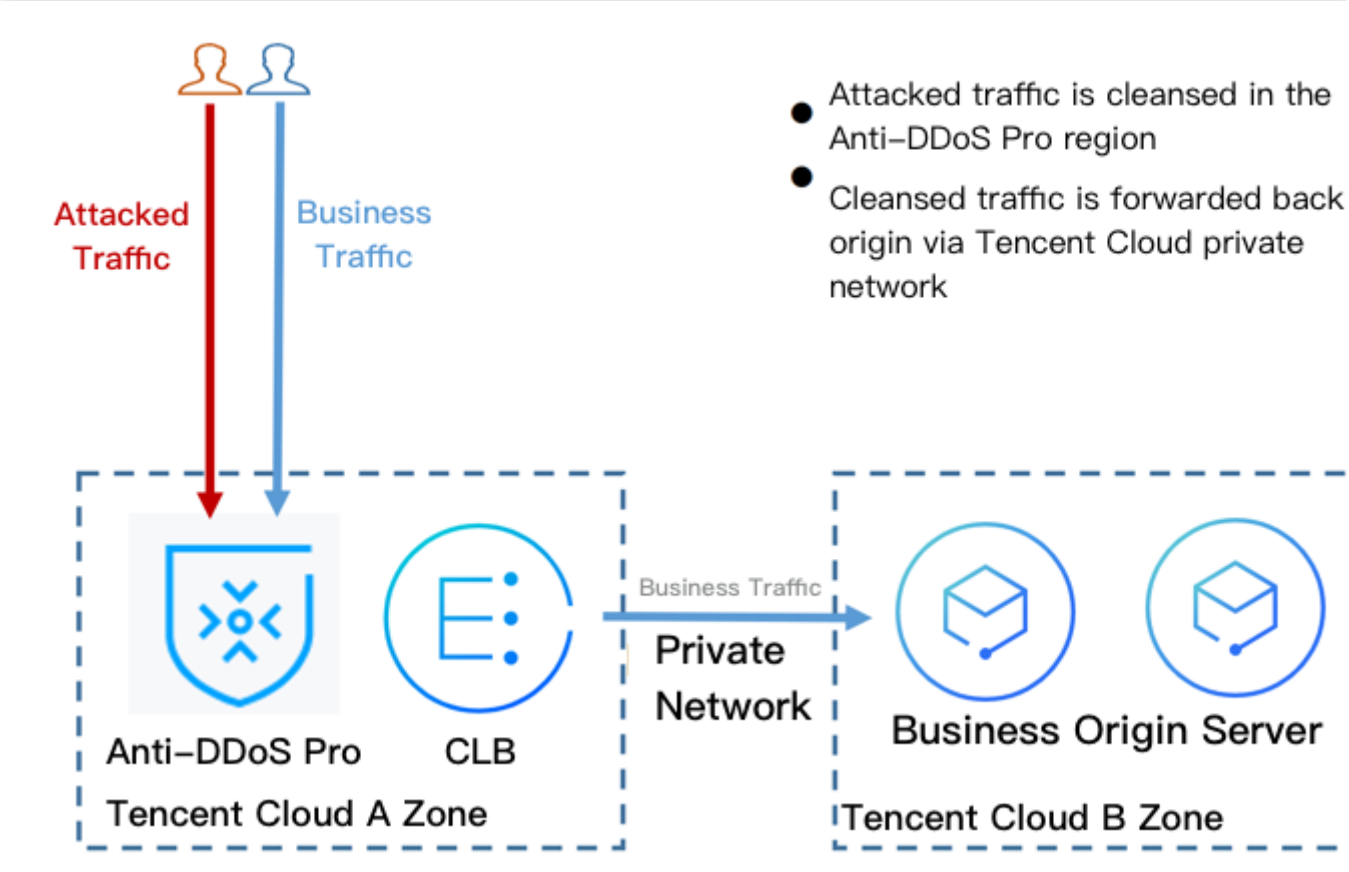
Background

Anti-DDoS Pro is available for Tencent Cloud users in Beijing, Shanghai, and Guangzhou regions only and guarantees all-out protection. Integrating the local cleansing center capability, all-out protection aims to spare no effort to successfully defend against each DDoS attack. In addition, all-out protection will be adjusted according to the actual network status. Anti-DDoS Pro is not available in Chengdu, Chongqing, and other regions in the Chinese mainland. If your business's real server is deployed in Tencent Cloud and you need to use the protection capability of Anti-DDoS Pro in regions other than where your real server is located, you may consider the following solution.

Solution

This solution involves Anti-DDoS Pro, Cloud Load Balancer (CLB), and your real server. Firstly, you will need to deploy a CLB instance in a region where you have Anti-DDoS Pro resources and bind the CLB to the Anti-DDoS Pro instance. Next, configure the private network forwarding rules for the CLB to ensure that your business can be accessed through the public IP of the CLB.
Normally, business traffic will be routed to the public IP of the real server or directly to the public IP of the CLB in another region. The business traffic will access the nearest real server.
If attacks occur, business traffic will be routed to the IP of the CLB to cleanse the attack traffic. After the traffic is cleansed, the CLB will forward the traffic back to the real server via Direct Connect lines in the Tencent Cloud private network.

The following figure describes the details of the solution:



Benefits

The DDoS protection capability will no longer be limited by regions and can be up to 300 Gbps.
The business traffic will be forwarded via Direct Connect lines in the Tencent Cloud private network with high reliability and low latency.
You will enjoy all the advantages brought by Tencent Cloud Anti-DDoS network. All your public IPs will be BGP IPs and the latency will be very low.

Tips

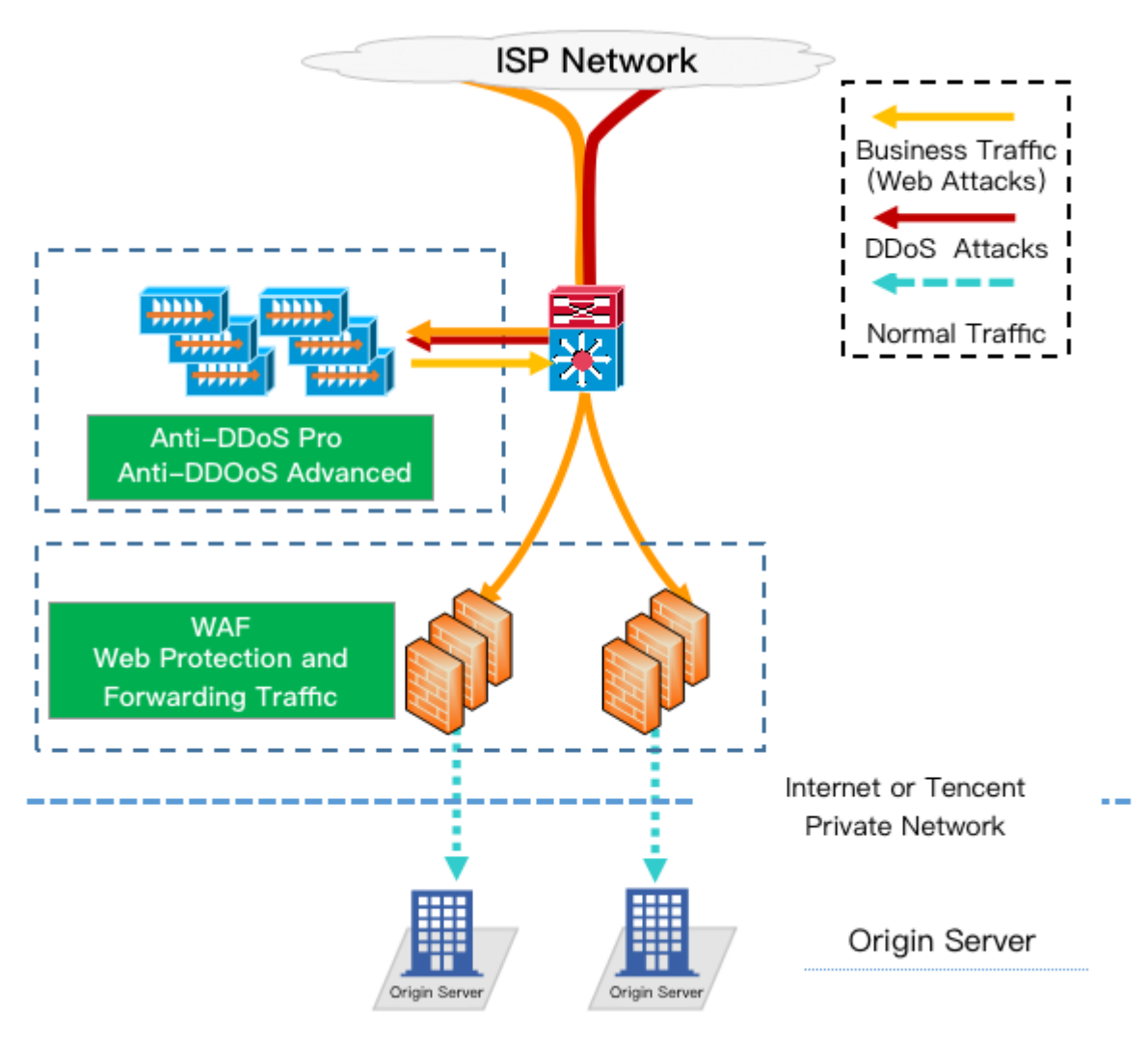
Deploy Anti-DDoS Pro and CLB in advance.
Establish a business availability monitoring system so that you can promptly notice and respond to any problem with access to the real server when the automatic switching mechanism is not deployed.
Test regularly, familiarize yourself with the solution details, and solve potential problems.

