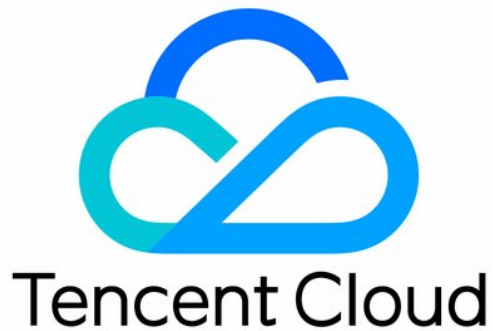


Anti-DDoS

Operation Guide

Product Documentation



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

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

Trademark Notice



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

Service Statement

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

Contents

Operation Guide

Operation Overview

Protection Overview

Usage Limits

Asset Center

Cloud Assets

云上防护实例

Viewing Instance Information

Managing Protected Objects

Setting Instance Names and Tags

Modifying Elastic Protection Bandwidth

Unblocking Protected IPs

Business Connection

Quick IP Connection

Domain Name Connection

IP Connection

Port Connection

Configuring Session Persistence

Configuring Health Check

Smart Scheduling

Protection Configuration

DDoS Protection

DDoS Protection Levels

IP Blocklist/Allowlist

Port Filtering

Protocol Blocking

Watermark Protection

Connection Attack Protection

AI Protection

Regional Blocking

IP and Port Rate Limit

Feature Filtering

CC Protection

CC Protection and Cleansing Threshold

Intelligent CC Protection

Precise Protection

CC Frequency Limit

Regional Blocking

IP Blocklist/Allowlist

Security Operations

Attack Analysis

Business Analysis

Operation Logs

Service Management

Unblocking Service

Viewing Blocking Time

Unblocking an IP

Connecting a Blocked Server

Alert Service

Setting Security Event Notifications

Setting Notification Methods

Operation Guide

Operation Overview

Last updated : 2024-07-01 11:33:59

This document lists the references for common operations while using Anti-DDoS Basic, Anti-DDoS Pro, and Anti-DDoS Advanced. Such operations include but are not limited to configuring instances, viewing statistics reports, viewing operation logs, and setting security event notifications.

Overview and use limits

[Protection Overview](#)

[Use Limits](#)

Assets

[Cloud Asset List](#)

[Viewing Instance Information](#)

[Managing Protected Objects](#)

[Setting Instance Names and Tags](#)

[Modifying Elastic Protection Bandwidth](#)

[Unblocking Protected IPs](#)

Business connection

[Quick IP Connection](#)

[Port Connection](#)

[Domain Name Connection](#)

[IP Connection](#)

Scheduling and unblocking

[Smart Scheduling](#)

Protection configuration

DDoS protection

- [DDoS Protection Level](#)
- [IP Blocklist/Allowlist](#)
- [Port Filtering](#)
- [Protocol Blocking](#)
- [Watermark Protection](#)
- [Connection Attack Protection](#)
- [AI Protection](#)
- [Regional Blocking](#)
- [IP and Port Speed Limit](#)
- [Attribute Filtering](#)

CC protection

- [CC Protection and Cleansing Threshold](#)
- [Intelligent CC Protection](#)
- [Precise Protection](#)
- [CC Frequency Limit](#)
- [Regional Blocking](#)
- [IP Blocklist/Allowlist](#)

Security operations

- [Attack Analysis](#)
- [Business Analysis](#)
- [Operation Logs](#)

Service management

- [Viewing Blocking Time](#)
- [Unblocking IPs](#)
- [Connecting to blocked servers](#)
- [Setting Security Event Notifications](#)
- [Setting Notification Methods](#)


Protection Overview

Last updated : 2024-07-01 11:33:59

Viewing attack statistics

1. Log in to the new [Anti-DDoS console](#), click **Overview** on the left sidebar, and then click the **Protection Overview** tab.
2. In the **Security landscape** section, you can easily see the real-time security status of your business IP.

Security landscape ⓘ



Safe

No abnormal traffic detected.

Latest attack: -- Attack type: No attack yet

3. The attack statistics section displays the following data.

Total attacks	Attacked IPs
0 times	0
Peak attack bandwidth	Peak attack packet rate
0 bps	0 pps

Field description:

Total attacks: The total number of attacks against the resources connected to Anti-DDoS Basic/Pro, and Anti-DDoS Advanced IPs.

Attacked IPs: The total number of attacked IPs connected to Anti-DDoS Basic/Pro, and Anti-DDoS Advanced IPs.

Blocked IPs: Number of all blocked resource IPs connected to the public network, including customer IPs connected to Anti-DDoS Basic/Pro, and Anti-DDoS Advanced IPs.

Peak attack bandwidth: The maximum attack bandwidth of the current attack events.

Peak attack packet rate: The maximum attack packet rate of the current attack events.

Peak attack request: The highest request rate in the current attack events.

Viewing defense statistics

1. Log in to the new [Anti-DDoS console](#), click **Overview** on the left sidebar, and then click the **Protection Overview** tab.
2. In the **Real-time defense** section, you can easily see the business IP security status.



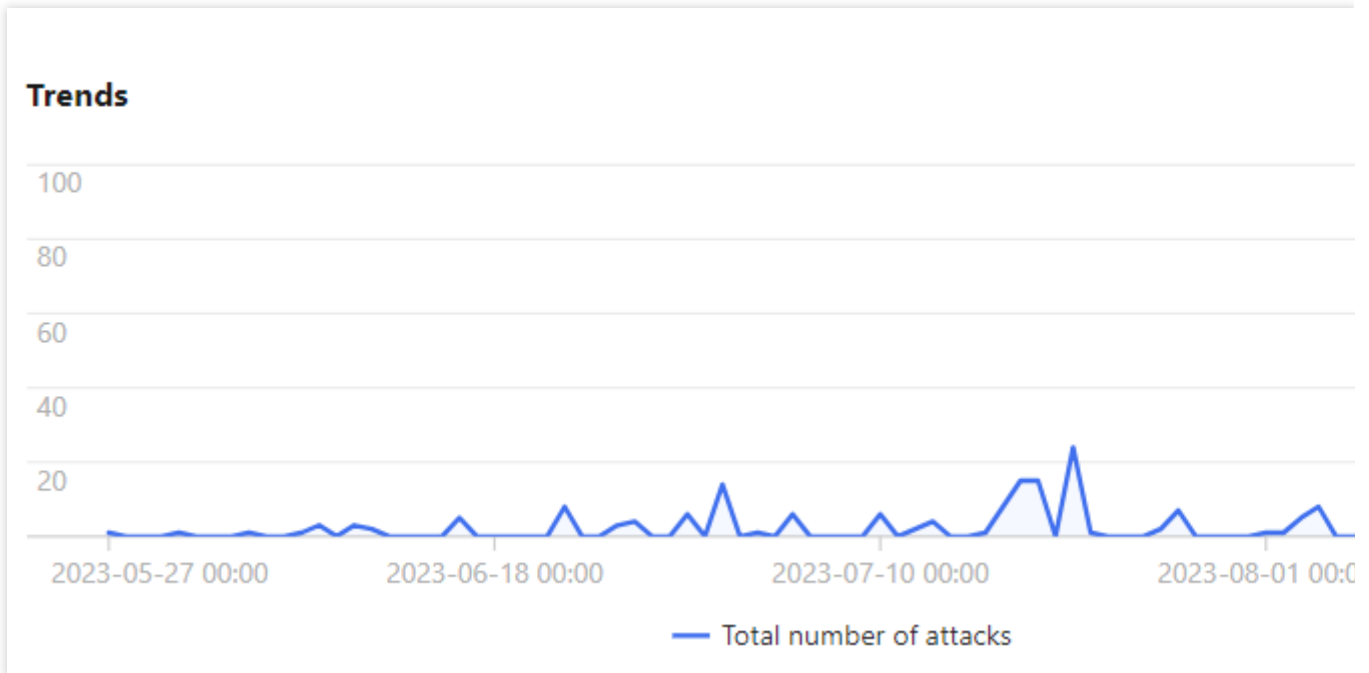
Field description:

Total IPs: Number of all resource IPs, including customer IPs connected to Anti-DDoS Basic/Pro, and Anti-DDoS Advanced IPs.

Protected IPs: Number of customer IPs connected to Anti-DDoS Pro and Anti-DDoS Advanced IPs.

Blocked IPs: Number of all blocked resource IPs connected with the public network, including customer IPs connected to Anti-DDoS Basic/Pro, and Anti-DDoS Advanced IPs.

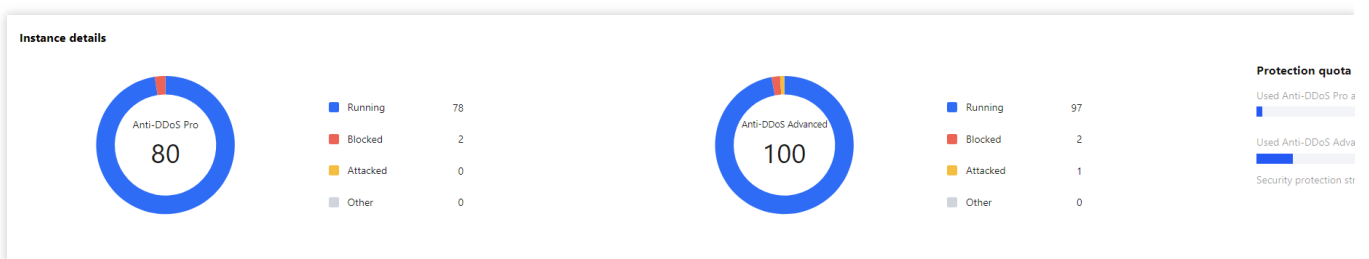
3. **Trends:** This section displays the total number of attacks on your resources.



4. Recommended actions: This section provides recommended actions for attacked IPs connected to Anti-DDoS Basic, allowing you to quickly upgrade your Anti-DDoS service.

Viewing instance details

1. Log in to the new [Anti-DDoS console](#), click **Overview** on the left sidebar, and then click the **Protection Overview** tab.
2. The **Instance details** section displays the security status of Anti-DDoS resources, providing an easy and complete way to know the distribution of insecure businesses. On the right, the protection quota usage is shown, including the used protection quota of Anti-DDoS Pro and that of Anti-DDoS Advanced.



View recent events

1. Log in to the new [Anti-DDoS console](#), click **Overview** on the left sidebar, and then click the **Protection Overview** tab.
2. The **Recent events** section shows you all the recent attack events. For attack analysis and source tracing, click **View details** to enter the event details page.

Recent Events						
Attack name	Anti-DDoS Resources	Instance Name	Defense Type	Attack time	Attack duration	Attack status
SYNFLOOD attacks				Started at: 2023-08-10 20:50:00 Ended at: 2023-08-10 20:57:00	7 mins	Attack ended
SYNFLOOD attacks				Started at: 2023-08-03 12:13:00 Ended at: 2023-08-03 12:18:00	5 mins	Attack ended

3. In the **Attack information** section of the event details page, you can view the detailed attack information for the selected period, including the attacked IP, status, attack type (which is sampled data), peak attack bandwidth and attack packet rate, and attack start and end time.

SYNFLOOD attacks ✕

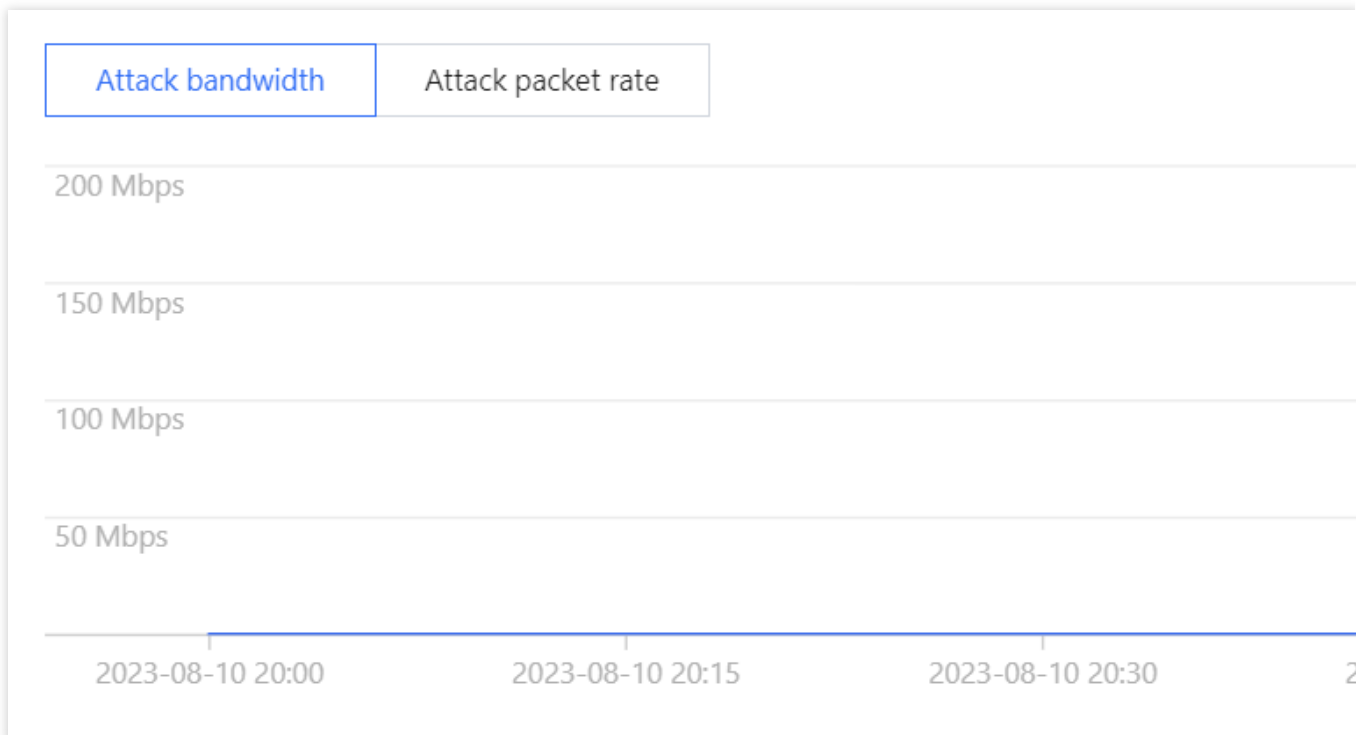
Attack information

Anti-DDoS Resources		Peak attack bandwidth	Mbps	
Status	<ul style="list-style-type: none"> ● Attack ended 	Peak attack packet rate	ps	
Attack type	SYNFLOOD	Attack started		
	OD	Attack ended		

4. In the **Attack trend** section of the event details page, you can view the trend of attack bandwidth and attack packet rate and easily find the peak traffic.

Note:

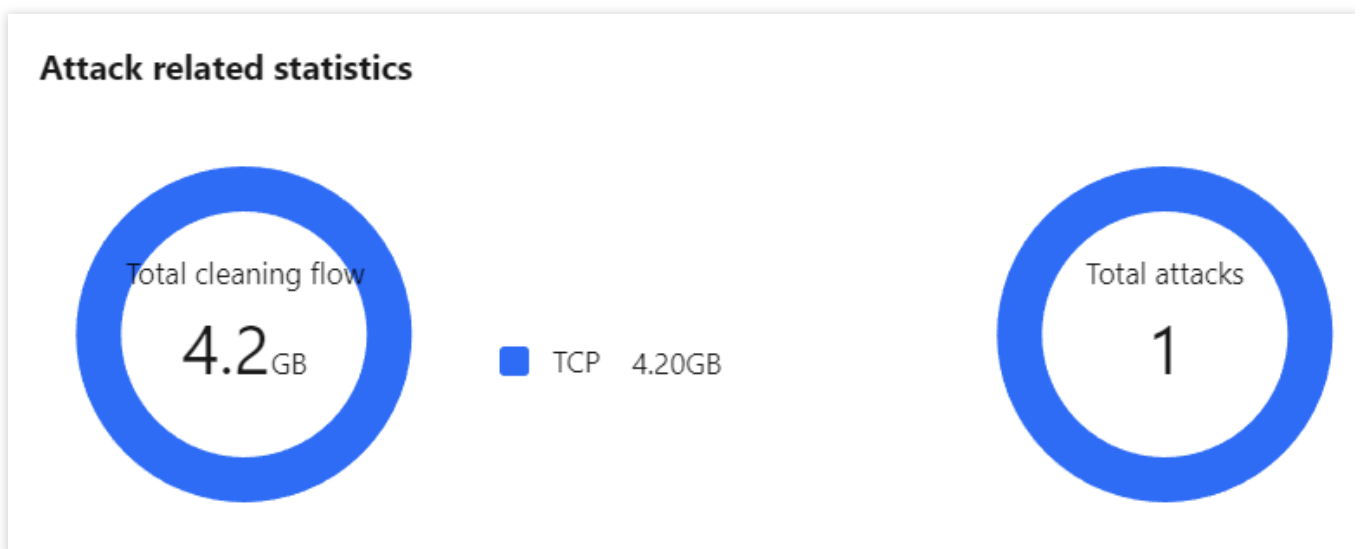
This section provides complete, real-time data in the attack period.



5. In the **Attack statistics** section of the event details page, you can view how attacks are distributed over different attack traffic protocols and attack types.

Note:

This section provides sampled data in the attack period.



Parameter description:

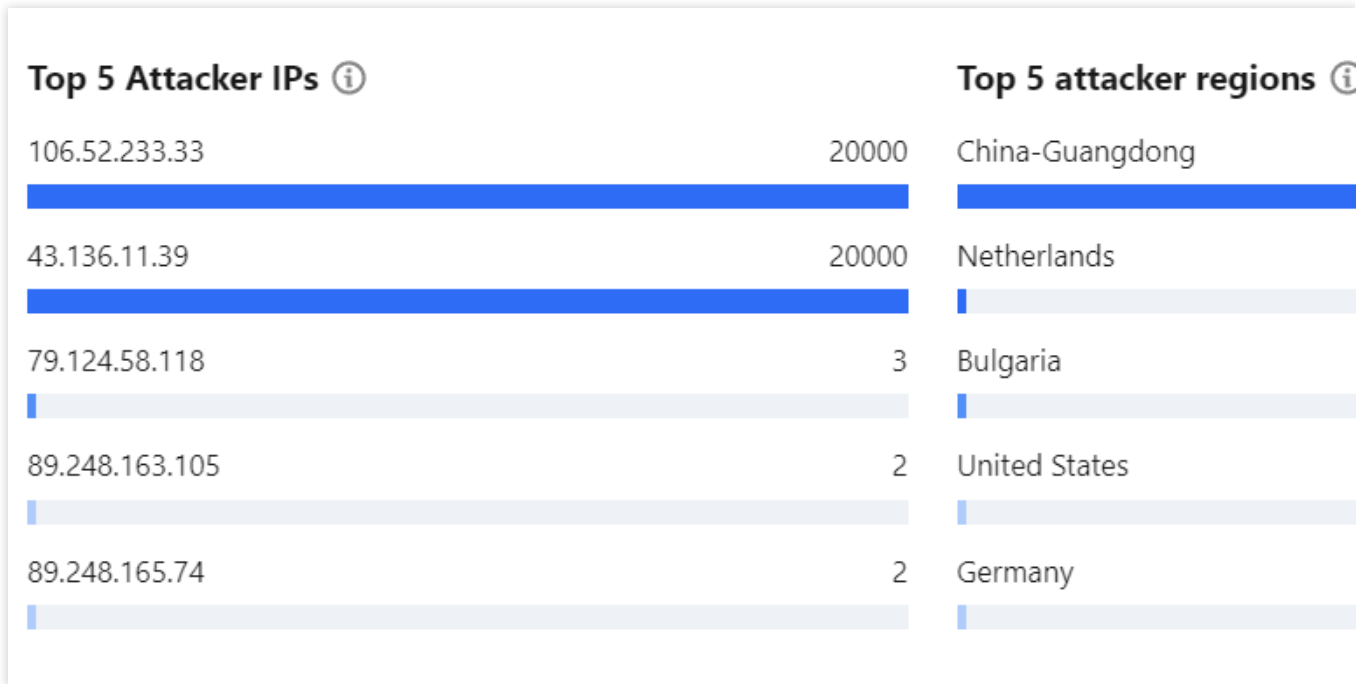
Attack traffic protocol distribution: It displays how attacks on the selected Anti-DDoS instance are distributed over different attack traffic protocols within the queried period.

Attack type distribution: It displays how attacks on the selected Anti-DDoS instance are distributed over different attack types within the queried period.

6. The **Top 5** sections of the event details page displays the top 5 attacker IP addresses and the top 5 attacker regions, which is helpful to precise protection configuration.

Note:

This section provides sampled data in the attack period.



7. In the **Attacker information** section of the event details page, you can view the sampled data of the attack period, including the attacker IP, region, total attack traffic, and total attack packets.

Note:

This section provides sampled data in the attack period.

Attacker information		
Attacker IP	Region	Total attack traffic
104.237.156.209	United States	44B
106.52.233.33	China-Guangdong	21.2 MB
139.162.144.109	Germany	40B

8. You can view the recent DDoS attacks in the **Recent events** section.

Select an event and click **View details**. You will see the attacker IP, source region, generated attack traffic, and attack packet size on the right, which can be used for attack and source analysis.

Recent Events						
Attack name	Anti-DDoS Resources	Instance Name	Defense Type	Attack time	Attack duration	Attack status
SYNFLOOD attacks			Anti-DDoS Basic	Started at: Ended at:	7 mins	Attack ended
SYNFLOOD attacks			Anti-DDoS Basic	Started at: Ended at:	5 mins	Attack ended

Select an event and click **Packet Download**. In the attack packet list, select an ID, and click **Download** to download the attack packet sample data, with which you can create a protection plan.

Attack Packet List		
ID	Time	Operation
	2023-08-10 20:50:04	Download
	2023-08-10 20:50:04	Download

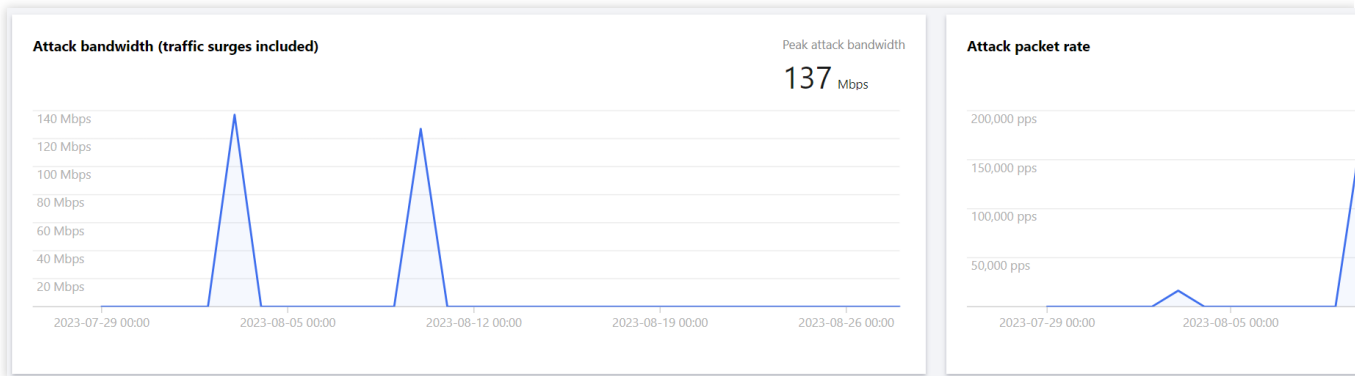
Total items: 2 10 / page 1 / 1 page

Viewing DDoS protection details

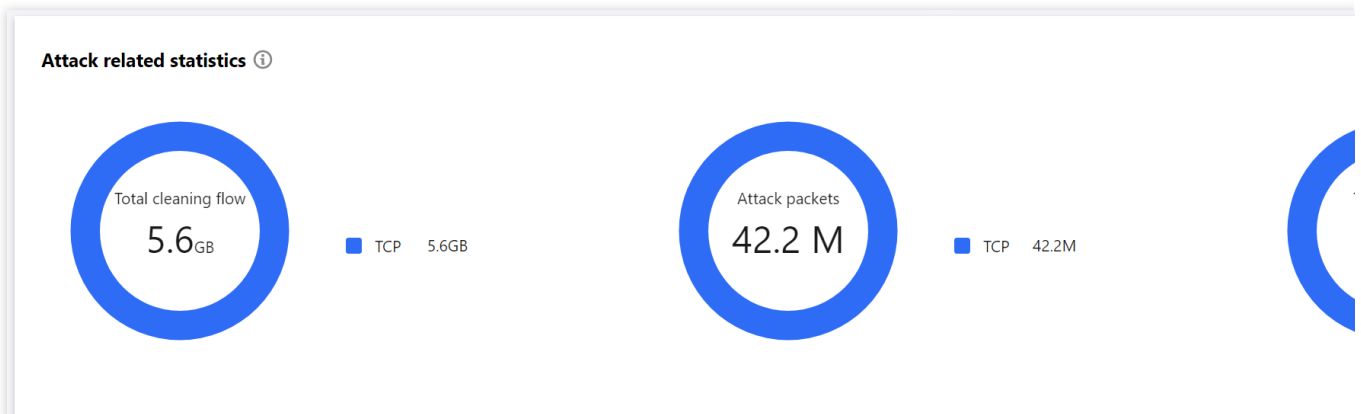
1. Log in to the new [Anti-DDoS console](#), click **Overview** on the left sidebar, and then click the **Attacks** tab.
2. In the **DDoS attack** tab, select a query period, target region, and an Anti-DDoS Pro instance to check whether the instance has been attacked. The complete attack data is displayed by default.

