Anti-DDoS
Operation Guide

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

Operation Guide
Operation Overview

Last updated: 2026-03-11 17:22:16

When you use **Anti-DDoS Basic**, **Anti-DDoS Pro**, and **Anti-DDoS Advanced**, you may encounter issues such as configuring instances, viewing statistical reports, checking operation logs, and setting security event notifications. This article will introduce common operations when using Anti-DDoS protection for your reference.

Overview and Limits

Protection Overview
Use Limits

Asset Center

Cloud Asset List
Viewing Instance Information
Manage Protection Objects
Set Instance Alias and Tags
Upgrade Protection
Modify Elastic Protection Bandwidth
Renew an Instance
Unblock Protection IP

Business Integration

IP Transparent Access
Port Access
Domain Name Access
IP Integration

Scheduling and Unblocking

Intelligent Scheduling

Protection Configuration

Anti-DDoS Protection

Anti-DDoS Severity Level
IP Blocklist and Allowlist

CC Attack Prevention

Security Operations

Service Management

Protection Overview

Last updated: 2026-03-11 17:20:44

Viewing Attack Situation

1. Log in to the Anti-DDoS (New Version) Console, and in the left sidebar, click **Protection Overview** > **Protection Overview** to enter the Protection Overview page.
2. In the real-time defense situation module, business IP status data is displayed, allowing a quick understanding of the business IP health status.

3. In the attack situation module, you can also directly view various data situations.

Field Descriptions:

- Total number of attacks: The total number of attacks received, including those on basic protection services and those accessing anti-DDoS instances.

- Number of attacked IPs: The total number of business IPs that have been attacked. This includes the number of IPs attacked under basic protection, the number of business IPs attacked after accessing Anti-DDoS Pro, and the number of high-defense IP instances attacked.
- Number of blocked IPs: The number of business IPs that have been blocked from all external network access. This includes business IPs under basic protection, business IPs that have accessed Anti-DDoS Pro, and high-defense IP instances.
- Attack peak: The highest attack bandwidth in the current attack event.
- Attack packet rate: The highest attack packet rate in the current attack event.
- Peak attack requests: The highest number of attack requests in the current attack event.

Viewing Defense Situation

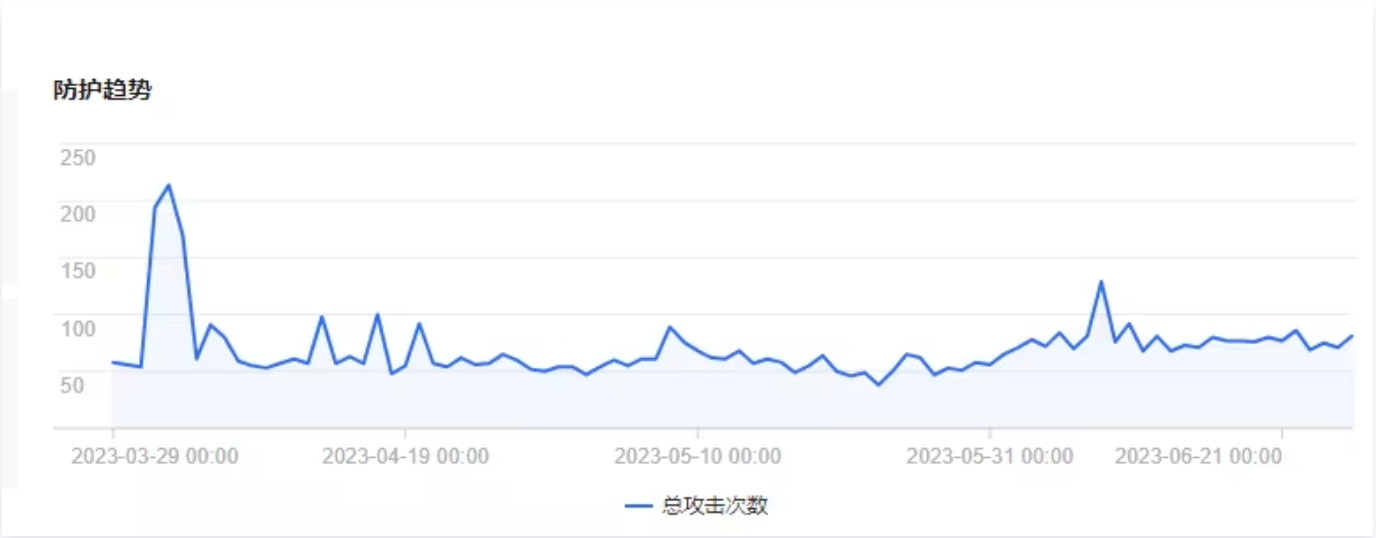
1. Log in to the Anti-DDoS (New Version) Console, and in the left sidebar, click **Protection Overview** > **Protection Overview** to enter the Protection Overview page.
2. In the real-time defense situation module, business IP status data is displayed, allowing a quick understanding of the business IP health status.

Field Descriptions:

- Total IPs: The total number of all business IPs, including those with basic protection, those connected to Anti-DDoS Pro, and high-defense IP instances.
- Defended IP count: Business IPs that have accessed Anti-DDoS Pro and high-defense IP instances.
- Blocked IP count: The number of business IPs that are blocked from all external network access. Includes business IPs of basic protection, business IPs connected to

Anti-DDoS Pro, and high-defense IP instances.

3. In the defense situation module's protection trend, the total number of attacks on all businesses within a week is displayed, allowing for a quick understanding of recent attack status distribution.



4. In the defense situation module's recommended action, business IPs under basic protection status that are attacked are displayed, suggesting access to advanced protection. This facilitates users in quickly connecting attacked IPs to advanced protection to ensure business security.

Viewing Protection Instance Description

1. Log in to the Anti-DDoS (New Version) Console, and in the left sidebar, click **Protection Overview** > **Protection Overview** to enter the Protection Overview page.
2. In the protection instance details module, the security status of anti-DDoS resources is displayed, allowing for a quick and comprehensive understanding of the distribution of risky businesses. On the right side, the protection quota status is displayed, which allows for a quick understanding of the used protection quotas for Anti-DDoS Pro and Anti-DDoS IP.

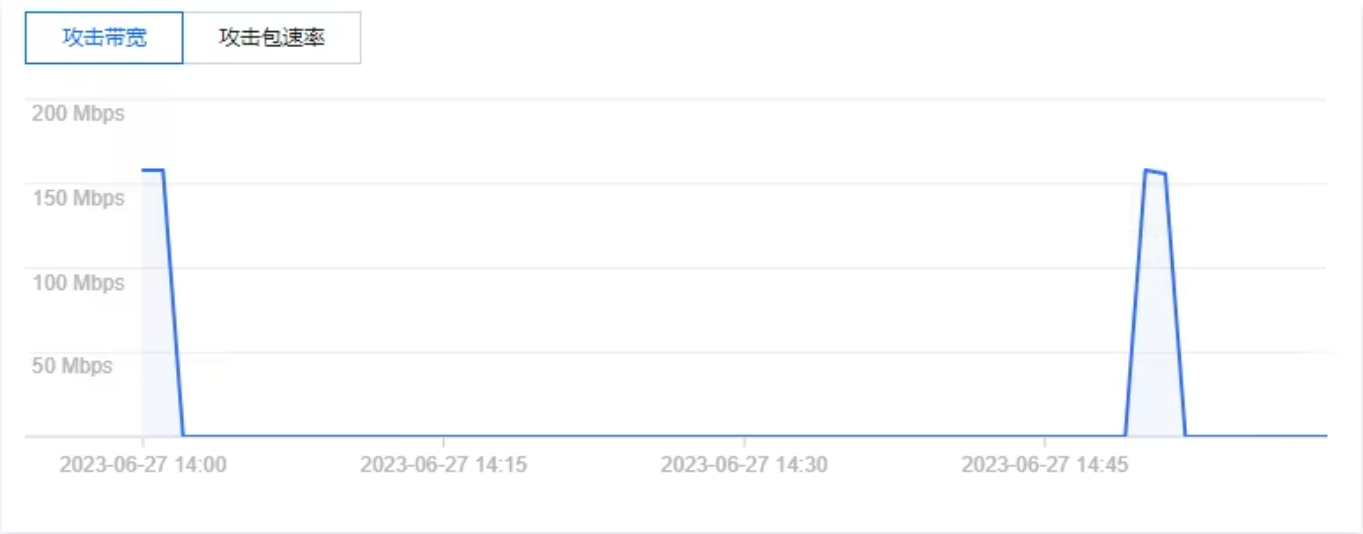
Viewing Recent Security Events

1. Log in to the Anti-DDoS (New Version) Console, and in the left sidebar, click **Protection Overview** > **Protection Overview** to enter the Protection Overview page.
2. In the recent security events module, the latest total number of attack events is displayed. Click **View Details** to enter the event details page, providing support for DDoS attack analysis and trace the source.

3. In the attack information module on the event details page, view the attack situation of IPs within that time range, including attacked IPs, status, attack type (sampling data), peak attack bandwidth, peak attack packet rate, start time, end time, and basic information.

4. In the attack trend module on the event details page, you can view the trend of network attack traffic bandwidth or attack packet rate. When an attack occurs, the peak of the attack traffic can be clearly seen in the traffic trend chart.

> **Note:**
> The data here is the full real-time data for that attack time period.



5. In the attack statistics module on the event details page, you can view the distribution of attacks under the two data dimensions of attack traffic protocol distribution and attack type distribution.

> **Note:**
> The data here is the attack sampling data within that attack time period, not full data.

Field Description:

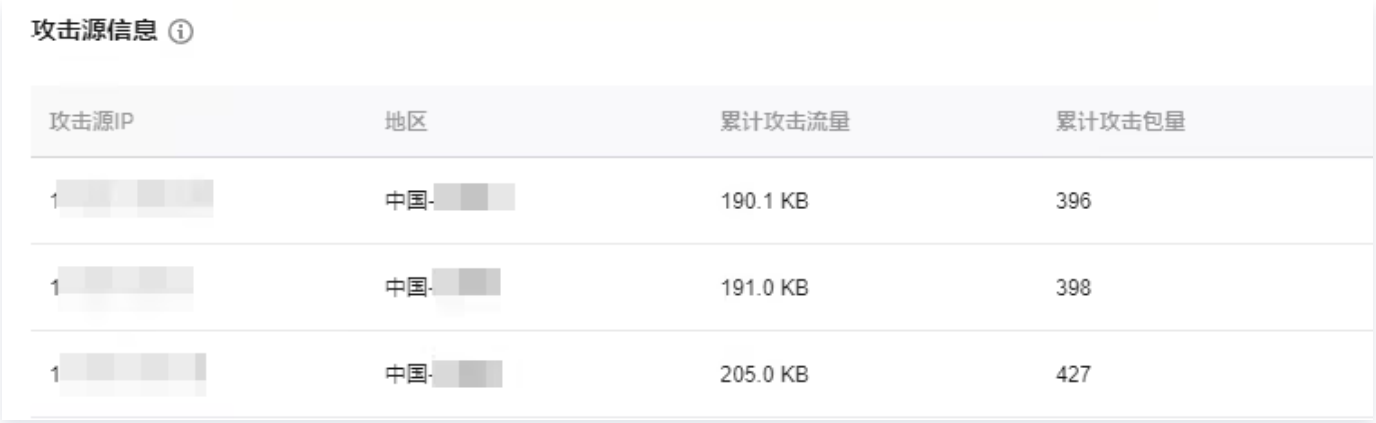
- Attack traffic protocol distribution: View the proportion of total attack traffic by each protocol in the attack events suffered by the selected Anti-DDoS instance within the specified time range.
- Attack type distribution: View the proportion of the total number of each attack type suffered by the selected Anti-DDoS instance within the specified time range.

6. In the "TOP5 Display" module on the event details page, you can view the top 5 attack source IPs and top 5 attack source regions, accurately grasping the detailed situation of the attack sources is conducive to the formulation of precise protection strategies.

> **Note:**
> The data here is the attack sampling data within that attack time period, not full data.

7. In the attack source information module on the event details page, you can view the random sampling data of the attack details within that attack period, displaying as much detail as possible about this attack, mainly including the attack source IP, region, cumulative attack traffic, and cumulative attack packet volume.

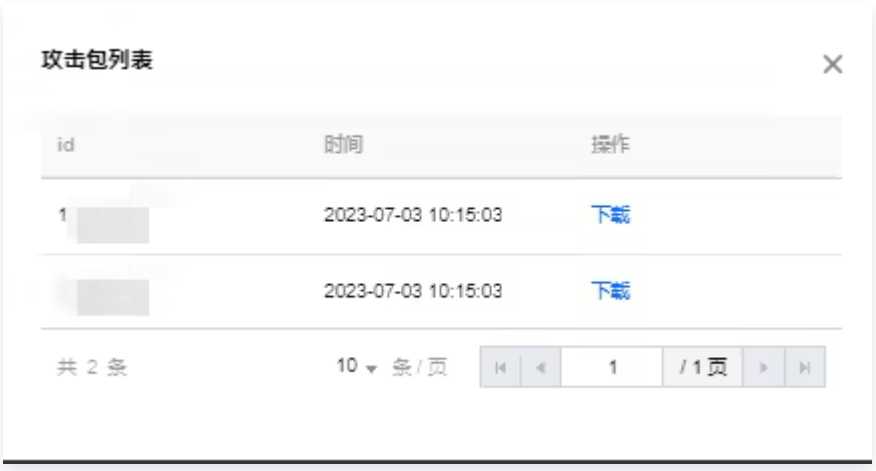
> **Note:**
> The data here is the attack sampling data within that attack time period, not full data.



8. In the recent security events module, DDoS attack events that have been suffered can be displayed.
   - Select the required event, click **View Details**, and the specific details of the event will be displayed on the right. It supports viewing attack source information, attack source

region, generated attack traffic, and attack packet volume size, etc., providing support for users to conduct DDoS attack analysis and trace the source.

- Select the required event, click to download the attack packet, in the attack packet list, select the required ID, and you can download the attack packet sampling data for this attack time period to understand the attack data and type in detail, providing data support for users to formulate targeted protection solutions.

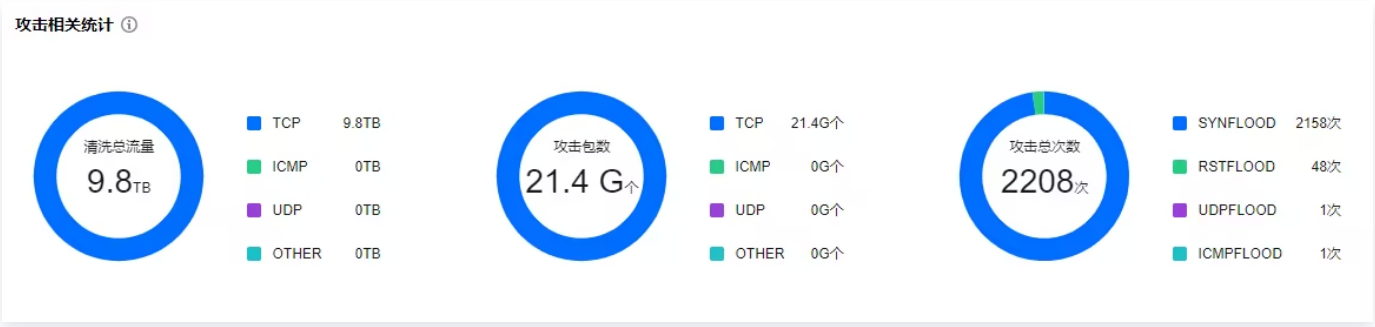


Viewing DDoS Attack Protection Status

1. Log in to the Anti-DDoS (New Version) Console, and in the left sidebar, click **Protection Overview** > **Attack Situation**.
2. On the DDoS Attack tab, set the query time range, select the target region, circuit, and Anti-DDoS Pro instance, and check whether there is an attack. By default, the DDoS attack data of all assets is displayed.

3. View the information of attacks suffered by the selected Anti-DDoS Pro instance within the queried period, including the trends of attack traffic bandwidth and attack packet rate.

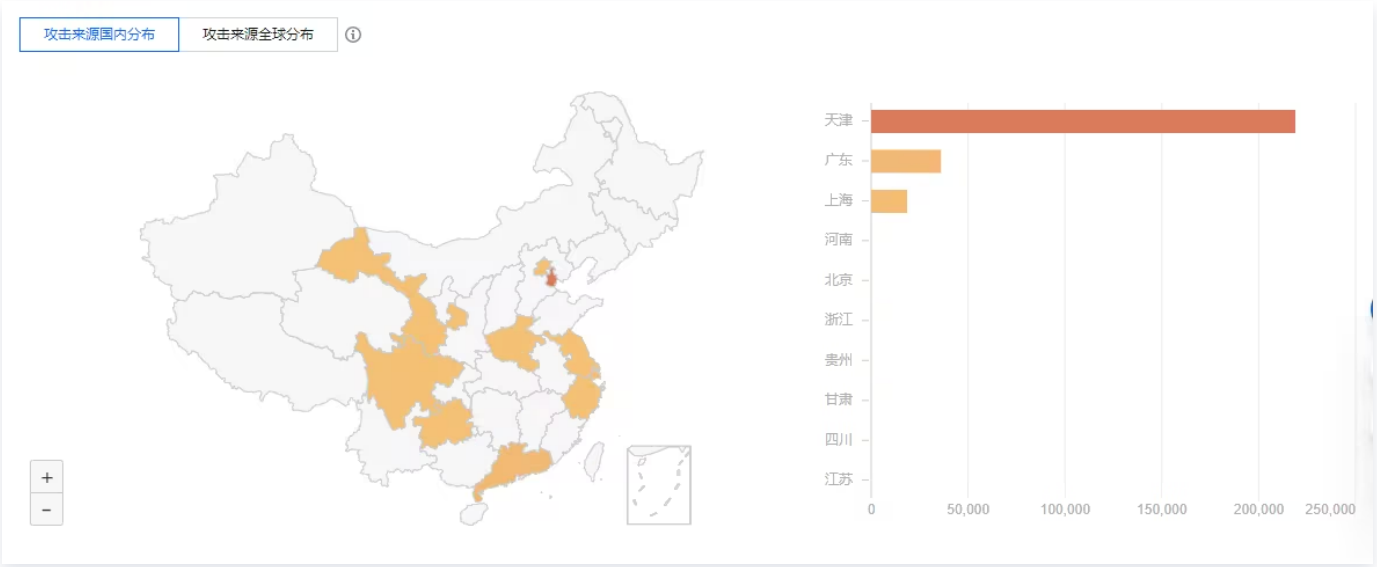
4. In the attack statistics module, you can view how the attacks distribute across different attack traffic protocols, attack packet protocols, and attack types through the attack traffic protocol distribution, attack packet protocol distribution, and attack type distribution.



Field Description:

- Attack traffic protocol distribution: View the proportion of total attack traffic by each protocol in the attack events suffered by the selected Anti-DDoS instance within the specified time range.
- Attack packet protocol distribution: View the proportion of the total number of attack packets by each protocol in the attack events suffered by the selected Anti-DDoS instance within the specified time range.
- Attack type distribution: View the proportion of the total number of each attack type suffered by the selected Anti-DDoS instance within the specified time range.

5. In the attack source module, you can view the distribution of attack sources at home and abroad within that time range for the suffered DDoS attack events, so that users can clearly understand the situation of attack sources and provide a basic basis for further protective measures.



Viewing CC Attack Prevention Status

1. Click **CC Attack** tab, set the query time range, select the target region and high-protection package instance, and check whether there is a CC attack.

2. Users can select the required time to view the trend and request rate data of the selected anti-DDoS instance. By observing the total request rate, attack request rate, total requests, and the number of attack requests, the degree of business impact can be determined.

Field Description:

- Total request rate: Statistic the rate (QPS) of the total request traffic received by the anti-DDoS instance currently.
- Attack request rate: Statistic the rate (QPS) of the attack request traffic currently.
- Total requests: Statistic the total number of requests received by the anti-DDoS instance currently.
- Attack request count: Statistic the count of attack requests received by the anti-DDoS instance currently.

3. In the recent security event module, if there is a CC attack, the system will record information such as the start time, end time, attacked domain name, total request peak value, attack request peak value, and attack source. Click **View Details** to display the specific details of the event. Supports viewing attack information, attack trend, and detailed CC records.

Use Limits

Last updated: 2026-03-11 17:21:21

Anti-DDoS Basic

Protection Object Limitation

Provide free basic Anti - DDoS protection for cloud products such as CVM, CLB and NAT Gateway in Tencent Cloud.

Anti-DDoS Pro Package

Protection Object Limitations

Anti-DDoS Pro is only applicable to Tencent Cloud services, including CVM, CLB, WAF, NAT gateway, VPN gateway, and lightweight application server, etc.

Connection Restrictions

Anti - DDoS Pro only supports binding to Tencent Cloud public network IPs in the same region.
Allowlist/Blocklist Configuration Limitations

- The total number of records (IP address + IP range) supported by the DDoS allowlist and blocklist combined is up to 100.
- CC URL allowlist configuration is not supported at this time.

Region Limitation

Anti - DDoS Pro can only be bound to Tencent Cloud devices in the same region. The currently available purchase regions include: Beijing, Shanghai, Guangzhou, Hong Kong (China), Singapore, Seoul, Tokyo, Bangkok, Frankfurt.

> **Note:**
> Currently, Anti-DDoS Pro for overseas regions is sold through the allowlist method. If you wish to purchase Anti-DDoS Pro for overseas regions, you can directly contact us to open an allowlist.

DDoS Protective IP

Protection Object Recommendations

It is recommended to use Anti - DDoS Advanced to provide protection for business IPs or domain names inside and outside Tencent Cloud, supporting protection for website (layer - 7) services and non - website (layer - 4) services.

Forwarding Capability Limitation

One Anti - DDoS Advanced instance supports 60 forwarding rules by default (a total of 60 for layer - 4 access and layer - 7 access), and up to 500 forwarding rules at most. Under the non - website (layer - 4) protocol, each rule supports 20 origin server IPs/domain names, while under the website (layer - 7) protocol, it supports 16 origin server IPs/domain names.

> **Note:**
> The number of forwarding rules is the total number of specification entries for TCP/UDP protocol + HTTP/HTTPS protocol forwarding, which can be upgraded to a maximum of 500 entries. For TCP and UDP protocols, if the same forwarding port value is used, two rules need to be configured.

Allowlist/Blocklist Configuration Limitations

- The DDoS allowlist and blocklist combined support up to 100 IP addresses.
- URL allowlist configuration is not supported.

Regional Limitation

Currently, Anti-DDoS Advanced is available both in and outside Chinese Mainland. Specifically, it is supported in the following regions outside Chinese Mainland: Hong Kong (China), Taiwan (China), Singapore, Seoul, Tokyo, Virginia, and Frankfurt.

Asset Center
Cloud Asset List

Last updated: 2026-03-26 15:40:09

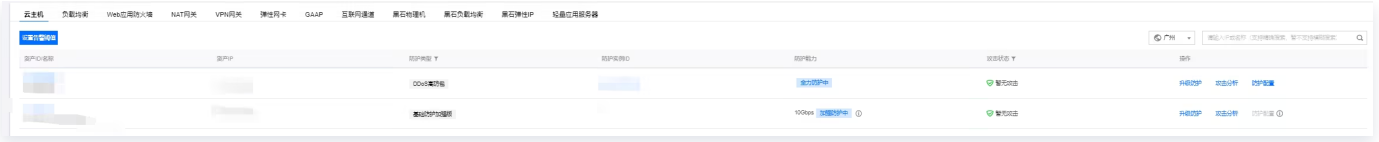
View Asset Security Status

1. Log in to the Anti-DDoS (New Version) Console, and in the left sidebar, click **Cloud Asset List** page.
2. In the asset security status module, business IP security status data is displayed, allowing for a quick understanding of the business IP security status.

3. In the asset protection status module, business IP protection status data is displayed, enabling a quick understanding of the business IP security status and direct connection to protection.

View Asset Instance Description

1. Log in to the Anti-DDoS (New Version) Console, and in the left sidebar, click **Cloud Asset List** page.
2. Taking Cloud Host as an example. On the details page, you can view detailed information about the asset, including asset instance name, IP address, protection type, protection instance ID, protection capability, attack status, and more.



Using Anti-DDoS high defense can enhance the DDoS protection capability for the following products:

- Cloud Virtual Machine: It is a scalable computing service provided by Tencent Cloud. Using CVM eliminates the need to estimate resource usage and make upfront investments required with traditional servers, helping you quickly launch any quantity of CVMs in a short time and instantly deploy applications.
- Cloud Load Balancer: Provides secure and fast traffic distribution services. Access traffic can be automatically distributed to multiple CVMs in the cloud through CLB, expanding the system's service capabilities and eliminating single points of failure.
- Web Application Firewall: It is an AI-based one-stop solution for web business operation risk protection.
- NAT Gateway: It is a kind of IP address conversion service that provides SNAT and DNAT capabilities and can provide secure and high-performance internet access services for resources in Virtual Private Cloud (VPC).
- VPN Connections: It is a transmission service based on network tunneling technology, which realizes the connection between local data center and resources on Tencent Cloud. It can help you quickly build a secure and reliable encrypted tunnel on the Internet.
- Cloud Bare Metal: It is a physical server rental service that can be purchased on demand and pay-as-you-go, providing you with a dedicated, high-performance, and secure isolated physical server cluster in the cloud.
- Global Application Acceleration: Global Application Acceleration Platform (GAAP) relies on high-speed channels, forwarding clusters, and smart routing technology between global nodes to achieve proximity access for users worldwide. It helps businesses solve the problem of global users experiencing lag or high latency by connecting directly to the origin server area through high-speed channels.
- Elastic Network Interface: It is an elastic network interface bound to CVMs in a Virtual Private Cloud (VPC), which can be freely migrated among multiple CVMs. Elastic Network Interfaces are very helpful in configuring and managing networks and building highly reliable network solutions.
- Tencent Cloud Lighthouse: It is a new generation of out-of-the-box, lightweight cloud server products aimed at lightweight application scenarios. It helps small and medium-sized enterprises and developers to build websites, web applications, mini programs/mobile games, apps, e-commerce applications, cloud storage/image hosting, and various development and testing environments on the cloud conveniently

and efficiently. Compared to ordinary CVMs, it is simpler and closer to applications. It is sold in the form of packages that include basic cloud resources and high-bandwidth traffic packages. It integrates popular open-source software for one-click application building, providing a simple cloud experience.