Using Anti-DDoS Pro Together with WFA

Last updated：2024-07-01 11:38:27

Anti-DDoS Pro can be used together with Web Application Firewall (WAF) to provide you with comprehensive protection.
Providing DDoS protection capability of hundreds of Gbps at one click, Anti-DDoS Pro can easily defend against DDoS attacks and ensure the smooth operation of your business.
WAF can block web attacks in real time to ensure the security of your business data and information.

Deployment scheme



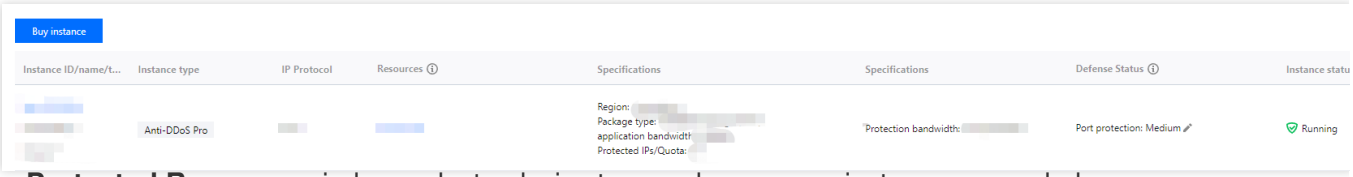
Directions

Configuring WAF

For more information on quick connection to WAF, see Getting Started with WAF.

Configuring Anti-DDoS Pro

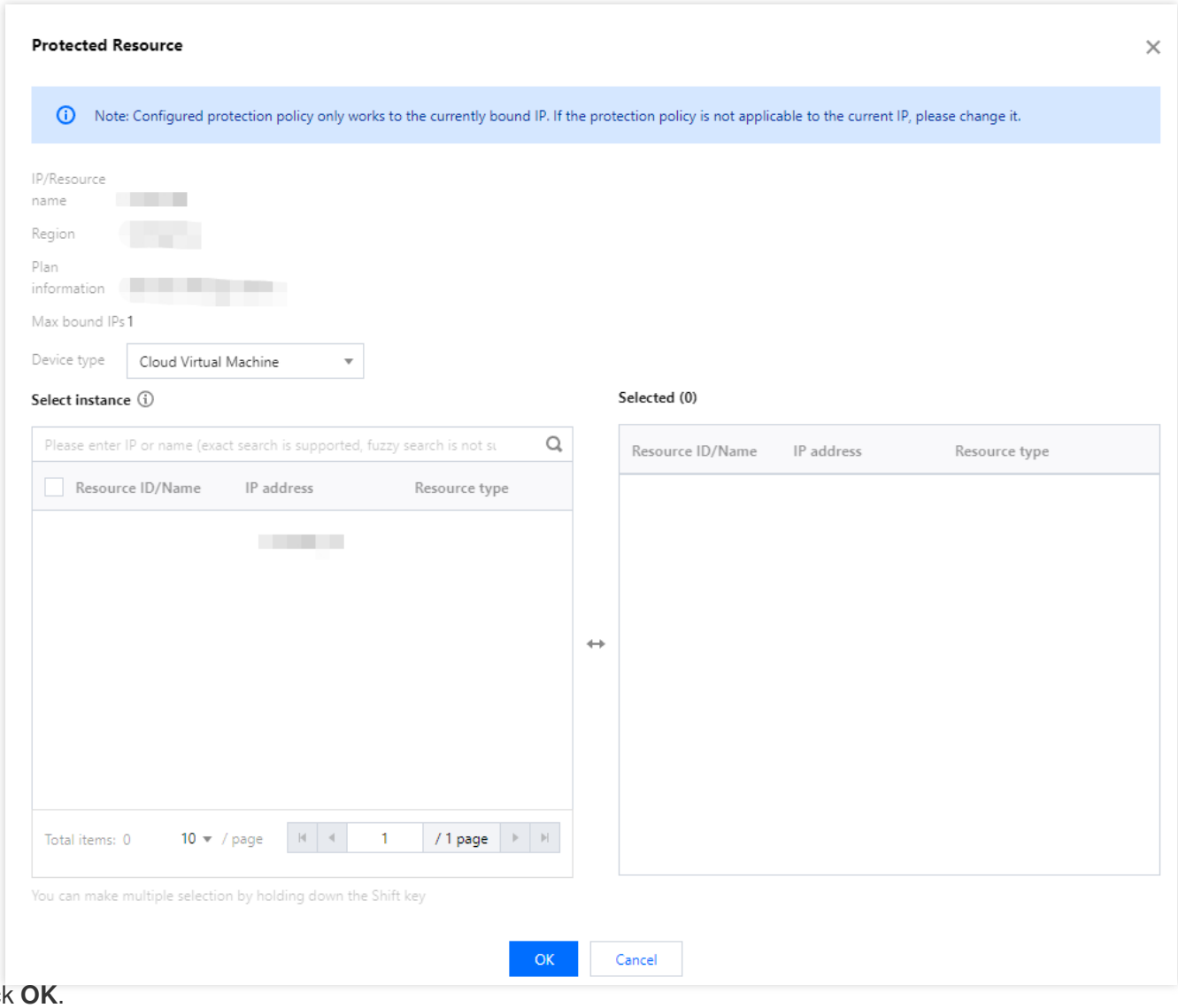
1. Log in to the new Anti-DDoS console, and click **Anti-DDoS Instances** on the left sidebar.
2. On the **Anti-DDoS Instances** page, select a target instance and click **Protected Resource** in the **Operation** column.



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

Device type: Public cloud resources (such as CVM, CLB, and WAF) with public IPs are supported.

Select instance: You can select multiple instances (no more than the maximum number of bound IPs).



4. Click **OK**.

Suggestions on Stress Tests

Last updated：2024-07-01 11:38:27

A stress test is designed to simulate DDoS attacks. To ensure the quality of the test, you are advised to read this document carefully before conducting a stress test.