DDoS Attack		CC attack	
Anti-DDoS Pro	All regions	Please select	Last 1 hour Last 6 hours Today Last 7 days Last 15 days

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



4. In the **Attack statistics** section, you can view how the attacks are distributed across different attack traffic protocols, attack packet protocols, and attack types.



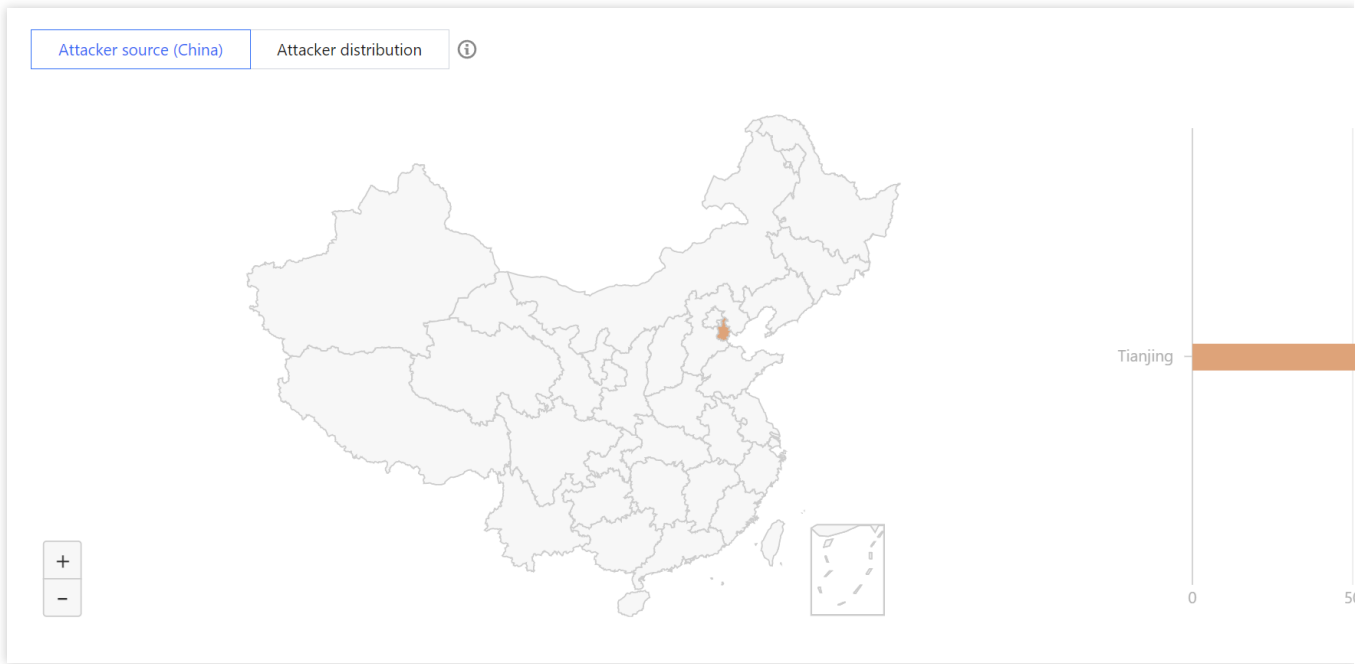
Parameter description:

Attack traffic protocol distribution: It displays how attacks on the selected Anti-DDoS instance are distributed over different attack traffic protocols within the queried period.

Attack packet protocol distribution: It displays how attacks on the selected Anti-DDoS instance are distributed over different attack packet protocols within the queried period.

Attack type distribution: It displays how attacks on the selected Anti-DDoS instance are distributed over different attack types within the queried period.

5. In the attack source section, you can view the distribution of DDoS attack sources in and outside the Chinese mainland within the queried period, so that you can take further protective measures.



Viewing CC protection details

1. In the **CC attack** tab, select a query period, target region, and an Anti-DDoS Pro instance to check whether the instance has been attacked.

Overview

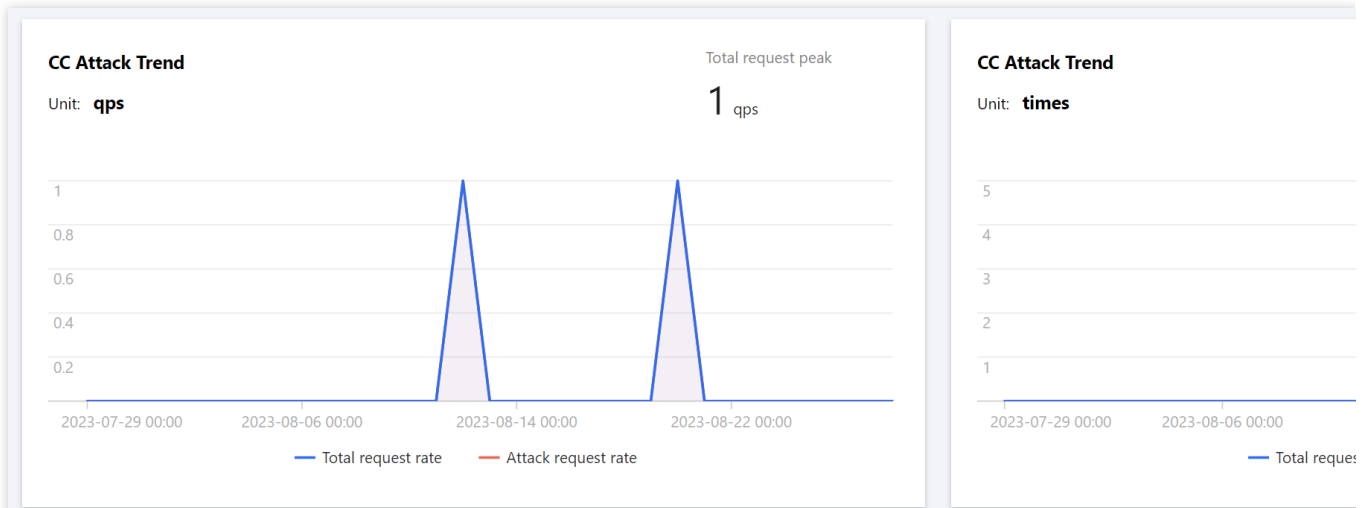
Protection Overview **Attacks**

DDoS Attack **CC attack**

Anti-DDoS Pro ▼

All regions ▼ Please select ▼ Last 1 hour Last 6 hours Today Last 7 days Last 15 days **Last 30 d**

2. You can select a query period to view the following data to identify the impact of attacks on your business.



Parameter description:

Total request rate: The rate of total traffic of requests received (in QPS).

Attack request rate: The rate of attack traffic (in QPS).

Total requests: The total number of requests received.

Attack requests: The number of attack requests received.

3. You can view recent CC attacks in the **Recent events** section. Click **View details** on the right of an event to display the attack start and end time, attacked domain name, total request peak, attack request peak, and attacker IP. You can also check the attack information, attack trends, and detailed CC records.

Usage Limits

Last updated : 2024-07-01 11:33:59

Anti-DDoS Basic

Scope

Free Anti-DDoS service for CVM, CLB, and NAT Gateway instances.

Anti-DDoS Pro

Scope

CVM, CLB, WAF, NAT Gateway, VPN Gateway, and Lighthouse instances.

Connection limits

An Anti-DDoS Pro instance can only be bound to Tencent Cloud public IPs in the same region.

Limit on access control list

For DDoS protection, up to 100 records (IPs + IP ranges) can be blocked or allowed in the access control list.

For CC protection, a URL allowlist is not supported.

Limit on regions

An Anti-DDoS Pro instance can only be bound to Tencent Cloud devices in the same region. Supported regions:

Beijing, Shanghai, Guangzhou, Hong Kong (China), Singapore, Seoul, Tokyo, Bangkok, and Frankfurt.

Note:

To purchase an Anti-DDoS Pro instance in regions outside the Chinese mainland, please [contact us](#).

Anti-DDoS Advanced

Applicable scope

IPs and domain names for website (layer-7) and non-website (layer-4) businesses in and outside Tencent Cloud.

Limits on the forwarding capability

By default, one Anti-DDoS Advanced instance supports a total of 60 forwarding rules (L4 + L7). At most, an Anti-DDoS Advanced instance can support 500 forwarding rules. For non-website (layer-4) protocols, each rule supports 20 real server IPs or domain names. For website (layer-7) protocols, each rule supports 16 real server IPs or domain names.

Note:

The total number of forwarding rules is the sum of forwarding rules for TCP/UDP and HTTP/HTTPS, and the maximum total number can be up to 500. For TCP and UDP, if the same forwarding port number is used, two different forwarding rules need to be configured.

Limit on access control list

Up to 100 IP addresses can be added to the blocklist and allowlist in total.

A URL allowlist is not supported.

Limit on regions

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

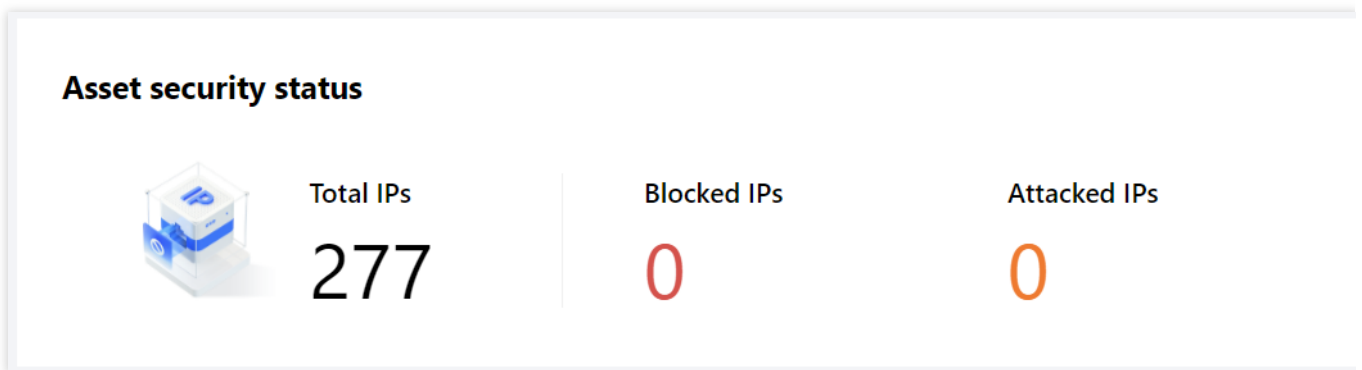
Asset Center

Cloud Assets

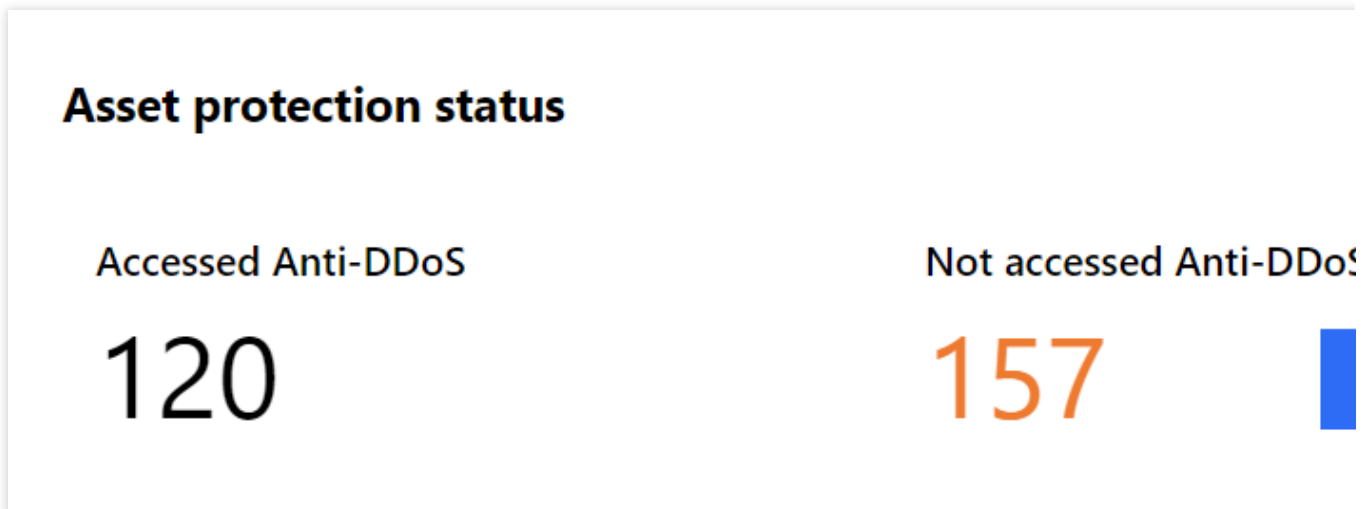
Last updated : 2024-07-01 11:33:59

Viewing asset security status

1. Log in to the new [Anti-DDoS console](#) and click **Cloud Assets** on the left sidebar.
2. In the **Asset security status** section, you can see the business IP security data.

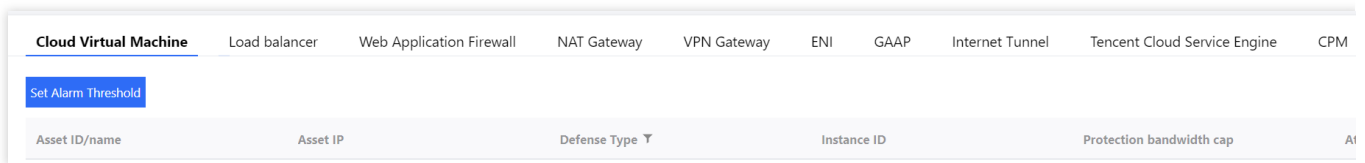


3. In the **Asset protection status** section, you can see the business IP protection data and directly connect to the Anti-DDoS service.



Viewing asset instance details

1. Log in to the new [Anti-DDoS console](#) and click **Cloud Assets** on the left sidebar.
2. Take CVM as an example. On the details page, you can view the detailed information of a CVM asset, including the asset name, asset IP, defense type, Anti-DDoS instance ID, protection bandwidth cap, and attack status.



Anti-DDoS can be activated for the following products:

Cloud Virtual Machine (CVM): This is a scalable cloud computing service that frees you from estimation of resource usage and upfront investment. With Tencent Cloud CVM, you can launch any number of CVM instances and deploy applications quickly.

Cloud Load Balancer (CLB): This is a service that distributes traffic to multiple CVM instances securely and quickly so as to eliminate single points of failure for higher availability.

Web Application Firewall (WAF): This is an AI-based, one-stop web service protection solution.

NAT Gateway: This is a service that supports IP address translation and provides the SNAT and DNAT capabilities. It provides secure and high-performance internet access for resources in virtual private clouds (VPCs).

VPN Connection: This is a transfer service based on network tunneling technology that brings about connectivity between local IDCs and resources on Tencent Cloud. It can help you quickly build a secure and reliable encrypted tunnel on the internet.

Cloud Bare Metal (CBM): This is an on-demand pay-as-you-go physical server rental service that provides high-performance, securely isolated physical server clusters for cloud users.

Bare Metal Cloud Load Balancer (Bare Metal CLB): It virtualizes multiple physical servers in the same availability zone into a high-performance and high-availability application service pool by setting a virtual IP (VIP) address.

Bare Metal Elastic IP (Bare Metal EIP): A Bare Metal EIP address is an IP address dedicated to dynamic cloud computing, and it is a public IP address that can be separately applied for.

Global Application Acceleration Platform (GAAP): This is a PaaS product that allows optimum access latency for businesses across the globe. Via high-speed connections, cluster forwarding, and intelligent routing among global nodes, it enables users in different regions to access the closest nodes and forwards traffic to the origin server, reducing access lag and latency.

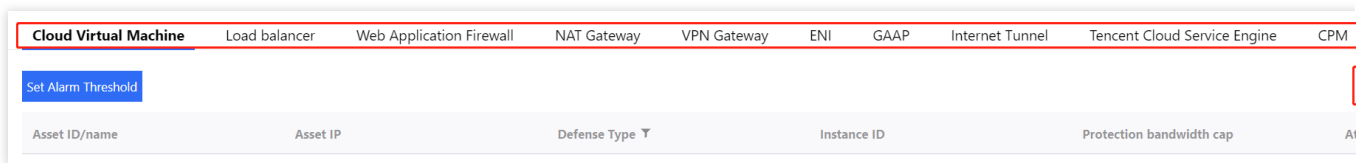
Elastic Network Interface (ENI): An ENI is used to bind a CVM instance within a VPC, and it can be freely migrated among CVM instances. ENIs can help configure and manage networks, as well as develop highly reliable network solutions.

Tencent Cloud Lighthouse: This is a new-gen, out-of-the-box cloud server service for small- and medium-sized enterprises (SMEs) and developers. It is designed for cloud-based lightweight use cases, such as websites, web applications, mini programs, mini games, apps, ecommerce, cloud storage, image hosting, and various development and testing environments. It is easier to use than traditional cloud server services and integrates common basic cloud

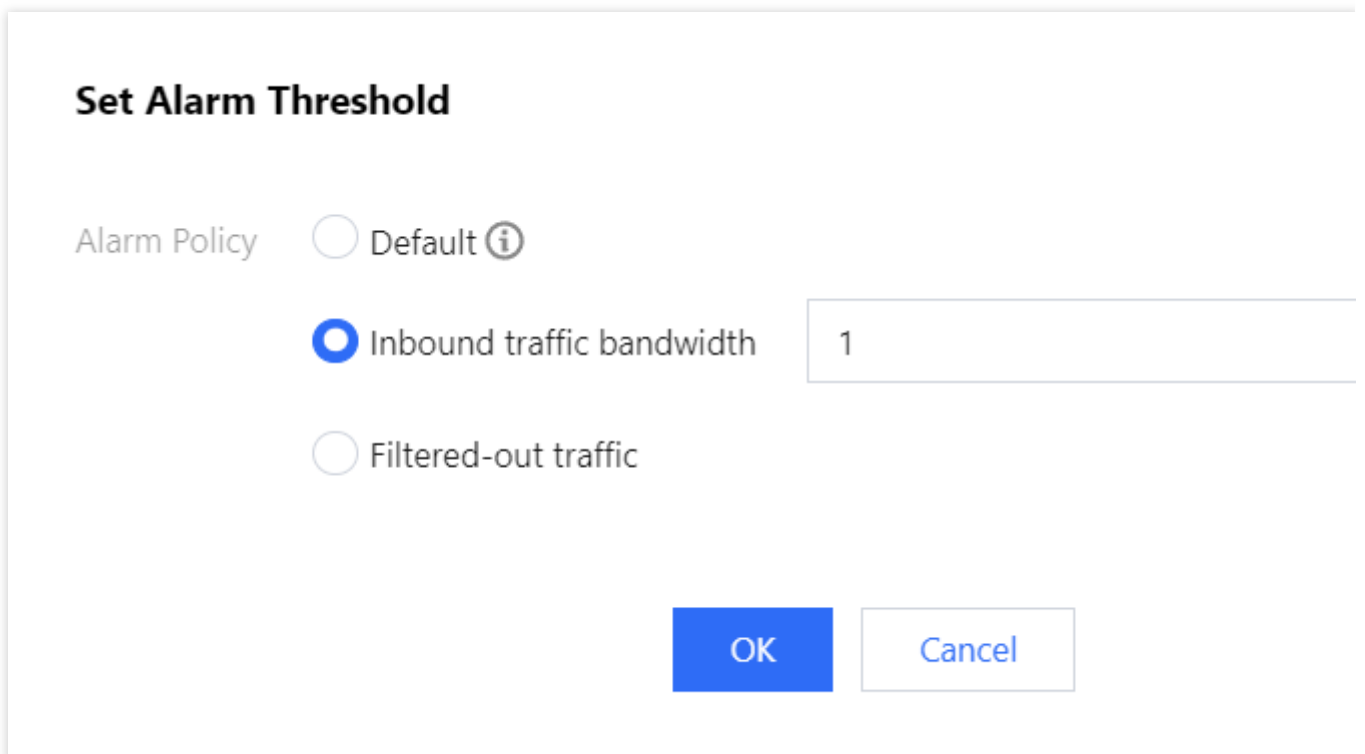
services into different high-bandwidth/traffic packages. Such packages contain popular open-source software programs, enabling you to build applications swiftly and enjoy a minimalist cloud experience.

Managing cloud assets

1. Log in to the new [Anti-DDoS console](#) and click **Cloud Assets** on the left sidebar.
2. Click a product tab and find the asset you want to manage. If there are many instances, you can use the search box in the top right corner for filtering.



3. After selecting the asset, you can perform the following operations on it:
Click **Set Alarm Threshold**, set an alarm policy as needed, and click **OK**.



The screenshot shows the 'Set Alarm Threshold' dialog box. The title is 'Set Alarm Threshold'. Under 'Alarm Policy', there are three radio button options: 'Default' (with an information icon), 'Inbound traffic bandwidth' (which is selected), and 'Filtered-out traffic'. To the right of the 'Inbound traffic bandwidth' option is a text input field containing the number '1'. At the bottom of the dialog, there are two buttons: 'OK' (blue) and 'Cancel' (white with a blue border).

Upgrade protection. When business growth requires the same Anti-DDoS instance to protect multiple business IPs, you can upgrade protection to cover all business IPs. For more information, see [Upgrading Protection](#).

Click **Attack analysis** to view the attack data.

Click **Configurations** to view the DDoS protection configurations.

云上防护实例

Viewing Instance Information

Last updated : 2024-07-01 11:33:59

1. Log in to the new [Anti-DDoS console](#) and click **Anti-DDoS Instances** on the left sidebar.
2. On the **Anti-DDoS Instances** page, you can view the basic information (such as the base protection bandwidth and running status) of your purchased Anti-DDoS Pro instances and the basic information and elastic protection configuration of your purchased Anti-DDoS Advanced instances.

Directions

The following shows you how to view the information of the Anti-DDoS Pro instance "bgp-0000jt3".

1. Log in to the new [Anti-DDoS console](#) and click **Anti-DDoS Instances** on the left sidebar.
2. On the **Anti-DDoS Instances** page, select a region or protection package in the top right corner. Find and click the instance ID "bgp-0000jt3" to view the instance details. If there are many instances, you can use the search box in the top right corner for filtering.

