Anti-DDoS Pro

Best Practice

Product Documentation

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

Best Practice

Remote Protection Scheme with Anti-DDoS Pro

Last updated：2020-07-07 16:10:31

Background

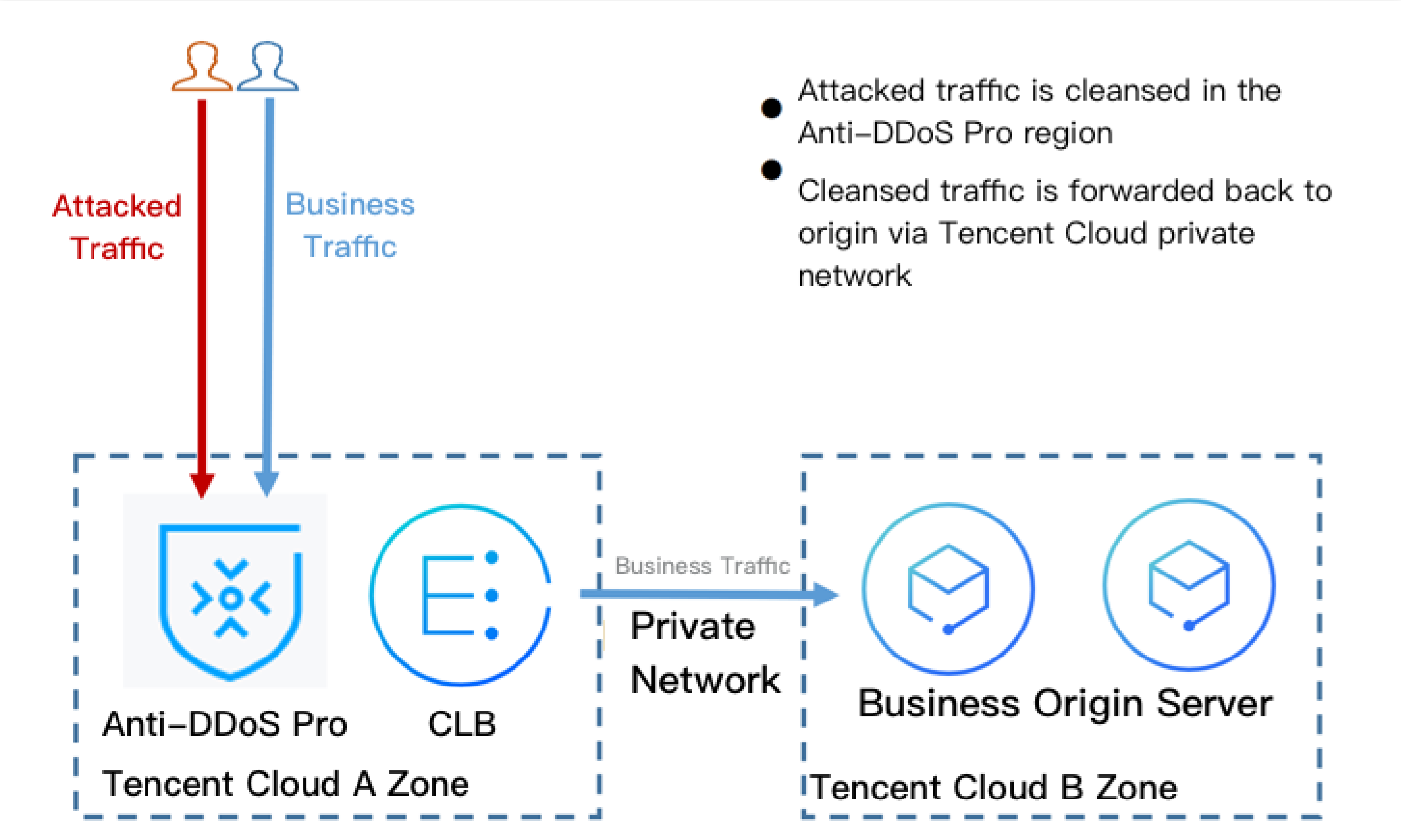
Anti-DDoS Pro provides up to 300 Gbps of protection bandwidth in Shanghai but a lower bandwidth in Guangzhou and Beijing. In addition, Anti-DDoS Pro is not available in Chengdu, Chongqing, and other regions in Mainland China. If your business real server is deployed in Tencent Cloud and you need to use the DDoS protection capability in regions other than the region 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. First, you will need to deploy a CLB instance in the region where you have Anti-DDoS Pro resources and bind it to your Anti-DDoS Pro instance. Then, configure the private network forwarding rules for CLB to ensure that your business can be accessed through the public IP of the CLB instance.

- Under normal circumstances, business traffic will be resolved to the public IP of the real server or directly to the public IP of the CLB instance in another region for nearby access to the real server.
- If attacks occur, business traffic will be resolved to the CLB IP for the Anti-DDoS Pro instance to cleanse the traffic. After the traffic is cleansed, CLB will forward the traffic back to the real server through private network Direct Connect.

The following figure describes the details of the solution:



Benefits

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

Suggestions and Notes

- Deploy Anti-DDoS Pro and CLB instances in advance.
- Establish a business availability monitoring system so that you can promptly detect and respond to any problem with access to the real server if no automatic switching mechanism is deployed.
- Test regularly, familiarize yourself with the solution details, and solve potential problems promptly.