Note:

The following suggestions are mainly about the influence of DDoS protection on stress testing. You may also need to consider other test-related factors, such as network bandwidth, linkage loads, or other basic resources.

Adjusting protection policies

Disable CC protection policies, or set the HTTP request threshold for CC protection to a value higher than the maximum value of your stress test.

Disable DDoS protection policies, or set the cleansing threshold for DDoS protection to a value higher than the maximum value of your stress test.

Limiting the traffic and the number of requests in the stress test

The bandwidth of your stress test should be lower than 1 Gbps; otherwise, attack protection may be triggered.

The number of HTTP requests in your stress test should be no more than 20,000 requests per second (QPS); otherwise, attack defense may be triggered.

The number of new connections established per second, the maximum number of connections, and the number of inbound packets per second in your stress test should be less than 50,000, 2,000,000, and 200,000, respectively.

Note:

If the traffic and number of requests in your stress test will exceed the above ranges, please contact Tencent Cloud Technical Support. We will offer support during your stress test.

Evaluating the influence of the stress test in advance

You are recommended to contact Tencent Cloud solution architects or Tencent Cloud Technical Support before your stress test to evaluate possible consequences and develop risk avoidance measures.

Solutions to Real Server IP Exposure

Last updated：2024-07-01 11:38:27

Some attackers may record real server IP history, and the exposed IPs allow them to bypass Anti-DDoS Pro and directly attack your real server. In this case, we recommend that you change the real server IP.
Before changing the real server IP, you can refer to this document to check the risk factors to prevent the new IP from disclosure.

Checklist

Checking DNS records

Check all DNS records of the attacked real server IP, including the DNS records of subdomain names, MX (Mail Exchanger) records, and NS (Name Server) records. Make sure all these records are configured to point to the Anti-DDoS Advanced IP, so that the DNS is not resolving to the new real server IP directly.

Checking for information disclosure and command execution vulnerabilities

Check websites or business systems for possible information disclosure vulnerabilities, such as phpinfo() disclosure and sensitive information leakage on Github.
Check websites or business systems for command execution vulnerabilities.

Checking for trojans and backdoors

Check the real server for potential trojans, backdoors, and other hidden dangers.

Other suggestions

To prevent attackers from scanning the C range or other similar IP ranges, do not use the same IP or an IP similar to the old IP as the new real server IP.
We recommend you prepare the backup linkage and the backup IP in advance.
We recommend you set the scope of access sources to prevent malicious scanning.

Creating an Anti-DDoS EIP

Last updated：2024-07-01 11:38:27

Note:

Only a standard account supports creating **Anti-DDoS EIPs**. If you are not certain about your account type, please contact us.

Step 1. Purchase an Anti-DDoS Pro (Enterprise) instance

Go to the Anti-DDoS Pro buy page and purchase an instance. For more information, see Purchase Guide.

Step 2. Create a BGP bandwidth package

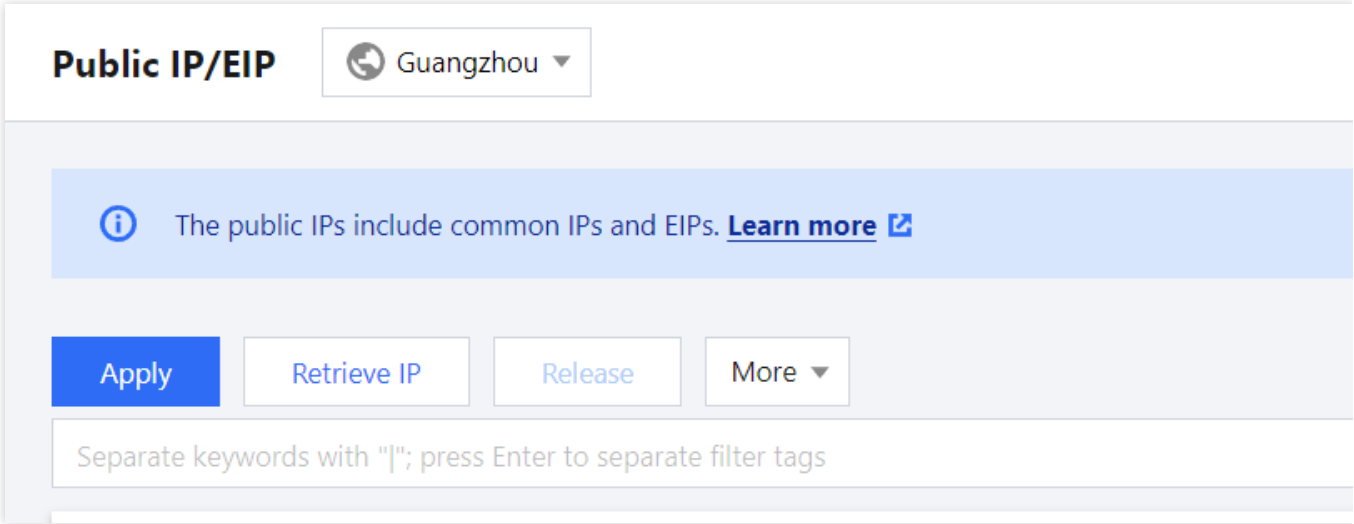
See Creating an IP Bandwidth Package to create a BGP bandwidth package.

Note:

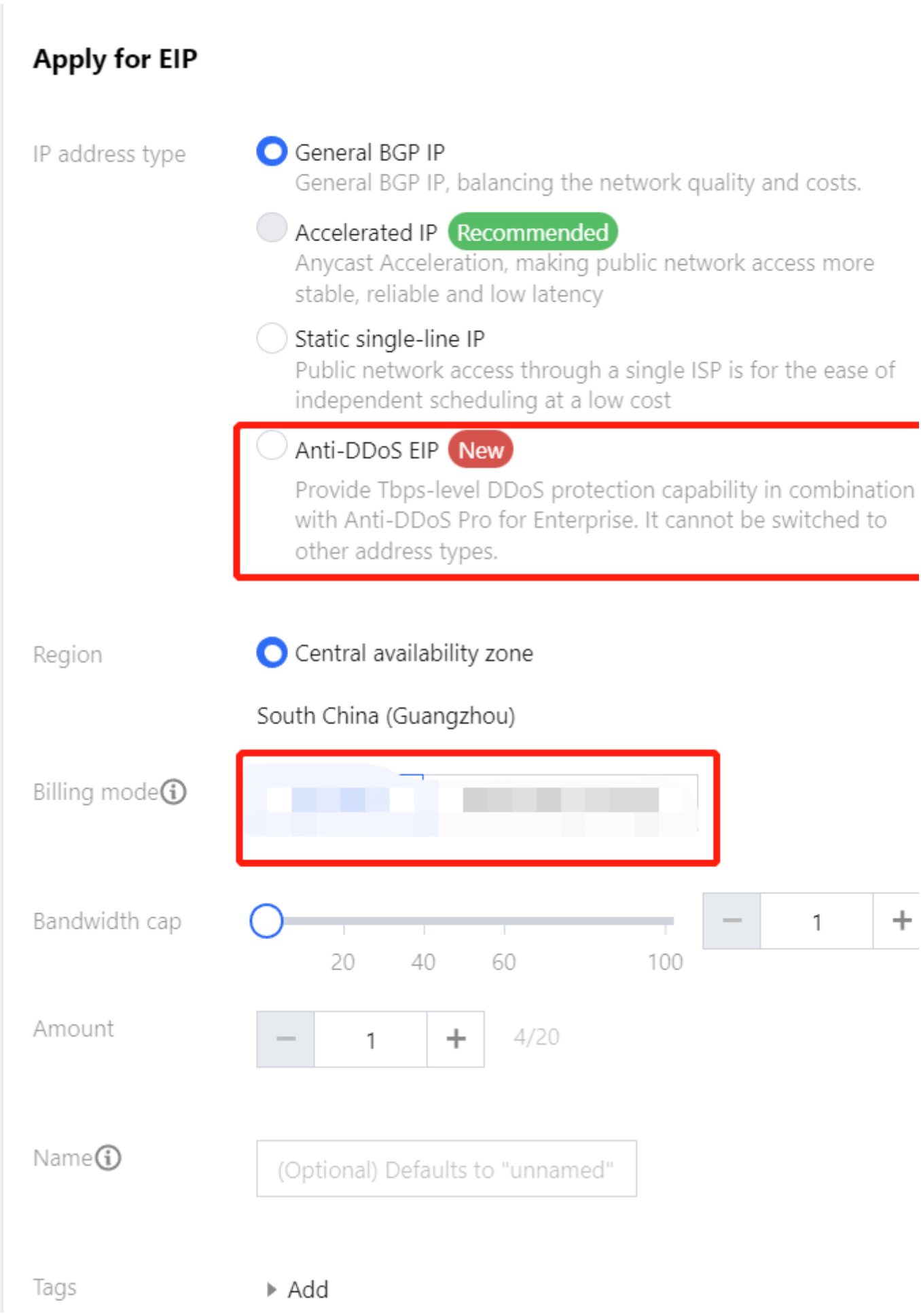
If you already have created a general BGP bandwidth package in the target region, please skip to Step 3.