Manage Cloud Assets

1. Log in to the Anti-DDoS (New Version) Console, and in the left sidebar, click **Cloud Asset List**.
2. On the Cloud Asset List page, you can click on the products at the top to find the assets for that product. If there are many instances, you can use the search box in the upper right corner to filter.

3. After selecting the desired asset, you can perform the following operations on it:
   - Click **Set Alarm Threshold** to customize alarm policies according to your needs, click **Yes**.

   - Upgrade protection. When business growth requires one Anti-DDoS Pro to protect multiple business IPs, you can upgrade the protection to cover all business IPs. For details, see Upgrade Protection.

- Click **Attack Analysis**, and the page will jump to the protection overview (general view) page to view the attack situation.

- Click **Protection Configuration**, and the page will jump to the Anti-DDoS protection page to view the Anti-DDoS protection configuration.

Cloud Anti-DDoS Instance Viewing Instance Information

Last updated: 2026-03-11 18:05:11

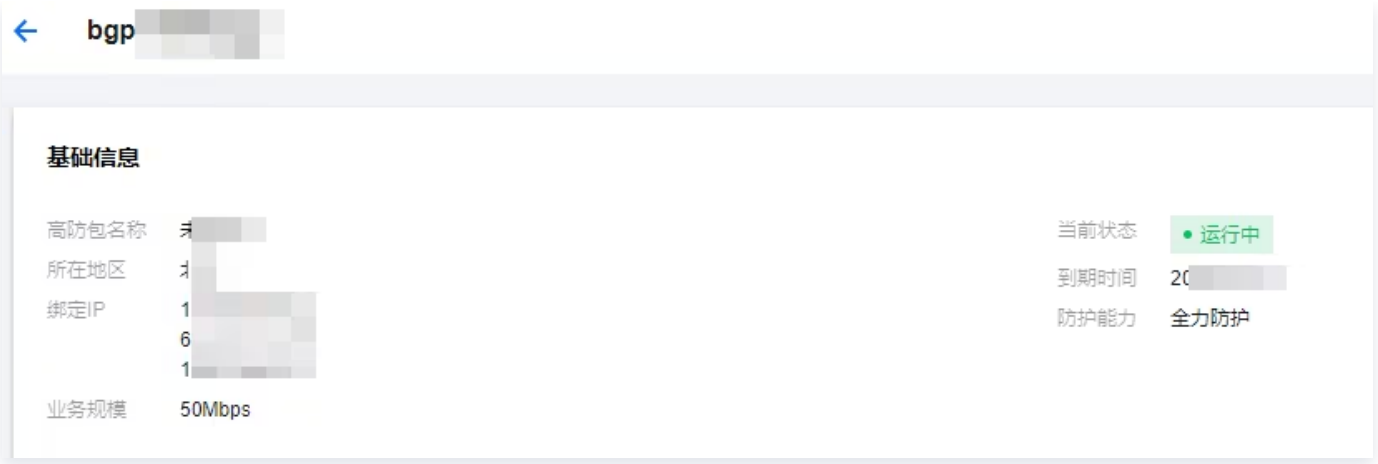
1. Log in to the Anti-DDoS (New Version) console, click on **Anti-DDoS instances** in the left sidebar, and enter the Anti-DDoS instances page.
2. On the Anti-DDoS instances page, you can view the basic information (such as the base protection peak bandwidth and running status) of your purchased Anti-DDoS Advanced packages; the basic information (such as the base protection peak bandwidth and running status) of your purchased Anti-DDoS Advanced IPs and the elastic protection configuration of the instances.

Operation Steps

For Example: View the Instance Information Of the Anti-DDoS Pro "Bgp-00000jt3"

1. Log in to the Anti-DDoS (New Version) console, click on **Anti-DDoS instances** in the left sidebar, and enter the Anti-DDoS instances page.
2. On the Anti-DDoS instances page, you can click on **All Regions** at the top to select a region or choose **protection package type** to find the Anti-DDoS Pro with the instance ID "bgp-00000jt3". Click on the ID "bgp-00000jt3" to view the detailed information of the instance. If there are many instances, you can use the **search box** in the upper right corner to filter.

3. View the following information on the pop-up page:

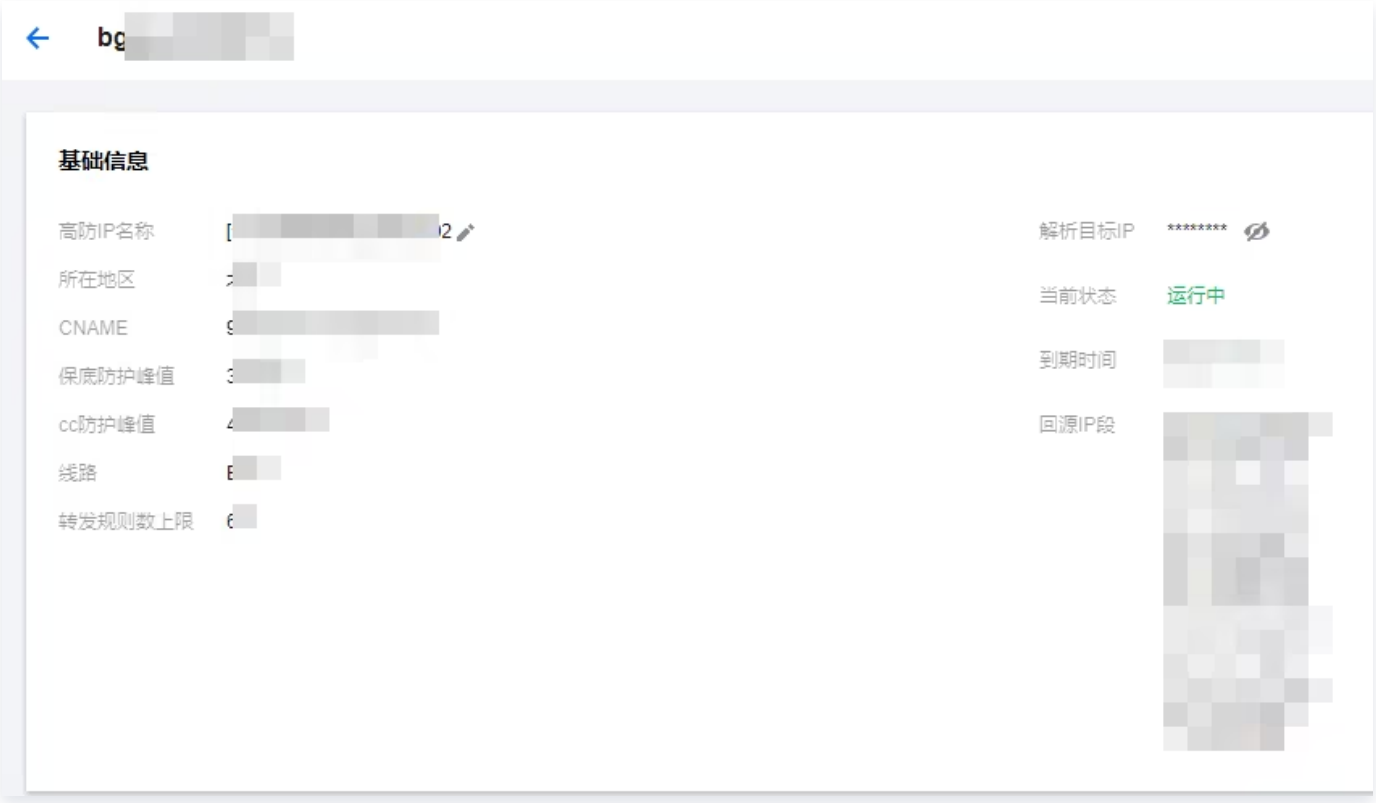


Parameter Name	Description
Anti-DDoS Name	The name of this Anti-DDoS Pro instance, used to identify and manage the Anti-DDoS instance. The length is 1 - 20 characters, and the character type is not restricted. The resource name is customized by the user according to actual business requirements.
Region	The region selected when purchasing Anti-DDoS.
Current Status	Current usage status of the Anti-DDoS instance. Statuses include running, scrubbing in progress, and blocking, etc. • Creating: Creating an anti-DDoS instance. • Running: Instance protection in progress. • Under attack: Under attack. • Blocking: Blocking the instance. • Unblocking: The instance is being unblocked. • Recycling: The instance has expired and is being recycled.
Expiration time.	Calculated based on the purchase duration selected at the time of purchase and the specific time of payment for the purchase order, accurate to the second. Within 7 days before the expiration of the Anti-DDoS resources, the system will push a reminder that the resources are about to expire to you. The message will be notified to the creator of the Tencent Cloud account and all collaborators via Message Center, Short Message Service, mail, WeChat, etc. (the actual reception method depends on your subscription configuration in the message center). For details, please refer to Instructions on Arrears.

Example: View the Instance Information Of the High-Protection IP Instance "Bgpip-0000070j"

1. Log in to the Anti-DDoS (New Version) Console, and click on **Cloud Protection Instances** in the left sidebar to enter the Cloud Protection Instances page.
2. On the Cloud Protection Instances page, select the desired instance, click on "ID" to view the detailed information of the instance. If there are many instances, you can use the search box in the upper right corner to filter.

3. View the following information on the pop-up page:



Parameter Name	Description
High-protection IP name	The name of this Anti-DDoS IP instance, used to identify and manage the Anti-DDoS IP instance. The length is 1 – 20 characters, and the character type is not restricted. The resource name is customized by the user according to actual business requirements.
Resolve target IP	This Anti-DDoS IP instance has an IP with anti-DDoS attributes. This IP address will be replaced periodically.

	Note: It is recommended to change your DNS resolution address to CNAME to avoid DNS resolution failure.
Region	The region selected when purchasing Anti-DDoS IP.
Current status	The current usage status of the Anti-DDoS IP instance. Statuses include running, scrubbing in progress, and blocking, etc.
CNAME	The CNAME of this Anti-DDoS Advanced instance. It resolves to an IP with anti-DDoS attributes through the scrubbing center and then forwards it back to the origin server to achieve protection. **Note: It is recommended to change your DNS resolution address to CNAME to avoid DNS resolution failure.**
Baseline protection peak value.	The base protection bandwidth capacity of this Anti-DDoS Advanced IP instance, that is, the base protection peak value selected when purchasing. If elastic protection is not enabled, the base protection peak value is the maximum protection peak value of the Anti-DDoS service instance.
Expiration time.	It is calculated based on the purchase duration selected when purchasing and the specific time of placing the purchase order, accurate to the second level. Tencent Cloud will push information about the upcoming expiration of the service and remind you to renew in time to the creator of your Tencent Cloud account and all collaborators through in-site messages, SMS and emails within 7 days before this time.
Tag	Indicates the tag name to which this Anti-DDoS Advanced instance belongs, which can be edited and deleted.
Origin-Pull IP Range	The IP used by the cleaning cluster to forward to the origin server.

Manage Protection Objects

Last updated: 2026-03-11 17:55:40

Anti-DDoS Pro provides stronger anti-DDoS protection for Tencent Cloud public IPs. It supports Tencent Cloud services including CVM, CLB, NAT, and WAF.
Based on actual business needs, users can add or remove the protection object IPs of Anti-DDoS Pro instances.

Prerequisites

To set the protection object IP, you need to successfully proceed to purchase Anti-DDoS Pro.

> **Note:**
> Anti-DDoS Pro (enterprise edition) is only effective for high-protection EIP under Tencent Cloud Elastic IP. To use the enterprise edition Anti-DDoS Pro, you need to replace the ordinary IP on the cloud with a high-protection EIP. The purchase of the enterprise edition Anti-DDoS Pro must be in the same region as the cloud resources to be bound, and it will only take effect after binding to the high-protection EIP. For details on high-protection EIP operations, please refer to High-protection EIP Creation and Usage Guide.

Operation Steps

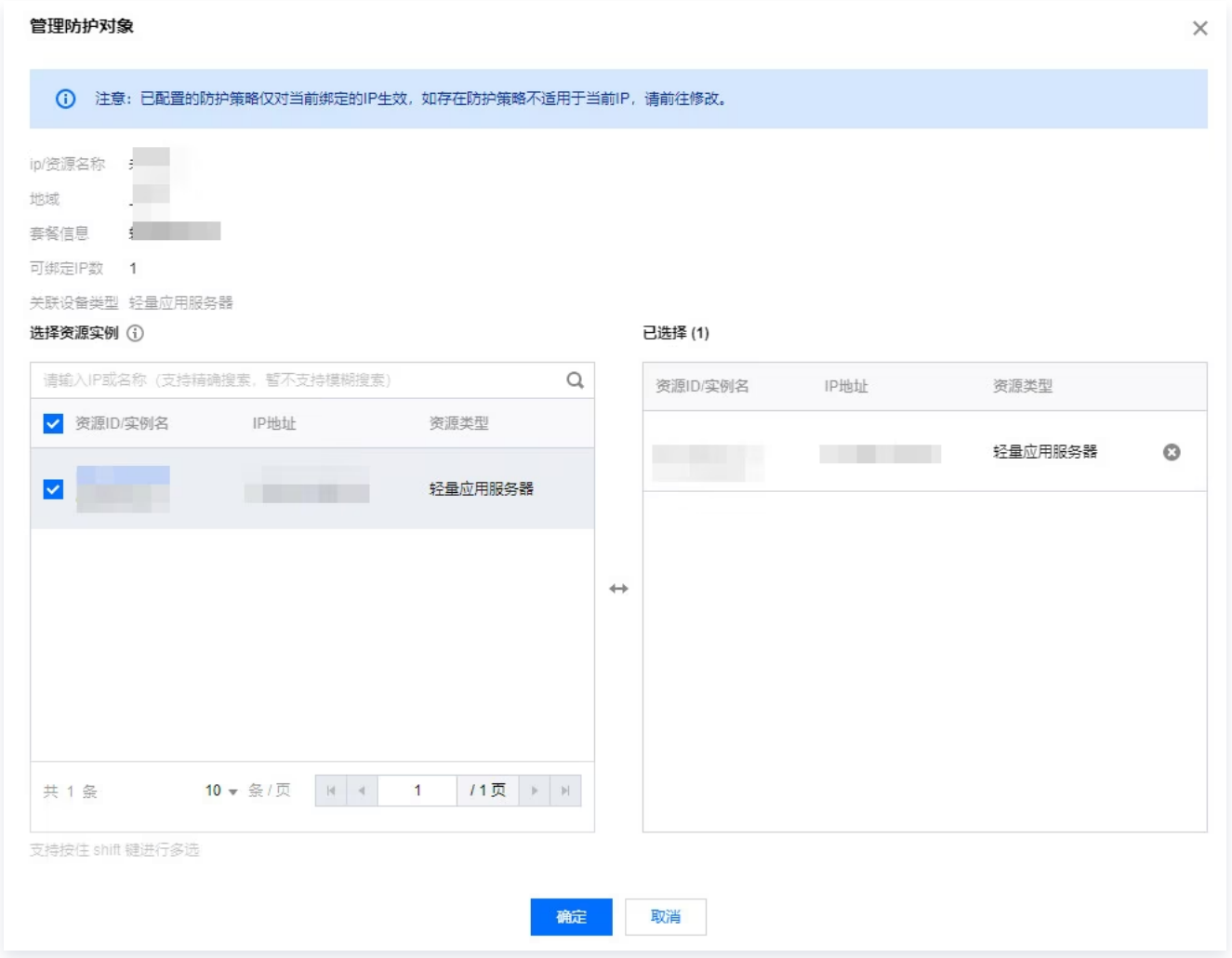
1. Log in to the Anti-DDoS Pro console, and click **Anti-DDoS instances** in the left sidebar.
2. On the Anti-DDoS instance page, click **Managing Protected Object** in the row of the target Anti-DDoS Pro instance.

3. On the **manage protection object** page, select the associated device type and resource instance according to actual protection needs.
   - Associated device types: Supports resources with public IP addresses in public cloud such as Cloud Host, Cloud Load Balancer, Web Application Firewall, etc.

> **Note:**

> The Enterprise Edition of Anti-DDoS Package only supports Anti-DDoS EIP.

- Select resource instance: Click the checkbox in front of the resource ID to add the resource to the protection object of Anti-DDoS Pro. Multiple selections are allowed, and the number of selected resource instances cannot exceed the number of bindable IPs.
- Selected: Click **Delete** behind the resource to remove the resource from the protection object of Anti-DDoS Pro.



> **Note:**
> - If an IP of Anti-DDoS Pro is under attack or blocked, the user is not allowed to unbind the IP.
> - When associating cloud assets, batch search and selection are supported.
> - Currently, it supports detecting the Destroyed status of CLB and CVM products and performing unbinding.

4. Click **OK**.

Setting Instance Alias and Tag

Last updated: 2025-03-19 21:39:56

When using multiple Anti-DDoS Pro instances or Anti-DDoS Advanced instances, you can quickly identify and manage the instances by setting the "resource name".

Prerequisites

You need to successfully purchase Anti-DDoS Pro or Anti-DDoS Advanced.

Operation Steps

Method 1

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, click the second row of the "ID/Name" column of the target instance , and enter the name.

> **Note:**
> The name length is 1 - 20 characters, and there is no restriction on the character type.

Method 2

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, click the instance ID in the "ID/Name/Tag" column of the target instance to enter the Basic Info page of the instance.

3. On the Basic Info page of the instance, click ✎ on the right side of the Anti-DDoS Pro name or Anti-DDoS IP name, and enter the name.

> **Note:**
> The name length is 1 – 20 characters, and there is no restriction on the character type.

Upgrade Protection

Last updated: 2026-03-11 17:52:39

When business growth requires the same anti-DDoS protection for multiple business IPs, you can upgrade the protection to cover all business IPs.

Prerequisites

To set the protection object IP, you need to successfully purchase DDoS Protection Pack or DDoS High Defense IP.

Operation Steps

1. Log in to the Anti-DDoS (New Version) console, and click on **Anti-DDoS instances** in the left sidebar.
2. On the Anti-DDoS instances page, select the target instance, and click **Upgrade**.

3. On the upgrade page, select the number of IPs, protection times, and business scale according to actual protection needs.
   - IP Quantity: Upgrade the number of IPs supported by anti-DDoS.
   - Protection Times: Upgrade the number of protections provided by anti-DDoS in one month.
   - Business Scale: The normal business scale of the protected business, which can be selected according to the estimated maximum peak value of business inbound or outbound traffic.

4. Click **Confirm Access** to complete the payment and upgrade.

Modify Elastic Protection Bandwidth

Last updated: 2026-03-11 17:53:18

The elastic protection peak value refers to the range of capabilities that Anti-DDoS can provide to resist attack traffic. If the attack traffic exceeds the maximum protection peak value, the attacked IP will be blocked.

Prerequisites

You need to successfully purchase Anti-DDoS Advanced.

Operation Steps

1. Log in to the Anti-DDoS (New Version) console, and click **Anti-DDoS instances** in the left sidebar.
2. In the protection specification of the target Anti-DDoS Advanced IP instance row, click after the elastic peak value .

3. In the set elastic protection pop-up, select the elastic protection peak value according to actual protection needs.

> **Note:**
> Because the peak value and fees of elastic protection are affected by different regions and versions, the actual peak value and fees of elastic protection are

> subject to the display in the console.

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

Renewing an Instance

Last updated: 2026-03-11 18:05:59

The expiration time of Anti-DDoS Pro/Anti-DDoS Advanced is approaching. Renew the Anti-DDoS Pro to enjoy continuous and stable Anti-DDoS Protection.

Prerequisites

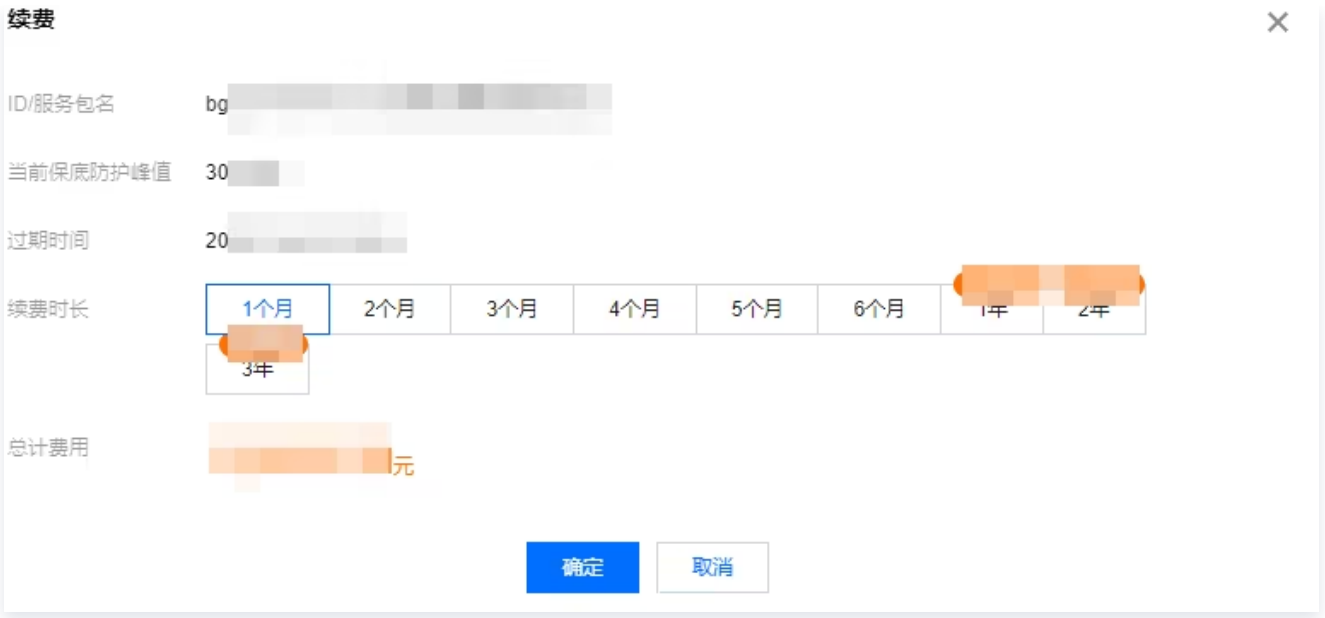
To set the protection object IP, you need to successfully purchase Anti-DDoS Pro package or Anti-DDoS Advanced IP.

Operation Steps

1. Log in to the Anti-DDoS (New Version) Console, and click on **Anti-DDoS Instances** in the left sidebar.
2. In the operation column on the right side of the row where the target Anti-DDoS Pro/high-protection IP instance is located, click **Renew**.

3. On the renewal page, select the renewal duration according to actual protection needs:
   - Anti-DDoS Pro: Renewal duration supports 3 months, 6 months, 1 year, 2 years, 3 years.

   - Anti-DDoS Advanced: Renewal duration supports 1 month, 2 months, 3 months, 4 months, 5 months, 6 months, 1 year, 2 years, 3 years.



4. Click **OK** to complete the payment process.

Deleting Instances

Last updated: 2025-03-19 21:40:46

When an instance is no longer in use, you can Contact Us to delete the instance.

Note:

- Once the read-write instance is deleted, the data cannot be retrieved.
- After the instance is deleted, the IP resources will be released simultaneously. Please confirm that no business is accessing the instance before deletion.

Unblock Protection IP

Last updated: 2025-03-19 21:40:58

Anti-DDoS provides the feature of unblocking for protected IPs that enter the blocked state. You can log in to the Anti-DDoS (New Version) Console to perform self-service unlocking operations.

Self-Service Unlocking Count

Users who use **DDoS Protection Pack** or **DDoS Protective IP** will have three chances of self-service unblocking every day. The system resets the chance counter daily at midnight. Unused chances cannot be accumulated for the next day.

Note:

- Before performing the unblock operation, it is recommended that you first check the estimated unblock time. The estimated unblock time may be delayed due to some factors. If you can accept the estimated time, no manual operation is required.
- When the self-service unlocking quota for the day is 0, it is recommended to increase the quantity of protection IPs and the frequency of protection to defend against large traffic attacks and avoid being continuously blocked.
- The unblock count for Anti-DDoS Pro (lightweight version) is three times per month.

Self-Service Unlocking Operation

1. Log in to the DDoS Protection (New Edition) Console, and click on **Unblocking Service** in the left sidebar.
2. On the unblocking operation page, find the protected IP with the status "Auto-unblocking", and click **Unblock**.

Unblocking Operation Records

1. Log in to the DDoS Protection (New Edition) Console, and select **Unblocking Service** > **Unblock Record** in the left sidebar.
2. On the unblock record page, filter by time range to view all unblocking operation records, including auto-unblocking, self-service unlocking, and other operation records.