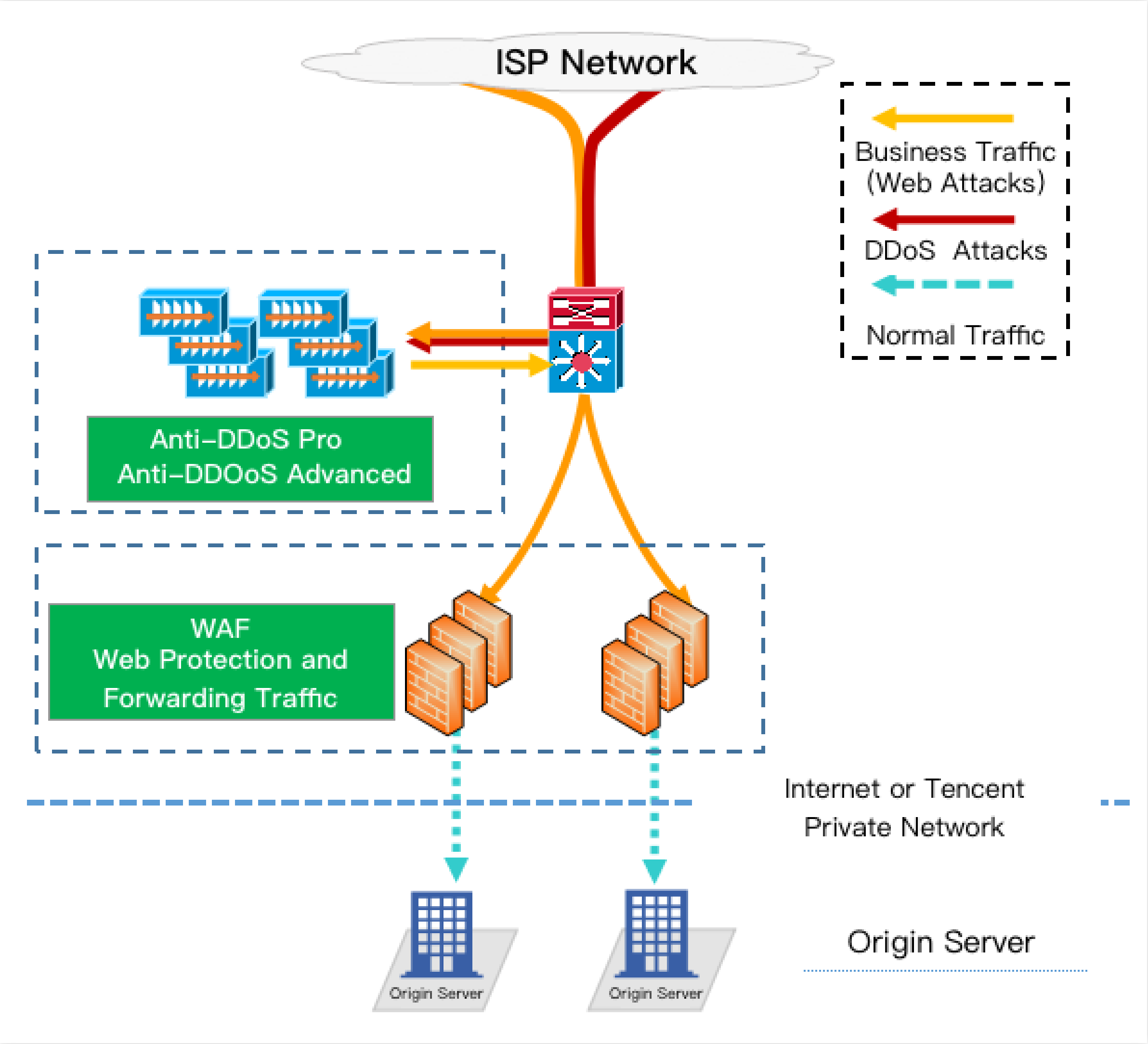
Using Anti-DDoS Pro Together with WFA

Last updated：2021-08-17 11:10:27

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



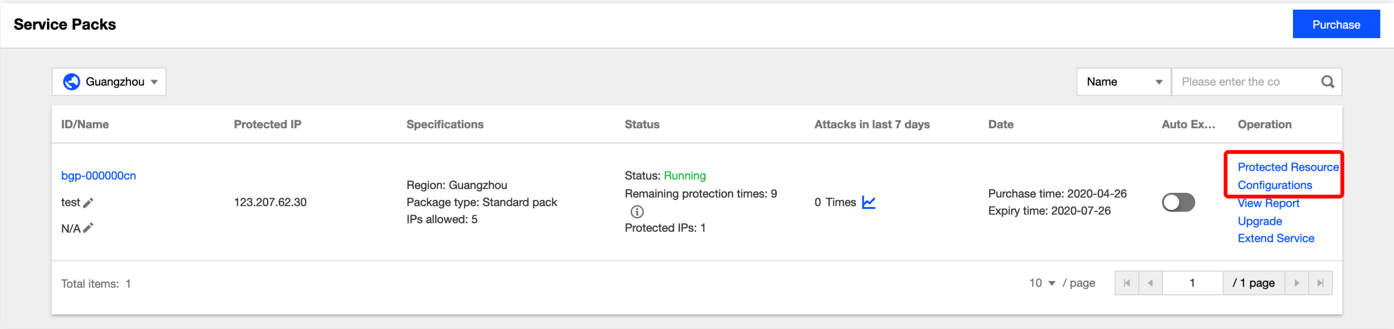
Directions

Configuring WAF

For more information on quick integration with WAF, please see Getting Started with WAF.

Configuring Anti-DDoS Pro

1. Log in to the new Anti-DDoS Pro Console and click **Anti-DDoS Pro Instance** on the left sidebar.
2. Select the region of the target Anti-DDoS Pro instance and click **Manage Protected Object** in the "Operation" column of the instance.