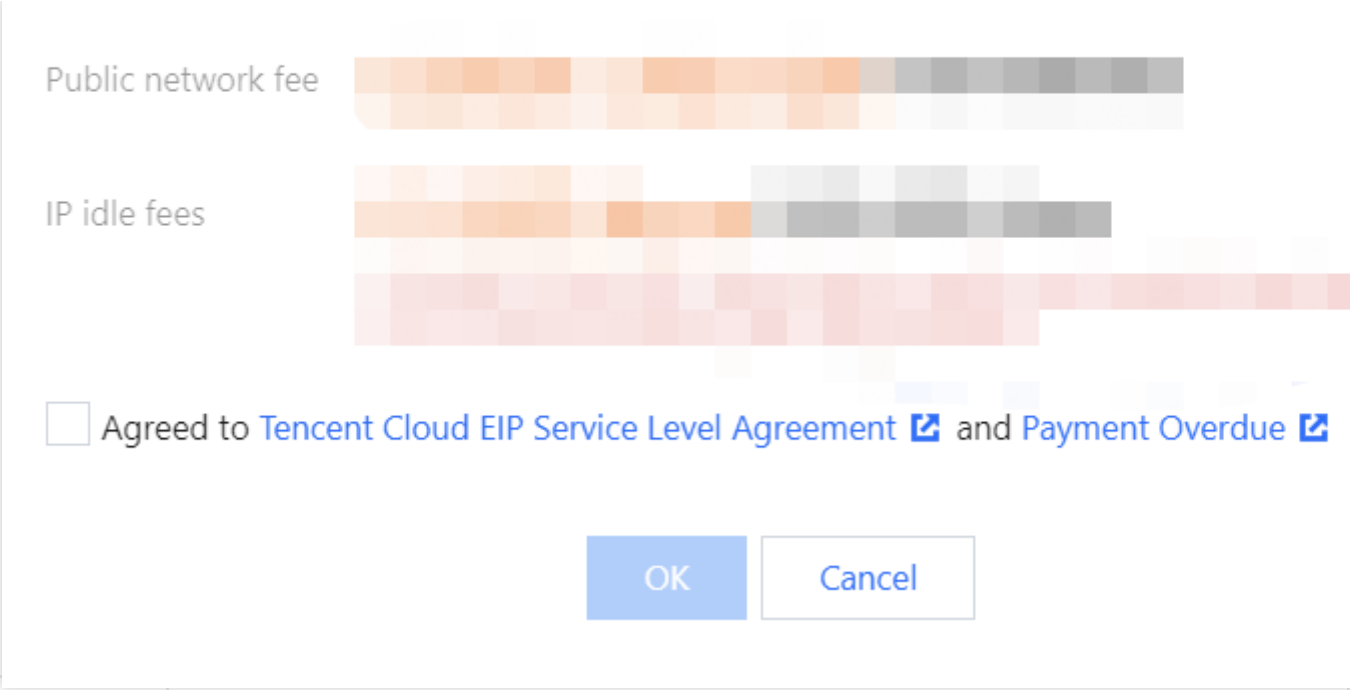
Step 3. Create an Anti-DDoS EIP

1. Log in to the CVM console and click **Public IP** on the left sidebar.
2. On the **Public IP/EIP** page, select a region and click **Apply**.



3. In the **Apply for EIP** pop-up window, configure relevant parameters and click **OK**.





Parameter	Description
IP address type	Select **Anti-DDoS EIP**.
Billing mode	Only bandwidth package is supported.
Bandwidth package	Select the wanted general BGP bandwidth package.
Bandwidth cap	Set the bandwidth cap as needed and allocate bandwidth resources reasonably.
Anti-DDoS Pro for Enterprise	Select the Anti-DDoS Pro instance you want to bind.
Amount	Select the quantity of EIPs to be applied and ensure that it does not exceed the total quota.
Name	(Optional) Enter an EIP instance name.
Tags	You can add a tag and use it for permission management.

Related operations

To bind cloud resources to the EIP, please contact us.

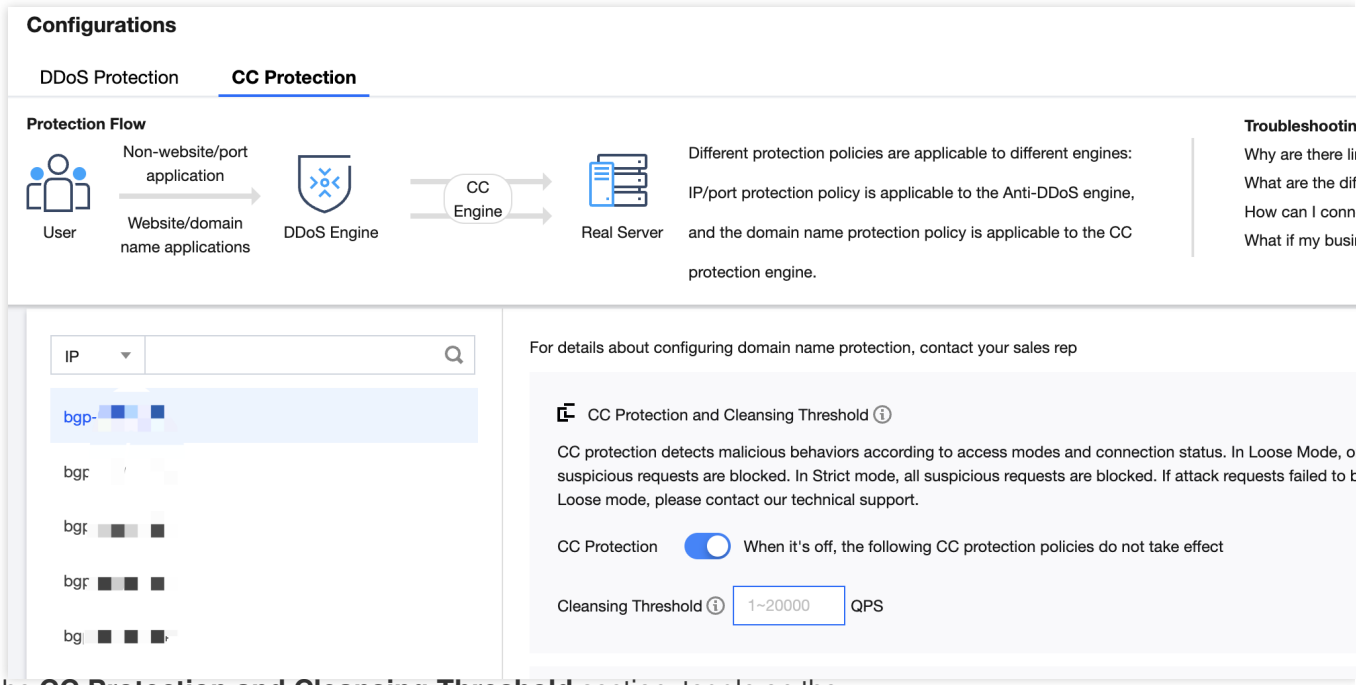
Configuration Directions and Notes on CC Protection Policies

Last updated：2024-07-01 11:38:27

Anti-DDoS Advanced provides CC attack protection. The protection policy features protection level, cleansing threshold, precise protection, CC frequency limit, and so on. After connecting your business, you can configure CC attack protection policy as instructed in this document to use Anti-DDoS Advanced to safeguard your business.