Instance ID/name...	Instance type	IP Protocol	Resources ⓘ	Specifications	Specifications	Defense Status ⓘ	Instance status
bgp-0000jt3		IPv4		Region: [redacted] Package type: [redacted] application bandwidth: [redacted] Protected IPs/Quota: 0/300	Protection bandwidth cap: [redacted]	Port protection: Medium ↕	Running

3. On the pop-up page, you can view the following information:

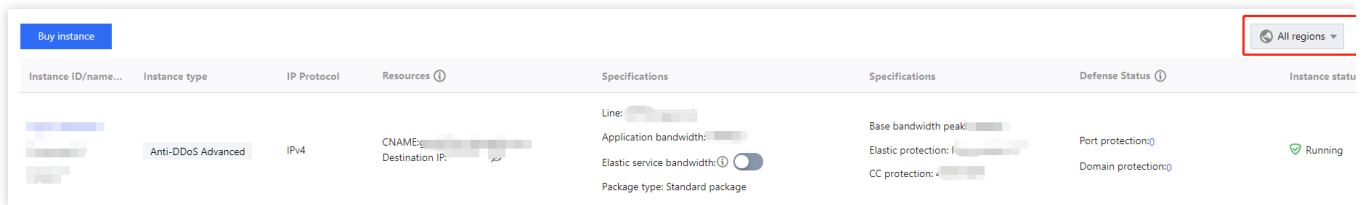
Basic information	
Anti-DDoS Pro instance name	[redacted]
Region	[redacted]
Bound IP	[redacted]
Application bandwidth	[redacted]

Parameter	Description
Instance name	The name of the Anti-DDoS Pro instance for easier instance identification and management. You can set a custom instance name containing 1-20 characters of any type as needed.

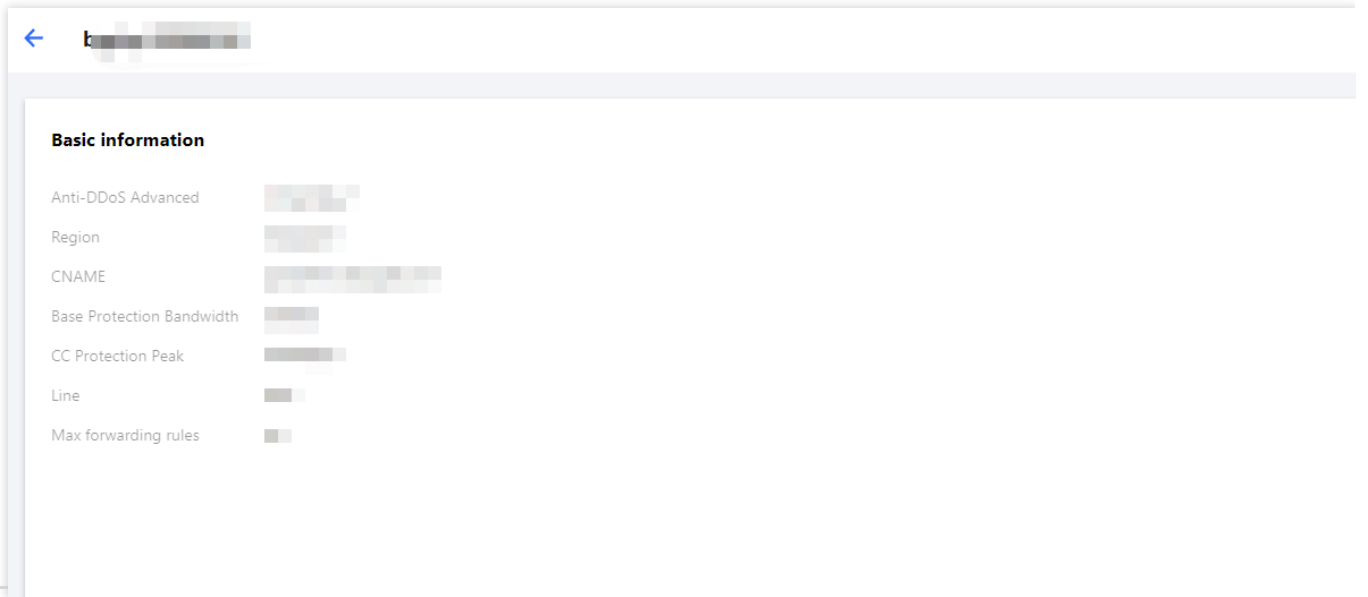
Region	The region selected when the Anti-DDoS Pro instance is purchased.
Current status	<p>The current status of the Anti-DDoS Pro instance, such as Running, Cleansing, and Blocked.</p> <p>Creating: The instance is being created.</p> <p>Running: The instance is providing protection.</p> <p>Attacked: Under attacks.</p> <p>Blocked: The instance is blocked.</p> <p>Unblocking: The instance is being unblocked.</p> <p>Reclaiming: The instance has expired and is being repossessed.</p>
Expiration time	It is calculated based on the purchase period selected at the time of purchase and the specific time of payment, accurate to the second. Within seven days before the expiration of an Anti-DDoS resource, Tencent Cloud will push expiration reminders to the account creator and all collaborators via Message Center, SMS, email, or WeChat (subject to your configuration in the Message Center).

The following shows you how to view the information of an Anti-DDoS Advanced instance.

1. Log in to the new [Anti-DDoS console](#) and click **Anti-DDoS Instances** on the left sidebar.
2. On the **Anti-DDoS Instances** page, click the ID of the Anti-DDoS Advanced instance that you want to view the details. If there are many instances, you can use the search box in the top right corner for filtering.



3. On the pop-up page, you can view the following information:



Parameter	Description
Instance name	The name of the Anti-DDoS Advanced instance for easier instance identification and management. You can set a custom instance name containing 1-20 characters of any type as needed.
Destination IP	The protective IP of the Anti-DDoS Advanced instance. It may change from time to time. To avoid DNS resolution failure, you are recommended to change the DNS resolution address to the assigned CNAME.
Region	The region selected when the Anti-DDoS Advanced instance is purchased.
Current status	The current status of the Anti-DDoS Advanced instance, such as Running , Cleansing , and Blocked .
CNAME	The CNAME of the Anti-DDoS Advanced instance. The CNAME will be resolved to the protective IP that forwards cleansed traffic to the real server. To avoid DNS resolution failure, you are recommended to change the DNS resolution address to the assigned CNAME.
Base protection bandwidth	The base protection bandwidth you select when you purchase the instance. If elastic protection is not enabled, base protection bandwidth is the maximum bandwidth of the instance.
Expiration time	It is calculated based on the purchase period selected at the time of purchase and the specific time of payment, accurate to the second. Within seven days before the expiration of an Anti-DDoS resource, Tencent Cloud will push expiration and renewal reminders to the account creator and all collaborators via Message Center, SMS, or email (subject to your configuration in the Message Center).
Tag	The tag name of the Anti-DDoS Advanced instance, which can be edited and

	deleted.
Forwarding IP range	The IPs that forward cleansed traffic back to the real server.

Managing Protected Objects

Last updated : 2024-07-01 11:33:59

Anti-DDoS Pro provides Tencent Cloud public IPs with stronger anti-DDoS capability. It supports Tencent Cloud services such as CVM, CLB, NAT, and WAF.

You can add protected IPs to or delete them from Anti-DDoS Pro instances as needed.

Prerequisite

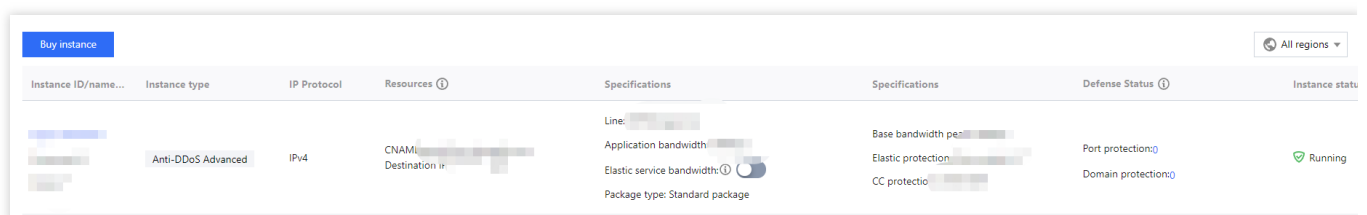
To set protected IPs, you need to purchase an [Anti-DDoS Pro instance](#) first.

Note:

An Anti-DDoS Pro (Enterprise) instance takes effect only after it is bound to an Anti-DDoS EIP. You need to change your IP to an Anti-DDoS EIP. The instance must be located in the same region with the bound cloud resource. For more information, see [Creating an Anti-DDoS EIP](#).

Directions

1. Log in to the new [Anti-DDoS console](#) and click **Anti-DDoS Instances** on the left sidebar.
2. Click the **Protected Resource** on the right of the target Anti-DDoS Pro instance.



The screenshot shows a table of Anti-DDoS Pro instances. The table has columns for Instance ID/name, Instance type, IP Protocol, Resources, Specifications, Specifications, Defense Status, and Instance status. A 'Buy instance' button is visible in the top left, and 'All regions' is in the top right. The table contains one row with the following details:

Instance ID/name...	Instance type	IP Protocol	Resources	Specifications	Specifications	Defense Status	Instance status
[Redacted]	Anti-DDoS Advanced	IPv4	CNAME: [Redacted] Destination IP: [Redacted]	Line: [Redacted] Application bandwidth: [Redacted] Elastic service bandwidth: [Redacted] Package type: Standard package	Base bandwidth per: [Redacted] Elastic protection: [Redacted] CC protection: [Redacted]	Port protection: [Redacted] Domain protection: [Redacted]	Running

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

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

Note:

An Anti-DDoS Pro (Enterprise) instance takes effect only after it is bound to an Anti-DDoS EIP.

Select instance: To add one or more resource instances for protection, tick the checkbox for the resource ID. The number of selected resource instances cannot exceed the maximum number of bound IPs.

Selected: To delete a selected resource instance, click **Delete** on the right of it.

Configurations

DDoS Protection Logic

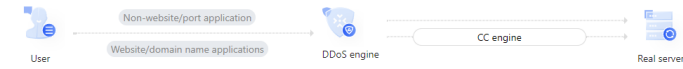
The policy takes effect on all traffic that passes through Anti-DDoS Pro, and the hit rule executes the protection action.

The effective priority of different policy types is:

IP Blocklist/Allowlist > Port Filtering > Block by protocol > Connection Attack Protection > Watermark Protection > Feature Filtering > Block by location > IP/Port Speed Limit

Protection Flow

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



CNAME

Instance

Protected Application

DDoS protection level

Anti-DDoS collects and analyzes the characteristics of history attacks, blocks messages that do not comply with the protocol specifications, and blocks abnormal TCP connections. In Loose Mode, only suspicious messages are blocked. In Strict mode, all suspicious messages are blocked. If attack messages failed to be blocked in the Strict mode, or the normal messages are blocked in Loose mode, please contact our technical support.

Strict Medium Loose

Protection subpolicy

IP Blocklist/Allowlist

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

Configured 0 blocklists, 0 allowlists Set

Port filtering

Block or allow traffic t

Configured 0 rules Set

Protocol blocking

Block requests of the specified protocol according to the traffic to Anti-DDoS. If your application does not use UDP, it's recommended to block all UDP requests.

Configured 0 rules Set

Watermark Protection

The application end a from the client is emb

Enabled 0 rules Set

Connection attack protection

Set refined protection policies targeting connection attacks

Configured 0 rules Set

AI Protection

The AI engine learns t CC attacks, and can et

Defense status:

Regional blocking

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

Configured 0 rules Set

IP/Port rate limit

Controls access to the

Configured 0 rules Set

Feature Filtering

Configure custom blocking rules based on specific IP, TCP, UDP, message header, and content.

Note:

- Unbinding a blocked IP from Anti-DDoS Pro instances is not allowed.
- Searching for and selecting more than one associated cloud resource at once is supported.
- CLB and CVM instances that are detected terminated will be unbound.
- 4. Click **OK**.

Setting Instance Names and Tags

Last updated : 2024-07-01 11:33:59

When multiple Anti-DDoS Pro or Anti-DDoS Advanced instances are used, you can set a name for them to quickly identify and manage them.

Prerequisite

You have purchased an Anti-DDoS Pro or Anti-DDoS Advanced instance.

Directions

Method 1




1. Log in to the new [Anti-DDoS console](#) and click **Anti-DDoS Instances** on the left sidebar.
2. Click the



icon on the second row in the **Instance ID/name/tag** column of the target instance and enter a name.




Note:

The name can contain 1-20 characters of any type.

Instance ID/name...	Instance type	IP Protocol	Resources ⓘ	Specifications	Specifications	Defense Status ⓘ	Instance status ▾
Unname  None 		IPv4		Region: Package type: application bandwidth: Protected IP/Quota:	Protection bandwidth cap:	Port protection:	 Running

Method 2

1. Log in to the new [Anti-DDoS console](#) and click **Anti-DDoS Instances** on the left sidebar.
2. Click the ID of the target instance in the **Instance ID/name/tag** column to enter its basic information page.

Instance ID/name...	Instance type	IP Protocol	Resources ⓘ	Specifications	Specifications	Defense Status ⓘ	Instance status
bc 		IPv4		Region: Package type: 1 application bandwidth: ps Protected IPs/Quota: 0/300	Protection bandwidth cap:	Port protection: Medium 	 Running

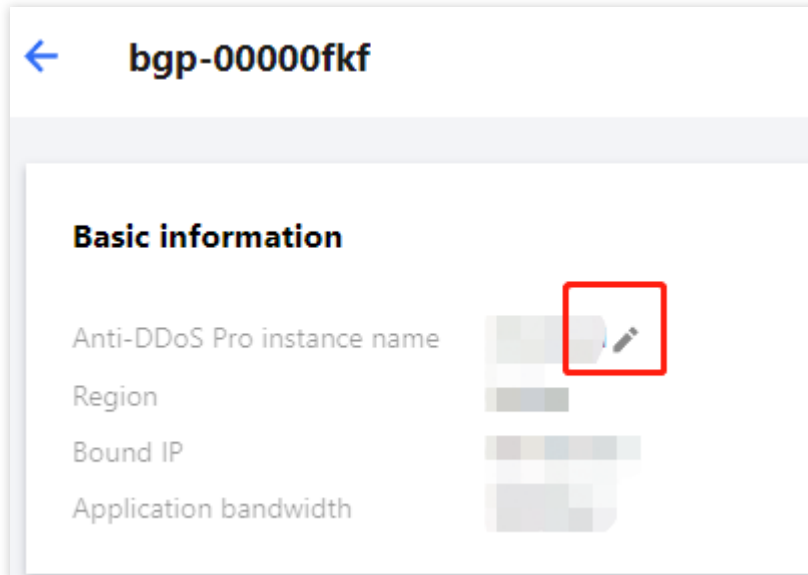
3. Click the



icon on the right of the instance name and enter a name.

Note:

The name can contain 1-20 characters of any type.



Modifying Elastic Protection Bandwidth

Last updated : 2024-07-01 11:33:59

Elastic protection bandwidth refers to the maximum bandwidth that an Anti-DDoS instance can provide to deal with attack traffic. Once the attack traffic exceeds the maximum protection bandwidth, the attacked IP is blocked.

Prerequisite

Purchase an [Anti-DDoS Advanced instance](#).

Directions

1. Log in to the new [Anti-DDoS console](#) and click **Anti-DDoS Instances** on the left sidebar.
2. In the **Specifications** column of the target Anti-DDoS Advanced instance row, click the



icon on the right of **Elastic Protection**.

Instance ID/name...	Instance type	IP Protocol	Resources ⓘ	Specifications	Specifications	Defense Status ⓘ	Instance status
[Redacted]	Anti-DDoS Advanced	IPv4	CNAM: [Redacted] Destination IP: [Redacted]	Line: [Redacted] Application bandwidth: 50Mbps Elastic service bandwidth: ⓘ <input type="checkbox"/> Package type: Standard package	Base bandwidth peak: 20Gbps Elastic protection: Not enabled ⓘ ✎ CC protection: 40000 QPS	Port protection: ⓘ Domain protection: ⓘ	Running
[Redacted]	Anti-DDoS Advanced	IPv4	CNAM: [Redacted] Destination IP: [Redacted]	Line: [Redacted] Application bandwidth: 100Mbps Elastic service bandwidth: ⓘ <input type="checkbox"/> Package type: Standard package	Base bandwidth peak: 30Gbps Elastic protection: Not enabled ⓘ CC protection: 40000 QPS	Port protection: ⓘ Domain protection: ⓘ	Running

3. In the **Configure elastic protection** pop-up window, select an elastic protection bandwidth as needed.

Configure elastic protection

ID/Instance name: bgpip-00000561 / Unnamed

Base Protection: 20Gbps

Elastic Protection Bandwidth: 30Gbps 40Gbps 50Gbps 60Gbps 70Gbps 80Gbps 90Gbps 100Gbps 150Gbps

Billing: Elastic protection is not triggered and is not charged.
 If the bandwidth peak of the day when the attack occurs exceeds 20Gbps, the fee will be calculated by the billing tier where the bandwidth peak falls into.
 The billing tier is as follows

Elastic Protection Bandwidth(Gbps)	20~30	30~40	40~50	50~60	60~70	70~80	80~90	90~100	100~120	120~150	150~200
0>Elastic protection fee (USD/day)	400	700	800	1200	1800	2200	2500	2700	2900	3200	4000

Note: Elastic protection bandwidth and corresponding fees may vary by region and edition. The specific information is displayed in the console.

4. Click **OK**.

Unblocking Protected IPs

Last updated : 2024-07-01 11:33:59

Anti-DDoS allows you to manually unblock blocked IPs in the new [Anti-DDoS console](#).

Chances for manual unblocking

Each Anti-DDoS Pro or Anti-DDoS Advanced user has three chances of manual unblocking every day. The system resets the chance counter daily at 00:00 midnight. Unused chances will not be carried over to the next day.

Note:

Before unblocking an IP, please check the estimated unblocking time which may be affected by some factors and will be postponed. If you accept the estimated time, you do not need to operate manually.

If your manual unblocking chances are used up for the day, you can increase the number of protected IPs and times of protection to defend against high-traffic attacks and avoid continuous blocking.

Directions for manual unblocking

1. Log in to the new [Anti-DDoS console](#) and click **Unblocking Service** on the left sidebar.
2. Find the protected IP in the **Auto unblocking** status and click **Unblock** in the **Operation** column on the right.

Unblocking records

1. Log in to the new [Anti-DDoS console](#), click **Unblocking Service** on the left sidebar, and then click the **Unblocking records** tab.
2. You can check all unblocking records in a specified period, including records of automatic unblocking and manual unblocking.

Total blocking times	Blocked IPs	Manual unblocking quota	Available daily quota	Manual unblockings
130	0 times	3	3	13

Blocked IPs **Unblocking records**

Last 24 hours Last 7 days Last 30 days **Last 90 days** 2023-06-02 00:00 ~ 2023-08-31 23:59

IP	Defense Type	Blocking time	Actual unblocking time
[REDACTED]	Anti-DDoS Pro	2023-08-17 19:46:00	2023-08-18 07:46:02
[REDACTED]	Anti-DDoS Basic	2023-08-17 19:46:00	2023-08-18 07:46:02

Business Connection Quick IP Connection

Last updated : 2024-07-01 11:33:59

Note:

Quick IP access allows you to quickly bind an Anti-DDoS Pro instance to a cloud asset. Note that for an Anti-DDoS Pro (Enterprise) instance, you need to first unbind the cloud asset from the original public IP and bind it to an EIP in the CVM console. If you want to hide the IP of the real server, please select access via port or access via domain name.

Prerequisite

You have purchased an [Anti-DDoS Pro instance](#) .

Directions

1. Log in to the new [Anti-DDoS console](#), click **Business Access** on the left sidebar, and then click the **Quick IP access** tab.
2. On the **Quick IP access** tab, click **Start Access**.
3. In the pop-up page, select an Anti-DDoS instance and resource instances as needed.

IP access

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

Select an instance

Region

Plan information Standard Package (BGP)

Protected IPs 1 remaining to protect/total 1

Application bandwidth

Protected Asset Type

Select instance ⓘ

Please enter IP or name (exact search is supported, fuzzy search is no)

<input type="checkbox"/>	Resource ID/Name	IP address	Resource type
<input type="checkbox"/>			

Total items: 0 10 / page 1 / 1 page

Selected (0)

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

You can make multiple selection by holding down the Shift key

Note

Unbinding a blocked IP from an Anti-DDoS Pro instance is not allowed.

Searching for and selecting more than one associated cloud resource at once is supported.

CLB and CVM instances that are detected terminated will be unbound.

4. Click **OK**.

Domain Name Connection

Last updated : 2024-07-01 11:33:59

Note:

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

Connecting a rule

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

Application Accessing

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

Access via Domain Name

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

Start Access Batch import Batch export Batch delete

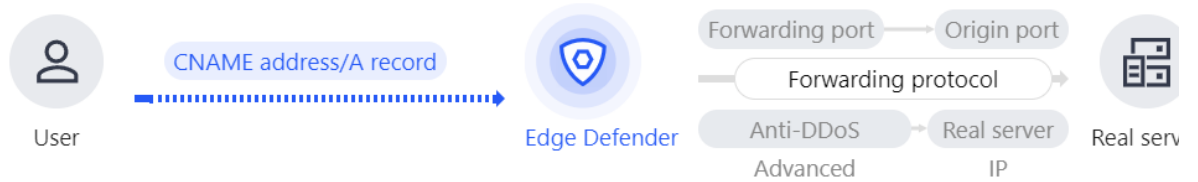
3. In the pop-up window, select an associated instance ID and click **Next: Set Protocol Port**.

Note:

You can select multiple instances.

Access via Domain Name

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



* Associated Instance

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

Access via Domain Name

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



* Forwarding protocol

 http

80

 https

443

 Forward via HTTP for HTTPS requests

* Select certificate

Please select

Certificate source

Tencent Cloud-managed certificate [SSL certificate management](#)

(The certificate can protect confidential data against theft and tampering, including user information and financial information)

* Application domain name

The domain name cannot exceed

Recommended to enable protection configuration

 CC Protection + CC AI Protection ⓘ

5. Select a forwarding method, specify a real server IP & port or real server domain name, and add an alternate real server and set the weight if you have one. Then click **Next: Modify DNS Resolution**.

Note:

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

Access via Domain Name

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

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

* Real Server IP & Port

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

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

6. Click **Complete**. Connected rules will be displayed in the access list. You can check whether they are connected successfully in **Access status**.

Note:

When the connection fails due to certification configuration errors, you will get a prompt "Failed to obtain the certificate. Please go to [SSL Certificate Management](#) to view details".

To avoid seconds of interruptions, update the certificate for connected domain names during off-peak periods.

<input type="checkbox"/>	http	80	Disable	Configure ⓘ	Unavailable	Failed to configure
--------------------------	------	----	---------	-------------	-------------	---

Editing a rule

1. On the [Access via domain name](#) page, select the rule you want to edit and click **Configure** in the **Operation** column.

<input type="checkbox"/>	Application do...	Forwarding prot...	Forwarding port	Real server IP/Site	Associate high defense r...	Health check	Session persiste...	Access Status
<input type="checkbox"/>			80			Disable Configure ⓘ	Disable Edit	✔ Success
<input type="checkbox"/>			80			Disable Configure ⓘ	Unavailable	✔ Success

2. On the **Configure layer-7 forwarding rule** page, modify parameters and click **OK** to save changes.

Configure layer-7 forwarding rule

Associate high defense resources ⓘ
Up to 60 rules can be added, 1 added now

Domain name Enter a domain name containing up to 67 characters.