Business Integration
Transparent IP Access

Last updated: 2026-03-11 18:03:36

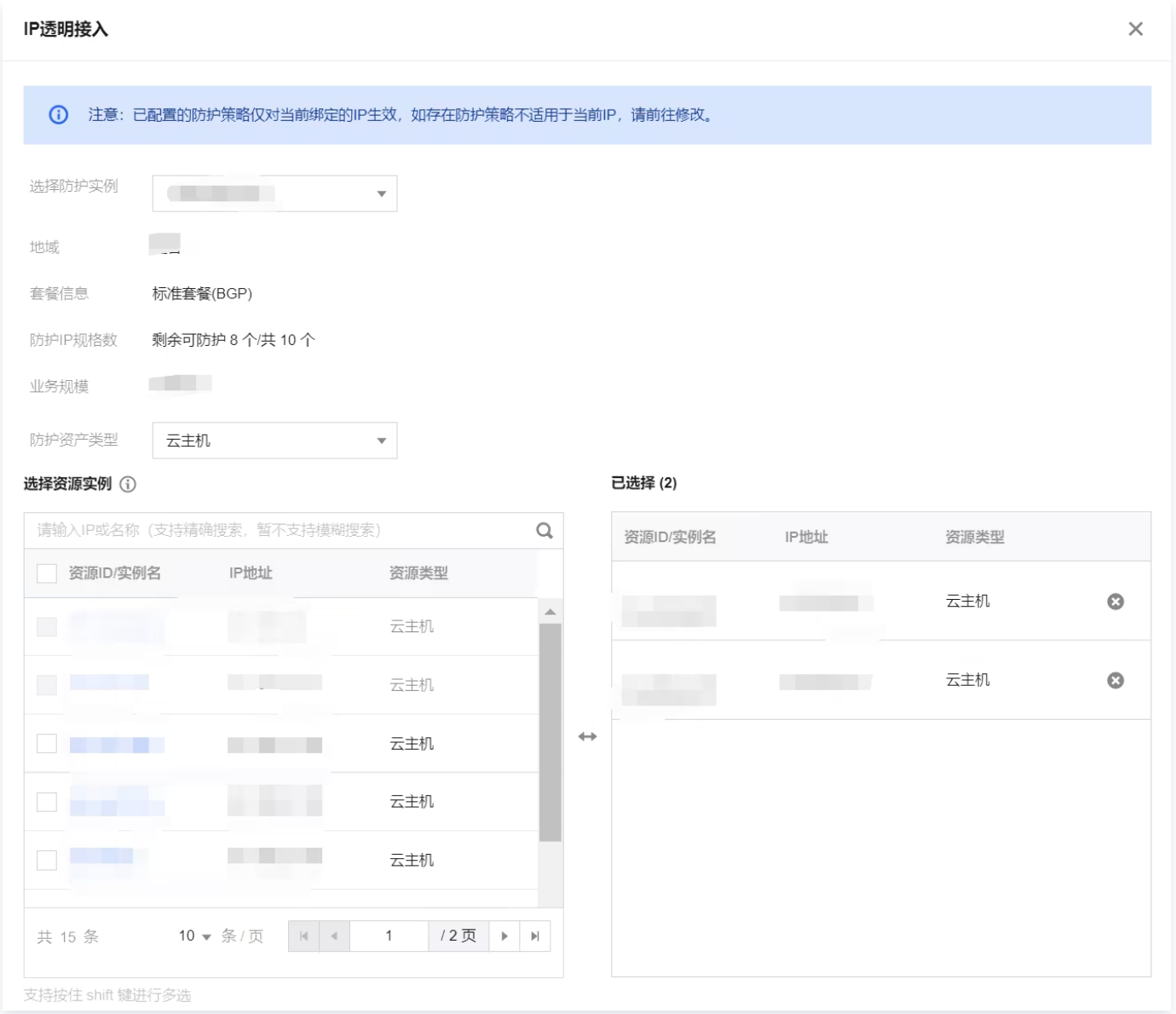
> **Note:**
> IP transparent access is an access method for directly binding cloud assets to DDoS high-protection packages, which allows connect with one click and has convenient configuration; if the instance you purchased is a DDoS high-protection package (enterprise edition), you need to go to the cvm console to unbind the original public IP and rebind EIP. If you need to hide the source station IP externally, please select port business or domain business access according to business needs through the form of high-protection IP.

Prerequisites

To set the protection object IP, you need to successfully purchase Anti-DDoS Pro.

Operation Steps

1. Log in to the DDoS Protection (New Edition) console, and in the left sidebar, click **Business Access** > **IP Transparent Access**.
2. On the IP Transparent Access page, click **Start Access**.
3. On the IP Transparent Access page, select a protection instance.



Note:

- If an IP is in blocking status for Anti-DDoS Pro, the user is not allowed to unbind the IP.
- When associating cloud assets, batch search and selection are supported.
- Currently, it supports detecting the Destroyed status of CLB and CVM products and performing unbinding.

4. Click **OK** to proceed.

Domain Integration

Last updated: 2025-03-19 21:41:29

> **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 three-network resources)

Access Rules

1. Log in to the Anti-DDoS (New Version) Console, and in the left sidebar, 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:**
> Multi-select is supported, allowing multiple instances to be integrated simultaneously.

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

5. Choose an origin-pull method, enter the origin server IP + Port or origin server domain name. If there is a backup origin server, select the backup origin server, add the backup origin server and its weight, and click **Next: Modifying DNS Resolution**.

> **Note:**
> Standby origin server: When the origin server forwarding has an exception, it will automatically switch to forward to the standby origin server.

6. Click **Complete**. The connected rules will appear in the domain access list. Check the access status to see if the connection is successful.

> **Note:**
> - When the configuration fails due to a certificate issue, a bubble reminder will appear on the right side of the access status saying "Failed to obtain the selected certificate. Please go to SSL Certificate Management for details."
> - When a domain name that has been successfully connected updates its certificate, there will be a momentary disconnection lasting for a few seconds. If

> you need to update the certificate, it is recommended to do so during the off-peek period.

Configure the Rules

1. On the domain access page, select the required rules and click **Configuration** in the operation column.

2. On the page of configuring layer-7 forwarding rules, you can modify related parameters and click **Yes** to save.

Delete Rule

1. On the domain access page, it supports deleting single or multiple rules in batches.
   - Single: Select the desired rule, click **Delete** in the operation column, and a pop-up window for deleting the rule will appear.

   - Batch: Select one or more rules, click **Batch Deletion**, and a pop-up window for deleting the rule will appear.

2. In the delete rule pop-up, click **Delete** to delete the selected rules.

IP Integration

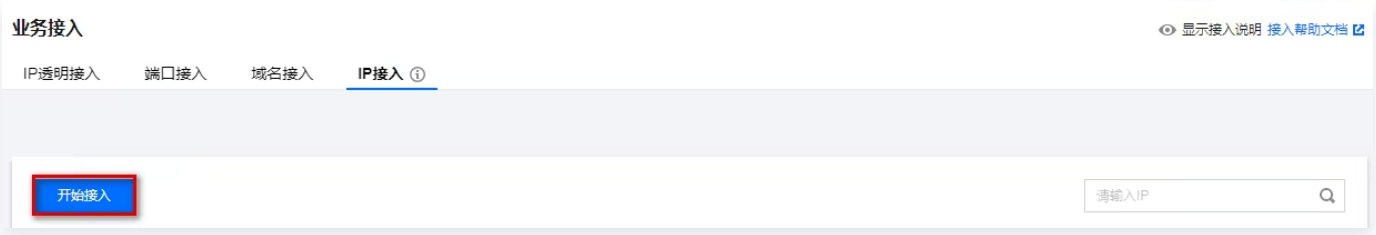
Last updated: 2025-03-19 21:41:40

Prerequisites

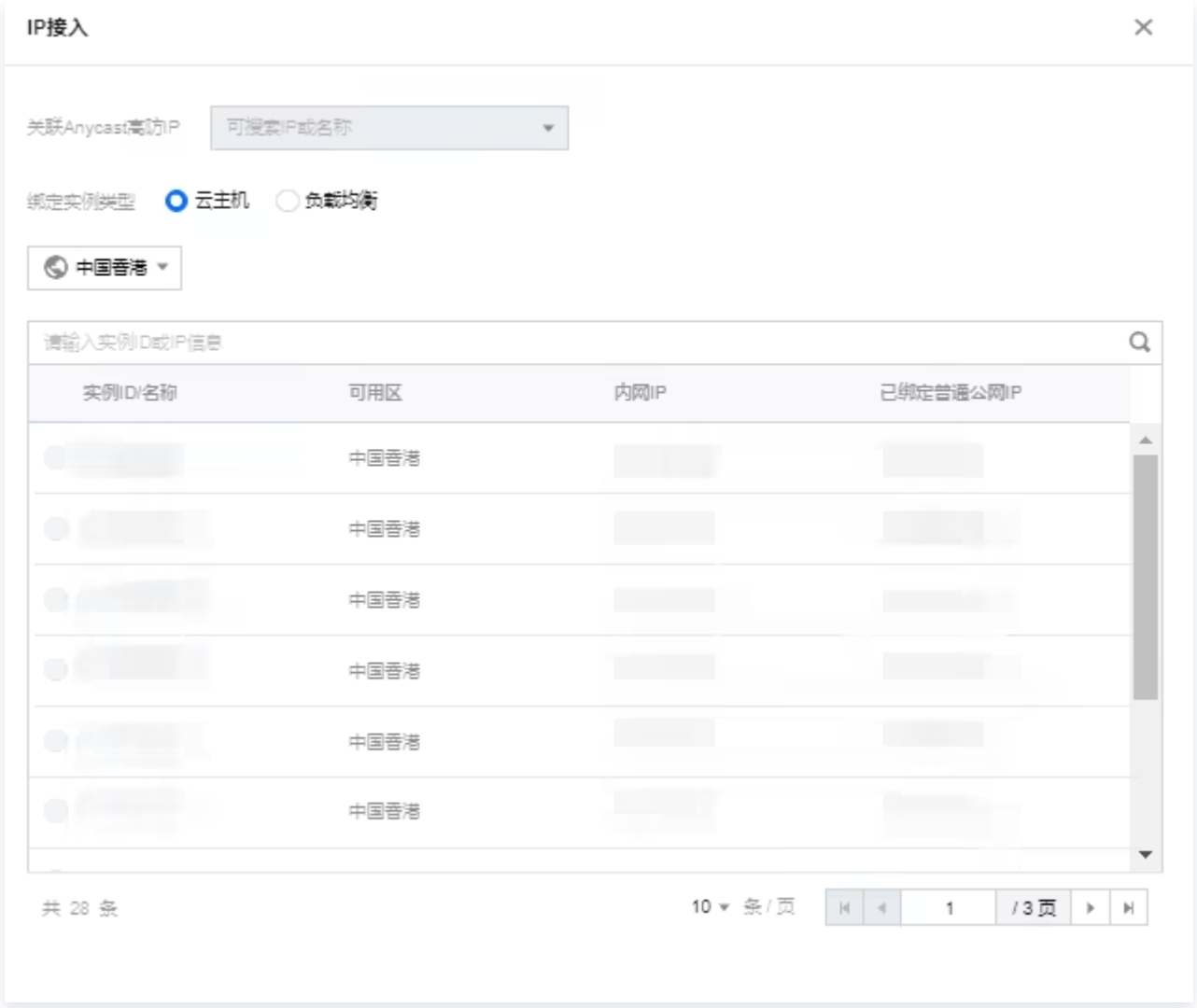
Before binding the protected IP, you need to successfully purchase Anti-DDoS Advanced (overseas enterprise version). If you need to purchase, please Contact Us.

Access Rule

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



3. On the IP Access page, select the associated Anycast High Defense IP.



Delete Rule

1. On the IP Access page, select the desired rule, click **Delete** in the operation column, and a pop-up dialog box for deleting the rule will appear.

2. In the pop-up dialog box for deleting the rule, click **Delete** to delete the selected rule.

Port Integration

Last updated: 2025-03-19 21:41:59

> **Note:**
> High-defense resources 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 three-network resources)

Integration Rule

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

3. On the Port Business Access page, select the associated instance ID, and click **Next: Protocol Port**.

> **Note:**
> Multi-select is supported, and multiple instances can be integrated at the same time.

4. Select a forwarding protocol, enter the forwarding port and origin server port, and click **Next: Origin-pull Method**.

5. Select an origin-pull method, enter the origin server IP + port or origin server domain name. If there is a backup origin server, you can select it, add the backup origin server and its weight, and click **Next: Modify DNS Resolution**.

Note:

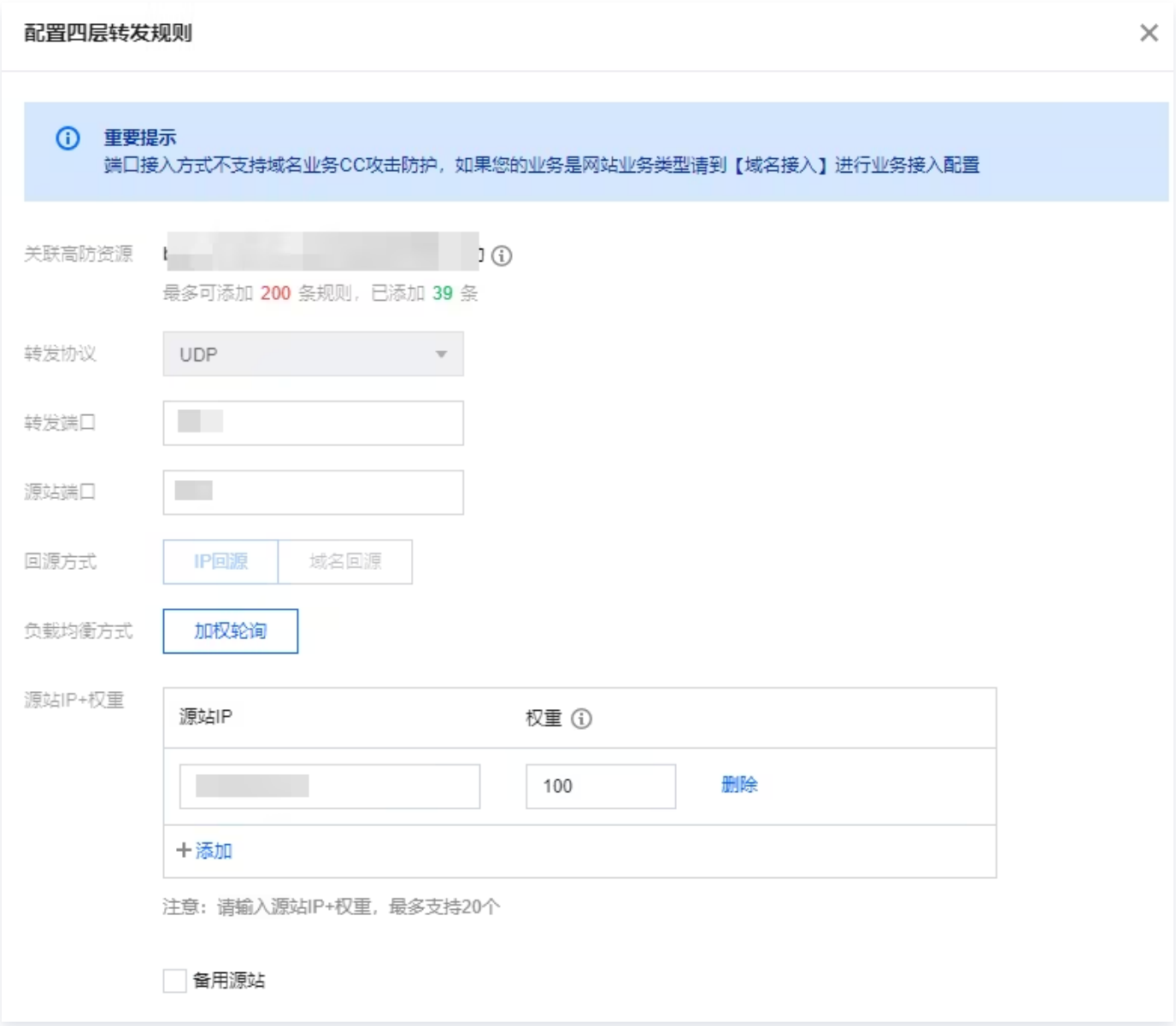
- Backup Origin Server: When the origin server forwarding encounters an exception, it will automatically switch to forward to the backup origin server.
- In the **second step of protocol port** for port business access. After entering the forwarding port, it will be determined whether this port under this high-defense IP resource has been occupied. If it is occupied, you cannot proceed to the next step.

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

Configure the Rules

1. On the Port Access page, select the required rule and click **Configuration** in the operation column.

2. On the Configure Layer-4 Forwarding Rule page, you can modify related parameters and click **OK** to save.



Query Rule

On the Port Access Page, click the search box to query rules by origin server IP/domain name, origin server port, associated Anti-DDoS Advanced instance, forwarding protocol, forwarding port, and associated Anti-DDoS resource (CNAME) keywords.

Delete Rule

1. On the Port Access page, you can delete single or multiple rules.
   - Single: Select the desired rule, click **Delete** in the operation column, and a pop-up window for deleting the rule will appear.

   - Batch: Select one or more rules, click batch delete, and a pop-up window for deleting the rule will appear.

2. In the delete rule pop-up, click **Delete** to delete the selected rule.

Configuring Session Persistence

Last updated: 2025-03-19 21:42:11

Anti-DDoS Advanced provides session persistence based on the ip address for non-website business protection, and supports forwarding requests from the same ip address to the same real server for processing.
In Layer 4 forwarding scenarios, simple session persistence is supported. The session persistence time can be set to any integer value between 30 seconds and 3600 seconds. If this time threshold is exceeded and there are no new requests in the session, the connection is automatically disconnected.

Operation Steps

1. Log in to the Anti-DDoS (New Version) Console, and in the left directory, click **Business Access** > **Port Access**.
2. On the Port Access tab, select the target Anti-DDoS Advanced IP instance and corresponding rule, click **Edit** under its session persistence column.

3. On the session persistence editing page, set the hold time, and click **OK**.

> **Note:**
> Session persistence is disabled by default. When setting the persistence time, it is recommended to use the default value.

Configuring Health Check

Last updated: 2025-03-19 21:42:24

Use Cases

Anti-DDoS Advanced IP uses health checks to help users automatically identify the running status of real servers and automatically isolate abnormal servers, thereby reducing the impact of backend server anomalies on overall business availability.

Layer-4 Business Health Check

The health check mechanism for Layer 4 business protection in Anti-DDoS IP is as follows: an Anti-DDoS cluster node initiates access requests to the server port specified in the configuration. If access to the port is normal, the real server is considered to be running normally; otherwise, it is considered to be running exceptionally.
Under the TCP protocol, check whether the port can be connected. Under the UDP protocol, use ping for reachability checks.

Layer-7 Business Health Check

The health check mechanism of Anti-DDoS Advanced Layer 7 business protection is that the anti-DDoS forwarding cluster sends HTTP requests to the real servers to check the backend services. The anti-DDoS system determines whether the service is normal based on the HTTP return status code.
Users can customize the status represented by response codes. Assuming in a certain scenario, the HTTP return values are http_1xx, http_2xx, http_3xx, http_4xx and http_5xx, users can check http_1xx and http_2xx as the normal service status according to business needs, then the values returned from http_3xx to http_5xx represent an abnormal status.

> **Note:**
> When configuring forwarding rules, if only one origin server IP is configured in a single rule, the health check feature will not be enabled. This feature is suitable for enabling when there are multiple origin server IPs.

Operation Steps

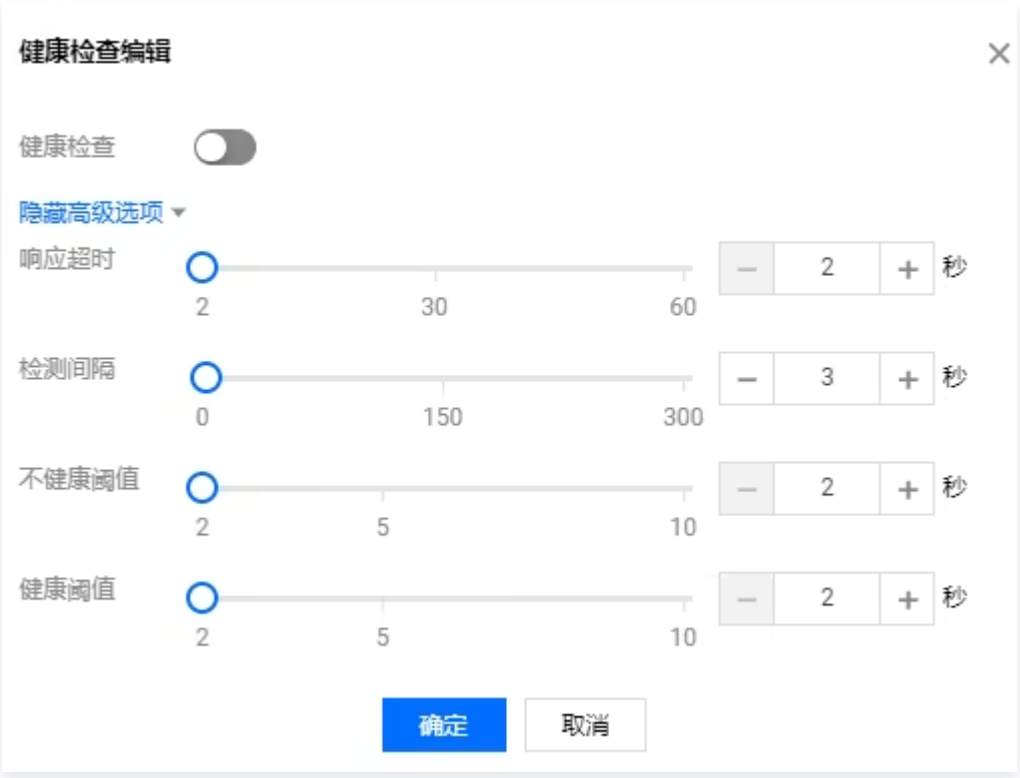
Layer-4 Business Health Check Configuration

1. Log in to the Anti-DDoS (New Version) Console, and click **Business Access** > **Port Access** in the left sidebar.

2. On the Port Access tab, select the target Anti-DDoS Advanced IP instance and corresponding rule, and click **Edit** under its health check column.

3. On the Health Check editing page, click **Show Advanced Options**, set the configuration items, and then click **Yes** to confirm.

> **Note:**
> - The health check is enabled by default. When configuring the health check, it is recommended to use the default value.
> - Under the TCP protocol, check whether the port can be connected. Under the UDP protocol, use ping for reachability check.



Layer-7 Business Health Check Configuration

1. Log in to the Anti-DDoS (New Version) Console, and click **Business Access** > **Domain Access** in the left sidebar.
2. On the Domain Access tab, select the target Anti-DDoS Advanced IP instance and corresponding rule, and click **Configuration** under its health check column.

3. On the health check editing page, click **Show Advanced Options**, set the configuration items, and then click **Yes** to confirm.

> **Note:**
> Health check is disabled by default.

Configuration Items Description

Layer 4 Health Check

Configuration	Description

Item	
Response timeout	The maximum timeout for each health check response. If the real server does not respond correctly within the specified time, it is considered a health check failure.
Check interval	The interval at which health checks are performed.
Unhealthy threshold	When the health check status is successful, if it receives a health check failure status for n consecutive times (n is the filled value), it is identified as unhealthy, and the console displays an exception.
Health threshold	When the health check status is a failure, if it receives a health check success status for n consecutive times (n is the filled value), it is identified as healthy, and there is no display on the console.

Layer-7 Health Check

Configuration Item	Description
Check interval	The interval at which health checks are performed is 15 seconds by default.
Unhealthy threshold	When the health check status is successful, if it receives a health check failure status for n consecutive times (n is the filled value), it is identified as unhealthy, and the console displays an exception.
Health threshold	When the health check status is a failure, if it receives a health check success status for n consecutive times (n is the filled value), it is identified as healthy, and there is no display on the console.
HTTP request method and inspection path URL	By default, the HEAD method is used, and the server only returns the response message header. If the GET method is used, the server returns the complete response message. The corresponding backend server needs to support HEAD and GET. • If the page used for health checks is not the default homepage of the application server, users need to specify the specific inspection path. • If the HTTP HEAD request limits the parameters of the host field, users need to specify the inspection path, that is, the URI used for the health check page file.
HTTP Status	The HTTP status codes for determining whether the health check is normal. By default or without any selection, the values are http_1xx,

Code Detection	http_2xx, http_3xx and http_4xx. If the HTTP return status code is not the default value, it is identified as unhealthy, and modification is supported.

Intelligent Scheduling

Last updated: 2026-03-11 17:56:57

Use Cases

Generally, each account may have multiple anti-DDoS instances, and each anti-DDoS instance has at least one Anti-DDoS line. Therefore, there may be multiple Anti-DDoS lines under each account. When you add a business to an anti-DDoS instance for protection, it means that you have configured an Anti-DDoS line as the protection route for the business. If your business configuration has multiple Anti-DDoS lines as protection routes, you need to consider the scheduling method of the business traffic, that is, how to schedule the business traffic to the optimal Anti-DDoS line for protection to ensure business access speed and high availability.
Currently, the Anti-DDoS service provides a priority-based CNAME intelligent scheduling feature. You can select the anti-DDoS instance and set the priority of the Anti-DDoS line according to actual needs.

Note:
- The anti-DDoS instances that support setting resolution include Anti-DDoS packages and Anti-DDoS IPs, where Anti-DDoS IPs comprise BGP protective IPs, China Telecom protective IPs, China Unicom protective IPs, and China Mobile protective IPs.
- Intelligent scheduling is not required if there is only one Anti-DDoS line.