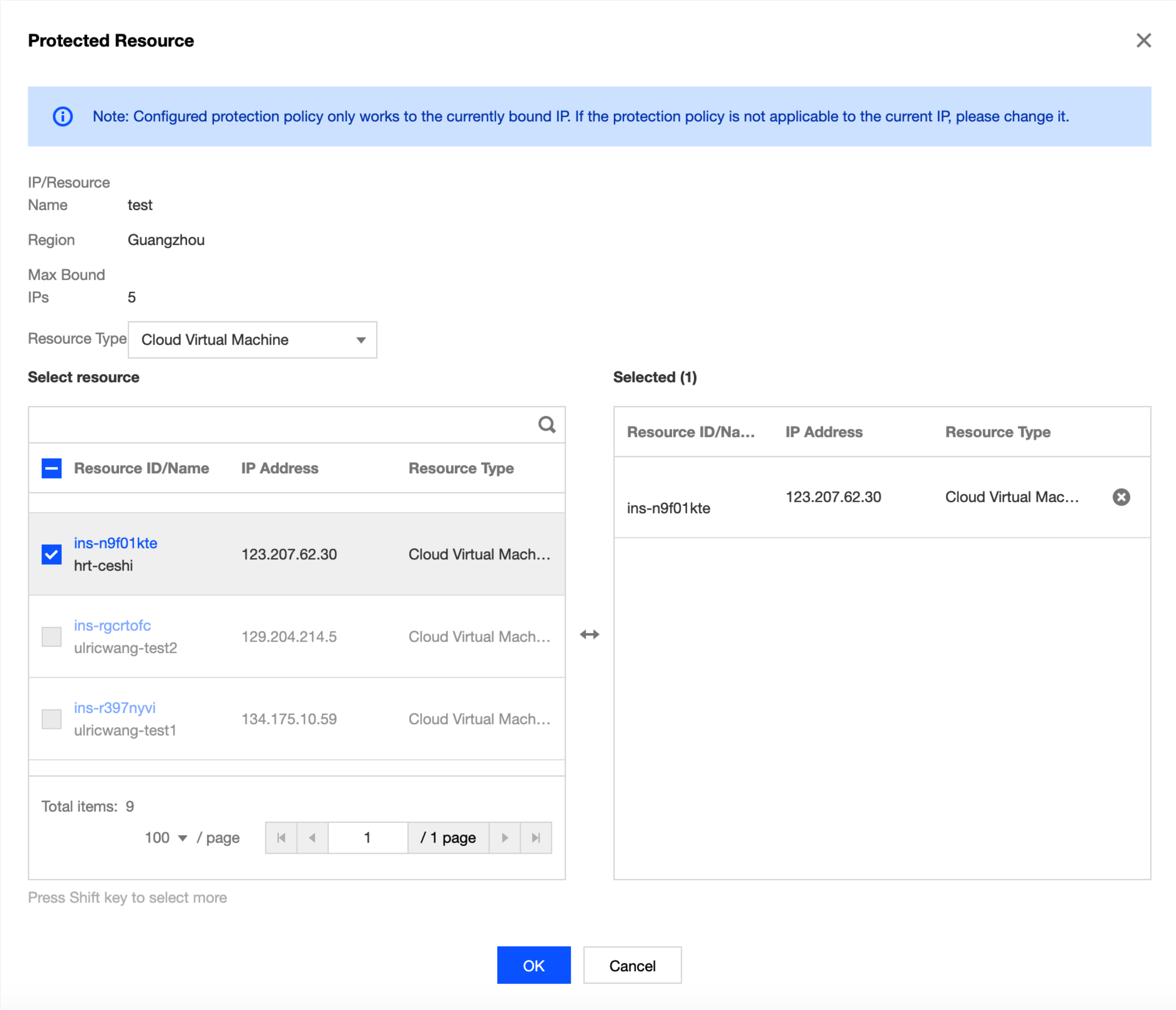
Service Packs

ID/Name	Protected IP	Specifications	Status	Attacks in last 7 days	Date	Auto Ex...	Operation
bgp-000000cn test N/A	123.207.62.30	Region: Guangzhou Package type: Standard pack IPs allowed: 5	Status: Running Remaining protection times: 9 Protected IPs: 1	0 Times	Purchase time: 2020-04-26 Expiry time: 2020-07-26	○	Protected Resource Configurations View Report Upgrade Extend Service

Total items: 1   10 / page   1   / 1 page

3. On the protected object management page, select "Resource Type" and "Resource Instance" as needed.
   - Resource Type: resources with public network IPs in the public cloud are supported, such as CVM, CLB, and WAF.

- Resource Instance: you can select multiple instances (no more than the number of "bindable IPs").



Protected Resource

Note: Configured protection policy only works to the currently bound IP. If the protection policy is not applicable to the current IP, please change it.

IP/Resource Name	test
Region	Guangzhou
Max Bound IPs	5
Resource Type	Cloud Virtual Machine

Select resource

	Resource ID/Name	IP Address	Resource Type
☑	ins-n9f01kte hrt-ceshi	123.207.62.30	Cloud Virtual Mach...
□	ins-rgcrtofc ulricwang-test2	129.204.214.5	Cloud Virtual Mach...
□	ins-r397nyvi ulricwang-test1	134.175.10.59	Cloud Virtual Mach...

Total items: 9

100 / page 1 / 1 page

Selected (1)

Resource ID/Na...	IP Address	Resource Type
ins-n9f01kte	123.207.62.30	Cloud Virtual Mac...

Press Shift key to select more

4. After completing the configuration, click **OK**.

Suggestions on Stress Test for Business System

Last updated：2022-07-06 14:45:33

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

> Note：
> The following suggestions are mainly about the impact of DDoS protection on stress testing. You may also need to consider other test-related factors, such as network bandwidth, linkage loads, and 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 Traffic and Number of Requests in 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 protection 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 Impact of Stress Test in Advance

You are recommended to contact Tencent Cloud solution architects or Tencent Cloud Technical Support before you conduct the stress test to evaluate possible consequences and develop risk aversion measures.

Solution to Exposed Real Server IP

Last updated：2020-07-07 16:10:34

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, you are recommended to change the actual real server IP.
You can refer to this document before changing the real server IP to check the risk factors and prevent the new IP from disclosure.

Checklist

Checking DNS resolution history

Check all the DNS resolution records of the attacked real server IP, including resolution records of sub-domain names, MX (mail exchanger) records of mail servers, and NS (name server) records. Make sure that all these records are configured to the protected IP so that the DNS will not resolve to the new real server IP.

Checking for information disclosure and command execution vulnerabilities

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

Checking for trojans and backdoors

Check your real server for potential trojans, backdoors, and other hidden risks.

Other Suggestions

- To prevent attackers from scanning C range or other similar IP range, you are not recommended to use the same IP or an IP similar to the old IP as the new real server IP.
- You are recommended to prepare the standby linkage and IP in advance.
- You are recommended to set the scope of access sources to prevent malicious scanning.

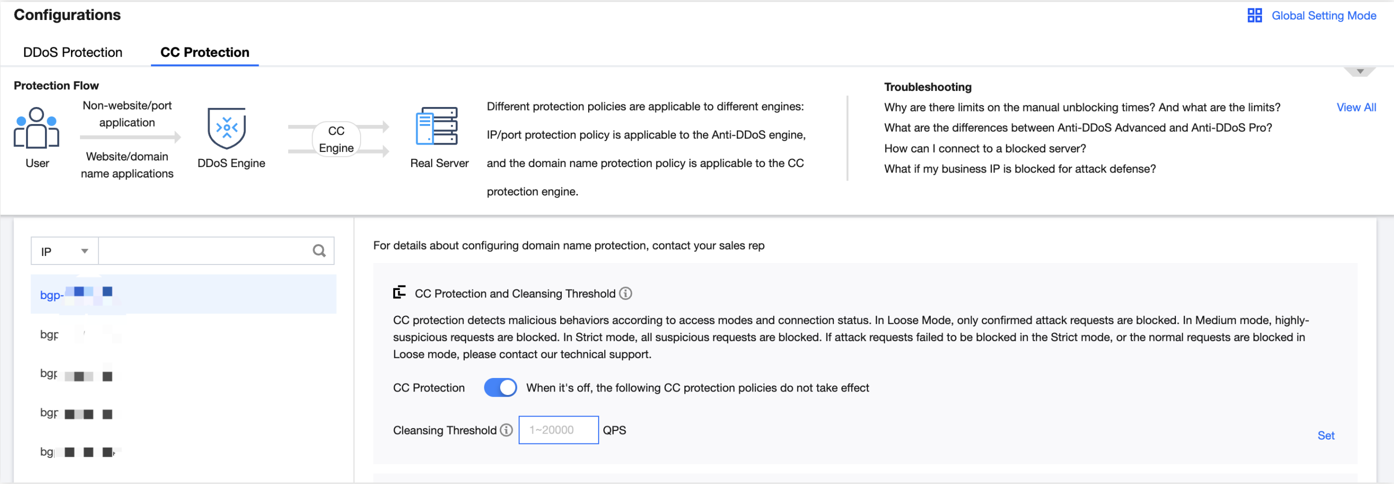
Configuration Directions and Notes on CC Protection Policy

Last updated：2022-06-13 17:14:23

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

Step 1: Set Cleansing Threshold

1. Log in to the Anti-DDoS Pro console and select **Anti-DDoS Pro (New)** > **Configurations** > **CC Protection**.
2. Select an Anti-DDoS Pro instance ID in the list on the left, such as "bgp-00xxxxxx".