Directions

1. Log in to the new Anti-DDoS console, and click **CC Protection** on the left sidebar.
2. Select a domain name from the left list, such as `212.64.xx.xx bgpip-000002je` > `http:80` > `www.xxx.com&quot;` .

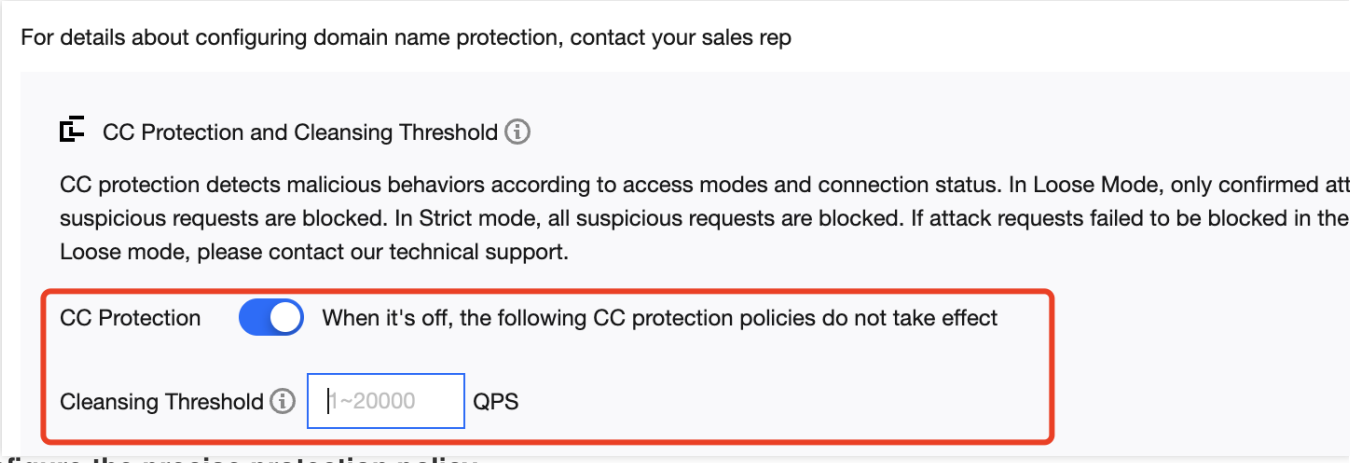


3. In the **CC Protection and Cleansing Threshold** section, toggle on the  switch and set a cleansing threshold.

Note:

The CC protection will be enabled once you set a cleansing threshold. A value that is 1.5 times your common business peak is recommended.

The cleansing feature will remain disabled if no threshold value is set, and the protection level, precise protection, and CC frequency limit you configured in the console will not be in effect even when your business is under CC attacks. For more information, see CC Protection and Cleansing Threshold.



4. **Configure the precise protection policy.**

When your business is under attack, we recommend deriving the attack characteristics from the specific attack request information obtained through packet capture, middleware access logs, and other protection devices to configure your precise protection policy based on your business.

You can enable precise protection to configure protection policies combining multiple conditions of common HTTP fields, such as **uri**, **ua**, **cookie**, **referer**, and **accept** to screen access requests. For the requests that match the conditions, you can configure CAPTCHA to verify requesters or a policy to automatically discard the packets.

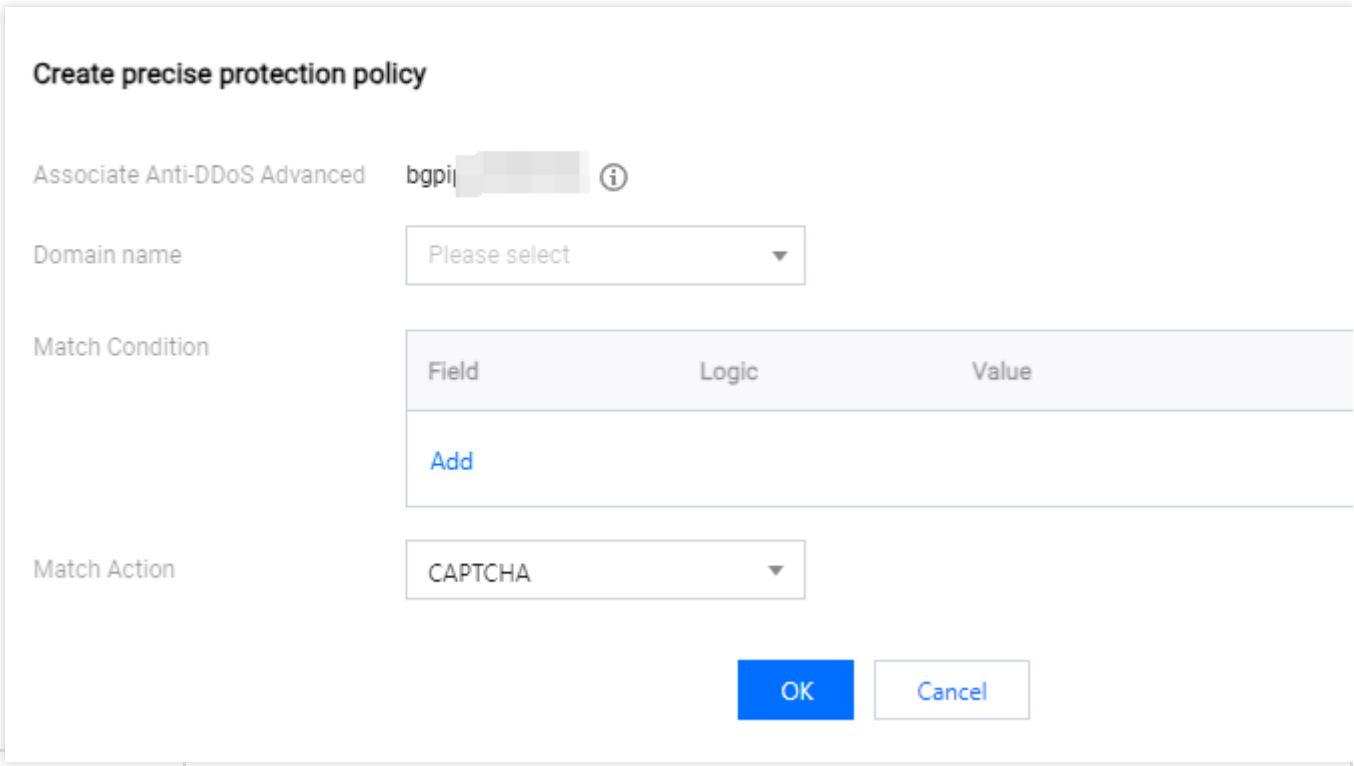
4.1 Click **Set** in the **Precise Protection** section to enter the precise protection rule list.