Priority Scheduling Method

It means that all DNS requests are responded to by the Anti-DDoS line with the highest priority, that is, all access traffic is scheduled to the current Anti-DDoS line with the highest priority. You can edit the priority of the Anti-DDoS line. The default priority is 100. The smaller the value of the priority, the higher the priority of the Anti-DDoS line. The specific scheduling rules are as follows:

- If the anti-DDoS instance configured for the business includes multiple different Anti-DDoS lines with the same priority, it will respond according to the ISP source of the DNS request. When one of the Anti-DDoS lines is blocked, it will be scheduled in the order of BGP > telecommunications > China Unicom > mobile > outside Chinese mainland (including Hong Kong (China), Taiwan (China)).
- If all Anti-DDoS lines with the same priority are blocked, the access traffic will be automatically scheduled to the currently available Anti-DDoS line with the next highest priority.

> **Note:**
> If there is no available Anti-DDoS line with the second highest priority, automated scheduling cannot be performed, and business access will be interrupted.

- If the anti-DDoS instance configured for the business includes multiple identical Anti-DDoS lines with the same priority, it will be scheduled in a cloud load balancer manner, distributing the access traffic evenly to these identical ISP Anti-DDoS lines for processing.

Example

Suppose you have the following anti-DDoS instances: BGP protective IPs 1.1.1.1 and 1.1.1.2, protective IP 2.2.2.2 of China Telecom, and protective IP 3.3.3.3 of China Unicom. The priorities of 1.1.1.1, 2.2.2.2 and 3.3.3.3 are all 1, and the priority of 1.1.1.2 is 2. Under normal circumstances, all traffic is scheduled to a group of Anti-DDoS lines with a current priority of 1 for distribution and processing. Therefore, traffic from China Unicom is scheduled to 3.3.3.3 for processing, traffic from China Telecom is scheduled to 2.2.2.2 for processing, and traffic from other ISPs is scheduled to 1.1.1.1 for processing. When 1.1.1.1 is blocked, the access traffic under this IP will be automatically scheduled to 2.2.2.2 for processing. When both 1.1.1.1 and 3.3.3.3 are blocked, the access traffic originally scheduled to 1.1.1.1 and 3.3.3.3 will be distributed to 2.2.2.2 for processing. When all Anti-DDoS lines in this group are blocked, the traffic will be scheduled to 1.1.1.2 for processing.

Prerequisites

- Before enabling intelligent scheduling, please connect the business that needs protection to the anti-DDoS instance for protection.

> **Note:**
> - If you need to add the IP of the cloud product to be protected to the purchased high-protection package instance, see Anti-DDoS Pro Quick Start.
> - If you need to add Layer-4 or Layer-7 services to the purchased Anti-DDoS Advanced instance, see Anti-DDoS Advanced port access or domain access.

- Before modifying DNS resolution, you need to successfully purchase a DNS product, such as Tencent Cloud's DNS.

Set Route Priority

Please refer to the following steps and set the priorities for your anti-DDoS instances according to the imagined scheduling scheme:

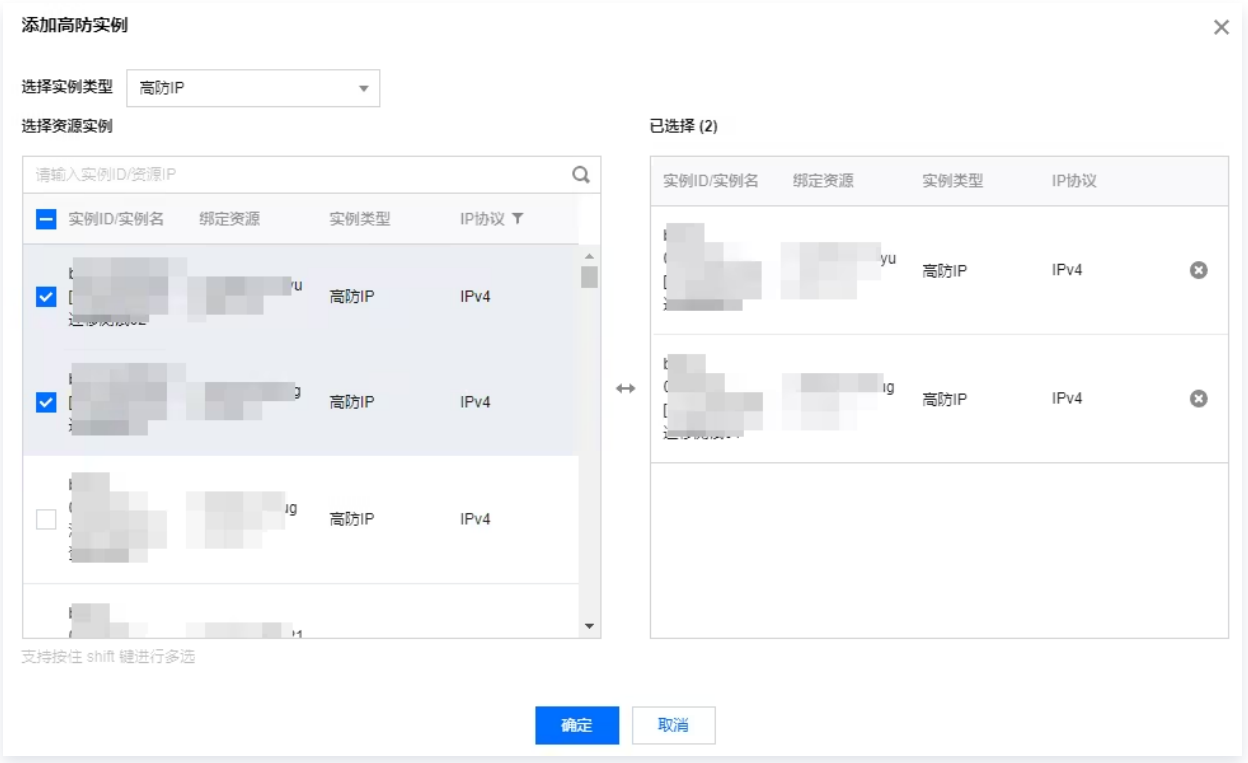
1. Log in to the Anti-DDoS (New Version) Console, and click on **Intelligent Scheduling** in the left sidebar.
2. On the Intelligent Scheduling page, click on **Create Scheduling Policy**, and the system will automatically generate a CNAME record.

3. On the Create Intelligent Scheduling page, the TTL value defaults to 60 seconds, with a range from 1 (second) to 3600 (seconds). The scheduling mode defaults to priority. Rollback time is the waiting time when multiple resources trigger the rollback process during linkage. Considering the unblock waiting time and avoiding frequent linkage switching, the minimum time is 10 minutes. The default recommended setting is 60 minutes.

4. On the Create Intelligent Scheduling page, there are two modes: Priority Mode and Directional Mode, with operations as follows:

4.1 Priority Mode: Set by priority (using numerical values), providing scheduling between resources.

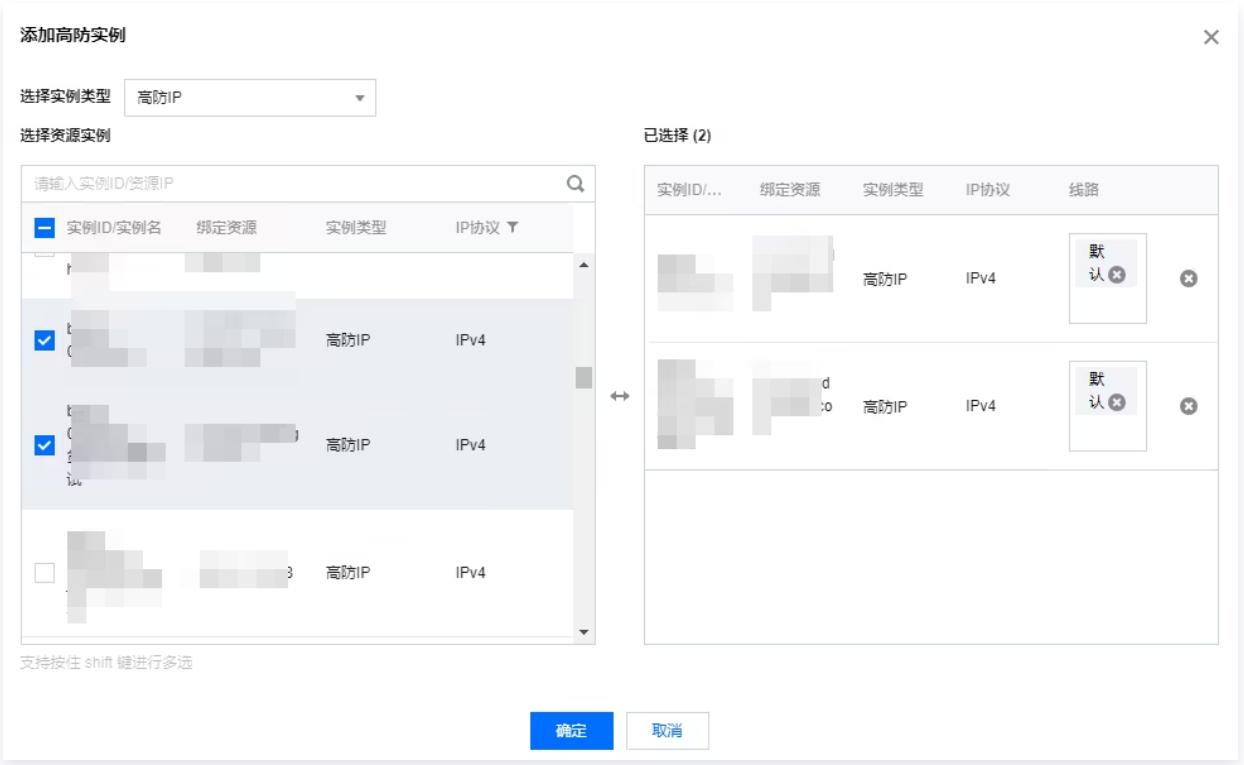
4.1.1 Click **Add Anti-DDoS Resource IP**, select the anti-DDoS instances and IPs that need intelligent scheduling, and click **OK**.



4.1.2 After selecting the high-defense IP instance, the domain resolution of the instance's high-defense line is enabled by default, and then set its priority.

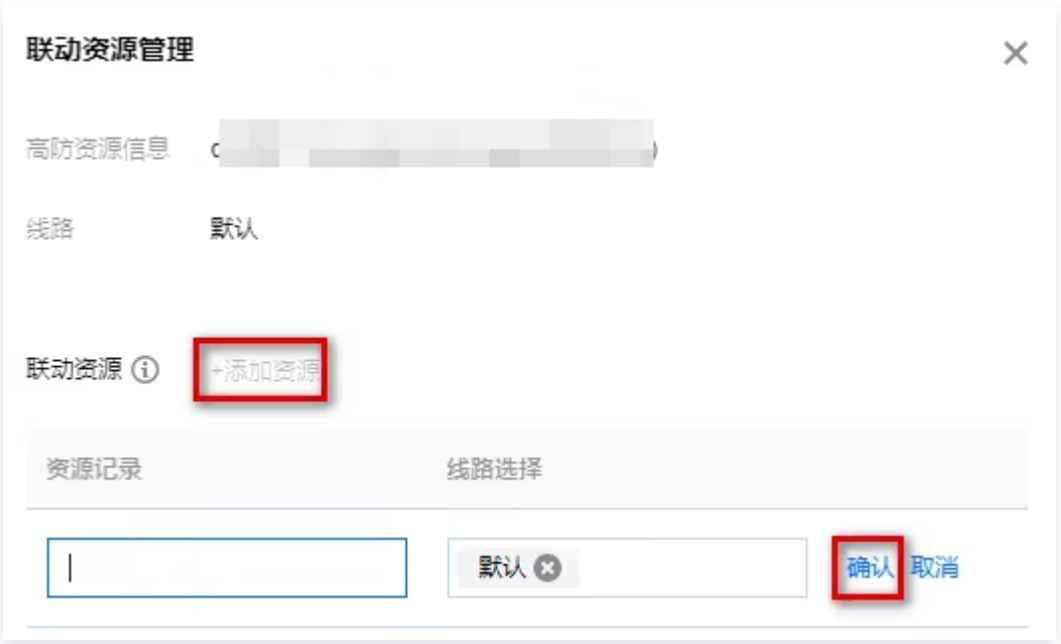
4.2 Directional Mode: Specify the scheduling relationship between resources through directional mode.

4.2.1 Click **Add Anti-DDoS Resource IP**, select the anti-DDoS instances and IPs that need intelligent scheduling, choose the required line, and click **OK**.



4.2.2 On the Create Intelligent Scheduling page, see the selected scheduling resources, click **Configure Linked Resources**.

4.2.3 On the linkage resource management page, click **Add Resource**, enter the linked IP, select the corresponding line, and click **OK** to configure the scheduling relationship between specified resources.



Example

For example, if you want to schedule business traffic to the BGP protective line first, when the BGP protective line is attacked and blocked, the traffic will be automatically scheduled to the China Telecom protective line. If the China Telecom protective line is also blocked, then the traffic will be scheduled to the China Unicom protective line. When the blockage of the BGP protective line is lifted, the traffic will automatically resume scheduling to the BGP protective line.
Priority setting method: You can set the priority of the anti-DDoS instance of the protection business that belongs to the BGP protective line to 1, set the priority of the China Telecom protective line to 2, and keep the priority of the China Unicom protective IP line unchanged to meet the above scheduling scheme.

资源ID	IP地址	线路	优先级	地区	运行状态	域名解析	操作
net-00000		联通	100	华东地区(上海)	运行中		解除绑定
bgpip-00000		电信	2	华东地区(上海)	运行中		解除绑定
bgp-00000		BGP	1	华东地区(上海)	运行中		解除绑定

If you do not want the China Unicom protective IP line to join the traffic scheduling mechanism for the time being, click to disable domain resolution, and then re-enable domain resolution and set the priority as needed later. If you want to remove this line from the current scheduling mechanism, you can directly find the row where the corresponding instance of this line is located and click to unbind.

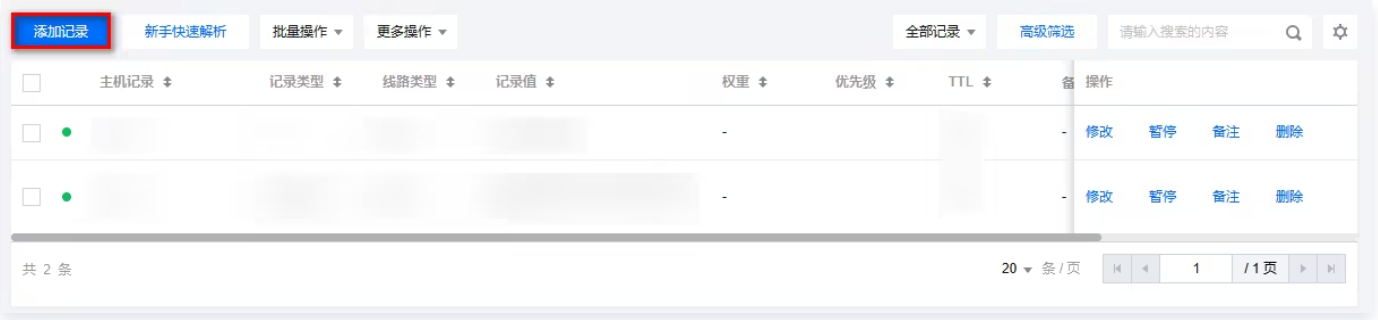
Modify DNS Resolution

Before using CNAME intelligent scheduling, it is recommended that you modify the CNAME record of the business domain DNS to the CNAME automatically generated by the Anti-DDoS intelligent scheduling system, so that all user access traffic to the business website is directed to the high-defense system.

1. Log in to Tencent Cloud DNS Console, and in the left navigation bar, click **My Resolution**.
2. On the My Resolution page, find the row of the target domain name and click **Resolution**.

3. Click **Add Record**, enter the domain name for which you want to add a record, select CNAME for the record type, enter the CNAME address generated by the smart scheduling system in the record value, and click **OK**.

> **Note:**
> Click **Batch Operation** > **Add Records in Batch** to add resolution records in batch.



Protection Configuration
Anti-DDoS Protection
Anti-DDoS Severity Level

Last updated: 2025-03-19 21:44:00

Use Cases

The Anti-DDoS service provides a feature to adjust protection policies, offering three protection levels for you to choose from against DDoS attacks. The specific protection operations for each level are as follows:

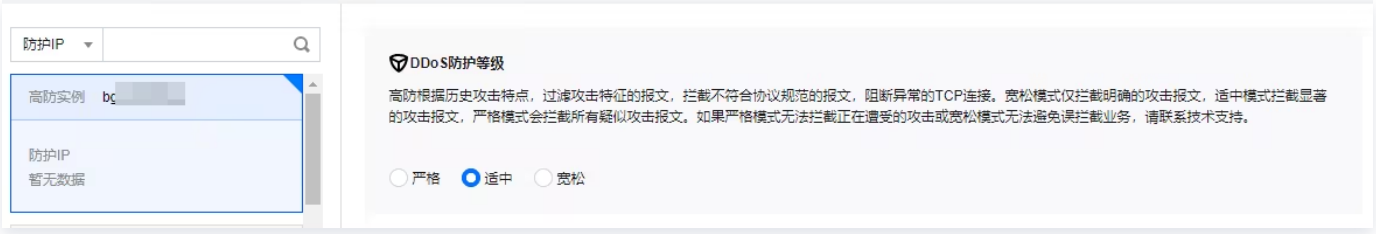
Protection Level	Protection Operations	Description
Relaxed	• Filter SYN and ACK packets with clear attack patterns. • Filter TCP, UDP, and ICMP packets that do not conform to protocol specifications. • Filter UDP packets with clear attack patterns.	• The cleaning policy is relatively lenient, only protecting against attack packets with clear attack patterns. • It is recommended to enable when false blocking is suspected, as there may be attack pass-through in case of complex attacks.
Moderate	• Filter SYN and ACK packets with clear attack patterns. • Filter TCP, UDP, and ICMP packets that do not conform to protocol specifications. • Filter UDP packets with clear attack patterns. • Filter common UDP-based attack packets. • Conduct active verification on some access source IPs.	• The cleaning policy adapts to the vast majority of businesses and can effectively protect against common attacks. • Default is moderate mode.

Strict	• Filter SYN and ACK packets with clear attack patterns. • Filter TCP, UDP, and ICMP packets that do not conform to protocol specifications. • Strictly check and filter UDP packets with clear attack features and UDP-based attack packets. • Conduct active verification on some access source IPs. • Filter ICMP attack packets.	The cleaning policy is relatively strict, and it is recommended to use it when attack pass-through occurs in normal mode.

Note:
Takes effect when the protected IP is under attack.

Operation Steps

1. Log in to the Anti-DDoS (New Version) console, and click on **Anti-DDoS** in the left sidebar.
2. In the left list of the Anti-DDoS page, select the ID of the Anti-DDoS package/IP, such as "bgp-00xxxxxx".



3. In the Anti-DDoS severity card, set the severity level as needed.

IP Blocklist and Allowlist

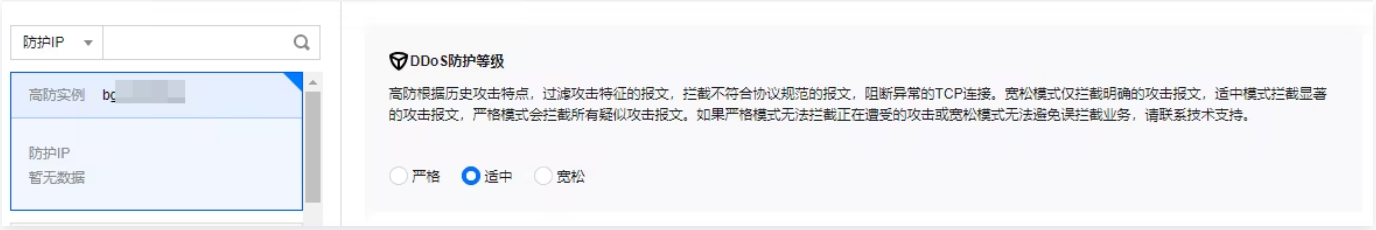
Last updated: 2025-03-19 21:44:13

DDoS high defense supports blocking or allowing source IPs accessing DDoS high defense by configuring IP blocklists and allowlists, thereby restricting users accessing your business resources. After configuring IP blocklists and allowlists, when an IP in the allowlist accesses, it will be directly allowed without being filtered by any protection policies. When an IP in the blocklist accesses, it will be directly blocked.

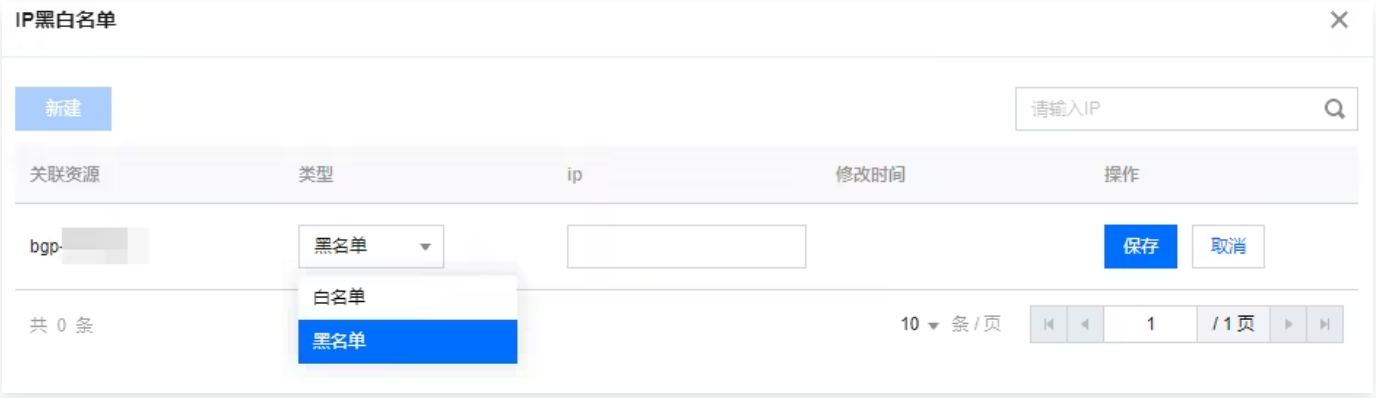
> **Note:**
> Takes effect when the protected IP is under attack.

Operation Steps

1. Log in to the Anti-DDoS (New Version) Console, and click **Anti-DDoS** in the left sidebar.
2. In the list on the left of the DDoS Protection page, select the ID of Anti-DDoS Pro/anti-DDoS IP, such as "bgp-00xxxxxx".



3. In the IP Blocklist and Allowlist card, click **Settings** to enter the IP Blocklist and Allowlist page.
4. On the IP Blocklist and Allowlist page, click **Create**, select the type of blocklist or allowlist, fill in the relevant fields, and click **Save**.



5. After the creation is completed, a new IP blocklist and allowlist rule will be added to the IP Blocklist and Allowlist list. You can click **Delete** in the right operation column to delete the

IP blocklist and allowlist rule.

Port Filtering

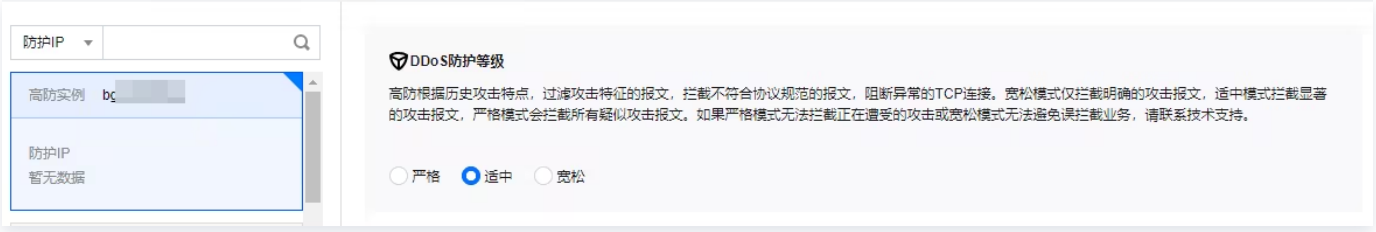
Last updated: 2025-03-19 21:44:26

DDoS high defense supports one - click banning or allowing the source traffic accessing DDoS high defense based on ports. After enabling port filtering, you can customize the combination of protocol type, source port range and destination port range according to needs, and set the protection policy actions of discarding, allowing and continuing for the matched rules. Port filtering can accurately formulate port - setting protection policies for the accessed source traffic.

> **Note:**
> Takes effect when the protected IP is under attack.

Operation Steps

1. Log in to the Anti-DDoS (New Version) Console, and click on **Anti-DDoS** in the left sidebar.
2. In the list on the left of the DDoS Protection page, select the ID of the Anti-DDoS Pro/Anti-DDoS IP, such as "bgp-00xxxxxx".



3. In the port filtering card, click **Settings** to enter the port filtering page.
4. On the port filtering page, click **Creation** to create a port filtering rule. Select different protection actions and fill in relevant fields as needed, then click **Save**.

> **Note:**
> Supports selecting multiple instance resources for batch creation. Instances that are not bound to a protection resource are not allowed to create rules.

5. After the creation is complete, a new port filtering rule will be added to the port filtering list. You can click **Configuration** in the operation column on the right to modify the port filtering rule.