Different protection policies are applicable to different engines: IP/port protection policy is applicable to the Anti-DDoS engine, and the domain name protection policy is applicable to the CC protection engine.

Why are there limits on the manual unblocking times? And what are the limits?
What are the differences between Anti-DDoS Advanced and Anti-DDoS Pro?
How can I connect to a blocked server?
What if my business IP is blocked for attack defense?

For details about configuring domain name protection, contact your sales rep

CC Protection and Cleansing Threshold ⓘ

CC protection detects malicious behaviors according to access modes and connection status. In Loose Mode, only confirmed attack requests are blocked. In Medium mode, highly-suspicious requests are blocked. In Strict mode, all suspicious requests are blocked. If attack requests failed to be blocked in the Strict mode, or the normal requests are blocked in Loose mode, please contact our technical support.

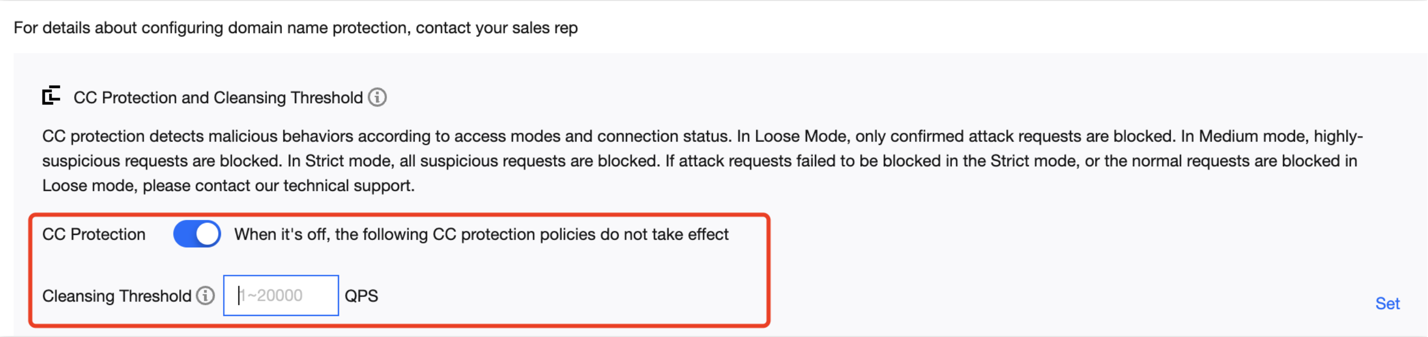
CC Protection: When it's off, the following CC protection policies do not take effect

Cleansing Threshold ⓘ 1~20000 QPS Set

3. To enable CC protection in the "CC Protection and Cleansing Threshold" section, click and set a cleansing threshold.

> Note：
>
> - The Anti-DDoS Advanced CC protection will be enabled once you set a cleansing threshold. A value that 1.5 times your common business peak is recommended.
> - The Anti-DDoS Pro 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, please see CC Protection and Cleansing Threshold.



For details about configuring domain name protection, contact your sales rep

CC Protection and Cleansing Threshold

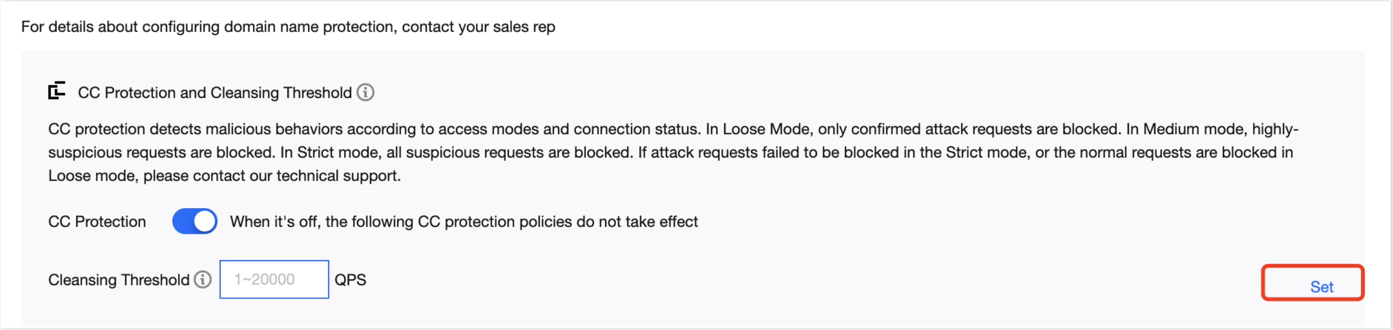
CC protection detects malicious behaviors according to access modes and connection status. In Loose Mode, only confirmed attack requests are blocked. In Medium mode, highly-suspicious requests are blocked. In Strict mode, all suspicious requests are blocked. If attack requests failed to be blocked in the Strict mode, or the normal requests are blocked in Loose mode, please contact our technical support.

CC Protection: When it's off, the following CC protection policies do not take effect