Protocol http https ✔

Forward via HTTP for HTTPS requests

Certificate source Tencent Cloud-managed certificate [SSL certificate management](#)

Certificate

Set Forwarding Method

Real server IP

Real server IP	Origin port	
<input type="text" value=""/>	<input type="text" value=""/>	Delete

[+ Add](#)

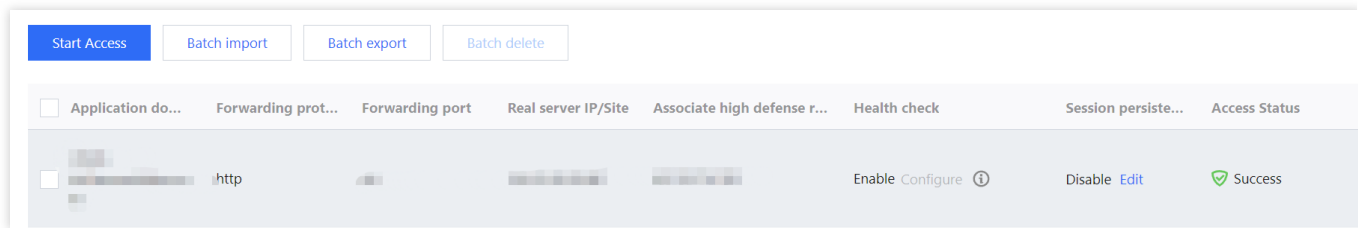
Please enter the combination of real server IP and port. Up to 16 entries are allowed.

Alternate Real Server

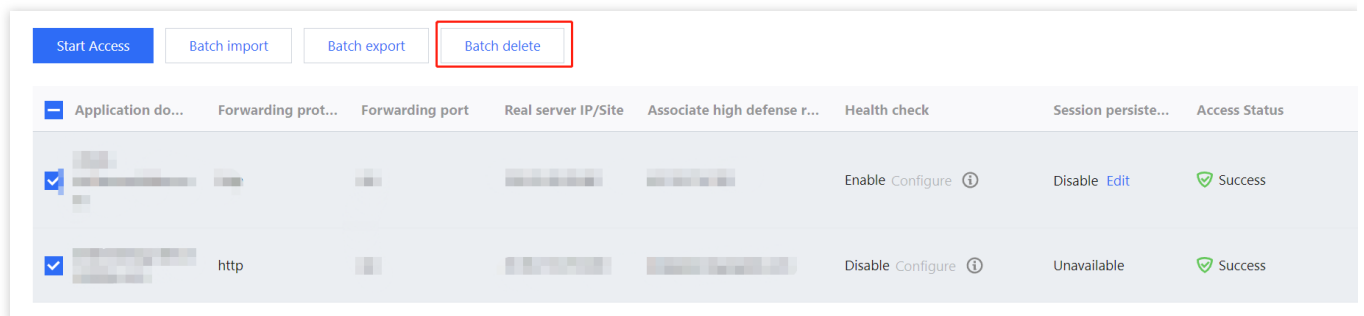
Deleting a rule

1. On the [Access via domain name](#) page, you can delete one or more rules.

To delete a rule, select the rule you want to delete and click **Delete** in the **Operation** column.



To delete multiple rules, select more than one rule and click **Batch delete**.



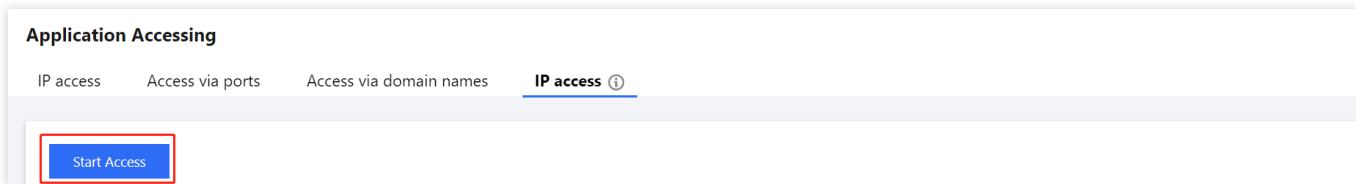
2. In the pop-up window, click **Delete**.

IP Connection

Last updated : 2024-07-01 11:33:59

Connecting a rule

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



3. In the **Associate Anycast IP** field, select an Anycast IP.

IP access

Associate Anycast IP

Search by IP or name

Instance type Cloud Virtual Machine Load balancer Hong Kong (China) ▼

Enter the instance ID/IP

Instance ID/name

Availability zone

Private IP

No data yet

Total items: 0

10 ▼ / page



Deleting a rule

1. On the [IP access page](#), click **Delete** in the **Operation** column of the rule that you want to delete.

Start Access

Instance ID/name	Anycast Anti-DDoS Advanced	Protected resource type	Protected Resource ID/Name	Defense Status	Binding status
[REDACTED]	[REDACTED]	Cloud Virtual Machine	[REDACTED]	• Running	• Bound
[REDACTED]	[REDACTED]	Cloud Virtual Machine	[REDACTED]	• Running	• Bound

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

Port Connection

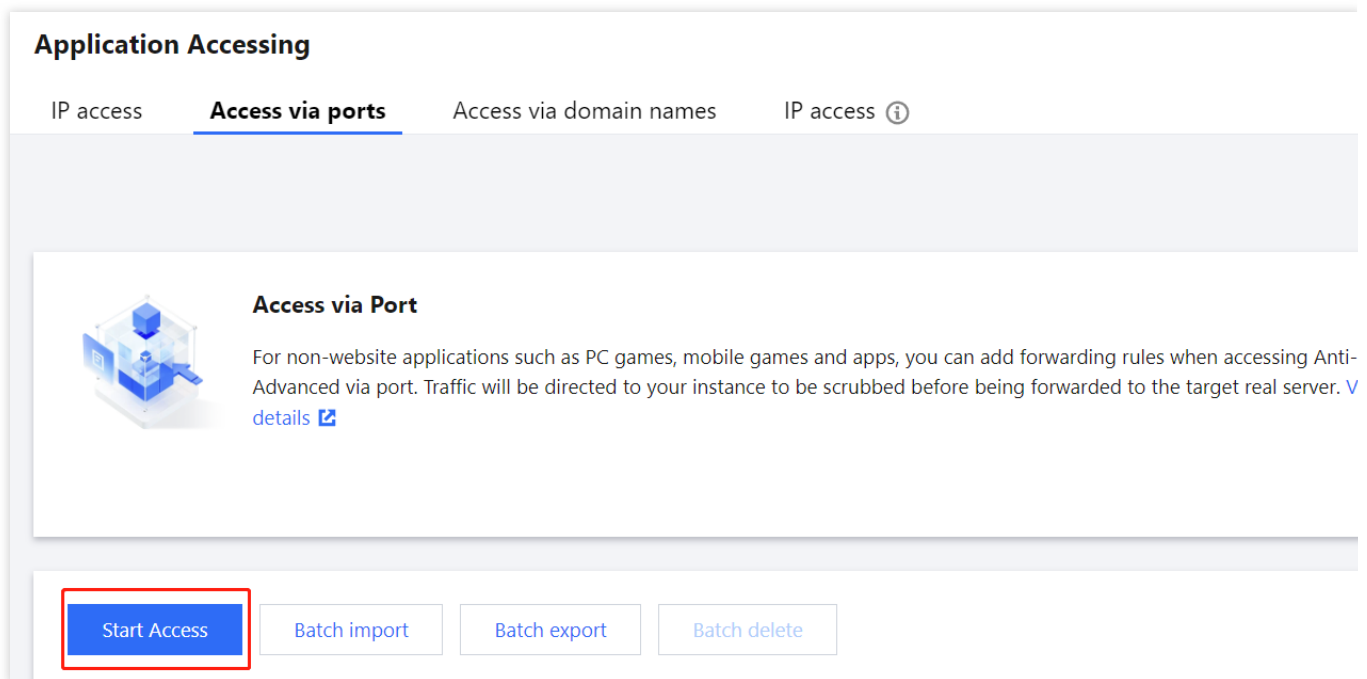
Last updated : 2024-07-01 11:33:59

Note:

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

Connecting a rule

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



The screenshot shows the 'Application Accessing' interface. At the top, there are four tabs: 'IP access', 'Access via ports' (which is selected and underlined), 'Access via domain names', and 'IP access' with an information icon. Below the tabs, there is a section titled 'Access via Port' with a blue icon of a server and a lock. The text below the icon reads: 'For non-website applications such as PC games, mobile games and apps, you can add forwarding rules when accessing Anti-Advanced via port. Traffic will be directed to your instance to be scrubbed before being forwarded to the target real server. [View details](#)'. At the bottom of the page, there are four buttons: 'Start Access' (highlighted with a red border), 'Batch import', 'Batch export', and 'Batch delete'.

3. In the pop-up window, select an associated instance ID and click **Next: Set Protocol Port**.

Note:

You can select multiple instances.

Access via Port

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

* Associated Instance

4. Select a forwarding protocol, specify a forwarding port and real server port, and then click **Next: Set Forwarding Method**.

Access via Port

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

* Forwarding protocol TCP UDP

* Forwarding port

* Origin port

5. Select a forwarding method, specify a real server IP & port or real server domain name, and add an alternate real server and set the weight if you have one. Then click **Next: Modify DNS Resolution**.

Access via Port

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

User → CNAME address/A record → Edge Defender → Forwarding port ↔ Origin port → Real server
 Edge Defender ↔ Forwarding protocol ↔ Real server
 Anti-DDoS Advanced → Real server IP

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

* Real Server IP & Weight

Real server IP	Weight ⓘ	
<input type="text" value="Enter the real server (eg: 1.1.1.1)"/>	<input type="text" value="0-100"/>	Delete
+ Add		

Please enter the combination of real server IP + weight. It supports up to 20 entries.

Note:

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

If the forwarding port you specify in the second step **Set Protocol Port** is occupied, you cannot proceed to the next step.

6. Click **Complete**.

Editing a rule

1. On the [Access via port](#) page, select the rule you want to edit and click **Configure** in the **Operation** column.

<input type="checkbox"/>	Forwa...	Forwa...	Origin port	Origin	Associate high defense re...	Load balancing mode	Health check	Session persistenc
<input type="checkbox"/>	UDP						Disable Edit ⓘ	Disable Edit
<input type="checkbox"/>	TCP						Disable Edit ⓘ	Disable Edit

2. On the **Configure layer-4 forwarding rule** page, modify parameters and click **OK** to save changes.

Configure layer-4 forwarding rule



Important

CC Attack Protection is not available for port-accessed applications. To use CC Attack Protection domain names".

Associate high defense resources

Up to 60 rules can be added, 20 added now

Forwarding protocol

UDP

Forwarding port

Origin port

Set Forwarding Method

Forwarding via IP Forwarding via domain name

Load balancing mode

Weighted round robin

Real Server IP & Weight

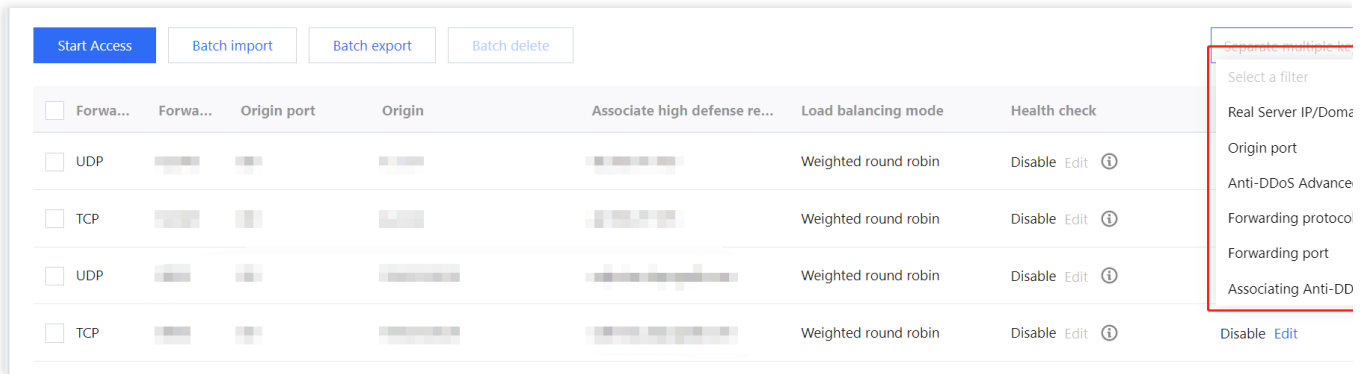
Real server IP	Weight
<input type="text"/>	<input type="text"/>
+ Add	

Please enter the combination of real server IP + weight. It supports

Alternate Real Server

Querying a rule

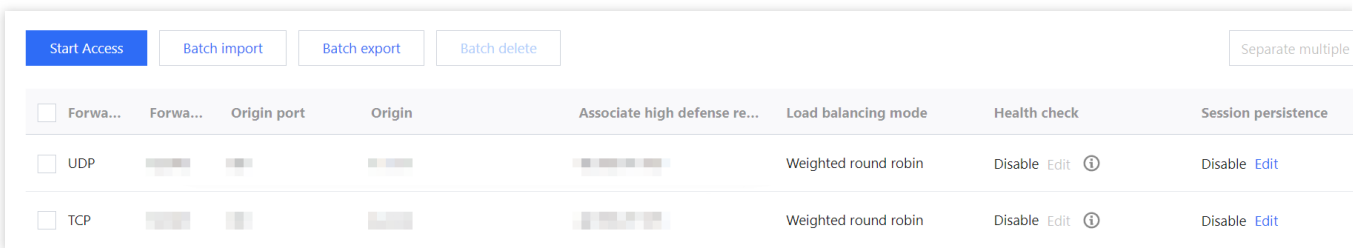
On the [Access via port](#) page, enter a real server IP/domain name, real server port, forwarding protocol, forwarding port, or an associated instance or associated CNAME resource in the search box.



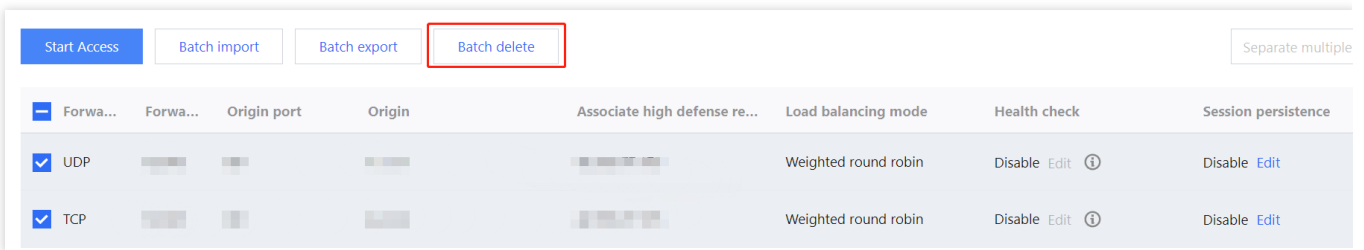
Deleting a rule

1. On the [Access via port](#) page, you can delete one or more rules.

To delete a rule, select the rule you want to delete and click **Delete** in the **Operation** column.



To delete multiple rules, select more than one rule and click **Batch delete**.



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

Configuring Session Persistence

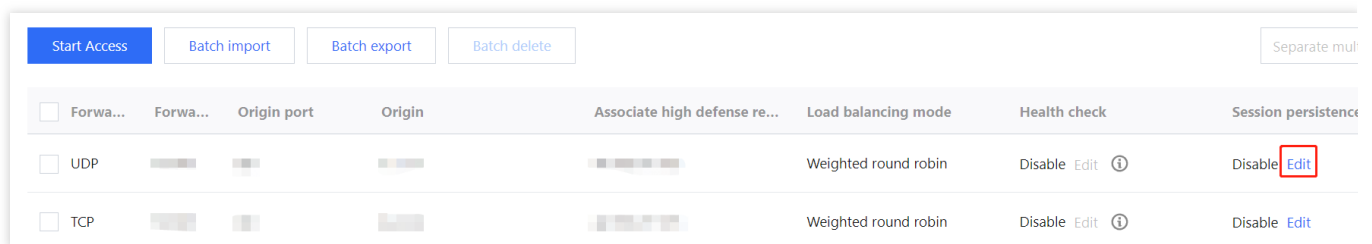
Last updated : 2024-07-01 11:33:59

For non-website services, Anti-DDoS Advanced provides IP-based session persistence, which can forward requests from the same IP address to the same backend server for processing.

Layer-4 forwarding supports simple session persistence. The session persistence period can be 30 to 3600 seconds. If there is no new request in this period, the connection will be disconnected.

Directions

1. Log in to the new [Anti-DDoS console](#), click **Business Access** on the left sidebar, and then click the **Access via port** tab.
2. Select an Anti-DDoS Advanced instance and rule. Then click **Edit** in the **session persistence** column.

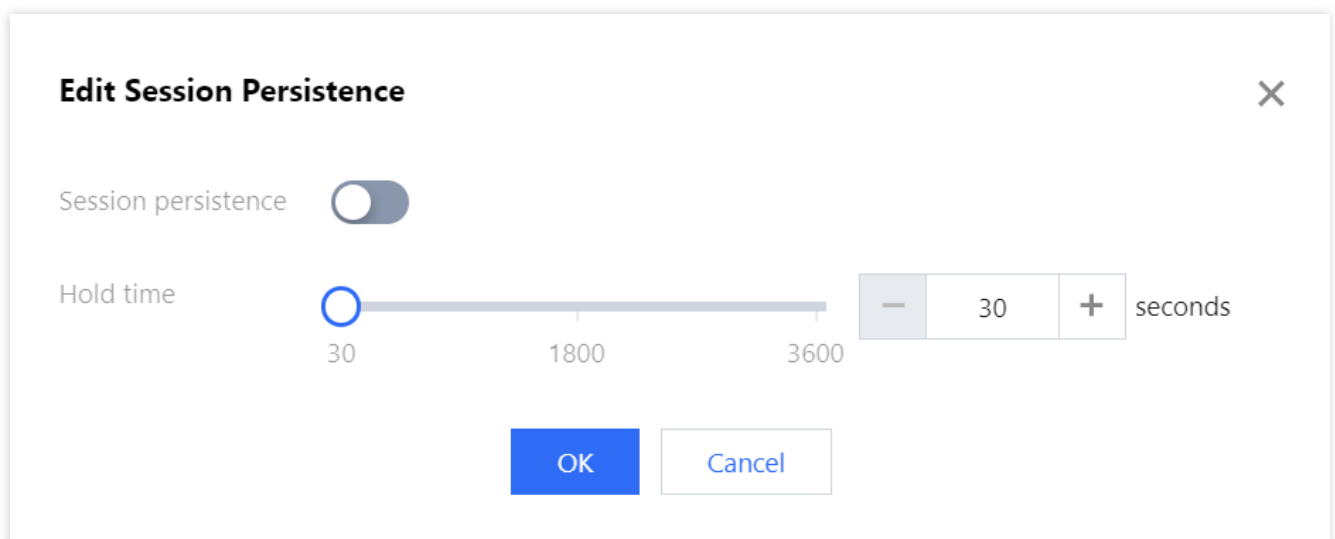


<input type="checkbox"/>	Forwa...	Forwa...	Origin port	Origin	Associate high defense re...	Load balancing mode	Health check	Session persistence
<input type="checkbox"/>	UDP					Weighted round robin	Disable Edit ⓘ	Disable Edit
<input type="checkbox"/>	TCP					Weighted round robin	Disable Edit ⓘ	Disable Edit

3. In the **Edit Session Persistence** dialog box, select a persistence time and click **OK**.

Note:

Session persistence is disabled by default. It's recommended to keep the default persistence period.



Edit Session Persistence

Session persistence

Hold time 30 1800 3600 30 seconds

Configuring Health Check

Last updated : 2024-07-01 11:33:59

Use cases

Anti-DDoS Advanced health checks identify the running status of backend servers, where abnormal servers will be isolated to reduce the impact on overall business availability.

Layer-4 health check

The Anti-DDoS Advanced layer-4 health check mechanism is as follows: The Anti-DDoS cluster nodes initiate an access request to the server port specified. If the port can be accessed normally, the backend server is running properly; otherwise, the backend server is not running normally.

Under TCP protocol, the mechanism checks if the port can be connected, while under UDP protocol, it determines whether the port is reachable with the `ping` command.

Layer-7 health check

The Anti-DDoS Advanced layer-7 health check mechanism is as follows: The Anti-DDoS cluster nodes initiate an HTTP request to the backend server and determine whether the backend server works properly according to the HTTP response status code.

HTTP response status codes can be user-defined. Assume that HTTP response status codes include `http_1xx`, `http_2xx`, `http_3xx`, `http_4xx`, and `http_5xx`. You can select `http_1xx` and `http_2xx` to indicate that the service is normal, then the unselected codes `http_3xx`, `http_4xx`, and `http_5xx` represent that the service is not working properly.

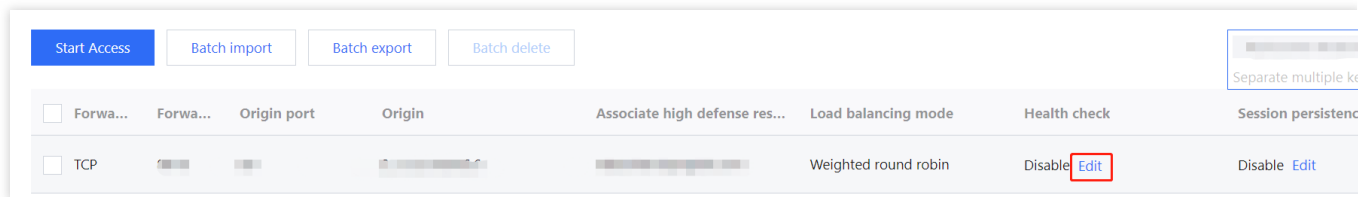
Note:

If only one real server IP is configured in a single forwarding rule, the health check feature cannot be enabled. This feature is used when multiple real server IPs are configured.

Directions

Layer-4 health check configuration

1. Log in to the new [Anti-DDoS console](#), click **Business Access** on the left sidebar, and then click the **Access via port** tab.
2. On the **Access via port** tab, select an Anti-DDoS Advanced instance and rules and then click **Edit** in the **Health check** column.

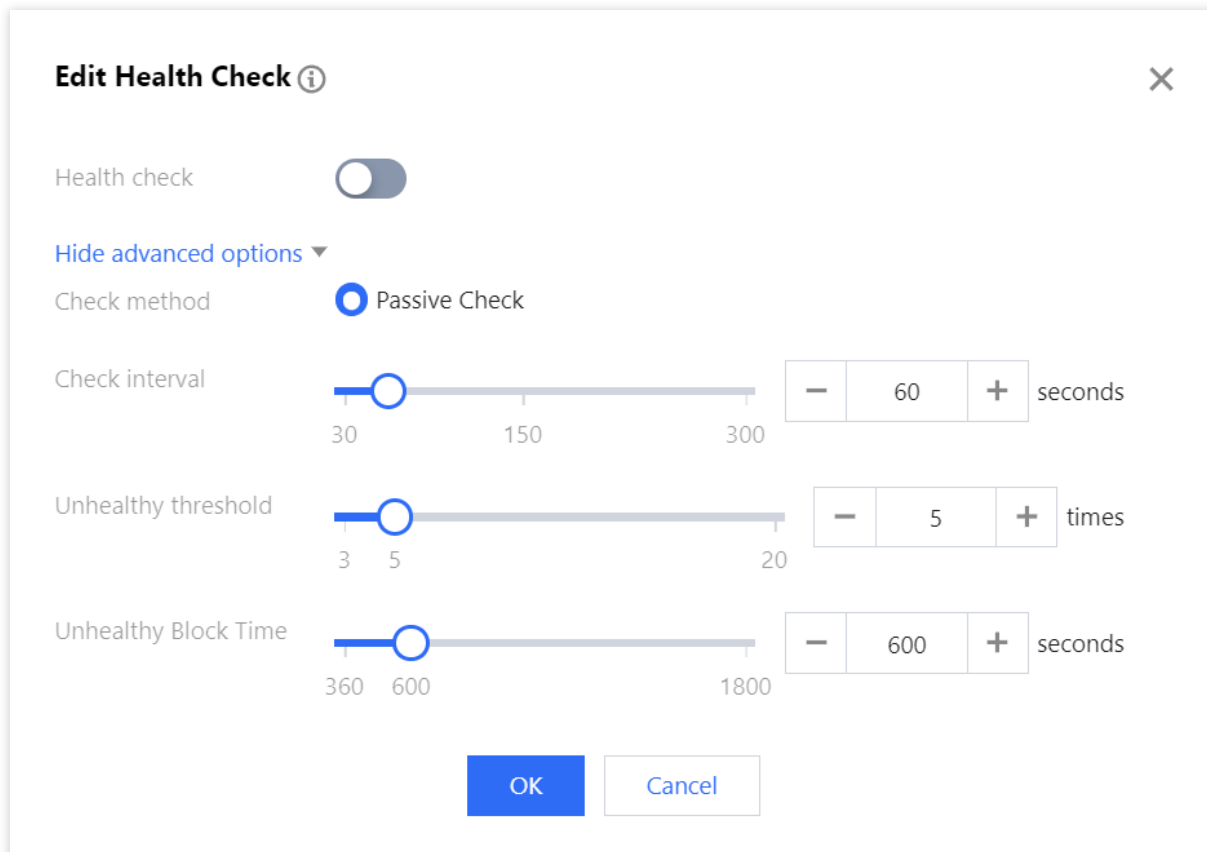


3. On the **Edit Health Check** dialog box, click **Display advanced options**, configure the required fields, and then click **OK**.