Protocol Ban

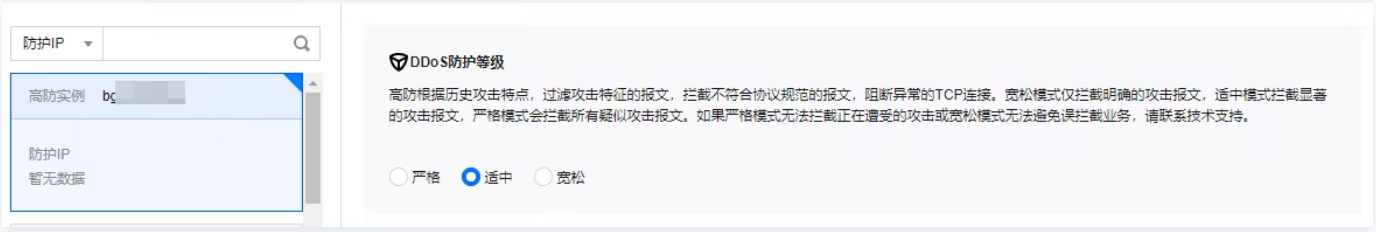
Last updated: 2025-03-19 21:44:39

DDoS high defense supports one - click banning of source traffic accessing DDoS high defense according to protocol type. You can configure ICMP protocol ban, TCP protocol ban, UDP protocol ban and other protocol bans. After the configuration is completed, when attack traffic is detected to have relevant access requests, it will be directly intercepted.
Due to the connectionlessness of the UDP protocol (for example, TCP has a three - way handshake process), it has natural security flaws. If you don't have UDP services, it is recommended to ban the UDP protocol.

> **Note:**
> Takes effect when the protected IP is under attack.

Operation Steps

1. Log in to the Anti-DDoS (New Version) Console, and click on **Anti-DDoS** in the left sidebar.
2. In the list on the left of the DDoS Protection page, select the ID of Anti-DDoS Pro/anti-DDoS IP, such as "bgp-00xxxxxx".



3. In the protocol blocking card, click on **Settings** to enter the protocol blocking page.
4. On the protocol blocking page, click on  to modify the protocol blocking rule switch.

Watermark Protection

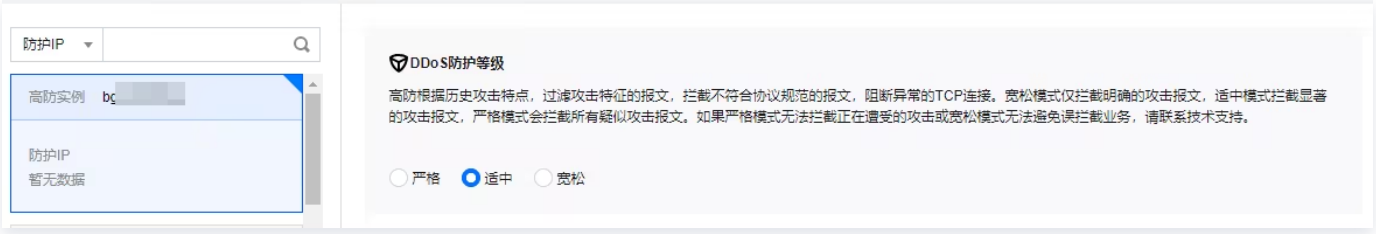
Last updated: 2025-03-19 21:44:51

DDoS high defense supports adding watermark protection to messages sent by the business end. Within the range of UDP and TCP message ports you configure, the business end and DDoS protection end share the watermark algorithm and key. After the configuration is completed, each message sent by the client is embedded with watermark features, while attack messages have no watermark features. This can distinguish attack messages and discard them. By accessing watermark protection, it can efficiently and comprehensively protect against layer-4 CC attacks, such as simulate service message attacks and replay attacks.

> **Note:**
> Takes effect when the protected IP is under attack.

Operation Steps

1. Log in to the Anti-DDoS (New Edition) console, and click on **Anti-DDoS** in the left sidebar.
2. In the list on the left of the DDoS Protection page, select the ID of Anti-DDoS Pro/anti-DDoS IP, such as "bgp-00xxxxxx".



3. In the watermark protection card, click on **Settings** to enter the watermark protection page.
4. On the watermark protection page, click on **Create**, fill in the relevant fields, and click on **Confirm** to create a watermark protection rule.

5. After the creation is completed, a new watermark protection rule will be added to the watermark protection list. You can click on **Configure Key** in the right operation column to view and configure the key.

6. On the Configure Key interface, the user can view or copy the key, and supports adding or deleting keys. Only when there are two keys can one key be deleted. There can be at most two watermark keys.

Connection Attack Protection

Last updated: 2025-03-19 21:45:03

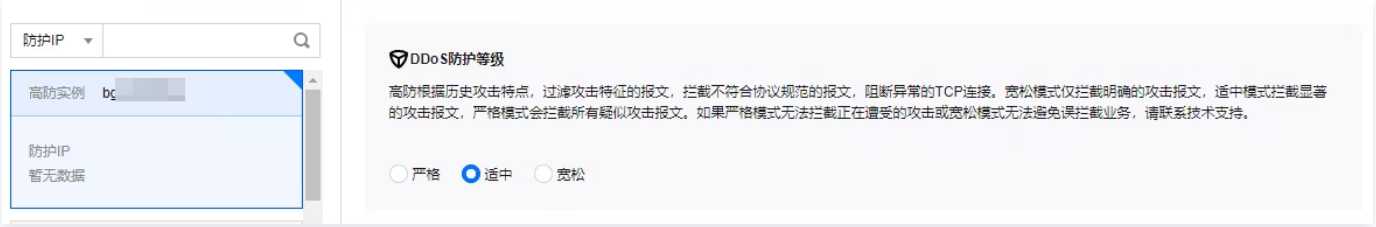
When a connection exception occurs, DDoS high defense supports automatic initiation of a punishment policy for blocking. After the maximum number of exceptional connections from the source IP is enabled for protection, if DDoS high defense detects that the same source IP frequently initiates a large number of messages in an exceptional connection state within a short period of time, it will include the source IP in the blocklist for blocking punishment. The blocking time is 15 minutes, and access can be restored after the blocking time has passed.

Note:

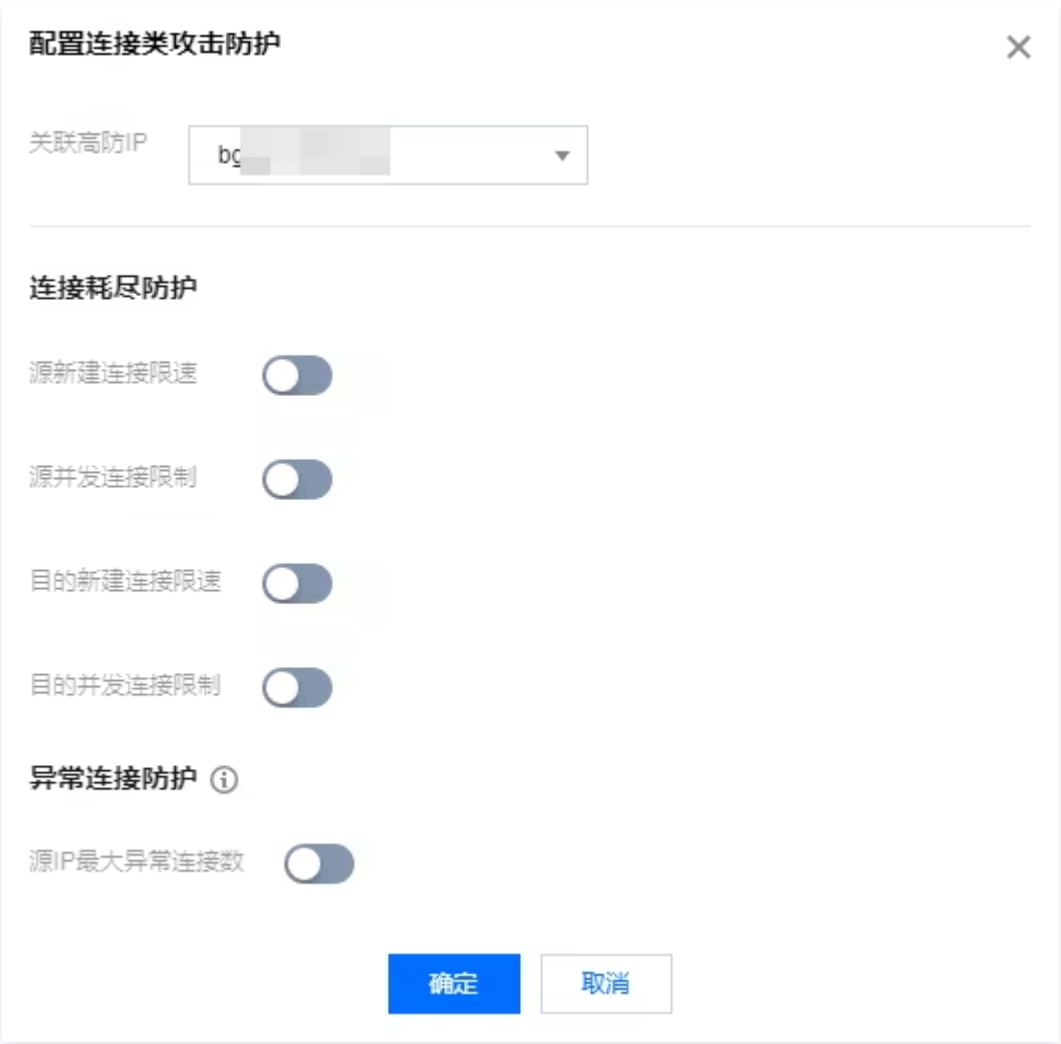
- The customized edition of the lightweight application server (Lighthouse) does not support custom protection configuration for DDoS protection.
- Link-type attack protection supports the following fields:
  - Source create connection rate limiting: Limit the frequency of creating new connections based on the source address port.
  - Source concurrent connection limit: The number of active TCP connections of the access source reaches the limit at a certain moment.
  - Target create connection rate limiting: Limit the frequency of creating new connections for the target IP address port.
  - Target concurrent connection limit: The number of active TCP connections to the target IP address reaches the limit at a certain moment.
  - Maximum number of abnormal connections for source IP: The maximum number of abnormal connections supported by the access source IP.
- Takes effect when the protected IP is under attack.

Operation Steps

1. Log in to the Anti-DDoS (New Version) console, and click **Anti-DDoS** in the left sidebar.
2. In the list on the left of the DDoS Protection page, select the ID of Anti-DDoS Pro/anti-DDoS IP, such as "bgp-00xxxxxx".



3. In the connection attack protection card, click **Settings** to enter the connection attack protection page.
4. On the connection attack protection page, click **Create**, enable connection flood protection and abnormal connection protection, and click **Confirm**.



5. After the creation is completed, a new connection attack protection rule will be added to the connection attack protection list. You can click **Configure** in the right operation column to modify the abnormal connection rule.

AI Protection

Last updated: 2025-03-19 21:45:14

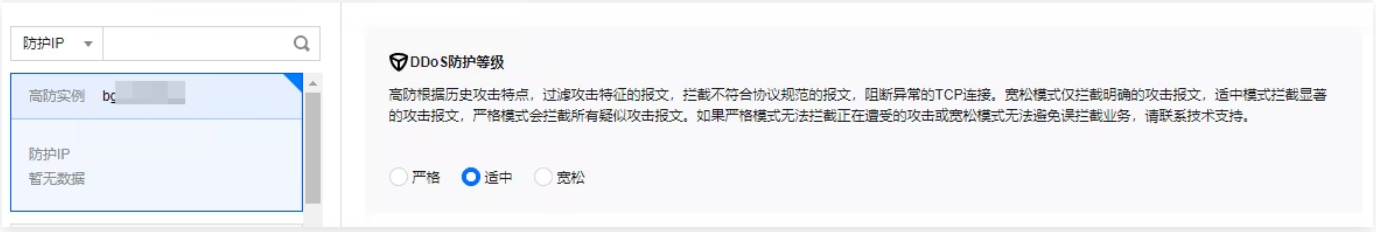
DDoS high defense supports intelligent AI protection feature. After enabling AI protection, DDoS high defense will autonomously learn the connection baseline and traffic characteristics through the algorithm, adaptively adjust the cleaning strategy, detect and block layer-4 CC attacks, providing the best defense effect.

Note:

- Anti-DDoS Pro (lightweight version) does not support custom protection configuration for Anti-DDoS and CC protection.
- It takes effect when the protected IP is under attack.

Operation Steps

1. Log in to the Anti-DDoS (New Version) Console, and click on **Anti-DDoS** in the left sidebar.
2. In the list on the left of the DDoS Protection page, select the ID of Anti-DDoS Pro/anti-DDoS IP, such as "bgp-00xxxxxx".



3. In the AI protection card, click to turn on the AI protection switch.

Regional Block

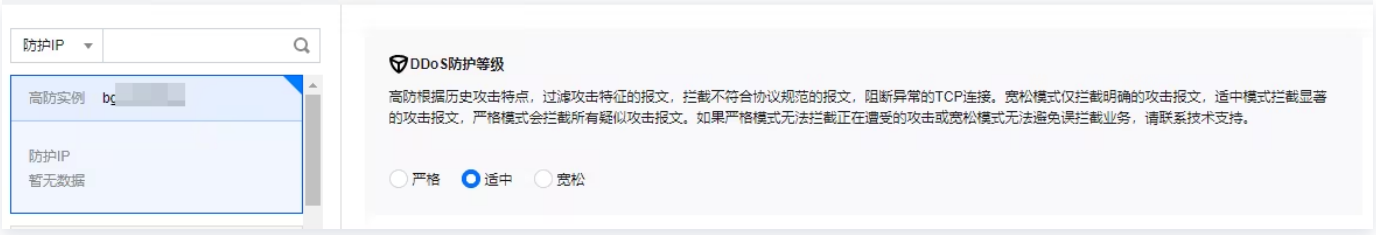
Last updated: 2025-03-19 21:45:25

DDoS high defense supports one-click blocking of source traffic accessing DDoS high defense according to the geographic area of the source IP at the cleaning node. Supports regional and national traffic blocking.

> **Note:**
> Takes effect when the protected IP is under attack.

Operation Steps

1. Log in to the Anti-DDoS (New Version) Console, and click on **Anti-DDoS** in the left sidebar.
2. In the list on the left of the DDoS Protection page, select the ID of Anti-DDoS Pro/anti-DDoS IP, such as "bgp-00xxxxxx".



3. On the regional block card, click **Settings** to enter the regional block page.
4. On the regional block page, click **Create**, select the blocked region, and click **Confirm** to create a regional block rule.

5. After the creation is completed, a new regional block rule will be added to the regional block list. You can click **Configure** in the right operation column to modify the regional block rule.

IP Port Rate Limiting

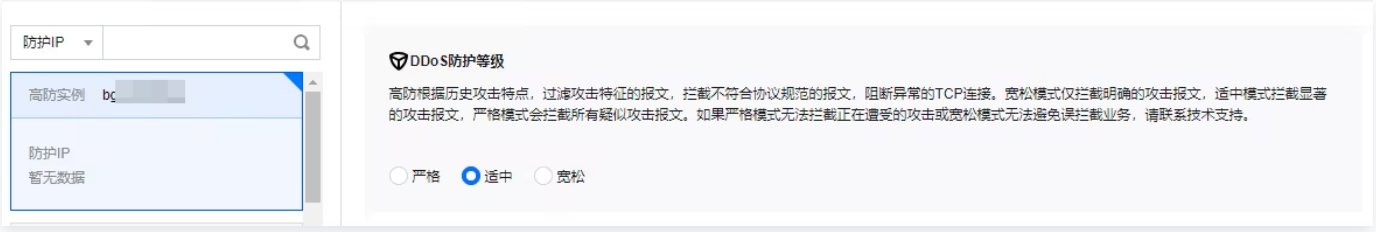
Last updated: 2025-03-19 21:45:38

Anti-DDoS provides support for traffic access throttling based on the dimension of IP + port for business IPs.

> **Note:**
> Takes effect when the protected IP is under attack.

Operation Steps

1. Log in to the Anti-DDoS (New Version) Console, and click **Anti-DDoS** in the left sidebar.
2. In the list on the left of the DDoS Protection page, select the ID of the Anti-DDoS Pro/Anti-DDoS IP, such as "bgp-00xxxxxx".



3. In the IP Port Speed Limit card, click **Settings** to enter the IP Port Speed Limit page.
4. On the IP Port Speed Limit page, click **Create** to pop up the Create IP Port Speed Limit window.

5. In the Create IP Port Speed Limit window, select the required protocol, port and speed limit mode, enter the speed limit threshold, and click **Yes** to create an IP port speed limit rule.

6. After the creation is completed, a new IP port speed limit rule will be added to the IP port speed limit list. You can click **Settings** in the operation column on the right to modify the IP port speed limit rule.

Feature Filtering

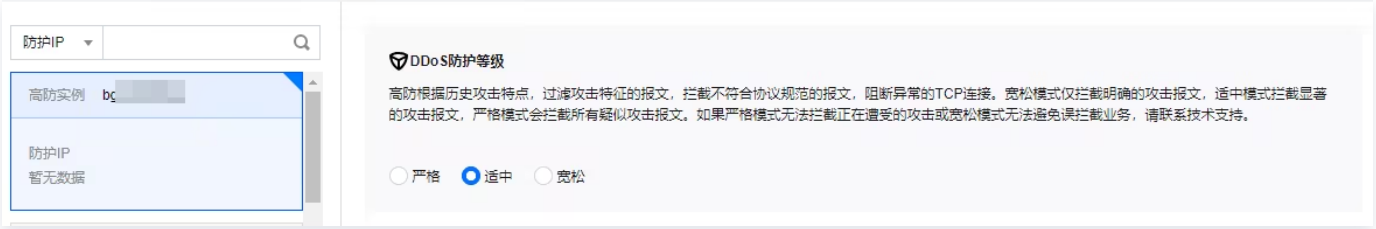
Last updated: 2025-03-19 21:45:50

DDoS high defense supports custom interception policies based on features in IP, TCP, UDP message headers or payloads. After feature filtering is enabled, you can combine match conditions such as source port, destination port, message length, IP message header or payload, and set policy actions such as pass, drop, drop and blocklist for 15 minutes, continue protection, etc. for requests that hit the conditions. Feature filtering can accurately formulate protection policies for business message features or attack message features.

> **Note:**
> Takes effect when the protected IP is under attack.

Operation Steps

1. Log in to the Anti-DDoS (New Version) Console, and click on **Anti-DDoS** in the left sidebar.
2. In the list on the left of the DDoS Protection page, select the ID of Anti-DDoS Pro/anti-DDoS IP, such as "bgp-00xxxxxx".



3. In the feature filtering card, click on **Settings** to enter the feature filtering page.
4. On the feature filtering page, click on **Create** to pop up the create feature filtering window.

5. In the create feature filtering window, create a feature filtering rule, select different protection actions and fill in related fields according to your needs, and click on **Yes**.

6. After creation, a new feature filtering rule will be added to the feature filtering list. You can click on **Configuration** in the operation column on the right to modify the feature filtering rule.

CC Protection
CC Protection Switch and Threshold Clearing

Last updated: 2025-03-19 21:46:03

Protection Description

CC protection determines malicious behavior based on access characteristics and connection status to block hacker attacks. Different protection policies can be configured according to different attack scenarios to ensure business stability. The threshold clearing is the threshold for the high-defense product to initiate the cleansing action.

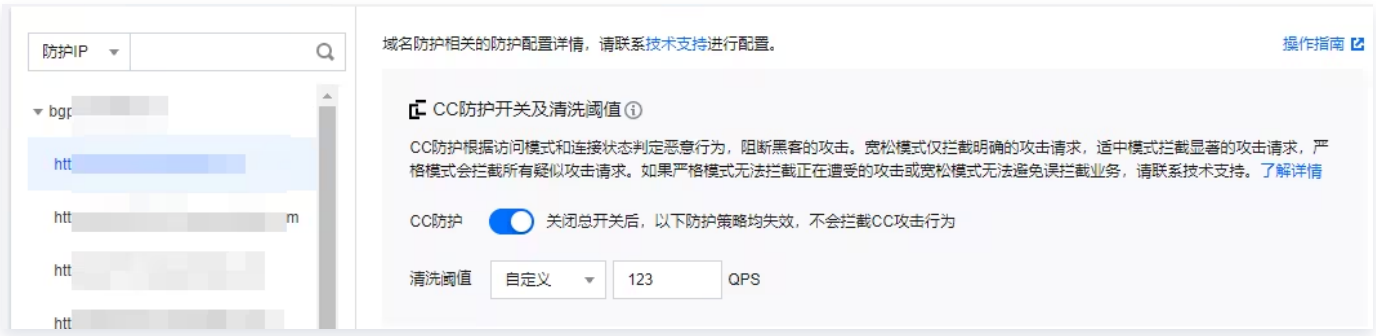
> **Note:**
> Takes effect when the protected IP is under attack.

Prerequisites

1. You need to have successfully purchased Anti-DDoS Advanced and set the protection object.
2. CC protection currently only supports the enforcement of rules for domain name integration.

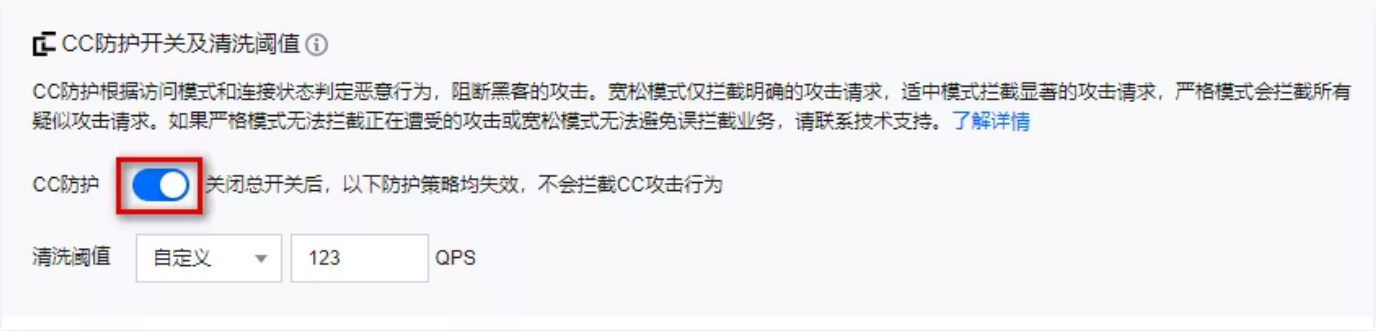
Operation Steps

1. Log in to the Anti-DDoS (New Version) console, and click CC protection in the left sidebar.
2. In the left list of the CC protection page, select the domain name under the ID of the high-protection IP.



3. In the right CC protection switch and threshold-clearing card, click to enable CC protection. After the protection is enabled, you must set the threshold-clearing; otherwise,

CC protection cannot be activated.



> **Note:**
> The CC protection switch is the main switch to control whether to enable CC protection. Only after it is turned on can the protection policies below take effect.

4. The threshold-clearing is the threshold for the high-protection product to initiate the cleaning action. When the accessed domain receives HTTP requests exceeding the threshold-clearing, CC protection is triggered. After CC protection is enabled, the threshold-clearing of the business instance adopts the default value (recommended). As the accessed business traffic changes, the Anti-DDoS system will automatically learn and generate a set of exclusive default thresholds based on the AI algorithm. At the same time, you can also customize the threshold-clearing according to actual business conditions.

> **Note:**
> - The customized specific threshold can be set to 1.5 times the normal business peak.
> - The smaller the customized threshold, the stricter the detection requirement.
> - When the threshold clearing is lower than the default value, there may be false termination. When the threshold clearing is higher than the default value, there may be transparent transmission. It is recommended to enable the default threshold clearing.

Intelligent CC Protection

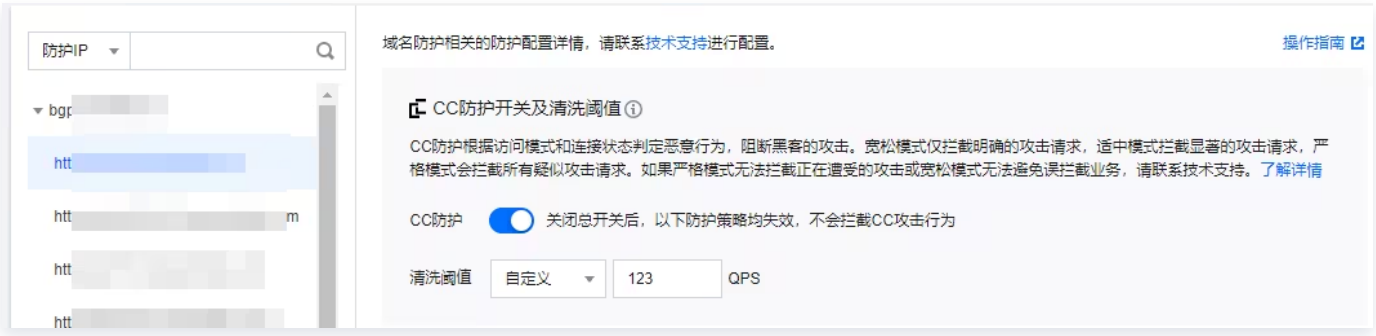
Last updated: 2025-03-19 21:46:15

After enabling intelligent protection, AI intelligent protection leverages Tencent Cloud's big data capabilities to self-learn the website business traffic baseline, analyze attack anomalies with algorithms, and automatically issue precise protection rules to dynamically adjust the business protection model, helping you timely detect and block malicious attacks.

> **Note:**
> Takes effect when the protected IP is under attack.