4.2 Click **Create**. In the pop-up window, enter the required fields, and click **OK**. For more information, see Precise Protection.

Note:

If a policy involves multiple HTTP fields, the policy can be matched if all conditions are met.

Anti-DDoS Advanced supports configuring precise protection for HTTPS businesses.



Field	Description
uri	The URI of an access request.
ua	The identifier and other information of the client browser that initiates an access request.
cookie	The cookie information in an access request.
referer	The source website of an access request, from which the access request is redirected.
accept	The data type to be received by the client that initiates the access request.
Match Action	Discard: Discards packets without verifying the requester. CAPTCHA: Verifies the requester through algorithms.

5. **Set the CC frequency limit.**

Anti-DDoS Advanced supports configuring CC frequency policy for connected web businesses to restrict the access frequency of source IPs. You can customize a frequency policy to apply CAPTCHA and discard on source IPs if any IP accesses a certain page too frequently in a short time.

5.1 Click **Set** in the **CC Frequency Limit** section enter the frequency limit rule list.

5.2 Click **Add Rule**. In the pop-up window, enter the required fields, and click **OK**. For detailed configurations, see CC Frequency Limit.

Note:

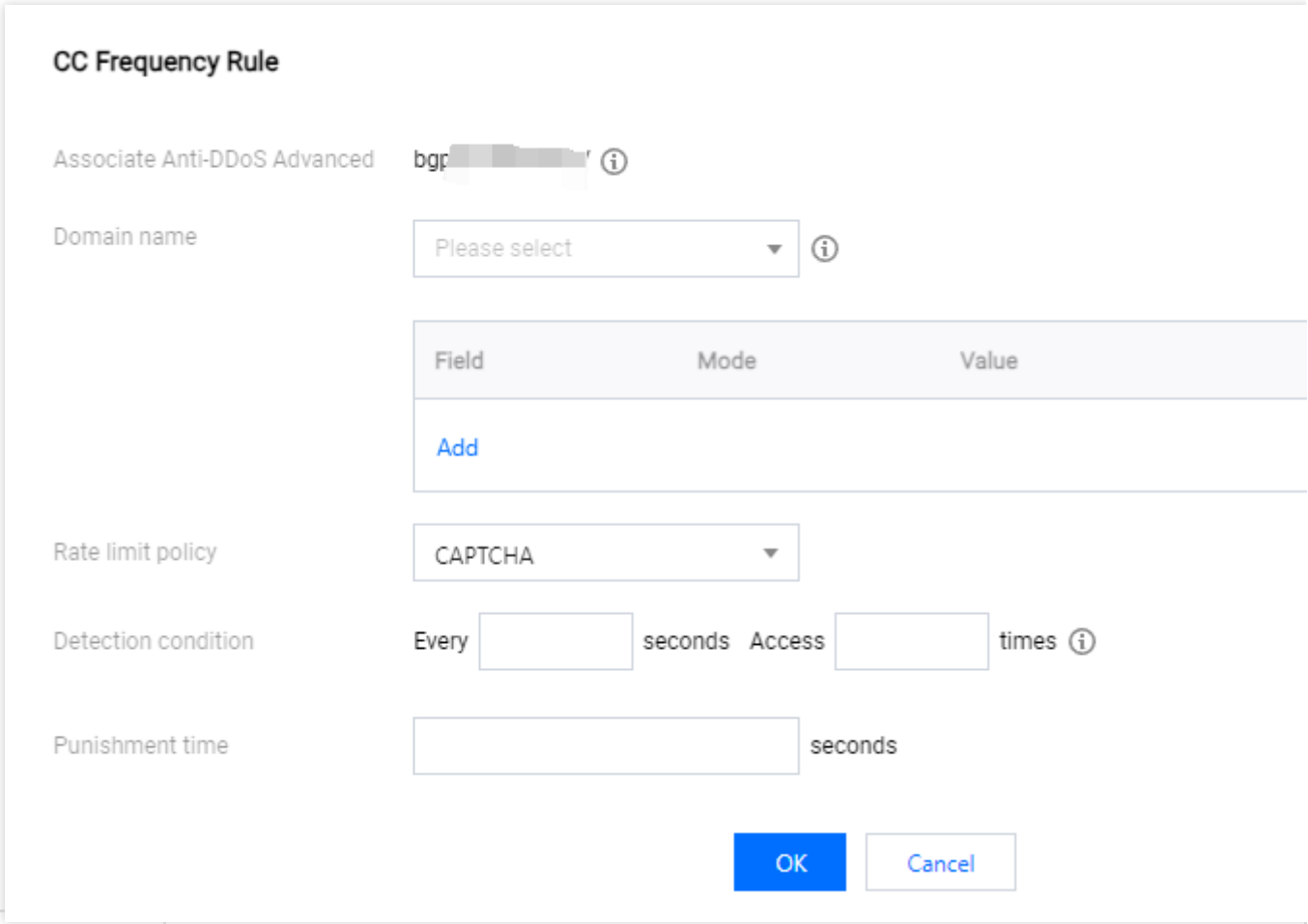
When configuring a CC frequency limit policy regarding the URI, you need to configure a frequency limit on the directory `/` first and the match mode must be **Equal to**. Then you can configure the URI access frequency limit on

other directories.

If a source IP accesses the `/` directory of the domain name for more than the set number of times in the set period, the set action (**CAPTCHA** or **Discard**) will be triggered.

If a frequency limit policy is configured for the `/` directory of a domain name, the detection time of the domain name's other directories must be the same.

If the request URI contains any unfixed string, you can set the match mode to **Include**, so that URIs with the set prefix will be matched.



Field	Description
Cookie	The cookie information in an access request.
User-Agent	The identifier and other information of the client browser that initiates an access request.
Uri	The URI of an access request.
Rate limit policy	Discard: Discards packets without verifying the requester. CAPTCHA: Verifies the requester through algorithms.
Detection condition	Set the access frequency based on your business, for which a value 2 to 3 times the common number of access requests is recommended. For example, if your website is accessed

	averagely 20 times per minute, you can configure the value to 40 to 60 times per minute or adjust it according to the attack severity.
Punishment time	The longest period is a whole day.

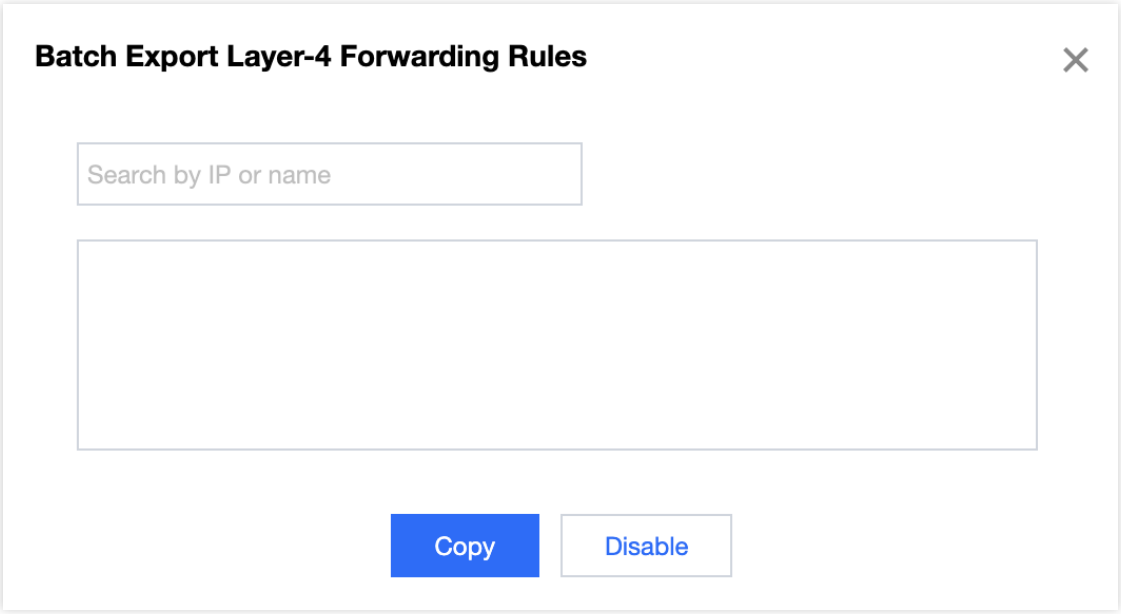
Syncing Forwarding Rules to New Anti-DDoS Advanced Instances