Note:

By default, layer-4 health check is enabled. We recommend you use the default values when you configure this feature.

Under TCP protocol, the mechanism checks if the port can be connected, while under UDP protocol, it determines whether the port is reachable with the `ping` command.



Layer-7 health check configuration

1. Log in to the new [Anti-DDoS console](#), click **Business Access** on the left sidebar, and then click the **Access via domain name** tab.
2. On the **Access via domain name** tab, select an Anti-DDoS Advanced instance and rules and then click **Configure** in the **Health check** column.

<input type="checkbox"/>	Application do...	Forwarding prot...	Forwarding port	Real server IP/Site	Associate high defense r...	Health check	Session persiste...	Access Status
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	Disable Configure ⓘ	Disable Edit	Success
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	Disable Configure ⓘ	Unavailable	Success

3. On the **Edit Health Check** dialog box, click **Display advanced options**, configure the required fields, and then click **OK**.

Note:

By default, layer-7 health check is disabled.

Edit Health Check ⓘ ✕

Health check

[Hide advanced options](#) ▼

Application domain name [blurred]

Check method ⓘ Passive Check Active check

Check interval 30 150 300 60 seconds

Unhealthy threshold 3 5 20 5 times

Unhealthy Block Time 360 600 1800 600 seconds

HTTP Status Code Detection http_1xx http_2xx http_3xx http_4xx
 http_5xx

When the status code is http_1xx, http_2xx, http_3xx and http_4xx, the backend server is considered alive.

Configuration item description

Layer-4 health check

Configuration item	Description
Response timeout	Maximum response timeout for a health check. If the backend server does not respond properly within the specified time, the health check will be considered as failed.
Check interval	Interval between two health checks
Unhealthy threshold	When the health check status is "succeeded", but the health check status "failed**" is received for n times (n is the entered number) in a row, the backend server will be considered unhealthy, and "abnormal" will be displayed in the console.
Healthy threshold	When the health check status is "failed", but the health check status "succeeded" is received for n times (n is the entered number) in a row, the backend server will be considered healthy, and nothing will be displayed in the console.

Layer-7 health check

Configuration item	Description
Check interval	Interval between two health checks. Default: 15 seconds.
Unhealthy threshold	When the health check status is "succeeded", but the health check status "failed**" is received for n times (n is the entered number) in a row, the backend server will be considered unhealthy, and "abnormal" will be displayed in the console.
Healthy threshold	When the health check status is "failed", but the health check status "succeeded" is received for n times (n is the entered number) in a row, the backend server will be considered healthy, and nothing will be displayed in the console.
HTTP request method and check path URL	The HEAD method is used by default, and the server returns only the header of the response packet. If the GET method is used, the server returns the complete response packet. The corresponding backend server needs to support HEAD and GET. If the page used for health check is not the default homepage of the application server, you need to specify a specific check path. If the host field parameter is specified in the HTTP HEAD request, you need to specify the check path, that is, the URI of the page file used for the health check.
HTTP status code detection	It determines whether the HTTP status code is healthy. By default, http_1xx, http_2xx, http_3xx, and http_4xx are selected. If you use the default settings and the returned HTTP status code is not the default value, the server will be considered unhealthy. You can modify the settings for this configuration item.

Smart Scheduling

Last updated : 2024-07-01 11:33:59

Use cases

Each account can have multiple Anti-DDoS instances, and each instance has at least one protective line; therefore, there can be multiple protective lines under one account. Once your business is added to an Anti-DDoS instance, a protective line will be configured for it. If multiple protective lines have been configured, you need to choose the optimal business traffic scheduling method, i.e., how to schedule business traffic to the optimal line for protection while ensuring high business access speed and availability.

Anti-DDoS features priority-based CNAME smart scheduling, where you can select an Anti-DDoS instance and set the priority of its protective line as needed.

Note:

DNS reconfiguration is supported for Anti-DDoS Pro instances and Anti-DDoS Advanced instances (including instances for BGP, China Telecom, China Unicom, and China Mobile).

Smart scheduling is not needed if an instance has only one line.

Priority-based scheduling

All access traffic are first scheduled to the line of the highest priority. You can adjust the priority value of lines, which is 100 by default. The smaller the value, the higher the priority. The specific scheduling rules are as follows:

When an Anti-DDoS instance contains multiple lines from different ISPs and of the same priority, a response is made based on the ISP of the specific DNS request in the following order: BGP > China Telecom > China Unicom > China Mobile > ISPs outside the Chinese mainland.

If all the lines of the same priority are blocked, access traffic is automatically scheduled to the available line of the second-highest priority.

Note:

If no protective lines of the second-highest priority are available, automatic scheduling cannot be performed, and business access will be interrupted.

If the Anti-DDoS instance configured for your business contains multiple protective lines from the same ISP and of the same priority, access traffic will be evenly distributed to such lines.

Examples

Assume that you have the following Anti-DDoS instances: BGP protective IPs 1.1.1.1 and 1.1.1.2, China Telecom protective IP 2.2.2.2, and China Unicom protective IP 3.3.3.3, of which the priority of 1.1.1.2 is 2 and that of the rest is

1. Normally, all traffic will be scheduled to the protective lines with the current priority of 1. Specifically, traffic from China Unicom will be scheduled to 3.3.3.3, that from China Telecom to 2.2.2.2, and that from other ISPs to 1.1.1.1. If 1.1.1.1 is blocked, access traffic under this IP will be automatically scheduled to 2.2.2.2. If both 1.1.1.1 and 3.3.3.3 are blocked, traffic supposed to be scheduled to them will be distributed to 2.2.2.2, and if 2.2.2.2 is blocked too, traffic will be scheduled to 1.1.1.2.

Prerequisite

Connect your service with Anti-DDoS.

Note:

To add the IP of your Tencent Cloud product to a purchased Anti-DDoS Pro instance, see [Getting Started with Anti-DDoS Pro](#).

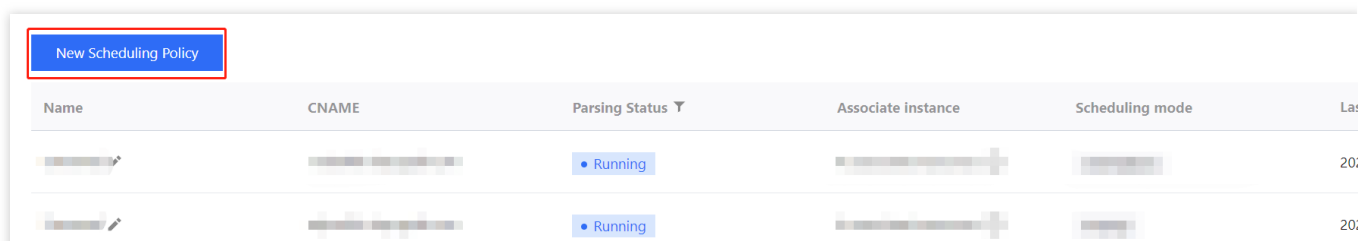
To connect layer-4 or layer-7 services to an Anti-DDoS Advanced instance, see the [Port Connection](#) or [Domain Name Connection](#).

To modify the DNS resolution, you need to purchase a DNS service, such as Tencent Cloud DNSPod.

Setting line priority

Please follow the steps below to set priorities for your protective instances based on your scheduling scheme:

1. Log in to the [Anti-DDoS console](#) and click **Smart Scheduling** on the left sidebar.
2. Click **New Scheduling Policy** to generate a CNAME record.



The screenshot shows the 'New Scheduling Policy' button highlighted with a red box. Below it is a table with the following columns: Name, CNAME, Parsing Status, Associate instance, Scheduling mode, and Last updated. Two rows are visible, both with a 'Running' status.

Name	CNAME	Parsing Status	Associate instance	Scheduling mode	Last updated
[Redacted]	[Redacted]	Running	[Redacted]	[Redacted]	20:...
[Redacted]	[Redacted]	Running	[Redacted]	[Redacted]	20:...

3. On the **Create smart scheduling policy** page, the TTL value defaults to **60 seconds** and ranges from 1 to 3600 seconds. The default scheduling mode is **Priority**. **Switchback time** refers to the waiting time for triggering the switchback process when multiple resources are linked. Considering the waiting time for unblocking and to avoid frequent triggering of switchover, the minimum value allowed for switchback time is 10 minutes and the default value 60 minutes is recommended.

Create smart scheduling policy ✕

Name

CNAME

TTL value 60 seconds

Mode ⓘ Priority Mode Orientation Mode

Switchback time ⓘ

Linkage resources ⓘ [Add Anti-DDoS IP](#) [Add non-Anti-DDoS IP](#)

IPv4

Anti-DDoS Resources	IP Protocol	Priority	Line	Region	Status	Domain ...	Operation
No data yet							

IPv6

Anti-DDoS Resources	IP Protocol	Priority	Line	Region	Status	Domain ...	Operation
No data yet							

4. On the **Create smart scheduling policy** page, two modes are provided: priority and directional. Operation instructions for the two modes are as follows:

4.1 Priority mode: Set by priority (by numerical value) to provide scheduling between resources.

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

Add Anti-DDoS instance

Select instance type

Select instance

Enter the instance ID/resource IP

<input type="checkbox"/>	Instance ID/name	Bind resource	Instance type
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]
<input checked="" type="checkbox"/>	[blurred]	[blurred]	[blurred]
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]

Selected (1)

Instance ID/name	Bind resource
[blurred]	[blurred]

You can make multiple selection by holding down the Shift key

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

IPv4					
Anti-DDoS Resources	IP Protocol	Priority	Line	Region	Status
[blurred]	IPv4	100	outside the Chinese mainland	Sao Paulo	Running

IPv6					
Anti-DDoS Resources	IP Protocol	Priority	Line	Region	Status
[blurred]	IPv6	100	BGP	Shanghai	Running

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

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

Add Anti-DDoS instance

Select instance type: Anti-DDoS Advanced

Select instance

Enter the instance ID/resource IP 🔍

<input type="checkbox"/>	Instance ID/...	Bind resource	Instance type	IP Proto...
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]	[blurred]
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]	[blurred]
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]	[blurred]
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]	[blurred]
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]	[blurred]
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]	[blurred]

↔

Selected (1)

Instance ID/...	Bind resource	Instance type	IP Proto...
[blurred]	[blurred]	[blurred]	[blurred]

You can make multiple selection by holding down the Shift key

OK
Cancel

4.2.2 On the **Create smart scheduling policy** page, click **Configure linkage resources** on the right of the target resource.

IPv4

Anti-DDoS Resources	Line type	Status ⓘ	Number of linkage r...	Operation
[REDACTED]	Default	Running	0	Configure Unbind

4.2.3 In the **Linkage resource management** window, click **Add resource**, enter an IP and select a line, and click **OK** to configure the scheduling relationship between the specified resources.

Linkage resource management

High Defense Resource Information [REDACTED]

Line Default

Linkage resources ⓘ [+Add resource](#)

Resource Record Select line

Example

Assume that you want to implement the following scheme: The business traffic will be scheduled to a BGP protective line first; if it is blocked due to attacks, the traffic will be automatically scheduled to a China Telecom protective line; if it is blocked too, the traffic will be scheduled to a China Unicom protective line; and after the BGP protective line is unblocked, the traffic will be scheduled to it automatically.

To implement this scheduling scheme, set the priority of the BGP line in the Anti-DDoS instance to 1 and that of the China Telecom line to 2, and keep the priority of the China Unicom line unchanged.

Anti-DDoS Resources	IP Protocol	Priority	Line	Region	Status	Domain ...	O
[Redacted]	[Redacted]	100	outside the Chinese mainland	Hong Kong (China)	Running	<input checked="" type="checkbox"/>	U
[Redacted]	[Redacted]	100	BGP	Shanghai	Running	<input checked="" type="checkbox"/>	U
[Redacted]	[Redacted]	100	outside the Chinese mainland	Sao Paulo	Running	<input checked="" type="checkbox"/>	U
[Redacted]	[Redacted]	100	BGP	Guangzhou	Running	<input checked="" type="checkbox"/>	U

If you do not want the China Unicom protective line to be in the traffic scheduling scheme, click



to disable DNS resolution for it, and you can enable DNS resolution again and set its priority when necessary. If you want to delete it from the current scheduling scheme, you can locate the row of its corresponding instance and click **Unbind**.

Modifying DNS resolution

Before using a CNAME record for smart scheduling, you are recommended to change the CNAME record of your business domain name DNS to the CNAME record automatically generated by the smart scheduling system of Tencent Cloud Anti-DDoS, to which all access traffic will be directed.

Protection Configuration

DDoS Protection

DDoS Protection Levels

Last updated : 2024-07-01 11:33:59

Use cases

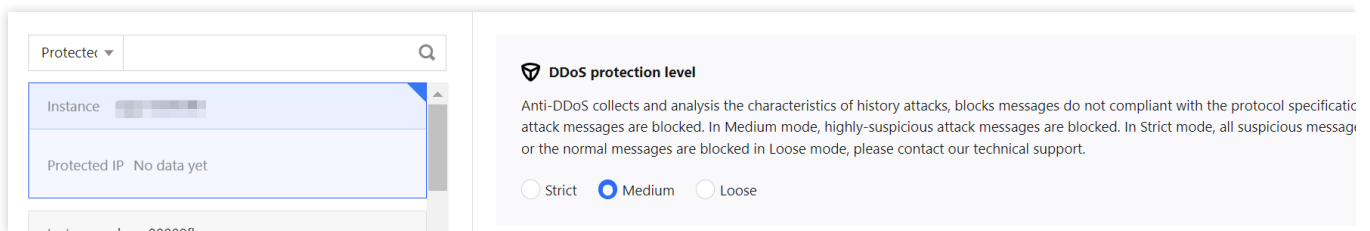
Anti-DDoS provides three available protection levels for you to adjust protection policies against different DDoS attacks. The details are as follows:

Protection level	Protection action	Description
Loose	<p>Filters SYN and ACK data packets with explicit attack attributes.</p> <p>Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specification.</p> <p>Filters UDP data packets with explicit attack attributes.</p>	<p>This protection level uses a loose cleansing policy and defends against only explicit attack packets. We recommend that you choose this protection level when normal requests are blocked. Complex attack packets may bypass the security system.</p>
Medium	<p>Filters SYN and ACK data packets with explicit attack attributes.</p> <p>Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specification.</p> <p>Filters UDP data packets with explicit attack attributes.</p> <p>Filters common UDP-based attack packages.</p> <p>Actively verifies the source IP addresses of some access attempts.</p>	<p>This protection level uses a cleansing policy that is suitable for most businesses and capable of defending against common attacks.</p> <p>This is the default protection level.</p>
Strict	<p>Filters SYN and ACK data packets with explicit attack attributes.</p> <p>Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specification.</p> <p>Strictly checks and filters UDP data packets with explicit attack attributes and UDP-based attack packets.</p>	<p>The cleansing policy is strict. We recommend you use this level when attack packets bypass the security system in the Normal mode.</p>

Actively verifies the source IP addresses of some access attempts.
Filters ICMP attack packages.

Directions

1. Log in to the new [Anti-DDoS console](#) and click **DDoS Protection** on the left sidebar.
2. Select an Anti-DDoS instance ID in the list on the left, such as "bgp-00xxxxxx".



3. In the **DDoS protection level** section, choose a protection level.

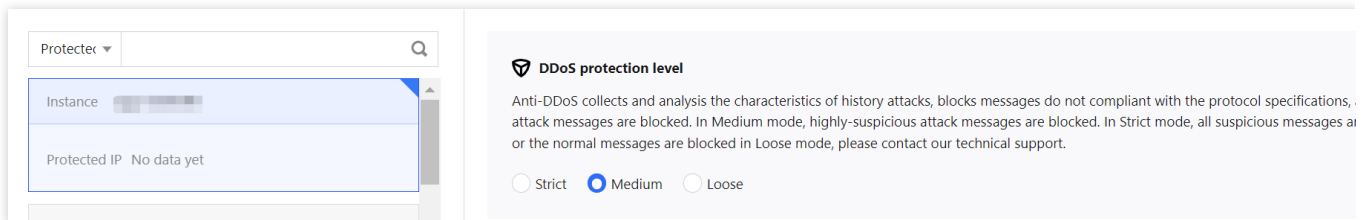
IP Blocklist/Allowlist

Last updated : 2024-07-01 11:33:59

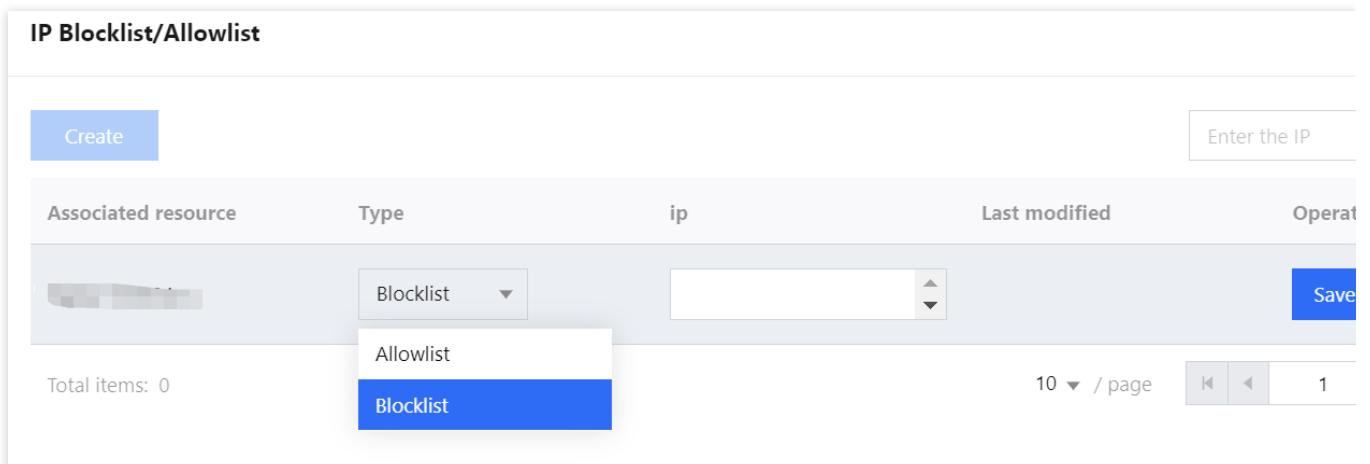
Anti-DDoS supports configuring the IP blocklist and allowlist to block or allow source IPs accessing the Anti-DDoS service, restricting the users from accessing your business resources. IPs in the allowlist are allowed to access without being filtered by any protection policy, while access requests from IPs in the blocklist are directly denied.

Directions

1. Log in to the new [Anti-DDoS console](#) and click **DDoS Protection** on the left sidebar.
2. Select an Anti-DDoS instance ID in the list on the left, such as "bgp-00xxxxxx".



3. In the **IP blocklist/allowlist** section, click **Set**.
4. In the pop-up window, click **Create**, select **Blocklist** or **Allowlist** as the type, enter an IP, and click **Save**.



5. Now the rule is added to the **IP blocklist/allowlist** window. You can click **Delete** on the right of the rule to delete it.

IP Blocklist/Allowlist

Create

Enter the IP

Associated resource	Type	ip	Last modified	Operati
[Redacted]	Blocklist	[Redacted]	2022-01-14 19:19:41	Set D

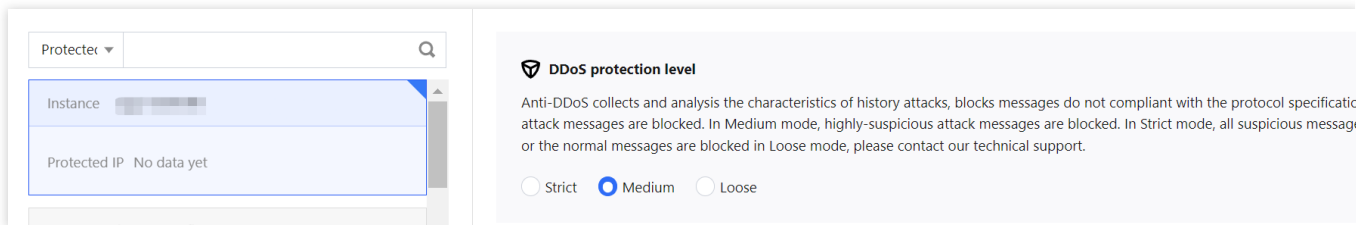
Port Filtering

Last updated : 2024-07-01 11:33:59

Anti-DDoS enables you to block or allow inbound traffic by ports. After port filtering is enabled, you can create rules by setting the protocol type, source port range, destination port range, and action (discard/allow/continue).

Directions

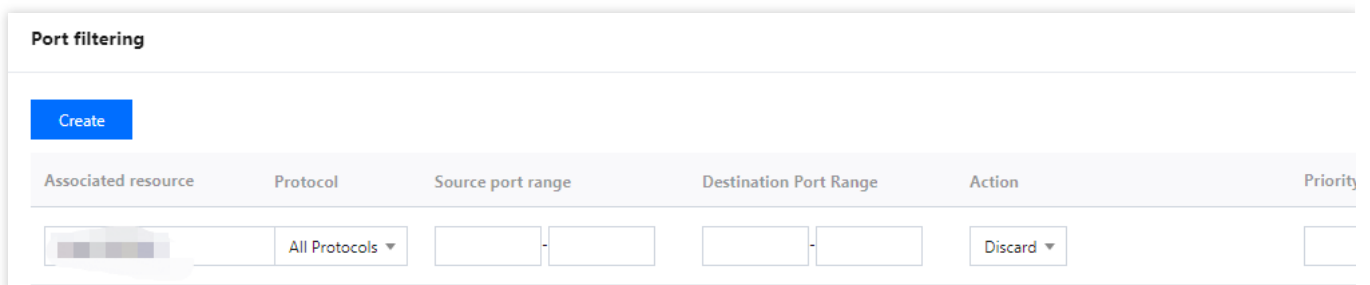
1. Log in to the new [Anti-DDoS console](#) and click **DDoS Protection** on the left sidebar.
2. Select an Anti-DDoS instance ID in the list on the left, such as "bgp-00xxxxxx".



3. In the **Port filtering** section, click **Set**.
4. On the **Port filtering** page, click **Create** to create a rule. Select an action, enter the required fields, and click **Save**.

Note:

You can create a rule for multiple instances at a time. Rules cannot be created for instances without protected resources.



5. After the rule is created, it is added to the port filtering list. You can click **Configure** on the right of the rule to modify it.