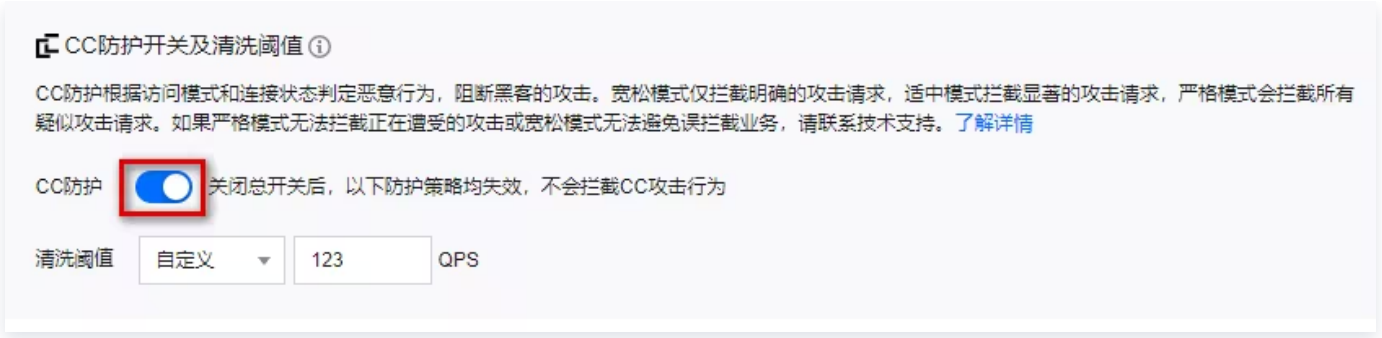
Operation Steps

1. Log in to the Anti-DDoS (New Version) Console, and click CC Protection in the left sidebar.
2. In the left list of the CC Protection page, select the domain name under the ID of the high-protection IP.



3. In the CC Protection switch and threshold-clearing card, click to turn on the CC Protection switch. Once the protection is enabled, you must set the threshold-clearing; otherwise, intelligent CC Protection cannot be used.

> **Note:**
> - The threshold clearing is the threshold for the anti-DDoS product to initiate the cleansing action. When the HTTP requests received by the specified domain exceed the threshold, CC protection will be triggered.
> - When the IP of the Anti-DDoS Pro is the same as the IP of the "Web Application Firewall", you need to go to Web Application Firewall Console to enable CC protection for this IP first. For details, see CC Protection Rule Settings.



4. In the intelligent CC Protection card, click  to enable intelligent protection.

5. Click **View** to see the intelligently generated protection rules. If adjustments are needed, click **View** on the right to edit the intelligent protection rules.

> **Note:**
> - After enabling intelligent CC protection, protection rules are automatically generated based on each attack.
> - Protection mode: The rules issued under intelligent protection have a single valid period. After a single attack ends, the protection rules automatically become invalid and are cleared.
> - Observation mode: Only the rule display is generated and it does not take effect.

6. Intelligent protection rules are automatically generated and take effect based on a single attack. The rules issued under intelligent protection have a single valid period. After a single attack ends, the protection rules automatically become invalid and are cleared. According to protection needs, you can click **delete** to remove the corresponding protection rules.

Precise Protection

Last updated: 2025-03-19 21:46:27

Use Cases

Anti-DDoS IP supports precise protection policies for connected web applications. With precise access control enabled, you can configure protection policies that combine conditions based on common HTTP fields, such as URI, UA, Cookie, Referer, and Accept, to filter access requests. For requests that meet the conditions, you can set up CAPTCHA verification or policies to drop or allow the requests. Precise protection supports customized protection policies for various business scenarios, enabling precise and targeted CC defense.

> **Note:**
> Takes effect when the protected IP is under attack.

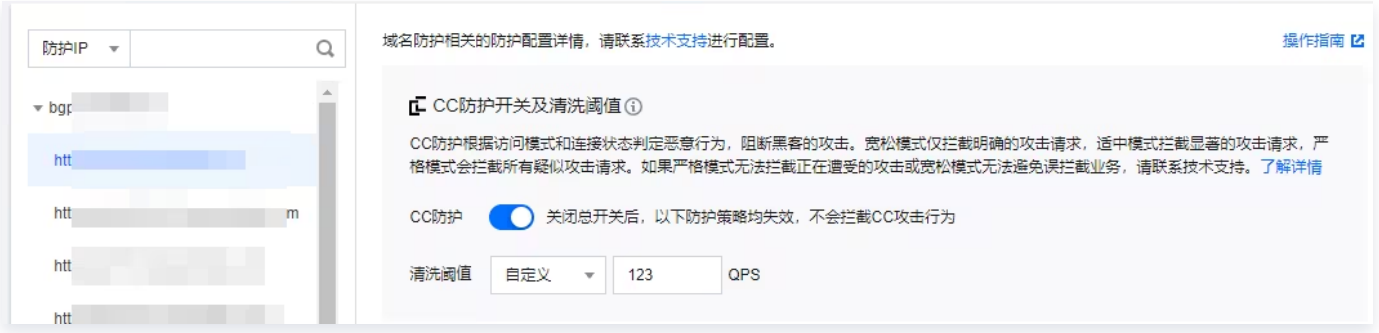
Match conditions define the request features to be identified, specifically referring to the attribute features of HTTP fields in access requests. The precise protection rules support the following matched HTTP fields as shown in the table below.

Match Fields	Field Description	Applicable Logic
URI	Match the URI of the request. For example: /example.html • Ignore case • Exclude Hostname • Exclude query parameters	Equal, include, exclude
URL	Match the URL of the request. For example: /example.html?region=cn • Ignore case • Exclude Hostname • Include URL query parameters	Equal, include, exclude
Path	Match the path part of the request URL. For example: /example.html or /api/v2/login • Ignore case • Exclude Hostname • Exclude query parameters	Equal, include, exclude

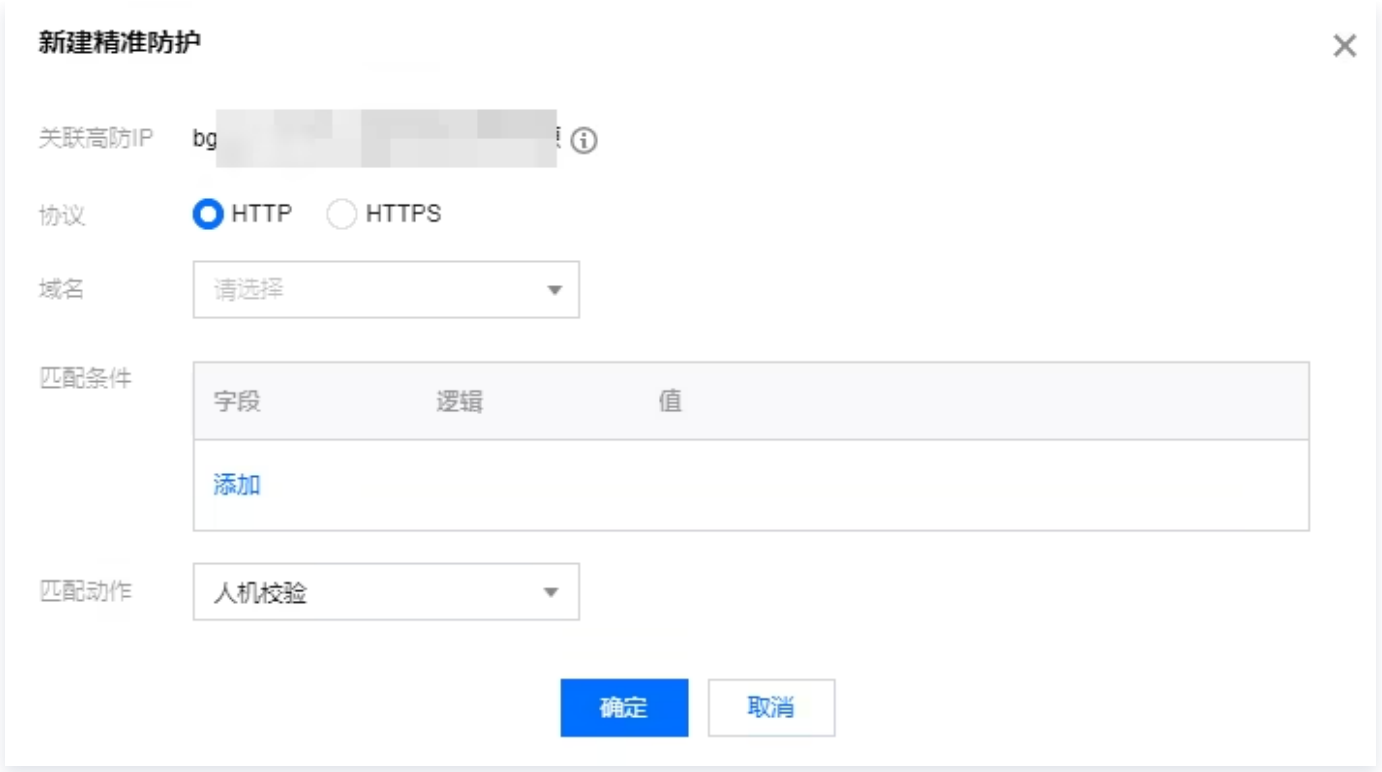
UA	Information related to the client browser identification that initiates the access request	Equal, include, exclude
Cookie	Match the specified request Cookie header parameter value, and the Cookie parameter name needs to be specified. • Ignore case	Equal, include, exclude
Referer	The source website of the access request, that is, which page jump generates this access request	Equal, include, exclude
Accept	The data type that the client initiating the access request expects to receive	Equal, include, exclude
Srcip	The source website of the access request	Equal, not equal to

Operation Steps

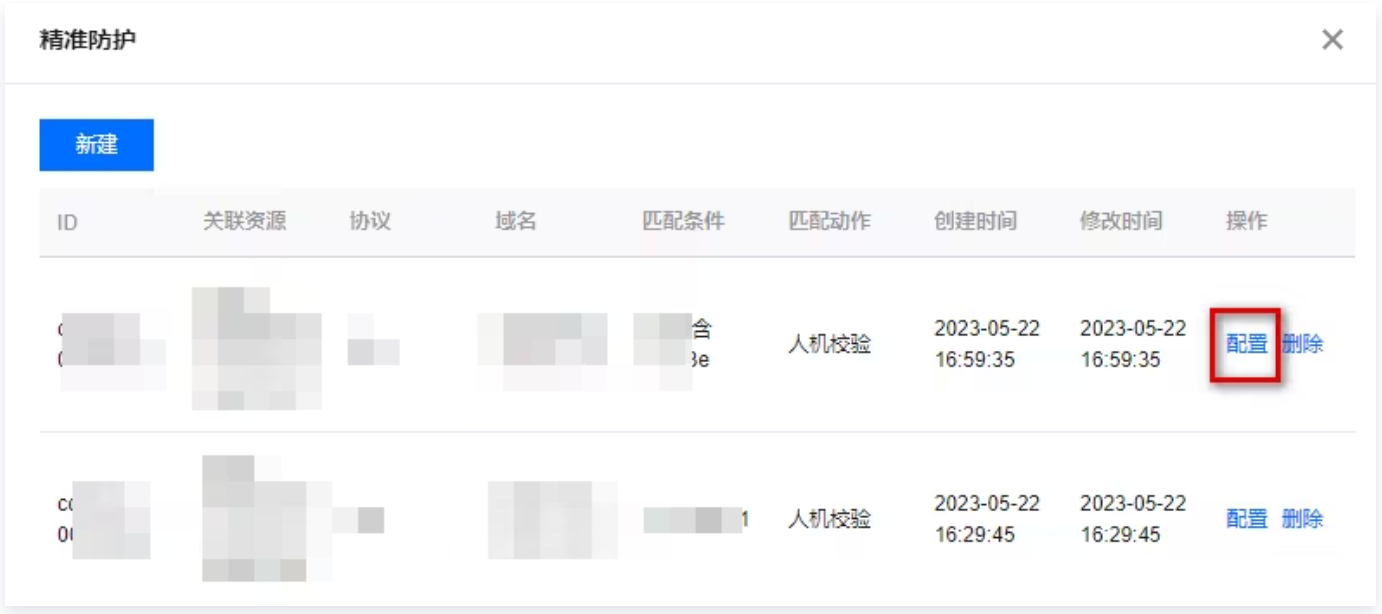
1. Log in to the Anti-DDoS (New Version) Console, and click on CC Protection in the left sidebar.
2. In the left list of the CC protection page, select the domain name under the ID of the high-defense IP.



3. In the precise protection card, click **Settings** to enter the precise protection page.
4. On the precise protection page, click **Create** to create a precise protection rule, fill in the relevant fields, and after completion, click **Yes**.



5. After the creation is completed, a new precise protection rule will be added to the precise protection list. You can click **Configuration** in the operation column on the right to modify the precise protection rule.



CC Frequency Limit

Last updated: 2025-03-19 21:46:39

DDoS High Defense IP provides CC frequency limit protection policies for connected web services, supporting the restriction of source IP access frequency. Once frequency control protection is enabled, it takes effect automatically, defaulting to a super lenient protection mode. Frequency control protection offers multiple protection modes for you to adjust according to different scenarios. You can also customize frequency limiting rules, so when a single source IP accesses a certain page too frequently in a short time, CAPTCHA will be set or a discard policy will be adopted.

> **Note:**
> Takes effect when the protected IP is under attack.

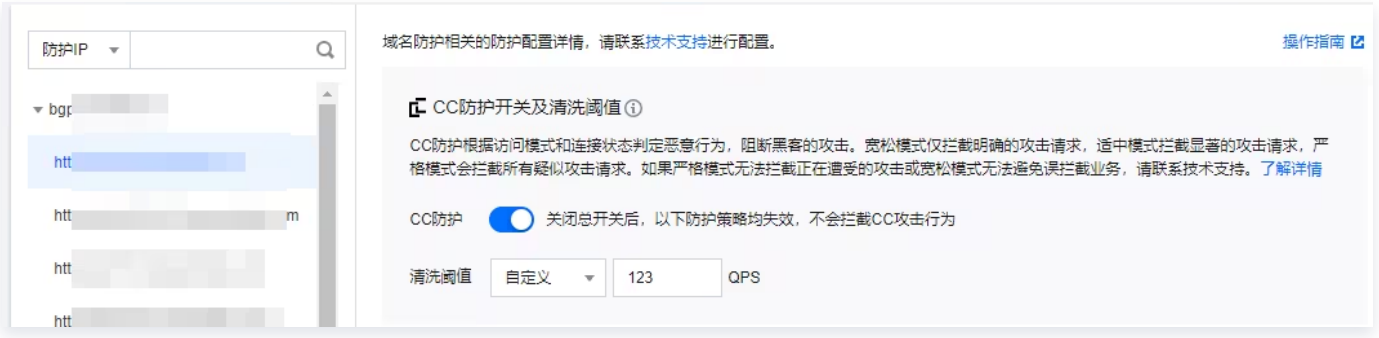
Frequency control protection provides different protection modes, allowing you to adjust the frequency control policy according to the real-time traffic exception of the website, specifically including the following modes.

Grading Classification	Description
Loose level	The CC protection policy at this level is relatively loose, and there may be a risk of a small number of exceptional requests passing through. Note: When an attack occurs, you can switch the protection level for protection. You can also configure a custom CC frequency limiting policy for protection.
Moderate level	The human-machine verification algorithm will be initiated, and visitors are allowed to access the origin server only after passing the algorithm verification. Note: This protection level is only applicable to web site services and not applicable to API/APP services. If it is an API/APP service, please configure a custom CC frequency limiting policy for protection. Attack emergency: When the access traffic to the origin server suddenly increases, causing the server load to be too high or the response to be abnormal, you can choose this level for protection.
Strict level	Human-machine identification verification will be carried out for every visitor across the network, and the verification algorithm will be upgraded at the

	same time, making the authentication process stricter, which may result in some false positives. Note: This protection level is only applicable to web site services and not applicable to API/APP services. If it is an API/APP service, please configure a custom CC frequency limiting policy for protection.
Attack emergency	When the access traffic to the origin server suddenly increases, causing the server load to be too high or the response to be abnormal, you can choose this level for protection.
Custom	Protection is carried out based on the set custom frequency control rules, and access frequency limitation is implemented for traffic whose features meet the conditions set by the frequency control rules.

Operation Steps

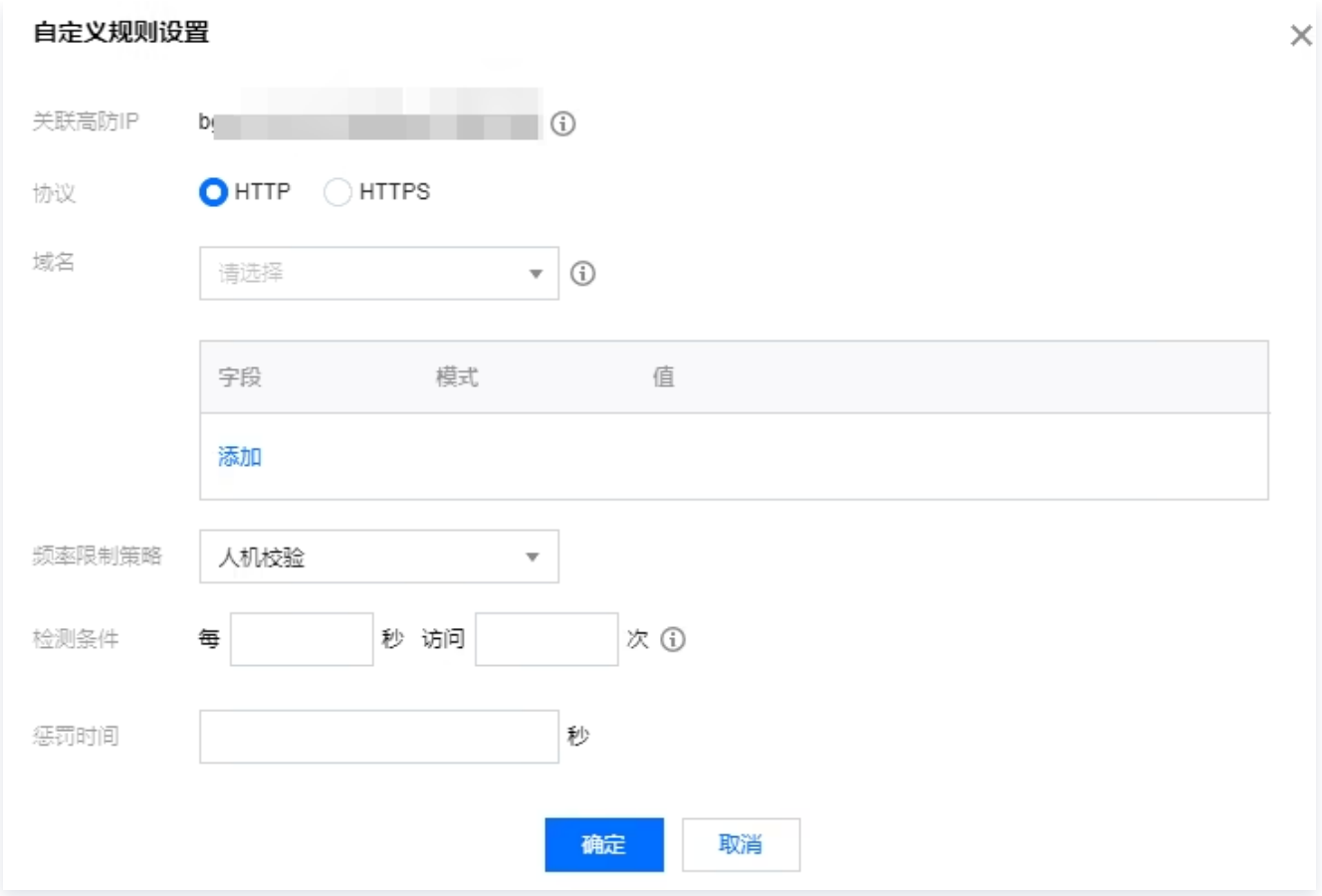
1. Log in to the Anti-DDoS (New Version) Console, and click **CC Protection** in the left sidebar.
2. In the left list of the CC Protection page, select the domain name under the ID of the high-protection IP.



3. In the CC Frequency Limit card, click  to enable the CC Frequency Limit feature, select the protection level that meets your business needs, and click **Settings** to enter the CC Frequency Limit list.

4. In the CC Frequency Limit rule list, all rules under the domain name are displayed by default. Click **Add Rule** to create a frequency limit rule and fill in the relevant fields.

> **Note:**
> - When no rules are created, the customized level cannot be enabled.
> - After optimization, there is no need to add the default rule; frequency control speed limits for subdomains are also supported.



5. After completing the creation, a new CC Frequency Limit rule will be added to the CC Frequency Limit list. You can click **Configuration** in the right operation column to modify the CC Frequency Limit rule.

Regional Ban

Last updated: 2025-03-19 21:46:50

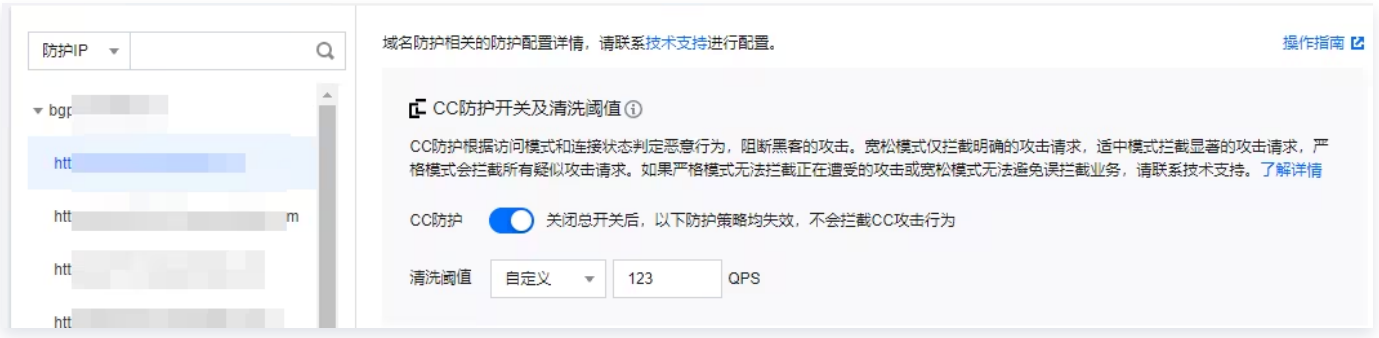
Anti-DDoS Advanced supports setting access request blocking policies based on geographic regions for website businesses that have been connected to protection. After enabling the regional blocking feature for domain names, you can block all access requests from specified regional source IPs to website businesses with one click. Supports traffic blocking in multiple regions and countries.

Note:

- After configuring regional blocking, attack traffic in that region will still be counted and recorded by the platform, but will not flow into the business origin server.
- Takes effect when the protected IP is under attack.

Operation Steps

1. Log in to the Anti-DDoS (New Version) console, and click **CC protection** in the left sidebar.
2. In the left list of the CC protection page, select the domain name under the ID of the high-protection IP.



3. In the region block card, click **Settings** to enter the region block page.
4. On the region block page, click **Create**, select IP, Protocol, domain name and the blocked region, and click **Yes** to create a region block rule.

5. After the creation is completed, a new region block rule will be added to the region block list. You can click **Configuration** in the operation column on the right to modify the region block rule.

IP Blocklist and Allowlist

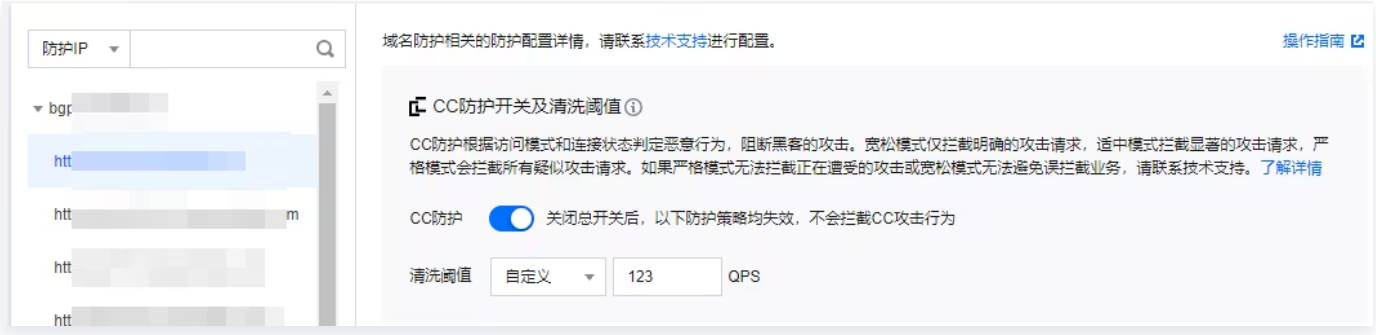
Last updated: 2025-03-19 21:47:01

Anti-DDoS Advanced supports configuring IP blocklists and allowlists to ban or allow access to websites protected by Anti-DDoS Advanced, thereby restricting users who access your business resources. After configuring the IP blocklist and allowlist, when an IP in the allowlist accesses, it will be directly allowed without any protection policy filtering. When an IP in the blocklist accesses, it will be directly blocked.

Note:
The filtering of IP allowlist and blocklist takes effect only when a CC Attack occurs.
- IPs in the allowlist will be directly allowed when accessing, without passing through any protection policy filtering.
- IPs in the blocklist will be directly blocked when accessing.
- Takes effect when the protected IP is under attack.

Operation Steps

1. Log in to the Anti-DDoS (New Version) Console, and click **CC Protection** in the left sidebar.
2. In the left list of the CC Protection page, select the domain name under the ID of the high-protection IP.



3. In the IP Blocklist and Allowlist card, click **Settings** to enter the IP Blocklist and Allowlist page.
4. On the IP Blocklist and Allowlist page, click **Create**, fill in the relevant fields, and after completion, click **Save**.