Last updated：2024-07-01 11:38:27

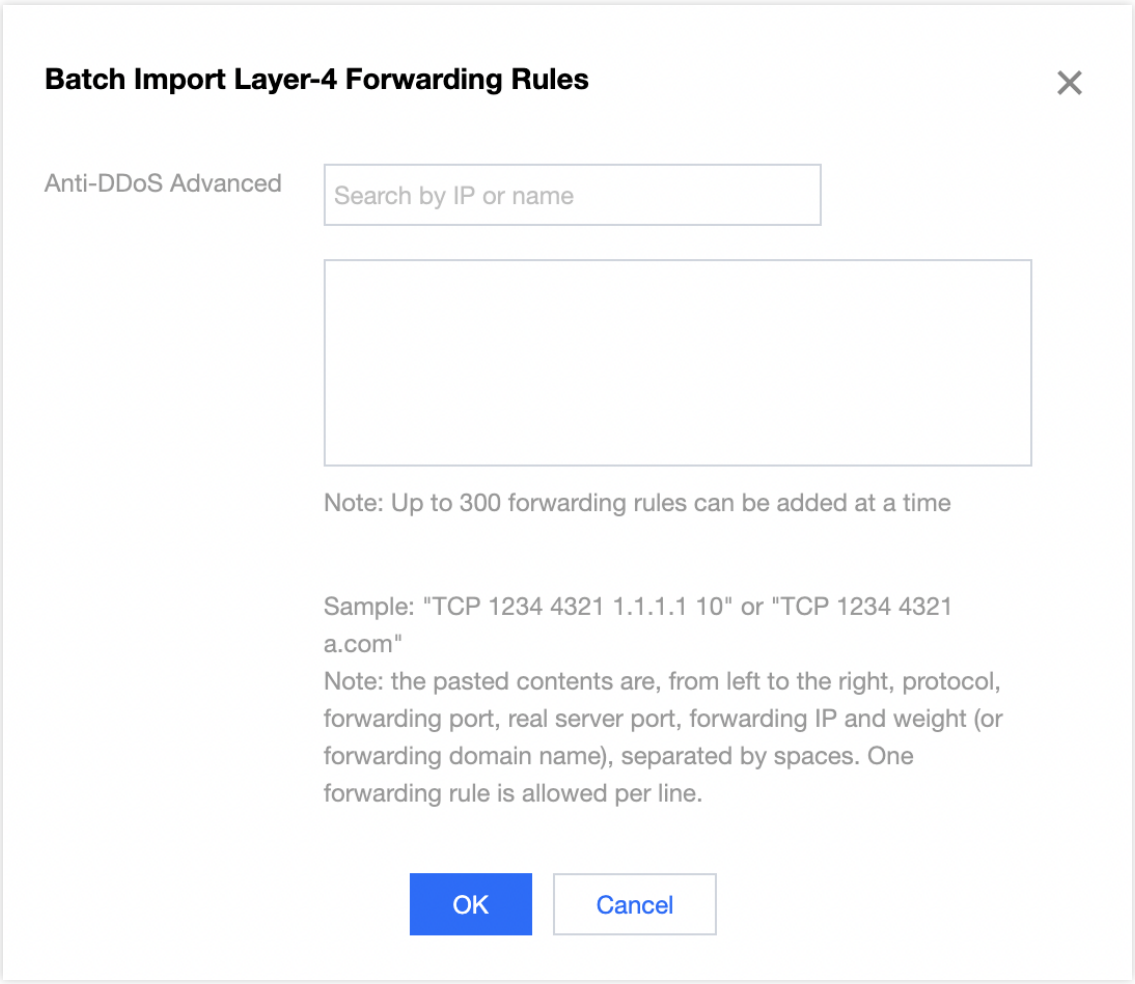
This document describes how to quickly sync forwarding rules when configuring multiple Anti-DDoS Advanced instances or non-BGP Anti-DDoS Advanced instances.

Directions

1. Log in to the new Anti-DDoS console, click **Business Access** on the left sidebar, and then click the **Access via port** tab.
2. On the **Access via port** page, click **Batch export**.
3. Enter an Anti-DDoS Advanced instance in the input box. All the forwarding rules configured for the instance will be displayed. Select forwarding rules to export and click **Copy**.



4. On the **Access via port** page, click **Batch import**.
5. Enter the new Anti-DDoS Advanced instance (with no forwarding rules configured) in the **Anti-DDoS Advanced** input box, paste the copied content in the input box below, and click **OK**.



6. Now you can view the forwarding rules in the list.

Smart Scheduling of CTCC/CUCC/CMCC Traffic

Last updated：2024-07-01 11:38:27

This document describes how to schedule traffic from CTCC, CUCC, and CMCC through smart scheduling.

Overview

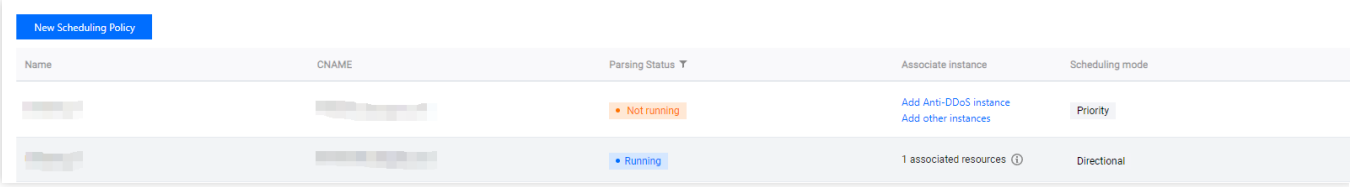
With a non-BGP Anti-DDoS Advanced instance, business traffic can be forwarded according to the source ISP of DNS requests, which is a common traffic scheduling method. You can configure smart scheduling to schedule the traffic from CTCC, CUCC, CMCC, or other ISPs to the Anti-DDoS Advanced instances of CTCC, CUCC, CMCC, and other ISPs respectively.