Cleansing Threshold: 1~20000 QPS

Step 2: Set CC Protection Level

1. Click **Set** in the **CC Protection and Cleansing Threshold** section to enter the rule list.



For details about configuring domain name protection, contact your sales rep

CC Protection and Cleansing Threshold

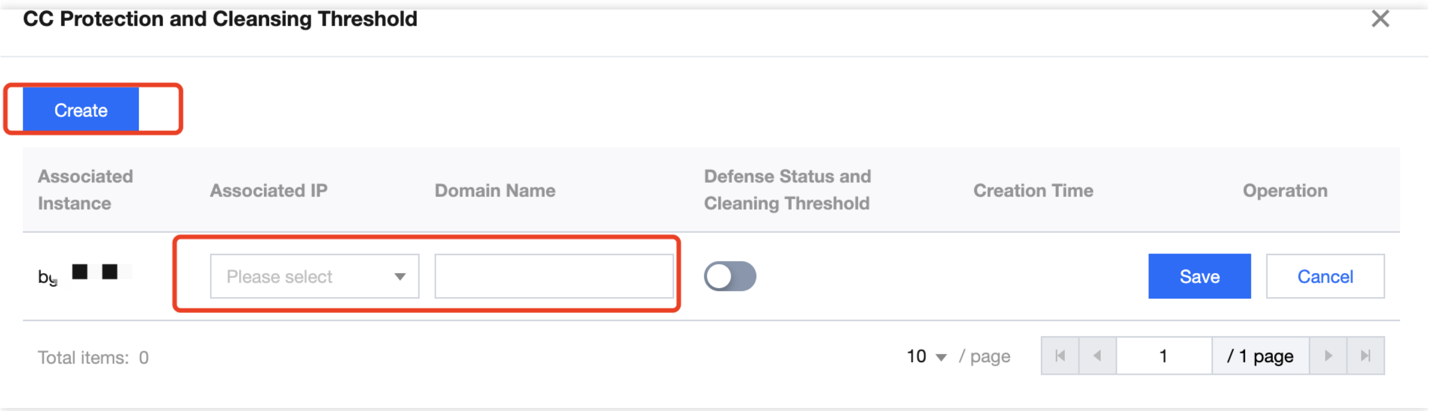
CC protection detects malicious behaviors according to access modes and connection status. In Loose Mode, only confirmed attack requests are blocked. In Medium mode, highly-suspicious requests are blocked. In Strict mode, all suspicious requests are blocked. If attack requests failed to be blocked in the Strict mode, or the normal requests are blocked in Loose mode, please contact our technical support.

CC Protection: When it's off, the following CC protection policies do not take effect

Cleansing Threshold: 1~20000 QPS

2. Click **Create**. Select an associated IP and a domain name, and set the defense status and cleaning threshold.

> Note：
>
> - Wildcard domain names are not supported.
> - When you create CC frequency limiting rules, CC protection is enabled by default.
> - Connected Anti-DDoS Pro instances will use the default cleansing threshold, and the system will generate a baseline based on historical patterns of your application traffic. You can set a cleansing threshold for a single domain name.



CC Protection and Cleansing Threshold

Associated Instance	Associated IP	Domain Name	Defense Status and Cleaning Threshold	Creation Time	Operation
by [redacted]	Please select ▾		○		Save Cancel

Total items: 0

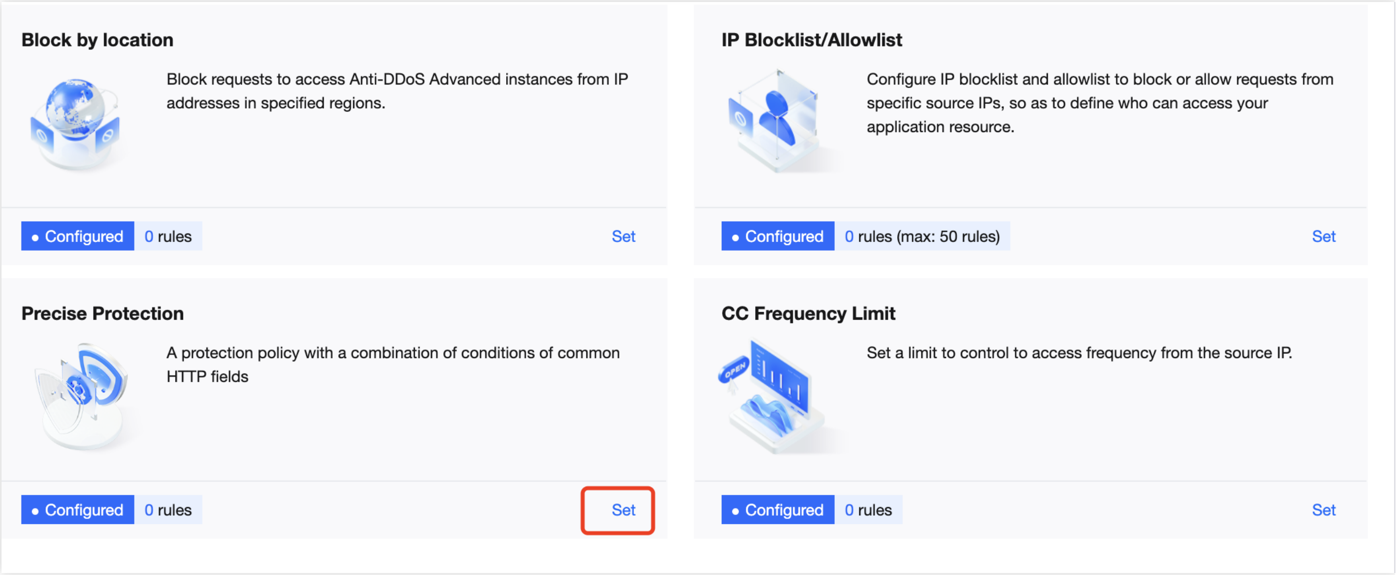
3. Click **Save**.

Step 3: Set 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.

1. Click **Set** in the **Precise Protection** section to enter the rule list.



Block by location

Block requests to access Anti-DDoS Advanced instances from IP addresses in specified regions.

● Configured 0 rules Set

IP Blocklist/Allowlist

Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.