5. After creation, a new IP Blocklist and Allowlist rule will be added to the list. You can click **Delete** in the right operation column to delete the IP Blocklist and Allowlist rule.

Security Operations
Attack Analysis

Last updated: 2025-03-19 21:47:16

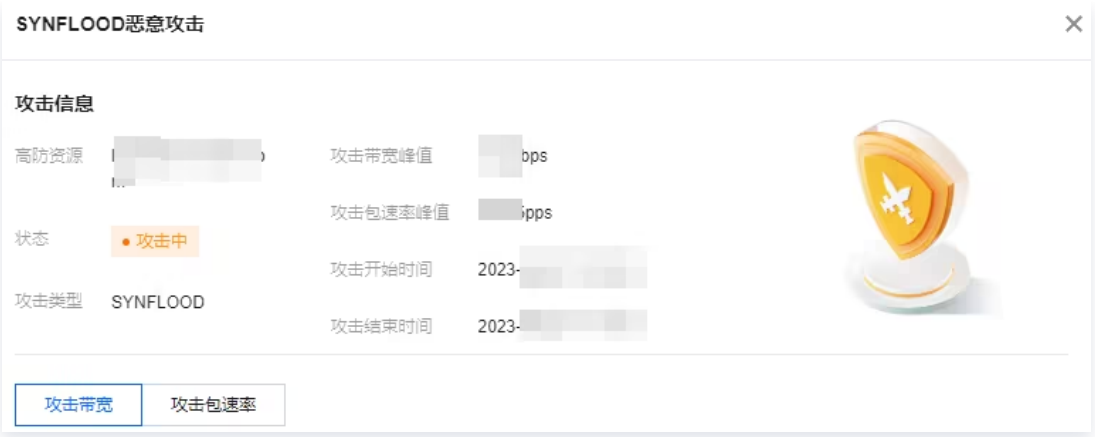
Viewing Attack Overview Statistics

1. Log in to the Anti-DDoS (New Version) Console, and click on **Attack Analysis** in the left sidebar.
2. In the attack overview statistics module, you can view the total number of attacks on the current business, total blocking times, attacks in progress, blocks in progress, peak attack bandwidth, and peak attack request value. On the right, you can view the attack trend for 7 days/30 days.

Viewing Recent Security Events

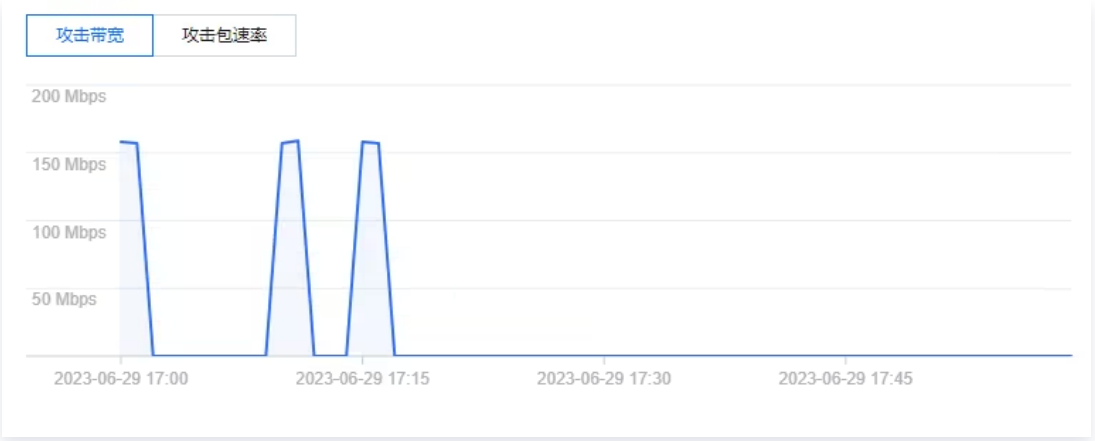
1. On the event details page, you can display the details of this attack as comprehensively as possible through asset ID/IP address, mainly including attack source name, attacked asset, IP address, attack time, duration, peak value, protection instance ID, protection type, and attack status.

2. In the attack information module on the event details page, view the attack situation of the IP within this time range, including attacked IP, status, attack type (sampling data), peak attack bandwidth, peak attack packet rate, start time, end time, and basic information.



3. In the attack trend module on the event details page, you can view the trend of network attack traffic bandwidth or attack packet rate. When an attack occurs, the peak of the attack traffic can be clearly seen in the traffic trend chart.

> **Note:**
> The data here is the full real-time data during this attack time period.



4. In the attack statistics module on the event details page, you can view the distribution of attacks under the two data dimensions of attack traffic protocol distribution and attack type distribution.

> **Note:**
> The data here is the attack sampling data within this attack time period, not full data.

Field Description:

- Attack Traffic Protocol Distribution: View the proportion of total attack traffic for each protocol in the attack events suffered by the selected high-protection package instance within this time range.
- Attack Type Distribution: View the proportion of the total number of each attack type suffered by the selected high-protection package instance within this time range.

5. In the "TOP5 Display" module on the event details page, you can view the top 5 attack source IPs and top 5 attack source regions to accurately grasp the detailed situation of the attack sources, which is convenient for formulating precise protection strategies.

> **Note:**
> The data here is the attack sampling data within this attack time period, not full data.

6. In the attack source information module on the event details page, you can view the sampled data of the attack details within this attack period to display the details of this attack as comprehensively as possible, mainly including attack source IP, region, cumulative attack traffic, and cumulative attack packet volume.

> **Note:**
> The data here is the attack sampling data within this attack time period, not full data.


攻击源信息

攻击源IP	地区	累计攻击流量	累计攻击包量
[redacted]	[redacted]	638.9 KB	1331
[redacted]	[redacted]	690.7 KB	1439
[redacted]	[redacted]	489.6 KB	1020

Business Analysis

Last updated: 2025-03-19 21:47:28

Anti-DDoS supports viewing logs within the past 90 days, including the number of protection days, connected businesses, and attacked businesses. If necessary, you can search by instance ID.

Operation Steps

1. Log in to the Anti-DDoS (New Version) Console, and click on **Business Analysis** in the left sidebar.
2. On the Business Analysis page, click on **Immediate Processing**.

3. On the Protection Pending page, the following operations are supported:
   - Click **Unblock** to jump to the unblock center.

   - Click **Upgrade Protection** to enter the upgrade page, and select "IP Quantity" and "Protection Times" according to actual protection needs.

Operation Log

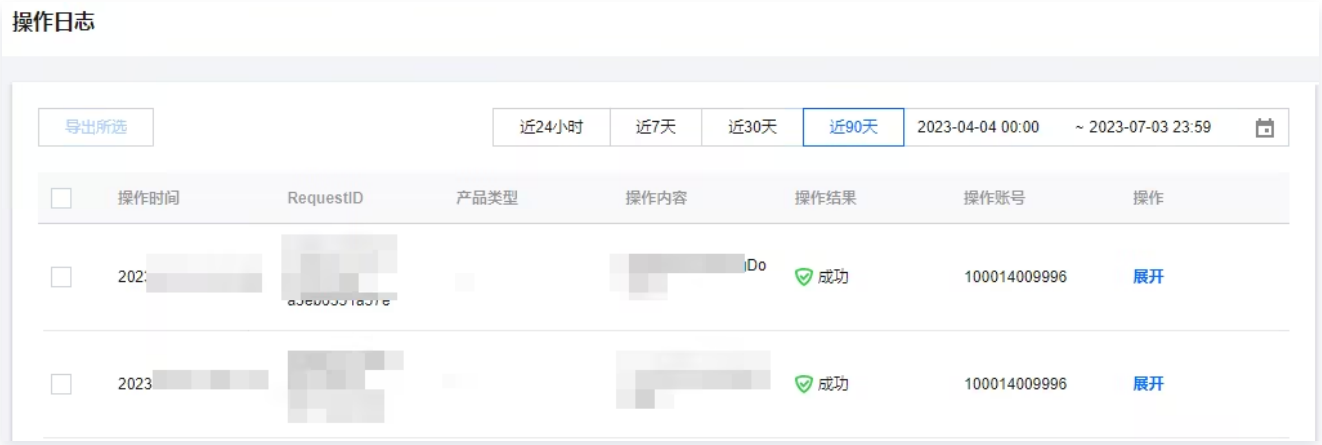
Last updated: 2025-03-19 21:47:41

The Anti-DDoS (new version) console supports viewing logs of important operations within the past 90 days. The logs that can be viewed include the following categories:

- Protection Object IP Replacement Log
- Anti-DDoS Policy Modification Operation Log
- Cleaning Threshold Adjustment Log
- Protection Level Change Log
- Resource Name Modification Log

Operation Steps

1. Log in to the Anti-DDoS (New Version) Console, and click on **Operation Log** in the left sidebar.
2. On the Operation Log page, you can set the time range to query related operation records.



Cloud Log Service (CLS) Log Delivery

Last updated: 2025-03-19 21:47:53

Anti-DDoS provides a log shipping feature. Through log shipping, you can collect slow log and error log data from Anti-DDoS instances and ship it to Cloud Log Service (CLS) for analysis, enabling quick monitoring and troubleshooting of business issues. This document describes how to enable or disable the log shipping feature via the console.

Note:
- Before using this feature, make sure you have activated CLS.
- Only Anti-DDoS Pro instances and Anti-DDoS IP instances support the log delivery feature.

Field Description

General Fields For DDoS Attack Start

Field Name	Data Type	Description
AttackStartTime	Timestamp ISO8601	The time when the DDoS attack started. Example value: 2024-10-14T05:13:43Z, which represents 05:13:43 in the UTC+0 time zone on October 14, 2024, equivalent to 13:13:43 in the UTC+8 time zone (Beijing time) on October 14, 2024.
AttackTraffic	String	Attack traffic (unit: Mbps)
AttackPacketRate	String	Attack packet rate (unit: pps)
AttackTrafficType	Integer	Type of attack traffic

General Fields For DDoS Attack End

Field Name	Data Type	Description
AttackStartTime	Timestamp ISO8601	The time when the DDoS attack started. Example value: 2024-10-14T05:13:43Z, which represents 05:13:43 in the UTC+0 time zone on October 14, 2024,

		equivalent to 13:13:43 in the UTC+8 time zone (Beijing time) on October 14, 2024.
AttackEndTime	Timestamp ISO8601	The time when the DDoS attack ended. Example value: 2024-10-14T05:13:43Z, which represents 05:13:43 in the UTC+0 time zone on October 14, 2024, equivalent to 13:13:43 in the UTC+8 time zone (Beijing time) on October 14, 2024.
AttackTrafficPeak	String	Peak attack traffic (unit: Mbps)
AttackTrafficType	Integer	Type of attack traffic
CumulativeCleanedTraffic	String	Cumulative cleaning traffic (unit: Mbps)

General Fields For CC Attack Start

Field Name	Data Type	Description
AttackStartTime	Timestamp ISO8601	Start time of the CC attack. Example value: 2024-10-14T05:13:43Z, which represents 05:13:43 in the UTC+0 time zone on October 14, 2024, equivalent to 13:13:43 in the UTC+8 time zone (Beijing time) on October 14, 2024.
CurrentRequestRate	String	Current request rate (unit: QPS)
CurrentCleaningRate	String	Current cleaning rate (unit: QPS)

General Fields For CC Attack End

Field Name	Data Type	Description
AttackStartTime	Timestamp ISO8601	Start time of the CC attack. Example value: 2024-10-14T05:13:43Z, which represents 05:13:43 in the UTC+0 time zone on October 14, 2024, equivalent to 13:13:43 in the UTC+8 time zone (Beijing time) on October 14, 2024.
AttackEndTime	Timestamp ISO8601	End time of the CC attack. Example value: 2024-10-14T05:13:43Z, which represents 05:13:43 in the

		UTC+0 time zone on October 14, 2024, equivalent to 13:13:43 in the UTC+8 time zone (Beijing time) on October 14, 2024.
MaxRequestRate	String	Maximum request rate (unit: QPS)
MaxCleaningRate	String	Maximum cleaning rate (unit: QPS)
CumulativeBlockedIllegalRequestCount	String	Cumulative number of intercepted illegal requests (unit: QPS)

General Fields For Blocking Event

Field Name	Data Type	Description
BlockTime	Timestamp ISO8601	IP blocking time. Example value: 2024-10-14T05:13:43Z, which represents 05:13:43 in UTC+0 time zone on October 14, 2024, equivalent to 13:13:43 in UTC+8 time zone (Beijing time) on October 14, 2024.
ExpectedUnblockTime	Timestamp ISO8601	Estimated IP unblocking time. Example value: 2024-10-14T05:13:43Z, which represents 05:13:43 in UTC+0 time zone on October 14, 2024, equivalent to 13:13:43 in UTC+8 time zone (Beijing time) on October 14, 2024.
AttackTrafficPeak	String	Peak attack traffic (unit: Mbps)
BlockType	Integer	Blocking type

General Fields For Unblocking Event

Field Name	Data Type	Description
UnblockTime	Timestamp ISO8601	IP unblocking time. Example value: 2024-10-14T05:13:43Z, which represents 05:13:43 in UTC+0 time zone on October 14, 2024, equivalent to 13:13:43 in UTC+8 time zone (Beijing time) on October 14, 2024.
UnblockMethod	Integer	Exposed to blocking method
RemainingSelfUnblockCoun	String	Current remaining self-service unlocking count

tToday		

Example Of a Log

Example Of a Single DDoS Attack Start Log


```
{
"AttackTraffic":"309999"
"AttackPacketRate":"988888"
"AttackStartTime":"2024-11-27T17:50:38Z"
"AttackTrafficType":"TCPFLOOD"
}
```


Example Of a Single DDoS Attack End Log


```
{
"AttackTrafficPeak":"309999"
"AttackStartTime":"2024-11-27T17:51:14Z"
"AttackEndTime":"2024-11-27T18:06:14Z"
"AttackTrafficType":"TCPFLOOD"
"CumulativeCleanedTraffic":"80"
}
```


Example Of a Single CC Attack Start Log


```
{
"CurrentCleaningQPS":"999999"
"CurrentRequestQPS":"123456"
"AttackStartTime":"2024-11-27T16:25:00Z"
}
```


Example Of a Single CC Attack End Log


```
{
"MaxCleaningQPS":"999999"
"AttackStartTime":"2024-11-27T16:45:00Z"
"AttackEndTime":"2024-11-27T16:55:00Z"
"CumulativeBlockedIllegalRequestCount":"9"
```

```
"MaxRequestQPS":"123456"
}
```

Example Of a Single Blocking Event Log

```
{
"ExpectedUnblockTime":"2024-11-28T16:55:00Z"
"AttackTrafficPeak":"20029"
"BlockType":"tix"
"BlockTime":"2024-11-27T17:00:00Z"
}
```

Example Of a Single Unblocking Event Log

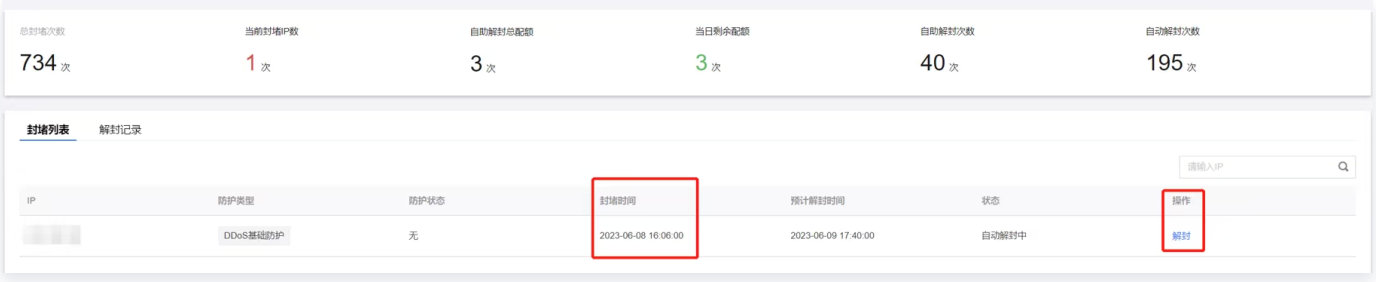
```
{
"UnblockMethod": "Automatic Unblocking"
"RemainingSelfUnblockCountToday":"3"
"UnblockTime":"2024-11-27T17:01:00Z"
}
```

Service Management
Unblocking Center
View Blocking Time

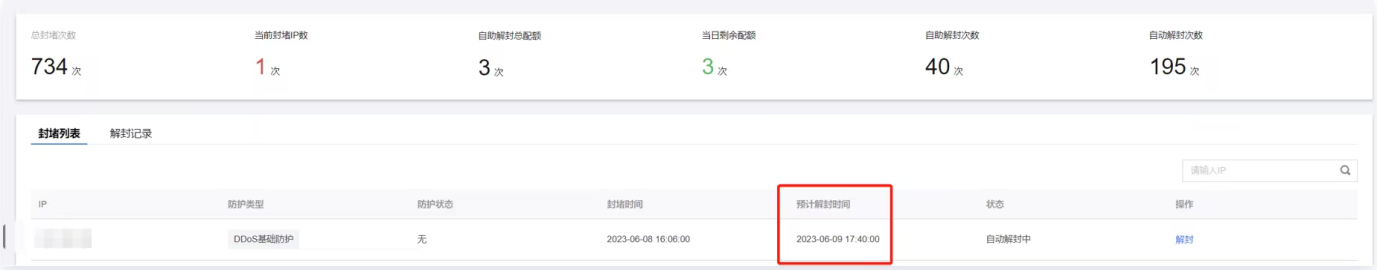
Last updated: 2026-03-11 17:18:43

View the Unblocked IP Time

1. Log in to the Anti-DDoS (New Version) Console, and click on **Unblocking Service** in the left sidebar.
2. On the Unblocking Service page, under the Unblock List tab, select the row of the desired IP to view its **Blocking Time** at the corresponding field.

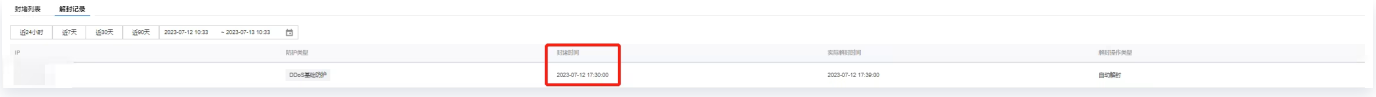


3. On the Unblock List tab, select the row of the desired IP to view its **Estimated Unblocking Time** at the corresponding field.

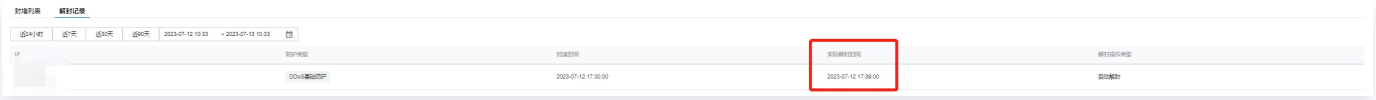


View Unblocked IP Time

1. Log in to the Anti-DDoS (New Version) Console, and click on **Unblocking Service** > **Unblock Record** in the left sidebar.
2. On the Unblock Record tab, select the row of the desired IP to view its **Blocking Time** at the corresponding field.



3. On the Unblocking Operation Records page, select the row of the desired IP, and you can view the actual unblocking time of the IP at **Estimated Unblocking Time**.



Unblocking

Last updated: 2025-03-19 21:48:18

Auto Unblocking

No need for manual operation. Just wait until the estimated unblocking time is reached, and it will be automatically unblocked. You can follow the following steps to view the estimated unblocking time:

1. 1. Log in to the Anti-DDoS (New Version) Console. In the left sidebar, click **Unblocking Service**.
2. On the unblocking list tab of the unblocking service page, select the located row of the desired IP. You can view the blocking time of this IP in "Blocking Time".

Bind Anti-DDoS Premium to Unblock

- When a blocked IP is bound to an Anti-DDoS Pro (excluding the lightweight version and High Defense Insurance), binding Anti-DDoS Premium to Unblock will be automatically enabled.
- Users who use Anti-DDoS Pro (excluding the lightweight version and High Defense Insurance) will obtain **binding Anti-DDoS Premium to unblock** count corresponding to the specification of "protected IP number" of their high-defense package instance per month.
- If an Anti-DDoS Pro (excluding the lightweight version and High Defense Insurance) is downgraded during use in the current month, reducing the specification of "protected IP number", the system will update the number of unblocking times simultaneously and reduce the unused **binding Anti-DDoS Premium to unblock** count.
- On the first day of each month, the number of **binding Anti-DDoS Premium to unblock** will be reset according to the "protected IP number" at the end of last month.

Number of Self-Service Unblocks

- Users who use Anti-DDoS Pro (excluding the lightweight version, inclusive version, and High Defense Insurance) and Anti-DDoS Advanced will have three self-service unblocking opportunities per day. If the number of unblocking operations exceeds three on the day, they will be unable to perform unblocking operations. The system will reset the number of self-service unblocking times at zero point every day. The unblocking times not used on the day will not accumulate to the next day.
- Users who use Anti-DDoS Pro (Lightweight Edition) are provided with three self-service unblocking capabilities per month. The self-service unblocking capability can only be used to unblock lightweight server resources.
- Users who use the 10Gbps specification of Anti-DDoS Pro (Inclusive Edition) are provided with three self-service unblocking capabilities per month. After exceeding three times in the current month, they will be unable to perform the unblocking operation.

Note:

- If there are multiple anti-DDoS products in the same account, the upper limit of the number of times for self-service unblocking of that account is three times per day.
- Since unblocking involves the risk management strategy of the backend system of Tencent Cloud Anti-DDoS, unblocking may fail (unblocking failure will not deduct your remaining number of unblocking times). Please be patient and try again after waiting for a period of time.
- Before performing the unblocking operation, it is recommended that you first view the estimated unblocking time. The estimated unblocking time may be postponed due to some factors. If you can accept the estimated time, there is no need for manual operation.
- When the manual unblocking quota for the day is 0, it is recommended to enhance the base protection capability or elastic protection capability so that you can sufficiently defend against high-traffic attacks and avoid being continuously blocked.

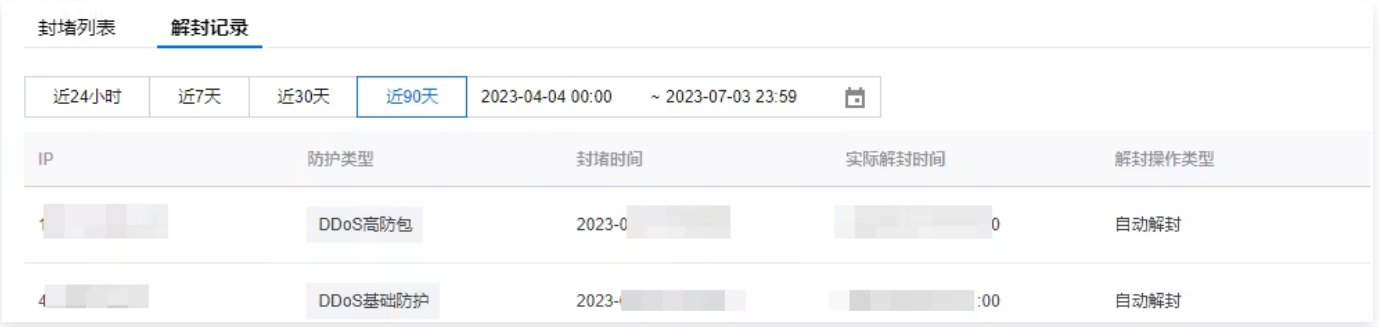
Self-Service Unblocking

1. 1. Log in to the Anti-DDoS (New Version) Console. In the left sidebar, click **Unblocking Service**.
2. On the unblocking list tab of the unblocking service page, find the protected IP with a status of "Auto Unblocking". In the right operation column, click **Unblock**.

3. In the Unblock dialog box, click **Confirm**. You will receive a prompt message indicating that the unblock was successful. This means that the blocking status has been successfully removed. You can refresh the page to confirm whether the protected IP has been restored to the running status.

Unblocking Operation Records

1. Log in to the Anti-DDoS (New Version) Console. In the left sidebar, click **Unblocking Service** > **Unblock Record**.
2. On the Unblock Record tab, filter by time range to view all unblocking operation records, including automatic unblocking, self-service unblocking and other operation records.



Connect To the Blocked Server

Last updated: 2025-03-19 21:48:30

This document introduces how to connect to a blocked server.

Operation Steps

1. Log in to the Cloud Virtual Machine console, click on **Instance** in the left sidebar to enter the instance page.
2. On the instance page, click on the region dropdown list at the top left corner to switch regions.
3. On the instance page, click on the search box and use keywords such as "instance name", "instance ID", and "instance status" to find the corresponding blocked server.

4. In the row of the blocked server, click on **Log In** to pop up the Log in to Linux Instance window.

5. In the Log in to Linux Instance window, click on **VNC Log-in** to connect via browser VNC method.

Alarm Center
Setting Security Event Notifications

Last updated: 2025-03-19 21:48:43

When the protected IP connected to your Anti-DDoS Pro is under attack, the attack ends, the IP is blocked, or the block is lifted, Tencent Cloud will send you alarm messages via channels such as Message Center, SMS, email, and WeChat. The actual receiving method is subject to your subscription configuration in Message Center.

- You will receive an attack start Note when the attack begins.
- You will receive an attack end Note 15 minutes after the attack ends.
- You will receive a block Note when the IP is blocked.
- You will receive an unblock Note when the IP is unblocked.

You can modify the recipient and reception method of alarm messages according to actual conditions.