Prerequisite

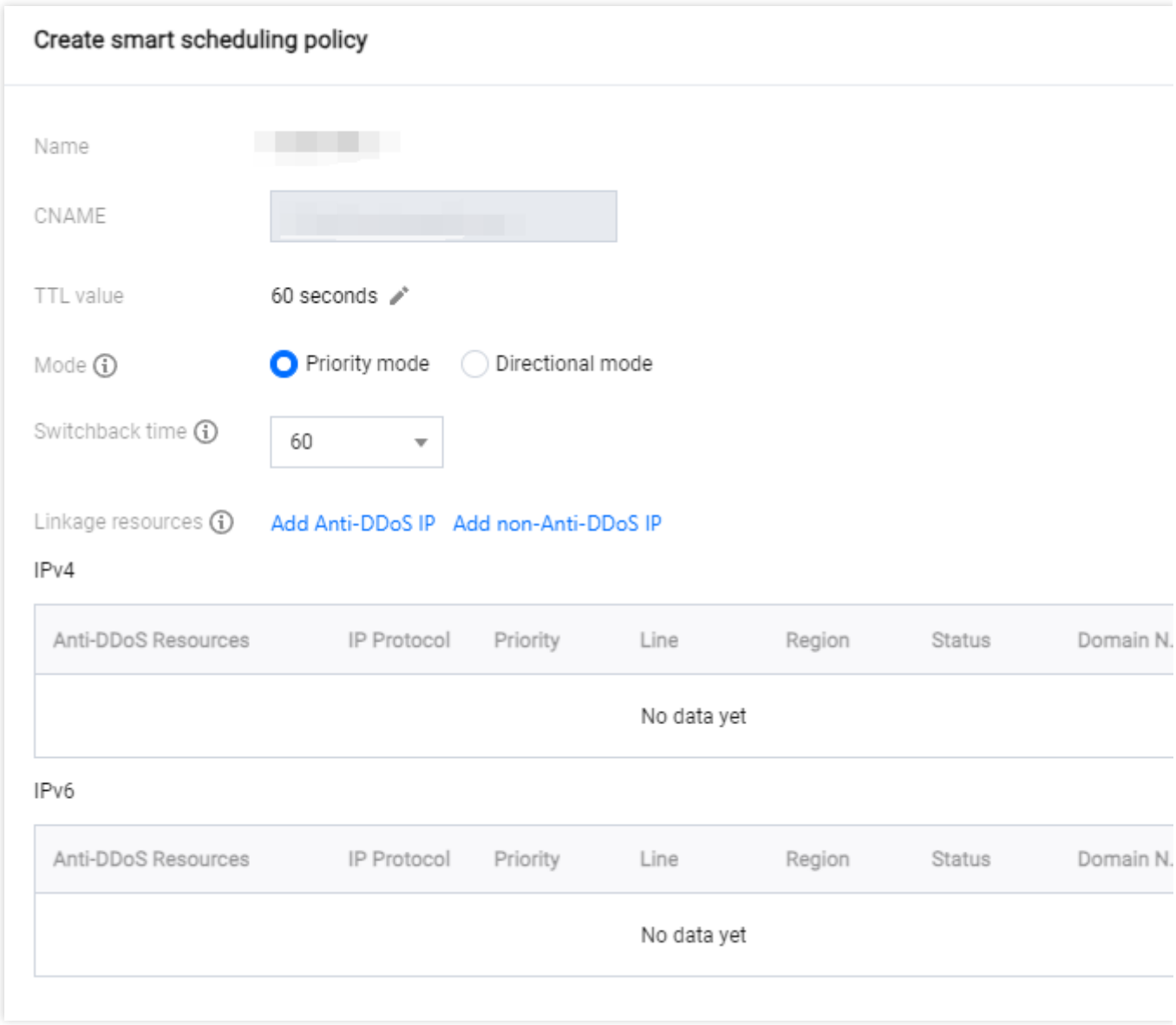
Before enabling smart scheduling, please connect your business to your Anti-DDoS instance.
If you need to add the IP of your protected Tencent Cloud product to a purchased Anti-DDoS Pro instance, see Getting Started.
If you need to connect your layer-4 or layer-7 business to an Anti-DDoS Advanced instance, see Port Connection or Domain Name Connection.
To modify the DNS resolution, you need to purchase a DNS service, such as Tencent Cloud DNSPod.

Directions

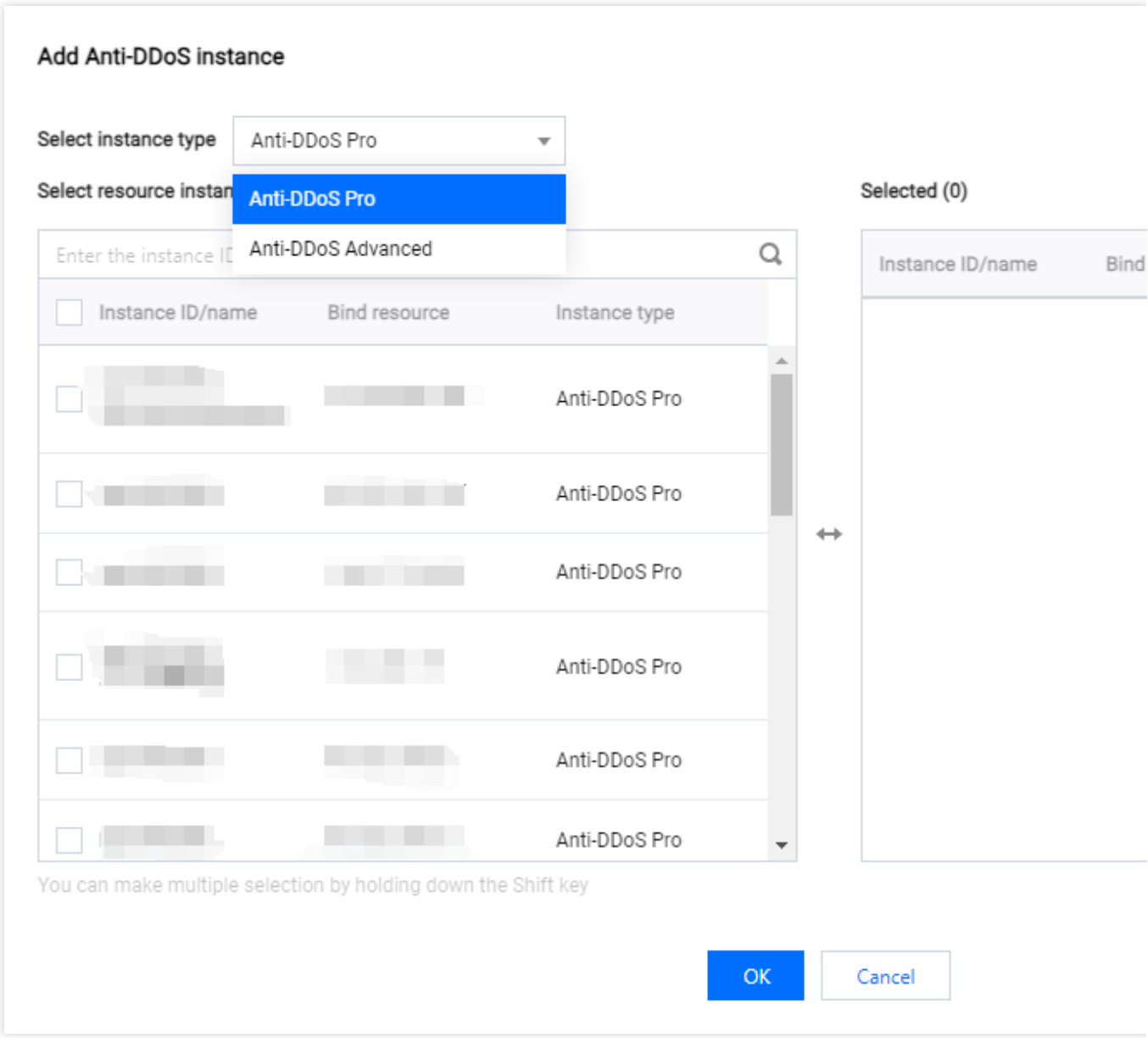
1. Log in to the new Anti-DDoS console, and click **Smart Scheduling** on the left sidebar.
2. Click **New Scheduling Policy** to generate a CNAME record.



3. The TTL value defaults to **60 seconds** and ranges from 1 to 3600 seconds. The default scheduling mode is **Priority**.



4. Click **Add Anti-DDoS IP**, select the target Anti-DDoS instance and IP, and click **OK**.



5. After the instance is added, DNS resolution is enabled for its protective line by default. At this point, you can set the priority.

Note:

The priority of the three ISPs must be the same to guarantee that DNS requests can receive responses according to the source ISPs.

For smart scheduling configurations, see Smart Scheduling.