● Configured 0 rules (max: 50 rules) Set

Precise Protection

A protection policy with a combination of conditions of common HTTP fields

● Configured 0 rules Set

CC Frequency Limit

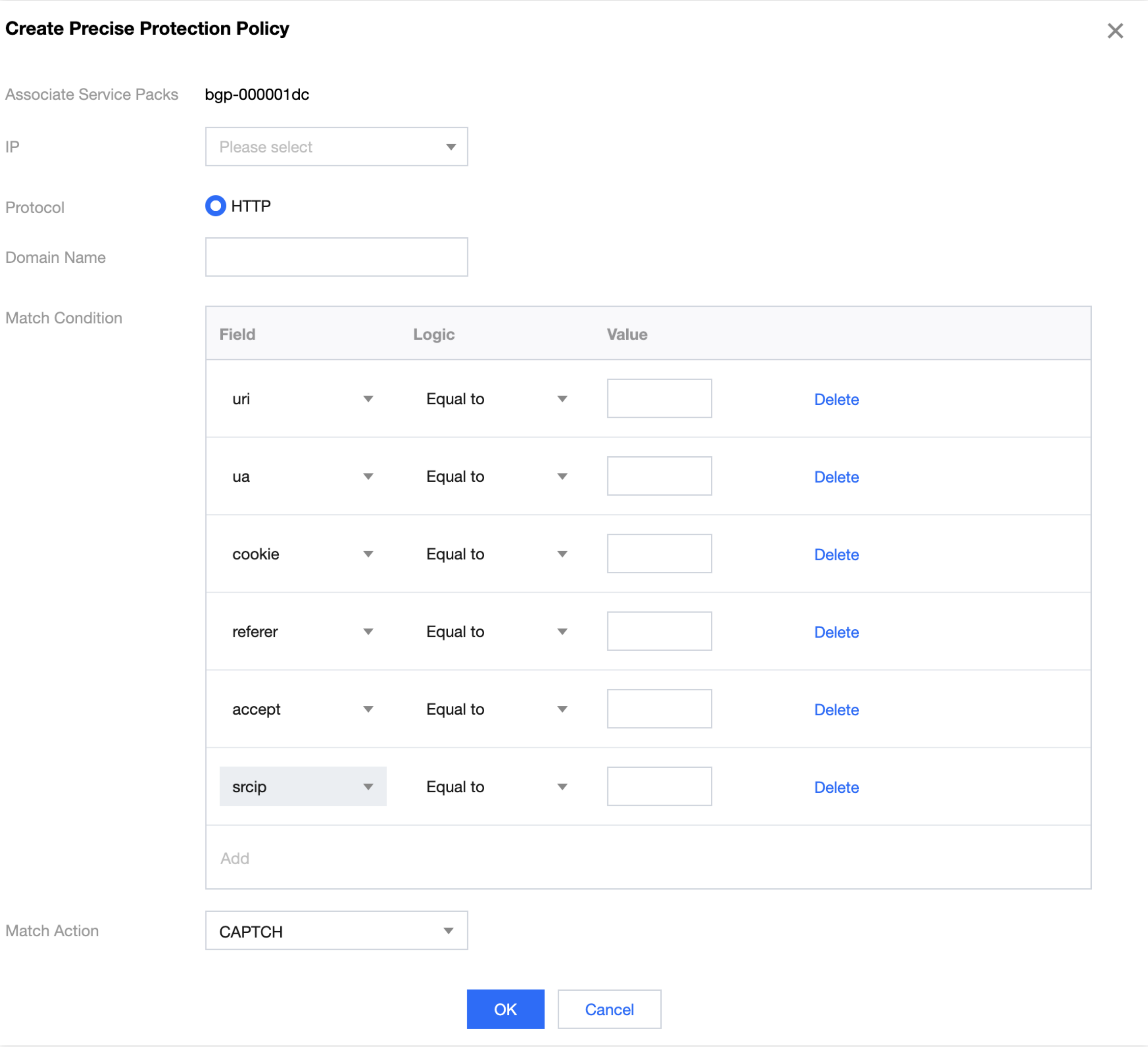
Set a limit to control to access frequency from the source IP.

● Configured 0 rules Set

2. Click **Create**. On the pop-up page, enter the required fields, and click **OK**. For more information, please see Precise Protection.

Note：

- If a policy involves multiple HTTP fields, the policy can be matched if all conditions are met.
- Precise protection for HTTPS businesses is currently supported for Anti-DDoS Advanced but not for Anti-DDoS Pro.



Create Precise Protection Policy

Associate Service Packs: bgp-000001dc

IP: Please select

Protocol: ● HTTP

Domain Name:

Match Condition

Field	Logic	Value	
uri	Equal to		Delete
ua	Equal to		Delete
cookie	Equal to		Delete
referer	Equal to		Delete
accept	Equal to		Delete
srcip	Equal to		Delete

Match Action: CAPTCH

Field description:

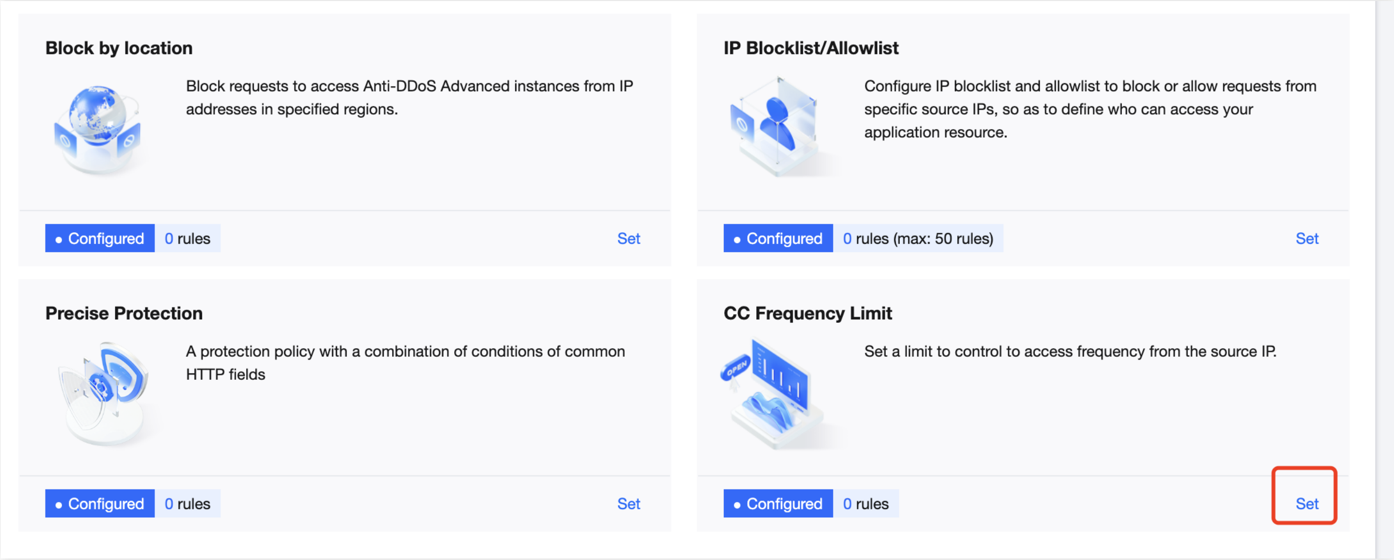
Field	Field Description

Field	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 condition	CAPTCHA and discard • Discard: discards packets without verifying the requester. • CAPTCHA: verifies the requester through algorithms. • Allow: allows the requests that match the specified conditions.

Step 4: Set 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.

1. Click **Set** in the **CC Frequency Limit** section to enter the rule list.



Block by location

Block requests to access Anti-DDoS Advanced instances from IP addresses in specified regions.

IP Blocklist/Allowlist

Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.