Port filtering

Create

Associated resource	Protocol	Source port range	Destination Port Range	Action	Priorit
	All Protocols				
	All Protocols				

Protocol Blocking

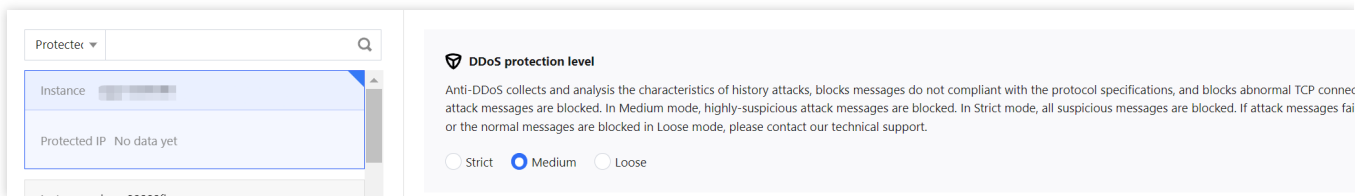
Last updated : 2024-07-01 11:33:59

Anti-DDoS supports blocking the source traffic accessing Anti-DDoS instances based on specified protocols, such as ICMP, TCP, and UDP. Requests over the specified protocols are blocked directly.

UDP is a connectionless protocol, which is vulnerable to attacks. It's recommended to block UDP requests unless necessary.

Directions

1. Log in to the [Anti-DDoS console](#) and click **DDoS Protection** on the left sidebar.
2. Select an Anti-DDoS instance ID in the list on the left, such as "bgp-00xxxxxx".



3. In the **Protocol blocking** section, click **Set**.
4. On the pop-up page, click



to enable or disable a protocol blocking rule.

Protocol blocking				
Associated resource	Block ICMP protocol	Block TCP protocol	Block UDP protocol	Block of
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Total items: 1 10 / page 1 / 1

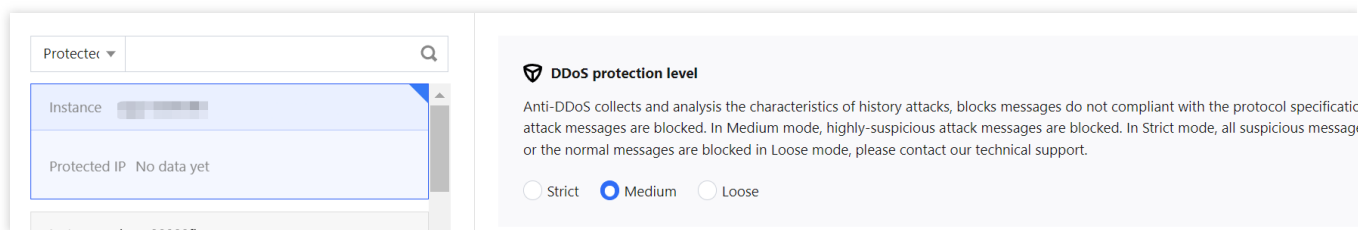
Watermark Protection

Last updated : 2024-07-01 11:33:59

Anti-DDoS supports watermark protection for messages sent by the business client. Within the range of the UDP and TCP message ports configured, the business client and Anti-DDoS share the same watermark algorithm and key. After the configuration is completed, every message sent from the client will be marked with the watermark while attack messages will not, so that the attack messages can be identified and discarded. Watermark protection can effectively and comprehensively defend against layer-4 CC attacks, such as analog business packet attacks and replay attacks.

Directions

1. Log in to the new [Anti-DDoS console](#) and click **DDoS Protection** on the left sidebar.
2. Select an Anti-DDoS instance ID in the list on the left, such as "bgp-00xxxxxx".



3. In the **Watermark protection** section, click **Set**.
4. On the pop-up page, click **Create**, enter the required fields, and click **OK** to create a watermark protection rule.

Create watermark protection policy ✕

Associate Anti-DDoS Pro b. [redacted] ▼

Watermark Check Mode Normal Compact

Port

Protocol	Port
Add	

Whether to ignore destination IP+port check

Watermark offset

OK
Cancel

5. After the rule is created, it is added to the watermark protection list. You can click **Key configuration** to view and configure a key.

Watermark Protection


Create


Associated resource	Protocol port	Whether to ignore destina...	Offset	Check mode
[redacted]	[redacted]	<input checked="" type="checkbox"/>	0	Normal

Total items: 1
10 ▼ / page

6. On the key configuration page, you can also copy, add, or delete a key. A key can be deleted if you have another key. Up to two watermark keys can be created.

Key information

 Each application can have up to 2 keys. To add a new key, please delete the old key first. When there is only one valid

Key	Status	Generati
	Enabled	2022-05-

Add key

Disable

Connection Attack Protection

Last updated : 2024-07-01 11:33:59

Anti-DDoS can automatically trigger blocking policies to block suspicious connection . With **Max abnormal connections from source IP** enabled, a source IP that frequently sends a large number of messages with abnormal connection status will be added to the blacklist. The source IP will be blocked for 15 minutes. After that, it will recover access to the business.

Note:

The Lighthouse edition does not support custom DDoS protection configurations.

The following fields are supported:

New connections from source IP: It limits the rate of new connections from source IP addresses.

Concurrent connections from source IP: It limits the number of active TCP connections from source IP addresses at any time point.

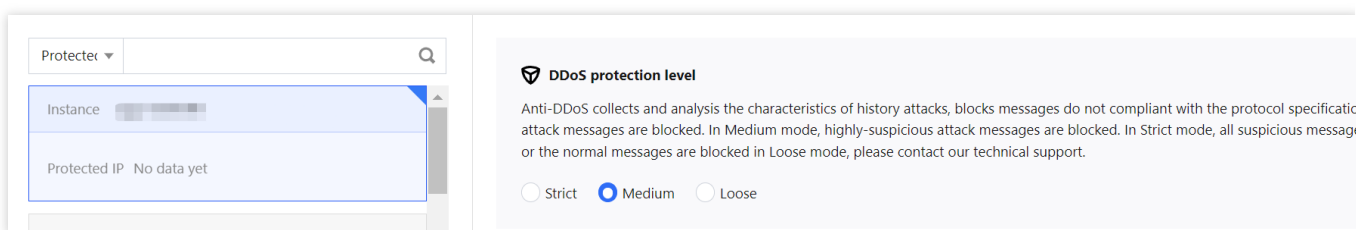
New connections to destination IP: It limits the rate of new connections to destination IP addresses.

Concurrent connections to destination IP: It limits the number of active TCP connections to destination IP addresses at any time point.

Max abnormal connections from source IP: It limits the maximum number of abnormal connections from source IP addresses.

Directions

1. Log in to the new [Anti-DDoS console](#) and click **DDoS Protection** on the left sidebar.
2. Select an Anti-DDoS instance ID in the list on the left, such as "bgp-00xxxxxx".



3. In the **Connection attack protection** section, click **Set**.
4. On the pop-up page, click **Create**, enable **Connection flood protection** and **Abnormal connection protection**, and click **OK**.

Configure Connection Attack Protection ✕

Associate Anti-DDoS Advanced [Redacted] ▼

Connection flood protection

New connections from source IP

Concurrent connections from source IP

New connections to destination IP

Max concurrent connections to destination IP

Abnormal connection protection ⓘ

Max abnormal connections from source IP

OK
Cancel

5. After the rule is created, it is added to the attack protection list. To modify the rule, click **Configure** in the **Operation** column on the right.

Connection attack protection					
	Create				<input type="button" value="Enter"/>
Associated resource	New connections from source IP	Concurrent connections from source IP	New connections to destination IP	Max concurrent connections to destination IP	Max a conne sourc
	Disable	Disable	Disable	Disable	Disabl

AI Protection

Last updated : 2024-07-01 11:33:59

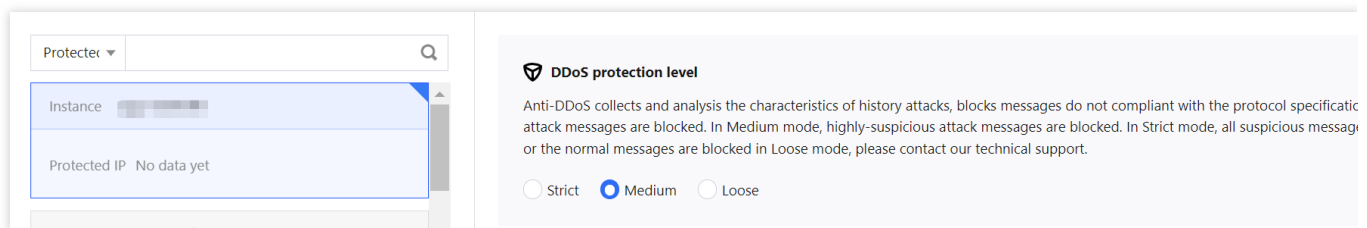
Anti-DDoS supports AI protection, which is to learn connection baselines and traffic features automatically, auto-tune its cleansing policies, and detect and block layer-4 CC attacks.

Note:

Anti-DDoS Pro (Light) does not support custom protection configurations for DDoS protection and CC protection.

Directions

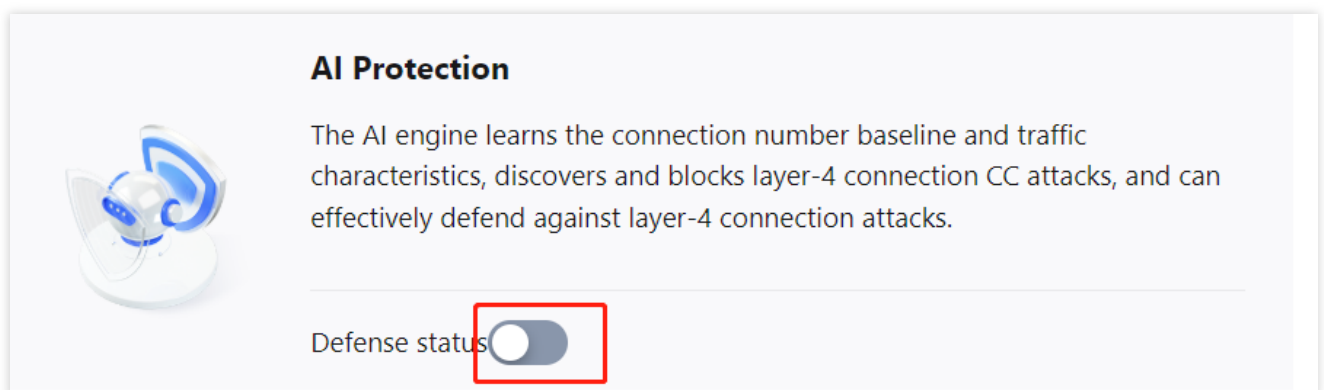
1. Log in to the new [Anti-DDoS console](#) and click **DDoS Protection** on the left sidebar.
2. Select an Anti-DDoS instance ID in the list on the left, such as "bgp-00xxxxxx".



3. Click



in the **AI protection** section to enable the setting.



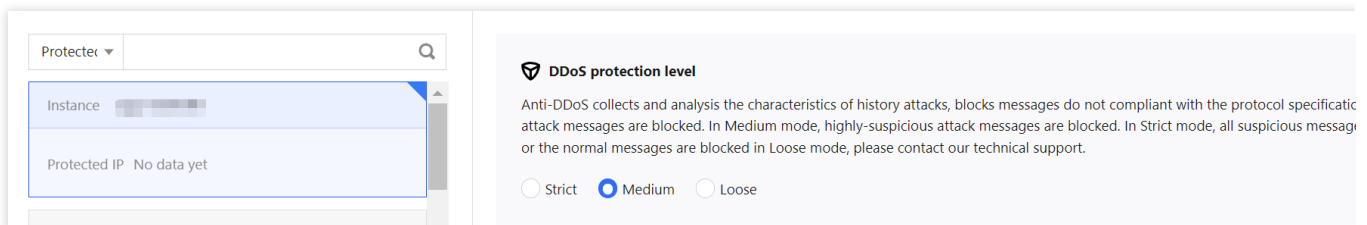
Regional Blocking

Last updated : 2024-07-01 11:33:59

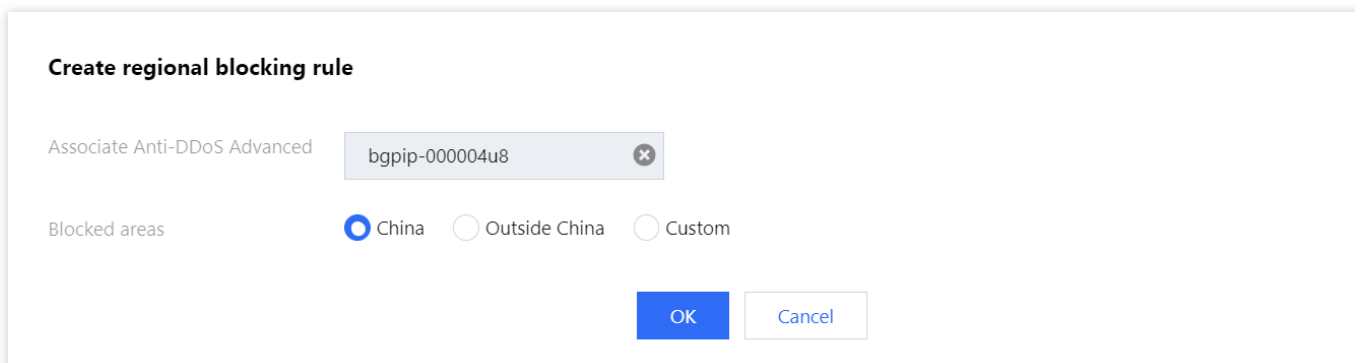
Anti-DDoS allows you to block traffic from source IP addresses in specific geographic locations at the cleansing node, with just one click. You can block traffic from whatever regions or countries you need.

Directions

1. Log in to the new [Anti-DDoS console](#) and click **DDoS Protection** on the left sidebar.
2. Select an Anti-DDoS instance ID in the list on the left, such as "bgp-00xxxxxx".



3. In the **Regional blocking** section, click **Set**.
4. On the **Regional blocking** page, click **Create**, select a region, and click **OK** to create a rule.



5. After the rule is created, it is added to the regional blocking list. You can click **Configure** on the right of the rule to modify it.

Regional blocking

Create

Ent

Associated resource	Blocked areas	Operat
[Redacted]	Outside China	Config

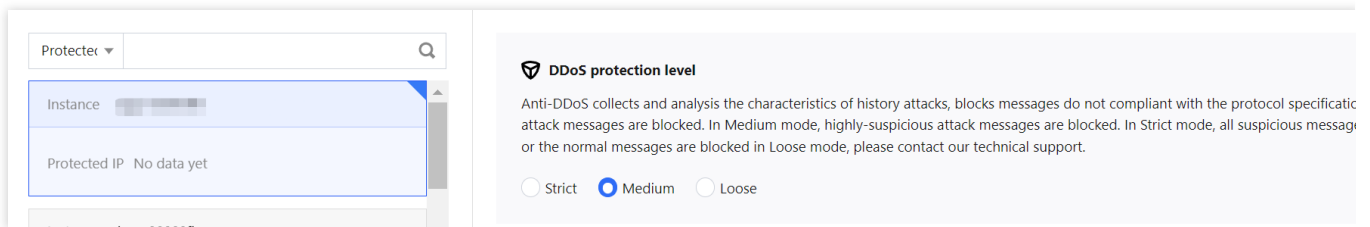
IP and Port Rate Limit

Last updated : 2024-07-01 11:33:59

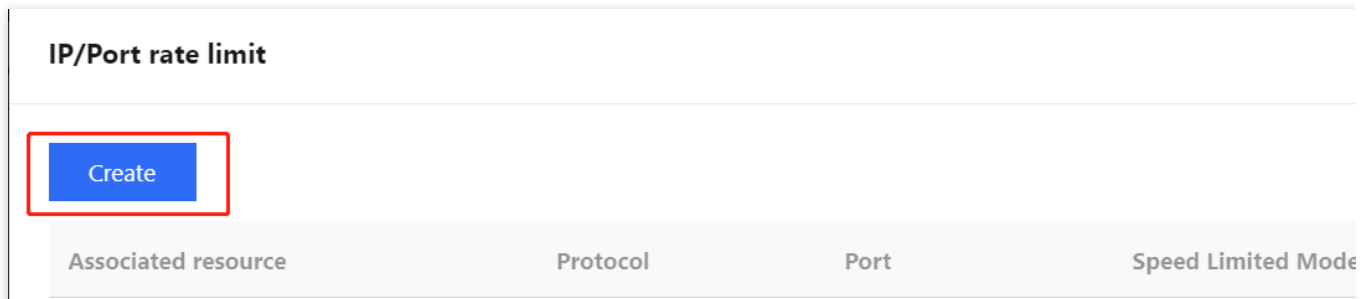
Anti-DDoS allows you to limit traffic rate for business IPs and ports.

Directions

1. Log in to the new [Anti-DDoS console](#) and click **DDoS Protection** on the left sidebar.
2. Select an Anti-DDoS instance ID in the list on the left, such as "bgp-00xxxxxx".



3. In the **IP/Port rate limit** section, click **Set**.
4. On the **IP/Port rate limit** page, click **Create**.



5. In the pop-up window, select a protocol, port, and limit mode, enter a rate limit, and click **OK**.

Create IP/port rate limit

Associate Anti-DDoS Advanced

Protocol ALL TCP UDP SMP Custom

Port

Please enter port numbers or port ranges; one entry per line; up to 8 entries can be entered.
 Port range: 0-65535

Speed Limited Mode

Speed Limit ⓘ bps
 pps

6. After the rule is created, it is added to the rate limit list. You can click **Configure** on the right of the rule to modify it.

IP/Port rate limit

Associated resource	Protocol	Port	Speed Limited Mode
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	By source IP

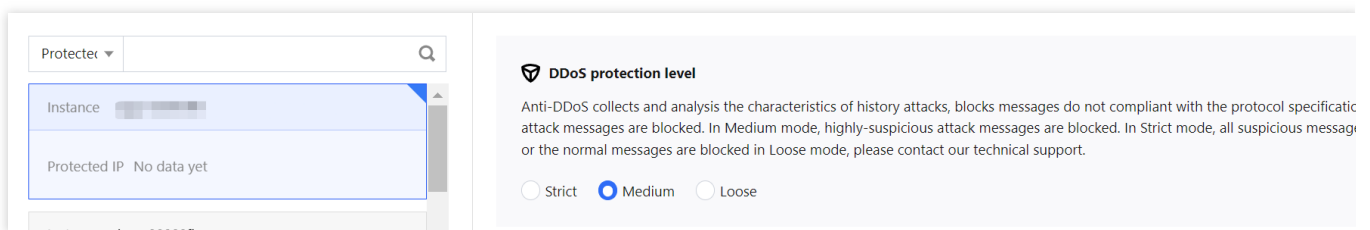
Feature Filtering

Last updated : 2024-07-01 11:33:59

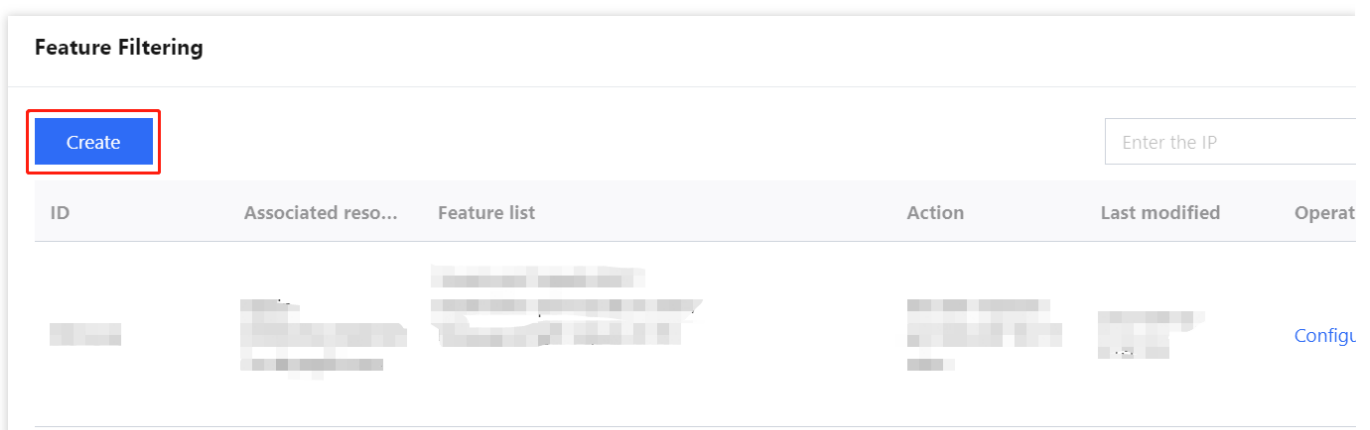
Anti-DDoS supports configuring custom blocking policies against specific IP, TCP, UDP message headers or loads. After enabling feature filtering, you can combine the matching conditions of the source port, destination port, message length, IP message header or load, and set the protection action to allow/block/discard matched requests, reject requests and block the IP for 15 minutes, discard requests and block the IP for 15 minutes, continue protection, and so on. With feature filtering, you can configure precise protection policies against business message features or attack message features.

Directions

1. Log in to the new [Anti-DDoS console](#) and click **DDoS Protection** on the left sidebar.
2. Select an Anti-DDoS instance ID in the list on the left, such as "bgp-00xxxxxx".



3. In the **Feature filtering** section, click **Set**.
4. Click **Create** to create a feature filtering rule.



5. In the pop-up window, select an action, enter the required fields, and click **OK**.

Create feature filtering rule

Associate Anti-DDoS Advanced

Filter feature

Field	Logic	Value
Add		

Action

Allow
 Block
 Discard
 Reject requests and block IP for 15 mins
 Discard requests and block IP for 15 mins
 Continue protection ⓘ

6. After the rule is created, it is added to the feature filtering list. To modify the rule, click **Configure** in the **Operation** column on the right.

Feature Filtering

ID	Associated reso...	Feature list	Action	Last modified	Oper...
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	2021-09-02 21:41:35	<input type="button" value="Configure"/>

CC Protection

CC Protection and Cleansing Threshold

Last updated : 2024-07-01 11:33:59

Protection description

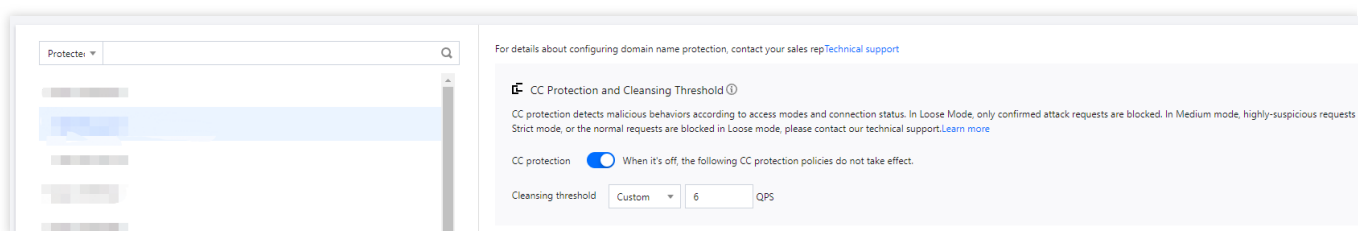
CC protection identifies and blocks CC attacks based on access attributes and connection status. It provides scenario-specific configurations for you to create protection policies, helping secure your business. It also supports setting the cleansing threshold.

Prerequisite

1. You have purchased an Anti-DDoS Advanced instance and set an object to protect.
2. Only CC protection rules configured for instances connected via domain names take effect.

Directions

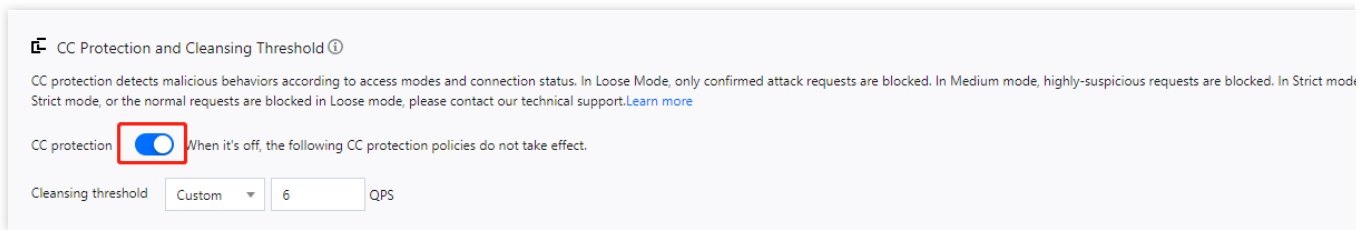
1. Log in to the new [Anti-DDoS console](#), click **CC protection** on the left sidebar.
2. Select a domain name from the IP list on the left.