Operation Steps

1. Log in to the Anti-DDoS (New Version) Console, and click on **Alarm Notification** in the left sidebar.
2. In the feature cards on the right, you can set the "Single IP Inbound Traffic Alarm Threshold", "DDoS Threshold-clearing", and "CC Threshold-clearing" respectively.

3. Click on **Advanced Settings** of the feature card to enter the alarm configuration list and set different alarm thresholds for each high-protection package resource.
   - Single IP inbound traffic alarms

   - DDoS Cleaning Threshold

CC Cleaning Traffic Alarm

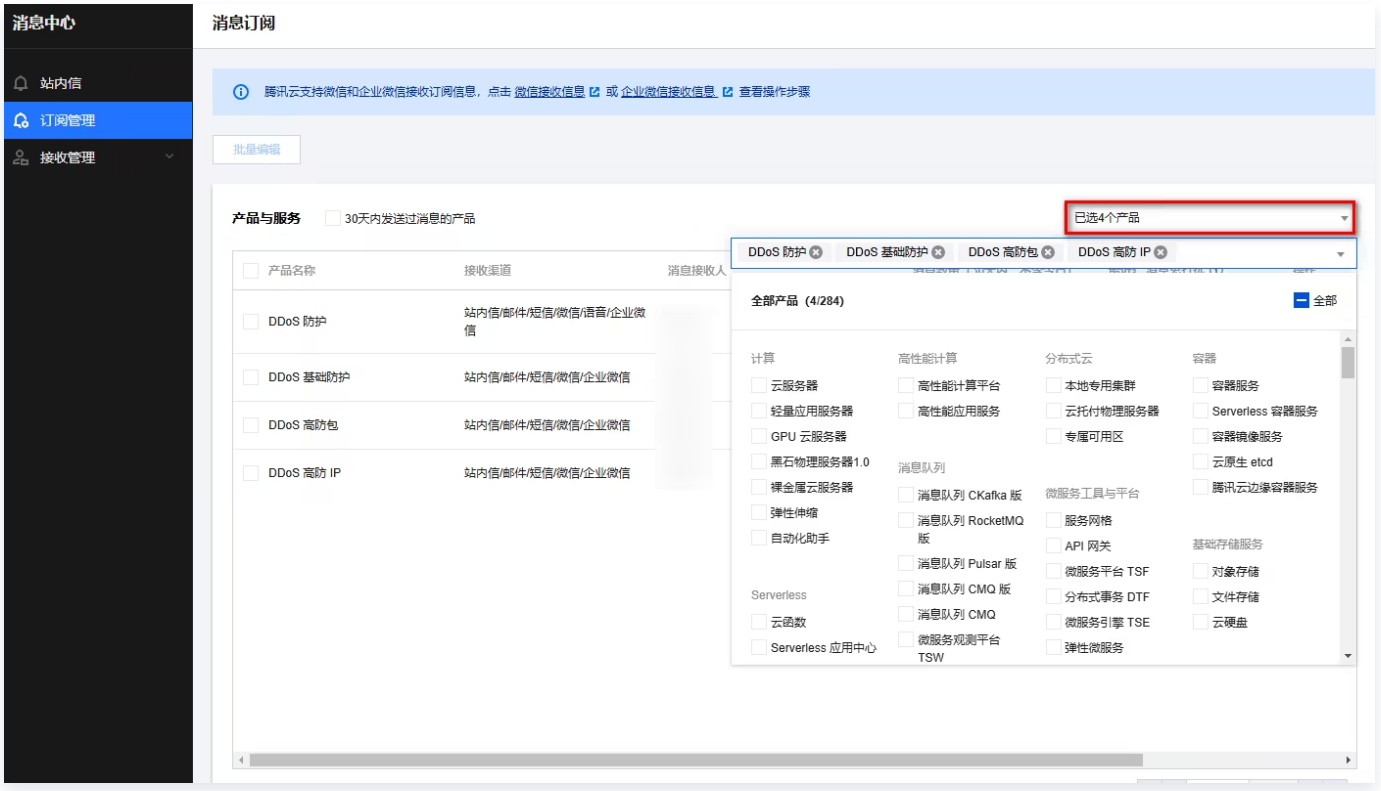
Set Notification Methods

Last updated: 2025-03-19 21:51:01

1. Log in to your Tencent Cloud account and enter Message Center.

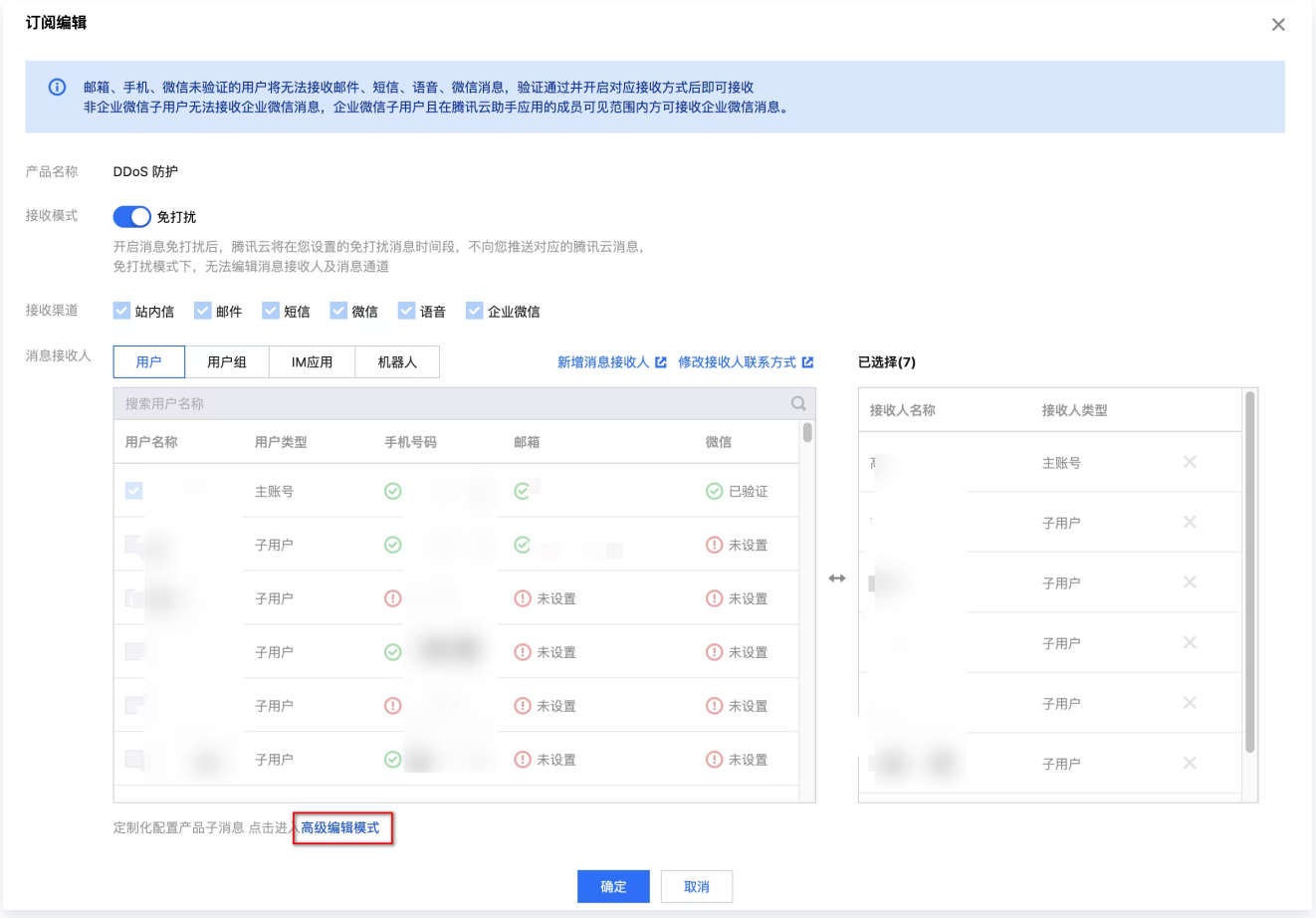
> **Note:**
>
> You can also log in to the console, click on  in the upper right corner, and on the pop-up page, click **View More** to enter the message center.

2. In the left directory, click **Subscription Management** and select the products for which you want to receive messages.

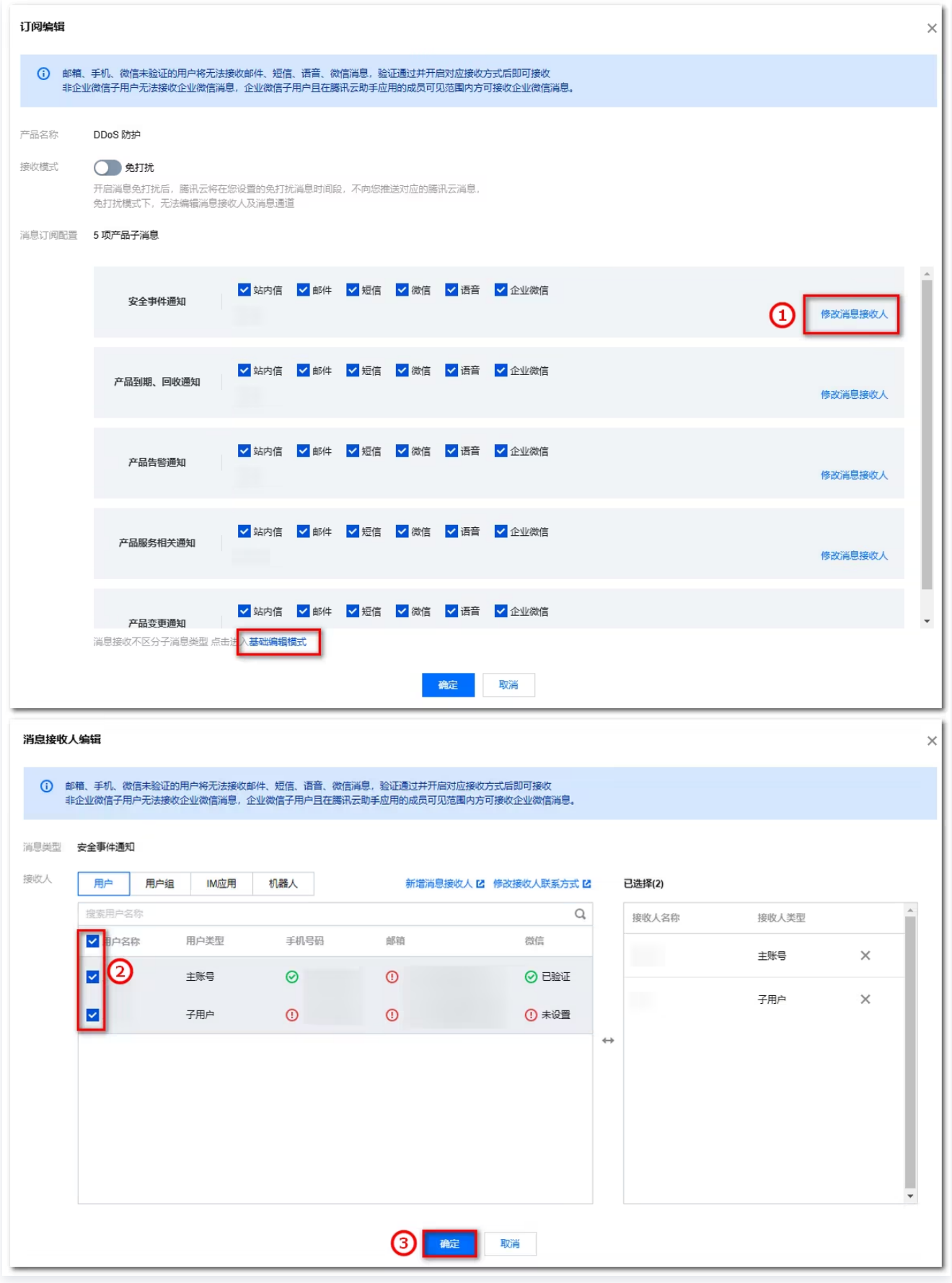


3. On the Message Subscription page, select the reception method and click **Edit**.

4. In the Subscription Edit pop-up, there are Basic Mode and Advanced Mode, and you can switch modes at the lower left corner.
   - Basic editing: Set the Message Recipient and click **Yes** after completion.



   - Advanced editing: Click **Modify Message Recipient** on the right side of the product sub-message to set the Message Recipient, and click **Yes** after completion.



CAM Overview

Last updated: 2025-03-19 21:51:14

If you use Anti-DDoS services in Tencent Cloud, please be aware that although these services are managed by different personnel, they all share your cloud account key, which may lead to the following issues:

- The risk of key leakage is increased as it is shared by multiple people.
- The access permission of other people cannot be restricted, which may easily lead to security risks due to misoperations.

To address this problem, you can use Cloud Access Management (CAM) to assign different individuals to manage different services through sub-accounts, thereby avoiding the aforementioned issues. By default, sub-accounts do not have permission to use Anti-DDoS or its related resources, and you need to create policies to grant the necessary permissions to sub-accounts. If you do not need to manage access to Anti-DDoS-related resources for sub-accounts, you can skip this section. Skipping this part will not affect your understanding and use of the rest of the documentation.

> **Note:**
> Applicable to users of Anti-DDoS Basic, Anti-DDoS Pro, and Anti-DDoS Advanced.

CAM

Cloud Access Management (CAM) can help you securely and conveniently manage access to Tencent Cloud services and resources. You can use CAM to create sub-users, user groups, and roles, and control their access scope through policies. CAM supports user and role SSO capabilities, allowing you to set up interconnection capabilities between users within your enterprise and Tencent Cloud based on specific management scenarios.
The Tencent Cloud root account you initially created has full access to all services and resources under the account. It is recommended to protect the credentials of the root account, use sub-users or roles for daily access, enable multi-factor authentication, and periodically rotate keys.
Policies can authorize or deny users access to specified resources to complete specified tasks. When using CAM, you can associate policies with a user or a group of users for permission control. Anti-DDoS has been integrated with CAM, and you can use CAM to control permissions for Anti-DDoS-related resources.

Relevant Concepts

CAM User

CAM User is an entity you create in Tencent Cloud, and each CAM user is only associated with one Tencent Cloud account. Your registered Tencent Cloud account identity is **Root Account**, and you can create **Sub-Accounts** with different permissions through User Management for collaboration. The types of sub-accounts include Sub-user, Collaborator, and Message Recipient.

Policies

Policy is a syntax specification used to define and describe one or more permissions. Tencent Cloud's policy types are divided into preset policies and custom policies.

- Preset policy: A policy created and managed by Tencent Cloud. It is a collection of some common permissions frequently used by users, such as full read/write permission for resources. Preset policies have a wide range of operation objects and coarse operation granularity. And they are system - preset and cannot be edited by users.
- Custom policy: A policy created by the user, which allows for fine - grained permission division. For example, associate a usage policy with a sub - account, so that it has the right to manage the scaling group of Auto Scaling but has no right to manage the cloud database instance.

Resources

Resource (resource) is an element of the policy, describing one or more operation objects, such as the launch configuration and scaling group of AS.

Authorizable API Operations and Resource Types

Last updated: 2026-03-11 18:06:37

Overview

This document will introduce the resource types, API operations, and preset policies that can be authorized for Anti-DDoS. You can use the visual operations in the Cloud Access Management (CAM) console to grant preset permission policies to sub-accounts. If you need to grant more detailed permissions to sub-accounts, please refer to the relevant product API descriptions and Authorization Policy Syntax below this document.

Preset Policy

Anti-DDoS Preset Policy

Anti-DDoS preset policies are as follows:

Policies	Description
QcloudAntiDDoSFullAccess	Full read-write access to Anti-DDoS
QcloudAntiDDoSReadOnlyAccess	Read-only access to Anti-DDoS

Preset Policies For Other Products

The Anti-DDoS preset policies do not include permissions related to other Tencent Cloud products. Usually, you also need to grant preset policies for other products to fully use all features of the Anti-DDoS console. You can grant the following relevant preset policies to sub-accounts:

Policies	Description
QcloudCVMReadOnlyAccess	Read-only access to CVM resources.
QcloudAPIGWReadOnlyAccess	Read-only access to API Gateway (API Gateway)
QcloudTSEReadOnlyAccess	Read-only access permissions for Tencent Cloud microservice engine (TSE)
QcloudBMEIPReadOnlyAccess	Read-only access to Blackstone Elastic IP (BM EIP)

QcloudBMInnerReadOnlyAccess	Read-only access permissions for Blackstone physical server (BM)
QcloudBMLBReadOnlyAccess	Read-only access permissions for Blackstone Cloud Load Balancer (BM LB)
QcloudLighthouseReadOnlyAccess	Read-only access permission for Light Application Server (Lighthouse)

Customizing Policies

Authorizable Resource Type

Resource type describes the hierarchical relationship of resources and is used to specify the specific resource for operations. For example, if a sub-user needs to query the list of Anti-DDoS Pro instances in a certain region, they can configure the resource type of Anti-DDoS in the policy through Cloud Access Management (CAM).

Resource Type	Description	Resource Description Method
antiddos	High-protection package instance	qcs::antiddos:${Region}:${uin}/${Owneruin}:antiddos/${resourceId}

Authorizable Operations and Product Permissions

To configure more precise Anti-DDoS resource access control, you need to configure the product's API Operation Permissions for the sub-user. The specific operation permissions are as follows:

API Operation	Description
cvm:DescribeInstances	Obtain instance list
lighthouse:DescribeInstances	Obtain the Lighthouse instance list
clb:DescribeLoadBalancers	Obtain the CLB instance list
vpc:DescribeNatGateways	Obtain the NAT Gateway list
vpc:DescribeVpngateways	Obtain the VPN Gateway list

vpc:DescribeNetworkInterfaces	Obtain the Elastic Network Interface list
vpc:DescribeDirectConnectGateways	Obtain the Direct Connect Gateway list
apigateway:DescribeExclusiveInstancesStatus	Obtain the status of an exclusive gateway instance
tke:DescribeClusters	Obtain the Cluster list
bmlb:DescribeLoadBalancers	Obtain the Blackstone CLB instance list
bmvpc:DescribeEips	Obtain the Blackstone Elastic IP
tag:GetTagKeys	Obtain the Tag key list.

Authorization Policy Syntax

Last updated: 2025-03-19 21:56:47

Overview

This document will introduce you to the authorization policy syntax related to Anti-DDoS, making it easier for you to perform more detailed authorization operations.

Policy Syntax

CAM policies supported by Anti-DDoS.

```
{
        "version":"2.0",
        "statement":
        [
            {
                "effect":"effect",
                "action":["action"],
                "resource":["resource"],
            }
        ]
}
```

- The **version** is required, currently only allowing a value of "2.0".
- **statement** is used to describe the detailed information of one or more permissions. This element includes the permissions or permission sets of multiple other elements such as effect, action, resource, and condition. A policy has one and only one statement element.
- **Effect** describes whether the statement produces an "allow" or "explicit deny" result. It includes allow (permission) and deny (explicit denial) two situations. This element is required.
- **Action** is used to describe the operations that are allowed or denied. Operations can be APIs (described with a name prefix) or feature sets (a specific set of APIs described with a permid prefix). This element is required.
- **Resource** describes the specific data of the authorization. Resources are described using a six-section format. The resource definition details will vary for each product. This element is required.

Operations Of Anti-DDoS

In the Cloud Access Management (CAM) policy statement, you can specify any API operation from any service that supports CAM. For Anti-DDoS, use the API prefixed with `antiddos:`. For example: `antiddos:DescribeListBGPInstances` or `antiddos:DescribeCloudProtectInstance`.
If you want to specify multiple operations in a single statement, separate them with commas as follows:

```
"action":
["antiddos:DescribeListBGPInstances","antiddos:DescribeCloudProtectInstance"]
```

You can also use wildcard characters to specify multiple operations. For example, you can specify all operations whose names begin with the word "Describe" as follows:

```
"action":["antiddos:Describe*"]
```

If you want to specify all operations in Anti-DDoS, use the * wildcard as follows:

```
"action": ["antiddos:*"]
```

Resource Path Of Anti-DDoS

Each CAM policy statement has its own applicable resources. The general format of the resource path is as follows:

```
qcs:project_id:service_type:region:account:resource
```

- **QCS**: The abbreviation of qcloud service, indicating it's the cloud resource of Tencent Cloud.
- **project_id**: It describes the project information. It is only for compatibility with early CAM logic and does not need to be filled in.
- **Service_type**: The product abbreviation, such as: antiddos.
- **Region**: Regional information, such as: ap-guangzhou.
- **Account**: The root account information of the resource owner, such as: `uin/1234567890`.
- **Resource**: Specific resource details for each product, such as: `antiddos/bgp-00000012` or `antiddos/*`. For example, you can specify an anti-DDoS instance (bgp-00000012), as shown below:

```
"resource":["qcs::antiddos:ap-guangzhou:uin/1234567890:antiddos/bgp-
00000012"]
```

You can also use the * wildcard character to specify all instances belonging to a specific account, as shown below:

```
"resource":["qcs::antiddos:ap-guangzhou:uin/1234567890:antiddos/*"]
```

If you want to specify all resources, or if a particular API action does not support resource-level permissions, use the wildcard (*) in the Resource element, as shown below:

```
"resource": ["*"]
```

To specify multiple resources in one instruction, separate them with a comma. The following is an example of specifying two resources:

```
"resource":["resource1","resource2"]
```

The following table describes the resources that Anti-DDoS can use and the corresponding resource description methods. In the table below, words prefixed with $ are aliases.

- Among them, region refers to the area.
- Among them, account refers to the account ID.
- Among them, resourceId refers to the anti-DDoS instance ID.

Resources	Resource Description Method In Authorization Policies
High-defense instance	`qcs::${antiddos}:${Region}:uin/${OwnerUin}:antiddos/${resourceId}`

Example Of Authorizing With Policies

Last updated: 2026-03-11 18:07:06

Overview

You can grant users permission to view and use specific resources in the Anti-DDoS console by using Cloud Access Management (CAM) policies. This document provides examples of permissions for viewing and using specific resources, guiding users on how to use the policies for specific parts of the console.

Operation Example

Full Read/Write Policy For Anti-DDoS

If you want users to have the permission to manage Anti-DDoS instances, you can apply the policy QcloudAntiDDoSFullAccess to them. This policy allows users to operate all resources under Anti-DDoS, but you also need to grant related permissions for protection resource products to ensure that users can use Anti-DDoS normally. For details on permissions, see Authorizable API Operations and Resource Types. The specific steps are as follows: Follow the instructions in Authorization Management to authorize the preset policy QcloudAntiDDoSFullAccess to users.

Read-Only Policy For Anti-DDoS

If you want users to have the permission to query Anti-DDoS instances but not the permission to operate resources, you can apply the policy QcloudAntiDDoSReadOnlyAccess to them. This policy is designed to achieve its purpose by granting users permissions to operate all operations in Anti-DDoS that start with "Describe" and "List". In addition, you also need to grant users related permissions for protection resource products to ensure they can use Anti-DDoS normally. The specific steps are as follows: Refer to Authorization Management to authorize the preset policy QcloudAntiDDoSReadOnlyAccess to users.

Authorize User To Have Specific Anti-DDoS Operation Permissions Policy

If you want to grant users specific Anti-DDoS operation permissions, you can associate the following policies with them. The specific steps are as follows:

1. Log in to the CAM console, and in the left sidebar, click **Policies**.
2. On the Policy page, click **Create Custom Policy**, select **Create by Policy Syntax** and **Blank Template**, click **Next**.
3. On the Edit Policy page, create a custom policy.

This policy allows users to have all operation permissions for the Anti-DDoS instance with ID bgp-1 in Guangzhou. The policy content can be set by referring to the following policy syntax:

```
{
 "version": "2.0",
 "statement": [
  {
      "action": ["antiddos:*"],
      "resource": ["qcs::antiddos:ap-guangzhou::antiddos/bgp-1"],
      "effect": "allow"
  }
 ]
}
```

4. After clicking **Finish**, find the created policy, and in the "Operation" column of the policy row, click **Associate User/User Group/Role**.
5. In the pop-up "Associate User/User Group/Role" window, check the users to be associated, click **OK** to complete the operation of associating users through policies.

> **Note:**
> The account field here is empty, representing the resources under the root account to which the CAM user creating the policy belongs. If you still have questions, refer to Resource Description Method.

Authorize User To Have Specific Regional Anti-DDoS Operation Permissions Policy

If you want to grant users specific Anti-DDoS operation permissions in a certain region, you can associate the following policy with them. The specific steps are as follows:

1. Log in to the CAM console, and in the left sidebar, click **Policies**.
2. On the Policy page, click **Create Custom Policy**, select **Create by Policy Syntax** and **Blank Template**, click **Next**.
3. On the Edit Policy page, create a custom policy.

   This policy allows users to have all operation permissions for Anti-DDoS instances in the Guangzhou region. The policy content can be set by referring to the following policy syntax:

```
{
 "version": "2.0",
```

```
  "statement": [
    {
        "action": ["antiddos:*"],
        "resource": ["qcs::antiddos:ap-guangzhou::*"],
        "effect": "allow"
    }
  ]
}
```

4. After clicking **Finish**, find the created policy, and in the "Operation" column of the policy row, click **Associate User/Group/Role**.
5. In the pop-up "Associate User/User Group/Role" window, check the users to be associated, click **OK** to complete the operation of associating users through policies.

Custom Policies

If you feel that the preset policies do not meet your requirements, you can achieve your goal by creating custom policies. For specific steps, please refer to Policies. For more Anti-DDoS related policy syntax, please refer to Authorization Policy Syntax.