Precise Protection

A protection policy with a combination of conditions of common HTTP fields

CC Frequency Limit

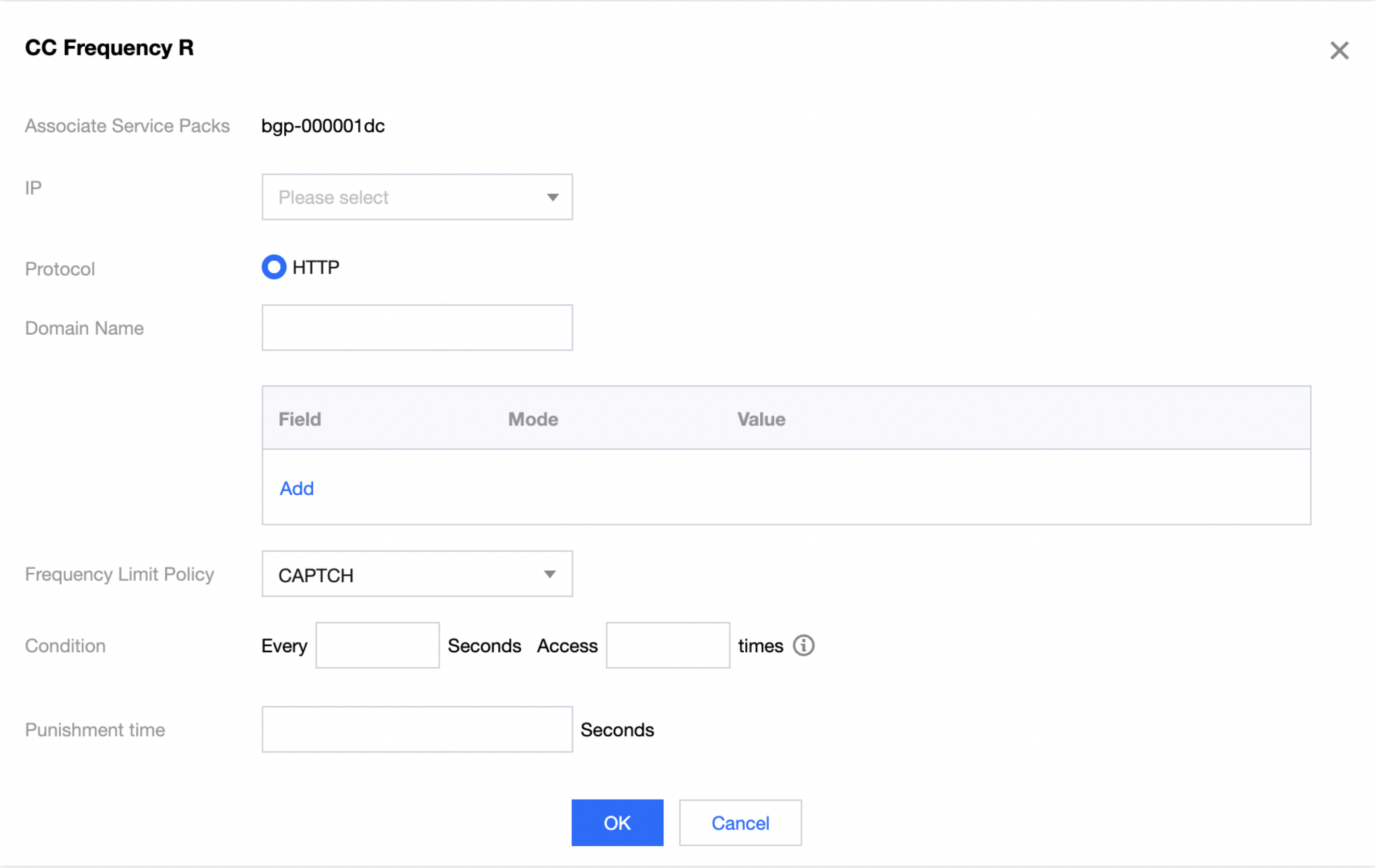
Set a limit to control to access frequency from the source IP.

2. You can create new rules, or edit existing rules by changing the defense level.

> Note：
>
> If the Anti-DDoS Advanced CC attack protection is enabled, the cleansing will be triggered when there is attack traffic, of which the detection strictness is the protection level. There are five available levels for you to select based on actual attacks: **Loose**, **Urgent Medium**, **Strict** and **Custom**. For more information, please see CC Protection and Cleansing Threshold.

3. Click **Create**. On the pop-up page, enter the required fields, and click **OK**. For detailed configurations, please see CC Frequency Limiting.

> Note：
>
> - Newly created rules only take effect in the "Custom" mode.
> - When configuring a CC frequency limit policy targeting the URI field, you need to configure a frequency limit on the directory `/` first and the match mode must be "equals 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, then the frequency 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.



CC Frequency R

Associate Service Packs	bgp-000001dc
IP	Please select
Protocol	● HTTP
Domain Name	
Frequency Limit Policy	CAPTCH
Condition	Every Seconds Access times
Punishment time	Seconds

Field	Mode	Value
Add		

Field description:

Field	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.
Frequency limit policy	CAPTCHA and discard • Discard: discards packets without verifying the requester. • CAPTCHA: verifies the requester through algorithms. • Allow: allows the requests that match the specified conditions.
Check 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.

Field	Field Description
Blocking time	The longest period is a whole day.

DDoS Simulation Testing Policy

Last updated：2022-08-29 11:00:07

Some customers who have subscribed to Tencent Anti-DDoS Proundefined Anti-DDoS Advanced or EdgeOne services may want to simulate a DDoS attack to verify whether the Anti-DDoS service functions as expected. This can be achieved via DDoS simulation testing.

DDoS simulation testing is permitted on Tencent Cloud. Howeverundefined you can only conduct DDoS simulation testing against your own application or services. You are aware of the risk of all DDoS simulation testing and responsible for the actions of the tester(s). It’s recommended to perform such tests in staging environments or during non-peak hours to minimize the impact on the production environment.

To avoid any impact to other customers’ services on Tencent Cloudundefined you must inform Tencent Cloud team at least 3 working days before you launch a DDoS simulation testundefined and provide the following information. And you agree to terminate the simulation testing at any point of time when you receive a suspension request from Tencent Cloud team.

- Attack origin region
- Attack duration
- Attack window
- Attack method (optional)
- Bandwidth size or range
- Target IPs/range/zones
- Target Ports
- Protocol
- Max packet/bit rate
- Contact in case of emergency (Nameundefined email and mobile)

Creating Anti DDoS EIP

Last updated：2023-06-25 14:43:31

> Note：
>
> **Anti DDoS EIP** is available only to bill-by-IP accounts.

Step 1: Purchase an Anti-DDoS Pro (Enterprise)

Log in to the Anti-DDoS console and go to the Anti-DDoS Pro Purchase Page. For more information, see Purchase Directions.