3. In the **CC Protection and Cleansing Threshold** section, click



to enable CC protection and set a cleansing threshold.

**Note:**

This switch controls whether to enable CC protection. Only when it is turned on, the protection policy below it take effect.

4. The cleansing threshold is a threshold for Anti-DDoS services to start cleansing traffic. If the number of HTTP requests sent to the specified domain name exceeds the threshold, CC protection will be triggered. After CC protection is enabled, your Anti-DDoS Advanced instance will use the default cleansing threshold (recommended) to protect your business, and the Anti-DDoS system will generate a dedicated set of default thresholds based on the historical patterns of your business traffic. You can also set a cleansing threshold as needed.

Note:

If you want to set a custom threshold, a value that is 1.5 times your common business traffic peak is recommended. A smaller threshold means stricter detection.

If the threshold is lower than the default value, it may lead to false positives. If the threshold is higher than the default value, abnormal requests may be passed through. Therefore, the default threshold is recommended.

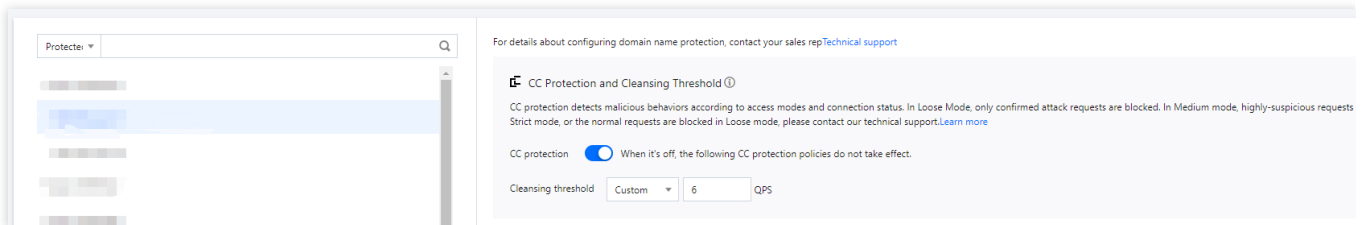
Intelligent CC Protection

Last updated : 2024-07-01 11:33:59

Intelligent CC protection is an AI-powered protection feature leveraging Tencent Cloud's big data capability. It provides a dynamic protection model to auto-generate rules for detecting and blocking malicious attacks based on website traffic patterns and algorithm-utilized attack analysis.

Directions

1. Log in to the new [Anti-DDoS console](#), and click **CC Protection** on the left sidebar.
2. Select a domain name from the left list.



3. In the **CC Protection and Cleansing Threshold** section, click

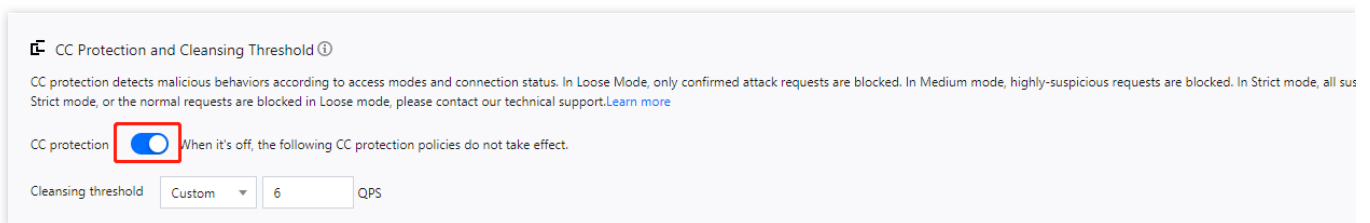


to enable CC protection and set a cleansing threshold before enabling intelligent CC protection.

Note:

The cleansing threshold is a threshold for Anti-DDoS services to start cleansing traffic. If the number of HTTP requests sent to the specified domain name exceeds the threshold, CC protection will be triggered.

If the IP bound to the Anti-DDoS Pro instance is from WAF, you need to first enable CC protection for the IP in the [WAF console](#). For more information, see [CC Protection Rule Settings](#).



4. In the **Intelligent CC Protection** section, toggle on the



switch.

Intelligent CC protection new

After enabling intelligent protection, AI intelligent protection is based on Tencent Cloud's big data capabilities, which can self-learn website business traffic baselines, analyze attack anomalies with algorithms, and automatically discover and block malicious attacks in time. Suggestion: Please wait 24 hours for this function for the first time (including switching traffic scenarios), and then turn it on after 24 hours of AI intelligent learning traffic. [Learn more](#)

Intelligent CC protection

Defense Status Mode

After CC AI Protection is enabled, CC AI Protection automatically generates protection rules based on each attack. The rules issued by intelligent protection have a single validity period. After a single attack ends, the protection rules will expire and be removed. (Add client IPs to the IP allowlist if you do not have them blocked.) Please click View on the right to edit smart protection rules.

5. Click **View** to view the auto-generated protection rules. You can make changes to these rules if necessary.

Note:

When intelligent CC protection is enabled, the protection rules are auto-generated when an attack occurs.

Protect mode: Applies auto-generated protection rules to defend against each specific attack. After the attack ends, the rules are automatically deleted.

Observe mode: Rules are displayed but not activated.


Intelligent CC protection

Smart protection rules are auto-generated and only effective for each attack. Once a single attack ends, the protection rules will expire and be removed. (Add client IPs to the IP allowlist if you do not have them blocked.)

On/Off Defense Status Mode ▾

Mode
Observe mode

Total 0 rules Enter the IP

Domain name	Condition	Action ▾	Valid at	Expiration time
 No data yet				

6. To delete a rule, click **Delete** on the right of the rule you want to remove.

Precise Protection

Last updated : 2024-07-01 11:33:59

Use Cases

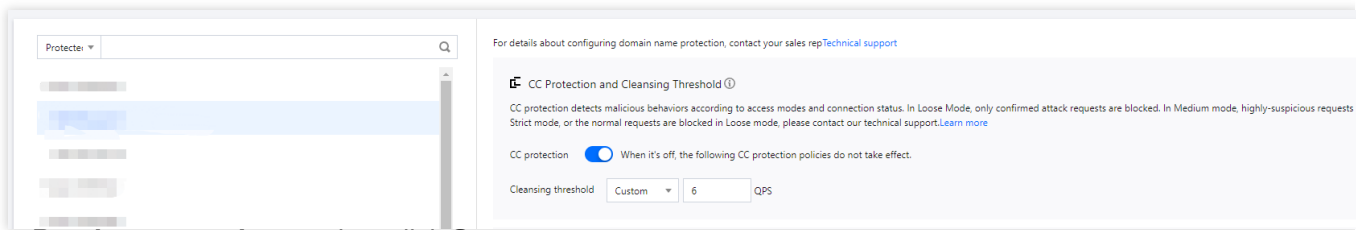
Anti-DDoS Advanced supports precise protection for connected web businesses. With precise protection enabled, you can configure protection policies combining multiple conditions of common HTTP fields, such as **uri**, **ua**, **cookie**, **referer**, and **accept** to screen access requests. For requests that match the conditions, you can configure CAPTCHA to verify the requesters or a policy to automatically drop or allow the requests. Precise protection is available for policy customization in various use cases to precisely defend against CC attacks.

Match conditions define the request characteristics to be verified, that is, the attribute characteristics of HTTP fields in a request. Precise protection supports verifying the following HTTP fields:

Field	Description	Logic
uri	URI of an access request	Equal to, include, and exclude
ua	Identifier and other information of the client browser that initiates an access request	Equal to, include, and exclude
cookie	Cookie information in an access request	Equal to, include, and exclude
referer	Source website of an access request, from which the access request is redirected	Equal to, include, and exclude
accept	Data type to be received by the client that initiates the access request	Equal to, include, and exclude
script	Source web address of the access request	Equal to and not equal to

Directions

1. Log in to the new [Anti-DDoS console](#) and click **CC Protection** on the left sidebar.
2. Select a domain name from the left list.



3. In the **Precise protection** section, click **Set**.

4. On the pop-up page, click **Create**, enter the required fields, and click **OK** to create a precise protection rule.

Create precise protection policy

Associate Anti-DDoS Advanced

Protocol HTTP HTTPS

Domain name

Condition

Field	Logic	Value
Add		

Match Action

5. After the rule is created, it is added to the rule list. You can click **Configure** on the right of the rule to modify it.

Precise Protection

Create

ID	Associated resource	Protocol	Domain name	Condition	Match Action	Creation time	Last modified
[blurred]	[blurred]	http	[blurred]	uri Equal to 11	CAPTCHA	2023-09-01 11:57:02	2023-09-01 11:57:02

CC Frequency Limit

Last updated : 2024-07-01 11:33:59

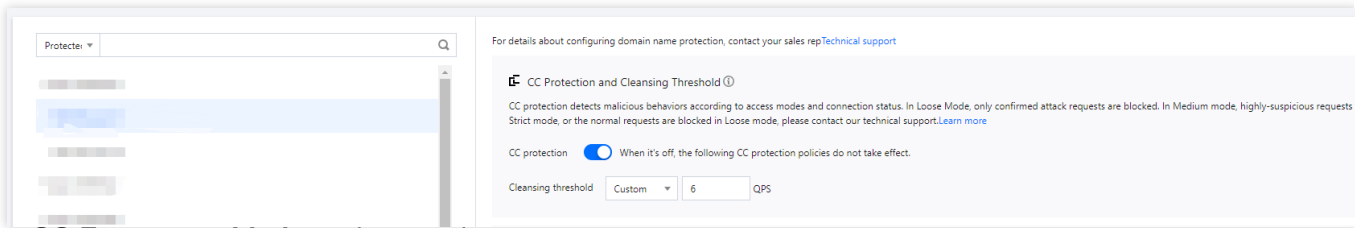
Anti-DDoS Advanced supports CC frequency limiting for connected web businesses to restrict the access frequency of source IPs. CC frequency limiting provides multiple protection levels and is set to **Loose** by default. You can customize a frequency limiting rule to apply CAPTCHA and discard on source IPs if any IP accesses a certain page too frequently in a short time.

You can adjust your frequency limiting rules using the following protection levels based on the real-time traffic:

Level	Description
Loose	<p>At this level, there may be a risk that a small number of abnormal requests can bypass the rule.</p> <p>Note that you can change the protection level when attacks occur or configure custom CC frequency limiting rules for protection.</p>
Medium	<p>This level verifies the identity of visitors using CAPTCHA. Only requests from verified visitors are forwarded to the real server.</p> <p>Note that this level is only applicable to website businesses. For API- or app-based businesses, please configure custom CC frequency limiting rules instead of using the default configurations.</p> <p>Urgent: When requests to access the real server surge and cause a high load or abnormal response, you can select this level.</p>
Strict	<p>This level verifies the identity of visitors using CAPTCHA. It may lead to false positives due to stricter verification.</p> <p>Note that this level is only applicable to website businesses. For API- or app-based businesses, please configure custom CC frequency limiting rules instead of using the default configurations.</p>
Urgent	<p>When requests to access the real server surge and cause a high load or abnormal response, you can select this level.</p>
Custom	<p>This level can limit the access frequency of requests that match the configured custom rules.</p>

Directions

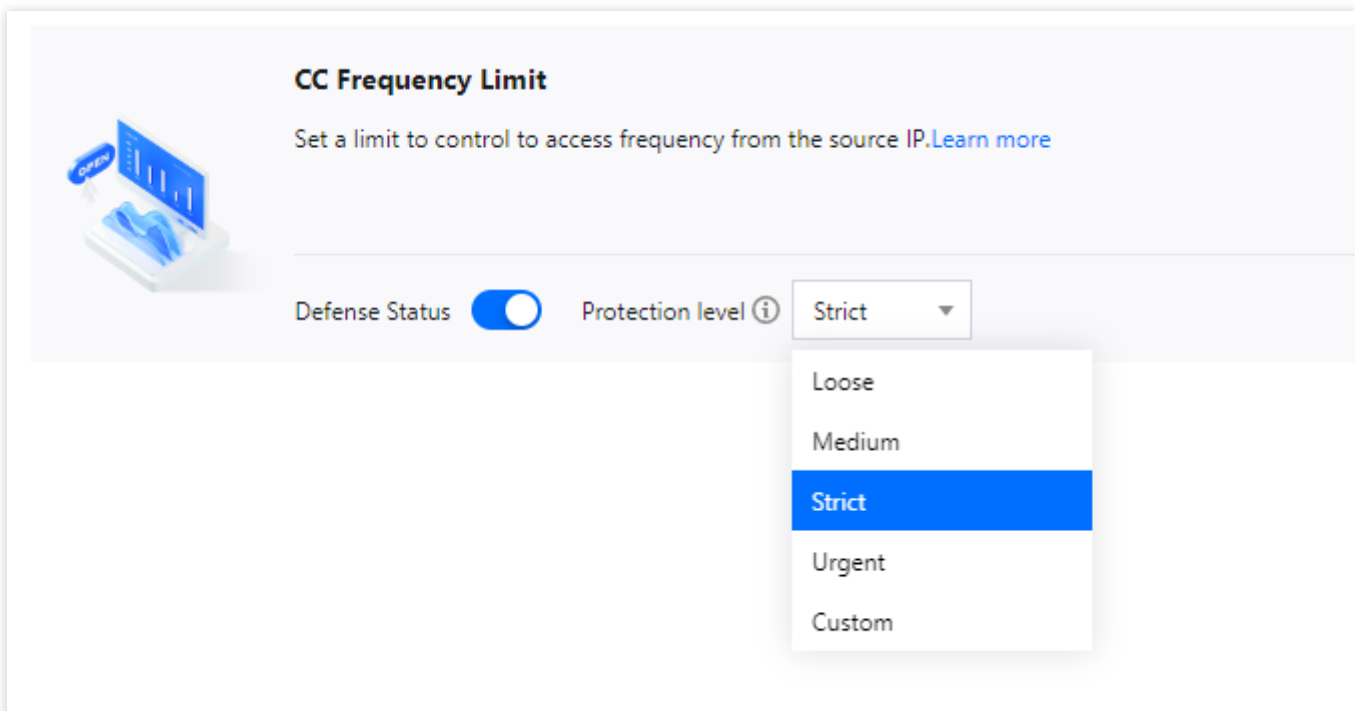
1. Log in to the new [Anti-DDoS console](#), and click **CC Protection** on the left sidebar.
2. Select a domain name from the left list.



3. In the **CC Frequency Limit** section, toggle on



, select a proper protection level as needed, and click **Set** to enter the rule list page.




4. Click **Add Rule** and enter the required fields to create a frequency limiting rule. All rules for this domain are displayed on the rule list page by default.

Note:

If no frequency limiting rules are created, the **Custom** level cannot be enabled.

After optimization, you don't have to add the default rule before creating a rule, and you can configure CC frequency limiting rules for subdomain names.

CC Frequency R

Associate Anti-DDoS Advanced 

Protocol HTTP HTTPS

Domain name ⓘ








Field	Mode	Value
Add		

Rate limit policy

Condition Every seconds Access times ⓘ

Punishment time seconds

5. After the rule is created, it is added to the rule list. You can click **Configure** on the right of the rule to modify it.

Rule ID	Domain name	Detection period (seconds)	Detection times	Matching ty...	Matching value	Action	Blocking Period (s)
						CAPTCHA	

6.

Regional Blocking

Last updated : 2024-07-01 11:33:59

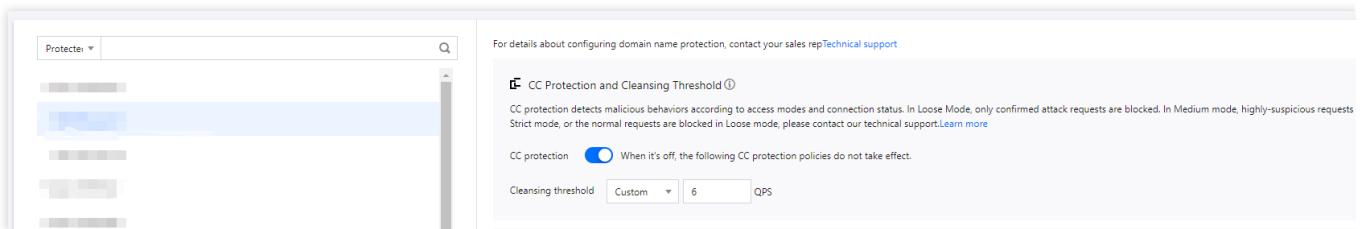
Anti-DDoS Advanced allows you to block website access requests from source IP addresses in specific geographic locations with just one click. You can block all website access requests from whatever regions or countries you need.

Note:

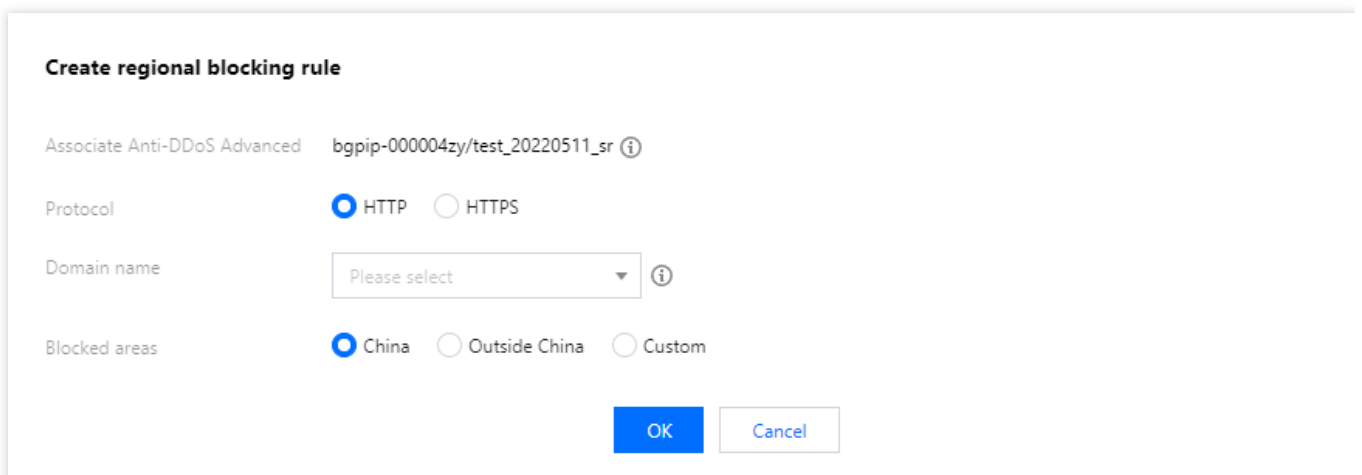
After you configure regional blocking, attack traffic targeting the specified countries/regions will still be recorded but will not be allowed to your real server.

Directions

1. Log in to the new [Anti-DDoS console](#), and click **CC Protection** on the left sidebar.
2. Select a domain name from the left list.



3. In the **Regional blocking** section, click **Set**.
4. On the pop-up page, click **Create**, select an instance, protocol, domain name, and region, and click **OK**.



5. After the rule is created, it is added to the list. To modify the rule, click **Configure** in the **Operation** column on the right.

Regional blocking

Create

Associated resource	Protocol	Domain name	Blocked areas	Last modified	Op
[blurred]	[blurred]	[blurred]	[blurred]	2022-06-30 15:46:03	Co

IP Blocklist/Allowlist

Last updated : 2024-07-01 11:33:59

Anti-DDoS Advanced supports configuring the IP blocklist and allowlist to block and allow IPs accessing your business resources connected to Anti-DDoS Advanced, restricting the users from accessing your resources. IPs in the allowlist are allowed to access without being filtered by any protection policy, while access requests from IPs in the blocklist are directly denied.

Note:

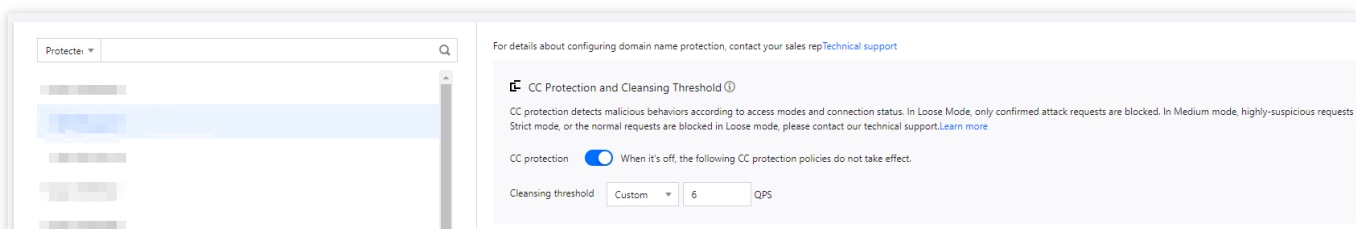
The IP blocklist and allowlist filtering takes effect only when your business is under CC attacks.

IPs in the allowlist are allowed to access resources without being filtered by any protection policy.

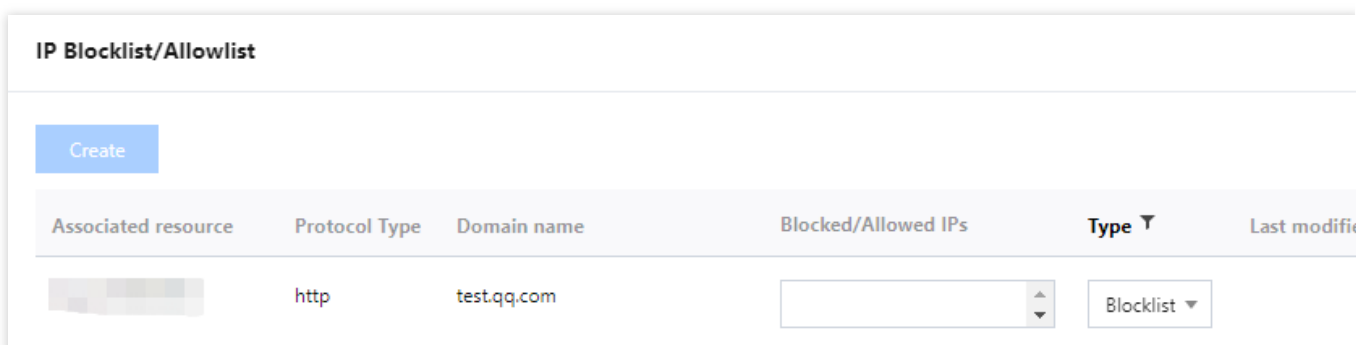
Access requests from IPs in the blocklist are directly denied.

Directions

1. Log in to the new [Anti-DDoS console](#), and click **CC Protection** on the left sidebar.
2. Select a domain name from the IP list on the left.



3. Click **Set** in the **IP Blocklist/Allowlist** section.
4. Click **Create**, enter the required fields, and click **Save**.



5. Now the rule is added to the **IP Blocklist/Allowlist** section. You can click **Delete** on the right of the rule to delete it.

IP Blocklist/Allowlist

Create

Associated resource	Protocol Type	Domain name	Blocked/Allowed IPs	Type ▼	Last
					2022

6.

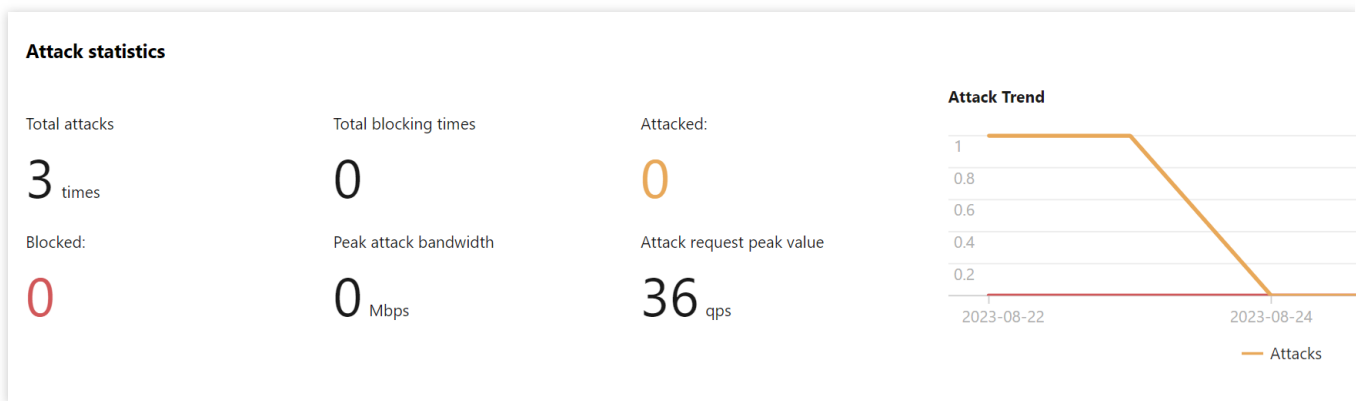
Security Operations

Attack Analysis

Last updated : 2024-07-01 11:33:59

Viewing attack statistics

1. Log in to the new [Anti-DDoS console](#) and click **Attacks** on the left sidebar.
2. In the **Attack statistics** section, you can view the total number of attacks the current business has experienced, the total number of times of blocking, the number of ongoing attacks, the number of IPs being blocked, peak attack bandwidth, and attack request peak. On the right, you can view the 7-day and 30-day attack trends.



View recent security events

1. The event details page displays detailed information on attacks by asset ID and IP address. Such information includes attack name, attacked asset, IP address, attack time, attack duration, attack peak, instance ID, defense type, and attack status.


Attack name	Attacked assets	IP address	Attack type	Attack time	Attack duration	Attack Peak	Insta
SYNFLOOD attacks	[blurred]	[blurred]	DDoS Attack	Start: [blurred] Ended at: [blurred]	7 mins	Peak attack bandwidth: [blurred] Peak attack packet rate: [blurred]	--
SYNFLOOD attacks	[blurred]	[blurred]	DDoS Attack	Start: [blurred] Ended at: [blurred]	5 mins	Peak attack bandwidth: [blurred] Peak attack packet rate: [blurred]	--

2. In the **Attack information** section of the event details page, you can view the detailed attack information for the selected period, including the attacked IP, status, attack type (which is sampled data), peak attack bandwidth and attack packet rate, and attack start and end time.

SYNFLOOD attacks

Attack information

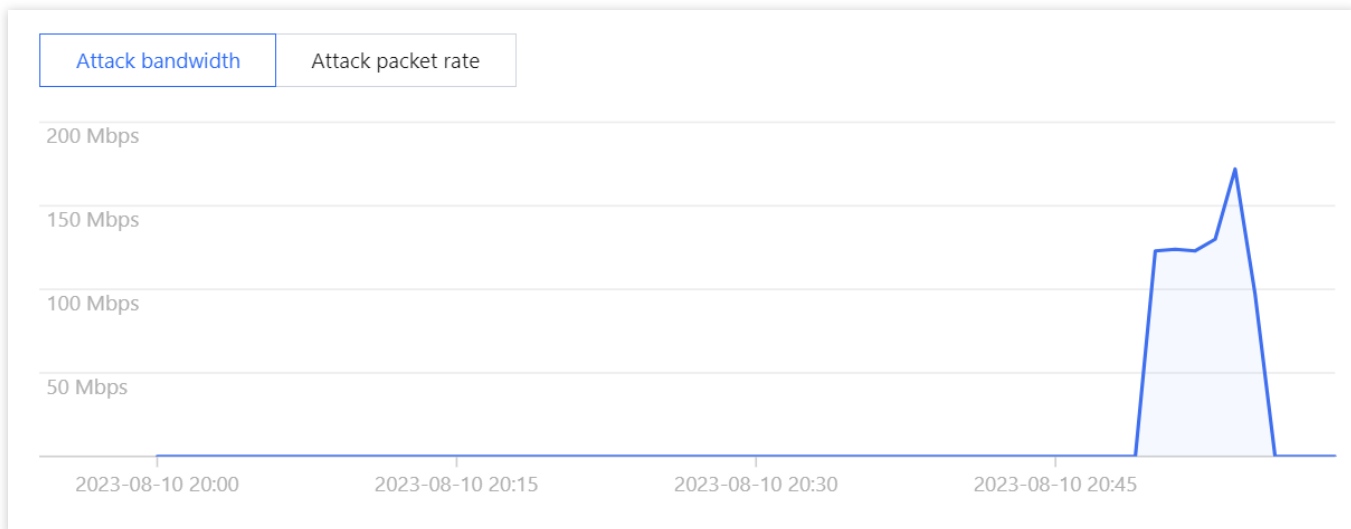
Anti-DDoS Resources		Peak attack bandwidth	Mbps
Status	<ul style="list-style-type: none">Attack ended	Peak attack packet rate	ps
Attack type	SYNFLOOD	Attack started	
		Attack ended	



3. In the attack trend section of the event details page, you can view the trend of attack bandwidth and attack packet rate and easily find the peak traffic.

Note:

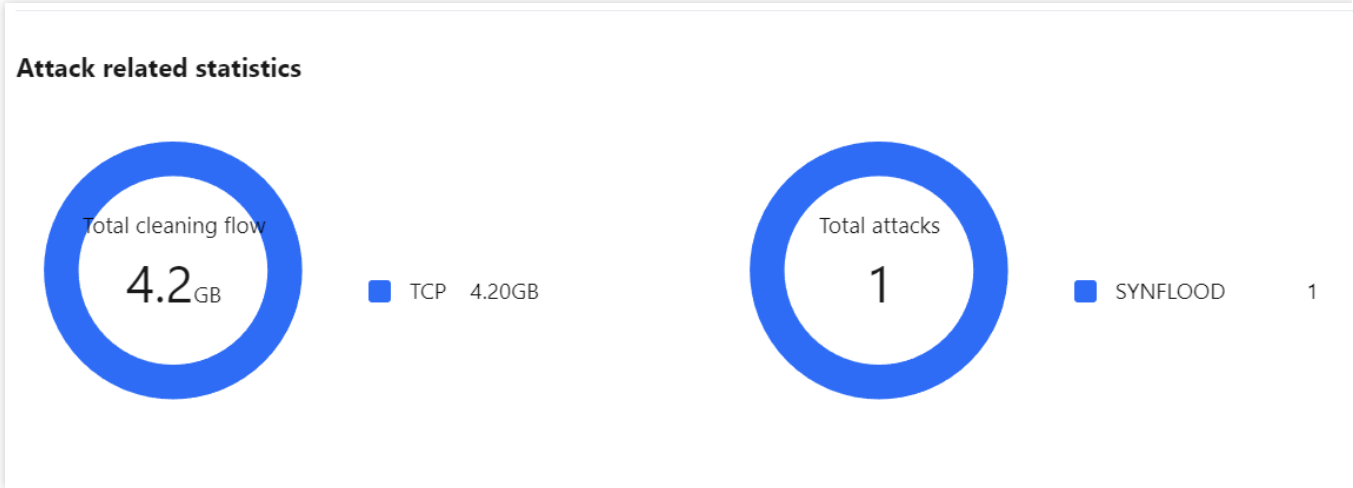
This section provides complete, real-time data in the attack period.



4. In the **Attack statistics** section of the event details page, you can view how attacks are distributed over different attack traffic protocols and attack types.

Note:

This section provides sampled data in the attack period.



Field description:

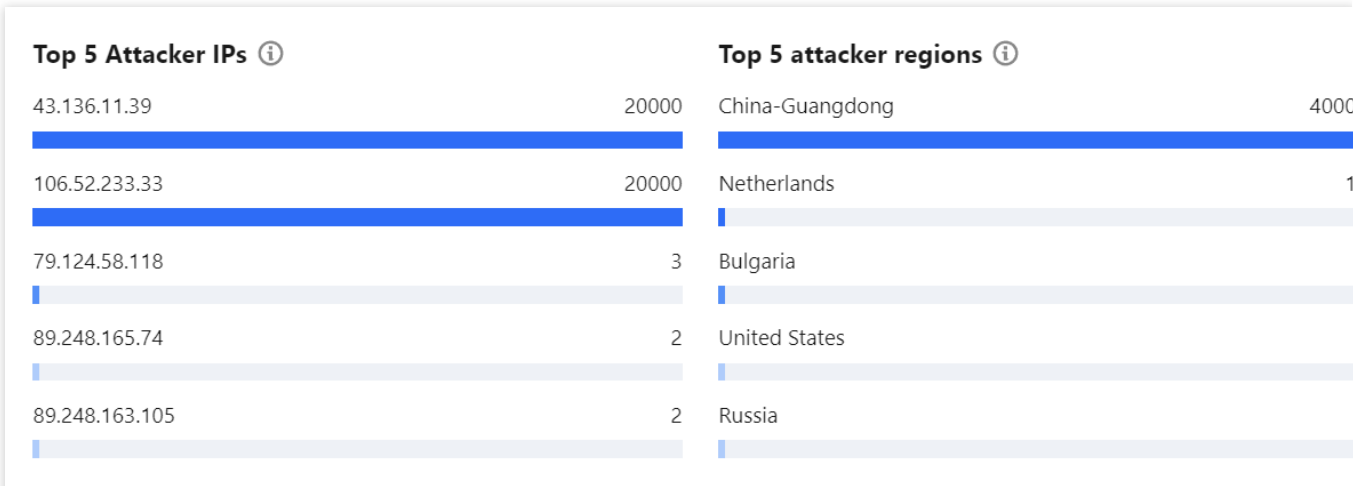
Attack traffic protocol distribution: displays how attacks on the selected Anti-DDoS instance distribute over different attack traffic protocols within the queried period.

Attack type distribution: displays how attacks on the selected Anti-DDoS instance distribute over different attack types within the queried period.

5. The **Top 5** sections of the event details page display the top 5 attacker IP addresses and the top 5 attacker regions. This is helpful for precise protection configuration.

Note:

This section provides sampled data in the attack period.



6. In the **Attacker information** section of the event details page, you can view the sampled data of the attack period, including the attacker IP, region, total attack traffic, and total attack packets.

Note:

This section provides sampled data in the attack period.

Attacker information ⓘ

Attacker IP	Region	Total attack traffic	Total Attack Packets
104.237.156.209	United States	44B	1
106.52.233.33	China-Guangdong	21.2 MB	20000
139.162.144.109	Germany	40B	1
139.59.91.13	India	40B	1
143.42.1.201	United States	44B	1
178.120.185.120	Belarus	52B	1
183.83.188.85	India	52B	1
185.156.73.107	Netherlands	40B	1
185.215.167.68	Germany	40B	1
185.233.19.227	China Hong Kong	44B	1

Total items: 30

 1 / 3 pages

Business Analysis

Last updated : 2024-07-01 11:33:59

Anti-DDoS allows you to view the number of protection days, connected businesses, and attacked businesses for the past 90 days. You can also search by instance ID.

Directions

1. Log in to the new [Anti-DDoS console](#) and click **Assets** on the left sidebar.
2. On the **Business analysis** page, click **Handle now**.



3. On the **To-do** page, perform the following operations:
Click **Unblock** to go to the unblocking service page.



- Click **Upgrade protection** to go to the upgrade page. Select the number of IPs and times of protection as needed.

升级 ✕

ⓘ 高防IP产品在2022年3月24日进行调整。不支持升级至50Gbps规格。点击[查看详情](#)

ID/服务包名 bg [REDACTED]

过期时间 20 [REDACTED]

保底防护带宽

20	30	50	60	100	300
----	----	----	----	-----	-----

业务带宽

-	100	+
---	-----	---

 Mbps

转发规则数

60	70	80	90	100	150	200	250	300	350
400	450	500							

总计费用 ¥ [REDACTED]

Operation Logs

Last updated : 2024-07-01 11:33:59

The new Anti-DDoS console allows you to view the logs of important operations in the past 90 days. The types of viewable logs are as follows:

Logs of protected IP replacement

Logs of Anti-DDoS protection policy modification

Logs of cleansing threshold adjustment

Logs of protection level change

Logs of resource name modification

Directions

1. Log in to the new [Anti-DDoS console](#) and click **Logs** on the left sidebar.
2. On the **Operation Logs** page, you can set a time range to view operation logs.

<input type="checkbox"/>	Operation time	Request ID	Product type	Action	Result
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Anti-DDoS Basic	[REDACTED]	Success

Total items: 1

Service Management

Unblocking Service

Viewing Blocking Time

Last updated : 2024-07-01 11:33:59

Checking the estimated unblocking time

1. Log in to the new [Anti-DDoS console](#) and click **Unblocking Service** on the left sidebar.
2. In the **Blocked IPs** tab, check the blocking time of the IP in **Blocking time**.

总封堵次数	当前封堵IP数	自助解封总配额	当日剩余配额	自助解封次数	
734 次	1 次	3 次	3 次	40 次	
封堵列表 解封记录					
IP	防护类型	防护状态	封堵时间	预计解封时间	状
	DDoS基础防护	无	2023-06-08 16:06:00	2023-06-09 17:40:00	自

3. In the **Blocked IPs** tab, check the estimated unblocking time of the IP in **Estimated unblocking time**.

总封堵次数	当前封堵IP数	自助解封总配额	当日剩余配额	自助解封次数	
734 次	1 次	3 次	3 次	40 次	
封堵列表 解封记录					
IP	防护类型	防护状态	封堵时间	预计解封时间	状
	DDoS基础防护	无	2023-06-08 16:06:00	2023-06-09 17:40:00	自

Checking the actual unblocking time

1. Log in to the new [Anti-DDoS console](#), click **Unblocking Service** on the left sidebar, and then click the **Unblocking records** tab.
2. Check the blocking time of the IP in **Blocking time**.

Blocked IPs **Unlocking records**

Last 24 hours Last 7 days Last 30 days **Last 90 days** 2023-06-03 00:00 ~ 2023-09-01 23:59

IP	Defense Type	Blocking time	Actual unblocking time
[REDACTED]	Anti-DDoS Pro	2023-08-17 19:46:00	2023-08-18 07:46:02
[REDACTED]	Anti-DDoS Basic	2023-08-17 19:46:00	2023-08-18 07:46:02

3. Check the actual unblocking time of the IP in **Actual unblocking time**.

Blocked IPs **Unlocking records**

Last 24 hours Last 7 days Last 30 days **Last 90 days** 2023-06-03 00:00 ~ 2023-09-01 23:59

IP	Defense Type	Blocking time	Actual unblocking time
[REDACTED]	Anti-DDoS Pro	2023-08-17 19:46:00	2023-08-18 07:46:02
[REDACTED]	Anti-DDoS Basic	2023-08-17 19:46:00	2023-08-18 07:46:02

Unblocking an IP

Last updated : 2024-07-01 11:33:59

Auto unblocking

With auto unblocking, you only need to wait until blocked IPs are unblocked automatically. You can check the predicted unblocking time as follows:

1. Log in to the new [Anti-DDoS console](#), and click **Unblocking Service** on the left sidebar.
2. Check the blocking time of the IP in **Blocking time** on the unblocking page.

Chances for manual unblocking

Each Anti-DDoS user has three chances of manual unblocking every day. The system resets the chance counter daily at 00:00 midnight. Unused chances will not be carried over to the next day.

Note:

The unblocking may fail for risk management reasons. A failed attempt does not count as a chance. Please wait for a while and then try again.

Before unblocking an IP, please check the predicted unblocking time which may be affected by some factors and will be postponed. If you accept the predicted time, you do not need to operate manually.

If your manual unblocking chances are used up for the day, you can upgrade the base protection capability or the elastic protection capability to defend against high-traffic attacks and avoid continuous blocking.

Manual unblocking

1. Log in to the new [Anti-DDoS console](#) and click **Unblocking Service** on the left sidebar.
2. Find the protected IP in the **Auto unblocking** status and click **Unblock** in the **Operation** column on the right.

解封中心				
总封堵次数	当前封堵IP数	自助解封总配额	当日剩余配额	自助解封次数
734 次	1 次	3 次	3 次	40 次

封堵列表		解封记录		
IP	防护类型	防护状态	封堵时间	预计解封时间
[REDACTED]	DDoS基础防护	无	2023-06-08 16:06:00	2023-06-09 17:40:00

3. Click **OK** in the **Unblock Blocked IP** dialog box. If you receive a notification indicating successful unblocking, the IP has been successfully unblocked. You can refresh the page to check whether the protected IP is in running status.

Unblocking records

1. Log in to the new [Anti-DDoS console](#), click **Unblocking Service** on the left sidebar, and then click the **Unblocking records** tab.
2. You can check all unblocking records in a specified period, including records of automatic unblocking and manual unblocking.

Blocked IPs		Unblocking records		
Last 24 hours Last 7 days Last 30 days Last 90 days		2023-06-02 00:00 ~ 2023-08-31 23:59 <input type="text"/>		
IP	Defense Type	Blocking time		Actual unblocking time
[REDACTED]	Anti-DDoS Pro	2023-08-[REDACTED]		2023-08-[REDACTED]
[REDACTED]	Anti-DDoS Basic	2023-08-[REDACTED]		2023-08-[REDACTED]

3.

Connecting a Blocked Server

Last updated : 2024-07-01 11:33:59

This document describes how to connect to a blocked server.

Directions

1. Log in to the [CVM console](#) and click **Instances** on the left sidebar.
2. Click the drop-down list in the top left corner to switch regions.
3. In the search box, search for the blocked server by instance name, ID, or status.
4. Click **Log In** on the right of the blocked server to display the **Log in to Linux Instance** pop-up window.
5. In the pop-up window, select **Login over VNC** and click **Log In Now** to connect to the server via browser VNC.

Alert Service

Setting Security Event Notifications

Last updated : 2024-07-01 11:33:59

You can configure policies in the [Message Center](#) to receive messages for the following events.

An attack starts.

An attack ends for 15 minutes.

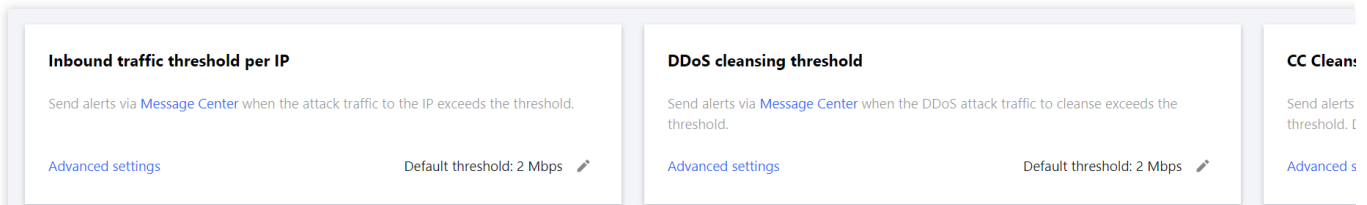
An IP is blocked.

An IP is unblocked.

You can modify the recipients and how they receive the messages as needed.

Directions

1. Log in to the [Anti-DDoS console](#) and click **Alerts** on the left sidebar.
2. You can now set the **inbound traffic threshold per IP**, **DDoS cleansing threshold**, and **CC cleansing threshold**.



3. Click **Advanced settings** in each section to enter the alarm setting list and set different thresholds for each instance.

Set the inbound traffic threshold per IP.

<input type="checkbox"/> Resource instance	Bound IP	Inbound traffic alarm threshold (Mbps)
<input type="checkbox"/> [blurred]	[blurred]	2
<input type="checkbox"/> [blurred]	[blurred]	2

Set the DDoS cleansing threshold.

Batch modify

<input type="checkbox"/> Resource instance	Bound IP	DDoS cleansing threshold (Mbps)
<input type="checkbox"/> [REDACTED]	[REDACTED]	2
<input type="checkbox"/> [REDACTED]	[REDACTED]	2

Set the CC cleansing alarm.

Batch modify

<input type="checkbox"/> Resource instance	Bound IP	Cleansing Threshold (in QPS)
<input type="checkbox"/> bgp-00000fj8	43.152.105.135	2
<input type="checkbox"/> bgp-00000fj6	114.117.128.21	2

Setting Notification Methods

Last updated : 2024-07-01 11:33:59

1. Log in to your Tencent Cloud account and go to the [message center](#).

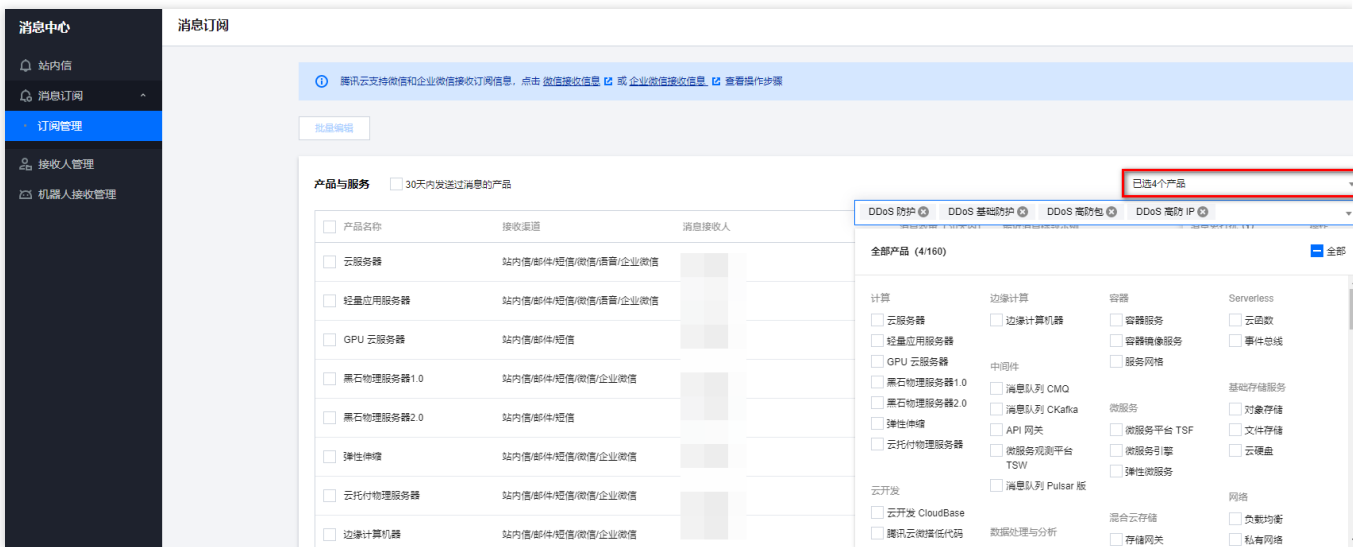
Note:

You can also log in to the [console](#), click



in the top right corner, and click **View more** to enter the message center.

2. In the left sidebar, click **Message Subscription > Subscription Management**, and then select the products that you want to receive messages about.



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



4. In the pop-up window, set message recipients and click **OK**.

订阅编辑

① 邮箱、手机、微信未验证的用户将无法接收邮件、短信、语音、微信消息，验证通过并开启对应接收方式后即可接收。非企业微信子用户无法接收企业微信消息，企业微信子用户且在腾讯云助手应用的成员可见范围内方可接收企业微信消息。

产品名称 DDoS 高防 IP

接收模式 免打扰

开启后，该产品的短信、语音、微信消息将无法接收，站内信、邮件、企业微信消息正常接收（勾选该消息通道时），免打扰模式下，无法编辑消息接收人及消息通道

接收渠道 站内信 邮件 短信 微信 语音 企业微信

消息接收人

用户 用户组 IM应用 机器人

[新增消息接收人](#) [修改接收人联系方式](#)

已选择(1)

搜索用户名称

<input checked="" type="checkbox"/>	用户名称	用户类型	手机号码	邮箱	微信
<input checked="" type="checkbox"/>	主账号		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> 已验证

接收人名称	接收人类型
	主账号 <input type="button" value="X"/>

定制化配置产品信息 点击进入 [高级编辑模式](#)