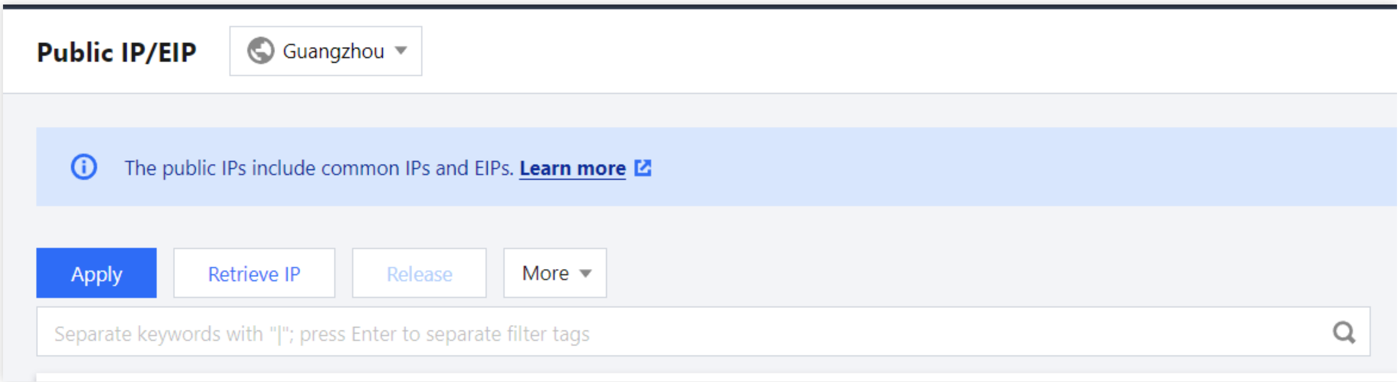
Step 2: Create a BGP Bandwidth Package

Create a BGP bandwidth package. For details, see Creating an IP Bandwidth Package.

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

Step 3: Create an Anti DDoS EIP

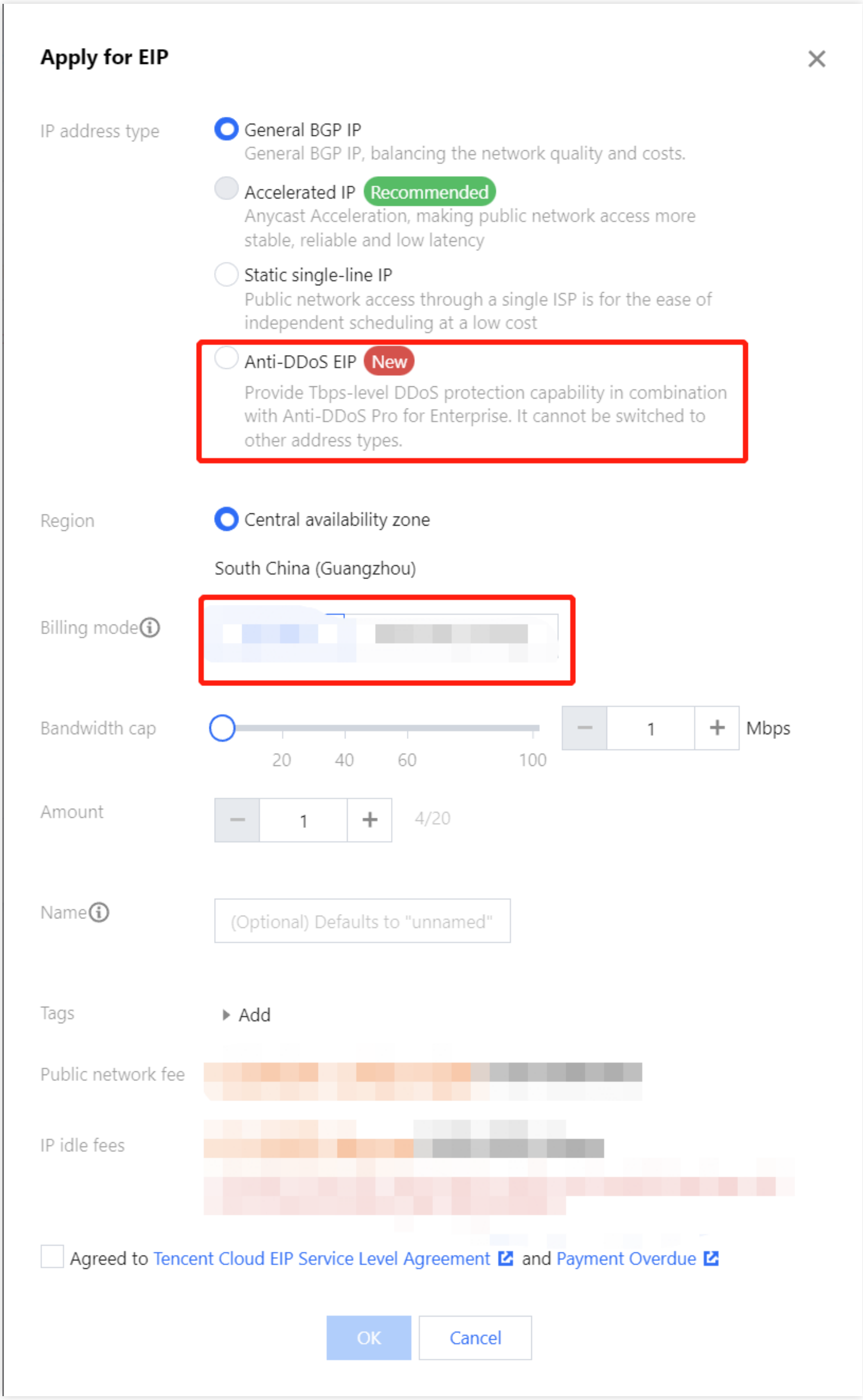
1. Log in to the CVM console and click ** Public IP** in the left sidebar.
2. Select a region on the page that appears and click **Apply**.



The public IPs include common IPs and EIPs. Learn more

Separate keywords with "|"; press Enter to separate filter tags

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



Apply for EIP

IP address type
- ● General BGP IP
  General BGP IP, balancing the network quality and costs.
- ○ Accelerated IP Recommended
  Anycast Acceleration, making public network access more stable, reliable and low latency
- ○ Static single-line IP
  Public network access through a single ISP is for the ease of independent scheduling at a low cost
- ○ Anti-DDoS EIP New
  Provide Tbps-level DDoS protection capability in combination with Anti-DDoS Pro for Enterprise. It cannot be switched to other address types.

Region: ● Central availability zone

South China (Guangzhou)

Billing mode: [redacted]

Bandwidth cap: 1 Mbps

Amount: 1 4/20

Name: (Optional) Defaults to "unnamed"

Tags: Add

Public network fee: [redacted]

IP idle fees: [redacted]

□ Agreed to Tencent Cloud EIP Service Level Agreement and Payment Overdue

Parameter	Description
IP type	Select **Anti DDoS EIP**

Parameter	Description
Billing mode	Only bandwidth package is supported
Bandwidth package	Select the desired **general BGP bandwidth package**
Bandwidth cap	Set the bandwidth cap as needed and allocate bandwidth resources reasonably
Anti-DDoS Pro (Enterprise)	Select the target **Anti-DDoS Pro (Enterprise) instance**
Quantity	Select the quantity of EIPs to be applied and ensure that it does not exceed the total quota
Name	EIP instance name (optional)
Tag	You can add a tag and use it for permission management

Related Operations

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